Université Abderrahmane Mira –Bejaia

Faculté des Sciences Exactes

Département d'Informatique

Option Administration et sécurité des réseaux

Mémoire de fin de cycle

En vue de l'obtention du Diplôme de Master professionnel en Informatique
Option : Administration et Sécurité des Réseaux

Thème :

Interconnexion et ségmentation des sites distants –VPN et VLAN- Cas d'étude : SCS

Réalisé par:

M^{elle} OUHNIT Meriem

M^{elle} SALMI Mounia

Setenu devant le jury composé de :

Président : Dr AMROUN Kamal

Encadreur : Pr TARI Abdelkamal

Encadreur : Mr ELSAKAANE Nadim

Examinatrice : Mme BENNAI Sofia

Examinatrice : Mme TAMITI Kenza

Année universitaire : 2017/2018

Remerciements

Avant d'entamer ce projet de fin de Formation, nous tenons à exprimer notre sincère gratitude envers tous ceux qui nous ont aidés ou ont participé au bon déroulement de ce projet.

Nous sommes particulièrement reconnaissants à :

Encadreur : Mr ELSAKAANE Nadim

Encadreur: Pr TARI A.Kamel

D'avoir accepté de diriger notre travail qui nous a beaucoup aider, nous les remercions pour leurs qualités humaines et professionnelles, pour leurs patiences, leurs directives, leurs remarques constructives et leurs aides inestimables.

Nos remerciements vont également à l'ensemble du personnel du district (SCS) de Bejaia, pour l'aide et tous les moyens qu'ils nous ont offert.

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

Merci à tous

Dédicace

A la mémoire de mon père que Dieu l'accueille en son vaste paradis,

A ma mère, nulle dédicace n'est susceptible de vous exprimer ma profonde affection, mon immense gratitude pour tous les sacrifices que vous avez consacrés pour moi.

A mes chères sœurs que j'aime plus que tout au monde.

A mes frères et mon beau frère.

A mes chères nièces et mes chers neveux.

A toute ma famille.

A mon binôme et toute sa famille.

A tout mes amis (es).

Mounia Salmi.

A mes cher parents qui m'ont soutenus et donner la force et la volonté durant ma scolarité.

A mes sœurs et frères.

A mes beaux frères et belles sœurs.

A mes chers neveux et chères nièces.

A toute ma famille.

A mon binôme et toute sa famille.
A tout mes amis (es) kahian, salima, mounia, rachida, kenza, lamia, walid, salim, sliman,…...

Meriem Ouhnit.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AES **A**dvanced **E**ncryption **S**tandard

