République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

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

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

De MASTER ACADEMIQUE

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Présenté par :

M elle AIBOUD Noura

M elle AHMED ZAID Sonia

Thème

Proposition d'une solution de filtrage de sites web indésirables en vue de l'optimisation d'un réseau informatique

Mr OUALLOUCHE, Maitre de conférences B, UMMTO, Président

Mr LAZRI, Maitre de conférences A, UMMTO, Encadreur

Mr CHELI, Maitre consistant A, UMMTO, Examinateur

Soutenu le : 02/07/2018

Remerciements

Nous tenons à remercier tout d'abord DIEU le tout puissant qui nous a donné, durant toutes ces années, la santé, le courage et la foi pour arriver a ce jour.

Nous ne pouvons réellement trouver, les expressions éloquentes que mérite notre encadreur : Mr LAZRI Mourad, ainsi que toutes les personnes de centre de calcul de Hasnaoua afin de les remercier pour leurs sympathies, leurs encouragements, leurs aide, leurs dévouement pour le travail et leurs présence au cours de cette étude

Nous adressons nos remerciements aux membres de jury qui nous ont fait l'honneur d'évaluer, d'examiner, d'enrichir ce travail.

Nos remerciements vont également à tous les enseignants et les responsables de notre faculté de génie électrique et d'informatique.

Dédicaces

Aux être qui me sont les plus chers

« MES PARENTS »

Pour leurs AMOUR leur EDUCATION et leurs SACRIFICES.

A mes frères et mes sœurs, pour qui je souhaite la réussite dans leurs projets en avenir.

A toute ma famille.

A ma binôme.

A tous mes amis.

A tous ceux qui m'ont aidé à faire ce travail.

AIBOUD Noura

Je dédie ce travail à :

-Mon très cher oncle Farid,

- Ma très chère mère,

- Ma très chère grand- mère,

- Mon très cher père,

-A mes tendres frère et sœurs,

-A tous mes oncles, tantes, cousins et cousines,

-A ma binôme,

-A tout mes ami(e)s et camarades,

-A ceux que j'aime et qui m'aiment,

AHMED ZAID Sonia

Sommaire

LISTE DES FIGURES

GLOSSAIRE

A

ACL: Access Control List

ADSL: Asymetric Digital Subscriber Line

ATM: Asynchronous Transfert Mode

AUI: Attachment unit interface

B

BGP: Border Gateway Protocol

BNC: Bayonet Neill–Concelman connector

C

CA: Certificate Authority

D

DCE: Data Circuit Equipement

DHCP: Dynamic Host Configuration Protocol.

DTE: Data Terminal Equipement

E

EIGRP: Enhanced Interior Gateway Routing Protocol

ETCD : Equipement Terminal de Circuit de Données

ETTD : Equipement Terminal de Traitement de Données

F

FDDI: Fiber Distributed Data Interface

FTP: File Transfert Protocol

H

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Security.

I

ICMP: Internet Control Message Protocol

IGMP: Internet Group Management Protocol

IGRP: Interior Gateway Routing Protocol

IP: Internet Protocol

IPSec: Internet Protocol Security

IS-IS: Intermediate System-to-Intermediate System

ISO: International Organization for Standardization

L

LAN: Local Area Network

N

NAT: Network Address Translation

NRZ: Non Retour à Zéro

M

MAC: Media Access Control

MAN: Metropolitan Area Network

MAU: Multistation Access Unit

O

OSI: Open Systems Interconnection

OSPF: Open Shortest Path First

P

PAN: Personal Area Network

PAT: Port Address Translation

PF: Packet Filter

PKI: Public Key Infrastructure

R

RIP: Routing Information Protocol

RZ: Retour à Zéro

S

SMTP: Simple Mail Transport Protocol

SSH: Secure Shell

SSL: Secure Sockets Layer

T

TCP: Transmission Control Protocol

U

UDP: User Datagram Protocol

URL: Uniform Resource Locator

V

VPN: Virtual Private Network

W

WAN: Wide Area Network

Introduction

Introduction

Les réseaux informatiques sont devenus ces dernières années, des axes majeurs de communication. L'accroissement des trafics en télécommunications révèlent les besoins grandissants d'échanges privés et professionnels. Ces transmissions de données imposent une ouverture des systèmes d'informations 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. 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 certains 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 pour la sécurité informatique afin d'identifier les sources de menaces et ses dégâts informationnels et permet d'avoir un réseau optimal, des applications utilisées pour sécurités ont été développées par [1, 2].

Dans ce contexte, nous allons implémenter une application permettant de filtrer des sites indésirables au niveau d'un réseau local. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivantes :

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

Pour mener à bien notre travail, nous avons structuré ce mémoire en quatre chapitres :

Dans le premier chapitre, nous donnons des généralités et concepts des réseaux informatiques.

Le deuxième chapitre est consacré à la présentation des notions de base de la transmission de flux de données dans un réseau informatique.

Dans le troisième chapitre, nous exposons le problème de la sécurité dans un réseau informatique.

Dans le quatrième chapitre, nous proposons la solution pour optimiser le réseau informatique. Nous terminons notre travail par une conclusion dans laquelle une perspective est proposée.

Chapitre I

Généralités sur les réseaux informatiques

I. Préambule :

Nous exposons dans ce chapitre quelques généralités sur l'architecture des réseaux de communications. Nous présenterons divers définitions et concepts propres au domaine des réseaux informatique, notons bien qu'il ne s'agit pas de détailler avec précision le monde des réseaux informatique mais de donner les notions de base.

II. Définition d'un réseau informatique :

Un réseau est un ensemble d'équipements électroniques (ordinateurs, imprimantes, scanners, modems, routeurs, commutateurs...) interconnectés et capables de communiquer (émettre et recevoir des messages) par l'intermédiaire d'un support de communication.

Un réseau informatique permet donc l'échange d'informations (messageries, transfert de fichiers) et le partage des ressources (imprimante).

Il a pour objectif :

- Le partage des fichiers, d'applications et de ressources matérielles.
- La communication entre les personnes ou entre processus.
- L'unicité de l'information.

III. Catégories de réseaux informatiques :

On distingue quatre catégories de réseaux informatiques selon leur taille (nombre de machines) et leur étendue (voir figure I.1) :

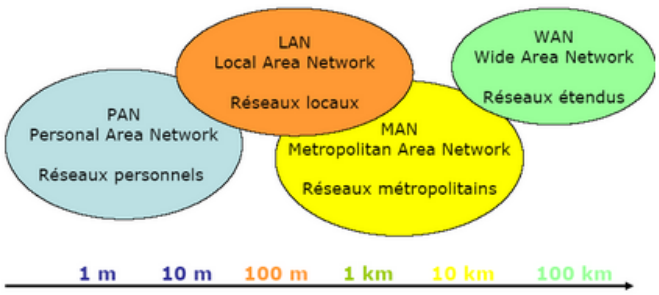

Figure I.1 : Classification des réseaux selon la taille.

- **PAN (Personal Area Network):**

Il désigne un réseau restreint d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle. Ces réseaux interconnectent sur quelques mètres les équipements personnels tels que des téléphones mobiles.

- **LAN (Local Area Network) :**

C'est un réseau informatique à une échelle géographique relativement restreinte, il est utilisé pour relier les ordinateurs entre eux (par exemple d'une habitation particulière, d'une entreprise, d'une salle informatique, d'un bâtiment). L'infrastructure est privée et est gérée localement. La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

- **MAN (Métropolitain Area Network) :**

Un réseau métropolitain est défini à l'échelle d'un quartier, il peut couvrir l'étendue d'une ville. Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). Ils s'étendent à des distances allant de deux kilomètres jusqu'à une dizaine de kilomètre et ne dépassant pas les 200 kilomètres.

- **WAN (Wide Area Network):**

Le WAN permet l'interconnexion de plusieurs LANs ou MANs sur de grandes distances géographiques, à l'échelle d'un pays ou mondiale. A la différence du LAN qui est un réseau privé, le WAN emprunte les infrastructures publiques telles Internet, ou celles d'un opérateur.

IV. Topologies des réseaux :

On peut différencier les réseaux selon leur structure ou plus précisément leur topologie. La topologie d'un réseau décrit la manière dont les nœuds sont connectés. On distingue deux types de topologies :

IV.1. La topologie physique :

Elle correspond à la disposition physique des différents équipements les uns par rapport aux autres. Il en existe généralement:

❖ **Topologie en bus :**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial (voir figure I.2). Les connecteurs utilisés sont de types : connecteur en T. Le mot « bus» désigne la ligne physique qui relie les machines du réseau. Une seule station émet sur le bus. Lorsque celle-ci émet, la trame parcourt tout le bus jusqu'à ce qu'elle arrive au destinataire. A chaque extrémité, le réseau est terminé par une résistance (appelé bouchon) pour empêcher l'apparition de signaux parasites. L'exemple le plus courant de ce type de réseau est le réseau Ethernet.

Figure I.2 : la topologie en bus.

❖ **Topologie en anneau :**

Il s'agit d'un réseau local dans lequel les nœuds sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) (voir figure I.3). Les données circulent sur un anneau d'un nœud à l'autre. A un instant donné, un seul nœud peut émettre sur le réseau. Il ne peut donc pas se produire de collision entre deux messages contrairement au cas du réseau de type bus. Un jeton (qui est en fait une trame de donnée) circule en permanence le long de la boucle.

Lorsqu' aucun nœud n'émet de message, le jeton est dans un état libre (trame vide). Seul le nœud qui a envoyé le message est en attente d'un accusé de réception. Les autres nœuds n'étant pas en alerte, se contentent de retransmettre l'accusé de réception sans le lire. Lorsque le jeton arrive à la station émettrice celle-ci vérifie l'accusé de

réception, retire son message et rend le jeton libre et ainsi de suite… Cette topologie est utilisée par les réseaux Token-Ring et FDDI.

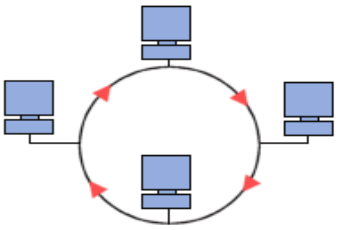

Figure I.3 : la topologie en anneau.

❖ **Topologie en étoile :**

Dans un réseau en étoile, chaque nœud du réseau est relié à un nœud central (Switch ou hub) par un câble RJ45 (voir figure I.4). Ce nœud est un appareil qui recevant un signal de données par une de ses entrées, va retransmettre ce signal à chacune des autres entrées sur lesquelles sont connectés des ordinateurs ou périphériques, voir d'autres nœuds.

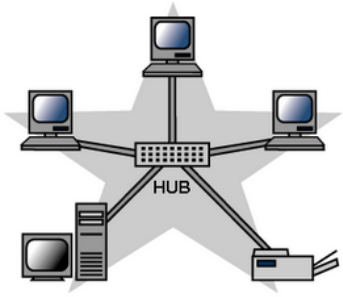

Figure I.4 : la topologie en étoile.

IV.2. La topologie logique :

Désigne le mode de circulation des données d'une machine vers une autre. On distingue:

➢ **Réseaux point à point :**

Ces réseaux sont caractérisés par un canal de communication qui ne relie que deux machines (liaison point à point), c'est-à-dire que pour arriver à sa destination, un message doit transiter par plusieurs machines intermédiaires.

Pour permettre l'échange d'information entre deux éléments d'un réseau, il faut nécessairement pouvoir adresser les membres du réseau. Une technique consiste à ajouter l'adresse du destinataire à chaque message. Comme le destinataire n'est pas forcément relié directement à l'expéditeur, le message va transiter par des nœuds intermédiaires qui décodent l'adresse et qui envoient le message sur le prochain nœud dans la bonne direction.

En cas de panne d'un élément, le réseau tombe en panne.

- **Réseaux de diffusion :**

Consiste à partager un seul support de transmission, chaque message envoyé par un équipement sur le réseau est reçu par tous les autres (voir figure I.5). A tout moment chaque équipement a le droit d'envoyer un message sur le support, il faut juste écouter au préalable si la voie est libre, sinon il doit attendre.

Les réseaux locaux adoptent pour la plupart des cas, le mode diffusion sur une architecture en bus ou en anneau.

La rupture du support provoque l'arrêt du réseau, par contre la panne d'un des éléments ne provoque pas la panne globale du réseau.

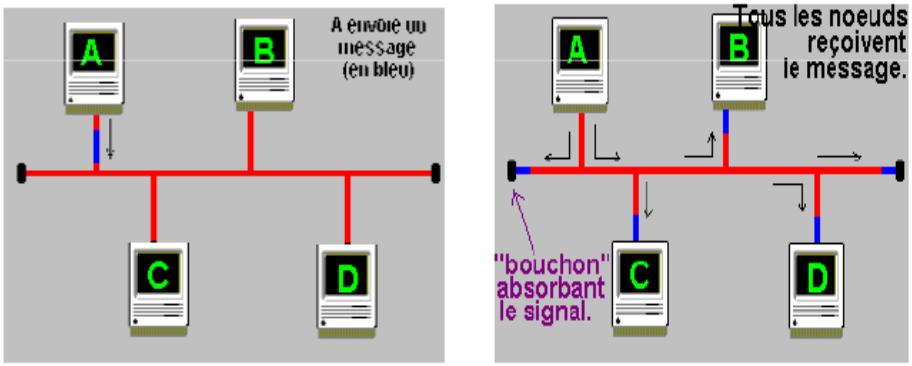

Figure I.5 : le mode de diffusion.

V. Architecture réseau :

Un réseau permet de connecter des ordinateurs entre eux, mais les besoins sont très divers, depuis le réseau domestique ou d'une toute petite entreprise jusqu'aux réseaux des grandes sociétés. Deux approches fondamentalement différentes, encore que l'une peut facilement évoluer vers l'autre :

a. Client-serveur :

Cette architecture centralise des ressources sur un serveur qui offre des services pour des clients. Ces services peuvent être :

- Connexion à Internet.
- Impression.
- Utilisation des applications.

L'architecture client/serveur désigne un mode de communication à travers un réseau entre plusieurs programmes ou logiciels :

- Le processus client envoie des requêtes pour demander un service.
- Le processus serveur attend les requêtes des clients et y répond en offrant le service.

Les avantages :

Parmi les avantages on a :

- ✓ Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "poste à poste".
- ✓ Les serveurs étant toujours en service (sauf en cas de panne), les ressources sont toujours disponibles pour les utilisateurs.
- ✓ Un administrateur gère le fonctionnement du réseau et les utilisateurs n'ont pas à s'en préoccuper.

Les inconvénients :

Il y en a quelques-uns :

- ✓ La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste".
- ✓ Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.
- ✓ Le coût est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.

- ✓ Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer un fonctionnement au moins minimum en cas de panne.

Ce type de réseau est évidemment le plus performant et le plus fiable. Vous l'aurez compris, ce n'est pas la solution la plus simple pour un réseau domestique, c'est cependant ce type d'architecture que l'on retrouve sur les réseaux d'entreprise, qui peut parfaitement supporter plusieurs centaines de clients, voire plusieurs milliers.

b. Poste à poste :

Les postes de travail sont simplement reliés entre eux par le réseau. Aucune machine ne joue un rôle particulier. Chaque poste peut partager ses ressources avec les autres postes. C'est à l'utilisateur de chaque poste de définir l'accès à ses ressources. Il n'y a pas obligatoirement d'administrateur attitré.

Les avantages :

Il y en a quelques uns :

- ✓ Il est facile de mettre en réseau des postes qui étaient au départ isolés.
- ✓ Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.
- ✓ Cette méthode est pratique et peu coûteuse pour créer un réseau domestique.

Les inconvénients :

Parmi les inconvénients on a :

- ✓ Chaque utilisateur a la responsabilité du fonctionnement du réseau.
- ✓ Les outils de sécurité sont très limités.
- ✓ Si un poste est éteint ou s'il se plante, ses ressources ne sont plus accessibles.
- ✓ Le système devient ingérable lorsque le nombre de postes augmente.

Ce type de réseau n'offre de réel intérêt que dans une configuration particulière :

- Les postes sont peu nombreux (pas plus d'une dizaine).
- Les utilisateurs restent attachés à un poste dont ils sont responsables.

VI. Commutation :

Il existe plusieurs types de commutation, dont les principaux sont :

❖ La commutation de circuit :

Elle consiste à créer dans le réseau un circuit particulier entre l'émetteur et le récepteur (voir figure I.6), avant que ceux-ci ne commence à échanger des informations. Ce circuit sera propre aux deux entités communiquant et il sera libéré lorsque l'une des deux coupera sa communication. Par contre si, pendant un certain temps, les deux entités ne s'échangent rien, le circuit leur reste quand même attribué. C'est pourquoi, un même circuit (ou portion de circuit) pourra être attribué à plusieurs communications en même temps. Cela améliore le fonctionnement global du réseau, mais pose des problèmes de gestion (files d'attente, mémorisation,…).

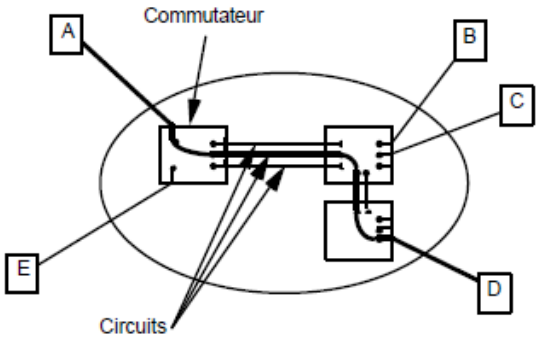

Figure I.6 : principe de la commutation de circuit.

❖ La commutation de messages :

Elle consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation en nœud de commutation (voir figure I.7). Chaque nœud attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant.

Ce mode de commutation a pratiquement disparu au profit de la commutation de paquets.

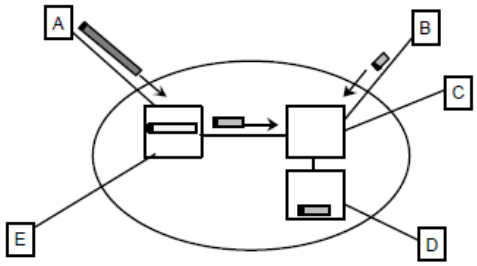

Figure 1.7 : principe de la commutation de messages.

❖ La commutation de paquets :

Un message émis est découpé en paquets et, par la suite, chaque paquet est commuté à travers le réseau comme dans le cas des messages. Les paquets sont envoyés indépendamment les uns des autres (voir figure I.8). Chaque nœud redirige chaque paquet vers la bonne liaison et le récepteur final va reconstituer le message émis en réassemblant les paquets. Ceci nécessitera un protocole particulier, car les paquets peuvent ne pas arriver dans l'ordre initial, soit qu'ils ont emprunté des routes différentes, soit parce que l'un d'eux a dû être réémis, suite à une erreur de transmission.

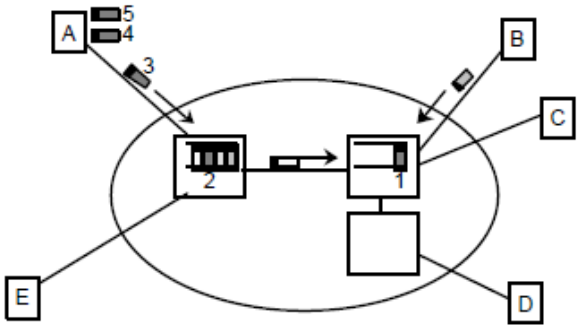

Figure I.8 : principe de la commutation de paquet.

❖ La commutation de cellules :

Une cellule est un paquet particulier dont la taille est toujours fixée à 53 octets. C'est la technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode), qui opèrent en mode connecté, où avant toute émission de cellules, un chemin virtuel est établi, par lequel passeront toutes les cellules. Cette technique mêle donc la commutation de circuits et la commutation de paquets de taille fixe, permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés.

