République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane MIRA de Béjaïa
Faculté des Sciences Exacte
Département d'Informatique

MEMOIRE DE FIN DE CYCLE

En vue d'obtention du diplôme de Master professionnel en Informatique
Spécialité : Administration et Sécurité des Réseaux

THEME

Mise en place d'un pare-feu d'entreprise open source PfSense

Présenté par :

BOUCHERBA Khadidja

ZIANE Saloua

Encadré par :

Pr. BOUKERRAM Abdellah

Membres du jury :

Président: M^me^ HAMZA Lamia

Examinateur[1]: M^me^ AIT KACI AZZOU Samia

-Promotion 2015-

Remerciements

Nous tenons à saisir cette occasion et adresser nos sincères remerciements et nos profondes reconnaissances à Dieu le tout puissant et miséricordieux qui nous a donné la force et la patience d'accomplir ce travail.

Nous tenons à remercier Pr A. Boukerram notre promoteur pour ses précieux conseils et son orientation ficelée tout au long de notre recherche, et à remercier notre encadreur Mr L. Benali pour leurs aides précieux durant la période de notre stage. Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions. Enfin, nous tenons également à remercier toutes nos familles et nos ami(e)s et tous ceux qui ont participé de prés ou de loin à la réalisation de ce travail.

Dédicaces

On a le plaisir de dédier ce travail reflétant notre effort consenti durant le cursus universitaire à :

Nos chers parents, pour lesquels nulle dédicace ne peut exprimer nos sincères sentiments, pour leur patience illimitée, leurs encouragements continus, leur aide, en témoignage de nos profond amour et respect pour leurs grands sacrifices.

A nos chers frères et sœurs pour leur grand amour et leur soutien; qu'ils trouvent ici l'expression de notre haute gratitude.

A Toutes nos familles sans exception, à tous nos chers amis(e) pour leurs encouragements, et à tous ceux qu'on aime.

A tous nos enseignants.

A tous le personnel du département Informatique.

A toutes les personnes qui nous ont apporté de l'aide.

TABLE DES MATIÈRES

CHAPITRE IV: Réalisation

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS

ACL : Access Control List

BMT : Bejaia Méditerranéen Terminal

DMZ : Demilitarised Zone

DNS : Domain Name Server

EPB : Entreprise Portuaire de Bejaia

FTP : File Transfer Protocol

HTTP : Hyper Text Transfer Protocol

LAN : Local Area Network

NAT : Network Address Translation

NTP : Network Time Protocol

PfSense : Packet Filter Sense

TCP : Transfer Control Protocol

UDP : User Datagram Protocol

URL : Uniform Resource Locator

VPN : Virtual Private Network

WAN : Wide Area Network

Introduction générale

Le développement du réseau Internet, et de ses déclinaisons sous forme d'Intranets et d'Extranets, soulève des questions essentielles en matière de sécurité informatique. L'accroissement des trafics en télécommunication révèlent les besoins grandissants d'échanges privés et professionnels. Ces transmissions de données imposent une ouverture des systèmes d'information vers l'extérieur, notamment vers Internet. Celle-ci entraine une certaine dépendance des entreprises et des personnes vis-à-vis des services qu'offre Internet. Ainsi conjuguées, cette ouverture et cette dépendance rendent l'entreprise vulnérable aux risques. C'est pour cela que la sécurité Internet est devenue un sujet de recherche très intense. Ces recherches ont permis le développement de certaines dispositifs de sécurité comme les pare-feux, les antivirus et les systèmes de cryptographie pour protéger les systèmes informatiques.

Vu l'importance et l'obligation de l'élaboration d'un pare-feu, chaque organisme doit établir un pare-feu pour la sécurité informatique afin d'identifier les sources de menace et ses dégâts informationnels.

C'est dans cette optique que s'inscrit notre travail: établir un Pare-feu de sécurisation d'un réseau informatique.

Un pare-feu, appelé aussi ‘‘coupe-feu’’, ‘‘garde-barrière’’ ou ‘‘firewall’’ en anglais, est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers ou externe (Internet). Ce système permettant de filtrer les paquets de données échangés avec le réseau. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes :

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

Organisation du mémoire: ce mémoire s'articule autour de quatre principaux chapitres :

- Le premier chapitre, est un survol sur les généralités de la sécurité informatique, où on présente les outils nécessaires pour l'assurer,
- Le deuxième chapitre décrit brièvement les différentes architectures de pare-feu,

- Le troisième chapitre, comprend deux phase : une phase de l'analyse du projet, suivie d'une phase de conception qui définit l'installation et la configuration basique d'un pare-feu,
- Le dernier chapitre présente la phase de réalisation : clôturer la mise en place du pare-feu par le paramétrage de quelques packages qu'il présente.

Une conclusion générale reprenant les points forts de ce travail, termine ce mémoire, suivie de perspectives futures.

CHAPITRE I

GÉNÉRALITÉS

Introduction

Chaque ordinateur connecté à Internet et d'une manière plus générale à n'importe quel réseau informatique, est susceptible d'être victime d'une attaque d'un pirate informatique. Ainsi, il est nécessaire de se protéger de ces attaques réseaux en installant un dispositif de protection.

Dans ce chapitre, nous faisons un survol des notions de sécurité informatique, et nous allons montrer les moyens et les dispositifs de sécurité utilisés pour l'assurer. Nous étudierons en particulier, les Pare-feux, les Proxys et les VPNs (réseaux privés virtuels).

I .1. Le système d'information et la sécurité [1]

1. Présentation

Le système d'information représente l'ensemble des données de l'entreprise ainsi que ses infrastructures matérielles et logicielles. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à s'assurer que les ressources matérielles et logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité** qui garantit que les données sont bien celles que l'on croit être, qu'elles non pas été altérées durant la communication (de manière fortuite ou intentionnelle),
- **La confidentialité** qui consiste à rendre l'information inintelligible à d'autres personnes, autres que les seuls acteurs de la transaction,
- **La disponibilité** qui permet de garantir l'accès à un service ou à des ressources,
- **La non-répudiation** de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction,
- **L'authentification** qui consiste à assurer l'identité d'un utilisateur, c'est-à-dire a garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

2. Nécessité d'une approche globale

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivant :

- **La sensibilisation** des utilisateurs aux problèmes de sécurité,
- **La sécurité logique :** c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation,
- **La sécurité des télécommunications :** technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.,
- **La sécurité physique :** soit la sécurité au niveau des infrastructures matérielles.

3. Mise en place d'une politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droit d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des ressources possèdent uniquement les droits qui leur ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences,
- Elaborer des règles et des procédures à mettre en ouvre dans les différents services de l'organisation pour les risques identifiés,
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés,

- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation en matière de sécurité.

I.2. Les attaques informatiques [1]

1. Présentation

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une **attaque** est l'exploitation d'une faille (vulnérabilité ou brèche) d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plus part lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de **pirates informatiques**.

Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mieux s'y préparer.

Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système,
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles,
- Glaner des informations personnelles sur un utilisateur,
- Récupérer des données bancaires,
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.),
- Troubler le bon fonctionnement d'un service,
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée, etc.

2. Types d'attaques

Il est ainsi possible de catégoriser les risques de la manière suivante :

- **Accès physique :** il s'agit d'un cas où l'attaquant a accès aux locaux, éventuellement même aux machines :
  - ✓ Coupure de l'électricité,
  - ✓ Extinction manuelle de l'ordinateur,
  - ✓ Vandalisme,
  - ✓ Ouverture du boîtier de l'ordinateur et vol de disque dur,
  - ✓ Ecoute du trafic sur le réseau,
  - ✓ Ajout d'éléments (clé USB, point d'accès Wifi……).
- **Interception de communications :**
  - ✓ Vol de session,
  - ✓ Usurpation d'identité,
  - ✓ Détournement ou altération de messages.
- **Dénis de service :** il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
  - ✓ Exploitation de faiblesses des protocoles TCP/IP,
  - ✓ Exploitation de vulnérabilité des logiciels serveurs.
- **Intrusions :**
  - ✓ Balayage de ports,
  - ✓ Elévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application,
  - ✓ Maliciels : (virus, vers, et chevaux de Troie).
- **Ingénierie sociale :** dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! en effet, c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique.
- **Trappes :** il s'agit d'une porte dérobée dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur.

I.3. Les dispositifs de protection

Il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des attaques réseaux en installant un dispositif de protection (Pare-feux, antivirus, réseaux privés virtuels, systèmes de

détection d'intrusions, Proxys, etc.) permettant d'ajouter un niveau de sécurisation supplémentaire [1]**.**

I.3.1. Pare-feu

1. Présentation

Un **Pare-feu** [appelé aussi Coupe-feu, Garde-barrière ou **Firewall**], est un système permettant de protéger un ordinateur, ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers [notamment Internet]. Le Pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau (cartes réseau) suivantes :

- Une interface pour le réseau à protéger (réseau interne),
- Une interface pour le réseau externe [1].

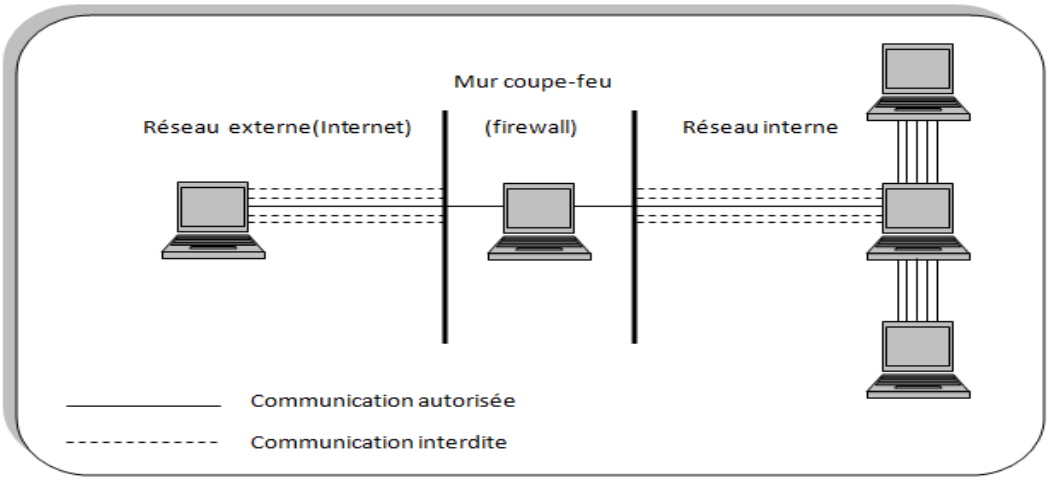

Figure I.1: Pare-feu

La configuration du Firewall est telle que les données arrivant sur l'une des cartes ne soient pas transmises directement sur l'autre mais de manière sélective, selon des critères de filtrage déterminés lors de sa configuration [2].

Le filtrage réalisé par le Pare-feu constitue le premier rempart de la protection du système d'information.

Le système Pare-feu est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local [ou la machine local] et un ou

plusieurs réseaux externes. Il est possible de mettre un système Pare-feu sur n'importe qu'elle machine et avec n'importe quel système pourvu que :

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

Dans le cas où le système Pare-feu est fourni dans une boîte noire << clé en main>>, on utilise le terme d'**Appliance** [1].

Selon la nature de l'analyse et de traitements effectués par un Firewall, différents types de Firewalls existent. Ils se distinguent le plus souvent en fonction du niveau de filtrage des données auquel ils opèrent : niveau 3 (IP), niveau 4 (TCP, UDP) ou niveau 7 (FTP, HTTP, etc.) du modèle OSI. Dans le cas de la fonction du routeur (Firewall routeur), il analyse chaque paquet de données selon les informations contenant dans le paquet (adresses IP, numéro de port, type de paquet).

Les Pare-feu de base opèrent sur un faible nombre de couches du modèle TCP/IP, tandis que les plus sophistiqués en couvrent un plus grand nombre et sont ainsi plus efficaces

Indépendamment ou en complément d'une architecture utilisant ces dispositifs, il existe des services additionnels tels : la traduction d'adresse réseau (NAT) et les réseaux privés virtuels (VPN) [3].

2. Principe de fonctionnement

Un système Pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion [allow],
- De bloquer la connexion [deny],
- De rejeter la demande de connexion sans avertir l'émetteur [drop].

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

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : « tout ce qui n'est pas explicitement autorisé est interdit »,
- Soit d'empêcher les échanges qui ont été explicitement interdites.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication [1].

3. Les différents types de filtrage [1]

- **Filtrage simple de paquets**

Un système Pare-feu fonctionne sur le principe du **filtrage simple de paquets** (stateless packet filtring). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangés entre une machine du réseau extérieur et une machine du réseau interne transitent par le Pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le Firewall :

- Adresse IP de la machine émettrice,
- Adresse IP de la machine réceptrice,
- Type de paquet (TCP, UDP, etc.),
- Numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

- **Filtrage dynamique**

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine client.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir des ports à laisser passer ou à interdire. Pour y remédier, le système de **filtrage dynamique de paquets** est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Le terme anglosaxon est **stateful inspection** ou stateful paket filtring, se traduit en français par « filtrage de paquets avec état ».

Un dispositif Pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre coté du Pare-feu. L'ensemble des paquets transitant dans le cadre de cette connexion sont implicitement acceptés par le Pare-feu.

- **Filtrage applicatif**

Le filtrage applicatif permet comme son nom l'indique de filtrer les communications application par application. Ce filtrage opère donc au niveau 7 (couche application) du modèle OSI. Le filtrage applicatif suppose donc, une connaissance des applications présentes sur le réseau, et notamment de la manière dont les données sont échangées (ports, etc.).

Un Firewall effectuant un filtrage applicatif est appelé généralement **passerelle applicative (ou Proxy),** car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés.

Le Proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes, précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

Par ailleurs, le Proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et connaître les failles afférentes pour être efficace.

Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy, afin de limiter les risques de compromission.

4. Pare-feu personnel

Dans le cas où la zone protégée se limite à l'ordinateur sur lequel le firewall est installé on parle de **Firewall personnel** (pare-feu personnel).

Ainsi, un Firewall personnel permet de contrôler l'accès au réseau des applications installées sur la machine, et notamment empêcher les attaques du type cheval de Troie, c'est-à-dire des programmes nuisibles ouvrant une brèche dans le système afin de permettre une prise en main à distance de la machine par un pirate informatique.

Le Firewall personnel permet en effet de repérer et d'empêcher l'ouverture non sollicitée de la part d'applications non autorisées à se connecter [1].

5. Zone démilitarisée (DMZ)

Les systèmes Pare-feu (Firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes.

C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de **cloisonnement des réseaux** (le terme isolation est parfois également utilisé).

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, serveur de messagerie, serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.

On parle ainsi de **Zone démilitarisée** (notée **DMZ**, Demilitarised Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

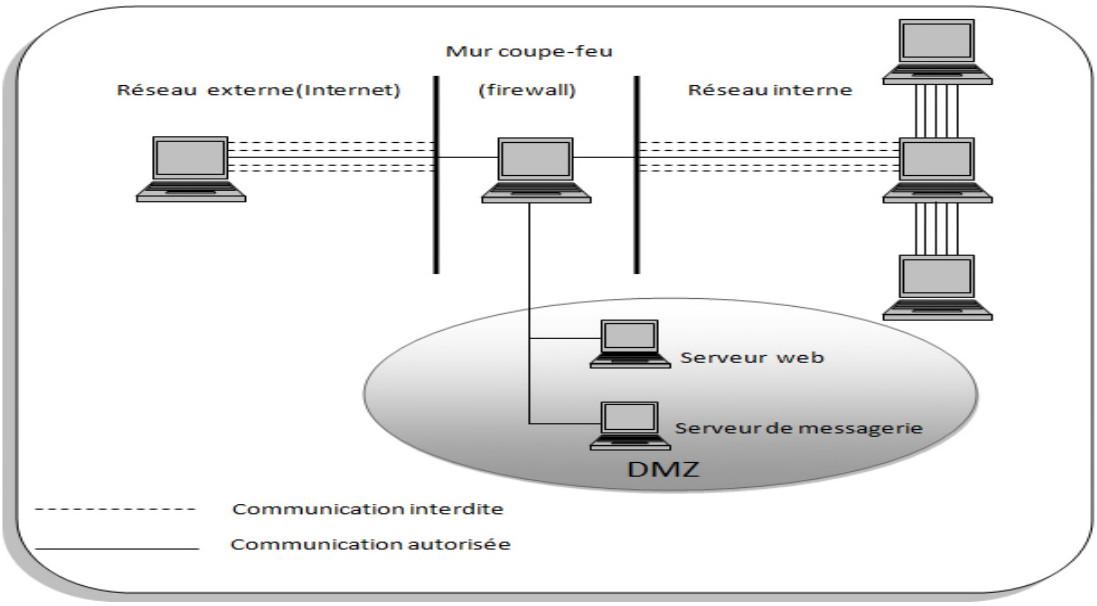

Figure I.2: Exemple d'une zone démilitarisée (DMZ)

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- trafic du réseau externe vers la DMZ autorisé,
- trafic du réseau externe vers le réseau interne interdit,
- trafic du réseau interne vers la DMZ autorisé,
- trafic du réseau interne vers le réseau externe autorisé,
- trafic de la DMZ vers le réseau interne interdit,
- trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques de l'entreprise [1].

6. Les limites de système Pare-feu

Un système Pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du Pare-feu.

De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.

Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le Pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies. Par ailleurs, il est recommandé d'effectuer une **veille de sécurité** (en s'abonnant aux alertes de sécurité) afin de modifier le paramétrage de son dispositif en fonction de la publication des alertes.

La mise en place d'un Firewall doit donc se faire en accord avec une véritable politique de sécurité [1].

7. Le choix d'un Firewall pour l'entreprise

La façon de configurer un Firewall et de le gérer est tout aussi importante que les capacités intrinsèques qu'il possède.

Toutefois, lorsque le choix s'impose, on prendra en considération les critères suivants :

- La nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, vidéoconférence, etc.),
- Type de filtres, niveau de filtrage (niveau applicatif, niveau TCP, niveau IP, possibilité de combiner ces niveaux),
- Facilités d'enregistrement des actions et des événements pour audits future,
- Les outils et facilités d'administration (interface graphique ou lignes de commandes, administration distante après authentification de gestionnaire, etc.),
- Simplicité de configuration et de mise en œuvre,
- Sa capacité à supporter un tunnel chiffré permettant éventuellement de réaliser un réseau privé virtuel (VPN pour Virtuel Private Network),
- La disponibilité d'outils de surveillance, d'alarmes, d'audit actif,
- Possibilité d'équilibrage de charges et de gestion de la bande passante de réseau,
- L'existence dans l'entreprise de compétences en matière d'administration du système d'exploitation du firewall,
- Son prix [2], [3].

8. Recommandations

Sans vouloir être exhaustive, voici quelques directives contribuant à sécuriser un environnement Internet :

- Un Firewall doit être protégé et sécurisé contre des accès non autorisés (notion de système de confiance possédant un système d'exploitation sécurisé),
- Tous les trafics entrants et sortants doivent passer par le Firewall,
- Seul le trafic défini par la politique de sécurité comme étant valide et autorisé peut traverser le Firewall,
- Si les données du réseau interne sont vraiment sensibles, il faut alors accéder à Internet par des machines détachées du réseau interne,
- Un Firewall ne peut pas protéger l'environnement à sécuriser contre des attaques ou des accès illicites qui ne passent pas par lui. Il n'est d'aucune efficacité en ce qui concerne des délits perpétrés à l'intérieur de l'entreprise,
- Un Firewall n'est pas un anti-virus, il faut donc le protéger de manière complémentaire contre des infections virales [2].

I.3.2. Serveurs mandataires (Proxy)

1. Présentation

Un serveur Proxy, appelé aussi serveur mandataire est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local, utilisant parfois des protocoles autre que le protocole TCP/IP et Internet.

