République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

UNIVERSITE ABDERRAHMANE MIRA – BEJAIA

FACULTE DES SCIENCES EXACTES

DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'étude

En vue de l'obtention du diplôme de Master en informatique

Option : Administration et Sécurité des Réseaux

THEME

Mise en place d'une architecture VPN-IPsec pour le compte De CEVITAL

Soutenus devant le jury composé de :

Président :

Mr. BAADACHE Abderrahmane (MCA)

Examinateur :

Mr. AISSANI Sofiane (MAA)

Encadrant :

Mr. AKILLAL Abdellah (MAB)

Encadrant du stage :

Mr. YESSAD Hani

Réalisé par :

Mr. BAA Adel

Mr. SAKER Karim

DÉDICACES

Je dédie cet humble travail avec grand amour, sincérité et fierté :

A mes chers parents RACHID ET FATIHA, source de tendresse, de noblesse et d'affectation.

A mes chèrs amis en témoignage de la fraternité, avec mes souhaits de bonheur de santé et de succès.

Et à tous les membres de ma famille.

A tout qui compulse ce modeste travail.

DÉDICACES

Je dédie cet humble travail avec grand amour, sincérité et fierté :

A mes chers parents KHELAF ET NOUARA, source de tendresse, de noblesse et d'affectation.

A mes chères sœurs Nadia, Karima Kahina, Nassima, Fadila, Hanane, Samira, mon cher frère Nassim et sa chère épouse Laldja, en témoignage de la fraternité, avec mes souhaits de bonheur de santé et de succès.

Et à tous les membres de ma famille.

A tous mes amis et à tout qui compulse ce modeste travail.

Table des matières

Liste des abréviations

VSAT : Very *Small Aperture Terminal*

SLC : Smart Link Communication

IP : Internet Protocol

WAN : Wide Area Network

DMZ : Demelitrized Zone

IT : Information Technology

MPLS : Multi Protocol Label Switching

VPN : Virtual Private Network

RPV : Réseaux Privé Virtuel

CPU : Central Processing Unit

POP : Point Of Presence

FR : Frame Relay

QOS : Quality Of Service

OSI : Open Sysyems Interconnection

IETF : Internet Engineering Task Force

RFC : Request For Comments

PPTP : Point To Point Tunneling Protocol

L2F : Layer 2 Forwarding

ATM : Asynchronous Transfert Mode

PPP : Point To Point Protocol

SDH : Synchronous Digital hierarchy

LSR : Label Switch Router

LER : Label Edge Router

FEC : Forwarding Equivalence classes

VPI : Virtual Path Identifier

VCI : Virtual Channel Identifier

SSL : Secure Socket Layer

TLS : Transport Layer Security

FTP : File Transfert Protocol

TCP : Transport Control Protocol

HTTPS : HyperText Transfert Protocol Secured

MAC : Media Access Control

AH : Authentification Header

ESP : Encapsulation Security Payload

IKE : Internet Key Exchange

UDP : User Datagram Protocol

PSK : Pre-shared Key

RSA : Rivest Shamir Adelman

PKI : Public Key Infrastructure

Introduction Générale

Pour les entreprises comme pour les individus, l'internet est présenté comme une matière première dans le monde virtuelle ; nul ne peut s'empasser de son utilisation d'autant plus pour les entreprises.

L'internet a transformé la façon dont les entreprises gèrent leur affaires, or l'utilisation de cette dernière n'est pas sans danger car des échanges d'informations critiques, classées confidentielles faites par ces entreprises via ce grand réseau sont vulnérable et facile à être interceptées.

Ce qui engendre un risque de modification, vol d'information par de tierces personnes, et ce qui peut compromettre le développement de ces entreprises.

Pour y remédier des politiques de la sécurité informatique ont été misent en place afin d'assurer la confidentialité et garder ses données secrètes.

Parmi elles, les VPNs qui offrent un moyen d'échange sécurisé avec une mise en œuvre à faible cout.

Ce qui est notre finalité dans notre projet, c'est pouvoir relier les différents sites de l'entreprise CEVITAL et permettre leur interconnexion d'une manière sécurisée à travers un réseau public d'un opérateur afin que les communications au sein de ce dernier se réalisent d'une manière transparente grâce à cette solution.

Ce mémoire est structuré en trois chapitres comme suit :

Chapitre I : Présentation du cadre du projet et de l'entreprise d'accueil.

Chapitre II : Généralités sur les VPNs ou nous essayons de définir ce concept des VPNs et de présenter les différents protocoles qui y sont utilisés.

Chapitre III : Configuration et Tests qui est notre partie pratique ou nous concevant notre architecture réseau et faire les configurations nécessaires au niveau des routeurs afin de créer les tunnels VPNs entre les sites.

1

Présentation de l'organisme d'accueil

1.1. Introduction

Dans ce chapitre introductif nous allons présenter l'entreprise dans laquelle nous effectuons notre stage afin de réaliser notre projet de fin d'étude, ensuite nous ferons le point sur le thème de notre travail et les objectifs fixés.

1.2. Présentation de l'entreprise

Cevital Agro-industrie est une filiale du Groupe Cevital, créée en 1998.

Implantée au sein du port de Bejaia, Cevital Agro-industrie dispose de plusieurs unités de production :

1. deux raffineries de sucre ;
2. une unité de sucre liquide ;
3. une raffinerie d'huile ;
4. une margarinerie ;
5. une unité de conditionnement d'eau minérale ;
6. une unité de fabrication et de conditionnement de boisson rafraichissante et une conserverie.

Elle possède également plusieurs silos portuaires ainsi qu'un terminal de déchargement portuaire d'une capacité de 2000 tonnes/heure.

De plus elle exporte ses produits dans plusieurs pays, notamment en : Europe, au Maghreb, au Moyen Orient et en Afrique de l'Ouest. Elle compte parmi ses clients de grandes marques mondiales d'agro-business, tel que : Coca Cola, Kraft Food, Danone…

Cevital est le plus grand complexe privé en Algérie et le leader en Afrique et dans le bassin méditerranéen dans l'industrie du sucre et l'huile végétale. **[1]**

1.2.1 Organigramme de l'entreprise

Voici un organigramme représentant la composition des directions de l'entreprise

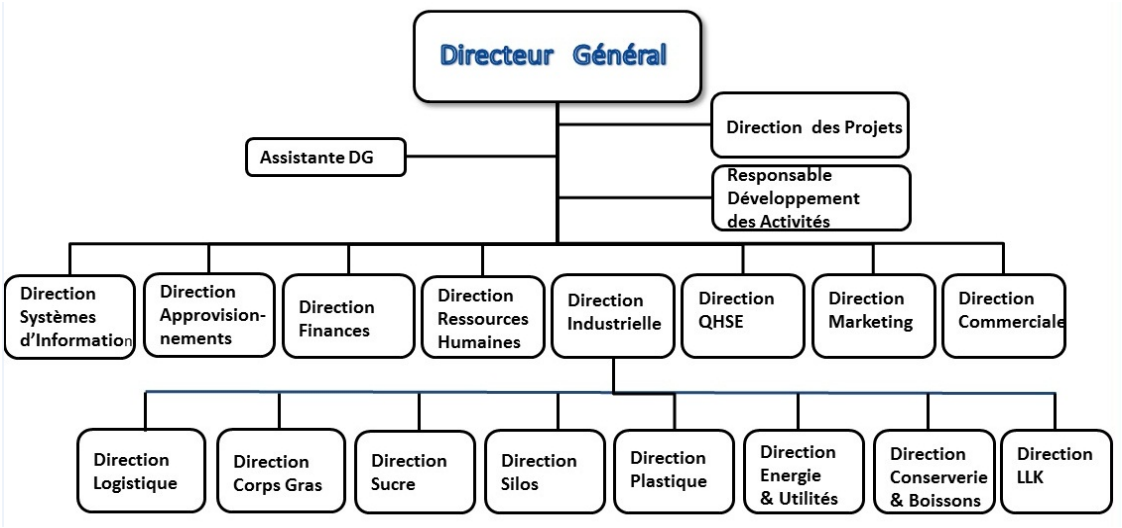

Figure 1 : Organigramme général de cevital

1.3. Directions de l'entreprise :

Dans ce qui suit nous allons citer les rôles de quelques directions, à savoir :

1.3.1 La direction des Finances

Le rôle de cette direction est :

- préparer et mettre à jour les budgets ;
- tenir la comptabilité et préparer les états comptables et financiers.
- pratiquer le contrôle de gestion. **[2]**

1.3.2 La direction commerciale

Elle a en charge de commercialiser toutes les gammes des produits et le développement du Fichier clients de l'entreprise. Et de la gestion de la relation client. **[2]**

1.3.3 La direction Industrielle

Elle est chargée de l'évolution industrielle des sites de production et définit, avec la direction générale, les objectifs et le budget de chaque site. Elle analyse les dysfonctionnements sur chaque site (équipement, organisation…) et recherche les solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail. Elle anticipe aussi les besoins en matériel et supervise leur achat (étude technique, tarif, installation…). Elle est aussi responsable du politique environnement et sécurité ainsi participe aux études de faisabilité des nouveaux produits. **[2]**

1.3.4 La direction des ressources humaines

Cette direction a pour mission :

- D'assurer un support administratif à l'ensemble du personnel de CEVITAL.
- piloter les activités du social
- assiste à la direction générale ainsi que tous les managers sur tous les aspects de gestion ressources humaines.
- Elle garantit également le recrutement
- chargé de la gestion des carrières et identifie les besoins de mobilité. **[2]**

1.3.5 La direction Approvisionnements

Dans le cadre de la stratégie globale d'approvisionnement et des budgets alloués (investissement et fonctionnement), cette direction met en place les mécanismes permettant de satisfaire les besoins en matières et en service afin de permettre la réalisation des objectifs de production et de vente. **[2]**

La direction Logistique

Cette direction expédie les produits finis, prenant la responsabilité de charger les camions, à livrer aux clients sur site et des dépôts.

Elle assure, et gère le transport de tous les produits finis, que ce soit au moyen propre (camion de cevital), ou en moyens de transport des clients. **[2]**

La direction des Silos

Cette direction décharge les matières premières vrac arrivées par navire ou camions vers les points de stockage et stocke dans les conditions requises les matières premières.

Elle est chargée aussi de :

- D'expédier et transférer vers les différents utilisateurs de ces produit dont l'alimentation de raffinerie de sucre et les futures unités de trituration ;
- De faire également l'entretien et maintien en état de services les installations des unités silos. **[2]**

1.3.8 La direction des boissons

Le pôle boissons et plastique comprend trois unités industrielles situées en dehors du site de Bejaia :

1- Unité LALLA KHEDIDJA domiciliée à agouni-gheghrane (wilaya de TIZI OUZOU) a pour vocation principale la production d'eau minérale et de boissons carbonatées à partir de la célèbre source de Lala Khedidja.

2- Unité plastique, installée dans la même localité, assure la production des besoins en emballages pour les produits de :

- Margarine
- les Huiles et à terme des palettes, des étiquettes...etc.

3- Unité COJEK, implantée dans la zone industrielle d'EL KSEUR, elle transforme des fruits et légumes frais en jus, Nectars et conserves. **[2]**

1.3.9 La direction Corps Gras

Le pole corps gras est constitué des unités de production suivantes :

- une raffinerie d'huile de 1800 T/J
- un conditionnement d'huile de 2200T/J,
- une margarinerie de 600T/J
- une unité chimique
- Hydrogénation
- pate chocolaterie

La mission principale de cette direction est de raffiner et de conditionner différentes huiles végétales ainsi que la production de différentes types de margarines et beurre. **[2]**

1.3.10 La direction pôle Sucre

Le pôle sucre est constitué de quatre unité de production :

- Une raffinerie de sucre solide 300T/J.
- Une unité de sucre liquide 600T/J.
- Une unité de conditionnement de sucre 200T/J (mise en service mars 2010)

Sa vocation est de produire du sucre solide et liquide dans le respect des normes de qualité. Ses produits sont destinés aux industriels et aux particuliers et ce pour le marché local et à l'export. **[2]**

1.3.11 La direction QHSE (Qualité Hygiene et Securité)

Cette direction met en place, maintient et améliore les différents systèmes de management et référentiels pour se conformer aux standards internationaux

Elle veille aussi au respect des exigences réglementaires produits, environnement et sécurité. **[2]**

1.3.12 La direction Maintenance et travaux neufs

Elle gère et déploie avec le directeur Industriel et les directeurs des pôles les projets d'investissement relatifs aux lignes de production, bâtiments et énergie/utilité (depuis la définition du processus jusqu'à la mise en route de la ligne ou de l'atelier).

Elle rédige aussi les cahiers de charges en interne et négocie avec les fournisseurs et les intervenants extérieurs.

Cette direction met en place et intègre de nouveaux équipements industriels et procédés, planifie et assure la maintenance pour l'ensemble des installations. **[2]**

1.3.13 La direction Système d'informations:

Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise.

Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mis à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité permanente et en toute sécurité.

Elle définit, également, dans le cadre des plans pluriannuels, les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies. **[2]**

Organigramme de la direction système d'information :

Ce service est organisé comme suit :

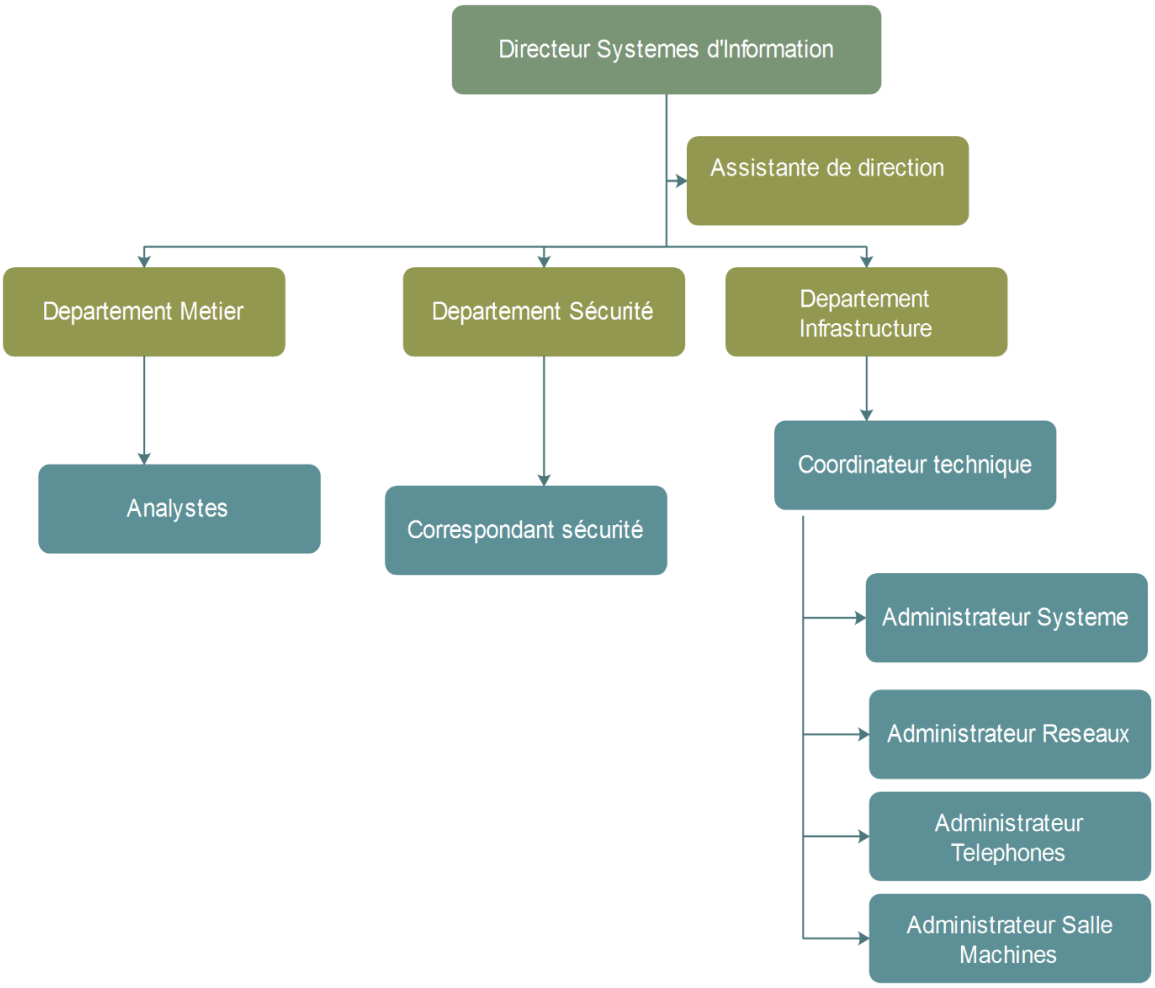

Figure 2 : Organigramme du service Système d'informations

1.4 Architecture du réseau informatique de Cevital

Cevital dispose d'un réseau commuté (téléphonique) de taille importante composé d'une plateforme de services reliant les sites locaux dans chacune des entités physiques. Il est constitué de plusieurs équipements dont :

- un seul Switch (*EtherSwitch router),* qui a une architecture réseau en étoile
- des routeurs et des firewalls, pour la plupart, de marque Cisco
- équipements satellitaires VSAT (*Very Small Aperture Terminal)* pour établir la communication entre différents sites interconnectés

Cette architecture est également composée des opérateurs SLC (*Smart Link Communication)* qui sont utilisés comme étant des liaisons d'accès à Internet avec des adresses IP publics.