VII. Les outils d'interconnexions :

Un réseau local sert à interconnecter les ordinateurs d'une organisation, Toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas, des équipements spécifiques sont nécessaires.

Voici les différents composants servants à la liaison, au routage et au contrôle du réseau. Tous ces composants peuvent être inactifs (hubs, ponts, répéteur), n'influant que sur la réémission du signal ou actifs (switch, routeurs) servant au routage, hardware au software des trames.

❖ **Le Pont : (Bridge)**

C'est un dispositif matériel, qui permette d'échanger les informations sur le réseau, il est utilisé pour interconnecté deux réseaux utilisant le même protocole. Il travaille au niveau logique de la deuxième couche de modèle OSI (Liaison de donnée). Le pont se base sur l'adresse MAC et le nom de la station sur le réseau pour savoir si la trame doit traverser le pont ou non. En d'autres termes, les informations ne passeront le pont que si elles doivent aller d'un réseau à l'autre.

Comme les ponts fonctionnent sur les couches basses du réseau, ils sont utilisables à peu près avec tous les protocoles. Ils n'offrent cependant que la possibilité d'interconnecter des réseaux physiques, ce qui limite considérablement leur emploi.

➢ **Son rôle :**

- Il est capable de filtré les trames on ne laisse passé que celles dans l'adresse correspond à une machine situé à l'opposé du pont.
- Il sert à relier de petits réseaux isolé, et leurs permet de fonctionner ensemble. C'est ce que l'on appelle un " INTER-RESEAU".
- De façon générale le pont améliore grandement les performances d'un réseau.

❖ **Le répéteur :**

Les répéteurs servent à prolonger la longueur des supports de transmissions, à savoir des câbles, des ondes, des fibres, …etc., qui relient tous les périphériques sur un réseau.

C'est un connecteur combinant à la fois un récepteur et un émetteur qui compense les pertes de transmissions sur une ligne, une fibre, un câble ou une onde, et ceci sur un réseau sans on modifier le contenu.

❖ **Le routeur :**

Les routeurs sont plus puissants, ils sont capables d'interconnecter plusieurs réseaux utilisant le même protocole entre eux (voir figure I.9). Ils travaillent au niveau de la couche 3 du modèle OSI (couche réseau), et tous les protocoles n'utilisent pas cette couche. C'est pourquoi l'on parle de protocoles "routables" ou "non routables". Les routeurs disposent d'une table de routage qui leur permet d'aiguiller les trames vers le bon réseau. Ils permettent une structure maillée, indispensable pour la construction de l'INTERNET.

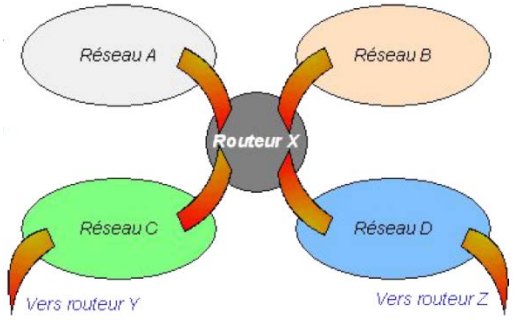

Figure I.9 : plusieurs réseaux interconnectant par un routeur.

❖ **La passerelle :**

Une passerelle est une interface permettant de faire communiquer entre deux réseaux n'utilisant pas le même protocole (relier les réseaux de types différents). Lorsqu'une passerelle reçoit des informations, elle les traduit sous forme d'informations que le réseau destinataire peut comprendre. Quand un réseau ne reconnait pas l'adresse de destination des informations, il transmet ces informations à un autre réseau en utilisant "une passerelle par défaut", cette dernière est très utilisée sur les réseaux TCP/IP tel qu'internet.

❖ **Le modem :**

C'est un périphérique de communication entre deux ordinateurs distant, en effet il permet d'échanger des données par l'intermédiaire d'un réseau téléphonique pour parcourir des grandes distances.

❖ **Le commutateur (Switch) :**

Est un équipement qui relie plusieurs câbles ou fibre au réseau informatique, ou au réseau de télécommunication. Il permet de créer des circuits virtuels et également de diriger les informations vers une destination précise sur ce réseau (il envoie les données uniquement aux destinataires qui doivent les recevoir). Un Switch permet d'assurer la sécurité des informations transmises sur ce réseau.

Le fonctionnement d'un Switch se base sur l'adresse MAC, pour pouvoir envoyer les données au destinataire approprié, et il comporte dans sa mémoire une table nommée « Table d'adresse MAC » cette table contient une correspondance de l'adresse MAC d'un ordinateur et le nom de l'interface auquel est connecté.

❖ **Le concentrateur (Hub) :**

Point de connexion commun aux périphériques d'un réseau. Généralement utilisé pour la connexion de segments d'un réseau local. Un concentrateur comporte plusieurs ports (voir figure I.10). Lorsque les données arrivent à l'un des ports, elles sont copiées vers les autres ports de sorte que tous les segments du réseau local puissent voir les données (tous les ordinateurs reçoivent les données envoyés par le concentrateur).

Figure I.10 : mini hub 16/8 ports.

VIII. Description du modèle OSI :

Le modèle OSI (Open Systems Interconnection) ou « modèle de référence pour l'interconnexion des systèmes » ouverts a été normalisé par l'ISO (International Standardization Organisation) dans les années 80.

Ce modèle définit une architecture de référence permettant la communication entre différents systèmes hétérogènes. Les tâches à effectuer sont structurées en 7 niveaux appelés couches (voir figure I.11).

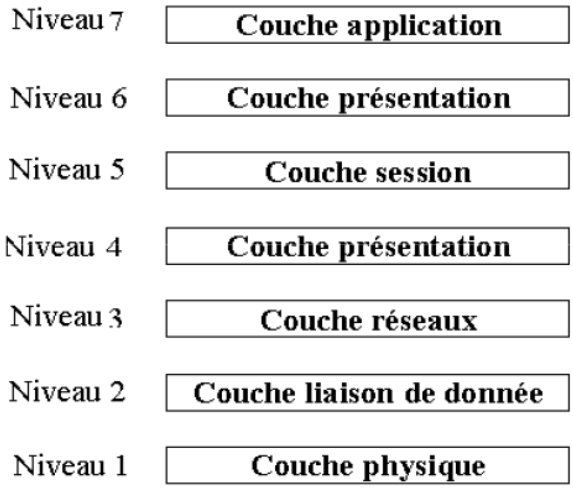

Figure I.11 : modèle de référence OSI.

1. La couche physique :

Elle décrit les caractéristiques physiques de la communication, comme le média utilisé (câbles cuivre, fibre optique ou radio), et tous les détails associés comme les connecteurs, les types de codage, le niveau des signaux, ... et les distances maximales. Elle assure la transmission des bits de la trame de la couche supérieure sur le réseau physique.

2. La couche de liaison :

Elle spécifie comment les paquets de la couche supérieure seront transportés. Elle assure la mise en trames, leurs acheminements sans erreurs et la méthode d'accès au réseau physique.

3. La couche réseau :

Elle résout le problème de l'acheminement des paquets à travers un réseau. Elle permet de transférer des données pour de nombreux protocoles de plus haut niveau.

4. La couche transport :

Cette couche est responsable du transport des données de bout en bout (c'est-à-dire de processus à processus) au travers du réseau.

5. La couche session :

Elle établit une communication entre émetteur et récepteur en assurant l'ouverture et la fermeture des sessions.

6. La couche présentation :

Cette couche met en forme les informations échangées pour les rendre compatibles avec l'application destinatrice, dans le cas de dialogue entre systèmes hétérogènes. Elle peut comporter des fonctions de traduction, de compression, d'encryptage, ...

7. La couche application :

Elle va apporter les services de base offerts par le réseau pour les logiciels applicatifs.

IX. Architecture de TCP/IP :

TCP/IP représente l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données.

TCP/IP est une suite de protocoles TCP/IP signifie « Transmission Control Protocol/Internet Protocol ».

- ✓ **TCP :** ce protocole a en charge le découpage du message en datagrammes, le réassemblage à l'arrivée avec remise dans le bon ordre, ainsi que la réémission de ce qui a été perdu.
- ✓ **IP :** il assure le routage des datagrammes.

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches (voir figure I.12).

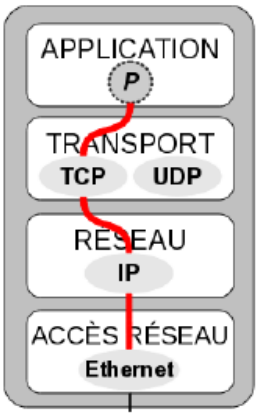

Figure I.12 : Les 4 couches du modèle TCP/IP.

- **La couche accès réseau:**

Est l'interface avec le réseau et est constituée d'un driver du système d'exploitation et d'une carte d'interface de l'ordinateur avec le réseau.

- **La couche internet :**

Gère la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol).

- **Couche transport :**

Assure tout d'abord la communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol), FTP (File Transfert Protocol) ou non fiable dans le cas de UDP (User Datagram Protocol).

- **La couche application :**

Est celle des programmes utilisateurs comme telnet (connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transport Protocol), etc.

X. Adressage IP :

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière. En effet, un même routeur interconnectant deux réseaux différents possède une adresse IP est toujours représentée dans une notation décimale pointée constituée de quatre nombres (1 par octet), compris enter « 0 » et « 255 », et séparés par un point (exemple : 192.49.144.1 est une adresse IP).

A. Les classes d'adresse IP :

Plus précisément, une adresse IP est constituée d'une paire (id. de réseau, id. de machine) et appartient à une certaine classe (A, B, C, D ou E) selon la valeur de son premier octet (voir figure I.13).

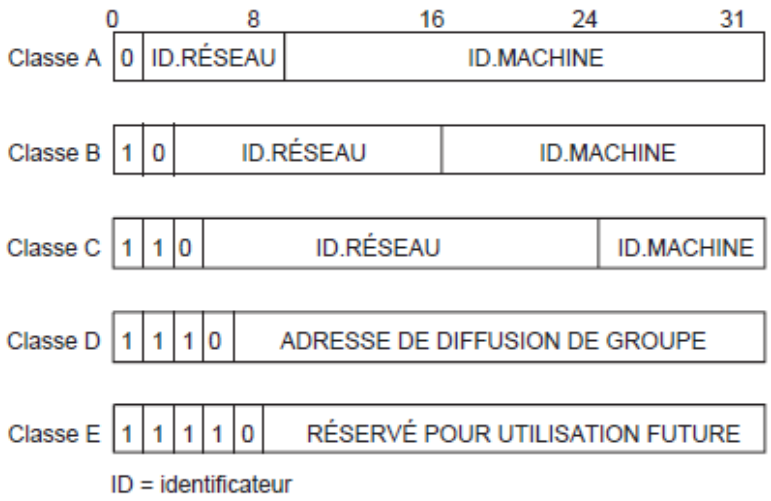

Figure I.13 : Structure générale d'une adresse IP.

- ✓ **Les adresses de classe A :** Destinée aux réseaux de très grande taille, avec un très grand nombre d'ordinateurs, la classe A autorise 16 millions d'adresses différentes.
- ✓ **Les adresses de classe B :** classe intermédiaire destinée aux réseaux de grande taille tels que ceux des multinationales et des organismes de recherche. Il peut y avoir jusqu'à 16384 adresses, et chaque réseau correspondant à une adresse en classe B peut gérer 65000 adresses de machine.

- ✓ **Les adresses de classe C :** Destinée aux petits réseaux, la classe C autorise plus de 2 millions d'adresses réseau, mais chacun de ces réseaux en classe C ne peut proposer que 255 adresses différentes pour les machines qu'il réunit.
- ✓ **Les adresses de classe D et E :** sont réservées pour mettre en œuvre le mécanisme de diffusion de groupe.

B. Notion de sous-réseaux et de masque :

La hiérarchie à deux niveaux (réseau et machine) de l'adressage IP s'est rapidement révélée insuffisante à cause de la diversité des architectures des réseaux d'organisation connectés. La notion de sous-réseau fut introduite en 1984 et a conservé le format de l'adresse IP sur 32 bits. Dans un réseau subdivisé en plusieurs sous-réseaux, on exploite autrement le champ identifiant de machine de l'adresse IP. Celui-ci se décompose désormais en un identifiant de sous-réseau et un identifiant de machine. Remarquons que ce découpage n'est connu qu'à l'intérieur du réseau lui-même. En d'autres termes, une adresse IP, vue de l'extérieur, reste une adresse sur 32 bits. On ne peut donc pas savoir si le réseau d'organisation est constitué d'un seul réseau ou subdivisé en plusieurs sous-réseaux.

Le masque de sous-réseau (netmask) est alors utilisé pour différencier les bits réservés à l'adressage des sous-réseaux de ceux qui correspondent à la machine. Il contient des 1 sur toute la partie identifiant le réseau et les bits de sous-réseau et des 0 sur la partie réservée au numéro de machine dans le sous-réseau.

Lorsqu'une station d'un (sous-)réseau veut émettre un message à une autre, elle compare sa propre adresse à celle du destinataire, bit à bit en utilisant le masque de sous-réseau. Si sur toute la partie identifiée par les 1 du masque de sous-réseau, il y a égalité, les deux stations se trouvent dans le même (sous-)réseau, le message peut donc être transmis directement, sinon, il est envoyé à la machine qui assure l'acheminement du message vers l'extérieur (le routeur).

XI. Discussion :

Dans ce chapitre nous avons décrit brièvement le réseau informatique dont on a définit le réseau informatique ainsi que ses catégories et ses topologies, comme on a parlé de ses deux architectures client/serveur et poste à poste. La deuxième chose que

nous avons exposé c’est la notion de la commutation qui est une technique largement utilisée, puis les outils d'interconnections, les modèles de référence et ensuite l'adressage.

Chapitre II
Transmission du flux de données dans un réseau informatique

I. Préambule :

Pour la transmission de l'information nous avons besoin d'un support de transmission et d'une technique qui nous permet de la véhiculer sur ce support. Le principe de propagation des ondes constitue la base des techniques de transmission. La fiabilité de la liaison entre deux sites échangeant des informations dépend énormément des caractéristiques du support de transmission utilisé, telles que la bande passante, la capacité, la qualité du conducteur etc.

II. Les différents supports de transmission :

Pour relier les diverses entités d'un réseau, plusieurs supports de transmission de données peuvent être utilisés :

1. Les câbles coaxiaux :

Un câble coaxial est un support de transmission au niveau des réseaux, il permet de relier les ordinateurs pour échangées des données. Pour connecter les ordinateurs entre eux, il faut utiliser les connecteurs de types BNC « T » au niveau des réseaux en bus, il faut en plus ajouter " un bouchant de terminaison" aux extrémités de câble pour absorbées les signaux.

Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure (voir figure II.1).

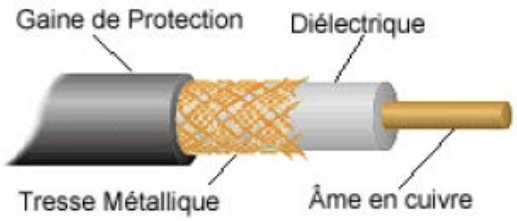

Figure II.1 : coupe d'un câble coaxial.

On distingue habituellement deux types de câbles coaxiaux:

- **Le 10Base2 - câble coaxial fin :**

Est un câble de fin diamètre (6 mm), de couleur blanche (ou grisâtre) par convention. Très flexible il peut être utilisé dans la majorité des réseaux, en le connectant directement sur la carte réseau. Il permet de transporter un signal sur une distance d'environ 185 mètres sans affaiblissement.

- **Le 10Base5 - câble coaxial épais :**

Est un câble blindé de plus gros diamètre (12 mm) et de 50 ohms d'impédance. Il a longtemps été utilisé dans les réseaux Ethernet, ce qui lui a valu l'appellation de « Câble Ethernet Standard ». Etant donné que son âme à un plus gros diamètre, la distance susceptible d'être parcourue par les signaux est grande, cela lui permet de transmettre sans affaiblissement des signaux sur une distance atteignant 500 mètres, Sa bande passante est de 10 Mbps. Il est donc employé très souvent comme câble principal pour relier des petits réseaux dont les ordinateurs sont connectés avec du câble coaxial fin. Il est moins flexible que le câble coaxial fin.

2. Le câble à paire torsadée :

Est un câble téléphonique constitué à l'origine de deux fils de cuivre isolés et enroulés l'un sur l'autre (voir figure II.2). Actuellement on utilise plutôt des câbles constitués de deux ou quatre paires torsadées. Elle est très répandue, de connexion facile et d'un faible coût, mais elle possède une faible immunité aux bruits. Pour améliorer les performances, on utilise la paire torsadée blindée, plus résistante aux perturbations électromagnétiques, et qui autorise un débit pouvant aller jusqu'à 16 Mbits/s. D'une manière générale, les performances (et les coûts) de ce support dépendent de la qualité des matériaux employés et des détails de réalisation.

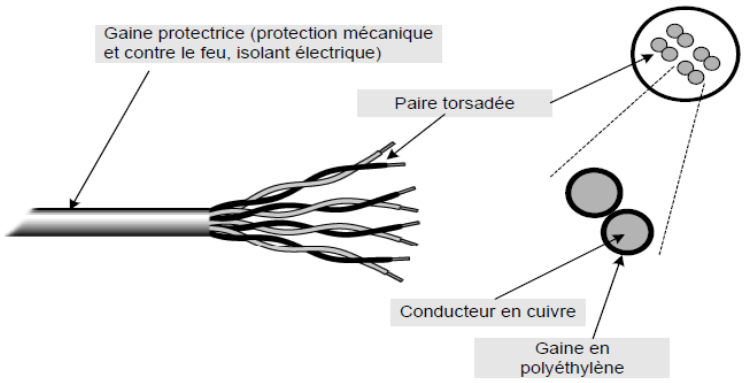

Figure II.2 : Câble en paires de fils torsadés.

3. La fibre optique :

C'est un support de transmission très utilisée dans les réseaux de grandes tailles.

Une fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de lumière et sert dans la transmission de données par la lumière. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux.

Les différents rayons lumineux issus de la source sont guidés par le fil de verre en suivant un principe de réflexion interne qui se produit au niveau de la frontière entre le cœur et la gaine (voir figure II.3). Si la réflexion ne laisse subsister qu'un seul rayon, car le diamètre du fil est très réduit, alors on parle de fibre monomode, sinon lorsqu'il existe plusieurs rayons simultanément, on parle de fibre multimode. Enfin, la bande passante d'une fibre optique étant très large (plusieurs Mhz), il est aisé de réaliser du multiplexage fréquentiel, pour faire transiter simultanément plusieurs communications. [8]

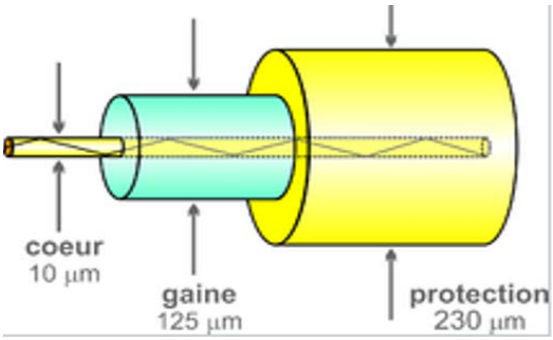

Figure II.3 : la fibre optique.

4. Le système sans fil :

Sont possibles grâce à des liaisons infrarouges, laser ou hertziennes sur des courtes distances et grâce aux faisceaux hertziens pour les liaisons satellitaires. Les débits sont très élevés, mais les transmissions sont sensibles aux perturbations et les possibilités d'écoute sont nombreuses.

Les faisceaux hertziens utilisent des ondes électromagnétiques se propageant sur un milieu aérien. Un faisceau hertzien est constitué à l'aide d'un ensemble de relais terrestres permettant l'émission et la réception des ondes électromagnétiques ; ces ondes sont caractérisées par une bande passante très large, variant de 4 GHz à 6 GHz. La distance entre les relais varie entre 50 Km et 100 Km.