La plupart du temps le serveur Proxy est utilisé pour le web, il s'agit alors d'un Proxy HTTP. Toutefois il peut exister des serveurs Proxy pour chaque protocole applicatif (FTP, etc.) [1].

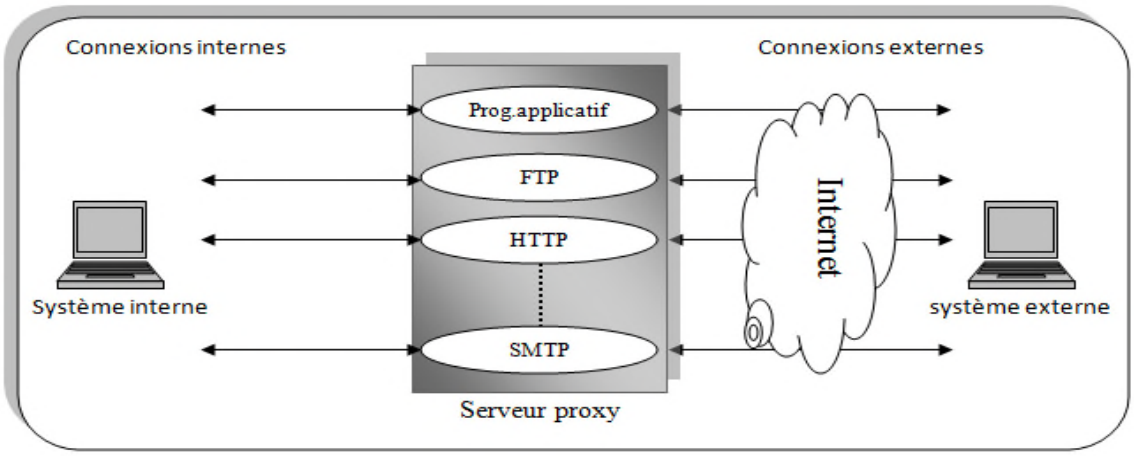

Figure I.3: Architecture d'un Proxy

2. Principe de fonctionnement

Le principe de fonctionnement d'un serveur Proxy est assez simple : il établit en lieu et place de l'utilisateur le service invoqué par celui-ci (FTP, etc.) (Figure I.3). Ainsi lorsqu'un utilisateur se connecte à l'aide d'une application cliente configurée pour utiliser un serveur Proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur Proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête (le serveur Proxy contacte le serveur externe sollicité sur internet avec sa propre adresse ou une adresse issue d'un pool d'adresses IP libres). Le serveur va ensuite donner sa réponse au Proxy, qui va à son tour la transmettre à l'application cliente [1]. Le Proxy cache de la sorte toute l'infrastructure du réseau local et ne dévoile en aucun cas les adresses des machines internes (masquage d'adresse) [2].

3. Fonctionnalités d'un serveur Proxy

Avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Les serveurs Proxys sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités [1].

- **Cache**

La plus part des Proxys assurent ainsi une fonction de **cache** (caching), c'est-à-dire la capacité à garder en mémoire (en « cache ») les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible. En

effet, en informatique, le terme de « cache » désigne un espace de stockage temporaire de données (le terme de « tampon » est également parfois utilisé).

Un serveur Proxy ayant la possibilité de cacher (néologisme signifiant « mettre en mémoire cache ») les informations est généralement appelé **serveur Proxy-cache**.

Cette fonctionnalité implémentée dans certains serveurs Proxys permet d'une part de réduire l'utilisation de la bande passante vers Internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs.

Toutefois, pour mener à bien cette mission, il est nécessaire que le Proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

- **Filtrage**

D'autre part, grâce à l'utilisation d'un Proxy, il est possible d'assurer un suivi des connections via la constitution des journaux d'activités (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de **filtrer les connexions** à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs.

Le filtrage basé sur l'adresse des ressources consultées est appelé **filtrage d'URL.**

Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de **liste blanche**, lorsqu'il s'agit d'une liste de sites interdits on parle de **liste noire**.

En fin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés….) est appelée **filtrage de contenu.**

- **Authentification**

Dans la mesure où le Proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour **authentifier les utilisateurs**, c'est–à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans

les fichiers journaux des accès identifiés. Ce type de mécanisme lorsqu'il est mise en œuvre pose bien évidement de nombreux problèmes relatifs aux libertés individuelles et aux droits des personnes.

4. Translation d'adresses (NAT)

Son principe consiste à modifier l'adresse IP source ou destination, dans l'en-tête d'un datagramme IP lorsque le paquet transite dans le Pare-feu (Proxy) en fonction de l'adresse source ou destination et du port source ou destination.

Lors de cette opération, le Pare-feu garde en mémoire l'information lui permettant d'appliquer la transformation inverse sur le paquet de retour. La traduction d'adresse permet de masquer le plan d'adressage interne (non routable) à l'entreprise par une ou plusieurs adresses routables sur le réseau externe ou sur Internet. Cette technologie permet donc de cacher le schéma d'adressage réseau présent dans une entreprise derrière un environnement protégé [3].

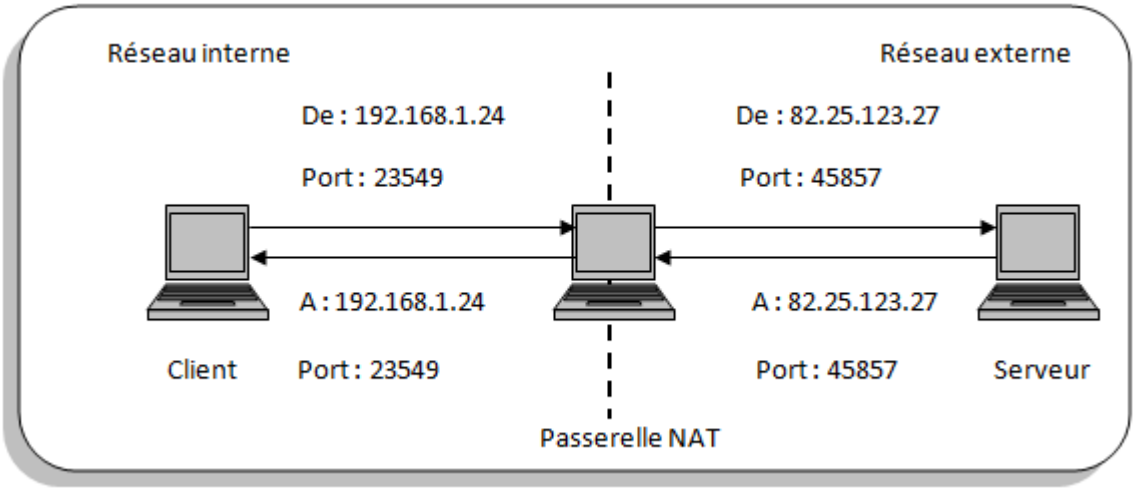

Figure I.4: Translation d'adresses (NAT)

- **Translation statique**

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

La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à Internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où *n* adresses IP routable sont nécessaires pour connecter *n* machines du réseau interne [1].

- **Translation dynamique**

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (PAT, Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP de la passerelle [1].

5. Reverse Proxy

On appelle Reverse-Proxy (en français le terme de relais inverse est parfois employé) un serveur Proxy-cache « monté à l'inverse », c'est-à-dire un serveur Proxy permettant non pas aux utilisateurs d'accéder au réseau Internet, mais aux utilisateurs d'internet d'accéder indirectement à certains serveurs internes.

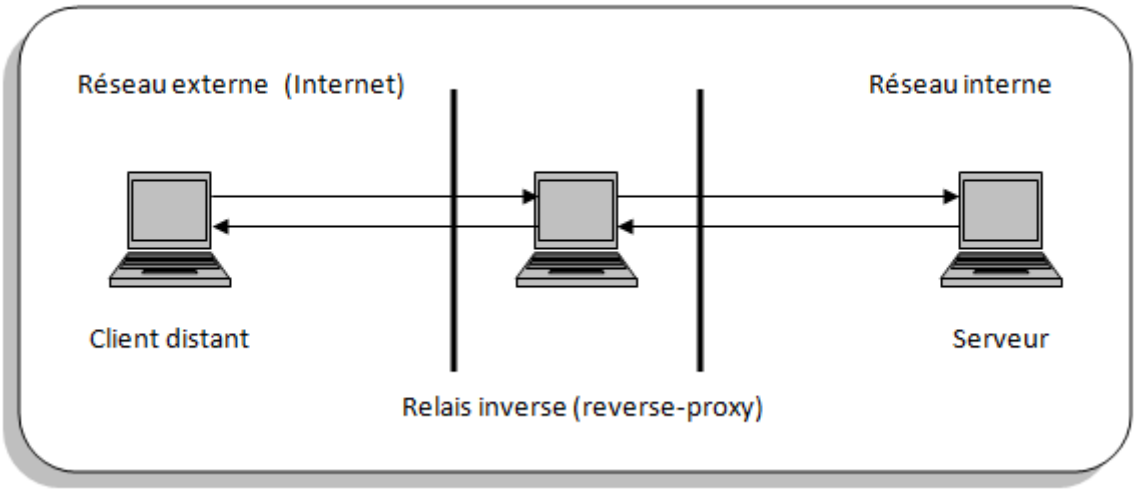

Figure I.5: Reverse-Proxy

Le Reverse-Proxy sert ainsi de relais pour les utilisateurs d'Internet souhaitant accéder à un site web interne en lui transmettant indirectement les requêtes. Grâce au Reverse-Proxy, le serveur web est protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne. D'autre part, la fonction du cache du reverse-Proxy peut permettre de soulager la charge du serveur pour lequel il est prévu, c'est la raison pour laquelle un tel serveur est parfois appelé « accélérateur », (server accelerator).

Enfin, grâce à des algorithmes perfectionnés, le Reverse-Proxy peut servir à répartir la charge en redirigeant les requêtes vers différents serveurs équivalents ; on parle alors de **répartition de charge**, (load balancing) [1].

I.3.3. Réseaux privés virtuels

1. Présentation

Il arrive ainsi souvent que les entreprises éprouvent le besoin de communiquer avec les filiales, des clients ou même du personnel géographiquement éloignées via internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi, il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La solution consiste à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation (**tunneling**), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de **réseau privé virtuel** (noté **RPV** ou **VPN**, Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit **virtuel** car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et **privé** car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données [1].

2. Mise en œuvre de liaisons sécurisées

L'échange de données confidentielles entre les personnels nomades et l'entreprise ou entre différentes entités implique la mise en œuvre de liaisons sécurisées, physiques (lignes louées spécialisées) ou virtuelles (VPN) en liaison avec un Pare-feu.

Trois types de solutions de VPN existent associées avec un Pare-feu :

- Intégrée comme service du Pare-feu,
- Systèmes autonomes placés devant le Pare-feu,
- Systèmes autonomes placés derrière le Pare-feu (solutions logicielles).

L'échange de données entre sites distants de la même entreprise peut aussi être effectué en utilisant une liaison spécialisée ou dédiée utilisant les services d'un opérateur de télécommunication. Cette solution permet de s'affranchir de toutes les menaces liées à l'utilisation du réseau Internet, mais elle représente un coût plus important [3].

3. Fonctionnement d'un VPN

Un réseau privé virtuel repose sur un protocole, appelé **protocole de tunneling**, c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

L'expression **tunnel chiffré** est utilisée pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle **client VPN** l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et **serveur VPN** (ou plus généralement **serveur d'accès distant**) l'élément chiffrant et déchiffrant les données du coté de l'organisation.

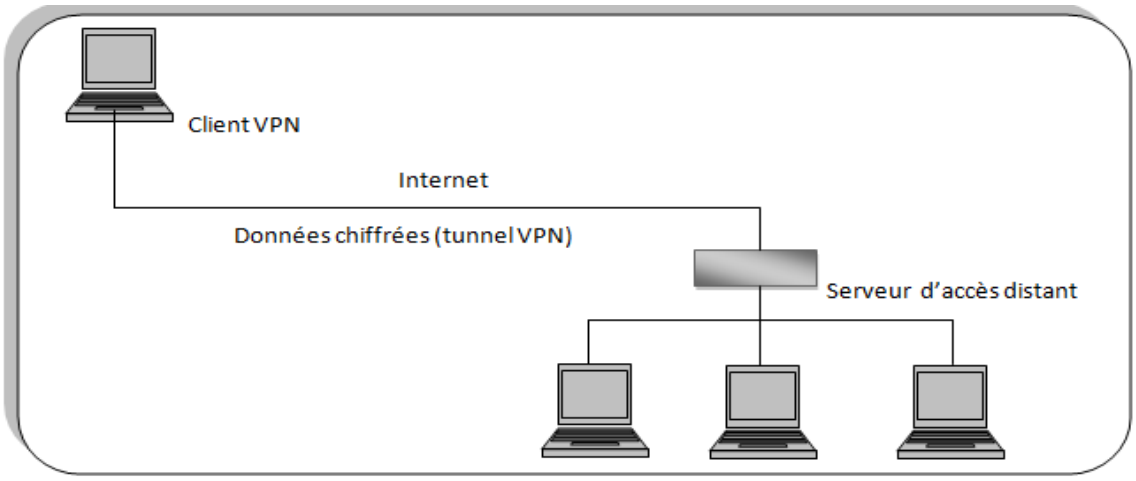

Figure I.6: Réseau privé virtuel (VPN)

De cette façon, lorsqu'un utilisateur a besoin d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée.

L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur [1].

4. Protocoles de tunneling

Les principaux protocoles de tunneling sont les suivants :

- ✓ **PPTP** (point-to-point tunneling protocol) est un protocole de niveau 2 développé par Microsoft, 3 Com, Ascend, US Robotics et ECI Telematics,
- ✓ **L2F** (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi obsolète,
- ✓ **L2TP** (Layer Two Tunneling Protocole) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2,
- ✓ **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP [1].

Conclusion

La sécurité des réseaux informatiques est un sujet d'actualité. Ces systèmes sont trop ouverts, avec le grand nombre de réseaux que constitue Internet, ce qui fait que la sécurité de ces réseaux n'est pas totalement garantie. Les Pare-feux, les Proxys et les réseaux privés virtuels sont des outils développés et utilisés pour renforcer davantage cette idée de sécurité. Pour définir des mécanismes de sécurisation, il est nécessaire de définir avant tout, les objectifs de sécurité, pour obtenir tant que possible une sécurisation assez fiable de réseaux.

CHAPITRE II

ARCHITECTURES DE FIREWALL

Introduction

Le terme de " Firewall " est un terme qui parfois prête à confusion. En effet, il regroupe tous les systèmes de sécurité qui fonctionnent en connexion avec un réseau. Il en existe différents types d'architectures que nous allons étudier.

II.1. Analyse technique préalable

La mise en activité d'un environnement Firewall doit impérativement s'accompagner d'une réflexion à propos de l'objectif que l'on veut réellement atteindre, de la politique de sécurité et d'utilisation du réseau que l'établissement souhaite voir respectée, ainsi que des moyens que l'on est prêt à y mettre. Il faut que la politique de sécurité soit acceptée par tous, sinon, on tentera de la contourner, avec les conséquences que l'on peut imaginer.

Ce n'est qu'une fois cette politique définie, dans ses grandes lignes que le choix de solutions techniques et organisationnelles peut être opéré. Ceci pour dire que ce n'est pas la technologie qui doit imposer une politique de sécurité, mais plutôt c'est la politique de sécurité qui doit dicter les solutions.

De nombreux constructeurs proposent leurs solutions, et parfois, les moins onéreuses ne sont pas les plus mauvaises. D'autre part ce choix devra également prendre en compte le niveau des ressources humaines disponibles, pour l'installation, la configuration et la maintenance du produit.

Les produits de sécurité nécessitent un investissement de départ pour l'installation, mais également un suivi constant. L'engagement doit en être pris dès le départ. Ainsi du temps «d'administrateurs compétents et rigoureux» doit être prévu pour le suivi de l'exploitation.

Il faut donc trouver une solution adaptée aux besoins, aux moyens, à l'environnement, et à la culture de l'entreprise.

Grâce à cette analyse on pourra connaître les avantages, les inconvénients ainsi que le fonctionnement des différentes architectures de Firewall.

II.2. Types d'architectures

Le Firewall n'est pas seulement une solution logicielle de sécurité implantée sur une machine, c'est aussi une architecture réseau de machines filtrantes.

L'approche simpliste d'un Firewall localisé sur une machine jouant le rôle de grand chef d'orchestre n'a plus cours à présent dans les grandes entreprises, car elle est trop peu sécurisée en cas de panne ou faille dans cette unique défense.

La mise en place de plusieurs filtres de différents niveaux assurent une meilleure sécurité du réseau, mais ils s'accompagnent d'un coût plus élevé.

1. Firewall avec routeur de filtrage

La solution Firewall la plus simple, mais aussi la moins sûre, se borne au réseau. On l'obtient en configurant le routeur qui assure la connexion avec l'Internet [8]. Le routeur doit être configuré avec une liste d'accès. L'image suivante illustre cette solution appelée Firewall avec routeur de filtrage :

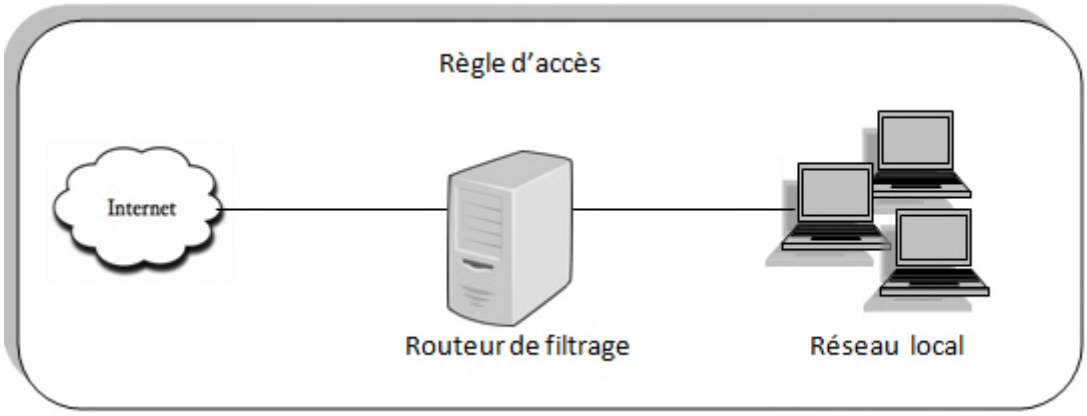

Figure II.1: Firewall avec routeur de filtrage

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

- les adresses IP, les numéros de ports,
- D'autres informations dans le paquet comme les drapeaux TCP,

- le type de la règle, c'est-à-dire soit une autorisation soit un refus de faire traverser le paquet.

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

Avantages : facilité de configuration, bon marché, de plus il fournit des traces exploitables avec la possibilité d'alarmes pour :

- Une vérification du bon fonctionnement des filtres du routeur,
- Il y ait encore un peu de temps pour réagir si le routeur est compromis.

Inconvénients : lorsque le routeur est contourné ou paralysé, le réseau entier est ouvert.

Exemples :

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

Règles	Action	Protocole	Source		Destination	
			Adresse	Port	Adresse	Port
1	Autoriser	TCP	*	*	Serveur	80
2	Autoriser	TCP	Serveur	80	*	*
3	Interdit	*	*	*	*	*

Liste d'accès n°1

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

- La règle 2 est symétrique de la première. Elle autorise le routeur à laisser passer les réponses du serveur au client distant.
- La règle 3 empêche tout autre paquet de traverser le routeur. Elle permet d'appliquer la philosophie : tout ce qui n'est pas explicitement autorisé est interdit.

