

**République Algérienne Démocratique et Populaire**  
**Ministère de l'Enseignement Supérieur et de la**  
**Recherche Scientifique Université A. MIRA-BEJAIA**

**Faculté de Technologie**  
**Département Génie Electrique**



## **MEMOIRE DE FIN D'ETUDE**

Présenté en vue de l'obtention du diplôme :

### **MASTER EN TELECOMMUNICATIONS SPECIALITE RESEAUX ET TELECOMMUNICATIONS**

Présenté par :

- ABDERRAHMANI Mohammed oubelkacem  
- AIT MOKRANE Hind

**Thème**

**Mise en place d'un proxy Squid sous CentOS Linux**

Soutenu le 30 juin 2018

#### **Les membres de jury :**

**Mlle. Y. ACHOUR**

**Promotrice**

**Mr. N. BENAMIROUCHE**

**Président**

**Mlle. L. BOUCHOUCHA**

**Examinatrice**

**2017/2018**

## Table des matières

- *Liste des figures*
- *Les abréviations*
- *La bibliographie*
- *Introduction générale: ----- 1*

**I. Chapitre I : 3**

- 1. Introduction : ..... 3**
- 2. Généralités sur les réseaux informatiques ..... 3**
  - 2.1. Définition d'un réseau Informatique ..... 3
  - 2.2. L'intérêt d'un réseau : ..... 3
  - 2.3. Classification des réseaux : ..... 4
  - 2.4. Equipement matériels d'un réseau : ..... 8
  - 2.5. Architecture des réseaux : ..... 10
  - 2.6. Adressage IP : ..... 15
  - 2.7. Routage IP: ..... 16
- 3. Conclusion : ..... 17**

**II. Chapitre II : ..... 18**

- 1. Le concept de sécurité de réseau : ..... 18**
  - 1.1. Présentation : ..... 18
  - 1.2. Terminologie de la sécurité informatique ..... 18
  - 1.3. Les objectifs de la sécurité : ..... 19
  - 1.4. Aspect technique de la sécurité informatique : ..... 19
  - 1.5. Mise en place d'une politique de sécurité : ..... 20
- 2. Les attaques informatiques : ..... 21**
  - 2.2. Types d'attaques : ..... 21
- 3. Dispositifs de protection : ..... 22**
  - 3.1. Cryptographie : ..... 22
  - 3.2. Réseaux privés virtuels : ..... 24
    - 3.2.1. Fonctionnement d'un VPN : ..... 25
  - 3.3. Le par feu (fire wall) : ..... 25
    - 3.3.1. Principe de fonctionnement d'un pare feu : ..... 26
  - 3.4. PfSens : ..... 27
  - 3.5. La zone dématérialisé DMZ : ..... 28
  - 3.6. Système de détection d'intrusion : ..... 29

3.7.Serveurs mandataires (Proxy) : .....	29
3.7.1.Principe de fonctionnement : .....	29
3.7.2.Les fonctionnalités du proxy : .....	29
<b>4. Conclusion : .....</b>	<b>31</b>
<b>III. Chapitre III : .....</b>	<b>32</b>
<b>1. Introduction : .....</b>	<b>32</b>
<b>2. Approche par intégration d'un serveur mandataire: .....</b>	<b>32</b>
<b>3. Présentation de l'EPB : .....</b>	<b>32</b>
<b>4. Analyse du projet : .....</b>	<b>36</b>
<b>5. Ressources matérielles et logiciels : .....</b>	<b>36</b>
5.1.Ressource matérielles : .....	36
5.2. Ressource logiciels : .....	36
<b>6. Installation et configuration de CentOs 7 : .....</b>	<b>38</b>
<b>7. Installation et configuration du serveur Squid : .....</b>	<b>42</b>
7.1. Fichier et répertoire SQUID.....	43
7.2. Paramètres à mettre en place au niveau d'Active Directory: .....	43
7.3. Configuration du serveur Squid : .....	49
7.4. Les Helpers : .....	50
7.5. Le fichier Squid.conf: .....	51
<b>8. Intégration de l'authentification LDAP : .....</b>	<b>56</b>
<b>9. Lancement et maintenance du serveur Squid : .....</b>	<b>57</b>
9.1. Lancement du serveur Squid : .....	57
9.2. Création des répertoires swap : .....	58
9.3. Maintenance du serveur Squid : .....	59
<b>10. Phase de Test (coté client) : .....</b>	<b>60</b>
<b>11. SquidGuard : .....</b>	<b>62</b>
11.1. Présentation : .....	63
<b>12. L'antivirus clamav : .....</b>	<b>65</b>
12.1. Définition : .....	65
12.2. Installation de clamav .....	65
<b>13. Conclusion : .....</b>	<b>66</b>
<b>Conclusion générale .....</b>	<b>67</b>

## **Listes des figures :**

Figure 1.1: Topologie Bus.....	5
Figure 1.2: Topologie Anneau .....	6
Figure 1.3: Topologie Arbre.....	6
Figure 1.4: Topologie Etoile .....	7
Figure 1.5: Topologie Maillé .....	7
Figure 1.6: Topologie Hybride.....	8
Figure 1.7: Les connecteurs .....	11
Figure 8: Fonctionnement du client/serveur.....	12
Figure 1.9: Modèle OSI /TCP IP.....	14
Figure 1.10: Trame d'Adresse IP.....	15
Figure 2.1: Illustration de chiffrement à clé Symétrique.....	23
Figure 2.2: Illustration de chiffrement à clé Asymétrique .....	23
Figure 2.3: Pare feu .....	26
Figure 2.4: Zone dématérialisé DMZ.....	28
Figure 3.1: Schémas du réseau global de l'EPB .....	33
Figure 3.2 : Segment du réseau touché par l'étude.....	34
Figure 3.3: Menu boot de l'installation.....	35
Figure 3.4: Menu choix de langue.....	36
Figure 3.5: Menu de répertoire d'installation .....	37
Figure 3.6: Choix de la destination .....	38
Figure 3.7: Ecran d'installation.....	39
Figure 3.8: Commande pour paramétrer la carte réseau .....	39
Figure 3.9: Menu de Paramétrage réseau .....	40
Figure 3.10:Activation de la carte réseau.....	40
Figure 3.11: Configuration de la carte réseau .....	41
Figure 3.12: Vérification des configurations.....	41
Figure 3.13: Commande pour télécharger la liste des composants .....	42
Figure 3.14: Commande pour télécharger la liste des composants .....	42
Figure 3.15: Commande pour mettre à jour le système .....	42
Figure 3.16: Commande pour redémarrer le système .....	42
Figure 3.17: Installation de squid.....	42
Figure 3.18: Création d'une nouvelle unité d'organisation (1).....	43

Figure 3.19: Création d'une nouvelle unité d'organisation (2) .....	44
Figure 3.20: Création d'un groupe d'utilisateur (1) .....	44
Figure 3.21: Création d'un groupe d'utilisateur (2) .....	45
Figure 3.22: Création d'un nouvel utilisateur (1) .....	45
Figure 3.23: Création d'un nouvel utilisateur (2) .....	45
Figure 3.24: Création d'un nouvel utilisateur (3) .....	46
Figure 3.26: Délégation de contrôle l'utilisateur squid .....	47
Figure 3.27: Sélection de l'utilisateur squid .....	47
Figure 3.28: Figure 41: Sélection des rôles ç déléguer .....	48
Figure 3.29: Ajout de l'utilisateur au Groupe 1 (1) .....	48
Figure 3.30: Ajout de l'utilisateur au groupe 1 (2) .....	49
Figure 3.31: Vérification de la connectivité vers Windows server .....	49
Figure 3.32: Vérification de la connectivité vers squid .....	49
Figure 3.33: Commande test pour le basic_ldap_auth .....	50
Figure 3.34: Commande test pour l'ext_ldap_group_acl .....	51
Figure 3.34: Exemple d'ACL (1).....	52
Figure 3.35: Exemple d'ACL (2).....	52
Figure 3.36: Les ACL relatif au port de la communication .....	52
Figure 3.37: Port ouvert/fermé par défaut .....	53
Figure 3.38: Autorisation par défaut (1).....	53
Figure 3.39: Autorisation par défaut (2).....	53
Figure 3.40: Autorisation par défaut (3).....	53
Figure 3.41: Le port du serveur proxy.....	54
Figure 3.42: Code pour l'authentification LDAP sur squid.....	56
Figure 3.43: Les ACL relatif aux groupes d'Active Directory .....	56
Figure 3.44: Lancement du serveur squid .....	57
Figure 3.45: Menu d'aide du programme squid.....	58
Figure 3.46: Création du répertoire Swap .....	58
Figure 3.47: Vérification de l'état du serveur .....	59
Figure 3.48: Définition du serveur proxy sous internet explorer .....	60
Figure 3.49: Fenêtre d'authentification.....	60
Figure 3.50: Page d'erreur .....	61
Figure 3.51: Installation de epel-release .....	61
Figure 3.52: Installation de squidGard .....	62

Figure 3.53: Intégration des blacklist au squidGard .....	63
Figure 3.54: Définition des ACL.....	64
Figure 3.55:Installation de l'antivirus clamav .....	65
Figure 3.56: scan du répertoire.....	66

## ***Liste des abbreviations:***

### **A:**

**ACL:** Access Control List

**AD:** Active Directory

**ADSL:** Asymmetric Digital Subscriber Line

**ARPT :** Autorité de Régulation de la Poste et des Télécommunications

**ATM:** Asynchronous Transfer Protocol

### **C:**

**CentOS:** Community enterprise Operating System

### **D:**

**DNS:** Domain Name System

**DMZ:** Demilitarized zone

### **E :**

**EPB:** Entreprise Portuaire Bejaia

### **G:**

**GNS:** Graphical network simulator

**GNU:** General Public License

### **F:**

**FTP:** File Transfer Protocol

### **H:**

**H-IDS:** Host Based Intrusion Detection System

**HTTP:** Hyper Text Transfer Protocol

### **I:**

**IDS:** Intrusion Detection System

**IOB:** Ighil Oberouak

**ISO:** International Standardization Organization

**IP:** Internet Protocol

**IEEE:** Institute of Electrical and Electronics Engineers

### **L:**

**LAN:** Local Area Network

**LDAP:** Lightweight Directory Access Protocol

**LDPU:** Logical Protocol Data Unit

**M:**

**MAN:** Metropolitan Area Network

**N:**

**NAT:** Network Address Translation

**NIC:** Network Interface Card

**N-IDS:** Network Based Intrusion Detection System

**O:**

**OSI:** Open Systems Interconnection

**P:**

**PAN:** Personnel Area Network

**S:**

**SMTP:** Simple Mail Transfer Protocol

**T:**

**TCP:** Transmission Control Protocol

**U:**

**UDP:** User Datagram Protocol

**V:**

**VPN:** Virtual Private Network

**W:**

**WAN:** Wide Area Network



## *Remerciements*

*La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui on voudrait témoigner toute notre reconnaissance.*

*On voudrait tout d'abord adresser toute notre gratitude le grand remerciement à notre encadreur « Dr. Achour », pour ses conseils et ses dirigés du début à la fin de ce travail.*

*Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.*

*Enfin, nous tenons également à remercier toutes nos familles et nos ami(e)s et tous ceux qui ont participé de près ou de loin à la réalisation de ce travail*

### *Introduction Général :*

L'informatique est devenue très ouverte au monde extérieur du fait de la démocratisation de l'ordinateur personnel et l'avènement de l'Internet. Ce dernier est un outil incontournable et il réunit plein d'utilisateurs à travers le monde avec 3.82 milliards d'internautes, soit 51% de la population mondiale et 822 240 nouveaux sites Internet mis en ligne chaque jour (en 2017), et le site Internet World Stat avance le chiffre de 18 580 000 internautes en Algérie. Et ce chiffre ne cesse d'augmenter.

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

Un accès internet fiable et performant est un besoin majeur pour l'activité des entreprises et des collectivités. Réseau, échanges d'e-mails ou d'informations, contacts avec les clients et les fournisseurs, toutes les relations sont maintenant Interdépendantes.

En effet l'utilisation d'Internet dans l'entreprise est en perpétuelle tension entre autonomie et contrôle. La publication de chartes d'utilisation qui stipule les restrictions de l'utilisation d'internet au sein de l'entreprise, témoigne malgré sa diffusion importante, de l'inachèvement du processus d'appropriation collective de la technologie, et donc l'entreprise doit se doter de moyens de contrôle sur l'utilisation d'internet dans son enceinte.

L'un des plus importants de ces dispositifs est le serveur mandataire proxy, qui sert d'intermédiaire entre les utilisateurs et internet, pour ainsi définir les niveaux d'accès entre les différents utilisateurs et restreindre l'accès à certains sites ou à un certain type de contenu (images, vidéos, mails ...etc.). On peut lui attribuer également l'analyse du trafic web afin d'y détecter des activités malveillantes. Enfin un proxy sert de cache web, c'est-à-dire qu'il permet la mise en cache de site web, en gardant une copie des documents transitant par son biais, et répondre aux requêtes ultérieures à partir de ses copies, sans recourir au serveur Web d'origine. En résumé, un serveur mandataire est d'une utilité capitale dans une architecture réseau, au vu de ses nombreux avantages qu'il offre.

Pour cela notre travail a eu lieu au sein de l'entreprise portuaire de Bejaia, qui de par son envergure et la place importante qu'elle tient sur le marché national, et face à la concurrence assez présente sur les marchés dans lesquelles elle s'active, elle doit maximiser sa productivité pour confirmer son rang et pouvoir étendre ces activités, et son infrastructure réseau tient une place importante dans cette productivité, vu que l'ensemble des données générées par les différents services de l'entreprise sont

stockées et manipulées sur les machines et les serveurs de cette infrastructure réseau, donc cette dernière doit d'être sécurisée pour ainsi garantir la confidentialité, l'intégrité et la disponibilité de ces données-là.

Et pour bien éclairer notre objet d'étude nous avons organisé la présentation de ce travail en trois chapitres :

- ❖ Le premier chapitre est consacré aux généralités sur les réseaux
- ❖ Le deuxième chapitre est focalisé sur les généralités de la sécurité informatique, où on présente les outils nécessaires pour l'assurer
- ❖ Le troisième chapitre présente la problématique de notre travail, la solution proposée, les outils de réalisation et l'ensemble des configurations faites dans le cadre de son implémentation

Nous allons terminer notre mémoire par une conclusion générale.

## 1. Introduction

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines .Or la sécurité informatique est le problème majeur qui touche les réseaux informatiques. De nos jours, il prend de plus en plus de place dans la gestion des réseaux d'entreprise ainsi que dans les usages des particuliers toujours plus nombreux à se connecter à Internet.

La transmission d'informations sensibles et le besoin d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place des réseaux informatiques.

La sécurité informatique tient dans l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

Il convient d'identifier les exigences fondamentales en sécurité informatique, il est nécessaire de se protéger de ces attaques réseaux en installant un dispositif de protection.

## 2. Généralités sur les réseaux informatiques

### 2.1 Définition d'un réseau informatique :

Un réseau informatique est un élément indispensable pour assurer la communication entre deux ou plusieurs ordinateurs. Cette connexion entre les machines permet d'échanger des informations. Un parc informatique est généralement constitué d'un ou plusieurs réseaux informatiques. Ces entités sont connectées entre elles par l'intermédiaire de lignes physiques appelées lignes de communications qui servent au transport et l'échange de données et d'informations.

Il existe différents types de réseaux informatiques : internet, intranet, extranet [1].

### 2.2. L'intérêt d'un réseau :

Les réseaux sont bien évidemment nés d'un besoin d'échange d'informations. Ainsi, une entreprise possédant plusieurs sites de production peut avoir un ordinateur sur chaque site pour gérer, par exemple, stocks, salaires, production...etc.

Le besoin de communication va inciter le manager à connecter ses ordinateurs pour pouvoir extraire et échanger des informations concernant toute l'entreprise [2].

Dans ce cas beaucoup d'objectifs vont apparaître, comme :

- Partage des ressources et des données dans un environnement sécurisé (imprimantes, logiciels, disques durs).
- Accès multiple et à distance, à travers des stations utilisateurs.
- Intégration traitement de données et bureautique (accès base de données).
- Harmonisation des logiciels de l'entreprise.
- Interconnexion de matériel hétérogène.
- Satisfaction des besoins de communications (mail, échange d'information).
- Commande de machine à distance.
- Gain de temps et réduction de coût.
- Fiabilité des applications des données sur plusieurs sites.

### **2.3. Classification des réseaux :**

Les réseaux sont classés selon de multiples critères :

#### **2.3.1. Distance :**

On distingue différents types de réseaux selon leur étendue. On fait généralement quatre catégories de réseaux : [2]

- Réseau PAN (Personnel Area Network)
- Réseau LAN (Local Area Network)
- Réseau MAN (Metropolitan Area Network)
- Réseau WAN (Wide Area Network)

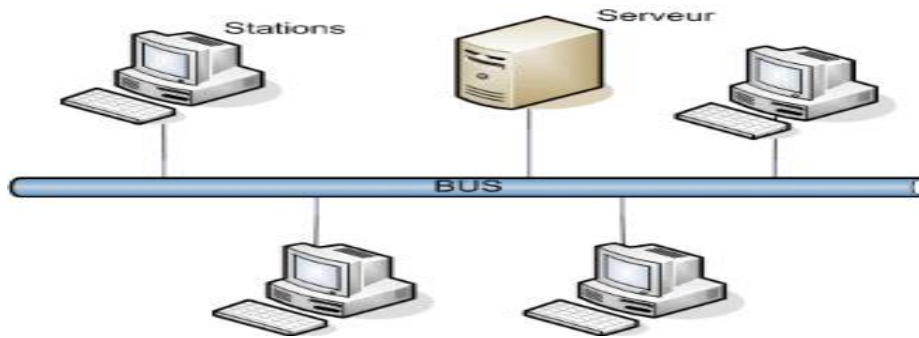
#### **2.3.2. Topologie physique :**

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la topologie physique, qui décrit comment les machines sont raccordées au réseau.

##### **▪ La topologie en BUS :**

La plus simple des topologies de base un réseau de type BUS se compose d'une longueur continue du câble chaque station accède directement au réseau qui relie deux dispositifs ou

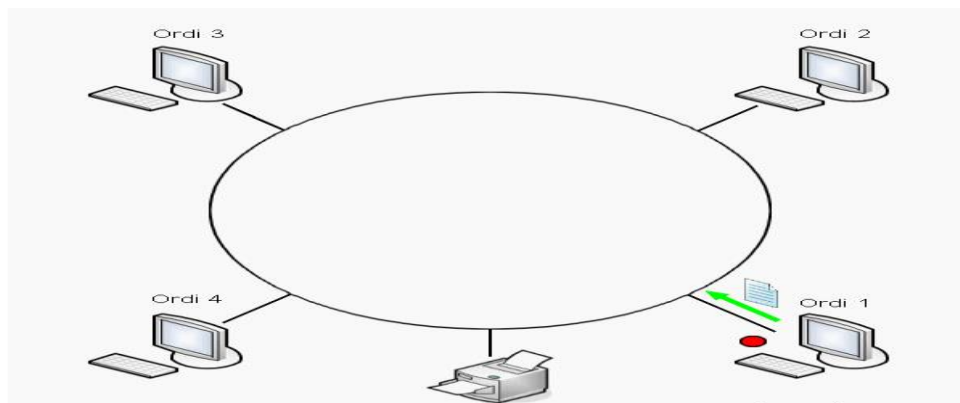
plus. Il est également appelé réseau Back Bone. Ils autorisent des débits importants (>100 Mbit/s sur 100 m). Il est possible d'y insérer une nouvelle station sans perturber les communications en cours. Cependant, la longueur du bus est limitée par l'affaiblissement du signal « figure 1.1 ». [3]



**Figure 1.1 :** Topologie Bus

▪ **La topologie anneau :**

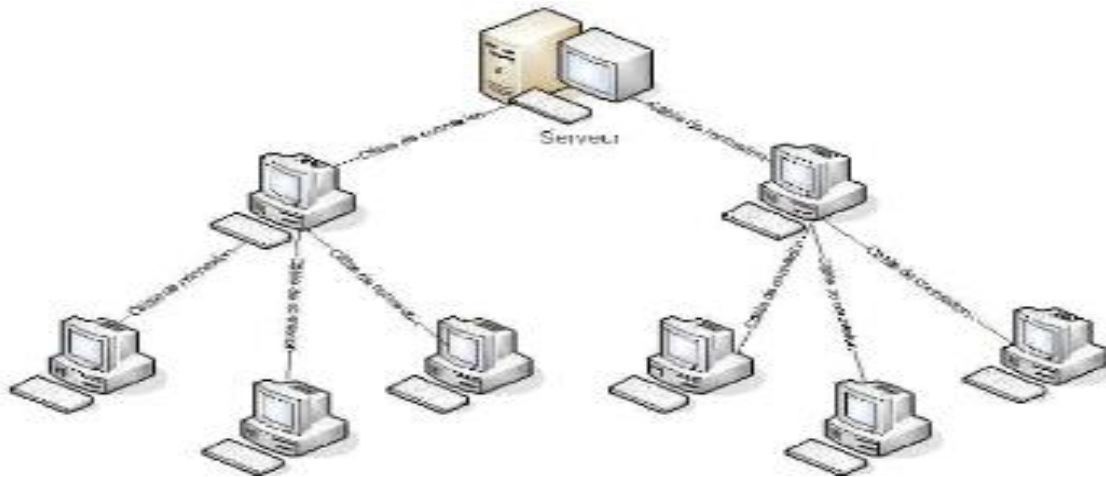
Cette topologie repose sur une boucle fermée, en anneau (ring), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud qui se comporte comme un récepteur (élément actif). Les concentrateurs en anneau (MAU - Multistation Acces Unit) sont des équipements passifs ou actifs (L'information circule dans un seul sens) qui par un jeu de relais électromagnétiques, permettent aux stations de s'insérer facilement dans le réseau. [4]



**Figure 1.2 :** Topologie Anneau

- **La topologie arbre :**

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence « figure 1.3 ». [3]

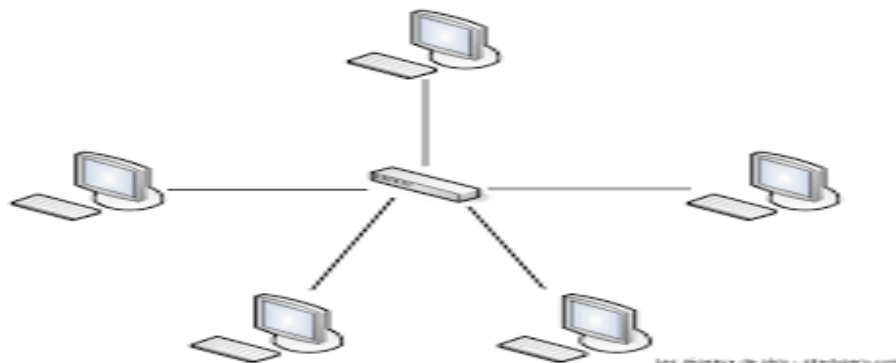


**Figure 1.3 :** Topologie Arbre

- **La topologie étoile (star):**

Elle est composée de l'ordinateur individuel relié à un point central sur le réseau. Le réseau Étoile est le type le plus commun de réseau. [5]

La topologie étoile autorise des dialogues entre nœud très performants. La défaillance d'un poste n'entraîne pas celle du réseau, cependant le réseau est très vulnérable à celle du nœud central « figure 1.4 ».



