الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

UNIVERSITE BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار –عنابـــــــــــة

Faculté : TECHNOLOGIE
Département : ELECTRONIQUE
Domaine : SCIENCES ET TECHNIQUES
Filière : Télécommunications
Spécialité : Réseaux et Télécommunications

Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème:

Configuration d'un tunnel VPN-ASA Sécurisé

Présenté par : *BEDJOU LAMISS* *BOUZIDI ANFEL*

Encadrant : *SAHRAOUI LEILA* *M.C.B* *UMBA*

Jury de Soutenance :

BRIK FATIMA	M.C.A	UMBA	Président
SAHRAOUI LEILA	M.C.B	UMBA	Encadrant
BOUCHAALA ALI	M.A.A	UMBA	Examinateur

Année Universitaire : 2021/2022

Remerciements

Nous remercions, Tout d'abord, ALLAH pour la volonté, la force, la santé et la Patience qu'il nous a donnée afin de réaliser ce travail.

Nous tenons à adresser nos plus chaleureux remerciements à notre Directrice de mémoire ***Mme SAHRAOUI Leila****, pour sa présence à tout moment, sa confiance et sa patience, ainsi que pour ses remarques pertinentes et ses Contributions considérables, tout au long de la réalisation de ce travail.*

Je remercie également les membres de jury de nous avoir fait l'honneur en acceptant d'examiner et de juger notre travail ***Melle BRIK Fatima*** *et* ***Mr BOUCHAALA Ali****.*

Enfin, Nous remerciements nos amis (es) et nos familles et tous ceux qui nous ont assistés de près ou de loin dans la réalisation de ce projet de fin d'étude.

Dédicaces

Je dédie ce travail :

*A mes très chère parents **FARIDA** et **NAWRI**pour leur amour inestimable, leur confiance, leur soutien, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer. Que Dieu les garde.*

*A mes frères **SKANDER** et **DEYA**. Et à tous les membres de ma famille pour leur appui et leur encouragement.*

*A mes copines **Rania** et **Safa** pour leurs encouragements permanents, et leur soutien moral.*

A tous mes Ami(e)s ainsi que toutes les personnes qui m'ont soutenu Et aidé tout au long de mes études.

Merci d'être toujours là pour moi.

BEDJOU LAMISS

Dédicace

De toute mon cœur je dédie ce modeste travail à toutes les personnes qui
compte beaucoup pour moi:
À mes chers parents Ali et Dounia qui m'ont donné leur soutien sans limite depuis toujours.
Le plus beau résultat au cours de mes années d'étude a été obtenu grâce à eux, que

Dieu les préserves pour moi

À mes chères frères Chamssou et Khaled et Malek qui ont toujours été présent pour moi.
À mes chère amis,
À Mon binôme Bedjou Lamiss pour sa collaboration au cours de la
réalisation de ce travail.
A tout ceux qui sont chères, proches à mon cœur et à tout ceux qui
m'ont aidé à réaliser ce travail.

Bouzidi Anfel

Résumé

La sécurité des systèmes informatique rend la communication et le partage de données fiable et moins vulnérable aux attaques cybercriminels.

Notre projet de fin d'étude concerne la mise en place et la configuration d'une architecture d'entreprise sécurisée à base de pare-feu ASA, ainsi que la création d'un tunnel VPN d'entreprise pour assurer la connexion à des sites distants et des clients nomades,

La configuration a été effectuée sous le logiciel Cisco Packet Tracer, des tests de connexion et de contrôle ont été réalisés pour assurer et garantir l'intégrité et la confidentialité des données avec le protocole IPsec.

Mots clés : Sécurité réseau, tunnel VPN, ASA, protocole IPsec

Abstract

The security of computer systems makes communication and data sharing reliable and less vulnerable to cybercriminal attacks.

Our project concerns the implementation and configuration of a secure business architecture based on ASA firewalls, as well as the creation of a business VPN tunnel to ensure connection to sites, remote and nomadic customers.

The configuration was carried out under the Cisco Packet Tracer software, connection and control tests were carried out to ensure and guarantee the integrity and confidentiality of the data with the IPsec protocol.

Keywords: Network security, VPN tunnel, ASA, IPsec protocol

ملخص

أمن أنظمة الكمبيوتر يجعل الاتصال ومشاركة البيانات موثوقة وأقل عرضة لهجمات المجرمين الإلكترونيين.

يتعلق مشروعنا بتنفيذ وتكوين بنية مؤسسية آمنة استنادًا إلى جدران الحماية ASA ، بالإضافة إلى إنشاء نفق VPN للشركة لضمان الاتصال بالمواقع البعيدة والعملاء الرحل.،

تم إجراء التكوين باستخدام برنامج Cisco Packet Tracer ، وتم إجراء اختبارات الاتصال والتحكم لضمان سلامة البيانات وسريتها باستخدام بروتوكول IPsec.

الكلمات الأساسية: أمان الشبكة ، ASA ، VPN ، بروتوكول IPsec

Liste des abréviations

ACL: Access Control List.

AES : Application Environment Service.

AH : Authentification Heade.

ASA : Adaptative Security Appliance.

CRL : Certificate Revocation List.

DHCP : Dynamique Host Configuration Protocol.

DMZ : Demilitarized Zone.

DNS : Domain Name System.

DES : Data Encryption Standard.

ESP : Encapsulating Security Payload.

FAI : Fournisseur d'Accès à Internet

FTP : File Transfer Protocol.

GRE : Generic Routing Encapsulation.

HTML: Hyper Text Markup Language.

HTTP : Hypertext Transfert Protocol.

SDN : Software Defined Network.

IKE : Internet Key Exchange.

IP : Internet Protocol.

IPSec : Internet Protocol Security.

IPS: Intrusion prevention systems.

IPv4 :Internet Protocol version 4.

IPv6 :Internet Protocol version 6.

ISAKMP : Internet Security Association and Key Managemet Protocol.

ISP : Internet Service Providers.

ICMP : Internet Control Message Protocol.

IETF : Internet Engineering Task Force.

L2F : Layer 2 Forwarding.

L2TP : Layer Two Tunneling Protocol.

LAC : L2TP Access Concentrator.

LAN : Local area network.

LER : Label Edge Router.

LNS : L2TP Network Server.

LSP : Label Switched Path.

LSR : Label Switching Router.

MPLS : Multi-Protocol Label Switching.

NAT : Network Address Translation.

NAS : Network Attached Storage.

PPTP : Point To Point Tunneling Protocol.

PPP : Point To Point Protocol.

PAT : Port Address Translation.

RAS : Remote Access Server.

SDN : Software Defined Network.

SHA : Secure Hash Algorithm.

SSH : Secure Shell.

SSL : Secure Socket Layer.

OSI : Open System Interconnection.

TCP : Transmission Control Protocol

UDP : User Datagram Protocol.

VPN : Virtual Private Network.

VLAN : Virtual Local Area Network.

WAN: Wide Area Network.

Table des figures :

Figure	Titre	N°
Figure 1.1	Analyse du trafic	5
Figure 1.2	Capture des paquets	5
Figure 1.3	Usurpation d'identité	6
Figure 1.4	Le Rejeu	7
Figure 1.5	Attaque Man-In-The-Middle	7
Figure 1.6	Les Pare –feu	10
Figure 2.1	Architecture d'un VPN d'accès	14
Figure 2.2	Architecture d'un VPN intranet	15
Figure 2.3	Architecture d'un VPN extranet	15
Figure 2.4	VPN en étoile	16
Figure 2.5	VPN maillé	16
Figure 2.6	VPN poste à poste	17
Figure 2.7	VPN de poste Nomade à site Entreprise	18
Figure 2.8	VPN site à site	19
Figure 2.9	PPTP : Encapsulation	22
Figure 2.10	Architecture L2TP	23
Figure 2.11	Position du SSL en couche	24
Figure 2.12	architecture du VPNSSL	26
Figure 2.13	Utilisation d'ESP en mode transport	28
Figure 3.1	Bâtiment de Cisco Systems	30
Figure 3.2	Logo du logiciel Cisco Packet Tracer	31
Figure 3.3	ASA (Adaptative Security Appliance)	32

Figure 3.4	Matériels utilisés	33
Figure 3.5	l’architecture de réseau	34
Figure 3.6	Création du réseau VPN	41

Liste des Tableaux

Tableau d'adressage ……35

Sommaire

Introduction Générale 1

Chapitre1 :Service Sécurité Réseaux

Introduction

1. Définition et objectifs de la sécurité réseau. 3

1.2. Les types de sécurité réseau 3

1.2.1. La sécurité physique 3

1.2.2. La sécurité logique 4

1.2.3. La sécurité administrative. 4

2. Les Attaques. 4

2.1. Définition 4

2.2. Le But 4

2.3. Les types d'attaque. 5

2.3.1. Les attaques passives 5

2.3.1.1. Les Attaque contre la communication. 6

2.4. Les attaques actives. 6

2.5. Autres Attaques. 7

2.5.1. Intrusion. 7

2.5.2. Le craquage de mot de passe 8

2.6 .Attaque logicielles 8

2.6.1 Les virus 8

2.6.2 Le cheval de Troie. 8

2.6.3 Les vers. 9

2.6.4 L'écoute du réseau (snifing) 9

3. Les mécanismes de défenses et méthodes de protections 9

3.1 Les Antivirus. 9

3.2. La cryptographie. 9

3.2.1. Chiffrement symétrique. 9

3.2.2. Chiffrement asymétrique 9

3.3. Les Pare –feu 10

3.3.1. Fonctionnement d'un système pare-feu. 10

3.4. Politique de défenses 11

4. Conclusion 12

Chapitre2 : Les Réseaux Privés Virtuel (VPN)

Introduction 13

1.Le réseau privé virtuel VPN 13

1.1 Définition 13

1.2. Les différents types de VPN 13

1.2.1. Le VPN d'accès 14

1.2.2. L'intranet VPN. 14

1.2.3 L'extranet VPN 15

1.3. Topologie des VPN 16

1.4. Les différentes architectures des VPN. 16

1.4.1 VPN d'entreprise 16

1.4.1.1 De poste à poste. 17

1.4.1.2 De poste à site 17

1.4.1. 3 De site à site 18

1.4.2. Intérêts d'un VPN. 19

1.4.3. Les caractéristiques d'un VPN. 20

1.4.4. Les avantages et les inconvénients de VPN.. 20

2. Les Protocoles. 21

2.1 Protocoles utilisés dans le VPN. 21

2.1.1. PPP 21

2.1.2. Le protocole PPTP 21

2.1.3. L2F. 22

2.1.4. L2TP. 22

2.1.5. Le protocole SSH 23

2.1.6. Le protocole SSL 23

2.1.6.1. Les fonctionnalités de SSL. 24

2.1.6.2. Architecture du VPN SSL 25

2.1.6.3. Les caractéristiques du VPN-SSL 26

2.2 Niveau 2 et 3. 27

2.2.1 MPLS 27

2.2.1.1 Fonctionnalité 27

2.2.1.2 Principes MPLS 27

2.2.2. IPSec. 27

2.2.2.1. Mécanismes de sécurité IPSEC 28

3. Conclusion 29

Chapitre 3 : Simulation et Tests

Introduction 30

1. Logiciel de simulation 30

1.2. Présentation du système Cisco Paquet Tracer 30

2. SIMULATION 31

2.1. Les types de matériels utilisés 31

2.1.2. Le Cisco ASA 5505. 31

2.1.3. Le principe des niveaux de sécurité 32

2.2. Le DMZ 33

3. l'architectured'un réseau sécurisé d'entreprise. 34

3.1. Composition du schéma deSimulation 34

3.2. Tableau d'adressage 35

3.3. Configuration des routeurs 35

3.3.1. Le routeur 1 35

3.3.2. Le routeur 2 36

3.3.3. Le routeur 3 36

3.3.4.Vérification de la connexion. 36

4. Configurationdu module L'ASA. 37

4.1. Configuration le nom d'hôte, le nom de domaine et le mot de passe 37

4.2. Configuration les interfaces inside etoutside 37

4.3. Configuration l'interface DMZ VLAN 3 37

4.4. Configuration de protocole de routage 38

4.5. Configuration du NAT 38

4.6. La configuration de L'ICMP 38

4.7. Configuration de DHCP 39

4.8. Configuration de ASA 39
4.8.1. Configuration de SSH 39
4.8.2. Établissez une session SSH 39
5.La configuration de l'ACL sur le serveur DMZ. 40
6. Création d'un réseau VPN pour une entreprise. 41
6.1. Création de VPN IPSec. 41
6.1.2. Configuration de ISAKMP 42
6.1.2.1. Première étape : Activation du protocole ISAKMP. 42
6.1.2.2. Deuxième étape : créer la policy-map 42
6.2. Création du tunnel VPN avec tunnel-group et la clé de partage 43
6.2.1 Tunnel group 43
6.2.2 La clé de partage 43
6.3. Création d'une transform-set 43
6.4. Configuration de la liste de contrôle d'accès (ACL) 44
6.5. Configuration de Crypto Map 44
6.6. Application de la Crypto Map à l'interface de sortie 45
7. Vérification 45
7.1. Vérification des opérations ISAKMP 45
7.2. Vérification du transform-set sur le routeur 3 46
7.3. Vérification de la crypto-map 46
8. Test de connexion 46
9. Conclusion. 47
Conclusion générale 48
Références Bibliographiques 49

La sécurité informatique est un concept de protection d'un système informatique contre toute violation, intrusion et dégradation ou vol de données au sein d'un système d'information. Avec l'essor de l'internet, et l'utilisation par la majorité des entreprises et des organisations de processus informatisés, les menaces visant les systèmes d'informations n'ont cessés d'augmenter et de se développer, faisant aujourd'hui de la sécurité informatique une nécessité majeure. La sécurité consiste à minimiser la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles, afin d'assurer la confidentialité, l'intégrité, et l'authentification du système [1].

En effet, Les attaques réalisées par des utilisateurs malveillants et visant à exploiter les vulnérabilités de système d'information sont de plus en plus fréquentes avec différent impact sur le système comme les attaques de communication, l'usurpation d'identité, les attaques logiciel, les virus,….etc. Afin de minimiser les effets des attaques, des mécanismes de défense ont été crée comme le cryptage, les antivirus et les pare-feu.