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

Règles	Action	Protocole	Source		Destination	
			Adresse	Port	Adresse	Port
1	Autoriser	TCP	*	*	Serveur	80
2	Autoriser	TCP	Serveur	80	*	*
3	Autoriser	TCP	{Site}	*	*	80
4	Autoriser	TCP	*	80	{Site}	*
5	Interdit	*	*	*	*	*

Liste d'accès n°2

- Ces deux nouvelles règles (3 et 4) permettent aux équipements internes d'émettre vers l'extérieur des paquets ayant comme port de destination le numéro 80 et de recevoir de l'extérieur des paquets ayant pour source le port 80. L'ensemble des machines du site (représentées par {site}) peuvent être données en listant les numéros de réseaux du site [9].

2. Passerelle double- le réseau bastion

Il existe une autre possibilité permettant de réaliser un Firewall d'application à peu de frais : la passerelle double. Comme son nom l'indique, il s'agit d'un ordinateur inclus à la fois dans les deux réseaux Internet et Intranet. Cette machine doit être équipée de deux cartes réseau. Comme elle est la seule soupape de sécurité entre les deux réseaux, elle doit être configurée avec le plus grand soin.

La passerelle double n'autorise aucun trafic IP entre les réseaux. On l'appelle également réseau bastion, car il contrôle tous les services accessibles de l'extérieur comme de l'intérieur du réseau interne tels que les serveurs Web, FTP et Mail. Un " Serveur Proxy " supplémentaire est également configuré pour permettre aux utilisateurs du réseau interne

d'accéder à Internet. Le nom "réseau bastion" découle des mesures particulières de protection qui sont prises en prévision de possibles intrusions.

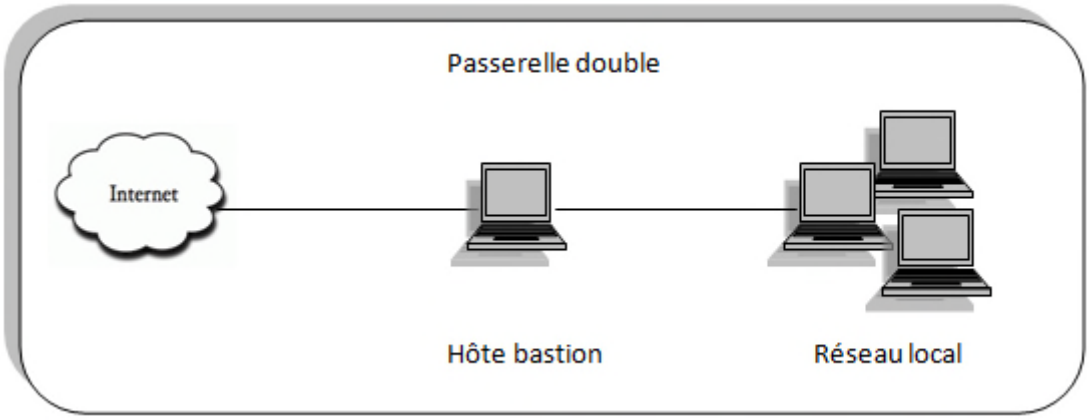

Figure II.2: La passerelle double

La passerelle double est la possibilité la plus simple pour réaliser un Firewall d'application n'autorisant aucun trafic IP entre les réseaux.

Avantages : bon marché.

Inconvénients : du fait de tout ce qu'elle doit faire (routage et application), une telle configuration pourrait rencontrer des problèmes de performance.

- s'ils parviennent à s'introduire sur le réseau bastion par logiciel, les pirates peuvent accéder au réseau tout entier (car c'est le seul rempart contre l'adversité) [8].

3. Firewalls avec réseau de filtrage

La combinaison des deux méthodes est ici plus sûre et efficace. Au niveau du réseau, un routeur sous écran est configuré de façon à n'autoriser les accès de l'extérieur et de l'intérieur que par l'intermédiaire du réseau bastion sur lequel fonctionnent tous les serveurs assurant les serveurs Internet. Cette possibilité est appelée Firewall avec réseau de filtrage. L'image suivante illustre cette solution :

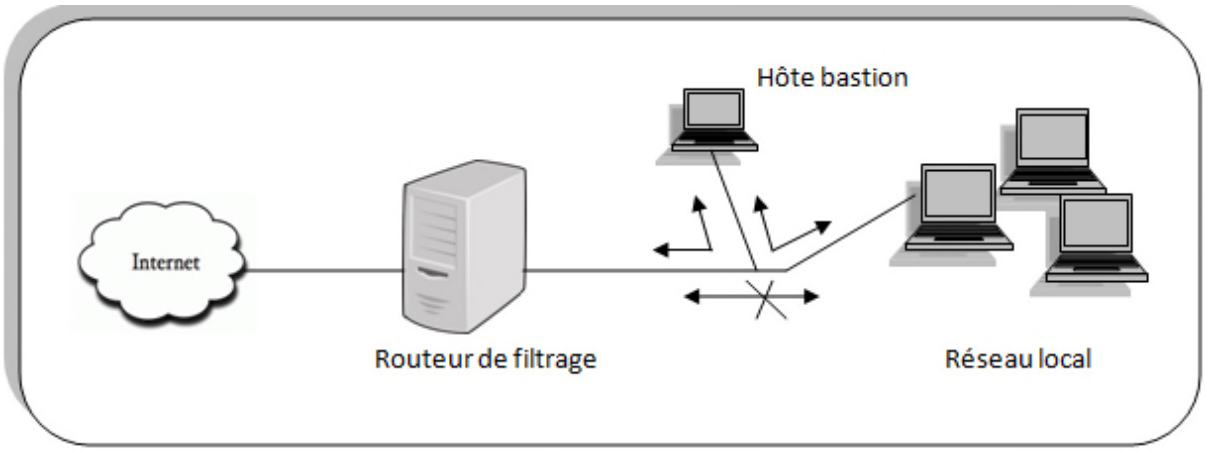

Figure II.3: Firewall avec réseau de filtrage

Firewall avec réseau de filtrage dans lequel seuls les accès au réseau bastion sont autorisés.

Pour la grande majorité des entreprises, cette solution est sûre et abordable, car les prestataires Internet assurent la seconde partie de la protection à l'autre bout de la ligne. En effet, votre entreprise y est également connectée à un routeur, et le trafic de données est réglé par un serveur Proxy au niveau de la couche application. Les pirates doivent par conséquent franchir deux obstacles.

Avantages : bon marché et sûr lorsque le prestataire est équipé en conséquence.

Inconvénients : le système comporte deux niveaux de sécurité distincts, le routeur et le réseau bastion. Si l'un des deux est paralysé, le réseau est menacé dans son intégralité [8].

4. Firewall avec sous-réseau de filtrage

Cette solution est de loin la plus sûre, mais également la plus onéreuse. Un Firewall avec sous-réseau de filtrage se compose de deux routeurs sous écran. L'un est connecté à Internet, et l'autre à l'intranet/LAN. Plusieurs réseaux bastions peuvent s'intercaler pour former entre ces deux routeurs, en quelque sorte, leur propre réseau constituant une zone tampon entre un Intranet et l'Internet appelée " zone démilitarisée ".

De l'extérieur, seul l'accès aux réseaux bastions est autorisé. Le trafic IP n'est pas directement transmis au réseau interne. De même, seuls les réseaux bastions, sur lesquels des

serveurs Proxy doivent être en service pour permettre l'accès à différents services Internet, sont accessibles à partir du réseau interne. L'image suivante illustre cette variante :

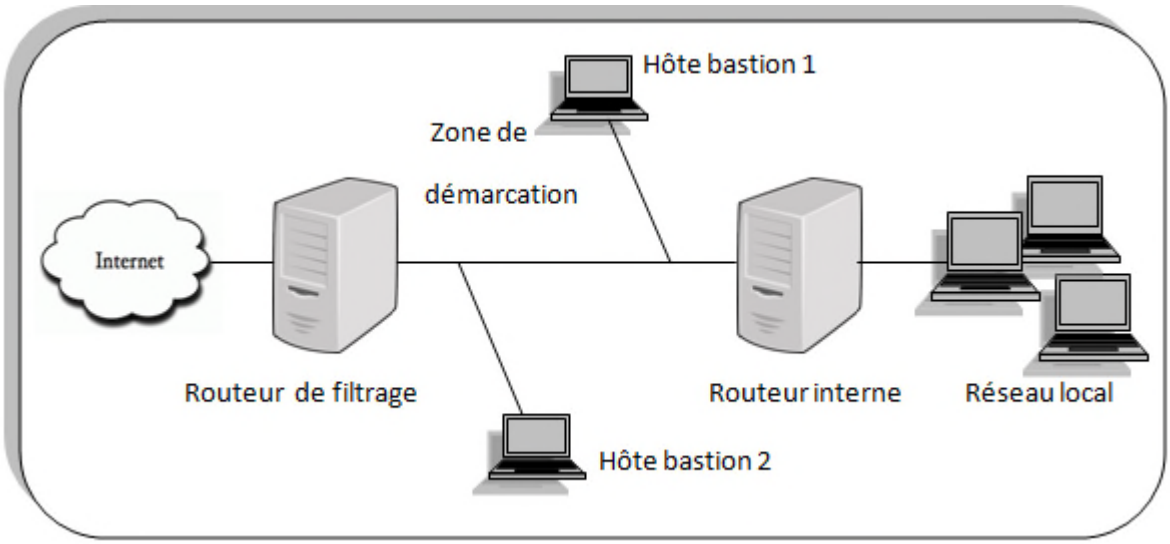

Figure II.4: Firewall avec sous-réseau de filtrage

Pour s'introduire sur le réseau d'entreprise à travers ce Firewall, il faut franchir les deux routeurs, ainsi que les réseaux bastions intercalés.

- Le Routeur interne :
  - Autorise le trafic entre le bastion 1 et les machines internes et inversement.
  - Interdit tout autre trafic.
- Le Routeur externe :
  - Filtre le trafic entre le monde extérieur et le bastion 2.
  - Interdit tout autre trafic direct (donc pas de trafic direct entre le réseau interne et l'extérieur).
- Les deux bastions peuvent discuter sans aucune règle => zone démilitarisée (DMZ).
- Le bastion interne :
  - Assure les fonctions de DNS vis à vis du réseau interne en envoyant ses requêtes au bastion externe.
  - Assure les fonctions de proxy avec authentification pour les applications distantes (Telnet, FTP, etc.).
  - Assure le relais du Mail sortant (SMTP).

- Le bastion externe :
    - Filtre au niveau applicatif les paquets en direction du réseau interne.
    - Assure le relais du Mail entrant.
    - Assure les fonctions de DNS vis à vis du réseau externe.

Avantages : système Firewall très sûr.

Inconvénients : coût d'investissement élevé, il faut fournir un effort d'installation, et d'administration important [8].

Conclusion

Il y'a plusieurs types d'architectures de Pare-feu, chacune d'elle présente ses inconvénients et ses avantages. Donc pour la mise en place d'une architecture Firewall on a toujours recours à revoir ces différentes architectures et choisir une selon les besoins, les moyens, et la politique de sécurité que l'entreprise souhaite voir respectée.

CHAPITRE III

ANALYSE ET CONCEPTION

Introduction

Dans ce chapitre nous présentons ; l'objectif du projet et l'analyse concurrentielle qui est une étape cruciale dans le choix du pare-feu à mettre en œuvre suivie de la phase de conception, étape charnière entre l'analyse du projet et la réalisation technique du pare-feu.

III.1. Analyse du projet

1. Présentation de l'organisme d'accueil

BMT (Bejaia Méditerranéen Terminal) est une jointe venture entre l'Entreprise Portuaire de Bejaia (EPB) et Portek Systems & Equipment. EPB, autorité portuaire qui gère le port de Bejaia. PORTEK Systems and Equipment, filiale du Groupe PORTEK, est un opérateur de Terminaux à conteneurs présent dans plusieurs ports dans le monde, spécialisé dans les équipements portuaires.

L'activité principale de BMT est la gestion et l'exploitation du Terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients.

1.1. L'organigramme de l'entreprise

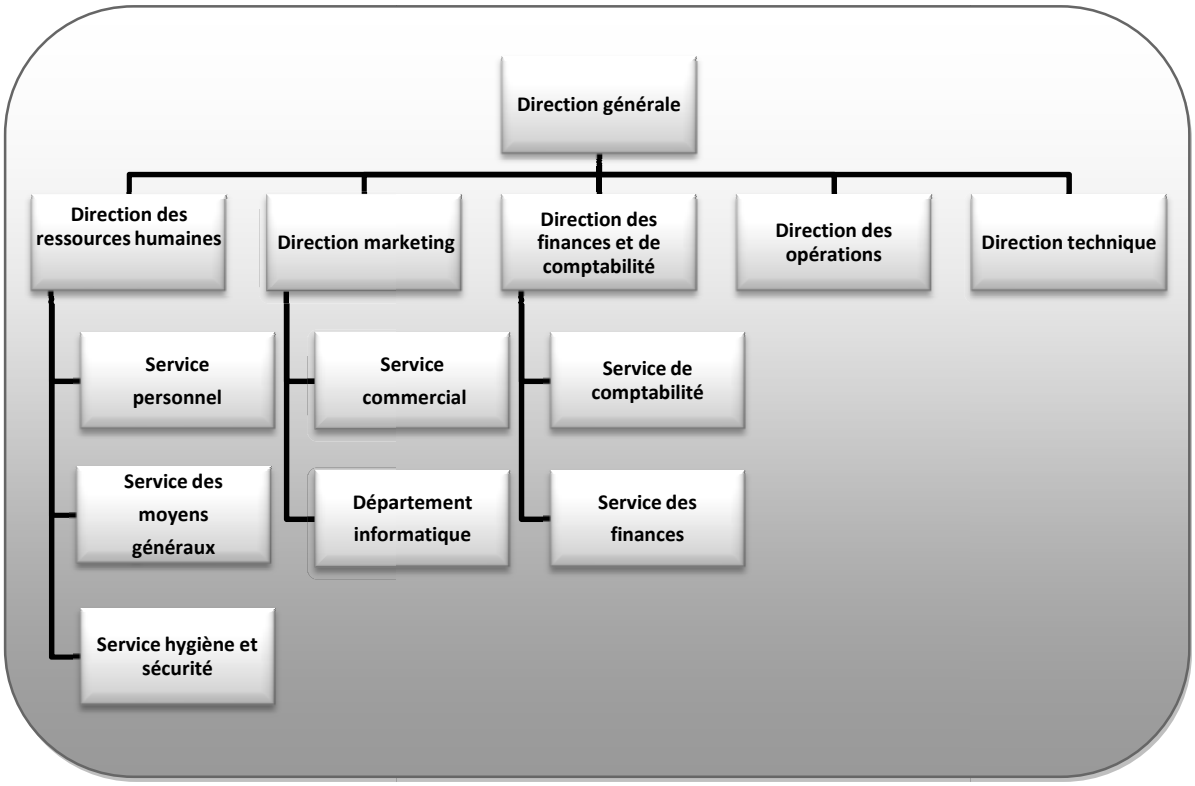

Figure III.1: Organigramme de l'entreprise

1.2. Département informatique

C'est un service qui appartient à la direction marketing.

Ses principales fonctions sont :

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

1.3. Les missions de la BMT

- Traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des navires porte-conteneurs et des conteneurs,
- La manutention sur navire aussi bien le chargement et le déchargement des conteneurs et leurs entreposages dans les zones de stockage,
- Le déchargement des céréales selon la capacité de la BMT.

1.4. L'objectif de la BMT

- Faire du Terminal à Conteneur de BMT un terminal aux normes internationales pouvant rivaliser avec les terminaux les mieux gérés au monde assurant une productivité et un profit garantissant son succès et sa pérennité,
- La création et la gestion d'un centre de formation,
- Une fiabilité de l'information.

Pour la réalisation de la « fiabilité de l'information » on a besoin d'une solution pour la sécurité du réseau de l'entreprise, qui correspond à l'essence même de notre travail.

2. Présentation du projet

Le projet consiste à mettre en place un firewall open source pour la sécurité de réseau LAN de l'entreprise et ce en permettant : le filtrage applicatif, le Filtrage d'URL (Uniform Ressource Locator) et la supervision de la bande passante.

L'objectif de ce projet dans lequel s'intègre notre travail, consiste en l'implémentation d'une architecture réseau sécurisée.

3. Analyse concurrentielle

L'analyse concurrentielle est une étape très importante pour le choix du pare-feu. Elle consiste à déterminer les principaux concurrents du pare-feu afin d'extraire leurs aspects positifs et négatifs. Pour cela nous avons choisi d'étudier deux pare-feu, qui sont PfSense et IPCOP.

Le tableau ci-dessous représente une étude comparative de PfSense et IPCOP [10] :

IPCOOP	PfSense
Basé sur Linux (Gratuit)	Basé sur Free BSD (Gratuit)
Caractéristiques: • DHCP (Dynamic Host Configuration Protocol) • DNS (Domain Name System) • NTP (Network Time Protocol) • NAT (Network address translation) • VPN : IPSec • QoS (traffic chapping) : Priorité selon type de trafic, lissage de trafic (limitation) • Un serveur proxy Web • Filtrage d'URL (SquidGuard) • Filtrage dynamique • Supervision de la bande passante.	Caractéristiques: • DHCP • DNS • NTP • NAT • VPN : IPSec, PPTP, L2TP • Load Balancing (Equilibrage de charge) • Multi-WAN • QoS (traffic chapping) : Priorité selon type de trafic, lissage de trafic (limitation) • Un serveur proxy Web (Squid) • Filtrage d'URL (SquidGurad) • Portail captif • Filtrage simple de paquet • Filtrage dynamique • Supervision de la bande passante (Ntop) • Mises à jour automatique

Tableau III.1: Analyse concurrentielle (IPCOOP/PfSense)

- Au vu de ce comparatif, les deux solutions s'adaptant aux critères de sécurité dont nous avons besoin [Serveur proxy (filtrage applicatif), filtrage d'URL (SquidGuard), supervision de la bande passante]. Mais, il se trouve que PfSense possède plus de fonctionnalités que IPCOOP (mises à jour automatique, Portail captif, Load Balancing, Multi-WAN). Notre choix est ainsi porté sur le logiciel PfSense Open Source qui grâce à ses différentes fonctionnalités, apportera la sécurité nécessaire au réseau local de l'entreprise.

- **Multi-WAN** : support de multiples interfaces réseaux WAN.
- **Un portail captif** : est une structure permettant un accès rapide à Internet. Lorsqu'un utilisateur cherche à accéder à une page Web pour la première fois, le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur 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 à un serveur HTTP. Ceci permet à tout ordinateur équipé d'un navigateur HTML et d'un accès Wifi de se voir proposer un accès à

Internet. Les identifiants de connexion (identifiant, mot de passe) de chaque utilisateur sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant. Une fois l'utilisateur authentifié, les règles du Firewall le concernant sont modifiées et celui-ci se voit alors autorisé à utiliser son accès pour une durée limitée fixée par l'administrateur. A la fin de la durée définie, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session [4].

4. Diagramme de Gantt

Le diagramme de Gantt est un outil standard de gestion de projets utilisé pour planifier efficacement les tâches et suivre ensuite leurs progressions. Il offre une représentation graphique du projet en planifiant les tâches sur un calendrier [11].

4.1. L'objectif de diagramme de Gantt

Organiser un diagramme de Gantt peut prendre un certain temps, mais il permettra d'en gagner beaucoup par la suite étant donné l'efficacité du travail. Un diagramme de Gantt**,** est aussi très pratique pour ne pas travailler à la dernière minute ou pour ne pas manquer de temps, comme il indique les priorités (ce qui est plus important) et nous évite d'entreprendre les tâches dans le désordre.

