République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Mémoire De Fin de Cycle

En vue d'obtention d'un diplôme de Master professionnel en Informatique

Spécialité : Administration et Sécurité des Réseaux

THÈME

Mise en place d'une architecture VPN IPsec, cas d'étude :

Entreprise GPL NAFTAL de Béjaia

Réalisé par :

M^{elle} AGBARI Célia et M^{elle} BAKOUR Yasmine.

Soutenu le 06/09/2020 devant le jury composé de :

Président	**M^{r}. BOUZIDI Zair**	**U. A/Mira Béjaïa.**
Examinateur	**Mme. HALFOUNE Nadia**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. BOUDRIES Abdelmalek**	**U. A/Mira Béjaïa.**

Promotion 2019-2020

Remerciements

Nous remercions avant tout Dieu qui nous a aidé et donné la patience, le courage et la force d'achever ce travail.

Nous remercions notre encadreur M^r^ BOUDRIES Abdelmalek d'avoir accepté de diriger ce travail, et pour ses précieux conseils et encouragements, sans lesquels cette étude n'aurait pas vu le jour.

Nous exprimons également notre gratitude aux membres du jury, qui nous ont honorés en acceptant de juger ce modeste travail.

Nous tenons à remercier sincèrement nos parents et nos frères, qui nous ont donné la force et le courage.

Nous tenons à remercier tous les enseignants qui ont assurés notre formation Durant notre cycle universitaire. Ainsi, que tout le personnel du département informatique.

Que tous ceux qui nous ont aidé, de près ou de loin, à mener à bout ce travail trouvent ici notre reconnaissance et toute notre gratitude.

Dédicaces

A nos chers parents qui n'ont pas cessé de nous encourager et de se Sacrifier afin que nous puissions réussir que Dieu leur accorde santé, amour, bonheur et longue vie ; Aucune dédicace ne pourra compenser leurs sacrifices.

A nos frères, à qui nous souhaitons tous le meilleur dans ce monde.

A nos familles : cousins, cousines, tantes et oncles.

A tous nos ami(e)s et à tous ceux qui nous connaissent.

Célia AGBARI et Yasmine BAKOUR

Table des matières

Liste des tableaux

Table des figures

Liste des Abréviations

ADSL *: Asymmetric Digital Subscriber Line*
AH *: Authetification header*

BS *: Blind Spoofing*

CD ROM *: Compact Disc -Read Only Memory*
CPU *: central processing unit*

DMZ *: DeMilitarized Zone*
Dos *: Déni de Service*
DOS *: disk operating system*

ERDP *: entreprise de raffinage et de distribution de produit pétrolier*
ESP *: Encapsulating Security Playload*

FTP *: File Transfer Protocol*

GPL *: Gaz de Pétrole Liquéfié*

HTTPS *: HyperText Transfer Protocol Secure*

IDS *: Intrusion Detection System*
IETF *: Internet Engineering Task Force, : Internet Engineering Task Force*
IKE *: Internet Key Exchange*
Ip *: Internet Protocol*
IPsec *: Internet Protocol Security*

L2F *: Layer 2 Forwarding*
L2TP *: Layer 2 Tunneling Protocol*
LAN *: Local Area Network*

MPLS *: MultiProtocol Label Switching*

NBS *: Non Blind Spoofing*

OSI *: Open Systems Interconnection*

PMC *: Personnel et Moyen Commun*
PPP *: Point to Point Protocol*
PPTP *: Point to protocole Point Tunneling Protocol*

QoS *: Quality Of Service*

RFC *: requests for comments*

SA *: Security association*

SAD *: Security association Database*
SFP *: Small Form-Factor Pluggable*
SP *: Security Policy*
SPD *: Security Political Database*
SPI *: Security Parameters Index*
SSL *: Secure Socket Layer*
SSTP *: Secure Socket Tunneling Protocol*
STP *: Spanning Tree Protocol*

TCP *: Transmission Control Protocol*

UND *: unité NAFTAL de distribution unité NAFTAL de distribution*
UTP *:* Unshielded Twisted Pair

VPN *: Virtual Private Network*

Introduction générale

L'Internet s'impose comme un outil stratégique incontournable, la mobilité s'accroît et devient un élément central d'organisation. Le développement des réseaux et du haut débit a profondément bouleversé le transfert et l'échange de données et permet désormais une communication performante, fluide et très sécurisée.

Aujourd'hui, les entreprises créent de plus en plus de succursales partout dans le monde, et donc leurs besoins de communiquer et d'échanger des données et des informations avec ces derniers sont devenus une nécessité et la sécurité de ces échanges est primordiale. Mais pas que ça, le télétravail est devenu aussi très courant et très utilisé et parfois une nécessité, comme la crise sanitaire du covid19, ce qui a permis au monde de poursuivre ses activités grâce au télétravail.

Pour répondre à ces besoins, les entreprises utilisent des réseaux déjà prêts à l'exploitation, ou bien elles créent leur propre réseau (réseau de télécommunication, des réseaux sans fils, Internet, etc.) et ce en utilisant de différents composants physiques tels que les routeurs, les switchs, les ordinateurs, les systèmes informatiques et les protocoles.

Le réseau le plus utilisé est l'internet, c'est vrai que ces réseaux et ces composants répondent à ces besoins, mais cette solution n'est pas sans risque, car elle présente des menaces et des vulnérabilités sur les données échangées qui sont confidentielles et très importantes, ce qui engendre un risque de vol, d'interception, de modification ou de destruction de ces informations, qui peut causer de grands problèmes à l'entreprise et des dommages compromettant ainsi son développement.

De ce fait les entreprises se trouvent dans l'obligation de sécuriser leur réseau et mettre en place des politiques de sécurité informatique pour assurer la confidentialité des données et les garder en toute sécurité.

Parmi ces solutions on trouve les VPN, qui proposent d'échanger des données en toute sécurité en les encapsulant et les transmettant à travers des tunnels virtuels à des coûts réduits.

L'objectif de notre travail, consiste alors à mettre en place une architecture VPN IPsec afin d'établir une communication sécurisée entre la direction GPL NAFTAL de Bejaïa et ses différents districts et ce à travers un tunnel virtuel sécurisé (VPN) avec le protocole IPsec, permettant ainsi un échange de données sécurisé et sûr.

Ce mémoire est composé de quatre chapitres :

Le premier s'intitule « « Présentation de l'organisme d'accueil », qui est le noyau de notre travail. Nous avons établi une présentation générale de l'organisme d'accueil ainsi que le service où nous avons effectué notre stage, de là, nous avons soulevé les différents problèmes rencontrés, et proposé une solution à ces derniers.

Le deuxième chapitre est dédié à « la sécurité informatique ». En effet nous décrivons la sécurité informatique et présentons les menaces et les différentes attaques auxquelles un réseau peut être exposé.

Le troisième chapitre concerne les « Généralités sur les VPN et le protocole IPsec ». Dans ce chapitre, nous avons présenté les VPN, et les protocoles les plus communément utilisé avec ce dernier et plus précisément le protocole IPsec qui consiste la majeure partie de notre projet.

« La réalisation et l'implémentation » fera l'objet du quatrième chapitre dans lequel nous définirons les outils utilisés. Nous illustrerons également quelques captures de la configuration réalisée.

Enfin, nous conclurons ce travail en résumant les connaissances acquises durant la réalisation du projet.

Chapitre 01

Présentation de l'organisme d'accueil

1.1 Introduction

Dans ce chapitre introductif, nous allons présenter l'entreprise dans laquelle nous avons effectué notre stage afin de réaliser notre projet de fin d'étude, nous allons commencer par présenter un petit historique et quelques activités de NAFTAL ensuite les activités de GPL (Gaz de Pétrole Liquéfié) NAFTAL de Bejaïa et nous allons finir par faire une étude de l'existant.

1.2 Présentation de l'entreprise NAFTAL

1.2.1 Historique

NAFTAL est une entreprise de service public dans le cadre du plan national de développement économique et social, issue de SONATRACH.

Avant le 24 février 1971, le monopole de raffinage et de distribution des produits pétroliers était sous contrôle des entreprises étrangères, mais depuis la nationalisation des hydrocarbures, l'entreprise de raffinage et de distribution de produit pétrolier (ERDP) a été créée par le décret N°80/101 du 06 avril 1980 et entrée en activité le 01 janvier 1982.

Le 04 mars 1985, les anciens districts (Carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (unité NAFTAL de distribution).

En 1987, L'activité de raffinage est séparée de l'activité de distribution, et désormais une entreprise chargée de la distribution et de la commercialisation des produits pétroliers après les avoirs conditionnés (gaz du pétrole liquéfié, carburants, lubrifiants, pneumatique, bitumes et autre produits spéciaux) a été créé sous le sigle de « NAFTAL ».

A partir de 1998, elle change de statut et devient société par action filiale à 100% de SONATRACH,

1.2.2 Les missions et activités principales de l'entreprise

NAFTAL a pour mission principale, la distribution et la commercialisation des produits pétroliers sur le marché national. Elle intervient dans les domaines suivants :

- L'enfûtage des GPL
- La formulation de bitumes
- La distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux.

Les principales activités de l'entreprise NAFTAL sont :

- Le traitement du gaz naturel où gaz associés.
- Le raffinage du pétrole.
- La liquéfaction du gaz naturel.
- Commercialisation des produits pétroliers et raffinés sur le marché national.
- Commercialisation des pneumatiques de grandes marques dans diverses catégories de véhicules : tourisme, camionnette, poids lourds…
- Commercialisation d'une gamme complète de lubrifiants qui couvre toutes les applications du secteur automobile et industriel.

1.2.3 Objectifs de l'entreprise NAFTAL

NAFTAL a deux principaux objectifs :

✓Satisfaire la demande nationale.
✓Rentabiliser ses moyens de conditionnement et de la distribution.

1.3 Présentation de GPL NAFTAL Bejaïa

Dans cette partie nous allons présenter le district GPL NAFTAL, les services qui le composent et les différents rôles de ces derniers.

1.3.1 Description et rôle de chaque service de l'entreprise

- ✓ **Service sûreté :** Assure la sécurité au sein de l'entreprise.
- ✓ **Service juriste :** Il veille à ce que tout document signé ou qui doit être signé soit conforme au règlement.
- ✓ **Service sécurité industriel :** ce service se charge d'assurer la protection et préservation du personnel, du patrimoine industriel et de l'environnement.
- ✓ **Département informatique :** Il se charge d'assurer la coordination de l'activité informatique au niveau de l'entreprise NAFTAL.
- ✓ **Département exploitation :** Il se charge des tâches suivantes :
  - Suivie des performances des moyens de transport.

- Diriger et programmer les moyens de transports, et établir un plan adéquat de distribution de Provisionnement.
- Il s'occupe du conditionnement du gaz butane vrac en bouteille de 13 kg et de 3kg.
- Il veille à la disponibilité du produit pour la clientèle qu'il soit conditionné en vrac ou en GPL.

✓ **Département technique :** son rôle est d'assurer la gestion des projets dans leurs phases d'étude et de supervision des travaux.

✓ **Département commercial :** il se charge des différentes transactions entre l'entreprise et les clients et s'occupe de l'étude du marché de l'environnement ou le produit sera destiné à la commercialisation.

✓ **Département finance et comptabilité :** ce département a pour mission de s'occuper de tous les flux financiers de l'entreprise et veille à la sincérité des comptes du district et à la concordance des écritures comptable avec les flux physiques et financiers. Ce département se compose de 3 services :

- ➢ Service trésorerie qui se charge des recettes et des dépenses.
- ➢ Service comptabilité générale qui s'occupe des bilans et des inventaires.
- ➢ Service budgets et coûts se charge de l'ajustement des budgets prévisionnels d'investissement et de fonctionnement du district et des crédits.

✓ **Département personnel et moyen commun :** il est chargé principalement du recyclage et la mise à niveau du personnel des différentes structures de l'entreprise**.**

Nous illustrons la direction et les différents services de GPL NAFTAL dans la figure 1.

1.3.2 Les activités principales du district GPL

✓ Organiser et développer la commercialisation et la distribution des produits pétroliers et dérivés.

✓ Veiller au respect des normes et consignes de sécurité sur toute la chaine GPL (transport, installation d'enfûtage et de stockage).

✓ Développer les infrastructures de stockage et de distribution.

✓ Moderniser les infrastructures pour améliorer la productivité, la sécurité et la gestion.

✓ Développer et valoriser les GPL sous toutes ses formes particulièrement vrac et gaz carburant.

✓ Promouvoir, participer et veiller à l'application de la normalisation et du control de la qualité des produits.

✓ Développer le partenariat et la coopération dans le domaine des GPL.

✓ Participer et veiller à la mise en œuvre des actions visant le renforcement de l'intégration économique.

✓ Assurer la maintenance des équipements matériels roulants.

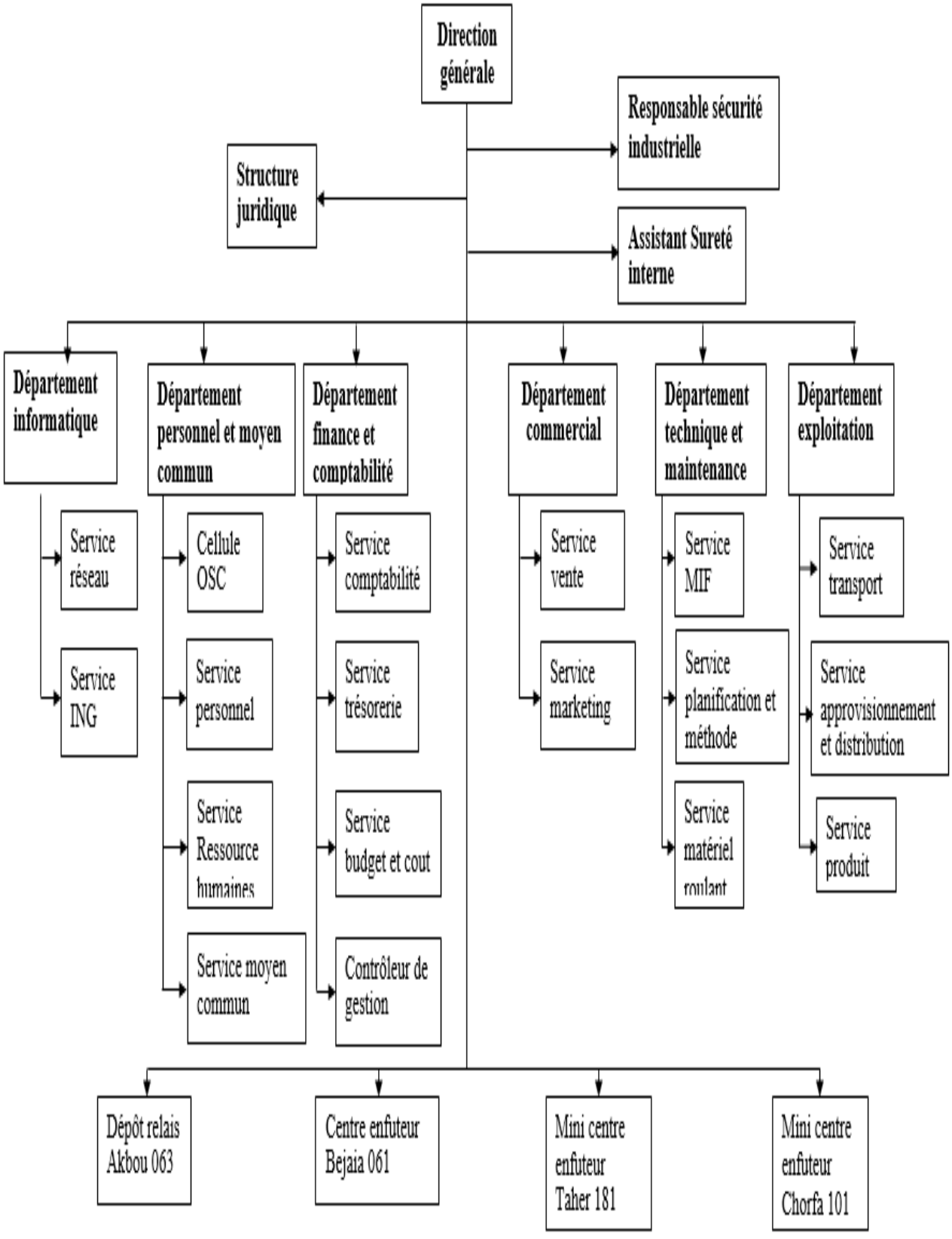

Figure 1: Organigramme de l'entreprise Naftal

1.4 Etude du réseau de l'entreprise

1.4.1 Infrastructure matérielle

GPL NAFTAL de Béjaia dispose d'un réseau informatique important, il est composé de 4 blocs séparés, chaque bloc représente un sous réseau possédant un switch. Ces blocs sont des armoires qui contiennent des équipements différents et chaque bloc se trouve dans un service.

