Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Licence en Informatique

Thème

La sécurité réseau, étude le cas de service Openvpn

Réalisé par :

- Melle BELHARIZI Asmaà

Présenté le 27 Juin 2013 devant la commission d'examination composée de MM.

-Mr BENAISSA Mohamed *(Encadreur)*

-Mme DIDI Fedoua *(Examinateur)*

-Mme LABRAOUI Nabila *(Examinateur)*

Année universitaire : 2012-2013

Remerciement

Je tiens à saisir cette opportunité pour adresser mes sincères remerciements et ma profonde reconnaissance aux personnes suivantes qui m'ont accompagné tout au long de la préparation de mon mémoire :

À Monsieur le Professeur benaissa Mohamed Pour ses précieux conseils qui m'ont guidé et dirigé tout au long de l'année.

J'adresse également mes remerciements, à tous mes enseignants, qui m'ont donnée les bases de la science, Je remercie très sincèrement, les membres de jury d'avoir bien voulu accepter de faire partie de la commission d'examinateur.

Et surtout à mes amies et à ma famille qui m'ont apporté un soutien incontestable en priant et en m'encourageant tout au long de cette année.

Et finalement, je tiens à remercier toute personne qui a contribué de n'importe qu'elle manière à l'élaboration de ce mémoire.

Merci...

Dédicace

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, donc Je dédie ce travail :

A mes chers parents jamais je ne saurais m'exprimé quant aux sacrifices et aux dévouements que vous consacrés à mon éducation et mes études. Les mots expressifs soient-ils restent faibles pour énoncer ma gratitude hautement profonde.

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance

A mes sœurs Meriem, Assia, Aicha et Sarah

Et à toute la famille BELHARIZI et BELOUADI sans Exception.

A tous mes amis.

Melle Belharizi Asmaà

TABLE DE MATIERE

Chapitre III: Réseau Privé Virtuel : VPN

Chapitre IV: Installation et configuration d'un serveur messagerie Postfixun suivi par serveur ftp

Chapitre V scénario pour protéger les messages échangées par un service de messagerie électronique et un service de transfert des fichiers via openvpn

Introduction générale :

De nos jours, la communication est un outil indispensable pour toute entreprise. A l'origine, la communication était facile du fait qu'une société était composée d'une seule entité ou de plusieurs entités géographiquement proches. Le problème et les besoins sont apparus lorsque les sociétés ont commencé à s'implanter sur plusieurs sites, tout autour d'un pays ou même à l'étranger.

Au cours du temps, les besoins en communication des entreprises ont beaucoup évolué, aussi bien qualitativement que quantitativement. Les informations électroniques échangées se développent au détriment du support papier et la qualité de l'information échangée augmente. De plus, les applications et les systèmes distribués font d'avantage parti intégrante de la structure d'un grand nombre d'entreprises. Les interlocuteurs des entreprises sont de plus en plus variés ce qui provoque des communications externes vers les entreprises amies, les fournisseurs et les clients.

L'évolution rapide des technologies de l'information et des télécommunications a permis la construction d'une infrastructure mondiale de communication, l'Internet. De nos jours, l'Internet assure la communication entre les différents sites d'une même entreprise ou entre différentes entreprises. Pourtant, l'utilisation de ce réseau public pour échanger des données confidentielles pose problème. En conséquent, les réseaux privés virtuels ont été conçus pour remédier à ce problème de sécurité.

Internet dans ce contexte là n'a pas la vocation d'être une zone sécurisée. La plupart des données y circule à nue. On à alors recours à des algorithmes de cryptage, pour garder nos données confidentielles et alors Un réseau Vpn repose sur un protocole appelé "Protocol de tunneling». Protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise. Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant Ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet. Les données à transmettre peuvent être prises en charge par un protocole différent d'Ip. Dans

Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation.

L'objectif principal de notre travail est basé sur la sécurisation d'un service de messagerie électronique plus un service de transfert des fichiers ftp via un tunnel VPN (Virtual Private Network).

Notre mémoire est décomposée comme suite :

le premier chapitre, comporte une Introduction à la virtualisation (le cas de virtualbox), dans le deuxième chapitre, nous présentons une Introduction initial à la sécurité informatique , le troisième chapitre détaille le Réseau Privé Virtuel : VPN, le quatrième chapitre comporte l'étude et d'Installation plus la configuration d'un serveur de messagerie électronique suivi par un serveur ftp (file transfer protocol) et le dernier chapitre traite la Simulation d'un scénario pour protéger les messages échangées par un service de messagerie électronique et un service de transfert des fichiers via openvpn

Une partie pratique qui fait l'objectif de notre projet on utilisons la distribution ubuntu linux.

ChapitreI :
Introduction à la virtualisation
(le cas de virtualbox)

Enfin, démarrer la machine virtuelle. OK à tous les messages. Cliquer sur Installer Ubuntu.

V -Conclusion

La virtualisation est un domaine en pleine croissance, qui évolue très rapidement. Les entreprises peuvent s'en servir pour différents usages, aux besoins de leur fin. Les différentes solutions de virtualisation existantes utilisent des technologies variées, en fonction des buts du projet. Certaines technologies permettent de faire cohabiter plusieurs systèmes d'exploitation, d'autres cloisonnent un unique système en plusieurs compartiments indépendants. Certaines s'appuient sur les capacités du matériel pour améliorer les performances alors que d'autres nécessitent un système d'exploitation modifié pour cohabiter avec la solution de virtualisation.

Nous sommes intéressé par la machine virtuelle crée par virtualbox afin de tester notre réseau privé virtuel vpn.

Dans le chapitre suivant, nous présentons les notions de base de la sécurité réseau.

I- Introduction :

La Virtualisation est une couche d'abstraction proche du matériel, c'est une vue multiple d'un matériel unique, en sérialisant les appels vus concurrents de l'extérieur. La virtualisation recouvre l'ensemble des techniques matérielles et/ou logiciels qui permettent de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation, plusieurs instances différentes et cloisonnées d'un même système ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machine physiques distinctes. Chaque outil de virtualisation implémente une ou plusieurs de ces notions :

- couche d'abstraction matérielle et/ou logicielle.
- système d'exploitation hôte (installé directement sur le matériel).
- systèmes d'exploitations (ou applications, ou encore ensemble d'applications) « virtualisé(s) » ou « invité(s) ».
- partitionnement, isolation et/ou partage des ressources physiques et/ou logiciels.
- *images manipulables* : démarrage, arrêt, sauvegarde et restauration, sauvegarde de contexte, migration d'une machine physique à une autre.
- *réseau virtuel* : réseau purement logiciel, interne à la machine hôte, entre hôte et invités.

II- Intérêt de la virtualisation :

Les intérêts sont :

- Utilisation optimale des ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives).
- Installation, déploiement et migration facile des machines virtuelles d'une machine physique à une autre, notamment dans le contexte d'une mise en production à partir d'un environnement de qualification ou de pré-production, livraison facilitée.
- Économie sur le matériel par mutualisation (consommation électrique, entretien physique, monitoring, support, compatibilité matérielle, etc..).

- Installation, tests, développements, réutilisation avec possibilité de recommencer arrêt du système hôte.
- Sécurisation et/ou isolation d'un réseau (arrêt des systèmes d'exploitation virtuels, mais pas des systèmes d'exploitation hôtes qui sont invisibles pour l'attaquant, tests d'architectures applicatives et réseau).
- Isolation des différents utilisateurs simultanés d'une même machine (utilisation de type site central).
- Allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné.
- Diminution des risques liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de puissance (nouveau serveur etc..) étant alors transparente. **[1]**

III- Comparaison des différentes techniques de Virtualisation :

Les systèmes de virtualisation partent donc du principe de l'utilisation de couches logicielles intermédiaires. Afin d'avoir une idée théorique des performances des applications au sommet, il faut comparer verticalement l'empilage de couches. Il faut garder à l'esprit qu'il est possible d'élargir les schémas en rajoutant des environnements virtualisés consommant également des ressources de l'hôte, en mémoire puis en disque.

III.1 Machine Virtuelle :

Une machine virtuelle est un logiciel qui tourne sur l'OS hôte, ce logiciel permettant de lancer un ou plusieurs OS invités, c'est l'archétype de la solution de virtualisation par empilement de systèmes. La machine virtualise le matériel (ce qui passe généralement par une émulation partielle) pour les systèmes d'exploitation invités : les systèmes d'exploitation invités croient dialoguer directement avec le matériel. En pratique on a recours à une émulation logicielle des périphériques, et parfois aussi de tout ou partie de la machine. **[2]**

III.2 Virtualisation d'OS, Isolateur :

Un isolateur est un logiciel permettant d'isoler l'exécution des applications dans des contextes ou zones d'exécution, c'est l'archétype de la solution de virtualisation par "juxtaposition". L'isolateur permet ainsi de faire tourner plusieurs fois la même

application (à base d'un ou plusieurs logiciels) prévue pour ne tourner qu'à une seule instance par machine.

Notons que cette technologie consiste en quelque sorte à généraliser la notion de "contexte" Unix : ce dernier isole les processus (mémoire, accès aux ressources), on ajoute alors : une isolation des périphériques (c'est le rôle de l'isolateur), voire leur partage, les systèmes de fichiers donc les fichiers eux-mêmes et leurs accès. **[2]**

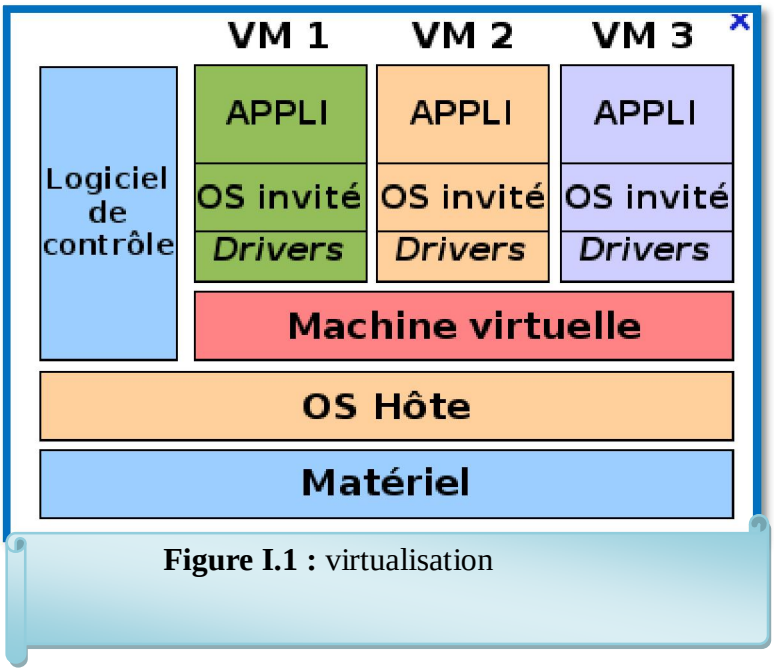


Figure I.1 : virtualisation

III.3 Hyperviseur complet :

Partant du principe, exposé précédemment, qu'une approche pour une virtualisation efficace consiste à affiner les couches, une première approche consiste à proposer un noyau léger (de type micro-noyau par exemple), lequel est accompagné d'outils de supervision, et adapté pour faire tourner des systèmes d'exploitation natifs. Pour réussir cette approche, soit on émule le matériel (et on revient aux performances de la machine virtuelle pour les I/O), soit on dispose des instructions dédiées à la virtualisation. **[2]**

III.4 Paravirtualiseur :

Un paravirtualiseur est un noyau hôte allégé et optimisé pour ne faire tourner que des noyaux de systèmes d'exploitation invités, adaptés et optimisés. Les applications en espace utilisateur des systèmes d'exploitation invités tournent ainsi sur une pile de deux noyaux optimisés, les systèmes d'exploitation invités ayant conscience d'être virtualisés. Cette approche offre l'avantage d'être utilisable en l'absence des instructions spécifiques,

mais elle est impraticable pour des systèmes non libres pour lesquels l'éditeur ne fera pas l'effort d'adaptation. **[2]**

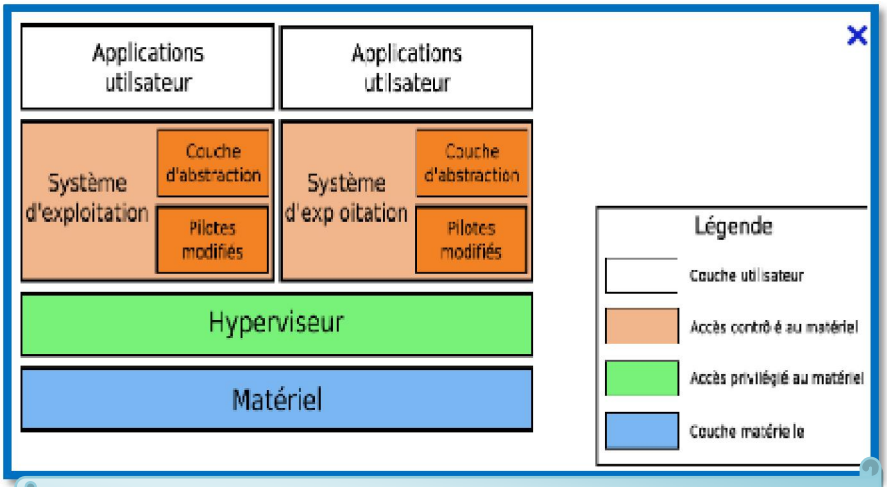


Figure I.2 : Hyperviseur

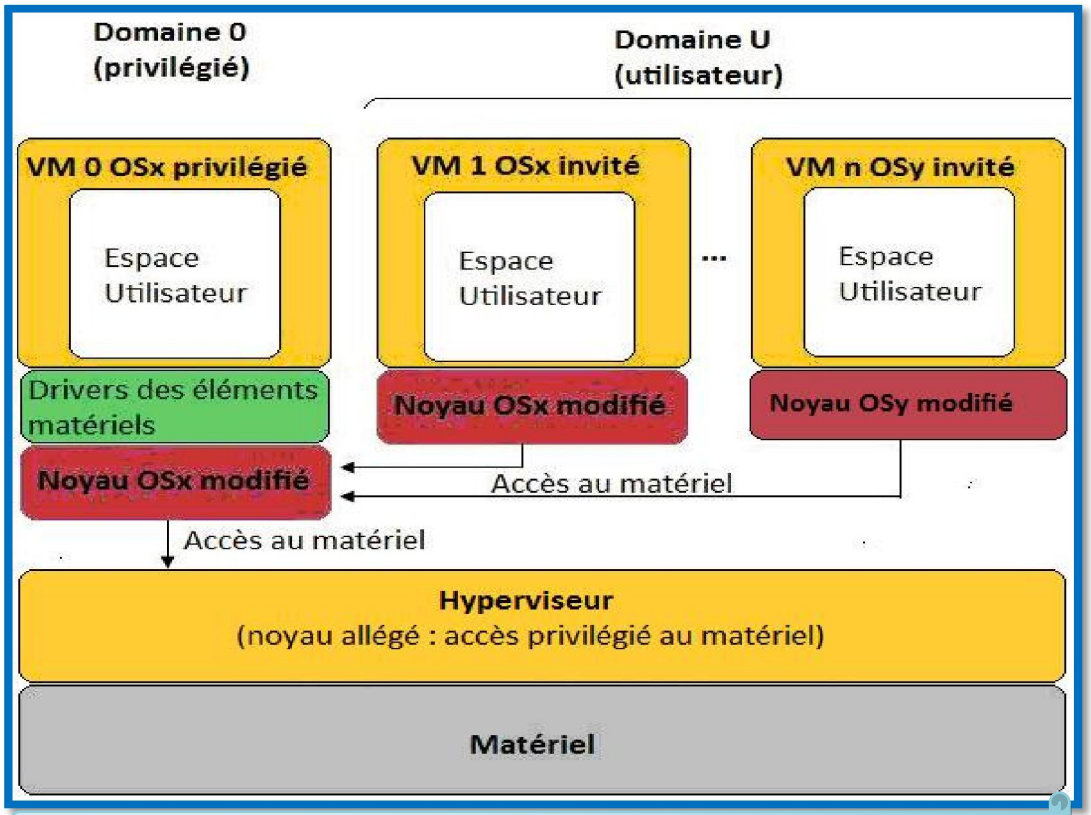


Figure I.3 : Les couches de virtualisation

IV- VirtualBox :

IV.1 Présentation :

VirtualBox est un produit qui se présente comme "seule solution professionnelle de virtualisation distribuée sous licence GPL". Il se présente accompagné d'utilitaires destinés à faciliter la création de machines virtuelles, disques et montages CD/DVD (fichiers .iso testés). Cependant, le site d'Innotek est très clair sur les limites de la version Open Source. La version Open Source est disponible packagée, il faut le noter, pour un nombre important de distributions (dont OpenSuse, Mandriva, Fedora, RHEL et Ubuntu).

IV.2 Fonctionnement global de VirtualBox :

Sous VirtualBox, la manipulation des machines virtuelles nécessite plusieurs étapes :

- ***Création d'un disque dur virtuel (VDI) :*** Nous pouvons soit créer un disque virtuel de taille fixe, soit utiliser un live-cd. Cette deuxième solution permet d'obtenir un disque virtuel n'occupant que peu de place.
- ***Créer une nouvelle machine virtuelle :*** Un fichier de description de la machine, comportant des différents paramètres de configuration, est crée.
- ***Rattacher le disque VDI et l'image ISO :*** du système d'exploitation invité à la machine virtuelle.
- ***Configurer le réseau :*** de la machine virtuelle.
- ***Lancer la machine virtuelle.***

Pour exécuter ces actions, il existe plusieurs possibilités :

- grâce à **l'interface graphique**, on peut réaliser ses actions sans difficultés. On peut également manipuler les disques VDI et les images ISO rattachées aux machines virtuelles via le gestionnaire de disque virtuel.
- On peut aussi utiliser la **commande** VboxManage. **[1]**

IV.3 Créations d'une machine virtuelle ubuntu :

Avant de créer la machine virtuelle ubuntu, Il faut télécharger les paquets pour utiliser dans l'installation de virtualbox sur la machine linux quand l'installation est terminée il

suffit de redémarrer la machine pour obtenir une application qui se trouve dans les outils système (oracle VM virtualBox) donc nous pouvons créer une machine virtuelle

Etape01 : Démarrez VirtualBox et cliquez sur créer.

Figure I-4 : VirtualBox

Etape02: Dans l'écran suivant on peut choisir le nom de notre machine virtuelle. On met le nom que l'on souhaite, mais il est préférable d'être relativement explicite surtout si l'on est amené gérer plusieurs machines virtuelles (par exemple "Linux Debian") pour s'y retrouver.

Il faut choisir le system d'exploitation et le version comme cet exemple

- Système d'exploitation : Linux
- Version : ubuntu

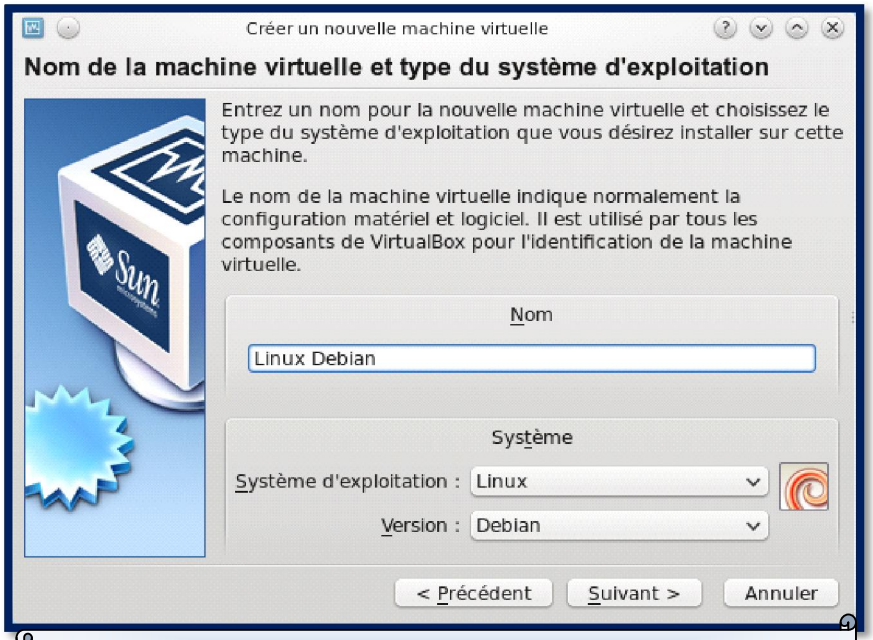


Figure I-5 : Machine virtuelle

***Etape03*:** Il faut choisir la taille de la mémoire vive (ici 256Mo).

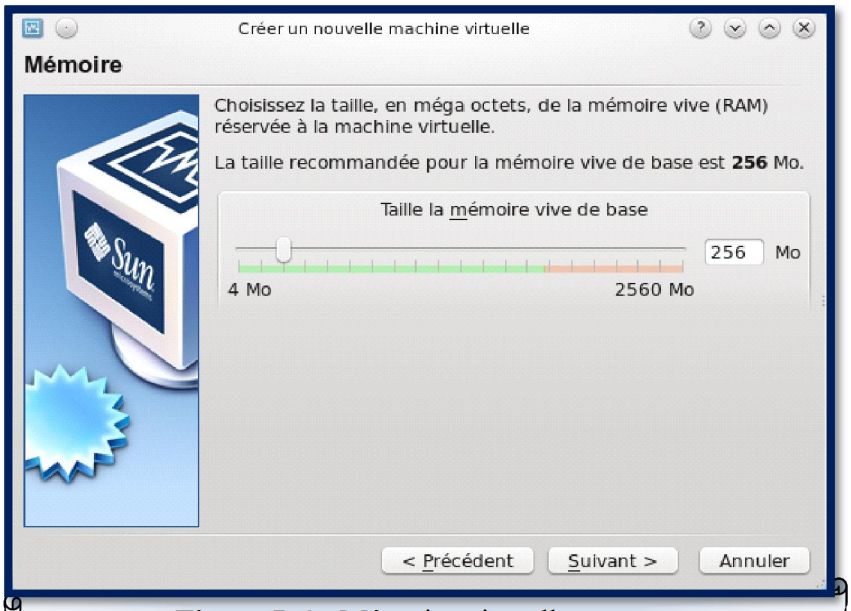


Figure I-6 : Mémoire virtuelle

Etape04:Créer un disque dur virtuel.

