République algérienne démocratique et populaire

Ministère de l'enseignement
supérieur et de la
recherche scientifique

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

Mémoire

En vue de l'obtention du diplôme

MASTER ACADEMIQUE

En **R**éseau **M**obilité et les **S**ystèmes **E**mbarqués

Mise en place d'un VPN dans un réseau d'entreprise.

Etudié et réalisé par

M^{elle} **AMIAR** Djida

Encadré par

Mme : **Aoudjit** Rachida

PROMOTION : 2013/2014

REMERCIEMENTS

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

Je tiens à remercier particulièrement mon enseignante

et ma promotrice madame **AOUDJIT RACHIDA,**

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

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

Enfin, mes remerciements s'adressent aux membres du jury

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

Dédicaces

Je dédie ce travail à toute ma

Famille

&

tous mes amis(es)

DJIDA

SOMMAIRE

Chapitre III: Application

Listes des figures :

Chapitre 1 : Introduction à la sécurité informatique et les réseaux privé virtuelles

Chapitre II : VPN's et le protocole IPsec

Chapitre III : Application

Liste des tableaux :

Chapitre III : Application

Introduction générale

La quasi-totalité des flux d'informations sur Internet utilisent le protocole TCP/IP (couches 3 et 4). Une grande partie des protocoles (POP/SMTP/FTP) utilisent d'autres protocoles de communication au mieux binaires, au pire en clair. Les protocoles encryptant leurs données sont relativement spécialisés et donc assez peu utilisés (ssh, https, pop3-ssl...) pourtant, il est extrêmement facile sur Internet pour une personne ayant accès à un périphérique de routage (serveur classique ou routeur) de voir tous les paquets circulants sur le réseau. Par exemple, on peut facilement analyser les trames relatives à la consultation des emails. Par défaut dans le protocole POP3, les mots de passe circulent en clair sur le réseau. Ainsi, il est facile d'obtenir le mot de passe du compte pop d'un utilisateur sans pour autant avoir le moindre accès au poste client ou au serveur.

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

Vu l'objectif des entreprise ont et l'estime qu'on lui accorde, j'ai jugé bon de porter mon choix sur ce sujet qui s'intitule : « Mise en place d'un réseau VPN dans une entreprise » afin de faire profiter à l'entreprise cette étude et au monde scientifique mes connaissances acquises durant mon parcours universitaire.

Il est affirmé qu'un travail scientifique, pour être bien précis, doit être délimité. Raison pour laquelle, je ne vais pas aborder toutes les questions liées à la conception d'un réseau VPN car elles paraissent une matière très complexe. Ainsi, j'ai pensé limiter mon étude en établissement d'un tunnel VPN site à site utilisant le protocole Ipsec qui offre :

- ✓ **Authentification** : garantir que les données reçues proviennent de l'expéditeur déclaré.
- ✓ **Confidentialité** : Les données transportées ne peuvent être lues que par les tiers communicants.
- ✓ **Intégrité** : garantit que les données n'ont pas été modifiées durant leur transfert.
- ✓ **Anti-rejeu** : élimine les paquets dupliqués.

Vu la grandeur du sujet que j'ai abordé, mon travail sera subdivisé en trois chapitres, dans le premier chapitre j'ai donné quelques notions fondamentales sur l'architecture et la sécurité des réseaux informatique, dans le chapitre qui suit, j'ai développé le concept et l'architecture des VPNs, et j'ai terminé par une mise en place d'un VPN au sein d'un réseau que j'ai proposé moi-même.

Chapitre I

Généralités sur les réseaux informatiques

Introduction

Un réseau informatique est un maillage de micro-ordinateurs interconnectés dans le but du partage des informations et du matériel. Quelque soient le type de systèmes informatiques utilisés au sein d'une entreprise, leur interconnexion pour constituer un réseau est obligatoire. La constitution de celui-ci passe par une conception qui consiste à définir :
- l'architecture des réseaux ;
-Les outils de sécurité ;
-…
C'est les points sur lesquelles on va se baser durant ce chapitre.

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

I.1 Architecture physique :

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

I.1.1.Topologie des réseaux :

- ***Topologie en bus***

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

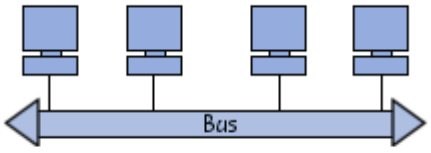


Figure I.1 : Topologie en bus.

Avantage : facile à mettre en œuvre et de posséder un fonctionnement simple

Inconvénient*:* si la ligne de transmission est défectueuse, l'ensemble du réseau en est affecté.

- ***Topologie en étoile***

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

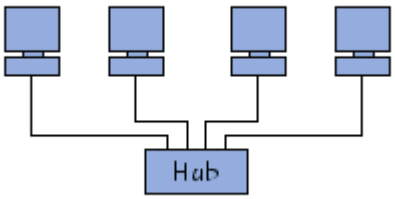


Figure I.2 : Topologie en étoile.

Avantage : beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau

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

- **Topologie en anneau**

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

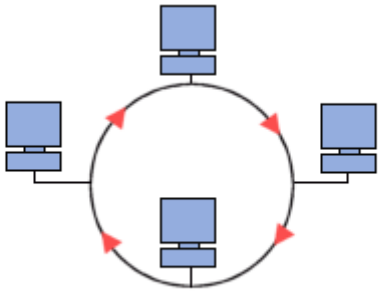


Figure I.3 : Topologie en anneau

- **Topologie maillée**

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

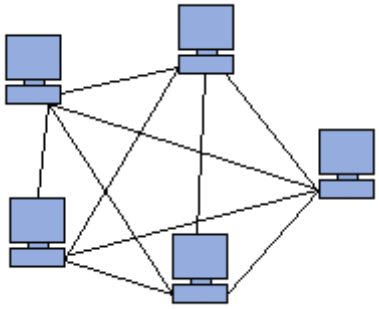


Figure I.5 : Topologie maillée

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

Inconvénient : le nombre de liaisons nécessaires qui devient très élevé.

I.1.2 support physique :

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

- **Câble coaxial**

Le câble coaxial en anglais coaxial cable, a longtemps été le câblage de prédilection, pour la simple raison qu'il est peu coûteux et facilement manipulable (poids, flexibilité, ...).

- **Câble paire torsadée**

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

- **Fibre optique**

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

I.1.3 Equipements d'interconnexion

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

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

- **Répéteur**

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

- **Hub**

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

- **Switch**

Un switch ou commutateur réseau est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et de télécommunication. Le commutateur établit et met à jour une table, dans le cas du commutateur pour réseau Ethernet il s'agit de la table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée, en fonction des adresses MAC sources des trames reçues sur chaque port.

- **Routeur**

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

- **Passerelle**

La passerelle relie des réseaux hétérogènes, elle dispose des fonctions d'adaptation et de conversion de protocoles à travers plusieurs couches de communication jusqu'à la couche application.
On distingue les passerelles de transport qui mettent en relation les flux de données d'un protocole de couche transport ;
Les passerelles d'application qui quant à elles réalisent l'interconnexion entre applications de couches supérieures.

- **Firewall**

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

I .2 .Architecture logique

I .2 .1. Introduction

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

I.2.2. Adressage IP :

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

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

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

I.2.3 .Plan d'adressage

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

I.2.4. Routage

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

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

II. Sécurité des réseaux

II.1.Introduction

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

Comme solution de ce problème, l'utilisation des VPNs (Réseaux privés virtuels) permettent de transporter les données en toutes sécurité, en utilisent des connexions virtuelles routées via Internet.

Avant de parler sur les VPN, je vous donne un aperçu général sur la sécurité informatique, les menaces , les techniques d'attaque ...

II.2.Les menaces :

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

- **Virus**

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

- **Vers :**

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

- **Spywares :**

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

- **Hijackers :**

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

- **Troyen :**

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

- **Backdoor**

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

- **Spam**

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

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

- **Mailbombing**

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

II.3.Les techniques d'attaques :

- **Déni de service :**

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

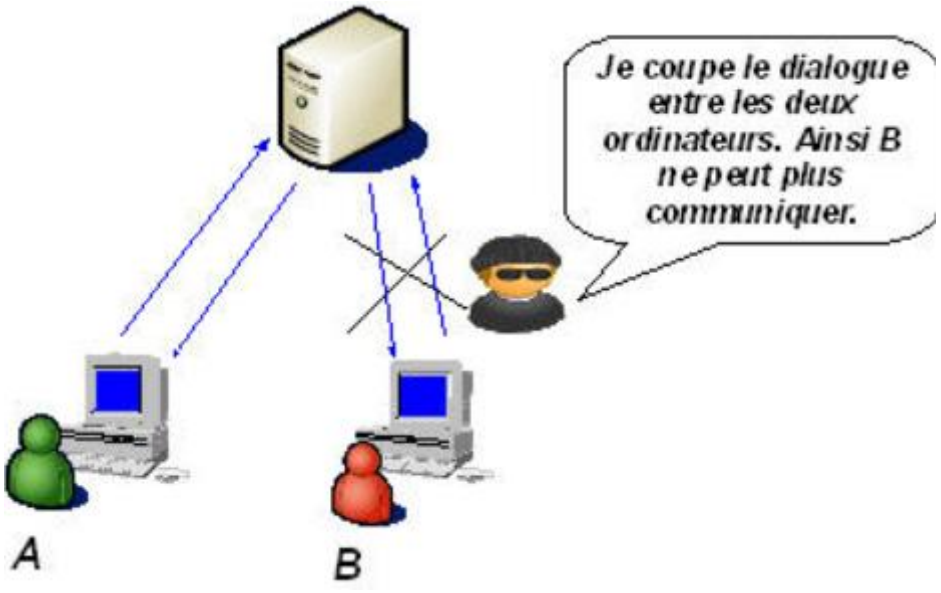


Figure I.6: Dénis de service.

- **Sniffing :**

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

Figure I .7 : le sniffing

- **Scanning**

Le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanné. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C'est un outil très utile pour les hackers. Cela leur permet de connaitre les points faibles d'une machine

et ainsi de savoir par où ils peuvent attaquer. D'autant plus que les scanners ont évolué. Aujourd'hui, ils peuvent déterminer le système d'exploitation et les applications associées aux ports.

Figure II.8 : Scanning

Social engineering :

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

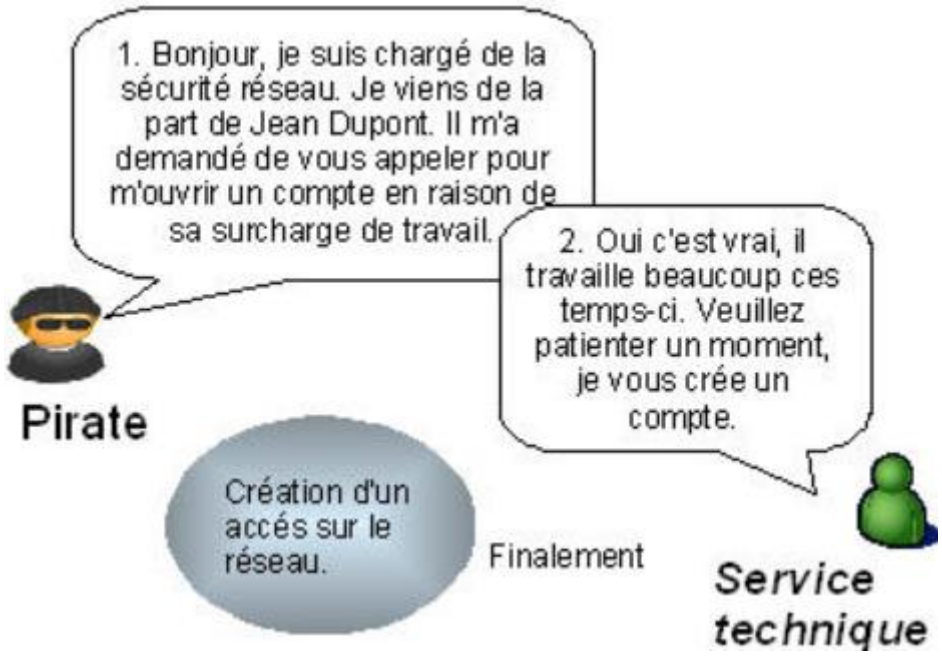


Figure I.9 : Le social engineering

- **Cracking :**

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

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

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

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

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

- **Spoofing :**

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

- **Usurpation de l'adresse IP**
  Une adresse IP correspond en gros à l'adresse postale d'un ordinateur. Ainsi, en changeant d'adresse IP, on peut se faire passer pour un autre ordinateur et obtenir des informations sensibles qui ne nous sont pas destinées.
- **Usurpation de l'adresse e-mail**
  Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur. Mais, il est possible de changer l'adresse. Ainsi, un pirate peut vous envoyer un mail en usurpant l'adresse de votre supérieur.

- **Man in the Middle :**

Man in the Middle signifie l'homme du milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un

pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme du milieu.

Figure I .10 : man in the middle

- **Hijacking**

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

Figure II .10 : Hijaching

- **Buffer OverFlow**

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

II.2.4.1.But d'attaques :

Interruption : Vise la disponibilité des informations.

Figure I.6: Interruption des données.

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

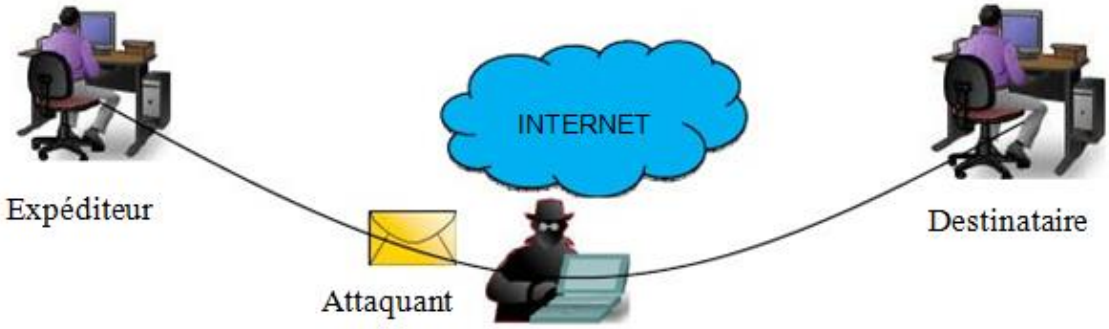


Figure I.7 : Interception des données

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

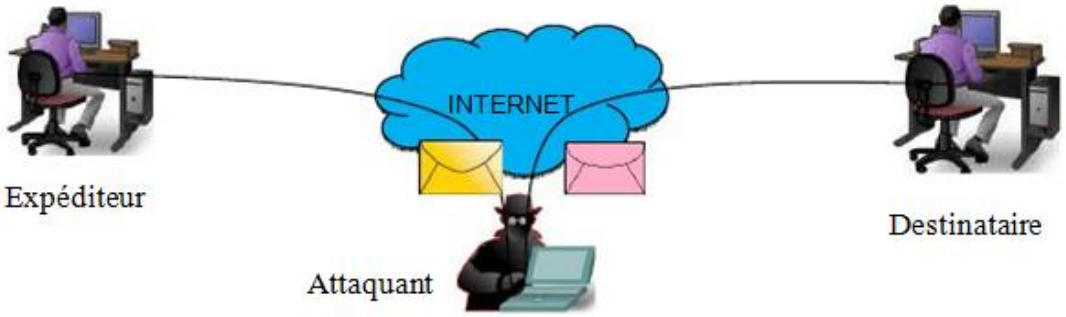


Figure I. 8 : Modification des données

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

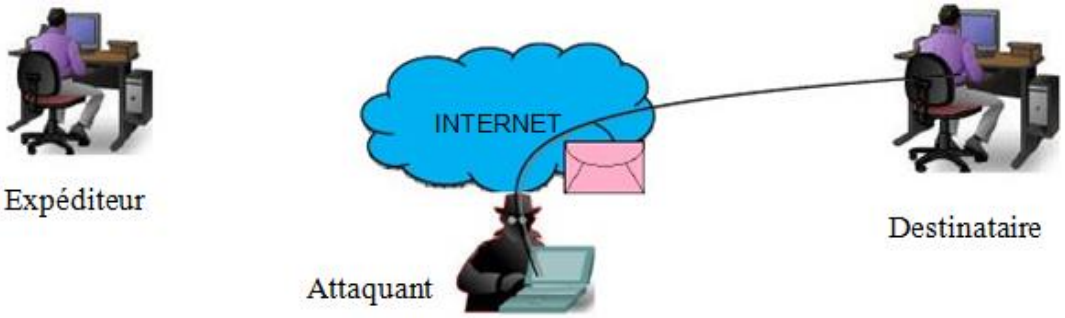


Figure I.9 Fabrication des données.

II.5.Moyennes et technique de sécurité

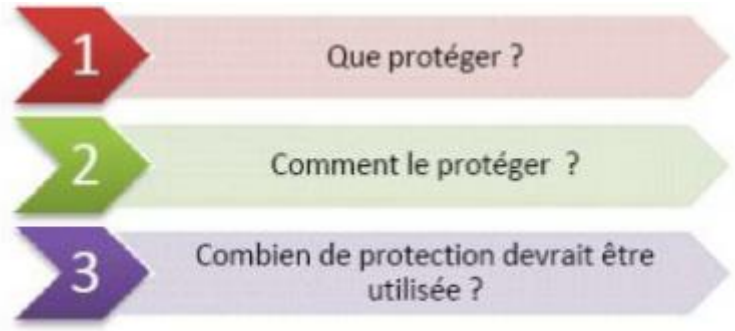
La tâche la plus difficile quand on traite la sécurité ou bien quand on définit la politique de sécurité que l'entreprise doit suivre, est probablement la phase de planification dans laquelle on développe une solution pour répondre aux besoins en sécurité et les objectifs de notre entreprise. En examinant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

• Une politique de sécurité cohérente et simple devrait être créée, basée sur la stratégie et les objectifs de l'entreprise (c.à.d. aider l'entreprise à atteindre ces objectifs, et non l'entraver par des procédures trop rigides qui vont gêner les utilisateurs dans leur travail et diminuer le rendement).

• La politique de sécurité devra décider du choix des solutions et des produits de sécurité, mais pas l'inverse.

• La gestion de sécurité devrait être centralisée sous une seule plateforme, de préférence d'un même constructeur afin de faciliter le déploiement, le contrôle et le support de la solution.

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



- **Authentification :**

La première étape afin de protéger les ressources d'un réseau est de pouvoir vérifier l'identité des utilisateurs. Cette vérification s'appelle authentification.
L'authentification est la procédure mise en œuvre notamment pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée.

- **Cryptographie :**

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

- **Logiciels antivirus**

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

- **Pare-Feu**

C'est un routeur ou serveur d'accès désigné comme tampon entre les réseaux publics connectés et un réseau privé, ou bien entre Internet et le réseau interne d'une entreprise. En pratique, le pare-feu consistera en une architecture, plutôt qu'un matériel ou un logiciel précis. Cette architecture intégrera alors une série de composants matériels et logiciels qui eux tenteront précisément d'assurer le niveau de sécurité requis.

L'architecture la plus en vogue actuellement est basé sur une « Zone démilitarisée » Communément appelée DMZ (Demilitarized Zone) comme illustré dans la figure suivante.

