الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-

Faculté des Sciences et des Sciences Appliquées

كلية العلوم والعلوم التطبيقية

Référence : ...../MM/2021

المرجع:...../م م/ 2021

Mémoire de Master

Présenté au

Département : Génie Électrique
Domaine : Sciences et Technologies
Filière : Télécommunications
Spécialité : Systèmes des Télécommunications

Réalisé par :

ATROUNE Sofia

Et

AMER Salma

Thème

Mise en place d'une solution VPN

Soutenu le: **30/10/2021**

Devant la commission composée de :

Dr : SAOUD Bilal	M.C.A	Université de Bouira	Président
Dr. AYAD Mouloud	M.C.A	Université de Bouira	Rapporteur
Dr. REZKI Mohamed	M.C.B	Université de Bouira	Examinateur

Année Universitaire: 2020-2021

Dédicaces 1

A ma très chère maman « LOUIZA » qui ma soutenu et encouragé durant toute ma vie.

Qu'elle trouve ici le témoignage de ma profonde reconnaissance. Merci pour maman sans toi je ne serais pas ici aujourd'hui. Je t'aime

A la mémoire de mon père « MOHAMED » décédé trop tôt, qu'il apprécie cet humble geste comme preuve de reconnaissance de la part de sa fille, j'aurais aimé que tu sois à mes cotés pour voir la fierté dans tes yeux que dieu l'accueil dans son vaste paradis

A mes frères et sœurs : Serhane, Sonia, Sofiane, Sarra.

A mon oncle « YOUCEF » qui m'as toujours soutenu et encouragé.

A ma moitie, mon binôme SALMA ainsi que sa famille AMER.

SOFIA.

Dédicaces 2

Je dédie ce modeste travail à :

Ma mère, aucun hommage ne pourrait être à la hauteur de l'amour dont elle ne cesse de me combler. Que dieu lui procure bonne santé et longue vie.

A la mémoire de mon père que dieu l'accueil dans son vaste paradis. A celui qui j'aime beaucoup et qui m'a soutenue tout au long de ce projet.

A mon frère FATEH et son fil AMAYASSE, mes sœur : TIHA, HANAN, MIMI, NOUNACHE, ZINEB.

A toute ma famille et mes amis

A mon binôme Sofia et toute la famille ATROUNE.

Et à tous ceux qui ont contribué de près ou de loin pour que ce travail soit possible, je vous dis merci.

SALMA.

Remerciements

Ce travail a été effectué au sein du Département des Sciences et sciences appliquées de l'Université de Bouira.

Je tiens à remercier, en premier lieu, Dr. AYAD Mouloud, Directeur de ce mémoire, pour ses conseils et son aide.

Nous remercions également tous les membres du jury pour l’intérêt qu’ils ont porté à notre travail :

Enfin, on associe à ces remerciements tous ceux qui ont contribué à réaliser ce travail.

Résumé

En ces temps modernes la sécurité des données est un paramètre très important pour le bon fonctionnement de tout réseau informatique. C’est la raison pour laquelle les ingénieures du domaine devraient mettre en place une gestion, des mécanismes de sécurité et des protocoles plus robustes et efficaces pour protéger leurs réseaux. Dans ce contexte nous avons étudié la technologie VPN qui permet aux utilisateurs et administrateurs de systèmes d'information de bénéficier des mêmes conditions d'utilisation, de fonctionnement et de sécurité que les réseaux privés via les réseaux publics. Cette nouvelle technologie permet aux utilisateurs d'accéder à distance à un réseau privé afin de partager leurs données de manière discrète grâce à un protocole sécurisé, qui est le principal outil de mise en œuvre VPN. Dans ce projet, nous avons utilisé Packet Tracer pour la création de VPNs site à plusieurs sites, et ce en se basant sur le protocole IPSec dans son modetunnel.

Mots clés : sécurité, VPN, Tunnel, IPsec, packet tracer.

Table des Matières

Remerciements I
Résumé II
Table des Matières III
Liste des Figures IV
Liste des Tableaux VI
Listes des Acronymes et Symboles VIII

Introduction Générale 1

Chapitre 1 :Généralités sur les réseaux informatiques.

I.1. Introduction 2
I.2. Définition d'un réseau 2
I.3. Intérêt d'un réseau 2
I.4. Topologie d'un réseau 2
I.4.1. Topologie physique 2
a. Topologie bus 3
b. Topologie étoile 3
c. Topologie en anneau 4
d.Topologie maillée 4
I.5. Architecture réseaux 5
I.6. Type de réseaux 5
I.6.1. Réseau local LAN 5
I.6.2. Réseaux métropolitains MAN 6
I.6.3. Réseaux étendus WAN 6
I.7. Les différents dispositifs de la connéctivité 7
I.7.1. Les répéteurs 7
I.7.2. HUB 7
I.7.3. Switch 8
I.7.4. Les ponts 8
I.7.5. Les retours 8
I.7.6. Passerelles 9
I.8. Notion de protocole 9
I.9. Le Modèle OSI 9
I.9.1. Les couche du modèle OSI 9
I.10. Le modèle TCP/IP 10
I.10.1. Comparaison entre le modèle TCP/IP et OSI 11
I.11. Format de l'adresse IP 12
I.11.1. Notation d'adresse IP 12

Table des Matières

I.12. Conclusion 13

Chapitre 2 : Concepts généraux sur les VPNs.

II.1. Introduction 14
II.2. Sécurité de l'information 14
II.2.1. Les téchniques d'attaques 14
a. Attaque contre la communication 14
b. Interposition 15
c. Coupure 15
II.2.2. Les types d'attaques 15
a. Les attaques logicielles 15
b. Autres attaques 15
II.2.3. Les méthodes de protéction 15
II.3. Description d'un réseau privé virtuel VPN 15
II.3.1. Définition d'un VPN 15
II.3.2. Fonctionnemennt de VPN 15
II.3.3. Types des VPNs 16
II.3.3.1. Intranet VPNs 16
II.3.3.2. Extranet VPNs 17
II.3.3.3. VPNs d'accès 17
II.4. Les protocoles de VPN 17
II.4.1. Le PPTP (Point to Point Tunneling Protocol) 18
II.4.2. Le L2TP (Layer 2 Tunneling Protocol) 18
II.4.3. Le SSTP (Secure Socket Tunneling Protocol 18
II.4.4. Open-VPN 18
II.4.5. IKE (Internet Protocol Security) 18
II.4.6. IPSec (Internet Protocol Security) 18
II.5. Diffie Hellman (DH) 19
II.6. Principe de cryptage 19
II.7. Exemple d'algorithmes de chiffrement symétrique 20
II.7.1. DES (Data Encryption Standard) 20
II.7.2. 3DES (Triple DES) 20
II.7.3. AES (Advandes Encryption Standard) 20
II.8. Exemple d'algorithmes de chiffrement asymétrique 20
II.8.1. RSA (Rivest Shamir Adleman) 20
II.9. Fonction de hachage 20
II.9.1. MD-5 (Message Digest 5) 21
II.9.2. SHA (Secure Hash Algorithme) 21
II.10. Avantages et inconvénients des VPNs classiques 21

Table des Matières

III.1. Introduction 22
Chapitre3 : Mise en place d'un réseau VPNs
III.2. Présentation du simulateur « Cisco Packet Tracer » 22
III.3. Installation et configuration de IPsec VPN Tunnel 23
III.3.1. Tables d'adressage 23
III.3.2. Méthode de configuration 24
III.3.3. Configuration des équipements 24
III.3.3.1. Configuration des retours 24
III.3.3.2. Configuration des PCs 27
III.3.3.3. Configuration de l'IPsec sur les retours R1 et R3 28
III.4. Test de connectivité 30
III.5. Conclusion 33
Conclusion Générale **34**
Références **35**

Liste des Figures

Fig. I.1. Topologie en bus 3
Fig. I.2. Topologie étoile 3
Fig. I.3. Topologie en anneau 4
Fig. I.4. Topologie maillée 5
Fig. I.5. Réseau local LAN 6
Fig. I.6. Réseau métropolitaine 6
Fig. I.7. Réseauétendu WAN 4
Fig. I.8. Répéteur 7
Fig. I.9. Hub 7
Fig. I.10.Switch 8
Fig. I.11. Routeur 8
Fig. I.12. Le modèle TCP/IP 11
Fig. I.13. Les modèles OSI et TCP/IP 12
Fig. I.14. Adresse IP 12
Fig. I.15. Structure de l'adresse IP 13
Fig. II.1.L'intranet VPN 16
Fig. II.2. L'extranet VPN 17
Fig. II.3.VPN d'accès 17
Fig. III.1.Architecture du réseau sous Cisco Packet Tracer 22
Fig. III.2. Interface CLI (Command Line Interface) 24
Fig. III.3. Configuration du hostname 25
Fig. III.4. Configuration du mot de passe 25
Fig. III.5. Configuration des interfaces 26
Fig. III.6. Configuration IP route pour R1. 26
Fig. III.7. Configuration IP route pour R3 26
Fig. III.8. Vérification de la licence de sécurité 26
Fig. III.9. Activation de la licence de sécurité 27
Fig. III.10. Configuration des PCs 27
Fig. III.11. Configuration ACL pour R1 28
Fig. III.12. Configuration ACL pour R3 28
Fig. III.13. Configuration des ISAKMP policy et ISAKMP key 29
Fig. III.14. Configuration des propositions IPsec pour R1 29

Fig. III.15. Configuration des propositions IPsec pour R3 29
Fig. III.16. Configuration de la crypto map pour R1..... 30
Fig. III.17. Configuration de la crypto map pour R3..... 30
Fig. III.18. Application de la crypto map sur l'interface G0/0 : (R1 et R3) 30
Fig. III.19. Test de connectivité 1 31
Fig. III.20. Test de connectivité 2 31
Fig. III.21. Vérification du statuts d'ISAKMP pour R1 et R3..... 32
Fig. III.22. Vérification d'ISAKMP policy pour R1 et R3 32
Fig. III.23. Vérification IPsec pour R1 et R3..... 32
Fig. III.24. Vérification de la crypto map.....33

Liste des Tableaux

Tab.I.1. Modèle OSI 10
Tab.III.1. Table d'adressage..... 23

Listes des Acronymes et Symboles

- **Acronymes**

ACL	Access Control List
IPsec	Internet Protocol Security
VPN	Virtual Private Network
LAN	Local Area Network
OSI	Open System Interconnexion
HUB	Host Unit Broadcast
MAC	Media Access Control
MAN	Metropolitain Area Network
WAN	Wide Area Network
COI	Centre d'inertie (Center of Inertia)
LF	Logique floue
AG	Algorithme génétique
ISO	Organisation Internationale de Normalisation
TCP/IP	Transmission Control Protocol/Internet Protocol
VLAN	Virtual Area Network
PPTP	Point to Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
SSTP	Secure Socket Tunneling Protocol
IKE	Inetrnet Protocol Security
DES	Data Encryption Standard
3DES	Triple DES
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman
MD-5	Message Digest 5
SHA	Secure Hash Algorithme
CLI	Command Line Interface
ACL	Acess Control List
ISAKMP	Internet Security Association and Key Management Protocol

Introduction Générale

De nos jours, l'internet est considéré comme la plus grande source d'information qui existe au monde. Toute entreprise ou établissement ayant un accès à cet outil est en possession de diverses informations privées, peuvent être en proie de cyber attaques. Ces cybers attaques ont pour but d'interrompre le fonctionnement d'un réseau informatique, d'intercepter et modifier les informations. Afin qu'on puisse éviter les risques de ces attaques, il faut impérativement garantir une sécurité du réseau informatique de l'entreprise et le rendre moins vulnérable.

