République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle
En vue d'obtention du diplôme de Master professionnel
Option : Administration et Sécurité des Réseaux

Thème

Étude et amélioration de l'architecture réseau de la Banque de l'Agriculture et du Développement Rural de Béjaïa

Réalisé par :

AZOUAOU Lamine
BOURICHE Adel

Président	Mme GHIDOUCHE Kahina	Maître Assistant Classe B	U. A. Mira
Examinateur	Mme BOUKERRAM Samira	Maître Assistant Classe A	U. A. Mira
Examinateur	Mlle BENNAI Sofia	Doctorante	U. A. Mira
Promoteur	M. TARI Abdelkamel	Professeur	U. A. Mira
Co-promoteur	M. ELSAKEN RAGAB Nadim	Doctorant	U. A. Mira
Encadreur	M. BRADAI Elhadi	Responsable de centre de maintenance informatique	BADR Béjaïa

Année Universitaire 2016/2017

Dédicaces

Je dédie ce modeste travail :

À mes très chers parents ;
À mon frère et mes sœurs ;
À ma précieuse famille, mes grands parents, oncles et tantes, mes cousins et cousines ;
À mon binôme Adel ainsi que sa famille ;
À tous mes amis.

Lamine

Je dédie ce modeste travail :

À mes très chers parents ;
À mes frères, mes belles-sœurs, ma nièce Malak et mes neveux Ramzi et Sifou ;
À la mémoire de ma défunte grand-mère que dieu l'accueil dans son vaste paradis ;
À mon binôme Lamine ainsi que sa famille ;
À une personne très particulière qui se reconnaîtra toute seul ;
À tous mes amis, sur leur tête Lyes MADI.

Adel

Remerciements

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

On remercie vivement le Professeur ***TARI Abdelkamel*** *d'avoir accepté d'être notre promoteur.*

On rend hommage à monsieur ***ELSAKEN RAGAB Nadim*** *pour sa patience, pour le suivi ininterrompu, pour ses conseils et son appui tout au long de ce projet.*

On adresse nos sincères remerciements à monsieur ***BRADAI Elhadi*** *qui nous a accueillis dans son équipe et son soutien tout au long de notre stage. On ne saurait dire combien nos échanges et ses nombreux conseils nous ont été précieux.*

On est très reconnaissant à madame ***GHIDOUCHE Kahina*** *d'avoir accepté de présider le juré de notre soutenance. Nos remerciements s'adressent aussi aux éxaminateurs composés de madame* ***BOUKERRAM Samira*** *et mademoiselle* ***BENNAI Sofia*** *d'avoir accepté de juger ce modeste travail.*

Nous remercions du fond de nos cœurs nos parents et notre famille pour les encouragements et le soutien qu'ils nous ont apportés tout au long du parcours qui nous a menées jusqu'ici.

Enfin, on ne serait terminé sans exprimer nos remerciements les plus sincères à tous nos professeurs de l'université A. MIRA et à tout le personnel administratif, plus particulier, à madame ***LAHDIRI Ghania*** *le chef de service secrétariat faculté des sciences exactes.*

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AAA	**A**uthentification **A**utorisation **A**ccounting.
AES	**A**dvanced **E**ncryption **S**tandard.
AES-GCM	**A**dvanced **E**ncryption **S**tandard-**G**alois **C**ounter **M**ode.
ACL	**A**cess **C**ontrol **L**ist.
AH	**A**uthentication **H**eader.
ALE	**A**gences **L**ocales d'**É**xploitation.
BADR	**B**anque de l'**A**griculture et du **D**éveloppement **R**ural.
DES	**D**ata **E**ncryption **S**tandard.
DH	**D**iffie **H**ellman.
DMZ	**D**e**M**ilitarized **Z**one.
DSL	**D**igital **S**ubscriber **L**ine.
ESP	**E**ncapsulating **S**ecurity **P**ayload.
FAI	**F**ournisseur d'**A**ccès **I**nternet.
GAB	**G**uichet **A**utomatique **B**ancaire.
GRE	**G**eneric **R**outing **E**ncapsulation.
GRE	**G**roupe **R**égional d'**É**xploitation
IDS	**I**ntrusion **D**etection **S**ystem.
IETF	**I**nternet **E**ngineering **T**ask **F**orce.
IKE	**I**nternet **K**ey **E**xchange.
IMAP4	**I**nteractive **M**ail **A**ccess **P**rotocol.
IP	**I**nternet **P**rotocol.
IP/MPLS	**I**nternet **P**rotocol/**M**ulti **P**rotocol **L**abel **S**witching.
IPSec	**I**nternet **P**rotocol **S**ecurity.
IPX	**I**nternetwork **P**acket e**X**change.
ISAKMP	**I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol.

ISO	**I**nternational **S**tandard **O**rganization.
LAN	**L**ocal **A**rea **N**etwork.
LCP	**L**ink **C**ontrol **P**rotocol.
L2F	**L**ayer **T**wo **F**owarding.
L2TP	**L**ayer **T**wo **T**unneling **P**rotocol.
MAC	**M**edia **A**ccess **C**ontrol.
MAN	**M**etropolitan **A**rea **N**etwork.
MD5	**M**essage **D**igest.
MDA	**M**ail **D**elivery **A**gent.
MTA	**M**ail **T**ransfer **A**gent.
MTU	**M**aximum **T**ransmission **U**nit.
MUA	**M**ail **U**ser **A**gent.
NCP	**N**network **C**ontrol **P**rotocol.
OSI	**O**pen **S**ystem **I**nterconnection.
PAN	**P**ersonal **A**rea **N**etwork.
PC	**P**ersonnel **C**omputer.
PFS	**P**erfect **F**orward **S**ecrecy.
POP3	**P**ost **O**ffice **P**rotocol.
PPP	**P**oint-to-**P**oint **P**rotocol.
PPTP	**P**oint-to-**P**oint **T**unneling **P**rotocol.
PSK	**P**re-**S**hared **K**ey.
RFC	**R**equests **F**or **C**omments.
RSA	**R**ivest **S**hamir **A**dleman.
SA	**S**ecurity **A**ssociation.
SAD	**S**ecurity **A**ssociation **D**atabase.
SHA	**S**ecure **H**ash **A**lgorithm.
SMTP	**S**imple Mail **T**ransfer **P**rotocol.
SP	**S**ecurity **P**olicy.
SPD	**S**ecurity **P**olicy **D**atabase.
SPI	**S**ecurity **P**arameter **I**ndex.
STP	**S**hielde **T**wisted **P**aire.
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol.
UTP	**U**nshielded **T**wisted **P**aire.

VPN	**V**irtual **P**rivate **N**etwork.
VLAN	**V**irtual **L**ocal **A**rea **N**etwork.
WAN	**W**ide **A**rea **N**etwork.

Introduction générale

À l'époque dans laquelle on est, l'exploitation de la technologie pour développer et accentuer notre capacité de communication arrive à un tournant. La généralisation de l'utilisation d'internet au niveau mondial s'est réalisée plus vite que personne n'aurait pu l'imaginer. La croissance exponentielle de ce réseau mondial induit un bouleversement des interactions sociales, commerciales, politiques et personnelles.

Parmi les principes fondamentaux de l'existence humaine, le besoin de communiquer arrive juste après le besoin de survie. Le besoin de communiquer est aussi important pour nous que l'air, l'eau et la nourriture. Les démarches que nous utilisions pour communiquer changent et évoluent sans cesse au fil du temps. Alors que nous avons été par le passé restreins aux interactions en face a face. Aujourd'hui, grâce aux réseaux informatiques modernes nous sommes plus connectés que jamais, les personnes communiquent de manière illimitée instantanément quelque soit la distance ou l'environnement où ils se trouvent.

Un réseau informatique est aujourd'hui devenu primordial au sein d'une entreprise. Il permet le transfert, l'exploitation, la centralisation et la sécurité des données, en effet, il permet de travailler en équipe de manière productive.

L'administration des réseaux informatiques est un domaine bien trop vaste et qui évolue trop rapidement et s'affirme aujourd'hui comme une activité clé de toute entreprise. Suite à ses fonctionnalités, ces outils d'échange de données et de partage d'informations en temps réel doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve. L'administrateur réseau doit arriver à déjouer des envahisseurs virtuels qui disposent de nouvelles armes de plus en plus sophistiquées. Autre difficulté l'arrivée de nouveaux employés qui n'ont pas toujours conscience de l'importance à accorder à la sécurité informatique, or il est particulièrement désagréable de voir son travail ruiné par un intrus qui aurait modifié, voire effacé, la configuration de ses équipements, il est préférable de conserver en sûreté les configurations de tous les équipements, pour pouvoir les restaurer rapidement en cas de problème.

La sécurisation des données bancaires de la BADR s'inscrit dans un thème général, celui de la sécurité informatique, un sujet fondamental, important, pour les établissements bancaires qui doivent lutter contre toutes formes de fraudes dans le but de protéger, en quelque sorte les capitaux, l'argent confié par les clients.

À travers l'objectif que l'entreprise s'est assignée, on estime lui accorder une attention soutenue, et pour cela nous avons jugé bon de porter notre choix sur ce sujet qui s'intitule : « Étude et amélioration de l'architecture réseau de la Banque de l'Agriculture et du Développement Rural de Béjaïa ».

Étudier en profondeur l'infrastructure informatique et le réseau existant de la BADR en par-

ticulier afin de déceler les lacunes et les problèmes lors de l'exécution des tâches journalières. Proposer une architecture meilleure dans l'objectif d'apporter une réelle plus-value et de répondre aux exigences de l'entreprise et en faire une synthèse.

Pour la réalisation de ce système et pour mener à bien notre travail, nous avons adopté un plan qui s'articule autour de quatre chapitres :

- ✓ Dans le premier chapitre, le mémoire traite les généralités sur les réseaux et la sécurité informatique en partant sur des trucs basiques, le champ d'application étant plutôt étendu, nous nous limiterons à quelques technologies fondamentales.

- ✓ Le second chapitre, nous faisons la présentation de l'entreprise qui nous a accueillis pendant notre stage, nous allons évoquer la problématique ainsi, que la solution appropriée.

- ✓ Le troisième chapitre est focalisé sur les réseaux locaux virtuels, les réseaux privés virtuels et la messagerie, leurs principes et fonctionnement, leurs différents types et les différents protocoles utilisés pour leur réalisation.

- ✓ Le quatrième et dernier chapitre traite la partie pratique de notre travail, nous abordons la configuration et la mise en œuvre des solutions proposées.

En ce qui concerne la méthodologie du travail, on a effectué des recherches bibliographique et aussi sur les sites web, ce qui nous a permis de cerner notre recherche.

Nous terminons ce manuscrit avec une conclusion générale.

Chapitre 1

Généralités sur les Réseaux et la Sécurité Informatique

Introduction

Le domaine des réseaux est en pleine effervescence, chaque année qui s'écoule apporte sa moisson de nouvelles technologies, offrant une série d'équipements matériels et de processus logiciels afin d'assurer la transmission des données. Le développement accéléré de cette technologie, le nombre important d'utilisateurs et les possibilités qu'offrent les réseaux actuellement font de lui un outil vulnérable, en effet les informations qui transigent entre les différentes machines se trouvant sur le réseau n'en découle pas sans risque. À compter de ce moment-là que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue une activité inévitable afin de garantir la protection, la confidentialité, l'intégrité et le contrôle d'accès des données qui circulent sur ce réseau.

Dans ce premier chapitre, nous expliquons les principes et le fonctionnement des réseaux et présentons en détail les matériels et architectures protocolaires sur lesquels ils se fondent, aussi nous passons en revue la sécurité informatique, les différentes attaques qui pourraient les affecter ensuite donner les principales mesures et stratégies de protection qui permettront de faire face à ces menaces.

1.1 Définition d'un réseau

Un réseau informatique est un moyen de communication formé d'un ensemble d'équipements appelés nœuds interconnectés selon des règles et des protocoles permettant à des individus ou à des groupes de partager des informations et des services.

Ces interconnexions peuvent concerner l'échange des flux d'informations, accès et la manipulation des ressources à tout utilisateur du réseau, indépendamment de leur emplacement physique ou de celui de la ressource [1].

1.2 Les différents types de réseaux

On distingue généralement quatre différents types de réseaux classés en fonction de leur taille, leur vitesse de transfert des données ainsi que leur étendue : [2]

⊙ **PAN (Personal Area Network) :** le réseau personnel centré sur l'utilisateur, permet d'interconnecter des équipements informatiques dans un espace d'une dizaine de mètres souvent de faible portée [2].

⊙ **LAN (Local Area Network) :** les réseaux locaux dont la portée sont limités de quelques mètres à plusieurs centaines de mètres. C'est le type de réseau que l'on peut installer chez soi, dans des bureaux ou dans un immeuble [2].

⊙ **MAN (Metropolitan Area Network) :** un réseau métropolitain couvre des communications sur des plus longues distances, interconnectant souvent plusieurs réseaux LAN, il s'étend à quelques dizaines de kilomètres [2].

⊙ **WAN (Wide Area Network) :** les réseaux étendus Constitués de réseaux de type LAN, voire MAN sont capables de transmettre les informations sur plusieurs centaines voire milliers de kilomètres à travers le monde entier [2].

Les différentes catégories des réseaux informatiques sont illustrées dans la figure suivante :

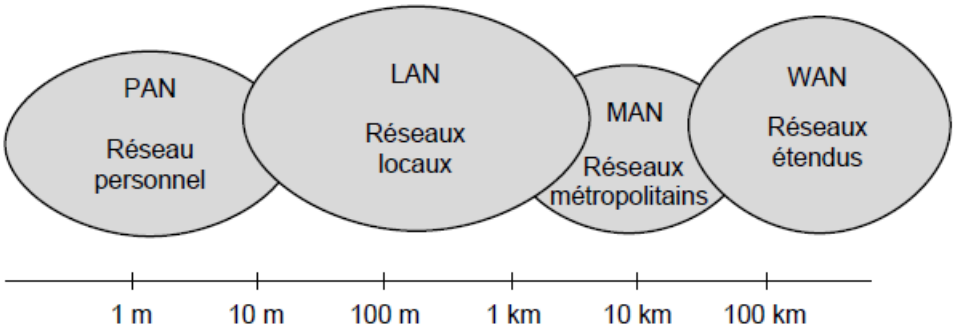


FIGURE 1.1 – Type des réseaux [4]

1.3 Les Topologies des réseaux

Une topologie caractérise la façon dont les différents équipements réseaux sont positionnés les uns par rapport aux autres. Il convient de distinguer :

- **la topologie physique :** la topologie physique définit la façon dont les systèmes finaux sont physiquement interconnectés. De ce fait les équipements sont reliés les uns aux autres par une connexion filaire par câble ou une connexion sans fil passant par les ondes radio [3].
- **la topologie logique :** désigne la manière dont un réseau transmet les trames d'un nœud à l'autre. Cette configuration est composée de connexions virtuelles entre les nœuds d'un réseau. Ces chemins de signaux logiques sont déterminés par les protocoles de couche liaison de données [3].

  A) **Topologie en bus :** la topologie en bus repose sur un câblage, sur lequel viennent se connecter des nœuds. Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux. La quantité de câbles utilisés est minimale et ne nécessite pas de point central. L'inconvénient majeur repose sur le fait qu'une seule coupure du câble empêche toute station d'échanger des informations sur le réseau [4].

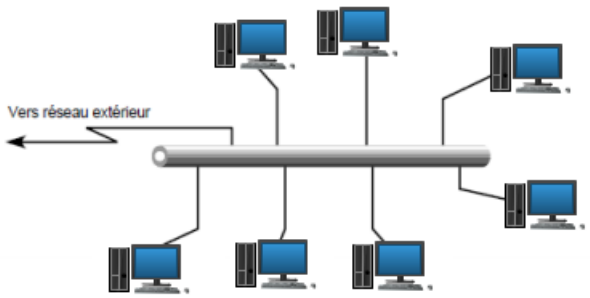


FIGURE 1.2 – La topologie en bus [4]

B) **Topologie en anneau :** les ordinateurs sont chainés entre eux, le premier étant connecté au dernier, afin de former l'anneau. Les trames transitent par chaque nœud, qui se comporte comme un répéteur. Les concentrateurs en anneau permettent l'insertion de stations dans un réseau [4].

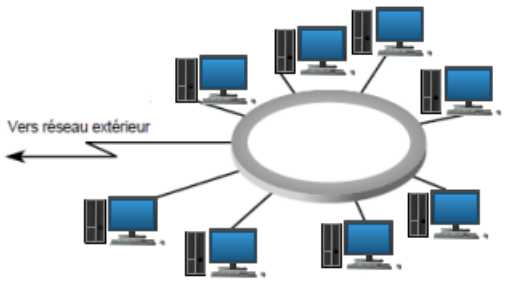


FIGURE 1.3 – La topologie en anneau [4]

C) **Topologie en étoile :** la topologie en étoile repose, quant à elle, sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère. Il intègre une fonction de répéteur. Ces points centraux sont appelés des concentrateurs (hubs). Il est possible de créer une structure hiérarchique en constituant un nombre limité de niveaux [4].

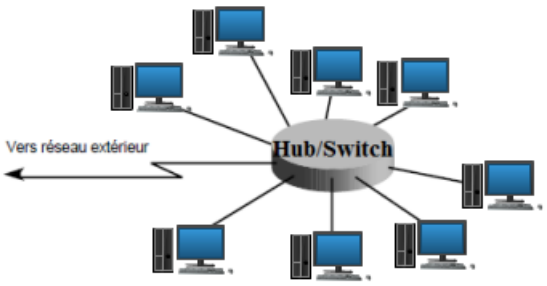


FIGURE 1.4 – La topologie en étoile [4]

D) **Topologie en arbre :** dans l'architecture en arbre, les postes sont reliés entre eux de manière hiérarchique, l'arbre est caractérisé par une structure arborescente. À chaque intersection correspond un hub alimenté électriquement, dont le rôle est de répéter, dans toutes les directions possibles. Cette caractéristique permet, à partir de n'importe quelle station, d'atteindre toutes les autres [4][5].

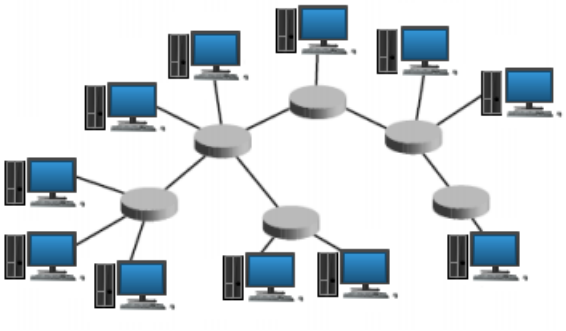


FIGURE 1.5 – La topologie en arbre [4]

1.4 Architecture des réseaux

Pour transférer les données, les réseaux peuvent être organisés selon deux façons : les réseaux pair à pair et les réseaux clients serveurs.

- **Peer to peer (pair à pair) :** sur l'architecture d'un réseau pair à pair, les ordinateurs participant fassent à la fois office de serveur et de client sur le réseau [3].
- **Clients et serveurs :** sur un réseau clients serveurs, Les clients sont des ordinateurs équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher. Les serveurs sont des ordinateurs équipés de logiciels leur permettant de fournir des informations aux clients [3].

1.5 Équipements d'interconnexion d'un réseau local

⊙ **Carte réseau :** carte réseau se charge de contrôler les transmissions sur le câble et permet de connecter un périphérique au réseau. La carte réseau Ethernet est utilisées dans les connections filaires.

⊙ **Concentrateur (Hub) :** c'est un élément matériel qui est considéré comme une multiprise informatique possédant un certain nombre de ports, permettant de concentrer le trafic réseau provenant de plusieurs équipements terminaux, et de générer le signale [5][6].

⊙ **Commutateur (switch) :** c'est un pont multiport qui concentre également les câbles en provenance de toutes les machines du réseau, mais contrairement aux hubs, le switch possède une mémoire ou il stocke les adresses de toutes les machines qui lui sont connectées [5][6].

⊙ **Routeur :** c'est un matériel d'interconnexion qui joue le rôle de pont ou de commutateur, il examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire pour atteindre une destination. Le routeur connait la liste de tous les segments du réseau existants qu'il conserve dans sa table de routage, cette dernière doit répondre à toutes les demandes émise par les paquets en mémoire [5][6].

⊙ **Répéteur (repeater) :** c'est un équipement simple considéré comme non intelligent, il régénère un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Il répète automatiquement les signaux qui lui arrivent et transitent d'un support vers un autre support [5][6].

⊙ **Pont (bridge) :** au contraire d'un répéteur, un pont est considéré comme un équipement intelligent, capable de reconnaître les adresses des blocs d'information qui transitent sur le support physique. Il peut filtrer les trames et laisse passer les blocs destinés au réseau raccordé [5][6].

⊙ **Modem (modulateur démodulateur) :** le modem est un périphérique qui permet de transmettre et de recevoir les données numériques en signaux analogiques et inversement pouvons être acheminés par une ligne téléphonique [6].

⊙ **Passerelle (gateway) :** les passerelles jouent le rôle d'intermédiaire en permettant d'établir une communication entre des architectures réseaux différentes. Servant notamment à faire l'interface entre des protocoles différents [5][6].

1.6 Support d'interconnexion

On distingue 3 types de câble :

1.6.1 Le câble coaxial

C'est le câble le plus ancien, il est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant afin de limiter les perturbations dues au bruit externe. Des débits supérieurs à 100 Mbit/s peuvent être atteints [5][7].

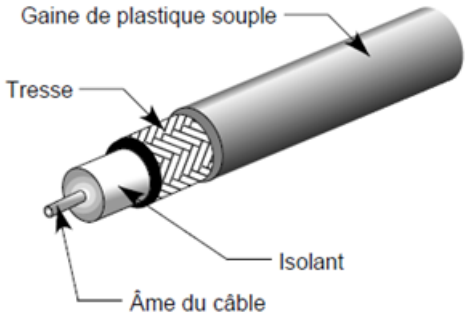


FIGURE 1.6 – Câble coaxial [4]

1.6.2 Le câble pair torsadé

Est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants. On distingue deux types de paires torsadées :

- **Paire non blindées UTP (Unshielded Twisted Paire) :** c'est le type de paires torsadée le plus utilisé et le plus répondu pour les réseaux locaux, se compose de quatre paires de fils à code couleur qui ont été torsadés, puis placés dans une gaine en plastique souple qui les préserve des dégâts matériels mineurs. Le fait de torsader les fils permet de limiter les interférences. Il peut transmettre un signal d'information sur un segment de 100 mètres au maximum pour une bande passante de 10 Mbit/s à 10 Gbit/s [5][7].
- **Paires blindées STP (Shielde Twisted Paire) :** utilise une gaine de meilleur qualité et plus protectrice que la gaine utilisée en câble UTP, il permet une transmission plus rapide et sur une plus longue distance [5][7].

1.6.3 La fibre optique

La fibre optique est un support de transmission de signaux sous forme d'impulsions lumineuses, elle se compose d'un un fil en verre très pur et transparent. Contrairement aux fils de cuivre, les câbles à fibre optique peuvent transmettre des signaux avec moins d'atténuation et sont entièrement protégés des perturbations électromagnétiques et radioélectriques [5][7].

