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

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

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

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes
de MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**

Filière : **Informatique**

Spécialité : **Réseaux, Mobilité et Systèmes Embarqués**

Présenté par

M^r.: DERRIDJ Amar

M^elle.: YAGOUB Dyhia

Thème

Conception et Implémentation d'une Architecture Réseau.
< CAS : ENIEM >

Mémoire soutenu publiquement le 18/07/2016 devant le jury composé de :

Président : M^r HABET Mohammed-Said

Encadreur: M^r *Soulaha Mohammed ourabah*

Co-Encadreur : M^r F.TALEB

Examinateur: M^r YASLI

Examinateur: M^r BELATTAF

REMERCIEMENTS

Je remercie d'abord le bon Dieu de m'avoir donné le courage, la patience et la volonté fine d'accomplir mon parcours.

Je tiens à remercier particulièrement mon enseignante

Et mon promoteur Mr: M. ourabeh. soualah

etMr. TALEB Ferhat pour leurs qualité d'encadrement et pour leurs suivi, leurs orientation, leurs remarque pertinente et précieuses durant la réalisation du notre projet.

de m'avoir fait confiance et m'avoir encouragé tout au long de ce projet.

Un grand merci à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Enfin, mes remerciements s'adressent aux membres du jury

qui vont me faire l'honneur de juger mon travail.

Dédicaces

Je dédie ce modeste travail

ADieu le tout puissant de m'avoir prêté longue vie
Pour arriver au terme de ce projet.
A mes très chersparents qui ont veillez sur moi pour que
je me retrouve là où je suis aujourd'hui.
Ama très chère sœur Dehbia.
Amesneveux Hamid& Mohand& Aylane.
A toute ma famille et mes proches.
Atous mes amiesavec qui j'ai partagé des beaux et inoubliables
moments de ma vie : Anis, Hakim, Hacène,Jugurtha,
Samia, Massi, Zahir et Samy…..
Et toute la promotion Master II 2015
Atoutes les personnes qui m'ont aidé de prés et de loin.

Amar…

Dédicaces

Je dédie ce modeste travail

ADieu le tout puissant de m'avoir prêté longue vie
Pour arriver au terme de ce projet.
A mes très chersparents qui ont veillez sur moi pour que
Je me retrouve là ou je suis aujourd'hui.
Ama très chère sœurAldjia.
Ames frèreSaid, Amirouche, Massi ,Takfarinas.
A toute ma famille et mes proches.A mon binôme
Amar & sa famille.
Atous mes amiesavec qui j'ai partagé des beaux et inoubliables moments de ma vie : Samia, Fazia, djamila, Aymene, Faroudja…..

Atoutes les personnes qui m'ont aidé de prés et de loin.

DYHIA…

Chapitre II

Chapitre IV

Introduction Général

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plus part raccordés à l'Internet.

En ce moment, les entreprises ont pensé à trouver une solution pour gérer leur trafiques réseau mais elles cherchent toujours des solutions moins couteuses et efficaces, en effet, si un représentant a besoin d'accéder à distance au réseau privé de son entreprise alors qu'il est à des milliers de kilomètres de celle-ci, le coût de l'appel téléphonique sera extrêmement élevé, notamment si l'entreprise a plusieurs bureaux à travers tout un pays.

L'entreprise Nationale des Industriels de l'Electroménager (ENIEM) est une entreprise Spécialisée dans la production et la commercialisation des produits électroménagers, elle manipule une masse de données importante, en effet elle voudrait améliorer ces capacités. Dans ce contexte l'ENIEM veut une technique qui permet de résoudre des problèmes de très grande taille en un bref délai.

Pour la bonne organisation de notre travaille nous avons adopté le plan suivant :

- **Chapitre 1 :«**présentation de l'organisme d'accueil » : il donne une idée générale sur l'entreprise ENIEM et situe le cadre de notre travail.
- **Chapitre 2 :** « généralités sur les réseaux informatiques » : étant un moyen très important pour la transmission de données, les réseaux informatiques
- **Chapitre 3 :**SécuritéInformatique

  Différentes aspects sécurités Informatique (FIREWALL, ANTIVIRUS, ACL, VLAN etc……).
- **Chapitre 4** : Conception et Réalisation

Chapitre I

Présentation de l'organisme d'accueil

Introduction

L'économie nationale traverse actuellement une phase difficile et les entreprises publiques &économiques doivent faire des efforts pour se conformer à un nouvel environnement dont l'étape essentielle et vitale est l'adaptation de leurs produits aux nouvelles exigences technologiques et aux normes internationales.

L'ENIEM qui a une place parmi les géants de l'électroménager à travers le monde a engagé un certain nombre d'opérations, à même de lui permettre d'atteindre cet objectif. C'est ainsi qu'après la suppression des CFC en avril 1997, il s'est fixé comme second objectif de la certification de l'entreprise. Cette dernière opération a connu un grand succès et l'entreprise se trouve certifié à l'ISO 9002 depuis juillet 1998.

Vu l'importance de l'ENIEM, ainsi que son activité intense, nous avons effectué notre stage au sein de celle-ci.

Figure I.1. ENIEM

I.1. Présentation de l'ENIEM

I.1.1 Historique

L'entreprise **N**ationale des **I**ndustries de **l**'Electro**m**énager**« ENIEM»** est le fruit d'un contrat signé le 21 /08/1971 avec un groupe d'entreprises Allemandes pour une valeur de 400millions Dinars. Elle est issue de la restructuration de l'entreprise **SONELEC** (**So**ciété **N**ationale de fabrication et du montage **El**ectrique et **El**ectronique) le 2 janvier 1983, et disposait à sa création de :

- Complexe d'appareils ménagers (CAM) de T.O, Entré en production le juin 1977.
- Aujourd'hui son capital social est de 2.957.500,00 Da détenu en totalité (100%) par l'état.
- Unité lampe de Mohammedia(ULM) entrée en production le février 1979.

Dans le cadre des réformes économiques décidées par le gouvernement, l'ENIEM a été transformée juridiquement, le 8 octobre 1989, d'une entreprise publique et économique (EPE) à celui d'une société par actions (SPA).Depuis 1996 l'entreprise est organisée en unités, et filialise l'unité lampes de Mohammedia. Elle était repartie en trois organisations : **U**nité **L**ompe **M**ohammedia « l'ULM », **U**nité **S**anitaire **M**ELIANA « l'USM » et le **C**omplexe d'**A**ppareil **M**énager « CAM », à son tour le CAM est reparti en cinq unités le 1997.

L'ENIEM est la première entreprise de Maghreb à être certifiée ISO 9002 depuis le premier juillet 1998 par les experts de l'association française de l'assurance de la qualité (AFAQ), puis gratifiée en 2003 de l'ISO 9001 <<version 2000>>. A noter que les produits ENIEM sont 0% CFC (Chlora Fluora Carbones), et ce depuis 1997.
Le champ d'activité de l'entreprise ENIEM consiste à la production, le développement, la recherche dans le domaine de l'électroménager, ainsi que la prise en charge de la fonction commerciale, la promotion des exportations et de service après-vente. Actuellement, l'entreprise ENIEM est constituée de :

- ✓ La direction générale.
- ✓ Unité froid.
- ✓ Unité cuisson.
- ✓ Unité climatisation.
- ✓ Unité présentation techniques(UPT).
- ✓ Unité commerciale (UC).
- ✓ Unité produit sanitaires.
- ✓ La filiale FILAMP.

I.1.2 Situation géographique de l'ENIEM

Le complexe d'appareils ménagers (CAM) se trouve au sein de la zone industrielle d'Oued AISSI 10 Km àl'est de Tizi-Ouzou. Il s'étale sur une superficie de 55 hectares et relève administrativement de lacommune de TIZI-RACHED, Daïra de L.N.I.La filiale sanitaire est installé à MILIANA, wilaya d'AIN DEFLA et la filialelampe à MOHAMMADIA, wilaya de MASCARA. La direction générale se situe au chef-lieu de TIZI-OUZOU à proximité de
L'ancienne gare ferroviaire.

I.1.3 Missions

Dans le cadre de développement économique et social, l'ENIEM assure les fonctions suivantes :La production, le montage, la commercialisation et la recherche dans les différentes branches de l'électroménagernotamment :

- ✓ Les équipements ménagers domestiques.
- ✓ Les équipements industriels.
- ✓ Le petit appareil ménager.

Elle assure également la production :

- ✓ Des appareils réfrigérateurs et congélateurs des différentes capacités (160L à 520L).
- ✓ Des cuisiniers à gaz 4 et 5 feux, dont la production atteint 150 000 appareils par ans.
- ✓ Des climatiseurs types fenêtres et Split système (1CV à 2,5 CV) : à raison de 500 000 appareils par ans.

I.1.4.Objectifs

Parmi les principaux objectifs de l'ENIEM nous citons :

- ✓ Mettre en place un système de management environnement selon la norme ISO 14001.
- ✓ Développer la formation et la communication.
- ✓ Développer les produits.
- ✓ Augmenter les productions.
- ✓ Améliorer les chiffres d'affaires.

NB/ A savoir que l'ENIEM a atteint un taux de production de 97% des objectifs.

I.1.5.Organisation

L'ENIEM se présente comme suit :

- Elle est administrée par un conseil d'administration et dirigé par le directeur général.
- Le directeurgénéral exerce son autorité hiérarchique et fonctionnelle sur l'ensemble des directions et des unités

Pour mettre en évidence tous ces points, nous présentons dans ce qui suit l'organigramme général de l'**ENIEM** :

Organigramme général de l'ENIEM

Figure. I .2 organigramme général de l'ENIEM

I.2. Mode d'organisation

I.2.1. Les directions

1. Direction générale

La direction générale, l'unique entité qui est responsable de la stratégie et du développement de l'entreprise. Elle exerce son autorité hiérarchique et fonctionnelle sur l'ensemble des directions et des unités.

2. Direction des ressourceshumaines

En cohérence avec la politique qualité de l'entreprise, la fonction Ressources humaines accroit la mobilisation et la valorisation du personnel qui assure des servicesclient.

Elle pilote le recrutement, l'accueil, l'information et gère le plan de carrière dupersonnel. Elle conçoit le plan de formation à partir du recueil des besoins collectifs etindividuels et s'assure de son exécution.

Elle supervise la gestion administrative et légale pour le personnel et les pouvoirspublics en respectant les objectifs de conformité, de fiabilité et délais.

Elle doit en outre :

- ✓ Encourager les actions nécessaires à la rationalisation des effectifs et àl'émergence des compétences.
- ✓ Rédiger, vérifier et approuver les dispositions décrites, relatives aufonctionnement efficace de son activité.
- ✓ Définir et exécuter les plans de formation en fonction des besoins de l'entreprise en suivant les niveaux de qualification du personnel.

3. Direction des finances et comptabilité

Cette direction est auditée au moins une fois par un commissaire au compte, sa mission globale est :

- ✓ Garant des obligations légales, des règles comptables et des procédures de l'entreprise, dont elle vérifie l'application par la mise en œuvre d'un contrôle interne.
- ✓ Recherche et mobilise dans les meilleures conditions de délai et de cout le besoins en ressources financières.
- ✓ Analyse les équilibres financiers de l'entreprise.
- ✓ Etudie et met en place la stratégie financière de l'entreprise (plan de financement à long terme).
- ✓ Gère la trésorerie (recette et dépenses).
- ✓ Contrôle les déclarations fiscales périodiques.
- ✓ Analyse les couts et les prix de revient.
- ✓ Met à la disposition des responsables opérationnels l'information financière nécessaire.

- ✓ Rédige, vérifie et approuve les dispositions décrites relatives au fonctionnement efficace de son activité. finit la politique bancaire et l'orientation budgétaire.

4. Direction développement et partenariat

Responsable des études et du développement des produits finis ainsi que des actions de partenariat et de sous-traitance. Ainsi elle :

- ✓ Définit et supervise les actions de développement du produit existant et l'élargissement de la gamme en fonction du marché.
- ✓ Suit avec direction industrielle les actions de développement des processus de fabrication et de modernisation de l'outil de production, en vue de l'amélioration de la rentabilité et des conditions de travail.
- ✓ Participe à la définition de l'organisation de la production dans l'objectif de la flexibilité et de la réduction des couts de fabrication.
- ✓ Définit et concrétise des actions de sous-traitance et de partenariat.
- ✓ Développe d'autres créneaux pour l'utilisation maximale des capacités technologiques de l'entreprise.

5. Direction industrielle

Elle est chargée de développer et de mettre en place les moyens et l'organisation industrielle nécessaire à la réalisation de la production en agissant sur les approvisionnements, les moyens et les techniques de production.

- ✓ Définit les programmes de production en fonction de la demande commerciale et des capacités installées avec le souci de rentabilité optimale.
- ✓ Veille à l'optimisation et l'adaptation des approvisionnements en utilisant au mieux les capacités financières de l'entreprise pour assurer des stocks homogènes et productifs.
- ✓ Suit la réalisation des programmes de production et préconise des solutions d'adaptation en cas de difficultés.
- ✓ Améliore la gestion de la production en relation avec la structure informatique (GPAO).
- ✓ Entreprend et suscite des études de modernisation, de renouvellement, d'optimisation et d'installation des moyens de production.
- ✓ Prend en charge l'industrialisation des nouveaux produits ou modifiés dans le cadre du développement.
- ✓ Organise et anime l'industrialisation de nouveaux produits.
- ✓ Se tient informée des évolutions des techniques de fabrication des appareils électroménagers et les étudie avec l'opportunité de leur adoption.
- ✓ Veille au renforcement des dispositifs de contrôle qualité à toutes les stades de la préparation technique, de soutien et de la fabrication de produits et ce, en étroite collaboration avec les responsables qualité.
- ✓ Définit une politique d'amélioration de la maintenance des équipements de productions et en assure le suivi.

6. Direction qualité

Elle à une liaison fonctionnelle avec toutes les directions ainsi toute l'unité existe dans l'organigramme de l'entreprise, elle est représentée par six assistants :

- ✓ Assistant qualité de coordinateur.
- ✓ Assistant qualité de l'unité froide.
- ✓ Assistant qualité de l'unité cuisson.
- ✓ Assistant qualité de l'unité climatisation.
- ✓ Assistant qualité de l'unité prestation technique.
- ✓ Assistant qualité de l'unité commerciale.

Une des principales missions est de formuler, avec la direction Générale, une politique qualité spécifique qui fixe des orientations précises et qui permet le déploiement d'objectifs dans toute l'entreprise. Les acteurs internes sont ainsi mobilisés autour d'actions clés créatrices de valeur pour les clients. Cette formation vous permet d'acquérir les outils pour réussir cette compétition, déployer un plan d'actions à forte valeur ajoutée.

7. Direction planification et contrôle de gestion

Cette direction est responsable du contrôle de la gestion, de l'audit finance ainsi que du budget de l'entreprise.

Cependant elle :

- ✓ Réalise et présente tous les travaux permettant de produire une information complète et cohérente des activités de l'entreprise (production, commercialisation, approvisionnement et finance).
- ✓ Exploite et analyse les informations relatives aux agrégats de gestion afin de préconiser les actions correctives nécessaires avec toute l'anticipation attendue.
- ✓ Planifie un programme annuel d'audits finance et organise sa réalisation.
- ✓ Exploite les résultats des audits finance, les interprète et fait les recommandations nécessaires.
- ✓ Prépare, établit et suit le budget de l'entreprise.
- ✓ Contrôle et consolide les rapports d'activités.

8 .Direction juridique

La Direction Juridique conseille la Direction Générale, au sein du siège et dans les pays, et fournit des avis et recommandations sur les dossiers stratégiques. Elle propose des parcours riches et divers qui permettent à ses équipes d'enrichir leur expertise et de la développer en abordant des sujets de plus en plus techniques et complexes.

Les équipes juridiques apportent conseil et contrôle afin d'assurer la protection de l'activité et du bien du groupe conformément aux lois et réglementations en solidité. Quelque fonction de cette direction :

- ✓ inventez, rédigez et négociez tout type de contrats.
- ✓ Vous assurez la sécurité juridique des opérations au regard des règles du droit de la concurrence.
- ✓ assurez la réservation et la conservation, dans tous les pays, des noms de domaine et des adresses Internet pour les affaires dont vous avez la charge.
- ✓ intervenez pour conseiller les juristes internes et les responsables opérationnels sur les problématiques de droit de la concurrence.

9. Direction de marketing et de la communication

La direction du Marketing et de la Communication décide en collaboration avec le président directeur général, des politiques commerciales et de communication et les met en œuvre par la conception et l'élaboration des méthodes et outils de gestion nécessaires :

- ✓ Conduit les travaux d'études, d'analyse et de synthèse relative aux tendances et évolutions des marchés intérieurs et extérieurs.
- ✓ Elabore, en conformité avec la politique commerciale de l'entreprise, toute action concernant les schémas de distribution des produits finis, d'implantation d'antennes de vente au niveau national et international.
- ✓ Contribue avec les structures concernées de l'entreprise à l'élaboration des annuels et pluriannuels de production, de commercialisation et de développement.
- ✓ Participe à la politique de détermination des barèmes de prix.
- ✓ Elabore un plan de communication interne et les mettent en œuvre après approbation de la direction de l'entreprise.
- ✓ Elabore avec la direction commerciale le plan de communication externe et les mettent en œuvre après approbation de la direction de l'entreprise.
- ✓ Etablit les enquêtes clients en vue de mesurer le niveau de satisfaction de la clientèle.
- ✓ Initie et suscite des actions d'amélioration continue de la communication en relation avec l'environnement externe et médiatique de l'entreprise.
- ✓ Dirige toutes les opérations d'exportation de produits finis vers l'étranger.

I.2.2. Les unités

En plus des directions L'ENIEM est organisée sous formes d'unité.

1. Unité FILAMP (filiale)

L'unité FILAMP de Mohammedia (ULM) a démarré en février 1979 pour fabriquer des lampes d'éclairage domestique ainsi que des lampes de réfrigérateurs. Elle est devenue filiale à 100% ENIEM le 01 janvier 1997.

2. Unité commercial (UC)

Cette unité est chargée de la commercialisation des produits de l'entreprise, de la promotion des exportations et de la gestion du réseau SAV (service Après-vente).Composée essentiellement, d'une direction commerciale

Cette direction a sous sa tutelle sept départements qui collaborent pour mettre en œuvre la stratégie commerciale de l'entreprise.

- ✓ Département Vente : il se compose de trois services :
  - Service client.
  - Service vente.
  - Service synthèse et recouvrement.
- ✓ Département Distribution : Composé de deux services :
  - Service magasin produits finis.
  - Service programmation.
- ✓ Département Marketing.
- ✓ Département Service Après-vente.
- ✓ Département Finance et Comptabilité : Composé de deux services :
  - un service comptabilité générale.
  - un service finances.
- ✓ Département ARGH : Composé de deux services :
  - service gestion du personnel.
  - service moyens généraux.
- ✓ Département Contrôle de Gestion.

3. Unité Cuisson (U CUIS)

Cette unité a pour mission ; la production et le développement des produits de cuisson à gaz, électrique ou mixte et tout produit de technologie similaire, elle produit des cuisinières à gaz 04 et 05 feux. Comporte quatre (04) ateliers de fabrication :

- ✓ Atelier mécanique : s'occupe de la fabrication de composants d'alimentation en gaz et des différentes grilles de cuisinières.
- ✓ Atelier tôlerie : s'occupe de la fabrication des différentes pièces en tôle.
- ✓ Atelier d'assemblage.

Ainsi qu'un labo essais gazinières.

4. Unité climatisation (UCL)

Cette unité fait dans la production et le développement des produits de climatisation, de chauffage et annexes :

- ✓ Equipements de climatisation individuels et collectifs.
- ✓ Activités annexes : chauffe-eau, chauffe bain et radiateur à gaz butane.

Composée essentiellement de quatre (04) ateliers de fabrication :

- ✓ Atelier tôlerie.
- ✓ Atelier peinture.
- ✓ Atelier montage final.
- ✓ Atelier montage d'appareils de chauffage.

5. Unité produits sanitaires

L'unité produite sanitaires est acquise par l'entreprise ENIEM en l'an 2000. Elle n'entre pas dans le périmètre de certification de l'entreprise. La mission de l'unité est de produire ainsi développer des produits sanitaires (baignoires, lavabos et éviers…).

6. Unité froid(UF)

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 fabriquéssous 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 60.000appareils de 520L par an. Dont les modèles sous licence LEMATIC-Liban- 1993.

7. Unité de prestations techniques (UPT)

Principalement de gérer et d'exploiter les moyens communs (production d'énergie et utilités) utilisés dans le processus de production des autres unités, ainsi que de la gestion des totalités des infrastructures communes (bâtiments, voirie, éclairage…).
Cette unité assure également, les pièces mécaniques nécessaires à l'entretien des équipements de production, la conception et la fabrication de nouveaux moyens (moules, outils, gabarits…). Constituée d'ateliers de mécanique et de deux (02) stations :

- ✓ Station de production d'énergie et des fluides, elle produit de l'eau surchauffée, de la vapeur et de l'air comprimé.
- ✓ Station de neutralisation, s'occupe de traitement des rejets industriels avant leur évacuation.

Et un laboratoire de métrologie qui se charge de l'étalonnage et de la vérification des de mesure.

I.3. présentation du domaine d'Etude

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.

I.3.1.Organigramme de l'Unité de Prestation Technique :

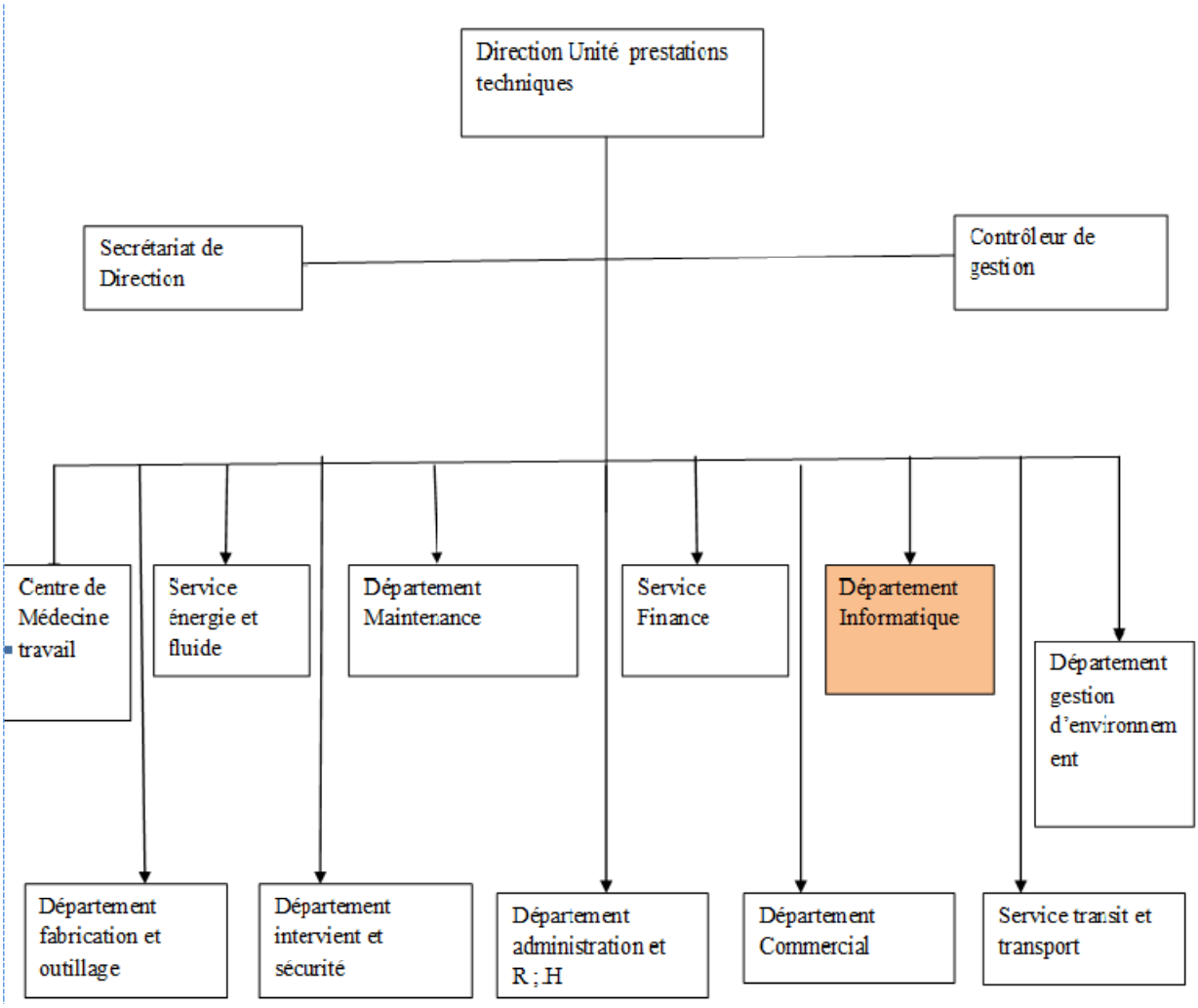


Figure I.3: Unité de Prestation Technique.

I.4. Le Réseau informatique de l'entreprise l'ENIEM

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

I.4.1.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, RuggedWriter 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).

I.4.2. Caractéristiques de ce réseau

Parmi ces caractéristiques, La topologie choisie est celle dite étoile, vu la configuration dusite, à savoir : deux bâtiments en formes de T.
Le schéma général du câblage est défini selon le nombre de bureaux et le nombred'utilisateurs par bureau.
Tous les bureaux sont dotés d'au moins une prise. Il en existe en tout 170 prises (actuellementil n'y a que 65 micro- ordinateurs connectés). Toutes les prises d'un même étage ou tous lesordinateurs d'un même étage avec ses différentes unités et fonctions sont reliées à un Switchcontenu dans une armoire, cette dernière est reliée par un câble fibre optique à un Switch ditfédérateur contenu dans l'armoire centrale installée au niveau de la salle machine au sous-soldu 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 nedoit pas dépasser 100 mètres.

I.4.3.Les armoires de brassage existantes

- ✓ **L'armoire de d'étage centrale (Fig. I.4)**

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 fibreoptique).
- 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.

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

I.4.4.Description du système du serveur HP3000/A500

✓ **La face arrière :**

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 à515 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.

✓ **La face avant:**

Elle est composée des éléments suivants :

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

I.4.5. Caractéristiques matériels et logicielles

designation	**caractéristique**
4PC hp Compaq	-system windows XP service pack 1 original -CPU Intel pentuim4 2,4G HZ -RAM DDR1 512Mo -disquedur 40Go
7PC hp Compaq	-system windows XP service pack 1 original -CPU Intel pentuim4 2,4G HZ -RAM DDR1 1Go - disquedur 80Go
1PC hp Compaq (serveur proxy)	-DDR RAM 1Go -CPU Intel pentuim4 2,4G HZ -disquedur 40Go
2PC Alfatron serveur de Domain Server dereplication	-system Windows 2003 serveur -CPU Intel core i3 -RAM DDR3 2Go -disquedur 300Go
1PC serveur de License solidworks	-system serveur 2003 -CPU Intel xeon / inside -RAM DDR3 6Go -disquedur 2To
Grand onduleur Emerson network power	Mode: libert NXe2
2stations de climatisationairwelle	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 50/60Hz 6/3A 400W

Tableau I.1 : des Caractéristiques matérielles et logicielles

I.4.5.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 clients.

I.5. Présentation du Département Informatique de l'ENIEM

I.5.1 Organigramme de département informatique

Le département informatique se compose de deux services :

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

I.5.2 Aspect humain

I.5.2.1 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.

I.5.2.2 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.

I.5.2.3 Chef de service développement système informatique

La tâche 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)**

Son 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 faciliter 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.

I.6. Conclusion

Dans ce chapitre, les ressources constituantes 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.

Introduction

Les réseaux informatiques sont parmi les outils qui ont marqués le plus d'évolution technologique de ces dernières années àtravers leur généralités et leur utilisation sur l'échèle mondial. Aujourd'hui, les réseaux sont tellement répondus qu'ils touchent tous les aspects de notre vie quotidienne : commerce, banque, travail ….

La constitution passe par une conception qui consiste à définir l'architecture des réseaux; Les outils de sécurité ;…

C'est les points sur lesquelles on va se baser durant ce chapitre.

I. Architecture réseau :

On distingue l'architecture physique et logique :

I.1 Architecture physique

La topologie physique c'est l'arrangement physique des équipements dans le réseau c.-à-d comment les équipements (que ça soit des machines ou des switchs ou des routeurs,...) sont mis et placés dans le réseau. On peut avoir une topologie en bus, en étoile, en anneau,…

I.1.1.Topologie des réseaux

- ✓ **Topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Figure II.1 : Topologie en bus.

Avantage

Facile à mettre en œuvre et de posséder un fonctionnement simple

Inconvénient

Si la ligne de transmission est défectueuse, l'ensemble du réseau en est affecté.

✓ Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Figure II.2 : Topologie en étoile.

Avantage

Beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau

Inconvénient

Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

✓ Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

Figure II.3 : Topologie en anneau

✓ Topologie maillée

Une topologie maillée correspond à plusieurs liaisons point à point. (Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités.) Chaque terminal est relié à tous les autres.

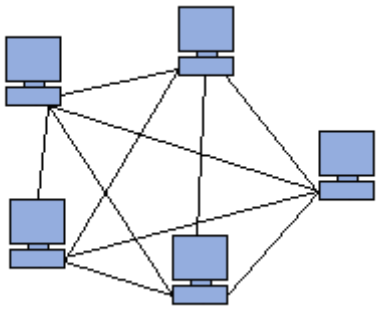


Figure II.4 : Topologie maillée

Avantage

Un seul câble, Accès égale pour tous les pc.

Inconvénient

Toute panne au niveau d'un élément ou coupure de câble bloque le réseau

Avantage

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet).

Inconvénient

Le nombre de liaisons nécessaires qui devient très élevé.

I.1.2 support physique

C'est le moyen avec lequel les déférentes topologies que je viens de citer sont reliées entre eux :

✓ Câble paire torsadée

Dans sa forme la plus simple, le câble à paire torsadée (en anglais *Twisted-pair cable*) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants.

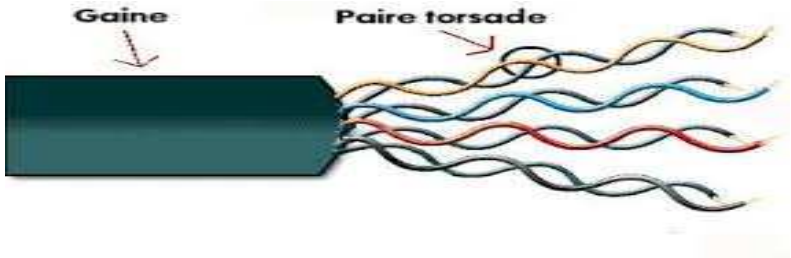


Figure II.5 : le câble à paire torsadée.

