REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE YAHIA FARES DE MEDEA



Faculté de **T**echnologie

Mémoire de fin d'études de Master

Département : **Génie électrique**
Filière : **Automatique et Systèmes**

Creation des VPN pour la cyber sécurité des systemes industriels

---

Présenté par :

BENKHAOUA Hamza

HAMADOU Billel

Proposé et Dirigé par :

Dr ABBADI Amel

Mme AMRI Amel

Promotion 2020

Remerciement :

Nos premiers remerciements s'adressent à Dieu le tout puissant, qui nous a permis d'avoir la santé, le courage et la volonté de mener à bien ce travail.

Nous tenons aussi à remercier notre encadreuse **Dr ABBADI Amel**, et co-encadreuse **Madame AMRI Amel** qui *nous ont aimablement orientés et assidument dirigés notre travail et* qui ont été présentes à tout moment de la réalisation de ce projet et surtout sans laquelle ce modeste travail n'aurait jamais vu le jour, ainsi que les membres du jury pour l'intérêt qu'ils ont portés à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Nous remercions également tous les professeurs qui ont contribués de près ou de loin à notre formation universitaire, sans oublier toute personne qui nous ont aidés à mener à terme notre projet.

Merci à tous.

ملخص :

يعد تأمين الاتصالات بين مختلف مستخدمي الشبكة أحد العناصر الأساسية للأمن السيبراني التي يجب ضمانها،لاسيما في حالة نقل البيانات بين الوحدات الصناعية المختلفة لشركة ما.

تحقيقا لهذه الغاية , تقدم هذه الأطروحة حلا يعتمدعلى الشبكات الخاصة الافتراضية VPN من موقع إلى موقع.

و خلال هذا العمل ،كان من الضروري إجراء دراسة نظرية حول أساسيات شبكات الكمبيوتر و الأمن السيبراني والشبكات الافتراضية الخاصة. قبل إنشاء نفق VPN باستعمال برنامج Cisco Packet Tracer ،من أجل تأمين نقل البيانات بين شبكتين محليتين باستخدام بروتوكول IPsec .

كلمات مفتاحية :الشبكة, الأمن السيبراني, الشبكات الخاصة الإفتراضية, نفق, أمن بروتوكول الإنترنت.

Abstract:

Securing communications between different network users is one of the basic elements of cyber security which must be guaranteed, especially in the case of data transmission between different industrial units of a company.

For that, this thesis presents a solution based on a site-to-site virtual private networks VPNs. During this work, it was necessary to do a theoretical study about computer networks, cyber security and virtual private networks before creating a VPN tunnel using Cisco Packet Tracer program, in order to secure data transmission between two local networks using the IPsec protocol.

Key words: Network, Cybersecurity, Virtual Private Networks, Tunnel, IPsec.

Résumé :

La sécurisation des communications entre les différents utilisateurs d’un réseau est l'un des éléments de base de la cybersécurité qui doit être assuré, notamment dans le cas de transmission de données entre différentes unités industrielles d'une entreprise.

Pour cela, ce mémoire présente une solution basée sur les réseaux privés virtuels VPN site à site. Au cours de ce travail, il a été nécessaire de mener une étude théorique sur les réseaux informatiques, la cybersécurité et les réseaux privés virtuels avant de créer un tunnel VPN en utilisant l’environnement Cisco Packet Tracer, afin de sécuriser la transmission de données entre deux réseaux locaux à l'aide du protocole IPsec.

Mots clés : Réseau, cybersécurité, Réseaux Privés Virtuels, Tunnel, IPsec.

Liste des abréviations :

A

ACL : Access Control List
AH : Authentification Header

C

CLI : Commande Langage Interface

D

DTP : Dynamic Trunking Protocol

E

ESP : Encapsulation Security Payload

F

FTP : File Transfert Protocol

I

IPSec : Internet Protocol Security
IP : Internet Protocol
IKE : Internet Key Exchange

L

LAN : Local Area Network
LLC : Logical Link Control
L2TP : Layer 2 Tunneling Protocol
L2F : Layer 2 Forwarding

M

MAC : Media Access Control
MAN : Métropolitains Area Network
MPLS : Multi Protocol Label Switching

O

OSI : Open Systems Interconnection

P

PPP : Point To Point Protocol
PPTP : Point-to-Point Tunneling Protocol
PSK : Pre-shared Key

Q

QOS : Quality Of Service

T

TLS : Transport Layer Security
TCP : Transmission Control Protocol

V

VLAN : Virtuel Local Area Network
VPN : Virtual Private Network

W

WAN : Wide Area Network

Liste des figures :

Page

Chapitre 1 :

Figure 1.1: Topologie en bus……..5

Figure 1.2: Topologie en étoile……...5

Figure 1.3 : Topologie en anneau……...5

Figure 1.4 : Modèle OSI……..7

Figure 1.5 : La communication entre les périphériques finaux……...7

Figure 1.6 : Modèle TCP/IP……9

Figure 1.7 : Pare-feu……...12

Figure 1.8 : ACL……13

Figure 1.9 : Proxy……...15

Figure 1.10: Les VLANs……16

Figure 1.11: VPN……16

Chapitre 2 :

Figure 2-1 : Encapsulation des paquets IP……...18

Figure 2.1 : Exemple d'un VPN site à site……19

Figure 2.3 : Exemple d'un VPN poste à site……20

Figure 2.4 : Exemple d'un VPN poste à poste……..21

Figure 2.5 : Exemple d'emploi d'IPsec entre deux sites distants……...26

Figure 2.6 : Utilisation d'ESP en mode transport……...28

Figure 2.7 : Utilisation d'AH en mode transport……28

Figure 2.8 : Utilisation d'ESP en mode tunnel……29

Figure 2.9 : Utilisation d'AH en mode tunnel……..29

Chapitre 3 : Page

Figure 3.1 : Logo de logiciel Packet Tracer……..31

Figure 3.2 : Architecture du réseau sous Packet Tracer…….32

Figure 3.3 : Interface CLI……..33

Figure 3.4 : Exemple de configuration de Hostname sur le routeur 1…….34

Figure 3.5 : Configuration des interfaces du routeur R1……..35

Figure 3.6 : Configuration des interfaces du routeur R2……..35

Figure 3.7 : Configuration des interfaces du routeur R3……..36

Figure 3.8 : Configuration d'adresse IP pour PC-A……..36

Figure 3.9 : Configuration d'adresse IP pour PC-C……..36

Figure 3.10 : Exemple de configuration de la fréquence d'horloge sur R1…….37

Figure 3.11 : Exemple de désactivation de la recherche DNS sur R1……..37

Figure 3.12 : Configuration du protocole de routage OSPF sur le routeur R2……..37

Figure 3.13 : Configuration du protocole de routage OSPF sur le routeur R1……..38

Figure 3.14 : Configuration du protocole de routage OSPF sur le routeur R3……..38

Figure 3.15 : Exemple de configuration des modes console et vty sur le routeur R2…39

Figure 3.16 : Résultat de vérification de connectivité entre PC_A et PC_C……..40

Figure 3.17 : Résultat de vérification de connectivité entre R1 et R3……40

Figure 3.18 : Activation du protocole ISAKMP sur R1……...41

Figure 3.19 : Création d'une politique de négociation de clés sur le routeur R1……...41

Figure 3.20 : Création d'une politique de négociation de clés sur le routeur R3……...42

Figure 3.21 : Création de la clé pré-partagée sur le routeur R1……..42

Figure 3.22 : Création de la clé pré-partagée sur le routeur R3……..42

Figure 3.23 : Configuration de la trasform-set sur R1…….43

Figure 3.24 : Définition de la durée de vie de la clé pré-partagée……43

Figure 3.25 : création d'ACL sur R1……...44

Figure 3.26 : Création d'ACL sur R3……..44

Figure 3.27 : Création de la crypto-map sur R1…….45

Figure 3.28 : Création de la crypto-map sur R3…….46

Figure 3.29 : Application de la crypto-mapà l'interface appropriée sur R1……46

Page

Figure 3.30 : Application de la crypto-map à l'interface appropriée sur R3……...47

Figure 3.31: Test de transfert des données……..47

Figure 3.32 : Exécution de la commande Ping étendu……48

Figure 3.33 : Vérification de la « transform-set »…….…….48

Figure 3.34 : Vérification de la crypto-map……...49

Figure 3.35 : Vérification des paramètres d'IPsec……50

Figure 3.36 : Vérification des opérations ISAKMP……...50

Liste des tableaux :

Page

Chapitre 3

Tableau 3.1 : Table d'adressage des dispositifs utilisés……32

Table des matières :

Page

Introduction Générale…….....1

CHAPITRE 1 : GENERALITES SUR LES RESEAUX ET LA CYBER SECURITE DES RESEAUX

1.1 Introduction……3

1.2 Les réseaux informatiques…….3

1.2.1 Définition d'un réseau…….3

1.2.2. Classification des réseaux…….....3

1.2.2.1 Les réseaux locaux : Local Area Network (LAN)……..3

1.2.2.2 Les réseaux étendus : Wide Area Network (WAN)……..4

1.2.2.3 Les réseaux intermédiaires : Metropolitains Area Network (MAN)……...4

1.2.3 Caractéristiques des réseaux……..4

1.2.3.1 Les supports de transmission…….4

1.2.3.2 Les topologies d'un réseau……..4

1.2.3.3 Réseau fiable…….5

1.2.4 Le modelé de référence OSI……...6

1.2.4.1 Le principe du modèle OSI…….6

1.2.4.2 Rôle des différentes couches……8

1.2.5 Le modèle TCP/IP……...8

1.2.5.1 Présentation du protocole TCP/IP…….8

1.2.5.2 Descriptions du modèle TCP/IP…….9

1.3 La cyber sécurité……...10

1.3.1 Objectifs du cyber sécurité……10

1.3.1.1 L'authentification……10

1.3.1.2 L'intégrité…….10

1.3.1.3 La confidentialité……..11

Page

1.3.1.4 La disponibilité ……..11

1.3.1.5 La non-répudiation……11

1.3.2 Terminologie du cyber sécurité……...11

1.3.2.1 Vulnérabilité……...11

1.3.2.2 Menace……11

1.3.2.3 Risque……..11

1.3.2.4 Attaque……11

1.3.3 Solutions de sécurité……..11

1.3.3.1 Pare-feu……...11

1.3.3.2 Les listes de contrôles d'accès (ACL)……...12

1.3.3.3 Proxy……14

1.3.3.4 Les VLAN……15

1.3.3.5 Les VPNs……..16

1.4 Conclusion……..17

CHAPITRE 2 : GENERALITES SUR LES VPNs

2.1 Introduction……...18

2.2 Définition d'un VPN…….18

2.3 Typologie des VPNs……..19

2.3.1 VPN d'entreprise……19

2.3.1.1 Les différents types de VPNs d'entreprise……19

2.3.1.2 Avantages et inconvénients du VPN entreprise……...21

2.3.2 VPN operateur……22

2.3.2.1 Caractéristiques du VPN operateur site à site…….22

2.3.2.2 Avantages et inconvénients du VPN operateur……22

Page

2.4 Principaux protocoles…….23

2.4.1 Niveau 2……23

2.4.1.1 PPTP (Point to Point Tunneling Protocol)…….23

2.4.1.2 L2F (Layer 2 Forwarding)……...23

2.4.1.3 L2TP (Layer 2 Tunneling Protocol)……23

2.4.2 Niveau 2 et 3……..23

2.4.2.1 MPLS (Multi Protocol Label Switching)…….23

2.4.2.2 Fonctionnalité…….24

2.4.2.3 Principe MPLS……...24

2.4.3 Niveau 3……..25

2.4.3.1 SSL/TLS……..25

2.4.3.2 SSH……..25

2.4.3.3 IPSEC …….25

2.5 Conclusion……30

CHAPITRE 3 : CONFIGURATION ET TESTS

3.1 Introduction……...31

3.2 Packet Tracer……31

3.3 Architecture du réseau…….31

3.3 Table d'adressage……..32

3.4 Configuration……33

3.4.1 Configuration de base……...34

3.4.1.1 Configuration de Hostnames……..34

3.4.1.2 Configuration des adresses IP et MAC……34

3.4.1.3 Configurez une fréquence d'horloge……37

3.4.1.4 Désactivation de la recherche DNS……..37

3.4.1.5 Configuration de protocole de routage……37

Page

3.4.1.6 Configuration des mots de passe pour les modes console et vty……39

3.4.1.7 Vérification de la connectivité……...40

3.4.2 Configuration de VPN site à site……..40

3.5 Vérification du tunnel VPN…….47

3.5.1 Test de transfert des données……...47

3.5.2 Exécution de la commande Ping étendu…….48

3.5.3 Vérification de la méthode de cryptage des données « transform-set » ……..48

3.5.4 Vérification de la crypto-map……..49

3.5.5 Vérification des paramètres d'IPsec……49

3.5.6 Vérification des opérations ISAKMP……..50

3.6 Conclusion…….51

Conclusion Générale……..52

Introduction Générale

INTRODUCTION GENERALE

Depuis très longtemps l'humanité a rêvée d'un monde communicant sans frontières où la possibilité n'a pas de limite. C'est de ces besoins que l'informatique est créée. Cette science utilise des machines appelées automates, calculateurs, ordinateurs, formant entre eux des ensembles complexes dites systèmes informatiques.

L'évolution de la technologie qui a accompagnée l'apparition de ces équipements a créé d'autre besoin. De là les réseaux informatiques sont apparues pour la première fois en 1960 comme un moyen qui relie ces équipements entre eux, et qui couvre le besoin de partage d'informations et de données entre les différents périphériques d'un réseau.

Les réseaux doivent répondre aux exigences de fiabilité. Cela signifie que le réseau doit être tolérant aux pannes, évolutif. Il peut fournir la qualité de service attendue et assurer la sécurité des informations et des ressources. Donc il est nécessaire de prend en considération les menaces et des failles de sécurité potentielles lors de la mise en œuvre d'un réseau.

Mais le grand bond que les systèmes d'information ont fait c'était avec l'apparition d'internet, le plus grand réseau existant. Ce nouveau terme qui signifie "réseau de réseaux"offre un grand éventail de possibilités, les réseaux n'étaient plus limités, ils pouvaient enfin communiquer entre eux. Les réseaux et l'internet ont modifié notre façon de communiquer, d'apprendre, de travailler et de nous divertir. La nécessité de les utiliser était devenue plus qu'indispensable.

Pour les entreprises comme pour les individus, l'internet est présenté comme un outil dans le monde virtuel. Or l'utilisation de cette dernière n'est pas sans danger puisque l'échange d'information, via ce grand réseau peut être intercepté. Ce qui crée un risque de modification ou de vol d'information, dont il peut provoquer un mauvais impact sur plusieurs niveaux d'une entreprise.

Aujourd'hui, la capacité de communication via un réseau sécurisé est devenue un élément essentiel pour la continuité des systèmes d'informations d'une entreprise quelle que soit son domaine d'activité, sa taille et sa répartition géographique. Pour cela des politiques du cyber sécurité ont été misent en place. Parmi elles, les VPNs qui offrent un moyen d'échange d'information d'une manière sécurisée à travers un réseau public.

Dans le présent mémoire, nous présenterons la relation entre les réseaux et le cyber sécurité et nous montrons les étapes que nous avons suivies pour réaliser une connexion via un VPN, comme une des solutions proposées pour la communication sécurisée entre deux entités.

Structuré en trois chapitres, ce mémoire est organisé comme suit :

Chapitre 1 : Intitulé << **Généralités sur les réseaux et la cyber sécurité** >> où nous présenterons quelques concepts de base des réseaux informatiques, et certaines notions sur la cyber sécurité.

Chapitre 2 : Intitulé << **Généralités sur les VPNs** >> ou nous essayons de définir le concept des VPNs et de présenter les différents protocoles qui y sont utilisés.

Chapitre 3 : intitulé << **Configuration et Tests** >> ou nous faisons les configurations nécessaires au niveau des routeurs et périphériques finaux afin de créer un tunnel VPN.

Nous terminons notre travail par une conclusion sur l'ensemble de cette étude et nous donnons quelques perspectives qui ont pu être dégagées à la lumière de notre étude et des résultats obtenus.

Chapitre 1 : Généralités sur les réseaux et la cyber sécurité

CHAPITRE 1 :

GENERALITES SUR LES RESEAUX

ET

LA CYBER SECURITE DES RESEAUX

1.1 Introduction :

Dans le cadre de ce mémoire, nous nous intéressons à la sécurité des systèmes industriels.
Plus spécialement à la création des réseaux virtuels privés (Virtual Private Network *abrégé* en anglais VPN). Nous allons commencer par expliquer le fonctionnement des réseaux, et définir certains concepts de base du cyber sécurité.
Nous avons divisé ce premier chapitre en deux grandes parties. Dans la première, nous allons essayer d'approcher les notions des réseaux informatiques, ces caractéristiques, le modèle OSI ainsi que du modèle TCP/IP, puis dans la deuxième partie nous allons passer à la cyber sécurité, ses objectifs, son impact sur les réseaux et leurs utilisations.

1.2 Les réseaux informatiques

Dans cette première partie, nous allons définir quelques notions sur les réseaux informatiques.

1.2.1 Définition d'un réseau

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou de personnes connectés ou maintenus en liaisons et dont le but est d'échanger des informations ou des biens matériels [1].

Un réseau informatique est un ensemble des éléments physique ou des périphériques de communications liés entre eux par des supports au but de partager l'information.

1.2.2. Classification des réseaux

Les différents types des réseaux connus sont variés en fonction de la taille de la zone couverte, le nombre d'utilisateurs connectés, la vitesse de transfert d'information, aussi bien que le nombre et les types des services disponibles sur un tel réseau.

1.2.2.1 Les réseaux locaux : Local Area Network (LAN)

Les LANs sont des réseaux qui relient un groupe de périphériques finaux, couvrent un espace limité et peu étendue, ils possèdent un seul gestionnaire et fournissent une bande passante très élevée.

1.2.2.2 Les réseaux étendus : Wide Area Network (WAN)

Réseau étendu: interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.
Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.

1.2.2.3 Les réseaux intermédiaires : Metropolitains Area Network (MAN)

Les MANs sont des réseaux qui couvrent une zone assez large qu'un LAN, mais moins étendue qu'un WAN. Généralement, c'est les grandes entreprises qui administrent ce type de réseau.

1.2.3 Caractéristiques des réseaux :

Un réseau est caractérisé par sa topologie, les médias (support) de transmission et son degré de fiabilité.

1.2.3.1 Les supports de transmission :

Ces supports construisent le canal à travers lequel l'information se déplace, nous citons :

a. **Les fils métalliques :** comme le câble coaxial ou torsadé dont l'information est codée en impulsions électriques.
b. **Les fibres de verre (Fibre Optique) :** l'information est transportée autant que des impulsions lumineuses.
c. **Support sans fil :** il utilise les longueurs d'onde de spectre électromagnétique pour codée l'information.

1.2.3.2 Les topologies d'un réseau :

Les topologies d'un réseau fournissent une représentation visuelle des connexions réseau. Il existe deux types de diagrammes de topologie [2] :

a. **Diagramme de topologie logique :** Il donne une identification des périphériques, les ports et les schémas d'adressage.
b. **Diagramme de topologie physique :** Il montre l'emplacement physique des éléments d'un réseau et la manière de câblage utilisée.

Trois topologies physiques sont habituellement connues

- **Topologie en bus :** Dans une topologie en bus tous les périphériques sont connectés à un seul canal de transmission par des câbles intermédiaires.

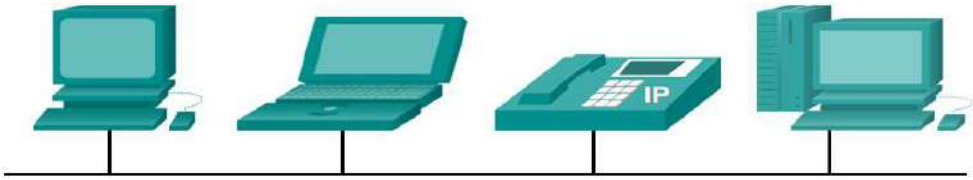


Figure 1.1: Topologie en bus

- **Topologie en étoile :** Selon une topologie en étoile les périphériques sont tous connectés à un périphérique central appelé HUB (Switch) lequel représente un point de jonction à qui les autres périphériques sont connectés.