Quand nous bâtissons le diagramme de Gantt, nous devons connaître :

- **La tâche à réaliser :** installation et configuration d'un firewall PfSense.
- **Le temps disponible pour accomplir le projet :** compter environ trois mois.
- **Les outils dont nous avons besoin :** livres, notes de cours, sites Internet, les mémoires similaires.
- **Les soutiens qui nous entourent :** promoteur, camarades, familles…
- **Les points faibles :** le manque d'expérience dans le domaine.

La figure III.2, indique les tâches nécessaires à la réalisation de ce projet et leurs durées d'achèvement. Elle comporte deux axes :

- L'axe horizontal représente la durée totale du projet, divisée en tranches de temps.
- L'axe vertical représente les tâches qui composent le projet. Chacune est représentée par une barre horizontale.

Temps / Tâches	Mars				Avril				Mai				Juin			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Notions de Basse																
Analyse de projet + élaboration de cahier des charges																
Réalisation de cahier des charges																
Préparation de la soutenance																

⟶ Durée estimé

——— Temps de réalisation

Figure III.2: Digramme de Gantt

III.2.Conception

1. Les logiciels utilisés

- VMware Workstation 10.0
- PfSense V 2.0.2
- Windows XP Professional

1.1. Présentation de VMware Workstation

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle pendant son fonctionnement [12].

1.2. Présentation de PfSense

PfSense (distribution logicielle), ou ≪ **P**acket **F**ilter **Sense** ≫ est un routeur / pare-feu open source basé sur FreeBSD. Il date de 2004 à partir d'un fork de m0n0wall par Chris Buechler et Scott Ullrich. PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (*packet filter*), il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q) [5].

Les avantages principaux de PfSense sont les suivants :

- Il est adapté pour une utilisation en tant que pare-feu et routeur,
- Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement,
- Il offre des options de firewalling /routage plus évolué qu'IPCOP,
- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres,
- Simplicité de l'activation / désactivation des modules de filtrage,
- Système très robuste basée sur un noyau FreeBSD,
- Des fonctionnalités réseaux avancées [5], [13].

1.3. Présentation de FreeBSD

FreeBSD est un système d'exploitation de type Unix librement disponible, largement utilisé par des fournisseurs d'accès à Internet, dans des solutions tout-en-un et des systèmes embarqués et partout où la fiabilité par rapport à un matériel informatique est primordiale. FreeBSD est le résultat de presque trois décennies de développement continu, de recherche et de raffinement. L'histoire de FreeBSD commence en 1979, avec BSD [6].

2. Installation et Configuration basique de PfSense sous VMware

L'architecture à suivre pour la mise en place de PfSense est la suivante :

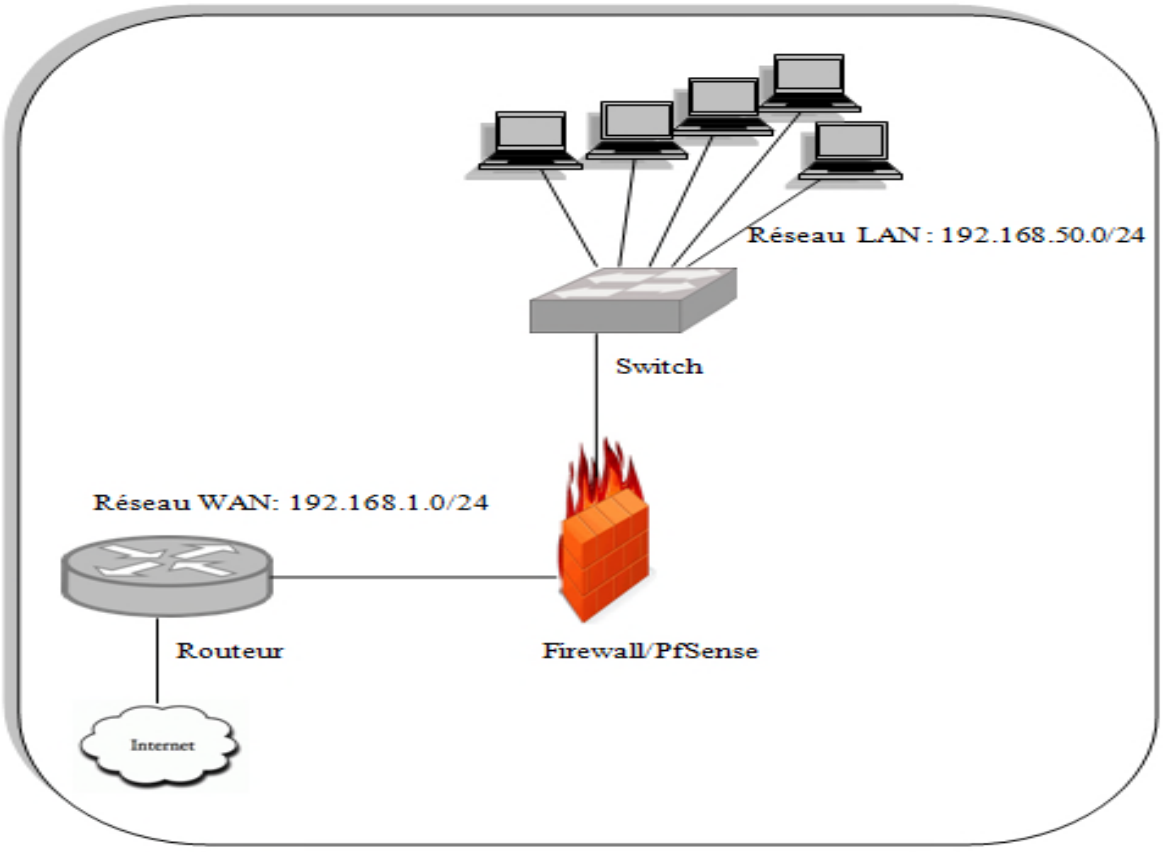

Figure III.3: Architecture réseau avec Firewall PfSense

2.1. Installation de PfSense

- Création d'une machine virtuelle :

On crée une Machine Virtuelle sous VMware avec les spécifications suivantes :

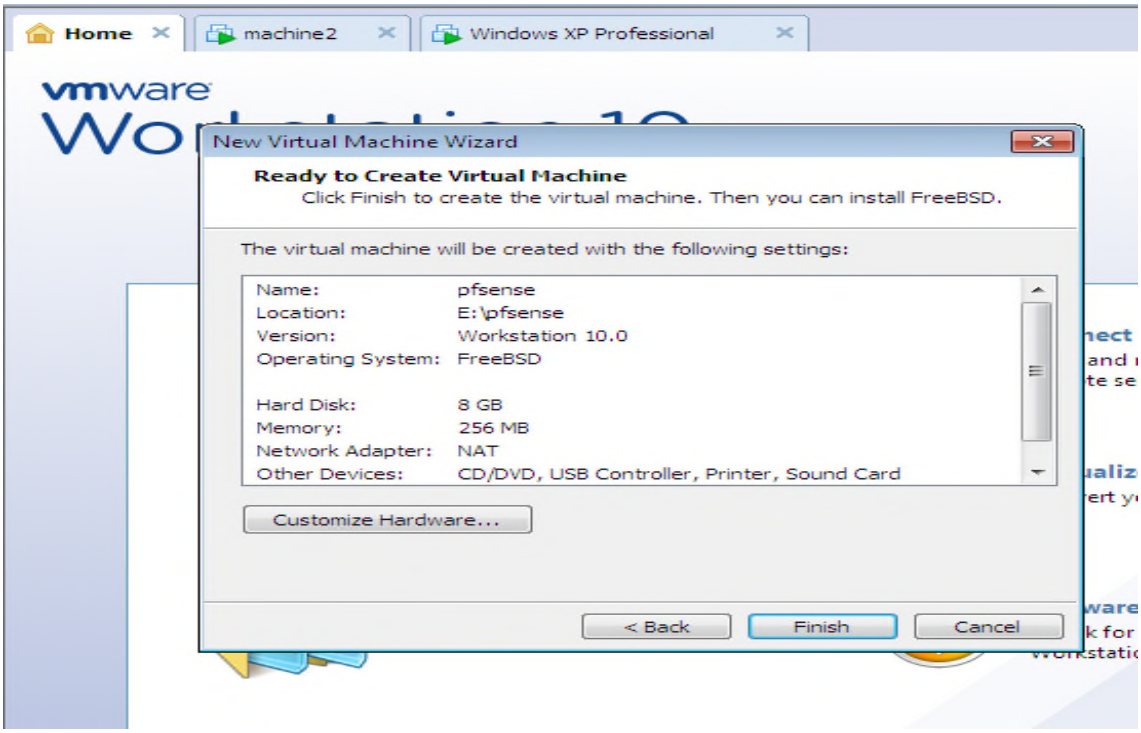

Figure III.4: Machine virtuelle

- On clique sur **Finish**, cette fenêtre s'affiche :

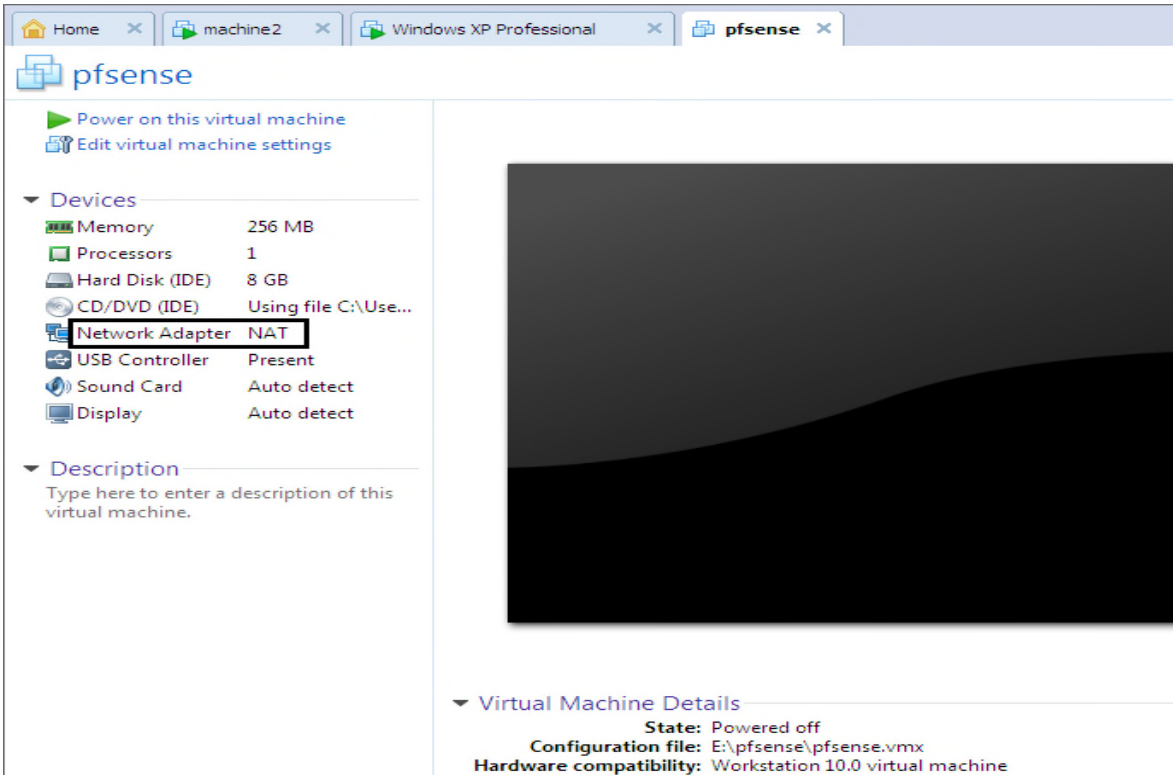

Figure III.5: Machine virtuelle: compatibilité du matériel virtuel

- Avant de commencer l'installation, notre machine doit être équipée en minimum de deux cartes réseaux. Pour ce projet on va utiliser deux interfaces (2 cartes réseaux):
  - ✓ LAN (VMnet0): pour qu'on puisse communiquer localement avec le serveur PfSence.
  - ✓ WAN (VMnet1): pour qu'on puisse se connecter à Internet.

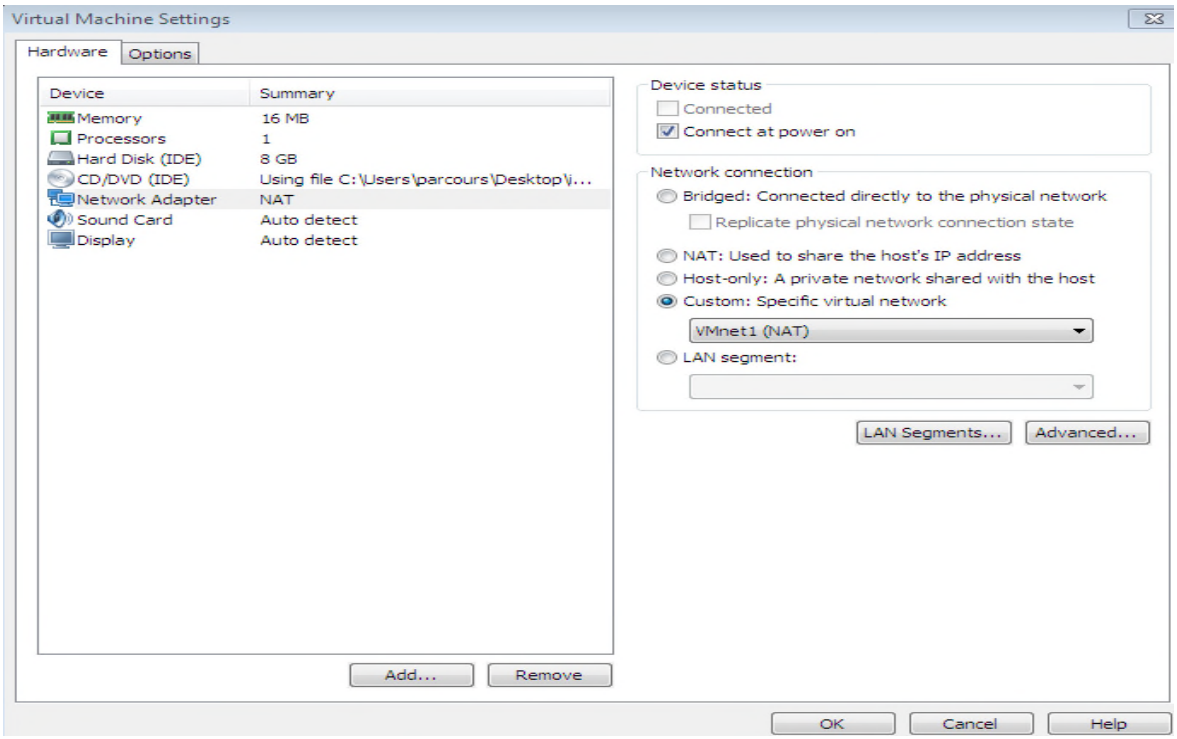

Figure III.6: Machine virtuelle: installation de la carte réseau WAN

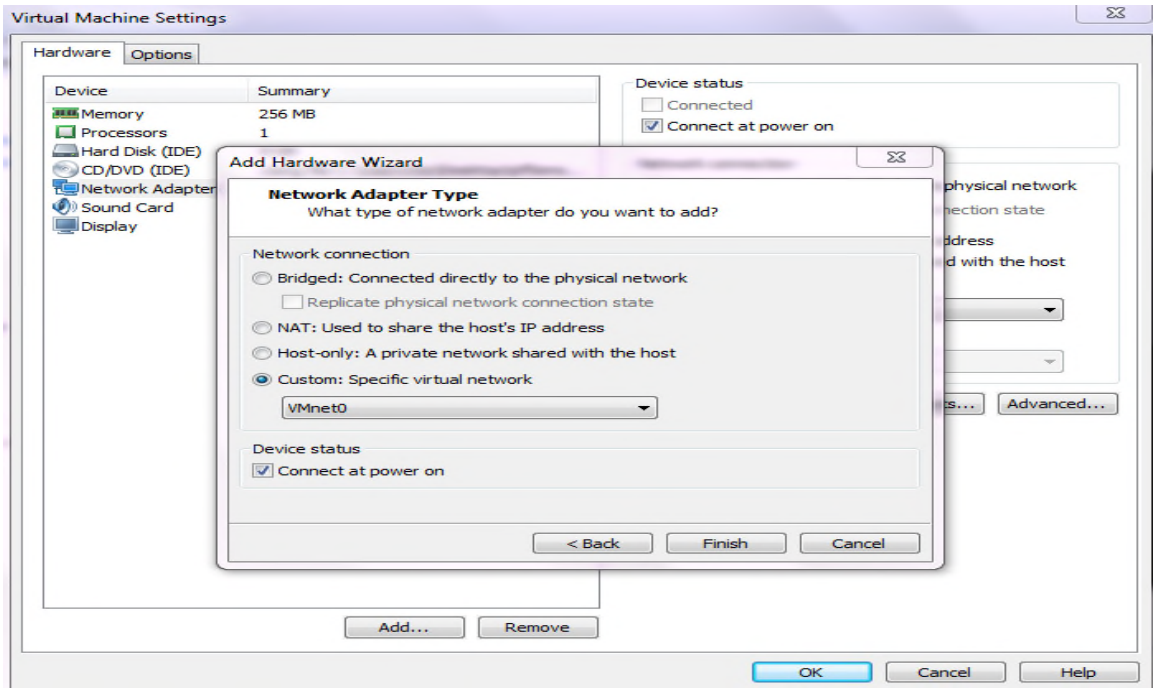

Figure III.7: Machine virtuelle: installation de la carte réseau LAN

- Configuration des cartes réseau sous Virtual Network Editor :
  - ✓ Configuration de la carte réseau LAN :

On configure la carte en mode Hoste-only pour qu'elle puisse se connecter avec le réseau LAN.

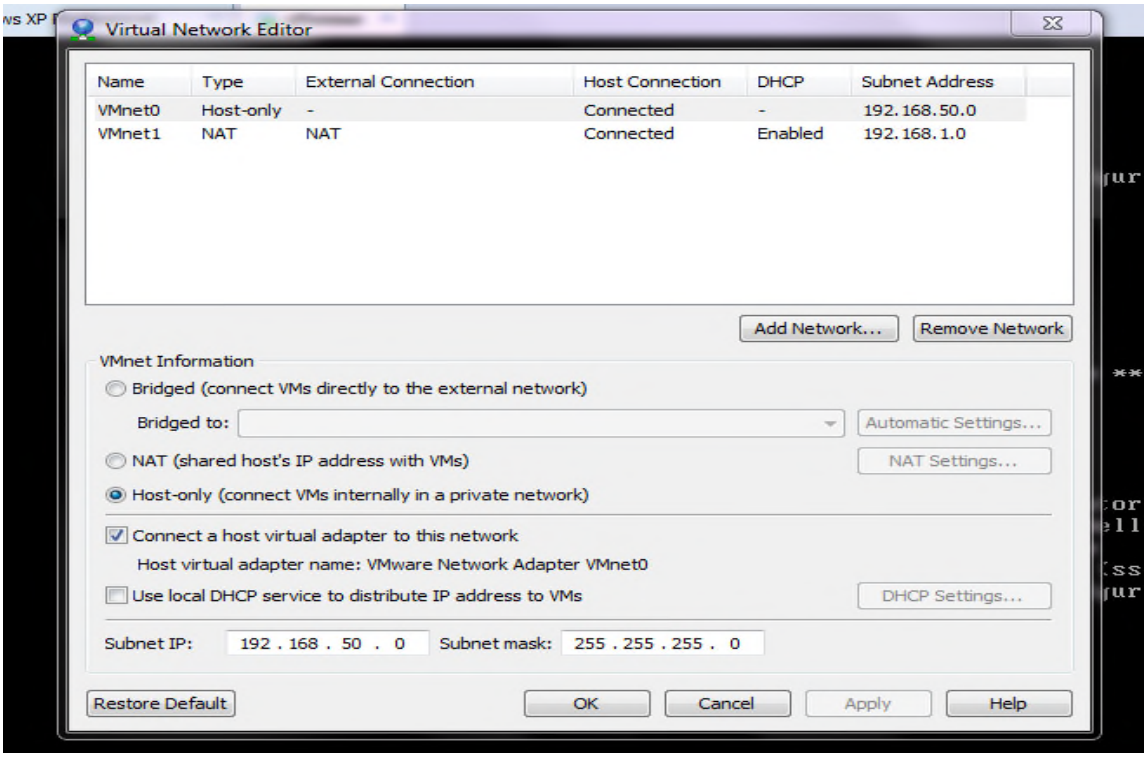

Figure III.8: Configuration de la carte réseau LAN sous Virtual Network Editor

✓ Configuration de la carte réseau WAN :

On configure la carte en mode NAT (ce mode utilisé pour le partage de l'adresse IP).