L'objectif de notre projet est de mettre en exécution un mécanisme de sécurisation de données ainsi que leurs échanges entre deux réseaux locaux. En plus, il est nécessaire de segmenter le réseau local de chaque entreprise en plusieurs LAN virtuels, pour réduire les domaines de collisions et éviter les congestions. Ce qui permet de renforcer la sécurité au niveau du réseau local. Pour pouvoir atteindre et concrétiser cet objectif, nous avons à notre disposition des solutions de sécurisation, parmi lesquelles, on a opté pour le protocole IPSec qui est le principal outil qui nous permettra d'implémenter les VPN.

Pour bien mener ce travail, nous avons organisé notre mémoire en trois chapitres structurés comme suit : Le premier chapitre s'intitule « Généralités sur les réseaux informatique » où nous présentons quelques concepts de base des réseaux informatiques. Dans le deuxième chapitre titré « Concepts généraux sur les VPNs » nous définirons en premier lieu sur la sécurité de l'information puis sur ce qu'est un réseau privé virtuel, ensuite nous parlons de son fonctionnement et de ses objectifs. Nous finirons par citer les différents protocoles de mise en place, principalement l'IPSec, sa compréhension nous aidera dans la réalisation. Dans le troisième et dernier chapitre, nous allons enfin passer à la « Réalisation », on premier lieu nous introduirons l'outils et logiciel ayant servi à l'élaboration du projet, tout en expliquant les configurations, nous passerons ensuite au deuxième lieu qui sera consacrée à l'implémentation de la solution VPN grâce au protocole IPSec. Enfin, dans la conclusion générale, nous ferons une récapitulation du travail effectué ainsi que l'expérience acquise.

Chapitre 1:

Généralités sur les réseaux informatiques.

I.1. Introduction :

En connectant tous les postes de travail, périphériques, terminaux et autres unités de contrôle de flux, les entreprises d'un réseau informatique peuvent effectivement échanger divers éléments (fichiers, imprimantes, etc.) et l'échanger des données, même par e-mail et messagerie instantanée. Il permet également des liaisons de serveur de données, de communication et de serveur de fichiers.

I.2. Définition d'un réseau :

C'est est un groupe des terminaux relier ensemble et qui exploite les mêmes ressources informative (word, png…) ou matérielle (imprimante) ou logiciel [1].

I.3. Interet d'un réseau :

Voici quelques-uns des avantages des réseaux informatiques :

- Partage de fichiers.
- Partage des ressources.
- Capacité de stockage accrue.
- La communication entre les membres du réseau.

I.4. Topologie d'un réseau :

La topologie d'un réseau constitue l'organisation ou la relation des périphériques réseaux et les interconnexions existantes entre eux comprennent deux types de topologies différentes utilisées pour décrire les réseaux.

I.4.1 Topologie physique :

Elle illustre l'emplacement physique des dispositifs intermédiaires et l'installation des câbles, on distingue les topologies suivantes :

- Topologie étoile ou étoile étendue.
- Topologie maillée.
- Topologie bus.
- Topologie anneau.

a. Topologie bus : Tous les périphériques du réseau sont connectés à un seul câble ou à une seule ligne. En général, le terme fait référence à la façon dont divers appareils sont configurés dans un réseau. Pour communiquer entre eux l'appareil envoie un message de diffusion sur le fil que tous les autres appareils voient, mais seul le destinataire prévu accepte et traite réellement le message.

- **Avantage :**

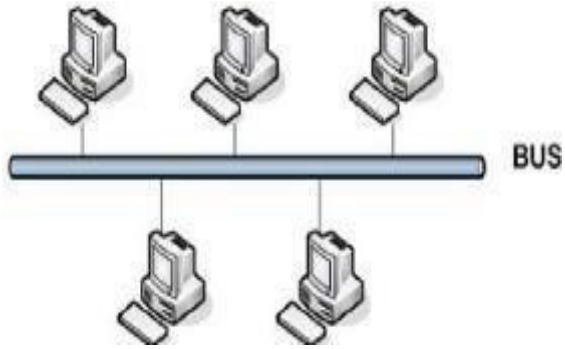


Figure I.1 : Topologie en bus [2].

- Cela fonctionne bien lorsque vous avez un petit réseau.
- C'est la topologie de réseau la plus simple pour connecter des ordinateurs ou des périphériques de manière linéaire.
- Il ne nécessite pas beaucoup de câblage par rapport aux alternatives

- **Inconvénient :**

- Il peut être difficile d'identifier les problèmes si tout le réseau tombe en panne.
- Il peut être difficile de résoudre les problèmes de périphériques individuels.
- La topologie en bus n'est pas idéale pour les grands réseaux.
- Si un câble principal est endommagé, le réseau tombe en panne.

b. Topologie étoile :

C'est une topologie dans laquelle tous les nœuds sont connectés à un périphérique central, formant ainsi une étoile. Deux types de périphériques fournissant un point de connexion central commun aux nœuds du réseau sont un Hub et un Switch.

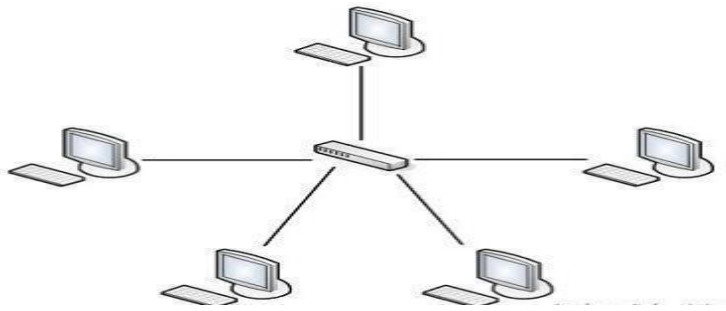


Figure 1.2 : Topologie étoile [2].

- **Avantage :**
  - Facile d'ajouter un autre ordinateur au réseau.
  - Chaque lien est indépendant l'un de l'autre, si un appareille s'arrête le réseau continue à fonctionner
- **Inconvénients :**
  - L' implémentation peut avoir un coût plus élevé, notamment si vous utilisez un commutateur ou un routeur comme périphérique central.
  - Le périphérique réseau central détermine les performances et le nombre de nœuds que le réseau peut gérer.
  - Si l'ordinateur central, Switch ou Hub tombe en panne, tout le réseau tombe en panne et tous les ordinateurs sont déconnectés du réseau.

c. Topologie en anneau :

Dans un réseau en anneau, les ordinateurs sont en boucle et chaque ordinateur échange les données à tour de rôle. Tous les messages de communication sont déplacés dans le sens horaire ou antihoraire vers le même répertoire. Seul l'hôte qui détient un jeton peut envoyer des données, et les jetons sont libérés dès que l'autre hôte reçoit les données.

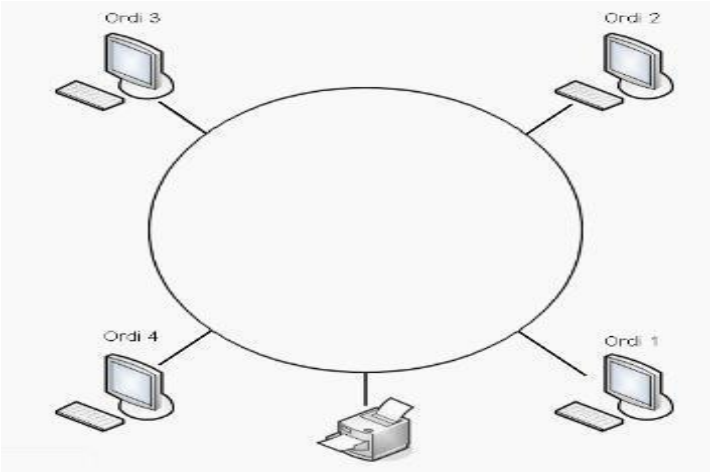


Figure I.3 : Topologie en anneau [2].

d. Topologie maillée :

C'est une topologie de réseau dans laquelle tous les nœuds de réseau sont connectés les uns avec les autres. Il n'existe pas de concept de commutateur (Switch) central, de hub ou d'ordinateur qui serve de point de communication central pour la transmission des messages.

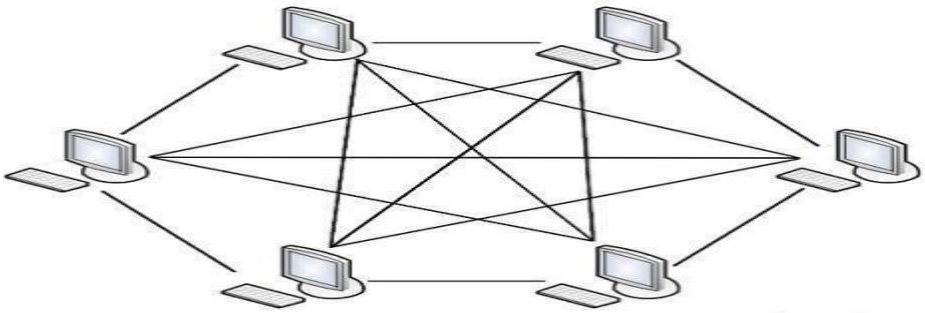


Figure I.4 : Topologie maillée [2].

- **Avantages :**

  - Chaque connexion peut porter sa propre charge de données
  - Il est robuste
  - Une faute est diagnostiquée facilement
  - Assure la sécurité et la confidentialité

- **Inconvénient**
  - L'installation et la configuration sont difficiles si la connectivité devient plus importante
  - Le coût de câblage est de plus en plus élevé dans le cas d'une topologie maillée Entièrement connectée
  - Le câblage en masse est requis

I.1. Architecture réseaux :

L'architecture du réseau c'est la structure et la représentation fonctionnelle du réseau. On trouve deux modèles de ce derniers :

- **Architecture d'égal à égal (peer to peer parfois appelée poste à poste) :** Le réseau est appelé réseau peer-to-peer, chaque ordinateur du réseau peut agir à tour de rôle en tant que client et serveur. Dans cette structure, la gouvernance est décentralisée.

- **Architecture client-serveur :** L'architecture client-serveur est basée sur le serveur qui gère le réseau.

I.6. Type de réseaux :

Il existe différentes sortes de réseaux, On distingue plusieurs types de réseaux qui se différencient entre eux en fonction de la distance entre les systèmes informatiques, ou encore en fonction de la technologie qui permet de les mettre en œuvre et la vitesse de transfert des données ainsi que leur étendue.

Réseaux locaux ou LAN (Local Area Network).

- Réseaux métropolitains ou MAN (Metropolitain Area Network).
- Réseaux étendus ou WAN (Wide Area Network).