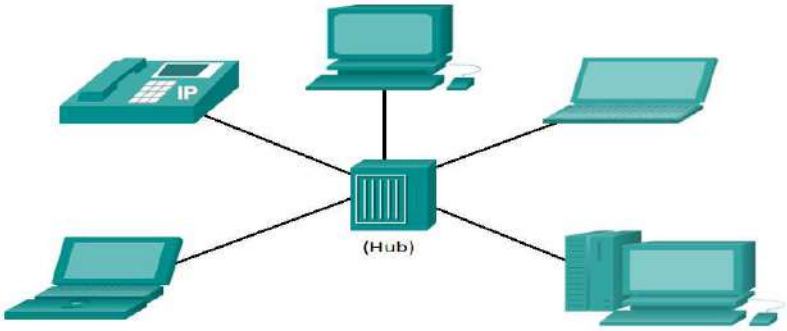


Figure 1.2: Topologie en étoile

- **Topologie en anneau :** Suivant une topologie en anneau les périphériques sont connectés entre eux et à un répartiteur (appelé MAU, Multistation Access Unit), c'est l'élément qui gère le temps de la communication entre les différents périphériques, chacun son tour d'une façon successive et bouclée.

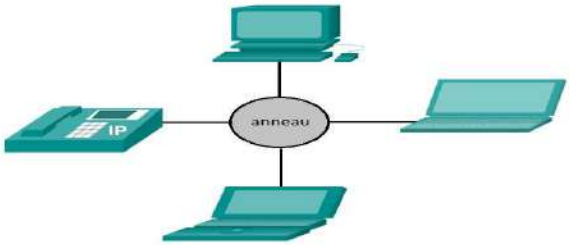


Figure 1.3 : Topologie en anneau

1.2.3.3 Réseau fiable :

L'exécution d'une suite d'applications sur un réseau nécessite qu'il répand aux certains exigences au but de garantir l'ensemble des services adoptés par ce dernier.

Par conséquences un réseau pour qu'il soit fiable, il doit avoir quatre caractéristiques de base :

a. Tolérance aux pannes :

Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes, de telle sorte que le nombre de périphériques affectés soit le plus faible possible. Il est également conçu de façon à permettre une récupération rapide en cas de panne [2].

b. Évolutivité :

Un réseau évolutif est un réseau qui donne la possibilité d'ajouté des utilisateurs supplémentaires et de prendre en charge des nouvelles applications sans perdre des performances des services fournis aux utilisateurs de réseau.

c. Qualité de service (QDS) :

La **qualité de service (QDS)** ou **quality of service (QoS)** est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets….

d. Sécurité :

La sécurité d'une infrastructure réseau repose sur plusieurs points. Elle implique non seulement une sureté des périphériques par une interdiction de tout accès non autorisés mais aussi la disponibilité des données aux utilisateurs confirmés, bien sur sans menace, tout en garantissant que les données ne soient pas modifiées lors d'une opération de transmission.

1.2.4 Le modelé de référence OSI :

Le **modèle OSI** (de l'anglais **O**pen **S**ystems **I**nterconnection) est une norme de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO (**I**nternational **O**rganization for **S**tandardization en français Organisation Internationale de Normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

1.2.4.1 Le principe du modèle OSI :

Le modèle OSI est basé sur 7 couches de communication (figure 1.4.)

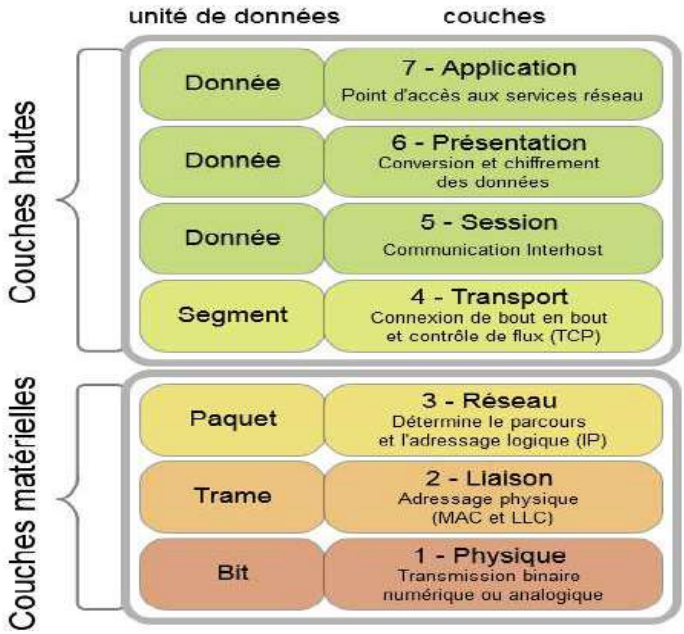


Figure 1.4 : Modèle OSI

- **Exemple de communication entre deux PC**

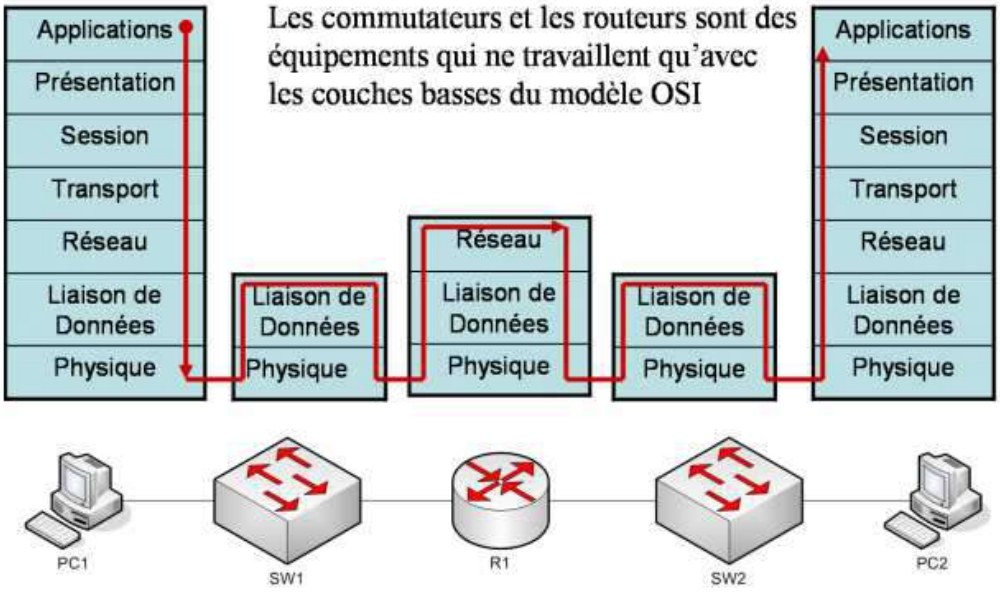


Figure 1.5 : La communication entre les périphériques finaux

L'évolutions de l'information de la couche application a la couche physique se nomme l'encapsulation.

Ce processus est inversé lorsque les données sont arrivées à destination, dans laquelle l'ensemble des changements appliqués sur les trames arrivés est dite désencapsulation.

1.2.4.2 Rôle des différentes couches :

- **La couche physique :** Cette couche se charge de la transmission et la réception des données informatiques au format binaire (0 et 1).
    - ✓ sur une paire de cuivre, c'est un signal électrique qui définit le 0 et un autre signal électrique qui définit le 1.
    - ✓ sur une fibre optique, c'est la lumière envoyée dans la silice qui s'en occupe
    - ✓ sur du sans-fil, …….
- **La couche liaison des données :** Les protocoles de cette couche sont les responsables sur la construction des trames et la gestion d'adressage.
- **La couche réseau** : Cette couche s'intéresse aux données utiles dans la trame et les adresses des périphériques sur le réseau pour assurer l'échange des données entre des périphériques finaux bien identifiés.
- **La couche transport :** Son rôle est de rassembler et segmenter les données pour les préparées à la couche réseau, ainsi qu'elle indique les fautes de transport et les corrigées.
- **La couche session :** Elle s'occupe non seulement de dialogue et la gestion d'échange des données entre les périphériques mais aussi de la sureté de connexion.
- **La couche présentation :** Elle donne une représentation compréhensible des données pour l'utilisateur ainsi que les applications.
- **La couche application :** Cette couche fait l'interface entre l'homme et la machine. Votre browser (firefox, safari,chrome…), votre logiciel de messagerie (outlook, thunderbird…) .....

1.2.5 Le modèle TCP/IP :

C'est au début des années 1970 que le premier modèle de protocole possédant plusieurs couches pour les communications inter-réseau a été créé. Celui-ci est appelé modèle Internet ou encore modèle TCP/IP grâce aux protocoles TCP et IP qui sont les plus dominants dans ce modèle. Il est défini sous la forme de quatre catégories de fonctions ou quatre couches.

1.2.5.1 Présentation du protocole TCP/IP :

Au contraire des protocoles qui sont spécifiques chacun à un fournisseur ou une entreprise, le protocole TCP/IP est une norme ouverte.

- **Le protocole IP (Internet Protocol) :**

Ce protocole permet de gérer l'acheminement des paquets d'une machine à une autre, ainsi que l'adressage.

- **Le protocole TCP (Transmission Control Protocol) :**

TCP est le protocole responsable des données contenues dans les paquets envoyés ainsi que leur ordre de réception. Le protocole TCP exige la confirmation de la réception des données et assure ainsi une fiabilité de communication entre les différentes hôtes du réseau.

En cas de perte de données lors de leur transfert, la retransmission des données perdues est assurée par ce protocole.

1.2.5.2 Descriptions du modèle TCP/IP :

Le modèle TCP/IP contient une suite de quatre couches comme suit (figure 1.6):

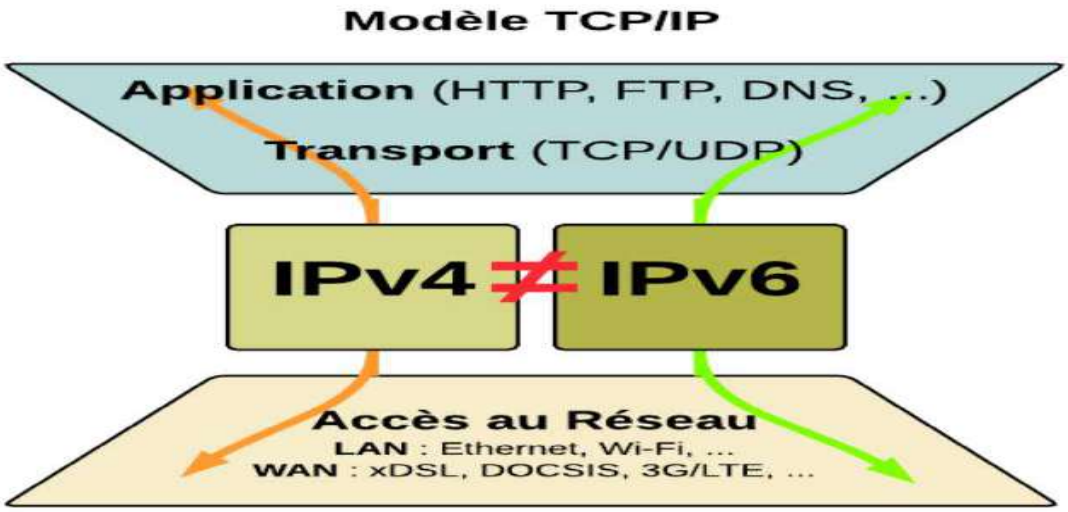


Figure 1.6 : Modèle TCP/IP

- **La couche application :**
  - ✓ Elle est la couche de communication qui s'interface avec les utilisateurs.
  - ✓ Exemples de protocoles applicatifs : HTTP, DNS, DHCP, FTP, …
  - ✓ Elle s'exécute sur les machines hôtes.
- **La couche transport :** Le TCP est un de ses protocoles.
  - ✓ Elle est responsable du dialogue entre les hôtes terminaux d'une communication.
  - ✓ Les applications utiliseront TCP pour un transport fiable et UDP sans ce service.
  - ✓ Les routeurs NAT et les pare-feux opèrent un filtrage au niveau de la couche transport
- **La couche internet :** Parmi ses protocoles elle contient le protocole IP.
  - ✓ Elle permet de déterminer les meilleurs chemins à travers les réseaux en fonction des adresses IPv4 ou IPv6.
  - ✓ Les routeurs transfèrent le trafic IP qui ne leur est pas destiné.
- **La couche accès réseau :**
  - ✓ Le protocole TCP/IP ne s'occupe pas de la couche Accès Réseau

- ✓ Elle organise le flux binaire et identifie physiquement les hôtes
- ✓ Elle place le flux binaire sur les supports physiques
- ✓ Les commutateurs, cartes réseau, connecteurs, câbles, etc. font partie de cette couche

1.3 La cyber sécurité

La cybersécurité englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des données, sensibles ou non, au sein d'une infrastructure numérique. Et cela nécessite d'utiliser des protocoles, des technologies, des périphériques et des programmes permettant de sécuriser les données et de limiter les risques qu'ils soient externes ou internes.

La plus part des menaces externes sont diffusées par internet comme les virus, chevaux de Troie, les logiciels espions et publicitaires, Attaques zero-day, Attaques de pirates et Attaques par déni de service.

Non seulement les menaces externes doivent être prisent en considération lors de la sécurisation d'un réseau mais aussi celles qui sont internes, dont l'expérience montre que la plupart des violations des données est une conséquence principalement d'une malle utilisation à l'intérieur du réseau à cause d'une perte ou d'un vol de périphériques, de la mauvaise utilisation d'un périphérique par un employé ou dans un contexte professionnel, d'un employé malveillant.

Par conséquent, lors d'une création d'une politique de sécurité, il est important de prendre en compte à la fois les menaces externes et internes.

La protection d'un réseau ne consiste pas à utiliser une solution unique pour toutes les menaces existantes. Pour cette raison, plusieurs solutions de sécurité sont appliquées en plusieurs couches, en cas d'une faille au niveau d'un des composants de sécurité d'autres peuvent prendre la relève.

Au niveau des entreprises et afin d'augmenté le degré de sécurité, tous les périphériques du réseau doivent être sécurisés, cela inclut les routeurs, les commutateurs, les périphériques finaux et même les dispositifs de sécurité.

1.3.1 Objectifs du cyber sécurité :

Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger. La sécurité des systèmes d'information vise à assurer les propriétés suivantes:[4]

1.3.1.1 L'authentification : L'identification des utilisateurs est primordiale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

1.3.1.2 L'intégrité : S'assurer que les données ne sont pas altérées de façon fortuite, les éléments considérés doivent être exactes et complets.

1.3.1.3 La confidentialité : Limiter l'accès aux informations qu'aux personnes autorisées.

1.3.1.4 La disponibilité : Garantir le fonctionnement du système sans faille, et l'accès aux services et ressources installées avec le temps de réponse voulu.

1.3.1.5 La non-répudiation : permettant de garantir qu'une transaction ne peut être niée ;

1.3.2 Terminologie du cyber sécurité :

L'ensemble des termes utilisés dans le domaine du cyber sécurité peut se résumer comme suit [5] :

1.3.2.1 Vulnérabilité : Une vulnérabilité ou une faille est une faiblesse dans un système ou un logiciel permettant à un attaquant de porter atteinte à la sécurité d'une information ou d'un système d'information.

1.3.2.2 Menace : Ce sont les actions potentiellement nuisibles à un système informatique. Les menaces peuvent être le résultat de plusieurs actions en provenance de plusieurs origines.

1.3.2.3 Risque : Un risque désigne la probabilité d'un événement dommageable ainsi que les coûts qui s'ensuivent, le risque dépend également des montants des valeurs à protéger.

1.3.2.4 Attaque : Une attaque est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant des systèmes et généralement préjudiciables. Et parmi les différentes attaques qui existent on trouve les Virus.

1.3.3 Solutions de sécurité:

Les exigences de sécurité du réseau doivent prendre en compte l'environnement réseau, ainsi que les différentes applications et les exigences informatiques.

Les réseaux domestiques et professionnels doivent pouvoir sécuriser leurs données tout en garantissant la qualité de service attendue de chaque technologie. En outre, la solution de sécurité mise en œuvre doit être capable de s'adapter aux nouvelles tendances et à l'évolution du réseau.

Les composants de sécurité réseau d'un réseau domestique ou d'un réseau de petit bureau doivent inclure, au minimum des antivirus et des logiciels de protection contre les programmes malveillants où leur fonction est d'empêcher la contamination des périphériques finaux par un programme malveillant.

Les réseaux plus étendus et les réseaux des grandes entreprises ont souvent d'autres exigences relatives à la sécurité [2].

1.3.3.1 Pare-feu :

Le pare-feu est une solution de sécurité qui s'occupe des menaces externes, installé entre deux réseaux ou plus. Il sert à gérer le trafic et de contrôler l'accès entre eux, tout en contribuant à interdire les accès non autorisés.

Un pare-feu peut être sous forme de programme installé sur les hots ou encore tout dispositif indépendant installé au bord du réseau et lié aux autre périphériques.

Les pare-feu emploient différentes manières pour autorisé ou interdire les accès à un réseau. Ces méthodes sont les suivantes:

- **Filtrage des paquets :** interdit ou autorise l'accès pour les trames reçus selon les adresses IP ou MAC.
- **Filtrage des applications :** interdit ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de ports.
- **Filtrage d'URL :** interdit ou autorise l'accès à des sites web en fonction d'URL ou de mots clés spécifiques.

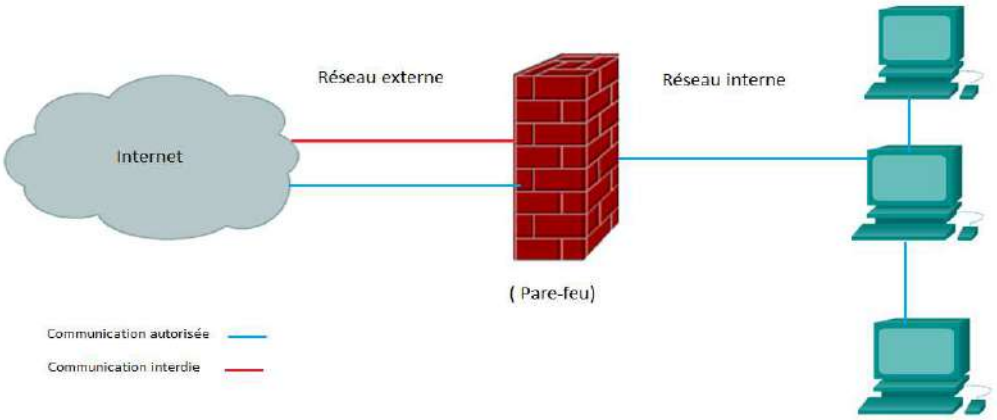


Figure 1.7 : Pare-feu

1.3.3.2 Les listes de contrôles d'accès (ACL) :

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter.

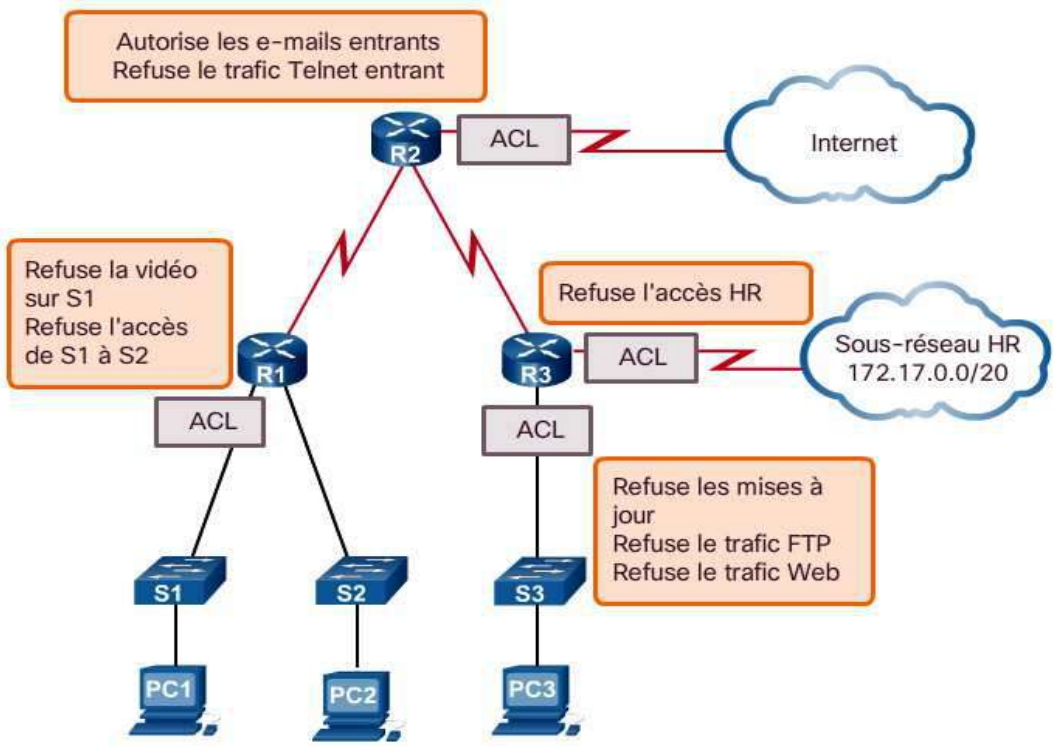


Figure 1.8 : ACL

L'acceptation et 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 [6].

a. L'intérêt d'utiliser des ACL:

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès : [7]

- ✓ Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances.
- ✓ Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée.
- ✓ Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section.