Les entreprises ont besoin de réseaux de communication qui assurent la connexion entre les sites distants, leurs partenaires et leurs clients de façon transparente. La communication entre les sites distants, se fait généralement via Internet. Malheureusement, les sites web ne sont pas très bien protégées et précaire aux attaques des cybercriminels. En plus des mécanismes de défenses, plusieurs méthodes de sécurité ont été conçues. Parmi ces méthodes, les VLAN, le NAT, les ACL, VPN, …etc. [2]

Effectivement de nombreuses sociétés et internautes choisissent d'utiliser des services VPN. En effet, le réseau privé virtuel VPN (Virtual Private Network) peut garantir la sécurité et la confidentialité des données, qui circulent de manière cryptée par Internet. Un réseau VPN facilite les communications entre l'entreprises et ses partenaires ou les communications internes d'une entreprise dans le cas d'un réseau d'entreprise réparti sur un, deux ou plusieurs sites distants.

Un VPN permet de s'étendre virtuellement, grâce à la technologie de tunnel, les données échangées dans le tunnel peuvent être sensibles et représente une cible de cyber-attaques. Afin de rendre le système sécurisé et fiable, on utilise différent protocole de cryptage tels que SSL/TLS, SSH et IPsec [3].

Dans ce concept, L'objet de ce projet est de réaliser un réseau sécurisé d'entreprise à base de pare-feu ASA (Adaptative Security Appliance), en utilisant le logiciel Cisco Packet Tracer, puis de créer un réseau VPN, donnant ainsi la possibilité d'accès aux sites distant, aux clients et partenaire nomades le pouvoir de ce connecté au système.

Notre mémoire est structuré autour de trois chapitres :

- le premier chapitre présente une étude générale sur la sécurité des réseaux informatique, en définissant les attaques et les mécanismes de défense.

- Le deuxième chapitre est consacré au réseau VPN ces caractéristiques, les différentes architectures du réseau, ainsi que les protocoles utilisés pour la sécurité.

- le troisième chapitre expose la mise en place et la configuration d'une architecture d'entreprise sécurisé à base de pare- feu ASA la deuxième partie est dédier à la création de réseau VPN d'entreprise pour assurer la connexion à distance. La simulation et les tests ont été réalisés avec le logiciel Cisco Packet Tracer.

Enfin nous terminerons notre document avec une conclusion générale et des perspectives.

CHAPITRE 1

SERVICE SÉCURITÉ RÉSEAUX

Introduction :

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

Dans ce chapitre nous allons présenter les attaques les plus fréquentes et les notions des sécurités, ainsi que les mécanismes de défenses.

1. Définition et objectifs de la sécurité réseau :

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

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles, ce qui implique la réalisation des fonctions essentielles suivantes [4] :

• **Confidentialité :** les données (et l'objet et les acteurs) de la communication ne peuvent pas être connues d'un tiers non-autorisé et seules les personnes autorisées aient accès aux ressources échangées.

• **Authenticité :** consistant à assurer que seules les personnes autorisées aient accès aux ressources. L'identité des acteurs de la communication est vérifiée.

• **Intégrité :** les données de la communication n'ont pas été altérées (garantir que les données sont bien celles que l'on croit être).

• **Non-répudiation :** les acteurs impliqués dans la communication ne peuvent nier y avoir participé.

• **Disponibilité :** les acteurs de la communication accèdent aux données dans de bonnes conditions.

1.2. Les types de sécurité réseau [5] :

On distingue trois catégories de sécurité réseau.

1.2.1. La sécurité physique :

La sécurité physique concerne tous les aspects liés à l'environnement dans lequel les ressources sont installées. Elle peut inclure :

- la sécurité physique des salles de serveurs, des périphériques réseau, etc.

- la prévention des accidents et des incendies.

- les systèmes de l'alimentation ininterrompue.

- la surveillance vidéo, etc**.**

1.2.2. La sécurité logique :

La sécurité logique fait référence à la mise en œuvre d'un système de contrôle d'accès, par logiciel, pour sécuriser les ressources. Elle peut inclure :

- l'application d'une stratégie de sécurité fiable pour les mots de passe.

- l'instauration d'un modèle d'accès s'appuyant sur l'authentification, l'autorisation et la traçabilité.

- la configuration correcte des pare-feu de réseau.

- l'installation des IPS (systèmes de prévention d'intrusion).

- l'utilisation des VPN (réseau privé virtuel), etc.

1.2.3. La sécurité administrative :

La sécurité administrative permet d'assurer le contrôle interne d'une organisation à l'aide d'un manuel des procédures.

Elle peut inclure :

-la prévention des erreurs et des fraudes.

- définir les responsabilités respectives des différents intervenants ou opérateurs.

- protéger l'intégrité des biens et des ressources de l'entreprise.

- assurer l'enregistrement de toutes les opérations concernant la manipulation du matériel.

- gérer rationnellement les biens de l'entreprise.

- assurer une gestion efficace et influente des activités.

2. Les Attaques :

2.1. Définition :

Une « attaque » est l'action d'exploiter les failles d'un système informatique à des fins non connues par un intrus dans le système est généralement nuisibles [6].

2.2. Le But :

- obtenir un accès au système.

- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.

- ramasser des informations personnelles sur un utilisateur.

-récupérer des données bancaires.

- s'informer sur l'organisation (entreprise de l'utilisateur, etc.).

-troubler le bon fonctionnement d'un service.

-utiliser le système de l'utilisateur comme « rebond » pour une attaque.

-utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée [7].

2.3. Les types d'attaque :

Les attaques peuvent être classées en deux catégories **: "passive" et "active".**

2.3.1. Les attaques passives :

Une attaque passive tente de prendre ou d'utiliser les informations du système, mais n'affecte pas les ressources du système, relativement difficile à détecter mais plus facile à prévenir. Ces attaques nuisent à la confidentialité des données [1] [6].

Il y a deux types d'attaques passives :

A. Analyse du trafic :

Dans une attaque d'analyse de trafic, l'attaquant essaie de détecter le chemin de communication entre l'expéditeur et le destinataire. L'analyse du trafic ne modifie pas les données.

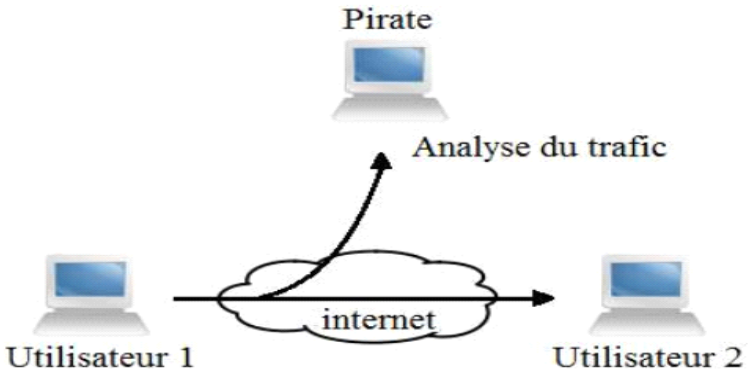


Figure 1.1 : Analyse du trafic

B. Capture des paquets :

Ce type d'attaque consiste à capturer le contenu d'un message (conversation téléphonique, email, fichiers ...) [6]. Pour empêcher la lecture des messages, on peut utiliser le cryptage [8].

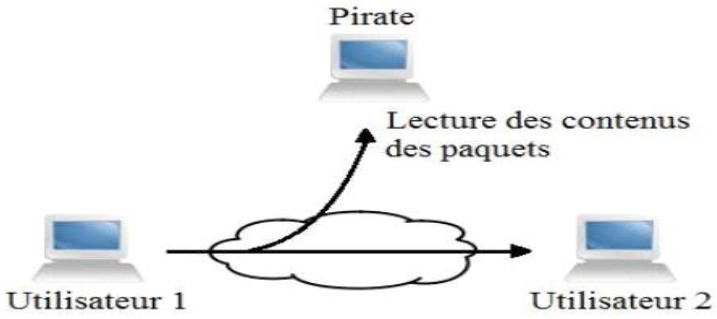


Figure 1.2: Capture des paquets

2.3.1.1. Les Attaques contre la communication :

Les Attaque contre la communication sont présentées comme des attaques passive puisque elles n'ont pas d'impact sur la modification de données.

C'est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations transmises ou stockées, l'information n'est pas altérées par celui qui en emporte une copie. Ces attaques sont donc indétectables par le système et peuvent seulement être relevées et contourné par des mesures préventives [9]. On y trouve :

A. L'interposition :

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

Exemple : le vol d'adresse (IP spoofing).

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

B. La Coupure :

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

2.4. Les attaques actives :

Dans le cas d'une attaque active, l'attaquant apporte quelques modifications aux données échangées et peut même générer de faux messages [8]. Ils sont plus faciles à détecter, mais souvent difficiles à prévenir [6].

Ils ont résultent différents types d'attaques, notamment :

A. Usurpation d'identité (Masquerading) :

Ce type d'attaque consiste à se faire passer pour un utilisateur autorisé dans un réseau [6].

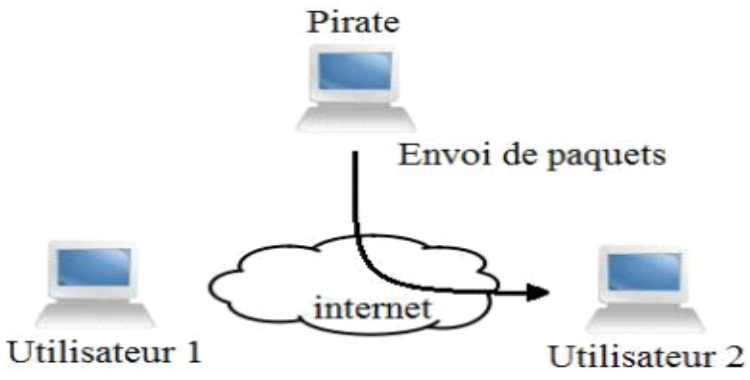


Figure 1.3 : Usurpation d'identité

B. Rejeu (Replay) :

Cette attaque consiste à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire [6].

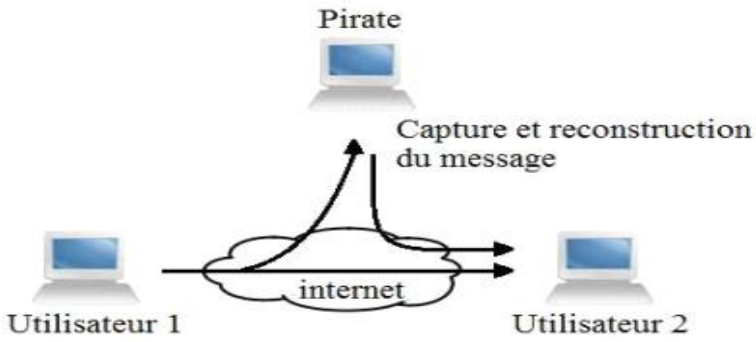


Figure 1.4 : Le Rejeu

C. L'homme au milieu (man-in-the-middle) :

Ce type d'attaque vise l'interception des communications entre deux parties (personne, ordinateur) [2] et la modification du contenu du message d'origine [6].

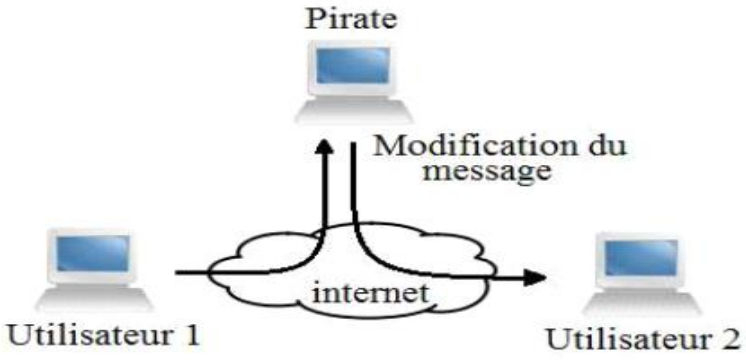


Figure 1.5: Attaque Man-In-The-Middle

E. Déni de service (Denial of service) :

Le déni de service est une attaque active visant à rendre un service indisponible. L'attaquant supprime tous les messages adressés à une destination particulière.

Une autre forme de déni de service est la perturbation du réseau entier, le surchargeant avec des messages inutiles d'une façon qui dégrade le rendement [6].

2.5. Autres Attaques :

2.5.1. Intrusion :

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

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

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

2.5.2. Le craquage de mot de passe :

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courant (et de leur variantes), ou par la méthode de brute force (toute les combinaisons sont essayées jusqu'à trouver la bonne), cette technique longue, souvent peut utilisée à moins de bénéficier de l'appui d'un très grand nombre de machine [9].

2.6. Attaque logicielles :

2.6.1 Les virus :

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

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

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

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

2.6.2 Le cheval de Troie :

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

- Récupération des mots de passe grâce à keylogger.
- Administration illégale à distance d'un ordinateur.
- Relais utilisé par les pirates pour effectuer des attaques.

- Serveur de spam (envoi en masse des e-mails).

2.6.3 Les vers :

Un ver est un programme indépendant, qui se copie d'ordinateur en ordinateur .La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter. Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur .Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus ; un ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles [9].

2.6.4 L'écoute du réseau (snifing) :

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

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

3. Les mécanismes de défenses et méthodes de protections :

3.1 Les Antivirus :

Se sont des logiciels permettant de détecter et de supprimé les virus informatiques sur n'importe quel support de stockage tel que : disque dur, disquette, CD-ROM, etc…

Ce type de logiciel sont géré par des mis à jours régulières pour détecter et mémorise les nouvelles formes de virus en circulation, afin d'être efficace [9].

3.2. La cryptographie :

La cryptographie est une composition de technique permettant de modifier et transformer les données pour dissimuler leur contenu et empêcher leur modification ou leur utilisation illégale.

Ceci est accessible, en effectuent des transformations inverses avec des algorithmes de déchiffrements. Dans le but de préserver la confidentialité des données et de garantir leur intégrité et leur authenticité. Cela est utilisé grâce à des clés de chiffrement de taille différentes pour protéger les données et les rendre moins sensible [9].

Les algorithmes de chiffrement se divisent en deux catégories :

3.2.1. Chiffrement symétrique :

Pour ce chiffrement l'émetteur et le récepteur utilisent la même clé secrète qui est appliquée à un algorithme donné pour chiffrer ou déchiffrer des données ou un texte.

