

République algérienne démocratique et populaire

Ministère de l'enseignement
supérieur et de la
recherche scientifique



Université Mouloud
Mammeri Tizi-Ouzou
Faculté de génie électrique
et informatique
Département Informatique

Mémoire

En vue de l'obtention du diplôme

MASTER ACADEMIQUE

En **Réseau Mobilité** et les **Systèmes Embarqués**

Implémentation d'un réseau vpn cas :Entreprise ENIEM.

Etudié et réalisé par

M^{me} : **Hadji** kahina

Encadré par

M^{me} : **Hadaoui rebiha**

PROMOTION : 2014/2015

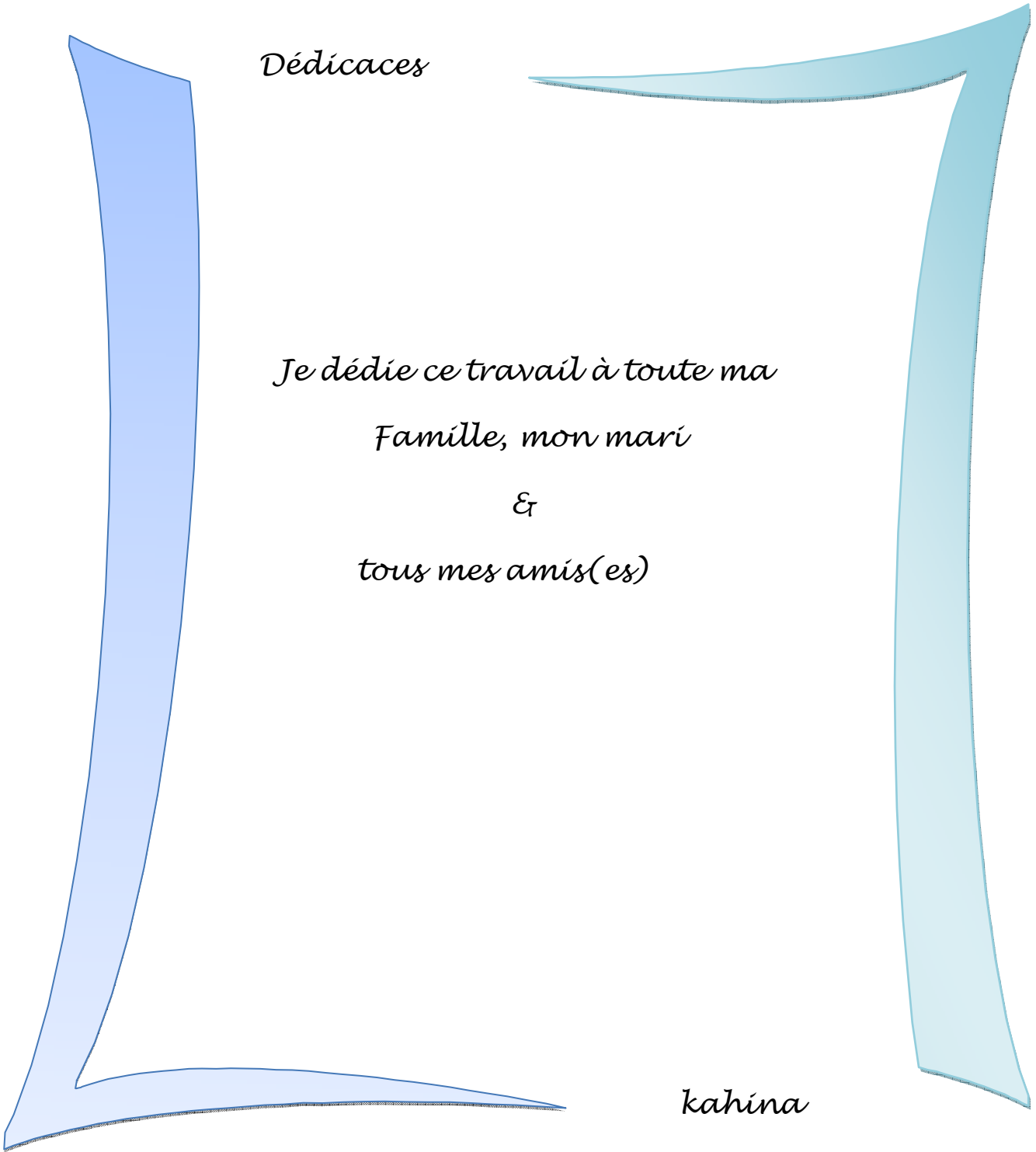
REMERCIEMENTS

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

Je tiens à remercier particulièrement mon enseignante et ma promotrice madame HADAoui REBIHA, 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 travail à toute ma
Famille, mon mari
&
tous mes amis(es)*

kahina

SOMMAIRE

Introduction générale

Chapitre I : introduction à la sécurité informatique et les réseaux privés virtuelles

Partie I. Réseaux

I.1.Introduction	1
I.2. Définition	1
I.3. Objectifs des réseaux.....	1
I.4. Classification des réseaux.....	2
I.4.1. LAN.....	2
I.4.2. MAN.....	2
I.4.3. WAN.....	2
I.5.Fonctionnement des réseaux.....	2
I.5.1. Modèle OSI.....	3
I.5.2. Modèle TCP/IP.....	5

Partie II. Sécurité informatique

II.1.Introduction	7
II.2. Objectifs	7
II.3. Services principaux de la sécurité réseau.....	7
II.4. Objectifs des hackers.....	8
II.5. Politique des hackers.....	8
II.5.1 reconnaissance du système.....	9
II.5.2. exploitation du système.....	10
II.5.3. préservation d'accès.....	10
II.5.4. effacement des traces.....	11
II.6. Différents types d'attaques.....	11
II.6.1. attaques réseaux.....	11
II.6.2.attaques applicatives.....	13
II.6.3.attaques par déni de service.....	14
II.6.4.attaques virales.....	16
II.7.Outils de sécurité.....	16
II.7.1. cryptographie,signature électronique et certificat.....	17

19
19
20
21
21
21
22
23

.

II.7.2. Mots de passes	19
II.7.3. FireWall	19
II.7.4. Scanners de vulnérabilités	20
II.7.5. Fichiers historiques.....	21
II.7.5. VPN	21
II.7.6. pot de miel	21
II.7.7. IDS	22
Conclusion.....	23

Chapitre II :Les VPNs

II.1.Introduction	24
II.2.définition d'un VPN	24
II .2.Les VPN en entreprise	25
II.3.Principe de fonctionnement d'un VPN	27
II.4.Les principaux avantages d'un VPN.....	27
II.5.Les caractéristiques d'un VPN	27
II .6. Les différentes architectures possibles.....	28
II.7.Description du fonctionnement	31
II.7.1.le protocole PPP	31
II.7.2 : Les différent protocoles utilisé pour l'établissement d'un VPN	32
II.7.3. Le protocole de Niveau 3 : IPSEC	34
II .8.Algorithmes utilisés par ipsec	40
II .8.1.Algorithmes symétrique	40
II .8 .2.Les algorithmes asymétriques	44
Conclusion	46

Chapitre III : Présentation de l'Organisme d'Accueil

I. Introduction	47
II.Présentation de l'ENIEM	48
II.1.Unité froid	48
II.2.Unité Cuisson	48
II.3.Unité Climatisation	49
II.4.Unité Commerciale	49
II.5.Unité Prestations Techniques	49
II.6. Organigramme générale de l'entreprise	50
III.Présentation du champ d'études	51
III.1-Organigramme de l'Unité de Prestation Technique	51
III.2. Le Réseau informatique de l'entreprise l'ENIEM	52
II.1.Un Réseau client/serveur.....	52
II.2.Les armoires de brassage existantes	52
II.3.Description du système du serveur HP3000/A500	53
II.4.Caractéristiques matériels et logicielles	56
II.5.l'aspect logiciel.....	57
IV.Présentation du Département Informatique de l'ENIEM.....	58
IV.1Organigramme de département informatique	58
IV.2.Aspect humain.....	59
V. Conclusion	60

Chapitre IV : Conception et Réalisation

IV.I-CONCEPTION	61
I.1.Etude de l'existant Critique et suggestion.....	61
I.2.présentation du réseau existant.....	61
I.3. fonctionnement du réseau existant	62
I.4.Les critique du réseau existant	63
I.5.Solutions proposées	63
IV.II. Réalisation.....	63
II.1. Outils utilisés pour la réalisation du projet	63
I.2.Topologie pour la Simulation d'une liaison VPN site-à-site	64
I.3. Configuration de VPN site to site	64
I.3.1. Etablissement d'un tunnel Isec site-à-site.....	64
I.4. Table d'adressage	64
I. 5. Configuration de base des routeurs	65
I.5.1. Test de connexion et de routage	66
I.6. Configuration de VPN site to site.....	67
I.6.1. Etablissement d'un tunnel Isec site-à-site.....	67
I.7. Vérification	74
I.8.Analyse du trafic à l'aide de Wireshark	77
Conclusion	78

Introduction générale

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.

Cette merveilleuse ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique. Les utilisateurs de l'Internet ne sont pas forcement pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques. Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée..) et pour une entreprise (perte du savoir faire, atteinte à l'image de marque, perte financière..). Pour cela, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise. Dans ce contexte, les VPNs constituent une bonne alternative pour mieux protéger le réseau informatique.

Les VPNs connaissent de nos jours un essor important et constituent un investissement des entreprises. Ils sont déployés dans des zones précises du réseau ou sur des machines particulières pour compléter le travail des pare-feu, Un pare-feu agit comme une première barrière externe pour repousser les pirates informatiques, tandis qu'un système de détection d'intrusion vise à repérer ceux qui auraient transpercé ce premier périmètre de défense.

Vu la grandeur du sujet que on a abordé, ce travail sera subdivisé en quatre chapitres, la premier on donnera quelques notions fondamentales sur l'architecture et la sécurité des réseaux informatique, dans le chapitre qui suit, on développera le concept et l'architecture des VPNs, la troisième présentation de l'ENIEM, et on terminé par une mise en place d'un VPN au sein du réseau de l'entreprise ENIEM.

Chapitre I : Généralités sur les réseaux informatiques

Partie I: Réseau informatique

I.1. Introduction :

Les réseaux informatiques sont nés d'un besoin d'échanger des informations de manière simple et rapide entre les machines. Lorsqu' on travaillait sur une machine, toutes les informations nécessaires au travail étaient centralisées sur celle-ci. Pour des raisons de coûts et de performances, on a manipulé plusieurs machines. Les informations ont du alors être dupliquées sur les différentes machines du même site. Puis on a éprouvé le besoin d'échanger des informations entre des sites, d'où l'évolution du besoin d'échanges de l'information.

I.2. Définition : [1]

Un réseau (Network) est un ensemble d'ordinateurs et périphériques interconnectés. Il permet de faire circuler des données informatiques et ainsi d'échanger du texte, des images, de la vidéo ou du son entre chaque équipement selon des règles et protocoles bien définis.

I.3. Objectifs d'un réseau : [86]

Un réseau informatique permet:

- Le partage des fichiers et des périphériques, applications et imprimantes
- La communication entre personnes (grâce au courrier électronique, la discussion en direct,..)
- La communication entre processus (entre des machines industrielles)
- La garantie de l'unicité de l'information (bases de données)
- Le transfert des données
- Le jeu à plusieurs,...

I.4. Classification des réseaux : [3] [84]

On peut classer les réseaux selon la distance qui sépare les ordinateurs en trois catégories :

- LAN (local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

I.4.1. LAN

LAN signifie *Local Area Network* (en français *Réseau Local*). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

I.4.2. MAN

Les MAN (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kms) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

I.4.3. WAN

Un WAN (*Wide Area Network ou réseau étendu*) interconnecte plusieurs LAN à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

I.5. Fonctionnement d'un réseau

Pour assurer le bon fonctionnement d'un réseau, il faut réunir les supports physiques nécessaires et prévoir une bonne architecture logicielle et une normalisation de celle-ci s'impose. Deux familles d'architectures ont vu le jour : La première s'appelle **le Modèle OSI**. La seconde est **l'architecture TCP/IP**. Détaillons chacune d'elles : [1]

I.5.1. Le Modèle OSI (Open System Interconnexion) : [1] [3] [85]

Ce modèle est une norme définie par *ISO* (International Standardization Organisation). Fondé sur un principe énoncé par *JULES CESAR* « Diviser pour mieux régner ». Ce modèle est composé de sept couches (elles seront détaillées ultérieurement) : ***couche physique, liaison de données, réseau, session, transport, présentation et application.***

Ce modèle permet la communication entre plusieurs réseaux hétérogènes, cette communication passe donc par un ensemble de couches empilées:

- Chaque couche a un rôle précis (conversion, routage, découpage, vérification etc.)
- Chaque couche dialogue avec la couche juste au dessus et celle juste au dessous : elle fournit des services à la couche dessus et utilise les services de la couche dessous.
- Chaque couche encapsule les données venant de la couche dessus en y ajoutant ses propres informations avant de les passer à la couche dessous (opération inverse dans l'autre sens).
- Les données traversent les couches vers le bas quand elles sont envoyées et elles remontent les couches à la réception.

Voyons donc le rôle de chacune de ces couches : [3]

1. Couche physique : C'est le support de transmission lui-même : un fil de cuivre, une fibre optique etc.

2. Couche Liaison de données : En charge d'encoder (ou moduler) les données pour qu'elles soient transportables par la couche physique et fournit également la détection d'erreur de transmission et la synchronisation.

3. Couche réseau : En charge du transport, de l'adressage et du routage des paquets.

4. Couche Transport : En charge de la liaison d'un bout à l'autre. Cette couche s'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.

5. Couche Session : En charge d'établir et maintenir des sessions (c'est-à-dire débiter le dialogue entre machines, vérifier que l'autre machine est prête à communiquer, s'identifier, etc.).

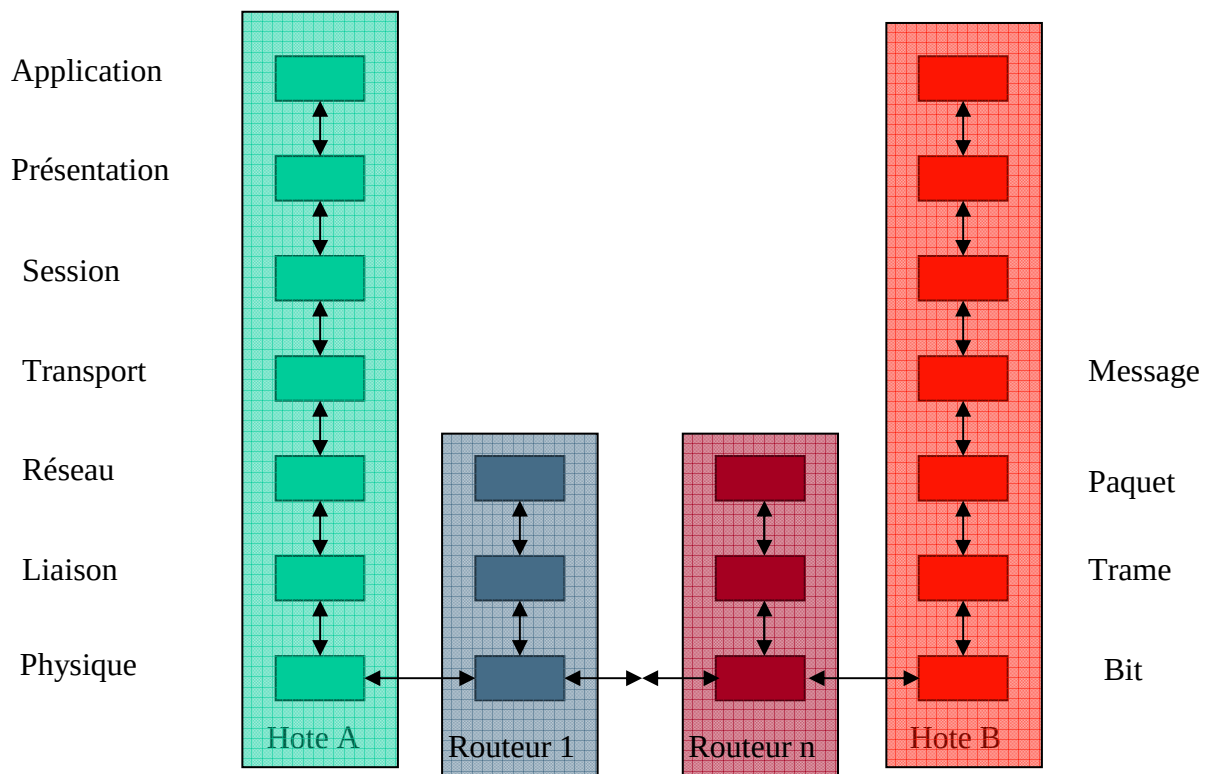


Figure I.7 : Modèle de référence OSI

6. Couche Présentation : Encharge de la représentation des données (de telle sorte qu'elle soit indépendante de microprocesseur ou du système d'exploitation par exemple) et éventuellement du chiffrement.

7. Couche application : Représente la couche la plus élevée du modèle OSI, elle utilise les services de la couche présentation (indirectement des autres couches) pour exécuter une application spécifique. L'application peut être un échange des courriers, transfert des fichiers ou toute autre application réseau.

Au niveau de chaque couche un ensemble de protocole est intégré. Un protocole réseau est un langage que vont utiliser toutes les machines d'un réseau pour communiquer entre elles.

HTTP, FTP, TCP, IP, ICMP, et la totalité des autres protocoles entrent dans le modèle OSI.

I.5.2. Le Modèle TCP/IP [2] [3]

Développé par l'armée américaine. Ils désigne en fait deux protocoles étroitement liés : un protocole de transport TCP (Transmission Control Protocol), et un protocole réseau IP (Internet Protocol). Le modèle TCP/IP est en fait une architecture réseau à quatre couches : ***couche hôte réseau, Internet, couche transport et application***. Détaillons chacune de ces couches :

- 1. Couche hôte réseau** : Cette couche semble regrouper les couches : physique et liaison de données du modèle OSI. Elle permet à un hôte d'envoyer des paquets IP sur le réseau
- 2. Couche Internet** : Cette couche est la clé de voûte de l'architecture IP. Cette couche réalise l'interconnexion des réseaux (hétérogènes). Son rôle est de permettre l'injection des paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination, les paquets peuvent arriver dans le désordre, le contrôle de l'ordre est la tâche des couches supérieures. L'implémentation officielle de cette couche est le protocole IP [3].
- 3. Couche transport** : Son rôle est le même que celui de la couche transport du modèle OSI. Officiellement, cette couche n'a que deux implémentations : le protocole *TCP* et le protocole *UDP* (User Datagram Protocol) [3]
- 4. Couche application** : Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles.

On s'est en effet aperçu avec l'usage que les logiciels réseaux n'utilisent que très rarement ces deux couches (Présentation et session), et finalement, le modèle OSI dépouillé de ces deux couches ressemble fortement au modèle TCP/IP.

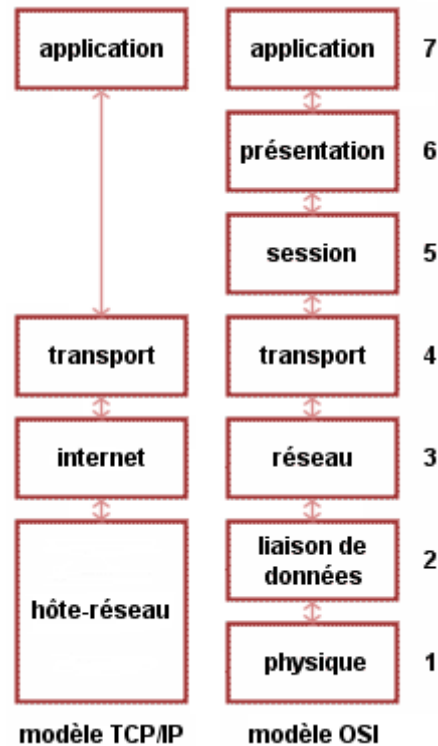


Figure I .2 : Modèle TCP et OSI

TCP/IP est le protocole utilisé dans le réseau Internet. L'implémentation de ce modèle engendre malheureusement des vulnérabilités dus au failles des langages de programmation utilisés dans l'implémentation (exp : langage C). Ces vulnérabilités peuvent être exportées par les attaquant pour réaliser leurs attaques, d'où le problème de la sécurité réseau.

Partie II: Sécurité réseau

II.1. Introduction

Les entreprises ouvrent leur système d'information à leurs partenaires et fournisseurs via internet. Cette merveilleuse ouverture, qui permet de faciliter la communication engendre malheureusement des risques importants dans le domaine de sécurité de l'entreprise.

Les ordinateurs connectés de l'entreprise ont des failles qui peuvent être exploitées par des **hackers**¹ pour réaliser ses attaques. Les conséquences de ces attaques peuvent être lourdes (perte d'information, vol d'information, perte financière, accès à des informations confidentielles, etc..). Par conséquent, il est important d'être conscient de ces menaces et de prendre des mesures adéquates afin de se protéger de ces attaques, pour cela, les administrateurs sécurisent de plus en plus leur système d'informations en utilisant diverses solutions comme : mot de passe, pare feu, la cryptographie, les scanners de vulnérabilités, antivirus, et les systèmes de détection d'intrusions. Nous détaillons dans la suite chacune de ces méthodes et nous soulignons leurs limites.

II.2. Objectifs de la sécurité informatique [5]

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, etc. Néanmoins, les points principaux sont les suivant : [5]

- Empêcher la divulgation non autorisée des données.
- Empêcher la modification non autorisée des données.
- Empêcher l'utilisation non autorisée des ressources réseaux ou informatique de façon générale.

II.3. Services Principaux de la sécurité réseau

Pour remédier aux failles et pour contrer les attaques, la sécurité informatique se base sur un certain nombre de services qui permettent de mettre en place une réponse appropriée à chaque menace. Les principaux services sont : [6]

¹ Le terme « hacker » est souvent utilisé pour designer un pirate informatique.

-La confidentialité : La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

-L'intégrité de données : Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

-La disponibilité : Permettant de maintenir le bon fonctionnement du système informatique.

-La non répudiation : Permettant de garantir qu'une transaction ne peut être niée.

-L'authentification : L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

II.4. Objectifs des hackers

Les motivations des hackers (Selon les individus) peuvent être multiples. On y retrouve : [7]

- Vérification de la sécurité d'un système.
- Espionnage.
- L'attraction de l'interdit.
- Le désir d'argent (voler un système bancaire par exemple).
- Le besoin de renommées (impressionner des amis).
- L'envie de nuire.
- Pour apprendre.
- Etc.

II.5. Politique des hackers [8] [10]

La Meilleure façon de protéger son système informatique est de procéder de la même manière que les pirates, afin de cartographier les vulnérabilités² du système : [8] [10]

² Vulnérabilité : trou de sécurité (en anglais security hole) désignant les failles de sécurité.

II.5.1. Reconnaissance du système [21]

Avant qu'un hacker ne s'introduit dans le système informatique, il cherche dans un premier temps les failles c'est-à-dire, des vulnérabilités visibles à la sécurité du système : dans les protocoles, les systèmes d'exploitation, les applications, ou même le personnel d'une organisation. Pour cela, il utilise plusieurs moyens :

- **Reconnaissance passive [9] [21]**

Le hacker partage librement ses découvertes et évite la destruction intentionnelle des données. Une des attaques les plus répandues l'écoute du trafic **Sniffing**. Le principe consiste à installer une sonde sur le réseau pour capter le trafic et le sauvegarder dans des fichiers journaux. L'analyse de ces fichiers permet de connaître les machines installées sur le réseau, et de déterminer les ports ouverts, et les systèmes d'exploitations utilisées.

- **Reconnaissance active [9]**

A ce niveau, l'attaquant ne se restreint pas à inspecter les données échangées entre les différents hôtes cependant, il initie lui même des connexions réseau pour tester le comportement des machines, il cherche des informations précises concernant les hôtes accessibles, l'emplacement des routeurs et des pare-feux. Parmi les techniques les plus utilisées pour acquérir ces informations, nous évoquons les utilitaires : **Ping [102]**, **TraceRoute [103]** et **Nmap [104]**.

II.5.2. Exploitation du système [9]

Une fois le hacker a localisé les applications vulnérables, il exploite ensuite leurs faiblesses. L'intrus cherche à gagner un accès au réseau, cible en lançant diverses attaques. (Dans la suite nous détaillons quelques attaques).

II.5.3. Préservation d'accès [9]

Les attaquants installent des **portes dérobées**³ pour pouvoir retourner facilement aux systèmes compromis. Par exemple, ils créent de nouveaux comptes et les utilisent lors des prochains accès. Cette procédure est facilement détectable si un administrateur vérifie constamment l'intégrité des fichiers.

II.5.4. Effacement des traces [8] [10]

Une fois la porte dérobée est créée, l'attaquant cherche aussitôt à effacer ses traces. Il essaie de restituer les mêmes propriétés des fichiers (date de création, de modification, dernière utilisation, etc..), pour garder la même signature, ceci force les administrateurs à enregistrer les événements sur des machines distinguées pour mieux protéger les fichiers de sécurité.

II.6. Différents types d'attaques

II.6.1. Les attaques réseaux [10] [11] [8]

Les attaques réseaux les plus connues aujourd'hui sont :

- **Spoofing IP**

Le spoofing IP est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement, il s'agit d'une mascarade de l'adresse IP au niveau des paquets émis, c'est-à-dire une modification des paquets envoyés afin de faire croire au destinataire qu'ils proviennent d'une autre machine.

³ Porte dérobée : faille créer par le pirate.

- **Spoofing ARP**

Le spoofing ARP est une technique qui modifie le cache ARP. Le cache ARP contient une association entre les adresses matérielles des machines et les adresses IP, l'objectif du pirate est de conserver son adresse matérielle, mais d'utiliser l'adresse IP d'un hôte approuvé. Ces informations sont simultanément envoyées vers la cible et vers le cache. A partir de cet instant, les paquets de la cible seront routés vers l'adresse matérielle du pirate.

- **Spoofing DNS**

Le système DNS (Domain Name System) a pour rôle de convertir un nom de domaine en son adresse IP et réciproquement, à savoir : convertir une adresse IP en un nom de domaine. Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émises par une victime. Il existe deux types de méthode: [5] [14]

- **DNS ID spoofing** L'attaquant essaie de répondre à un client en attente d'une réponse d'un serveur DNS, avec une fausse réponse et avant que le serveur DNS ne réponde.
- **DNS Cache Poisoning** L'attaquant essaie d'empoisonner le cache (table de correspondance IP- nom _machine) du serveur DNS.

- **Désynchronisation TCP [86]**

Le protocole TCP permet d'assurer le transfert des données de façon fiable, bien qu'il utilise le protocole IP (qui n'intègre aucun contrôle de livraison de datagramme) grâce à un système d'accusés de réception (ACK) permettant au client et au serveur de s'assurer de la bonne réception mutuelle des données.

Lors de l'émission d'un segment, un numéro d'ordre (appelé aussi numéro de séquence) est associé, et un échange de segments contenant des champs particuliers (appelés *drapeaux*, en anglais *flags*) permet de synchroniser le client et le serveur. Ce dialogue (appelé *poignée de mains en trois temps*) permet d'initier la communication, il se déroule en trois temps, comme sa dénomination l'indique:

- Dans un premier temps, la machine émettrice (le client) transmet un segment dont le drapeau SYN est à 1 (pour signaler qu'il s'agit d'un segment de synchronisation), avec un numéro d'ordre C , que l'on appelle numéro d'ordre initial du client
- Dans un second temps la machine réceptrice (le serveur) reçoit le segment initial provenant du client, puis lui envoie un accusé de réception, c'est-à-dire un segment dont le drapeau ACK est à 1 (accusé de réception) et le drapeau SYN est à 1 (car il s'agit là encore d'une synchronisation). Ce segment contient un numéro de séquence S . Le champ le plus important de ce segment est le champ accusé de réception (ACK) qui contient le numéro d'ordre initial du client, incrémenté de 1
- Enfin, le client transmet au serveur un accusé de réception, c'est-à-dire un segment dont le drapeau ACK est à 1, et dont le drapeau SYN est à zéro (il ne s'agit plus d'un segment de synchronisation). Son numéro d'ordre est incrémenté et le numéro d'accusé de réception représente le numéro de séquence initial du serveur incrémenté de 1

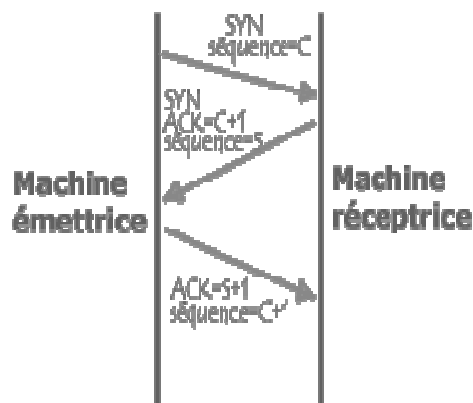


Figure II.2 : Synchronisation TCP [86]

L'attaquant peut rediriger le trafic TCP, pour cela il envoie des paquets malformés au client avec une adresse IP correspondant à celle du serveur en y plaçant des mauvais numéros de séquences, le client va croire qu'il a perdu la connexion et stoppera ses échanges avec le serveur. Mais si l'attaquant envoie les bons numéros de séquences au serveur, il récupérera la connexion pour lui.

