République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira - Bejaia -Faculté des Sciences Exactes

Département d'Informatique

Mémoire de fin de cycle en vue de l'obtention d'un master professionnel

Option : Administration et sécurité des réseaux

Thème

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

Présenté par :

M elle BOUCHERIT Siham

M r KHALED Wassim

Soutenu devant le jury composé de :

M r MEHAOUED Kamal

M r AMROUN Kamel

M me ELBOUHISSI Houda

Promotion 2020/2021

Remerciements

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à notre encadreur **MR** <<MEHAOUED.K>> pour sa patience, sa disponibilité et surtout ses judicieux conseils.

Nos plus sincères remerciements vont à tous les membres de jury qui nous ont fait l'honneur de juger notre travail.

Nos remerciements vont enfin à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

Dédicaces

__J__e dédie ce modeste travail à :

__M__es très chers parents à qui je doits tout, je profite de les remercier

Pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et

Le sacrifice qu'ils ont fait pour moi, que Dieu les protège et les

Entoure de sa bénédiction.

***A** Mes chères sœurs IMANE, IKRAM et HADIL.*

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

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

***A** ma binôme Siham je te souhaite beaucoup de sucées.*

Khaled Wassim

Dédicaces

***J**e dédie ce modeste travail*

***A** ma Chère Mère Cherifa*

***A** mon Chère Père Rabah*

Autant de phrases et d'expressions aussi éloquentes soit-elles et ne

Sauraient exprimer ma gratitude et ma reconnaissance. Vous avez su

M'inculquer le sens de la responsabilité. De l'optimisme et de la

Confiance en soi face aux difficultés de la vie. Vos conseils ont toujours Guidé mes pas vers la réussite. Votre patience sans fin, votre Compréhension et encouragement sont pour moi le soutien Indispensable que vous avez toujours su m'apporter. j vous dois ce que je suis aujourd'hui et ce que je serai demain et je ferai toujours de mon mieux pour rester votre fierté et ne jamais vous décevoir. Que dieu le tout puissant vous préserve, vous accorde santé, bonheur, quiétude de l'esprit et vous protège de tout mal.

***A** mes Frères et mes belles sœurs Mounir, Ferhat, Yacine, Imene, Amel et Lydia.*

Pour leur soutien moral et leurs soutien précieux tout au long de mes

Études.

***A** ma famille, mes proches et à ceux qui me donnent de l'amour et de la vivacité.*

***A** mon binôme Wassim je te souhaite beaucoup de sucées.*

Boucherti Siham

Table des matières

Chapitre II : Concepts de sécurité réseaux

Table des figures

Liste des tableaux

Liste des Abréviations

AP	Access Point
ACK	Acknowledgement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
OSI	Open System Interconnection
ARP	Adresse Résolution Protocole
ACL	Access Control List
DNS	Domain Name System
DHCP	Dynamique Host Configuration Protocol
DES	Data Encryptions Standard
FTP	File Transfert Protocole
GSM	Global Systeme Mobile
GNS3	Graphical Network Simulateur
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IOS	Iphone OS et le système d'exploitation mobile développé par Apple
ICMP	Internet Control Message Protocol
IGP	Interior Gateway Protocol
IPsec	Internet Protocol Security
LAN	Local Area Network
L2TP	Layer To Tunneling Protocol
L2F	Layer Two Forwarding .Protocole d'encapsulation
MMF	Multi Mode Fibre
MAN	Métropolitain Area Network
MAC	Media Access Control
NAT	Network Address Translation

PAN	Personale Area Network
PPP	Point To Point Protocol
PPTP	Point To Point Tunneling Protocol
RARP	Reverse Adresse Résolution Protocole
RIP	Routing Information Protocol
SMF	Single Mode Fiber
SMTP	Simple Mail Transfert Protocole
SSL	Secure Socket Layer
SSH	Secure Shell
TCP	Structured Query Language
UDP	User Datagram Protocol
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
NAS	Network Attached Storage
DNS	Domain Name System
PAT	Port Address Translation
IPX	Internetwork Packet Exchange
RPV	Réseau privé virtuel
MMF	Multi Mode Fibre

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.

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.

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.

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.

Chapitre I : Généralités sur les réseaux

I.1 Préambule

Les réseaux informatiques sont nés pour la nécessité de créer des terminaux distants entre eux. Ils ont tellement contribué à l'entreprise alors ils sont indispensables. Leur objectif est d'assurer l'inter connectivité des ordinateurs afin qu'ils communiquent entre eux et échangent des données.

Dans ce chapitre, nous allons aborder les définitions d'un réseau et ses topologies et protocoles les plus utilisés.

I.2 Que signifie réseau

Un réseau informatique est un ensemble d'éléments matériels et logiciels reliés entre eux dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme numérique.

Un réseau est constitué d'équipements appelés nœuds. En fonction de leur étendue et de leur domaine d'applications, ces réseaux sont catégorisés.

I.3 Pourquoi des réseaux

L'objectif premier des réseaux est la mise en commun de ressources, assurant notamment:

- le **partage** de l'information. En informatique, celle-ci existe sous différentes formes : Fichiers ; documents ; données....
- La **communication** entre personnes grâce au courrier électroniques, la discussion en direct, ...
- La garantie de **l'unicité de l'information** lors d'une mise à jour de bases de données.
- la mise en place d'outils de travail collaboratif.
- La communication entre processus.

I.4 Classification des réseaux (définition +schéma)

Un réseau est constitué d'équipements appelés nœuds. En fonction de leur étendue et de leurs domaines d'applications.

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

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

I.4.1 Selon leurs tailles

Nous prenons en compte généralement 4 catégories de réseaux informatiques différenciés par la distance maximale séparant les points les plus éloignes du réseau : PAN, MAN, LAN et WAN.

I.4.1.1 Réseau PAN (Personale Area Network) :

Ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tel que : le GSM, portable ….d'un même utilisateur. [2]

I.4.1.2 Réseaux LAN (Local Area Network) :

Un LAN est un réseau situé généralement dans la même entité géographique (entreprise, campus,...). Des LAN peuvent être interconnectés pour former des réseaux plus grands (WAN, MAN,...). On dit alors que le LAN est un sous-réseau du réseau auquel il est connecté. [2]

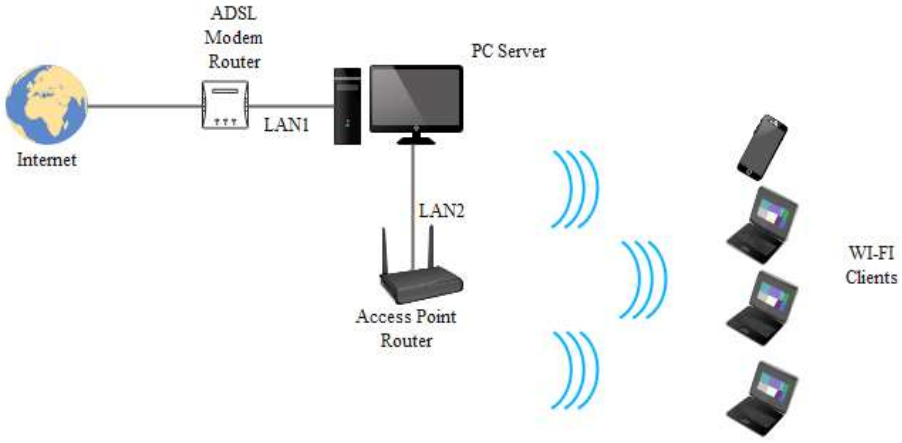

Figure I.1. Réseau LAN

I.4.1.3 Réseau MAN (Métropolitain Area Network) :

Ce type de réseaux est récent et garde les avantages des LAN sur de plus longues distances de l'ordre de la ville. [2]

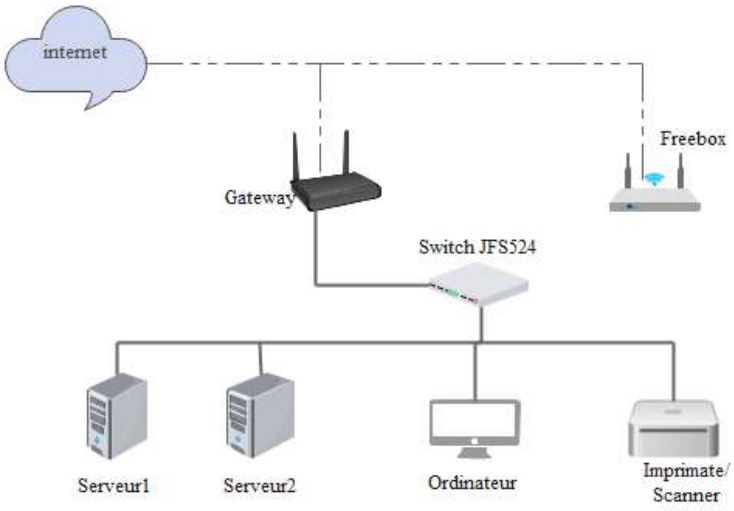

Figure I.2. Réseau MAN

I.4.1.4 Réseau WAN (Wide Area Network):

Réseau grande distance. Un WAN est un réseau qui se mesure sur une grande échelle géographique. Certaines sociétés, généralement internationales (IBM, UNISYS, AT&T, AIR France, ...) disposent souvent de tels réseaux à l'échelle planétaire. [2]

- Internet est un réseau de type WAN

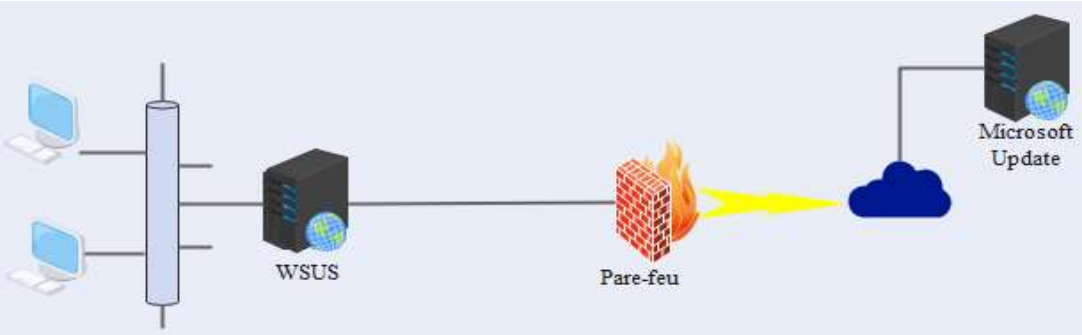

Figure I.3. Réseau WAN

I.4.2 Selon la Topologie

I.4.2.1 Définition de la topologie

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce aux 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 :

I.4.2.2 Topologie en bus :

Chaque machine est reliée à un câble appelé bus.

Figure I.4. Topologie en bus

Repose sur un câblage sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnections, périphériques…). Il s'agit d'un support multipoints .Le câble est l'unique élément matériel constituant le réseau et seul les nœuds génèrent le signal. [4]

I. 4.2.2.1 Principe de fonctionnement

Sur un câble de type bus, on utilise souvent un système CSMA/CD (Carrière Sens Multiple Access / Collision Détection) Accès multiple avec détection de porteuse et détection des collisions.

4.2.3 Topologie en anneau (ring) :

Chaque machine est reliée à une autre de façon à former un anneau

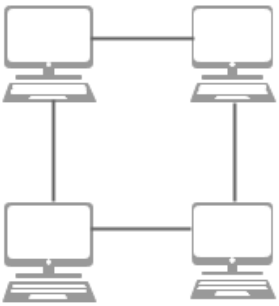

Figure I.5. Topologie en anneau

Dans ce type de topologie les ordinateurs sont placés en cercle sur un câble sans terminaison (en fait ils sont reliés par des câbles aller/retour à un Concentrateur passif qui relie chaque ordinateur au suivant). Chaque Ordinateur joue le rôle de répéteur pour amplifier le signal et le faire repartir. La Méthode d'Accès à ce type de câblage est celle du passage de « jeton ».