- ✓ Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces du routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- ✓ Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- ✓ Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

b. Les types des listes de contrôle d'accès:

Il existe trois types d'ACL que voici [7] :

- ✓ **Listes de contrôle d'accès standard :** Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.
- ✓ **Listes de contrôle d'accès étendues :** Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.
- ✓ **Listes de contrôle d'accès nommées :** Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

1.3.3.3 Proxy :

Un système mandataire (Proxy) repose sur un accès à l'internet par une machine dédiée: le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales, et exécute les requêtes pour le compte de ces dernières [8].

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (http, FTP, SMTP, etc.) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, etc.).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés [7].

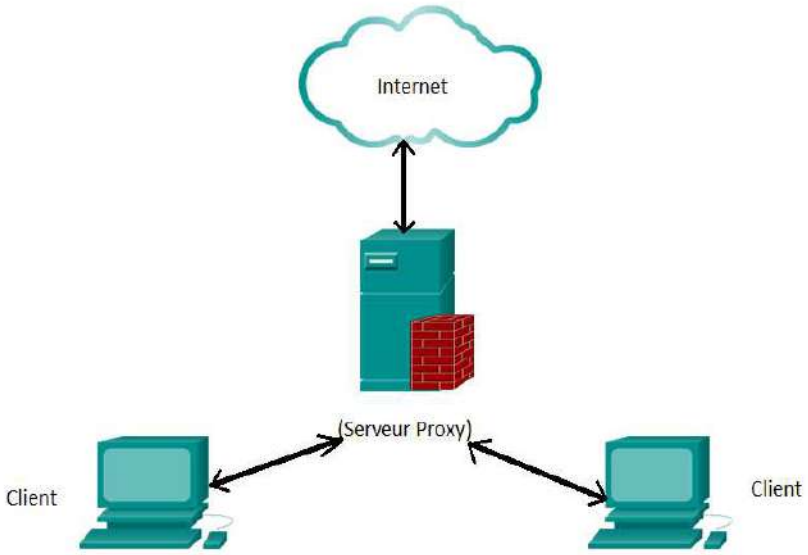


Figure 1.9 : Proxy

1.3.3.4 Les VLAN :

Les VLAN représentent un procédé de regroupement des périphériques dans un LAN d'une manière indépendante de la localisation géographique sur le réseau.

Un VLAN permet aux administrateurs de segmenter le réseau en groupes par rapport à ses fonctions, quel que soit l'emplacement physique des utilisateurs ou des périphériques avec une garantie de communication entre ces dernies comme s'ils étaient sur la même section.

Les VLANs entrainent un certain niveau de sécurité. En effet, les attaques utilisant le broadcast sont contenues au sein d'un VLAN (DHCP spoofing, overflow…). De plus, des règles de sécurité pourront être ajoutées sur les communications entre les VLANs permettant ainsi d'apporter une nouvelle couche de sécurité à la défense en profondeur de l'entreprise.

Par Conséquent les données sensibles seront séparés du reste du réseau ce qui réduit les menaces de violation. Il existe différents types de VLAN tels que:

- **VLAN par port:** Chaque port des commutateurs est configuré pour être affecter à un VLAN.
- **VLAN par adresse:** Chaque adresse MAC représente un VLAN ce qui crée une indépendance par rapport à la localisation géographique.
- **VLAN par protocole:** Dans ce type la segmentation est faite par rapport aux hôtes qui utilisent un protocole similaire ou par mot de passe.

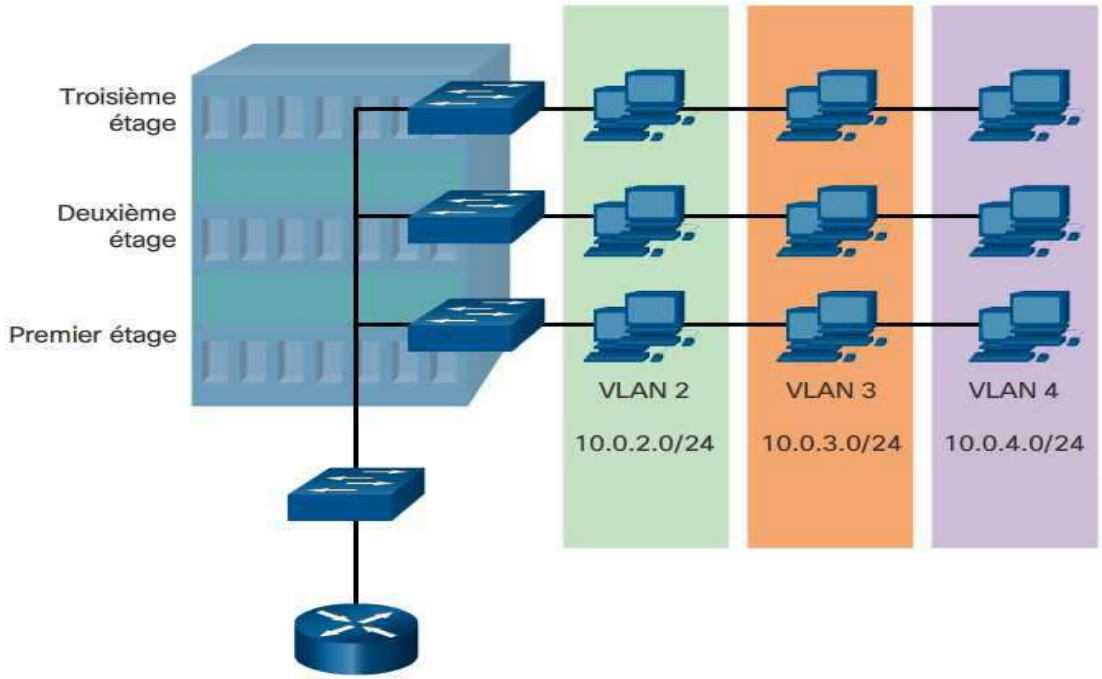


Figure 1.10: Les VLANs

1.3.3.5 Les VPNs :

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers des réseaux peu sûrs comme peut l'être le réseau Internet. Les VPNs ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics [9].

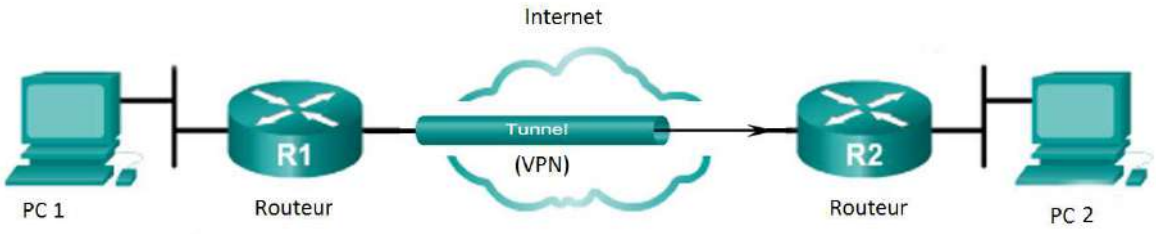


Figure 1.11: VPN

1.4 Conclusion :

Ce chapitre nous a donné l'opportunité en premier lieu de découvrir et de mieux comprendre les concepts de base des réseaux informatiques, où nous avons découvris les modèles OSI et TCP/IP, et en deuxième lieu de comprendre les notions et objectifs du cyber sécurité, où nous avons présenté les différentes politiques sécuritaires, comme les pare-feu, les proxys, les ACLs et surtout les VPNs qu'on va les aborder en détails dans le chapitre suivant.

Chapitre 2 : Généralités sur les VPNs

CHAPITRE 2 :

GENERALITES SUR LES VPNs

2.1 Introduction :

Dans ce chapitre on va d'abord déterminer ce qu'est un VPN (Virtuel Private Network). Ensuite on classifie les VPN suivant leur principe d'utilisation. Enfin nous terminerons en présentant les principaux protocoles utilisés lors de la réalisation d'un VPN.

2.2 Définition d'un VPN :

Un VPN (Virtuel private network) ou RPV en français (Réseau privé virtuel) est un tunnel sécurisé garantissant la communication entre deux entités. Cet échange des données est effectué d'une façon privée au travers des réseaux peu sécurisé comme le réseau internet. Ce qui permet la sécurisation des données sensibles lors de son échange en privé sur un réseau publique.

Durant le fonctionnement de VPN, un tunnel rassemble des paquets IP avec des adresses internes qui sont confiés à un équipement tel qu'un router ou un pare-feu. Celui-ci les envois sur un canal souvent public (internet) à l'extrémité distante. Pour cela, les paquets internes sont encapsulés dans des paquets IP avec des adresses IP public des extrémités destinataire et source. L'équipement distant désencapsule chaque paquet pour remettre sur le réseau des paquets doté des adresses locales source et destination [10].

Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables [7].

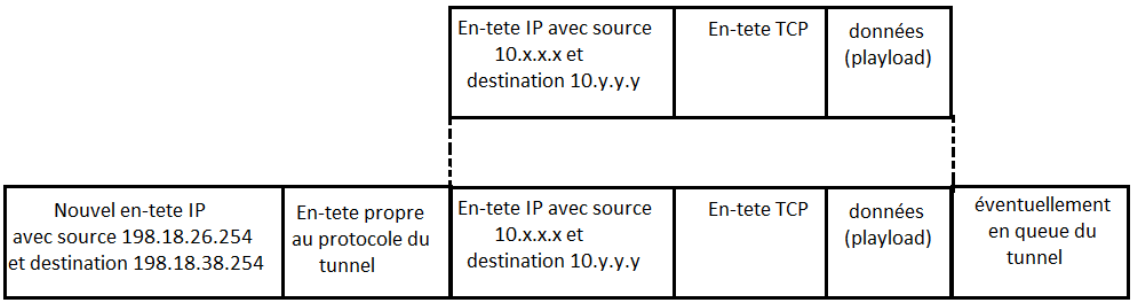


Figure 2-1 : Encapsulation des paquets IP

2.3 Typologie des VPNs :

Il existe deux grandes catégories de VPN : le VPN d'entreprise et le VPN d'opérateur.

Chacune des familles contient des avantages et des inconvenants, ils peuvent exister les deux simultanément au sein d'une même entreprise car elles ne sont pas exclusive l'une de l'autre.

2.3.1 VPN d'entreprise :

Dans ce cas de VPN, l'entreprise est le responsable de contrôle des VPN entre les différents points à l'intérieur de l'entreprise, ainsi qu'entre ses sites situés à l'extérieur de cette dernière.

2.3.1.1 Les différents types de VPNs d'entreprise

Il existe trois types de VPNs d'entreprise

a. VPN site à site :

C'est un des cas les plus fréquents. Il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, ou d'un client. Mais il faut également que tout ou partie des machines des deux réseaux puissent communiquer avec celles du réseau distant en utilisant les adresses privées de chaque réseau.

Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments matériels (routeurs ou pare-feu) situés à la frontière entre le réseau interne et le réseau publique de chaque site. Ce sont ces matériels qui prennent en charge le cryptage, l'authentification et le routage des paquets.

Dans le cas de l'utilisation des matériels spécifiques, des processeurs spécialisés peuvent prendre en charge la partie cryptographique la plus consommatrice de ressources CPU [10].

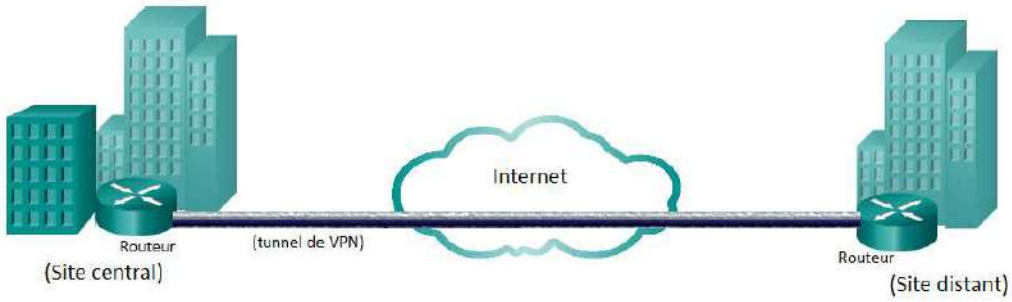


Figure 2.1 : Exemple d'un VPN site à site

Parmi les avantages et les inconvénients de cette configuration nous pouvons citer [11] :

- **Avantages des VPNs site à site**
  - ✓ Le cryptage est souvent pris en charge par des processeurs spécialisés, ce qui améliore notablement les performances.
  - ✓ Une grande facilité pour le contrôle de trafic autorisé.
  - ✓ Aucun impact sur les performances des poste puisque ceux-ci ne font pas de cryptage.

- ✓ La possibilité d'initier les VPN d'un côté ou de l'autre.

- **Inconvénients des VPNs site à site**
  - ✓ Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.
  - ✓ L'établissement des VPN nécessite que les deux extrémités soient bien identifiées soit par une adresse IP publique fixe, soit par un nom référencé dans des DNS officiels.

b. VPN poste à site :

Les VPNs poste à site est également une utilisation très fréquente des VPN qui consiste à permettre à des utilisateurs distants (travailleurs à domicile…) d'accéder aux ressources de l'entreprise via un VPN.

Afin de réaliser cette solution, un matériel (firewall, routeur…) sera mis en place sur le site central, constituant le point de terminaison de tous les VPN de ce dernier. Et un logiciel gérant le type de protocole choisi et compatible avec le matériel du site central est installé du côté des postes de travail distant. Dans certain cas, ce logiciel est déjà présent dans le système d'exploitation de ces postes, dans d'autre cas, il est nécessaire d'installer ce composant logiciel [10].

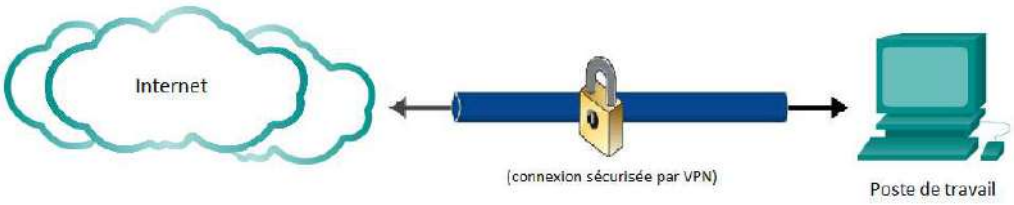


Figure 2.3 : Exemple d'un VPN poste à site

Parmi les avantages et les inconvénients de cette configuration nous pouvons trouver [11] :

- **Avantages des VPNs poste à site:**
  - ✓ L'accès du poste nomade (mobile) peut se faire de n'importe quel point de la planète doté d'un accès Internet.
  - ✓ La transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification.

- **Inconvénients des VPNs poste à site**
  - ✓ Une installation logicielle est généralement nécessaire sur le poste distant
  - ✓ Le cryptage impose une charge non négligeable au poste distant, ce qui peut en dégrader les performances
  - ✓ Le cryptage n'est pas assuré au-delà du firewall du site central.

c. VPN poste à poste :

Dans ce cas, l'objectif est d'établir un canal sécurisé de bout en bout entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux différents reliés eux-mêmes par un VPN site à site.

Pour cette configuration, nous ne faisons intervenir que des composants logiciels : un logiciel client sur le poste « demandeur » et un logiciel utilisé en serveur sur le poste « destinataire» [10].

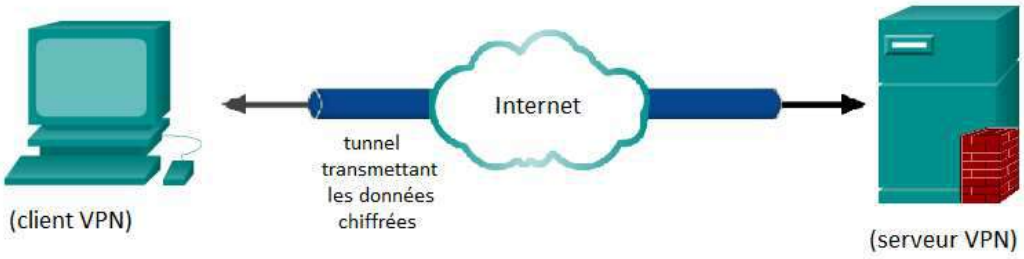


Figure 2.4 : Exemple d'un VPN poste à poste

Parmi les avantages et les inconvénients de cette configuration nous pouvons donner [11] :

- **Avantages des VPNs poste à poste :**

Le principal intérêt dans cette solution est que la conversation entre les deux postes est parfaitement protégée de bout en bout. C'est donc une très bonne option pour les communications les plus sensibles.

- **Inconvénients des VPNs poste à poste :**
  - ✓ Le cryptage est uniquement logiciel d'où un possible impact sur les performances en cas de fort débit, notamment quand les deux extrémités sont sur le même réseau local.
  - ✓ Quand les postes se situent sur des locaux sépares par internet il est nécessaire que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent autorisés par les firewalls situés sur chaque site, cela nécessite également des translations d'adresses puisque les machines concernées sont rarement dotées d'adresses IP publiques et cela n'est pas sans poser quelques problèmes.
  - ✓ Elle est inapplicable sur des matériels peu intelligents.

2.3.1.2 Avantages et inconvénients du VPN entreprise [11] :

Les principaux avantages de cette solution sont :

- ✓ Une indépendance quasi-totale vis-à-vis des opérateurs, ce qui fait que la solution peut être bâtie avec des opérateurs différents selon les sites.
- ✓ Pas de contrat à signer, à dénoncer pour la mise en place et la suppression de ces VPNs.
- ✓ Pas de frais mensuels autres que ceux de l'abonnement internet servant de support à ces VPNs.
- ✓ Une grande souplesse pour déplacer les tunnels, changer les périmètres ou contrôler le trafic y circulant.
- ✓ Maitrise des protocoles de sécurité (authentification, cryptage, filtrage ……).

Mais il y'a quelques inconvénients :

- ✓ Aucune garantie de temps de rétablissement en cas de défaillance.
- ✓ Aucune garantie de performances puisque ces VPNs ont pour support un lien internet.

2.3.2 VPN operateur :

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des engagements de performances et de disponibilité il est plus judicieux, mais évidemment plus couteux, de faire appel à un opérateur qui va donc mettre en place un réseau privatif entre tous les sites.

Ce réseau tient plus d'un réseau de tunnels que d'un véritable réseau VPN mais il est assez courant de parler quand même d'un VPN operateur car il est quand même difficile, sans la complicité du personnel de l'opérateur, d'intercepter les communications échangés entre les sites [10].

2.3.2.1 Caractéristiques du VPN operateur site à site :

Chaque site est relié au POP (Point Of Presence) le plus proche avec le medium souhaité (ADSL, SDSL, fibre optique …….) et un routeur complètement contrôlé par l'opérateur. Ensuite on établit des tunnels ou des circuits privatifs entre les différents sites au moyen des différents liens interconnectant ses POP.

La technologie pour ce faire varie en fonction des avancées technologiques et c'est ainsi que nous sommes passés des réseaux en Frame-Relay (Relai de trame) aux réseaux MPLS (MultiProtocol Label Switching) qui sont maintenant les plus courants dans ce cadre-là.

Selon le désir du client et les possibilités techniques ou budgétaires, ce réseau privatif peut être bâti avec différentes topologies :

- Tous les sites secondaires convergent vers le site central et c'est celui-ci qui fait le relais : technologie en hub (ou en Etoile).
- Tous les sites peuvent communiquer directement entre eux : (full mesh) ou maillage complet.
- Les sites les plus importants peuvent communiquer entre eux et les secondaires passent obligatoirement par un des sites principaux.
- L'opérateur supervise la totalité du réseau et peut affecter des classes de service selon le type de trafic, ce qui permet de rendre prioritairement certains flux [10].

2.3.2.2 Avantages et inconvénients du VPN operateur :

Les principaux avantages de ce type de réseaux sont :

- ✓ Une transparence totale vis-à-vis des postes du réseau.
- ✓ Une possibilité de mettre en place de la QOS (Quality Of Service) pour privilégier les trafics les plus prioritaires et garantir à ceux-ci un maximum de bande passante.
- ✓ Une assurance sur les performances proposées par le réseau aussi bien en termes de débit que de temps de transit des messages.

Il y'a néanmoins de points à considérer comme des inconvénients :

- ✓ Le cout engendré par l'abonnement de chaque site à ce réseau operateur.
- ✓ La nécessité d'avoir un opérateur unique pour l'ensemble du réseau mis en VPN.
- ✓ Afin que les messages échangés dans ce réseau privatif ne puissent ne capturés, il faut ajouter un protocole de cryptage entre les stations ou entre les sites. [10]

2.4 Principaux protocoles :

Voici une brève description des protocoles les plus utilisés concernent les VPN qu'ils soient d'entreprise ou d'opérateur. On les présente suivant leurs placements dans les couches OSI (Open Systems Intercinnection).