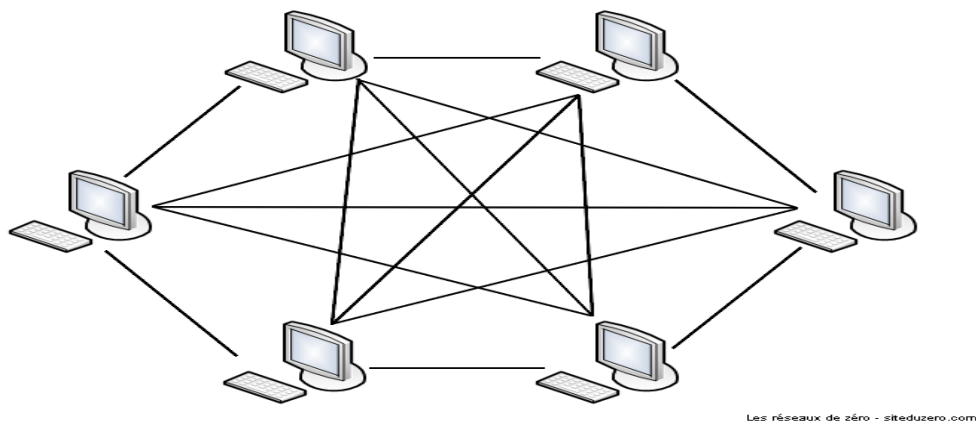
**Figure 1.4 :** Topologie Etoile

- **Topologie maillée :**

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

Cette topologie se rencontre dans les grands réseaux de distribution. L'information peut parcourir le réseau suivant des itinéraires divers.

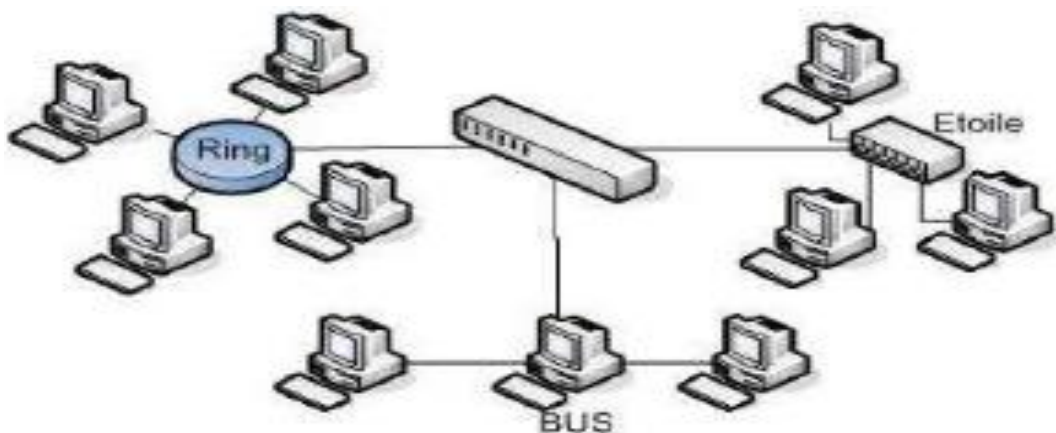
En cas de rupture d'un lien, l'information peut quand même être acheminée « figure 1.5 ». [5]



**Figure 1.5 :** Topologie Maillé

- **La topologie Hybride :**

La topologie hybride de réseau emploie un mélange de différents genres de structures de réseau, comme STAR, BUS et RING «figure 1.6 ».



**Figure 1.6 :** Topologie Hybride



### 2.3.3. Débit :

- Réseaux locaux :
  - Traditionnel : Ethernet 10, 100Mbits/s
  - Haut débit : ATM 155 ou 662 Mbits/s
- Réseaux large échèles :
  - Epine dorsale France –USA, 155Mbits/s
  - Par utilisateur, faible débit
- Modem : 9,6 ; 33,4 ou 56 Kbits/s

### 2.3.4. Mode de transmission :

- **Filaire :**

Le réseau filaire classique utilise des câbles Ethernet pour relier les équipements réseaux. Les caractéristiques d'un réseau Ethernet sont la rapidité, la fiabilité et la sécurité. [6]

- **San fil :**

La transmission des données est basée sur une liaison utilisant des ondes radioélectriques (ou infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies, se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

Parmi ces technologies on peut citer particulièrement: Bluetooth, wifi.

## 2.4. Equipement matériels d'un réseau :

La première chose à mettre en œuvre pour constituer le réseau est la transmission des informations d'un équipement à l'autre on distingue :

### 2.4.1. Le support de transmission:

Ce sont les matériels utilisés pour relier physiquement les équipements d'un réseau. On cite succinctement quelques-uns des supports de transmission les plus utilisés : Le câble coaxial, La paire torsadée, La fibre optique, La liaison sans fil. [7]

### 2.4.2. les équipements d'interconnexion

- **Répéteur** : c'est un dispositif non intelligent, qui répète automatiquement les signaux qui lui arrivent et transitent d'un support vers un autre support.
- **Concentrateur (Hub)** : Le Hub est un dispositif permettant la connexion de plusieurs nœuds sur un même point d'accès sur le réseau, en se partageant la bande passante totale. C'est le fameux point central utilisé pour le raccordement des différents ordinateurs dans un réseau de topologie physique en étoile.
- **Le pont (bridge)** : il filtre le trafic entre deux segments physiques en fonction des adresses MAC. Le point d'accès Wi-Fi est une sorte de ponts. [8]
- **Le Commutateur (Switch)** : en général, les stations de travail d'un réseau Ethernet sont connectées directement à lui. Un commutateur relie les hôtes qui sont connectés à un port en lisant l'adresse MAC comprise dans les trames. Intervenant au niveau de la couche 2, il ouvre un circuit virtuel unique entre les nœuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports
- **Routeur (router)** : Un routeur est un équipement d'interconnexion de réseau informatique permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.
- **Passerelle (Gateway)** : Une passerelle (point d'accès) est souvent utilisée pour relier différents types de réseaux ensemble. Le *Gateway* est employé pour passer l'information d'un réseau à l'autre. Une passerelle peut être un dispositif physiquement relié au réseau et transfère l'information entre réseaux. Une passerelle peut également être un logiciel qui permet à deux protocoles différents d'échanger l'information sur le réseau. [1]
- **Pare feu** : Encore appelé fire wall ou coupe-feu, le pare feu c'est un système permettant de protéger un ordinateur des intrusions provenant du réseau.  
On l'utilise pour protéger le LAN des attaques provenant de l'extérieur [7].

### 2.4.3. Les serveurs et les stations de travail

#### Définition d'un serveur:

un serveur est à la fois un ensemble de logiciels et l'ordinateur les hébergeant. Son rôle est de répondre de manière automatique à des demandes envoyées par des clients via le réseau.

Les principales utilisations d'un serveur sont : [8]

- **le serveur de fichiers** (*file server*) : est utilisé pour le stockage et le partage de fichiers. Les fichiers placés dans les mémoires de masse du serveur peuvent être manipulés simultanément par plusieurs clients.
- **Le serveur d'impression** : est utilisé comme intermédiaire entre un ensemble de clients et un ensemble d'imprimantes. Chaque client peut envoyer des documents à imprimer aux imprimantes reliées au serveur [8].
  - **le serveur de base de données** : est utilisé pour stocker et manipuler des données contenues dans une ou plusieurs bases de données et partagées entre plusieurs clients.
  - **le serveur de courrier** : est utilisé pour stocker et transmettre du courrier électronique
  - **le serveur web** stocke et manipule les pages d'un site Web et les transmet sur demande au client.
  - **le serveur mandataire** (*proxy*) : reçoit des demandes, les contrôle, puis les transmet à d'autres serveurs. Il peut être utilisé pour accélérer le traitement des demandes (mémoire cache), ou faire appliquer des réglages de filtrage [3].

#### 2.4.4. Les équipements intermédiaires :

- **Network Interface Card (NIC)**: Chaque carte d'interface de réseau a une adresse unique. Cette adresse MAC est employée pour identifier chaque carte d'interface de réseau quand l'information est envoyée ou reçue sur le réseau [9].
- **Les prises**: Il s'agit de l'élément permettant de réaliser la jonction mécanique entre la carte réseau et le support physique (la prise RJ-45 à huit contacts).
- **Le transmetteur** (appelé aussi adaptateur ou transceiver) : Un adaptateur est un dispositif qui permet de relier deux appareils ou deux pièces, qui n'ont pas été initialement conçus pour être assemblés.
- **Les connecteurs** : Il existe plusieurs types de cartes Ethernet qui se distinguent par leur connecteur : [9]
  - BNC pour l'Ethernet en bus
  - RJ45 pour l'Ethernet en étoile
  - AUI pour l'Ethernet en bus ou en étoile
- **Connecteurs optique** : Le connecteur le plus répandu est sans doute le connecteur de type ST, mais il a l'inconvénient de se présenter sous la forme de deux prises, une fiche émission et une fiche réception, de même que le connecteur de type SC.



**Figure 1.7** : les différents connecteurs

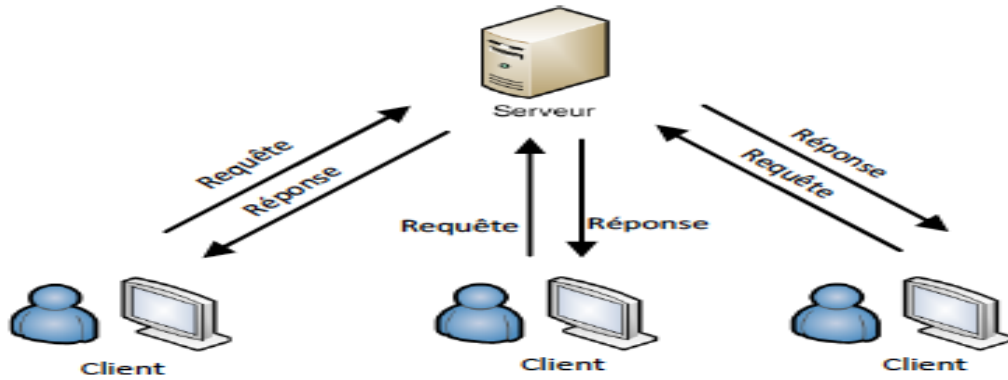
## 2.5. Architecture des réseaux :

### 2.5.1. à Point (Peer to Peer / égal à égal) :

Dans une architecture d'égal à égal (*Peer to Peer*), chacun des ordinateurs du réseau est libre de partager ses ressources. Toutes les machines sur le réseau ont les mêmes droits, Son faible coût et sa simplicité peuvent séduire, mais c'est un système difficile à administrer, et assez peu sécurisé car aucun maillon du système n'est totalement fiable. Il est assez difficile à faire évoluer, et n'a d'intérêt que pour un réseau de moins de dix utilisateurs [10].

### 2.5.2. Client / Serveur (Server Based) :

Dans un système client/serveur, des machines clientes sont reliées à un serveur qui leur fournit des services communs. Ce système permet de centraliser et de sauvegarder les données. De plus, il permet une meilleure sécurité, car le nombre de points d'entrée permettant l'accès aux données est assez réduit. L'administration est plus fine et se fait essentiellement au niveau du serveur. Enfin, ce type de réseau est évolutif, car il est possible de supprimer ou d'ajouter de nouvelles machines sans perturber le fonctionnement du réseau et sans modifications majeures ; la gestion des utilisateurs est donc simplifiée « figure 1.8 » [11].



**Figure 1.8 :** Fonctionnement du client/serveur

- Le client émet une requête vers le serveur grâce à son adresse, demandant un service.
  - Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente.
- Dans cette architecture le serveur a une grande tolérance à la panne, notamment s'il traite plusieurs clients.

### 2.5.3. Modèle OSI :

L'ISO (International Standardisation Organisation) a normalisé sa propre architecture sous le nom d'OSI (Open Systems Interconnection). L'architecture ISO est la première à avoir été définie, et ce de façon relativement parallèle à celle d'Internet (TCP/IP). La distinction entre les deux est que l'architecture ISO définit formellement les différentes couches, tandis que l'architecture Internet s'applique à réaliser un environnement pragmatique (pratique). Le modèle de référence OSI comporte sept niveaux, ou couches, plus un médium physique, que l'on appelle parfois couche 0 correspond au support physique de communication chargé d'acheminer les éléments binaires d'un point à un autre jusqu'au récepteur final. Ce médium physique peut prendre diverses formes, allant du câble métallique aux signaux hertziens, en passant par la fibre optique et l'infrarouge. Le modèle OSI n'est pas une véritable architecture de réseau, car il ne précise pas réellement les services et les protocoles à utiliser pour chaque couche. Il décrit plutôt ce que doivent faire les couches. Néanmoins, l'ISO a écrit ses propres normes pour chaque couche, et ceci de manière indépendante au modèle.

**Couche physique (*physical*) :** La couche physique gère la communication avec l'interface physique afin de faire transiter ou de récupérer des données, Elle fournit les moyens mécaniques, électriques, fonctionnels, à l'activation, au maintien et à la désactivation des connexions physiques destinées à la transmission des éléments binaires entre entités de liaisons La transmission est effectuée comme une séquence des bits sur un circuit de communication

**Couche liaison (*data Link*) :** La couche liaison s'occupe de la bonne transmission de l'information entre les nœuds via le support, en assurant la gestion des erreurs de transmission et les synchronisations des données.

**Couche réseau (*network*) :** La couche réseau a en charge de déterminer le choix de la route entre les nœuds afin de transmettre de manière indépendante l'information ou les différents paquets la constituant en prenant en compte en temps réel le trafic. Elle assure également un certain nombre de congestion qui ne sont pas gérés par la couche de liaison. [18]

**Couche transport (*message*) :** Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux. [14]

**Couche session :** Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne [14].

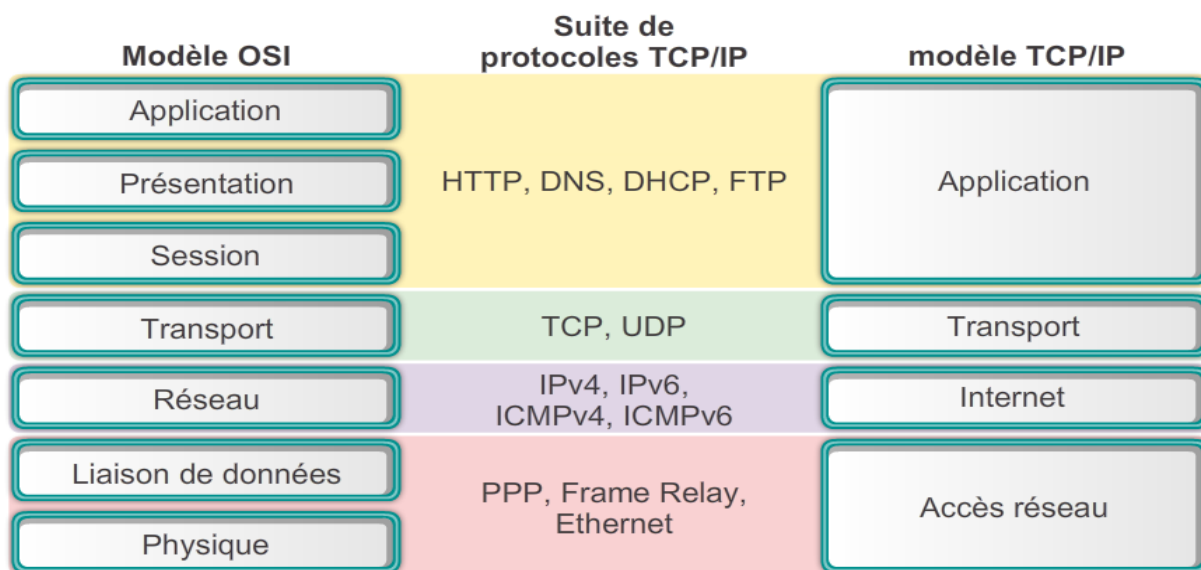
**Couche présentation :** Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

**Couche application :** Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie... [15].

### 2.5.4. TCP/IP :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise par-dessus un protocole réseau, IP (Internet Protocol). Ce qu'on entend par modèle TCPIP, c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP, comme nous le verrons plus bas, s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI. En effet, contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation ; la normalisation est venue ensuite. Cet historique fait toute la particularité de ce modèle, ses avantages et ses inconvénients.



**Figure 1.9:** Modèle OSI / TCP IP

#### La couche hôte réseau

Cette couche regroupe la couche physique et liaison de données du modèle OSI. A en charge la communication avec l'interface physique afin de transmettre ou de récupérer les données qui lui sont transmis de la couche supérieure [16].

### **La couche internet**

Correspond à la couche réseau du modèle OSI, s'occupe de l'acheminement des paquets à la bonne destination.

Le protocole IP assure intégralement les services de cette couche, le format et la structure des paquets IP sont précisément définis [18].

### **La couche transport**

Son rôle est le même que celui de la couche transport du modèle OSI, gère le fractionnement et le réassemblage en paquet de flux de données à transmettre, le routage ayant pour conséquence un arrivage de paquets dans un ordre incertain. Cette couche s'occupe également du réagencement ordonnée de tous les paquets d'un même message.

Les deux principaux protocoles pouvant assurer les services de ces couches :

- TCP (transmission control Protocol) : protocole fiable, assure une communication sans erreurs par un mécanisme question/réponse/confirmation/synchronisation (orienté connexion).
- UDP (User Datagram Protocol) : protocole non fiable, assure une communication rapide mais pouvant contenir des erreurs en utilisant un mécanisme question/réponse (sans connexion).

### **La couche application**

Similaire à la couche application du modèle OSI, correspond aux différentes applications utilisant les services réseaux pour communiquer à travers un réseau.

Un grand nombre de protocoles divers de haut niveau permettant d'assurer les fonctionnalités de cette couche :

- Telnet : ouverture de session à distance.
- FTP (File Transfer Protocol) : protocole de transfert de fichier
- HTTP (Hyper Text Transfer Protocol) : protocole de Transfert de HyperText
- SMTP (Simple Mail Transfer Protocol) : protocole de Transfert d'email
- DNS (Domain Name System) : nom de domaine



## 2.6. Adressage IP :

### L'adresse IPv4

L'adresse IP d'un nœud est l'identifiant logiciel unique de ce nœud sur le réseau par lequel le nœud est directement joignable. Cette adresse, modifiable à volonté par simple configuration logicielle, est codée sur 32 bits regroupés en 4 octets (d'où le nom IPv4), généralement noté xxx.xxx.xxx.xxx (dite notation décimale pointé) ou chaque « xxx » représente un entier de 0 à 255 et séparé par un point. On distingue deux parties dans l'adresse IP :

- une partie des nombres à gauche désignent le réseau (appelé **net-ID**) ;
- les nombres de droite désignent les ordinateurs de ce réseau (appelé **host-ID**) [18].