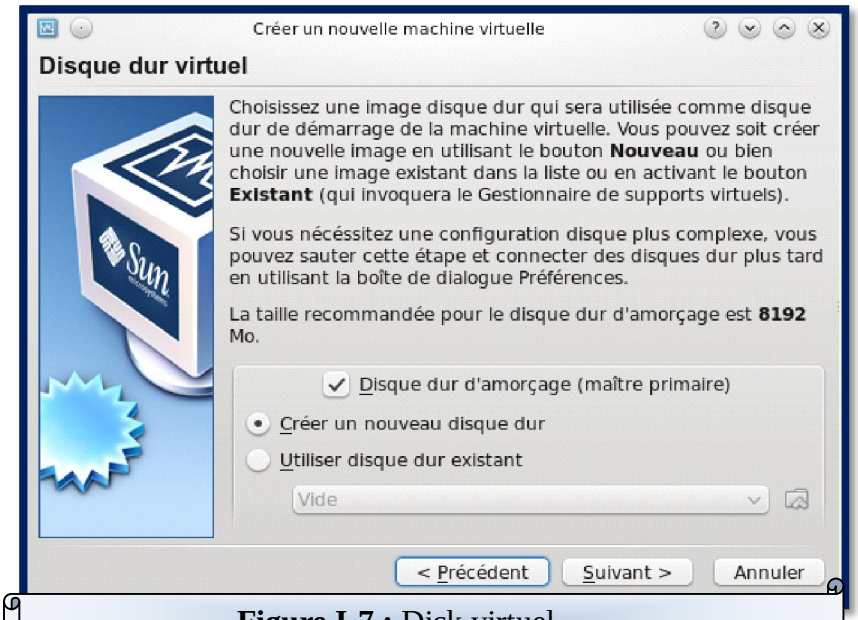


Figure I-7 : Dick virtuel

Etape05:Assistant de création de disque dur virtuel.

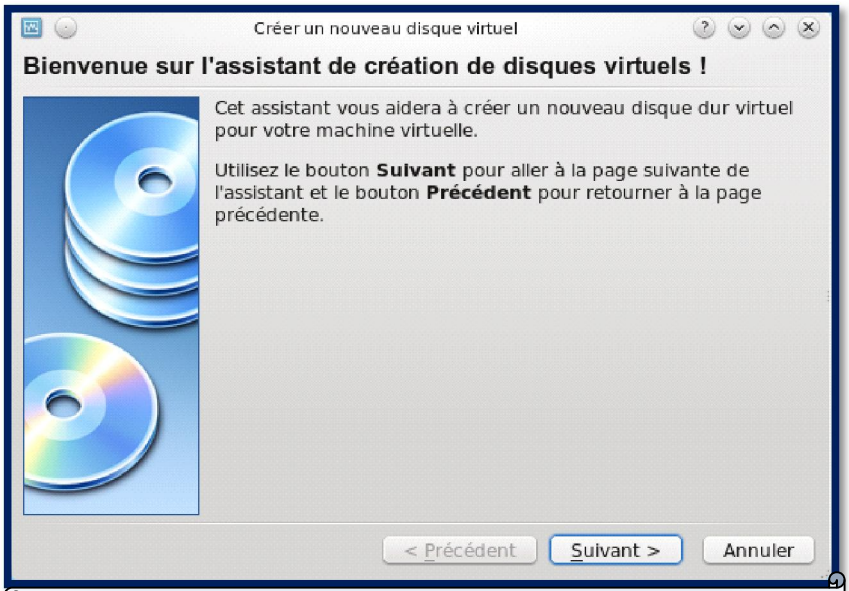


Figure I-8 : Création disk virtuel

Etape06:Fichier de taille variable.

Figure I-9 : Image disque virtuelle

Etape07: Préciser la taille maximale (ici 8,00 GB)

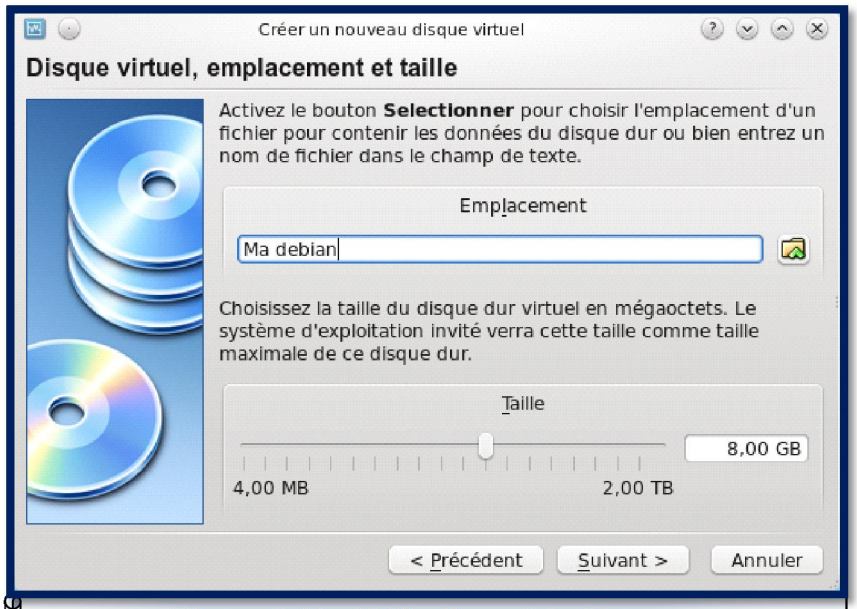


Figure I-10 : Taille disque Machine

Etape08: fin de la création de machine virtuelle.

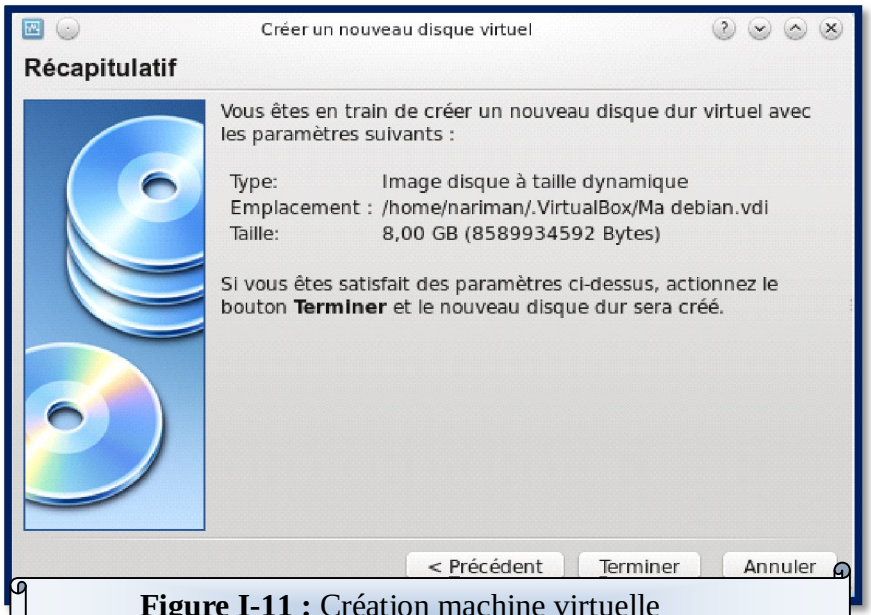


Figure I-11 : Création machine virtuelle

Votre nouvelle machine virtuelle est sélectionnée mais éteinte, allons sur Configuration.

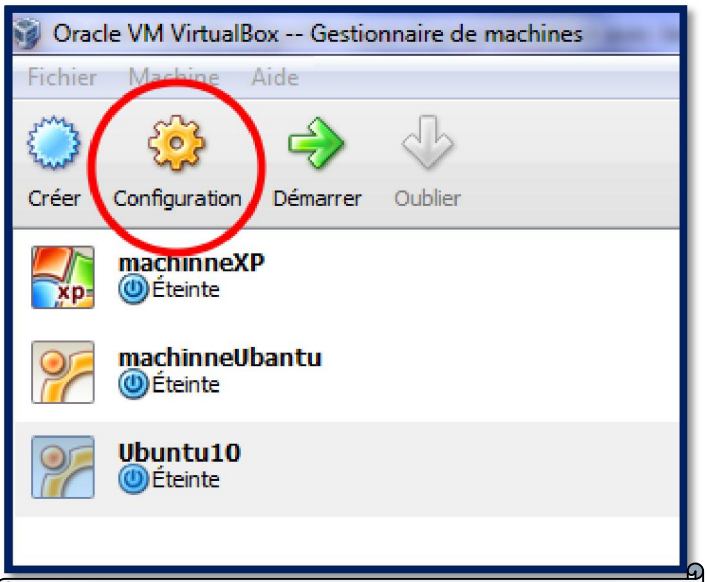


Figure I-12 : Configuration virtualbox

Sélectionner Stockage, puis le CD vide.

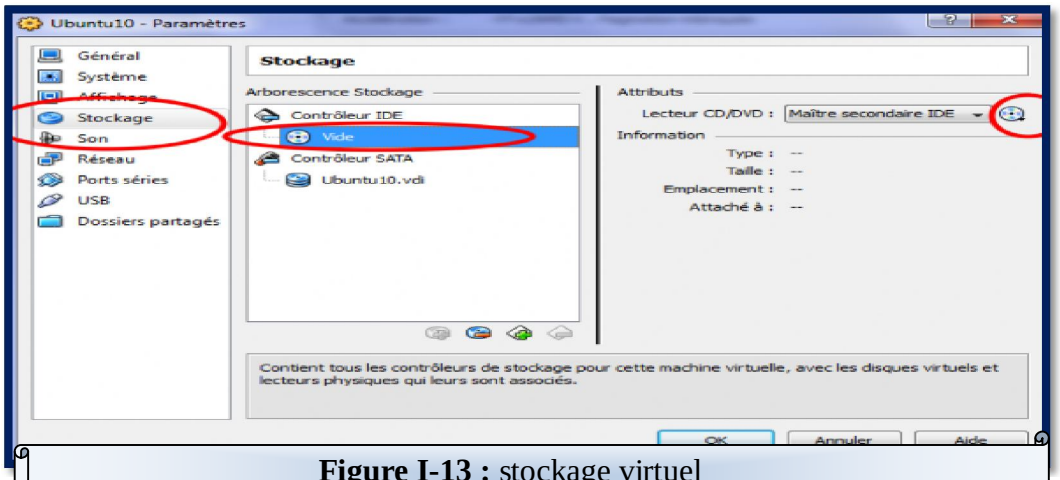


Figure I-13 : stockage virtuel

Cliquer sur la petite icône de CD la plus à droite. Puis cliquer sur « Choisissez un fichier de CD/DVD virtuel ».

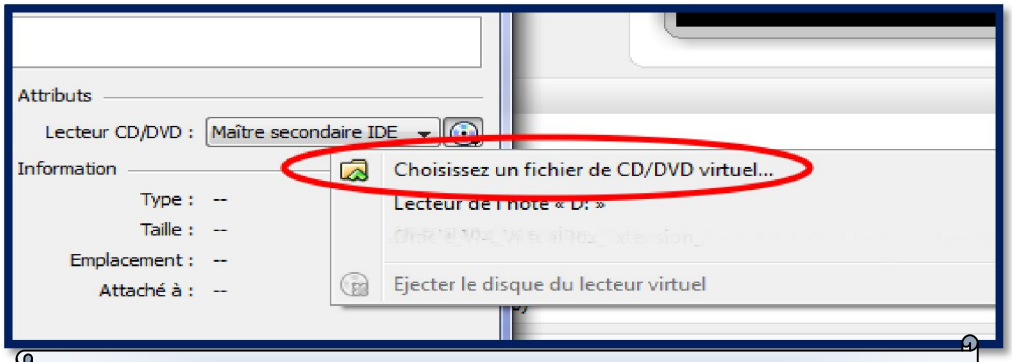


Figure I-14 : paramètre de configuration machine virtuelle

Sélectionner le fichier iso d'installation d'Ubuntu (ici « ubuntu-10.10-desktop-i386-fr.iso »). OK aux messages suivant.

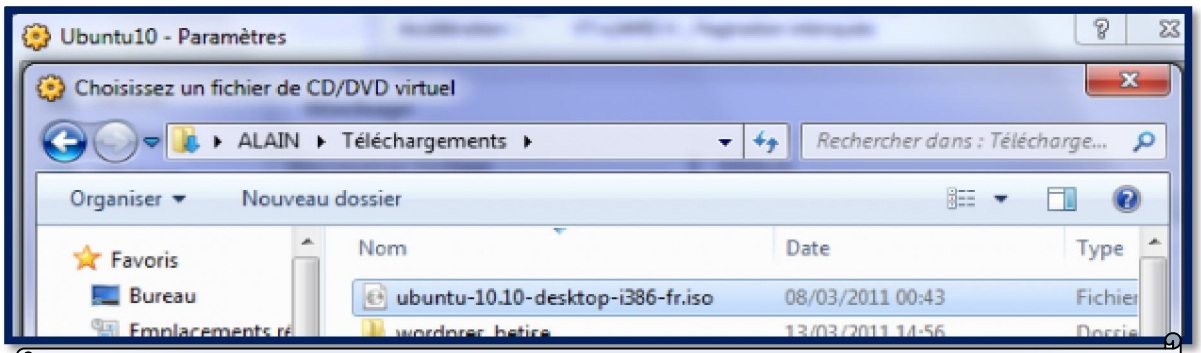


Figure I-15 cd/dvd virtuel

Chapitre II:
Introduction à la sécurité dans un réseau

I Introduction :

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines. Un seul mot " sécurité " recouvre des aspects très différents à la fois techniques, organisationnels et juridiques. D'un point de vue technique, la sécurité recouvre à la fois l'accès aux informations sur les postes de travail, sur les serveurs ainsi que le réseau de transport des données. Nous concentrerons sur les problèmes posés par la sécurité des informations lors des échanges au travers de réseaux publics ou privés. Internet, le réseau des réseaux, est un outil qui permet à tous les ordinateurs quel que soit leur type de communiquer entre eux. La technologie utilisée (TCP/IP) a permis de simplifier la mise en place des réseaux, donc de réduire le coût des télécommunications. En revanche, les fonctions de sécurité ne sont pas traitées par ce protocole.

II Gestion de sécurité :

Nous définissons la sécurité des systèmes d'information et des réseaux, tout d'abord en termes de risques et de menaces qu'ils encourent. À partir de l'analyse de ces derniers, nous rappelons l'importance de la politique de sécurité .Risques et menaces sont deux concepts fondamentaux pour la compréhension des techniques utilisées dans le domaine de la sécurité. Le risque est une fonction de paramètres qu'on peut maîtriser à la différence de la menace qui est liée à des actions ou des opérations émanant de tiers. Dans un réseau, a fortiori dans un grand réseau, la sécurité concerne non seulement les éléments physiques (câbles, modems, routeurs, commutateurs…) mais aussi les éléments logiques, voire volatils, que représentent les données qui circulent. Le responsable de la sécurité doit analyser l'importance des risques encourus, les menaces potentielles et définir un plan général de protection qu'on appelle politique de sécurité. **[6]**

II.1 Risques :

Les risques se mesurent en fonction de deux critères principaux : la vulnérabilité et la sensibilité. La vulnérabilité : Désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher. Un élément de ce réseau

peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau.

La sensibilité : Désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques.

Exemples : le câble constituant le média d'un réseau local lorsqu'il passe dans des espaces de service protégés, l'armoire de sauvegarde des logiciels de tous les commutateurs du réseau…

Enfin, selon les niveaux de sensibilité et de vulnérabilité, on distingue souvent quatre niveaux de risques, selon qu'ils sont acceptables, courants, majeurs ou inacceptables.

- *Acceptables :* Ils n'induisent aucune conséquence grave pour les entités utilisatrices du réseau. Ils sont facilement rattrapables : pannes électriques de quelques minutes, perte d'une liaison…
- *Courants :* Ce sont ceux qui ne portent pas un préjudice grave. Ils se traduisent, par exemple, par une congestion d'une partie du réseau.
- *Majeurs :* Ils sont liés à des facteurs rares. Ils causent des préjudices ou des dégâts importants, mais ils peuvent encore être corrigés.
- *Inacceptables :* Ils sont, en général, fatals pour l'entreprise. Exemple : la destruction du centre informatique et de l'ensemble des sauvegardes des programmes et données. **[6]**

II.2 Menaces :

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien (menaces passives) ou qu'elles perturbent effectivement le réseau (menaces actives).

- Les menaces passives : consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle-même. Il en résulte des difficultés à détecter ce type de malveillance, car elles ne modifient pas l'état du réseau. La méthode de prélèvement varie suivant le type de réseau. Sur les réseaux câblés, on peut imaginer un branchement en parallèle grâce à des

appareils de type analyseurs de protocole ou une induction (rayonnement électromagnétique).

- Les menaces actives : nuisent à l'intégrité des données. Elles se traduisent par différents types d'attaques. On distingue le brouillage, le déguisement (modification des données au cours de leur transmission, modification de l'identité de l'émetteur ou du destinataire), l'interposition (création malveillante de messages en émission ou en réception). **[6]**

II.3 Politique de sécurité :

La définition d'une politique de sécurité nécessite d'abord l'analyse des informations qui circulent ou qui sont stockées (analyse de leur importance pour l'entreprise, analyse du coût que représenterait leur perte) et celles des menaces qu'on peut objectivement envisager. Nous ne détaillerons ici que les aspects de la sécurité directement liés au réseau, sans aborder la protection contre le dégât des eaux, le contrôle d'accès physique aux bâtiments, la mise en place d'onduleurs et de générateurs pour maintenir l'alimentation électrique stable. **[6]**

III Services de sécurité :

L'ISO a défini six services de sécurité : authentification, contrôle d'accès, confidentialité et intégrité des données, non-répudiation et protection contre l'analyse du trafic.

III.1 Authentification :

Le service d'authentification garantit l'identité des correspondants ou des partenaires qui communiquent. On distingue deux cas d'authentification simple et un cas d'authentification mutuelle :

- L'authentification de l'origine : Elle assure que l'émetteur est celui prétendu. Le service est inopérant contre la duplication d'entité. Comme le précédent, il s'agit d'authentification simple.
- L'authentification mutuelle : Elle assure que les deux entités émettrice et réceptrice se contrôlent l'une l'autre. Le service d'authentification est inutilisable dans le cas d'un réseau fonctionnant en mode sans connexion : dans

les réseaux, comme dans la vie courante, l'authentification nécessite un échange entre les deux partenaires.

III.2 Contrôle d'accès :

Le service de contrôle d'accès empêche l'utilisation non autorisée de ressources accessibles par le réseau. Par « utilisation », on entend les modes lecture, écriture, création ou suppression. Les ressources sont les systèmes d'exploitation, les fichiers, les bases de données, les applications. Pour contrôler les accès aux ressources, il faut d'abord authentifier les utilisateurs afin de s'assurer de leur identité qui est transportée dans les messages d'initialisation et ensuite établir une liste des droits d'accès associés à chacun.

III.3 Confidentialité des données :

Garantir la confidentialité des données empêche une entité tierce (non autorisée, le plus souvent en état de fraude passive) de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données. Un message ou un échange de messages à sa confidentialité garantie dès lors que tout utilisateur non autorisé qui aurait pu le récupérer ne peut pas l'exploiter. Il n'est pas obligatoire de mettre en place des procédures pour empêcher cette « récupération ».

III.4 Intégrité des données :

Garantir l'intégrité des données assure au récepteur que les données reçues sont celles qui ont été émises. Les données ont pu être altérées, de manière accidentelle ou de manière délibérée à la suite d'une fraude active. On distingue différents niveaux de service selon les mécanismes mis en œuvre. Par ailleurs, l'intégrité possède une portée plus ou moins grande (le message complet ou un champ spécifique du message seulement). Lorsque la communication a lieu en mode non connecté, seule la détection des modifications peut être mise en œuvre. Le récepteur refait le calcul sur le message qu'il a reçu et compare les deux blocs de contrôle d'erreurs. Il vérifie ainsi l'intégrité du message, cette seule méthode est insuffisante pour détecter des messages insérés dans un flux de données. Les protections mises en œuvre s'inspirent du même principe.

III.5 Non-répudiation :

La non-répudiation de l'origine fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi d'un message ou le contenu d'un message effectivement reçu. La non-répudiation de la remise fournit à l'émetteur une preuve empêchant le récepteur de contester la réception d'un message ou le contenu d'un message effectivement émis.

III.6 Protection contre l'analyse de trafic :

Le secret du flux lui-même empêche l'observation du flux de transmission de données, source de renseignements pour les pirates. Ce cas s'applique aux situations où on a besoin de garder la confidentialité sur l'existence même de la relation entre les correspondants. **[12]**

IV Cryptographie :

IV.1Définition :

La cryptographie regroupe l'ensemble des méthodes permettant de communiquer de façon confidentielle par des voies de communications susceptibles d'être espionnées .Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce que l'on appelle le chiffrement, qui à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement le déchiffrement est l'action légitime qui permet de retrouver l'information en clair à partir de données chiffrées. Dans la cryptographier moderne, les transformations en question sont des fonctions mathématiques appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clé.

