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

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

FACULTE DU **G**ENIE **E**LECTRIQUE ET D' **I**NFORMATIQUE
DEPARTEMENT D' ELECTRONIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Télécommunication et réseaux**

Présenté par
TINHINANE TEBANI

Thème

Simulation d'un tunnel VPN-SSL pour la sécurisation d'une interconnexion de deux réseaux LANs

Mémoire soutenu publiquement le 12/07/ 2015 devant le jury composé de :

M. Mourad LAZRI
Maître de conférences classe A, UMMTO, Président

M. Fethi OUALLOUCHE
Maître de conférences classe B, UMMTO, Encadreur

M. Mohamed Mecharek
Expert 1er degré, LET Algérie télécom, Co-Encadreur

M.Slimane HAMEG
Maître de conférences classe A, UMMTO, Examinateur

M. Yahia ATTAF N
Maître de conférences classe A, UMMTO, Examinateur

Remerciement

Je remercie en premier lieu Dieu tout puissant de m'avoir accordé la puissance et la volonté pour terminer ce travail.

Je tiens à exprimer mes plus sincères remerciements à mon promoteur ***Mr OUALLOUCHE*** *qui m'a aidé tout au long du travail.*

Mes remerciements les plus vifs s'adressent aussi à messieurs le président et les membres du jury d'avoir accepté d'examiner et

D'évaluer mon travail.

J'exprime également ma gratitude à tous les enseignants qui ont collaboré à ma formation depuis le premier cycle d'étude jusqu'à la fin du cycle universitaire.

Un grand merci également à Mr BERKAT et a

ma famille pour leurs aides considérables.

Dédicace

***J**e dédie ce modeste travail à :*

***M**es très chers parents yema et baba qui m'ont toujours soutenu.*

***M**on grand père (jedi) et **M**es deux grands-mères (yema azi et jida yamina)*

M**es chère sœurs **LAMIA et son mari MERZOUK, MASSILA et son mari MUSTAFA , KARINE et CILYA

M**on très cher frère **YACINE

M**on adorable neveu **MOHAMED

***M**a future nièce **TOUTAH NOUNOU** .*

***M**r **FEZANI** Karim que je remercie beaucoup pour son soutien*

***M**es oncles et leurs familles*

***M**a tente **NADIA** et ses enfants*

***T**ous mes ami(e)s ainsi qu'à tous ceux qui me sont chers.*

***E**t à toute personne m'ayant fait part de son savoir.*

TEBANI Tinhinane

Glossaire

Glossaire

ARP : **A**dresse **R**ésolution **P**rotocole

ACL : **A**ccess **C**ontrol **L**ist

BGP : **B**order **G**ateway **P**rotocol

DNS : **D**omain **N**ame **S**ystem

DHCP : **D**ynamique **H**ost **C**onfiguration **P**rotocol

DES : **D**ata **E**ncryptions **S**tandard

EGP: **E**xterior **G**ateway **P**rotocol

FTP : **F**ile **T**ransfert **P**rotocole

GSM: **G**lobal **S**ysteme **M**obile

GRE: **G**eneric **R**outing **E**ncapsulation

GNS3: **G**raphical **N**etwork **S**imulateur

HTTP: **H**ypertext **T**ransfer **P**rotocol

HTTPS: **H**ypertext **T**ransfer **P**rotocol **S**ecure

IP: **I**nternet **P**rotocol

IOS: Iphone **OS** et le système d'exploitation mobile développé par Apple

ICMP : **I**nternet **C**ontrol **M**essage **P**rotocol

IGP : **I**nterior **G**ateway **P**rotocol

IPsec : **I**nternet **P**rotocol **S**ecurity

LAN: **L**ocal **A**rea **N**etwork

L2TP: **L**ayer **T**o **T**unneling **P**rotocol

L2F : **L**ayer **T**wo **F**orwarding .Protocole d'encapsulation

MMF : **M**ulti **M**ode **F**ibre

MAN : **M**étropolitain **A**rea **N**etwork

Glossaire

MAC : **M**edia **A**ccess **C**ontrol

NAT : **N**etwork **A**ddress **T**ranslation

NAS : **N**etwork **A**ttached **S**torage

OSI : **O**pen **S**ysteme **I**ntrconnection

PAN : **P**ersonale **A**rea **N**etwork

PAT : **P**ort **A**ddress **T**ranslation

PPP: **P**oint **T**o **P**oint **P**rotocol

PPTP : **P**oint **T**o **P**oint **T**unneling **P**rotocol

RARP : **R**everse **A**dresse **R**ésolution **P**rotocole

RIP : **R**outing **I**nformation **P**rotocol

SMF: **S**ingle **M**ode **F**iber

SMTP : **S**imple **M**ail **T**ransfert **P**rotocole

SSL : **S**ecure **S**ocket **L**ayer

SSH : **S**ecure **S**hell

TCP : **S**tructured **Q**uery **L**anguage

UDP : **U**ser **D**atagram **P**rotocol

VPN : **V**irtual **P**rivate **N**etwork

VLAN : **V**irtual **L**ocal **A**rea **N**etwork

Glossaire

Liste des figures

Chapitre 1 : Généralités Sur Les Réseaux

Chapitre 2 : Concepts de Sécurité

Chapitre 3 : Les protocoles utilisés dans le VPN

Chapitre 4 : Mise en place d'un tunnel VPN-SSL

Liste des figures

Liste des tableaux

Sommaire

Sommaire

Introduction

Introduction

L'utilisation du réseau Internet n'est plus sécurisée de nos jours. Ceci est dû essentiellement à l'augmentation de la demande sur l'utilisation du réseau Internet et l'implantation des entreprises sur différents sites. La communication entre ces sites se fait généralement via Internet. Malheureusement, les sites web ne sont pas très bien protégées et vulnérable aux attaques des cybercriminels [1].

L'internet assure la communication entre les différents sites d'une même entreprise. Pourtant sont utilisation pose un grand problème de sécurité. Par conséquents, les méthodes de sécurité ont été conçu pour remédier à ces problèmes. Parmi ces méthodes ; nous pouvons citer l'antivirus, la cryptographie symétrique et asymétrique, les pare-feu, les VLAN, le NAT, les ACL, VPN, …etc [2].

De nombreux internautes choisissent d'utiliser les services VPN que l'entreprise Cisco a développé. En effet, une gamme de solutions de sécurité basée sur le réseau privé virtuel (VPN) est proposée.

Le VPN repose sur un protocole appelé « Protocol de tunneling ». Ce 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 via Internet après avoir identifie l'émetteur et le destinataire [3].

L'objectif principal de ce travail est basé sur la simulation d'une interconnexion sécurisée entre deux LAN. Celle-ci est assurée par un tunnel VPN (virtuel privât network) utilisant le protocole SSL/TLS (Secure socket layer /transport layer Security)

Notre mémoire est structuré en 4 chapitres.

Le premier chapitre présente des généralités sur les réseaux, les topologies, classification des réseaux, le model OSI.

Le deuxième chapitre est consacré à l'étude des principes de sécurité, les attaques et les méthodes de sécurité en basant sur le VPN.

Dans le 3éme chapitre, nous présentons les différents protocoles du VPN et le principe du VPN-SSL.

Dans le 4éme chapitre, nous présentons la simulation d'une connexion VPN-SSL entre deux sites distants.

Nous terminons notre mémoire par une conclusion et une bibliographie.

Chapitre 1
Généralités sur Les Réseaux

1. Préambule

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants entres eux. Ils ont beaucoup apporté pour les entreprises et les sociétés, ce qui les a rendus indispensables. Leur but est d'assurer l'interconnexion des ordinateurs afin qu'ils puissent se communiquer entre eux et d'échanger des données.

Dans ce chapitre nous allons définir un réseau et présenter les topologies et les protocoles les plus utilisés.

2. Définition d'un Réseau

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles afin que les utilisateurs et les applications qui fonctionne sur ces dernières puissent échanges des informations.

Le terme réseau en fonction de son contexte peut :

- désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qu'est le cas lorsqu'on parle de l'Internet.
- décrire la façon dont les machines d'un site sont interconnectées
- spécifier les protocoles qui sont utilisés pour que les machines communiquent on peut parler de réseau TCP/IP.

3. Objectif d'un réseau

3.1. Partage de ressources

Rendre accessible a chaque membre de réseaux les programmes, données, équipements indépendamment de leur localisation physique [4] :

- de partager les fichiers.
- le transfert de fichier.
- le partage d'application : compilateur, système de gestion de base de données.
- partage d'imprimante.

3.2. Grande fiabilité

Duplication des données sur plusieurs sites, ainsi si l'une est inutilisable (panne matérielle de la machine..), on peut utiliser une des copies. Aussi la présence de plusieurs unités centrales fait que si l'une est en panne les autres peuvent prendre en charge son travail.

3.3. Réduction de couts

Les gros ordinateurs bien qu'ils soient plus performants que les petits ordinateurs sont Beaucoup plus chers, l'idée est de construire des systèmes a base de ces derniers afin de Réduire le cout même si cela au détriment de la performance.

4. Sens de transmission

Pour communiquer des informations entre deux points il existe différentes possibilités pour le sens de transmission [1] :

- liaisons unidirectionnelles.
- liaisons bidirectionnelles,
- liaisons bidirectionnelles simultanées.

5. Les supports de transmission

Pour transmettre des informations d'un point à un autre, il faut un canal qui servira de chemin pour le passage de ces informations. Ce canal est appelé canal de transmission ou support de transmission. En réseau informatique, téléinformatique ou télécoms, on distingue plusieurs sortes de support de transmission [6]:

1. Les câbles à paires torsadées
2. Les câbles coaxiaux
3. Les câbles à fibre optique
4. Les liaisons infrarouges
5. Les liaisons hertziennes

5.1. Les câble à paires torsadées

Les câbles à paires torsadées (twisted pair câbles) sont des câbles constitués au moins de deux brins de cuivres entrelacés en torsade (le cas d'une paire torsadée) et recouverts des isolants[6].

En réseau informatique, on distingue plusieurs types de câbles à paires torsadées :

- Les câbles STP
- Les câbles UTP
- Les câbles FTP

- Les câbles FFTP
- Les câbles SFT
- Les câbles SSTP

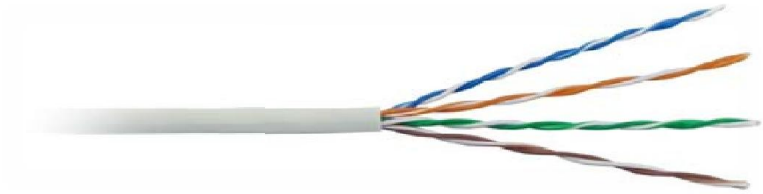

Figure.1. câble à paires torsadées

5.2. Les câbles coaxiaux

Le câble coaxial est composé d'un fil de cuivre entouré successivement d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure.
On distingue deux types de câbles coaxiaux [6] :

- les câbles coaxiaux fins
- es câbles coaxiaux épais

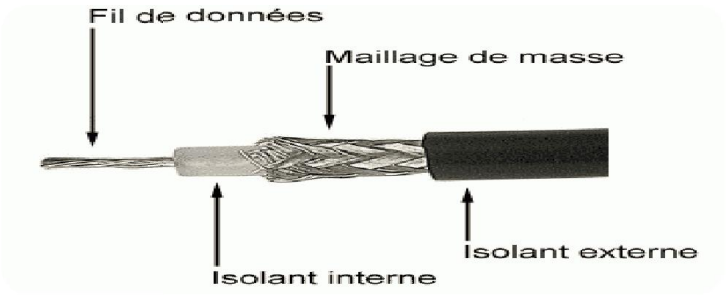

Figure.2. câble coaxial

Le câble coaxial fin (thinNet) ou 10 base-2 (le nom 10 base-2 est attribué grâce à la norme Ethernet qui l'emploie) mesure environ 6mm de diamètre. Il est en mesure de transporter le signal à une distance de 185m avant que le signal soit atténué.

Le câble coaxial épais (thickNet) appelé aussi 10 base-5 grâce à la norme Ethernet qui l'emploie, mesure environ 12mm de diamètre. Il est en mesure de transporter le signal à une

distance de 500m avant que le signal soit atténué. Pour le raccordement des machines avec les câbles coaxiaux, on utilise des connecteurs BNC.

5.3. Les câbles à fibre optique

La fibre optique reste aujourd'hui le support de transmission le plus apprécié. Il permet de transmettre des données sous forme d'impulsions lumineuses avec un débit nettement supérieur à celui des autres supports de transmissions filaires [6].

La fibre optique est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice comme présentée par la figure suivante :

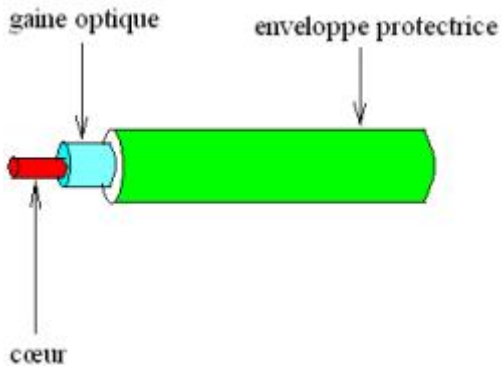

Figure.3. La fibre optique

On distingue deux sortes des fibres optiques :

- les fibres multi modes
- les fibres monomodes

Les fibres multimodes ou MMF (Multi Mode Fibre) ont été les premières fibres optiques sur le marché. Le cœur de la fibre optique multimode est assez volumineux, ce qui lui permet de transporter plusieurs trajets (plusieurs modes) simultanément. Il existe deux sortes de fibre multimode :

La fibre multimode à saut d'indice et la fibre optique multimode à gradient d'indice. Les fibres multimodes sont souvent utilisées en réseaux locaux.

La fibre monomode ou SMF (Single Mode Fiber) a un cœur si fin. Elle ne peut pas transporter le signal qu'en un seul trajet. Elle permet de transporter le signal à une distance beaucoup plus longue (50 fois plus) que celle de la fibre multimode. Cette fibre est utilisée dans des réseaux à long distance.

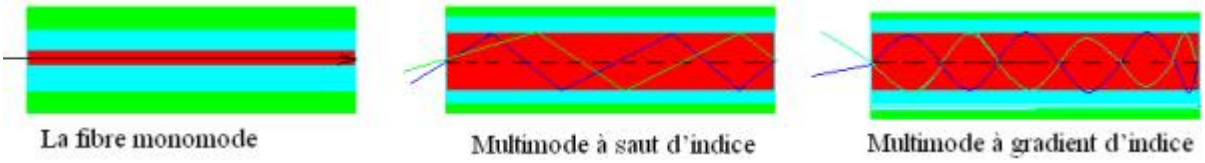

Figure.4. les types de fibre optique

5.4. Les liaisons infrarouges

La liaison infrarouge est utilisée dans des réseaux sans fil (réseaux infrarouges). Il lie des équipements infrarouges qui peuvent être soit des téléphones soit des ordinateurs… théoriquement les liaisons infrarouges ont des débits allant jusqu'à 100Mbits/s et une portée allant jusqu'à plus de 500m [6].

5.5. Les liaisons hertziennes

La liaison hertzienne est une des liaisons les plus utilisées. Cette liaison consiste à relier des équipements radio en se servant des ondes radio [6].

Voici quelques exemples des systèmes utilisant la liaison hertzienn

- Radiodiffusion
- Télédiffusion
- Radiocommunications
- Faisceaux hertziens
- Téléphonie
- Le Wifi
- Le Bluetooth

6. Classification des réseaux

Nous pouvons classifier les réseaux selon plusieurs aspects. Parmi lesquels :

- leurs tailles
- leurs topologies.
- La méthode d'accès aux données

6.1. Selon leurs tailles

Nous comptons compte généralement 4 catégories de réseaux informatiques différenciées par la distance maximale séparant les points les plus éloignes du réseau [7] :

6.1.1. Réseau PAN (Personale Area Network) :

Ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tel que : le GSM, portable ….d'un même utilisateur …

6.1.2. Réseaux LAN (Local Area Network) :

Ou encore le correspond par leurs tailles aux réseaux d'entreprise ils servent au transport de toutes les informations numérique de l'entreprise. La distance de câblage est de quelques centaines de mètres [7].

6.1.3. Réseau MAN (Métropolitain Area Network) :

Ils permettent l'interconnexion des entreprises ou des départements sur un réseau spécialise a haut débit. Ce type correspondent a une interconnexion de quelques bâtiments se trouvent dans une ville (campus) [7].

6.1.4. Réseau WAN (Wide Area Network):

Sont destines comme leurs noms l'indiquent, a transporter des données numériques sur des distances a l'échelle d'un pays voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise des infrastructures au niveau du sol essentielle !ment des grands réseaux de fibre optique soit hertzienne comme les réseaux satellite [7].

6.2. Selon la Topologie

6.2.1. Définition de la topologie

Un réseau informatique est constitue d'ordinateurs relies entre eux grâce au matériels (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique ; il en existe trois [7] :

6.2.2. Topologie en bus

Le bus, est un segment central ou circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

L'avantage du bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est, de plus, très facile a mettre en place. Par contre, en cas de rupture du bus, le réseau devient inutilisable [7].