Nous allons à présent présenter les différents matériaux utilisés dans chaque service :

- **La direction** : nous trouvons dans ce service l'armoire principale, elle contient :
  - Un routeur de la marque Cisco 2911 : il permet d'interconnecter deux ou plusieurs réseaux. Le router permet d'acheminer les messages vers la destination à travers sa table de routage.
  - Un Switch Cisco CATALYSTE 2960 : Ce Switch est une configuration fixe, empilable commutateur autonome qui fournit un accès rapide à vitesse filaire Ethernet et Gigabits Ethernet [20].
  - Un panneau de brassage : Il relie les ports des différents équipements réseau aux arrivées des câbles du réseau et à des connecteurs situés sur une baie de brassage. Assurant ainsi une commutation de haute qualité.
  - Deux tiroirs optiques : Les tiroirs sont destinés aux raccordements des câbles en vue d'assurer la distribution sur d'autres câbles ou sur des équipements actifs. Ces fonctions principales sont donc l'arrimage du câble, l'épissurage et le raccordement. Toutes ces fonctions peuvent être réparties sur différents contenants.
  - Un terminal qui joue le rôle d'un adaptateur entre le port Rj45 et le port SFP (Small Form-Factor Pluggable).
  - Un point d'accès (modem) : c'est un dispositif qui permet aux périphériques sans fil de se connecter à un réseau câblé ou au réseau Internet à l'aide d'une connexion radio. Il est habituellement relié à un routeur (par l'intermédiaire d'un réseau câblé), mais il peut aussi faire partie intégrante du routeur lui-même.

Cette armoire est reliée à celle du service des ressources humaines avec un câble Rj45 et à celle du département commercial avec une fibre optique.

En plus de cette armoire nous trouvons dans la direction le serveur qui est la partie la plus importante de toute l'architecture de l'entreprise.

- **Département commercial** : Nous trouvons dans l'armoire de ce département :

- Un tiroir optique.
- Un switch fibre optique CATALYSTE 3750.
- Un panneau de brassage.

Elle est reliée à celle de la direction avec une fibre optique.

- **Service des ressources humaines** : Nous trouvons dans l'armoire de ce service :
  - Un switch Cisco 2911.
  - Un panneau de brassage.

Elle est reliée à celle du service PMC et à celle de la direction avec un câble Rj45 cascade.

- **Service PMC (Personnel et Moyen Commun)** : Dans l'armoire de ce service nous trouvons :
  - Un switch Cisco 2911.
  - Un panneau de brassage.

Elle est reliée à celle du service des ressources humaines avec un câble Rj45 cascade.

Cette architecture est également dotée d'une ligne ADSL qui est utilisée comme étant une liaison d'accès à internet.

1.4.2 Supports de transmission

Afin de relier les différents équipements utilisés, l'entreprise NAFTAL a opté pour deux types de médias :

- **Le câble à paire torsadée :** On distingue deux catégories : le câblage « UTP », terminé par des connecteurs RJ45 et le câble à paire torsadée blindée « STP ».

  Ce type de câble a pour but principal de limiter la sensibilité aux interférences.
- **La fibre optique :** c'est un fil dont l'âme, très fine, en verre ou en plastique a la propriété de conduire la lumière et sert pour la fibroscopie, l'éclairage ou la transmission de données numériques [21].

La table 1 récapitule les différentes caractéristiques de ces supports.

Désignation	Qté
Prises réseaux RJ45 catégorie 6	118
Câble de postes souple 4 paires FTP 3m catégorie 6	118
Fil de terre	0
Borne de terre	0
Câbles de fibre optique souple 6 brins	150m
Tiroir optique avec jarretières	2
Connecteurs de fibre optique	0
Coupleur de fibre optique	4

Table 1: Les supports de transmission.

1.4.3 Gestion de la sécurité

Afin d'assurer la sécurité au sein du réseau, l'entreprise NAFTAL a eu recours à différents moyens :

- ✓ Utilisation d'un firewall qui permet de filtrer les paquets et ainsi autoriser l'accès à un certain type de trafic et interdisant d'autres.
- ✓ Utilisation d'une application de sécurité (Kaspersky Security) pour surveiller l'état de ses machines.
- ✓ Utilisation du contrôleur de domaine « Active Directory » qui est un service d'annuaire développé par Microsoft à destination des domaines Windows permettant de localiser, de sécuriser, de gérer et d'organiser des ressources (fichiers, utilisateurs, groupes, périphériques et appareils réseau) [21]. Et ce dans le but de faciliter la gestion de l'information.

1.4.4 La gestion des employés

Chaque employé dans cette entreprise possède un compte sur son ordinateur crée par le département informatique dès son arrivée et qui est sécurisé par un mot de passe.

L'authentification de l'utilisateur et l'autorisation d'accès à son poste de travail est assuré par le serveur qui demande le nom d'utilisateur et le mot de passe au moment où l'employer allume son pc.

Le serveur fournira également aux employés des dossiers partagés, accessibles à quelques-uns et non à d'autres personnes, en fonction du poste de l'employé.

La figure 2 présente l'architecture du réseau local de GPL NAFTAL Bejaïa.

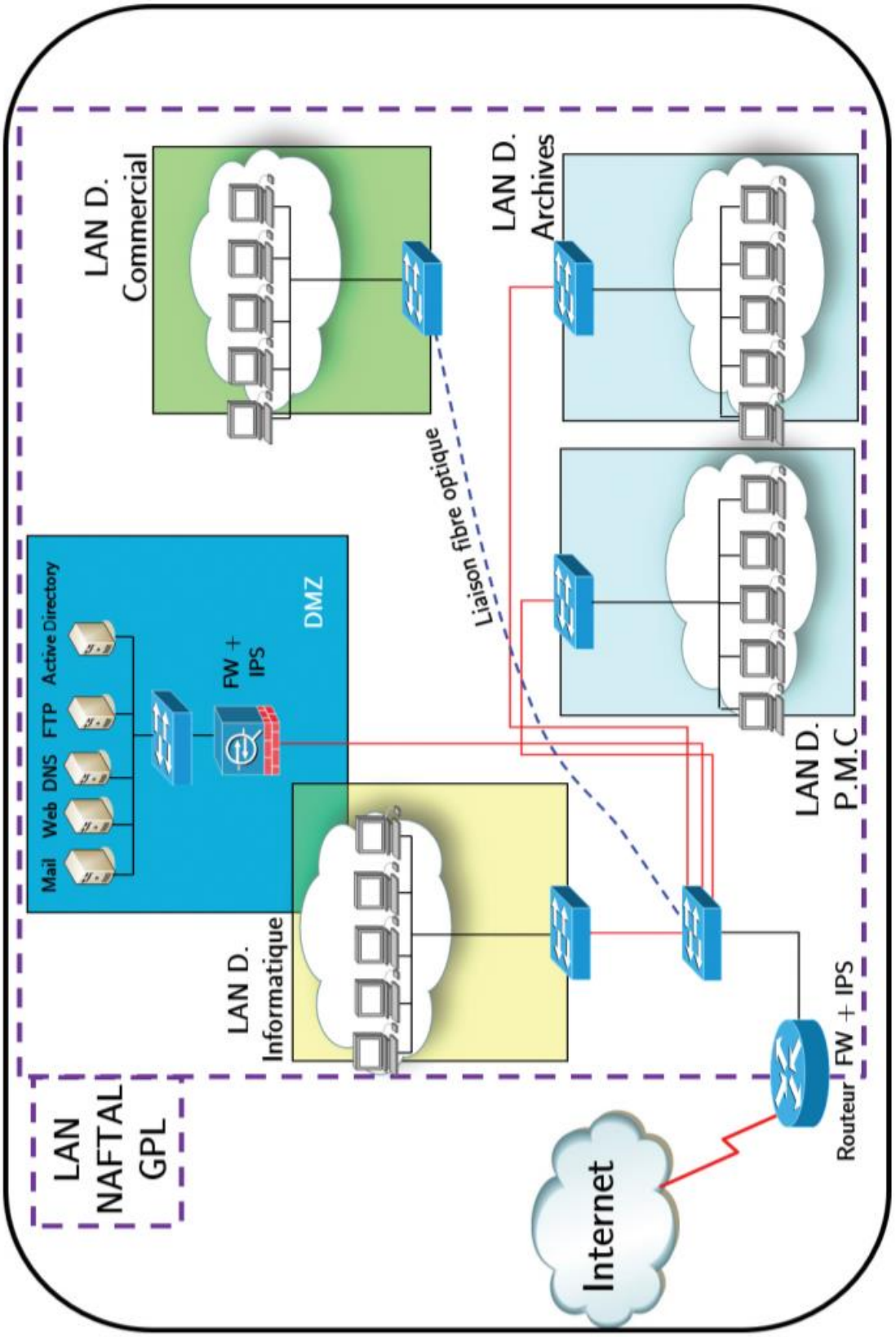

Figure 2: Architecture du réseau GPL

1.5 Présentation du contexte du projet

Dans ce projet nous allons en premier lieu étudier en profondeur les réseaux privés virtuels (VPN) et découvrir les différents aspects de sécurité de ce réseau.

L'intérêt de cette étude est d'établir une communication sécurisée entre la direction GPL NAFTAL de Bejaïa avec ses différents districts (Jijel, Akbou et Bouira), qui sont actuellement relié à travers un réseau Internet. Cette communication sécurisée se fera à travers un VPN (Virtual Private Network) utilisant le protocole de sécurité IPsec (Internet Protocol Security).

1.5.1 Problématique

Après avoir analysé l'état actuel des communications de l'entreprise avec les districts à laquelle elle est reliée, on a soulevé les différents problèmes suivants :

- Les échanges de données se font à travers un réseau public (Internet) ou un réseau privé (opérateur), ce qui rend les échanges vulnérables et ainsi y'a un risque d'atteinte à leur sécurité.

- Même si l'entreprise est dotée d'un Active directory il y'a un risque d'attaque ou de piratage au niveau du réseau interne car ce dernier n'assure pas totalement le contrôle des intrusions externes à l'entreprise. Il est donc facile de récupérer le mot de passe d'un employé et ainsi accéder à des données confidentielles.

1.5.2 Solution proposée

Après avoir analysé le contexte du système actuel, nous avons suggéré de mettre en place une architecture VPN site-à-site avec le protocole IPsec entre les sites distants du district GPL NAFTAL Bejaia ; Dans le but de remédier aux différentes lacunes soulevées durant notre stage à des coûts réduits mais garantissant la performance, la sécurité, la confidentialité et la disponibilité des données échangées.

1.6 Conclusion

Dans ce chapitre nous avons commencé par présenter le district GPL NAFTAL de Bejaia, ce qui nous a permis de nous familiariser avec ce dernier, puis nous avons étudié la topologie de son réseau et pris la connaissance des matériaux utilisés pour enfin dégager ses faiblesses, parmi elles la sécurité, ce qui nous mènera dans le chapitre suivant à détailler la sécurité informatique.

Chapitre 02

La sécurité informatique

2.1 Introduction

La sécurité des systèmes informatiques constitue un enjeu crucial, et elle est devenue un problème majeur dans la gestion des systèmes informatiques.

En effet, Quand on parle de sécurité, nous faisons référence aux pirates, virus, vers, cheval de Troie, etc. Ils profitent de failles des protocoles, du système, mais surtout du fait que le réseau n'était pas développé dans une optique « sécurité ».

Tout au long de ce chapitre, notre intérêt se porte sur les principales menaces pesant sur la sécurité informatique ainsi que les mécanismes de défense et l'importance de la politique de sécurité.

2.2 Définition

La sécurité informatique consiste à protéger les ressources matérielles ou logicielles (ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données) contre les attaques malveillantes et atteindre un certain niveau de protection par un ensemble des moyens outils, techniques et méthodes.

La sécurité informatique permet aussi de garantir que seules les personnes ou autres systèmes autorisés interviennent sur le système et ont accès aux données, sensibles ou non [1], [3].

2.3 Objectif de la sécurité informatique

La sécurité informatique à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, Néanmoins, les principaux points sont les suivants :

- **Authentification** : Est une procédure qui permet à un système informatique de vérifier l'identité d'une personne ou d'un ordinateur par un élément d'information que l'utilisateur connaît (mot de passe), un élément que l'utilisateur possède (carte à puce) ou une caractéristique physique propre à l'utilisateur (la biométrie).

- **Confidentialité :** Garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources qui leur sont destinées. Tout accès indésirable doit être empêché.

Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

  - Limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
  - Le chiffrement des données de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

- **Intégrité** : assurer que l'information contenue dans les objets n'est ni créée, ni altérée, ni détruite de manière non autorisée. L'intégrité peut être définie comme la capacité du système à empêcher la corruption d'informations par les fautes accidentelles ou intentionnelles, et à garantir leur mise à jour correcte [4].
- **Disponibilité :** garantir l'accès aux ressources, au moment voulu, aux personnes habilitées d'accéder à ces ressources.
- **Non-répudiation** : C'est la propriété qui assure la preuve de l'authenticité d'un acte de la manière suivante :

  - **La non-répudiation de l'origine :** elle fournit au récepteur une preuve empêchant l'émetteur de contester l'envoi d'un message ou le contenu d'un message effectivement reçu.
  - **La non-répudiation de la remise :** elle fournit à l'émetteur une preuve empêchant le récepteur de contester la réception d'un message ou le contenu d'un message effectivement émis.

2.4 Domaines d'application de la sécurité informatique

La sécurité informatique intervient dans plusieurs domaines, nous allons les présenter ci-dessous :

- **La sécurité physique et environnementale :** La sécurité physique et environnementale concerne tous les aspects liés à la maîtrise des systèmes et de l'environnement dans lesquels ils se situent [7]. Elle repose essentiellement sur :
  - La protection de l'environnement (d'incendie, inondation ...ect)
  - Contrôle des accès physiques aux locaux, équipements et infrastructures
  - L'usage d'équipements qui possèdent un bon degré de sûreté de fonctionnement et de fiabilité
  - La redondance physique des infrastructures et sources énergétiques.
  - Le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver.
  - Le plan de maintenance préventive et corrective des équipements.
- **La sécurité logique :** La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts

et à la protection des données. Elle s'appuie généralement sur la cryptographie, des procédures de contrôle d'accès logique et d'authentification, des procédures de détection de logiciels malveillants, de détection d'intrusions et d'incidents et aussi sur des procédures de sauvegarde et de restitution des informations sur des supports fiables sécurisé et protéger.

- **La sécurité applicative :** La sécurité applicative comprend le développement pertinent de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels. Elle repose sur un ensemble de facteur tel que :

  - L'intégration de mécanismes de sécurité, d'outils d'administration et de contrôle de qualité dans les applications,
  - La robustesse des applications
  - Respect des normes de développement propre à la technologie employée et aux contraintes d'exploitabilité).
- **La sécurité de l'exploitation :** La sécurité de l'exploitation doit permettre un bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, et des mises à jour.

- **Sécurité des infrastructures de télécommunication :** La sécurité des télécommunications consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information, et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

2.5 Problèmes liés à la sécurité informatique

Les systèmes informatiques sont exposés à différents types de problèmes et de menaces. Nous allons citer ci-dessous les risques les plus courants :

- **Vulnérabilités :** Les vulnérabilités représentent les failles ou faiblesses des entités qui composent ou interagissent avec le système informatique. Elles sont susceptibles d'être exploitées par des éléments menaçants, utilisant une méthode d'attaque pour consulter, détruire, usurper ou modifier un bien. Elle peut être humaine, technologique, organisationnelle ou une mise-en-œuvre [5].

- **Menaces :** C'est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système et généralement préjudiciable. Nous distinguons deux types d'attaques :

  - **Menaces passives :** Une personne malveillante tente de lire ou d'utiliser les informations du système, nuisant ainsi à la confidentialité des données.

- **Menaces actives :** Une personne malveillante tente de modifier les ressources du système ou d'affecter leur fonctionnement.

Ce type de menaces porte atteinte à l'intégrité et à la disponibilité des ressources.

- **Intrusions :** Une intrusion est une attaque malveillante d'origine interne ou externe, qui permet à un utilisateur illégitime d'exploiter une vulnérabilité dans le système afin contrôler ou d'accéder à certaines ressources. Une intrusion peut prendre la forme d'un virus, d'un ver ou d'un cheval de Troie.

- **Logiciels malveillants :** Un logiciel malveillant est un programme informatique qui réalise volontairement une action allant à l'encontre de l'intérêt de l'utilisateur. Ils exploitent les vulnérabilités d'un autre programme pour causer des dommages ou usurper des données. Ils viennent sous diverses formes : certains se reproduisent, d'autres détruisent ou volent des informations. Ils peuvent être classés selon [7] :

  - Mode d'exécution ;
  - Mode de propagation ;
  - Les activités malicieuses ;

Parmi ces logiciels, on peut citer :

Virus : un virus est un programme qui se reproduit en accolant son code à un autre programme du système ou d'une application et qui est susceptible d'entrainer diverses perturbations dans le fonctionnement de l'ordinateur. Ce programme est capable de s'installer sur un ordinateur à l'insu de son utilisateur légitimes et il peut ainsi se propager à d'autres ordinateurs via le réseau [7][8].