III. Caractéristiques globales des supports de transmission :

Quelle que soit la nature du support, le signal désigne le courant, la lumière ou l'onde électromagnétique transmis. Certaines caractéristiques des supports (bande passante, sensibilité aux bruits, limites des débits possibles) en perturbent la transmission. Leur connaissance est nécessaire pour fabriquer de bons signaux, c'est-à-dire les mieux adaptés aux supports utilisés.

a. Bande passante :

La bande passante est la bande de fréquences dans laquelle les signaux appliqués à l'entrée du support de transmission ont une puissance de sortie supérieure à un seuil donné (après traversée du support). Le seuil fixé correspond à un rapport déterminé entre la puissance du signal d'entrée et la puissance du signal trouvé à la sortie (voir figure II.4). En général, on caractérise un support par sa bande passante à 3 dB (décibels), c'est-à-dire par la plage de fréquences à l'intérieur de laquelle la puissance de sortie est, au pire, divisée par deux. On note « Ps » la puissance de sortie et « Pe » la puissance d'entrée.

Les supports ont une bande passante limitée. Certains signaux s'y propagent correctement (ils sont affaiblis mais reconnaissables à l'autre extrémité), alors que d'autres ne les traversent pas (ils sont tellement affaiblis ou déformés qu'on ne les reconnaît plus à la sortie). Intuitivement, plus un support a une bande passante large, plus il transporte d'informations par unité de temps.

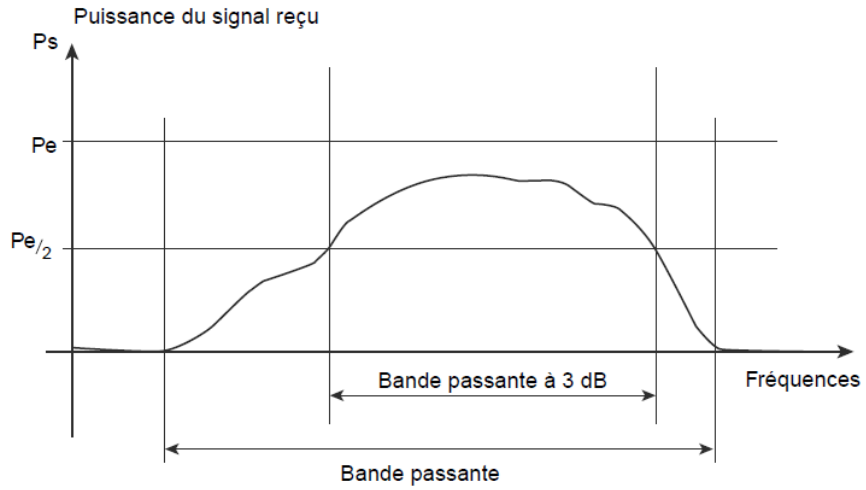

Figure II.4 : Notion de bande passante.

b. Bruits et distorsions :

Les supports de transmission déforment les signaux qu'ils transportent, même lorsque leurs fréquences sont adaptées (voir figure II.5). Diverses sources de bruit perturbent les signaux : parasites, phénomènes de diaphonie… Certaines perturbations de l'environnement introduisent également des bruits (foudre, orages pour le milieu aérien, champs électromagnétiques dans des ateliers…).

Par ailleurs, les supports affaiblissent et retardent les signaux. La distance est un facteur d'affaiblissement, très important pour les liaisons par satellite. Ces déformations,

appelées distorsions, sont gênantes pour la bonne reconnaissance des signaux en sortie, d'autant qu'elles varient avec la fréquence et la phase des signaux émis.

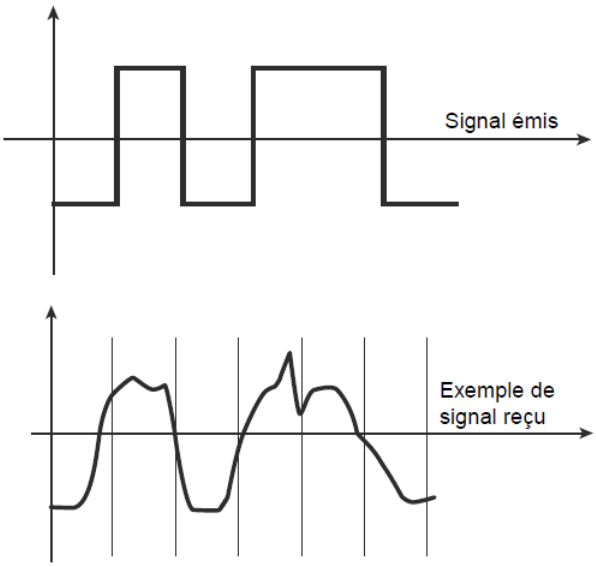

Figure II.5 : Signal émis et exemple de signal reçu.

Même lorsque les signaux sont adaptés aux supports, on ne peut pas garantir leur réception correcte à 100 %. Le récepteur d'un signal doit prendre une décision dans un laps de temps très court. De ce fait, cette décision peut être mauvaise. Par exemple, un symbole « 1 » émis donne une décision symbole « 0 » reçu, ce qui constitue une erreur de transmission.
Les fibres optiques sont les meilleurs supports, car le taux d'erreur y est très faible : 10^{-12} (une mauvaise décision pour 10^{12} bits transmis). Les câbles et les supports métalliques présentent des taux d'erreur moyens. Les liaisons sans fil ont un taux d'erreur variable, sensible aux conditions météorologiques.

c. Capacité limitée des supports de transmission :

La capacité d'un support de transmission mesure la quantité d'informations transportée par unité de temps. Les caractéristiques que nous venons de voir fait que la capacité d'un support est limitée.

d. Qualité des câbles :

Le choix d'un support de transmission dépend de nombreux éléments. Des considérations économiques (le prix de revient, le coût de sa maintenance, etc.) interviennent en plus des facteurs techniques, de même que la nature des signaux propagés, puisque l'équipement de transmission de données contient une partie spécifique au support.

IV. Adaptation des signaux aux supports :

Considérons deux terminaux qui veulent communiquer (voir figure II.6). Chaque terminal contient, en plus de l'unité émettrice/réceptrice des données, une unité de contrôle de la communication. Le signal généré par le terminal peut ne pas être adapté au support de communication. On rajoute alors un équipement d'adaptation du signal au support (par exemple, un modem pour la connexion de l'ordinateur au réseau téléphonique). Ces équipements d'adaptation forment les extrémités du circuit de données.

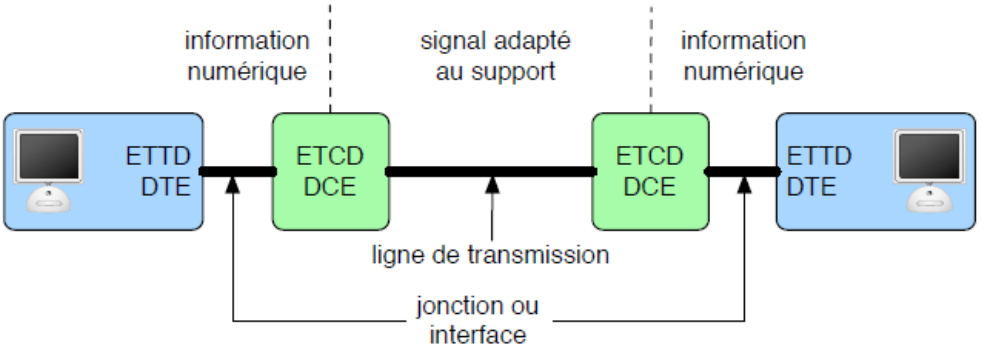

Figure II.6 : adaptation d'un signal à un support de transmission.

- L'Équipement Terminal de Traitement de Données (ETTD) ou Data Terminal Equipment (DTE) : contrôle les communications.
- L'Équipement Terminal de Circuit de Données (ETCD) ou Data Circuit Equipment (DCE) : réalise l'adaptation du signal entre l'ETTD et le support de transmission.

On distingue deux modes d'adaptation du signal :

IV.1. La transmission en bande de base :

La transmission en bande de base consiste à envoyer directement les suites de bits sur le support à l'aide de signaux carrés constitué par un courant électrique pouvant prendre deux valeurs (5 volts ou 0 par exemple).

Dans la figure II.6, nous trouverons quelques exemples de codage de l'information pour une transmission en bande de base :

- **Le code tout ou rien :** c'est le plus simple, un courant nul code le « 0 » et un courant positif indique le « 1 ».
- **Le code NRZ (non retour à zéro) :** pour éviter la difficulté à obtenir un courant nul, on code le « 1 » par un courant positif et le « 0 » par un courant négatif.

- **Le code bipolaire :** c'est aussi un code tout ou rien dans lequel « 0 » est représenté par un courant nul, mais ici le « 1 » est représenté par un courant alternativement positif ou négatif, pour éviter de maintenir des courants continus.
- **Le code RZ (retour à zéro) :** le « 0 » est codé par un courant nul et le « 1 » par un courant positif, qui est annulé au milieu de l'intervalle de temps prévu pour la transmission d'un bit.
- **Le code Manchester :** ici aussi le signal change au milieu de l'intervalle de temps associé à chaque bit. Pour coder un « 0 », le courant sera négatif sur la première moitié de l'intervalle et positif sur la deuxième moitié ; pour coder un « 1 », c'est l'inverse. Autrement dit, au milieu de l'intervalle, il y a une transition de base en haut pour un « 0 » et de haut en bas pour un « 1 ».
- **Le code Miller :** on diminue le nombre de transitions en effectuant une transition (de haut en bas ou l'inverse) au milieu de l'intervalle pour coder un « 1 » et en effectue pas de transition pour un « 0 » suivi d'un « 1 ». Une transition est effectuée en fin d'intervalle, pour un « 0 » suivi d'un autre « 0 ».

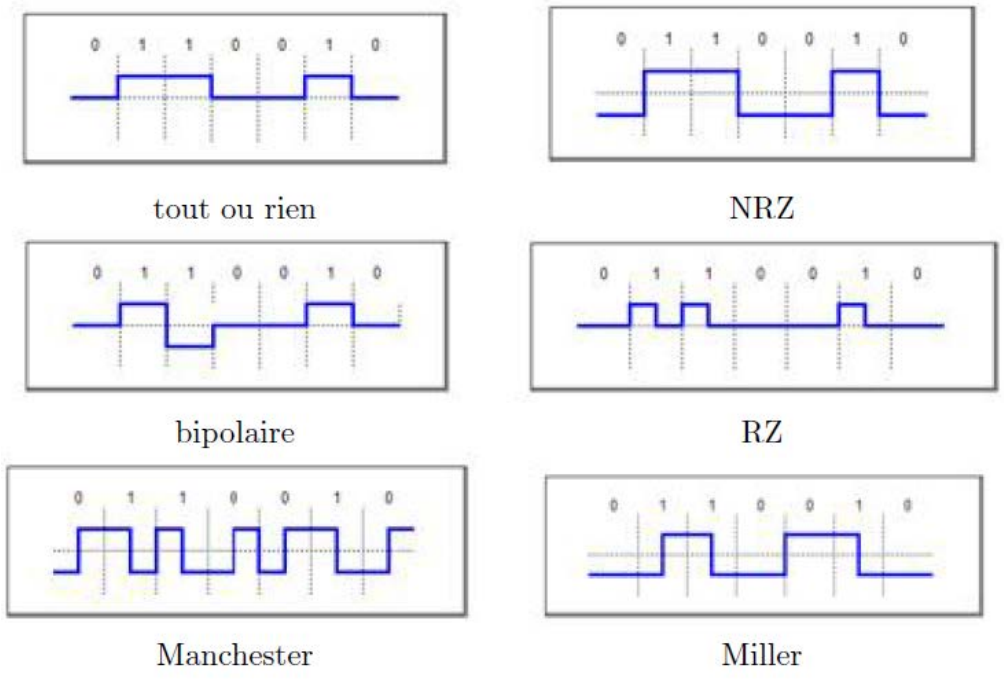

Figure II.7 : exemples de codage en bande de base.

IV.2. La transmission large bande :

Translate le spectre du signal à émettre dans une bande de fréquence mieux admise par le système. Il existe trois types de modulations (voir figure II.7) :

- La modulation d'amplitude.
- La modulation de phase.
- La modulation de fréquence

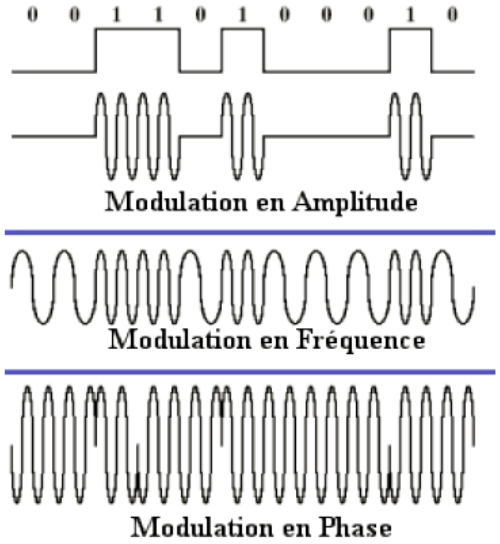

Figure II.8 : Exemple de modulation d'un signal.

Le modem prend un signal en bande de base et va le moduler, c'est-à-dire le mettre sous une forme analogique particulière. Cette transformation est du type numérique/analogique et permet d'éliminer un certain nombre de dégradations qui sont occasionnées par la distance parcourue par le signal dans le câble.

V. Modes d'acheminement des données :

Quelque que soit l'architecture physique d'un réseau, on trouve deux modes de fonctionnement (ou de transmissions) différents :

- Mode avec connexion.
- Mode sans connexion.

➢ Mode avec connexion :

Le mode avec connexion consiste à faire appel à trois phases distinctes :

- ✓ Etablissement de la connexion.
- ✓ Transfert de données.
- ✓ Libération de la connexion.

Les avantages du mode avec connexion sont :

- La sécurisation du transport des données par l'identification claire et nette de l'émetteur et du récepteur.
- Une certaine fiabilité du transport par l'acquittement de chaque message par le récepteur signalant ainsi à l'émetteur que son envoi est bien arrivé.
- La possibilité d'établir à l'avance des paramètres de qualité de service en définissant les limites admissibles pour le transfert de données (par exemple, la taille maximale des paquets échangés, le débit de la liaison, etc.).

En revanche, le mode avec connexion présente quelques inconvénients tels que :

- ❖ La lourdeur de la mise en place de la connexion (temps d'émission plus long).
- ❖ La difficulté à établir des communications multipoint (plusieurs requêtes de même nature).

➢ Mode sans connexion :

Dans le mode sans connexion, les blocs de données, appelés datagrammes, sans émis sans vérifier à l'avance si l'équipement à atteindre est bien actif. C'est alors aux équipements gérant le réseau d'acheminer le message. Les données peuvent être perdues, dupliquées, délivrées dans le désordre ou corrompues.

VI. Transmission parallèle et transmission série :

Dans la pratique, l'unité d'information traitée par un ordinateur est rarement le bit. Il s'agit le plus souvent d'un ensemble de « n bits », d'un caractère ou d'un ensemble de caractères.

➢ Transmission parallèle :

Une transmission parallèle est une transmission dans laquelle les chiffres binaires (signaux) peuvent être émis simultanément sur plusieurs voies. Par exemple, pour transmettre un octet à la fois, on émet huit signaux sur huit voies différentes. Ces voies peuvent être physiques, « n » lignes téléphoniques ou un bus. Il est clair qu'une telle solution devient prohibitive par son prix lorsque l'émetteur et le récepteur sont distants. Ce mode de transmission ne pourrait être intéressant que pour les liaisons courtes.

- **Transmission série :**

Une transmission série est une transmission dans laquelle les chiffres binaires (signaux) se succèdent dans le temps. Généralement, à la sortie d'une machine (par exemple terminal ou ordinateur) l'information à transmettre (les chiffres binaires) se présente en parallèle. Pour émettre l'information binaire en série sur une voie de transmission, il est nécessaire d'avoir un matériel qui réalise la transformation parallèle-série. Un registre à décalage peut réaliser cette transformation (voir figure II.8).

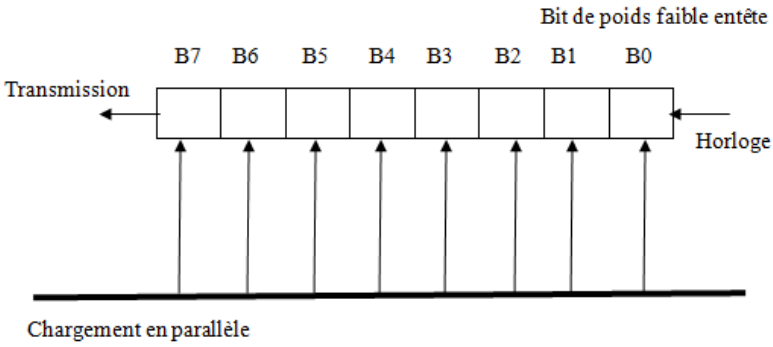

Figure II.9 : Transformation d'un signal parallèle en série.

Au rythme d'un signal d'horloge, le contenu du registre est décalé d'une position à gauche, le bit « B7 » est alors émis. A la réception, le mécanisme inverse doit être prévu pour paralléliser les bits binaires qui arrivent en série à l'aide d'un registre à décalage (voir figure II.9). A chaque arrivée d'un bit, les précédents sont décalés d'une position à gauche ; lorsque le registre est plein, il pourra être vidé en parallèle.

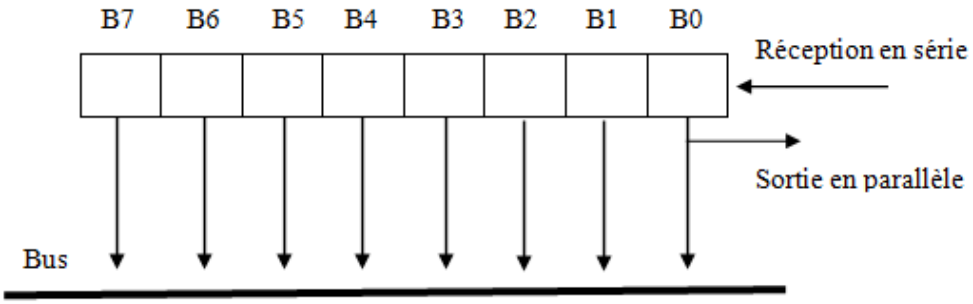

Figure II.10 : Transformation d'un signal série en parallèle.

Le matériel qui réalise la sérialisation et la parallélisation des informations est appelé un coupleur.

- **Un coupleur (carte réseau)** :

Assure l'interface entre la machine dans laquelle elle est montée et un ensemble d'autres équipements connectés sur le même réseau.

VII. Sens de transmission :

Pour communiquer des informations entre deux points il existe différentes possibilités pour le sens de transmission :

- Liaisons unidirectionnelles.
- Liaisons bidirectionnelles.
- Liaisons bidirectionnelles simultanées.

❖ La liaison unidirectionnelle ou simplex a toujours lieu dans le même sens Emetteur/Récepteur (voir figure II.10).

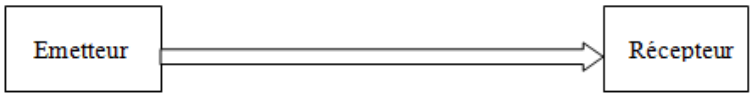

Figure II.11 : liaison unidirectionnelle.

❖ La liaison bidirectionnelle ou à l'internat ou semi-duplex ou half-duplex permet de faire dialoguer l'émetteur et le récepteur à tour de rôle (voir figure II.11).

Figure II.12 : liaison bidirectionnelle.

❖ La liaison bidirectionnelle simultanée ou duplex ou full-duplex permet une transmission simultanée dans les deux sens (voir figure II.12).