II.6.2. Les attaques applicatives : [10] [11] [8]

- **Injection SQL [14]**

Les attaques par **injection de commandes SQL** sont des attaques visant les sites web s'appuyant sur des bases de données relationnelles.

Dans ce type de sites, des paramètres sont passés à la base de données sous forme d'une requête SQL. Ainsi, si le concepteur n'effectue aucun contrôle sur les paramètres passés dans la requête SQL, il est possible à un pirate de modifier la requête afin d'accéder à l'ensemble de la base de données, voire à en modifier le contenu.

Le principe de cette attaque consiste à injecter du code supplémentaire au sein des requêtes a fin de leurrer l'interpréteur SQL.

Par exemple contourner les mécanismes d'authentification via les entrées imprévues. Considérons par exemple la requête SQL (II.1). Cette requête permet de vérifier le mot de passe de l'utilisateur *\$varNom* en consultant la table utilisateur. Seulement un intrus peut s'identifier avec un nom d'un utilisateur légitime puis entrer un mot de passe de la forme **cmoi OR TRUE**.

La requête SQL (II.1) se transforme en (II.2) [14] et sera toujours vérifiée si l'utilisateur *\$varNom* existe dans la table utilisateur.

select * from utilisateur where nom = \$varNom and mot2passe = \$varPasse (II.1)

select * from utilisateur where nom = \$varNom and True (II.2)

L'attaquant peut créer son propre compte, en utilisant le nom d'un utilisateur légitime requête (II.3) [14]

SELECT * from client where mon='joe ;insert into utilisateurs values('mon_login','mon_password') (II.3)

- **Les bugs [14]**

Tout logiciel comporte des bogues dont certains représentent des trous de sécurité ou des anomalies qui permettent de violer le système sur lequel tourne le programme. Si c'est un programme d'application réseau, ces trous peuvent être exploités à distance via Internet. Les plus connus de ces bugs et les plus intéressants, en ce qui concerne leur exploitation sont les buffers overflows.

Buffer overflow : consiste à mettre plus d'informations (et surtout d'autres informations) en mémoire que celle-ci n'est disposée à en recevoir.

Conséquences :

- Le débordement du buffer peut écraser l'adresse de retour au programme appelant : plantage (attaque de type déni de service).
- L'adresse de retour peut être remplacée par l'adresse d'un code malicieux.

II.6.3. Les attaques par déni de service [15][17]

Les attaques par déni de service (souvent abrégé **DOS**, en anglais Denial of service) consistent à paralyser temporairement (rendre inactif pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à des sociétés dont l'activité repose sur un système d'information. En l'empêchant de fonctionner.

- **La technique dite du smurf [86]**

La technique du *smurf* est basée sur l'utilisation de serveurs broadcast pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau que lui. Le scénario d'une attaque est le suivant :

La machine attaquante envoie un **ping [102]** à un (ou plusieurs) serveurs broadcast en falsifiant sa propre adresse IP (l'adresse à laquelle le serveur devrait théoriquement répondre par un pong) et en fournissant l'adresse IP de la machine cible. Lorsque le serveur broadcast va dispatcher le ping sur tout le réseau, toutes les machines du réseau vont répondre par un pong, que le serveur broadcast va rediriger vers la machine cible. Ainsi lorsque la machine attaquante adresse le ping à plusieurs serveurs broadcast situés sur des réseaux différents, l'ensemble des réponses de tous les ordinateurs des différents réseaux vont être reroutées sur la machine cible.

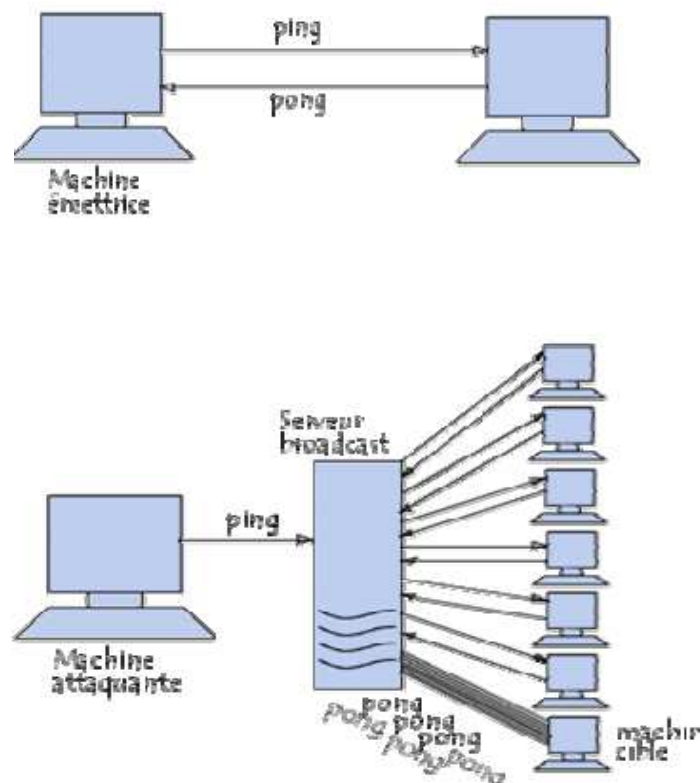


Figure II.3 : Exemple d'attaque [86]

- **SYN FLOOD [6]**

Son objectif est de rendre indisponible un service TCP offert sur une machine. Le principe de cette attaque est de créer des connexions TCP semi-ouvertes sur la machine cible

afin de remplir la file d'attente où sont stockées les demandes d'ouverture de connexions. L'attaquant envoie un grand nombre de requêtes SYN à la machine cible et remplace son adresse source avec l'adresse d'une machine indisponible ou inexistante afin que les réponses SYN/ACK ne soient jamais reçues et que donc les messages ACK ne soient jamais générés, ce qui signifie que la file d'attente restera pleine. Les conséquences de cette attaque sont que toutes les requêtes arrivant sur le port TCP cible seront ignorées et de ce fait le service fourni sur ce port sera indisponible. Dans certains cas, la machine peut aussi devenir indisponible.

- **Fragmentation [22]**

L'attaquant sature la connexion en envoyant des fragmentations déclenchant des exceptions (faille de la pile TCP/IP de *Windows 95* et *98*).

II.6.4. Les attaques virales [13]

Il existe principalement quatre types de menaces distinctes :

- **Virus [13]** : Se reproduisent en infectant le corps de programmes hôtes
- **Vers [13]** : Le vers se duplique et se propage à travers le réseau, par courrier électronique par exemple.
- **Chevaux de Troie [13]** : Exécutent des tâches malignes en se cachant dans un programme sain. Il peut par exemple voler des mots de passe, copier des données, ou exécuter toute autre action nuisible.

Trappes (portes dérobées) [13] : Permet à un utilisateur externe de prendre le contrôle d'une application par des moyens détournés.

II.7. Outils de sécurité [28]

Nous avons constaté que les attaquants disposent de plusieurs moyens pour réussir leurs attaques. La disponibilité des outils d'attaques et la richesse des sources d'informations accentuent le risque des intrusions. Par conséquent, les administrateurs sécurisent de plus en plus leurs systèmes informatiques. Ils s'appuient sur diverses solutions comme les pare-feux, la cryptographie, le mot de passe, les scanners de vulnérabilités et les systèmes de détection d'intrusions. Nous détaillons dans la suite chacune de ces méthodes et nous soulignons leurs limites.

II.7.1. Cryptographie, Signature électronique et Certificat [18] [19] [20]

-Cryptographie [20]

Le mot cryptographie est un terme générique désignant l'ensemble de techniques permettant de chiffrer des messages. Chiffrer un message consiste à le transformer au moyen d'un algorithme mathématique afin de le rendre inintelligible, sauf pour celui qui possède le moyen (une clé) de le déchiffrer. L'encryption des informations électroniques transitant par le réseau, est utilisée pour assurer la confidentialité et l'authenticité des transactions.

Le chiffrement se fait généralement à l'aide d'une clé de chiffrement, le déchiffrement nécessite quant à lui une clé de déchiffrement. Nous distinguons deux types de clés : [20]

- **Les clés symétriques :** Il s'agit de clés utilisées pour le chiffrement ainsi pour le déchiffrement. Nous parlons alors de chiffrement symétrique ou de chiffrement à clé secrète.

Le Data Encryption Standard (DES) est un exemple de crypto système à clé secrète.

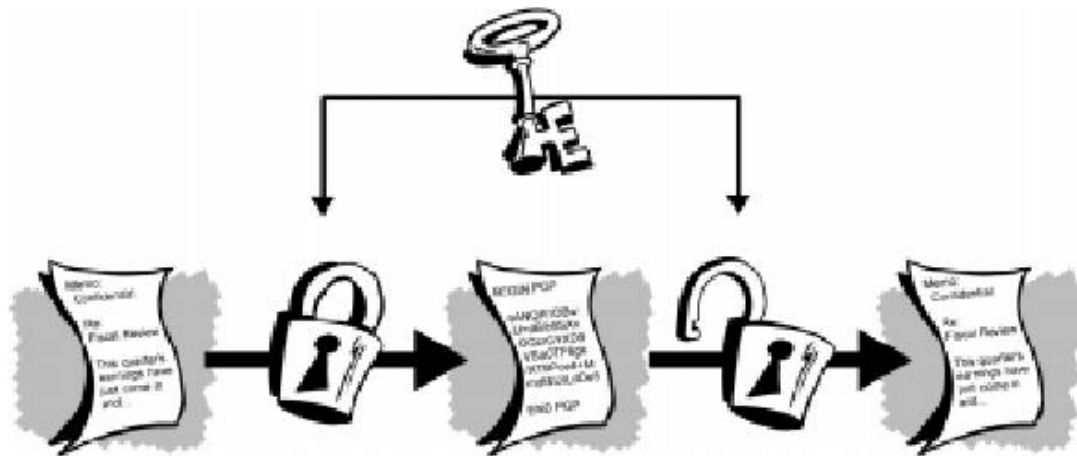


Figure II.4 : Les clés symétriques [20]

- **Les clés asymétriques :** Il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas nous utilisons une paire de clé, une clé publique qui chiffre les données, et une clé privée correspondante, aussi appelée clé secrète, qui sera utilisée pour le déchiffrement.

Algorithme de Signature Digitale (DSA) est un exemple d'algorithme à clé publique.

Les attaquants peuvent construire (nous l'appelons aussi cryptanalyse) un message chiffré en clair à l'aide des méthodes mathématiques. Ainsi, tout crypto système doit nécessairement être résistant aux méthodes de cryptanalyse.

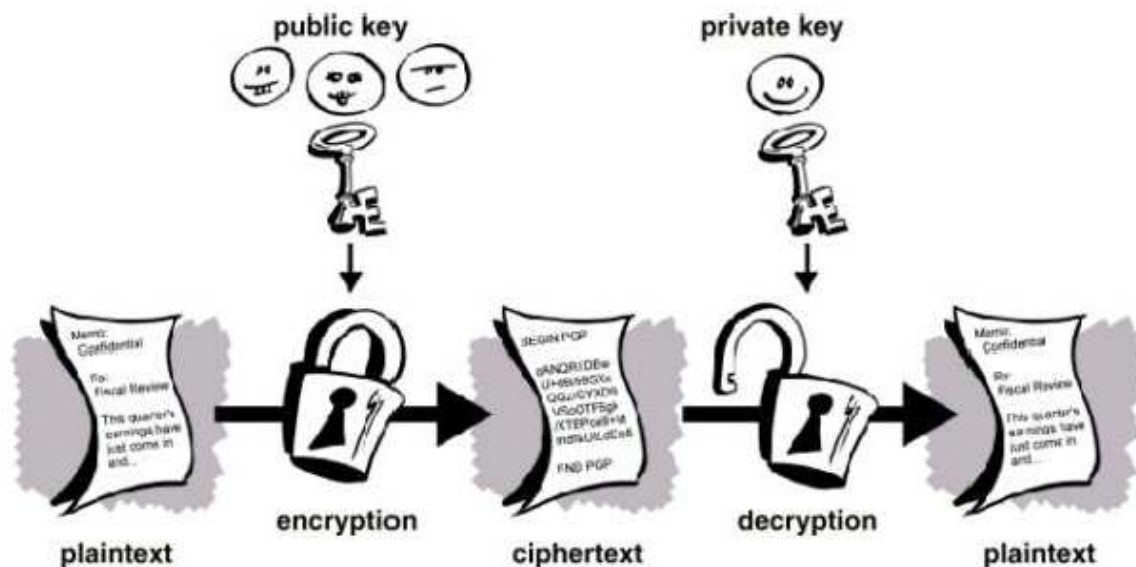


Figure II.5 : Les clés asymétriques [20]

-Signature électronique [18][20]

Signature électronique est un code digital permet à la personne qui reçoit une information de contrôler l'authenticité de son origine , et également de vérifier que l'information en question est intacte. Aussi, les signatures électroniques permettent l'authentification et le contrôle de l'intégrité et également la non répudiation.

-Certificat [19]

Certificat est Document électronique, carte d'identité émis par une autorité de certification. Il valide l'identité des interlocuteurs d'une transaction électronique, associe une identité à une clé publique d'encryptions et fournit des informations de gestion sur le certificat et le détenteur.

II.7.2. Mots de passes [87]

Une personne peut être authentifiée par une combinaison d'une identification et d'un mot de passe, (code secret personnel). Le mot de passe doit posséder certaines caractéristiques qui sont : non trivial, difficile à deviner, régulièrement modifié. Cependant si l'attaquant accède au fichier de mot de passe, il pourra s'introduire dans le système sécurisé.

II.7.3. Firewall [50]

Un Firewall est un assemblage matériel (ordinateur) et des logiciels installés sur celui ci dont l'objectif principal est de protéger le réseau interne contre les accès et actions non autorisés en provenance de l'extérieur, en contrôlant le trafic entrant et sortant.

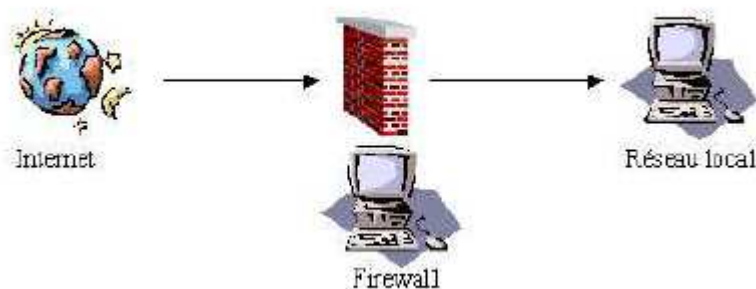


Figure II.6 : Placement d'un firewall [100]

Il existe plusieurs types de techniques de firewall : [28]

- La technique de filtrage des paquets : chaque paquet d'informations entrant ou sortant est accepté ou rejeté selon des règles établies par l'utilisateur.
- La technique des serveurs Proxy : qui empêche l'extérieur de connaître les adresses internes du réseau.
- La technique des passerelles : qui fournissent des systèmes de sécurité pour établir des connexions TCP/IP entre l'extérieur et l'intérieur ou pour certains services comme *FTP* et *TELNET*.

Les inconvénients d'un firewall sont [28] :

- Ne couvre pas tous les risques de sécurité. Par exemple il n'assure pas la confidentialité des informations, n'authentifie pas l'origine des informations, ne vérifie pas l'intégrité des informations, ne protège pas contre les attaques internes.
- Une très forte configuration de firewall augmente la sécurité mais peut alerter le fonctionnement du réseau.
- Le pirate peut détruire le système et ainsi permettre l'accès à tous les individus. C'est en général ce qui se passe.
- l'attaquant peut contourner le firewall

II.7.4. Scanners de vulnérabilités [9]

Les scanners de vulnérabilités automatisent la découverte des failles de sécurité. Ils sont utilisés par les attaquants pour localiser les faiblesses du réseau cible. De plus, les administrateurs peuvent en tirer profit pour corriger les vulnérabilités de leurs systèmes informatiques. Nous citons à titre d'exemple Nessus [24], Whisker [25] et Saint [26].

Cependant les scanners présentent quelques limites qui peuvent être résumées en trois points : l'exhaustivité, la mise à jour et l'exactitude. En effet, malgré le grand nombre de

vulnérabilités détectées, les scanners d'aujourd'hui sont inaptes à déterminer toutes les faiblesses possibles.

De plus, la mise à jour de ces produits ne suit pas le rythme de la découverte des nouvelles vulnérabilités. Enfin, la modification des bannières des services scannés permet de dissuader facilement le scanner ce qui entraîne parfois un responsable de sécurité à chasser des vulnérabilités fantômes.

II.7.5. Fichiers historiques [72]

La consultation régulière des fichiers historiques constitués doit notamment permettre de vérifier les anomalies dans le trafic des transactions. Par exemple, les messages répétitifs en provenances d'une même adresse extérieure et rejetés par le Firewall peuvent être un signe d'essai d'intrusion. Cependant, ces fichiers peuvent être consultés par les hackers afin d'effacer leurs traces. Pour cela, les administrateurs sauvegardent des copies de ces fichiers (back up) dans des endroits sécurisés et sur des machines différentes.

II.7.6. Réseau Privé Virtuel [28]

Un réseau VPN (*Virtual Privat Network*) est un service qui permet d'établir des connexions sécurisées privées (c'est-à-dire faire un réseau privé) sur un réseau public comme Internet (nous détaillons cette approche dans le chapitre suivant).

II.7.8. Pot de miel [9] [63]

Les pots de miels sont des systèmes qui simulent plusieurs services réseaux pour leurrer des intrus en exposant des vulnérabilités connues délibérément.

Un attaquant pense que ces services vulnérables sont actifs et qu'il peut les utiliser pour s'introduire dans le réseau. Il s'y colle pendant un certain temps. Pendant ce temps l'administrateur enregistre les activités de l'intrus pour découvrir ses actions et ses techniques.

Une fois ces techniques sont connues. L'administrateur emploie ces informations plus tard pour durcir la sécurité sur les serveurs réels.

II.7.9. Systèmes de détection d'intrusions [41]

- **Contexte**

Le concept de système de détection d'intrusions a été introduit en 1980 par *Anderson* [32]. Mais le sujet n'a pas eu beaucoup de succès. Il a fallu attendre la publication d'un modèle de détection d'intrusions par *Denning* [33] en 1987 pour marquer réellement le départ du domaine. En 1988, il existait au moins trois prototypes. [33]

La recherche dans le domaine s'est ensuite développée, le nombre de prototypes s'est énormément accru. Le gouvernement des États-Unis a investi des millions de dollars dans ce type de recherches dans le but d'accroître la sécurité de ses machines. [33]

- **Intrusion**

Une intrusion est toute utilisation d'un système informatique à des fins autres que celles prévues, généralement dues à l'acquisition de privilèges de façon illégitime. [35]

Une intrusion dans un système informatique est aussi définie par *Heady et al.* [36] comme: [37] « *N'importe quel ensemble d'actions essayant de compromettre l'intégrité, la confidentialité ou l'accessibilité d'une ressource* ».

Actuellement les **IDS** sont très populaires à cause de : [31]

- l'évolution continue des attaques.
- l'apparition de nouvelles attaques.
- la nécessité de détecter et réagir le plus vite possible aux attaques survenant dans le réseau.

Snort [66] est un exemple de **IDS** Open Source disponible au grand public basé sur l'approche par connaissance.

Conclusion

Nous avons constaté dans ce chapitre, que la sécurité réseau est un point primordial. Les administrateurs déploient des solutions de sécurité efficaces, capables de protéger le réseau de l'entreprise. Dans ce contexte, les VPNs constituent une bonne alternative pour mieux protéger le réseau informatique. Nous détaillons dans le chapitre II, les qualités d'un VPN, et la sécurisation des accès distant avec VPN.

II.1. Introduction

Nous avons présenté au Chapitre I un scénario possible d'attaques sur le réseau de l'entreprise et les différents mécanismes de protections contre ces attaques. Malgré leur grand intérêt, ils présentent des lacunes dues à l'évolution des techniques utilisées par les hackers. Ainsi et dans l'impossibilité de détecter toutes les attaques, le système de détection d'intrusions tente de déceler les attaques qui passent inaperçues à travers les mécanismes de sécurité. Un VPN est l'acte de la création et la configuration d'un réseau privé virtuel .

Après la courte introduction des systèmes de détection d'intrusions présentée au Chapitre I, dans ce chapitre, nous détaillons les qualités requises d'un tunnel VPN , son utilité , le critère de choix et un état de l'art des approches proposées dans la littérature.

II.2. définition d'un VPN

Un réseau privé virtuel (VPN) est l'extension d'un réseau privé qui englobe des liens à travers les réseaux publics ou partagés comme l'Internet. Avec un VPN, vous pouvez envoyer des données entre deux ordinateurs à travers un réseau partagé ou public d'une manière qui émule une liaison privée point à point.[39]

durant tout ce chapitre on a privilégié les VPN de niveau 3 en détaillant particulièrement le protocole IPSec.

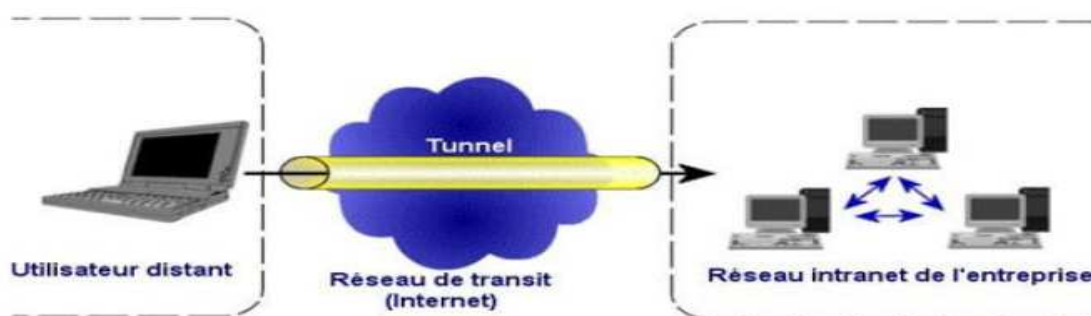


Figure II.1 : Schéma d'un accès VPN.[4]

Limites de responsabilité VPN niveau 2 et 3 :

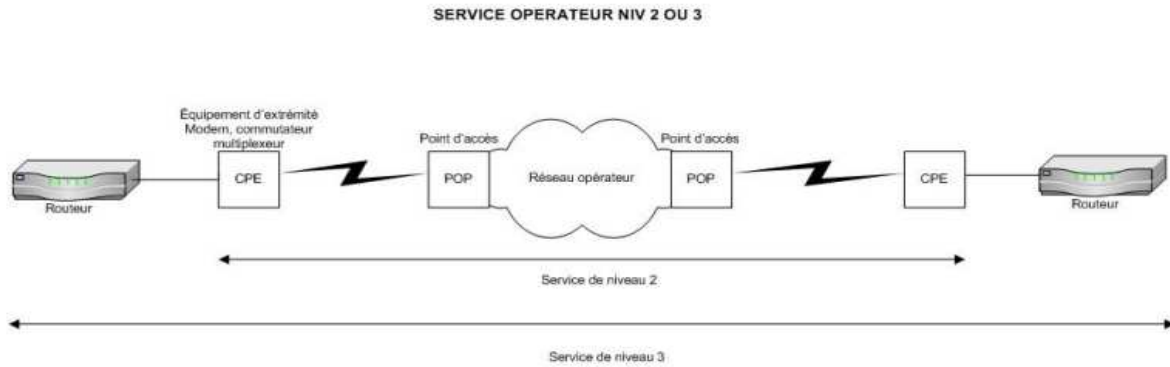


Figure II.2: Service Niveau 2 ou 3. [16]

- **Les VPN de niveau 2 : [16]**

Ils reposent sur Frame Relay et ATM. L'opérateur garantit au client la bande passante demandée ainsi que le niveau de service souhaité, avec des engagements de résultats.

- **Les VPN de niveau 3 : [16]**

Ils reposent sur IP et MPLS. L'opérateur s'engage sur une qualité de service équivalente voire supérieure, à celle pouvant être offerte par le niveau 2.

- **Les VPN IPSec (niv 3) : [16]**

Ils reposent sur le protocole de cryptage IPSec (protocole IPSec détaillé plus loin). On crée un tunnel crypté qui garantit la confidentialité des informations vis-à-vis des autres utilisateurs. Si le réseau IP est celui de l'opérateur, celui-ci peut s'engager sur une qualité de service. Si le réseau IP est l'internet, l'opérateur ne s'engage quasiment sur aucune qualité de service.

II .2.Les VPN en entreprise :

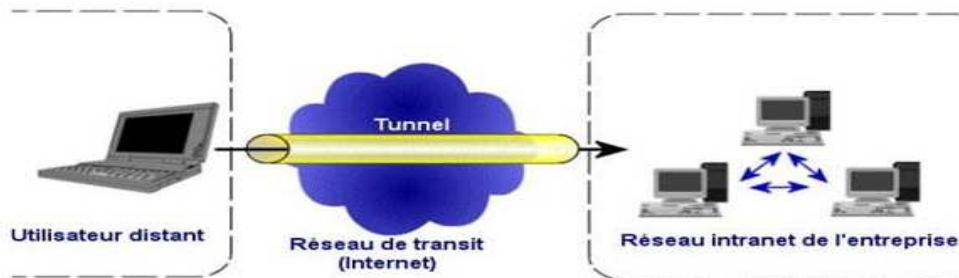
Les entreprises font de plus en plus appel à des réseaux privés virtuels (VPN) pour relier à leurs réseaux, leurs filiales, leurs télétravailleurs, leurs partenaires et d'autres utilisateurs. Alternative aux solutions d'appels à distance.. Les VPN permettent de transférer en sécurité des données, pour un coût plus faible par l'utilisation d'Internet, à priori, déjà disponible.

Suivant les besoins ; on réfère

4ce 3types de VPN :

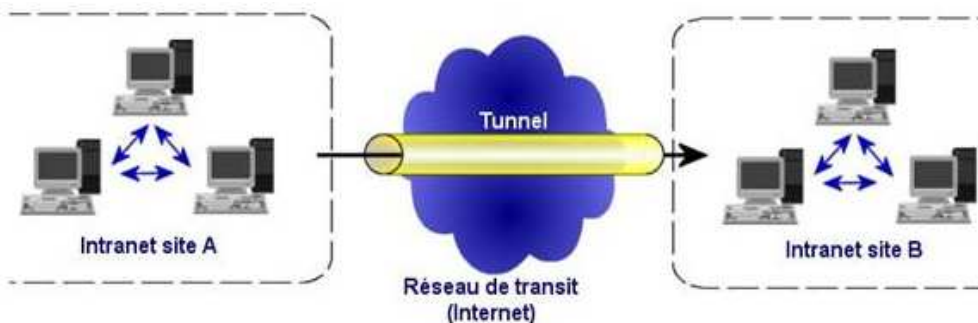
- **Le VPN d'accès :[4]**

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise, l'utilisation se sert d'une connexion internet afin d'établir une liaison sécurisée.



- **L'internet VPN :**

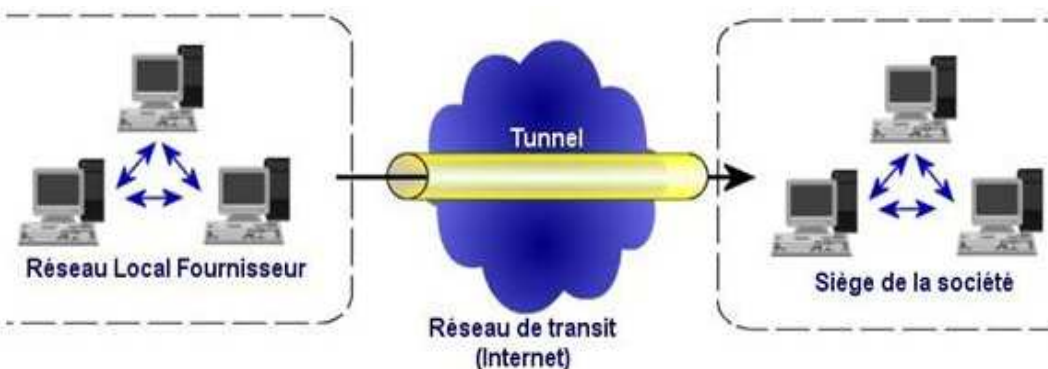
Il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'internet (partage de données, de ressources, exploitation de serveurs distant.