✓ Fibre optique

L'intégration de la fibre optique dans le système de câblage est liée au fait que celle-ci résout les problèmes d'environnement grâce à son immunité aux perturbations électromagnétiques ainsi qu'à l'absence d'émission radioélectrique vers l'environnement extérieur.

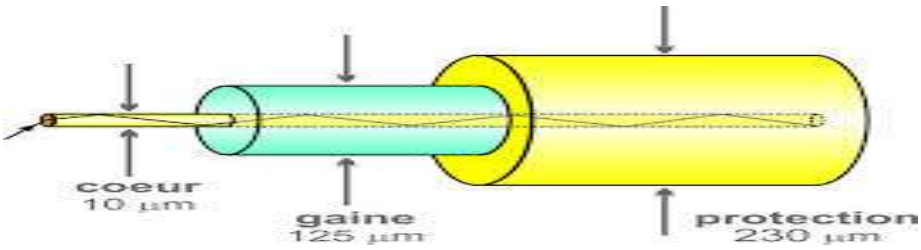


Figure II.6 : la fibre optique.

I.1.3 Equipements d'interconnexion

L'interconnexion de réseaux peut être locale: les réseaux sont sur le même site géographique ; dans ce cas, un équipement standard (répéteur, routeur etc ...) suffit à réaliser physiquement la liaison. Elle peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..).

Le choix d'un équipement d'interconnexion demeure un compromis entre les fonctions désirées et le coût.

✓ Répéteur

Un répéteur est un équipement qui permet d'étendre la portée du signal sur le support de transmission en générant un nouveau signal à partir du signal reçu.
Le but de cet élément est d'augmenter la taille du réseau.

Figure II.7 : le répéteur.

✓ Hub

Le hub est un répéteur qui transmet le signal sur plus d'un port d'entrée-sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet sur tous les autres ports.

Figure II.8: le hub.

✓ Switch

Un switch ou commutateur réseau est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication. Le commutateur établit et met à jour une table, dans le cas du commutateur pour réseau Ethernet il s'agit de

la table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port.

Figure II.9 : le Switch (commutateur).

✓ Routeur

Aussi appelé commutateur de niveau 3 car il y effectue le routage et l'adressage, il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations.

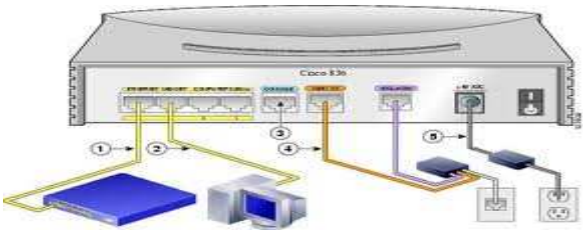


Figure II.10 : le routeur.

✓ Passerelle

La passerelle relie des réseaux hétérogènes, elle dispose des fonctions d'adaptation et de conversion de protocoles à travers plusieurs couches de communication jusqu'à la couche application.

On distingue les passerelles de transport qui mettent en relation les flux de données d'un protocole de couche transport ;

Les passerelles d'application qui quant à elles réalisent l'interconnexion entre applications de couches supérieures.

Figure II.11 : la passerelle.

- ✓ **Firewall**

Un *firewall* (ou pare-feu) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

I.1.4 Protocoles et modèles de protocoles

Un protocole est un ensemble de règles précises qui servent à coordonner les communications entre les différentes entités d'un réseau. Généralement, chaque protocole se charge d'une fonction bien déterminée et ne s'occupe que de celle-ci.

Par souci de standardisation des protocoles de communications des réseaux informatiques, l'ISO (International Standardisation Organisation) a publié le modèle OSI (Open Systems Interconnections). Ce modèle comporte sept classes de protocoles dites couches. Chacune offre un certain nombre de fonctionnalités. Il représente un modèle de référence.

Un autre modèle, plus simplifié, est apparu : c'est le modèle TCP/IP. Ce dernier régit aujourd'hui presque tous les réseaux de la planète. Il représente une simplification du modèle OSI, en regroupant quelques couches pour avoir à la fin quatre couches.

La **Table 2-1** donne une comparaison entre les deux modèles.

Modèle OSI	Protocoles	Modèle TCP/IP
Couche Application	DNS, SMTP, POP3, VOIP…	Couche Application
Couche Présentation	MIME, HTML, XML, MPEG, Vidéotex…	
Couche Session	Telnet, SSH, FTP, HTTP, HTTPS...	
Couche Transport	TCP, UDP…	Couche Transport
Couche Réseau	IPv6, IPv4, RIP, IGRP, OSPF, ICMP…	Couche Internet
Couche Liaison de données	Ethernet, Token Ring, FDDI, WIFI…	Couche Accès au réseau
Couche Physique	Médias réseaux et codage (NRZ, Miller…)	

Table II.1 : Protocoles des modèles OSI et TCP/IP.

I .2 .Architecture logique

La topologie logique désigne la manière dont laquelle les données sont transmise par le réseau.

I.2.2. Adressage IP

Toutes les couches réseau, de la couche physique à l'application en passant par les couches liaison, réseau et transport, utilisent des adresses afin d'identifier l'émetteur et le destinataire. Chaque couche utilise un système d'adressage spécifique qui répond à un besoin précis.

L'adressage de niveau 2 est géographiquement limité à un réseau local ou à une liaison point

à point d'un réseau étendu.

L'adressage de la couche 3 permet d'identifier les stations à un niveau supérieur. Il assure la continuité entre des réseaux physiques qui utilisent différents systèmes d'adressage.

I.2.3 .Plan d'adressage

Lorsque vous devez créer un réseau d'entreprise, ce réseau restreint à un site ou interconnectant différents sites de l'organisation, il est primordial de réfléchir à un plan d'adressage. Cette opération a pour but de définir pour chaque réseau physique (LAN et WAN) une adresse IP. Chaque ordinateur, chaque composant actif doit avoir un moyen d'être identifié sur le réseau. Pour cela, une adresse IP lui est attribuée. Il y a deux types d'adressage IP, « privée» qui permet la communication interentreprises et « publique » utilisée pour la communication vers, ou depuis Internet. Un organisme spécialisé fournit les adresses IP publiques. C'est donc un plan d'adressage IP privée que vous êtes sensés définir.

I.1.3. Adressage MAC

L'adresse MAC est une adresse de couche liaison de données, standardisée, qui est nécessaire pour chaque unité reliée à un réseau local. C'est une adresse qui caractérise les cartes réseau.

Une adresse MAC est composée de 6 octets, avec une structure normalisée par l'IEEE. Elle est divisée en deux parties de même longueur. Celle du poids fort identifie le constructeur de la carte réseau et celle du poids faible est attribuée, par le constructeur lui-même, de manière unique pour chaque carte réseau. Le couple assure l'unicité des adresses MAC dans le monde.

Elle est également appelée adresse matérielle, adresse de couche MAC ou adresse physique.

I.2.4. Routage

Internet et les réseaux IP sont composés d'un ensemble de réseaux reliés via des machines particulières que l'on appelle routeurs. Pour la communication au sein de ces réseaux, le protocole IP est capable de choisir un chemin (également appelé une route) suivant lequel les paquets de données seront relayés de proche en proche jusqu'au destinataire. C'est ainsi que le routage IP fonctionne de façon totalement décentralisée au

niveau des machines qui constituent le réseau. Aucune n'a une vision globale de la route que prendront les paquets de données.

I.2.5Messagerie électronique

La messagerie électronique représente l'un des services les plus importants, fourni par lesréseaux informatiques. Elle est implantée dans le réseau de l'ENSI à l'aide du serveur POSTFIX qui représente une solution alternative du serveur smtp SENDMAIL. Chaque utilisateur possède une boîte aux lettres qu'il consulte sur le serveur, après authentification bien sûr, à l'aide des protocoles POP3 et IMAP4. Pour ceci, beaucoup de logiciels peuvent être utilisés, par exemple Outlook pour Windows et Evolution pour linux. Le serveur POSTFIX peut livrer du courrier vers l'extérieur, en le configurant pour communiquer avec le serveur de messagerie du fournisseur d'accès

II. Sécurité des réseaux

II.1.Introduction

Les réseaux informatiques sont devenus un outil indispensable pour La plupart des entreprises, elles l'utilisent pour l'échange des informations avec les bureaux de leurs agences, des bureaux aux domiciles, les sites de leurs partenaires commerciaux et les télétravailleurs distants, pour bénéficier des services de commerce électronique ou des activités globales, mais le problème est de garantir que les informations qui circulent dans le réseau restent protégées.

II.2.Les menaces

La menace est l'éventualité alarmante que quelque chose se produise, et qui pourra porter atteinte à un système informatique, en d'autres termes, une menace est un événement ou action susceptible de violer la sécurité d'un système informatique.

- ✓ **Virus**

Un virus est un programme qui se reproduit en s'insérant partiellement dans d'autres fichiers, Tant que le virus n'a pas été exécuté, vous ne risquez rien. Mais, lorsqu'il est activé, il peut vous endommager votre système, supprimer des données, formater un disque dur. La majorité des virus se propagent par courrier électronique en pièce-jointe.

- ✓ **Vers**

Un ver (en anglais Worm) est un programme qui se propage d'ordinateur à ordinateur via un réseau comme l'Internet. Ainsi, contrairement à un virus, le vers n'a pas besoin d'un programme hôte pour assurer sa reproduction. Son poids est très léger, ce qui lui permet de se propager à une vitesse impressionnante sur un réseau, et pouvant donc saturer ce dernier.

- ✓ **Spywares**

Aussi appelé mouchard ou espiogiciel ; en anglais spyware est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

- ✓ **Hijackers :**

Un Hijacker, ou pirate de navigateur, utilise les failles de sécurité d'internet explorer pour s'installer sur votre ordinateur. Ce genre de programme s'installe donc juste en surfant sur le net, souvent sur des sites "louches" (sites de piratage, de patch noc pour jeux, ...).

- ✓ **Troyen :**

Un troyen (en anglais trojan horse) tire son nom du mythe du cheval de Troie. Ce programme a une apparence saine, souvent même attirante, mais lorsqu'il est exécuté, il effectue, discrètement ou pas, des actions supplémentaires. Ces actions peuvent être de toute forme, comme l'installation d'une backdoor par exemple.

- ✓ **Backdoor**

Une backdoor (en français, une porte dérobée) est un moyen laissé par une personne malveillante pour revenir dans un système. Par exemple, un pirate, après avoir pénétré une machine peut se créer un compte secret. Ainsi, il pourra revenir la prochaine fois facilement.

- ✓ **Spam**

Le spamming (ou encore pourriel, courrier rebut) consiste à envoyer des messages appelés "spam" à une ou plusieurs personnes. Ces spams sont souvent d'ordre publicitaire. Tous les points suivant sont considérés comme du spamming.

- Envoyer un même mail, une ou plusieurs fois à une ou plusieurs personnes en faisant de la publicité.
- Poster un ou plusieurs messages dans un forum qui n'a rien à voir avec le thème.
- Faire apparaître un message publicitaire lorsque l'on navigue sur un site.

✓ **Mailbombing**

Le mailbombing s'apparente un peu au spamming puisqu'il a pour but de provoquer une gêne pour la victime. Mais cette fois, le but n'est pas le même, il s'agit de saturer la boîte aux lettres électronique de la victime en envoyant plusieurs mails, des milliers par exemple.

II.3.Les techniques d'attaques

✓ **Déni de service**

Une attaque par déni de service (en anglais Denial of Service, DoS) est une attaque qui a pour but de mettre hors-jeu le système qui est visée. Ainsi, la victime se voit dans l'incapacité d'accéder à son réseau. Ce type d'attaque peut aussi bien être utilisé contre un serveur d'entreprise qu'un particulier relié à internet. Tous les systèmes d'exploitation sont également touchés : Windows, Linux, Unix.

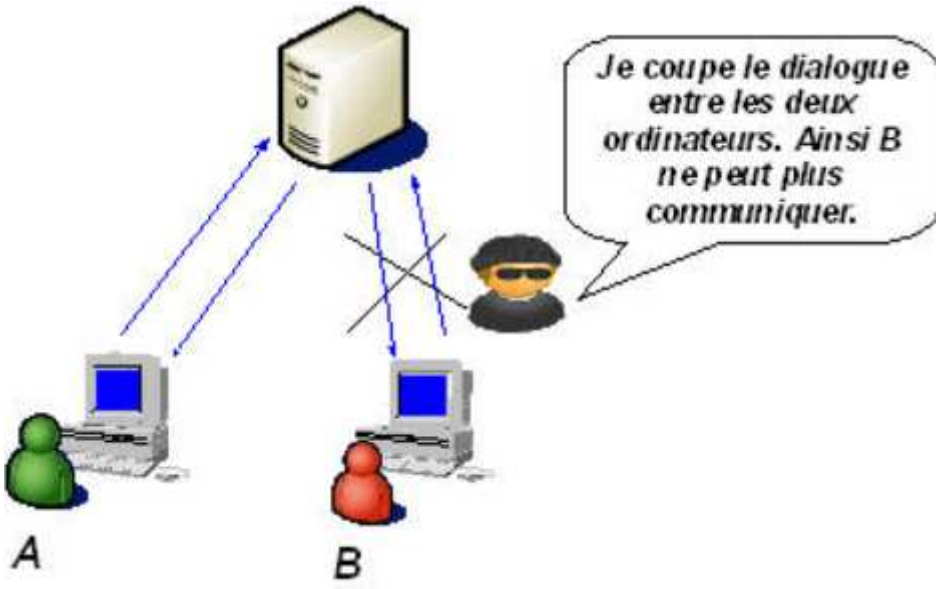


Figure II.12: Dénis de service.

- ✓ **Sniffing**

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles. Exemple : Soit une entreprise possédant 100 ordinateurs reliés entre eux grâce à un hub. Maintenant, si un pirate écoute le trafic réseau entre 8h et 10h (heure de connexion du personnel), il pourra lire tous les noms d'utilisateurs ainsi que leur mot de passe.

Figure II .13: le sniffing

- ✓ **Scanning**

Le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanné. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C'est un outil très utile pour les hackers. Cela leur permet de connaitre les points faibles d'une machine et ainsi de savoir par où ils peuvent attaquer. D'autant plus que les scanners ont évolué. Aujourd'hui, ils peuvent déterminer le système d'exploitation et les applications associées aux ports.

Figure II.14: Scanning.

- ✓ **Social engineering**

Le social engineering est l'art de manipuler les personnes. Il s'agit ainsi d'une technique permettant d'obtenir des informations d'une personne, qu'elle ne devrait pas donner en temps normal, en lui donnant des bonnes raisons de le faire. Cette technique peut se faire par téléphone, par courrier électronique, par lettre écrite, ... Cette attaque est souvent sous-estimée puisqu'elle n'est pas d'ordre informatique. Pourtant, une attaque par social engineering bien menée peut se révéler très efficace. Elle n'est donc pas à prendre à la légère.

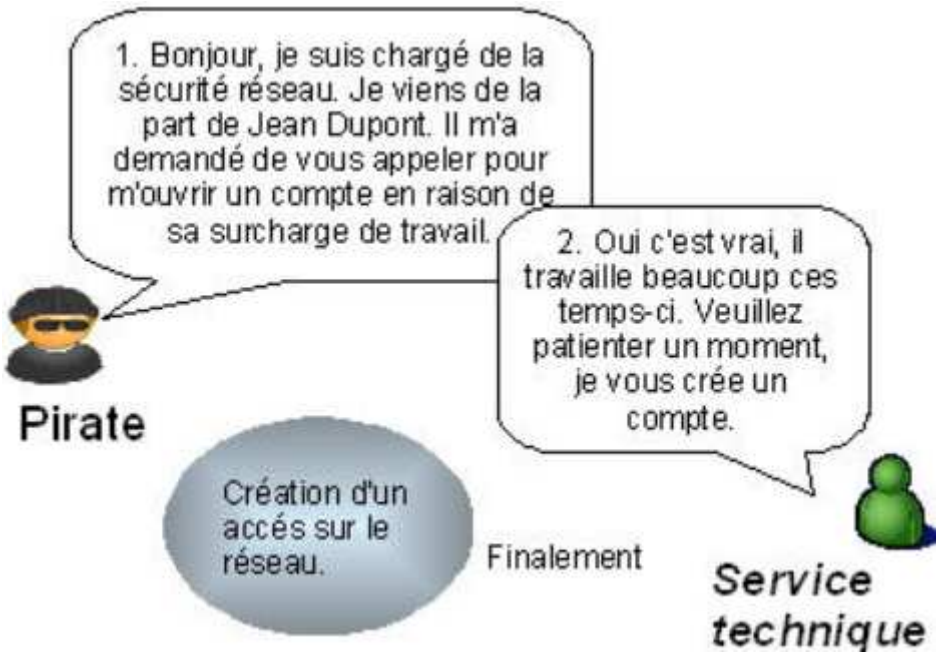


Figure II.15 : Le social engineering

- ✓ **Cracking**

Le crackage des mots de passe consiste à deviner le mot de passe de la victime. Malheureusement, beaucoup d'utilisateurs mal avertis de cette technique mettent des mots de passe évidents comme leur propre prénom ou ceux de leurs enfants. Ainsi, si un pirate, qui a espionné sa victime auparavant, teste quelques mots de passe comme le prénom des enfants de la victime, il aura accès à l'ordinateur. D'où l'utilité de mettre des bons mots de passe. Mais même les mots de passe les plus robustes peuvent être trouvés à l'aide de logiciels spécifiques appeléscraqueur.

Ces logiciels peuvent tester des mots de passe selon trois méthodes :

- ➢ **Attaque par dictionnaire**

Le logiciel teste tous les mots de passe stockés dans un fichier texte. Cette méthode est redoutable car en plus de sa rapidité, elle aboutit généralement puisque les mots de passe des utilisateurs sont souvent des mots existants.

- ➢ **Attaque hybride**

Le logiciel teste tous les mots de passe stockés dans un fichier texte et y ajoute des combinaisons. Par exemple, thomas01. Cette méthode est redoutable également puisque beaucoup de personnes mettent des chiffres après leur mot de passe pensant bien faire.

- ➢ **Attaque brute-force**

Le logiciel teste toutes les combinaisons possibles. Ainsi ce genre d'attaque aboutit à chaque fois. Heureusement, tester toutes les combinaisons prends beaucoup de temps. D'où l'utilité de changer de mots de passe régulièrement.

- ✓ **Spoofing**

L'usurpation (en anglais spoofing) consiste à se faire passer pour quelqu'un d'autre. Il y a beaucoup d'utilité pour un pirate d'usurper une identité. Voici quelques exemples d'usurpations, mais ce ne sont pas les seules :

- **Usurpation de l'adresse IP**

Une adresse IP correspond en gros à l'adresse postale d'un ordinateur. Ainsi, en changeant d'adresse IP, on peut se faire passer pour un autre ordinateur et obtenir des informations sensibles qui ne nous sont pas destinées.

- **Usurpation de l'adresse e-mail**

Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur. Mais, il est possible de changer l'adresse. Ainsi, un pirate peut vous envoyer un mail en usurpant l'adresse de votre supérieur.

✓ **Man in the Middle**

Man in the Middle signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu.

Figure II .16: man in the middle

✓ **Hijacking**

Un pirate peut craquer (cible) le mot de passe de la session. Mais si vous choisissez un mot de passe robuste, cela lui prendra beaucoup de temps. Alors pourquoi ne pas

attendre que la victime se connecte sur la session et prendre sa place ? Ainsi, le pirate contourne le processus d'authentification. Et justement, il le fait, c'est le principe du détournement de session (en anglais hijacking). Ensuite, s'il veut pouvoir dialoguer avec le serveur, il doit mettre hors-jeu la victime. Pour cela, il peut lui lancer une attaque par déni de service (cible). Mais, il peut aussi se mettre en écoute et enregistrer tout le trafic en espérant recueillir des informations sensibles comme des mots de passe.

Figure II .17 : Hijaching

- ✓ **Buffer OverFlow**

Un débordement de tampon (en anglais Buffer OverFlow ou BoF) est une attaque très utilisée des pirates. Cela consiste à utiliser un programme résidant sur votre machine en lui envoyant plus de données qu'il n'est censé en recevoir afin que ce dernier exécute un code arbitraire. Il n'est pas rare qu'un programme accepte des données en paramètre. Ainsi, si le programme ne vérifie pas la longueur de la chaîne passée en paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande.

II.4.But d'attaques

- ✓ **Interruption :** Vise la disponibilité des informations.

Figure II.18: Interruption des données.

- ✓ **Interception**: Vise la confidentialité des informations.

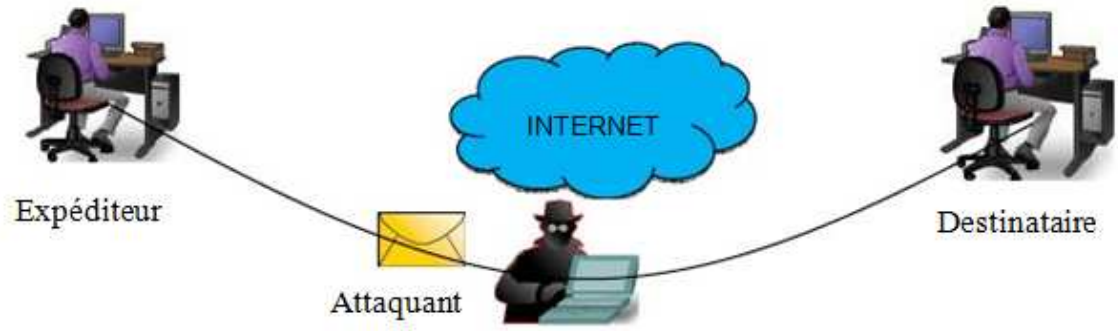


Figure II.19: Interception des données

- ✓ **Modification** : vise l'intégrité des informations.

Figure II.20: Modification des données

- ✓ **Fabrication** : Vise l'authenticité de la source ou de la destination des informations.

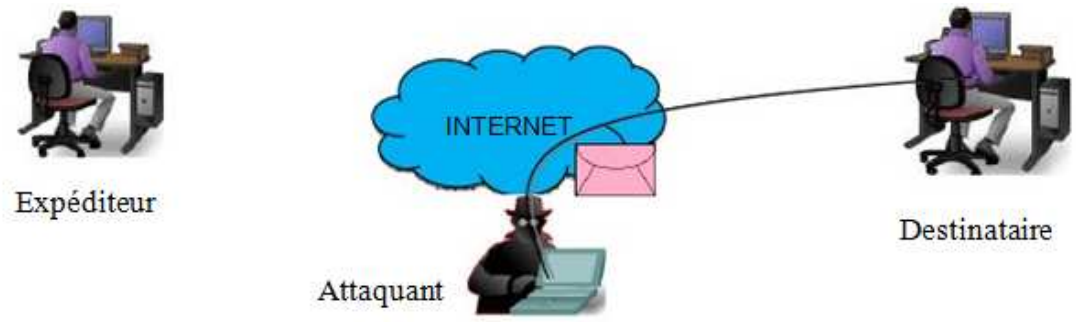


Figure II.21 : Fabrication des données.

II.5.Moyennes et technique de sécurité

La tâche la plus difficile quand on traite la sécurité ou bien quand on définit la politique de sécurité que l'entreprise doit suivre, est probablement la phase de planification dans laquelle on développe une solution pour répondre aux besoins en sécurité et les objectifs de notre entreprise. En examinant le réseau et en identifiant les zones et les composants critiques et à risque, on devrait prendre une approche, pour créer un plan de sécurité, avec diverse objectifs en perspectives :

- ❖ Une politique de sécurité cohérente et simple devrait être créée, basée sur la stratégie et les objectifs de l'entreprise (c.à.d. aider l'entreprise à atteindre ces objectifs, et non l'entraver par des procédures trop rigides qui vont gêner les utilisateurs dans leur travail et diminuer le rendement).
- ❖ La politique de sécurité devra décider du choix des solutions et des produits de sécurité, mais pas l'inverse.
- ❖ La gestion de sécurité devrait être centralisée sous une seule plateforme, de préférence d'un même constructeur afin de faciliter le déploiement, le contrôle et le support de la solution.

En général, une bonne politique de sécurité devrait aborder les questions suivantes:

✓ Authentification

La première étape afin de protéger les ressources d'un réseau est de pouvoir vérifier l'identité des utilisateurs. Cette vérification s'appelle 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.

✓ Cryptographie

Les récents développement de la cryptographie permettent de résoudre les nombreux problèmes menaçants la vie privé ou la sécurité sur internet, la cryptographie est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information telle la confidentialité, l'intégralité des données, authentification d'entités, et l'authentification de l'originalité des données.

✓ Logiciels antivirus

La plupart des ordinateurs sont dotés d'un logiciel antivirus capable de détecter les menaces virales s'il est régulièrement mis à jour et correctement entretenu.

✓ Pare-Feu

C'est un routeur ou serveur d'accès désigné comme tampon entre les réseaux publics connectés et un réseau privé, ou bien entre Internet et le réseau interne d'une entreprise. En pratique, le pare-feu consistera en une architecture, plutôt qu'un matériel ou un logiciel précis.

Cette architecture intégrera alors une série de composants matériels et logiciels qui eux tenteront précisément d'assurer le niveau de sécurité requis.

✓ Filtres de Paquets

Le principe fondamental d'un filtre de paquets est comme son nom l'indique, permet de filtrer les paquets circulant sur un réseau. Plus précisément, on peut même dire que le filtrage s'effectue sur les paquets traversant une interface réseau.

✓ Les Proxys

Les proxys sont des serveurs fonctionnent au niveau des protocoles de la couche application du modèle TCP/IP. Ceux-ci servent d'intermédiaire, entre un client du réseau interne, et des serveurs situés à l'extérieur du réseau de l'entreprise.

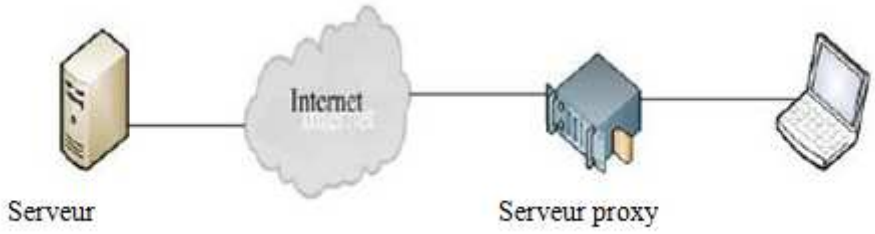


Figure II.23: Emplacement de serveur proxy.

✓ Système de détection d'intrusions

Un système de détection d'intrusions fournit une surveillance constante du réseau. Ce système analyse les flux de paquets de données du réseau à la recherche d'activités non autorisées, telles que les attaques de pirates, et permet aux utilisateurs de répondre aux failles dans la sécurité avant que les systèmes ne soient compromis.

✓ VPN

Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une abstraction permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local. Toute la partie de routage pour atteindre le ou les autres ordinateurs est gérée de façon transparente par le logiciel de VPN, créant un tunnel.

II.6 Caractéristiques d'un réseau fiable

Un réseau solide est un réseau qui offre :

✓ **Disponibilité** : autrement dit la capacité à être prêts à fournir un service

(La probabilité qu'un service soit en bon état de fonctionnement à un instant donné). Si le réseau venait à être inaccessible, la communication et la collaboration s'arrêteront, ainsi la productivité de des utilisateurs se verrait réduite. La disponibilité touche les aspects tels que :

- **Les liaisons avec le réseaupublic**

  Chaque contrat avec un opérateur doit garantir par exemple un certain délai de rétablissement du lien en cas de dysfonctionnement. Ce même principe doit être définit en interne.

- **Les équipements matériels d'interconnexion**

  Il est important de conclure des contrats de maintenance avec des entreprises sous-traitantes pour le dépannage des équipements en cas de panne, et d'obtenir une garantie lors de l'achat du matériel. Une sous-estimation de ces aspects peut engendrer de graves conséquences sur la productivité d'une entreprise.

- ✓ **Tolérance aux pannes**

La tolérance aux pannes (on dit également « insensibilité aux pannes ») désigne une méthode de conception permettant à un système de continuer à fonctionner, éventuellement de manière réduite au lieu de tomber complètement en panne, lorsque l'un de ses composants ne fonctionne plus correctement.

Tout dispositif technique permettant de palier à ces différentes pannes sans interrompre la bonne marche du système peut être considérée comme tolérant les pannes.

- ✓ **Sécurité**

Les problèmes liés à la sécurité, souvent très onéreux, peuvent être l'indisponibilité des serveurs, du réseau, les vols d'information, des attaques qui viennent parfois du réseau local. Les outils pour y remédier sont tellement disparates (un peu à tous les niveaux) et ne colmatent qu'une partie des failles du fait des nouvelles sorties. De plus le protocole réseau IP qui n'assure aucune fiabilité ne rend pas cette tâche facile. Vue l'importance de la sécurité, il s'avère utile de coupler plusieurs outils et mécanismes pour au moins s'assurer une meilleure protection.

- ✓ **Qualité de service**

Qui dit qualité de service dit la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de débit, latence (délai de transmission), taux de perte de paquets, gigue (variation de la latence). Ce problème ne se pose pas quand la bande passante est à profusion, c'est le cas généralement des LAN. Par contre le besoin d'assurer une qualité de service s'impose quand la bande passante est limitée et chère, c'est le cas dans les WAN, la difficulté augmente avec la présence d'un ou de plusieurs opérateurs.

Conclusion

La politique de sécurité permet de transcrire le travail de modélisation effectué pour comprendre les risques et leurs impacts, en des mesures concrètes de sécurité. Sa spécification est un des garants du bon dimensionnement des mesures de sécurité et d'une gestion efficace. Elle donne de la cohérence à la gestion et permet d'adopter vis à vis des risques et menaces, une attitude préventive et proactive et pas seulement réactive. Elle permet de lier la stratégie de sécurité de l'entreprise à sa réalisation opérationnelle.

La bonne réalisation d'une politique de sécurité permet au mieux, de maîtriser les risques informatiques, tout en réduisant leur probabilité d'apparition.

Dans le chapitre suivant, je vais détailler une technique de sécurité réseau eu utilisant les différentes aspects sécurités Informatique (FIREWALL, ANTIVIRUS, ARECHETICTURE, ACL, VLAN ……)

Chapitre II

Généralités sur les réseaux informatiques

Introduction

Les réseaux informatiques sont parmi les outils qui ont marqués le plus d'évolution technologique de ces dernières années àtravers leur généralités et leur utilisation sur l'échèle mondial. Aujourd'hui, les réseaux sont tellement répondus qu'ils touchent tous les aspects de notre vie quotidienne : commerce, banque, travail ….

La constitution passe par une conception qui consiste à définir l'architecture des réseaux;Les outils de sécurité ;…

C'est les points sur lesquelles on va se baser durant ce chapitre.