Notons également que le signal n'est jamais régénère, ce qui limite la longueur des câbles. Cette topologie est utilisée dans les réseaux Ethernet 10 base 2 et 10 base 5.

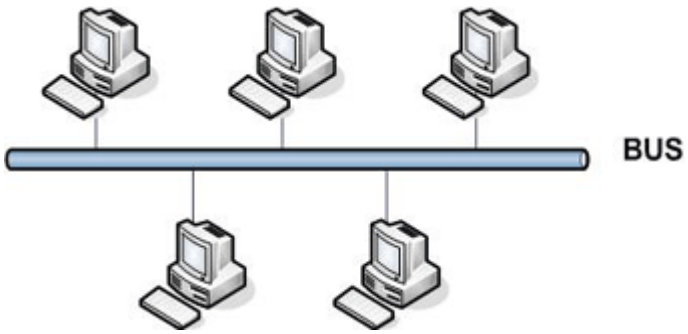

Figure .5. Topologie en bus

6.2.3. Topologie en anneau (ring)

Développée par IBM, cette architecture est principalement utilisée par les réseaux token ring. Ce dernier la technique d'accès par « jeton ». Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite…
Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénère par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable. L'interconnexion de plusieurs anneaux n'est pas facile à mettre en œuvre [7].

Cette topologie est utilisée par les réseaux token ring et fddi

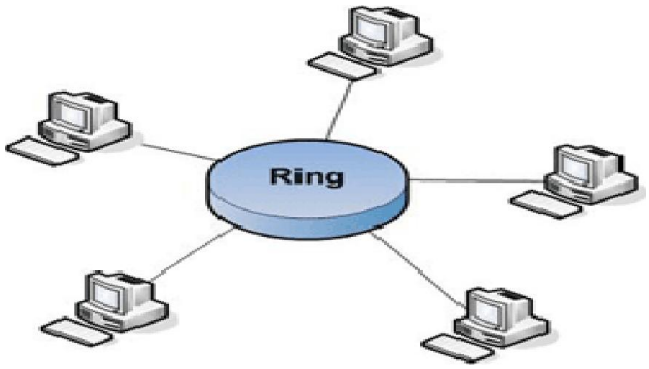

Figure.6. topologie en anneau

6.2.4. Topologie en étoile (star)

C'est la topologie la plus courante. Toutes les stations sont reliées à un seul composant central (concentrateur). Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub).

Ce type de réseau est facile à mettre en place et a surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres

topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies [7].

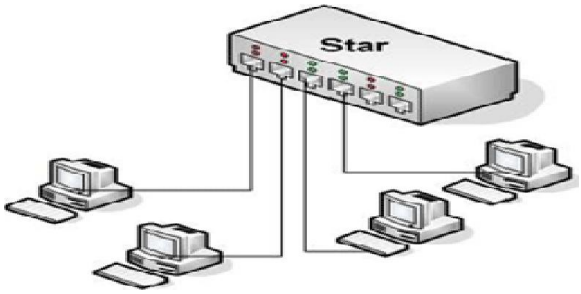

Figure. 7. Topologie en étoile

6.2.5. Structure hybride

La structure hybride de réseau emploie un mélange de différentes structures de réseau, comme l'anneau, le bus et également l'étoile [7].

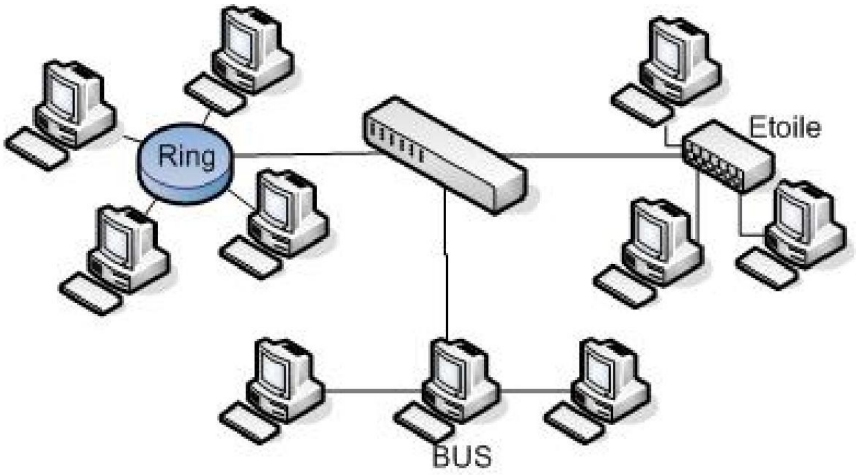

Figure.8. Structures hybride

7. Interconnexion

Les réseaux hétérogènes formant internet sont relies entre eux grâce a des dispositifs d'interconnexion (passerelles, routeurs, ponts …) qui assurent le transfert des données [7]

7.1. Les ponts

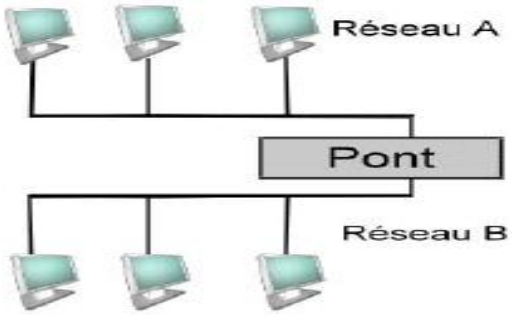

Figure .9. Deux réseaux relient avec un pont

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situes de l'autre cote du pont (figure 9*)*.

Un pont possède deux connexions a deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (mac) du destinataire et de l'émetteur. si jamais le pont ne connait pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel cote du réseau se trouve l'émetteur [7].

Ainsi le pont est capable de savoir si émetteur et destinataire sont situes du même cote ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau.

7.2. Les passerelles

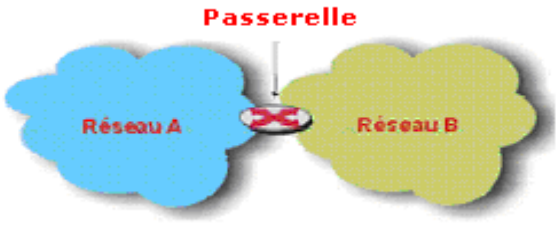

Figure.10.deux réseaux reliés avec passerelle

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun des réseaux. Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données [7].

7.3. Les routeurs

Un routeur est un matériel de communication de réseaux informatique destine au routage. Son travail est de limiter les domaines de diffusion et de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé, afin que ce dernier atteigne sa destination finale le plus rapidement possible. Ce processus nomme routage intervient a la couche 3 (couche réseau) du modèle OSI .

La fonction de routage consiste à traiter les adresses IP en fonction de leur adresse réseau définie par le masque de sous-réseaux (par défaut ou personnalise) et a les diriger en fonction de l'algorithme de routage et de sa table de routage (celle ci contient la correspondance des adresses réseau avec les numéros de port physique du routeur ou sont connectes les autres réseaux). (choisir-son-adsl.fr)[7].

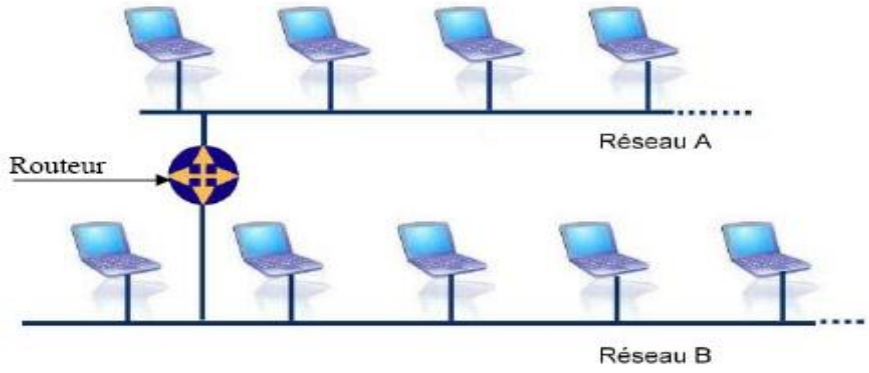

Figure .11. Routeur connecter a deux réseaux locaux

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quelque soit l'architecture.

7.4. Les hubs (concentrateurs)

Le hub est également appelé concentrateur ou répétiteur. C'est un boitier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire) [7].

7.5. Switch

Un commutateur réseau (en anglais, Switch) est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boitier disposant de plusieurs (entre 4 et 100) ports Ethernet. Il a donc la même apparence qu'un concentrateur (hub)

Contrairement à un concentrateur, un commutateur ne se contente pas de reproduire sur tous les ports chaque trame qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilises pour remplacer des concentrateurs [7].

8. Le modèle OSI

Le modèle OSI (open system interconnexion model) défini en 1977 régit la communication entre 2 systèmes informatiques selon 7 niveaux. A chaque niveau, les deux systèmes doivent communiquer "compatibles". En matériel réseau, nous n'utilisons que les couches inferieures, jusqu'au niveau 3. Ces niveaux sont également appelés couches.

L'OSI est un modèle de base normalise par l'international standard organisation (iso).

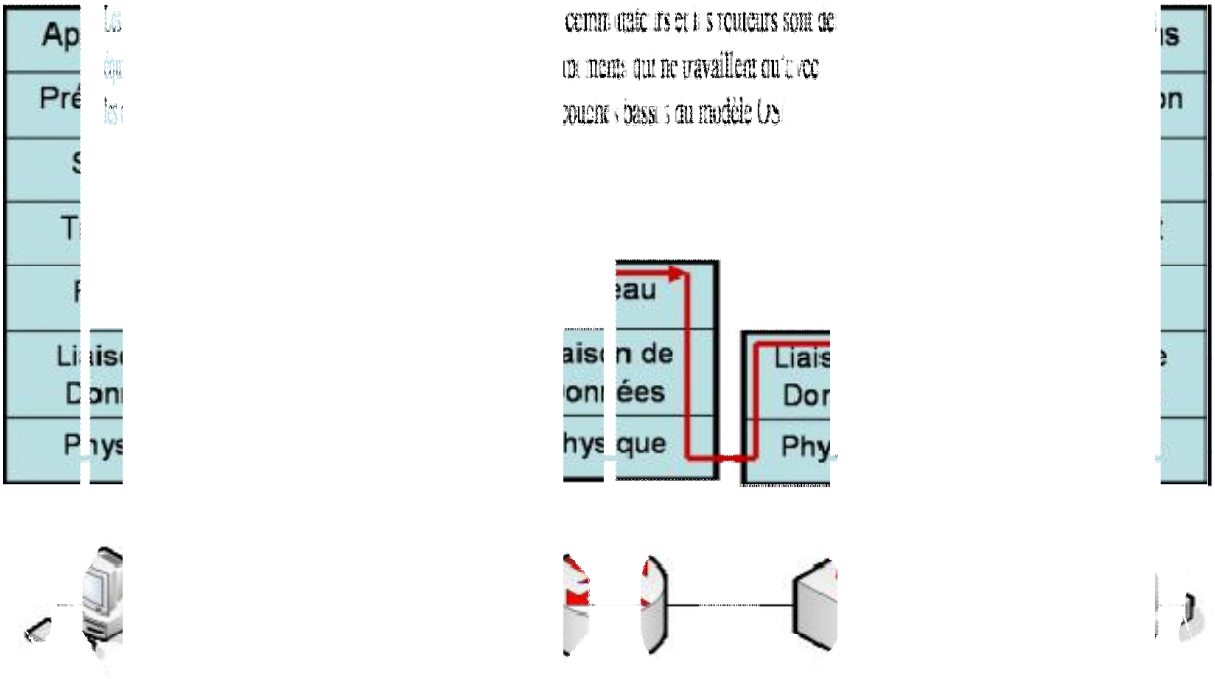

Figure.12. Le model OSI

- **niveau 7 (application)**: gère le format des données entre logiciels.
- **niveau 6 (présentation)**: met les données en forme, éventuellement de l'encryptage et de la compression, par exemple mise en forme des textes, images et vidéo.
- **niveau 5 (session)**: gère l'établissement, la gestion et coordination des communications
- **niveau 4 (transport)**: s'occupe de la gestion des erreurs, notamment avec les protocoles UDP et TCP/IP
- **niveau 3 (réseau)**: sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles IP (adresse et le masque de sous-réseau) et ICMP. utilise par les routeurs et les Switch mangeables.
- **niveau 2 (liaison de données)**: utilise les **adresses mac**. le message Ethernet a ce stade est la trame, il est constitue d'un en-tête et des informations. l'en-tête reprend l'adresse mac de départ, celle d'arrivée + une indication du protocole supérieur.
- **niveau 1 (physique)**: gère les connections matérielles et la transmission, définit la façon dont les données sont converties en signaux numériques: ça peut-être un câble coaxial, paires sur RJ45, onde radio, fibre optique, ...

8.1. L'avenir d'OSI

Au niveau de son utilisation et implémentation, et ce malgré une mise à jour du modèle en 1994, OSI a clairement perdu la guerre face à TCP/IP. Seuls quelques grands constructeurs dominant conservent le modèle mais il est amené à disparaître d'autant plus vite qu'Internet (et doncTCP/IP)explose.

Le modèle OSI restera cependant encore longtemps dans les mémoires pour plusieurs raisons. C'est d'abord l'un des premiers grands efforts en matière de normalisation du monde des réseaux. Les constructeurs ont maintenant tendance à faire avec TCP/IP, mais aussi le WAP, l'UMTS etc. ce qu'il devait faire avec OSI, à savoir proposer des normalisations dès le départ. OSI marquera aussi les mémoires pour une autre raison : même si c'est TCP/IP qui est concrètement utilisé, les gens ont tendance et utilisent OSI comme le modèle réseau de référence actuel. En fait, TCP/IP et OSI ont des structures très proches, et c'est surtout l'effort de normalisation d'OSI qui a imposé cette "confusion" générale entre les 2 modèles. On a communément tendance à considérer TCP/IP comme l'implémentation réelle d'OSI [8].

9. Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprime. Ainsi, a la réception, le message est dans son état original [8].

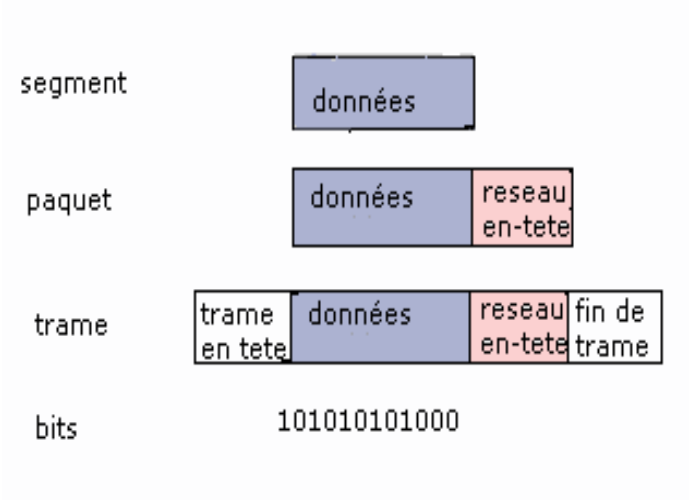

Figure.13. principe d'encapsulation.

10. Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-a-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon que l'on attend de la communication. Certains protocoles seront par exemple spécialises dans l'échange de fichiers (FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP). Sur internet par exemple les protocoles utilises font partie d'une suite de protocoles, c'est-a-dire un ensemble de protocoles relies entre eux. Cette suite de protocole s'appelle TCP/IP [8].

10.1. Protocole TCP

Protocole sécurise d'échange de données : crée dans le but d'établir une communication de haute fiabilité entre deux taches exécutées sur deux ordinateurs autonomes et raccordes a un réseau (protocole oriente connexion) [8].

10.2. Protocole UDP

Le protocole UDP (user data gram Protocol) a été crée dans le but d'établir comme le TCP une communication entre deux ordinateurs mais il ne fournit pas de contrôle d'erreur (il n'est pas oriente connexion) [8].

10.3. Architecture de TCP/IP

TCP/IP fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, TCP (transfert contrôle protocole) se charge du transport de bout en bout pour toute application alors que IP (internet protocole) est responsable du routage a travers le réseau.

D'autres protocoles sont aussi inclus comme ARP (adressa résolution protocole), ftp (file transfert protocole), SMTP (simple mail transfert protocole) [8].

TCP/IP est structure en quatre niveaux :

- l'interface réseau (1 et 2 du modèle OSI).
- le routage (3 du modèle OSI).
- le transport (4 et 5 du modèle OSI).
- l'application (5,6et7 du modèle OSI).