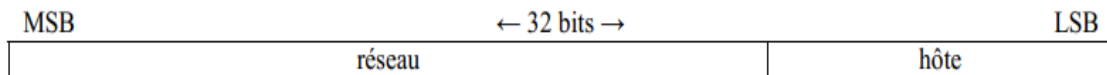


Figure 1.10 : Trame Adresse IP

### Plan d'adressage :

Le plan d'adressage est de définir pour chaque réseau physique (LAN et WAN) une adresse IP. Chaque ordinateur ou composant actif doit avoir un moyen d'être identifié sur le réseau.

Pour cela, une adresse IP lui est attribuée. Il y a deux types d'adressage IP :

- adresse IP privée qui permet la communication inter-entreprises ;
- adresse IP publique utilisée pour la communication vers/ou depuis Internet.

Un organisme spécialisé fournit les adresses IP publiques. C'est donc un plan, d'adressage IP privée que nous sommes censés définir [19].

## 2.7. Routage IP:

### Définition :

Le routage IP, désigne le processus de détermination du chemin par lequel les paquets transitent de la source à la destination.

La route est représentée par la liste ordonnée des différentes machines intermédiaires et successive par lesquelles la communication s'effectue, machines appelées routeurs. De ce fait, sur un réseau, le rôle des routeurs se limite à analyser les paquets qu'ils reçoivent, puis à les acheminer à destination ou à informer l'expéditeur que le destinataire est inconnu et inaccessible. Il achemine ou relaie des paquets en fonction d'itinéraires définis dans sa table de routage [11].

La table de routage, quant à elle, est une base de données qui établit une corrélation entre les adresses IP d'un segment de réseau et l'adresse IP des interfaces du routeur. Nous pouvons opter soit pour un routage statique soit pour un routage dynamique en fonction des besoins

- **Le routage statique** : consiste à configurer manuellement chaque table de routage, ce qui implique une maintenance et une mise à jour manuelle. En routage statique, les routeurs ne se partagent pas de données, ce qui fait du routage un réseau adapté pour les cas de petite taille.
- **Le routage dynamique** : se présente comme solution adéquate lorsqu'un réseau atteint une taille assez importante et devient très lourd d'ajouter des entrées dans les tables de routage à la main. Le routage dynamique permet de mettre à jour les entrées dans les différentes tables de routage de façon plus souple.

## 3. Conclusion :

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

Dans la suite de notre étude nous allons parler des généralités sur la sécurité des réseaux informatiques et des techniques de protections de l'information qui y circulent.

## Introduction :

Chaque ordinateur connecté à Internet et d'une manière plus générale à n'importe quel réseau informatique, est susceptible d'être victime d'une attaque qui visent non seulement à prendre connaissance ou à modifier l'information mais aussi à paralyser le système. Il demeure essentiel de protéger adéquatement toutes ses ressources informatiques contre tout incident de nature accidentelle ou intentionnelle qui pourrait éventuellement occasionner des pertes ou des dommages considérables.

Ainsi, il est nécessaire de se protéger de ces attaques réseaux en installant un dispositif de protection.

Dans ce chapitre on va donner un aperçu sur les concepts de sécurité et ses éléments dans un réseau.

## 1. Le concept de sécurité de réseau :

### 1.1. Présentation :

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

### 1.2. Terminologie de la sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces. Nous allons brièvement évoquer quelques mots clés qui sont largement repris dans la littérature informatique lorsque la sécurité est abordée : [20]

- **Une vulnérabilité** : c'est une faiblesse le plus souvent cachée touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial. L'expression faille de sécurité est également employée [20].

- **Une menace** : La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe à l'entreprise. La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces dernières sont difficiles à réaliser
- **Une attaque** :est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel) ou bien même de l'utilisateur à des fins non autorisées par le propriétaire du système et généralement répréhensibles
- **Un risque** : est le degré d'exposition des actifs informationnels aux menaces, en fonction de la valeur de ces actifs et des mesures en place pour en préserver la sécurité

### 1.3. Les objectifs de la sécurité :

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

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

### 1.4. Aspect technique de la sécurité informatique :

Les problèmes techniques actuels de sécurité informatique peuvent, au moins provisoirement, être classés en deux grandes catégories :

- **la sûreté de fonctionnement** (safety), qui concerne l'ensemble des mesures prises et des moyens utilisés pour se prémunir contre les dysfonctionnements du système.
- **la sécurité** (security), proprement dite, qui regroupe tous les moyens et les mesures prises pour mettre le système d'information à l'abri de toute agression.

### **1.5. Mise en place d'une politique de sécurité :**

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

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

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés,
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

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

## **2. Les attaques informatiques :**

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

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

Afin de contrer ces attaques il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives.

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles
- glaner des informations personnelles sur un utilisateur
- récupérer des données bancaires
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- troubler le bon fonctionnement d'un service
- utiliser le système de l'utilisateur comme rebond pour une attaque
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

## 2.1. Types d'attaques :

Toute acte sur un système dont l'intention est de nuire au moins à l'une des propriétés de sécurité est qualifié de malveillant, et constitue de ce fait une attaque sur ce système [24].

Il existe quatre grands types d'attaques :

- **Attaques d'accès :** Une attaque d'accès ou une attaque d'interception est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information, et peut se produire par plusieurs techniques telles que : l'homme du milieu (Man-In-The-Middle), le sniffing, les chevaux de Troie, porte dérobée, Le craquage de mots de passe
- **Les attaques de modification :** consistent à modifier les informations (intercepte des données et les modifie avant de les envoyer au destinataire). Ce type d'attaque est dirigé contre l'intégrité de l'information.

Elle peut se présenter sous forme de Virus, vers et chevaux de Troie, canular ...

- **Les attaques par saturation (Attaques par déni de service) :** sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.

Il existe différentes attaques par saturation on cite : Le flooding, le débordement de tampon , le smurf ....

- **Les attaques de répudiation** : sont des attaques contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passés. Exemple Le IP spoofing [25].

### 3. Dispositifs de protection :

De nos jours, toutes les entreprises possédant un réseau local possèdent aussi un accès à Internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable... et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'informations confidentielles, ... Les mobiles sont nombreux et dangereux.

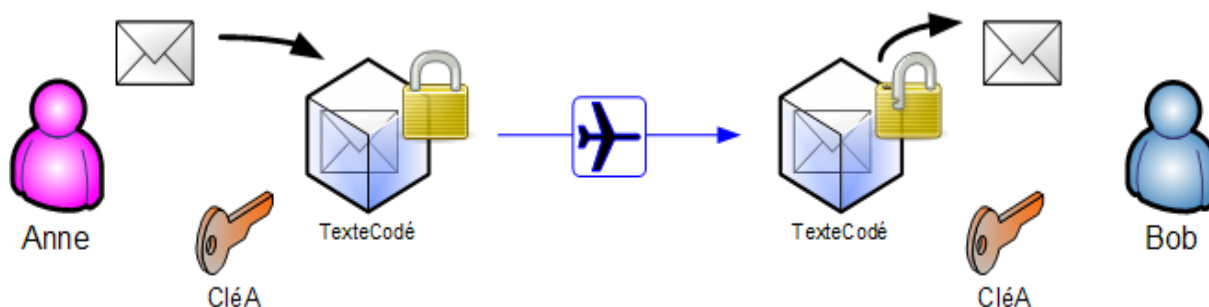
Pour parer à ces attaques, IL est nécessaire de se protéger des attaques réseaux en installant un dispositif de protection dans le but de le protéger des intrusions son nombreux on citera :

#### 3.1. Cryptographie :

Le chiffrement est un procédé qui permet de transformer un message en clair, lisible par tous, en un message codé uniquement compréhensible par qui dispose du code. [28]

- **Cryptographie symétrique** :

La cryptographie symétrique consiste à utiliser la même clé pour le chiffrement ainsi que pour le déchiffrement. Il est donc nécessaire que deux interlocuteurs se soient mis d'accord sur une clé privée, où ils doivent utiliser un canal sécurisé pour l'échanger « figure 2.1 ».



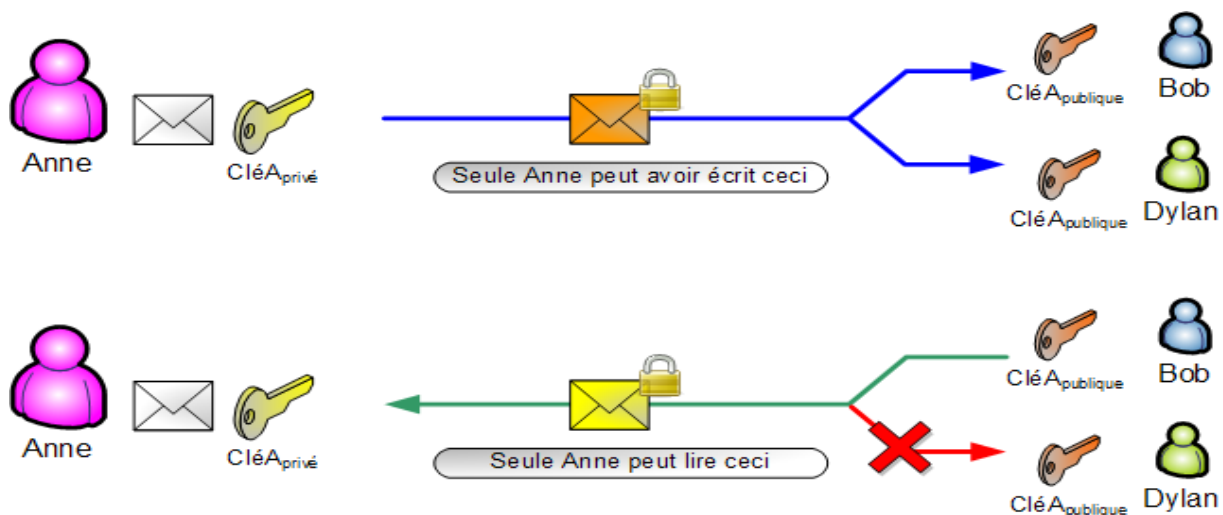
**Figure 2.1** : Illustration de chiffrement à clé Symétrique

- **Cryptographie asymétrique**

Pour résoudre le problème de l'échange de la clé secrète, un nouveau type de cryptographie a été inventé, il s'agit de la cryptographie asymétrique. Elle désigne une méthode cryptographique faisant intervenir une paire de clés asymétrique (publique, privée). Elle utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est rendue publique et distribuer librement, et la clé privée quant à elle n'est jamais distribuée et doit être gardé secrète. En pratique elle est utilisé pour :

- L'échange d'une clé symétrique.
- La signature d'un hachage d'un message.

Les trois algorithmes à clé publique suivants sont les plus fréquemment employés : RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), Diffie\_Hellman « Figure 2.2 ».



**Figure 2.2:** illustration de chiffrement à clé Asymétrique

### 3.2. Réseaux privés virtuels :

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 d'une organisation car le chemin emprunté n'est pas défini à l'avance. 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 le Réseau Privé Virtuel (noté RPV ou VPN, acronyme de Virtual Private Network) pour désigner le réseau ainsi artificiellement créé. Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données [29].

### 3.2.1. Fonctionnement d'un VPN :

Avec Le VPN, la sécurité en ligne est optimisée à plusieurs niveaux. 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 cryptée avec un algorithme de niveau Top-Secret) qui vous protège contre les pirates et les intrus qui tentent d'écouter ou d'obtenir les informations sensibles vous concernant.

Car, même si Internet est un réseau public, les VPN permettent aux ordinateurs de s'y connecter en privé. L'ordinateur étant caché derrière de nombreux serveurs VPN, personne n'est en mesure de s'immiscer dans votre connexion. La plupart des influences extérieures malveillantes comme celles des cybers pirates ou des attaques de réseau sont repoussées par les serveurs VPN en fournissant un niveau supplémentaire de sécurité numérique impénétrable qui protège vos actions en ligne.

### 3.3. Le par feu (fire wall) :

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

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

Le pare-feu a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de

confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante). Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège [30]

Le filtrage se fait selon divers critères, les plus courants :

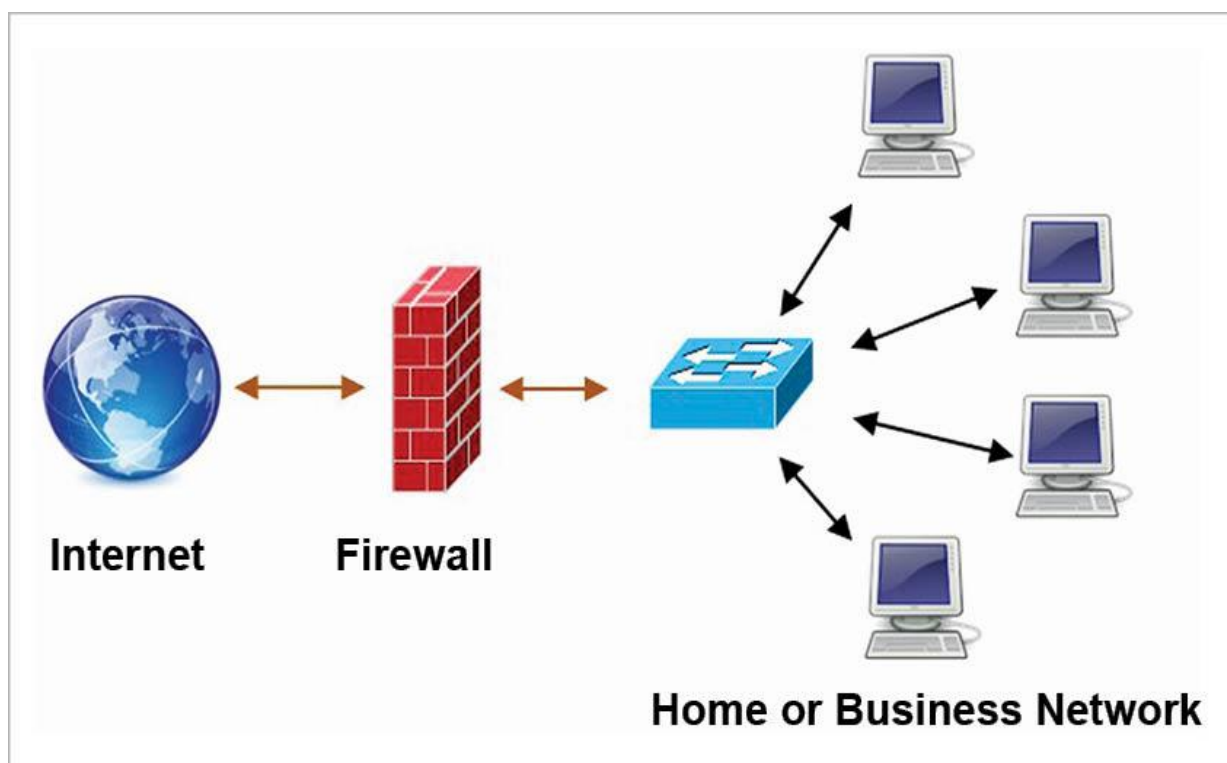
- L'origine ou la destination des paquets (adresse IP, port TCP ou UDP, interface réseau...)
- Les options contenues dans les données (fragmentation, validité)
- Les données elles-mêmes (taille, correspondance a un motif)
- Les utilisateurs pour les plus récents.

Un pare feu fait souvent office de routeur et permet d'isoler le réseau en plusieurs zones de sécurité appelées DMZ (zone démilitarisée). [31]

Le pare feu se présente essentiellement sous deux formes :

- **Logiciel** : un programme qui fonctionne dans votre ordinateur et assure le rôle de filtrage des connexions.
- **Matérielle** : un composant physique de votre réseau domestique qui inclut un logiciel pare feu. Un pare feu matérielle doit être présent dans un réseau informatique (entre un réseau public et un réseau privé).

Pare feu figure 2.3



**Figure 2.3 :** Pare feu

### 3.3.1. Principe de fonctionnement d'un pare feu :

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

- Autoriser la connexion (Allow).
- Bloquer la connexion (Deny).
- Rejeter la demande de connexion sans avertir l'émetteur (Drop) .

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

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

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

### 3.4. PfSense :

PfSense (distribution logicielle), ou « **Packet Filter Sense** » est un routeur / pare-feu open source basé sur FreeBSD. Il date de 2004 à partir d'un fork de m0n0wall par Chris Buechler et Scott Ullrich. PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur. Basé sur PF (*packet filter*), il est réputé pour sa fiabilité. Et l'installation en mode console, il s'administre ensuite simplement depuis une interface web [29].

### 3.5. La zone dématérialisé DMZ :

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

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

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

On parle ainsi de Zone démilitarisée (notée DMZ, Demilitarised Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile [27]

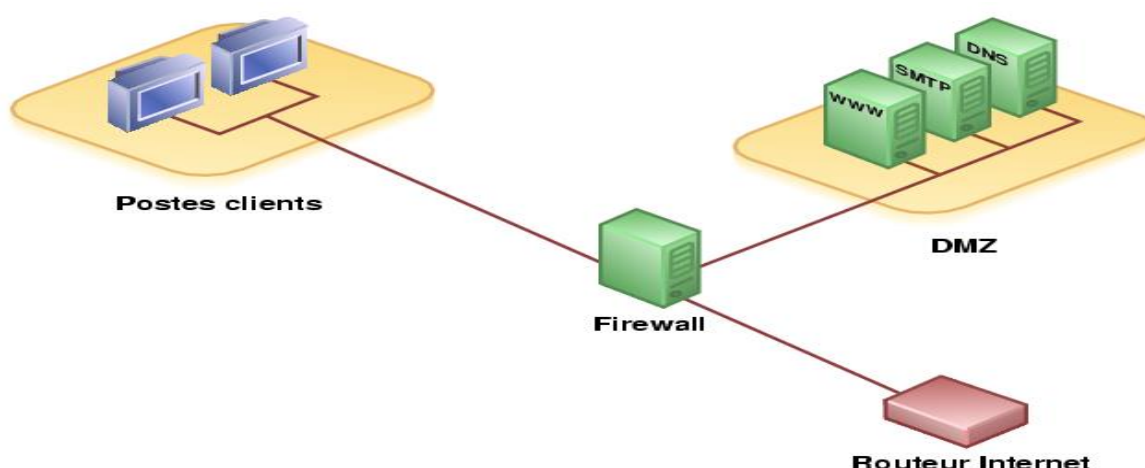


Figure 4 : zone dématérialisé DMZ

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

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

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

### 3.6. Système de détection d'intrusion :

Un système de détection d'intrusions (IDS, de l'anglais Intrusion Detection System) est un périphérique ou processus actif qui analyse l'activité du système et du réseau pour détecter toute entrée non autorisée et / ou toute activité malveillante. La manière dont un IDS détecte des anomalies peut beaucoup varier ; cependant, l'objectif principal de tout IDS est de prendre sur le fait les auteurs avant qu'ils ne puissent vraiment endommager vos ressources.

Les IDS protègent un système contre les attaques, les mauvaises utilisations et les compromis. Ils peuvent également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus. Selon les méthodes de détection que vous choisissez de déployer, il existe plusieurs avantages directs et secondaires au fait d'utiliser un IDS. [37]

Il existe deux grandes familles distinctes d'IDS :

- **Les N-IDS** (*Network Based Intrusion Detection System*) : ils assurent la sécurité au niveau du réseau.
- **Les H-IDS** (*Host Based Intrusion Detection System*) : ils assurent la sécurité au niveau des hôtes.

### 3.7. Serveurs mandataires (Proxy) :

Le serveur proxy aussi appelé serveur mandataire est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, le serveur proxy est une fonction informatique client-serveur qui a pour but de relayer des requêtes entre une fonction cliente et une fonction serveur, Dans sa forme la plus simple un serveur proxy facilite les communications entre un client et un serveur sans modifier les requêtes ou les réponses. Quand un client demande une ressource sur un serveur, le serveur proxy contourne cette requête en se présentant lui-même comme étant le client au près du serveur de destination, si une réponse est reçue, celui-ci retourne la réponse au client, donnant l'impression que la communication est directe entre le serveur et le client [26].

#### 3.7.1. Principe de fonctionnement :

- Un client envoie sa requête.
- Le proxy la récupère et la renvoie.
- Le serveur répond au proxy.
- Le proxy renvoie la réponse au client .

L'avantage du proxy est que le client devient invisible pour internet, si un client est derrière un proxy, les autres machines sur internet penseront qu'il s'agit du serveur. [38]

#### 3.7.2. Les fonctionnalités du proxy :

- **Le cache (caching) :**

Le cache c'est la capacité à garder en mémoire les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les 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).

Cette fonctionnalité implémentée dans certains serveurs proxy 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.

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.

- **Le filtrage :**

Il est possible d'assurer un suivi des connexions (*logging* ou *tracking*) via la constitution de journaux d'activité (*logs*) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet. Il est ainsi possible de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de *liste blanche*, lorsqu'il s'agit d'une liste de sites interdits on parle de *liste noire*. Enfin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés, ...) est appelé filtrage de contenu.

- **L'authentification :**

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 mis en œuvre pose bien évidemment de nombreux problèmes relatifs aux libertés individuelles et aux droits des personnes...