IV.2Technique de chiffrement :

La sécurisation des échanges entre l'utilisateur et les différents services du réseau passe par un chiffrement des transactions. Deux systèmes de chiffrement s'offrent à nous, le chiffrement à clé symétrique et celui à clé asymétrique. La cryptographie symétrique, également dite à clé secrète est la plus ancienne forme de chiffrement. Il s'agit de chiffrer le message envoyé grâce à une clé qui sera réutilisée par le destinataire pour déchiffrer le message crypté.

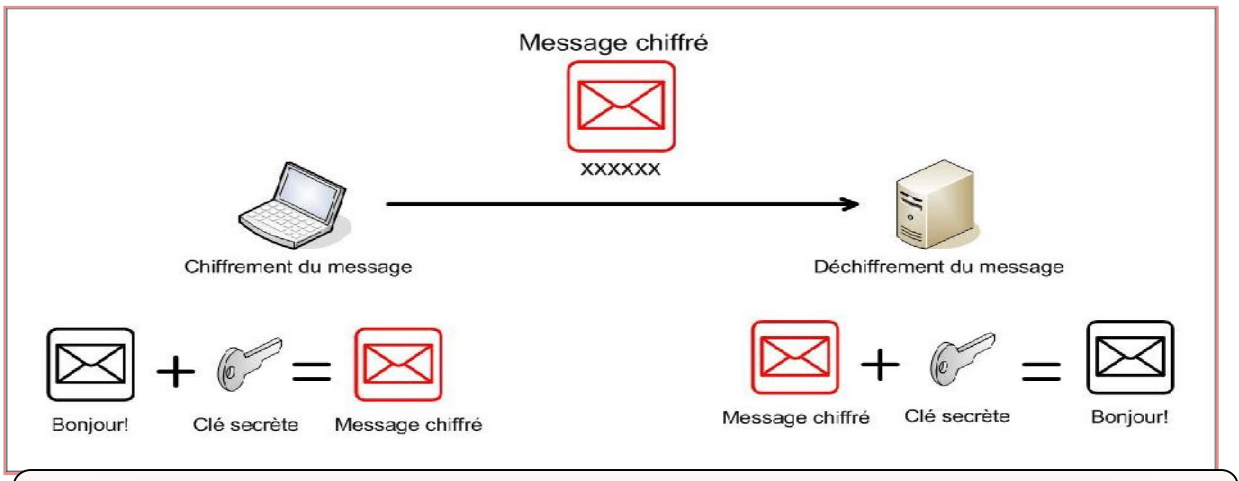


Figure II-1 : Cryptographie clé secrète

Le problème de cette méthode est que tous les utilisateurs possèdent alors la même clé partagée, la sécurité n'existe plus puisque pour déchiffrer les transactions d'un autre utilisateur il suffit d'utiliser la clé unique que tous les utilisateurs possèdent.

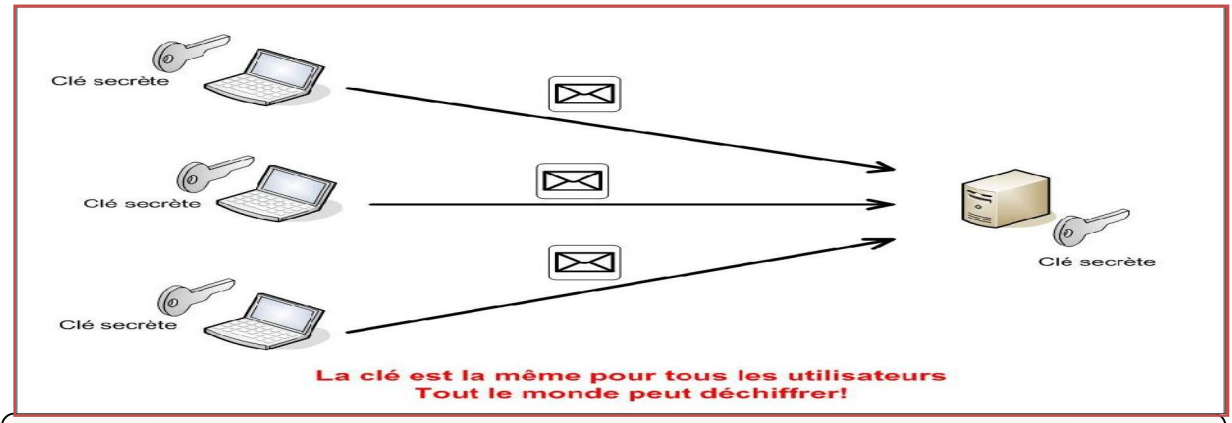


Figure II-2 : Chiffrement symétrique

Chiffrement asymétrique (clé publique) :

Dans un crypto système asymétrique, les clés existent par paires (le terme de bi-clés est généralement employé) :

- Une clé publique pour le chiffrement
- Une clé secrète pour le déchiffrement

Ainsi, dans un système de chiffrement à clé publique, les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée). A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire. Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

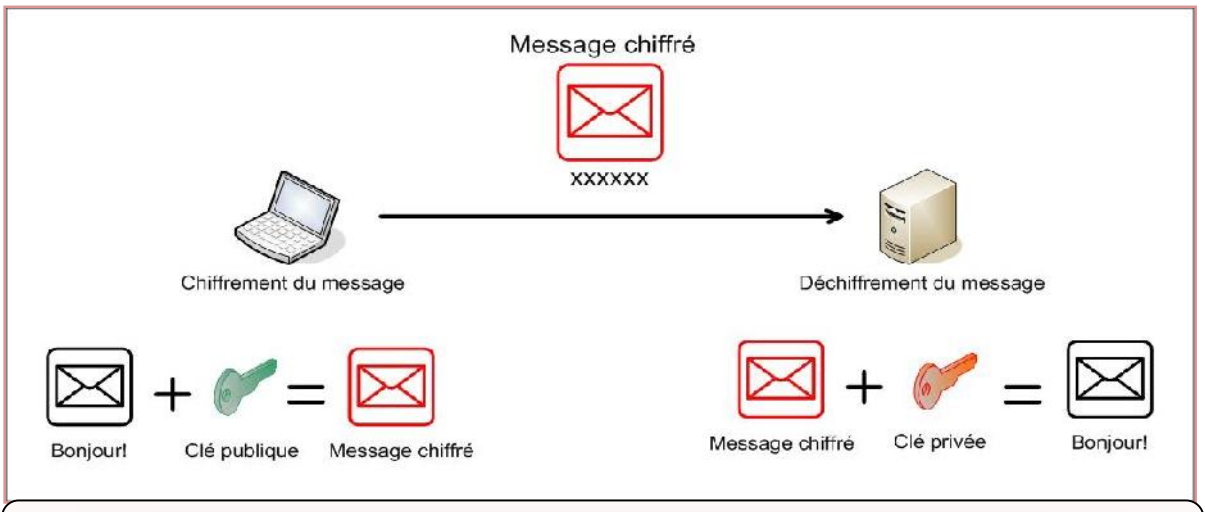


Figure II-3 : Cryptographie à clé publique

A titre d'image, il s'agit pour un utilisateur de créer aléatoirement une petite clé en métal (la clé privée), puis de fabriquer un grand nombre de cadenas (clé publique) qu'il dispose dans un casier accessible à tous (le casier joue le rôle de canal non sécurisé). Pour lui faire parvenir un document, chaque utilisateur peut prendre un cadenas (ouvert), fermer une valisette contenant le document grâce à ce cadenas, puis envoyer la valisette au propriétaire de la clé publique (le propriétaire du cadenas). Seul le propriétaire sera alors en mesure d'ouvrir la valisette avec sa clé privée.

[16]

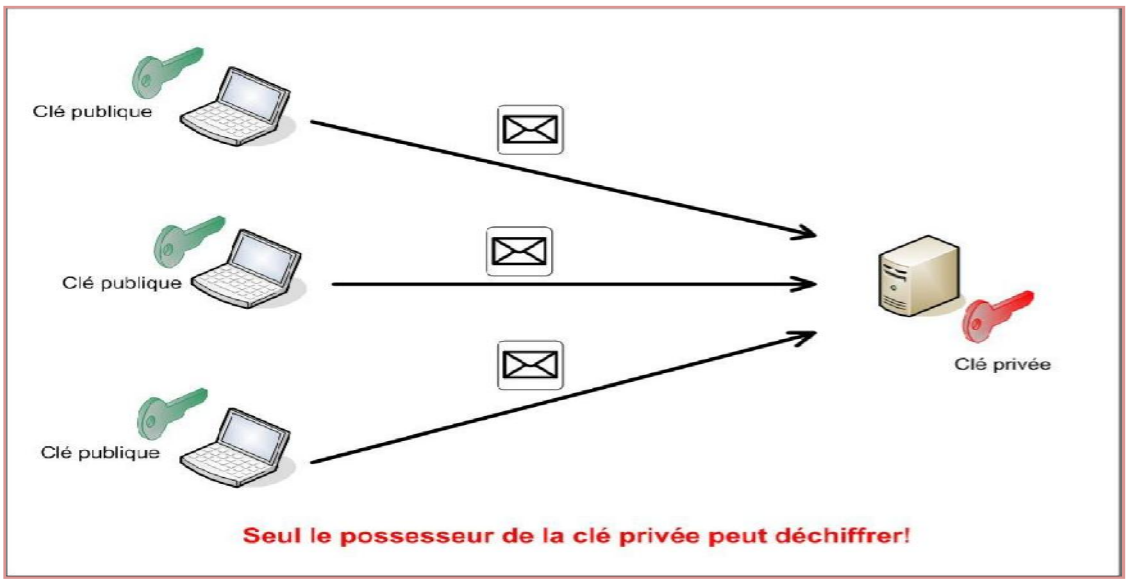


Figure II-4 : Cryptographie asymétrique

IV.3Comparaison deux méthodes de chiffrement dans la sécurité de réseau :

a Pour le Chiffrement symétrique :

Comme nous l'avons dit précédemment, dans ce système, chaque utilisateur posséderait la même clé, qui est également la même que celle du point d'accès. Dans ce cas de figure, un utilisateur mal intentionné pourrait écouter le trafic qui passe entre un autre utilisateur et le réseau. Cet échange est chiffré, cependant il est aisé pour n'importe quel utilisateur de le déchiffrer puisqu'il suffit pour cela d'utiliser la clé secrète que tout le monde possède.

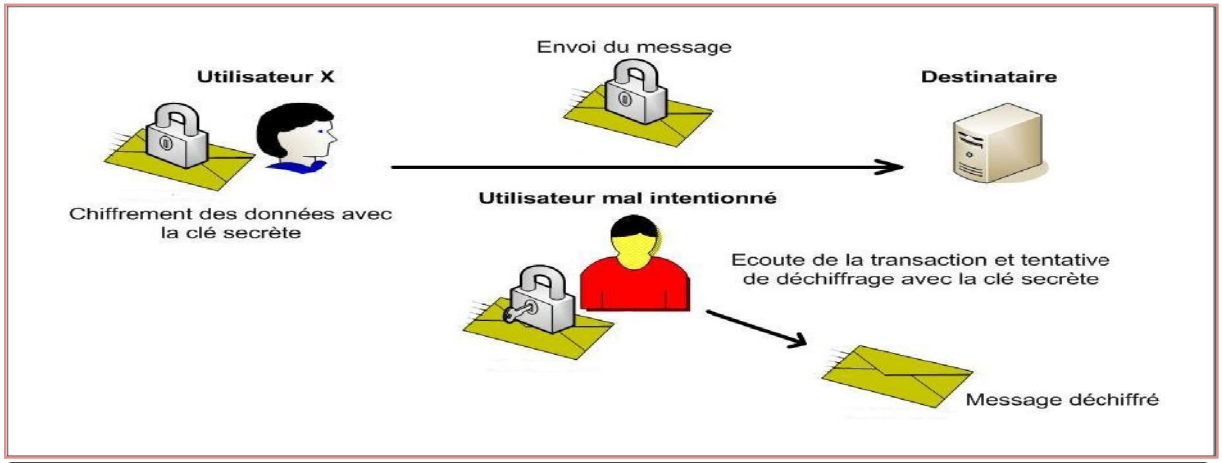


Figure II-5 : exemple attaque (symétrique)

b Pour le Chiffrement asymétrique :

Dans ce système, chaque utilisateur possède la clé publique du destinataire. Cependant seul le destinataire possède la clé privée qui permet de déchiffrer le message .Dans ce cas de figure un utilisateur mal intentionné qui essayerait d'écouter le trafic transitant sur le réseau capturerait des messages chiffrés. Il lui serait impossible de les déchiffrer car il ne possède pas la clé privée nécessaire à ce déchiffrement. **[16]**

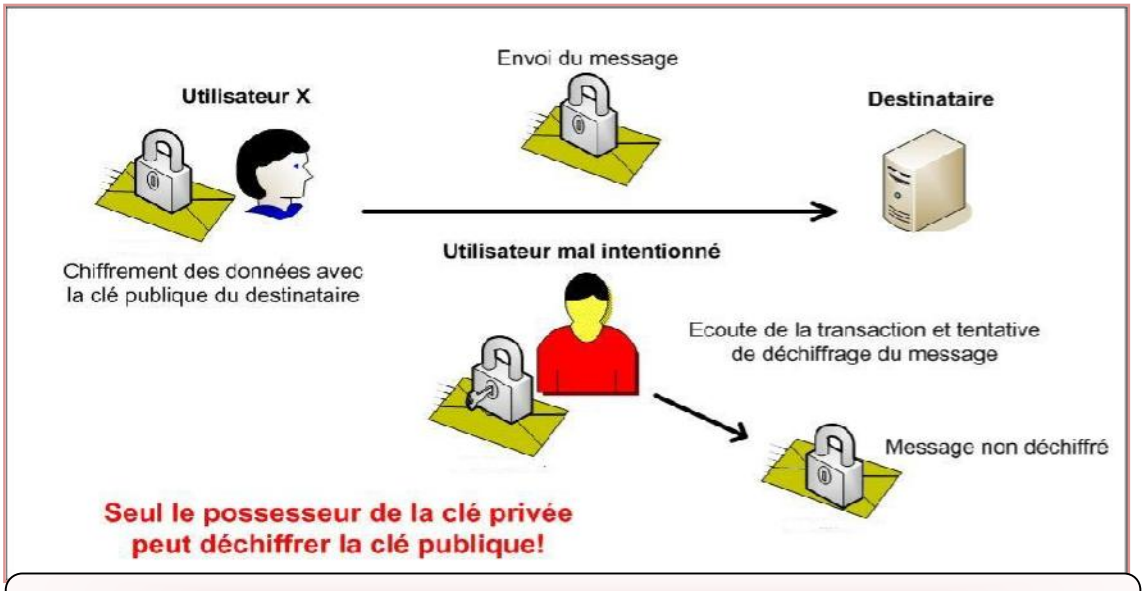


Figure II-6 : exemple attaque (asymétrique)

V -Conclusion :

Dans ce chapitre, nous avons présenté une introduction générale sur la sécurité informatique et les notions de base de la cryptographie, en distingue deux grandes classes des méthodes cryptographique, les cryptographies symétriques à clé secrète et le cryptage asymétrique à clé publique. Le prochain sera consacré aux notions de base d'un réseau virtuel privé (vpn)

chapitreIII:
Réseau Privé Virtuel : VPN

I Introduction :

Un VPN (Virtual Private Network) ou Réseau Privé Virtuel en français est une connexion inter-réseau permettant de relier 2 réseaux locaux différents de façon sécurisé par un protocole de tunnelisation.

Le but de notre travail est de créer un tunnel entre le client et le serveur pour que le client situé dans le réseau externe accède à mon réseau local. Pour une communication avec un poste de mon LAN, le client passera donc par le tunnel jusqu'au serveur OpenVPN et sera ensuite routé sur mon LAN.

II La tunnelisation :

La tunnelisation est un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie.

II.1 Principe :

Le terme tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc normalement incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. De plus, créer un tunnel signifie aussi encapsuler un protocole dans un protocole de même niveau du modèle OSI (IP dans IPSec par exemple). Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer les données à l'entrée et serveur VPN (ou plus généralement serveur d'accès distant) l'élément déchiffrant les données en sortie. **[3]**

Exemple :

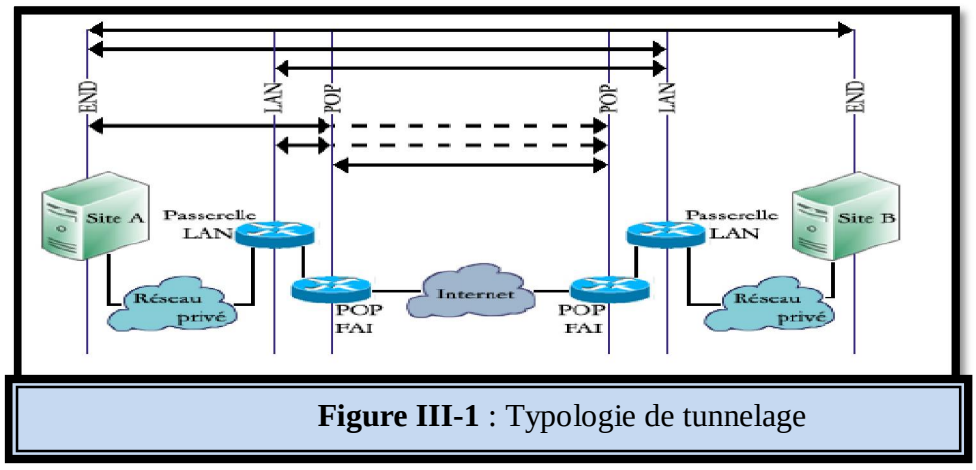


Figure III-1 : Typologie de tunnelage

III Différentes protocoles de tunnelisation :

Il existe de nombreuses implémentations de VPN selon les protocoles utilisés pour Chiffrer les données. De nos jours principalement trois protocoles sont utilisés à grande échelle :

- ***Le Point-to-Point Tunneling Protocol (PPTP)***
- ***Le Layer Two Tunneling Protocol (L2TP)***
- ***Le protocole Secure Sockets Layer (SSL) et IPsec*** **[10]**

III.1 Le protocole PPTP :

Est un protocole développé par US Robotics, 3Com, Microsoft et Ascend Communications. C'est un protocole d'encapsulation de bout en bout sur IP qui permet la mise en place de VPN au-dessus d'un réseau public. L'idée de base du protocole est de permettre l'encapsulation de datagrammes non TCP/IP, comme AppleTalk et IPX, pour être téléportés à travers un réseau IP. Ce protocole utilise quelques concepts de base : **[10]**

PPP (Point to Point Protocol)

Est un protocole de couche 2 qui permet l'échange de paquets entre deux extrémités. Ce protocole est souvent utilisé pour échanger des données entre deux ordinateurs reliés par une ligne sérielle ou téléphonique.

NAS (Network Access Server) est un serveur acceptant la connexion PPP. Un fournisseur d'accès Internet a un NAS sur lequel les clients se connectent à travers une ligne analogique.

PAC (PPTP Access Controller) représente tout élément réseau connecté à une ligne téléphonique client PPTP.

PNS (PPTP Network Server) représente tout élément réseau qui implémente la partie serveur du protocole PPTP. Le PNS est appelé serveur PPTP.

PPTP en tant que protocole ne compte que deux intervenants : le PAC, une machine distante connectée à Internet et le PNS, un serveur appartenant au réseau privé auquel on désire se connecter.