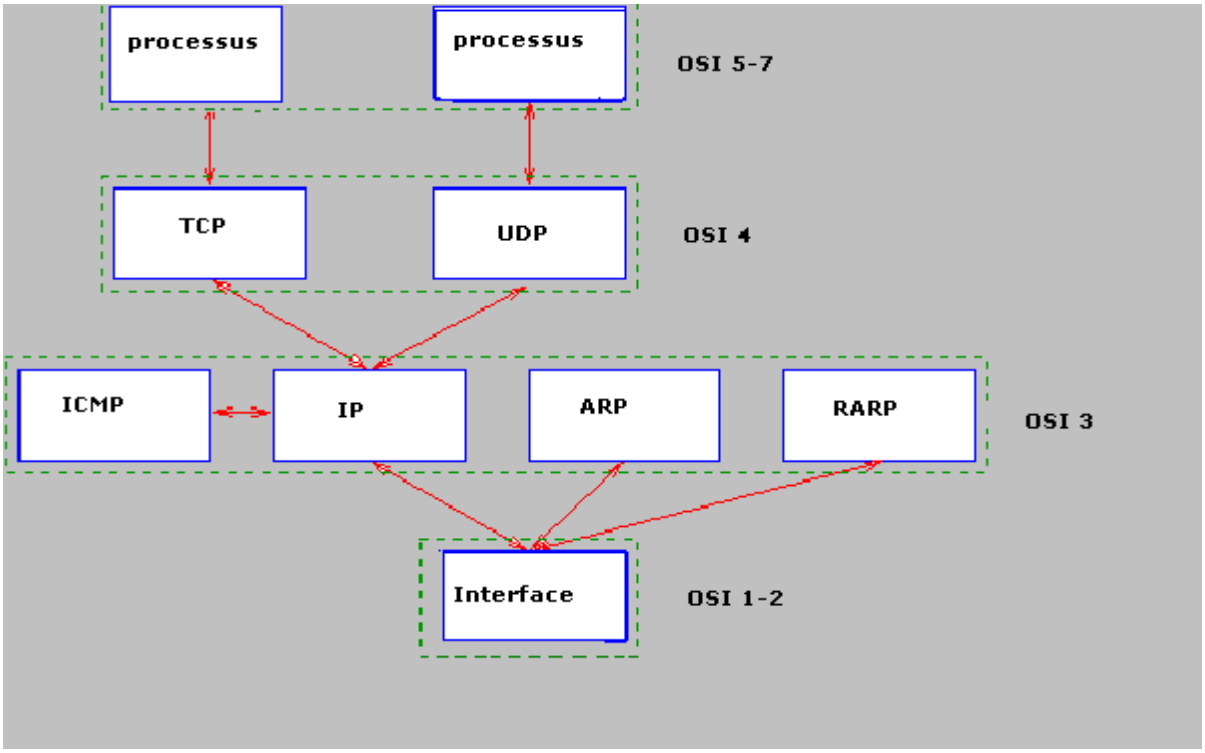

Figure.14. architecture TCP/IP.

10.4. Protocole ipv4

10.4.1. Protocole IP

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, mais le rôle le plus important de ce protocole est d'acheminer les données a travers un ensemble de réseaux interconnectes grâce a la gestion des adresses IP.

Pour cela il utilise des numéros de 32 bits, que l'on écrit sous forme de 4 numéros allant de0 a 255 (4 fois 8 bits), on les note sous la forme **xxx.xxx.xxx.xxx** ou chaque **xxx** représente un entier de 0 a 255.[8]

Par exemple, **194.153.205.26** est une adresse IP ont peux distinguer deux parties dans une adresse IP :

- les nombres de gauche désignent le réseau (on l'appelle **net id**)
- les nombres de droite désignent les ordinateurs de ce réseau (on l'appelle **host id**)

10.4.2. Adressage

Chaque ordinateur du réseau internet dispose d'une adresse IP unique codée sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque interface de réseau. Une adresse IP est toujours représentée dans une notation décimale pointée constituée de 4 nombres (1 par octet) compris chacun entre 0 et 255 et sépares par un point.

Plus précisément, une adresse IP est constituée d'une paire *(*id. de réseau, id. de machine*)* et appartient a une certaine classe (a, b, c, d ou e) selon la valeur de son premier octet, comme détaille dans la (figure 16)

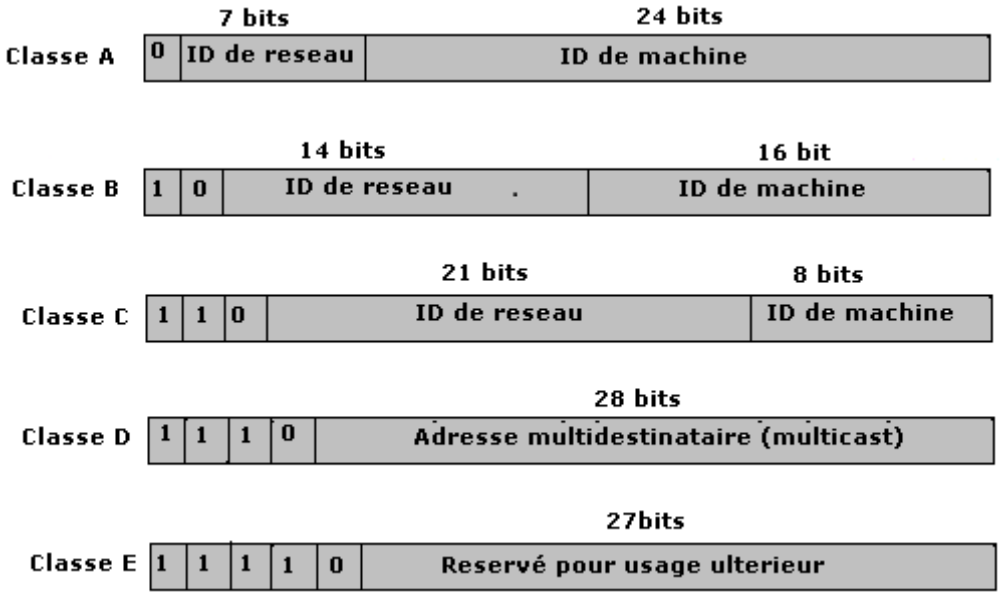

Figure.15. les cinq classes d'adresses IP

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

Classe	Adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C	192. 0. 0. 0 à 223. 255. 255. 255
D	224. 0. 0. 0 à 239. 255. 255. 255
E	240. 0. 0 .0 a 247. 255. 255. 255

Figure.16. l'espace d'adresse

10.5 .ARP et RARP

Ces protocoles permettent de convertir l'adresse logique en adresse physique et vice versa.

10.5.1. Protocole ARP

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

machine connectée au réseau possède un numéro d'identification sur 48 bits. Ce numéro est un numéro unique qui est fixe des la fabrication de la carte réseau en usine.

Toutefois, la communication sur internet ne se fait pas directement a partir de ce numéro (car il faudrait modifier l'adressage des ordinateurs a chaque fois que l'on change une carte réseau) mais a partir d'une adresse dite logique attribuée par un organisme. On parle alors de l'adresse IP [8] .

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaitre leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête (contenant l'adresse de la machine demandée) sur le réseau. Chaque machine du réseau compare par la suite l'adresse logique reçue, avec la sienne. Si l'une des machines s'identifie à cette adresse, elle répondra alors à ARP par une requête contenant son adresse physique, qui va stocker la couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu.

10.5.2. RARP (reverse ARP)

Il est dans le réseau internet. Permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique.

11. Le DNS

Le DNS est le mécanisme qui permet de convertir le symbolique en adresse IP, lorsque les machines communiquent sur un réseau informatique, c'est toujours par l'utilisation d'une adresse (IP ou autre) source ou destination. Mais ces adresses bien que nécessaires, sont difficiles a mémoriser et ne permettent pas de souplesse dans les configurations des stations.

Pour quelqu'un de normalement constitue, il est difficile de se souvenir de 55.124.198.56 alors que www.victim.com sera assez aise à mémoriser, c'est le but du protocole DNS : fournir une association (adresse IP, nom FQDN) et inversement.

Le service DNS est donc utilise pour la « résolution de noms », cette opération consiste a fournir aux clients DNS qui en font la demande une association adresse IP, un nom symbolique et vice-versa [8].

12. DHCP

Le protocole DHCP (dynamique host configuration Protocol) attribue automatiquement des adresses IP aux équipements branches au réseau. Lorsqu'un client essaie de se brancher au réseau, une demande de paramètres de configuration est envoyée au serveur DHCP. Une fois que le serveur a reçu le message, le serveur DHCP envoie une réponse au client, qui comprend les informations de configuration, puis enregistre en mémoire les adresses qui ont été attribuées. DHCP utilise le protocole *bootp* pour communiquer avec les clients. Les clients doivent renouveler leur adresse ip a 50 % de la période d'utilisation, puis de nouveau a 87,5 %, en envoyant un message *dhcprequest*. Les hôtes clients conservent leur adresse ip jusqu'a l'expiration de leur période d'utilisation, ou lorsqu'ils envoient une commande *dhcprelease. ipconfig* et *winipcfg* sont des utilitaires exécutes a partir de la ligne de commande et qui permettent de vérifier les informations de l'adresse IP qui a été attribuée a l'hôte client [8].

13. Le routage IP

Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP a travers les divers réseaux d'un internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme. D'une manière générale on distingue la remise directe, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et la remise indirecte qui est mise en œuvre dans tous les autres cas, c'est-a-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final [8] .

13.1. Table de routage

Table de routage spécifique à chaque routeur qui permet de déterminer vers quelle voie de sortie envoyer un datagramme destine à un réseau quelconque. Évidemment, à cause de la structure localement arborescente d'internet la plupart des tables de routage ne sont pas très grandes. Par contre, les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux. D'un point de

vue fonctionnel une table de routage contient des paires d'adresses du type (*d*, *r*) ou *d* est l'adresse IP d'une machine ou d'un réseau de destination et l'adresse IP du routeur suivant sur la route menant a cette destination.

13.1.1 .routage interne

13.1.1.1. RIP

L'un des protocoles de routage les plus populaires est RIP(routing information Protocol) qui est un protocole de type vecteur de distance. C'est-a-dire que les messages échanges par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage. Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'«infini». Ceci implique que RIP ne peut être utilise qu'a l'intérieur des réseaux qui ne sont pas trop étendus [8].

13.1.1.2. OSPF

Est un nouveau type de protocole de routage dynamique qui élimine les limitations de RIP. C'est un protocole d'état de liens, c'est-a-dire qu'ici un routeur n'envoie pas des distances à ses voisins, mais il teste l'état de la connectivite qui le relie a chacun de ses voisins. Il envoie cette information à tous ses voisins, qui ensuite le propagent dans le réseau. Ainsi, chaque routeur peut posséder une carte de la topologie du réseau qui se met à jour très rapidement lui permettant de calculer des routes aussi précises qu'avec un algorithme centralise.

En fait, RIP de type et OSPF, sont des protocoles IGP (interior gateway protocol) permettant d'établir les tables des routeurs internes des systèmes autonomes.

Figure .17. Interconnexion de systèmes autonomes.

Dans chaque système autonome les tables sont maintenues par un IGP et sont échangées uniquement entre routeurs du même sous-système. Pour obtenir des informations sur les réseaux externes, ceux de l'autre système autonome, ils doivent dialoguer avec les routeurs externes r1 et r2. Ceux-ci sont des points d'entrée de chaque système et via la liaison qui les relie, ils échangent des informations sur la connectivite grâce à EGP (exterior gateway protocol) ou BGP (border gateway protocol) qui remplace EGP actuellement [8] .

13.1.2. Routage externe

13.1.2.1. BGP (border gateway protocol)

c'est le protocole de routage externe le plus utilisée sur l'internet .BGP gère le routage base sur une politique qui utilise des raison non techniques (des considérations routage politiques, organisationnelles ou de sécurité) pour prendre les décisions en matière de routage .BGP améliore la capacité d'un système autonome a choisir entre différentes routes et a implanter des politiques de routage sans se baser sur une autorise centrale de routage (dans le d'absence de passerelle centrales)[8].

14. ICMP

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

Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe quel datagramme IP sur l'Internet. Une erreur engendrée par un message ICMP ne peut donner naissance à un autre message ICMP [8].

15. Discussion

L'utilisation des réseaux d'ordinateurs partageant des serveurs apporte une grande souplesse. Les réseaux permettent l'accès à de très nombreuses ressources et c'est pour cela qu'on observe une augmentation de la demande sur l'utilisation des réseaux. Par conséquent, les risques augmentent.

Chapitre 2
Concepts de sécurité

1. Préambule

De nos jours l'utilisation de l'Internet n'est plus sûre. Souvent, les transmissions de données ainsi que les sites web ne sont pas bien protégées et sont vulnérables aux attaques des cybercriminels. La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines fonctionnent d'une façon optimale. La mise en œuvre d'une politique de sécurité est indispensable au sein d'un réseau afin de le protéger de toute sorte d'intrusions malveillantes.

Dans ce chapitre nous allons présenter les attaques les plus fréquentes et les notions de sécurité et en particulier le VPN.

2. Définition de la sécurité

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles, ce qui implique la réalisation des fonctions essentielles suivantes :

- Disponibilité.
- Confidentialité.
- Intégrité.
- Non répudiation.
- Authentification.

3. Objectifs

Le système d'information est généralement définit par l'ensemble des données ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler .Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité,** c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- **La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;

- **La disponibilité,** permettant de maintenir le bon fonctionnement du système d'information ;
- **Le non répudiation**, permettant de garantir qu'une transaction ne peut être niée ;
- **L'authentification,** consistant à assurer que seules les personnes autorisées aient accès aux ressources.

4. Les techniques d'attaques

4.1. Attaque contre la communication

Est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations transmises ou stockées, l'information n'est pas altérées par celui qui en prélève une copie. Ces attaques sont donc indétectables par le système et peuvent seulement êtres parées par des mesures préventives [9].

4.2. Interposition

Il s'agit d'un déguisement en émission ou en réception, il consiste à tromper les mécanismes d'authentification pour se faire passer pour un utilisateur (personne ou service disposant des droits dont on a besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité [9].

Exemple : le vol d'adresse (IP spoofing)

Ce type d'attaque n'implique rien de plus que l'usurpation d'une adresse source. Cela consiste à utiliser une machine en se faisant passer pour une autre.

4.3. Coupure

Est un accès avec modification à des informations transmises sur des voies de communication, il s'agit donc d'une attaque contre l'intégrité [9].

4.4. Attaque logicielles

4.4.1. Les virus

Un virus est un bout de programme glissé volontairement dans une application dans le but de nuire. Il est possible d'attraper un virus avec n'importe quelle application que l'on a installée et que l'on exécute, ce n'est pas un problème typique d'une connexion permanente.

Un virus ne peut être introduit dans sa machine que si l'on exécute une application infectée, application récupérée sur l'Internet ou sur n'importe quel autre support informatique : disquette, CD ROM … . [9]

Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions.
- Ouverture sans précautions de documents contenant des macros.
- Pièce jointe de courrier électronique (exécutable, script type VBs…).
- Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier (normalement JavaScript est sans danger).

4.4.2. Le cheval de Troie

Un cheval de Troie ou trojen n'est ni un virus ni un ver, parce qu'il ne se reproduit pas. Un cheval de Troie introduit sur une machine dans le but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet. Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un cheval de Troie [9] :

- Récupération des mots de passe grâce à keylogger.
- Administration illégale à distance d'un ordinateur.
- Relais utilisé par les pirates pour effectuer des attaques.
- Serveur de spam (envoi en masse des e-mails).

4.4.3. Les vers

Un ver est un programme indépendant, qui se copie d'ordinateur en ordinateur .La différance entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter.

Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur .Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise.

Comme un virus ; un ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles [9].

4.4.4. L'écoute du réseau (snifing)

Grace à un logiciel appelé 'sniffer ', il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées.

Si quelqu'un se connecte par Telnet par exemple à ce moment-la, son mot de passe transitant en clair sur le net, il sera aisé de le lire.De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception [9].

5. Autres attaques

5.1. Attaques par déni de service (dos)

Une attaque par déni de service (DoS, Dinial Of Service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services aux ressources d'une organisation. Il s'agit la plus part de temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Le principe de ces attaques consiste à envoyer des paquets IP ou des données de taille afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent [9] .

5.2. Intrusion

L'intrusion dans un système informatique à pour but la réalisation d'une menace et donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique…etc.

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valide sur les machines qu'il a recensées, pour se faire, plusieurs méthodes sont utilisées par le pirate :[9]

- L'ingénierie sociale, c'est –à-dire en contactant directement certaine utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leur mot de passe.
- La consultation de l'annulaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des noms d'utilisateur valides.
- L'exploitation des vulnérabilités des logiciels.
- Les attaques par force brute, consistant à essayer de façon automatique différents mots de passe sur une liste de compte.

5.3. Attaques de l'homme de milieu

L'attaque de l'homme de milieu ou main-in-the-middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous contrôle d'un pirate.

Ce dernier peut transformer à sa façon les données à la volée, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur [9].

5.4. Usurpation d'adresse IP (IP spoofing)

L'usurpation d'adresse IP est une technique consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement [9].

5.5. Le craquage de mot de passe

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courant (et de leur variantes), ou par la méthode de brute force (toute les combinaisons sont essayées jusqu'à

trouver la bonne), cette technique longue, souvent peut utilisée à moins de bénéficier de l'appui d'un très grand nombre de machine [9].

6. Les méthodes de protections

6.1. Antivirus

Logiciel permettant de détecter et de supprimé les virus informatiques sur n'importe quel type de stockage (disque dur, disquette, CD-ROM, etc.).Pour être efficace ce type de logiciel demande des mises à jour très fréquentes au cours desquelles il mémorise les nouvelles formes de virus en circulation [9].