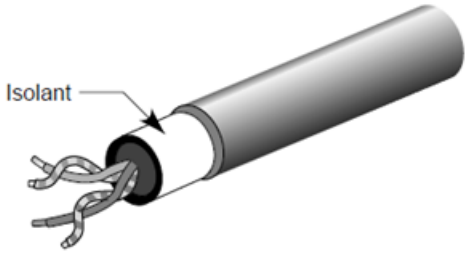


FIGURE 1.7 – Câble à pair torsadé [4]

On distingue deux types de fibre optique :

- **Fibre optique monomode :** son cœur présente un très faible diamètre et elle fait appel à la technologie coûteuse qu'est le laser dans laquelle ne peut envoyer qu'un seul rayons lumineux, elle est répandue dans les réseaux longue distance pour une bande passante de 10 Mbit/s à 100 Gbit/s [5][7].
- **Fibre optique multimode :** son cœur est supérieure elle utilise des émetteurs LED pour envoyer des impulsions lumineuses, elle est généralement utilisée dans les réseaux locaux et fournit une bande passante allant jusqu'à 10 Gbit/s [5][7].

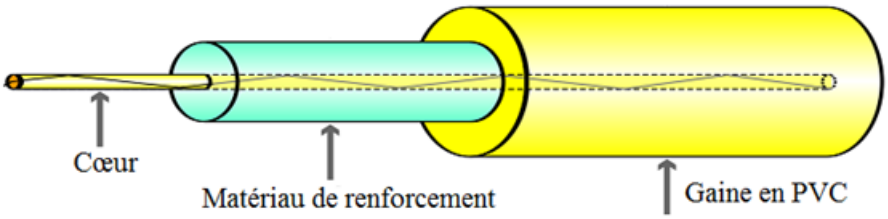


FIGURE 1.8 – Câble fibre optique [7]

1.7 Le modèle OSI (Open System Interconnection)

L'interconnexion des systèmes ouverts (OSI) de l'organisme ISO (Organisation Internationale de normalisation), appelé modèle de référence est un ensemble de règles que les machines terminales doivent respecter pour que la communication soit possible. Ce modèle se compose de sept couches, chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes [1].

FIGURE 1.9 – Le modèle OSI

- **Couche physique :** la couche physique a pour rôle la transmission de bits sur un canal de transmission [8].
- **Couche liaison de données :** cette couche se charge de détecter et de corriger les erreurs de transmission de la couche inférieure. Les objets échangés sont appelés trames [8].
- **Couche réseau :** la couche réseau à pour rôle d'interconnecter les réseaux entre eux, et de déterminé la façon dont les paquets sont routés de la source vers la destination [8].
- **Couche transport :** assure la transmission des messages de bout en bout de la source à la destination [8].
- **Couche session :** permet d'établir des sessions qui offrent aux utilisateurs la gestion de leur dialogue, les interrompe ou les reprendre tout en assurant la cohérence des données échangés [8].
- **Couche présentation :** cette couche met en forme les données transmises pour les rendre compréhensibles par le destinataire [8].
- **Couche application :** fournit le moyen de s'échanger les informations entre les programmes fonctionnant sur l'ordinateur et les autres services des réseaux [8].

1.8 Présentation de la pile protocolaire TCP/IP

Le modèle référence TCP/IP (pour Transmission Control Protocol/Internet Protocol) est une suite de protocoles. Particulièrement inspiré de modèle OSI repose sur un modèle de conception à quatre couches, chacune des couches de ce modèle est homologue à une ou plusieurs couches du modèle de référence OSI [9].

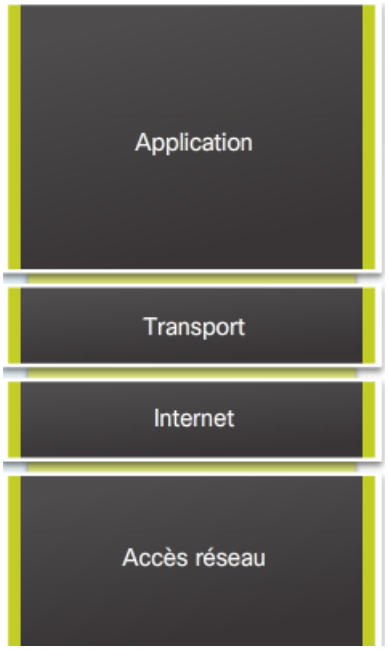


FIGURE 1.10 – Le modèle TCP/IP

⊙ **La couche accès réseau**

La couche accès réseau correspond aux couches liaisons de données et physique du modèle OSI. Elle a comme principales fonctions :

- S'occupe de l'envoi des paquets TCP/IP sur le support du réseau, et de la création des paquets TCP/IP qui transitent sur ce support.
- les périphériques matériels et les supports qui constituent le réseau [9].

⊙ **La couche internet**

La couche internet est similaire à la couche réseau du modèle OSI. Elle a comme principales fonctions : [9]

- Assume des fonctions d'adressage et de mise en paquets.
- Spécifie le meilleur chemin à travers le réseau.

⊙ **La couche transport**

La couche transport prend en charge les responsabilités de la couche transport du modèle OSI ainsi que certaines responsabilités de la couche session. Elle a comme principales fonctions : [9]

- Fournit les services de session et de communication par datagrammes à la couche application.
- Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.
- Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.
- Assure le contrôle d'erreurs et du contrôle de flux entre les extrémités.

⊙ **La couche application**

- Offre aux applications la possibilité d'atteindre les services des autres couches et indique les protocoles qu'elles utiliseront pour échanger des données.
- Représente les éléments d'informations pour l'utilisateur, ainsi que du codage et l'inspection du dialogue.

1.9 Comparaison des modèles de références OSI et TCP /IP

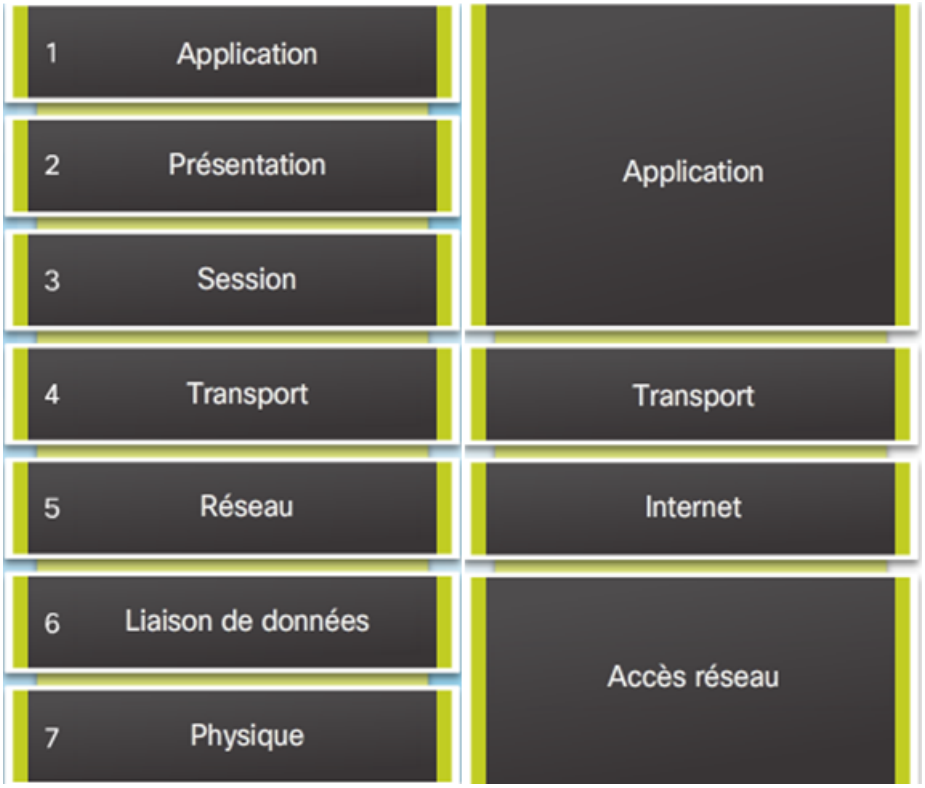


FIGURE 1.11 – Comparaison des modèles OSI et TCP/IP

Les modèles de références OSI et TCP/IP ont beaucoup de points communs. Ils reposent tous deux sur le concept de pile de protocoles indépendants. Malgré cette similitude, les deux modèles présentent également de nombreuses différences.

Tout d'abord, il y a le nombre de couches sept dans le modèle OSI et quatre dans le modèle TCP/IP.

Ensuite, le concept, le modèle OSI repose au centre de trois concepts les services, les interfaces et les protocoles. Quant au modèle TCP/IP, n'a jamais clairement fait la distinction entre les services, les interfaces et les protocoles.

Enfin, le type de communication, Le modèle OSI autorise les deux types de communication (mode avec connexion et sans connexion) dans la couche réseau, mais uniquement le mode avec connexion dans la couche transport. Le modèle TCP/IP ne prend en charge qu'un mode dans la couche réseau (sans connexion), mais deux dans la couche transport, ce qui donne le choix aux utilisateurs [10][11].

1.10 Adressage

⊙ **Protocole IP :** c'est un protocole réseau de niveau 3 du modèle OSI, il s'occupe de l'dressage IP.

⊙ **Adressage IP :** c'est un adressage codé sur 32 bits, chaque interface possède une adresse IP fixée par l'administrateur du réseau local ou attribuée de façon dynamique par un serveur DHCP. L'adresse IP identifie l'emplacement d'un hôte sur le réseau et doit être unique.

⊙ **Classes d'adresse IP :** il existe 5 classes d'adressage : [12]

- **Classe A :** 8 bits utilisés pour l'adresse réseau et 24 pour l'adresse machine. Le premier bit du poids fort est à '0'.
- **Classe B :** 16 bites utilisés pour l'adressa réseau et 16 bits pour l'adresse machine. Les deux premiers bits du poids fort sont à '10'.
- **Classe C :** 24 bits utilisés pour l'adresse réseau et 8 pour l'adresse machine. Les trois premiers bits du poids fort sont à '110'.
- **Classe D :** 8 bits utilisés pour l'adresse réseau et 24 bits pour l'adresse machine. Les quatre premiers bits du poids fort sont à '1110'.
- **Classe E :** 8 bits utilisés pour l'adressa réseau et 24 pour l'adresse machine. Les quatre premiers bits de poids fort sont à '1111'.

⊙ **Adresses réservées** :

- **Adresse d'acheminement par défaut (route par défaut) :** 0.X.X.X destinés à un réseau inconnu.
- **Adresse de bouclage (loopback) :** 127.X.X.X elle sert à tester le fonctionnement de la carte réseau. On utilise généralement 127.0.0.1
- **Adresse réseau :** c'est tous les bits d'hôtes qui sont positionnés à '0'.
- **Adresse de diffusion :** c'est tous les octets d'hôtes qui sont positionnés à 255.
- **Adresse privées :** elles sont utilisées pour les réseaux locaux :
  - Pour la classe A (10.0.0.1 à 10.255.255.254).
  - Pour la classe B (172.16.0.1 à 172.31.255.254).
  - Pour la classe A (192.168.0.1 à 192.168.255.254).

1.11 Sécurité informatique

La sécurité informatique est primordiale pour faire face aux multitudes de dangers, elle consiste à éviter qu'un curieux individu lie ou, plus mal encore, modifier des messages destinés à d'autres.

La sécurité s'attaque aux problèmes de capture et rejeu de message légitimes et aide a démasqué ceux qui nient être les acteurs de tel ou tel message.

1.11.1 Objectifs de la sécurité informatique

Pour assurer la sécurité d'un réseau il faut se tenir compte de quatre domaines étroitement imbriqués : [13]

☞ **La confidentialité :** assurer que l'information ne soit divulguée ou révélée qu'aux personnes autorisées.

☞ **L'authentification :** s'assurer de l'identité d'un interlocuteur avant de lui révéler des informations confidentielle ou de traiter avec lui.

☞ **La disponibilité :** l'accès par un sujet autorisé aux ressources et informations du système doit être toujours possible.

☞ **Non répudiation :** s'applique aux signatures, c'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut dénier l'avoir effectué.

1.11.2 Menaces pour la sécurité

La sécurisation d'un réseau exige l'utilisation de protocoles, de technologies, de périphériques, d'outils et de techniques permettant de sécuriser les données et de restreindre les risques. Ces menaces peuvent être externes ou internes. De nombreuses menaces externes pour la sécurité réseau se diffusent aujourd'hui par internet [14].

Les menaces externes les plus fréquentes pour les réseaux sont les suivantes :

⊙ **Virus, vers, et chevaux de troie :** logiciels malveillants et code arbitraire s'exécutant sur un périphérique utilisateur.

⊙ **Logiciels espions et publicitaires :** logiciels installés sur un périphérique utilisateur qui récolte discrètement des informations sur l'utilisateur.

⊙ **Attaques zero-day, également appelées attaques zero-hour :** attaques qui se produisent le jour où une vulnérabilité est détectée.

⊙ **Attaques de pirates :** offensives lancées sur des ressources réseau par une personne qui possède de solides connaissances en informatique.

⊙ **Attaques par déni de service :** attaques conçues pour ralentir ou bloquer les applications et les processus d'un périphérique réseau.

⊙ **Interception et vol de données :** attaques visant à obtenir des informations confidentielles à partir du réseau d'une entreprise.

⊙ **Usurpation d'identité :** attaques visant à récolter les informations de connexion d'un utilisateur afin d'accéder à des données privées.

À l'instar des menaces externe. Il est également important de prendre en compte les menaces internes. D'importantes études affirment que la majorité des violations de données se produisent par la maladresse des utilisateurs internes du réseau. Ces infractions peuvent découler d'une perte ou d'un vol de périphériques, de la mauvaise utilisation d'un périphérique par un employé ou, dans un contexte professionnel, d'un employé malveillant.

1.11.3 Stratégies de la sécurité

La stratégie de sécurité consistante à mettre en œuvre des moyens et des dispositifs pour objectif la protection des systèmes d'information. Elle comprend un ensemble de règles définissant une stratégie.

En voici les principaux dispositifs permettant de sécuriser un réseau contre les attaques.

- **Un pare-feu**
  Est un dispositif informatique matériel et/ou logiciel qui contribue à combler le manque de sécurité de tout système informatique et permet d'appliquer une politique d'accès aux ressources réseau (serveurs) en se comportant comme un filtre de paquets. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur le trafic, ou encore toutes les connexions entre les réseaux. Le filtrage réalisé par le par pare-feu constitue le premier rempart de la protection du système d'information. Son installation est incontournable dans le réseau local de l'entreprise ce qui lui permet de contrôler l'accès des ressources externes vers l'intérieur mais également entités éloignés de l'entreprise mais reliées par un réseau de type extranet [1] [15].

1. **extranet :** une entreprise peut utiliser un extranet pour fournir un accès sécurisé aux personnes qui travaillent pour une autre entreprise, mais qui ont besoin d'accéder aux données de l'entreprise en question.

- **Zone démilitarisée**
  La DMZ est une interface de sous-réseau placé entre un réseau interne de confiance et un réseau externe non sécurisé. Elle dispose de différents dispositifs de filtrage réseau, mais aussi de relais applicatifs dans l'objectif de ne rien laisser entrer directement au sein de l'infrastructure [16].

- **La technologie AAA**
  - **L'authentification :** il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assuré au moins d'un secret partagé ou d'un logiciel approuvé [17].
  - **Autorisation :** elle intervient à issue de l'authentification. Une fois que l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les actions qu'il demande. L'autorisation est gérée au moyen de liste ACL ou de stratégie [17].
  - **Traçabilité :** permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau [17].

- **Liste de contrôle d'accès (ACL)**
  Les listes de contrôle d'accès sont des instructions qui expriment une liste de règle, imposées par l'opérateur, donnant un control supplémentaire sur les paquets reçus et transmis par le routeur. Les listes de contrôle d'accès permettent d'autorisé ou de refuser des paquets, que ce soit en entrée ou en sortie vers une destination [25].

- **Systèmes de détection d'intrusion**
  Un IDS (Intrusion Detection System) est le système d'alarme du réseau. Au travers des outils de détection qui viennent compléter les fonctions du pare-feu. Seul l'IDS permet d'informer des accès non autorisés ou des intrusions dans les réseaux. Les pare-feu qui opèrent avec les IDSs sont capables de détecter automatiquement les menaces venant de l'extérieur plus rapidement qu'une vérification par un opérateur [13].

- **Proxys**
  Un proxy (mandataire), c'est un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Il existe deux types principaux de proxy, les proxy de type applicatif et les proxy de type circuit. Les proxy applicatifs interviennent au niveau 7, ou application, avec pour objectif de rompre le modèle client-serveur pour passer au modèle client-client. Les seconds ne permettent pas une connexion TCP de bout en bout et sont plutôt destinés à du trafic sortant d'utilisateurs authentifiés.

- **Les réseaux privés virtuel (VPNs)**
  Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécuriséentre une source et une destination. Grace à un principe de tunnel (tunneling)dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées. Un des grands intérêts des VPNs est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'internet. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service n'est garantie [18].

- **Les réseaux local virtuel (VLANs)**
  Les VLANs offrent une solution pour regrouper les stations et les serveurs en ensembles indépendants, de sorte à assurer une bonne sécurité des communications.
  Ce mécanisme permet de créer plusieurs réseaux virtuels au sein d'un même réseau physique et d'allouer des configurations spécifiques pour chaque réseau virtuel créé.

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères [15].

1.12 Conclusion

Au terme de ce chapitre, nous avons définit les concepts fondamentaux dans les réseaux Informatiques, ainsi que le besoin de la sécurité informatique. Le chapitre suivant va porter sur une étude du réseau existant au sein de la BADR ainsi qu'une synthèse de ses faiblesses et leurs solutions.

Chapitre 2

Étude de l'existant

Introduction

Dans ce chapitre, nous commencerons par une présentation globale de l'entreprise où nous avons eu l'honneur d'effectuer notre stage à la BADR, les éléments constituant le réseau informatique de celle-ci, son périmètre de sécurité en plus de son organisation afin d'en déduire les différents points faibles du réseau, les risques et menaces auxquels elle y est exposée. Pour y remédier une nouvelle architecture améliorée du réseau sera proposée dans le présent chapitre afin de pallier les problèmes mis en évidence tout en passant par le volet modernisation dans le but d'aboutir à un réseau qui accompagnera la croissance de l'entreprise.

2.1 Présentation de la BADR

La Banque de l'Agriculture et du Développement Rural BADR, est une institution financière nationale créée le 13 mars 1982 sous la forme juridique de société par actions. Son capital social est de 33 000 000 000 de DA. Constituée initialement de 140 agences, son réseau compte actuellement plus de 300 agences et 39 directions régionales. Quelques 7 000 cadres et employés activent au sein des structures centrales, régionales et locales. La densité de son réseau et l'importance de son effectif font de la BADR la première banque à réseau au niveau national. Elle constitue aujourd'hui le premier support pour le développement de l'économie agricole et rurale et s'est imposée dans le secteur financier et banquier algérien comme l'acteur incontournable et le leader incontesté dans le financement des secteurs de l'agriculture, des industries agroalimentaires, de la pèche et de l'aquaculture [26].

2.2 Mission et objectif de la BADR

2.2.1 Ses principales missions

- Le traitement de toutes les opérations de crédit, de change et de trésorerie ;
- L'ouverture de comptes ;
- La réception des dépôts à vue et à terme ;
- La participation à la collecte de l'épargne ;
- La contribution au développement du secteur agricole ;
- L'assurance de la promotion des activités agricoles, agro-alimentaires, agro-industrielles et artisanales ;
- Le contrôle avec les autorités de tutelle de la conformité des mouvements financiers des entreprises domiciliées.

2.2.2 Ses principaux objectifs

- L'augmentation des ressources aux meilleurs coûts et rentabilisation de celles-ci par des crédits productifs et diversifiés dans le respect des règles ;
- La gestion rigoureuse de la trésorerie de la banque tant en dinars qu'en devises ;
- L'assurance d'un développement harmonieux de la banque dans les domaines d'activités la concernant ;
- L'extension et le redéploiement de son réseau ;
- La satisfaction de ses clients en leurs offrant des produits et services susceptibles de répondre à leurs besoins ;
- L'adaptation d'une gestion dynamique en matière de recouvrement ;
- Le développement commercial par l'introduction de nouvelles techniques managériales telles que le marketing, et l'insertion de nouvelles gammes de produits.

2.3 Présentation du champ d'étude

2.3.1 Présentation du Groupe Régional d'Exploitation de Béjaïa

La BADR est représentée au niveau de la wilaya de Béjaïa par un Groupe Régional d'Exploitation (GRE), et de treize Agences Locales d'Exploitation (ALE), réparties à travers différentes localités pour mieux se rapprocher de sa clientèle.

Agence Béjaïa 357, c'est l'agence principale au niveau de la wilaya de Béjaïa, elle occupe la même bâtisse que le GRE, située sur la rue de la liberté, elle est la plus impliquée et possède plus de prérogatives que les autres agences, elle est aussi responsable de leurs alimentations en liquidité (Dinars et Devise).