- **L'extranet VPN :**

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires .Elle ouvre alors son réseau local à ces derniers .Dans ce cas, il est nécessaire d'avoir une authentification fort de utilisateurs, aussi qu'une trace des différentes accès.

De plus, seule une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.



II.3.Principe de fonctionnement d'un VPN :

La création d'un VPN nécessite la création d'un tunnel. Un tunnel est un canal de communication dans lequel circuleront les données cryptées.

Le principe du VPN est donc basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. La source peut ensuite éventuellement chiffrer les données (on parle alors de VPN chiffrés) et les achemine en empruntant ce chemin virtuel.

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas le protocole de tunnelling encapsule les données en rajoutant un entête permettant le routage des trames dans le tunnel.

Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

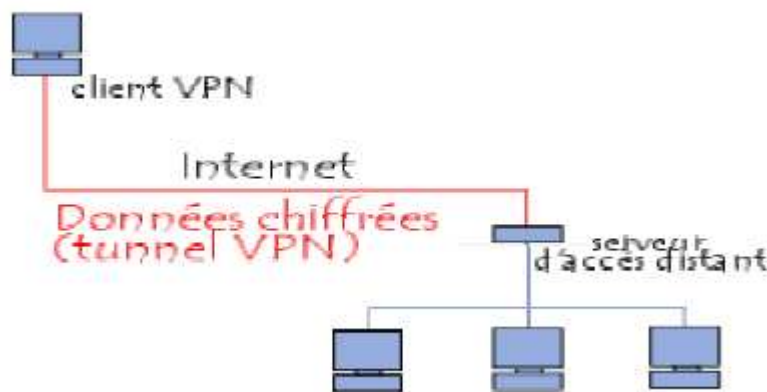


Figure II .3 : Tunnel VPN [16]

II.4.Les principaux avantages d'un VPN :

- Continuité : assure la continuité de transmission de donnée
- Sécurité : assure des communications sécurisées et chiffrées
- Economie : utilise internet en tant que média principal de transport, ce qui évite les couts liée à une ligne dédiée.

II.5.Les caractéristiques d'un VPN.[4]

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur** : seuls les utilisateurs autorisés doivent avoir accès au canal VPN.
- **Cryptage des données** : lors de leur transport sur le réseau public les données doivent être protégées par un cryptage efficace.
- **Gestion de clé** : les clés de cryptage pour le client et pour le serveur doivent pouvoir être générées et régénérées
- **Prise en charge multi protocole** : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux public en particulier IP.

II .6. Les différentes architectures possibles : [4]

- **De poste à poste :**

C'est le cas d'utilisation le plus simple. Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de bases de données entre deux serveurs d'une entreprise disposant de chaque côté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation.

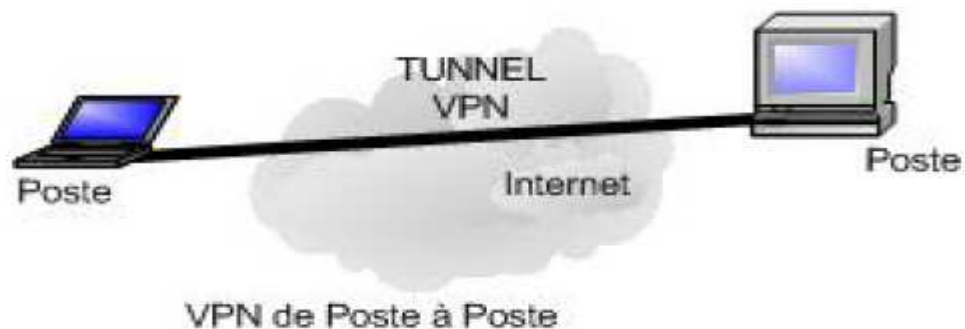


Figure II .4 : VPN de poste à poste.

- **De poste à site :**

Un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion Internet. Le développement de l'ADSL favorise ce genre d'utilisation. Attention toutefois à interdire l'accès Internet depuis le poste «localement». Pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise. Ce point est important et rejoint la réflexion plus large de la sécurité des sites mis en relation par un VPN. Lorsque les niveaux de sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux. S'il existe une faille de sécurité sur un site (ou sur un poste nomade), celle-ci peut être exploitée.

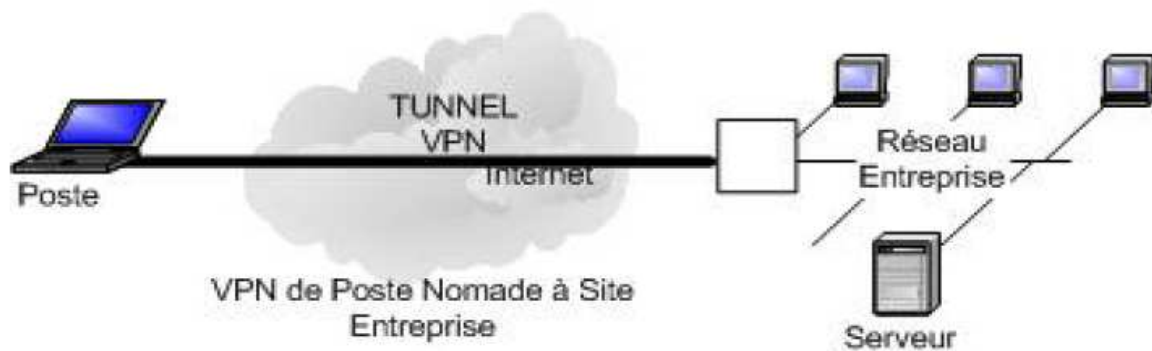


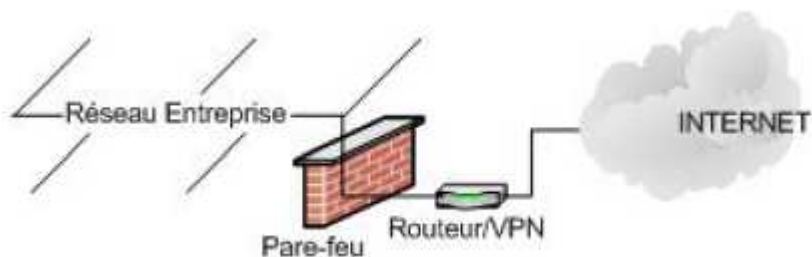
Figure II. 5 : VPN de poste Nomade à site Entreprise.

- **De site à site :**

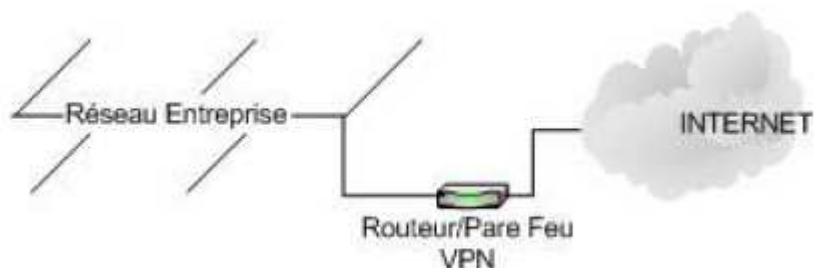


Différentes installations peuvent être mises en place pour la connexion de deux sites distants à l'aide d'un VPN :

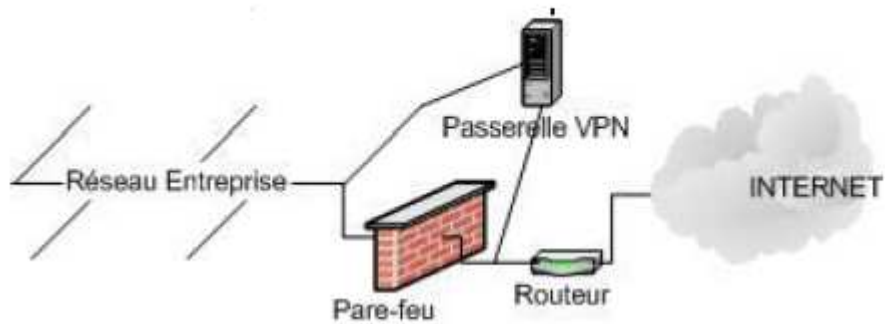
- a. **Routeur/VPN placé après le pare-feu :**



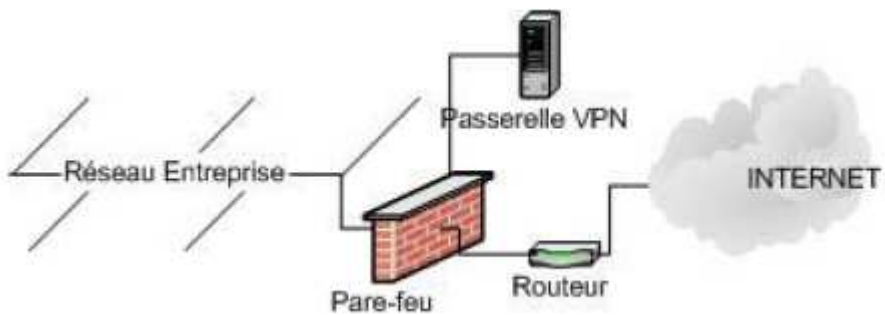
- b. **Routeur/pare-feu/VPN intégré :**



- c. **Passerelle VPN situé en parallèle du pare-feu** : le flux de données passant par la passerelle VPN n'est pas traité par le pare-feu :



- d. **Pare-feu, Routeur et Passerelle VPN en DMZ**



II.7.Description du fonctionnement : [16]

II.7.1.le protocole PPP :

Le protocole PPP (Point to Point Protocol) n'est pas un protocole permettant l'établissement d'un VPN mais il est très souvent utilisé pour transférer les informations au travers d'un VPN. . Ce protocole permet le multiplexage simultané de plusieurs protocoles de niveau 3 du modèle OSI. Il encapsule des paquets IP, IPX , ... dans des trames PPP, puis transmet ces paquets PPP encapsulés à travers la liaison point à point. PPP est donc utilisé entre un client distant et un serveur d'accès distant.

Les différentes méthodes d'authentification :

- **Le protocole PAP :**

Le protocole PAP (Password Authentication Protocol ou le protocole d'authentification par mot de passe) est une méthode simple pour établir l'identité du site distant. Elle est semblable à la procédure login d'une session sur un serveur. Cette procédure est effectuée seulement après que la liaison ait été établie. Dans le cadre d'une authentification utilisant le protocole PAP, le client s'authentifie auprès du serveur en lui envoyant un paquet « Authentication-Request » contenant l'identité du client et le mot de passe associé. Le serveur compare ces données à celle contenu dans son fichier d'authentification.

L'inconvénient de cette technique est que le mot de passe transite « en clair » sur la liaison.

- **Le protocole CHAP :**

Le protocole CHAP (Challenge Handshake Authentication Protocol) est un protocole d'authentification pour PPP à base de challenge, ce qui le rend bien plus sûr que son pendant PAP .Dans le cadre de l'utilisation du protocole CHAP, le serveur envoie au client un paquet contenant un challenge (mot de 16 bits) défini aléatoirement et son nom. Le client récupère dans sa table définie localement, à l'aide du nom du serveur, le secret correspondant. Le client combine le secret approprié avec le challenge, chiffre ce résultat et le résultat du chiffrement est retourné au serveur avec le nom du client. Le serveur effectue alors les mêmes opérations et si les deux résultats sont identiques la connexion du client est acceptée.

Format de la trame PPP :

Fanion	Adresse	Contrôle	Protocole	Données	FCS	Fanion
01111110	11111111	00000011	16 bits		16 bits	01111110

Figure II .6 : Format d'une trame PPP.

II.7.2 : Les différents protocoles utilisés pour l'établissement d'un VPN

Il existe quatre protocoles principaux permettant l'établissement d'un VPN :

- Le protocole PPTP (Point to Point Tunneling Protocol) mis au point par la société Microsoft ;

- Le protocole L2F (Layer Two Forwarding) mis au point par la société CISCO ;
- Le protocole L2TP (Layer Two Tunneling Protocol) ;
- Le protocole IPSEC.

PPTP et L2TP sont tous deux des protocoles de niveau 2.

- **Le protocole PPTP :**

PPTP (Point to Point Tunneling Protocol) est le protocole standard pour créer des VPN sous Windows. Il encapsule les paquets dans du PPP, lui-même encapsulé dans du GRE (Generic Routing Encapsulation). PPTP permet à PPP d'être transporté dans un tunnel au travers d'un réseau IP mais n'apporte aucun changement au protocole PPP. PPTP emploie deux canaux : une connexion de contrôle et une connexion de données avec GRE. PPTP permet le chiffrement des données PPP mais aussi leur compression et confère au protocole, un niveau supplémentaire de sécurité et de communication multi-protocolaire sur internet.

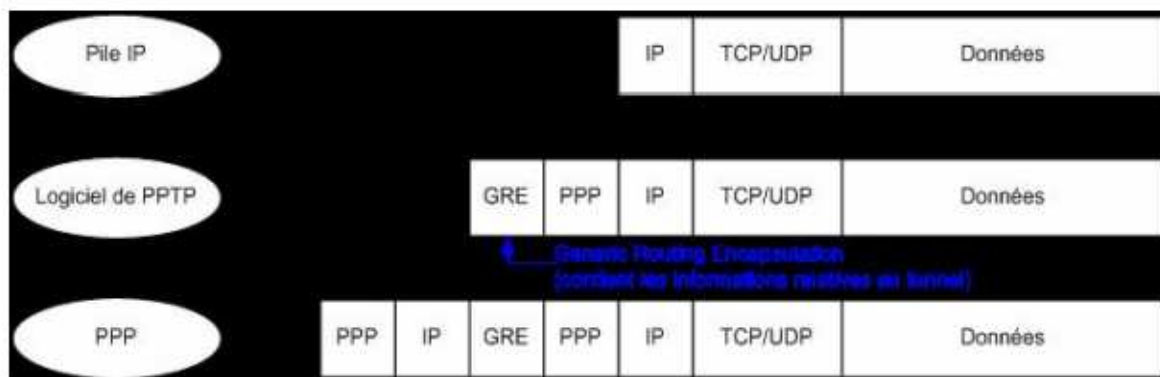


Figure II.7 : Format de trame PPTP.

L'avantage principal de ce protocole est que le client est disponible pour toutes les versions de Windows depuis Windows 95. De plus il est extrêmement facile à configurer.

Cependant PPTP a un gros inconvénient. Effectivement ce protocole a de nombreuses failles de sécurité :

- hachage de mot passe faible
- défaut de conception du protocole challenge/réponse
- erreur dans l'implémentation du protocole de chiffrement
- ...

Pour pallier à ces failles, Microsoft ont créé PPTPv2. Ce protocole a donc supprimé une grande partie des failles de sécurité. Cependant ce protocole est toujours vulnérable à des attaques hors-ligne visant à deviner le mot de passe. C'est pourquoi, actuellement, PPTP n'est pas recommandé pour des applications où la sécurité est un facteur très important.

- **Le protocole L2F :**

Le protocole L2F (**L**ayer **2** **F**orwarding ou transfert de couche 2), protocole développé par CISCO. Il permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Le serveur L2F désencapsule les paquets et les envoie sur le réseau.

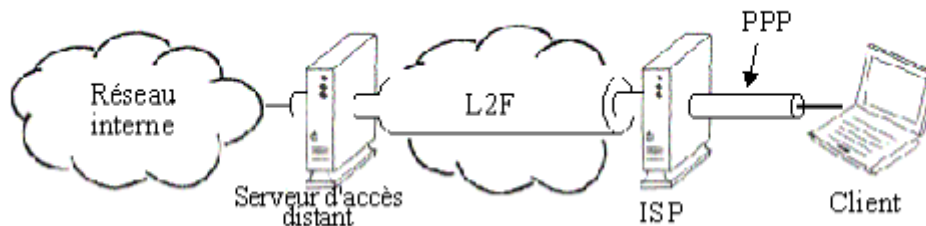


Figure II.8 : Tunnel L2F.

- **Le protocole L2TP :**

L2TP résulte de la fusion des protocoles PPTP et L2F et permet d'encapsuler PPP et de le transporter sur UDP. L2TP permet le transport en tunneling de trames PPP par-dessus un réseau de transit de manière aussi transparent que possible pour les applications et les utilisateurs.

L2TP apporte des fonctionnalités de sécurité comme l'authentification et le chiffrement (CHAP, secret communs, etc.). Cependant ces fonctionnalités semblent peu importantes par rapport aux mécanismes apportés par IPSec. De plus ces fonctionnalités, sur L2TP, ne sont pas forcément de bout en bout. Une des alternatives est de sécuriser L2TP avec IPSec, qui encapsule le L2TP dans l'en-tête ESP.

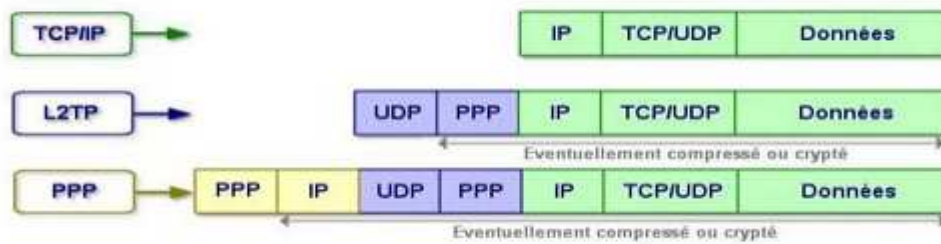


Figure II.8 : encapsulation L2TP

II.7.3. Le protocole de Niveau 3 : IPSEC : [16]

Aujourd'hui, le protocole le plus utilisé pour la mise en place des VPN est IPsec. Il est l'un des standards le plus diffusé et le plus ouvert. Effectivement IPsec offre plusieurs services : le chiffrement, le contrôle d'intégrité et l'authentification. De plus, il est nativement implémenté dans IPV6 qui le rend par conséquent comme le protocole incontournable pour les communications sécurisées dans les années à venir.

Les objectifs de la sécurité d'IPsec sont :

- Authentification de l'origine des données pour le trafic IP par signature RSA.
- Contrôle d'intégrité des paquets IP par la fonction hmac_md5, hmac_sha_1.
- Confidentialité des données assurée par le chiffrement symétrique DES, 3DES, AES...
- Confidentialité limitée du flux d'esprit.
- Protection anti-rejeu : les paquets chiffrés capturés ne seront pas acceptés en cas de rejeu.
- Contrôle des accès : seul le trafic qui rencontre une politique spécifique est autorisé au niveau des accès.

Les fonctionnalités d'IPsec peuvent être implémentées soit directement dans le système d'exploitation, soit ajoutées en tant que composant optionnel sous la forme d'un ensemble logiciel spécifique ou d'un équipement matériel indépendant.

IPsec fonctionne selon deux modes différents : mode transport et mode tunnel.

Le mode transport conserve l'en-tête IP original.

Le mode tunnel crée un nouvel en-tête IP pour envoyer le paquet original par le tunnel.

Ces deux modes s'appliquent aux VPN. Le mode transport est utilisé pour sécuriser le trafic dans les tunnels créés par L2TP ou GRE, tandis que le mode tunnel combine sécurité et tunneling pour IPsec.

a. Protocoles liée au traitement des paquets (ou Format IPSec)

IPSec autorise deux formats d'en-tête : AH et ESP.

- AH (Authentication Header), défini dans le RFC 2402

Le protocole AH garantit l'authentification de l'origine des données, le contrôle d'intégrité de l'ensemble du paquet (données + en-têtes IP) et des services anti-rejeu limités et optionnel. AH ne garantit pas la confidentialité et n'est donc pas accompagné d'un algorithme de chiffrement. L'en-tête AH est positionné entre l'en-tête IP et l'en-tête du protocole de la couche supérieure.

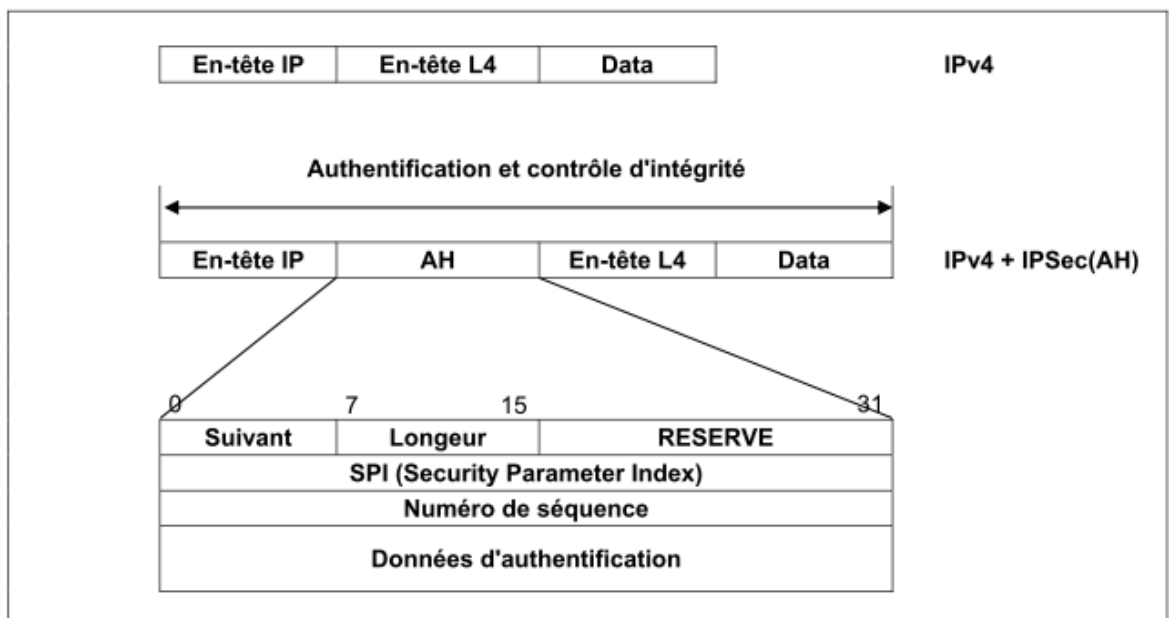


Figure II.9: En-tête AH

Le champ le plus important de cet en-tête est le champ Données d'authentification. Ce champ est de taille variable et contient le résultat de la fonction de vérification de l'intégrité. Cette fonction calcule l'ICV (Integrity Check Value) qui est généré à partir des champs immuables de l'en-tête IP (version, taille, source, ...), des champs de l'en-tête pouvant être modifiés mais prédictibles (adresse de destination), de certains champs de l'en-tête AH et des données (au sens IP du terme, soit tout ce qui reste après l'en-tête AH). L'ICV est un MAC (Message Authentication Code). Tous les champs de cet en-tête sont détaillés dans l'annexe.

- ESP (Encapsulating Security Payload), défini dans le RFC 2406

Le protocole ESP est un en-tête de protocole inséré dans un datagramme IP pour garantir la confidentialité, l'authentification de l'origine des données, l'anti-rejeu et les services d'intégrité des données.

ESP garantit la confidentialité grâce à une unité de chiffrement et l'intégrité des données grâce à un authentifiant. Dans un paquet IPv4, un nouvel en-tête généré par ESP est inséré immédiatement après l'en-tête IP. Avec IPv6, l'en-tête généré par ESP devient l'une des extensions d'en-tête.

Avant d'ajouter l'en-tête qui lui est propre, le protocole ESP réalise le chiffrement des données et ajoute les octets de padding (remplissage due à l'utilisation de certains algorithmes de chiffrement), si nécessaire.

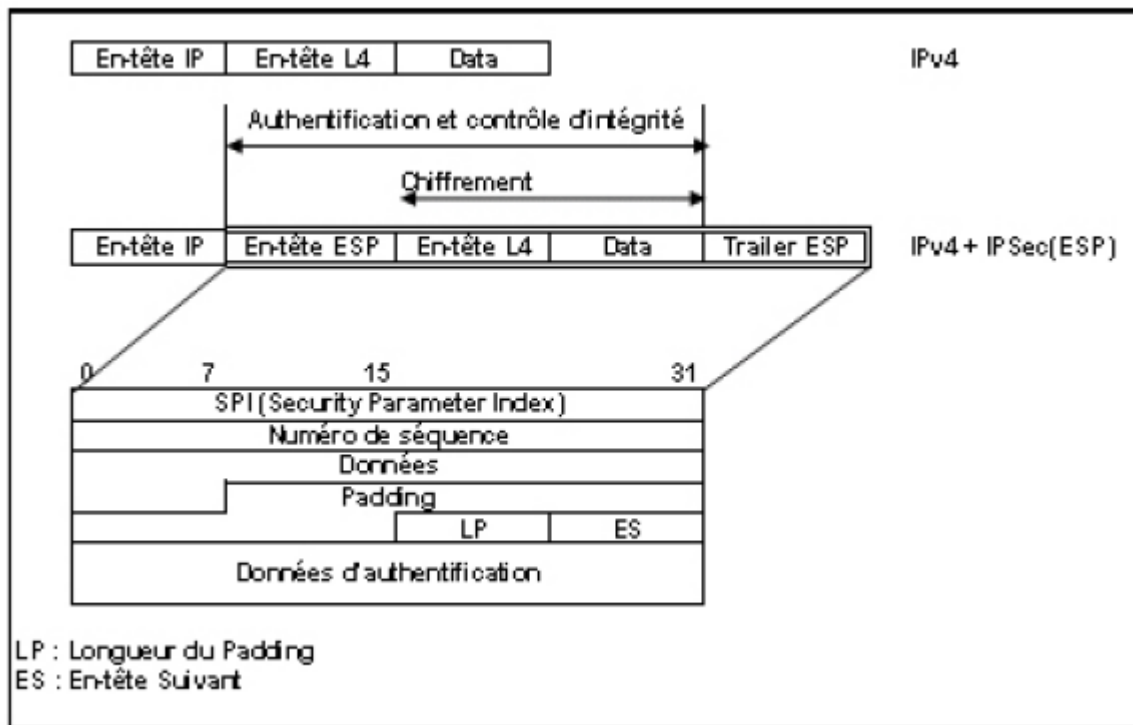


Figure II.10 : En-tête ESP

- AH et ESP

Il est également possible de cumuler les deux modes, ESP et AH afin d'obtenir la protection des données (chiffrement via ESP et authentification et contrôle d'intégrité de la partie ESP) et l'authentification et le contrôle d'intégrité de tout le paquet grâce à AH.

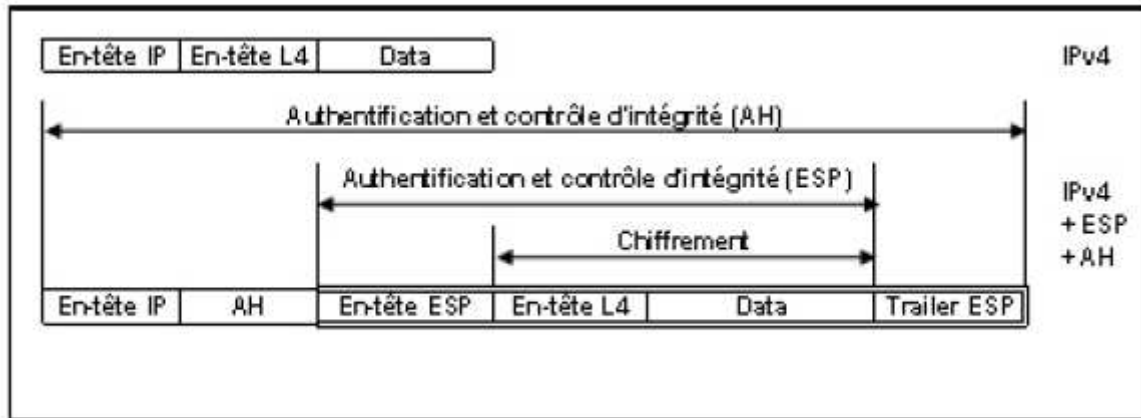


Figure II.11 : En-tête AH et ESP.

b. SA (Security Association) :

Il est important que la politique de sécurité IPSec soit configurée de manière cohérente sur les homologues IPSec. Pour cela, on définit des associations de sécurité (SA) qui sont conservées dans une base de données et, comme cette dernière contient des informations sensibles, elle doit être placée dans un endroit sûr dont l'accès est sévèrement contrôlé. Cette SA définit l'ensemble des opérations IPSec devant être appliquées aux datagrammes qui y affèrent.

Chaque SA contient un certain nombre de paramètres. Quelques-uns peuvent être utilisés comme des sélecteurs désignant quels types de paquets doivent être protégés. On peut utiliser l'adresse IP de la source et de la destination, les numéros de port et les types de protocoles comme sélecteurs.

Une SA est une relation à sens unique entre un émetteur et un destinataire. Par conséquent les SA sont unidirectionnelles. Pour protéger le trafic dans les deux directions, on doit établir deux SA.