- **La sécurité :**

La fonction de sécurité : le serveur peut constituer une barrière entre Internet et le réseau local ou privé des entreprises.

- **La translation d'adresse (NAT) :**

Un proxy peut éventuellement remplacer un routeur et effectuer la translation d'adresse NAT (Network Address Translation). « Méthode de traduction d'adresses IP non routables en adresses routables et réciproquement, qui permet de connecter un réseau local ou privé à de nombreuses machines en n'utilisant qu'une connexion par modem câble ou ADSL ».

- **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. La translation d'adresse statique permet ainsi de connecter des machines du réseau, interne à Internet de manière transparente

➤ Translation dynamique :

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

• **Reverse Proxy :**

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

Le Reverse-Proxy sert ainsi de relais pour les utilisateurs d'Internet souhaitant accéder à un site web interne en lui transmettant indirectement les requêtes. Grâce au Reverse-Proxy, le serveur web est protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne. D'autre part, la fonction du cache du reverse-Proxy peut permettre de soulager la charge du serveur pour lequel il est prévu, c'est la raison pour laquelle un tel serveur est parfois appelé « accélérateur », (server Accelerator). Enfin, grâce à des algorithmes perfectionnés, le Reverse-Proxy peut servir à répartir la charge en redirigeant les requêtes vers différents serveurs équivalents ; on parle alors de répartition de charge, (load balancing).

#### **4. Conclusion :**

La croissance des réseaux d'information et de communication à l'échelle internationale, s'est corrélativement accompagnée d'une aggravation des risques et des menaces associées. Pour cela, nous avons donné une vue globale sur la sécurité des réseaux, où nous avons énuméré quelques attaques qui peuvent perturber et corrompre le fonctionnement du réseau, et cité quelques techniques pour atténuer ces dernières.

Le chapitre suivant, sera consacré à l'une des techniques d'atténuation d'attaque citée précédemment, qui est le proxy.



## 1. Introduction :

L'informatique est aujourd'hui un composant critique de l'entreprise, le partage de données est devenu une des tâches primordiales dans le souci de rendre tout au clair et à la portée de tous via le réseau de l'entreprise. Ce dernier est de plus en plus accessible, mais il recèle de nombreux dangers, souvent ignorés par beaucoup d'utilisateurs.

D'où on se pose les questions suivantes :

- Comment avoir un contrôle et un audit sur les contenus consultés par les utilisateurs du réseau ?
- Comment contrôler sa bande passante ?
- Comment protéger les utilisateurs des contenus malicieux ?

Dans ce chapitre, on va présenter en détail l'acheminement de notre travail, qui consiste à mettre en place un proxy Squid sous CentOS Linux.

## 2. Approche par intégration d'un serveur mandataire :

L'approche consiste à proposer une solution aux problèmes liés à l'utilisation d'internet au sein de l'entreprise, en mettant en place un proxy Squid open source qui en plus d'être puissant et rapide, est une solution gratuite. Il permet d'atteindre nos objectifs pour renforcer la sécurité de réseau LAN de l'entreprise et ce en permettant :

- L'accès des utilisateurs à Internet sera soumis à une authentification.
- L'accès à internet sera réalisé par niveaux, donc chaque groupe d'utilisateur aura un accès plus ou moins restreint.
- Un cache web : sauvegarde des pages et documents pour une utilisation ultérieure
- Intégration d'un anti-virus pour l'analyse du trafic.
- L'anonymat de l'identité de l'utilisateur.

## 3. Présentation de l'EPB :

L'entreprise portuaire de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Le port est consacré au commerce international et aux hydrocarbures. Il est classé 2<sup>ème</sup> port d'Algérie en termes d'activité commerciale et 3<sup>ème</sup> port pétrolier. Il est également le 1<sup>er</sup> port du bassin méditerranéen certifié pour les trois systèmes ISO 9001.2000 pour la qualité, ISO 14000 pour l'environnement et pour

l'hygiène, santé et sécurité au travail, et à avoir ainsi installé un système de management intégré.

#### a. Département informatique

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

Ses principales fonctions sont :

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

#### 4. Analyse du projet :

La « figure 3.1 » représente le réseau global de l'EPB, c'est un réseau redondant aux panes, avec deux fournisseurs d'accès internet Algérie Télécom et ICOSNET, il est sécurisé par deux pare-feu et une DMZ, et constitué de deux zones logistiques TEXTER et IGHIL OUBEROUAK qui sont relié au réseau globale via des tunnels VPN.

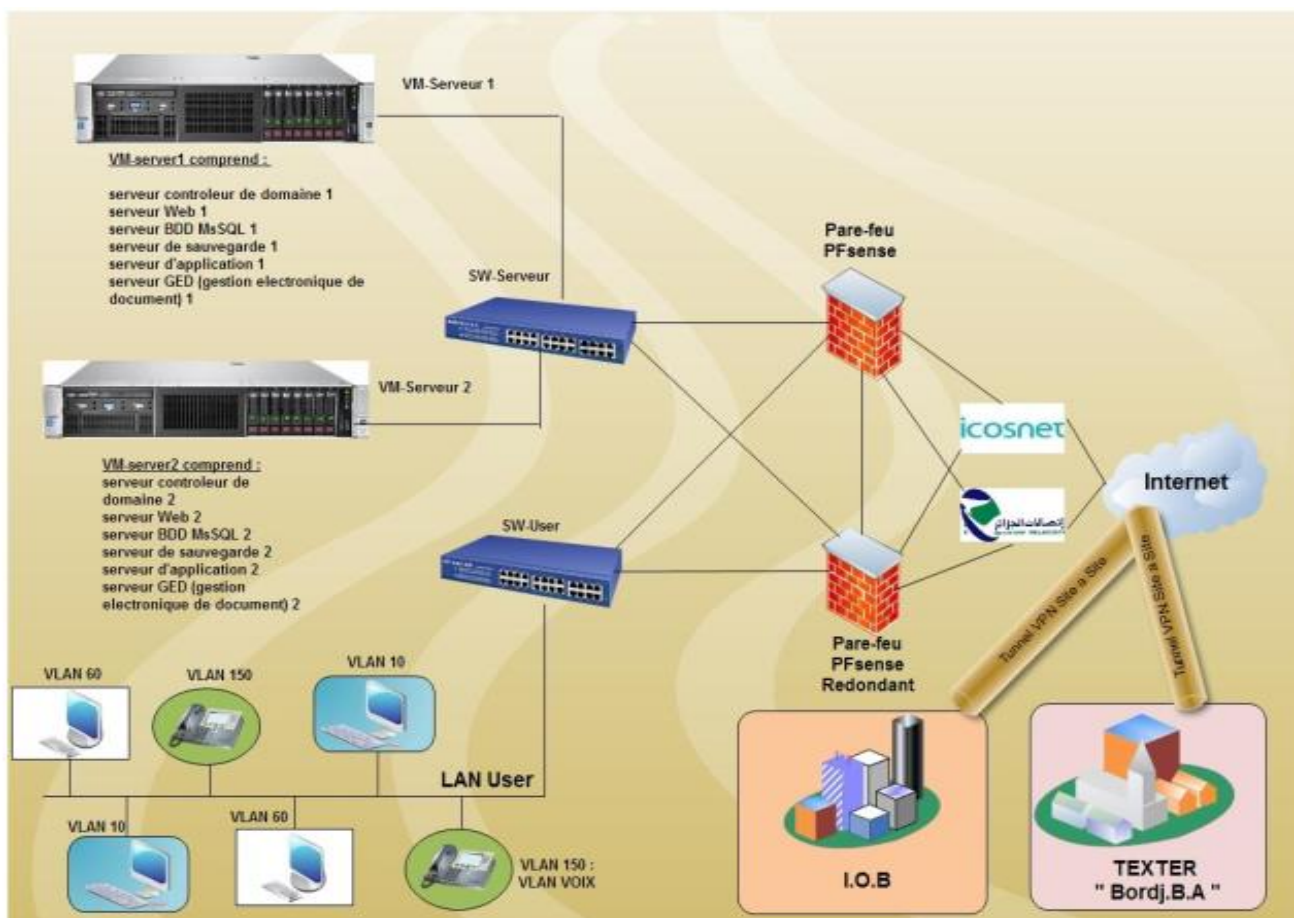
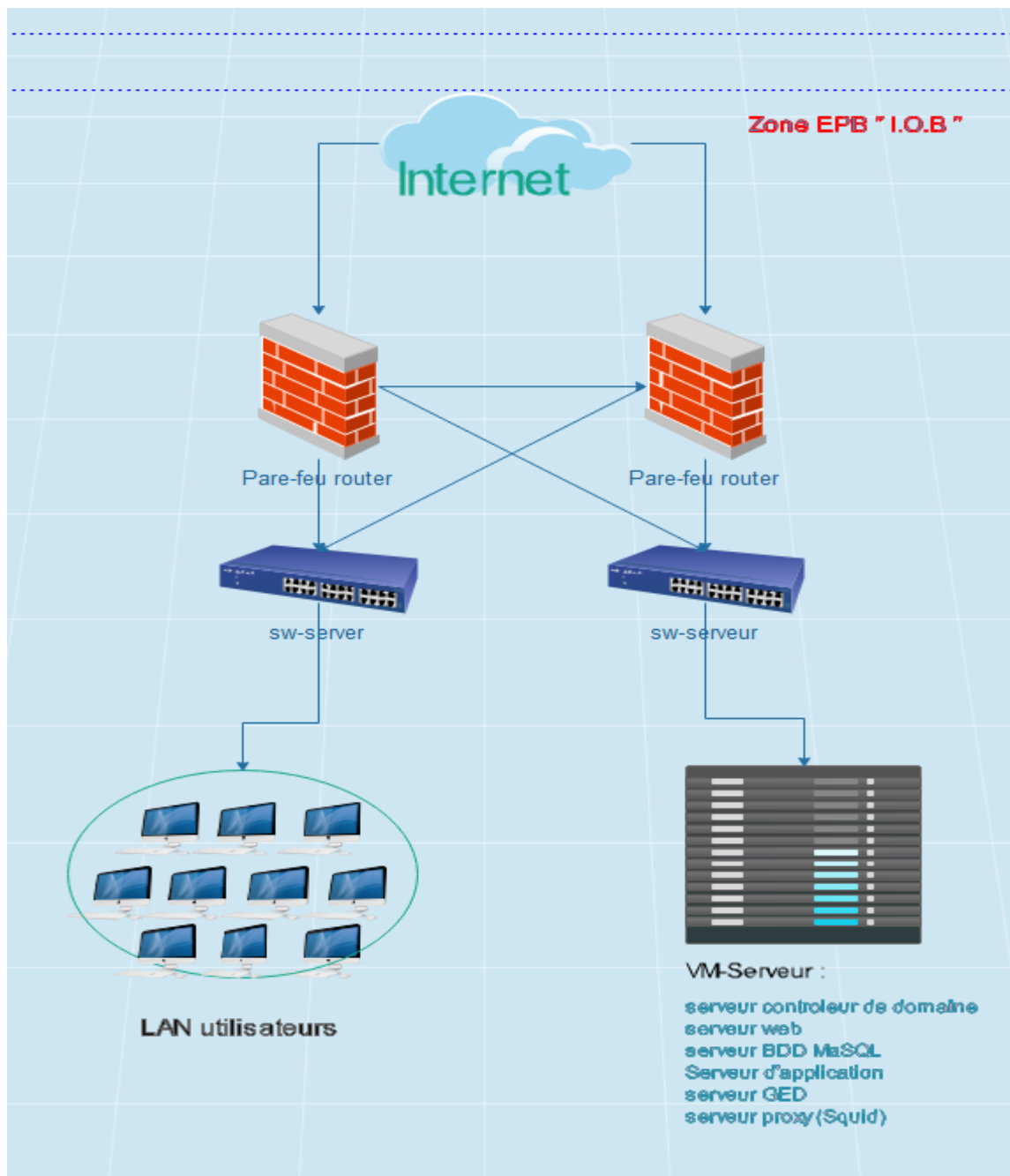


Figure 3.1 : Schéma du réseau globale EPB

La « figure 3.2 » est un segment du réseau qui est touché par notre étude (zone Ighil Ouberouak).

Le segment de ce dernier se caractérise par :

- Architecture redondante aux pannes.
- Sécurisés par deux par feu, DMZ, plus notre serveur proxy.



**Figure 3.2:** segment du réseau touché par l'étude

## 5. Ressources matérielles et logiciels :

### 5.1. Ressources matérielles :

L'entreprise Portuaire de Bejaia dispose d'un parc informatique très vaste

### 5.2. Ressources logiciels :

Pour les logiciels utilisés durant notre travail, on cite :

#### 5.2.1. Présentation de VMware Workstation:

C'est la version station de travail du logiciel. Elle 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 existant 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. [42]

#### 5.2.2. Présentation de GNS3 :

GNS3 (Graphical Network Simulation) est une solution libre disponible sous Windows, GNU/Linux et MacOS. GNS3 est un logiciel utilisé pour simuler différents périphériques virtuels et les dispositifs réels comme les routeurs, commutateurs... Il utilise Dynamips qui est un logiciel d'émulation pour simuler des périphériques virtuels. L'interface est graphique, elle est simple et agréable d'utilisation. [39]

#### 5.2.3. Présentations des systèmes d'exploitation :

- **Windows 7 professionnel :**

C'est un système d'exploitation de la société Microsoft, sorti le 22 octobre 2009 et successeur de Windows Vista. Bien que le système s'appelle Windows 7, Windows 7 possède le noyau amélioré de son prédécesseur, avec comme lourde tâche de laver l'échec commis par son aîné. [43]

- **Windows server 2016 R2 :**

C'est un système d'exploitation pour serveurs x64 de Microsoft, destiné aux serveurs d'entreprise. Il est connu aussi sous le nom Windows Server vNext .

Microsoft Windows Server est conçu pour fournir aux entreprises la plateforme la plus productive pour virtualiser des charges de travail, alimenter des applications et protéger des réseaux. Il propose une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web. Du groupe de travail au centre de données,

Windows Server 2016 propose des fonctionnalités nouvelles et extrêmement utiles, et des améliorations importantes au système d'exploitation de base. Windows Server propose une gamme de nouvelles technologies de sécurité améliorées, ce qui renforce la protection du système d'exploitation et offre une base solide pour exécuter et construire une entreprise.

#### Active directory :

Active Directory est le nom du service d'annuaire de Microsoft, Le service d'annuaire *Active Directory* est basé sur les standards TCP/IP : DNS, LDAP, Kerberos, etc.

Le service d'annuaire Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone, etc.) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, etc.

Active Directory permet de recenser toutes les informations concernant le réseau, que ce soient les utilisateurs, les machines ou les applications. Il permet à un utilisateur de retrouver et d'accéder à n'importe quelle ressource identifiée par ce service.

- **CentoS7 :**

CentOs est une distribution Linux orientée Entreprises, basée sur les sources de Red Hat Enterprise Linux, principalement destinée aux serveurs disponibles de manière libre et gratuite. Chaque version de CentOs est supportée pendant 10 ans (par des mises à jour de sécurité). Une nouvelle version de CentOs sort approximativement tous les 2 ans et chaque version de CentOs est mise à jour régulièrement (tous les 6 mois environs) afin de supporter le matériel le plus récent. Cela donne un environnement Linux sécurisé, à faible maintenance, stable, prévisible et reproductible. [40]

- **Squid :**

Squid est un serveur proxy/cache libre très connu du monde Open Source. Ce serveur est complet et propose une multitude d'options et de services qui lui ont permis d'être largement adopté par les professionnels.

Squid est un proxy de cache pour le Web prenant en charge HTTP, HTTPS, FTP et plus encore. Il fonctionne sur la plupart des systèmes d'exploitation disponibles, y compris Windows et est sous licence GNU GPL. Il existe un plugin à ce dernier, SquidGard, qui permet de filtrer les informations demandées par les clients. [41]

- **Serveur IBM x3550 :**

Le serveur IBM System x3550 Type 7978 est un serveur 1U1 monté en armoire, conçu pour le traitement de gros volumes de transactions réseau. Equipé d'un processeur à quatre cœurs ultra-performant, il convient parfaitement aux environnements réseau qui demandent des microprocesseurs extrêmement performants, une architecture d'entrée-sortie souple et une grande facilité de gestion. [45]

## 6. Installation et configuration de Cent Os7 :

- Après avoir téléchargé la dernière version de CentOS 7 disponible sur le site officiel <https://www.centos.org/download/>, (nous avons choisi la version minimale).
- On insère le CD/USB dans la machine, et on va démarrer la machine en choisissant de booter avec notre support.

### 6.1. Installation de cent OS :

- Dans le premier menu qui apparaît on choisit **Test This media & Install CentOS**

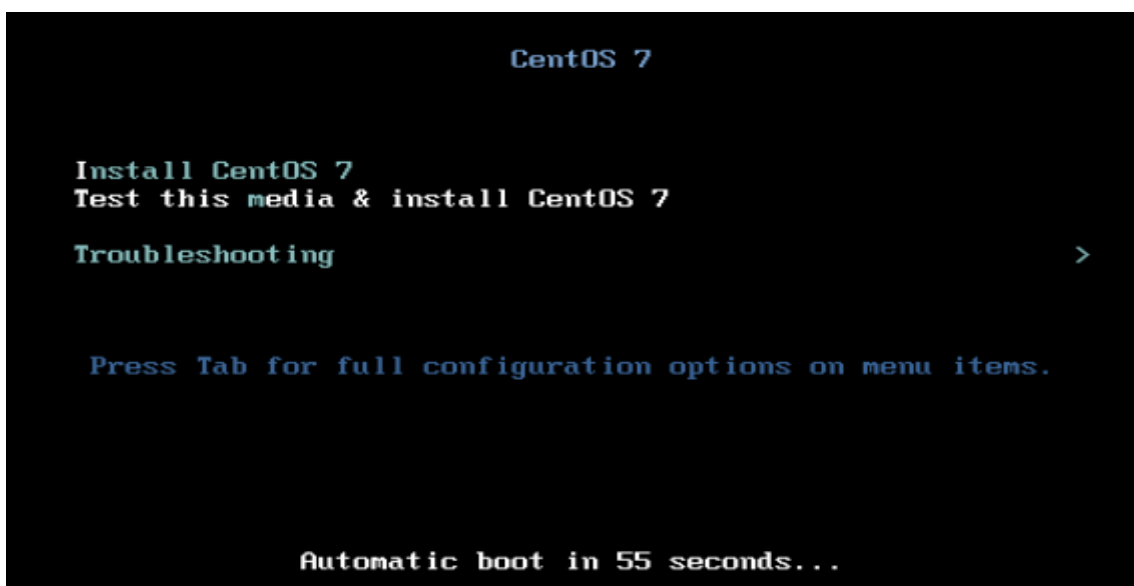


Figure 3.3 : Menu boot de l'installation

- Ensuite on confirme la vérification et l'installation en appuyant sur **ENTRER**

```

- Press the <ENTER> key to begin the installation process.

[ OK ] Started Show Plymouth Boot Screen.
[ OK ] Reached target Paths.
[ OK ] Reached target Basic System.
[ OK ] Started Device-Mapper Multipath Device Controller.
      Starting Open-iSCSI...
[ OK ] Started Open-iSCSI.
      Starting dracut initqueue hook...
[ 7.392865] sd 0:0:0:0: [sdal] Assuming drive cache: write through
[ 10.566617] dracut-initqueue[549]: mount: /dev/sr0 is write-protected, mounting read-only
[ OK ] Started Show Plymouth Boot Screen.
[ OK ] Reached target Paths.
[ OK ] Reached target Basic System.
[ OK ] Started Device-Mapper Multipath Device Controller.
      Starting Open-iSCSI...
[ OK ] Started Open-iSCSI.
      Starting dracut initqueue hook...
[ 10.566617] dracut-initqueue[549]: mount: /dev/sr0 is write-protected, mounting read-only
[ OK ] Created slice system-checkisomd5.slice.
      Starting Media check on /dev/sr0...
/dev/sr0: bf13079b8b04c488db62d43f0c3446a0
Fragment sums: 8df27d8348bd51a48df53351faafa2dafd639fc9b5eddc896684e747e3e8
Fragment count: 20
Press [Esc] to abort check.
Checking: 006.1%_

```

Figure 3.4 : écran d'installation

- Une interface graphique va apparaître, nous commençons par choisir la langue (pour notre cas on a choisie Français) et on clique sur le bouton **continuer**.



Figure 3.5 : Menu de choix de langue

- Dans le menu principal de l'installation nous choisissons l'emplacement de l'installation dans le menu **DESTINATION DE L'INSTALLATION**.

