REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Mouloud Mammeri de Tizi Ouzou

Faculté de Génie Electrique et Informatique
Département Informatique

Mémoire de fin d'etudes

En vue de l'obtention du diplôme de Master 2 Académique
En Informatique
Option : Réseau Mobilité Systèmes Embarqués

THEME

Sécurisation des Communications Client-serveur sur Multiples Plates-Formes (Microsoft/Linux)

Réalisé par:
Zaidi Samir
Soumah Salifou

Proposé par :
M^r^ Taleb (Co-Promoteur)

Dirigé par :
M^r^ Djamah (Promoteur)

Année Universitaire : 2014/2015

Nous tenons avant tout de remercier le bon DIEU qui nous a donné la volonté et le courage pour la réalisation de ce modeste travail.

Nous remercions vivement Mr Djamah notre promoteur et Mr Taleb notre Co promoteur pour leurs précieuses assistantes, leurs disponibilités et leurs soutiens qu'ils nous ont accordé tout au long de ce projet.

Que les membres de jury trouvent ici l'expression de nos sincères remerciements pour l'honneur qu'ils nous font en acceptant de juger notre travail.

Nous tenons aussi à remercier tous les professeurs du Département Informatique qui ne cessent de ménager aucun effort pour la réussite des étudiants du Département.

Que cette page soit aussi le parfait témoignage de notre gratitude envers tous nos amis qui nous ont aidés, de près ou de loin, à élaborer ce travail.

Nous tenons aussi à remercier l'Entreprise ENIEM, de nous avoir accordé un Stage Pratique de trois (3) au sein de leur Structure.

Dedicace

Je tiens à dédier ce modeste travail à :

- *Mes très chers parents qui m'ont toujours poussé vers l'avant ;*
- *Mes frères, mes sœurs et toue la famille*
- *A ma tutrice en Algérie Mme Yattara*
- *A Tous mes amis et Compatriotes en Algérie*
- *A la communauté des étudiants étrangers de Tizi-Ouzou*
- *A Tous les professeurs du Département informatique*
- *A tous mes amis Algériens*
- *Tous mes voisins et amis du quartier ENTAG*
- *A tous les étudiants de Master 2 RMSE en Particulier et à tous les étudiants du département informatique en générale*

Mr SOUMAH SALIFOU

Dedicace

Je dédie ce modeste travail à :

- *Mes parents pour leur amour inestimable, leurs confiances, Leurs soutiens, leurs sacrifices et leurs patiences tout le long de ma vie.*

- *A mes chers oncles : Hakim, Amar.*
- *A ma chère amie Nora.*
- *A mon très cher frère : Haçene.*
- *A tous mes amis (es) de la promotion 2014/2015.*
- *A mon cher amie et binôme, avec lequel j'ai eu le plaisir de partager ce travail, et à tous les membres de sa famille.*

Zaidi Samir.

Sommaire du Chapitre I : Présentation de l'Organisme d'Accueil

Sommaire du Chapitre II : Généralités sur les Réseaux Informatiques

Sommaire du Chapitre III : Concepts de Base de la Sécurité Réseau

Sommaire du Chapitre IV : Systèmes d'Exploitation Client-serveur

Sommaire du Chapitre 5 : Conception et Réalisation

Table des Illustrations

Table des illustrations

.

Introduction Générale

Les réseaux informatiques deviennent de plus en plus considérables, et font partie intégrante du fonctionnement des entreprises, Cette situation a d'énormes conséquences sur leur sécurité.

En effet, un réseau doit assurer la confidentialité, l'intégrité et la disponibilité de ses données. Cet objectif justifie à lui seul la nécessité d'accorder une attention particulière à la sécurisation des réseaux informatiques, La Sécurité d'un Réseau est de garantir que l'ensemble des ressources du Réseau fonctionnent de façon optimale et que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés. La sécurisation d'un réseau n'est pas simple à réaliser car elle nécessite un long processus qui remonte jusqu'à la conception de son architecture. Le réseau est constitué d'un ensemble de systèmes hétérogènes, de nombreux services, qui ne cessent d'évoluer. Il est donc essentiel d'élaborer une politique de sécurité et la mettre en œuvre dès la conception même des infrastructures.

Pour cela, de nombreuses techniques de sécurisation sont mises en place, afin d'assurer le respect de bonnes pratiques de sécurités. Parmi ces techniques, on cite l'utilisation: de filtrage des paquets via un pare-feu, d'Annuaire permettant d'identifier et d'authentifier les utilisateurs (Active Directory),

- de politique de groupe (GPO),
- de Zone Démilitarisée (DMZ),
- de segmentation logique du Réseau Local en VLANS,
- de VPN

C'est dans cette logique que ce travail s'inscrit pour optimiser la Sécurité du Réseau de L'ENIEM sous le thème : **la Sécurisation des communications Client-serveur sur Multiples Plateformes (Microsoft/Linux)** en passant par les Chapitres suivants :

Chapitre I : Présentation de l'Organisme d'Accueil, dans ce chapitre, le champ d'étude **<<ENIEM>>** dans son intégralité afin de mieux cerner la portée de ce projet.

Chapitre II : Généralités sur les Réseaux Informatiques, dans cette partie, un accent est mis sur les différentes notions de base des Réseaux Informatiques.

Chapitre III : Concepts de Base de la Sécurité Réseau, dans ce chapitre, les différentes menaces, dangers, risques, vulnérabilités liées à l'insécurité Réseau seront discutées et les différentes mesures de précaution pour optimiser la sécurité du Réseau seront recensées.

Chapitre IV : systèmes d'exploitation Client-serveur : dans ce chapitre, l'intérêt des exploitations Réseau, des Serveurs et l'avantage qu'offre l'architecture Client-serveur dans un Réseau Local seront mis en évidence.

Chapitre v : Conception et Réalisation : c'est dans cette partie, que les solutions apportées pour l'optimisation de la sécurité du Réseau de L'ENIEM ainsi que leur déploiement et mise en œuvre seront explicités.

Chapitre I : Présentation de L'Organisme d'Accueil

I. Introduction :

Dans un environnement économique sans cesse en évolution, les entreprises sont confrontées à des contraintes du marché dont les plus concurrentielles doivent pouvoir apporter de nouvelles réponses de type :

- Une offre plus grande de produits et services.
- Des délais de plus en plus courts.
- Des prix plus bas et des quantités livrées plus grandes.
- Des niveaux de qualité et de services supérieurs.

Pour relever ces défis et être tous les jours plus performants, les entreprises s'organisent, se modernisent et cherchent de nouvelles solutions comme l'informatisation. Aujourd'hui la place de l'informatique est essentielle dans les entreprises car elle accroit leur compétitivité en dehors du fait de résoudre les problèmes comme la paie, la tenue des stockes, la comptabilité, la communication etc., Elle apporte aussi une aide au niveau du marketing et des décisions.

Notre projet de fin d'études à été mené pendant un stage de trois mois au sein de l'Entreprise Nationale des Industries de l'Electroménager (ENIEM).

Figure I.1 : Bloc Administratif ENIEM (Entreprise Nationale des Industries de l'Electroménager)

II. Présentation de l'ENIEM

a. Situation géographique

Le siège social de l'entreprise ENIEM se situe au chef-lieu de la willaya de Tizi-Ouzou. Les unités de production froid, cuisson et climatisation sont implantées dans la zone industrielle Aissat Idir Oued-Assi distante de 7 KM du chef-lieu de la willaya. Elle s'étend sur une surface totale de 55 hectares. LA filiale sanitaire est installée à Miliana Willaya de Ain dafla, et la filiale lampe à Mohammedia Willaya de Mascara.

b. Activités de l'entreprise

L'activité de L'ENIEM se concentre sur la fabrication de réfrigérateurs, cuisinières, et climatiseurs.

Cette activité est assurée par des unités de productions: unité froid, unité cuisson, unité climatiseurs, unité prestation technique, unité commercial.

2.1 Unité froid : elle est composée de 3 lignes de production:

a. Une ligne de fabrication de réfrigérateur petit modèle :

Les capacités installées sont de 110.000 réfrigérateurs par année, dont les modèles fabriqués sous licence BOSCH Allemagne 1977.

b. Une ligne de réfrigérateurs grands modèles :

Les capacités installées sont de 390.000 réfrigérateurs par année dont les modèles fabriqués sous licence TOSHIBA- JAPON6-1987.

c. Une Ligne de congélateurs bahut et réfrigérateurs de 520 L :

Elle assure la production des **réfrigérateurs.** Les capacités installées sont de 60.000 appareils de 520L par an. Dont les modèles sous licence LEMATIC-Liban- 1993.

2.2 Unité Cuisson :

Elle assure la production des cuisinières, et les capacités installées sont de 150000 cuisinières par an fabriquées sous licence TECHNO GAZ- Italie – 1991.

2.3 Unité Climatisation :

Elle s'occupe de la fabrication des climatiseurs, soit une capacité d'environ 60.000 climatiseurs par année sous Licence AIWELL - France 1977 de différents modèles.

2.4 Unité Commerciale :

Ses activités sont :

- ✓ La distribution et l'exportation des produits ENIEM.
- ✓ Le service après-vente (à travers avec ses moyens propres et un réseau d'agents agréés).

2.5 Unité Prestations Techniques :

Cette unité assure les fonctions de soutien aux unités de production dans les domaines de :

- ✓ Réparation des outils et moules.
- ✓ Fabrication de pièces de rechange mécanique.
- ✓ Conception et réalisation d'outillages.
- ✓ Gestion des énergies et fluides.
- ✓ Gardiennage et sécurité.
- ✓ Travaux d'imprimerie.
- ✓ Travaux de menuiserie.
- ✓ Travaux de nettoyage.
- ✓ Prestation informatique.

Organigramme générale de l'entreprise

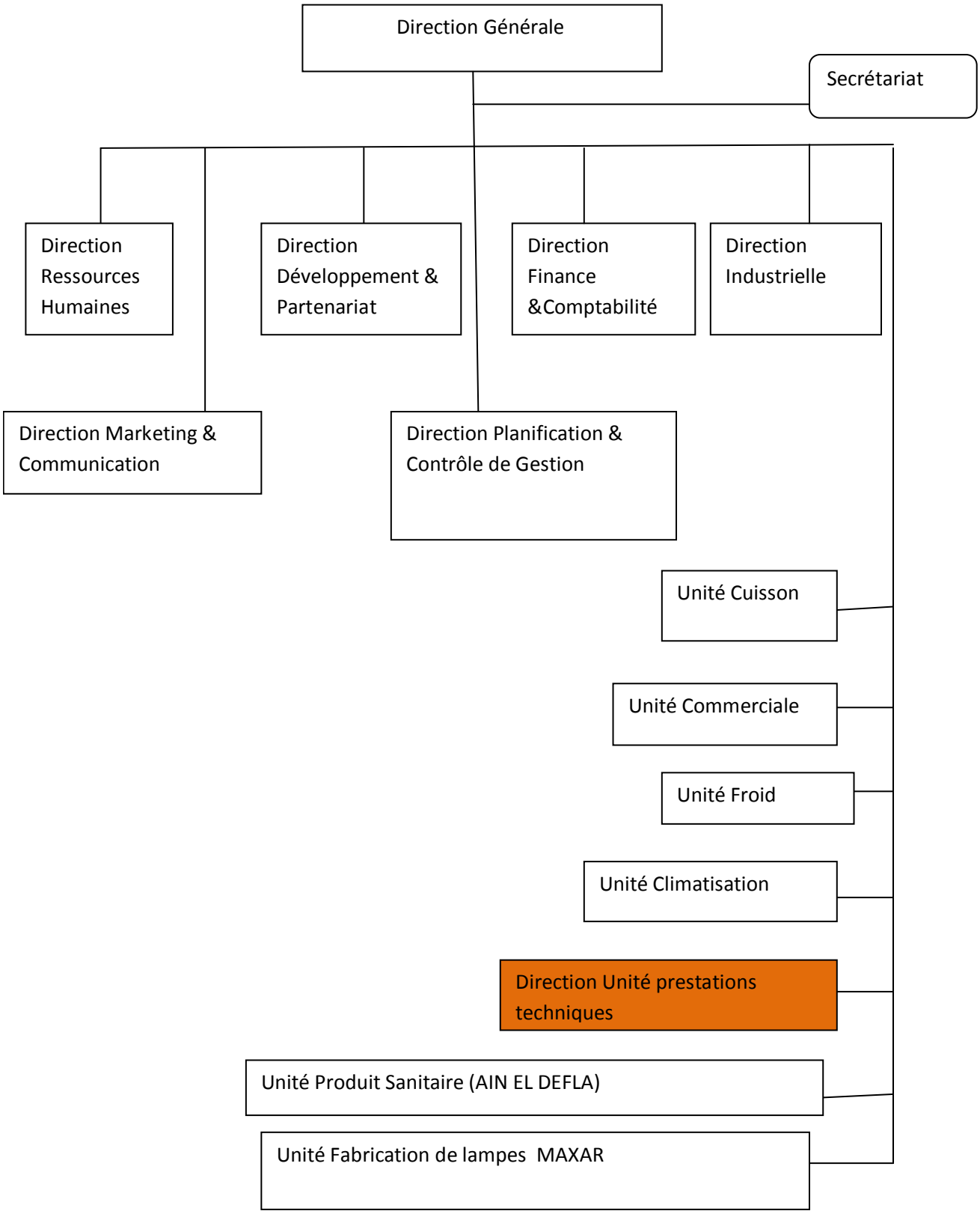


Figure I.2 : Organigramme générale de l'entreprise

III. Présentation du champ d'études :

Cette partie permettra de mieux définir le domaine d'étude et de mieux apercevoir ses objectifs, elle aidera aussi à relever les éventuels manques et anomalies dans le système existant dans le champ d'étude qui est l'unité de prestation technique.

III.1-Organigramme de l'Unité de Prestation Technique :

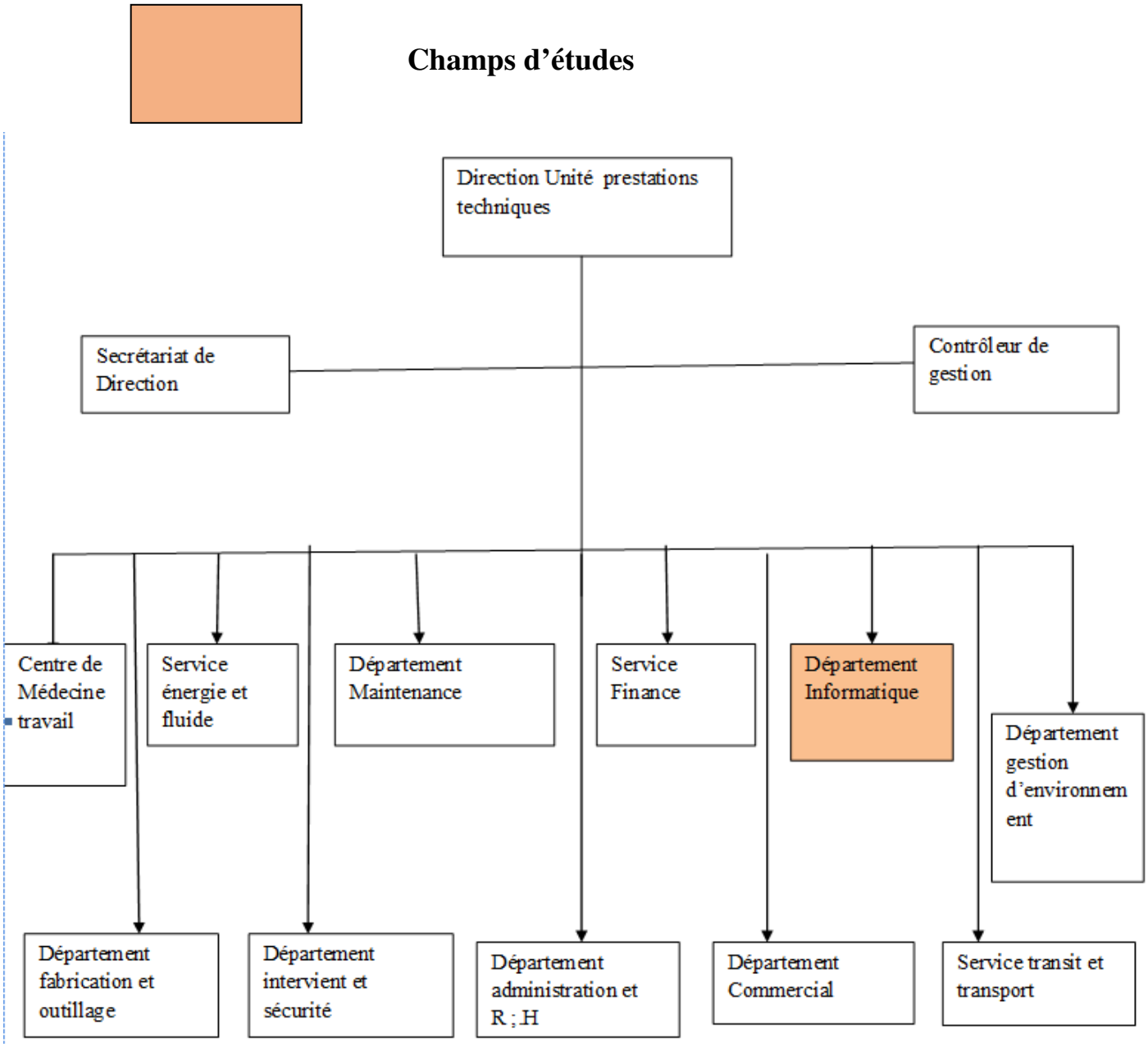


Figure I.3: Unité de Prestation Technique

III.2. Le Réseau informatique de l'entreprise l'ENIEM :

L'ENIEM utilise un réseau LAN, ce réseau est constitué de:

a. Un Réseau client/serveur :

Ce réseau est composé de 39 terminaux dont 27 écrans HP (modèle 700/92 A, 2392A) et 12 imprimantes HP (modèle 2563B, 2934A, Rugged Writer 480) reliés au serveur (HP3000/A500) par des liaisons directes (distances inférieures ou égales à 1200mètres), modem (pour les distances supérieures à 1200mètres), et multiplexeur modem (pour les installations de plusieurs terminaux distants).

- Caractéristiques de ce réseau :

Parmi ces caractéristiques, La topologie choisie est celle dite étoile, vu la configuration du site, à savoir : deux bâtiments en formes de T.

Le schéma général du câblage est défini selon le nombre de bureaux et le nombre d'utilisateurs par bureau.

Tous les bureaux sont dotés d'au moins une prise. Il en existe en tout 170 prises (actuellement il n'y a que 65 micro- ordinateurs connectés). Toutes les prises d'un même étage ou tous les ordinateurs d'un même étage avec ses différentes unités et fonctions sont reliées à un Switch contenu dans une armoire, cette dernière est reliée par un câble fibre optique à un Switch dit fédérateur contenu dans l'armoire centrale installée au niveau de la salle machine au sous sol du bâtiment B.

Le réseau est composé de 06 armoires départagées dans 03 bâtiments, une à chaque étage. L'emplacement est dicté par la distance maximale entre un Switch et un poste de travail, qui ne doit pas dépasser 100 mètres.

b. Les armoires de brassage existantes :

- **L'armoire de d'étage centrale (Fig.5)**

.Elle est constituée des éléments suivants :

- ✓ 02 panneaux de brassage à 16 ports : contiennent des connecteurs RJ45 (câble torsadé).
- ✓ 01 Switch d'étage Cisco : contient des ports RJ45 et des ports GBIC (pour câble fibre optique).
- ✓ 01 onduleur : pour avoir le temps à sauvegarder les données.

- ✓ 01 Switch fédérateur : contient 7 ports GBIC.
- ✓ 03 tiroirs optiques : qui relient les armoires des blocs.
- ✓ 01 Panneau électrique à 06 prises sous onduleur : pour alimenter les périphériques actifs.

Cette figue nous présente l'armoire d'étage centrale (fig. I.4)

Fig. I.4 L'armoire d'étage centrale

- **L'armoire de brassage (Fig. I.5)**

Elle est constituée des éléments suivants :

- ✓ 01 Switch Cisco.
- ✓ 01 panneau de brassage à 16 ports.
- ✓ 01 tiroir optique.
- ✓ 01 panneau d'alimentation

Fig. I.5 L'armoire de brassage

c. Description du système du serveur HP3000/A500 :

- **La face arrière (Fig. I.6):**

Le serveur est composé de DTC (Data Terminal Circuit) qui gère deux types de panneaux, DDP (Panneau de Distribution Direct) et MDP (Panneau de Distribution Modem). Les ports sur le DDP sont du type RJ45 (norme RS423) et numérotés de 100 à 115, 200 à 215 pour les ports écrans et de 300 à 315 pour les ports imprimantes.

Les ports sur le MDP sont du type DB25 (norme RS232) et numérotés de 400 à 415, 500 à 515 pour les ports écrans et de 600 à 615 pour les ports imprimantes.

La face arrière des ports DTC est composée des ports AUI et des ports BNC T (Thinlan port) et chacun de ces derniers sont connectés entre eux avec un câble coaxial qui est connecté à son tour au convertisseur Ethernet (10 base 2 to 10 base T). La sortie du convertisseur est un port RJ45 est connectée à l'armoire centrale.

Il est aussi équipé d'une unité centrale dont la face arrière est rassemblée de :

Console UPS port qui peut être connecté à 3 consoles sorties DB9 avec des câbles HP24252 (UPS : pour brancher l'onduleur) :

- ✓ Rempote : c'est une console secondaire, elle est mise en marche lorsque la console principale se bloque.
- ✓ Console principale.
- ✓ Une console LAN 10 base T (console réseau).

Le dérouleur : pour lire les cartes de l'ancien système.

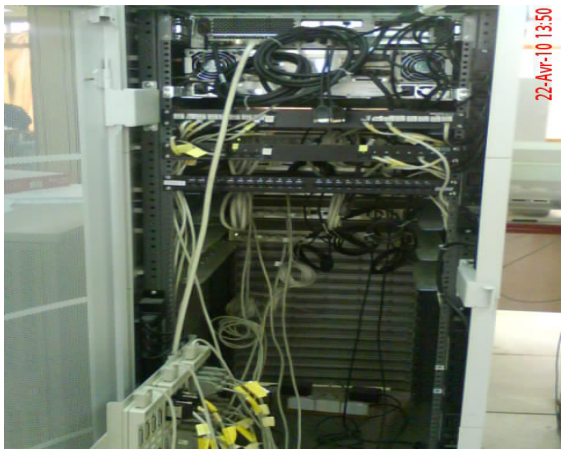


Fig. I.6 La face arrière

- **La face avant (Fig. I.7) :**

Elle est composée des éléments suivants :

- ✓ Lecteur de cassettes DLT.
- ✓ Lecteur DVD.
- ✓ Lecteur DDS.

Fig. I.7 La face avant

d. Caractéristiques matériels et logicielles

désignation	caractéristique
4PC hp Compaq	-system windows XP service pack 1 original -CPU Intel pentuim4 2,4G H_z -RAM DDR1 512Mo -disque dur 40Go
7PC hp Compaq	-system windows XP service pack 1 original -CPU Intel pentuim4 2,4G H_z -RAM DDR1 1Go - disque dur 80Go
1PC hp Compaq (serveur proxy)	-DDR RAM 1Go -CPU Intel pentuim4 2,4G H_z -disque dur 40Go
2PC Alfatron serveur de Domain Server de réplication	-system Windows 2003 serveur -CPU Intel core i3 -RAM DDR3 2Go -disque dur 300Go
1PC serveur de License solidworks	-system serveur 2003 -CPU Intel xeon / inside -RAM DDR3 6Go -disque dur 2To
Grand onduleur Emerson network power	Model: libert NXe20 Capacity: 20kva/16kw
2stations de climatisation airwelle	Model: INF3900A Courant → 380v
-Imprimante matriciel grand format - 1MAGNAL 820C (SEDCO) 3-PRINTRONIX PSA -imprimant matriciel Epson LQ-2080	Model : PRINTRONIX (P/N) P5205B-12 Mode in : SINGPORE Rating: 100-120/200-240v 50/60H_z 6/3A 400W

Tableau des Caractéristiques matérielles et logicielles

e. l'aspect logiciel :

Les différents logiciels utilisés :

- ✓ **Réflexion x :** est un émulateur d'accès au serveur depuis les différentes fonctions.
- ✓ **EASY** : est une application installée dans le serveur pour gérer la comptabilité des différentes unités.
- ✓ **COBOL :** L'engage de programmation avec lequel toutes les applications opérationnelles sont développées.
- ✓ **ACPAE** : Gestion de la paie (calcul de la paie).
- ✓ **Système MM0909 :** pour la pièce de recharge.
- ✓ **Système MM ref :** gestion de la production pour l'unité froid.
- ✓ **Système MM cuis** : gestion de la production pour l'unité cuisson.
- ✓ **Système achat :** tout ce qui est relatif à la fonction achat.
- ✓ **Système MM3000 pour la gestion de production :** il se charge de la production et tenue du stock des matières premières et pièces de recharges.
- ✓ **Gestion de la comptabilité** : on trouve la comptabilité clients, fournisseurs, générale, analytique, budget et d'autres.
- ✓ **Windows server 2008** installé sur le serveur
- ✓ **Windows 7** installé sur les autre machines clientes

IV. Présentation du Département Informatique de l'ENIEM

IV.1 Organigramme de département informatique :

Le département informatique se compose de deux services :

1) Service développement des systèmes informatiques (SDSI).
2) Service exploitation informatique (SEI)

Figure I.8: Organigramme de département informatique

IV.2 Aspect humain

IV.2.1 Chef de département :

Anime et contrôle tous les travaux de conception, de mise en place, maintenance et de développement des systèmes de gestion informatique des unités.

IV.2.2 Chef de service exploitation :

Il veille sur la gestion d'ensemble de moyens informatiques de saisie, de traitement de transmissions et de restitution de l'information, assiste les utilisateurs et interviens sur les incidents.