6.2. La cryptographie

La cryptographie est un ensemble de technique permettant de transformer les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale. Ceci Permet d'obtenir un texte, en effectuent des transformations inverses (ou encore des algorithmes de déchiffrements).Désormais, elle sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

La taille des clés de chiffrement dépond de la sensibilité des données à protéger. Plus ces clés sont longues plus le nombre de possibilités de clés important, par conséquent il sera difficile de deviner la clé [9] .

Les algorithmes de chiffrement se divisent en deux catégories :

6.2.1. Chiffrement symétrique

Dans ce cas de chiffrement, l'émetteur et le récepteur utilisent la même clé secrète qu'ils appliquent à un algorithme donné pour chiffrer ou déchiffrer un texte.

Ce cryptage à un inconvénient ; puisqu'il faut que les deux parties possèdent la clé secrète, il faut donc la transmettre d'un bout à l'autre, ce qui risqué sur un réseau non fiable comme internet car la clé peut ainsi être interceptée.

6.2.2. Chiffrement asymétrique

Ces systèmes se caractérisent par la présence d'une entité pour chaque interlocuteur désirant communiquer des données. Chaque interlocuteur possède une bi-clé ou couple de clés calculées l'une en fonction de l'autre.

- Une premier clé, visible, appelée clé publique est utilisée pour chiffrer un texte en clair.
- Une deuxième clé, secrète, appelée clé privée est connue seulement par le destinataire, qui est utilisé pour déchiffrer un texte.

7. Pare –feu

Un pare- feu (appelé aussi **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (internet).

Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante [9] :

- Une interface pour le réseau à protéger (réseau interne) ;

Une interface pour le réseau externe.

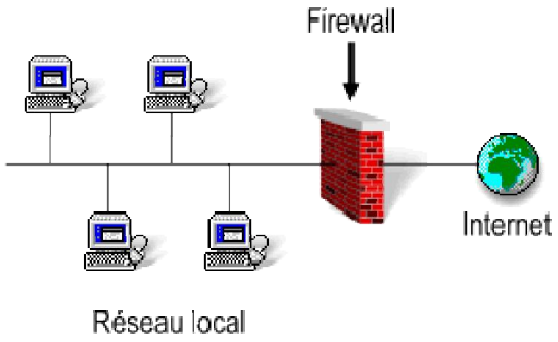

Figure.18. Pare –feu

Le système firewall est un système logiciel ou matériel, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes.Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel systèmes pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic.

- Le système soit sécurisé.
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Dans le cas ou le système pare-feu est fourni dans une boite noire « clé en main », on utilise le terme d' « Appliance ».

7.1. Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit autoriser uniquement la communication ayant été explicitement autorisées.
- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sure, mais elle impose toutefois une définition précise et contraignante des besoins en communication [9].

8. Les VLAN

Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement [2].

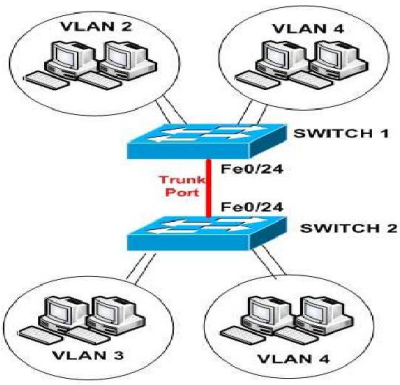

Figure.19. Exemple de VLAN.

9. Le NAT

Dans les entreprises de grandes tailles, différents réseaux interconnectés peuvent utiliser les mêmes adresses IP .Pour que la communication soit possible entre nœuds des deux coté, il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable.

Des équipements de translation d'adresse NAT (Network Address Translation) sont chargés d'adopter cette fonctionnalité .Ils permettent le changement d'une adresse IP par une autre [2] .

Trois types d'adresse sont possibles :

- La translation de port PAT (Port Address Translation), joue sur une allocation dynamique des ports TCP ou UDP, en conservant l'adresse IP d'origine.
- La conversion dynamique d'adresses (NAT dynamique) change à la volée d'adresse IP par rapport à une externe disponible dans une liste.
- La conversion statique d'adresse (NAT statique), effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe.

10. Les ACL

Les listes de contrôle d'accès (Access Control List) ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau.

Les ACL semblent avoir toujours existé sur les routeurs et rares sont les configurations où elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques.

Cependant leur mode de définition est employé pour catégoriser les réseaux en vue, entre autre, de les injecter dans un protocole de routage ou de les soumettre à une règle de qualité de service [2].

11. Les réseaux privés virtuel (VPN)

11.1. Définition

11.1.1. Réseau privé

Couramment utilisés dans les entreprises, les réseaux privés entreposent souvent des données confidentielles à l'intérieur de l'entreprise. De plus en plus, pour des raisons d'interopérabilité, on y utilise les mêmes protocoles que ceux utilisés dans l'Internet. On appelle alors ces réseaux privés « intranet ». Y sont stockés des serveurs propres à l'entreprise en l'occurrence des portails, serveurs de partage de données, etc. ... Pour garantir cette confidentialité, le réseau privé est coupé logiquement du réseau internet. En général, les machines se trouvant à l'extérieur du réseau privé ne peuvent accéder à celui-ci. L'inverse n'étant pas forcément vrai. L'utilisateur au sein d'un réseau privé pourra accéder au réseau internet.

11.1.2. Réseau privé virtuel

L'acronyme VPN correspond à *Virtual Private Network*, c'est-à-dire un réseau privé virtuel. Dans les faits, cela correspond à une liaison permanente, distante et sécurisée entre deux sites d'une organisation**.** Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme Internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partagés ou publics, tels qu'Internet. Il permet d'échanger des données entre deux ordinateurs sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

11.2. Le principe de fonctionnement d'un VPN

Le VPN repose sur un protocole de tunnellisation (*tunneling*), c'est-à-dire un protocole qui permet le passage de données cryptées d'une extrémité du VPN à l'autre grâce à des algorithmes. On emploi le terme « tunnel » pour symboliser le fait que les données soient cryptées et de ce fait incompréhensible pour tous les autres utilisateurs du réseau public (ceux qui ne se trouvent pas aux extrémités du VPN).

Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN

(ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.

De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée.

A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur. Pour émuler une liaison point à point, les données sont encapsulées, ou enrobées, à l'aide d'une en-tête qui contient les informations de routage pour leur permettre de traverser le réseau partagé ou public jusqu'à leur destination finale. Pour émuler une liaison privée, les données sont cryptées à des fins de confidentialité. Les paquets interceptés sur le réseau partagé ou public restent indéchiffrables sans clé de décryptage. La liaison servant à l'encapsulation et au cryptage des données privées est une connexion VPN.

Etant donné que chaque point d'un réseau VPN est relié au réseau central par le biais d'un tunnel, reliant la machine à un gateway. Ainsi, tous les utilisateurs passent par le même "portail**",** ce qui permet de gérer la sécurité des accès, ainsi que le trafic utilisé par chacun. En effet, malgré son aspect sécurisé, un réseau VPN reste une extension du réseau principal vers chaque employé qui y accède, ce qui augmente d'autant le risque de failles. Centraliser les entrées au réseau permet de renforcer la sécurité, et de mieux gérer la taille prise par le réseau étendu [10].

11.3. Les différents types de VPN

Parmi ces différents types on peut citer les :

-Le VPN d'accès

-Intranet VPN

-Extranet VPN

11.3.1. Le VPN d'accès

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

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

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un Nas compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée Ce qui peut poser des problèmes de sécurité.
- Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs [10].

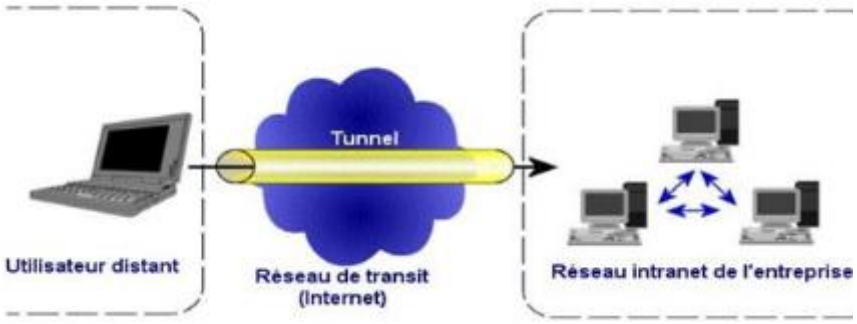

Figure .20. VPN connectant un utilisateur distant à un intranet privé

11.3.2. L'intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite.

Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable [10] .

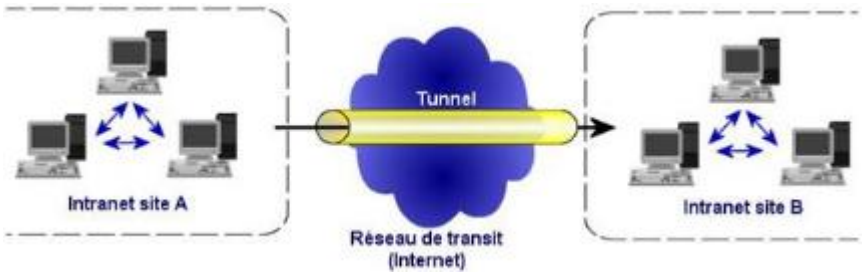

Figure .21. VPN connectant 2 sites distants par l'Internet

11.3.3. 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 cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci [10].

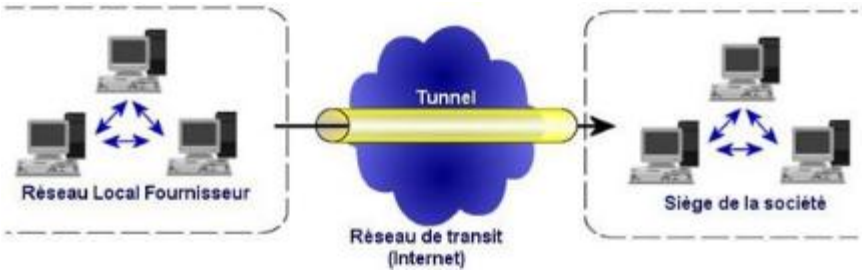

Figure .22.VPN connectant des sites clients au site de l'entreprise

11.4. Les différentes architectures des VPN

11.4.1. De poste à poste

C'est le cas d'utilisation le plus simple. Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de base de données entre deux serveurs d'une entreprise disposant de chaque coté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation [10].

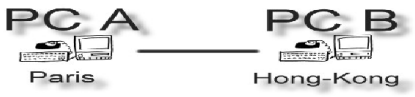

Figure.23. VPN de poste à poste

11.4.2. De poste à site

Un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion Internet. Le développement de l'ADSL favorise ce genre d'utilisation.

Attention toutefois à interdire l'accès Internet depuis le poste «localement». Pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise.

Ce point est important et rejoint la réflexion la plus la large de la sécurité des sites mis en relation avec VPN. Lorsque les niveaux de la sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux, s'il existe une faille de sécurité sur un site (ou sur un poste normale), celle- ci peut être exploitée [10].

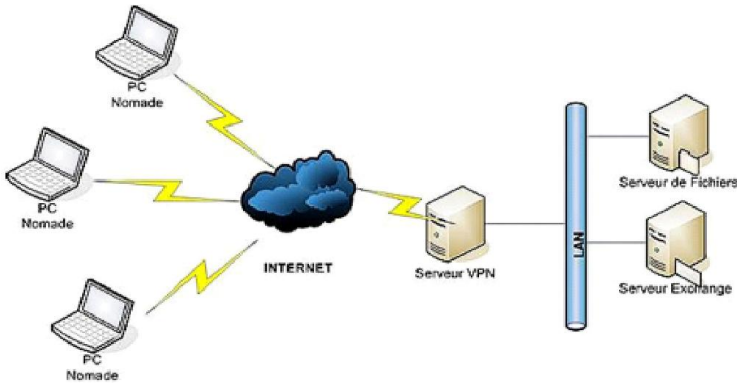

Figure.24. VPN de poste Nomade à site Entreprise

11.4.3. De site à site

Elle correspond à un type d'infrastructure de réseau étendu, c'est-à-dire que l'interconnexion entre les VPN remplace et améliore les réseaux privés existants. Elle utilise pour relier un site avec une des filiales, à moindre coût et en toute sécurité [10].

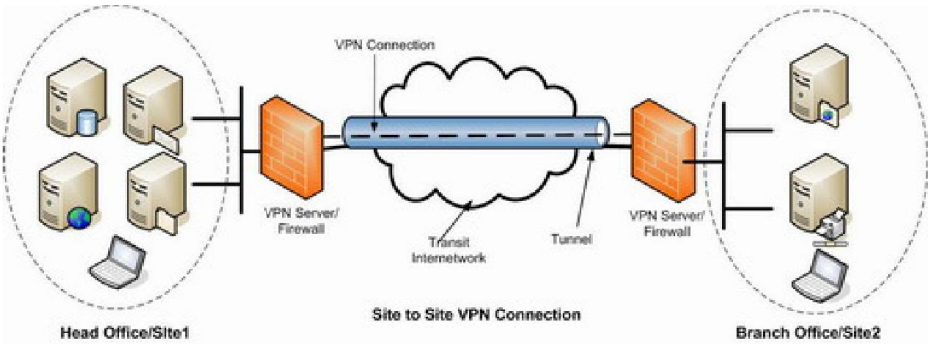

Figure.25. VPN de site à site

11.5. Topologie des VPN

Les VPN s'appuient principalement sur Internet comme support de transmission, avec un protocole d'encapsulation et un protocole d'authentification, au niveau des topologies, on retrouve des réseaux privés virtuels en étoile, maillé ou partiellement maillé [11].

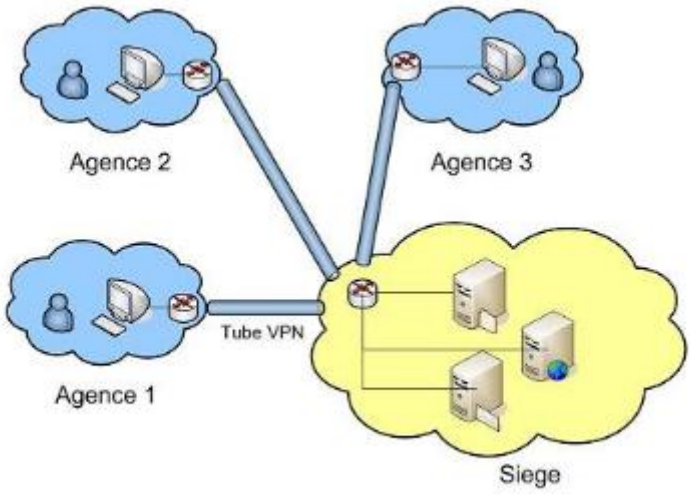

Figure.26. VPN en étoile

Dans cette topologie toutes les ressources sont centralisées au même endroit et c'est à ce niveau qu'on retrouve le serveur d`accès distant ou serveur VPN, dans ce cas de figure tous les employés du réseau s'identifient ou s'authentifient au niveau du serveur et pourront ainsi accéder aux ressources qui se situent sur l'intranet.

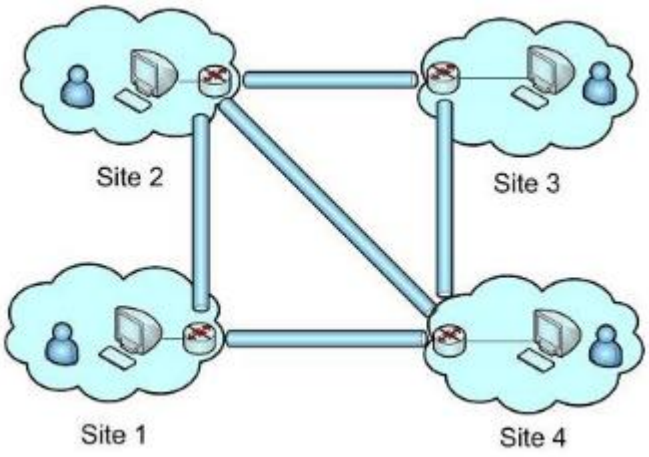

Figure.27. VPN maillé

Dans cette autre topologie les routeurs ou passerelles présents aux extrémités de chaque site seront considérés comme des serveurs d'accès distant, les ressources ici sont

décentralisées sur chacun des sites autrement dit les employés pourront accéder aux informations présents sur tous les réseaux [11].

11.6. Intérêts d'un VPN

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local.

Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. On peut facilement imaginer un grand nombre d'applications possibles :

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades.
- Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante.
- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet.
- Les connexions VPN permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, tel qu'Internet, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée.
- Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante [11].

11.7. Les caractéristiques d'un VPN

Une solution de VPN devrait fournir au moins l'ensemble des caractéristiques suivantes :

- **Authentification d'utilisateurs :** seuls les utilisateurs autorisés de la connexion VPN doivent pouvoir s'identifier sur le réseau virtuel.
- **Cryptage des données :** nécessite de cryptage des données pour protéger les données changées entre le client et le serveur VPN.
- **Adressage :** attribuer au client VPN une adresse IP privée lors de la connexion au réseau distant et garantir que cette adresse reste confidentielle.
- **Filtrage de paquet :** mise en place de filtres sur l'interface correspondant à la connexion à Internet du serveur VPN.
- **Gestion des clés :** les clés de cryptage pour le client et le serveur doivent être générées et régénérées.
- **Support multi protocoles** : les plus utilisés sur les réseaux publics en particulier IP.