Avec ce cryptage la clé secrète est transmise d'un bout à l'autre, c'est un risqué surtout avec un réseau non fiable comme internet car la clé peut ainsi être interceptée. Sa sécurité est dépendante du niveau de sécurité des clefs.

3.2.2. Chiffrement asymétrique :

Ce système se caractérise par la présence d'un concept pour chaque interlocuteur afin de communiquer des données. Chaque interlocuteur possède une bi-clé ou couple de clés calculées l'une en fonction de l'autre.

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

3.3. Les Pare-feu :

• **Le pare-feu** : appelé aussi firewall en anglais, C'est un concept logiciel ou matériel du réseau informatique contrôlant les communications qui circule. C'est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante les interfaces réseau (interne et externe).

Son rôle est de assurer le respect de la politique de sécurité du réseau, qui définisse quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).

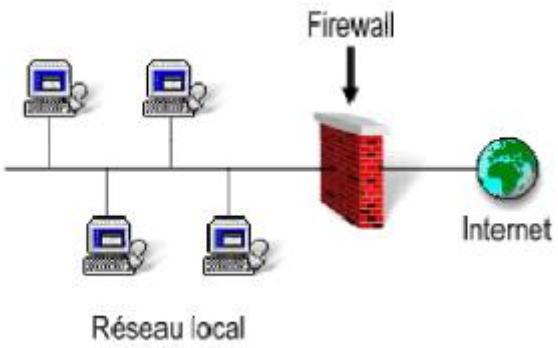


Figure 1.6 : Les Pare –feu

Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel systèmes pourvu que :

- La machine soit robuste pour traiter le trafic.
- Le système soit sécurisé.
- Seul le service de filtrage de paquets est permit fonctionne sur le serveur [10].

3.3.1. Fonctionnement d'un système pare-feu :

Un système pare-feu applique une politique de contrôle d'accès « ensembles de règles prédéfinies » entre les deux réseaux permettant de:

• Autoriser le paquet (allow).

• Bloquer le paquet (deny).

• De rejeter la demande de connexion sans avertir l'émetteur (drop).

Une raison pour l'utilisation de DROP plutôt que DENY est d'éviter de donner des informations sur les ports qui sont ouverts. Bloquer des paquets donne les raisons exactes pour lesquelles le paquet a été bloqué.

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité.

On distingue habituellement deux types de politiques de sécurité permettant soit:

• d'autoriser uniquement les communications ayant été explicitement autorisées :Principe d'interdiction par défaut (recommandée).

• d'empêcher les échanges qui ont été précisément interdits [11].

3.4. Politique de défenses :

• **La Signature numérique :** des données ajoutées pour vérifier l'intégrité ou l'origine des données.

• **le Bourrage de trafic :** données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic. C'est une technique de transmission permanente d'un flot d'informations inutiles pour cacher celles qui sont importantes [12].

• **la notarisation des échanges :** qui conserve une trace de l'échange auprès d'un tiers de confiance, pour prouver ultérieurement l'existence même de la communication [12].

• **Contrôle d'accès :** vérifie les droits d'accès d'un acteur aux données. Ce qui n'empêche pas l'exploitation une vulnérabilité du système.

• **Détection d'intrusion :** surveillé le réseau a fin de repéré les activités anormales ou suspectes. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime.

• **Journalisation ("logs") :** Enregistrement des activités de chaque acteur. Permet de constater et de détecter si des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.

• **Analyse des vulnérabilités ("Security audit"):** identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu en temps réel.

• **Contrôle du routage :** sécurisation du trafic et des chemins de communications (liens et équipements d'interconnexion).

• **Contrôle d'accès aux communications :** le moyen de communication n'est utilisé que par des interlocuteurs autorisés. Par VPN ou le tunnel.

• **Horodatage :** marquage sécurisé des instants significatifs.

• **Certification :** preuve d'un fait, d'un droit accordé.

• **Distribution de clefs :** distribution sécurisée des clés entre les entités concernées.

• **Authentification :** L'authentification est nécessaire au bon fonctionnement des autres mécanismes. Mais elle peut être nuisible au système, car authentifier un acteur peut se faire en utilisant une ou plusieurs de ses éléments :

Par mot de passe : la date anniversaire, le surnom ou prénom personnel.

Par une carte à puce : information biométrique (empreinte digitale, oculaire ou vocale).

• **La protection physique** : peut fournir une protection totale, mais qui peut être excessive. Par ex. isoler complètement son système est une solution qui peut être trop radicale [13].

4. Conclusion :

La sécurité informatique, consiste à s'assurer que les ressources matérielles ou logicielles d'une entreprises sont protégés et que les données partagés transite via un système fiable et sécurisé. Comme il existe une multitude de menaces et attaques qui rend les systèmes informatisés vulnérable, la sécurité est basés sur plusieurs mécanises et logiciel pour rendre le système fiable et assurer les connexions et le partage.

Dans ce concept nous avons présenté dans ce chapitre les attaques les plus fréquentes et les notions des sécurités, ainsi que les mécanismes de défenses.

CHAPITRE2

LES RÉSEAUX PRIVÉS VIRTUEL (VPN)

Introduction :

Ce chapitre est dédié au réseau privé virtuel (VPN), on présente ici les types de réseaux VPN, les différentes topologies et architecture du réseau ainsi que les protocoles associés.

Sur Internet, on ne sait pas par où passent les données car les chemins changent. Ces données peuvent donc être écoutées ou interceptées. Il n'est donc pas envisageable de faire connecter deux LAN entre eux par Internet sans moyen sécurisé pour l'acheminement des données échangées. Les réseaux LAN sont relativement sûr car ils sont quasiment toujours derrière une série de pare-feu ou coupés d'Internet, et que le chemin emprunté par les données ne quitte pas l'entreprise. Ils cherchent aussi à pouvoir se connecter à des sites distants et à communiquer avec leurs clients et partenaires de façon transparente. Cependant ils sont toutefois soumis à plusieurs attaques comme l'attaque dite « man-in-the- middle » par exemple.

Il existe alors deux solutions :

- relier les deux sites par une ligne spécialisée mais hors de prix.
- créer un réseau privé virtuel sécurisé autrement dit un VPN qui encapsule les données dans un tunnel crypté, permettant ainsi la connexion de façon sécurisée des ordinateurs distants à travers une liaison non fiable (Internet). C'est dans cette vision que de nombreuses entreprises l'utilisent afin de permettre à leurs utilisateurs, à distance et hors lieu de travail de se connecter au réseau d'entreprise [14].

1. Le réseau privé virtuel VPN :

1.1 Définition :

L'acronyme VPN correspond à Virtual Private Network, c'est-à-dire un réseau privé virtuel, est un tunnel sécurisé permettant la communication entre deux entités au travers un réseau peu sûrs comme l'internet.

Cette solution est moins coûteuse au niveau de la sécurisation dans le partage des informations entre un client et le site d'une entreprise par exemple. Le VPN se base sur des protocoles faisant appel au mécanisme de tunneling. Le protocole de tunneling encapsule les données en rajoutant une entête permettant le routage des trames dans le tunnel. Ces protocoles permettent d'établir une liaison sécurisée d'une extrémité à l'autre du tunnel VPN afin d'assurer la communication des données [15].

1.2. Les différents types de VPN [16] :

Parmi ces différents types on peut citer les :

- Le VPN d'accès
- Intranet VPN
- Extranet VPN

1.2.1. Le VPN d'accès :

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

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise.

- Sur la deuxième méthode ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs [17].

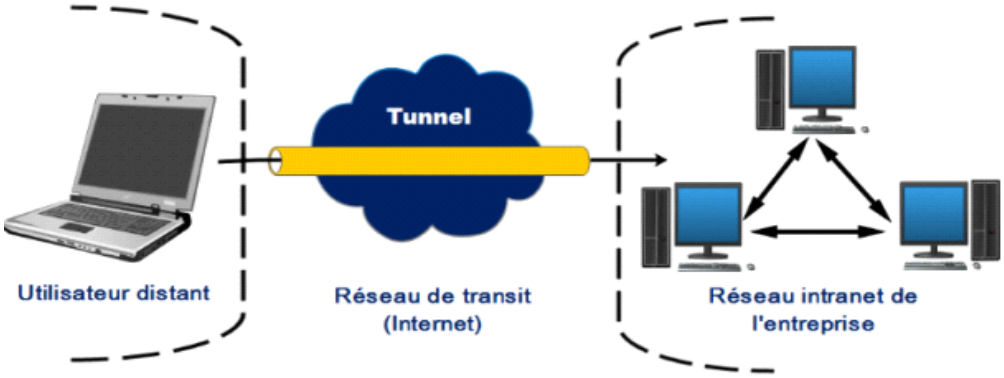


Figure 2.1 : Architecture d'un VPN d'accès [18]

1.2.2. L'intranet VPN :

Une entreprise possédant plusieurs sites distants utilise l'intranet VPN est pour relier au moins deux intranets entre eux toutes en garantissant la sécurité, la confidentialité et l'intégrité des données. Un VPN permet aux utilisateurs éloignés de se connecter à un réseau. Dans ce cas, on parle de l'intranet VPN car il s'agit aussi de connecter plusieurs clients distants à un site de l'entreprise [17].

Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux

paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite.

Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable [18].

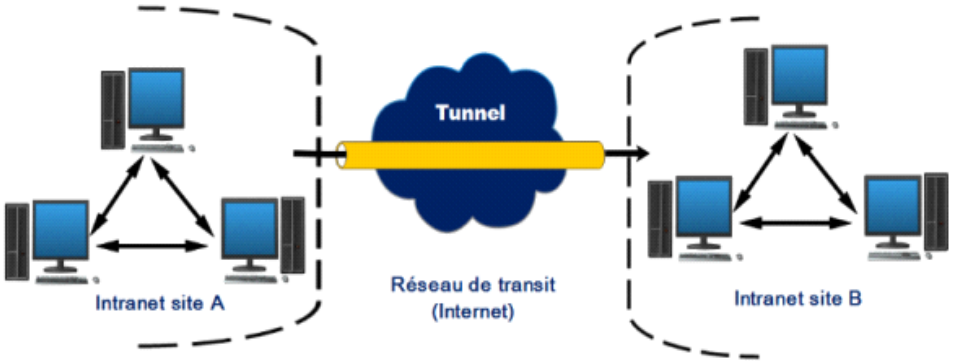


Figure 2.2 : Architecture d'un VPN intranet [18]

1.2.3 L'extranet VPN :

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

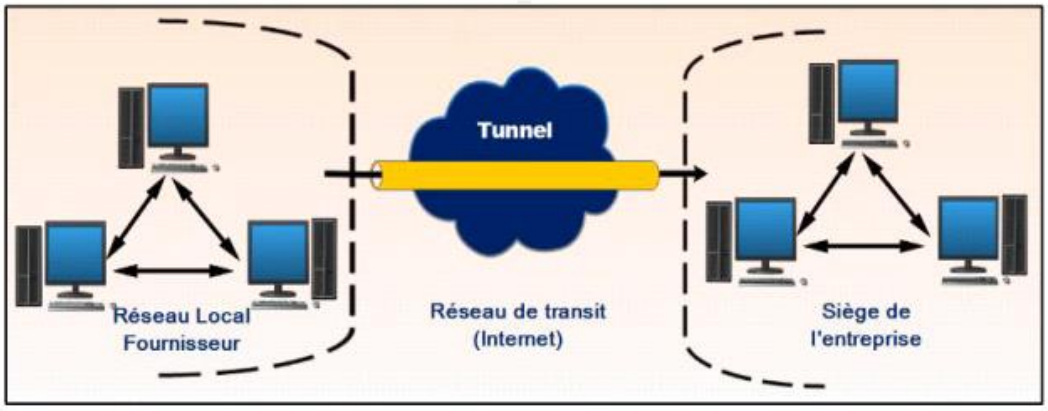


Figure 2.3 : Architecture d'un VPN extranet [18]

Les utilisateurs externes n'ont pas accès à l'ensemble de l'Intranet, mais seulement à certaines zones donc l'accès à l'Extranet est possible à partir de plusieurs endroits. L'accès dans un extranet est limité à certaines informations qui sont différents par rapport aux groupes et les rôles d'utilisateurs. Par exemple, les fournisseurs et les clients ont des droits d'accès différents.

1.3. Topologie des VPN :

Les réseaux VPN basé principalement sur Internet, utilise généralement des topologies en étoile, maillé ou partiellement maillé[19].

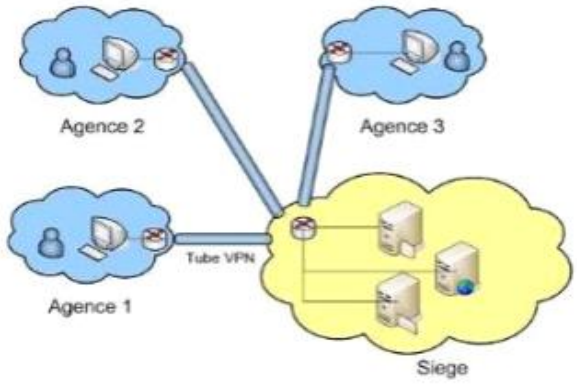


Figure 2.4 : VPN en étoile

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

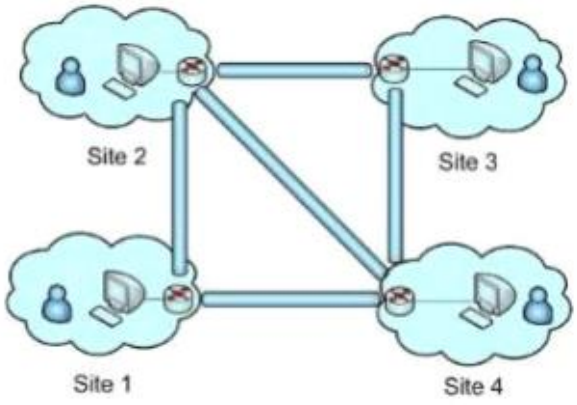


Figure 2.5: VPN maillé

Dans cette autre topologie les routeurs ou passerelles présents aux extrémités de chaque site seront considérés comme des serveurs d'accès distant, les ressources ici sont décentralisées sur chacun des sites autrement dit les employés pourront accéder aux informations présents sur tous les réseaux [19].