- **Agent maintenance et réseau informatique :**

Surveille le réseau et maintient la machine dans un état propre.

- **Le gestionnaire de système d'exploitation :**

Procède au chargement des énergies (air conditionné électricité via onduleur) des ordinateurs et du système d'exploitation.

IV.2.3 Chef de service développement système informatique :

La tache de ce poste consiste à assurer la maintenance des différents systèmes et leurs adaptations aux exigences nouvelles. Elle assure également le développement de nouveaux systèmes conformément au plan informatique.

- **Administrateur système informatique (comptabilité) :**

Sont rôle est de réaliser les différents programmes de l'application et ce par :

- ✓ Un découpage de l'unité de traitement en programme.
- ✓ Une écriture de programme dans la langue choisie.
- ✓ La mise au point des tests de contrôle, la correction et la finalisation de programme.
- ✓ Rédiger un dossier d'exploitation pour le compte de la structure concernée.
- ✓ Assiste les utilisateurs et suit le déroulement des phrases de lancement.
- ✓ Assiste les utilisateurs dans l'application dont il a la charge.
- ✓ Assiste sa hiérarchie dans l'élaboration et le maintien de la documentation.

- **Administrateur système informatique :(stock, pièce de rechange, gestion personnelle, etc)**

  Assurer l'analyse organique de l'étude, à savoir l'élaboration de la solution qui a été retenue par :

  - ✓ Une reprise de la chaîne fonctionnelle pour la découper en unité de traitement qui correspond à des programmes définissants pour chacune d'elles, un mode de stockage des programmes, fichiers, etc. et de l'enchaînement des opérations à effectuer.
  - ✓ La confection de dossier d'exploitation définissant les conditions
  - ✓ La maintenance des systèmes.

- **Administrateur système informatique : (paie)**

  Assure l'étude de l'application et rend compte à sa hiérarchie.

  Assure l'analyse fonctionnelle du projet conformément au planning de réalisation préétabli par la hiérarchie par :

  - ✓ Une étude approfondie du cahier des charges (choix de méthodes d'analyse, flux, et diagramme d'information, production de données et élaboration d'un dictionnaire de données, élaboration de la base de données, et élaboration de procédure.
  - ✓ Un découpage de l'application en module simple de manière à facilité la compréhension de l'écriture, l'exploitation et la maintenance des programmes.
  - ✓ L'établissement d'un dossier d'analyse qui comporte l'objet de l'application et la solution technique.

V. Conclusion :

Dans ce chapitre, les ressources constituants le réseau informatique de l'ENIEM ont été décrites, ainsi force est de constater que le département informatique joue un rôle colossale dans le raccordement des activités de cette entreprise. Du bloc administratif aux ateliers de fabrication, le département informatique est présent pour tous et répond aux besoins de tout un chacun par le biais d'un réseau informatique mis en place qui sera abordé tout au long de ce projet à travers les chapitres qui suivent.

Chapitre II: Généralités sur les Réseaux Informatiques

II.1 Introduction :

Les technologies informatiques ont acquis une place importante dans le quotidien, les activités professionnelles ainsi que le temps libre de chacun. Les ordinateurs permettent de stocker une grande quantité de données et d'y effectuer une variété de tâches. De nouveaux appareils apparaissent sur le marché et élargissent l'utilisation des informations numériques.

Ce progrès fournit de nouvelles façons de communiquer et de travailler, basées sur l'échange des informations entre machines (personnes) distantes d'une manière rapide et sure.

Les réseaux sont nés à cause du volume et de la diversité des informations à échanger qui ne cessent de croitre.

Actuellement les réseaux informatiques permettent l'interconnexion de tous types d'ordinateurs : de gros serveurs, des stations de travails, des ordinateurs personnels ou de simples terminaux graphiques, à l'aide de support de plus en plus variés, câbles, fibre optique, air. Aujourd'hui, les réseaux se retrouvent à l'échelle planétaire. Le besoin d'échanger de l'information est en pleine évolution.

Dans ce chapitre, les concepts de base des réseaux informatiques sont abordés dans les lignes suivantes :

II.2 Définition d'un réseau:

Un réseau est un ensemble d'équipement (ordinateurs, stations de travail, cartes réseaux, modems, imprimantes réseaux, liaison téléphonique,…), interconnectés les un aux autres, grâce à des liaisons de communication filaires (câbles réseau, fibre optique, …) ou non filaires (ondes radio, antenne…) et échangeant des informations sous formes de données numériques suivant des règles bien définies.

II.3 Objectifs des Réseaux :

Le rôle du réseau est l'acheminement des données entre les stations terminales ou hôtes. Le réseau est constitué de nœuds interconnectés entre eux par des liens. Les nœuds du réseau remplissent les deux fonctions élémentaires suivantes :

- **la transmission**: cette fonction permet l'adaptation des données à transmettre sur le

support de transmission (paire métallique, fibre optique, air);

- **la connectivité:** cette fonction permet le transfert des données entre une entrée et une sortie du nœud du réseau.

L'utilisation des réseaux informatiques répond aux besoins de **partages des ressources**, c'est-à-dire, de rendre accessibles à chaque membre du réseau les programmes, les données et les équipements indépendamment de leur localisation physique. Tout en garantissant l'unicité de l'information lors des mises à jour des bases de données. Cette utilisation conduit à une communication et une organisation plus efficace.

Un autre avantage est la **réduction des couts**. Il est évident que le partage de périphériques entraine directement une réduction des couts. Il faut aussi constater que les petits ordinateurs ont un meilleur rapport prix/performances que les gros.

D'autres avantages des réseaux: la possibilité d'augmenter graduellement les performances du système par adjonction de processeurs lorsque la charge de travail croit, avec le modèle client/serveur, on peut ajouter à volonté de nouveaux clients ou de nouveaux serveurs.

II.4 Classification des Réseaux informatiques :

La classification est faite selon des critères bien déterminées qui se base sur l'étendue du réseau, sa topologie et selon la commutation des données.

3.1. Selon l'étendue :

On distingue différents types de réseaux selon leur taille (en termes de surface couverte), On fait généralement les catégories de réseaux suivantes:

3.2. Réseau PAN (Personnel area network) :

La plus petite étendue de réseau .Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, en utilisant les technologies sans fil telles que Bluetooth ou infra rouge.

3.3. Réseau LAN (Local area network) :

Ces réseaux s'étendant sur quelques mètres à quelques kilomètres, reliés entre eux des ordinateurs, des serveurs
se trouvant dans zone géographique relativement petite, appartenant à une même entreprise ou établissement.
Les réseaux locaux sont généralement des réseaux à diffusion car toutes les machines les constituants sont reliées à une même liaison.
La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps et 1 Gbps.
Ex: Ethernet, Token-ring, wifi.

3.4. Réseau MAN (Métropolitain area network):

Les réseaux métropolitains sont des réseaux qui sont généralement utilisés pour interconnecter un ensemble de réseaux locaux géographiquement dispersés, et peuvent couvrir une circonscription géographique importante, un grand campus ou une ville.

Ex: INTERANET, WI-MAX, FDDI, ATM

3.5. Réseau WAN (Wide area network):

Un réseau WAN assure généralement le transport d'information sur de grande distance. C'est un réseau public déployé par des opérateurs ou fournisseurs de service, qui assure l'interconnexion des LAN. Le réseau WAN est constitué de réseaux d'accès, de réseaux d'agrégation et d'un cœur de réseau. Le plus connu des WAN est Internet, les débits offerts par ces réseaux vont de quelques Kbit/s.
Ex: X25, INTERNET, SATELLITE, ATM

1m 10m 100m 1km 10km 100km

Figure II.1 Classification des réseaux informatique selon leurs tailles

NB : Les autres classifications sont entre autres la classification selon la topologie physique (en étoile, en anneau, en bus) et logique (commutation de circuit, de messages, de paquets).

II.5 Le Modèle OSI :

1. Introduction

La problématique liée aux Réseaux informatiques sont extrêmement nombreux, et les moyens, solutions et protocoles permettant d'y répondre sont presque tout aussi nombreux parmi lesquels, nous pouvons citer entre autre le problème d'évolutivité, de meilleures compatibilité et interopérabilité entre les diverses technologies liées aux réseaux informatiques, ce pendant il est nécessaire d'organiser, de structurer et hiérarchiser voir standardiser les moyens technologiques associées aux réseau informatiques, d'où la naissance du **Modèle OSI**.

La plupart des systèmes de communication sont construits selon une architecture en couches c'est-à-dire une segmentation en plusieurs niveaux empilés l'une sur l'autre, qui ont chacune des finalités différentes mais participent tous à la transmission de la communication entre plusieurs nœuds.

2. Définition

Le modèle **OSI (Open System interconnexion**) est un modèle générique et standard d'Architecture d'un Réseau en 7 couches, élaboré par l'organisme **ISO (International Standardization Organisation)** en 1984, afin de normaliser la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau.

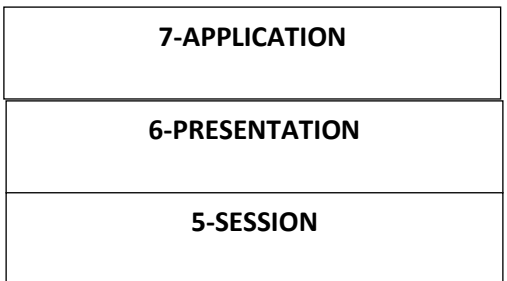


Figure II.2: Schéma des couches OSI

3. Transmission des données à travers le Modèle OSI :

La transmission des données à travers le Modèle OSI utilise le principe de communication virtuelle en utilisant les interfaces inter-couches, il y a donc encapsulation des données à chaque interface 'H : Header (entête), T : Trailer (en-queue) dont voici une illustration qui explicite ce processus d'encapsulation au niveau de chaque couche.

NB :

Entête et En-queue : C'est l'ajout des informations à celles fournies par la couche précédente, ces informations sont appelées Entête, si elles sont rajoutées devant ou En-queue, si elles sont rajoutées à la fin.

Encapsulation : Les informations d'une couche sont insérées dans la couche suivante entant que données, ce phénomène se répète de couche en couche et il est appelé encapsulation, l'inverse de ce processus est appelé décapsulation.

AH : entête application	**RH** : entête réseau
PH : entête présentation	**LH** : entête liaison de données

SH : entête session	**TH** : en-queue de la liaison de données
TH : entête transport	**PH** : entête Physique

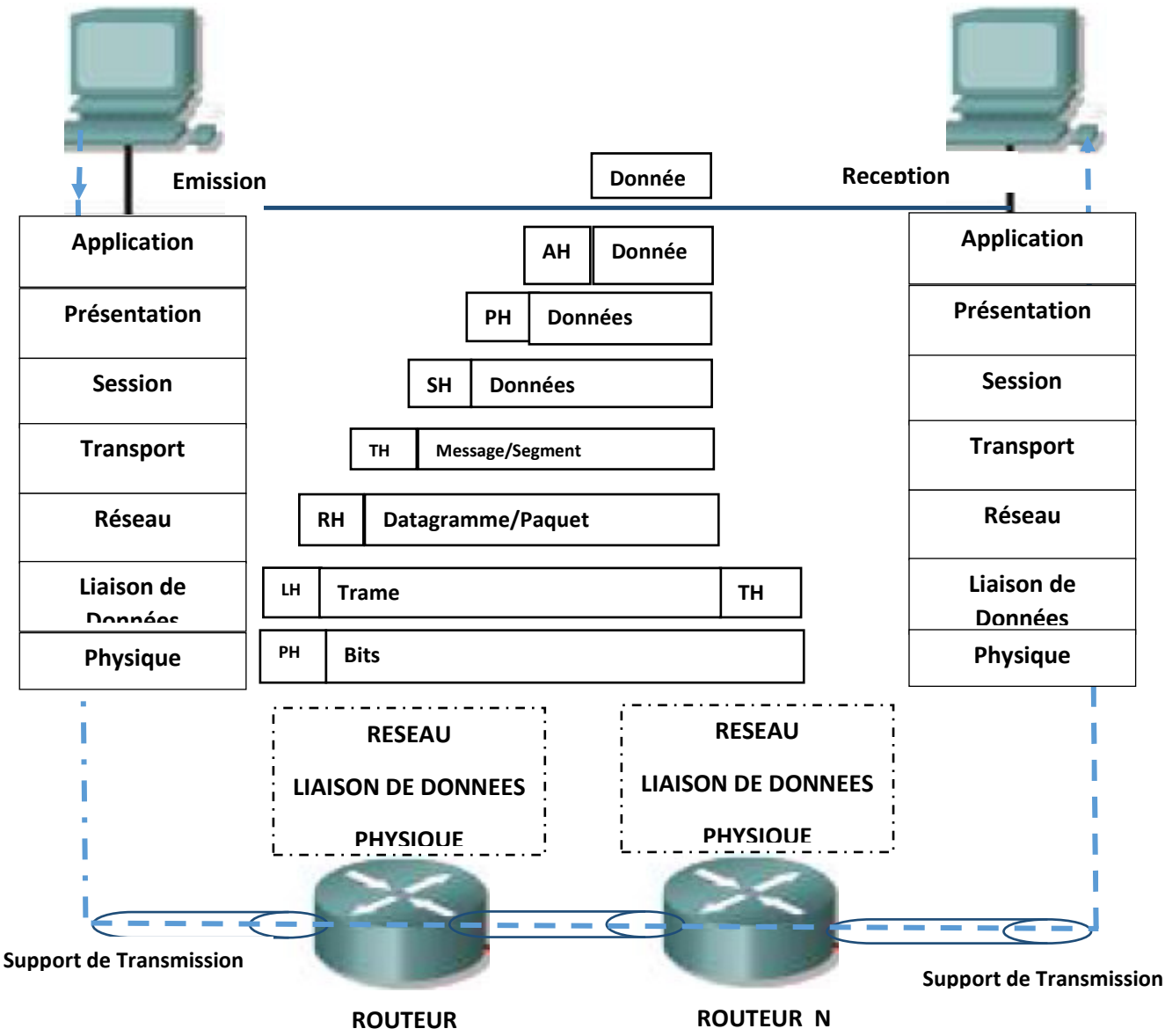


Figure II.3: Transmission des données à travers le Modèle OSI

4. Description résumée de chaque couche :

Couche 7 : Application

Elle ne contient pas les applications utilisateurs, mais elle assure des communications à l'aide des processus, entre les couches inférieurs et les applications utilisateurs (transfert de fichiers, courriers électroniques, elle fournit des services et des interfaces de commutation aux utilisateurs.

Quelques protocoles associés : DNS, TFTP, Telnet,FTP (File Transfert Protocol),TFTP (Trivial File Transfer Protocol) SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), HTTP (HyperText Transfer Protocol).

Couche 6 : Présentation

Elle assure la mise en forme des données, la conversion des codes (ASCII, ebcdic…), si nécessaire pour délivrer à la couche application un message dans une syntaxe compréhensible, elle peut aussi assurer le cryptage et la compression des données.

Quelques protocoles associés : ASCII, EBCDIC, MIDI, MPEG, PICT, TIFF, JPEG.

Couche 5 : Session

Elle assure l'échange des données, transaction entre deux applications distantes, elle assure surtout la synchronisation et le séquencement de l'échange par la détection et la reprise de celui-ci en cas d'erreur, cette gestion du dialogue et de synchronisation permet l'ouverture et la fermeture des sessions (communication).

Quelques protocoles associés : Le système NFS (Network File System), Le langage d'interrogation structuré (SQL), L'appel de procédur.e distant (RPC)

Couche 4 : Transport

Elle assure le contrôle de transfert de bout à bout des informations entre deux (2) systèmes d'extrémités, afin de rendre le transport transparent pour les couches supérieures, elle assure le découpage des messages en paquets pour le compte de la couche réseau et les reconstitue pour les couches supérieures en contrôlant ainsi la cohérence de la transmission.

Quelques protocoles associés : TCP ou UDP

Couche 3 : Réseau

Elle assure l'acheminement, le routage (choix du chemin à parcourir à partir des adresses) afin de transmettre les paquets de manière indépendante l'information ou des différents paquets la constituant en prenant en compte en temps réel le trafic, cette couche assure aussi un certain nombre de contrôle de congestion qui ne sont pas gérés par la couche liaison de données entre les deux systèmes d'extrémités, à travers les relais, et elle définit la taille des paquets.

Quelques protocoles associés : IP, IPX, ICMP, ARP, RARP, Ping, Traceroute.

Couche 2 : Liaison de Données

Elle assure, le maintien de la connexion logique, le transfert des blocs de données (les trames et les paquets), la détection et la correction des erreurs dans ceux-ci, son rôle principal est de fournir à la couche supérieure (couche réseau) un moyen de communication fiable sans erreurs de transmission, en assurant un contrôle de flux de données, de l'adressage physique, un transfert fiable des données, détection des erreurs de transmission et reprise.

Quelques protocoles associés : IEEE 802.2, 802.3, 802.5, PPP, HDLC.

Couche 1 : Physique

Elle assure l'établissement et le maintien de la liaison physique, elle gère la communication avec l'interface physique afin de faire transiter ou de récupérer les données sur le support de transmission, qui peut être électrique, mécanique, fonctionnel ou procédural.

Quelques protocoles associés : IEEE 802.3, 802.5, Ethernet, carte réseau (connecteurs physiques - BNC, AUI, RJ-45, etc.), médias (câble coaxial, câble à paires torsadées non blindées, fibre optique), répéteur, concentrateur, ETCD et ETTD, bits, codage.

II.6 Le Protocole TCP/IP:

1. Définition

Le protocole TCP/IP, développé originellement par le ministère de la défense Américain en 1981, propose l'évolution de concepts déjà utilisés en partie pour le réseau historique ARPNET (1972), et est employé en très forte proportion sur le réseau internet , au-delà de son aspect historique, TCP/IP doit aussi son succès à son indépendante vis-à-vis de tout constructeur informatique.

En réalité, TCP/IP définit une suite de divers protocoles probabilistes, appelé aussi modèle DOD (Département of Défense), pour la communication sur un réseau informatique, notamment le protocole TCP (Transmission Control Protocol) et le protocole IP (Internet Protocol) qui sont parmi les principaux protocoles de ce modèle.

Ce qu'on entend par "modèle TCP/IP", 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.

Modèle TCP/IP

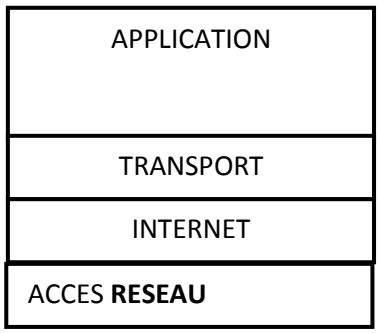


Figure II.4: Modèle TCP

2. Comparaison entre le Modèle OSI et le Modèle TCP/IP

Comme le montre la figure II.4, le modèle TCP-IP n'est constitué que de 4 couches. Ce sont des couches d'abstraction, c'est-à-dire, ce sont des couches qui cachent les détails d'implémentation de la communication et leurs noms ne veulent pas forcément dire ce qu'elles font mot pour mot :

- Le modèle OSI quant à lui est constitué de 7 couches distinctes. Les trois premières couches du modèle OSI correspondent à la couche applicative du modèle TCP-IP.

- Tous les deux modèles ont une couche de transport, la couche réseau du modèle OSI correspond à la couche Internet du modèle TCP-IP.

- Les couches liaisons de données et physique du modèle OSI forment une seule couche pour le modèle TCP-IP : Accès réseau.

- Les couches Application, Présentation, Session et Transport sont dites « couches hôtes (**Host layers** en anglais)», en d'autres termes se sont des couches qui « concernent » les hôtes directement. Tandis que les couches Réseau, Liaison et Physique sont des couches de médias (**Media layers**), elles sont plus liées au média qu'à l'hôte directement.

- Voici un schéma de comparaison entre les deux modèles :

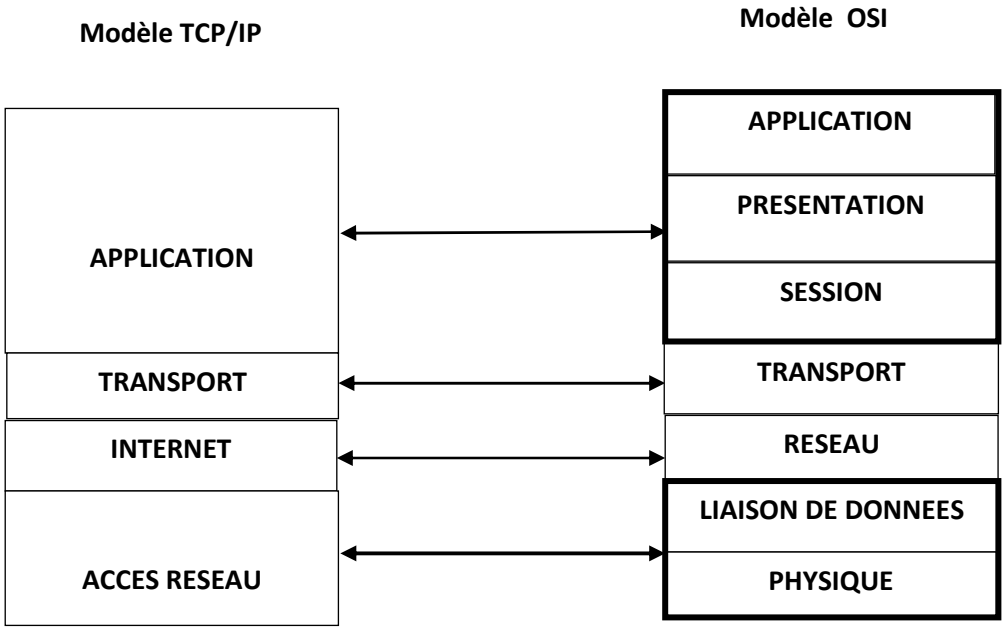


Figure II.5: Comparaison entre les deux Modèles OSI et TCP/IP

3. Les Protocoles TCP, UDP, IP :

Protocole TCP

Le protocole TCP (transmission control Protocol) : fournit un protocole fiable, orienté connexion, au-dessus d'IP, il assure les services attendus de la couche transport du Modèle TCP/IP, son rôle est donc le fractionnement et réassemblage en paquets des segments de données qui transitent via le protocole IP, de garantir l'ordre et la remise des paquets, de vérifier l'intégralité des données qu'ils contiennent.

Afin de fiabiliser la communication, le TCP doit aussi réordonner les paquets avant de les assembler, et doit aussi gérer les paquets erronés et perdus, pour cela TCP fonctionne en

mode connecté en utilisant deux mécanismes mettant en œuvre un principe de synchronisation/question/réponse/confirmation, ce protocole exige également que le destinateur accuse réception de données.

Protocole UDP

Le protocole UDP (User Data Protocol) est un complément du protocole TCP qui offre un **service de datagrammes sans connexion** qui ne garantit ni la remise ni l'ordre des paquets délivrés, pas de réassemblage en paquets des segments de données qui transitent via IP, ce pendant UDP n'assure aucun autre service supplémentaire, pas de ré ordonnancement, pas de suivi de la communication à l'aide d'accusé de réception, pas de control de flux.

Le Protocole UDP fonctionne en mode non connecté, c'est-à-dire qu'il ne garantit pas la transmission des données, et c'est alors à l'application qui communique via UDP de gérer éventuellement les problèmes de pertes, de duplication, de retard.

Protocole IP

Le Protocole IP (Internet Protocol), assure le service attendu de la couche du réseau du modèle TCP/IP, son rôle est donc de gérer de l'acheminement des paquets (issus de la couche transport) entre les nœuds de manière indépendant.

Le Protocole IP offre un fonctionnement non fiable et sans connexion, à base d'envoi/Réception de datagrammes flux de bits structurés).

- **Non fiable** : absence de garantie que les datagrammes arrivent à destination, les datagrammes peuvent être perdus, retardé, altérés ou dupliqués sans que ni la source ou la destination ne le sachent, on parle de remise au mieux (**Best effort delivery**)

- **Sans connexion** (mode non connecté) : chaque datagramme est traité et donc acheminé de manière totalement indépendante des autres.

- **Schéma du Datagramme IP**

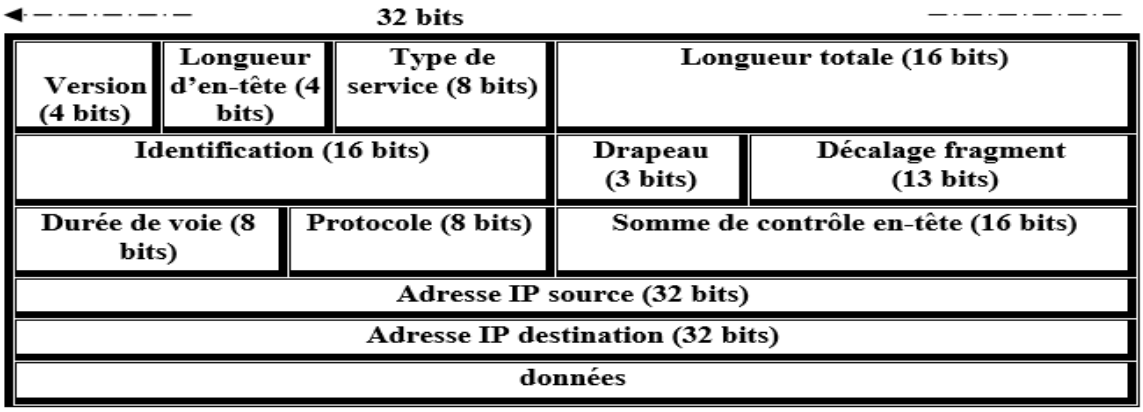


Figure II.6: Structure du Datagramme IP

II.7 Adressage IPV4 :

Dans sa version 4, IP définit une adresse sur 4 octets. Une partie définit l'adresse du réseau (Net ID ou Subnet ID suivant le cas), l'autre partie définit l'adresse de l'hôte dans le réseau (Host ID). La taille relative de chaque partie varie suivant la classe choisie.