Une session PPTP commence par la connexion d'un ordinateur distant (PAC) au NAS du fournisseur d'accès Internet (FAI). Une connexion PPP est ainsi établie entre l'ordinateur

distant et le serveur du FAI. Par la suite, une connexion de contrôle PPTP est initiée entre le PAC et le serveur d'accès au réseau distant (PNS) permettant de négocier les termes du tunnel PPTP, d'établir la notion de session ou de notifier l'arrivée d'un appel au PNS. Cette connexion peut être initiée par les deux extrémités, que ce soit le PAC ou le PNS. Après les négociations précédentes un tunnel PPTP est créé entre le PAC et le PNS. Ce tunnel véhicule des paquets PPP qui sont encapsulés grâce au protocole générique d'encapsulation GRE (est un protocole de mise en tunnel qui permet d'encapsuler n'importe quel type de paquet dans n'importe quel protocole de niveau 3). Etant donné que le tunnel mis en place véhicule des paquets PPP, une session PPP peut être établie entre le

PAC et le PNS. Ainsi un lien PPP entre les deux extrémités peut être créé sans devoir se connecter directement via une ligne téléphonique ce qui peu réduire le coût de la communication et accroître le taux de transfert. C'est le but de PPTP. Le tunnel entre les deux extrémités, l'ordinateur distant et le PNS, est un tunnel de niveau 2 qui permet le transport de datagrammes de bout en bout (voir figure 3.2).

et qui est en mesure de gérer les protocoles PPP et PPTP. Le PAC est souvent appelé

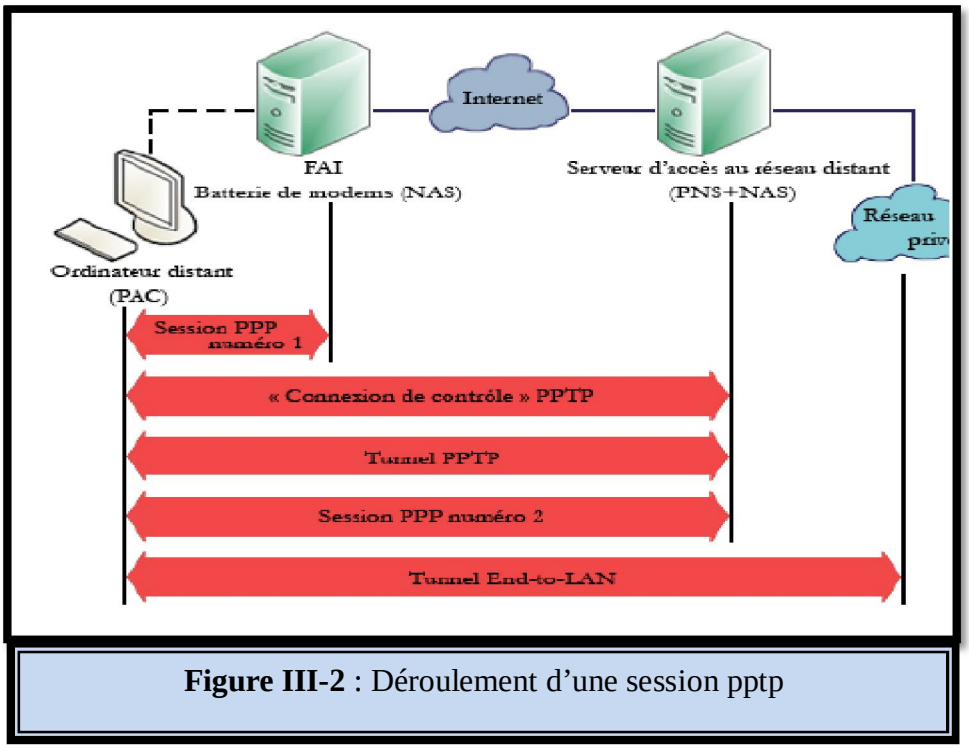


Figure III-2 : Déroulement d'une session pptp

Les données initiales à transmettre sont enrichies d'informations par encapsulations

successives. La figure 3.3 montre la double encapsulation PPP due aux deux sessions ppp négociées : la première avec le NAS du FAI et la deuxième avec le NAS du réseau privé distant. **[6]**

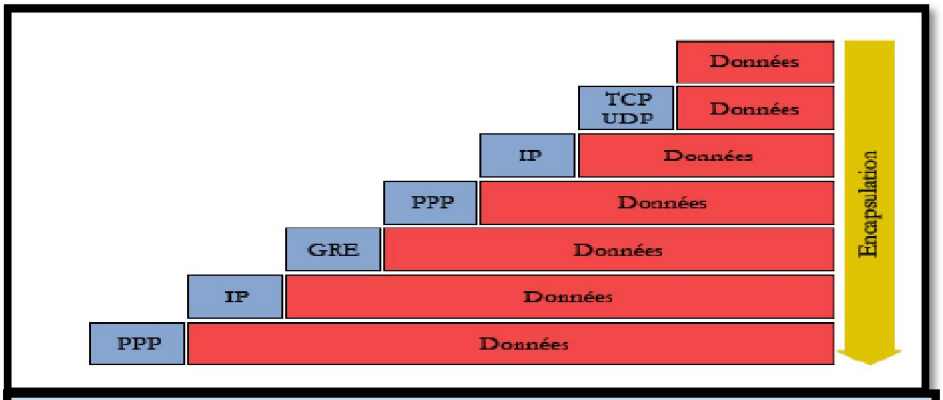


Figure III-3 : Encapsulations successives dans pptp

III.2 Le protocole L2TP (Layer Two Tunneling Protocol)

Le protocole L2TP est un protocole standard de tunnelisation très proche de PPTP. Ainsi le protocole L2TP encapsule des trames protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS). Il faut deux types de serveur pour utilise L2TP :

- *LAC (L2TP Access Concentrator) :* Il sert à fournir un moyen physique pour se connecter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et construit le tunnel vers les LNS.
- *LNS (L2TP Network Server) :* Il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel. **[10]**

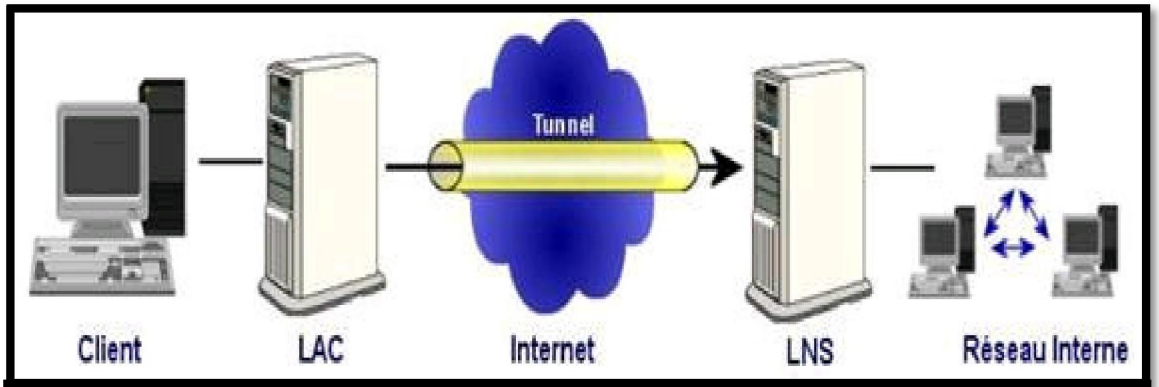


Figure III-4 : Exemple pour le protocole L2TP

III.3 Le protocole SSL : Secure Socket Layer

Il permet de crypter toutes les données échangées entre le client et le serveur de façon à ce que seul le serveur puisse décrypter ce qui vient du client et inversement. Un éventuel pirate ne peut pas, dans un temps raisonnable, décrypter les informations. SSL peut servir de support à n'importe quel protocole en clair comme, HTTP, POP ou IMAP afin de le sécuriser. Il permet d'assurer les trois fonctionnalités suivantes :

- La confidentialité des échanges grâce au cryptage symétrique.
- L'intégrité des données grâce aux fonctions de hachage.
- L'authentification des entités communicantes grâce aux certificats.

Depuis quelques années protocole ssl est utilisé pour sécuriser les VPN. Ce protocole n'est utilisable que pour la sécurisation de flux TCP. Il est largement utilisé pour HTTP, qui devient HTTPS, mais peut être implémenté pour d'autres protocoles comme POP, SMTP.

L'établissement d'un tunnel SSL entre un client et un serveur se fait en plusieurs étapes, avec authentification mutuelle. **[9]**

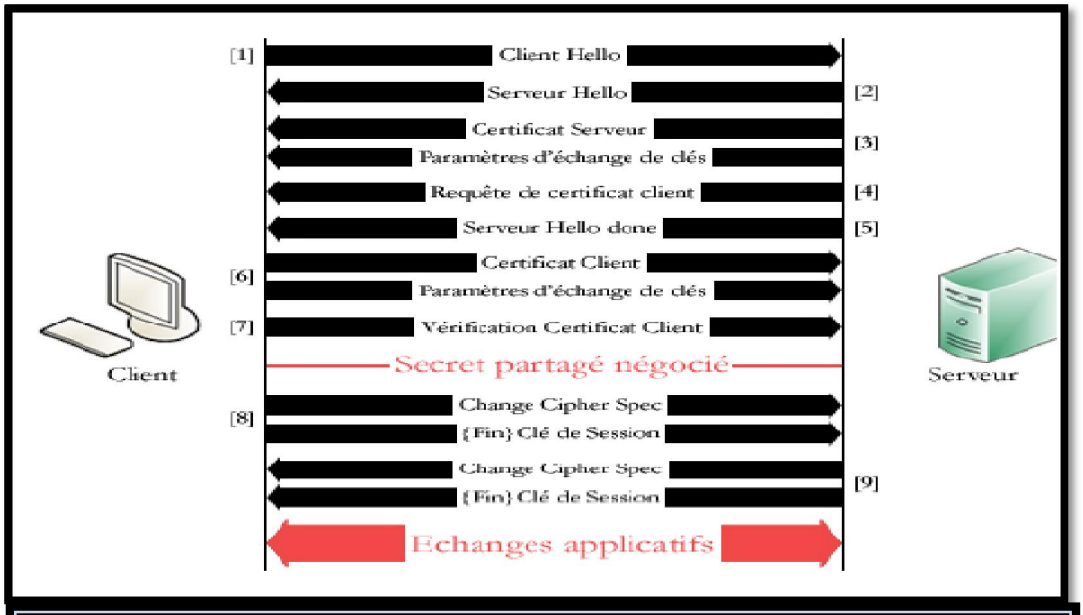


Figure III-5 : Le protocole ssl

III.4 Le protocole IPSec (Internet Protocol Security) :

IPsec est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Il est compatible IPv4 et IPv6. IPsec est basé sur deux mécanismes. Le premier

AH (Authentification Header) pour vise à assurer l'intégrité et l'authenticité des datagrammes IP. Le second ESP (Encapsulating Security Payload) aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement.

IPSec est nativement un protocole de tunnelage. Pourtant, ce protocole propose aussi des mécanismes de sécurisation des échanges entre utilisateurs des VPN. IPSec assure l'authenticité des extrémités, la confidentialité et l'intégrité des échanges grâce aux algorithmes et mécanismes de chiffrement. **[9]**

IV Les différents types de VPN :

Il existe trois types standards d'utilisation des VPNs :

- **Le VPN d'accès :**

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée. **[12]**

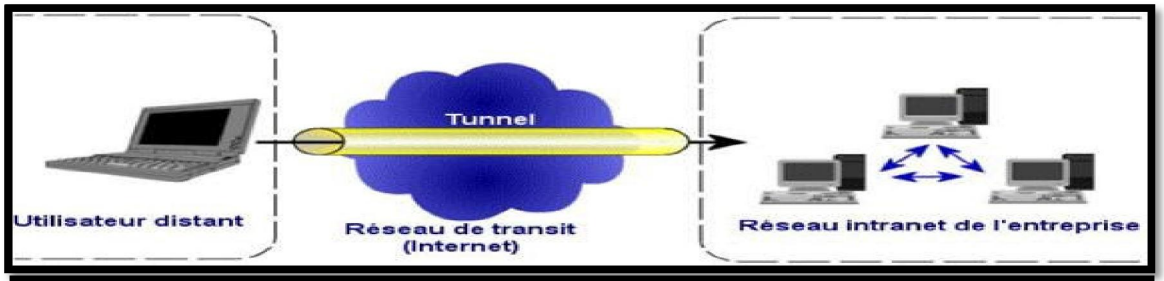


Figure III-6 : Le vpn d'accès

- **L'intranet 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. **[4]**

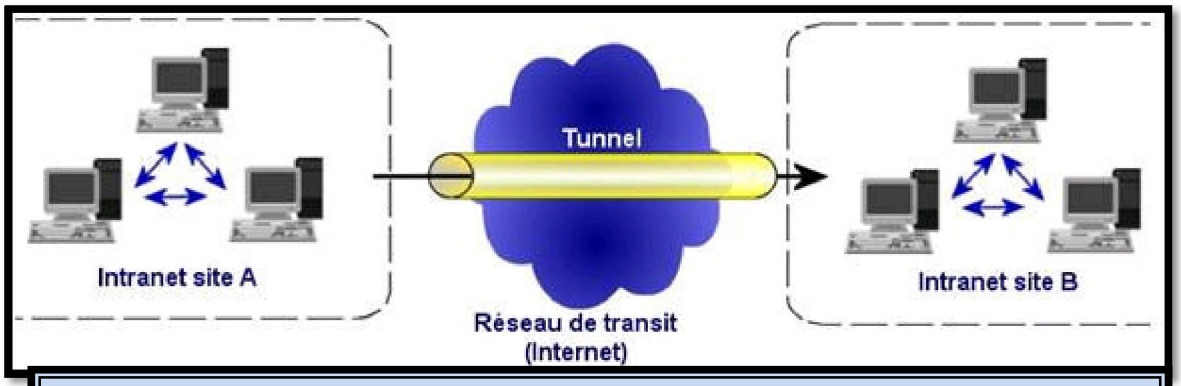


Figure III-7 : L'intranet vpn

- **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 forte des utilisateurs, ainsi qu'une trace des différents accès. **[4]**

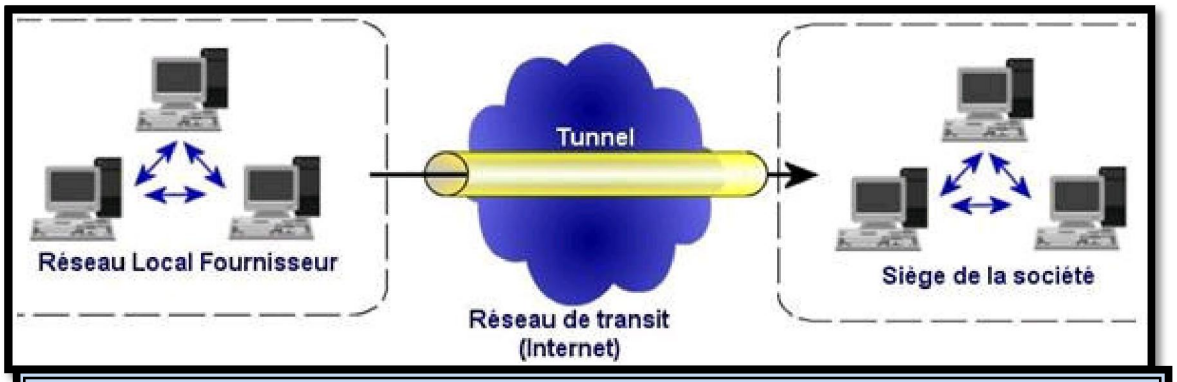


Figure III-8 L'extranet vpn

V Avantages et inconvénients de VPN :

Cout :

Pour mettre en place un VPN, il est nécessaire avant tout de disposer d'une connexion à Internet. Le coût d'une telle connexion est abordable pour l'ensemble des entreprises et des particuliers avec l'avènement de l'ADSL et du câble.

Temps de mise en œuvre :

Lorsque la connexion Internet existe, le temps de mise en œuvre du VPN est fonction de la complexité de la solution ou de la technologie choisie. Il peut aller de quelques jours

à quelques semaines en fonction de la complexité de l'environnement. En revanche, l'ajout d'un site dans un VPN existant peut se faire en quelques heures.

Performances :

La performance d'un VPN est globalement liée à la performance d'Internet. En conséquence, il est impossible de garantir une bande passante ou un temps de réponse entre deux sites interconnectés.

Sécurité :

Les VPN s'appuient sur des technologies de chiffrement robustes et la génération et la mise en place des clés de chiffrement est sous le contrôle du propriétaire du VPN. Le niveau de confidentialité est donc très élevé. Les lignes louées sont également considérées comme très sûres parce que non mutualisées. Mais rien n'empêche une personne mal intentionnée située chez le fournisseur de service d'écouter le trafic. **[6]**

VI Configuration tunnel vpn :

Il existe 2 configurations possibles d'OpenVPN suivant le type de réseau que l'on souhaite mettre en place et suivant le contexte réseau : VPN ponté (interface tap) et VPN routé (interface tun). La configuration VPN routé est plus performante et plus fiable que le ponté. Le VPN ponté est utilisé dans une architecture réseau local, alors que le VPN routé peut aussi bien être utilisé dans cette architecture que pour relier 2 réseaux à travers l'internet. C'est cette configuration routée qui sera utilisée dans notre projet. Voici le schéma global des réseaux pour lequel la configuration proposée est valable. A vous de l'adapter selon votre structure.

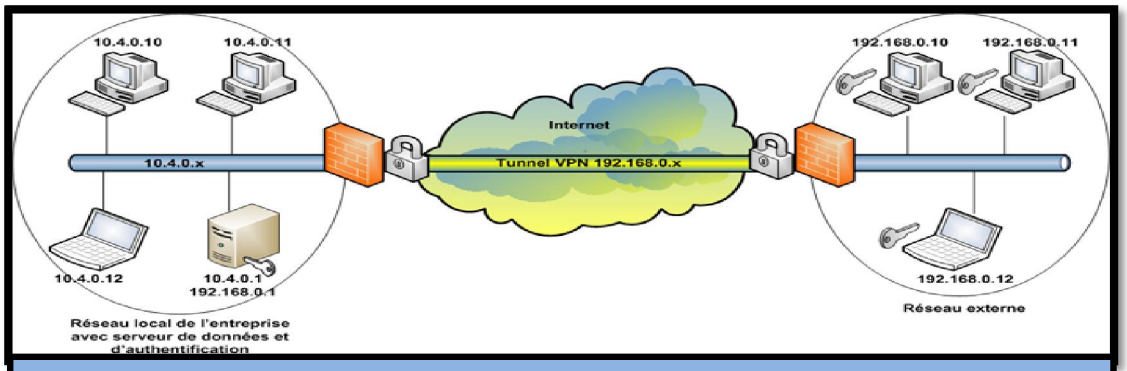


Figure III.9 : Architecture réseau avec tunnel VPN

La création des clés et certificats d'authentification est terminés. Nous allons passer à la configuration du serveur et des clients. Afin de configurer au mieux le serveur et les clients, il est nécessaire de préparer le terrain. **[11]**

VII Conclusion :

Les VPN permettent donc aux réseaux privés de s'étendre et de se relier entre eux au travers d'Internet. Pour s'équiper, les grandes entreprises auront tendance à se tourner vers des solutions clés en main ou des équipements dédiés (boitiers électroniques, routeurs).Les petites entreprises ou les particuliers, quant à eux, iront plutôt vers des solutions logicielles moins coûteuses. L'étude a principalement porté sur l'installation et la configuration d'OpenVPN. Ce logiciel Open Source basé sur OpenSSL à pour, lui, l'avantage d'une mise en place facile. Il existe malgré tout d'autres solutions, comme celle de Microsoft avec le protocole PPTP (Point to Point Tunneling Protocol) et surtout IPSec qui n'a pas été testé ici notamment en raison d'une sous-estimation de sa complexité. En effet, les concepts développés dans IPSec, sa configuration et la mise en place d'un tunnel basé sur cette technologie sont d'un abord autrement plus difficile que celui d'OpenVPN. Malgré tout, cette voie mérite d'être sérieusement explorée, IPSec étant nativement implanté dans les piles IPv4 et IPv6.

Chapitre IV:
Installation et configuration d'un serveur messagerie Postfixun suivi par serveur ftp

I Introduction :

Un serveur de mail est un service de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Pour envoyer ou recevoir des messages, un utilisateur doit utiliser un client de messagerie comme mail ou mutt sous linux. La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

Dans ce chapitre, nous présentons les différentes étapes de configuration et installation d'un serveur de connexion à distance et un serveur de messagerie électronique postfix. Il seront les outils nécessaire pour tester notre réseau virtuel privé vpn.