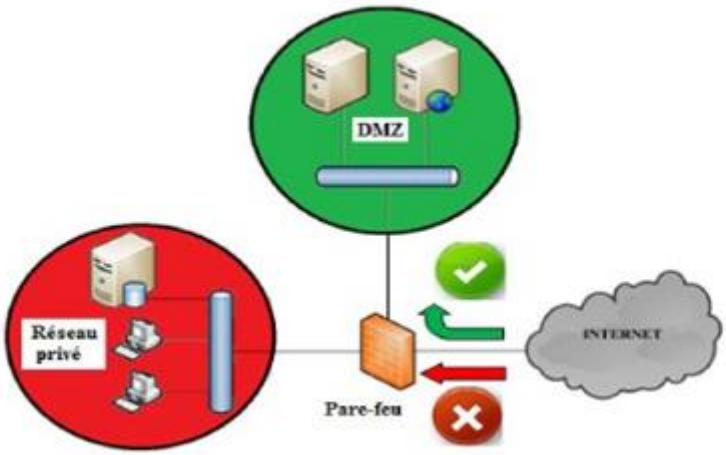


Figure I. 10: Architecture DMZ.

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

- **Filtres de Paquets**

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

- **Les Proxys**

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

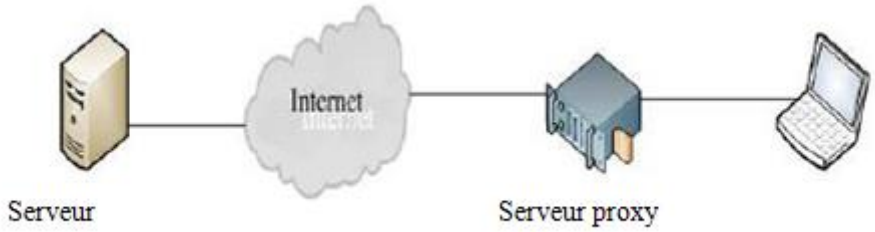


Figure I.11: Emplacement de serveur proxy.

- **Système de détection d'intrusions**

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

- **VPN** :

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

II.7 Caractéristiques d'un réseau fiable

Un réseau solide est un réseau qui offre :

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

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

- **Les liaisons avec le réseau** public : chaque contrat avec un opérateur doit garantir par exemple un certain délai de rétablissement du lien en cas de dysfonctionnement. Ce même principe doit être définit en interne.

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

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

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

- **Sécurité** : les problèmes liés à la sécurité, souvent très onéreux, peuvent être l'indisponibilité des serveurs, du réseau, les vols d'information, des attaques qui viennent parfois du réseau local. Les outils pour y remédier sont tellement disparates (un peu à tous les niveaux) et ne colmatent qu'une partie des failles du fait des nouvelles sorties. De plus le protocole réseau IP qui n'assure aucune fiabilité ne rend pas cette tâche facile. Vue

l'importance de la sécurité, il s'avère utile de coupler plusieurs outils et mécanismes pour au moins s'assurer une meilleure protection.

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

Conclusion

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

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

Dans le chapitre suivant, je vais détailler une technique de sécurité réseau qui est les VPN utilisant le protocole Ipsec.

Chapitre II

Les VPNs

II.1.Introduction

Un VPN (Virtual Private Network ou RPV Réseau Privé Virtuel), au sens le plus large, consiste à établir un réseau logique entre deux points, en utilisant les ressources de réseaux physiques.

J'ai privilégié les VPN de niveau 3 en détaillant particulièrement le protocole IPSec. C'est ce qu'on va voir ensemble durant tout ce chapitre.

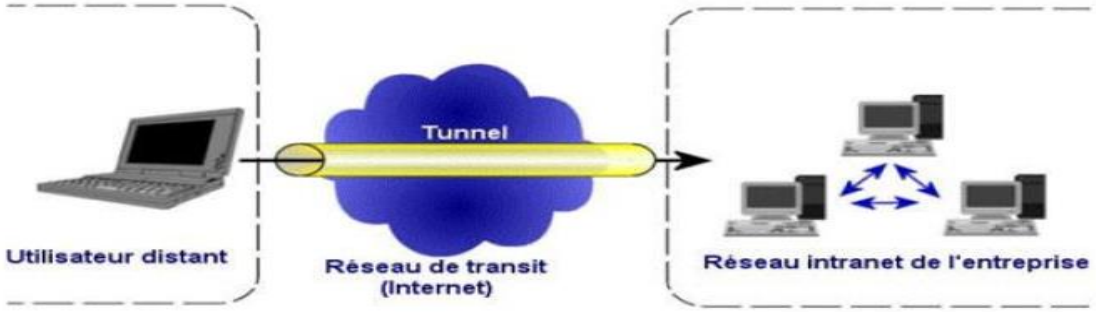


Figure II.1 : Schéma d'un accès VPN

Limites de responsabilité VPN niveau 2 et 3 :

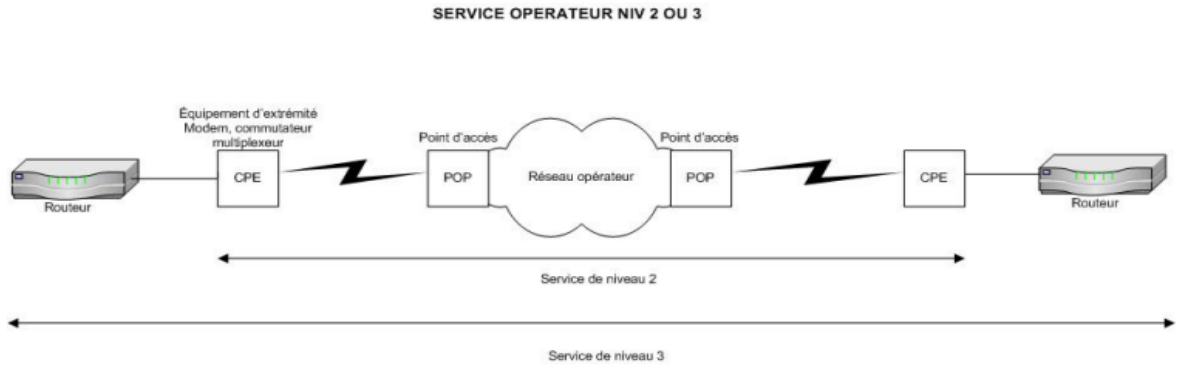


Figure II.2: Service Niveau 2 ou 3.

- **Les VPN de niveau 2 :**

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

- **Les VPN de niveau 3** :

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

- **Les VPN IPSec (niv 3) :**

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

II .2.Les VPN en entreprise :

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

Suivant les besoins ; on référence 3types de VPN :

- **Le VPN d'accès** :

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

- **L'internet VPN** :

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

- **L'extranet VPN** :

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

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

.

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

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

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

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

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

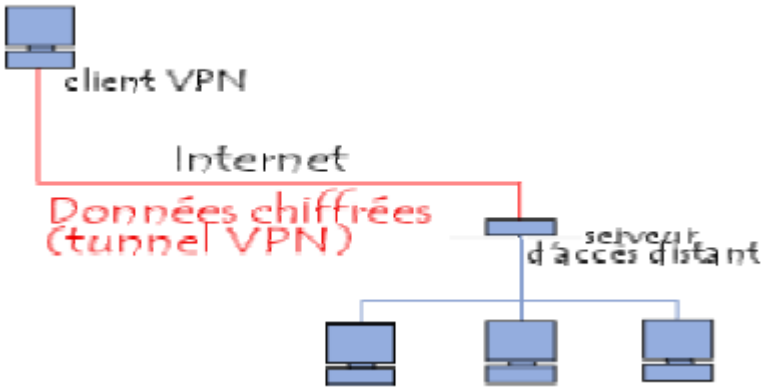


Figure II .3 : Tunnel VPN

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

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

II.5.Les 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 différentes architectures possibles :

- **De poste à poste :**

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

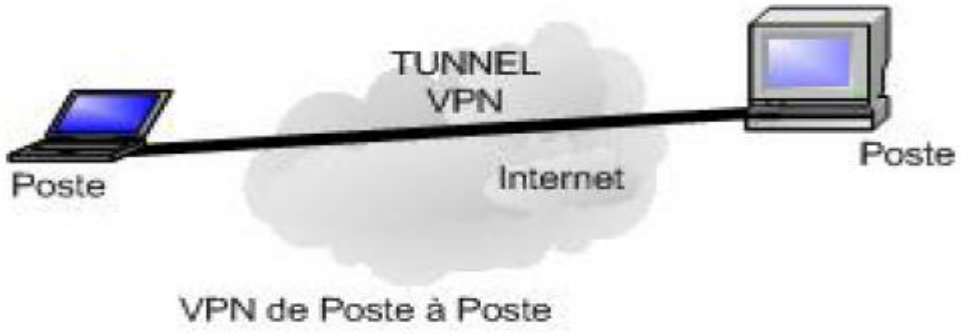


Figure II .4 : VPN de poste à poste.

- **De poste à site :**

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

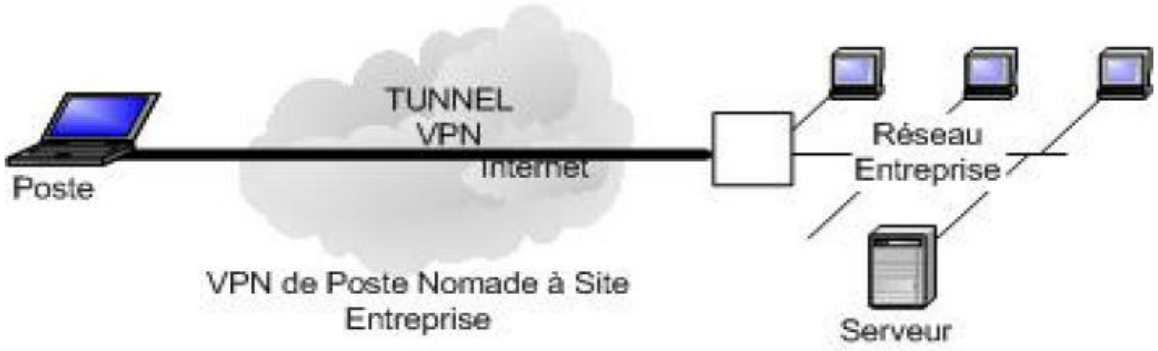
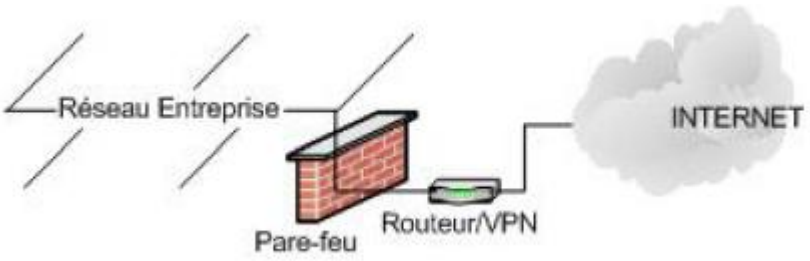


Figure II. 5 : VPN de poste Nomade à site Entreprise.

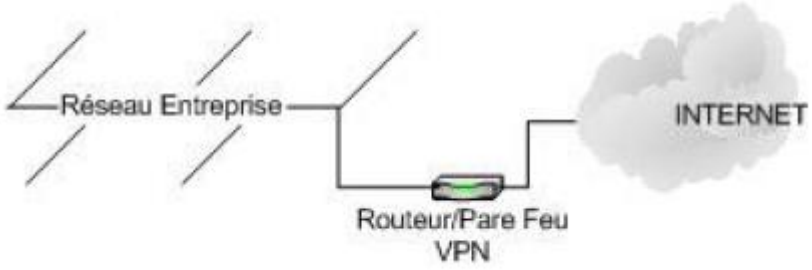
- **De site à site :**

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

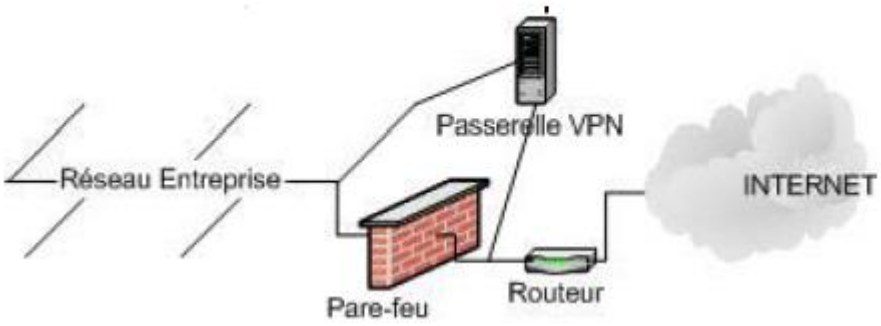
a. Routeur/VPN placé après le pare-feu :



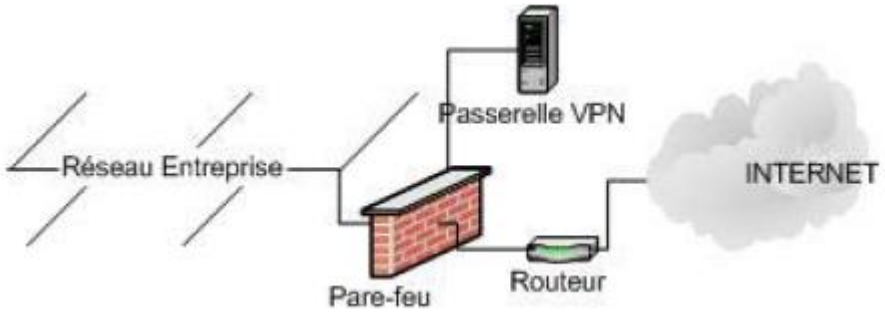
b. Routeur/pare-feu/VPN intégré :



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



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



II.7.Description du fonctionnement :

II.7.1.le protocole PPP :

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

Les différentes méthodes d'authentification :

- **Le protocole PAP :**

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

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

- **Le protocole CHAP :**

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

Format de la trame PPP :

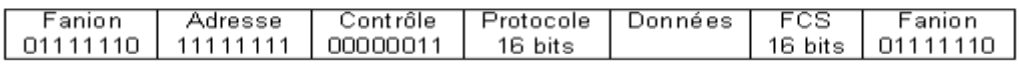


Figure II .6 : Format d'une trame PPP.

III.7.2 : Les différant protocoles utilisé pour l'établissement d'un VPN

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

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

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

- **Le protocole PPTP :**

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

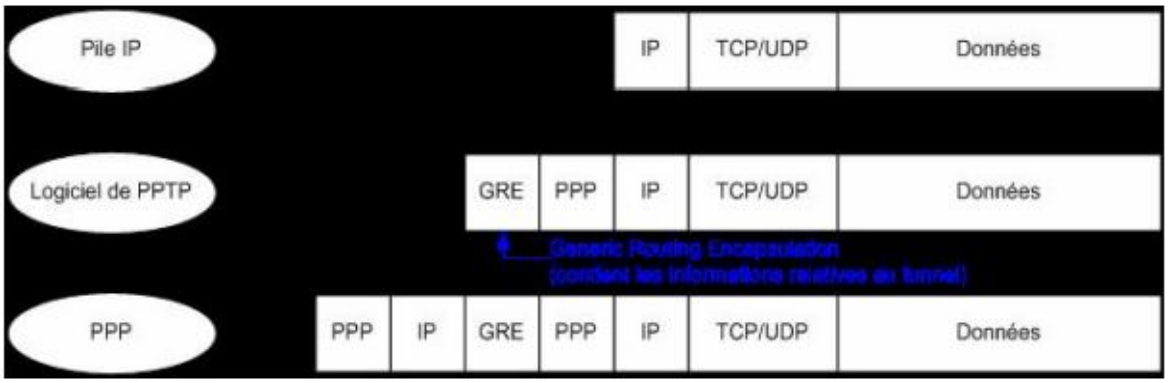


Figure II.7 : Format de trame PPTP.

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

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

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

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

- **Le protocole L2F :**

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

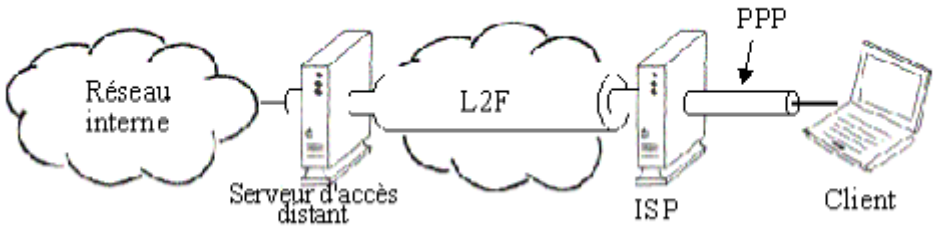


Figure II.8 : Tunnel L2F.

- **Le protocole L2TP :**

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

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

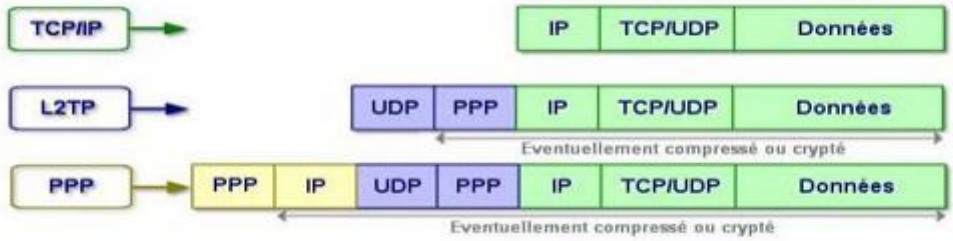


Figure II.8 : encapsulation L2TP

II.7.3. Le protocole de Niveau 3 : IPSEC :

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

Les objectifs de la sécurité d'IPSec sont :