Pour pouvoir transmettre un ordinateur doit être en possession du jeton libre ce qui évite toute collision sur le réseau. [4]

I.4.2.4 Topologie en étoile (star)

Toutes les stations sont reliées à un seul composant central (concentrateur). [4]

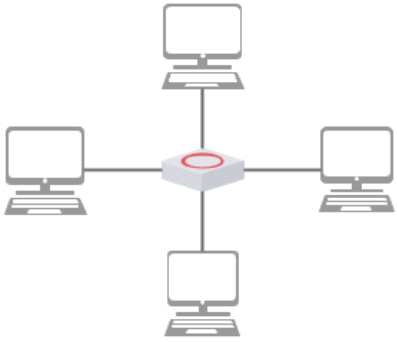

Figure I.6. Topologie en étoile

I.4.2.5 Structure hybride

La structure hybride de réseau emploie un mélange comme l'anneau, le bus et également l'étoile. [4]

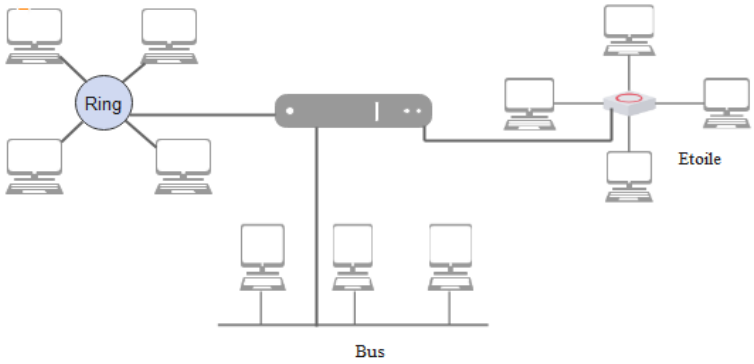

Figure I.7. Structures hybride

I.5 Sens de transmission

Pour communiquer des informations entre deux points il existe différentes possibilités, pour le sens de transmission : [3]

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

I.6 Les supports de transmission

Un réseau suppose plusieurs équipements informatiques (ordinateurs fixes ou portables, divers équipements électroniques, téléphones, assistants numériques personnels…) situés à distance les uns des autres. La première chose à mettre en œuvre pour constituer le réseau est la transmission des informations d'un équipement à l'autre : on utilisant des supports de transmission. C'est le support (généralement filaire, c'est-à-dire sous forme de câble, de plus en plus non filaire) qui relie les ordinateurs entre eux. [5]

Les principaux supports physiques utilisés dans les réseaux locaux sont les suivants:

I.6.1 support filaire :

I.6.1.1 Les câbles à paire torsadée

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. [5] Comme le montre dans la figure suivante.

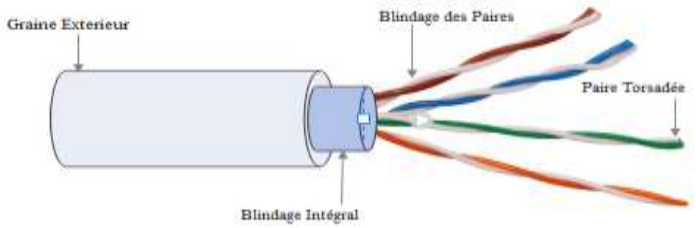

Figure I.8. Câble à paires torsadées

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

I.6.2 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. [5]

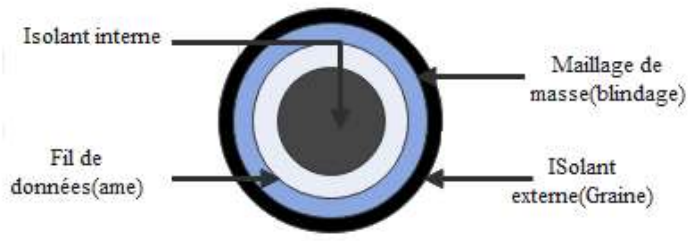

Figure I.9. Câble coaxial

On distingue deux types de câbles coaxiaux :

- les câbles coaxiaux fins
- les câbles coaxiaux épais

I.6.2.1 Le câble coaxial fin (thinNet)

(Ou 10 base 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.

I.6.2.2 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.

I.6.3 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, l'information circule sous forme lumineuse. [5]

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

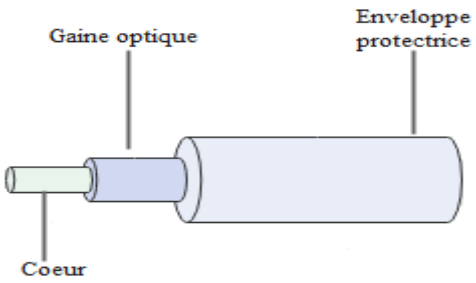

Figure I.10. La fibre optique

On distingue deux sortes des fibres optiques :

- les fibres multi modes
- les fibres monomodes

I.6.3.1 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.

I.6.3.2 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, comme présentée par la figure suivante :

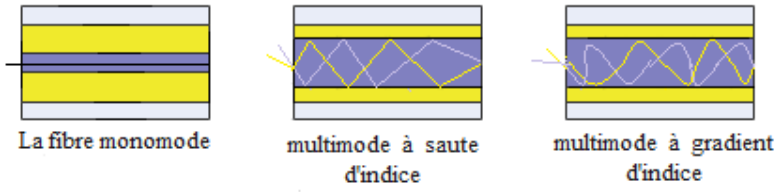

Figure I.11. Les types de fibre optique

I.6.3.2.1 Avantages

- très grande fiabilité
- débit élevé
- utilisation sur de grandes distances (jusqu'à 50 km)

I.6.3.2.2 Inconvénient

-coût élevé

I.7 support Sans fil :

I.7.1 Les liaisons infrarouges

L 'IrDA, appelé infrarouge, est encore aujourd'hui une technologie de transmission sans fil très répandue (PC portable, PDA, téléphone portable, etc.). Le protocole IrDA est conçu pour le transfert des données, en utilisant la lumière infrarouge. Avec une connectivité rapide, sans installation. Faible coût. Sécurisation de transmission. [5]

I.7.1.1 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. [5]

Voici quelques exemples des systèmes utilisant la liaison hertzienne

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

I.7.1.1.1 Bluetooth

La technologie Bluetooth est une technologie de réseaux sans fils d'une faible portée, de l'ordre de quelques dizaines mètres à un peu moins d'une centaine de mètres, permettant de relier des périphériques (imprimantes, téléphones portables, appareils domestiques, oreillettes sans fils, souris, clavier, etc.) et des ordinateurs et assistants personnels (PDA) entre-deux sans liaison filaire. [5]

I.7.1.1.2 Wifi

Le Wifi, pour Wireless Fidélité, est une technologie standard d'accès sans fil à des réseaux locaux. Le principe est d'établir des liaisons radio rapides entre des équipements et des bornes reliées aux réseaux Haut Débit. Grâce au Wifi, il est possible de créer des réseaux locaux sans fils à haut débit. [5]

I.7.1.1.3 Wi max

Le Wi max est un standard de transmission sans fil à haut débit. Fonctionnant à 70 Mbit/s, il est prévu pour connecter les points d'accès Wifi à un réseau de fibres optiques, ou pour relayer une connexion partagée à haut débit vers de multiples utilisateurs.

Cette technologie apparue en France en décembre 2003 menace sur le papier le Wifi grâce à des débits théoriques sept fois supérieurs et une couverture qui s'étend jusqu'à 50 kilomètres là où les bornes Wifi se limitent à quelques centaines de mètres. [5]

I.8 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.

I.8.1 Les Ponts

Un pont (bridge) est un dispositif permettant de relier des réseaux de même nature.

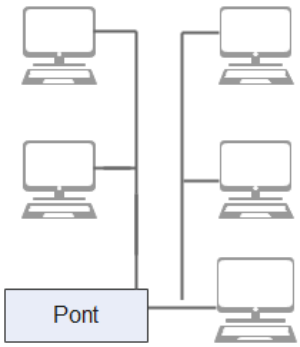

Figure I.12. Deux réseaux relient avec un pont.

I.8.2 Les passerelles

Une passerelle (Gateway) est un dispositif permettant d'interconnecter des architectures de réseaux différentes .Elle assure la traduction d'un protocole d'un haut

niveau vers un autre, comme représentée par la figure suivante :

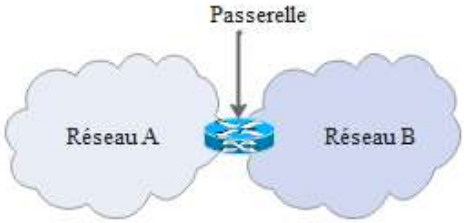

Figure I.13. Deux réseaux reliés avec passerelle

I.8.3 Les routeurs

Un routeur (router) est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale, comme le montre dans la figure en dessous .

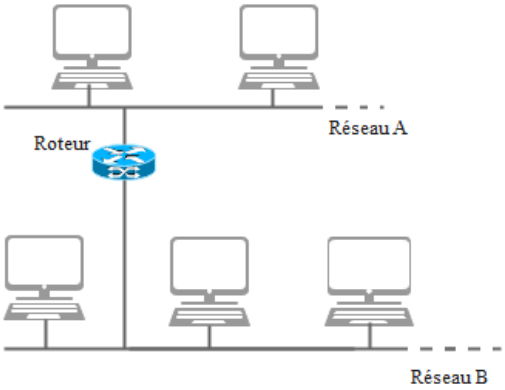

Figure I.14. Routeur connecter a deux réseaux locaux

Les routeurs fonctionnent grâce à des tables de routage et des protocoles de routage.

I.8.4 Les hubs (concentrateurs)

Un Hub (ou concentrateur) sert à regrouper plusieurs liaisons d'un même type en une seul, comme par exemple les câbles Ethernet d'ordinateur (on lie alors les PC au hub par câble droit) ou les câbles USB de périphériques externes.

Actuellement, la fonction de concentrateur est souvent incluse dans celle de routeur : il est courant de voir des hubs/ routeur sur des réseaux domestiques ne nécessitant pas un nombre énorme de ports.

I.8.5 Switch (Commutateur)

Le commutateur (en anglais Switch) est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI. Le commutateur analyse les trames

arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de commutation ou de réseaux commutés). Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

I.9 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, lesdeux systèmes doivent communiquer "compatibles". En matériel réseau, nous n'utilisons que les couches inferieures, jusqu'au niveau 3. Ces niveaux sont égalementappelés couches. [17] [18]

L'OSI est un modèle de base normalise par l'international standard organisation (iso), représentée par la figure en dessous.

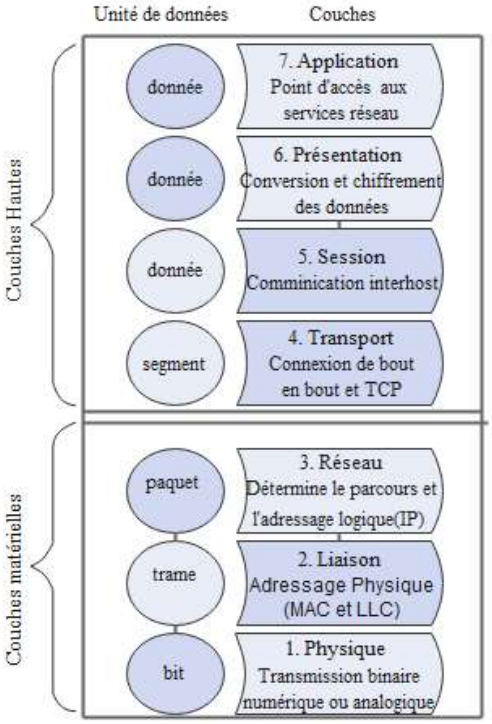

Figure I .15. Le model OSI

Niveau 7 (application): gère le format des données entre logiciels.

Niveau 6 (présentation): assure la mise en forme des données en forme, éventuellement de l'encryptage et de la compression, par exemple mise en forme des textes, imageset vidéo.

Niveau 5 (session): gère l'établissement, la gestion et coordination des communications.

Niveau 4 (transport): s'occupe de la gestion des erreurs, protocoles UDP et TCP.

Niveau 3 (réseau): sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles (IPadresse et le masque de sous-réseau) et ICMP. Utilise par les routeurs et lesSwitch mangeables.

Niveau 2 (liaison de données) : utilise les adresses mac. Le message Ethernet àce stade est la trame, il est constitué 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 uncâble coaxial, paires sur RJ45, onde radio, fibre optique, ...

I.9.1 L'avenir du modèle OSI

Au niveau de son utilisation et implémentation, et ce malgré une mise à jour du modèle en 1994, 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.

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 » généraleentre les 2 modèles. On a communément tendance à considérer TCP/IP comme l'implémentation réelle d'OSI. [17] [18]

I.10 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 aupaquet 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, à la réception, le message est dans son état original. [9]

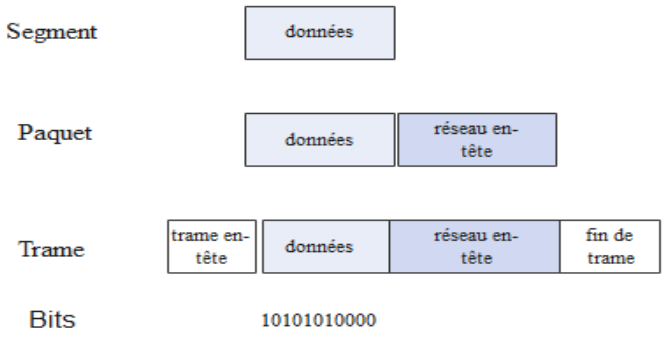

Figure I.16. Principe d'encapsulation

I.11 Définition d'un protocole

C'est un ensemble de règles qui régissent les échanges de données ou le comportement collectif de processus ou d'ordinateurs en réseaux ou d'objets connectés. Un protocole a pour but de réaliser une ou plusieurs tâches concourant à un fonctionnement harmonieux d'une entité générale. [9]

I.11.1 Protocole TCP (Transmission contrôle Protocol)

Est un protocole fiable, orienté connexion qui permet l'acheminement sans erreur de paquets issues d'une station a une autre.

I.11.2 Protocole UDP

Le trafic UDP est prioritaire sur TCP. Le but est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

I.11.3 Le modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais il contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. [4] [5] Comme le montre dans la figure ci après.

