République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

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

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

Mémoire de Fin d'Etudes de MASTER PROFESSIONNEL

Domaine : **Mathématiques et Informatique**
Filière : **Informatique**
Spécialité : **Ingénierie des systèmes d'information**

Présenté par
Anis GAOUAOUI
Abdelghani ISSOLAH

Thème

Implémentation d'une solution VPN pour sécuriser le réseau d'une entreprise < CAS : ENIEM >

Mémoire soutenu publiquement le 27/06/ 2016 devant le jury composé de :

Président : Mr Mohamed RAMDANE
Encadreur : M^{me} Ghenima BOURKACHE
Co-Encadreur : Mr Ferhat TALEB
Examinateur : M^{me} Samia BELLATAF
Examinateur : Mr Younes YACINE

REMERCIEMENTS

Nous faillirons à la tradition si nous n'exprimions ici notre gratitude envers tous ceux qui ont collaboré à la réalisation de notre projet, pour cela :

- *Nous remercions d'abord le bon Dieu de nous avoir donné le courage, la patience et la volonté afin d'accomplir notre parcours.*

- *Nous tenons à exprimer notre profonde reconnaissance et nos vifs remerciements à notre promotrice, Madame BOURKACHE, pour tous sesconseils précieux et ses encouragements.*

- *Nous adressons également nos remerciements au personnel de L'entreprise Nationale des Industries de l'Electroménager en particulier Mr. TALEB Ferhat notre encadreur pour le temps précieux qu'il nous a consacré, ses remarques pertinentes et précieuses, ses conseils et ses encouragements.*

- *Nous adressons nos remerciements également aux jurys, pour l'honneur qu'ils nous ont fait en acceptant de juger notre travail.*

- *Nous tenons à remercier, par ailleurs, tous les enseignants du département d'Informatique qui nous ont apporté leur aide, d'une manière ou d'une autre, tout au long de notre cursus.*

- *Notre gratitude va également à nos parents, pour leur aide et leur soutien.*

- *Enfin, nous tenons à remercier tous nos frères et sœurs, nos proches, et nos amis, ainsi que tous les étudiants de notre section.*

Dédicaces

Je dédie ce modeste travail

A mes très chers parents pour leurs sacrifices et leurs encouragements que dieu les protègent.

A ma chère et regrettée grand-mère que dieu l'accueille dans son vaste paradis.

A mon cher grand père que dieu le protège et le garde pour nous.

A mes chers frères et sœurs.

A mon cousin Mohammed et sa femme.

A mon cher binôme Abdelghani.

A tous mes ami(e) s

Anis … ✍

Dédicaces

Je dédie ce modeste travail
A mes très chers parents auxquels je souhaite une longue vie pleine de bonheur
A toute ma famille
A tous mes amis
A tous les étudiants du département Informatique

Abdelghani… ✍

Sommaire

SOMMAIRE

Chapitre II :Virtual Private Network

Chapitre III : Présentation de l'organisme d'accueil

Chapitre IV : conception et réalisation

SOMMAIRE

Liste Des Figures

CHAPITRE I

CHAPITRE II

CHAPITRE III

CHAPITRE IV

Liste Des Figures

Chapitre III

CHAPITRE IV

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 forcements 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.

Vu la grandeur du sujet que on a abordé, ce travail sera subdivisé en quatre chapitres :

- **Chapitre I :** Généralités sur les réseaux et la sécurité informatique : dans ce chapitre nous allons présenter certains concepts sur les réseaux informatiques.
- **Chapitre II :** Les VPN : dans ce chapitre nous allons aborder les technologies VPN et les protocoles de leur mise en place.
- **Chapitre III :** Présentation de l'organisme d'accueil: dans ce chapitre nous allons recueillir les informations qui nous permettent de mettre en œuvre notre travail au sein de l'entreprise.
- **Chapitre IV :** Conception et réalisation

I.1.Introduction

L'informatique est devenue un outil incontournable de gestion d'organisation, de production et de communication. Le réseau informatique de l'entreprise met en œuvre des données sensibles, les stockes, les partage en interne, les communique parfois à d'autres entreprises ou personnes ou les importe à partir d'autre sites .cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Vu l'importance des informations qui sont souvent véhiculées dans les réseaux, dés qu'un ordinateur d'un réseau est relié à Internet, la question de la sécurité se pose car l'Internet est une voie à double sens, c'est-à-dire elle permet non seulement d'émettre mais aussi de recevoir des informations mais il n'assure pas la sécurité de ces transactions. La garantie de la sécurité de ces informations est devenue un défi majeur pour les concepteurs des réseaux informatiques. Toutefois le constat est que ceux qui font usage des réseaux ignorent parfois les risques auxquels ils sont exposés lorsqu'une mesure de sécurité n'est pas mise en place. Les réseaux les plus sécurisés disposent très souvent d'un outillage matériel et logiciel afin d'assurer une sécurité optimale.

Tout au long de ce chapitre nous allons présenter quelques mécanismes qui assurent différents services de sécurité

I.2- Généralités sur les réseaux informatiques [1]

I.2.1- Définition d'un réseau informatique [1]

Un réseau informatique est un ensemble d'ordinateurs et périphériques connectés les unes aux autres afin d'assurer des échanges informatiques tel que le transfert des fichiers, le partage de ressources (imprimantes et données), la messagerie ou l'exécution de programmes a distance.

Le terme réseau en fonction de son contexte peut désigner plusieurs choses:

- Désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qui est le cas lorsqu'on parle de l'internet.
- Décrire la façon dont les machines d'un site sont interconnectées
- Spécifier les protocoles qui sont utilisés pour que les machines communiquent.

Networking : Mise en œuvre des outils et des taches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources.
On appelle nœud (node) l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions (un ordinateur, un routeur, un concentrateur, un commutateur).

I.2.2- Les avantages de la mise en réseau

Un réseau informatique peut servir plusieurs buts distincts :

- ✓ Partager des ressources logicielles(applications)
- ✓ Partager des ressources matérielles(imprimantes).

- ✓ Partager des données.
- ✓ Communication entre personnes distantes (courrier électronique, discussion en direct,etc.)
- ✓ Communication entre processus (machines industrielles).
- ✓ Diminuer les couts.
- ✓ Organisations efficaces.
- ✓ Accès aux données en temps réel.

I.2.3-Classification des réseaux :

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs, que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques.

On peut classifier ces réseaux selon l'étendue et la topologie et selon l'organisation :

I.2.3.1- Selon l'étendue :

En fonction de la localisation, la distance et du débit, les réseaux sont classés en trois catégorie

1. LAN (Local Area Network)

Réseaux local, intra entreprise permettant l'échange de données et le partage de ressources. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

La vitesse de transfert de données d'un réseau local varie entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

2. MAN (Métropolitain Area Network):

Réseau métropolitain qui permet la connexion de plusieurs sites à l'échelle d'une ville. Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kms). Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

Dans un MAN on trouve des commutateurs ou des routeurs interconnectés par des liens hauts débits (en général en fibre optique)

3. WAN (Wide Area Network):

Réseau à l'échelle d'un pays, généralement celui des opérateurs. Le plus connu des WAN est internet.

Un WAN (ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.
Les débits disponibles sur un WAN résultent d'un arbitrage avec le cout des liaisons (qui augmente avec la distance).
Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

I.2.3.2-Selon la Topologie (Méthode d'accès)

1. **La topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau, elle désigne le fait que lors de l'émission de données sur le bus par une station de travail, l'ensemble des stations de travail connectées sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopie.

Figure I.1 : La topologie en bus

Cette topologie a pour avantage d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donnée que si l'une des connexions est défectueuses, c'est l'ensemble du réseau qui est affecté.

2. **La topologie en anneau**

L'information circule le long de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie.

Figure I.2 : La topologie en anneau

Dans cette topologie chaque ordinateur joue le rôle d'un répéteur en générant de nouveau le signale avant de le transmettre à l'ordinateur suivant, mais tout l'anneau doit être réinitialisé après chaque problème.

3. La topologie en étoile

L'ensemble des stations de travail est connecté à un concentrateur qui examine le contenu du message, le régénère et ne le transmet qu'à son destinataire. C'est en réalité un réseau de "n" liaisons point par point, car il établit un circuit entre une paire d'utilisateurs.

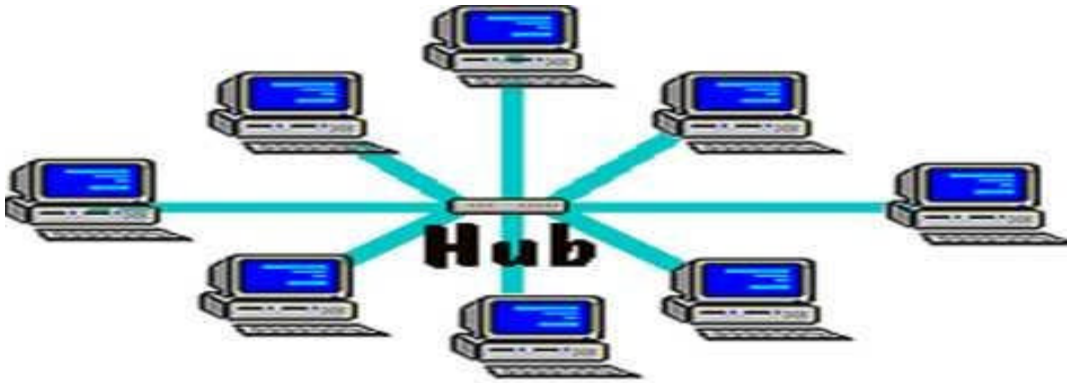


Figure I.3 : La topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivent une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du concentrateur sans paralyser le reste du réseau.

En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire.

I.2.3.3- Classification selon l'organisation

1. Egale à Egale (Peer to Peer)

Les postes de travail sont simplement reliés entre eux par le réseau. Aucune machine ne joue un rôle particulier. Chaque poste peut partager ses ressources avec les autres postes. C'est à l'utilisateur de chaque poste de définir l'accès à ses ressources. Il n'y a pas obligatoirement d'administrateur attiré, donc chaque poste est à la fois serveur et client. Ce type de réseau n'offre de réel intérêt que dans une configuration particulière dont les postes sont peu nombreux (pas plus d'une dizaine), et les utilisateurs restent attachés à un poste dont ils sont responsables.

- ✓ **Les avantages**

- Il est facile de mettre en réseau des postes qui étaient au départ isolés.
- Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.
- Dans un groupe de travail, l'imprimante peut être utilisée par tous.
- Cette méthode est pratique et peu couteuse pour créer un réseau domestique.

- ✓ **Les inconvénients**

- Chaque utilisateur a la responsabilité du fonctionnement du réseau.
- Les outils de sécurités sont très limités.
- Si un poste est éteint ou s'il se "plante", ses ressources ne sont plus accessibles.
- Le système devient ingérable lorsque le nombre de postes augmente.
- Lorsqu'une ressource est utilisée sur une machine, l'utilisateur de cette machine peut voir ses performances diminuer

2. Client/serveur

Ce type de réseau est le plus performant et le plus fiable. C'est ce type d'architecture que l'on retrouve sur les réseaux d'entreprise, qui peut parfaitement supporter plusieurs centaines de clients, voire plusieurs milliers.

- ✓ **Les avantages**

- Les serveurs sont conçus pour le partage de ressource et ne servent pas de station de travail. Il suffit de les dimensionner en fonction de la taille du réseau et du nombre de clients susceptible de s'y connecter.
- Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "Peer to Peer".
- Ils proposent également des fonctions avancées à l'usage des utilisateurs comme par exemple les profils itinérants qui permettent à un utilisateur (sous certaines conditions) de retrouver son environnement de travail habituel, même s'il change de poste de travail.

- Les serveurs étant toujours en service (sauf en cas de panne…), les ressources sont toujours disponibles pour les utilisateurs.
- Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en œuvre.

✓ **Les inconvénients**

- La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste", et le cout est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.
- Elle nécessite impérativement la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.
- Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer le fonctionnement en cas de panne.

I.2.4. Similitudes entre les différents types de réseaux

Les différents types de réseaux ont généralement les points suivants en commun :

- **Serveurs** : ordinateurs qui fournissent des ressources partagées aux utilisateurs par un serveur de réseau.
- **Clients** : ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau.
- **Support de connexion** : conditionne la façon dont les ordinateurs sont reliés entre eux.
- **Données partagées** : fichiers accessibles sur les serveurs du réseau.

  Imprimantes et autres périphériques partagés : fichiers, imprimantes ou autres éléments utilisés par les usagers du réseau.
- **Ressources diverses** : autres ressources fournies par le serveur.

I.2.5. La communication sur un réseau

La transmission d'information entre deux programmes d'informatiques sur deux machines différentes passe par deux modèles : le modèle OSI ou le modèle TCP/IP. Ces deux normes permettent à chaque partie de la communication de dialoguer. Chaque modèle inclut plusieurs couches. Le terme couche est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs niveaux de protocoles.

L'intérêt d'un modèle en couches est de séparer le problème en différentes parties selon leur niveau d'abstraction. Ainsi, chaque couche du modèle communique avec une couche adjacente, utilise les services de couches inférieures et fournit des services à la couche de niveau supérieur.

I.2.5.1. Le modèle OSI et le model TCP/IP[3]

1. Le modèle OSI :

1.1. Les différentes couches du modèles OSI :

Le modèle OSI est un modèle qui comporte 7 niveaux différents le transfert de données, ces niveaux sont également appelés couches.

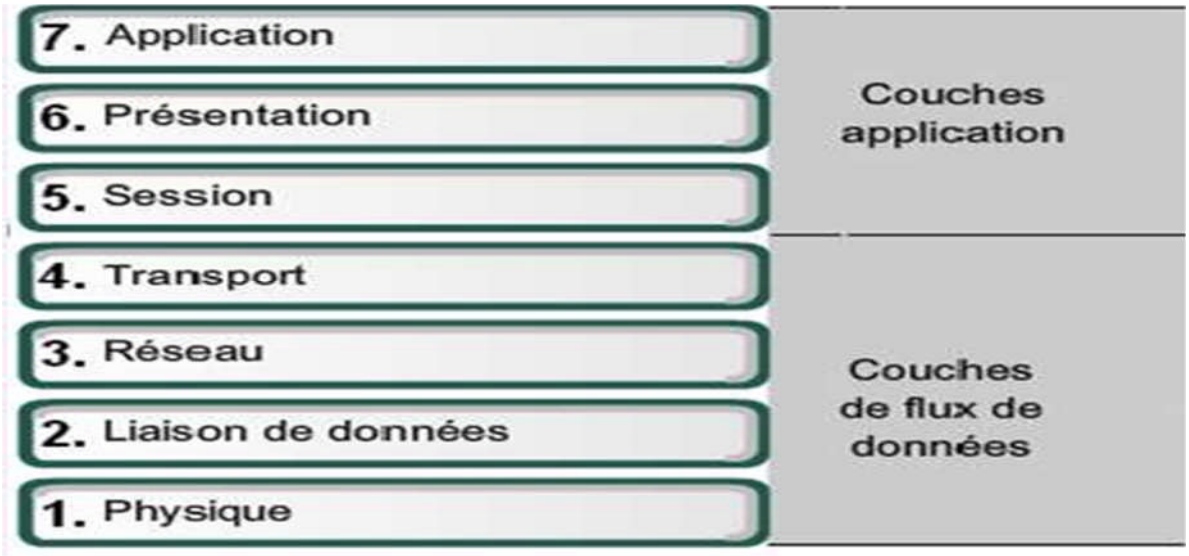


Figure I.4 : Les 7 couches du modèle OSI

Couche Application(7)

- Sert d'interface entre les applications a chaque extrémité du réseau;
- Permet d'échanger des données entre les programmes s'exécutant sur hôtes source et de destination.

Couche Présentation(6)

- Codage et conversion des données de la couche application afin que les données issues du périphérique source puissent être bien interprétées sur le périphérique de destination
- Compression des données de sorte que celles-ci puissent être décompressées par le périphérique de destination;
- Chiffrement des données en vue de leur transmission et déchiffrement des données reçues par le périphérique de destination.

Couche Présentation (5)

- Permet d'initier un dialogue entre les applications source et de destination;
- Initier et maintenir un dialogue;

- Redémarrer les sessions interrompues ou inactives pendant une longue période.

Couche transport(4)

- Permet l'acheminement de bout en bout sans se soucier des relais intermédiaires;
- Fragmentation du message en unités plus dites paquets;
- Multiplexage.

Couche réseau(3)

- Permet l'acheminement de bout en bout en tenant compte des nœuds intermédiaires;
- Routage et ordonnancement des paquets.

Couche liaison de données(2)

- Structuration des données en trames;
- Masquer les caractéristiques physiques;
- Contrôle d'erreur à l'émission et à la réception.

Couche physique(1)

- Assurer la transmission de bits entre les entités physiques;
- Spécifie la nature du support de communication;
- Le mode de connexion et le brochage le cas échéant;
- La technique de codage des bits en signaux électriques;
- Les tensions et les fréquences utilisées.

1.2.Les avantages du modèle OSI

- ❖ Réduit la complexité
- ❖ Uniformise les interfaces
- ❖ Facilite la conception modulaire
- ❖ Assure l'interopérabilité de la technologie
- ❖ Accélère l'évolution
- ❖ Simplifier l'enseignement et l'acquisition des connaissances

2- Le modèle TCP/IP[4] :

Le modèle TCP/IP est inspiré du modèle OSI. Il fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, mais ne contient, lui, que quatre couches. Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

TCP (Transfert Contrôle Protocole) : se charge du transport de bout en bout pour toute application.

IP (Internet Protocole) : est responsable du routage à travers le réseau.

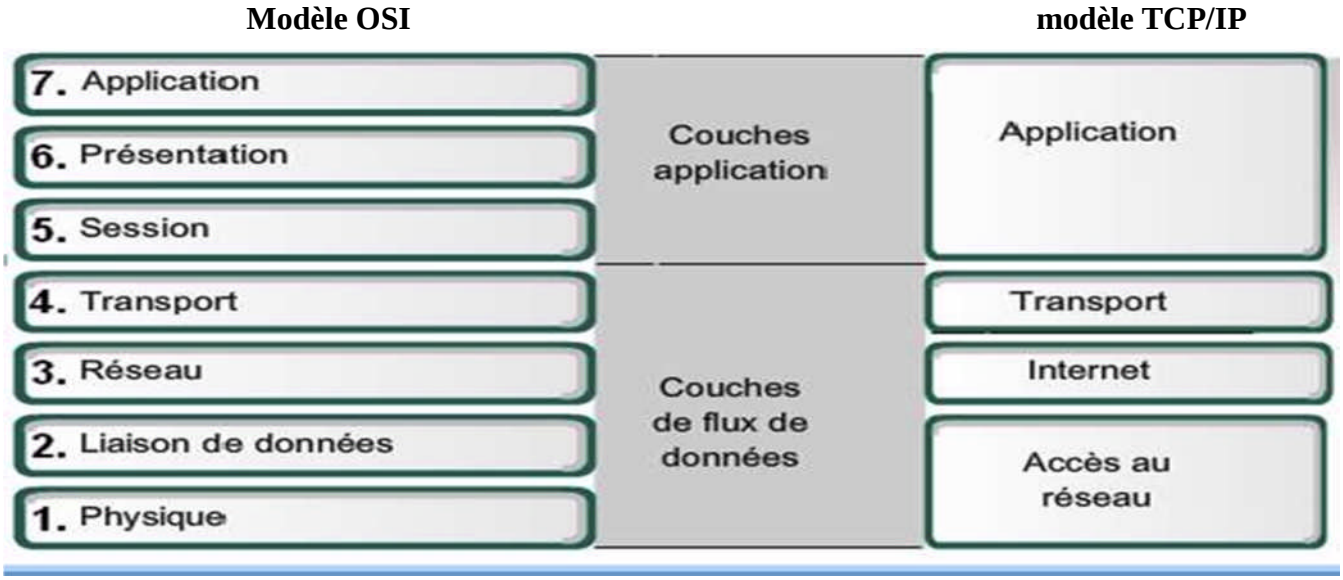


Figure I.5. Les couches du modèle TCP/IP

Couche application(4)

- Elle englobe l'application standard du réseau (Telnet, SMTP,FTP…).

Couche transport(3)

- Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.

Couche Internet(2)

- Elle est chargée de fournir le paquet de données (datagramme).

Couche Accès réseau (1)

- Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.

I.2.6- Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état originel.

- Le paquet de données est appelé **message** au niveau de la couche application
- Le message est ensuite encapsulé sous forme de **segment** dans la couche transport. Le message est donc découpé en morceaux avant envoi.
- Le segment une fois encapsulé dans la couche Internet prend le nom de **datagramme**.
- Enfin, on parle de **trame** au niveau de la couche accès réseau

I.2.7 -Les différents protocoles

✓ **Protocole TCP**

TCP (Transmission Contrôle Protocole) est l'un des principaux protocoles de la couche transport, créé dans le but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs autonomes et raccordés à un réseau. TCP est un protocole orienté connexion (il permet à deux machines qui communiquent de contrôler l'état de la transmission). Les caractéristiques principales du protocole TCP sont les suivants:

- Remettre en ordre les datagrammes à l'aide du protocole IP.
- Vérifier le flot de données afin d'éviter une saturation du réseau.
- Formater les données en segments de longueur variable afin de les remettre au protocole IP.
- Faire circuler simultanément des informations provenant de sources distinctes sur une même ligne.
- Permet l'initialisation et la fin d'une communication.

✓ **Protocole UDP**

Le protocole UDP (User Datagram Protocol) est comme TCP, un protocole de transport de données. Cependant, contrairement à TCP, on qualifie l'UDP de transmission « en mode non connecté et non fiable » ou encore de protocole « non orienté connexion ». Ceci signifie simplement que la machine émettrice envoie des données sans parvenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première.

Les données sont ainsi envoyées sous forme de bloc (datagramme). Il n'y a pas de contrôle d'erreur.

✓ **Protocole IP**

Le protocole IP fait partie de la couche internet, c'est l'un des protocoles des plus importants d'internet car il permet l'élaboration et le transport des datagrammes IP, sans toutefois en assurer la livraison. En réalité le protocole IP traite les datagrammes IP indépendamment les un des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire du message grâce à trois champs :

- Le champ adresse IP : c'est l'adresse de la machine, Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de 0 à255 (4 fois 8 bits), on les note sous la forme xxx.xxx.xxx.xxx ou chaque xxx représente un entier de 0 à255.
- Le champ masque de sous-réseau : un masque de sous-réseau permet au protocole IP de déterminer la partie de l'adresse IP qui concerne le réseau.
- Le champ passerelle par défaut : il permet au protocole internet de savoir à quelle machine remettre le datagramme si jamais la machine de destination n'est pas sur le réseau local.

✓ **Protocole ARP**

Le protocole ARP (Adress Resolution Protocol) a un rôle important parmi les protocoles de la couche internet de la suite TCP/IP, car il permet de connaitre l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle protocole de résolution d'adresse.

Le protocole ARP interroge les machines du réseau pour connaitre leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache. Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. Les machines du réseau vont comparer cette adresse logique à la leur, si l'une d'entre s'identifie à cette adresse, la machine va répondre à ARP qui va stocker le couple d'adresse dans la table de correspondance et la communication va pouvoir avoir lieu.

✓ **Protocole RARP**

Le protocole RARP (Reverse Adress Resolution Protocol) est beaucoup moins utilisé, il signifier protocole ARP inversé, il permet à une station de connaitre son adresse IP à partir d'une adresse table de correspondance entre adresse physique (MAC) et adresse IP hébergée par une passerelle située sur le même réseau.

✓ **Protocole ICMP**

Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer des messages de contrôle ou d'erreur vers d'autre machines ou passerelles. ICMP rapporte les messages d'erreurs à l'émetteur initial. Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontrées sur l'Internet : machine destination

déconnectée, durée de vie des datagrammes expirée, congestion de datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagramme IP et sont routés comme n'importe quel datagramme IP sur l'Internet. Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP.

✓ **Protocole FTP**

Le protocole FTP (File Transfer Protocol) définit la façon laquelle des données doivent être transférées sur TCP/IP. Le protocole FTP a pour objectifs de :

- Permettre un partage de fichiers entre deux machines distantes.
- Permettre une indépendance aux systèmes de fichiers des machines clientes et serveur.
- Permettre de transférer des données de manière efficace.

✓ **Protocole TELNET**

Le protocole TELNET est un protocole standard d'internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Il utilise un modèle client/serveur qui permet d'exécuter à distance. Il est souvent utilisé pour exécuter des commandes sur un serveur à partir d'un terminal.
Le TELNET est utile non seulement pour récupérer des emails, des informations et des programmes mais également pour l'entretien de site web, et la configuration de routeur à distance. Le serveur TELNET n'est pas sécurisé, toutes les informations (y compris le compte d'utilisateur et le mot de passe) circulent en clair sur le réseau.
Lorsque le protocole TELNET est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.

✓ **Protocole SMTP**

Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier d'une machine à une autre. Ce protocole fonctionne en mode connecté, il est par défaut sur le port 25.

✓ **Protocole POP3**

Le protocole POP3 (Port Office Protocole version 3) occupe le port 110, il est nécessaire pour les personnes n'étant pas connectées en permanence à internet de pouvoir consulter les mails reçus hors connexion.

I.3. La sécurité informatique :

Le réseau Internet est devenu un outil essentiel de communication depuis sa mise en service. Dès qu'un ordinateur d'un réseau est relié à Internet, la question de la sécurité se pose car l'Internet est une voie à double sens, c'est-à-dire elle permet non seulement d'émettre mais aussi de recevoir

des informations mais il n'assure pas la sécurité de ces transactions. La garantie de la sécurité de ces informations est devenue un défi majeur pour les concepteurs des réseaux informatiques. Tout au long de ce chapitre nous allons présenter quelques mécanismes qui assurent différents services de sécurité.

I.3.1. La sécurité:[2]

Les utilisateurs d'Internet doivent prendre un minimum de précautions, car leurs ordinateurs peuvent être facilement attaqués. La sécurité informatique est mise en œuvre pour éviter ce genre de problèmes, elle désigne un ensemble de techniques et de bonnes pratiques pour protéger les ordinateurs et les données qui y sont stockées, si elles sont élaborées par des spécialistes, les plus simples doivent être connues et mises en œuvre par les utilisateurs. La sécurité informatique est l'ensemble de moyens et de mesures mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles, et aussi pour empêcher l'utilisation non autorisée et le mauvais usage d'un ensemble de connaissances, de faits, de données ou de moyens.

I.3.2. Pourquoi les systèmes sont vulnérables ?

- La sécurité est chère et +/-difficile à mettre en œuvre.
- La sécurité ne peut être sure à100%.
- La politique de sécurité est complexe et basée sur des jugements humains
- Les organisations acceptent (parfois) de courir le risque, la sécurité n'est pas une priorité
- De nouvelles technologies (et donc vulnérabilités) émergent en permanence
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes.

I.3.3 Un système ne peut être sur a 100%

- Il est impossible de garantir la sécurité totale
- Les bugs dans les programmes courants et les systèmes d'exploitation sont nombreux
- La cryptographie a ses faiblesses : les mots de passe peuvent être cassés
- Même un système fiable peut être attaqué par des personnes abusant de leurs droits
- Plus les mécanismes de sécurité sont stricts, moins ils sont efficaces
- On peut s'attaquer aux systèmes de sécurité eux-mêmes…

I.3.4. 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 :

- 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.