Les classes d'adresses :

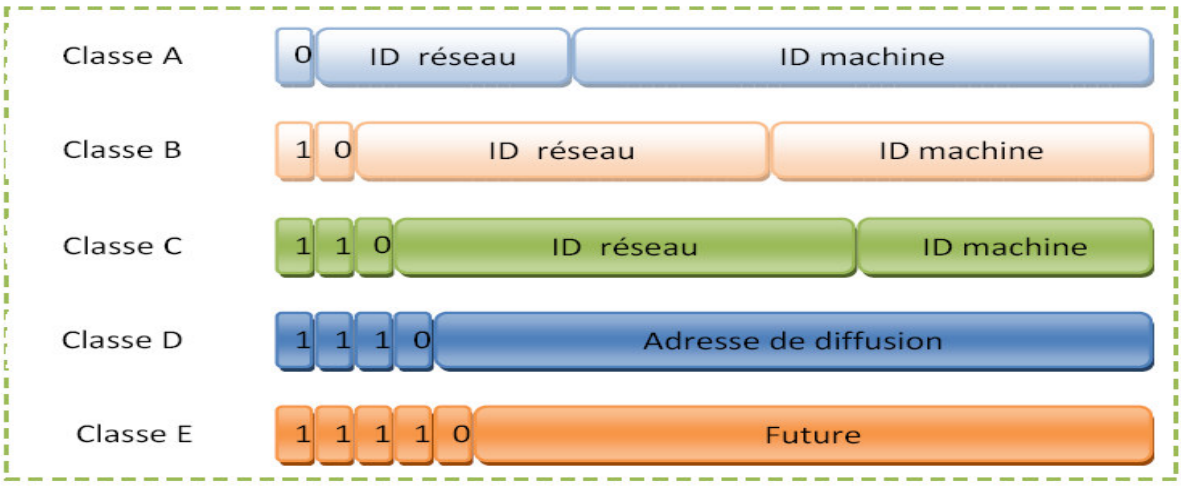


Figure II.7 : les cinq classes d'adresses IP.

Les adresses "privées" :

Les adresses suivantes (RFC 1918) peuvent également être librement utilisées pour **monter un réseau privé** :

Classe A : 10.0.0.1 à 10.255.255.254

Classe B : 172.16.0.0 à 172.31.255.254

Classe C : 192.168.0.0 à 192.168.255.254

Aucun paquet provenant de ces réseaux ou à destination de ces réseaux, ne sera routé sur l'Internet.

Exemple:

Soit l'adresse IP suivante : 192.168.149.0

Le Masque de sous Réseau :

Le masque permet de segmenter de la façon la plus correcte l'adresse du réseau, et ainsi de séparer les machines sensibles du reste du réseau, et prévoir l'évolution du réseau.

A chaque classe d'adresses, est associé un masque de réseau de réseau, ou netmask, qui est constitué de 32 bits. Le tableau suivant fournit l'espace d'adressage d'IPV4 et le masque par défaut des trois classes traditionnelles.

Nom de la classe	Plage d'adressage	Masque par défaut
Classe A	0.0.0.1 à 126.255.255.254	255.0.0.0
Classe B	128.0.0.1 à 191.255.255.254	255.255.0.0
Classe C	192.0.0.1 à 192.223.255.255	255.255.255.0

Adresses réservées :

L'adresse d'acheminement (route par défaut) : est de type 0.X.X.X.

Tous les paquets destinés à un réseau non connu, seront dirigés vers l'interface désignée par 0.0.0.0, elle est également l'adresse utilisée par une machine pour connaitre son adresse IP durant une procédure d'initialisation (DHCP).

L'adresse de bouclage (*loopback*): l'adresse de réseau 127 n'est pas attribuée à une société, elle est utilisée comme adresse de bouclage dans tous les réseaux. Cette adresse sert à tester le fonctionnement de votre carte réseau.

L'adresse de réseau : est une adresse dont tous les bits d'hôte sont positionnés à 0 (ex 128.10.0.0 adresse de réseau du réseau 128.10 de classe B). Elle est utilisée pour désigner tous les postes du réseau. Cette adresse est utilisée dans les tables de routage.

L'adresse de diffusion : est une adresse dont tous les bits d'hôte sont positionnés à 1 (ex : 128.10.255.255 adresse de diffusion du réseau 128 de classe B).

Elle est utilisée pour envoyer un message à tous les postes du réseau.

II.8 Conclusion :

Ce chapitre est consacré à l'étude générale sur les réseaux informatiques. Les réseaux peuvent être divisés en LAN, MAN, WAN, ce sont des réseaux d'interconnexion dont chacun d'eux ayant ses caractéristiques propres selon des topologies spécifiques, leurs méthode d'accès et aussi les modes de connexion, ainsi que les supports de transmission utilisés. L'utilisation de réseaux d'ordinateurs partageant des serveurs apporte une grande souplesse. Pour les individus les réseaux permettent l'accès à de très nombreuses ressources.

Chapitre III : Concepts de Base de la Sécurité Réseau

III.1 Introduction :

Les réseaux informatiques deviennent de plus en plus complexes, dynamiques et hétérogènes. Cette situation a d'énormes conséquences sur leur sécurité. D'où la nécessité d'accorder une attention particulière à la sécurisation des réseaux informatiques. Toutefois, il est estimé que la plupart des malveillances informatiques ont une origine ou complicité interne aux organismes. Il faut notamment protéger l'accès et la manipulation des données et autres ressources du réseau par des mécanismes d'authentification, d'autorisation et de contrôle d'accès.

Ce chapitre défini le terme de sécurité Réseau ainsi que les méthodes des attaques utilisées et les différents mécanismes de défense.

III.2 Définition de la sécurité Réseau

L'ensemble des données et des ressources matérielles et logicielles d'une entreprise représente un patrimoine essentiel de celle-ci, il convient donc de les protéger, et c'est à ce point qu'intervient la sécurité Réseau.

III.3 Objectifs de la sécurité Réseau

La sécurité Réseau a pour objectif de mettre en place et maintenir l'ensemble des moyens techniques et humains permettant de garantir que les ressources informatiques, et en particulier les données manipulées par celles-ci, seront disponibles en tout instant et que les

personnes autorisées pourront les accéder et les modifier, dans ce cas, on doit toujours s'assurer qu'à tout instant les services de sécurité suivants sont vérifiés:

- **La confidentialité** : La confidentialité est un service de sécurité qui consiste à s'assurer que seules les personnes autorisées peuvent prendre connaissance d'un ensemble de données.

- **L'intégrité des données**: L'intégrité est la capacité de protéger les données contre toute modification non autorisée. Garantir l'intégrité des données assure au récepteur que les données reçues sont celles qui ont été émises.

- **Authentification** : L'Authentification est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée.

- **La non-répudiation** : Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est-à-dire aucun des correspondants ne pourra nier l'envoi ou la réception du message.

- **Disponibilité (availability) :**c'est la prévention de rétention non autorisée d'information ou de ressources, C'est donc la garantie que les données sont disponibles dans les conditions normales de temps, de délai et de performance définies.

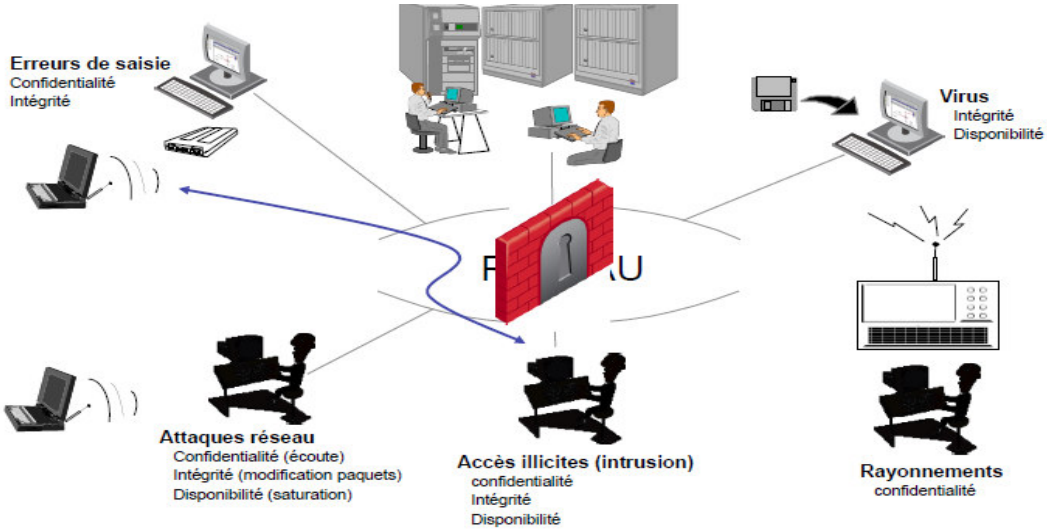


Figure III.1 : Objectif de la Sécurité Réseau

III.4 Présentation de l'insécurité informatique

III.4.1 Les types de pirates informatiques

Le carder : Le carder est impliqué dans la réalisation de fausses cartes bancaires.

Le phreaker : Le phreaker est spécialisé dans le vol d'unités téléphoniques dans les autocommutateurs.

Le hacker : Le hacker est un expert des systèmes d'exploitation. Il cherche à mettre en évidence les points faibles des systèmes mais s'interdit leur exploitation malveillante.

Les crackers : Beaucoup moins scrupuleux que les hackers, Les crackers n'hésitent pas à utiliser les points faibles des systèmes à des fins nuisibles.

III.4.2 Les programmes malveillants (malware) :

C'est un logiciel développé dans le but de nuire à un système informatique. Voici les principaux types de programmes malveillants :

- ✓ **Le virus** : Programme se dupliquant sur d'autres ordinateurs.
- ✓ **Le ver** : Exploite les ressources d'un ordinateur afin d'assurer sa reproduction.
- ✓ **Le Cheval de Troie** : Programme à apparence légitime qui exécute des routines nuisibles sans l'autorisation de l'utilisateur.

III.4.3 Vulnérabilité :

Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitées par une menace.

III.4.4 Menaces :

Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité

III.4.5 Sinistres (Impact) :

Est le résultat (pertes et dommages) de la concrétisation de risque.
Exemple : altération des données, panne d'équipement informatique.

III.4.6 Contre-mesure :

La contre-mesure est un ensemble d'actions ou outils matériels ou logiciels permettant de sécuriser un système face aux menaces.

III.4.7 Risque :

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système. Traiter le risque c'est prendre en compte les menaces et les vulnérabilités

III.4.8 Attaques :

Afin de pouvoir « **Attaquer** » un serveur, il est nécessaire de savoir quels sont les services qu'il octroie, pour les connaitre, il est possible d'utiliser un mappage des ports nommés aussi appelé « **Scan** » de ports ; une fois ces ports sont connus, on peut alors lancer diverses attaques dont nous verrons plus tard quelques standards :

1. Définition

Une attaque est toute action compromettant la sécurité de l'information, C'est la réalisation d'une menace ; C'est une atteinte à l'une des composantes de la sécurité suivante :

- Confidentialité : divulgation des données ;
- Intégrité : Falsification ou modification des données ;
- Disponibilité : dénis de service

2. Quelques attaques :

- **Un virus :** un virus est un petit code dans celui de l'application ciblée qui va exécuter des opérations plus ou moins destructrices sur votre machine.
  Les virus existent depuis que l'informatique est née et se propageaient initialement par disquettes de jeux ou logiciels divers...

  Une fois implanté sur son programme hôte, le greffon possède aussi en général la capacité de se recopier sur d'autres programmes, ce qui accroît la virulence de l'infection et peut contaminer tout le système (modification, destruction de fichiers, effacement du disque dur, allongement des temps de traitement, manifestations visuelles ou sonores plus ou moins inquiétantes, etc…

- **Les sniffers :**

Un sniffer est un petit dispositif, logiciel ou matériel, qui permet de "voir" les informations qui transitent par la machine où il se trouve. Il ne sert pas seulement à capturer le texte saisi sur la machine mais toutes les informations provenant des machines du réseau passant par la machine en question.

- **Intrusion :**

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques :vol, fraude, incident diplomatique, chantage…

- **Déni de Service (DoS, Denial of Service) :**

Une attaque en déni de service consiste à bloquer une machine cible en lui envoyant des requêtes inutiles. Cela l'empêche de rendre le service pour lequel on l'a installée. L'attaque la plus simple est l'inondation par des ping (messages ICMP Echo Request) ou des messages ICMP avec beaucoup de données forçant les différents intermédiaires à traiter la fragmentation. La machine cible passe son temps à répondre aux sollicitations reçues et n'a plus de disponibilité pour son propre service.

- **Les chevaux de Troie :**

Un cheval de Troie est un programme qui se cache dans un autre Programme apparemment au-dessus de tout soupçon. Quand la victime lance ce programme, elle lance en même temps le cheval de Troie caché.
Un chevale de Troie peu faire :

- ✓ voler des mots de passe ;
- ✓ copier des données sensibles ;
- ✓ exécuter toute autre action nuisible.

- **social engeneering :**

En utilisant les moyens usuels (téléphone, email…) et en usurpant une identité, un pirate cherche à obtenir des renseignements confidentiels auprès du personnel de l'entreprise en vue

d'une intrusion future. Seule une formation du personnel permet de se protéger de cette attaque.

III.5 Politique de sécurité :

1. Définition :

Une politique de sécurité d'un réseau est un ensemble de règles visant à protéger ses ressources d'éventuels incidents de sécurité dommageables pour son activité. Elle détermine pour chaque action entreprise si elle doit être autorisée ou non. **[III.1]**

III.6 Mécanismes de défense :

Pour s'assurer que seules les personnes autorisées ont accès à l'information et que le service est rendu correctement, un ensemble de mécanismes doivent être mis en place. Parmi ces mécanismes, on peut citer:

1. La cryptographie:

La cryptographie est une science qui étudie les outils servant à sécuriser les informations. De tout temps, l'art du chiffrement-déchiffrement a été employé. Le chiffrement et le déchiffrement des données sont effectués par des algorithmes cryptographiques. Ces algorithmes reposent généralement sur des problèmes mathématiques complexes, difficiles à résoudre, tels que la factorisation des nombres premiers, les logarithmes discrets, etc. Il existe deux grands types d'algorithmes cryptographiques, ceux dits symétrique ou à clé secrète et ceux dits asymétrique ou à clé publique.

a. Le cryptage symétrique :

Le cryptage à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryption Standard) AES, IDEA et RSA.

b. Cryptage asymétrique :

Ce n'est pas la même clé qui crypte et qui décrypte les messages. L'utilisateur possède une clé privée et une clé publique. Il distribue sa clé publique et garde secrète sa clé privée. Dans ce type d'application, tout le monde peut lui écrire en utilisant la clé publique, mais seul l'utilisateur destinataire pourra décrypter et donc lire le message avec sa clé privée.

3. Authentification :

L'authentification est la procédure mise en œuvre notamment pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée.

4. Mots de passe :

Le moyen le plus simple et le plus classique de s'assurer que seules les personnes autorisées peuvent accéder à une certaine partie du réseau est de protéger certaines zones du réseau par un mot de passe.

5. Certificats numériques :

Les certificats numériques sont généralement utilisés à des fins d'identification, lors de l'établissement de tunnels sécurisés sur Internet, comme c'est le cas dans les réseaux virtuels privés (VPN) et sont émis par une autorité de certification.

6. Réseau privé virtuel (VPN) :

On désigne par réseau privé virtuel (VPN, Virtual Private Network) un réseau d'entreprise sécurisé, constitué de plusieurs sites reliés par Internet. La traversée d'Internet est vue comme un tunnel, dans lequel les données de l'entreprise sont chiffrées et transitent d'un bout à l'autre. Pour mettre en œuvre ce mécanisme de tunnel, on utilise un protocole spécial pouvant assurer plusieurs services selon les besoins de l'entreprise : confidentialité, intégrité des données, authentification des machines d'extrémité. Le principal protocole de tunnel est utilisé au niveau réseau : il s'agit d'IPSec (IP Security), cette solution est modulaire et situe la sécurité au niveau de la couche Transport 7.

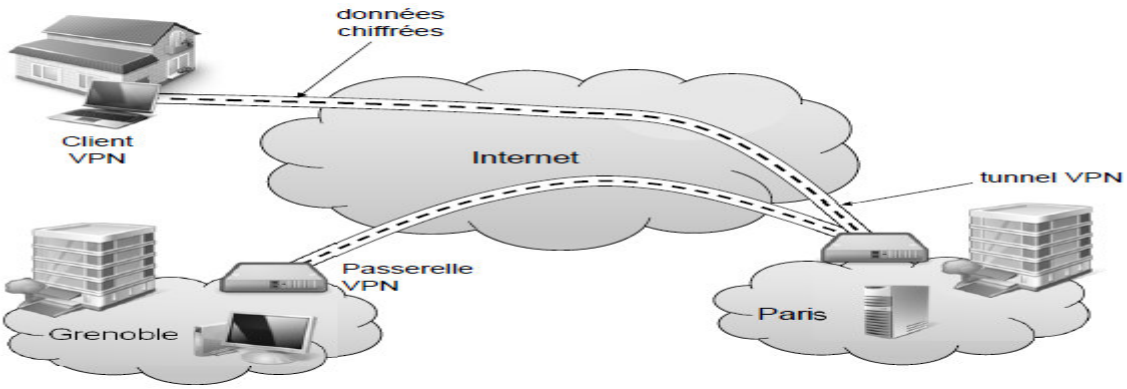


Figure III.2: Réseau Privé Virtuel

7. Antivirus : [III.1]

Ces derniers sont des programmes contenant une base de données de tous les codes malicieux connus (base antivirale)**,** qui permettent donc de détecter, de supprimer et éventuellement de réparer les fichiers infectés par les virus.

Les anti-virus utilisent trois techniques pour la détection qui sont : Sondage de virus : (le scanning), Vérificateurs d'intégrité, Vérificateurs de comportement.

8. Pare-feu :

En fait, le mot **pare-feu** souvent utilisé un peu abusivement, signifie qu'on instaure une série de protections en un point particulier entre deux entités connectées, en l'occurrence entre Internet et le réseau interne d'une entreprise.

Le pare-feu est un système aux fonctions de filtrage évoluées. Chaque paquet reçu est examiné, une décision de rejet ou d'acceptation est prise en fonction de nombreux critères :

- Adresse source.
- Adresse destination.
- Port source.
- Port destination.
- Le protocole transporté (ICMP, UDP...).
- La valeur de certains flags (ACK, SYN...).

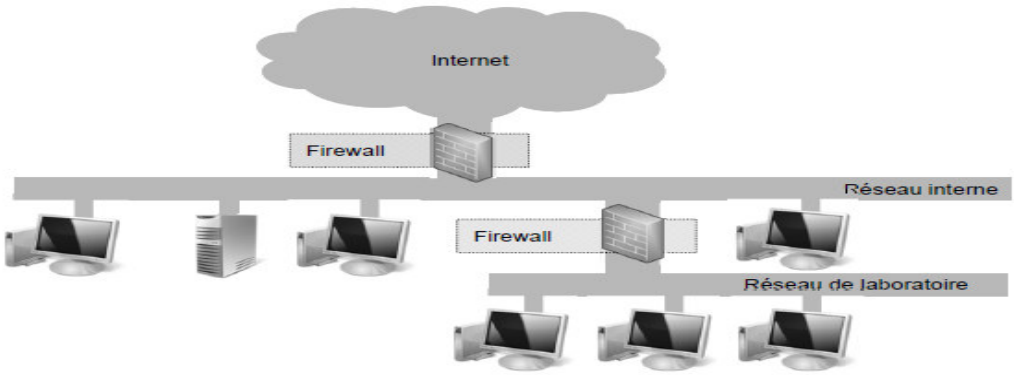


Figure III.3 : Firewalls hiérarchiques

L'architecture la plus en vogue actuellement est basée sur une « **zone démilitarisée** » Communément appelée DMZ (Demilitarized zone).

Elle consiste à placer un réseau Intermédiaire entre l'accès Internet et le réseau interne (éventuellement plusieurs). Cette DMZ sera isolée, aussi bien vis à vis de l'Internet que du réseau local, par des systèmes de filtrage (filtres de paquets). Ensuite, les éventuels serveurs nécessaires à l'entreprise devant continuer à être accessibles de l'extérieur seront connectés directement sur cette DMZ, de manière à les séparer du réseau interne, Par exemple, on pourra y trouver un serveur Web, un serveur DNS, un serveur de mails, un serveur FTP...

Dans le cas où l'un de ces serveurs serait compromis, le filtrage entre la DMZ et le réseau interne doit être capable en plus d'assurer une protection suffisante.

Bien évidemment, cette architecture doit être adaptée plus précisément à la structure d'une entreprise précise, et éventuellement intégrer des composants supplémentaires, tels que des proxys et autres dispositifs.

9. Système de détection d'intrusions :

Un système de détection d'intrusions est un dispositif matériel et/ou logiciel de surveillance permettant de repérer des activités anormales ou suspectes sur la cible analysée, en déclenchant un avertissement, une alerte, sans pour autant les bloquer, à l'inverse d'un système de prévention d'intrusion qui a la capacité de bloquer ou de supprimer les paquets suspects.

III.7 Les protocoles de sécurité :

1. **Protocole SSL (Secure Socket Layer) ou TLS (Transport Layer Security):**

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

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité.

2. Le protocole SSH (Secure Shell):

Le protocole **SSH** est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau).

3. S-HTTP (Secure HTTP) :

S-HTTP est un procédé de sécurisation des transactions http reposant sur une amélioration du protocole HTTP. Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle.

4. Le protocole IPSec :

IPSec est le principal protocole pour la création des tunnels, il est de niveau 3 du modèle OSI, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux

IP. IPSec a d'autres avantages que la sécurisation du trafic, il permet par exemple d'économiser la bande passante grâce à la compression des en-têtes des paquets. Il fonctionne sous deux modes :

- **Mode transport :** il encrypte directement les échanges entre les deux machines.
- **Mode tunnel :** il encapsule les paquets encryptés dans de nouveaux entêtes IP. Il est conçu pour les passerelles VPN

III.8 Conclusion

Plusieurs risques liés à la sécurité ont augmenté. Chaque nouvelle pratique vient avec de nouvelles menaces d'où l'importance d'acquérir des outils pour protéger les systèmes informatiques.il reste toujours que la sécurité des systèmes informatiques est beaucoup plus compliquée.

Chapitre IV : Systèmes d'Exploitation Client-serveur

IV.1.Introduction

Ces dernières années ont vu une évolution majeure des systèmes d'information, à savoir le passage d'une architecture centralisée à travers de grosse machines (mainframes) vers une architecture distribuée basée sur l'utilisation de serveurs et de postes clients grâce à l'utilisation des PC et des réseaux. Au cours de ces années, le modèle client/serveur également appelé « architecture client/serveur » est très différent du modèle point à point en cela qu'il permet de vraiment dédier des systèmes informatiques à la fonction des serveurs :serveur d'applications, de bases de données, de messagerie, de sites web etc...

Cette évolution a été possible essentiellement grâce à deux facteurs qui sont :

- la baisse des prix de l'informatique personnelle.
- le développement des réseaux.

IV.2.Définition :

L'architectures client-serveur est un modèle de fonctionnement logiciel qui peut se réaliser sur tout type d'architectures matérielle (petites ou grosses machines), à partir du moment où ces architectures peuvent être interconnectées.

On parle de fonctionnement logiciel dans la mesure où cette architecture est basée sur l'utilisation de deux types de logiciels, à savoir un logiciel serveur et un logiciel client s'exécutant normalement sur deux machines différentes. L'élément important dans cette architecture est l'utilisation de mécanismes de communication entre les deux (2) applications.

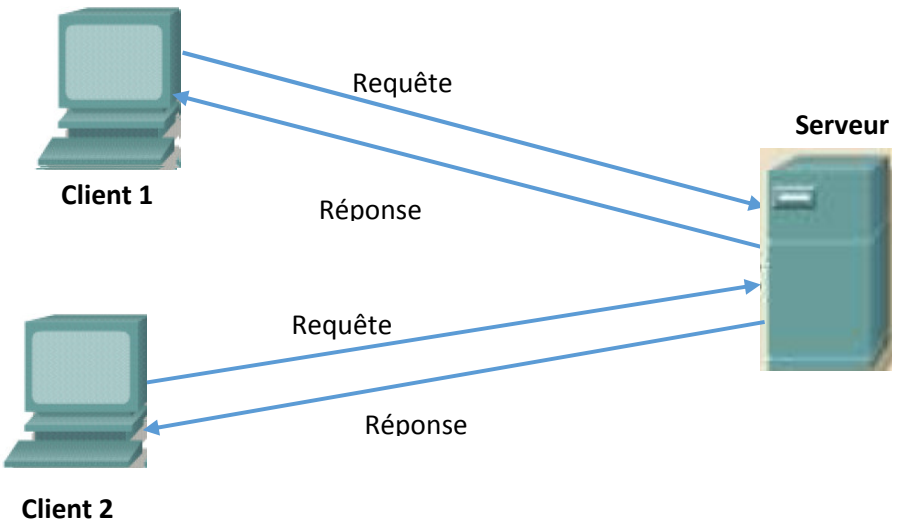


Figure IV.1 : Fonctionnement Client/serveur

Client :
Les caractéristiques d'un client sont les suivants : Il est d'abord Actif (ou Maitre), il envoie des requêtes au serveur, il attend et reçoit les réponses du serveur.

Serveur : Un serveur est initialement passif, il attend, il est à l'écoute, prêt à répondre aux requêtes envoyées par des clients, dès qu'une requête lui parvient, il la traite et envoie une réponse.

Requête (Request): c'est un message transmis par un client à un server décrivant Le service sollicité par le client.

Réponse (reply) :c'est un message transmis par serveur à un client à l'exécution d'une opération contenant des paramètres de retour de l'opération.

Dialogue : Le client et le serveur doivent bien sûr utiliser le même protocole de communication, un serveur est généralement capable de servir plusieurs clients simultanément.