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

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

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

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

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

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

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

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

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

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

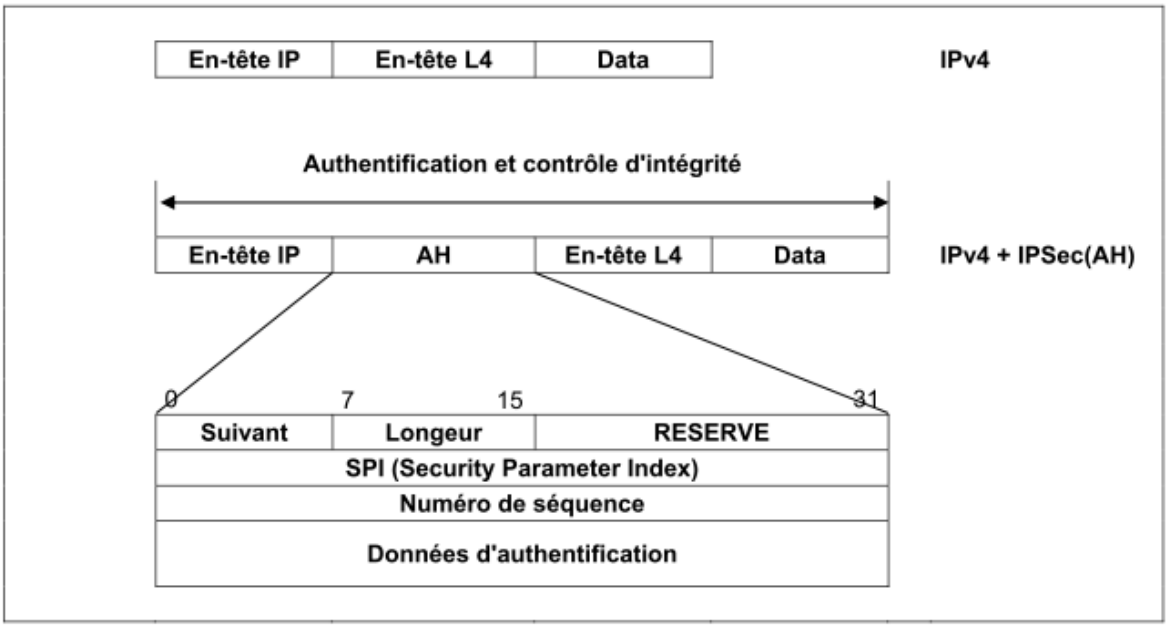


Figure II.9: En-tête AH

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

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

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

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

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

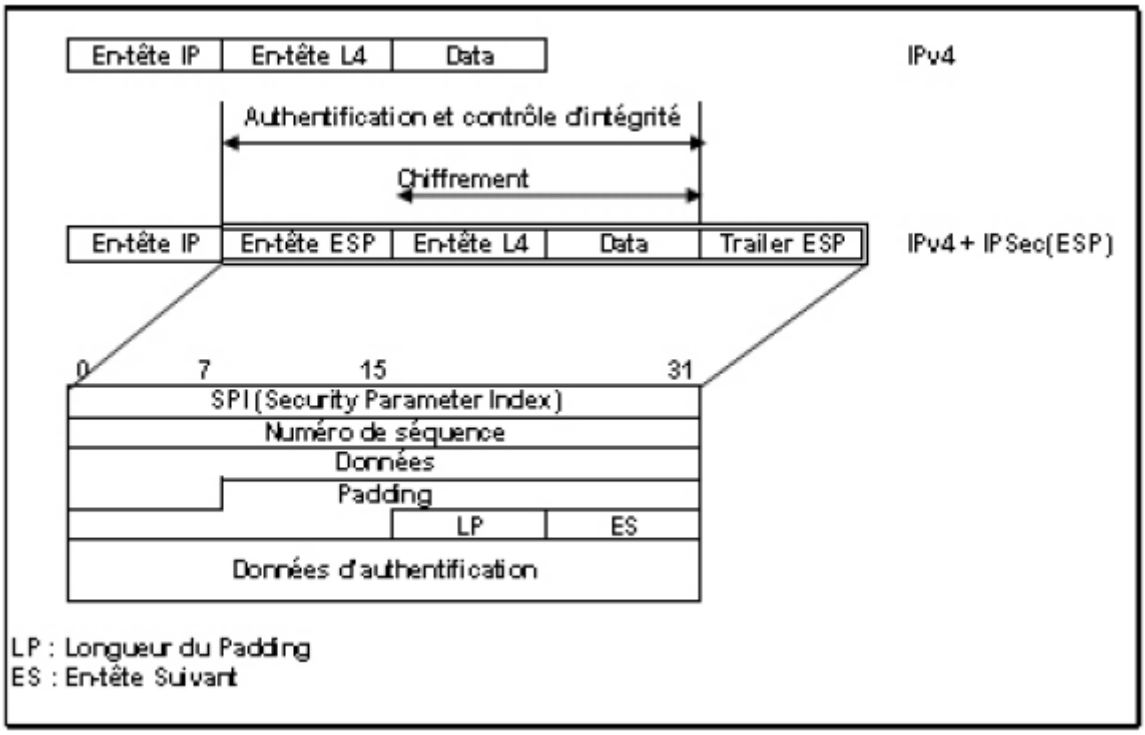


Figure II.10 : En-tête ESP

- AH et ESP

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

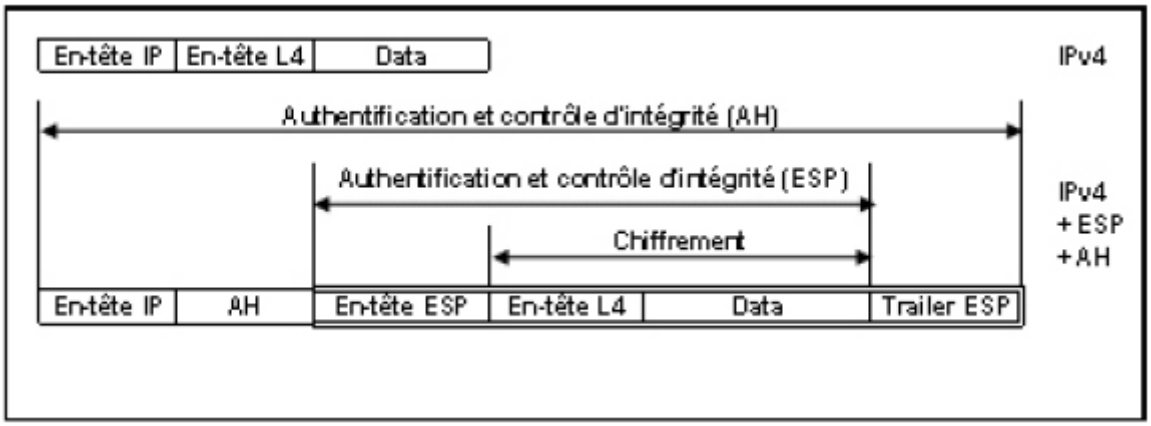


Figure II.11 : En-tête AH et ESP.

b. SA (Seturity Association) :

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

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

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

Les SA contiennent les éléments suivants :

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

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

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

Figure II. 12 : Exemple d'une base SA

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

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

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

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

Le protocole IKE utilise l'infrastructure du protocole ISAKMP pour échanger des clés et définir des SA entre deux machines. IKE utilise également le protocole Oakley pour la création des clés et le protocole SKEME pour les échanger. IKE permet donc de négocier automatiquement des SA. Il fonctionne sur UDP(via le port 500.

Les négociations IKE se font en deux phases :

- **phase I :** elle permet de mettre en place un canal sécurisé afin de protéger les négociations qui se déroulent lors de la deuxième phase.

- **Phase II** : elle permet de négocier les SA qui seront utilisées par IPSec pour protéger le trafic.

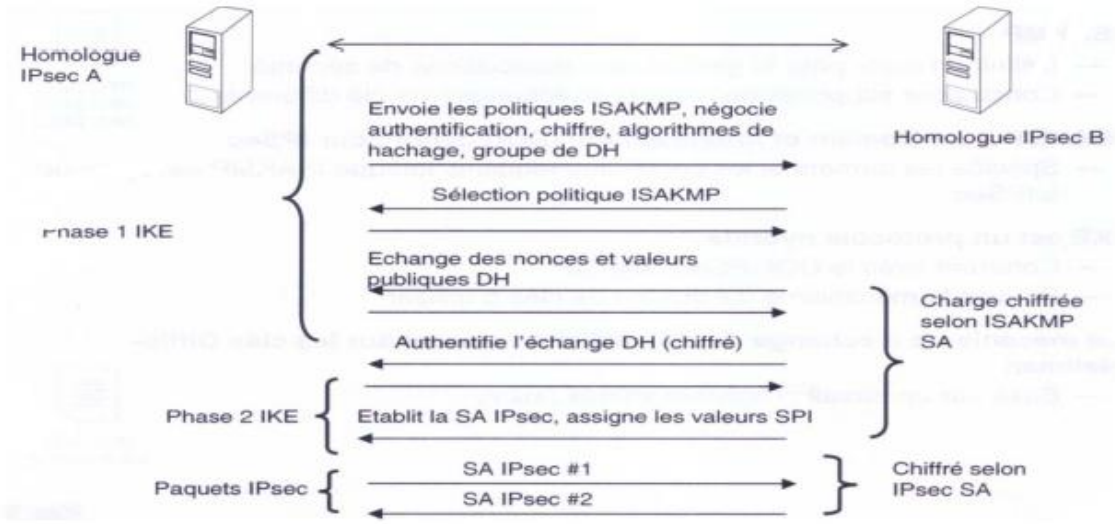


Figure II.12 : Echanges ISAKMP IKE.

- **IKE phase I :**

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

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

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

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

- **IKE phase II :**

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

II .8.Algorithmes utilisés par ipsec

Les algorithmes utilisés par IP sec sont :

II .8.1.Algorithmes symétrique

- ***L'algorithme DES :***

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

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

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

Les grandes lignes de l'algorithme sont :

- **Phase 1** : Préparation - Diversification de la clé :

1. Le texte est découpé en blocs de 64 bits.
2. On diversifie aussi la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés 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 de permutations.
- Phase 4 : Permutation finale :

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

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

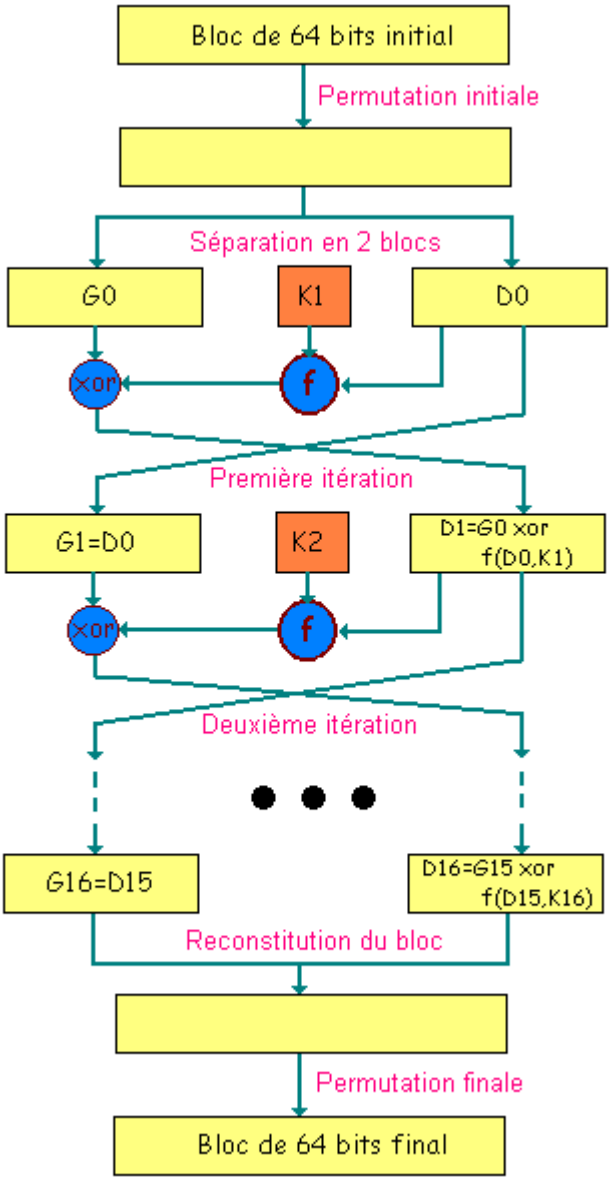


Figure II.13: Schéma de l'algorithme DES

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

Face à la faiblesse de l'algorithme DES, la solution a semblé être dans un premier temps l'adoption de l'algorithme surnommé triple DES, algorithme consistant en trois applications de l'algorithme DES à la suite les uns des autres avec 2 clés différentes (d'où une longueur de clé de 2*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.14: Schéma de l'algorithme Triple – DES – 112 bits

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

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

- ***L'algorithme AES :***

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

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

Les principaux inconvénients de chiffrement symétrique :

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

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

II .8 .2.Les algorithmes asymétriques

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

Le premier crypto-système asymétrique, RSA 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.

II .8.3.Les fonctions de hachages

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

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

- SHA-1 (Secure Hash Algorithm, Algorithme de Hachage Sécurisé version 1), comme MD5, est basé sur MD4. Il fonctionne également à partir de blocs de 512 bits de données et produit par contre des condensés de 160 bits en sortie.

- SHA-2 (Secure Hash Algorithm 2) a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits. Il sera bientôt la nouvelle référence en termes de fonction de hachage.

Conclusion

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

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

Chapitre III

Application

Chapitre III

Application

III.1 .Introduction

Ce chapitre est la dernière partie de mon travail, donc je vais m'intéresser à la mise en œuvre de mon application en établissant une interconnexion entre deux sites distants utilisant un VPN.

Durant ce chapitre je vais donner :

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

III.2. Présentation du réseau.

Je suppose un réseau contenant :

- 1Site central.

- 4 sites distants.

III.3. Topologie du réseau :

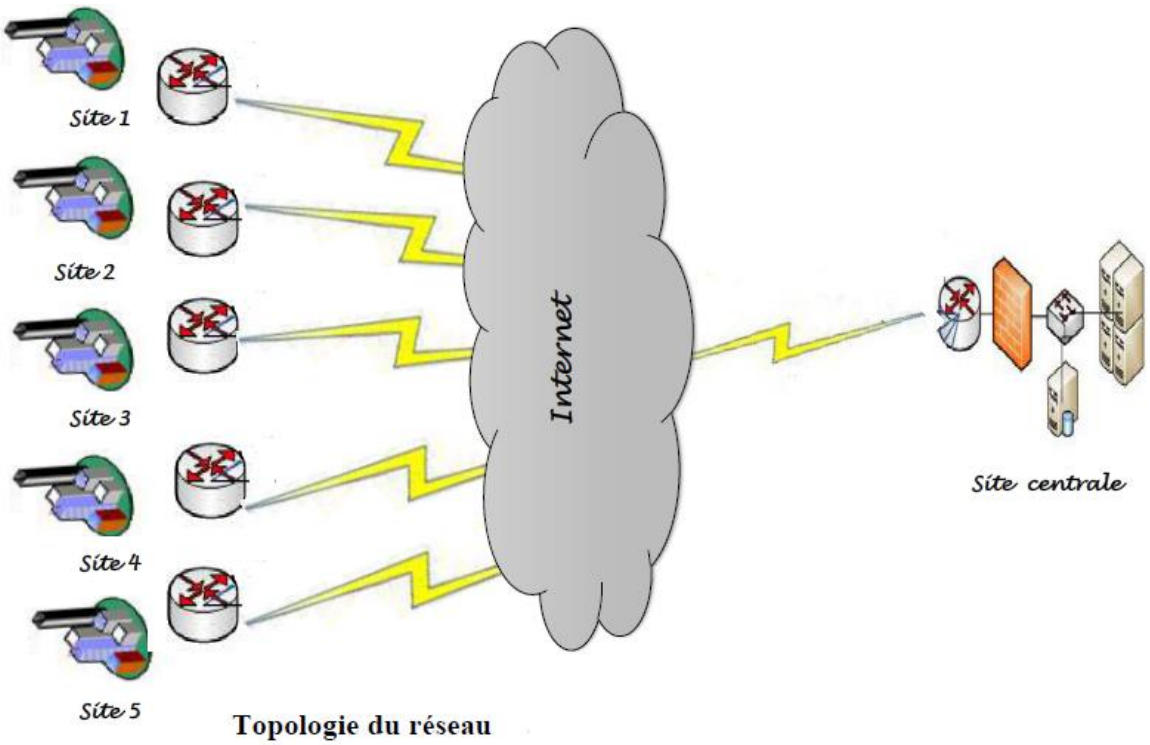


Figure III.1: Topologie du réseau

III.4.Établissement du cahier de charge :

Création d'un accès distant sécurisé basé sur les VPNs :

• Réalisation des VPNs site à site entre le site centrale et les différentes agences afin de sécuriser l'interconnexion entre eux.

III.5. Outils utilisés pour la réalisation du projet :

- **Emulateur GNS3 (Graphical Network Simulator)**

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

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

III.6.Topologie pour la Simulation d'une liaison VPN site-à-site :

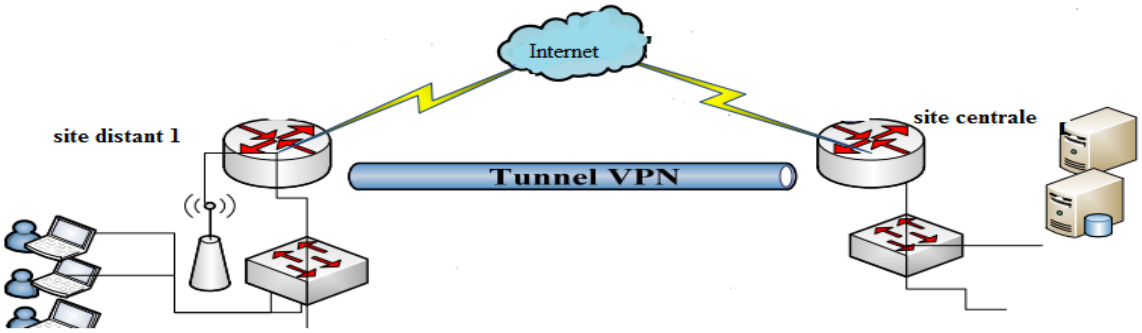


Figure III.2. : Topologie du réseau entre deux sites distants

III.5. Table d'adressage

Équipements	Interface	Adresse ip	Masque sous réseau	Passerelle par défaut	Area
R1	loopback 0	1.1.1.1	255.255.255.255	N /A	0
	f0/0	200.1.1.1	255.255.255.0	N /A	0
	f0/1	200.2.2.1	255.255.255.0	N /A	0
R2	loopback 0	1.1.1.2	255.255.255.255	N /A	0
	f0/0	200.1.1.2	255.255.255.0	N /A	0
	f0/1	10.1.1.2	255.255.255.0	N /A	1
R3	loopback 0	1.1.1.3	255.255.255.255	N /A	0
	f0/0	200.2.2.3	255.255.255.0	N /A	0
	f0/1	10.2.2.3	255.255.255.0	N /A	2
R4	Loopback 0	1.1.1.4	255.255.255.255	N /A	1
	f0/0	10.1.1.4	255.255.255.0	N /A	1
R5	loopback 0	1.1.1.5	255.255.255.255	N /A	2
	f0/0	10.2.2.5	255.255.255.0	N /A	2

Tab. III.1 : Table d'adressage

D'où j'aurai la topologie suivante :

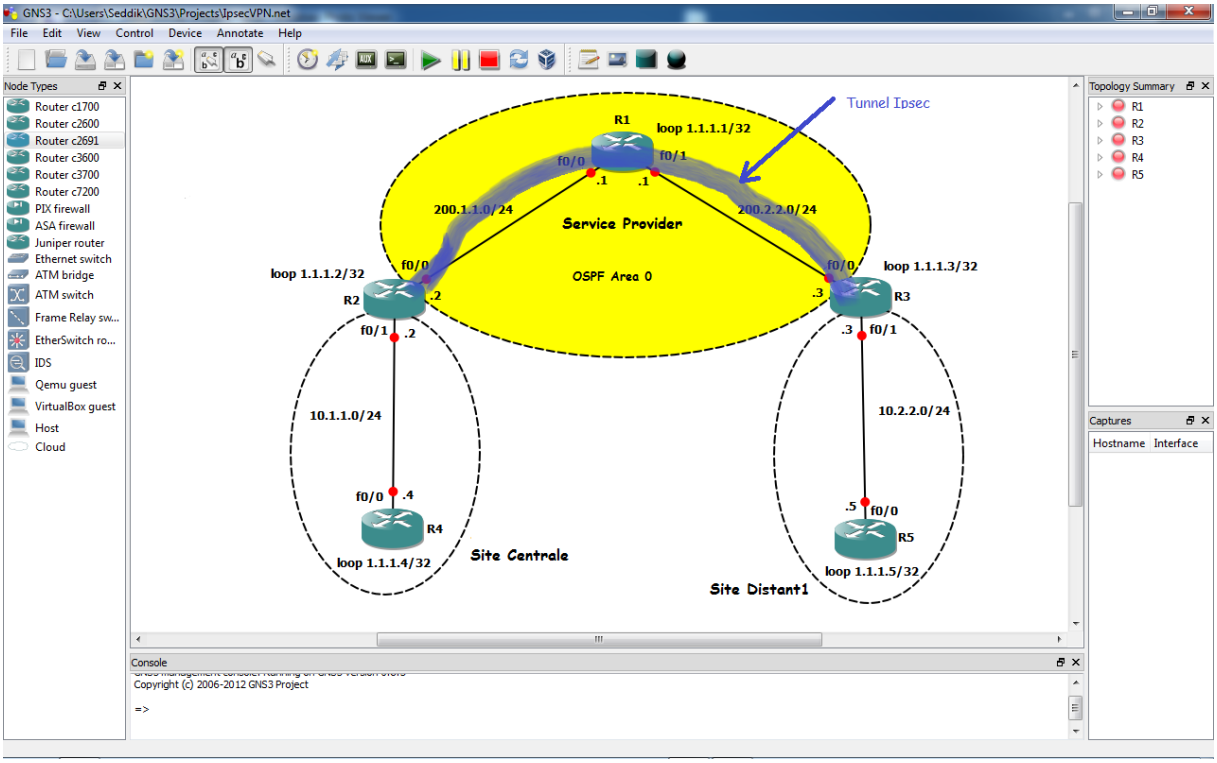


Figure III.3 : Architecture de mon réseau.