1.4. Les différentes architectures des VPN :

1.4.1. VPN d'entreprise :

Dans ce cas, l'entreprise garde le contrôle de l'établissement des VPN entre ses différents points de présence ainsi qu'entre ses postes situés à l'extérieur de l'entreprise et les sites principaux.

1.4.1.1. De poste à poste :

Le VPN poste à poste assure une conversation de bout en bout protéger. Il peut présenter des conversations se déroulant sur un réseau local, Il est donc particulièrement indiqué dans des contextes où le besoin de confidentialité, est primordial.

Il s'agit de mettre en relation deux serveurs. Ce cas d'utilisation exige le besoin de synchronisation de base de données entre deux serveurs d'une entreprise disposant de chaque côté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation (figure 2.6) [20].

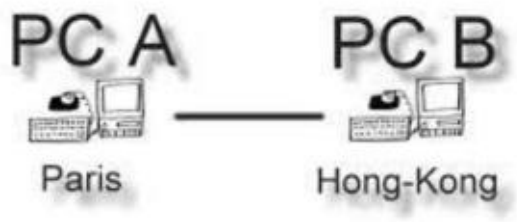


Figure 2.6 : VPN poste à poste

Le poste à poste désigne également une conversation entre deux postes d'utilisateurs que la connexion entre un poste de travail et un serveur. Généralement ce dernier cas est le plus souvent utilisé [21].

- **Avantages et inconvénients :**

Les données sont totalement protégées de bout en bout.

Par contre, il de nombreux inconvénients :

➢ Les performances en cas de fort débit sans affectées car le cryptage est uniquement logiciel.

➢ Quand les postes se situent sur des locaux sépares par internet il est nécessaire de pouvoir échanger des messages avec des protocoles et des ports 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 provoque des problèmes. [20]

1.4.1.2. De poste à site :

Un utilisateur distant a besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion Internet.

Le VPN poste à site présente plusieurs avantages. Il permet à n'importe quelle machine distante de joindre une ou plusieurs machines d'un autre réseau en utilisant seulement les adresses privées.

Il est donc utilisable pour joindre depuis un poste distant des ordinateurs mais aussi pour atteindre des imprimantes, des fax, des webcams. La demande est de plus en plus forte pour ce type de service avec le développement des cartes 3G et des fonctions modem des téléphones portables, les individus qui sont obligés à travailler à

distance depuis le train, l'hôtel, les déplacements des clients consolide également cette demande. [21]

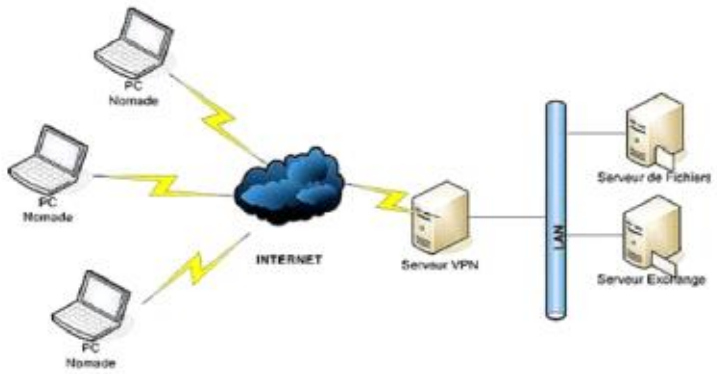


Figure 2.7 : VPN de poste Nomade à site Entreprise

- **Avantages et inconvénients :**

➢ L'accès du poste mobile peut se faire de n'importe quel point du monde avec un à accès Internet

Assurer la transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification. L'avantage est que le côté de la connexion entre le poste et le pare-feu de l'entreprise est chiffré. Par contre, celui entre le pare-feu et les postes du réseau local ne l'est pas puisque le cryptage, côté site central, est assuré par le pare-feu.

Les inconvénients de cette configuration :

➢ Nécessite une installation logicielle sur le poste distant.

➢ Le cryptage exige une charge au poste distant, cela peut dégrader les performances.

➢ Le cryptage n'est pas assuré au-delà du firewall du site central [20].

1.4.1.3. De site à site :

Le VPN site à site consiste à relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, d'un prestataire ou d'un client. Mais il faut également que tout ou une partie des machines des deux réseaux puissent communiquer avec celles du réseau distant en utilisant les adresses privées de chaque réseau.

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.

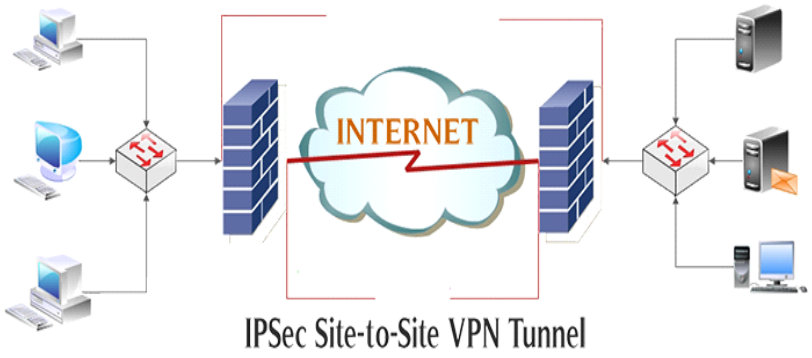


Figure 2.8: VPN site à site

Avantages et inconvénients :

- La prise en charge du Le cryptage par des processeurs spécialisés, pour de meilleures performances.
- les postes ne sont pas concernés par le cryptage donc aucun impact sur leurs performances.
- Contrôler facile du trafic autorisé.
- la possibilité d'initier les VPN des deux côté.

Mais cette configuration présente aussi quelques inconvénients :

- Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.
- les deux extrémités doivent être bien identifiées soit par une adresse IP publique fixe, soit par un nom référencé dans des DNS officiels pour l'établissement des VPN.

1.4.2. Intérêts d'un VPN :

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

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

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades.

-Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante.

- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet.

-Les connexions VPN permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, tel qu'Internet, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée.

-Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante [20].

1.4.3. Les caractéristiques d'un VPN :

Une solution du VPN devrait procurer les caractéristiques suivantes [21] [22] :

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

1.4.4. Les avantages et les inconvénients de VPN :

Les VPN disposent de nombreux avantages [17] :

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

Cependant ils peuvent aussi représenter quelques inconvénients :

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

2. Les Protocoles :

Plusieurs protocoles peuvent être utilisés dans le cas d'une sécurité réseau par VPN.

2.1. Protocoles utilisés dans le VPN :

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

2.1.1. PPP :

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

Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP [21].

2.1.2. Le protocole PPTP :

Le protocole PPTP (Point To Point Tunneling Protocol) tunnel du niveau 2 du modèle OSI, est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau

Le PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression.

Le principe de protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (GenericRouting Encapsulation) .[21]

Le tunnel PPTP se caractérise par :

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

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

PPTP : Encapsulation

Protocole qui utilise une connexion PPP à travers le réseau TCP/IP pour établir une connexion VPN: Le client PPTP se connecte à un serveur d'accès (NAS) chez l'ISP : Initiation d'une connexion PPP vers l'ISP pour accéder à Internet. Le NAS établit ensuite une connexion VPN utilisant PPTP vers le serveur VPN

Trois composants [19] :

- La connexion PPP.
- La Connexion de contrôle PPTP.
- Encapsulation et transmission des données PPTP.

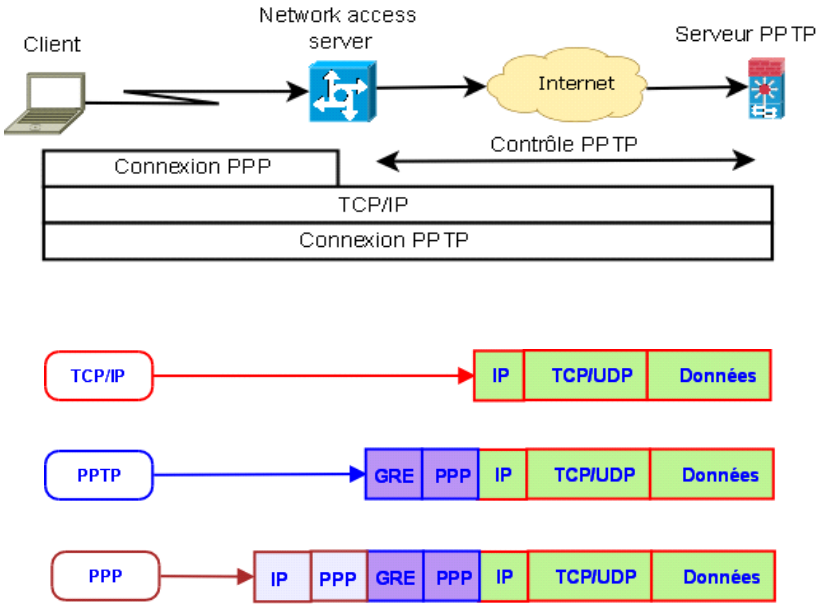


Figure 2.9 : PPTP : Encapsulation [19]

2.1.3. L2F :

L2F tunnel de niveau 2 du model OSI il a été développé par Cisco Systems comme une alternative au protocole PPTP. Comme ce dernier il s'appuie sur la couche deux de modèle OSI. Il est par contre beaucoup plus souple sur les protocoles réseaux utilisés. En effet, PPTP ne peut être encapsulée que dans des paquets IP alors que L2F peut aussi être encapsulé dans du X25 par exemple. Comme pour PPTP, L2F permet d'utilisation de différentes méthodes d'authentification [21].

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

2.1.4. L2TP :

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

L2TP repose sur deux concepts :

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

Un élément intéressant de L2TP est l'utilisation d'UDP. Ce qui est distingué par une vitesse d'acheminement supérieur [21].

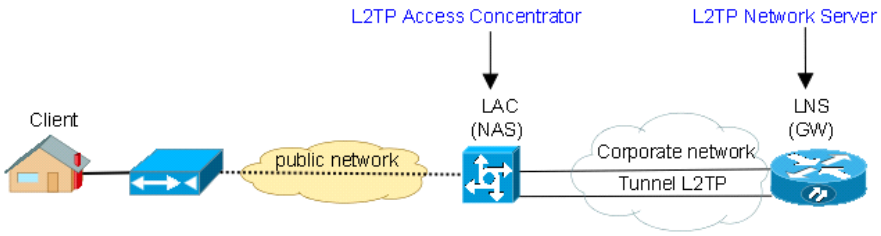


Figure 2.10 : Architecture L2TP [19]

2.1.5. Le protocole SSH :

SSH (securshel) est un tunnel de la couche 7 du model OSI, c'est un protocole permettant d'établir une cession interactive chiffré entre un client et un serveur. Ainsi, les flux d'information entre ces deux entités sont cryptés ce qui garantit la confidentialité.

De plus, il permet l'identification de la machine distante. L'algorithme utilisé pour la négociation des clés est RSA (dont le brevet a expiré aux USA ce qui permet une utilisation publique légale). Une fois l'échange des clés effectué, la communication entre les deux machines se fait en utilisant un chiffrage symétrique. Les principaux algorithmes utilisé dans SSH sont triple DES (3DES)

La plupart des fonctionnalités cryptographiques étant implémentés dans la bibliothèque Open SSL. La version du protocole SSH utilisé est la version 2, la première version de ce protocole souffrait d'une grosse faille de sécurité [10] [21].

2.1. 6. Le protocole SSL :

Récemment arrivé dans le monde des VPN, les VPN à base de SSL présente une alternative séduisante face aux technologies contraignantes que sont les VPN présentés jusqu'ici. Les VPN SSL présentent en effet le gros avantage de ne pas nécessiter du coté client plus qu'un navigateur Internet classique. En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur internet est implémenté en standard dans les navigateurs modernes.

SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application [23].

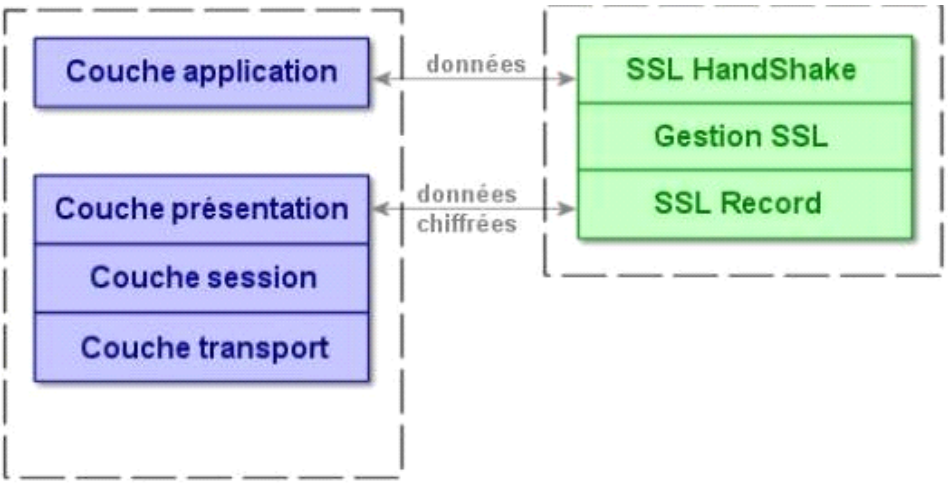


Figure 2.11 : Position du SSL en couche [23].

SSL procède deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

Il fournit un intérêt très important dans la mesure où coté client, il ne nécessite qu'un navigateur Internet Standard. Ce protocole est utilisé en standard pour les transactions sécurisées sur Internet. L'inconvénient néanmoins de ce type de protocole est qu'il se limite au protocole https [21].

2.1.6.1. Les fonctionnalités de SSL :

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser.

Le client commence par vérifier la validité du certificat du serveur. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client.

Le client vérifie aussi la date de validité du certificat et peut également consulter une CRL (Certificate Revocation List). Si toutes les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Le serveur peut alors envoyer un test au client, que le client doit signer avec sa clé privée correspondant à son propre certificat. Ceci est fait de façon à Ce que le serveur puisse authentifier le client.

De nombreux paramètres sont échangés durant cette phase : type de clé, valeur de la clé, algorithme de chiffrage …

La phase suivante consiste en l'échange de données cryptées (protocole SSL Records). Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases du protocole sont [23] :

- Segmentation des paquets en paquets de taille fixe.
- Compression (mais peu implémenté dans la réalité).
- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message, de données …

- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshake.
- Ajout d'un entête SSL au paquet.