AH **A**uthentication **H**eader

ACL **A**ccess **C**ontrol **L**ist

ARP **A**ddress **R**esolution **P**rotocol

DES **D**ata **E**ncryption **S**tandard

DOS **D**enial **O**f **S**ervice

DSA **D**igital **S**ignature **A**lgorithm

ESP **E**ncapsulation **S**ecurity **P**ayload

EIGRP **E**nnhanced **I**nterior **G**ateway **R**outing **P**rotocol

FAI **F**ournisseur **A**ccès **I**nternet

GNS3 **G**raphical **N**etwork **S**imulator

IKE **I**nternet **K**ey **E**xchange

ISO **I**nternational **S**tandards **O**rganisation

IP **I**nternet **P**rotocol

IPSec **I**nternet **P**rotocol **S**ecurity

ICMP **I**nternet **C**ontrol **M**essage **P**rotocol

ISAKMP **I**nternet **S**ecurity **K**ey **M**anagement **P**rotocol

LACP **L**ink **A**ggregation **C**ontrol **P**rotocol

LAN **L**ocal **A**rea **N**etwork

MAN **M**etropolitain **A**rea **N**etwork

MD5 **M**essage **D**igest5

OSI **O**pen **S**ystem **I**nterconnect

PAN **P**ersonal **A**rea **N**etwork

QoS **Q**ualité **O**f **S**ervice

RSA Ronald **R**ivest, Adi **S**hamir et Leonard **A**dleman

SA **S**ecurity **A**ssociation

SAD **S**ecurity **A**ssociation **D**tabase

SCS **S**oummam **C**omputer **S**ystem

SHA **S**ecurity **H**ash **A**lgorithm

SP **S**ecurity **P**olicy

SPD **S**ecurity **P**olicy **D**atabase

SPI **S**ecurity **P**arameter **I**ndex

TCP **T**ransfer **C**ontrol **P**rotocol

UDP **U**ser **D**atagram **P**rotocol

VLAN **V**irtual **L**ocal **A**rea **N**etwork

VPN **V**irtual **P**rivate **N**etwork

VTP **V**lan **T**runk **N**etwork

Introduction générale

De nos jours, l'internet est considéré comme la plus grande source d'information qui existe au monde. Toute entreprise ou établissement ayant un accès à cet outil est en possession de diverses informations privées, peuvent être en proie de cyber attaques.

Ces cybers attaques ont pour but d'interrompre le fonctionnement d'un réseau informatique, d'intercepter et modifier les informations.

Afin qu'on puisse éviter les risques de ces attaques, il faut impérativement garantir une sécurité du réseau informatique de l'entreprise et le rendre moins vulnérable. L'objectif de notre projet est de mettre en exécution un mécanisme de sécurisation de données ainsi que leurs échanges entre deux réseaux locaux de l'entreprise SCS. En plus, il est nécessaire de segmenter le réseau local de chaque entreprise en plusieurs LAN virtuels, pour réduire les domaines de collisions et éviter les congestions. Ce qui permet de renforcer la sécurité au niveau du réseau local.

Pour pouvoir atteindre et concrétiser cet objectif, nous avons à notre disposition des solutions de sécurisation, parmi lesquelles, on a opté pour le protocole IPSec qui est le principal outil qui nous permettra d'implémenter les VPN.

Pour bien mener ce travail, nous avons organisé notre mémoire en quatre chapitres structurés comme suit :

Le premier chapitre s'intitule «**Généralités sur les réseaux et la sécurité informatique** » où nous présentons quelques concepts de base des réseaux informatiques et certaines notions sur la sécurité informatique.

Dans le deuxième chapitre titré «**Réseaux privés virtuels**» nous définirons en premier lieu ce qu'est un réseau privé virtuel, ensuite nous parlons de son fonctionnement et de ses objectifs. Nous finirons par citer les différents protocoles de mise en place, principalement l'IPSec, sa compréhension nous aidera dans la réalisation.

Le troisième chapitre nommé «**Etude préalable** » aura pour objectif de mieux comprendre l'organisme et sa structure, nous allons donc évoquer la problématique ainsi que la solution adéquate.

Dans le quatrième et dernier chapitre, nous allons enfin passer à la «**Réalisation**», on premier lieu nous introduirons les outils et logiciels ayant servi à l'élaboration du projet, tout en expliquant les configurations, nous passerons ensuite au deuxième lieu qui sera consacrée à l'implémentation de la solution VPN grâce au protocole IPSec.

Enfin, dans la conclusion générale, nous ferons une récapitulation du travail effectué ainsi que l'expérience acquise.

Introduction

Le besoin de communication et de partage a poussé l'industrie informatique à s'orienter vers les réseaux et travailler d'avantage pour les sécurisés. Dans ce premier chapitre nous allons aborder le concept des réseaux informatiques, ensuite nous allons passer aux différents concepts de la sécurité informatique, ces objectives, les différentes attaques et la sécurité dans les réseaux informatique.