I.3.5. Notion de risque en informatique :

Le risque peut se résumer par l'équation suivante :

Risque = Vulnérabilité x Menace x Impact

- ***Les menaces***

  Désigne l'ensemble des éléments (généralement externes) pouvant atteindre les ressources informatiques d'une organisation.

- ***Les vulnérabilités***

  Expriment toutes les faiblesses des ressources informatiques qui pourraient être exploitées par des menaces, dans le but de les compromettre.

- ***L'impact***

  Est le résultat de l'exploitation d'une vulnérabilité par une menace et peut prendre différentes formes : perte financière, affectation de l'image de marque, perte de crédibilité…etc.

I.3.6. 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 :

-La confidentialité : demande que l'information sur le système ne puisse être *lue* que par les personnes autorisées.

-L'intégrité de données : Le service d'intégrité assure la conformité de l'information. Il permet aux utilisateurs d'avoir la certitude que l'information est correcte et qu'elle n'a pas été modifiée par un individu non autorisé. Le service d'intégrité protège les systèmes contre les attaques de modifications. Comme pour la confidentialité le service d'intégrité doit collaborer avec le service de responsabilité pour identifier correctement les personnes et ainsi même les modifications de fichiers à l'extérieure de l'entreprise peuvent être détectées.

-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.

I.3.7. 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'attirance 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.

I.3.8- Politique des hackers :

La Meilleure façon de protéger son système informatique est de procéder de la même manière que les pirates, afin de cartographier les vulnérabilités du système :

I.3.8.1- Reconnaissance du système

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**

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**

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 par feux. Parmi les techniques les plus utilisées pour acquérir ces informations, nous évoquons les utilitaires : **Ping [102]**, **Trace Route [103]** et **Nmap [104].**

I.3.8.2. Exploitation du système

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).

I.3.8.3. Préservation d'accès

Les attaquants installent des **portes dérobées** 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.

I.3.8.4. Effacement des traces

Une fois la porte dérobée est crée, 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.

I.3.9. Différents types d'attaques :[3]

I.3.9.1. Les attaques réseaux:

Les attaques réseaux les plus connues aujourd'hui sont :

1. **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.

2. **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.

3. **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:

- **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**

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 de1

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 récupèrera la connexion pour lui.

I.3.9.2. Les attaques applicatives:

1. Injection SQL :

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 (I.1) se transforme en (I.2) et sera toujours vérifiée si l'utilisateur

$var Nom existe dans la table utilisateur.

select * from utilisateur where nom = $varNom and mot2passe=$varPasse (I.1) select * from utilisateur where nom = $varNomandTrue (I.2)

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

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

2. Les bugs :

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.

I.3.9.3. Les attaques par déni de service:

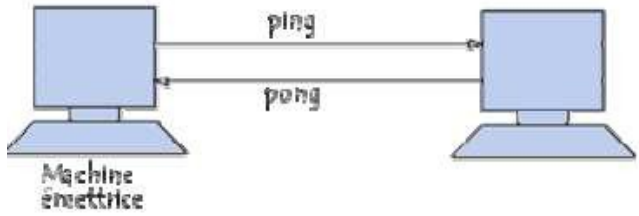
Les attaques par déni de service (**DOS**) est différent des autres types d'attaque en cela qu'elles n'occasionnent pas de dommages irréversibles sur le réseau. Au lieu de cela, elles tentent de

mettre le réseau hors service en bombardant un ordinateur particulier (un serveur ou un dispositif du réseau) ou en ralentissant le débit des liaisons réseau jusqu'à ce que les performances soient suffisamment médiocres pour irrites les clients et occasionner un manque à gagner pour l'entreprise.

1. La technique dite du smurf:[4]

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.



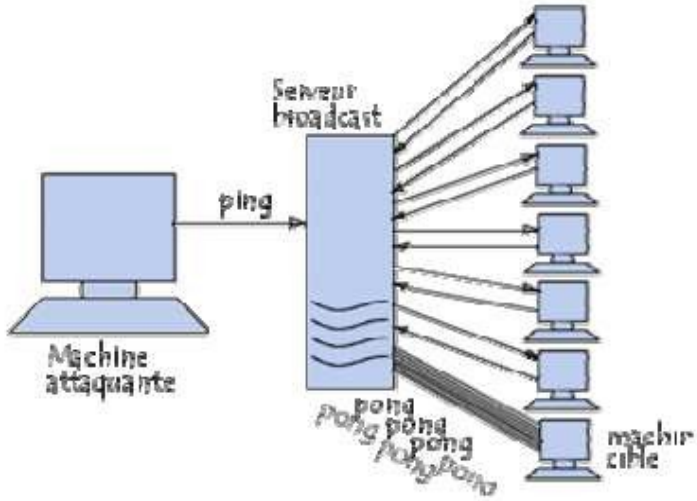


Figure I.6 : Exemple d'attaque**[4]**

2. SYN FLOOD

Est une attaque réseau par saturation (déni de service) exploitant le mécanisme de poignée de main (3-way handshake), lorsqu'un client établit une connexion à un serveur :

- ✓ Le client envoie une requête SYN.
- ✓ Le serveur répond alors par paquet SYN/ACK
- ✓ Et enfin le client valide la connexion par un paquet ACK (*acknowledgement*, qui signifie *accord* ou *remerciement*).

3. Fragmentation

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

I.3.9.4. Les attaques virales:

Il existe principalement plusieurs types de menaces distinctes :

1. Les virus :

Les virus sont des programmes autonomes conçus pour se reproduire et se diffuser de manière autonome. Deux éléments caractérisent un virus :

- ✓ La façon dont il se reproduit et infecte le système informatique.
- ✓ Les actions délétères qu'il va réaliser.

2. Les vers :

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

3. La bombe logique :

La bombe logique est constituée d'une simple fonction destructrice insérée dans un programme d'usage général, son activation se déclenche lorsqu'une condition particulière est remplie par exemple l'effacement de données et programmes dés qu'un nom ne figure plus dans la liste du personnel. Elle peut également agir à compter d'un nombre donné d'instruction ou encore lors de l'accès à un enregistrement particulier. La fonction destructrice reste en sommeil tant que l'événement programmé n'a pas lieu.

4. Les chevaux de Troie :

Les chevaux de Troie (Trojanhorses) tirent leur nom de la célèbre légende mythologique. Comme dans cette dernière, les troyens utilisent une ruse agir de façon invisible, le plus souvent en se greffant sur un programme anodin. Les chevaux de Troie ne reproduisent pas (en tout cas, ce n'est pas leur objectif premier). Ce sont à la base de simples programmes destinés à être exécutés à l'insu de l'utilisateur.

5. Le piratage :

C'est-à-dire l'accès non autorisé d'un tiers à tout ou partie du système d'information de l'entreprise. Le pirate qui obtient un accès, même de niveau utilisateur, peut alors à sa guise modifier les données, arrêter certain serveurs vitaux, voire détruire l'ensemble des informations. Il s'agit bien sûr d'un risque majeur.

6. Les trappes :

Une trappe ou **backdoor** est un point d'entrée dans un système informatique qui passe au-dessus des mesures de sécurité les plus communes. C'est généralement un programme caché ou un composant électronique qui rend le système inefficace. Ce peut être aussi une modification volontaire du code d'un programme, qui permet très facilement à son développeur de créer son propre outil d'intrusion.

I.3.10. Quelques techniques de défenses:

- Installer un anti-virus et le tenir à jour.
- Installer un Pare-feu ou Firewell ou bien Garde Barrière : contrôle l'accès à un ordinateur et affiche un message dès qu'un intrus essaye d'y pénétrer.
- Installer un logiciel anti-espion.
- Sauvegarder ses données sur des supports extérieures.
- Authentification : assurance que l'expéditeur d'un message est bien la personne qu'il prétend être, elle peut se faire par mot de passe.
- Contrôle d'accès : ensemble des stratégies et mesures adoptées par une entreprise pour se prémunir contre les différentes formes d'intrusions.
- Cryptographie (chiffrement) : est l'art de rendre des données secrètes.
- Test de vulnérabilité : outil de détection des failles dans les systèmes de protections.
- Test d'intrusion : exploiter une vulnérabilité pour essayer d'accéder à un système.
- Audit : définir les types d'événements à inspecter sur tous les systèmes (exemple : établissement des connexions).

I.3.11. La planification de la sécurité du réseau :

Elle comporte quatre étapes :

a) Préparation : c'est la définition des limites et de la portée de la sécurité du réseau, inventaire et évaluation des biens informatiques et énoncé de la nature délicate de l'information résidant dans le réseau et circulant sur celui-ci.

b) Évaluation des menaces et exposition à celles-ci : c'est la détermination des menaces qui pèsent sur chaque bien du réseau, incidences pour l'organisation si ces menaces se matérialisaient et

probabilité que cela se produise. Les résultats de cette étape permettent d'établir des degrés d'exposition pour chaque scénario sur les biens informatiques.

c) Évaluation des risques : à partir des degrés d'exposition établis pour les biens informatiques menacés, on analyse les points vulnérables du réseau et l'efficacité des mesures de protection en place afin de déterminer les risques associés à chaque scénario.

d) Politique de sécurité du réseau : c'est la préparation d'une politique de sécurité du réseau qui établit les étapes requises afin de réduire les risques à des niveaux acceptables.

I.3.12. Outils de la sécurité:

I.3.12.1. Cryptographie : [5]

Les récents développement de la cryptographie permettent de résoudre les nombreux problèmes menaçants la vie privé ou la sécurité sur internet, la cryptographie est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information telle la confidentialité, l'intégralité des données, authentification d'entités, et l'authentification de l'originalité des données ,C'est un ensemble de techniques qui fournit la sécurité de l'information. La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne peuvent être lues par personne à l'exception du destinataire convenu.

- **Les concepts généraux de la cryptographie :**

La cryptographie repose sur quatre concepts généraux : le texte en claire, l'algorithme cryptographique, le texte codé et la clé.
Le texte en claire : est le message sous sa forme originale, que se soit avant le chiffrement ou après le déchiffrement.
L'algorithme Cryptographique : est l'opération mathématique utilisé pour chiffrer ou déchiffrer le message.
Le texte codé : est le message après qu'il a été chiffré. Le message du texte codé apparait confus et intangible aux personnes auxquels il n'est pas destiné.
La clé : est un ensemble unique de caractère (tel qu'un nombre ou un mot de passe) que le chiffre utilise pour chiffrer et déchiffrer le message.

- **La cryptographie permet d'assurer :**

1. **La confidentialité :**

La confidentialité est le premier problème posé à la cryptographie, il se résout par la notion de chiffrement.

1.1. Chiffrement :

Pour crypter un message ou un texte qu'on appellera texte en clair, on lui applique une série d'opérations simples telles que la substitution et la permutation suivant des règles bien définies qui ne sont connues que par l'émetteur et le récepteur du message dans le but de le rendre inintelligible pour les tiers non autorisés (cryptogramme ou texte chiffré) et on appelle ce procédé chiffrement.
Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans le monde de l'informatique moderne, les transformations en question sont des algorithmes construits à base de fonctions mathématiques qui dépendent d'un paramètre qu'on appelle clé de chiffrement/déchiffrement. [5]
Clé : Ensemble des données d'entrée de l'algorithme qui transforme le texte clair en texte chiffrée et inversement. Il existe deux grandes familles d'algorithmes cryptographiques à base de clefs :

a. Les algorithmes à clef privée : (Chiffrement symétrique) :

Le chiffrement à clé privée exige que toutes les parties qui sont autorisées à lire l'information aient la même clé que celle qui est utilisée pour le chiffrement des données. Clef de chiffrement = clé de déchiffrement

- Comme exemple d'algorithme à clé privée, on peut citer : Kerberos, Data Encryption Standard, International Data Encryption Algorithmes...

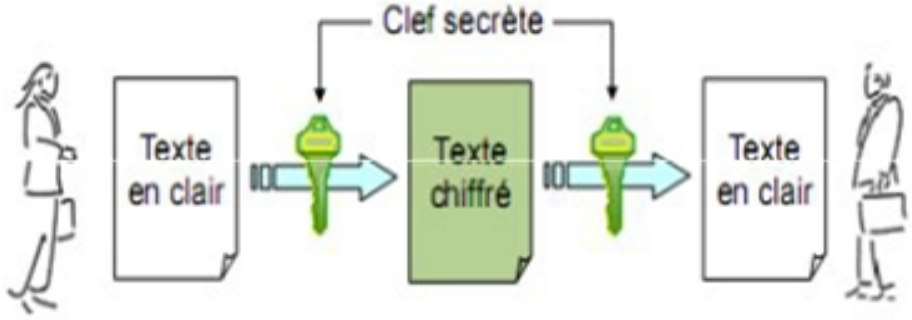


Figure I.7 : Schéma représentant le chiffrement symétrique [5]

b. Les algorithmes à clef publique : (Chiffrement asymétrique) :

Clef de chiffrement ≠ clé de déchiffrement

Le chiffrement asymétrique se base sur deux clés (une privée et une autre publique) pour chiffrer et déchiffrer les messages. Ces clefs sont distinctes et générées en même temps et elles dépondent étroitement l'une de l'autre, c.à.d. lorsqu'on chiffre avec l'une des clés, on doit forcément déchiffrer avec l'autre. Ainsi en utilisant la clef publique, tout le monde peut chiffrer un message que seul le propriétaire de la clef privée pourra déchiffrer, et inversement, si on utilise la clef privée pour le chiffrement, tout le monde (ceux qui possèdent la clé publique) peut déchiffrer. [5]

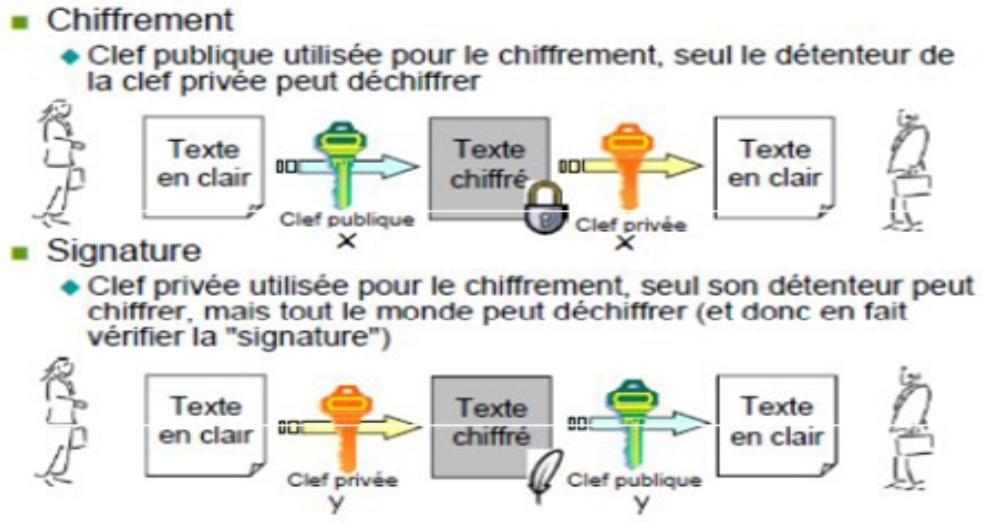


Figure I.8 : Cryptographie à clef publique [5]

On peut identifier la provenance des données chiffrées par à la clef privée puisque une seule personne la possède, et donc lorsqu'une personne déchiffre le message avec sa clé publique, elle sait très bien d'où le message provient.

2. Intégrité et authenticité :

Authenticité=Authentification + Intégrité

Souvent on utilise le terme authentification afin de désigner l'authenticité, mais notez bien que l'authentification et l'intégrité sont inséparables. Lorsqu'un échange d'informations se présente au travers d'un canal de communication peu sûr, le destinataire aimerait bien s'assurer que le message s'émane de l'auteur auquel il est attribué et qu'il n'a pas été altéré pendant son voyage à travers le canal.

- **Authentification :** Consiste à s'assurer que les données s'émanent bien de l'expéditeur et non pas d'un autre utilisateur ou autre personne qui se prend pour l'expéditeur même.
- **Intégrité :** Consiste à s'assurer que les données n'ont pas été modifiées durant leur transfert. Pour répondre à ces deux critères, les signatures et les certificats numériques sont apparus.

2.1. Signature numérique:

Un des avantages majeurs de la cryptographie à clé publique est qu'elle procure une méthode permettant d'utiliser des signatures numériques. Les signatures numériques permettent 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 [6]. Ainsi, les signatures numériques des systèmes à clé publique permettent l'authentification et le contrôle d'intégrité des données. Une signature numérique procure également la non-répudiation, ce qui signifie qu'elle empêche l'expéditeur de contester ultérieurement qu'il ait bien émis cette information. Ces éléments sont au moins aussi importants que le chiffrement des données, sinon davantage. Une signature numérique a le même objet qu'une signature

manuelle. Toutefois, une signature manuelle est facile à contrefaire. Une signature numérique est supérieure à une signature manuelle en ce qu'elle est pratiquement impossible à contrefaire et, de plus, elle atteste le contenu de l'information autant que l'identité du signataire.
La norme ISO 7498-2 définit la signature numérique comme étant des données rajoutées à une unité de données ou une transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données en question (seul l'expéditeur est apte à générer la signature).
Sur le plan conceptuel, il est recommandé d'utiliser une clef privée car seul son possesseur pourra générer la signature et toute personne possédant la clef publique correspondante est apte de la vérifier.
La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature numérique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

- **Authentique :** L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- **Infalsifiable :** La signature ne peut pas être falsifiée. Quelqu'un d'autre ne peut se faire passer pour un autre.
- **Non réutilisable:** La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- **Inaltérable :** Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- **Irrévocable :** La personne qui a signé ne peut le nier.

La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique.
Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres.

2.2. Fonction de hachage :

Lors d'échanges de messages chiffrés, il est important de pouvoir s'assurer que le message n'a pas été altéré ou modifié par un tiers pendant l'envoi. Les fonctions de hachage permettent alors de s'assurer de l'intégrité du message. Aussi appelée fonction de condensation, une fonction de hachage est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe, la chaîne résultante est appelée empreinte (digest en anglais) ou condensé de la chaîne initial [7]. La fonction de hachage est une fonction à sens unique, c'est-à-dire qu'elle doit permettre de trouver

facilement l'empreinte à partir du message, et d'empêcher de retrouver le message à partir de l'empreinte. Elle doit aussi être très sensible, pour qu'une petite modification du message entraîne une grande modification de l'empreinte . Autre caractéristique d'une fonction de hachage, est qu'elle doit être sans collision, c'est-à-dire qu'il est impossible de trouver deux messages ayant la même empreinte. En envoyant le message accompagné de son empreinte, le destinataire peut ainsi s'assurer de l'intégrité du message en recalculant le résumé à l'arrivée et en le comparant à celui reçu. Si les deux résumés sont différents, cela signifie que le message n'est plus le même que l'original, et qu'il a été altéré ou modifié.

Exemple : **MD5 (Message Digest 5)** qui fournie une empreinte de 128 bits. **SHA** (Secure Hash Algorithm) qui donne une empreinte de 160 bits.

NB : On utilise souvent le terme fonction de hachage pour désigner fonction de hachage à sens unique sans collisions.

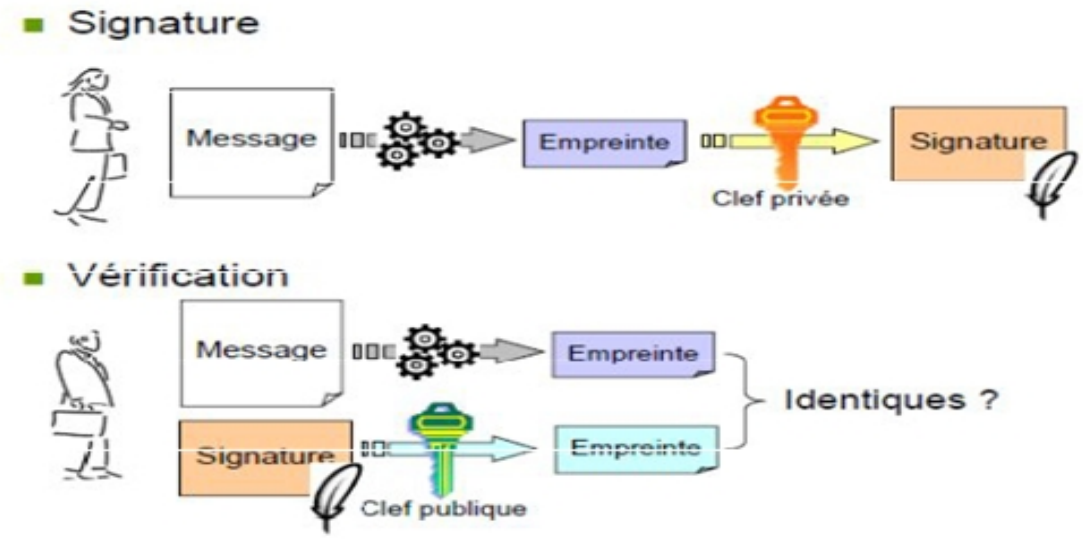


Figure I.9: Exemple de méthode de signature numérique. [5]

2.3. Certificat électronique :

Dans un environnement de clé publique, il est essentiel de s'assurer que la clé publique avec laquelle vous chiffrer les données est celle du destinataire concerné et non une contrefaçon.

Un certificat numérique ou électronique fonctionne en gros comme une pièce d'identité matérielle. Un certificat numérique est une information attachée à une clé publique, et qui permet de vérifier que cette clé est authentique, ou valide. Les certificats numériques sont utilisés pour contrecarrer les tentatives de substituer une clé falsifiée à la clé véritable. [7] Un certificat numérique comporte trois éléments:

- Une clé publique.
- Une information de certification ('l'identité' de l'utilisateur, comme son nom, son adresse e-mail, etc.).
- Une ou plusieurs signatures numériques.

L'objet de la signature numérique sur un certificat est de garantir que les informations de certification ont été contrôlées par une autre personne ou organisme. La signature numérique

ne garantit pas l'authenticité du certificat complet, elle garantit seulement que les informations d'identité ainsi signées correspondent bien à la clé publique à laquelle elles sont attachées.

I.3.12.2. firewall : [8]

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.

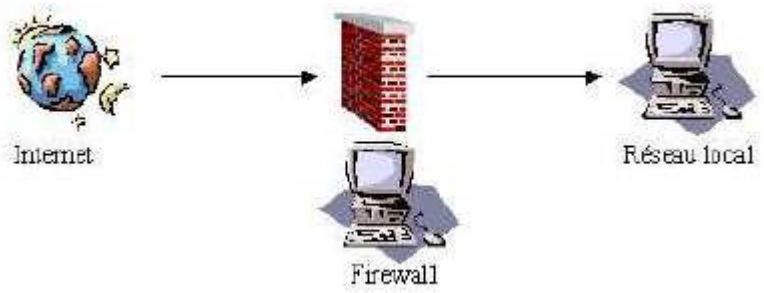


Figure I.10 : Placement d'un firewall

Il existe plusieurs types de techniques de firewall :

- 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 :

- 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

I.3.12.3. Mots de passes :

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.

I.3.12.4. Réseau Privé Virtuel (VPN) :[9]

Les réseaux privés virtuels (VPN : Virtual Private Network) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service n'est garantie (nous détaillons cette approche dans le chapitre suivant).

I.3.12.5. Système de détection d'intrusion : [10]

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte) [14]. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

- Les familles de systèmes de détection d'intrusion

Il existe trois grandes familles distinctes d'IDS :

- Les NIDS (Network Based Intrusion Detection System), qui surveillent l'état de la sécurité au niveau du réseau.
- Les HIDS (HostBased Intrusion Detection System), qui surveillent l'état de la sécurité au niveau des hôtes.
- Les IDS hybrides, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.

Les HIDS sont particulièrement efficaces pour déterminer si un hôte est contaminé et les NIDS permettent de surveiller l'ensemble d'un réseau contrairement à un HIDS qui est restreint à un hôte.

1. **NIDS (IDS réseau)**

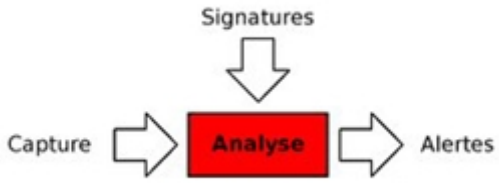


Figure I.11 : Les trois parties d'un NIDS

Un NIDS se découpe en trois grandes parties : La capture, les signatures et les alertes.

- **Capture**

La capture sert à la récupération de trafic réseau. En général cela se fait en temps réel, bien que certains NIDS permettent l'analyse de trafic capturé précédemment.

La plupart des NIDS utilisent la bibliothèque standard de capture de paquets libpcap. La bibliothèque de capture de paquets Packet Capture Library est portée sur quasiment toutes les plates-formes, ce qui permet en général aux IDS réseau de suivre.

Le fonctionnement de la capture d'un NIDS est donc en général fortement lié à cette libpcap. Son mode de fonctionnement est de copier (sous Linux) tout paquet arrivant au niveau de la couche liaison de données du système d'exploitation. Une fois ce paquet copié, il lui est appliqué un filtre BPF (Berkley Packet Filter), correspondant à l'affinage de ce que l'IDS cherche à récupérer comme information.

Il se peut que certains paquets soient ignorés car sous une forte charge, le système d'exploitation ne le copiera pas.

Le comportement de la libpcap est différent dans le monde BSD, puisqu'il lui attache le fichier périphérique /dev/bpf, permettant ainsi aux NIDS de ne pas avoir besoin des droits super utilisateur pour capturer le trafic mais simplement de pouvoir lire sur ce fichier sur lequel les filtres sont directement compilés.

Aussi, le trafic analysé n'est pas forcément égal à celui du trafic entrant, étant donné que la libpcap agit à une couche en dessous du pare-feu (qui agit au niveau réseau).

- **Signatures**

Les bibliothèques de signatures (approche par scénario) rendent la démarche d'analyse similaire à celle des antivirus quand ceux-ci s'appuient sur des signatures d'attaques. Ainsi, le NIDS est efficace s'il connaît l'attaque, mais inefficace dans le cas contraire. Les outils commerciaux ou libres ont évolué pour proposer une personnalisation de la signature afin de faire face à des attaques dont on ne connaît qu'une partie des éléments. Les outils à base de signatures requièrent des mises à jour très régulières.

Les NIDS ont pour avantage d'être des systèmes temps réel et ont la possibilité de découvrir des attaques ciblant plusieurs machines à la fois. Leurs inconvénients sont le taux élevé de faux positifs qu'ils génèrent, le fait que les signatures aient toujours du retard sur les attaques de type 0day et qu'ils peuvent être la cible d'une attaque.

- **Alertes**

Les alertes sont généralement stockées dans les journaux du système. Cependant il existe une norme qui permet d'en formaliser le contenu, afin de permettre à différents éléments de sécurité d'interopérer. Ce format s'appelle IDMEF (pour Intrusion Detection Message Exchange Format). IDMEF est popularisé par le projet « Prélude », qui offre une infrastructure permettant aux IDS de ne pas avoir à s'occuper de l'envoi des alertes. Cela

permet aux IDS de n'avoir qu'à décrire les informations qu'il connaît et Prélude se charge de le stocker pour permettre une visualisation humaine ultérieurement.