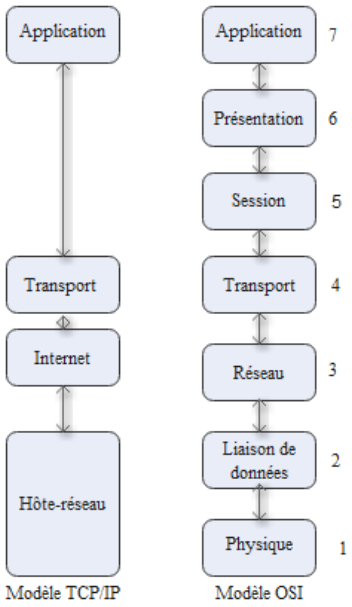

Figure I.17. Architecture TCP/IP

I.11.4 Protocol ipv4

IPv4 désigne la version 4 du protocole Internet (IP). Il s'agit de la version actuellement la plus utilisée dans le monde pour attacher une adresse IP à un ordinateur. Cette dernière prend la forme d'une succession de chiffres décimaux (4 avec l'IPv4), comme 182.23.178.44. Avec la multiplication du nombre d'ordinateurs

Reliés au réseau Internet, l'**IPv4** est officiellement arrivée à court de possibilités pour offrir des combinaisons d'adresse IP. [9]

I.11.4.1 Protocol IP

IP est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisées sans connexion. Le terme « optimisé » souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP et de leur ordre de réception.

Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

I.11.4.2 A dressage

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. demachine) et appartient a une certaine classe (a, b, c, d ou e) selon la valeur de son premier octet, comme détaille dans la (figure 18).

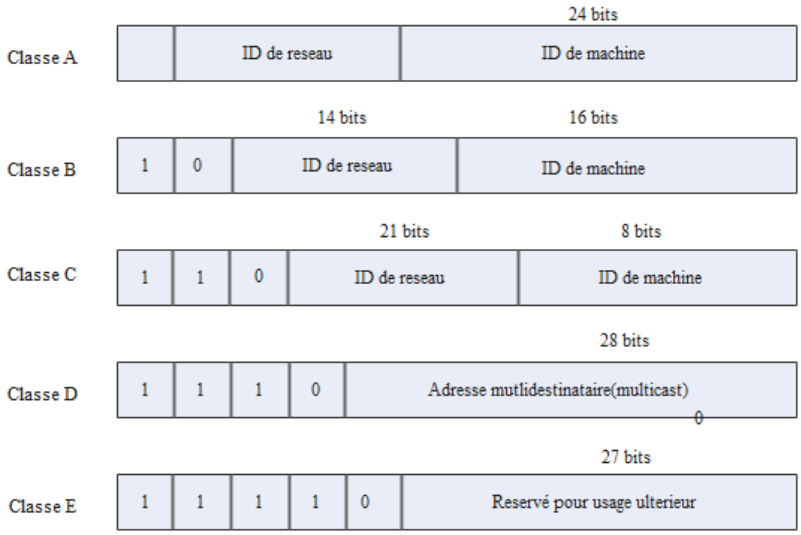

Figure I.18. Les cinq classes d'adresses IP

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

Classe	Adresse
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 à 247.255.255.255

TABLE I.1. l'espace d'adresse

I.11.5 ARP et RARP

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

I.11.5.1 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 fixé lors de 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.

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. [9]

I.11.5.2 RARP (reverse ARP)

Il est dans le réseau internet. Permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique. [9]

I.12 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 à fournir aux clients DNS qui en font la demande une association adresse IP, un nom symbolique et vice-versa. [9]

I.13 DHCP

Après obtention des paramètres fournis par un serveur DHCP, le client est capable de communiquer avec n'importe quel autre utilisateur d'Internet.

• Le service DHCP garantit l'unicité d'une adresse IP dans le réseau. C'est une aide précieuse pour l'administrateur du réseau puisqu'il permet de supprimer la configuration manuelle des machines du réseau (celle-ci reste toujours possible et doit être compatible avec l'allocation dynamique). En outre, il évite les erreurs liées à cette configuration manuelle.

• Il sera très utile pour le déploiement d'un grand parc de machines qui possèdent les mêmes caractéristiques et dont la seule différence est la configuration réseau.

Quand un client en demande une @ pour la première fois, le serveur lui en fournit une qu'il n'a pas encore utilisée.

• S'il a déjà distribué toutes ses adresses IP, il réutilise celle d'un client qui n'est plus connecté au réseau.

• Quand un client a déjà obtenu dynamiquement une adresse IP lors d'une connexion antérieure, le serveur lui fournit a priori la même adresse, si c'est possible.

• Il peut y avoir plusieurs serveurs DHCP actifs simultanément dans le réseau (pour assurer une redondance du service et optimiser les performances d'accès).

• À l'inverse, il n'est pas indispensable d'en avoir un pour chaque sous réseau. DHCP peut fonctionner à travers des routeurs, en utilisant des relais. [9]

I.14 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, soitle 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. [9]

I.14.1 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. [9]

I.14.1.1 Routage interne

I.14.1.1.1 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. [9]

I.14.1.1.2 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 unalgorithme centralise.

En fait, RIP de type et OSPF, sont des protocoles IGP (interior gateway protocol) permettant d'établir les tables des routeurs internes des systèmesautonomes. [9] Comme présentée par la figure en dessous.

Figure I.19 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.

I.14.1.2 Routage externe

I.14.1.2.1 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 à choisir entre différentes routes et a implanter des politiquesde routage sans se baser sur une autorise centrale de routage (dans le d'absence de passerelle centrales). [9]

I.15 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 ICMPne peut donner naissance à un autre message ICMP. [9]

I.16 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 surl'utilisation des réseaux. Par conséquent, les risques augmentent.

Chapitre II : Concepts de sécurité réseaux

II.1 Préambule

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l'appelle également sécurité informatique ou sécurité des systèmes d'information.

Vous pouvez la rencontrer dans de nombreux contextes, de l'informatique d'entreprise aux terminaux mobiles. Elle peut être divisée en plusieurs catégories.

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 sécuritéest 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 lesnotions de sécurité et en particulier le VPN.

II.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 essentiellessuivantes: [16]

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

II.3 Objectifs

Le système d'information est généralement défini par l'ensemble des données ainsi que les ressources matérielles et logicielles de l'entreprise permettant de les stocker oude les faire circuler Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. [16]

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 : garantir que les données sont bien celles que l'on croit être.
- La disponibilité : maintenir le bon fonctionnement du système d'information.
- La confidentialité : rendre l'information intelligible à d'autres personnesqui sont les acteurs d'une transaction.
- Le non répudiation : garantir qu'une transaction ne peut être niée.
- L'authentification : assurer que seules les personnes autorisées aient accèsaux ressources.

II.4 Les techniques d'attaques

II.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 altérée par celui qui en prélève une copie. Ces attaques sont donc indétectablespar le système et peuvent seulement êtres parées par des mesures préventives. [18]

II.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. [16]

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.

II.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. [18]

II.4.4 Attaque logicielles

Peut-être décrite comme un logiciel indésirable installé dans votre système sans votre consentement. Il peut s'attacher à un code légitime et se propager, se cacher dans des applications utiles ou se reproduire sur Internet.

Voici quelques-uns des types de logiciels malveillants les plus courants : [18]

II.4.4.1 Les virus

Un virus est un bout de programme glissé volontairement dans une applicationdans 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'importequel autre support informatique : disquette, CD ROM … .
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). [6]

II.4.4.2 Le Cheval de Troie

Un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte déguisé sous une fausse apparence) mais qui, une fois installé exerçait une action nocive totalement différente de sa fonction officielle.

Actuellement le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spam, l'ouverture d'un accès pour un pirate. [18]

II.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. [18]

II.4.4 Attaque logicielles

Peut-être décrite comme un logiciel indésirable installé dans votre système sans votre consentement. Il peut s'attacher à un code légitime et se propager, se cacher dans des applications utiles ou se reproduire sur Internet.

Voici quelques-uns des types de logiciels malveillants les plus courants : [18]

II.4.4.1 Les virus

Un virus est un bout de programme glissé volontairement dans une applicationdans 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'importequel autre support informatique : disquette, CD ROM …

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 sansdanger).

II.4.4.2 Le Cheval de Troie

Un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte déguisé sous une fausse apparence) mais qui, une fois installé exerçait une action nocive totalement différente de sa fonction officielle.

Actuellement le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spam, l'ouverture d'un accès pour un pirate.

II. 4.4.3 Les vers

Un ver est un logiciel malveillant, qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique. Contrairement à un virus informatique, un ver n'a pas besoin d'un programme hôte pour se reproduire, il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

L'objectif du ver est d'espionner l'ordinateur où il se trouve, offrir une porte dérobée à des pirates informatiques, détruire les données de l'ordinateur infecté et envoyer de multiples requêtes vers un serveur Internet dans le but de le saturer (déni de service). Il a pour effet le ralentissement de la machine infectée.

II.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 desavoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception.

II.5 Autres attaques

II.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 des 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.

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. [18]

II.5.2 Intrusion

L'intrusion dans un système informatique a 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 : [18]

- 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.

II.5.3 Attaque de l'homme de milieu

L'attaque de l'homme de milieu ou man-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. [18]

II.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. [18]

II.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. [18]

II.6 Les méthodes de protections

II.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. [18]

II.6.2 La cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle nous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire. [18]

La cryptographie est divisée en deux types :

II.6.2.1 Chiffrement symétrique

Dans le chiffrement symétrique, une même clé est partagée entre l'émetteur et le récepteur. Cette clé dite symétrique est utilisée par l'émetteur pour chiffrerle message te par le récepteur pour le déchiffrer en utilisant un algorithme de chiffrement symétrique. Comme le montre la figure en dessous.

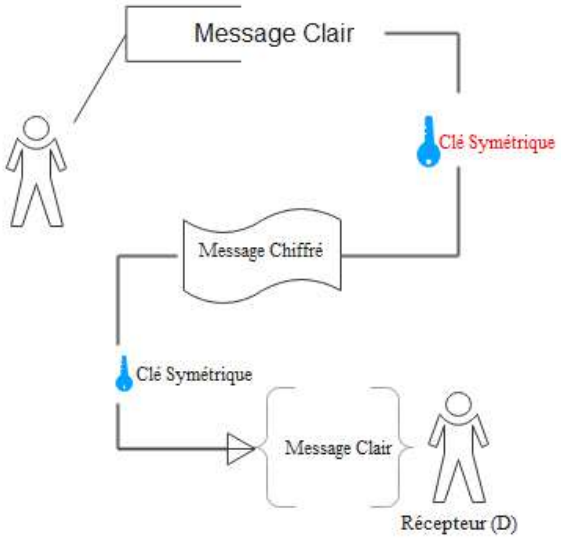

Figure II.20. Chiffrement symétrique

II.6.2.2 Chiffrement asymétrique

La Cryptographie asymétrique ou à clé publique, est un procédé asymétrique utilisant une paire de clés pour le cryptage :

Une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Nous pouvons ainsi publier notre clé publique tout en conservant notre clé privée secrète. Tout utilisateur possédant une copie de notre clé publique peut ensuite crypter des informations que nous seuls pouvons lire.

D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter.

Seule la personne disposant de la clé privée correspondante peut les décrypter Comme le montre dans la figure en dessous.

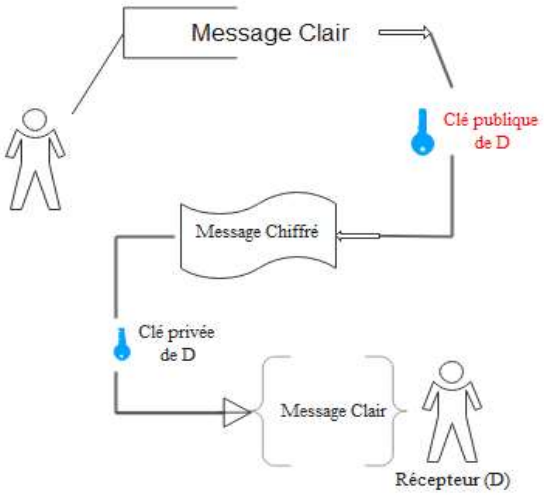

Figure II.21. Chiffrement asymétrique

II.6.3 Pare –feu

Un pare-feu est un système ou un groupe de systèmes qui gère les contrôles d'accès entre deux réseaux. Ces dispositifs filtrent les trames des différentes couches du modèle TCP/IP afin de contrôler leur flux et de les bloquer en cas d'attaques, celles-ci pouvant prendre plusieurs formes.

Le filtrage réalisé par le pare-feu constitue la première défense de la protection du système d'information. Il peut être composé de périphériques comportant des filtres intégrés dont la fonction principale est de limiter et de contrôler le flux de trafic entre les différentes parties des réseaux…[15] Comme le montre dans la figure en dessous.