I.6.1. Réseau local LAN :

Ce sont des réseaux de taille plus ou moins modeste, complexes, qui permettent l'échange de données informatiques et le partage de ressources (données, disques durs, périphériques divers, etc.). L'étendue géographique des réseaux locaux ne dépasse pas 10 km (ex. : pour un immeuble ou un campus). Le débit, ou la vitesse de communication, varie de quelques Mbps à 100 Mbps. Le nombre de stations ne dépasse généralement pas 1 000 [3].

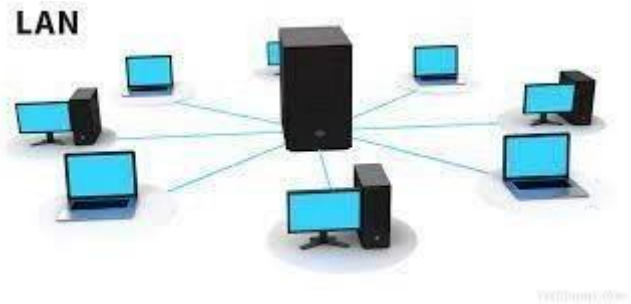


Figure I.5 : Réseau local LAN [2].

I.6.2. Réseaux métropolitains MAN :

Les réseaux métropolitains permettent l'interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une zone urbaine dont l'étendue géographique n'excède pas 200 km. Ces réseaux peuvent être privés ou publics. Ils se distinguent aussi par leurs taux d'erreurs de communication. Le débit est élevé car supérieur à 100 Mbps (sur liens de fibre optique) [3].

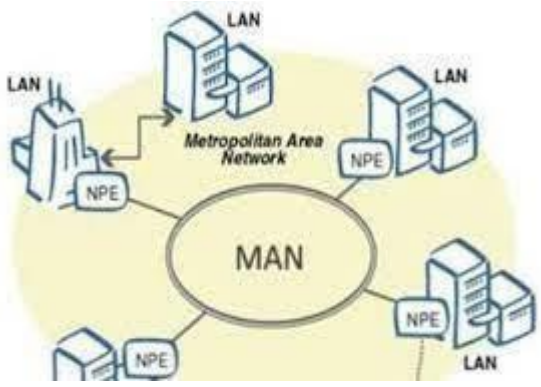


Figure I.6 : réseau métropolitaine MAN [2].

I.6.3. Réseaux étendu WAN :

Un réseau WAN (Wide Area Network), est un réseau étendu ou régional. Ce type de réseau informatique est généralement constitué de plusieurs sous-réseaux (LAN) et couvre une grande zone géographique comme un pays, ou un continent.

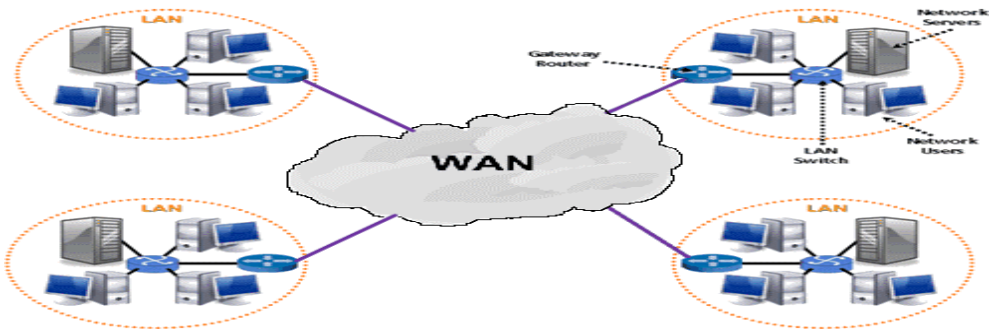


Figure I.7 : Réseau étendu WAN [2].

I.7. Les différents dispositifs de la connectivité :

I.7.1. Les répéteurs :

Le répéteur encore appelé régénérateur est un équipement électronique servant à dupliquer et à réadapter un signal numérique pour étendre la distance maximale entre deux nœuds d'une réseau.il fonctionne uniquement au niveau physique (couche 1 du modèle OSI: Open System Interconnexion). En d'autres termes, il ne fonctionne qu'au niveau des informations binaires se propageant le long de la ligne de transmission, et ne peut pas interpréter les paquets d'informations.

Figure I.8 : Répéteur [2].

I.7.2. HUB (concentrateur) :

Le Hub (en anglais Host Unit broadcast) c'est un dispositif réseau qui fonctionne sur la couche 1 du modèle OSI. C'est un multi-port qui peut regrouper tous les flux réseau sur ses ports et envoyer l'intégralité du flux dans le réseau sans se soucier de l'envoi / réception des nœuds Il n'est pas conçu pour décoder l'entête du paquet pour y trouver l'adresse MAC (Media Access Control) du destinataire.

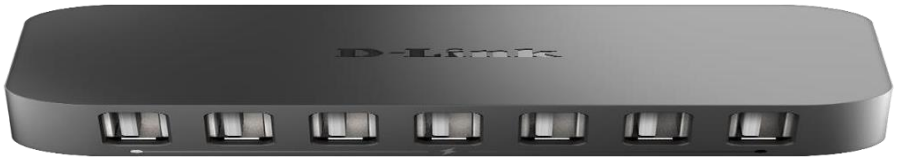


Figure I.9 : Hub [2]

I.7.3. Switch (commutateur) :

Un commutateur c'est un appareil qui connecte plusieurs segments de réseau (câble ou fibre optique) sur un réseau informatique. Il dispose de plusieurs ports entre 4 et 100. Contrairement à un concentrateur, un commutateur ne réplique pas seulement chaque trame qu'il reçoit sur tous les ports. Sur la base de l'adresse que la trame va atteindre, il sait déterminer à quel port la trame doit être envoyée. Ce commutateur est généralement utilisé pour remplacer le concentrateur.

Figure I.10 : Switch [2].

I.7.4. Les ponts :

Un pont est un équipement informatique d'infrastructure de réseaux de type passerelle. Il fonctionne sur la couche liaison de données du modèle OSI. Son objectif est d'interconnecter deux segments de réseaux distincts, soit de technologies différentes, soit de même technologie, mais physiquement séparés à la conception pour diverses raisons (géographique, extension de site etc.).

I.7.5. Les retours :

Un routeur est un périphérique de réseau informatique qui permet aux paquets de données d'être acheminés entre deux ou plusieurs réseaux pour déterminer le chemin que les paquets de données emprunteront. Il a généralement un connecteur RJ45 pour se connecter à un commutateur ou un PC, et peut également avoir une antenne pour la communication sans fil.

Figure I.11 : Routeur [2].

I.7.6. Passerelles :

En anglais Gateway est un dispositif permettant de relier deux réseaux informatiques différents, comme par exemple un réseau local et l'Internet. Ainsi, plusieurs ordinateurs ou l'ensemble du réseau local peuvent accéder à l'internet par l'intermédiaire de la passerelle. Le plus souvent, elle sert aussi de pare-feu, ce qui permet de contrôler tous les transferts de données entre le local et l'extérieur. Elle ne doit pas être confondue avec un pont (couche2) et un routeur (couche 3).

I.8. Notion de protocole :

C'est un ensemble règle requise pour les entités qui ont généralement besoin de collaborer à distance, en particulier pour établir et maintenir l'échange d'informations entre ces entités.

I.9. Le modèle OSI :

Le modèle OSI (en anglais Open System Interconnexion), est un modèle de communication entre ordinateur proposé par l'ISO (Organisation Internationale de Normalisation) afin d'établir des normes de communication entre les ordinateurs du réseau. La norme complète, de référence ISO7498 est globalement intitulée « Modèle Basique de référence pour l'interconnexion des systèmes ouvertes (OSI) », il est devisé en sept couches numérotées.

I.9.1. Les couches du modèle OSI :

- **La couche physique :**

Elle est située au niveau 1 du modèle OSI et peut convertir des bits de données en signaux, et vice versa, pour envoyer et recevoir des trames.

- **La couche liaison de donnée :**

Elle se trouve au niveau 2, elle est utilisée pour le codage, le décodage et l'organisation logique des bits de données. Les paquets de données sont encadrés et adressés par cette couche.

- **La couche réseau :**

Elle se trouve au niveau 3, permet la connexion et le transfert de paquets de données entre différents appareils ou réseaux. Elle fournit les chemins de routage de données pour la communication réseau.

- **La couche transport :**

Responsable de la communication de bout en bout sur un réseau. Sa fonction principale est de recevoir des données de la couche session, de les diviser en petits morceaux si nécessaire, puis de les transmettre à la couche réseau et de s'assurer que les données atteignent correctement l'autre côté.

- **La couche session :**

La couche session contrôle les connexions entre plusieurs ordinateurs. La couche de session suit les dialogues entre les ordinateurs, également appelés sessions. Cette couche établit, contrôle et termine les sessions entre les applications locales et distantes.

- **La couche présentation :**

Elle est utilisée pour présenter les données à la couche application (couche 7) dans un format précis, bien défini et normalisé.

- **La couche application :**

Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur.

Le modèle OSI

Couche	Fonction
Couche n° 7 : application (couche sémantique)	Gère l'échange des données entre deux ordinateurs
Couche n° 6 : présentation (couche syntaxique)	Assure l'intégrité des données quelle que soit la plate-forme
Couche n° 5 : session	Gère les communications entre les deux systèmes
Couche n° 4 : transport	Assure le transport et l'intégrité des données
Couche n° 3 : réseau	Assure le routage des données sur le réseau
Couche n° 2 : liaison des données	Contrôle le flux des informations
Couche n° 1 : couche physique	Spécifie le matériel du réseau et son fonctionnement

Tableau I.1 : Modèle OSI [4].

I.10. Le modèle TCP/IP :

TCP/IP signifie Transmission Control Protocol/Internet Protocol (Protocol de contrôle des transmissions/Protocole Internet). TCP/IP est un protocole de liaison de données utilisé sur Internet. Son modèle est divisé en quatre couches distinctes. Utilisées ensemble, elles peuvent également être appelées une suite de protocoles.

Cette dernière est mise en place pour répondre à un nombre de critères :

- Acheminement des paquets de données sur le réseau.
- Utilisation d'un système d'adressage.
- Contrôle des erreurs de transmission de données.

Les différentes couches du TCP/IP :

- **La couche accès au réseau :**

La couche de liaison de données, également appelée couche d'interface réseau ou couche physique, gère les parties physiques de l'envoi et de la réception de données à l'aide du câble Ethernet, du réseau sans fil, de la carte d'interface réseau, du pilote de périphérique de l'ordinateur, etc.

- **La couche internet :**

La couche Internet, également appelée couche réseau, contrôle le mouvement des paquets sur le réseau.

- **La couche transport :**

La couche transport fournit une connexion des données fiable entre deux appareils. Elle divise les données en paquets, accuse réception des paquets qu'elle a reçus de l'autre appareil et s'assure que ce dernier accuse réception des paquets qu'il reçoit.

- **La couche application :**

Elle englobe les applications standards du réseau.