III. 8. 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.

III.8.1. Test de connexion et de routage :

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

- **R1 :**

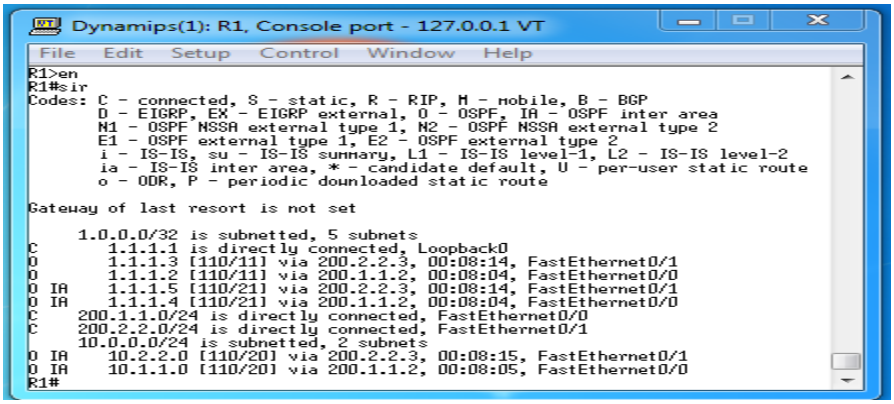


Figure III .4 : Résultats de la commande sir pour R1

- **R2**

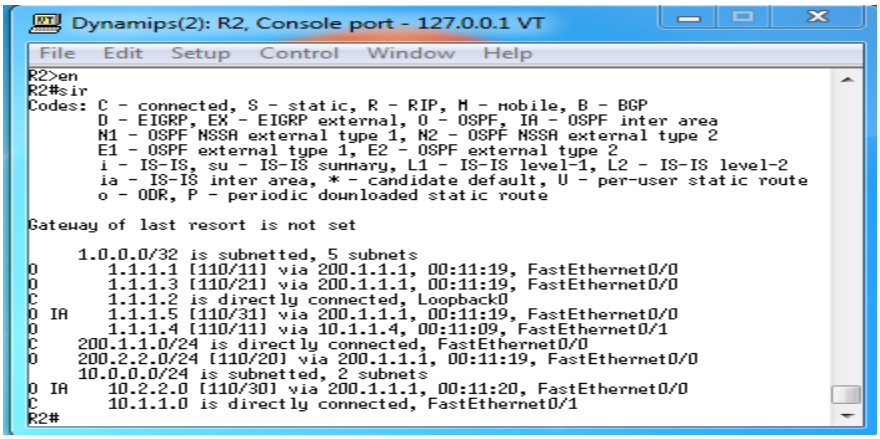


Figure III.5 : Résultats de la commande sir pour R2

- **R3**

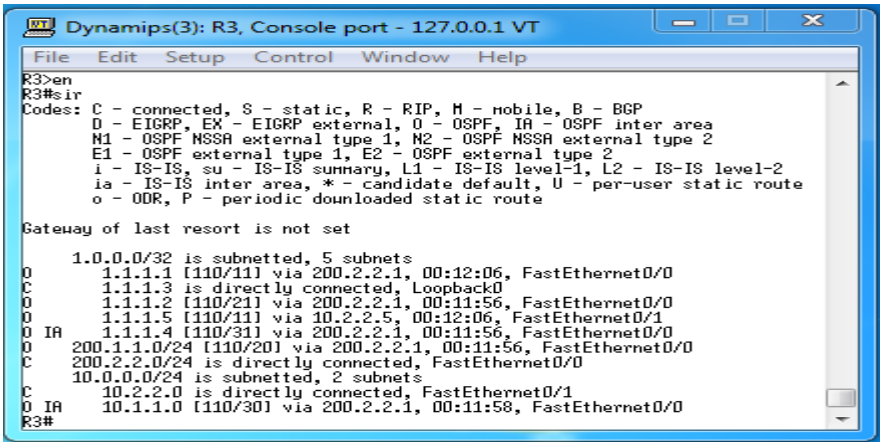


Figure III.6 : Résultats de la commande sir pour R3

- **R4**

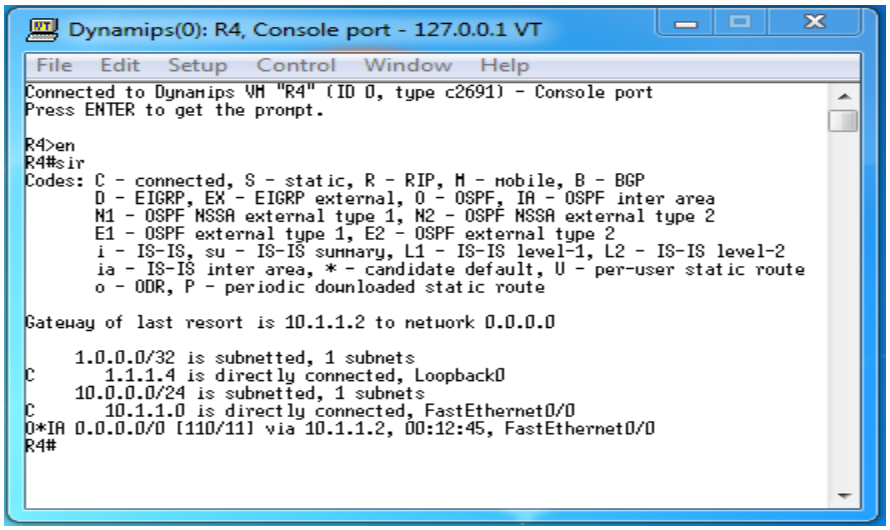


Figure III.7 : Résultats de la commande sir pour R4

- **R5**

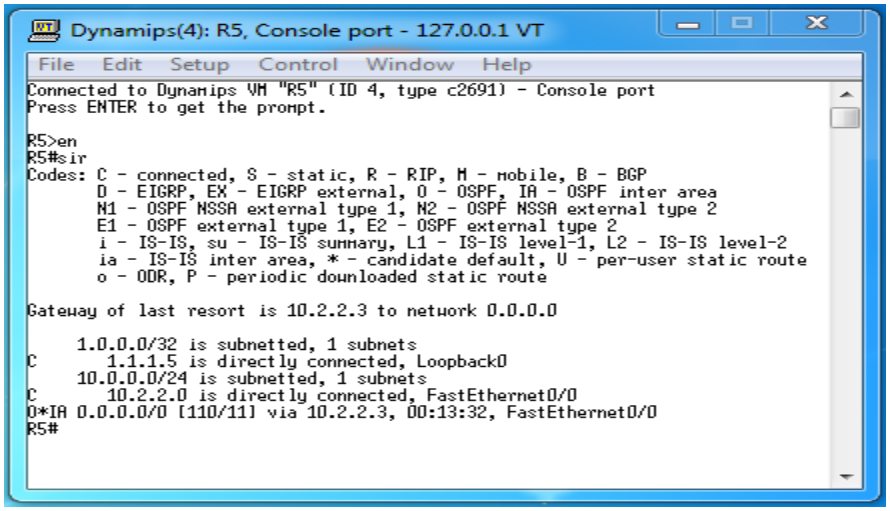


Figure III.8 : Résultats de la commande sir pour R5

III.9. Configuration de VPN site to site :

III.9.1. Etablissement d'un tunnel Ipsec site-à-site

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

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

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

Définir les paramètres du tunnel IKE (Policy ISAKMP)

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

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

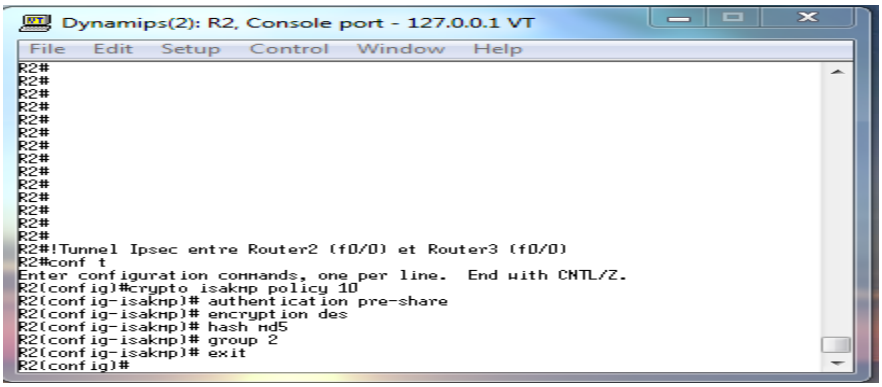


Figure III. 9 : Configuration Policy ISAKMP pour le site central.

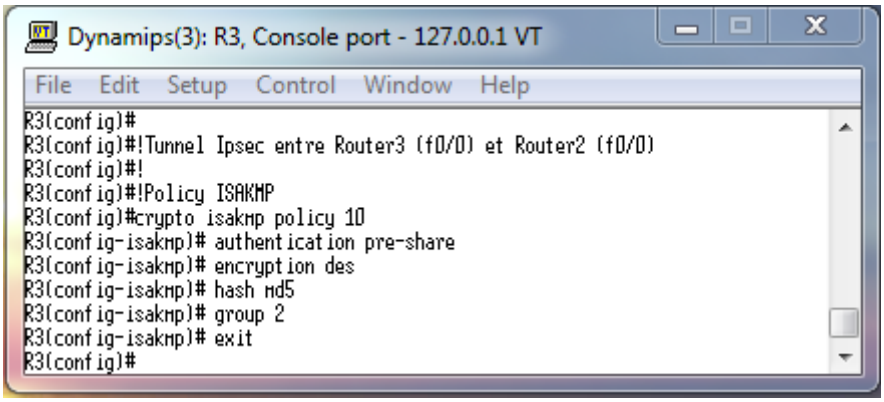


Figure III.10. Configuration Policy ISAKMP pour le site distant 1

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

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

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

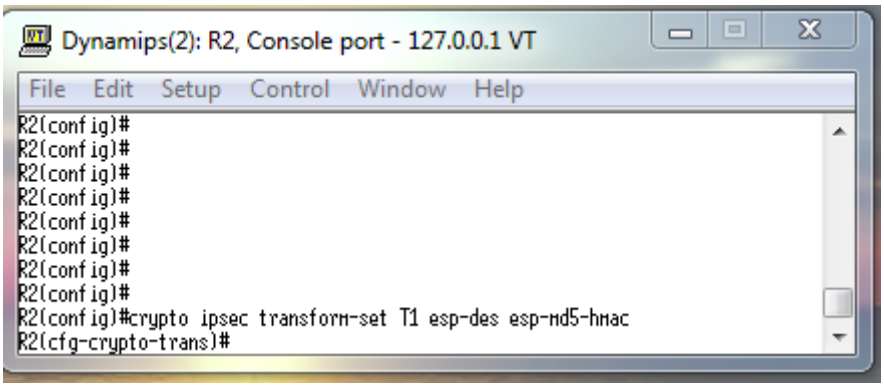


Figure III.11. Configuration des paramètres du tunnel ipsec pour le site central 'R2'

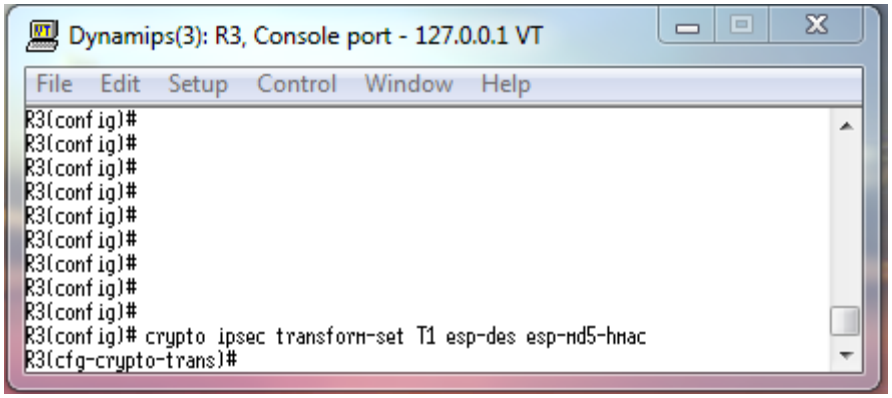


Figure III.12 Configuration des paramètres du tunnel ipsec pour le site distant 1 'R3'

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

Etape 3 : Configuration Pre-shared key avec le peer

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

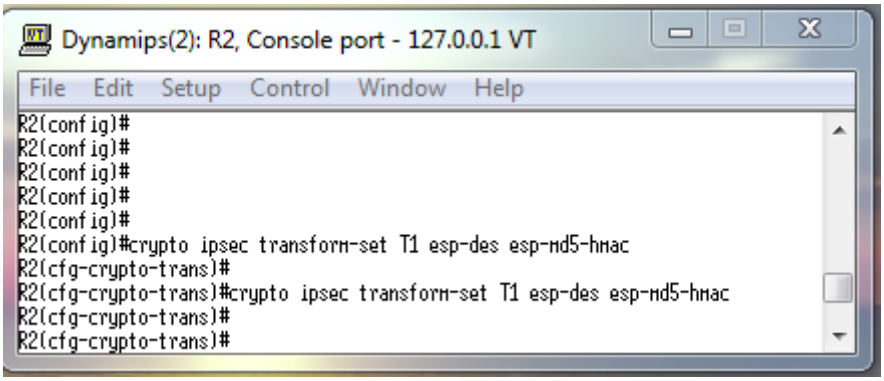


Figure III.13. Configuration du tunnel ipsec pour le site centrale

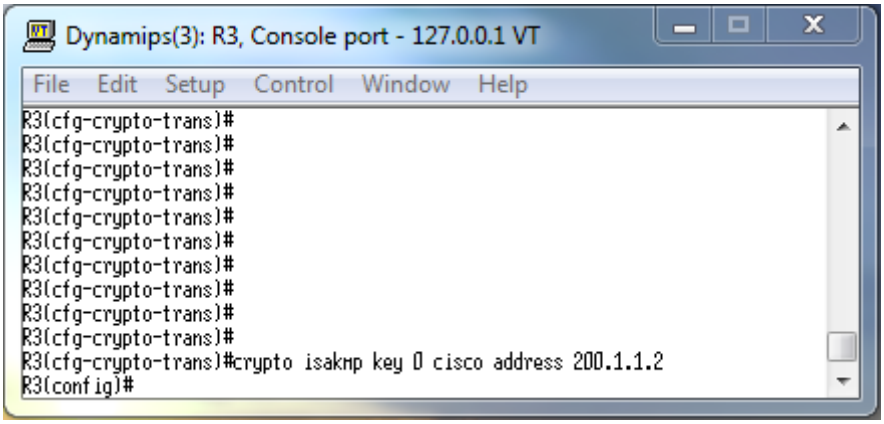


Figure III.14 : Configuration du tunnel ipsec pour le site disant 1

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

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

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

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

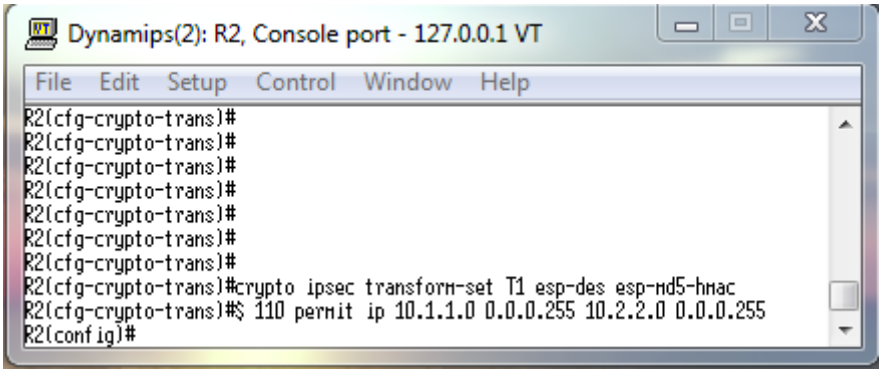


Figure III.15. Configuration des listes de contrôle pour le site central

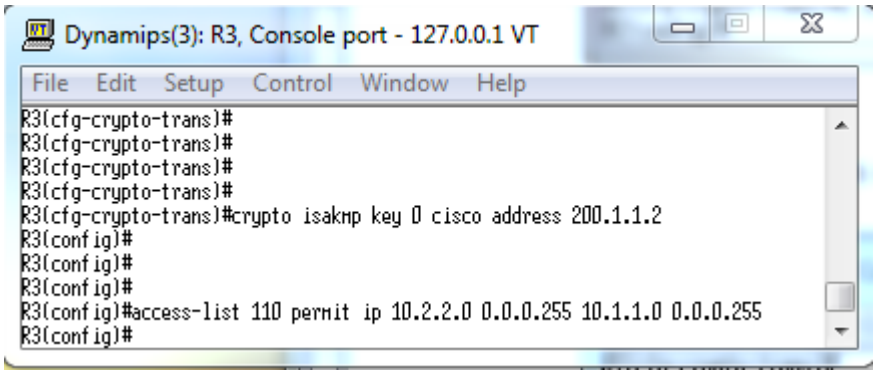


Figure III.16. Configuration des listes de contrôle pour le site distant 1

- **Etape 5 : Définir la crypto map**

Création d'une crypto map pour regrouper les paramètres précédant

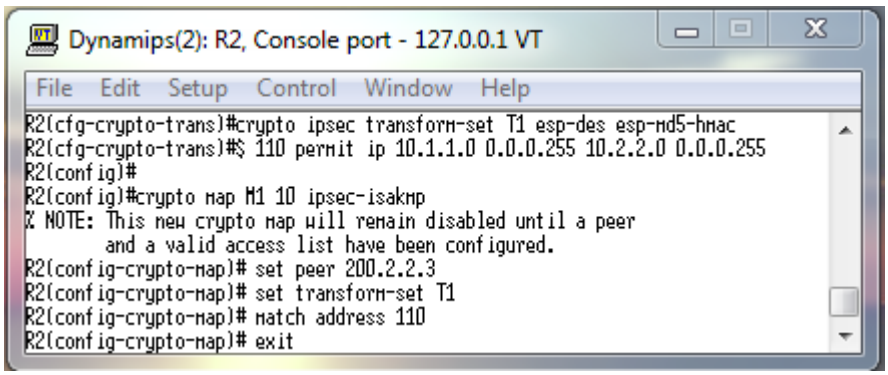


Figure III.17 : Configuration de la crypto map pour le site central

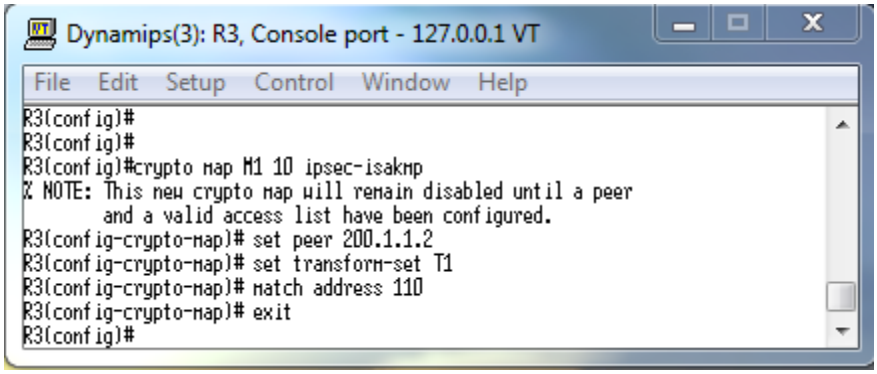


Figure III .18. Configuration de la crypto map pour le site distant 1

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

- Activée pour le trafic correspondant à l'access-list VPN
- Destination du tunnel 200.1.1.2
- Cryptage selon le transform-set M1