Les SA contiennent les éléments suivants :

- **L'index des paramètres de sécurité** ou SPI.
- **L'adresse IP de la source et de la destination.**
- **Le nom** : soit l'identifiant d'un utilisateur, soit le nom d'une machine. Un identifiant d'utilisateur permet de différencier le trafic issu d'une personne en particulier.

- **Le protocole de sécurité** : AH ou ESP.
- **Les paramètres d'authentification** : algorithme de chiffrements, clés...
- **Les protections contre la répllication** : un compteur de séquences et un indicateur de dépassement de séquence. Le compteur génère le numéro de séquence des en-têtes AH et ESP. Il est positionné à 0 lors de l'établissement de la SA et est incrémenté de 1 chaque fois que vous utilisez la SA pour sécuriser un paquet.
- **Le mode utilisé** : mode transport ou mode tunnel.
- **La durée de vie de la SA** indiquée en unité de temps ou en nombres d'octets. Lorsqu'une association de sécurité expire, les paquets qui lui sont associés sont généralement détruits jusqu'à ce qu'une nouvelle SA soit négociée. Pour éviter la destruction des paquets, il est possible de négocier une nouvelle SA avant que la précédente expire.
- **Les paramètres de fragmentation (PMTU).**

SPI	IP source	IP destination	Protocole de sécurité	Mode	Paramètres de la SA (clés, etc)	Type	Pointeur vers les entrées SPD
580	192.168.2.1	192.168.4.1	ESP	Tunnel	...	Entrant	7

Figure II. 12 : Exemple d'une base SA

c. Les protocoles IPSec de gestion et d'échange de clés :

La présence de mécanismes de chiffrement implique la prise en compte des problématiques de gestion de clés et de leur distribution à l'ensemble des systèmes destinés à être source et/ou destination d'une communication IPSec.

Pour la gestion et la distribution des clés, je peux, soit opter pour une gestion manuelle dans le cas de petites infrastructures, soit pour une gestion automatique. Pour cela le protocole IKE (Internet Key Exchange), défini dans le RFC 2409, a été défini comme protocole par défaut pour la gestion et la distribution des clés. IKE est un protocole qui combine des éléments, des définitions et des fonctionnalités issus de protocoles tels que ISAKMP, SKEME et Oakley pour la gestion et l'échange de clés ou de SA.

Le protocole ISAKMP (Internet Security Association and Key Management Protocol), défini dans le RFC 2408, apporte une infrastructure permettant de définir et d'administrer des SA entre deux ordinateurs peuvent communiquer de manière sécurisée. ISAKMP a un DOI (Domain of Interpretation) défini pour être utilisé avec IPSec. Ce DOI permet de spécifier les formats et les conditions requises lorsqu'ISAKMP est appliqué à IPSec.

Le protocole IKE utilise l'infrastructure du protocole ISAKMP pour échanger des clés et définir des SA entre deux machines. IKE utilise également le protocole Oakley pour

la création des clés et le protocole SKEME pour les échanger. IKE permet donc de négocier automatiquement des SA. Il fonctionne sur UDP(via le port 500).

Les négociations IKE se font en deux phases :

- **phase I** : elle permet de mettre en place un canal sécurisé afin de protéger les négociations qui se déroulent lors de la deuxième phase.
- **Phase II** : elle permet de négocier les SA qui seront utilisées par IPSec pour protéger le trafic.

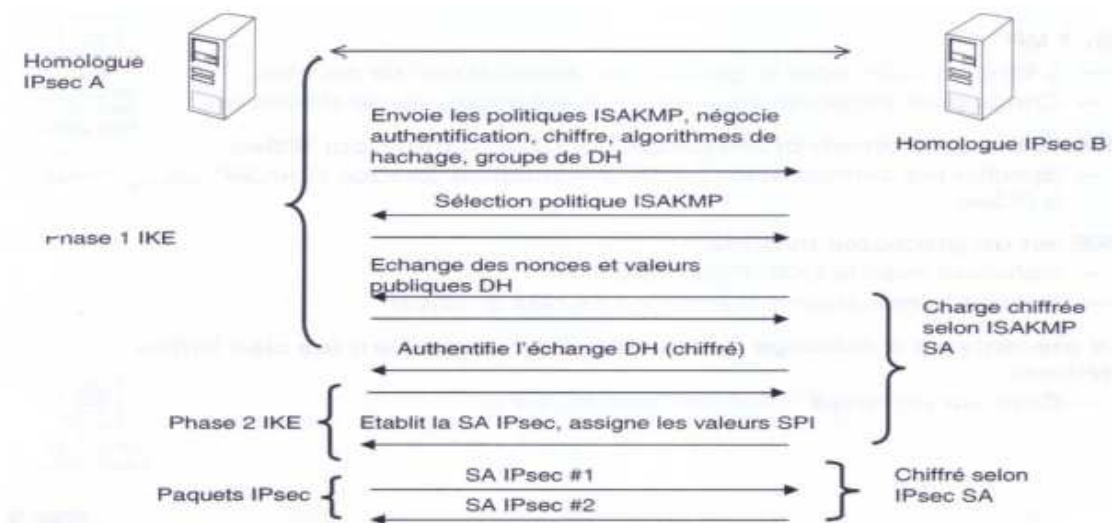


Figure II.12 : Echanges ISAKMP IKE.

- **IKE phase I :**

Le canal sécurisé est mis en place en négociant une SA ISAKMP entre les terminaisons. Il est noté que ces SA sont bidirectionnelles contrairement aux SA IPsec qui sont unidirectionnelles.

Il existe deux modes de fonctionnement pour cette phase : le mode principal et le mode agressif. Dans le mode principal, six échanges sont nécessaires (3 aller-retour). Les deux premiers échanges permettent de négocier les méthodes d'authentification (clés prépartagées, algorithme de clés publique, signatures numériques) et de chiffrement (DES, 3DES, AES), ainsi que les algorithmes de hachages (MD5, SHA-1) et les groupes

Diffie-Hellman (algorithme d'échange de clés). En effet le premier échange consiste en quelque sorte à une proposition de l'homologue IPSEC A sous forme d'une liste de protocoles au sein de laquelle l'homologue IPSEC B doit faire son choix. Ce choix est spécifié dans le deuxième échange. Dans les deux échanges suivants, les extrémités mettent en place les clés partagées qui sont échangées par l'intermédiaire du protocole Diffie-Hellman. Pour finir la phase I, les extrémités s'identifient mutuellement en utilisant les méthodes négociées lors des premiers échanges.

Dans le mode agressif, seulement trois échanges sont nécessaires. Ce mode est en fait une forme compacte du mode principal. Le nombre d'échange entre les terminaisons est le principal avantage de ce mode. Cependant il requiert une grande puissance de calcul puisque les opérations sont effectuées immédiatement en réponse au premier message et il est plus vulnérable. C'est pourquoi le groupe de travail d'IPSec songe à faire disparaître ce mode.

- **IKE phase II :**

Le protocole pour la deuxième phase des négociations s'appelle QM (Quick Mode). Ce mode rapide permet l'échange de trois messages et autorise les négociations ayant recours à une ou plusieurs SA. N'importe quelle extrémité peut prendre l'initiative et les SA qui seront négociées seront stockés dans la base de données SA de chaque extrémités. Avec QM, les deux parties se trouvent dans l'obligation de négocier un protocole IPSec ou une combinaison de protocoles qui sera utilisé par chaque SA. Comme dans la phase I, les extrémités échangent des propositions. Cette proposition comprend une liste de procédure de protection pour chaque SA négociée. De plus, chaque proposition est accompagnée d'informations complémentaires comme la durée de vie de la SA, un groupe de Diffie-Hellman, un indicateur de mode (mode transport ou tunnel) et des informations sur les clés.

II .8.Algorithmes utilisés par ipsec

Les algorithmes utilisés par IP sec sont :

II .8.1.Algorithmes symétrique

- **L'algorithme DES :**

Les États-Unis, ont tenté d'imposer un algorithme, unique, baptisé DES (Data Encryption Standard), en insistant sur les problèmes d'interopérabilité et aussi de sécurité et d'économie. La seule faiblesse révélée de cet algorithme est la longueur de la clé (56 bits), jugée trop courte pour les moyens de calcul actuels. La clé du DES est une chaîne de 64 bits (succession de 0 et de 1), mais en fait seuls 56 bits servent réellement à définir la clé. Les bits 8, 16, 24, 32, 40, 48, 56 et 64 sont des bits de

parité (c'est-à-dire bits de détection d'erreur). Le 8ème bit est calculé de sorte que sur les 8 premiers bits, il y ait un nombre impair de 1. Par exemple, si les 7 premiers bits sont 1010001, le 8ème bit est 0. Ceci permet d'éviter les erreurs de transmission.

Il y a donc pour le DES 2^{56} clés possibles, soit environ 72 millions de milliards possibilités.

Les grandes lignes de l'algorithme sont :

- **Phase 1** : Préparation - Diversification de la clé :
 1. Le texte est découpé en blocs de 64 bits.
 2. On diversifie aussi la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés $K_1, \dots, K_{16}$ à 48 bits. Les K_i sont composés de 48 bits de K, pris dans un certain ordre.
- **Phase 2** : Permutation initiale :
 1. Pour chaque bloc de 64 bits x du texte, on calcule une permutation finie $y=P(x)$. y est représenté sous la forme $y=G_0D_0$, G_0 étant les 32 bits à gauche de y , D_0 les 32 bits à droite.
- **Phase 3** : Itération :
 1. On applique 16 rondes d'une même fonction. A partir de $G_{i-1}D_{i-1}$ (pour i allant de 1 à 16), on calcule G_iD_i en posant :
 - $G_i=D_{i-1}$.
 - $D_{i-1}=G_{i-1} \text{ XOR } f(D_{i-1}, K_i)$: XOR est le OU exclusif bit à bit, et f est une fonction de confusion, suite de substitutions et de permutations.
- **Phase 4** : Permutation finale :
 1. On applique à $G_{16}D_{16}$ l'inverse de la permutation initiale.
 2. $Z=P^{-1}(G_{16}D_{16})$ est le bloc de 64 bits chiffré à partir de x .

Cet algorithme peut être représenté par le schéma ci-après :

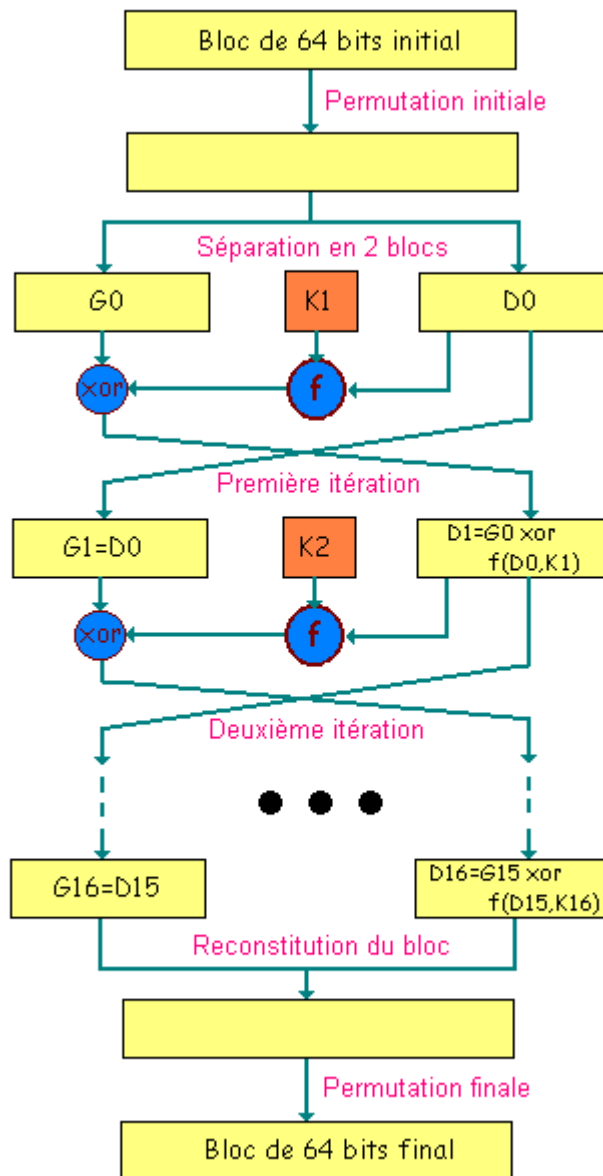


Figure II.13: Schéma de l'algorithme DES

- **L'algorithme Triple – DES (3-DES) :**

Face à la faiblesse de l'algorithme DES, la solution a semblé être dans un premier temps l'adoption de l'algorithme surnommé triple DES, algorithme consistant en trois applications de l'algorithme DES à la suite les uns des autres avec 2 clés différentes (d'où une longueur de clé de $2 \times 56 = 112$ bits) ou 3 clés différentes (d'où une longueur de clé de $3 \times 56 = 168$ bits). Les deux schémas suivants illustrent les deux implémentations possibles de l'algorithme triple-DES :



Figure II.14: Schéma de l'algorithme Triple – DES – 112 bits



Figure II.15: Schéma de l'algorithme Triple – DES – 168 bits

Si l'algorithme triple DES est largement suffisant à l'heure actuelle en terme de chiffrement d'informations, il est par contre trois fois plus lent que le DES. C'est pourquoi, le NIST (National Institute of Standards and Technologies) a lancé un nouvel appel d'offres pour créer un successeur au DES : l'AES (Advanced Encryption System).

- **L'algorithme AES :**

Le cahier des charges de l'algorithme AES comportait les points suivants :

- évidemment, une grande sécurité ;
- une large portabilité : l'algorithme devant remplacer le DES, il est destiné à servir aussi bien dans les cartes à puces, aux processeurs 8 bits peu puissants, que dans des processeurs spécialisés pour chiffrer des milliers de télécommunications à la volée ;
- la rapidité ;
- une lecture facile de l'algorithme, puisqu'il est destiné à être rendu public ;
- un chiffrement par blocs de 128 bits, les clés comportant 128, 192 ou 256 bits.

Les principaux inconvénients de chiffrement symétrique :

Le chiffrement symétrique des données, s'il présente l'avantage d'être rapide, présente néanmoins un certain nombre d'inconvénients :

- le nombre de clés secrètes à posséder augmente de façon exponentielle en fonction du nombre d'interlocuteurs ;
- le changement de clé doit être fréquent de manière à éviter une compromission de clés ;
- un mécanisme d'échange de clés de façon sécurisée doit être mis en place.

II .8 .2.Les algorithmes asymétriques

- **L'algorithme RSA :**

Le premier crypto-système asymétrique, RSA créé par Ronald Rivest, Adi Shamir et Leonard Adleman. Il repose sur la difficulté d'un problème proche de celui de la factorisation. Déchiffrer un message codé avec RSA sans connaître la clé secrète correspondante nécessite d'être capable de résoudre un problème très difficile.

Dans l'exemple suivant on va essayer d'établir un échange de message entre Alice et Bob en utilisant l'algorithme RSA pour mieux expliquer son principe.

Si Bob souhaite recevoir des messages chiffrés en utilisant l'algorithme RSA, il procède de la façon suivante :

Phase 1 : Création des clés : Bob crée 4 nombres p , q , e et d : p et q sont deux grands nombres premiers distincts. Leur génération se fait au hasard, en utilisant un algorithme de test de primalité probabiliste. Le produit de ces deux nombres est noté n ;

e est un entier premier avec le produit $(p-1)(q-1)$;

d est tel que $ed=1$ modulo $(p-1)(q-1)$ c'est-à-dire que $ed-1$ est un multiple de $(p-1)(q-1)$.

Phase 2 : Distribution des clés : Le couple (n, e) constitue la clé publique de Bob qu'il rend disponible à tous. Le couple (n, d) constitue sa clé privée. Bob garde celle-ci secrète.

Phase 3 : Envoi du message codé : Alice veut envoyer un message chiffré à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et $n-1$. Alice possède la clé publique (n, e) de Bob. Elle calcule $C=M^e \bmod n$. C'est ce dernier nombre qu'elle envoie à Bob.

Phase 4 : Réception du message codé : lorsque Bob reçoit C , il calcule à l'aide de sa clé privée $D=C^d \bmod n$. D'après un théorème du mathématicien Euler, $D=M^{de}=M \bmod n$. Il a donc reconstitué le message initial.

II .8.3.Les fonctions de hachages

Une fonction de hachage est une fonction qui calcule à partir d'une large chaîne de caractères une chaîne de caractère réduite. Le résultat est dénommé un « digest » ou « empreinte ». Une fonction de hachage permet de représenter les données de façon certaine tout en réduisant la taille utile qui sera réellement chiffrée.

Les algorithmes de hachage les plus utilisés sont :

- MD4 et MD5 (Message Digest version 4 et 5) qui furent développées par Ron Rivest. MD5 produit des hachés de 128 bits en travaillant les données originales par blocs de 512 bits.

- SHA-1 (Secure Hash Algorithm, Algorithme de Hachage Sécurisé version 1), comme MD5, est basé sur MD4. Il fonctionne également à partir de blocs de 512 bits de données et produit par contre des condensés de 160 bits en sortie.
- SHA-2 (Secure Hash Algorithm 2) a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits. Il sera bientôt la nouvelle référence en termes de fonction de hachage.

Conclusion

IPsec est un protocole très complet qui peut répondre à beaucoup de besoins en matière de sécurité et s'adapter à de nombreuses situations. Sa conception en fait un système très sûr et sa nature de norme garantit l'interopérabilité entre les équipements de différents fournisseurs. Ces avantages, couplés à la prédominance grandissante du protocole IP, font d'IPSec un acteur important de la sécurité des réseaux informatiques.

Dans le chapitre suivant je vais utiliser ce protocole pour implémenter un VPN site-à-site.

I. Introduction :

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

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

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

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



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

II. Présentation de l'ENIEM

a. Situation géographique

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

b. Activités de l'entreprise

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

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

II.1. Unité froid : elle est composée de 3 lignes de production:

a. Une ligne de fabrication de réfrigérateur petit modèle :

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

b. Une ligne de réfrigérateurs grands modèles :

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

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

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

II.2. Unité Cuisson :

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

II.3.Unité Climatisation :

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

II.4.Unité Commerciale :

Ses activités sont :

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

II.5.Unité Prestations Techniques :

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

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

Organigramme générale de l'entreprise

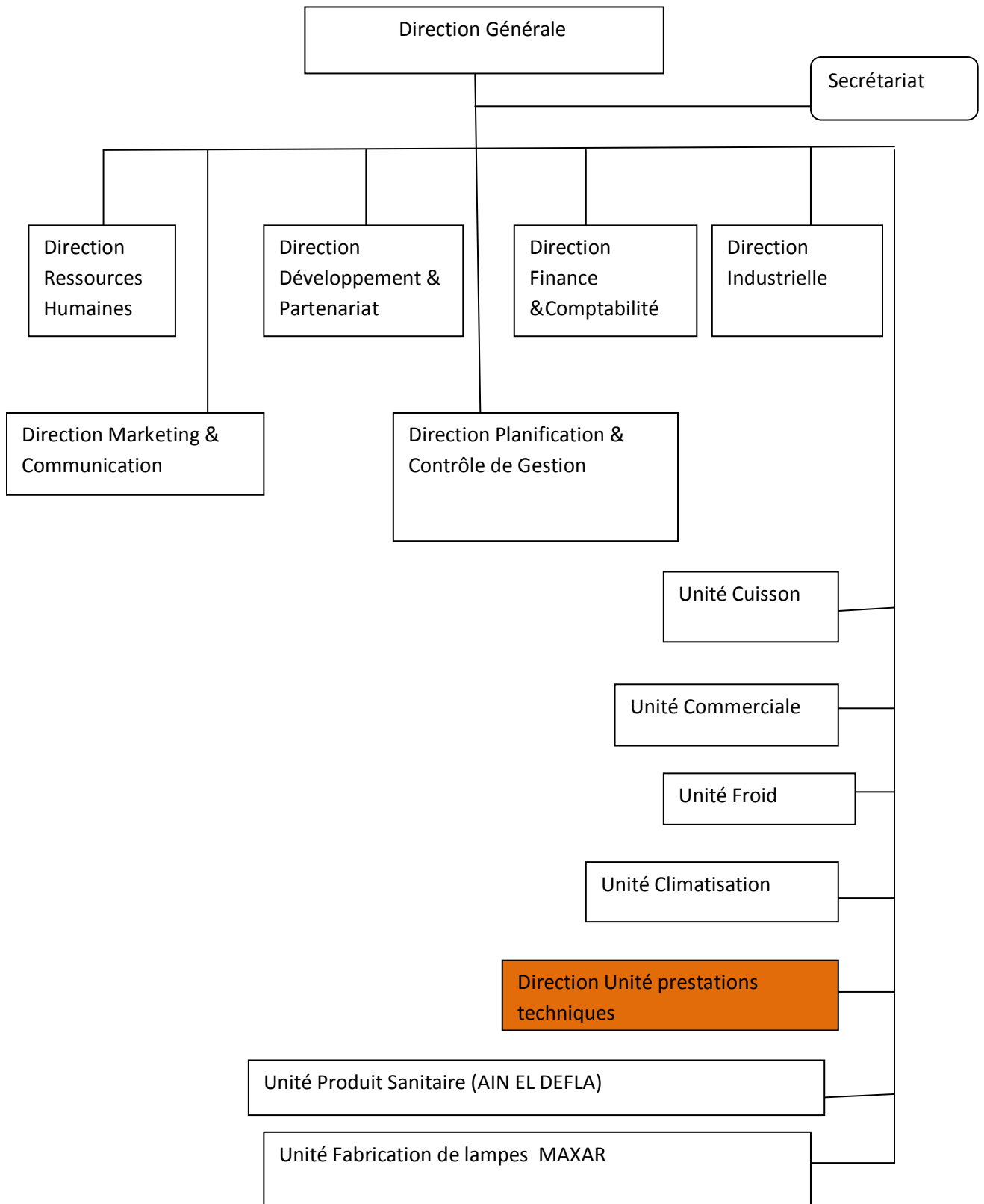


Figure III.2 : Organigramme générale de l'entreprise

III. Présentation du champ d'études :

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

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

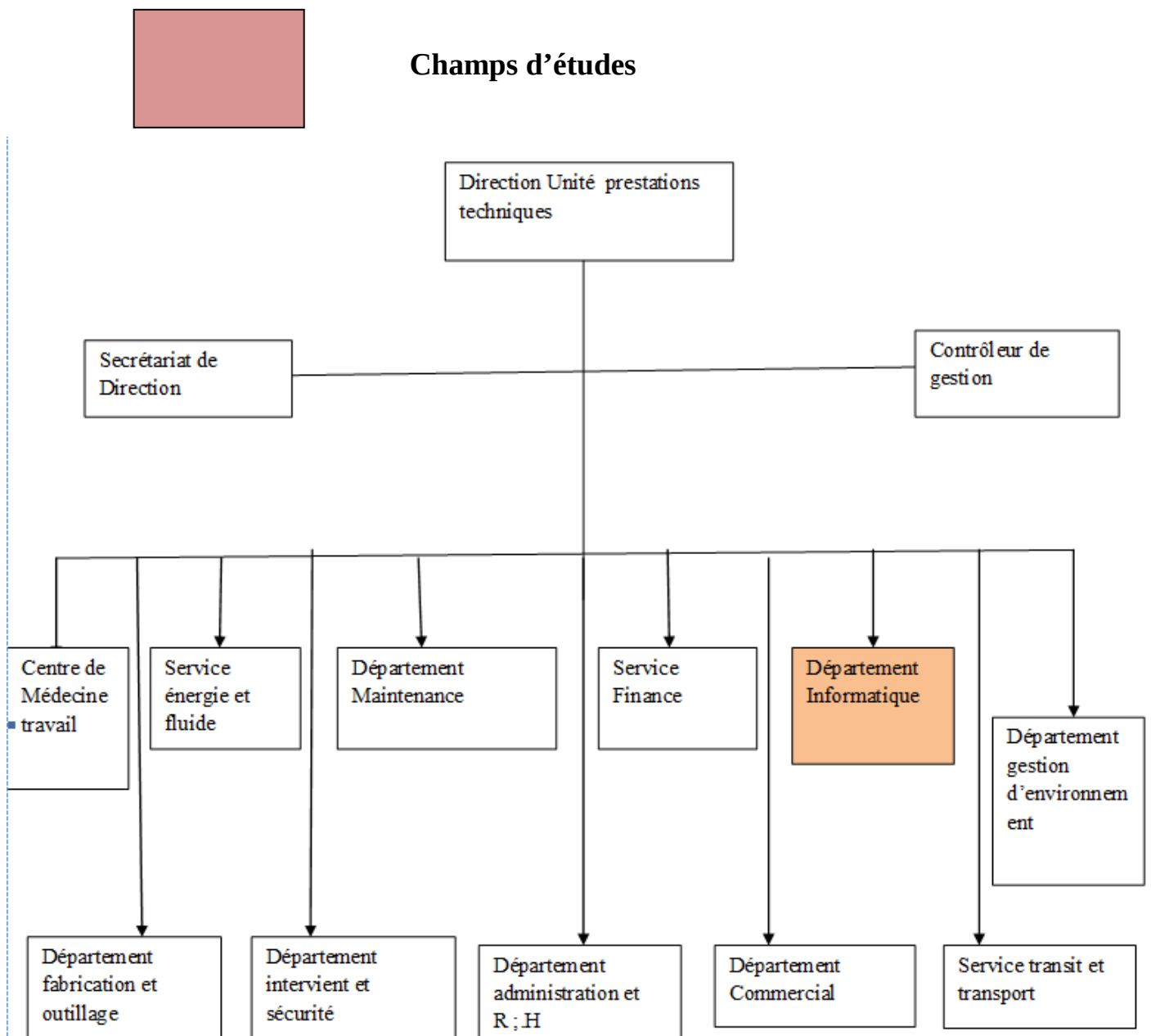


Figure III.3: Unité de Prestation Technique

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

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

II.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, Rugged Writer 480) reliés au serveur (HP3000/A500) par des liaisons directes (distances inférieures ou égales à 1200mètres), modem (pour les distances supérieures à 1200mètres), et multiplexeur modem (pour les installations de plusieurs terminaux distants).