Dans le tableau qui suit, viennent ensuite les 12 autres agences qui son classées comme tel : [19]

N° Agence	Désignation	Adresse
357	BÉJAÏA	Rue de la liberté
358	AKBOU	Rue LARBI TOUATI
359	AMIZOUR	Cité des 154 Logements BP38
360	KHERRATA	Rue CHAHID ALLIK LAMRI BP 64
361	SOUMMAM	Avenue BEN BOULAID
362	SIDI-AICH	Rue du 1er novembre BP 37
363	TAZMALT	Centre commercial de TAZMALT
364	YEMMA GOURAYA	Boulevard de la SOUMMAM
365	SEDDOUK	Rue BENIKEN MOHAND SAID
366	AOKAS	Centre commercial BP 77 BIS
367	OUZELLAGUEN	Route nationale BP 15
368	EL KSEUR	Rue MARKHOUF ABDELAZIZ
369	SOUK El Ténine	Cité des 83 logements

Table 2.1 – Liste des différentes ALE de Béjaïa

Les différentes structures du GRE de la BADR de Béjaïa sont présentées dans l'organigramme ci-dessus : [19]

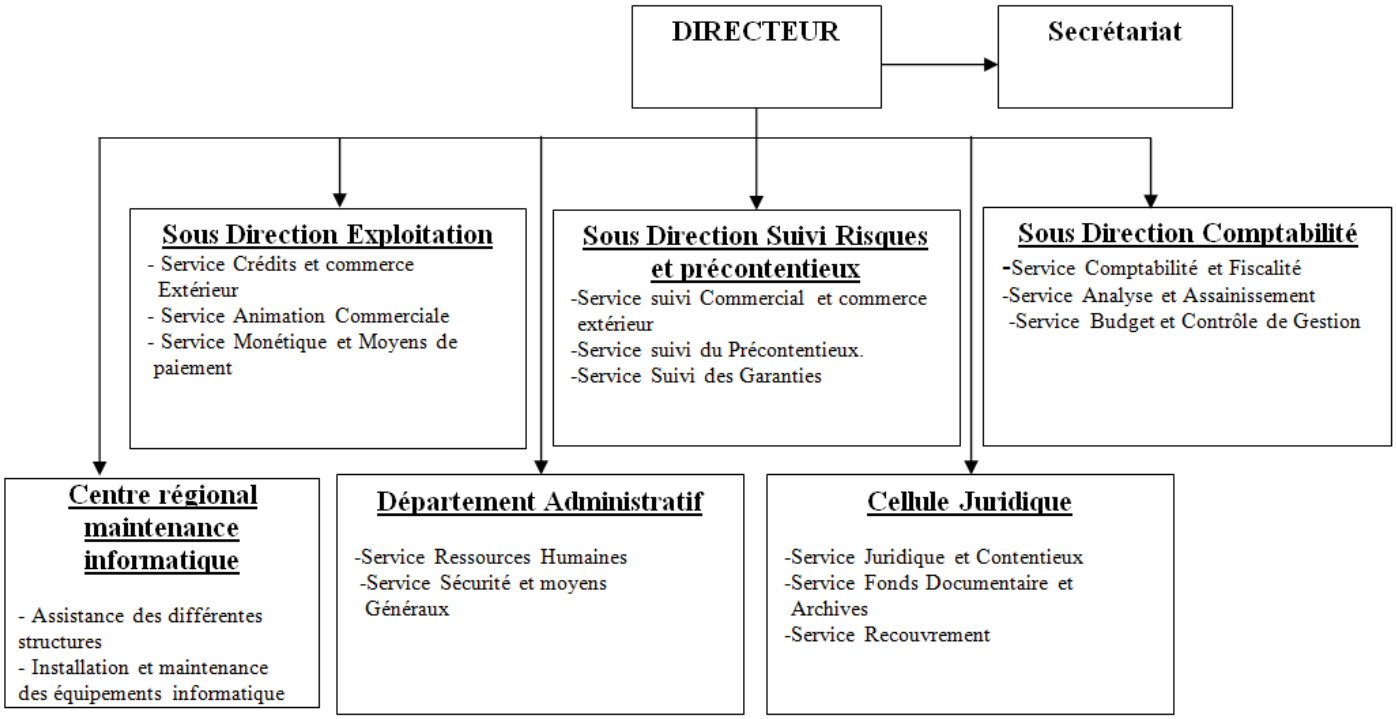


FIGURE 2.1 – Organigramme générale du groupe régional d'exploitation de Béjaïa [19]

2.4 Les ressources informatiques de la BADR

2.4.1 Les ressources matérielles

Représentée dans les quarante huit wilayas du pays avec plus de trois cent structures, la BADR dispose d'un parc informatique impressionnant, un des plus importants au niveau national et le plus grand dans son secteur. Le GRE de Béjaïa comme chaque structure de la BADR que ce soit un autre GRE, une ALE, une inspection ou une direction centrale, dispose d'une salle informatique aménagée spécialement pour le fait, d'un réseau électrique ondulé indépendant et un générateur, elle abrite aussi les serveurs, l'armoire de brassage, les équipements de télécommunication, les onduleurs, l'imprimante arrière guichet et les équipements de vidéo surveillance. Tandis que les postes de travail qui se composent en général d'une unité centrale, d'un écran et d'une imprimante, évidemment d'une prise ondulée, une de réseau et une autre téléphonique, sont répartis sur les différents services selon l'activité. On notera aussi que chaque agence possède en moyenne une quinzaine de postes, ajoutons à cela les GAB (Guichet Automatique Bancaire) [19].

2.4.2 La redondance matérielle

Sachant que le serveur de l'exploitation est la pièce maîtresse dans cette architecture client-serveur, si ce dernier tombe en panne c'est toute l'activité de la structure victime qui sera paralysée, tandis que l'arrêt d'un poste de travail ne peut en aucun cas mettre en péril toute l'activité de la structure. Etant consciente de ce risque la BADR a misé sur la redondance pour ce qui concerne les serveurs d'exploitation afin de parer aux pannes matériels habituelles. Tel que les crashs disques, la détérioration des lecteurs, les problèmes d'alimentations ...etc. La redondance est devenue le premier critère pour l'acquisition des serveurs d'exploitation [19].

Nous citerons à titre d'exemple :

Les serveurs HP Proliant ML350 dotés de deux alimentations hot plug indépendantes l'une de l'autre, si le premier compartiment tombe en panne le deuxième prend automatiquement le relai sans interruption. Egalement un contrôleur de six disques SCSI hot plug (branchement à chaud) équipé de deux disques durs configurés en raid1 [19].

Le serveur HP Cluster regroupe deux serveurs HP Proliant DL380 identiques connectés entre eux. Avec une baie de sauvegarde reliée à son tour aux deux serveurs. La baie peut contenir jusqu'à 14 disques durs et deux contrôleurs SCSI indépendants elle est également dotée de deux alimentations hotplug [19].

2.4.3 Les systèmes d'exploitation

La BADR utilise deux systèmes d'exploitation : [19]

- Windows XP Professionnel ;
- Windows Serveur 2003.

2.5 L'architecture du réseau de la BADR

L'architecture du réseau de l'entreprise de la BADR de Béjaïa est une architecture client-serveur. L'armoire de brassage regroupe tous les équipements réseau permettant aux utilisateurs de l'entreprise de pratiquer leurs tâches journalières respectives.

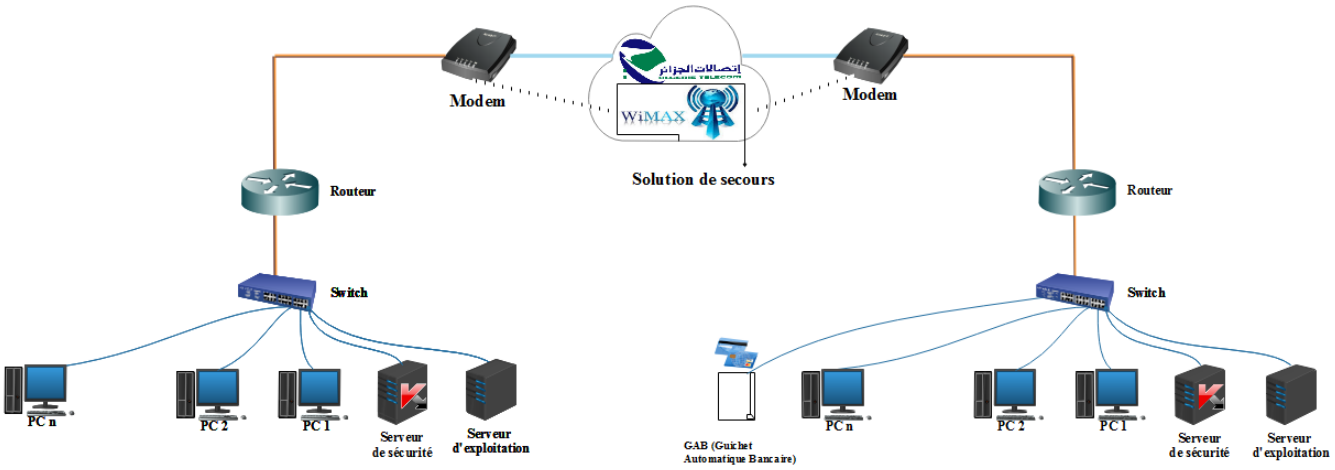


FIGURE 2.2 – Architecture réseau de la BADR

- **Connexion internet :** la BADR a opté pour le réseau RMS d'Algérie Telecom qui est un réseau multiservices de nouvelle génération NGN, de type IP/MPLS et d'envergure nationale. Ce réseau est destiné à l'interconnexion des équipements et réseaux informatiques. Ajouter à cela la BADR dispose d'un réseau de secours utilisant une liaison satellitaire avec des terminaux d'émission réception par satellite en parallèle avec la connexion filaire [19].
- **Sécurité**
  - **Pare-feu :** la BADR utilise un pare-feu logique c'est bien celui de Kaspersky Lab intégré à l'antivirus qui est installé sur tous les postes de travail, sur tous les serveurs Windows et sur le serveur central qui est connecté à internet [19].
  - **Anti-virus :** un des plus grands investissements de la BADR dans le domaine de la sécurité informatique. Apres des audits de sécurité effectués par des prestataires

reconnues mondialement dans ce domaine et vu les spécificités du système informatique de la BADR, il a était décidé de mettre en place une solution antivirus centralisée, deux facteurs majeurs ont été à l'origine de cette décision c'est bien l'administration de la solution et le suivi des mises à jours. Tandis que le choix des fournisseurs s'est joué sur quelques atouts techniques évidemment, et de l'offre financière de ces derniers conformément à la loi algérienne sur les marchés [19].

Les informaticiens de la BADR ont finalement opté pour la solution de Kaspersky Lab avec ses quatre applicatives cités ci-dessus :

Kaspersky Windows Workstation : un antivirus pour la plateforme Windows destiné aux postes de travail.

Kaspersky 6.0 Windows Servers : un antivirus pour les serveurs.

Kaspersky Administration Kit : un programme d'administration de la solution Kaspersky sur le réseau.

Net Agent : un utilitaire qui relie les postes de travail aux serveurs d'administration.

- **Salle machine :** contient les ressources nécessaires au bon fonctionnement du LAN de la BADR, et considéré comme le noyau du réseau où reposent toutes les activités de l'entreprise. Et se compose de Switch, de modem et de différentes machines serveurs.

2.6 L'architecture physique du réseau du GRE de Béjaïa

L'architecture du réseau local de groupe régional d'exploitation (GRE) de Béjaïa est représentée comme suit :

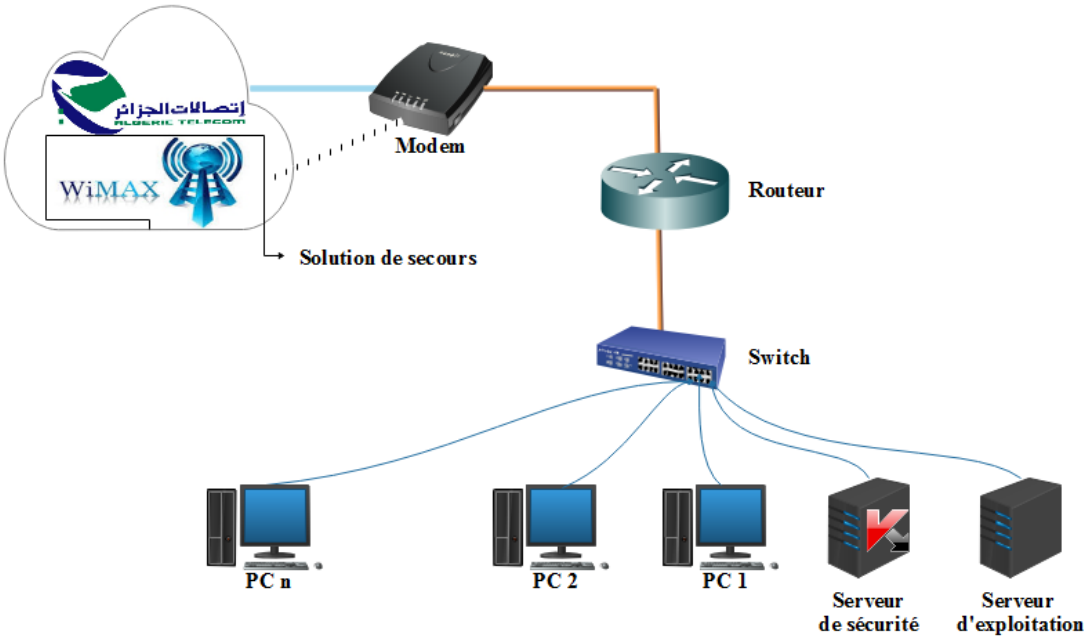


FIGURE 2.3 – Architecture physique du réseau du GRE de Béjaïa

2.7 L'architecture physique du réseau d'une Agence

L'architecture du réseau local d'une agence local d'exploitation (ALE) de Béjaïa est représentée comme suit :

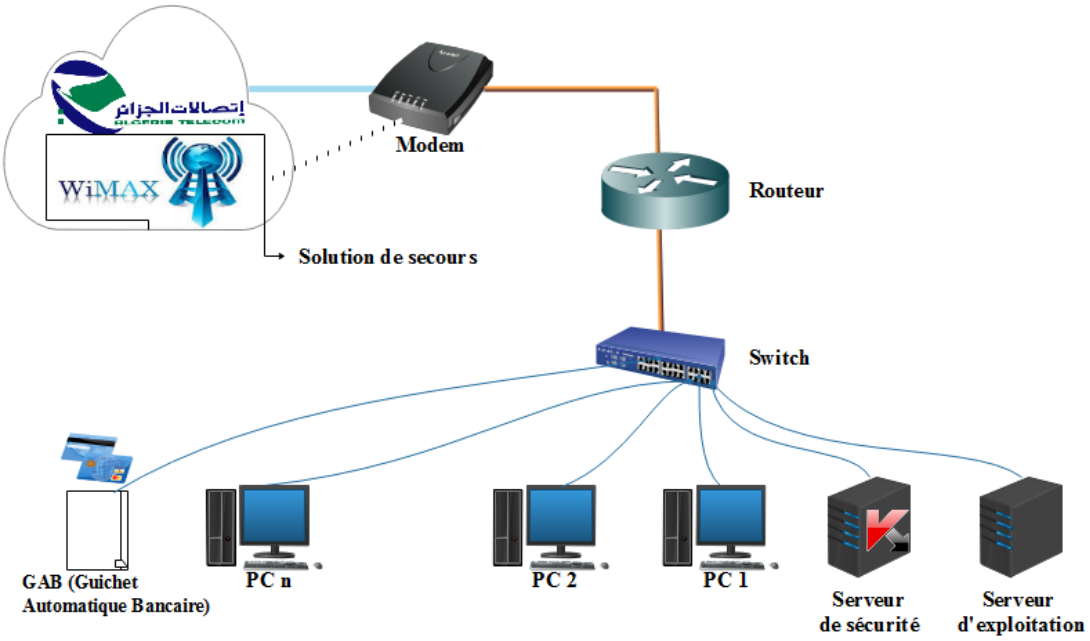


FIGURE 2.4 – Architecture physique du réseau d'une Agence

2.8 L'architecture logique du réseau du GRE

Dans ce tableau nous spécifions les adresses et masques utilisés au niveau du GRE de Béjaïa avec la passerelle associe à ce réseau (10.6.100.1) [19].

Prenons une adresse d'un hôte utilisé dans ce réseau par exemple l'adresse « 10.6.100.3 »

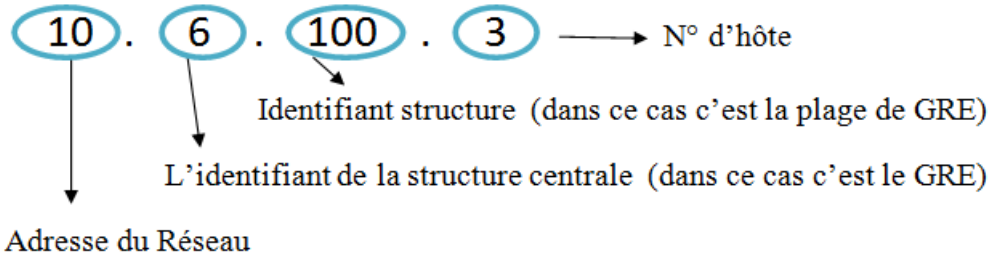


FIGURE 2.5 – Architecture logique du réseau du GRE

2.8.1 La Table d'adressage du GRE

Utilisateur	Adresse	Masque	Passerelle
SERVEUR 1	10.6.100.2	255.255.255.0	10.6.100.1
SERVEUR 2	10.6.100.3	255.255.255.0	10.6.100.1
PC 1	10.6.100.4	255.255.255.0	10.6.100.1
PC 2	10.6.100.5	255.255.255.0	10.6.100.1
.	.	.	.
.	.	.	.
.	.	.	.
PC n	10.6.100.n	255.255.255.0	10.6.100.1

Table 2.2 – Table d'adressage du GRE

2.9 L'architecture logique du réseau d'une Agence

Le tableau aborde les adresses et le masque utilisé au niveau d'une agence, on remarque que l'adressage reste presque le même par rapport à l'adressage soulevé dans le tableau précédent, la seule différence est au niveau de l'identificateur du GRE. Dans ce cas au lieu d'un identificateur global, nous précisons le matricule et le numéro de l'agence appartenant à ce GRE [19].

Exemple : quelques matricules des agences appartenant au GRE 100

N° Agence	Désignation	Identifiant agence
357	Béjaïa	1
358	AKBOU	2
359	AMIZOUR	3
360	KHERRATA	4
361	SOUMMAM	5

Table 2.3 – Matricules des agences appartenant au GRE de Béjaïa

Dans ce tableau nous prenons le cas de la Agence 357 (agence de la rue de la liberté) dans l'identifiant est 1.

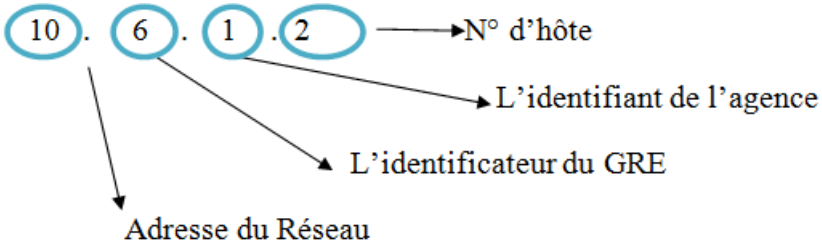


FIGURE 2.6 – Architecture logique du réseau de l'agence 357 (Béjaïa)

2.9.1 La table d'adressage d'une agence

Utilisateur	Adresse	Masque	Passerelle
SERVEUR 1	10.6.1.2	255.255.255.0	10.6.1.1
SERVEUR 2	10.6.1.3	255.255.255.0	10.6.1.1
PC 1	10.6.1.4	255.255.255.0	10.6.1.1
PC 2	10.6.1.5	255.255.255.0	10.6.1.1
.	.	.	.
.	.	.	.
.	.	.	.
PC n	10.6.1.(n-1)	255.255.255.0	10.6.1.1
GAB	10.6.1.n	255.255.255.0	10.6.1.1

TABLE 2.4 – Table d'adressage d'une agence

2.10 Problématique

Un réseau informatique est aujourd'hui devenu primordial au sein d'une entreprise, en effet il est utilisé pour enregistrer et gérer en interne des informations financières, des renseignements sur les clients et les systèmes de paie des employés. Grâce à un réseau informatique d'entreprise, les collaborateurs peuvent partager de nombreux types de services d'informations différents entre eux, des données et des applications dans le but d'accomplir leurs tâches, et ce de façon sûre et productive.

La Banque de l'Agriculture et du Développement Rural, BADR en sigle, est une institution financière bancaire jouant un rôle important dans la société Algérienne. Elle finance l'économie en

collectant l'épargne de ses clients et en donnant des crédits à ceux qui en ont besoin moyennant des intérêts et des garanties bien définis. Elle travaille essentiellement sur la base de confiance.

La sécurisation des données bancaires de la BADR s'inscrit dans un thème général, celui de la sécurité informatique, un sujet fondamental, important, pour les établissements bancaires qui doivent lutter contre toutes formes de fraudes dans le but de protéger, en quelque sorte les capitaux, l'argent confié par les clients.

Àfin de pouvoir cerner au mieux notre étude et être plus objectifs dans notre problématique, nous avons pris comme échantillon le groupe régional d'exploitation (GRE) où nous avons eu l'honneur d'effectuer notre stage de mise en situation professionnelle. Cependant, la première constatation qu'on a tirée est que l'architecture du réseau local de la Banque de l'Agriculture et du Développement Rural est une architecture très simple, plate, ou tout le monde se trouve dans le même domaine de diffusion.

En outre, la deuxième démarche était de s'intéresser aux menaces auxquelles elle est confrontée et aux différentes démarches sécuritaires de la BADR que nous avons jugé nécessaire d'avoir une vue globale sur les valeurs de son système informatique ainsi répondre à la première question qu'on doit se poser avant d'entamer quelconque démarche visant la sécurité informatique : que doit-on protéger ?

La BADR est une entreprise composée d'un GRE et de plusieurs Agences Locales d'Exploitation (ALE) distantes qui souhaite en tirer les avantages d'une liaison internet entre ces différents sites pour d'éventuelles tâches d'administration à distance, elle est aussi composée d'une plateforme de services qui souhaite les relier et partager les ressources en toutes sécurité. Le trafic inter-réseau était non sécurisé, toute les informations du réseau de l'entreprise circulaient en clair sur internet, par conséquent, ces données sont vulnérables et sensibles ce qui induit a des menaces qui sont liées à des actions ou des opérations émanant de tiers. L'importance des risques encourus, les menaces potentielles et définir un plan général de protection que l'on appelle politique de sécurité.

Toutefois, la mise en œuvre d'une politique de sécurité nécessite d'abord l'analyse des informations qui circulent et leur importance pour l'entreprise, analyse du coût que représenterait leur perte et celles des menaces que l'on peut objectivement envisager de résoudre.

2.11 Solution proposée

Pour mieux répondre au besoin de la BADR nous avons opté pour :

(i) La segmentation du réseau local du GRE en plusieurs LAN virtuels. Cette solution va permettre de :

- ☞ Créer un ensemble de groupe logique isolé pour améliorer la sécurité.
- ☞ Réduire le domaine de diffusion et la quantité de trafic inutile sur le réseau afin d'augmenter les performances de ce dernier.
- ☞ Faciliter la gestion du réseau.

Les VLANs représentent une technologie récente permettant d'appliquer plusieurs optimisations sur les réseaux locaux. Il est aujourd'hui de plus en plus répandu sur les réseaux LAN.

Un Réseau Local Virtuel est un réseau local regroupant un ensemble de machines de façon logique et non physique, en définissant une segmentation logique fondée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

(ii) La mise en place d'un VPN Site à Site permet au Groupe Régional d'Exploitation (GRE) de se connecter et de crypter la circulation d'informations d'un bout à l'autre via un tunnel d'une façon sécurisée avec les différentes Agences Locales d'Exploitation (ALE). Ce procédé, distant et sécurisé va permettre aux administrateurs de la GRE :

- ☞ Un accès au réseau local des ALE.
- ☞ D'effectuer des tâches d'administration efficacement au niveau de LAN des ALE.
- ☞ Communiquer, partager des fichiers et des programmes avec les ALE.

Un bon compromis consiste à utiliser internet comme support de transmission à partir d'un protocole "d'encapsulation" (en anglais tunneling, d'où la prononciation impropre parfois du terme "tunnellisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (VPN, acronyme de Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit virtuel, car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.

Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre cout, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie, il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti.

(iii) La mise en place d'un serveur de messagerie électronique au niveau du GRE. Cette solution va permettre de :

- ☞ Communiquer d'une manière rapide (temps réel).
- ☞ Protéger les communications échangés entre le personnel.
- ☞ Faciliter la gestion du réseau.

Le serveur de messagerie électronique est devenue un moyen incontournable dans l'internet des entreprises. Il permet l'échange d'informations, la gestion d'agendas, de contacts et de tâches qui assurent le stockage des informations.