Vers : un ver est un programme semblable au virus mais qui est autonome. Il peut s'auto-reproduire automatiquement grâce à une vulnérabilité logicielle, et se déplacer à travers un réseau, en utilisant les mécanismes réseaux, sans avoir réellement besoin d'un support logique ou physique pour se propager [8].

Cheval de troie : c'est un programme en apparence légitime, qui est dissimulé au sein d'un autre programme. En lançant ce dernier, le trojan caché s'active, ouvrant ainsi une ou plusieurs portes virtuelles sur la machine. L'hacker peut alors s'introduire dans le système de manière invisible et ainsi détourner, diffuser ou détruire des informations, ou encore ouvrir une porte dérobée [7][8].

Portes dérobées : une porte dérobée est un logiciel de communication caché, installé par un virus ou par un cheval de Troie, dont l'objectif est de contourner les procédures d'authentification afin de fournir un accès à distance à un ordinateur via le réseau, et un control presque total sur la machine attaquée, permettant ainsi :

- Échange de fichiers ;
- Modification des paramètres systèmes ;
- Tuer des processus ;
- Ouverture/fermeture du lecteur CD ROM ;

Logiciels espions : un logiciel espion est un programme qui recueil des informations au sein du système où il est installé à l'insu des utilisateurs, à un agent externe sans autorisation.

Logiciels publicitaires : un logiciel publicitaire est un logiciel qui lors de son utilisation, affiche des annonces publicitaires menant à des sites commerciaux, qui sont renouvelées à chaque nouvelle connexion à Internet. Leurs principaux buts sont d'observer les habitudes de navigation de l'internaute, et dans le pire des cas, le vol des informations personnels.

Rootkit : un rootkit, aussi appelé « outils de dissimulation d'activité » est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est de dissimuler les processus de l'attaquant, et d'inclure des backdoors afin de pouvoir reprendre l'accès plus tard et exploiter des logiciels pour attaquer d'autres systèmes [7].

2.6 Attaques informatiques

Une attaque informatique est définie comme une faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire, y compris les attaques lancées par des outils automatiques : vers, virus, etc. [9]. L'objectif principal de cette démarche consiste à voler des informations et obtenir des données confidentielles, troubler le bon fonctionnement d'un service, utiliser le système compromis pour attaquer un autre ou même dans un but lucratif.

Les hackers utilisent plusieurs techniques d'attaques pour nuire à un système informatique. On distingue trois types d'attaques :

2.6.1 Attaques directes

C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son ordinateur à l'aide d'un logiciel ou d'un script lui permettant d'envoyer directement les paquets à la victime [10].

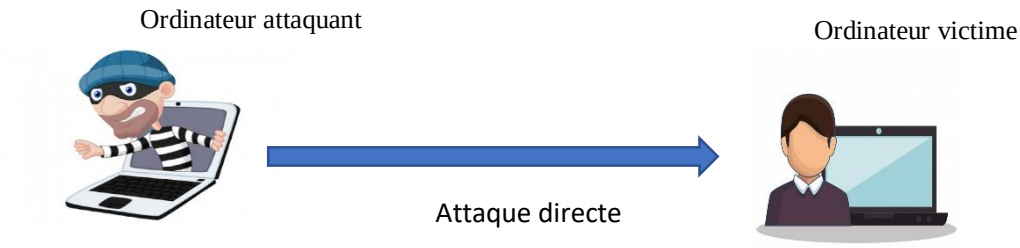

Figure 3: Attaque direct

2.6.2 Attaques indirectes par rebond

Appelée « attaque indirecte par rebond » car le principe est d'envoyer les paquets d'attaque à l'ordinateur intermédiaire, qui à son tour répercute l'attaque vers la victime.
Ce type d'attaque est appréciée des personnes malveillantes, car elle permet de :

- Masquer l'identité de l'hacker ;
- Utiliser les ressources de l'ordinateur intermédiaire pour attaquer car il est plus puissant (CPU, bande passante …) [10].

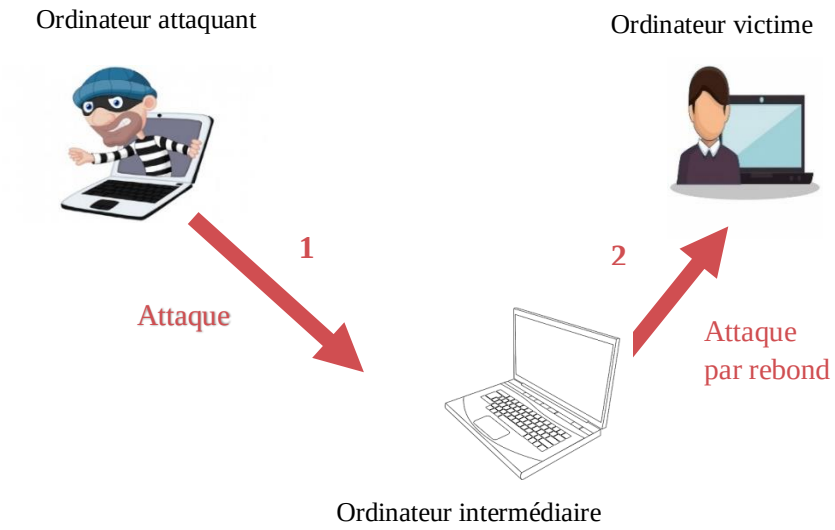

Figure 4: Attaque indirecte par rebond

2.6.3 Attaques indirectes par réponse

Cette attaque est dérivée de l'attaque indirecte par rebond, et offre les mêmes avantages à l'hacker.

Dans ce type d'attaque, l'attaquant envoie une requête à l'ordinateur intermédiaire au lieu de lui envoyer une attaque pour qu'il la répercute. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime [10].

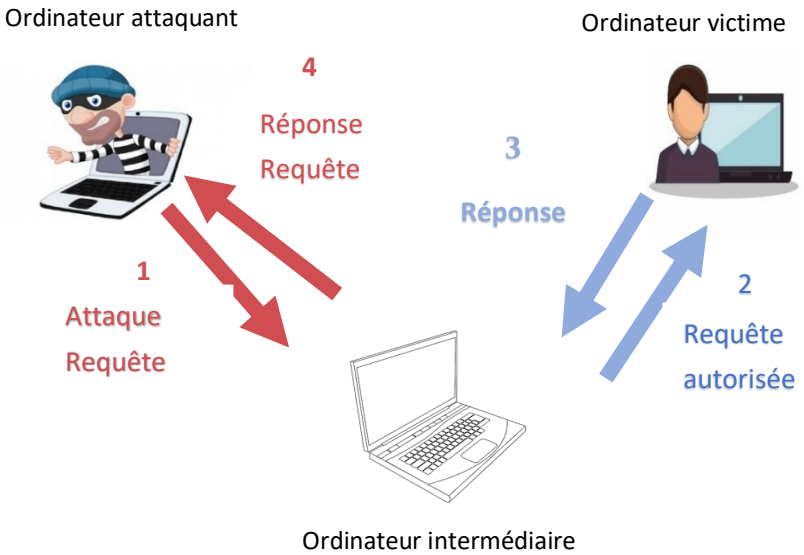

Figure 5: Attaque indirecte par réponse

2.7 Classification des attaques

On distingue quatre catégories d'attaques :

2.7.1 Attaques par interruption

Cette attaque porte atteinte à la disponibilité des ressources, car une pièce maitresse du système est détruite ou devenue indisponible ou inutilisable.

Exemple :

- **Déni de service (Dos)** : c'est une attaque qui a pour but de saturer un router ou un serveur afin d'obtenir le contrôle d'une machine ou d'un réseau ou de le détruire [12], et permet aussi de paramétrer un système d'information.

2.7.2 Attaques par interception

Cette attaque porte atteinte à la confidentialité des données. Une tierce partie qui peut être une personne, un programme ou un ordinateur, peut avoir un accès non autorisé à certaines pièces essentielles du système [11].

Exemple :

- **Man in the middle :** désigne un modèle de cyberattaque dans lequel un cybercriminel installe, physiquement ou logiquement, un système contrôlé appelé « sniffer » entre le système de la victime et une ressource Internet qu'elle utilise. L'objectif de l'attaquant est d'intercepter, de lire ou de manipuler toute communication entre la victime et sa ressource sans se faire remarquer.

2.7.3 Attaques par modification

Dans cette catégorie d'attaques, une tierce partie obtient un accès non autorisé à une pièce maitresse du système et tente de le modifier. Cette pratique porte atteinte à l'intégrité des ressources [11].

Exemple :

- **XSS (Cross-Site Scripting) :** est une faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur le navigateur web visitant la page tels que l'usurpation de l'identité de la victime,le vol d'information.

2.7.4 Attaques par fabrication

C'est une attaque portée à l'authenticité. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier [11].

Exemple :

- **Ip spoofing :** Le spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible. Le pirate ensuite attaque le serveur cible en utilisant l'adresse IP falsifier [13].

2.8 Politique de sécurité

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité du réseau d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie. Chaque entreprise ou organisme doit se doter d'une politique de sécurité de l'information afin de protéger ses biens. Il s'agit également d'une question de crédibilité face à ses clients, fournisseurs et actionnaires [8].

La sécurité d'un réseau est la sécurité des éléments qui le compose, il existe plusieurs mécanismes et dispositifs de sécurité, parmi eux :

2.8.1 Les antivirus

Les antivirus sont des logiciels capables d'identifier, neutraliser, éliminer et mettre en quarantaine des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programmes modifiants ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur, et parfois, ils permettent aussi de réparer les fichiers infectés sans les endommager [13]. Ils utilisent pour cela de nombreuses techniques, parmi lesquelles :

- Le contrôle général du système de l'ordinateur.
- Les signatures suspectes.
- Les instructions et ordres suspects.
- La surveillance des lecteurs de supports amovibles.

2.8.2 Les pare-feu (firewalls)

Un pare-feu est une structure logicielle ou matérielle située entre l'utilisateur et le monde extérieur afin de protéger le réseau interne des intrusions extérieures. Ses dispositifs permettent de filtrer les trames des différentes couches du modèle TCP/IP afin de contrôler le flux de trafic et accorder ou refuser à certains hôtes l'accès à une section réseau. Les rôles d'un pare-feu sont :

- Limiter le trafic réseau et accroitre les performances.
- Déterminer le type de trafic qui sera acheminé ou bloqué.
- Contrôler le flux de trafic.
- Fournir un niveau de sécurité d'accès réseau de base.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- Translation d'adresses ou de ports.

2.8.3 La DMZ (DeMilitarized Zone)

Une zone démilitarisée (ou DMZ, DeMilitarized Zone) est une zone de réseau privée ne faisant partie ni du LAN privé ni de l'Internet. La DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire formant ainsi un sous réseau. Ce sous réseau est isolé par un firewall qui bloque les données parvenant d'un réseau internet d'accéder au réseau local mais avec des règles de filtrage moins contraignantes [14].

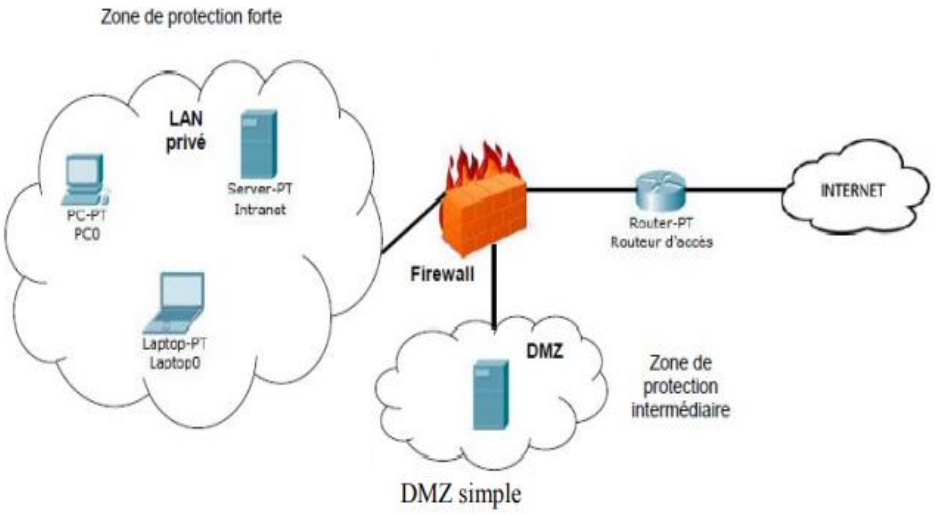

Figure 6: Mise en place d'une DMZ

Il est possible d'augmenter le niveau de sécurité de la DMZ en introduisant un deuxième pare-feu, avec des règles moins restrictives introduites par le premier firewall.

2.8.4 Les IDS (Intrusion Detection System)

Un IDS (Intrusion Detection System), est un mécanisme permettant d'écouter le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et ainsi prévenir les risques d'intrusions [15]. Ils fournissent un complément technologique aux firewalls en leur permettant une analyse plus intelligente du trafic. Les produits de détection d'intrusions (IDS), développés parallèlement aux firewalls, permettent d'analyser plus finement les informations afin de détecter les véritables attaques et en évitant le plus possible les fausses alertes.

Il existe deux niveaux d'IDS : les IDS systèmes et les IDS réseau ;

- **Les IDS systèmes (host IDS) :** analysent le fonctionnement et l'état des machines sur lesquels ils sont installés afin de détecter les attaques.
  Ces IDS sont limités et ne peuvent détecter les attaques provenant de la couche réseau tels que les attaques de type DOS.
- **Les IDS réseaux (Network IDS) :** analysent quant à eux le trafic qu'ils aspirent en temps réel. Ensuite les paquets sont décortiqués puis analysés, et en cas de détection d'intrusion, des alertes sont envoyées.

Il existe deux différentes approches qui permettent de détecter les intrusions :

- **Les IDS à signature :** le profil de chaque attaque est représenté par un ensemble de signature, qui est habituellement définie comme une séquence d'évènements et de conditions relatant une tentative d'intrusion.

Cette approche consiste à rechercher les empreintes d'attaques connues, et si une attaque est détectée, une alarme peut être remontée (si l'IDS est en mode actif, sinon, il se contente d'archiver l'attaque).

- **Les IDS comportementaux :** la principale fonctionnalité de ce type d'IDS est la détection d'anomalie. Leur déploiement nécessite une phase d'apprentissage pendant laquelle l'outil va apprendre le comportement "normal" des flux applicatifs présents sur son réseau.
  Ainsi, chaque flux et son comportement habituel doivent être déclarés, et si un flux anormal a été détecté et ne pourra spécifier la criticité de l'attaque, l'IDS se chargera d'émettre une alarme.

2.9 Conclusion

Au cours de ce chapitre nous avons présenté les aspects fondamentaux de la sécurité informatique à savoir : la confidentialité et l'intégrité des données, mais aussi les différentes attaques qui portent atteinte à la sécurité d'un réseau informatique et les mécanismes de défenses requises.

Chapitre 03

Généralité sur les VPN et sur le protocole IPsec

3.1 Introduction

Toutes les entreprises sont une cible pour les pirates et tout autre système qui vise à nuire à la sécurité des données. Et afin de remédier à ces problèmes et surtout pour protéger les données échangées entre les différents sites de l'entreprise, cette dernière utilise des méthodes de sécurité telle que la tunnelisation.

En parlant de tunnelisation on parle de protocoles, et parmi les protocoles de tunnelisation les plus utilisé on cite IPsec.

Dans ce chapitre nous allons nous intéresser aux VPN notamment leurs cas d'utilisation, leurs avantages, leurs contraintes et les principaux protocoles utilisés, ensuite nous allons détailler le protocole IPsec.

3.2 Définition des Réseaux privés virtuels (VPN)

Le VPN (Virtual Private Network) permet d'établir des connexions sécurisées privées (un réseau privé) au travers d'un réseau public comme l'Internet. Ce dernier est réalisé avec les techniques d'encryptions et d'authentification, en assurant la qualité de services requise par les applications.

Un réseau VPN repose sur le protocole de tunneling. Ce protocole permet de circuler les informations de l'entreprise de façon crypté d'un bout à l'autre du tunnel. Le principe du tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite les données sont chiffrées à la source, puis acheminées en empruntant ce chemin virtuel.

Le VPN permet un accès peu couteux aux intranets et aux extranets de l'entreprise en simulant un réseau privé, alors qu'ils utilisent en réalité une infrastructure partagée comme internet [15].

3.3 Cas d'utilisation

On peut trouver plusieurs cas d'utilisation d'un VPN dont :

- Connexion à distance pour les utilisateurs mobiles ou télétravailleurs.
- Connexion de sites distants.