1.4.1 Les équipements de la topologie

Nous allons définir les différents équipements utilisés dans le réseau de l'entreprise Cevital

1.4.1.1 Définition d'un routeur

Un routeur est un matériel de communication de réseau informatique destiné au routage. Il est responsable de la transmission de paquets à travers différents réseaux et de déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé.

La destination du paquet IP peut être un serveur Web se trouvant dans un autre pays ou un serveur de messagerie situé sur le réseau local. Les routeurs doivent transmettre ces paquets de manières rapide et efficace. **[3]**

1.4.1.2 Définition d'un EtherSwitch routeur

Les modules Cisco EtherSwitch offrent aux entreprises la possibilité d'intégrer sur une même plateforme la commutation et le routage. Ils réunissent le routage de réseau WAN de niveau 3 avec la commutation non bloquante de niveau 2.

Ils associent également la simplicité de configuration, la facilité de déploiement et l'administration intégrée. **[4]**

1.4.1.3 Définition d'un firewall

Un pare-feu (*firewall*), est un outil informatique (matériel et/ ou logiciel) conçu pour protéger un ordinateur ou un réseau d'ordinateur des intrusions provenant d'un réseau tiers (notamment internet). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les paquets de données échangés avec le réseau. **[4]**

1.4.1.4 Définition d'un DMZ

Dans les réseaux informatiques une zone démilitarisée (*Demilitrized Zone)* est un sous-réseau séparé du réseau local de l'entreprise et du réseau public extérieur (Internet) par un pare-feu, qui permet d'empêcher les utilisateurs d'avoir accès directement à un serveur qui contient des données de l'entreprise, donc le pare-feu

bloquera les accès au réseau local pour garantir sa sécurité et les services capables d'être accédés depuis Internet seront située en DMZ. **[5]**

1.4.1.5 Définition de SLC

SLC (*Smart Link Communication)* est l'opérateur de WiMax et large bande des entreprises en Algérie, qui permet à ces dernières de partager, traiter et stocker des informations principales à leurs activités en toute sécurité. Il met à la disposition de Ces clients une ressource qui combine un réseau WiMax et large bande, une infrastructure IT des réseaux et des solutions de télécommunications. **[5]**

1.4.1.6 Définition d'un VSAT

Le VSAT (*Very Small Aperture Terminal)* est un système qui repose sur le Principe d'un site principal (le hub) et d'une multitude de point distants (les stations VSAT).

Le hub est le point le plus important du réseau, c'est lui qui transite toutes les Données qui circulent dans celui-ci, il est structuré d'une antenne et plusieurs appareils. C'est aussi lui qui gère tous les accès à la bande passante. **[6]**

Le réseau de l'entreprise est conçu comme suit :

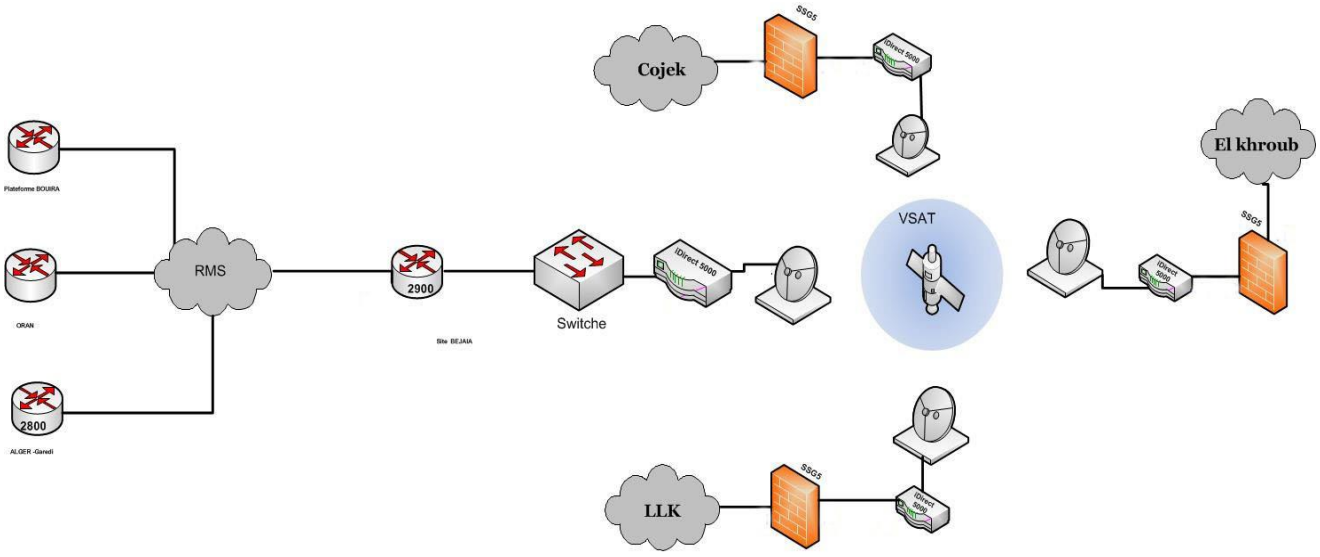

Figure 3 : Schéma d'interconnexion Réseaux WAN-VSAT

1.5 Présentation du contexte du projet :

Notre projet consiste à établir une connexion sécurisée entre les différents sites de l'entreprise CEVITAL, dont les communications sont faites à travers un réseau backbone d'un operateur privé (ooredoo) utilisant le protocole MPLS.

L'intérêt majeur de ce travail est de découvrir les différents aspects de la sécurité sur la transmission des données dans un réseau, à savoir, les réseaux privé virtuel (VPN).

1.5.1 Problématique :

De nombreuses difficultés de communications et de diffusion d'informations sont rencontrées lors de l'utilisation des liaisons satellitaires VSAT parmi lesquelles nous avons le problème de cout. En effet d'après notre encadrant de l'organisme d'accueil, l'entreprise dépense plus de quatre-vingts millions par mois.

En plus, si l'élément central du VSAT « le hub » tombe en panne, cela empêche la communication entre les différents sites du réseau. Ajouter à ceci le temps de latence qui est très élevé (environ 260 ms).

Ce qui les a poussés à changer d'architecture, en passant des VSAT à une architecture terrestre en fibre optique proposée par un fournisseur privé.

D'où la nécessité d'une intervention faisant appel aux moyens de sécurité informatique, car lors d'échange des données entre ses différents sites, ces données transitent par le réseau privé (opérateur), ce qui les rendent possible d'être interceptées et rend la communication vulnérable.

1.5.2 Solution proposée :

Nous avons opté pour la solution VPN site-à-site qui consiste à mettre en place une liaison permanente, distante et sécurisée entre les différents sites du groupe CEVITAL; afin de résoudre au mieux les différentes préoccupations manifestées par les responsables informatiques de CEVITAL.

Il est néanmoins important de préciser que la solution retenue garantie la confidentialité, la sécurité et l'intégrité des données sur des canaux privés. Cette solution VPN site-à-site permet d'obtenir une liaison sécurisée à moindre cout.

Conclusion

Dans ce premier chapitre consacré à la présentation du cadre du projet et l'entreprise dont nous avons effectués notre et sur qui est portée notre sujet d'étude, ce qui nous aidera à mieux voir la portée et la faisabilité de la solution proposée au problème.

2

Généralités sur les VPN

2.1 Introduction :

Dans ce chapitre nous allons d'abord définir ce qu'est pour nous un VPN (Virtuel private network) ou RPV en français (Réseau privé virtuel).

Nous établirons en suite une classification de ces VPN d'abord selon leur contexte d'utilisation. Ensuite nous présentons rapidement les principaux protocoles. Enfin nous terminerons en donnant quelques indications pour nous guider dans le choix lors de la mise en place de VPN.

2.2 Définition d'un VPN :

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sécurisés comme peut l'être le réseau internet.

Un tunnel rassemble des paquets IP avec des adresses internes qui sont confiés à un équipement tel qu'un router ou un pare-feu. Celui-ci les envois sur un canal souvent public (internet) à l'extrémité distante. Pour cela, les paquets internes sont encapsulés dans des paquets IP avec des adresses IP public des extrémités destinataire et source. L'équipement distant désencapsule chaque paquet pour remettre sur le réseau des paquets doté des adresses locales source et destination. **[7]**

Dans la figure suivante, nous allons expliquer de façon simplifiée l'opération d'encapsulation :

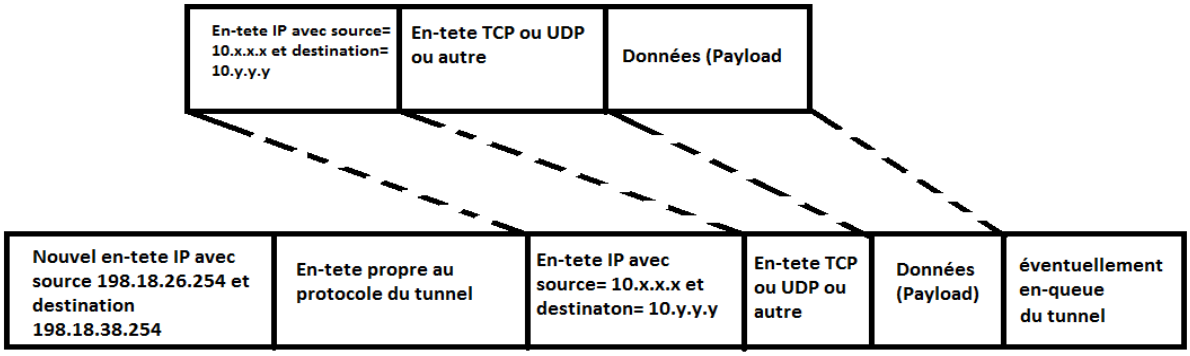

Figure 4 : Encapsulation des paquets IP

2.3 Typologie des VPN

On peut distinguer deux grandes catégories de VPN: le VPN d'entreprise et le VPN d'opérateur.

Chacune d'entre elle présente ses avantages et ses inconvenants et elles ne sont pas exclusive l'une de l'autre puisqu'il n'est pas rare de trouver les deux présentes simultanément au sein d'une même entreprise.

2.3.1 VPN d'entreprise

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

2.3.1.1 VPN site à site

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

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

Dans le cas de l'utilisation des matériels spécifiques, des processeurs spécialisés peuvent prendre en charge la partie cryptographique la plus consommatrice de ressources CPU.**[7]**

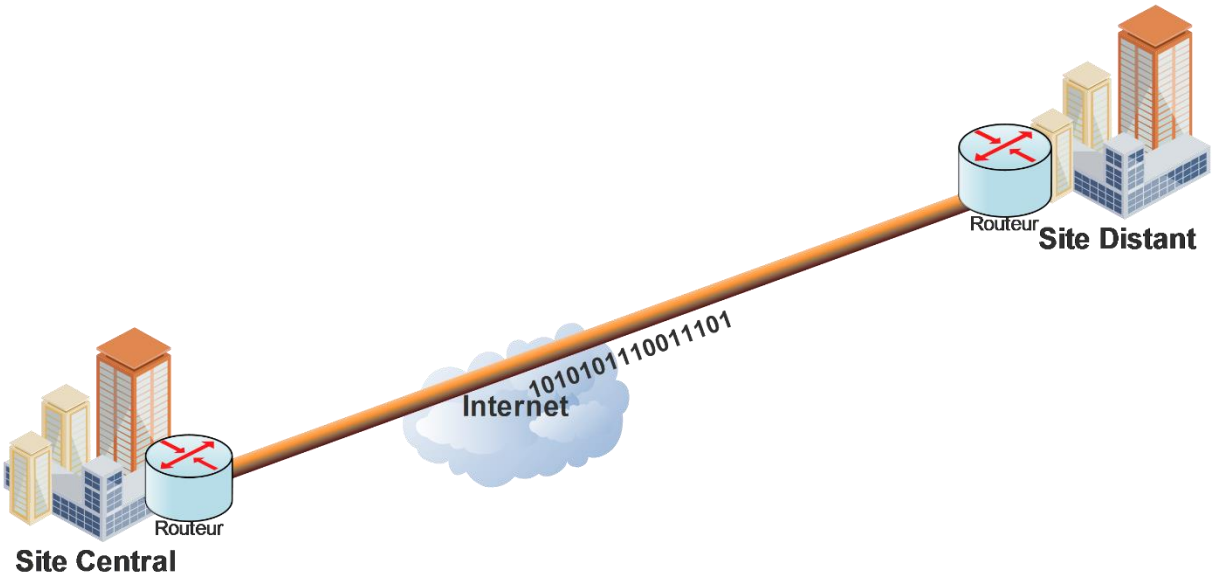

Figure 5 : Exemple d'un VPN site à site

Avantages et inconvénients :

Parmi les avantages procurés par cette configuration nous pouvons citer :

- Le cryptage est souvent pris en charge par des processeurs spécialisés, ce qui améliore notablement les performances.
- Une grande facilité pour le contrôle de trafic autorisé.
- Aucun impact sur les performances des poste puisque ceux-ci ne font pas de cryptage.
- La possibilité d'initier les VPN d'un côté ou de l'autre.

Mais cette solution présente aussi quelques inconvénients :

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

2.3.1.2 VPN poste à site :

C'est également une utilisation très fréquente des VPN que celle consistant à permettre à des utilisateurs distants (travailleurs à domicile…) d'accéder aux ressources de l'entreprise via un VPN.

Afin de réaliser cette solution, un matériel (firewall, routeur…) sera mis en place sur le site central, constituant le point de terminaison de tous les VPN de ce dernier. Et un logiciel gérant le type de protocole choisi et compatible avec le matériel du site central est installé du côté des postes de travail distant. Dans certain cas, ce logiciel est déjà présent dans le système d'exploitation de ces postes, dans d'autre cas, il est nécessaire d'installer ce composant logiciel. **[7]**

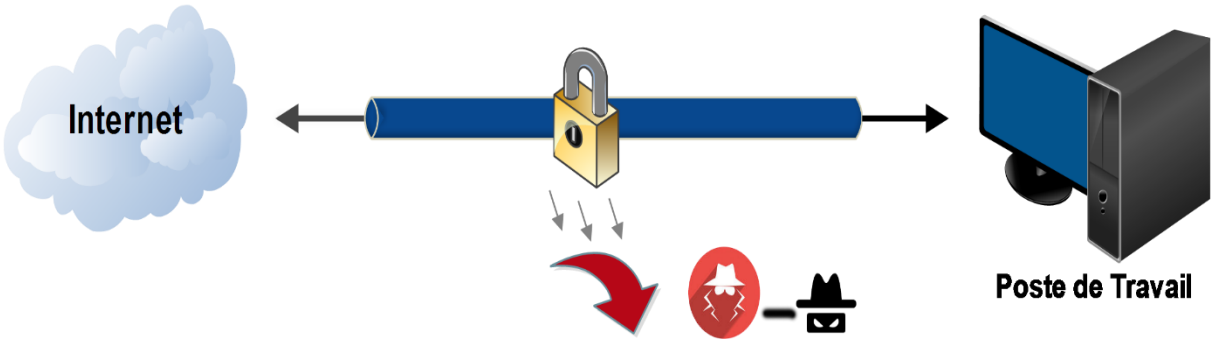

Figure 6: Exemple d'un VPN poste à site

Avantages et inconvénients :

Parmi les avantages de cette solution, on trouve :

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

Nous pouvons aussi trouver des inconvénients à cette configuration :

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

2.3.1.3 VPN poste à poste :

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

Pour cette configuration, nous ne faisons intervenir que des composants logiciels : un logiciel client sur le poste « demandeur » et un logiciel utilisé en serveur sur le poste « destinataire ». **[7]**

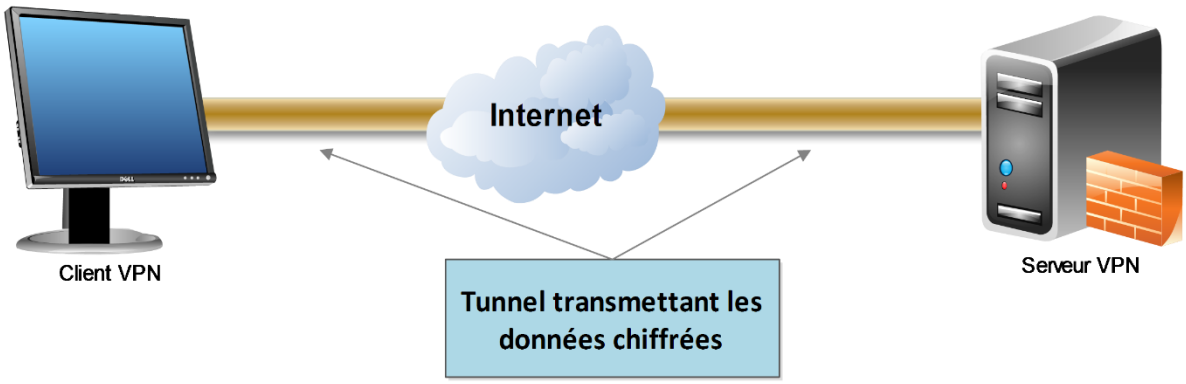

Figure 7: Exemple d'un VPN poste à poste.