2.HIDS (IDS machine)

Les HIDS, pour Host base d IDS, signifiant "Système de détection d'intrusion machine" sont des IDS dédiés à un matériel ou système d'exploitation. Généralement, contrairement à un NIDS, le HIDS récupère les informations qui lui sont données par le matériel ou le système d'exploitation. Il y a pour cela plusieurs approches : signatures, comportement (statistiques) ou délimitation du périmètre avec un système d'ACL(Access Control List). Un HIDS se comporte comme un daemon ou un service standard sur un système hôte qui détecte une activité suspecte en s'appuyant sur une norme. Si les activités s'éloignent de la norme, une alerte est générée. La machine peut être surveillée sur plusieurs points :

- Activité de la machine : nombre et listes de processus ainsi que d'utilisateurs, ressources consommées, ...
- Activité de l'utilisateur : horaires et durée des connexions, commandes utilisées, messages envoyés, programmes activés, dépassement du périmètre défini...
- Activité malicieuse d'un ver, virus ou cheval de Troie

Un autre type d'HIDS cherche les intrusions dans le « noyau » (kernel) du système, et les modifications qui y sont apportées. Certains appellent cette technique « analyse protocolaire ». Très rapide, elle ne nécessite pas de recherche dans une base de signature.

Le HIDS a pour avantage de n'avoir que peu de faux positifs, permettant d'avoir des alertes pertinentes. Quant à ses inconvénients il faut configurer un HIDS par poste et demande une configuration de chaque système.

3. IDS hybride

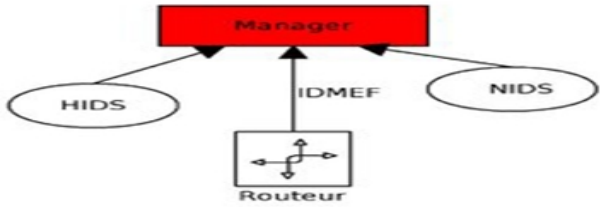


Figure I.12 : Architecture d'un IDS hybride

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF) permettant à des composants divers de communiquer et d'extraire des alertes plus pertinentes.

Les avantages des IDS hybrides sont multiples :

- Moins de faux positifs
- Meilleure corrélation
- Possibilité de réaction sur les analyseurs

➢ Liste des IDS connus :

• IDS réseau (NIDS) : Snort, Bro, Enterasys, Check Point, Tipping point, AIDA(Adaptive Intrusion Detection)

• IDS système (HIDS) : AIDE, Chkrootkit, DarkSpy, FCheck, IceSword, Integrit, Nabou, OSSEC, Osiris, Prelude LML, Rkhunter, Rootkit Unhooker, Samhain,

Tripwire.

Ces IDS servent, entre autres, à vérifier qu'un système n'a pas été compromis (par un rootkit par exemple). Ils utilisent des sommes de contrôle (MD5, SHA-1, …) des programmes exécutables pour s'assurer qu'ils n'ont pas été modifiés.

• IDS hybride : Prelude, OSSIM.

I.3.12.6. Pot de miel :

Dans le jargon de la sécurité informatique, un pot de miel, ou honeypot, est une méthode de défense active qui consiste à attirer, sur des ressources (serveur,programme, service), des adversaires déclarés ou potentiels afin de les identifier et éventuellement de les neutraliser.

Le terme désigne à l'origine des dispositifs informatiques spécialement conçus pour susciter des attaques informatiques. Son usage s'est étendu à des techniques relevant de l'ingénierie sociale et du renseignement humain.

➢ **Principes de fonctionnement**

Le but de ce leurre est de faire croire à l'intrus qu'il peut prendre le contrôle d'une véritable machine de production, ce qui va permettre à l'administrateur d'observer les moyens de compromission des attaquants, de se prémunir contre de nouvelles attaques et lui laisser ainsi plus de temps pour réagir. [6]

Une utilisation correcte d'un pot de miel repose essentiellement sur la résolution et la mise en parallèle de trois problématiques :

- la surveillance
- la collecte d'information
- l'analyse d'information.

❖ Surveillance

Il faut partir du principe que toute information circulant sur le réseau à destination ou non du pot de miel est importante. De ce fait, la surveillance doit absolument être constante et doit porter aussi bien au niveau local qu'au niveau distant. Cette surveillance de tous les instants repose sur :

- l'analyse du trafic réseau ;
- l'analyse pré compromission ;
- la journalisation des événements.

❖ Collecte d'informations

La collecte d'informations est possible grâce à des outils appelés renifleurs qui étudient les paquets présents sur le réseau et stockent les événements dans des bases de données. On peut également collecter des informations brutes grâce à des analyseurs de trames.

❖ Analyse d'informations

C'est grâce à l'analyse des informations recueillies que l'on va pouvoir découvrir les défaillances du réseau à protéger et les motivations des attaquants.

➢ Différents types de pot de miel

On compte deux types de pots de miel qui ont des buts et des fonctionnalités bien distincts :

- Les pots de miel à faible interaction ;
- Les pots de miel à forte interaction.

❖ **Pots de miel à faible interaction**

Ils sont les plus simples de la famille des pots de miel. Leur but est de recueillir un maximum d'informations tout en limitant les risques en offrant un minimum de privilèges aux attaquants.

On peut ranger, par exemple, la commande netcat dans cette catégorie. Netcat peut écouter un port particulier et enregistrer dans un journal toutes les connexions, ainsi que les commandes entrées. Ce programme permet donc d'écrire dans un fichier toutes les commandes entrées par des agresseurs. Cependant, ce type d'écoute reste très limité car il faut exécuter la commande pour chaque port que l'on souhaite observer.

Dans la même famille, on peut citer :

- Honeyd, de Niels Provost, qui est un pot de miel virtuel capable d'émuler des machines ou un réseau virtuel dans le but de leurrer les hackers. C'est l'un des pots de miel à faible interaction qui offre le plus de possibilités.
- Specter, qui permet d'émuler des services classiques (web, FTP, etc.). Il ne permet pas à l'attaquant l'accès total à un système d'exploitation, ce qui limite son intérêt.

❖ **Pots de miel à forte interaction**

Ce type de pot de miel peut être considéré comme le côté extrême du sujet puisqu'il repose sur le principe de l'accès à de véritables services sur une machine du réseau plus ou moins sécurisée.

Les risques sont beaucoup plus importants que pour les pots de miel à faible interaction. Il apparaît donc nécessaire de sécuriser au maximum l'architecture du réseau pour que l'attaquant ne puisse pas rebondir et s'en prendre à d'autres machines.
Les deux grands principes d'un tel pot de miel sont :

- le contrôle de données : pour observer le maximum d'attaques, le pot de miel à forte interaction doit accepter toutes les connexions entrantes et au contraire limiter les connexions sortantes pour éviter tout débordement. Cependant, il ne faut en aucun cas interdire toutes les connexions sortantes pour ne pas alerter l'attaquant. Un bon compromis entre sécurité et risque de découverte du leurre est donc nécessaire. [7]

- la capture des données : avec un pare-feu ou un système de détection d'intrusion (SDI).
  - le pare-feu permet de loguer et de rediriger toutes les tentatives d'attaque aussi bien internes qu'externes.
  - le SDI permet d'enregistrer tous les paquets circulant pour pouvoir reconstruire la séquence d'attaque. Il peut permettre également, grâce aux iptables, de rediriger les paquets compromis vers le pot de miel. Il vient donc en complément d'un pare-feu et sert également de sauvegarde au cas où celui-ci tomberait.
  - les informations générées seront redirigées vers une machine distante et non stockées sur la machine compromise en raison du risque de compromission de ces données. Il faut également relever l'existence de pots de miel plus spécifiques comme les pots de miel anti-spam ou anti-virus.

Les honeys pot sont des systèmes employés pour leurrer des intrus en exposant des vulnérabilités connues délibérément. Une fois qu'un intrus trouve un honey pot , il est plus probable que l'intrus s'y colle pendant un certain temps. Pendant ce temps, l'administrateur pourra enregistrer les activités de l'intrus pour découvrir ses actions et ses techniques. Une fois qu'il connaît ces techniques, il peut employer ces informations plus tard pour durcir la sécurité sur des serveurs réels de l'entreprise.

Il y a différentes manières de construire et placer des honeys pot. Le honey pot devrait avoir des services communs en fonctionnement. Ces services communs incluent le serveur telnet (port 23), le serveur HTTP (port 80), le serveur ftp (port 21) et ainsi de suite. L'administrateur devra placer le honey pot quelque part près du serveur de production de sorte que les intrus puissent facilement le prendre pour un vrai serveur. Par exemple, si les serveurs de production ont les adresses 192.168.10.21 et 192.168.10.23 du Internet Protocol (IP), l'administrateur assignera une adresse IP comme 192.168.10.22 dans le honey pot. Il peut également configurer le firewall et/ou routeur pour réorienter le trafic de quelques ports vers le honey pot où l'intrus pensera que il/elle se relie à un vrai serveur. L'administrateur devra prendre quelques précautions comme créer un mécanisme d'alerte, de sorte que quand votre honey pot est compromis, il vous l'annonce immédiatement, et aussi, de garder des fichiers de log sur une autre machine afin que l'intrus n'ait pas la capacité de supprimer ces fichiers (lorsque le honey pot est compromis). [A8] Dans le meilleur des cas, un honey pot devrait ressembler à un vrai système. L'administrateur doit créer de faux fichiers de données, comptes d'utilisateur... pour assurer que l'intrus s'y croit vraiment. Ceci donnera envie à l'intrus de

rester sur le honey pot pendant longtemps et ainsi l'administrateur pourra enregistrer plus d'activité.

I.4. Conclusion :

Tout au long de ce chapitre nous avons abordé les différents mécanismes de sécurité tels que le chiffrement, les signatures numériques et les certificats électroniques. Ces mécanismes garantissent les différents services de sécurité : confidentialité, intégrité, disponibilité, responsabilité et non répudiation. Dans le chapitre prochain on va présenter l'un des mécanismes de sécurité récent, les VPN (Virtual Private Network) ou bien en français RPV (Réseau Privé Virtuel) .

II.1 Introduction :

Nous avons présenté dans le premier Chapitre 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 [11]

L'acronyme VPN correspond à Virtual Private Network, c'est-à-dire un réseau privé virtuel, est devenu un terme courant dans l'informatique d'entreprise et le domaine des réseaux. Dans les faits, cela correspond à une liaison permanente, distante et sécurisées entre deux sites d'une organisation. Cette liaison autorise la transmission des données cryptées par le biais d'un réseau non sécurisé, tel qu'Internet. En d'autre termes, un réseau privé virtuel est l'extension d'un réseau prive qui englobe les liaisons sur des réseaux partages ou publics, tel qu'Internet. Il permet d'échanger des données entre deux entités sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

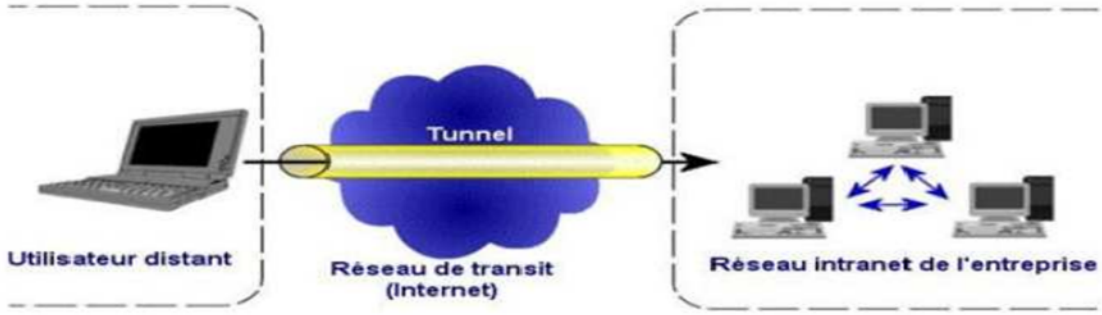
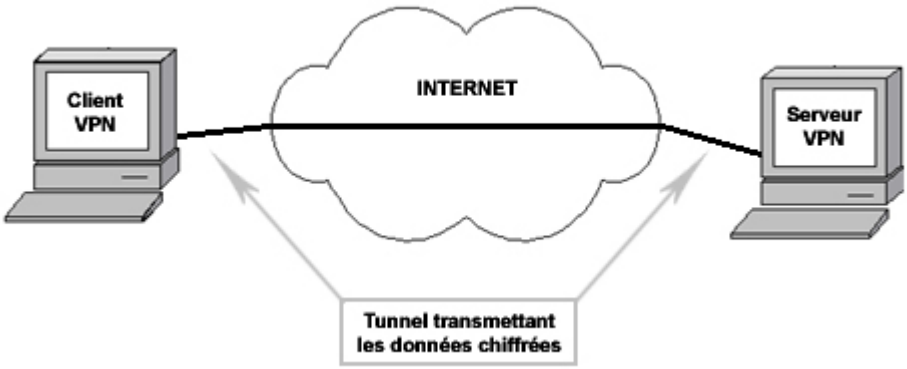


Figure II.1 : Schéma d'un accès VPN.

II.3.Fonctionnement d'un VPN :[11]

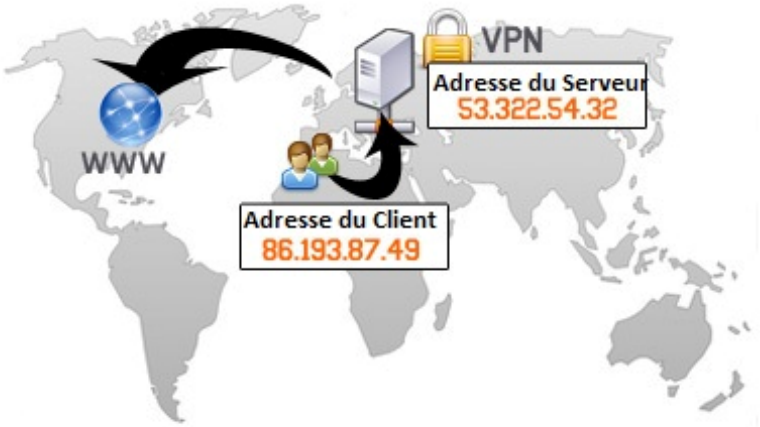
Un VPN repose sur un ou des protocoles, appelé protocoles de tunnelisation (ou tunneling). Comme énoncé dans l'introduction, ce sont des protocoles permettant aux données passant entre deux réseaux physiques d'être sécurisées par des algorithmes de chiffrage. On utilise d'ailleurs le terme de « tunnel » pour mettre l'accent sur le fait qu'entre l'entrée et la sortie d'un VPN les données sont chiffrées et protégées. Lorsqu'un VPN est établi entre deux réseaux physiques, l'élément qui permet de chiffrer et de déchiffrer les données du coté client (ou utilisateur) est

nommé « Client VPN ». On appelle « Serveur VPN » l'élément qui chiffre et qui déchiffre les données du côté de l'organisation.



Dans les faits, nous établissons une connexion sécurisée avec le serveur qui nous propose le service VPN.

Ce serveur VPN nous connecte sur Internet en masquant notre adresse IP par son adresse IP.



Une communication VPN peut donc être de client à serveur mais il est à prendre en considération qu'elle peut aussi se faire de serveur à serveur.

Il existe d'autres types d'utilisation des VPN :

- **L'intranet VPN**
- **L'extranet VPN**

II.4. Les principes avantages de VPN : [11]

Les principaux avantages d'un VPN :

- **Sécurité :** assure des communications sécurisé et chiffrées.
- **Simplicité :** utilise les circuits de télécommunication classiques.
- **Economie :** utilise internet en tant que media principal de transport, ce qui évite les couts liés à une ligne dédiée.

II.5. Les contraintes d'un VPN :

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 différents types de VPN :[11]

Il existe 3 types standards d'utilisation des Vpn. En étudiant ces schémas d'utilisation, il est possible d'isoler les fonctionnalités indispensables des Vpn :

- VPN d'accès.
- Intranet VPN.
- Extranet VPN

1. Le Vpn d'accès :

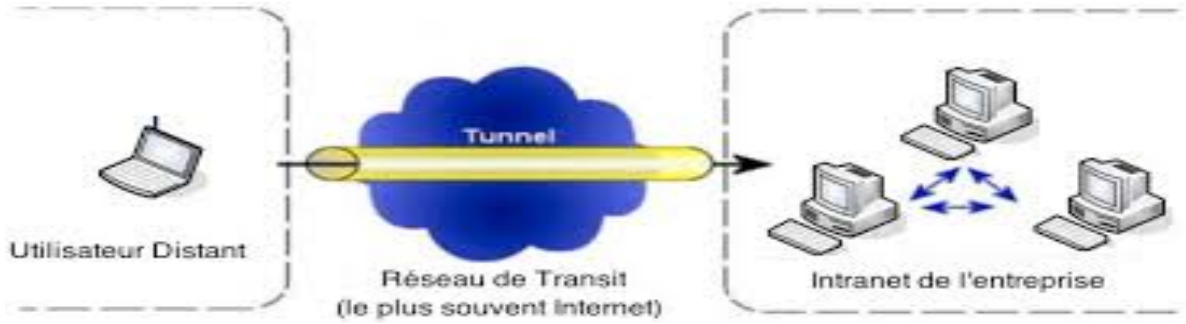


Figure II.2 : Schéma d'un accès VPN.**[4]**

Le VPN d'accès : Le Vpn d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion Vpn. Il existe deux cas:

1- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
2- L'utilisateur possède son propre logiciel client pour le Vpn auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un Nas compatible avec la solution Vpn choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.

Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Nous verrons que pour pallier Ce problème certaines entreprises mettent en place des Vpn à base de SSL, technologie implémentée dans la majorité des navigateurs Internet du marché.

Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le Vpn d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe", par un algorithme dit "Tokens sécurisés" (utilisation de mots de passe aléatoires) ou par certificats numériques.

2. L'intranet VPN :

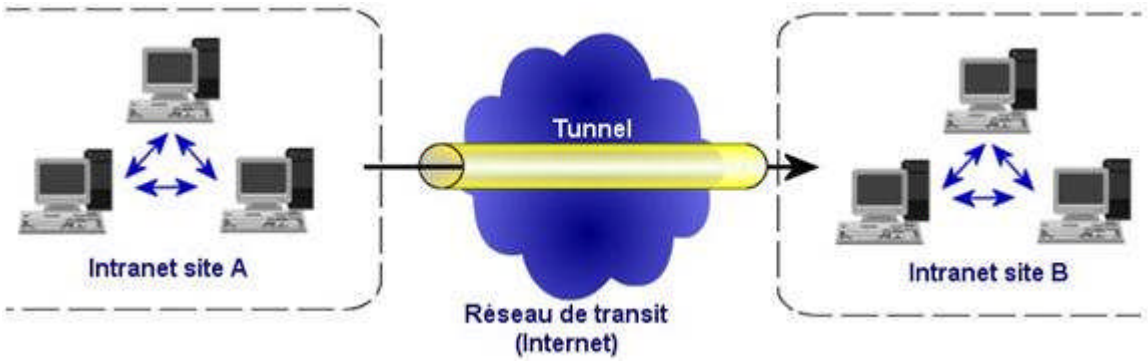


Figure II.3 : VPN connectant un utilisateur distant a un intranet privé

L'intranet VPN : L'intranet Vpn est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le Vpn (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation Ip dans Ip pour assurer une sécurité raisonnable.

3. L'extranet VPN :

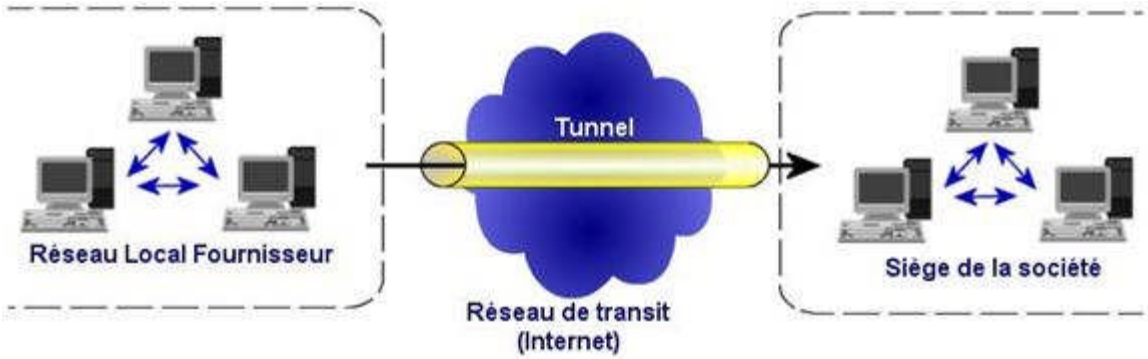


Figure II.4:VPN connectant deux sites distants par Internet.

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 cadre, il est fondamental que l'administrateur du Vpn puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

II.7. Protocoles utilisés pour réaliser une connexion Vpn :[11][14]

Il existe plusieurs protocoles dit de tunnellisation qui permettent la création des réseaux VPN :

II.7.1-PPP (Point to Point Protocol):

Ppp (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets Ip, Ipx et Netbeui dans des trames Ppp, puis transmet ces paquets encapsulés au travers de la liaison point à point. Ppp est employé généralement entre un client d'accès à distance et un serveur d'accès réseau (Nas). Le protocole Ppp est défini dans la Rfc 1661 appuyé de la Rfc 2153.

Une connexion PPP est composée principalement de trois parties :

- Un protocole pour encapsuler les datagrammes.
- Un protocole de contrôle de liaison (Lcp - Link Control Protocol) pour établir, configurer et tester la connexion de liaison de données.
- Plusieurs protocoles de contrôle de réseaux (Ncps - Network Control Protocol) pour établir et configurer les différents protocoles de couche réseau.

Les données encapsulées dans une trame PPP sont appelées paquets.ces paquets sont généralement des datagrammes.

Le format d'une trame PPP :

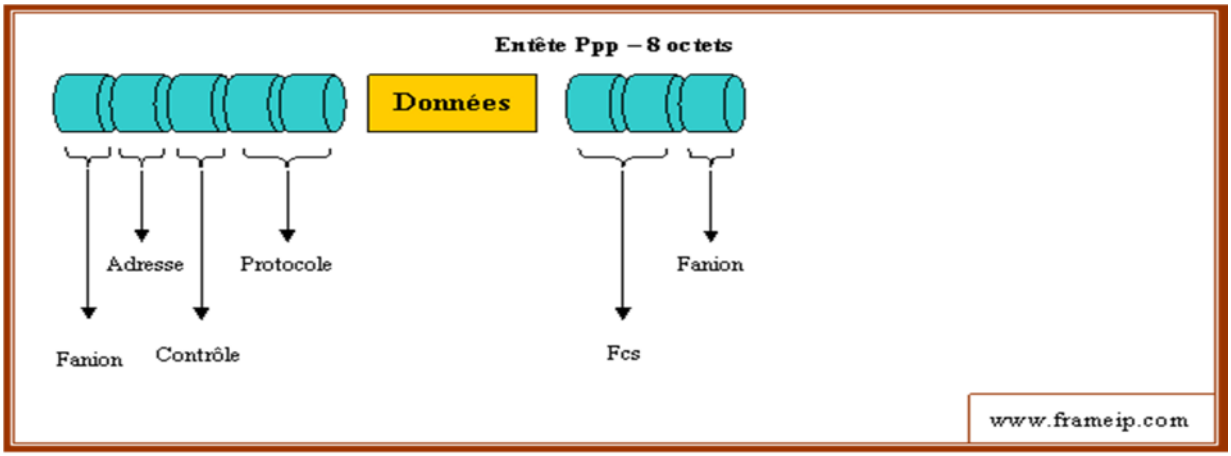


Figure II.5: la trame PPP.

- Fanion - Séparateur de trame égale à la valeur 01111110. Un seul drapeau est nécessaire entre 2 trames.
- Adresse - Ppp ne permet pas un adressage individuel des stations donc Ce champ doit être à 0xFF (toutes les stations). Toute adresse non reconnue entraînera la destruction de la trame.
- Contrôle - Le champ contrôle doit être à 0x03
- Protocole - La valeur contenue dans Ce champ doit être impaire (l'octet de poids fort étant pair). Ce champ identifie le protocole encapsulé dans le champ informations de la trame. Les différentes valeurs utilisables sont définies dans la Rfc « assign number » et représentent les différents protocoles supportés par Ppp (Osi, Ip, Decnet IV, Ipx...), les Ncp associés ainsi que les Lcp.
- Données - De longueur comprise entre 0 et 1500 octets, Ce champ contient le datagramme du protocole supérieur indiqué dans le champ "protocole". Sa longueur est détectée par le drapeau de fin de trame, moins deux octets de contrôle.
- Fcs (Frame Check Sequence) - Ce champ contient la valeur du checksum de la trame. Ppp vérifie le contenu du Fcs lorsqu'il reçoit un paquet. Le contrôle d'erreur appliqué par Ppp est conforme à X25.

Une session PPP (de l'ouverture à la fermeture) se déroule comme suit :

- ❖ L'or de la connexion, un paquet LCP est envoyé.
- ❖ Dans le cas de demande de l'authentification de la part de serveur, un paquet correspondant à un protocole d'authentification peut être envoyé (PAP, Password Authentification Protocol.
- ❖ Une fois la communication établie, PPP envoie des informations de configuration grâce au protocole NCP.
- ❖ Les datagrammes à envoyer sont transmis sous forme de paquet.
- ❖ A la déconnection un paquet LCP est envoyé pour mettre fin a la session.

Voici la liste des services pouvant être offerts par PPP :

- ✓ Permet à un serveur d'accès a distance de recevoir des appels entrants, et de garantir l'accès au réseau qui a des logiciels d'accès distant d'autres éditeurs, conformes aux normes PPP.
- ✓ Les normes PPP autorisent également des fonctions avancées qui ne sont pas disponibles avec l'ancienne norme, notamment SLIP.

II.7.2- PPTP (Point To Point Tunneling Protocol):[11]

PPTP, est un protocole qui utilise une connexion Ppp à travers un réseau Ip en créant un réseau privé virtuel (Vpn). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. Ainsi, PPTP est une solution très employée dans les produits Vpn commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP

est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression. L'authentification se fait grâce au protocole Ms-Chap de Microsoft qui, après la cryptanalyse de sa version 1, a révélé publiquement des failles importantes. Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de Ms-Chap plus sûre. La partie chiffrement des données s'effectue grâce au protocole MPPE (Microsoft Point-to-Point Encryption).

Le principe du protocole PPTP est de créer des paquets sous le protocole Ppp et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole Gre (Generic Routing Encapsulation). Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type Ppp et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets Ppp dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel Pptp. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP.