Un autre type d'Architecture Réseau est le Pair à Pair (**Peer to Peer en Anglais ou P2P**), dans lequel chaque ordinateur est à la fois client et Serveur.
Les systèmes pair-à-pair permettent à plusieurs ordinateurs de communiquer via un réseau, de partager simplement des fichiers le plus souvent, mais également des flux multimédia ou encore un service (comme la téléphonie avec Skype par exemple), … sur internet.
L'utilisation d'un système pair-à-pair nécessite pour chaque nœud l'utilisation d'un logiciel particulier. Ce logiciel, qui remplit alors à la fois les fonctions de **client et de serveur**.

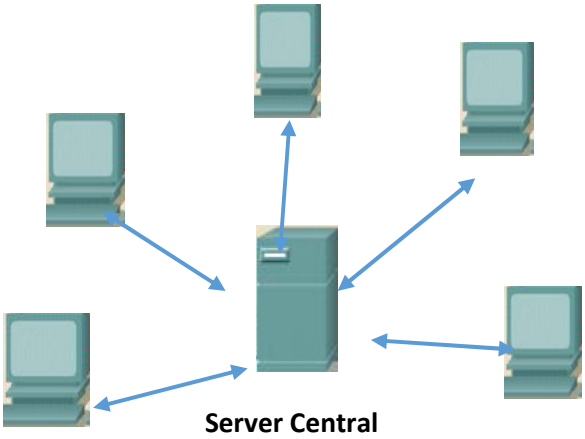


Figure IV.2 : Architecture Client/serveur

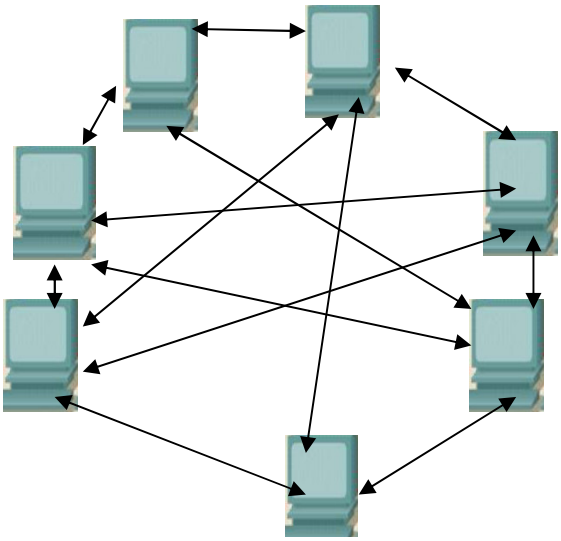


Figure IV.3 : Architecture Peer to Peer

Le mode client/serveur n'est pas le modèle parfait, n'y en a pas !

Connaissant les avantages et les inconvénients par rapport au mode distribué (par exemple pair à pair), vous pourrez choisir celui qui vous convient.

Avantages

Toutes les données sont centralisées sur un seul serveur, on a donc « un contrôle de sécurité simplifié ».

Toute la complexité/puissance peut être déportée sur le(s) serveur(s), les utilisateurs utilisant simplement un client léger.

IV.3.Les différents modèles du client/serveur

En fait, les différences sont essentiellement liées aux services qui sont assurés par le serveur, on distingue couramment :

IV.3.1.Modèle client/serveur de données

Dans ce cas, le serveur assure des tâches de Gestion Stockage et de traitement de données, c'est le cas plus connu de client-serveur qui est utilisé par tous les grands SGBD.

La Base de données avec tous ses outils (maintenances, sauvegarde) est installé sur un poste serveur, sur les clients, un logiciel d'accès est installé permettant d'accéder à la base de données du server.

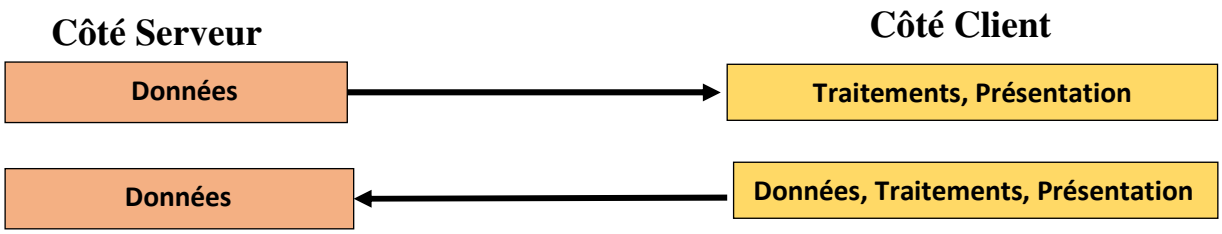


Figure IV.4 : Le Modèle Client-Serveur de Données

Inconvénient :

- Trafic réseau encore assez important

IV.3.2.Modèle client/serveur de présentation

Dans ce cas, la présentation des pages affichées par le client est intégralement prise en charge par le serveur, cette organisation présente l'inconvénient de générer un fort trafic réseau.

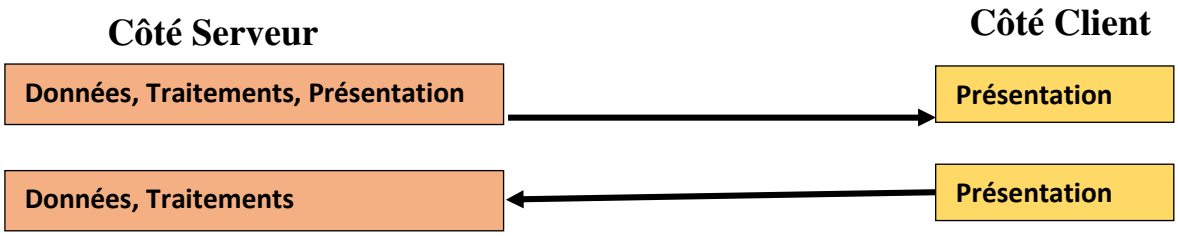


Figure IV.5 : Le Modèle Client-Serveur de Présentation

Inconvénient

- Fort trafic du réseau
- Le poste client conserve une position esclave par rapport au serveur

IV.3.3.Modèle client-serveur de traitement

Dans ce cas, le serveur effectue des traitements à la demande du client, il peut s'agir de traitement particulier sur des données, de vérification de formulaires de saisie, de traitements d'alarmes.

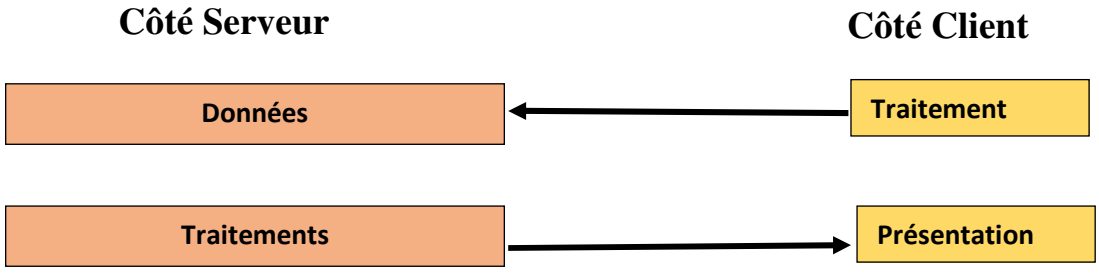


Figure IV.6 : Le Modèle Client-serveur de Traitement

Avantage :

- Les données et les traitements sont idéalement réparties pour équilibrer la charge des serveurs et des clients, les données sont proches des utilisateurs.

Inconvénients :

- Mise en œuvre plus complexe

IV.4-Les déférents types d'architectures de client /serveur

L'architecture client-serveur permet à une application de s'adressé à une application physiquement à distance, à travers un protocole d'échanges standardisés, pour lui demander de réaliser une tache pour son propre compte. Parmi ces types d'Architecture, on distingue :

IV.4.1- Architecture deux tiers (deux niveaux) :

Dans une architecture deux tiers, encore appelée client-serveur de première génération ou client-serveur de données, le poste client demande une ressource et le serveur la lui fournit directement sans faire appel a un autre serveur intermédiaire.

IV.4.2-Architecture trois tiers (trois niveaux) :

Il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :

1. Le client **:** le demandeur de ressources
2. Le serveur d'application (appelé aussi **middleware**) : le serveur chargé de fournir la ressource mais en faisant appel à un autre serveur.
3. Le serveur secondaire (généralement un serveur de base de données), fournissant un service au premier serveur

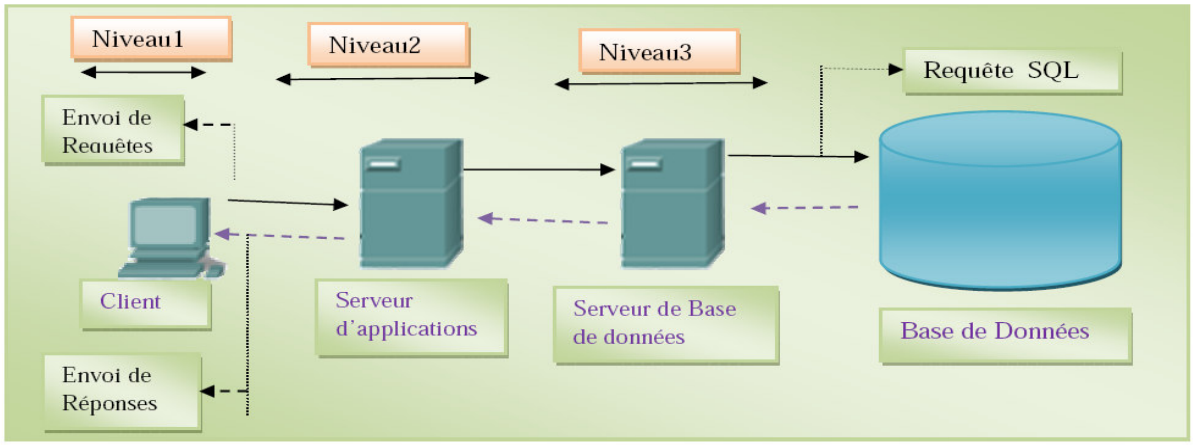


Figure IV.7 : Architecture deux tiers (deux niveaux)

IV.4.3- Architecture n tierces

L'architecture n-tiers a été pensée pour pallier aux limitations des architectures trois tiers et concevoir des applications puissantes et simples à maintenir. Ce type d'architecture permet de distribuer plus librement la logique applicative, ce qui facilite la répartition de la charge entre tous les niveaux.

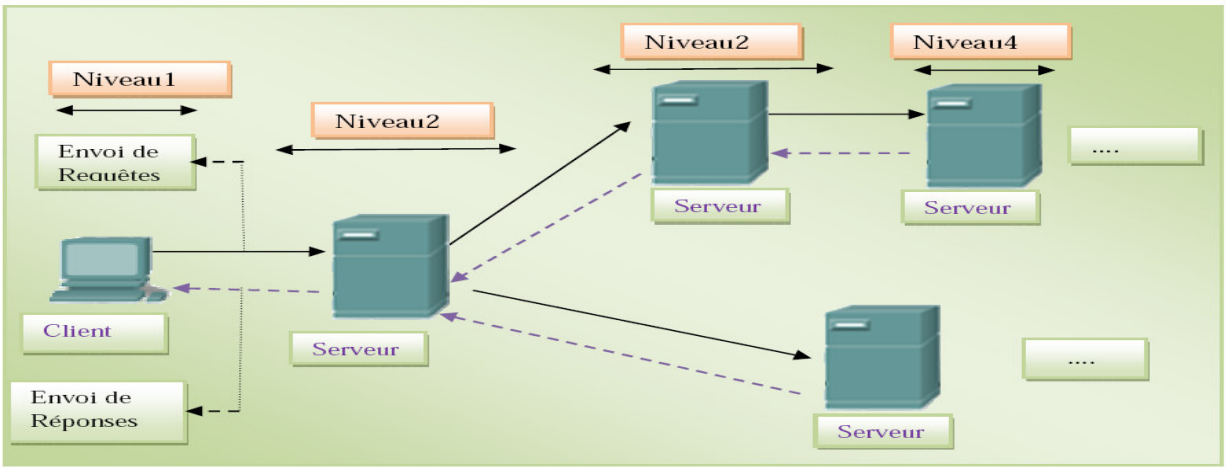


Figure IV.8: Architecture n tiers (n niveaux)

IV.5-Middleware

Définition : on appelle Middleware (**Middle**=milieu et **war**e=Software qui veut dire logiciel (ou logiciel médiateur en français), littéralement « élément du milieu », l'ensemble des couches réseau et services logiciel qui permettant les dialogues entre les clients et les serveurs. il est souvent hétérogène, en d'autre terme il constitue l'ensemble des services logiciels construits au-dessus du protocole de transport afin de permettre l'échange Requête-réponse de manière transparente en cachant l'hétérogénéité des composants mis en jeu.

Parmi les middlewares qui permettent l'interopérabilité entre applications homologues (de même nature), on peut distinguer deux grandes familles:

- Les middlewares qui permettent l'invocation synchrone de fonctions et méthodes, parmi lesquels on trouve la famille des request brokers, avec CORBA ou encore DCOM.
- Les middlewares d'échange asynchrones, qui sont principalement à base de messages, ce sont les MOMs, les Message Oriented Middleware.

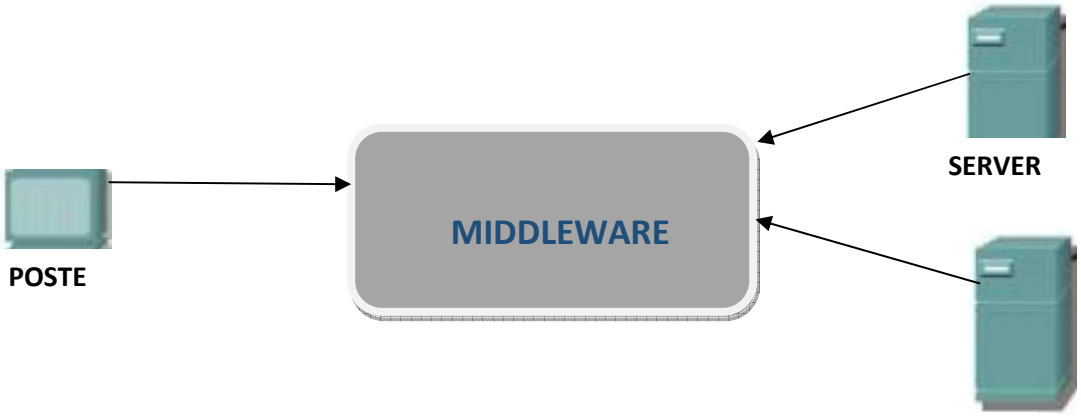


Figure IV.9 : Schéma de Middleware entre client/server

IV.6-Les systèmes d'exploitation

IV.6.1- Définition d'un système d'exploitation

Le **système d'exploitation** est un ensemble de programme permet de faire fonctionner tous les composants matériels de l'ordinateur, ainsi que toutes les applications qui sont compatibles avec lui. Le système d'exploitation (SE ou OS en anglais pour operating system) est une interface entre d'une part le matériel et l'utilisateur et ses logiciels d'autre part.

IV.6.2- Un système d'exploitation réseau :

Le système d'exploitation réseau, appelé aussi NOS (Network Operating System) est installé sur un serveur dont le rôle est de piloter et contrôler le réseau local.

IV.6.3- Le rôle du système d'exploitation réseau :

Ses principales fonctions sont :

- ✓ La gestion du partage des ressources : disques, fichiers, imprimantes, modem... Coordonner les accès simultanés à la même ressource
- ✓ La gestion des droits d'accès des utilisateurs :
  - Créer et gérer les comptes des utilisateurs qui ont accès au réseau
  - Définir les permissions des utilisateurs et des groupes (lire, enregistrer, supprimer, exécuter, …)
- ✓ La gestion des communications internes et externes du réseau local.
- ✓ Assurer la sécurité du réseau et des données qui y sont stockées.
- ✓ Il permet l'exécution d'application, telle qu'une application de messagerie électronique ou le transfert de fichiers par exemple.

- ✓ Il offre aux utilisateurs une interface mieux adaptée à leurs besoins, et permettant de manipuler l'ordinateur et d'en faire usage (en partageant un disque dur ou d'accéder aux ressources partagées, par exemple).

IV.6.4- Etudes d'un Système d'exploitation Réseau : Windows 7 :

4.1-Définition :

Windows 7 (précédemment connu en tant que **Blackcomb** et **Vienna**) est un système d'exploitation de la société Microsoft, sorti le 22 octobre 2009 et successeur de la sixièmes version nommée Windows Vista. Et est conçu pour être un système d'exploitation plus fin que son prédécesseur, avec des performances plus rapides et moins de problèmes de compatibilité. Windows 7 a été libéré en conjonction avec Windows Server 2008 R2.

4.2. Sécurité :

- le Security Center était également amélioré et intégré des outils comme Windows Defender afin de se prémunir des malwares.
- Le contrôle de compte utilisateur permet de protéger la machine.
- Mise en place d'un nouveau moyen de se connecter au réseau d'entreprise avec DirectAccess uniquement pour la version Entreprise ou Intégrale

Windows 7 présente les exigences minimales suivant :

- **Processeur** : 1GHz (ou supérieur) processeur 32-bit (x86) ou bien 64-bit (x6432-bit (x86) or 64-bit (x64) processor
- **Mémoire** : 1 GB de RAM ou bien 2 GB de RAM pour la version 64-bit.
- **Disque dure :** 16 GB d'espace disque disponible pour les fichiers système ou bien 20 GB pour la version 64-bit.

IV.6.5-Systèmes d'exploitation dédiés aux serveurs:

Un serveur dédié étant principalement destiné à un usage intensif sur le réseau, son système d' exploitation est généralement choisi en fonction de ses capacités à gérer cette fonctionnalité. Il est bien plus qu'un serveur de page web et dans ce sens on préférera un OS offrant le maximum de services associés.

5.1-Windows Server 2012 :

5.1.1-Présentation :

Microsoft Windows Server 2012 est un système d'exploitation serveur complet, polyvalent et puissant qui se base sur les améliorations que Microsoft a apportées à Windows Server 2008 R2. Le premier release officiel de Windows Server 2012 a été déployé en septembre 2012. Windows Server 2012 et Windows 8 partagent un certain nombre de caractéristiques car ils font partie du même projet de développement. Ces fonctionnalités partagent une base de code commune qui couvre de nombreux domaines du système d'exploitation, notamment la gestion, la sécurité, le réseau et le stockage. En raison de cela, la majeure partie de ce que vous savez sur Windows 8 s'applique aussi à Windows Server 2012.

5.1.2-Définition :

Microsoft Windows Server 2012 est une nouvelle génération du système d'exploitation Windows Server conçue pour aider les administrateurs système à rationaliser leurs infrastructures.

Il faut savoir si l'ordinateur que nous allons installer ou mettre à niveau est capable d'exécuter Windows server 2012, Windows server 2012 présente les exigences minimales suivant :

- **Processeur** : 1.4-GHz (ou supérieur) processeur x64 ; 2 processeurs minimum, 64 processeurs maximum.
- **Mémoire** : 512 Mo de RAM ou supérieur ; 2 To maximum.
- **Disque dure :** 32 Go d'espace disque disponible pour les fichiers système (les ordinateurs avec plus de 16 Go de RAM demande plus d'espace disque disponible pour la pagination, l'hibernation et les fichiers supprimés).
- **Adaptateur réseau** : Même si aucune carte adaptateur réseau n'est exigée pour l'installation du système d'exploitation Windows 2012 server, elle est nécessaire pour la connexion à un réseau. Le système peut prendre en charge plus d'une carte réseau.

La sécurité : Concernant la sécurité, Windows Server 2012 profite des améliorations suivantes :

- **Windows Right management Server** : il s'agit d'un service inclus dans Windows Server 2012, qui permet de gérer ce que chacun a le droit de faire d'un document donné (modification, transfert, impression).

- **Network Access Protection(NAP) :** il s'agit de la technologie de Microsoft permettant aux administrateurs réseau de définir des niveaux spécifiques d'accès au réseau d'un ordinateur en se fondant sur la santé de son système (Information sur un ordinateur ou restreindre l'accès à un réseau).

- **Windows BitLocker Drive Encryption** : il s'agit du chiffrement complet de l'espace de stockage, est une fonctionnalité clé de Windows Server 2012 améliorant la protection des serveurs, des postes de travail, ordinateurs portables et autres équipements mobiles**.**

- **Read-Only Domain Controller(RODC)** : c'est un contrôleur de domaine en lecteur seule,. Le RODC fournit une authentification locale pour les utilisateurs des succursales et des agences sans copier entièrement à base de données Active Directory, ce qui réduit les risques.

- **Active Directory Federation Services (ADFS) :**
  Le rôle fournit un service fédéré de gestion des identités. Il identifie et authentifie un utilisateur qui souhaite accéder à un extranet.. Avec ADFS, l'utilisateur peut donc accéder à des applications et aux systèmes distincts dans des entreprises indépendantes.

- **Direct Access**: Cette fonction sécurisée permet d'accéder au réseau depuis n'importe quel ordinateur ou périphérique. Elle est plus rapide que les connexions VPN typiques et offre l'accès hors site au partage des fichiers, aux équipements sur site et à d'autres ressources.

Le web :

Le serveur web intégré nativement à Windows serveur 2012 est:

- **Internet Information Server 8.0 (IIS 8) :** propose une architecture très modulaire qui permet d'installer que les composants strictement nécessaire à ce que l'on veut faire.

Cela réduit la surface d'attaque de l'infrastructure web. Il permet également d'augmenter le nombre d'application web hébergées par serveur.

- **Windows SharePoint Services 3.0** (WSS 3.0) **:** est une partie de Windows Server 2012 qui permet de réduire le temps que les utilisateurs passent à chercher et à analyser des informations.

5.1.3-Annuaire Active Directory :

1) Définition :

Active Directory est un service d'annuaire extensible et évolutif qui permet de répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Il renferme des informations relatives aux objets d'un réseau et facilite leur recherche et leur utilisation pour les administrateurs et les utilisateurs .il existe depuis la version 2000, Le service d'annuaire Active Directory peut être mis en œuvre sur Windows 2000 Server, Windows Server 2003 , Windows Server 2008 et Windows Server 2012.

Un serveur informatique hébergeant l'annuaire Active Directory est appelé « contrôleur de domaine ». Les domaines qui utilisent les services Active Directory sont nommés domaines active Directory.

Active Directory est le cœur de Microsoft Windows Server 2012. Il peut être installé sur des serveurs exécutant Microsoft Windows Server 2012, Standard Edition, Entreprise Edition et Datacenter Edition

Structure d'«Active Directory» :

1. **Domaines :**

Un domaine Active Directory est tout simplement un groupe d'ordinateurs faisant partie d'un réseau et partageant une même base de données d'annuaire. Chaque domaine possède un nom unique.

L'espace de nommage est réalisé grâce au système DNS. Un domaine peut avoir plusieurs sous-domaines : on crée ainsi une arborescence. Le séparateur est le point.

1) **Sous-domaines :** est un ensemble de domaines rattaché au domaine racine en formant un arbre et un espace de noms contigus.

Exemple : univ.com est le domaine racine et
Etudiant.univ.com, professeur.univ.com sont des sous domaines du domaine univ.com

2. Arbres de domaines :

Est une structure de domaines, constitué du domaine racine, qui possède un ou plusieurs domaines enfants, qui peuvent eux-mêmes possédés des domaines enfants qui constituent les feuilles de l'arborescence et qui partagent un schéma et un catalogue global communs.

. domaine.com,
sous1.domaine.com, sous2.domaine.com et projet.sous1.domaine.com forment un arbre.

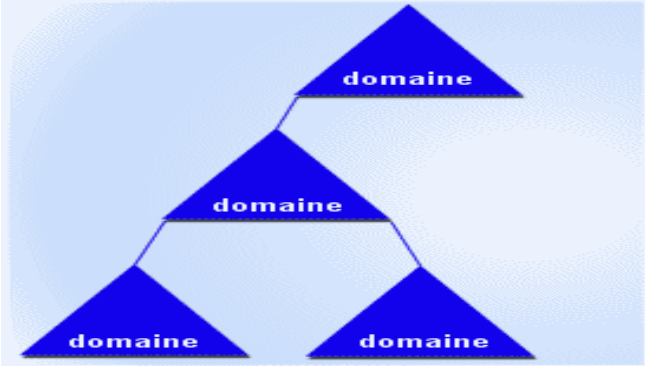


Figure IV.10 : Arbres de domaines

3. Forêts :

Une forêt est constituée d'une ou plusieurs arborescences de domaines ne formant pas d'espace de noms contigu mais partageant un schéma, une configuration et un catalogue global commun.

La structure d'Active Directory lui permet de gérer de façon centralisée des réseaux pouvant aller de quelques ordinateurs à des réseaux d'entreprises répartis sur de multiples sites.

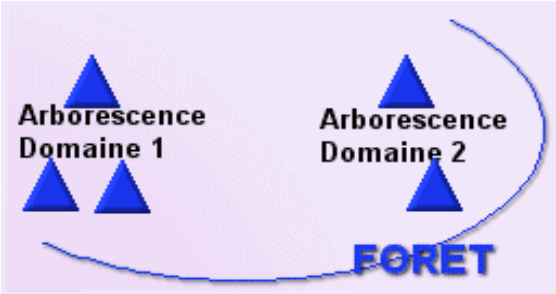


Figure IV.11 : Structure de la Forêt

5.2-Linux (GNU /Linux) : [VI.1]

5.2.1-Introduction

Qu'est ce que Linux :

Linux ou GNU/Linux est un système d'exploitation libre multitâche, multi-plateforme et multi utilisateur de type Unix. Le système d'exploitation dans son ensemble représente le résultat des efforts convergents de nombreux projets développés en mode collaboratif qui se sont déployés via Internet : le projet GNU, le noyau Linux, le système de fenêtrage X Window, et certains logiciels produits par les équipes des Unix libres FreeBSD , OpenBS et NetBSD.