Avantages et inconvénients :

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

Par contre, elle présente de nombreux inconvénients

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

Avantages et inconvénients du VPN entreprise :

Les principaux avantages de cette solution sont :

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

Mais il y'a quelques inconvénients :

- aucune garantie de temps de rétablissement en cas de défaillance.
- aucune garantie de performances puisque ces VPN ont pour support un lien internet.

2.3.2 VPN Operateur

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

Ce réseau tient plus d'un réseau de tunnels que d'un véritable réseau VPN mais il est assez courant de parler quand même d'un VPN operateur car il est quand même difficile, sans la complicité du personnel de l'opérateur, d'intercepter les communications échangés entre les sites. **[7]**

2.3.2.1. Caractéristiques du VPN operateur site à site :

Chaque site est relié au POP (Point Of Presence) le plus proche avec le medium souhaité (ADSL, SDSL, fibre optique .....) et un routeur complètement contrôlé par l'opérateur.

Ensuite établit des tunnels ou des circuits privatifs entre les différents sites au moyen des différents liens interconnectant ses POP.

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

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

- tous les sites secondaires convergent vers le site central et c'est celui-ci qui fait le relais : technologie en hub (ou en Etoile).
- tous les sites peuvent communiquer directement entre eux : full mesh ou maillage complet.
- les sites les plus importants peuvent communiquer entre eux et les secondaires passent obligatoirement par un des sites principaux.
- l'opérateur supervise la totalité du réseau et peut affecter des classes de service selon le type de trafic, ce qui permet de rendre prioritairement certains flux.**[7]**

Avantages et inconvénients du VPN operateur :

Les principaux avantages de ce type de réseaux sont :

- une transparence totale vis-à-vis des postes du réseau,
- une possibilité de mettre en place de la QOS (Quality Of Service) pour privilégier les trafics les plus prioritaires et garantir à ceux-ci un maximum de bande passante,

- une assurance sur les performances proposées par le réseau aussi bien en termes de débit que de temps de transit des messages.

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

- le cout engendré par l'abonnement de chaque site à ce réseau operateur.
- la nécessité d'avoir un opérateur unique pour l'ensemble du réseau mis en VPN.
- afin que les messages échangés dans ce réseau privatif ne puissent ne capturés, il faut ajouter un protocole de cryptage entre les stations ou entre les sites.**[7]**

2.4. Principaux protocoles :

Voici une brève description des protocoles les plus communément utilisés dans le cadre de VPN qu'ils soient d'entreprise ou d'opérateur.

Ils sont classés ici selon leur place dans les couches OSI (Open Systems Interconnection) mais ce classement peut se révéler arbitraire pour certains d'entre eux qui recouvrent en fait plusieurs niveaux.

2.4.1. Niveau 2 :

Ces VPN encapsulent les données dans des trames et ce sont ces trames que va véhiculer le tunnel dans une communication point à point.

Nous sommes donc bien ici au niveau 2 du modèle OSI. La plupart des protocoles situés ici sont progressivement délaissés au profit de protocoles plus souples comme peuvent l'être ceux des niveaux 3 à 7.

2.4.1.1 PPTP (Point to Point Tunneling Protocol):

Ce protocole fortement soutenu par Microsoft est très simple mais assez limité. Il est en fort déclin maintenant selon Jean-Paul ARCHIER l'auteur du livre « les VPN fonctionnement, mise en œuvre et maintenance des Réseaux Privé Virtuels ». **[7]**

En Principe, il permet de créer des trames sous le protocole PPP et les encapsuler dans un datagramme IP.

2.4.1.2. L2F (Layer 2 Forwarding) :

Cisco a développé ce protocole autour des années 1996.L'IETF a en fait un standard en 1998 avec le RFC 2341.Son fonctionnement est assez voisin de PPTP. **[7]**

2.4.1.3 L2TP (Layer 2 Tunneling Protocol) :

Dérivé de PPTP et de L2F ce protocole est maintenant un des protocoles VPN implantés nativement sur les machines Windows, ce qui explique son succès.**[7]**

2.4.2. Niveau 2 et 3

2.4.2.1 MPLS

Le protocole MPLS (Multi Protocol Label Switching) est souvent considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est pourquoi on lui affecte souvent un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnelles. Son placement en tant que protocole de VPN peut être contesté lorsqu'il est utilisé dans ses fonctions de base.
En effet il ne met pas en œuvre certaines fonctions de sécurité telles que le cryptage, ce qui est en principe un prérequis du VPN. **[10]**

2.4.2.2 Fonctionnalité

La première fonctionnalité de MPLS consiste à accélérer la transmission des informations au sein d'un backbone IP, car l'acheminement est basé sur la reconnaissance d'un Label qui permet dans le réseau de transit de ne plus se préoccuper de l'adresse mais de traiter le message en fonction de ce Label.
La seconde est de permettre la création de VPN (Virtual Private Network) ou groupe fermé d'utilisateurs. **[10]**
MPLS est une technologie toujours en cours de standardisation à l'IETF. L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des gigarouteurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

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

2.4.2.3 Principes MPLS

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

A l'entrée du réseau MPLS, les paquets IP se voient insérés un label par le "Ingress Label Edge Routeur" ou "Ingress LER" (interface d'entrée ou point de départ d'une donnée). Les LER sont les routeurs MPLS se situant à la périphérie du réseau de l'opérateur. Les paquets labélisés sont ensuite commutés vers le cœur du réseau selon son numéro de label. Les routeurs MPLS du cœur de réseau, les Label Switching Router, commute ensuite les labels jusqu'au LER de sortie (Egress LER). Le chemin qui a été pris par le paquet, et préalablement établi, au travers du réseau s'appelle un Label Switched Path (LSP). **[10]**

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

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

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

L'affectation des étiquettes aux paquets dépend des groupes ou des classes de flux FEC (forwarding équivalence classes). Les paquets appartenant à une même classe FEC sont traités de la même manière. Le chemin établi par MPLS appelé LSP (Label Switched Path) est emprunté par tous les datagrammes de ce flux.

L'étiquette est ajoutée entre la couche 2 et l'en-tête de la couche 3 (dans un environnement de paquets) ou dans le champ VPI/VCI (identificateur de chemin virtuel/identificateur de canal virtuel dans les réseaux ATM (Asynchronous Transfert Mode)).

Le switch LSR du nuage MPLS lit simplement les étiquettes, applique les services appropriés et redirige les paquets en fonction des étiquettes. Ce schéma de consultation et de transfert MPLS, offre la possibilité de contrôler explicitement le routage en fonction des adresses source et destination, facilitant ainsi l'introduction de nouveaux services IP. **[10]**

2.4.3. Niveau 3

Nous retrouvons ici les protocoles opérant au moins au niveau 3, donc au niveau paquet.

2.4.3.1. SSL/TLS

Ce protocole ou plutôt ces protocoles sont en plein essor car très simples de mise en œuvre et utilisant le port (443), ce qui facilite le franchissement des firewalls. Dans un certain nombre de cas, ils ne nécessitent qu'un simple navigateur pour être utilisables. Ils sont maintenant implémentés de façon native dans d'autres logiciels (client de messagerie, client FTP). **[7]**

2.4.3.2 SSH

Ce protocole était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son essor est limité à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint. Néanmoins il reste encore un protocole à considérer pour certains usages. **[7]**

2.4.3.3. IPSEC

Ce protocole très populaire est un des plus robustes et des plus versatiles mais il est aussi un des plus complexes.

IPsec permet, par encapsulation, de protéger les données échangé en plusieurs aspects :

- Confidentialité
- Intégrité des données
- anti-rejeu

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

Le dialogue IPsec est généralement possible entre ces différents systèmes et équipements. Dans de nombreux cas, l'utilisation d'IPsec présente un rapport "bénéfice en sécurité" sur "coût" appréciable dans la mesure où cette technologie est prise en charge nativement par la plupart des systèmes clients et des équipements réseau et ne nécessite donc généralement pas d'investissements lourds. **[12]**

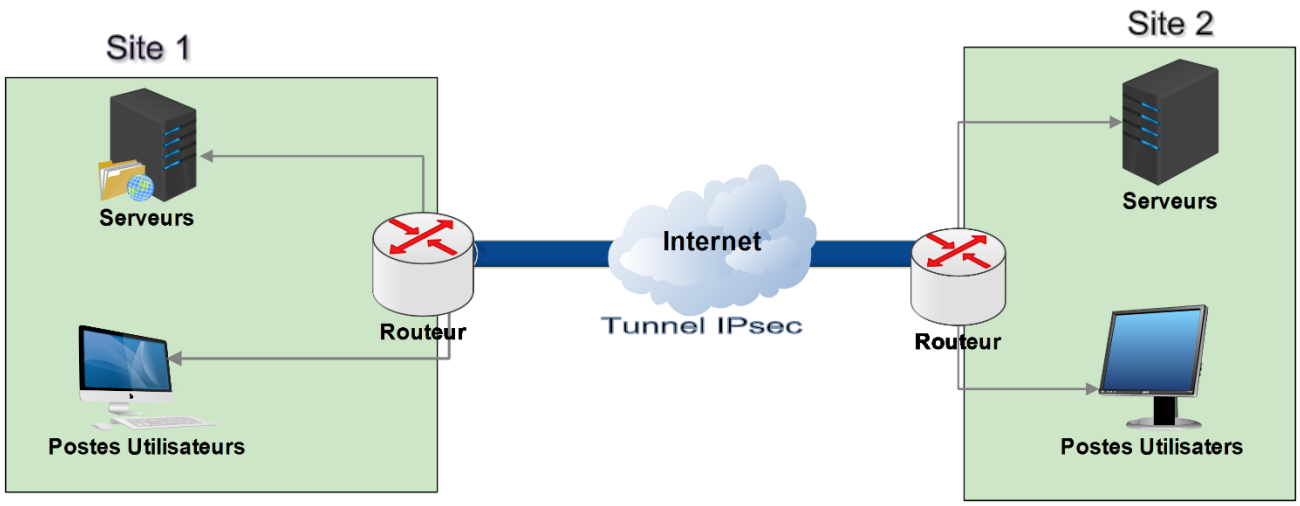

Figure 8: Exemple d'emploi d'IPsec entre sites distants.

2.4.3.3.1 Comparaison avec TLS

Il est fréquent de voir IPsec comparé au protocole TLS . Il est vrai que les deux echnologies permettent de bénéficier de mécanismes de confidentialité, d'intégrité ou d'authentification. Il existe toutefois plusieurs différences importantes, qui tendent à faire préférer IPsec.
TLS agit beaucoup plus haut dans la pile réseau qu'IPsec, en se plaçant au-dessus de la couche transport réalisée par TCP. TLS est souvent employé pour sécuriser d'autres protocoles.
c'est ainsi que fonctionne par exemple le protocole HTTPS. C'est toutefois sur un autre usage que ce protocole entre en concurrence avec IPsec, à savoir la mise en oeuvre de « VPN-SSL ». Cette méthode consiste à encapsuler un flux réseau dans une session TLS.
Certaines solutions de ce type proposent de s'appuyer sur un navigateur pour se dispenser de la nécessité de déployer un client spécifique sur les postes utilisateurs.
Le premier inconvénient de TLS est que les opérations liées à la sécurité sont effectuées en espace utilisateur, au sein du processus utilisateur.
Ces opérations (et les secrets qu'elles manipulent) sont alors nettement plus exposées aux attaques que dans le cas d'IPsec où les opérations critiques se déroulent au sein du noyau ou dans des processus dédiés. Cela est d'autant plus vrai dans le cas où le client VPN s'appuie sur un navigateur, logiciel présentant une surface d'attaque considérable, y compris à distance.
En outre, sur le plan cryptographique, plusieurs éléments plaident en faveur d'IPsec. D'une part, IPsec permet plus largement l'utilisation d'algorithmes modernes recommandés par les bonnes pratiques, que ce soit en termes de prise en compte dans les standards ou d'implantations concrètes dans les logiciels disponibles sur le marché. D'autre part, dans IPsec, l'utilisation des primitives cryptographiques est légèrement meilleure au regard des bonnes pratiques.
IPsec recourt, par exemple, à un fonctionnement « Encrypt-then-MAC », méthode considérée plus sûre que le « MAC-then-Encrypt » employé par TLS.
Enfin, on peut observer que le détournement de TLS de l'usage en recourant à des « VPN SSL » n'est pas une solution idéale.
L'encapsulation de paquets de la couche réseau en couche applicative conduit notamment à avoir une en-tête TCP « externe » sans aucune corrélation avec l'éventuelle en-tête TCP « interne », ce qui débouche sur un fonctionnement non optimal des mécanismes de contrôle de congestion. **[12]**

2.4.3.3.2 Fonctionnement d'IPsec

IPsec, de par ses subtilités, est souvent partiellement compris et peu maîtrisé. Les choix de configuration, y compris ceux par défaut, ne sont pas toujours judicieux et l'emploi d'IPsec peut alors offrir un niveau de sécurité plus faible que celui attendu. **[12]**

2.4.3.3.3 Services fournis par IPsec

Les services de sécurité fournis par IPsec reposent sur deux protocoles différents qui constituent le cœur de la technologie IPsec :

– **AH** : « Authentication Header » (protocole n°51) dont la version la plus récente est normalisée par la RFC 4302 ;

– **ESP** : « Encapsulation Security Payload » (protocole n°50) dont la version la plus récente est normalisée par la RFC 4303.

Ces deux protocoles peuvent être utilisés indépendamment ou, plus rarement, de manière combinée.

AH : intégrité et authentification des paquets

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

ESP : confidentialité, intégrité et authentification des paquets

Le protocole ESP permet quant à lui d'assurer la confidentialité, l'intégrité et, employé avec IKE, l'authentification des données échangées. Il garantit aussi une protection contre le rejeu. Il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH). **[12]**

2.4.3.3.4 Mode Transport et Tunnel

Indépendamment du choix entre AH et ESP, il est possible d'utiliser IP sec dans deux modes Distincts : le mode tunnel et le mode transport. Le mode tunnel rend le service attendu dans la majorité des cas.

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

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

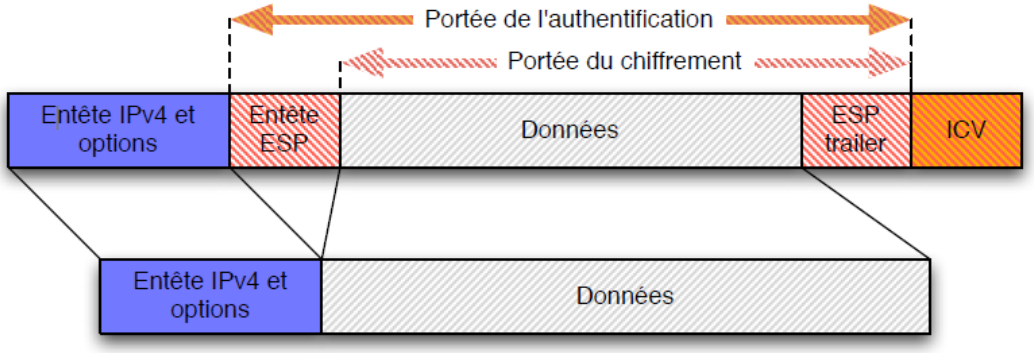

Figure 9: Utilisation d'ESP en mode transport.