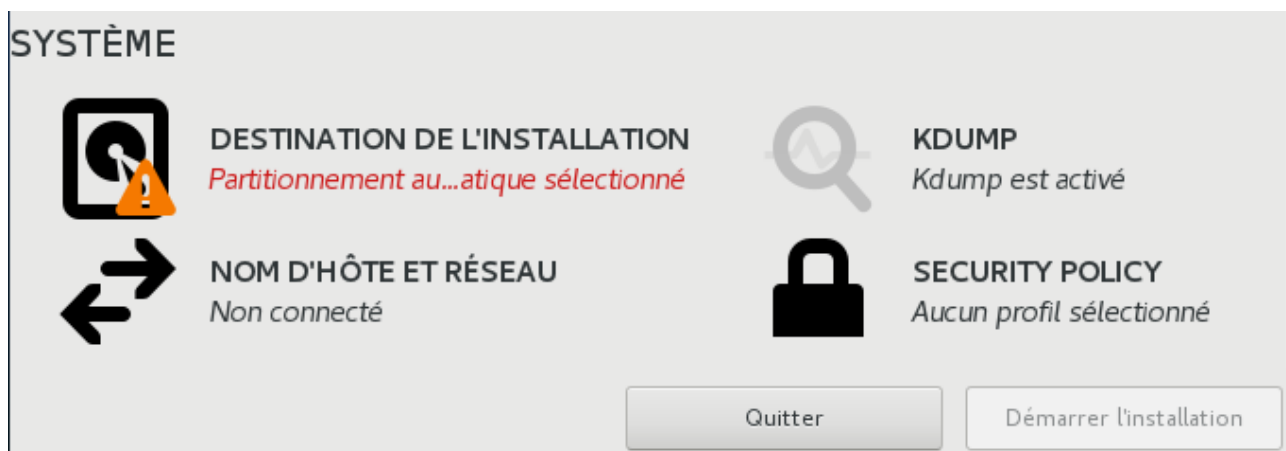


Figure 3.6 : Menu de répertoire d'installation

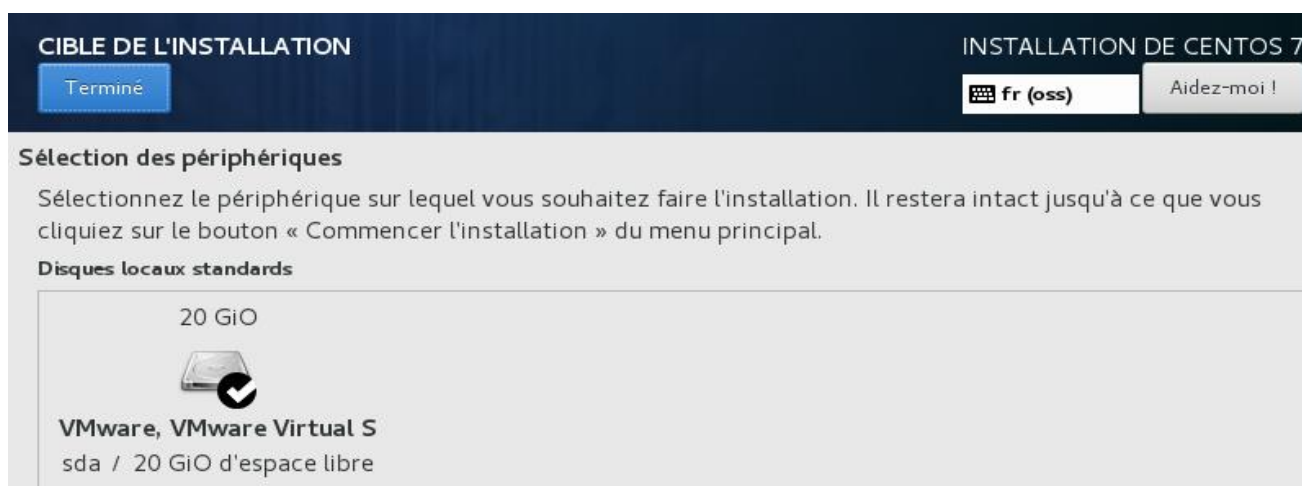


Figure 3.7 : choix de la destination

- Après avoir choisi la destination et confirmer avec le bouton **Terminé**, nous revenons au menu principal et on clique sur **Démarrer l'installation** (pour le reste des paramètres définis par défaut conviennent à notre installation) et un écran de chargement apparaîtra où nous pourrons définir le mot de passe de l'utilisateur **root** et créer éventuellement d'autres utilisateurs si on le souhaite.



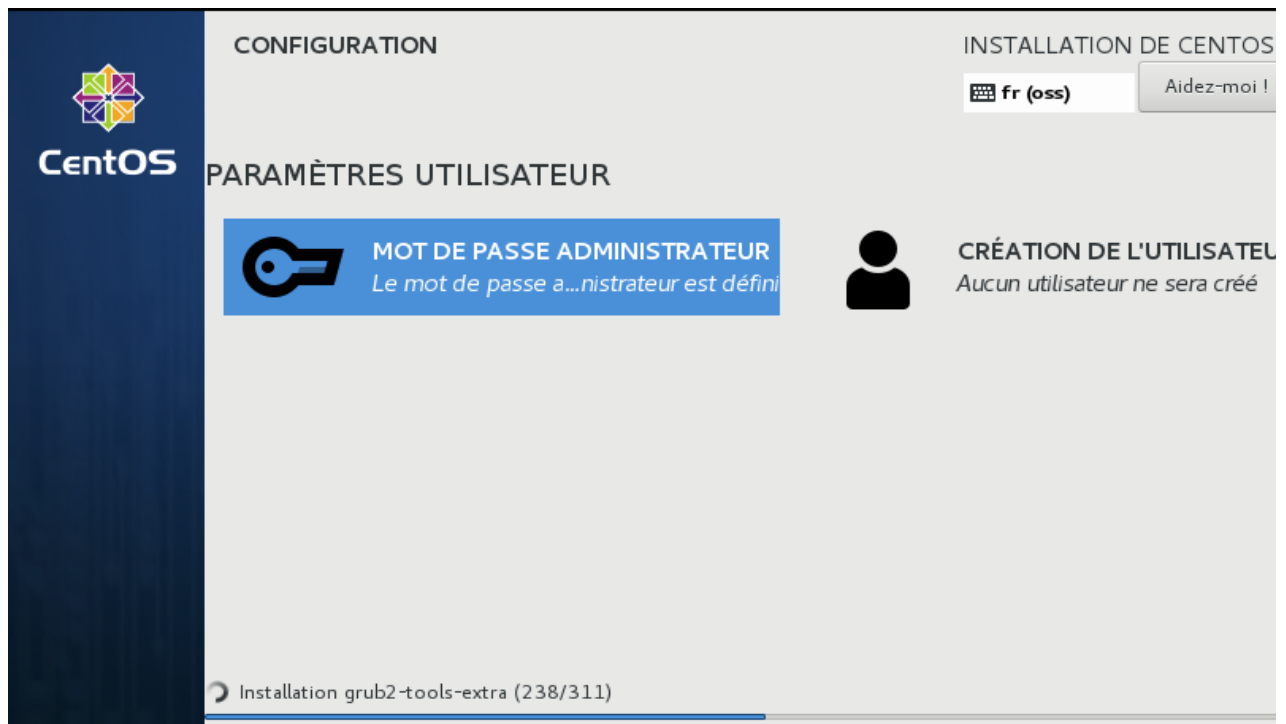


Figure 3.8 : Ecran d'installation

- En mode console, nous utilisons une interface graphique pour paramétrer notre carte réseau, avec la commande suivante :

```
[root@epb ~]# nmtui_
```

Figure 3.9 : commande pour paramétrer la carte réseau

- Dans un premier temps on doit sélectionner **Activer une connexion** pour activer la carte réseau.
  - Dans ces menus, on se déplace avec les flèches et la touche tabulation.

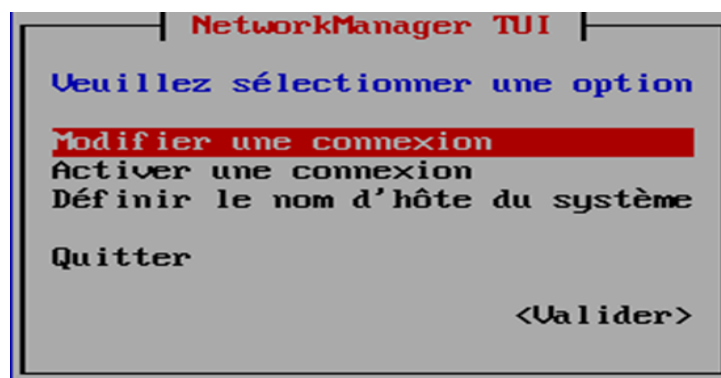


Figure 3.10 : Menu de paramétrage réseau

- Puis on sélectionne l'interface réseau **ens33** et on clique sur **Activer**



Figure 3.11 : activation de la carte réseau

- Pour configurer les paramètres de la connexion, on relance l'utilitaire **nmtui** et on sélectionne **Modifier une connexion**, on va sélectionner la carte et on clique sur **Modifier**.

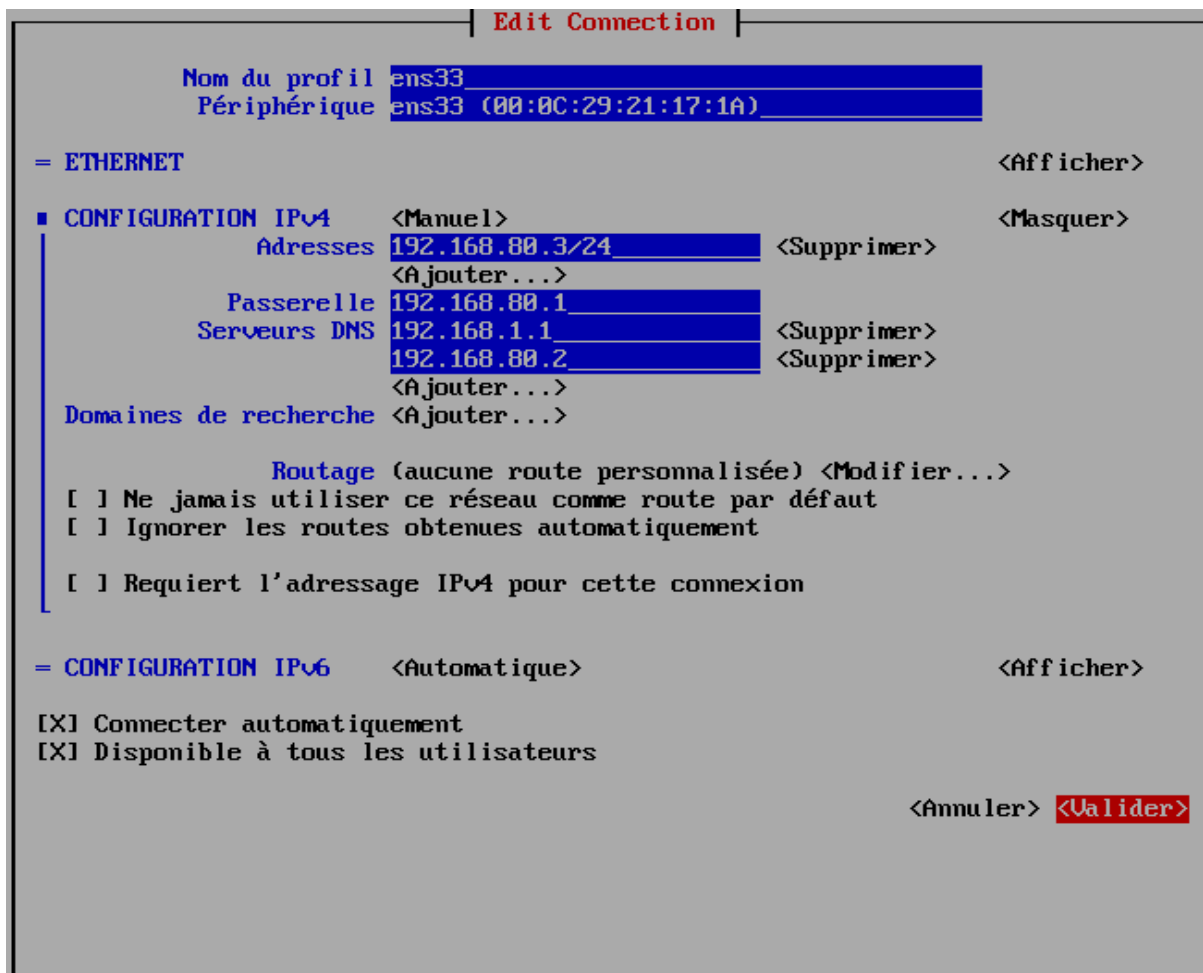


Figure 3.12 : configuration de la carte réseau

- On affecte les paramètres indiqués en dessus et on clique sur **Valider** puis **Quitter**  
Et on redémarre le service réseau en utilisant la commande :

```
#systemctl restart network
```

- on vérifie l'état de l'interface réseau configuré :

```
[root@epb ~]# nmcli d
PÉRIPHÉRIQUE  TYPE      ÉTAT      CONNEXION
ens33         ethernet  connecté  ens33
lo            loopback  non-géré  --
[root@epb ~]# _
```

Figure 3.13 : vérification des configurations

- ensuite, nous introduisons la commande **yum list updates** pour télécharger la liste de tous les composants qui seront mis à jour.

```
[root@epb ~]# yum list updat
Modules complémentaires chargés : fastestmirror
Determining fastest mirrors
```

Figure 3.14 : commande pour télécharger la liste des composants

- Et on lance la mise à jour du système CentOS :

```
[root@epb ~]# yum update -y
```

Figure 3.15 : commande pour mettre à jour du système

- A la fin de l'installation des mises à jour on redémarre le système :

```
[root@epb ~]# reboot
```

Figure 3.16: commande pour redémarrer le système

## 7. Installation et configuration du serveur Squid :

- On procède au téléchargement et l'installation de Squid proxy

```
[root@epb ~]# yum install squid
Modules complémentaires chargés : fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.mirror.iweb.ca
 * extras: centos.mirror.iweb.ca
 * updates: centos.mirror.iweb.ca
base                               | 3.6 kB | 00:00:00
extras                             | 3.4 kB | 00:00:00
updates                             | 3.4 kB | 00:00:00
(1/2): extras/7/x86_64/primary_db   | 143 kB | 00:00:26
(2/2): updates/7/x86_64/primary_db 71% [=====] | 54 kB/s | 1.0 MB | 00:00:07 ETA
```

Figure 3.17 : installation de Squid

### 7.1. Fichier et répertoire Squid :

Nous aborderons ici les principaux fichiers et répertoire relatif à Squid que nous serons amenés à utiliser dans la suite de notre travail :

- `/sbin/squid` : est le programme Squid en question, que nous exécuterons parfois avec des options (`-k -z ...etc`).
- `/etc/squid.conf` est le fichier de configuration de serveur squid.
- `/etc/squid.conf.default` une copie du fichier `squid.conf` (configuration par défaut).
- `/etc/squid.conf.documented` est une documentation complète sur le fichier `squid.conf` et ses multiples syntaxes.
- `/libexec/` répertoire contenant les programmes d'aide comme le `cachemgr.cgi`.
- `./libexec/cachemgr.cgi` programme offrant une interface web pour le monitoring du serveur Squid.

### 7.2. Paramètres à mettre en place au niveau d'Active Directory :

Nous commençons par créer une unité d'organisation pour les utilisateurs de Squid server, on va taper `dsa.msc` dans la barre de recherche du menu **Démarrer** puis **Entrer**.

- **Utilisateurs et ordinateurs Active Directory** s'ouvre. Clic droit sur le domaine `epb.loc` ensuite **Nouveau**, puis sur **Unité d'organisation**.

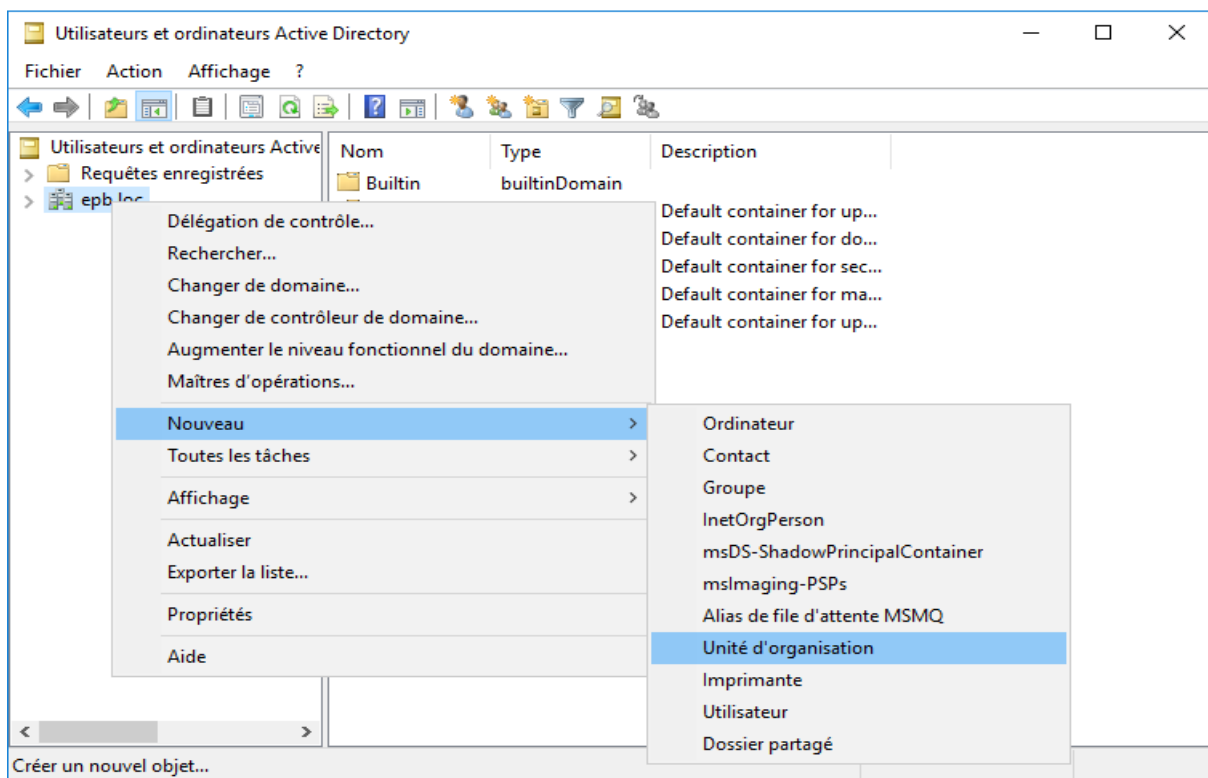


Figure 3.18 : Création d'une nouvelle unité d'organisation (1)

- une fenêtre apparaît on choisit le nom de l'unité d'organisation et on clique sur **OK**

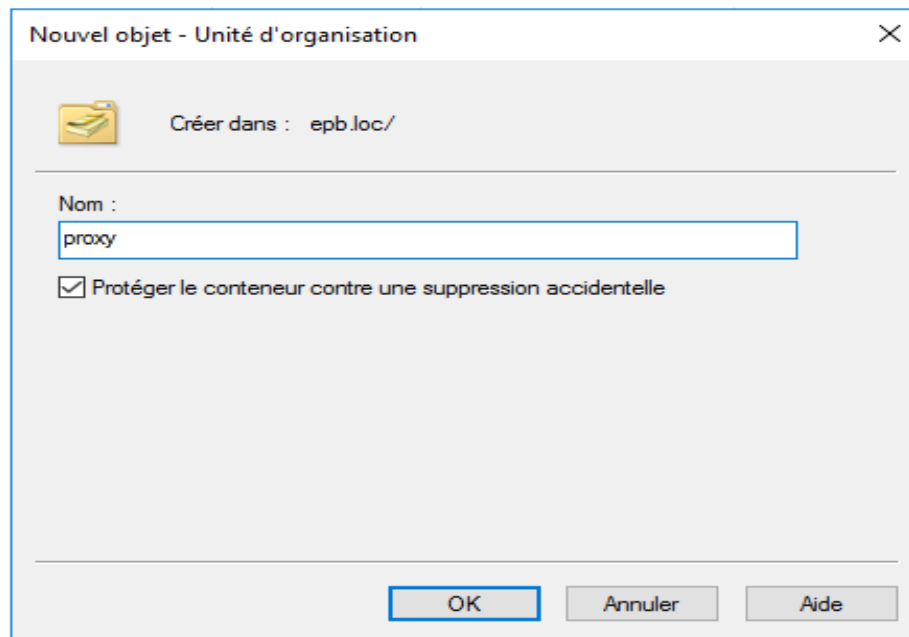


Figure 3.19 : Création d'une nouvelle unité d'organisation (2)

- on procède à la création des groupes d'utilisateurs qui vont nous servir à catégoriser les utilisateurs selon leurs droits d'accès à internet. Nous allons créer 3 groupes (groupe1, groupe2 et groupe3), pour cela on fait clic droit sur l'UO (**proxy**) > **Nouveau** > **Groupe** :