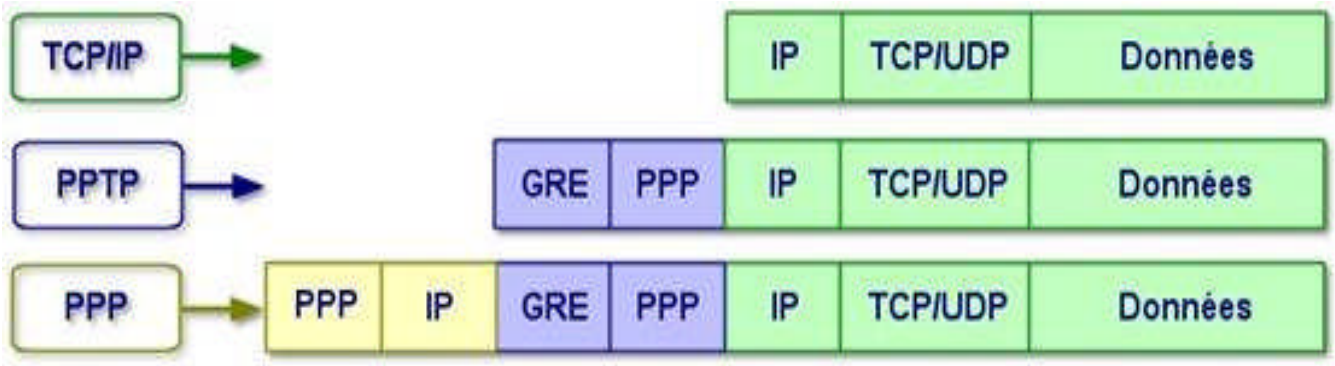


Figure II.6: La trame PPTP

Le tunnel PPTP se caractérise par :

- une initialisation du client.
- une connexion de contrôle entre le client et le serveur
- ainsi que par la clôture du tunnel par le serveur.

Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établit une connexion de type PPP et permet de faire circuler des données sur Internet.

Par la suite, une deuxième connexion est établi Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

Tout trafic client conçu pour internet emprunte la connexion physique normale, alors que le trafic

conçu pour le réseau prive distant, passe par la connexion virtuelle de PPTP.

Plusieurs protocole peuvent être associé à PPTP afin de sécuriser, et compresser les données .ainsi, pour le processus d'identification, il possible d'utiliser les protocoles PAP (Password Authentification Protocol). Pour le cryptage de données, il possible d'utiliser les fonctions de MPPE (Microsoft Point to Point Encryption).En fin, une compression de bout en bout peut être réalisée par MPPC (Microsoft Point to Point Compression).

Ces divers protocoles permettent de réaliser une connexion VPN complète. Mais les protocoles suivants permettent un niveau de performance et de fiabilité bien meilleur.

- ✓ Le protocole PPP prendre en charge plusieurs méthodes d'authentification ainsi que la compression des données et leur cryptage.
- ✓ La plus part des versions du protocole PPP permettent d'automatiser l'ensemble de la procédure d'ouverture de session.
- ✓ Le protocole PPP prend également en charge plusieurs protocoles de réseau local. Nous pouvant utiliser TCP/IP ou IPX comme protocole réseau.

PPP et le fondement de protocole PPTP et L2TP utiliser dans les connections VPN sécurisées. PPP est la principale norme de la plupart des logiciels d'accès distant.

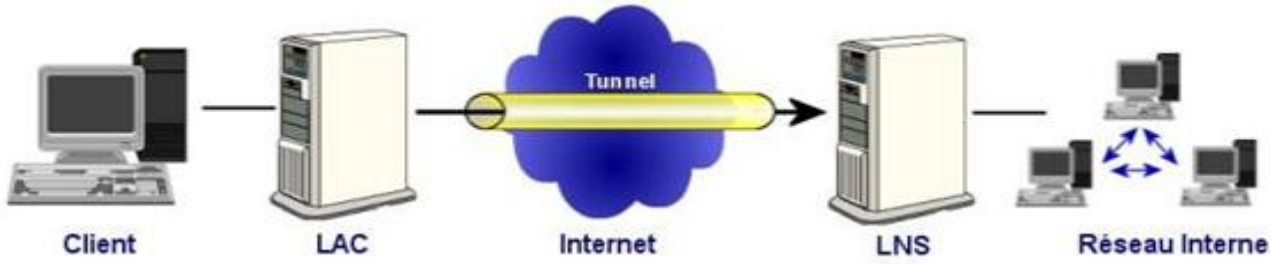
II.7.3-L2F (Layer Two Forwarding):[11]

Le protocole L2F est un protocole crée par Cisco.il est assez similaire a PPTP étant donne qu'il démarre par l'ouverture d'une connexion PPP du client vers le fournisseur d'accès internet.

Cependant, contrairement au protocole PPTP, le tunnel ici est transparent pour le client. C'est le NAS du FAI qui met en place le tunnel entre lui-même et le serveur d'accès du réseau distant : c'est le monde forcé, par opposition au mode volontaire utilise par PPTP. Cela entraine une perte de la maitrise de la sécurité vu que les données seront visibles par le FAI.L2F est adapté aux intranet VPN.

II.7.4-L2TP (Layer Two Tunneling Protocol):[11]

L2tp, est issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco Systems, Microsoft, Ascend, 3Com ainsi que d'autres acteurs clés du marché des réseaux. Il permet l'encapsulation des paquets Ppp au niveau des couches 2 (Frame Relay et Atm) et 3 (Ip). Lorsqu'il est configuré pour transporter les données sur IP, L2tp peut être utilisé pour faire du tunnelling sur Internet. L2tp repose sur deux concepts : les concentrateurs d'accès L2tp (Lac : L2tp Access Concentrator) et les serveurs réseau L2tp (Lns : L2tp Network Server). L2tp n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'Ipsec et L2tp.



II.7.4.1- Concentrateurs d'accès L2tp (Lac : L2tp Access Concentrator) :

Les périphériques Lac fournissent un support physique aux connexions L2tp. Le trafic étant alors transféré sur les serveurs réseau L2tp. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté Rtc ou alors à un système d'extrémité Ppp prenant en charge le protocole L2tp. Ils assurent le fractionnement en canaux de tous les protocoles basés sur Ppp. Le Lac est l'émetteur des appels entrants et le destinataire des appels sortants.

II.7.4.2-Serveur réseau L2tp (Lns : L2tp Network Server) :

Les serveurs réseau L2tp ou Lns peuvent fonctionner sur toute plate-forme prenant en charge la terminaison Ppp. Le Lns gère le protocole L2tp côté serveur. Le protocole L2tp n'utilise qu'un seul support, sur lequel arrivent les canaux L2tp. C'est pourquoi, les serveurs réseau Lns, ne peuvent avoir qu'une seule interface de réseau local (Lan) ou étendu (Wan). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface Ppp du concentrateur d'accès Lac : async. Rnis, Ppp sur Atm ou Ppp sur relais de trame. Le Lns est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le Lns qui sera responsable de l'authentification du tunnel.

II.7.5- IPSEC (Internet Protocol Security):[12]

IP sec, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme Ipsec pour Ip Security Protocols. Ipsec est basé sur deux mécanismes. Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par Ce "protocole" ne sont pas encodées. Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole Ike permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans Ipsec.

IPSec (Internet Protocol Security) est probablement le protocole VPN le plus utilise

aujourd'hui. Il fait son apparition en1995.
IPSec est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure

- La confidentialité (grâce au cryptage),
- l'authentification (qui permet d'être certain de l'identité de l'émetteur)
- l'intégrité des données (s'assurer que personne n'a pu avoir accès aux informations).
- La protection des données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP.
- Sécurisation de transport des données lors des échanges internes et externes, la stratégie IPSec permet à l'administrateur réseau d'assurer une sécurité efficace pour son entreprise contre toute attaque venant de l'extérieur.

IPSec peut fonctionner selon deux mode, selon ce que en veut l'on faire : mode tunnel et mode transport. On pourra également faire une combinaison de ces deux mode, on parlera alors de mode nesting (il s'agit en fait d'encapsuler IPSec dans de l'IPSec).

II.7.5.1- Services offerts par IPSec : [12]

Le protocole IPSec est destiné à fournir différents services de sécurité. Voici la liste des services pouvant être offerts par IPSec. Quelque soit le mode utilisé ces services seront disponible:

- **Authentification des extrémités :** chaque extrémité du tunnel va s'identifier avant d'entamer la communication des données. Cela permet de s'assurer que l'on dialogue avec la personne convenue.de plus, pour chaque paquet échangé, IPSec permettra de s'assurer qu'il a été émis par la bonne machine (authenticité des donnés).
- **Confidentialité des données :** évite que quelqu'un qui intercepterait les donnes ne puise les interpréter. On utilisera pour cela des techniques de cryptographie.
- **Intégrité des données :** IPSec permet de s'assurer qu'un paquet n'a subit aucune modification durant son trajet.
- **Protection contre le rejeu :** permet de détecter une tentative d'attaque consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau.

Ces différentes caractéristiques permettent à l'hôte A de crypter ses données et de les envoyer vers l'hôte B via le réseau, puis à l'hôte B de les recevoir et de les décoder afin de les lire sans que personne ne puisse altérer ou récupérer ces données.

II.7.5.2- les sous –protocoles d'IPSec :[12]

II.7.5.2.1- le protocole AH (Authentification header) :

Le protocole AH est conçu pour assurer l'intégrité en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données (pas de confidentialité).

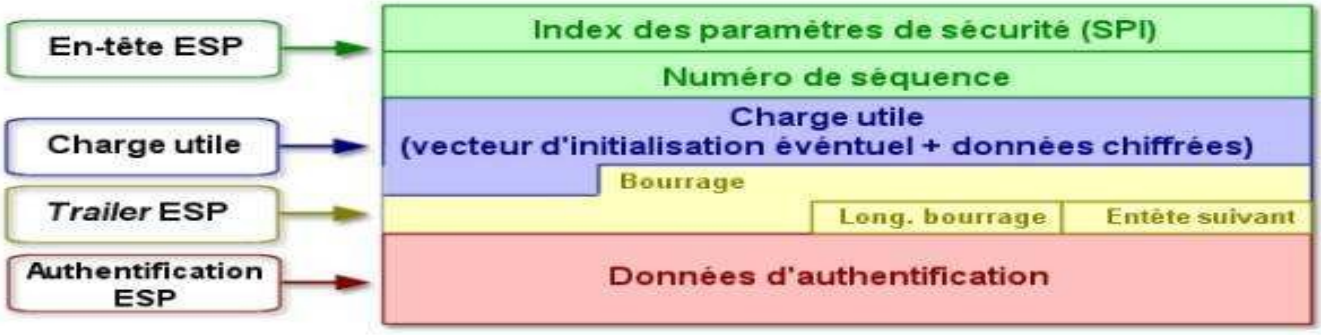
Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé « valeur de vérification d'intégrité ». La protection contre le rejeu se fait grâce à un numéro de séquence.

II.7.5.2.2-Le Protocole ESP (Encapsulaing Security Payload) :[12]

Le protocole ESP peut assurer, au choix, un ou plusieurs des services suivants :

- Confidentialité (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel).
- Intégrité des données en mode non connecté.
- Authentification de l'origine des données.
- Protection partielle contre le rejeu.

La confidentialité peut être sélectionnée indépendamment des autres services, mais son utilisation sans intégrité/authentification (directement dans ESP ou avec AH) rend le trafic vulnérable à certains types d'attaques actives qui pourraient affaiblir le service de confidentialité



Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets.
Les données d'authentification ne sont présentes que si Ce service a été sélectionné.
Voyons maintenant comment est appliquée la confidentialité dans Esp.

L'expéditeur :

- ✓ Encapsule, dans le champ "charge utile" d'ESP, les données transportées par le datagramme original et éventuellement l'en-tête IP (mode tunnel).
- ✓ Ajoute si nécessaire un bourrage.

- ✓ Chiffre le résultat (données, bourrage, champs longueur et en-tête suivant).
- ✓ Ajoute éventuellement des données de synchronisation cryptographiques (vecteur d'initialisation) au début du champ "charge utile".

II.7.5.3. IPSec en mode tunnel et transport :[12]

II.7.5.3.1.Mode transport

Le mode transport prend un flux de niveau transport et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans ce mode, l'insertion de la couche IPSec est transparente entre TCP et IP. TCP envoie ses données vers IPSec comme il les enverrait vers IPv4.

On peut utiliser AH si la confidentialité des données n'est pas essentielle ou si elle est assurée par une autre couche, ou ESP si on veut s'assurer de la confidentialité des données. En mode transport, les données sont prises au niveau de la couche 4 du modèle OSI (couche transport). Elles sont cryptées et signées avant d'être transmises à la couche IP.

II.7.5.3.2.Mode tunnel

Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPSec. L'encapsulation IPSec en mode tunnel permet le masquage d'adresses.

Ainsi, si on utilise AH, on signera l'intégralité du paquet IP encapsulé pour s'assurer de son intégrité et de son authenticité. Avec ESP, le paquet sera en plus entièrement crypté, permettant de s'assurer de la confidentialité des données, et de se protéger partiellement contre l'analyse du trafic en cryptant les adresses IP source et destination.

Le schéma ci-dessous permet de se faire une idée plus claire des différences entre les deux modes :

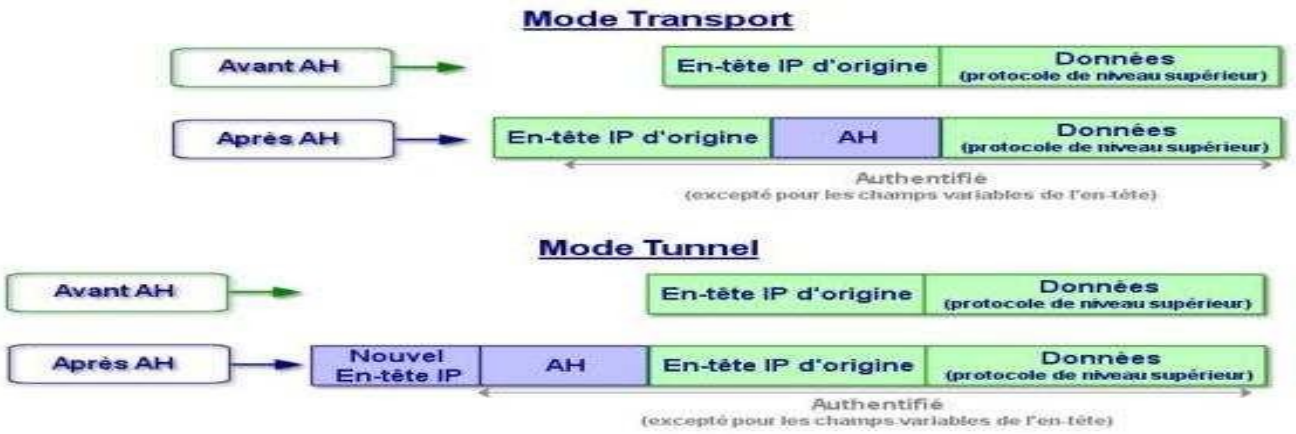


Figure II.7 : la différence entre le mode tunnel et transport.

La différence entre ces deux modes :

- Dans le mode transport, l'en-tête extérieur est produite par la couche IP c'est-à-dire sans masquage d'adresse, alors que dans le mode tunnel l'encapsulation IPSec permet le masquage d'adresses.
- Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

II.7.5.4. Algorithmes utilisés par ipsec: [4]

Les algorithmes utilisés par IP sec sont :

II .6.9.1. 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 actuel.

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 8,16,24,32,40,48,56et64 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 64bits.
2. On diversifie aussi la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés K1,...,K16 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 :

- $G_i=D_{i-1}$.
- $D_{i-1}=G_{i-1}$ 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 depermutations.
- Phase 4 : Permutation finale:

1. On applique à $G_{16}D_{16}$ l'inverse de la permutationinitiale.
2. $Z=P^{-1}(G_{16}D_{16})$ est le bloc de 64 bits chiffré à partir dex.

Cet algorithme peut etre représenté par le shéma ci-après

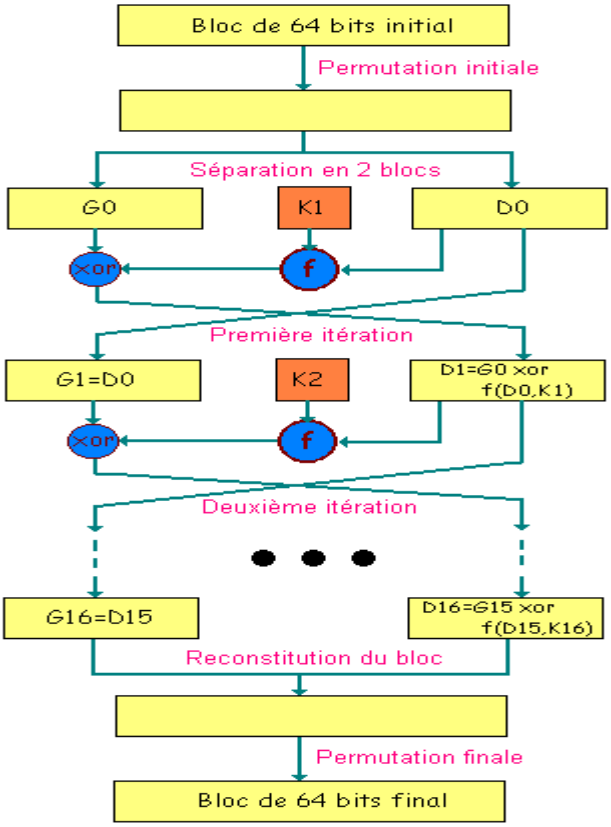


Figure II.8: Schéma de l'algorithme DES

- ***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*56 = 112 bits) ou 3 clés différentes (d'où une longueur de clé de 3*56=168 bits). Les deux schémas suivants illustrent les deux implémentations possibles de l'algorithme triple- DES :

Figure II.9: Schéma de l'algorithme Triple – DES – 112 bits

Figure II.10: 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 256bits.

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 .6 .2.Les algorithmes asymétriques

- ***L'algorithme RSA:***

Le premier crypto-système asymétrique, RSA crié 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 $D=C^d \pmod n$. D'après un théorème du mathématicien Euler, $D=M^{de}=M \pmod n$. Il a donc reconstitué le message initial.

- **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.

II.7.6-le protocole SSH

Le protocole SSH (Secure Shell) et utilisé pour établir un accès sécurisé permettant d'effectuer des opérations sensible sur des machines distantes suivant une architecture client /serveur. Il se compose d'un client qui sera invoqué sur la machine initiatrice de la communication et d'un serveur qui doit tourner sur la machine destinataire. Il va créer une communication sécurisé, en authentifiant les deux parties et en garantissant le secret de la communication et son intégrité.

Le principale objectif de SSH était de résoudre le problème de transmission en clair de toutes les informations sur le réseau (LAN ou Internet) ouvrant la porte a tout les attaque de type homme du milieu(Man-In-The-Middle).

SSH est classiquement utilisé pour une fois la communication sécurisée établie, exécuter un interpréteur de commandes, un Shell, mais il est possible de faire passer a travers un canal sécurisé n'importe quel trafic TCP(X11, SMTP, etc..), ce qui offre une grande flexibilité. On appelle ce lacrée un tunnel SHH.

II.7.7- Le protocol SSL :[13]

Récemment arrive dans le monde des VPN, les VPN SSL présentent en effet un gros avantage de ne pas nécessiter du coté client plus qu'un navigateur internet classique. En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur internet et implémenté en standard dans les navigateurs modernes.

SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal un canal de communication sécurisé avec une autre application.

SSL a deux grandes fonctionnalités :

- L'authentification du serveur et du client a l'établissement de la connexion.
- Le chiffrement des données durant la connexion.

II.7.7.1. Fonctionnement

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par vérification de la validité du certificat du serveur. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client. Le client vérifie aussi à date de validité du certificat et peut également consulter une CRL (Certificat Revocation

List). Si toutes les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Le serveur peut alors envoyer un test au client, que le client doit signer avec sa clé privée correspondant à son propre certificat. Ce ci est fait de façon a ce que le serveur puisse de nombreux paramètres sont échangés durant cette phase : type de clé, valeur de la clé, algorithme de chiffrage

La phase suivante consiste à l'échange de données cryptées (protocole SSL records). Les clés générer avec le protocole handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangé

Les différentes phases du protocole SSL sont :

- Segmentation des paquets en paquets de taille fixe.
- Compression.
- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message,…
- Chiffrement des paquets et du résultat du hachage a l'aide de la clé symétrique générée lors du handshake.
- Ajout d'un en-tête SSL au paquet.

II.7.8 La gestion des clefs pour Ipsec : Isakmp et Ik

Les protocoles sécurisés présentés dans les paragraphes précédents ont recours à des algorithmes cryptographiques et ont donc besoin de clefs. Un des problèmes fondamentaux d'utilisation de la cryptographie est la gestion de ces clefs. Le terme "gestion" recouvre la génération, la distribution, le stockage et la suppression des clefs.

IKE (Internet Key Exchange) est un système développé spécifiquement pour Ipsec qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet. Il est composé de plusieurs éléments : le cadre générique Isakmp et une partie des protocoles Oakley et Skeme. Lorsqu'il est utilisé pour Ipsec, IKE est de plus complété par un "domaine d'interprétation" pour Ipsec.

II.7.8.1-Isakmp (Internet Security Association and Key Management Protocol):

Isakmp a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs (et plus généralement des associations de sécurité). Il comporte trois aspects principaux :

- Il définit une façon de procéder, en deux étapes appelées phase 1 et phase 2 : dans la première, un certain nombre de paramètres de sécurité propres à Isakmp sont mis en place, afin d'établir entre les deux tiers un canal protégé ; dans un second temps, Ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et Esp par exemple).

- Il définit des formats de messages, par l'intermédiaire de blocs ayant chacun un rôle précis et permettant de former des messages clairs.
- Il présente un certain nombre d'échanges types, composés de tels messages, qui permettant des négociations présentant des propriétés différentes : protection ou non de l'identité, perfect forward secrecy...

II.7.8 .2 - Ike (Internet Key Exchange):

IKE utilise Isakmp pour construire un protocole pratique. Il comprend quatre modes :

- Le mode principal (Main mode)
- Le mode agressif (Aggressive Mode)
- Le mode rapide (Quick Mode)
- Le mode nouveau groupe (New Groupe Mode)

Main Mode et Aggressive Mode sont utilisés durant la phase 1, Quick Mode est un échange de phase 2. New Group Mode est un peu à part : Ce n'est ni un échange de phase 1, ni un échange de phase 2, mais il ne peut avoir lieu qu'une fois qu'une SA Isakmp est établie ; il sert à se mettre d'accord sur un nouveau groupe pour de futurs échanges Diffie-Hellman.

II.7.9- comparaison des différents protocoles :

Chaque protocole présenté permet de réaliser des solutions performantes de VPN. Nous allons ici aborder les points forts et les points faibles de chacun de ses protocoles.

II.7.9.1- VPN-SSL :

Présentée comme la solution miracle pour permettre aux itinérants de se connecter aux applications réparties de l'entreprise, les VPN-SSL souffrent de problèmes principalement liés aux navigateurs web utilisés. Le but d'utiliser des navigateurs web est de permettre aux utilisateurs d'utiliser un outil dont ils ont l'habitude, et qui ne nécessite pas de configuration supplémentaire. Cependant lorsqu'un certificat expire l'utilisateur doit aller manuellement le renouveler.

Cette opération peut poser un problème aux utilisateurs novices .De plus sur la majorité des navigateurs web la consultation des listes de certificats révoqués n'est pas activée par défaut : toute la sécurité de SSL reposant sur ces certificats ceci pose un grave problème de sécurité. Rien n'empêche de plus le client de télécharger une version modifiée de son navigateur pour pouvoir utiliser de nouvelles fonctionnalités. Rien ne certifie que le navigateur n'a pas été modifié et que son autorité de certification en soit bien une.

Enfin Un autre problème lié à l'utilisation de navigateurs web comme base au VPN est leur spécificité au monde web. En effet par défaut un navigateur n'interceptera que des communications HTTPS ou éventuellement FTPS. Toutes les communications venant d'autre type

d'applications (Microsoft Outlook, ou une base de données par exemple) ne sont pas supportées. Ce problème est généralement contourné par l'exécution d'une application dédiée dans le navigateur.

Mais ceci implique également la maintenance de cette application (s'assurer que le client possède la bonne version, qu'il peut la télécharger au besoin).

II.7.9.2- PPTP:

PPTP présente l'avantage d'être complètement intégré dans les environnements Windows. Ceci signifie en particulier que l'accès au réseau local distant pourra se faire via le système d'authentification de Windows NT : RADIUS et sa gestion de droits et de groupe. Cependant comme pour beaucoup de produits Microsoft, la sécurité est le point faible:

- ✓ Mauvaise gestion des mots de passe dans les environnements mixtes Windows 95/NT;
- ✓ Faiblesses dans la génération des clés de session : réalisé à partir d'un hachage du mot de passe au lieu d'être entièrement générées au hasard. (facilite les attaques « force brute »).
- ✓ Identification des paquets non implémentée : vulnérabilité aux attaques de type « Spoofing».

II.7.9.3- L2TP/IPSec:

Les mécanismes de sécurité mis en place dans IPSec sont plus robustes et plus reconnus que ceux mis en place par Microsoft dans PPTP. Par défaut le protocole L2TP utilise le protocole IPSec. Cependant si le serveur distant ne le supporte pas L2TP pourra utiliser un autre protocole de sécurité. Il convient donc de s'assurer que l'ensemble des équipements d'un VPN L2TP implémente bien le protocole IPSec. IPSec ne permet d'identifier que des machines et non pas des utilisateurs. Ceci est particulièrement problématique pour les utilisateurs itinérants. Il faut donc prévoir un service d'authentification des utilisateurs. Dans le cas de connexion dial-up c'est de connexion qui sera utilisé pour authentifier l'utilisateur. Mais dans le cas d'une connexion via internet il faudra prévoir une phase d'authentification supplémentaire à l'établissement du tunnel. D'autre part IPSec n'offre aucun mécanisme de QOS ce qui limite ses applications. Toutes les applications de voix sur IP ou de vidéo sur IP sont impossibles ou seront amenées a être complètement dépendantes des conditions de trafic sur l'internet public.

Enfin IPSec à cause de la lourdeur des opérations de cryptage/décryptage réduit les performances globales des réseaux. L'achat de périphériques dédiés, coûteux est souvent indispensable.

II.8. 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 quatrième chapitre nous allons présenter l'implémentation d'une solution VPN en utilisant le Protocol ipsec

Introduction :

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

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

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

FIGURE III.1. ENIEM

III.1. Présentation de l'ENIEM :

III.1.1 Historique :

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

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

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

L'ENIEM est la première entreprise de Maghreb à être certifiée ISO 9002 depuis le premier juillet 1998 par les experts de l'association française de l'assurance de la qualité (AFAQ), puis gratifiée en 2003 de l'ISO 9001 <<version 2000>>. A noter que les produits ENIEM sont 0% CFC (Chlora Fluora Carbones), et ce depuis 1997.