- Caractéristiques de ce réseau :

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

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

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

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

II.2.Les armoires de brassage existantes :

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

.Elle est constituée des éléments suivants :

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

Chapitre III : Présentation de l'Organisme d'Accueil

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

Cette figure nous présente l'armoire d'étage centrale (fig. III.4)



Fig. III.4 L'armoire d'étage centrale

- **L'armoire de brassage (Fig. III.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. III.5 L'armoire de brassage

II.3.Description du système du serveur HP3000/A500 :

- **La face arrière (Fig. III.6):**

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

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

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

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

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

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

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

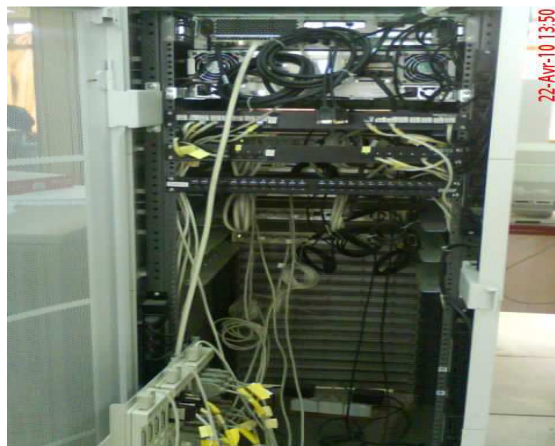


Fig. III.6 La face arrière

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

Elle est composée des éléments suivants :

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



Fig. III.7 La face avant

II.4.Caractéristiques matériels et logicielles

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

Tableau des Caractéristiques matérielles et logicielles

II.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 autres machines clientes

IV. Présentation du Département Informatique de l'ENIEM

IV.1 Organigramme de département informatique :

Le département informatique se compose de deux services :

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

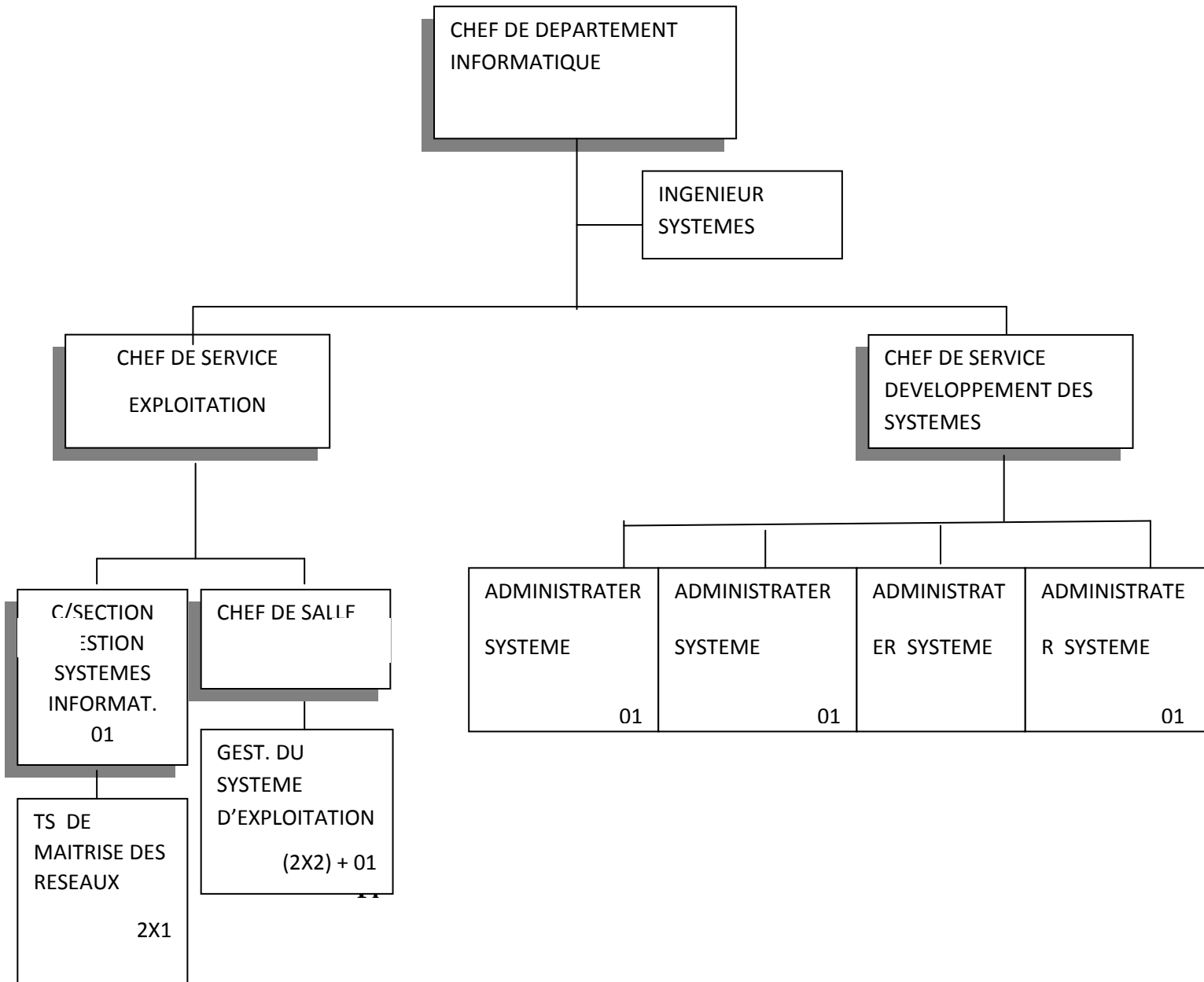


Figure III.8: Organigramme de département informatique

IV.2 Aspect humain

IV.2.1 Chef de département :

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

IV.2.2 Chef de service exploitation :

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

- **Agent maintenance et réseau informatique :**

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

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

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

IV.2.3 Chef de service développement système informatique :

La 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 phases 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.

V. Conclusion :

Dans ce chapitre, les ressources constituant 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.

IV.I-CONCEPTION :

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

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

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

I.2.présentation du réseau existant :

Comme la figure le montre le réseau existant contient :

- Sept SWITCH
- Un server de base de données
- Un server web
- Un SWITCH fédérateur
- Des ordinateurs (pc)
- Un modem pour une connexion au réseau internet

En effets, six SWITCHs de ce réseau sont départagés dans deux bâtiments et chaque bâtiment est composé de trois étages (donc en tout on a six étages) et il ya un SWITCH dans chaque étage de chaque bâtiment, et ils désignent les unités de l'ENIEM suivantes : Unité froid, Unité climatisation, Unités cuisson, et département informatique tan-dis-que le septième SWITCH appartient à l'unité prestation technique qui se trouve au sous sol du bâtiment.

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

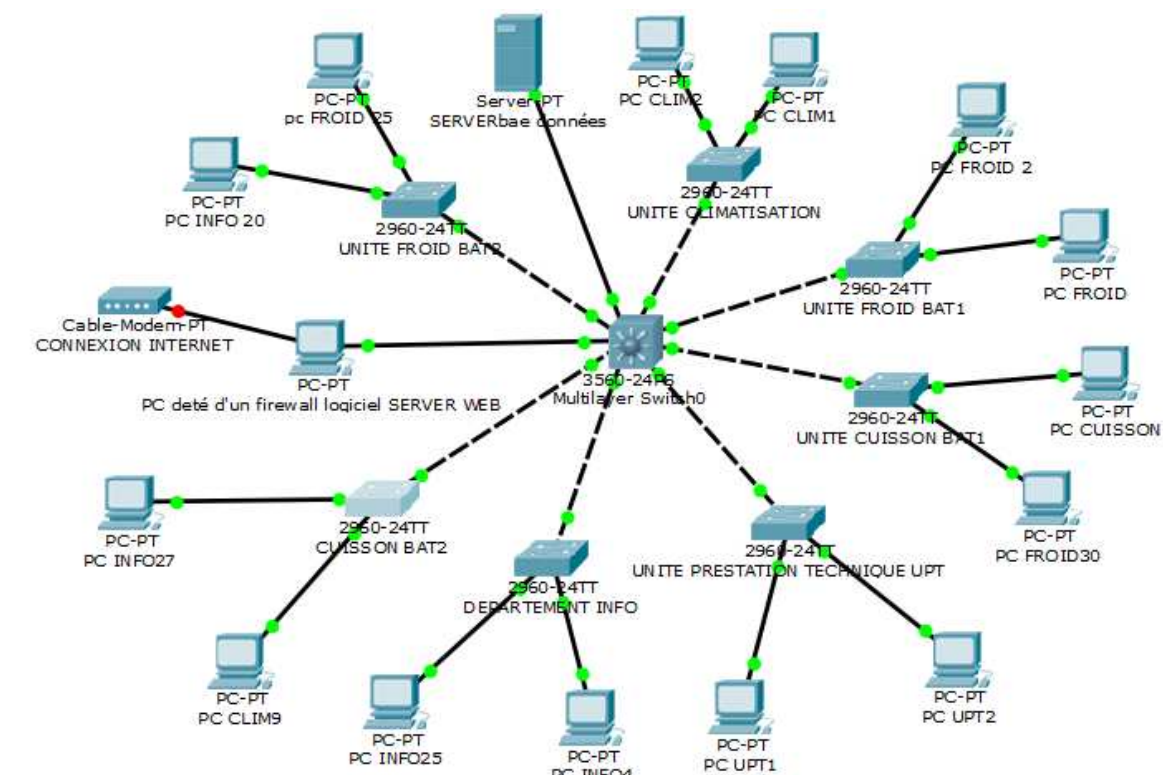


Figure IV.1 : présentation du réseau existant

I.3. fonctionnement du réseau existant :

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

Ainsi le réseau mis en œuvre dans la figure V.I.2 indique qu'un ordinateur peut émettre un trafic vers n'importe quel destinataire voulu et aussi, recevoir du n'importe quelle source. Donc tout les PCs se connectent entre eux.

➤ Explication

La configuration de tous les équipements d'interconnexions (les SWITCH, le fédérateur) présentés dans la figure est dit : configuration basique cela veut dire que cette configuration est limitée à l'utilisation d'un seul VLAN par défaut (natif) et que la configuration des switches n'utilise que des mots de passes et une adresse IP, autrement dit tous les SWITCHs se trouvent dans un seul sous réseau et c'est ce que explique le fait que tous les SWITCHs, 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 relié à l'un des ports libres qui se trouvent dans le switch de l'unité cuisson.

I.4. Les critiques du réseau existant :

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

-  **Critique1** : les switchs du réseau sont configurables mais non configurés.
Exemple tout les switch sont considérés comme des switchs simples .
-  **Critique 2** : le réseau est installé anarchiquement et non administré.
Exemple : 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.
Exemple : la sécurité du réseau existant est basée uniquement sur l'utilisation d'un firewall logiciel.
-  **Critique4** : manque d'une interconnexion entre l'entreprise ENIEM et sa direction générale.

I.5. Solutions proposées :

A l'issue d'une étude préalable de l'unité prestation technique au sein de l'entreprise nous avons opté pour l'implémentation du plans de sécurité suivants :

- ❖ La Segmentation du Réseau local en VLAN pour renforcer la Sécurité interne.
- ❖ Installation d'un routeur pour relier l'entreprise ENIEM au routeur de sa direction générale (DG), et réalisation d'un VPN site à site entre l'entreprise ENIEM et sa direction générale afin de sécuriser l'interconnexion entre eux.

IV.II. Réalisation

II.1. Outils utilisés pour la réalisation du projet :

➤ Emulateur GNS3 (Graphical Network Simulator)

GNS3 est un Émulateur de retours Cisco qui permet de manipuler IOS (Internetwork Operating System) Cisco et de les utiliser en émulation complète sur un simple ordinateur.

- **Wireshark** : C'est un sniffer qui permet d'écouter le trafic réseau.. .
- **Routeurs CISCO** avec 2691 avec IOS Advanced-Sécurité.
- **PC à 4G de RAM**

I.2.Topologie pour la Simulation d'une liaison VPN site-à-site :

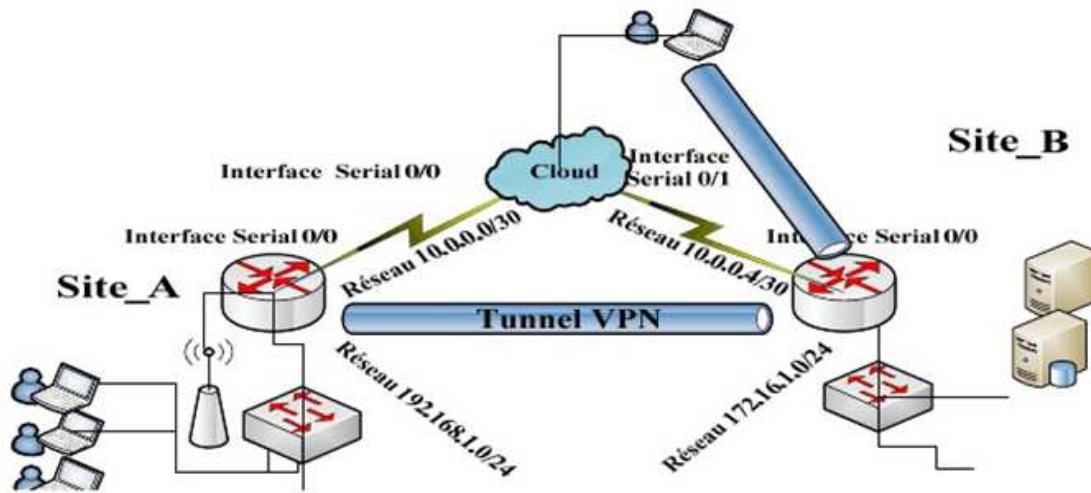


Figure IV.2: Topologie du réseau

I.3. Configuration de VPN site to site :

I.3.1. Etablissement d'un tunnel Ipcsec site-à-site :

Il faut savoir que le VPN se configure juste sur les Routeurs d'extrémités dans ce cas c'est Router (R2) et Router(R3) :

I.4. Table d'adressage

Équipements	Interface	Adresse ip	Masque sous réseau	Passerelle par défaut	Area
R1	loopback 0	1.1.1.1	255.255.255.255	N /A	0
	f0/0	200.1.1.1	255.255.255.0	N /A	0
	f0/1	200.2.2.1	255.255.255.0	N /A	0
R2	loopback 0	1.1.1.2	255.255.255.255	N /A	0
	f0/0	200.1.1.2	255.255.255.0	N /A	0
	f0/1	10.1.1.2	255.255.255.0	N /A	1
R3	loopback 0	1.1.1.3	255.255.255.255	N /A	0
	f0/0	200.2.2.3	255.255.255.0	N /A	0
	f0/1	10.2.2.3	255.255.255.0	N /A	2

Tab. IV.1 : Table d'adressage

D'où on aura la topologie suivante :

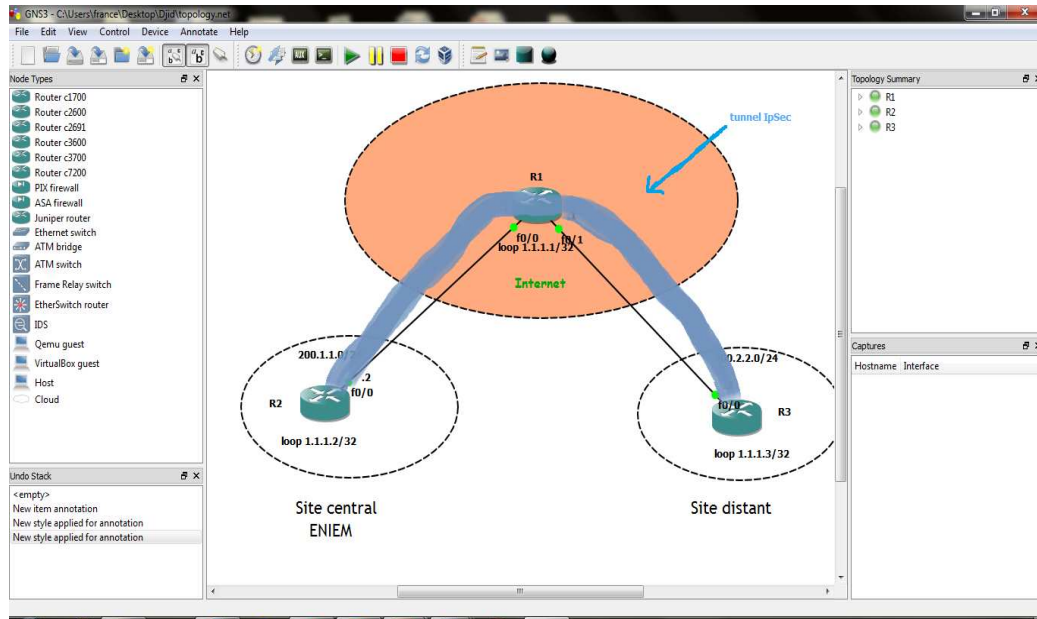


Figure IV.3 : Architecture du réseau.

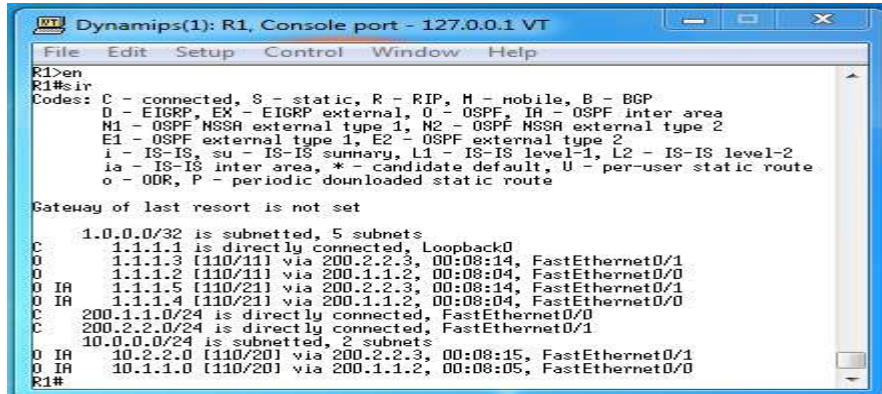
I. 5. Configuration de base des routeurs :

- Les noms des routeurs.
- Configuration des lignes consoles et VTY
- Configuration des interfaces séries et fastethernet.
- Configuration de routage dynamique.
- Test de connexion et de routage avec la commande Ping et show.

I.5.1. Test de connexion et de routage :

Résultat de la commande « show ip route » ou en utilisant l'alias « sir », pour :

- R1 :



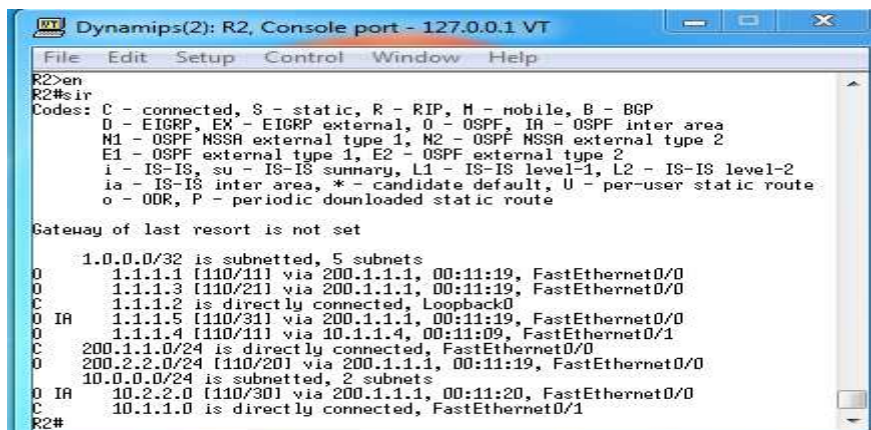
```
Dynamips(1): R1, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R1>en
R1#sir
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        M1 - OSPF NSSA external type 1, M2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 5 subnets
    C      1.1.1.1 is directly connected, Loopback0
    O      1.1.1.3 [110/11] via 200.2.2.3, 00:08:14, FastEthernet0/1
    O      1.1.1.2 [110/11] via 200.1.1.2, 00:08:04, FastEthernet0/0
    O IA   1.1.1.5 [110/21] via 200.2.2.3, 00:08:14, FastEthernet0/1
    O IA   1.1.1.4 [110/21] via 200.1.1.2, 00:08:04, FastEthernet0/0
    C      200.1.1.0/24 is directly connected, FastEthernet0/0
    C      200.2.2.0/24 is directly connected, FastEthernet0/1
    C      10.0.0.0/24 is subnetted, 2 subnets
    O IA   10.2.2.0 [110/20] via 200.2.2.3, 00:08:15, FastEthernet0/1
    O IA   10.1.1.0 [110/20] via 200.1.1.2, 00:08:05, FastEthernet0/0
R1#
```

Figure IV .4 : Résultats de la commande sir pour R1

- R2



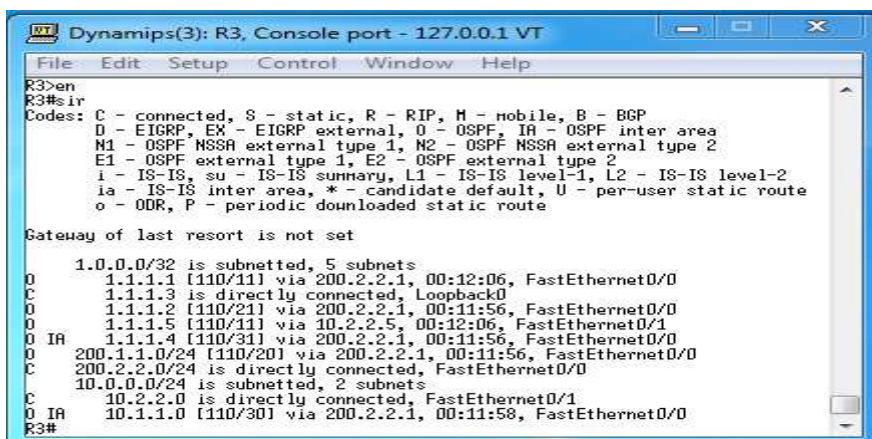
```
Dynamips(2): R2, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R2>en
R2#sir
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        M1 - OSPF NSSA external type 1, M2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 5 subnets
    O      1.1.1.1 [110/11] via 200.1.1.1, 00:11:19, FastEthernet0/0
    O      1.1.1.3 [110/21] via 200.1.1.1, 00:11:19, FastEthernet0/0
    C      1.1.1.2 is directly connected, Loopback0
    O IA   1.1.1.5 [110/31] via 200.1.1.1, 00:11:19, FastEthernet0/0
    O      1.1.1.4 [110/11] via 10.1.1.4, 00:11:09, FastEthernet0/1
    C      200.1.1.0/24 is directly connected, FastEthernet0/0
    O      200.2.2.0/24 [110/20] via 200.1.1.1, 00:11:19, FastEthernet0/0
    C      10.0.0.0/24 is subnetted, 2 subnets
    O IA   10.2.2.0 [110/30] via 200.1.1.1, 00:11:20, FastEthernet0/0
    C      10.1.1.0 is directly connected, FastEthernet0/1
R2#
```

Figure IV.5 : Résultats de la commande sir pour R2

- R3



```
Dynamips(3): R3, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R3>en
R3#sir
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        M1 - OSPF NSSA external type 1, M2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 5 subnets
    O      1.1.1.1 [110/11] via 200.2.2.1, 00:12:06, FastEthernet0/0
    C      1.1.1.3 is directly connected, Loopback0
    O      1.1.1.2 [110/21] via 200.2.2.1, 00:11:56, FastEthernet0/0
    O      1.1.1.5 [110/11] via 10.2.2.5, 00:12:06, FastEthernet0/1
    O IA   1.1.1.4 [110/31] via 200.2.2.1, 00:11:56, FastEthernet0/0
    O      200.1.1.0/24 [110/20] via 200.2.2.1, 00:11:56, FastEthernet0/0
    C      200.2.2.0/24 is directly connected, FastEthernet0/0
    C      10.0.0.0/24 is subnetted, 2 subnets
    O IA   10.2.2.0 is directly connected, FastEthernet0/1
    O IA   10.1.1.0 [110/30] via 200.2.2.1, 00:11:58, FastEthernet0/0
R3#
```

Figure IV.6 : Résultats de la commande sir pour R3

I.6. Configuration de VPN site to site :

I.6.1. Etablissement d'un tunnel Isec site-à-site

Il faut savoir que le VPN se configure juste sur les Routeurs d'extrémités dans mon cas c'est Router 3 (f0/0) et Router2 (f0/0) :

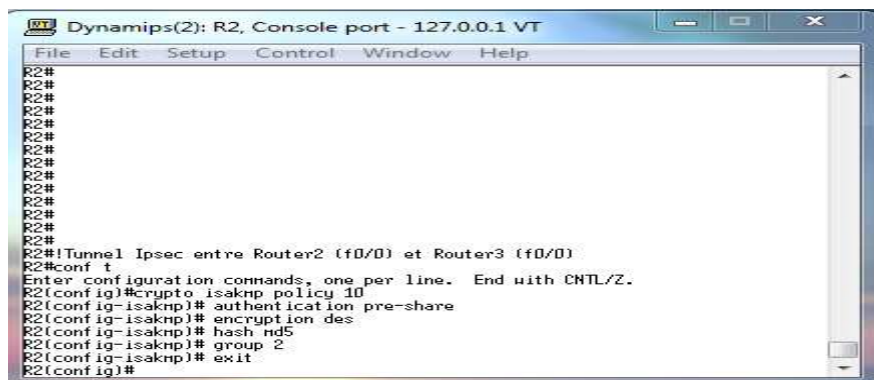
Je vais configurer la police qui détermine quelle encryptions on utilise, quelle Hash quelle type d'authentification, etc

- **Etape 1 : Configuration des paramètres ISAKMP**

Définir les paramètres du tunnel IKE (Policy ISAKMP)

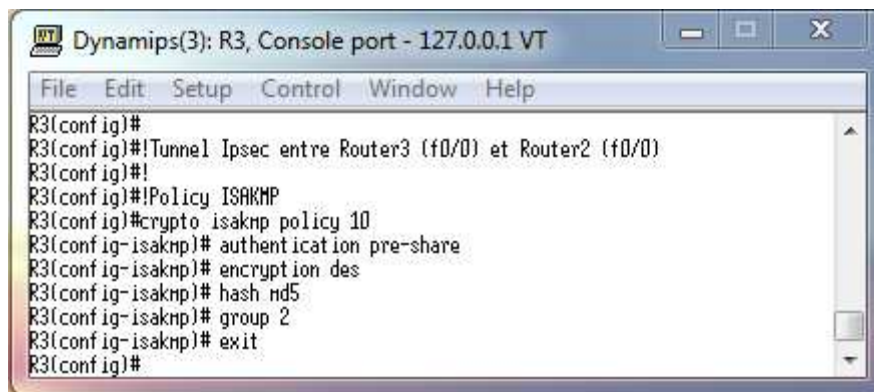
Je crée donc ici une stratégie avec un numéro de séquence 10. Ce numéro indique la priorité de l'utilisation de la stratégie. Plus petit est ce nombre plus la priorité est grande. On définit ensuite les paramètres:

- Encryptage DES
- Authentification par clé pré-partagées
- Algorithme de hachage md5



```
Dynamips(2): R2, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#!Tunnel Isec entre Router2 (f0/0) et Router3 (f0/0)
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#crypto isakmp policy 10
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption des
R2(config-isakmp)# hash md5
R2(config-isakmp)# group 2
R2(config-isakmp)# exit
R2(config)#
```

Figure IV. 9 : Configuration Policy ISAKMP pour le site central.



```
Dynamips(3): R3, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R3(config)#
R3(config)#!Tunnel Isec entre Router3 (f0/0) et Router2 (f0/0)
R3(config)#!
R3(config)#!Policy ISAKMP
R3(config)#crypto isakmp policy 10
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# encryption des
R3(config-isakmp)# hash md5
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)#
```

Figure IV.10.Configuration Policy ISAKMP pour le site distant 1

- **Etape 2 : Configuration des paramètres Ipsec**

On a maintenant terminé la configuration de la partie qui gère la négociation des clés etc. La deuxième partie consiste à définir comment les données seront cryptées.

Tout d'abord on crée la méthode de cryptage (transform-set) que l'on nomme T1.

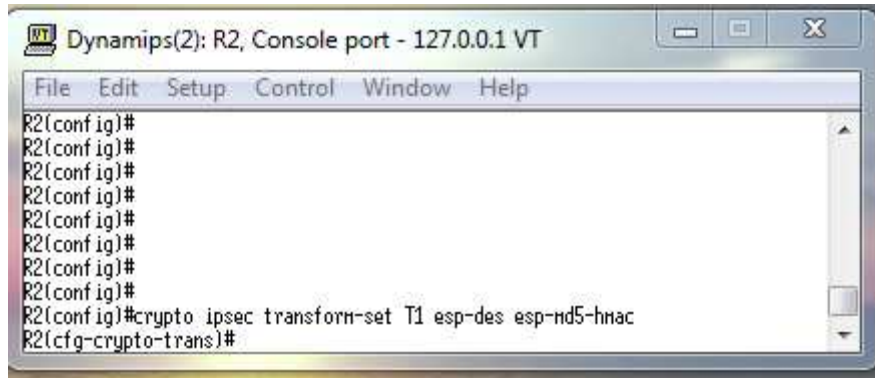


Figure IV.11. Configuration des paramètres du tunnel ipsec pour le site central 'R2'

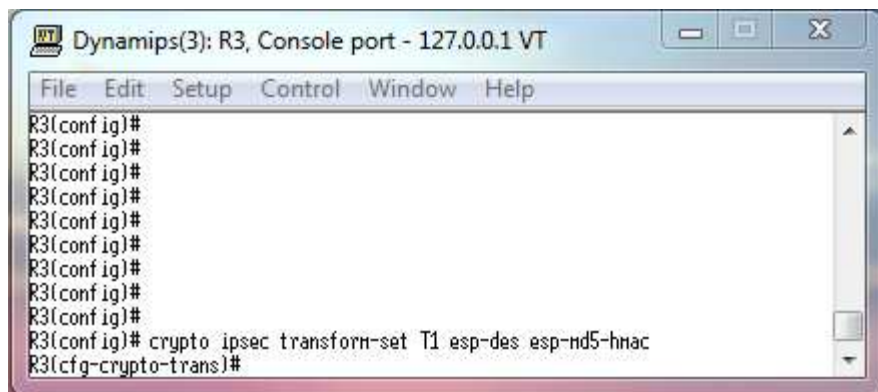


Figure IV.12 Configuration des paramètres du tunnel ipsec pour le site distant 1 'R3'

Esp-des est la méthode de cryptage, esp-md5-hmac est la méthode d'authentification

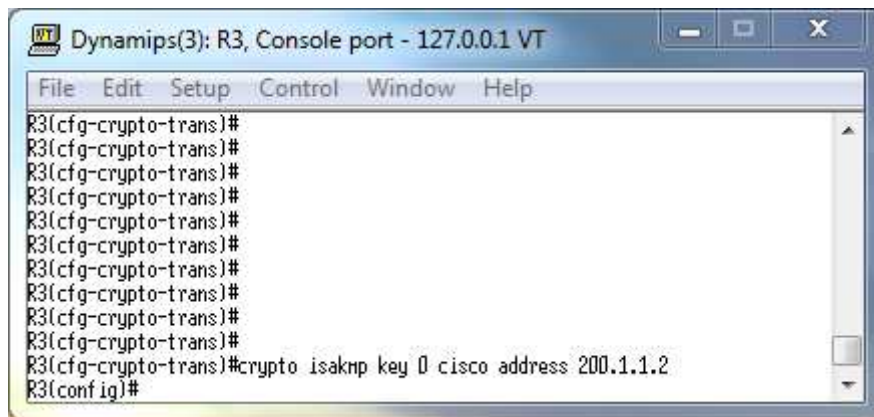
Etape 3 : Configuration Pre-shared key avec le peer

Définir le secret partagé entre les 2 équipements établissant un tunnel Ipsec



```
Dynamips(2): R2, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#crypto ipsec transform-set T1 esp-des esp-md5-hmac
R2(cfg-crypto-trans)#
R2(cfg-crypto-trans)#crypto ipsec transform-set T1 esp-des esp-md5-hmac
R2(cfg-crypto-trans)#
R2(cfg-crypto-trans)#
```

Figure IV.13. Configuration du tunnel ipsec pour le site centrale



```
Dynamips(3): R3, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#
R3(cfg-crypto-trans)#crypto isakmp key 0 cisco address 200.1.1.2
R3(config)#
```

Figure IV.14 : Configuration du tunnel ipsec pour le site distant 1

Voilà j'ai ensuite la clé pré-partagée, ici « Cisco » qu'on associe avec l'adresse de l'autre bout du tunnel donc 200.1.1.2.