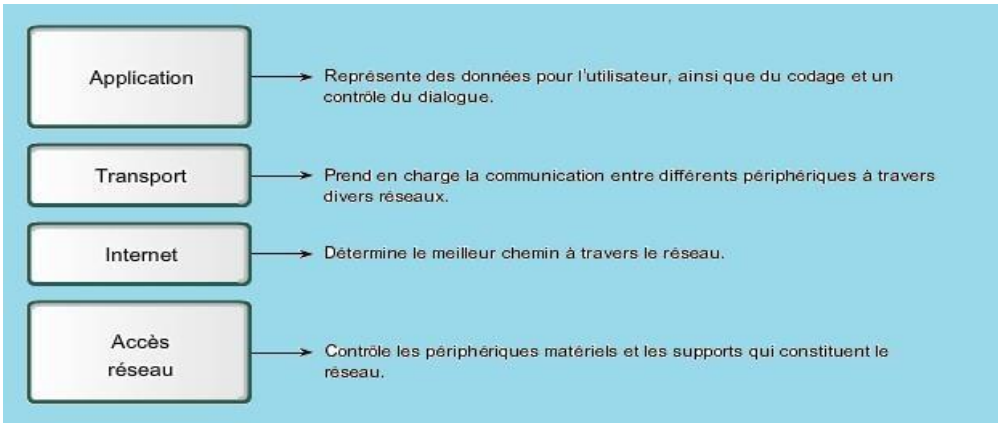


Figure I.12 : Le modèle TCP/IP [4].

I.10.1. Comparaison entre le modèle TCP/IP et OSI :

Ces deux modèles sont très similaires, les deux sont des modèles de communication à couche et utilisent l'encapsulation de données. On distingue deux différences majeures :

- TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau

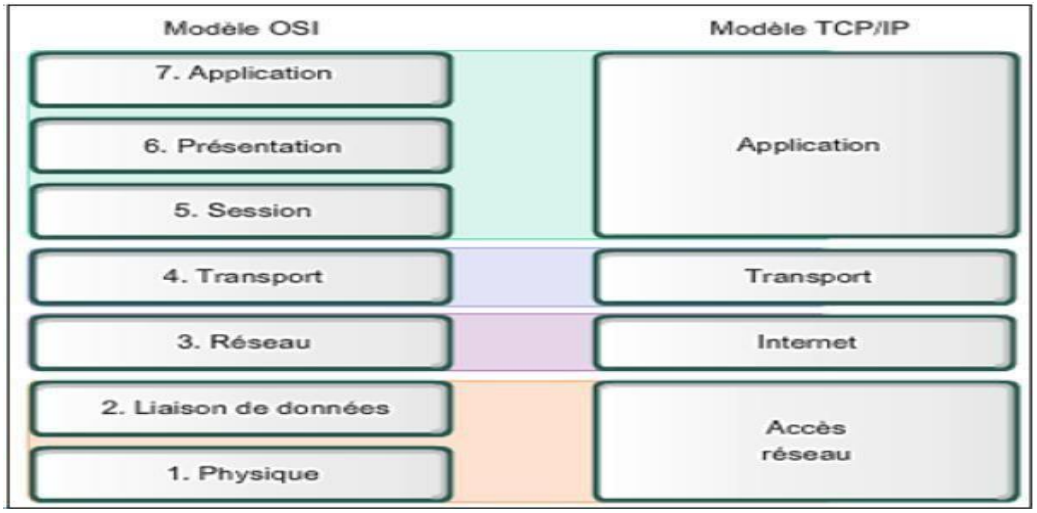


Figure I.13 : Les modèles OSI et TCP/IP [4].

I.11. Format de l'adresse IP :

I.11.1. Notation d'adresse IP :

Le système d'adresse IP fournit une fonction similaire à un système ou à un code postal, qui envoie des informations à une personne et reçoit des informations d'autres personnes. Ce système d'adressage utilise la troisième couche du modèle OSI pour transmettre des informations au destinataire, et nous avons des adresses IP de version 4 et 6 (appelées respectivement IP v4 et IPv6). L'adresse IPv4 est une adresse codée sur 32 bits, identifiée par 4 entiers compris entre 0 et 255, séparés par des points [5].

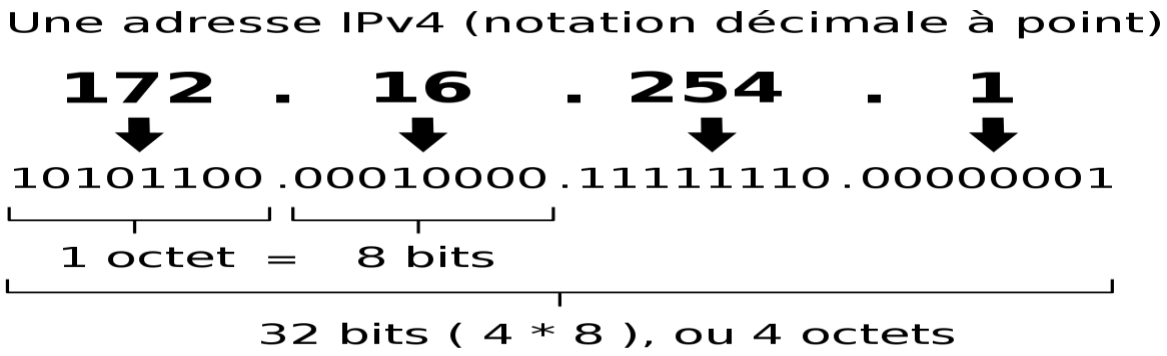


Figure I.14 : Adresse IP [6].

Elle contient à la fois un identifiant réseau (Net ID) et un identifiant équipement (Host ID)

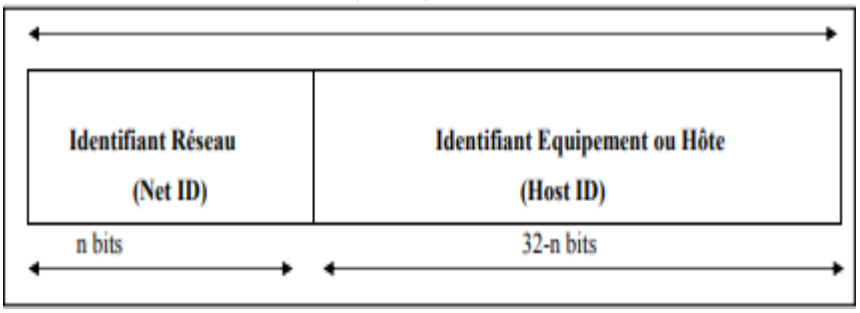


Figure I.15 : Structure de l'adresse IP [6].

I.11.2. Masque sous-réseau :

Le masque de sous-réseau est un nombre de 32 bits utilisé pour distinguer les composants du réseau d'adresse IP en divisant l'adresse IP en une adresse réseau et une adresse d'hôte. Cela se fait à l'aide de mathématiques binaires, où l'adresse réseau est multipliée par les bits du masque de sous-réseau. Comme l'adresse IP, le masque de sous-réseau est écrit en notation décimale à points. Le masque de sous-réseau est également appelé masque d'adresse.

Et par défaut on les retrouve comme suit

- Classe A : 255.0.0.0
- Classe B : 255.255.0.0
- Classe C : 255.255.255.0

I.12. Conclusion :

Dans ce chapitre, on a parlé sur les concepts de base des réseaux informatiques. Ils permettent d'accéder à beaucoup de ressources et c'est la cause de l'augmentation de la demande sur l'utilisation des réseaux. Les risques augmentent. Dans le chapitre suivant, nous présenterons les concepts de base de la technologie VPN.

Chapitre II:

Concepts généraux sur les VPNs.

II.1. Introduction :

Sur internet, on ne sait pas où vont les données, car le routage change, donc les données peuvent être interceptées. Par conséquent, sans protection de sécurité, il est impossible de connecter les deux réseaux locaux entre eux via internet. Dans ces conditions, l'internet fournit une solution VPN idéale pour tirer pleinement parti des fonctionnalités du réseau et se connecter à des emplacements distants. Il existe deux options pour une communication sécurisée entre deux réseaux locaux : la première c'est la connexion des deux emplacements via une ligne dédiée mais coûteuse. La deuxième c'est la création d'un réseau privé virtuel sécurisé (le VPN). Dans ce chapitre, nous nous concentrons sur la deuxième solution qui est le réseau privé virtuel pour sécuriser l'information.

II.1. Sécurité de l'information :

Ce sont des méthodes utilisées pour éliminer la vulnérabilité d'un système informatique aux menaces accidentelles ou délibérées auxquelles il peut être confronté. En d'autres termes, il s'agit d'un ensemble de technologies qui garantissent que les ressources du système d'information d'une organisation (matériel ou logiciel) ne sont utilisées que dans le contexte dans lequel elles doivent être utilisées..[7]

Les exigences de base de cette dernière se reprennent à garantir :

- Disponibilité : Les informations système doivent toujours être disponibles pour le personnel autorisé..
- Confidentialité : Les informations du système ne doivent être divulguées qu'aux personnes autorisées.
- Intégrité : Les informations sur le système doivent pouvoir être modifiées uniquement par les personnes autorisées.

II.2.1. Techniques d'attaques :

a. Attaque de communication : C'est un type d'attaque de confidentialité, qui consiste à accéder aux informations transmises ou stockées, les informations ne sont pas altérées par ceux qui les copient, ces attaques ne sont pas donc détectables par le système et ne peuvent être réparées qu'avec des mesures préventives.

b. Interposition : Ce type consiste à tromper les mécanismes d'authentification pour se faire passer pour un utilisateur (personne ayant les droits dont nous avons besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité (le ip spoofing qui est un vol d'adresse IP).

c. Coupure : Il s'agit d'un accès avec modification des informations transmises par les communications, il s'agit donc d'une attaque d'intégrité.

II.2.2. Les types d'attaques :

a. Les attaques logicielles :

- Les virus.
- Les vers.
- Le cheval de Troie.

b. Autres attaques :

- Balayage de port.
- Usurpation d'adresse IP (IP spoofing).
- Attaque par déni de service (dos dinial of service)

II.2.3. Les méthodes de protection :

- Antivirus.
- La cryptographie.
- Le pare –feu (firewall).
- Les VLAN (virtual Area Network).
- VPN (Virtual Private Network)

II.3. Description d'un réseau privé virtuel VPN :

II.3.1. Définition d'un VPN :

Le réseau privé virtuel VPN correspond à un tunnel sécurisé à l'intérieur d'un réseau. Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP (Internet Protocol) différente [8].

II.3.2. Fonctionnement de VPN :

Le VPN est basé sur un principe appelé tunnel. Ce principe permet de crypter les informations de l'entreprise et de les transmettre d'un bout à l'autre du tunnel. Cela donne à l'utilisateur l'impression qu'il est directement connecté au réseau. Le principe de tunnel consiste à construire un lien virtuel après avoir identifié l'émetteur et le récepteur. Ensuite, la source chiffre les données et les achemine en empruntant ce lien virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets, ou aux

extranets d'entreprise, les réseaux VPNs d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée.