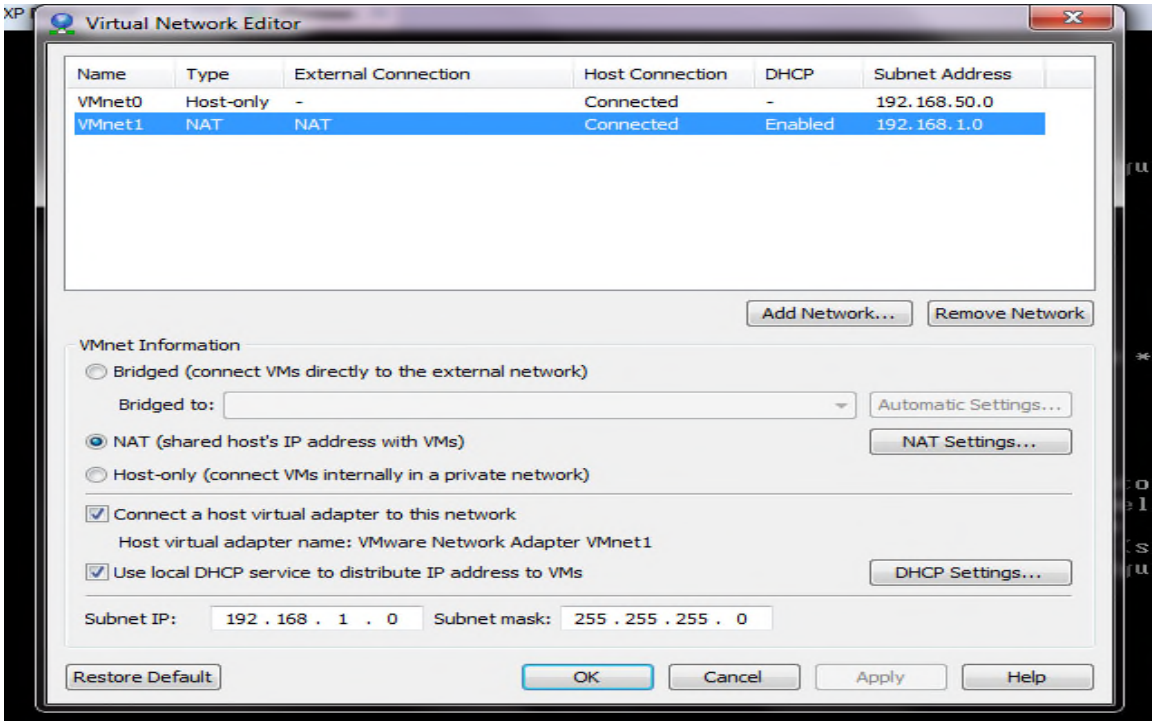

Figure III.9: Configuration de la carte réseau WAN sous Virtual Network Editor

- On clique sur **power on this vertual machine** pour commencer l'installation de PfSense. La fenêtre suivante s'affiche. On choisit le 1er choix.

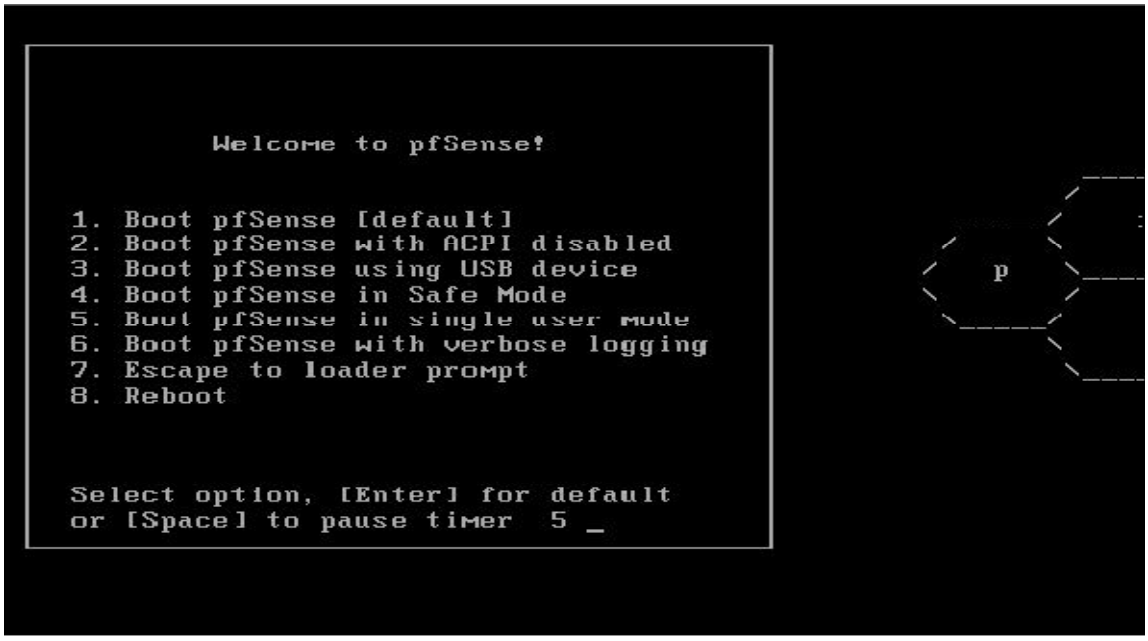

Figure III.10: PfSense-installation: mode de démarrage

- Durant l'installation, PfSense détecte automatiquement les cartes réseaux disponibles, et il y attribue respectivement les noms le0, le1.

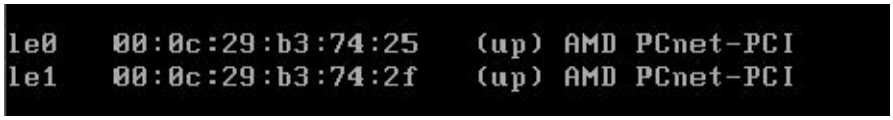

Figure III.11: PfSense: assignation des interfaces réseaux

- La première question que nous rencontrons durant l'installation est la suivante :

On répond par *n* (No) car on n'aura pas besoin des VLANs.

- PfSense demande d'affecter chaque interface (ici le 0, le1) à une interface WAN ou bien à un LAN.

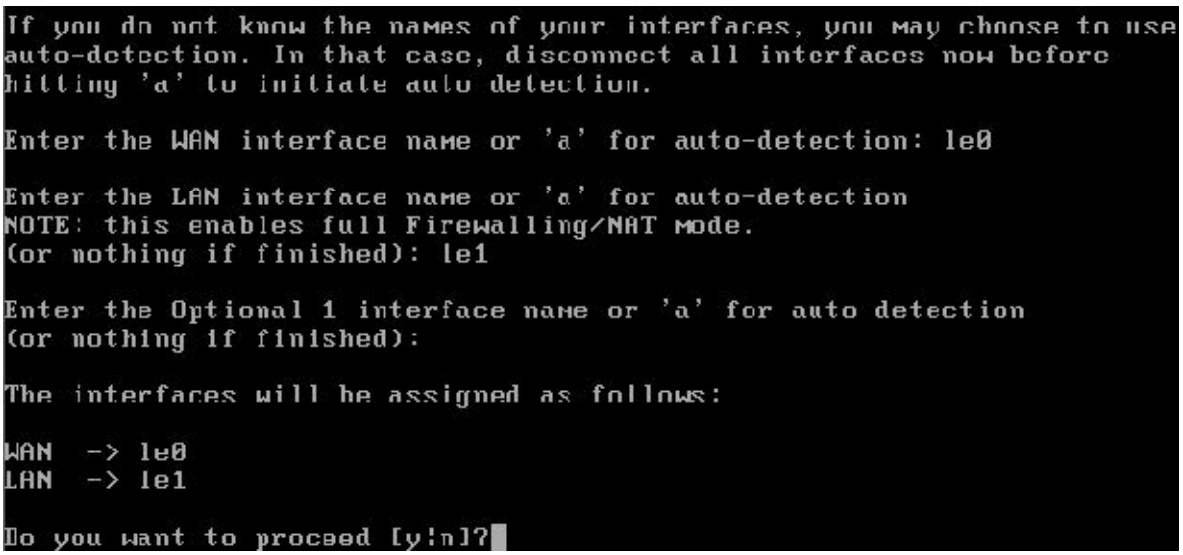

Figure III.12: PfSense: assignation de l'interface WAN et LAN

- La figure ci-dessus montre qu'on a affecté le0 au LAN, le1 au WAN.
- L'installation se termine ici.

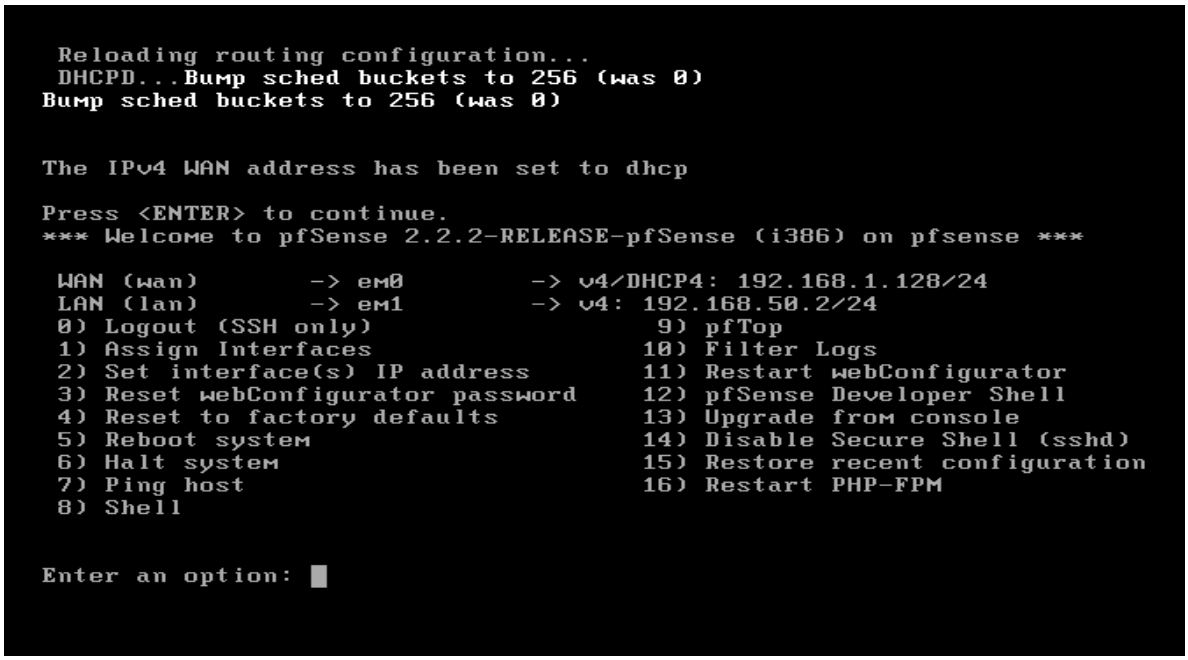

Figure III.13: PfSense: installation terminée

- Les adresses IP des interfaces WAN et LAN sont attribuées par nous-mêmes par le choix de l'option 2 (l'@ IP de WAN attribuée par le serveur DHCP, l'@ LAN attribuée statiquement).
- Pour se connecter à l'interface web de configuration de PfSense on utilise l'adresse IP de l'interface LAN : http://192.168.50.2. Cette page s'affiche :

Figure III.14: Page d'identification de PfSense

- Le couple « Username/Password » par défaut est « admin/pfSense ».

2.2. Configuration basique de PfSense

À ce stade- là, on doit configurer basiquement notre serveur, pour cela on choisit :

Setup Wizard du menu **System**, puis on tape **Next**.

Figure III.15: Déclaration du Serveur DNS

- Hostname : le nom du Host.
- Domain : le domaine si c'est déjà établi, sinon on laisse le choix par défaut.
- Primary (Secondary) DNS Server : l'adresse primaire (secondaire) du serveur DNS à utiliser (on utilise le Serveur DNS de Google : 8.8.8.8).

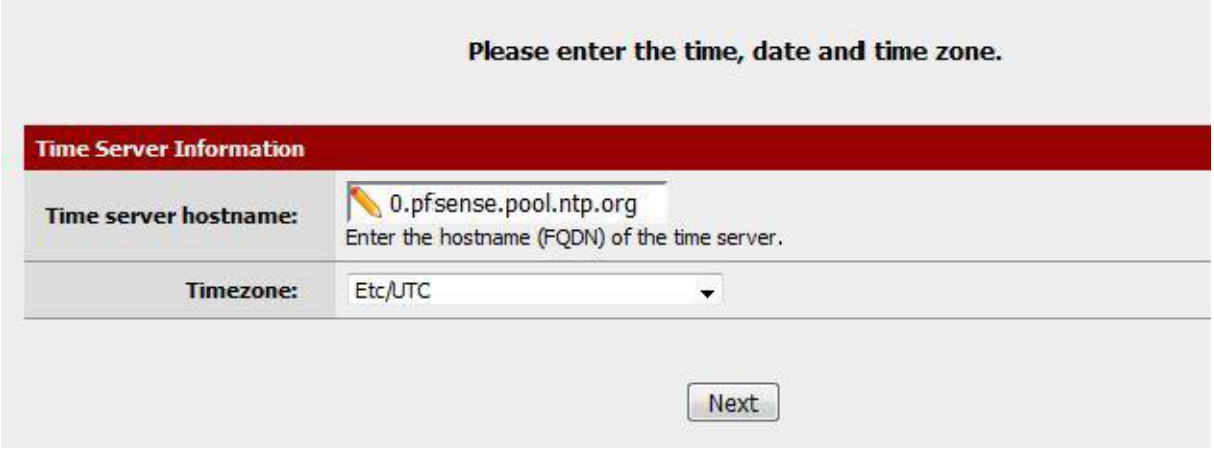

Figure III.16: Déclaration du Serveur d'horloge

- Ici on déclare le serveur d'horloge avec lequel on doit se synchroniser, par défaut c'est *0.pfsence.pool.ntp.org* (on le laisse par défaut).
- Puis **Next**, on arrive à une étape très importante, on doit configurer notre interface WAN.

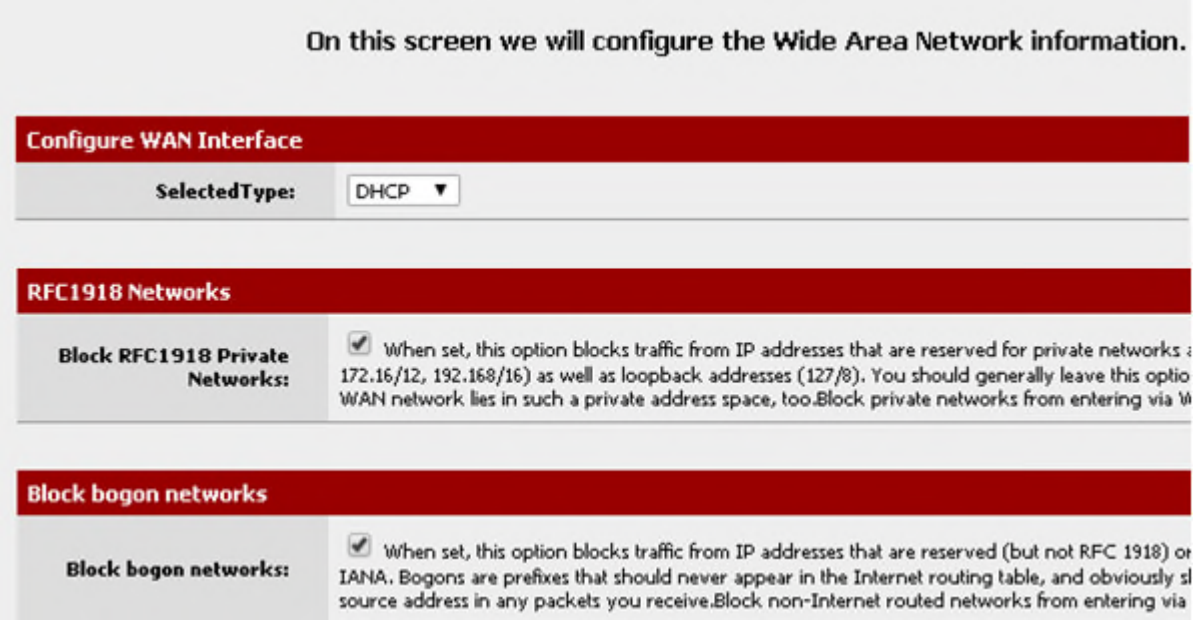

Figure III.17: Configuration de l'interface WAN

- Block RFC1918 Private Networks : pour bloquer tous le trafic issu des adresses privées ou de loopback.
- Block bogon Networks : Pour bloquer les paquets dont l'adresse source est non définie par l'IANA.
- Puis en cliquant **Next**, on arrive à la configurer de l'interface LAN.

Figure III .18: Configuration de l'interface LAN

- C'est simple ici, on affecte une adresse IP à l'interface LAN, puis on clique sur **Nexte,** cette page s'affiche (permet de changer le mot de passe de l'interface Web) :

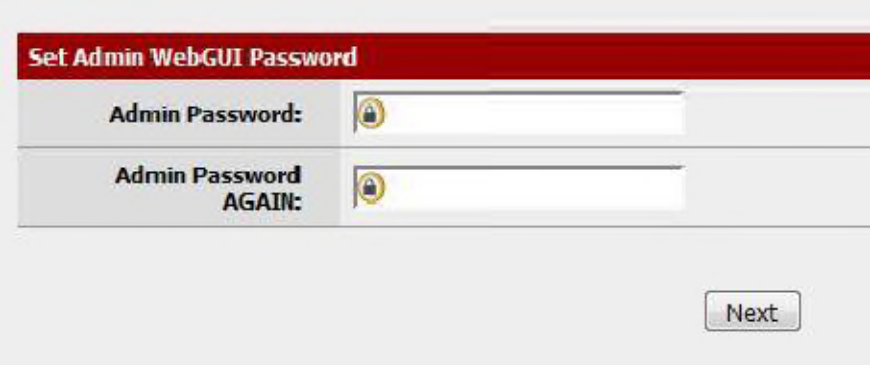

Figure III.19: Configuration de mot de passe

- Puis **Reload** pour que PfSense prend en charge la nouvelle configuration.

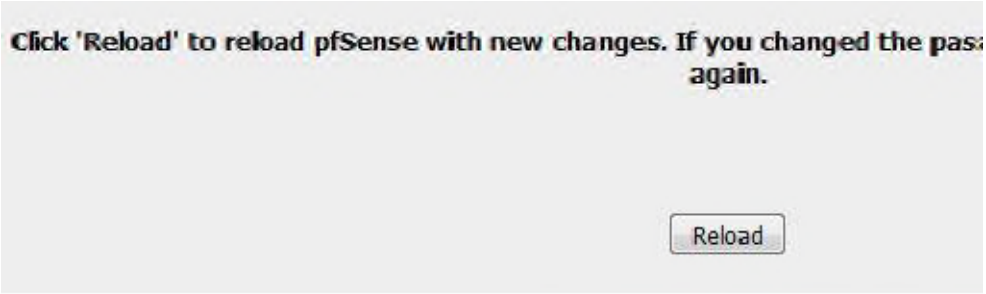

Figure III.20: Le rechargement de la configuration

À partir de ce moment-là, Internet est accessible à toutes les machines du réseau, sans restriction ni filtre.