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

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

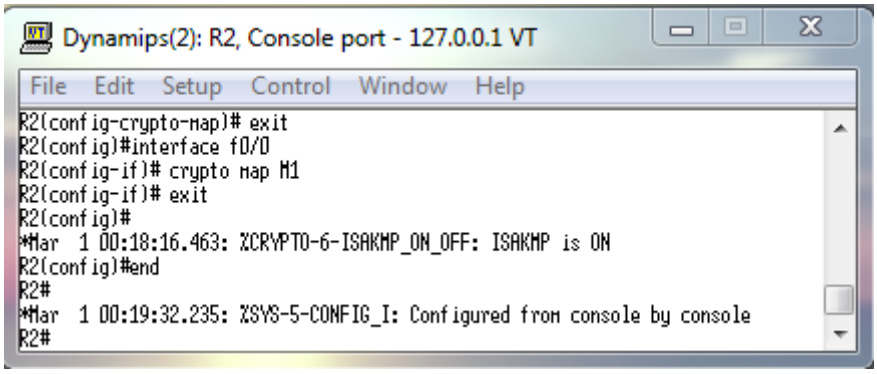


Figure III.19. Application de la crypto map à l'interface pour le site central

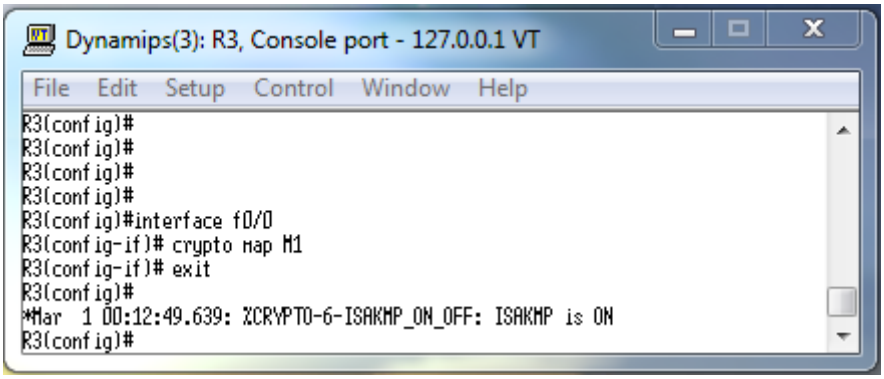


Figure III .20. Application de la crypto map à l'interface pour le site distant 1

- **Générer le trafic intéressant**

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

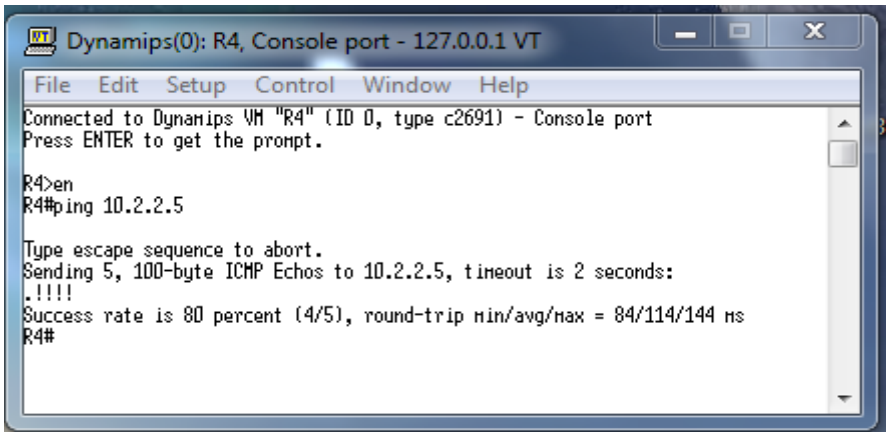


Figure III.21.Résultat du : ping 10.2.2.5

Le message observé sur R2 :

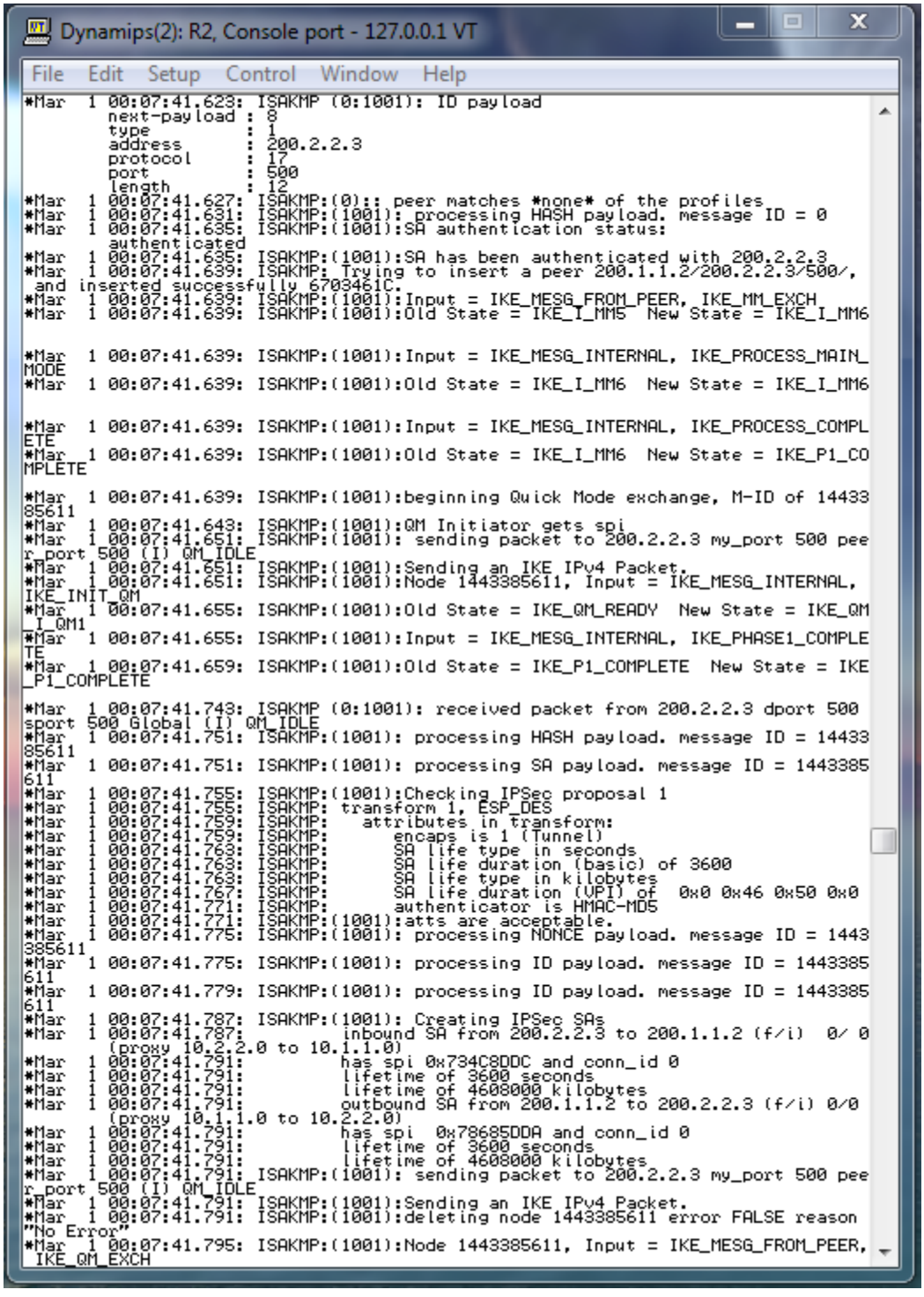


Figure III.22.Résultat su Ping 10.2.2.5 sur R2

III.10. Vérification :

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

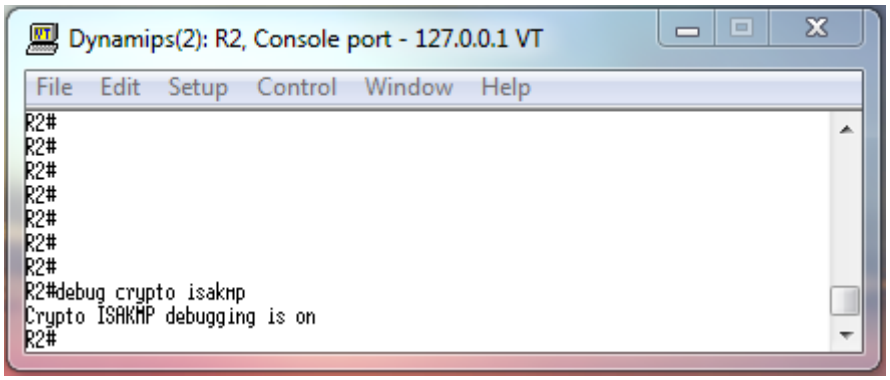


Figure III.23. Résultat de la commande « debug crypto isakmp » sur R2

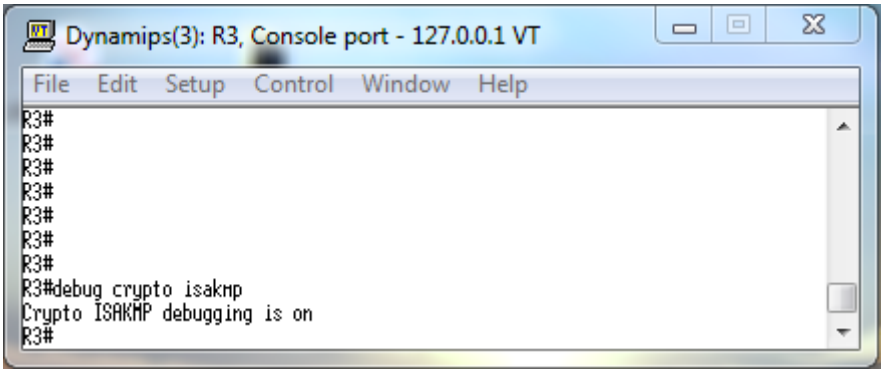


Figure III.24.Résultat de la commande « debug crypto isakmp » sur R3

- voir le status du tunnel Ipsec

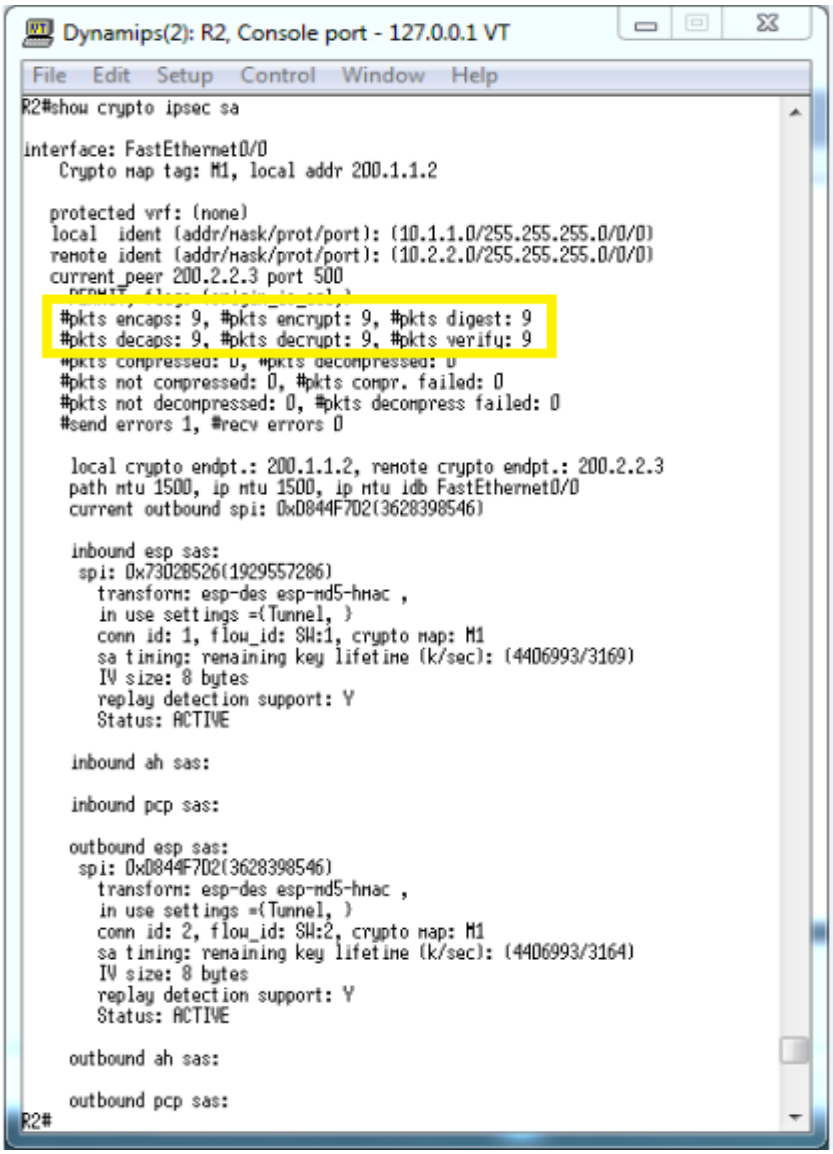


Figure III. 25. Résultat de la commande sur R2 « show crypto ipsec sa »

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

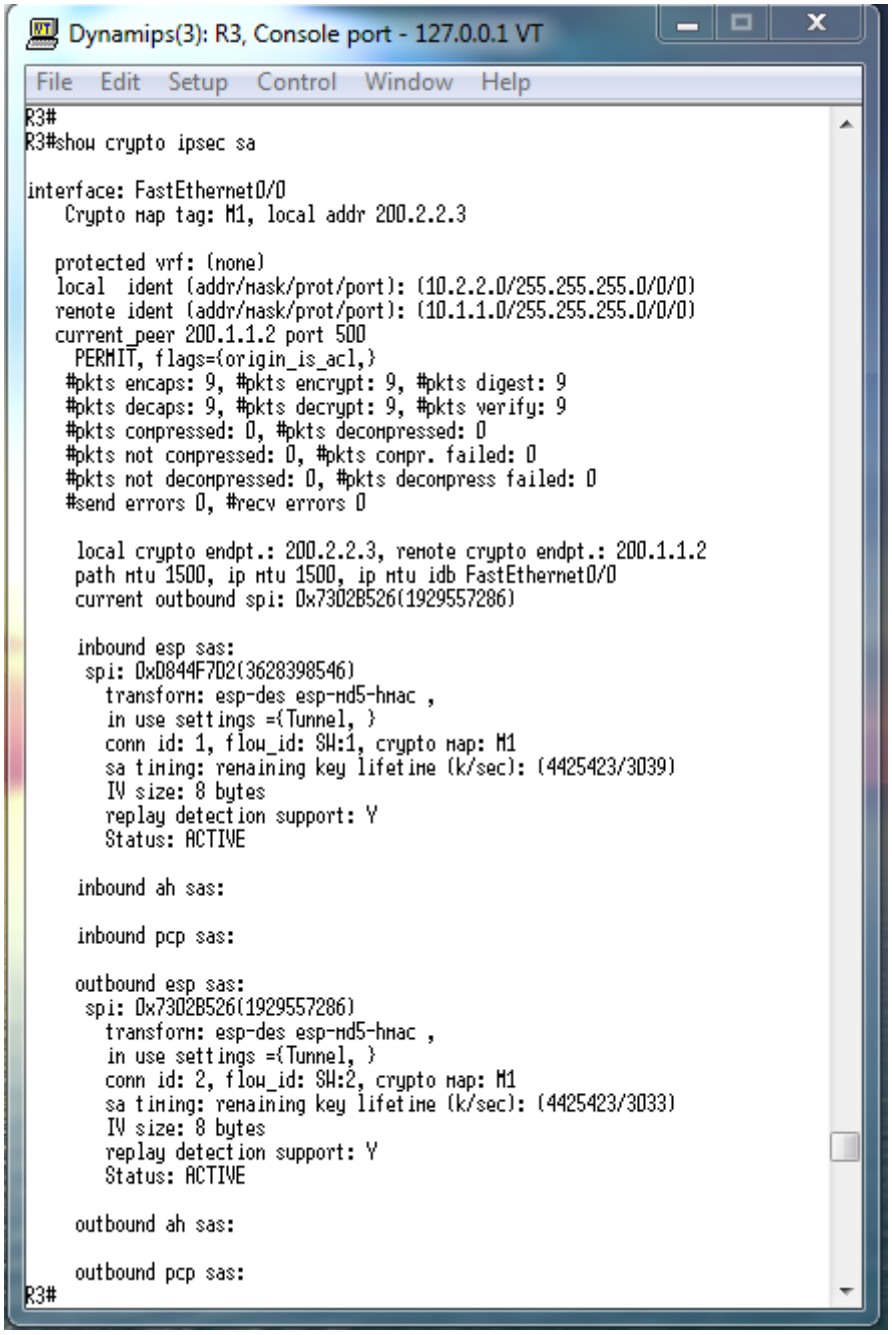


Figure III .26.Résultat de la commande sur R3 « show crypto ipsec sa »

III.11.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.

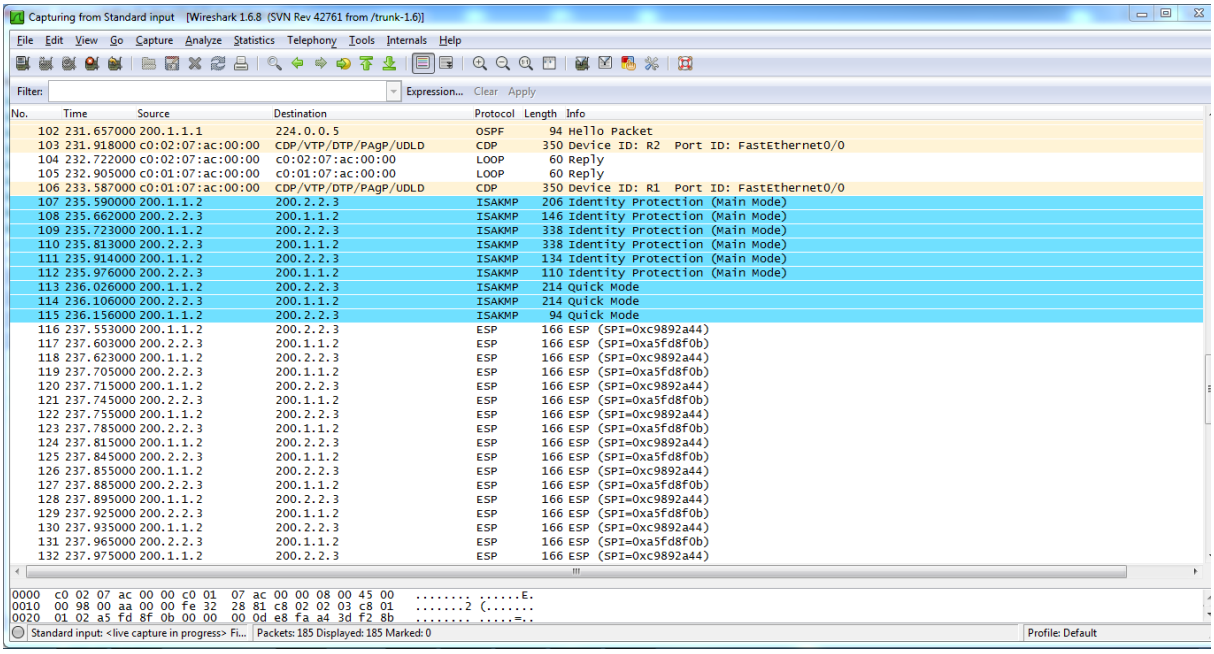


Figure III .27. Résultat de l'analyse avec Wireshark.