I. Architecture réseau :On distingue l'architecture physique et logique :

I.1 Architecture physique

La topologie physique c'est l'arrangement physique des équipements dans le réseau c.-à-d comment les équipements (que ça soit des machines ou des switchs ou des routeurs,...) sont mis et placés dans le réseau. On peut avoir une topologie en bus, en étoile, en anneau,…

I.1.1.Topologie des réseaux

- ✓ **Topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

Figure II.1 : Topologie en bus.

Avantage

Facile à mettre en œuvre et de posséder un fonctionnement simple

Inconvénient

Si la ligne de transmission est défectueuse, l'ensemble du réseau en est affecté.

✓ Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Figure II.2 : Topologie en étoile.

Avantage

Beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau

Inconvénient

Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

✓ Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

Figure II.3 : Topologie en anneau

Avantage

Un seul câble, Accès égale pour tous les pc.

Inconvénient

Toute panne au niveau d'un élément ou coupure de câble bloque le réseau

✓ Topologie maillée

Une topologie maillée correspond à plusieurs liaisons point à point. (Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités.) Chaque terminal est relié à tous les autres.

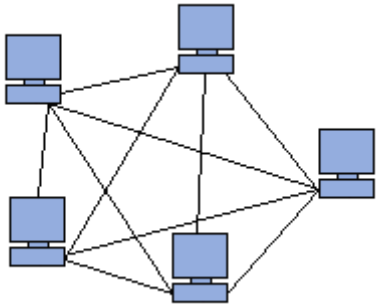


Figure II.4 : Topologie maillée

Avantage

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet).

Inconvénient

Le nombre de liaisons nécessaires qui devient très élevé.

I.1.2 support physique

C'est le moyen avec lequel les déférentes topologies que je viens de citer sont reliéesentre eux :

- ✓ **Câble paire torsadée**

Dans sa forme la plus simple, le câble à paire torsadée (en anglais *Twisted-pair cable*) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants.

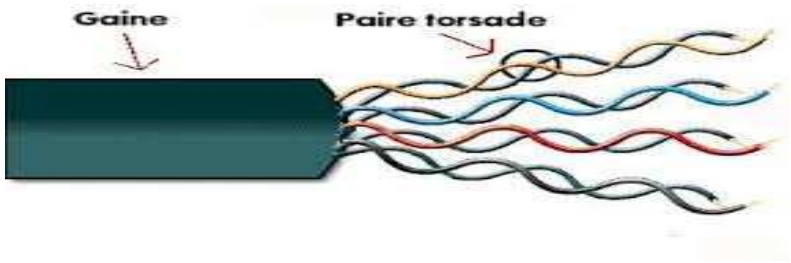


Figure II.5 : le câble à paire torsadée.

- ✓ **Fibre optique**

L'intégration de la fibre optique dans le système de câblage est liée au fait que celle-ci résout les problèmes d'environnement grâce à son immunité aux perturbations électromagnétiques ainsi qu'à l'absence d'émission radioélectrique vers l'environnement extérieur.

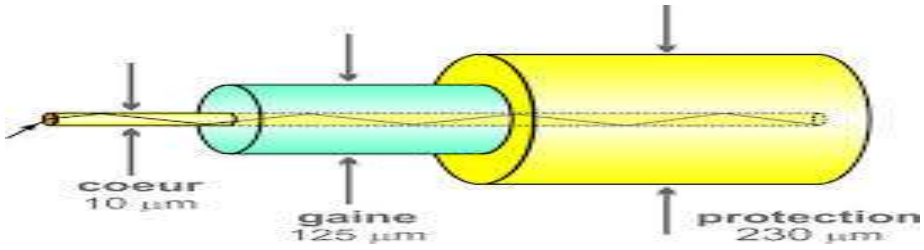


Figure II.6 : la fibre optique.

I.1.3 Equipements d'interconnexion

L'interconnexion de réseaux peut être locale: les réseaux sont sur le même site géographique ; dans ce cas, un équipement standard (répéteur, routeur etc ...) suffit à réaliser physiquement la liaison. Elle peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..).

Le choix d'un équipement d'interconnexion demeure un compromis entre les fonctions désirées et le coût.

✓ Répéteur

Un répéteur est un équipement qui permet d'étendre la portée du signal sur le support de transmission en générant un nouveau signal à partir du signal reçu.
Le but de cet élément est d'augmenter la taille du réseau.

Figure II.7 : le répéteur.

✓ Hub

Le hub est un répéteur qui transmet le signal sur plus d'un port d'entrée-sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet sur tous les autres ports.

Figure II.8: le hub.

✓ Switch

Un switch ou commutateur réseau est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication. Le commutateur établit et met à jour une table, dans le cas du commutateur pour réseau Ethernet il s'agit de

la table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port.

Figure II.9 : le Switch (commutateur).

✓ Routeur

Aussi appelé commutateur de niveau 3 car il y effectue le routage et l'adressage, il permet d'interconnecter deux ou plusieurs réseaux. Possédant les mêmes composants de base qu'un ordinateur, le routeur sélectionne le chemin approprié (au travers de la table de routage) pour diriger les messages vers leurs destinations.

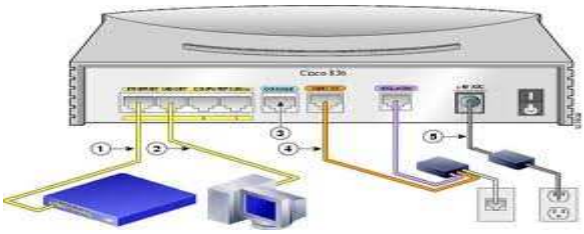


Figure II.10 : le routeur.

✓ Passerelle

La passerelle relie des réseaux hétérogènes, elle dispose des fonctions d'adaptation et de conversion de protocoles à travers plusieurs couches de communication jusqu'à la couche application.

On distingue les passerelles de transport qui mettent en relation les flux de données d'un protocole de couche transport ;

Les passerelles d'application qui quant à elles réalisent l'interconnexion entre applications de couches supérieures.

Figure II.11 : la passerelle.

- ✓ **Firewall**

Un *firewall* (ou pare-feu) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

I.1.4 Protocoles et modèles de protocoles

Un protocole est un ensemble de règles précises qui servent à coordonner les communications entre les différentes entités d'un réseau. Généralement, chaque protocole se charge d'une fonction bien déterminée et ne s'occupe que de celle-ci.

Par souci de standardisation des protocoles de communications des réseaux informatiques, l'ISO (International Standardisation Organisation) a publié le modèle OSI (Open Systems Interconnections). Ce modèle comporte sept classes de protocoles dites couches. Chacune offre un certain nombre de fonctionnalités. Il représente un modèle de référence.

Un autre modèle, plus simplifié, est apparu : c'est le modèle TCP/IP. Ce dernier régit aujourd'hui presque tous les réseaux de la planète. Il représente une simplification du modèle OSI, en regroupant quelques couches pour avoir à la fin quatre couches.

La **Table 2-1** donne une comparaison entre les deux modèles.

Modèle OSI	Protocoles	Modèle TCP/IP
Couche Application	DNS, SMTP, POP3, VOIP…	Couche Application
Couche Présentation	MIME, HTML, XML, MPEG, Vidéotex…	
Couche Session	Telnet, SSH, FTP, HTTP, HTTPS...	
Couche Transport	TCP, UDP…	Couche Transport
Couche Réseau	IPv6, IPv4, RIP, IGRP, OSPF, ICMP…	Couche Internet
Couche Liaison de données	Ethernet, Token Ring, FDDI, WIFI…	Couche Accès au réseau
Couche Physique	Médias réseaux et codage (NRZ, Miller…)	

Table II.1 : Protocoles des modèles OSI et TCP/IP.

I .2 .Architecture logique

La topologie logique désigne la manière dont laquelle les données sont transmise par le réseau.

I.2.2. Adressage IP

Toutes les couches réseau, de la couche physique à l'application en passant par les couches liaison, réseau et transport, utilisent des adresses afin d'identifier l'émetteur et le destinataire. Chaque couche utilise un système d'adressage spécifique qui répond à un besoin précis.

L'adressage de niveau 2 est géographiquement limité à un réseau local ou à une liaison point à point d'un réseau étendu.

L'adressage de la couche 3 permet d'identifier les stations à un niveau supérieur. Il assure la continuité entre des réseaux physiques qui utilisent différents systèmes d'adressage.

I.2.3 .Plan d'adressage

Lorsque vous devez créer un réseau d'entreprise, ce réseau restreint à un site ou interconnectant différents sites de l'organisation, il est primordial de réfléchir à un plan d'adressage. Cette opération a pour but de définir pour chaque réseau physique (LAN et WAN) une adresse IP. Chaque ordinateur, chaque composant actif doit avoir un moyen d'être identifié sur le réseau. Pour cela, une adresse IP lui est attribuée. Il y a deux types d'adressage IP, « privée» qui permet la communication interentreprises et « publique » utilisée pour la communication vers, ou depuis Internet. Un organisme spécialisé fournit les adresses IP publiques. C'est donc un plan d'adressage IP privée que vous êtes sensés définir.

I.1.3. Adressage MAC

L'adresse MAC est une adresse de couche liaison de données, standardisée, qui est nécessairepour chaque unité reliée à un réseau local. C'est une adresse qui caractérise les cartes réseau.

Une adresse MAC est composée de 6 octets, avec une structure normalisée par l'IEEE. Elle est divisée en deux parties de même longueur. Celle du poids fort identifie le constructeur dela carte réseau et celle du poids faible est attribuée, par le constructeur lui-même, de manièreunique pour chaque carte réseau. Le couple assure l'unicité des adresses MAC dans le monde.

Elle est également appelée adresse matérielle, adresse de couche MAC ou adresse physique.

I.2.4. Routage

Internet et les réseaux IP sont composés d'un ensemble de réseaux reliés via des machines particulières que l'on appelle routeurs. Pour la communication au sein de ces réseaux, le protocole IP est capable de choisir un chemin (également appelé une route) suivant lequel les paquets de données seront relayés de proche en proche jusqu'au destinataire. C'est ainsi que le routage IP fonctionne de façon totalement décentralisée au niveau des machines qui constituent le réseau. Aucune n'a une vision globale de la route que prendront les paquets de données.

I.2.5Messagerie électronique

La messagerie électronique représente l'un des services les plus importants, fourni par lesréseaux informatiques. Elle est implantée dans le réseau de l'ENIEM à l'aide du serveur POSTFIX qui représente une solution alternative du serveur smtp SENDMAIL. Chaque utilisateur possède une boîte aux lettres qu'il consulte sur le serveur, après authentification bien sûr, à l'aide des protocoles POP3 et IMAP4. Pour ceci, beaucoup de logiciels peuvent être utilisés, par exemple Outlook pour Windows et Evolution pour linux. Le serveur POSTFIX peut livrer du courrier vers l'extérieur, en le configurant pour communiquer avec le serveur de messagerie du fournisseur d'accès

II. Sécurité des réseaux

II.1.Introduction

Les réseaux informatiques sont devenus un outil indispensable pour La plupart des entreprises, elles l'utilisent pour l'échange des informations avec les bureaux de leurs agences, des bureaux aux domiciles, les sites de leurs partenaires commerciaux et les télétravailleurs distants, pour bénéficier des services de commerce électronique ou des activités globales, mais le problème est de garantir que les informations qui circulent dans le réseau restent protégées.

II.2.Les menaces

La menace est l'éventualité alarmante que quelque chose se produise, et qui pourra porter atteinte à un système informatique, en d'autres termes, une menace est un événement ou action susceptible de violer la sécurité d'un système informatique.

- ✓ **Virus**

Un virus est un programme qui se reproduit en s'insérant partiellement dans d'autres fichiers,Tant que le virus n'a pas été exécuté, vous ne risquez rien. Mais, lorsqu'il est activé, il peut vous endommager votre système, supprimer des données, formater un disque dur. La majorité des virus se propagent par courrier électronique en pièce-jointe.

- ✓ **Vers**

Un ver (en anglais Worm) est un programme qui se propage d'ordinateur à ordinateur via un réseau comme l'Internet. Ainsi, contrairement à un virus, le vers n'a pas besoin d'un programme hôte pour assurer sa reproduction. Son poids est très léger, ce qui

lui permet de se propager à une vitesse impressionnante sur un réseau, et pouvant donc saturer ce dernier.

- ✓ **Spywares**

Aussi appelé mouchard ou espiogiciel ; en anglais spyware est un logiciel malveillant qui s'installe dans un ordinateur dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données.

- ✓ **Hijackers :**

Un Hijacker, ou pirate de navigateur, utilise les failles de sécurité d'internet explorer pour s'installer sur votre ordinateur. Ce genre de programme s'installe donc juste en surfant sur le net, souvent sur des sites "louches" (sites de piratage, de patch noc pour jeux, ...).

- ✓ **Troyen :**

Un troyen (en anglais trojan horse) tire son nom du mythe du cheval de Troie. Ce programme a une apparence saine, souvent même attirante, mais lorsqu'il est exécuté, il effectue, discrètement ou pas, des actions supplémentaires. Ces actions peuvent être de toute forme, comme l'installation d'une backdoor par exemple.

- ✓ **Backdoor**

Une backdoor (en français, une porte dérobée) est un moyen laissé par une personne malveillante pour revenir dans un système. Par exemple, un pirate, après avoir pénétré une machine peut se créer un compte secret. Ainsi, il pourra revenir la prochaine fois facilement.

- ✓ **Spam**

Le spamming (ou encore pourriel, courrier rebut) consiste à envoyer des messages appelés "spam" à une ou plusieurs personnes. Ces spams sont souvent d'ordre publicitaire. Tous les points suivant sont considérés comme du spamming.

- Envoyer un même mail, une ou plusieurs fois à une ou plusieurs personnes en faisant de la publicité.
- Poster un ou plusieurs messages dans un forum qui n'a rien à voir avec le thème.
- Faire apparaître un message publicitaire lorsque l'on navigue sur un site.

✓ **Mailbombing**

Le mailbombing s'apparente un peu au spamming puisqu'il a pour but de provoquer une gêne pour la victime. Mais cette fois, le but n'est pas le même, il s'agit de saturer la boîte aux lettres électronique de la victime en envoyant plusieurs mails, des milliers par exemple.

II.3.Les techniques d'attaques

✓ **Déni de service**

Une attaque par déni de service (en anglais Denial of Service, DoS) est une attaque qui a pour but de mettre hors-jeu le système qui est visée. Ainsi, la victime se voit dans l'incapacité d'accéder à son réseau. Ce type d'attaque peut aussi bien être utilisé contre un serveur d'entreprise qu'un particulier relié à internet. Tous les systèmes d'exploitation sont également touchés : Windows, Linux, Unix.

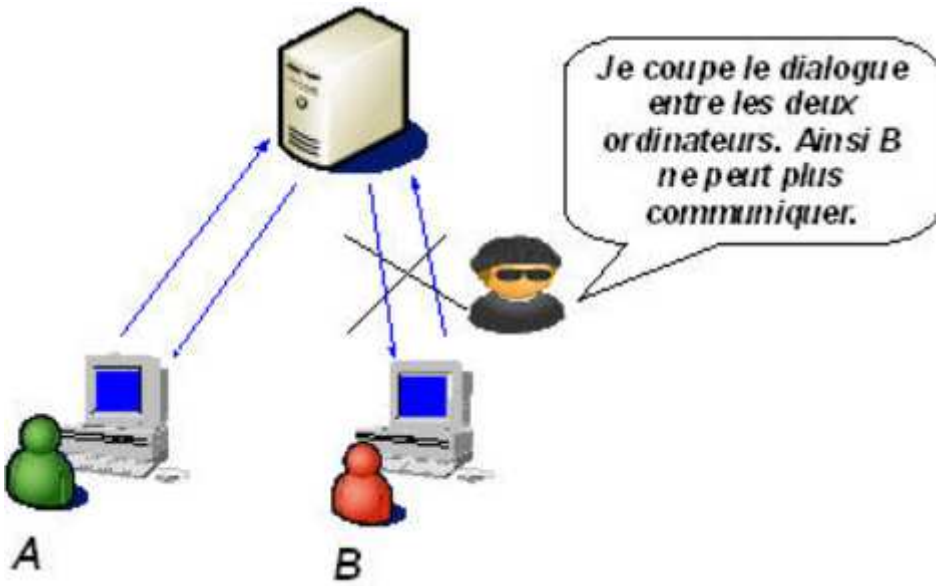


Figure II.12: Dénis de service.

- ✓ **Sniffing**

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles. Exemple : Soit une entreprise possédant 100 ordinateurs reliés entre eux grâce à un hub. Maintenant, si un pirate écoute le trafic réseau entre 8h et 10h (heure de connexion du personnel), il pourra lire tous les noms d'utilisateurs ainsi que leur mot de passe.

Figure II .13:le sniffing

- ✓ **Scanning**

Le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanné. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C'est un outil très utile pour les hackers. Cela leur permet de connaitre les points faibles d'une machine et ainsi de savoir par où ils peuvent attaquer. D'autant plus que les scanners ont évolué. Aujourd'hui, ils peuvent déterminer le système d'exploitation et les applications associées aux ports.

Figure II.14: Scanning.

- ✓ **Social engineering**

Le social engineering est l'art de manipuler les personnes. Il s'agit ainsi d'une technique permettant d'obtenir des informations d'une personne, qu'elle ne devrait pas donner en temps normal, en lui donnant des bonnes raisons de le faire. Cette technique peut se faire par téléphone, par courrier électronique, par lettre écrite, ... Cette attaque est souvent sous-estimée puisqu'elle n'est pas d'ordre informatique. Pourtant, une attaque par social engineering bien menée peut se révéler très efficace. Elle n'est donc pas à prendre à la légère.

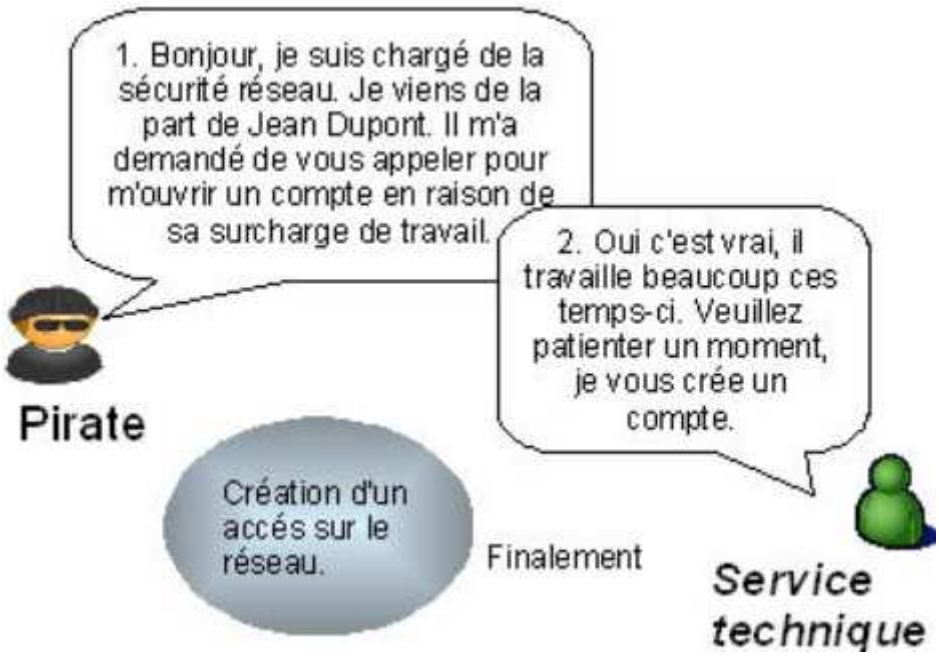


Figure II.15 : Le social engineering

- ✓ **Cracking**

Le crackage des mots de passe consiste à deviner le mot de passe de la victime. Malheureusement, beaucoup d'utilisateurs mal avertis de cette technique mettent des mots de passe évidents comme leur propre prénom ou ceux de leurs enfants. Ainsi, si un pirate, qui a espionné sa victime auparavant, teste quelques mots de passe comme le prénom des enfants de la victime, il aura accès à l'ordinateur. D'où l'utilité de mettre des bons mots de passe. Mais même les mots de passe les plus robustes peuvent être trouvés à l'aide de logicielsspécifiques appeléscraqueur.

Ces logiciels peuvent tester des mots de passe selon trois méthodes :

- ➢ **Attaque par dictionnaire**

Le logiciel teste tous les mots de passe stockés dans un fichier texte. Cette méthode est redoutable car en plus de sa rapidité, elle aboutit généralement puisque les mots de passe des utilisateurs sont souvent des mots existants.

- ➢ **Attaque hybride**

Le logiciel teste tous les mots de passe stockés dans un fichier texte et y ajoute des combinaisons. Par exemple, thomas01. Cette méthode est redoutable également puisque beaucoup de personnes mettent des chiffres après leur mot de passe pensant bien faire.

- ➢ **Attaque brute-force**

Le logiciel teste toutes les combinaisons possibles. Ainsi ce genre d'attaque aboutit à chaque fois. Heureusement, tester toutes les combinaisons prends beaucoup de temps. D'où l'utilité de changer de mots de passe régulièrement.

- ✓ **Spoofing**

L'usurpation (en anglais spoofing) consiste à se faire passer pour quelqu'un d'autre. Il y a beaucoup d'utilité pour un pirate d'usurper une identité. Voici quelques exemples d'usurpations, mais ce ne sont pas les seules :

- **Usurpation de l'adresse IP**

Une adresse IP correspond en gros à l'adresse postale d'un ordinateur. Ainsi, en changeant d'adresse IP, on peut se faire passer pour un autre ordinateur et obtenir des informations sensibles qui ne nous sont pas destinées.

- **Usurpation de l'adresse e-mail**

Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur. Mais, il est possible de changer l'adresse. Ainsi, un pirate peut vous envoyer un mail en usurpant l'adresse de votre supérieur.

✓ **Man in the Middle**

Man in the Middle signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu.

Figure II .16: man in the middle

✓ **Hijacking**

Un pirate peut craquer (cible) le mot de passe de la session. Mais si vous choisissez un mot de passe robuste, cela lui prendra beaucoup de temps. Alors pourquoi ne pas

attendre que la victime se connecte sur la session et prendre sa place ? Ainsi, le pirate contourne le processus d'authentification. Et justement, il le fait, c'est le principe du détournement de session (en anglais hijacking). Ensuite, s'il veut pouvoir dialoguer avec le serveur, il doit mettre hors-jeu la victime. Pour cela, il peut lui lancer une attaque par déni de service (cible). Mais, il peut aussi se mettre en écoute et enregistrer tout le trafic en espérant recueillir des informations sensibles comme des mots de passe.

Figure II .17 : Hijaching

- ✓ **Buffer OverFlow**

Un débordement de tampon (en anglais Buffer OverFlow ou BoF) est une attaque très utilisée des pirates. Cela consiste à utiliser un programme résidant sur votre machine en lui envoyant plus de données qu'il n'est censé en recevoir afin que ce dernier exécute un code arbitraire. Il n'est pas rare qu'un programme accepte des données en paramètre. Ainsi, si le programme ne vérifie pas la longueur de la chaîne passée en paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande.

II.4.But d'attaques

- ✓ **Interruption :** Vise la disponibilité des informations.

Figure II.18: Interruption des données.

- ✓ **Interception**: Vise la confidentialité des informations.

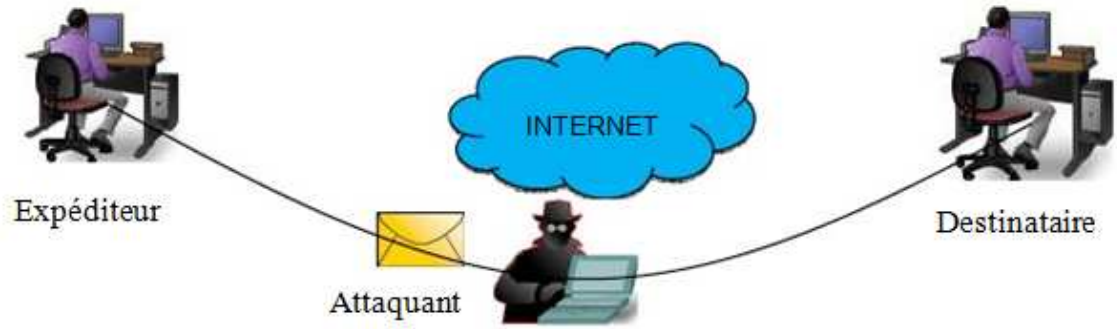


Figure II.19: Interception des données

- ✓ **Modification** : vise l'intégrité des informations.

Figure II.20: Modification des données

- ✓ **Fabrication** : Vise l'authenticité de la source ou de la destination des informations.

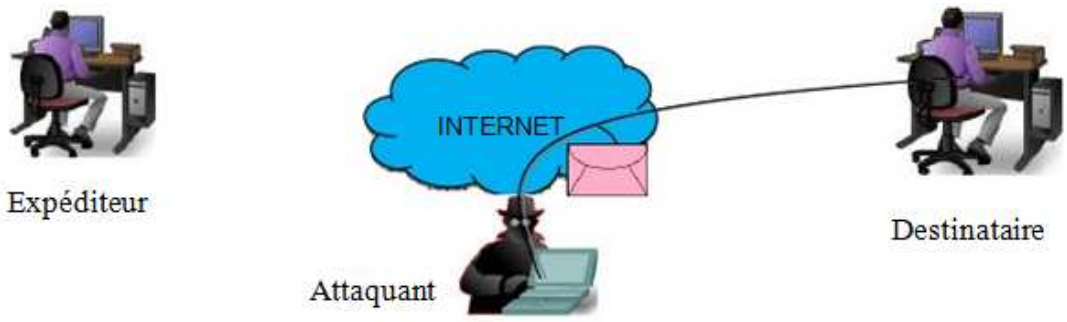


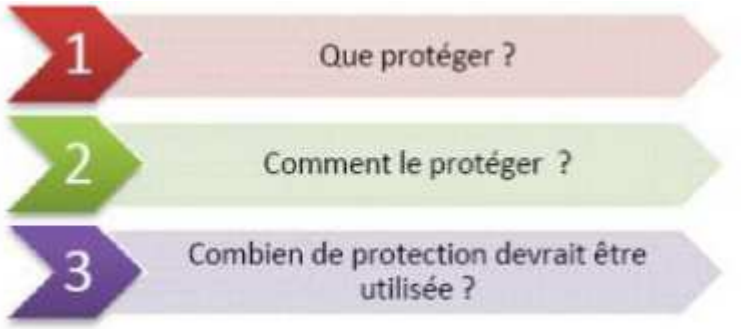
Figure II.21 : Fabrication des données.

II.5.Moyennes et technique de sécurité

La tâche la plus difficile quand on traite la sécurité ou bien quand on définit la politique de sécurité que l'entreprise doit suivre, est probablement la phase de planification dans laquelle on développe une solution pour répondre aux besoins en sécurité et les objectifs de notre entreprise. En examinant le réseau et en identifiant les zones et les composants critiques et à risque, on devrait prendre une approche, pour créer un plan de sécurité, avec diverse objectifs en perspectives :

- ❖ Une politique de sécurité cohérente et simple devrait être créée, basée sur la stratégie et les objectifs de l'entreprise (c.à.d. aider l'entreprise à atteindre ces objectifs, et non l'entraver par des procédures trop rigides qui vont gêner les utilisateurs dans leur travail et diminuer le rendement).
- ❖ La politique de sécurité devra décider du choix des solutions et des produits de sécurité, mais pas l'inverse.
- ❖ La gestion de sécurité devrait être centralisée sous une seule plateforme, de préférence d'un même constructeur afin de faciliter le déploiement, le contrôle et le support de la solution.

En général, une bonne politique de sécurité devrait aborder les questions suivantes:



✓ Cryptographie

Les récents développement de la cryptographie permettent de résoudre les nombreux problèmes menaçants la vie privé ou la sécurité sur internet, la cryptographie est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information telle la confidentialité, l'intégralité des données, authentification d'entités, et l'authentification de l'originalité des données.

✓ Logiciels antivirus

La plupart des ordinateurs sont dotés d'un logiciel antivirus capable de détecter les menaces virales s'il est régulièrement mis à jour et correctement entretenu.

✓ Pare-Feu

C’est un routeur ou serveur d’accès désigné comme tampon entre les réseaux publics connectés et un réseau privé, ou bien entre Internet et le réseau interne d'une entreprise. En pratique, le pare-feu consistera en une architecture, plutôt qu'un matériel ou un logiciel précis.

Cette architecture intégrera alors une série de composants matériels et logiciels qui eux tenteront précisément d'assurer le niveau de sécurité requis.

✓ Filtres de Paquets

Le principe fondamental d'un filtre de paquets est comme son nom l'indique, permet de filtrer les paquets circulant sur un réseau. Plus précisément, on peut même dire que le filtrage s'effectue sur les paquets traversant une interface réseau.

✓ Les Proxys

Les proxys sont des serveurs fonctionnent au niveau des protocoles de la coucheapplication du modèle TCP/IP. Ceux-ci servent d'intermédiaire, entre un client du réseau interne, et des serveurs situés à l'extérieur du réseau de l'entreprise.

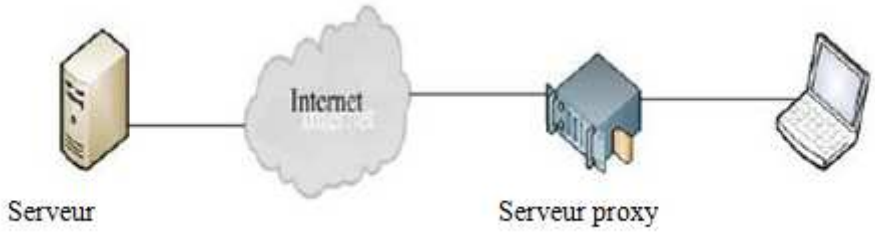


Figure II.23: Emplacement de serveur proxy.

✓ Système de détection d'intrusions

Un système de détection d'intrusions fournit une surveillance constante du réseau. Cesystème analyse les flux de paquets de données du réseau à la recherche d'activités nonautorisées, telles que les attaques de pirates, et permet aux utilisateurs de répondre aux faillesdans la sécurité avant que les systèmes ne soient compromis.

✓ VPN

Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une abstraction permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local. Toute la partie de routage pour atteindre le ou les autres ordinateurs est gérée de façon transparente par le logiciel de VPN, créant un tunnel.

II.6 Caractéristiques d'un réseau fiable

Un réseau solide est un réseau qui offre :

✓ **Disponibilité** : autrement dit la capacité à être prêts à fournir un service

(Laprobabilité qu'un service soit en bon état de fonctionnement à un instant donné). Si le réseau venait à être inaccessible, la communication et la collaboration s'arrêteront, ainsi la productivité de des utilisateurs se verrait réduite. La disponibilité touche les aspects tels que :

- **Les liaisons avec le réseaupublic**

  Chaque contrat avec un opérateur doit garantir par exemple un certain délai de rétablissement du lien en cas de dysfonctionnement. Ce même principe doit être définit en interne.