Le 0 indique que j'ai défini la clé en texte clair, en opposition avec une clé déjà cryptée si on la copie d'un « show run » d'un routeur ou l'encryptage des mots de passe est activé.

- **Etape 4 : Définir le trafic intéressant**

Définir le trafic intéressant, c'est à dire le trafic à protéger par un tunnel Isec



Figure IV.15. Configuration des listes de contrôle pour le site central



Figure IV.16. Configuration des listes de contrôle pour le site distant 1

- **Etape 5 : Définir la crypto map**

Création d'une crypto map pour regrouper les paramètres précédant

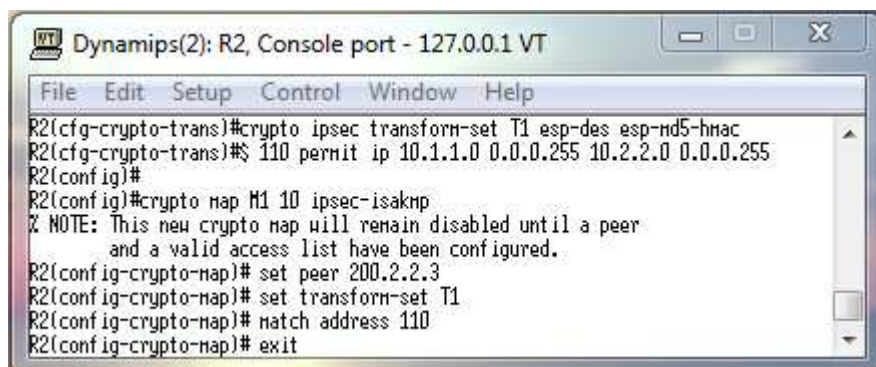


Figure IV.17 : Configuration de la crypto map pour le site central

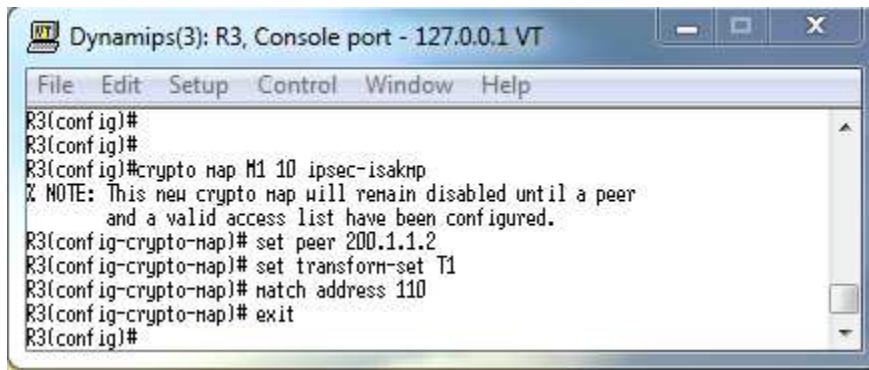


Figure IV.18. Configuration de la crypto map pour le site distant 1

On a donc créé ici une Crypto-map nommée M1 dans laquelle on intègre une séquence 10 (une seule crypto-map par interface, mais on peut ajouter plusieurs maps en leur indiquant des numéros de séquence différents), avec les paramètres suivants:

- Activée pour le trafic correspondant à l'accès-list VPN
- Destination du tunnel 200.1.1.2
- Cryptage selon le transform-set M1
- **Etape 6 : Appliquer la Crypto map à l'interface outside**

La dernière étape consiste à appliquer cette crypto-map à l'interface f0/0.

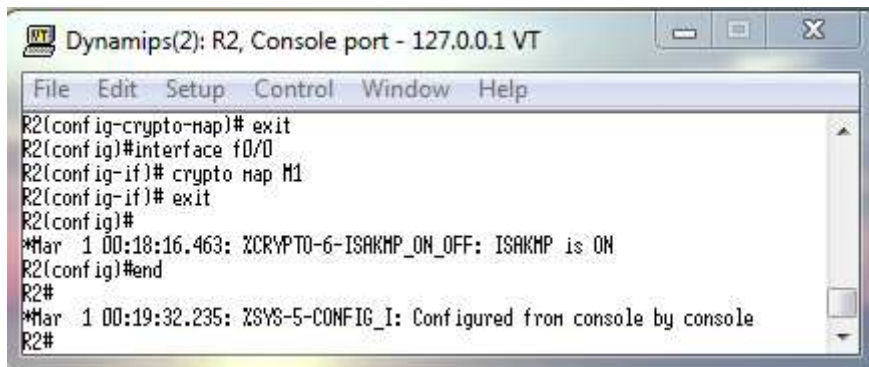


Figure IV.19. Application de la crypto map à l'interface pour le site central

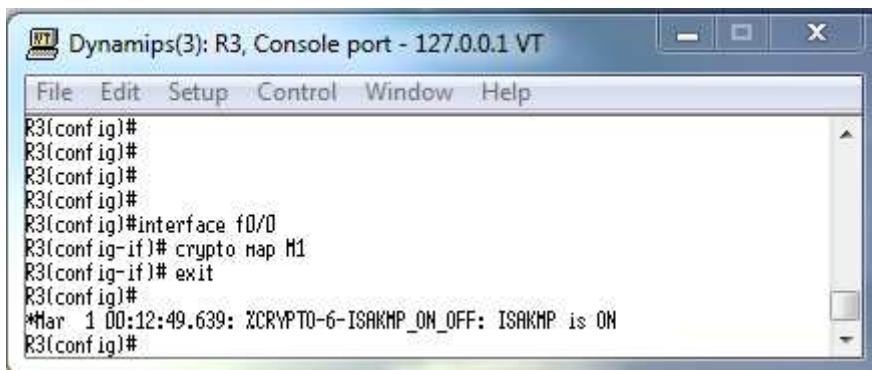
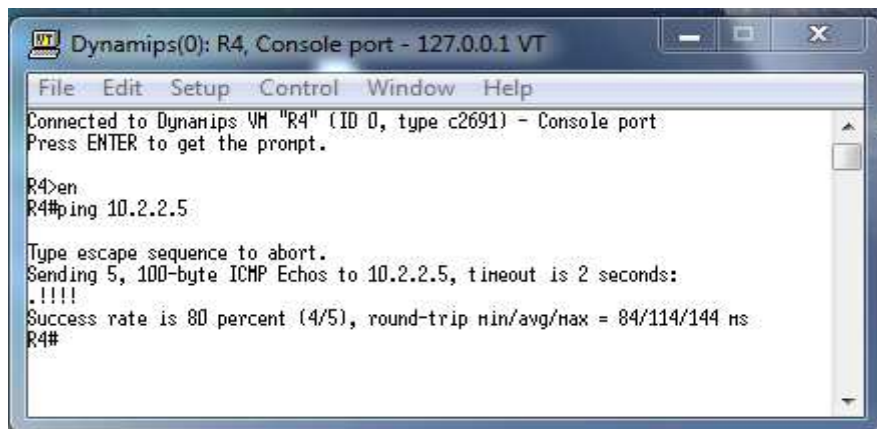


Figure IV .20. Application de la crypto map à l'interface pour le site distant 1

- **Générer le trafic intéressant**

A partir de R4, faire ping sur l'adresse IP de l'interface f0/0 de R5



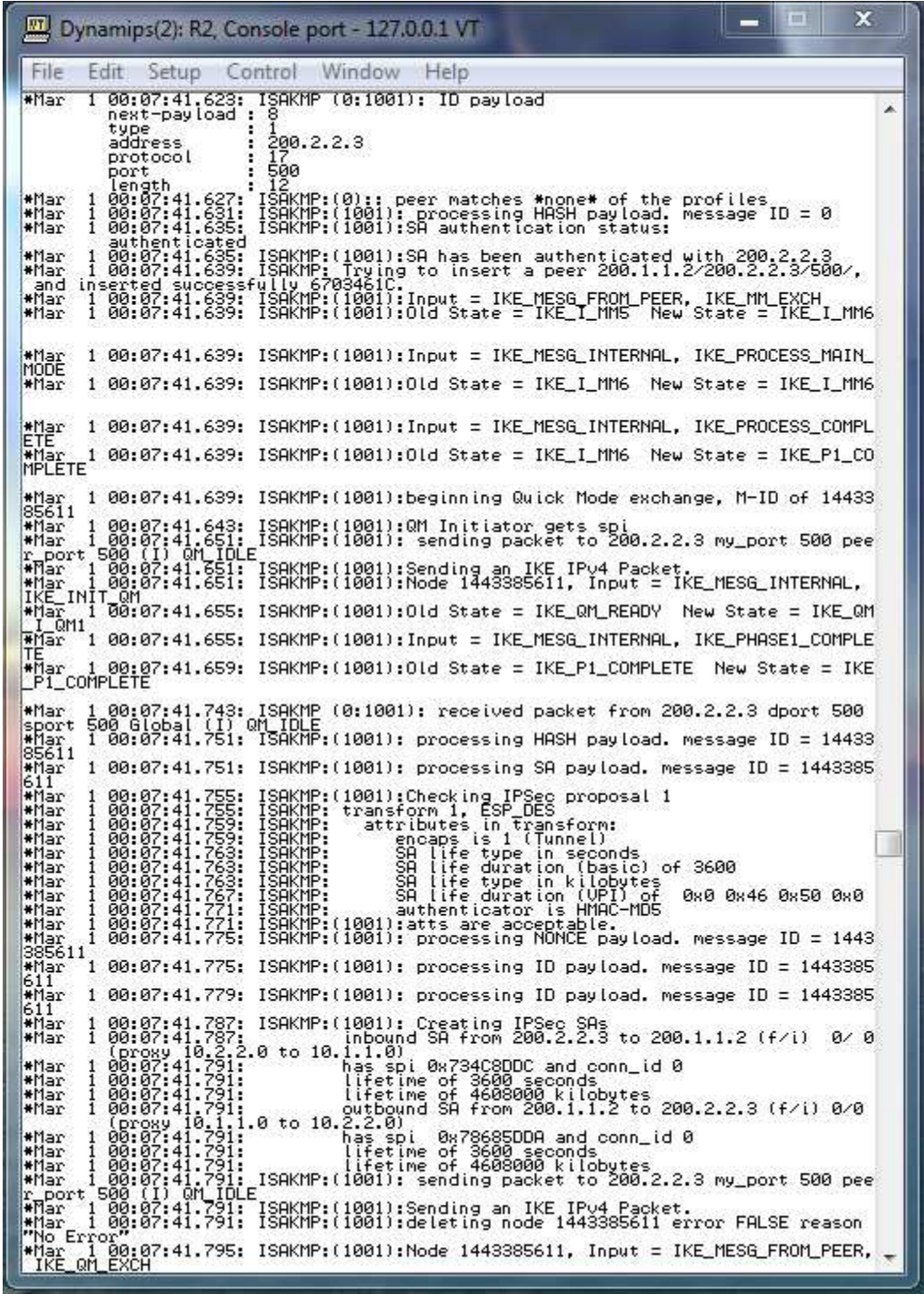
```
Dynamips(0): R4, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
Connected to Dynamips VM "R4" (ID 0, type c2691) - Console port
Press ENTER to get the prompt.

R4>en
R4#ping 10.2.2.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.5, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/114/144 ms
R4#
```

Figure IV.21.Résultat du : ping 10.2.2.5

Le message observé sur R2 :



```
Dynamips(2): R2, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
*Mar 1 00:07:41.623: ISAKMP (0:1001): ID payload
  next-payload : 8
  type : 1
  address : 200.2.2.3
  protocol : 17
  port : 500
  length : 12
*Mar 1 00:07:41.627: ISAKMP:(0):: peer matches *none* of the profiles.
*Mar 1 00:07:41.631: ISAKMP:(1001):: processing HASH payload. message ID = 0
*Mar 1 00:07:41.635: ISAKMP:(1001)::SA authentication status:
  authenticated
*Mar 1 00:07:41.635: ISAKMP:(1001)::SA has been authenticated with 200.2.2.3
*Mar 1 00:07:41.639: ISAKMP: Trying to insert a peer 200.1.1.2/200.2.2.3/500/,
  and inserted successfully 6703461C.
*Mar 1 00:07:41.639: ISAKMP:(1001)::Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Mar 1 00:07:41.639: ISAKMP:(1001)::Old State = IKE_I_MM5 New State = IKE_I_MM6

*Mar 1 00:07:41.639: ISAKMP:(1001)::Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_
MODE
*Mar 1 00:07:41.639: ISAKMP:(1001)::Old State = IKE_I_MM6 New State = IKE_I_MM6

*Mar 1 00:07:41.639: ISAKMP:(1001)::Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPL
ETE
*Mar 1 00:07:41.639: ISAKMP:(1001)::Old State = IKE_I_MM6 New State = IKE_P1_CO
MPLETE

*Mar 1 00:07:41.639: ISAKMP:(1001)::beginning Quick Mode exchange, M-ID of 14433
85611
*Mar 1 00:07:41.643: ISAKMP:(1001)::QM Initiator gets spi
*Mar 1 00:07:41.651: ISAKMP:(1001):: sending packet to 200.2.2.3 my_port 500 pee
r port 500 (I) QM_IDLE
*Mar 1 00:07:41.651: ISAKMP:(1001)::Sending an IKE IPv4 Packet.
*Mar 1 00:07:41.651: ISAKMP:(1001)::Node 1443385611, Input = IKE_MSG_INTERNAL,
IKE_INIT_QM
*Mar 1 00:07:41.655: ISAKMP:(1001)::Old State = IKE_QM_READY New State = IKE_QM
I_QM1
*Mar 1 00:07:41.655: ISAKMP:(1001)::Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLE
TE
*Mar 1 00:07:41.659: ISAKMP:(1001)::Old State = IKE_P1_COMPLETE New State = IKE
_P1_COMPLETE

*Mar 1 00:07:41.743: ISAKMP (0:1001): received packet from 200.2.2.3 dport 500
sport 500 Global (I) QM_IDLE
*Mar 1 00:07:41.751: ISAKMP:(1001): processing HASH payload. message ID = 14433
85611
*Mar 1 00:07:41.751: ISAKMP:(1001): processing SA payload. message ID = 1443385
611
*Mar 1 00:07:41.755: ISAKMP:(1001):Checking IPsec proposal 1
*Mar 1 00:07:41.755: ISAKMP: transform 1, ESP_DES
*Mar 1 00:07:41.759: ISAKMP: attributes in transform:
  encaps is 1 (tunnel)
*Mar 1 00:07:41.759: ISAKMP: SA life type in seconds
*Mar 1 00:07:41.763: ISAKMP: SA life duration (basic) of 3600
*Mar 1 00:07:41.763: ISAKMP: SA life type in kilobytes
*Mar 1 00:07:41.767: ISAKMP: SA life duration (UPI) of 0x0 0x46 0x50 0x0
*Mar 1 00:07:41.771: ISAKMP: authenticator is HMAC-MD5
*Mar 1 00:07:41.771: ISAKMP:(1001):atts are acceptable.
*Mar 1 00:07:41.775: ISAKMP:(1001): processing NONCE payload. message ID = 1443
385611
*Mar 1 00:07:41.775: ISAKMP:(1001): processing ID payload. message ID = 1443385
611
*Mar 1 00:07:41.779: ISAKMP:(1001): processing ID payload. message ID = 1443385
611
*Mar 1 00:07:41.787: ISAKMP:(1001): Creating IPsec SAs
*Mar 1 00:07:41.787: inbound SA from 200.2.2.3 to 200.1.1.2 (f/i) 0/0
(proxy 10.2.2.0 to 10.1.1.0)
  has spi 0x734C80DC and conn_id 0
  lifetime of 3600 seconds
  lifetime of 4608000 kilobytes
*Mar 1 00:07:41.791: outbound SA from 200.1.1.2 to 200.2.2.3 (f/i) 0/0
(proxy 10.1.1.0 to 10.2.2.0)
  has spi 0x78685DDA and conn_id 0
  lifetime of 3600 seconds
  lifetime of 4608000 kilobytes
*Mar 1 00:07:41.791: ISAKMP:(1001): sending packet to 200.2.2.3 my_port 500 pee
r port 500 (I) QM_IDLE
*Mar 1 00:07:41.791: ISAKMP:(1001)::Sending an IKE IPv4 Packet.
*Mar 1 00:07:41.791: ISAKMP:(1001)::deleting node 1443385611 error FALSE reason
"No Error"
*Mar 1 00:07:41.795: ISAKMP:(1001)::Node 1443385611, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
```

Figure IV.22.Résultat su Ping 10.2.2.5 sur R2

I.7. Vérification :

- Voir tous les échanges IKE pour les tunnels IKE et Ipsec :

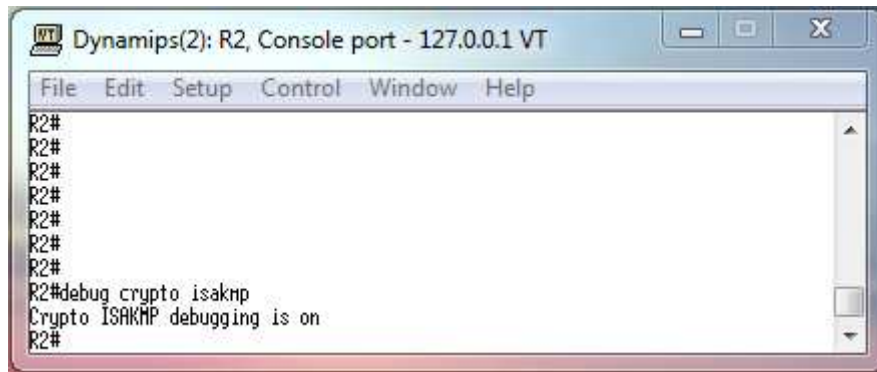


Figure IV.23. Résultat de la commande « debug crypto isakmp » sur R2

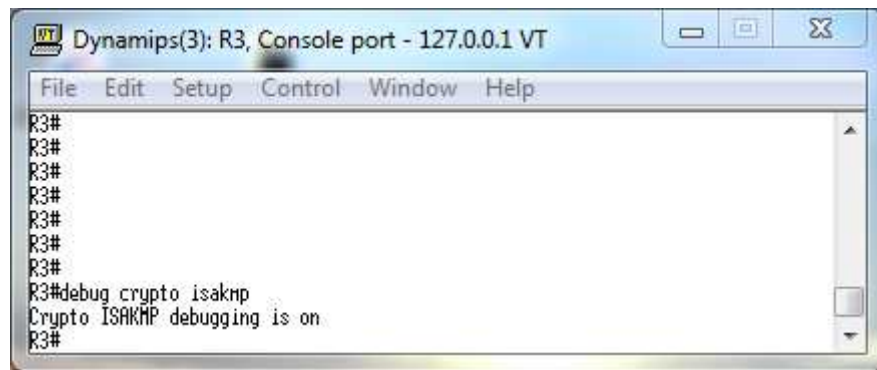
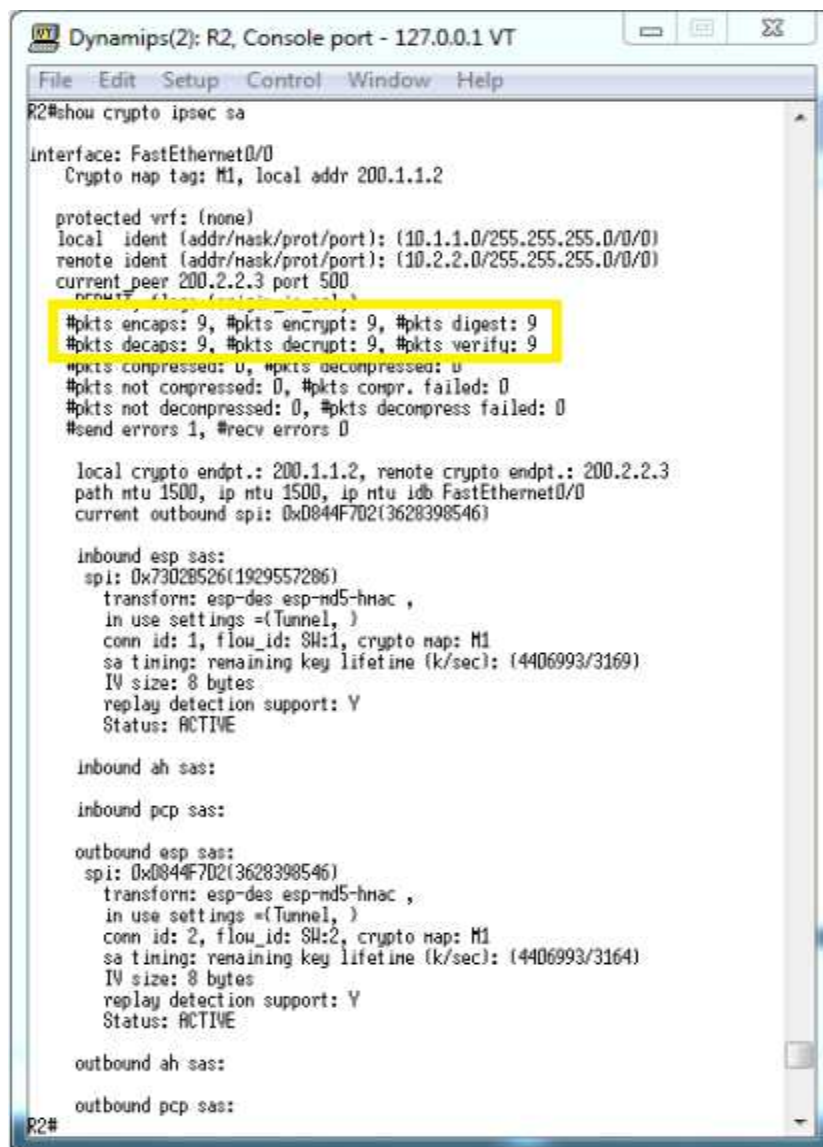


Figure IV.24. Résultat de la commande « debug crypto isakmp » sur R3

- voir le status du tunnel Ipsec



```
Dynamips(2): R2, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R2#show crypto ipsec sa
Interface: FastEthernet0/0
Crypto map tag: M1, local addr 200.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
current_peer 200.2.2.3 port 500
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 200.1.1.2, remote crypto endpt.: 200.2.2.3
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x0844F7D2(3628398546)

inbound esp sas:
spi: 0x73D2B526(1929557286)
transform: esp-des esp-md5-hmac ,
in use settings =(Tunnel, )
conn id: 1, flow_id: SW:1, crypto map: M1
sa timing: remaining key lifetime (k/sec): (4406993/3169)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x0844F7D2(3628398546)
transform: esp-des esp-md5-hmac ,
in use settings =(Tunnel, )
conn id: 2, flow_id: SW:2, crypto map: M1
sa timing: remaining key lifetime (k/sec): (4406993/3164)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

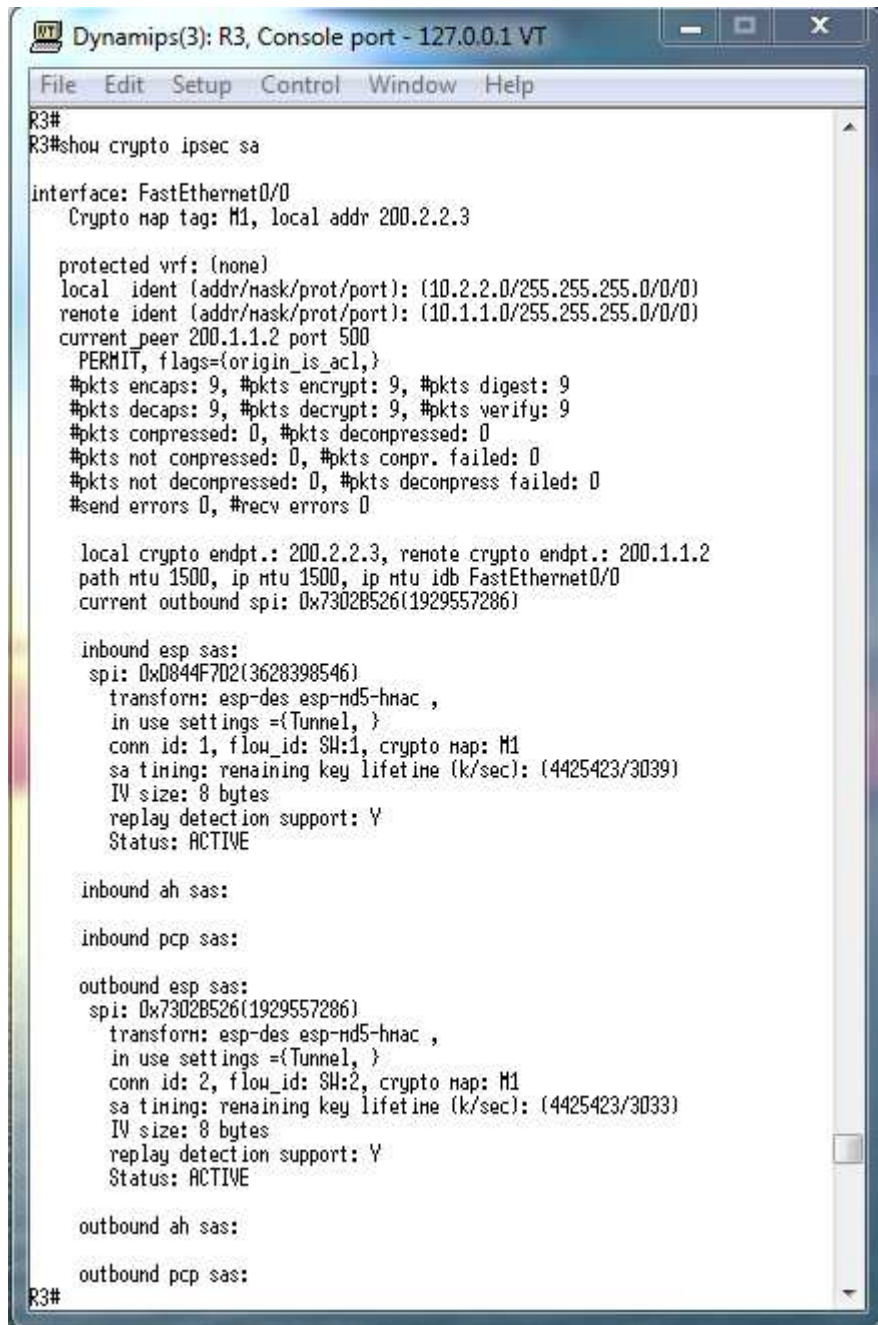
outbound ah sas:

outbound pcp sas:

R2#
```

Figure IV. 25. Résultat de la commande sur R2 « show crypto ipsec sa »

Les deux lignes entourées en jaune indiquent les paquets reçus et envoyés par le tunnel VPN.



```
Dynamips(3): R3, Console port - 127.0.0.1 VT
File Edit Setup Control Window Help
R3#
R3#show crypto ipsec sa

interface: FastEthernet0/0
  Crypto map tag: M1, local addr 200.2.2.3

protected vrf: (none)
local ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer 200.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 200.2.2.3, remote crypto endpt.: 200.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x73028526(1929557286)

inbound esp sas:
  spi: 0x0844F702(3628398546)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 1, flow_id: SH:1, crypto map: M1
    sa timing: remaining key lifetime (k/sec): (4425423/3039)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x73028526(1929557286)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 2, flow_id: SH:2, crypto map: M1
    sa timing: remaining key lifetime (k/sec): (4425423/3033)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

R3#
```

Figure IV.26.Résultat de la commande sur R3 « show crypto ipsec sa »

I.8. Analyse du trafic à l'aide de Wireshark

La figure suivante représente le résultat de l'analyse des paquets à l'aide de Wireshark, ce résultat contient les adresses sources et destinations, type de protocole et la longueur de l'information capturée.