On note que le classement de ces protocoles est arbitraire vu que certains d'entre eux recouvrent plusieurs niveaux.

2.4.1 Niveau 2 :

Dans une communication par VPN la plupart des protocoles situés au niveau 2 du modèle OSI sont progressivement délaissés au profit de protocoles plus souples comme l'être ceux des niveaux 3 à 7[11].

Il est à signaler que les VPN encapsulent les données dans les trames qui vont être envoyé à travers le tunnel.

2.4.1.1 PPTP (Point to Point Tunneling Protocol):

Ce protocole fortement soutenu par Microsoft est très simple mais assez limité. Il est en fort déclin maintenant selon Jean-Paul ARCHIER l'auteur du livre « les VPN fonctionnement, mise en œuvre et maintenance des Réseaux Privé Virtuels » [10].

Il crée les trames sous le protocole PPP et les encapsuler dans des paquets IP.

2.4.1.2 L2F (Layer 2 Forwarding) :

Cisco a développé ce protocole autour des années 1996. L'IETF a en fait un standard en 1998 avec le RFC 2341. Son fonctionnement est assez voisin de PPTP [10].

2.4.1.3 L2TP (Layer 2 Tunneling Protocol) :

Dérivé de PPTP et de L2F ce protocole est maintenant un des protocoles VPN implantés nativement sur les machines Windows, ce qui explique son succès [10].

2.4.2 Niveau 2 et 3 :

2.4.2.1 MPLS (Multi Protocol Label Switching) :

Le protocole MPLS (Multi Protocol Label Switching) est souvent considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est pourquoi on lui affecte souvent un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnelles. Son placement en tant que protocole de VPN peut être contesté lorsqu'il est utilisé dans ses fonctions de base. En effet il ne met pas en œuvre certaines fonctions de sécurité telles que le cryptage, ce qui est en principe un prérequis du VPN [12].

2.4.2.2 Fonctionnalité :

La première fonctionnalité de MPLS consiste à accélérer la transmission des informations au sein d'un backbone IP, car l'acheminement est basé sur la reconnaissance d'un Label qui permet dans le réseau de transit de ne plus se préoccuper de l'adresse mais de traiter le message en fonction de ce Label. La seconde est de permettre la création de VPN (Virtual Private Network) ou groupe fermé d'utilisateurs [12].

MPLS est une technologie toujours en cours de standardisation à l'IETF. L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des gigarouteurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

- ✓ Intégration IP/ATM
- ✓ Création de VPN
- ✓ Flexibilité : possibilité d'utiliser plusieurs types de media (ATM, FR, Ethernet, PPP, SDH).
- ✓ Differential Services (DiffServ)
- ✓ Routage multicast
- ✓ Traffic Enginnering permettant de définir des chemins de routage explicites dans le réseau IP [11].

2.4.2.3 Principe MPLS :

Basée sur la permutation d'étiquettes, un mécanisme de transfert simple offre des possibilités de nouveaux paradigmes de contrôle et de nouvelles applications. Au niveau d'un LSR (Label Switch Router) du nuage MPLS, la permutation d'étiquette est réalisée en analysant une étiquette entrante, qui est ensuite permutée avec l'étiquette sortante et finalement envoyée au saut suivant.

A l'entrée du réseau MPLS, les paquets IP se voient insérés un label par le "Ingress Label Edge Routeur" ou "Ingress LER" (interface d'entrée ou point de départ d'une donnée).

Les LER sont les routeurs MPLS se situant à la périphérie du réseau de l'opérateur. Les paquets labélisés sont ensuite commutés vers le cœur du réseau selon son numéro de label. Les routeurs MPLS du cœur de réseau, les Label Switching Router, commute ensuite les labels jusqu'au LER de sortie (Egress LER). Le chemin qui a été pris par le paquet, et préalablement établi, au travers du réseau s'appelle un Label Switched Path (LSP) [12].

La première fois que le datagramme d'un flux arrive à un Ingress E-LSR. Ce label est supprimé à l'autre extrémité par le Egress E-LER. Donc le mécanisme est le suivant:

1. Le Ingress LSR (E-LSR) reçoit les paquets IP.
2. Réalise une classification des paquets.
3. Y assigne un label et transmet les paquets labellisés au nuage MPLS.

En se basant uniquement sur les labels, les LSR du nuage MPLS commutent les paquets labellisés jusqu'à l'Egress LSR qui supprime les labels et remet les paquets à leur destination finale.

L'affectation des étiquettes aux paquets dépend des groupes ou des classes de flux FEC (forwarding équivalence classes). Les paquets appartenant à une même classe FEC sont traités de la même manière.

Le chemin établi par MPLS appelé LSP (Label Switched Path) est emprunté par tous les datagrammes de ce flux. L'étiquette est ajoutée entre la couche 2 et l'en-tête de la couche 3 (dans un environnement de paquets) ou dans le champ VPI/VCI (identificateur de chemin virtuel/identificateur de canal virtuel dans les réseaux ATM (Asynchronous Transfert Mode)).

Le switch LSR du nuage MPLS lit simplement les étiquettes, applique les services appropriés et redirige les paquets en fonction des étiquettes. Ce schéma de consultation et de transfert MPLS, offre la possibilité de contrôler explicitement le routage en fonction des adresses source et destination, facilitant ainsi l'introduction de nouveaux services IP [12].

2.4.3 Niveau 3 :

Les protocoles de ce niveau sont responsables des paquets.

2.4.3.1 SSL/TLS :

Ce protocole ou plutôt ces protocoles sont en plein essor car très simples de mise en œuvre et utilisant le port (443), ce qui facilite le franchissement des firewalls. Dans un certain nombre de cas, ils ne nécessitent qu'un simple navigateur pour être utilisables. Ils sont maintenant implémentés de façon native dans d'autres logiciels (client de messagerie, client FTP) [10].

2.4.3.2 SSH :

Ce protocole était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment).

Son essor est limité à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint. Néanmoins il reste encore un protocole à considérer pour certains usages [10].

2.4.3.3 IPSEC :

Ce protocole très populaire est un des plus robustes et des plus versatiles mais il est aussi un des plus complexes. IPsec permet, par encapsulation, de protéger les données échangé en plusieurs aspects :

- ✓ Confidentialité
- ✓ Intégrité des données
- ✓ Anti-rejeu

Plusieurs versions se sont succédé et divers éléments additionnels ont été définis. Un très grand nombre d'équipements réseaux, en particulier les routeurs et les pare-feux, permettent l'utilisation d'IPsec. De même, les principaux systèmes d'exploitation pour micro-ordinateurs ou ordiphones (téléphone intelligent) prennent en charge IPsec nativement. Le dialogue IPsec est généralement possible entre ces différents systèmes et équipements.

Dans de nombreux cas, l'utilisation d'IPsec présente un rapport "bénéfice en sécurité" sur "coût" appréciable dans la mesure où cette technologie est prise en charge nativement par la

plupart des systèmes clients et des équipements réseau et ne nécessite donc généralement pas d'investissements lourds [13].

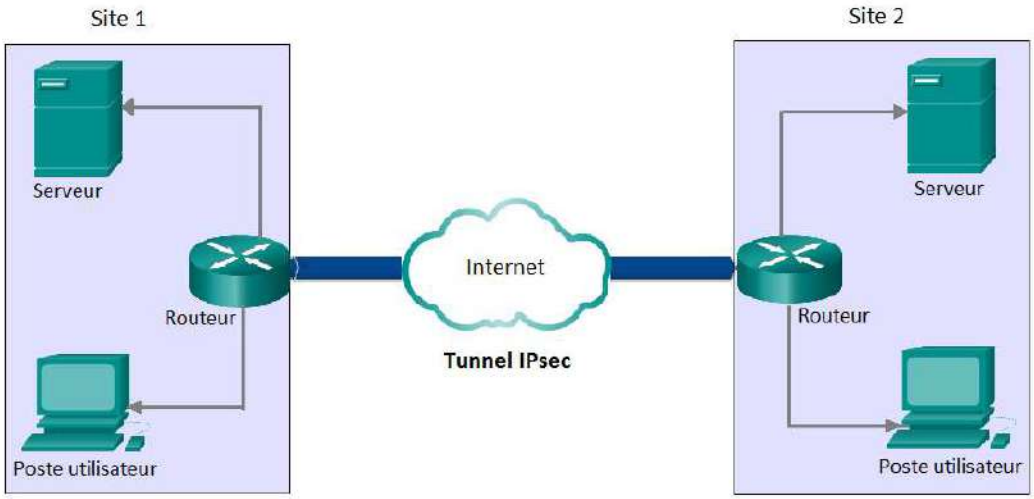


Figure 2.5 : Exemple d'emploi d'IPsec entre deux sites distants

a. Comparaison entre le protocole IPsec et le protocole TLS :

Il est fréquent de voir IPsec comparé au protocole TLS. Il est vrai que les deux technologies permettent de bénéficier de mécanismes de confidentialité, d'intégrité ou d'authentification.

Il existe toutefois plusieurs différences importantes, qui tendent à faire préférer IPsec. TLS agit beaucoup plus haut dans la pile réseau qu'IPsec, en se plaçant au-dessus de la couche transport réalisée par TCP. TLS est souvent employé pour sécuriser d'autres protocoles.

C'est ainsi que fonctionne par exemple le protocole HTTPS. C'est toutefois sur un autre usage que ce protocole entre en concurrence avec IPsec, à savoir la mise en œuvre de « VPN-SSL ». Cette méthode consiste à encapsuler un flux réseau dans une session TLS.

Certaines solutions de ce type proposent de s'appuyer sur un navigateur pour se dispenser de la nécessité de déployer un client spécifique sur les postes utilisateurs.

Le premier inconvénient de TLS est que les opérations liées à la sécurité sont effectuées en espace utilisateur, au sein du processus utilisateur. Ces opérations (et les secrets qu'elles manipulent) sont alors nettement plus exposées aux attaques que dans le cas d'IPsec où les opérations critiques se déroulent au sein du noyau ou dans des processus dédiés.

Cela est d'autant plus vrai dans le cas où le client VPN s'appuie sur un navigateur, logiciel présentant une surface d'attaque considérable, y compris à distance.

En outre, sur le plan cryptographique, plusieurs éléments plaident en faveur d'IPsec. D'une part, IPsec permet plus largement l'utilisation d'algorithmes modernes recommandés par les bonnes pratiques, que ce soit en termes de prise en compte dans les standards ou d'implantations concrètes dans les logiciels disponibles sur le marché.

D'autre part, dans IPsec, l'utilisation des primitives cryptographiques est légèrement meilleure au regard des bonnes pratiques. IPsec recourt, par exemple, à un fonctionnement «Encrypt-then-MAC», méthode considérée plus sûre que le « MAC-then-Encrypt » employé par TLS.

Enfin, on peut observer que le détournement de TLS de l'usage en recourant à des « VPN SSL » n'est pas une solution idéale. L'encapsulation de paquets de la couche réseau en couche applicative conduit notamment à avoir une en-tête TCP « externe » sans aucune corrélation avec l'éventuelle en-tête TCP « interne », ce qui débouche sur un fonctionnement non optimal des mécanismes de contrôle de congestion [13].

b. Fonctionnement d'IPsec :

IPsec, de par ses subtilités, est souvent partiellement compris et peu maîtrisé. Les choix de configuration, y compris ceux par défaut, ne sont pas toujours judicieux et l'emploi d'IPsec peut alors offrir un niveau de sécurité plus faible que celui attendu [13].

c. Services fournis par IPsec:

Les services de sécurité que l'IPsec garantis sont fondés sur les protocoles AH et ESP, qui sont souvent utilisé d'une façon indépendante ou bien dans une minorité des cas en combinaison entre eux.

- **Intégrité et authentification des paquets (AH):**

Le protocole AH, qui est utilisé de manière moins fréquente qu'ESP, permet d'assurer l'intégrité, il est employé avec IKE (Internet Key Exchange), et assure l'authentification des paquets IP. C'est à dire qu'AH permet d'une part de s'assurer que les paquets échangés n'ont pas été altérés et d'autre part de garantir l'identité de l'expéditeur d'un paquet. Il garantit aussi une protection contre le rejeu [11].

- **Confidentialité, intégrité et authentification des paquets (ESP):**

Le protocole ESP permet quant à lui d'assurer la confidentialité, l'intégrité, il est employé avec IKE et assure aussi l'authentification des données échangées. Il garantit aussi une protection contre le rejeu. Il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH) [13].

d. Mode Transport et Tunnel :

Indépendamment du choix entre AH et ESP, il est possible d'utiliser IPsec dans deux modes distincts : le mode tunnel et le mode transport.

Le mode tunnel rend le service attendu dans la majorité des cas. Dans le mode transport, les données associées à AH ou à ESP viennent se greffer sur le paquet IP initial (c'est à dire celui qu'on aurait envoyé en l'absence d'IP sec). Le paquet IP résultant contient un paquet AH ou ESP qui contient lui-même le contenu du paquet initial (un segment TCP par exemple).

On peut remarquer que l'en-tête IP initiale doit être modifiée : son champ protocole doit indiquer 50 ou 51 pour ESP ou AH en lieux et place par exemple de 6 (TCP) ou 17 (UDP). C'est l'en tête (AH ou ESP) qui indiquera le protocole encapsulé qui était auparavant indiqué dans l'en-tête IP [11].

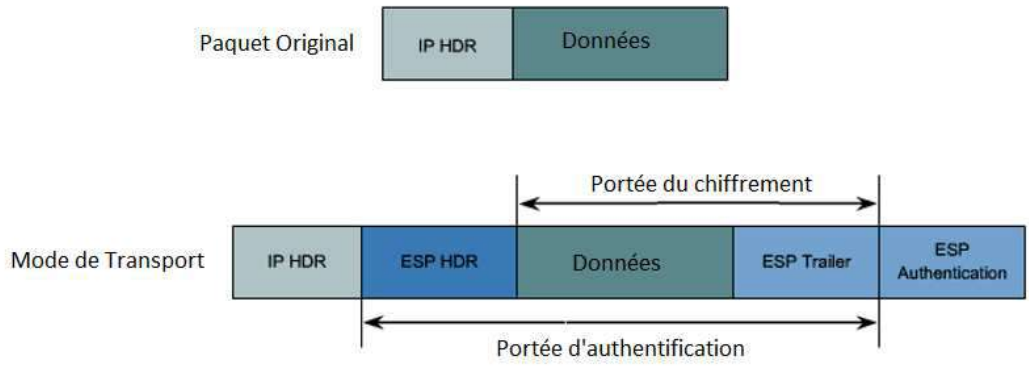


Figure 2.6: Utilisation d'ESP en mode transport.

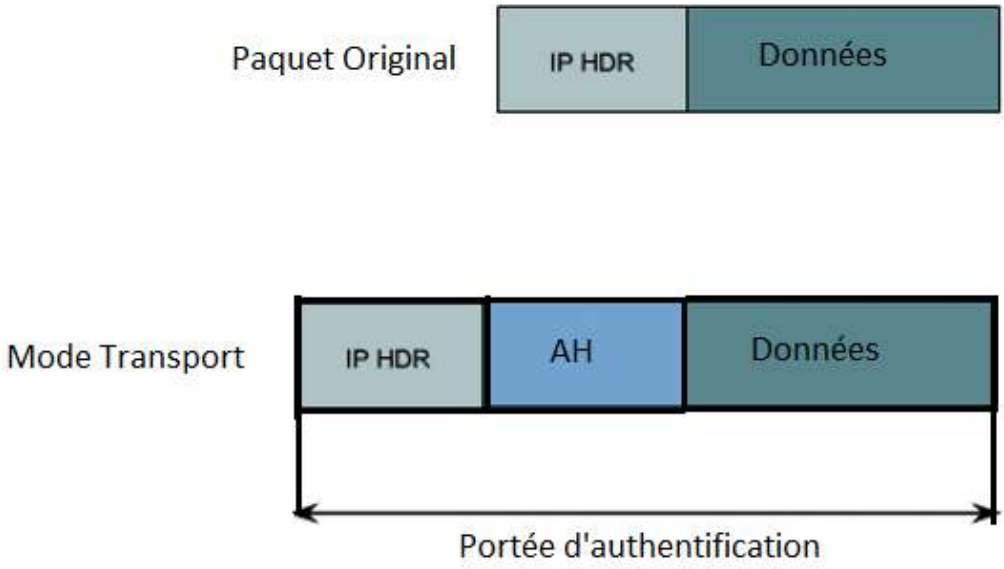


Figure 2.7 : Utilisation d'AH en mode transport

Dans le mode tunnel en revanche, un nouveau paquet IP est généré pour contenir un paquet AH ou ESP qui contient lui-même le paquet IP initial sans modification. Dans ce mode, il y a donc en définitive deux en-têtes IP.

L'en-tête externe sera effectivement utilisé pour le routage dès l'émission du paquet. L'en-tête interne, qui peut être chiffrée dans le cas où l'on utilise ESP avec le service de confidentialité, ne sera traité que par le destinataire (du paquet externe). Elle sera ignorée par les équipements réseau situés entre l'émetteur et le destinataire.

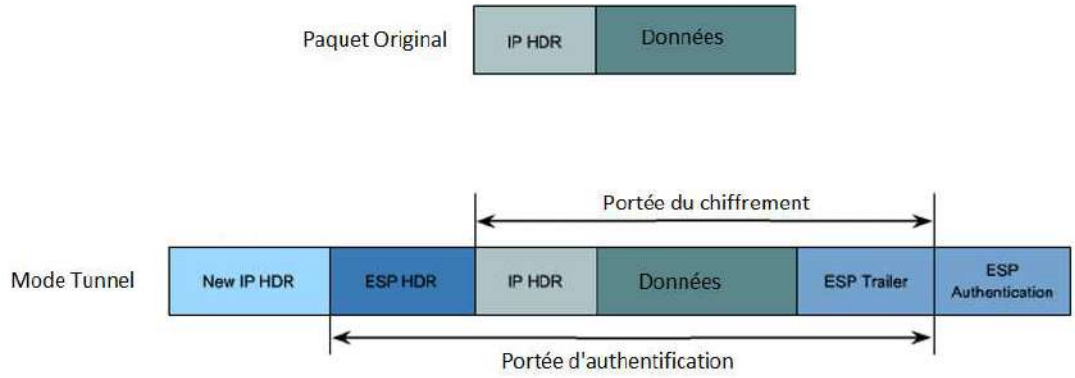


Figure 2.8 : Utilisation d'ESP en mode tunnel

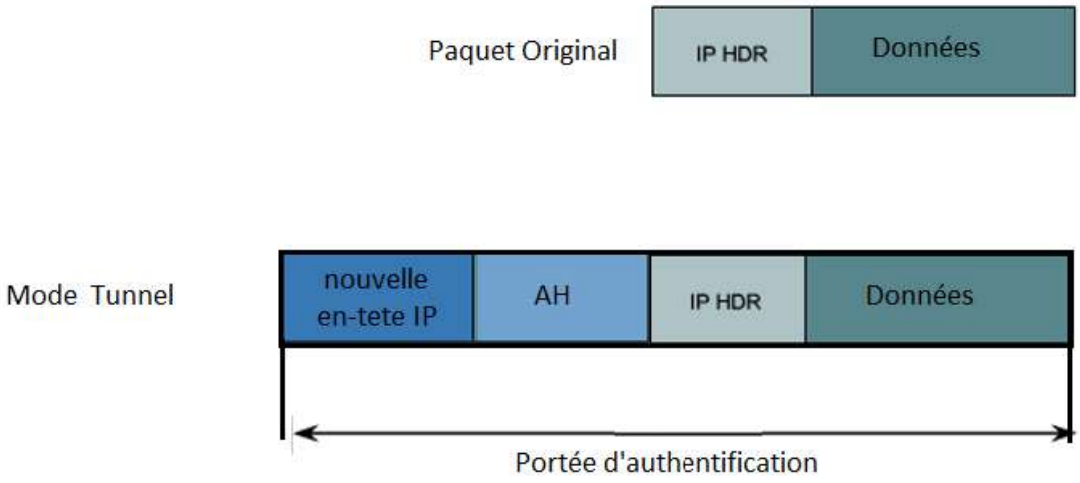


Figure 2.9 : Utilisation d'AH en mode tunnel

Le mode tunnel se prête bien à un scénario d'accès distant à un réseau privé au travers d'un réseau public. Il permet de masquer sur les tronçons publics l'adressage interne du réseau privé, fréquemment non routable sur le réseau public.

IPsec est utilisé sur le réseau public entre le client et une passerelle qui extrait le paquet IP interne et l'injecte dans le réseau privé (et réciproquement pour le sens de communication inverse).