Donc le SSL procède trois phases principales qui sont :

A. Authentification du serveur :

Qui permet à un utilisateur d'avoir une confirmation de l'identité du serveur. Cela est assuré par les méthodes de chiffrement à clés publique. Cette opération est indispensable, car le client doit pouvoir être certain de l'identité de son interlocuteur [21].

B. Authentification du client :

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

C. Chiffrement des données :

Garantir la confidentialité des données à la réception, car toutes les données qui transitent entre l'émetteur et le destinataire, sont chiffrées par l'émetteur. Assurer aussi leur intégrité grâce souvent à des mécanismes de Chiffrement mis en place entre l'émetteur et le récepteur [21].

2.1.6. 2. Architecture du VPN SSL

L'architecture du réseau présenté dans la figure suivante illustre le VPN-SSL typique et le tunnel VPN-SSL.

Le VPN-SSL typique des utilisateurs inclut, les associés et les clients, les gens connectés des à distance et utilisateurs mobiles.

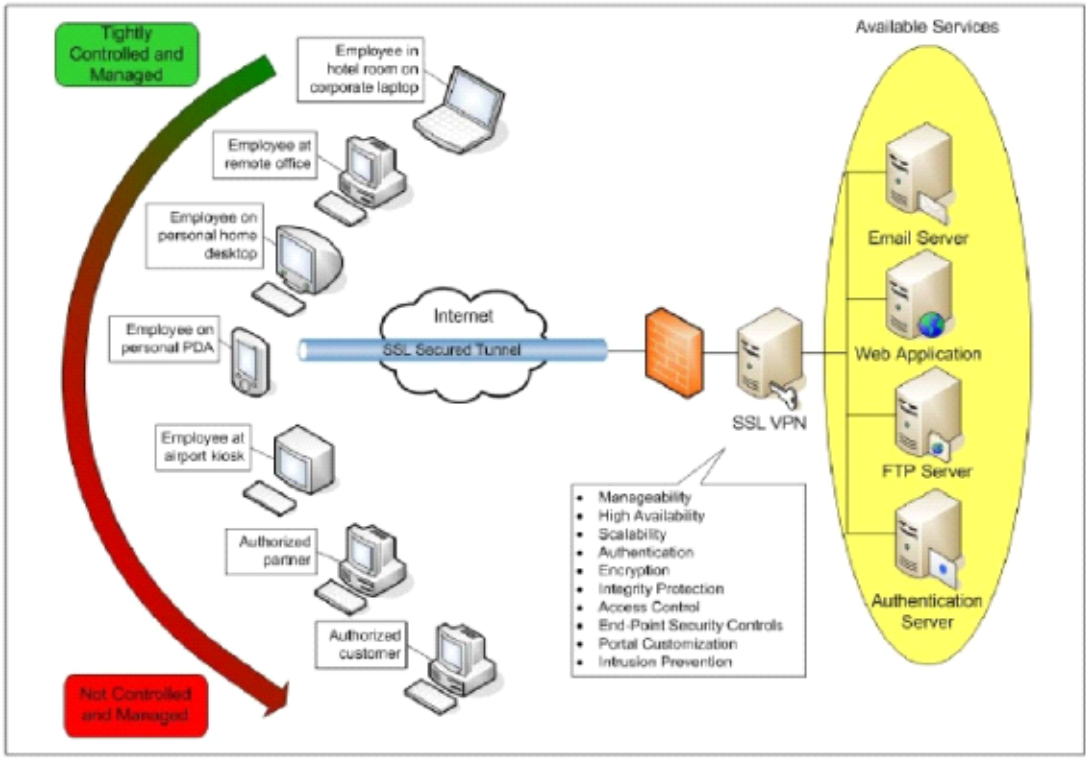


Figure 2.12 : Architecture du VPN SSL [10]

Le matériel des clients incluent les types divers de dispositifs, comme des kiosques publics, des ordinateurs individuels domestiques comme le pc, ou des smart-phones, qui peuvent ou ne peut pas être contrôlé ou géré par l'organisation. Le VPN incluant un emplacement, un aéroport, un café, ou une chambre d'hôtel. Tout le trafic est crypté. Le VPN-SSL en passerelle est le critère pour la connexion sécurisé et fournit des services divers [10].

2.1.6. 3. Les caractéristiques du VPN-SSL :

A. Possibilité de gestion :

La possibilité de gestion inclut la gestion du dispositif, le rapport de statut et l'enregistrement. Le VPN-SSL assure la disponibilité des services à tout moment. [10]

B. Adaptabilité :

L'adaptabilité est la capacité de supporter plus d'utilisateurs, des sessions simultanées et la sortie que VPN-SSL seul peut manipuler [10].

C. Personnalisation :

La personnalisation est la capacité de contrôler l'apparition du VPN-SSL que les utilisateurs voient quand ils accèdent au page web. Les tunnels personnalisés sont souvent nécessaires pour utiliser le VPN-SSL dans le cas des Smartphones [10].

2.2. Niveau 2 et 3 :

2.2.1 MPLS :

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. [10]

2.2.1.1 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. [10]

2.2.1.2. Principes MPLS :

Utilisant la permutation d'étiquettes, 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 niveau 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).[10]

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.

2.2.2. IPSec :

IPSEC (Internet Protocol Security) est une suite de protocoles normalisés par l'IETF qui fournit des services de sécurisation des données au niveau de la couche réseau. Il présente l'avantage d'être à la fois commun aux normes Ipv4 et Ipv6 [24].

Il assure les services ci-dessous [24] :

- **Confidentialité :** service qui consiste à rendre impossible l'interprétation de données si on n'en est pas le destinataire. C'est la fonction de chiffrement qui assure ce service en transformant des données intelligibles (en clair) en données inintelligibles (chiffrées).

- **Authentification :** service qui permet de s'assurer qu'une donnée provient bien de l'origine de laquelle elle est censée provenir.

-L'intégrité: service qui consiste à s'assurer qu'une donnée n'a pas été altérée accidentellement ou frauduleusement.

-Gestion des clés: mécanisme de négociation de la longueur des clés de chiffrement entre deux éléments IPSEC et d'échange de ces clés.

-Protection contre le rejeu : service qui permet d'empêcher les attaques consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau pour obtenir la même autorisation que ce paquet à entrer dans le réseau. Ce service est assuré par la présence d'un numéro de séquence.

2.2.2.1. Mécanismes de sécurité IPsec:

IPsec basé sur à deux mécanismes de sécurité pour le trafic IP :

➢AH (AuthentificationHeader).

➢ ESP (Encapsulation Security Payload).

• AH : Le protocole AH assure l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification, tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejet [25]. AH est approprié lorsque la confidentialité n'est pas requise ou n'est pas permise.

• ESP : Le protocole ESP assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel.

La technologie IPsec présente deux modes de fonctionnement qui sont :

-Le mode « transport » :

Dans le cas du mode transport, les données sont prises au niveau de la couche 4 du modèle OSI (couche transport). Elles sont cryptées et signées avant d'être transmise à la couche IP.

Etant donné que le mécanisme s'applique au niveau de la couche transport, il n'y a pas de masquage d'adresse c'est le principale défaut.

-Le mode « tunnel » :

Le mode tunnel, dans lequel l'encapsulation IPsec a eu lieu après que les données envoyées par l'application ont traversé la pile de protocole jusqu'à la couche IP incluses. Dans ce cas, il y a bien masquage des adresses.

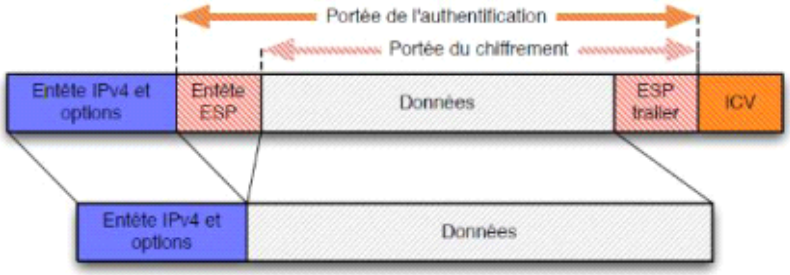


Figure 2.13 : Utilisation d'ESP en mode transport [16].

• Avantage:

- Une passerelle IPsec et IPsec sur les clients.

• Inconvénients :

- IPsec le système d'authentification est obligatoire ne permet d'identifier que des machines et non pas des utilisateurs.
- IPsec le cryptage et décryptage réduit les performances globales des réseaux. L'achat de périphériques dédiés, coûteux est souvent indispensable. Nécessite un bon débit réseau.

• Utilisation :

- Intranet, extranet (Sites à sites).

3. Conclusion :

Se connecté à l'internet via un réseau privé virtuel (VPN) représente une solution sécurisé qui repose sur un protocole appelé « Protocol de tunneling ». Effectivement le VPN peut garantir la sécurité et la confidentialité des données qui circulent de manière cryptée sur le réseau avec les différents protocoles de cryptage comme, le SSL et l'IPsec. Dans ce chapitre nous avons exposé les caractéristiques du réseau VPN, les différentes architectures VPN et les protocoles de cryptages les plus utilisés dans ce système.

CHAPITRE 3

SIMULATION ET TESTS

Introduction :

Ce chapitre présente la partie simulation de notre travail, ou nous allons procéder à la configuration d'un réseau de société sécurisé à base pare-feu (ASA). En suite un tunnel VPN est créé pour donner la possibilité et la permission à des clients d'accéder avec un réseau privé et d'assurer l'échange de données entre eux d'une façon sécurisé à base de protocole de cryptage. La simulation a été réalisée avec le logiciel Cisco Packet Tracer.

1. Logiciel de simulation :

2.1. Présentation du système Cisco paquet tracer:

Cisco Systems est une société informatique américaine spécialisée dans le matériel réseau tel que les routeurs et les commutateurs Ethernet et opère dans le monde entier. Fondée en 1984 par Leonard Bosack et Sandra Lerner, elle est basée à San Jose, en Californie [26].

Figure 3.1 : Bâtiment de Cisco Systems

Packet Tracer est un logiciel développé par le CISCO qui permet de construire un réseau physique virtuel et de simuler le comportement des protocoles sur le réseau.

L'utilisateur peut bâtir son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ensuite ces équipements doivent être reliés via des connexions (câbles divers, Point d'accès ...ect).Lorsque l'ensemble des équipements soient reliés, il est possible chacun d'entre eux, de configurer les adresses IP et les services disponibles. [26]

Figure 3.2 : Logo du logiciel Cisco Packet Tracer

2. Simulation :

2.1. Les types de matériels utilisés :

- Les routeurs : Ils fonctionnent au niveau réseau (couche 3 du modèle OSI), son objectif est l'interconnexion des sous-réseaux géo-localisés ou distants à travers des liaisons longues distances.

- Les commutateurs: aussi appelé SWITCH, fonctionnent au niveau Liaison, il a la mêmes fonction qu'un pont mais utilisent des ports dédiés et non partagés.

- Les connexions ou appelé (câblage), on trouve plusieurs types tels que la fibre optique, câble coaxial, câble droit, câble série, etc.

- Les ordinateurs.

- Les réseaux étendus (WAN).

- la sécurité (Cisco ASA 5505).

-Le DMZ assure la connexion du réseau interne pour le besoin d'accès externe.

2.1.2. Le Cisco ASA 5505 (pare-feu) : est une Appliance de sécurité complète pour les petites entreprises. Il comporte un pare-feu de haute performance, SSL VPN, IPsec VPN et plusieurs services réseaux dans une même Appliance. C'est un module de prévention d'intrusion qui surveille et effectue des analyses en temps réel du trafic. Lorsque le système repère une activité non-autorisée, il peut mettre fin à la connexion en cours, bloquer l'hôte attaquant, enregistrer l'incident, et envoyer une alerte au gérant du réseau.

Figure 3.3 : ASA (Adaptative Security Appliance)

2.1.3. Le principe des niveaux de sécurité : Les ASA sont des périphériques orientés Sécurité. Associe une philosophie avec des commandes les plus basiques pour la configuration des interfaces. Ainsi, à chaque interface est associé un nom et un niveau de sécurité, qui déterminent les politiques de sécurité associées. Les niveaux de sécurité vont de 0 à 100.

Le niveau de sécurité 100 correspond à une confiance totale et un besoin accru de protéger ce réseau, exemple : réseau interne tandis que 0 correspond à un réseau dont on se méfie et dont la protection ne nous concerne pas exemple : Internet. Le nom **Inside** à une interface, on lui attribue automatiquement un niveau de sécurité de 100. Tout autre nom d'interface, notamment **Outside**, implique un niveau de sécurité de 0. Toutefois, il est possible de modifier le niveau de sécurité manuellement.

Les niveaux de sécurité des interfaces influent sur les points suivants : Accès réseau : par défaut seules les communications depuis les interfaces de plus haut niveau vers celle de plus bas niveau peuvent avoir lieu (ces communications sont sortantes).

Si les interfaces ont le même niveau, le trafic peut être autorisé entre elles avec la commande same security-traffic permit inter-interface :

- Moteurs d'inspection : les comportements de certains moteurs d'inspection s'adaptent en fonction du niveau de Filtrage, les filtrages HTTP et FTP s'appliquent uniquement aux connexions sortantes.
- Contrôle NAT : doit être configuré pour les connexions sortantes.

- Commande est ablished : cette commande autorise les communications des interfaces de plus bas niveau vers celles de plus haut niveau si la connexion a été établie auparavant par l'interface de plus haut niveau. [27] [28]

Le Cisco ASA 5525-X C'est un Dispositif de sécurité. Il s'inscrit dans la phase Adaptive Threat Defense de la stratégie Self-Defending Network (SDN) de Cisco, et comprend les modèles ASA 5510, 5520 et 5540. Conçus pour couvrir les besoins des entreprises de toute taille, ces innovations offrent une administration unifiée et des capacités d'évolution pour le fonctionnement de services simultanés. Les ASA 5525-x apportent des services de défense adaptative contre les menaces et comprennent des défenses, la sécurité d'application et le confinement ainsi que le contrôle réseau. Elles assurent ainsi une protection unifiée et approfondie des ressources critiques [27] [28].