No.	Time	Source	Destination	Protocol	Length	Info
102	231.657000	200.1.1.1	224.0.0.5	OSPF	94	Hello Packet
103	231.918000	c0:02:07:ac:00:00	CDP/VTP/DTP/PagP/UDLD	CDP	350	Device ID: R2 Port ID: FastEthernet0/0
104	232.722000	c0:02:07:ac:00:00	c0:02:07:ac:00:00	LOOP	60	Reply
105	232.905000	c0:01:07:ac:00:00	c0:01:07:ac:00:00	LOOP	60	Reply
106	233.587000	c0:01:07:ac:00:00	CDP/VTP/DTP/PagP/UDLD	CDP	350	Device ID: R1 Port ID: FastEthernet0/0
107	235.590000	200.1.1.2	200.2.2.3	ISAKMP	208	Identity Protection (Main Mode)
108	235.662000	200.2.2.3	200.1.1.2	ISAKMP	146	Identity Protection (Main Mode)
109	235.723000	200.1.1.2	200.2.2.3	ISAKMP	338	Identity Protection (Main Mode)
110	235.813000	200.2.2.3	200.1.1.2	ISAKMP	338	Identity Protection (Main Mode)
111	235.914000	200.1.1.2	200.2.2.3	ISAKMP	134	Identity Protection (Main Mode)
112	235.976000	200.2.2.3	200.1.1.2	ISAKMP	110	Identity Protection (Main Mode)
113	236.026000	200.1.1.2	200.2.2.3	ISAKMP	214	Quick Mode
114	236.106000	200.2.2.3	200.1.1.2	ISAKMP	214	Quick Mode
115	236.156000	200.1.1.2	200.2.2.3	ISAKMP	94	Quick Mode
116	237.553000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
117	237.603000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
118	237.623000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
119	237.705000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
120	237.715000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
121	237.745000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
122	237.755000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
123	237.785000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
124	237.815000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
125	237.845000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
126	237.855000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
127	237.885000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
128	237.895000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
129	237.925000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
130	237.935000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)
131	237.965000	200.2.2.3	200.1.1.2	ESP	166	ESP (SPI=0xa5fd8f0b)
132	237.975000	200.1.1.2	200.2.2.3	ESP	166	ESP (SPI=0xc9892a44)

0000 c0 02 07 ac 00 00 c0 01 07 ac 00 00 08 00 45 00 E.
0010 00 98 00 aa 00 00 fe 32 28 81 c8 02 03 c8 01 2 (.....
0020 01 02 35 fd 8f 0b 00 00 00 e8 fa a4 3d f2 8b
Standard input: <live capture in progress> Fil... Packets: 185 Displayed: 185 Marked: 0 Profile: Default

Figure IV.27. Résultat de l'analyse avec Wireshark.

Conclusion

Dans ce chapitre on a mis au point une solution sécurisée basée sur les VPN de types Site-à-site basés sur le protocole IPsec ce qui nous a permis de comprendre le principe de fonctionnement, l'utilité et l'importance de cette solution pour la sécurité de l'import quel réseau informatique .

Conclusion générale

A travers ce projet de fin d'étude, nous avons vu ensemble un aperçu des différentes possibilités afin de déployer un VPN, et particulièrement la solution que représente IPSec. en effet on a pour objectif de vous donner les concepts qui tournent autour de cette solution et de vous montrer un exemple de déploiement.

En effet grâce à cette nouvelle technologie, permis aux employés de se relier entre eux a travers internet. Cette solution mise en place, est une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basé sur le protocole IPSec, ce dernier est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

A la fin, ce projet m'a permis de comprendre le principe de fonctionnement des VPNs et les paramètres à prendre en considération pour réussir leur implémentation.

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

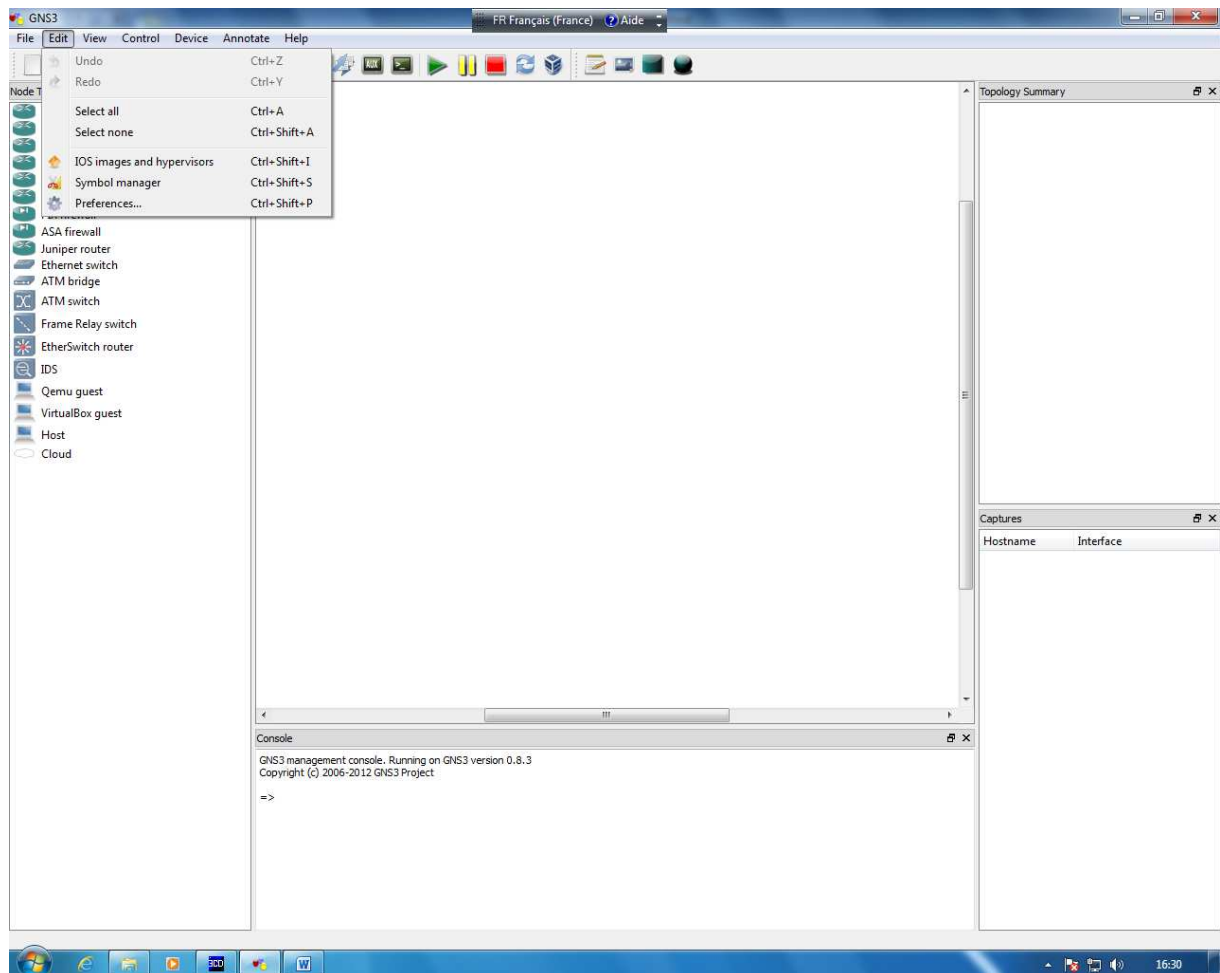
I. Installation et configuration de GNS3 sur PC ayant au moins 4GO de RAM.

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

1 - Installer l'application GNS3 et la lancer

2 – configurer l'URL de l'IOS

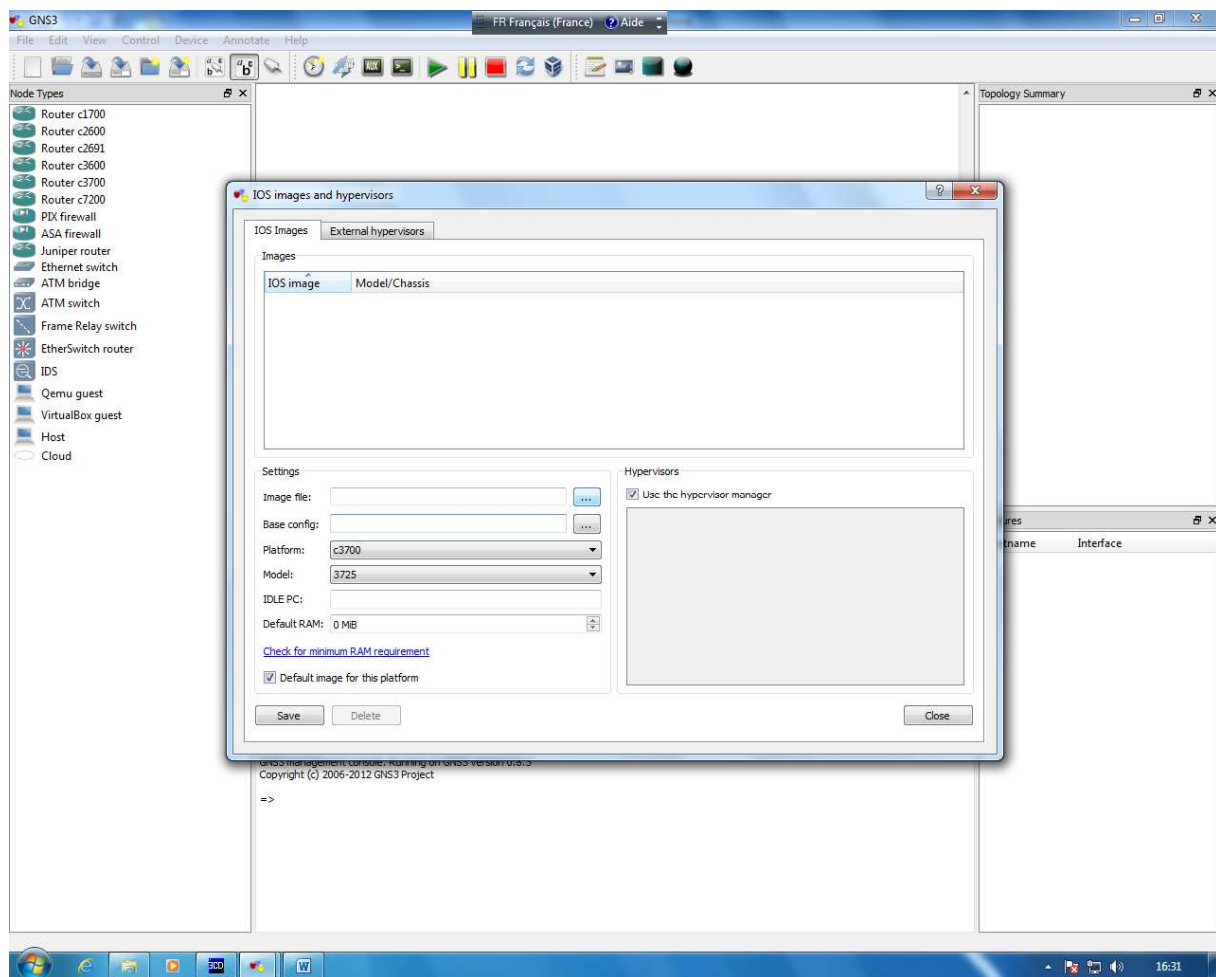
Edit >> IOS image and Hypervisor



Annexe

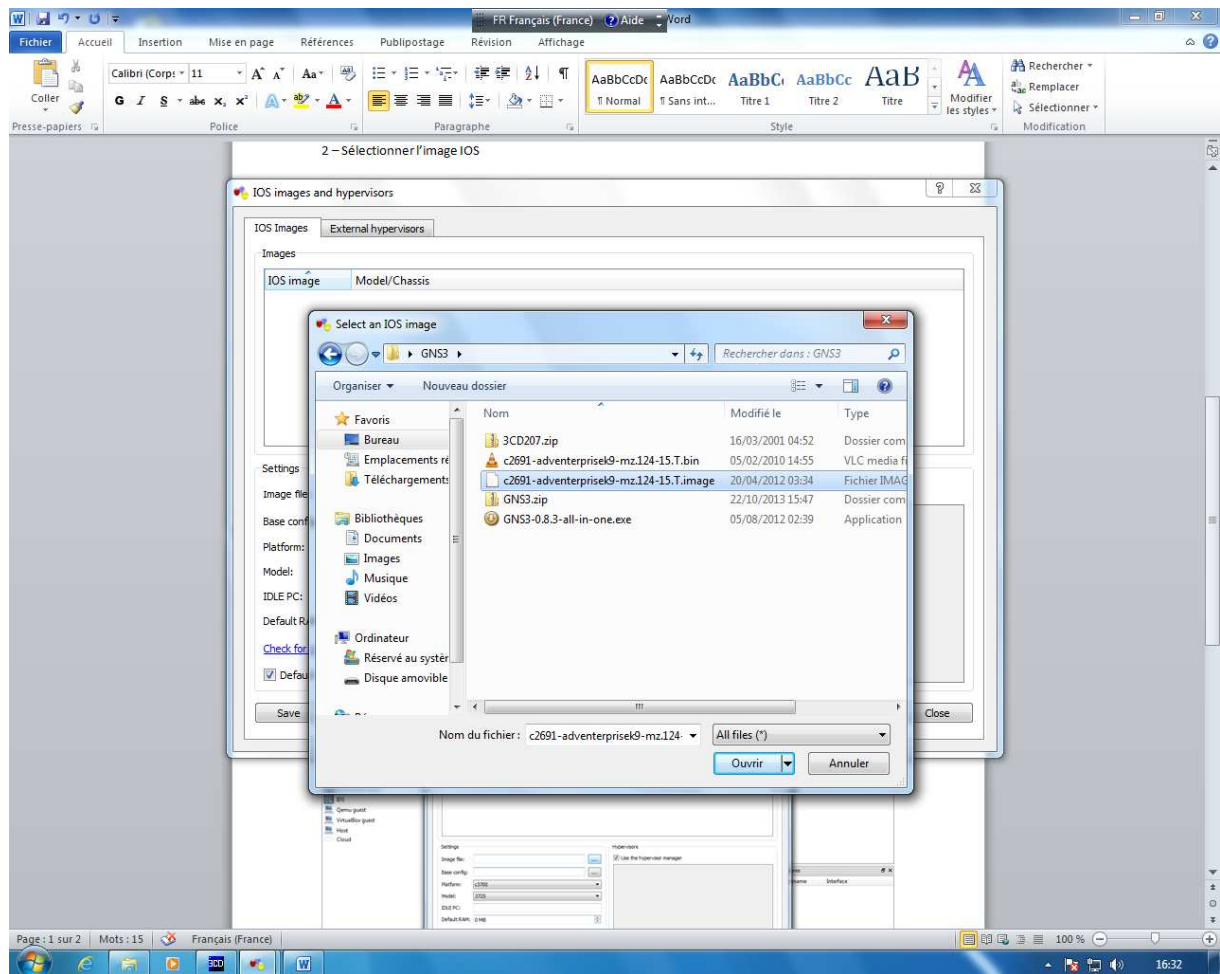
3 – Sélectionner l'image IOS

Cliquer sur le bouton face à "Image file:"



Annexe

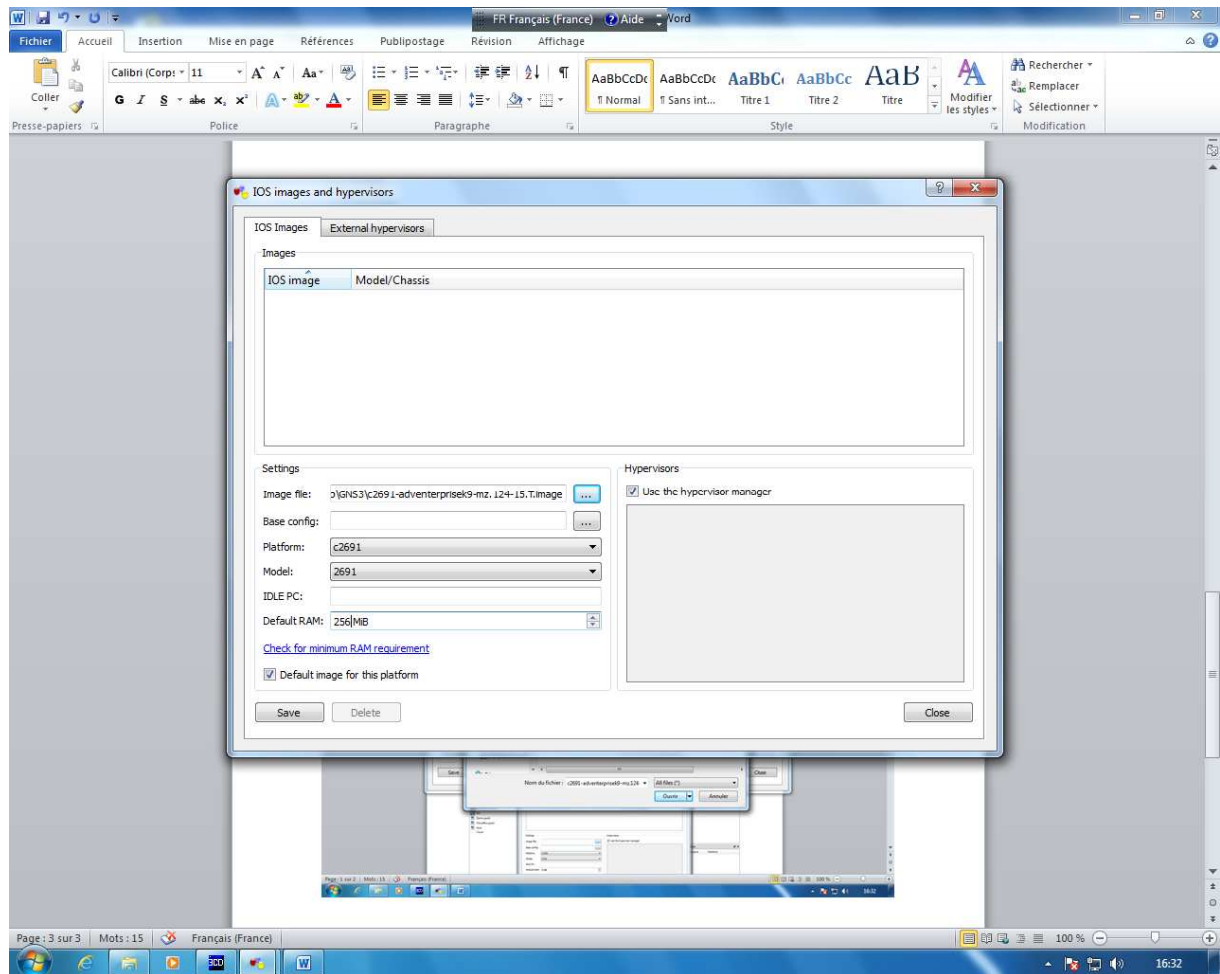
4 – Sélectionner l'IOS (décompressé) et cliquer sur bouton <<Ouvrir>>



Annexe

5 – Modifier la capacité mémoire des routeurs émulés de 128 ==> 256 MB

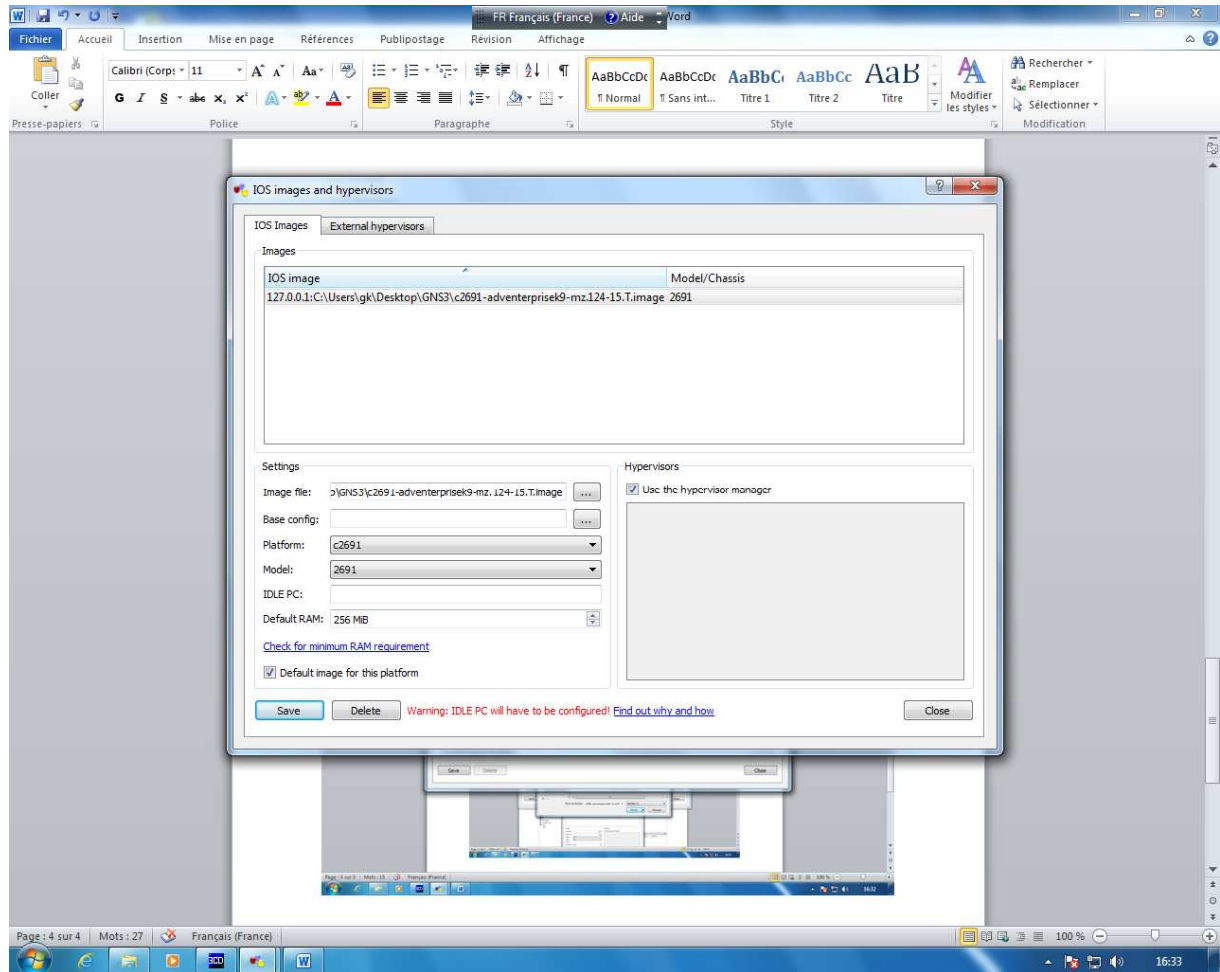
Modifier le contenu des champs <<Default RAM>>



Annexe

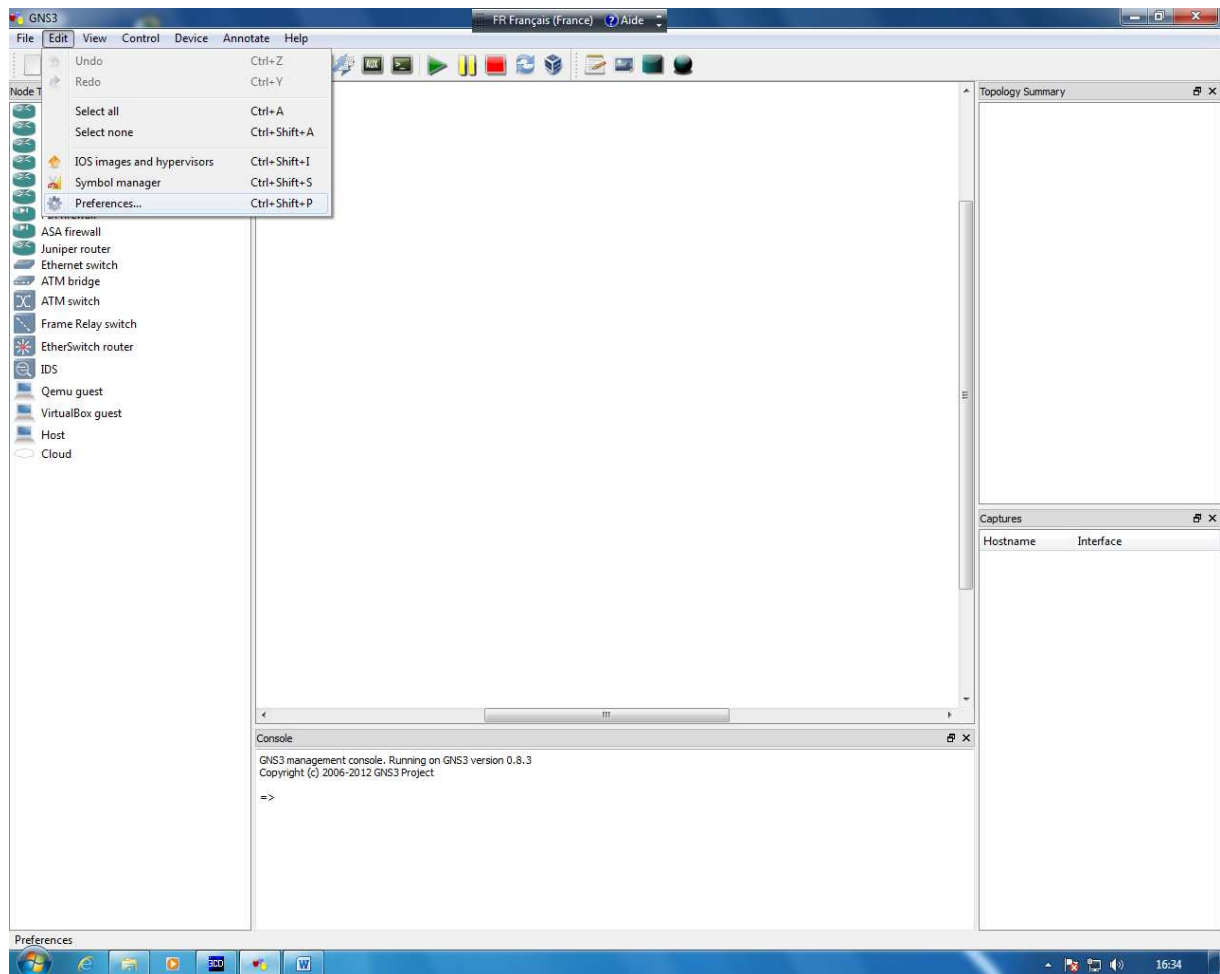
6 – Cliquer <<Save>> et <<Close>>

Ignorer le message en rouge "Warning Idle PC"