3.4 Avantages des VPN

Parmi les atouts des VPN on cite :

- **La sécurité :** assure des communications sécurisées et chiffrées.
- **La simplicité :** utilise les circuits de télécommunication classique.
- **L'économie :** les économies sur les budgets alloués à la connectivité. Ces économies sont obtenues en remplaçant les connexions longues distances via des lignes louées privées par une connexion unique à Internet sur laquelle on implémente des tunnels VPN afin de réaliser un réseau privé à travers Internet.

3.5 Contraintes des VPN

Pour assurer la transparence vis-à-vis des utilisateurs et des applications qui y ont accès, un VPN doit être capable de mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur : Accès au canal autorisé uniquement aux utilisateurs enregistrés.
- Cryptage des données : Les données doivent être cryptées lors de leurs acheminements sur le réseau public.
- Gestion de clés : les clés de cryptages pour le serveur et le client doivent pouvoir être générées.
- Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics, en particulier IP.

3.6 Typologies des VPN

Il existe deux catégories de VPN : VPN d'entreprise et VPN d'opérateur qui peuvent être utilisé simultanément ou séparément au sein d'une même entreprise.

Nous allons ci-dessous les définir et présenter les différents atouts et inconvénients de chacune d'elles.

3.6.1 VPN d'entreprise

Dans ce cas l'entreprise garde le contrôle des établissements des VPN entre ses différents points de présence ainsi qu'entre ses postes situés à l'extérieur de l'entreprise et les sites principaux. Il existe trois types de VPN d'entreprise et qui sont : les VPN site à site, les VPN poste à site, et les VPN poste à poste.

3.6.1.1 VPN site à site

Les VPN Site-à-Site aussi appelés router-à-router construisent un réseau virtuel qui unit des réseaux issus de localisations variées pour les connecter à Internet et maintenir des communications sécurisées et privées entre eux. Ce type de VPN se base sur intranet afin de relier le réseau des bureaux principaux au reste des bureaux d'une même entreprise, et se base sur extranet lorsqu'il s'agit de relier une entreprise à une autre.

Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments Matériels (routeurs ou pare-feu) situés entre le réseau interne et le réseau publique de chaque site et se sont ces derniers qui se chargent de l'authentification, du routage des paquets, du cryptage et du décryptage [19].

Avantages et inconvénients

Parmi les atouts que présente le VPN site à site, nous citons :

- Il permet à deux machines de réseaux différents de se joindre en utilisant seulement les adresses privées.
- Le travail de mise en tunnel est effectué par les équipements d'extrémité (routeurs ou firewalls), ce qui d'une part permet de ne pas charger les postes de travail et d'autre part permet d'utiliser éventuellement des composants électroniques dédiés au cryptage par exemple, d'où de meilleures performances.

En l'occurrence cette solution présente quelques contraintes :

- Il ne permet pas de protéger la conversation de bout en bout puisque le flux est seulement crypté entre les deux extrémités du tunnel (routeurs ou pare-feu).
- L'établissement des VPN nécessite que les deux extrémités soient bien identifiées soit par une adresse IP publique fixe, soit par un nom référencé dans des DNS officiels.

3.6.1.2 VPN poste à site

Ce type de VPN est aussi fréquemment utilisé et permet aux utilisateurs distants (télétravailleurs …) d'accéder aux ressources de l'entreprise via un VPN. Pour cela, un utilisateur distant a simplement besoin d'un client VPN installé sur son ordinateur pour se connecter au site de l'entreprise.

Afin de réaliser cette solution, un matériel (firewall, routeur…) sera mis en place sur le site central, constituant le point de terminaison de tous les VPN de ce dernier. Et un logiciel gérant le type de protocole choisi et compatible avec le matériel du site central est installé du côté des postes de travail distant. Dans certain cas, ce logiciel est déjà présent dans le système d'exploitation de ces postes, dans d'autre cas, il est nécessaire d'installer ce composant logiciel [19].

Avantages et inconvénients

Parmi les atouts que présente le VPN poste à site, nous citons :

- Permet potentiellement à n'importe quelle machine distante, qu'elle soit isolée ou sur un réseau, de joindre une ou plusieurs machines d'un autre réseau en utilisant seulement les adresses privées.
- Communication cryptée entre le poste et le pare-feu de l'entreprise.
- Transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification.

En l'occurrence cette solution présente quelques contraintes :

- Une installation logicielle est généralement nécessaire sur le poste distant

- Le cryptage impose une charge non négligeable au poste distant, ce qui peut en dégrader les performances.
- Le cryptage n'est pas assuré au-delà du firewall du site central.

3.6.1.3 VPN poste à poste

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

Pour cette configuration, nous ne faisons intervenir que des composants logiciels : un logiciel client sur le poste « demandeur » et un logiciel utilisé en serveur sur le poste « destinataire » [19].

Avantages et inconvénients

Le VPN poste à poste présente comme intérêt majeur de protéger la conversation de bout en bout. Il est donc particulièrement indiqué dans des contextes où le besoin de confidentialité est primordial.

- La mise en place d'un réseau de VPN entre tous les postes (ou une grande partie) serait compliquée à déployer d'un point de vue pratique.
- L'utilisation de protocoles de VPN en maillage d'un nombre important de postes peut avoir un impact négatif sur leurs performances ainsi que sur les besoins en matière d'assistance aux utilisateurs finaux.
- Le cryptage est uniquement logiciel d'où un possible impact sur les performances en cas de fort débit, notamment quand les deux extrémités sont sur le même réseau local.

3.6.2 VPN opérateur

C'est un réseau privatif mis en place par un opérateur afin d'interconnecter plusieurs sites d'une entreprise. Ce type de réseau est plus couteux que les VPN d'entreprise mais offre de grandes performances, la disponibilité et une communication sécurisée entre les différents sites. On parle alors plus de réseaux de tunnels que de véritable réseau VPN [19].

Avantages et inconvénients :

Parmi les atouts que présente ce type de réseau on cite :

- Permet de réduire la complexité d'un grand réseau.
- Ajouter de la QoS sur les liaisons en fonction des relations entre les différents sites pour privilégier les trafics les plus prioritaires et garantir à ceux-ci un maximum de bande passante.
- Offre une assurance sur les performances proposées par le réseau aussi bien en termes de débit que de temps de transit des messages.

En l'occurrence cette solution présente quelques contraintes :

- Les couts sont élevés.
- Il faut avoir un seul opérateur pour l'ensemble du réseau VPN.

- Ajouter un protocole de cryptage entre les postes ou les sites pour assurer la confidentialité des échanges.

3.7 Protocoles utilisés

Un réseau privé virtuel ou VPN sécurise et rend anonyme votre connexion Internet en vous connectant à un serveur distant avant d'accéder à des sites Web. La connexion à ce serveur est également cryptée, ce qui ne signifie qu'aucune de vos requêtes Web ne peut être vue par le monde extérieur, et ce grâce aux protocoles de cryptage utilisés.

Nous allons présenter ci-dessous les protocoles les plus communément utilisés avec les VPN.

3.7.1 Protocole PPP (Point to Point Protocol)

C'est un protocole de la couche liaison de données qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garanti l'ordre d'arriver des paquets, mais non sécurisé.

PPP est généralement employé entre un client d'accès à distance et un serveur d'accès réseau [15].

3.7.2 Protocole PPTP (Point to protocole Point Tunneling Protocol)

C'est un protocole de la couche liaison de données qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN) pour envoyer des données depuis un périphérique distant, authentifié uniquement par un mot de passe. Il n'implique donc aucune installation de matériel supplémentaire.

Le principe de ce protocole est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP [15].

Avantages et inconvénients :

Parmi les avantages de ce protocole on cite :

- Facilité d'installation et de configuration sur toutes les plateformes (Windows, Mac os, Linux…).
- C'est un protocole fluide et rapide.

Néanmoins il présente quelques inconvénients :

- Niveau de sécurité faible à cause de l'absence de cryptage des données.
- Il est facilement blocable par les fournisseurs d'accès à internet.

3.7.3 Protocole L2TP (Layer 2 Tunneling Protocol)

L2TP est un protocole réseau de la couche liaison de données qui permet de créer des réseaux privés virtuels (VPN) entre un opérateur de collecte de trafics tels qu'ADSL ou les opérateurs de téléphonies et les fournisseurs d'accès à internet.[15].

Ce protocole est basé sur deux protocoles de tunneling plus anciens appelés L2F et un protocole PPTP et à lui seul il ne fournit pas de cryptage, pour cette raison, il est souvent associé à un protocole de cryptage IPsec.

Avantages et inconvénients

Parmi les avantages de ce protocole on cite :

- Crypte les données et offre une meilleure sécurité que le protocole PPTP.
- Assure l'intégrité et l'authentification des données d'origine.
- Utilise le protocole UDP, ce qui le rend plus rapide et plus facile à configurer avec certains pares-feux.

Néanmoins, ce protocole présente certains désavantages :

- Ce protocole encapsule les données deux fois ce qui le rend un peu lent.
- Coûts élevés.

3.7.4 Protocole SSTP (Secure Socket Tunneling Protocol)

SSTP est l'un des protocoles les plus sécurisés utilisés dans les tunnels VPN. Il a été développé par Microsoft mais il est aussi compatible avec Linux.

Ce protocole est un type de tunnel VPN qui fournit un mécanisme pour transporter PPP ou L2TP à travers un canal SSL, et ce dernier fournit une sécurité au niveau transport avec une négociation de clés le chiffrement, et le contrôle de l'intégrité des données. L'utilisation de SSL sur le port TCP HTTPS permet à SSTP de passer facilement à travers les pare-feu et les serveurs proxy.

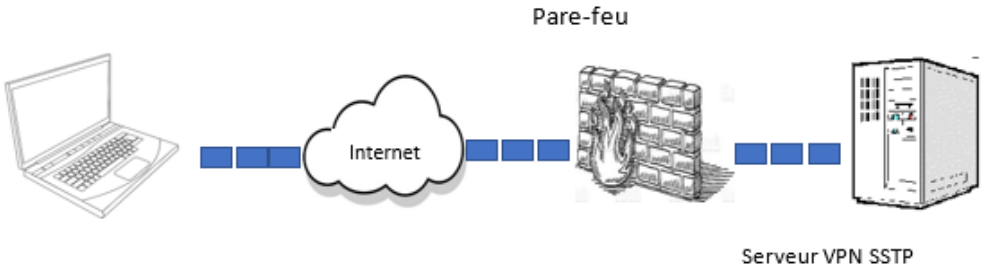

Figure 7: Protocole VPN SSTP

Avantages et inconvénients

Parmi les avantages de ce protocole on cite :

- A la capacité de contourner la plupart des pares-feux grâce au port qu'il utilise.
- Offre le plus haut niveau de sécurité à savoir un cryptage AES 256 bits.
- Développé par Microsoft entièrement compatible avec Windows.

Néanmoins il présente les inconvénients suivants :

- Vitesse lente en raison du haut niveau de cryptage qu'il offre.
- Il ne peut être audité par aucune autre tierce partie pour vérifier ses vulnérabilités car il appartient à Microsoft.

3.7.5 Protocole SSL (Secure Socket Layer)

SSL est un protocole de la couche transport du modèle OSI, utilisé par une application pour établir un canal de communication sécurisé avec une autre application. Pour cela, il assure l'authentification du serveur et du client à l'établissement de la connexion et il chiffre les données durant la connexion.

Le protocole SSL est celui qui est utilisé en standard pour les transactions sécurisées sur internet et ne nécessite qu'un navigateur internet standard, néanmoins il présente un inconvénient car il se limite au protocole https, ce qui n'est pas le seul besoin de connexion des entreprises.

3.7.6 Protocole IPsec (Internet Protocol Security)

IPSec a été conçu pour sécuriser les communications réseau à partir de la couche réseau ce qui lui permet donc de sécuriser tout type d'applications et protocoles réseau basés sur IP. Il a été conçu de manière à être supporté par Ipv4 et a été intégré dans le protocole Ipv6.

Le protocole IPSec vient complémenter le protocole IP. Ainsi, il intègre des notions essentielles de sécurité au datagramme IP qui vont assurer l'authenticité, l'authentification et le cryptage [15].

3.8 Présentation de IPsec

3.8.1 Généralités

IPsec (Internet Protocol Security) est un protocole de sécurité développé par l'IETF (RFC 2401) en 1995, c'est un protocole de la couche 3 du modèle OSI (couche réseau) qui désigne un ensemble de mécanismes destinés à protéger le trafic au niveau d'IP (IPv4 ou IPv6).

L'intérêt principal de l'IPsec reste sans conteste son mode dit tunneling c'est-à-dire d'encapsulation d'IP qui lui permet entre autres de créer des VPN. Il permet la liaison entre deux systèmes informatiques, en toute sécurité, en prenant appui sur un réseau existant [16].

Optionnel dans IPv4, IPsec est obligatoire pour toute implémentation d'IPv6. Une fois IPv6 en place, il sera ainsi possible à tout utilisateur désirant des fonctions de sécurité d'avoir recours à IPsec.

3.8.2 Aspect technique

IPsec est en effet basé sur plusieurs protocoles différents normalisés par l'IETF qui fournissent des services de sécurisations des données : le protocole principal utilisé est IKE (Internet Key Exchange, RFC 2409) qui a pour rôle de gérer la négociation entre les deux machines.

En plus d'IKE, IPsec repose aussi sur les deux protocoles AH (Authetification header) et ESP (Encapsulating Security Playload) qui visent à sécuriser les communications IP en

assurant la confidentialité, l'authentification et l'intégrité des données grâce aux algorithmes de chiffrements et les algorithmes d'authentifications.

Ces deux protocoles, AH et ESP, peuvent être utilisés séparément ou combinés pour caractériser le niveau de sécurité voulu. De plus, il est possible d'indiquer les algorithmes de hachage ou de cryptage voulu lors d'une communication [17].

Les clés de session sont de type symétrique (définition manuelle des clés) ou asymétrique (génération automatique des clés).

3.8.3 Les services proposés par IPsec

Le protocole IPsec offre plusieurs services que l'on va citer ci-dessous :

- **L'authentification :** cette authentification mutuelle permet de s'assurer de l'identité de son interlocuteur, elle est basée sur des clés pré-partagées, des certificats, des adresses IP…ect
- **L'intégrité :** IPsec permet de s'assurer que le paquet n'a pas été modifié durant son trajet (empêche l'attaque active).
- **La confidentialité :** IPsec permet d'empêcher à n'importe quel attaquant de lire ou d'intercepter les données transmises (empêche l'attaque passive)
- **La non-répudiation :** IPsec permet d'identifier l'émetteur d'un paquet de sorte que ce dernier ne puisse nier d'être l'auteur du message (en utilisant la signature numérique).
- **Protection contre les écoutes et analyses de trafic** : IPSec utilise le mode tunneling qui consiste à chiffrer les adresses IP réelles de la source et de la destination, ainsi que tout l'en-tête IP correspondant, afin d'empêcher tout attaquant à l'écoute d'inférer des informations sur les identités réelles des extrémités du tunnel, sur les protocoles utilisés au-dessus d'IPSec, sur l'application utilisant le tunnel (timing-attacks et autres) [2].
- **L'anti-rejeu :** IPsec aide à la protection contre les attaques qui consiste à capturer un ou plusieurs paquets pour les envoyer au destinataire sans avoir besoin de les déchiffrés pour bénéficier des mêmes avantages que l'émetteur initial [2].

3.8.4 Les modes de IPsec

Nous allons présenter ci-dessous tous les modes utilisés pas le protocole IPsec :

- **Mode transport :** le mode transport est souvent utiliser pour protéger les données en provenance de couches supérieures (généralement ce sont des données). Dans ce mode, les entêtes IP ne sont pas modifiés, on chiffre ou on authentifie juste la partie data d'un paquet IP.

  IPsec est intégré entre l'entête IP d'origine et l'entête du protocole transporté. Ce mode est souvent utilisé pour sécuriser une connexion de bout en bout entre deux utilisateurs.

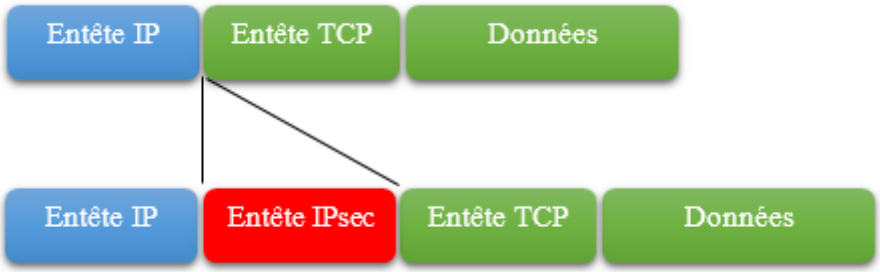

Figure 8:IPsec en mode transport

- **Mode tunnel :** dans le mode tunnel on protège tout le paquet (y compris l'entête IP) et on l'encapsule dans un nouveau paquet avec un nouvel entête IP qui sert à transporter le paquet le long du tunnel, au bout duquel l'ancien en-tête va être rétabli pour pouvoir acheminer le paquet vers sa destination réelle.