Le champ d'activité de l'entreprise ENIEM consiste à la production, le développement, la recherche dans le domaine de l'électroménager, ainsi que la prise en charge de la fonction commerciale, la promotion des exportations et de service après-vente. Actuellement, l'entreprise ENIEM est constituée de :

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

III.1.2 Situation géographique de l'ENIEM :

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

III.1.3 Missions :

Dans le cadre de développement économique et social, l'ENIEM assure les fonctions suivantes :

La production, le montage, la commercialisation et la recherche dans les différentes branches de l'électroménager notamment :

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

Elle assure également la production :

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

III.1.4. Objectifs :

Parmi les principaux objectifs de l'ENIEM nous citons :

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

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

III.1.5.Organisation :

L'ENIEM se présente comme suit :

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

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

Organigramme général de l'ENIEM

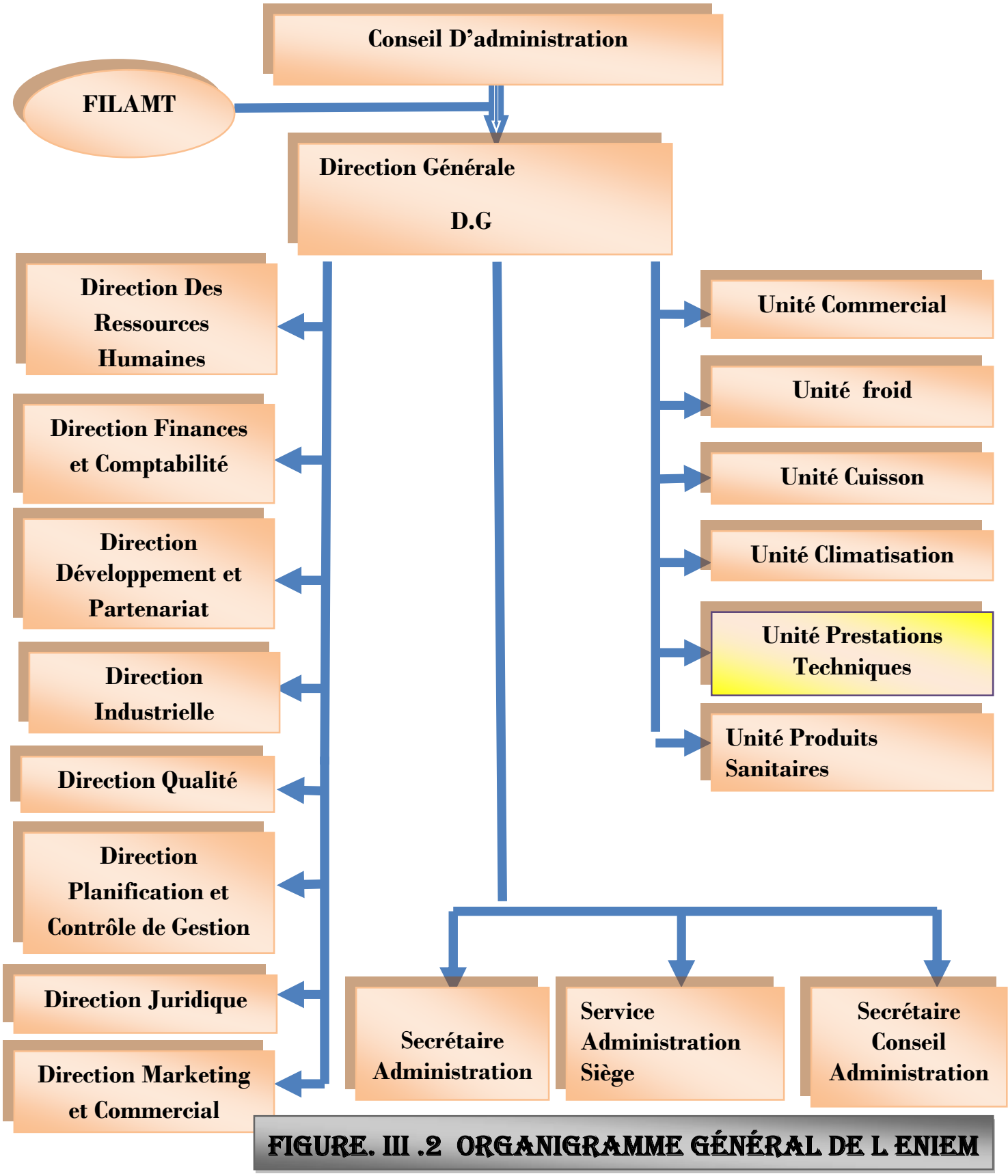


FIGURE. III .2 ORGANIGRAMME GÉNÉRAL DE L ENIEM

Domaine d'étude

III.2. Mode d'organisation :

III.2.1. Les directions :

1. Direction générale :

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

2. Direction des ressources humaines :

En cohérence avec la politique qualité de l'entreprise, la fonction Ressources humaines accroit la mobilisation et la valorisation du personnel qui assure des services client.
Elle pilote le recrutement, l'accueil, l'information et gère le plan de carrière du personnel. Elle conçoit le plan de formation à partir du recueil des besoins collectifs et individuels et s'assure de son exécution.

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

Elle doit en outre :

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

3. Direction des finances et comptabilité :

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

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

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

4. Direction développement et partenariat :

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

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

5. Direction industrielle :

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

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

6. Direction qualité :

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

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

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

7. Direction planification et contrôle de gestion :

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

Cependant elle :

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

8 .Direction juridique :

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

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

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

9. Direction de marketing et de la communication :

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

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

III.2.2. Les unités :

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

1. Unité FILAMP (filiale) :

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

2. Unité commercial (UC) :

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

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

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

3. Unité Cuisson (U CUIS) :

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

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

Ainsi qu'un labo essais gazinières.

4. Unité climatisation (U CL) :

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

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

Composée essentiellement de quatre (04) ateliers de fabrication :

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

5. Unité produits sanitaires :

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

6. Unité froid(UF) : elle est composée de 3 lignes de production:

a. Une ligne de fabrication de réfrigérateur petit modèle :

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

b. Une ligne de réfrigérateurs grands modèles :

Les capacités installées sont de 390.000 réfrigérateurs par année dont les modèles 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.

7. Unité de prestations techniques (UPT) :

Principalement de gérer et d'exploiter les moyens communs (production d'énergie et utilités) utilisés dans le processus de production des autres unités, ainsi que de la gestion des totalités des infrastructures communes (bâtiments, voirie, éclairage…).

Cette unité assure également, les pièces mécaniques nécessaires à l'entretien des équipements de production, la conception et la fabrication de nouveaux moyens (moules, outils, gabarits…). Constituée d'ateliers de mécanique et de deux (02) stations :

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

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

III.3. présentation du domaine d'Etude :

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

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

Champs d'études

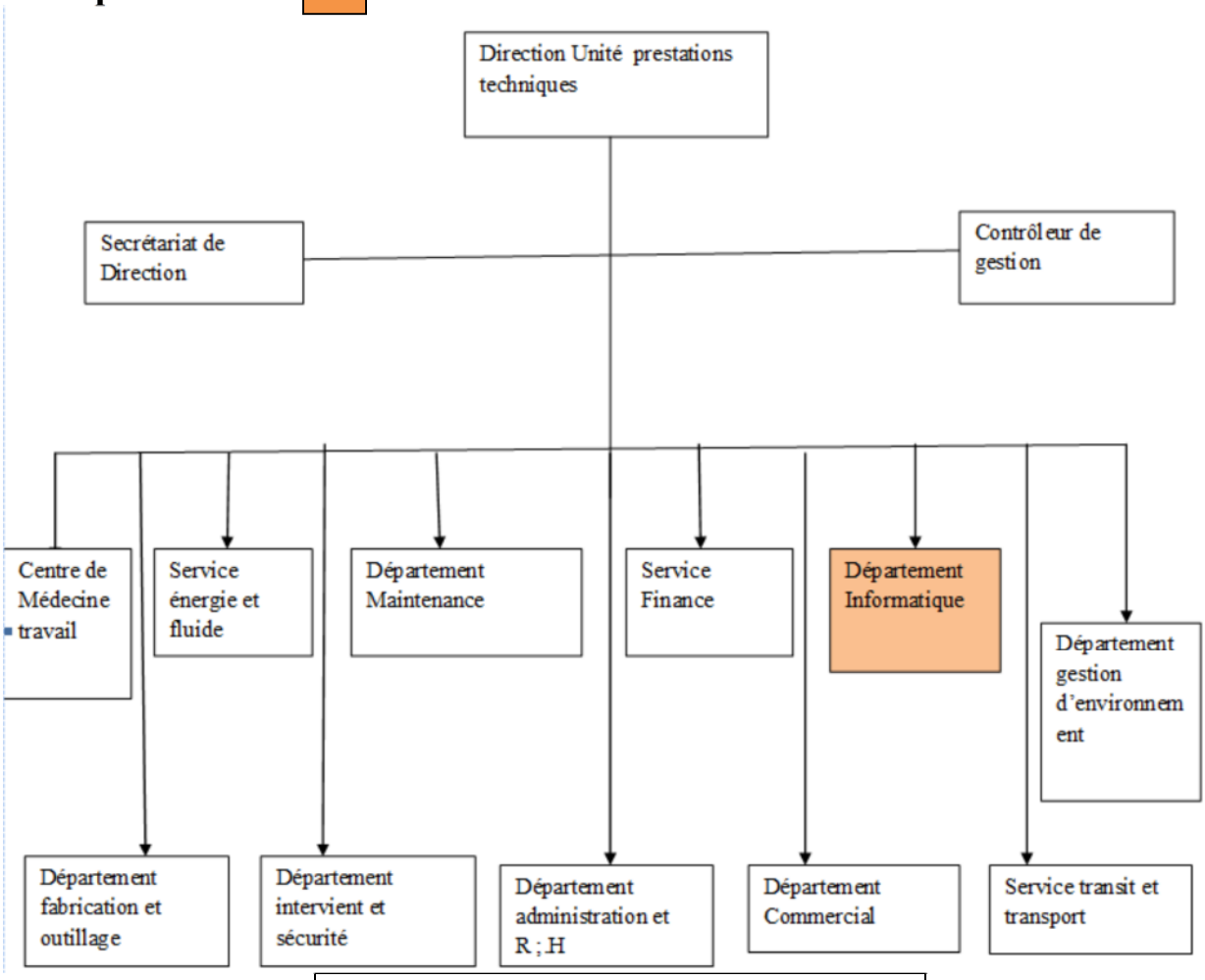


Figure III.3: Unité de Prestation Technique

III.4. Le Réseau informatique de l'entreprise l'ENIEM :

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

III.4.1.Un Réseau client/serveur :

Ce réseau est composé de 39 terminaux dont 27 écrans HP (modèle 700/92 A, 2392A) et 12 imprimantes HP (modèle 2563B, 2934A, 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).

III.4.2. 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.

III.4.3.Les armoires de brassage existantes :

• L'armoire de d'étage centrale

Elle est constituée des éléments suivants :

- 02 panneaux de brassage à 16 ports : contiennent des connecteurs RJ45 (câble torsadé).
- 01 Switch d'étage Cisco : contient des ports RJ45 et des ports GBIC (pour câble fibre optique).
- 01 onduleur : pour avoir le temps à sauvegarder les données.
- 01 Switch fédérateur : contient 7 ports GBIC.
- 03 tiroirs optiques : qui relient les armoires des blocs.
- 01 Panneau électrique à 06 prises sous onduleur : pour alimenter les périphériques actifs.

la figure III.4 présente l'armoire d'étage centrale

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 d'étage centrale

III.4.4.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.

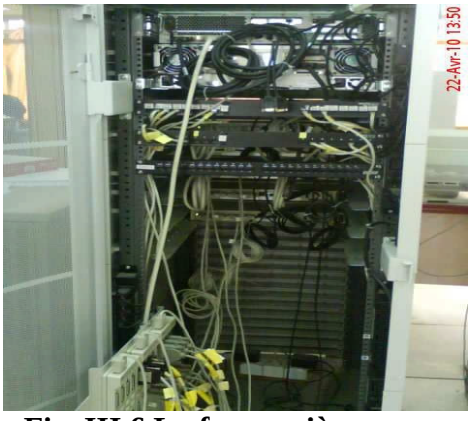


Fig. III.6 La face arrière

• **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

III.4.5. Caractéristiques matériels et logicielles

désignation	caractéristique
4PC hp Compaq	-system windows XP service pack 1 original -CPU Intel pentuim4 2,4G Hz -RAM DDR1 512Mo -disque dur 40Go
7PC hp Compaq	-system windows XP service pack 1 original -CPU Intel pentuim4 2,4G Hz -RAM DDR1 1Go - disque dur 80Go
1PC hp Compaq (serveur proxy)	-DDR RAM 1Go -CPU Intel pentuim4 2,4G Hz -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 (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 III.1 : des Caractéristiques matérielles et logicielles

III.4.5.l'aspect logiciel :

Les différents logiciels utilisés :

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

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

III.5.1 Organigramme de département informatique :

Le département informatique se compose de deux services :

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

III.5.2 Aspect humain :

III.5.2.1 Chef de département :

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

III.5.2.2 Chef de service exploitation :

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

- **Agent maintenance et réseau informatique :**

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

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

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

III.5.2.3 Chef de service développement système informatique :

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

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

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

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

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

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

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

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

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

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

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

III.6. Conclusion :

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

INTRODUCTION :

Ce chapitre est la dernière partie de notre travail, donc nous allons nous intéresser à la mise en œuvre de notre application en établissant une interconnexion entre deux sites distants utilisant un VPN.

Durant ce chapitre nous allons donner :

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

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 et 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 serveur 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 y a 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 a 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 appartienne à l'armoire d'étage où se trouve le SWITCH fédérateur auquel sont relié les six autres Switchs par la fibre optique.

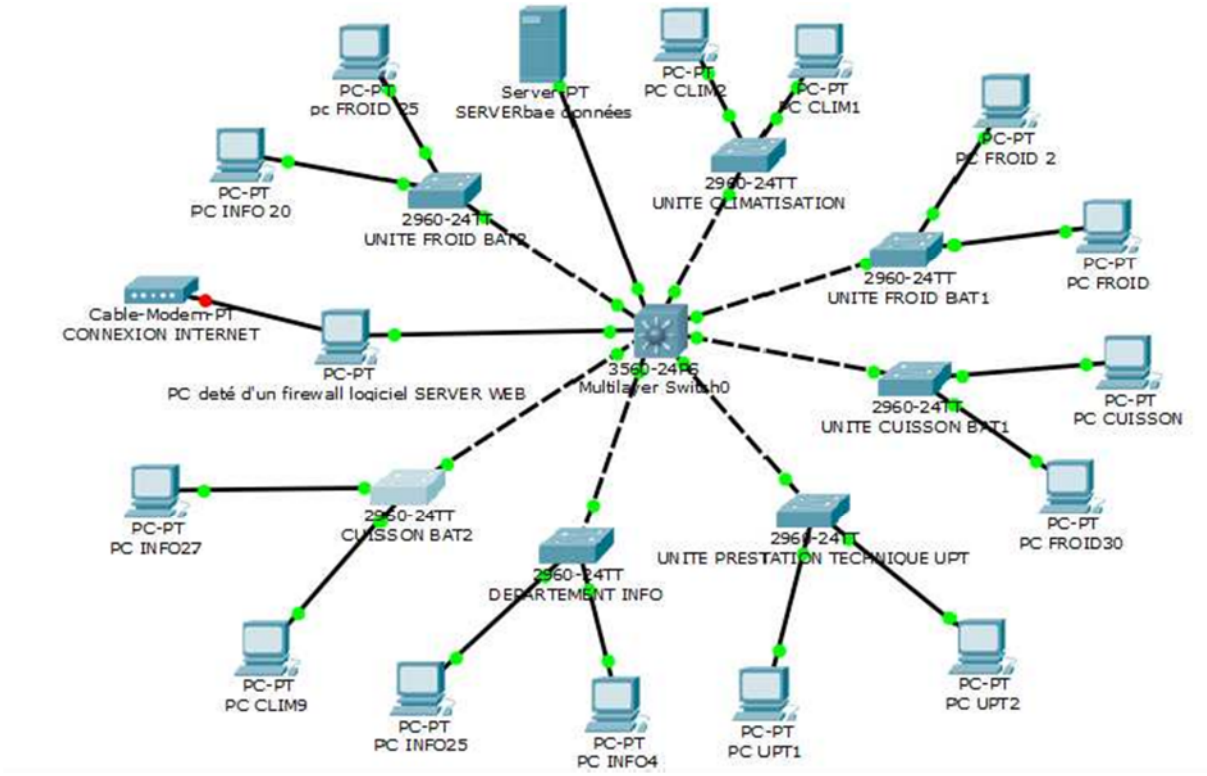


Figure IV.1 : présentation du réseau existant

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 connecter 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 limité à l'utilisation d'un seul VLAN par défaut (natif) et que la configuration des switchs 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 a leurs déférents 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 a l'unité froid mais comme les ports de ce dernier sont tous utilisés donc il est reliés a l'un des ports libres qui se trouvent dans le switch de l'unité cuisson.

I.4.Les critiques du réseau existant:

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

- **Critique1** : les switchs du réseau sont configurables mais non configurés.
  Tout les switch sont considérés comme des switchs simples.

- **Critique 2** : le réseau est installé anarchiquement et non administré.
  Des fonctions de différentes unités se trouvent sur le même switch et non administrés.

- **Critique3** : le réseau installé est non sécurisé contre les intrusions d'une façon fiable.
  La sécurité du réseau existant est basée uniquement sur l'utilisation d'un firewall logiciel.

- **Critique4** : manque d'une interconnexion entre l'entreprise ENIEM (Oued aissi) et sa direction générale (Tizi-Ouzou).

I.5. Solutions proposées:

Quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité, il reste difficile, voire, impossible, d'assurer la sécurité 100 pour cent.

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

Dans cette solution nous essaierons de minimiser au maximum les risques d'attaques et les points vulnérables de l'entreprise en accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

Donc A l'issu d'une étude préalable de l'unité prestation technique au sien 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.

II. Réalisation

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

- **Emulateur GNS3 (Graphical NetworkSimulator):**

GNS3 (Graphical Network Simulateur). Un logiciel open source qui est a la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel.

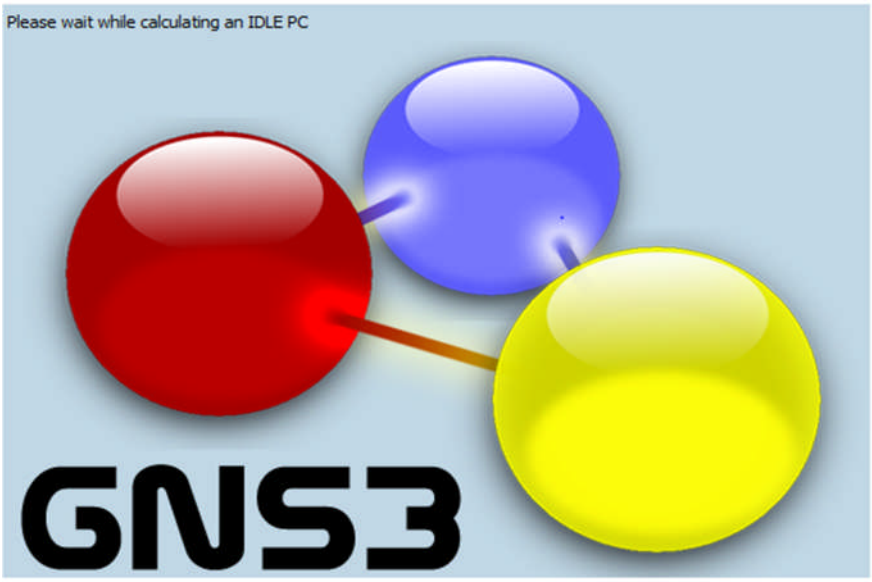


Figure IV.2 :GNS3 8.4.1

- **La VMware Workstation 9 :**

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

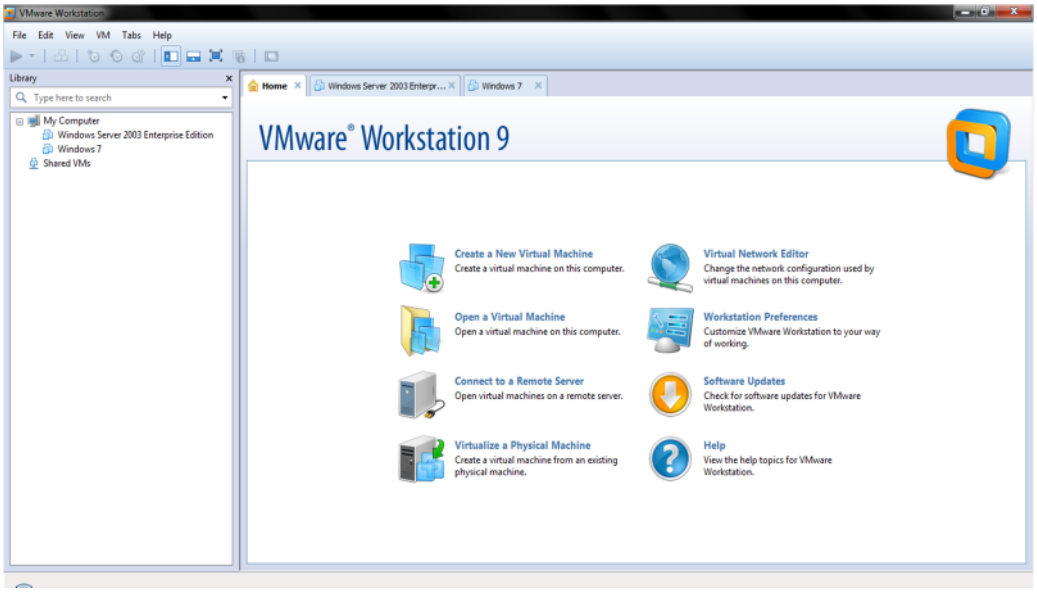


Figure IV.3 : VMware Workstation 9

- **Microsoft Windows Server 2003 :**

Microsoft Windows Server 2003 est conçu pour fournir aux entreprises la plate-forme la plus productive pour virtualiser les charges de travail en utilisant la virtualisation intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web.

Figure IV.4 : Windows server 2003

- **Wireshark :**

Est un logiciel d'analyse réseau (sniffer) qui permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP, puis regroupés en blocs d'informations et analysés par le logiciel.

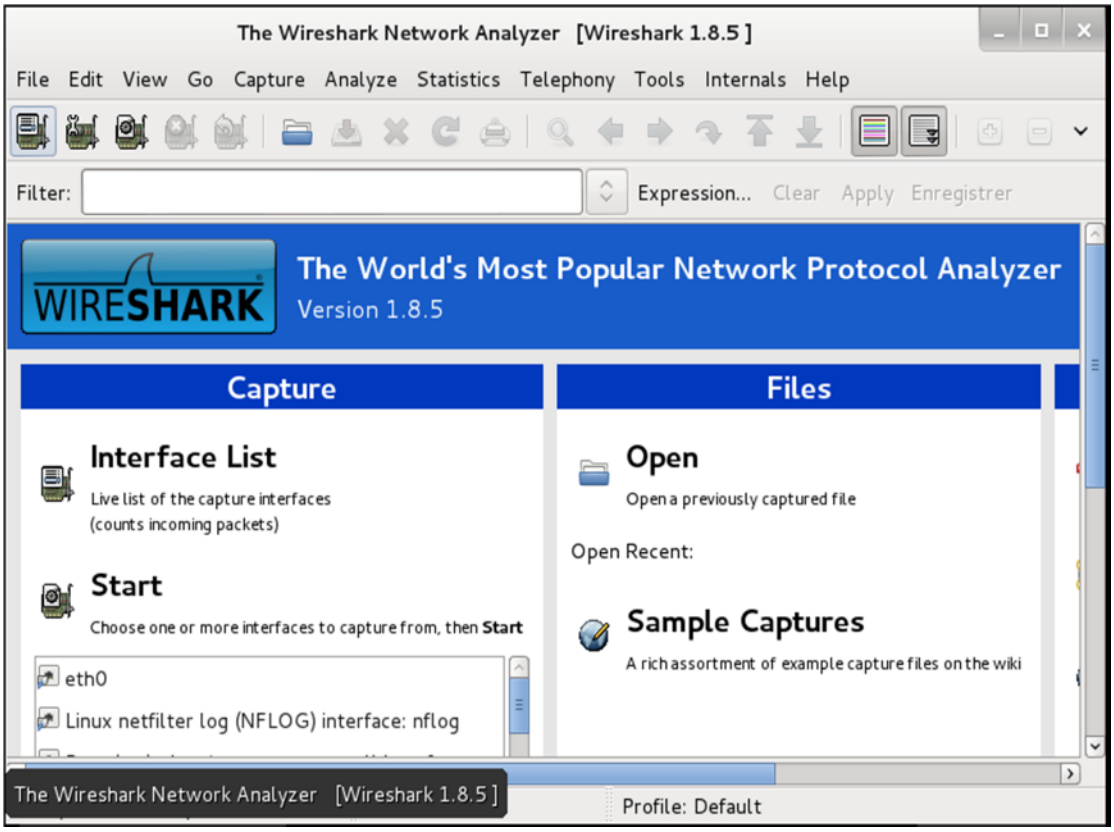


Figure IV.4 : Wireshark

- **Routeurs CISCO** avec 3600 avec IOS Advenced-Securité.
- PC hp620 à **4G de RAM**

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

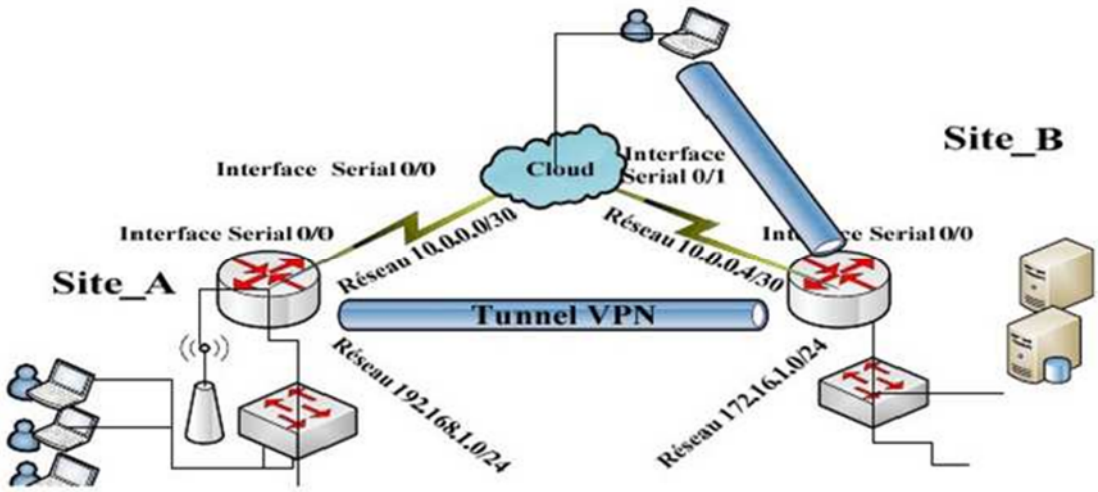


Figure IV.5: Topologie du réseau

II.3.Configuration de VPN site to site:

II.3.1.Etablissement d'un tunnel IP sec 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)

II.4. Table d'adressage

Équipements	Interface	Adresse ip	Masque sous réseaux	Passerelle p 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	192.168.1.254	255.255.255.0	N /A	1
R3	loopback 0	1.1.1.3	255.255.255.255	N /A	0
	f0/0	200.2.2.2	255.255.255.0	N /A	0
	f0/1	192.168.3.254	255.255.255.0	N /A	2

TAB. IV.1 : Table d'adressage

D’où on aura la topologie suivante :

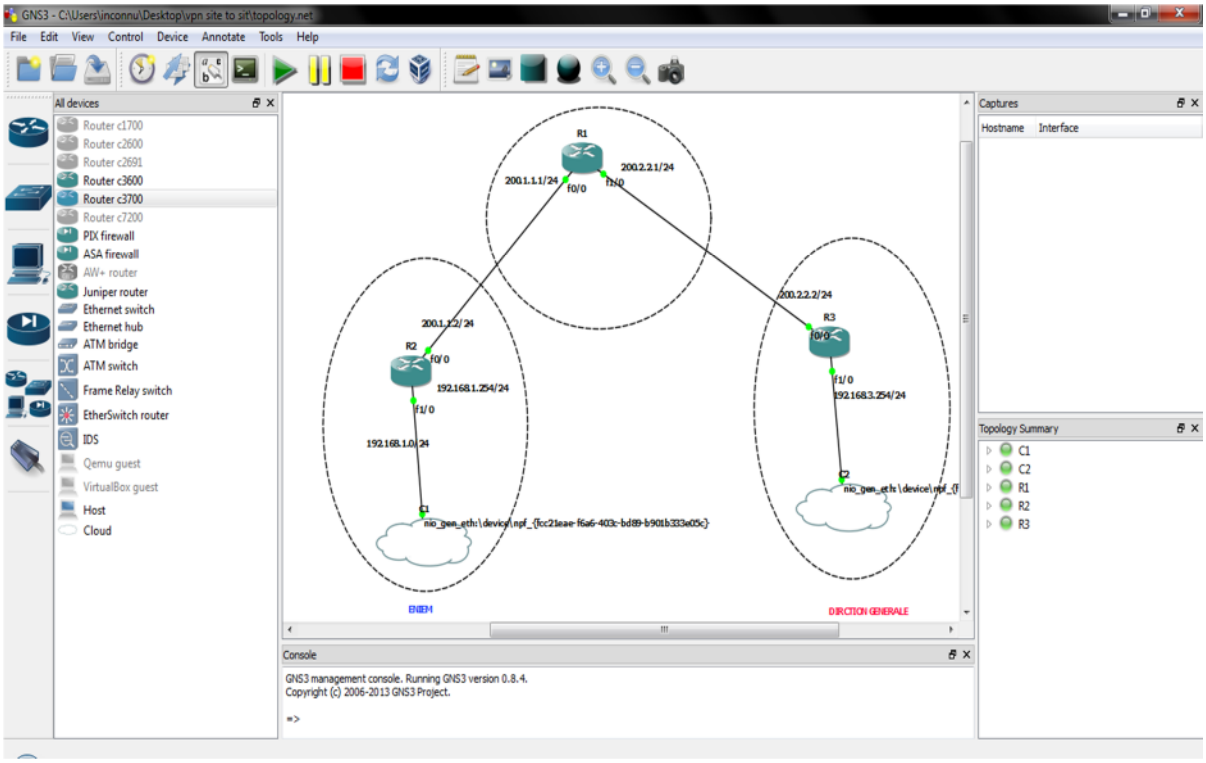


Figure IV.6 : Architecture du réseau.