Debian GNU/Linux :

Debian GNU / Linux ou simplement Debian est une des plus anciennes et dans l'intervalle, l'un des systèmes d'exploitation les plus largement utilisés dans le monde.

Le projet Debian a été créé par Ian Murdock en 1993, initialement sous le patronage du projet GNU de la Free Software Foundation. Aujourd'hui, les développeurs Debian le voient comme un descendant direct du projet GNU.

5.2.2-Définition :

Debian GNU/Linux est une distribution spécifique du système d'exploitation Linux est distribuée logiciel open-source libre sous la licence GNU, on trouve habituellement le système GNU–Linux sur de grands serveurs et des systèmes multi–utilisateurs.

5.2.3-Avantages de Debian GNU/Linux :

La distribution Debian présente plusieurs avantages:
Un avantage non négligeable de cette distribution est également sa gestion de l'installation de paquets, transparente et structurée, ainsi que le nombre d'outils disponibles.

Debian respecte totalement la philosophie du monde du logiciel libre. De plus, il existe une forte communauté d'utilisateurs autour de cette distribution, il est donc assez aisé de trouver de la documentation fiable et abondante.

Concernant les virus, la légende selon laquelle les systèmes d'exploitation Linux y sont invulnérables est erronée :

- ✓ les utilisateurs de Linux n'ont pas les droits administrateur, et ne peuvent donc pas modifier les fichiers système. Il est ainsi difficile pour un virus d'infecter la machine,
- ✓ Linux oblige à déclarer si un fichier est exécutable ou non. Ce n'est pas l'extension qui détermine si un fichier est exécutable. Il est donc difficile d'exécuter un fichier sans le vouloir, en pensant que c'était un fichier d'un autre type,
- ✓ Linux est open-source, c'est- à-dire que tout le monde peut examiner son code source, y compris des experts en sécurité. Les failles ont donc plus de chances d'être détectées.

V. Conclusion

Le modèle client /serveur facilite l'intégration des nouvelles technologies dans les systèmes d'information de l'entreprise, ces applications tournent souvent sur de nombreux serveurs, elles sont au cœur du fonctionnement de l'entreprise.

Chacun de systèmes étudiés est désigné pour certaines fonctionnalités ; Windows Server 2012, Linux Debian et Windows 7 pour les postes clients

Chapitre V: Conception et Réalisation

V.I-CONCEPTION :

I.1.Etude de l'existant Critique et suggestion

Au cours de trois mois de stage pratique mené à l'entreprise ENIEM, une étude approfondie du Réseau de l'ENIEM a été menée avec l'aide de notre Encadreur **Mr Taleb Farhath, Chef de Section Réseau et Maintenance Informatique à l'ENIEM**, pour une meilleure compréhension de l'environnement informatique de l'organisme d'accueil.

Cette étude nous a aidé à ressortir les problèmes de fonctionnement du réseau de l'ENIEM afin de déterminer la portée du projet, de la solution à implémenter, ainsi que des décisions à prendre pour le choix de la solution et son déploiement. Dans cette partie le pourquoi de cette solution, de chaque service à déployer, jusqu'à leur mise en œuvre seront expliqués.

I.2.Critique :

Après avoir fait une étude menée sur les différents services de l'organisme d'accueil «ENIEM», les remarques suivantes sont ressorties:

- Le système devient de plus en plus lent, cette lenteur est une conséquence de la topologie choisit pour les caractéristiques des serveurs utilisés.
- Manque de sécurité des données (virus, intrusion ….etc.)
- Déplacement des employés pour imprimer.
- Circulation des informations sur les supports de stockage (flash disque….).
- Absence de partage de données entre les différents bureaux.
- Accès à internet non administré et non Sécurisé.
- Absence de contrôle sur l'état de travail des utilisateurs
- Mauvaise et manque de communication entre les différents postes du réseau.
- Absence d'un Server Web et de Messagerie.
- Absence d'un Pare-feu pour sécuriser l'accès vers l'extérieur
- Vu l'étendue et l'importance du Réseau de L'ENIEM, L'Architecture physique n'est pas conforme à une architecture de sécurisation.

I.3.Suggestion :

Afin de parer aux problèmes posés et après discussion avec les responsables, la solution de mise en œuvre consisterait en la conception et le redéploiement d'une Architecture Réseau Sécurisée pour le réseau local (Bloc Administratif) administré sous serveur Windows 2012 et Serveur Linux (Débian).

I.4.Solution et objectifs de l'étude :

L'enjeu principal d'une architecture réseau Sécurisée, est de pouvoir réglementer les accès aux Ressources du Réseau tant à partir du Réseau Local qu'à partir de l'extérieur, tout en essayant au maximum de limiter les failles éventuelles (attaques ou vols d'informations) afin d'accroître la Sécurité du Réseau Local. En effet, face à des applications telles que la Messagerie, le Serveur Web, qui permettent la Mobilité donc les Accès d'origines diverses, il est important de définir une architecture fiable de sécurisation du Réseau. L'implémentation d'une telle Architecture, abordée dans les lignes suivantes, aboutira à un gain en termes de performance et de Sécurité du Réseau :

- Réinstallation et aménagement d'un réseau local filaire client/serveur administré sous Windows serveur 2012 et d'autre système d'exploitation client (Windows 7).
- Mise en place d'un Annuaire Active Directory pour une gestion centralisée des ressources et planification des accès à ces ressources à travers les paramètres de sécurité dans Windows server 2012 appelé GPO (Group Policy Object).
- Installation d'antivirus sur les ordinateurs du réseau.
- Partage des périphériques (imprimante, scaner, etc.) et ressources logiciels (partage d'accès à la connexion internet, etc) et partage de fichiers.
- Mise en place d'un pare-feu pour la sécurité du réseau Local (filtrage des paquets, Accès VPN, Control de flux)
- La Segmentation du Réseau local en VLAN pour renforcer la Sécurité interne.
- Installation et configuration d'un Serveur et d'un Serveur de Messagerie dans une zone DMZ (zone démilitarisée)

I.5.Planification du Déploiement

I.5.1. Architecture du réseau existant (Département Informatique)

Avec l'architecture existante donnée ci dessous, si on arrive à pirater l'un des réseaux des services, il sera facile d'accéder aussi aux serveurs car ils font partie du même sous réseau, c'est pourquoi de cacher l'identité de chaque sous réseau par la technique de VLAN.

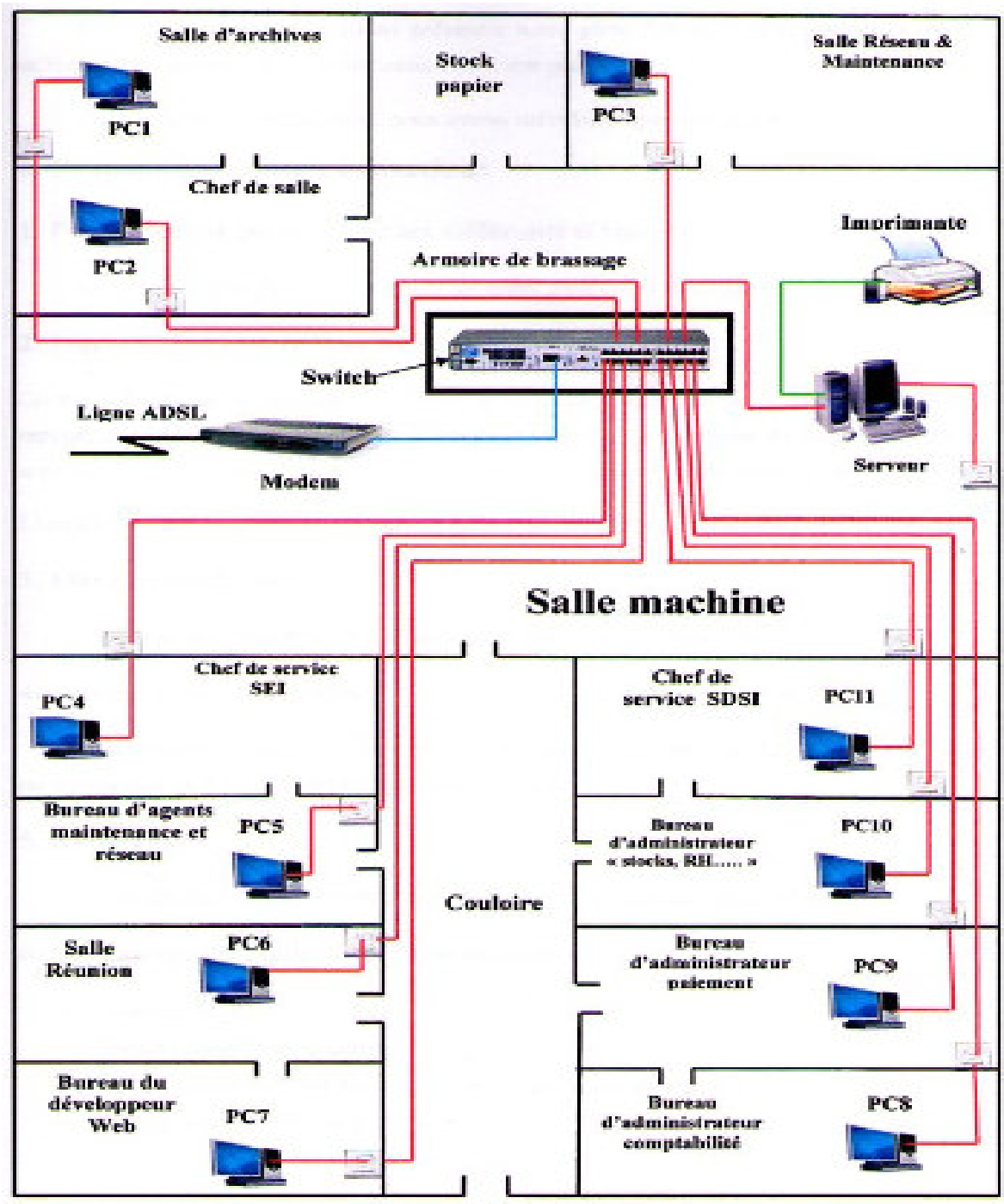


Figure V.1 : Architecture Physique du Réseau de L'ENIEM (Département Informatique)

5.2.Outils utilisés (Matériels et Logiciels) :

Nom	Systèmes d'exploitation	Services Installés	Spécifications Techniques	Adresse IP
Server1 DC1-ENIEM	Windows Server 2012	Active Directory DNS DHCP	RAM 512 Mo jusqu'à 2 To Processeur 1.4 GHz Disque Dur : 32 GO	IP Lan : 192.168.2.4
Server2 DEBIAN-ENIEM	Linux Debian	Server Web Server de Mail	RAM : 512 Mo Processeur Intel ou AMD CPU : 1.4 GHz DD : 5GB	IP Lan : 192.168.10.100 192.168.10.101
Pare-feu SOPHOS-ENIEM	Type…de Sophos	Agent de mise à jour des anti-virus Paramètres de Sécurité (restriction des accès) et VPN	Filtrage de paquets Mise en œuvre de la DMZ	IP Lan : 192.168.2.100 192.168.10.1 IP WAN : 172.168.10.1
PC	Système d'exploitation Window 7		RAM : 1 Go Processeur 1 GHz Disque Dur : 16 GB	IP Lan : IP WAN :
Switch	De type Cisco		port USB port ADSL ports FXO ports RJ-45	IP Lan : 192.168.2.2
Machine Virtuelle	VMWARE		Pour la Simulation	

5.3. Architecture de déploiement:

Dans cette nouvelle architecture, le réseau de l'ENIEM est scindé en deux parties : le réseau local et la DMZ. Une liaison avec le réseau public est aussi prévue sur cette architecture.

Dans la nouvelle infrastructure, un firewall (ENIEM-SOPHOS) sur lequel seront implémentés les paramètres de Sécurité est aussi installé. Il jouera le rôle de passerelle entre le réseau ~~de~~ local de L'ENIEM et le réseau public. Il y aura aussi deux serveurs (DC1-ENIEM, DEBIAN-ENIEM) sur lesquels seront déployés les différents services.

Vu l'étendue du Réseau de l'ENIEM et le nombre d'étages, le Réseau a été segmenté en VLAN par étage et non par Service. Cette nouvelle Architecture est mieux adaptée en termes de Sécurité que l'Ancienne.

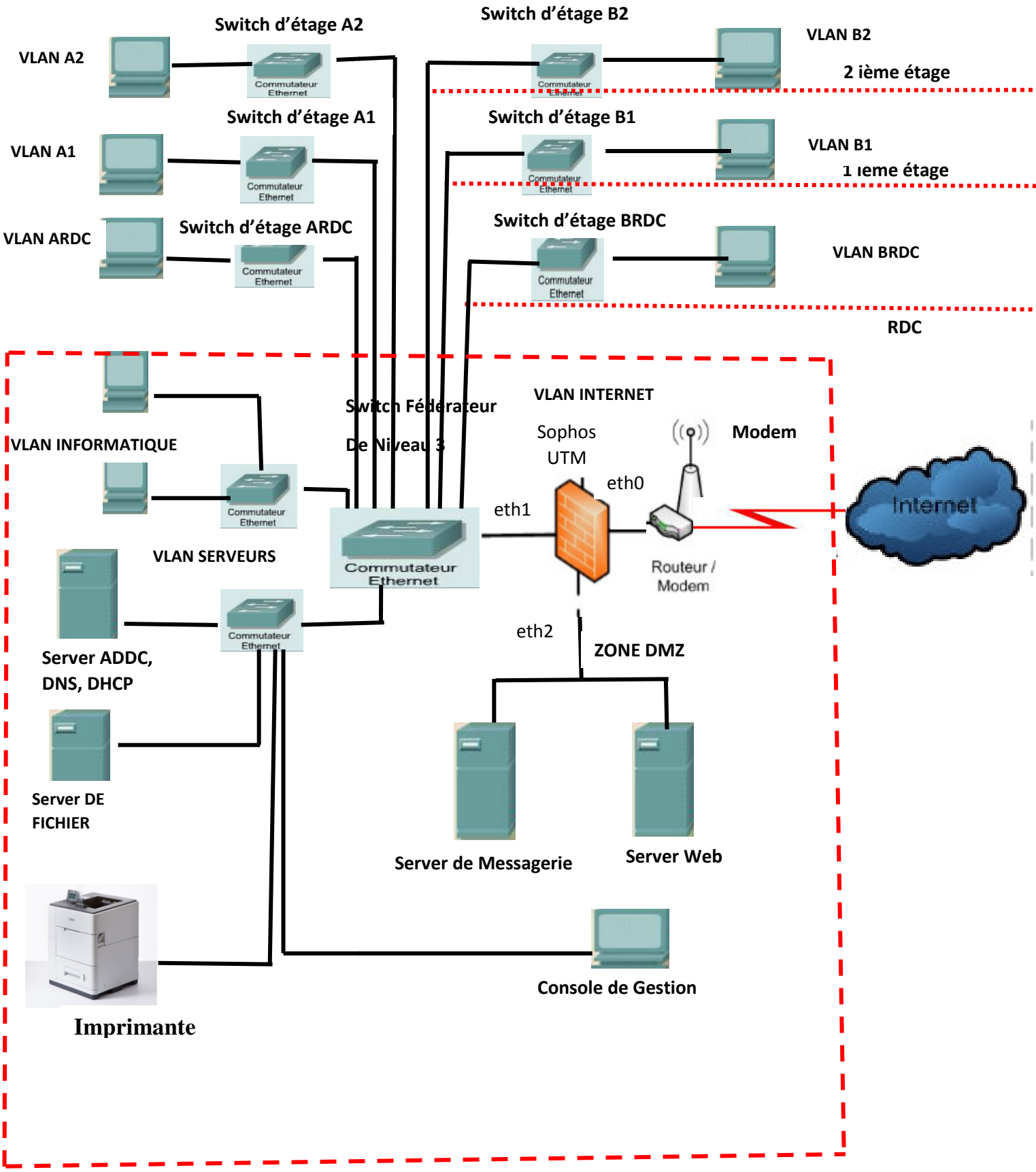


Figure V.2 : Architecture de Mise en œuvre.

5.4.Plan Adressage :

Pour ne pas remettre en cause le plan d'adressage en place, la même classe d'adressage (classe C) a été gardée, et le choix du masque de Sous réseau est dû au nombre Sous Réseaux et également au nombre de machines par Sous réseau : avec ce masque chaque sous réseau peut supporter jusqu'à 254 hôtes. Ce qui est largement suffisant. Le plan d'adressage adopté est le suivant :

Noms	Nbre d'hôtes	Id-vlan	Sous Réseau	Passerelle	Masque de Sous Réseau
VLAN INFORMATIQUE	25	10	192.168.2.0/24	192.168.2.1	255.255.255.246
VLAN SERVEURS	35	20	192.168.2.16/24	192.168.2.17	
VLAN INTERNET	20	30	192.168.2.32/24	192.168.2.33	
VLAN ARDC	45	40	192.168.2.48/24	192.168.2.49	
VLAN BRDC	14	50	192.168.2.64/24	192.168.2.65	
VLAN B1	25	60	192.168.2.80/24	192.168.2.81	
VLAN A1	30	70	192.168.2.96/24	192.168.2.97	
VLAN A2	55	80	192.168.2.112/24	192.168.2.123	
VLAN B2	60	90	192.168.2.128/2	192.168.2.129	

5.5. Les Différents Services à Installer :

Spécification des besoins

Suite à la critique de l'existant, quelques besoins ont été relevés afin de pallier aux contraintes précédemment mentionnées.

- **Besoins fonctionnels**

Les besoins fonctionnels expriment une action qui doit être menée sur l'infrastructure à définir en réponse à une demande. C'est le besoin exprimé par les utilisateurs; ce besoin peut être exprimé de manière fonctionnelle mettant en évidence les fonctions de services et les fonctions techniques:

- La Segmentation du Réseau : cette solution permet de Segmenter le réseau physique, de configurer des VLANS (Virtual Local Area Network) qui présentent les intérêts suivants:

- Améliorer la gestion du réseau.
- Optimiser la bande passante.
- Séparer les flux.
- Fragmentation : réduire la taille d'un domaine de broadcast,
- Sécurité : permet de créer un ensemble logique isolé pour améliorer la sécurité. Le seul moyen pour communiquer entre des machines appartenant à des VLAN différents est de passer par un routeur.

- Configuration de Windows Server 2012 sur le quel seront déployés les services suivants :

Un Contrôleur de Domaine (DC1.ENIEM.LAN): Le rôle principal du contrôleur de domaine (installé sur Windows server2012), est la centralisation de l'administration du Réseau de L'ENIEM, sur le quel est installé un annuaire 'Active Directory' qui est une fonctionnalité dans Windows Server 2012 permettant de centraliser les ressources et veiller sur leur exploitation. Sur le même Serveur, ils seront installés et configuré :

Un Serveur DHCP : pour l'allocation dynamique des Adresses aux postes de travail

Un Serveur de Fichier : pour le partage des fichiers et des dossiers, et monter aussi un lecteur Réseau, afin de permettre à chaque utilisateur ou groupe d'utilisateurs de n'accéder qu'aux fichiers ou dossiers qui lui est dédié dans le serveur.

Un Serveur DNS: pour la Résolution des noms de domaines.

- Configuration de Linux Debian (Debian-ENIEM) version Whezzy sur lequel, les services suivants sont déployés:

  - **Service web (Appache2) :** c'est le serveur Web le plus utilisé par les hébergeurs de sites web, notre choix sur Appache2, est dû à sa robustesse et différents paramètres qu'il offre pour héberger plusieurs sites web, ainsi qu'à sa sécurisation. Dans ce travail, il sera installé et configurer un server web Appache2 et héberger un site web en guise d'exemple pour voir exactement si notre Server web fonctionne bien.

  - **Service Messagerie (Postfix):** Le serveur de messagerie est un logiciel de courrier électronique ayant pour vocation de transférer les messages électroniques d'un serveur à un autre. La Messagerie Postfix a été choisie, car elle est open source et libre et offre beaucoup de paramètres et méthodes d'accès aux boites aux lettres. Pour rendre plus souple l'utilisation du Serveur de Messagerie Postfix, il sera installé l'utilitaire RoundCube pour avoir une interface de gestion Graphique.

  - **Service DNS Bind9 :** Ce Service, va permettre, d'associer un nom à une adresse IP à de chaque machine connectée au réseau. Ce principe de fonctionnement suscite une unicité des noms et le respect d'un nommage hiérarchique avec le domaine existant. Dans le cadre de ce projet, un Serveur DNS BIND9 a été installé sur le Serveur Débian, . Son rôle principal est de faire correspondre les noms de domaine suivants aux adresses suivantes :
    - Pour le server Web: www.eniem.com à l'adresse IP : 192.168.10.100
    - Pour de Messagerie : mail.eniem.com ou www.mail.eniem.com à l'adresse IP : 192.168.10.101

- **Configuration d'un Pare-feu (firewall en anglais) de Type SOPHOS** :

  Le SOPHOS est un outil de sécurité très puissant. C'est un pare-feu open source et libre de dernière génération, utilisé de nos jours par plusieurs Entreprises. Son rôle principal sera de filtrer les paquets, les datagrammes, en appliquant les règles de gestion des paquets arrivant et allant vers d'autres machines (sources/destinations) afin de renforcer la sécurité. Il interviendra aussi pour surveiller chaque message entrant /sortant ; le transmettre/rejeter suivant le contenu des champs de l'en-tête, de la

taille du message ou de son contenu et jouera également le rôle d'une passerelle vers l'extérieur.

Dans le cadre de ce travail, le pare-feu SOPHOS sera le pont (bridge) de Sécurité de notre solution à implémenter, Il contiendra trois cartes Réseaux :

- Une carte Réseau ethernet0 pour l'accès depuis l'extérieur, d'adresse 10.10.10.2
- Une Carte Réseau ethernet1 pour l'accès au Réseau local ayant pour adresse 192.168.2.100
- Une Carte Réseau ethernet2 pour l'accès depuis la zone DMZ au niveau de laquelle sont placés les serveurs de Messagerie et Web, ayant l'adresse 192.168.10.1

5.6. Création des «VLANs» dans le Switch fédérateur

Vlans au niveau du Switch Fédérateur : le Switch fédérateur joue le rôle d'un «VTP Server» (VLAN Trunk Protocol) qui permettra de créer, supprimer, modifier, et synchroniser les VLANS, c'est-à-dire il va permettre de déployer les configurations pour les autres «Switch» d'étages, qui vont jouer le rôle de «VTP Client», d'une manière automatique.

Les étapes de configuration des Vlans dans le Switch Fédérateur sont données ci dessous:

1-Créer les «Vlans» nécessaires dans le Switch fédérateur

2-Configurer les ports entre le «Switch» fédérateur et les autres «Switch» d'étages en mode Trunk

3- Configurer les ports entre les postes de travail et le «Switch» fédérateur en mode Access

4-Affecter les «Vlans» aux adresses IP de chaque sous Réseau

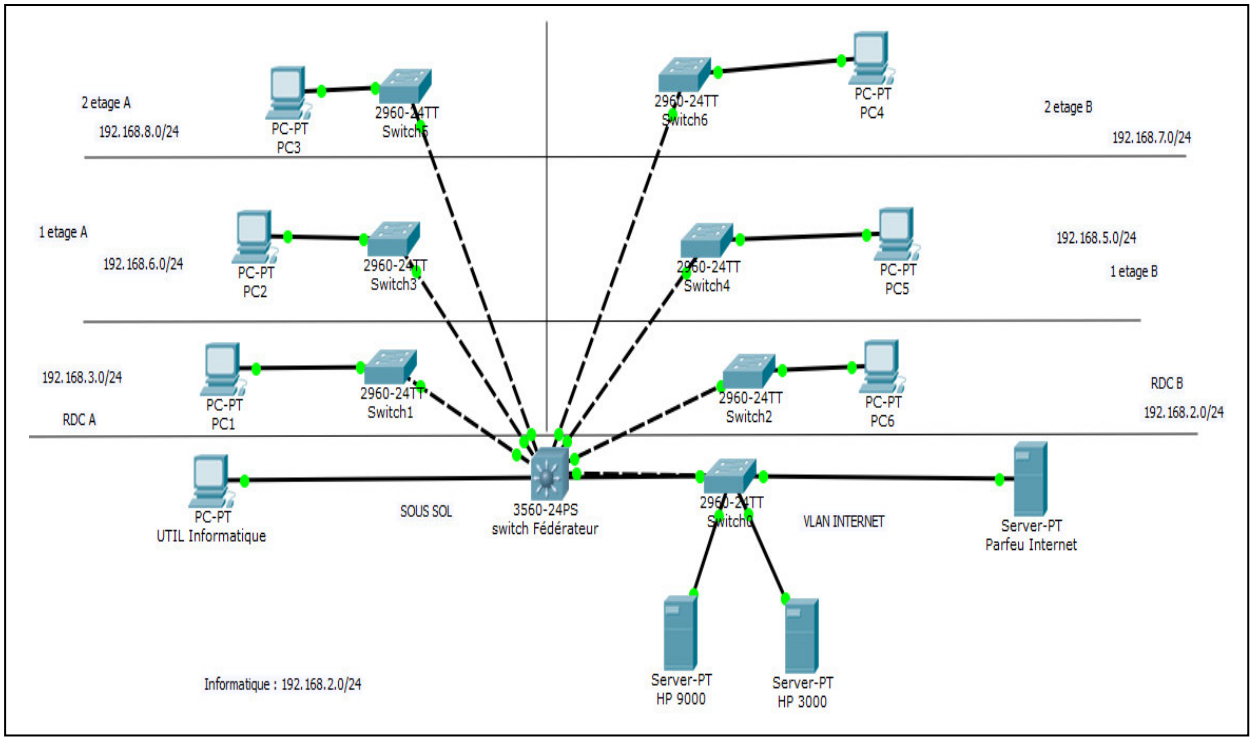
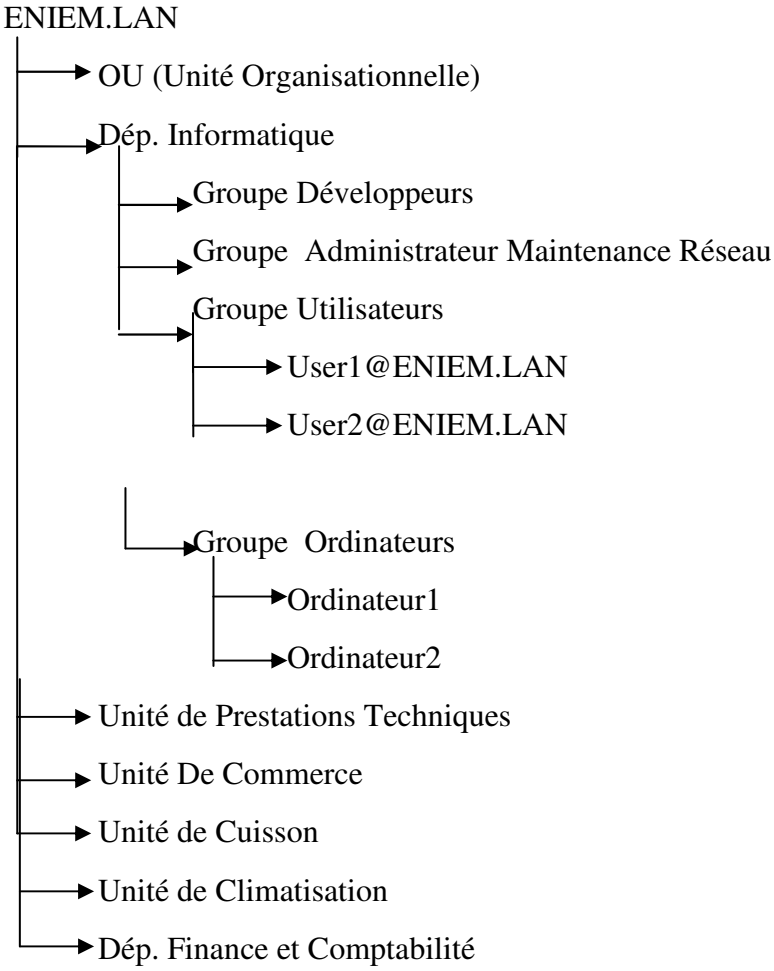


Figure V.3 : Schéma de simulation des VLANS

II.2. Configuration de Windows server 2012 :

Afin de configurer «Active Directory» dans le cadre de ce travail, un contrôleur de Domaine est crée dans une nouvelle forêt appelé ENIEM.LAN ayant la Structure Suivante:



V.II.Réalisation (Phase de Mise en Œuvre)

Quelques phases d'installation et de configuration de la structure d'«Active Directory» sont données ci-dessous:

II.1.Configuration de «Active Directory»

L'option «Manage-> Add Roles and Features» permet d'accéder à L'assistant des rôles pour sélectionner le serveur dans lequel «Active directory» doit être installé.