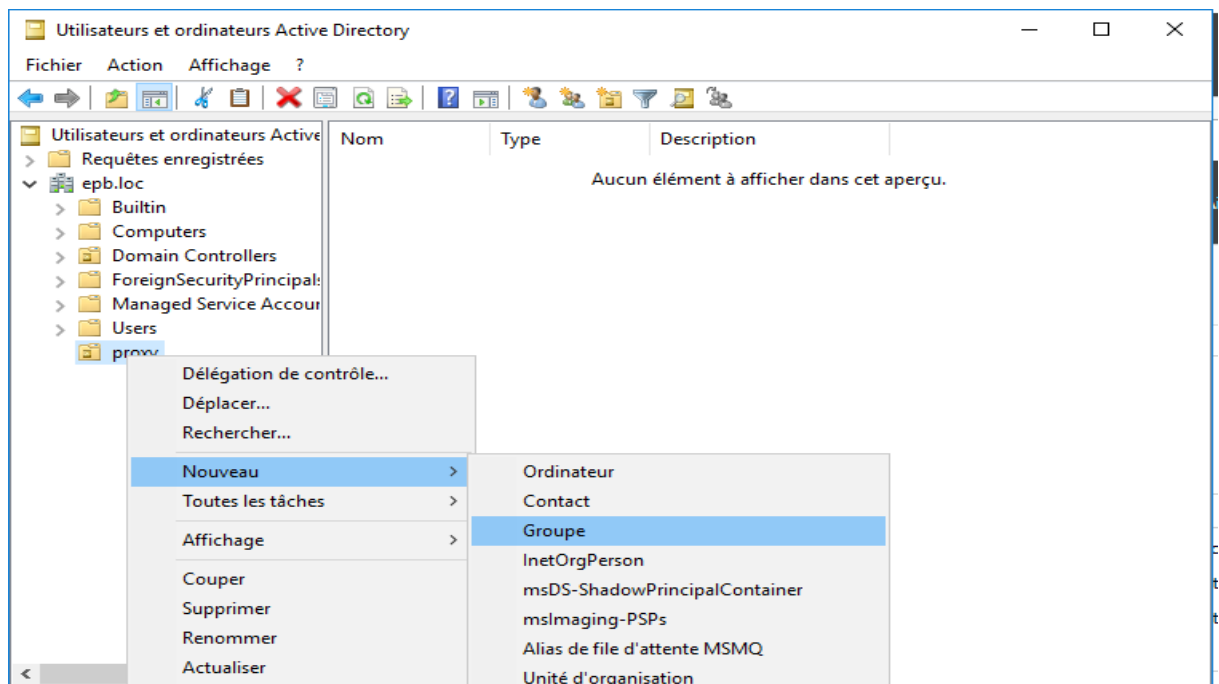
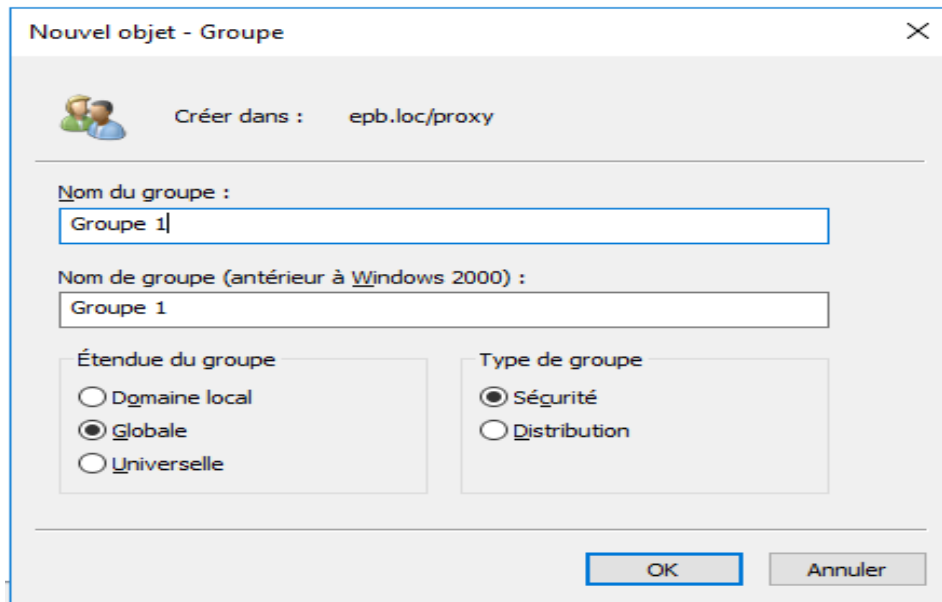


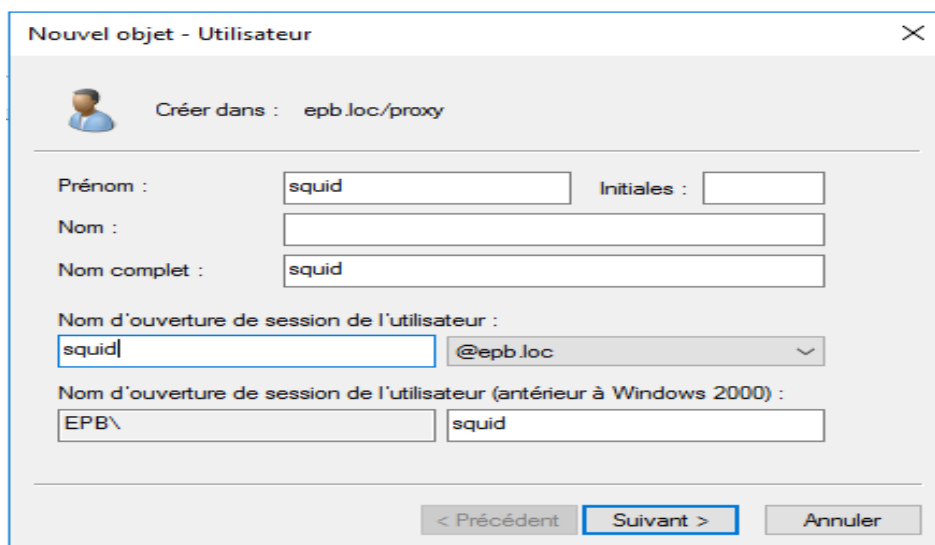
Figure 3.20 : Création d'un groupe d'utilisateur (1)

- On nomme le groupe et on clique **OK** en gardant les paramètres par défaut.



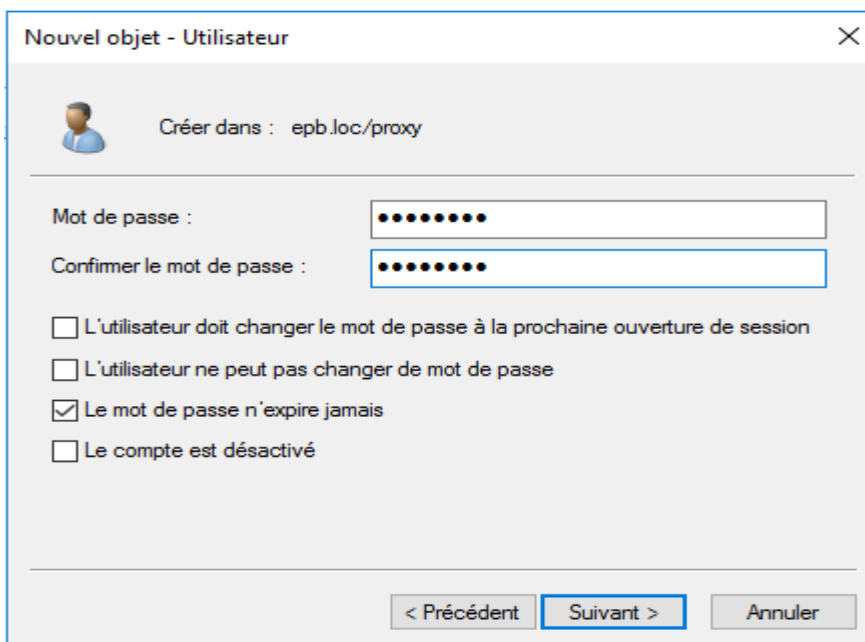
**Figure 3.21** : Création d'un groupe d'utilisateur (2)

- Et on répète les mêmes instructions pour la création du Groupe 2 et Groupe3.
- On crée l'utilisateur **Squid** auquel on va léguer des privilèges pour pouvoir authentifier et définir l'appartenance des utilisateurs :
  - 1) Clic droit sur **l'unité d'organisation**
  - 2) **Nouveau**, puis on clique sur **Utilisateur**.
  - 3) Dans **Prénom**, on tape le prénom de l'utilisateur.
  - 4) Dans **Initiales**, on tape les initiales de l'utilisateur.
  - 5) On modifie le **Nom complet** pour ajouter des initiales.
  - 6) Dans **Nom d'ouverture de session de l'utilisateur**, on tape le nom d'ouverture de session de l'utilisateur, on clique sur **Suivant**



**Figure 3.22** : Création d'un nouvel utilisateur (1)

- Dans **Nouvel objet - Utilisateur**, **Mot de passe** et **Confirmer le mot de passe**, on tape, le mot de passe de l'utilisateur, puis on sélectionne les options de mot de passe appropriées.



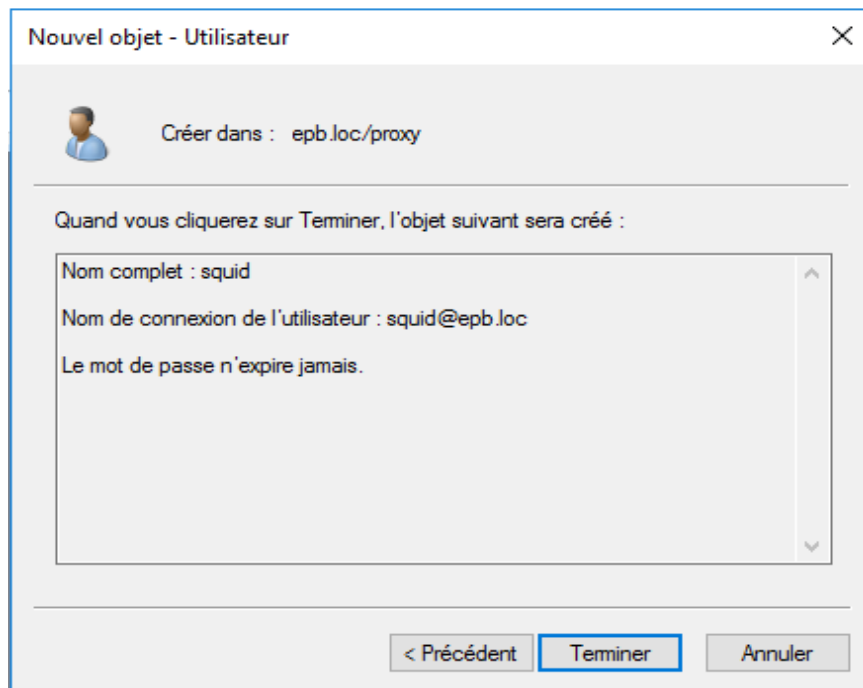
The screenshot shows a dialog box titled "Nouvel objet - Utilisateur" with a close button (X) in the top right corner. Below the title bar, there is a user icon and the text "Créer dans : epb.loc/proxy". The main area contains two password input fields: "Mot de passe :" and "Confirmer le mot de passe :", both filled with ten black dots. Below these fields are four checkboxes:

- L'utilisateur doit changer le mot de passe à la prochaine ouverture de session
- L'utilisateur ne peut pas changer de mot de passe
- Le mot de passe n'expire jamais
- Le compte est désactivé

At the bottom, there are three buttons: "< Précédent", "Suivant >" (highlighted with a blue border), and "Annuler".

Figure 3.23 : Création d'un nouvel utilisateur (2)

- On clique sur **Suivant** pour passer en revue les paramètres du nouveau compte d'utilisateur, puis on clique sur **Terminer**.



The screenshot shows the same dialog box "Nouvel objet - Utilisateur" with a close button (X) in the top right corner. Below the title bar, there is a user icon and the text "Créer dans : epb.loc/proxy". The main area contains the text "Quand vous cliquerez sur Terminer, l'objet suivant sera créé :" followed by a scrollable text box containing:

- Nom complet : squid
- Nom de connexion de l'utilisateur : squid@epb.loc
- Le mot de passe n'expire jamais.

At the bottom, there are three buttons: "< Précédent", "Terminer" (highlighted with a blue border), and "Annuler".

Figure 3.24 : Création d'un nouvel utilisateur (3)

- Maintenant on délègue les droit d'accès à cet utilisateur, on fait un clic droit sur l'OU **proxy**, et on clique sur **Délégation de contrôle**.

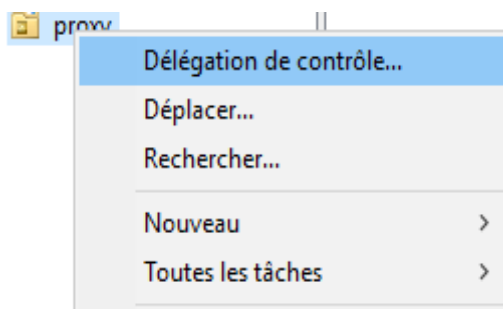


Figure 3.25 : délégation de contrôle à l'utilisateur squid

- On clique sur **Suivant**, dans la fenêtre qui suit on clique sur **ajouter** pour ajouter notre utilisateur « squid ».

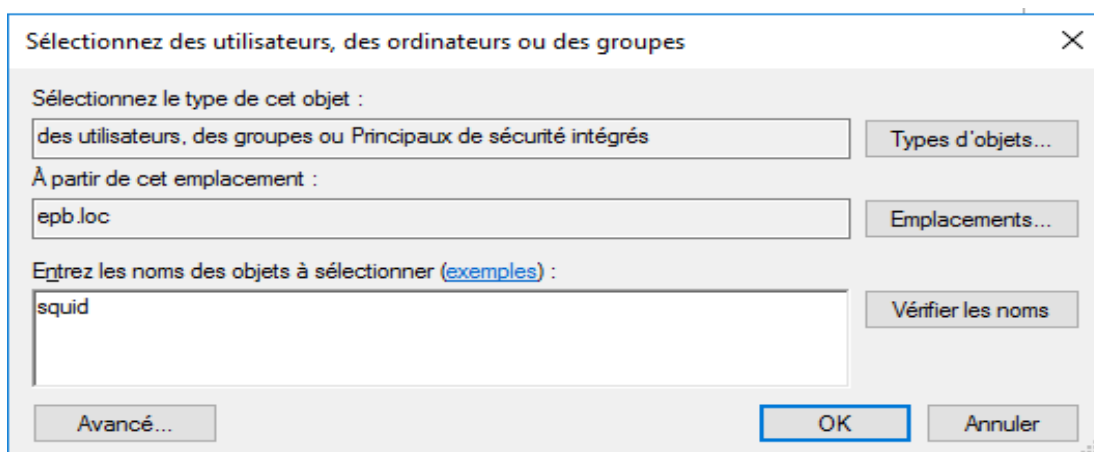
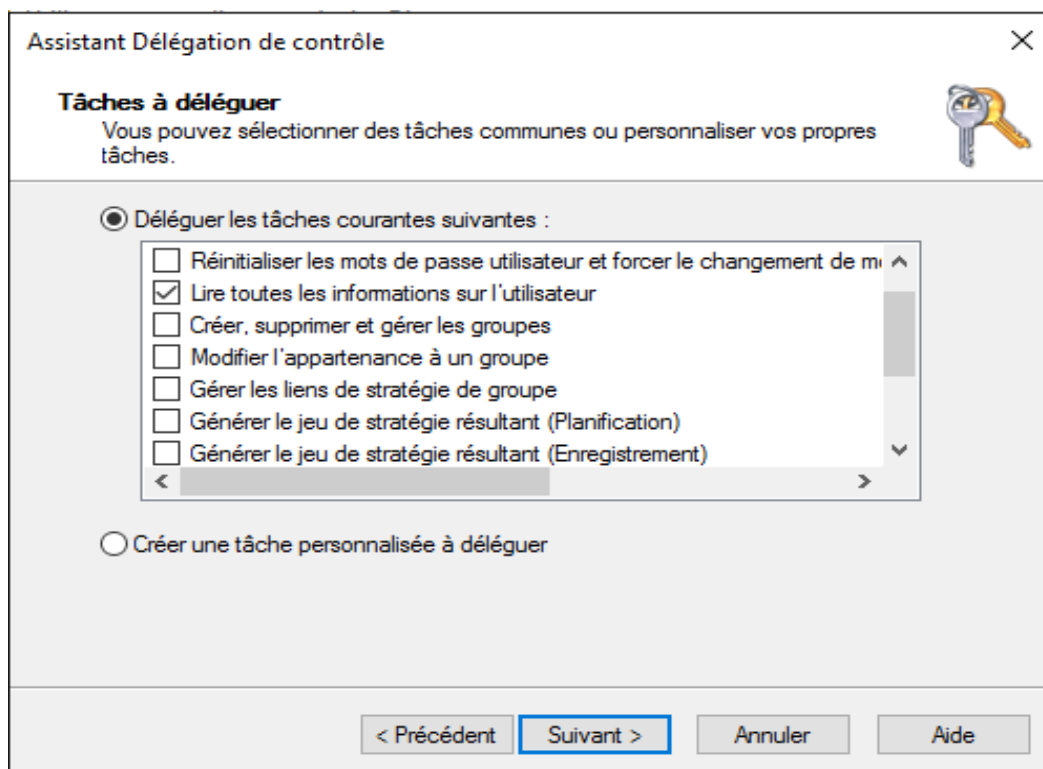


Figure 3.26 : sélection de l'utilisateur Squid

- On finit par confirmer en cliquant sur **OK** puis **Suivant**
- Et on coche les deux cases :
  - Lire toutes les informations sur l'utilisateur.
  - Lire toute les informations sur : InetOrgPerson

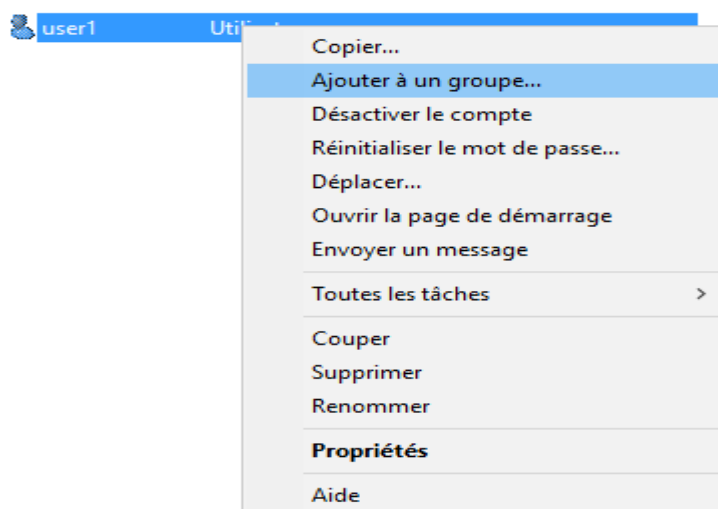
Comme la « figure 3.27 »





**Figure 3.27** : sélection des rôles à déléguer

- Et on finit par cliquer sur **Suivant** puis **Terminer**.
- Enfin on ajoute les utilisateurs aux groupes selon leurs droits d'accès (Cette étape pourra être laissée pour la fin de la mise en place, mais dans notre cas nous avons créé trois utilisateurs (user1, user2, user3) que nous mettrons respectivement dans Groupe1, Groupe2 et Groupe3).  
Pour cela, un clic droit sur l'**utilisateur** puis **ajouter au groupe**.



**Figure 3.28** : Ajout de l'utilisateur au Groupe1 (1)

- On sélectionne le groupe auquel on souhaite l'ajouter « figure 3.29 ».