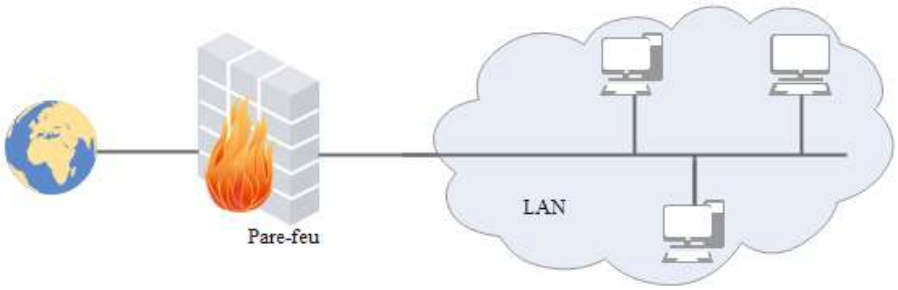

Figure II.22. Pare-feu

II.6.3.1 Un firewall comment ça marche

Le fonctionnement du pare-feu dépend de la politique de sécurité mise en œuvrepar le donneur d'ordre.

Il existe deux grandes politiques de sécurité :

- la plus sûre consiste à n'autoriser que les communications explicitement admises au nom du principe du moindre privilège.
- n'interdire que les échanges explicitement prohibés.

La première option est la plus efficace et la plus contraignante aussi. Le principe du moindre privilège fait qu'une action ne saurait être engagée qu'à la condition que son utilité fonctionnelle soit réelle. Le privilège désigne la possibilité d'exécuter une action telle que la capacité de créer, de lire ou de détruire un fichier. Dans le cadre du pare-feu il s'agit notamment d'appliquer les trois principales règles prédéfinies : accepter la connexion, la bloquer, refuser la demande de connexion sans prévenir l'émetteur. [15]

II.6.3.2 À quoi sert un firewall

Le Pare-feu sert naturellement à protéger un ou plusieurs ordinateurs contre des logiciels malveillants. Son utilité et son efficacité s'accroissent à mesure qu'il intègre des

fonctionnalités nouvelles.

II.7.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.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.). Comme le montre dans la figure en dessous. [14]

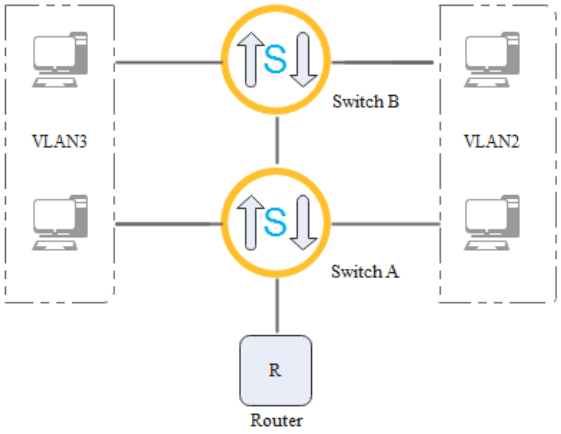

Figure II.23. Exemple de VLAN.

II.8. 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 cotés, 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 lechangement d'une adresse IP par une autre.

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. [9]

II.9. Les ACL

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur. Comme le montre dans la figure en dessous.

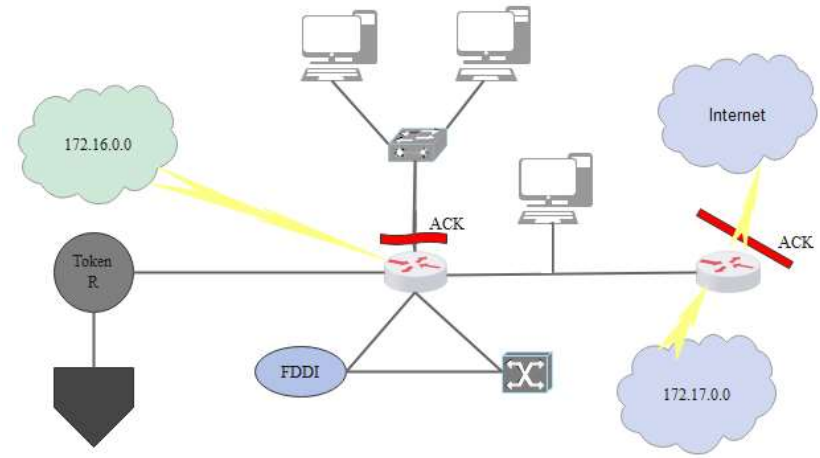

Figure II.24. ACL

Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation ou le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internet work Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau. [1]

II.10 Les réseaux privés virtuel (VPN)

II.10.1 Définition

II.10.1.1 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.

II.10.1.2 Réseau privé virtuel

VPN (Virtual Private Network) ou RPV (Réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques.

Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique. [7]

II.10.2 Le principe de fonctionnement d'un VPN

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN et parmi eux nous retrouvons : [7]

- Internet Protocol Security (IPSec).
- Layer 2 Tunneling Protocol (L2TP).
- Point-to-Point Tunneling Protocol (PPTP).
- Hybride VPN.

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 après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets de l'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé, comme Internet. [5]

II. 10.3 Les méthodes de connexion

Il existe plusieurs méthodes de connexion VPN, Parmi ces différentes Méthodes on peut citer les : [7]

-Le VPN d'accès

-Intranet VPN

-Extranet VPN

II.10.3.1 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, comme le montre dans la figure en dessous. [7]

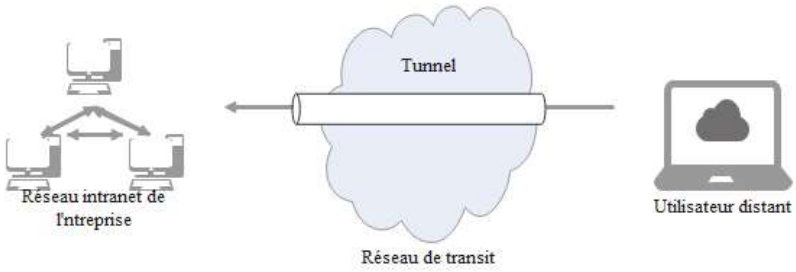

Figure II .25. VPN connectant un utilisateur distant à un intranet privé

II.10.3.2 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, Comme l montre dans la figure en dessous. [7]

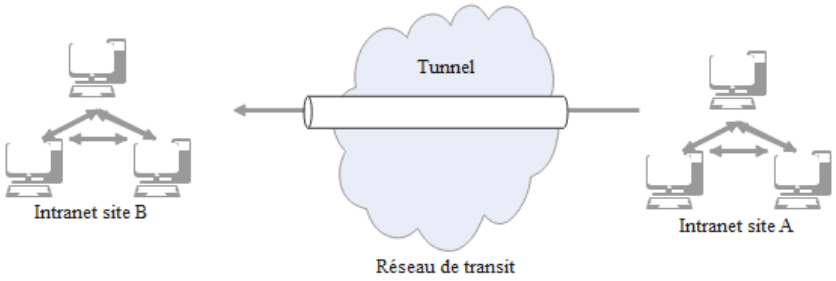

Figure II .26. VPN connectant 2 sites distants par l'Intranet

II.10.3.3 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, comme l représente dans la figure en dessous. [7]

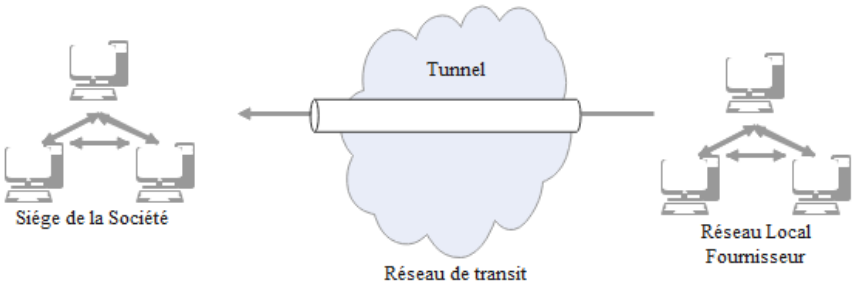

Figure II.27. VPN connectant des sites clients au site de l'entreprise

II.10.4. Les différentes architectures des VPN

II.10.4.1. 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] Comme le montre dans la figure en dessous.

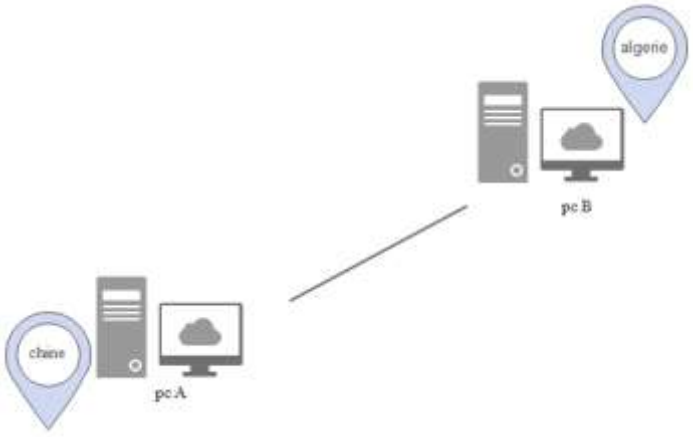

Figure II.28. VPN de poste à poste

II.10.4.2 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 ordinateurs 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] Comme le représente dans la figure en dessous.

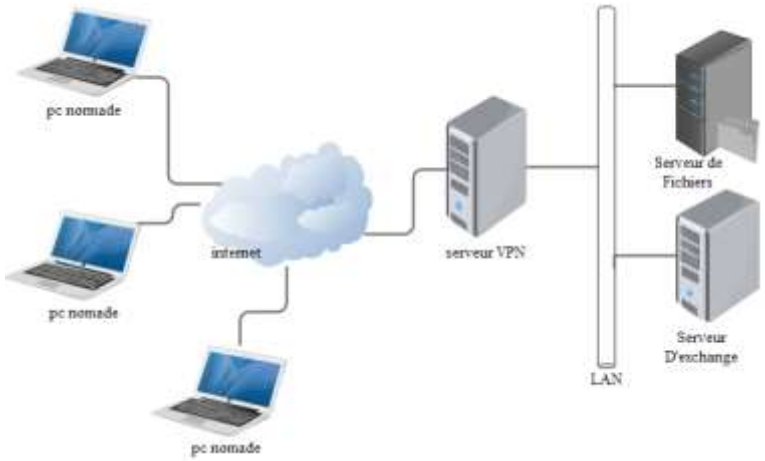

Figure II.29. VPN de poste Nomade à site Entreprise

II.10.4.3 De site à site

Elle correspond à un type d'infrastructure de réseau étendu, 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] Comme le montre dans la figure en dessous.

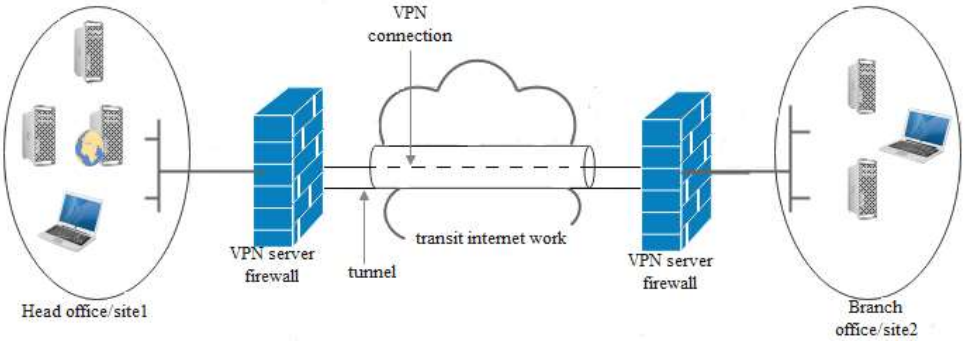

Figure II.30. VPN de site a site

II.10.5 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] comme le montre dans les deux figures en dessous.

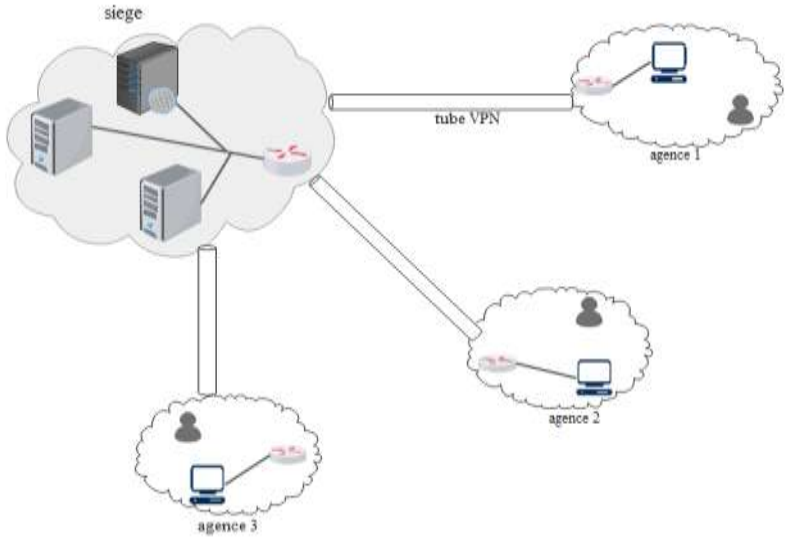

Figure II.31. VPN en étoile

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.