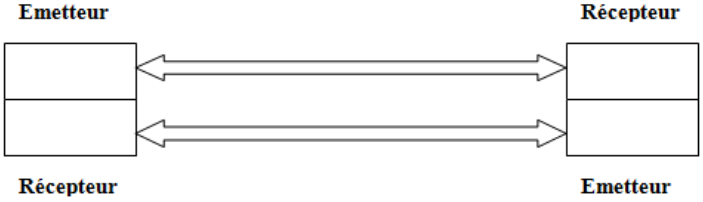

Figure II.13 : liaison bidirectionnelle simultanée.

VIII. Méthodes d'accès au support :

Les méthodes d'accès correspondent a la sous couche MAC de la couche 2 du modèle OSI. [9]

VIII.1. Accès par élection:

La gestion de l'accès au support est gérée par un arbitre fixe (gestion centralisée) ou par l'ensemble des stations (gestion distribuée). Exemple :

❖ Méthode du jeton (token ou Round Robin) :

Un jeton libre (séquence de bits prédéfinie) circule librement sur le réseau. Toute station désirant émettre doit d'abord s'emparer du jeton, émettre son message puis renvoyer le jeton a la station suivante. Il n'y a pas de collisions, les risques de saturation sont faibles mais cette méthode provoque des temps d'attente non négligeables.

VIII.2. Accès par compétition :

Chaque station peut émettre des qu'elle le désire (méthode aléatoire) ce qui implique un risque de conflits et donc des procédures de résolution de ces conflits. Exemple :

❖ CSMA/CD (Carrier Sense Multiple Access/Collision Detection) :

Avant d'envoyer un message, une station désirant émettre commence par écouter si aucun message ne transite sur le réseau. Ensuite le message est envoyé, mais la station reste à l'écoute car il est possible qu'une collision se produise si une autre station envoie une trame en même temps.

Dans ce cas, au moment ou elles s'aperçoivent de la collision, elles cessent la transmission. Chaque station attend un temps aléatoire et relance le processus.

IX. Routage IP : [5]

Le routage est l'une des fonctionnalités principales de la couche réseau et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme.

A. Principe de fonctionnement du routage :

Lorsqu'un ordinateur émet un message vers un autre, hors de son réseau, ce massage est transmis au routeur. Ce routeur effectue les actions suivantes :

- ✓ Lire l'adresse du destinataire.
- ✓ Consulte sa table de routage pour déterminer la route à suivre pour atteindre cette destination.
- ✓ Transmet le message au routeur suivant (ou au destinataire s'il est à côté).

B. Table de routage :

Un routeur utilise une table de routage pour déterminer le lieu d'expédition des paquets. La table de routage contient un ensemble de routes. Chaque route décrit la passerelle ou l'interface utilisée par le routeur pour atteindre un réseau donné. Une route possède quatre composants principaux :

- le réseau de destination.
- le masque de sous-réseau.
- l'adresse de passerelle ou d'interface.
- le coût de la route ou la mesure.

C. Types de routage :

1. Le routage statique :

Une route donnée liée aux routes statiques est dirigée par un administrateur. Cet itinéraire est similaire à une route statique car le chemin jusqu'à la destination est toujours le même et doit mettre à jour l'entrée liée à les routes statiques.

Les opérations de routage statique s'articulent par :

- ✓ L'administrateur réseau configure la route.
- ✓ Le routeur insère la route dans la table de routage.
- ✓ Les paquets sont acheminés à l'aide de route statique.

❖ Avantages du routage statique :

- Plus facile à comprendre par l'administrateur.
- La configuration est simple.
- Effectue des traitements sur le processeur minimal.

❖ Inconvénients du routage statique :

- La configuration et la maintenance posées un problème de temps.

- Des risques d'erreurs sur la configuration, surtout dans les grands réseaux.
- L'intervention de l'administrateur set requise pour assurer la mise à jour des informations relatives aux routes.

2. Le routage dynamique :

Utilise une route qu'un protocole de routage modifie automatiquement en fonction de changements de topologie ou de trafic. Les informations permettent aux routeurs de découvrir de nouveaux réseaux et également de trouver d'autres chemins en cas d'échec d'un lien vers un réseau actif.

❖ Avantages du routage dynamique :

- La maintenance de la configuration est simplifiée pour l'administrateur lors de l'ajout et de la suppression de réseaux.
- Plus évolutif, l'expansion du réseau ne présente généralement pas de problème.
- Les protocoles réagissent automatiquement aux modifications topologiques.
- La configuration présente moins de risques d'erreurs.

❖ Inconvénients du routage dynamique :

- Les ressources du routeur sont utilisées cycle de processeur, mémoire et bande passante du lien…etc.
- La configuration dispose plus de connaissances par l'administrateur, le dépannage et le contrôle.

D. Protocoles de routage IP :

Il existe plusieurs protocoles de routage dynamique IP. Voici quelques-uns des protocoles de routage dynamiques les plus répandus en matière de routage des paquets IP :

- protocole RIP (Routing Information Protocol)
- protocole IGRP (Interior Gateway Routing Protocol)
- protocole EIGRP (Enhanced Interior Gateway Routing Protocol)
- protocole OSPF (Open Shortest Path First)
- protocole IS-IS (Intermediate System-to-Intermediate System)
- protocole BGP (Border Gateway Protocol)

X. Discussion :

Dans ce chapitre on a présenté les principales notions et concepts de la transmission de données dans un réseau informatique, ainsi le routage qui consiste à faire transiter une information d'une machine à une autre à travers un réseau de plusieurs ordinateurs.

Chapitre III

La sécurité des réseaux informatiques

I. Préambule :

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. Les exigences fondamentales de la sécurité informatiques se résument à assurer:

- **La disponibilité** : L'information sur le système doit être toujours disponible aux personnes autorisées.
- **La confidentialité** : L'information sur le système ne doit être diffusée qu'aux personnes autorisées.
- **L'Intégrité** : L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées.
- **Non répudiation** : permet d'indiquer qu'une transaction ne peut être niée.

II. La politique de sécurité :

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

- ✓ Identifier les objectifs de sécurité de l'entreprise.
- ✓ Documenter les ressources à protéger.
- ✓ Identifier l'infrastructure réseau par des schémas et des inventaires à jour.
- ✓ Identifier les ressources vitales qui doivent être protégées, telles que les données de recherches et développement, les données financières et les relatives aux ressources humaines. Il s'agit d'une analyse des risques.

III. Les attaques informatiques :

Toutes les entreprises craignent les attaques informatiques, sans toujours savoir quelles formes celles-ci peuvent prendre. Ces dangers insidieux sont variés, mais on peut facilement identifier les menaces informatiques les plus courantes par leur mode d'opération. [4]

➢ Logiciel malveillant (Malware) :

Un logiciel malveillant est un terme générique englobant ces différentes menaces informatiques visant toutes à nuire à un ordinateur, un téléphone, une caisse enregistreuse, etc. Peu importe sa forme, un logiciel malveillant peut corrompre, effacer ou voler les données des appareils et réseaux d'une entreprise. Il peut subtiliser des données confidentielles, comme les numéros de carte de crédit de clients.

➢ Virus informatique:

De son côté, un virus informatique est un type de logiciel malveillant caché dans un logiciel légitime. Chaque fois qu'un utilisateur ouvre le logiciel infecté, il permet au virus de se propager. Il agit discrètement et se réplique à une vitesse fulgurante grâce aux échanges de données, que ce soit par une clé USB ou un réseau informatique.

➢ Ver informatique:

Le virus ne doit pas être confondu avec un ver informatique, qui se répand sur le réseau Internet. Ce dernier peut s'installer sur un ordinateur à partir d'un courriel, par téléchargement d'un fichier ou par messagerie instantanée. Il est beaucoup plus courant que le virus informatique de nos jours.

➢ Cheval de Troie:

Un cheval de Troie ou trojen n'est pas ni un ver ni un virus, parce qu'il ne se reproduit pas. Un trojen s'introduit sur une machine dans le but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour

créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet.

Les opérations suivantes peuvent être effectuées par intermédiaire d'un cheval de Troie :

- Récupération des mots de passe grâce à keylogger.
- Administration illégale à distance d'un ordinateur.
- Relais utilisé par les pirates pour effectuer des attaques.
- Serveur de spam (envoi en masse des e-mails).
- L'écoute de réseau (sniffing) : grâce à un logiciel appelé « sniffer », il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un se connecte par internet par exemple à ce moment la, son mot de passe transitant en clair sur le net, il sera aisé de lire et c'est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau.

➢ Attaque par déni de service:

L'attaque par déni de service est causée en inondant un serveur ou un site web de requêtes dans le but de le rendre indisponible. L'attaque par déni de service peut être perpétrée par un petit nombre de ressources. Un pirate peut utiliser son seul ordinateur pour contrôler d'autres ordinateurs infectés qui obéiront à ses commandes. Ces ordinateurs peuvent avoir précédemment été infectés par des virus ou des vers.

➢ Attaque de l'homme de milieu :

Consiste à faire passer les échanges réseaux entre deux systèmes par le biais d'un troisième sous contrôle d'un pirate. Ce dernier peut transformer à sa façon les données volées, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

➢ Balayage des ports :

C'est une technique servant à chercher les ports ouverts sur un serveur de réseau. Elle est utilisée par des administrateurs des systèmes informatiques pour contrôler la sécurité des serveurs de leurs réseaux, la même technique utilisée par les pirates pour

trouver les failles dans les systèmes informatiques. Un balayage de port effectué sur un système tiers est généralement considéré comme une tentative d'intrusion.

- **Usurpation d'adresse IP (IP spoofing) :**

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

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

IV. Les protocoles de sécurité : [6]

- **Protocole SSH (Secure Shell) :**

Permet à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : les données circulent entre le client et le serveur sont chiffrées dans un flux TCP en mode tunnel dans une session SSH.

- **Protocol SSL (Secure Sockets Layer):**

Le protocole SSL permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP (http, ftp,…).

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

Le SSL comme son nom l'indique est une couche (layer) supplémentaire sécurisé. Ce protocole va créer une sorte de canal sécurisé entre le client et le serveur. Grâce à un échange de clés entre eux, le serveur et le client vont établir une connexion chiffrée dont eux seuls pourront lire le contenu. Car seul le client et le serveur en possession de la clé de décryptage pourront déchiffrer les données reçues.

❖ Protocole IPSec (Internet Protocol Security) :

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

❖ HTTPS (http sécurisé) :

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

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

❖ Le protocole PKI (Public Key Infrastructure) :

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

V. 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.[6]

Parmi ces dispositifs on distingue :

1. Réseaux privés virtuels (VPN):

1.1. 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 VPN, Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.

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

1.2. 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 chiffréest utilisée pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) (voir figure III.1) 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 VPNl'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.

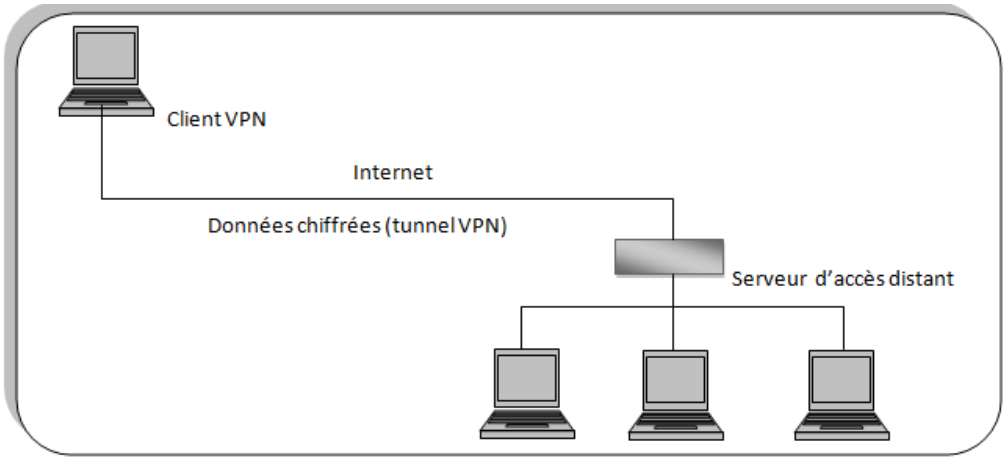

Figure III.1 : Réseau privé virtuel (VPN).

De cette façon, lorsqu'un utilisateur a besoin d'accéder au réseau privé virtuel, sarequête 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.

2. Serveurs mandataires (Proxy) :

2.1. Présentation :

Un serveur Proxy, appelé aussi serveur mandataire est à l'origine une machine faisantfonction d'intermédiaire entre les ordinateurs d'un réseau local, utilisant parfois desprotocoles autre que le protocole TCP/IP et Internet (voir figure III.2).

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

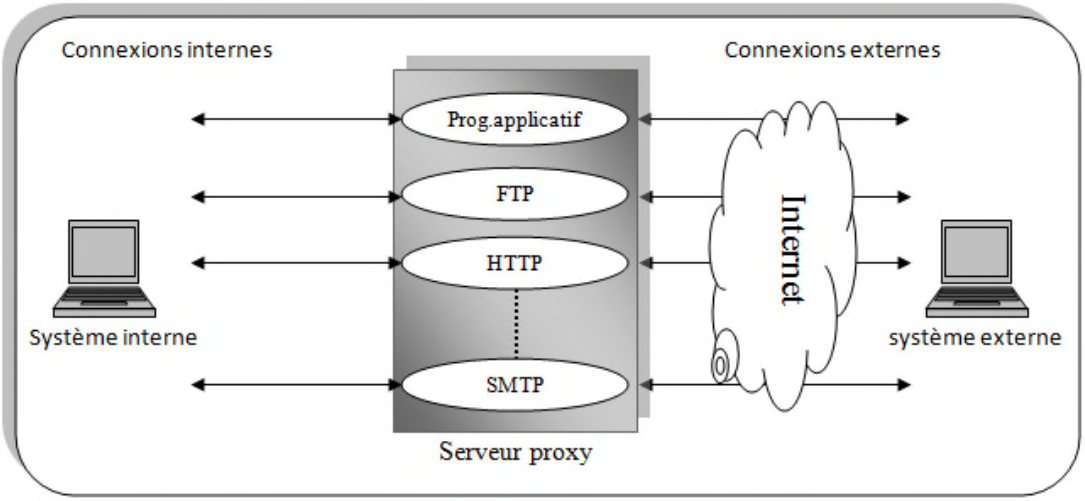

Figure III.2 : Architecture d'un Proxy.

2.2. Principe de fonctionnement :

Le principe de fonctionnement basique d'un serveur proxy est assez simple, il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet 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 va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

Les objets consultés par les clients sur internet, sont stockés en cache disque par le serveur. À partir du deuxième accès, la lecture se fera en cache, au lieu d'être réalisée sur le serveur d'origine. De ce fait il permet d'accélérer nos connexions à l'internet en plaçant en cache les documents les plus consultés.

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.

❖ 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 desconnections via la constitution des journaux d'activités (logs) en enregistrantsystématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de filtrer les connexionsà 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 deliste noire.

En fin l'analyse des réponses des serveurs conformément à une liste de critères (motsclés….) 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 œuvrepose bien évidement de nombreux problèmes relatifs aux libertés individuelles et aux droitsdes personnes.

3. Translation d'adresses (NAT) :

Son principe consiste à modifier l'adresse IP source ou destination, dans l'en-tête d'undatagramme IP lorsque le paquet transite dans le Pare-feu (Proxy) en fonction de l'adressesource ou destination et du port source ou destination (voir figure III.3).

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

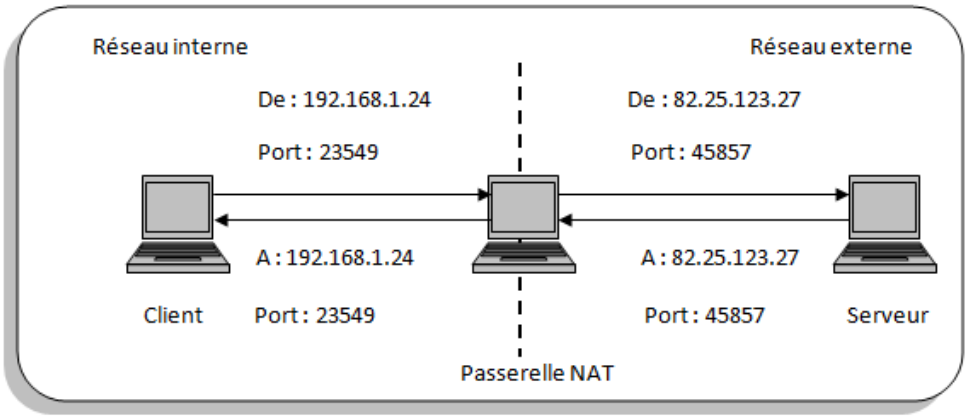

Figure III.3 : Translation d'adresses (NAT).

A. 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 réseauinterne à Internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où nadresses IP routable sont nécessaires pour connecter n machines du réseau interne.

B. Translation dynamique :

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduitd'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes lesmachines 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 chaquerequête 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.

4. Reverse Proxy :

On appelle Reverse-Proxy (relais inverse) 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'accéderindirectement à certains serveurs internes (voir figure III.4).

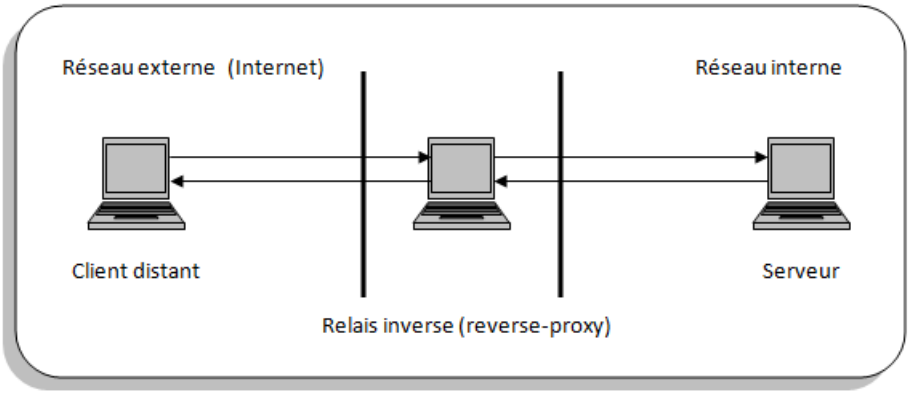

Figure III.4 : Reverse-Proxy.

5. Pare-feu :

5.1. 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 (voir figure III.5):

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

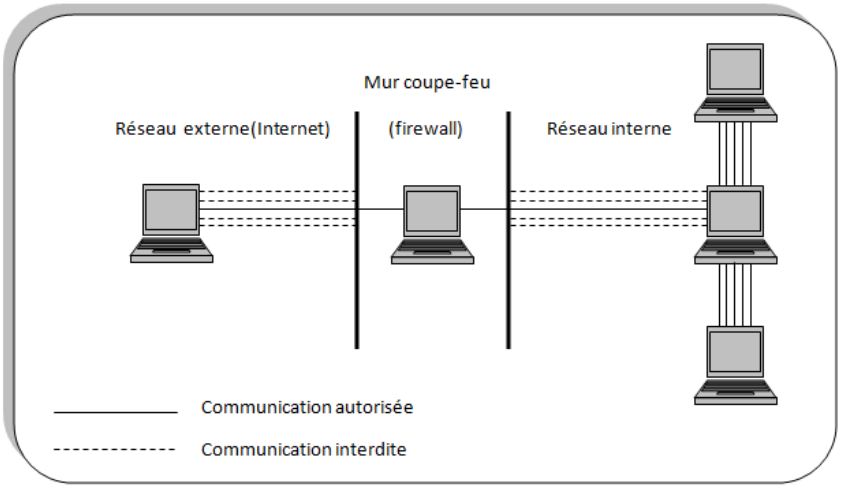

Figure III.5 : Pare-feu.