11.8. Cryptage et Authentification

11.8.1. Cryptage

La cryptographie est une méthode permettant de rendre secrètes (illisibles) des informations afin de garantir l'accès à un seul destinataire authentifié. Elle est essentiellement basée sur l'arithmétique : il s'agit de transformer les lettres qui composent le message en succession de chiffres, puis faire des calculs sur ces chiffres pour :

- D'une part les modifier de telle façon à les rendre incompréhensibles ;
- Faire en sorte que le destinataire saura les décrypter.

Le fait de coder un message de façon à le rendre secret s'appelle le cryptage. La méthode inverse est appelé décryptage, elle nécessite une clé de décryptage [11].

On distingue deux types de cryptage :

11.8.1.1. Cryptage symétrique

Le cryptage symétrique appelé également cryptage à clé secrète ou chiffrement conventionnel, utilise une même clé pour crypter et décrypter le message, très efficace et assez économe en ressource CUP. Les algorithmes de chiffrement les plus connus sont :

DES (Data Encryptions Standard) et 3DES et AES

Le principe problème de cette technique la distribution des clés dans un réseau étendu, nécessite de partager une seule clé avec chacun de nos correspondants.

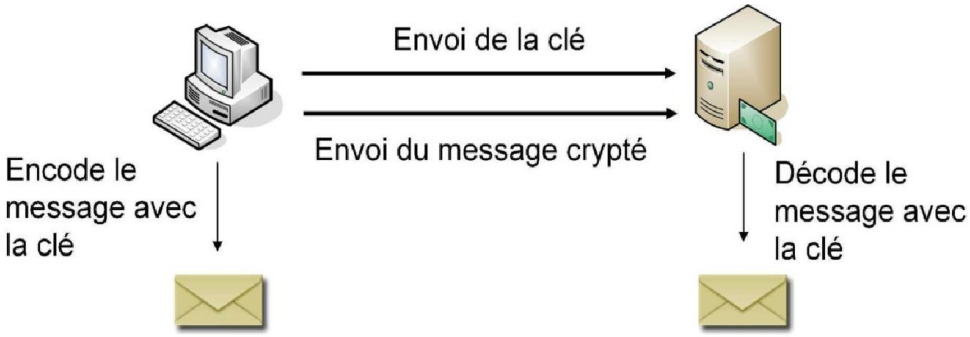

Figure. 28. Cryptage symétrique

On a un utilisateur A et un utilisateur B, lorsque l'utilisateur A veut envoyer son numéro de carte de crédit à l'utilisateur B il va décrypter avec une clé, le résultat de cryptage va transiter par Internet et lorsqu'il arrive à B il décrypte avec la même clé et on obtient le document initial qui contient le numéro de carte de crédit [11].

11.8.1.2. Cryptage asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire ; l'autre est publique et donc accessible par tout le monde.

Les clés publiques et privées sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décryptée qu'ave la clé privée correspondante, car ces deux clés générées au même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plus part des cryptages à clé privée il reste préférable pour 3 raisons :[12]

- Plus évolutif pur les systèmes possédant des millions d'utilisateurs ;
- Permet de signer le message donc garantir l'Authentification et la non- répudiation ;
- Supporte les signatures numériques.

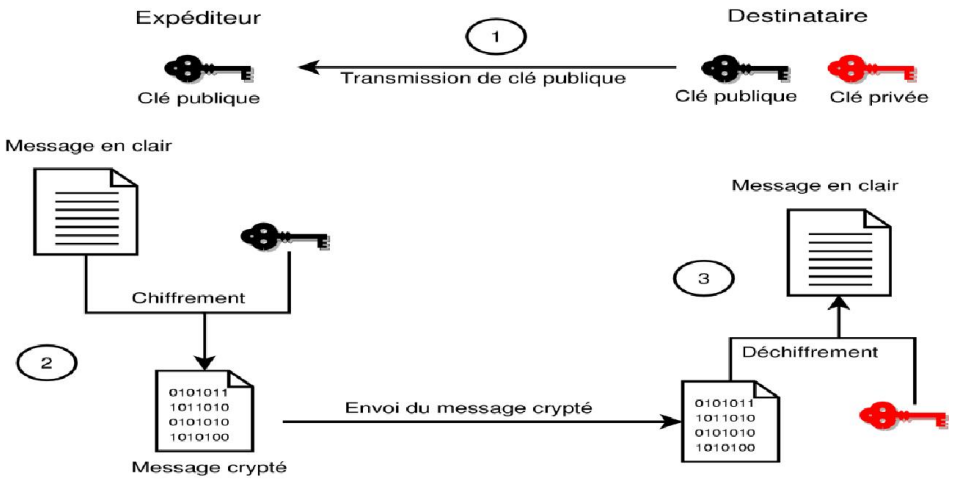

Figure.29. cryptage asymétrique

11.8.2. L'Authentification

Permettant de vérifier les identités présumées des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple), on parle de l'authentification simple. Lorsque nécessite plusieurs facteurs on parle de l'authentification forte.

L'authentification permet de vérifier les l'identité de l'utilisateur sur une des bases suivantes :

- Un élément d'information que l'utilisateur connaît (mot de passe, etc) ;
- Un élément que l'utilisateur possède (carte à puce, clé de stockage, certificat)
- Une caractéristique physique propre à l'utilisateur, on parle alors de biométrie (ADN, empreinte digitale, fond de rétine) [12].

L'authentification intervient à différents niveaux dans les couches de protocoles du modèle internet :

- Au niveau applicatif : http, FTP ;
- Au niveau transport: SSL, SSH ;
- Au niveau réseau: IPSEC ;
- Au niveau transmission: PAP, CHAP.

11.9. Les avantages et les inconvénients de VPN

Comme nous venons de le voire les VPN disposent de nombreux avantages : [12]

- Gratuité ou coût assez faible
- Confidentialité
- Sécurité assez efficace.
- Simplicité de la mise en place.

Cependant ils peuvent aussi représenter quelques inconvénients :

- Quelques failles de sécurité
- Utilisation de ressources matérielles importantes.

12. Discussion

L'une des solutions pour protéger un réseau est l'utilisation du VPN. Son principe est la création d'un tunnel virtuel via lequel les données transiteront sous forme cryptée. Cette solution sera envisagée pour une interconnexion de réseaux locaux ou alors pour la mise en place de solutions d'accès distants.

Chapitre 3
Les protocoles utilisés dans le VPN

1. Préambule

Plusieurs protocoles peuvent être utilisés dans le cas d'une sécurité réseau par VPN. Dans ce chapitre nous allons présentés ces protocoles et en particulier le SSL. Qui est présenté comme la solution pour permettre aux utilisateurs itinérants de se connecter aux applications réparties dans l'entreprise,

Dans se chapitre nous allons présenter les protocoles utilisé dans le VPN et quelques notions du SSL

2. Protocoles utilisés dans le VPN

Il existe plusieurs protocoles dit de tunnellisation qui permettent la création des réseaux VPN. Parmi ces protocoles, nous pouvons cités :

2.1.1. PPP

PPP (Point To Point Protocol) tunnel de la couche 2 du model OSI, est un protocole qui permet de transférer des données sur un lien synchrone. Il est full duplexe et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IPx dans des trames PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau.

Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP [10].

2.1.2. Le protocole PPTP

Le protocole PPTP (Point To Point Tunneling Protocol) tunnel du niveau 2 du model OSI, est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. Ainsi, PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression.

Le principe de protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP.PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation) [10].

Le tunnel PPTP se caractérise par :

- Une initiation du client ;
- Une connexion de contrôle entre le client et le serveur ;
- La clôture du tunnel par le serveur.

Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établit une connexion de type PPP et permet de faire circuler des donnés sur Internet. Par la suite, une deuxième connexion est établie. Elle permet d'encapsuler PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

2.1.3. L2F

L2F tunnel de niveau 2 du model OSI il a été développé par Cisco Systems comme une alternative au protocole PPTP. Comme ce dernier il s'appuie sur la couche deux de modèle OSI. Il est par contre beaucoup plus souple sur les protocoles réseaux utilisés. En effet, PPTP ne peut être encapsulée que dans des paquets IP alors que L2F peut aussi être encapsulé dans du X25 par exemple. Comme pour PPTP, L2F permet d'utilisation de différentes méthodes d'authentification [10].

L'authentification L2F est différente de celle de PPTP qui nécessite juste l'autorisation du RAS du LAN sur lequel on se connecte. En effet, l'authentification L2F nécessite l'approbation préalable du serveur RAS.

2.1.4. L2TP

L2TP (Layer To Tunneling Protocol) tunnel de la couche 2 du model OSI issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par Cisco, Microsoft, ainsi que d'autres acteurs du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (liaison de données) et 3 (réseau). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur Internet.

L2TP repose sur deux concepts :

- Les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator).
- Les serveurs réseau L2TP (LNS : L2TP Network Server).

Un élément intéressant de L2TP est l'utilisation d'UDP. Ce qui laisse entrevoir une vitesse d'acheminement supérieur. Cela implique également le fait que UDP offre des services moindres que TCP, il s'agit de les compenser ailleurs [10].

2.2. Le protocole IP Sec

2.2.1. Présentation du protocole IP Sec

IP Sec (Internet Protocol Security) est un protocole de la couche 3 du modèle OSI. Les concepteurs, S. Kent et R. Athinson de chez IETF (Internet Engineering Task Force) ont proposé une solution en novembre 1998 afin de répondre aux besoins directs du développement des réseaux en matière de sécurité. En effet, en sécurisant le transport des données lors d'échange internes et externes, la stratégie IP Sec permet à l'administrateur réseau d'assurer une sécurité efficace pour son entreprise contre toute attaque venant de l'extérieur [10].

2.2.2. Concept de base d'IP Sec

Le protocole IP Sec est destiné à fournir différents services de sécurité. Il permet grâce à plusieurs choix et options de définir différents niveaux de sécurité afin de répondre de façon adaptée aux besoins de chaque entreprise. La stratégie IP Sec permettant d'assurer la confidentialité, l'intégrité et l'authentification des données entre deux hôtes est gérée par un ensemble de normes et de protocoles :

- **Authentification des extrémités :** Elle permet à chacun de s'assurer de l'identité de chacun des interlocuteurs. Précisons que l'authentification se fait entre les machines et non entre utilisateurs, dans la mesure où IP Sec est un protocole de couche 3.
- **Confidentialité des données échangées:** Le contenu de chaque paquet IP peut être chiffré afin qu'aucune personne non autorisée ne puisse le lire.
- **Authenticité des données:** IP Sec permet de s'assurer que chaque paquet a bien été altéré lors du trajet.
- **Protection contre les écoutes et analyses de trafic :** Le monde tunneling (détaillé plus loin) permet de chiffrer les adresses IP réelles et les entêtes des paquets IP de l'émetteur et du destinataire. Ce mode permet ainsi de contrecarrer toutes les attaques de ceux qui voudraient intercepter des trames afin d'en récupérer leur contenu.

- **Protection contre le rejeu :** IP Sec intègre la possibilité d'empêcher un pirate d'intercepter un paquet afin de le renvoyer à nouveau dans le but d'acquérir les mêmes droits que l'envoyeur d'origine.

Ces différentes caractéristiques permettent à l'hôte A de crypter ses données et de les envoyer vers l'hôte B via le réseau, puis à l'hôte B de les recevoir et de les décoder afin de les lire sans que personne ne puisse altérer ou récupérer ces données [10].

2.3. Le protocole SSH

SSH (secur shel) est un tunnel de la couche 7 du model OSI, c'est un protocole permettant d'établir une cession interactive chiffré entre un client et un serveur. Ainsi, les flux d'information entre ces deux entités sont cryptés ce qui garantit la confidentialité. De plus, il permet l'identification de la machine distante. L'algorithme utilisé pour la négociation des clés est RSA (dont le brevet a expiré aux USA ce qui permet une utilisation publique légale).

Une fois l'échange des clés effectué, la communication entre les deux machines se fait en utilisant un chiffrage symétrique. Les principaux algorithmes utilisé dans SSH sont triple DES (3DES) ainsi que Blowfish. La plupart des fonctionnalités cryptographiques étant implémentés dans la bibliothèque Open SSL. La version du protocole SSH utilisé est la version 2, la première version de ce protocole souffrait d'une grosse faille de sécurité [10].

2.4. Le protocole SSL

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

SSL est le dernier arrivé dans le monde des VPN, mais il présente un grand avantage dans la mesure où coté client, il ne nécessite qu'un navigateur Internet Standard. Ce protocole est celui qui est utilisé en standard pour les transactions sécurisées sur Internet.

L'inconvénient néanmoins de ce type de protocole est qu'il se limite au protocole https, ce qui n'est pas le seul besoin de connexion des entreprises [10].

2.4.1. Les fonctionnalités de SSL

SSL a trois fonctions qui sont :

A. Authentification du serveur

Qui permet à un utilisateur d'avoir une confirmation de l'identité du serveur. Cela est fait par les méthodes de chiffrement à clés publique. Cette opération est importante, car le client doit pouvoir être certain de l'identité de son interlocuteur à qui par exemple, il va communiquer son numéro de carte de crédit [10].

B. Authentification du client

Selon les mêmes modalités que pour le serveur, il s'agit de s'assurer que le client est bien celui qu'il prétend.

C. Chiffrement des données

Toutes les données qui transitent entre l'émetteur et le destinataire, sont chiffrées par l'émetteur et déchiffrées par le destinataire, ce qui permet de garantir la confidentialité des données, ainsi que leur intégrité grâce souvent à des mécanismes également mis en place dans ce sens [10].

2.4.2. Le tunnel VPN SSL :

Les VPN permettent aux utilisateurs éloignés (à distance) avec les navigateurs internet qui permettent au contenu actif d'avoir accès au réseau protégé par une passerelle VPN. Les tunnels VPN-SSL ont beaucoup plus de capacités parce que l'on peut fournir des services plus facilement [13].

2.4.3. Principes de base du VPN SSL :

Les VPN-SSL fournissent l'accès à distance sécurisé aux ressources d'une organisation .Un VPN-SSL consiste en un ou plus de dispositifs VPN que les utilisateurs connectent à l'utilisation de leur navigateurs internet. Le dispositif est crypté avec le protocole SSL quand il y a le trafic entre le navigateur internet et VPN-SSL.

VPN-SSL fournissent aux utilisateurs éloignés l'accès aux applications web et les demandes de client/serveur et avec connectivité à réseaux internes. Ils offrent la polyvalence et la facilité d'emploi parce qu'ils utilisent le protocole SSL qui est inclus avec tout les

navigateurs web standard ; si le client n'exigent pas d'habitude de configuration par l'utilisateur [13].

2.4.4. Architecture du VPN SSL :

La figure fournit une vue de haut niveau de l'architecture typiqyue VPN-SSL. Cette architecture est le même tant pour le portail VPN-SSL que pour le tunnel VPN-SSL.

VPN-SSL typique des utilisateurs inclut les gens dans des fonctions éloignés à distance, des utilisateurs mobiles, désassociés et des clients.