2.12 Nouvelle architecture proposée

L'architecture du réseau de la BADR que nous proposons est présentée dans la figure suivante :

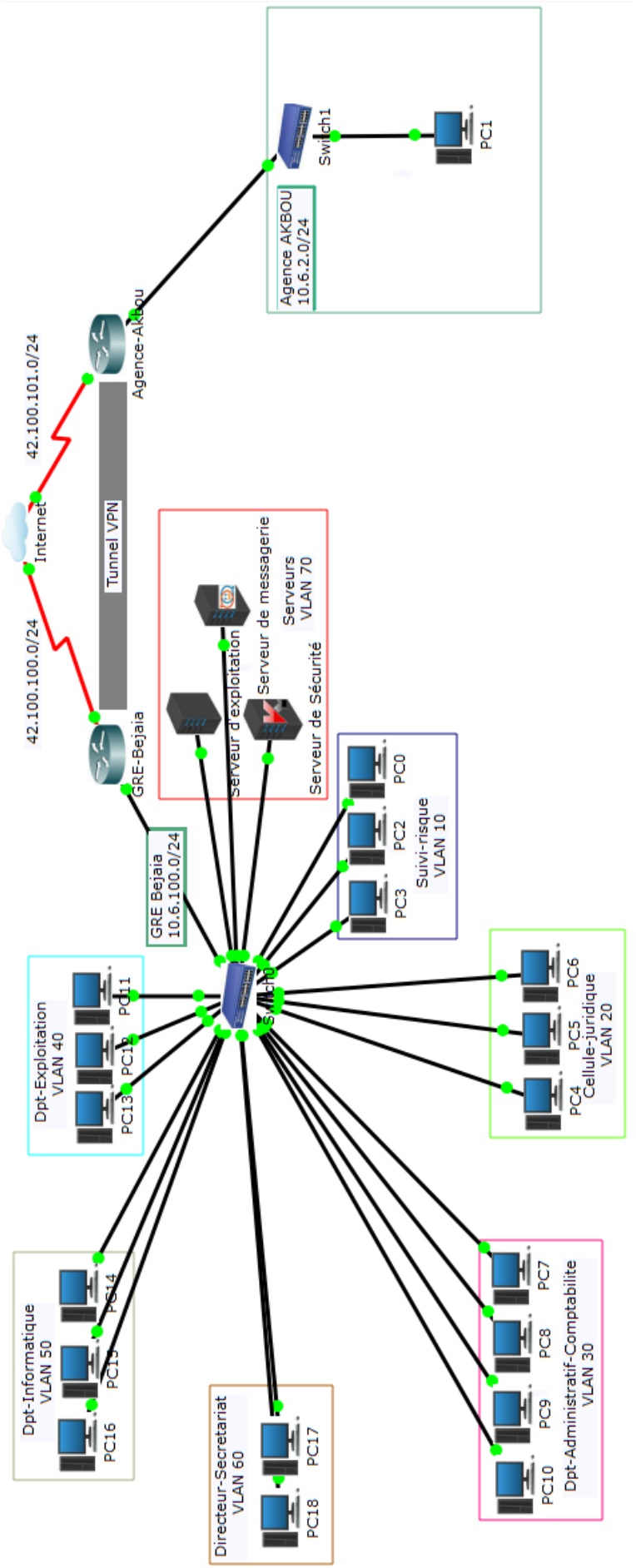


FIGURE 2.7 – Nouvelle architecture du réseau de la BADR réalisée sous Packet Tracer

2.13 Conclusion

Au cours de ce chapitre, nous avons présenté l'entreprise dans laquelle nous avons effectué notre stage, ce qui nous a permis de comprendre l'architecture réseau actuel de la BADR et d'éclaircir notre thème en mettant en avant notre problématique, en effet grâce à cette étude, nous avons pu critiquer cette architecture, suggérer quelques solutions et proposer une nouvelle architecture qui va offrir sans doute une meilleure sécurité et une meilleure souplesse au réseau de la BADR.

Le chapitre suivant se portera sur une étude générale des solutions retenues, ce qui nous permettra de meilleure planification du déploiement.

Chapitre 3

Étude des solutions retenues

Introduction

L'activité de ce chapitre est une étude détaillée sur les solutions proposées. Cette étude va nous permettre par la suite de mener à bien le projet. Pour cela, il se décomposera de trois parties. La première partie est consacrée à la solution VLAN, où nous expliquerons leurs concepts générale, et une description de leurs types leurs utilités et quelques protocoles permettant leur gestion. La deuxième partie va porter sur les VPNs auxquels nous allons présenter les principales caractéristiques des VPNs, à travers certaines définitions et principes de fonctionnement, les différents types ainsi que les détails sur le protocole IPSec. En dernier, la solution messagerie, où nous définirons la notion de la messagerie, les différents types et protocoles ainsi que l'architecture du service de messagerie.

3.1 Solution VLAN

3.1.1 Introduction au VLAN

Les performances réseau constituent un facteur important dans la productivité d'une entreprise. L'une des technologies permettant de les bonifier consiste à diviser de vastes domaines de diffusion en domaines plus petits. La fourniture d'un accès au LAN est une tâche généralement réservée au commutateur de la couche d'accès. Un réseau local virtuel (VLAN) peut être conçu sur un commutateur de couche 2 pour diminuer la taille des domaines de diffusion, de sorte qu'elle soit comparable à celle d'un périphérique de couche 3. Les VLANs sont habituellement intégrés à la conception du réseau, ce qui permet à ce dernier de s'adapter aux objectifs d'une entreprise.

3.1.2 Principe général des VLANs

Un VLAN produit un domaine de diffusion logique qui peut s'étaler sur plusieurs segments de réseau local physique. Les VLANs accordent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application, quel que soit l'emplacement physique de l'utilisateur ou du périphérique. Les périphériques d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLANs. N'importe quel port de commutateur peut appartenir à un VLAN. Les paquets monodiffusion, diffusion et multidiffusion sont transportés et diffusés seulement à des stations finales dans le VLAN dont proviennent les paquets. Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au VLAN doivent être transférés par un périphérique qui prend en charge le routage [20].

3.1.3 Avantages des VLANs

Les principaux avantages des VLANs sont les suivants : [20]

⊙ **Sécurité :** les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.

⊙ **Réduction des domaines de diffusion :** la division d'un réseau en plusieurs VLANs réduit le nombre de périphériques dans le domaine de diffusion.

⊙ **Meilleures performances :** le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques réduit la quantité de trafic inutile sur le réseau et augmente les performances.

⊙ **Réduction des coûts :** des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons existantes.

⊙ **Efficacité accrue du personnel informatique :** les VLANs facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseaux similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut aussi identifier facilement la fonction d'un VLAN en lui donnant un nom approprié.

⊙ **Gestion simplifiée de projets et d'applications :** les VLANs rassemblent des utilisateurs et des périphériques réseaux pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée. Une plate-forme de développement d'e-learning pour le personnel enseignant est un exemple de ce type d'application.

3.1.4 Types de VLANs

Plusieurs types de VLANs sont définis, selon le critère de commutation et le niveau auquel il s'effectue : [23]

- **VLAN par port (VLAN niveau 1)**
  Chaque port du commutateur est affecté à un VLAN donné. L'affectation des ports est statique, donc, l'administrateur peut savoir directement le VLAN d'appartenance d'un équipement. Cette technique est efficace dans les réseaux où les déplacements sont rares et contrôlés. En effet, une source externe ne peut y accéder au réseau, sauf si elle se branche sur le port appartenant au VLAN voulu à accéder, donc, un renforcement de la sécurité. Par contre, son inconvénient est sa lourdeur d'administration. En effet, si un matériel est déplacé et que l'on désire qu'il soit toujours dans le même VLAN, il faudra alors configurer le nouveau port [23].

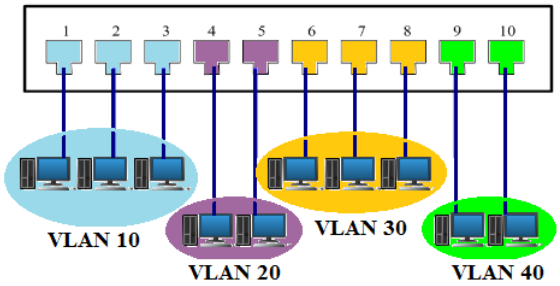


FIGURE 3.1 – VLAN par port [23]

- **VLAN par adresse MAC (VLAN niveau 2)**
  Consiste à définir un réseau virtuel en fonction des adresses MAC des stations. L'intérêt principal de ce type de VLANs est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables) [23].

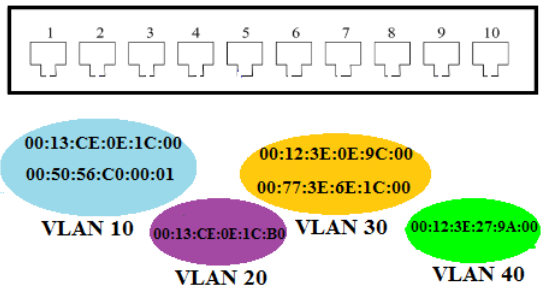


FIGURE 3.2 – VLAN par adresse MAC [23]

- **VLAN niveau 3**
  On distingue 2 types de VLANs de niveau 3 :
  - **Le VLAN par sous-réseau** : associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement [23].
  - **Le VLAN par protocole** : permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau [23].

3.1.5 Trunks de VLAN

Un trunk est une liaison point à point entre deux périphériques réseaux qui transporte plusieurs VLANs, il permet d'étendre les VLANs à l'ensemble d'un réseau. Sans trunk, les VLANs ne serviraient pas à grand-chose. Les trunks de VLAN permettent à tout le trafic VLAN de se propager entre les commutateurs, de sorte que les périphériques du même VLAN connectés à différents commutateurs puissent communiquer sans l'intervention d'un routeur.

Un trunk de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour plusieurs VLANs entre les commutateurs et les routeurs, il peut également être utilisé entre un périphérique réseau et un serveur ou un autre périphérique équipé d'une carte réseau 802.1Q appropriée [20].

3.1.6 Étiquetage des trames Ethernet pour l'identification des VLANs

Les commutateurs utilisent les informations de l'en-tête des trames Ethernet pour transférer les paquets, ils ne disposent pas de tables de routage. L'en-tête des trames Ethernet standard ne contient pas d'informations sur le VLAN auquel appartiennent les trames. Par conséquent, lorsque celles-ci sont placées sur un trunk, il convient d'ajouter les informations relatives au VLAN dont elles dépendent. Ce processus, appelé étiquetage, s'effectue à l'aide de l'en-tête IEEE 802.1Q.

L'en-tête 802.1Q inclut une étiquette de 4 octets insérée dans l'en-tête d'origine de la trame Ethernet, indiquant le VLAN auquel la trame appartient. Lorsque le commutateur reçoit une trame sur un port configuré en mode d'accès et associé à un VLAN, il insère une étiquette VLAN dans l'en-tête de trame, recalcule la séquence de contrôle de trame, puis envoie la trame étiquetée par un port trunk [20].

- **Détails du champ de l'étiquette VLAN**
  L'étiquette VLAN se compose d'un champ type, d'un champ priorité, d'un champ CFI (Canonical Format Identifier) et d'un champ d'ID de VLAN : [20]
  - **Type :** valeur de 2 octets appelée ID de protocole d'étiquette (TPID). Pour Ethernet, elle est définie sur une valeur hexadécimale 0x8100.
  - **Priorité utilisateur :** valeur de 3 bits qui prend en charge l'implémentation de niveaux ou de services.
  - **CFI (Canonical Format Identifier) :** identificateur de 1 bit qui active les trames Token Ring à transmettre sur des liaisons Ethernet.
  - **ID de VLAN (VID) :** numéro d'identification VLAN de 12 bits qui prend en charge jusqu'à 4 096 ID de VLAN.

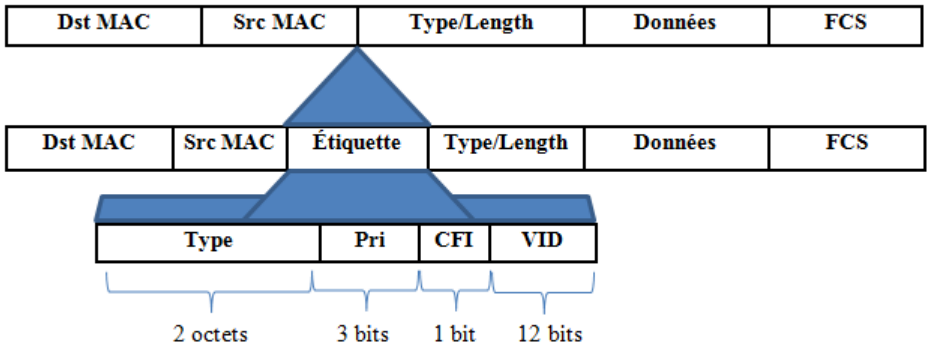


FIGURE 3.3 – Trames Ethernet de VLAN [20]

3.2 Solution VPN

3.2.1 Introduction au VPN

La sécurité est un problème lorsque les entreprises utilisent le réseau internet public pour mener à bien leurs activités. Les réseaux privés virtuels (VPNs) sont utilisés pour garantir la sécurité des données sur internet. Un VPN sert à créer un tunnel privé sur un réseau public. Les données peuvent être sécurisées à l'aide du chiffrement dans ce tunnel via internet et en utilisant une méthode d'authentification destinée à protéger les données de tout accès non autorisé.

3.2.2 Principe général des VPNs

Un réseau VPN repose sur un protocole nommé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptées d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié le destinataire et l'émetteur. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation [29].

3.2.3 Avantages des réseaux privés virtuels

Les avantages d'un VPN sont les suivants : [21]

⊙ **Sécurité :** consiste à inclure des mécanismes de sécurité offrant un niveau de sécurité très élevé grâce à l'utilisation de protocoles de chiffrement et d'authentification avancées qui protègent les données de tout accès non autorisé.

⊙ **Réductions des coûts :** les VPNs permettent aux entreprises d'utiliser un transport internet tiers et économique pour la connexion des bureaux et des utilisateurs distants au site principal, éliminant par conséquent le besoin de disposer de liaisons WAN. De plus, avec l'apparition de technologies économiques haut débit, telles que la technologie DSL, les entreprises peuvent utiliser les VPNs pour diminuer leurs coûts de connectivité tout en augmentant en même temps la bande passante de connexion à distance.

⊙ **Compatibilité avec la technologie haut débit :** les VPNs permettent aux travailleurs mobiles et aux télétravailleurs de bénéficier d'une connectivité haut débit rapide, comme la technologie DSL et le câble, pour accéder au réseau de leur entreprise. La connectivité haut débit offre flexibilité et efficacité. Les connexions haut débit rapides peuvent également être une solution rentable pour connecter des bureaux distants.

⊙ **Évolutivité :** les VPNs accordent aux entreprises d'utiliser l'infrastructure d'internet des FAI et des périphériques, ce qui permet d'ajouter facilement de nouveaux utilisateurs. Les grandes entreprises peuvent ajouter des volumes importants de capacité sans ajouter d'infrastructure importante.

3.2.4 Types de VPNs

Il existe deux types de réseaux privés :[21]

- VPN site à site ;
- VPN accès à distance.

- **VPN site à site**

  Un VPN site à site est créé lorsque les périphériques situés des deux côtés de la connexion VPN connaissent par avance la configuration VPN. Dans un VPN de site à site, les hôtes finaux envoient et reçoivent le trafic TCP/IP normal par l'intermédiaire d'une « passerelle » VPN. La passerelle VPN est responsable de l'encapsulation et du chiffrement de la totalité du trafic sortant issu d'un site spécifique. La passerelle VPN envoie ensuite ce trafic sur internet par le biais d'un tunnel VPN jusqu'à une passerelle VPN homologue au niveau du site cible. Lors de la réception, la passerelle VPN homologue élimine les en-têtes, déchiffre le contenu et relaie le paquet vers l'hôte cible au sein de son réseau privé.

  Un VPN site à site est une extension d'un réseau étendu classique. Les VPNs site à site

connectent entre eux des réseaux entiers. Ils peuvent par exemple connecter un réseau de filiale au réseau du siège d'une entreprise [21].

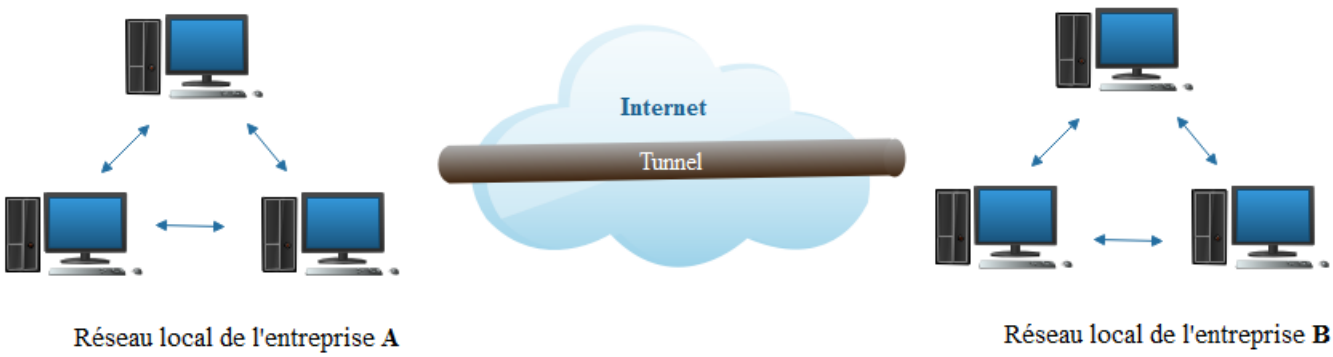


FIGURE 3.4 – VPN site à site [29]

- **VPN d'accès à distance**
  Un VPN d'accès à distance est utilisé pour la connexion d'hôtes individuels devant accéder en toute sécurité au réseau de leur entreprise via internet. Le VPN reste statique et les hôtes internes ne savent pas qu'un VPN existe. La connectivité internet utilisée par les télétravailleurs est généralement une connexion haut débit, DSL, sans fil ou par câble.

  Un VPN d'accès à distance est créé lorsque les informations sur le VPN ne sont pas configurées de manière statique, mais qu'elles permettent au contraire des modifications dynamiques. Ce VPN d'accès à distance peut également être activé et désactivé. Les VPNs d'accès à distance prennent en charge une architecture client-serveur, dans laquelle le client VPN (hôte distant) obtient un accès sécurisé au réseau de l'entreprise par l'intermédiaire d'un périphérique de serveur VPN à la périphérie du réseau [21].

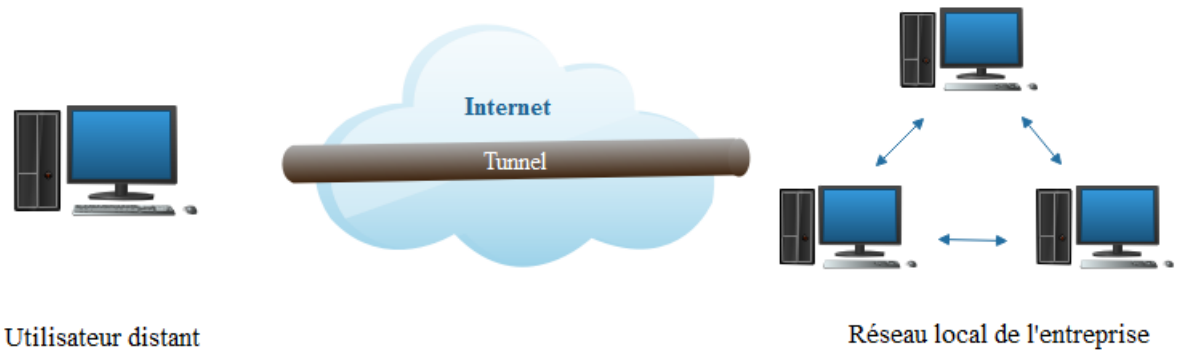


FIGURE 3.5 – VPN d'accès à distance [29]

3.2.5 Protocoles utilisés pour réaliser une connexion VPN

Il existe plusieurs protocoles dits de tunnellisation qui permettent la création des réseaux VPNs. Les technologies les plus utilisés pour la création de tunnels sécurisés pour tout type de flux sont GRE, PPP, PPTP, L2F, L2TP et IPSec.

3.2.5.1 Protocole GRE (Generic Routing Encapsulation)

Le protocole GRE est un exemple de protocole de tunneling VPN de site à site de base, non sécurisé. Le protocole GRE est un protocole de tunneling développé par Cisco est défini en tant que norme IETF (RFC 2784), capable d'encapsuler une large variété de types de paquets de protocoles au sein de tunnels IP. Le protocole GRE crée une liaison point à point vers des routeurs Cisco au niveau de points distants sur un inter-réseau IP.

Le protocole GRE est conçu pour gérer le transport du trafic multi-protocoles et multidiffusion IP entre deux ou plusieurs sites, qui peuvent ne posséder que de la connectivité IP. Il peut également encapsuler plusieurs types de paquets de protocoles au sein d'un tunnel IP [21].

3.2.5.2 Le protocole PPP (Point-To-Point Protocol)

Le Protocole point à point (PPP) fournit une méthode standard pour transporter les datagrammes multi-protocoles au-dessus des liens point par point. Le PPP est composé de trois composants principaux : [27]

1. Une méthode pour encapsuler les datagrammes multiprotocole.
2. Un Link Control Protocol (LCP) pour établir, configurer, et tester la connexion logique.
3. Une famille des protocoles de contrôle de réseau (NCP) pour établir et configurer différents protocoles de couche réseau.

3.2.5.3 Le Protocol PPTP (Point-to-Point Tunneling Protocol)

Définit par la RFC 2637, PPTP est un protocole de niveau 2 conçu par Microsoft qui permet des transferts sécurisés de données d'un client distant vers un serveur privé d'entreprise, il est une extension du protocole PPP.

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP (paquet, données encapsulées). PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation) pour les transmettre sur l'internet ou d'autres réseaux publics TCP/IP. PPTP peut aussi être utilisé en réseau privé site à site. Le protocole de tunnel point-à-point est maintenant obsolète [28][29][31].

3.2.5.4 Le protocole L2F (Layer Two Fowarding)

Le protocole L2F comme son nom l'indique est un protocole de niveau 2, développé par Cisco et décrit dans la RFC 2341.

Ce protocole permet à un serveur d'accès distant de véhiculer le trafic sur PPP, et de transférer ces données jusqu'à un serveur L2F. Ce serveur L2F désencapsule les paquets et les envoie sur le réseau. Comme PPTP, Il est désormais quasi-obsolète dans nos jours [28][30].

3.2.5.5 Le protocole L2TP (Layer 2 Tunneling Protocol)

Le protocole L2TP, définit par la RFC 2661 est issu de la convergence des protocoles PPTP et L2F. Il permet l'encapsulation des paquets PPP au niveau des couches 2 et 3 de modèle OSI. Lorsqu'il est configuré pour transporter les données sur IP, L2tp peut être utilisé pour faire du tunnelling sur internet. L2tp repose sur deux concepts : [29]

- Concentrateurs d'accès L2TP ;
- Serveur réseau L2tp.

3.2.5.6 Le protocole IPSec (Internet Protocol Security)

Le protocole IPsec est une norme IETF définit par la RFC 2401 qui décrit comment un VPN peut être configuré de manière sécurisée à l'aide d'internet Protocole (IP).

IPSec fonctionne au niveau de la couche réseau, en protégeant et en authentifiant les paquets IP entre les équipements IPSec participants (homologues). IPSec sécurise un chemin entre une paire de passerelles, une paire d'hôtes ou une passerelle et un hôte. En conséquence, le protocole IPSec peut en théorie protéger tout trafic d'application, car cette protection peut-être implémentée de la couche 4 à la couche 7 de modèle OSI.