5.2. Principe de fonctionnement :

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

- ✓ D'autoriser la connexion.
- ✓ De bloquer la connexion.
- ✓ De rejeter la demande de connexion sans avertir l'émetteur.

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtragedépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deuxtypes 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 unedéfinition précise et contraignante des besoins en communication.

5.3. Les différents types de filtrage :

a) Filtrage simple de paquets :

Un système Pare-feu fonctionne sur le principe du filtrage simple de paquets. 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 unemachine 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 applicationréseau).

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

b) Filtrage dynamique :

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

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

Un dispositif Pare-feu de type « stateful inspection » est ainsi capable d'assurer unsuivi 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 initieune connexion à une machine située de l'autre coté du Pare-feu. L'ensemble des paquetstransitant dans le cadre de cette connexion sont implicitement acceptés par le Pare-feu.

c) 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.

VI. Discussion :

La sécurité des réseaux informatiques est un sujet d'actualité. Ces systèmes sont tropouverts, avec le grand nombre de réseaux que constitue Internet, ce qui fait que la sécurité deces réseaux n'est pas totalement garantie. Les Pare-feux, les Proxys et les réseaux privésvirtuels sont des outils développés et utilisés pour renforcer davantage cette idée de sécurité.

Dans le prochain chapitre nous présenterons le pare-feu/routeurPfsense à travers lequel on traitera le filtrage des URLs qui une méthode qui permet d'optimiser le trafic échanger entre le client et le serveur.

Chapitre IV

Mise en place un filtrage avec Pfsense

I. Préambule :

Nous allons présenter dans ce chapitre la phase de réalisation de ce projet. En effet, nous présenterons les pré-requis utilisés afin de configurer Pfsense, ainsi que les étapes de son installation et de sa configuration. Nous allons traiter aussi le filtrage d'URL à travers Squid et SquidGuard en basant sur le Pfsense afin de bloquer certains sites indésirable ou dangereux comme les sites de piratage ce qui permet d'optimiser le trafic entre le client et le serveur.

II. Pré-requis :

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

- Une machine virtuelle « VMware Workstation 12 ».
- Un pare-feu « Pfsense » qui dispose de deux cartes réseaux, une pour l'interface LAN et l'autre pour l'interface WAN.

II.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. [10]

II.2. Présentation de PfSense :

PfSense est une distribution logicielle permettant de réaliser une passerelle réseau à partir d'un serveur. Il date de 2004 à partir d'un fork de m0n0wallpar Chris Buechler et Scott Ullrich. [12]

PfSense offre une solution complète de routage, filtrage, VPN et partage de connexion et intègre un grand nombre de composants tiers : serveur DHCP/DNS, serveur de temps, proxy web, monitoring, etc. La configuration se fait entièrement via uneinterface web. pfSense est disponible sous licence BSD.

Il offre une solution de firewall complète pour les entreprises :

- ✓ **Filtrage**
- ✓ **NAT** (Network Address Translation ; Mécanisme de conversion d'adressesIP non routables (internes ou privées) en adresses IP routables (sur internet), mis en place pour pallier la carence d'adresses IPv4.)
- ✓ **VPN (IPSEC, SSL …) (**virtual Private Network), traduit en français, « Réseau Privé Virtuel ».
- ✓ **Qualité de Service**
- ✓ **Gestion des VLAN** (Grace au VLAN un administrateur réseau pourra ainsi intervenir sur un secteur précis de l'entreprise. Ces propriétés apportent en fait une grande facilité de gestion.)
- ✓ **Serveur DHCP** (Un serveur DHCP (ou service DHCP) est un serveur (ou service) qui délivre des adresses IP aux ordinateurs qui se connectent surle réseau)
- ✓ **Serveur DNS** (Le serveur DNS va permettre de faire la relation entrenom d'ordinateur et adresse IP)
- ✓ **Portail Captif**
- ✓ **Solution proxy**
- ✓ **Filtrage d'url**
- ✓ **Antivirus sur certains flux**

II.3. Présentation de FreeBSD :

FreeBSD est un système d'exploitation de type Unix librement disponible, largementutilisé par des fournisseurs d'accès à Internet, dans des solutions tout-en-un et des systèmesembarqués 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 etde raffinement. L'histoire de FreeBSD commence en 1979, avec BSD [9].

III. Installation et configuration basique de PfSense sous VMware :

L'architecture à suivre pour la mise en place de PfSense est la suivante
(voir figure IV.1) :

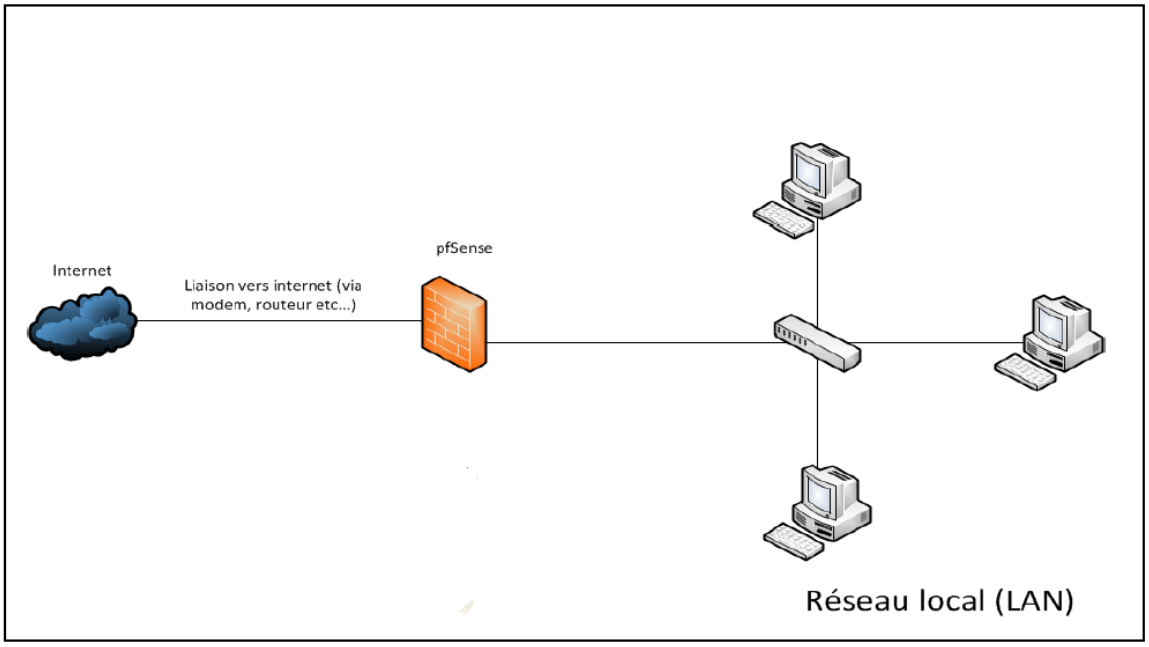

Figure IV.1 : Architecture réseau avec PfSense.

1. Installation de PfSense :

❖ Création d'une machine virtuelle :

Nous avons créé une Machine Virtuelle sous « VMware Workstation 12 » sous le nom de « pfsense » (voir figure IV.2) :

Figure IV.2 : création d'une machine virtuelle sous VMware.

Avant de commencer l'installation, notre machine doit êtreéquipée en minimumde deux cartes réseaux. Nousallons utiliser deux interfaces :

- LAN: pour qu'on puisse communiquer localement avec le serveur PfSence.
- WAN: pour qu'on puisse se connecter à internet.

❖ **Les étapes de l'installation :**

Pour commencer, nous avons inséré le CD pour démarrer l'installation.

Lorsque le premier écran apparaît nous avons choisi la première option **« Boot Multi User [enter] »** (voir figure IV.3) :

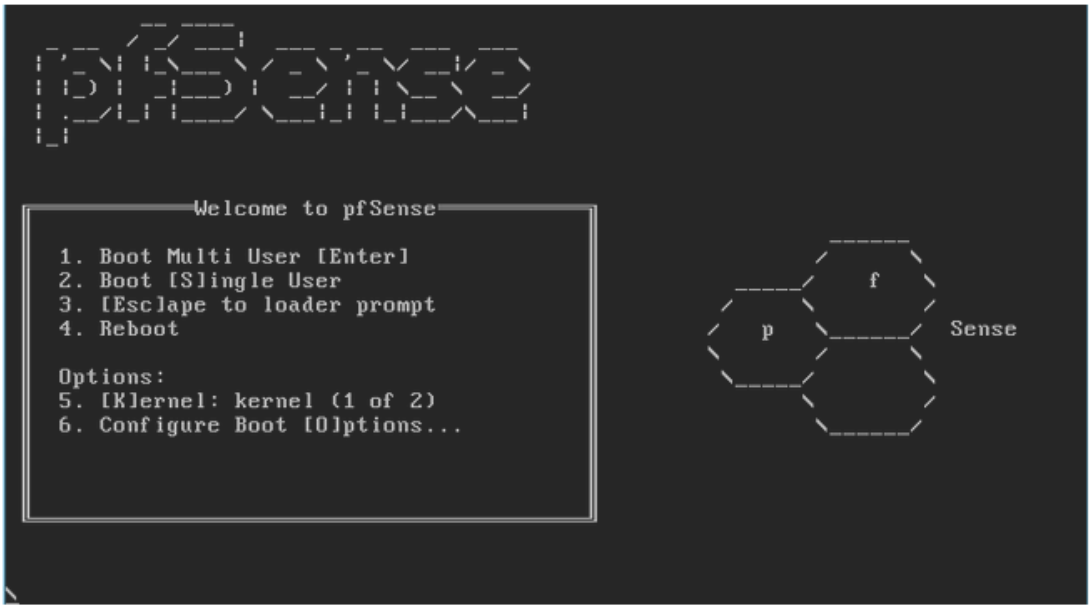

Figure IV.3 :page d'ouverture de pfsense.

Après nous avons la figure ci-contre :

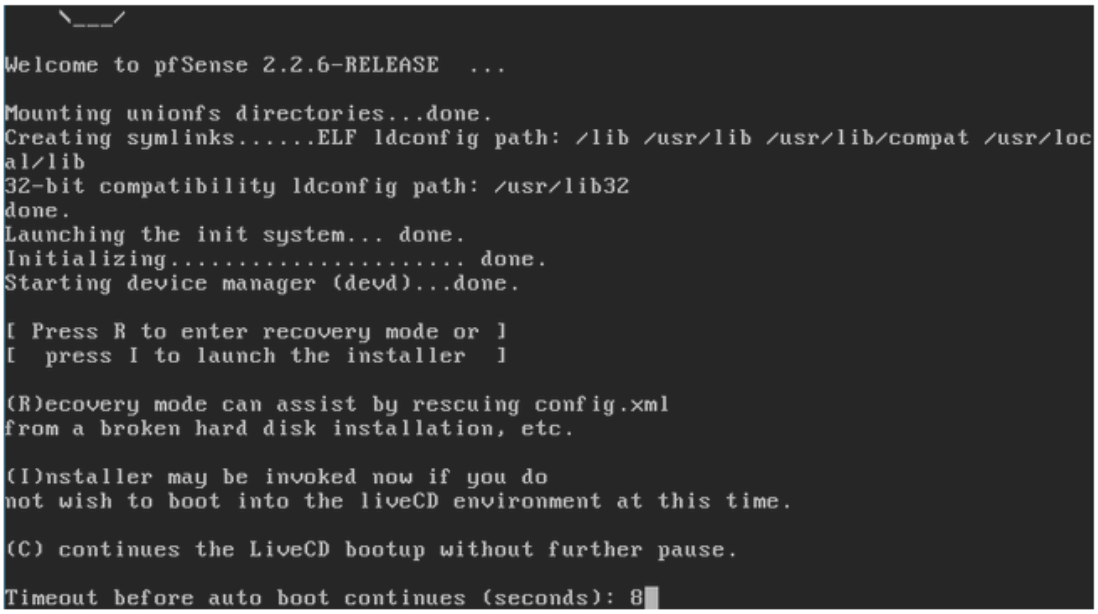

Figure IV.4 : choix du démarrage de CD.

Nous avons sélectionné « **Accept these Settings** » (en appuyant sur la flèche du bas) et ensuite nous avons appuyé sur entrer (voir figure IV.5):

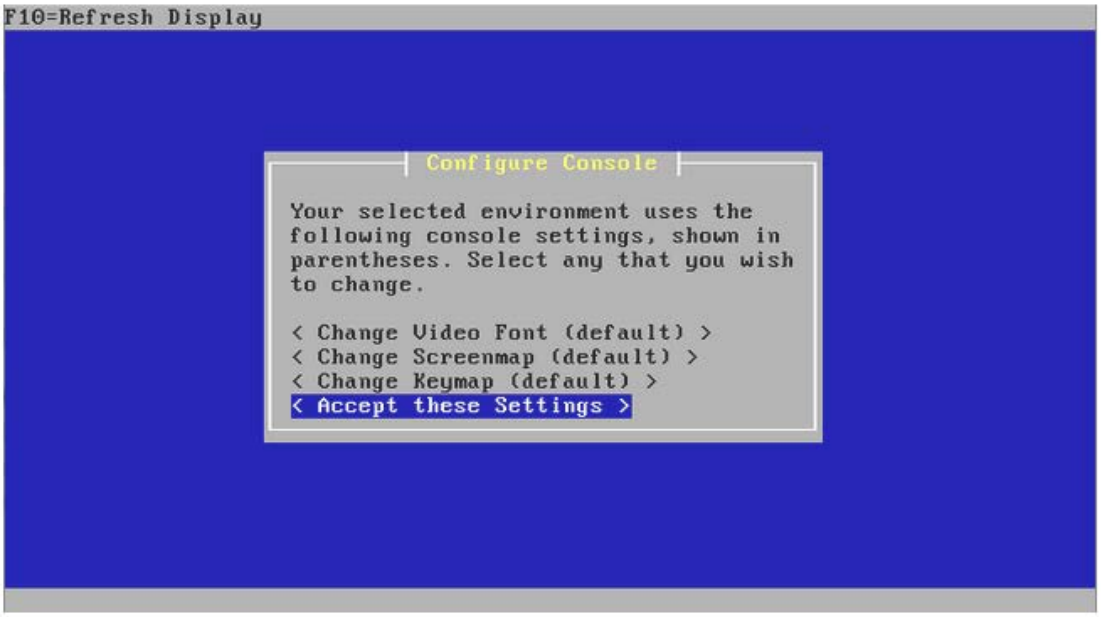

Figure IV.5 : écran d'installation 1.

Nous avons appuyé ensuite sur « **Quick/Easy Install** » (voir figure IV.6) :

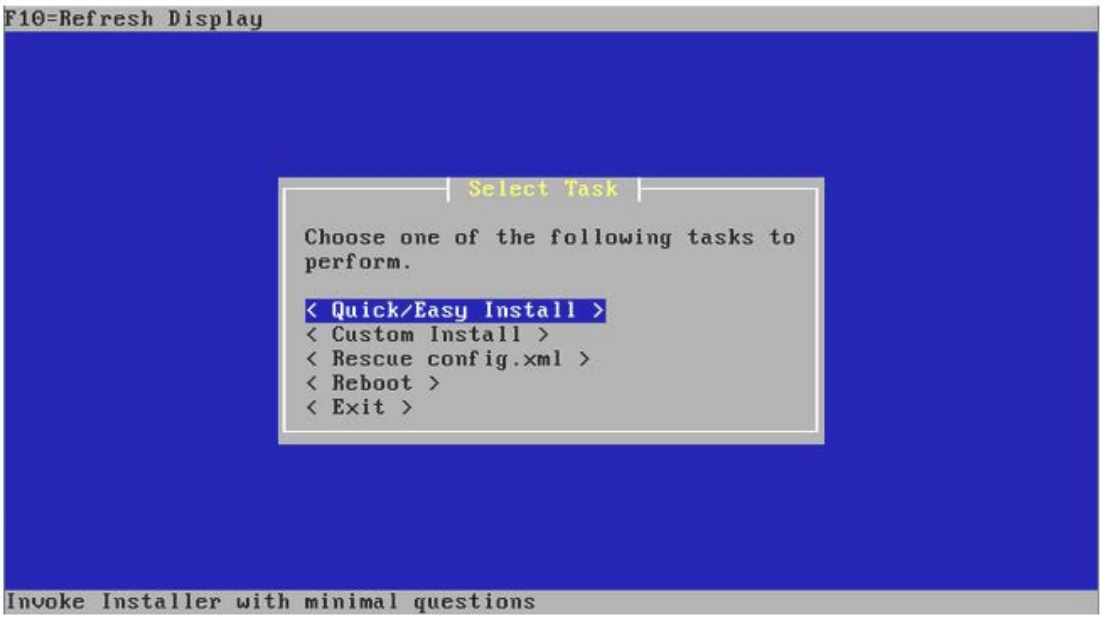

Figure IV.6 : écran d'installation 2.

Nous avons cliqué sue **« OK »** pour que l'installation débute (voir figure IV.7) :

Figure IV.7 : écran d'installation 3.

Nous avons choisi le noyau standard **« Standard Kernel »** et nous avons appuyé sur entrer (voir figure IV.8) :

Figure IV.8 : écran d'installation 4.

À l'écran suivant nous avons appuyé sur **« reboot »** pour continuer l'installation (voir figure IV.9), et nous avons retiré le CD de l'installation :

Figure IV.9 :écran d'installation 5.

Après quelques minutes Pfsense sera intégralement installé.

L'installation se termine ici et nous avons arrivé à l'écran suivant (voir figure IV.10):

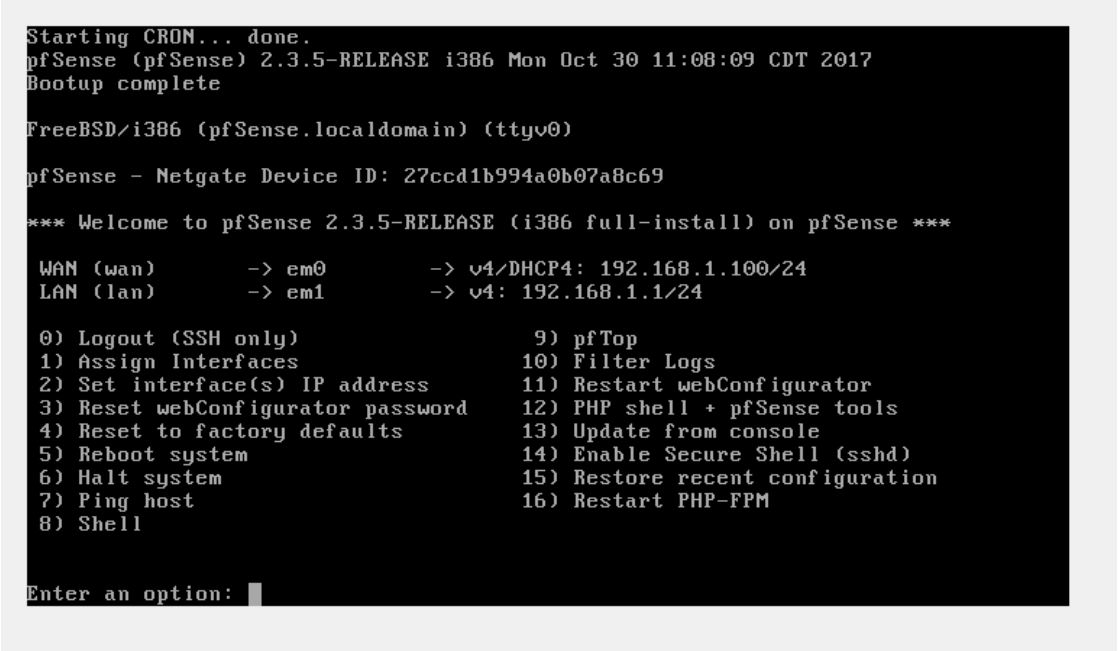

Figure IV.10 : écran principal.