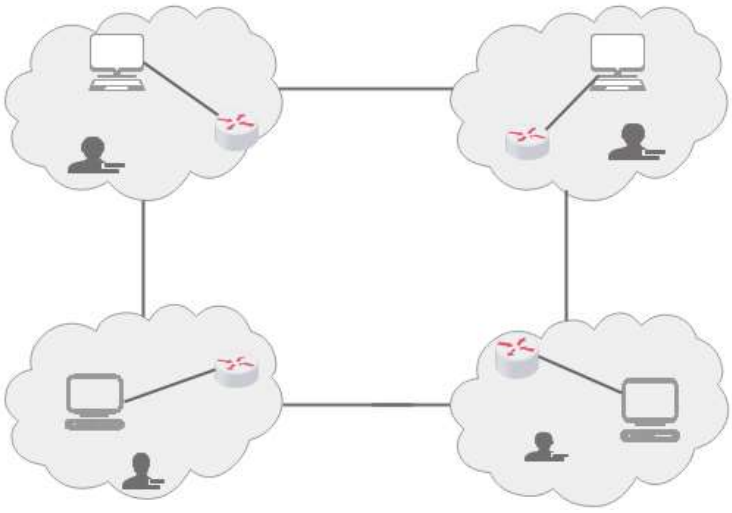

Figure 32. VPN maillé

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.

II.10.6 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 : [11]

- 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.

II.10.7 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.

II.10.8 Cryptage et Authentification

II.10.8.1 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. [12]

On distingue deux types de cryptage :

II.10.8.1.1 Cryptage symétrique

Le cryptage à clé privée ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages, Comme le représente dans la figure en dessous.

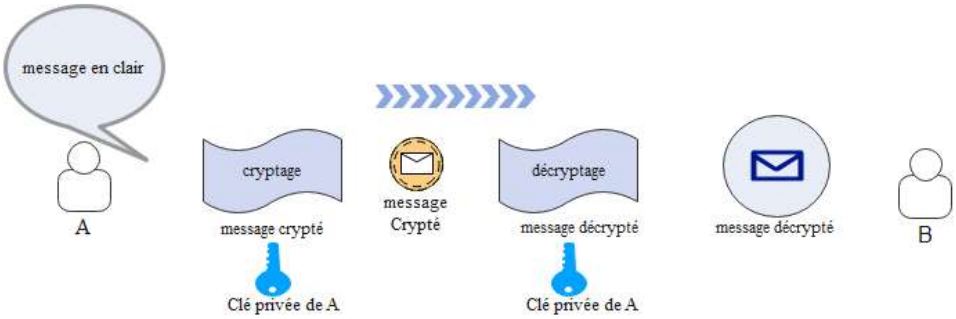

Figure II.33. Cryptage symétrique

II.10.8.1.2 Cryptage asymétrique

Pour pallier la complexité induite par la gestion de la distribution des clés par cryptographie symétrique. Un autre type de cryptage qualifié d'asymétrique a été conçu et utilisé largement dans le monde de l'internet.

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

- Une première clé, visible, appelé 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, Comme le montre dans la figure en dessous.

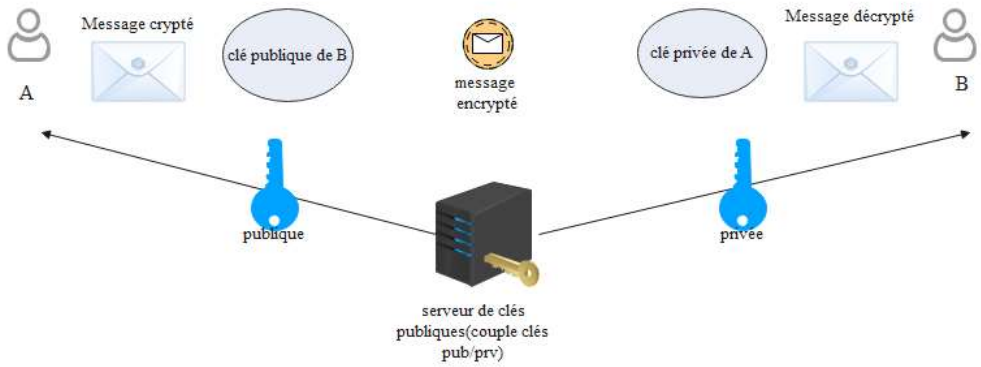

Figure II.34. Cryptage asymétrique

II.10.8.2 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). [13]

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. Il existe plusieurs

II.10.9 Les avantages et les inconvénients de VPN

Comme nous venons de le voire les VPN disposent de nombreux avantages, Il existe plusieurs raisons pour lesquelles il est judicieux utiliser un VPN. En voici quelques-unes des plus importantes : [13]

- Gratuité ou coût assez faible.
- Confidentialité.
- Sécurité assez efficace.
- Simplicité de la mise en place.
- Un VPN Vous Permettra d'Accéder à du Contenu Géo-Restreint.
- Un VPN Peut Accélérer vos Connexions.

Cependant ils peuvent aussi représenter quelques inconvénients, Il est important de comprendre que les « inconvénients » ne doivent pas être considérés comme un désavantage, mais plutôt comme un défi à surmonter.

- Quelques failles de sécurité.
- Utilisation de ressources matérielles importantes.
- Les VPN Ne Sont Pas la Panace.
- Un VPN Peut Coûter Cher.
- Utiliser un VPN Peut s'Avérer Compliqué.

II.11 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 III : Les protocoles utilisés dans le VPN

III.1 Préambule

Le VPN offre la possibilité de choisir parmi plusieurs protocoles celui qui correspond le mieux à nos besoins de performance et de sécurité. D'une manière générale, un protocole VPN se réfère à la façon dont il déplace les données d'un point à un autre. Cela affecte la vitesse de la connexion et le niveau de sécurité des utilisateurs.

Les différences entre les protocoles VPN sont liées à la façon dont la connexionest adaptée à un usage spécifique. Dans ce chapitre nous allons présenter 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 ce chapitre nous allons présenter les protocoles utilisés dans le VPN etquelques notions du SSL.

III.2 Protocoles utilisés dans le VPN

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

III.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 distanceet un serveur d'accès réseau.
Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocolesPPTP ou L2TP. [14]

III.2.1.2 Le protocole PPTP

De l'anglais Point-to-point tunneling protocol ou protocole d'encapsulation. C'est le type de protocole VPN le plus souvent utilisé.

Ce protocole PPTP crée effectivement un tunnel privé pour envoyer des données vers et depuis un ordinateur ou un appareil mobile.

Les périphériques sont authentifiés à l'aide d'un mot de passe, ce qui implique qu'il n'y a pas de matériel supplémentaire nécessaire. A lui seul, PPTP ne fournit aucun cryptage de données ou aucune mesure de sécurité supplémentaire.

Les connexions PPTP sont également faciles à bloquer pour lesfournisseurs de services Internet. Cependant, il existe des avantages à utiliser unVPN PPTP – c'est le protocole le plus facile à configurer et à utiliser, et il peut aussi vous offrir une performance stable et une vitesse fiable. [14]

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 données sur Internet. Par la suite, une deuxième connexion est établie, elle permet d'encapsuler PPP dans des datagrammes IP. C'est cette deuxième connexion quiforme le tunnel PPTP.

III.2.1.2.1 Avantages

Ce protocole VPN est facile à installer et à configurer sur votre ordinateur portable, ordinateur ou appareil mobile. La connexion PPTP assure généralement une bonne vitesse et est acceptée par la majorité des appareilsmobiles.

III.2.1.2.2 inconvénients

Ce protocole VPN peut être facilement bloqué par les fournisseurs d'accès Internet.

III.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 despaquets 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. [14]

L'authentification L2F est différente de celle de PPTP qui nécessite justel'autorisation du RAS du LAN sur lequel on se connecte.

En effet, l'authentification L2F nécessite l'approbation préalable du serveur RAS.

III.2.1.4 L2TP

De l'anglais Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec). Ce protocole fonctionne d'une manière similaire à PPTP, mais il offre la confidentialité et l'intégrité des données supplémentaires grâce à un processus de multi-authentification. Comme PPTP, L2TP sur IPSec peut être installé facilement sur tout appareil Apple, Windows ou Androïde.

En raison des caractéristiques de sécurité supplémentaires qu'il contient, l'utilisation d'un protocole VPN L2TP sur IPSec peut être plus lente lors du transfert d'un volumeélevé d'information. [14]

L2TP repose sur deux concepts :

- Les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrateur).
- 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 UDPoffre des services moindres que TCP, il s'agit de les compenser ailleurs.

III.2.1.4.1 Avantages

Le protocole L2TP/IP Sec est facile à installer et à configurer sur votre ordinateur portable, votre ordinateur ou votre appareil mobile. C'est aussi l'undes meilleurs protocoles VPN pour contourner les restrictions de réseaux et lesfournisseurs de services Internet.

III.2.1.4.2 inconvénients

La connexion VPN L2TP peut être plus lente. Le protocole L2TP/IP Sec peut également être facilement bloqué par certains fournisseurs d'accès Internet.

III.2.1.5 OPENVPN

Comme son nom l'indique, OpenVPN ou PPTP est un protocole VPN open source qui utilise Secure Socket Layer (SSL) pour créer une authentification pour une connexion Internet cryptée.

Etablir une connexion OpenVPN peut êtredifficile pour les utilisateurs qui n'ont pas de compétences techniques, Le VPN le rend simple, avec notre logiciel. Dans l'ensemble, le protocole OpenVPN. [14]

III.2.1.6 HybridVPN

Le VPN fait partie d'une nouvelle génération de fournisseurs de services qui offre un HybridVPN combinant à la fois une connexion VPN de niveau SSL et un proxy Smart DNS. Un proxy Smart DNS est un service optionnel qui simplifiele processus pour un utilisateur, afin de lui permettre d'accéder à des contenus géographiquement limités. De fait, les utilisateurs bénéficient de la sécurité, de la fiabilité et de l'anonymat d'un VPN, avec la facilité d'utilisation et la liberté d'un Smart DNS.

Vous pourrez également profiter d'une vitesse et d'une fiabilité exceptionnelles pour regarder des médias ou des vidéos ou des sites graphiques longs à télécharger. [14]

III.2.2 Le protocole IP Sec

III.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 interneset 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. [19]

III.2.2.2 Les services 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. [19]

Services de sécurités offerts par s offerts par IP sec :

- Authentification des extrémités.
- Confidentialité des données échangées.
- Authenticité des données.
- Intégrité des données échangées.
- Protection contre les écoutes et analyses de trafic
- Protection contre le rejeu.

Ces différentes caractéristiques permettent à l'hôte A de crypter ses données etde 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 cesdonnées.

III.2.2.3 IPsec permet :

- La mise en place de VPN.
- Sécuriser les accès distants (Utilisation nomade).
- Protection d'un serveur sensible.

III.2.2.4 Composants d'IP sec

• Protocoles de sécurité :

– Authentication Header (AH).
– Encapsulation Security Encapsulation Security Payload (ESP).

• Protocole d'échange de clefs :

– Internet Key Exchange (IKE).

• Bases de données internes :

– Security Policy Database (SPD).
– Security Association Database (SAD) [19].

III.2.3 Le protocole SSH (Secure Shell)

SSH est `à la fois la définition d'un protocole et un ensemble de programmes Utilisant ce protocole, destinés à permettre aux utilisateurs d'ouvrir, depuis une machine cliente, des sessions interactives sécurisées `a distance sur des serveurs et de transférer des fichiers entre eux.

- échange de clés de chiffrement.
- toutes les trames sont chiffrées.
- impossible de lire les trames sur le réseau via un sniffer.
- remplaçant de login, Telnet et rsh.

De plus il permet l'identification de la machine distante L'algorithme Utilisé pour la négociation des clés RSA (dont le brevet a expiré aux USA ce qui permet une Utilisation publique légale).

Les principaux algorithmes utilisé dans SSH sont triples 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. [19]

III.2.4 Le protocole SSL

SSL (Secure socket layer) est un protocole de couche 4 (niveau transport) utilisépar 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 au coté client, il ne nécessite qu'un navigateur InternetStandard. 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 http, ce qui n'est pas le seul besoin de connexion des entreprises. [19]

III.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 estimportante, 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. [19]

B Authentification du client

Selon les mêmes modalités que pour le serveur, il s'agit de s'assurer que leclient 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 àdes mécanismes également mis en place dans ce sens. [19

III.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]

III.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. [13]

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 tous les navigateurs web standards .