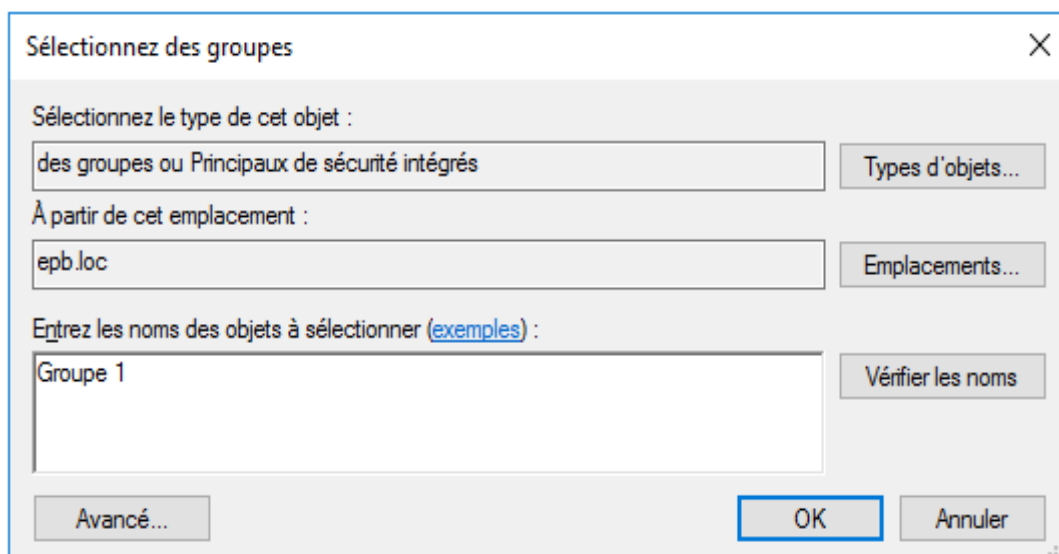


Figure 3.29 : Ajout de l'utilisateur au Groupe1 (2)

### 7.3. Configuration du serveur Squid :

- On commence par tester la connectivité vers le Windows Server :

```

[root@epb ~]# ping epb.loc
PING epb.loc (192.168.80.2) 56(84) bytes of data:
64 bytes from server2012.epb.loc (192.168.80.2): icmp_seq=1 ttl=128 time=0.444 ms
64 bytes from server2012.epb.loc (192.168.80.2): icmp_seq=2 ttl=128 time=0.405 ms
64 bytes from server2012.epb.loc (192.168.80.2): icmp_seq=3 ttl=128 time=0.362 ms

```

Figure 3.30 : vérification de la connectivité vers Windows Server

```

C:\Users\Administrateur>ping 192.168.80.3

Envoi d'une requête 'Ping' 192.168.80.3 avec 32 octets de données :
Réponse de 192.168.80.3 : octets=32 temps<1ms TTL=64
Réponse de 192.168.80.3 : octets=32 temps<1ms TTL=64
Réponse de 192.168.80.3 : octets=32 temps<1ms TTL=64
Réponse de 192.168.80.3 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.80.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

```

Figure 3.31 : vérification de la connectivité vers Squid

### 7.4.Les Helpers :

Pour communiquer avec des protocoles étrangers à Squid, il existe ce qu'on appelle des Helpers qui sont des scripts écrits dans différents langages (PHP, Python, C .. etc.) et qui servent dans notre cas à authentifier les utilisateurs et définir les groupes auxquels ils appartiennent dans une OU définie, et ces deux Helpers sont `basic_ldap_auth` et `ext_ldap_group_acl` et avant de les intégrer au fichier de configuration `squid.conf` on commence par tester leur bon fonctionnement avec les deux commandes suivantes :

#### a. Basic\_ldap\_auth :

```
[root@epb ~]# echo "user1 *Alpha*" : /usr/lib64/squid/basic_ldap_auth -R -b "dc=epb,dc=loc" -D "cn=squid,ou=proxy,dc=epb,dc=loc" -w "*Alpha*" -f "sAMAccountName=%s" -h 192.168.88.2
```

The image shows a terminal window with a command being executed. Six green arrows point to specific parts of the command: arrow 1 points to the user and password, arrow 2 points to the helper path, arrow 3 points to the domain name, arrow 4 points to the user and organization unit, arrow 5 points to the authentication command, and arrow 6 points to the server IP address.

Figure 3.32 : command test pour le `basic_ldap_auth`

1. On indique le nom d'utilisateur et son mot de passe.
2. On indique l'emplacement du Helper auquel on veut faire appel.
3. On indique le nom de domaine dans lequel on veut faire l'authentification (dc = Domain control).
4. On indique le nom de l'utilisateur (cn = Canonical Name), l'unité d'organisation auquel il appartient (OU = Organisation Unit), et le nom de domaine (dc), ensuite avec l'option `-w` on indique son mot de passe.
5. Commande pour l'authentification.
6. L'adresse du serveur AD.

On valide la commande avec la touche **Entrer** et on attend une réponse, si la réponse est **OK** ça voudrait dire que l'utilisateur Squid a réussi à authentifier l'utilisateur `user1`, si la réponse est **ERR SUCCESS** ça voudrait dire que les informations sur l'utilisateur sont erronée, et si la réponse est **ERR** cela peut être due à de diverses raisons : pour avoir des détails sur l'erreur on ajoute `-d` (debugmod) à la commande.

## b. Ext\_ldap\_group\_acl :

```
[root@epb ~]# echo "user1 groupe1" | /usr/lib64/squid/ext_ldap_group_acl -R -b "dc=epb,dc=loc" -D "cn=squid,ou=proxy,dc=epb,dc=loc" -w "*Alpha*" -f "(&(objectclass=person)(cn=%v) (memberof=cn=%a,ou=proxy,dc=epb,dc=loc))" -h 192.168.88.2
OK
```

Figure 3.33 : command test pour l'ext\_ldap\_group\_acl

1. On indique le nom de l'utilisateur à authentifier et son groupe.
5. la commande pour vérifier l'appartenance de l'utilisateur au groupe indiqué.
- Pour les parties 2/3/4/6 c'est la même chose que pour le premier Helper.

Une fois que les deux commandes répondent positivement nous passons au fichier de configuration squid.conf.

## 7.5.Le fichier Squid.conf :

Pour ouvrir le fichier de configuration et pouvoir le modifier, on doit utiliser un éditeur de texte, par default on utilisera **vi**, qui est une version de la distribution Unix, il est présent d'office sur la majorité des systèmes Unix actuels.

On ouvre le fichier de configuration squid.conf avec la commande suivante :

```
[root@epb]# vi /etc/squid/squid.conf
```

Le fichier « squid.conf » contient des réglages par défaut et certains paramètres sont proposés en commentaire :

- **Les ACL (Access Control List) :**

Pour contrôler tout ce qui passe par le serveur proxy, on utilise ce qu'on appelle les ACL (**Access Control List**). Les ACL sont des règles que le serveur applique. Cela permet par exemple d'autoriser ou d'interdire certaines transactions. On peut autoriser ou interdire en fonction du domaine, du protocole, de l'adresse IP, de numéro de port, d'un mot, on peut

aussi limiter sur des plages horaires. Les ACL ne fonctionnent pas d'elles-mêmes, elles ont besoin de 'http Access' autorisant ou interdisant ces ACL.

❖ Exemple :

- Dans cette exemple l'ACL sert à définir une plage d'adresse et à la nommer (service-réseaux est le nom de la plage d'adresse 172.16.0.0/12)
- Dans la deuxième ligne nous autorisant **service\_réseau** d'accéder à internet.

```
acl service_réseaux src 172.16.0.0/12
http_access allow service_réseaux
```

Figure 3.34 : Exemple d'ACL (1)

Les ACL peuvent se combiner pour répondre à des exigences plus complexes.

❖ Exemple :

Avec la deuxième ACL définissant le nom du domaine facebook.com, dans la troisième ligne, on autorise la plage d'adresse portant le nom de **service\_réseaux** à accéder à internet sauf au nom de domaine facebook.com « figure 3.35 »

```
acl service_réseaux src 172.16.0.0/12
acl fb url-regex -i facebook.com
http_access allow service_réseaux !fb
```

Figure 3.35 : Exemple d'ACL (2)

On trouve aussi dans le fichier de configuration squid.conf une liste d'acl pour les différents ports d'accès.

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443       # https
acl Safe_ports port 70        # gopher
acl Safe_ports port 210       # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280       # http-mgmt
acl Safe_ports port 488       # gss-http
acl Safe_ports port 591       # filemaker
acl Safe_ports port 777       # multiling http
```

Figure 3.36 : Les ACL relatif au port de communication

- Par défaut aussi les seuls ports autorisés sont sécurisés (HTTPS et SSL)

```
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
```

**Figure 3.37** : Port Ouvert/Fermé par défaut

- D'autres autorisations sont disponibles par défaut :
- Pour le cachemgr (module à mettre en place pour le monitoring via un navigateur)  
Par défaut l'accès est réservé au localhost, c'est-à-dire qu'on peut y accéder à travers la machine hébergeant le serveur seulement.

```
# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
```

**Figure 3.38** : autorisation par défaut (1)

- L'accès à internet est autorisé au serveur et aux machines sous le réseau local

```
http_access allow localnet
http_access allow localhost
```

**Figure 3.39** : autorisation par défaut (2)

- Et enfin une règle interdisant l'accès à toutes les machines (allow étant prioritaire sur le deny), ce qui va faire que l'accès à internet sera interdit à toutes les machines sauf celles qui y sont autorisées.

```
http_access deny all
```

**Figure 3.40** : autorisation par défaut (3)

- **Paramètre du cache :**

Sous les paramètres définissant les règles d'accès on trouve les paramètres relatifs au serveur proxy et son cache.

a. Le port http :

- Dans sa forme la plus simple, on indique le port que le serveur proxy va écouter.

```
# Squid normally listens to port 3128
http_port 3128
```

**Figure 3.41** : le port du serveur proxy

b. Le port ICP :

- Conserver le port 3130. Ceci permet de communiquer avec des proxy-cache parents ou voisins.

c. Cache-mem :

\_ Correspond au cache mémoire, la valeur dépend du système. Par défaut squid utilise 8 Mo. Cette taille doit être la plus grande possible

Squid offre la possibilité de contrôler les objets que nous voulons garder en mémoire cache pour optimiser les performances, avec la commande :

*memory\_cache\_mode*

- On peut définir la manière dont Squid server va utiliser l'espace cache disponible en mémoire, et dans notre cas nous garderons le paramètre par défaut qui est le suivant :

*memory\_cache\_modealways*

d. définition des limites des remplacements des objets :

- avec cache\_mem il faut régler cache\_mem\_low et cache\_mem\_high qui sont des valeurs limite de remplissage du cache mémoire. Par défaut les valeurs sont 75 % et 90 %. Lorsque la valeur de 90 % est atteinte le cache mémoire se vide jusqu'à 75 %. Les valeurs par défaut sont correctes dans la plupart des cas.

Dans notre étude nous utiliserons ces deux directives avec les valeurs suivantes :

**cache\_swap\_low 91**

**cache\_swap\_high 92**

## e. Spécifier l'espace cache dans la RAM :

- Il est important dans le choix de ce paramètre de comprendre que si on réserve un espace trop important de la mémoire RAM le système en souffrira, et donc l'efficacité du caching se trouvera réduite, de même que si l'espace est trop réduit. Alors avant de définir l'espace mémoire qui sera réservé pour le caching on vérifie la consommation du système en mémoire avec la commande :

**free -m**

- Et ainsi pouvoir définir dans le fichier de configuration d'espace RAM alloué au cache en ajoutant la ligne de commande suivante :

*cache\_mem 1024 MB*

## f. La taille maximale d'un objet dans la mémoire :

puisque nous avons un espace limité pour le caching des objets, nous devons utiliser cet espace de façon optimisée, nous allons limiter la taille maximum des objet à 1 Mo, parce que si la taille des objets est grande cela voudrait dire que le nombre d'objets en cache sera réduit, et donc l'efficacité du cache s'en trouvera réduite, et on spécifie donc la taille maximale d'un objet dans la RAM avec la ligne de commande suivante :

*maximum\_object\_size\_in\_memory 1 MB*

## g. Les paramètres du répertoire cache :

*cache\_dirufs /var/spool/squid 102400 16 256*

- *Cache\_dir* : indiquer ici le volume du cache. Si on a plusieurs disques, on utilise plusieurs fois cette ligne. Si squid ne fonctionne pas bien ou s'arrête parfois sans raison apparente, il faut vérifier qu'on a un cache assez important ou bien configuré.
- *Ufs* : format des fichiers cache utilisé par squid
- */var/spool/squid* : le répertoire du cache dans le disque dur.
- *102400* : l'espace réservée pour le cache en Mo, donc dans notre étude l'espace réservé pour la mémoire est de 100Go.
- *16* : nombre de sous-répertoire de premier niveau qui vont être créés.
- *256* : nombre de sous-répertoire de deuxième niveau qui vont être créés à l'intérieur de chaque sous-répertoire de premier niveau



- Il est aussi important d'indiquer les limites dans la taille des documents web qui vont être mis dans la mémoire cache en fonction de l'espace réservé. Nous allons mettre les valeurs suivantes : *Minimum\_object\_size 0 KB*

*Maximum\_object\_size 1 MB*

## 8. Intégration de l'authentification LDAP :

Pour l'intégration de l'authentification LDAP nous commençons par ajouter la ligne de commande suivante au fichier de configuration du server Squid (squid.conf), « figure 3.42 ».

```
auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -b "dc=epb,dc=loc" -D "cn=squid,ou=proxy,dc=epb,dc=loc" -w "*Alpha*" -f "sAMAccountName=%s" -h 192.168.80.2

auth_param basic children 5
auth_param basic realm veuillez vous identifier
auth_param basic credentialsttl 3 hour

external_acl_type ldap_group %LOGIN /usr/lib64/squid/ext_ldap_group_acl -R -b "dc=epb,dc=loc" -D "cn=squid,ou=proxy,dc=epb,dc=loc" -w "*Alpha*" -f "((&(objectclass=person) (sAMAccountName=%v) (memberof=cn=%a,ou=proxy,dc=epb,dc=loc)))" -h 192.168.80.2
```

**Figure 3.42 :** Code pour l'authentification LDAP sur Squid

- Dans les premiers et derniers paramètres, on y intègre les commandes qu'on a testées auparavant et qui sont relatif à l'utilisation des Helpers.
- **Auth\_param basic children 5** : nombre de processus des Helpers utilisés
- **Auth\_param basic realm** veuillez vous identifier: permet d'intégrer un message à la fenêtre d'authentification.
- **Auth\_param basic Credentialsttl 1 hour**: indique la durée pour laquelle l'utilisateur va être authentifié.

Les ACL relatif aux groupes Active Directory « figure3.43 »:

```
acl groupe1 external ldap_group groupe1
acl groupe2 external ldap_group groupe2
acl groupe3 external ldap_group groupe3

acl streaming url_regex -i youtube.com
acl RESsociaux url_regex -i facebook.com twitter.com
acl matin time SMTWH 8:00-12:00
acl aprmidi time SMTWH 13:30-17:00

http_access allow RESsociaux !matin !aprmidi
http_access allow groupe1
http_access allow groupe2 !streaming
http_access deny groupe3
```

**Figure 3.43 :** Les ACL relatif aux groupes Active Directory

- Les ACL nommée Groupe1, Groupe2, Groupe3 servent à intégrer les utilisateurs AD selon leur appartenance aux groupes créés dans l'unité d'organisation Proxy et qui portent le même nom que ces ACL.
- Ensuite on crée quatre ACL, la première pour les sites de streaming vidéo et la deuxième pour les réseaux sociaux, et enfin les deux derniers définissant les horaires de travail (matin et après-midi)
- Enfin pour les autorisations d'accès :
  - On interdit l'accès aux réseaux sociaux durant les horaires de travail (cette ACL est appliqué à tous les utilisateurs)
  - On autorise l'accès à internet aux utilisateurs du Groupe1
  - On autorise l'accès à internet aux utilisateurs du Groupe2 sauf pour les sites de streaming vidéo.
  - On interdit l'accès internet aux utilisateurs du Groupe3

## 9. Lancement et maintenance du serveur Squid :

### 9.1.Lancement du serveur Squid :

- Une fois la configuration du serveur Squid est terminée on lance ce dernier et on vérifie son état de fonctionnement comme la « figure 3.44 » :

```
[root@epb ~]# systemctl start squid
[root@epb ~]# systemctl enable squid
Created symlink from /etc/systemd/system/multi-user.target.wants/squid.service to /usr/lib/systemd/system/squid.service.
[root@epb ~]# systemctl status squid
■ squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; vendor preset: disabled)
   Active: active (running) since lun. 2018-06-11 01:54:09 CEST; 1min 20s ago
 Main PID: 1254 (squid)
    CGroup: /system.slice/squid.service
           └─1254 /usr/sbin/squid -f /etc/squid/squid.conf
             └─1256 (squid-1) -f /etc/squid/squid.conf
               └─1257 (logfile-daemon) /var/log/squid/access.log

juin 11 01:53:41 epb.loc systemd[1]: Starting Squid caching proxy...
juin 11 01:54:09 epb.loc systemd[1]: Started Squid caching proxy.
juin 11 01:54:09 epb.loc squid[1254]: Squid Parent: will start 1 kids
juin 11 01:54:09 epb.loc squid[1254]: Squid Parent: (squid-1) process 1256 started
```

Figure 3.44 : Lancement du serveur Squid

- Ou bien avec cette commande qui comporte des options qu'on peut énumérer en ajoutant l'option `-h` comme indiqué sur la « figure 3.45 » :

```

[root@epb ~]# /sbin/squid -h
Usage: squid [-cdhvzCFMRYX] [-n name] [-s s [-l facility]] [-f config-file] [-[au] port] [-k signal]
-a port    Specify HTTP port number (default: 3128).
-d level   Write debugging to stderr also.
-f file    Use given config-file instead of
           /etc/squid/squid.conf
-h         Print help message.
-k reconfi|rotate|shutdown|restart|interrupt|kill|debug|check|parse
           Parse configuration file, then send signal to
           running copy (except -k parse) and exit.
-n name    Specify service name to use for service operations
           default is: squid.
-s s [-l facility]
           Enable logging to syslog.
-u port    Specify ICP port number (default: 3130), disable with 0.
-v         Print version.
-z         Create missing swap directories and then exit.
-C         Do not catch fatal signals.
-D         OBSOLETE. Scheduled for removal.
-F         Don't serve any requests until store is rebuilt.
-N         No daemon mode.
-R         Do not set REUSEADDR on port.
-S         Double-check swap during rebuild.
-X         Force full debugging.
-Y         Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.

```

Figure 3.45 : menu d'aide du programme Squid

- Parmi ces options, celle qui reviendra le plus souvent est l'option `-k` qui est en rapport avec le processus Squid :

*/sbin/squid -k*

- `reconfigure` : recharge les paramètres du fichier `squid.conf` qui va nous permettre d'appliquer les nouveaux paramètres sans devoir redémarrer le serveur.
- `rotate` : permet de créer une copie des fichiers `.log` avant de les vider (cela permet d'avoir des fichiers log de petite taille et donc faciliter leur analyse)
- `shutdown` : permet d'arrêter le serveur Squid
- `interrupt` : forcer l'arrêt du serveur Squid
- `kill` : tuer les processus Squid
- `debug/check` : vérifier l'état du serveur et afficher les messages d'erreurs.

## 9.2.Création des répertoires swap :

Pour le lancement du serveur pour la première fois on doit commencer par créer les répertoires d'échange (*swap*) dont on indique le nombre et la taille de fichier de configuration `squid.conf`

```

[root@epb ~]# /sbin/squid -z

```

Figure 3.46 : création du répertoire swap

### 9.3.Maintenance du serveur Squid :

#### 9.3.1. La vérification de l'état du serveur :

La vérification de l'état du serveur est impérative pour assurer son bon fonctionnement, il nous permet d'afficher les erreurs relatives au serveur, ceci peut être fait avec les deux commandes suivantes « figure 3.47 »:

```
[root@epb ~]# /sbin/squid -k check
[root@epb ~]# /sbin/squid -k debug
[root@epb ~]#
```

**Figure 3.47** : vérification de l'état du serveur

S'il n'y a aucune réponse renvoyée par ces deux commandes, cela voudrait dire qu'il n'y a pas d'erreurs et que le serveur fonctionne correctement.

#### 9.3.2. Historique d'événements du serveur Squid :

L'historique d'événements du serveur Squid se trouve dans le fichier :

`/var/log/squid/cache.log`, c'est là que sont notées les actions faites par Squid, et c'est là qu'on peut avoir les détails sur l'état du serveur et les erreurs survenues lors de son exécution.

#### 9.3.3. L'audit du serveur Squid :

Squid journalise les transactions dans un fichier `access.log`. Ce fichier donne les informations sur les requêtes qui ont transité par Squid. Ce dernier offre la possibilité de voir les requêtes envoyées par les utilisateurs en détaillant :

- Le nom de l'utilisateur.
- Le port source et destination.
- L'adresse IP source et destination.
- Le port source et destination.
- Le type du document.
- L'état de la requête : Accpet / Denied.
- les dates indiquées dans le fichier `access.log` indique le temps en secondes depuis le 1 janvier 1970 (format epoch).

## 10.Phase de Test (coté client) :

Coté client, l'utilisateur ne peut pas se connecter à internet avant de configurer son navigateur et de s'être authentifié.

- Sous internet explorer :
1. Dans **Outils** -> Options **Internet**.
  2. On sélectionne l'onglet **Connexion** puis on clique sur **Réseau Local**.
  3. On coche sur **Serveur Proxy** et dans la fenêtre qui apparait on y indique l'adresse et le port de connexion du proxy :

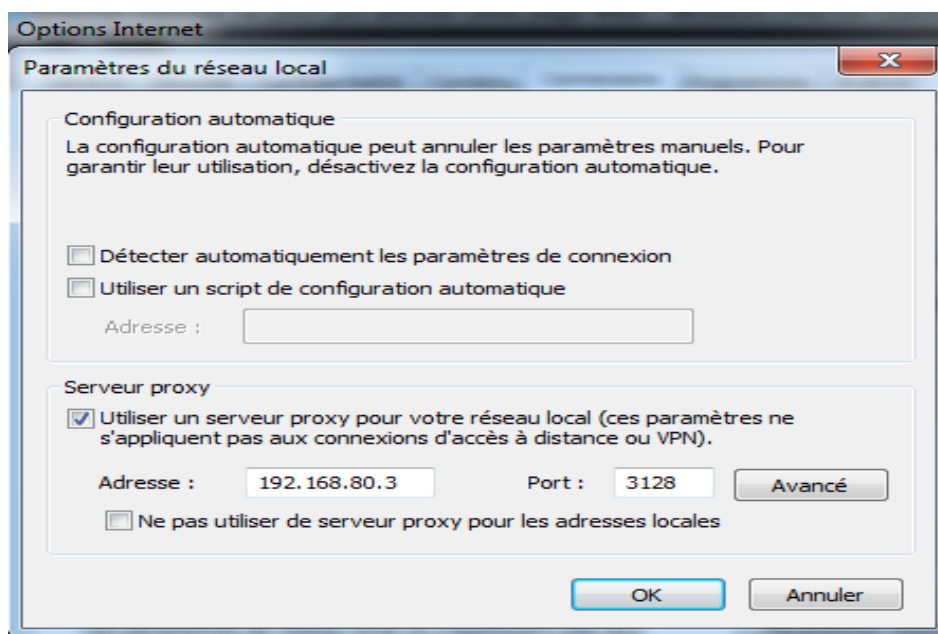


Figure 3.48 : Définition du serveur proxy sous internet explorer

Une fois le navigateur paramétré, on redémarre le navigateur et la fenêtre d'authentification apparait dans la « figure 3.49 »:

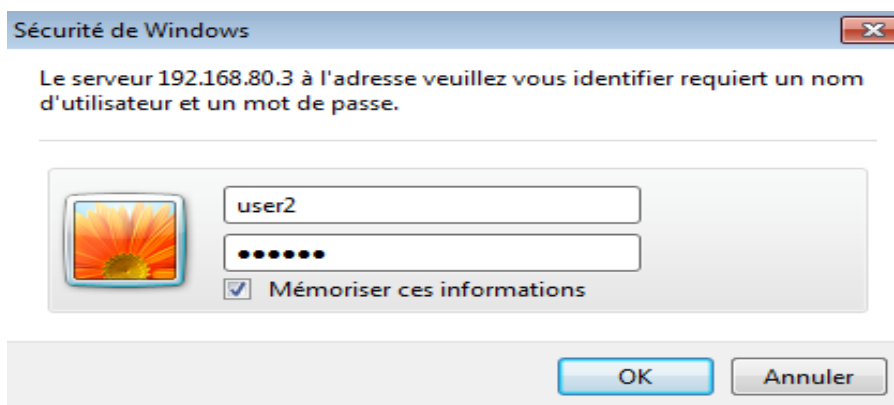


Figure 3.49 : fenêtre d'authentification

Une fois l'authentification confirmée, l'utilisateur peut se connecter dans la limite définie par l'administrateur, si l'utilisateur essaye d'accéder à un site dont il n'a pas l'accès, une page d'erreur apparaît :

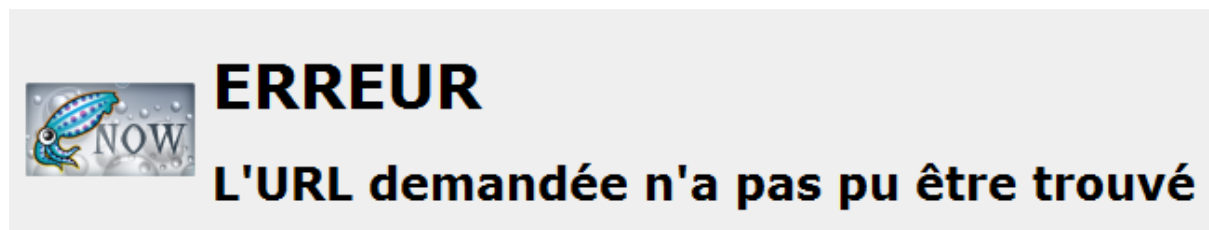


Figure 3.50 : page d'erreur

## 11.SquidGuard :

### 10.1. Présentation :

SquidGuard est un redirecteur d'URL, il utilise les listes noires avec le proxy Squid. SquidGuard est un module pour le serveur proxy Squid, qui ajoute des fonctionnalités plus avancées en matière de filtrage web. Il est utilisé pour limiter l'accès à certaines URL en fonction de l'utilisateur, de la machine, de l'heure, du contenu ... [44].

### 10.2. Installation de SquidGuard :

- Pour l'installation de squidguard, nous commençons par ajouter une nouvelle source de téléchargement (un nouveau Repository) avec la commande suivante « figure 3.51 »:

```
[root@epb ~]# yum install epel-release
Modules complémentaires chargés : fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.coreix.net
 * extras: mirrors.coreix.net
 * updates: mirrors.coreix.net
Résolution des dépendances
--> Lancement de la transaction de test
--> Le paquet epel-release.noarch 0:7-11 sera installé
```

Figure 3.51 : Installation de squidGuard (1)

- On télécharge le SquidGuard :

```
[root@epb ~]# yum install squidGuard
Modules complémentaires chargés : fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink
* base: mirrors.coreix.net
* epel: mirror.airenetworks.es
* extras: mirrors.coreix.net
* updates: mirrors.coreix.net
epel
(1/3): epel/x86_64/group_gz
```

Figure 3.52 : installation de squidGuard (2)

### 10.3. Configuration de SquidGuard :

- Nous commencerons par créer un répertoire pour les blacklists et nous procéderons au téléchargement de ses dernières :
  - `#cd /var/squidGuard` : on change la position du curseur vers le répertoire SquidGuard.
  - `#mkdirblacklist` : on crée un dossier blacklist à l'intérieur de répertoire SquidGuard.
  - `#yuminstallwget` : on installe le programme qui nous permettra de télécharger les blacklists.
  - `#wget ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz`  
: on télécharge le fichier compressé contenant les blacklists.
- Une fois le téléchargement est terminé on procède à l'extraction des fichiers du dossier compressé avec la commande suivante :
  - `#tar -xvf blacklists.tar.gz`

Ensuite nous éditerons le fichier squidGuard.conf avec l'éditeur de texte Vi :

```
#vi /etc/squid/squidGuard.conf
```

Modification sur le fichier SquidGuard.conf :

- Dans le fichier squidGuard.conf nous commencerons par définir les horaires de travail :

```
Time workhours {
    weekly mtwhf 8:00 – 17:00
    date      *.*.*
}
```

- Ensuite on définit les plages d'adresse des utilisateurs :

```
src admin {
    ip 192.168.80.3 255.0.0.0
    within workhours
}

src utilisateur {
    ip 172.16.2.32-172.16.2.100
}
```

- Et on ajoute les catégories de blacklistes en définissant le chemin des fichiers contenant les noms de domaines et les urls « figure 3.53 ».

```
dest proxy {
    domainlist blacklists/proxy/domains
    urllist blacklists/proxy/urls
    redirect http://google.com
}

dest ddos {
    domainlist blacklists/ddos/domains
    urllist blacklists/ddos/urls
    redirect http://google.com
}

dest hacking {
    domainlist blacklists/hacking/domains
    urllist blacklists/hacking/urls
    redirect http://google.com
}
```

**Figure 3.53 :** Intégration des Blacklist au squidguard



- **Redirect** : sert à définir le site vers lequel l'utilisateur va être redirigé. S'il essaye d'accéder à la catégorie de site définie, et dans ce cas la redirection se fait vers le moteur de recherche : google.com.

Remarque :

- la première catégorie de destination est d'une importance capitale pour l'efficacité du serveur proxy, en effet en bloquant l'accès à cette catégorie de site, ça évitera le contournement de notre proxy en passant sur un autre proxy sur internet « figure3.54 »
- On définit les ACL :

```

acl {
    admin {
        pass any
    }

    utilisateur {
        pass !proxy!ddos!hacking any
        redirect http://google.com
    }
}

```

**Figure 3.54** : Définition des ACL

- Et à la fin on sauvegarde le fichier et on compile les blacklists avec la commande suivante :

```
# squidGuard -b -d -C all
```

a. Modification sur le fichier Squid.conf :

- Au niveau du fichier de configuration du serveur Squid on ajoute la ligne suivante :

```
url_rewrite_program /usr/bin/squidGuard
```

- On sauvegarde le fichier de configuration et on rafraichit les paramètres utilisés par Squid server avec la commande suivante :

```
/etc/sbin/squid -k reconfigure
```

- Enfin on donne le droit de lecture au serveur proxy sur les fichiers des blacklist

```
chown -R squid /var/squidGuard/blacklists
```

## 12.L'antivirus clamav :

### 12.1. Définition :

Clam Anti-virus(Clamav) est un antivirus GPL pour UNIX en ligne de commande. Utilitaire pour une mise à jour automatique des bases de données virales via internet.

### 12.2. Installation de clamav :

1. On lance le téléchargement et l'installation de clamav et ses modules complémentaires, figure « 3.55 ».

On lance le téléchargement et l'installation de clamav et ses modules complémentaires

```
[root@epb ~]# yum install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-sstend clamav-devel clamav-lib clamav-server-systemd
Modules complémentaires chargés : fastestmirror
Loading mirror speeds from cached hostfile
* base: ftp.hosteurope.de
* epel: mirror.in2p3.fr
* extras: ftp.hosteurope.de
* updates: ftp.hosteurope.de
```

**Figure 3.55 :** installation de l'anti-virus clamav

2. On déplace le fichier clam.conf vers son répertoire par défaut :

```
cp /usr/share/clamav/template/clamd.conf /etc/clamd.d/clamd.conf
```

3. On supprime la ligne ou il est écrit Exemple du fichier clamd.conf pour que clamd puisse se lancer normalement (clamdaemon: est le programme qui nous offrira une protection en temps réel en scannant les objets transitant par le Proxy)

```
Sed -i '/^Exemple/d' /etc/clamd.d/clamd.conf
```

4. Dans le fichier de configuration clamd.conf on ajoute les deux lignes suivantes :

```
User root
```

```
LocalSocket /var/run/clamd.<SERVICE>/clamd.sock
```

5. On supprime la ligne ou il est écrit Exemple du fichier freshclam.conf pour qu'on puisse mettre à jour la base de données de clamav avec la commande freshclam:

```
sed -i '/^Example/d' /etc/freshclam.conf
```

6. On met à jour la base donnée de clamav avec ligne de commande suivante :

```
Frechclam
```

7. On teste le bon fonctionnement de l'anti-virus :

a- on télécharge un virus expérimental :

```
[root@epb clamav]# wget http://www.eicar.org/download/eicar.com
```

b- on scanne le répertoire dans lequel se trouve le virus expérimental:

```
[root@epb clamav]# clamscan --infected --remove --recursive
/var/lib/clamav/eicar.com: Eicar-Test-Signature FOUND
/var/lib/clamav/eicar.com: Removed.

----- SCAN SUMMARY -----
Known viruses: 4482413
Engine version: 0.99.1
Scanned directories: 1
Scanned files: 6
Infected files: 1
Data scanned: 25.60 MB
Data read: 178.49 MB (ratio 0.14:1)
Time: 42.841 sec (0 m 42 s)
```

**Figure 3.56** : scanne du répertoire

- Et là on remarque que le virus a été détecté et supprimé « figure 3.56 ».

### 13. Conclusion :

Parmi les nombreuses méthodes et solutions qui existent pour faire face aux nombreux problèmes de sécurité liés à l'utilisation d'internet et du Web en particulier dans les entreprises, beaucoup d'entre elles coutent bien chères pour l'entreprise.

Ainsi l'étude de l'existant est une étape très importante dans un projet pareil car on fera en sorte de mettre le maximum pour trouver une solution qui répond aux besoins et qui s'intègre facilement sans trop de charges dans l'architecture existante et dans l'idéal, a moindre coup, c'est pour cette raison là que nous avons opter pour la mise en place d'un serveur proxy squid sous CentOS Linux qui en plus de sa gratuité, améliore d'une façon nette et significative la sécurité et le contrôle qu'on peut avoir sur le trafic réseau.

### *Conclusion générale :*

De nos jours l'Internet est un réseau mondial public très utilisé et tout le monde y a accès. Cette interconnexion à Internet est directement exposée à des attaques informatiques complexes. Nous devons ainsi mettre en place une passerelle sécurisée entre notre réseau et Internet qui agit directement au niveau de la couche Application, pour Controller, vérifier et filtrer les requêtes destinée ou provenant du web.

Dans notre cas, nous avons opté pour la mise en place d'une solution, l'installation d'un serveur proxy, plus précisément le serveur proxy Squid qui en plus de sa gratuité, semblait répondre aux exigences de l'entreprise EPB au niveau contrôle du trafic web.

Nous avons vu durant cette étude que le rôle primordial du proxy squid est le cache c'est-à-dire garder les pages HTTP en local et les restituer aux clients. Il joue aussi le rôle de filtre et de sécurité. Nous avons vu que Squid peut bloquer l'accès à l'Internet à certains utilisateurs selon des critères bien définis ou même bloquer l'accès à certains sites que l'on juge dangereux ou inutiles en intégrant squidGard et on a installé un antivirus ClamAV à la solution afin de bloquer les virus et autres malware pour rendre internet plus sûr pour les utilisateurs. . Nous avons aussi vu que Squid pouvait être couplé à un annuaire LDAP de telle sorte que seuls nos utilisateurs de notre réseau disposant d'un compte dans l'annuaire avec login et mot de passe peuvent avoir l'Internet.

La solution proposer répond à ces objectifs et, grâce à l'ambivalence de squid et des plug-ins qui sont développés par la communauté qui l'entoure cette solution peut s'adapter sur de très nombreuses infrastructures, pouvant répondre à de nombreux besoins. Une fois de plus, l'utilisation d'application venant du monde libre permet le développement d'une solution gratuite et très complète

Ce travail a fait l'objet d'une expérience intéressante et très enrichissante, et a eu énormément d'apport sur nos connaissances et nos compétences, il nous a permis de nous familiarisé un peu plus avec L'environnement Linux, de comprendre un peu ses mécanismes, ainsi les concepts de sécurités des réseaux.

Finalement, cette expérience est très intéressante, et très riche en découverte et une bonne expérience acquise, ceci dit il peut encore être amélioré en utilisant le revers proxy.

## **Résumé :**

Avec l'évolution des usages de l'Internet, il devient nécessaire de garantir des conditions correctes de navigation et une protection minimale de la confidentialité des informations personnelles dans l'infrastructure système et réseau. Le service mandataire avec filtrage d'URLs est un outil indispensable dans la panoplie de sécurisation du trafic Web.

Pour cela on a mis en place un serveur proxy squid sous CentOS 7 Linux, nous avons vu durant cette étude que les fonctionnalités d'un proxy squid est le cache c'est-à-dire garder les pages HTTP en local et les restituer aux clients. Il joue aussi le rôle de filtre et de sécurité. Nous avons vu que Squid peut bloquer l'accès à l'Internet à certains utilisateurs selon des critères bien définis ou même bloquer l'accès à certains sites que l'on juge dangereux ou inutiles en intégrant squidGuard et on a installé un antivirus ClamAV à la solution afin de bloquer les virus et autres malware pour rendre internet plus sûr pour les utilisateurs. . Nous avons aussi vu que Squid pouvait être couplé à un annuaire LDAP de telle sorte que seuls nos utilisateurs de notre réseau disposant d'un compte dans l'annuaire avec login et mot de passe peuvent avoir l'Internet.

Finalement, cette expérience est très intéressante, et très riche en découverte et une bonne expérience acquise, ceci dit il peut encore être amélioré en utilisant le revers proxy.

## **Abstract**

As the use of the Internet evolves, it becomes necessary to ensure proper browsing conditions and minimum privacy protection for personal information in the system and network infrastructure. The proxy service with URL filtering is an indispensable tool in the set of securing web traffic.

For this we set up a proxy server squid CentOS 7 Linux, we saw during this study that the features of a proxy squid is the cache that is to keep the HTTP pages locally and return them to customers. It also plays the role of filter and security.

We have seen that Squid can block access to the Internet to certain users according to well-defined criteria or even block access to certain sites that are considered dangerous or unnecessary by integrating squidGard and we installed a ClamAV antivirus to the solution to block viruses and other malware to make the internet safer for users. .

We also saw that Squid could be linked to an LDAP directory so that only our users in our network with an account in the directory with login and password can have the Internet.

Finally, this experience is very interesting, and very rich in discovery and good experience acquired, that said it can still be improved by using the reverse proxy.

## **Bibliographie :**

- [1]. reseau-informatique <https://www.scribd.com/document/89874207/Stage-MHASOFT->
- [2]. « Vincent Herbert » Le protocole WEP, Mémoire 2007
- [3]. Reseaux-complet <https://fr.scribd.com/document/358369362/>
- [4]. Etude-des-methodes-et-protocoles-dacces-au-support-dans-un-reseau-informatique-Cas-de-LAN <https://www.memoireonline.com/06/12/5936/>
- [5].Notion de base <http://ensa-mecatronic.e-monsite.com/medias/files/re-p2-bases-2008>
- [6].« Briki Riad » Reseau, 2015 <https://fr.slideshare.net/brikiriadh/coursreseau-15>
- [7]. m\_Etude-de-la-mise-en-place-dun-reseau-informatique-dans-une-entite-etatique-decentralisee <https://www.memoireonline.com/02/17/9624/>
- [8]. PujolleGuy, « Les Réseaux » 6e Edition mise à jour, Edition Eyrolles 2009.
- [9]. Reseaux <http://mb13010.free.fr/COURS-TSI-SEQUENCE2/>
- [10]. <http://landrevie.gjl.free.fr/CommentCaMarche/initiation/peer>
- [11]. reseau-et-teleinfo <https://fr.scribd.com/document/149993616/>
- [12]. [http://www.si2s.com/lan/install\\_reseau\\_plus.asp](http://www.si2s.com/lan/install_reseau_plus.asp)
- [13]. [https://www.memoireonline.com/10/12/6380/m\\_Etude-portant-sur-implantation-dun-reseau-sans-fil-wifi--Cas-de-Green-Wisprot-S-P-R-L25](https://www.memoireonline.com/10/12/6380/m_Etude-portant-sur-implantation-dun-reseau-sans-fil-wifi--Cas-de-Green-Wisprot-S-P-R-L25).
- [14]. Analyse-de-protocoles <http://www.technologuepro.com/reseaux/Analyse-de-protocoles/Decapsulation-trame-Ethernet>
- [15]. Model OSI <http://www.frameip.com/osi/>
- [16]. Model TCP /IP <http://www.frameip.com/tcpip/>
- [17]. Réseau informatiques, Model OSI et Protocole TCP/IP
- [18]. Principes généraux <https://www.supinfo.com/articles/single/2047-principes-generaux-communication-reseau>
- [19]. Conception-et-deploiement-dune-architecture-reseau-securisee <https://www.memoireonline.com/11/11/4952/>
- [20]. CISCO la sécurité de réseaux « Vincent Remazeilles » Edition eni, 2009.
- [21]. L'Authentification de A à Z - Caline Villacres Ernst & Young LLP - Security & Technology 30 Services

- [23]. Laurent Bloch & Christophe Wolfhugel Sécurité informatique « Principes et méthode » , edition Eyrolles ,2006.
- [24]. Les attaques informatiques <https://fr.linkedin.com/pulse/les-types-dattaques-informatique-omar-tifouri>
- [25]. [http://www.academia.edu/15633432/Type\\_dattaques](http://www.academia.edu/15633432/Type_dattaques)
- [26]. Proxy squid <https://www.memoireonline.com/>
- [27]. DMZ <https://prezi.com/woln8zl1da1k/dmz/>
- [28]. Cryptographie et sécurité informatique « Dumont Renaud » 2010
- [29]. <http://vpndock.com/info/vpn/>
- [30]. Jean-François Pillou et Jean-Philippe Bay. Sécurité informatique.3ième édition, Dunod, Paris 2013
- [31]. <https://doc.ubuntu-fr.org/pare-feu>
- [32]. Ismail Rachdaoui. PFSense FreeBSB. Génie Réseaux et Télécommunications ENSA Marrakech, 2013. In:  
<http://fr.slideshare.net/ISMAILRACHDAOUI/installation-etconfiguration-de-pfsense>  
<https://www.scribd.com/document/328254543/>
- [33]. <http://ofppt.info/wp-content/uploads/2014/07/Diagnostic-des-7-Couches-reseau.pdf>
- [34]. Reseaux-informatiques <https://www.doc-etudiant.fr/Informatique/>
- [35]. <https://www.cairn.info/revue-annales-de-demographie-historique-2005-1-page-7.htm>
- [36]. <http://docplayer.fr/4094277-On-distingue-deux-categories-de-reseaux-le-reseau-poste-a-poste-et-le-reseau-disposant-d-un-serveur-dedie>
- [37]. <http://intrapole.com/spip.php?article22>
- [38]. SERVEUR PROXY <https://fr.scribd.com/doc/216107262/Serveur-Proxy>
- [39]. <https://www.supinfo.com/articles/single/3031-tutoriel-gns3>
- [40]. <https://linuxfr.org/tags/hat/public.atom>
- [41]. <https://www.1and1.fr/digitalguide/serveur/configuration/squid-le-serveur-de-cache-en-licence-libre/>
- [42]. <https://www.scribd.com/document/143995129/VMware>
- [43]. <https://www.microsoft.com/fr-FR/download/details.aspx?id=269>
- [44]. <http://www.squidguard.org/index.html>



[45]. IBM\_System\_x3550\_guide\_utilisation.