  Ce mode permet de relier deux passerelles étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prête à utiliser le protocole IPSec. Il est souvent utilisé pour créer des tunnels entre réseaux LAN distant [17].

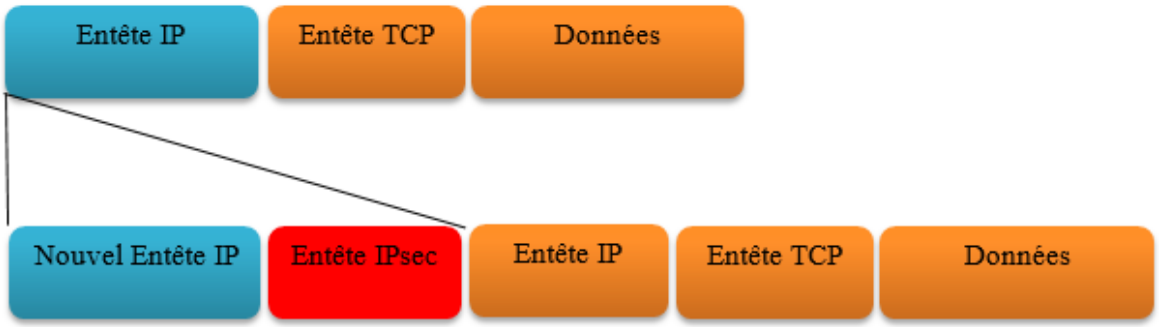

Figure 9: IPsec en mode Tunnel

3.8.5 Mécanisme de sécurité de IPsec

Il existe plusieurs mécanismes qui permettent d'assurer la sécurité d'un VPN. Nous allons présenter ci-dessous les mécanismes les plus communément utilisés :

3.8.5.1 AH (Authentification Header)

Il est conçu pour assurer l'intégrité, il est employé avec IKE, l'authentification des datagrammes IP sans chiffrement des données (i.e. sans confidentialité), et aussi permet de garantir la protection contre le rejeu. C'est à dire qu'AH permet d'une part de s'assurer que les paquets échangés n'ont pas été altérés et d'autre part de garantir l'identité de l'expéditeur d'un paquet [18].

Le contrôle d'intégrité s'effectue sur l'ensemble des paquets IP y compris les en-têtes, à l'exception des en-têtes variables par nature. Cela signifie en particulier que les adresses sources et destinations font partie des données protégées

La plupart des tunnels VPN n'utilisent pas le protocole AH car il ne propose pas le chiffrement.

L'en-tête AH se compose de 6 champs comme le décrit l'image suivante :

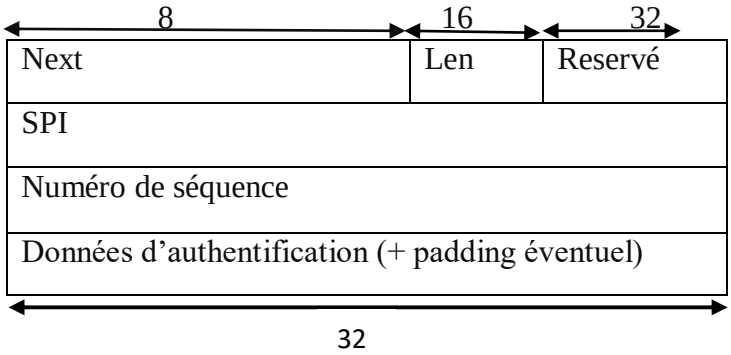

Figure 10: les différentes couches de Protocole de chiffrement AH

- Next : ce champ spécifie le protocole transporté.
- Len : Longueur de l'entête AH (de 2 à 32 bits).
- SPI : index unique définissant la SA (Security Association) pour ce paquet.
- Numéro de séquence : Compteur utile pour le mécanisme anti répétition.
- Données d'authentification : Ce champ contenant les signatures de hachages permettant d'authentifier l'émetteur et l'authenticité des données.

Le protocole AH peut être implémenté en mode transport ou tunnel comme suit :

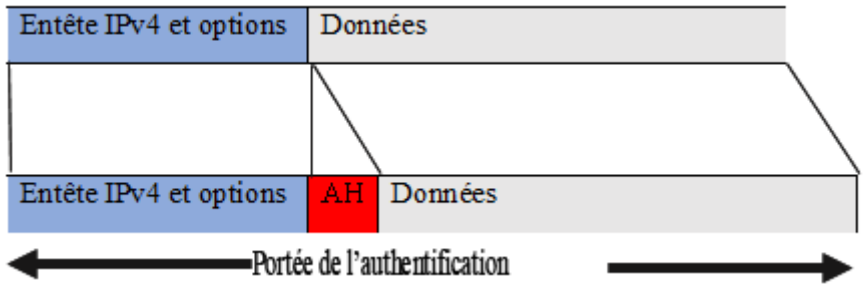

Figure 11: Utilisation de AH en mode transport

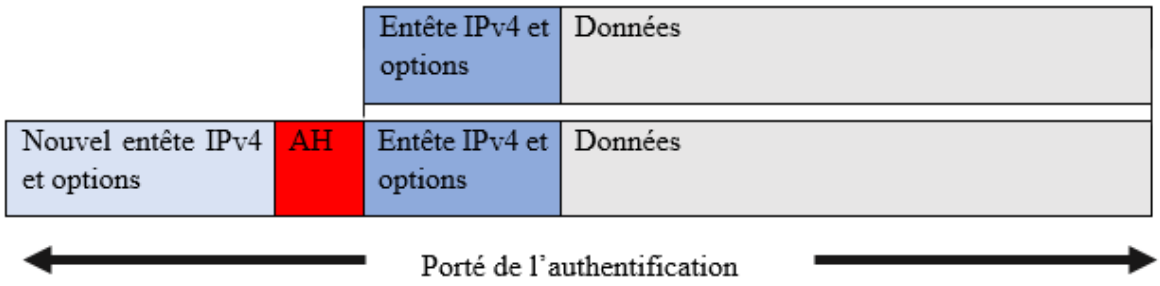

Figure 12: Utilisation de AH en mode tunnel

3.8.5.2 ESP (Encaplsulating Security Protocol)

Le protocole ESP permet d'assurer l'intégrité et, employé avec IKE, l'authentification des datagrammes IP, la confidentialité et aussi assure la protection contre le rejeu.

Certaines implémentations permettent la protection en confidentialité sans mécanisme de contrôle d'intégrité, comme Il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement [18].

Dans le protocole ESP, en mode transport seuls les données transportées par le datagramme IP qui seront protégées et non les en-têtes, autrement dit le « payload ». En mode tunnel, ce sera l'intégralité de datagramme qui sera protégé.

L'entête ESP contient 7 champs :

16	24	32
SPI		
Numéros de séquence		
Données		
Bourrage (0-255 octets)		
	Taille du bourrage	Entête suivante
Données authentification		

Figure 13: Les différentes couches de protocole de chiffrement ESP

- SPI (Security Parameters Index) : index unique définissant la SA pour ce paquet.
- Numéros de séquence : compteur utile au mécanisme d'anti-répétition.
- Données : donnée du protocole de couche supérieure.
- Bourrage : sert à l'encryptions des données. Certains protocoles nécessitent une certaine taille afin d'être plus efficace et/ou applicable.
- Taille du bourrage : indique la taille du bourrage.
- Entête suivante : Ce champ permet de spécifier le type du protocole transporté.
- Données Authentification (variable) : champs contenant les signatures de hachages permettant d'authentifier l'émetteur et l'authenticité des données. La taille de ce champ dépend des protocoles de hachage et d'encryptions utilisés.

Le protocole ESP peut être implémenté en mode tunnel ou en mode transport :

Le protocole ESP peut être implémenté en mode tunnel ou en mode transport :

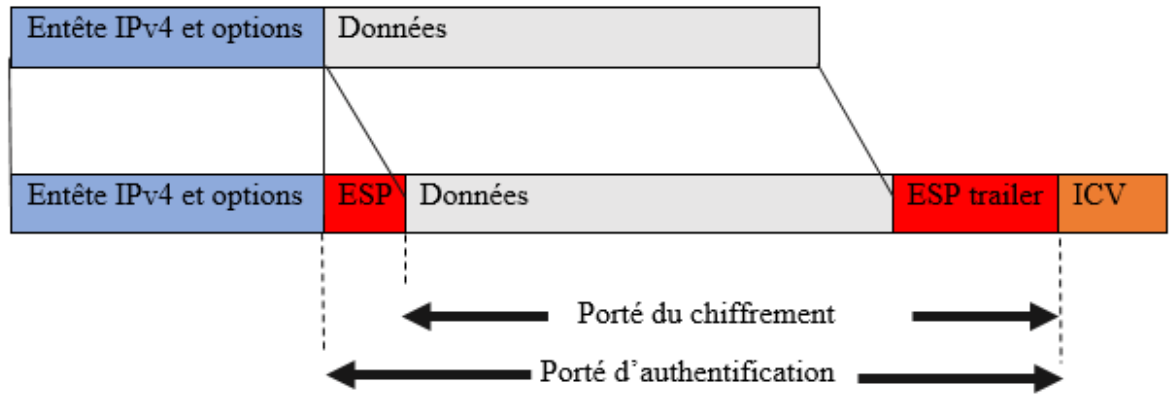

Figure 14: Utilisation de ESP en mode Transport

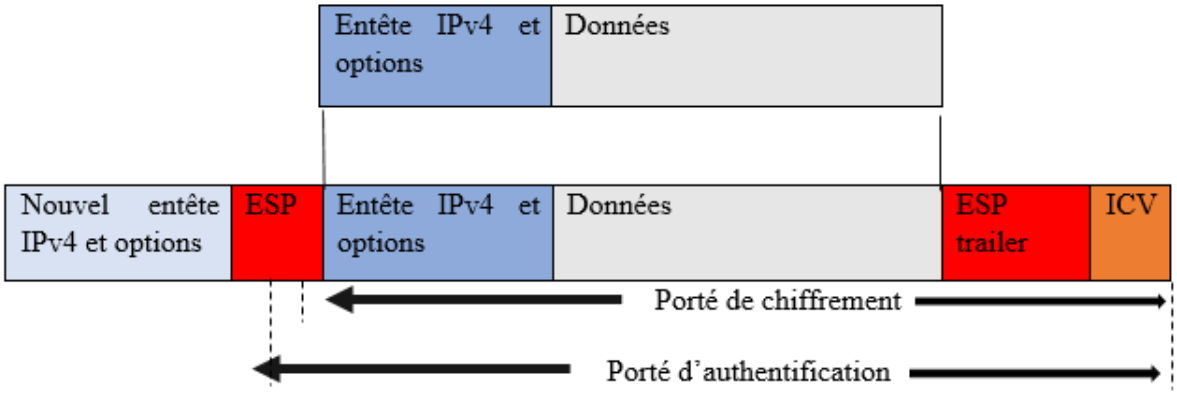

Figure 15: Utilisation de ESP en mode tunnel

3.8.6 Gestion des flux de sécurité

3.8.6.1 Security Policy (SP)

Une SP définie ce qui doit être traité sur un flux. Comment nous voulons transformer un paquet [17].

Chaque flux donné contient :

- Les adresses IP de l'émetteur et du récepteur.
- Par quel protocole il devra être traité (AH ou ESP).
- Le mode IPsec à utiliser (tunnel ou transport).
- Le sens de la liaison (entrante ou sortante).

Pour utiliser AH et ESP sur une communication, deux SP devront être créée, car une SP ne définit qu'un protocole de traitement à la fois.

3.8.6.2 Security association (SA)

Une association de sécurité IPSec est une structure de données servant à stocker l'ensemble des paramètres de sécurité associés à une communication. Une SA étant unidirectionnelle, il faut deux SA pour protéger les deux sens d'une communication. Les services de sécurité définis par la SA sont fournis par l'utilisation des protocoles AH ou ESP
Le rôle d'une SA est de spécifier, pour chaque adresse IP avec laquelle IPsec peut communiquer, les informations suivantes [17] :

- Le Security Parameter Index (SPI) : l'identifiant de la SA choisi par le récepteur.
- Le numéro de séquence, (éviter le rejeu).
- Les paramètres d'authentification (algorithmes et clés).
- Les paramètres de chiffrement (algorithmes et clés).
- La durée de vie de l'association
- Le mode du protocole IPSec (tunnel ou transport)

Chaque association est identifiée de manière unique à l'aide d'un triplet composé de :

- L’adresse de destination des paquets
- L’identifiant du protocole de sécurité (AH ou ESP)
- Le SPI.

3.9 Les bases de données SPD et SAD

3.9.1 SPD (Security Political Database)

Une base de politique de sécurité SPD (Security Political Database), permet de décider pour chaque paquet entrant ou sortant s’il va devoir attribuer des règles de sécurité et même s’il sera autorisé à passer. Cette base possède une référence vers la SA correspondante dans la base SAD.

3.9.2 SAD (Security association Database)

SAD est une base de données qui va contenir pour chaque SA les informations qui lui sont relatives, ce qui permettra de savoir comment traiter chaque paquet à envoyer. C’est une simple base de données qui va être consultée par la SPD.

3.10 Les négociations VPN IPsec

Les négociations VPN est un processus qui consiste à la création d’un tunnel VPN, pour cela les deux périphériques d’extrémités qui sont des pairs IPsec échangent une série de messages relatifs au chiffrement et à l'authentification puis tentent de s'accorder sur de nombreux paramètres.

Pour gérer les négociations entre deux routeurs (PC, Firewalls), IPsec utilise le protocole IKE (Internet Key Exchange), ce dernier gère la connexion entre les deux routeurs par deux phases : Phase1 et Phase 2.

3.11 La gestion des clés

Les protocoles de sécurité utilisent des algorithmes de cryptages qui nécessitent des clés de sécurité. La gestion de ces clés se fait avec deux protocoles spécifiques : le protocole ISAKMP et le protocole IKE.

3.11.1 Le protocole ISAKMP (Internet Security Association ans Key Management Protocol)

Le protocole ISAKMP a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clés (et plus généralement des associations de sécurité).

Il procède en deux phases distinctes :

- Phase 1 : un certain nombre de paramètres de sécurité propres à ISAKMP sont mis en place, ces éléments forme là SA/ISAKMP afin d'établir entre Les deux tiers un canal protégé. Contrairement aux SA IPSEC, la SA ISAKMP est bidirectionnelle. Elle servira à sécuriser l'ensemble des échanges ISAKMP futurs.
- Phase 2 : permet de négocier les associations de sécurité pour Les mécanismes de sécurité que L'on souhaite utiliser (AH et ESP par exemple). Les échanges de cette phase sont sécurisés grâce à la SA ISAKMP.

3.11.2 Le protocole IKE (Internet Key Echange)

Le protocole IKE a pour mission de sécuriser une connexion. Avant qu'une transmission IPsec soit réalisable, IKE se charge d'authentifier les deux parties tentant de se connecter au réseau informatique sécurisé, en échangeant des clés partagées. Ce protocole est utilisé pour la négociation des associations de sécurité IPSec. Ces SA établissent des secrets de session partagée à partir desquels des clés sont dérivées pour le chiffrement de données mises en tunnel.

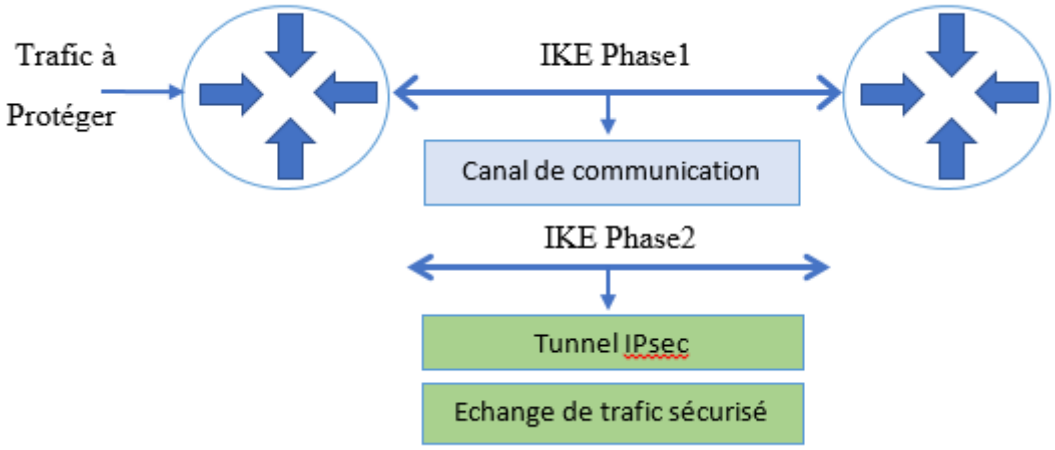

Figure 16: Les phases du protocole IKE

Ce protocole se déroule également en deux phases distinctes :

- Phase 01 : Dans les négociations de phase 1, les deux pairs échangent des informations d'identifications qui peuvent être un certificat ou des clés pré-partagées. Les périphériques se reconnaissent grâce à un identificateur fournit par chaque périphérique (ex : adresse IP, nom de domaine …) et négocient pour définir un ensemble commun de paramètres de phase 1 à utiliser. A la fin des négociations de Phase 1 les deux pairs disposent d'une association de sécurité (SA) de phase 1. Cette association de sécurité est valable pour un certain laps de temps. Après l'expiration de la SA de phase 1, si les deux pairs doivent terminer à nouveau les négociations de phase 2, ils doivent aussi reprendre les négociations de phase 1.
- Phase 02 : Les négociations de phase 2 débutent après l'achèvement des négociations de phase 1 par les deux pairs IPsec et l'établissement des associations de sécurité de phase1. Le but des négociations de Phase 2 est d'établir la SA de Phase 2 (parfois nommée SA IPsec) servant au transfert de données. Les SA IPsec sont un ensemble de spécifications de trafic qui indiquent au périphérique le trafic à envoyer sur le VPN et la manière de le chiffrer et de l'authentifier. Dans les négociations de phase 2, les deux pairs s'accordent sur un ensemble de paramètres de communication.