III.2.4.4 Architecture du VPN SSL

La figure 36 fournit une vue de haut niveau de l'architecture typique VPN-SSL. Cette architecture est le même tant pour le portail VPN-SSL que pour le tunnel VPN-SSL. [13]

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

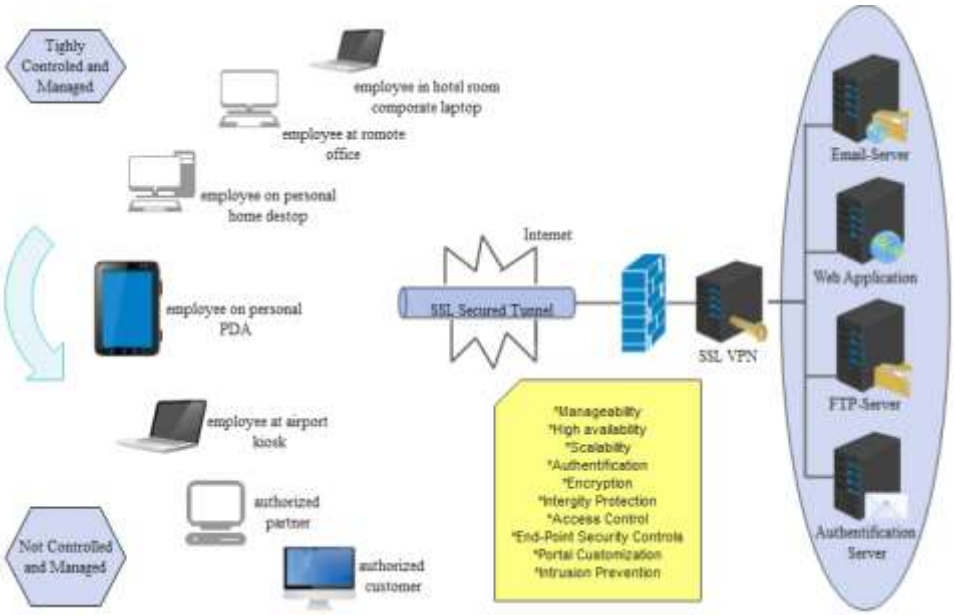

Figure III.35. Architecture du VPNSSL

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 peuvent pas être contrôlés ou gérés par l'organisation. Le VPN-SSL à n'importe quel emplacement incluant un aéroport, un café, ou une chambre d'hôtel. L'utilisateur du client au web est capable d'utiliser le détail VPN-SSL. Tout le trafic est crypté, il traverse des réseaux comme internet et le VPN-SSL. La passerelle est le critère pour la connexion sécurisé et fournit des services divers et des caractéristiques.

III.2.4.5 Les fonctions du VPN-SSL

La fourniture de l'accès éloigné sécurisé a une large variété d'utilisateurs, et des dispositifs a beaucoup d'emplacements, appelle à un ensemble divers des services de VPN-SSL et des caractéristiques. La plupart des VPN-SSL ont au moins une fonction principale suivante : [13]

III.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 [33] Comme le montre dans la figure en dessous

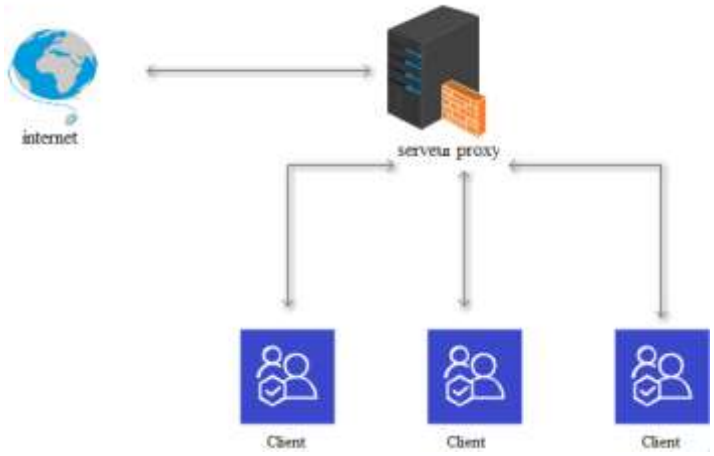

Figure III.36. Proxy

III.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]

III.2.4.6 Les caractéristiques du VPN-SSL :

III.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]

III.2.4.6.2 Adaptabilité

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

III.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]

III.2.4.7 Les services de sécurité du VPN-SSL sont :

III.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. [13]

III.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. [13]

III.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]

III.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. [13]

III.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. [13]

III.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. [13]

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 supporte 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 numérique utilisé 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 former le digital et signer des données avant l'envoie. L'autre critère, vérifie la signature utilisant la clé publique du pair. [13]

VPN-SSL a besoin d'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. Certains 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]

III.2.4.8 Inconvénients

Utilisation des certificats X .509.

III.2.4.9 Avantage

- Authentification forte du client.
- Maintenant, de nombreuses applications utilisant SSL/TLS.
- Confidentialité et intégrité des échanges.
- L'utilisateur utilise les mêmes logiciels sur son LAN.A l'extérieur .les communications sur LAN sont également sécurisées.

III.2.4.10 Utilisation

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

III.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 présenter les différentes les étapes qui nous permettront la bonne réalisation de notre application.

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

IV.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 aux utilisateurs dans un réseau local d'entreprise de se connecter avec des utilisateurs d'une autre entreprise de façon sécurisée.

IV.2 La topologie

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

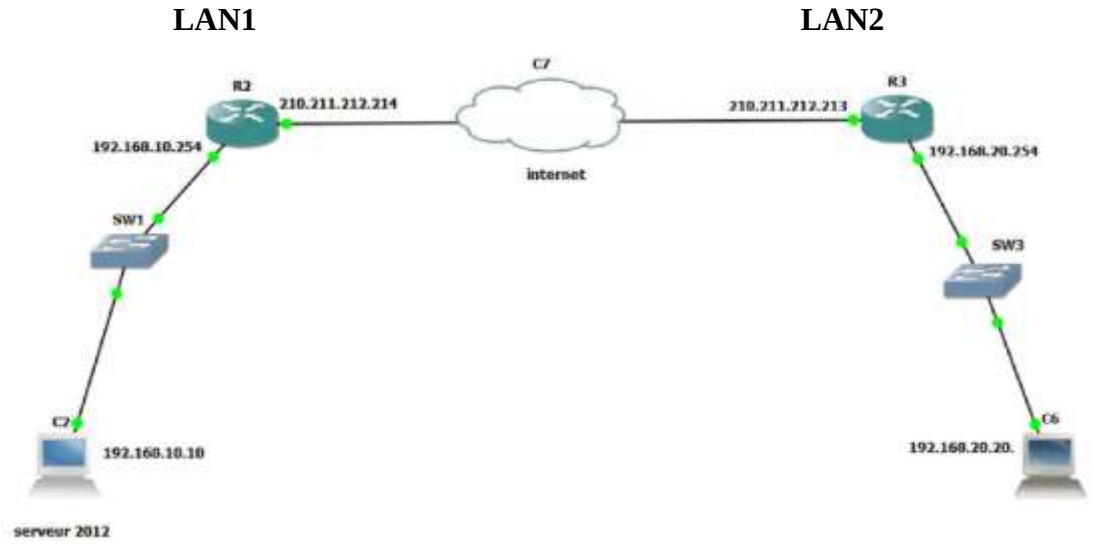

Figure IV.37. La topologie de la simulation du tunnel LAN to LAN

IV.3 Equipements requis

Pour faire fonctionner notre configuration, nous avons utilisé plusieurs équipements. Parmi lesquels :

- un serveur Windows
- un Switch
- routeur

Le serveur Windows est relié 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 de :

- une machine cliente
- un Switch SW3

- un routeur R3

La machine cliente reliée au Switch SW3 puis vers le routeur R. Les deux réseaux LANs sont connectés via Internet.

IV.4 Logiciels utilisés

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

IV.4.1 Le logiciel « GNS 3 »

a) Définition

GNS3 signifie Graphical Network Simulator, est un simulateur graphique de réseau qui permet l'émulation de réseaux complexe. Il est utilisé pour reproduire différentes systèmes d'exploitation dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Inter network Operating Systems). [8]

Figure IV.38. GNS3

b) Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à : [8]

- Dynamips : Emulateur d'IOS Cisco.

- Dynagen : Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.

- Qemu : Emulateur de système.

- Virtualbox : Logiciel permettant la création de machines virtuelles.

- Wireschark : est un logiciel pour analyser les trames.

Grâce à ces composants, GNS3 nous permet :

- Le design de topologies réseaux de haute qualité et complexes.

- Emulation de plusieurs plateformes de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.

- Simulation de switches Ethernet, ATM et Frame Relay.

- Connexion de réseaux simulés au monde réel.

- Capture de paquets grâce à Wireschark.

IV.4.1.1 Créer un projet sous GNS3

Nous allons lancez le logiciel GNS3

Figure IV.39. Raccourci GNS3

IV.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 IV.40. Ouverture d'un nouveau projet sur GNS3

IV.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 on exécute 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.

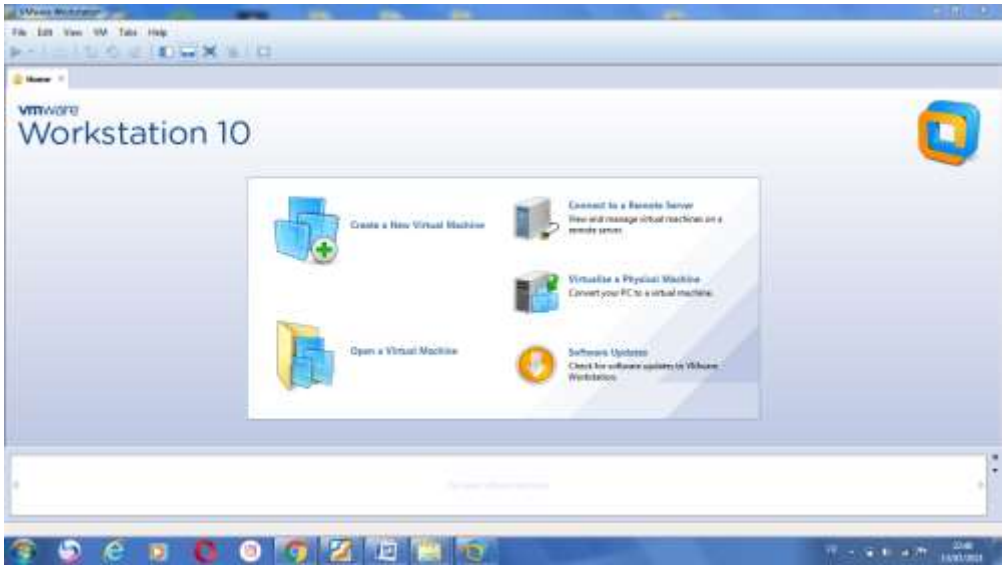

Figure IV.41. Fenêtre principale de VMware Worksation

IV.4.3 TFTP (Trivial File Transfer Protocol ou Protocole Simplifié de Transfert de Fichiers)

Est un protocole simplifié de transfert de fichiers, il fonctionne en UDP.sur le port 69. 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.

IV.4.4 Anyconnect-Win-2.7

Cisco Anyconnect VPN Client est un client VPN Propriétaire permettant de se connecter aux concentrateurs VPN Cisco. S'agit du client de nouvelle génération de l'éditeur, il est limité aux fonctionnalités de type SSL.

IV.5 Microsoft Windows Server 2012

Microsoft Windows Server 2012 est conçu pour fournir aux entreprises la plate-forme 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.

Cette version permet l'installation d'un nombre illimité de machines virtuelles sur un serveur avec maximum 2 processeurs.

IV.5.1 Ouverture et Configuration de Windows Serveur 2012

Nous allons ouvrir VM Workstasion 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.

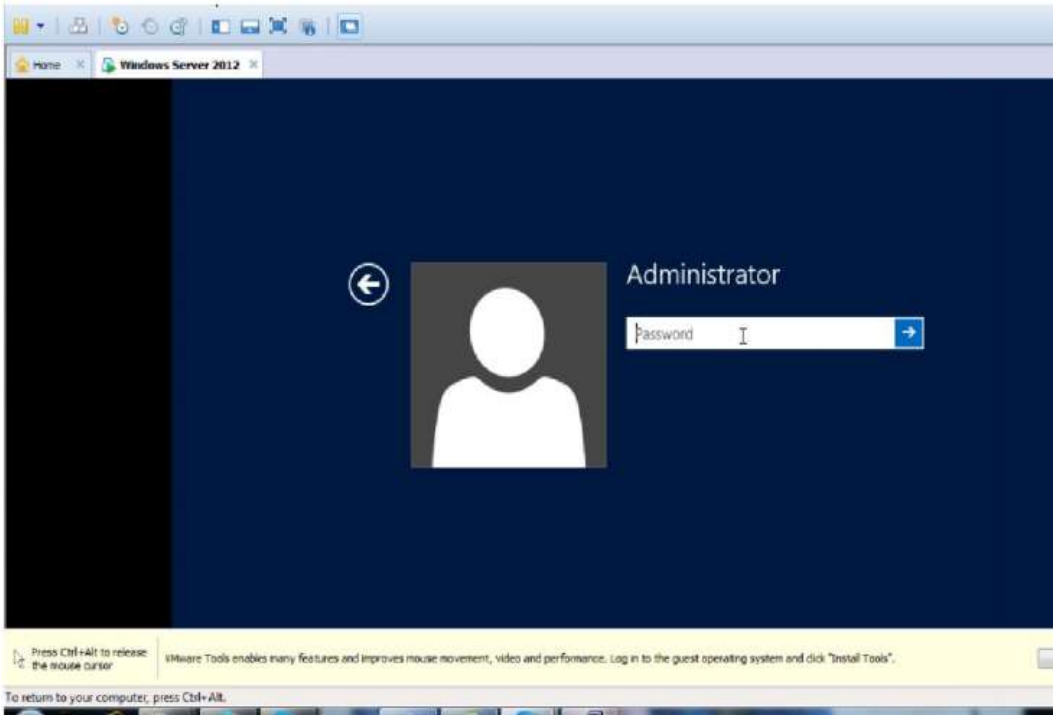

Figure IV.42. Machine virtuelle serveur crée avec VMware.