Une fois la configuration de déploiement choisie, une nouvelle forêt est ajoutée, avec un nom de domaine 'ENIEM.LAN'.

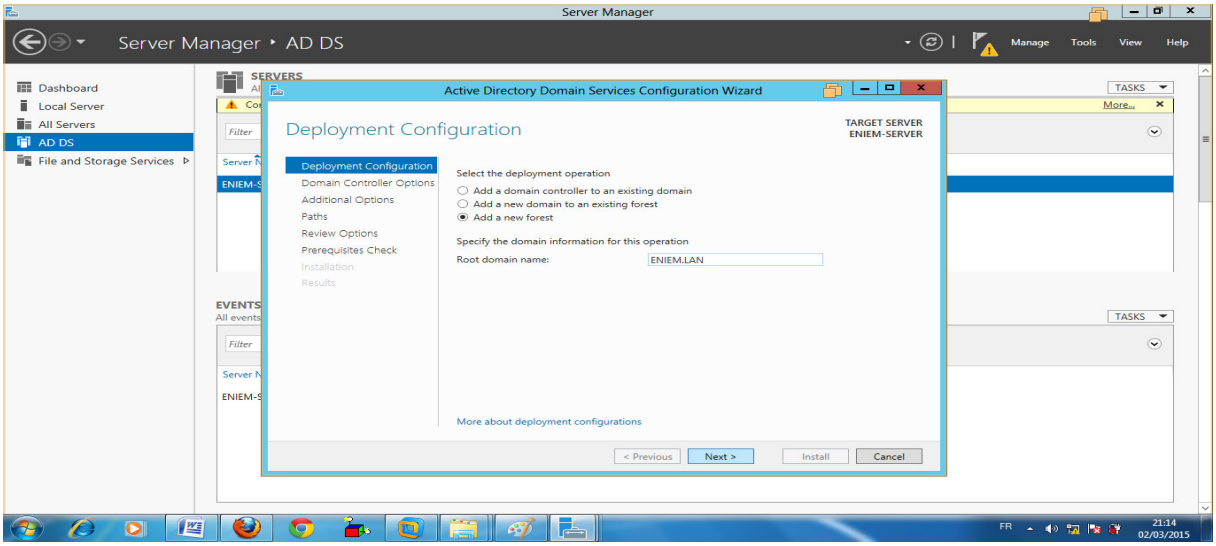


Figure V.4 : Configuration de l'annuaire active directory.

Un mot de passe qui va permettre de restaurer «Active Directory» est fourni. Puis l'installation est démarrée.

NB : Pour tenir compte de la nouvelle configuration du serveur, pour la suite de la configuration, il est nécessaire de le Redémarrer.

II.3.Créations des unités organisationnelles, les groupes, Utilisateurs, Ordinateurs, Les paramètres de sécurité GPO :

Unité Organisationnelle :

Dans cette phase les différentes unités d'organisation prévues dans notre champ d'étude seront créees.

- L'option «utilisateurs et ordinateurs active directory» permet de selectioner le domaine de travail et de spécifier les unités d'organisations désirées (Sous option : «ENIEM.LAN -> new->organisational unit»). La même procédure est appliquée pour la création des utilisateurs, des ordinateurs ainsi que les Groupes.

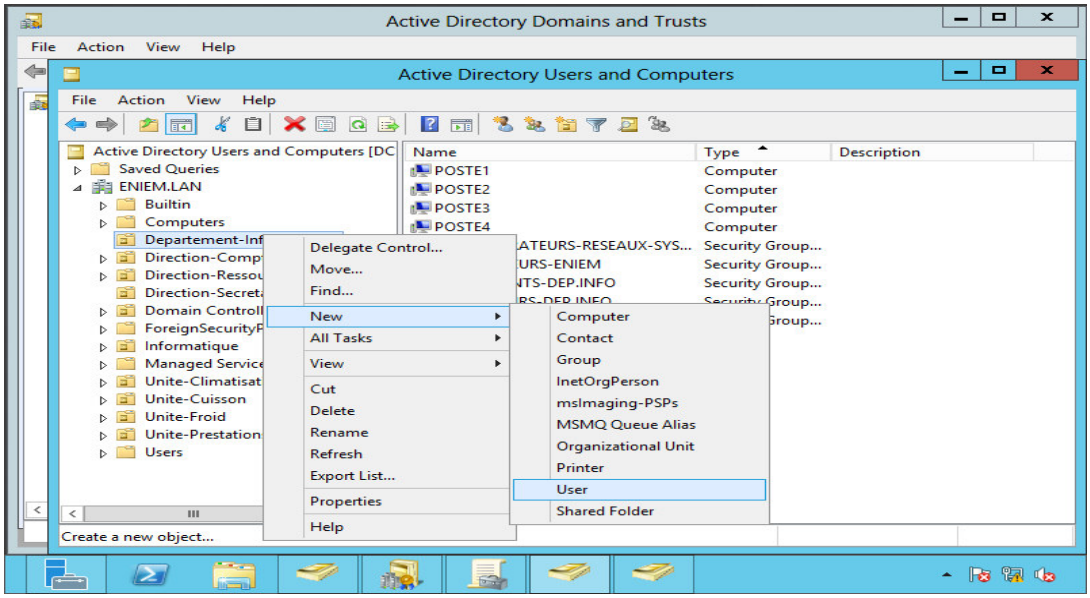


Figure V.5 : Création des comptes utilisateur.

- **Groupe Policy Manager (GPM) :**

Le GPM permet la mise en place des GPO sur certains Groupes afin de gérer leur accès aux ressources.

La création des GPOs dans le gestionnaire de serveur, se fait par le biais de l'option «tools->Groupe Policy Management», puis dans la sous option «Domaine->Eniem.lan», l'unité organisationnelle sur laquelle doit être appliqué le GPO est sélectionnée:

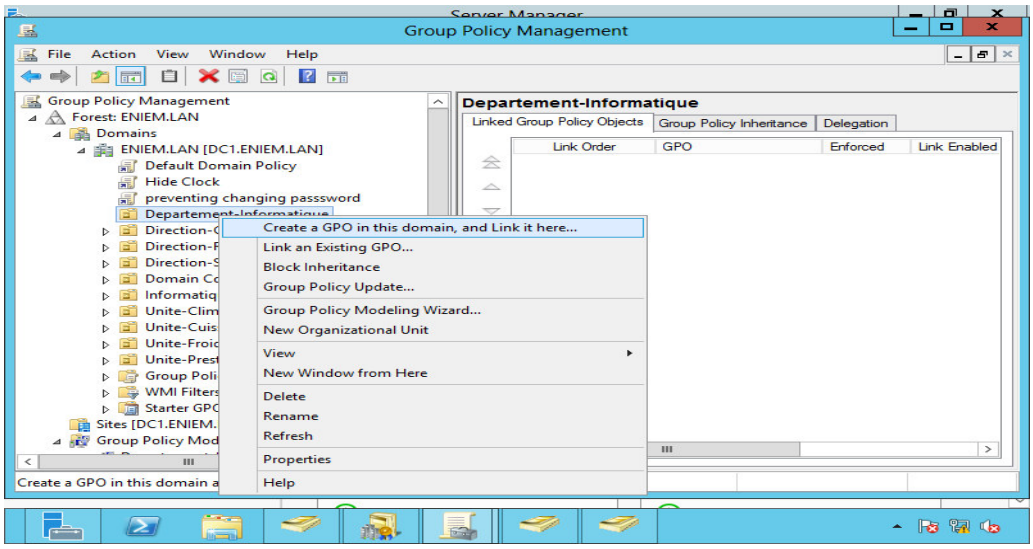


Figure V.6 : Création de la gestion des GPOs.

Un nom pour le GPO est requis pour sa création, puis l'option «éditer» permet de choisir l'objet GPO à appliquer:

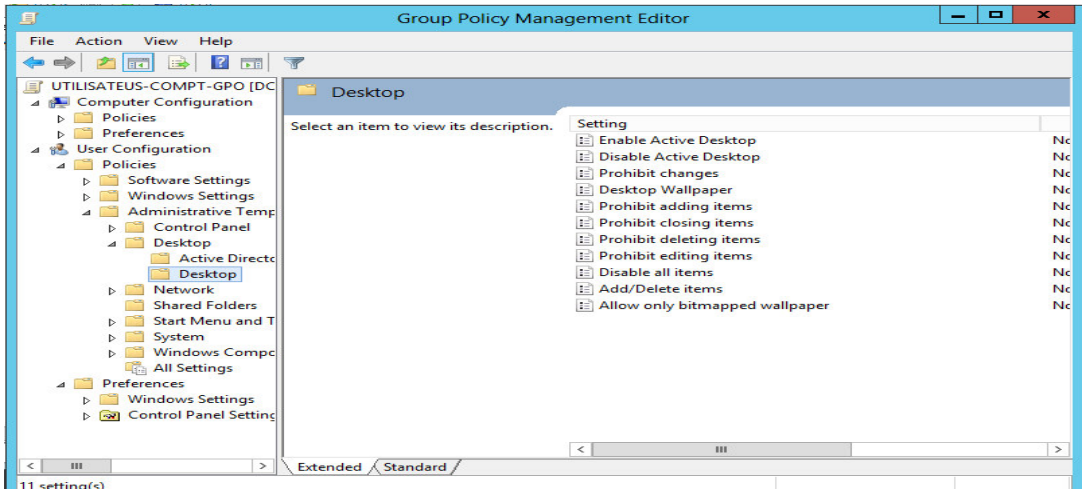


Figure V.7 : application des GPOs.

II.4.Installation et configuration d'un server DHCP :

Le «Gestionnaire de serveur» permet d'ajouter le rôle de « Serveur DHCP » au Serveur, en spécifiant un nom de serveur (le nom affecté dans le cadre de notre travail est «ENIEM-DHCP

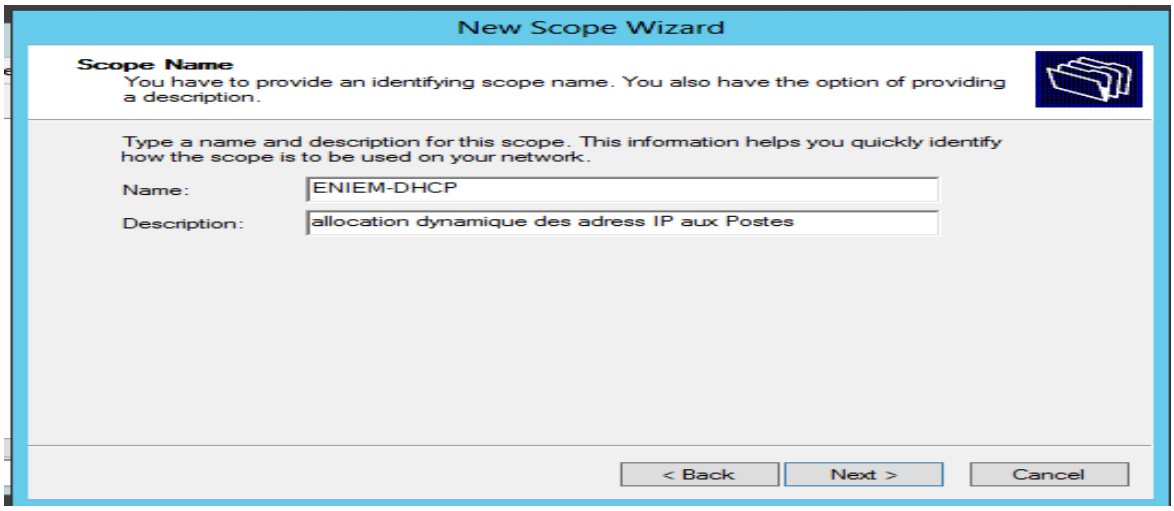


Figure V.8 : Configuration d'un server DHCP.

Puis une plage d'adresse IP pour notre serveur est spécifiée, le nom de domaine du serveur et son adresse IP sont donnés.

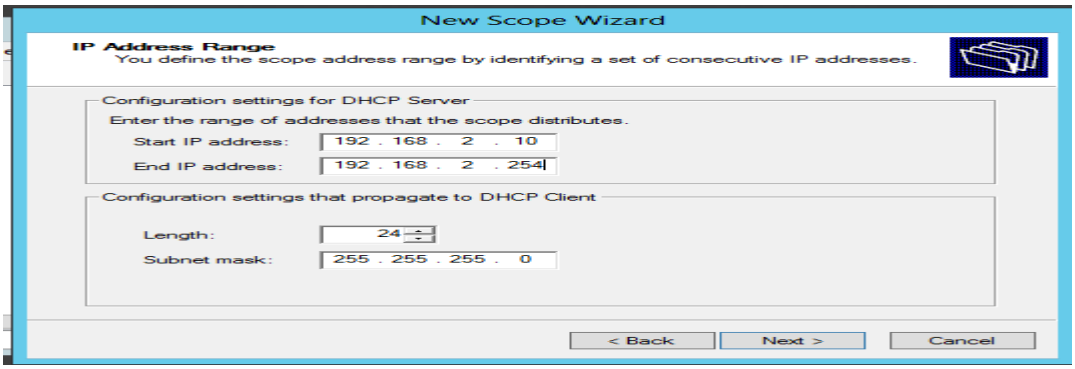


Figure V.9 : Configuration de la plage d'adresse pour DHCP.

II.5.Partage de Fichier et Monter un lecteur Réseau

A ce Niveau, il faut d'abord créer un dossier et le partagé, en choisissant **Everyone en Read/Write**, puis copier le chemin d'accès du dossier partagé, aller dans **Active Directory Utilisateurs et Ordinateurs** puis choisir l'utilisateur qui à le droit d'accéder à ce dossier, en faisant clic droit->puis **propriété**->. Choisir dans la fenêtre qui s'affiche l'élément **Profil** puis dans la partie **Profile Path** saisir la syntaxe suivante **\\nomduserver\%nom dedossier\%username%** puis cocher la case **Local Path** et coller dans la case le chemin du fichier copié lors du partage du dossier puis **Appliquer.**

Pour le montage d'un Lecteur Réseau, il suffit de cocher la case **connect** et une étiquette désignant le lecteur, coller le chemin d'accès du dossier partagé puis appliquer**.**

II.6.Installation de GNU / Linux Debian 7.3.0 :

Installation de GNU / Linux Debian 7.3.0 :

Il s'agit de la dernière version stable 7.3. Débian s'installe très facilement via Internet. Pour ce faire le choix de deux partions du disque a sélectionné:

- Une partition racine qui contiendra le système et tous ses composants (programmes, paramètres systèmes, etc.),
- et une partition (/home) qui va contenir les données des utilisateurs

Cette séparation permet de réinstaller le système en cas de problème sans perdre les données utilisateurs dans /home.

6.1Installation apache 2:

Apache est l'un des éléments les plus importants. C'est le serveur web qui va **délivrer les pages aux visiteurs**.

L'installation du serveur web apache version 2 avec ses dépendances se fait via la ligne de commande suivante :

Apt-get install apache2 apache2-common.

Pour vérifier il suffit de se connecter à l'adresse **http://127.0.0.1** ou bien **http://localhost** le massage suivant doit s'afficher : **It works!**

- Tous les fichiers de configuration sont présents dans le repertoire **/etc/apache2/**
- Tous les modes disponibles sont contenus dans le dossier **/etc/apache2/mods-available**
- Tous les modes activé sont dans **/etc/apache2/mods-enabled**. C'est la même chose avec les sites dans **/etc/apache2/sites-available** (et **enabled**).
- Par défaut, les sites sont dans le répertoire **/var/www**
- Les sites à héberger, nécessitent la création d'un fichier de configuration (appelé «Virtual Host») dans **/etc/apache2/sites-available** et activer ce site avec la commande **a2ensite**.

Un résumé des commandes utilisées dans apache2 est donné ci dessous:

- **a2enmod** : permet d'activer un mode pour apache (apache2 enable mod)
- **a2dismod** : permet de désactiver un mode (apache2 disable mod)
- **a2ensite** : active un site
- **a2dissite** : désactive un site
- **apache2ctl -t -D DUMP_MODULES** : permet de voir la liste des modules activés

6.2. Installation de PHP

PHP doit être installé pour gérer des **pages dynamiques**. La commande pour installer PHP et tous ses modules est la suivante:

Apt-get install libapache2-mod-php5 php5 php5-common.

6.3. Installation et Configuration de MySQL :

L'installation de MySQL permet de créer des tables SQL par la suite. Pour installer **MySQL**, il suffit de taper la commande :

apt-get install mysql-server mysql-client mysql-common

Lors de l'installation un mot de passe de super utilisateur est fournit.

Enfin il est très recommandé de lancer « **mysql_secure_installation** » pour sécuriser l'installation.

Puis rédemarrer le service mysql avec la commande :

/etc/init.d/mysql reload

6.4. Installation de «phpmyadmin» :

«**phpmyadmin**» est un SGBD bien plus pratique que «mysql» en ligne de commande. La commande suivante déclenche son installation :

apt-get install phpmyadmin

Durant l'installation il faut choisir le serveur web apache2 **avec la touche espace** du clavier et configurer la base de données utilisée avec la commande **dbconfig-common**.

Puis, un mot de passe de super utilisateur est fournit pour MySQL et phpadmin.

Une fois l'installation est terminée, redémarrer apache avec **/etc/init.d/apache2 reload**

Le lien **http://localhost/phpmyadmin/** permet de tester l'installation de phpmyadmin

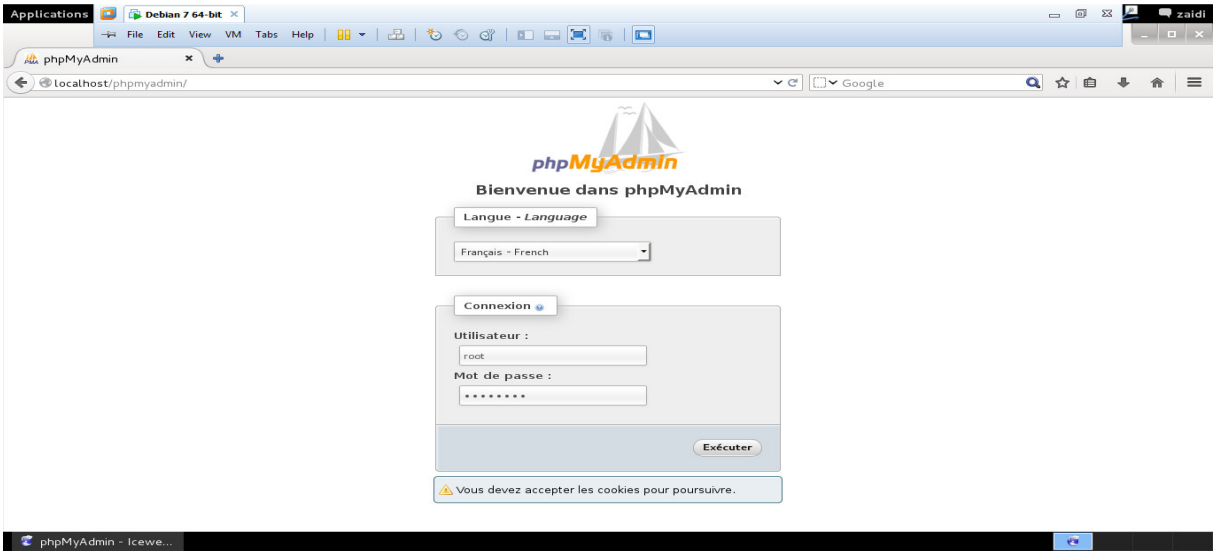


Figure V.10 : interface de phpmyadmin.

II.7.Installation et configuration d'un serveur de mail avec «Postfix» et «Courier» :

7.1. Installation de serveur de messagerie «Postfix»:

Dans le but d'envoyer des mails et pour gérer plusieurs adresses emails virtuelles (au moins une par nom de domaine) de la forme : contact@nomdedomaine.tld. il faut installer un serveur mail «Postfix».

L'installation de **postfix** se fait par la ligne de commande :

apt-get install postfix-mysql.

Remarque: Choisir « ***pas de configuration*** » pendant l'installation

Un paquet un peu spécial de postfix, avec une extension **-mysql,** a été installé. Cette version simplifie les choses, puisqu'elle permet d'utiliser une base de données MySQL pour stocker les différents comptes email et nom de domaine.

7.2. Création des tabe les SQL pour Postfix :

Il faut créer 3 tables pour Postfix :

- Une table « **domaines** » qui contient la liste des noms de domaine hébergés sur le serveur
- Une table « **comptes** » qui contient toutes les adresses emails virtuelles de la forme « contact@nomdedomaine.tld »
- Une table « **alias** » qui contient différents alias email qui ne sera pas utilisée.

Pour créer ces tables, il faut d'abord créer une base de données « postfix » avec un utilisateur « postfix » ayant tous les droits sur cette base.

7.3. Configuration de Postfix pour le lier à la BDD :

Une fois la base de données fonctionnelle avec toutes les tables et un utilisateur valide, et pour que les adresses mail puissent échanger des messages, Il faut relier postfix à la base de données avec la création des 5 fichiers de configurations pour expliquer à Postfix comment utiliser cette base de données.

Les fichiers de configuration à créer par requêtes sont :

- Une requête pour récupérer les Domaines: mysql-virtual_domaines.cf , Pour que postfix ait accès aux domaines, il faut écrire le code suivant dans /etc/postfix/mysql-virtual_domaines.cf

  Commande : nano /etc/postfix/mysql-virtual_domaines.cf

  hosts = 127.0.0.1
  user = postfix
  password = Mot de passe Mysql Postfix
  dbname = postfix
  select_field = 'virtual'
  table = domaines
  where_field = domaine
  additional_conditions = AND etat=1

- Une requête pour récupérer les Comptes email: mysql-virtual_comptes.cf

  Commande : nano /etc/postfix/mysql-virtual_comptes.cf

- Une requête pour récupérer les Alias: mysql-virtual_aliases.cf

  Commande: nano /etc/postfix/mysql-virtual_aliases.cf

- Une requête pour récupérer les correspondances Alias -> Comptes Mails: mysql-virtual_aliases_comptes.cf

  Commande : nano /etc/postfix/mysql-virtual_aliases_comptes.cf

- Une requête pour récupérer les Quotas: mysql-virtual_quotas.cf

  Commande : nano /etc/postfix/mysql-virtual_quotas.cf

7.4. Création de l'utilisateur et groupe vmail

Pour avoir une configuration assez propre et sécurisée, il faut créer un utilisateur et un groupe vmail qui se chargera de gérer/stocker les courriels sur les serveurs. Il faut préciser des UID et GID précis (5000) car ils seront utilisés plus tard dans un fichier de configuration.