Conclusion

Après avoir décrit l'analyse et à la conception du pare-feu PfSense mis en place, et expliciter les différentes étapes pour son installation et sa configuration basique, nous allons passer dans ce qui suit à la phase réalisation. Dans cette section, nous allons paramétrer également quelques paquets de firewall PfSense.

CHAPITRE IV

RÉALISATION

Introduction

Ce chapitre constitue le corps essentiel de ce mémoire, dans lequel nous allons clôturer la mise en place de PfSense. Nous effectuons le paramétrage de quelques packages qu'il présente, et ce, en effectuant les tests nécessaires à la vérification de la sécurité au niveau des multiples échanges effectués sur le réseau.

Quelques écrans montrant les fonctionnalités les plus importantes de l'application et les résultats des tests effectués sont également bien explicités dans ce dernier chapitre.

IV.1. Le filtrage d'URL

Pour pouvoir utiliser les fonctionnalités du proxy, il faut ajouter les packages « **Squid** » et « **SquidGuard** » puis les configurer.

1. Présentation de Squid

« **Squid** » est un serveur proxy/cache libre très connu du monde Open Source. Ce serveur est complet et propose une multitude d'options et de services qui lui ont permis d'être largement adopté par les professionnels. Il est capable de manipuler les protocoles HTTP, FTP, SSL**,** etc. [7].

2. Présentation de SquidGuard

« **SquidGuard** » est un redirecteur d'URL, il utilise les listes noires avec le proxy « Squid ». SquidGuard possède deux grands avantages : il est rapide et gratuit. Il est publié sous GNU Public License, licence gratuite [7].

SquidGuard peut être utilisé pour :

- Limiter l'accès Internet pour certains utilisateurs à une liste de serveurs Web et /ou des URLs qui sont acceptés et bien connus,
- Bloquer l'accès à des URLs correspondant à une liste d'expressions régulières ou des mots pour certains utilisateurs,
- Imposer l'utilisation de nom de domaine et interdire l'utilisation de l'adresse IP dans les URLs,
- Rediriger les URLs bloqués à une page d'informations relative à PfSense,

- Avoir des règles d'accès différentes selon le moment de la journée, le jour de la Semaine, date, etc.

3. Installation des packages: Squid et SquidGuard

Pour l'installation des paquets additionnels à PfSense il faut se rendre dans le menu **System ->Package Manager**.

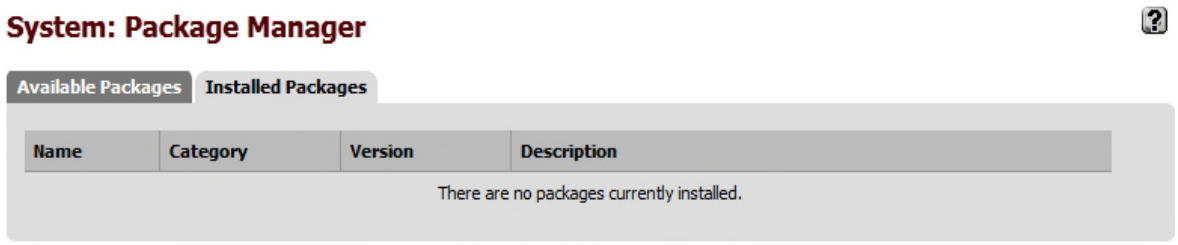

Figure IV.1: Menu System: Package Manager

L'onglet **« Installed Packages »** décrit les paquets installés sur la machine et l'onglet **« Available Packages »** ceux disponibles pour une installation.

Donc pour l'installation des packages, on choisit l'onglet **« Available packages »,** pour installer les package Squide et SquidGuard en cliquant sur le bouton « + ».

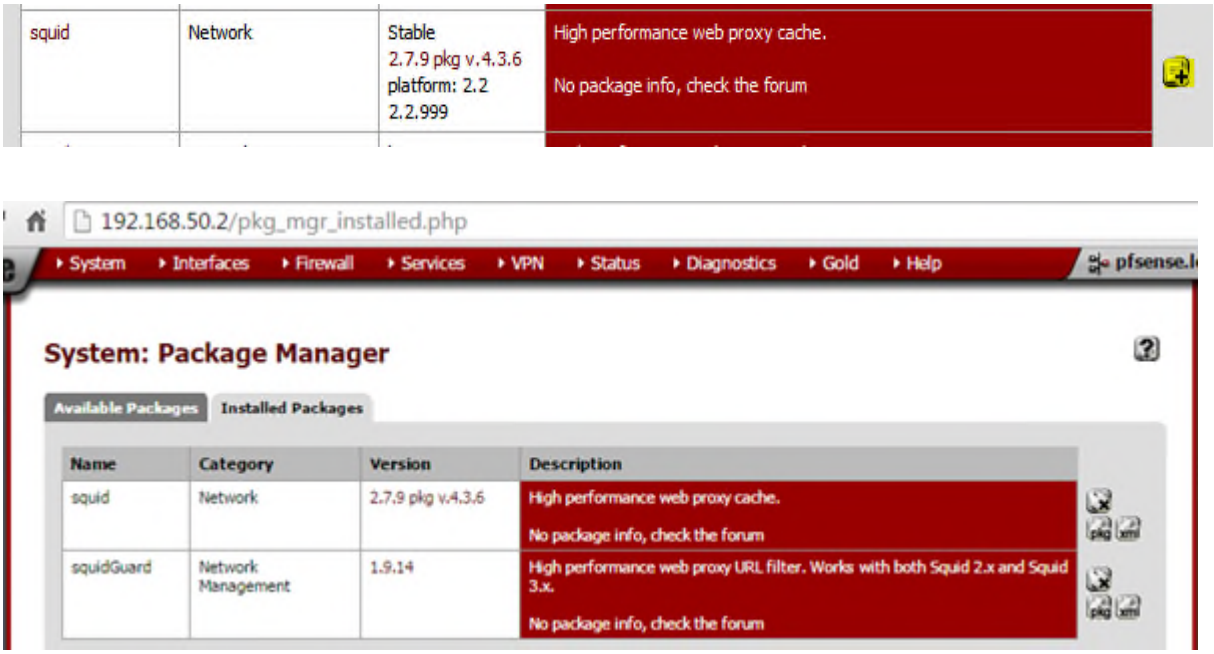

Figure IV.2: Installation des packages Squid et SquidGuard

Une fois les paquets installés, on passe à la configuration.

4. Configuration de Squid

Dans le menu **Services -> Proxy Server.**

Dans l'onglet **« General »,** on configure les options suivantes :

- Proxy interface : permet d'affecter Squid à une interface réseau,
- Allow users on interface : permet aux utilisateurs connectés à l'interface sélectionnée dans le champ « Proxy Interface » à utiliser le Proxy server,
- Transparent proxy : permet de transmettre toutes les demandes de port de destination 80 au serveur Proxy,
- Enable logging : permet d'activer la journalisation,
- Log store directory : le répertoire où les journaux seront stockés,
- Proxy port : 3128 -> port de serveur Proxy,
- Language : permet de Sélectionner la langue dans laquelle le serveur proxy affichera des messages d'erreur pour les utilisateurs.

Pour enregistrer la configuration on clique sur le bouton "Enregistrer" en bas de page

La figure suivante montre la configuration de serveur Proxy :

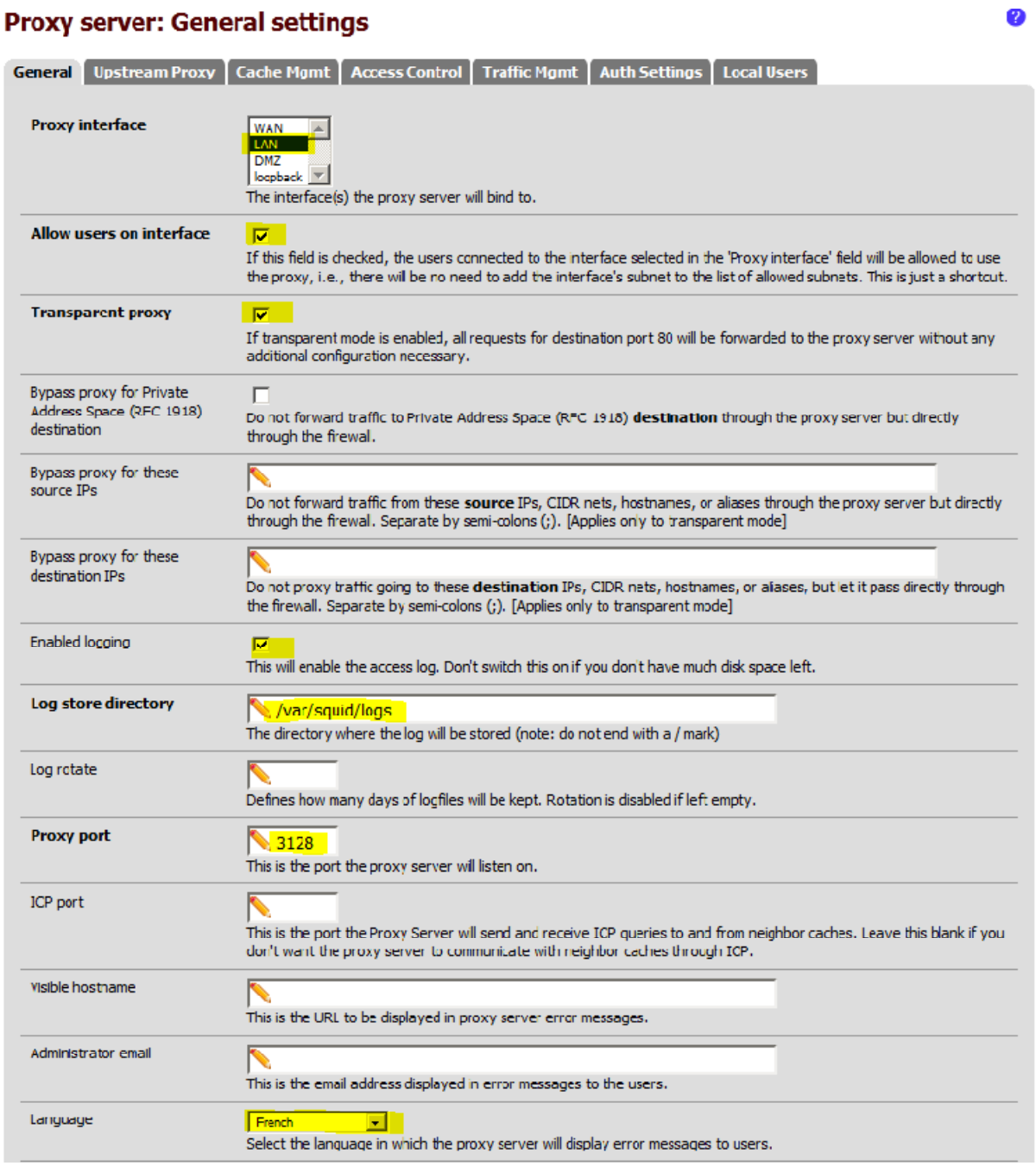

Figure IV.3: Configuration de Squid

5. Configuration de SquidGuard

Dans le menu **Services -> Proxy filter.**

Dans l'onglet **« General »,** on configure les options suivantes :

- Enable : permet d'activer SquidGuard,
- Enable GUI log : Permet d'avoir l'accès à la GUI de Filtre Proxy,

- Enable log : permet d'enregistrer les paramètres de Proxy filter comme des sites Web bloqués en Common ACL, Group ACL et Target Categories. Cette option est généralement utilisée pour vérifier les paramètres de filtrage,
- Enable log rotation : permet de faire pivoter les journaux tous les jours pour limiter la taille de fichier et de ne pas manquer d'espace disque,
- Blacklist : permet d'activer la blacklist (liste noire),
- Blacklist URL : permet de saisir le chemin d'accès à la liste noire. Nous avons utilisé la Blacklist « Shalla » téléchargeable ici : http://www.shallalist.de/Downloads/shallalist.tar.gz

Après, on sauvegarde la configuration (en cliquant sur **Save**) et activer le paquet SquidGuard en cliquant sur l'option **Apply** (après toute modification ultérieure de la configuration, on doit cliquer sur le bouton 'Apply').

La figure suivante montre la configuration de Proxy filter :

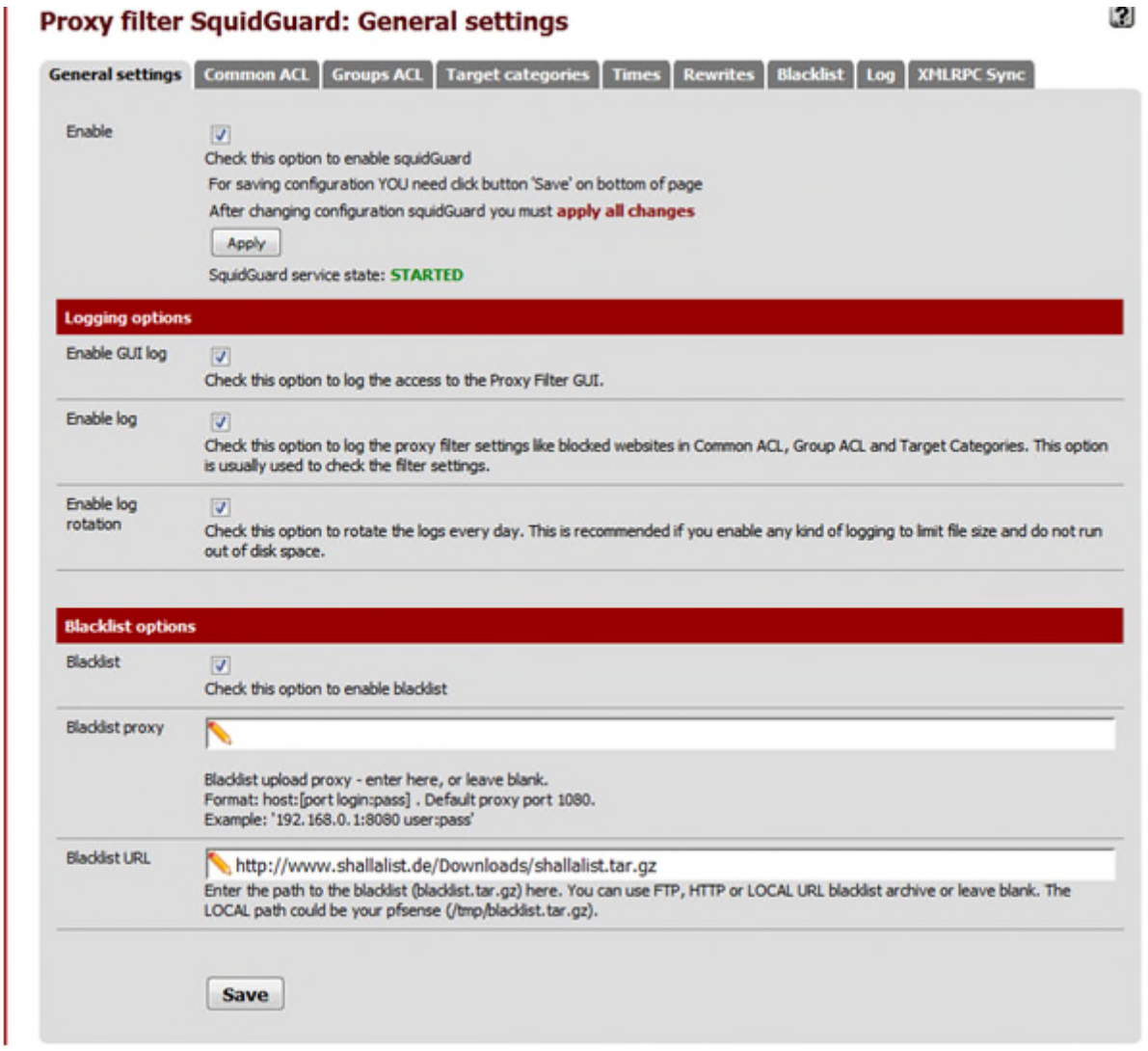

Figure IV.4: Configuration de SquidGuard

Ensuite, se rendre dans l'onglet « Blacklist », pour télécharger la Blackliste « Shalla » afin d'être intégrée à PfSense :

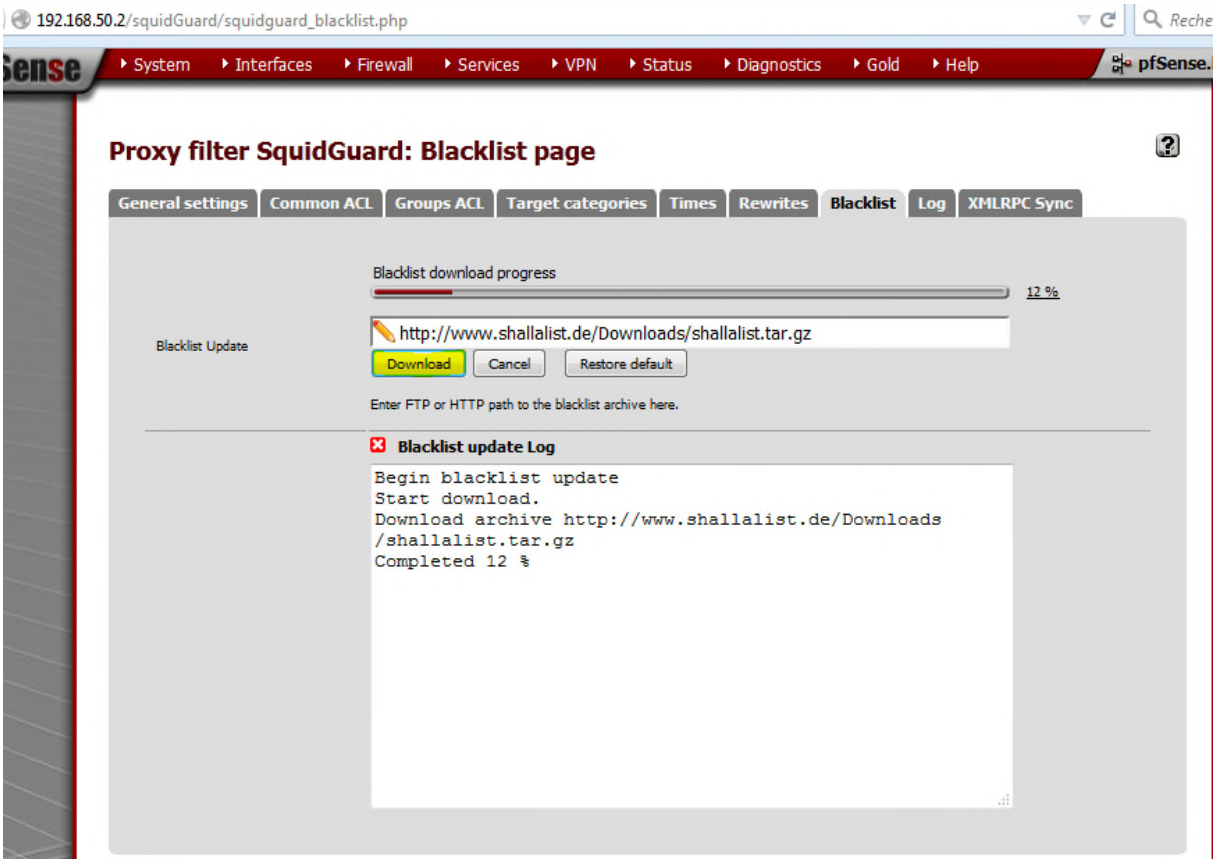

Figure IV.5: Téléchargement de la Blacklist

Une fois le téléchargement complété, se rendre dans l'onglet « Common ACL » pour cocher les éléments suivants :

- Do not allow IP-Addresses in URL: permet de bloquer l'accès aux sites Internet en utilisant les adresses IP.
- Use Safe Search engine : pour l'utilisation d'un moteur de recherche sécurisé,
- Log : cette option permet d'activer la journalisation pour une ACL.