Conclusion

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

Conclusion générale

A travers ce projet de fin d'étude, nous avons vu ensemble un aperçu des différentes possibilités afin de déployer un VPN, et particulièrement la solution que représente IPSec. J'ai en effet 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 au travers internet. Cette solution mise en place est une politique de réduction des couts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basé sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

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

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

Les Livers:

- IPSec, édition 2003 CampusPress.
- Les VPN sous Linux, édition 2003 CampusPress.
- Misc n°10 novembre decembre 2003.
- linux Magazine n°31 septembre 2001
- Les réseaux d'entreprises par la pratique, Luc Montagnier.
- Cours réseaux et télécoms, G.Pujolle.

Les sites Internet:

- www.guill.net
- www.zdnet.fr
- www.cisco.fr
- www.01net.com
- solutions.journaldunet.com
- www.francetelecom.com
- www.easynet.fr
- www.urec.cnrs.fr
- www.Supinfo-Projects.com
- www.securiteinfo.com
- www.commentcamarche.com
- www.editions-eyrolles.com/les réseau édition 2008
- www.frameip.com/vpn/.
- www.frameip.com/ipsec.
- www.securiteinfo.com

Vidéo

CBT NUGGETS CONCEPTS OF VPN TECHNOLOGY Video Training.

CBT NUGGETS UNDERSTANDING MPLS VPN Video Training.

CBT NUGGETS CONCEPTS OF VPN TECHNOLOGY Video Training.

CBT NUGGETS VPN CONCEPTS S Video Training.

CBT NUGGETS VPN SITE-TO-SITE CLI CONFIGURATION Video Training.

CBT NUGGETS VPN SITE-TO-SITE SDM CONFIGURATION Video Training.

CBT NUGGETS UNDRESTANDING VPN ARCHITECTURE Video Training.

CBT NUGGETS UNDRESTANDING VPN COMPONENTS-IPSEC AND ENCRYPTION Video raining.

Glossaire

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

ATM : Asynchronous Transfer Mod

UDP : User Datagram Protocol

RSA : Revenu de Solidarité Active

AES :Advanced Encryption Standard

TCP :Transmission Control Protocol

MAC : Media Access Control

SMTP :Simple Mail Transfer Protocol

CHAP :Challenge Handshake Authentication Protocol

MPLS :MultiProtocol Label Switching

PTP :Precision Time Protocol

DMZ: Demilitarized Zone

QM :Quick Mode

http : L'HyperText Transfer Protocol

FTP : File Transfer Protocol

DNS :Domain Name System

SSH : Secure Shell

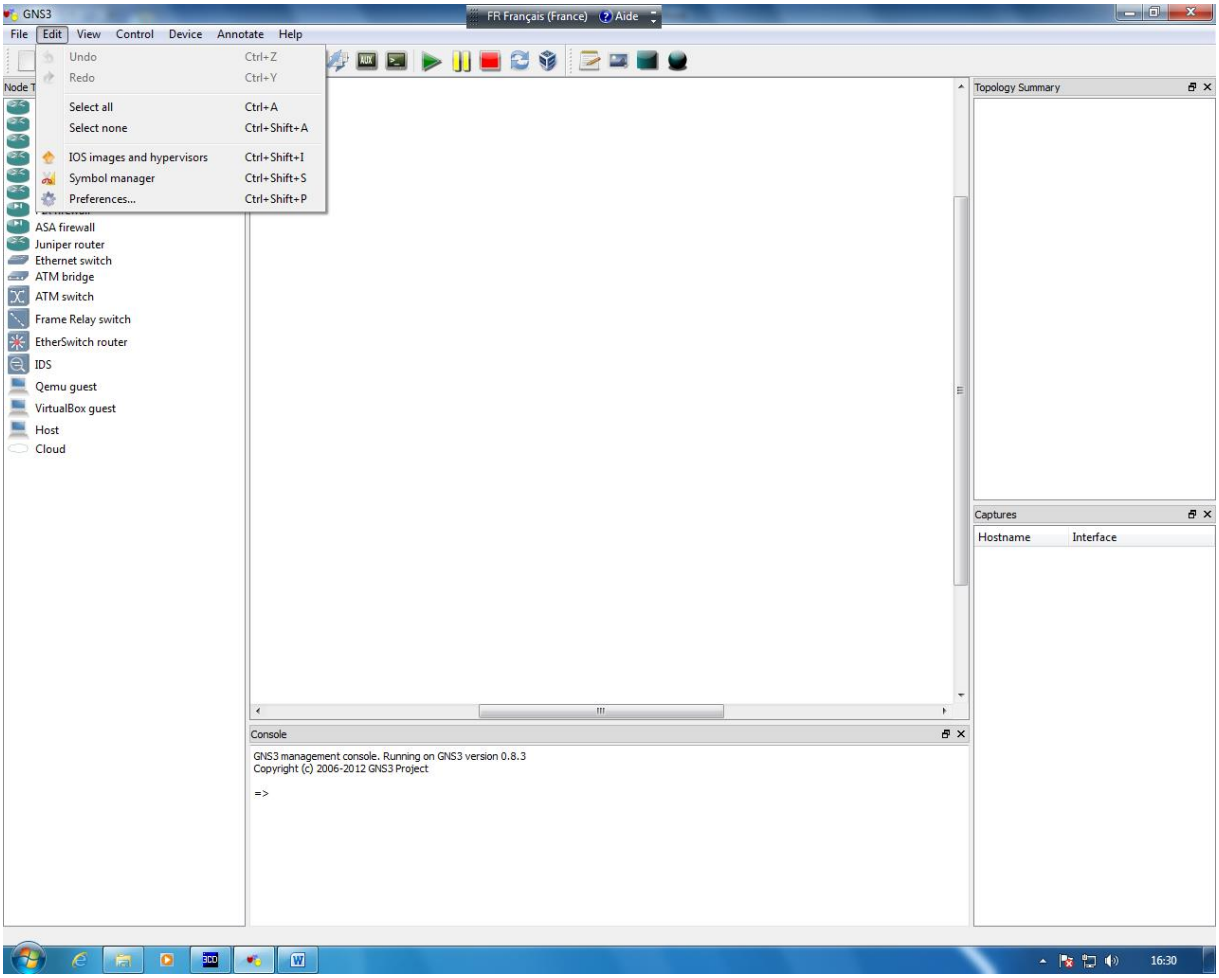
Annexe

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.

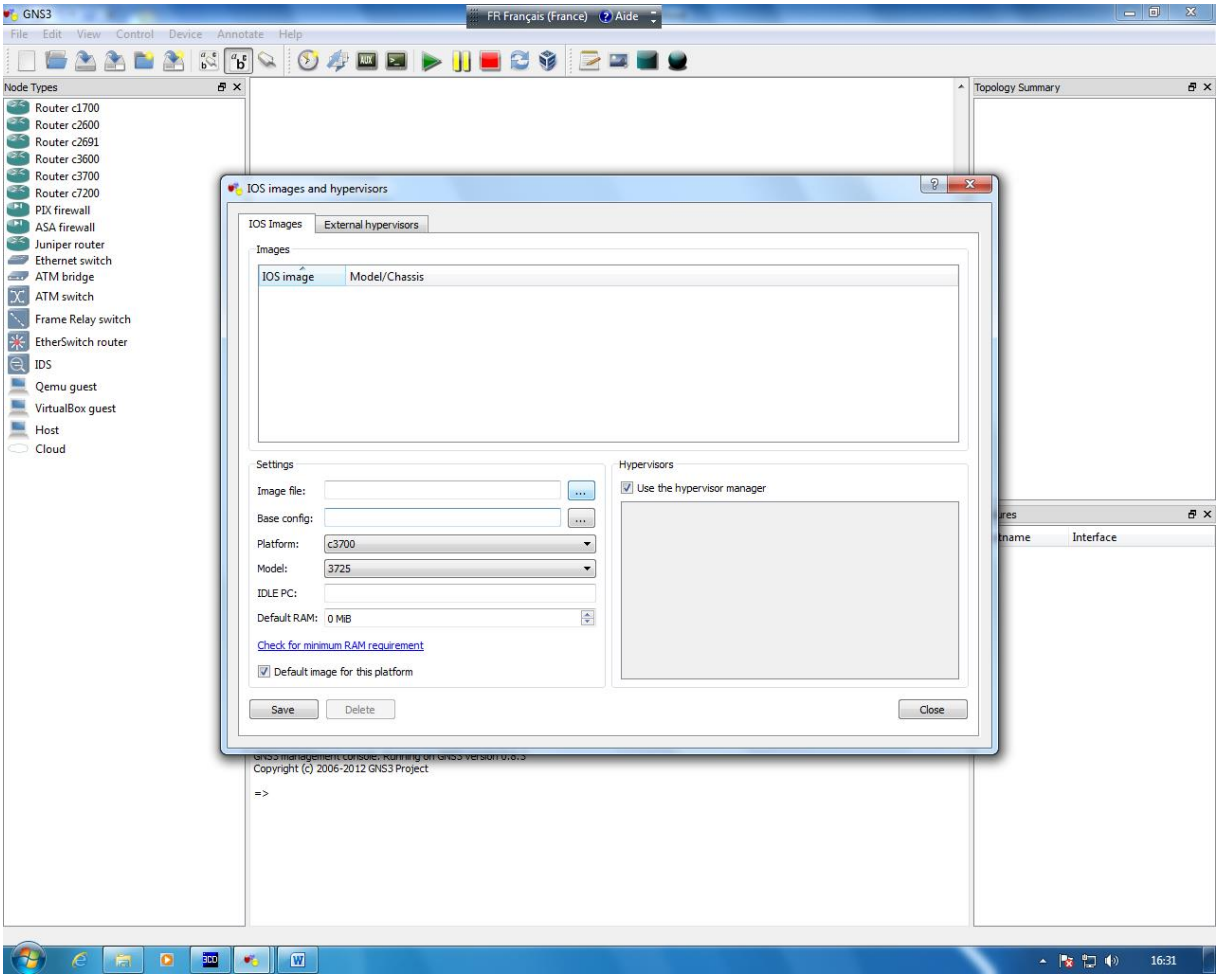
1 - Installer l'application GNS3 et la lancer
2 – configurer l'URL de l'IOS

Edit >> IOS image and Hypervisor

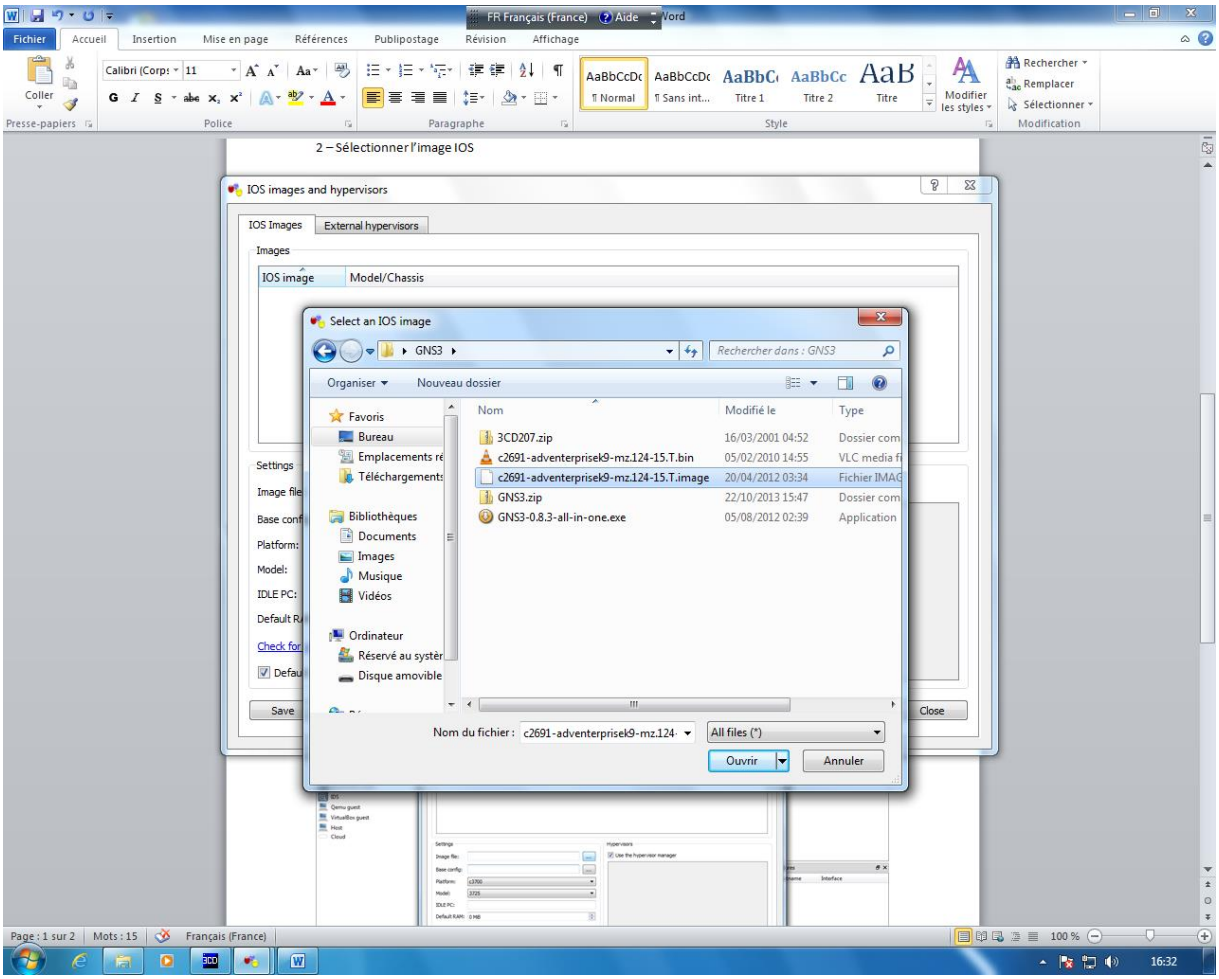


3 – Sélectionner l'image IOS

Cliquer sur le bouton face à "Image file:"

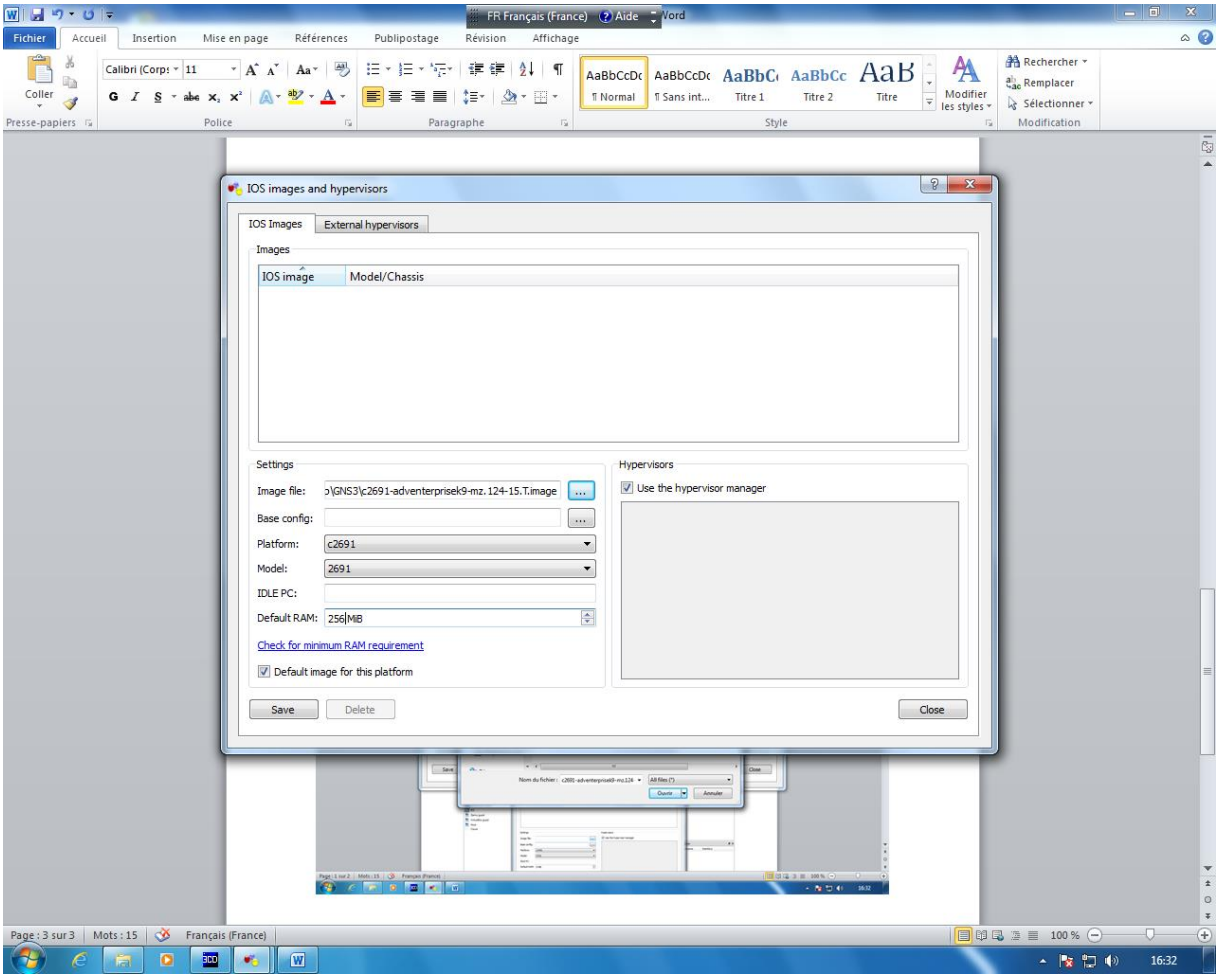


4 – Sélectionner l'IOS (décompressé) et cliquer sur bouton <<Ouvrir>>



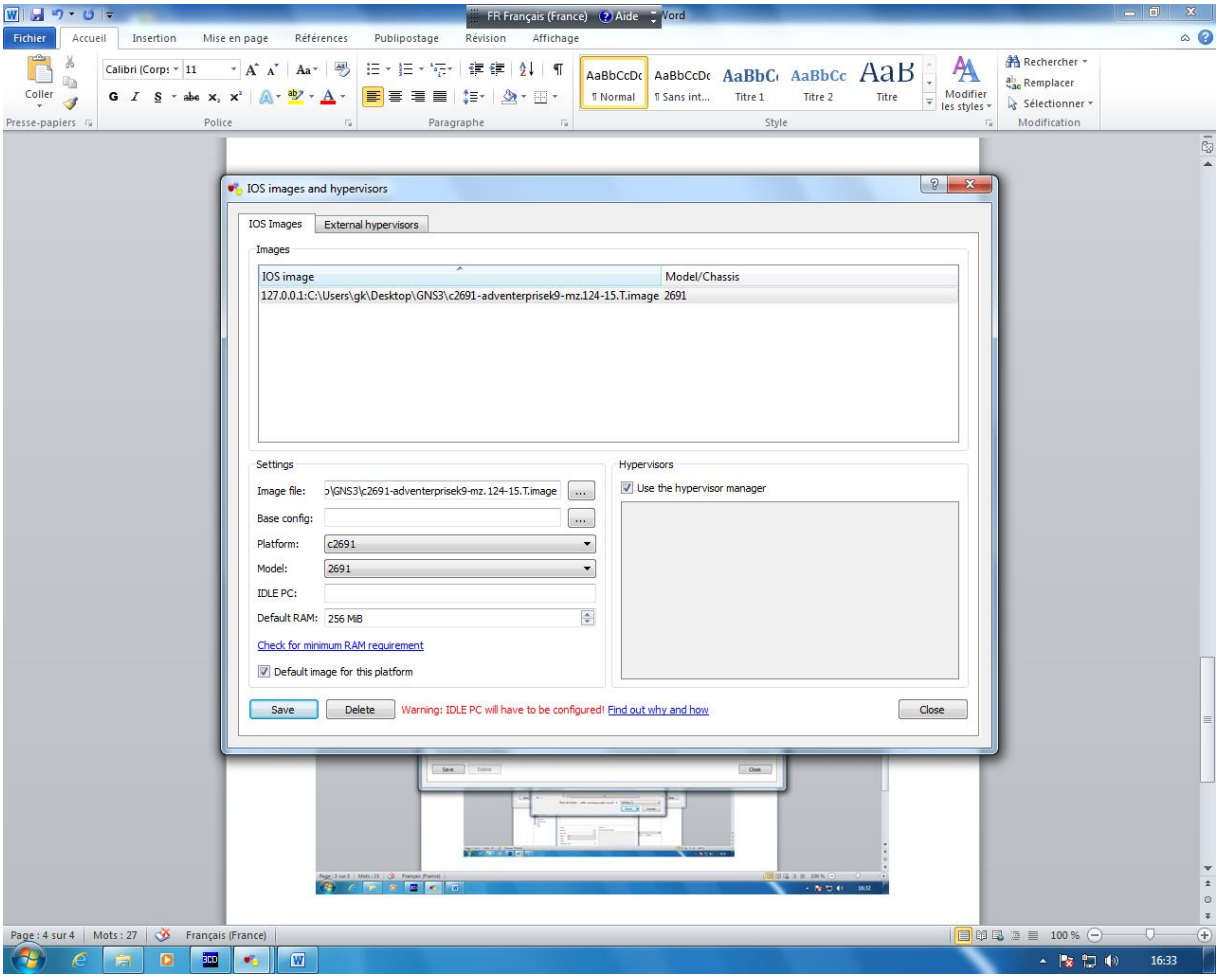
5 – Modifier la capacité mémoire des routeurs émulés de 128 ==> 256 MB