- **Les équipements matériels d'interconnexion**

  Il est important de conclure des contrats de maintenance avec des entreprises sous-traitantes pour le dépannage des équipements en cas de panne, et d'obtenir une garantie lors de l'achat du matériel. Une sous-estimation de ces aspects peut engendrer de graves conséquences sur la productivité d'une entreprise.

- ✓ **Tolérance aux pannes**

La tolérance aux pannes (on dit également « insensibilité aux pannes ») désigne une méthode de conception permettant à un système de continuer à fonctionner, éventuellement de manière réduite au lieu de tomber complètement en panne, lorsque l'un de ses composants ne fonctionne plus correctement.

Tout dispositif technique permettant de palier à ces différentes pannes sans interrompre la bonne marche du système peut être considérée comme tolérant les pannes.

- ✓ **Sécurité**

Les problèmes liés à la sécurité, souvent très onéreux, peuvent être l'indisponibilité des serveurs, du réseau, les vols d'information, des attaques qui viennent parfois du réseau local. Les outils pour y remédier sont tellement disparates (un peu à tous les niveaux) et ne colmatent qu'une partie des failles du fait des nouvelles sorties. De plus le protocole réseau IP qui n'assure aucune fiabilité ne rend pas cette tâche facile. Vue l'importance de la sécurité, il s'avère utile de coupler plusieurs outils et mécanismes pour au moins s'assurer une meilleure protection.

- ✓ **Qualité de service**

Qui dit qualité de service dit la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de débit, latence (délai de transmission), taux de perte de paquets, gigue (variation de la latence). Ce problème ne se pose pas quand la bande passante est à profusion, c'est le cas généralement des LAN. Par contre le besoin d'assurer une qualité de service s'impose quand la bande passante est limitée et chère, c'est le cas dans les WAN, la difficulté augmente avec la présence d'un ou de plusieurs opérateurs.

Conclusion

La politique de sécurité permet de transcrire le travail de modélisation effectué pour comprendre les risques et leurs impacts, en des mesures concrètes de sécurité. Sa spécification est un des garants du bon dimensionnement des mesures de sécurité et d'une gestion efficace. Elle donne de la cohérence à la gestion et permet d'adopter vis à vis des risques et menaces, une attitude préventive et proactive et pas seulement réactive. Elle permet de lier la stratégie de sécurité de l'entreprise à sa réalisation opérationnelle.

La bonne réalisation d'une politique de sécurité permet au mieux, de maîtriser les risques informatiques, tout en réduisant leur probabilité d'apparition.

Dans le chapitre suivant, je vais détailler une technique de sécurité réseau eu utilisant les différentes aspects sécurités Informatique (FIREWALL, ANTIVIRUS, ARECHETICTURE, ACL, VLAN ……)

Chapitre III

Sécurité informatique

Sécurité informatique

I. Définition de la sécurité informatique

La sécurité informatique est l'ensemble des techniques qui assurent les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

Politique de sécurité

La sécurité des systèmes d'information se charge généralement à garantir les droitsd'accès aux données et ressources d'un système, en mettant en place des mécanismesd'authentification et de contrôle. Ces mécanismes permettent d'assurer que les utilisateurs desdites ressources possèdent uniquement les droits qui leurs ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcherles utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ilspuissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il estnécessaire de définir dans un premier temps une politique de sécurité, c'est-à-dire :

- élaborer des règles et des procédures, installer des outils techniques dans les différentsservices de l'organisation (autour de l'informatique).
- définir les actions à entreprendre et les personnes à contacter en cas de détection d'uneintrusion.
- sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmesd'informations.
- préciser les rôles et responsabilités.

La politique de sécurité est donc l'ensemble des orientations suivies par une entité entermes de sécurité.

II. Les objectifs de la sécurité informatique

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, etc... Néanmoins, les points principaux points sont les suivants :

- empêcher la divulgation non-autorisée de données
- empêcher la modification non-autorisée de données
- empêcher l'utilisation non-autorisée de ressources réseau ou informatiques de façon générale

III.Les champs d'application de sécurité informatique

Ces objectifs s'appliquent dans différents domaines ou champs d'applications, chacun faisant appel à des techniques différentes pour atteindre le ou les mêmes objectifs; ces champs sont :

- la sécurité physique
- la sécurité personnelle
- la sécurité procédurale (au dit de sécurité. procédures informatiques...)
- la sécurité des émissions physiques (écrans, câbles d'alimentation, courbes de consommation de courant...)
- la sécurité des systèmes d'exploitation
- la sécurité des communications

IV. Les outils de sécurité informatique

IV.1.Firewall

IV.1.1. Définition de firewall

En informatique, un Firewall est un périphérique ou un ordinateur qui protège la partie privée d'un réseau de la partie publique. C'est en réalité l'élément qui permet de distinguer la partie privée du réseau de celle que l'on nommera publique (Internet,. . .), lui seul peut donc en atteindre les deux extrémités. Il permet donc de protéger le réseau privé éventuelles attaques provenant d'Internet et peut également contrôler certaines actions effectuées de l'intérieur du réseau privé.

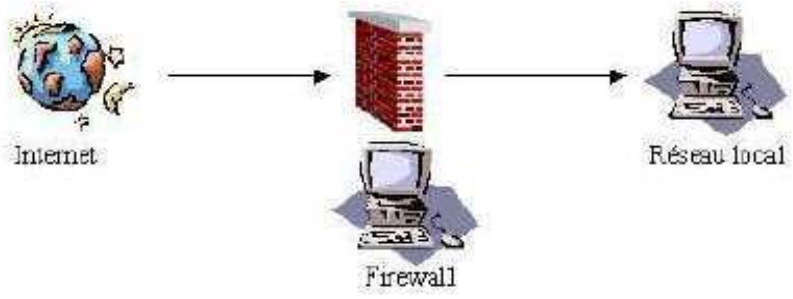


Figure III.1*:* Placement d'un firewall

IV.1.2. Rôle d'un firewall

Le rôle du firewall repose sur deux techniques de base:

- ✓ **Le filtrage des paquets de données**

  Est la technique la plus élémentaire pour protéger un réseau.

Chaque paquet reçu est comparé avec un ensemble de règles, pour choisir le traitement à réaliser.

- ✓ **Courroie de transmission**

  Sert à masquer les machines de votre réseau derrière le firewall.

Cela permet donc à un serveur de se faire passer pour la machine à l'origine d'un paquet.

IV.1.3. Principe de fonctionnement des *Firewalls*

Il y a en réalité deux principaux types de Firewall:

- **Firewall IP Filter ou Chokes :** ce type de Firewall travail au niveau des paquets transmis sur les réseaux, il permet de contrôler le flux de paquets en fonction de l'origine, de la destination, des ports et du type d'information contenue dans chacun d'eux. C'est un système relativement facile àmettre en place en instaurant un certains nombre de règles permettant de contrôler les paquets entrants ou sortants du réseau privé. Il s'agit soit d'un ordinateur soit d'un périphérique de communication permettant de restreindre le flux de paquets entre les réseaux.

- **Gates :** il s'agit d'un programme, d'un périphérique ou d'un ordinateur qui reçoit lesConnections des réseaux externes et les retransmet dans le réseau privé. Aucun utilisateurn'est autoriséà accéder à ce Gatespour des raisons de sécurité(seule une connections sur laconsole par l'administrateur est autorisée).

IV1.4. Différents types de firewalls

1. Pare-feu niveau réseau.(iptables, paquet filter, . . .)
   - ✓ Firewall fonctionnant à un niveau bas de la pile TCP/IP
   - ✓ Basé sur le filtrage des paquets
   - ✓ Possibilité (si mécanisme disponible) de filtrer les paquets suivant l'état de la connexion

   Intérêt : Transparence pour les utilisateurs du réseau
2. Pare-feu au niveau applicatif.(inetd, xinetd, . . .)
   - ✓ Firewall fonctionnant au niveau le plus haut de lapile TCP/IP
   - ✓ Généralement basé sur des mécanismes de proxy

   Intérêt : Possibilité d'interpréter le contenu du trafic
3. Pare-feu des applications. (/etc/ftpaccess pour ftp, . . .)
   - ✓ Restrictions au niveau des différentesapplications

IV.2. VLAN (réseaux locaux virtuels)

IV.2.1.Définition de VLAN

Un réseau local virtuel est un groupe logique d'unités ou d'utilisateurs qui peuvent êtreregroupés par fonction, service ou application peu importe l'emplacement de leursegment physique. La configuration d'un réseau local virtuel est effectuée dans lecommutateur par un logiciel. Les réseaux locaux virtuels ne sont pas uniformisés etnécessitent l'utilisation d'un logiciel propriétaire vendu par le fournisseur decommutateurs. Ce type de réseau est vu plus en détails à la section suivante.

IV.2.2.Lestypes de fonctionnement des VLAN

Il existe 3 types différents de VLAN :

VLAN de niveau 1 (ou VLAN par port)

On y définit les ports du commutateur (switch) qui appartiendront à tel ou tel VLAN. Cela permet entre autres de pouvoir distinguer physiquement quels ports appartiennent à quels VLAN.

VLAN de niveau 2 (ou VLAN par adresse MAC)

On indique directement les adresses MAC des cartes réseaux contenues dans les machines que l'on souhaite voir appartenir à un VLAN, cette solution est plus souple que les VLAN de niveau 1, car peu importe le port sur lequel la machine sera connectée, cette dernière fera partie du VLAN dans lequel son adresse MAC sera configurée (mais présente tout de même un inconvénient, car si le serveur contenant les adresses MAC tombe en panne, tout le réseau est alors affecté).

VLAN de niveau 3 (ou VLAN par adresse IP)

Même principe que pour les VLAN de niveau 2 sauf que l'on indique les adresses IP (ou une plage d'IP) qui appartiendront à tel ou tel VLAN.

Pour déployer des VLAN, cela sous-entend que le commutateur (switch) utilisé soit gérable et qu'il gère les VLAN du niveau désiré, à savoir également que plus le niveau de VLAN est élevé, plus le commutateur (switch) sera cher à l'achat.

IV.2.3.Le marché des VLAN

Le choix d'un type de fonctionnement et d'un mode de définition des *VLAN* doit être faitaprès une étude approfondie de l'utilisation du réseau. Une solution qui allieperformance, flexibilité, sécurité et facilité d'administration est celle qui assure unfonctionnement de type 2 (basé sur l'adresse *MAC*), tout en permettant une définitiondes *VLAN* à partir des adresses réseau, plus faciles à gérer que les adresses *MAC*.

L'offre commerciale est arrivée à maturité et le choix est vaste, les solutions nonpropriétaires peuvent être privilégiées dans un milieu en évolution rapide, oùl'interopérabilité est une contrainte forte. Il n'en demeure pas moins que les *VLAN $*restent encore des solutions propriétaires.

IV.2.3.Avantages VLAN

- ✓ la réduction de la charge des trafics en minimisant les domaines de diffusiondans un réseau;
- ✓ la formation de groupes virtuels;
- ✓ l'augmentation de la sécurité;
- ✓ la simplification de l'administration;
- ✓ la réduction des coûts

IV.2.4.Ladifférence entre les LAN et VLAN

Un réseau local (LAN) est défini par un domaine de diffusion dans lequel tous les hôtes reçoivent les messages de diffusion émis par n'importe quel autre hôte du réseau. Par définition, un réseau local est délimité par une interface d'équipement de niveau 3 du modèle OSI (couche réseau).

Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements de niveau 2 du modèle OSI (couche liaison). Le domaine de diffusion se retrouve ainsi réparti sur ces mêmes équipements de niveau 2. Ainsi, tous les hôtes appartenant au même réseau local (domaine de diffusion) constituent un groupe logique indépendant de la topologie physique du réseau.

IV.3 ACL (liste de contrôle d'accès)

IV.3.1. Définitions d'ACL :

Une liste d'accès est un mécanisme d'identification de trafic particulier. Une des applications d'une liste d'accès est de filtrer le trafic entrant ou sortant d'une interface de routeur.

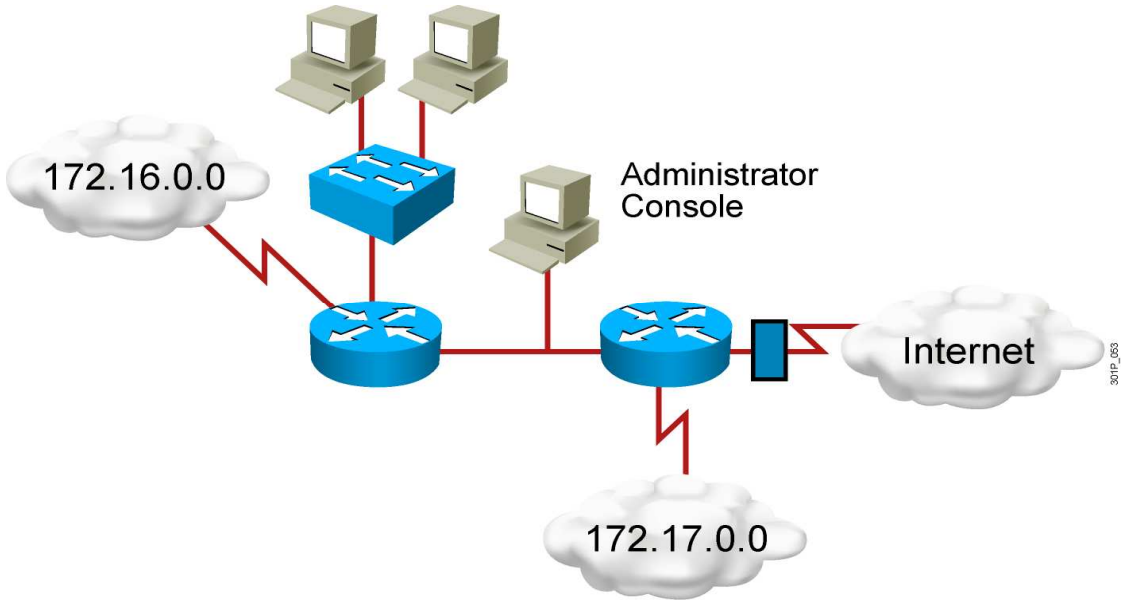


Figure III.2 : ACL

IV.3.2. Pourquoi utiliser une Liste de Contrôle d'Accès ?

L'utilisation des listes de contrôle d'accès peut engendrer des problèmes :

- La charge supplémentaire sur le routeur découlant de la vérification de tous les paquets réduit le temps disponible pour le transfert de ces paquets.
- Des listes de contrôle d'accès mal conçues augmentent encore plus la charge sur le routeur, pouvant provoquer une interruption du réseau.
- Des listes de contrôle d'accès mal positionnées peuvent bloquer le trafic qui devrait être autorisé et autoriser le trafic qui devrait être bloqué.

IV.3.3. Les différents types de Liste de Contrôled'Accès

Il existe trois Types de Liste de contrôle. Selon les objectifs de l'administrateur réseau, peux utiliser :

✓ Listes de contrôle d'accès standard

La liste de contrôle d'accès standard constitue le type le plus simple. Lors de la création d'une liste de contrôle d'accès IP standard, le filtre est basé sur l'adresse IP source d'un paquet.

Les listes de contrôle d'accès standard sont identifiées par le numéro qu'elles se voient attribuer. Pour les listes d'accès autorisant ou refusant le trafic IP, le numéro d'identification est compris entre **1** et **99** et entre **1 300** et **1 999**.

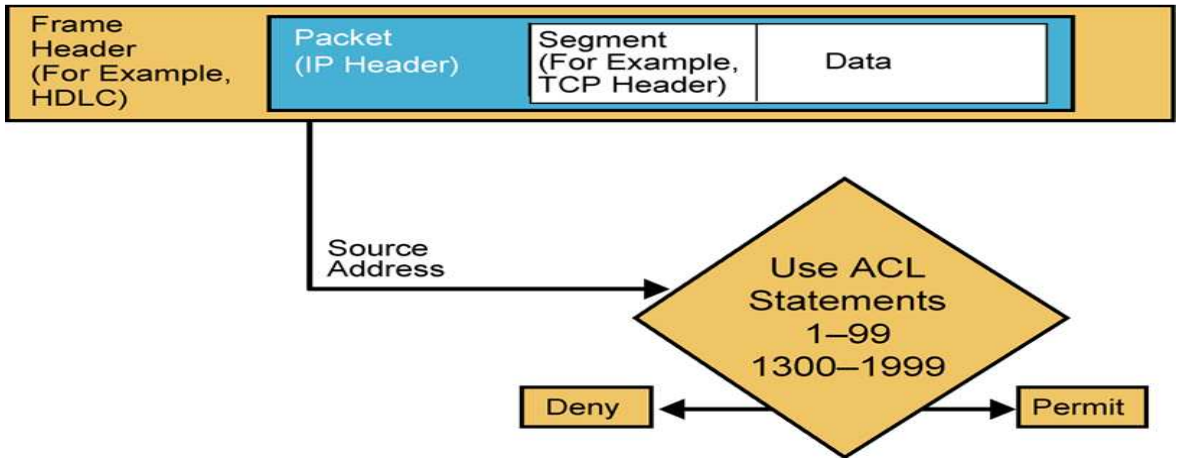


Figure III.3 : ACL standard

✓ Listes de contrôle d'accès étendues

Les listes de contrôle d'accès étendues filtrent non seulement sur l'adresse IP source, mais également sur l'adresse IP de destination, le protocole et les numéros de port

Les numéros des listes de contrôle d'accès étendues vont de **100** à **199** et de **2 000** à **2 699**.

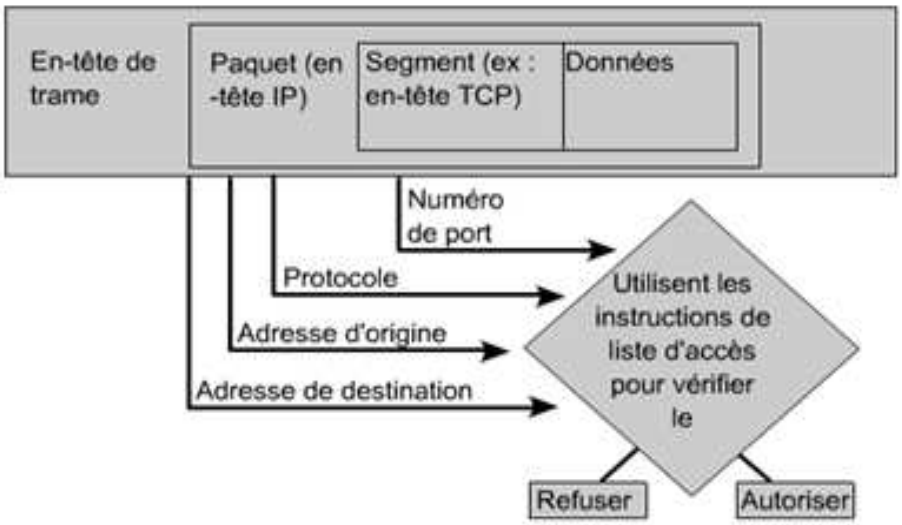


Figure III.4 : ACL étendues

IV.3.4.Différence entre les ACLS standards et étendues

L'ACL standard filtre uniquement sur les adresses IP sources. Elle est de la forme:**access-list numéro-de-la-liste {permit|deny} {host|sourcesource-wildcard|any}**L'ACL étendue filtre sur les adresses source et destination, sur le protocole et le numéro de port.Elle est de la forme: **access-list numéro de la liste {deny|permit} protocole source masque-source [operateur [port] destination masque-destination [operateur [port]][established][log]**

IV.3.5. Principales raison pour crées des listes de contrôle d'accès

- ✓ Limiter le trafic et accroitre les performances. En limitant le trafic vidéo
- ✓ Contrôler le flux de trafic, les ACL peuvent limite l'arrivée des misée à jour de routage
- ✓ Fournir un niveau de sécurité d'accès réseau de base les listes de contrôle d'accès permettent à un hôte d'avoir accès à la même section.
- ✓ Déterminer le type de trafic qui sera achemine ou bloque au niveau des interfaces de routeur.

- ✓ Autoriser un administrateur à control les zones auxquelles un client peut accéder sur un réseau.

IV.3.6. Implémentation des listes de contrôle d'accès « ACL »

Les listes de contrôle d'accès comprennent une ou plusieurs instructions. Chaque instruction **autorise** le trafic ou provoque le **refus** de celui-ci en fonction des paramètres spécifiés (**Permit/Deny**).

Lorsqu'on crée une instruction de liste de contrôle d'accès, **l'adresse IP** et le **masque générique** deviennent des champs de comparaison. Tous les paquets qui entrent sur une interface ou qui en sortent sont comparés à chaque instruction de la liste de contrôle d'accès afin de rechercher une correspondance. Le **masque générique** détermine le nombre de bits de l'adresse IP entrante qui correspondent à l'adresse de comparaison.

Dans une liste de contrôle d'accès, le **masque générique** spécifie un hôte ou une plage d'adresses à autoriser ou refuser.

IV.4 Les antivirus

IV.3 Définition d'antivirus

L'antivirus est des programmes qui permettent de détecter la présence de virus sur un hôte.

Les trois techniques antivirus les plus utilisées pour détecter les virus sont :

- ✓ Le Scanning : il consiste à rechercher un code spécifique qui est censé indiquer la présence d'un virus.
- ✓ Le moniteur de comportement : c'est un programme résidant, que l'utilisateur charge à partir du fichier AUTOEXEC.BAT et qui reste alors actif en arrière-plan, surveillant tout comportement inhabituel.
- ✓ Le contrôleur d'intégrité : ils signalent toute modification intervenue dans un fichier.

IV.4.2 L'efficacité de l'antivirus

Une étude menée dans les laboratoires Hewlett Packard conclue que les antivirus seraient en train de perdre la guerre contre les virus. En effet, le principe même de fonctionnement de l'antivirus n'est pas efficace puisque les vers informatiques se propagent trop rapidement par rapport au temps requis pour l'application des mises à jour.

IV.4.3 Mise à jour de l’antivirus

Cela pose donc la problématique de la mise à jour rapide de l’antivirus, et donc de la mise à disposition rapide des antidotes, et rien ne garantit que l’utilisateur finaleffectue des mises à jour assez régulières. Ni qu’un antivirus à propagation rapide n’aura pas déjà infecté des machines avant la mise à disposition des antidotes.

Conclusion

Obtenir un niveau de sécurité informatique suffisant pour prévenir les risquestechnologiques et informationnels est primordiale pour un bon fonctionnement des organismes. Il est important de pouvoir les identifier correctement pour circonscrire lespérimètres à mettre en place et protéger efficacement les valeurs qui doivent l’être. Ceciimplique une approche pluridisciplinaire et systémique de la sécurité globale de cetorganisme.

La sécurité informatique sera effective dans la mesure où l’on sait mettre en place desmesures de protection homogènes et complémentaires des ressources informatiques, mais aussi de l’environnement qui les héberge. Aux aspects purementtechniques de la sécurité, il faut associer la mise en œuvre efficace des procéduresd’exploitation et de gestion. Par ailleurs, le gérant de l’organisme doit être formé aux mesuresde sécurité et doit s’engager à les respecter.

Chapitre VI

CONCEPTION ET REALISATION

Introduction

Ce chapitre est la dernière partie de notre travail, donc nous allons nous intéresser à la mise en œuvre de notre application en établissant une nouvelle implémentation pour notre réseau qui consiste à segmenter le réseau actuel du bloc administratif en VLAN, en créant plusieurs sous réseau (Vlan) pour séparer les flux des différents utilisateurs, ainsi que définir des accès liste afin de pouvoir filtrer le trafic en fonction des besoins du réseau.

Durant ce chapitre nous allons donner :

- ✓ Une présentation de notre réseau.
- ✓ Les outils utilisés.
- ✓ Les différentes étapes de configuration.

IV.1.CONCEPTION

IV.1.1 .Etude de l'existant Critique etsuggestion

Au cours de trois mois de stage pratique mené à l'entreprise ENIEM, une étude approfondie du Réseau de l'ENIEM a été menée et Cette étude nous a aidé à suivre les problèmes de fonctionnement du réseau de l'ENIEM afin de déterminer la conduite 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.

IV.1.2.résentation du réseau existant

Comme la figure le montre le réseau existant contient :

- ✓ SeptSWITCH
- ✓ Deux serveursHPUX
- ✓ Un SWITCHfédérateur
- ✓ Des ordinateurs (pc)
- ✓ Mise en place de deux serveurs ALFATRON

Installation d'une solution de virtualisation PROXMOX sur les nouveaux serveurs

Après sur chaque serveur on a installé:

- Serveur Active directory
- Serveur proxy
- Serveur GLPI et système d'inventaire automatique OCS
- Serveur Anti-virus
- Serveur de Messagerie BLUEMIND
- Serveur de License pour Solidworks

En effets, on dispose de six Switch de telle sorte à les répartir dansdeux bâtiments, ainsi que chaque bâtiment est composé d'un Réez de chaussée et de deux étages, et dans chaque étage on mettra un Switch et qui désignera l'Unité de l'ENIEM, tan-dis-que le septième SWITCH appartient à l'unité prestation technique qui se trouve au sous-sol du bâtiment.

Tous les Switch des unités appartiennent à des armoires dites armoires de brassages sauf le SWITCH de l'unité informatique qui appartienne à l'armoire d'étage où se trouve le SWITCH fédérateur auquel sont relié les six autres Switch par la fibre optique.

IV.1.3. Le réseau existant

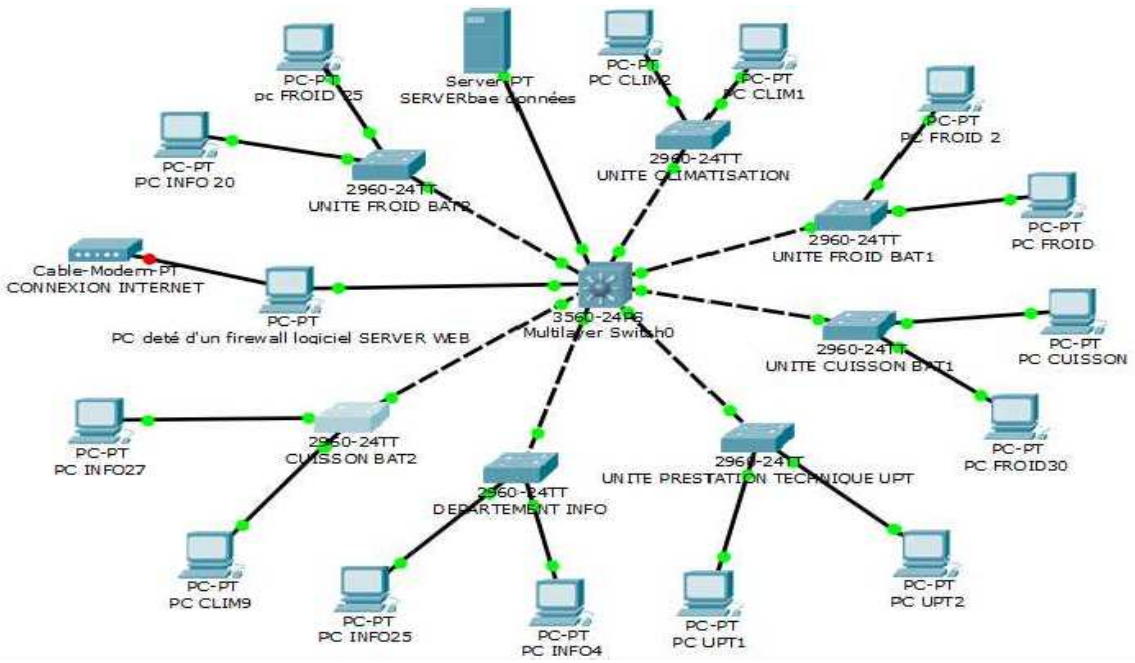


Figure IV.1 : présentation du réseau existant.

IV.1.4.fonctionnement du réseau existant

L'accès est permis de chaque unité émettrice vers n'importe quelle unité destinataire (accès non limité).

Aussi qu'on n'a pas une sécurisation sur les Switch, ce qui veut dire que chaque utilisateur peut y accéder à n'importe quel Switch d'étage ainsi qu'au Switch Fédérateur, alors un utilisateur peut modifier ou bien supprimer les configurations faites sur chacun d'eux ce qui crée un conflit et un débordement dans le réseau.

Ainsi le réseau mis en œuvre dans la figure **IV.1** indique qu'un ordinateur peut émettre un trafic vers n'importe quel destinataire voulu et aussi, recevoir du n'importe quelle source. Donc tous les PCs se connecter entre eux.

IV.1.4.1.Explication

La configuration de tous les équipements d'interconnexions (Switch d'étage, Switch fédérateur) présentés dans la figure est dite: configuration basique cela veut dire que cette configuration est limitée à l'utilisation d'un seul VLAN par défaut (natif) qui est le VLAN 1,et que la configuration des Switch n'utilise que des mots de passes et une adresse IP, autrement dit tous les Switch se trouvent dans un seul sous réseau et c'est ce que explique le fait que tous les Switch , ainsi que tous les ordinateurs connectés à leurs différents ports peuvent se voir et se connecté entre eux .

La figure nous montre aussi que dans un Switch d'une unité considérée on peut trouver des ordinateurs d'une autre unité qui lui y sont reliés, sachant que ces ordinateurs se trouvent tous dans un même sous réseau, par exemple l'ordinateur PCfroid.30 appartient à l'unité froid mais comme les ports de ce dernier sont tous utilisés donc il est reliés à l'un des ports libres qui se trouvent dans le Switch de l'unité cuisson.

IV.1.5.Les critiques du réseau existant

Apres avoir expliqué le fonctionnement du réseau local de l'entreprise ENIEM, nous avons arrivé à extraire les critique suivantes :

- ✓ **Critique1** : les Switch du réseau sont configurables mais non configurés.

  Tous les Switch sont considérés comme des Switchsimples.

- ✓ **Critique 2** : le réseau est installé anarchiquement et non administré.

  Des fonctions de différentes unités se trouvent sur le même Switch et non administrés.

- ✓ **Critique3** : le réseau installé est non sécurisé contre les intrusions d'une façon fiable.

  La sécurité du réseau existant est basée uniquement sur l'utilisation d'un firewalllogiciel.

- ✓ **Critique4** : Le réseau Local est relié à l'internet ce qui donne un passage au menaces extérieures.

IV.1.6. Les Solutions proposées

L'avènement de l'internet et des nouvelles technologies donnent une raison et une curiosité motivante aux pirates et aux malveillants de pénétrer de plus en plus dans les réseaux que ce soit par fun ou pour usurper des données et informations confidentielles.

Dans cette solution nous essayerons de minimiser au maximum les risques d'attaques et les points vulnérables de l'entreprise ainsi que le débordement interne du réseau.