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

2. Configuration des cartes réseaux :

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

L'adresse par défaut du LAN est « 192.168.1.1 », c'est l'adresse attribuée par le serveur DHCP, nous allons la modifier en attribuant« 10.2.0.64 » pour intégrer le Pfsense à notre réseau.

Nous avons choisi l'option **« 2 »** dans le menu principal de Pfsense (voir figure IV.6) pour changer les interfaces LAN et WAN. Après nous avons choisi l'option **« 2 »** pour modifier l'adresse de LAN (voir figure IV.11).

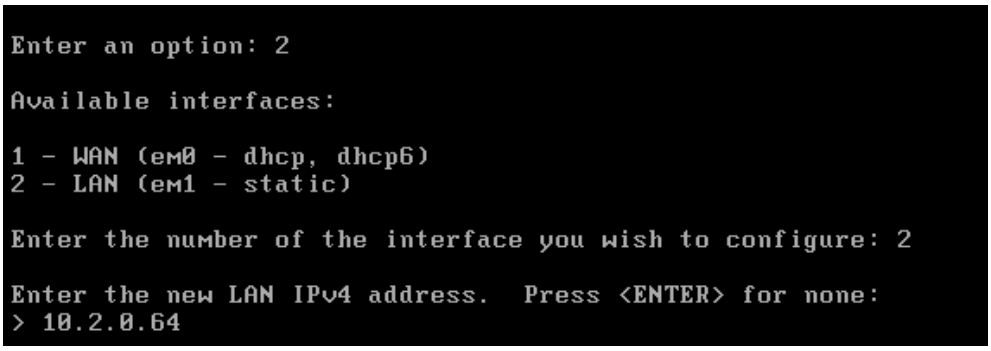

Figure IV.11 : Choix de l'interface à configurer.

Nous avons saisi la valeur 16 correspondant au masque 255.255.0.0 (voir figure IV.12) :

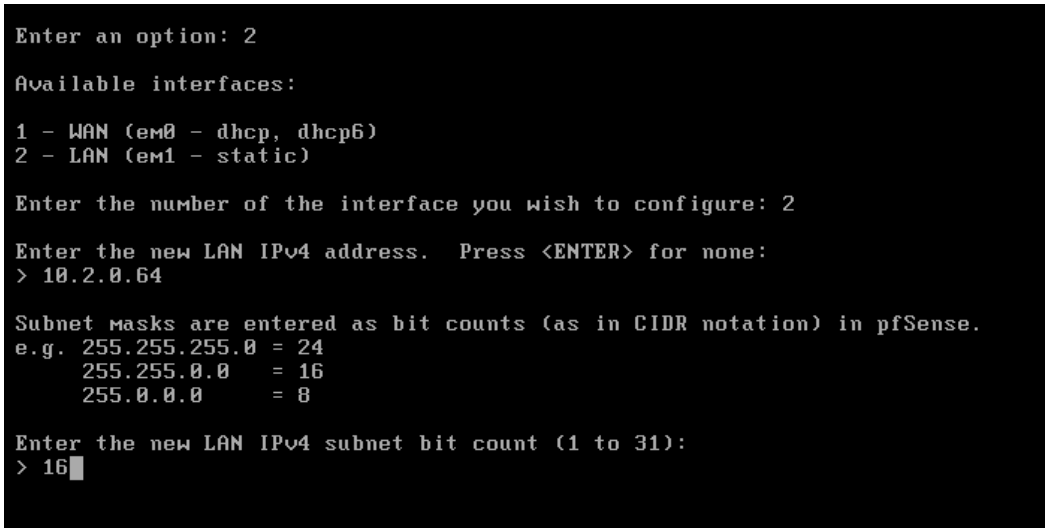

Figure IV.12 : Choix du masque sous réseau.

Nous appuyons deux fois sur **« Enter »,** une pour ne pas définir de passerelle et l'autre ne pas définir l'adresse IPv6. Entrer **« n »** pour« Non » afin de ne pas activer le service DHCP (voir figure IV.13).

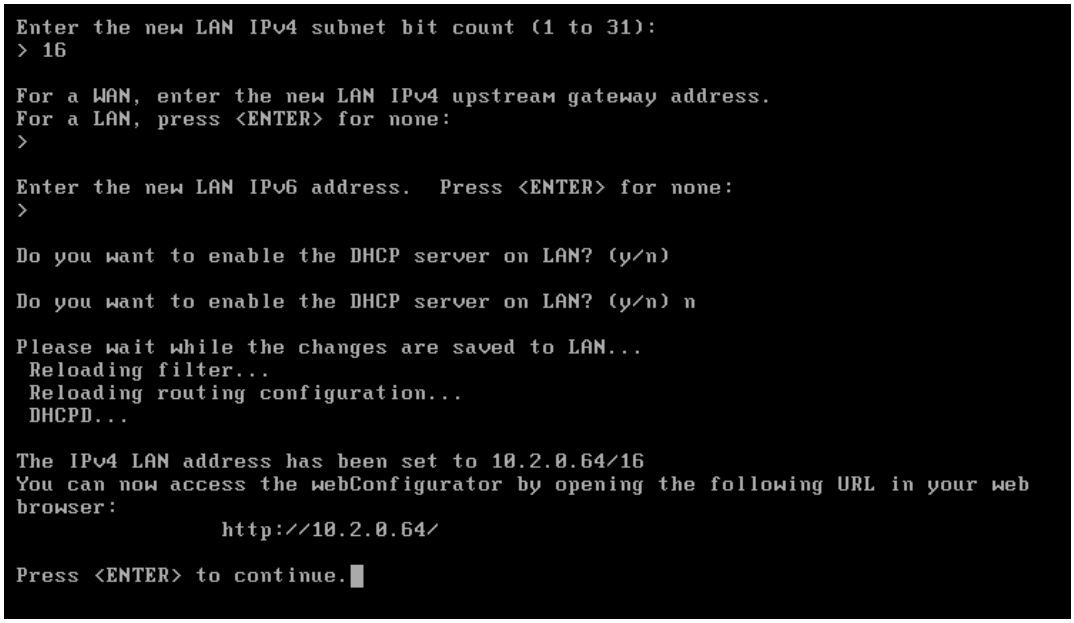

Figure IV.13 : configuration de l'interface LAN.

Notre interface est maintenant configurée, et nous avons arrivé à la figure suivante :

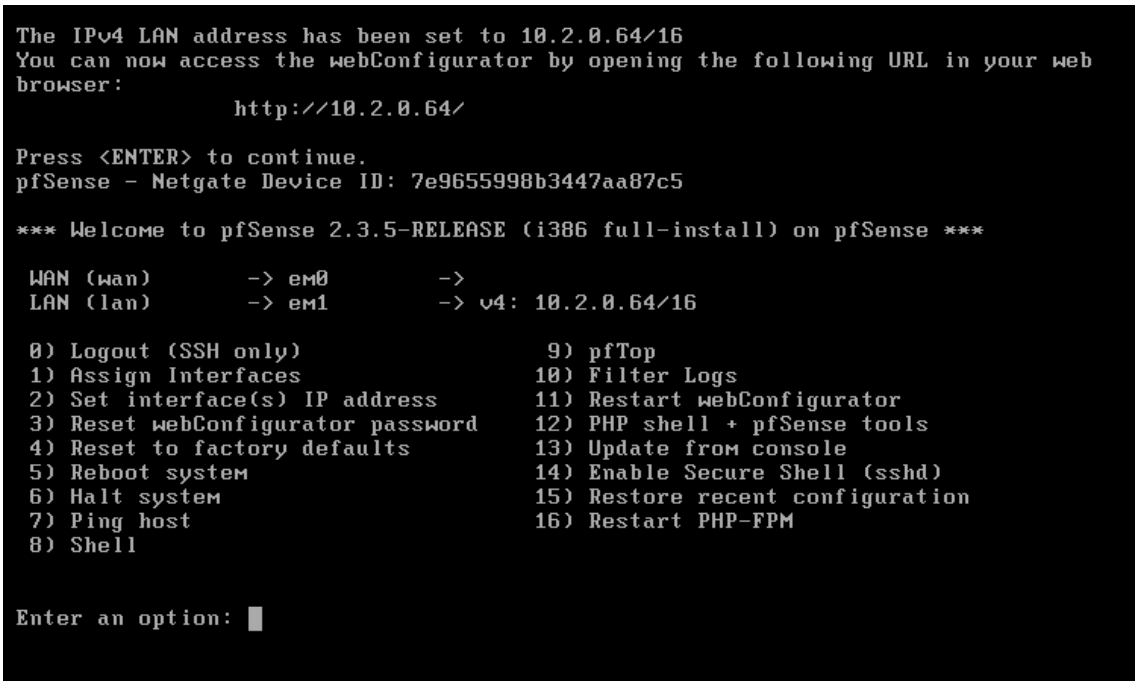

Figure IV.14 : fin de configuration de l'interface LAN.

Nous effectuons la même manipulation pour la carte réseau WAN.

3. Configuration de l'interface web :

Nous accédons à l'interface web en entrant l'adresse IP de« LAN » (10.2.0.64) dans un navigateur.Nous arrivons sur la page de connexion de PfSense (voir figure IV.15) dont les identifiants sont :

- ✓ Username : admin.
- ✓ mot de passe : pfsense.

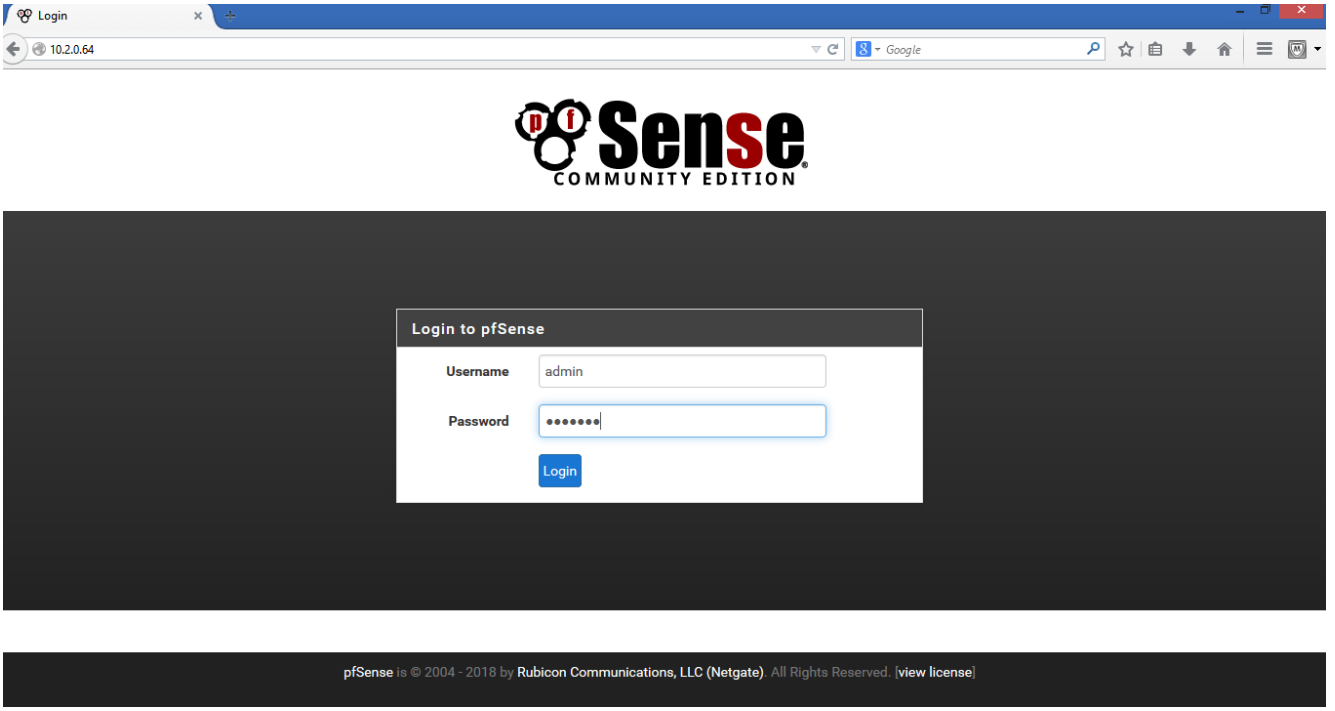

Figure IV.15 : Page de connexion de l'interface web.

Une fois connecté avec succès, il est possible d'accéder à l'interface web permettant l'administration de Pfsense. Lorsque nous saisissons le nom d'utilisateur et de mot de passe, la page d'accueil de Pfsense s'affiche (voir figure IV.16).

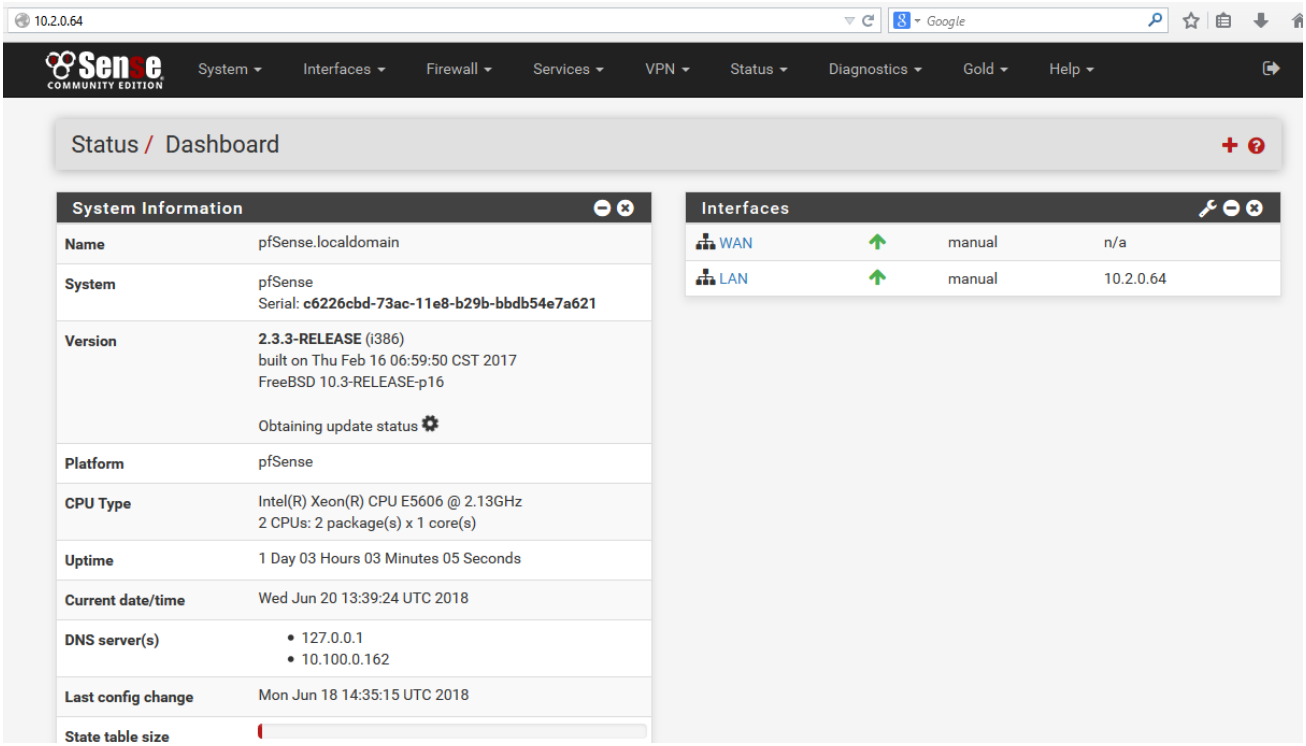

Figure IV.16 : Page d'accueil Pfsense.

4. Les différents onglets de Pfsense :

Nous avons des onglets qui fournissent plusieurs services :

- ✓ **System :** Permet de faire l'ensemble des réglages concernant le système lui-même.
- ✓ **Interfaces :** Permet la gestion des interfaces réseaux (LAN et WAN).
- ✓ **Firewall :** Permet de mettre en place toute les règles suivant de firewall.
- ✓ **Services :** Permet d'activer de nombreux services faisant de Pfsense un firewall multifonctions pouvant se transformer en serveur/relais DHCP ou bien encore en portail captif.
- ✓ **VPN :** Permet d'activer/désactiver le VPN, de mettre en place une sécurité via IPSec.
- ✓ **Status :** Permet de voir le status de l'ensemble des configurations.
- ✓ **Diagnostics :** Permet de donner des outils permettant le diagnostic d'un quelconque bug.

IV. Filtrage des URLs :

Le filtrage d'URL est une méthode pour bloquer l'accès à certains sites Web. Pour ce faire, nous proposons de télécharger quelques packages de Pfsense qui sontSquid et SquidGuard.

IV.1. Présentation de Squid et SquidGuard :

Squid est un proxy de cache pour le Web prenant en charge HTTP, HTTPS, FTP. Squid optimise le flux de données entre le client et le serveur pour améliorer les performances.

SquidGuard est un filtre, un redirecteur et un plugin de contrôle d'accès pour Squid. Il va notamment permettre d'appliquer sur un proxy une liste noire de sites ou mots-clés interdits. [13]

Avant de commencer le téléchargement des packages nous allons activer au début l'interface **« WAN »** (voir figure IV.17) :

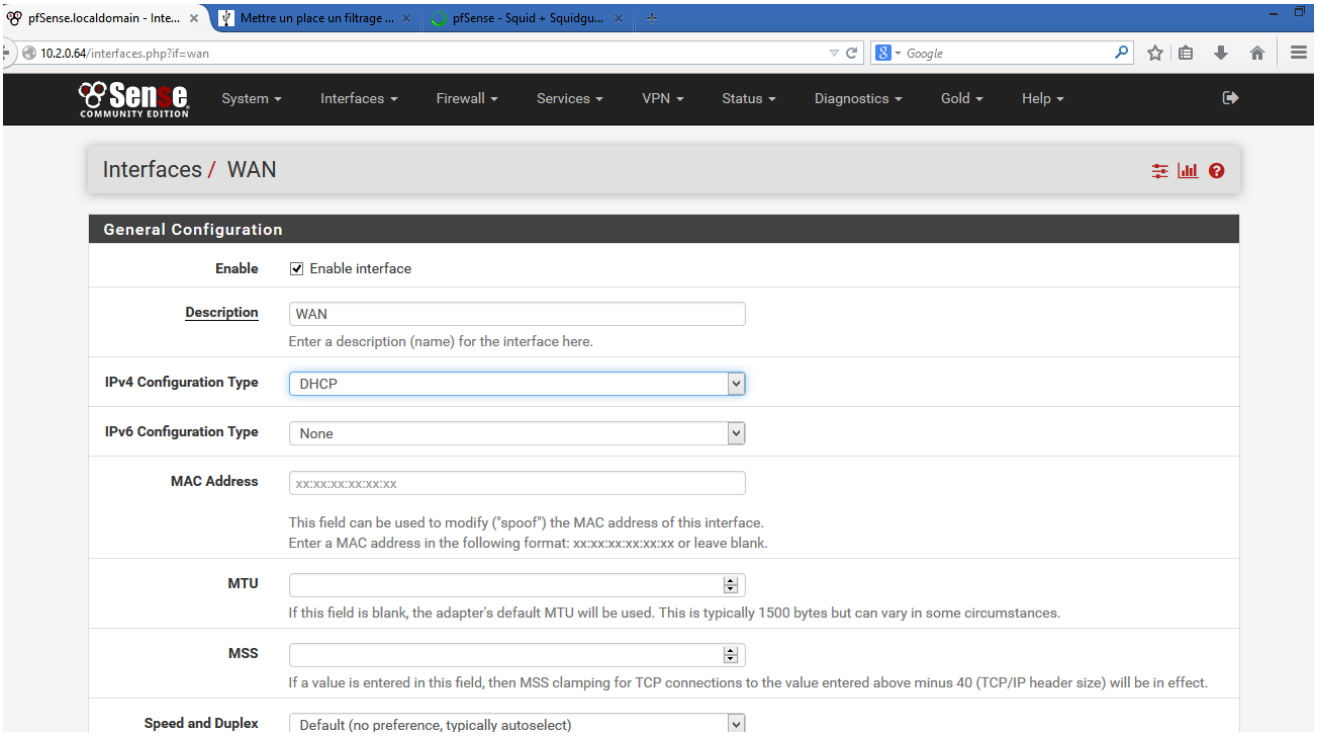

Figure IV.17 : configuration de l'interface WAN.