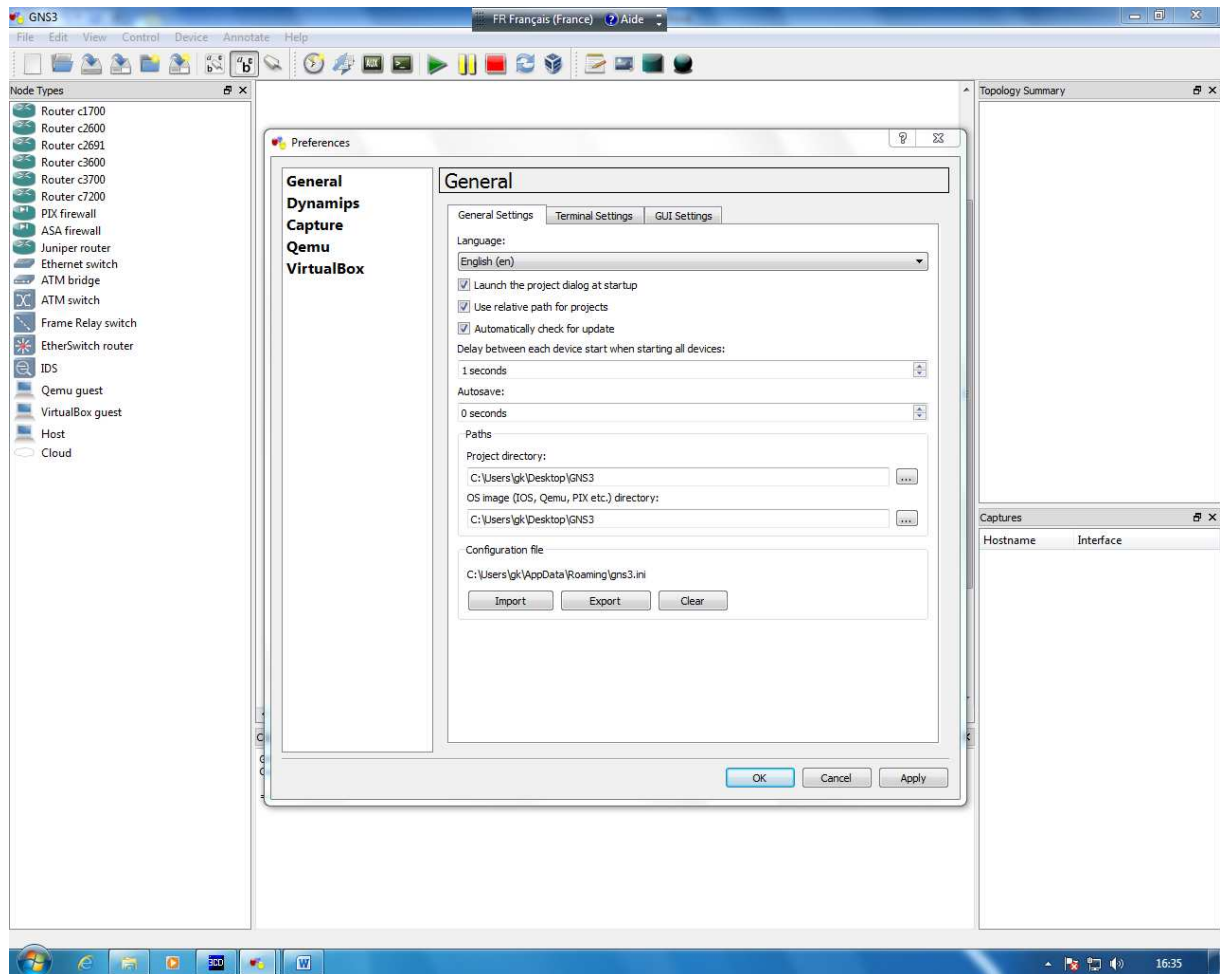
Annexe

Edit >> Préférence



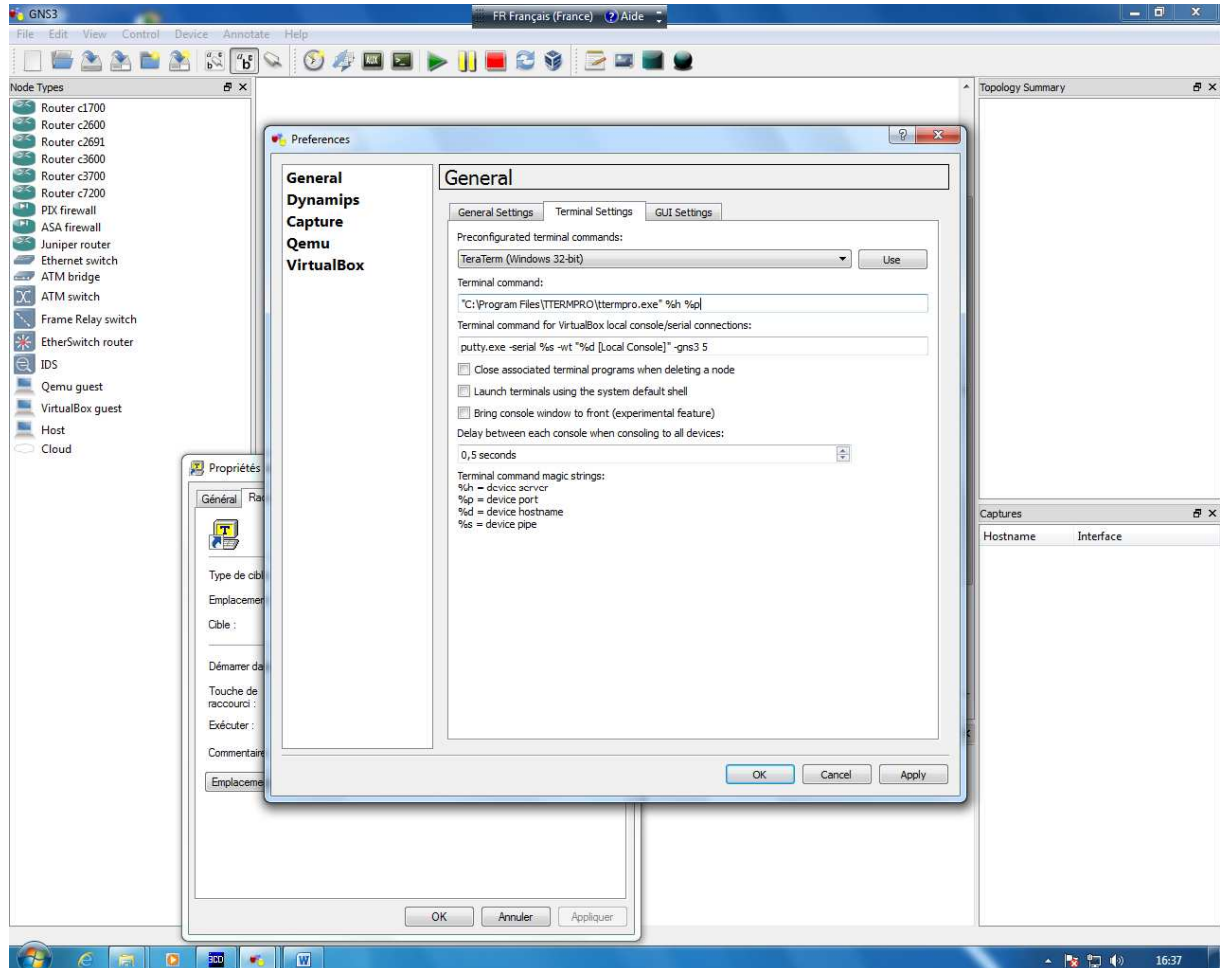
Annexe

7 – Modifier le répertoire par défaut et sélectionner le répertoire GNS3 créé sur le desktop.



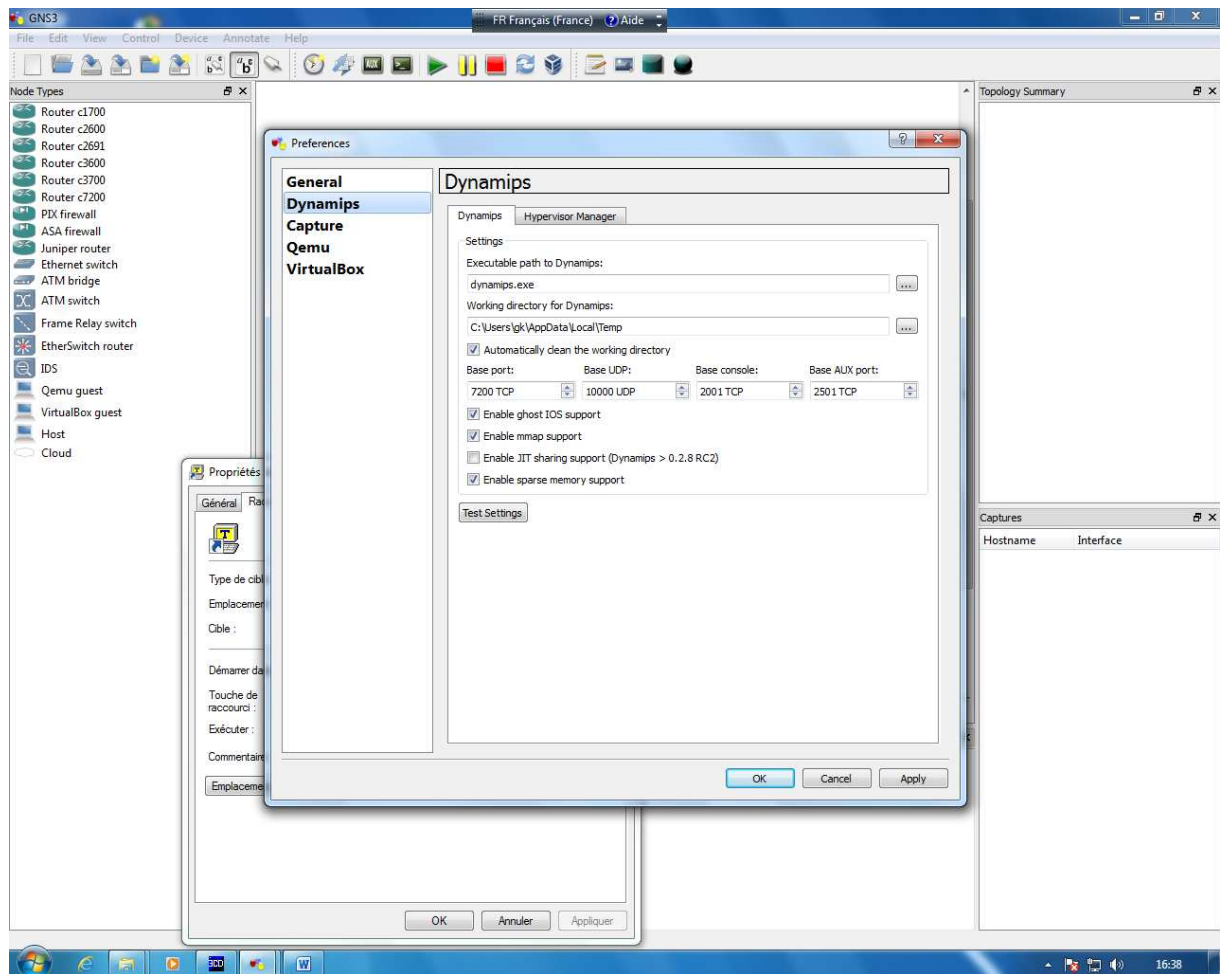
Annexe

8 – Si nécessaire sélectionner Teraterm (Windows 32) à la place de Putty par défaut
Sous Terminal command : copier l'URL de l'application Teraterm et ne laisser que les options %h %p



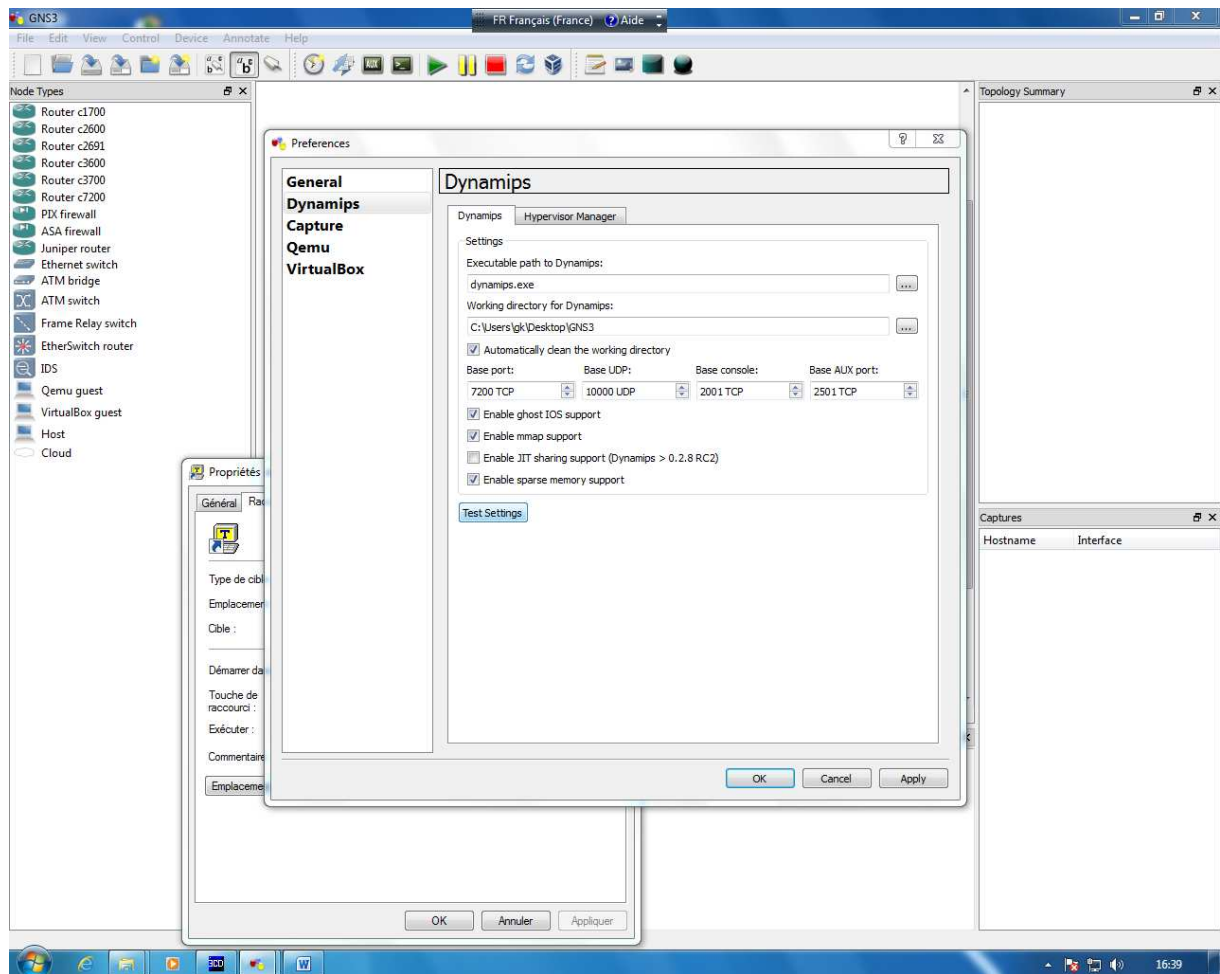
Annexe

Cliquer sur le bouton <Dynamips>>



Cliquer sur le bouton <<Test Settings>>, au bout de quelques secondes on doit voir le message en vert <<... successfully started>>

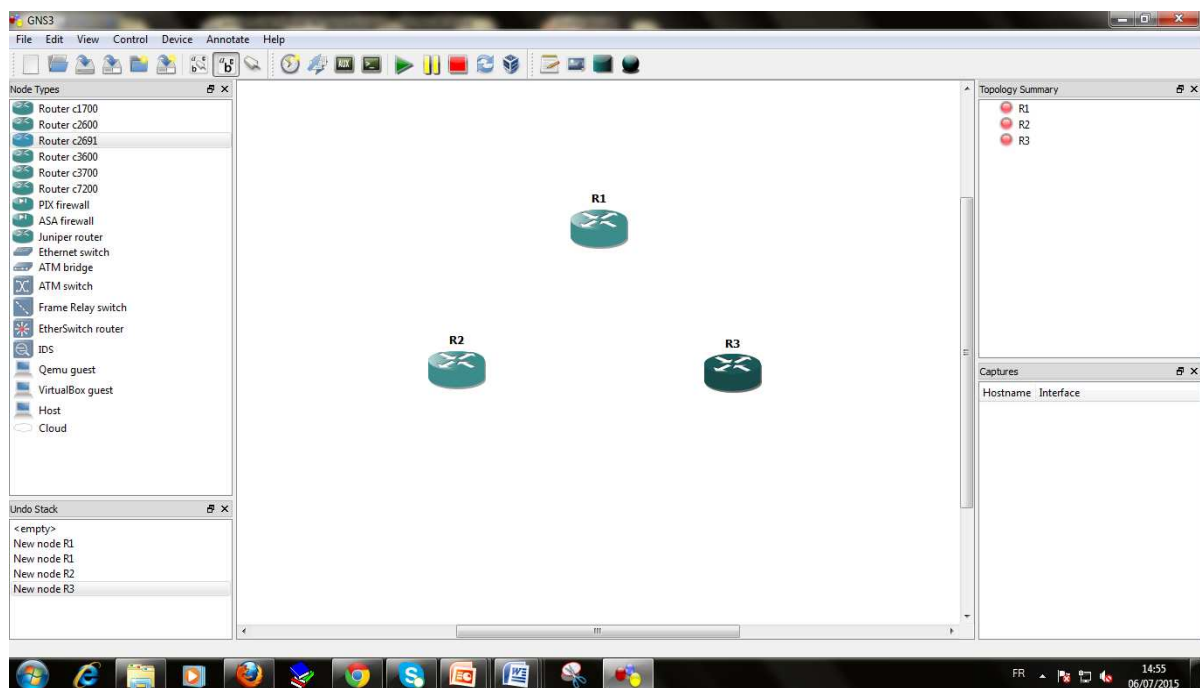
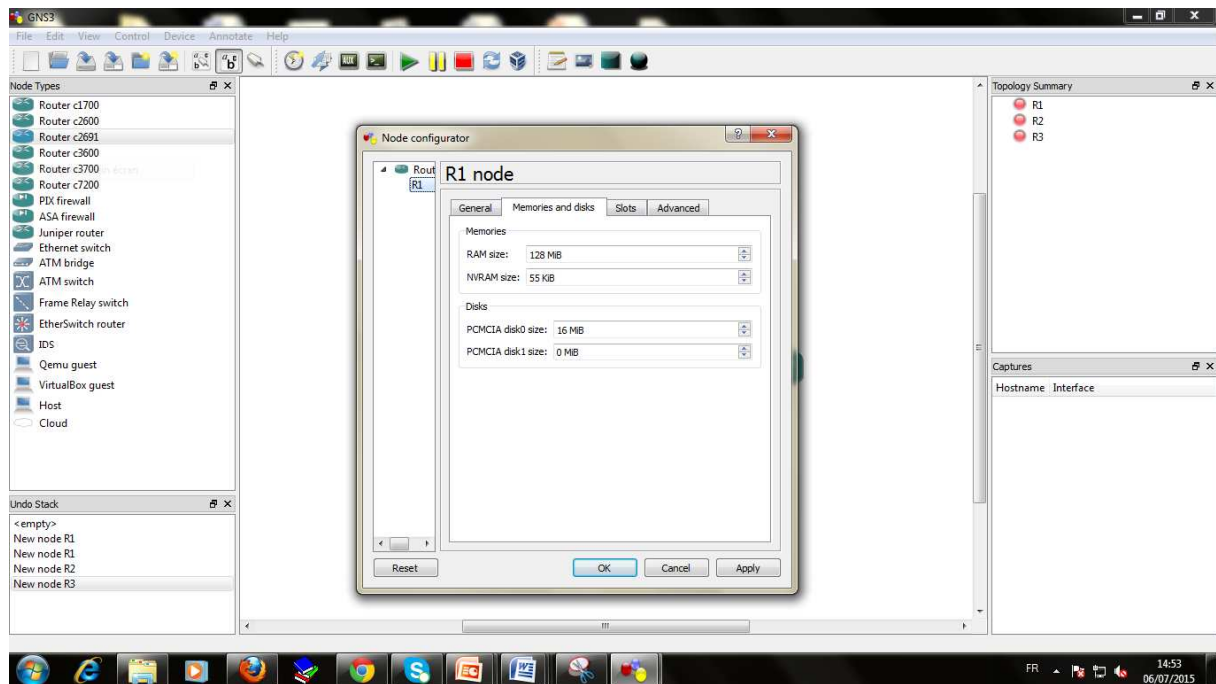
Annexe



Maintenant que la configuration de base est terminée, on ferme la fenêtre Preference. On fait drag and drop du routeur c2691, autant de routeurs que nécessaires.

On configure le hardware des routeurs. Par défaut le routeur est équipé de 2 interfaces Fostethernet. Si nécessaire on peut rajouter des WIC 1 ou 2T, pour avoir un ou 2 ports Série.

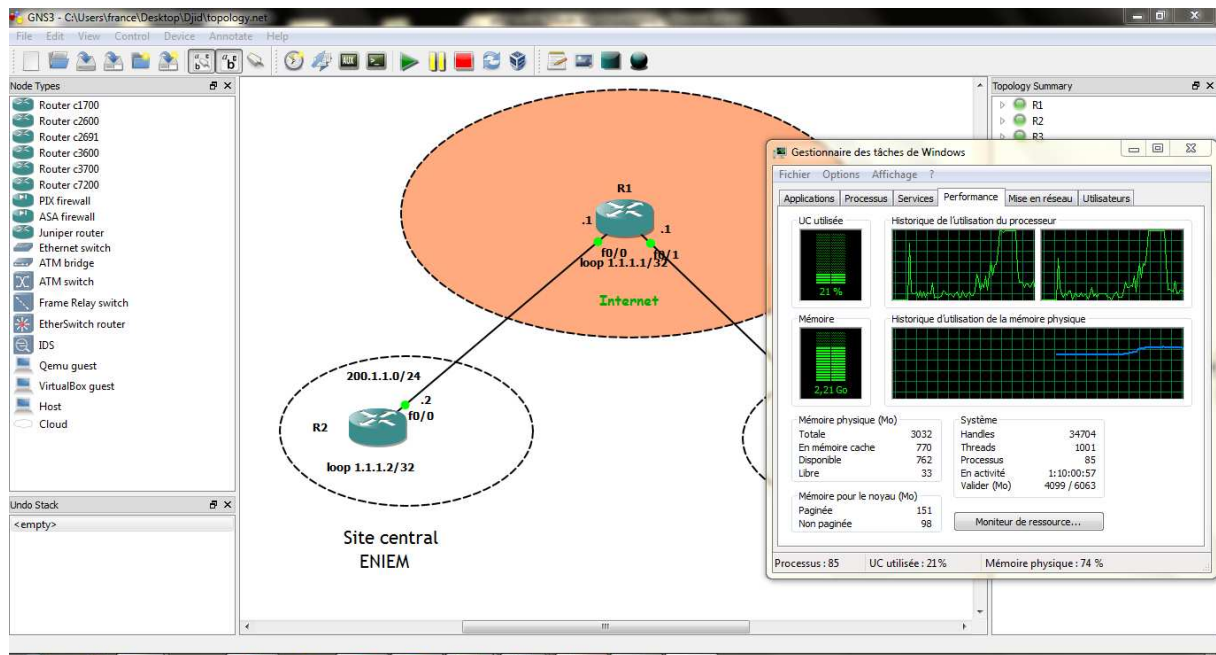
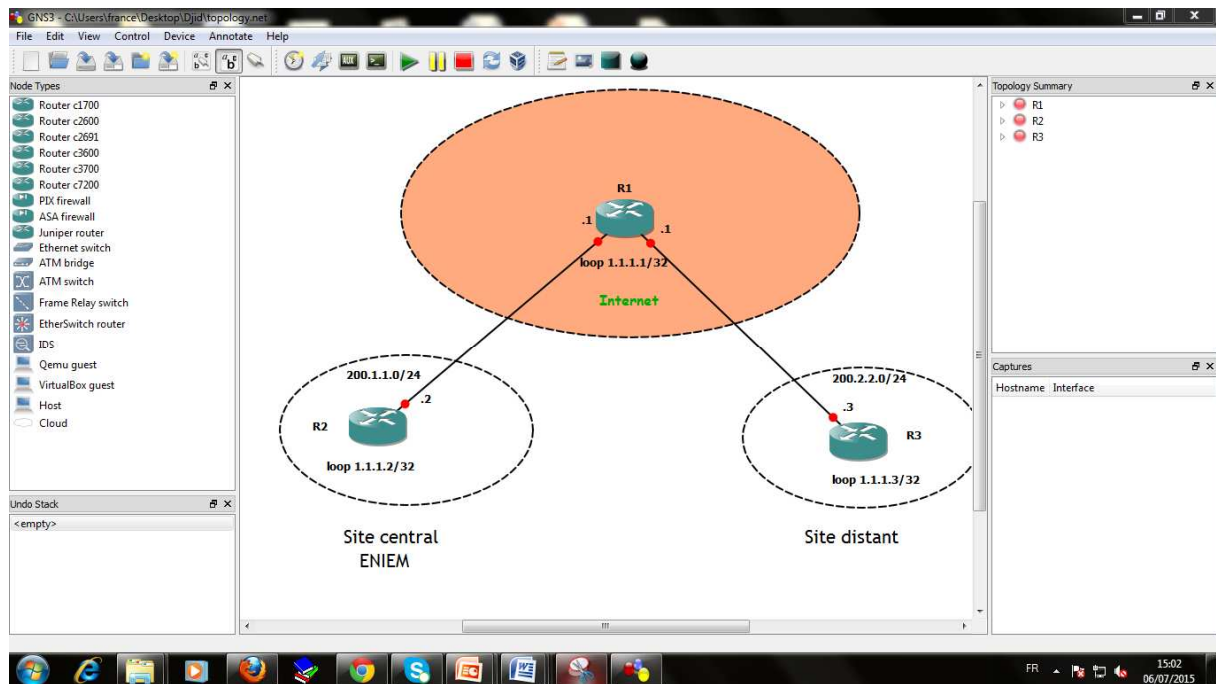
Annexe



Interconnection des différents routeurs.

Cliquer l'icone en haut située en dessous de <<Annotate>> et <<Help>> et sélectionner Fastethernet.

Annexe



Lancement des routeurs, cliquer en haut sur le bouton vert . Ou lancer individuellement les routeurs en cliquant droit et ...

Si on lance le gestionnaire des tâches on remarquera que la CPU plafonne à 100%.

Pour baisser cette charge, il suffit de lancer la fonction Idle PC, sélectionner la 1ère valeur ayant une étoile, si pas d'étoile sélectionner la première valeur.

Annexe

Le lancement de la fonction Idle PC peut être lancée sur un seul routeur allumé et la valeur sélectionnée s'appliquera à tous les autres routeurs.

Patienter quelques 30 secondes avant de pouvoir sélectionner 1 valeur.

Si la charge CPU ne descend pas, relancer la fonction Idle PC.

Annexe

II. Listes de quelques commandes CISCO :

« enable » ou « ena » ou « en » pour passer en mode administrateur sur l'équipement réseau.

Toutes les commandes indiquées ci-dessous sont à effectuer en mode administrateur. Pour obtenir de l'aide sur une commande faite nom de la commande suivie d'un point d'interrogation :

Exemple : show ?

Commandes	Descriptions
configure terminal ou conf t ou conf term	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
exit	Sort et remonte d'un cran dans la hiérarchie des menus
hostname ou host <hostname>	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet fastethernet Serial loopback <interface> ou int e fa s lo	Entre dans le mode de configuration de l'interface
ip address <address> <mask> ou ip add	Configure l'interface avec l'ip et le masque de réseau
no shutdown ou no shut	Active ou Désactive l'interface
copy running-config startup-config ou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
reload	Redémarre l'équipement réseau
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
show interfaces ou sh int	Donne une description détaillé sur les interfaces
show running-config ou sh run	affiche la configuration courante
show ip route ou sh ip route	affiche la table de routage
show ip protocols	affiche des informations sur les protocoles utilisés
show ?	donne toutes les commandes show disponibles

III. Etablissement d'un tunnel Isec site-à-site

1- Définir le trafic intéressant, c'est à dire le trafic à protéger par un tunnel Isec

Exemple :

```
access-list 110 permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255
```

2- Définir le secret partagé entre les 2 équipements établissant un tunnel Isec

!Pre-shared key avec le peer

```
crypto isakmp key cisco address 200.2.2.3
```

3- Définir les paramètres du tunnel IKE

!Policy ISAKMP

```
crypto isakmp policy 10
```

```
authentication pre-share
```

```
encryption des
```

```
hash md5
```

```
group 2
```

```
exit
```

4- Définir les paramètres du tunnel Isec

!Transform-set, parametres ipsec

```
crypto ipsec transform-set T1 esp-des esp-md5-hmac
```

5- Définir la crypto map

!Crypto map

```
crypto map M1 10 ipsec-isakmp
```

```
set peer 200.2.2.3
```

```
set transform-set T1
```

```
match address 110
```

Annexe

exit

6- Appliquer la crypto map

interface f0/0

crypto map M1

exit

Index

ENIEM : Entreprise Nationale des Industries de l'Electroménager.

AH : Authentification Header.

ECB : Electronic Code Book.

ESP : Encapsulating Security Payload.

FAI : Fournisseur d'Accès Internet.

IKE : Internet Key Exchange.

ISAKMP : Internet Security Association and Key Management Protocol

L2F : Layer Two Forwarding.

L2TP : Layer Two Tunneling Protocol.

LAC : L2TP Access Concentrator.

LNS : L2TP Network Server.

NAS : Network Access Server.

POP : Point of Presence.

PPP : Point to Point Protocole.

PPTP : Point to Point Tunneling Protocol.

SA : Security Association.

SLA : Service Level Agreement.

VPN : Virtual Private Network = RPV : Réseau Privé Virtuel.

IP : Internet Protocol

DOS : Denial Of Service

WAN :Wide Area Network

IPX Internetwork Packet Exchange

DES :Data Encryption Standard

MD5 :Message Digest 5

Index

ATM : Asynchronous Transfer Mod

UDP : User Datagram Protocol

RSA : Revenu de Solidarité Active

AES :Advanced Encryption Standard

TCP :Transmission Control Protocol

MAC : Media Access Control

SMTP :Simple Mail Transfer Protocol

CHAP :Challenge Handshake Authentication Protocol

MPLS :MultiProtocol Label Switching

PTP :Precision Time Protocol

DMZ: Demilitarized Zone

QM :Quick Mode

http : L'HyperText Transfer Protocol

FTP : File Transfer Protocol

DNS :Domain Name System

SSH : Secure Shell