Ce qui nous a permis à proposer ou bien à implémenter une nouvelle architecture plus sécurise et mieux administrer soit en Local ou à l'extérieur et tout cela c'est pour le bon déroulement du réseau de l'entreprise et qui a l'objectif suivant.

IV.1.6.1. Objectifs

Le projet consiste à segmenter le réseau actuel du Bloc Administratif en VLAN, en créant plusieurs sous réseau (Vlan) pour séparer les flux des différents utilisateurs. Cette segmentation va nous permettre les avantages ci-après:

- ✓ Une réduction des domaines de diffusion (Optimisation de la bande passante)
- ✓ Une administration souple et efficace etc….

Ainsi que dans chaque Switch on a défini des Listes de Contrôle d'Access pour gérer le flux des différents utilisateurs et de bien administré le réseau.

IV.2. Les solutions proposées

IV.2.1. L'architecture proposée

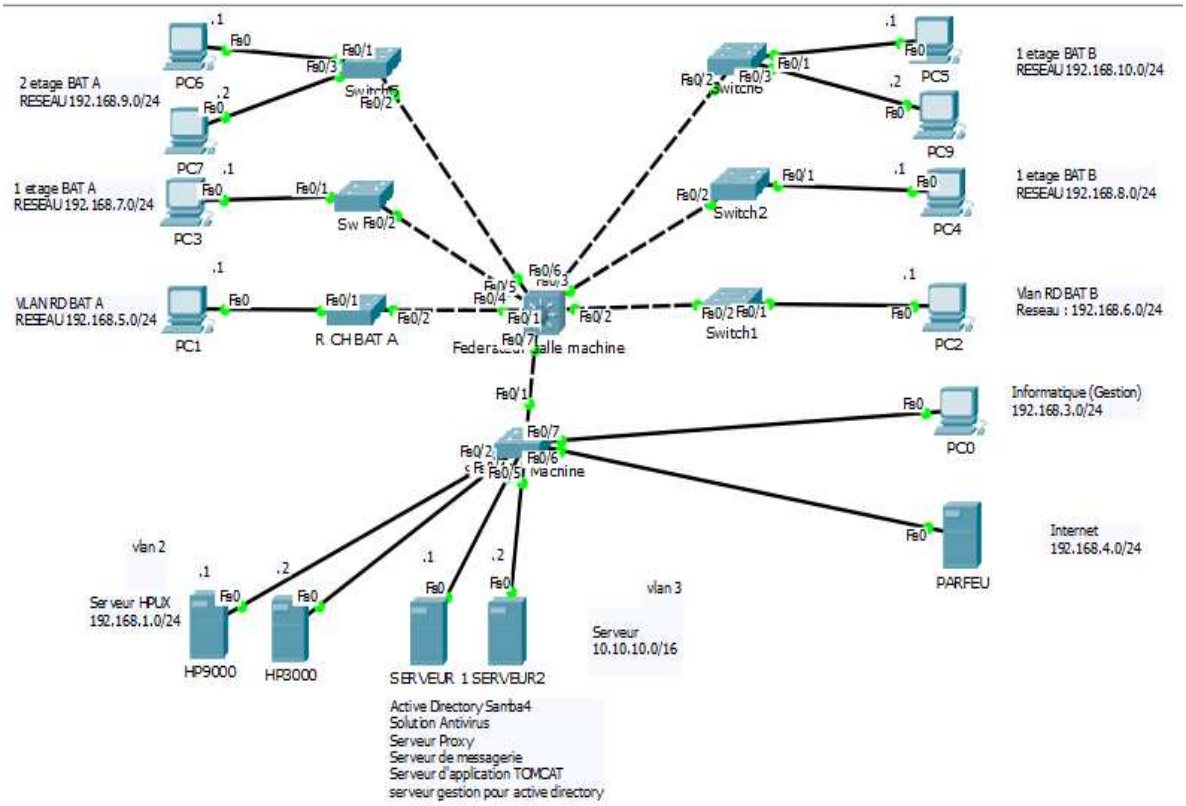


Figure IV.2.1 : L'architecture proposée.

IV.2.1.1.Déroulement du projet

- **Salle Machine**

1. Switch Fédérateur (Switch de niveau 3)

1- Création des Vlan au niveau du Switch Fédérateur

2- Configuration de toutes les interfaces en mode Trunk

3- Modification les paramètres de sécurités du Switch

4- Affectation des deux ports giga Ethernet sur VLAN SERVEUR

2. Switch d'étage (Switch de niveau 2)

1- Création des Vlan au niveau du Switch d'accès.

2- Configuration de deux ports fibre optique en mode Trunk

3- Affectation des ports aux Vlan approprient

- **Réez de chaussée :(A et B)**

3. Switch d'étage

1- Création des Vlan au niveau du Switch d'accès.

2- Configuration de deux ports fibre optique en mode Trunk

3- Affectation des ports aux Vlan approprient

- **1er Étage : (A et B)**

4. Switch d'étage

1- Création des Vlan au niveau du Switch d'accès.

2- Configuration de deux ports fibre optique en mode Trunk

3- Affectation des ports aux Vlan approprient

- **2eme Etage :(A et B)**

5. Switch d'étage

1- Création des Vlan au niveau du Switch d'accès.

2- Configuration de deux ports fibre optique en mode Trunk

3- Affectation des ports aux Vlan approprient

IV.2.1.2. Plan d'adressage des segments (VLAN)

ID VLAN	Nom Vlan	Réseau	Port	Passerelle
VLAN 2	Serveur HPUX	192.168.1.0/24		192.168.1.2
VLAN 3	Serveur	10.10.10.0/24	Gig0/1 et 0/2	10.10.10.3
VLAN 4	Internet	192.168.4.0/24		192.168.4.4
VLAN 5	Informatique	192.168.3.0/24		192.168.3.5
VLAN 99	Gestion	192.168.99.0/24	VLAN 99	192.168.99.99
VLAN 10	RDCA	192.168.5.0/24	Tous les ports	192.168.5.10
VLAN 11	RDCB	192.168.6.0/24	Tous les ports	192.168.6.11
VLAN 12	1ETGA	192.168.7.0/24	Tous les ports	192.168.7.12
VLAN 13	1ETGB	192.168.8.0/24	Tous les ports	192.168.8.13
VLAN 14	2ETGA	192.168.9.0/24	Tous les ports	192.168.9.14
VLAN 15	2ETGB	192.168.10.0/24	Tous les ports	192.168.10.15

Tab IV.1: Plan d’adressage des segments.

IV.2.1.3. La sécurisation des SWITCH par des ACL

Dans chaque SWITCH on a défini des Listes de Contrôle d'Access.

- SWITCH Fédérateur

Dans ce SWITCH on a défini des ACL qui nous aideront à limiter les accès Telnetet de le protéger contre toute les authentifications non autorise, ainsi que de sécuriser notre réseau pour empêcher les utilisateurs de se connecter entre eux.

- SWITCH d'étage

Dans ces SWITCH on a défini toujours des ACL afin de les protéger contre les accès Telnet des utilisateurs, qui peuvent mener des grands risques à la gestion de l'entreprise en supprimant ou bien modifiant les configurations initiales.

Et pour cela on à essayer de proposer une autre solution, d'introduire un Vlan de gestion qui est le département informatique de l'entreprise qui va s'occuper de la gestion de tous les SWITCH et utilisateurs.

IV.2.1.4. Remplacer le PIX par ASA

Apres que le firewall PIX eut été suspendu, une autre gamme dite ASA a vu le jour. Dans l'impossibilité d'effectuer une mise à jour de firewall PIX qui n'existe plus, il doitêtre remplacé par un autre firewall. Nous proposons le Firewall ASA.

Ce dernier regroupe trois éléments de la gamme Cisco en une seule plate-forme, le Cisco PIX firewall, le Cisco VPN 3000 Sériesconcentrateur, le Cisco IPS 4000 SériesSensor et le module qui le différencie vraiment du PIX, le CSC SSM, Content Security and Control Security Service Module pour ajouter ces fonctions <<Anti X>> alors que le PIX n'était qu'un firewall avec quelques fonctions VPN et sonde IPS assez limitées.

II. Réalisation

II.1. Outils utilisés pour la réalisation du projet

II.1.1.Emulateur GNS3 (Graphical NetworkSimulator)

Dans le but de se rapprocher le plus possible de la mise en œuvre d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 (Graphical Network Simulateur). Est un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel.

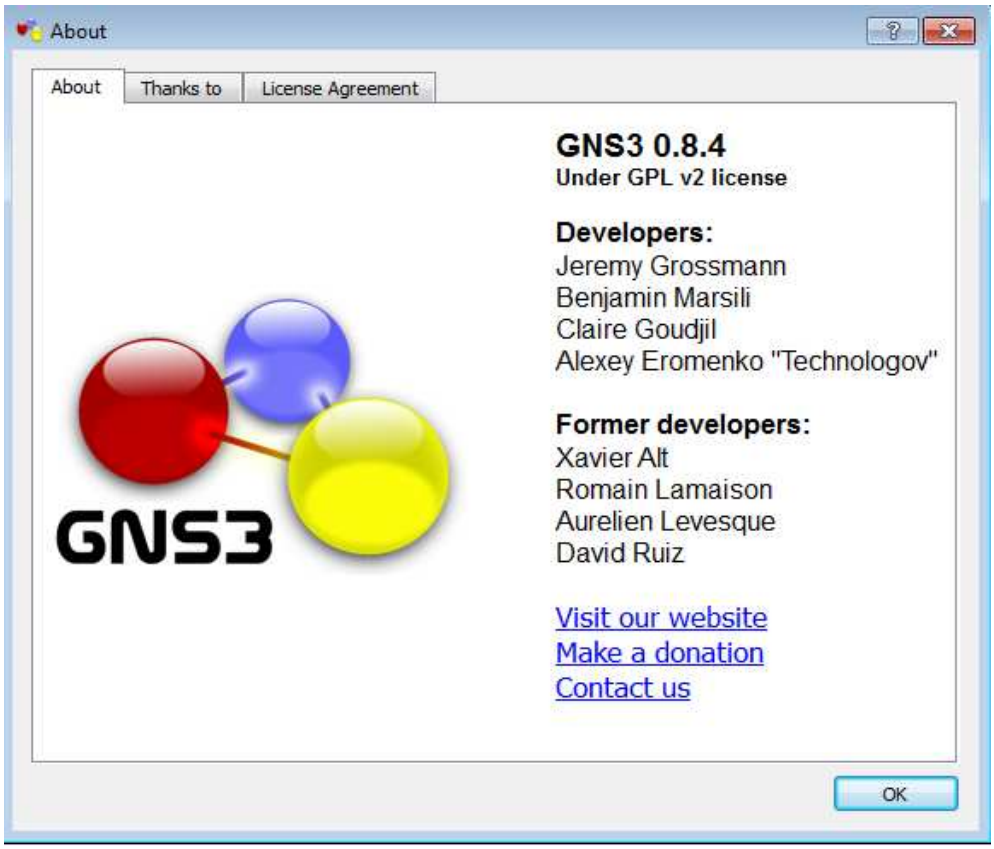


Figure IV.3:GNS3.

II.1.2.La VMware Workstation 9

La VMware Workstation 9 permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation, ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique.

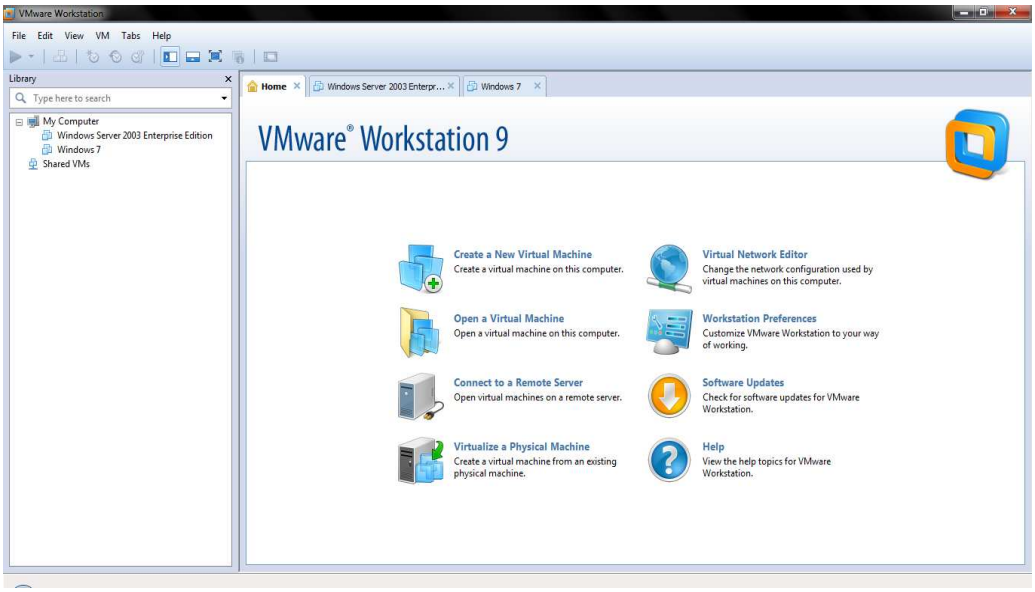


Figure IV.4: VMware Workstation 9.

II.1.3.Microsoft Windows Server 2008

Microsoft Windows Server 2008 est conçu pour fournir aux la plate-forme la plus productive pour virtualiser les charges de travail en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer de façon fiable des applications et des services Web.

FigureIV.5: Windows server 2008.

II.1.4.Active Directory

Pour réaliser la gestion des objets sans liens avec la disposition réelle des protocoles réseauxemployés, nous avons utilisé Active Directory qui est un annuaire des objets du réseau. Il permet aux utilisateurs de localiser, gérer et utiliser facilement les ressources, en organisant l'annuaire en sections, ce qui permet de suivre le développement d'une société (cas de l'ENIEM) allant de quelques objets à des millions d'objets. Combiné aux stratégies de groupes, Active Directory permet une gestion des postes distants de façon complètement centralisé.

Figure IV.6: Active Directory.

II.1.5. Les caractéristiques du PC utilisé

Vu que notre application exige de grandes ressources matérielles, l'utilisation d'un PC de haute qualité était primordiale pour regrouper les solutions proposes, réseaux et systèmes. Les caractéristiques du PC utilisé sont :

- ✓ RAMG
- ✓ Disque Dur 465G
- ✓ Processeur I3 x64 bits
- ✓ Système Windows 7 Professionnel x64 bits
- ✓ Prise en charge de la virtualisation

II.2. Les étapes suivies pour la mise de notre application

Vu qu'il est impossible d'implémenter toute l'infrastructure réseau de l'ENIEM avec les solutions réseaux et systèmes proposes. Nous avons simplifie l'architecture afin de tester le fonctionnement des solutions proposes dans notre architecture réelle. La figure suivante montre l'architecture simplifiée.

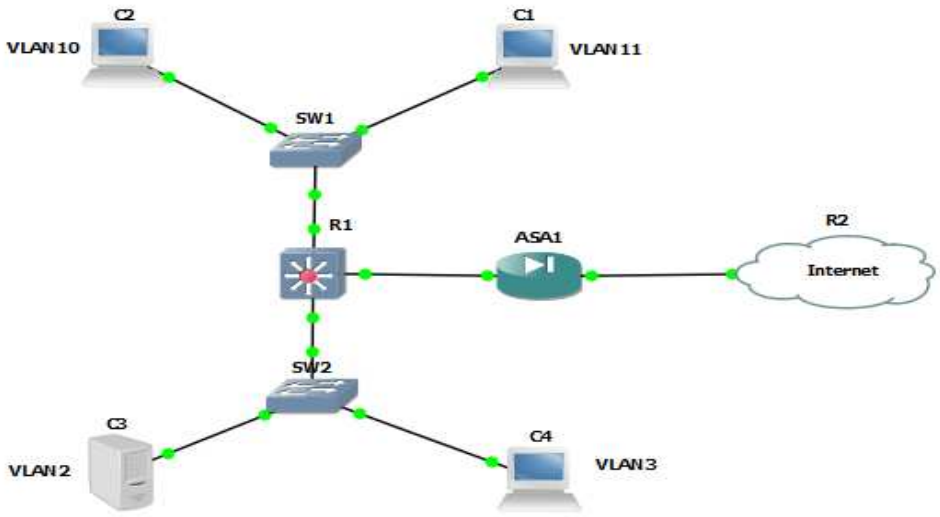


Figure IV.7 : Architecture simplifiée

Etape 1 : La configuration de base des Switch

1. Sécurisation de l'accès au mode d'exécution privilégié

Permet de configurer le commutateur pour qu'il exige un mot de passe lorsque un utilisateur tente d'y accéder au mode d'exécution privilégie.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ena
Switch(config)#enable se
Switch(config)#enable secret amar
Switch(config)#
```

Figure. IV.8: Sécurisation de l'accès au mode d'exécution privilégié.

2. La configuration de ligne de console

A l'ouverture de la console, un message d'activation de la console s'affiche, nous tapons les commandes suivantes comme la montre la figure ci-dessous pour activer la console.

```
Switch>en
Password:
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#lin
Switch(config)#line c
Switch(config)#line console 0
Switch(config-line)#pas
Switch(config-line)#password amar
Switch(config-line)#log
Switch(config-line)#logi
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#
```

Figure IV.9: La configuration de ligne de console.

3. La configuration de ligne VTY

Permet d'interdire les accès Telnet au périphérique sans authentification préalable.

```
User Access Verification

Password:

Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#li
Switch(config)#line v
Switch(config)#line vty 0 4
Switch(config-line)#pas
Switch(config-line)#password amar
Switch(config-line)#log
Switch(config-line)#logi
Switch(config-line)#login
Switch(config-line)#t
Switch(config-line)#transport i
Switch(config-line)#transport input t
Switch(config-line)#transport input telnet
Switch(config-line)#exit
Switch(config)#
```

Figure IV.10: La configuration de ligne VTY.

4. Le chiffrement des mots de passe

Empêche que les mots de passe soient indiqués en clair dans les informations de configuration.Cette commande a pour but d'empêcher les personnes non autorisées de lire les mots de passe dans le fichier de configuration.

```
User Access Verification

Password:

Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#se
Switch(config)#service p
Switch(config)#service password-encryption
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Figure IV.11: Le chiffrement des mots de passe.

Etape 2 : La configuration des VLAN

On est censé de créer quatre Vlan différents présentés dans l'architecture simplifié les deux premier nommés Client1 et Client2 sont créé dans le Switch d'étage nommé S1 et les deux autres nommés Gestion (qui est le Vlan de gestion) et serveur sont créé dans le deuxième Switch d'étage nommé S2.

1. Création de VLAN dans S1

Nous tapons les commandes suivantes comme la montre la figure ci-dessous :

```
User Access Verification

Password:

S1>en
Password:
S1#vla
S1#vlan d
S1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

S1(vlan)#vl
S1(vlan)#vlan 10 name Client1
VLAN 10 modified:
    Name: Client1
S1(vlan)#vlan 11 name Client2
VLAN 11 modified:
    Name: Client2
S1(vlan)#exit
APPLY completed.
Exiting....
S1#
S1#
```

Figure. IV.12: Création de VLAN dans S1.

2. La vérification de création de VLAN dans S1

Nous tapons les commandes suivantes comme la montre la figure ci-dessous :

```
User Access Verification

Password:

S1>en
Password:
S1#sh
S1#show vl
S1#show vlan br
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Client1                          active
11   Client2                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
S1#
```

FigureIV.13: La vérification de création de VLAN dans S1.

3. Création de VLAN dans S2

Nous tapons les commandes suivantes comme la montre la figure ci-dessous :

```
User Access Verification

Password:

S2>en
Password:
S2#vla
S2#vlan d
S2#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

S2(vlan)#vl
S2(vlan)#vlan 2 name serveur
VLAN 2 modified:
    Name: serveur
S2(vlan)#vla
S2(vlan)#vlan 3 name gestion
VLAN 3 modified:
    Name: gestion
S2(vlan)#exit
APPLY completed.
Exiting....
S2#
S2#
S2#
```

Figure IV.14: Création de VLAN dans S2.

4. La vérification de création de VLAN dans S2

Nous tapons les commandes suivantes comme la montre la figure ci-dessous :

```
User Access Verification

Password:

S2>en
Password:
S2#sh
S2#show v
S2#show vb
S2#show v
S2#show vl
S2#show vlan b
S2#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    serveur                           active
3    gestion                           active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
S2#
S2#
```

Figure IV.15: La vérification de création de VLAN dans S2.

5. Création de VLAN dans le Switch fédérateur

```
Switch#vl
Switch#vlan d
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#vlan 10 name Client1
VLAN 10 added:
    Name: Client1
Switch(vlan)#vlan 11 name Client1
VLAN #10 and #11 have an identical name: Client1
APPLY failed.
Switch(vlan)#vlan 11 name Client2
VLAN 11 added:
    Name: Client2
Switch(vlan)#vlan 2 name serveur
VLAN 2 added:
    Name: serveur
Switch(vlan)#vlan 3 name gestion
VLAN 3 added:
    Name: gestion
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#sh
```

Figure IV.16: Création de VLAN dans le Switch fédérateur.

6. La vérification de création de VLAN dans le Switch fédérateur

```
Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                   Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                   Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                   Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                   Gig0/2
2    serveur                             active
3    gestion                             active
10   Client1                             active
11   Client2                             active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
11   enet  100011     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch#
```

Figure IV.17: La vérification de création de VLAN dans le Switch fédérateur.

7. Affectation des différents ports d'accès aux différents VLAN

Après la création d'un VLAN, on voit bien que tous les ports appartient au par défaut qui est le VLAN 1, donc l'étape suivante consiste à les attribuer des ports. Un port d'accès peut appartenir à un seul VLAN à la fois.

7.1. Attribution de ports aux VLAN créé dans S1

```
User Access Verification

Password:

S1>en
Password:
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f
S1(config)#interface fastEthernet 0/2
S1(config-if)#sw
S1(config-if)#switchport m
S1(config-if)#switchport mode a
S1(config-if)#switchport mode access
S1(config-if)#sw
S1(config-if)#switchport a
S1(config-if)#switchport access VL
S1(config-if)#switchport access VLan 10
S1(config-if)#exit
S1(config)#
S1(config)#interface fastEthernet 0/3
S1(config-if)#switchport mode access
S1(config-if)#switchport access VLan 11
S1(config-if)#
S1(config-if)#
```

Fig. IV.18:Attribution de ports aux VLAN créé dans S1.

7.1.1. Vérification de l'appartenance de ports aux VLAN créé dans S1

```
User Access Verification

Password:

S1>en
Password:
S1#sh
S1#show vl
S1#show vlan br
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Client1                          active    Fa0/2
11   Client2                          active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
S1#
S1#
```

FigureIV.19:Vérification de l'appartenance de ports aux VLAN créé dans S1.

7.2. Attribution de ports aux VLAN créé dans S2

```
User Access Verification

Password:

S2>en
Password:
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#in
S2(config)#interface f
S2(config)#interface fastEthernet 0/2
S2(config-if)#sw
S2(config-if)#switchport m
S2(config-if)#switchport mode a
S2(config-if)#switchport mode access
S2(config-if)#sw
S2(config-if)#switchport a
S2(config-if)#switchport access v
S2(config-if)#switchport access vlan 2
S2(config-if)#exit
S2(config)#interface fastEthernet 0/3
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit
S2(config)#
S2(config)#
```

FigureIV.20: Attribution de ports aux VLAN créé dans S2.

7.2.1. Vérification de l'appartenance de ports aux VLAN créé dans S2

```
Password:
S2#sh
S2#show v
S2#show vb
S2#show vl
S2#show vlan b
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
2    serveur                          active    Fa0/2
3    gestion                          active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
S2#
```

Figure IV.21:Vérification de l'appartenance de ports aux VLAN créé dans S2.

Etape 3 : La configuration des VLAN sur plusieurs commutate

Lorsque les VLAN sont reparties sur plusieurs commutateurs, un lien particulier est mis en place entre les commutateurs. Ce lien configuré en mode TRUNK, transmet la trame en ajoutant 4 octets indiquant le VLAN d'appartenance.

La configuration des interfaces se fait comme suit :

1. Configuration des interfaces du Switch fédérateur en mode TRUNK

Les liaisons reliées au deux Switch d'étage doivent être configuré en mode TRUNK.

```
S_Fed#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S_Fed(config)#int
S_Fed(config)#interface f
S_Fed(config)#interface fastEthernet 0/1
S_Fed(config-if)#sw
S_Fed(config-if)#switchport t
S_Fed(config-if)#switchport trunk e
S_Fed(config-if)#switchport trunk encapsulation d
S_Fed(config-if)#switchport trunk encapsulation dot1q
S_Fed(config-if)#sw
S_Fed(config-if)#switchport m
S_Fed(config-if)#switchport mode t
S_Fed(config-if)#switchport mode trunk

S_Fed(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S_Fed(config-if)#exit
S_Fed(config)#interface fastEthernet 0/2
S_Fed(config-if)#switchport trunk encapsulation dot1q
S_Fed(config-if)#switchport mode trunk
S_Fed(config-if)#exit
S_Fed(config)#
```

FigureIV.22: Création des interfaces du Switch fédérateur en mode TRUNK.

1.1.Vérification de la configuration du TRUNK

```
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
 --More--
```

Figure IV.23:Vérification de la configuration du TRUNK.

2. Configuration de l'interface dans S1 en mode TRUNK

La liaison reliée au Switch fédérateur doit être configuré en mode TRUNK.

```
User Access Verification

Password:

S1>en
Password:
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f
S1(config)#interface fastEthernet 0/1
S1(config-if)#sw
S1(config-if)#switchport m
S1(config-if)#switchport mode t
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S1(config-if)#
```

FigureIV.24: Configuration de l'interface dans S1 en mode TRUNK.

2.1.Vérification de la configuration du TRUNK

```
S1(config)#do show in
S1(config)#do show int
S1(config)#do show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
S1(config)#
S1(config)#
```

Fig. IV.25:Vérification de laconfiguration du TRUNK TRUNK.

On suit le même raisonnement pour configurer les liaisons de S2 en mode TRUNK.

Etape 4 :Affectation des adresses IP au VLAN

Si on veut pouvoir administrer un commutateur à partir d'un client Telnet sur un pc, ou bien Pour accéder à distance à lui, une adresse IP et un masque de sous-réseau doivent être configurés sur l'interface SVI :

1. Configuration des interfaces virtuelle du Switch fédérateur

La commande **interface vlan n°_du_vlan** utilisée pour la première fois crée une interface SVI appelée VLAN **n°_du_vlan.** Pour chaque création d'interface SVI, on est certain que le VLAN correspondant est présent dans la base de données des VLAN.

```
S_Fed(config)#interface vlan 10
S_Fed(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S_Fed(config-if)#ip add
S_Fed(config-if)#ip address 192.168.10.10 255.255.255.0
S_Fed(config-if)#no sh
S_Fed(config-if)#no shutdown
S_Fed(config-if)#exit
S_Fed(config)#interface vlan 11
S_Fed(config-if)#
%LINK-5-CHANGED: Interface Vlan11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up

S_Fed(config-if)#ip address 192.168.10.10 255.255.255.0
% 192.168.10.0 overlaps with Vlan10
S_Fed(config-if)#ip address 192.168.11.11 255.255.255.0
S_Fed(config-if)#no shutdown
S_Fed(config-if)#exit
S_Fed(config)#interface vlan 2
S_Fed(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

S_Fed(config-if)#ip address 192.168.2.2 255.255.255.0
S_Fed(config-if)#no shutdown
S_Fed(config-if)#exit
S_Fed(config)#interface vlan 3
S_Fed(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

S_Fed(config-if)#ip address 192.168.3.3 255.255.255.0
S_Fed(config-if)#no shutdown
S_Fed(config-if)#exit
S_Fed(config)#
```

FigureIV.26: Configuration des interfaces virtuelle du Switch fédérateur.

1.1.Vérification de création des interfaces virtuelle du Switch Fédérateur

On a qu'à consulter le fichier de configuration en cours, on tapon la commande suivante show running-config :

```
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 192.168.2.2 255.255.255.0
!
interface Vlan3
 ip address 192.168.3.3 255.255.255.0
!
interface Vlan10
 ip address 192.168.10.10 255.255.255.0
!
interface Vlan11
 ip address 192.168.11.11 255.255.255.0
```

FigureIV.27:Vérification de création des interfaces virtuelle du Switch Fédérateur.

Etape 5 : Définir une adresse IP au VLAN de Gestion

Afin de pouvoir gérer les accès Telnet, et de mieux sécuriser notre système on a affecté une adresse IP pour chaque Vlan de Gestion crée.

Le VLAN de gestion a l'objectif suivant : Gérer les Switch d'étages et le Switch fédérateur à distance par Telnet.

1. Création et attribution d'une adresse IP au VLAN de gestion

1.1. Création et attribution d'une adresse IP au VLAN de gestion dans S1 et S2

Pour pouvoir gérer les deux Switch d'étage S1 et S2 par Telnet on a créé un vlan 99 nomme Gerant et l'attribuéune adresse IP comme suit : S1 aura comme adresse 192.168.99.100, et S2 aura 192.168.99.101.

1.1.1. Pour S1

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 99
S1(config-vlan)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-vlan)#name Gerant
S1(config-vlan)#exit
S1(config)#int
S1(config)#interface vl
S1(config)#interface vlan 99
S1(config-if)#ip add
S1(config-if)#ip address 192.168.99.100 255.255.255.0
S1(config-if)#no sh
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#
```

FigureIV.28: Création etattribution des adresses IP dans S1.

1.1.2. Pour S2

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 99
S2(config-vlan)#name Gerant
S2(config-vlan)#exit
S2(config)#int
S2(config)#interface vl
S2(config)#interface vlan 99
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S2(config-if)#ip add
S2(config-if)#ip address 192.168.99.101 255.255.255.0
S2(config-if)#no sh
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#
```

FigureIV.29: Création etattribution des adresses IP dans S2.

1.2. Création et attribution d'une adresse IP au VLAN de gestion dans le fédérateur

```
S_Fed#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S_Fed(config)#vlan 99
S_Fed(config-vlan)#name Gerant
S_Fed(config-vlan)#exit
S_Fed(config)#int
S_Fed(config)#interface vl
S_Fed(config)#interface vlan 99
S_Fed(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S_Fed(config-if)#ip add
S_Fed(config-if)#ip address 192.168.99.99 255.255.255.0
S_Fed(config-if)#no sh
S_Fed(config-if)#no shutdown
S_Fed(config-if)#exit
S_Fed(config)#
```

FigureIV.30: Création etattribution des adresses IP dans le fédérateur.

Pour que les clients puissent accéder au Switch fédérateur par Telnet, on doit rajouter une commande dans les Switch d'étagesqui est IP Default-Gateway 192.168.99.99.