IV.2. Téléchargement du package Squid et squidgard :

Pour installer les deux packages suivants, nous avons allé dans **« System / Package Manager / Available Packages »** (voir figure IV.18 et IV.19) :

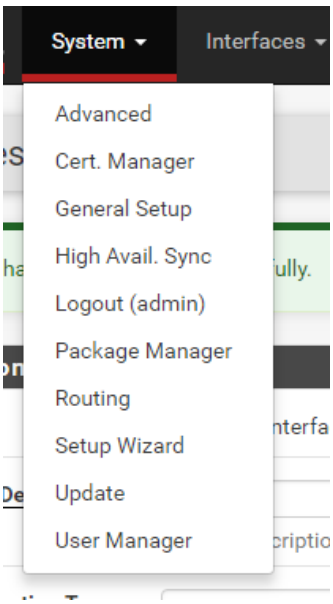

Figure IV.18 : Package manager.

Figure IV.19 : Avalaible packages.

IV.3. Configuration squid (proxy server) :

Pour commencer, nous avons allé dans le menu déroulant « **Services** »puis dans « **Proxy Server** ». Dans la partie **« General »,** nous avons rempli les champs comme le montre la capture d'écran ci-contre :

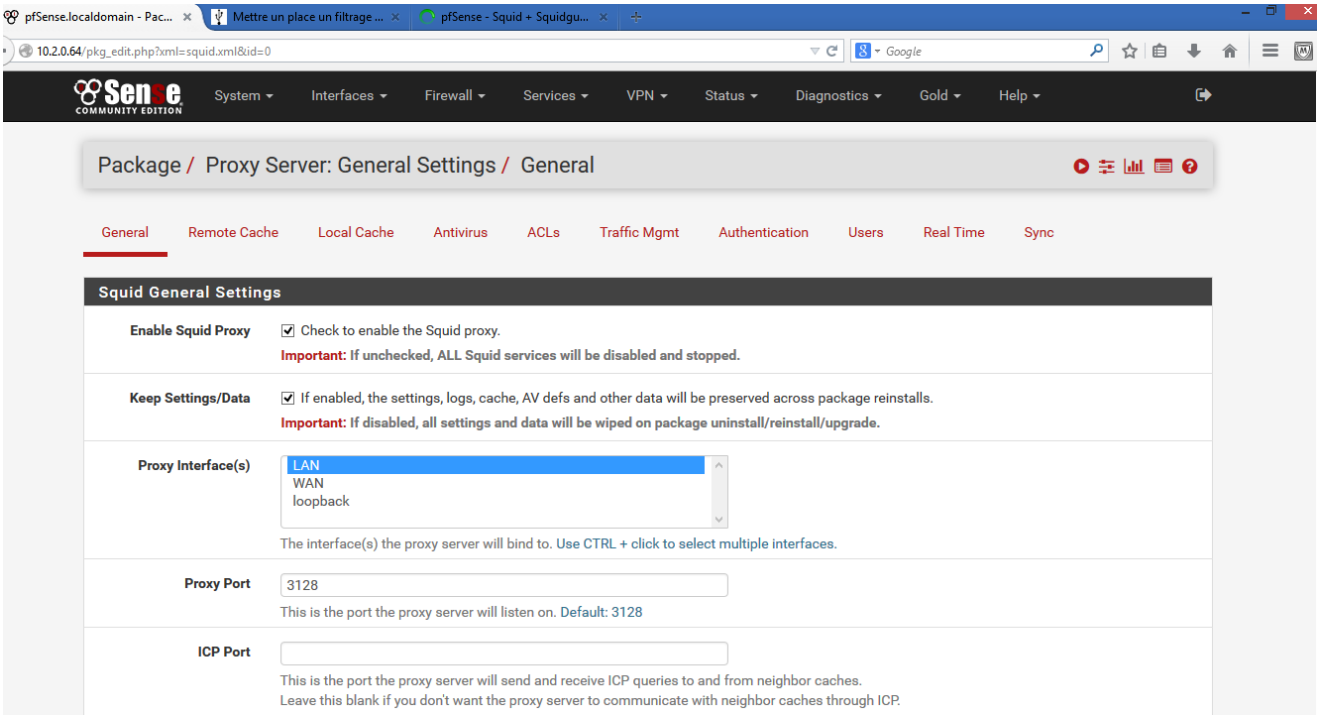

Figure IV.20 :activation de squid proxy server.

Le mode transparent http proxy redirige automatiquement tout le trafic Web entrant vers le serveur proxy Squid.

Nous avons activé le proxy transparent en cochant la case **« Transparent http proxy »** (voir figure IV.21) :

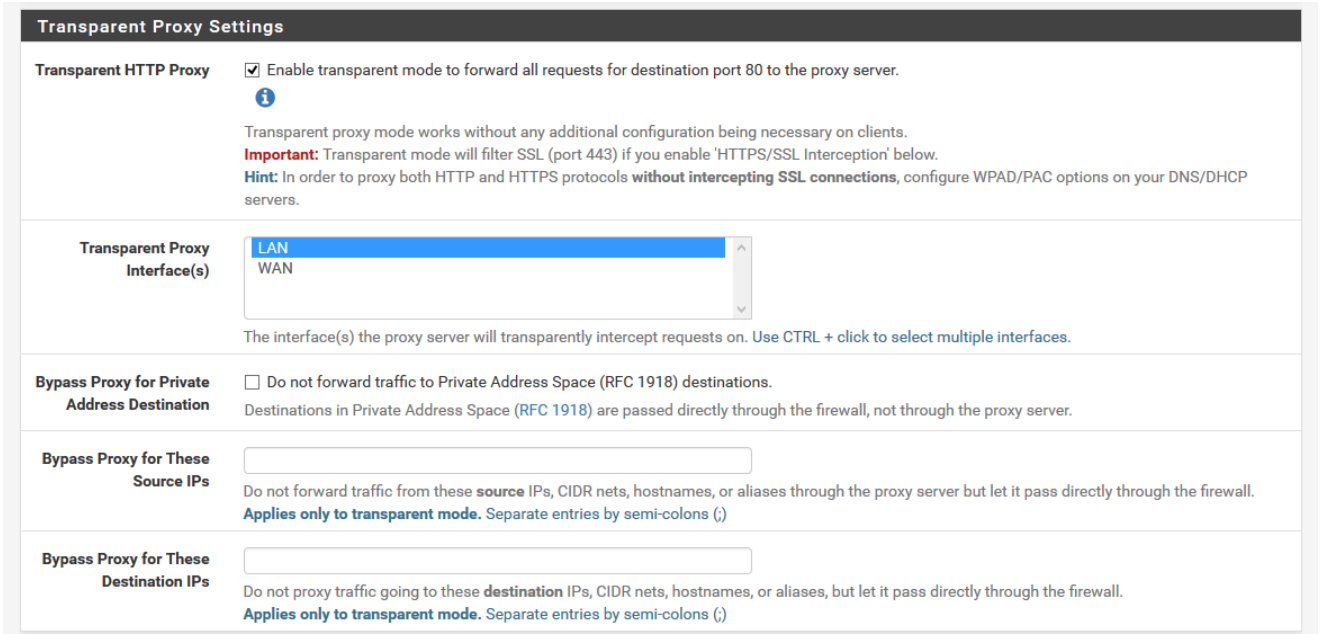

Figure IV.21 : activation de proxy transparent.

Dans **« Logging Settings »**nous avons coché**« Enable Access Logging »** pour activer les logs (voir figure IV.22) :

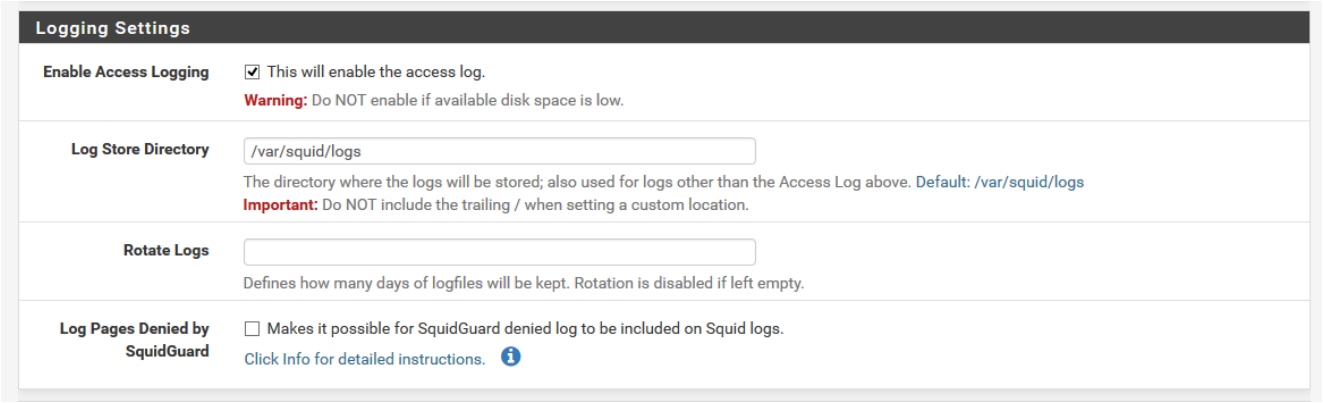

Figure IV.22: Activation des logs.

Nous avons sauvegardé les modifications avec **« Save »**(voir figure IV.23) :

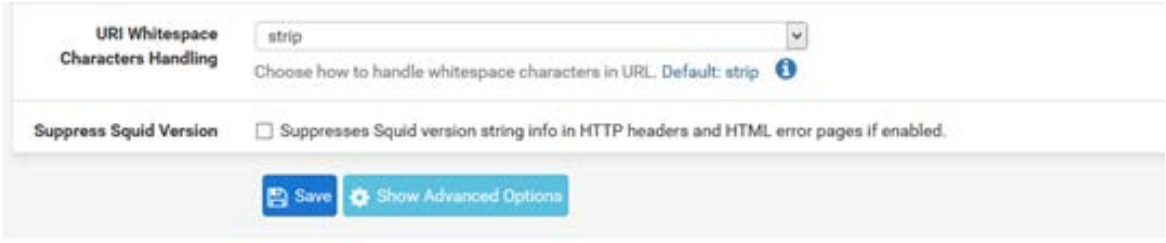

Figure IV.23 : la sauvegarde des modifications.

IV.4. ConfigurationSquidGuard (proxy filter http):

SquidGuard permet de filtrer et de contrôler les accès. Nous allons utiliser une blacklist complète avec beaucoup de catégories.

Lien de la blacklist**(http://www.shallalist.de/Downloads/shallalist.tar.gz).**

Nous avons allé dans le menu **« Services »** puis dans **« SquidGuard Proxy filter »**. Dans la partie **« General setting »**, nous avons rempli les champs comme dans la capture d'écran ci-contre :

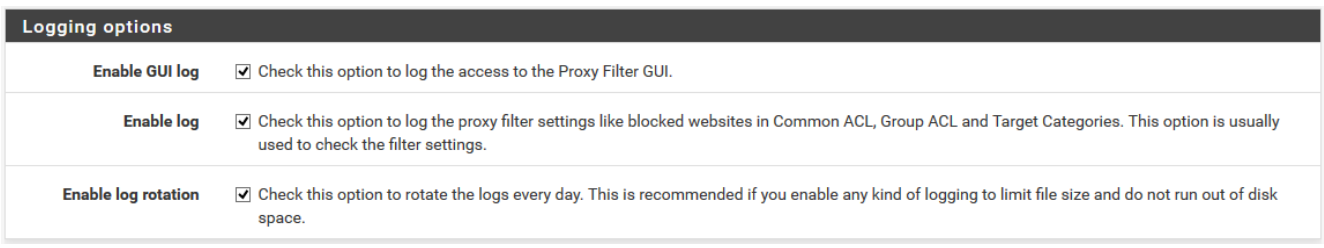

Figure 24 : activation des logs.

Dans **« Blacklist Options »**nous avons cochéle champ **« Blacklist »** pour pouvoir entrer l'URL de la **« blacklistshalla »** que nousavons téléchargé et nous avons cliqué sur **« Save »** pour sauvegarder les modifications (voir figure IV.25) :

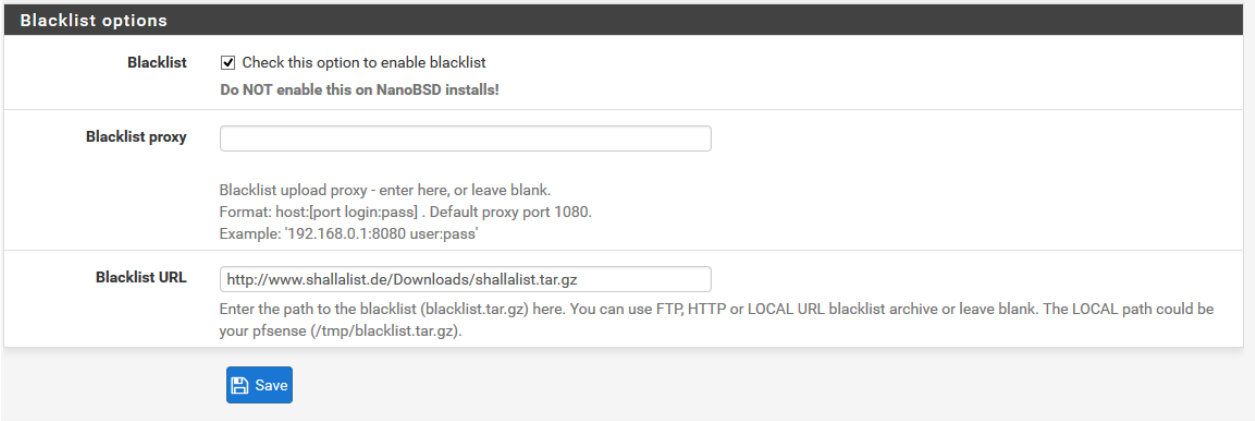

Figure IV.25 : activation de la blacklist.

Dans l'onglet blacklist, nous avons collé le lien de la blacklist et nous avons fait**« download »** pour télécharger la blacklist(voir figure IV.26) :

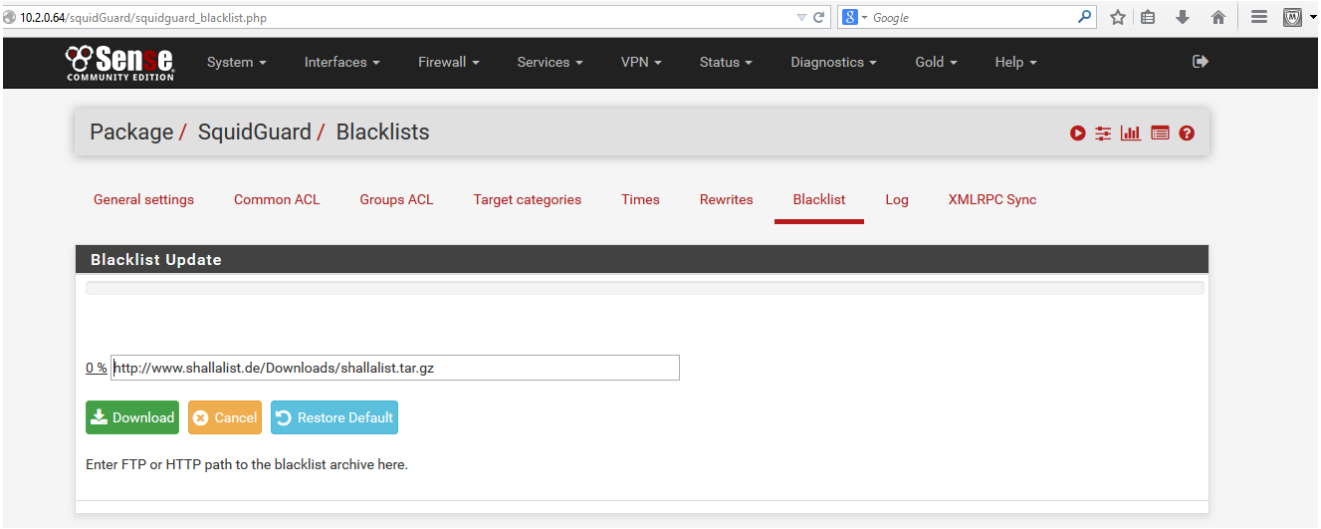

Figure IV.26 : téléchargement de la blacklistshalla.

Par défaut le proxy bloque toutes les catégories d'url, nous allons donc lui spécifier quelles catégories d'url nous voulons bloquer. Nous avons donc commencé par autoriser toutes les catégories puis nous avons interdit les catégories que nous ne voulons pas.

Pour cela avons allé dans l'onglet **« Common ACL »**et nous avons cliqué sur **« Target ruleslist »** et ensuite sur **« + »** pour avoir la liste noir téléchargée (voir figure IV.27) :

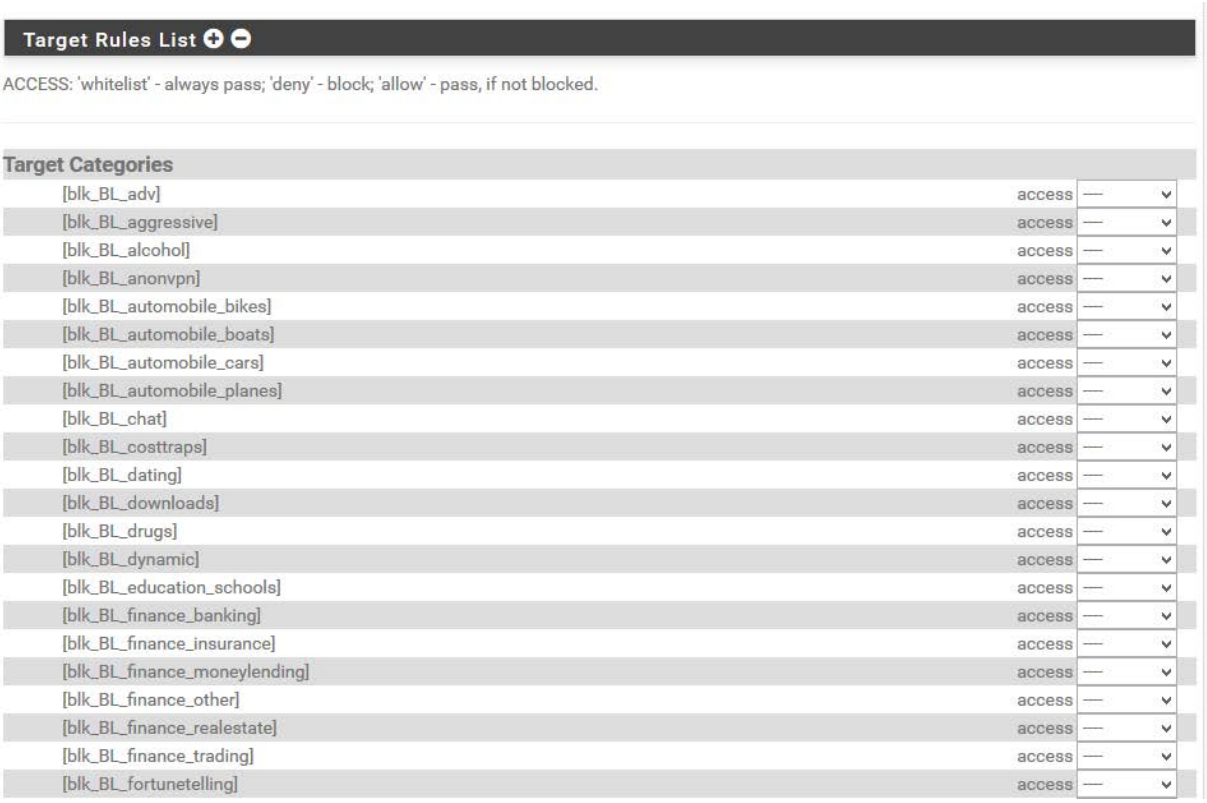

Figure IV.27 : la liste noire téléchargée.