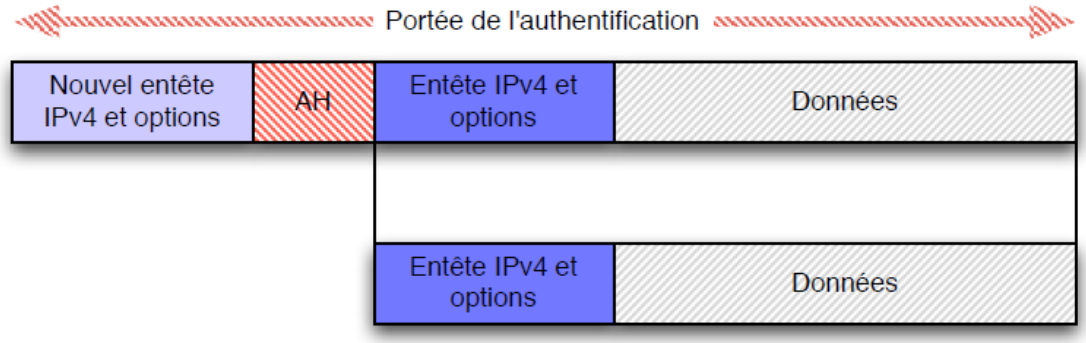

Figure 10 : Utilisation d'AH en mode transport

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

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

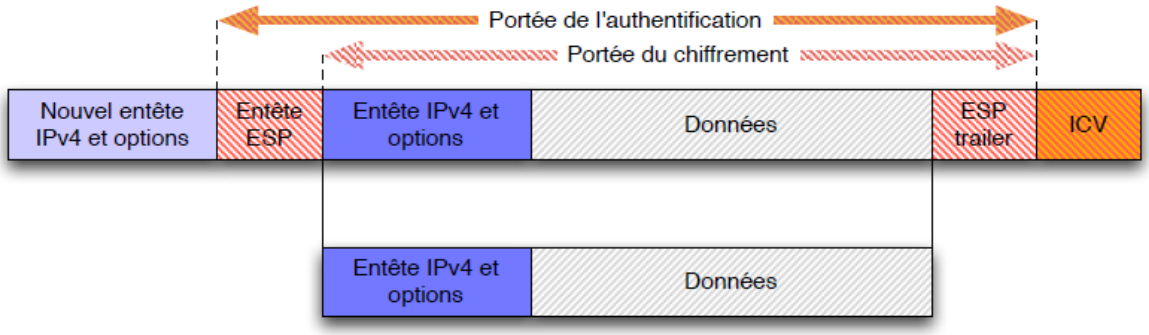

Figure 11 : Utilisation d'ESP en mode tunnel.

PS : ICV désigne l'« Integrity Check Value » : valeur utilisée par le mécanisme de contrôle d'intégrité, similaire au CRC dans une trame ethernet.

Figure 12 : Utilisation d'AH en mode tunnel

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

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

Naturellement, du fait de la duplication de l'en-tête IP, l'utilisation du mode tunnel résulte en des paquets plus gros qu'en mode transport pour une même quantité de données utiles.

La consommation en ressources réseau est donc plus importante. **[12]**

2.4.3.3.5 Security Policy

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

– de l'utilisation obligatoire ou facultative ou de la non-utilisation d'IPsec ;

– de l'utilisation du mode tunnel ou transport ;

– de l'utilisation d'AH ou d'ESP.

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

À l'image des règles de flux d'un pare-feu, les SP ont pour but de spécifier les flux que l'on veut autoriser et ceux que l'on veut interdire. **[12]**

2.4.3.3.6 Utilisation d'IKE

La négociation dynamique des algorithmes et clés d'une SA peuvent se faire grâce au protocole IKE, actuellement en version 2 (RFC 5996). **[12]**

2.4.3.3.7 Authentification des correspondants

L'authentification des participants à la première phase peut se faire soit au moyen d'un secret partagé (PSK : « Pre-Shared Key ») soit par utilisation d'un mécanisme de cryptographie asymétrique tel que RSA. Dans ce cas, il est possible d'utiliser une Infrastructure de Gestion de Clés (IGC ou PKI) pour certifier les clés publiques des participants et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes. **[12]**

Conclusion

Dans ce chapitre on a présenté les notions de base nécessaires au fonctionnement et la réalisation d'une solution VPN ainsi que les différents protocoles utilisés notamment IP sec, sur qui est porté notre choix.
Le chapitre fera l'objet de la réalisation et simulation d'une connexion VPN site-à-site.

3

Configuration et Tests

Introduction

Dans ce chapitre on entamera la configuration VPN du réseau de l'entreprise avec des tests qui démontreront son bon fonctionnement et on déploiera l'architecture permettant de relier les différents sites de l'entreprise, ainsi qu'une présentation des différents logiciels utilisés pour y parvenir.

3.1 Les outils de réalisation

3.1.1 GNS3

GNS3 est un simulateur de réseau graphique qui permet de concevoir facilement les topologies de réseau, puis exécuter des simulations sur eux. Nous pouvons même prolonger le réseau en le connectant à une topologie virtuelle.

Pour ce faire, GNS3 est basé sur Dynamips, Qemu (y compris son emballage) et en partie sur Dynagen, il a été développé en python et par PyQt.

GNS3 utilise également le la technologie SVG (Scalable Vector Graphics) pour fournir des symboles de haute qualité pour la conception de la topologie du réseau. **[9]**

- **Dynamips** : un émulateur d'image IOS qui permet de lancer des images binaires IOS Provenant de Cisco Systèmes.**[14]**

- **Dynagen** : une interface en mode texte pour Dynamips.**[14]**
- **IOS** : À l'instar d'un ordinateur personnel, un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation. Sans système d'exploitation, le matériel est inopérant. Cisco IOS est le logiciel système des périphériques Cisco.
  IOS signifie Internetworking Operating System**.[13],[3]**
- **Qemu**, est un logiciel libre de machine virtuelle, pouvant émuler un processeur et, plus généralement, une architecture différente si besoin. Il permet d'exécuter un ou plusieurs systèmes d'exploitation.**[11]**

GNS3 est un logiciel libre qui fonctionne sur de multiples plateformes, incluant Windows et Linux.

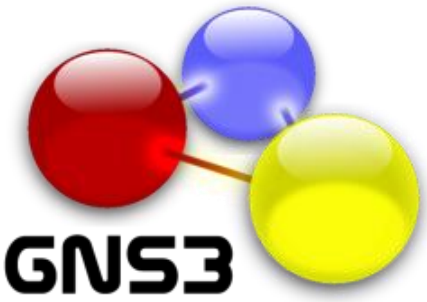

Figure 13 : Logo du logiciel GNS3

3.1.2 WIRESHARK

Wireshark est un analyseur de protocole de réseau ou Sniffer, anciennement publié sous le nom Ethereal. Ce programme est capable d'intercepter les paquets transmis sur le réseau et de compiler des statistiques sur l'utilisation du réseau.

Il permet à l'utilisateur de visualiser une liste de paquets capturés, analyser des données sur chaque paquet, et vue, au format hexadécimal, les données contenues dans ce paquet. Il a intégré des fonctionnalités de codage couleur qui aident l'utilisateur à identifier notamment types de trafic réseau, tels que DNS en bleu et en vert HTTP.

La plupart des informations affichées dans la figure peuvent être utilisées pour mettre en place le tri des filtres, ce qui simplifie le processus d'analyse données.**[8]**

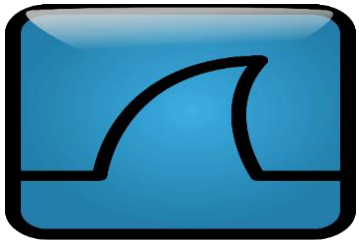

Figure 14 : Logo du logiciel Wireshark

3.2 Architecture du réseau

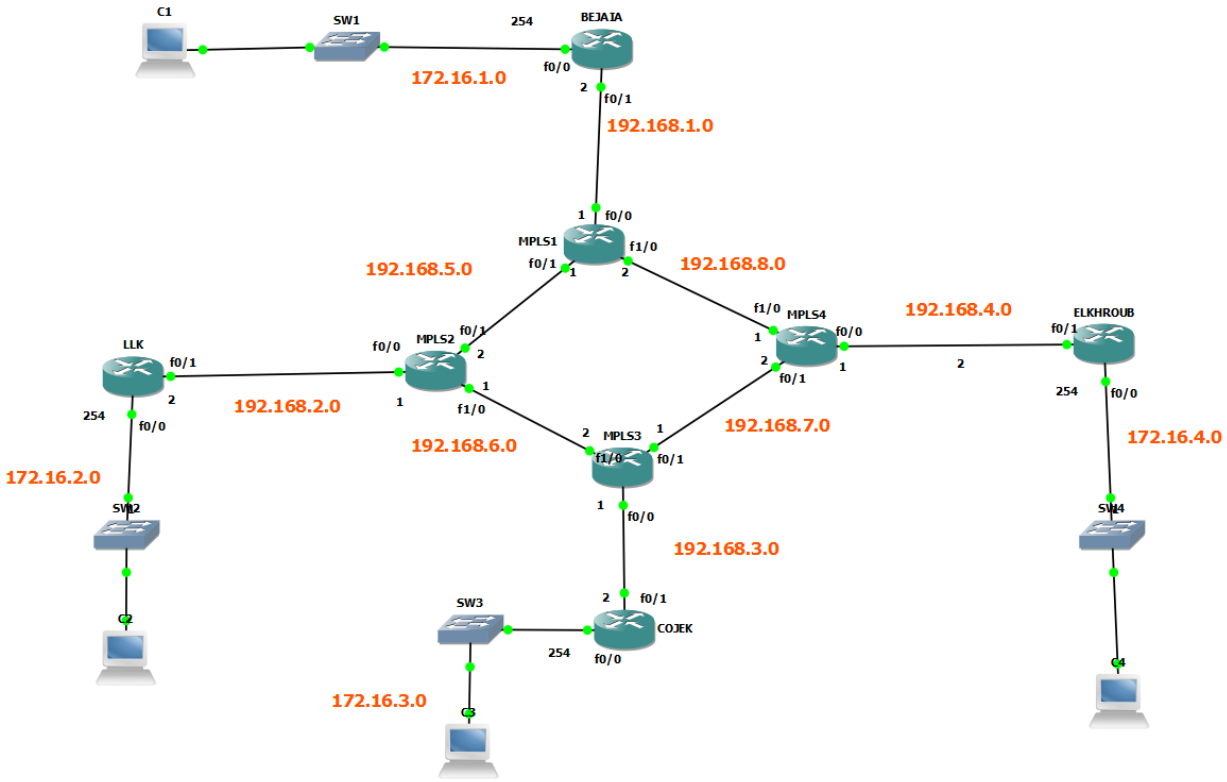

Figure 15 : Architecture du réseau sous GNS3

3.3 Configuration

A présent nous allons passer à la configuration des routeurs sur les différents sites.

3.3.1 Présentation des quatre sites

L'architecture ci-dessus relie quatre sites situés dans quatre villes différentes disposant chacun d'un réseau local que nous avons défini avec une adresse de classe B.

3.3.1.1 Site de Bejaia

Considéré comme le site central, le site de Béjaïa est représenté par un routeur Cisco de gamme 3725 pour lequel nous avons attribué les interfaces suivantes :

fo/0 : 172.16.1.254/24 (reliée au réseau local).

fo/1 : 192.168.1.2/30 (reliée au backbone Operateur).

Loopback 0 : 1.1.1.1/32.

-172.16.1.0 : On a choisi de la classe B pour segmenter le réseau en nombre suffisant de sous-réseaux afin de pouvoir représenter les différents services et dans chaque sous-réseau on peut avoir jusqu'à 2^8 hôtes.

-192.168.0.0 : pour relier les différents réseaux entre eux, et on prit un masque /30 car chaque routeur possède au maximum trois interfaces (adresses), d'où on a besoin de deux bits dans la partie hôte (2 bits ---> 4 hôtes).

-Loopback 0 : c'est une interface virtuelle qui permet le bon fonctionnement du routeur.

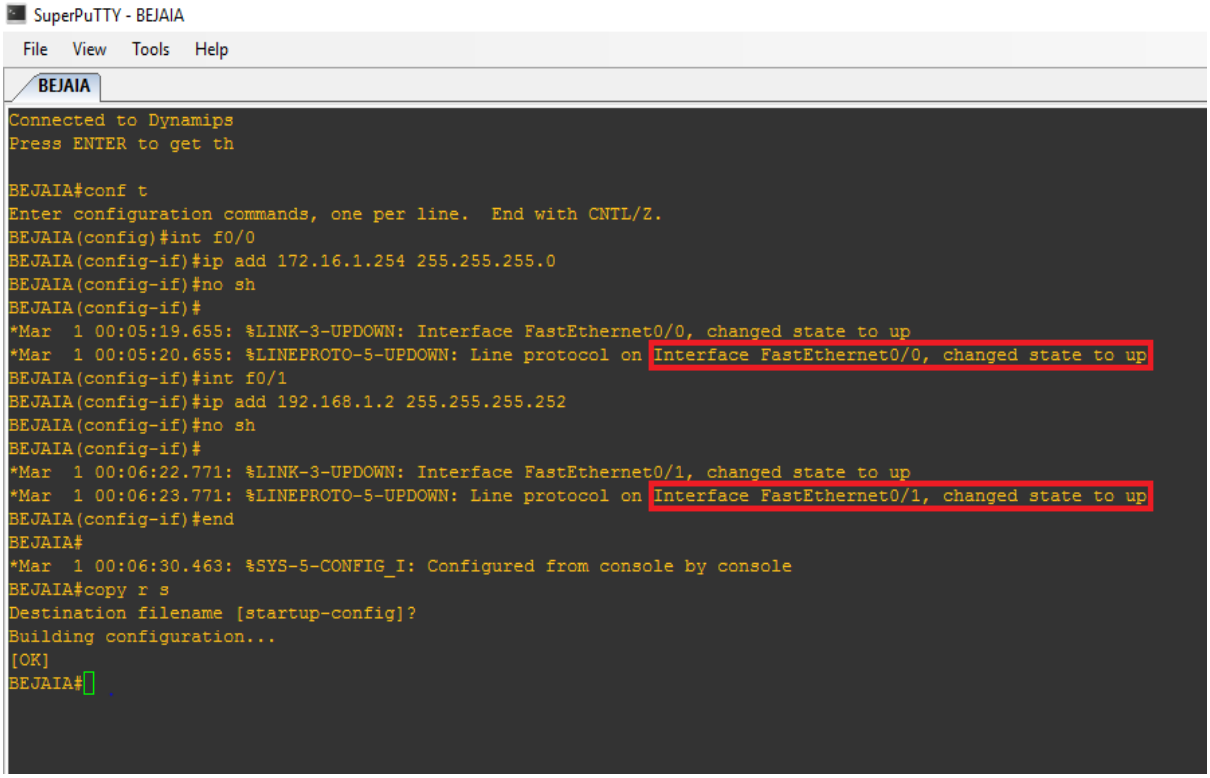

Figure 16 : Attribution des adresses aux interfaces du routeur BEJAIA.

On voit dans la figure, que les deux interfaces f0/0 et f0/1 sont activées avec succès (les deux rectangles en rouge).