Etape 6 : Test de connexion et d'accès

1. Ping du user de VLAN 11 au user de VLAN 10

```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=1ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

FigureIV.31:Résultat de la commande « Ping ».

2. Accès Telnet de user au Switch d'étage

```
PC>telnet 192.168.99.100
Trying 192.168.99.100 ...Open


User Access Verification

Password:
S10>exit

[Connection to 192.168.99.100 closed by foreign host]
PC>
PC>
PC>
PC>
PC>
PC>
PC>telnet 192.168.99.100
Trying 192.168.99.100 ...Open


User Access Verification

Password:
S1>en
Password:
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
```

FigureIV.32:Résultat de la commande « Telnet ».

3. Accès Telnet de user au Switch Fédérateur

```
PC>
PC>
PC>
PC>
PC>
PC>
PC>telnet 192.168.99.99
Trying 192.168.99.99 ...Open


User Access Verification

Password:
S_Fed>en
Password:
S_Fed#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S_Fed(config)#
S_Fed(config)#
S_Fed(config)#
S_Fed(config)#
```

FigureIV.33:Résultat de la commande « Telnet ».

Etape 7 : Sécurisation des Switch

Afin de sécuriser et de filtrer ou d'autoriser le trafic sur ce réseau on a décidé de mettre en œuvre des listes de contrôle d'accès.

L'entreprise ENIEM est composée de plusieurs départements, mais le département informatique va être le gestionnaire, en s'occupant de configurations des Switch, dans d'autres terme c'est lui qui aura l'autorisation d'accéder à tous les Switch ainsi que auratous les privilèges d'accéder aux autres utilisateurs.

1. Filtrer les accès Telnet dans S1 et S2

On va définir des Listes de Contrôle d'Accès dans S1 de telle sorte à empêcher tous les accès Telnet des utilisateurs sauf les utilisateurs du département informatique.

```
S1#
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)#
S1(config)#line v
S1(config)#line vty 0 4
S1(config-line)#acc
S1(config-line)#access-class 21 in
S1(config-line)#pass
S1(config-line)#password amar
S1(config-line)#log
S1(config-line)#logi
S1(config-line)#login
S1(config-line)#t
S1(config-line)#transport i
S1(config-line)#transport input t
S1(config-line)#transport input telnet
S1(config-line)#exit
S1(config)#acce
S1(config)#access-list 21 per
S1(config)#access-list 21 permit 192.168.3.0 0.0.0.255
S1(config)#acc
S1(config)#access-list 21 den
S1(config)#access-list 21 deny an
S1(config)#access-list 21 deny any
S1(config)#exit
S1#
```

FigureIV.34:Définir les ACL dans S1.

```
User Access Verification

Password:
Password:

S2>en
Password:
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#
S2(config)#
S2(config)#
S2(config)#line v
S2(config)#line vty 0 4
S2(config-line)#acc
S2(config-line)#access-class 21 in
S2(config-line)#
S2(config-line)#pas
S2(config-line)#password amar
S2(config-line)#t
S2(config-line)#transport i
S2(config-line)#transport input t
S2(config-line)#transport input telnet
S2(config-line)#logi
S2(config-line)#login
S2(config-line)#exit
S2(config)#acc
S2(config)#access-list 21 per
S2(config)#access-list 21 permit 192.168.3.0 0.0.0.255
S2(config)#ac
S2(config)#access-list 21 den
S2(config)#access-list 21 deny an
S2(config)#access-list 21 deny any
S2(config)#
```

FigureIV.35:Définir les ACL dans S2.

2. Filtrer le trafic ICMP « Ping »

Pour éviter que les utilisateurs se communiquent entre eux, on a défini des listes de contrôle d'accès sur le Switch fédérateur, et on a essayé de donner un exemple de ce filtrage de bloquer toutes les commande ICMP, sauf celles des utilisateurs du département informatique.

2.1.Définir des ACL

```
S_Fed>en
S_Fed#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S_Fed(config)#
S_Fed(config)#access-list 102 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255
```

FigureIV.36:Définition des ACL.

2.2.Application des ACL sur les interfaces

Une fois s'est défini ainsi, je vais appliquer des Access List sur les interfaces

```
S_Fed(config)#int
S_Fed(config)#interface f
S_Fed(config)#interface fastEthernet 0/1
S_Fed(config-if)#ip acc
S_Fed(config-if)#ip access-group 102 in
S_Fed(config-if)#exit
S_Fed(config)#
```

FigureIV.37: Application des ACL sur les interfaces.

Etape 8 : Test de connexion et d'accès par les VLAN après la création des ACL

1. Ping du user de VLAN 11 au user de VLAN 10

```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.11.11: Destination host unreachable.
Reply from 192.168.11.11: Destination host unreachable.
Reply from 192.168.11.11: Destination host unreachable.
Reply from 192.168.11.11: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.11.11: Destination host unreachable.
Reply from 192.168.11.11: Destination host unreachable.
Reply from 192.168.11.11: Destination host unreachable.
Reply from 192.168.11.11: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

FigureIV.38:Résultat de la commande « Ping ».

2. Accès Telnet de user au Switch d'étage

```
PC>telnet 192.168.99.100
Trying 192.168.99.100 ...Open

[Connection to 192.168.99.100 closed by foreign host]
PC>telnet 192.168.99.100
Trying 192.168.99.100 ...Open

[Connection to 192.168.99.100 closed by foreign host]
PC>telnet 192.168.99.100
Trying 192.168.99.100 ...Open

[Connection to 192.168.99.100 closed by foreign host]
PC>telnet 192.168.99.100
Trying 192.168.99.100 ...Open

[Connection to 192.168.99.100 closed by foreign host]
PC>
```

FigureIV.39:Résultat de la commande « Telnet ».

3. Accès Telnet de user au Switch Fédérateur

```
PC>telnet 192.168.99.99
Trying 192.168.99.99 ...
% Connection refused by remote host
PC>telnet 192.168.99.99
Trying 192.168.99.99 ...
% Connection refused by remote host
PC>telnet 192.168.99.99
Trying 192.168.99.99 ...
% Connection refused by remote host
PC>
```

FigureIV.40:Résultat de la commande « Telnet ».

Etape 9 : Test de connexion et d'accès du département informatique après la création des ACL

On avait dit précédemment que les utilisateurs du département informatique a tous les privilèges dans le réseau.

1. Ping du user de département informatique au user de VLAN 10

```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127
Reply from 192.168.10.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

FigureIV.41:Résultat de la commande « Ping ».

2. Ping du user de département informatique au user de VLAN 11

```
PC>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=0ms TTL=127
Reply from 192.168.11.1: bytes=32 time=0ms TTL=127
Reply from 192.168.11.1: bytes=32 time=1ms TTL=127
Reply from 192.168.11.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=0ms TTL=127
Reply from 192.168.11.1: bytes=32 time=1ms TTL=127
Reply from 192.168.11.1: bytes=32 time=0ms TTL=127
Reply from 192.168.11.1: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

FigureIV.42:Résultat de la commande « Ping ».

3. Accès Telnet de user du département informatique au Switch d'étage

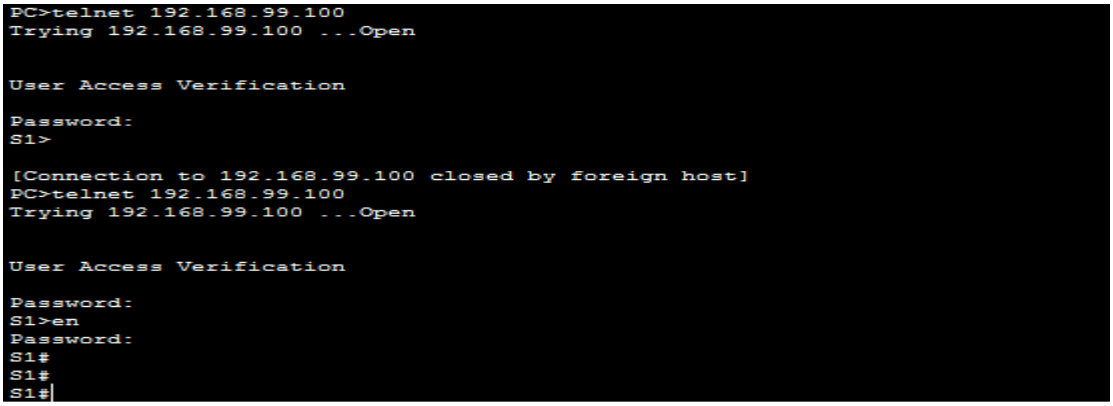


Fig. IV.43:Résultat de la commande « Telnet ».

4. Accès Telnet de user du département informatique au Switch Fédérateur

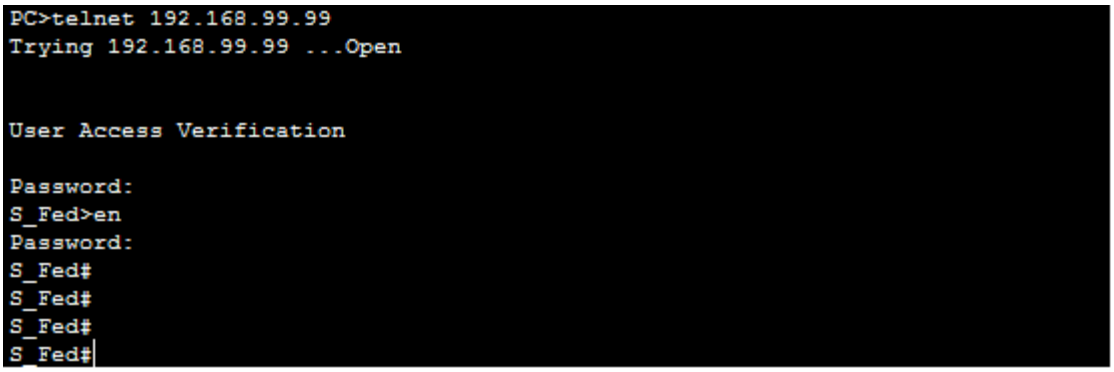


Fig. IV.44:Résultat de la commande « Telnet ».

Etape 10 : Installation et configuration du serveur Exchange 2007

L'installation du serveur de messagerie Exchange exige des prérequis.

1. Installation des prérequis et préparation d'Active Directory

La première solution est d'installer manuellement les différents rôles, configurer Active directory (Voir Annexe B), promouvoir le serveur en contrôleur de domaine, installer WEB IIS (Voir Annexe C), installer Microsoft Framework (Voir Annexe C) … Pour vérifier et installer les prérequis nous avons le choix de les ajouter au serveur via le gestionnaire de serveur ou bien via l'interpréteur de commande Power Shell.

2. Installation de Microsoft Exchange Server 2007

L'ensemble des étapes d'installation de l'Exchange sont détaillées dans l'annexe C.

3. Configuration de Microsoft Exchange 2007

3.1 .Configuration des bases de données

3.1. 1. Création d'une base de données

Lors de son installation, Exchange crée automatiquement une base de données par défaut.

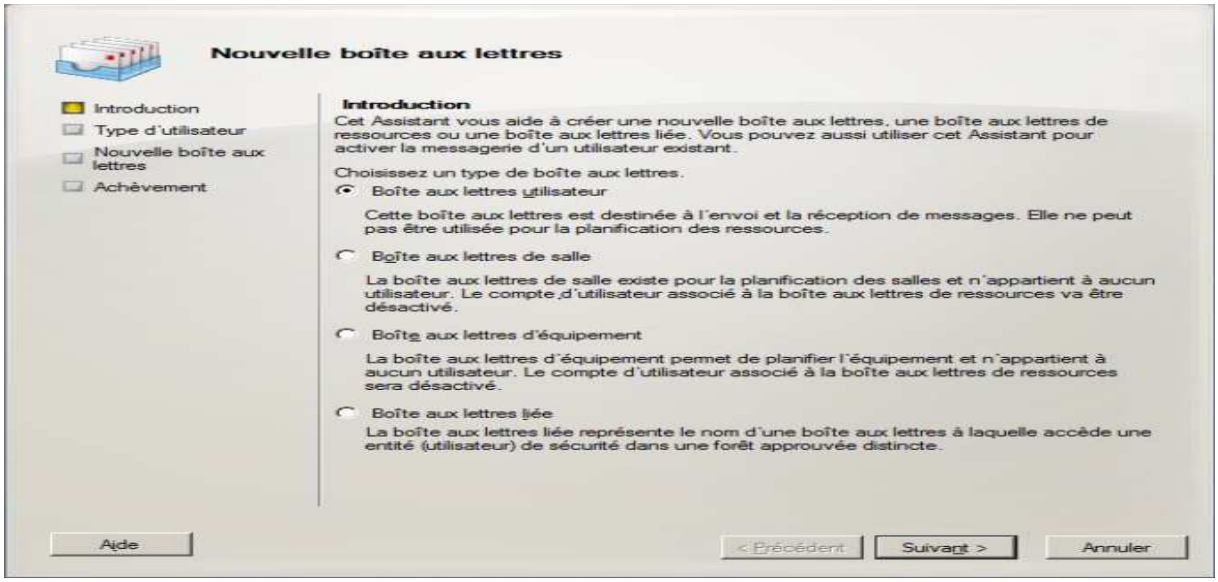
Néanmoins nous pouvons créer une nouvelle, pour la sécurité de notre système, depuis la console, Configuration de l'organisation=> boite aux lettres=> Nouvelle base de données de boite aux lettres. Puis nous indiquons le nom de la base de données ainsi que le serveur Exchange qui l'héberge.

3.1. 2. Création d'un compte de messagerie utilisateur

Il existe différents types de boites aux lettres :

- **Boite aux lettres utilisateur** : boite classique pour un utilisateur.
- **Boite aux lettres d'équipements** : permet de réserver des équipements.
- **Boite aux lettres de salle** : permet de réserver des salles de réunion.
- **Boite aux lettres liée** : permet d'associer une adresse mail avec un compte situé par exemple dans une forêt différente.

Pour créer un compte de messagerie on utilise les boites aux lettres utilisateurs. Pour ce faire, Configuration de destinataire ==> Boite aux lettres ==> nouvelle boite aux lettres.



FigureIV.45: Création de boite aux lettres utilisateur.

L'étape suivante, nous permet de sélectionner les utilisateurs existants ou de créer des nouveaux utilisateurs.

Fig. IV.46: Création de nouveaux utilisateurs

III. Conclusion

Dans ce chapitre, nous avons abordé les différents techniques et concepts qui sont indispensables dans les réseaux. On a également cité les contraintes et les failles ainsi que les problèmesfréquemment rencontré dans ce domaine puis, nous avons proposé notre solution afin de bien gérer notre réseau.

Conclusion Générale

Ce présent projet est élaboré dans le cadre d'un projet de fin d'études pourL'obtention du diplôme master Académique en Réseaux Mobilité et Systèmes Embarquée dont le stage pratique a été effectuée au sein de l'entreprise ENIEM.
Le travail qui nous a été confié consiste a :

- ✓ la conception et la réalisation de l'architecture physique du réseauinformatique de l'ENIEM.
- ✓ la configuration des services réseau de base (DNS, partagede la connexion à Internet, messagerie électronique, ….) ;
- ✓ l'implantation de quelques mécanismes assurant la sécurité.

Ce projet, nous a fait découvrir le monde de l'entreprise et nous a appris énormément dechoses. En effet, les réseaux informatiques au sens large font référence à de nombreusesnotions plus ou moins complexes. On a donc eu l'occasion au cours de ce stage de pouvoir
aborder de nombreux sujets. Et on a pris conscience de la complexité des réseaux informatiques et surtout de la sécurité réseaux.

Espérons qu'on va bénéficier de cette étude, pour l'appliquer dans la vieprofessionnelle, et valoriser l'ensemble de nos connaissances, et pas juste celles acquises pendant ce projet, mais aussi celles récoltées durant tout mon cursus universitaire.

ACL : Liste Contrôle Accès ;

AD DS: Active Directory Domain Services ;

AFAQ : Association Française Assurance Qualité ;

CAM : Complexe Appareils Ménagers ;

CFC: Chlora Fluora Carbones ;

CFC: Chlora Fluora Carbones ;

DDP : Panneau de Distribution Direct ;

DNS: Domain Name System;

DOS: Denial Of Service;

DTC: Data Terminal Circuit ;

ENIEM : Entreprise Nationale Industries Electroménager ;

EPE : Entreprise Publique Economique ;

FTP: FileTransfer Protocol ;

Http: Hyper Text Transfer Protocol;

IP: Internet Protocol;

ISO: International Standardisation Organisation , Open Systems Interconnections;

LAN : Local Area Network;

MDP : Panneau de Distribution Modem;

MAC: Media Access Control;

POP: Point of Presence;

SAV : Service Après-vente ;

SDSI : Service Développement Systèmes Informatiques ;

SEI : Service Exploitation Informatique ;

SPA : Société Par Actions ;

TCP: Transmission Control Protocol ;

U CUIS : Unité Cuisson ;

UCL : Unité Climatisation ;

UC : Unité Commerciale ;

UDP: User Datagram Protocol ;

UF : Unité Froid ;

ULM : Unité Lampe Mohammedia ;

UPT : Unité Présentation Techniques ;

USM : Unité **S**anitaire **M**ELIANA ;

VPN: Virtual Private Network = **RPV:** Réseau Privé Virtuel ;

VLAN: Virtual Local Area Network;

WAN: Wide Area Network.

Liste des figures

CHAPITRE I

CHAPITRE II

Liste des figures

CHAPITRE III

CHAPITRE IV

Liste des figures

Liste des figures

ANNEXE A

ANNEXE B

ANNEXE C

Chapitre I

Chapitre II

Chapitre IV

Les Livers

- Misc n°10 November December 2003.
- Les réseaux d'entreprises par la pratique, Luc Montagnier.
- Cours réseaux et télécoms, G.Pujolle.

Les sites Internet

- www.guill.net **:** site de cours en réseaux informatiques.
- www.zdnet.fr
- www.cisco.fr
- www.01net.com
- solutions.journaldunet.com
- www.francetelecom.com
- www.urec.cnrs.fr
- www.Supinfo-Projects.com
- www.securiteinfo.com
- www.commentcamarche.com
- www.editions-eyrolles.com/les réseau édition 2008.
- www.frameip.com/ipsec.
- www.securiteinfo.com

A.GNS3

Créer un répertoire GNS3 sur le bureau de votre PC➔ mettre l'IOS décompressé et l'application GNS3.

A.1.Installation de GNS3

GNS3 est téléchargeable depuis le site officiel de GNS3. La version téléchargerest. GNS3v0.8.4 all-in-one. Son installation est une succession de terme suivant.

A.2.L'ajout et configuration des IOS

Edit ➔ IOS image and Hypervisor

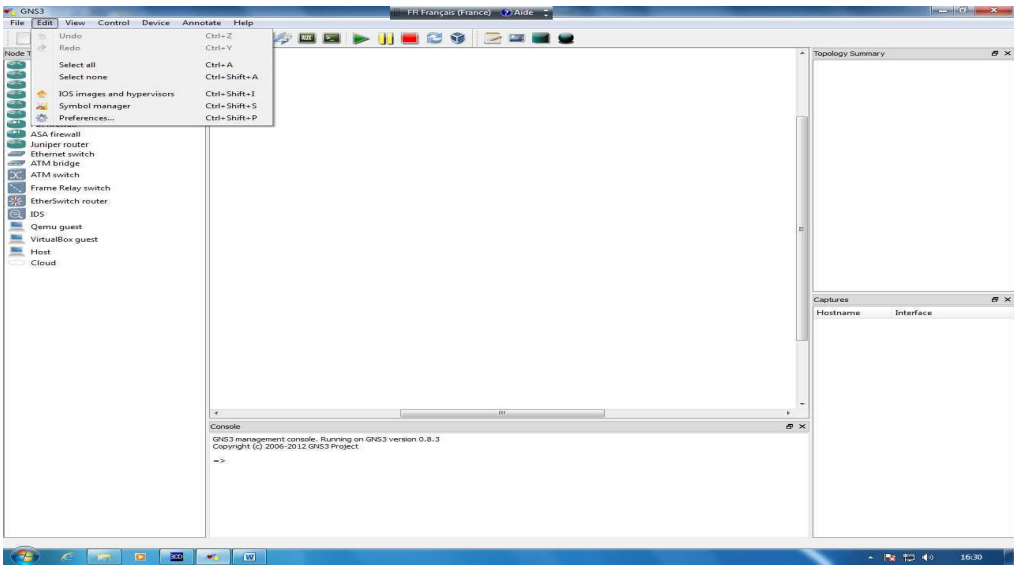


Figure A.1:L'ajout des IOS

L'IOS étant le système d'exploitation des équipements Cisco, il les gère en se basant sur l'architecture matérielle. Avant de configurer les IOS, il faut les télécharger. Apres le téléchargement, l'étape suivante consiste à lier l'IOS à son modèle d'équipement.

A.3. Sélectionner l'imageIOS

Cliquer sur le bouton face à "Image file" et sélectionnons l'IOS depuis son emplacement, puis choisissons l'IOS (décompressé) et cliquons sur bouton<<Ouvrir>>

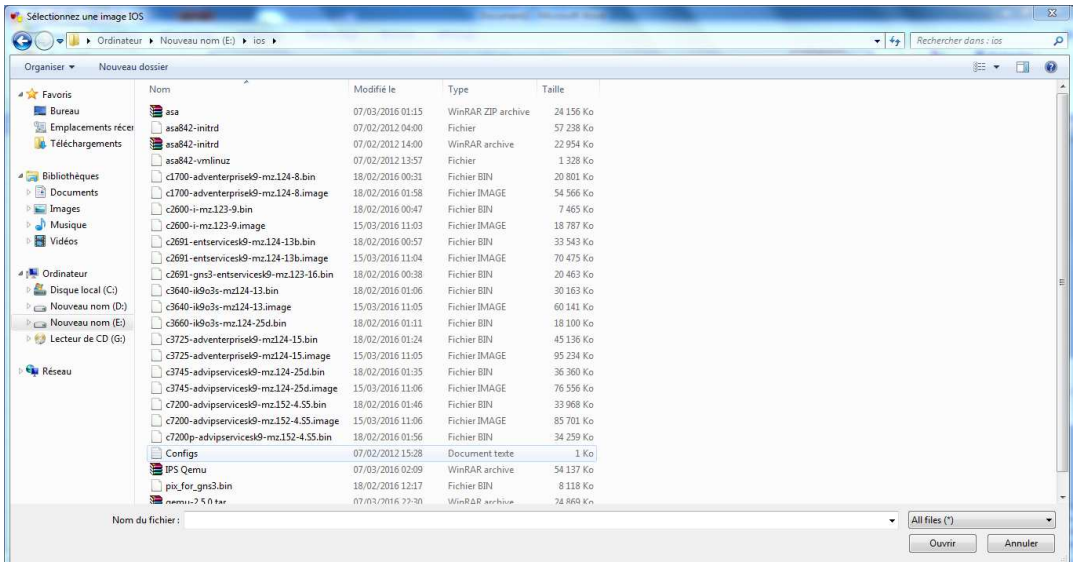


Figure A.2: La sélection de l'image IOS depuis son emplacement.

On a la possibilité de modifier la capacité mémoire des Switch émulés de 128 ==> 256 MB etModifions le contenu des champs <<DefaultRAM>>

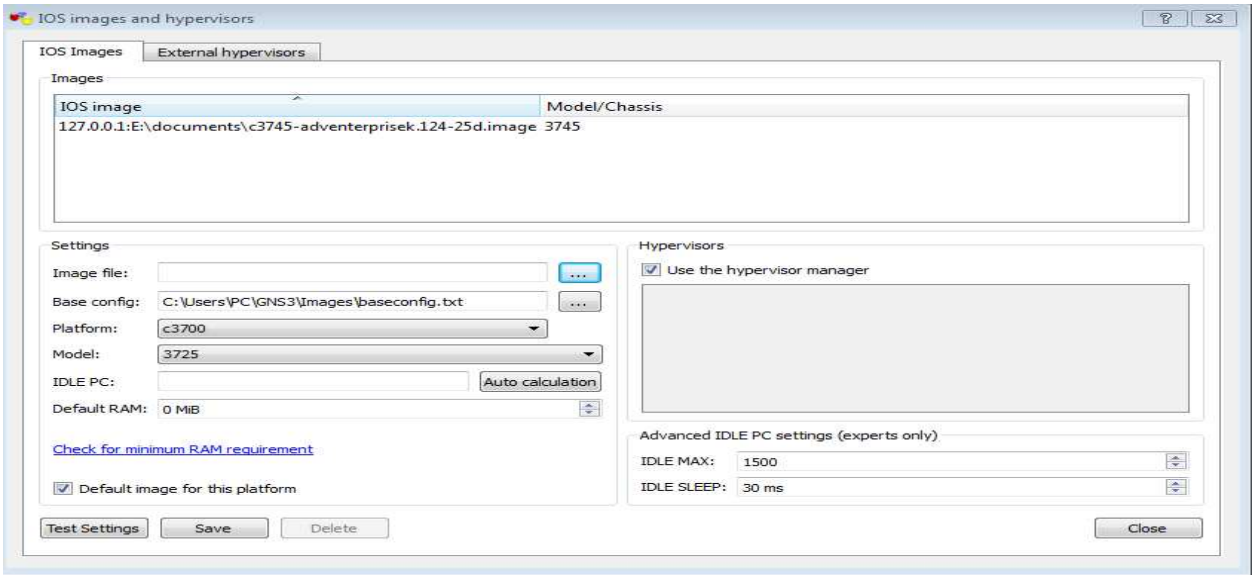


Figure A.3: Modifier la capacité mémoire des SWITH

Enfin sauvegardons en Cliquant sur Save puis Close.

Apres cliquons sur :

Edit ➔ Préférence

Cliquer sur le bouton <<Dynamips>>

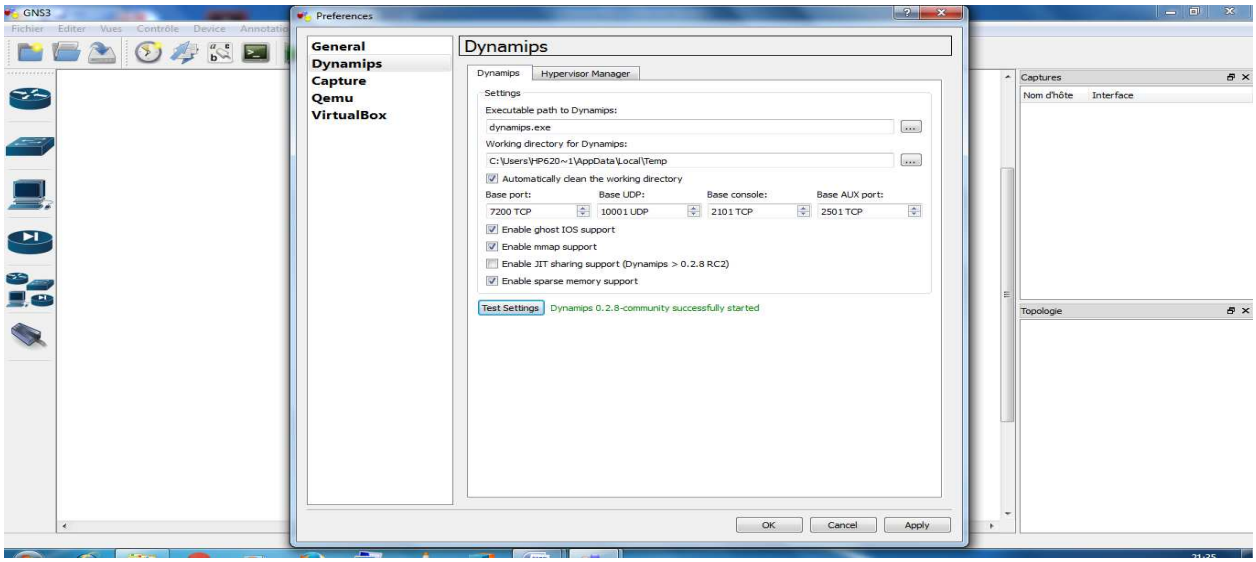


Figure A.4: Tester les paramètres recommandés.

Cliquer sur le bouton **<<Test Settings>>,** au bout de quelques secondes on doit voir le message en vert <<Dynamips 0.2.8-comunity successfullystarted>>.

A.4. Optimisation de l'utilisation des ressources CPU

GNS3 consommant les ressources matérielles, la CPU du PC utilisé peut atteindre des sommets comme ci-dessous.

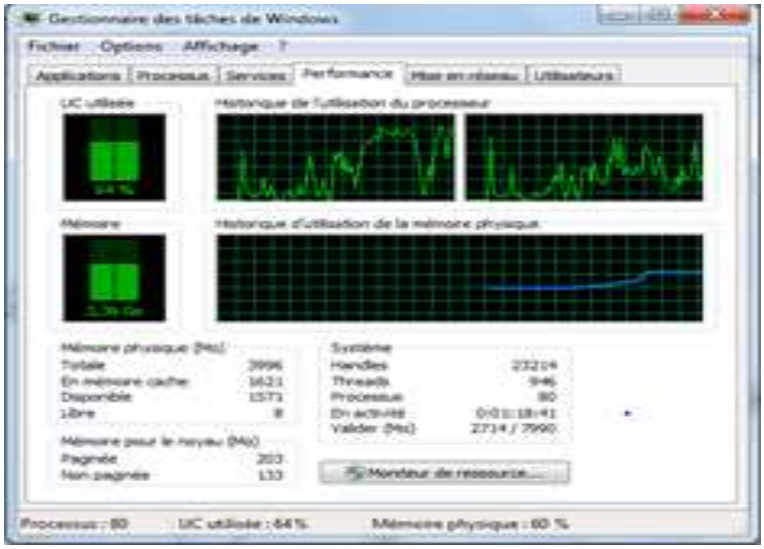


Figure A.5: Gestionnaire des taches de Windows.

Pour baisser cette charge, il suffit de lancer la fonction Idle PC**,** pour ce faire un clic droit sur le SWITCH Fédérateur et sélectionnonsIdle PC. Une fenêtre temporaire apparait le temps de calculer idle value, puis s'affiche un menu déroulantavce une ou plusieurs valeurs différentes de l'idle value. Il faut choisir la valeur ayant une étoile, si y'on n'a pas

on sélectionne la première valeur. Ainsi que le lancement de la fonction Idle PCpeut être lancée sur un seul SWITCH Fédérateur allumé et la valeur sélectionnée s'appliquera à tous les autres SWITCH Fédérateur.

L'utilisation de la CPU devrait revenir à niveau raisonnable (quelques %) si nonrelancer la fonction Idle PC.

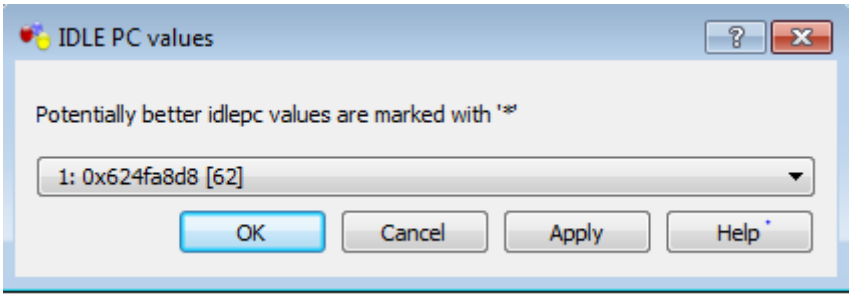


Figure A.6: Gestionnaire des taches de Windows.