IPSec est basé sur deux mécanismes le premier, AH, pour Authentification Header et Le second, ESP, pour Encapsulating Security Payload [21][29].

- **Le protocole AH (Authentication Header) :** AH est le protocole approprié à utiliser lorsque la confidentialité n'est pas requise. Comme son nom le laisse supposer, ce protocole va d'abord se préoccuper d'authentification, mais également d'assurer l'intégrité des données des paquets IP échangées. La totalité du texte est transmise en texte clair. Si le protocole AH est utilisé seul, sa protection est faible [18][21].
- **Le protocole ESP (Encapsulating Security Payload) :** ESP est un protocole de sécurité permettant la confidentialité et l'authentification grâce au chiffrement du paquet IP, ce chiffrement masque les données et l'identité de leur source et de leur destination. ESP authentifie le paquet IP interne et l'en-tête ESP. L'authentification permet d'identifier la source des données et de garantir leur intégrité. Bien que les fonctions de chiffrement et d'authentification soient facultatives dans ESP, vous devez en choisir au moins une [21].

(i) Implémentation IPSec

lors de la configuration d'une passerelle IPsec en vue de fournir des services de sécurité, un protocole IPsec doit être sélectionné. Les choix possibles sont des combinaisons des technologies ESP et AH. De manière réaliste, les options ESP ou ESP+AH sont presque toujours sélectionnées, car la méthode AH elle-même ne permet pas le chiffrement. Aussi La combinaison d'un groupe d'éléments constitutifs qui offre les options de confidentialité, d'intégrité et d'authentification des VPNs IPSec, comme le montre la figure suivante : [21]

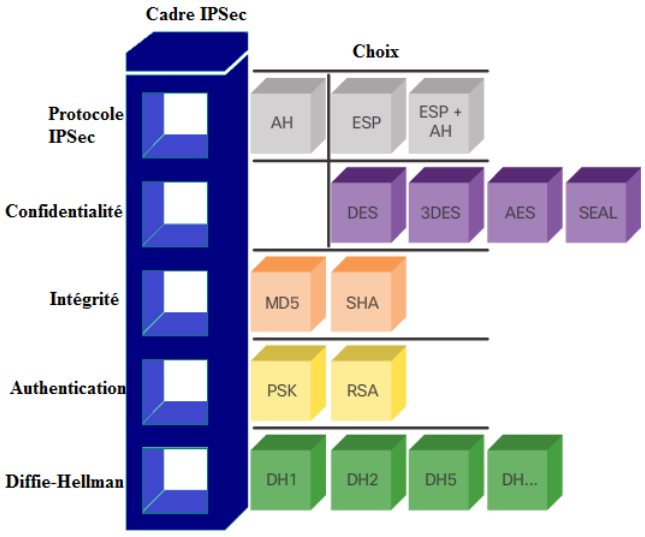


FIGURE 3.6 – Implémentation IPSec [21]

- **La confidentialité :** l'algorithme de chiffrement sélectionné doit de préférence correspondre au niveau de sécurité souhaitée : DES, 3DES ou AES. L'algorithme AES est fortement recommandé, avec AES-GCM pour une sécurité maximale.
- **Intégrité :** garantit que le contenu n'a pas été modifié lors du transit. Implémenté par le biais de l'utilisation d'algorithmes de hachage. Les choix possibles incluent les algorithmes MD5 et SHA.
- **Authentification :** représente la manière selon laquelle les périphériques sont authentifiés à chaque extrémité du tunnel VPN. Les deux méthodes sont PSK ou RSA.
- **Groupe d'algorithmes DH :** représente la manière selon laquelle une clé secrète partagée est établie entre des homologues. Diverses options sont possibles, mais l'algorithme DH24 est celui qui offre le plus de sécurité.

(ii) Mode de fonctionnement d'IPSec

Il existe deux modes d'utilisation d'IPSec : le mode transport et le mode tunnel.

- **Mode transport :** en mode transport, seules les données en provenance du protocole de niveau supérieur et transportées par le datagramme IP sont protégées. Ce mode n'est utilisable que sur des équipements terminaux, en effet en cas d'utilisation sur des équipements intermédiaires, on courrait le risque, suivant les aléas du routage, que le paquet atteigne sa destination finale sans avoir traversé la passerelle censée le déchiffrer [22][29].

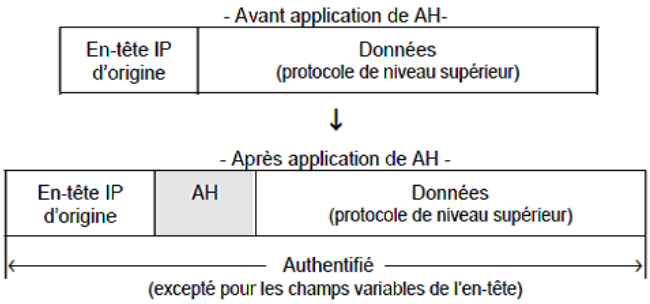


FIGURE 3.7 – Position de AH en mode transport [22]

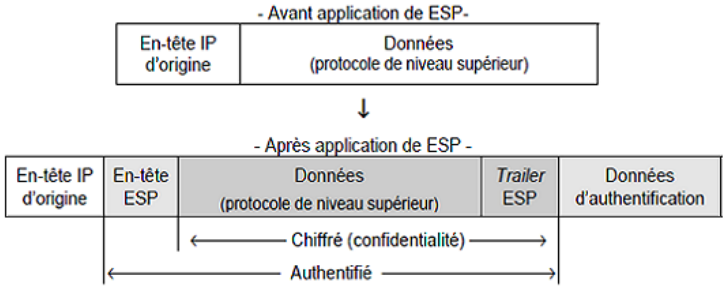


FIGURE 3.8 – Position de ESP en mode transport [22]

- **Mode tunnel :** en mode tunnel, l'en-tête IP est généralement protégé (authentification, intégrité et/ou confidentialité) et remplacé par un nouvel en-tête (encapsulation) qui sert à transporter le paquet jusqu'à la fin du tunnel, où l'en-tête original est rétabli (désencapsulation). Le mode tunnel est utilisé entre deux passerelles de sécurité. Ce mode permet d'assurer une protection plus importante contre l'analyse du trafic, car il masque les adresses de l'expéditeur et du destinataire final [22][29].

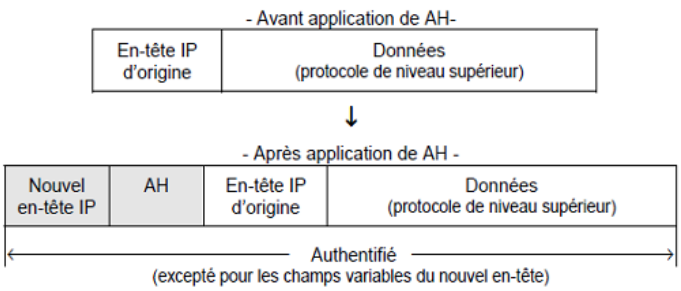


FIGURE 3.9 – Position de AH en mode tunnel [22]

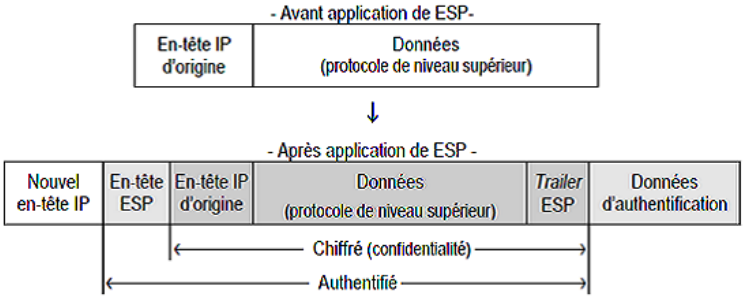


FIGURE 3.10 – Position de ESP en mode tunnel [22]

(iii) Détail du protocole

- **Gestion des flux IPSec :** les flux IPSec sont gérés unidirectionnellement. Ainsi, une communication bidirectionnelle entre deux machines utilisant IPSec sera définie par diverse processus pour chacun des sens de communication. Les procédés détaillés ci-dessous respectent tous deux cette loi [24].

  A) **Security Policy (SP) :** une SP défini ce qui doit être traité sur un flux. Comment nous voulons transformer un paquet [24].

  - Les adresses IP de l'émetteur et du récepteur (unicast, mulitcast ou broadcast) ;
  - 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).

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

  B) **Security Association (SA) :** une SA défini comment sera traité le paquet en fonction de sa SP associée. Elles ne sont que la réalisation des SP. Elle possède l'ensemble des propriétés de la liaison. Ainsi, elle sera représentée par une structure de données contenant les informations suivantes : [24]

  - Un compteur permettant de générer les numéros de séquence des entêtes AH et ESP.
  - Un flag (drapeau) permettant d'avertir qu'en cas de dépassement du compteur précédemment décrit, on doit interrompre la communication.
  - Une fenêtre d'anti répétition dans laquelle doit tomber le prochain numéro de séquence.
  - Information sur l'AH : algorithme d'authentification, clefs, durée de vie, etc.
  - Information sur l'ESP : algorithme d'authentification et de chiffrement, clefs, etc.
  - Mode IPSec : tunnel ou transport.
  - Durée de vie de la SA.
  - MTU.

    Une SA est identifiée à un seul et unique flux unidirectionnel grâce à trois champs :

  - L'adresse IP de destination (unicast, multicast ou broadcast) ;
  - Le protocole utilisé, AH ou ESP ;
  - Le SPI [1] (Security Parameter Index).

  C) **Base de données SPD et SAD :** tout système implémentant IPSec possède donc 2 bases de données distinctes dans lesquelles il stocke son SP (ici, SPDatabase) et son SA (ici, SADatabase) [24].

  - **La SPD (Security Policy Database) :** est la base de configuration d'IPSec. Elle permet de dire au noyau quel paquet IP doit traiter. C'est à sa charge de savoir avec quel SA fait-il le traitement.

1. **SPI :** est un indice (ou ID) sur 32 bits attribué au SA lors de sa création, sa génération dépendra du mode de gestion des clés de sessions. Il sert à distinguer les différentes SA qui aboutissent à une même destination et utilisant le même protocole.

- **La SAD (Security Association Database) :** stocke les SA afin de savoir comment traiter les paquets arrivant ou partant. Elles sont identifiées par les triplets :
  - Adresse de destination des paquets ;
  - Identifiant du protocole AH ou ESP utilisé ;
  - Un index des paramètres de sécurité (SPI) envoyé en clair dans les paquets.

(iv) Principe de fonctionnement d'IPSec

- **Trafic sortant :** lorsque la couche IPSec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPSec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises [29].
- **Trafic entrant :** lorsque la couche IPSec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPSec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité [29].

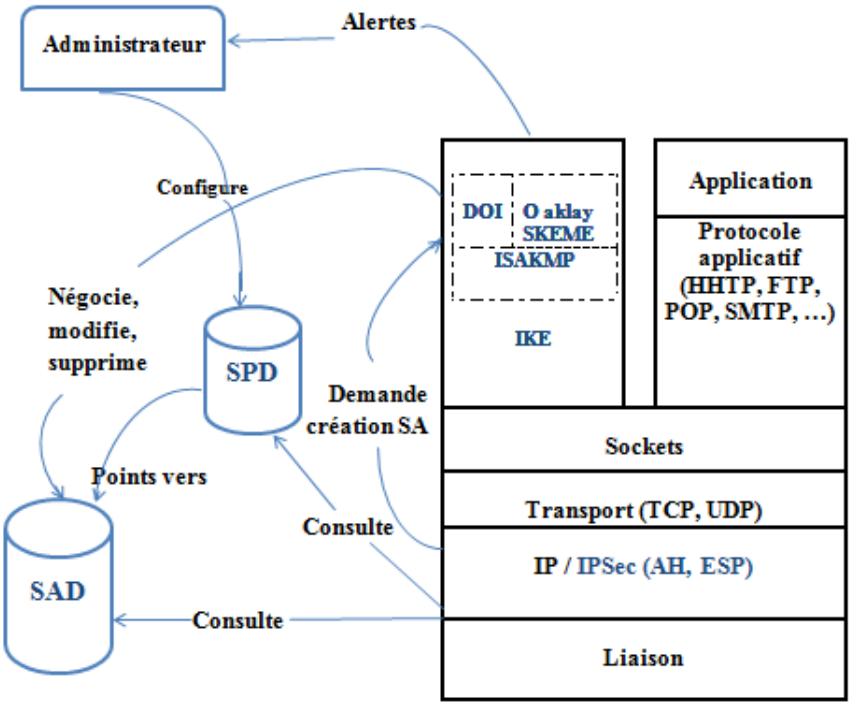


FIGURE 3.11 – Principe de fonctionnement d'IPSec [29]

(v) La gestion des clefs pour IPSec

Les services de protection offerts par IPSec s'appuient sur des algorithmes cryptographiques, et reposent donc sur des clefs qui sont : [29]

A) **ISAKMP (Internet Security Association and Key Management Protocol) : [29]**

Décrit dans la RFC 2408, il 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 clefs (et plus généralement des associations de sécurité). Il compte trois aspects principaux :

- Il définit une façon de procéder, en deux étapes appelées phase 1 et phase 2 : dans la première, un certain nombre de paramètres de sécurité propres à ISAKMP sont mis en place, afin d'établir entre les deux tiers un canal protégé, dans un second temps, ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et ESP).
- Il définit des formats de messages, par l'intermédiaire de blocs ayant chacun un rôle précis et permettant de former des messages clairs.
- Il présente un certain nombre d'échanges types, composés de tels messages, qui permettant des négociations présentant des propriétés différentes : protection ou non de l'identité, perfect forward secrecy...

B) **IKE (Internet Key Exchange) :**

IKE utilise ISAKMP, pour construire un protocole pratique. Il comprend les modes suivants : [29]

► **Phase 1 : Main Mode et Aggressive Mode**

Les attributs suivants sont utilisés par IKE et négociés durant la phase 1 : un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman.

Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs. Ces clefs dépendent des cookies, des aléas échangés et des valeurs publiques Diffie-Hellman ou du secret partagé préalable. Leur calcul fait intervenir la fonction de hachage choisit pour la SA ISAKMP et dépend du mode d'authentification choisi.

► **Phase 2 : Quick Mode**

Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1. L'authenticité des messages est assurée par l'ajout d'un bloc Hash après l'en-tête ISAKMP et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.

Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme IPSec. Chaque négociation aboutit en fait à deux SA, une dans chaque sens de la communication. Les échanges composant ce mode ont le rôle suivant :

- Négocier un ensemble de paramètres IPSec (paquets de SA).
- Échanger des nombres aléatoires, utilisés pour générer une nouvelle clef qui dérive de celle de la SA ISAKMP. De façon optionnelle, il est possible d'avoir recours à un nouvel échange Diffie-Hellman, afin d'accéder à la propriété de Perfect Forward Secrecy, qui n'est pas fournie si l'on se contente de générer une nouvelle clef à partir de l'ancienne et des aléas.
- Optionnellement, identifier le trafic que ce paquet de SA protégera, au moyen de sélecteurs (blocs optionnels IDi et IDr ; en leur absence, les adresses IP des interlocuteurs sont utilisées).

- **Les groupes : New Groupe Mode**

  Le groupe à utiliser pour Diffie-Hellman peut être négocié, par le biais de bloc SA, soit au cours du Main Mode, soit ultérieurement par le biais du New Group Mode. Dans les deux cas, il existe deux façons de désigner le groupe à utiliser :

  - Donner la référence d'un groupe prédéfini : il en existe actuellement quatre, les quatre groupes Oakley (deux groupes MODP et deux groupes EC2N).
  - Donner les caractéristiques du groupe souhaité : type de groupe (MODP, ECP, EC2N), nombre premier ou polynôme irréductible, générateurs...

- **Synthèse de la négociation IKE**

  Au final, le déroulement d'une négociation IKE suit le diagramme suivant :

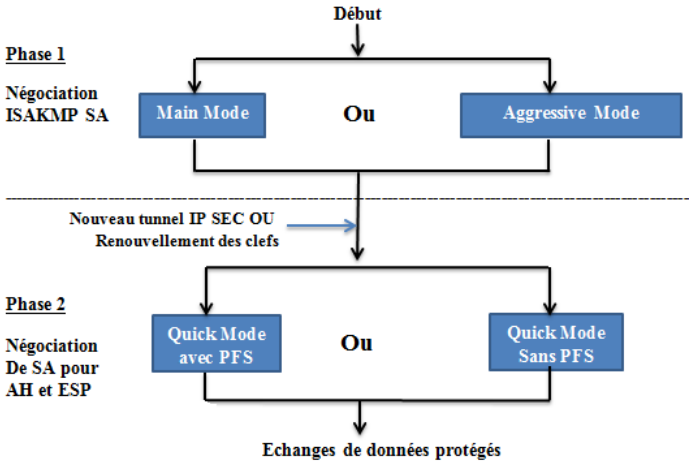


FIGURE 3.12 – Négociation IKE [29]

3.3 Solution messagerie

3.3.1 Introduction à la messagerie électronique

Les systèmes de messagerie électronique n'ont cessé d'évoluer depuis leur apparition. Permettant une communication sous format électronique dans des domaines restreints, ils sont désormais indispensables au sein des entreprises.

3.3.2 Définition de la messagerie électronique

La messagerie électronique, appelée aussi "electronic-mail" ou "E-mail" est l'outil le plus répandu dans l'internet des entreprises ou des particuliers. C'est un service gratuit qui est l'outil de base de la communication sur l'Internet privilégié entre des personnes distantes [32].

3.3.3 Avantage de la messagerie électronique

Les principaux avantages de la messagerie sont les suivants : [32]

- Rapidité de circulation des messages (temps réel).
- Possibilité d'envoyer un message même si le destinataire n'est pas connecté.
- Facilité d'utilisation.
- Gratuité pour les utilisateurs.

- La réduction de la mobilité au sein de l'entreprise ce qui permet ensuite un gain de temps.
- La messagerie fonctionne sur tous types de matériels, de réseaux...

3.3.4 Serveur de messagerie

Un serveur de messagerie a pour vocation de recevoir et d'envoyer le courrier électronique à travers le réseau. Un utilisateur n'est jamais en contact direct avec ce serveur, il utilise soit, logiciels de messagerie, soit un webmail, qui se charge de contacter le serveur pour envoyer ou recevoir les messages via internet.

3.3.5 Types de serveur de la messagerie électronique (Webmail)

3.3.5.1 Qmail server

Qmail est un serveur de messagerie électronique (Mail Transport Agent) pour Linux et autres dérivés d'Unix, il permet de mettre en place un service SMTP (Simple Mail Transfert Protocol) permettant l'envoi de courriels [35].

3.3.5.2 Microsoft Exchange server

Microsoft Exchange serveur est un logiciel de messagerie propriétaire de Microsoft, fréquemment utilisé par de grandes sociétés ainsi que dans le cloud. Ce logiciel a été conçu pour l'échange du courrier, la gestion des calendriers et des contacts. Toutes les informations sont stockées dans une base de données sur le serveur et sont accessibles à partir d'un grand nombre de systèmes clients : appareils mobiles, clients lourds Outlook, interface web, etc [36].

3.3.5.3 IBM Lotus Domino server

Domino est un serveur d'applications pour les clients Lotus Notes, mais peut aussi être accessible via un client web. Domino est un serveur de base de documents, il permet de gérer des données de tous types, mais structurer, il utilise pour cela des bases au format NSF [37].

3.3.5.4 Zimbra Collaboration Server

Zimbra Collaboration Server est un système de messagerie collaborative, permettant la gestion d'agendas et de contacts partagés, le stockage et l'édition de documents en ligne, ainsi que l'accès à une messagerie instantanée. Tous ces services sont accessibles au travers d'uneinterface web AJAX particulièrement moderne et agréable [38].

3.3.6 Les protocoles de communication (de transport)

Le fonctionnement du courrier électronique repose sur une série de protocoles de communication destinés à envoyer ses messages, de serveur à serveur, à travers l'Internet. Les principaux protocoles sont les suivants : SMTP, POP3 ou encore IMAP, chacun jouant un rôle bien précis.

3.3.6.1 SMTP (Simple Mail Transfer Protocol)

Définit par la RFC 821, le protocole SMTP est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point. Il s'agit d'un protocole fonctionnant en mode connecté, encapsulé dans une trame TCP/IP. Le courrier est remis directement au serveur de courrier du destinataire. Le protocole SMTP fonctionne grâce à des commandes textuelles envoyées au serveur SMTP (par défaut sur le port 25). SMTP définit le format des messages

comme la forme des adresses, les différents champs du courrier (FROM :, TO :, SUBJECT :, ...), ainsi que l'horodatage des mails [34].

3.3.6.2 POP3 (Post Office Protocol)

Définit par la RFC 1725, POP3 est un protocole qui va permettre à un client de messagerie de télécharger les messages d'un utilisateur situés sur un serveur de messagerie. Ce protocole est nécessaire pour les personnes qui ne sont pas connectées en permanence à internet afin de pouvoir consulter les mails reçus hors connexion. Le port dédié à POP3 est le numéro 110 [33] [34].

3.3.6.3 IMAP (Interactive Mail Access Protocol)

Ce protocole est très puissant, mais sa mise en place est assez délicate. Au contraire de POP qui n'offre qu'un accès exclusif à une boîte mail, IMAP est capable de gérer plusieurs boîtes simultanément avec des accès multiples. Le port dédié à l'IMAP est le numéro 143 [34].

3.3.7 Architecture du service de messagerie

Le service de messagerie est constitué de trois entités distinctes qui coopèrent et communiquent par le biais de protocoles bien défini afin d'assurer un service entre utilisateurs.

⊙ **MUA (Mail User Agent) :** est un programme qui permet à un client de lire, écrire un message électronique et de l'envoyer à l'agent de routage qui va l'injecter dans le système de messagerie via le protocole SMTP [33].

⊙ **MTA (Mail Transfer Agent) :** est un programme qui sert à transférer des messages électroniques entre des ordinateurs qui utilisent le protocole SMTP. Il est composé de deux agents : [33]

- Un agent de routage des messages ;
- Un agent de transport de messages.

⊙ **MDA (Mail Delivery Agent) :** c'est un programme utilisé par l'agent de transfert de Courriers ATC pour acheminer le courrier vers la boite aux lettres du destinataire spécifié. Il distribue le courrier dans les boîtes des utilisateurs spécifiés [33].