Partie I : généralité sur les réseaux

I.1 Définition

Un réseau informatique, c'est l'ensemble des ressources de communication (matérielles et logicielles), d'ordinateurs et des clients cherchant a exploiter ces ressources afin de répondre a un besoin d'échange d'informations**.**

I.2 Classification de réseaux informatique

Selon la distance maximale reliant deux points, ces réseaux peuvent être classés en quatre catégories [4]

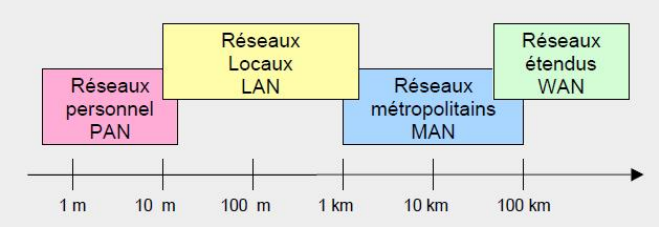


Figure I.1– Classification des réseaux sans fil suivant leur taille

I.2.1 Le réseau personnel

La plus petite étendue de réseau est nommée en anglais Personal Area Network (PAN). Centrée sur l'utilisateur, elle désigne une interconnexion d'équipement informatique dans un espace d'une dizaine de mètres.

I.2.2 Le réseau local (local Area Network)

C'est un réseau de taille supérieure au PAN, s'étendant sur quelques dizaines à quelques centaines de mètres.

I.2.3 Les réseaux MAN (Metropolitan Area Network)

Le réseau métropolitain assure des communications sur de longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizains de kilomètres.

I.2.4 Le réseau étendu

Les étendues des réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constitués de réseau de type LAN, et/ou MAN. Les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN le plus célèbre est réseau publique Internet.

I.3 Topologie Physique

Décrit comment les différents nœuds sont reliés entre eux. [1]

I.3.1 Topologie en anneau

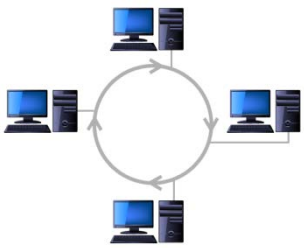


Figure I.2 – Réseau en anneau

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, nous avons donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va avoir la parole successivement.

I.3.2 Topologie en bus

Figure I.3 – réseau en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "Bus" désigne la ligne physique qui relie les machines du réseau.

I.3.3 topologie en étoile

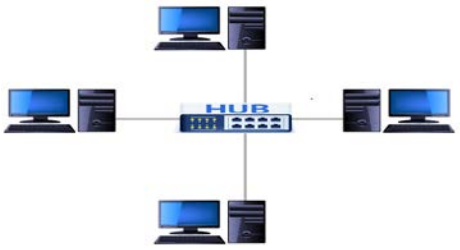


Figure I.4 – Réseau en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé *hub* ou *concentrateur*. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles nous pouvons connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes.

I.4 L'architectures Des Réseaux Informatique

Pour que les données transmises de l'émetteur vers le récepteur arrivent correctement avec la qualité de service exigée, il faut une architecture logicielle.

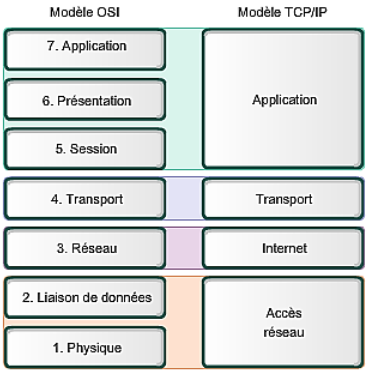


Figure I.5 – le modèle OSI et le modèle TCP/IP

I.4.1 Le modèle de référence OSI (Open Systems Interconnection)

Le modèle OSI a été créé par l'organisme ISO (International Organization for Standardization).Il écrit les fonctionnalités nécessaires à la communication entre ordinateurs et assure l'organisation de ces fonctions. Ce modèle est formé de 7 couches, ayant chacune des applications bien distinctes.

Les différentes couches sont : [5]

I.4.1.1 Niveau 7 : La couche applicative

Elle donne aux programmes de l'utilisateur le moyen d'accéder à l'environnement OSI et fournit tous les services directement utilisables par ces programmes, tel que l'envoi ou la réception de courrier électronique ou la navigation web.