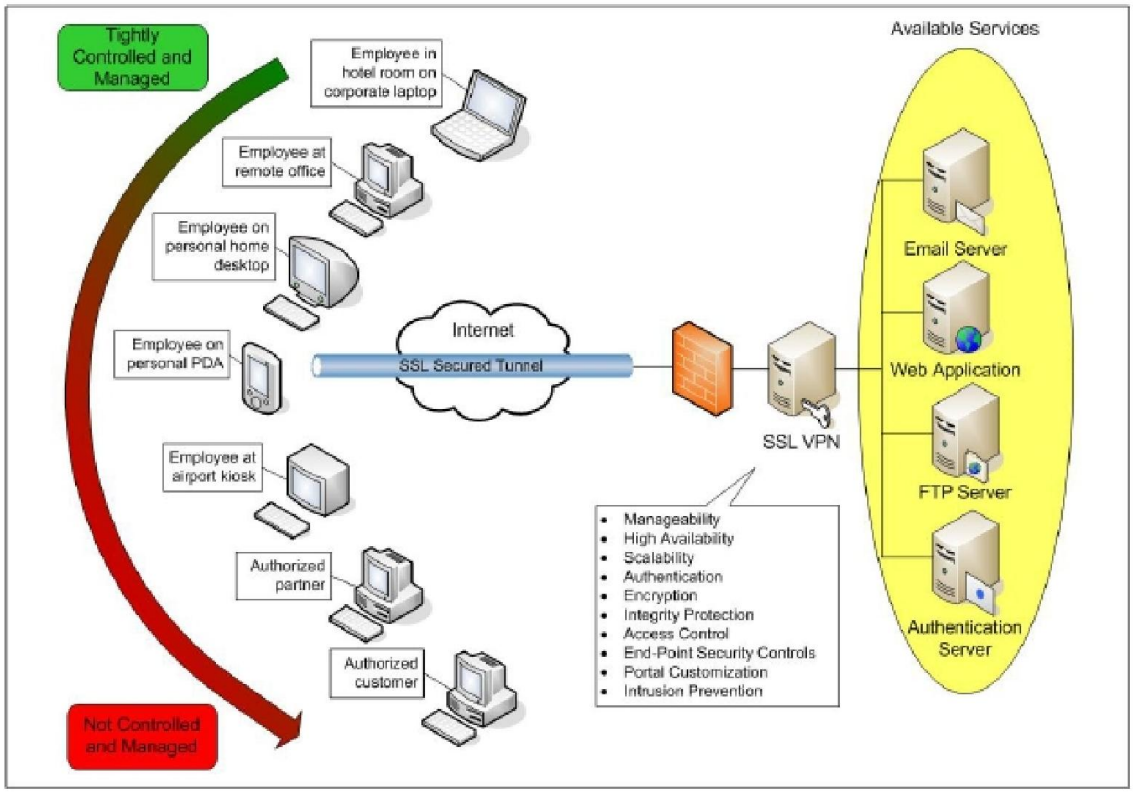

Figure.30. architecture du VPNSSL [13]

Les clients de matériel incluent les types divers de dispositifs, comme des kiosques publics, des ordinateurs individuels domestiques comme le pc, ou des smartphones, qui peuvent ou ne peut pas être contrôlé ou géré par l'organisation. Le VPN-SSL peut aussi être eu accès de n'importe quel emplacement incluant un aéroport, un café, ou une chambre d'hôtel, tant que l'emplacement a la connectivité à internet et l'utilisateur a un client web qui est capable d'utiliser le détail VPN-SSL. Tout le trafic est crypté comme il traverse des réseaux publics comme internet. Le VPN-SSL la passerelle est le critère pour la connexion sécurisé et fournit des services divers et des caractéristiques [13].

2.4.5. Les fonctions du VPN-SSL

La fourniture de l'accès éloigné sécurisé à une large variété d'utilisateurs, et des dispositifs à beaucoup d'emplacements, appelle à un ensemble divers des services de VPN-SSL et des caractéristiques. La plupart des VPN-SSL ont un ou plus de trois fonctions principales suivant :

2.4.5.1. Le proxy

Une procuration est un dispositif intermédiaire ou un programme qui fournit la communication et d'autres services entre un client et un serveur. Il a la capacité de se représenter comme le serveur au client et vice versa .Une procuration peut entretenir des demandes intérieurement ou traduire les informations et les transmettre à d'autres serveurs. Le Proxy est une fonction principale d'un VPN-SSL. La forme la plus simple d'un VPN-SSL implique proxy sécurisé de pages web. Le VPN-SSL agit comme une passerelle en servant d'intermédiaire [13].

2.4.5.2. Traduction d'applications

La traduction d'applications convertit des informations d'un protocole à un autre. Il est souvent utilisé pour convertir un protocole propriétaire vers un protocole plus largement utilisé ou standard. Il est aussi utilisé pour faciliter l'intégration des applications et la communication entre celles-ci.

La traduction d'applications utilise le proxy pour interagir avec les deux côtés de la connexion selon le protocole approprié. Le tunnel VPN-SSL utilise la traduction d'applications pour les systèmes qui n'ont pas d'interfaces Web. Ceci permet aux utilisateurs d'exploiter un simple navigateur Internet pour accéder aux applications qui n'ont pas leurs propres interfaces web [13].

2.4.6. Les caractéristiques du VPN-SSL

2.4.6.1. Possibilité de gestion

La possibilité de gestion inclut la gestion du dispositif, le rapport de statut et l'enregistrement. Le VPN-SSL assure la disponibilité des services à tout moment [13].

2.4.6.2. Adaptabilité

L'adaptabilité est la capacité de supporter plus d'utilisateurs, des sessions simultanées et la sortie que VPN-SSL seul peut manipuler [13].

2.4.6.3. Personnalisation

La personnalisation est la capacité de contrôler l'apparition du VPN-SSL que les utilisateurs voient quand ils accèdent au page web. Les tunnels personnalisés sont souvent nécessaires pour utiliser le VPN-SSL dans le cas des Smartphones [13].

2.4.7. Les services de sécurité du VPN-SSL sont

2.4.7.1. Chiffrage et protection d'intégrité

Le chiffrage protège la confidentialité des données, tandis que la protection d'intégrité assure que les données ne sont pas changées.

2.4.7.2. Contrôle d'accès

Le contrôle d'accès permet de limiter l'accès aux demandes formulées soit par l'utilisateur, soit par groupe d'utilisateurs.

2.4.7.3. Contrôle des critères de sécurité

Les contrôles des critères de sécurité valident la conformité de la sécurité d'un système client qui essaye d'utiliser le VPN-SSL. Ils incluent aussi les mécanismes de protection de la sécurité, comme des nettoyeurs du cache d'un navigateur Internet, qui enlèvent des informations sensibles [13].

2.4.7.4. Prévention d'intrusion

La prévention d'intrusion implique l'inspection des données après le décryptage dans le VPN-SSL afin d'éviter des attaques potentielles. Il peut aussi inclure la fonctionnalité d'anti-logiciel-malveillant pour détecter des virus.

2.4.7.5. Haute disponibilité et adaptabilité

Deux autres caractéristiques importantes pour le VPN-SSL sont la haute disponibilité et l'adaptabilité. Des hautes solutions de disponibilité de VPN-SSL utilisent deux ou plus des dispositifs configurés.

.2.4.7.6 Authentification

VPN-SSL supportent le service de sécurité d'identification directement par une méthode intégrée d'identification, ou indirectement via un serveur externe d'identification ; ou tous les deux .L'authentification de page WEB SSL traditionnelle compte sur l'authentification de coté de serveur, pour que les utilisateurs aient confiance en serveur avec qui ils communiquent.

L'authentification du VPN-SSL prend un pas ; une étape plus loin en exigeant tant l'authentification de coté de client que coté serveur. VPN-SSL supportent des méthodes d'authentification de client flexibles ,comme le nom d'utilisateur et le mot de passe ,des crêts à puce ,l'authentification a deux facteurs et des certificats numériques X.509.Pour l'utilisation de méthodes impliquant des jetons ,le VPN-SSL doit pouvoir manipuler les messages divers ,comme des requêtes de changement de PIN ,qui sont impliquées dans des solutions symboliques.

Quand des certificats numériques qui contiennent une clé publique. Un critère a son propre certificat numériques sont utilisés pour l'authentification de client .chaque critère a son propre certificat numérique qui contient une clé publique .un critère utilise la clé privée correspondante pour en forme digitale signer des données avant l'envoie cela é l'autre critère, qui vérifie la signature utilisant la clé publique du pair.

VPN-SSL besoin l'accès à l'information de groupe sur les serveurs d'identification depuis la sécurité et le contrôle d'accès est souvent exprimé en termes de groupes. Un certain des produits VPN-SSL utilisent aussi les informations contenues dans des serveurs d'identification pour prendre des décisions de contrôle d'accès supplémentaires, comme la limitation du nombre de mauvaises tentatives de mot de passe [13].

2.4.8. Inconvénients

Utilisation des certificats X .509

2.4.9. Avantage

- Authentification forte du client
- Maintenant, de nombreuses applications utilisent SSL/TLS.
- Confidentialité et intégrité des échanges

- L'utilisateur utilise les mêmes logiciel sur son Lan que à l'extérieur .les communications sur LAN sont également sécurisées.

2.4.10. Utilisation

- VPN d'accès (nomades à site)
- Intranet, extranet (sites à sites)
- LAN

3. Discussion

Ce chapitre est consacré à l'étude générale du VPN-SSL qui est le dernier arrivé dans le monde des VPN, mais il présente un grand avantage dans la mesure où coté client .Nous avons détaillé un peut sur ces caractéristiques et ces fonctions principale.

Dans le chapitre suivant nous allons présentés les différentes étapes qui nous permettrons la bonne réalisation de notre application.

Chapitre 4
Mise en place D'un tunnel VPN-SSL

1. Préambule

L'objectif de cette partie pratique est de sécuriser la connexion entre deux réseaux locaux. Cette sécurité est assurée par l'utilisation du protocole de tunneling qui est le VPN LAN to LAN en utilisant le protocole SSL. Ce dernier permet à des utilisateurs dans un réseau local d'entreprise de se connecter avec des utilisateurs d'une autre entreprise de façon sécurisée.

2. La topologie

Voici la topologie que nous avons choisi de mettre en place pour la création de notre VPN :

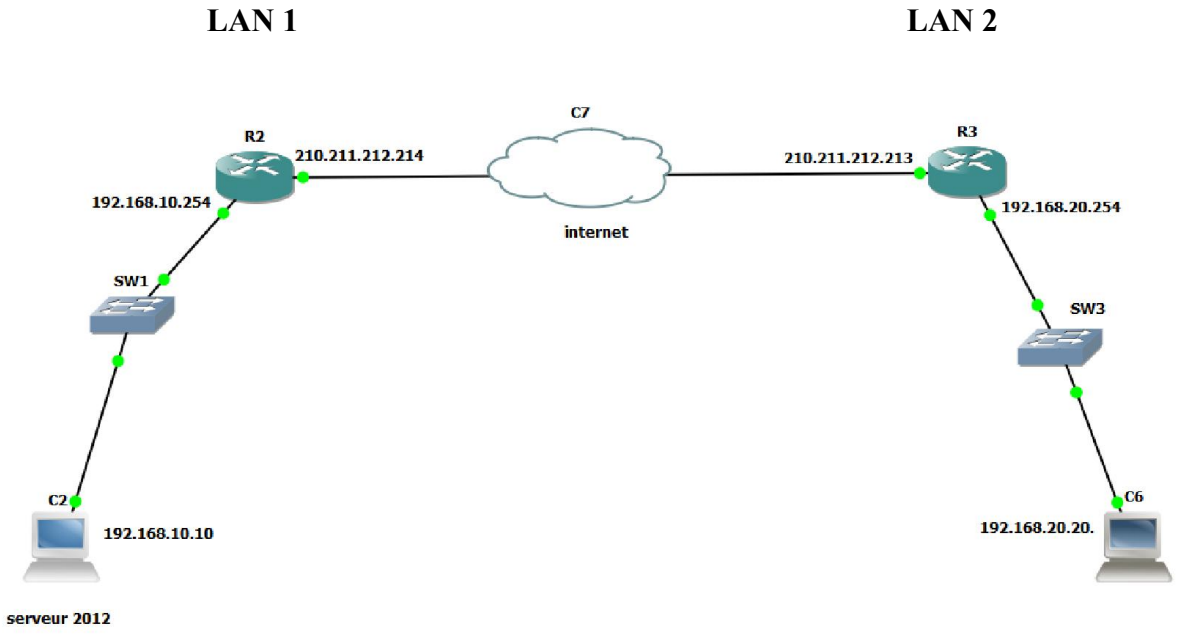

Figure.31. La topologie de la simulation du tunnel LAN to LAN

3. Equipements requis

Pour faire fonctionner notre configuration, nous avons utilisé plusieurs équipements. Parmi lesquels, un serveur Windows qui est relier à un Switch avec le routeur R 2. Ce dernier, nous allons le configuré de sorte qu'il soit dans le même réseau que le Switch SW1 et le serveur.

Pour faire le test du protocole SSL, nous avons créé un autre réseau LAN2 qui est composé d'une machine cliente reliée au Switch SW3 puis vers le routeur R3. Les deux réseaux LANs sont connectés via Internet.

4. Logiciels utilisés

Pour simuler et tester la topologie réseau décrite par la figure précédente, nous avons utilisés des logiciels et des outils de tests.

4.1. Le logiciel « GNS 3 »

GNS3 est un simulateur graphique d'équipements réseaux qui nous permet de créer des topologies de réseaux complexes et d'établir des simulations. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco. L'IOS est le système d'exploitation des routeurs et Switch et firewall Cisco.

4.1.1. Pour créer un projet sous GNS3

Nous allons lancez le logiciel GNS3 :

Figure.32. Raccourci GNS3

4.1.2. Nouveau Projet

Cochez les options « Sauver les NVRAMs et autres disques virtuels » et « Sauvegarder les startup-configs des IOS ». 'Nom du projet ' tapez ' Res 1 ' .cliquez sur le bouton 'OK'

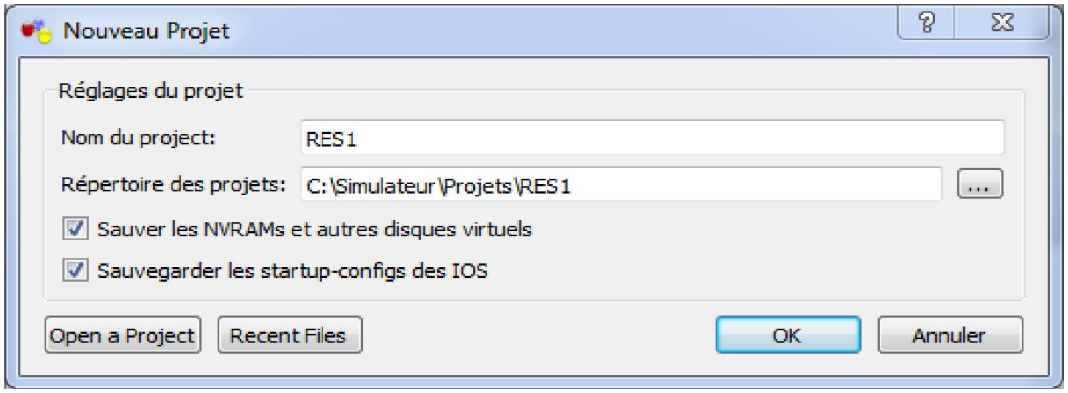

Figure .33. Ouverture d'un nouveau projet sur GNS3

4.2.VMware Workstation

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web.

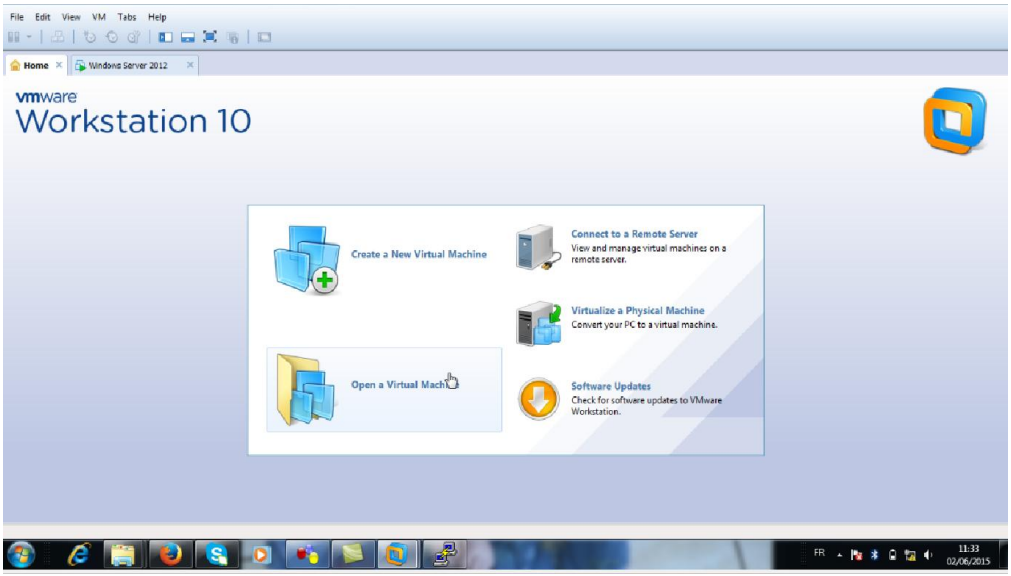

Figure.34. Fenêtre principale de VMware Worksation

4.3. TFTP (Trival File Transfer Protocol ou **protocole simplifié de transfert de fichiers)** est un protocole simplifié de transfert de fichiers, il fonctionne en UDP. Il est très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu …) ou pour démarrer un pc à partir d'une carte réseau

4.4. Anyconnect-win-2.7 : Cisco Anyconnect VPN client est un client **VPN propriétaire** permettant de se connecter aux concentrateurs VPN Cisco. Il s'agit du client de nouvelle génération de l'éditeur, il est limité aux fonctionnalités de type SSL,

5. Microsoft Windows Server 2012

Microsoft Windows Server 2012 est conçu pour fournir aux entreprises la plate-forme la plus productive pour virtualiser les charges de travail, en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web

5.1. Ouverture et configuration de Windows serveur 2012

Nous allons ouvrire VM Worworkstasion pour créer une nouvelle machine virtuelle. Puis nous installons Windows 2012 Server sur cette machine.

Au lancement de cette machine virtuelle, nous allons introduire un mot de passe comme indiqué par la figure suivante.