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

1. **Authentification d'utilisateur :** uniquement les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
2. **Gestion d'adresses** : Chaque client sur le réseau doit avoir une adresse IP privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.
3. **Cryptage des données :** Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
4. **Gestion de clés :** Les clés de chiffrement du client et du serveur doivent pouvoir être générées et régénérées.
5. **Prise en charge multi protocole :** La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

II.3.3. Types des VPNs :

Suivant les besoins on référence 3 types de VPN :

II.3.3.1. Intranet VPNs :

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

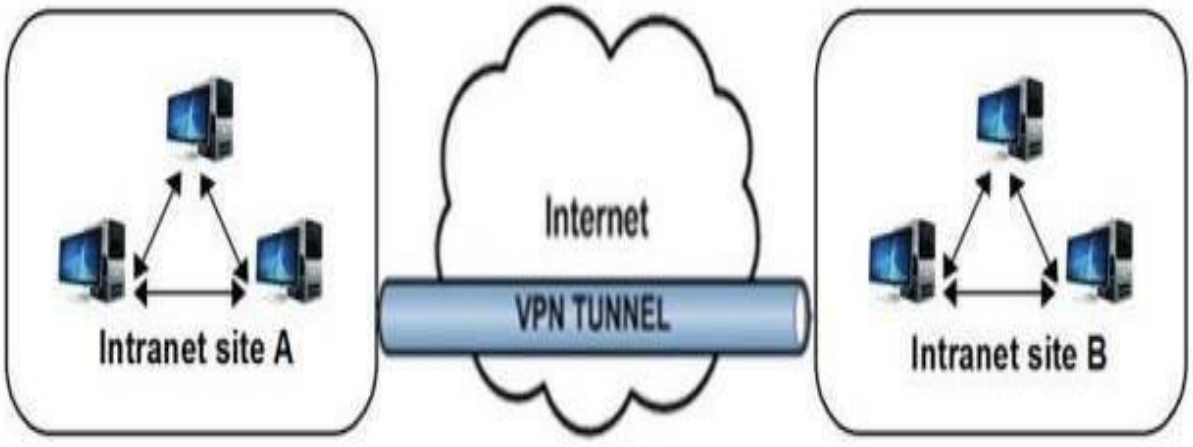


Figure II.1 : L'intranet VPN [5].

II.3.3.2. Extranet VPNs :

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et partenaires. Elle ouvre alors son réseau local à ces derniers, dans ce cas il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus en plus, seule une partie des ressources sera partagée, ce qui signifie une gestion rigoureuse des espaces d'échange.

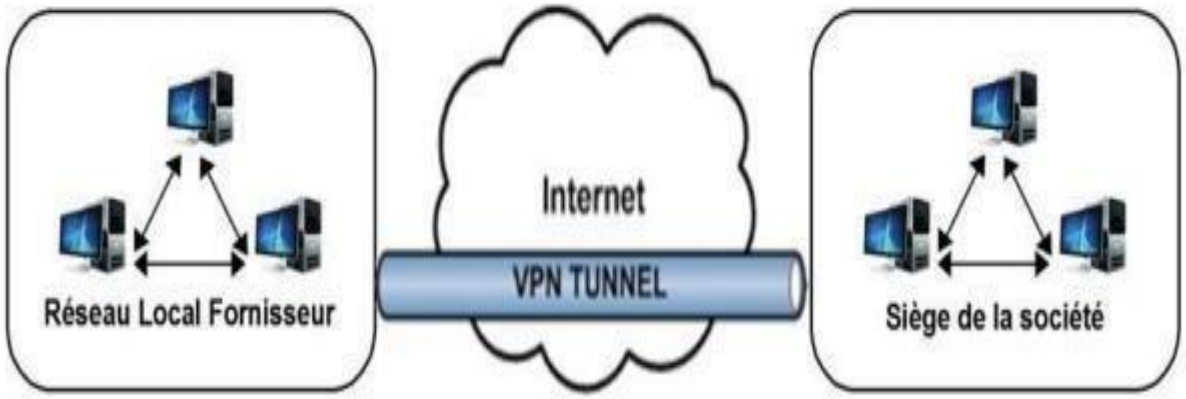


Figure II.2 : L'extranet VPN [5].

II.3.3.3. VPN d'accès :

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leurs entreprises. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.

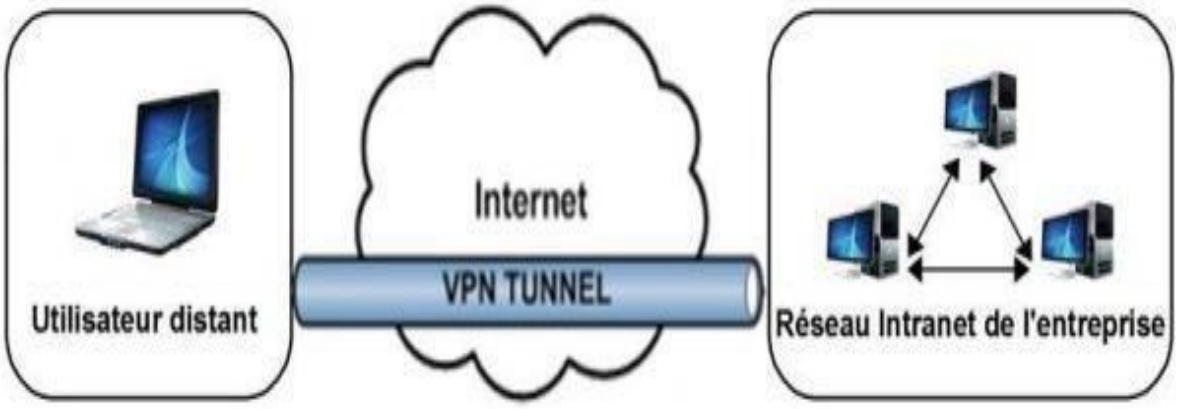


Figure II.3 : VPN d'accès [5].

II.4. Les Protocoles de VPN

Un réseau privé virtuel ou VPN protège et anonymise la connexion internet en se connectant à un serveur distant avant de visiter un site Web. La connexion à ce serveur est également cryptée, ce qui ne signifie qu'aucune requête Web ne peut être vue par le monde extérieur, et ce grâce aux protocoles de cryptage utilisés.

II.4.1. Le PPTP (Point to Point Tunneling Protocol):

Le protocole PPTP est l'un des protocoles plus communs, le plus faciles à mettre en place et le plus rapides. C'est pourquoi le PPTP est particulièrement utile pour les applications qui donnent la priorité à la vitesse, comme le streaming audio ou vidéo, ainsi que pour les appareils plus anciens avec des processeurs plus limités.

II.4.2. Le L2TP (Layer 2 Tunneling Protocol) :

Le protocole L2TP n'a aucune capacité de cryptage ou de confidentialité, il s'appuie sur le protocole IPSec pour un cryptage et une authentification puissante afin de rendre votre connexion plus sécurisée par rapport à PPTP. Il est également facile à configurer avec la plupart des systèmes d'exploitation.

II.4.3. Le SSTP: (Secure Socket Tunneling Protocol):

Le protocole SSTP est l'un des protocoles les plus sécurisés utilisé dans les tunnels VPN. Il est capable de contourner la plupart des pares-feux. Le protocole, bien qu'appartenant à Microsoft, est disponible à la fois pour VPN LINUX et les utilisateurs de MAC.

II.4.4. Open-VPN :

Ce protocole est largement utilisé en raison des divers avantages qu'il offre. Pour commencer, contrairement aux autres protocoles courants, Open VPN est compatible avec les systèmes d'exploitation mobiles tels qu'Android et IOS. Plus important encore, il peut contourner n'importe quel pare-feu et accéder à un certain nombre de ports pour la communication.

II.4.5. IKE (Internet Protocol Security):

Est un protocole de chiffrement par requête et réponse qui définit et maintient automatiquement les attributs d'association de sécurité (SA) dans un ensemble d'authentification (généralement IPSec) pour protéger le trafic. Le VPN IKEv2 est développé conjointement par Cisco et Microsoft. Il est hautement sécurisé, stable et facile à configurer. C'est actuellement l'un des protocoles VPN les plus rapides.

II.4.6. IPSec (Internet Protocol Security) :

L'IPSec est un cadre standard ouvert développé par l'IETF (Internet Engineering Task Force) pour fournir une sécurité cryptographique pour le trafic réseau et l'authentification de la source, des données, de la confidentialité, de l'intégrité et de la protection contre les erreurs et l'anti-relecture. Offrant un support pour IPv4 et IPv6, IPSec est déployé lorsqu'il s'agit de la mise en œuvre d'un VPN. Les termes VPN IPSec ou VPN sur IPSec font référence au processus de création de connexions via

le protocole IPSec. Il s'agit d'une méthode courante pour créer un lien crypté virtuel sur un internet non sécurisé.

IPSec est relativement difficile à configurer car il nécessite un logiciel client tiers, ne peut pas fournir de services via un navigateur Web et configure généralement des canaux d'accès à distance entre plusieurs ordinateurs dans plusieurs emplacements.

Le protocole IPSec fonctionne en deux modes distincts :

- **Mode transport :** Dans le mode transport, ce sont uniquement les données transmises qui sont chiffrées et bien authentifiées. Le reste du paquet IP est modifié et ce mode de routage du paquet n'est pas modifié, ce mode est utilisé pour une communication hôte à hôte.
- **Mode tunnel :** En mode tunnel, c'est la totalité du paquet IP qui est chiffré ou encore authentifié. Le paquet est ensuite encapsulé dans un nouveau paquet IP avec un nouvel IP en tête. A la différence au mode transport, ce mode supporte donc bien la traversée de NAT (Network Address Translation). Le mode tunnel est utilisé pour créer des réseaux privés virtuels permettant la communication de réseau à réseau, d'hôte à réseau ou encore d'hôte à hôte. IPSec crypte le trafic entre deux points de terminaison homologues, et le cryptage est fait entre les deux points de terminaison.

II.5. Diffie Hellman (DH) :

La DH est une méthode de cryptage spécifique développée par Whitfield Diffie et Martin Hellman [9]. Cette méthode permet à deux parties qui n'ont aucune connaissance préalable l'une de l'autre d'établir une clé secrète partagée, même sur un canal non sécurisé. Une telle clé peut être employée pour chiffrer les messages ultérieurs en utilisant un schéma de chiffrement à clé symétrique.

II.6. Principe de cryptage :

Le cryptage est un moyen de convertir les données d'un format lisible en un format codé et illisible à l'aide d'un algorithme. Ce format encodé ne peut être décodé qu'avec la bonne clé de décryptage. De nos jours, les algorithmes de cryptage se répartissent généralement en deux catégories :

- **Cryptage symétrique :** repose sur une clé publique et une clé privée identiques. C'est généralement considéré comme un algorithme "rapide".
- **Cryptage asymétrique :** Ce type d'algorithme (également connu sous le nom de cryptographie à clé publique) utilise différentes clés pour les processus de cryptage et de

décryptage. Bien que cela puisse être pratique, c'est aussi très risqué puisqu'une clé privée perdue ne peut normalement pas être restaurée.

II.7. Exemple d'algorithmes de chiffrement symétrique :

Il existe plusieurs algorithmes de chiffrement symétrique tels que : DES, 3DES, AES et autres.

II.7.1. DES (Data Encryption Standard) :

Il s'agit d'un algorithme de chiffrement symétrique par bloc utilisant une clé de 56 bits. En raison de sa vitesse d'exécution lente et de son espace de clé insuffisant, il n'est plus recommandé pour les attaques système sur les étapes intelligentes.