2.2. Le DMZ : Lorsque certaines machines du réseau interne ont besoin d'être accessible de l'extérieur (comme c'est le cas par exemple pour un serveur web, un serveur de messagerie, un serveur FTP public, ...) il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans compromettre la sécurité interne. On parle ainsi de zone démilitarisé (souvent notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. Ceci se crée en isolant les équipements du réseau (en restant connecté) et y assigné des commandes ACL pour régler ses communications avec le reste du réseau. [30]

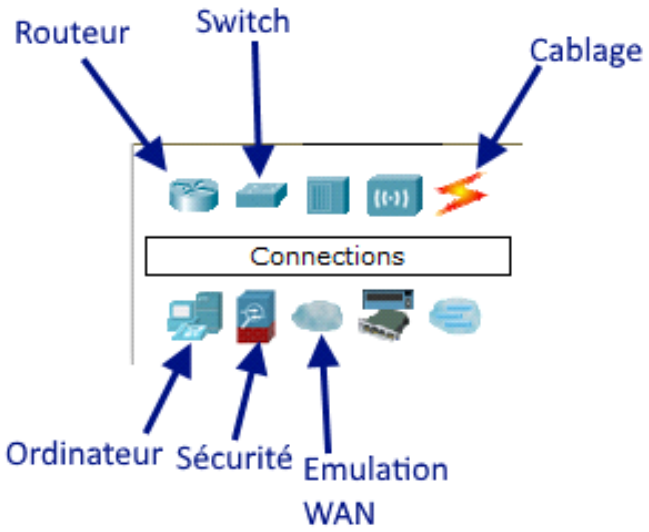


Figure 3.4 : Matériels utilisés.

3. l'architecture d'un réseau sécurisé d'entreprise :

Ce schéma est basé sur un dispositif de sécurité ASA (pare-feu) autour du quel est caractérisé un système **Inside** et un système **Outside**.

3.1. Composition du schéma de simulation :

- ASA 5505.
- Un système Outside qui possède trois Router et Switch et un PC.
- Un système Inside qui contient deux volets : Switch et un pc, une DMZ conçu avec un Switch et server.

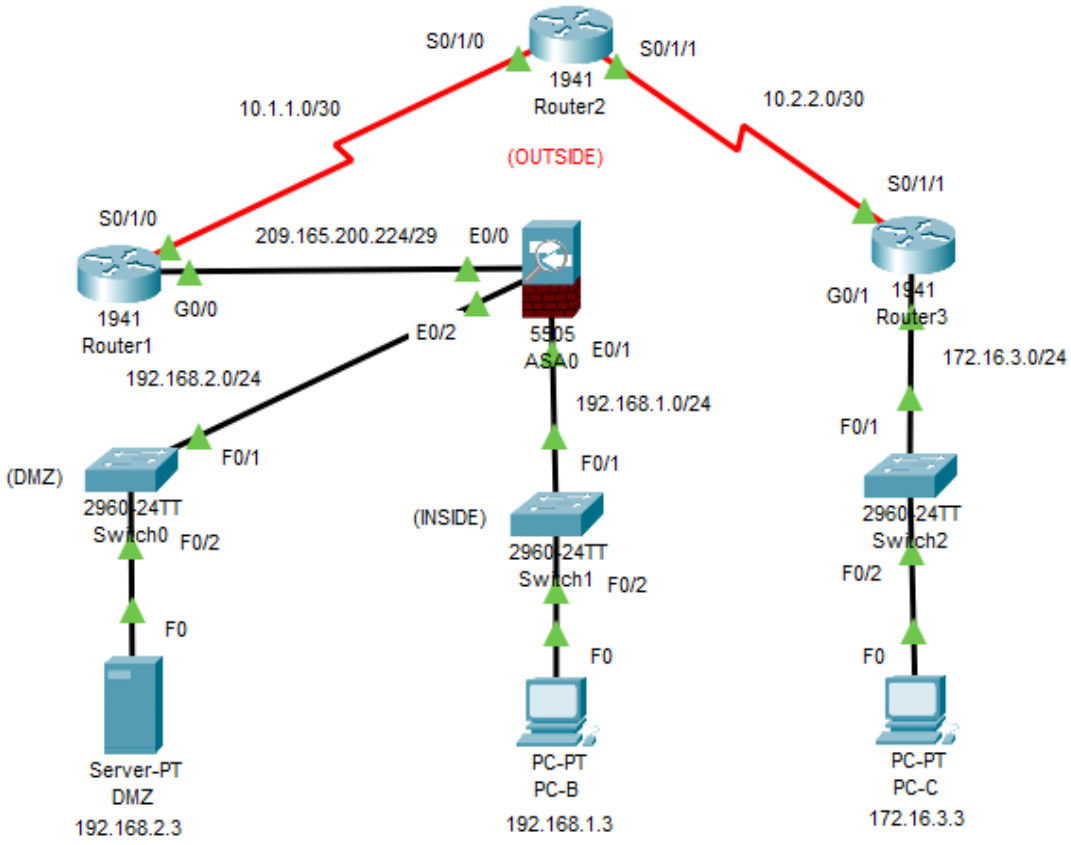


Figure 3.5 : l'architecture de réseau

3.2. Tableau d'adressage :

Device	Interface	Address IP	Le masque sous réseau
R1	S0/1/0	10.1.1.1	255.255.255.252
	G0/0	209.165.200.225	255.255.255.248
R2	S0/1/0	10.1.1.2	255.255.255.252
	S0/1/1	10.2.2.2	255.255.255.252
R3	S0/1/1	10.2.2.1	255.255.255.252
	G0/1	172.16.3.1	255.255.255.0
ASA	E0/0	209.165.200.226	255.255.255.248
	E0/1	192.168.1.1	255.255.255.0
	E0/2	192.168.2.1	255.255.255.0
DMZ	NIC	192.168.2.3	255.255.255.0
PC-B	NIC	192.168.1.3	255.255.255.0
PC-C	NIC	172.16.3.3	255.255.255.0

Dans les travaux pratiques, un fournisseur d'accès Internet (FAI) attribue l'espace d'adressage IP public 209.165.200.224/27 à une entreprise. Cela permet à l'entreprise de disposer de 30 adresses IP publiques. Les adresses 209.165.200.225 à 209.165.200.241 concernent l'attribution statique tandis que les adresses 209.165.200.242 à 209.165.2 00.254 concernent l'attribution dynamique.

3.3. Configuration des routeurs :

La première étape consiste à donner l'adresse IP pour chaque interface de routeur.

3.3.1. Le routeur 1 :

La configuration est la suivante :

```
Router(config)#hostname Router1
Router1(config)#int serial 0/1/0
Router1(config-if)#ip address 10.1.1.1 255.255.255.252
Router1(config-if)#clock rate 64000
Router1(config-if)#no shut
Router1(config-if)#exit
Router1(config)#interface g0/0
Router1(config-if)#ip address 209.165.200.225 255.255.255.248
Router1(config-if)#no shut
Router1(config-if)#exit
Router1(config)#ip route 0.0.0.0 0.0.0.0 Se0/1/0
```

3.3.2. Le routeur 2 :

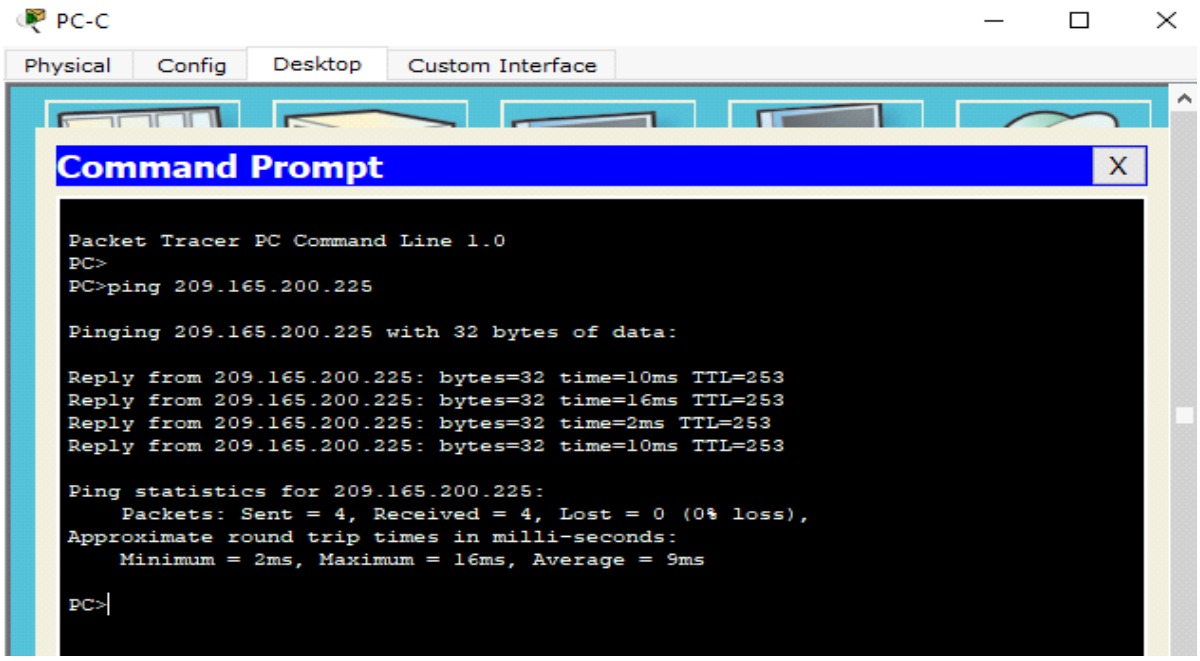
De même pour le routeur 2 :

```
Router(config)#hostname Router2
Router2(config)#interface serial 0/1/0
Router2(config-if)#ip address 10.1.1.2 255.255.255.252
Router2(config-if)#no shut
Router2(config-if)#exit
Router2(config)#interface serial 0/1/1
Router2(config-if)#ip address 10.2.2.2 255.255.255.252
Router2(config-if)#clock rate 64000
Router2(config-if)# no shut
Router2(config-if)# exit
Router2(config)#
Router2(config)# ip route 172.16.3.0 255.255.255.0 10.2.2.1
Router2(config)# ip route 209.165.200.224 255.255.255.248 10.1.1.1
Router2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
Router2(config)#end
```

3.3.3. Le routeur 3 :

```
Router3(config)#hostname Router3
Router3(config)#interface gigabitethernet 0/1
Router3(config-if)#ip address 172.16.3.1 255.255.255.0
Router3(config-if)#no shut
Router3(config-if)#exit
Router3(config)#int serial 0/1/1
Router3(config-if)#ip address 10.2.2.1 255.255.255.252
Router3(config-if)# no shut
Router3(config-if)#exit
Router3(config)# ip route 0.0.0.0 0.0.0.0 Se0/1/1
```

3.3.4. Vérification de la connexion:Ping de PC-C à Router1



Après un Ping de vérification, nous pouvons confirmer que les trois routeurs peuvent communiquer.

4. Configuration du module L'ASA :

Passons maintenant à la configuration de ASA .L'attribution des adresses se fait comme tout autre périphérique Cisco, mais on doit préciser la nature de l'interface Inside ou Outside et le niveau de sécurité de chaque interface.

Chaque interface ASA a un niveau de sécurité compris entre 0 et 100. Pour l'Inside, son niveau de sécurité est de 100 et l'Outsideest de 0.

4.1. Configurationle nom d'hôte, le nom de domaine et le mot de passe :

```
ciscoasa>enable
Password:
ciscoasa#config t
ciscoasa(config)#hostname ASA
ASA(config)#domain-name ccnasecurity.com
ASA(config)#enable password cisco123
```

4.2. Configuration les interfaces inside et outside :

```
ASA(config)#interface ethernet 0/1
ASA(config-if)#switchport access vlan 1
ASA(config-if)#no shut
ASA(config-if)#exit
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config-if)#security-level 100
ASA(config-if)#no shut
ASA(config-if)#exit
ASA(config)#inter ethernet 0/0
ASA(config-if)#switchport access vlan 2
ASA(config-if)#no shut
ASA(config-if)#exit
ASA(config)#interface vlan 2
ASA(config-if)# nameif outside
ASA(config-if)#ip address 209.165.200.226 255.255.255.248
ASA(config-if)#security-level 0
ASA(config-if)#no shut
ASA(config-if)#exit
ASA(config)#
```

4.3. Configuration l'interface DMZ VLAN 3 :

DMZ nous lui donnerons un niveau de sécurité de 70 pour l'accès à cette zone similaire aux réseaux internes et externes (pour donner le pouvoir d'accès internes et externes).

```
ASA(config)#interface vlan 3
ASA(config-if)#ip address 192.168.2.1 255.255.255.0
ASA(config-if)#no forward interface vlan 1
ASA(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA(config-if)#security-level 70
ASA(config-if)#no shut
```

Nous définissons l'interface physique ASA E0/2 sur DMZ VLAN 3 puis l'activation de l'interface.

```
ASA(config)#interface ethernet0/2
ASA(config-if)#switchport access vlan 3
```

Maintenant nous utilisons la commande **"show switch vlan"** pour afficher les VLAN internes et externes configurés sur l'ASA et pour afficher les ports attribués.

```
VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------------------------
1    inside                            up        Et0/1, Et0/3, Et0/4, Et0/5
                                                 Et0/6, Et0/7
2    outside                           up        Et0/0
3    dmz                               up        Et0/2
```

4.4. Configuration de protocole de routage :

Le routage permet au réseau d'assurer la connexion :

```
ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
```

Unping vers le Routeur 1 (10.1.1.1) pour confirmer la connexion :

```
ASA(config)#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

4.5. Configuration du NAT :

Le réseau LAN dispose d'une plage d'adresse privée alors que la DMZ dispose d'une plage d'adresse publique. Pour que les postes du réseau LAN puissent se connecter à internet il leur faut une adresse IP routable, Ce qui signifie l'utilisation d'un NAT dynamique. Contrairement au DMZ qui utilise un NAT statique. Les deux versions de NAT sont mises en application par l'ASA.

-Configuration depuis l'intérieur vers l'extérieur NAT Dynamique :

```
ASA(config)#object network inside-network
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#nat (inside,outside) dynamic interface
ASA(config-network-object)#end
```

-Configuration depuis la DMZ vers l'extérieur NAT Statique :

```
ASA(config)#object network dmz-server
ASA(config-network-object)#host 192.168.2.3
ASA(config-network-object)#nat (dmz,outside) static 209.165.200.227
```

4.6. La configuration de L'ICMP :

Ping du côté le plus sécurisé cela devrait normalement marcher. Mais par défaut, l'ASA ne suit pas l'état ICMP. Pour résoudre ce problème, nous entrons les commandes suivantes pour activer l'inspection ICMP :

```
ASA(config)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#exit
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#exit
ASA(config)#service-policy global_policy global
```

-Vérification :avec unPing d'un PC-B vers le Routeur 1 (209.165.200.225).