I.4.1.2 Niveau 6 : La couche de présentation

Elle s'occupe de la syntaxe et de la sémantique des informations transportées en se chargeant notamment de la représentation des données, de la lisibilité par la couche application d'un autre système, de l'utilisation d'un format commun.

I.4.1.3 Niveau 5 : La couche session

Elle se charge de négocier les conditions d'une session de communication entre deux hôtes, de créer cette session et de la détruire une fois la communication est terminée (sur demande de la couche de présentation).

I.4.1.4 Niveau 4 : La couche de transport

Elle se charge de la liaison d'un bout à l'autre et aussi responsable du bon acheminement des messages complets de l'émetteur au récepteur. S'occupe de la fragmentation des données en petits paquets et vérifie éventuellement qu'elles ont été transmises correctement.

I.4.1.5 Niveau 3 : La couche réseau

Elle assure toutes les fonctionnalités de relais et d'amélioration de services entre entités du réseau : l'adressage, le routage, la détection, etc.

I.4.1.6 Niveau 2 : La couche de liaison de données

Elle s'occupe d'encoder (ou moduler) les données pour qu'elles soient transportables par la couche physique, et fournit également la détection d'erreur de transmission et la synchronisation.

I.4.1.7 Niveau 1 : La couche physique

Elle s'occupe de la transmission des données proprement dit. Elle précise en particulier le type du média de communication, de format des éventuels connecteurs.

I.4.2. Le modèle TCP/IP (Transfer Control Protocol / Internet Protocol)

Le but du modèle TCP/IP (Transfer Control Protocol / Internet Protocol) était de permettre une interconnexion des réseaux, en offrant aux utilisateurs un mode commun d'adressage et des protocoles de communication indépendants des technologies utilisées, du nombre et de la position d'équipements d'interconnexion. Il est structuré en quatre couches. [6]

I.4.2.1 La couche d'accès au réseau

Aussi appelée couche hôte réseau, elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé. Cette couche renferme tous les détails sur la couche physique et la couche liaison de données du modèle OSI.

I.4.2.2 La couche Internet

Elle est chargée de fournir le paquet de données (datagramme Le but du protocole IP (Internet Protocol) est de masquer aux utilisateurs (et aux protocoles des couches supérieures)

la topologie et la multiplicité du réseau, en adoptant pour ce dernier un adressage universel (au moyen d'adresses IP), et en assurant le routage.

I.4.2.3 La couche transport

Elle assure l'acheminement des données. La couche transport renferme deux types de protocoles : le protocole TCP (Transmission Control Protocol) et le protocole UDP (User Datagram Protocol). Tous les deux utilisent IP comme couche réseau.

I.4.2.4 La couche application

Elle englobe les applications standards du réseau. Elle gère les protocoles de haut niveau, elle combine les fonctions des couches session, présentation et application du modèle OSI.

I.5 Les protocoles LAN

Parmi les protocoles dans les LAN on trouve :

I.5 .1 VLAN (Virtual LAN)

Un LAN (Virtual Local Area Network) Ethernet est un réseau local virtuel utilisant la technologie Ethernet, il permet de regrouper les éléments du réseau (utilisateurs, périphérique, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.) et sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.).[2]

I.5.2 Le protocole VTP (VLAN Trunking Protocol)

Le VTP est un protocole propriétaire de Cisco qui permet de configurer et de propager les VLANs à travers un réseau. Il y a trois modes de fonctionnent pour la mise en place du VTP : [3]

1. **Mode serveur** : les serveurs VTP peuvent créer, modifier et supprimer un VLAN et des paramètres de configuration VLAN pour l’ensemble du domaine. Ils envoient des messages. Ils envoient des messages VTP par tous les ports multi-VLAN.