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

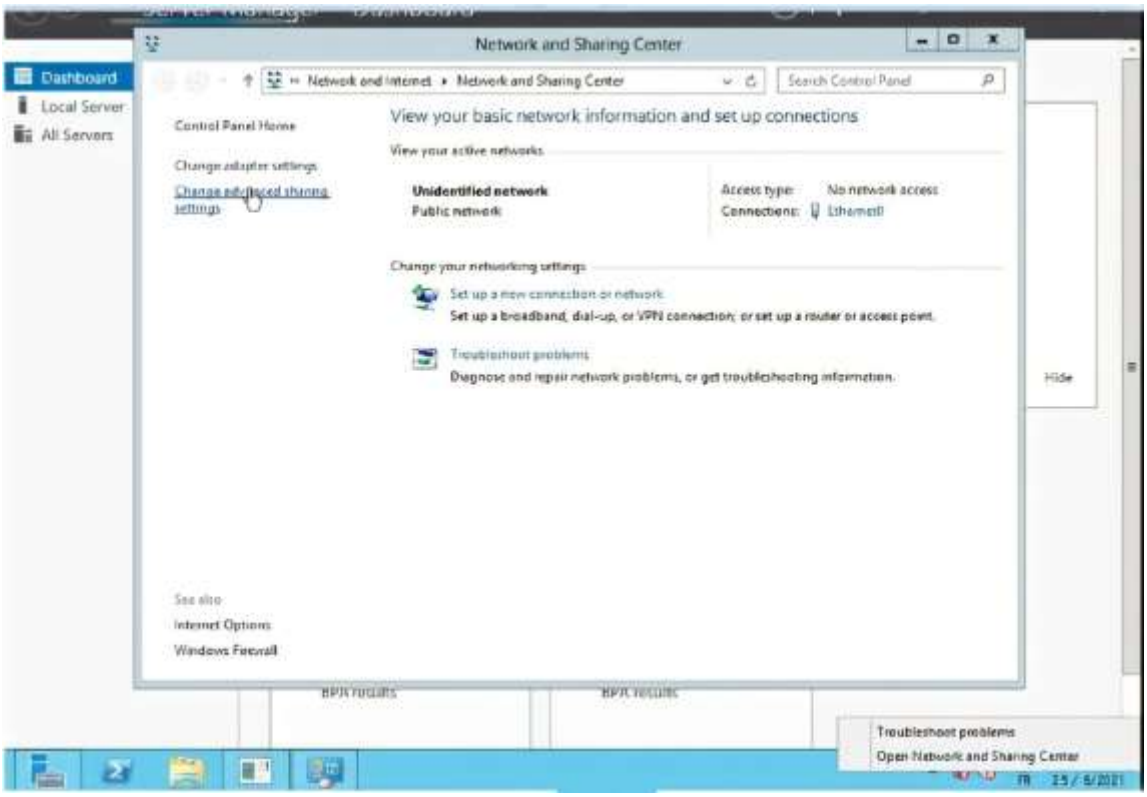

Figure IV.43. La fenêtre connexion réseau

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

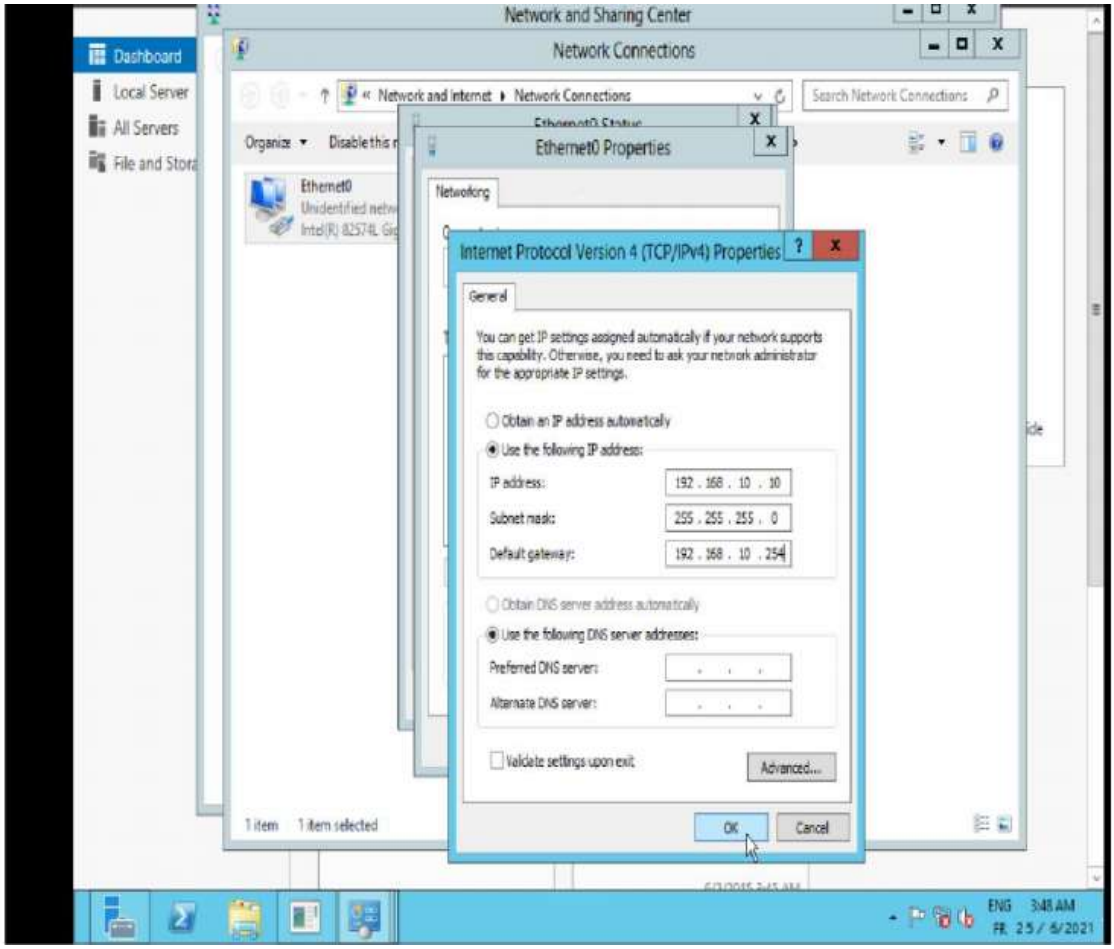

Figure.44. L'adresse IP configurée pour le serveur

IV.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.

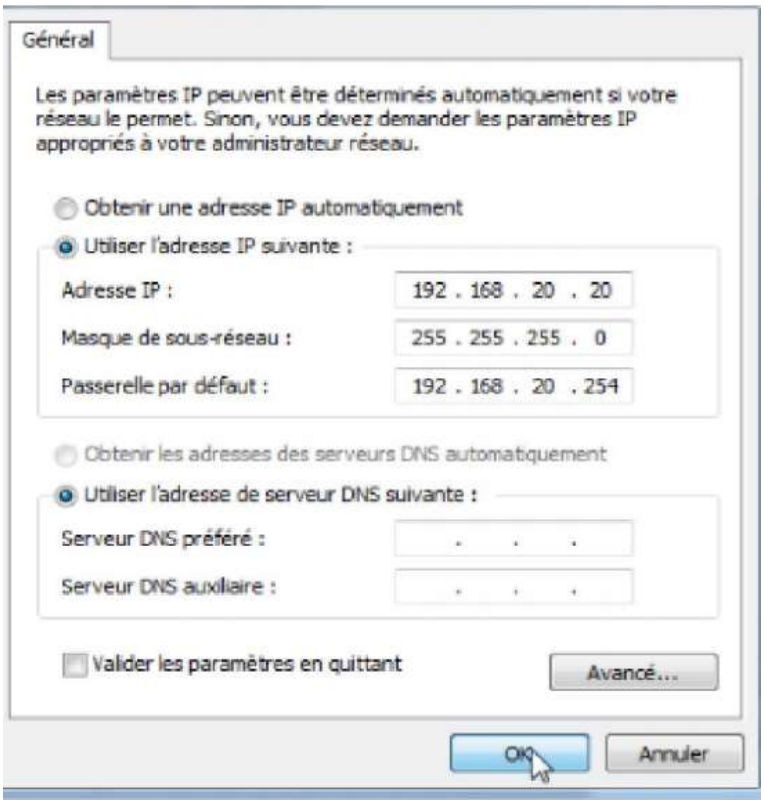

Figure IV.45. L'adresse IP configurée pour le poste client

IV.6 Configuration des Routeurs

IV.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
                          ^
% invalide input detected at '^' marker.

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

Les interfaces sont maintenant activées.

IV.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
```

Les interfaces sont maintenant activées.

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

```
R3#show ip interfs
R3#show ip interface brei
R3#show ip interface br
Interface                  Ip-Address      OK? METHODE Status                protocol
fastEthernet 0/0           192.168.20.254  YES manual  Up                    Up
fastEthernet 0/1           210.211.212.213 YES manual  Up                    Up
R3#
```

IV.6.3 Configuration du NAT (Traduction des Adresses Réseau)

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

Nous configurons le NAT avec les commandes : **Ip nat outsid** et **Ip nat insid**

```
R3#
R3#conf t
Enter configuration commande,one per line, End with CNIL/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)#
```

IV.6.4 Configuration de L'ACL :

Pour pouvoir autoriser le trafic entre un réseau de niveau de sécurité inférieur 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 seules les 20 adresses du LAN1 peuvent accéder au réseau 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 fas
R3(config)#ip nat inside source list 20 interface fastEthrnet 0/1
```

Pour afficher les adresses IP NAT interne et externe nous tapons cette commande : **Show ip nat translations.**

```
R3#
*july 14  19:37:11.687 : %SYS-S-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
i cmp  210.211.212.213:1 192.168.20.20:1   210.211.212.214:1 210.211.212.214:1
R3#
```

Pour sauvegarder nous tapons la commande **'wr'.**

IV.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 nex-mode1
```

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

```
R2(config)#aaa authentification 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 Algérie-Telecom**

```
R2(config)#Username tal Secret test123
R2(config)#webvpn gateway algerie-telecom
%Generating 1024 bit RSA ,Keys Wille 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 commande : **do show run b crypto**.

```
R2(config-webvpn-gateway)# ip add:
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
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
R2(config)#|
```

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
                                                      ^
 % Invalide input detected at '^' marker.

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

13-Assigner la nouvelle passerelle Web VPN que nous avons créée avec la commande : **Gateway Algérie-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 List''**.

```
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 créée, 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)#192.168.10.0  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 un 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 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 tunel webvpn-acl**.

27-Répartir et spécifier le trafic qui passera par le tunnel avec la commande **: svc adress-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 sortie avec 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 tunnelwebvpn-acl
R2(config-webvpn-group)#scv-add
R2(config-webvpn-group)#svc-address-pool sslpool
R2(config-webvpn-group)#svc-rek
R2(config-webvpn-group)#svc-rekey math
R2(config-webvpn-group)#svcsvc 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 apli
R2(config-webvpn-group)#svc apli inc
R2(config-webvpn-group)#svc apli include 192.168.10.0  255.255.255
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 29 :11:17:49.423: %SYS-S-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 fil name [startup-config]? configure t
%Error copying nvram : configure (invalide argument )
R2#configure   t
Enter configuration commands , one pr line .   End with CNIL/Z.
R2(config)#web
%incomplete commande.