Tout en bas de la liste, la catégorie **« Default access [all] »** est bloquée, nous avons donc l'autorisé en choisissant**« deny=autoriser »(**voir figure IV.28 et IV.29) :

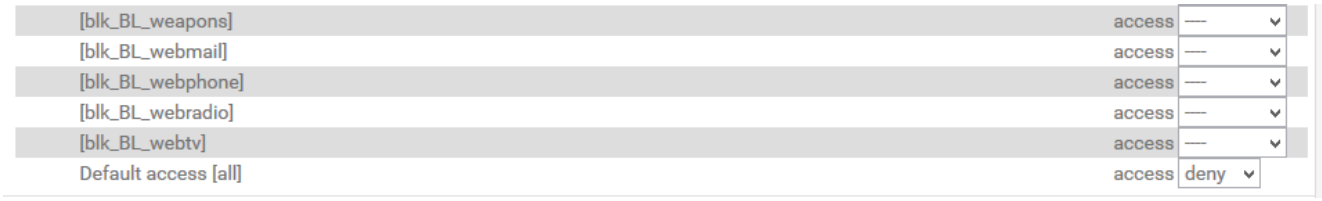

Figure IV.28: Toutes les catégories sont bloquées.

Figure IV.29: Toutes les catégories sont autorisées.

Dans notre cas nous avons pris comme exemple de bloquer l'accès à la catégorie [blk_bl_socialnet] (réseaux sociaux) comme le montre la figure IV.30 :

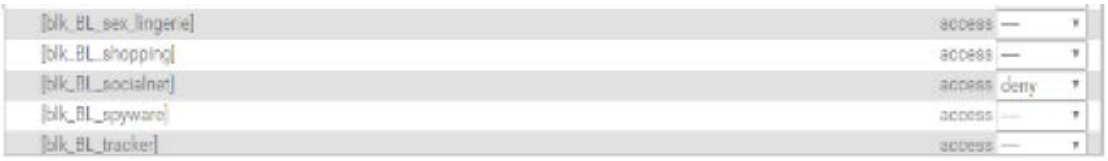

Figure IV.30 : blocage de la catégorie [blk_bl_socialnet].

Pour empêcher un utilisateur d'ignorer notre filtre d'URL en entrant l'adresse IPd'une page, nous avons activé l'option « **Do not allow IP Adress in URL »**et nous avons compléter le reste comme le montre la figure IV.31, ensuite nous avons enregistré avec **« Save ».**

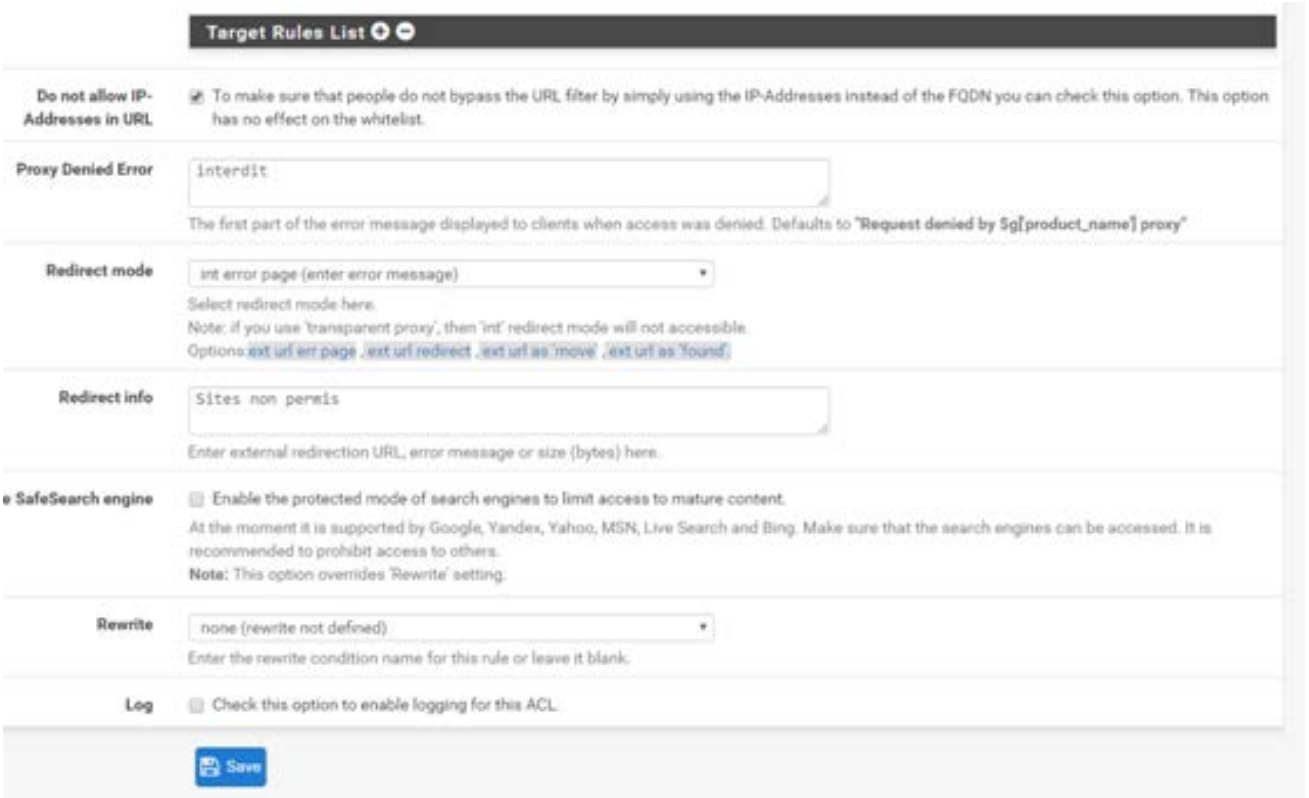

Figure IV.31 : information blacklist.

Lors de la page d'erreur nous devrions voir les termes choisis dans la liste des règles : **interdit** et **sites non permis.**

❖ Test du bon fonctionnement du projet :

Tout est configuré pour les connexions HTTP et nous pouvons tester.

Pour cela, nous avons allé vers un navigateur et nous avons fait entrer un des réseaux sociaux (dans notre cas, nous avons choisi le **« facebook »**) (voir figure IV.32) :

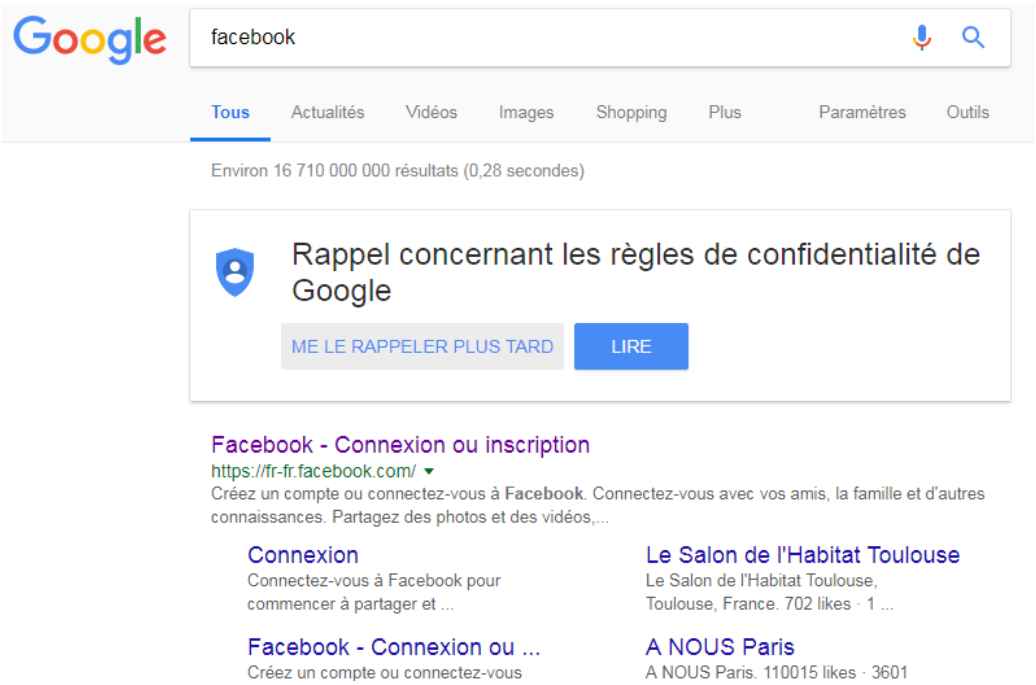

Figure IV.32 : page web.

En cliquant sur le lien nous remarquons que la page est bloquée et nous recevons bien les messages d'erreurs (voir figure IV.33) :

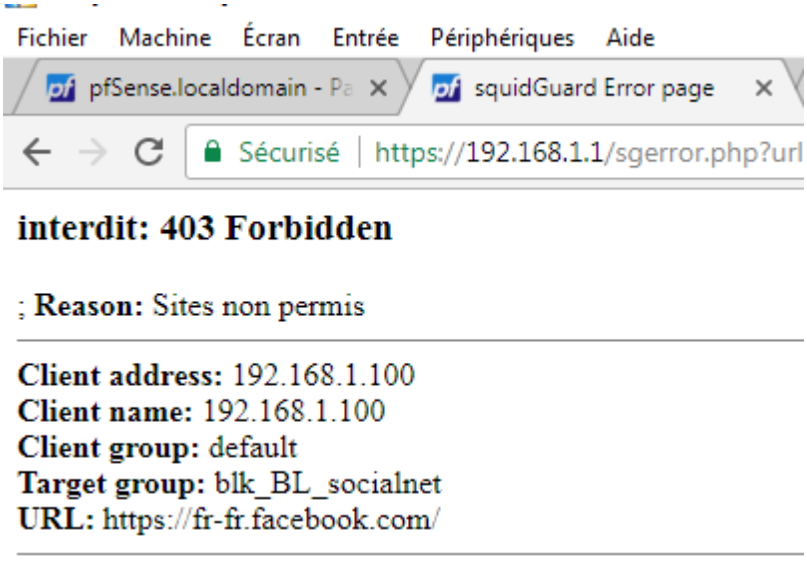

Figure IV.33 : Page web non autorisée.

Il est aussi possible de bloquer l'accès à certains sites par mots clés, ces règles sous pfSense se nomment **« Target Categories ».** Dans l'onglet **« Target categories »**nous

avons cliqué sur **« ADD ».** Nous avons créé une liste_noire pour interdire l'accès à netacad.com (voir figure IV.34) :

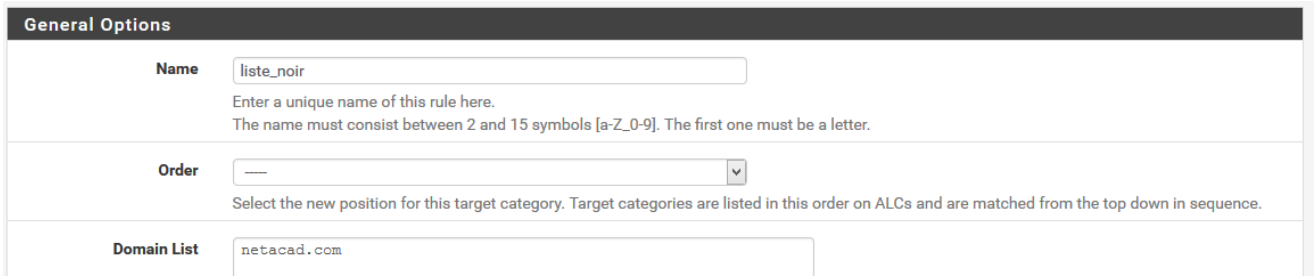

Figure IV.34: création d'une liste noire.

Ensuite il faut aller dans l'onglet **« Common ACL »** et dans la **« Target ruleslist »**nous avons choisi**« deny=bloqué »** pour la liste_noire crée (voir figure IV.35).

Figure IV.35 : Blocage de liste_noir.

Ensuite dans l'onglet **« general settings »**nous avons activé SquidGuard pour démarrer le service (nous avons fait**« apply »** après chaque modification) (voir figure IV.36) :

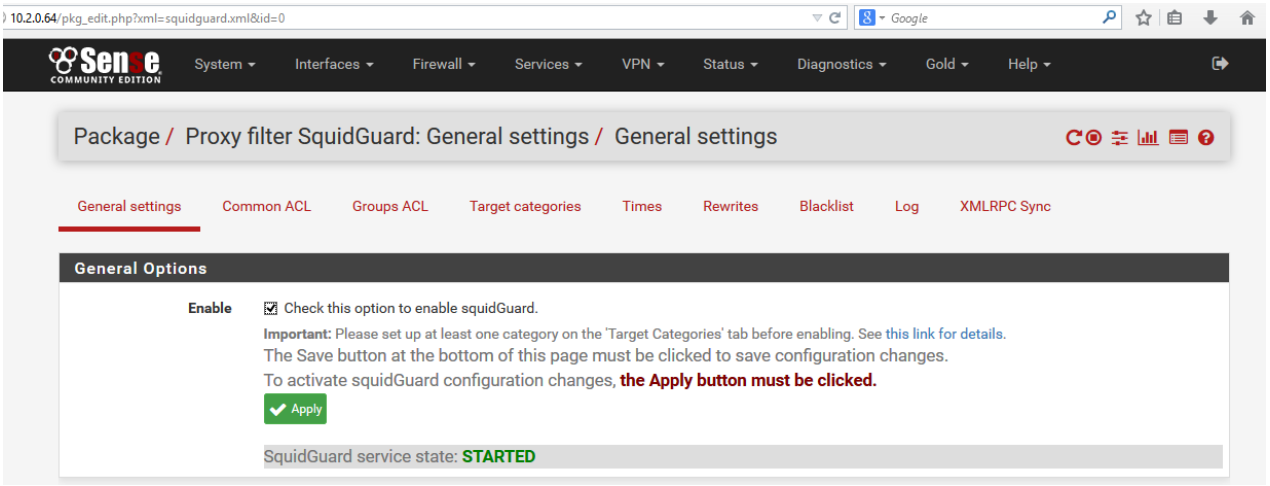

Figure IV.36 : activation de proxy filter SquidGuard.

❖ Test :

Dans notre liste_noire nous avions configuré le site « netacad.com », une station du réseau LAN ne peut donc pas accéder à ce site là. De même il n'est pas possible d'accéder à des sites web qui sont dans une catégorie « deny » (bloquée) (voir figure IV.37).

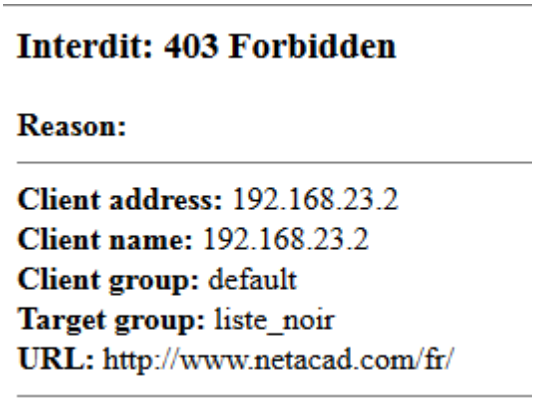

Figure IV.37 : page web bloquée.

V. Discussion :

Dans ce chapitre, nous avons présenté les pré-requis utilisés afin de configurer Pfsense, puis nous avons expliqué à travers plusieurs captures, les étapes de son installation et de sa configuration, à travers lesquelles nous avons traité le filtrage d'URL en basant sur Squid et SquidGuard.

Lors des tests que nous avons effectués, nous avons pu bloquer des sites indésirables. En effet, pour vérifier le fonctionnement du logiciel Pfsense, nous l'avons testé sur les sites Facebook et Netacad.com. L'application a bien fonctionné et les sites ont donc été bloqués.

Conclusion

Conclusion

Dans notre mémoire, nous avons implémenté une application permettant de filtrer des sites internet indésirables afin d'optimiser le réseau informatique. Cette application a consisté en l'utilisation d'un logiciel open source « PfSense » sous VMware qui permet de faire office de pare-feu et de routeur.

Dans le premier chapitre nous avons exposé les généralités et les concepts des réseaux informatiques. Dans le deuxième chapitre, nous avons présenté les différentes transmissions dans un réseau informatique. Des généralités sur la sécurité informatique ont été présentées dans le troisième chapitre. Nous avons proposé une solution à travers laquelle nous avons optimisé un réseau informatique en utilisant PfSense.

Le « pfsense » offre beaucoup de fonctionnalités très poussées et en plus de ça, il permet d'ajouter de packages qui lui sont permet d'être totalement modulable. Dans notre projet nous avons ajouté (installer et configurer) les packages « Squid » et « SquidGuard » afin de permettre le filtrage d'URL à travers lequel on peut réellement créer un système très robuste sur notre propre réseau.

En réalisant un ensemble de tests, après avoir établi une liste noire, nous avons pu bloquer les sites indésirables se trouvant cette liste avec cette solution. Pour permettre une vérification personnalisée, nous avons testé la solution sur les sites Facebook et Netacad.com. L'application a bien fonctionné et les sites ont donc été bloqués.

En perspectives, il serait intéressant de combiner plusieurs packages pour une meilleure sécurisation. En effet, le package SNORT permet la détection et la prévention d'intrusion réseaux et d'inclure des règles d'accès pour mieux gérer la bande passante.

BILIOGRAPHIE

[1] : Malek RAHOUAL, Patrick SIARRY, Réseaux informatiques, conception et optimisation, Edition TECHNIP, 2006.

[2] : José DORDOIGNE, Les réseaux : notions fondamentaux, Edition ENI.

[3] : Lylia BEKHTAOUI, Amal AMIR, Proposition d'une solution réseau au profit de la faculté GEI de l'U.M.M.T.O, Mémoire de fin d'études d'ingénieur d'état en électronique, 2008.

[4] : AIT ABED Leila, HABRECHE Souhila, teste de pénétration des réseaux avec implémentation de sécurité, mémoire de fin d'études de master en informatique, option réseau, mobilité et système embarqués, 2014.

[5] : IBEGHOUCHENE Amar, Protocoles de routage à état de liaisons, mémoire de fin d'étude de master II en électronique, option réseau et télécommunication, 2012.

[6] : SAADI Khadra, MESSAHEL Nouara, Installation et configuration d'un firewall logiciel [PFSense] « ENIEM », mémoire de fin d'étude de master II en électronique, option réseau et télécommunication, 2017.

Sites :

[7] : http://christian.caleca.free.fr/reseaux/, avril 2018

[8] : http://www.folan.net/wp-content/uploads/2013/09/livret-tout-savoir-sur-la-fibre-optique.pdf

[9]: http://www.pearson.fr/resources/titles/27440100468110/extras/introduction.pdf, juin 2018

[10] : http://www.formations-virtualisation.fr/vmware-definition-vmware.php, juin 2018

[11] : https://ademcalici.puzl.com/files/1571345/download/pfsensetuto.pdf, juin 2018

[12] : http://fr.slideshare.net/ISMAILRACHDAOUI/installation-etconfiguration-de-pfsense, juin 2018
[13] : http://fr.slideshare.net/marwenbencheikhali/rapportfiniale, juin 2018