II.7.2. 3DES (Triple DES) :

Il s'agit d'un algorithme de chiffrement par bloc symétrique qui combine 3 applications DES consécutives avec 2 ou 3 clés DES différentes dans le même bloc de données 64 bits.

II.7.3. AES (Advanced Encryption Standard) :

La norme de cryptage du gouvernement américain est approuvée par le National Institute of Standards and Technology (NIST). AES est un cryptage cryptographique qui utilise une longueur de bloc de 128 bits et une longueur de clé de 128, 192 ou 256 bits. En 2001, il remplace officiellement le Triple DES.AES peut être chiffré en un seul passage au lieu de trois, et sa taille de clé est supérieure aux 168 bits du Triple DES.

II.8. Exemple d'algorithmes de chiffrement asymétriques :

Dans chiffrement asymétrique, on trouve :

II.8.1. RSA (Rivest Shamir Adleman) :

Le RSA est un algorithme de cryptographie asymétrique. Asymétrique signifie en fait qu'il fonctionne sur deux clés différentes, à savoir la clé publique et la clé privée. Le RSA est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance ».

II.9. Fonction de hachage :

Le hachage est un cas particulier de chiffrement, il est irréversible. Le principe est que pourun message quelconque (variable), l'algorithme est capable de générer un message de taille fixe. A partir duquel il est impossible de trouver le message original. Les algorithmes de hachage les plus utilisés à l'heure actuelle sont MD-5 et SHA

II.9.1. MD-5 (Message Digest 5) :

Le MD-5 est une fonction de hachage utilisée en cryptographie. Message Digest 5 produit une valeur de hachage résultante de 128 bits. Généralement utilisée pour vérifier l'intégrité des données grâce à l'empreinte. Ceci peut se faire avec un programme comme md5sum pour MD-5.

II.9.2. SHA (Secure Hash Algorithme) :

Algorithme de hachage plus fort que MD-5 qui génère des messages chiffrés d'une taille de 160 bits.

II.10. Avantages et inconvénients des VPNs classiques :

Dans ce qui suit, nous allons introduire certains avantages et inconvénients des VPN comme suit :

- **Avantages :**
  - **La sécurité :** Assurer la sécurité de l'information et crypter les données pendant la communication
  - **La simplicité :** facile à utiliser pour adopter un système télécommunication classique.
  - **Économie :** L'internet est utiliser comme média principale de transport, ce qui évite les coûts liés à une ligne dédiée.
  - **Évolutivité :** Le VPN permet à l'infrastructure d'évoluer avec les besoins.
- **Inconvénients :**
  - Saturation des passerelles
  - Lourdeur de la connexion
  - Complexité de la communication
  - Manque de savoir maintenir les VPN en marche.

II.11. Conclusion :

Au cours de cette étude, nous avons pu comprendre la notion et le principe de fonctionnement de VPN à travers la définition de ses fonctionnalités et ses principaux d'avantages, et l'intérêt qu'ils y apportent dans le domaine des réseaux.

Chapitre 3:

Mise en place d’un réseau VPN .

III.1. Introduction :

Dans ce chapitre nous allons passer à la dernière étape qui est la simulation. C'est une étape capitale pour la mise en œuvre de notre projet dans le but de mettre en évidence l’efficacité de notre solution. C'est une solution qui permet aux utilisateurs itinérants d'accéder au privé et d'assurer l'échange de données entre eux de manière sécurisée à travers un tunnel VPN. La mise en place se fait à l'aide du simulateur « Cisco Packet Tracer ». Pour démontrer le bon fonctionnement de la liaison, nous effectuons différents tests de validation des configurations.

III.2. Présentation du simulateur « Cisco Packet Tracer » :

Le simulateur Cisco Packet Tracer est un simulateur créé par la société. Le simulateur permet aux étudiants, aux professeurs d'expérimenter le comportement d'un réseau. Le Packet Tracer fournit des fonctionnalités de simulation, de visualisation, de création, d'évaluation et de collaboration et facilite l'enseignement et l'apprentissage des technologies complexes.

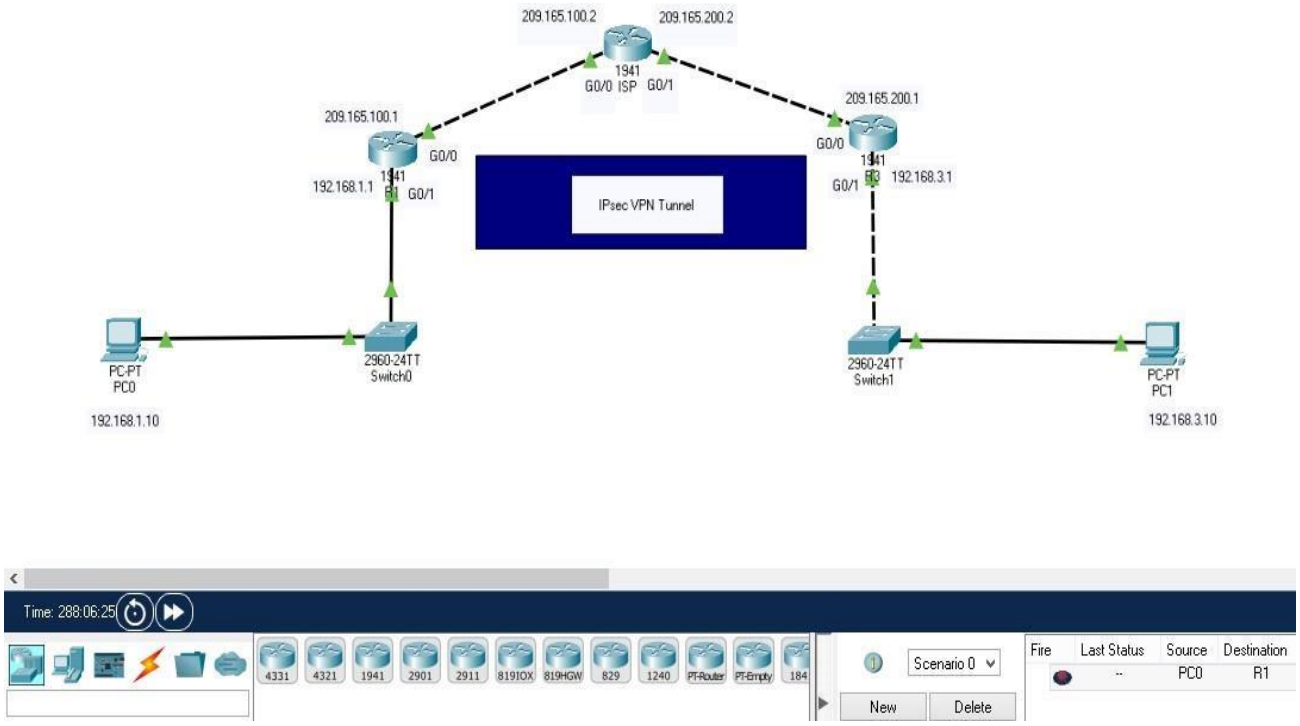


Figure III.1: Architecture du réseau sous Cisco Packet Tracer.

III.3. Installation et configuration de IPsec VPN Tunnel :

III.3.1. Table d'adressage :

Avant même d'entamer la configuration des routeurs et les paramètres VPN, on s'intéresse désormais à la conception du plan d'adressage. Le tableau d'adressage présente le plan d'adressage public ainsi que les segments privés (chaque site dispose d'un segment privé LAN).

Périphérique	Interfaces	Adresse IP	Masque sous réseau
R1	G0/1	192.168.1.1	255.255.255.0
	G0/0	209.165.100.1	255.255.255.0
ISP	G0/1	209.165.200.2	255.255.255.0
	G0/0	209.165.100.2	255.255.255.0
R3	G0/1	192.168.3.1	255.255.255.0
	G0/0	209.165.200.1	255.255.255.0
PC1	Carte réseau	192.168.1.10	255.255.255.0
PC2	Carte réseau	192.168.3.10	255.255.255.0

Tableau III.1 : Table d'adressage.

R1 : Routeur numéro 1.

ISP: Internet service provider (en français, fournisseur d'accès à Internet).

R3 : Routeur numéro 2.

PC1 : Ordinateur numéro 1.

PC2 : Ordinateur numéro 1.

III.3.2. Méthode configuration des équipements :

Pour la configuration des équipements de notre modèle on utilise le CLI (Command Line Interface)

- CLI (Command Line Interface) : est la principale interface utilisateur utilisée pour la configuration, la surveillance et la maintenance des périphériques Cisco. Cette interface

utilisateur vous permet d'exécuter directement et simplement des commandes Cisco IOS, que ce soit à l'aide d'une console ou d'un terminal de routeur, ou à l'aide de méthodes d'accès à distance.[10]

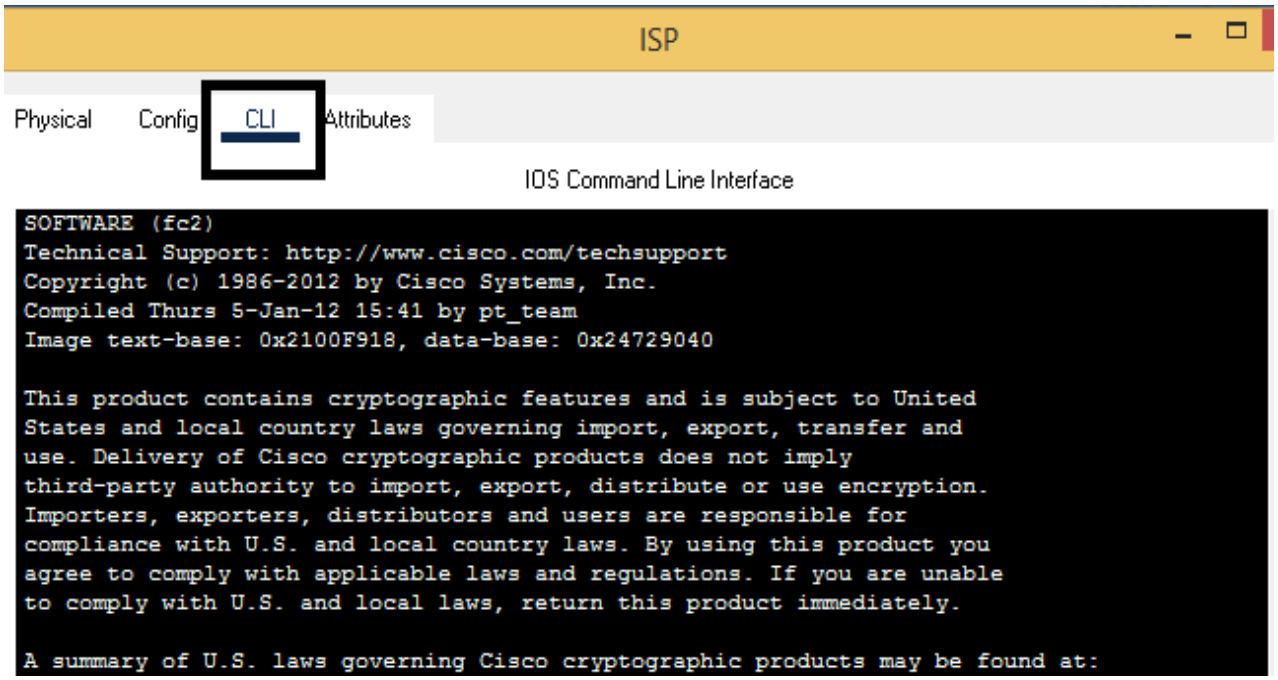


Figure III.2: Interface CLI (Command Line Interface).