3.12 Conclusion

Tout au long de ce chapitre, nous avons présenté le VPN et nous avons détaillé le protocole IPsec, ses sous protocoles, ses modes de fonctionnements et les services proposé par ce dernier. IPsec est le protocole le plus utilisé car il est conçu à la base pour IPv6**.**

Chapitre 04

Réalisation et implémentation

4.1 Introduction

Après avoir établi l'étude nécessaire et appropriée à notre projet, nous allons dans ce chapitre expliquer le processus de déploiement de l'architecture réseau qui relie les sites distants de l'entreprise en spécifiant les outils utilisés ainsi que l'illustration détaillée de la configuration réalisée et quelques vérifications et tests qui démontrent le bon fonctionnement de cette solution.

4.2 Les outils de réalisation

4.2.1 GNS3

GNS3 est un logiciel libre et open source, utilisé pour émuler, configurer tester et dépanner des réseaux virtuels et réels. Il permet d'exécuter des petites topologies composées de quelques appareils sur votre ordinateur, à ceux qui comptent plusieurs appareils hébergés sur plusieurs serveurs ou même sur le cloud [22].

GNS3 prend en charge les périphériques émulés et simulés

- Emulation : GNS3 imite ou émule le matériel d'un périphérique et vous exécutez des images réelles sur le périphérique virtuel [22].
- Simulation : GNS3 simule les caractéristiques et fonctionnalités d'un appareil tel qu'un commutateur [22].

Avantages et inconvénients

Ce protocole présente de nombreux atouts, nous allons citer quelques-uns :

- Logiciel gratuit.
- Logiciels open source.
- Pas de frais de licence mensuels ou annuels.
- Aucune limitation sur le nombre de périphériques pris en charge (la seule limitation est le matériel à disposition : CPU et mémoire).
- Prend en charge plusieurs options de commutation.

Néanmoins ce logiciel présente des limites :

- Les images Cisco doivent être fournies par l'utilisateur (télécharger sur Cisco.com, ou acheter une licence VIRL ou copier à partir d'un périphérique physique).
- Pas un package autonome, mais nécessite une installation locale de logiciel (GUI).
- GNS3 peut être affecté par la configuration et les limitations de votre PC en raison de l'installation locale (pare-feu et paramètres de sécurité, politiques des ordinateurs portables de l'entreprise, etc.).

4.2.2 WIRESHARK 

Wireshark est un logiciel d'analyse réseau (sniffer) permettant de visualiser l'ensemble des données transitant sur la machine qui l'exécute, et d'obtenir des informations sur les protocoles applicatifs utilisés. Les octets sont capturés en utilisant la librairie réseau PCAP, puis regroupés en blocs d'informations et analysés par le logiciel [21].

Wireshark implémente une interface graphique ainsi que plusieurs options de tri et filtrage des paquets. Il décode les paquets capturés et comprend les différentes structures (encapsulation) des protocoles de communication. Et afin de faciliter à l'utilisateur d'identifier le type de trafic capturé, un code couleur a été mis en place tel que le mauve clair pour le trafic TCP, vert pour le trafic http et bleu pour le trafic DNS et UDP [21].

4.3 L'architecture du réseau

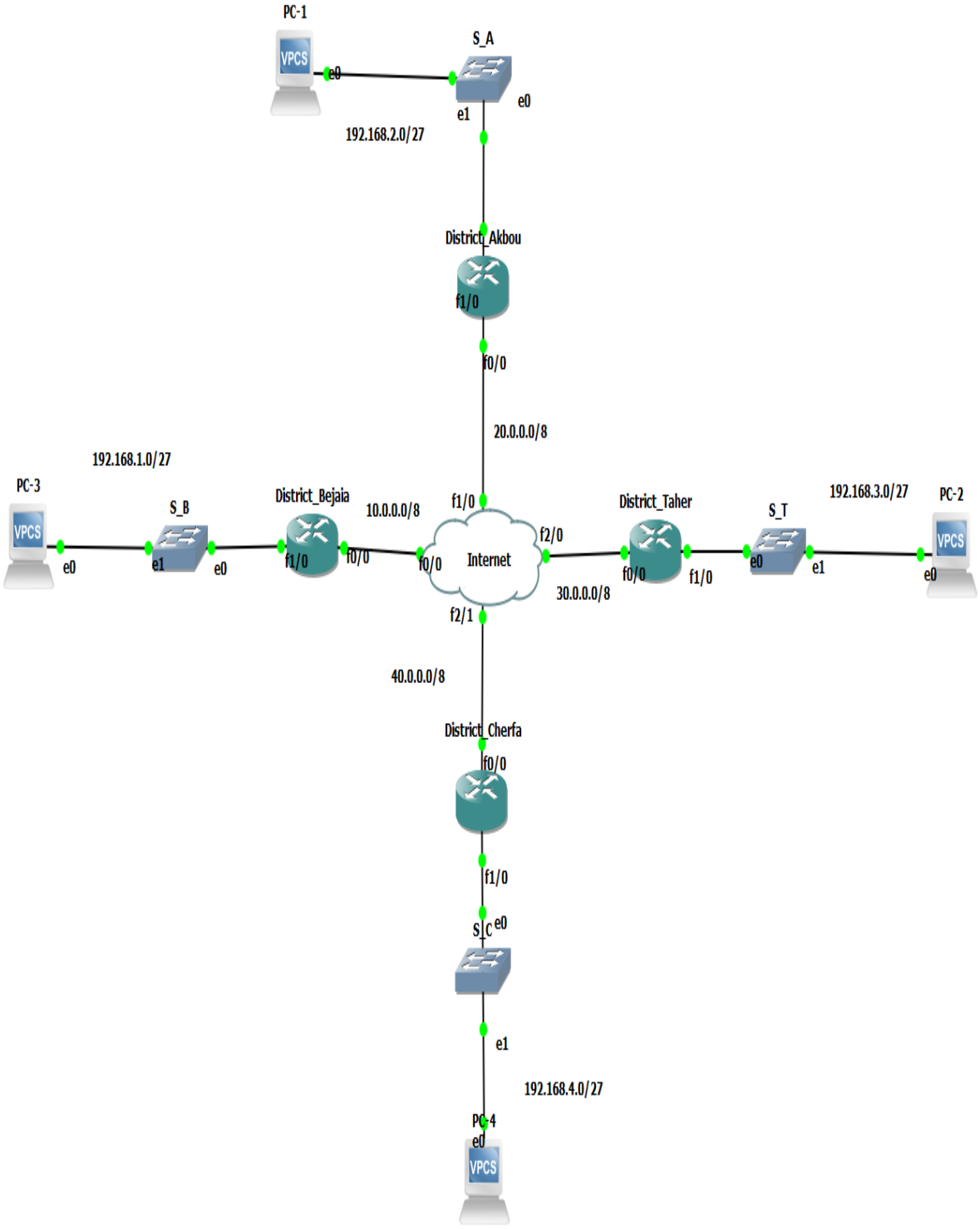

Figure 17: Architecture de réseau proposée

4.4 Plage d'adressage

Routeur	Interface	Adresse d'interface	Adresse du réseau	Masque
District_Bejaia	F1/0 F0/0	192.168.1.1/27 10.0.0.2/8	192.168.1.0 10.0.0.0	255.255.255.224 255.0.0.0
District_Taher_Jijel	F1/0 F0/0	192.168.3.1 /27 30.0.0.2 /8	192.168.3.0 30.0.0.0	255.255.255.224 255.0.0.0
District_Akbou	F1/0 F0/0	192. 168.2.1/27 20.0.0.2/8	192.168.2.0 20.0.0.0	255.255.255.224 255.0.0.0
District_Cherfa	F1/0 F0/0	192.168.4.1/27 40.0.0.2/8	192.168.4.0 40.0.0.0	255.255.255.224 255.0.0.0
Internet	F0/0 F1/0 F2/0 F2/1	10.0.0.1/8 20.0.0.1/8 30.0.0.1/8 40.0.0.1/8	10.0.0.0/8 20.0.0.0/8 30.0.0.0/8 40.0.0.0/8	255.0.0.0 255.0.0.0 255.0.0.0 255.0.0.0

Table 2: Table d'adressage

4.5 L'implémentation

Pour implémenter ce VPN ipsec dans notre architecture nous avons besoin de créer 6 VPN ce qui fait 3 tunnels VPN comme suit :

- 3 VPN au site de Béjaia.
- 1 VPN à Taher dans la wilaya de Jijel.
- 1 VPN à Akbou.
- 1 VPN à Cherfa dans la wilaya de Bouira.

Pour ce qui est des tunnels :

- 1 Tunnel entre le site de Béjaia et celui de Taher
- 1 Tunnel entre le site de Béjaia et celui de Cherfa
- 1 Tunnel entre le site de Béjaia et celui de Bouira

La configuration de ces VPNs se fait par plusieurs étapes :

Avant de commencer la configuration et l'implémentation des VPN nous allons d'abord faire la configuration des différentes interfaces des routeurs et configurer le routage avec un protocole.

4.6 La configuration des Interfaces et le routage

- **Router de Béjaia**

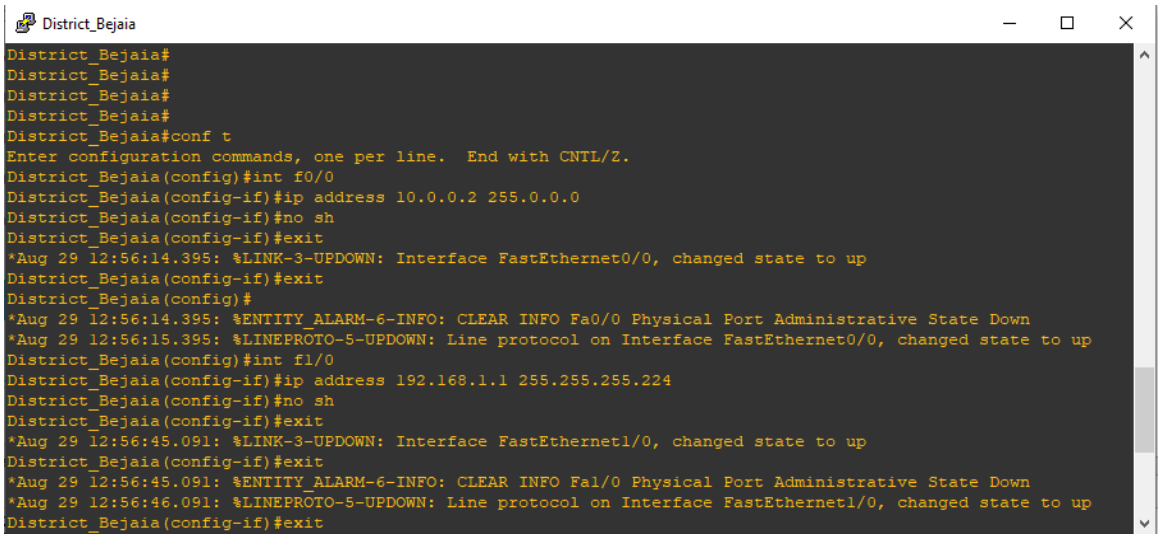

Figure 18: Configuration des adresses IP du district Béjaia

Pour le routage dynamique nous avons utilisé le protocole OSPF.

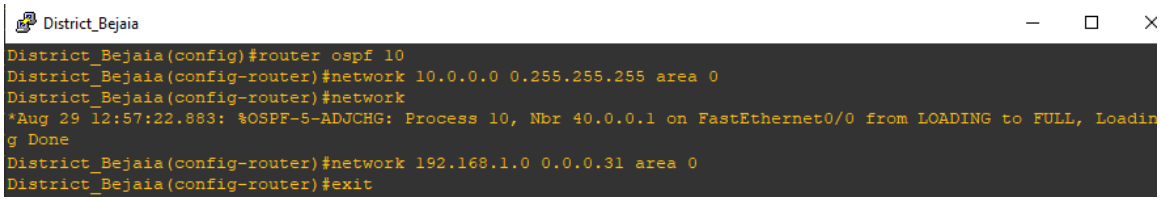

Figure 19: Configuration du routage dans le router du district de Béjaia

- **Router de Cherfa**

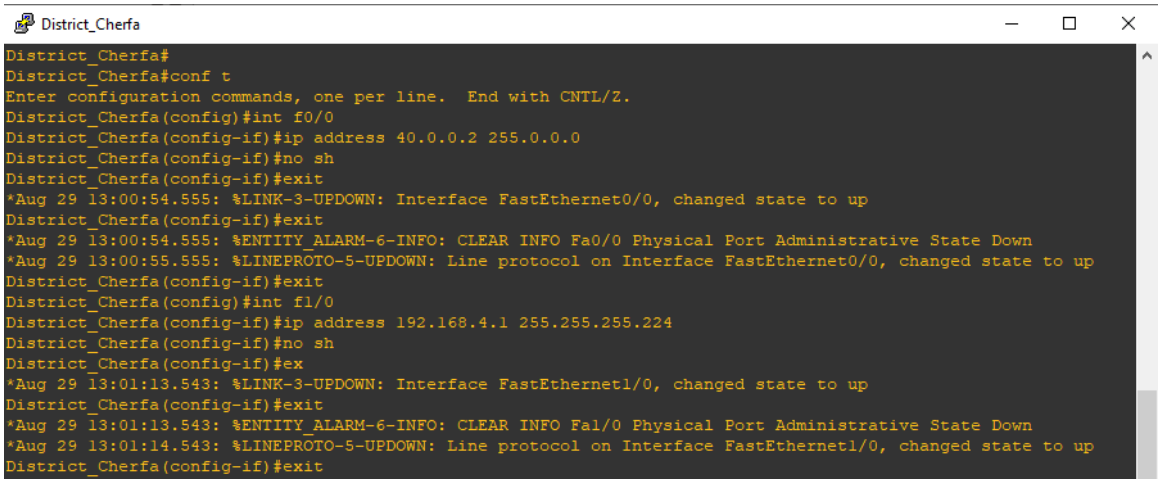

Figure 20: Configuration des adresses IP du router du district de Cherfa.