5.1. Le filtrage d'URL en utilisant la blacklist « Shalla »

Pour configurer la Blacklist, on clique sur la flèche verte pour afficher en détail les différentes listes regroupées par «catégorie».

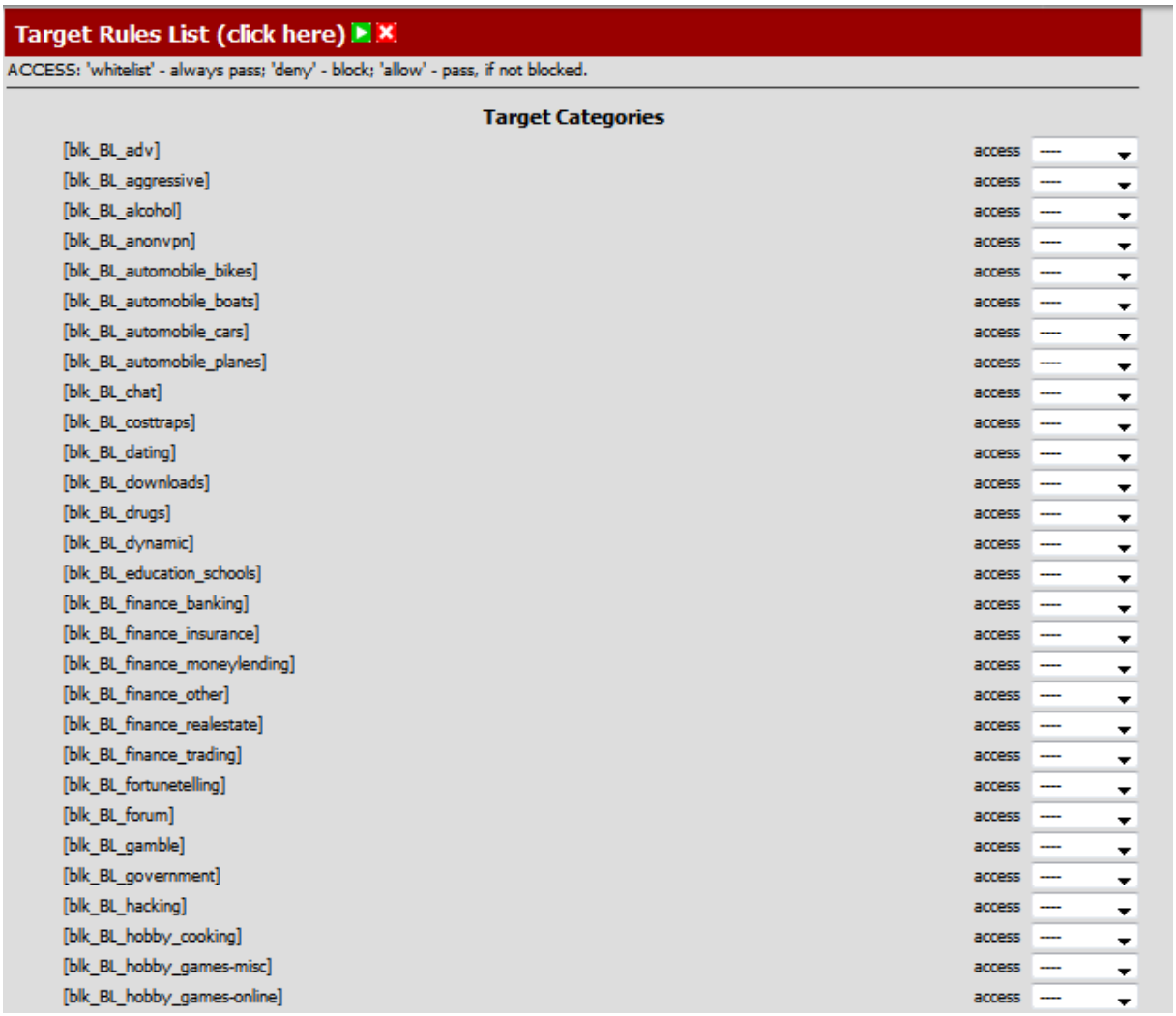

Figure IV.6: Catégories de la Blacklist « Shalla »

Pour chaque catégorie 4 configurations sont permises :

1. --- : catégorie non prise en compte,
2. white : catégorie toujours autorisée,
3. deny : catégorie non autorisée,
4. allow : catégorie autorisée sauf les sites appartenant à une autre catégorie non autorisé.

On bloque les catégories : alcohol, chat et gamble. Après, on sauvegarde la configuration.

La figure suivante montre la configuration de la commun ACL :

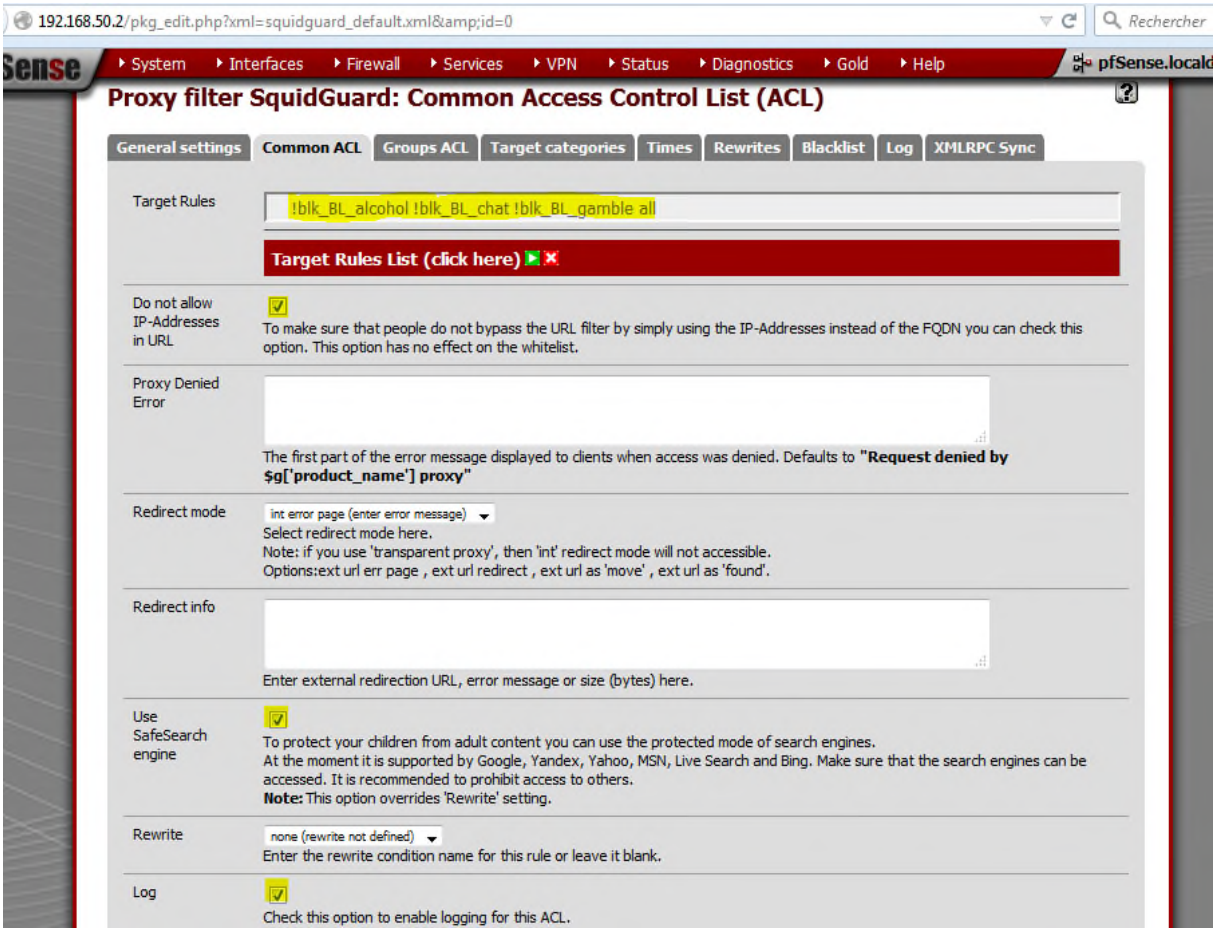

Figure IV.7: Configuration de Common Access Control List (ACL)

On teste l'accès au site **http://lotto.web.do/** qui se trouve dans la catégorie **gamble**, la page de redirection de proxy suivante s'affiche :

Figure IV.8: Résultat du test d'interdiction d'accès pour la catégorie « gamble »

5.2. Le filtrage d'URL en créant des ACLs

En plus de la Blacklist « Shalla », il est possible de bloquer des sites autorisés en créant des ACLs (blacklist) ou encore d'incorporer des Whitelist permettant d'autoriser des sites interdits par une BlackList.

Pour cela, on choisit, l'onglet (Target catégories), on clique sur Ajouter [+], pour créer deux ACLs : une ACL avec l'insertion des fragments de mots des URLs, une autre avec l'insertion des noms de domaine.

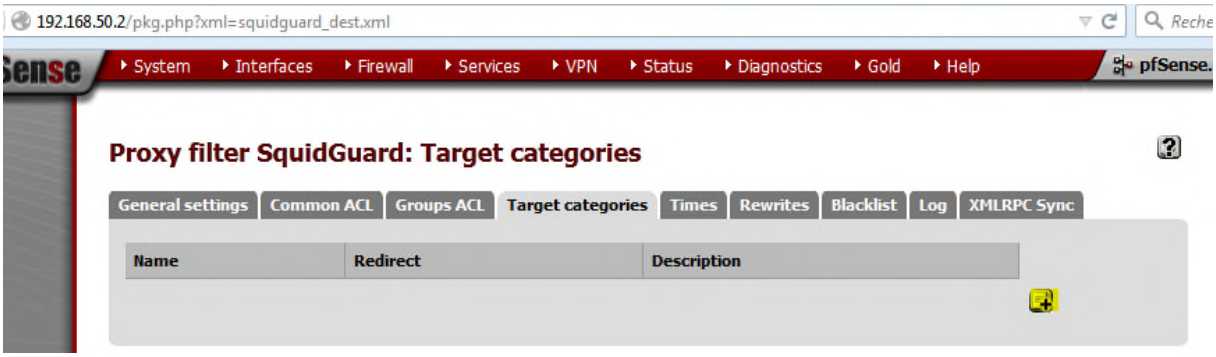

Figure IV.9: Onglet Target categories

5.2.1. ACL avec fragments de mots des URLs

Dans l'onglet apparu on configure les options suivantes :

- Name : permet d'insérer le nom de l'ACL,
- Regular Expression : permet d'insérer des fragments de mots des URLs de destination,
- Log : permet d'activer la journalisation pour une ACL.

Après, on sauvegarde la configuration en cliquant sur **Save.**

Pour décider s'il s'agit d'une Whitelist ou Blacklist, il faut aller modifier le choix dans Common ACL. Les deux ACL crée sont des blacklist.

La figure suivante montre la création de cette ACL :

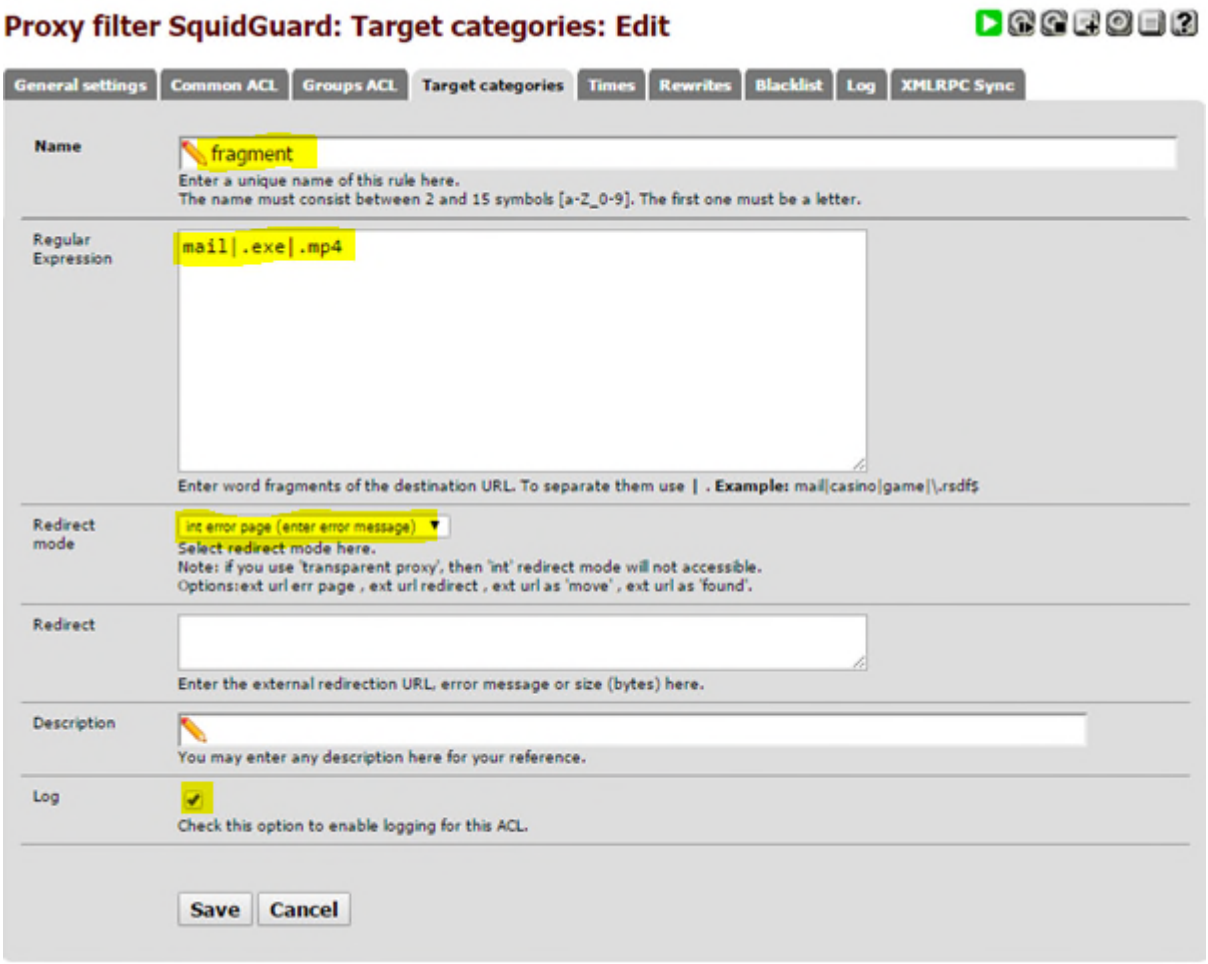

Figure IV.10: Création de l'ACL « fragment »

On teste l'accès aux sites : **www.hotmail.fr** , **download.skype.com/**…, les pages de redirection suivantes s'affichent :

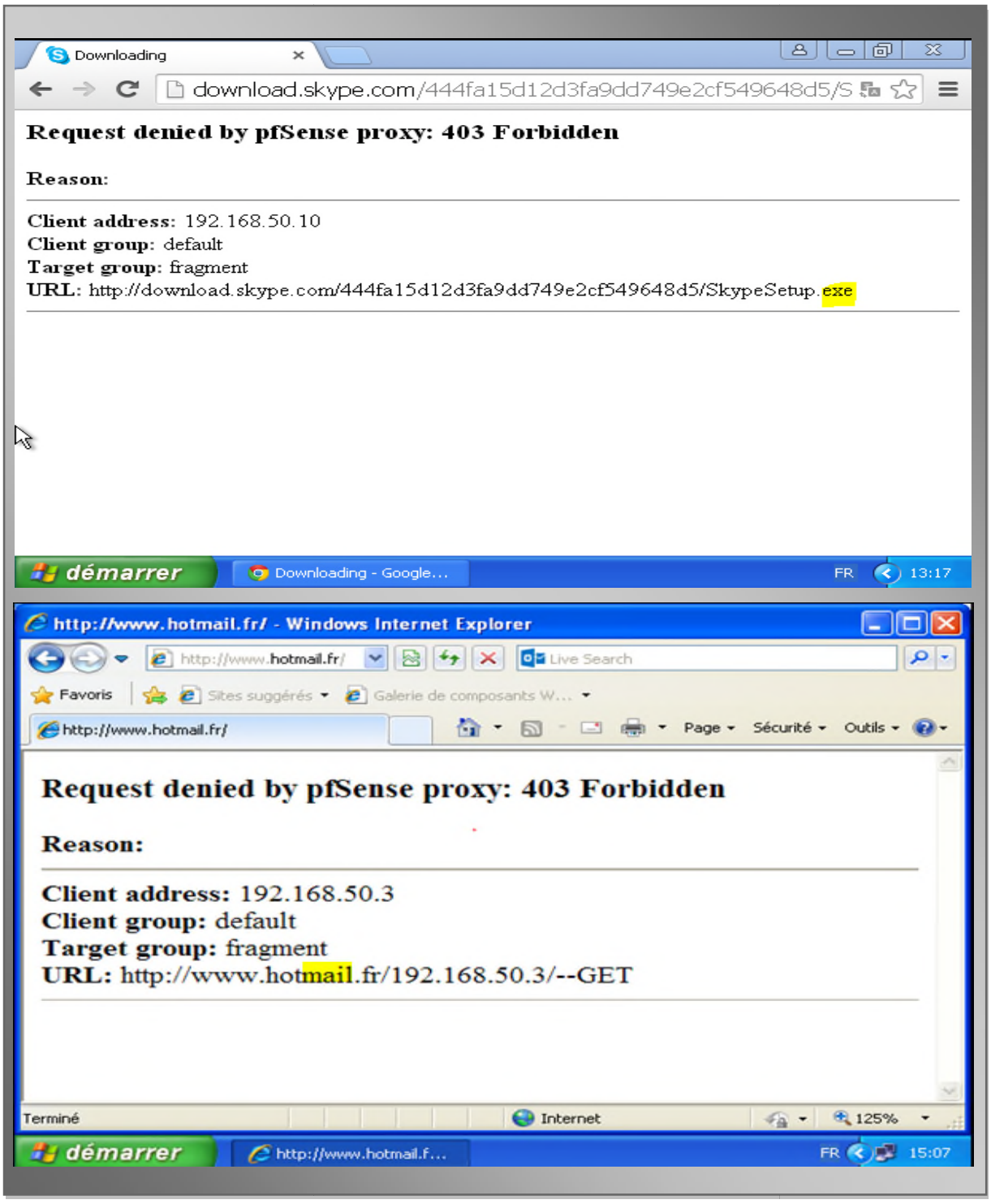

Figure IV.11: Résultats des tests d'interdiction d'accès pour l'ACL « fragment »

5.2.2. ACL avec des noms de domaine

Dans l'onglet apparu on configure les options suivantes :

- Name : permet d'insérer le nom de l'ACL,
- Domain List : permet d'insérer les noms de domaine de destination ou les adresses IP.
- Log : permet d'activer la journalisation pour une ACL.