Modifier le contenu des champs <<Default RAM>>

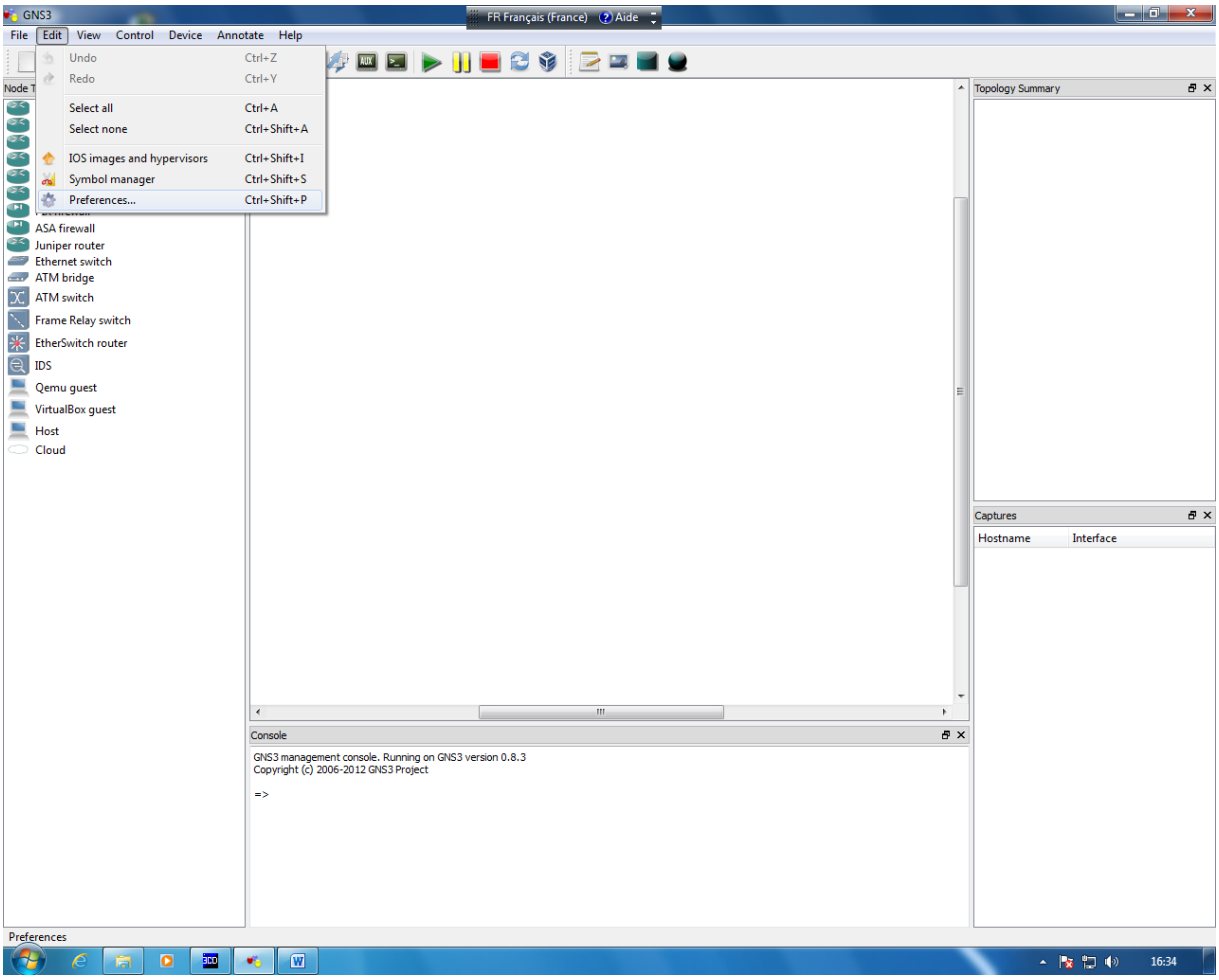


6 – Cliquer <<Save>> et <<Close>>

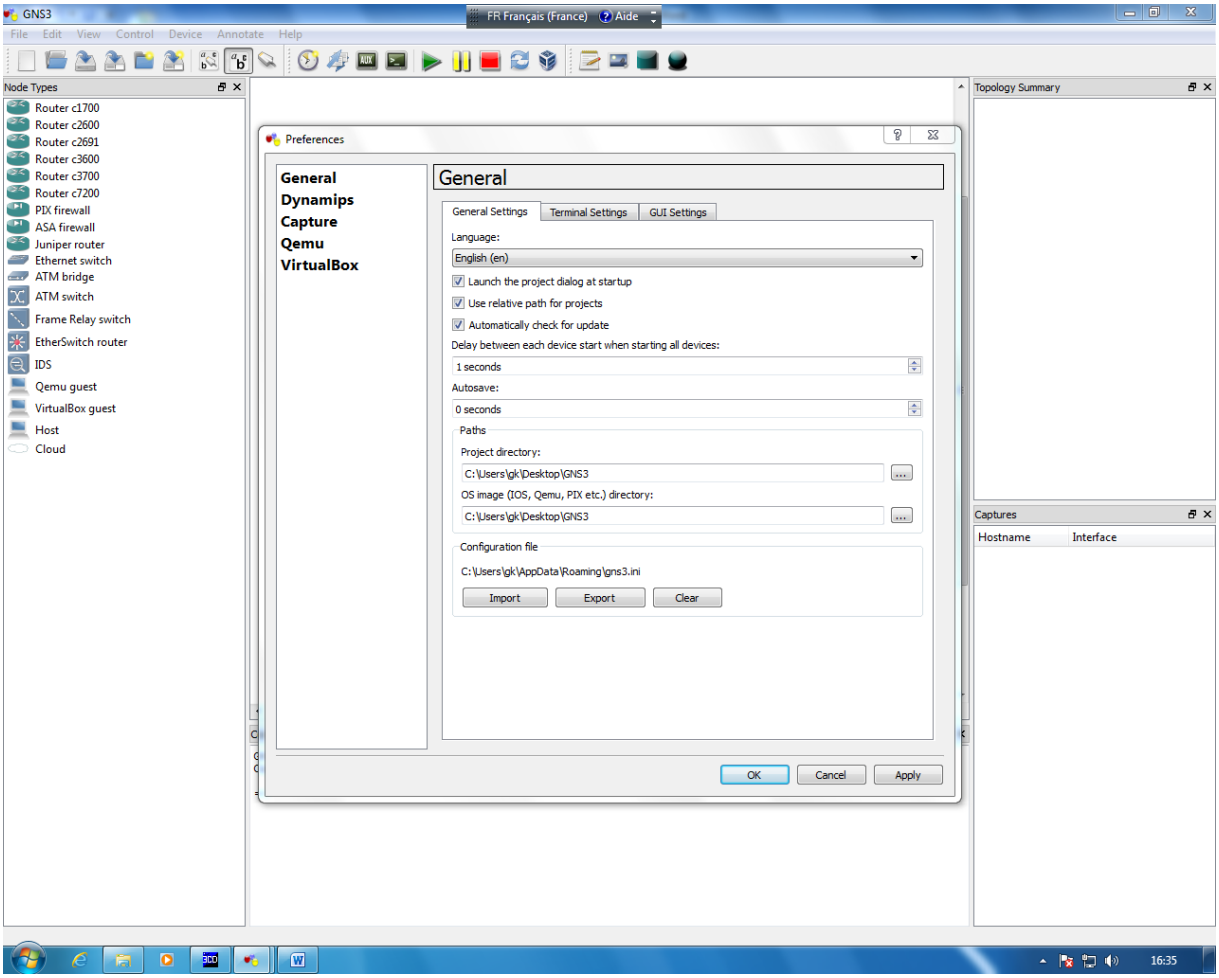
Ignorer le message en rouge "Warning Idle PC ...."



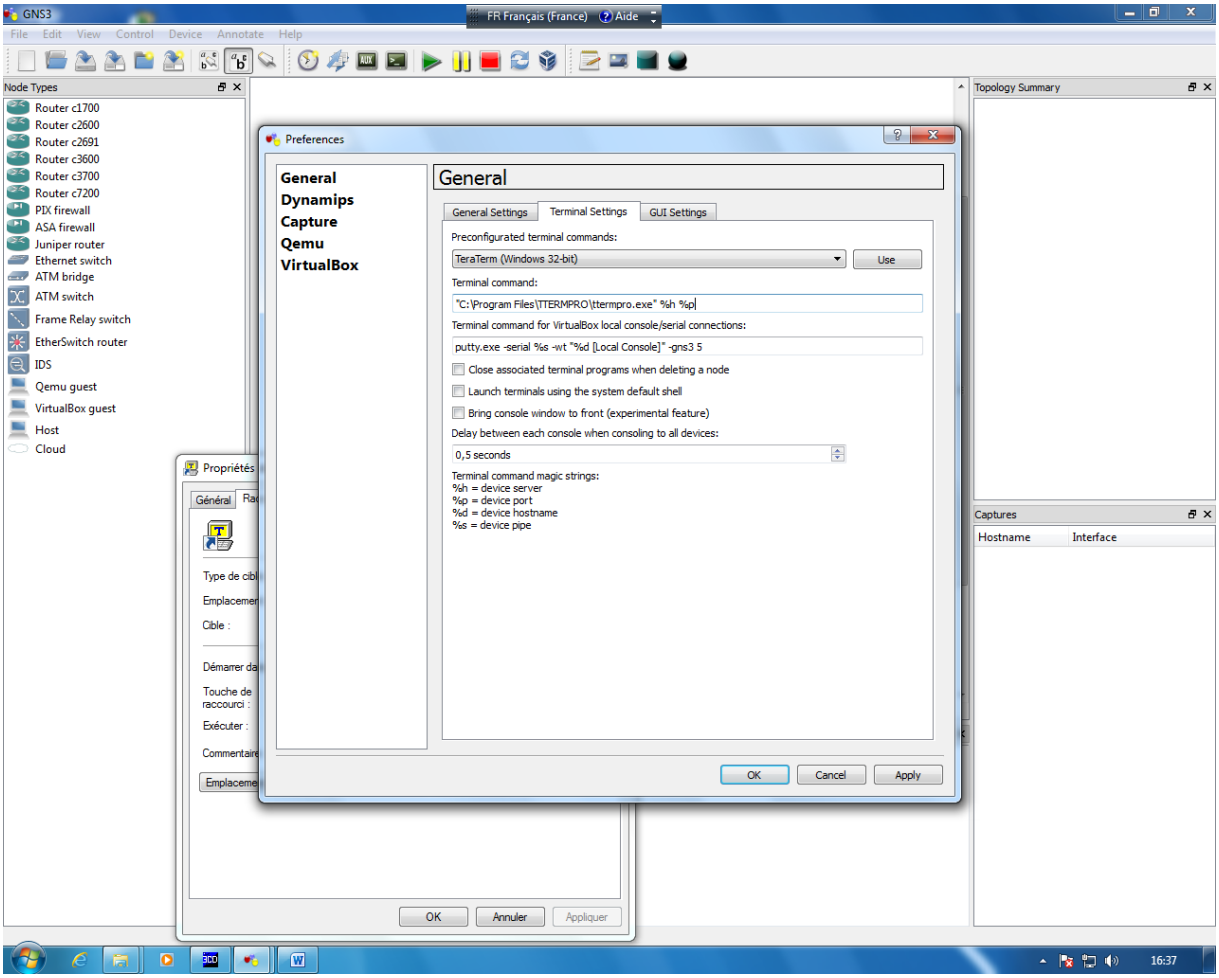
Edit >> Préférence



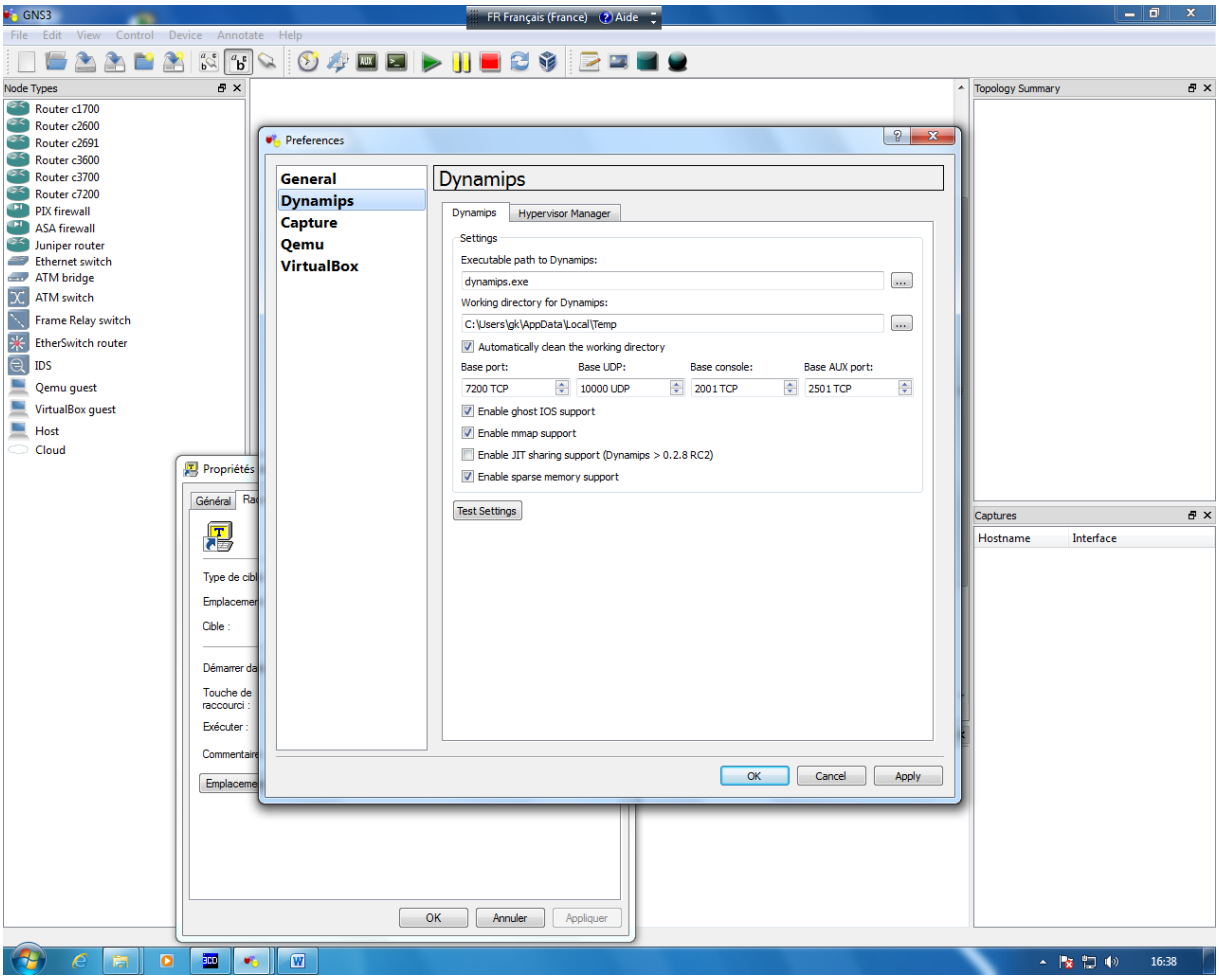
7 – Modifier le répertoire par défaut et sélectionner le répertoire GNS3 créé sur le desktop.