Nous avons utilisé OSPF comme protocole de routage car :

D'abord, il est utilisé dans l'architecture du réseau réel, ensuite c'est un protocole conçu pour gérer de large réseau (comme dans notre cas). Ainsi, il permet de diviser le domaine de routage afin de faciliter sa gestion. Enfin OSPF gère plus finement l'allocation des adresses

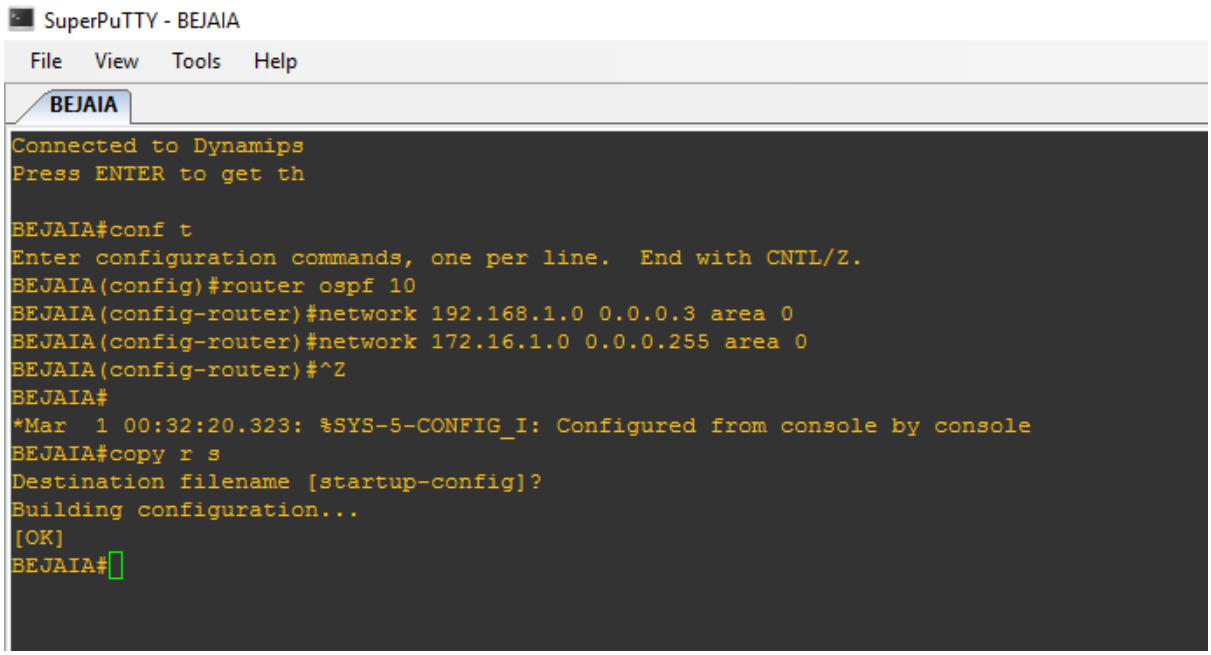

Figure 17 : routage OSPF sur le routeur du site BEJAIA.

3.3.1.2 Site Lalla Khedidja (LLK)

Il est représenté par un routeur Cisco de gamme 3725 pour lequel nous avons attribué les interfaces suivantes :

f0/0 : 172.16.2.254/24 (reliée au réseau local)

f0/1 : 192.168.2.2/30 (reliée au backbone Operateur).

Loopback 0 : 2.2.2.2/32.

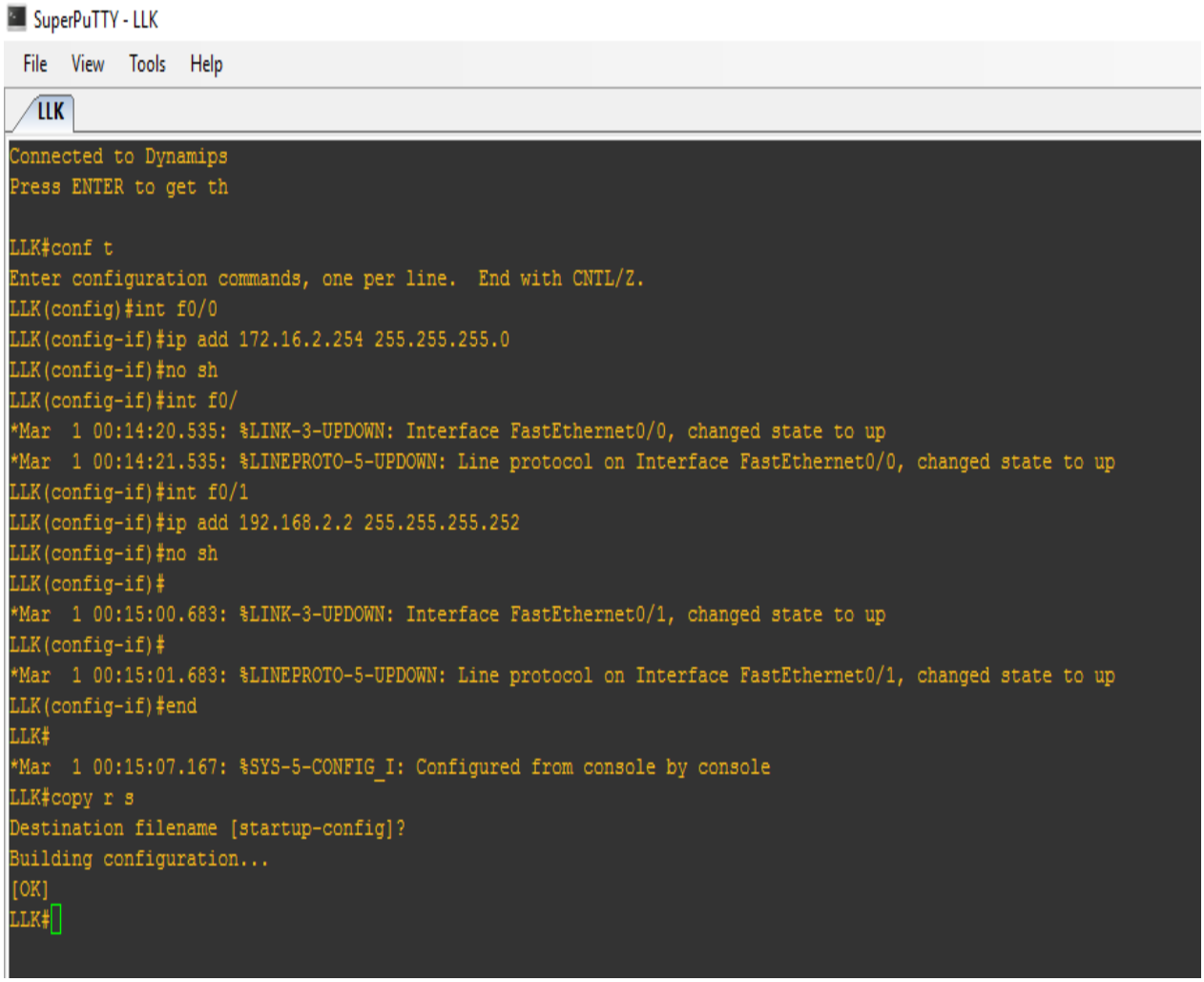

Figure 18 : Attribution des adresses aux interfaces du routeur LLK.

Nous avons utilisé aussi le protocole de routage OSPF :

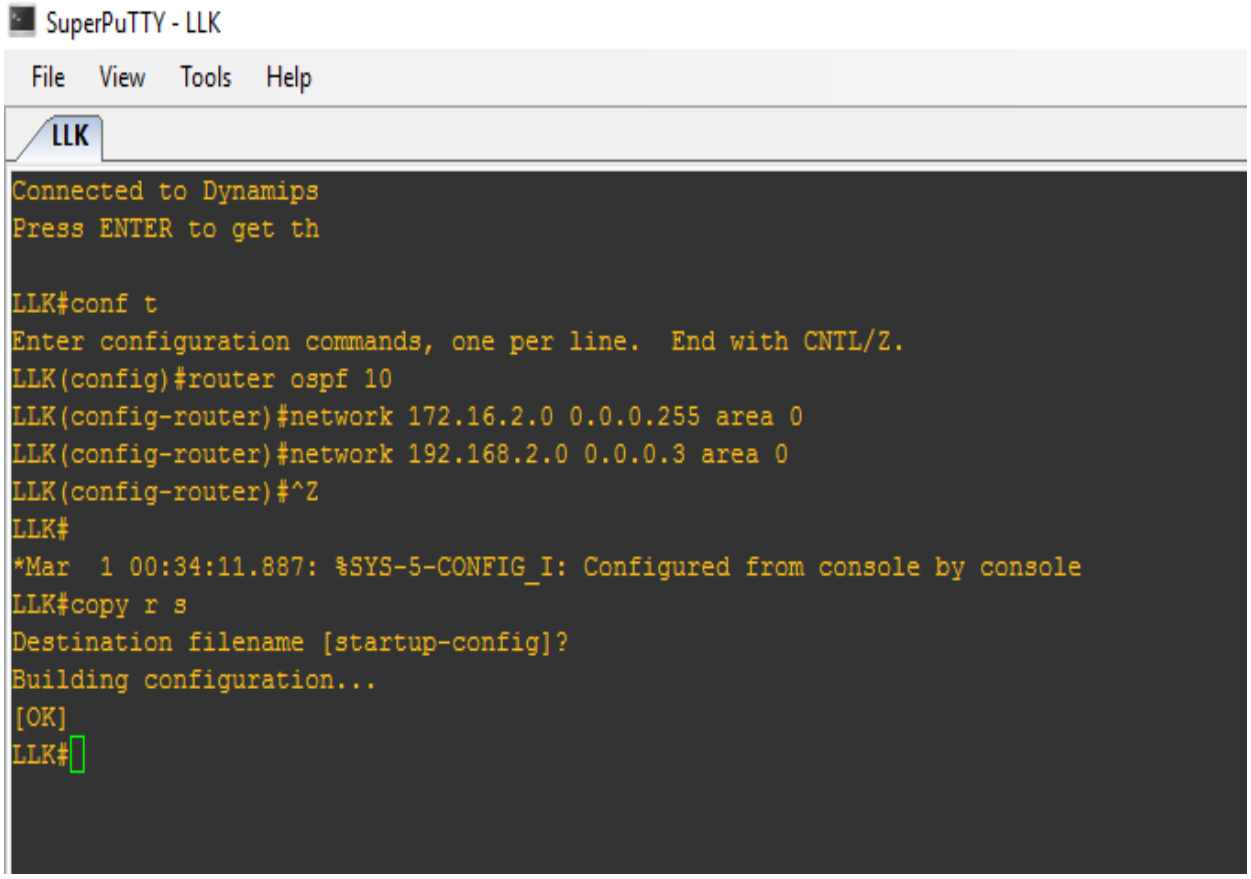

Figure 19 : routage OSPF sur le routeur LLK.

3.3.1.3 Site Cojek

Un routeur Cisco de gamme 3725 est utilisé dont les interfaces suivantes sont activées :

fo/o : 172.16.3.254/24 (reliée au réseau local)

fo/1 : 192.168.3.2/30 (reliée au backbone Operateur).

Loopback o : 3.3.3.3/32

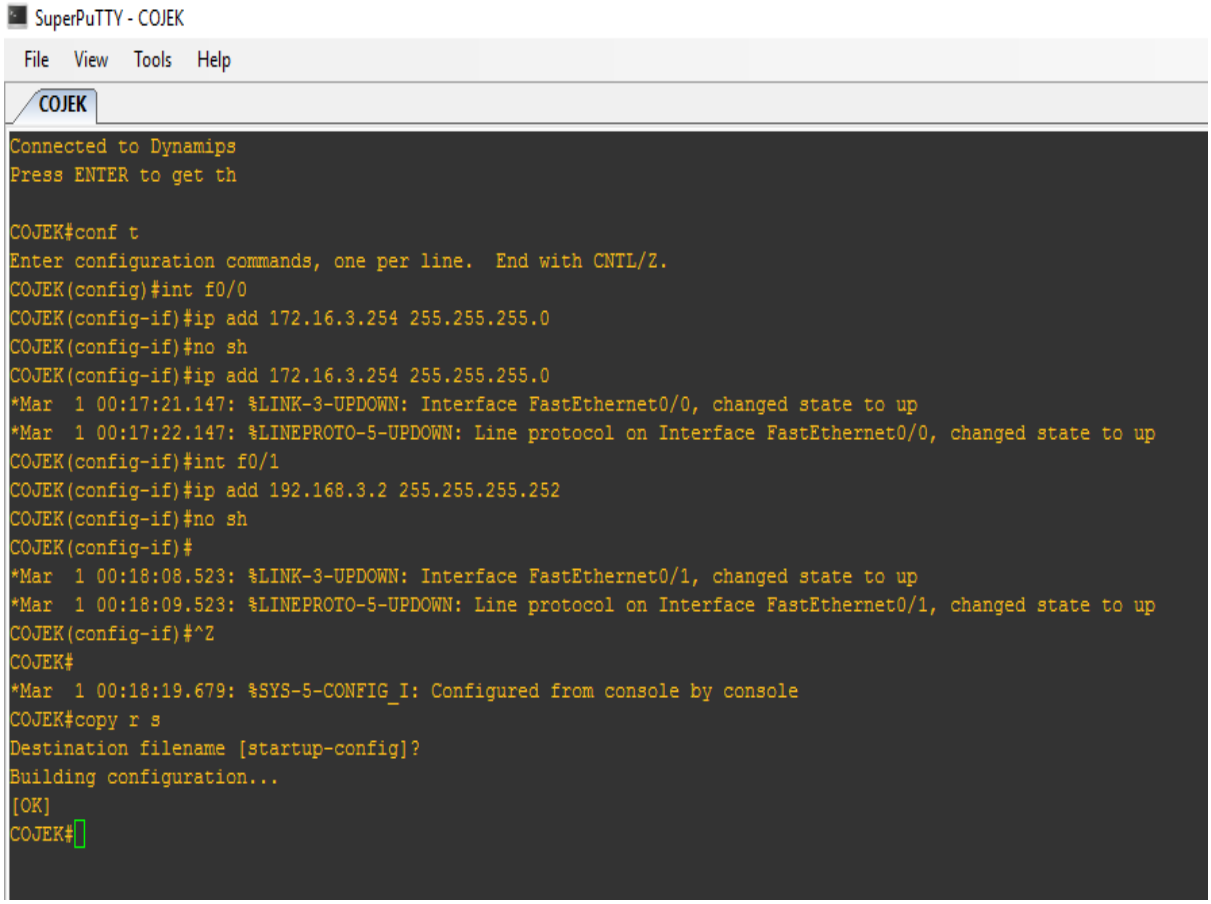

Figure 20 : Attribution des adresses aux interfaces du routeur COJEK.

Le protocole de routage OSPF employé :

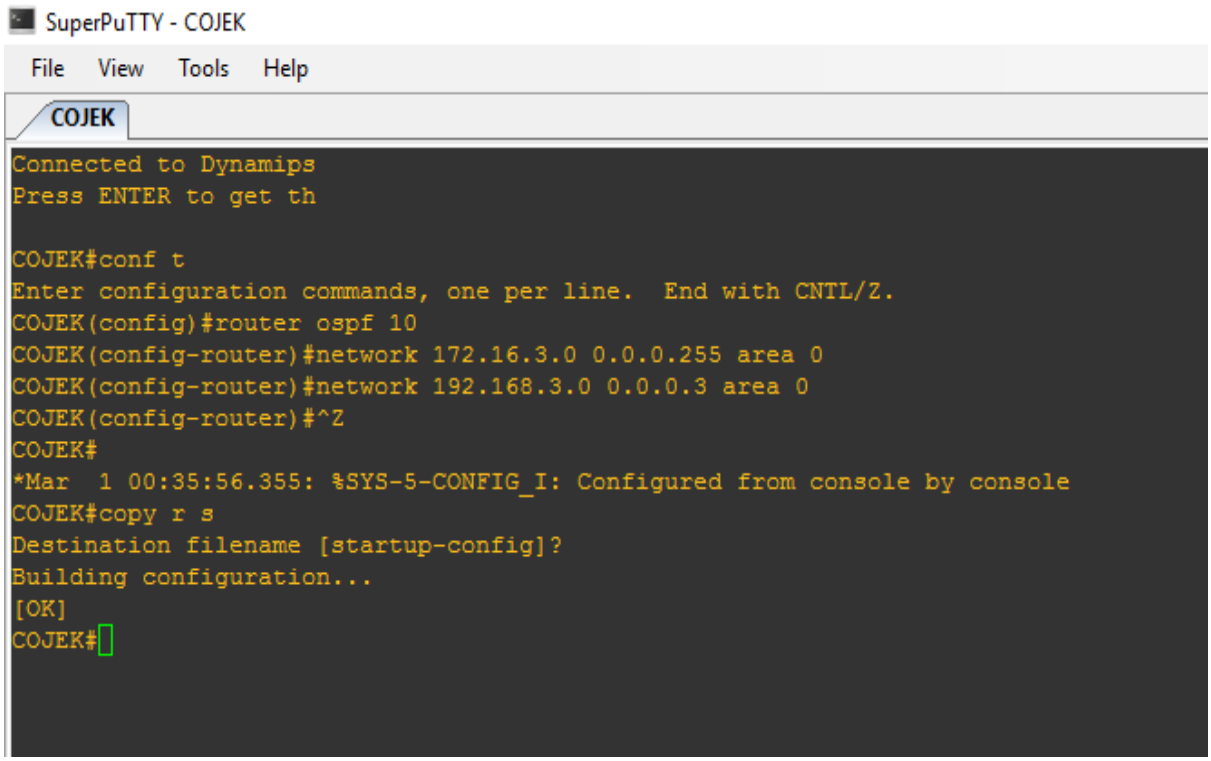

Figure 21 : routage OSPF sur le routeur COJEK.