Naturellement, du fait de la duplication de l'en-tête IP, l'utilisation du mode tunnel résulte en des paquets plus gros qu'en mode transport pour une même quantité de données utiles. La consommation en ressources réseau est donc plus importante [13].

e. Security Policy :

Le terme « Security Policy 'SP' » désigne, dans le contexte IPsec, le choix pour un lien unidirectionnel donné :

- ✓ De l'utilisation obligatoire ou facultative ou de la non-utilisation d'IPsec ;
- ✓ De l'utilisation du mode tunnel ou transport ;
- ✓ De l'utilisation d'AH ou d'ESP.

L'ensemble des SPs est regroupé dans une SPD : « Security Policy Database ».

À l'image des règles de flux d'un pare-feu, les SPs ont pour but de spécifier les flux que l'on veut autoriser et ceux que l'on veut interdire [13].

f. Utilisation d'IKE (internet Key Exchange) :

La négociation dynamique des algorithmes et clés d'une SA peuvent se faire grâce au protocole IKE, actuellement en version 2 (RFC 5996) [13].

Remarque : Une **association de sécurité** (SA, Security Association) IPsec spécifie les propriétés de sécurité que reconnaissent les hôtes lors de la communication.

g. Authentification des correspondants :

L'authentification des participants à la première phase peut se faire soit au moyen d'un secret partagé (PSK : « Pre-Shared Key ») soit par utilisation d'un mécanisme de cryptographie asymétrique tel que RSA (Rivest Shamir Adelman).

Dans ce cas, il est possible d'utiliser une Infrastructure de Gestion de Clés (IGC ou PKI) pour certifier les clés publiques des participants et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes [13].

2.5 Conclusion :

Ce chapitre nous a donné l'opportunité en premier lieu de découvrir et de mieux comprendre le concept des VPNs, où nous avons présenté ses notions de base et les différents protocoles nécessaires pour le fonctionnement d'un VPN.

Le but de ce chapitre est pour nous aider à faire une simulation d'une connexion VPN qui va être aborder dans le chapitre suivant.

Chapitre 3 : Configuration et Tests

CHAPITRE 3 :

CONFIGURATION ET TESTS

3.1 Introduction :

Dans ce chapitre on va effectuer une configuration VPN entre deux sites distants. En commence avec une représentation de logiciel utilisé avant d'exposer l'architecture permettant de réaliser l'idée désirée. Ensuite nous citerons les différents composants de l'architecture du réseau utilisée, ainsi qu'une explication des protocoles et les commandes exécutés sur les périphériques du réseau. Enfin, nous terminerons avec la vérification du bon fonctionnement de la configuration proposée afin de démontrer le bon fonctionnement de notre VPN configuré.

3.2 Packet Tracer :

C'est un logiciel flexible et interactif, dont il se présente comme est un simulateur de réseau graphique, qui prend en charge une large gamme de simulations physiques et logiques.

Packet Tracer fournit également des outils de visualisation pouvant nous aider à comprendre le fonctionnement interne d'un réseau. Aussi il permet de tester le comportement d'un réseau, de concevoir des modèles de réseau et de mettre en pratique des expériences et scénarios réseau [2].

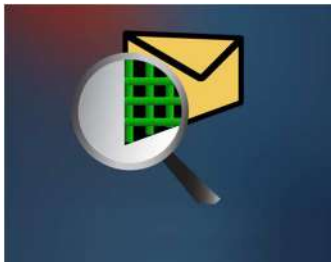


Figure 3.1 : Logo de logiciel Packet Tracer

3.3 Architecture du réseau :

Pour la réalisation de notre projet, on a choisi d'utiliser trois routeurs de la gamme cisco 1841, deux commutateurs de la gamme cisco 2960 et deux PCs.

L'ensemble de ces périphériques construit une architecture réseau où ils sont connectés à la façon montrée sur la figure 3.2.

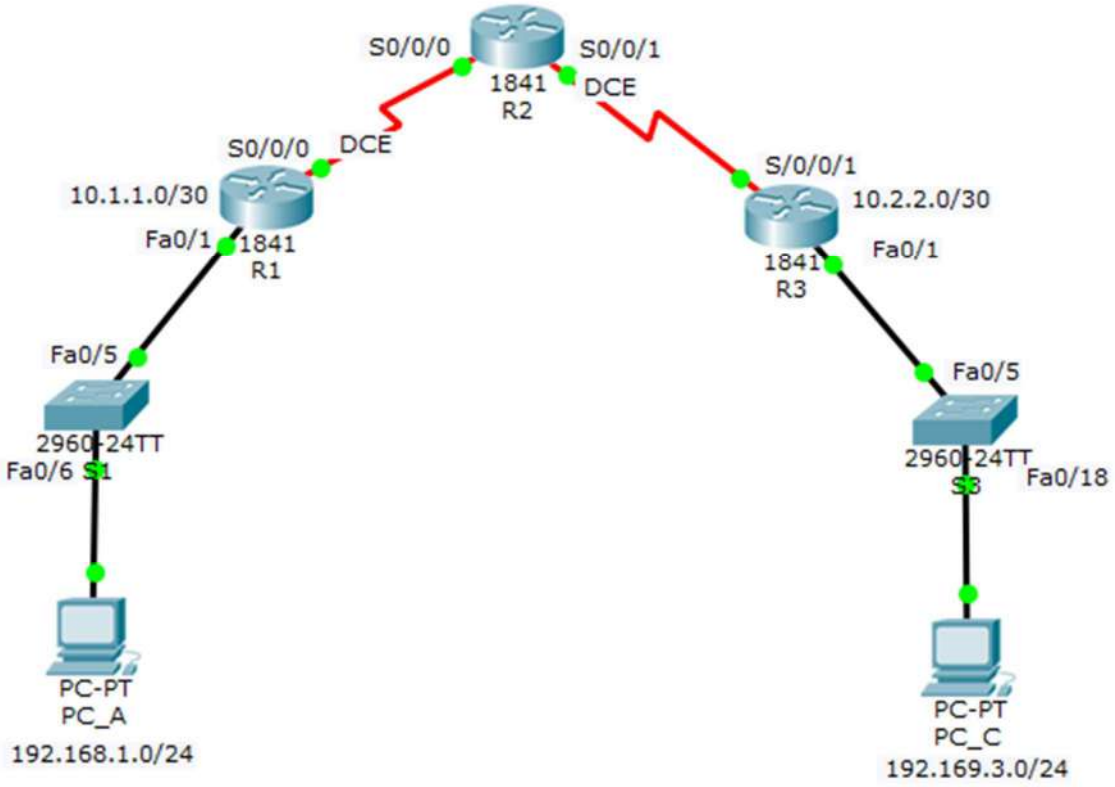


Figure 3.2 : Architecture du réseau sous Packet Tracer

3.3 Table d'adressage :

Chaque interface d'un périphérique doit être identifiée par une adresse pour quelle peut fonctionner. La figure (3.3) montre les différentes adresses utilisées pour chaque interface.

Dispositif	Interface	Adresse IP	Adresse MAC	Passerelle par défaut	Port de commutateur
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC_A	NIC	192.168.3.1	255.255.255.0	192.168.1.1	S1 Fa0/6
PC_C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 Fa0/18

Tableau 3.1 : Table d'adressage des dispositifs utilisés

3.4 Configuration :

Toutes les configurations des équipements du réseau seront réalisées au niveau de la **CLI** (**C**ommande **L**angage **I**nterface) (**Figure 3.4**). **CLI** est une interface de simulateur **Cisco Packet Tracer** qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes.

Nous allons lancer des séries des configurations sur tous les équipements du réseau. Dans ce qui suit, tout en montrant des exemples de chaque configuration.

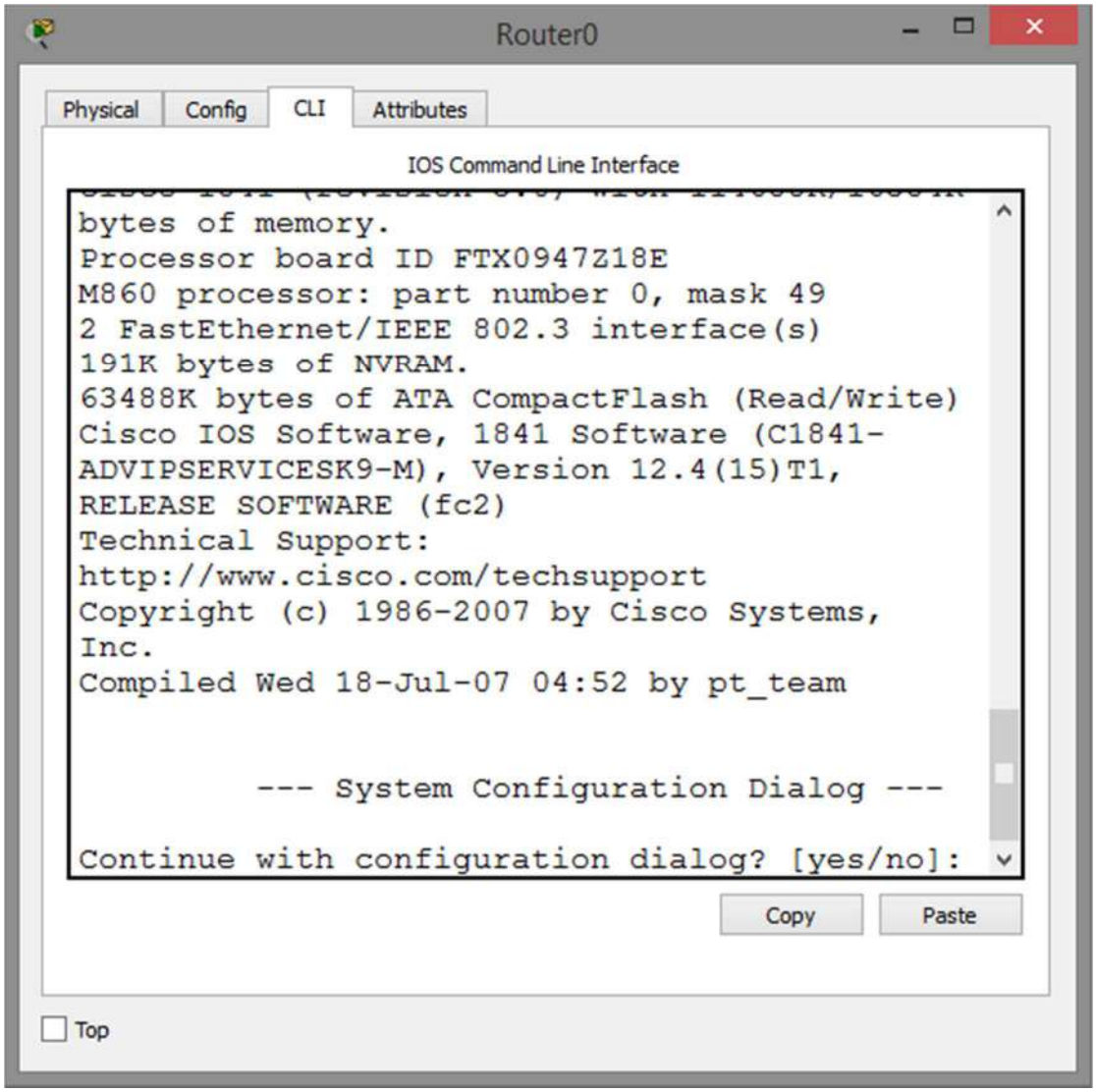


Figure 3.3 : Interface CLI

3.4.1 Configuration de base :

3.4.1.1 Configuration de Hostnames :

Cette configuration a pour but de renommer les périphériques par des noms significatifs. Donc on a choisi (R1, R2, R3) pour les routeurs, (S1, S2) pour les commutateurs et (PC_A , PC_C) pour les PCs. Sachant que c'est la même procédure pour tous.

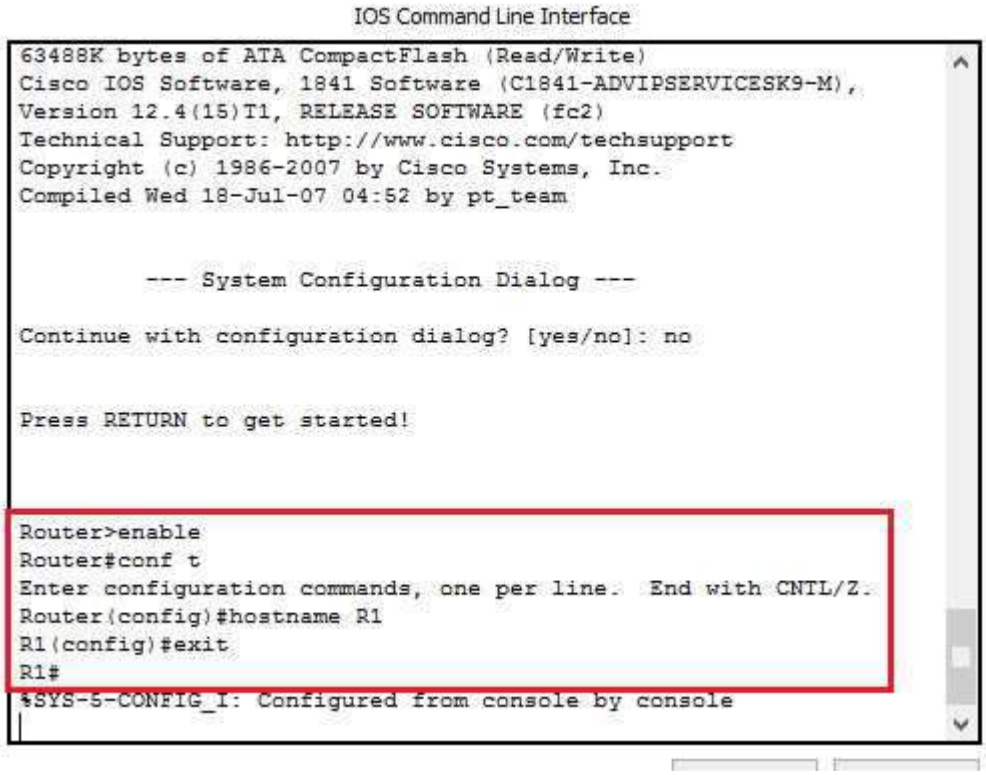


Figure 3.4 : Exemple de configuration de Hostname sur le routeur 1

3.4.1.2 Configuration des adresses IP et MAC :

On configure les interfaces des trois routeurs et les deux Pc, chacun par son adresse IP et MAC comme il est indiqué dans la table d'adressage.