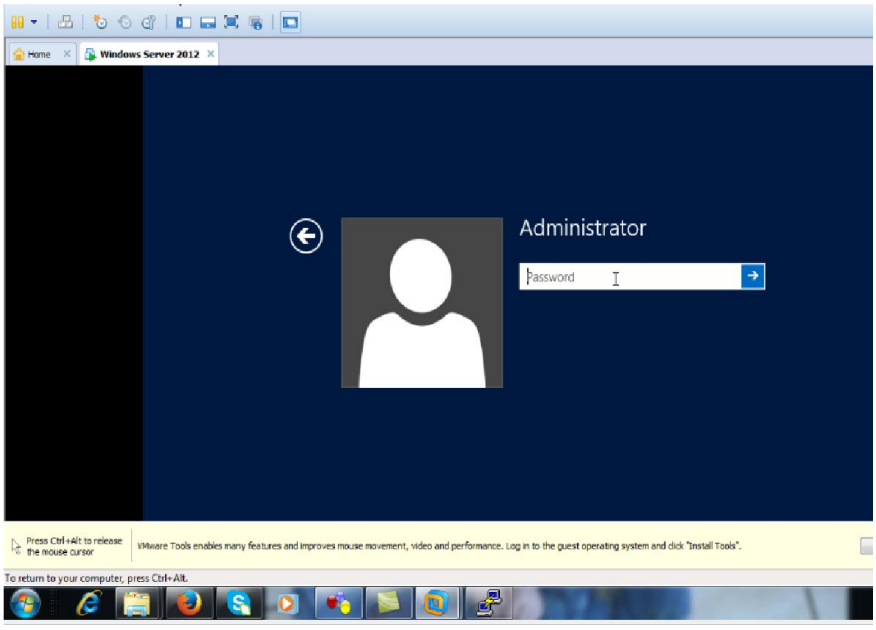

Figure .38. La machine virtuelle serveur crée avec VMware.

Ensuite, nous allons accéder à la fenêtre « Connexion réseau » pour introduire l'adresse IP et l'adresse de la passerelle du serveur.

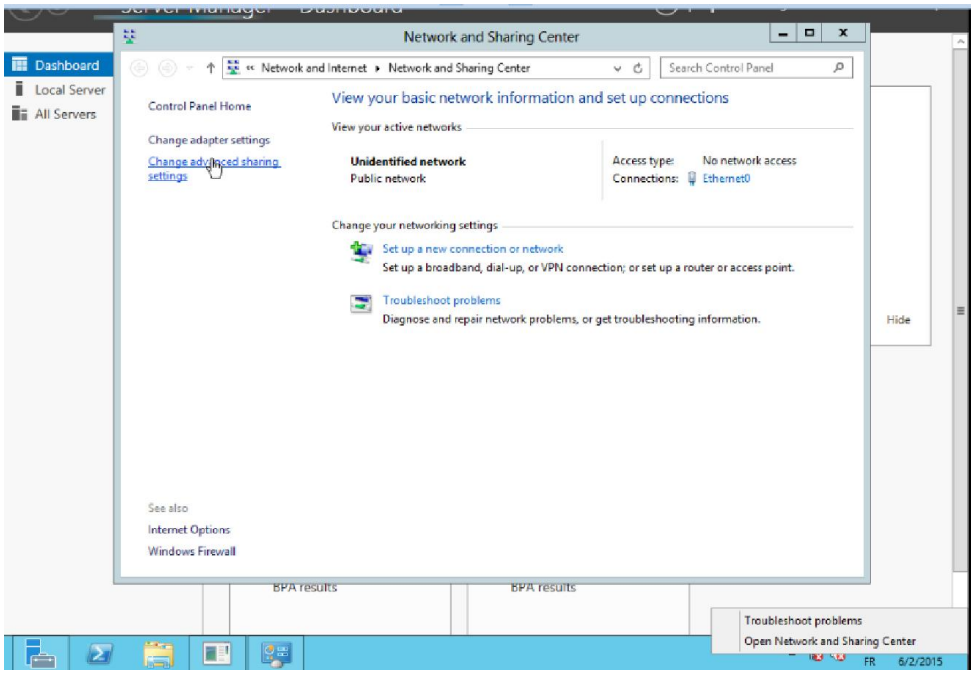

Figure .39. La fenêtre connexion réseau

L'adresse IP choisie pour le serveur est 192.168.10.254 et l'adresse de la passerelle sera 210.211.212.214.

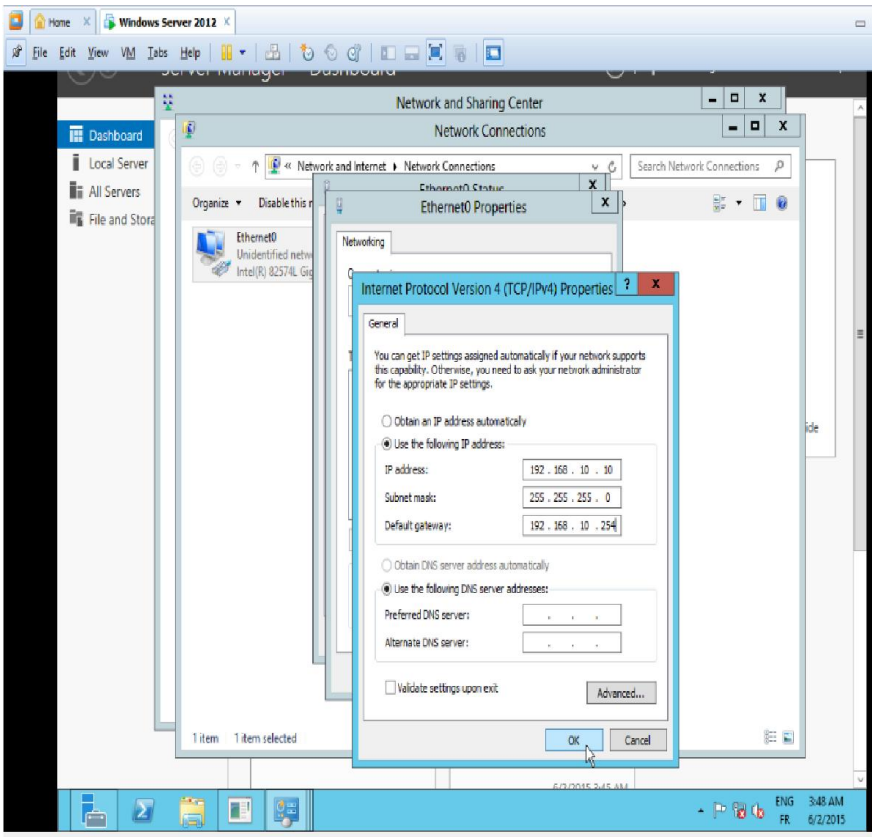

Figure.40. L'adresse IP configurée pour le serveur

5.2. Configuration du poste client

Nous allons saisir l'adresse IP de la machine cliente qui est 192.168.20.20 ainsi que l'adresse de la passerelle qui est 192.168.20.254

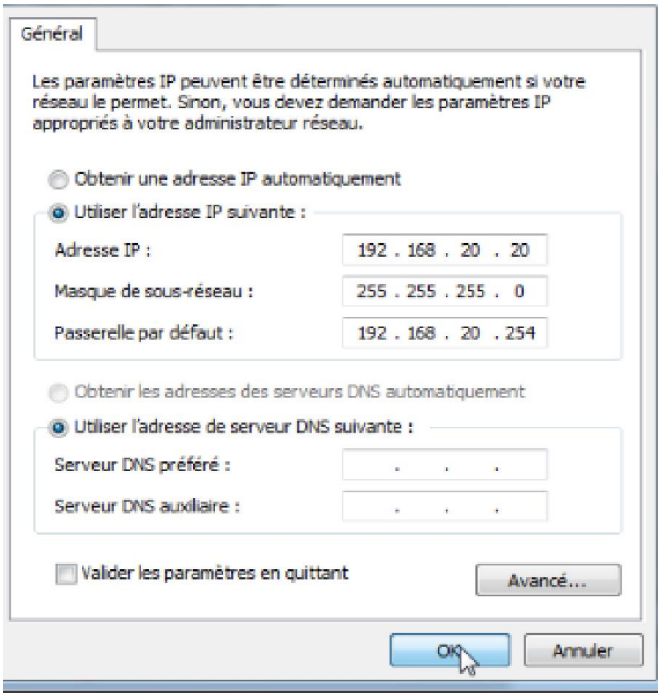

Figure.41. L'adresse IP configurée pour le poste client

6. Configuration des routeurs

6.1. Routeur R2

Configuration des interfaces du routeur R2 :

```
R2(config)#inter
R2(config)#interface fast
R2(config)#interface fastEthernet 0/0
R2(config-if)#ip addr
R2(config-if)#ip address 192.168.10.254 255.255.255.0
```

```
R2(config-if)#no shutdown
```

```
R2(config)#interface fas
R2(config)#interface fastEthernet 0/1
R2(config-if)#ip addre
R2(config-if)#ip address 210.211.212.214 255.255.255.252
R2(config-if)#no shut
R2(config-if)#no shutdown exit
                           ^
% Invalid input detected at '^' marker.

R2(config-if)#no shu
R2(config-if)#no shutdown
R2(config-if)#exit
```

Les interfaces sont maintenant activées.

6.2. Routeur R3

Configuration des interfaces du routeur R3 :

```
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip add
R3(config-if)#ip address 192.168.20.254 255.255.255.0
R3(config-if)#no sh
R3(config-if)#no shutdown
R3(config-if)#
```

```
R3(config)#interface fas
R3(config)#interface fastEthernet 0/1
R3(config-if)#ip add
R3(config-if)#ip address 210.211.212.213 255.255.255.252
R3(config-if)#no shut do
R3(config-if)#no shut
R3(config-if)#no shutdown
R3(config-if)#exit
```

Les interfaces sont maintenant activées.

Pour afficher les interfaces que nous avons configurées ont met la commande : **IP interface breif ou bien br**

```
R3#show ip interfa
R3#show ip interface brei
R3#show ip interface br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.20.254  YES manual up                    up
FastEthernet0/1            210.211.212.213 YES manual up                    up
R3#
```

6.3.Configuration du NAT (traduction des addresses reseau)

La fonction NAT dans un routeur traduit les adresses IP sources (interne) (privé) en addresses IP global (externe)(publique) .

Nous configurant le NAT avec les commandes : **ip nat outside** et **ip nat inside**

```
R3#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interfa
R3(config)#interface
R3(config)#interface fas
R3(config)#interface fastEthernet 0/0
R3(config-if)#ip nat inside
R3(config-if)#ip nat inside
```

```
R3(config-if)#interface fastethernet 0/1
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#
```

6.4. Configuration de l'ACL :

Pour pouvoir autoriser le trafic entre un réseau de niveau de sécurité inferieur à un autre réseau de niveau de sécurité supérieur, nous faisons appel aux ACL. Ces derniers permettent de mettre en place la stratégie de filtrage à appliquer

Nous configurons un ACL avec la commande suivante : **access-list ….. permit any**

Cette configuration montre que seul les 20 adresses du LAN1peuvent acceder au réseu LAN 2

```
R3(config)#access-list 20 permit any
R3(config)#ip nat inside sou
R3(config)#ip nat inside source list ?
  <1-2699>  Access list number for local addresses
  WORD      Access list name for local addresses
```

```
R3(config)#ip nat inside source list 20 interface fastEthernet 0/1
```

Pour afficher les adresses IP NAT interne et externe nous tapons cette commande :

Show ip nat translations

```
R3#
*Jun  2 14:39:10.687: %SYS-5-CONFIG_I: Configured from console by console
R3#show ip nat trans
R3#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 210.211.212.213:1 192.168.20.20:1    210.211.212.214:1  210.211.212.214:1
R3#
```

Pour sauvgarder nous tapons la commande '**wr**'

6.5. Configuration du VPN-SSL :

1-Créer l'association locale avec les adresses IP qui seront assignées aux utilisateurs VPN

Avec la commande ' **IP local pool** '

2-Créer le nouveau model d'authentification avec la commande : **aaa new-model**

```
R2(config)#ip local pool sslpool
%IP address not allowed in pool: 0.0.0.0
R2(config)#ip local pool sslpool 192.168.10.11 192.168.10.21
R2(config)#aaa new
R2(config)#aaa new-model
```

3-nous utilisons le type d'authentification local avec la commande : **aaa authentication login webssl local**

```
R2(config)#aaa authentication login webssl local
```

4-Créer le nom d'utilisateur et le mot de passe avec la commande : **username tal secret test123**

5-Créer une passerelle WEBVPN , cette commande va construire automatiquement un **certificat signé** avec la commande : **webvpn gatway algerie-telecom**

```
R2(config)#username tal secret test123
R2(config)#webvpn gateway algerie-telecom
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

6-Entrer une adresse IP et un port pour la passerelle qui est : **port 443**

7-Configurer le chiffrage de type chiffrage SSL ; pour surmonter la mise à jour de sécurité de Microsoft avec la commande : **ssl encryption rc4-md5**

8-donner le certificat à la passerelle web VPN de type : " point de confiance SSL ' le nom de certitude.avec la comande : **do show run b crypto**

```
R2(config-webvpn-gateway)#ip address 210.211.212.214 port 443
R2(config-webvpn-gateway)#ssl encryption rc4-md5
R2(config-webvpn-gateway)#do show run i b crypto
```

```
R2(config-webvpn-gateway)#ssl trustpoint tp-self-signed-4279256517
```

```
R2(config-webvpn-gateway)#inservice
R2(config-webvpn-gateway)#exit
```

9-Créer une page web VPN contexte de type : **Web VPN**

```
R2(config)#webvpn context tal-webvpn
```

10-Donner un titre à la page

11-taper le message de connexion mis à la page

12-Assigner l'authentification avec la commande : **aaa authentification list web ssl**

```
R2(config-webvpn-context)#title "algerietelecom-webvpn"
R2(config-webvpn-context)#login-message "webvpn login"
R2(config-webvpn-context)#aaa authenticat
R2(config-webvpn-context)#aaa authentication list web ssl
                                                      ^
% Invalid input detected at '^' marker.

R2(config-webvpn-context)#aaa authentication list webssl
AAA list webssl is not defined, default list will be used
```

13-Assigner la nouvelle passerelle Web VPN que nous avons créé avec la commande : **gatway algerie-telecom**

14-Définir le maximum des utilisateurs pour permettre l'accès au même temps avec la commande : **max users**

15-Créer le **URL** de la liste qui sera affichée au type de page : **"URL inscrivent" le nom de liste "**

```
R2(config-webvpn-context)#gate
R2(config-webvpn-context)#gateway algerie-telecom
Configure gateway algerie-telecom using "webvpn gateway" command before associating to context
```

```
R2(config-webvpn-context)#max-use
R2(config-webvpn-context)#max-users 10
R2(config-webvpn-context)#url-list "MyPages"
```

16-Définir l'entête de cette liste

```
R2(config-webvpn-url)#heading "MyPages"
```

17- Définir le nom et la valeur de l'url

```
R2(config-webvpn-url)#url-text companyweb url-value "http://companyweb.local"
R2(config-webvpn-url)#exit
```

18- Créer un ACL

```
R2(config)#acl webvpn-acl
```

19-Autoriser le trafic des utilisateurs VPN au type de réseau cible avec la commande : **permit ip 192.168.10.0 255.255.255.0**

20-Sortir du mode ACL

21-Créer un groupe politique de gestion avec la commande : **policy group sslpolicy**

22-attribuer la liste d'url que nous avons crée, avec la commande :

Url-liste url-list-name

```
R2(config-webvpn-acl)#permit ip 192.168.10.0 255.255.255.0
% Incomplete command.