R2(config)#de show disk0
Unformated partition , please format   it .
```

IV.7 Vérification

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

- Ping de la machine client du réseau 2 vers la passerelle du routeur R3 du même réseau.
- Ping e la machine client du réseau 2 vers la passerelle du routeur R2 du réseau 1.

- Ping du serveur du réseau 1 vers la passerelle du routeur R2 du même réseau.
- Ping du serveur du réseau 1 vers la passerelle du routeur R3 du réseau 2.
- Ping de la machine client du réseau 2 vers la passerelle du réseau WAN (internet).

Nous avons essayé notre test Ping et les résultats sont présentés ci –dessous :

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

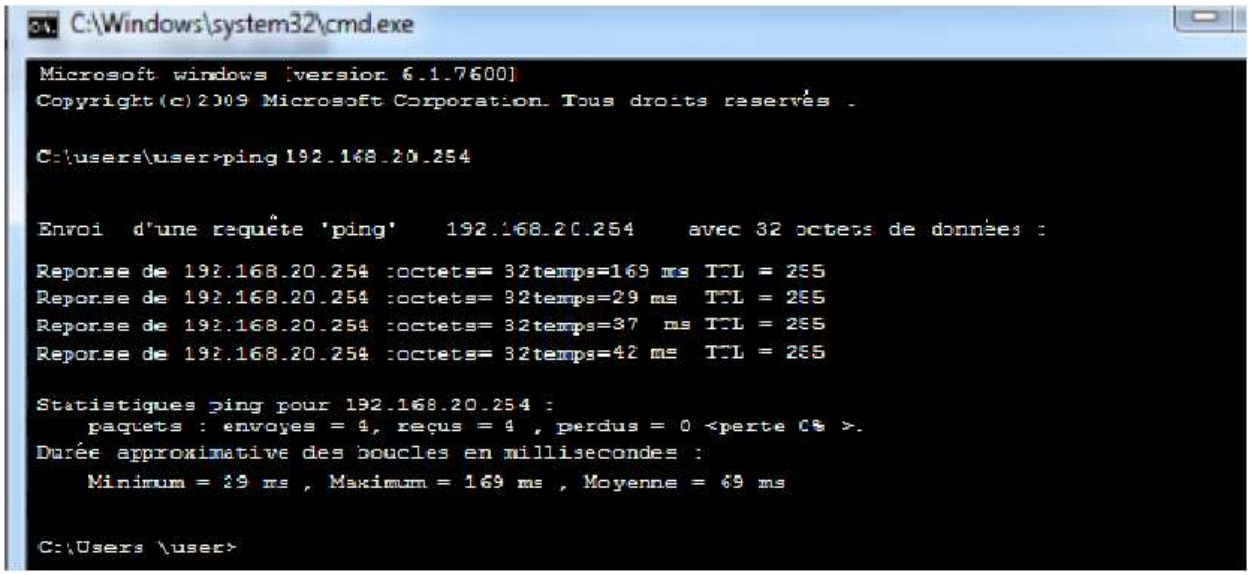

Figure IV.46. Ping de la machine vers la passerelle du LAN2

- Ping de la machine client du réseau 2 vers la passerelle du réseau 1.

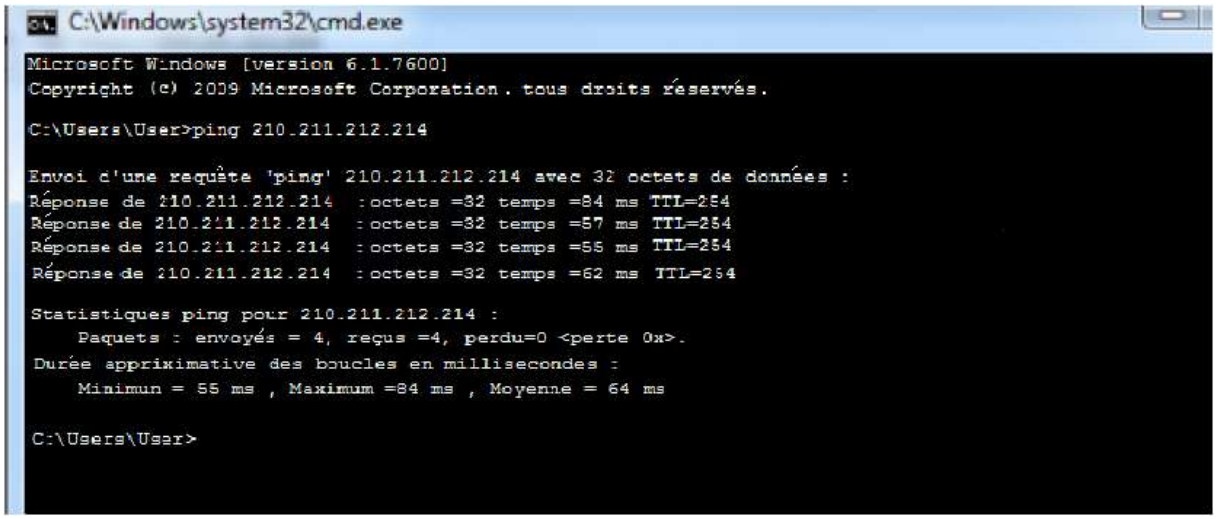

Figure IV.47. Ping de la machine vers la passerelle du LAN1

Nous avons testé la connexion de la machine cliente vers la passerelle de l'autre réseau LAN en traversant le réseau 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 que l'utilisateur du réseau peut accéder au deuxième réseau en toute sécurité.

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

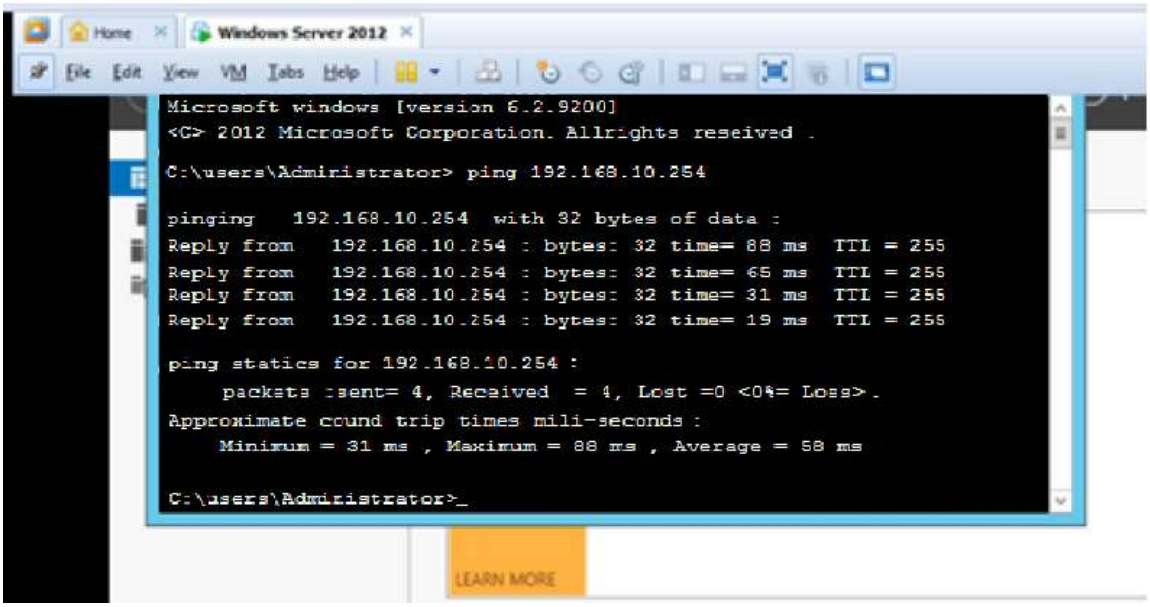

Figure.48. Ping du serveur vers le routeur du LAN 1

- Ping du serveur du réseau LAN 1 vers la machine client de réseau 2.

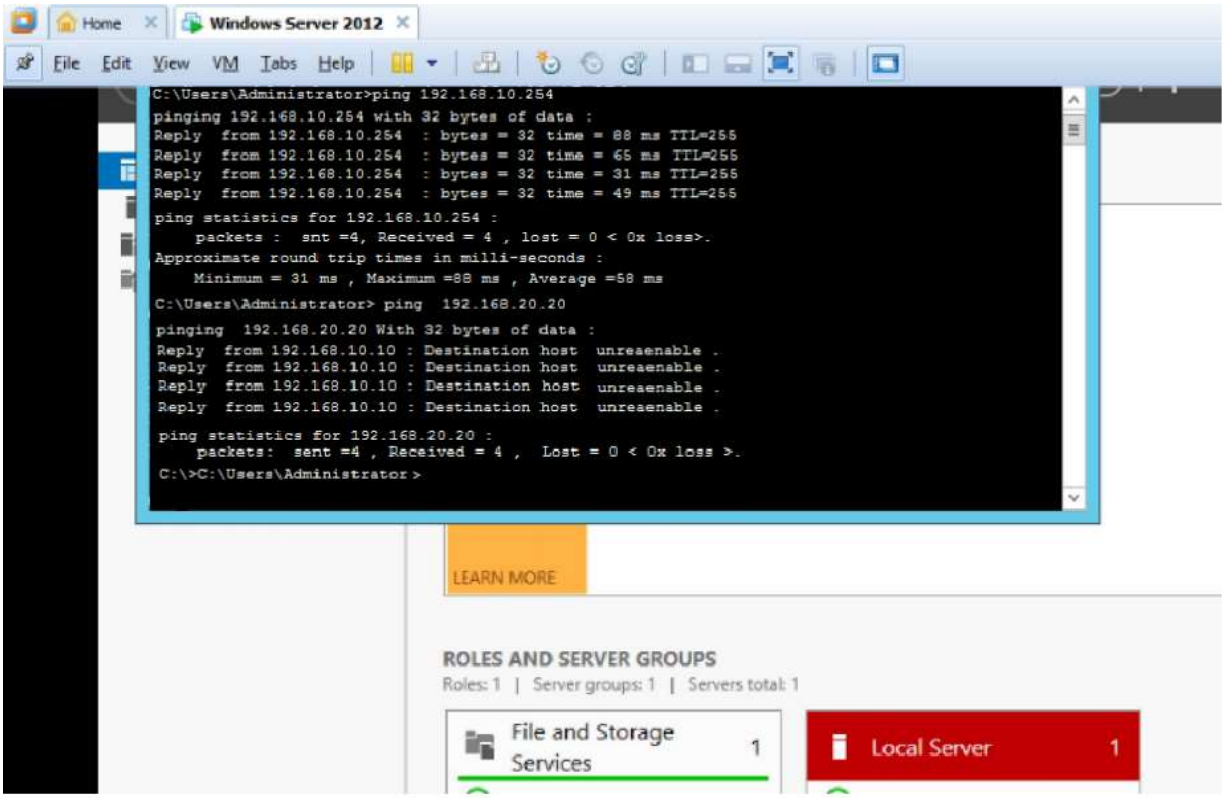

Figure IV.49. Ping du serveur vers la machine client

• Ping de la machine client vers la passerelle du réseau WAN (internet).

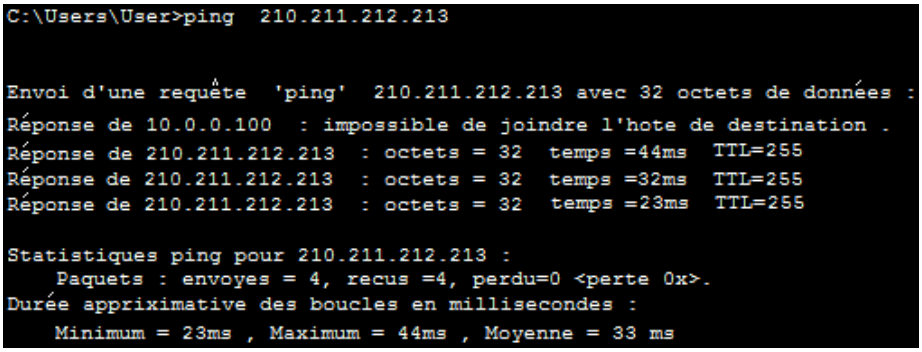

Figure IV.50. Ping de la machine client vers la passerelle WAN

Toutes les requêtes Ping sont réussies. On peut accéder d'un réseau un autre en toute sécurité.

IV.8 Discussion

D'après les résultats des tests, 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 LN1.

De Plus, le tunnel VPN créé permet de bloquer la plupart des menaces de sécurité réseau.

Conclusion

Dans ce mémoire, nous nous sommes intéressés à mettre en place une application permettant à l'utilisateur l'accès aux différentes ressources de l'entreprise de n'importe quel endroit. Nous avons simulé cette application en prenant comme exemple une machine cliente qui se connecte à une autre machine serveur. Ces tests sont réalisées 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]: IT NISRO, CLUB TUTO INFORMATIQUE, **les Listes de contrôle d'accès**, 2012.
[2]: José Dordoigne , Les réseaux Notions fondamentales , 2006.
[3]: G. Lehembre, Sécurité Wi-Fi: WEP, WPA, WPA2, Hakin9 Magazine, no 1, Janvier 2006.
[4]: Danièle Dromard, Dominique Seret, paris, 2009.

[5] : David Matjaba, réseaux informatiques .

[6]: Filiol, les virus informatiques, Springer Verlag, 2009.

[7]: Alex (shurf) frenkel, VPN Mentor, les différents type de VPN et quand les utiliser, 2021.

[8]: A.Ksiks. Etude et simulation sur GNS3 du service MP-BGP/VPN-IP, 2011.

[9]: FILS NZALAKUMBU DIALEMBA, Mémoire de fin d'études en ingéniera en informatique appliqué, Etude des protocoles de sécurité dans le réseau internet, Institut supérieur de techniques appliquées Kinshasa, 2007.

[10]: Melle Sadoud.lila, Melle saddedine .Malika, Mémoire de fin d'études en master 2 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]: Guillaume Desgeorge, La sécurité des réseaux, 2000.

[13]: Carlos M. Gutierrez, Guide To SSL VPNs, July 2008, US department of commerce.

[14]: **www.awt.be/web/sec/index.aspx.**

[15]: **http://www.guidepme.com.**

[16]: http://www.guidepme.com

[17]: C. Llorens, L. Levier, D.Valois, Août 2006, Tableaux de bord de la sécurité réseau, Eyrolles.

[18]: A. Tanenbaum, 2003, Réseaux 4éme édition, Pearson Education.

[19]: Sider.A & Houha.A, cours technologie internet Master 2, 2020/2021, Université de Bejaia.