II Serveur de connexion à distance Telnet

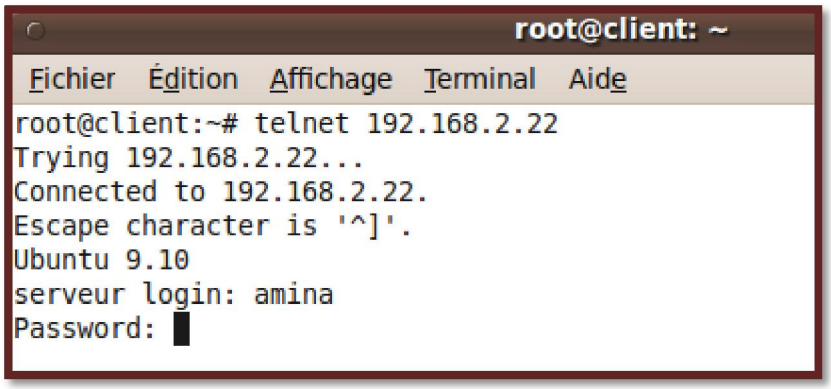
Telnet est le service permettant l'exécution de programmes à distance, en général sur un hôte de type Unix. La commande telnet vous permet de vous connecter sur une machine distante et d'y travailler exactement comme si vous étiez devant cet ordinateur.Lors de la connexion à une machine distante, vous devez fournir un nom d'utilisateur et un mot de passe car l'accès sur le port 23 est contrôlé. **[11]**

II.1 Test de serveur Telnet

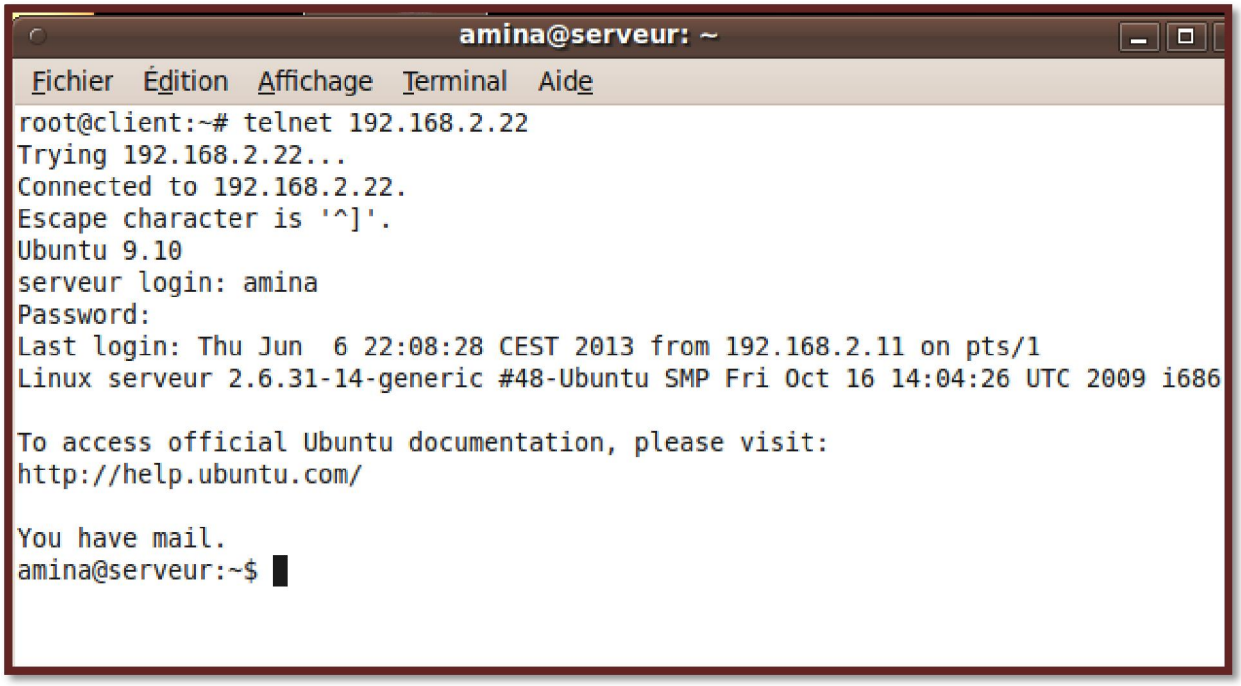
Installer les paquets de Telnet dans deux machines client et serveur, après redémarrer le serveur Telnet par la commande suivante :

Vérification de la disponibilité du serveur telnet :

Taper la commande Telnet avec l'adresse de la machine distance:



Résultat de connexion à la machine distance



II.2 Les étapes d'installation d'un serveur Telnet

Etape 1 : installation d'un client telnet (par défaut est installé sous linux ubuntu)

Etape 2 : installation d'un serveur telnetd (paquet : telnetd_0.17-36_i386.deb)

Etape3 : installation d'un super-serveur internet (paquet : openbsd-inetd_0.20080125-2ubuntu1_i386.deb)

Etape 4 : installation d'un service de sécurité tcpd (paquet tcpd.deb)

Etape 5 : vérifier si le fichier de configuration de super-serveur openbsd-inetd :

Contient la ligne (/etc/inetd.conf) suivante :

telnet stream tcp nowait root /usr/sbin/ftpd usr/sbin/in.telnetd

etape 6 : redémarer le super-serveur par la commande suivante :

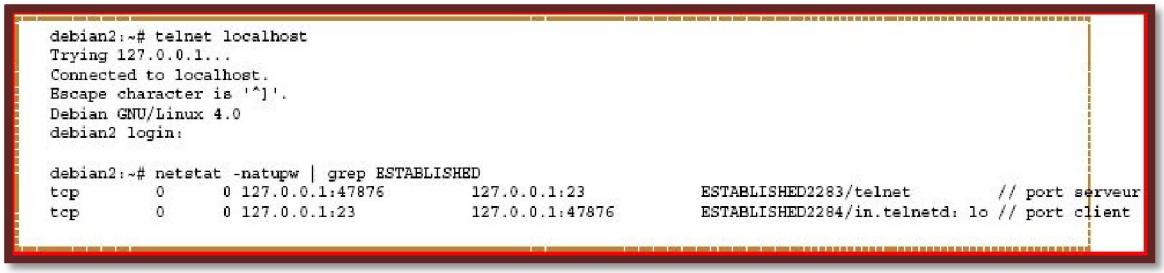
/etc/init.d/openbsd-inetd restart

Etape 7 : vérification si le service est en état marche : exécuter la commande suivante

Ps aux | grep telnet

Etape 8 : teste si le service telnet marche localement : exécuter la commande suivante

telnet localhost ou telnet 127.0.0.1



etape 9 : créer un nouveau utilisateur dans la machine serveur

useradd nom-utilisateur

passwd nom-utilisateur

etape10 : teste si le service telnet marche dans l'intranet (réseau locale)

A partir d'une autre machine cliente qui appartient au réseau locale en essai de faire une connexion a distance à la machine serveur :

Tel que @ip c'est l'adresse ip de la machine serveur (ou exécute le service telnet)

En exécute la commande suivante sur la machine cliente :

telnet @ip

telnet @ip 23 # 23 numéro de port et @ip c'est l'adresse de la machine serveur ou tourne le service telnet

III Serveur messagerie électronique Postfix

La gestion du courrier électronique a longtemps été un problème difficile sous Linux. Ceci principalement du fait de la complexité de paramétrage du serveur de courrier électronique Sendmail. Heureusement, des logiciels efficaces et plus simples comme Postfixsont apparus pour traiter la gestion du courrier électronique.

III.1 Acheminement du courrier électronique

Vous recevez et envoyer probablement des dizaines de messages électroniques par jour. Mais savez-vous ce qui se met en œuvre lorsque vous cliquez sur le bouton Envoyer de votre outil de messagerie ?

1. Celui-ci commence par contacter le serveur utilisé pour envoyer des messages

(MTA, Mail Transport Agent, agent de transport du courrier électronique), à l'aide du protocole SMTP (Simple Mail Transfer Protocol).

Il s'agit d'un programme (sendmail, postfix, Microsoft Exchange Server, etc.) qui accepte le contenu de votre message, ainsi que tous les en-têtes que votre outil de messagerie a pu ajouter.

2. Le serveur trait ensuite les adresses de l'émetteur et des destinataires, ainsi que les entêtes. En fonction des informations collectées, le serveur décide du traitement du message.

3. Celui-ci peut être acheminé immédiatement vers une boîte aux lettres locales; il peut être placé dans une file d'attente, jusqu'à son acheminement; ou il peut être transmis à un autre serveur.

4. Finalement, un serveur distant acceptera le message pour le placer dans une boîte aux lettres locale. Les boîtes aux lettres peuvent être organisées de manières très diverses ; sous Linux, il s'agit d'un fichier (/var/spool/mail/) contenant tous les messages non encore lus par le destinataire.

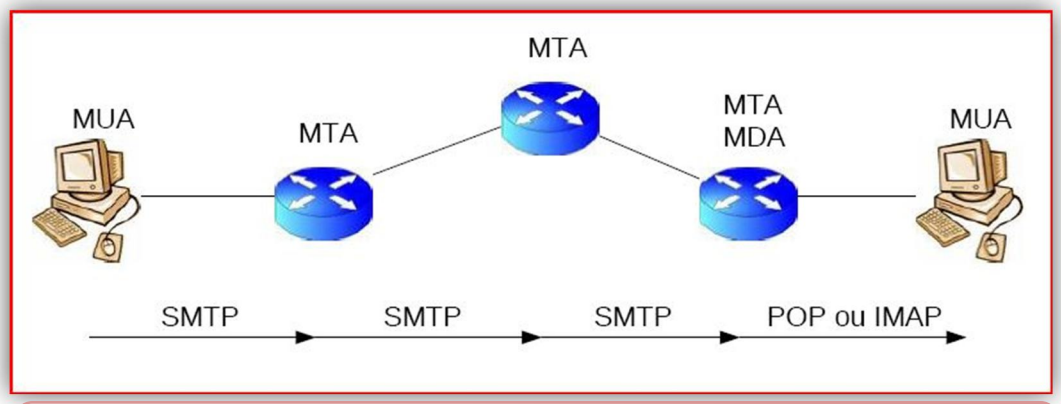


Figure IV-1 : messagerie électronique

5. Après un certain laps de temps, le message est retiré de la boîte aux lettres par l'outil de messagerie du destinataire (MUA, Mail User Agent : client messagerie). Un client s'exécutant sur la même machine que le serveur peut lire directement les messages dans le fichier approprié. A travers le réseau, il est nécessaire d'utiliser un protocole, par

exemple POP3 (Post Office Protocol : MDA : serveur de récupération des courriers électroniques). **[16]**

MUA (Mail User Agent) : client messagerie

L'agent utilisateur (MUA) est le programme dont vous vous servez pour communiquer avec le système de courrier électronique (client de courrier électronique). Sous Linux l'agent utilisateur le plus simple se nomme mail, mutt et pine.

Il s'agit d'un client très limité; incapable d'utiliser le protocole POP3, il ne peut lire que les messages d'une boîte aux lettres locale.

MTA (Mail Transfert Agent)

Un agent de transport (MTA, Mail Transport Agent), aussi appelé serveur de messagerie, comme postfix et sendmail. Il est utilisé pour l'envoi des courriers électroniques en utilisant le protocole SMTP (Simple Mail Transport Protocol : Port 25).

Le schéma global de système de messagerie

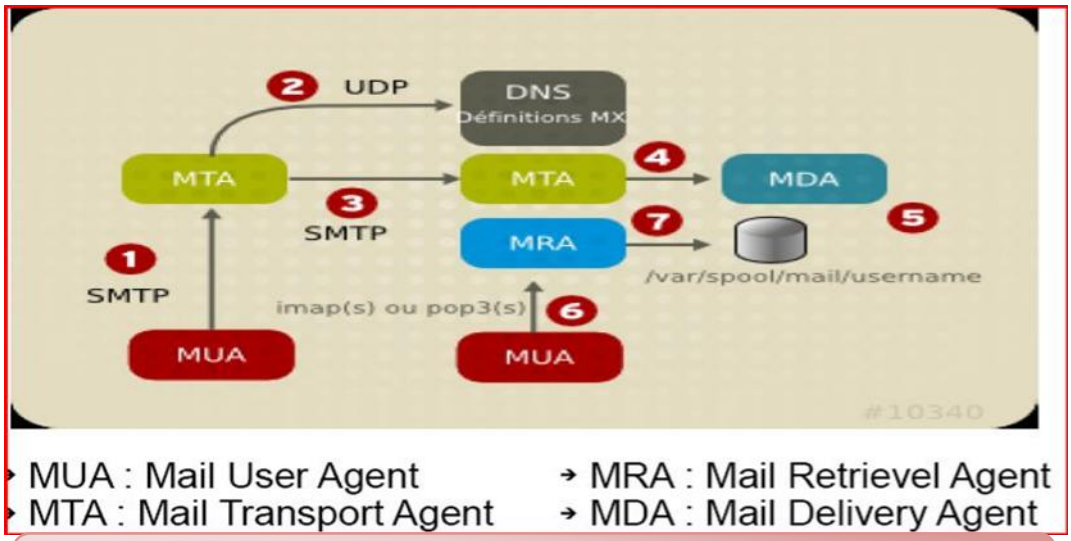


Figure IV-2 : Le schéma global de système de messagerie

III.2 Protocoles de messagerie électronique

Si l'on considère la quantité de MTA et de MUA disponibles, on peut légitimement se demander comment ces programmes réussissent à interagir. Le secret réside dans la standardisation.

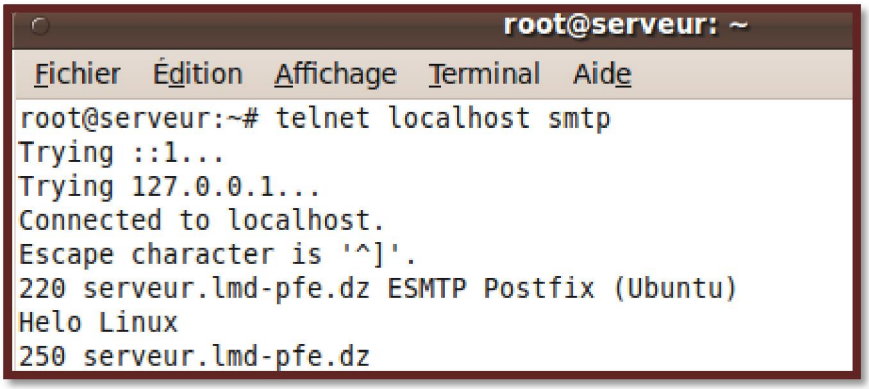
Tous les systèmes de messagerie utilisent un ensemble de protocoles commun. Tous les agents Linux se servent de répertoires, formats et mécanismes d'accès connus. En conséquence, même si un message peut être manipulé par une dizaine de programmes différents lors de son acheminement entre l'émetteur et le destinataire, le résultat final est la mise en place d'un système fiable.

SMTP : le protocole de transfert des messages

Simple Mail Transport Protocol Port 25

Tous les serveurs de courrier électronique reçoivent les messages à l'aide d'un mécanisme commun : SMTP, Simple Mail Transfert Protocol. Que le message soit envoyé par votre agent ou par un autre serveur, la méthode reste la même : le système émetteur se connecte au serveur à l'aide du protocole SMTP, indique l'auteur et le destinataire du message, et transfère le message proprement dit.

Voici un exemple qui illustre ce point :

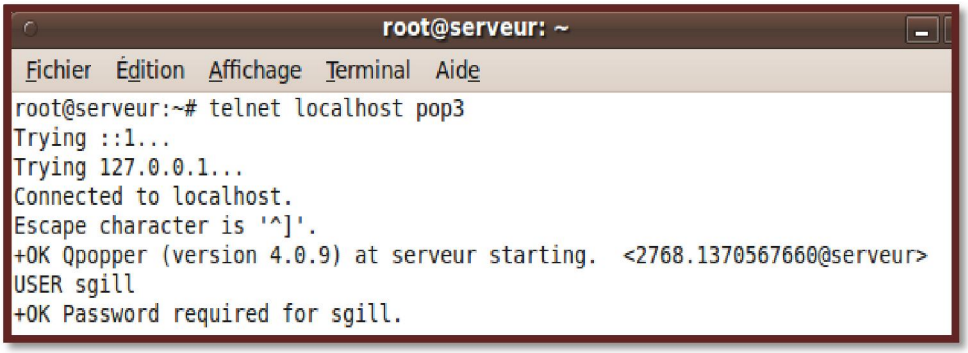


POP3 : le protocole serveur/destinataire (MDA) : Mail Delevred Agent

Protocole de récupération des courriers électroniques

Post Office Protocol Port 110

Le protocole SMTP permet d'acheminer un message un message vers un serveur de messagerie (MTA). Mais il n'offre aucun moyen d'amener le message jusqu'à sa destination finale, c'est-à-dire jusqu'à l'agent utilisateur (MUA) s'exécutant sur l'ordinateur du destinataire.



En d'autres termes, il est possible d'envoyer un message vers un serveur, via SMTP, mais il n'est pas possible de demander un message à un serveur. La lecture d'une boite aux lettres passe par un autre protocole, qui est souvent POP3 (Post Office Protocol). POP3 est facile à comprendre.

Tout comme SMTP, il peut être utilisé manuellement pour se connecter à un serveur :

La boite à la lettre

Sur un système Linux, votre boite aux lettres est un fichier situé dans le répertoire */var/spool/mail* et portant votre nom de login. Chaque message, dans ce fichier, débute par une ligne *From :* Cette ligne respecte un format bien défini, qui permet aux programmes de reconnaître la fin d'un message et le début du suivant. Après la ligne *From :* on trouve les différents en-têtes, que nous expliquerons dans la section suivante. Le dernier en-tête est suivi d'une ligne vierge, après laquelle se trouve le corps du message.

III.3 Configurer un serveur de mail avec postfix :

Le *Mail Transfer Agent Postfix*

Un *Mail Tranfer Agent (MTA)*, ou *SMTP daemon*, permet de transmettre des messages (mail) d'un ordinateur à un autre.

Pour envoyer un mail, on se connecte au serveur *SMTP* en s'authentifiant en utilisant un client de mail (outlook, thunderbird, mutt ...), qui transmet le message.

Le serveur *SMTP* applique des filtres (souvent antispam) sur le mail. Le *MTA* postfix a aussi des fonctionnalités de *Mail Delivery Agent (MDA)* qui lui permettent de livrer le courrier dans une mailbox (*mbox* ou *Maildir*).

Les clients utilisateur utilisent ensuite un serveur POP (Pop : serveur de récupération des courriers électroniques - MDA Mail Delivery Agent) pour aller chercher le mail dans la mailbox qui se trouve sur le serveur.

La configuration de base de *Postfix* se fait dans le fichier /etc/postfix/main.cf. On y spécifie essentiellement les filtres à appliquer au mail pour éviter que les utilisateurs ne reçoivent trop de spams, mais aussi pour éviter que le *MTA* ne soit utilisé comme relai par des spammeurs.

Postfix est un serveur qui peut seulement envoyer du courrier électronique

Les adresses email seront du style: nom_de_la_personne@nom_de_votre_domaine. Il y aura deux serveurs pour la réception des messages, un **POP** et un **Imap**

Le **Pop** permet de récupérer tous les courriers du serveur vers le client, tandis que l'**Imap** se synchronise avec le serveur, donc tous les mails restent sur le serveur pour ce dernier.

III.3.1 Installation du serveur Postfix

Installer le paquet de postfix, Pendant l'installation de Postfix, vous allez voir apparaître des fenêtre pour la configuration du serveur de mail, suivez ci-dessous le paramétrage de votre serveur.

1- Choisissez l'option "Site Internet"

2- Indiquez le nom des domaines autorisé, exemple lmd-pfe.dz (nom de domaine) .

Voila l'installation est terminée, allez voire dans le dossier: **/etc/postfix/**, si vous avez les fichiers suivants :

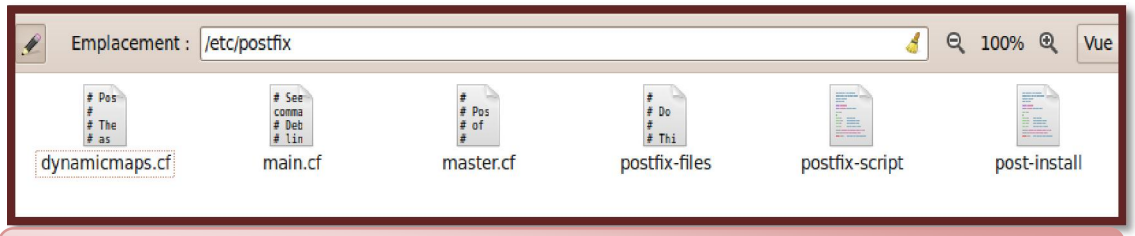


Figure IV-3 : fichiers de configuration de postfix

III.3.2 Configuration du serveur Postfix

Le fichier principale se nome **main.cf**, c'est le fichier principale de configuration du serveur de mail. Il est déjà rempli avec les options définies lors de l'installation, donc

Editez le fichier "**main.cf**", et modifier son contenu par les paramètres suivant :

Le fichier de configuration main.cf :

Ici regroupe les paramètres de fonctionnement de postfix. Ne pas modifier cette partie au risque de faire planter le serveur.

```
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
program_directory = /usr/lib/postfix
smtpd_banner = $myhostname ESMTP $mail_name
setgid_group = postdrop
biff = no
```

On définie les fichiers pour l'emploie des alliasses. Laisse tel que nous allons tout à l'heure configurer les ailasses

```
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

Maintenant on définie le domaine. Remplacer par le votre, exemple de nom de

Domaine : **lmd-pfe.dz**

```
mydomain = lmd-pfe.dz
```

Ensuite en met le nom d'hôte du serveur de mail. Remplacer "**serveur**", par le nom de votre serveur : serveur.lmd-pfe.dz

```
myhostname = serveur.lmd-pfe.dz
```

L'extension pour les mails envoyés depuis la machine. Remplacer "**lmd-pfe.dz**", par l'extension que vous désirez.

```
myorigin = $mydomain
```

Puis il faut indiquer la liste de domaine autorisé par Postfix.

```
mydestination = $myhostname, localhost.$mydomain, $mydomain
```

Ensuite on indique à Postfix dans quels réseaux il doit travailler. La remplacer "**192.168.2.0/24**", par votre réseau.

```
mynetworks = 192.168.2.0/24, 127.0.0.0/8
```

Vous pouvez utiliser un quota pour la taille des boîtes aux lettres. A noter que si la valeur est de zéro, alors la boîte est illimitée.