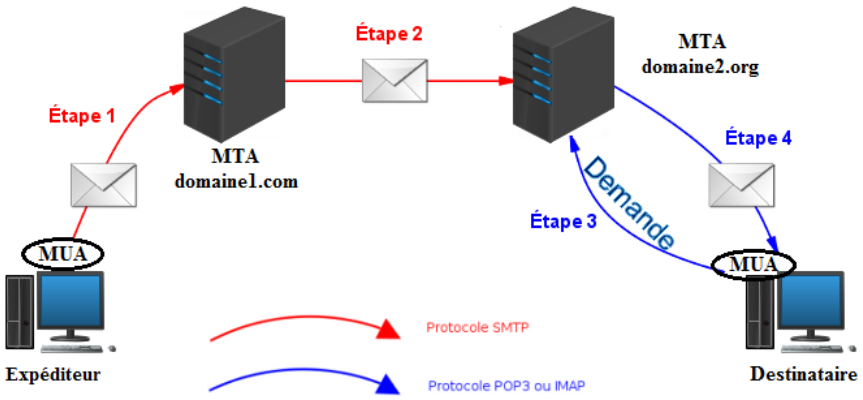


FIGURE 3.13 – Les quatre principales étapes du trajet d'un courrier électronique

3.3.8 Etude comparative des serveurs messagerie

Le tableau ci-dessous porte sur une étude comparative des différents serveurs de messagerie :

Serveur	Qmail	Exchange	Lotus Domino	Zimbra
Plate-forme d'installation	- Unix	- Windows	- Unix - Windows	- Unix
Fréquence d'utilisation en société	5 %	50 %	10 %	5 %
Fonctionnalités	- Synchronisation entre appareils (mobile, tablette, ordinateur). - Très modulable.	- Mail, Agenda, contact et tâches (synchroniser avec le mobile).	- Accessibilité depuis un mobile sous Windows phone ou une distribution Linux. Redondance au niveau de la messagerie automatiquement (service fournit à l'achat). - Extrêmement rapide.	- Accessibilité depuis un mobile grâce un logiciel qui se nomme « ZAS » qui permet une synchronisation en temps réel. - Le serveur est native pour les téléphones BlackBerry.
Prix	- Gratuit.	- Logiciel propriétaire pour 900€.	- 70€ par compte crée.	- Gratuit.
Sécurité	- Très sécurisé. - Réputé pour sa sécurité.	- Bonne sécurité car restreint a l'environnement Windows.	- Très sécurisé car d'origine il y a des modules installé dessus (cryptage).	- Très sécurisé car il utilise une solution externe (logiciel) pour la sécurité (Proofpoint).
LDAP ou AD (active directory)	- LDAP car sous UNIX.	- ADDS car spécifique à Windows.	- LDAP car fonctionne avec Linux mais ADDS car il peut très bien fonctionner sous Windows.	- LDAP car uniquement sous Linux.

Facilité d'administration	- En console donc faut connaître le Shell.	- Très simple car tous est expliqué (avec une assistance) et c'est graphique.	- Le plus simple car il est livré quasiment prêt, on juste à modifier quelques paramètres. En plus on est dans un environnement graphique.	- Compliqué car malgré l'environnement graphique le paramétrage reste complexe.

TABLE 3.1 – Tableau comparative des serveurs de messagerie

3.3.8.1 Explication de notre choix pour une messagerie Zimbra

À l'aide du tableau comparatif ci-dessus on peut remarquer que chaque serveur propose des services différents qui sont adaptés à certaines structures et à certains besoins bien précis. Cependant, notre choix s'est porté à Zimbra pour plusieurs raisons, d'abord, parce qu'il est très sécurisé, aussi, ses fonctionnalités répondent parfaitement à l'attente de l'entreprise, enfin, pour sa gratuité et son mode de développement ouvert.

3.4 Conclusion

Dans ce chapitre, nous avons effectué une présentation des réseaux locaux virtuels, des réseaux privés virtuels et de la messagerie ainsi les protocoles utilisés pour les réaliser. Le prochain chapitre va être consacré au côté pratique de la réalisation de notre travail.

Chapitre 4

Mise en œuvre des solutions retenues

Introduction

Après avoir étudié les solutions proposées du côté théorique, nous allons passer à la dernière étape qui est la réalisation. Dans ce chapitre, nous commencerons par une présentation de l'environnement de travail, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation de la nouvelle architecture.

4.1 Description de l'environnement de travail

4.1.1 Présentation de Packet Tracer

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc.

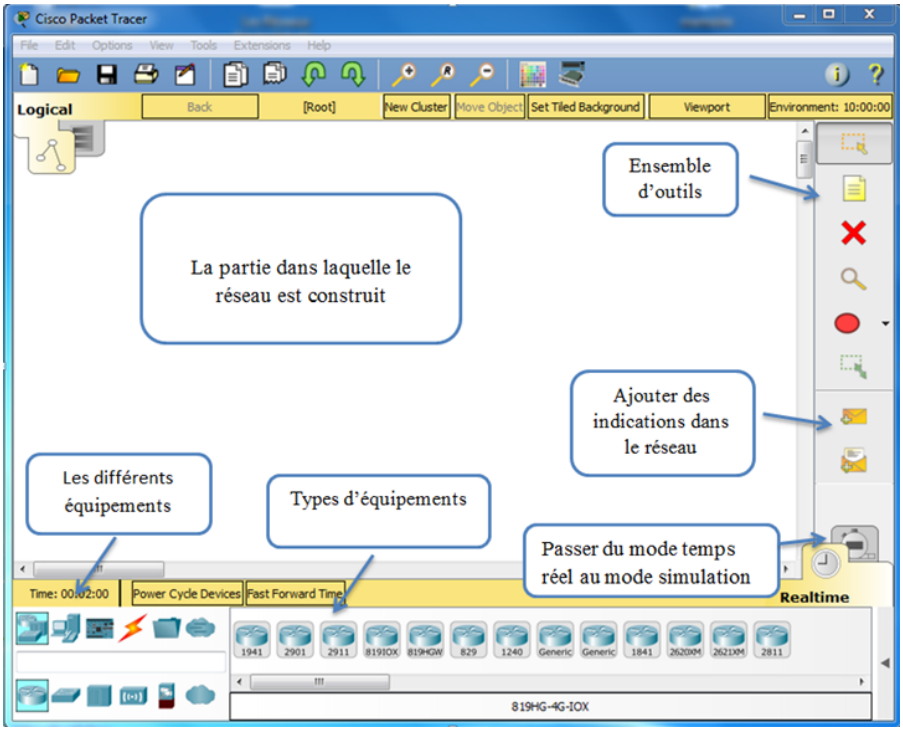


FIGURE 4.1 – Cisco Packet Tracer

4.1.2 Méthodes de configuration des équipements

Pour configurer les équipements, on utilise l'interface de ligne de commande (CLI), cette fenêtre peut être lancée avec un clic sur l'interface d'un routeur ou d'un commutateur (Figure 4.2).

La fenêtre CLI est l'interface de configuration des périphériques intermédiaires comme les commutateurs et les routeurs.

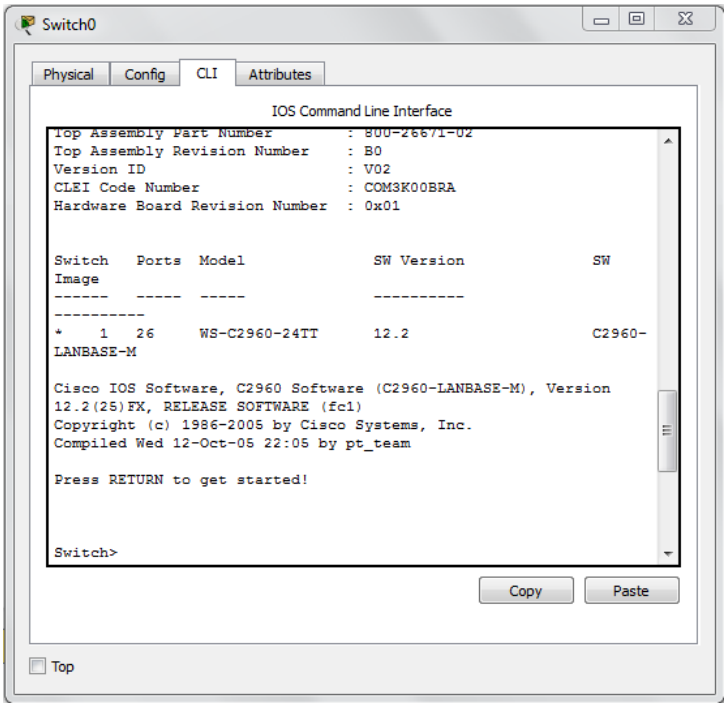


FIGURE 4.2 – Interface CLI

4.1.3 Présentation de GNS3

A) **Définition**

GNS3 (Graphical Network Simulator) est un logiciel utilisé pour reproduire différents systèmes d'exploitation réseau dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Internetwork Operating Systems) comme les routeurs, commutateurs. L'interface est graphique, elle est simple et agréable d'utilisation. Le fonctionnement se fait en mode drag and drop, on sélectionne un élément puis on « l'amène » dans la fenêtre principale du logiciel.

FIGURE 4.3 – Logo GNS3

Les principaux avantages de GNS3 est que l'on peut connecter le périphérique ou le réseau simulé au mode réel ainsi qu'à un périphérique réel, on peut aussi capturer les paquets transmis entre les appareils simulés dans GNS3 avec Wireshark [40].

B) **Les composants du logiciel**

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

- **Dynamips :** un émulateur d'image IOS provenant de Cisco Systems.
- **Dynagen :** une surcouche texte pour Dynamips.
- **Qemu :** émulateur générique et open source.
- **VirtualBox :** puissant logiciel de virtualisation de systèmes d'exploitation.
- **Wireshark :** est un analyseur de paquets, son but est de réaliser des captures de trames fournissant des informations sur des protocoles réseaux et dévoilant des failles de sécurité voir de localiser des pertes de performances sur le réseau.

4.1.4 Présentation de CentOS

CentOS est une distribution GNU/Linux principalement destinée aux serveurs. Tous ses paquets, à l'exception du logo, sont des paquets compilés à partir des sources de la distribution Linux Red Hat [1] Enterprise. Elle est donc semblable et compatible. C'est un système d'exploitation communautaire, qui est le résultat d'un groupe de contributeurs open source et d'utilisateurs qui travaillent ensemble pour développer des solutions Linux qui sont disponibles gratuitement pour les utilisateurs [39].

Figure 4.4 – Logo CentOS

4.2 Solution VLAN

4.2.1 Configuration des VLANs

Avant de commencer la configuration des VLANs, on va d'abord créer la table d'adressage correspondante.

Le tableau suivant représente les différentes informations relatives aux sous-réseaux associés aux VLANs de GRE de Béjaïa dont l'adresse de sous-réseau initial est 10.6.100.0/24. Ainsi que les différentes plages d'adressage réservées :

1. **Red Hat :** c'est le premier fournisseur mondial de solutions logicielles Open Source : technologies fiables et performantes de cloud, virtualisation, stockage, middleware et Linux.

La plage d'adresses	Masque sous-réseau	ID VLAN	Nom de VLAN	Adresses machines	Passerelle par default
10.6.100.0 (adresse sous-réseau) à 10.6.100.31 (adresse diffusion)	255.255.255.224	10	Suivi-risque	10.6.100.1 à 10.6.100.30	10.6.100.30
10.6.100.32 (adresse sous-réseau) à 10.6.100.63 (adresse diffusion)	255.255.255.224	20	Cellule-juridique	10.6.100.33 à 10.6.100.62	10.6.100.62
10.6.100.64 (adresse sous-réseau) à 10.6.100.127 (adresse diffusion)	255.255.255.192	30	Dpt-Administratif-Comptabilite	10.6.100.65 à 10.6.100.126	10.6.100.126
10.6.100.128 (adresse sous-réseau)				10.6.100.129	

à 10.6.100.159 (adresse diffusion)	255.255.255.224	40	Dpt-Exploitation	à 10.6.100.158	10.6.100.158
10.6.100.160 (adresse sous-réseau) à 10.6.100.191 (adresse diffusion)	255.255.255.224	50	Dpt-Informatique	10.6.100.161 à 10.6.100.190	10.6.100.190
10.6.100.192 (adresse sous-réseau) à 10.6.100.199 (adresse diffusion)	255.255.255.248	60	Directeur-Secretariat	10.6.100.193 à 10.6.100.198	10.6.100.198
10.6.100.200 (adresse sous-réseau) à 10.6.100.207 (adresse diffusion)	255.255.255.248	70	Serveurs	10.6.100.201 à 10.6.100.206	10.6.100.206

TABLE 4.1 – Table d'adressage des VLANs

4.2.2 Configuration du commutateur

Pour le configurer, nous utilisons la fenêtre CLI.

A) Configuration de base

- **Passage en mode privilégie, puis en mode de configuration global**

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

- **Configuration du mot de passe pour le mode privilégie et de hostname**

```
Switch(config)#enable secret class
Switch(config)#hostname SW-GRE
SW-GRE(config)#
```

- **Configuration de ligne console et les lignes vty**

```
SW-GRE(config-line)#password cisco
SW-GRE(config-line)#login
SW-GRE(config-line)#line vty 0 15
SW-GRE(config-line)#password cisco
SW-GRE(config-line)#login
```

- **Chiffrement de tous les mots de passe en clair**

```
SW-GRE(config)#service password-encryption
SW-GRE(config)#
```

B) Création des VLANs sur le commutateur SW-GRE

- **Création des differents VLANs**

```
SW-GRE#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW-GRE(vlan)#vlan 10 name Suivi-risque
VLAN 10 added:
    Name: Suivi-risque
SW-GRE(vlan)#vlan 20 name Cellule-juridique
VLAN 20 added:
    Name: Cellule-juridique
SW-GRE(vlan)#vlan 30 name Dpt-Administratif-Comptabilite
VLAN 30 added:
    Name: Dpt-Administratif-Comptabilite
SW-GRE(vlan)#vlan 40 name Dpt-Exploitation
VLAN 40 added:
    Name: Dpt-Exploitation
SW-GRE(vlan)#vlan 50 name Dpt-Informatique
VLAN 50 added:
    Name: Dpt-Informatique
SW-GRE(vlan)#vlan 60 name Directeur-Secretariat
VLAN 60 added:
    Name: Directeur-Secretariat
SW-GRE(vlan)#vlan 70 name Serveurs
VLAN 70 added:
    Name: Serveurs
SW-GRE(vlan)#
```

- **Vérification de la création des VLANs**

```
SW-GRE#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Suivi-risque                     active
20   Cellule-juridique                active
30   Dpt-Administratif-Comptabilite   active
40   Dpt-Exploitation                 active
50   Dpt-Informatique                 active
60   Directeur-Secretariat            active
70   Serveurs                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-GRE#
```

À l'aide de la commande **show vlan brief**, nous pouvons vérifier que les différents VLANs ont été créés.

C) **Attribution des ports (interfaces) du commutateur (SW-GRE) aux VLANs**

```
SW-GRE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-GRE(config)#interface range fastethernet 0/1 - 3
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 10
SW-GRE(config-if-range)#exit
SW-GRE(config)#interface range fastethernet 0/4 - 6
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 20
SW-GRE(config-if-range)#exit
SW-GRE(config)#interface range fastethernet 0/7 - 10
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 30
SW-GRE(config-if-range)#exit
SW-GRE(config)#interface range fastethernet 0/11 - 13
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 40
SW-GRE(config-if-range)#exit
SW-GRE(config)#interface range fastethernet 0/14 - 16
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 50
SW-GRE(config-if-range)#exit
SW-GRE(config)#interface range fastethernet 0/17 - 18
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 60
SW-GRE(config-if-range)#exit
SW-GRE(config)#interface range fastethernet 0/19 - 21
SW-GRE(config-if-range)#switchport mode access
SW-GRE(config-if-range)#switchport access vlan 70
SW-GRE(config-if-range)#exit
SW-GRE(config)#end
SW-GRE#
```

- **Vérification que tous les VLANs sont affectés aux différents ports du commutateur (SW-GRE)**

```
SW-GRE#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   Suivi-risque                     active    Fa0/1, Fa0/2, Fa0/3
20   Cellule-juridique                active    Fa0/4, Fa0/5, Fa0/6
30   Dpt-Administratif-Comptabilite   active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
40   Dpt-Exploitation                 active    Fa0/11, Fa0/12, Fa0/13
50   Dpt-Informatique                 active    Fa0/14, Fa0/15, Fa0/16
60   Directeur-Secretariat            active    Fa0/17, Fa0/18
70   Serveurs                         active    Fa0/19, Fa0/20, Fa0/21
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-GRE#
```

D) **Configuration du trunk du commutateur (SW-GRE)**

- **Activation du mode trunk**

```
SW-GRE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-GRE(config)#interface gigabitEthernet 0/1
SW-GRE(config-if)#switchport mode trunk
SW-GRE(config-if)#
```

GigabitEthernet 0/1 est l'interface de liaison vers le routeur (GRE-Bejaia).

- **Vérification que le trunk est opérationnel**

```
SW-GRE#show interface gigabitEthernet 0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

SW-GRE#
```

4.2.3 Configuration du routeur

A) **Routage inter-vlan au moyen de sous-interfaces**

- **Il s'agit ici de créer des sous interfaces virtuelles et de les adresser et d'ensuite permettre qu'elles communiquent**

```
GRE-Bejaia#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GRE-Bejaia(config)#interface gigabitEthernet 0/0.10
GRE-Bejaia(config-subif)#encapsulation dot1Q 10
GRE-Bejaia(config-subif)#ip address 10.6.100.30 255.255.255.224
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.20
GRE-Bejaia(config-subif)#encapsulation dot1Q 20
GRE-Bejaia(config-subif)#ip address 10.6.100.62 255.255.255.224
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.30
GRE-Bejaia(config-subif)#encapsulation dot1Q 30
GRE-Bejaia(config-subif)#ip address 10.6.100.126 255.255.255.192
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.40
GRE-Bejaia(config-subif)#encapsulation dot1Q 40
GRE-Bejaia(config-subif)#ip address 10.6.100.158 255.255.255.224
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.50
GRE-Bejaia(config-subif)#encapsulation dot1Q 50
GRE-Bejaia(config-subif)#ip address 10.6.100.190 255.255.255.224
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.60
GRE-Bejaia(config-subif)#encapsulation dot1Q 60
GRE-Bejaia(config-subif)#ip address 10.6.100.198 255.255.255.248
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.70
GRE-Bejaia(config-subif)#encapsulation dot1Q 70
GRE-Bejaia(config-subif)#ip address 10.6.100.206 255.255.255.248
GRE-Bejaia(config-subif)#no shutdown
GRE-Bejaia(config-subif)#exit
GRE-Bejaia(config)#end
GRE-Bejaia#
```

- **Vérification**

```
GRE-Bejaia#show ip route connected
C    10.6.100.0/27  is directly connected, GigabitEthernet0/0.10
C    10.6.100.32/27  is directly connected, GigabitEthernet0/0.20
C    10.6.100.64/26  is directly connected, GigabitEthernet0/0.30
C    10.6.100.128/27  is directly connected, GigabitEthernet0/0.40
C    10.6.100.160/27  is directly connected, GigabitEthernet0/0.50
C    10.6.100.192/29  is directly connected, GigabitEthernet0/0.60
C    10.6.100.200/29  is directly connected, GigabitEthernet0/0.70
C    42.100.100.0/24  is directly connected, Serial0/0/0

GRE-Bejaia#
```

À l'aide de la commande **show ip route connected**, nous pouvons vérifier que les différentes interfaces virtuelles ont été créées et connectées aux adresses respectives.

B) **Configuration des ACLs**

- **Il s'agit ici d'utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs**

```
GRE-Bejaia#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GRE-Bejaia(config)#ip access-list standard vlan-10
GRE-Bejaia(config-std-nacl)#deny 10.6.100.62 0.0.0.31
GRE-Bejaia(config-std-nacl)#deny 10.6.100.126 0.0.0.63
GRE-Bejaia(config-std-nacl)#deny 10.6.100.198 0.0.0.7
GRE-Bejaia(config-std-nacl)#deny 10.6.100.158 0.0.0.31
GRE-Bejaia(config-std-nacl)#permit any
GRE-Bejaia(config-std-nacl)#exit
GRE-Bejaia(config)#interface gigabitEthernet 0/0.10
GRE-Bejaia(config-subif)#ip access-group vlan-10 out
GRE-Bejaia(config-subif)#end
GRE-Bejaia#
```

- **Vérification que les ACLs sont créés**

```
GRE-Bejaia#show access-lists
Extended IP access list vpn-acl
    10 permit ip 10.6.100.0 0.0.0.255 10.6.2.0 0.0.0.255 (1 match(es))
Standard IP access list vlan-10
    10 deny 10.6.100.32 0.0.0.31
    20 deny 10.6.100.64 0.0.0.63
    30 deny 10.6.100.192 0.0.0.7
    40 deny 10.6.100.128 0.0.0.31
    50 permit any (1 match(es))
Standard IP access list vlan-20
    10 deny 10.6.100.0 0.0.0.31
    20 deny 10.6.100.64 0.0.0.63
    30 deny 10.6.100.192 0.0.0.7
    40 deny 10.6.100.128 0.0.0.31
    50 permit any (2 match(es))
Standard IP access list vlan-30
    10 deny 10.6.100.192 0.0.0.7
    20 deny 10.6.100.128 0.0.0.31
    30 permit any (2 match(es))
Standard IP access list vlan-60
    10 deny 10.6.100.0 0.0.0.31
    20 deny 10.6.100.32 0.0.0.31
    30 deny 10.6.100.64 0.0.0.63
    40 deny 10.6.100.128 0.0.0.31
    50 permit any (1 match(es))
Standard IP access list vlan-40
    10 deny 10.6.100.0 0.0.0.31
    20 deny 10.6.100.32 0.0.0.31
    30 deny 10.6.100.64 0.0.0.63
    40 deny 10.6.100.192 0.0.0.7
    50 permit 10.6.100.200 0.0.0.7
    60 permit 10.6.100.160 0.0.0.31
```

À l'aide de la commande **show access-lists**, nous pouvons vérifier que les différents ACLs sont effectivement créés.