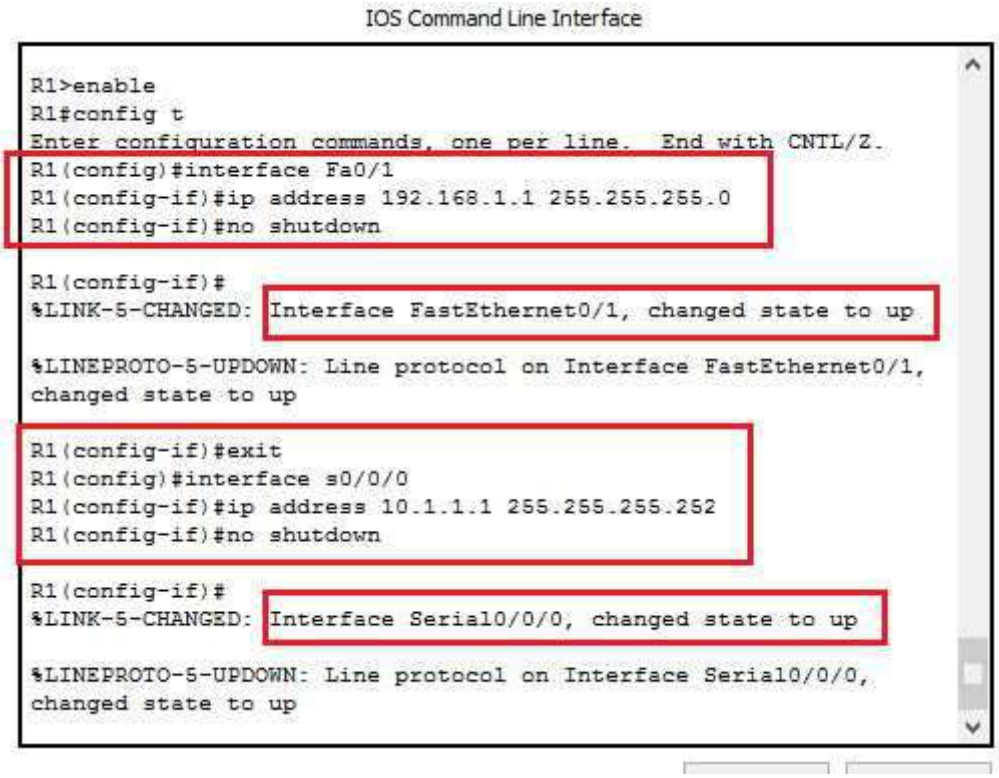


Figure 3.5 : Configuration des interfaces du routeur R1

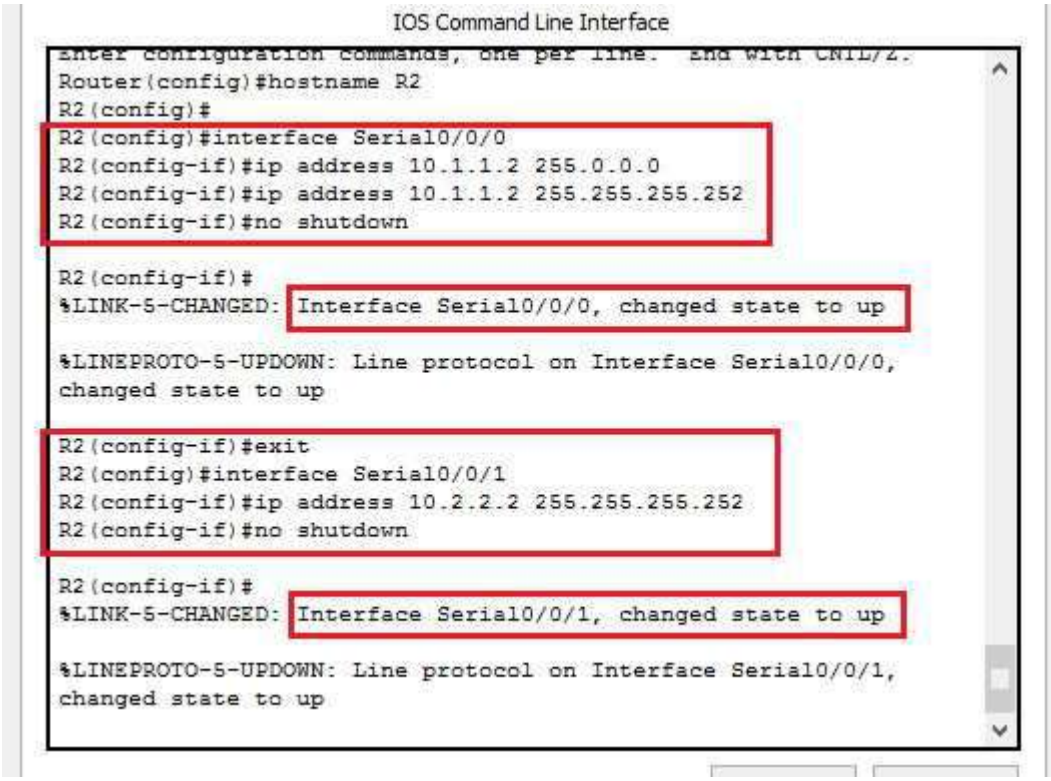


Figure 3.6 : Configuration des interfaces du routeur R2

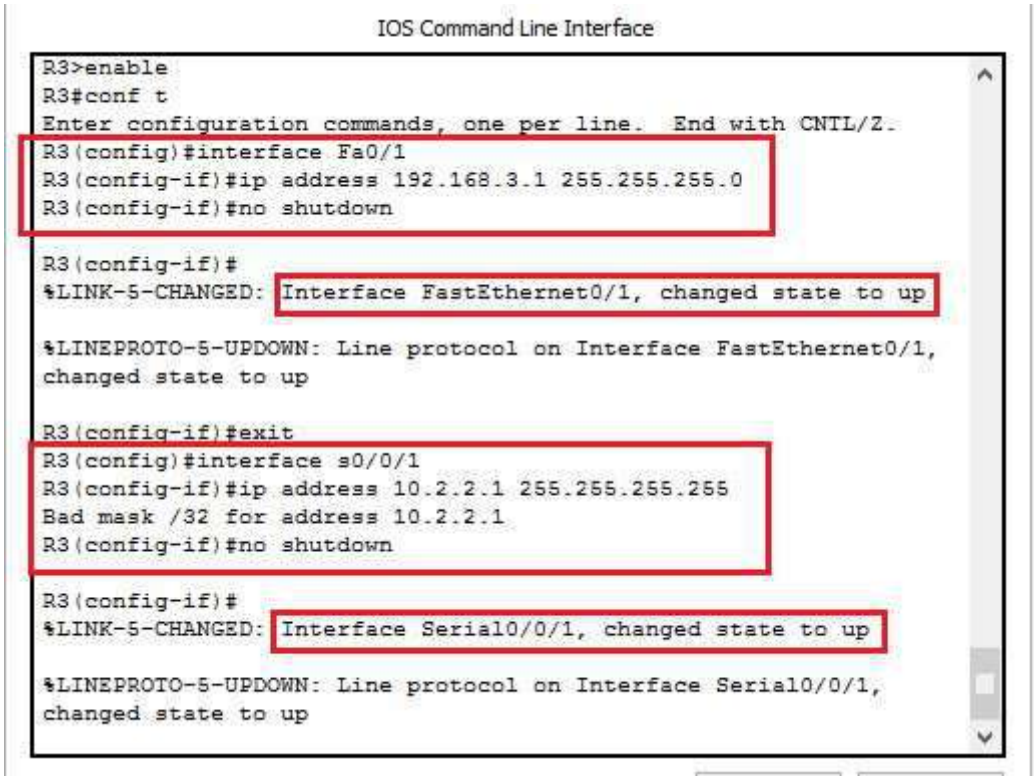


Figure 3.7 : Configuration des interfaces du routeur R3

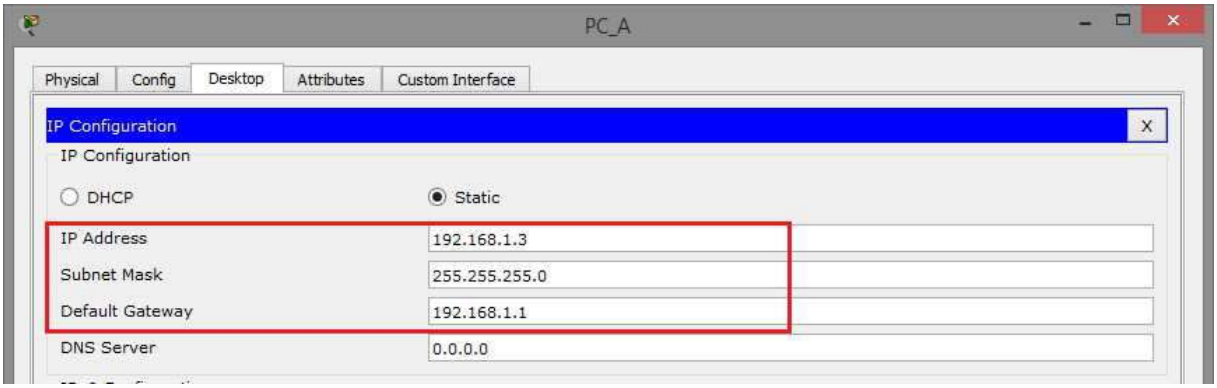


Figure 3.8 : Configuration d'adresse IP pour PC-A

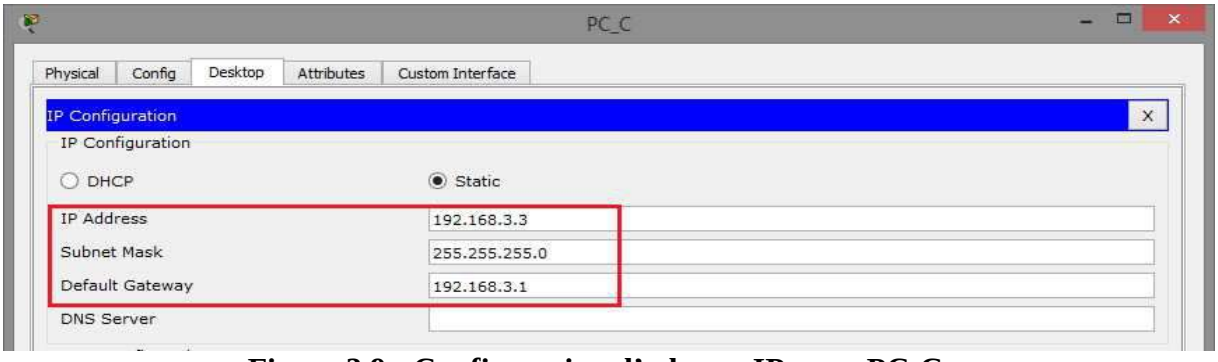


Figure 3.9 : Configuration d'adresse IP pour PC-C

3.4.1.3 Configurez une fréquence d'horloge :

On choisit 64000 pour les interfaces de routeur série avec un câble série DCE connecté.

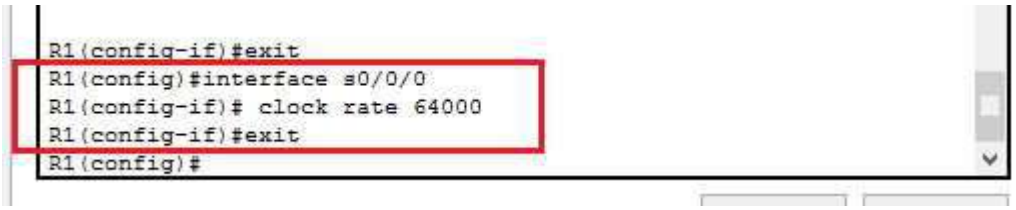


Figure 3.10 : Exemple de configuration de la fréquence d'horloge sur R1

3.4.1.4 Désactivation de la recherche DNS :

Pour empêcher le routeur de tenter de traduire des commandes mal saisies, nous désactivons la recherche **DNS**.



Figure 3.11 : Exemple de désactivation de la recherche DNS sur R1

3.4.1.5 Configuration de protocole de routage :

On a choisi d'utiliser l'**OSPF** (**O**pen **S**hortest **P**ath **F**irst) comme protocole de routage à cause de sa capacité de bien gérer les réseaux **WAN**, ainsi que le domaine de routage.

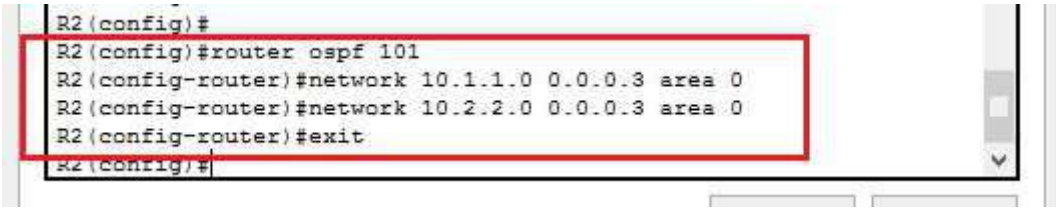


Figure 3.12 : Configuration du protocole de routage OSPF sur le routeur R2

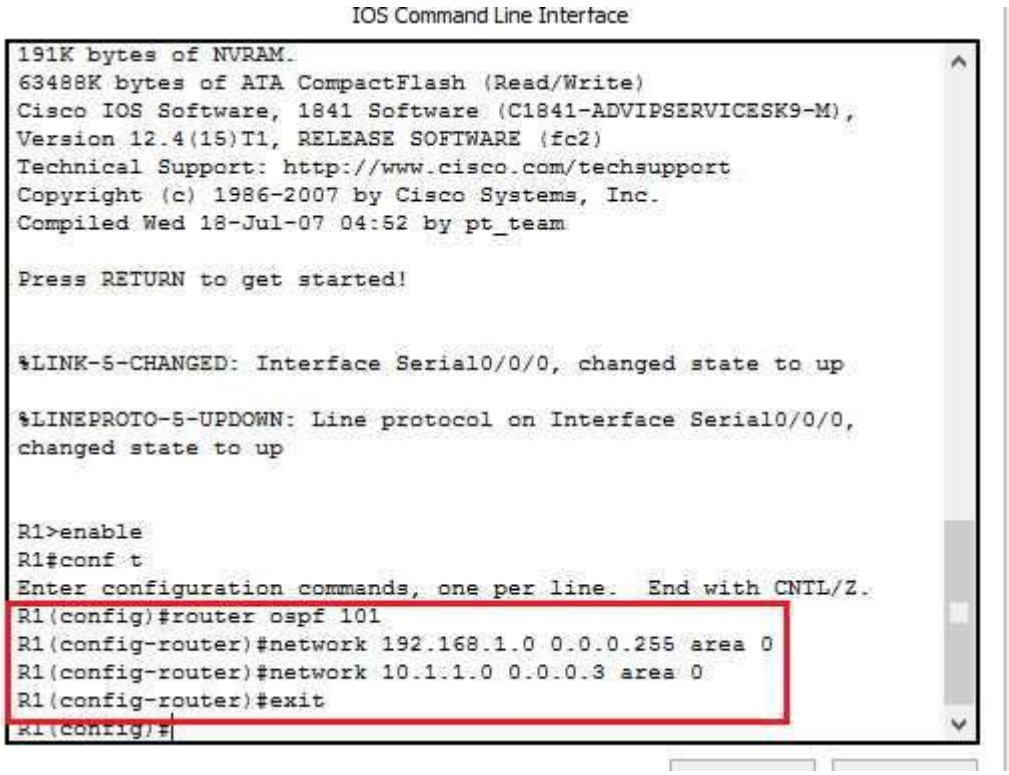


Figure 3.13 : Configuration du protocole de routage OSPF sur le routeur R1

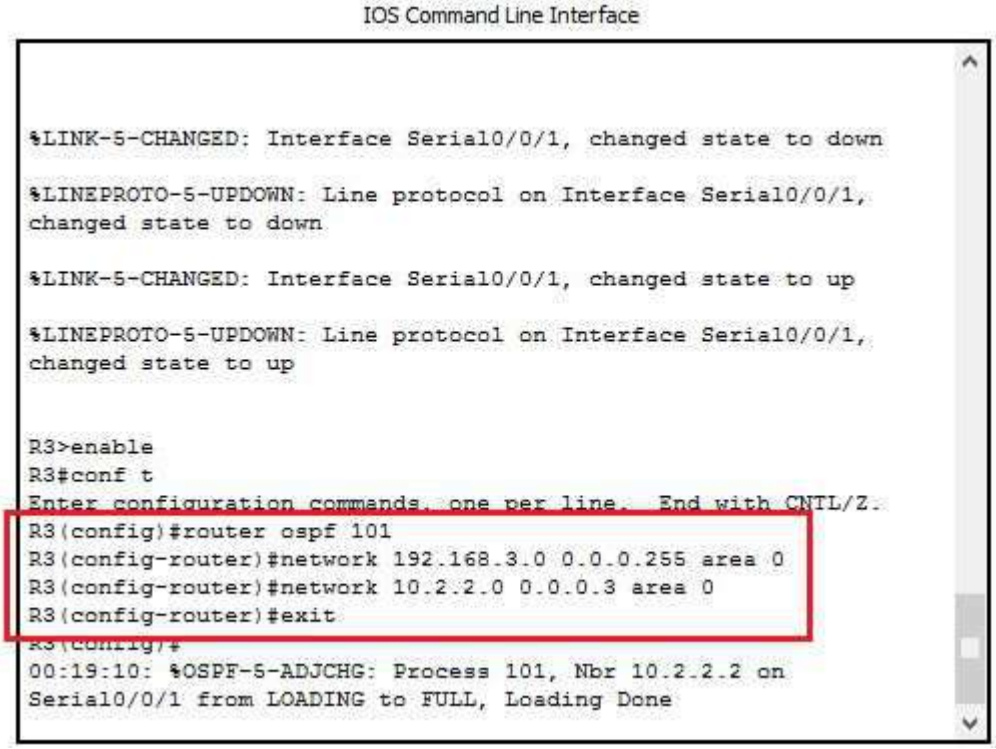


Figure 3.14 : Configuration du protocole de routage OSPF sur le routeur R3

3.4.1.6 Configuration des mots de passe pour les modes console et vty :

On fait la configuration de mots de passe « **ciscoconpass »** pour le mode **console** et « **ciscovtypass »**pour le mode **vty**. Pour plus de sécurité, la commande « **exec-timeout »**entraîne la déconnexion de la ligne après 5 minutes d'inactivité.

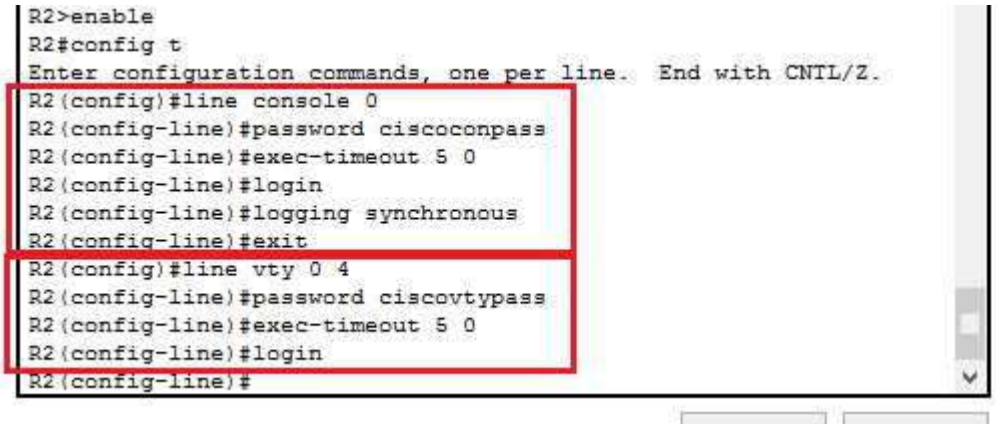


Figure 3.15 : Exemple de configuration des modes console et vty sur le routeur R2

- **Remarque :**

- Cette configuration est faite sur les trois routeurs **R1, R2** et **R3**.
- Pour encrypter les mots de passe des modes **console** et **vty** , on utilise la commande : « R1 (config)# **service password-encryption »**
- On utilise la commande « **securitypasswords** » pour définir une longueur minimale de mot de passe de 10 caractères.

« R1 (config) # **mots de passe de sécurité longueur min.10** »

- Pour enregistrer la configuration, on utilise la commande :

« R1# **copy running-config startup-config »**

3.4.1.7 Vérification de la connectivité :

Nous vérifions de la connectivité entre le **LAN R1** et le **LAN R3**, pour cela nous utilisons la commande **Ping** à partir de **PC_A** vers **PC_C** qui porte l'adresse **IP 192.168.3.3**.

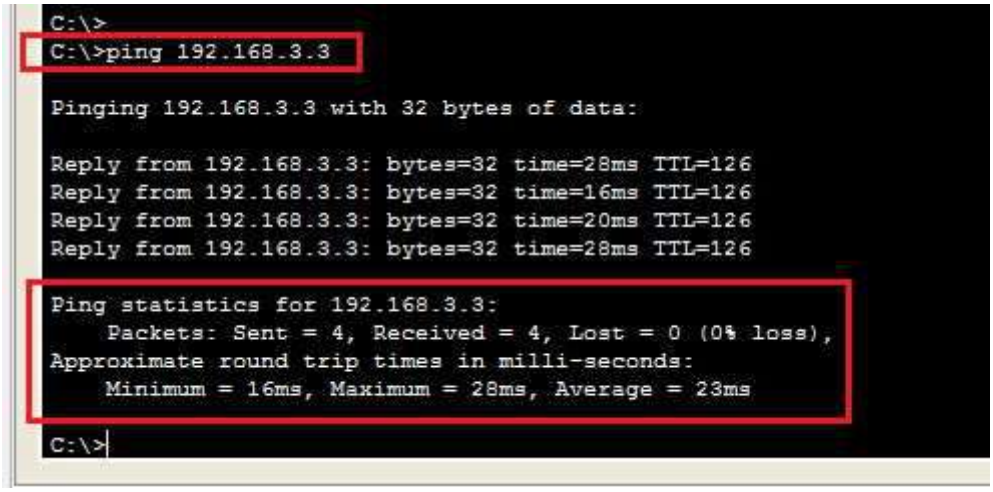


Figure 3.16 : Résultat de vérification de connectivité entre PC_A et PC_C

Et on fait un autre **Ping** à partir de Routeur **R1** destiné à l'interface d'entrée **S0/0/1** de routeur **R3**.

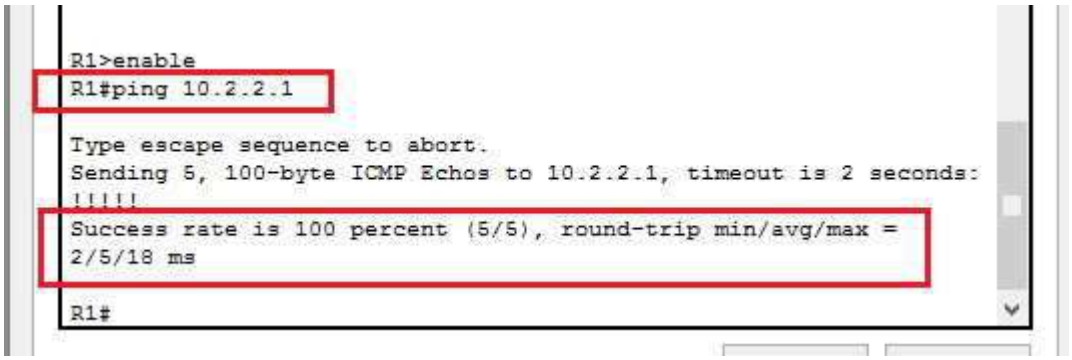


Figure 3.17 : Résultat de vérification de connectivité entre R1 et R3

3.4.2 Configuration de VPN site à site :

Remarque : la configuration pour création de **VPN** est faite juste sur les deux routeurs **R1** et **R3**, aucune configuration sur **R2** n'est faite.

- **Etape 1 :** Avant de commencer la création de **VPN**, il faut d'abord activer le protocole **ISAKMP** qui gère l'échange des clés qui seront utilisées entre les deux extrémités (**R1** et **R3**) du tunnel.

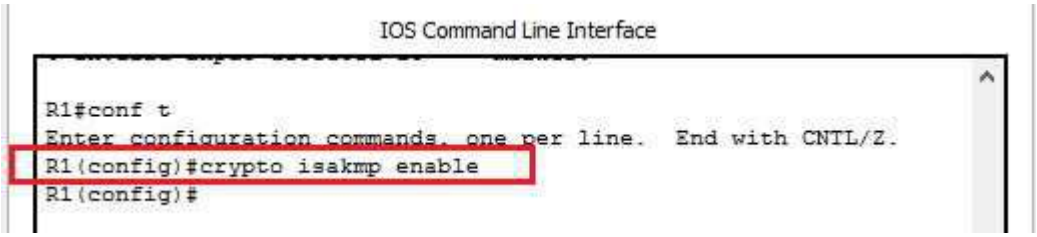


Figure 3.18 : Activation du protocole ISAKMP sur R1

- **Etape 2 : La création de « Policy_map » :**

C'est un protocole qui gère la négociation des clés et établit la liaison **VPN**. Il contient les éléments suivant :

- **Policy :** Elle définit la politique de connexion d'**ISAKMP**, et nous choisissons 10 comme degré de priorité de l'utilisation.
- **Pre-share :** C'est le type d'authentification utilisé qui sert à garantir que le paquet a bien été envoyé et signé par le pair distant.
- **Encryption:** Le choix de l'algorithme de chiffrement détermine le degré de confidentialité du canal de contrôle entre les deux extrémités dans notre cas on a choisi **aes 256** comme un algorithme de chiffrement.
- **Sha :** C'est l'algorithme de hachage utilisé pour contrôler l'intégrité des données. Il garantit que les données reçues d'un pair n'ont pas été falsifié pendant le transport.
- **Groupe 5 :** L'algorithme d'échange de **clef Diffie-Hellman.** il est utilisé pour créer une clé secrète partagée par les pairs qui n'ont pas été envoyé sur le réseau.
- **Lifetime 3600 :** Est la durée de vie de la clé de session (en secondes).