```
PC>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=0ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms TTL=254
Reply from 209.165.200.225: bytes=32 time=2ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 6ms
```

4.7. Configuration de DHCP :

```
ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
ASA(config)#dhcpd dns 209.165.201.2 interface inside
ASA(config)#dhcpd enable inside
```

4.8. Configuration de ASA :nous configurons ASA pour utiliser la base de données ASA locale pour l'authentification des utilisateurs SSH.

```
ASA(config)#username admin password admin1
ASA(config)#aaa authentication ssh console LOCAL
```

4.8.1. Configuration de SSH :

```
ASA(config)#ssh 192.168.1.0 255.255.255.0 inside
ASA(config)#ssh 172.16.3.3 255.255.255.255 outside
ASA(config)#ssh timeout 10
```

4.8.2. Établissez une session SSH :

Du PC-C vers l'ASA (209.165.200.226) :

```
C:\>ssh -l admin 209.165.200.226

Password:



ASA>
```

Du PC-B vers l'ASA (192.168.1.1) :

```
PC>ssh -l admin 192.168.1.1
Open
Password:
```

5.9. La configuration de l'ACL sur le serveur DMZ :

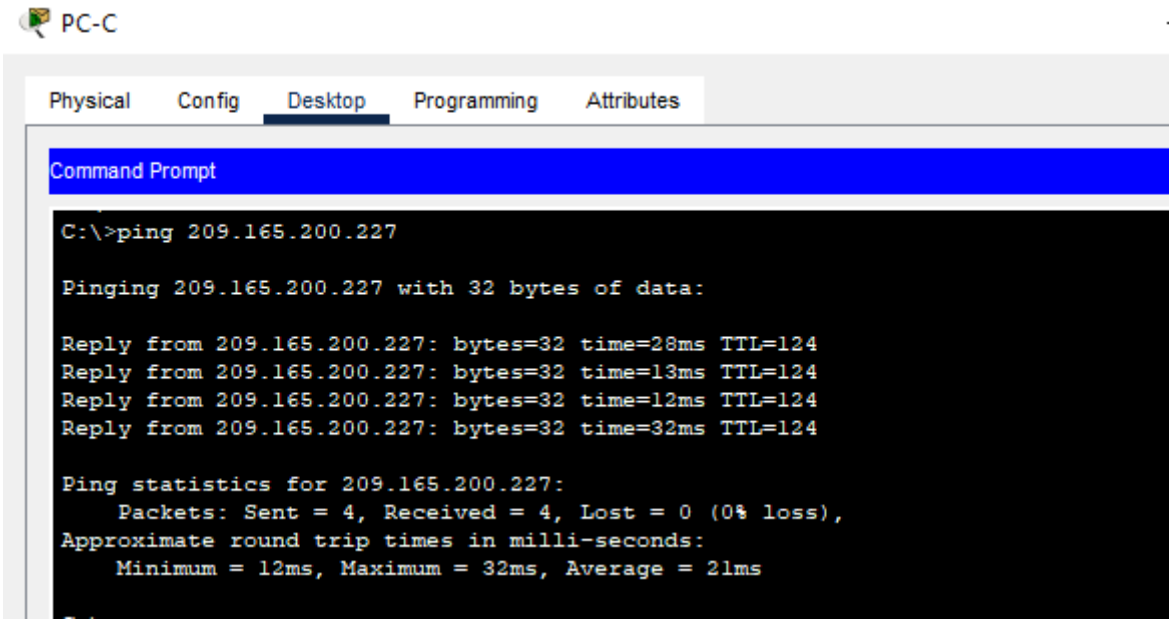
Les ACLs offrent la possibilité de positionner des droits d'accès supplémentaires. Avec les ACLs c'est possible de donner des droits à un utilisateur qui ne fait pas partie dans le groupe sans modifier les droits pour les autres. De même on peut autoriser des droits d'accès pour un groupe d'utilisateurs qui n'est pas le groupe du fichier. Il n'y a pas des limites concernant le nombre d'utilisateurs ou groupes à ajouter avec les ACLs.ACL sur un pare-feu ou un routeur filtrant, est une liste d'adresses ou de ports autorisés ou interdits par le dispositif de filtrage. [27] [29]

Donc pour pouvoir autoriser le trafic entre un réseau de niveau de sécuritéinférieur à un autre réseau supérieur, nous allons créer des access- list.

Ici, pour permettre l'accès au serveur DMZ côté internet, on configure une liste de contrôle d'accès nommées " OUTSIDE-DMZ".

```
ASA(config)#access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
ASA(config)#access-group OUTSIDE-DMZ in interface outside
```

Vérification : pour vérifie la connectivité on fait un Ping sur le PC-C vers l'adresse IP publique de la DMZ (209.165.200.227).



D'après la figure ci-dessus, un ping effectué, la connexion estétablit entre PC-C et la DMZ

6. Création d'un réseau VPN pour une entreprise :

Cette nouvelle architecture nous donne la possibilité de créer un réseau VPN afin de donner l'accès à un client ou un partenaire distant toute en assurant la sécurité lors de l'échange de données via un protocole de cryptage et de sécurité.

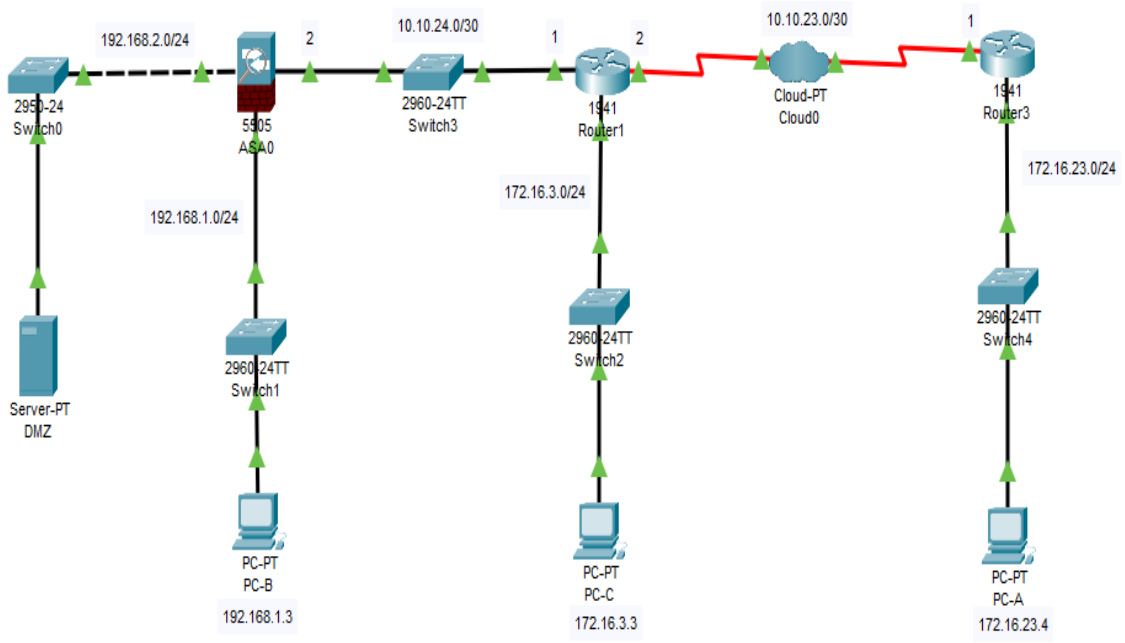


Figure 3.6 : Création du réseau VPN

6.1. Création de VPN IPSec :

Dans cette partie, nous allons configurer un tunnel VPN IPsec entre ASA et Le Routeur 3.

Nous avons 6 étapes à suivre pour la mise en place du VPN.

• Définir la politique ISAKMP (IKE Phase1: Méthode de chiffrement, durée de vie, méthode d'intégrité, ce qui va permettre de définir une IKE Security Association).

• Créer la clé partagée et un tunnel groupe par apport l'ASA seulement.

• Créer une transform-set (IKE Phase2: Nous allons configurer les politiques de sécurité IPSec «protocole esp, vérifier le type de liaison, afin d'avoir un IPSec Security Association).

• Mettre en place une ACL (qui définira quel trafic peut/doit emprunter le VPN).

• Créer un crypto map.

• Appliquer le crypto map à l'interface de sortie.

6.1.2. Configuration de ISAKMP :

ISAKMP (Internet Security Association and Key Management Protocol) est le protocole de négociation nécessaire pour que les deux hôtes se mettent d'accord sur une politique de sécurité. ISAKMP sépare la négociation en deux phases. La première phase crée un premier tunnel, qui protégera les négociations du protocole ISAKMP. La deuxième phase crée le tunnel qui protègera les données.

6.1.2.1. Première étape : Activation du protocole ISAKMP : nous devons activer le protocole ISAKMP sur l'interface outside sur ASA avec la commande :

```
ASA(config)#crypto ikev1 enable outside
```

et sur le Router 3 avec la commande :

```
Router3(config)#crypto isakmp enable
```

6.1.2.2. Deuxième étape : créer la policy-map : Voici les commandes que nous devons exécuter pour établir une politique ISAKMP sur ASA :

```
ASA(config)#crypto ikev1 policy 1
ASA(config-ikev1-policy)#authentication pre-share
ASA(config-ikev1-policy)#encryption aes
ASA(config-ikev1-policy)#hash sha
ASA(config-ikev1-policy)#group 2
ASA(config-ikev1-policy)#lifetime 86400
ASA(config-ikev1-policy)#exit
```

Sur le Routeur 3 :

```
Router3(config)#crypto isakmp policy 1
Router3(config-isakmp)#authentication pre-share
Router3(config-isakmp)#encryption aes
Router3(config-isakmp)#hash sha
Router3(config-isakmp)#group 2
Router3(config-isakmp)#lifetime 86400
Router3(config-isakmp)#exit
```

En rappel les détails de chaque commande utilisée ci-dessus [12] :

Crypto isakmppolicy 1 : Cette commande crée la stratégie ISAKMP numéro 1. Nous pouvions créer plusieurs stratégies, par exemple7, 8,9 avec une configuration différente. Les routeurs participant à la négociation de la phase 1 essaient de faire correspondre une stratégie ISAKMP à la liste des stratégies une par une. Si une stratégie est mise en correspondance, la négociation IPSec passe à la phase suivante. On crée donc ici une stratégie avec un numéro de séquence 1.

Ce numéro indique la priorité de l'utilisation de la stratégie. Plus petit est ce nombre plus la priorité est grande.

Authenticationpre-share : La méthode d'authentification est la clé pré-partagée.

Encryption AES : L'algorithme de cryptage AES (Advanced Encryption Standard Sera utilisé pour la confidentialité.

Hashsha : L'algorithme de hachage sha sera utilisé pour l'intégrité.

Group 2 : Méthode de distribution des clés partagées DH-2. Le groupe Diffie-Hellman utilisé ici est le groupe 2 pour la méthode d'échange des clés.

lifetime 86400 : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs. (En seconds).

Tous les paramètres ISAKMP doivent être les mêmes des deux côtés du tunnel, mis à part la durée de remplacement des clefs, qui doit être plus petite (ou égale) sur le répondeur que sur l'initiateur de la connexion.

6.2. Création du tunnel VPN avec tunnel-group et la clé de partage :

6.2.1 Tunnel group :

tunnel-group est une liste de paramètres de connexion utilisée pour créer un tunnel VPN. Là encore, la configuration est assez complexe, et nous ne rentrerons pas dans le détail. Par défaut, l'ASA contient deux tunnels groups enregistrés : le premier pour les tunnels End-to-Lan, et le second pour les tunnels Lan-to-Lan.

Nous créons un tunnel group sur ASA, à l'aide de la commande suivante :

```
ASA(config)#tunnel-group 10.10.23.1 type ipsec-l2l
```

6.2.2 La clé de partage :

Nous devons maintenant définir la clef pré-partagée entre les deux extrémités du tunnel.

ASA :

```
ASA(config)#tunnel-group 10.10.23.1 ipsec-attributes
ASA(config-tunnel-ipsec)#ikev1 pre-shared-key cisco8266
ASA(config-tunnel-ipsec)#exit
```

Routeur 3 :

```
Router3(config)#crypto isakmp key cisco8266 address 10.10.24.2
```

La clef pré-partagée «cisco8266» est utilisée ici pour éviter des erreurs et des pertes de temps. Mais dans la réalité, si nous devons choisir une clé pré-partagée, choisissons une combinaison de chiffres et de lettres suffisamment longue pour qu'elle n'apparaisse pas dans le dictionnaire et n'ait pas de signification spécifique (il faut qu'elle soit indéchiffrables).

6.3. Création d'une transform-set :

Lorsque nous créons un tunnel VPN, nous voudrions que des données moins sensibles soient moins bien protégées que des données très sensibles, afin d'économiser le temps du processeur et de la bande passante. C'est l'utilité de transform set. Ils sont associés à des ACL, elles-mêmes associées à des crypto map. Un transform set combine une méthode de cryptage et une méthode de hachage. Nous créerons le transform-set suivant sur :

ASA :

```
ASA(config)#crypto ipsec ikev1 transform-set VPN-SET esp-aes esp-sha-hmac
```

Routeur 3 :

```
Router3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

Voici le détail de la commande utilisée ci-dessus [10] [14] :

• **Crypto ipsectransform-set VPN-SET :** Crée un ensemble de transformation appelé VPN-SET.

• **esp-aes :** la méthode de cryptage AES et le protocole ESP IPSec seront utilisés.

• **esp-sha-hmac :** L'algorithme de hachage SHA sera utilisé.