```
mailbox_size_limit = 0
```

Indiquer le type de réseau utilise : réseau local :

```
myneworks style = subnet
```

Le répertoire de stockage des courriers électroniques reçus

```
mail_spool_directory = /var/mail
```

Déclaration le serveur messagerie postfix dans le serveur DNS de résolution de nom **:**

Dans la zone de résolution direct : **lmd-pfe.z**

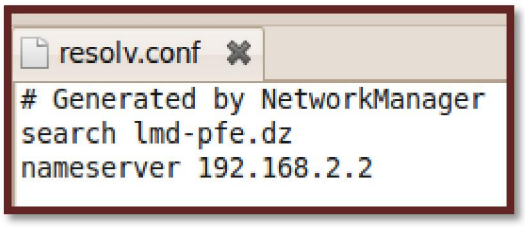
```
mail        IN      CNAME   serveur.lmd-pfe.dz.
@           IN      MX   5  serveur.lmd-pfe.dz.
```

Après démarrer le service Dns bind9 par la commande suivante :

/etc/init.d/bind9 restart

```
root@serveur: ~
Fichier  Édition  Affichage  Terminal  Aide
root@serveur:~# /etc/init.d/bind9 restart
* Stopping domain name service... bind9                    [ OK ]
* Starting domain name service... bind9                    [ OK ]
```

Enfin modifier le fichier **resolv.conf** et ajouter les deux lignes suivantes : (le fichier **resolv.conf** se trouve dans le chemin suivante **: /etc/resolv.conf**)



III.4 Installation d'un client messagerie (MUA) mail user agent :

Installation d'un client messagerie mutt (MUA)

Mutt permet de gérer une messagerie électronique sous UNIX. Il permet donc d'envoyer et de recevoir des messages, de gérer des boîtes aux lettres, d'utiliser des alias.

Installer le paquet mutt

apt-get install mutt

Tapez la commande mutt sur le shell pour lancer le client messagerie mutt

Vous avez l'écran suivant :

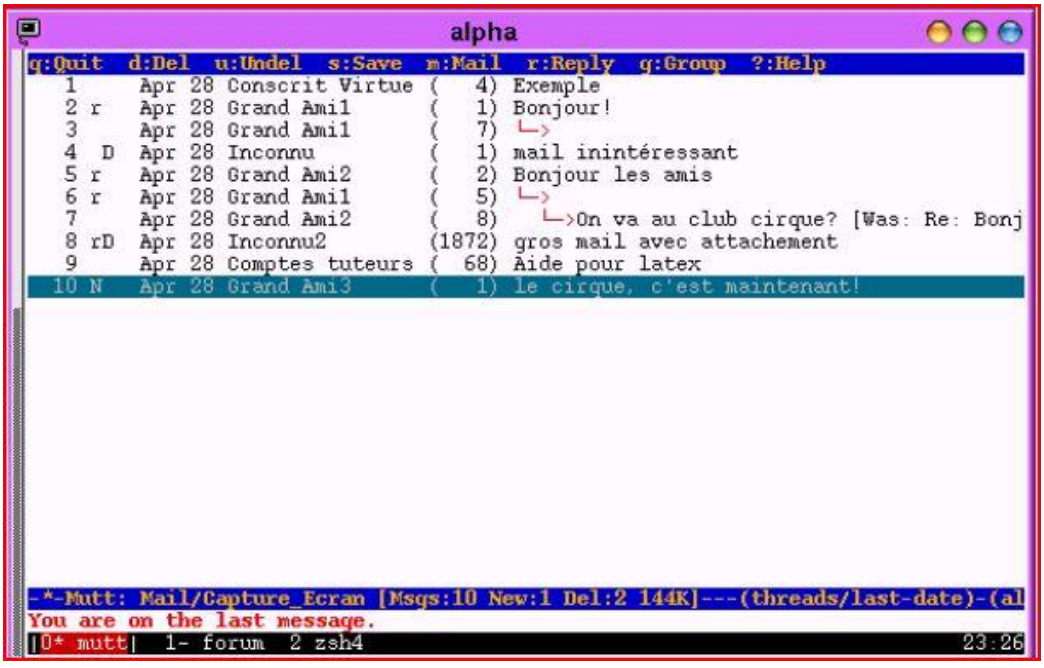


Figure IV- 4 : client messagerie mutt

Envoyer un courrier électronique par mutt

Pour envoyer un courrier, tapez « **m** » (message ou *mail*). mutt vous demande successivement :

To: : nom du destinataire.

Subject : le sujet du courrier. Il faut obligatoirement en mettre un.

Votre éditeur se lance et vous pouvez taper le texte du message. Quand vous sauvez et quittez l'éditeur, cet écran apparaît :

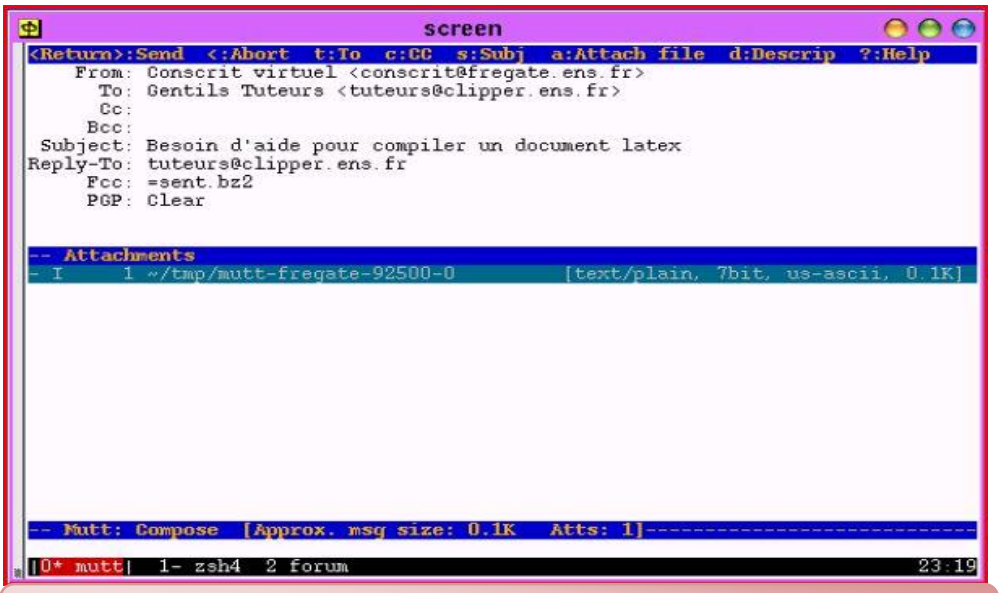


Figure IV-5 : envoi un message par mutt

IV Installation et Configuration du serveur FTP :

De nombreux transferts de fichiers ont lieu à chaque instant sur internet. Le vieux protocole ftp (File Transfert Protocol) est toujours aussi utilisé parce qu'il est simple et rapide à mettre en place. Pour les utilisateurs, un transfert FTP est aujourd'hui facilité grâce à divers clients FTP totalement graphique comme FileZilla.

L'objectif de TP est d'installer et configurer un serveur ftp (vsftp)

IV.1 Configuration de VsFTPd sous Ubuntu

Installation

L'installation sous Ubuntu est comme toujours des plus simples :

$ sudo apt-get install vsftpd

VsFTPd se configure via le fichier vsftpd.conf, positionné dans /etc sur la majorité des distributions.

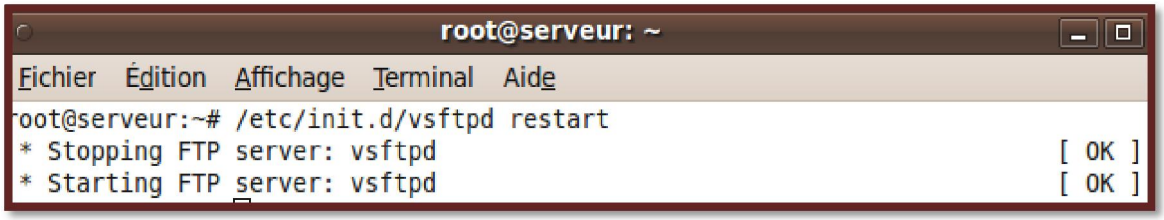
Le fichier de configuration par défaut est très restrictif, il n'autorise que les connexions anonymes, en lecture seule. Il fait écouter le serveur sur toutes les interfaces disponibles, sur le port 21, et peut être tout à fait suffisant pour mettre en place un simple partage de fichier accessible à tous.

Démarrer le serveur FTP

sudo /etc/init.d/vsftpd restart

arreter le serveur FTP

sudo /etc/init.d/vsftpd stop



V Conclusion

La messagerie électronique est devenue le système critique d'une entreprise puisque c'est le cœur de toutes communications entre employés. Le fonctionnement de ce service impactera directement sur l'activité d'une entreprise et dès lors, vous devrez réellement penser et préparer toute manipulation sur vos serveurs.

Si un service doit être favorisé (système de sauvegarde, sécurité, qualité de service, etc.), c'est celui ci. Nous avons décris dans ce chapitre les notions de base d'administration d'un serveur de messagerie plus un serveur de transfert de fichier vsftp.

Dans le chapitre suivant, nous présentons notre travail qui est basé sur la sécurité d'un service de messagerie électronique via un tunnel sécurisé VPN.

Chapitre V :
Scénario pour protéger les messages échangées par un service de messagerie électronique et un service de transfert des fichiers via openvpn

I Introduction :

OpenVPN est un logiciel libre permettant de créer facilement une liaison VPN site à site.

OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance ou de certificats. Il fonctionne sur un mode client/serveur, ce qui implique son installation sur les 2 sites distants, l'un côté client, l'autre côté serveur.

Dans ce chapitre, nous présentons comment en peut sécuriser un service de messagerie électronique et un service de transfert de fichier ftp via un tunnel sécurisé vpn.

II Architecture de réseau virtuel :

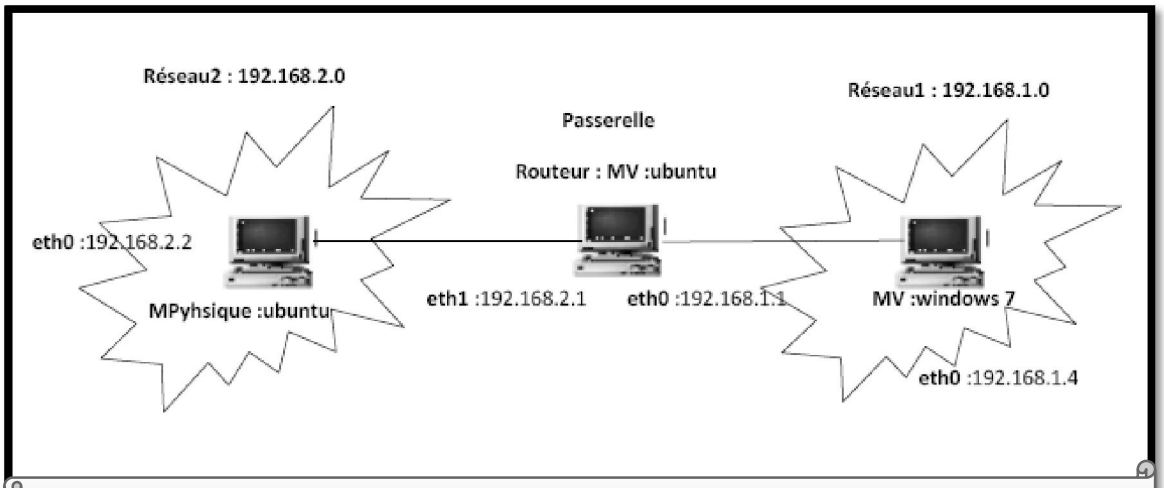


Figure V-1 : architecture de réseau virtuel

II.1 Configuration d'un routeur dans une machine :

Machine virtuelle ubuntu (routeur) :

Dans la machine virtuelle routeur on doit crée deux cartes réseaux virtuel :

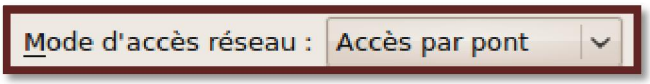
Aller dans la configuration réseau :

Carte réseau1 :

Choisir

Carte réseau 2:

Choisir

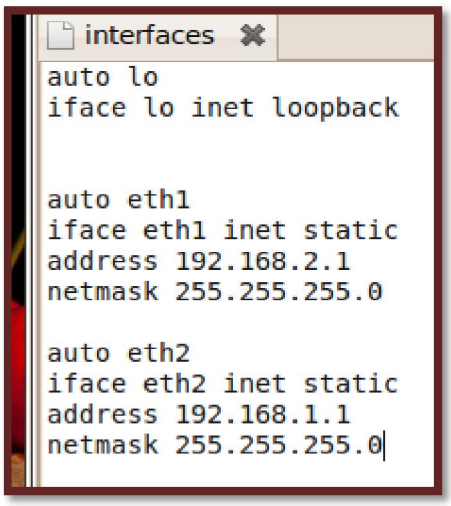


Configurer les deux cartes réseaux

eth1: 192.168.1.1

eth0 : 192.168.2.1

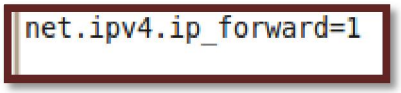
Aller ver le fichier /etc/netwok/interfaces est ajouter les lignes suivantes :



Donc activation la propriété de routage de la passerelle:

Aller vers le chemin **/etc/sysctl.conf** est activé la ligne suivante :

Premièrement en lève le # et ajoute



Machine hôte physique ubuntu :

Ajouter la configuration suivante dans le fichier /etc/network/interfaces :

```
auto lo
iface lo inet loopback
auto eth1
iface eth1 inet static
address 192.168.2.2
netmask 255.255.255.0

up route add -net 192.168.1.0/24 gw 192.168.2.1
```

Teste la connectivité entre les deux machines **:**

Teste le Ping :

Machine physique ubuntu :@IP: 192.168.2.2

- ping 192.168.1.1 (carte réseau1 de passerelle machine virtuelle ubuntu)

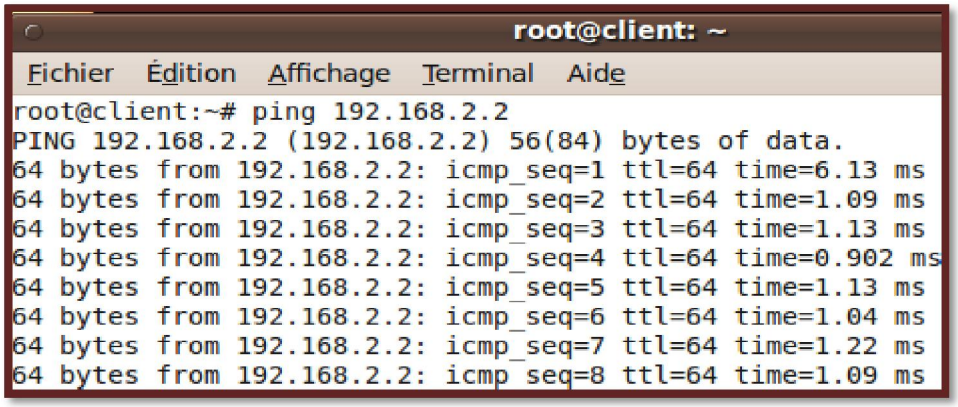
```
root@serveur: ~
Fichier  Édition  Affichage  Terminal  Aide
root@serveur:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.835 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.908 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.845 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.02 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.797 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=0.919 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=0.862 ms
```

- ping 192.168.2.1 (carte reseau2 de passerelle machine virtuelle ubuntu)