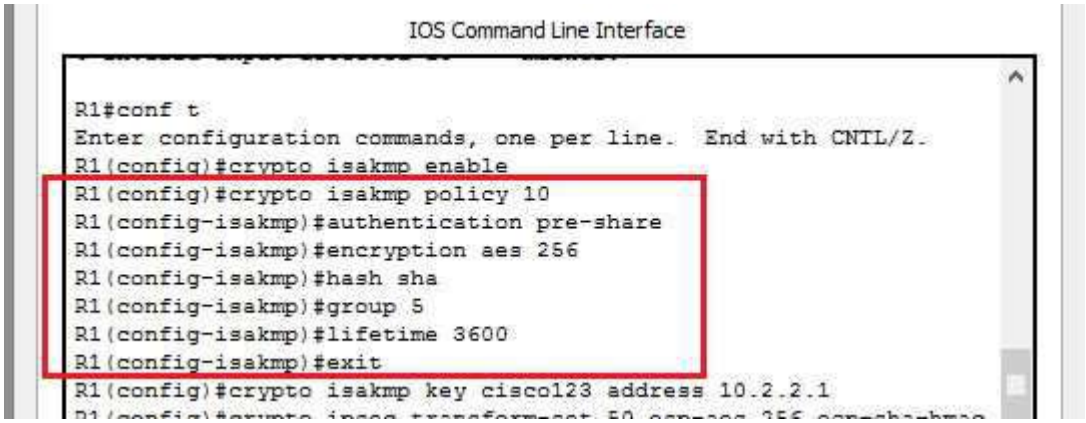


Figure 3.19 : Création d'une politique de négociation de clés sur le routeur R1

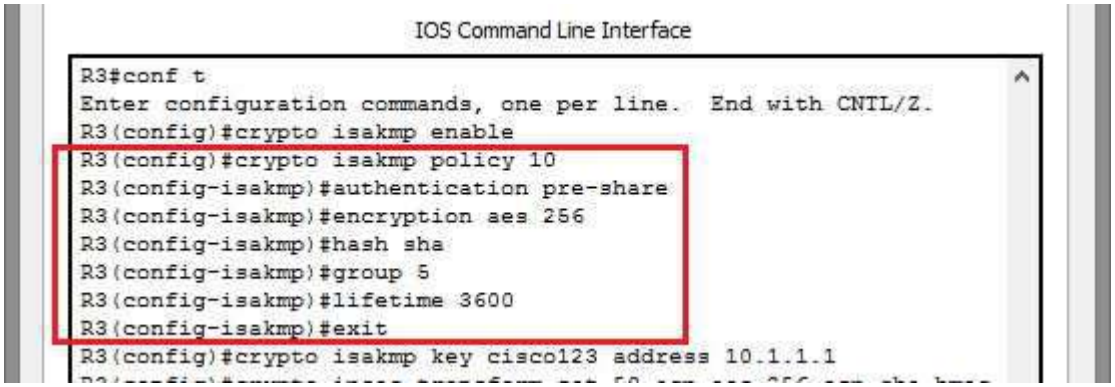


Figure 3.20 : Création d'une politique de négociation de clés sur le routeur R3

- **Etape 3 : La création de la clé pré-partagée (per-shared key) :**

Les clés pré-partagées sont utilisées comme méthode d'authentification dans la stratégie **IKE**, une clé doit être configurée sur chaque routeur des extrémités du tunnel **VPN.** Ces clés doivent correspondre pour que l'authentification soit réussie. Chaque adresse **IP** est utilisée pour configurer les mêmes **IKE** est également appelée adresse **IP** du point de terminaison **VPN** distant où cette commande est destiné vers l'adresse **IP** du pair distant.

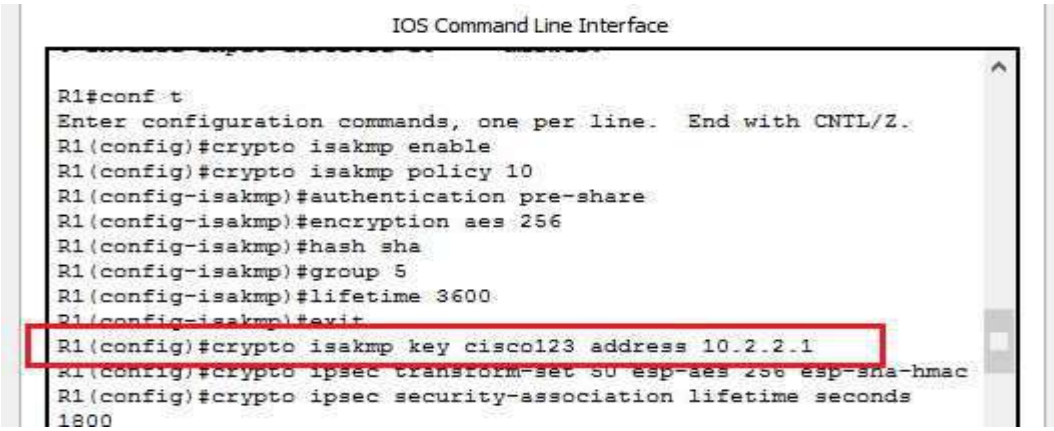


Figure 3.21 : Création de la clé pré-partagée sur le routeur R1

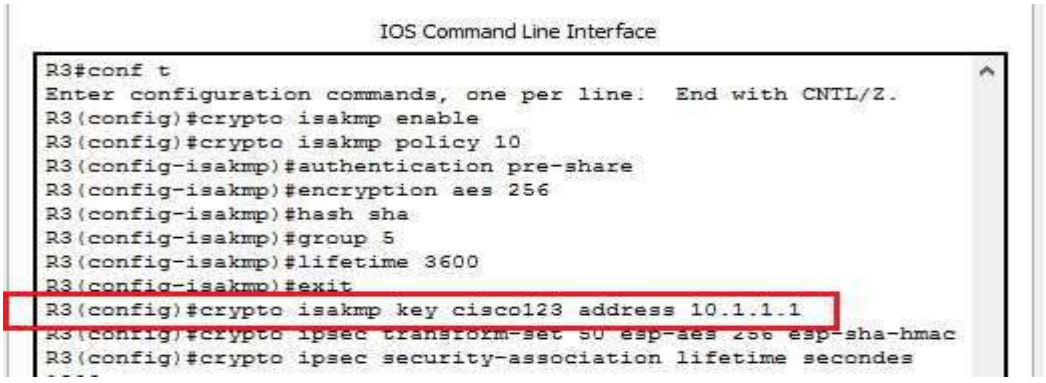


Figure 3.22 : Création de la clé pré-partagée sur le routeur R3

- **Etape 4 : Configuration d'IPsec :**

L'ensemble de transformations **IPsec** spécifie les algorithmes et fonctions cryptographiques (transformations) qu'un routeur utilise sur les paquets de données réels envoyés via le tunnel **IPsec**. Ces algorithmes incluent les services de chiffrement, d'encapsulation, d'authentification et d'intégrité des données qu'**IPsec** peut appliquer.

- **Phase 1 : Configuration de la méthode de cryptage des données « transform-set » :**

Sur **R1** et **R3**, on crée un ensemble de transformation utilisant un protocole de sécurité d'encapsulation **(ESP)** transformé avec un chiffrement **(AES 256)** et la fonction de hachage **SHA.**

Remarque :« esp-aes 256 » est la méthode de cryptage, et **« esp-sha-hmac »** est la méthode d'authentification.

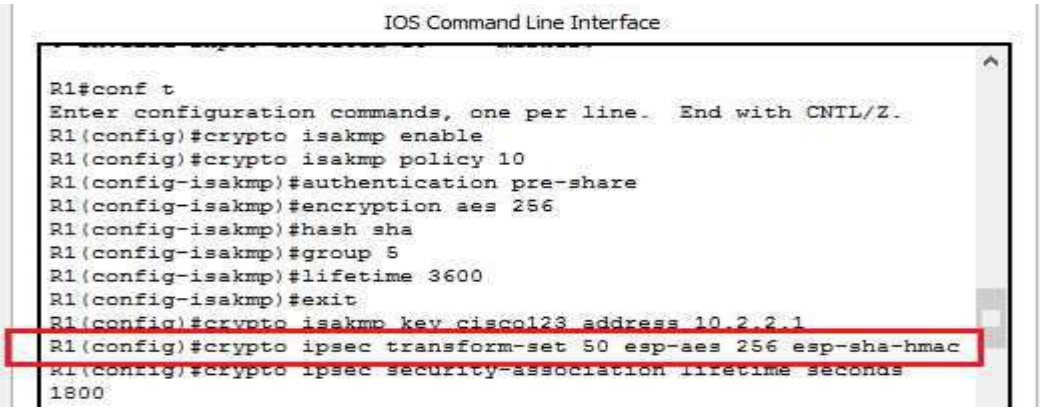


Figure 3.23 : Configuration de la trasform-set sur R1.

- **Phase 2 : Définition de la durée de vie de la clé pré-partagée :**

Sur R1 et R3, la durée de vie de la clé pré-partagée est exprimée en seconds (1800s).

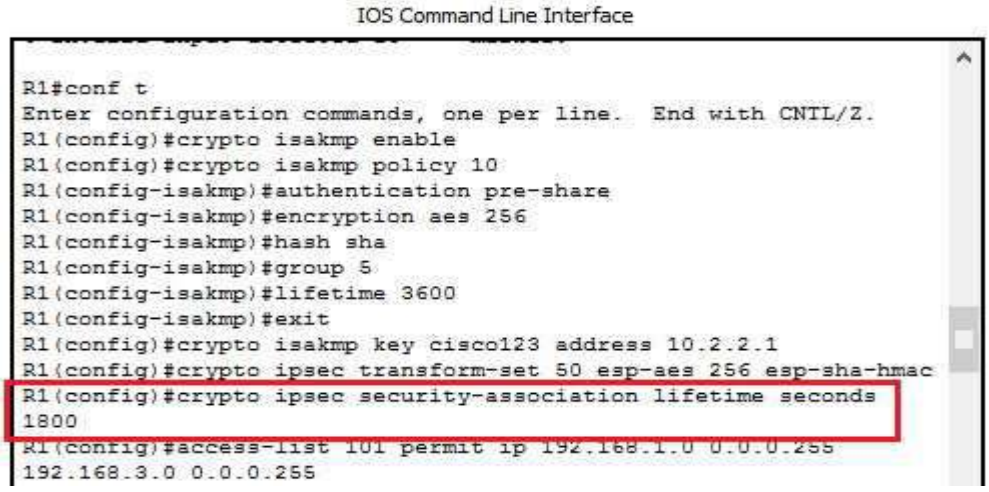


Figure 3.24 : Définition de la durée de vie de la clé pré-partagée

- **Phase 3 : Création des listes d'accès (access-lists) (ACL):**

Elles serviront à définir le trafic à trier par le tunnel **VPN**. Donc pour utiliser le cryptage **IPsec** avec le **VPN**, il est nécessaire de définir des listes d'accès étendues pour indiquer au routeur quel trafic est crypté.

Un paquet autorisé par une liste d'accès, utilisée pour définir le trafic **IPsec** est chiffré si la session **IPsec** est configurée correctement. Un paquet refusé par l'une de ces listes d'accès n'est pas abandonné, mais envoyé comme non chiffré. De plus, comme toute autre liste d'accès, il y a un refus implicite à la fin,

Dans notre cas, le trafic que nous souhaitons crypter est le trafic allant du **LAN Ethernet de R1** au **LAN Ethernet de R3**, ou l'inverse. Ces listes d'accès sont utilisées en sortie sur les interfaces de point de terminaison **VPN** et doivent refléter chaque autre.

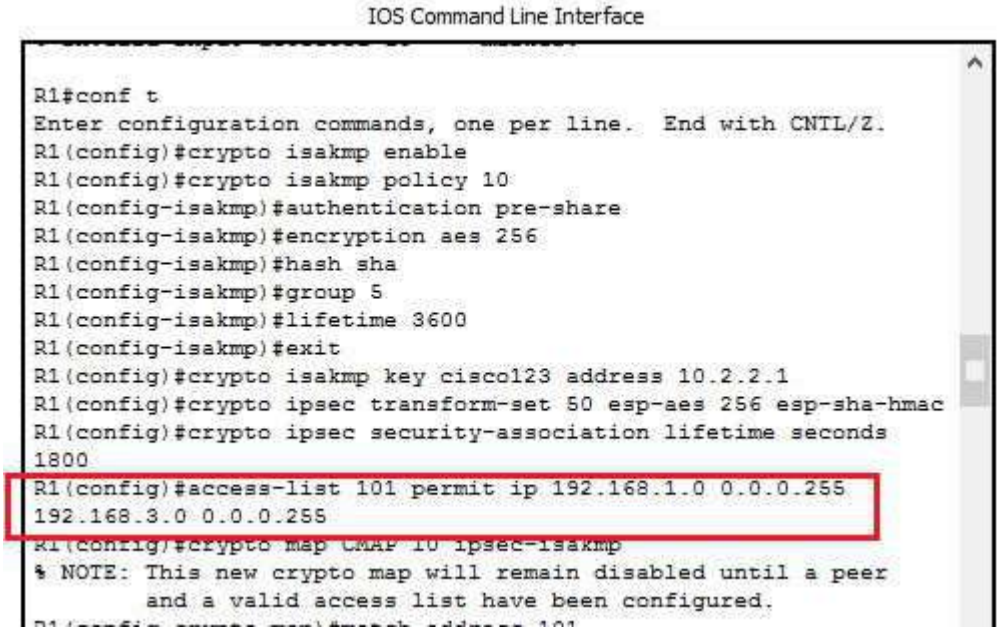


Figure 3.25 : création d'ACL sur R1

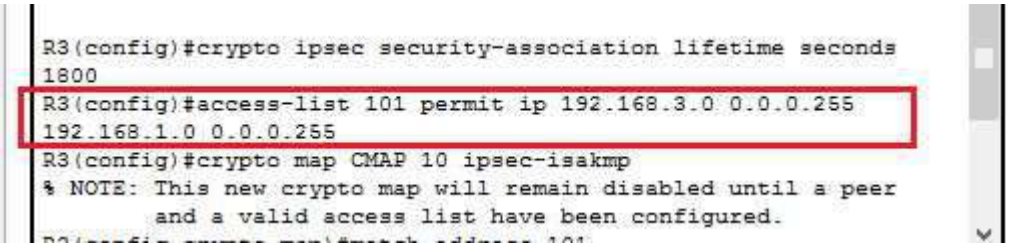


Figure 3.26 : Création d'ACL sur R3

- **Etape 5 : Création de la crypto-map :**

La carte cryptographique **« crypto-map »** associe le trafic qui correspond à une liste d'accès.

Nous créons une « **crypto-map** » nommée **CMAP** et choisissons **10** comme numéro de séquence et **IPsec-isakmp** comme type ce qui signifie que **IKE** est utilisé pour établir la sécurité **IPsec**.

Plusieurs instructions de **« crypto map »** peuvent appartiennent à la même « **crypto map »**, nous citons :

- La commande **« match addressaccess-list »** pour spécifier quelle liste d'accès définit le trafic à crypter.
- La commande **« set peer »** est utilisée sur chaque routeur du tunnel **VPN** accompagnée avec l'adresse **IP** de l'interface de l'autre point distant.
- On utilise la commande **«set transform-set »** pour que la « **crypto-map »** utilise la méthode de cryptage des données qu'on a déjà configurée.
- On utilise la commande **« set pfs »** pour défini le type de secret de transfert parfait, et on modifie également **l'IPsec** par défaut.
- On choisit **900** seconds comme durée de vie de l'association de sécurité.



Figure 3.27 : Création de la crypto-map sur R1

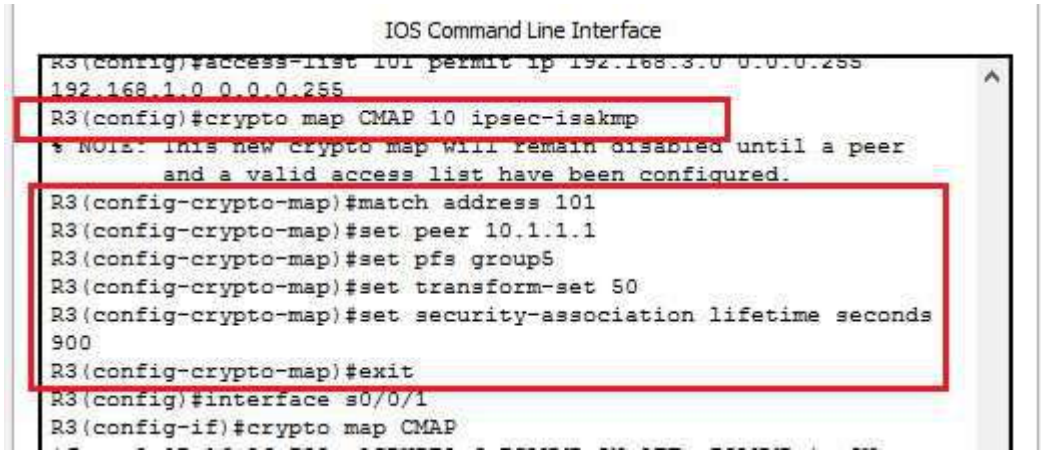


Figure 3.28 : Création de la crypto-map sur R3

- **Etape 6 : Application de la crypto-map :**

Après que la « **crypto-map »** est créée, elle peut être appliquée à une ou plusieurs interfaces. Les interfaces auxquelles il s'applique devraient être ceux qui font face au pair **IPsec.**

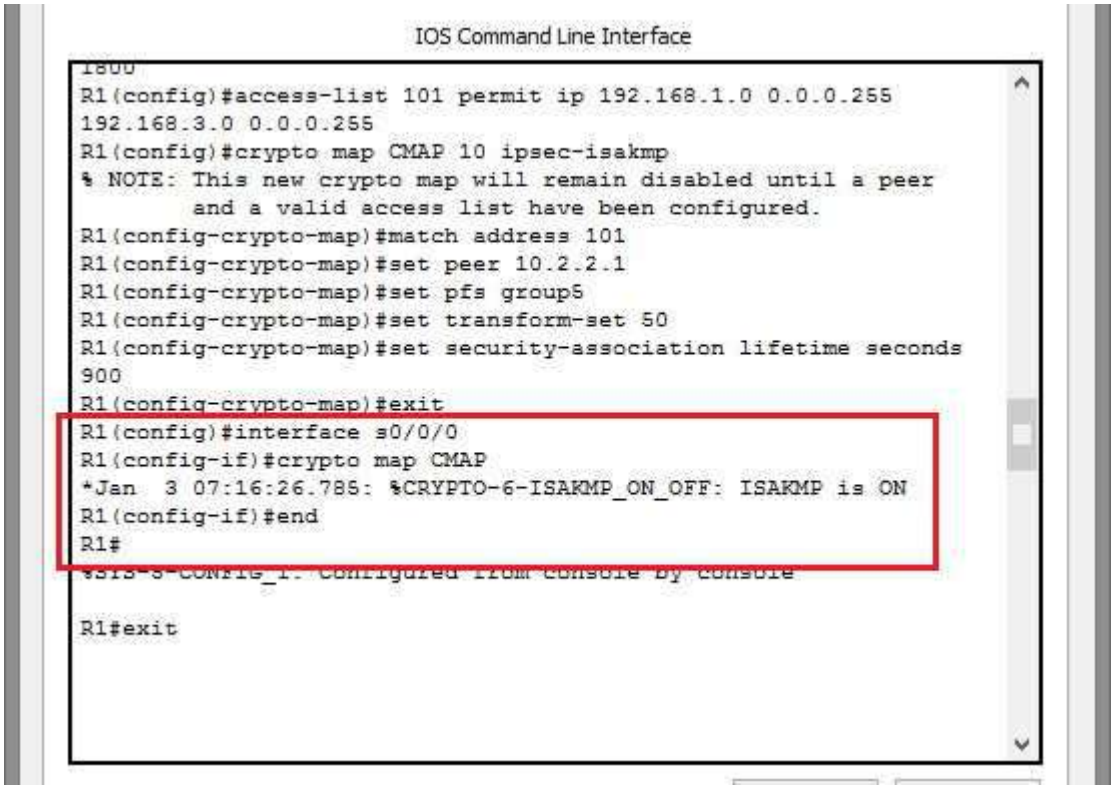


Figure 3.29 : Application de la crypto-mapà l'interface appropriée sur R1.

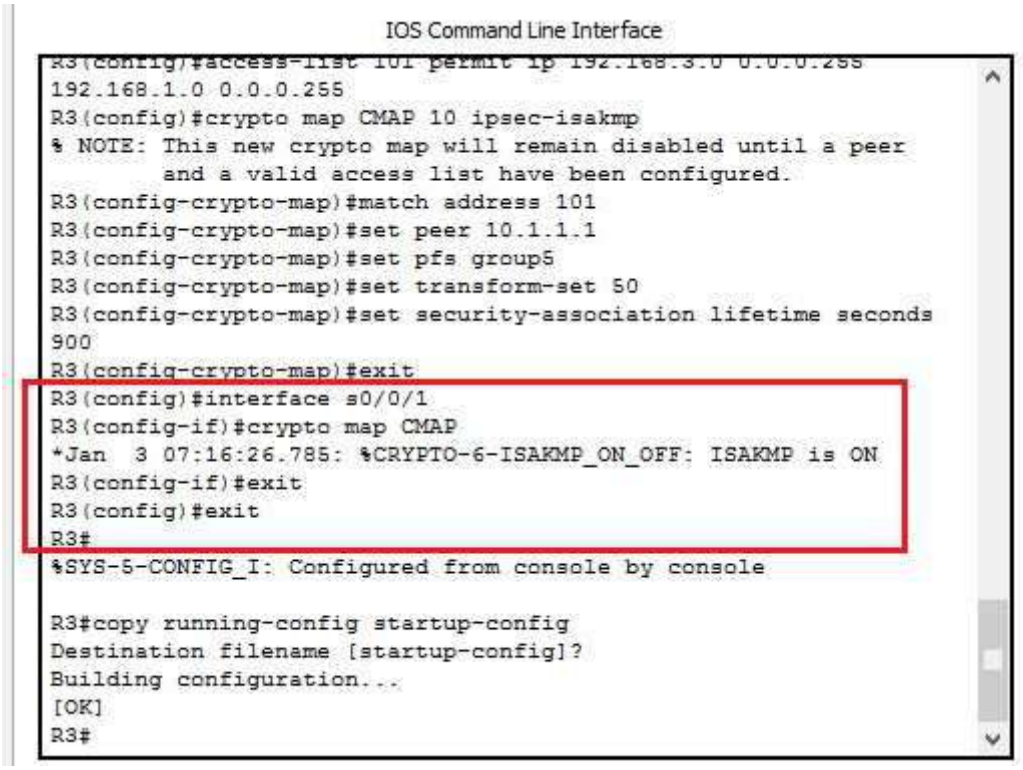


Figure 3.30 : Application de la crypto-map à l'interface appropriée sur R3.