Sur le Routeur 3 et fixer la durée de vie de l'association de sécurité IPSec à 3600 secondes.

```
Router3(config)#crypto ipsec security-association lifetime seconds 3600
```

6.4. Configuration de la liste de contrôle d'accès (ACL) :

Pour utiliser le cryptage avec le VPN IPSec, il est nécessaire de définir une liste d'accès étendue pour indiquer quel trafic il doit crypter. Le trafic permit par cette ACL sera chiffré dans le tunnel IPSEC, le reste non.

Dans ce cas, le trafic que nous voulons crypter est le trafic allant du LAN Ethernet de Routeur 3 vers le LAN Ethernet de ASA ou vice versa.

Nous utiliserons l'ACL suivante sur l'ASA :

```
ASA(config)#object network LOCAL_NET
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#exit
ASA#config t
ASA(config)#object network REMOTE_NET
ASA(config-network-object)#subnet 172.16.23.0 255.255.255.0
ASA(config-network-object)#exit
```

```
ASA(config)#access-list VPN-ACL extended permit ip object LOCAL_NET object REMOTE_NET
```

Et son miroir sur le Routeur 3 :

```
Router3(config)#ip access-list extended VPN-ACL
Router3(config-ext-nacl)#permit ip 172.16.23.0 0.0.0.255 192.168.1.0 0.0.0.255
Router3(config-ext-nacl)#exit
```

6.5. Configuration de Crypto Map :

La crypto map est l'élément qui rassemble tous les paramètres d'association de sécurité IPSec que nous avons créé précédemment. La crypto map définit le trafic à protéger (défini dans une liste d'accès), où envoyer le trafic protégé (l'adresse publique à l'autre extrémité du tunnel) et la sécurité à appliquer au trafic (application du transform set). Pour éviter les erreurs, nous définirons exactement les mêmes paramètres sur l'ASA et sur le Routeur. [1]

Voici les commandes à entrer sur l'ASA :

```
ASA(config)#crypto map VPN-MAP 10 match address VPN-ACL
ASA(config)#crypto map VPN-MAP 10 set peer 10.10.23.1
ASA(config)#crypto map VPN-MAP 10 set ikev1 transform-set VPN-SET
```

Et les commandes à entrer sur Routeur 3 :

```
Router3(config)#crypto map VPN-MAP 10 ipsec-isakmp
Router3(config-crypto-map)#set peer 10.10.24.2
Router3(config-crypto-map)#set transform-set VPN-SET
Router3(config-crypto-map)#match address VPN-ACL
Router3(config-crypto-map)#exit
```

6.6. Application de la Crypto Map à l'interface de sortie :

La configuration de routeur 3 et ASA est presque terminée nous devons appliquer la crypto map sur L'interface de sortie de :

ASA :

```
ASA(config)#crypto map VPN-MAP   interface outside
```

Routeur 3 :

```
Router3(config)#interface S0/0/0
Router3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

7. Vérification :

7.1. Vérification des opérations ISAKMP :

Pour vérifier ISAKMP, on tape **«show crypto isakmp sa»** comme indiqué :

ASA :

```
ASA#show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1
1   IKE Peer: 10.10.23.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_SA_ACTIVE
```

Routeur 3 :

```
Router3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.24.2      10.10.23.1      QM_IDLE           1077    0 ACTIVE (deleted)


IPv6 Crypto ISAKMP SA
```

Les deux figures précédentes signifie que les opérations de ISAKMP sont activées entre les deux extrémités du tunnel ASA (10.10.24.2) et le Routeur 3 (10.10.23.1).

7.2. Vérification du transform-set sur le routeur 3 :

```
Router3#show crypto ipsec transform-set
Transform set VPN-SET: {     { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Ici en présente les protocoles de cryptage esp-aes et esp-sha-hmac, utilisé sur le tunnel.

7.3. Vérification de la crypto-map :

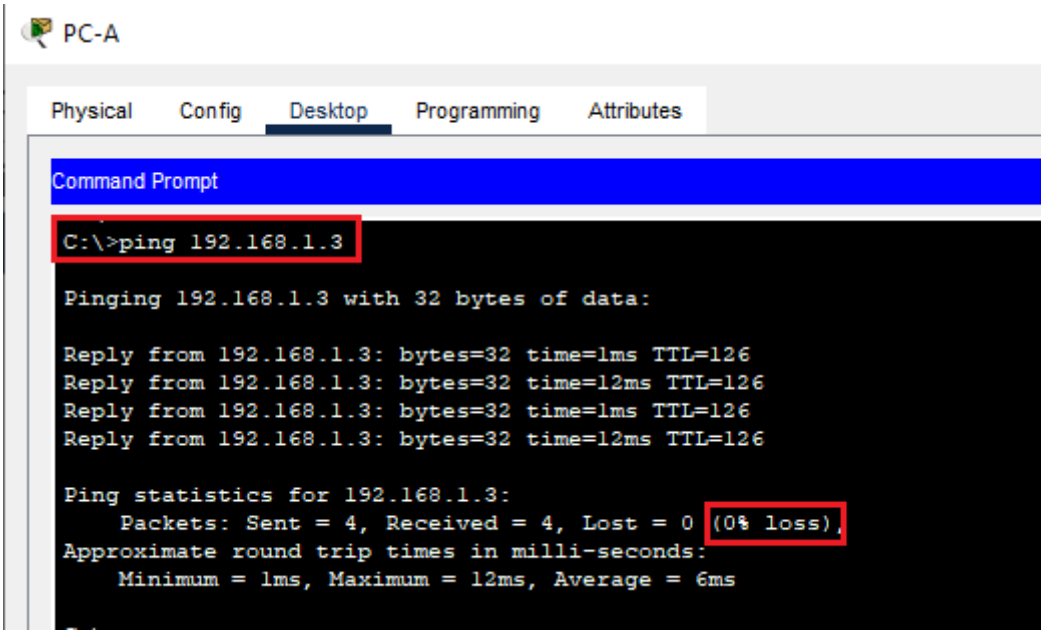
A l'aide de la commande « show crypto map », nous allons pouvoir tester la création de la crypto-map :

```
Router3#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 10.10.24.2
        Extended IP access list VPN-ACL
            access-list VPN-ACL permit ip 172.16.23.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 10.10.24.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/0/0
```

Nous avons vérifié la configuration de crypto map nommée « VPN-MAP » qui comprend tous les éléments créés précédemment, c'est-à-dire les Access-lists, les transform-set et l'interface assignée à la crypto-map. En remarque aussi la bonne configuration du cryptage avec le protocole IPSec.

8. Test de connexion :

Pour tester la connexion VPN, nous envoyons tout d'abord une requête Ping de PC-A (172.16.23.4) vers le PC-B (192.168.1.3).



D'après le Ping le trafic de connexion existe entre PC-A (172.16.23.4) et le PC-B (192.168.1.3).

9. Conclusion :

Dans la première partie de ce chapitre, nous avons présenté l'architecture de réseau d'entreprise sécurise à base d'un pare-feu (ASA) et les différents éléments de réseau ont été implémenté.

- Après la configuration des routeurs et tests de connexion nous avons procédé à la configuration de ASA avec les différentes étapes, test de connexion établi du PC-B vers le routeur 1 (outside).
- Configuration des ACL pour donner l'accès entre un réseau de niveau de sécurité inférieur (outside) à un autre réseau supérieur (DMZ).

Dans la deuxième partie, on a créé un tunnel VPN entre l'ASA et Routeur 3 pour donner l'accès aux clients et partenaires distants.

- La configuration de sécurité de réseau par de le protocole ISAKMP.
- Ensuite on a configuré les paramètres de IPSec.

Selon les tests effectués du Routeur 3 vers ASA, nous avons observé une connexion établit côté ASA la connexion est activée d'après la vérification de ISAKMP.

Apres les tests côté Routeur externe et côté interne ASA. Les résultats de simulation qui ont été réalisée sous le logiciel Cisco Packet Tracer confirment la validité de l'étude car le tunnel est sécurisé avec IPsec et la connexion est bien établit.

La sécurité des systèmes informatique est une nécessité majeure pour rendre la communication et le partage de données fiable et moins vulnérable aux attaques cybercriminels.

Dans notre projet de fin d'étude, nous avons présentés en premier lieu les différents attaques et définit leurs impact sur les systèmes informatisés, d'autre part nous avons également exposé les systèmes et les mécanises destinés à assurer la sécurité des réseaux de communications.

Nous avons abordés dans le deuxième chapitre le système de connexion à travers internet, le réseau privé virtuel VPN qui peut garantir la sécurité et la confidentialité des données, qui circulent de manière cryptée via un tunnel privé créer dans le but de facilité les communications entre les entreprises et leurs partenaires, pareillement il assure les communications internes d'une entreprise dans le cas d'un réseau d'entreprise réparti sur plusieurs sites distants.

Notre travail nous a permit :

-La mise en place et la configuration d'une architecture d'entreprise sécurisée à base de pare-feu ASA. Avec configurations et tests de connexion effectués sous le logiciel Cisco Packet Tracer.

-La création d'un tunnel VPN d'entreprise pour assurer la connexion à des sites distants et des clients nomades, cette connexion a été configurée avec une sécurité et cryptage via le protocole IPsec. Les tests de connexion et de cryptage ont été vérifiés avec succès.

Perspective :

Nous proposons l'implémentation pratique de cette simulation avec le GNS3 un logiciel libre qui fonctionne sur de multiples plateformes, qui permet la configuration et les tests de connexion. Il est très largement utilisé dans le domaine pratique.

Tester d'autres protocoles de connexion et de cryptage comme le SSL qui s'avère très utilisé dans le cas de connexion poste à site.

RÉFÉRENCES

BIBLIOGRAPHIQUES

Les Références Bibliographiques

[1] Mohan V.Pawar J.Anuradha "Network Security and Types of Attacks in Network" Procedia Computer Science Volume 48, 2015, Pages 503-506.

[2] Kamal Singh "Comprendre le cœur d'Internet : les réseaux d'opérateurs", cours en ligne Kamal Singh – Télécom Saint-Étienne 2020.

[3] C. Pham "Les réseaux grande distance Routage et réseaux de Routage et réseaux d'accès", Université de Pau et des Pays de l'Adour Département Informatique 2005.

[4] Raphael Yende, Support De Cours De Sécurité Informatique Et Crypto. 2018.

[5] Sadiqui.A Sécurité des réseaux informatiques, publié en grande Bretagne 2019 ISLTE Editions Ltd.

[6] Jules GBEDANDE 'Déploiement par GNS3 de VLANs sécurisés avec Snort_inline' Mémoire de fin de formation pour l'obtention du diplôme d'ingénieur de conception, Ecole polytechnique d'abomey-calavi , département de génie informatique et télécommunications 31 décembre 2015.

[7] Etienne Duris «Réseaux Informatique – Licence 3 »Université Paris-Est Marne, la Vallée, Janvier 2010.

[8]Technique avancées de sécurité et cryptographie, Master Recherche Faculté des Sciences de Monastir, Tunisie, 2015-2016.

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

[10] Tebani.T " Simulation d'un tunnel VPN-SSL pour la sécurisation d'une interconnexion dedeux réseaux LANs", Mémoire de fin d'études de master Génie électrique, Université Mouloud Mammeri De Tizi-Ouzou, 2015.

[11] M.Bada« la sécurité informatique chapitre4/Infrastructures réseau sécurisé » Université de Guelma Module : 2015-2016.

[12]Danièle DROMARD. Dominique SERET, « Réseaux Informatiques », *Encyclopædia Universalis* en Ligne, Consulte Le 28 Mai 2022

[13] Bernard Cousin, Sécurité des réseaux informatiques, Université de Rennes 1.

[14] S.lila, S .Malika, Mémoire de fin d'études en master2 réseau et télécommunication, Implémentation d'une solution d'interconnexion entre deux forets différents avec une relation d'approbation et VPN site a site 2016/2017.

[15]J.GBEDANDE. « Déploiement par GNS3 de VLANs sécurisés avec Snort_inline Mémoire de fin de formation pour l'obtention du diplôme d'ingénieur de conception .Université D'ABOMEY-CALAV Ecole Polytechnique D'ABOMEY-CALAVI Département De Génie Informatique et Télécommunications Option : Réseaux et Télécommunications (RT) 2015.

[16] Tinhinan.R, Fadhila.S « Etude et mise en place d'un réseau VPN » Mémoire de fin d'étude, Université Mouloud Mammeri De Tizi Ouzou Faculté Du Génie Electrique Et Informatique Département Electronique, 2016/2017.

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

[18] Jacob NDWO MAYELE," Déploiement d'un cœur de réseau IP/MPLS", Licence en génie informatique, Université de Kinshasa, 2016.

[19] Baa Adel Saker Karim « Mise en place d'une architecture VPN-IPsec » pour le compte de CEVITAL", Mémoire de fin d'études en vue de l'obtention du diplôme Master en en informatique, Option : Administration et Sécurité des Réseaux, Université Abderrahmane Mira BEJAIA, 2016

[20] Sadoud.L, Saddedine.M, « Implémentation d'une solution d'interconnexion entre deux forets différents avec une relation d'approbation et VPN site a site », Mémoire de fin d'études en master2 réseau et télécommunication ,2012/2013.

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

[22] Belhariz ASMA, « Sécurité réseau, étude le cas de service open-VPN » Mémoire de fin d'études licence en informatique, 27 juin 2013 Telemsen.

[23] https://www.frameip.com/vpn/

[24] https://wallu.pagesperso-orange.fr/pag-ipsec.htm

[25] Gauchard. D " Simulation Hybride des Réseaux IP-DiffServ-MPLS Multi-services sur Environnement d'Exécution Distribuée", Thèse de doctorat en Systèmes Informatiques, Université Toulouse III Paul Sabatier, 2003

[26] Z.HASNIA, B.YASMINE « Etude et Simulation d'une architecture réseau mixte sécurisée d'une Carte d'itinéraire IPSEC VPN et NAT » Mémoire de fin d'étude Systèmes des Télécommunications, Université Abdelhamid Ibn Badis de Mostaganem, 2019/2020.

[27] www.Cisco.com //ASA5500 (5505, 5510, 5520, etc) Séries Firewall Security A.mht, 2009

[28] Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6 - Starting Interface, 2010

[29]CISCOMADESIMPLE.BE «Configuration de base d'un Etherchannel entre deux Switch»,2007

[30] T.Delage, « Network Address Translation, Port Address Translation », GRETA VIVA5/IUT Valence, 2012