A.5. La connexion entre la carte réseau d'une machine virtuelle à un SWITCH.

A.5.1. La procédure

Ajoutons un Cloud (nuage) dans l'espace de travail en choisissant (Change Symbol), il est possible de le transformer en un autre équipement (une machine) et le connecter par un câble avec une interface du SWITCH. Celle-ci connecté, elle représente la carte réseau qui peut être configurée avec les paramètres IP pour une connexion logique à l'interface du SWITCH.

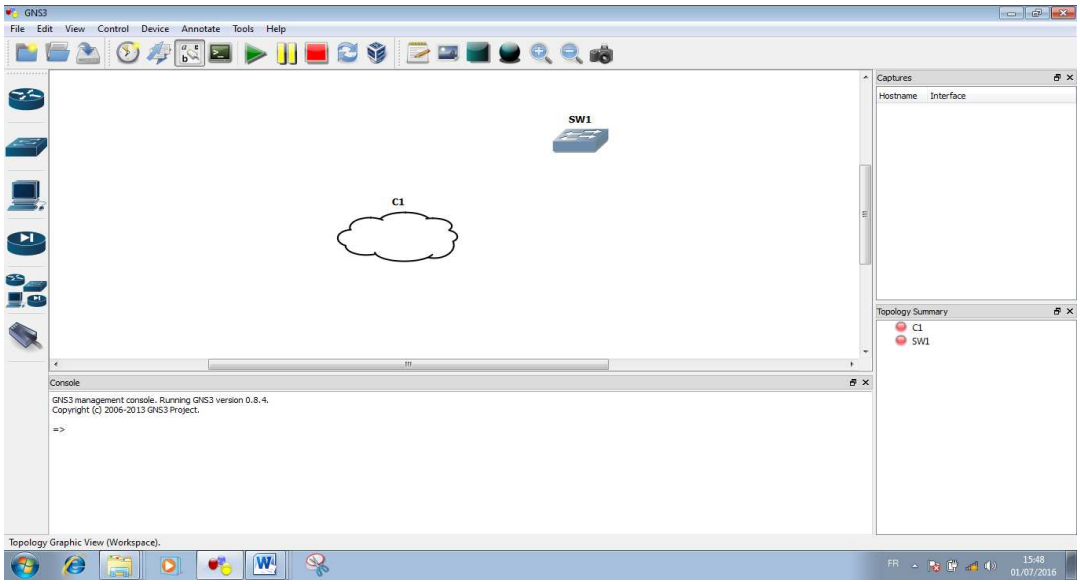


Figure A.7: La configuration du nuage.

En cliquant sur le bouton droit sur le nuage et puis sur configurer.

Lors de la configuration de la machine, la fenêtre Nodeconfigurator apparait. Elle liste les différentes cartes dont dispose la machine physique. Apres la sélection de la carte réseau voulue, il suffit de l'ajouter.

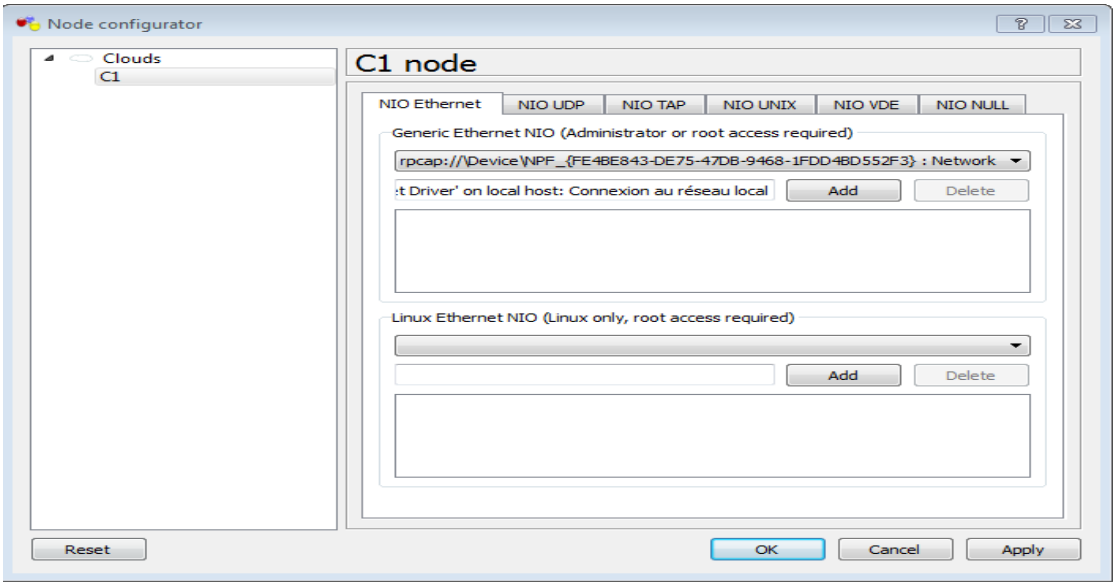


Figure A.8: Le choix de la carte réseau.

B.1. Présentation d'Active Directory

Active Directory est le nom du service annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire Active Directory est basé sur les standards TCP/IP, DNS,…….

Il doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone,….) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données,... Il permet de recenser tourtes les informations concernant le réseau, que ce soit les utilisateurs, les machines, ou les applications. Ainsi il constitue le noyau central de toute l'architecture réseau et a vocation à permettre à un utilisateur de retrouver et d'accéder à n'importe quelle ressource identifiée par ce service.

Active Directory est donc un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources te des droits associés, il constitue également un outil d'administration et de gestion de réseau. Il fournit à ce titre des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise.

Figure.B.1 : Active Directory

B.2. La structure d'Active Directory

B.2.1. Sites et Domaines

- ✓ **Sites :** Sites et services Active Directory procure une vue du conteneur Services, que vous pouvez utiliser pour afficher les objets liés aux services publiés dans les services AD DS (Active Directory Domain Services).

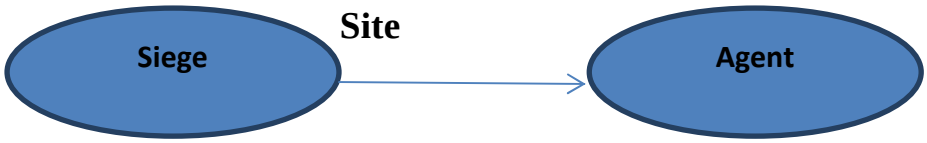


Figure.B.2 : Site

- ✓ **Domaine (ou sous-domaine) :** Le domaine au sens de l'AD est le niveau le plus bas. Il contient au moins un contrôleur de domaine (Ldap + Kerberos).

Il représente une organisation ou une partie d'une organisation.

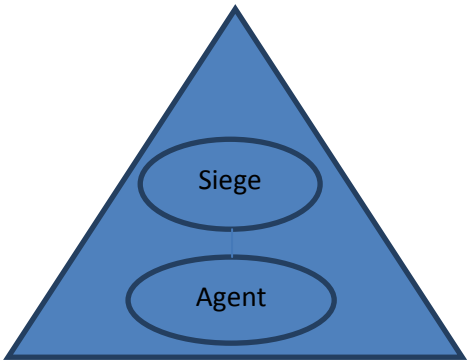


Figure.B.2 : Domaine

B.2.2. Arborescences et forêts

- ✓ **Arborescence :** Ensemble d'un domaine et de tous ses sous-domaines.
- ✓ **Forêt :** Ensemble d'arborescences qui appartient à la même organisation.

Au choix de l'architecte réseau, deux arborescences peuvent appartenir à une même forêt ou pas.

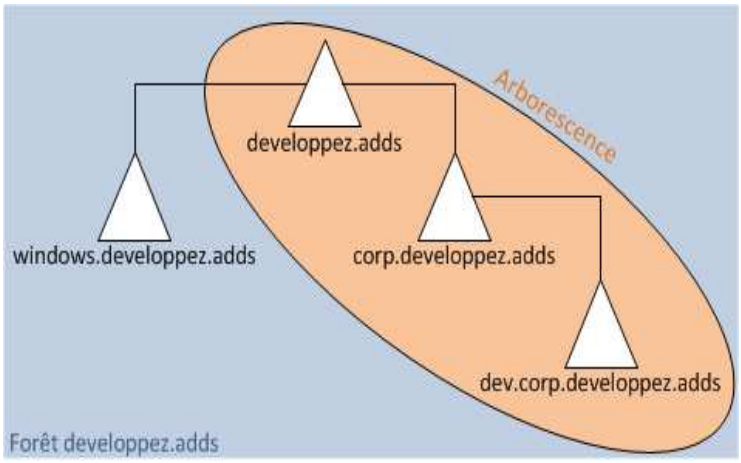


Fig.B.2 : Arborescences et forêts

B.2.3. Utilisateurs et ordinateurs

Chaque utilisateur dans Active Directory est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénom, login, adresse e-mail, téléphone, département,….). Cesattributs peuvent permettre de trouver des utilisateurs dans le domaine. Ils peuvent par exemple être utilisés dans Exchange pour constituer des listes dynamiques de distribution d'e-mails. Ces utilisateurs peuvent se voir attribuer des autorisations sur d'autres objets d'Active Directory. Lorsqu'il y a plusieurs utilisateurs, il est possible de les gérer par groupe.

Les ordinateurs disposent également de comptes spécifiques dans Active Directory. Ces comptes existent pour gérer la sécurité pour les accès à certaines ressources comme les stratégies de groupe, les login par exemple. On pourra également gérer les ordinateurs par groupe.

B.2.4. Groupes

Il existe deux types de groupes,le premier est le plus courant est le groupe de sécurité et le deuxième type est le groupe de distribution.

- **Le groupe de sécurité** : permet de gérer la sécurité pour l'accès et l'utilisation des ressources de réseau.
- **Le groupe de distribution** : permet simplement de gérer des listes de distribution d'e-mails dans un serveur de messagerie.

Pour ces groups il existe trois étendues :

- ✓ **Domaine local** : il est possible d'ajouter des comptes de n'importe quel domaine et/ou des groupes « Domaine local » du même domaine et/ou des groupes universelle/globaux de n'importe quel domaine. Les autorisations portent uniquement sur le domaine auquel le groupe appartient.
- ✓ **Globale** : il est possible d'ajouter des comptes du domaine d'appartenance et/ou des groupes globaux du domaine d'appartenance. Les autorisations peuvent être accorde dans n'importe quel domaine.
- ✓ **Universelle** : il est possible d'ajouter des comptes de n'importe quel domaine et/ou des groupes globaux et universels de n'importe quel domaine. Les autorisations pour cette étendue portent sur tout le contenu de la forêt.

B.2.4. DNS

Le DNS est la base d'Active Directory. C'est grâce au DNS que les postes utilisateurs ou serveurs membres du domaine peuvent trouver le ou les serveur(s) Active Directory. Pour trouver le serveur Active Directory, les utilisateurs vont demander au DNS l'enregistrement de type SRV ayant pour nom _ldap._tcp.developpez.adds (ou développez est le nom de domaine). Cet enregistrement SRV contient le nom du serveur qui possède l'annuaire ainsi que le port TCP à utiliser pour accéder à ce serveur en LDAP. Une requête DNS supplémentaire sera effectuée pour connaitre l'IP du serveur en question. Une fois le client saura quel serveur contacter, il pourra avoir accès (à condition d'avoir des identifiants) aux différentes ressources proposés grâce à l'Active Directory, comme partage de fichier et imprimantes, messagerie,….il est donc important pour l'architecture d'avoir un service DNS qui fonctionne correctement. Généralement, on utilise le serveur DNS fourni avec Windows Server et la plupart de temps, placer le serveur DNS sur le serveur Active Directory.

B.3. Installation d'Active Directory

Lancer la commande **DCPROMO** afin de démarrer l'assistant d'installation.

Figure.B.3 : Lancement de l'assistant d'installation d'Active Directory.

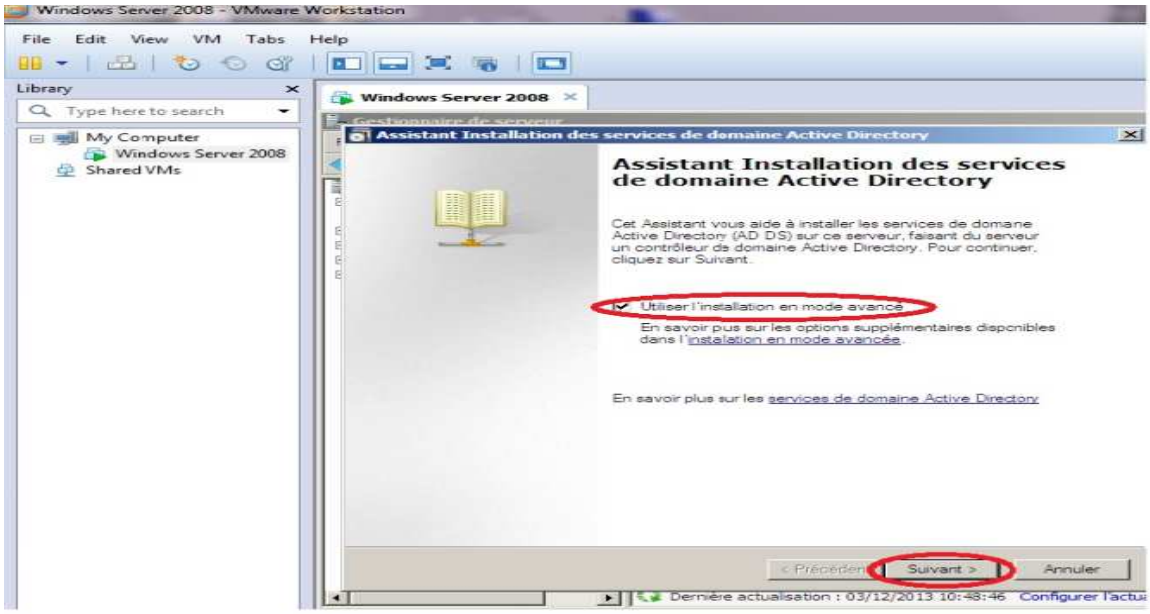


Figure.B.4: Mode d'installation d'Active Directory.

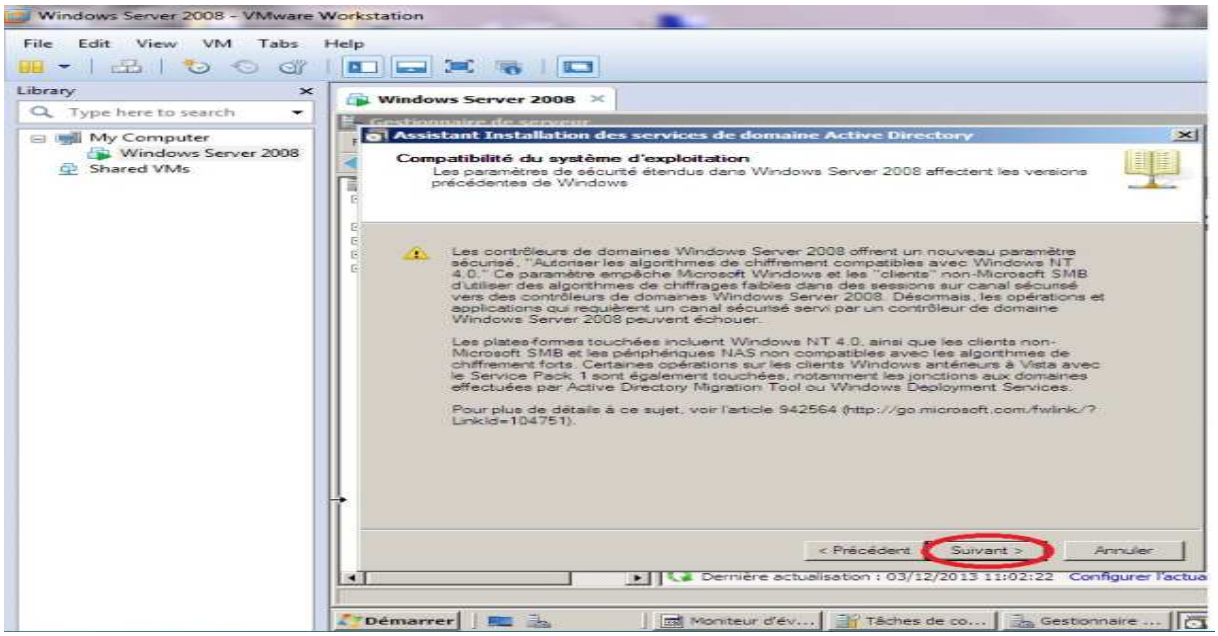


Figure.B.5 : Compatibilité des systèmes d'exploitation clients.

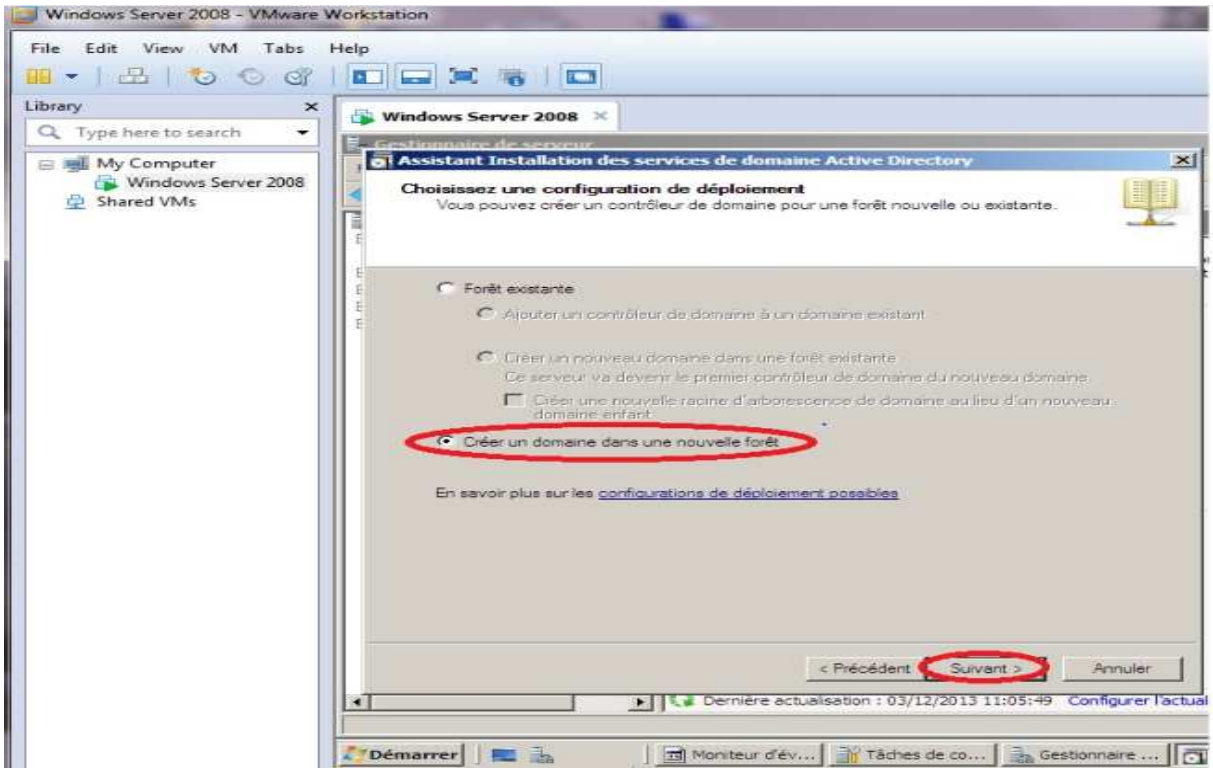


Figure.B.6 : Création du premier domaine dans une nouvelle forêt.

Le nom de mon domaine est eniem.local

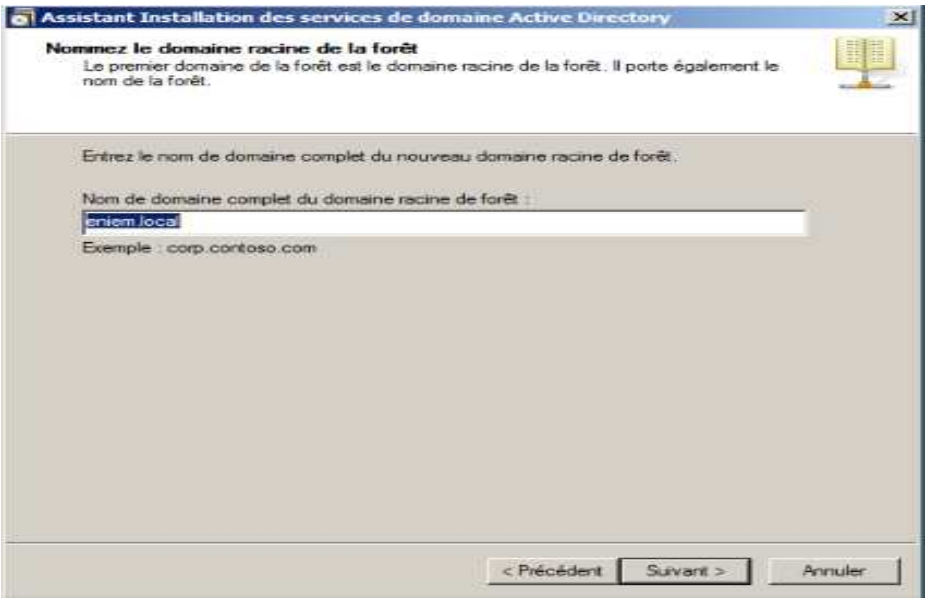


Figure.B.7 : Attribution d'un nom à mon nouveau domaine.

Le nom **NetBIOS** correspond généralement au nom **DNS.**

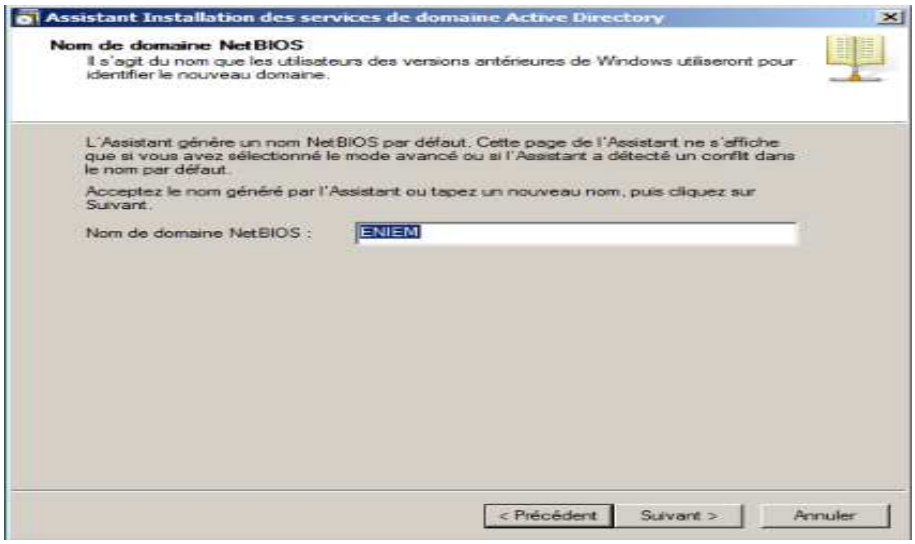


Figure.B.8 : Attribution d'un nom au DNS.

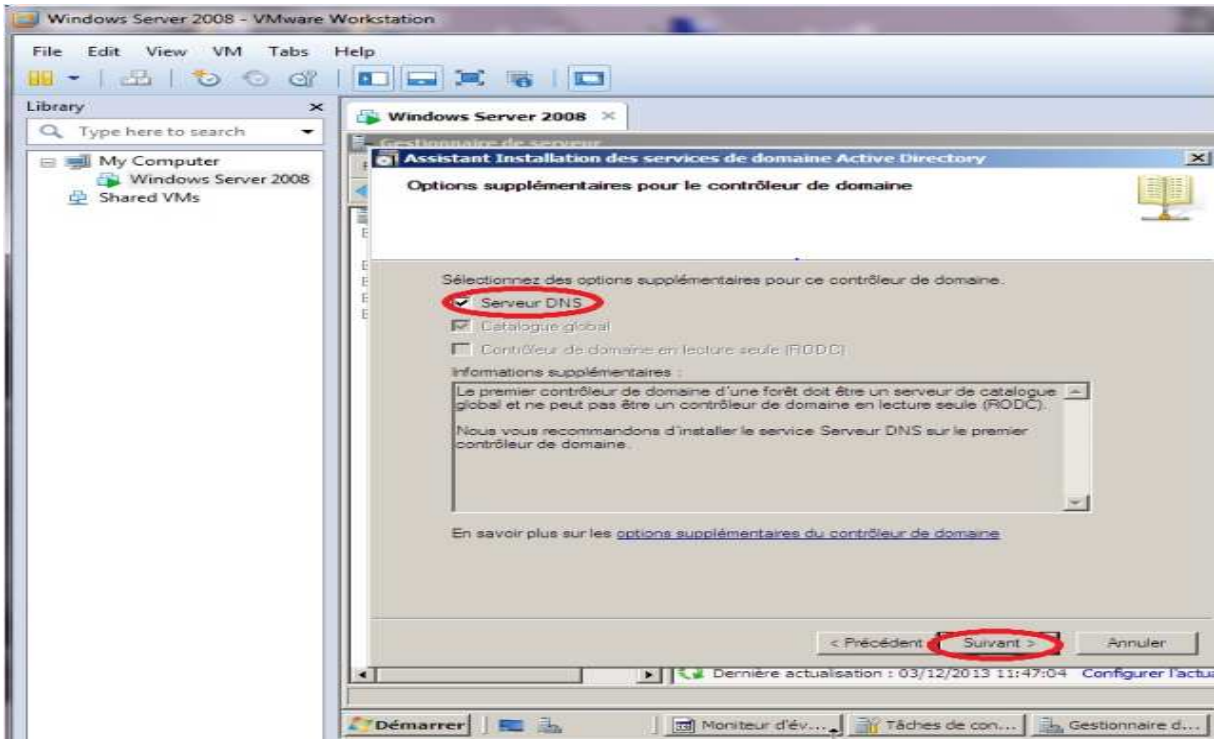


Figure.B.9 : Installation de DNS.

Ensuite donnons le chemin de la base de données et du journal Active Directory. Microsoft préconise des disques durs différents pour des raisons de performances et de meilleure récupération.

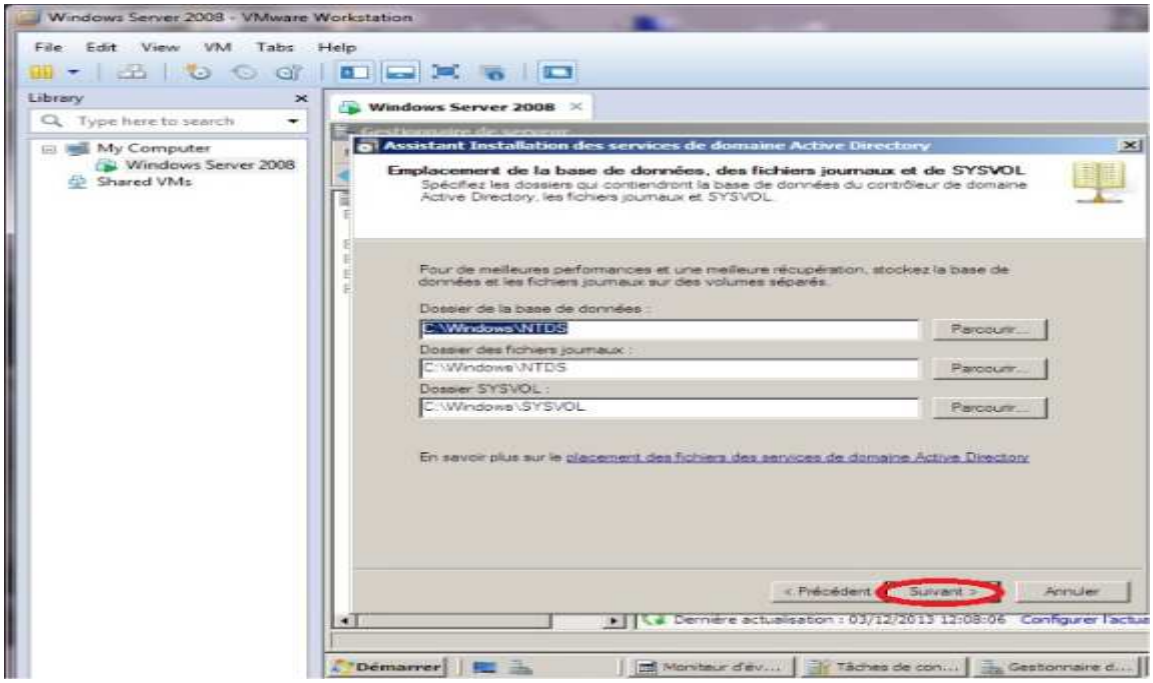


Figure.B.10 : Emplacements des données.

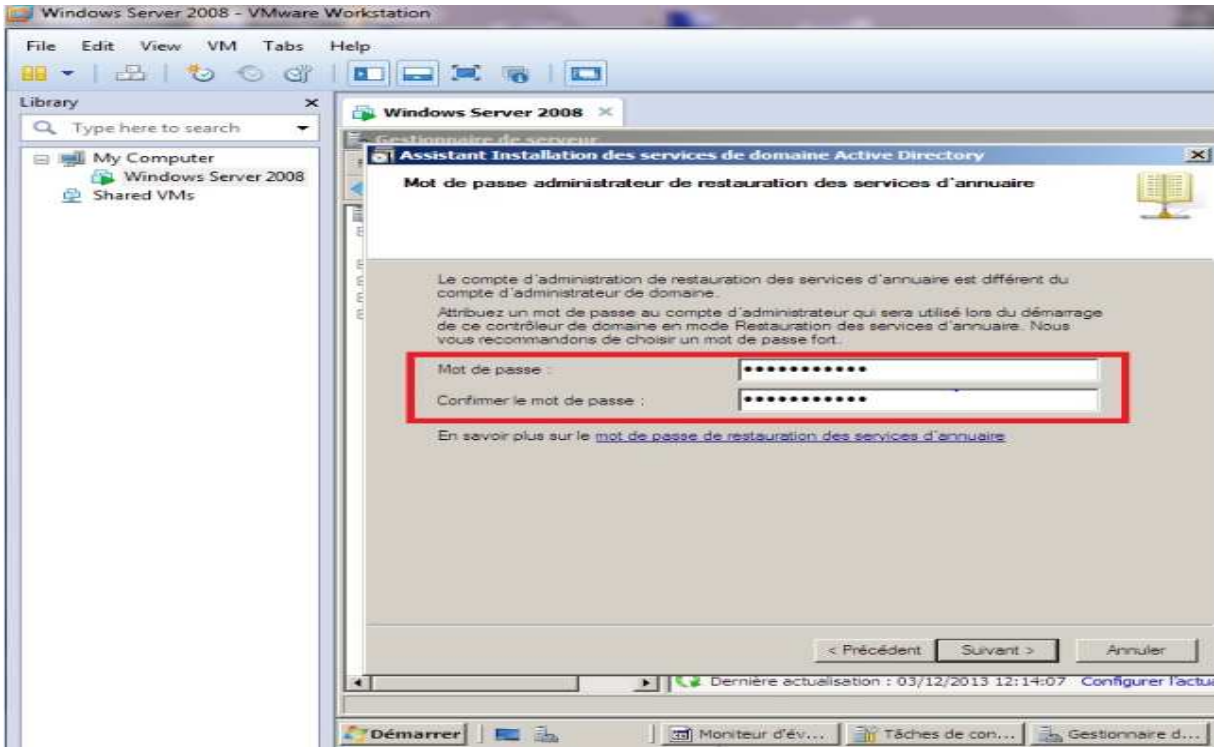


Figure.B.11 : Mot de passe administrateur.