III.3.3. Configuration des équipements :

Pour la mise en place de l'IPsec VPN Tunnel, on passe par une série de configurations. Dans ce qui suit, on va présenter la configuration des différents équipements.

III.3.3.1 Configuration des routeurs :

La configuration des équipements se fait par :

- Configuration du Hostname (Nomination des équipements).
- Configuration des mots de passes.
- Configuration des interfaces.
- Vérification et l'activation de licence de sécurité.

a. Configuration du hostname :

Dans la nouvelle version (8.0) du Packet Tracer on peut configurer le hostname sans utiliser la commande « hostname » comme suit :

```
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: ISP
```

Figure III.3 : Configuration du hostname.

b. Configuration du mot de passe :

L'étape suivante c'est la définition du mot de passe pour sécuriser le routeur.

```
  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: bouira

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: bouira
% Please choose a password that is different from the enable secret
  Enter enable password: vpn

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: azert
```

Figure III.4 : Configuration du mot de passe.

c. Configuration des interfaces :

L'étape suivante c'est la configuration des interfaces entre les équipements.

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#interface G0/0
ISP(config-if)#ip add 209.165.100.2 255.255.255.0
ISP(config-if)#no shut down
ISP(config-if)#exit
ISP(config)#interface G0/1
ISP(config-if)#ip add 209.165.200.2
% Incomplete command.
ISP(config-if)#ip add 209.165.200.2 255.255.255.0
ISP(config-if)#no shut down
ISP(config-if)#exit
ISP(config)#ip route 192.168.1.0 255.255.255.0 209.165.100.1
ISP(config)#ip route 192.168.3.0 255.255.255.0 209.165.200.3
ISP(config)#
```

Figure III.5 : Configuration des interfaces.

- **IP route pour le routeur R1 :**

```
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
```

Figure III.6 : Configuration IP route pour R1.

- **IP route pour le routeur R3 :**

```
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#
```

Figure III.7 : Configuration IP route pour R3.

d. Vérification et activation de la licence de sécurité :

L'étape suivante c'est la vérification et l'activation de la configuration.

- **Vérification :**

```
ISP>ena
Password:
ISP#show version
```

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
data          None          None          None

Configuration register is 0x2102
```

Figure III.8 : Vérification de la licence de sécurité.

- **Activation :**

```
ISP#
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#license boot module c1900 technology-package securityk9
```

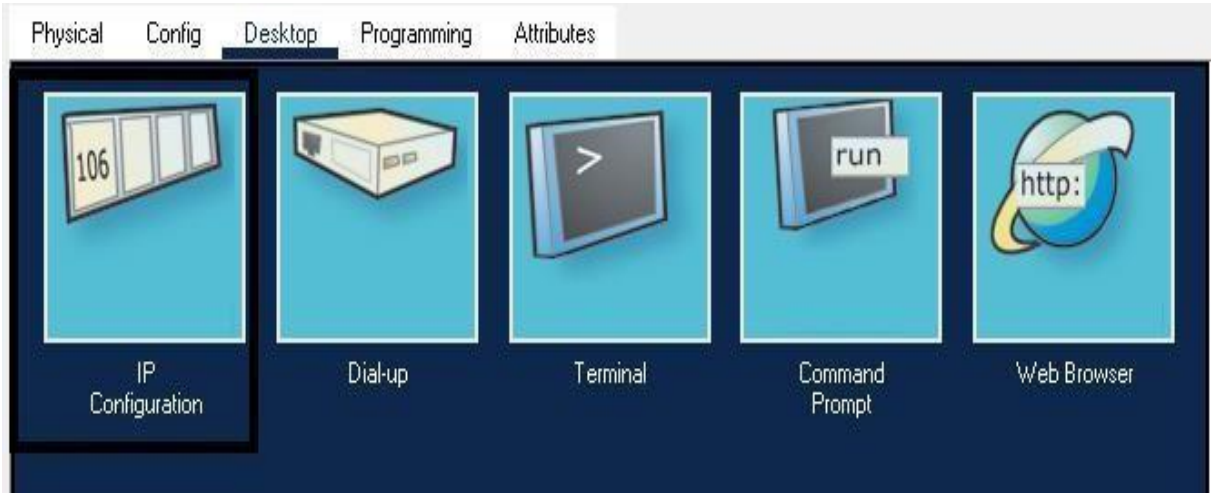
```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None
```

Figure III.9 : Activation de la licence de sécurité.

III.3.3.2. Configuration des PCs :

Après la configuration des routeurs, on passe à la configuration des terminaux (PCs).



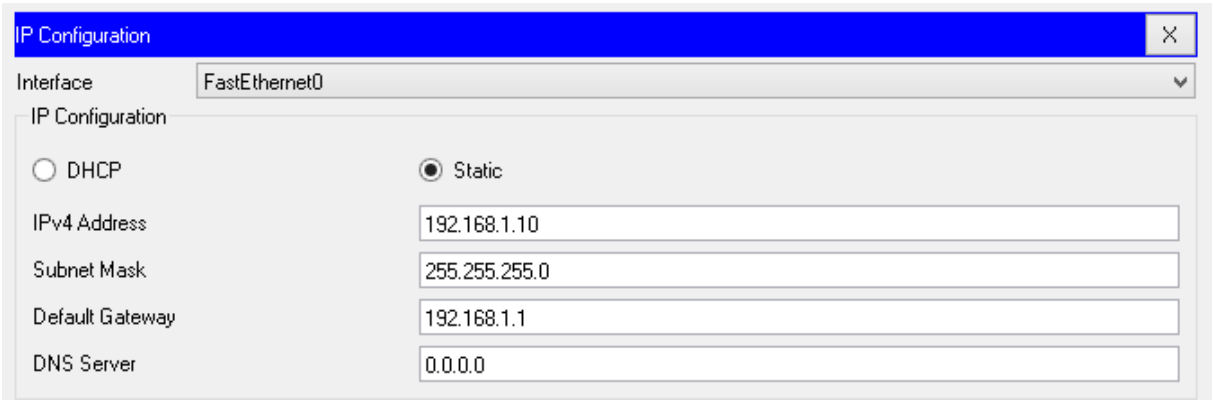


Figure III.10 : Configuration des PCs.

III.3.3.3. Configuration de l'IPsec sur les routeurs R1 et R3 :

Pour configurer IPsec sur les deux routeurs on passe par cinq étapes :

- Configuration des ACL (permettent de filtrer les accès entre les différents réseaux ou de filtrer les accès au routeur lui-même.)
- Configuration des ISAKMP policy (phase 1) ISAKMP key.
- Configuration des propositions IPsec.
- Configuration de la crypto map.
- Application de la crypto map sur l'interface G0/0.

a. Configuration des ACL (Access Control List) :

- **ACL (Access Control List) :** L'ACL a pour but d'avoir une fonction de filtrage, prenant en compte l'historique de la connexion en cours, afin de ne pas accepter le trafic qui n'est pas demandé à partir d'une zone spécifique. L'ACL réseau semble toujours exister sur le routeur, elle est rarement configurée ou non affichée, elle sert principalement à filtrer les paquets sur l'interface physique.

➢ Pour R1 :

```
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```

Figure III.11 : Configuration ACL pour R1.

➢ **Pour R3 :**

```
R3>ena
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

Figure III.12 : Configuration ACL pour R3

b. Configuration des ISAKMP policy et ISAKMP key : (R1 et R3)

Afin de configurer et de crypter les connexions, on utilise la commande de **crypto isakmp policy**.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakkmp key secretlkey address 209.165.200.1
                      ^
% Invalid input detected at '^' marker.

R1(config)#crypto isakmp key secretlkey address 209.165.200.1
A pre-shared key for address mask 209.165.200.1 255.255.255.255 already exists!
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure III.13 : Configuration des ISAKMP policy et ISAKMP key

c. Configuration des propositions IPsec :

- **Pour R1 :**

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#crypto ipsec transform-set R1->R3 esp-aes 256 esp-sha-hmac
```

Figure III.14 : configuration des propositions IPsec pour R1.

- **Pour R3 :**

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-sha-hmac
```

Figure III.15 : Configuration des propositions IPsec pour R3.

d. Configuration de la crypto map :

A l'aide de la commande « **crypto map** », on a créé la crypto-map.

- **Pour R1 :**

```
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set transform-set R1->R3
R1(config-crypto-map)#match adress 100
                              ^
% Invalid input detected at '^' marker.

R1(config-crypto-map)#match address 100
```

Figure III.16 : Configuration de la crypto map pour R1.

- **Pour R3 :**

```
R3(config)#crypto ipsec transform-set R3->R1 esp-aes 256 esp-sha-hmac
R3(config)#
R3(config)#crypto map map IPSEC-MAP 10 ipsec-isakmp
                          ^
% Invalid input detected at '^' marker.

R3(config)#
R3(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs group
% Ambiguous command: "set pfs group"
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#match address 100
```

Figure III.17 : Configuration de la crypto map pour R3.