Le routage avec le protocole OSPF :

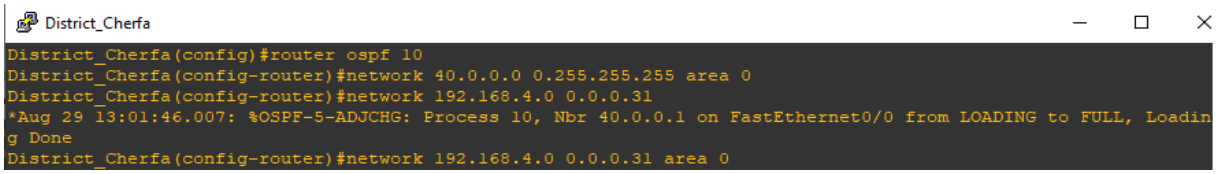

Figure 21: Configuration du routage dans le router du district de Cherfa

- **Router Internet**

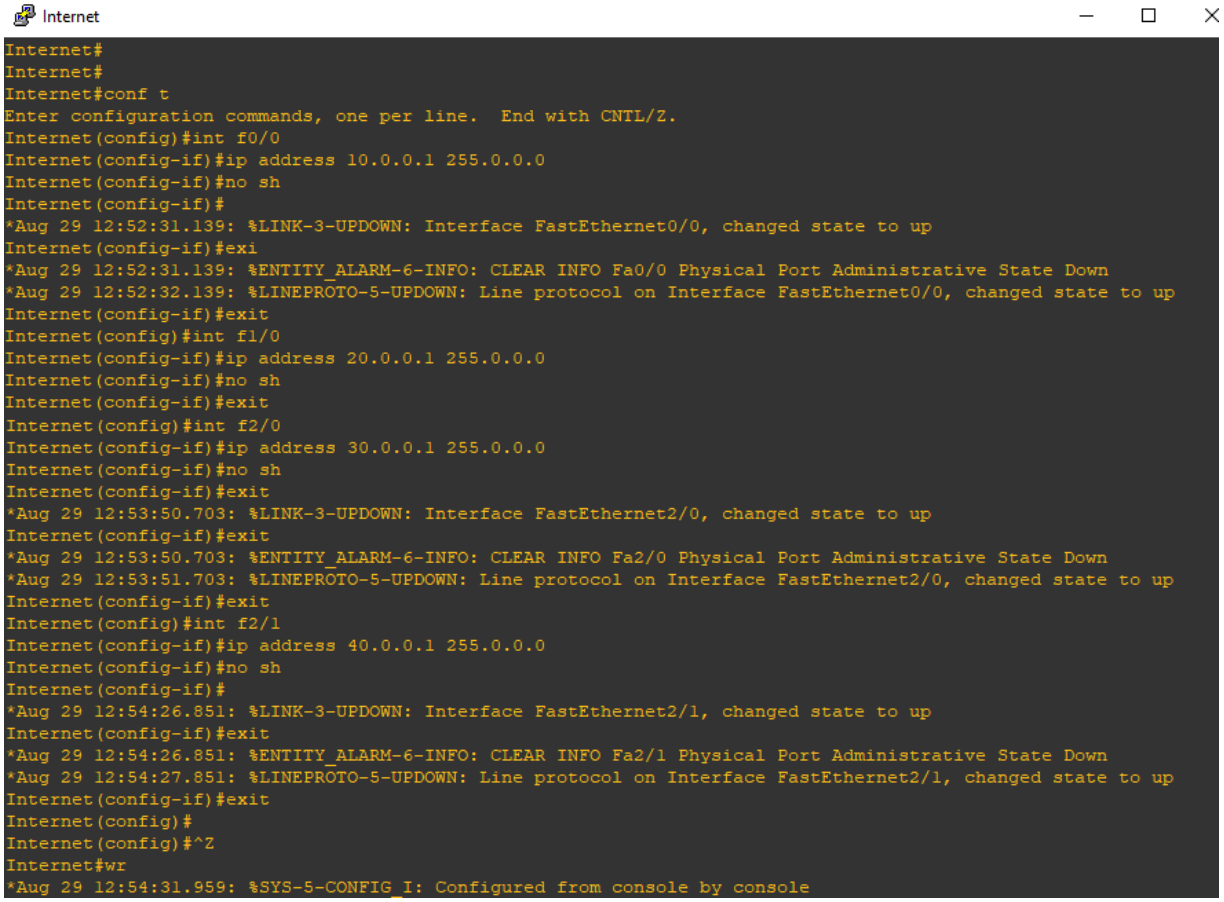

Figure 22: configuration du routage dans le router Internet

Le routage avec le protocole OSPF :

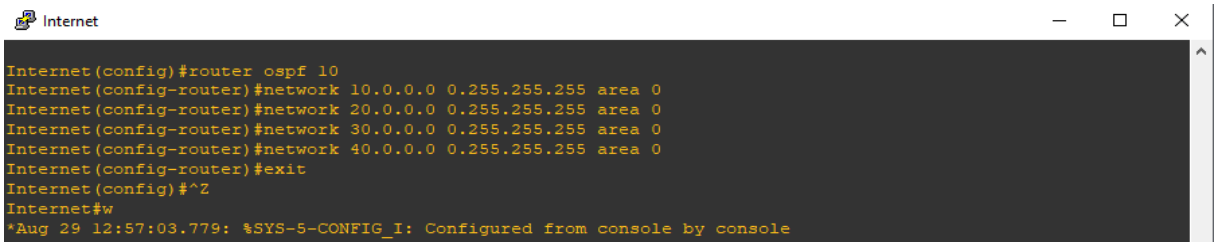

Figure 23: configuration du routage dans le router internet

4.7 La configuration du VPN IPsec

Dans cette partie, nous allons expliquer et illustrer la configuration de IPsec entre deux sites distants (site central de Béjaia et le site de Cherfa à Bouira).

1. **Site de Béjaia :** La configuration de ce site passe par plusieurs étapes :

- **La première étape** : On active les fonctions crypto du routeur.

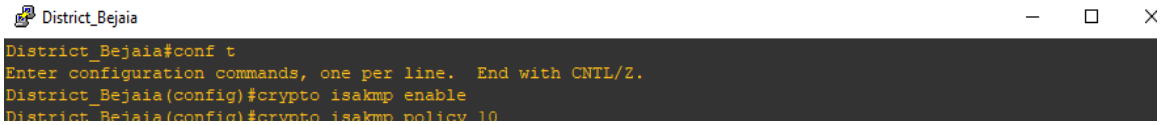

Figure 24: Activation des fonctions crypto du router du district de Béjaia

Crypto isakmp enable : cette commande permet d'entamer la configuration ISAKMP.

- **La deuxième étape** : dans cette étape, nous allons configurer la police qui détermine quelle encryptions on utilise, quelle fonction de hachage quelle type d'authentification, et la durée de vie d'une association de sécurité.

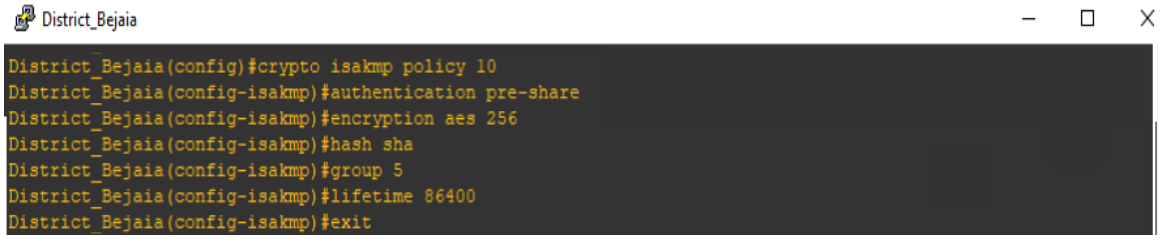

Figure 25: création d'une stratégie de négociation de clés

- Policy : cela définit la politique de connexion pour les SA (Security Association) de ISAKMP et un numéro indiquant la priorité de l'utilisation lui est attribué à la fin de la commande.
- ENCRYPTION : Nous avons utilisé AES comme algorithme de chiffrement.
- PRE-SHARE : Utilisation d'une clé pré-partagée comme méthode d'authentification.
- SHA : L'algorithme de hachage.
- GROUP 5 : Spécifie l'identifiant Diffie-Hellman pour l'échange de clef.
- LIFETIME : Spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs.

- **La troisième étape :** Dans cette étape nous allons configurer la clé :

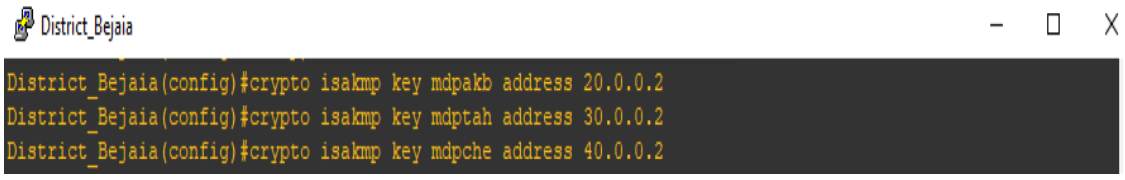

Figure 26 Configuration des clés pré-partagées

Définition des clés pré-partagées :
« mdpakb » pour l'authentification avec le site d'Akbou.
« mdptah » pour l'authentification avec le site de Jijel.
« mdpche » pour l'authentification avec le site de Cherfa.

- **La quatrième étape :** Configurer les options de transformations des données :

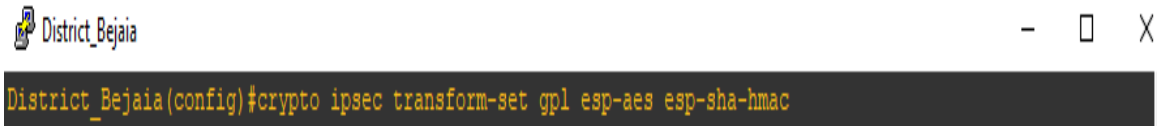

Figure 27: Configuration de la transform-set

Il faut noter que dans cette étape, nous devons utiliser les mêmes protocoles d'encryptions et de Hash utilisés dans la deuxième étape

Ensuite nous allons fixer une valeur de Lifetime (voir la figure 28).

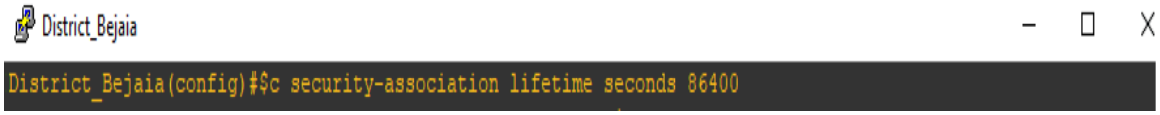

Figure 28: Définition de la durée de vie des clés

- **Cinquième étape :** Cette étape consiste à créer une access-list (ACL) qui va déterminer le trafic autorisé et le trafic à trier par le tunnel VPN.

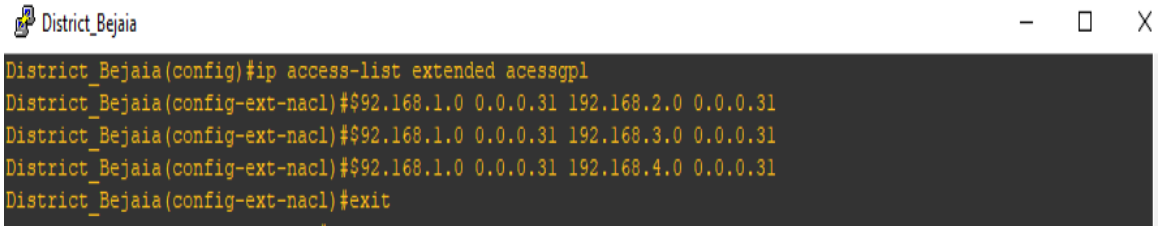

Figure 29: Création des access-list (ACL).

- **Dernière étape** : Dans cette dernière étape nous configurons la crypto map qui associe l'access-list, le trafic, et la destination. Ensuite, pour finir nous allons appliquer cette dernière sur l'interface de sortie (Dans notre cas FastEthernet 0/0) :

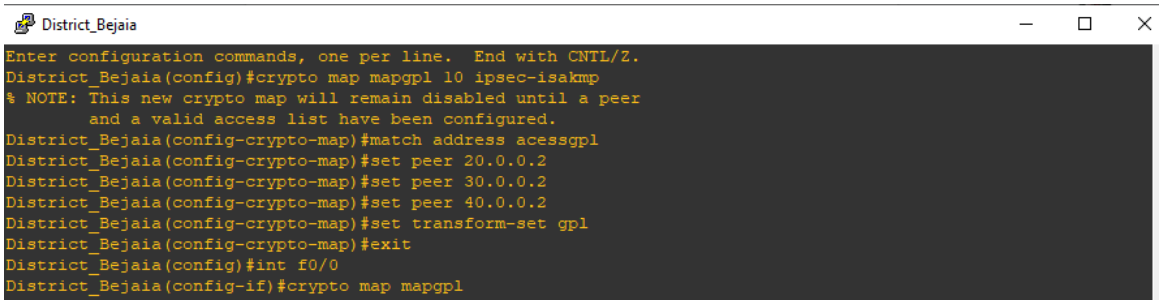

Figure 30: Création et application de la crypto map

2. **Le site de Cherfa :** La configuration de ce site est presque la même que la configuration du site de Béjaia, néanmoins nous allons expliquer les différentes étapes de la configuration.

- **La première étape**

District_Cherfa

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

Figure 31: Activation des fonctions crypto du router du district de Cherfa

- **La deuxième étape**

District_Cherfa

```
District_Cherfa(config)#crypto isakmp policy 10
District_Cherfa(config-isakmp)#authentication pre-share
District_Cherfa(config-isakmp)#encryption aes 256
District_Cherfa(config-isakmp)#group 5
District_Cherfa(config-isakmp)#hash sha
District_Cherfa(config-isakmp)#lifetime 86400
District_Cherfa(config-isakmp)#exit
```

Figure 32: Création d'une stratégie de négociation de clés

- **La troisième étape**

District_Cherfa

```
District_Cherfa(config)#crypto isakmp key mdpche address 10.0.0.2
```

Figure 33: Configuration de la clé pré-partagée

- **La quatrième étape**

District_Cherfa

```
District_Cherfa(config)#crypto ipsec transform-set gpl esp-aes esp-sha-hmac
District_Cherfa(cfg-crypto-trans)#exit
```

Figure 34: Configuration de la transform-set

- **La cinquième étape**

District_Cherfa

```
District_Cherfa(config)#ip access-list extended accessgpl
District_Cherfa(config-ext-nacl)#permit ip 192.168.4.0 0.0.0.31 192.168.1.0 0.$
District_Cherfa(config-ext-nacl)#exit
```

Figure 35: Création de l'access-list (ACL).

- **La Dernière étape**

District_Cherfa

```
District_Cherfa(config)#crypto map mapgpl 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
District_Cherfa(config-crypto-map)#match address accessgpl
District_Cherfa(config-crypto-map)#set peer 10.0.0.2
District_Cherfa(config-crypto-map)#set transform-set gpl
District_Cherfa(config-crypto-map)#exit
District_Cherfa(config)#int f0/0
District_Cherfa(config-if)#crypto map mapgpl
District_Cherfa(config)#ip access-list extended accessgpl
District_Cherfa(config-ext-nacl)#permit ip 192.168.4.0 0.0.0.31 192.168.1.0 0.$
District_Cherfa(config-ext-nacl)#exit
```

Figure 36: création et application de la crypto map

4.8 Vérification de l'établissement de tunnel et le transfert des données cryptées

Après avoir fini les différentes étapes de la configuration, nous passons à la dernière étape qui consiste à vérifier si le tunnel a été bien implémenté et que les données échangées entre les sites ont été cryptées.

Pour cela nous devons d'abord effectuer un ping pour vérifier s'il n'y a pas de problèmes, comme illustré dans la figure 37.

PC-3

```
PC-3> ping 192.168.4.10
84 bytes from 192.168.4.10 icmp_seq=1 ttl=63 time=60.164 ms
84 bytes from 192.168.4.10 icmp_seq=2 ttl=63 time=60.126 ms
84 bytes from 192.168.4.10 icmp_seq=3 ttl=63 time=54.277 ms
84 bytes from 192.168.4.10 icmp_seq=4 ttl=63 time=64.422 ms
84 bytes from 192.168.4.10 icmp_seq=5 ttl=63 time=74.531 ms
```

Figure 37: Ping de l'host de Béjaia vers l'host de Cherfa

4.9 Vérification des opérations ISAKMP

Nous allons Vérifier que le tunnel est opérationnel, ce qui signifie que la SA a été bien établie. Cette vérification se fait avec la commande « show crypto isakmp sa ».

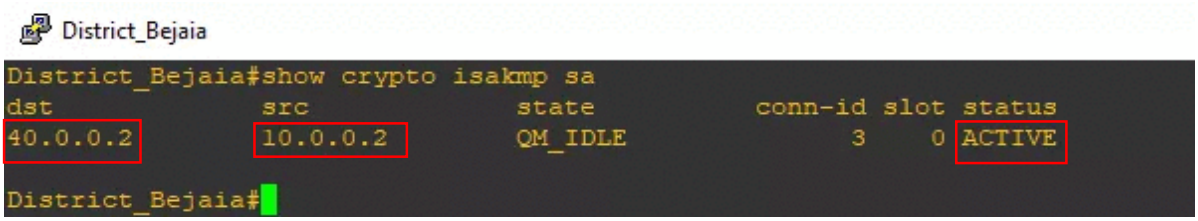

Figure 38: Vérification des opérations ISAKMP du district de Béjaia

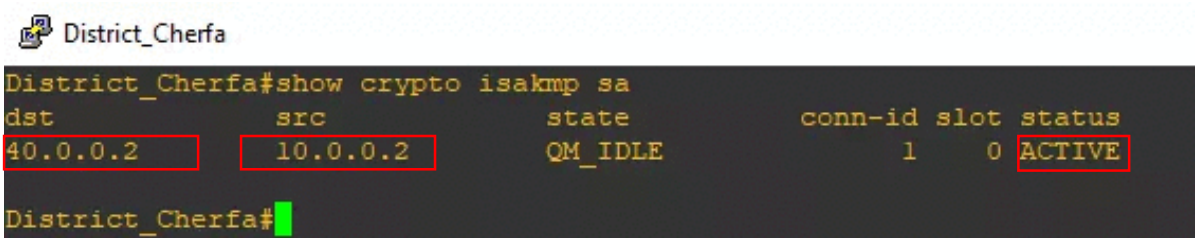

Figure 39: Vérification des opérations ISAKMP du district de Cherfa

Dans la figure 38 et la figure 39, on remarque que les opérations de ISAKMP entre le site de Béjaia (10.0.0.2) et le site de Cherfa (40.0.0.2) sont activées.