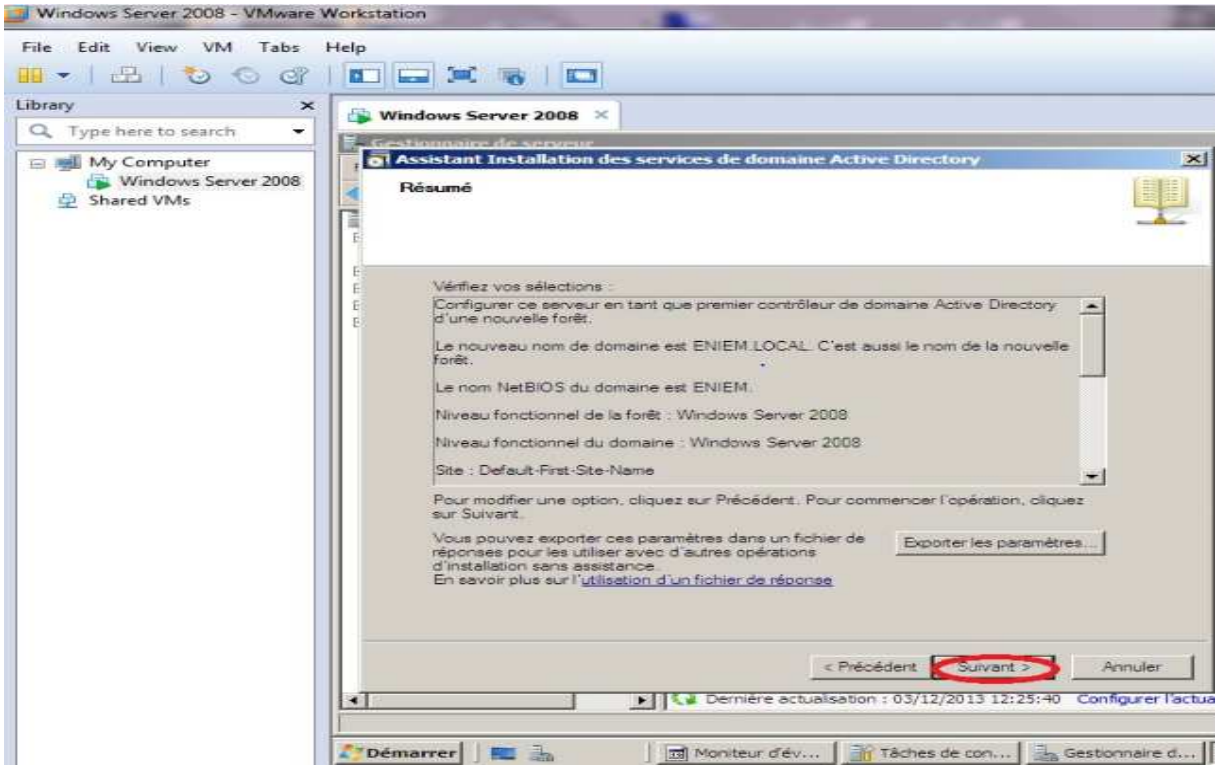


Fig.B.12 : Affichage du résumé.

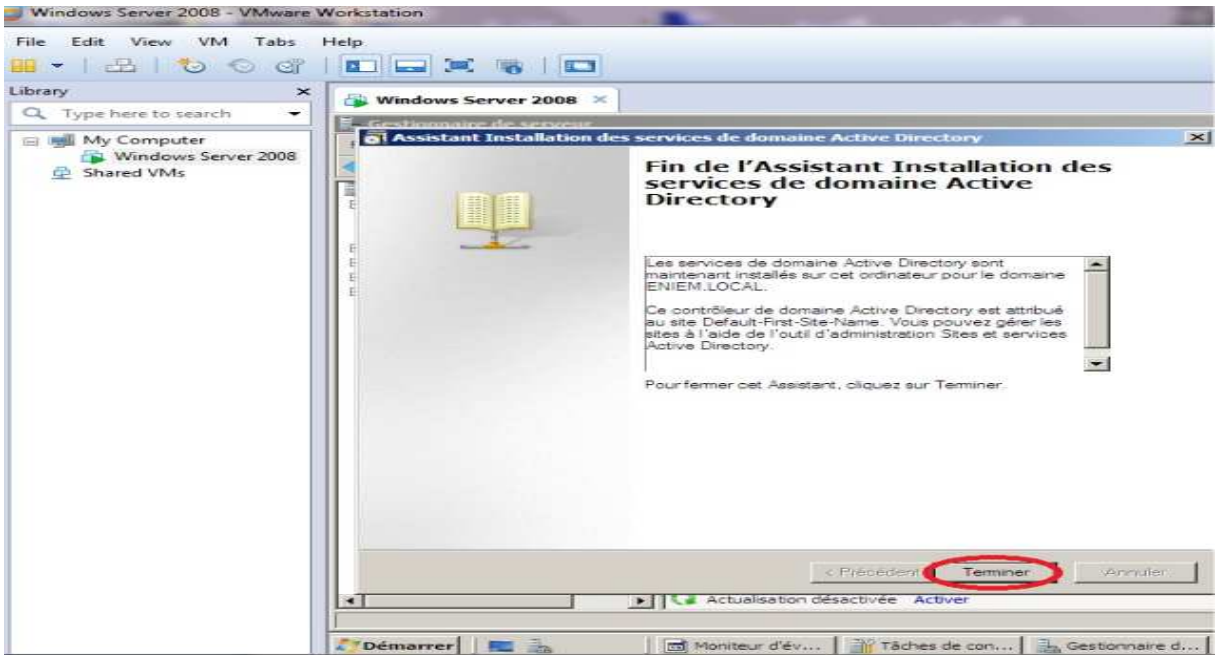


Fig.B.13 : Fin de l'installation d'Active Directory.

Une fois l'installation est terminée, on doit redémarrer le système

C.1. L'installation de rôle serveur web IIS

- Tous d'abord, on accède au menu « démarrer », et on choisit « outil administration »-> « gestionnaire de serveur ».

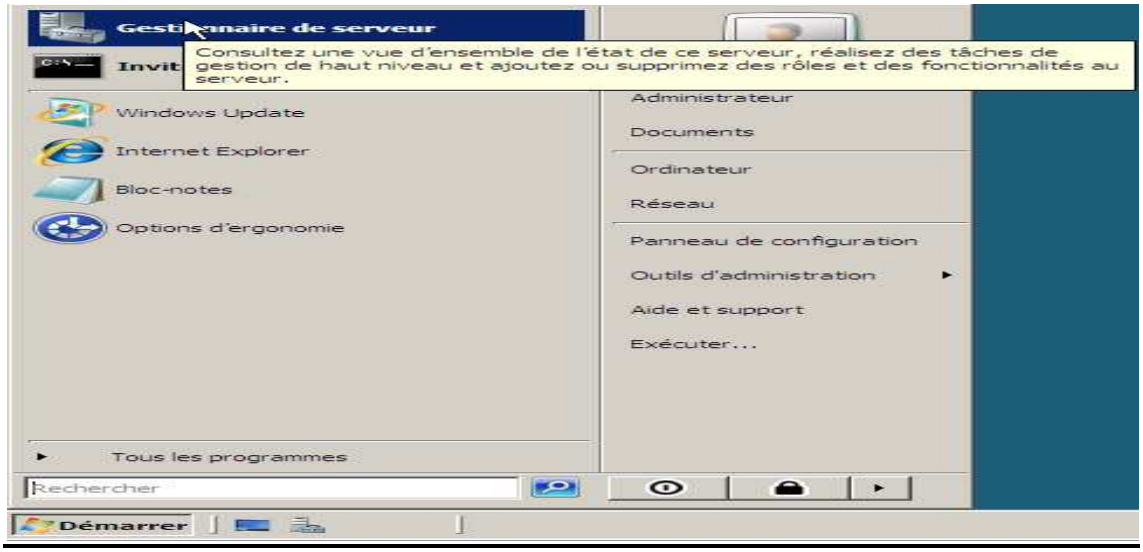


Figure C.1 : console de gestion de serveur.

✓ Dans l'arborescence à gauche on sélection « rôles », et on choisit « ajouter des rôles ».

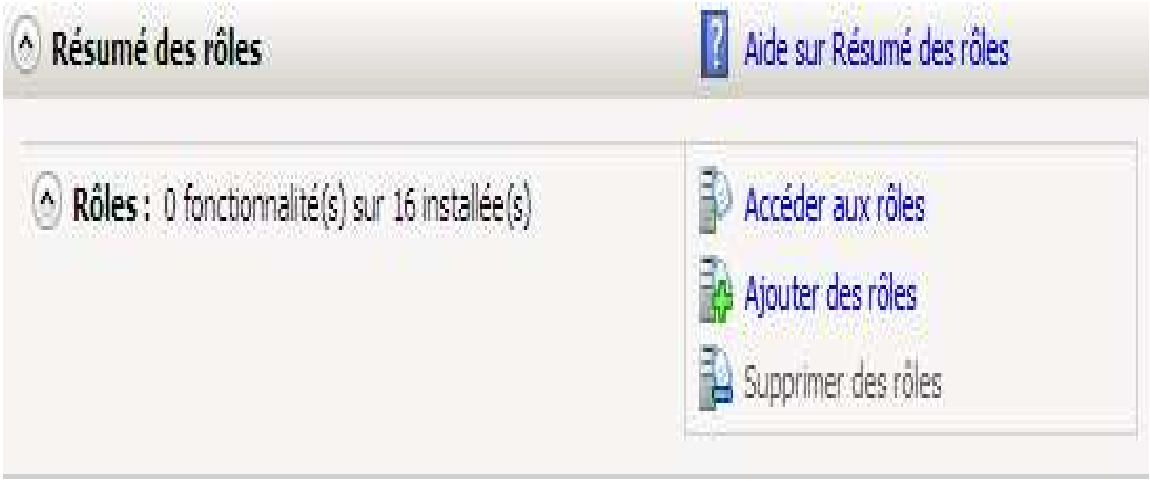


Figure.C.2 : ajout des rôles.

- ✓ Dans la liste des rôles disponibles avec Windows Server 2008, on coche « serveur web IIS », puis on clique sur suivant.

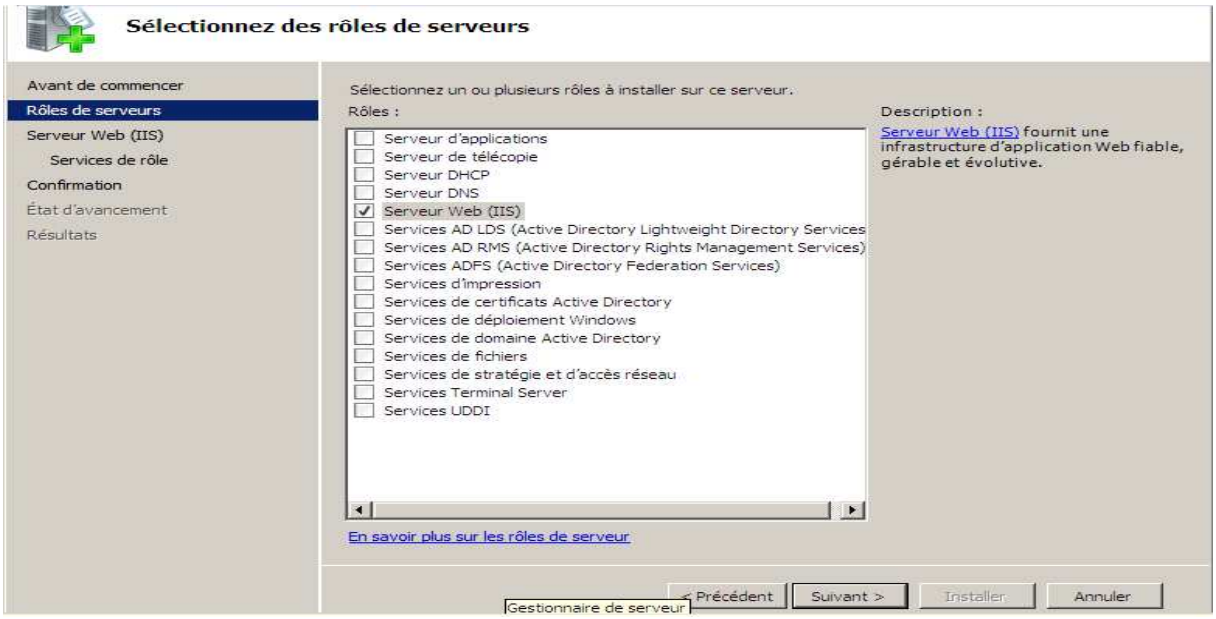


Figure.C.3 : ajout de rôle serveur web (IIS).

- ✓ Une fois qu'on a terminé l'installation de serveur IIS la fenêtre suivante s'affiche.

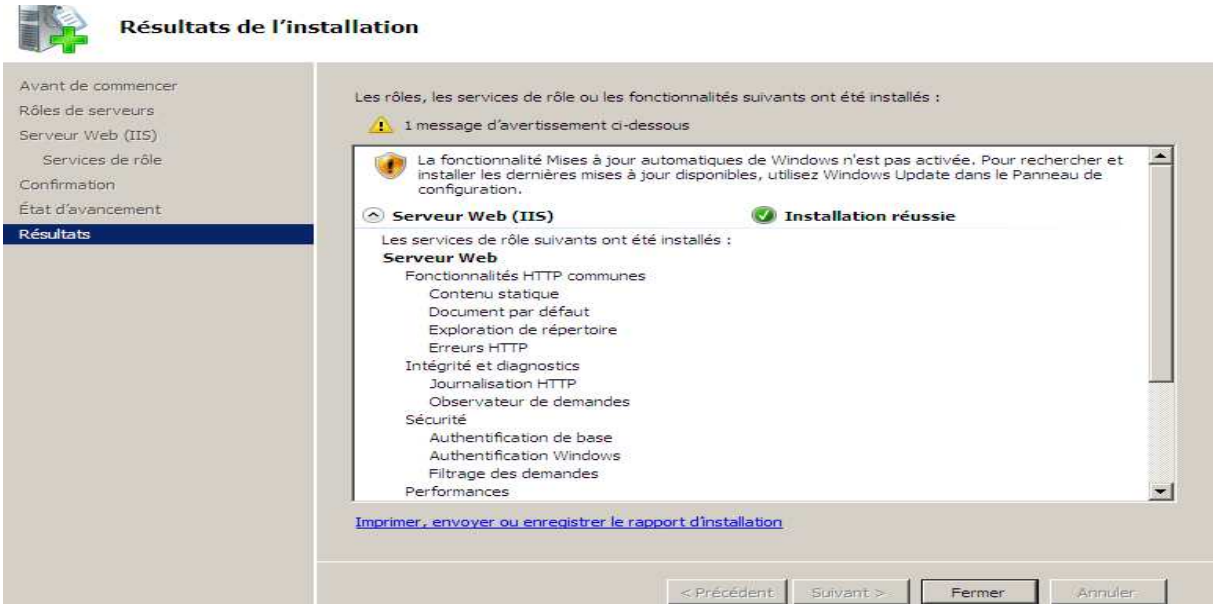


Figure.C.4 : fin d'installation de serveur web (IIS).

Afin de vérifier que votre installation c'est bien dérouler, on ouvre un navigateur Web, puis dans la barre d'adresse on tape : **http://localhost/**, l'image suivante qui apparaît dans notre navigateur.

Figure.C.5 : l'image de serveur web IIS.

C.2. L'installation de FonctionnalitéFramework

- Dans l'arborescence à gauche de la console de gestion de gestion de serveur on sélection « Fonctionnalités », et on choisit « ajouter des Fonctionnalités ».

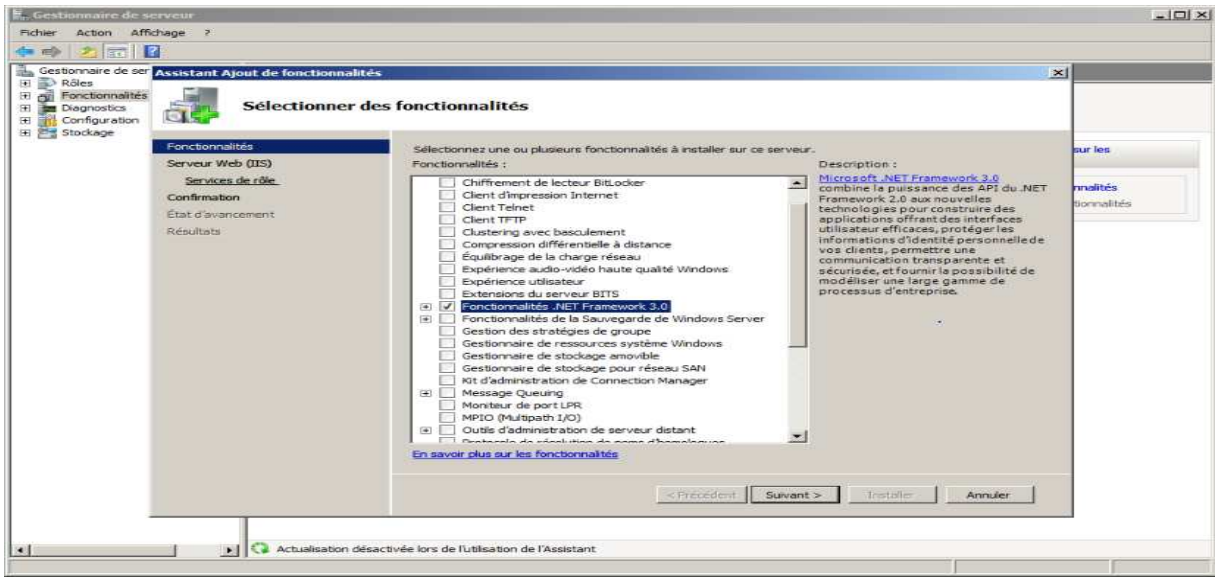


Figure.C.6 : ajout la fonctionnalité Framework.

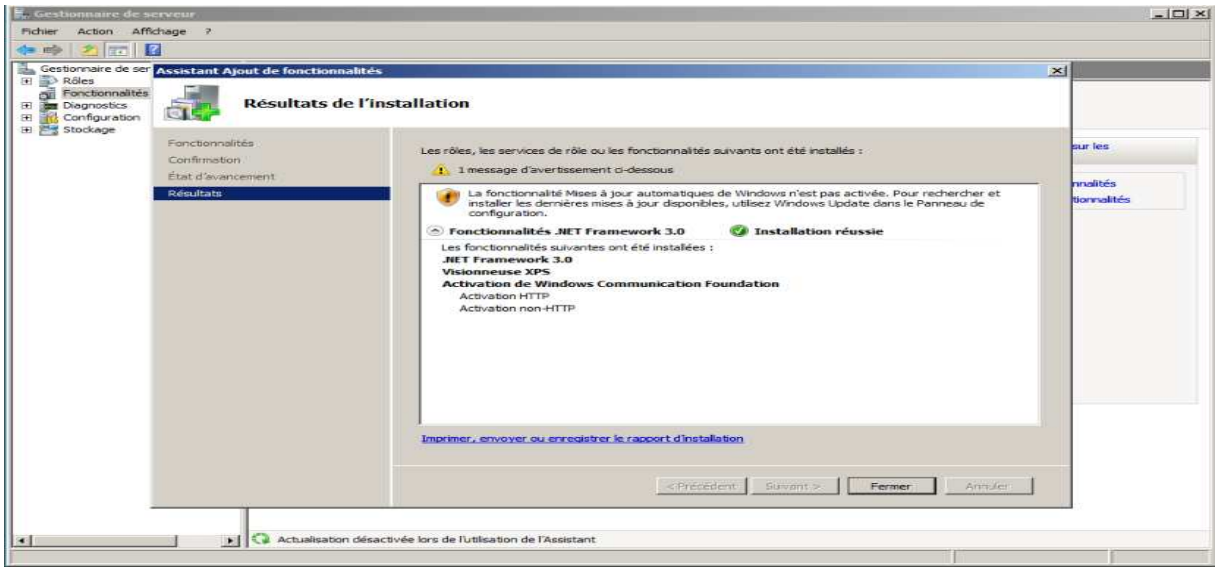


Figure.C.7 : fin d'installation de Framework.

C.3. Installation de Microsoft Exchange Server 2007

Une fois tous les prérequis valides, nous passons à l'étape d'installation d'Exchange 2007. Pour cela nous exécutons le fichier <<setup>> situé dans le dossier d'installation.

Figure.C.9 : Lancement d'installation de l'Exchange.

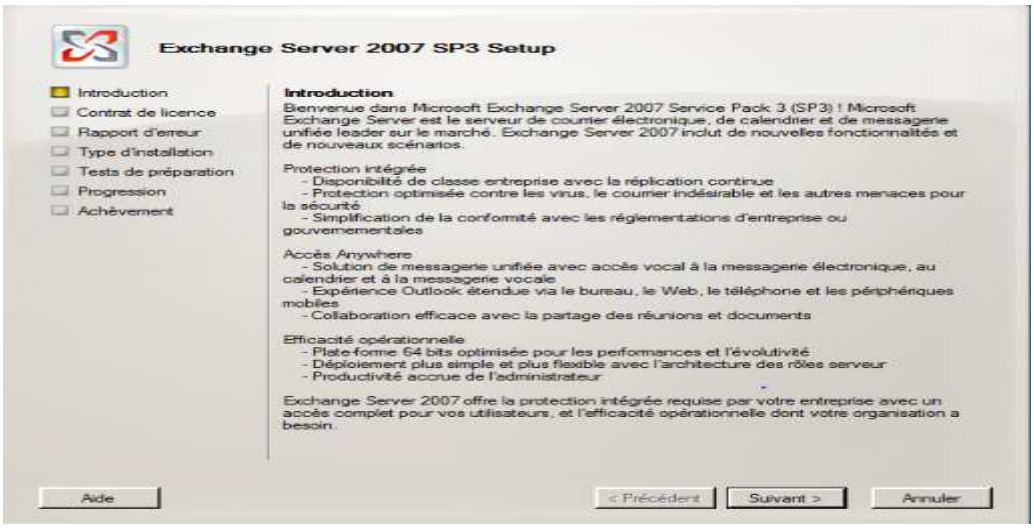


Figure.C.9 : Introduction.

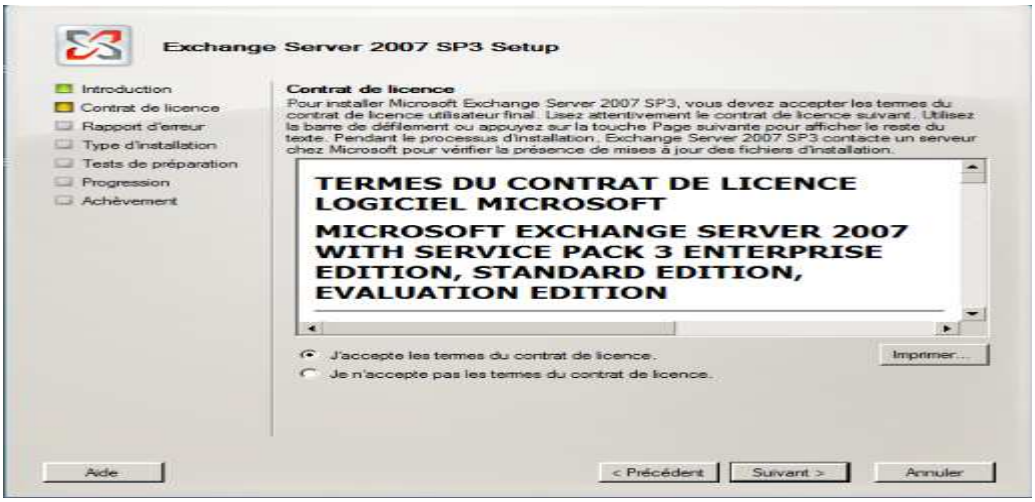


Figure.C.10 : Acceptation de la licence.

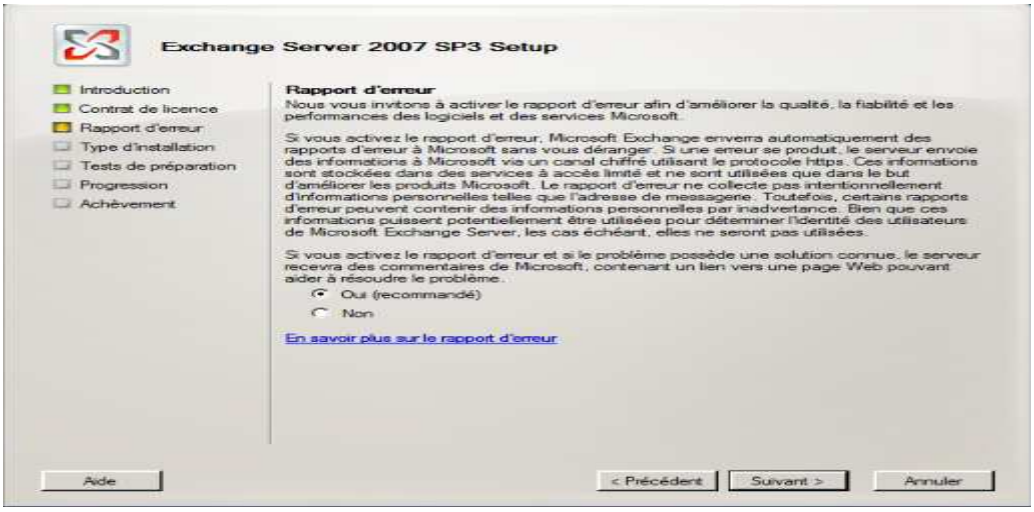


Figure.C.11 : Le choix de rapport d'erreur.

Après avoir passé l'introduction, accepté le contrat de licence et choisi notre mode de rapport d'erreur, nous avons le choix entre une installation typique ou personnalisée. L'installation personnalisée nous permet d'installer les rôles dont nous avons besoin alors que l'installation typique installera le rôle Hub ….etc. ainsi que les outils de gestion Exchange. Nous avons procédé à l'installation typique.

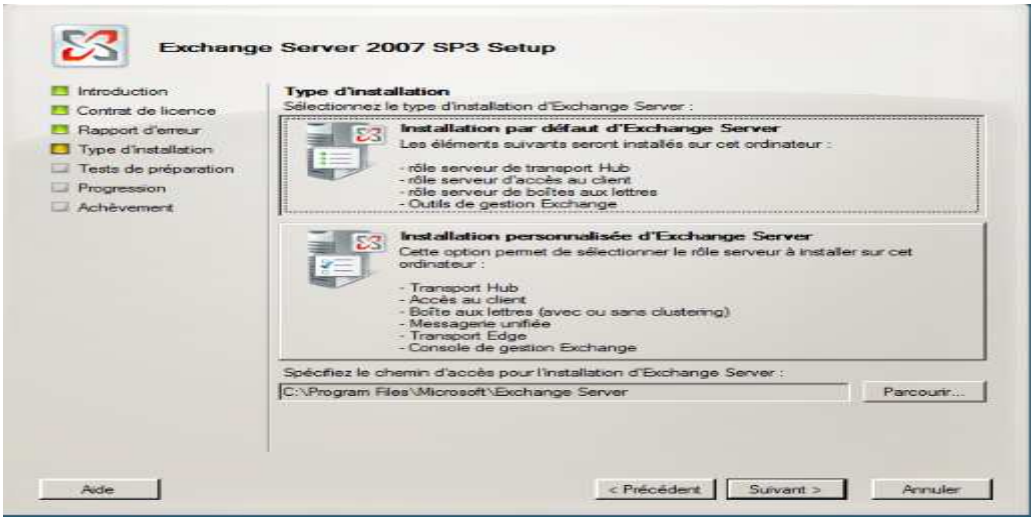


Fig.C.12 : Le choix de type d'installation.

Figure.C.13 : Spécification de nom de l'organisation.

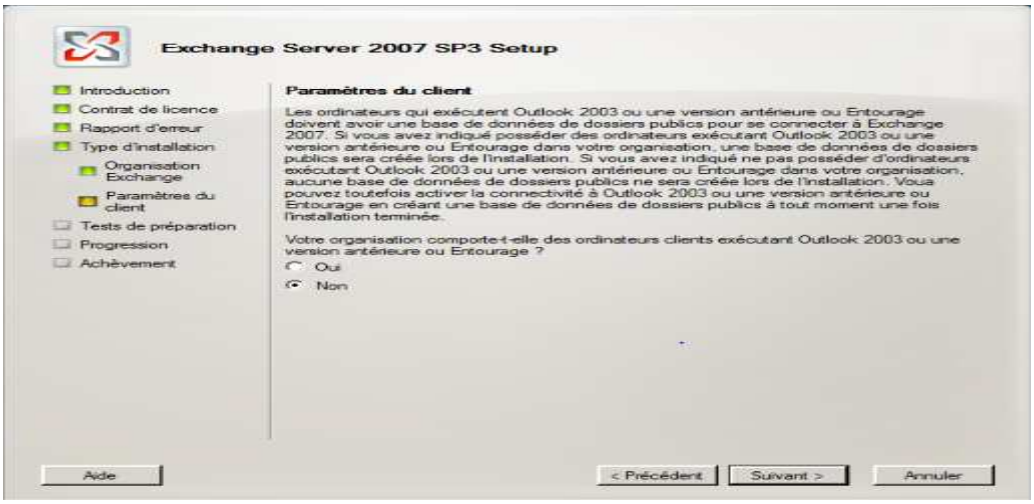


Figure.C.14 : Paramètre client.

Figure.C.15 : Achèvement.