e. Application de la crypto map sur l'interface G0/0 : (R1 et R3)

```
R1(config)#int g0/0
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure III.18 : Application de la crypto map sur l'interface G0/0 : (R1 et R3)

III.4. Test de connectivité :

Pour vérifier le bon fonctionnement de différents réseaux via les VPNs, nous effectuons un tests de connectivité. Le test se fait par l'envoie de la commande "ping" depuis le site principal vers les autres sites.

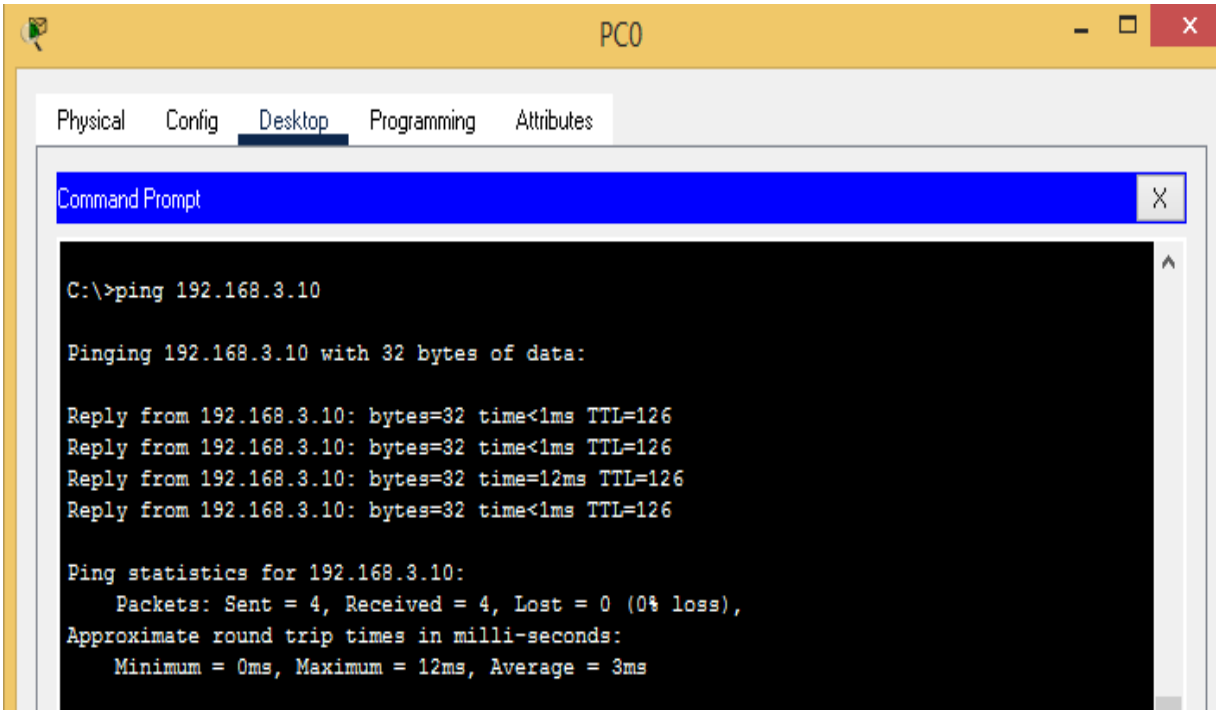


Figure III.20 : Test de connectivité 1

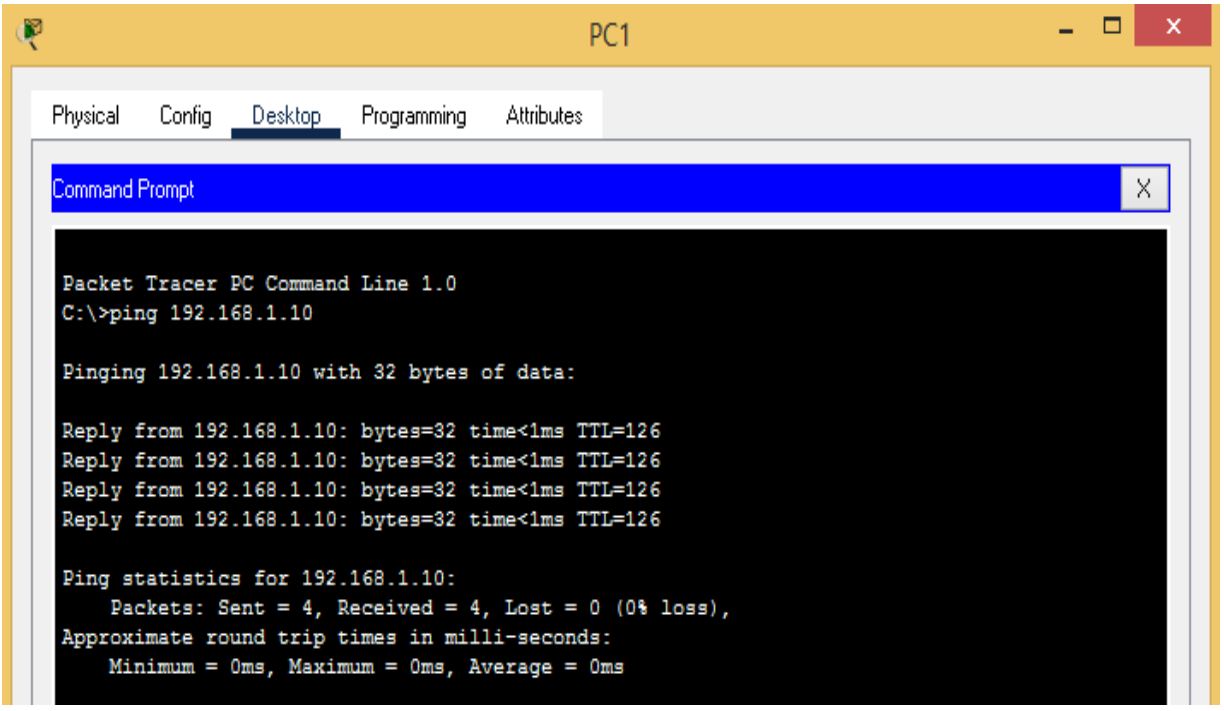


Figure III.20 : Test de connectivité 2.

```
R3#show crypto isakm sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
209.165.100.1   209.165.200.1   QM_IDLE           1023    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
209.165.200.1   209.165.100.1   QM_IDLE           1098    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Figure III.21 : Vérification du statut d'ISAKMP pour R1 et R3.

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
```

```
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #5 (1536 bit)
        lifetime:                86400 seconds, no volume limit
```

Figure III.22 : Vérification d'ISAKMP policy pour R1 et R3.

```
R1#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: IPSEC-MAP, local addr 209.165.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 209.165.200.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
```

```
R3#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: IPSEC-MAP, local addr 209.165.200.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 209.165.100.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

Figure III.23 : Vérification d'IPsec pour R1 et R3.

```
R1#show crypto map
Crypto Map IPSEC-MAP 10 ipsec-isakmp
        Peer = 209.165.200.1
        Extended IP access list 100
            access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
        Current peer: 209.165.200.1
        Security association lifetime: 4608000 kilobytes/86400 seconds
        PFS (Y/N): Y
        Transform sets={
                R1->R3,
        }
        Interfaces using crypto map IPSEC-MAP:
                GigabitEthernet0/0
```

Figure III.24 : Vérification de la crypto map.

A partir des tests ci-dessus, on remarque que les informations importantes et détaillées ainsi que les adresses du réseau local, sont transportées sans erreur ce qui confirme le bon fonctionnement de la solution VPN proposée.

III.5. Conclusion :

Dans ce chapitre nous avons élaboré et réalisé notre architecture VPN proposée. Nous avons procédé à la configuration des différents équipements et des protocoles qui doivent être effectués d'une manière correcte et sécurisée en utilisant le protocole IPSec. La mise en place de cette solution est faite à l'aide du simulateur « Cisco Packet Tracer ». A la fin, et pour démontrer le bon fonctionnement de la liaison, nous avons effectué différents tests de validation des configurations.

Conclusion Générale

Le secteur des technologies de l'information est en évolution, le présent travaille rapporte les résultats obtenus lors de la création d'un réseau VPN. Grâce à cette nouvelle technologie les employés peuvent partager leurs données en toutes sécurité via le protocole IPsec.

Tout d'abord, nous avons divisé notre travail en trois chapitre, le premier était des les généralité sur les réseaux informatiques, et le deuxième sur la sécurité de l'information les VPN (Virtual Private Network) le fonctionnement, les protocole necessaire pour la réalisation des réseaux vpn, le troisième et derniers chapitre sur la réalisation de notre projet .

En effet, la mise en oeuvre de VPN permet aux réseaux privés de s'étendre et de se relier à travers internet en toute sécurité et aussi cette dernière nous aide à réduire les couts liés à l'infrastructure réseau des entreprises.

Ce travail a fait l'objet d'une expérience intéressante, de plus nous avons enrichi nos connaissances déjà acquises dans plusieurs domaines dont de la sécurité informatique notamment la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau privé virtuel.

Références bibliographiques

1. Ouvrage

[1]Philippe Atelin, " Réseaux informatiques: Notions fondamentales ", 3e édition, ENI editions, p-408, 2009.

[3]Andrew Tanenbaum, "Les réseaux ", 3e édition, Interedition , p-795, 1997.

[8] Rafael Corvalan, Ernesto Corvalan, Yoann Le Corvic, "Les VPN : Principes, conception et déploiement des réseaux privés virtuels", 2iéme édition, Dunod, p-332, 2005.

3. Thèse

[7]Tinhinan RAHMANI, Fadhila SADAOUI, "Etude et mise en place d'un réseau VPN", Master spécialisté réseaux et télécommunication, Faculte du génie electrique et informatique, Université Mouloud Mammeri, TIZI OUZOU, Algérie, 2016.

4. Communication

[9]David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J.Alex Halderman,Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin et Paul Zimmermann, "Imperfect Forward Secrecy", How Diffie-Hellman Fails in Practice, Denver, Octobre 2015, DOI:10.1145/2810103.2813707, 2015.

5. Références bibliographiques électroniques

[2]https://www.memoireonline.com/ consulté le 15/05/2021.

[4] https://cisco.goffinet.org/ consulté le 26/05/2021.

[5] https://www.frameip.com/ consulté le 30/05/2021.

[6] https://wikipédia.com/ consulté le 18/06/2021.

[10] https://cisco.com/ consulté le 28/09/2021

ملخص

في الأزمنة الحديثة، يعد أمان البيانات معلمة مهمة جدًا للتشغيل السليم لأي شبكة كمبيوتر. هذا هو السبب في أن المهندسين في هذا المجال يجب أن يضعوا آليات وبروتوكولات أكثر قوة وكفاءة في الإدارة لحماية شبكاتهم. في هذا السياق ، قمنا بدراسة تقنية VPN التي تسمح لمستخدمي ومسؤولي أنظمة المعلومات بالاستفادة من نفس شروط الاستخدام والتشغيل والأمن مثل الشبكات الخاصة عبر الشبكات العامة. تتيح هذه التقنية الجديدة للمستخدمين الوصول عن بعد إلى شبكة خاصة لمشاركة بياناتهم بشكل سري من خلال بروتوكول آمن ، وهو أداة تنفيذ VPN الرئيسية. في هذا المشروع ، استخدمنا Packet Tracer لإنشاء شبكات VPN من موقع إلى مواقع متعددة ، بناءً على بروتوكول IPSec في وضع النفق الخاص به.

الكلمات المفتاحية: الأمن ، VPN ، النفق ، IPsec ، تتبع الحزمة.

Résumé

En ces temps modernes la sécurité des données est un paramètre très important pour le bon fonctionnement de tout réseau informatique. C'est la raison pour laquelle les ingénieures du domaine devraient mettre en place une gestion, des mécanismes de sécurité et des protocoles plus robustes et efficaces pour protéger leurs réseaux. Dans ce contexte nous avons étudié la technologie VPN qui permet aux utilisateurs et administrateurs de systèmes d'information de bénéficier des mêmes conditions d'utilisation, de fonctionnement et de sécurité que les réseaux privés via les réseaux publics. Cette nouvelle technologie permet aux utilisateurs d'accéder à distance à un réseau privé afin de partager leurs données de manière discrète grâce à un protocole sécurisé, qui est le principal outil de mise en œuvre VPN. Dans ce projet, nous avons utilisé Packet Tracer pour la création de VPNs site à plusieurs sites, et ce en se basant sur le protocole IPSec dans son mode tunnel.

Mots clés : sécurité, VPN, Tunnel, IPsec, packet tracer

Abstract

In recent years, data security is a crucial parameter for the proper functioning of any computer network. For these purposes, engineers in the field should put more robust and efficient management, security mechanisms and protocols to protect their networks. In this context, we have studied VPN technology which allows users and administrators of information systems to benefit from the same conditions of use, operation and security as private networks via public networks. This new technology allows users to remotely access a private network to share their data discreetly through a secure protocol, the primary VPN implementation tool. In this project, we used Packet Tracer to create site-to-multiple-site VPNs, based on the IPSec protocol in its tunnel mode.

Keywords: security, VPN, Tunnel, IPsec, packet tracer