3.3.1.4 Site Elkharoub

Comme pour les sites précédents, le routeur avec gamme 3725 est utilisée, où les liaisons FastEthernet avec les interfaces suivantes ont été activées :

f0/0 : 172.16.4.254/24 (reliée au réseau local)

f0/1 : 192.168.4.2/30 (reliée au backbone Operateur).

Loopback 0 : 4.4.4.4/32

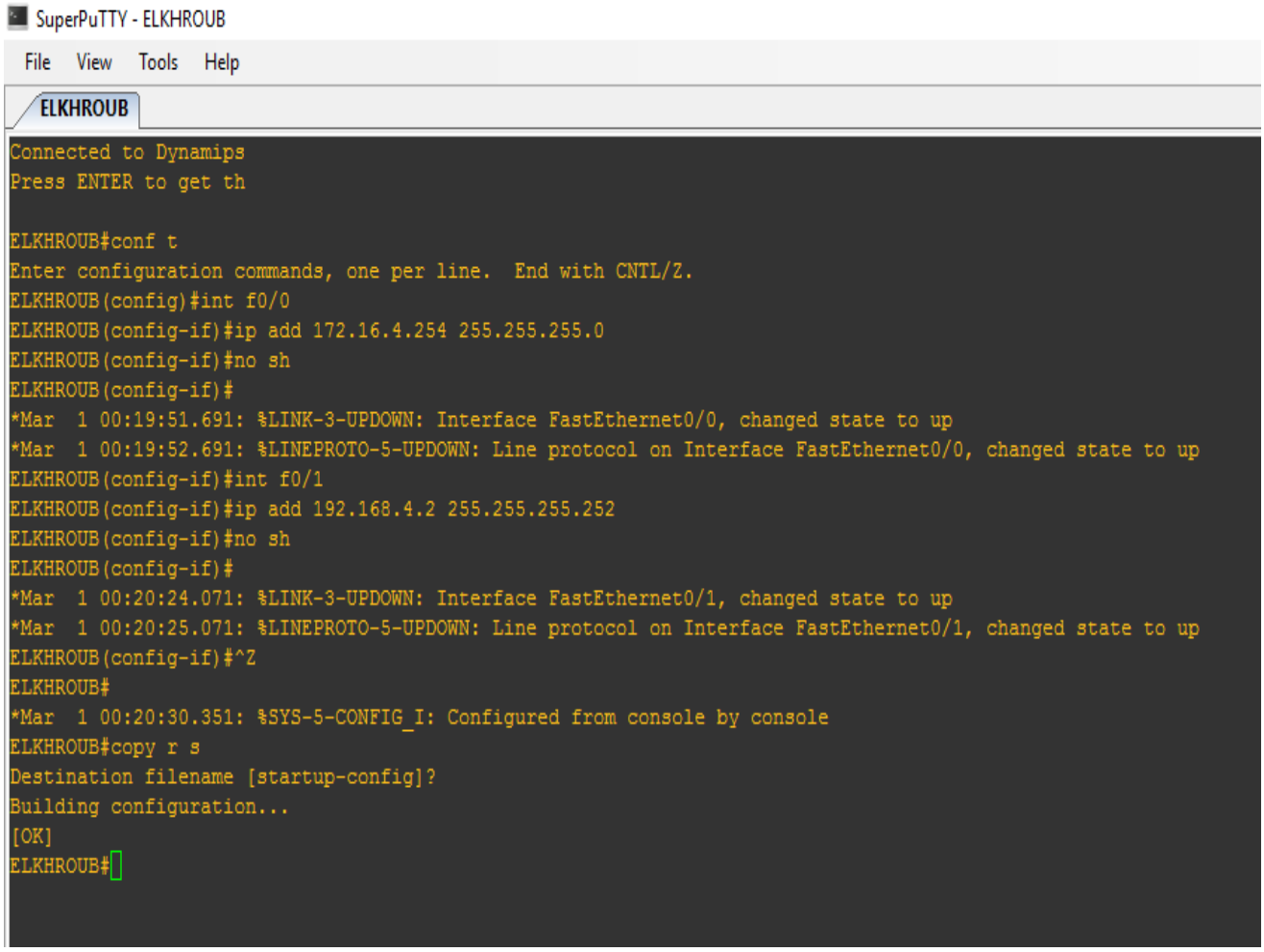

Figure 22 : Attribution des adresses aux interfaces du routeur ELKHROUB.

Comme les trois sites précédents le routage OSPF est utilisé :

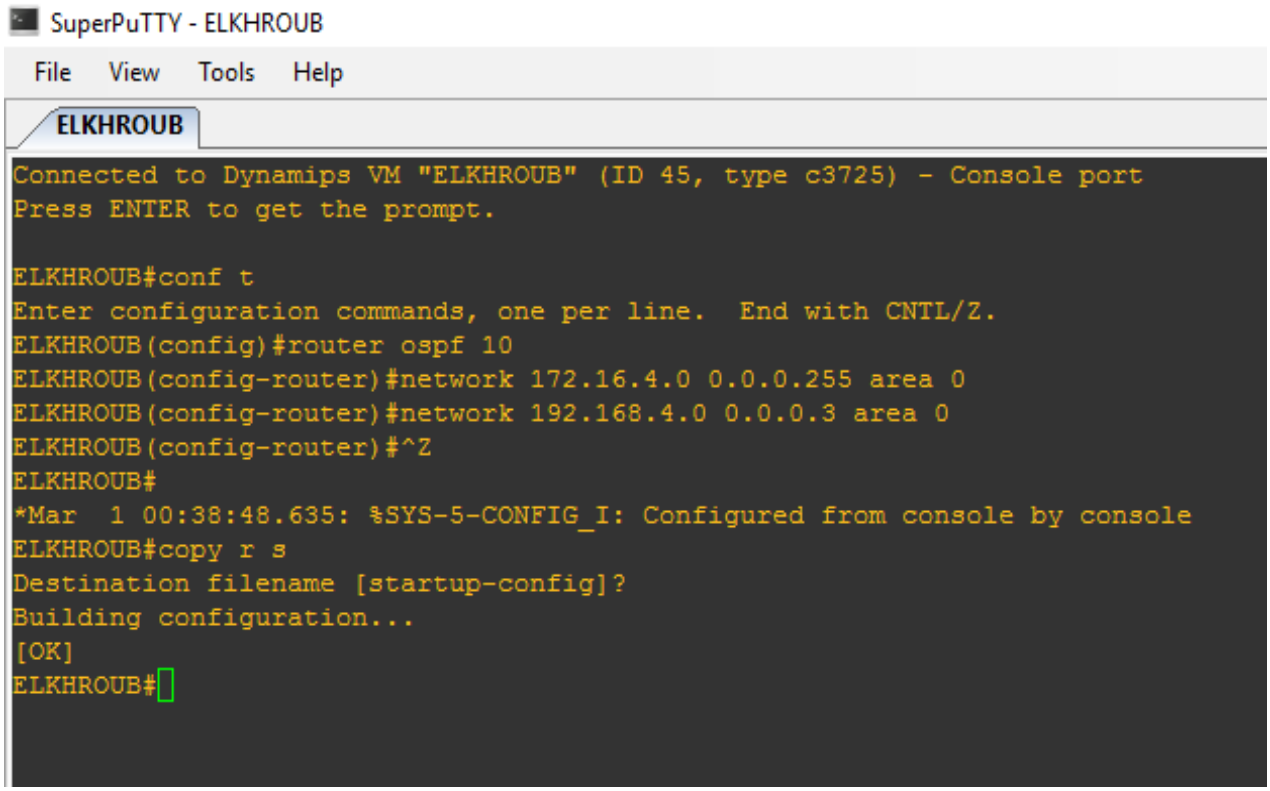

Figure 23 : routage OSPF sur le routeur ELKHROUB.

Après avoir réalisé la configuration sur les quatre sites en utilisant le routage dynamique avec le protocole OSPF (Open Shortest Path First) nous allons passer à l'activation de MPLS (Multi Protocol Layer Switching) sur le réseau backbone de l'opérateur afin d'avoir une architecture similaire au cas réel de celle de l'entreprise Cevital.

3.3.1.5 Vérification du routage

- Afin de pouvoir effectuer un test du routage, on lance un ping à destination de la passerelle du réseau local connecté à l'interface du routeur COJEK, le resultat est montré dans la figure suivante :

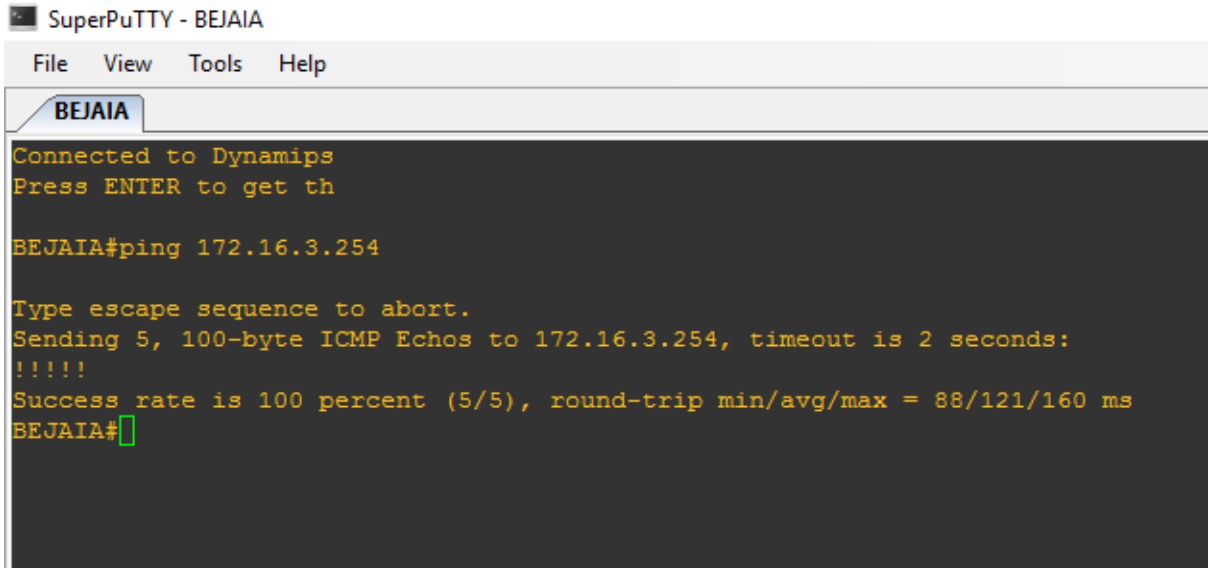

Figure 24: résultat d'une requête ICMP de BEJAIA vers COJEK.

Et un autre ping destiné à l'interface d'entrée du routeur ELKHROUB. Le resultat est montré à la figure suivante :

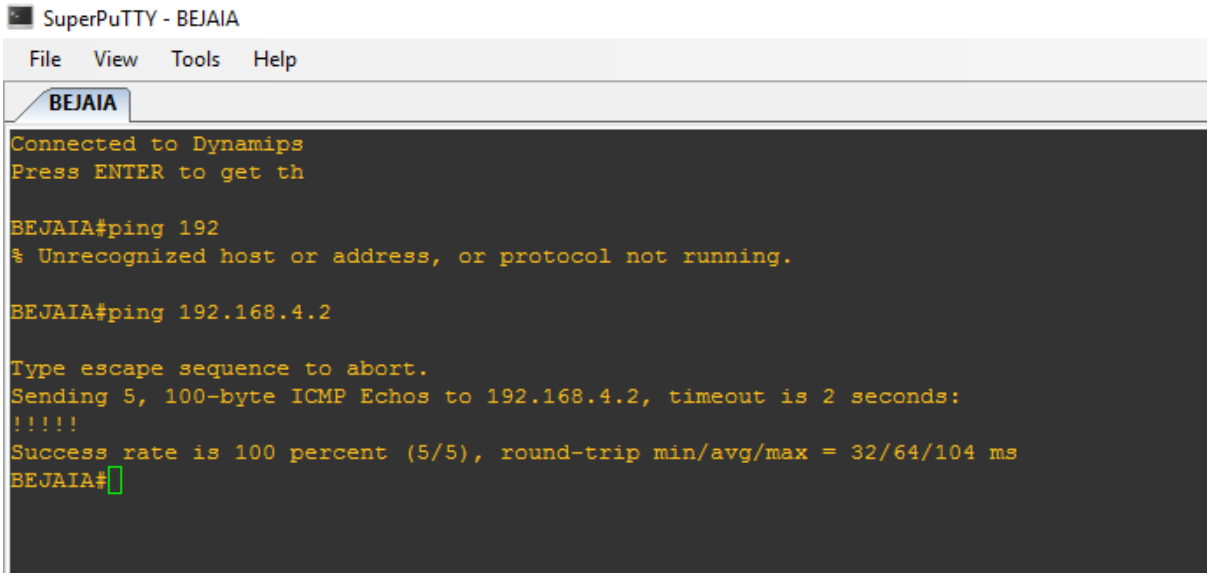

Figure 25: résultat d'une requête ICMP de BEJAIA vers ELKHROUB.

Avec une capture Wireshark (figure 25) :

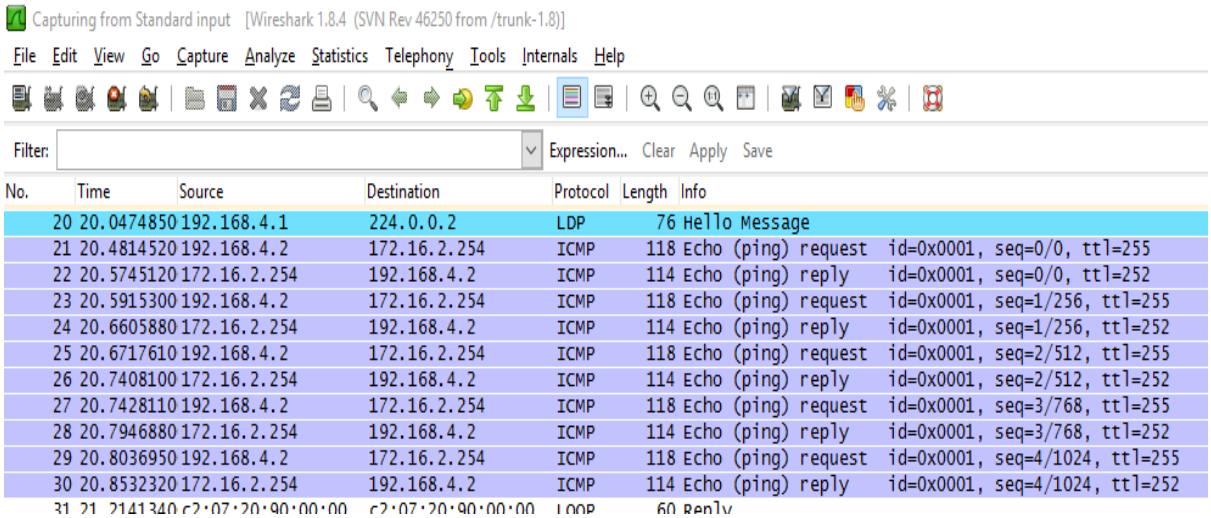

Figure 26 : résultat d'une requête ICMP sous Wireshark.

On remarque, après un ping, des échanges de messages entre les deux routeurs ELKHROUB (192.168.4.2) et LLK (172.16.2.254) grâce au protocole ICMP .

3.3.2 Activation de MPLS

Nous allons d'abord activer le protocole MPLS (le routage est déjà fait avec OSPF) sur les quatre routeurs du backbone de l'opérateur, nommés MPLS1, MPLS2, MPLS3, MPLS4.