Créer un groupe vmail avec le gid 5000 avec la commande :

groupadd -g 5000 vmail :

Créer un utilisateur vmail avec un uid 5000 et son répertoire personnel dans /var/spool/vmail. Ce répertoire regroupera les boîtes mail des utilisateurs

useradd -g vmail -u 5000 vmail -d /var/spool/vmail/ -m

7.5. Configuration de fichier principale main.cf :

Avant de pouvoir utiliser le système de courrier de Postfix. Quelques paramètres doivent être configurés. Postfix a plusieurs centaines de paramètres de configuration qui sont contrôlés par l'intermédiaire du fichier **main.cf**. Et la plupart ont des valeurs par défaut.
Par défaut le fichier est vide, car le choix de « *pas de configuration* » a été choisit auparavant pendant l'installation. Une fois cette configuration est terminée, on peut redémarrer Postfix et vérifier la configuration avec :

/etc/init.d/postfix restart
/etc/init.d/postfix check

7.6. Ajout d'adresses email virtuelles :

Pour compléter l'installation de postfix, il faut ajouter un nom de domaine et une adresse email virtuelle dans la base de données via phpmyadmin

- **Ajouter un nom de domaine :** Dans notre cas le domaine est **monmail.fr**
- **Ajouter une adresse virtuelle :** l'adresse virtuelle utilisée est contact@monmail.fr

Pour tester la configuration globale il suffit de se connecter avec telnet sur le port 25 et envoyer un email. De plus, l'envoi de ce premier mail créera automatiquement le dossier pour le nom de domaine dans /var/spool/vmail.

telnet 127.0.0.1 25
ehlo monmail.fr
mail from:<test@test.com>
rcpt to:<contact@monmail.fr>
data :
Bonjour
.
Quit

7.7. Installation de Courier pour la gestion de l'imap et pop :

1) Définition :

Courier doit être installé afin de gérer les protocoles «pop» et «imap», qui vont permettre de récupérer les emails via un client comme «Thunderbird» ou de mettre en place un «Webmin» comme «Roundcube». La liste des paquets à installer est la suivante:

- ✓ **courier-base**
- ✓ **courier-authdaemon**
- ✓ **courier-authlib-mysql**
- ✓ **courier-imap**
- ✓ **courier-pop**

2) Configuration :

La configuration de courrier permet de préciser qu'une base de données pour les adresses emails virtuelles est utilisée. le fichier «authdaemonrc» doit être modifié comme suit:

nano /etc/courier/authdaemonrc

authmodulelist="authmysql"

Les identifiants de connexion à la base de données et le nom des tables doivent être fournit et pour ce faire il faut modifier certaines lignes du fichier «authmysqlrc» :

nano /etc/courier/authmysqlrc

```
MYSQL_SERVER            localhost
MYSQL_USERNAME          postfix
MYSQL_PASSWORD          rootroot
MYSQL_DATABASE          postfix
MYSQL_USER_TABLE        comptes
MYSQL_CRYPT_PWFIELD     password
MYSQL_UID_FIELD         5000
MYSQL_GID_FIELD         5000
MYSQL_LOGIN_FIELD       email
MYSQL_HOME_FIELD        "/var/spool/vmail/"
MYSQL_MAILDIR_FIELD     CONCAT(SUBSTRING_INDEX(email,'@',1),'/',SUBSTRIN
G_INDEX(email,'@',1),'/')
```

Pour finir, il faut redémarrer les différents services courrier:

/etc/init.d/courier-authdaemon restart
/etc/init.d/courier-pop restart
/etc/init.d/courier-imap restart

7.8 Installation de «Webmail Roundcube» :

Le logiciel «webmail» sert d'interface entre un serveur de messagerie et un navigateur web.

«Webmail Roundcube» est une interface web pour consulter des courriers électronique (webmail).Il supporte les protocoles IMAP et SMTP.

- Téléchargement de la dernière version complète de «Roundcube» 1.1.1 sur le site https://roundcube.net/download/
- dé-zipper le fichier avec tar puis on crée un utilisateur pour héberger le code de roundcube :

tar -zxvf roundcubemail-1.1-stable.tar.gz
adduser roundcube

- Copier et renommer le dossier roundcubeemail-1.1 vers le repertoire /home/roundcube/www

mv roundcubemail-1.1 /home/roundcube/www

- changer l'utilisateur et le groupe pour que www appartienne à l'utilisateur roundcube.

chown -R roundcube:roundcube /home/roundcube

- Le code pour «Roundcube» est disponible dans le dossier /home/roundcube/www (comme pour les autres sites) et pour héberger ce site web dans apache, la technique d'hébergement virtuel est utilisée, (appellés des «virtual Hosts » dans Apache), d'où la nécessité de créer un fichier « virtual host » fonctionnant sous http (sur le port 80) :

vi /etc/apache2/sites-available/roundcube

```
<VirtualHost *:80>
ServerAdmin  send_to_samir91@yahoo.fr
ServerName  localhost
ServerAlias www.monmail.fr
DocumentRoot /home/roundcube/www
# SuexecUserGroup roundcube roundcube  on verra ça plus tard
  <Directory />
       Options FollowSymLinks
       AllowOverride All
 </Directory>
 <Directory /home/roundcube/www>
       Options FollowSymLinks MultiViews
       AllowOverride All
       Order allow,deny
       allow from all
 </Directory>
 ErrorLog ${APACHE_LOG_DIR}/error.log
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
LogLevel warn
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

- Creation de la base de données pour «Roundcube»:

La Création de la base de données pour Roundcube se fait dans phpmyadmin avec un utilisateur Roundcube qui possède tous les droits sur la base.

Roundcube à besoin d'une base de données prédéfinit, donc il faut importer le **fichier SQL mysql.initial.sql** pour créer les tables nécessaires à Roundcube avec la commande :

mysql -u root -p roundcubemail < /var/www/webmail/SQL/mysql.initial.sql

Puis un mot de passe de la base de données est fournit .

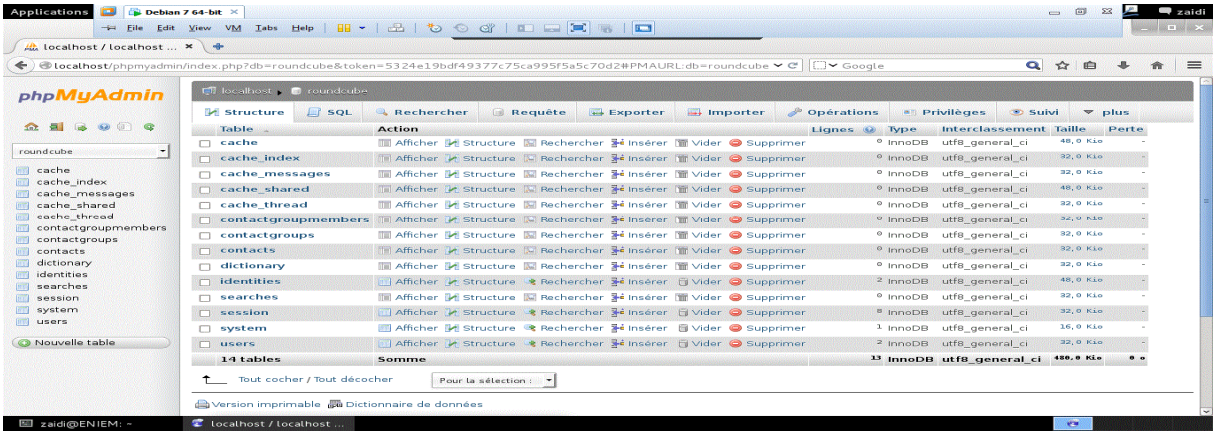


Figure V.11 : La base de données de roundcube

- Lancer l'installateur de roundcube sur la page **http://localhost/roundcube/installer.**
- A la fin de l'installation, enregistrer le contenue du fichier **config.inc.php** dans le répertoire **/home/roundcube/www/config**

La page http://localhost/roundcube permet d'afficher **le webmail**

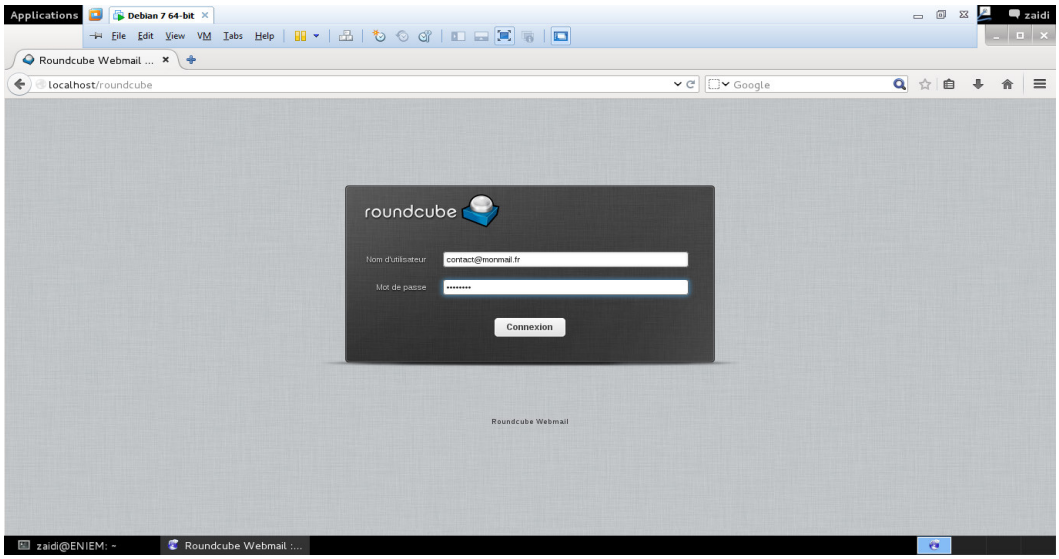


Figure V.12 : Roundcube Webmail / Login.

II.8.Hébergement d'un site web dans le serveur web apache:

Il faut configurer un site web statique avec l'adresse IP 127.0.0.1. Pour ce faire il faut procéder comme suit :

Comme apache est déjà installé, il faut créer un fichier « virtual host » fonctionnant sous http (sur le port 80) dans le répertoire **/etc/apache2/sites-available** avec **vi /siteEniem**

Puis redémarrer apache avec la commande :

service apache2 restart.

II.9.Installation et Configuration d'un serveur DNS :

1) Installation:

Il faut installer le paquet bind9 qui contient la dernière version du serveur de noms récursif **Bind** pour Debian.

Pour installer le serveur BIND9, il suffit d'installer le paquet **bind9** avec la commande :

apt-get install bind9

Tout se trouve dans le répertoire /etc/bind/ .

2) Configuration

Le but est de construire un serveur de nom local, qui sera capable de résoudre des noms d'hôtes sur le réseau interne à l'entreprise, mais également sur Internet.
Il faut créer un serveur DNS avec le domaine **Eniem.com** et l'adresse IP privées de serveur est **192.168.10.100**

- **Fixer l'adresse IP du serveur :**

  nano /etc/network/interfaces

This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).

The loopback network interface
auto lo
iface lo inet loopback

The primary network interface
allow-hotplug eth0
auto eth0
iface eth0 inet static
address 192.168.10.100
netmask 255.255.255.0
gateway 192.168.10.1
Broadcast 192.168.10.255

- Dans **/etc/hosts**, ajouter la ligne suivante pour que la résolution DNS pointe sur la machine (192.168.10.100)

192.168.10.100 Eniem.com

- Dans **/etc/resolv.conf** , modifier et entrez le domaine, la zone de recherche et le nom du serveur DNS comme suite :

Domain Eniem.com

Search Eniem.com

Nameserver 192.168.10.100

- **Configuration de la zone de recherché directe :**

Dans le repertoire **/etc/bind/,** Copier le fichier « db.local » en le renommant selon le nom de domaine :

cp db.local db.Eniem.com

ouvrir Le fichier nouvellement créé :

nano db.Eniem.com

Changez les paramètres en fonction du nom de serveur et du nom de domaine :

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     Eniem.com. root.Eniem.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@         IN      NS      Eniem.com.
@         IN      AAAA    ::1
@         IN      A       192.168.10.100
www       IN      A       192.168.10.101
mail      IN      A       192.168.10.100
;
www.mail  IN      CNAME   mail
```

- **Configuration de la zone de recherche inverse :**

Copier le fichier « db.127 » en le renommant avec :

cp db.127 db.Eniem.com.inv

Ouvrir et Changer les paramètres de fichier **db.Eniem.com.inv** en fonction du nom de serveur et du nom de domaine :

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     Eniem.com. root.Eniem.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
```

```
                    604800 )      ; Negative Cache TTL
;
@       IN      NS      Eniem.com.
101     IN      PTR     www.Eniem.com.
100     IN      PTR     mail.Eniem.com
```

- **Création de la zone locale :**

Le fichier **/etc/bind/named.conf** correspond au fichier de configuration principal.

Le fichier **/etc/bind/named.conf.local** correspond au fichier qui va contenir la définition de l'ensemble des domaines appellé zone.

Définir la zone Eniem.com et la zone inverse 10.168.192.in-addr.arpa de cette manière la double correspondance suivante est reconnue:

IP : Nom de domaine FQDN

Nom de domaine FQDN : IP

Créer une zone locale. Pour cela il faut éditer le fichier **named.conf.local** pour définir le domaine et le fichier contenant les enregistrements DNS.