R2(config-webvpn-acl)#$92.168.10.0 255.255.255.0 192.168.10.0 255.255.255.0
R2(config-webvpn-acl)#policy group sslpolicy
R2(config-webvpn-group)#url-list MyPages
```

23-Le client VPN doit être installé sur le PC juste après l achèvement de la session tunnel avec la commande : **functions svc-enabled**

24-Garder le client VPN installé sur le pc après que la session tunnel soit finie,avec la commande : le type ASV le client a installé **svc keep-client-in**

25-donner les adresses IP aux utilisateurs VPN de l'association d'adresse que nous avons créée précédemment avec la commande :**svc keep-client –installed**

26-Spécifier que le client établit un nouveau tunnel pendant crypto renégocie avec la commande : **filter tunnel webvpn-acl**

27-Répartir et spécifier le trafic qui passera par le tunnel avec la commande :**svc address-pool sslpool**

28-Sortir de la politique du groupe avec la commande : **-svc rekey method new-tunnel**

-Svc split include 192.168.10.0. 255.255.255.0

29-Le mode contrat collectif de sortie, tapez la sortieavec la commande : **exit**

```
R2(config-webvpn-group)#functions svc-enabled
R2(config-webvpn-group)#svc keep-client-in
R2(config-webvpn-group)#svc keep-client-installed
R2(config-webvpn-group)#filter tunnel webvpn-acl
R2(config-webvpn-group)#svc add
R2(config-webvpn-group)#svc address-pool sslpool
R2(config-webvpn-group)#svc rek
R2(config-webvpn-group)#svc rekey meth
R2(config-webvpn-group)#svc rekey method ne
R2(config-webvpn-group)#svc rekey method new-tunnel
R2(config-webvpn-group)#svc spli
R2(config-webvpn-group)#svc split inc
R2(config-webvpn-group)#svc split include 192.168.10.0 255.255.255.0
R2(config-webvpn-group)#exit
R2(config-webvpn-context)#
```

30-Définir la politique du groupe par défaut avec la commande :**default-group-policy sslpolicy**

31-Activez la configuration contexte du WEBVPN avec la commande : **inservice**

32-Sortir

33-Sortir

```
R2(config-webvpn-context)#defau
R2(config-webvpn-context)#default-group-policy sslpo
R2(config-webvpn-context)#default-group-policy sslpolicy
R2(config-webvpn-context)#inservi
R2(config-webvpn-context)#inservice
R2(config-webvpn-context)#exit
R2(config)#exit
R2#e
*Jun  4 11:17:49.423: %SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

34-Sauvegarder la configuration sous le mode privilégié avec la commande : **copy running-config startup-config**

35-Le type montre le disque avec la commande : **do show disk0**

```
R2#copy running-con
R2#copy running-config st
R2#copy running-config startup-config
Destination filename [startup-config]? configure t
%Error copying nvram:configure (Invalid argument)
R2#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#web
% Incomplete command.

R2(config)#do show disk0
Unformatted Partition, please format it.
```

7. Verification

Nous testons la création d'un tunnel VPN entre les deux réseaux en éffectuant les actions suivantes :

- Ping de la machine client du reseau 2 vers la passerelle du routeur R3 du meme reseau
- Ping de la machine client du reseau 2 vers la passerelle du routeur R2 du reseau 1
- Ping du serveur du reseau 1 vers la passerelle du routeur R2 du meme reseau
- Ping du serveur du reseau 1 vers la passerelle du routeur R3 du reseau 2
- Ping de la machine client du reseau 2 vers la passerelle du reseau WAN (internet)

Nous avons essayé notre tests ping et les resultats sont presentés ci –dessous :

- Ping de la machine client du réseau 2 vers la passerelle du routeur R3 du même réseau

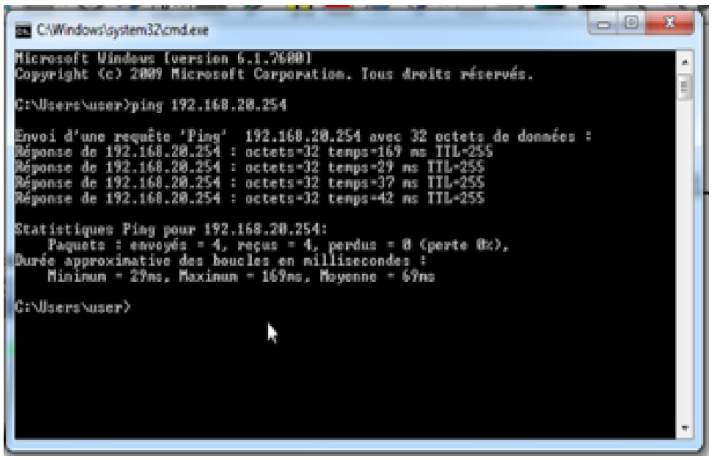

Figure.42. ping de la machine vers la passerelle du LAN2

- Ping de la machine client du reseau 2 vers la passerelle du reseau 1

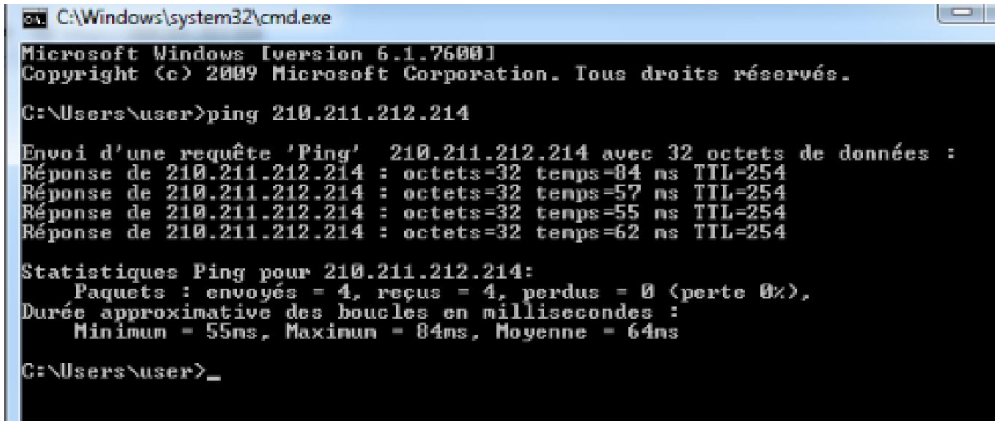

Figure.43. ping de la machine vers la passerelle du LAN 1

Nous avons tester la connexion de la machine cliente vers la passerelle de l'autre reseau LAN en traversant le reseau WAN (Internet). Nous avons utilisés la commande ping et nous avons obtenus 100% de paquets reçues. Ceci montre que le protocole SSL a bien été appliqué et que l'utilisateur du reseau peut accéder au deuxième reseau en toute securité.

- Ping du serveur du réseau 2 vers le routeur R2 du même réseau

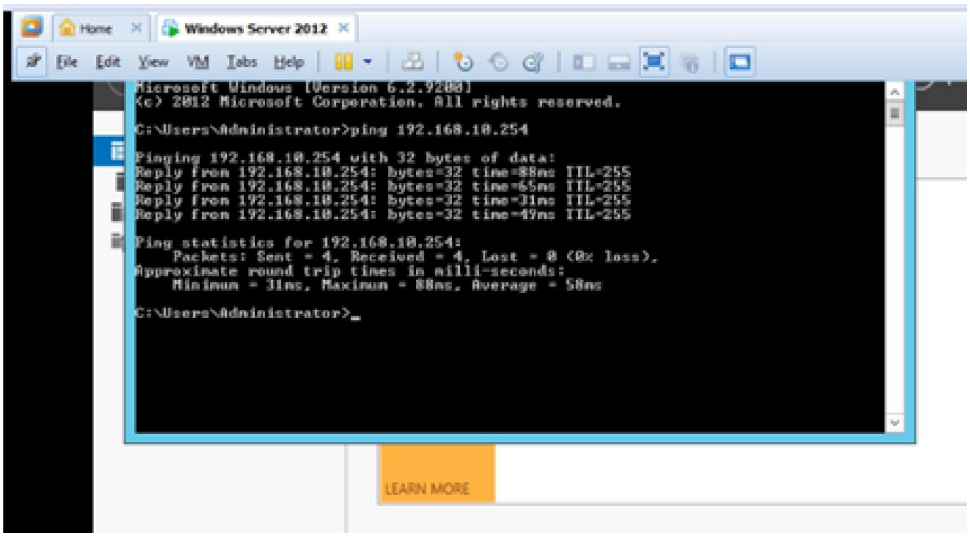

Figure.44. ping du serveur vers le routeur du LAN 1

- Ping du serveur du reseau LAN 1 vers la machine cilent de reseau 2

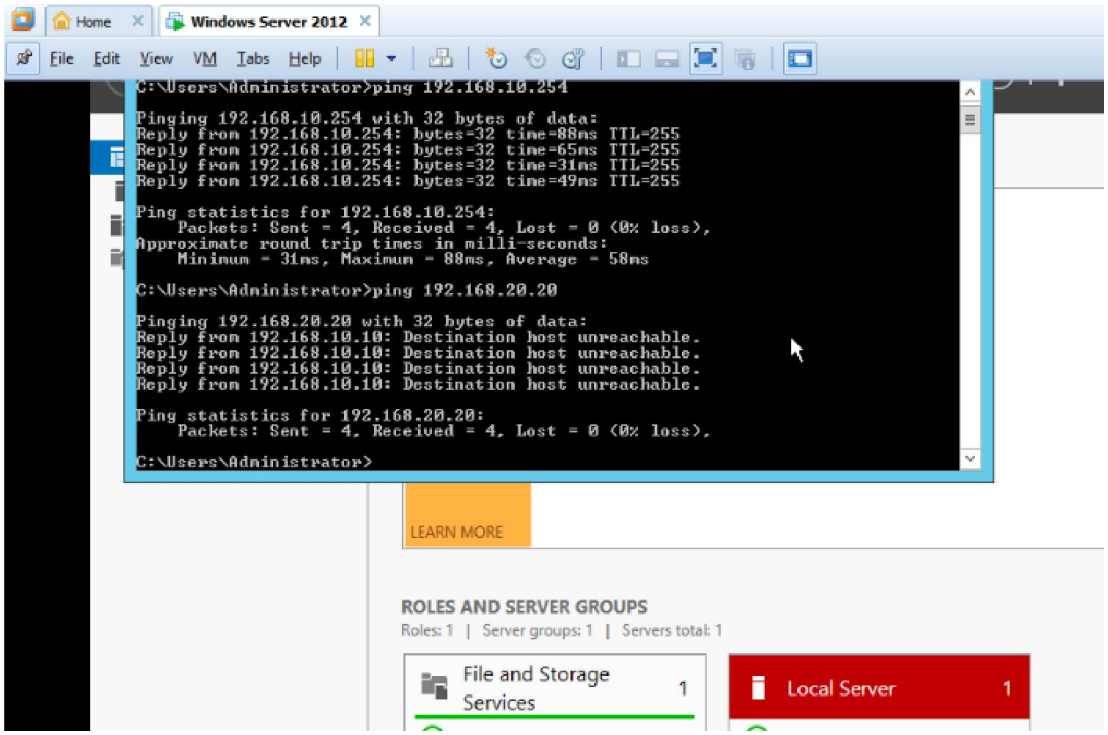

Figure.45. ping du serveur vers la machine client

- Pingé de la machine client vers la passerelle du réseau WAN (internet)

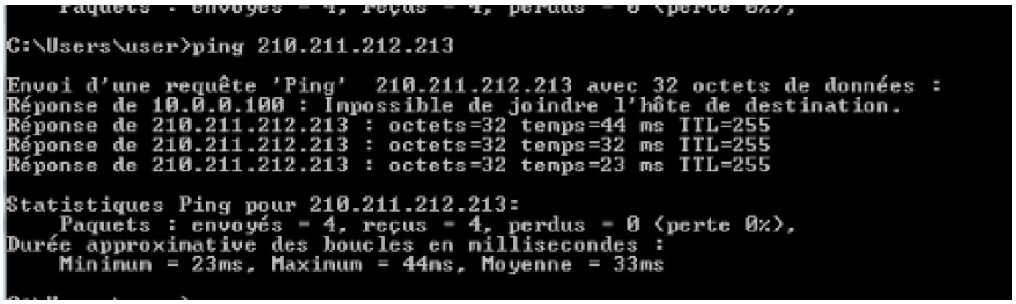

Figure.46. Ping de la machine client vers la passerelle WAN

Toute les requêtes Ping sont réussi on peut accéder d'un réseau a un autres on toute sécurité

8. Discussion :

D'après les résultats de la simulation, nous constatons que la liste de contrôle d'accès ACL, le NAT et le VPN-SSL appliqués aux routeurs R2 et R3 permettent de créer une connexion sécurisée entre deux réseaux LAN. En effet, les utilisateurs du LAN 1 ont accès aux ressources du réseau LAN 2. De plus, le tunnel VPN créé permet de bloquer la plupart des menaces de sécurité réseau.

Conclusion

CONCLUSION

Dans ce mémoire, nous nous sommes intéressé à mettre en place une application permettant à l'utilisateur l'accès aux différents ressources de l'entreprise de n'importe quel endroit. Nous avons simulée cette application en prenant comme exemple une machine cliente qui se connecte à une autre machine serveur. Cette simulation est réalisée en utilisant principalement GNS3 et VMware. Ensuite, nous avons configuré le protocole SSL dans les routeurs.

Nous avons aussi configuré l'ACL pour pouvoir autoriser le trafic entre un réseau de niveau de sécurité inferieur vers un autre niveau de sécurité supérieur en utilisant une stratégie de filtrage.

L'utilisation du NAT dans notre simulation permet la traduction des adresses IP privés en IP publiques.

Les tests de connexion effectués montrent le bon fonctionnement du VPN. Ce dernier reste une solution de sécurité permettant de relier entre deux sites distants.

Comme perspectives, nous proposons l'implémentation pratique de cette simulation et d'effectuer des attaques sur le réseau réalisé pour vérifier que le protocole SSL est très sécurisé.

Bibliographie

[1] : G. Lehembre, Sécurité Wi-Fi: WEP, WPA, WPA2, Hakin9 Magazine, no 1, Janvier 2006.

[2] : Jon Edney and William A. Arbaugh, Wi-Fi Protected Access and 802.11i, September 2004.

[3] : Melle Belhariz ASMA , mémoire de fin d' études licence en informatique , Sécurité réseau , étude le cas de service open-VPN ,27 juin 2013 a Tlemsan .

[4]: M. Ballasterons, Les technologies sans fil, ED Eyrolles, juin 2002.

[5] : Melle .Katia.Atoui ; Mémoire de fin d'etudes en master 2, Etude des protocoles Sur les réseaux informatique, 2010/2011 ,Tizi Ouzou.

[6] : Guy Pujolle, Les réseaux sans fil, ED Eyrolles, 5ème édition, 2006.

[7] : G. Pujolle, O. Salvatori et J. Nozick, Les Réseaux et Télécommunication, Édition Eyrolles, Paris, 2004.

[8] : Melle Abtout .Nadjia ,Douani .Dalila, Mémoire de fin d'études en master2 réseau et télécommunication , Sécurisation d'une infrastructure DMZ avec ASA 5510,2012/2013.

[9] : Melle Chekal . Saida ,Ait Dahmane .Nouara ,mémoire de fin d'études en master 2, mise en place d'un tunnel VPN implémenté sur ASA Cisco,2012/2013 université mouloud Mammeri Tizi Ouzou.

[10] : Melle Sadoud.lila, Melle saddedine .Malika, Mémoire de fin d'études en master2 réseau et télécommunication, Implémentation d'une solution d'interconnexion entre deux forets différents avec une relation d'approbation et VPN site a site.

[11] : Willan .Landri , master européen en informatique :« Mise en place d'une architecture VPN MPLS avec gestion du temps de connexion et de la bande passent utilisateur » ,2009.

[12] : Carlos M.Gutierrez , GuideTo SSL VPNs ,july 2008, US department of commerce .

Annexe

ALGERIE TELECOM

ALGERIE TELECOM, est une société par actions à capitaux publics opérant sur le marché des réseaux et services de communications électroniques

Sa naissance a été consacrée par la loi 2000/03 du 5 août 2000, relative à la restructuration du secteur des Postes et Télécommunications, qui sépare notamment les activités Postales de celles des Télécommunications

ALGERIE TELECOM est donc régie par cette loi qui lui confère le statut d'une entreprise publique économique sous la forme juridique d'une société par actions SPA.

Entrée officiellement en activité à partir du 1er janvier 2003, elle s'engage dans le monde des Technologies de l'Information et de la Communication avec trois objectifs :

-Rentabilité
-Efficacité
- Qualité de service

Son ambition est d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel.
Son souci consiste, aussi, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie.

Missions

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles…
- Développer, exploiter et gérer les réseaux publics et privés de télécommunications ;
- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

Les objectifs

ALGERIE TELECOM est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales ;
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications ;
- Développer un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.

Organisation d'Algérie Télécom

ALGERIE TELECOM est organisée en Divisions, Directions Centrales, et Régionales, a cette structure s'ajoutent deux filiales:
- Mobile (Mobilis)
- Télécommunications Spatiales (RevSat)

Le laboratoire des équipements de télécommunications (LET ALGER)

Est un établissement à caractère national dépondant de la direction territoriale d'Alger (Algérie Telecom).

Il a pour mission d'assure certaines taches

- **Département Bancaire (Transmission Données)**

- Réalisations des lignes X25.
- Exploitation des réseaux.
- Prise en charge des dérangements des lignes X25.

- **Département Approvisionnement**

- Pièces détachées (composants électroniques).
- Equipements informatiques.
- Equipements Réseaux.

- **Département WLL**

- Maintenance des terminaux WLL.

- **Département AXE**

- Maintenance des cartes AXE (Central téléphonique).

- **Service réseau informatique**

- Maintenance Soft et Hard des Micro Ordinateurs.
- Installation des réseaux d'entreprise LAN, WAN

C'est à cette dernière où se déroule le stage pratique, objet de l'élaboration du présent mémoire.

Intranet

Un **intranet** est un réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle qui utilise les mêmes protocoles qu'Internet (TCP, IP, HTTP, , etc...). Parfois, le terme se réfère uniquement au site web interne de l'organisation, mais c'est souvent une partie bien plus importante de l'infrastructure informatique d'une organisation. Dans les grandes entreprises, l'intranet fait l'objet d'une gouvernance particulière en raison de sa pénétration dans l'ensemble des rouages des organisations, et de la sécurité nécessaire à sa circonscription à l'entreprise. Les grands chantiers de l'intranetisation des entreprises sont :

1. La rapidité des échanges de données qui engendre une diminution des coûts de gestion
2. L'accessibilité des contenus et services
3. L'intégration des ressources
4. La rationalisation des infrastructures.

Extranet

Un **extranet** (ou réseau interne étendu) est un réseau de télécommunications de type internet conçu pour faciliter les échanges entre une organisation sociale et ses correspondants extérieurs.