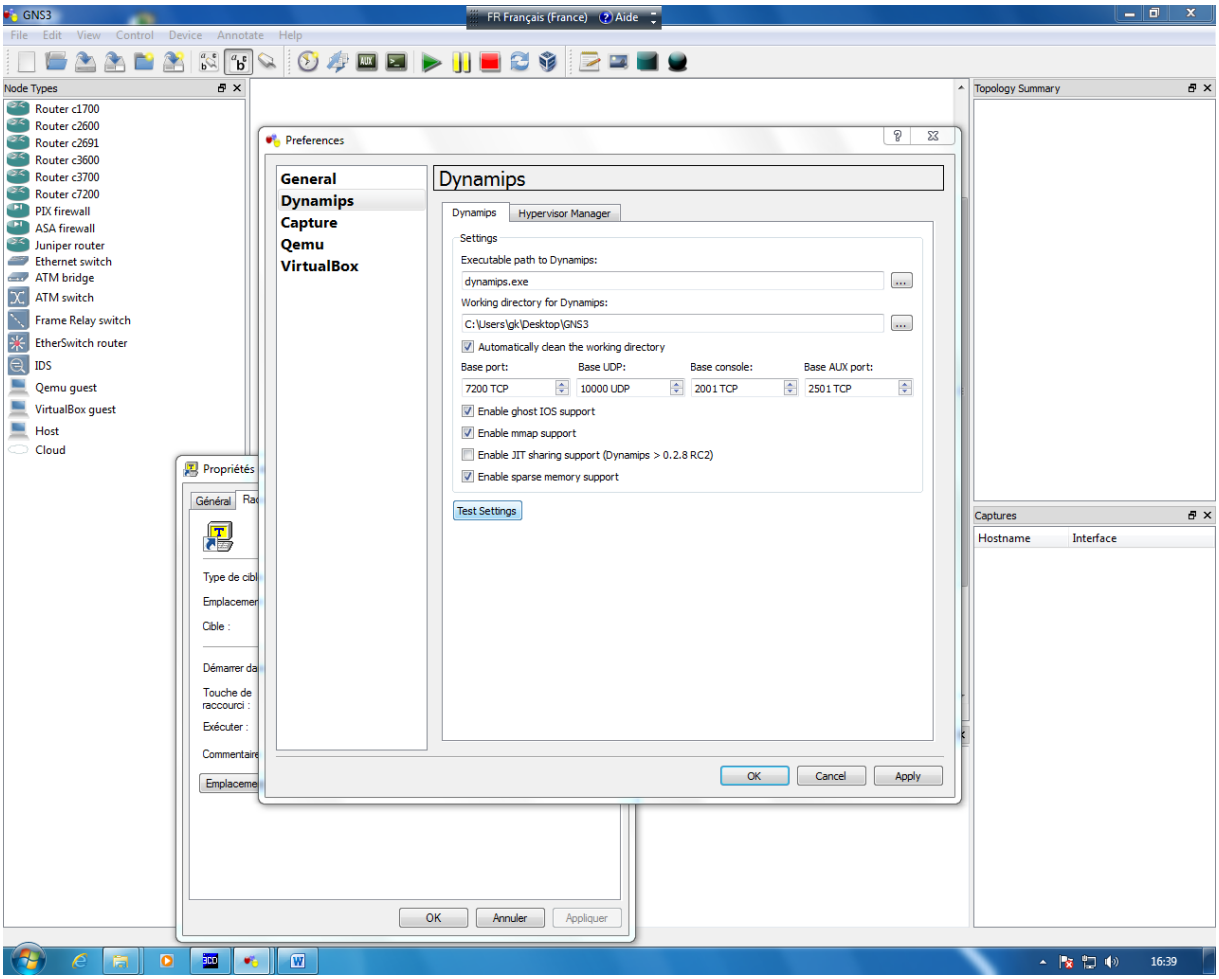
8 – Si nécessaire sélectionner Teraterm (Windows 32) à la place de Putty par défaut
Sous Terminal command : copier l'URL de l'application Teraterm et ne laisser que les options %h %p



Cliquer sur le bouton <Dynamips>>



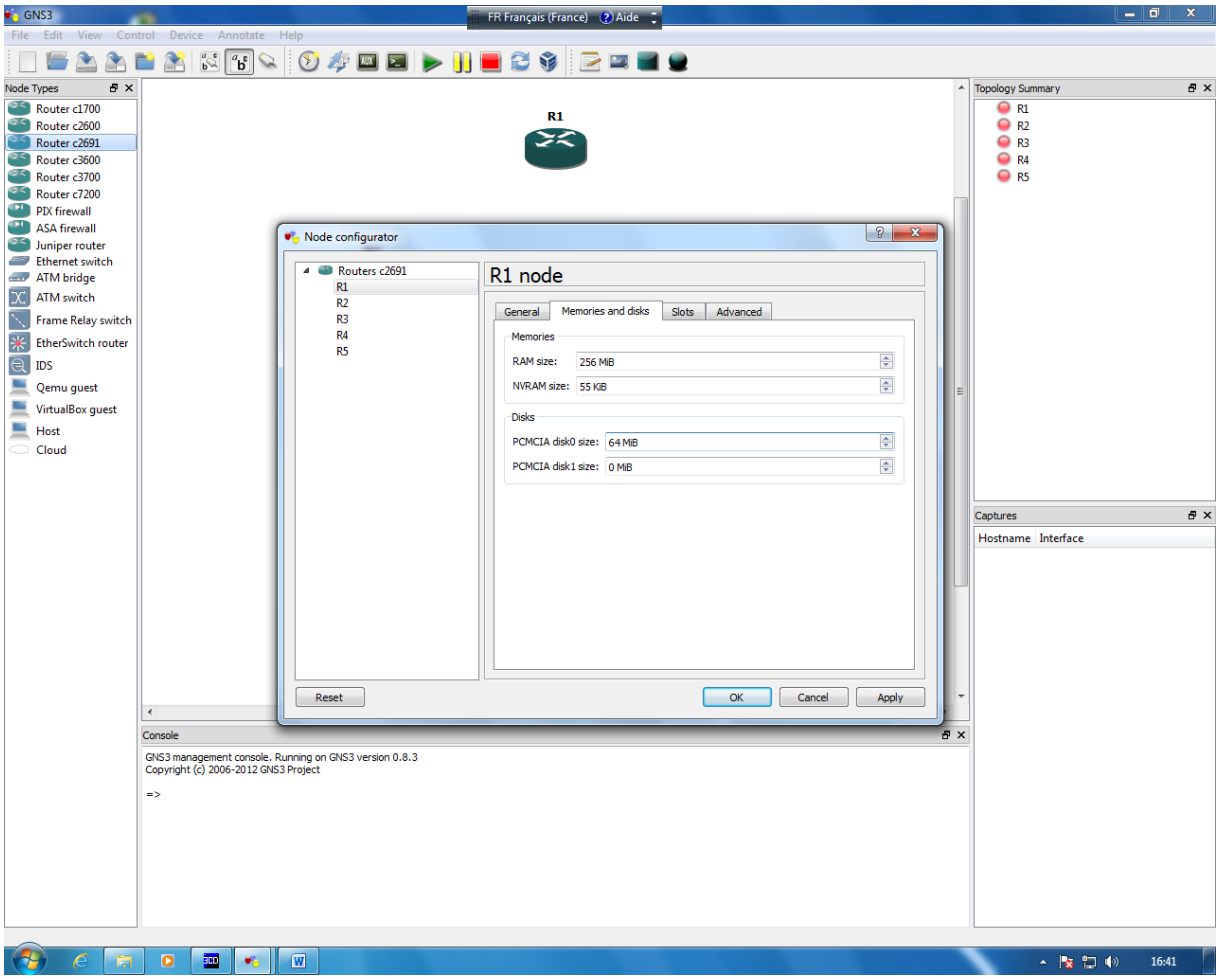
Cliquer sur le bouton <<Test Settings>>, au bout de quelques secondes on doit voir le message en vert <<... successfully started>>

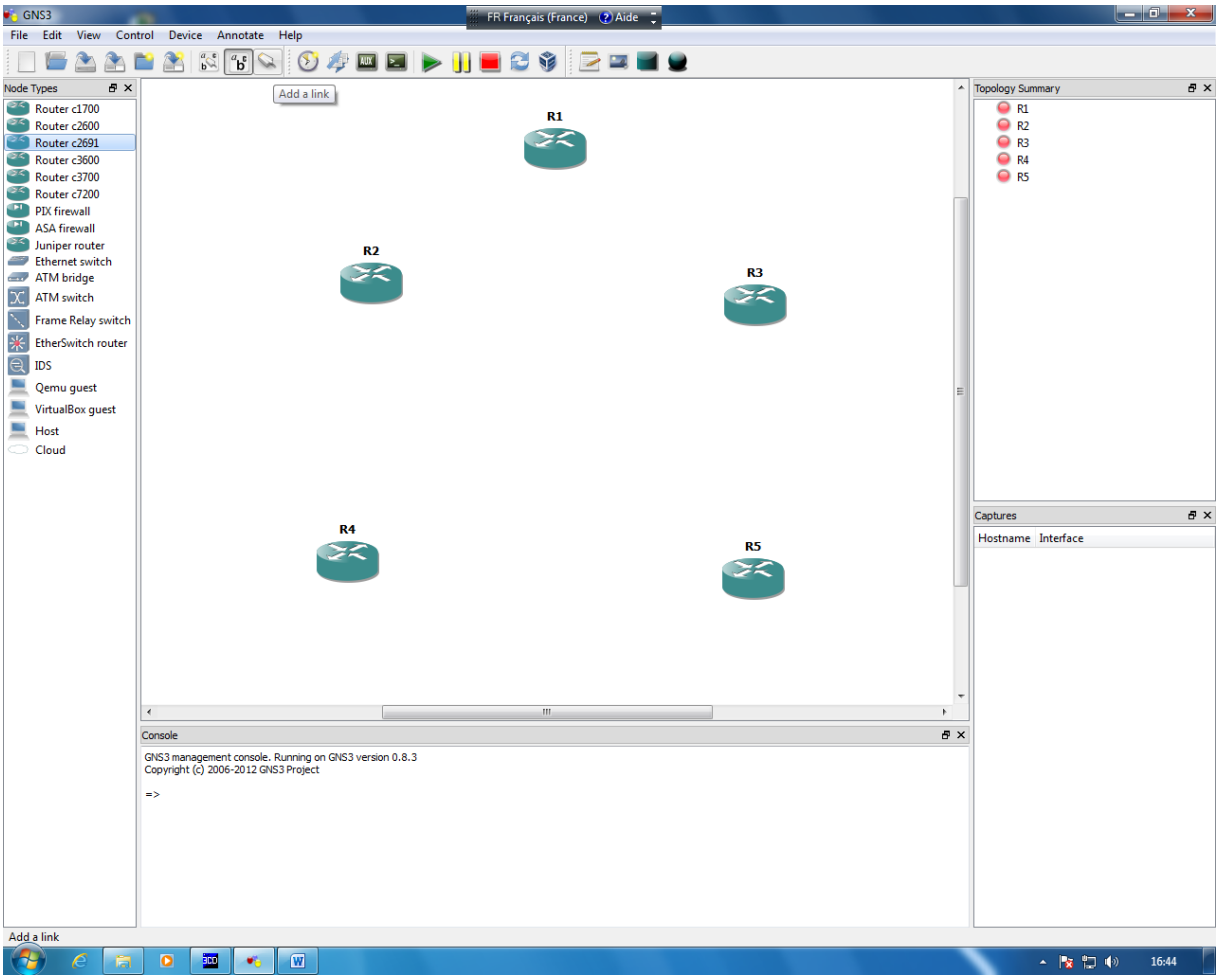


Maintenant que la configuration de base est terminée, on ferme la fenêtre Preference. On fait drag and drop du routeur c2691, autant de routeurs que nécessaires.

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

Annexe

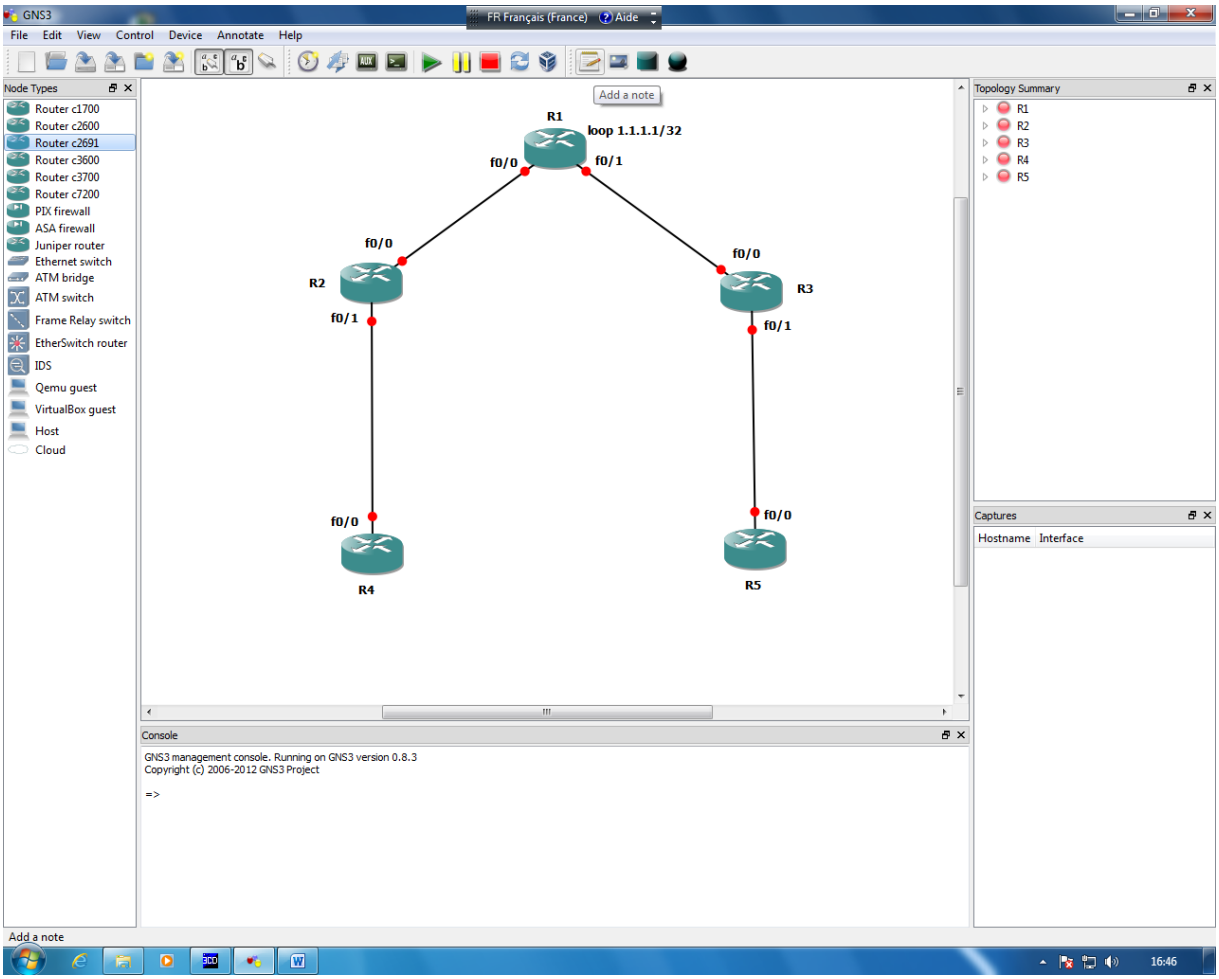

GNS3
File Edit View Control Device Annotate Help
FR Français (France) Aide
Node Types
Router c1700
Router c2600
Router c2691
Router c3600
Router c3700
Router c7200
PIX firewall
ASA firewall
Juniper router
Ethernet switch
ATM bridge
ATM switch
Frame Relay switch
EtherSwitch router
IDS
Qemu guest
VirtualBox guest
Host
Cloud
R1
Node configurator
Routers c2691
R1
R2
R3
R4
R5
R1 node
General
Memories and disks
Slots
Advanced
Memories
RAM size: 256 MiB
NVRAM size: 55 KiB
Disks
PCMCIA disk0 size: 64 MiB
PCMCIA disk1 size: 0 MiB
Reset
OK
Cancel
Apply
Topology Summary
R1
R2
R3
R4
R5
Captures
Hostname Interface
Console
GNS3 management console. Running on GNS3 version 0.8.3
Copyright (c) 2006-2012 GNS3 Project
=>
16:41

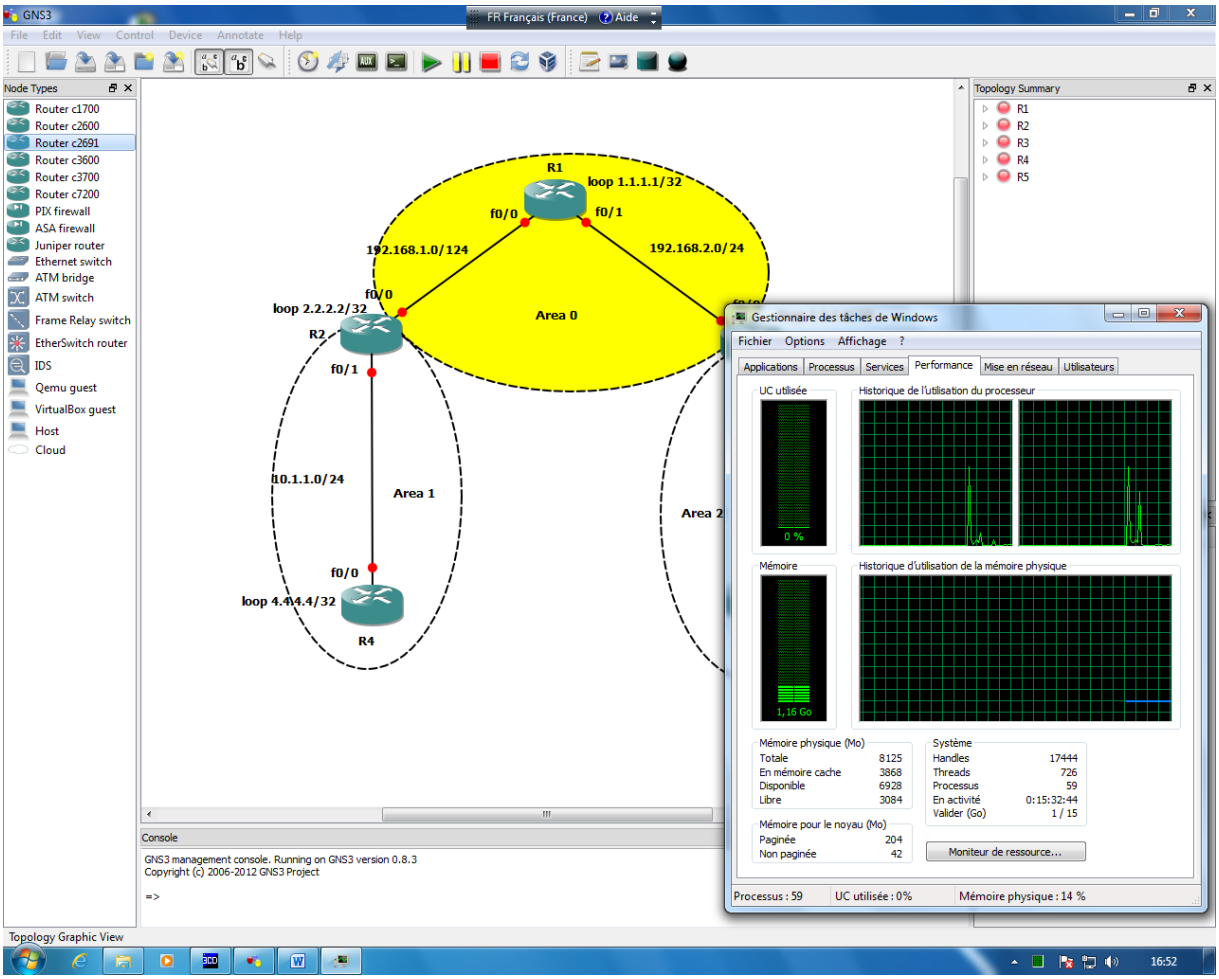


Interconnection des différents routeurs.

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

Annexe


GNS3
File Edit View Control Device Annotate Help
FR Français (France) Aide
Node Types
Router c1700
Router c2600
Router c2691
Router c3600
Router c3700
Router c7200
PIX firewall
ASA firewall
Juniper router
Ethernet switch
ATM bridge
ATM switch
Frame Relay switch
EtherSwitch router
IDS
Qemu guest
VirtualBox guest
Host
Cloud
Add a note
R1
loop 1.1.1.1/32
f0/0
f0/1
R2
R3
R4
R5
Topology Summary
R1
R2
R3
R4
R5
Captures
Hostname Interface
Console
GNS3 management console. Running on GNS3 version 0.8.3
Copyright (c) 2006-2012 GNS3 Project
=>
Add a note
16:46



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 » pour passer en mode administrateur sur l'équipement réseau.

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

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

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

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

Exemple :

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

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

```
!Pre-shared key avec le peer
crypto isakmp key cisco address 200.2.2.3
```

3- Définir les paramètres du tunnel IKE

```
!Policy ISAKMP
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash md5
 group 2
 exit
```

4- Définir les paramètres du tunnel Ipsec

```
!Transfrom-set, parametres ipsec
crypto ipsec transform-set T1 esp-des esp-md5-hmac
```

5- Définir la crypto map

```
!Crypto map
 crypto map M1 10 ipsec-isakmp
  set peer 200.2.2.3
  set transform-set T1
  match address 110
  exit
```

6- Appliquer la crypto map

```
 interface f0/0
  crypto map M1
  exit
```