3.5 Vérification du tunnel VPN :

3.5.1 Test de transfert des données :

Nous Exécutons la commande « **debugipospfevent** ». Pour voir les paquets **OSPF** bonjour passer entre **R1** et **R3**. Après on désactive le débogage avec la commande « **no debugipospfevent** » ou « **undebug all** ».

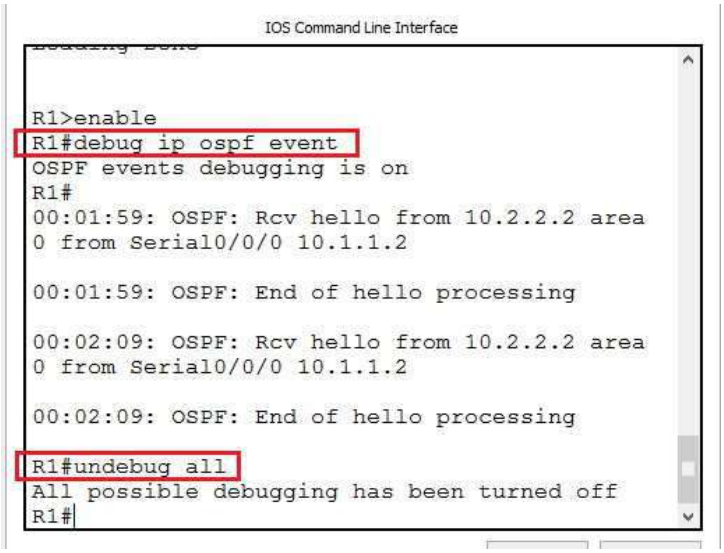


Figure 3.31: Test de transfert des données

3.5.2 Exécution de la commande Ping étendu :

La commande **Ping** étendu sert à permettre au utilisateur de choisir lui-même l'adresse source et destination malgré qu'il **Ping** à partir du **R1** dans ce cas on veut générer un trafic autorisé par **ACL(du 192.168.1.0 vers 192.168.3.0)** qui doit passer par le tunnel donc il doit être crypté par contre les premiers **Ping** génèrent un trafic non autorisé par **ACL** donc ce trafic est routé normal mais hors le tunnel et il n'est pas crypté (**exemple : de 10.1.1.1 vers 10.2.2.2 ou de 10.1.1.1 vers 192.168.3.1**).

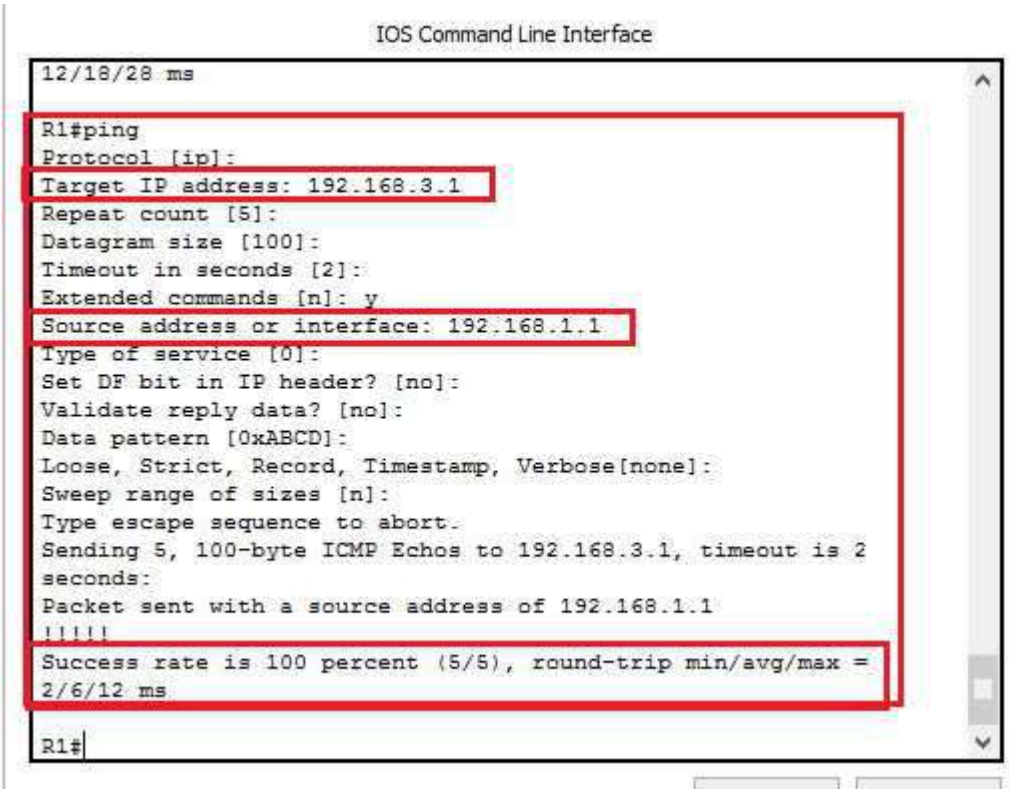


Figure 3.32 : Exécution de la commande Ping étendu

3.5.3 Vérification de la méthode de cryptage des données « transform-set » :

Nous utilisons la commande « **show crypto ipsectransform-set** » pour tester la configuration de la méthode de cryptage des données **‘’transform-set’’**.

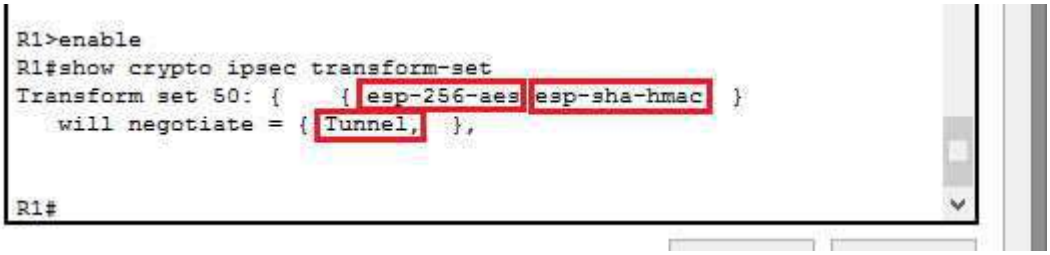


Figure 3.33 : Vérification de la « transform-set »

Le **« transform-set 50 »** utilise **‘’sha’’** pour l'authentification des paquets, **‘’256 aes’’** pour le chiffrement **‘’esp’’**. La transformation utilise le mode **tunnel**.

3.5.4 Vérification de la crypto-map :

On vérifie la création de la **crypto-map** avec la commande **« show crypto map »,** le résultat est présenté dans la figure ci-dessous.

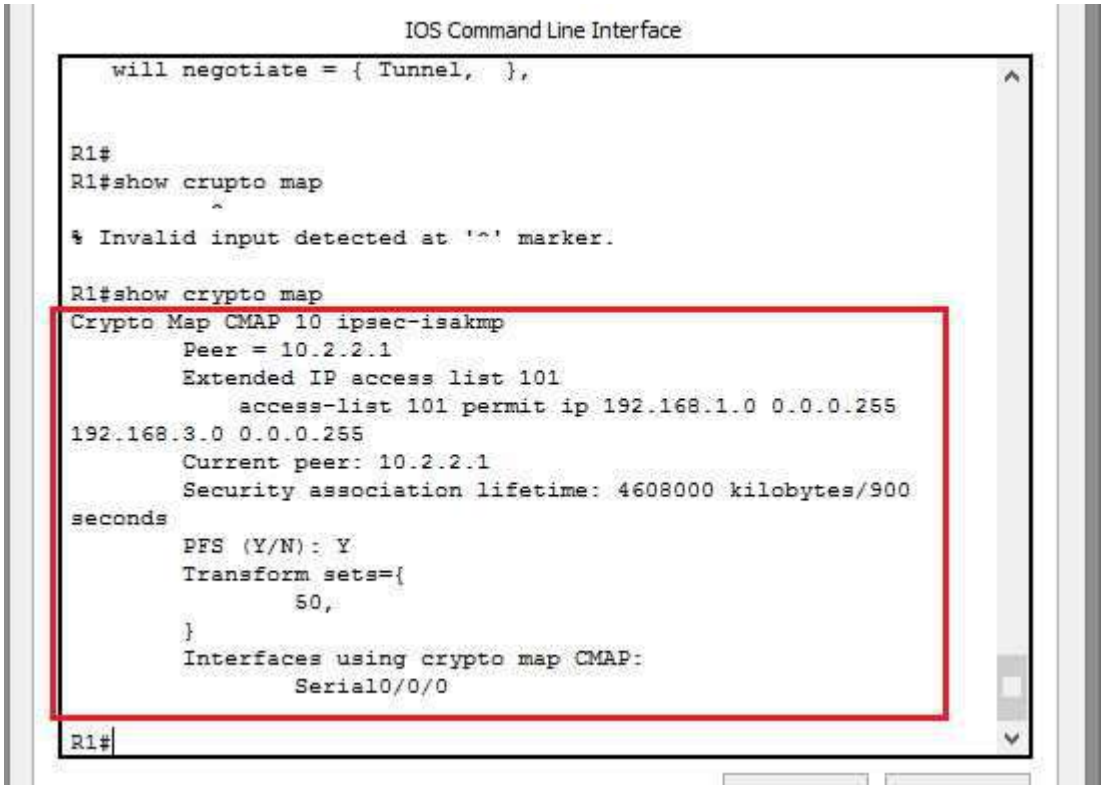


Figure 3.34 : Vérification de la crypto-map

La **crypto-map‘’CMAP’’** contient tous les éléments créés auparavant, comme les **access-lists**, les **transform-set** et l’interface appliquée à la **crypto-map**.

3.5.5 Vérification des paramètres d’IPsec :

A l’aide de la commande **« show crypto ipsec sa »** nous pouvons vérifier les paramètres **IPsec** configurés auparavant.

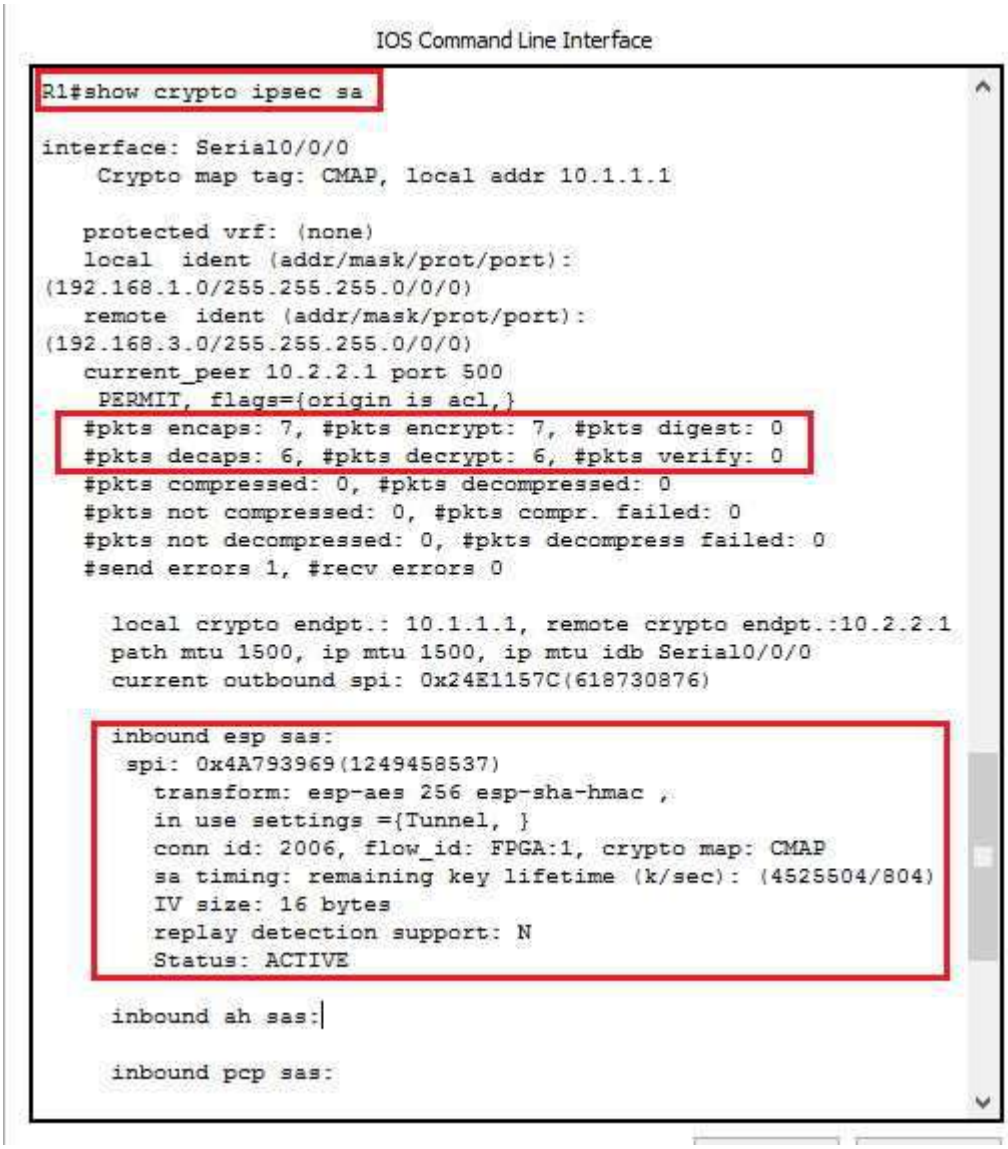


Figure 3.35 : Vérification des paramètres d'IPsec

3.5.6 Vérification des opérations ISAKMP :

On utilise la commande **« show crypto isakmp sa »,** le résultat est présenté dans la figure ci-dessous.

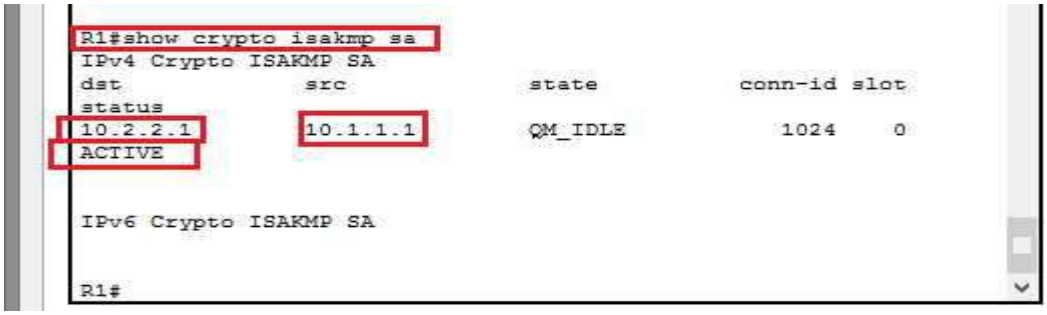


Figure 3.36 : Vérification des opérations ISAKMP.

On remarque sur la **figure 3.37** que les opérations d'**ISAKMP** sont **activées** entre les deux extrémités du tunnel **[R1 (10.1.1.1) et R (10.2.2.1)].**

3.6 Conclusion :

Dans ce chapitre on a défini une topologie réseau avec Packet Tracer avant d'établir une configuration de base sur les différents périphériques du réseau. Cette configuration basique contient les mots de passe, les adresses et le protocole de routage **OSPF**. Ensuit on a commencé à configurer une liaison **VPN** site à site sécurisé par le protocole **''IPsec''**, un chiffrement des données avec **''aes 256''**, une authentification avec la méthode **''esp-sha-hmac'',** les clés **pré-partagées** et les **ACL**s entre les différent sites.

Enfin, on a vérifié les résultats de notre configuration, en utilisant différentes commandes.

Conclusion générale

CONCLUSION GENERALE

Lors d'un échange des données entre des entités différentes, soit dans une même entreprise ou avec l'extérieur, la sécurité d'information et la confidentialité sont des exigences qui doivent être assurés.

À travers ce mémoire, on a essayé d'apporter une solution pour maitre cet échange en sécurité, alors nous avons abordé une solution basée sur les réseaux privés virtuels afin d'améliorer la sécurité de transfert des données sur un réseau.

En effet, nous avons présenté un travail divisé en trois chapitres, dont les deux premiers reposent sur une approche théorique et le dernier a été consacré à la réalisation.

Le premier chapitre est subdivisée en deux parties, la première a portée sur les généralités sur les réseaux, la deuxième est dédié au cyber sécurité et les différentes solutions connus dans le domaine.

Dans le second chapitre, nous avons abordé les généralités sur les VPNs et ces fonctionnalités, ainsi que les protocoles les plus utilisés.

La réalisation de notre solution proposée et ces résultats ont été exposés dans le dernier chapitre où nous avons présenté le Packet Tracer notre outil de simulation et la topologie réseau utilisés. Avant d'expliquer les différentes étapes de configuration, nous avons commencé avec la configuration de base qui contient les noms des périphériques constituants le réseau, les mots de passe et le protocole de routage OSPF utilisé.

Ensuite, on a passé à la configuration de VPN Ou nous avons utilisé le protocole de sécurité IPsec et d'autres différentes commandes utiles afin de créer un tunnel VPN. Après on a effectué une série de tests pour évaluer la configuration qu'a été faite et vérifier l'efficacité du VPN crée dans le but de sécuriser le trafic des données sur le réseau.

En fin, le travail sur l'idée exposée dans ce mémoire, nous a permis d'acquérir des connaissances très bénéfiques dans le domaine de la cybersécurité et de les approfondir, notamment pour la sécurité d'un réseau industriel grâce à l'implémentation d'un réseau privé virtuel (VPN).

Suite à cette étude, un certain nombre d'idées ont été dégagées. Ces dernières peuvent faire l'objet d'une suite de notre travail à savoir :

- Réaliser ce projet par configuration graphique à l'aide de logiciel **CCP** (**C**isco **C**onfiguration **P**rofessional).
- Avoir amélioré la sécurité de transfert des données en utilisant pas juste l'IPsec mais d'autres protocoles sur divers niveaux.

Bibliographie

Bibliographie :

[1] : JF.PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition dunod, 3 juin 2015.

[2] : https://www.netacad.com/fr Dernier accès mars 2020

[3] : P.ATELEN, Réseaux informatique notion fondamental, 3eme édition ENI, janvier 2009.

[4] : JF.PILLOU, Tout sur les systèmes d'information, Paris Dunod 2006.

[5] : https://www.securiteinfo.com Dernier accès mars 2020

[6] : http://www.linux-france.org Dernier accès mars 2020

[7] : KHELOUFI F, IKHLEF Y. Proposition de solution de sécurité pour le Réseau local de L'hôpital d'Amizour. Mémoire de Master d'Université Abderrahmane Mira de Béjaïa. Université Abderrahmane Mira de Béjaïa : 2016. 68 p.

[8] : S. GHERNAOUTI-HELIE, Sécurité informatique et réseaux, DUNOD, Paris, 2011.

[9] : http : //www-igm.univ-mlv.fr Dernier accès mai 2020

[10] : J.P ARCHIER, « Les VPN, fonctionnement et mise en œuvre », éditions eni, 2011 ;

[11] : BAA A, SAKER K. Mise en place d'une architecture VPN-IPsec pour le compte de CEVITAL. Mémoire de Master d'Université Abderrahmane Mira de Béjaïa. Université Abderrahmane Mira de Béjaïa : 2016. 59 p.

[12] : http://wallu.pagesperso-orange.fr/pag-mpls.htm Dernier accès mars 2020

[13] : Agence nationale de la sécurité des systèmes d'information. Secrétariat général de la défense et de la sécurité nationale Paris, N° DAT-NT-003/ANSSI/SDE/NP, le 3 août 2015,