Exemple d'activation sur l'un des routeurs(MPLS1) :

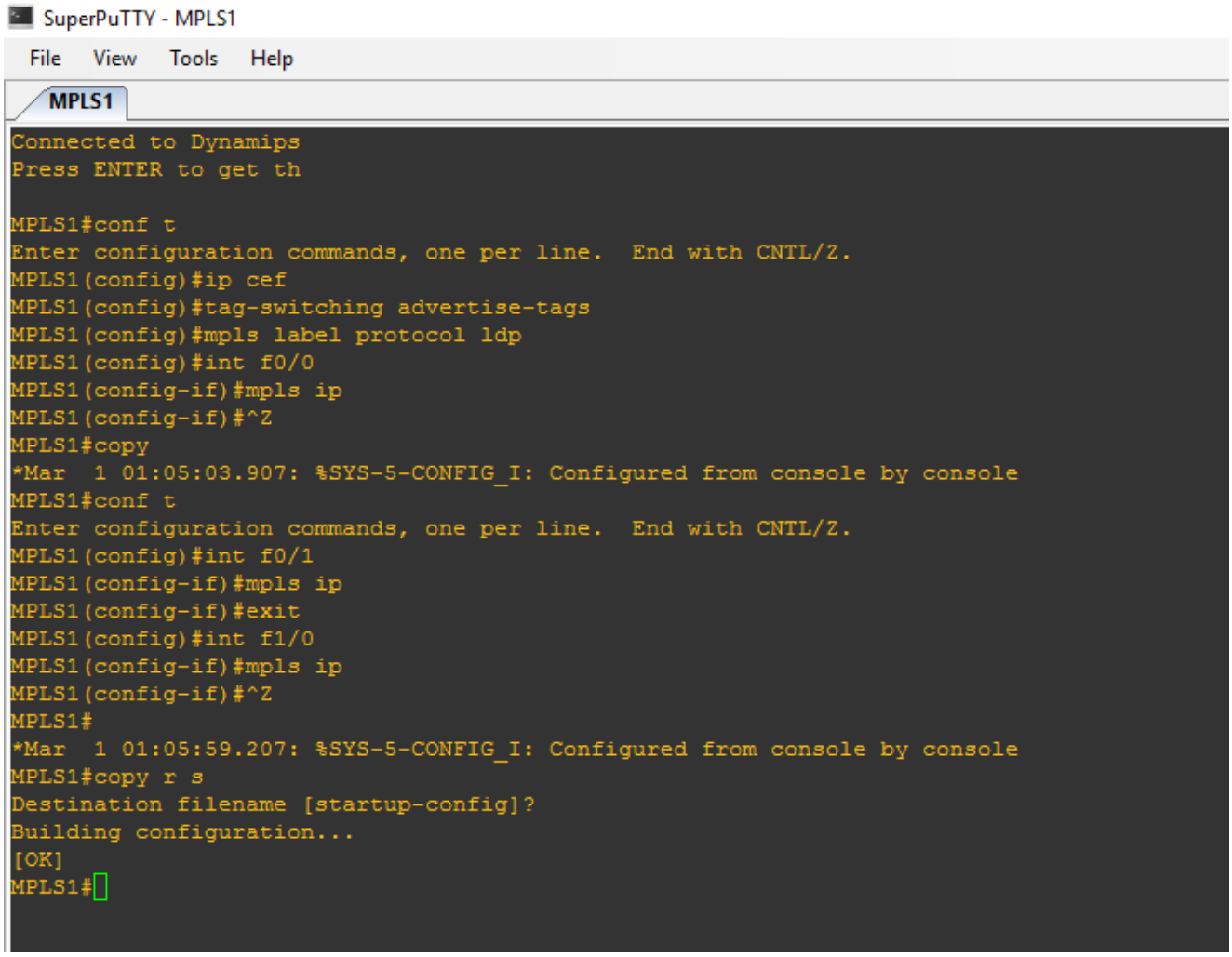

Figure 27 : Activation du MPLS sur le routeur MPLS1.

ip cef : permet d'activer Cisco Express Forwarding.

tag-switching advertise-tags : active MPLS et démarre la distribution des labels.

mpls label protocol ldp : permet d'utiliser le protocole LDP pour la distribution des labels.

mpls ip : permet d'encapsuler les paquets avant de les envoyer (doit être activer sur toutes les interfaces de sorties sauf celles connectées directement aux réseaux locaux).

3.3.2.1 Vérification du fonctionnement de MPLS

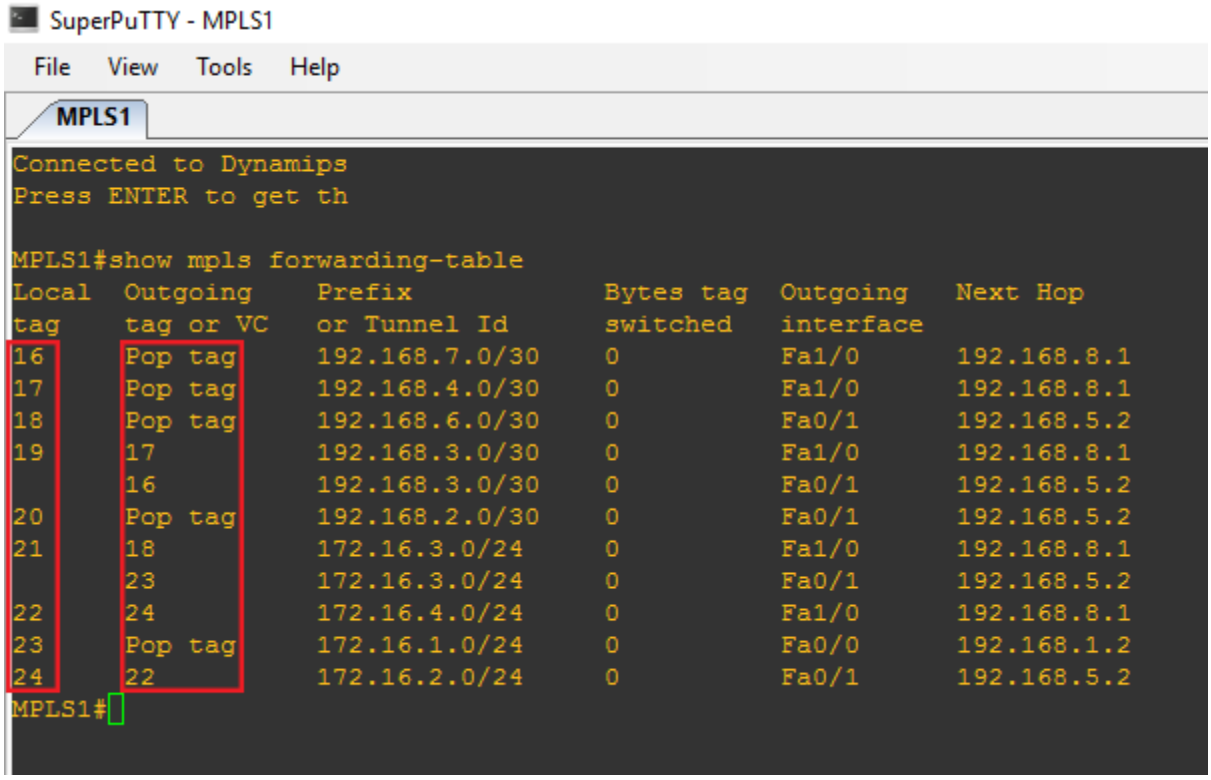

Figure 28 : Vérification de l'activation de MPLS sur le routeur MPLS1.

On aperçoit sur la figure que MPLS fonctionne sur les interfaces de sorties avec la commande « **show mpls forwarding-table** ».

PS : La configuration est la même pour les trois routeurs restants, à savoir MPLS2,MPLS3 et MPLS4

3.3.3 Création des VPNs site-à-site

Nous avons au total six VPNs, soit trois VPNs dans le routeur central Bejaia et un seul VPN sur chacun des autres sites (Lalla Khedija-Cojek-Elkhroub).

On passera à la création des tunnels VPNs entre les différents sites :

On aura trois tunnels VPN, donc six VPNs :

- Tunnel entre le site principal de Bejaia et le site Lalla Khedija (Tizi-Ouzou)
- Tunnel entre le site principal de Bejaia et le de Cojek(Elkseur)
- Tunnel entre le site principal de Bejaia et le site Elkhroub (Constantine)

Dans ce qui suit nous allons montrer la création du tunnel entre le site de BEJAIA et le site Lalla Khedidja abrégé LLK.

Nous allons procéder en quatre étapes :

- **Prémiere étape :** Activation du protocole ISAKMP : avant d'entamer la création des VPNs, nous devons activer le protocole qui gére l'échanges des clés qui seront utilisées entre les deux extrémités du tunnel.

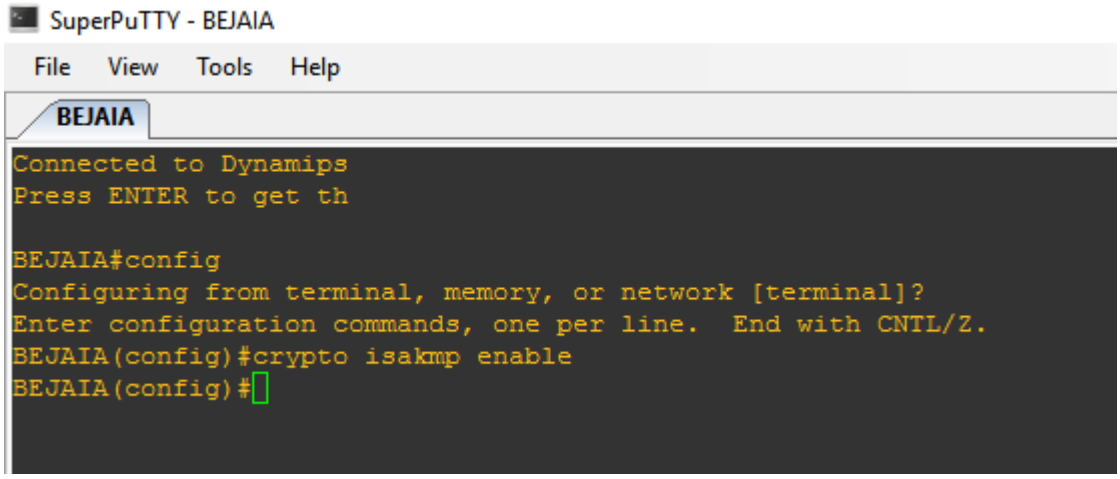

Figure 29 : Activation du protocole ISAKMP.

- **Deuxième étape :** créer la policy-map : il s'agit d'une stratégie de la gestion de négociation des clés et l'établissement de la liaison VPN.

Pour ceci il faut prendre en considération les éléments suivants :

Policy : qui définit la politique de connexion pour les SA (Security Association) de ISAKMP. Un numéro indiquant la priorité de l'utilisation lui est attribué à la fin de la commande.

Encryption: l'algorithme de chiffrement utilisé est aes.

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

Sha : l'algorithme de hachage.

Groupe 2 : L'algorithme d'échange de clef Diffie-Hellman est utilisé, par defaut c'est le groupe 1 qui est utilisé (768 bits), dans notre cas nous avons utilisé le groupe 2 (1024 bits).

86400 : est la durée de vie de la clé de session (en secondes).

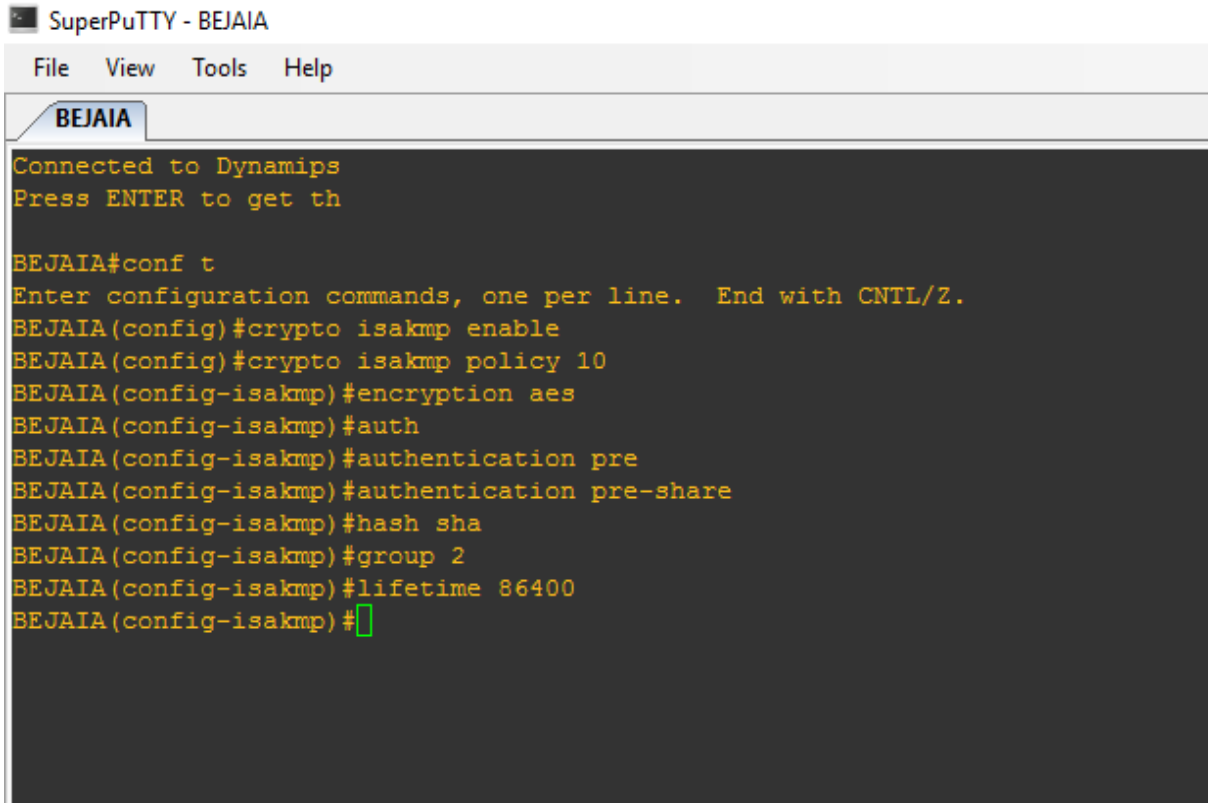

Figure 30 : Création d'une strategie de negociation de clés.

- **Troisième étape :** création de la clé pré-partagée (pre-shared key) VPN_VEVITAL.

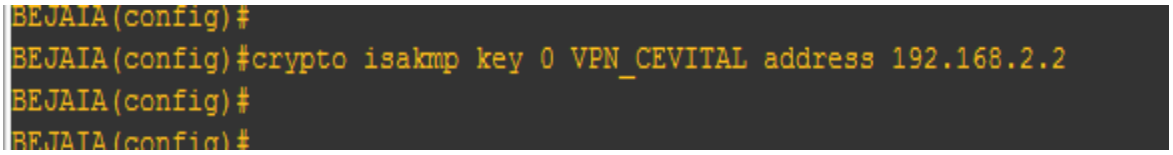

Figure 31 : création de la clé pré-partagée**.**

Le 0 signifie que la clé est definie en texte clair et qu'elle est associée à l'adresse 192.168.2.2

- **Quatrieme etape :** configuration d'IPsec :

Pour configurer IPsec les elements suivantes doivent etre configurées dans l'ordre.

Phase 1 : configurer la methode de cryptage des données « transform-set », que l'on nomme VPNSET.

PS : esp-aes est la methode de cryptage, esp-sha-hmac est la methode d'authentification.

```
BEJAIA(config)#
BEJAIA(config)#crypto ipsec tr
BEJAIA(config)#crypto ipsec transform-set VPNSET esp
BEJAIA(config)#crypto ipsec transform-set VPNSET esp-sh
BEJAIA(config)#crypto ipsec transform-set VPNSET esp-sha-hmac
Proposal with ESP is missing cipher
BEJAIA(config)#crypto ipsec transform-set VPNSET esp-aes esp-sha-hmac
BEJAIA(cfg-crypto-trans)#ex
BEJAIA(config)#
```

Figure 32 : configuration de la transform-set**.**

Phase 2 : definition de la durée de vie de la clé partagée, la durée de est exprimée en kilobytes (4096).

```
BEJAIA(config)#
BEJAIA(config)#crypto ipsec se
BEJAIA(config)#crypto ipsec security-association lifetime kil
BEJAIA(config)#crypto ipsec security-association lifetime kilobytes 4096
BEJAIA(config)#
BEJAIA(config)#
```

Figure 33 : définition de la durée de vie des clés**.**

Phase 3 : on crée les access-lists qui serviront à définir le trafic à trier par le tunnel VPN.

```
BEJAIA(config)#
BEJAIA(config)#ip acc
BEJAIA(config)#ip acces
BEJAIA(config)#ip access-list exten
BEJAIA(config)#ip access-list extended VPN
BEJAIA(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
BEJAIA(config-ext-nacl)#ex
BEJAIA(config)#
BEJAIA(config)#
```

Figure 34 : création des ACL**.**

Phase 4 : il ne reste qu'à rassembler tous ces éléments dans une crypto-map, qu'on a nommée BEJAIA_LLK.