```
root@serveur: ~
Fichier  Édition  Affichage  Terminal  Aide
root@serveur:~# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=9.00 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.843 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.854 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.849 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=64 time=1.14 ms
64 bytes from 192.168.2.1: icmp_seq=6 ttl=64 time=0.804 ms
64 bytes from 192.168.2.1: icmp_seq=7 ttl=64 time=0.918 ms
64 bytes from 192.168.2.1: icmp_seq=8 ttl=64 time=0.891 ms
```

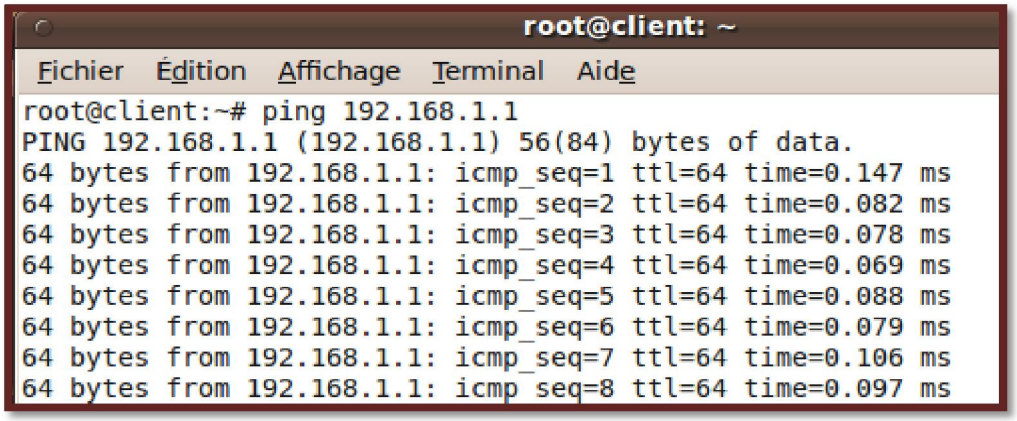
Machine virtuelle ubuntu qui joue le rôle d'une passerelle (routeur)

- Ping 192.168.2.2 (machine physique hote ubuntu)

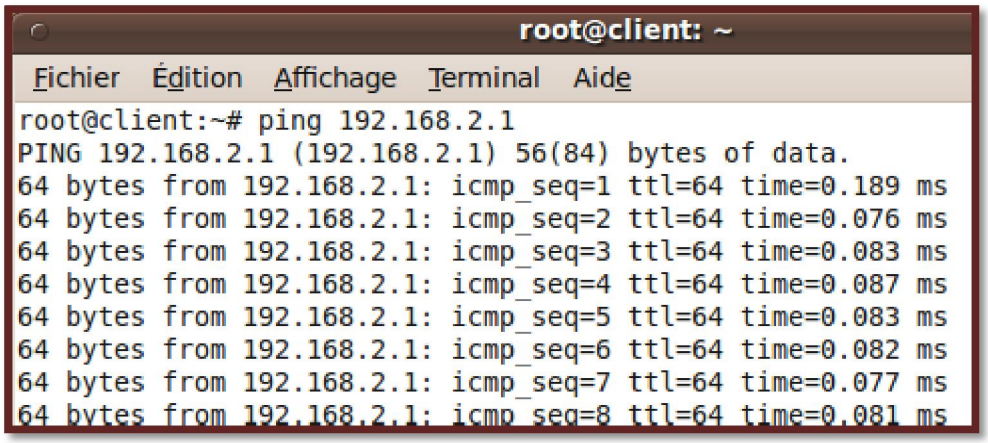


- Ping 192.168.1.1 (carte réseau1 de la passerelle)

:



- ping 192.168.2.1 (carte reseau2 de la passerelle)

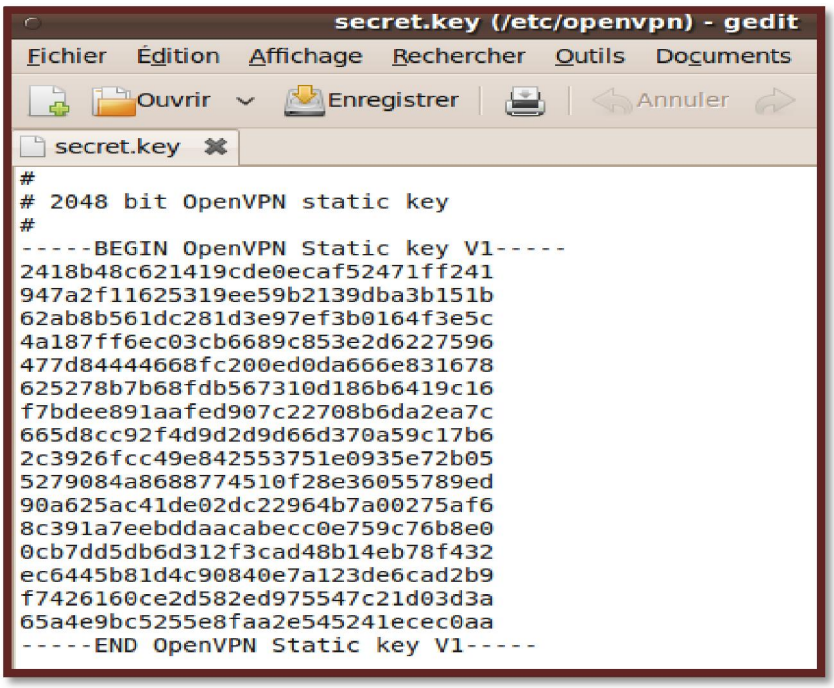


III L'installation et configuration de serveur openvpn

Installation d'openvpn sur les deux machine serveur et client.

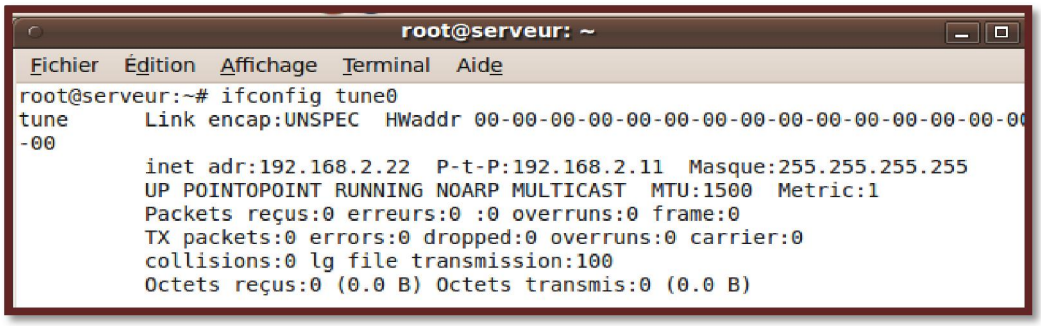
Les étapes d'installation openvpn dans la machine physique (serveur)

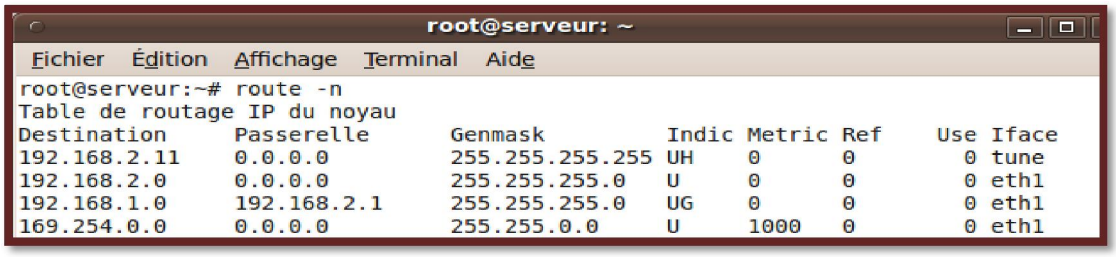
Génération et partage d'une clé secrète comme suivant :



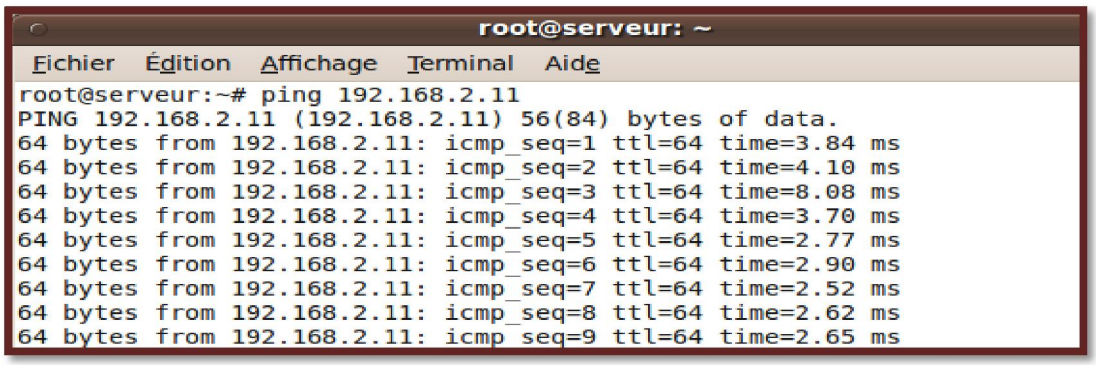
Configuration de la liaison sur machine physique (serveur). Le paramètre ifconfig est suivi de l'adresse IP associée à la carte virtuelle locale « tune0 » suivie de l'adresse IP de la carte distante comme suivant :

Vérification des interfaces et des routes comme suivant :





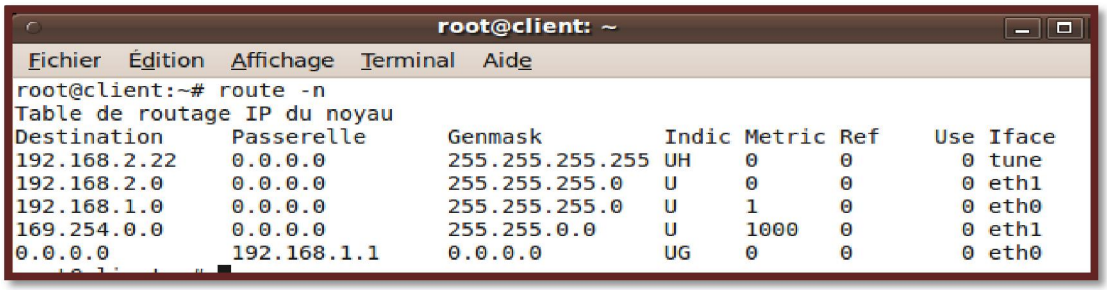
Test de la liaison virtuelle comme suivant :



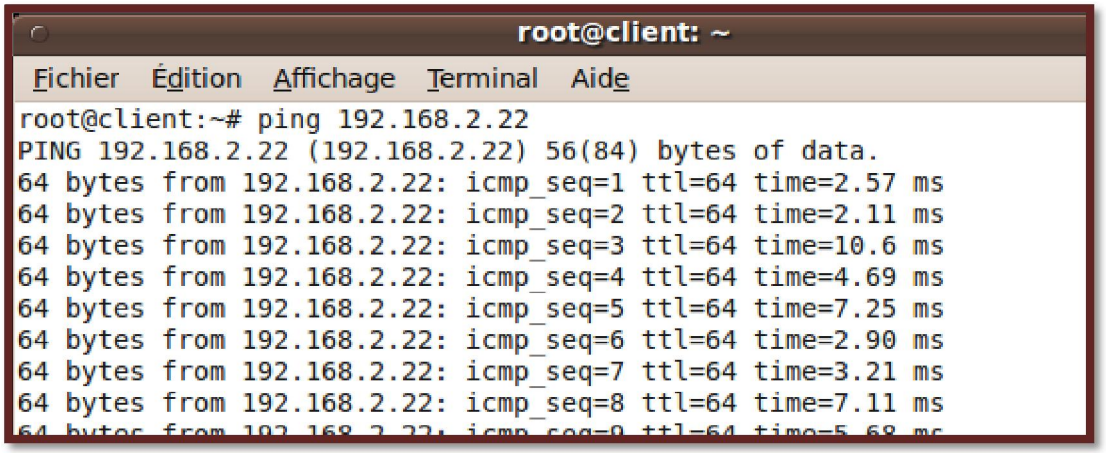
Configuration de la machine virtuelle (client)

Configuration de la liaison sur machine virtuelle (client) comme suit :

Vérification des interfaces et des routes comme suivant :



Test de la liaison comme suivant :



IV Logiciel de capture des paquets échangés dans un réseau

WIRESHARK :

Wireshark est un logiciel permettant de capturer et de décoder des trames circulant sur un réseau. Il fonctionne aussi bien sur Windows que Linux. L'objectif d'utiliser wireshark est de capturer les différentes trames dans les interfaces réseau physique et le tunnel de vpn.

Depuis le menu Démarrer, lancer l'application Wireshark. Vous devriez voir apparaître une fenêtre similaire à celle-ci : **[14]**

La fenêtre principale de **Wireshark** comporte trois zones

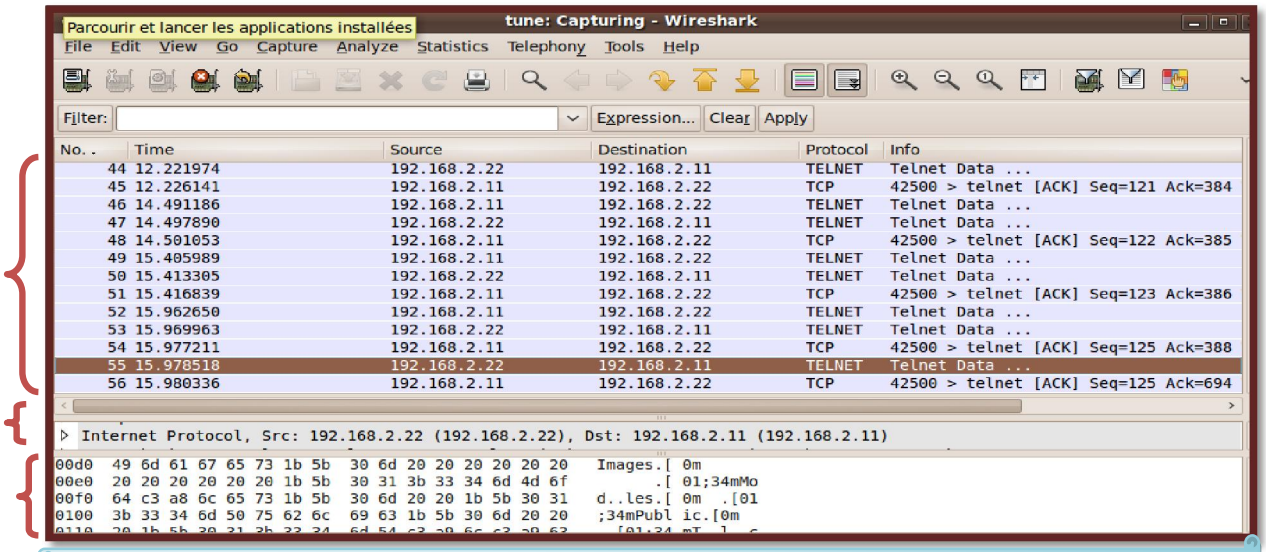


Figure V-2 : capture wireshark

Zone du haut : affichage des trames reçues dans l'ordre chronologique.

Zone du milieu : décodage des informations, protocoles par protocoles.

Zone du bas : affichage de la trame en hexadécimale**.**

V Sécurisation des messages de courriers électronique via un tunnel vpn

V.1 Installation et lancement d'un client messagerie mutt (MUA)

Mutt permet de gérer une messagerie électronique sous UNIX. Il permet donc d'envoyer et de recevoir des messages, de gérer des boîtes aux lettres, d'utiliser des alias. Installer le paquet mutt et Tapez la commande **mutt** sur le shell pour lancer le client messagerie mutt Vous avez l'écran suivant :

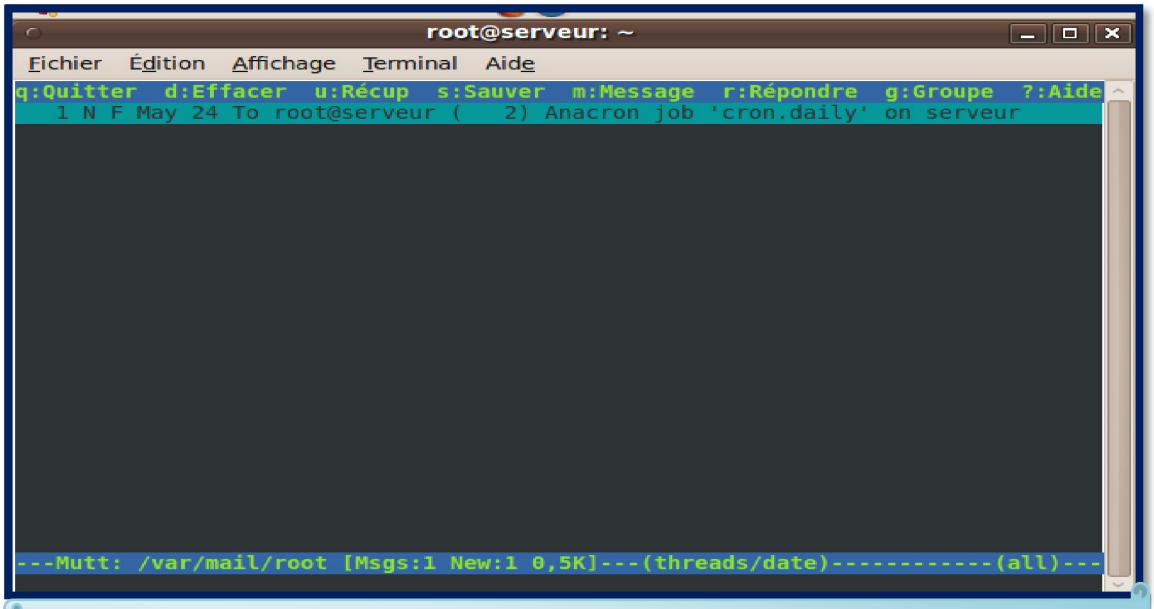
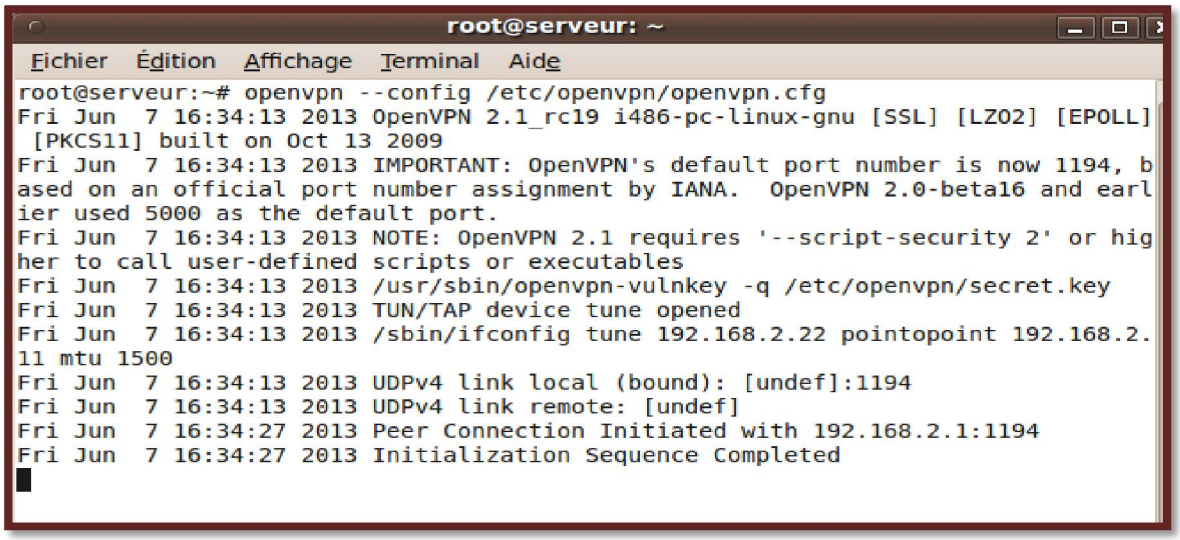


Figure V-3 : client messagerie électronique mutt

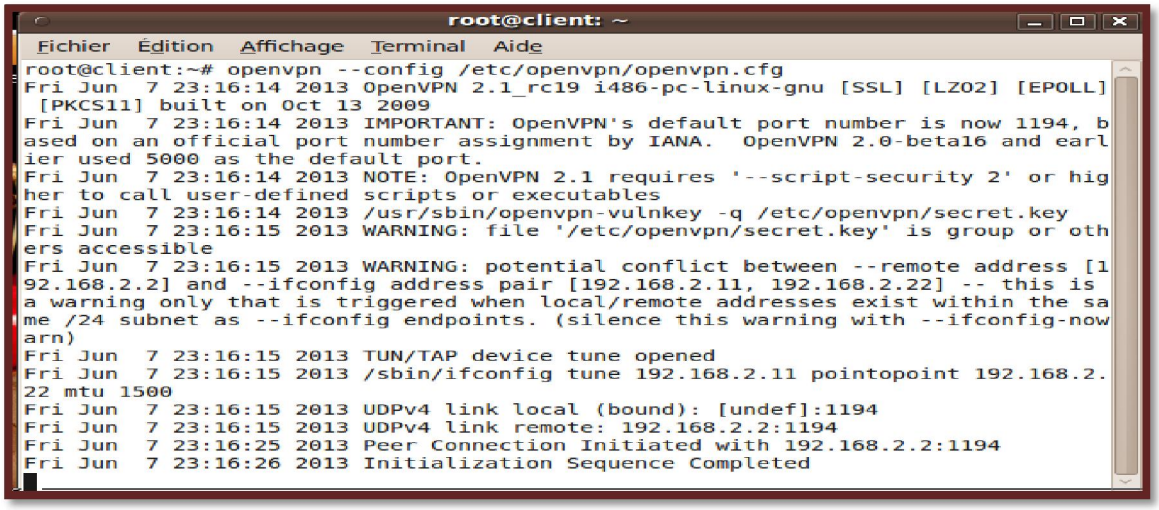
V.2 Les étapes pour Envoyer un courrier électronique par Mutt avec les captures de wireshark :

Étape 1: lancer le tunnel entre deux machines client- serveur comme suivant :

- Machine physique (serveur)



- Machine virtuelle (client)



Étape2: taper la commande mutt sur le Shell pour envoyer un message comme suivant :

Voila le message qui sera transmis dans le tunnel vpn et qui sera crypté et chiffré. Cela est bien monté dans l'analyse des paquets capturés par wireshark.

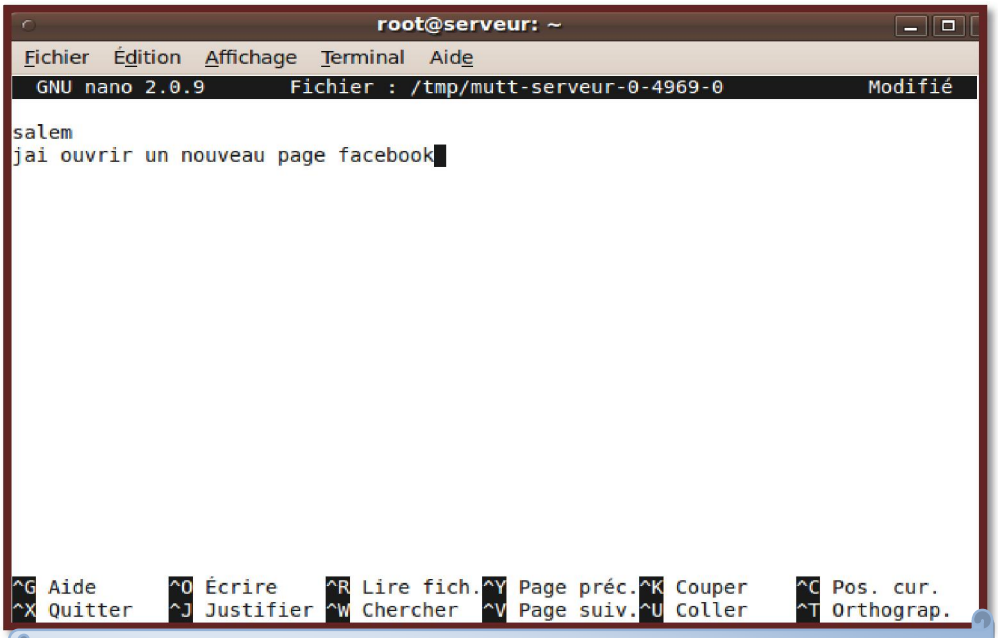
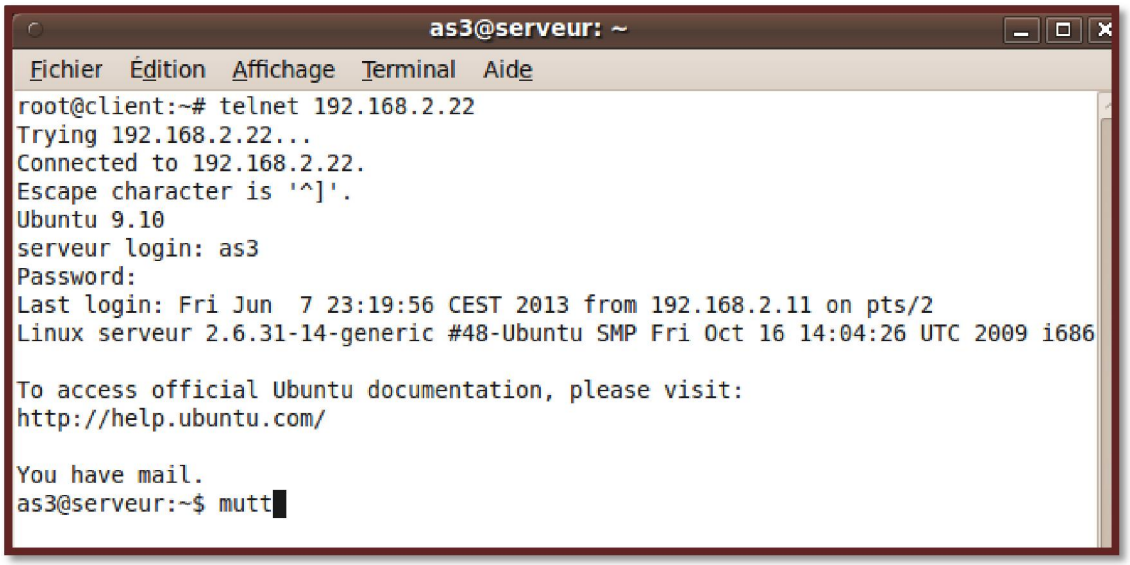


Figure V-4 : message envoyé via mutt

Étape 3 : lancer wireshark en moment de la connexion de la machine virtuelle ubuntu (client) au serveur de la messagerie électronique



Voila le résultat capturé par wireshark a partir de l'interface du tunnel qui une adresse ip 192.168.2.22:

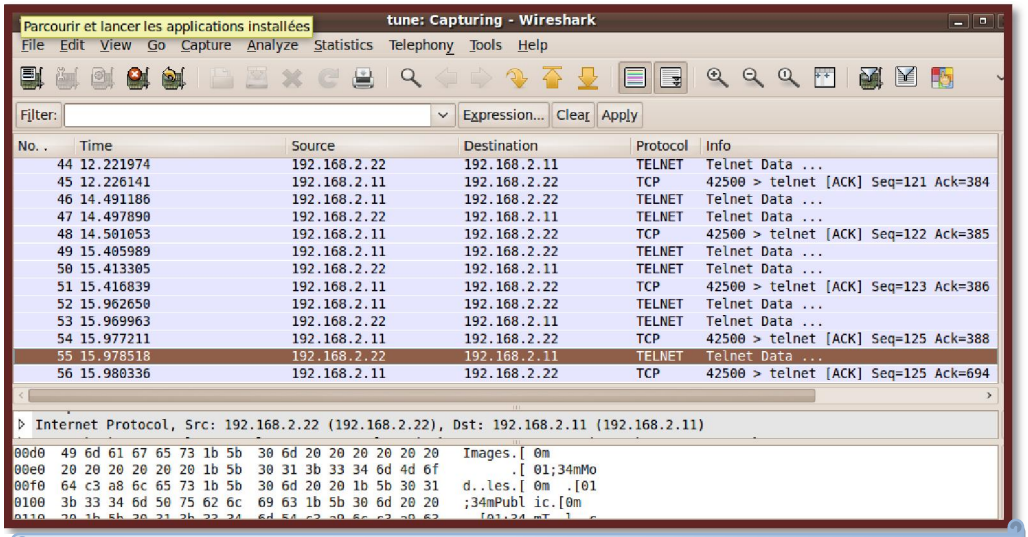
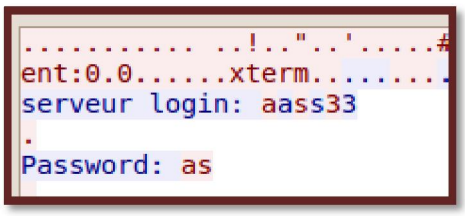


Figure V-5 : résultat de capture par wireshark

Voila les paquets capturé qui travers le tunnel :



```
You have mail.
]0;as3@serveur: ~.as3@serveur:~$ mmuutttt
```

```
From: root <root@serveur>.[K
To: as3@lmd-pfe.dz.[K
Subject: facebook.[K
User-Agent: Mutt/1.5.20 (2009-06-14).[K