II. 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.

II.5.1. Test de connexion et de routage :

Résultat de la commande « show ip route »

- R2 :

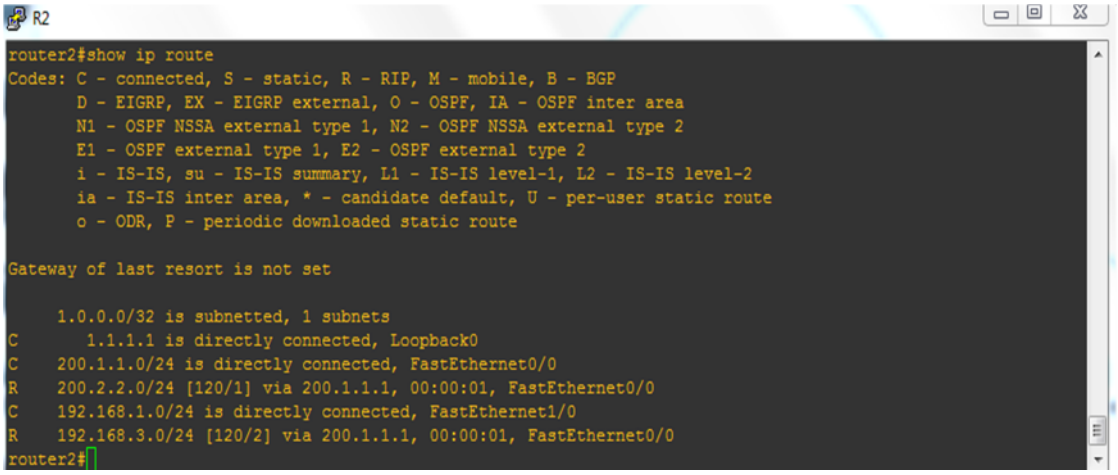


Figure IV.7: résultat de la commande « show ip route » sur R2

- R3 :

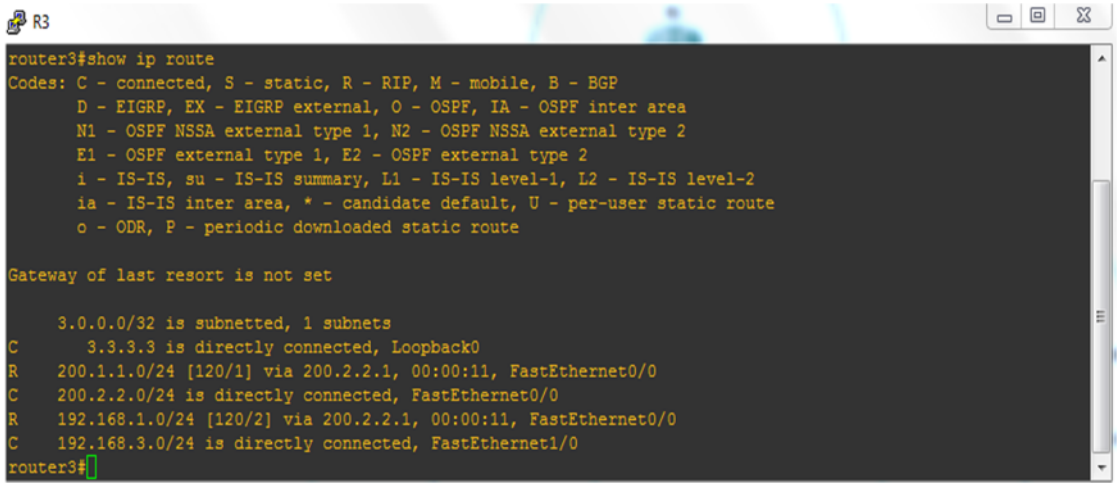


Figure IV.8 : résultat e la commande « show ip route» sur R3

- R1 :

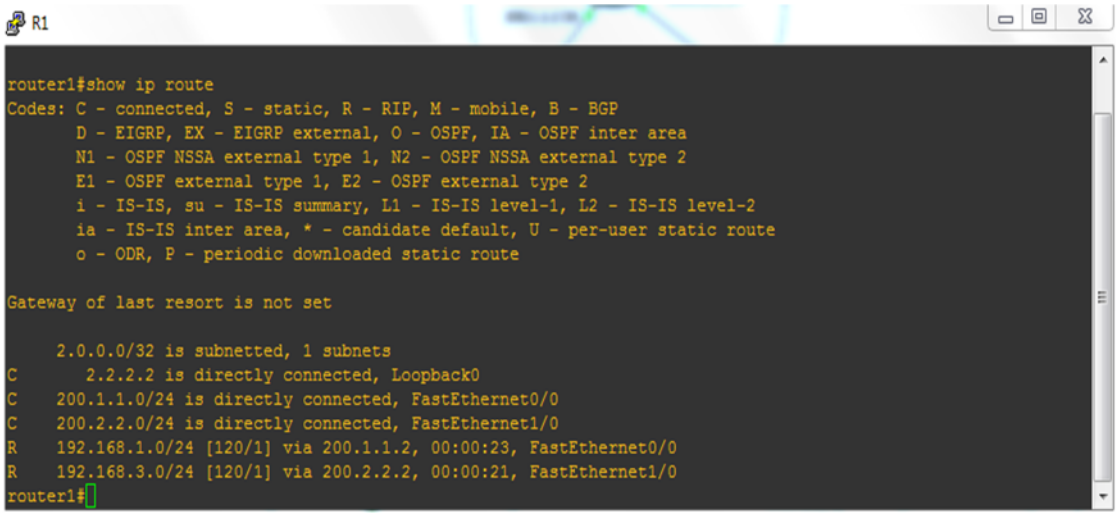


Figure IV.9 : résultat de la commande « show ip route » sur R1

II.6.Configuration de VPN site to site:

II.6.1. Etablissement d'un tunnel IP sec 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) :

Nous avons 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)

On 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

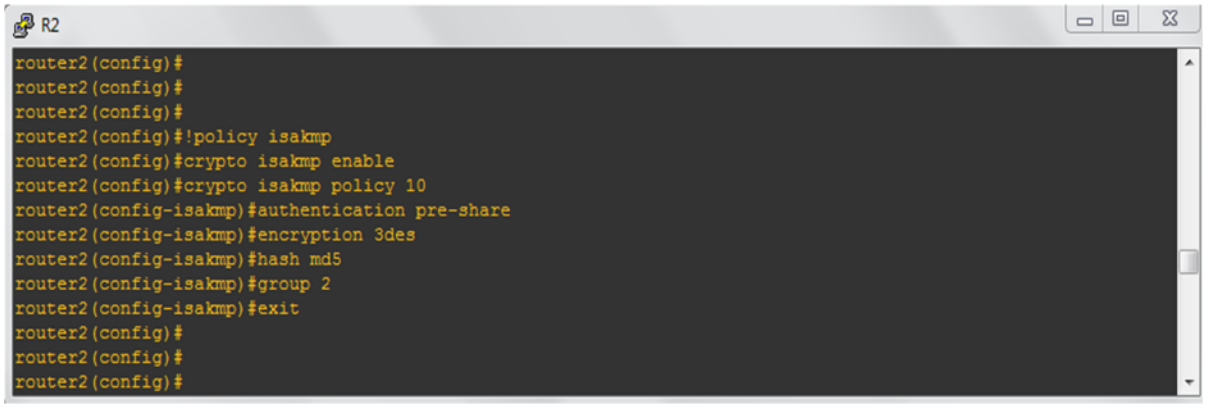


Figure IV. 10 : Configuration Policy ISAKMP pour le site distant

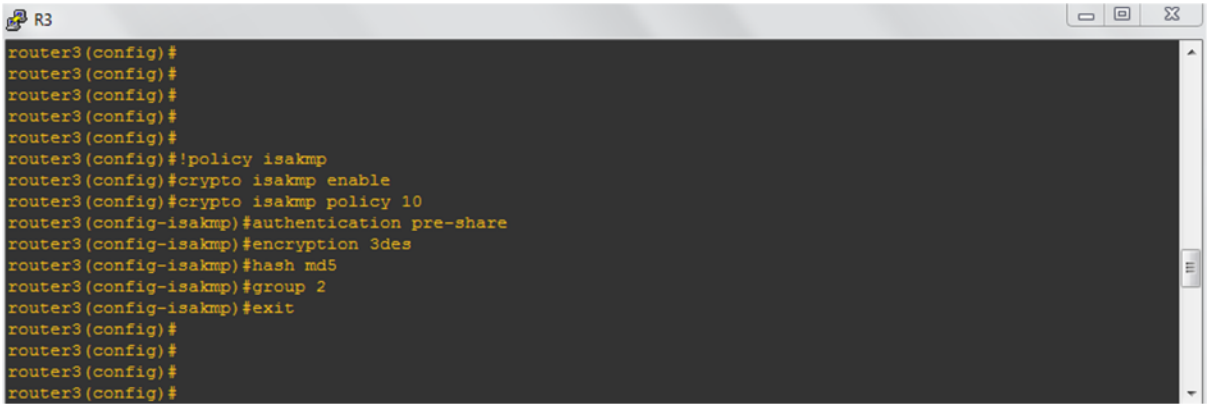


Figure IV.11.Configuration Policy ISAKMP pour la direction générale

- **Etape 2 : Configuration des paramètres IP sec :**

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 VPN.

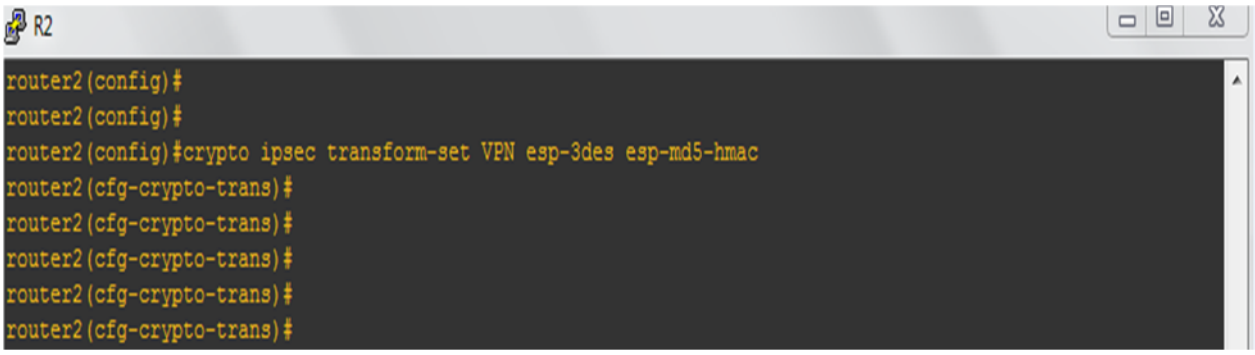


Figure IV.12. Configuration des paramètres du tunnel ipsec pour le site distant 'R2'

Figure IV.13. Configuration des paramètres du tunnel ipsec pour le site centrale '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 (Activer Isakmp)**

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

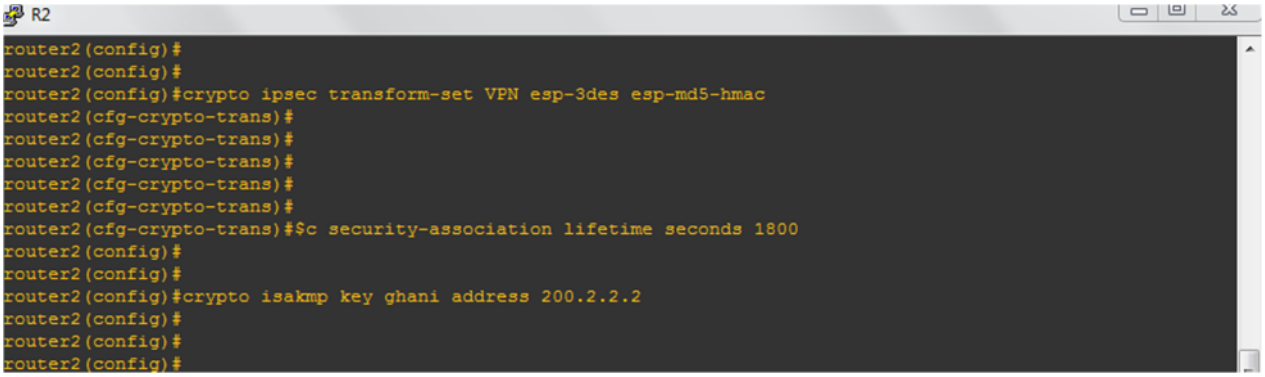


Figure IV.14. Configuration du tunnel ipsec pour le site distant

Figure IV.15: Configuration du tunnel ipsec pour le site centrale

Voilà on a ensuite la clé pré-partagée, ici « ghani » qu'on associe avec l'adresse de l'autre bout du

tunnel donc 200.1.1.2

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

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

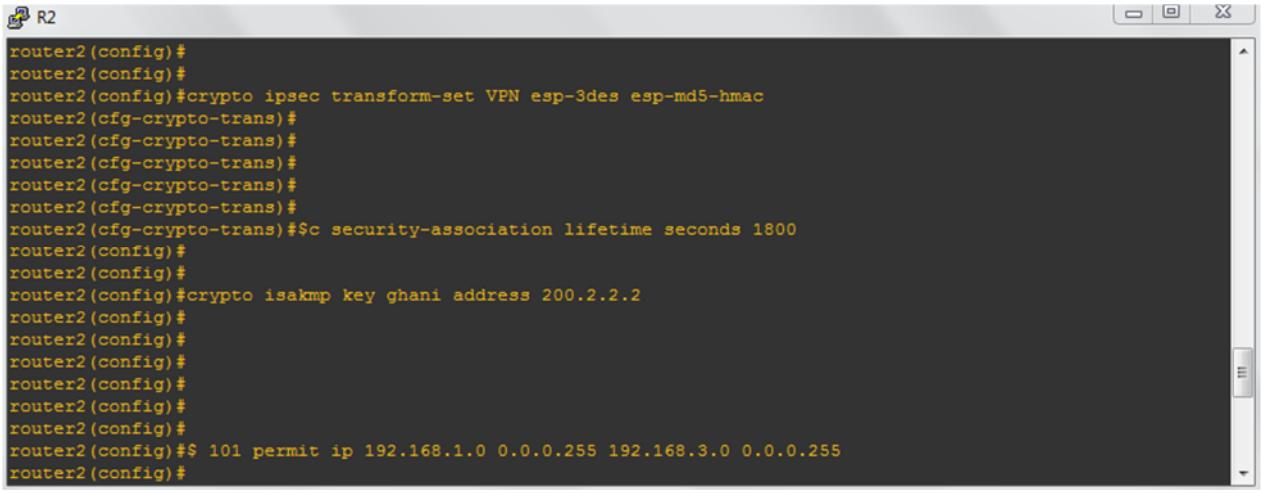


Figure III.16. Configuration des listes de contrôle pour le site distant

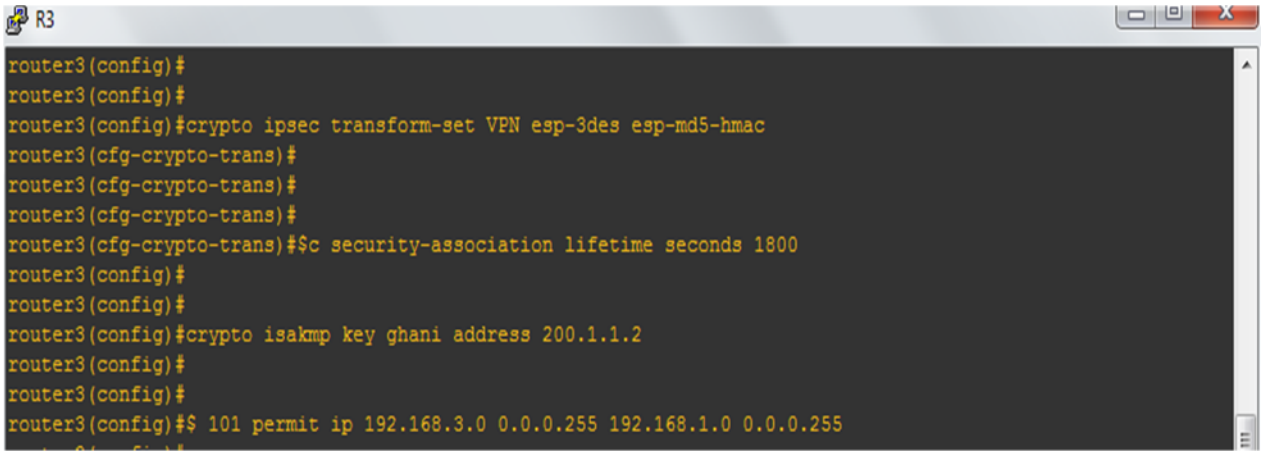


Figure III.17. Configuration des listes de contrôle pour le site centrale

- **Etape 5 : Définir la crypto map**

Création d'une crypto map pour regrouper les paramètres précédant

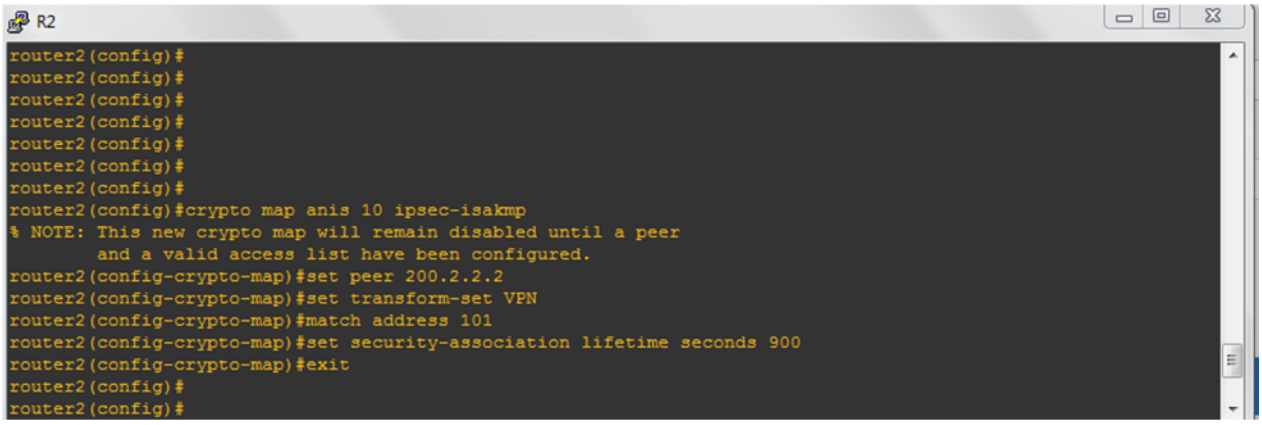


Figure IV.18 : Configuration de la crypto map pour le site distant

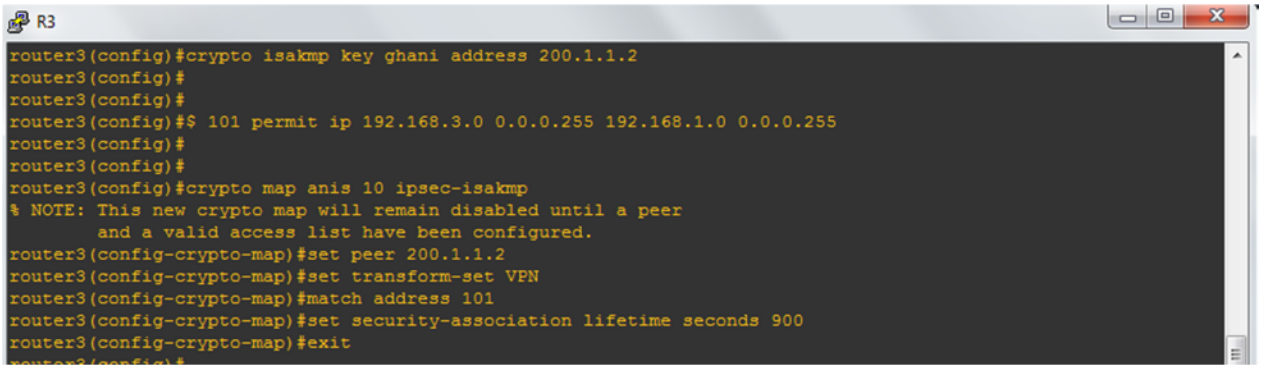


Figure IV.19 : Configuration de la crypto map pour le site centrale

On a donc créé ici une Crypto-map nommée « anis » 10 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'access-list VPN
- Destination du tunnel 200.1.1.2
- Cryptage selon le transform-set anis

- **Etape 6 : Appliquer la Crypto map à l'interface out side**

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

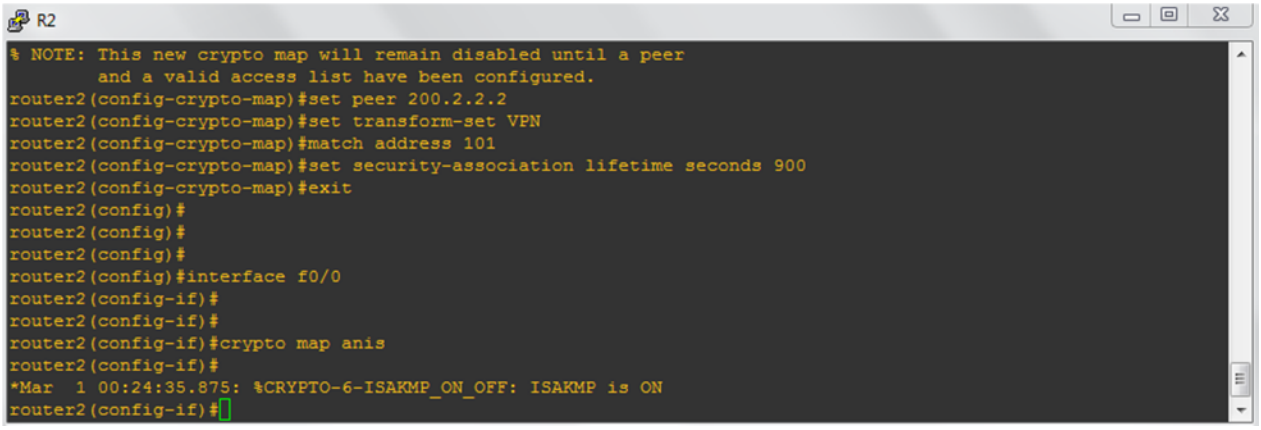


Figure IV.20. Application de la crypto map à l'interface pour le site distant

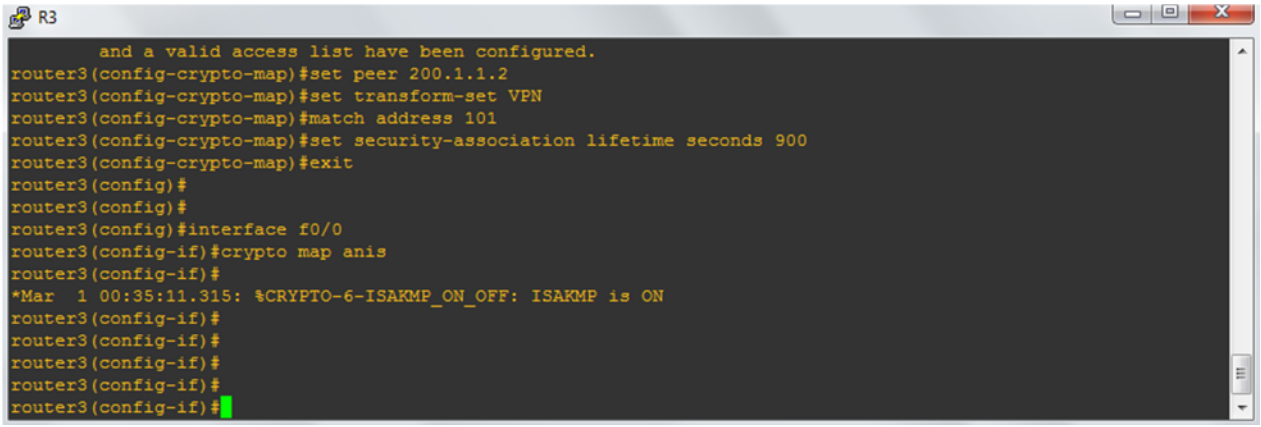


Figure IV .21. Application de la crypto map à l'interface pour le site centrale

- **Générer le trafic intéressant :**

A partir d'une machine (192.168.1.3) qui se trouve dans le site distant a Oued-Aissi, faire Ping sur l'adresse IP de serveur (192.168.3.3) qui se trouve dans la direction générale a Tizi-Ouzou.