```
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "Eniem.com" {
        type master;
        file "/etc/bind/db.Eniem.com";
        forwarders{};
};
zone "10.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.Eniem.com.inv";
        forwarders{};
};
```

Puis redémarrer le service :

/etc/init.d/bind9 restart

Enfin, pour tester le serveur DNS, accéder à l'interface de webmail en allant sur le lien **http://www.mail.eniem.com** et au serveur web avec **http://www.eniem.com**

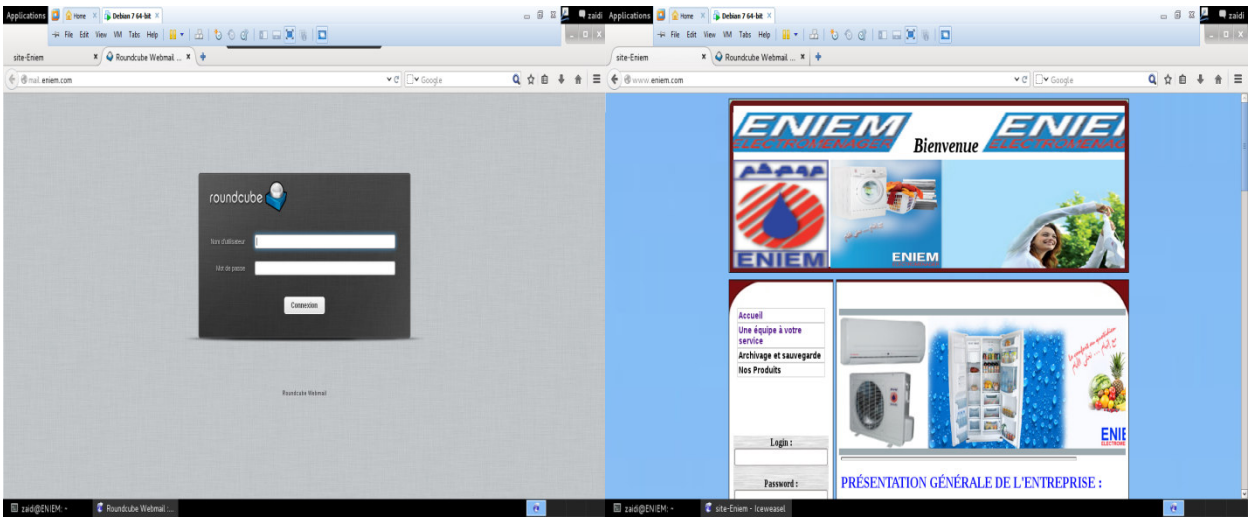


Figure V.13 : Shéma de test du DNS

II.10.Installation et configuration de pare-feu Sophos UTM 9.1 :

1) Installation :

Dans le premier écran de boot qui est déjà « prévenant », il y a des fonctions de dépannage sur l'image de boot. Sur le second écran d'installation, nouvel avertissement indiquant que le disque va être effacé.

Dans la phase d'installation suivante, le matériel est détecté et l'installeur affiche ensuite un résumé du matériel détecté. la disposition du clavier, la « time zone » et l'heure sont ensuite saisis.

La carte « Interne » (eth1) sur laquelle l'application Web d'administration sera utilisée et son adresse IP sont ensuite définies.

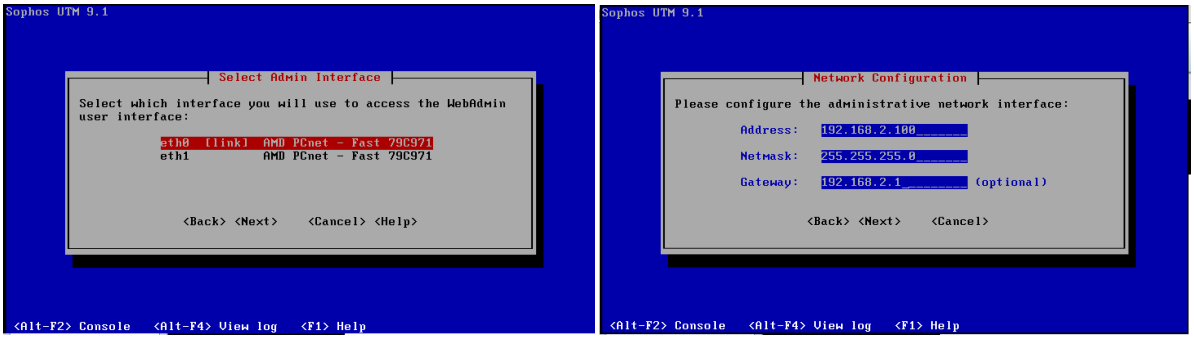


Figure V.14 : configuration de la carte réseau.

Utiliser une architecture 64bits,

L'installation continue, pendant quelques minutes et à la fin une demande de reboot avec une indication de la manière dont nous devons connecter à la console d'administration avec https://192.168.2.100:4444.

Au reboot un écran blanc, qu'on peut « colorer » en pressant F2 pour voir dans le détail les informations de chargement.

Figure V.15 : Lancement de pare-feu sophos

Première connexion sur le webadmin, la connexion se fait par la machine client windows 7 sur le lien https://192.168.2.100:4444

Configuration de pare-feu :

Dans Cette étape le pare-feu est configuré avec 2 cartes réseaux d'adresses IP suivantes :

- eth0: WAN interface (Ethernet) 10.10.10.2/24 sans DHCP
- eth1: LAN 192.168.2.100/24 sans DHCP

Une 3 éme carte réseau qui présente la DMZ est ajoutée avec l'interface de gestion du pare-feu comme suit

- eth2: DMZ 192.168.10.1/24 sans DHCP.

A la Première connexion sur le «Webadmin», le système affiche un écran des informations de l'entreprise, d'un mot de passe et de l'adresse mail de l'administrateur. Après enregistrement de ces paramètres (« perform basic setup »), un l'écran d'authentification du «Webadmin» pour la saisie des informations d'identification de l'administrateur est affiché.

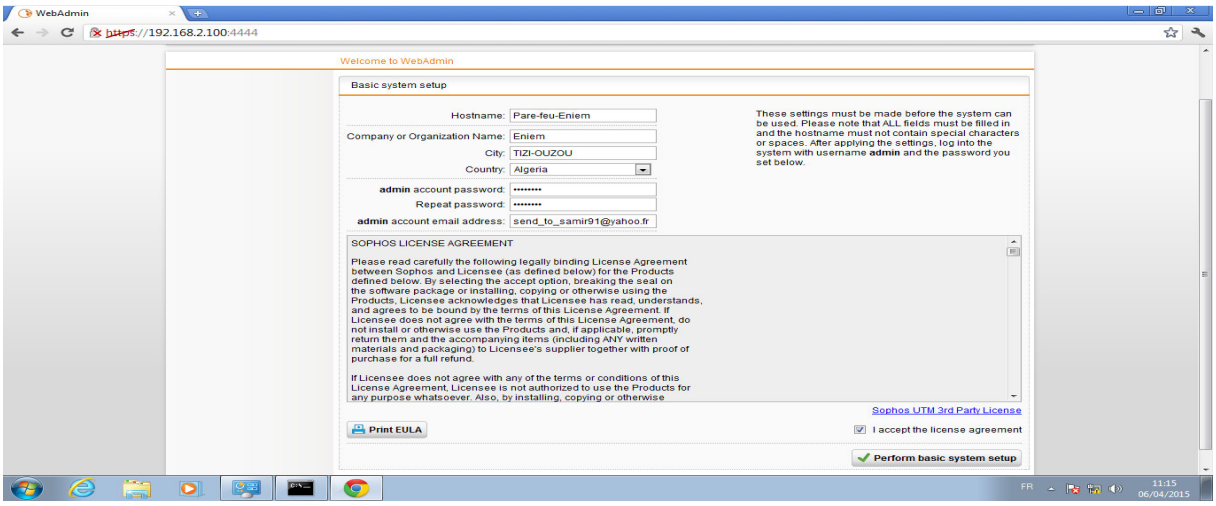


Figure V.16 : Paramétrage des informations d'identification d'administrateur.

Après avoir Entrez les informations d'identification d'administrateur un assistant de configuration petite est lancé.

L'étape suivante permet d'enter l'adresse IP de l' interface LAN avec le masque /24 :

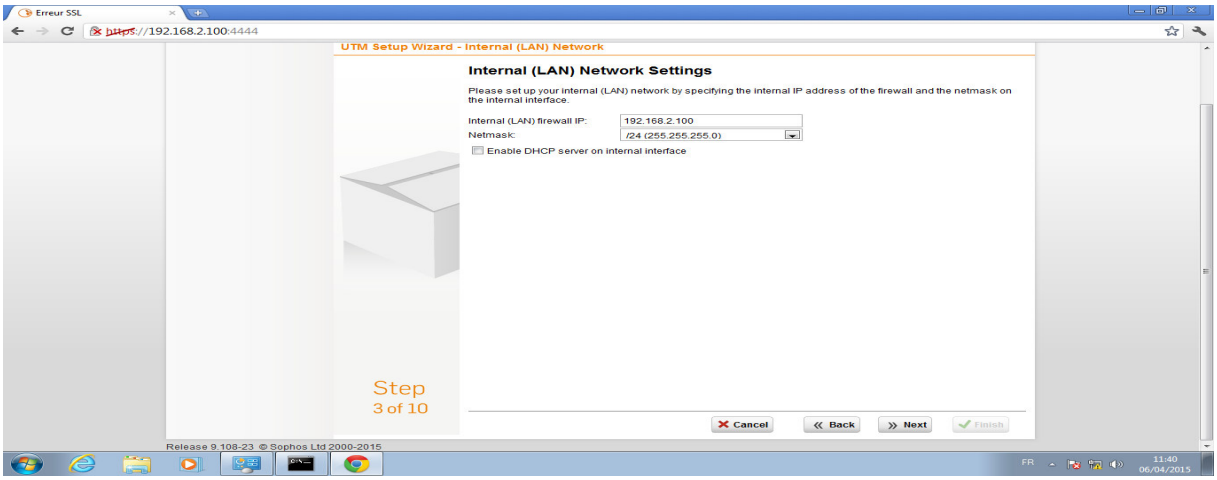


Figure V.17 : confirmation des informations pour l'interface interne

L'écran suivant invite à saisir les informations concernant la carte externe WAN : choisir eth0 avec l'adresse IP 10.10.10.2 /24

Puis choisir les règles de pare-feu et définir les services auxquels les clients du réseau local devraient être autorisés à accéder.

Il est aussi possible de spécifier certaines règles de groupe d'ips qui doit être actif dans la configuration initiale.

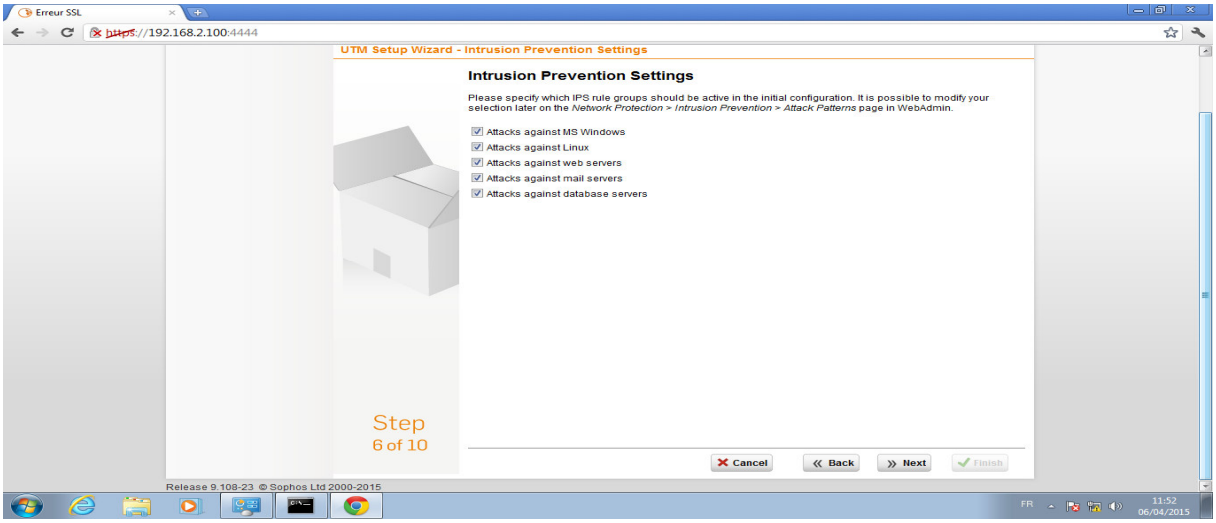


Figure V.18 : Spécification des règles ips.

Comme il est possible de :

- ✓ d'activer la visibilité du réseau
- ✓ de bloquer, ou réduire le débit pour certaines applications ou certains sites particuliers utilisant le protocole http (Facebook, Skype…) ou en « accélérer » certains.

L'écran suivant permet de paramétrer le filtrage web et le filtrage de pop3 (antivirus et spam), , pour lequel il faudra fournir l'adresse et le domaine concerné.

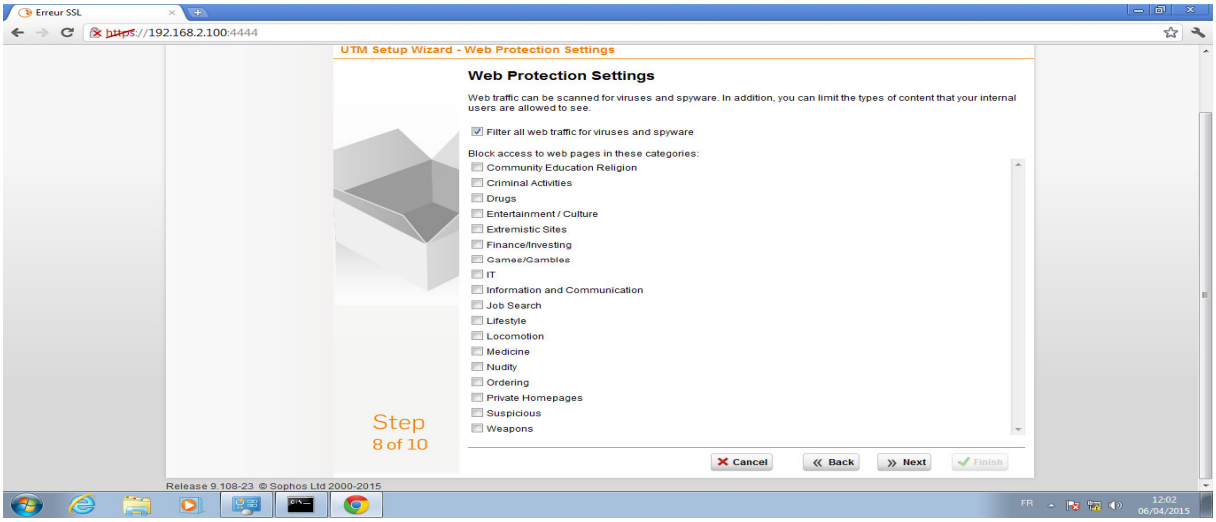


Figure V.19 : paramétrage du filtrage web

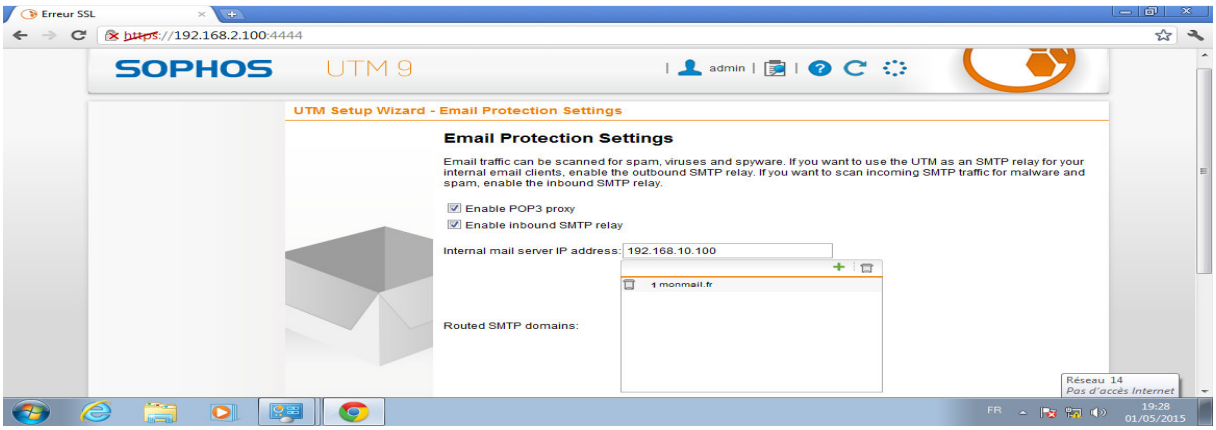


Figure V.20 :paramétrage de protection de mail

Un écran résumé de l'installation est affiché à la fin de cette dernière.

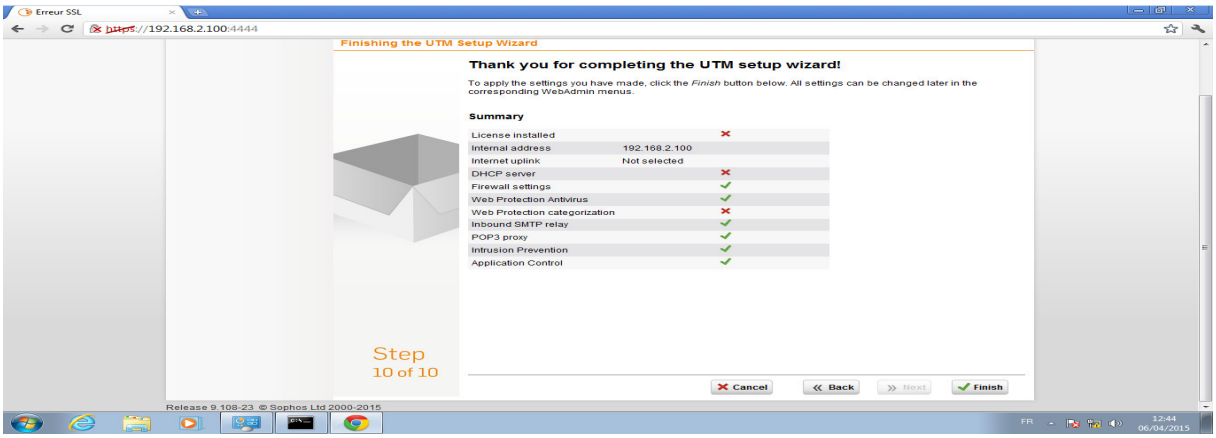


Figure V.21 : Résumer de l'installation.

II.11.Configuration de l'interface DMZ :

Une nouvelle interface pour la DMZ est configurée avec l'interface de gestion du pare-feu :

Dans l'option **interfaces et routage→Interfaces→Nouvelle interface** .

Fournir les informations suivantes pour la nouvelle interface.

- Une interface Ethernet statique sur eth2 de matériel avec un nom DMZ.
- l'adresse IP 192.168.10.1/24. sans définir une passerelle par défaut

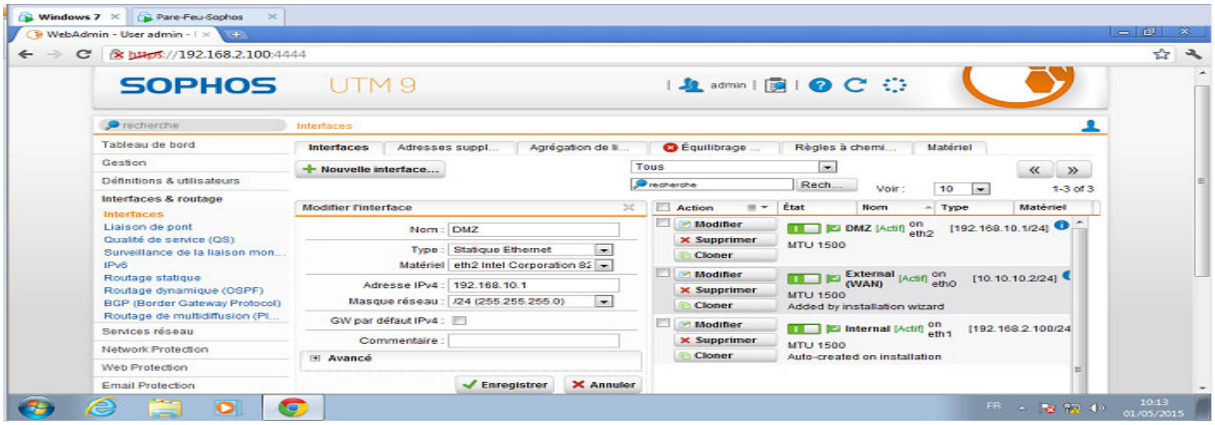


Figure V.22 : Configuration de l'interface DMZ.

NB : l'interrupteur permet d'activer l'interface.

II.12.Configuration Les ordinateurs de poste client sur le réseau interne :

Pour acceder à la « DMZ » (web mail et web serveur). Il suffit de modifier le protocole version 4 (TCP/IPv4) comme suite :

- Adresse IP:192.168.2.120
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.2.100
- Serveur DNS : 192.168.10.100

Une manière de s'assurer de la réussite de la connexion, c'est d'utiliser un « ping » entre les serveurs mail et web et un client connecté.

Le client peut accéder aux serveurs mail web avec http://www.eniem.com et http://mail.eniem.com:

II.13.Configuration d'une connexion « VPN » pour les utilisateurs externe :

Accès à distance via SSL :

La configuration d'un accès à distance à l'UTM, en utilisant le protocole Secure Sockets Layer (SSL) est décrit ci dessous.

La fonctionnalité Sophos 'VPN SSL réutilise le port TCP 443 pour établir un tunnel chiffré à l'entreprise, permettant d'accéder à des ressources internes.

- **Configuration des Profiles SSL :**

  Pour créer un Profile SSL, procéder comme suit :

- Choisir l'option **Accès à distance -> SSL-> Profils** puis la sous option **nouveau profil d'accès distant**

Un écran de saisie permet de fournir les informations suivantes :

- **Nom de profile** : donner un nom de profile (ex :SSL Profiles)
- **Utilisateur et groupe** : compte utilisateur (ex : « vpn_user1 »)
- **Les réseaux locaux**: les réseaux locaux qui devraient être accessibles aux clients SSL (interne (réseau) qui est le réseau interne 192.168.2.0/24).

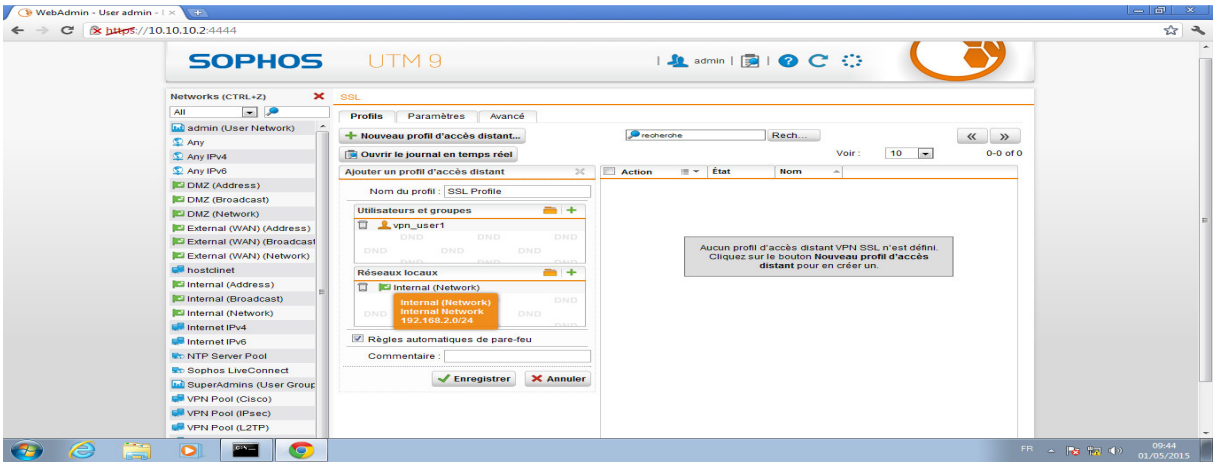


Figure V.23 : Interface de Configuration de profile SSL.

- **Configuration des paramètres avancés « SSL » :**

Dans la section Paramètres du serveur, seulement les paramètres suivants seront définit:

- **Remplacer le nom d'hôte**: donner l' adresse ip ethernet WAN 10.10.10.2

  Un pool d'adressage: Les paramètres par défaut attribuent des adresses IP à partir de l'espace privé 10.242.2.x / 24. Ce réseau est appelé Pool VPN (SSL). Laisser la valeur par défaut

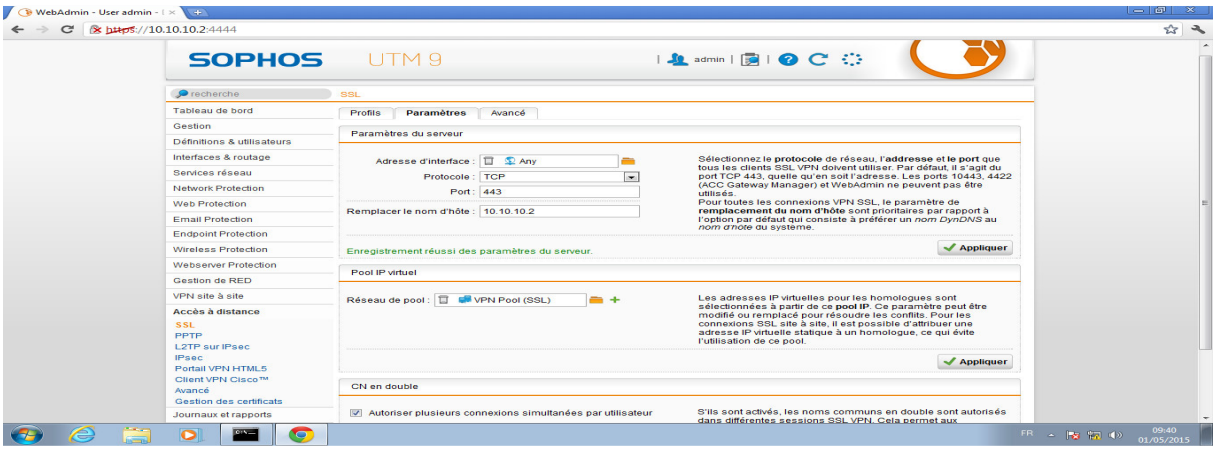


Figure V.24 : Interface des paramètres avancée de SSL

➢ **Création des règles de pare-feu :**

- **Définition d'une règle de pare-feu :**
- l'option **Firewall> onglet Règles de protection du réseau.** La Nouvelle règle est créée via les paramètres suivants:

Sources: l'hôte distant ou un utilisateur (ex: vpn_user1).

Services: ajouter les services autorisés.

Destination: ajouter les réseaux autorisés (ex: interne (réseau)) pour l'utilisateur distant pour être en mesure d'accéder à Internet,

Action: sélectionné Autoriser.

Par la suite il faut activer et enregistre cette règle.

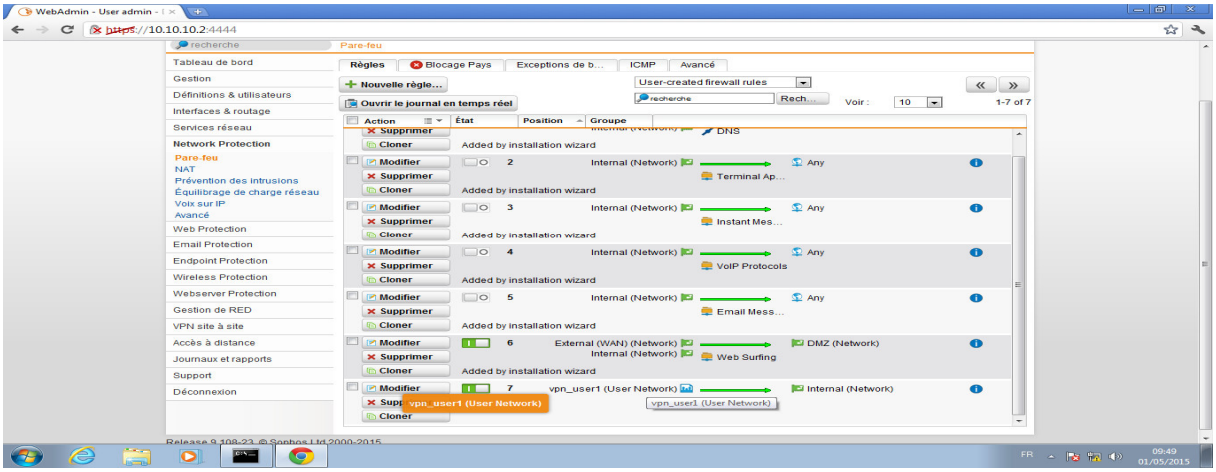


Figure V.25 : Interface des règles de pare-feu

➢ **Activer le portail d'utilisateur :**

- Dans l'option **Portail de d'utilisateur -> onglet Global Management**. L'utilisateur du portail doit être activé pour l'utilisateur d'accès distant. En spécifiant aussi les réseaux qui sont autorisés à accéder au portail de l'utilisateur (utiliser « **any »** l'accès aux réseaux interne et externe).

➢ **Configuration du client à distance :**

✓ D'abord Il faut modifier le protocole version 4 (TCP/IPv4) :

- Adresse IP:10.10.10.1
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 10.10.10.2
- Serveur DNS : 192.168.10.100

✓ **Obtention de logiciels et de certificats :**

- Le lien https: // 10.10.10.2 permet d'ouvrir le portail utilisateur Une note de sécurité sera affichée. Qui doit être acceptée.
- Après la Connexion au portail utilisateur avec les identifiants crée précédemment des outils et / ou la configuration guide pour la configuration de la connexion d'accès distant peuvent être téléchargés sur la page d'accès à distance

✓ **Installation du logiciel client VPN SSL :**

Après le téléchargement de logiciel client l'exécution de ce dernier permet de démarrer l'installation

- ✓ **Connexion au VPN :**

Après l'installation du logiciel, se connecter avec le nom d'utilisateur et le mot de passe puis L'état de la connexion est indiqué par l'icône VPN SSL. :

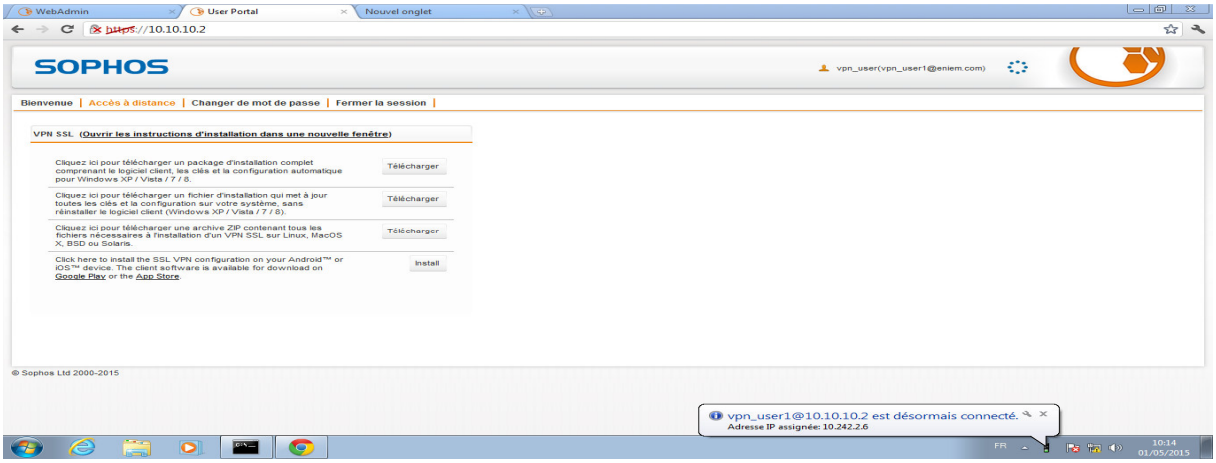


Figure V.26 :l'état de la connexion d'n client VPN.

II.14.Sécurité de pare-feu :

Les utilisateurs interne et externe ne peuvent accéder qu'à la DMZ. Ils ne peuvent pas accéder au réseau~~x~~ Lan de l'entreprise et grâce à la sécurité assurée par le pare-feu sophos , les requêtes Ping pour l'interface Lan et pour l'interface Wan ont été rejetées.

Un pirate ne peut jamais parvenir à l'adresse IP de l'interface utilisée pour le Wan et ses failles restent inexploitables.

V.2 Conclusion :

Le réseau est sécurisé et les usagers externes ne peuvent accéder qu'à la DMZ, par contre ils ne pourront pas accéder au réseau LAN, ni même percevoir son existence, ainsi la segmentation logique de l'architecture physique en VLAN et la mise en place d'un annuaire Active Directory pour la gestion centralisée des ressources, le réseau interne est aussi sécurisé.

Conclusion Générale

Ce travail a été principalement axé sur la sécurisation des communications client-serveur basées sur « multiples plates-formes» (Windows et linux). L'objectif de ce travail consiste en le déploiement des infrastructures réseaux et l'exploration des techniques de mise en œuvre de la sécurité d'un réseau local telles que les techniques de filtrage des paquets à travers un pare-feu, la segmentation en VLANs, les GPOs dans Windows server etc…..

Bien qu'étant un puissant outil pour sécuriser un réseau, une seule plate-forme toute seule ne peut fournir la protection complète souhaitée, ainsi la sécurité d'un réseau ne doit pas se baser sur un seul mécanisme. Une imbrication de mécanismes offre une garantie de sécurité bien supérieur, d'où la nécessité d'inclure des mécanismes multiples sur différents environnements.

Sécuriser un tel système consiste à assurer la confidentialité, l'intégrité et la disponibilité de ses données et ressources. De nombreux travaux ont été réalisés et plusieurs dispositifs de sécurité ont été proposés pour garantir ces propriétés. Parmi ces dispositifs les pare-feu occupent une place de premier ordre et sont des éléments cruciaux pour le renforcement d'une politique de sécurité. Ils sont largement déployés pour la sécurisation des réseaux informatiques. Le pare-feu est l'outil le plus utilisé pour sécuriser un réseau grâce à ses capacités de renforcer une politique de sécurité et d'enregistrer tous les aspects du trafic réseau.

Ce stage réalisé en entreprise à la fin de notre cycle de Master en sécurisation des communications client-serveur basé sur «multiples plates-formes» qui nous a permis de mettre en pratique et de consolider les connaissances acquises lors de notre cursus universitaire et de nos recherches personnelles. Grâce à ce travail, nous avons pu cerner des connaissances pratiques qui nous étaient inconnu auparavant, à savoir se familiariser avec le monde de travail en entreprise, car connaitre les pressions et les occupations des employés nous donnent l'opportunité de se préparer psychologiquement pour faire face à cette réalité.

En estimant que la solution proposée à notre organisme d'accueil «ENIEM » permettra de colmater les brèches constatées au niveau du département informatique, par le biais des deux plates-formes, il y aura non seulement une sécurité digne de ce nom mais aussi une gestion de réseaux effective, sans oublier un nombre important de fonctionnalités disponibles, et nous espérons aussi que ce travail sera utile pour la future génération.

Glossaire

LAN : Local Area Network

IP : Internet Protocol

HTTP : HyperText Transfert Protocol

GBIC : Gigabit Interface Converter

DTC : Data Terminal Circuit

DDP : Panneau de Distribution Direct

MDP : Panneau de Distribution Modem

AUI : Association des Utilisateurs Internet

BNC : Bayonet Neil-Concelman Connector

DCT : Discrete Cosine Transform

DVD : Digital Versatil Disque ou Digital Vidéos Disque

DDS : Digital Data Sotrage

SEI : Service Exploitation Informatique

SDSI : Service Développement des Systèmes Informatiques

MAN : Métropolitain Area Network

PAN : Personnel Area Network

WAN : Wide Area Network

OSI : Internationnal Standardization Organisation

DNS : Domain Name Service

ASCII : American Standard Code For Information Interchange

FTP : File Transfert Protocol

TFTP : Trivial File Transfert Protocol

SNMP : Simple Network Management Protocol

NFS : Network File Systèm

SQL : Strutured Query Langage

RPC : Remote Produre Call

TCP : Transport Control Protocol

UDP : Unit Data Protocol

ARP : Adresse Résolution Protocol

RARP : Reverse Adress Résolution Protocol

ICMP : Internet Control Message Protocol

AES : Advanced Encryption Standard

RSA : Rivest Shamir Adleman

VPN : Virtuel

HDLC : High Level Data Link Control

IEEE : Institute of Electrical and Electronic Engineer

ETCD : Equipement Terminal de Circuit de données

ETTD : Equipement Terminal de Tratement de données

DOD : Department of Defense

DOS : Deny of Service

IPSEE : IP Sécurity

SSL : Secure Socket Layer

TLC : Transport Layer Security

ACK :ACKnowledged

SYN : Synchroniser

DZM : Zone Démilitarisée

SSH : Secure Shell

SGBD : Système de Gestion des Base de Données

DCOM : Distruted Conponent Object Model

MOM : Message Oriented Middleware

NOS : Network Operating System

RAM : Random Access Memory

DHCP : Dynamic Host Configuration Protocol

NAP : Network Access Protection

RODC : Read Only Domain Controller

ADFS : Active Directory Fédération Service

SAM : Security Account

LDAP : Light Directory Access Protocol

AD : Active Directory **GPO** : Group Policy Management

BIBLIOGRAPHIE

LES LIVRES

[III.1]: N. Stouls and M.-L. Potet. Security policy enforcement through refinement process. In *Proc. of Formal Specification and Development in B, 7th International Conference of B Users (B2007), LNCS 4355*, pages 216–231. Springer-Verlag, January 2007.

[III.2]: *Andrew Tanenbaum*, **« Systèmes d'exploitation »,** 2e édition, PEARSON Education,2003

Laurent BlochChristophe Wol fhuge **Sécurité Informatique Principes et méthode à l'usage des DSI, RSSI et administrateurs,** 2e édition,2009

Emmanuel Viennet Réseaux Module ARS3 DUT GEII ,2012-2013

MEMOIRES

[1] Mémoire : *marfall n'diaga fall* **Théme :Sécurisation formelle et optimiséede réseaux informatiques,** faculté des sciences et de génie université laval québec,octobre 2010

[2] Mémoire : *Julien Iguchi-Cartigny* **théme Scénarios d'Attaques et Détection d'Intrusions** Université de limoges ,du 04 Mars au 30 Août 2013

LES SITES WEB

- http://www.tutoriels-video.fr/installation-et-configuration-dun-serveur-dedie-debia/
- http://paice.info/2014/03/sophos-utm-9-installation-configuration-et-parametrage-partie-1-version-gratuite/
- **[VI.1]** : www.wikipedia.org