4.2.4 Démonstration

- **Vérification de la connectivité entre le VLAN 10 (Suivi-risque) et le VLAN 70 (Serveurs)**

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.6.100.201

Pinging 10.6.100.201 with 32 bytes of data:

Reply from 10.6.100.201: bytes=32 time=12ms TTL=127
Reply from 10.6.100.201: bytes=32 time=14ms TTL=127
Reply from 10.6.100.201: bytes=32 time=13ms TTL=127
Reply from 10.6.100.201: bytes=32 time=12ms TTL=127

Ping statistics for 10.6.100.201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 14ms, Average = 12ms
```

Test réussi entre la machine serveur de sécurité du VLAN 70 (Serveurs) pingué par la machine PC3 (10.6.100.3) du VLAN 10 (Suivi-risque).

Les trois serveurs qui sont serveur de sécurité, serveur d'exploitation et serveur de messagerie, sont accessibles par tous les VLANs.

- **Vérification de la non-connectivité entre le VLAN 10 (Suivi-risque) et le VLAN 20 (Cellule-juridique)**

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.6.100.33

Pinging 10.6.100.33 with 32 bytes of data:

Reply from 10.6.100.30: Destination host unreachable.
Reply from 10.6.100.30: Destination host unreachable.
Reply from 10.6.100.30: Destination host unreachable.
Reply from 10.6.100.30: Destination host unreachable.

Ping statistics for 10.6.100.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

La communication est bloqué entre les deux VLANs.

4.3 Solution VPN

4.3.1 Exigences de VPN IPSec

Pour mettre en œuvre le VPN, il faut diviser le travail en deux étapes qui sont nécessaires pour obtenir le tunnel VPN IPSec. Ces étapes sont les suivantes :

(i) Configuration ISAKMP (phase 1 ISAKMP).

(ii) Configuration IPSec (phase 2 ISAKMP, ACL, crypto map).

(i) Configuration ISAKMP (phase 1 ISAKMP)

IKE n'existe que pour établir une SA pour IPSec. Il doit d'abord négocier cette SA (une SA ISAKMP) : les relations avec les routeurs des sites distants.
À présent, nous allons commencer à travailler sur le site de GRE de Béjaïa / routeur (GRE-Bejaia).

- **La première étape consiste à configurer la politique de sécurité ISAKMP**

```
GRE-Bejaia(config)#crypto isakmp policy 10
GRE-Bejaia(config-isakmp)#encryption AES 256
GRE-Bejaia(config-isakmp)#hash SHA
GRE-Bejaia(config-isakmp)#authentication pre-share
GRE-Bejaia(config-isakmp)#group 5
GRE-Bejaia(config-isakmp)#lifetime 200
GRE-Bejaia(config-isakmp)#exit
GRE-Bejaia(config)#
```

Description des commandes ci-dessus :

- AES : est un procédé de cryptage utilisé pour la phase 1.

- SHA : l'algorithme de hachage.

- Pre-share : utilisation d'une clé pré-partagée comme méthode d'authentification.

- Group : l'algorithme d'échange de clef Diffie-Hellman est utilisé.

- Lifetime : spécifie le temps de validité de la connexion avant une nouvelle négociation des clefs. Elle est exprimée en secondes.

- **Maintenant, il faut définir une clé pré partagée pour l'authentification des homologues (GRE-Bejaia et Agence-AKBOU) à l'aide de la commande suivante :**

```
GRE-Bejaia(config)#crypto isakmp key vpn-key address 42.100.101.1
GRE-Bejaia(config)#
```

À chaque fois que GRE-Bejaia tentera d'établir un tunnel VPN avec Agence-Akbou, cette clé partagée (vpn-key) sera utilisée.

(ii) Configuration IPSec (phase 2 ISAKMP, ACL, crypto map)

Pour configurer le protocole IPSec on a besoin de configurer les éléments suivants :

- Créer le Transform-set.
- Créer une ACL étendue.
- Créer la carte de chiffrement.
- Appliquer crypto map à l'interface publique.

- **Cette étape consiste à créer la transformation définie, utilisée pour protéger les données (IPSec) nommé « vpn-trans-set». ESP-AES définie l'algorithme de cryptage et SHA l'algorithme de hachage.**

```
GRE-Bejaia(config)#$c transform-set vpn-trans-set esp-aes 256 esp-sha-hmac
GRE-Bejaia(cfg-crypto-trans)#exit
GRE-Bejaia(config)#
```

- **L'ACL étendu que l'on crée nommé « vpn-acl » permettra de définir le trafic qui passera à travers le tunnel VPN. Dans notre projet, le trafic s'achemine du réseau 10.6.100.0/24 à 10.6.2.0/24.**

```
GRE-Bejaia(config)#ip access-list extended vpn-acl
GRE-Bejaia(config-ext-nacl)#permit ip 10.6.100.0 0.0.0.255 10.6.2.0 0.0.0.255
GRE-Bejaia(config-ext-nacl)#exit
GRE-Bejaia(config)#
```

- **La carte de chiffrement nommé « vpn-crypto-map » est la dernière étape d'installation et d'établissement du lien entre ISAKMP définie précédemment et la configuration IPSEC :**

```
GRE-Bejaia(config)#crypto map vpn-crypto-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
GRE-Bejaia(config-crypto-map)#description VPN connection a l'agence d'Akbou
GRE-Bejaia(config-crypto-map)#set peer 42.100.101.1
GRE-Bejaia(config-crypto-map)#match address vpn-acl
GRE-Bejaia(config-crypto-map)#set transform-set vpn-trans-set
GRE-Bejaia(config-crypto-map)#exit
GRE-Bejaia(config)#
```

- **Maintenant, il suffit d'appliquer la carte de chiffrement (vpn-crypto-map) sur l'interface de sortie de routeur :**

```
GRE-Bejaia(config)#interface Serial 1/0
GRE-Bejaia(config-if)#crypto map vpn-crypto-map
```

Dès que nous appliquons crypto map sur l'interface, nous recevons un message de routeur qui confirme ISAKMP : ISAKMP is ON.

```
*Jun  8 12:45:06.279: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
GRE-Bejaia(config-if)#
```

À ce stade, nous avons terminé la configuration VPN IPSec sur le premier Site. Les paramètres pour Agence-AKBOU sont identiques, la seule différence étant les adresses IP attribuées et les listes d'accès.

4.3.2 Démonstration

- **Vérification de la connectivité entre GRE-Bejaia et Agence-Bejaia**

```
GRE-Bejaia#ping 10.6.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/60/64 ms
GRE-Bejaia#
```

- **Vérifions les informations retournées par le VPN sur le GRE-Bejaia**

```
GRE-Bejaia#show crypto IPSec transform-set
Transform set vpn-trans-set: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },


GRE-Bejaia#
```

La commande **show crypto IPSec transform-set** nous a permis de savoir quel mode utilisé, dans notre cas c'est le mode tunnel.

- **La vérification de la MAP VPN**

```
GRE-Bejaia#show crypto map
Crypto Map "vpn-crypto-map" 10 ipsec-isakmp
        Description: VPN connection a l'agence d'Akbou
        Peer = 42.100.101.1
        Extended IP access list vpn-acl
            access-list vpn-acl permit ip 10.6.100.0 0.0.0.255 10.6.2.0 0.0.0.255
        Current peer: 42.100.101.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                vpn-trans-set,
        }
        Interfaces using crypto map vpn-crypto-map:
                Serial1/0

GRE-Bejaia#
```

L'exécution de la commande **show crypto map** permet d'afficher l'adresse IP de destination et l'interface de sortie qui est activée.

- **On vérifie les opérations d'IPsec**

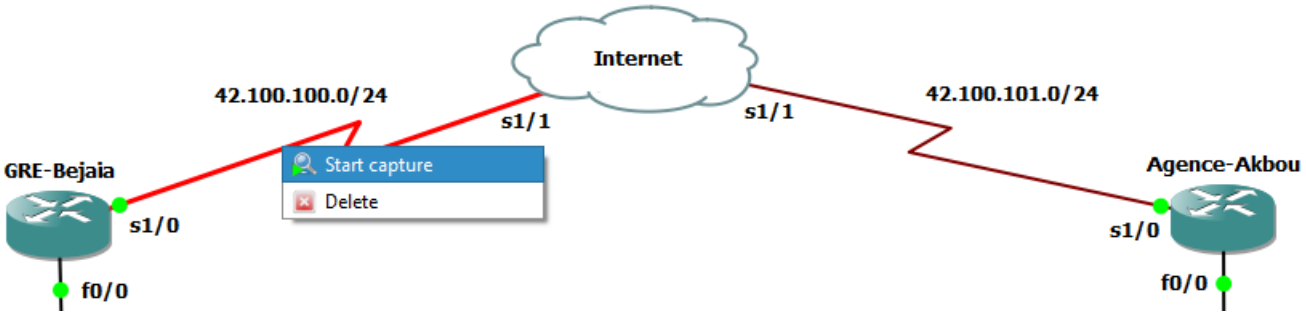
```
GRE-Bejaia#show crypto ipsec sa

interface: Serial1/0
    Crypto map tag: vpn-crypto-map, local addr 42.100.100.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.6.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.6.2.0/255.255.255.0/0/0)
   current_peer 42.100.101.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 42.100.100.1, remote crypto endpt.: 42.100.101.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
     current outbound spi: 0xB9692BF7(3110677495)

     inbound esp sas:
      spi: 0xC77CCC4F(3346844751)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: vpn-crypto-map
        sa timing: remaining key lifetime (k/sec): (4575393/3574)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB9692BF7(3110677495)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: vpn-crypto-map
        sa timing: remaining key lifetime (k/sec): (4575393/3561)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
GRE-Bejaia#
GRE-Bejaia#
```

L'exécution de la commande **show crypto IPSec** permet d'afficher l'interface de sortie (42.100.100.1) et l'interface d'entrée (42.100.101.1), les ACLs qui autorisent l'accès entre GRE-Bejaia et Agence-Bejaia avec le masque et le numéro de port, le nombre de paquets envoyés et reçus sont égaux et le mécanisme utilisé est ESP.

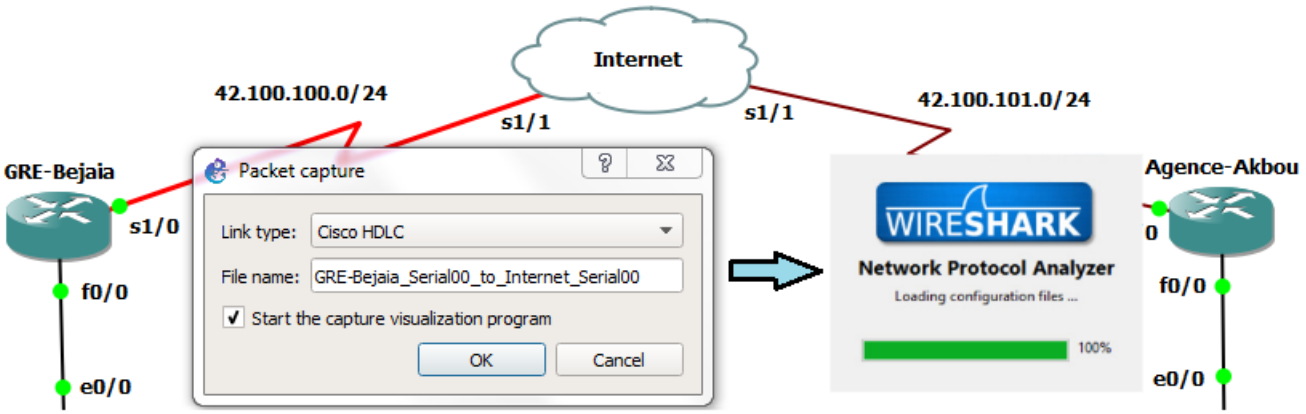
- **Pour finir, on vérifie les opérations d'isakmp**

```
GRE-Bejaia#show crypto isakmp sa
dst             src             state          conn-id slot status
42.100.101.1    42.100.100.1    QM_IDLE              1    0 ACTIVE

GRE-Bejaia#
```

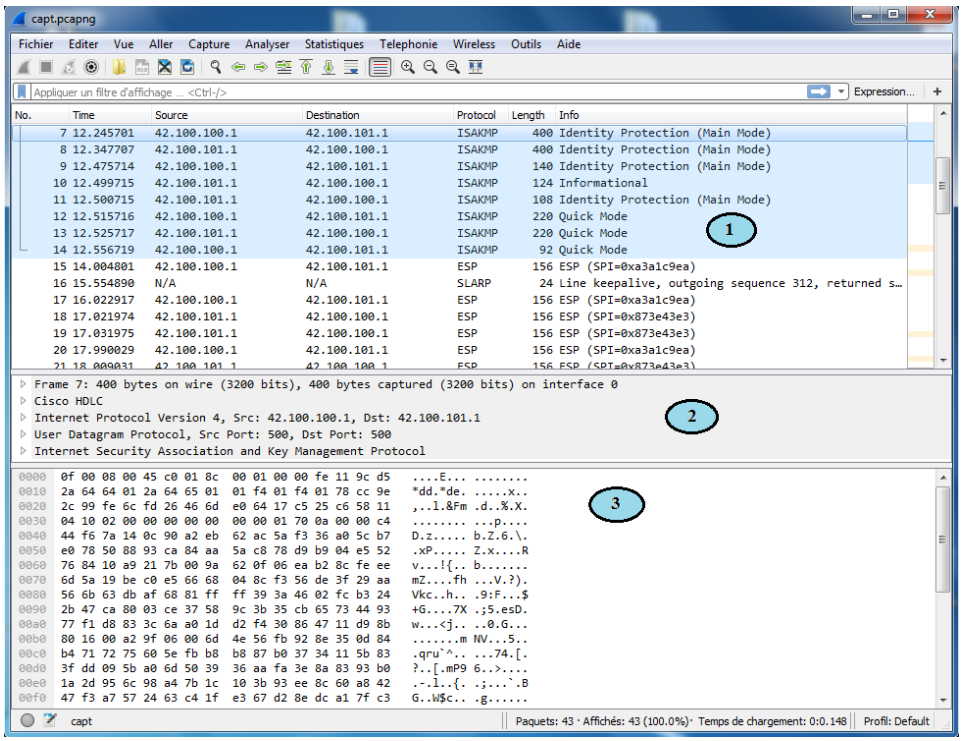
Pour mieux voir ce qui se passe sur notre architecture. On a refait une partie de notre topologie sous GNS3 qui offre la possibilité de capturer le trafic entre les homologues (GRE-Bejaia et Agence-Akbou) à l'aide de wireshark, pour cela on fait un clic droit sur le lien que nous voulons analyser et cliquer sur "Start capturing" voir la figure ci-dessous :



Nous devons ensuite choisir dans la liste proposée, l'interface que nous souhaitons analyser. Une fois choisie, dans la partie "Capture" de GNS3 apparaît notre première capture, on fait un clic droit dessus pour lancer wireshark, on peut ainsi analyser le trafic sur cette interface :



Les données passent à travers le tunnel VPN IPSec précédemment crée et elles sont cryptées :



- **Le volet 1 :** permet de recenser l'ensemble des paquets capturés. En spécifiant l'émetteur de la trame, le destinataire de la trame et le protocole réseau mis en œuvre.
- **Le volet 2 :** permet de visualiser la pile des protocoles employés dans la trame sélectionnée dans le premier volet.
- **Le volet 3 :** permet de visualiser l'ensemble du paquet capturé au format hexadécimal et la traduction ASCHII correspondante.

Protocole ISAKMP en phase 1

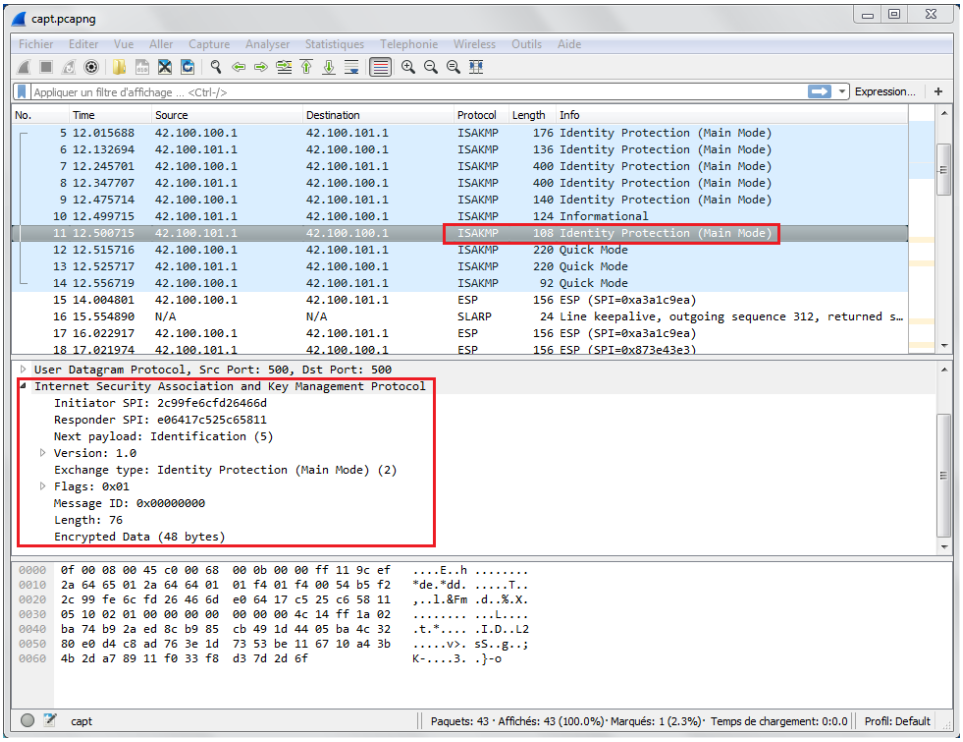


FIGURE 4.5 – Protocole ISAKMP en phase 1

Protocole ISAKMP en phase 2

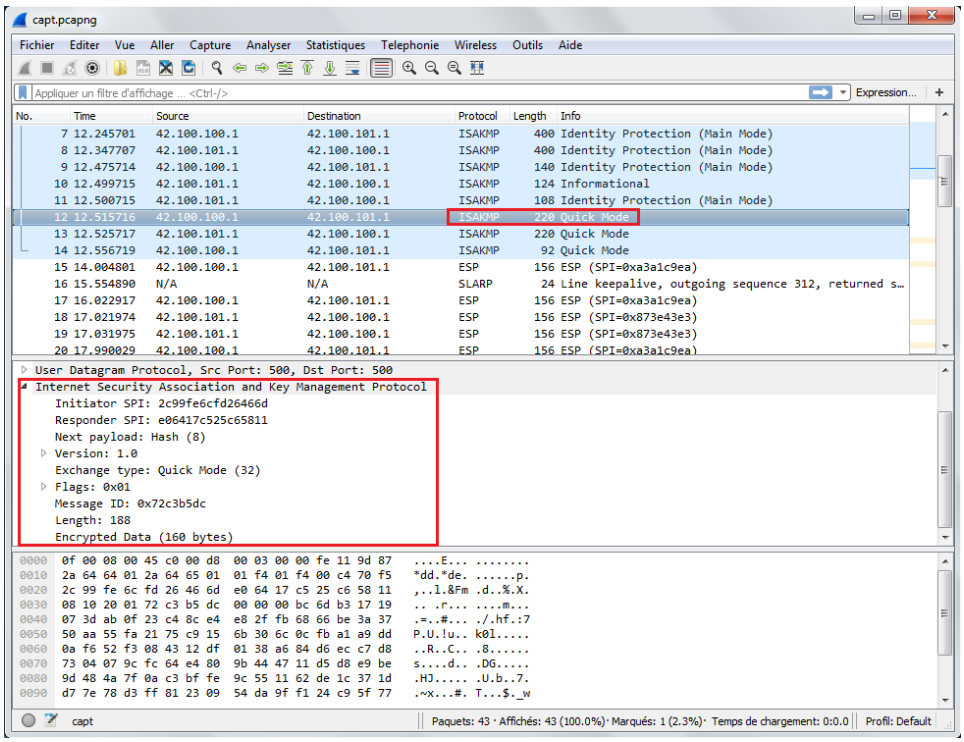


FIGURE 4.6 – Protocole ISAKMP en phase 2

Les messages échangés durant la phase 2 (Quick mode) sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase1 (main mode). L'authenticité des messages est assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP, et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.

4.4 Solution messagerie

4.4.1 Exigence de serveur messagerie

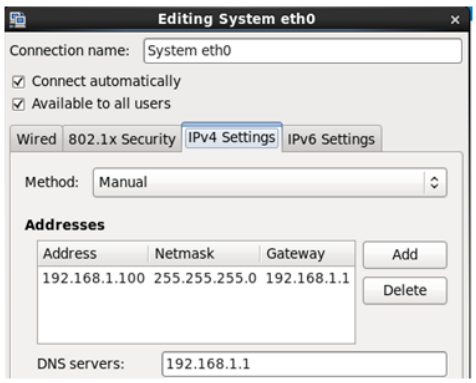
L'installation et la configuration du serveur vont se dérouler en deux grandes phases qui sont :

(i) Installation et configuration du serveur DNS.

(ii) Installation et configuration de Zimbra 8.7.7.

(i) Installation et Configuration du serveur DNS

- **Préparation de Notre Linux serveur (CentOS 6.9)**



Après avoir installé notre CentOS 6.9 qui est supporté par Zimbra, on va se rendre dans la configuration des interfaces réseau, en clic sur 'edit network ' puis 'network connexion' puis on change notre interface « eth0 » type de connexion IPV4 de automatic DHPC en manuel (configuration static).

- **Installation et configuration du serveur DNS (BIND9)**

```
[adel-lamine@badr Bureau]$ su
Mot de passe :
[root@badr Bureau]# yum install bind
```

L'exécution de la commande **yum install bind** permet de télécharger le BIND version 9.

- **Activation du service namad**

```
[root@badr Bureau]# chkconfig named on
```

La commande **chkconfig named** permet d'activer le service named.

- **Modification du dossier named.conf**

La commande **nano /etc/named.conf** permet d'accéder au répertoire

- **Lancement de notre répertoire named**

```
[root@badr Bureau]# service named start
Generating /etc/rndc.key:                                  [  OK  ]
Démarrage de named :                                       [  OK  ]
[root@badr Bureau]#
```

La commande service **named start** permet de lancer notre service

- **Création d'une zone dans le répertoire named.conf**

```
zone "linuxlab.local" IN {
        type master;
        file "linuxlab.local";
        allow-update { none; };
};
```

On va intégrer le domaine que l'on souhaite créer dans ce répertoire.

- **Modification de répertoire que l'on vient de créer linuxlab.local dans le répertoire named**

```
$TTL 1D
@       IN SOA  ns1.linuxlab.local. hostmaster.linuxlab.local. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS              ns1.linuxlab.local.
@       IN      MX      10      mail.linuxlab.local.
ns1     IN      A               192.168.1.100
mail    IN      A               192.168.1.100
```

La commande **nano /var/named/linuxlab.local** permet d'accéder au répertoire named. Ensuite on lui attribue l'adresse de notre serveur DNS et de notre serveur de messagerie et le MX (Mail eXchanger).

- **Modification du fichier named ownership**

```
[root@badr named]# chown root:named linuxlab.local
```

La commande **chown root :named linuxlab.local** permet de modifier le fichier namad ownership.

- **Relancement du service named**

```
[root@badr named]# service named reload
Rechargement named:                                        [  OK  ]
[root@badr named]#
```

La commande service **named reload** permet de relancer le service named.

- **Vérification si notre serveur DNS est opérationnel**

Les commandes suivantes permettent de tester si le serveur DNS est opérationnel :

— **dig @localhost ns1.linuxlab.local**

— **dig @localhost linuxlab.local MX**

— **dig @localhost linuxlab.local NS**

(ii) Installation et configuration de Zimbra 8.7.7

- **Mettre à jour le système (CentOS)**

```
[zimbra@badr ~]$ yum update
```

La commande **yum update** permet de mettre à jour notre système pour procéder à l'installation du Zimbra.

- **Téléchargement des prérequis pour l'installation du zimbra**

```
[zimbra@badr ~]$ yum install sudo sysstat libidn gmp libtool-ltdl compat-glib vixie-cron nc perl libstdc++.i686
```

La commande **yum install sudo sysstat libidn gmp libtool-ltdl compat-glib vixie-cron nc perl libstdc++.i686** permet de téléchargement les prérequis pour l'installation de zimbra.

- **Lancement de l'installation**

Avant de lancer l'installation, nous devons télécharger l'archive de zimbra la version compatible avec centos 6.9, après on le décompresse.