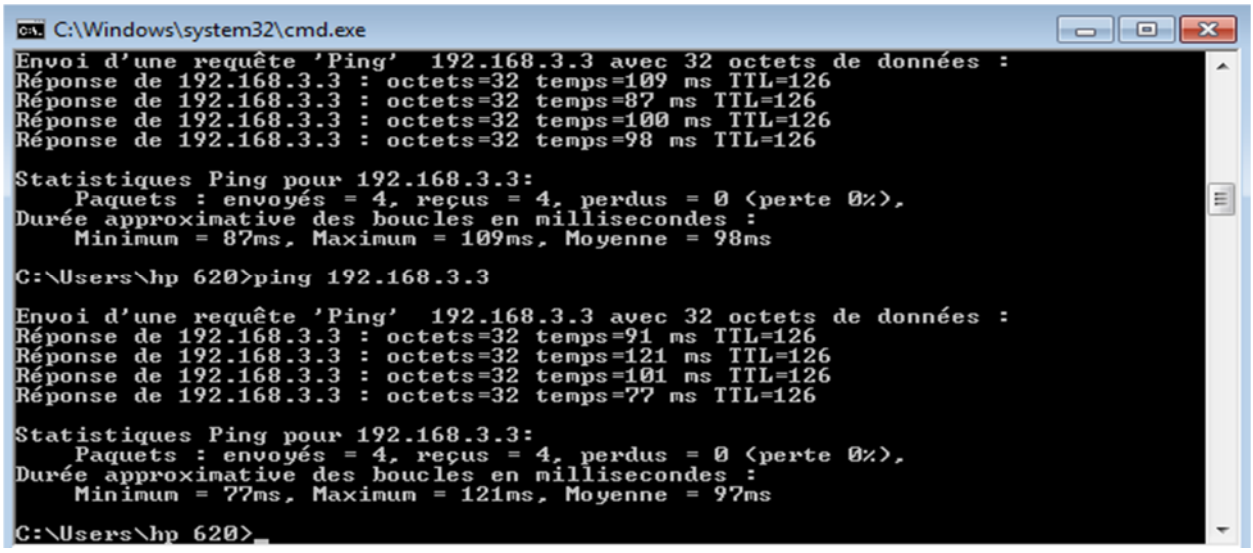


Figure IV.22.Résultat du : Ping 192.168.3.3

II.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

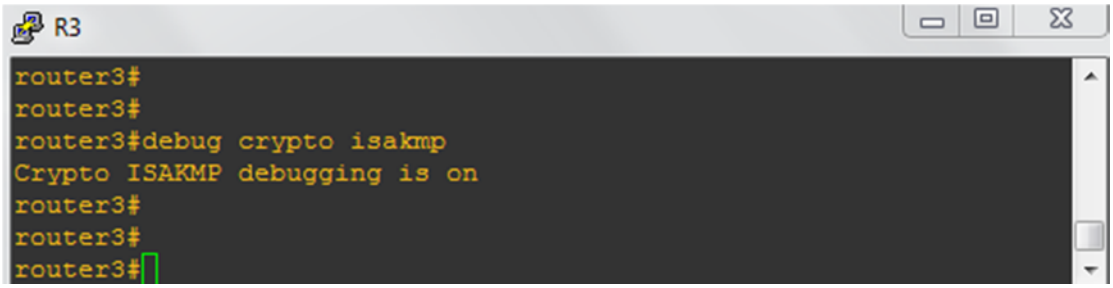


Figure IV.24. Résultat de la commande « debug crypto isakmp » sur R3

- voir le status du tunnel Ipsec

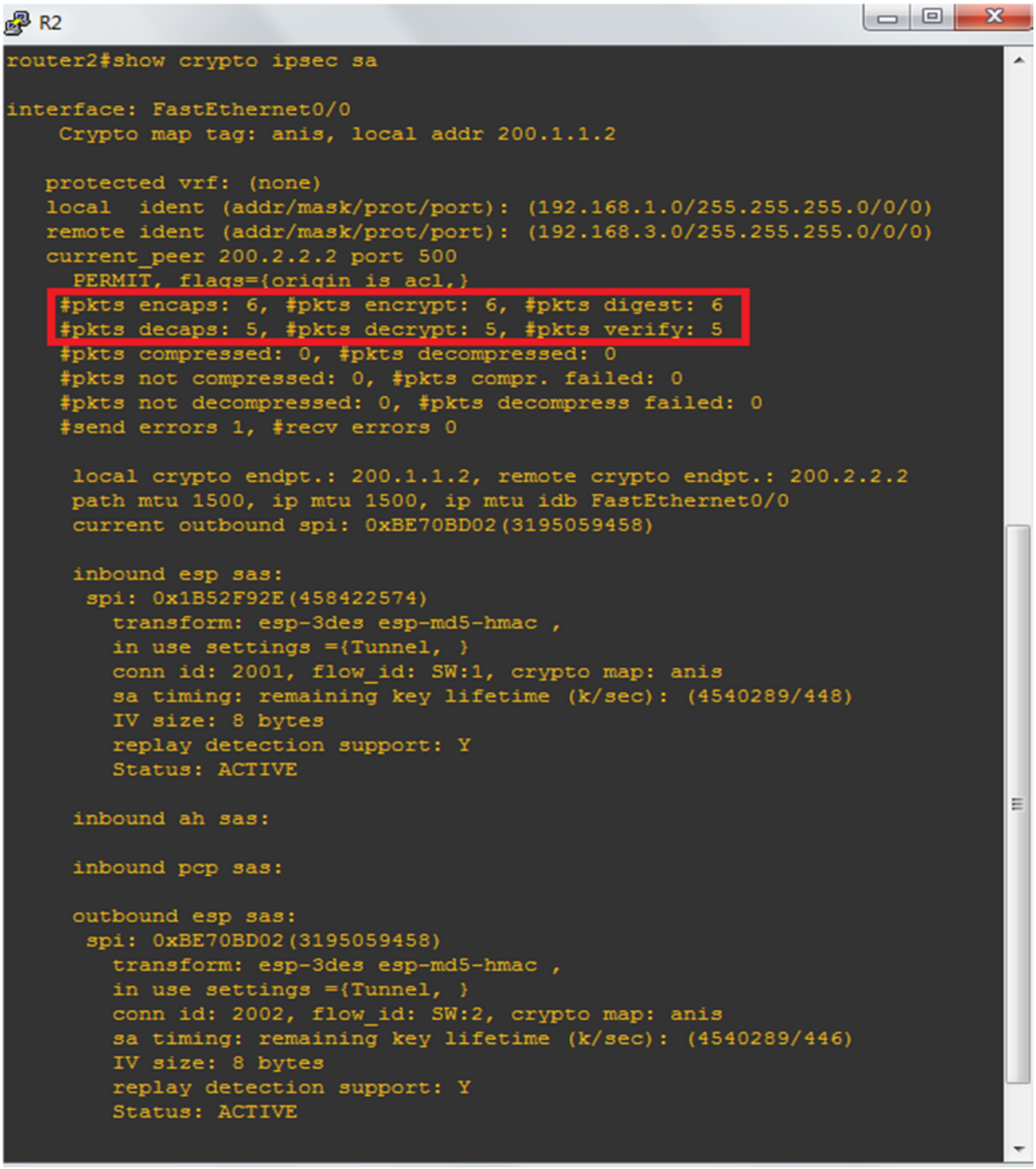


Figure IV. 25. Résultat de la commande sur R2 « show crypto ipsec sa »

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

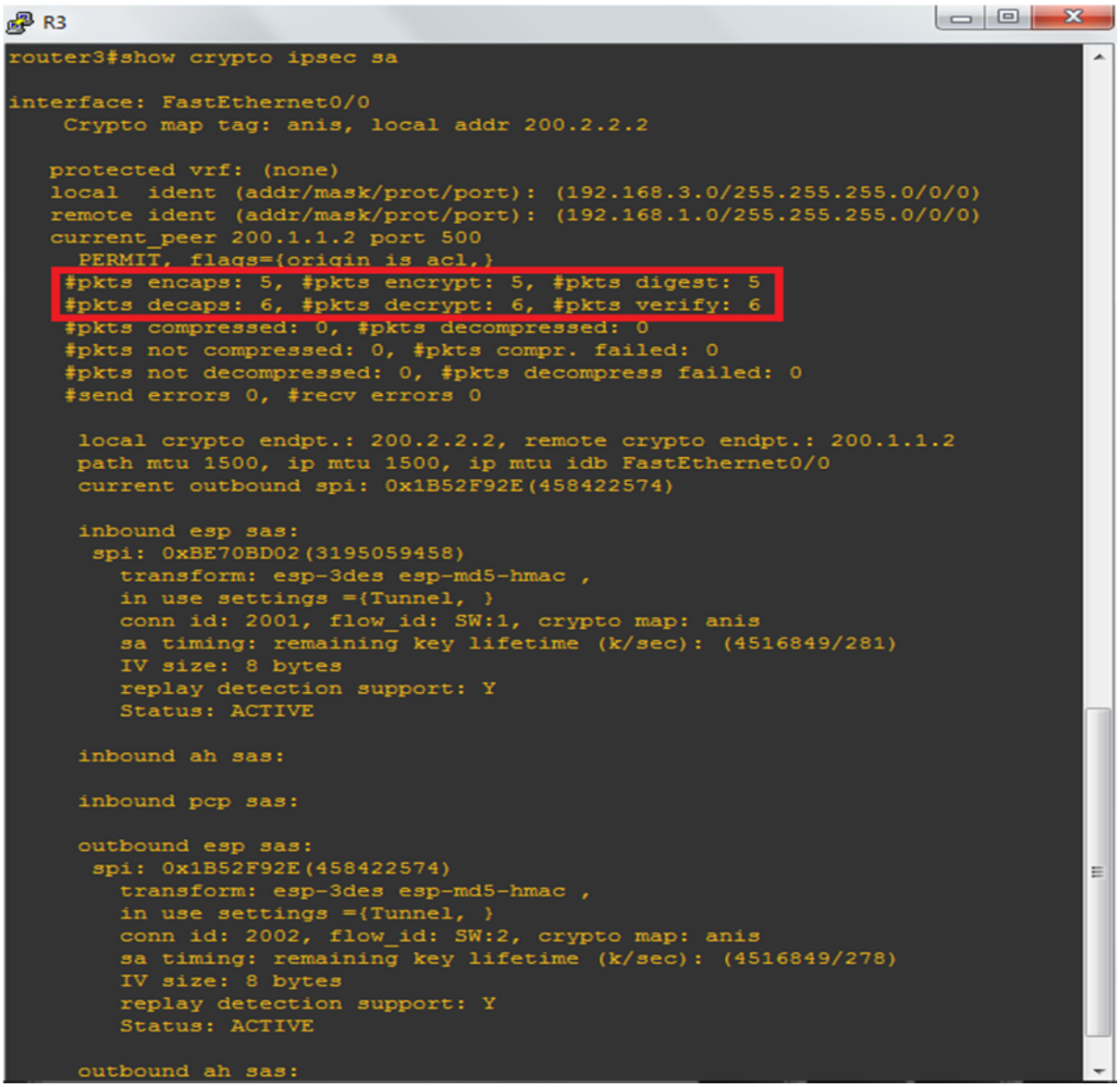


Figure IV .26.Résultat de la commande sur R3 « show crypto ipsec sa »

II.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 langueur de l'information capturée.

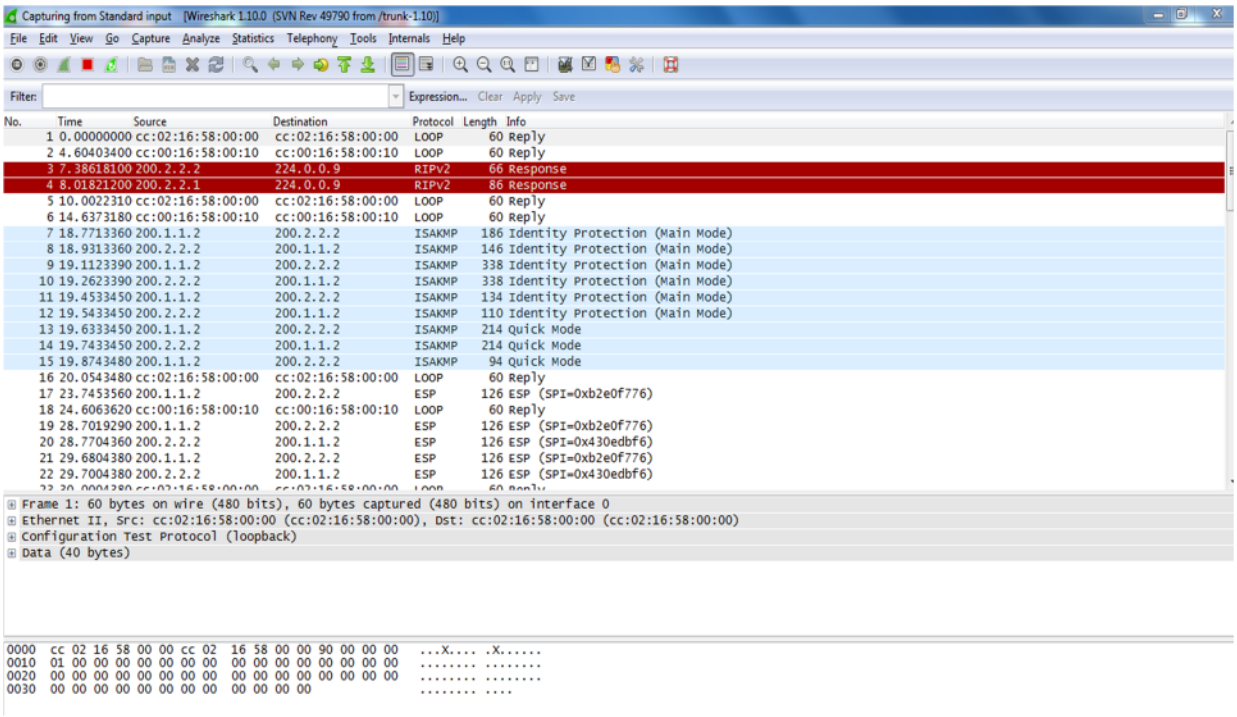


Figure IV.27. Résultat de l'analyse wireshark

III. Conclusion

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

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

[1] [Introduction aux réseaux informatiques de S.KrakOwiak]

[2] http://www.Wikipédia.org.

[3] Guillaume Desgeorge, ‘’La sécurité des réseaux’’

[4] www.commentcamarche.com

[5] : Cryptographie en pratique de Niels Ferguson et Bruce Schneier. Édition : Vuibert - 338 pages, 1er août 2004

[6] : Sécurité informatique (3ème édition) de Laurent Bloch, Christophe Wolfhugel. Édition : Eyrolles - 325 pages, 3eédition, 23 juin 2011

[7] : Solange Ghernaouti-Hélie « Sécurité Informatique et Réseaux » DUNOD 2006.

[8] livre :jean-françois PILLOU et JEAN-PHILIPPE BAY (tous sur la securité informatique)

[9]http://www.guill.net/La sécurité des réseaux.

[10] Andrew Hay and Daniel Cid « OSSEC HIDS Host-Based intrusion Detection system », Syngress edition, 2008

[11] http://www.frameip.com/vpn/

[12] http://www.frameip.com/ipsec/

[13] Sécurité informatique et réseaux 3éme edition ,auteur Solange Ghernouti-Hélie

[14]: Anne Henmi and Mark Lucas « Firewall policies and VPN Configurations », Syngress **edition, 2006**

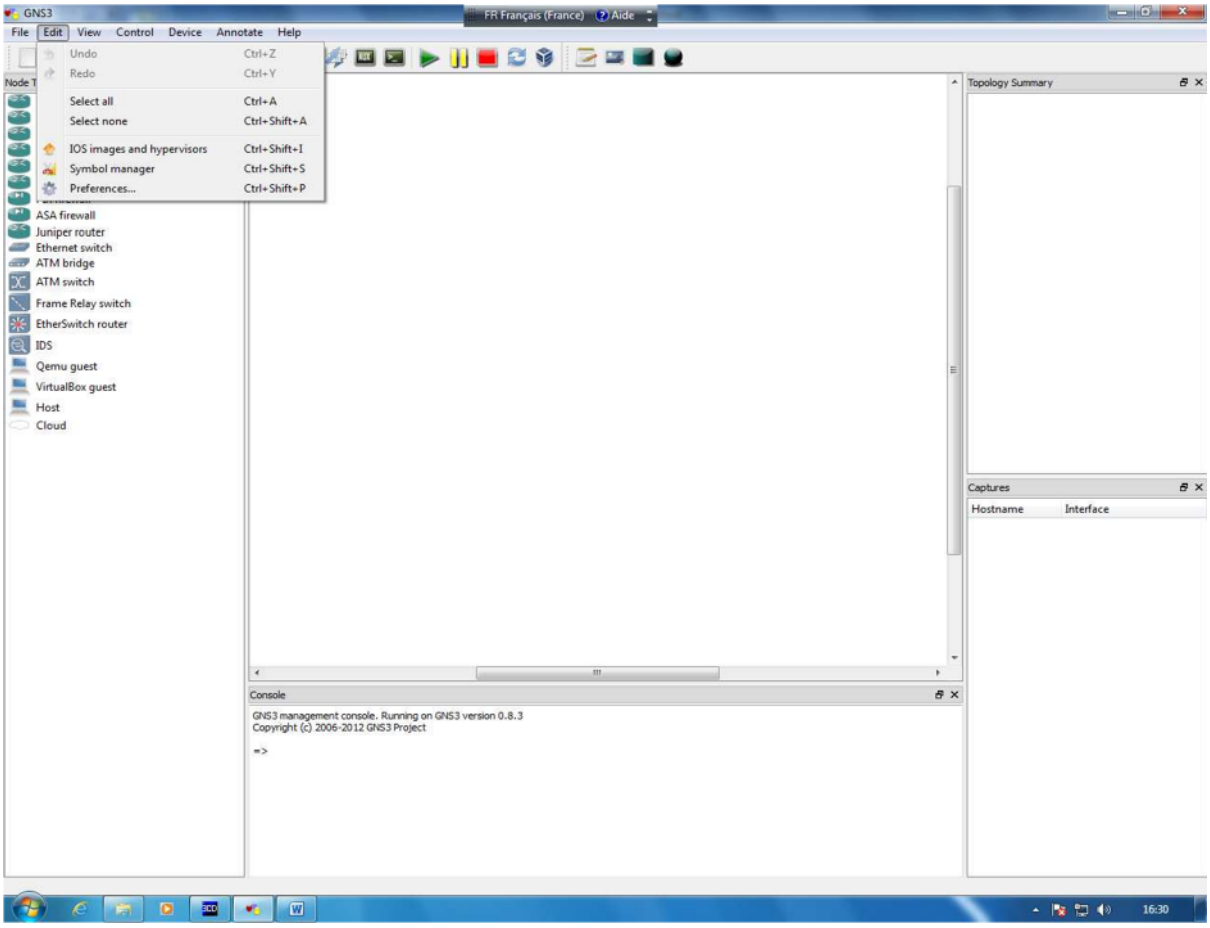
I. Installation et configuration de GNS3 sur PC ayant au moins 4GO de RAM.

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

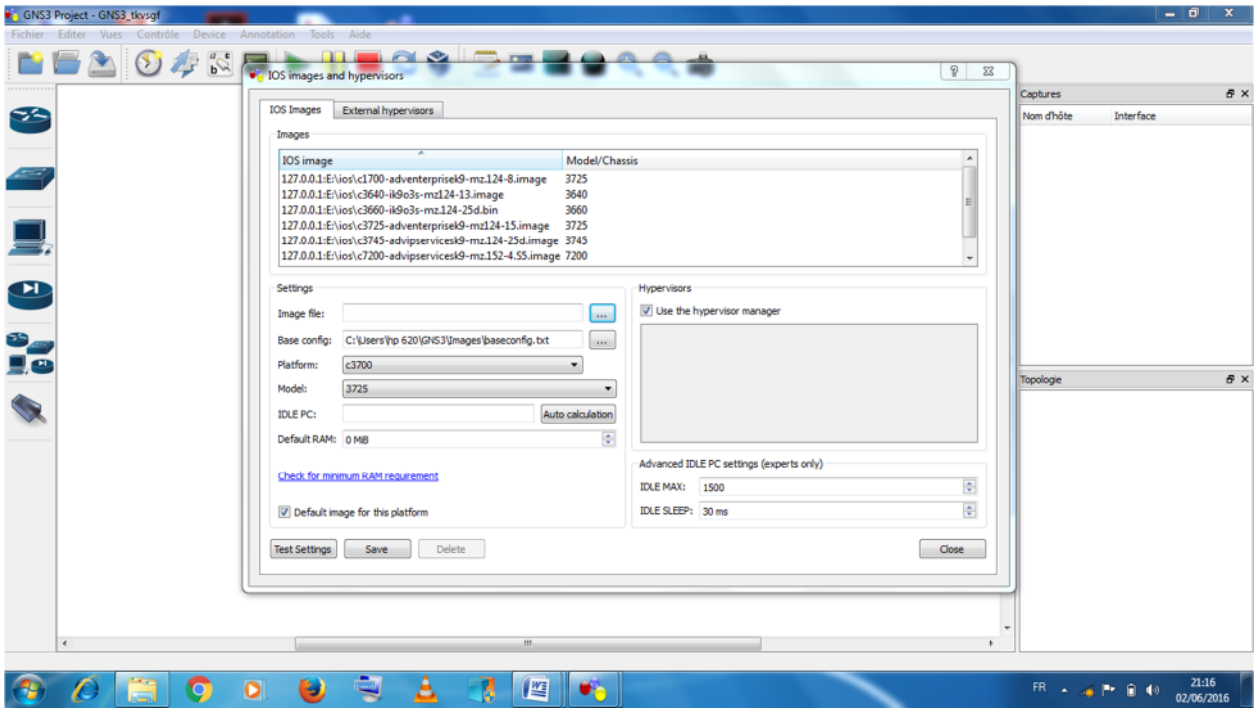
2 – configurer l'URL de l'IOS

Edit >> IOS image and Hypervisor

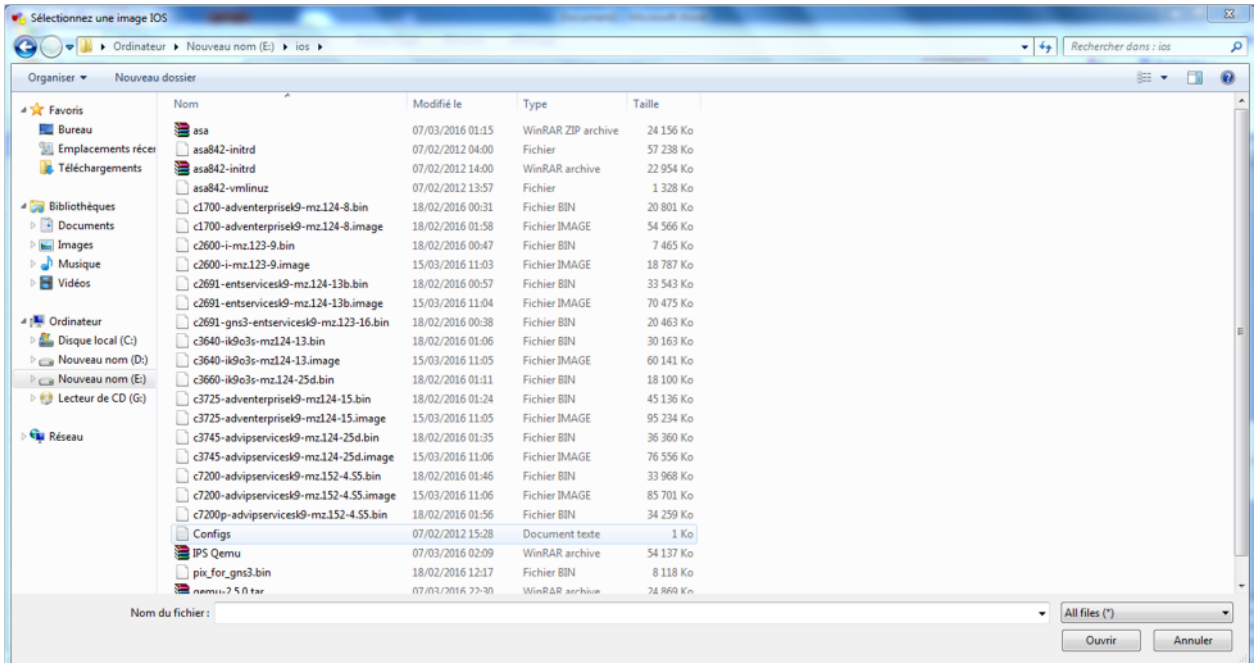


3 - Sélectionner l'imageIOS

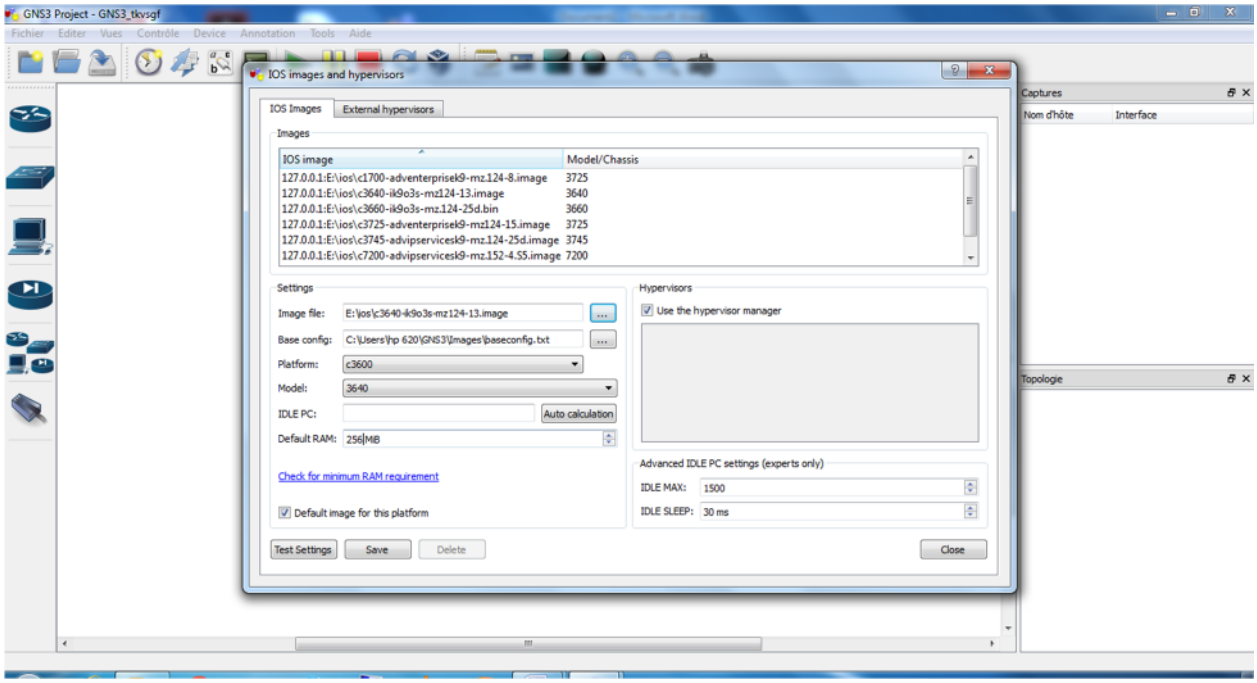
Cliquer sur le bouton face à "Image file"