.[37m.[40msalem
jai ouvrir un nouveau page facebook
.[34m.[40m.[K
```

Mais dans la machine physique (eth1), les messages capturés par wireshark seron crypté et chiffré comme suit :

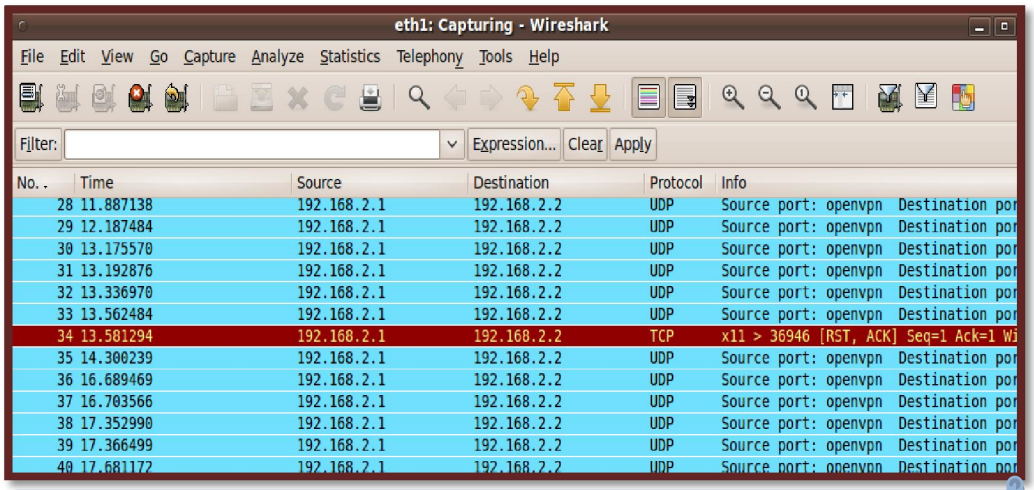


Figure V. 6 : interface réseau de capture

Les messages capturé sur l'interface physique eth1 (ils sont chiffrés)

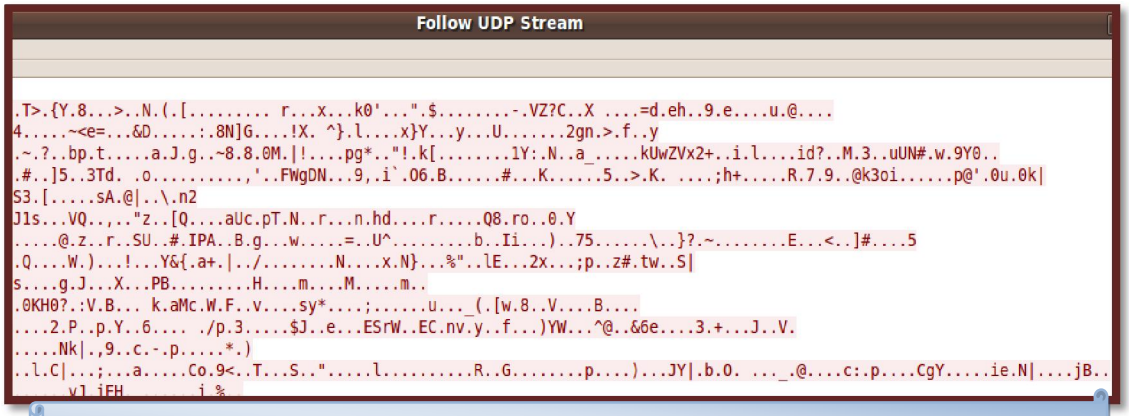


Figure V-7 : messages capturés chiffrés

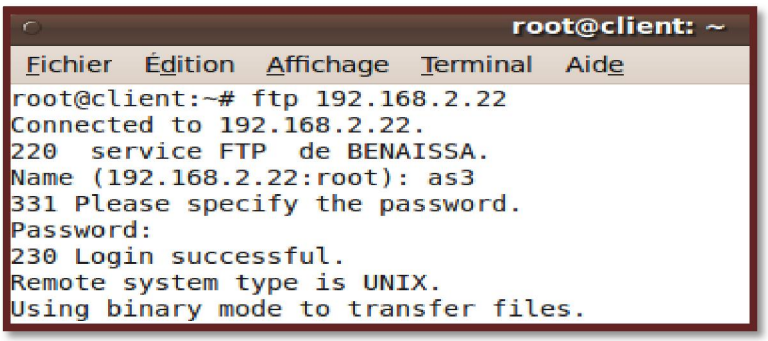
VI Sécurisation d'un service de transfert des fichiers vsftp via un tunnel vpn :

Nous avons déjà montré dans le chapitre 4 comment en installe un serveur de transfert des fichiers vsftp. Maintenant nous montrons comment en doit sécurisé les trames d'un serveur de transfert de fichiers via un tunnel securisé vpn

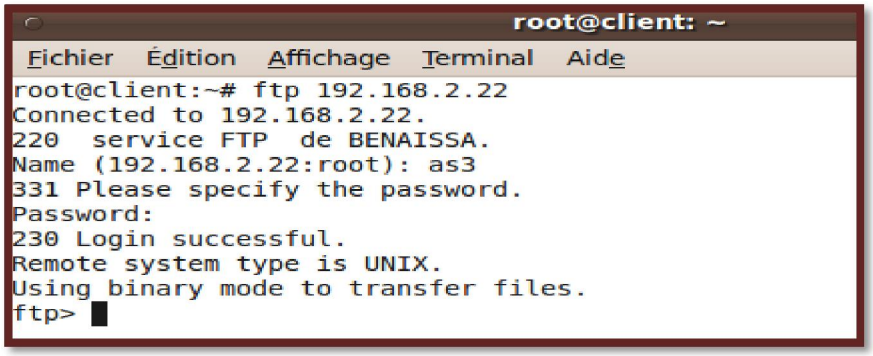
Étape 1: lancer le tunnel entre deux machines client- serveur comme premier étape de courrier électronique

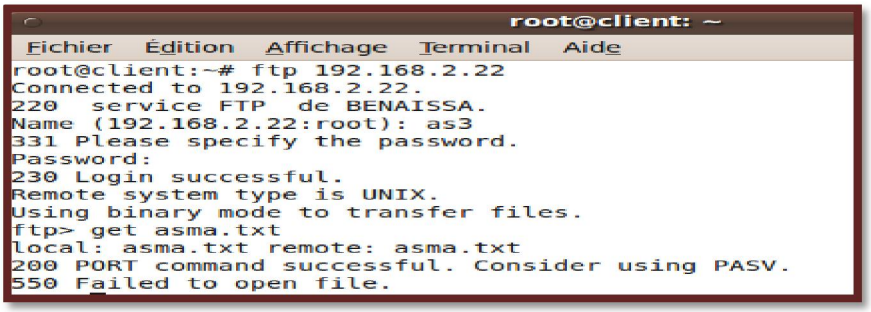
Étape 2: lancer wireshark en moment de la connexion à la machine virtuelle (client)

Comme suivant :



Connexion via ftp à la machine serveur vsftp (par un tunnel vpn)





Voila les paquets capturés par wireshark lors de la connexion via un ftp (le mot de passe et login seront aussi intercepté) les captures s'effectué sur le tunnel :

Voila les résultats de capture :

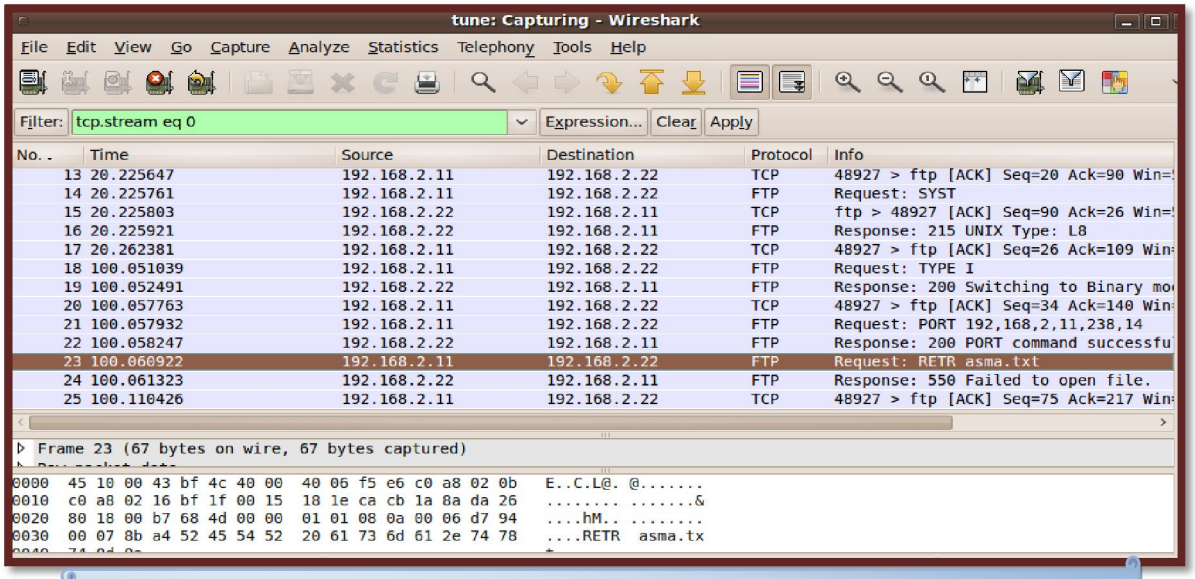


Figure V-8 : interface de capture

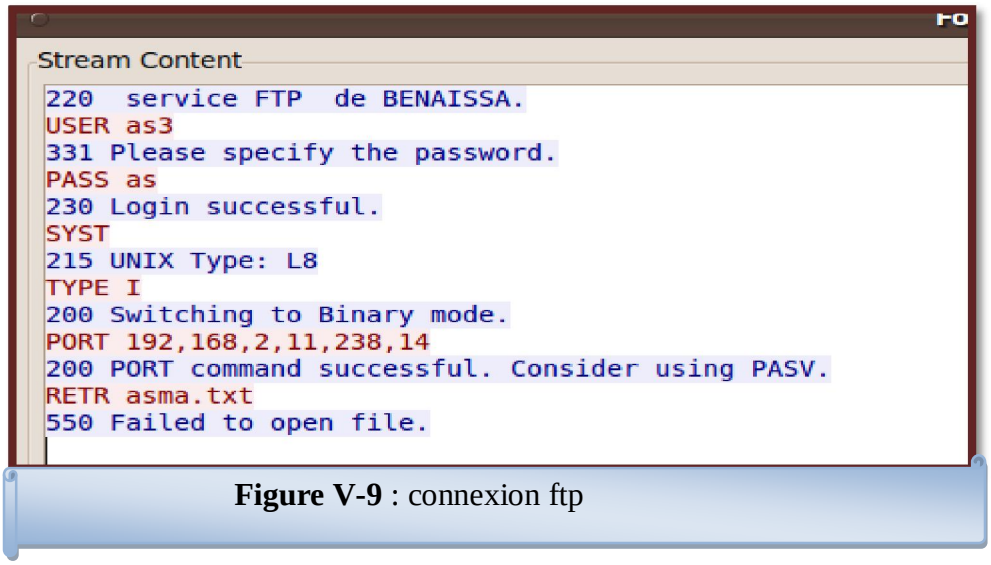


Figure V-9 : connexion ftp

Mais dans la machine physique (eth1) les paquets capturés par wireshark sont cryptés et chiffrés :

Voila le résultats de capturation :

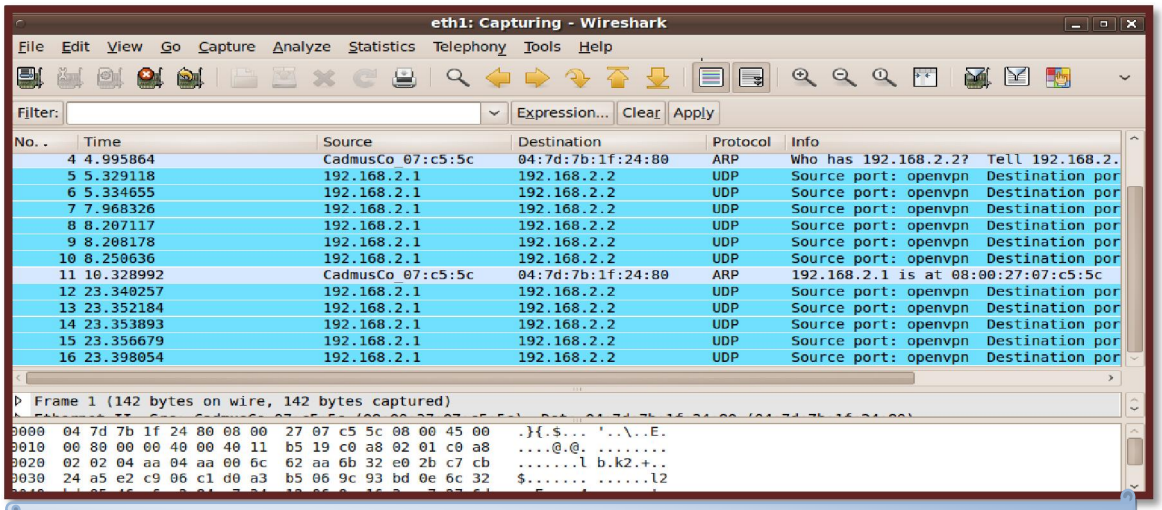
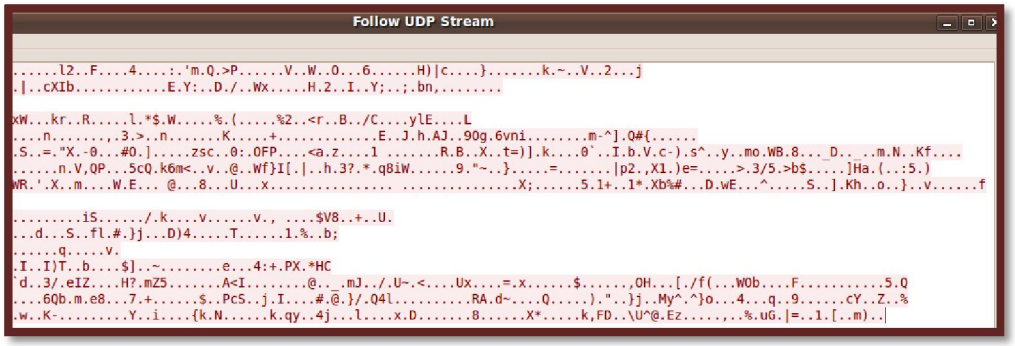


Figure V-10 : paquets capturés par wireshark

Le message est chiffré sur l'interface physique :



VII Conclusion :

Le courrier électronique et le transfert des fchiers via ftp se sont des applications Internet très importantes, ils sont à la base du travail collaborati. Ils facilitent en effet la communication et l'échange des données dans délais pouvant être très court.

Comme conclusion de notre travail, nous ponvons dire que le vpn assure bien la protection et la sécurité des mes messages transmis dans tunnel virtuel qui utilise plusieurs protocoles de sécurité et de chiffrement des données comme ipsec et ssl,

Conclusion générale :

Le besoin croissant des entreprises de communiquer entre des sites distants a donné naissance aux VPN. En effet, la raison d'être des VPN est d'offrir aux utilisateurs et aux administrateurs d'un système d'information, les mêmes conditions d'utilisation, d'exploitation et de sécurité à travers un réseau public que celles disponibles sur un réseau privé.

Le VPN est une technologie révolutionnaire et complexe qui repose sur l'utilisation de divers protocoles de tunnelage assurant un niveau de sécurité plus ou moins élevé.

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de la mise place d'un réseau VPN site-à-site. Nous avons en effet grâce à cette nouvelle technologie permis aux employés de partager de façon protégés leurs données via les protocoles de sécurité qui sont les principal outils permettant d'implémenter le VPN, ce partage était possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs dit « distants » situés en dehors du réseau local.

En effet, la mise en place de VPN site-à-site permet aux réseaux privés de s'étendre et de se relier entre eux au travers d'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 de sécurité comme ssl et 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..

Nous sommes intéressés dans notre mémoire par la protection et la sécurisation des données transmis via les services de messageries électronique et les services de transfert de fichier (ftp) en exploitant un tunnel VPN.

Comme conclusion, tout travail scientifique, nous n'avons pas la prétention de réaliser un travail sans critique et suggestion de la part de tout lecteur afin de le rendre plus meilleur

Bibliographie :

[1] BUCHER Aurélie, FRITZ Jean-Nicolas, LAMBERT Florian, LAMBERT Gaël, Virtualisation de réseau et supervision, Projet tutoré 2008-2009.

[2] Benoît DONNETTE, David HANNEQUIN, livre blanc LINAGORA de la virtualisation, Décembre 2007.

[3] « Les VPN – Principes, conception et déploiement des réseaux privés virtuels » par Rafael Corvalan, Ernesto Corvalan, Yoann Le Corvic

[4] « IPSec – L'ouvrage de référence pour le nouveau standard de sécurité pour Internet, les Intranets et les VPN » par Naganand Doraswamy, Dan Harkins Article : « Virtual Private Networks: an overview from the security perspective » par Ali Ahmed Ali, Tarek Abd El-Mageed, Salwa Al Gamal, Khalid Mostafa

[5] Hakim Benameurlaine, SERVICE TELNET, 2011.

[6] http://mi.cnrs-orleans.fr/Security/VPN/VTN.htm

[7] http://compnetworking.about.com/od/vpn/l/aa010701a.htm

[8] Mr BENAISSA Mohamed, classe Master-rsd cour d'Installation et configuration d'un serveur messagerie Postfix, 2010 / 2011.

[9] http://www.vpntools.com/vpntools_articles/ipsec-ssl.htm

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

[11] http://www.securite.org/db/reseau/tunnel

[12] http://solutionspme.lemondeinformatique.fr/articles/lire-choisir-parmi-trois-technologies-de-reseaux-prives-virtuels-pour-securiser-les-acces-distants-257.html Rapport de TER de Tsedeye TIBEBU, Andrei NEAGU 19

[13] http://solutionspme.lemondeinformatique.fr/articles/lire-choisir-parmi-trois-technologies-de-reseaux-prives-virtuels-pour-securiser-les-acces-distants-257.html

[14]http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=vpn&articleId=9002591&taxonomyId=143

[15] http://www.commentcamarche.net/initiation/vpn.php3

[16] Mathieu Dubois, Olivier Gatimel, Thomas Molle, Rapport du projet Portail Captif.

.

Liste des figures :

Liste des abréviations :

ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
CD	Compact Disque
DVD	Digital Versatile Disque
ESP	Encapsulating Security Payload
FTP	File Transfert Protocol
GPL	Licence publique générale GNU
FAI	Fournisseur D accès à Internet
GRE	Graduate Record Examination
HTTP	Hyper Texte Transfert Protocol
IP	Internet Protocol
IP Sec	Internet Protocol Security
IPV4	Internet Protocol version 4
IPV6	Internet Protocol version 6
IPX	Inter network paket Exchange

IMAP	Internet Message Access Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
LAC	Layer Access Concentrator
L2TP	Layer 2 Tunneling Protocol
LNS	Layer Network Server
L'OS hôte	L'Open Source hôte
MDA	Mail Delivery Agent
MTA	Mail Transfert Agent
MUA	Mail User Agent
NAS	Network Acess Server
OS	Open Source
OSI	International Organization for Standardization
PAC	PPTP Access Controller
PPTP	Point-to-Point Tunneling Protocol
PPP	Point-to-Point Protocol

POP	Post Office Protocol
PNS	Pipeline Nitrogen services
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
US	Universel Serial
VDI	Virtual Desktop Infrastructure
VM	Virtual Privat Network
VPN	Virtual Private Network
VSFTPD	very secure file transfer protocol Daemon

ملخص:

خلال العقد الماضي, عرفت استخدامات الشبكات الخاصة الافتراضية (VPN) نموا قويا نتيجة التسويق حيث سهلت شبكة الإنترنت تنفيذ الاقتصادية من الشبكة العامة العالمية وهذا أيضا بسبب الحاجة المتزايدة إلى التواصل وتبادل الموارد من مختلف المواقع البعيدة وأخيرا وليس آخرا بسبب الحاجة إلى المزيد من التنقل للمستخدمين الرحل للشركة. وقد ساعدت هذه الاحتياجات الأساسية إلى زيادة شعبية VPN.

ونحن مهتمون في ذاكرتنا من خلال حماية وتأمين الخدمات التي تنتقل عبر الرسائل الإلكترونية وخدمات البيانات ونقل الملفات (FTP) عن طريق تشغيل نفق VPN.

الكلمة: tunnel VPN، والبريد الإلكتروني وبروتوكول نقل الملفات خدمة أمن بروتوكول المسنجر، SSL، بتشفير IPSec .

Résumé:

Au cours de la dernière décennie, l'utilisation des réseaux privés virtuels (VPN) a connu une très forte progression à cause de la commercialisation d'Internet qui a facilité leur mise en œuvre économique sur un réseau public mondiale. Ceci est aussi dû au besoin croissant de communiquer et de partager des ressources de différents sites distants et non pas dernièrement à cause de la nécessité d'obtenir plus de mobilité pour les utilisateurs nomades d'une entreprise. Ces besoins fondamentaux ont contribué à accroître la popularité des VPN.

Nous sommes intéressés dans notre mémoire par la protection et la sécurisation des données transmis via les services de messageries électronique et les services de transfert de fichier (ftp) en exploitant un tunnel VPN.

Mot clés : tunnel vpn, messagerie électronique, service ftp, protocole de sécurité, OPENVPN, SSL, IPSEC, cryptographie.

Abstract:

During the last decade, the use of virtual private networks (VPN) experienced strong growth due to the commercialization of the Internet has facilitated their economic implementation of a global public network. This is also due to the growing need to communicate and share resources from different remote sites and last but not least because of the need for greater mobility for nomadic users of a company. These basic needs have helped to increase the popularity of VPN.

We are interested in our memory by protecting and securing the services transmitted via electronic messaging and data services, file transfer (ftp) by operating a VPN tunnel.

Keyword: tnnel vpn, email, ftp service security protocol OPENVPN, SSL, IPSEC encryption.