```
[root@badr Bureau]# cd
[root@badr ~]# cd /tmp/zcs-NETWORK-8.7.11_GA_1854.RHEL6_64.20170531151956
[root@badr zcs-NETWORK-8.7.11_GA_1854.RHEL6_64.20170531151956]# ./install.sh
```

La commande **./install.sh** permet de lancer l'installation.

- **Configuration des modules du Zimbra**

```
Store configuration

   1) Status:                              Enabled
   2) Create Admin User:                   yes
   3) Admin user to create:                admin@linuxlab.local
   4) Admin Password                       set
   5) Anti-virus quarantine user:          virus-quarantine.dtcrbapfz@linuxl
ab.local
   6) Enable automated spam training:      yes
   7) Spam training user:                  spam.puotytww@linuxlab.local
   8) Non-spam(Ham) training user:         ham.ccyf_qxwp@linuxlab.local
   9) SMTP host:                           badr.linuxlab.local
  10) Web server HTTP port:                8080
  11) Web server HTTPS port:               8443
  12) HTTP proxy port:                     80
  13) HTTPS proxy port:                    443
  14) Web server mode:                     https
  15) IMAP server port:                    7143
  16) IMAP server SSL port:                7993
  17) IMAP proxy port:                     143
  18) IMAP SSL proxy port:                 993
  19) POP server port:                     7110
  20) POP server SSL port:                 7995
  21) POP proxy port:                      110
  22) POP SSL proxy port:                  995
  23) Use spell check server:              yes
  24) Spell server URL:                    http://badr.linuxlab.local:7780/a
spell.php
  25) Configure for use with mail proxy:   TRUE
  26) Configure for use with web proxy:    TRUE
  27) Enable version update checks:        TRUE
  28) Enable version update notifications: TRUE
  29) Version update notification email:   admin@linuxlab.local
  30) Version update source email:         admin@linuxlab.local
  31) Install mailstore (service webapp):  yes
  32) Install UI (zimbra,zimbraAdmin webapps): yes
  33) License filename:                    /tmp/ZCSLicense.xml
```

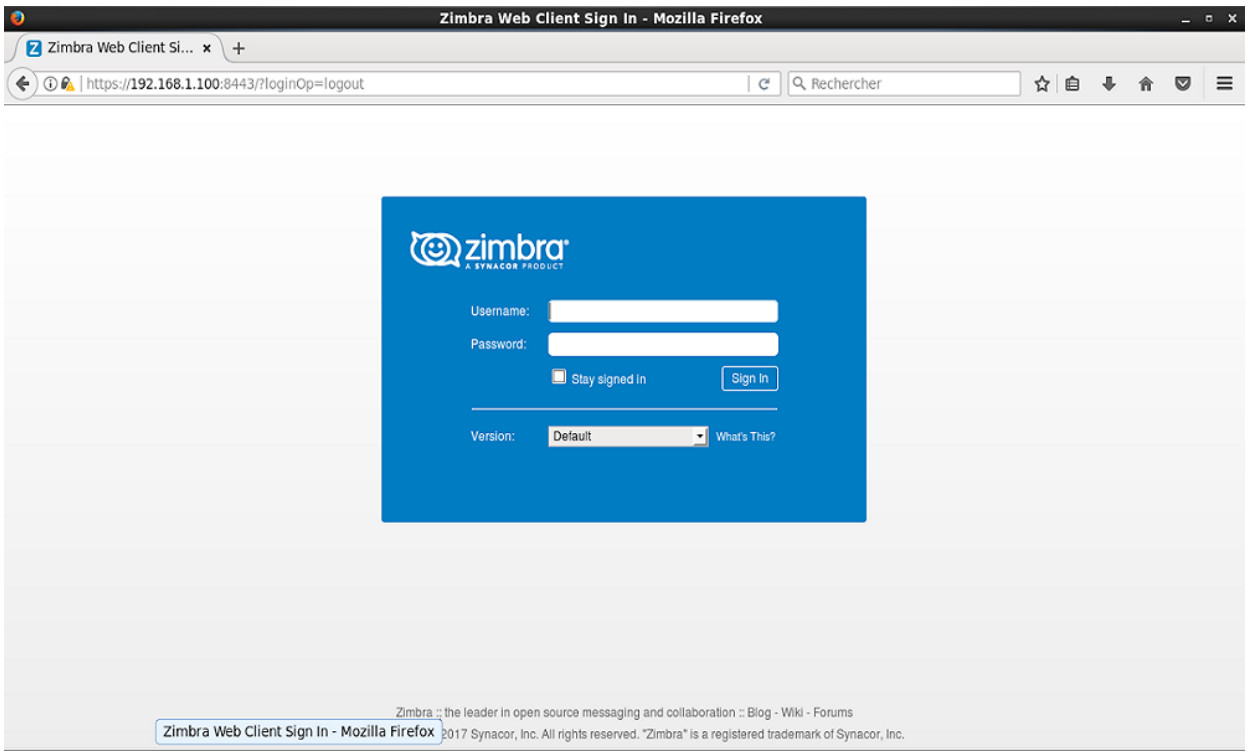
- **Finaliser l'installation des modules du Zimbra**

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                          Enabled
   3) zimbra-logger:                        Enabled
   4) zimbra-mta:                           Enabled
   5) zimbra-dnscache:                      Enabled
   6) zimbra-store:                         Enabled
   7) zimbra-spell:                         Enabled
   8) zimbra-convertd:                      Enabled
   9) Default Class of Service Configuration:
  10) Enable default backup schedule:       yes
   s) Save config to file
   x) Expand menu
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) 5
```

- **Verification que les modules Zimbra sont fonctionnel**

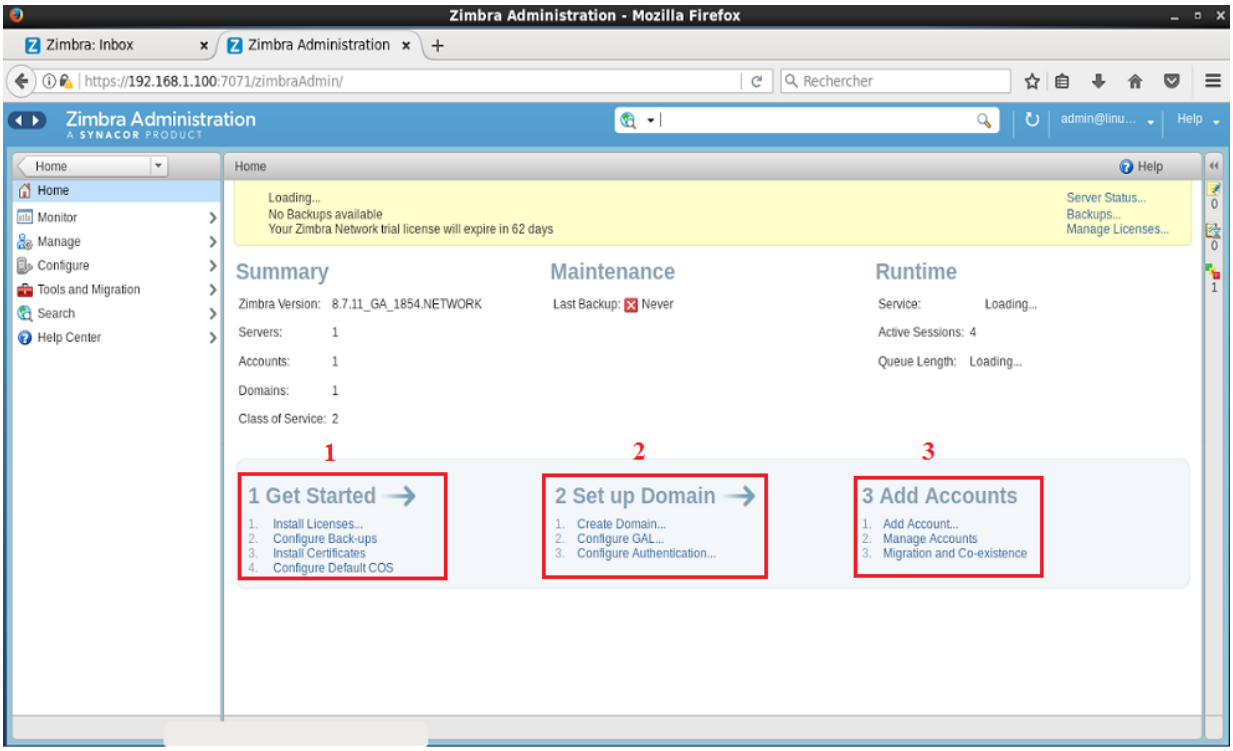
```
[zimbra@badr ~]$ zmcontrol status
Host badr.linuxlab.local
        amavis                  Running
        antispam                Running
        antivirus               Running
        convertd                Running
        ldap                    Running
        logger                  Running
        mailbox                 Running
        mta                     Running
        opendkim                Running
        service webapp          Running
        spell                   Running
        stats                   Running
        zimbra webapp           Running
        zimbraAdmin webapp      Running
        zimlet webapp           Running
        zmconfigd               Running
```

- **Administrer notre serveur de messagerie**

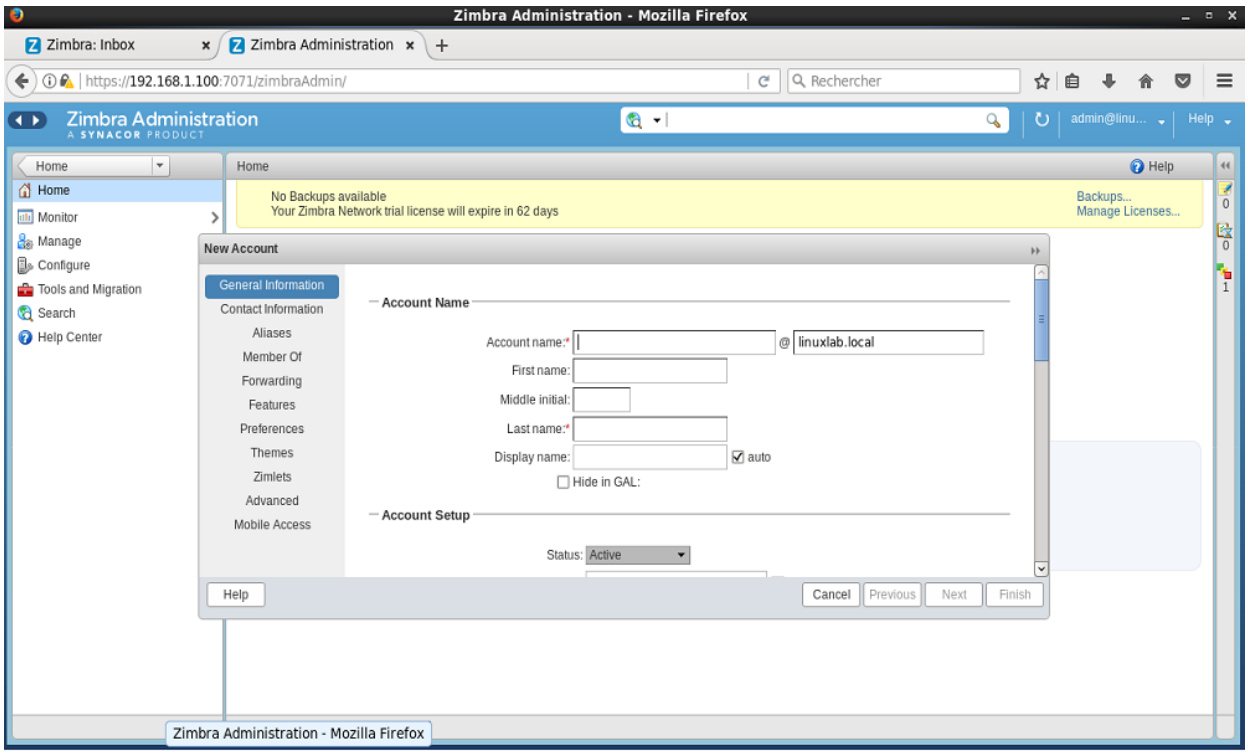


- Notre serveur Zimbra, est enfin prêt, alors on va se rendre à l'interface web administrateur avec le lien suivant : https ://linuxlab.local :7071

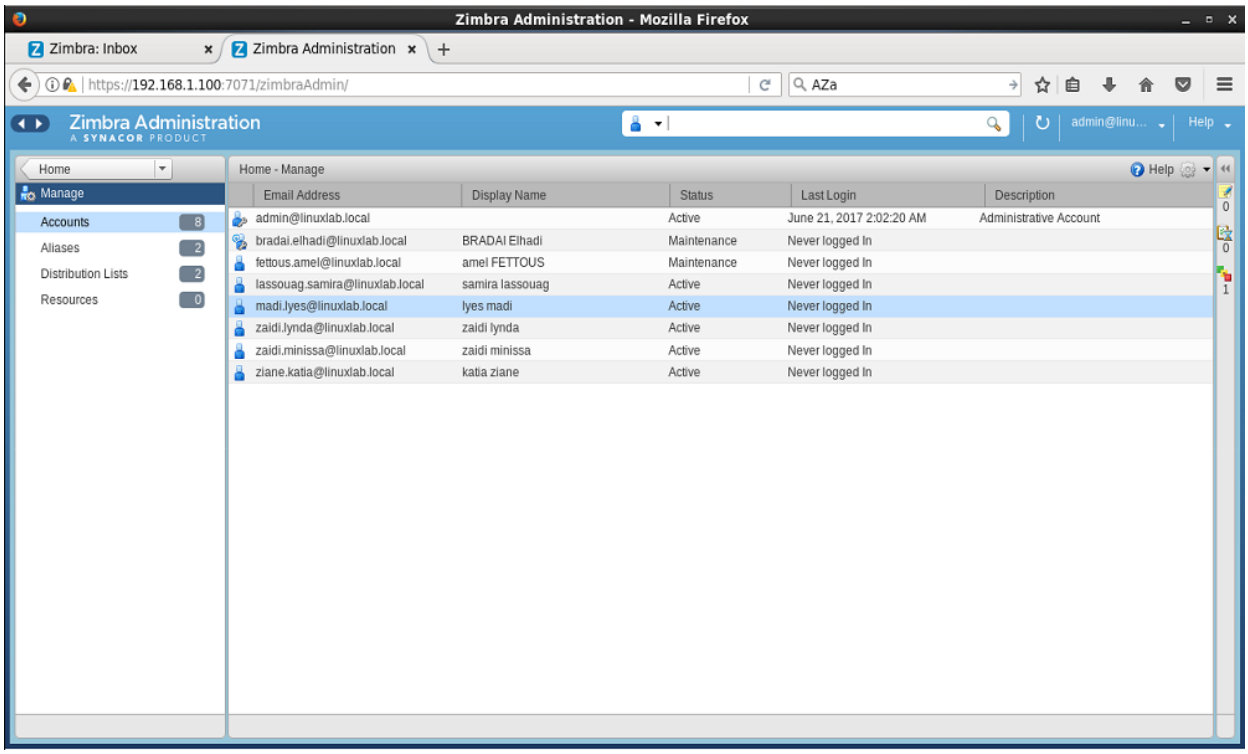
- Après avoir saisi le nom d'utilisateur et le mot de passe, l'interface administrateur se présente de cette façon :



- L'administrateur peut faire quelques tâches par exemple pour ajouter un compte, il utilise l'option 3 add accounts (ajouter un compte) après il remplit les différents champs et appuie sur « terminer »



- **Visualiser la liste des comptes créer, nous rendons dans manage puis accounts**



4.5 Conclusion

Dans ce chapitre, nous avons apporté des améliorations dans le réseau de la BADR pour donner un plus au fonctionnement de l'entreprise. Pour cela, nous avons présenté la phase de réalisation de notre projet en présentant les solutions mises en place, la démarche de travail, les étapes d'installation et de configuration, finalement, nous avons présenté les tests de validation effectués.

Conclusion générale

Au terme de ce projet, nous avons pu exploiter nos connaissances théoriques et pratiques acquises durant notre cycle universitaire pour améliorer l'architecture réseau de la banque d'agriculture et du développement rural de Bejaia.

Dans le dessein de réaliser notre projet, nous avons commencé par présenter quelques généralités sur les réseaux, la sécurité informatique, les principales caractéristiques des réseaux privés virtuels et des réseaux locaux virtuels et leur principe et fonctionnement.

Nous avons ensuite étudié l'architecture existante du réseau de la banque d'agriculture et du développement rural, ce qui nous a permis de proposer une nouvelle architecture avec meilleure fluidité et sécurité du réseau. Dans cette nouvelle architecture, nous avons proposé trois améliorations :

- ✓ En premier, un VLAN, où nous avons segmenté le réseau du GRE en VLAN dans un switch d'une manière à avoir un réseau fluide, une bande passante optimisée et une organisation souple et sécurisée.
- ✓ En deuxième, un VPN, permettant d'interconnecter des entités distantes (GRE et ALE), cela permettra d'assurer une protection aux échanges entre ces deux réseaux.
- ✓ En dernier, une messagerie, qui devient de plus en plus la solution de communication et d'échange de données au sein des grandes entreprises.

Ce projet à fait l'objet d'une étude théorique. Comme perspective, on propose quelques piste de développement pour le futur tel que l'étude de pannes et le taux de perte dans ce réseau et mettre en place ces différentes solutions dans l'entreprise d'accueil (BADR).

En définitive, comme tout travail scientifique, nous n'avons pas la prétention de réaliser un travail sans critique et suggestion de la part de tout lecteur afin de le rendre plus meilleur.

Bibliographie

Bibliographie

[1] Guy PUJOLLE, *Les Réseaux*. Edition 2014.

[2] José DORDOIGNE,*Réseaux informatique.* 4iéme Edition.

[3] COURS CCNA 1, chapitre 4, *Topologie physique et logique*. Netacad, 2017.

[4] Guy PUJOLLE, *Initiation aux Réseaux cours et exercice*. Edition Eyrolles, 2001.

[5] Guy PUJOLLE, *Les Réseaux*. Edition Eyrolles, 2008.

[6] J. F. CARPENTIER, *Tout sur les réseaux et internet*. Edition DUNOD, paris 2006.

[7] COURS CCNA 1, chapitre 4, *Suports réseaux*. Netacad, 2017.

[8] Andrew Tanenbaum - David Wetherall, *Réseaux*. 5 éme Edition, 2008.

[9] Sylvain Caicoya - Jean-Georges Saury,*TCP/IP le guide complet*. 2 éme Edition, 2008.

[10] Robin Burk, Martin Bligh, Thomas Lee et al,*TCP/IP*.Blueprints.

[11] B. Petit. Architecture des réseaux.*Cours et exercices Corrigés*.Ellipses, 2006.

[12] C. Pain-Barre, *Adressage IP*.IUT INFO, 2008-2009.

[13] J. F. CARPENTIER, *La sécurité informatique dans la petite entreprise*, 2iéme Edition, 2012.

[14] COURS CCNA 1, chapitre 1, *Sécurité du réseau*. Netacad, 2017.

[15] Guy PUJOLLE, *Les Réseaux*. Edition Eyrolles, 2014.

[16] Vincent REMAZEILLES, *La sécurité des réseaux avec CISCO*. Edition eni, 2009.

[17] Jean-luc, *Réseau d'entreprise par la pratique*. Edition EYROLLES, 2004.

[18] Jean-Paul. ARCHIER, *LES VPN Fonctionnement, mise en œuvre et maitenance des Réseaux Privés Virtuels*, 2010.

[19] Document interne de la BADR de béjaia

[20] COURS CCNA 2, chapitre 3, *VLAN*. Netacad, 2017.

[21] COURS CCNA 4, chapitre 7, *Réseaux privés virtuels (VPN)*. Netacad, 2017.

[22] Ghislaine LABOURET, *IPsec : présentation technique*, 2000.

[23] Roger SANCHEZ, *Les réseaux locaux virtuels (VLAN)*, certa janvier 2006-v1.0.

[24] Denis de REYNAL, Jehan-Guillaume de RORTHAIS et Sun Seng TAN. *Présentation sur les VPN*, UFR Ingénieurs, France, 2004.

Webographie

[25] `http://www.technologuepro.com/reseaux/Configuration-des-ACLs/les-ACLs.html`

[26] https://www.badr-bank.dz/index.php?id=presentation

[27] https://www.cisco.com/c/fr_ca/tech/wan/point-to-point-protocol-ppp/index.html

[28] wapiti.telecom-lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2001/Conion-Maubry/pptp.htm

[29] http://www.frameip.com/vpn/

[30] https://www.supinfo.com/articles/single/2460-principe-vpn

[31] https://technet.microsoft.com/fr-fr/library/cc768084.aspx

[32] https://www.sites.univ-rennes2.fr/urfist/messagerie_electronique_fonctionnement#1

[33] https://www.supinfo.com/articles/single/2521-gerer-securite-serveur-//messagerie-squirrelmail

[34] http://www.ens.math-info.univ-paris5.fr/cdc/sr-messagerie.html

[35] https://docs.tipimail.com/fr/integrate/smtp/servers/qmail/

[36] https://www.supinfo.com/articles/single/3758-microsoft-exchange-2016-//presentation-outils-administration

[37] https://www.ibm.com/support/knowledgecenter/fr/SSKTMJ_8.5.3/com.ibm.help.domino.admin85.doc/H_USING_THE_DOMINO_MAIL_SERVER_7032_OVER.html

[38] http://www.siloh.fr/Zimbra-Collaboration-Suite

[39] https://www.centos.org/about/

[40] http://eip.epitech.eu/2013/gns3/fr/project.html

Résumé

La Banque de l'Agriculture et du Développement Rural (BADR), est une institution financière bancaire jouant un rôle important dans la société Algérienne.
L'objectif de notre travail consiste à améliorer le réseau actuel de la BADR en lui proposant une nouvelle architecture, pour cela, nous avons procédé à une étude de l'architecture existante, ainsi que les dispositifs de sécurité mis en place. Ce qui nous a permis de la critiquer et de suggérer des améliorations afin de proposer une nouvelle architecture réseau plus souple et sécurisé. Sur le plan applicatif, nous avons segmenté le réseau du GRE en plusieurs VLANs par port et sous-réseau, par la suite nous sommes passés à la configuration des listes de contrôle d'accès (ACLs) afin de filtrer le trafic réseau. Aussi, nous avons configuré un tunnel sécurisé (VPN) basé sur le protocole IPSec reliant les deux réseaux GRE et ALE. Finalement, nous avons mis en place un serveur de messagerie Zimbra sous CentOS. Pour la simulation de notre topologie réseau, nous avons eu recours aux simulateurs de matériels réseaux CISCO Packet Tracer, qui nous a permis de configurer les différents composants et aussi au GNS3 qui s'intègre avec l'outil de capture et d'analyse de paquets Wireshark qui permet de capturer et de visualiser le transfert de données.

Mots clés : VLAN, ACL, VPN, IPSec, Zimbra, CentOS, CISCO Packet Tracer, GNS3, Wireshark.

Abstract

The Bank of Agriculture and Rural Development (BADR), is a banking financial institution playing an important role in the Algerian society.
The goal of our work is to improve the current network of the BADR by proposing a secure network architecture, in order to achieve that, we conducted a study of the current architecture and safety devices put in place. This allowed us to criticize it and to suggest improvements in order to propose a new network architecture that gives a better fluidity and safety. On the application side, we have segmented the GRE network into multiple VLANs by port and subnets, subsequently, we configured the access control lists (ACLs) to filter network traffic. Also, we have configured a secure tunnel (VPN) based on the IPSec protocol linking the two networks GRE and ALE. Finally, we installed zimbra messaging server under centOS. For the simulation of our network topology, we used the Cisco Packet Tracer network hardware simulators, which enabled us to configure the various components and also to the GNS3 which integrates with the package capture and analysis tool "Wireshark" which allows to capture and to visualize the data transfer.

Keywords : VLAN, ACL, VPN, IPSec, Zimbra, CentOS, CISCO Packet Tracer, GNS3, Wireshark.