Cette crypto-map est activée pour le trafic correspondant à l'access-list VPN Destination du tunnel 192.168.2.2, qu'on a activé selon la transform-set VPNSET

PS : 10 est le numéro de séquence de la crypto-map.

```
BEJAIA(config)#
BEJAIA(config)#crypto map BEJAIA_LLK 10 ipsec
BEJAIA(config)#crypto map BEJAIA_LLK 10 ipsec-is
BEJAIA(config)#crypto map BEJAIA_LLK 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
BEJAIA(config-crypto-map)#set peer 192.168.2.2
BEJAIA(config-crypto-map)#set tr
BEJAIA(config-crypto-map)#set transform-set VPNSET
BEJAIA(config-crypto-map)#EX
BEJAIA(config)#
```

Figure 35 : création de la crypto-map **.**

Phase 5 : application de la crypto-map à l'interface de sortie du routeur

```
BEJAIA(config)#int f0/1
BEJAIA(config-if)#crypto map BEJAIA_LLK
BEJAIA(config-if)#
*Mar  1 00:34:17.015: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
BEJAIA(config-if)#^Z
BEJAIA#
*Mar  1 00:34:22.107: %SYS-5-CONFIG_I: Configured from console by console
BEJAIA#copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
BEJAIA#
```

Figure 36 : Application de la crypto-map**.**

-pour le site LLK les mêmes étapes et les mêmes paramètres sont appliqués, la seule différence est d'inverser la création des access-list et les adresses d'entrée et de sortie sur les routeurs.

3.4 Vérification du tunnel VPN

Afin de tester la création de nos VPNs, on va vérifier la création des éléments créés précédemment :

3.4.1 Vérification du transform-set

```
BEJAIA#show crypto ipsec transf
BEJAIA#show crypto ipsec transform-set
Transform set VPNSET: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

Figure 37: vérification de la transform-set.

transform-set esp-aes utilise uniquement aes pour le chiffrement et sha pour l'authentification des paquets avec esp. le transform-set « «VPNSET » utilise sha pour

l'authentification des paquet, aes pour le chiffrement esp . la transformation utilise le mode tunnel.

3.4.2 Vérification de la crypto-map

A l'aide de la commande « show crypto map », nous allons pouvoir tester la creation de la crypto-map, cette commande verifie la configuration et montre la durée de vie de SA

```
BEJAIA#show crypto map
Crypto Map "BEJAIA_LLK" 10 ipsec-isakmp
        Peer = 192.168.2.2
        Extended IP access list VPN
            access-list VPN permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
        Current peer: 192.168.2.2
        Security association lifetime: 4096 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPNSET,
        }
        Interfaces using crypto map BEJAIA_LLK:
                FastEthernet0/1


BEJAIA#
```

Figure 38: verification de la crypto-map.

Ici, la crypto « BEJAIA_LLK » englobe tous les elements créés auparavant, à savoir les access-lists, les transform-set et l'interface assignée à la crypto-map.

3.4.3 Verification des parametres IPsec :

On vérifie les paramètres de de IPsec avec la commande « **show crypto ipsec sa** », le résultat est présenté dans la figure ci-dessous.

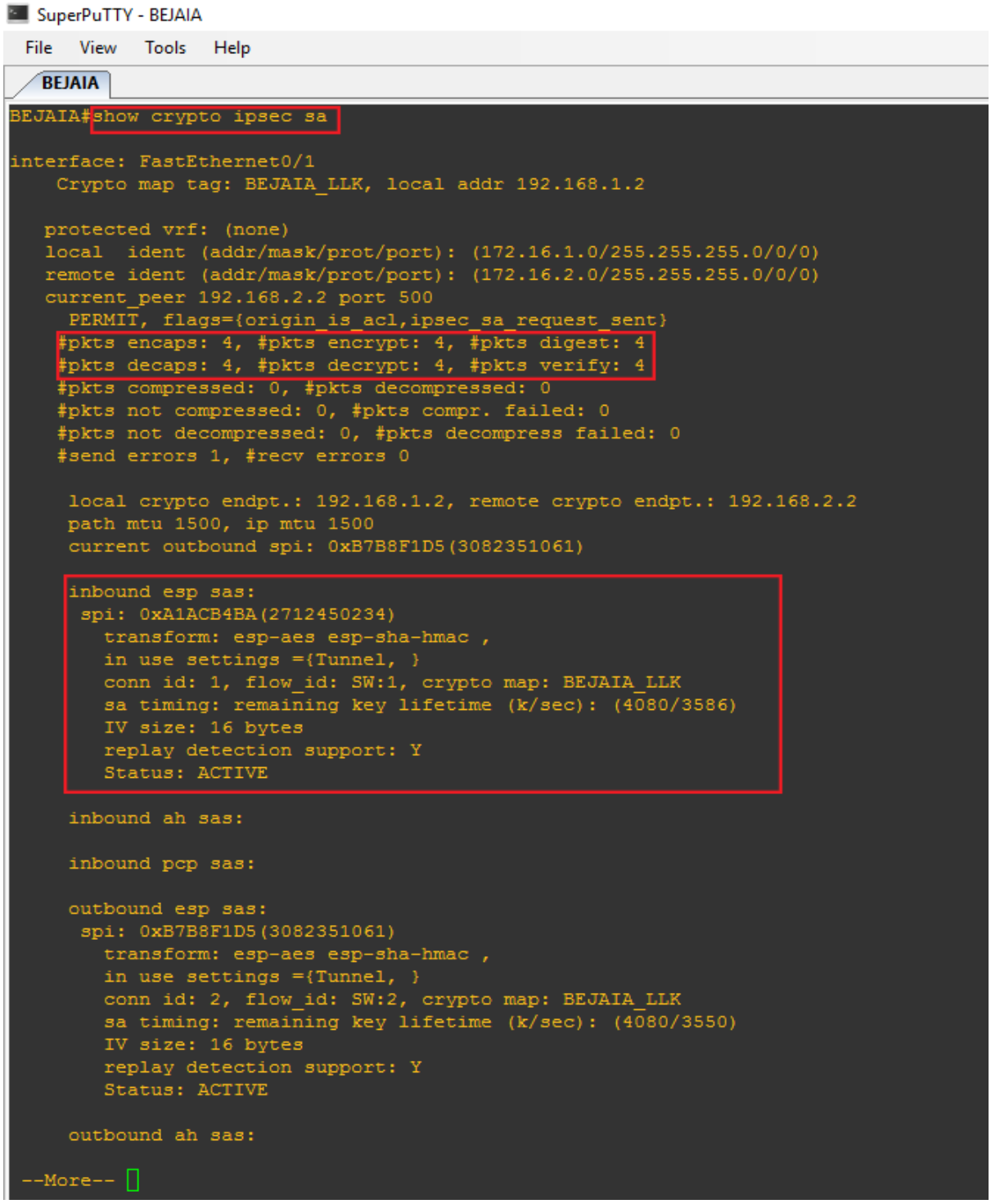

Figure 39 : verification des parametres IPsec.

3.4.4 Verification des operations ISAKMP

```
BEJAIA#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.2.2     192.168.1.2     QM_IDLE           1001    0 ACTIVE

IPv6 Crypto ISAKMP SA

BEJAIA#
```

Figure 40 : verification des operations d'ISAKMP.

On aperçoit sur la figure ci-dessus, que les opérations de ISAKMP sont activées entre les deux extrémités du tunnel BEJAIA (192.168.1.2) et LLK(192.168.2.2).

- Et on termine avec un test avec Wireshark, qui nous montre clairement que le trafic est bel et bien crypté avec le protocole ESP.

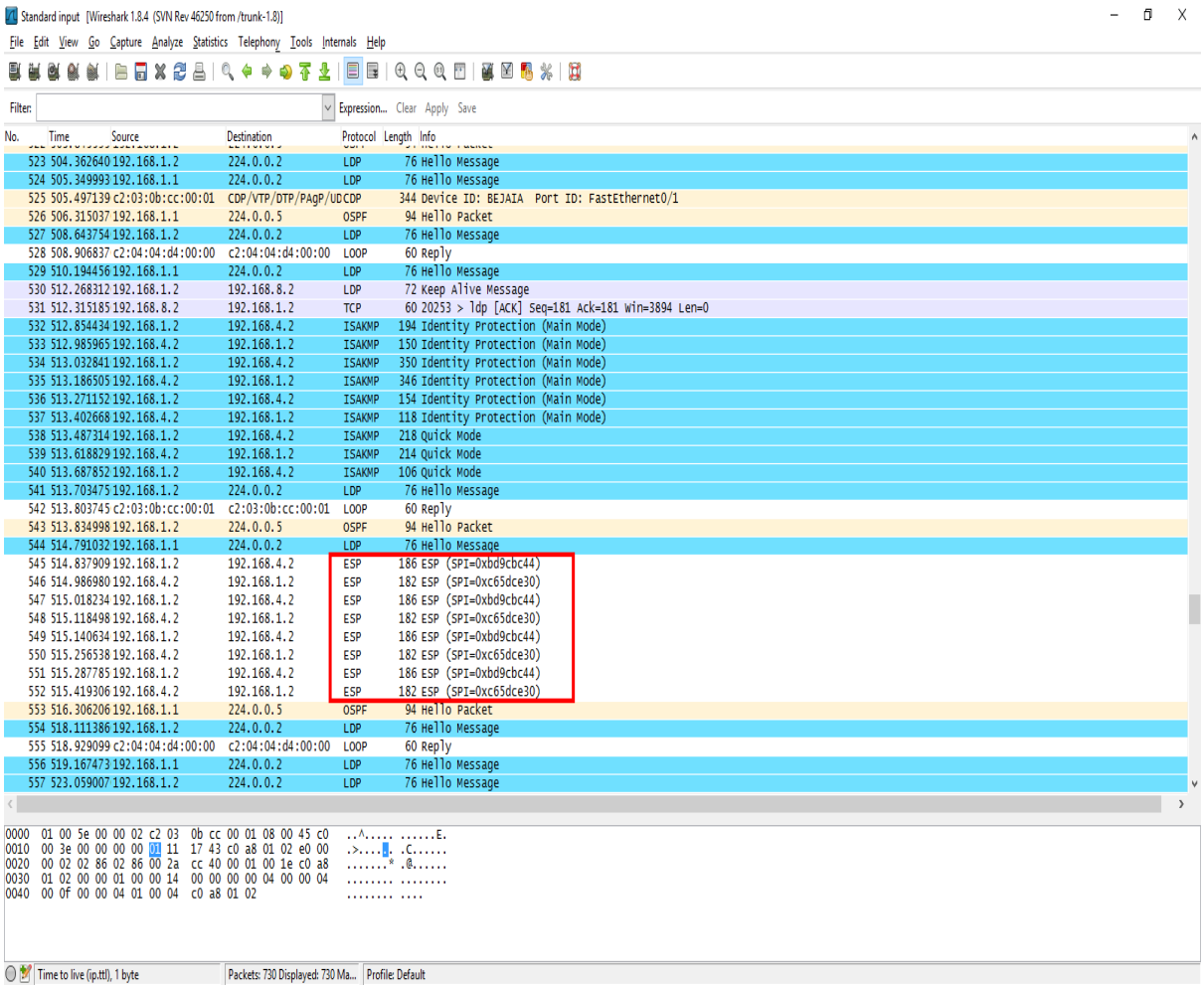

Figure 41 : resultat avec Wireshark

Conclusion

Dans ce chapitre Nous avons configuré une liaison VPN site-à-site sécurisé grâce au protocole IP sec, le chiffrement des données avec AES et les clés pré-partagées entre les différents sites; après avoir bien défini la topologie du réseau et le routage avec OSPF.

Cette solution est réalisée sous l'émulateur GNS3 qui permet l'utilisation des équipements réseaux réels (routeurs, fire-walls .....etc.).

Conclusion Générale

Lors de la transmission et la réception de données entre des différentes entités, sois au sein d'une même entreprise ou avec l'extérieur, garantir la transparence et le concept de confidentialité devient un enjeu majeur.

Dans notre travail, nous avons abordé les généralités sur les VPNs et ces fonctionnalités, ainsi le protocole de sécurité le plus utilisé, en l'occurrence IPsec qu'on a implémenté sur notre architecture réseau.

La réalisation de ce travail est faite comme suite :

- Tracer l'architecture réseau adapté à la topologie physique de l'organisme d'accueil déjà existante, où on a utilisé le routage dynamique avec le protocole OSPF.
- Activation du protocole MPLS sur le réseau backboone de l'opérateur (ooredoo), dans le but de coïncider avec le cas réel.
- Création des VPNs entre le site central de Bejaia et les trois autres sites.

Ce travail a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en termes de configuration dans un environnement GNS3. De plus nous avons enrichi nos connaissances déjà requise dans le domaine de la sécurité informatique notamment la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau privé virtuel (VPN).

Par contrainte de temps nous avons seulement implémenté le protocole IPSEC (site_to_site).

En termes de perspectives, nous envisagerons d'implémenter le protocole L2TP/IPSEC

Pour l'accès a distance que nous souhaitons réaliser. Nous visons aussi l'utilisation de système RADIUS qui est un protocole client/serveur permettant de centraliser des données d'authentification et de définir les accès d'utilisation au réseau.

Références bibliographiques

Ouvrages :

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

[3]A. VAUCAMPS, « Sécurité des routeurs et contrôle du trafic réseau », éditions eni, 2010**;**

[8] Joseph Gehring, "Software Projects with Computer Networks",CNT 4104,Florida Gulf Coast University, Fall 2011;

[13] A. ROUX , D. SEBA, «Cisco, Maitrisez la configuration des routeurs et des commutateurs », editions eni, date de parrution 19/12/2005 EAN : 9782746030503

Rapports:

[2] brochure d'accueil CEVITAL.

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

Sites Web:

[1] http://www.cevital.com/fr/cevital-agro-industrie.html, consulté le 27/04/2016.

[4] http://www.cisco.com/c/en/us/products/switches/index.html, consulté le 03/05/2016 ;

[5]https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html, consulté le 03/05/2016 ;

[6] http://www.cisco.com/c/en/us/products/interfaces-modules/ip-vsat-satellite-wan-module/index.html, consulté le 03/05/2016 ;

[9]http://icourse.cuc.edu.cn/computernetworks/cisco/Simulator/Dynamips /GNS3-0.4_documentation.pdf

[10] http://wallu.pagesperso-orange.fr/pag-mpls.htm

[11] QEMU, http ://fr.wikipedia.org/wiki/QEMU, date de consultation Mai 2016, consulté le 02/05/2016 ;

[14] http://icourse.cuc.edu.cn/computernetworks/cisco/Simulator/Dynamips/GNS3-0.4_documentation.pdf

Résumé

La sécurité des données est un paramètre très important voire crucial au sein d'une organisation, compte tenu des échanges d'informations qui se font au quotidien.

A cet effet, pour une entreprise possédant plusieurs sites distants, afin de sécuriser au mieux les communications entre ces derniers et les rendre transparentes à une entité étrangère, plusieurs techniques et concepts sont apparus à savoir les VPNs.

Nous nous sommes opté pour la création de VPNs site à site pour interconnecter les sites de l'entreprise CEVITAL, et ce en se basant sur le protocole IPSec dans son mode tunnel.

Dans notre projet, nous avons travaillé dans l'environnement de simulation GNS3 dans la réalisation.

Notre travail est divisé en trois parties : la première est la présentation du cadre du projet, notamment le réseau de l'entreprise CEVITAL. « aspects théoriques relatifs aux réseaux locaux virtuels. La deuxième est la présentation des aspects théoriques relatifs aux Réseaux Virtuels Privés. La troisième partie est la mise en œuvre comportant la simulation des VPNs créés.

Mot clés : Tunnel, IPSec, VPN, Sécurité, implémentation, Simulation, MPLS .

Abstract

The safety of the data is very a very important parameter even crucial within an organization, considering the information exchanges which are made on a daily basis.

For that purpose, for a company possessing several distant sites, to secure at best the communications between the latter and make them transparent to a foreign entity, several techniques and concepts appeared, namely the VPNs.

We were opted for the creation of VPNs site-to-site in order to interconnect the sites of the Company CEVITAL, by basing it on the protocol IPSec in its tunnel mode.

In our project, we worked in the environment of simulation GNS3in the realization.

Our work is divided into three parts: the first on is the presentation of the project, including the network of the company CEVITAL. The second is the presentation of the theoretical aspects of Virtual Private Networks. The third part is the implementation including simulation of the created VPNs.

Key words: Tunnel, IPSec, VPN, Safety, implementation, Simulation, MPLS.