Après, on sauvegarde la configuration en cliquant sur **Save.**

La figure suivante montre la création de cette ACL :

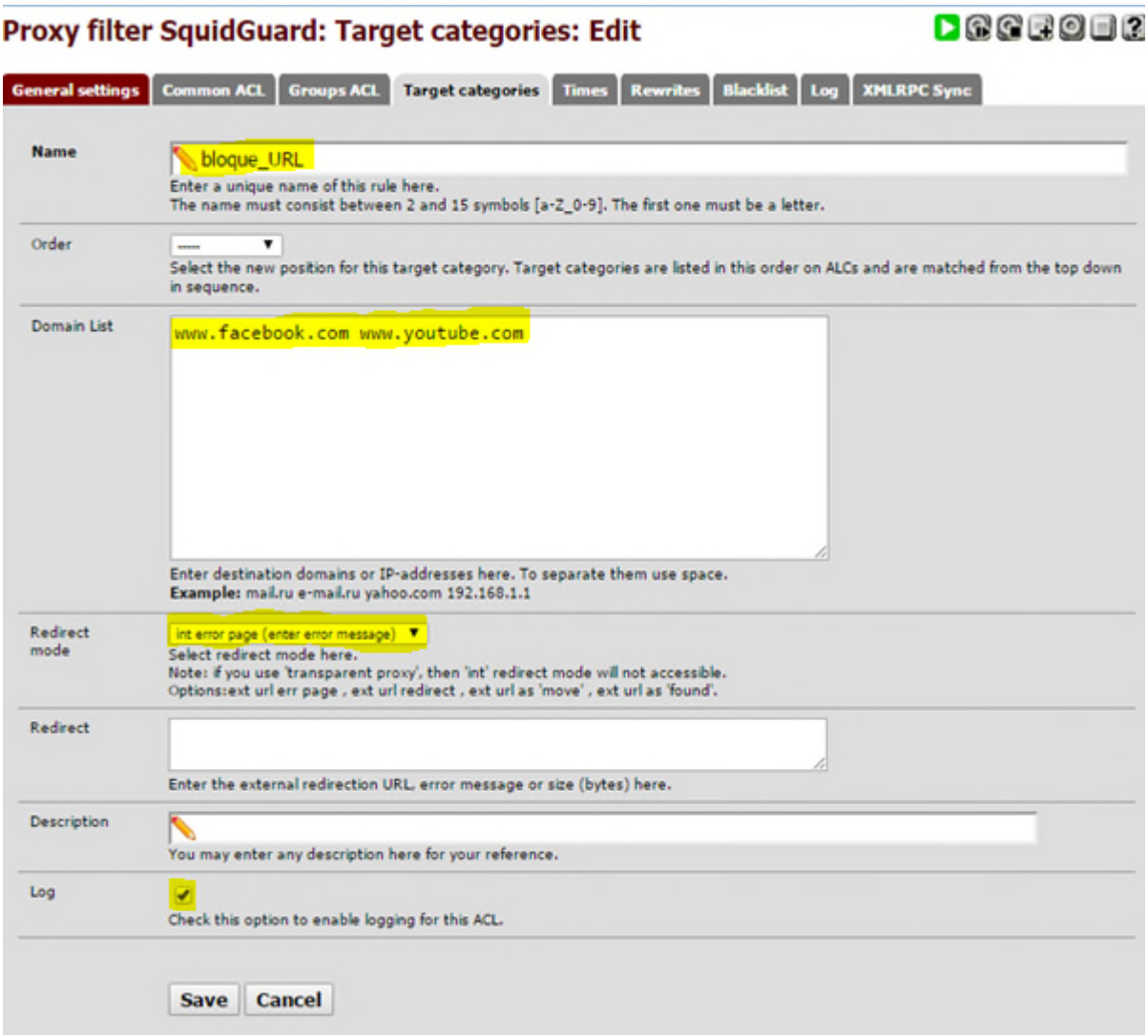

Figure IV.12: Création de l'ACL « bloque_URL »

En testant l'accès au site filtré : **www.facebook.com**, la page de redirection de proxy suivante s'affiche :

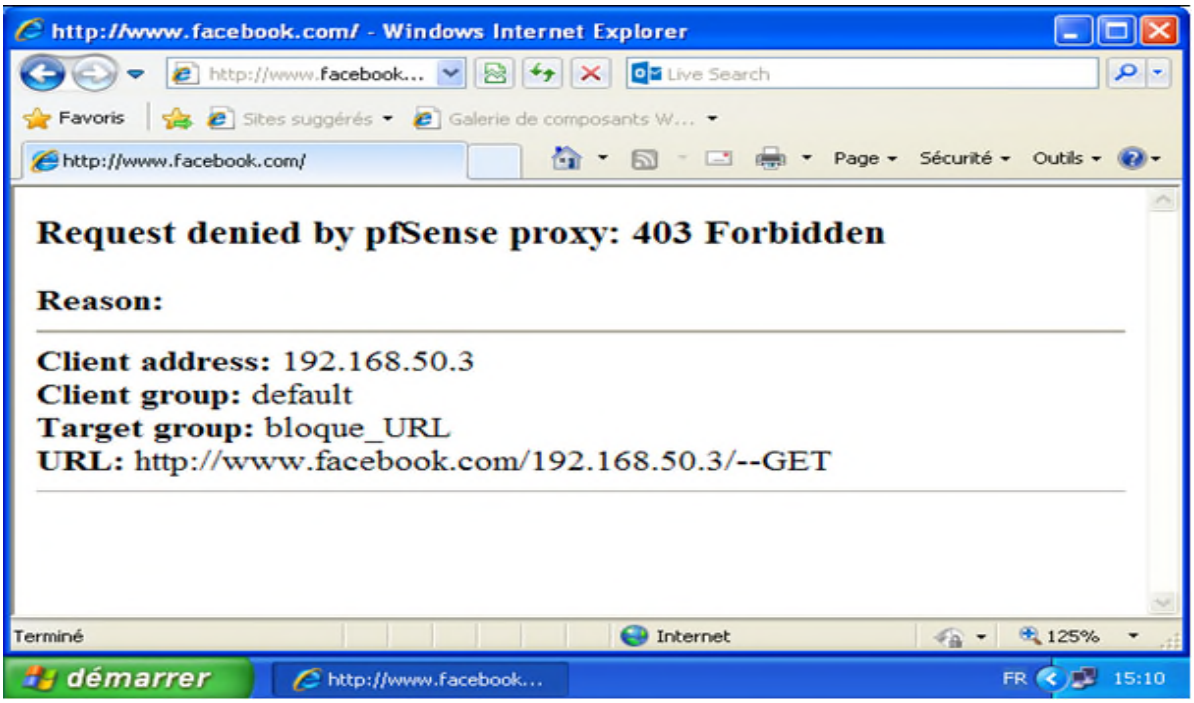

Figure IV.13: Résultat du test d'interdiction d'accès pour la catégorie « bloque_URL »

IV.2. Supervision de la bande Passante «Ntop»

1. Présentation de Ntop

Ntop est une sonde d'analyse du trafic réseau qui nous permet d'avoir un œil sur l'utilisation de notre réseau, en temps réel. Nous pouvons également le qualifier de superviseur de bande passante [4].

2. Installation et configuration

- Installation de Ntop :

Figure IV.14: Installation de package Ntop

- Configuration de Ntop :

Une fois l'installation terminée, se rendre dans le menu « **Diagnostics** -> **ntop settings** » pour initialiser **Ntop** et lancer le service correspondant.

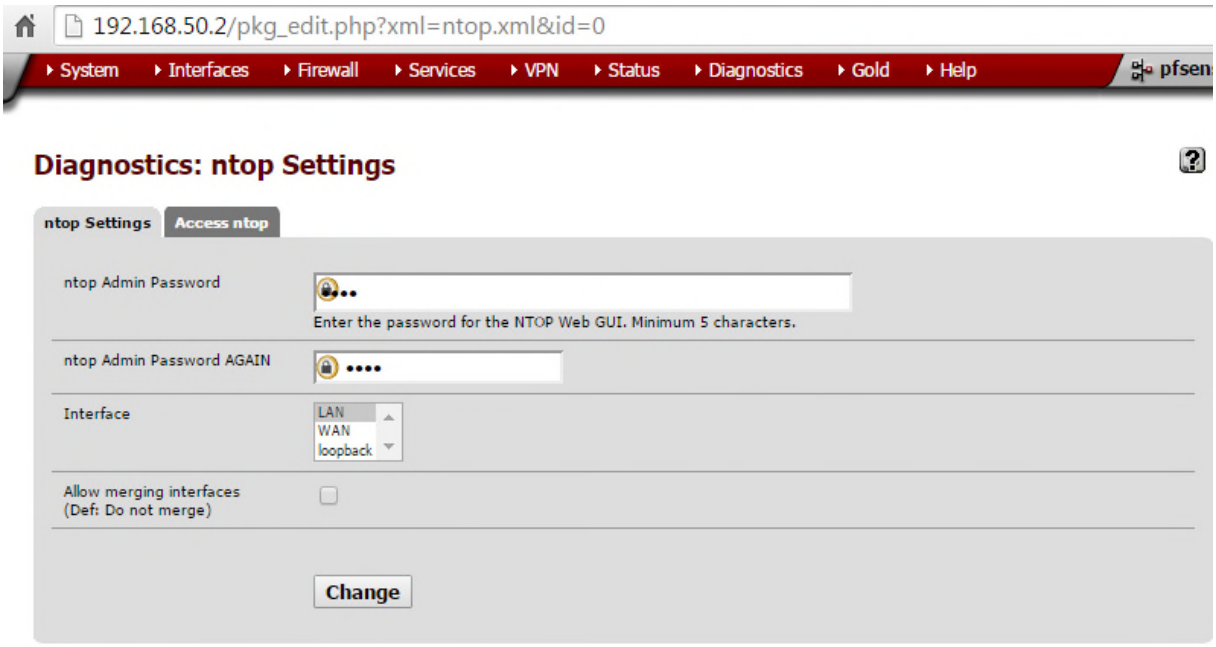

Figure IV.15: Configuration de compte administrateur

- Puis allons au menu « **Diagnostics** -> **ntop** » pour accéder aux statistiques générales de réseau LAN en temps réels. Nous avons obtenu les résultats suivants :

  ✓ La répartition totale du trafic par protocole :

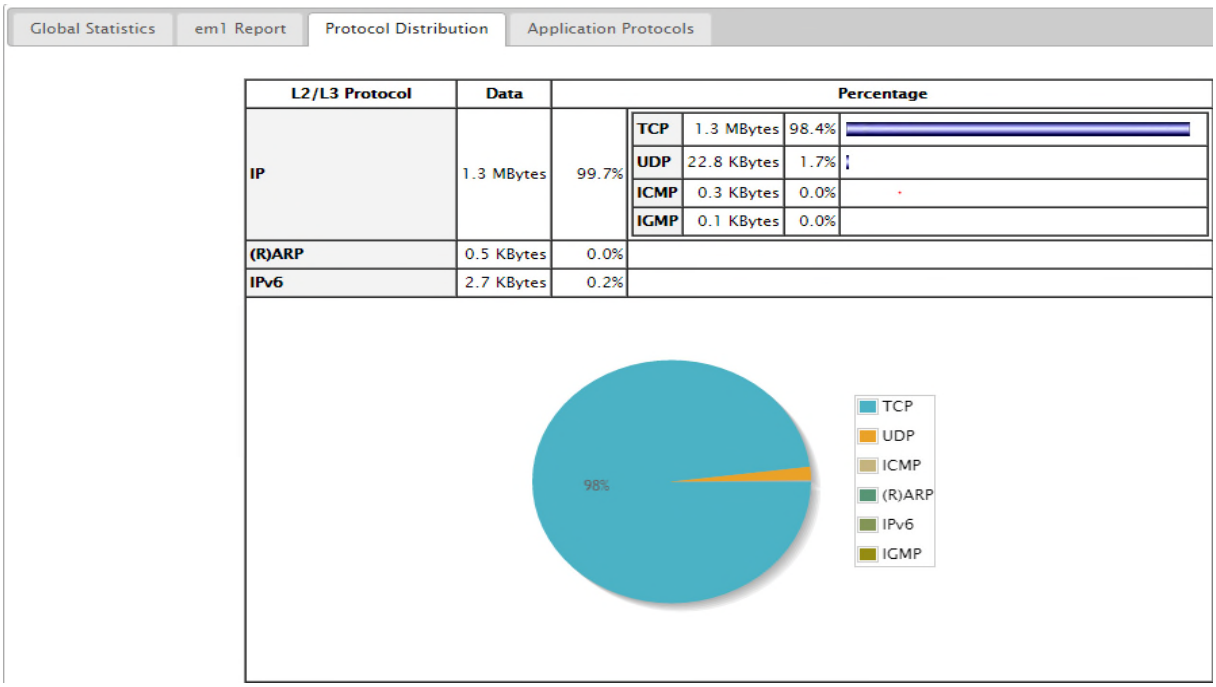

Figure IV.16: La répartition totale du trafic par protocole

✓ Ou encore un diagramme détaillé du trafic par services :

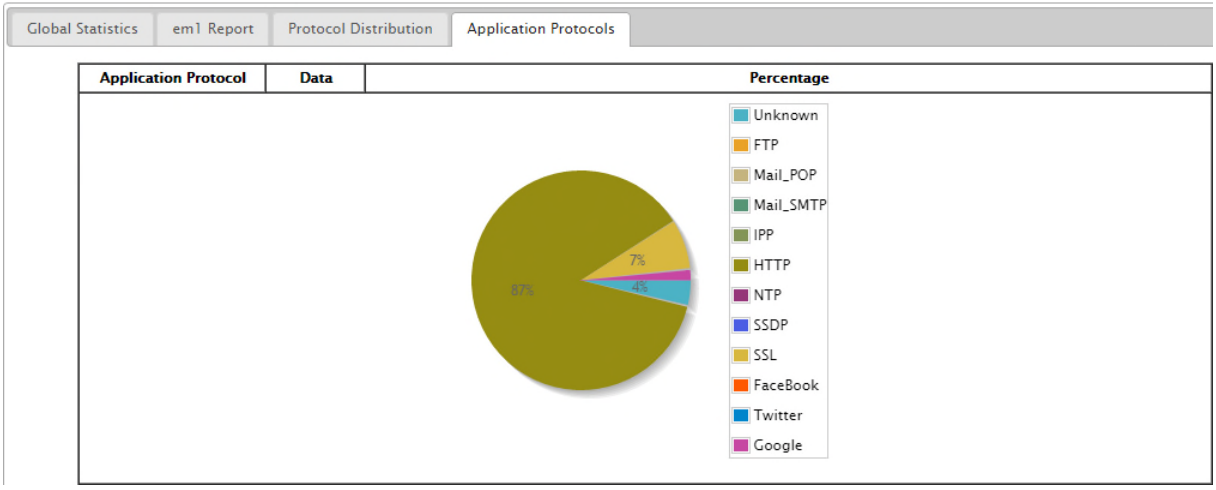

Figure IV.17: Diagramme du trafic par service

Conclusion

Dans ce chapitre nous avons utilisé une stratégie de filtrage en se servant des solutions libres, à savoir Squid pour le proxy et SquidGuard pour l'élément de filtrage. Tout l'intérêt ici réside dans la facilité de filtrage que Squid et SquidGuard peut nous fournir, tout en gardant une grande efficacité en se basant sur une liste noire « ici Shalla » mise à jour régulièrement. Nous gardons également la possibilité de rajouter simplement nos propres entrées. Tout ceci de manière transparente pour l'utilisateur.

Nous avons ajouté le paquet « Ntop : solution libre » qui permet la supervision de la bande passante.

Conclusion générale

Un pare-feu donc a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

Les recherches pour faire évoluer les technologies de filtrage sont nées du besoin de sécuriser les échanges réseaux. Pour améliorer ce filtrage il a été nécessaire de remonter dans les couches OSI, ce qui a été rendu possible grâce à une technologie logicielle et matérielle de plus en plus rapide.

Comme on peut le constater, les firewalls possèdent de multiples capacités qui peuvent différer en fonction de leurs types. Cette multitude de solutions impose donc une étude rigoureuse de la sécurité devant être mise en place.

Dans notre mémoire nous avons mis en place un firewall open source « PfSense » sous VMware qui permet de faire office de firewall et de routeur. Au delà de ça, il offre beaucoup de fonctionnalités très poussées comme : le NAT, le DHCP etc. De plus, l'ajout de packages (Paquets) permet à PfSense d'être totalement modulable et d'agrandir encore plus son panel de fonctionnalités. Dans notre projet nous avons ajouté (installer et configurer) le package « **Ntop** » pour la supervision de la bande passante et les packages « **Squid** » et « **SquidGuard** » afin de permettre le **filtrage d'URL**.

Perspectives futures :

- D'autres fonctionnalités avec le rajout des packages (exp: le paquet SNORT pour la détection et la prévention d'intrusion réseaux),
- Configuration d'autres services (exp: portail captif),
- Ce travail gagnerait davantage une fois le pare-feu testé sur des réseaux réels.

RÉFÉRENCES

Bibliographie :

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

[2] : Solange Ghernaouti -Hélie. Sécurité Internet « stratégies et technologies ». Dunod, Paris, 2000.

[3] : Jean- François Carpentier. La sécurité informatique dans la petite entreprise. 2ième édition, copyright-Edition ENI- Décembre 2012.

[4] : Anthony Costanzo, Damien Grillat, Lylian Lefrancois. Etude des principaux services fournis par PfSense. 2009. In: ftp://ftp.udg.co.cu/pub/others/pfsense%20firewall/PFsense.pdf

[5] : Ismail Rachdaoui. PFSense FreeBSB. Génie Réseaux et Télécommunications ENSA Marrakech, 2013. In: http://fr.slideshare.net/ISMAILRACHDAOUI/installation-et-configuration-de-pfsense

[6] : Michael W.Lucas. Le guide complet du FreeBSD. 2008. In http://www.pearson.fr/resources/titles/27440100468110/extras/introduction.pdf

[7]: Marwen Ben Cheikh Ali, Khlifa Hammami. Mise en place d'un firewall open source PfSense. Université de Tunis, 2012. In: http://fr.slideshare.net/marwenbencheikhali/rapport-finiale

Webographie :

[8] http://firewalls.chez.com/chapitre2.html: le firewall, une technique de protection

[9] http://wapiti.telecom-lille1.eu/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2000/Blick%20Lammari/site/firewall/fontionnement.htm: Les fonctionnalités d'un pare-feu

[10] https://saboursecurity.wordpress.com/2010/12/30/quelques-solutions-pare-feu-open-source/: Quelques solutions pare-feu Open Source

[11] http://www.diagramme-de-gantt.fr/: Le diagramme de GANTT

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

[13] http://www.todoo.biz/pfsense.php: Les solutions de firewalling OpenSource

Résumé

Les pare-feux sont devenus très populaires en tant qu'outils de sécurité pour les réseaux. Un firewall offre au système une protection d'un réseau interne, contre un certain nombre d'intrusions venant de l'extérieur, grâce à des techniques de filtrage rapides et intelligentes.

L'objectif de ce travail est la mise en place d'un firewall open source, PfSense comme solution. Ce pare-feu offre un panel de fonctionnalités de type NAT, DHCP, …etc., auquel nous avons ajouté le package « Ntop » pour la supervision de la bande passante et les paquets « Squid » / « SquidGuard » qui servent au filtrage d'URL et enregistrer l'utilisation de l'accès à Internet.

Mots clés: Pare-feu, Sécurité des réseaux, PfSense, Squid, SquidGuard, filtrage d'URL, Ntop.

Abstract

Firewalls have become very popular as security tools for networks. A firewall provides the system a very efficient protection of the internal network against, the intrusions coming from outside, stop potential damage and attacks, due to quick and intelligent filtering techniques.

The object of this work is "set up an open source firewall", PfSense as a solution. This firewall offers a range of features like: NAT, DHCP etc., to which we have added the package "Ntop" for the supervision of bandwidth and packages "Squid" / "SquidGuard" that serve to filter URLs and record the use of the Internet access.

Keyword: Firewalls, Networks security, PfSense, Ntop, Squid, SquidGuard, URL filtering.