Afin de visualiser l'échange de paquets entre les deux sites, nous avons effectué une capture avec Wireshark et grâce à cette dernière nous pouvons clairement voir que :

(1) L'échange des clés a été effectué avec le protocole ISAKMP.
(2) Le trafic a été crypté avec le protocole ESP.

Le résultat est illustré dans la figure 40.

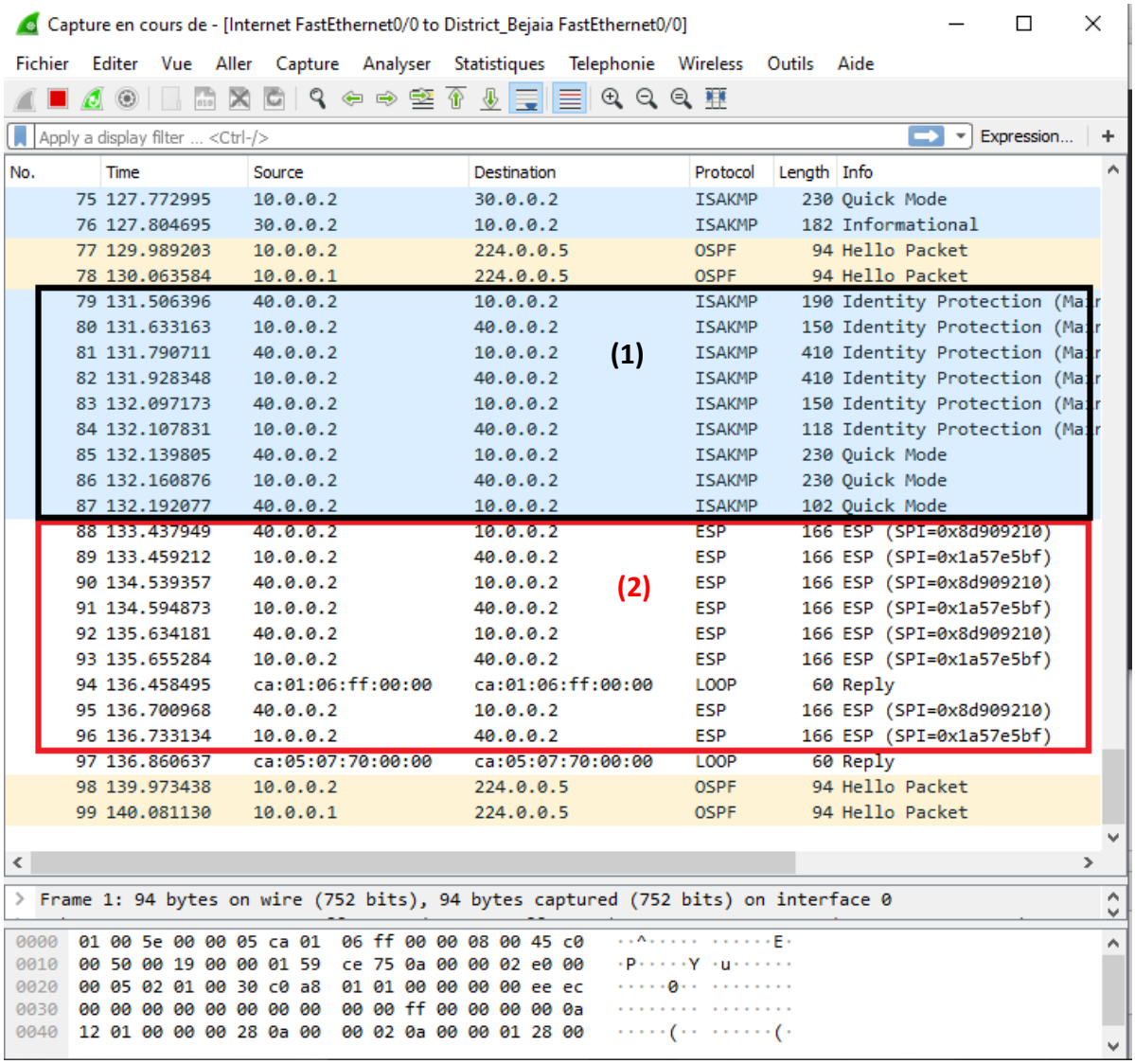

Figure 40: Résultat de la solution avec Wireshark

4.10 Vérification des paramètres IPsec

Pour vérifier les paramètres IPsec, et s'assurer que les données échangées ont été bien crypté et décrypté par les deux routeurs des deux sites nous utilisons la commande « show crypto ipsec sa », le résultat est illustré dans la figure 41, et la figure 42.

- Router du District_Béjaia

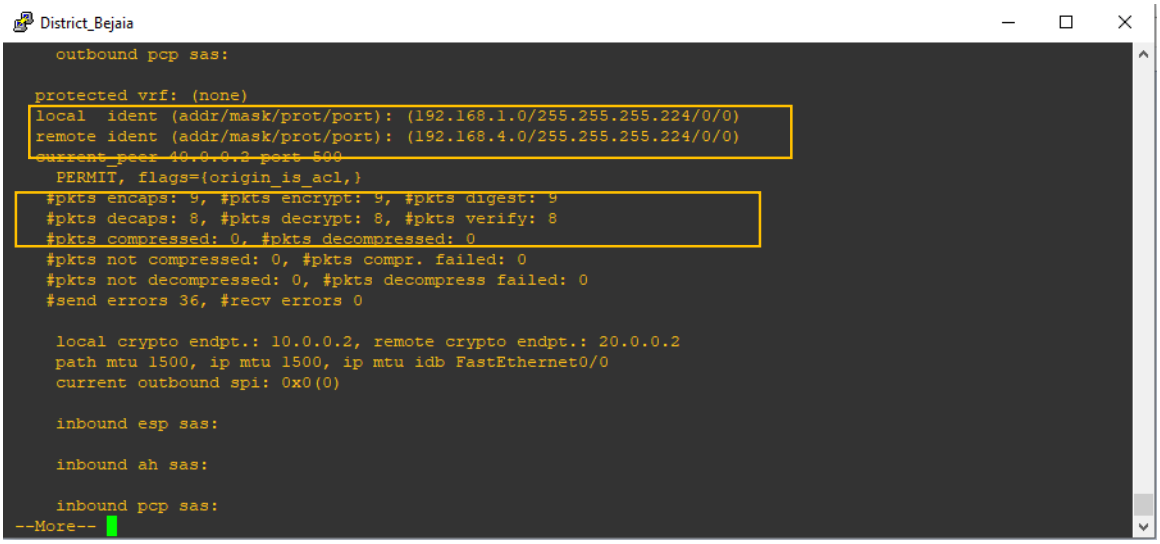

Figure 41: Vérification des paramètres IPsec du District_Béjaia

- Routeur District_Cherfa

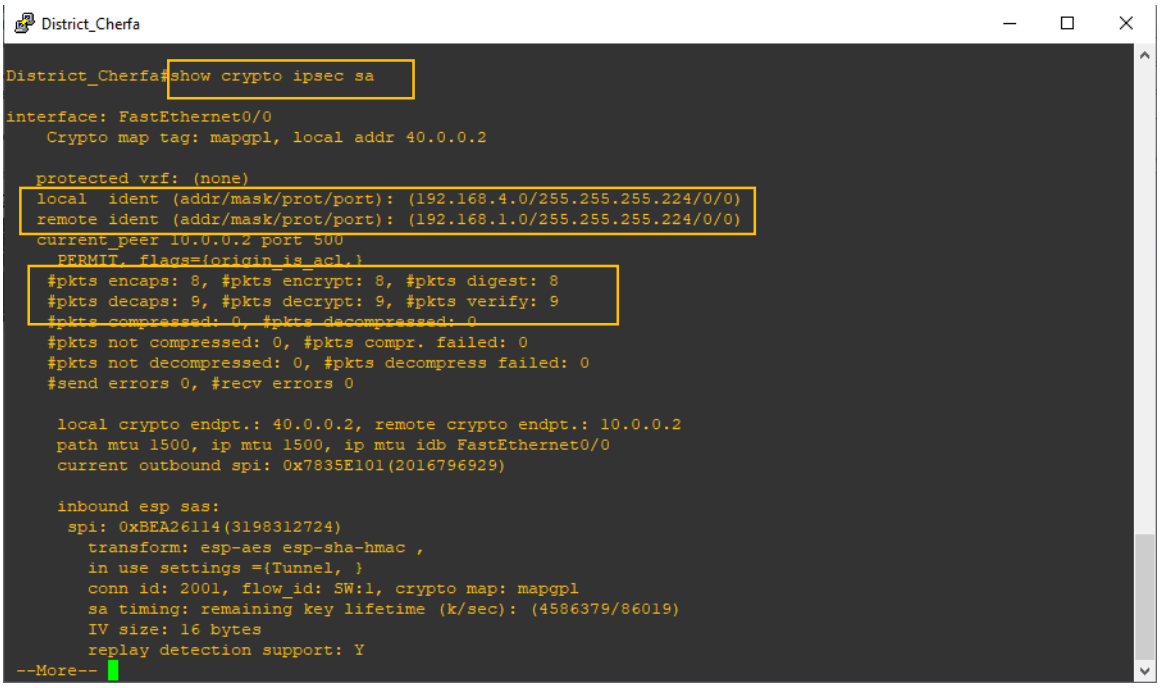

Figure 42: Vérification des paramètres IPsec du District_Cherfa

4.11 Conclusion

Dans ce chapitre, nous avons réalisé un VPN site-à-site sécurisé avec le protocole IPsec. Nous avons en premier lieu réalisé la topologie du réseau et établi un routage dynamique avec le protocole OSPF. Ensuite nous avons configuré la politique ISAKMP afin de déterminer les paramètres de sécurité qui doivent être utilisés dans le VPN (chiffrement avec AES, hachage avec l'algorithme SHA, Deffie Hellman groupe 5 pour l'échange de clés, etc.). Et pour finir, nous avons illustré la configuration complète réalisée dans notre simulation avec GNS3.

Conclusion générale

Le VPN a pris une dimension proportionnelle dans le développement d'internet. En effet, avec l'arrivée des technologies sans files, des problèmes de sécurité et de confidentialité ont été soulevés. Ces problèmes de sécurité représentent une grande problématique surtout lors d'échange de données sensibles. Les solutions VPN permettent d'y remédie et de garantir la fluidité et la sécurité des communications.

Notre étude, nous a permis d'avoir un aperçu sur les différentes possibilités nécessaires pour déployer un VPN. En l'occurrence, nous avons constaté qu'il existe une multitude de protocoles, de techniques et d'architectures pour déployer ce concept, et le choix de la solution à adopter pour le VPN dépendra néanmoins des besoins d'utilisation et de l'investissement financier que l'on va y mettre.

Dans notre projet, nous avons opté pour la solution VPN site-à-site avec le protocole IPsec qui reste la solution référente et la plus utilisé. Cette solution permet de réaliser un réseau privé sécurisé garantissant non seulement une communication performante et sécurisée entre les sites distants de l'entreprise, mais aussi offre la possibilité d'accès à distance au réseau de l'entreprise pour les télétravailleurs.

Suite à la situation précaire que traverse le monde, nous n'avons pas pu mettre en pratique cette solution au niveau de l'entreprise, et nous nous somme contenter d'une simulation sur la plateforme de GNS3.

Pour conclure, nous tenons à préciser que le présent travail nous a donné l'occasion d'approfondir nos connaissances dans le domaine de la sécurité informatique, le transfert de donnée et le déploiement d'une architecture VPN. Enfin sans un monde soumis aux nécessaires flux d'informations sensibles et confidentielles nous espérons avoir fait œuvre utile. Puisse nos Maitres trouver ici l'expression de notre éternelle gratitude.

Références bibliographiques

Bibliographie

[5] Guide N°650- Menaces sur les systèmes informatiques, version 12 septembre 2006

[6] DESWARTE Yves. Comment mesurer la sécurité informatique. Rapport technique, Laboratoire d'Analyse et d'Architecture des Systèmes, CNRS, 2000.

[7] Yosr Jarraya, Chamseddine Talhi. Logiciels malveillants. Rapport technique. Ecole de technologie supérieur (ETS) Département génie logiciel et TI. Automn 2002

[8] N. BATTAT. Les Systèmes de sécurité, Rapport technique, 2019.

[9] A. ESSAIDI, V. BOISTUAUD et N. DIOP. Conception d'une zone démilitarisée (DMZ). Mémoire de master en informatique, option réseau. Université de Marne la vallée. 2006-2007.

[11] Les virus informatique clusif 2005, page 10

[12] Jean-Olivier Gerphagnon, Marcelo Portes de Albuquerque, Marcio Portes de Albuquerque, attaque informatique, page 06.

[17] Tan Sun Seng – de Reynal – de Rorthais, Présentation sur les vpn. Informatique et réseaux 3em année. Université Marne La Valle : UFR Ingénieurs 2000, Février 2004.

[18] Agence national de la sécurité des systèmes d'information. Recommandations de sécurité relative à IPsec Pour la protection des flux réseau. Secrétariat générale de la défense et de la sécurité national. Paris aout 2015. No DAT-NT-003/ANSSI/SDE/NP

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

Sites web

[1] https://www.piloter.org/systeme-information/securite-informatique.html, consulté le 13/02/2020.

[2] https://www.securiteinfo.com, consulté le 27/05/2020.

[3] https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security, consulté le 16/06/2020.

[4] http://www.wikayanet.dz/index.php/fr/dossiers-securite/1178-la-securite-parlons-en-serieusement, consulté le 16/07/2020.

[10] https://www.rene-reyt.fr/documents/informatique/petit-resume-de-securite-informatique/securite-informatique-les-techniques-dattaque/, consulté le 30/06/2020.

[13] multimedia.plouider.infini.fr/IMG/pdf/Diaporamavirus_PDF.pdf, consulté le 30/06/2020.

[14] http://projet.eu.org/pedago/sin/ISN/8-securite_reseaux.pdf, consulté le 27/05/2020.

[15] https://doc.lagout.org/network/Introduction-aux-ids.pdf, consulté le 27/05/2020.

[16] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203461-ipsec-internet-protocol-security-definition-traduction/, consulté le 02/06/2020.

[20] https://www.cisco.com/, consulté le 15/04/2020.

[21] https://fr.wikipedia.org/, consulté le 15/04/2020.

[22] https://docs.gns3.com/, consulté le 25/08/2020.

Résumé

Aujourd'hui, les entreprises placent la sécurité au cœur de leurs priorités. La sécurité informatique est indispensable pour le bon fonctionnement d'un réseau informatique, est le choix de la politique de sécurité à adopter est primordiale. Pour cela plusieurs mécanismes de sécurité ont été élaborés et mis à la disposition des administrateurs afin de renforcer la sécurité des réseaux et les rendre plus performants et plus robustes.

Notre travail consiste à mettre en place une architecture VPN site-à-site sécurisée avec le protocole IPsec pour l'entreprise GPL NAFTAL de Béjaia. Cette solution permettra aux sites distants de l'entreprise de s'interconnecter via des tunnels sécurisés utilisant l'infrastructure réseau publique (Internet).

Afin de mettre en pratique l'étude réalisée sur les VPN IPsec, nous avons établi une simulation avec le simulateur GNS3 où nous avons réalisé la configuration des routeurs de la topologie proposée en réseau. Et pour finir, nous avons analysé les paquets qui transitent entre les sites grâce au logiciel Wireshark afin de s'assurer du bon fonctionnement des canaux sécurisé.

Mots clé : Réseau, Sécurité, Protocole, VPN, IPsec, GNS3, Wireshark.

Abstract

Today, compagnies place security at the heart of their priorities. Security is essential for the proper functioning of a computer network, and the choice of the security policy to adopt is paramount. To this end, several security mechanisms have been developed and made available to administrators in order to strengthen network security and make them more efficient and robust.

Our work consists in setting up a secure site-to-site VPN architecture using the IPsec protocol for the GPL NAFTAL company in Béjaia. This solution will allow the company's remote sites to interconnect via secure tunnels using the public network infrastructure (Internet).

In order to put into practice the study carried out on IPsec VPNs, we established a simulation with the GNS3 simulator where we carried out the configuration of the routers of the proposed network topology. And finally, we analyzed the packets that transit between the sites using Wireshark software to ensure the proper functioning of the secure channels.

Keywords: Network, Security, Protocol, VPN, IPsec, GNS3, Wireshark.