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

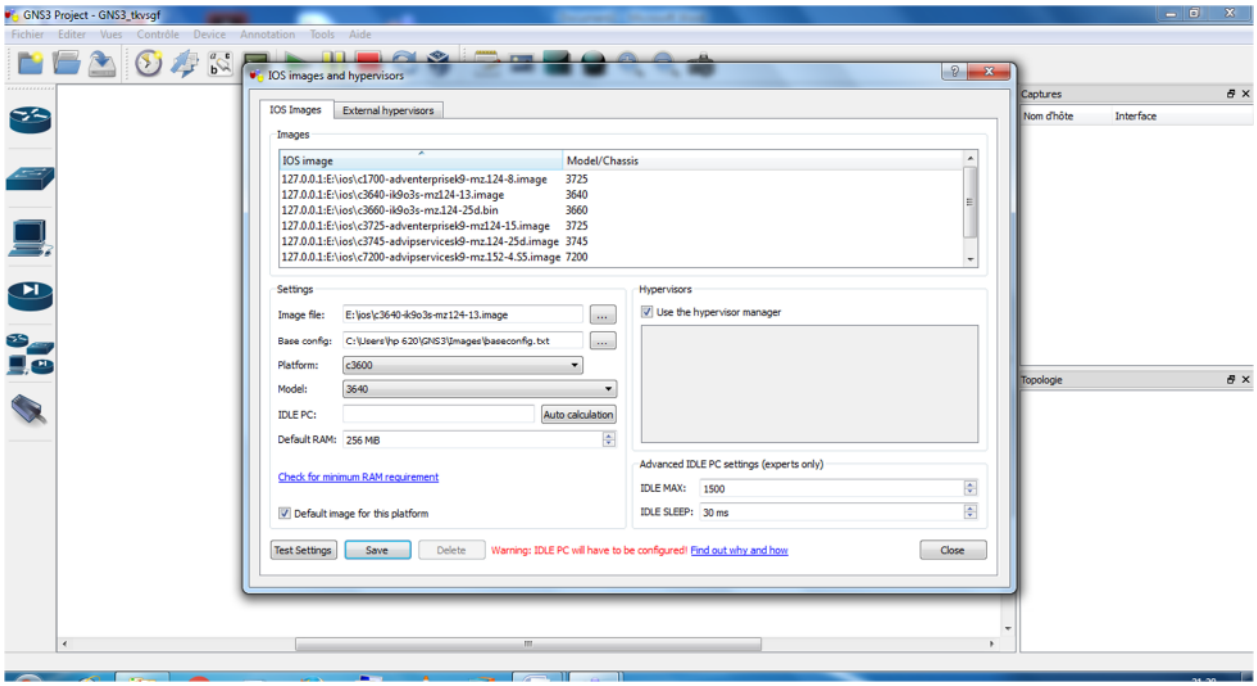


5 – Modifier la capacité mémoire des routeurs émulés de 128 ==> 256 MB Modifier le contenu des champs <<DefautRAM>>

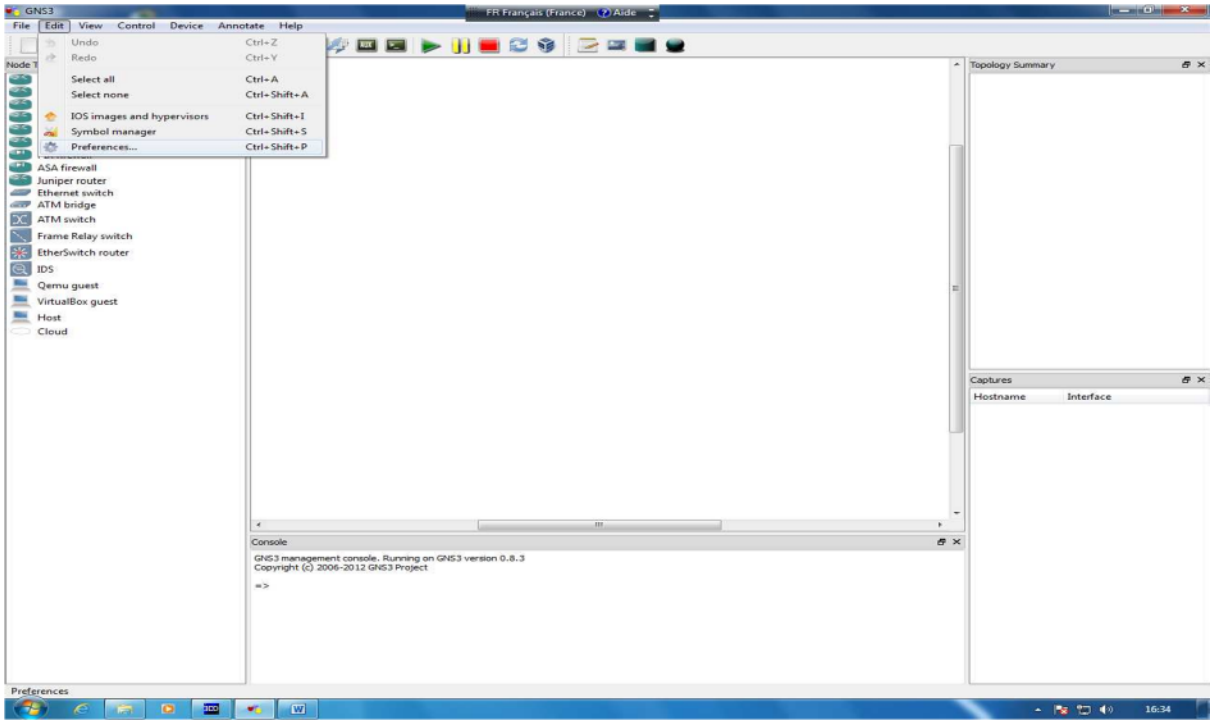


6– Cliquer<<Sauve>>et<<Close>>

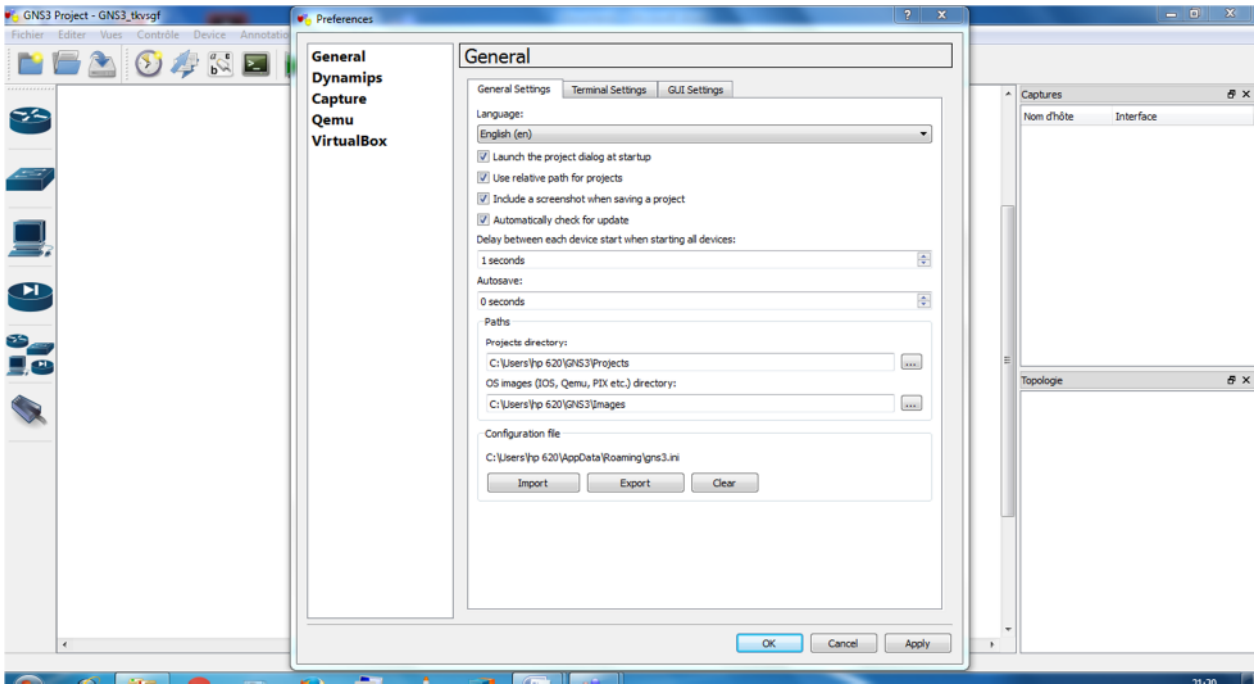
Ignorer le message en rouge "Warning Idle PC ...."



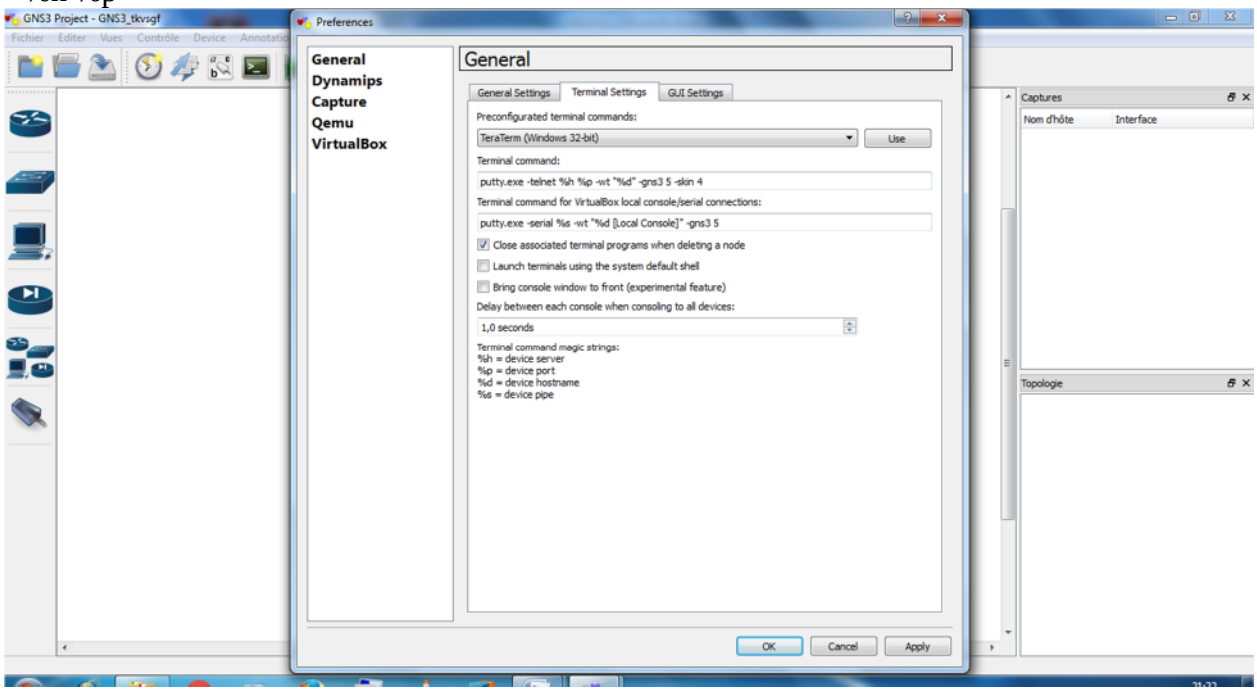
Edit >> Préférence



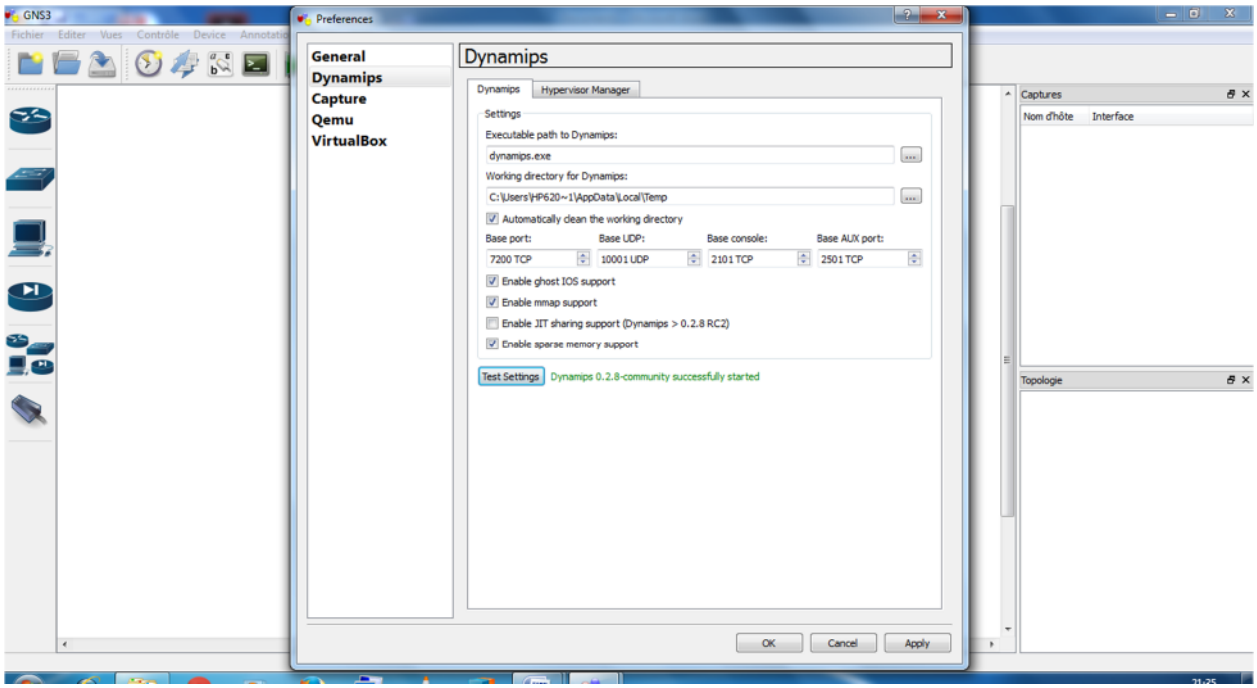
7– Modifier le répertoire par défaut et sélectionner le répertoire GNS3 créé sur ledesktop.



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



Cliquer sur le bouton <Dynamips>>

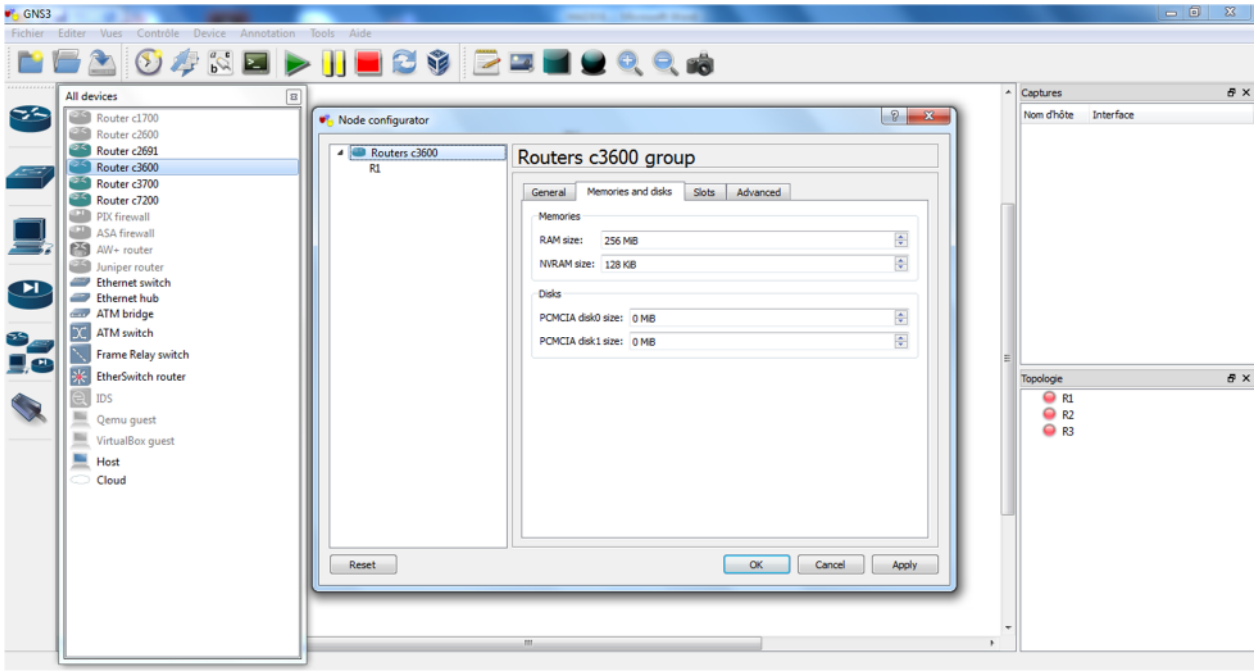


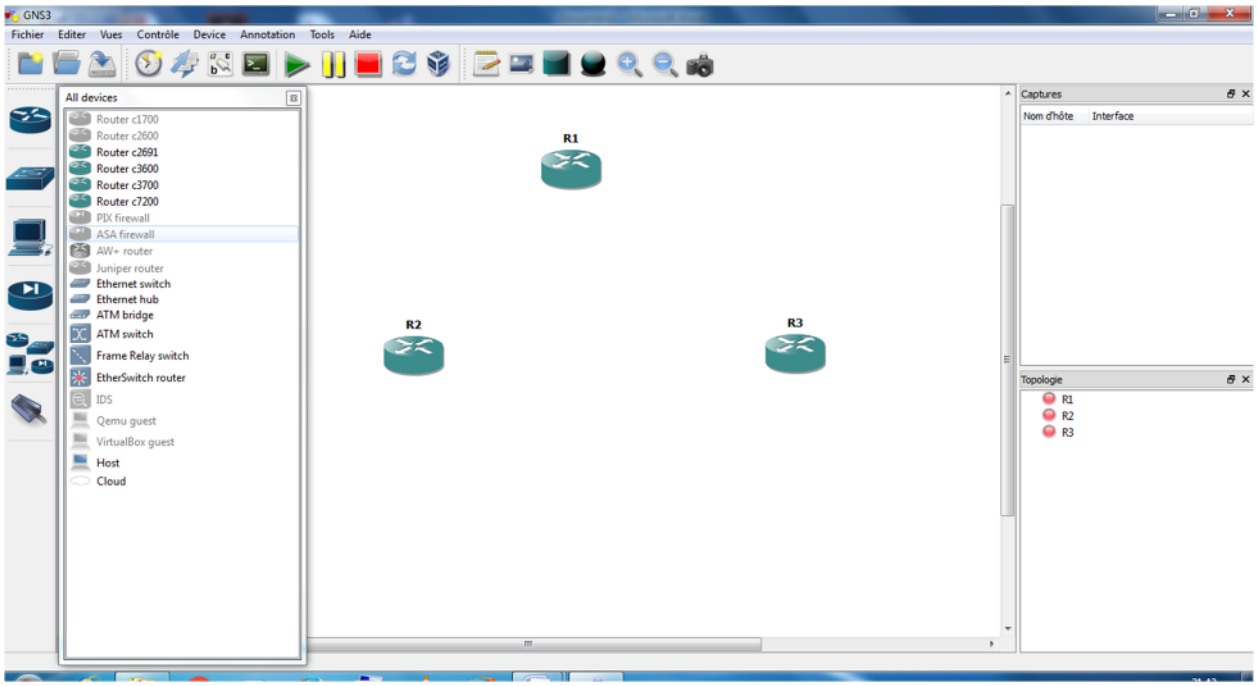
Cliquer sur le bouton **<<Test Settings>>,** au bout de quelques secondes on doit voir

le message en vert <<... successfullystarted>>

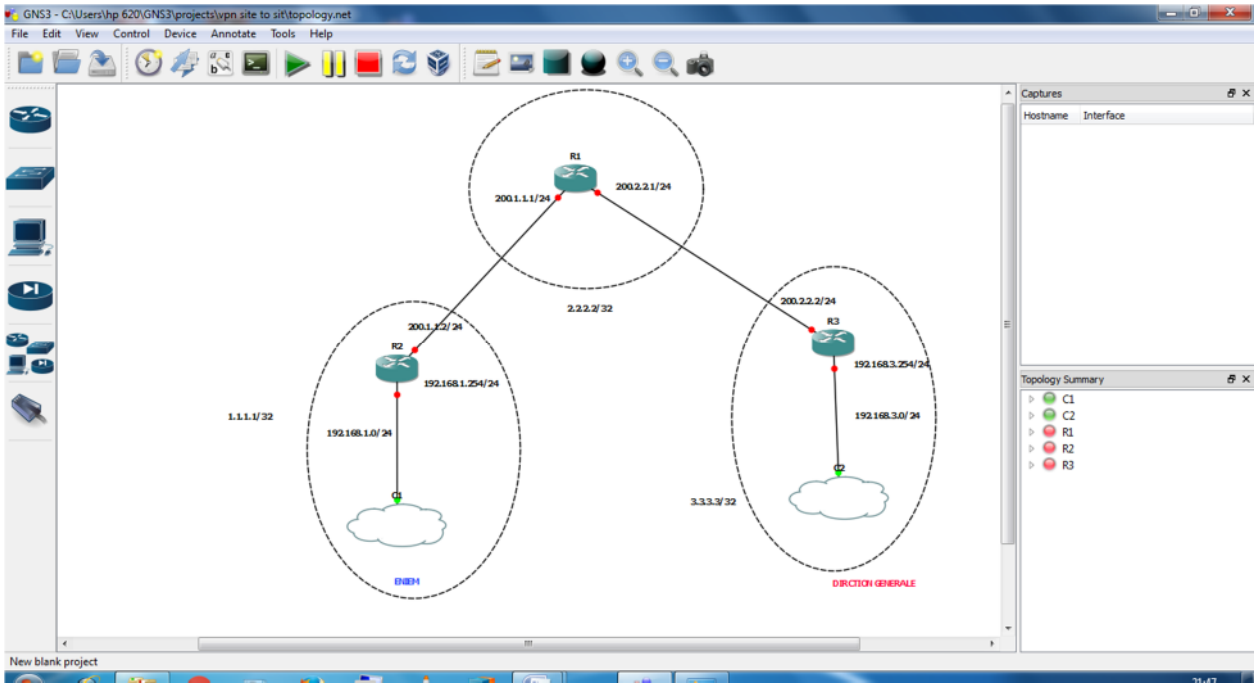
Maintenant que la configuration de base est terminée, on ferme la fenêtre Preference. On fait drag and drop du routeur **c3600**, autant de routeurs que nécessaires.

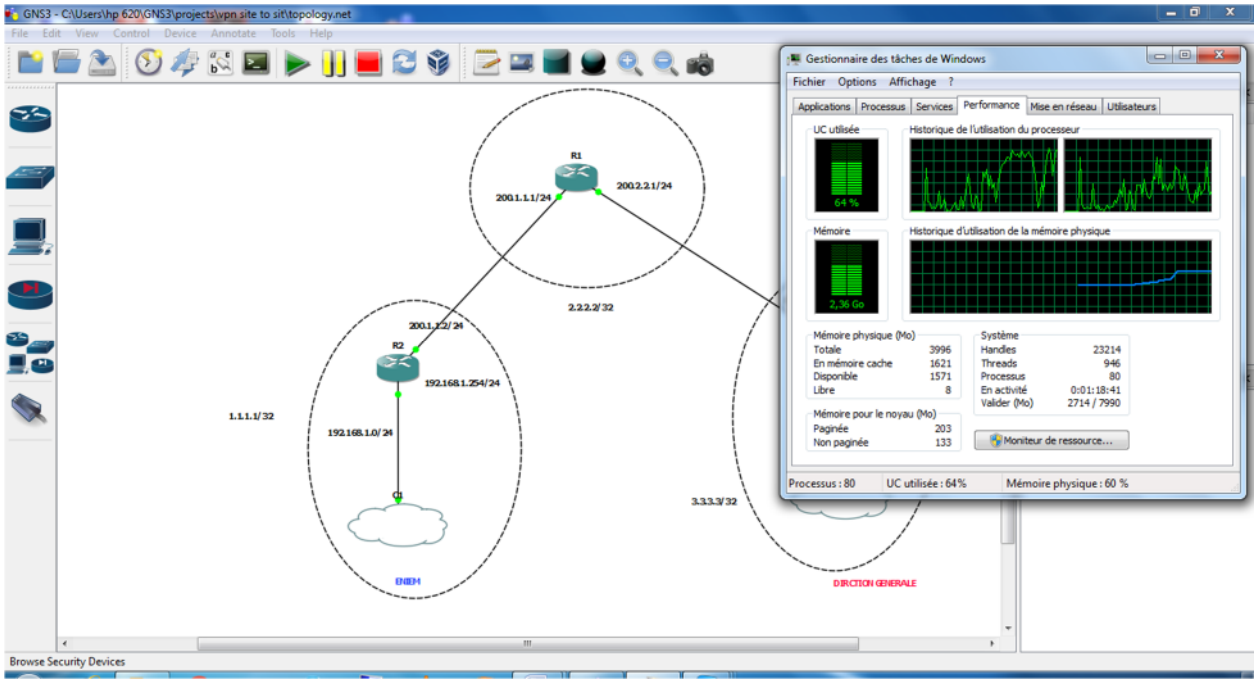
On configure le hardware des routeurs. Par défaut le routeur est équipé de 2 interfaces Fostethernet. Si nécessaire on peut rajouter des WIC 1 ou 2T, pour avoir un ou 2 ports Série.





Interconnection des différents routeurs.
Cliquer l'icone en haut située en dessous de **<<Annotate>>** et **<<Help>>** et sélectionner Fastethernet





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.

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.

II .Listes de quelques commandes CISCO:

«enable»ou«ena»ou«en»pourpasserenmodeadministrateursur l'équipementréseau.

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 confterm	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>ouint e | fa | s | lo	Entre dans le mode de configuration de l'interface
ip address <address><mask>ouip add	Configure l'interface avec l'ipet le masque de réseau
no shutdown ou no shut	Active ouDésactivel'interface
copy running-config startup-configou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
reload	Redémarrel'équipementréseau
ping [<address>]	ping seul, permet de faire un pingétendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
show interfaces oushint	Donne une description détaillé sur les interfaces
show running-configoush run	affiche la configuration courante
show ip route ouship 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 Ipsecsite-à-site

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

Exemple:

access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

2- Définir le secret partagé entre les 2 équipements établissant un tunnelIpsec

!Pre-shared key avec le peer

cryptoisakmp key ghani address 200.2.2.2

3- Définir les paramètres du tunnelIKE

!Policy ISAKMP

cryptoisakmp policy 10

authentication pre-

share encryption des

hash

md5

group 2

exit

4- Définir les paramètres du tunnelIpsec

!Transfrom-set, parametresipsec

cryptoipsec transform-set VPN esp-des esp-md5-hmac

5- Définir la cryptomap

!Crypto map

crypto map anis 10 ipsec-isakmp

set peer 200.2.2.2

set transform-set anis 10

match address 10

exit

6- Appliquer la crypto

map interfacef0/0

cryptomapanis

exit

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 Agrement.

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