2. **Mode client** : les clients VTP ne peuvent pas créer, modifier ou supprimer des informations VLAN. Le seul rôle des clients VTP est de traiter les modifications VLAN et d'envoyer des messages VTP par tous les ports multi-VLAN.
3. **Mode transparent** : les switchs transmettent des annonces VTP mais ignorent les informations contenues dans le message.

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :

- Il faut assigner le même nom de domaine de VTP à chaque switch.
- L'option trunk pour l'interconnexion des switch doit être activée.

Le rôle de VTP est maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun. Ce domaine est organisé hiérarchiquement : le serveur VTP diffuse ses configurations VLAN, tandis que le client VTP met à jour sa configuration VLAN en fonction des informations reçu du serveur. En outre, le protocole VTP facilite la gestion et la surveillance des réseaux VLAN. [3]

Partie II : Sécurité informatique

II.1 Définition

La sécurité informatique est une discipline qui se préoccupe de la protection de l'intégrité et de la confidentialité des informations stockées dans un système informatique, afin de réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles**.**

II.2 Objectifs de la sécurité informatique

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. [7]

La sécurité informatique vise généralement cinq principaux objectifs :

- La confidentialité

La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

- **L'intégrité**

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

- **La disponibilité**

L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

- **La non-répudiation**

La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

- **L'authentification**

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

II.3 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire des termes techniques bien défini nous définissons certains termes associé: [8] [9]

- **vulnérabilité (faiblesse/ faille)**

Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une vulnérabilité peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

- **Menaces**

Ce sont les violations potentielles de la sécurité. C'est l'ensemble des personnes, choses et événements qui posent danger pour un patrimoine en termes de confidentialité, d'intégrité et de disponibilité. Il existe deux types de menaces accidentelles (expositions) et les menaces intentionnelles (attaques).

- **Risque**

Le risque désigne la probabilité d'un événement dommageable ainsi que les coûts qui s'ensuivent. Le risque dépend également du montant des valeurs à protéger.

- **Intrusions dans le système (hacking)**

Le hacking, ou piratage informatique, n'est pas une notion précisément définie, mais porte sur toutes sortes de manipulations non autorisées effectuées sur des ordinateurs étrangers. Le hacking décrit l'intrusion non autorisées dans le système informatique d'une entreprise. Il consiste souvent à utiliser des programmes d'espionnage ciblé (espiogiciels, cheval de Troie).

- **Attaque**

Une attaque désigne un accès ou une tentative d'accès non autorisés à un système. Nous distinguons entre les attaques passives (obtention sans autorisation d'information, perte de confidentialité) et les attaques actives (modification non autorisée des données, perte de l'intégrité, perte de disponibilité).

II.4 Les attaques courantes

Il existe un nombre important d'attaques informatiques ayant chacune des objectifs différents, dans ce qui suit nous citons quelques attaques courantes : [10]

- ***Le sniffing***

Cette attaque se fait avec un logiciel appel "sniffer" placé sur un ordinateur du même réseau que la machine cible, le sniffer intercepte toutes les trames que la carte réseau d'un ordinateur reçoit et qui ne lui sont pas destinées. Grâces à ça on peut savoir par exemple les pages web que consultent les personnes sur le réseau ou bien les mails envoyés et reçus.

- ***L'IP spoofing***

Cette attaque consiste à ce faire passer pour une autre machine qui a des privilèges ou droits élevés (root) dans l'accès à un serveur cible en falsifions son adresse IP

- ***Le Dos (Denial of Service)***

Le déni de service est une attaque qui vise à rendre un service, un système ou un réseau indisponible. En général, il exploite les faiblesses d'implémentation, les faiblesses de l'architecture d'un réseau ou d'un protocole.

- ***Le craquage de mots de passe***

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants, ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne).

- ***Virus***

Les virus sont des programmes, généralement écrits en langage machines, susceptibles de s'introduire dans un ordinateur et de s'y exécuter. L'exécution peut produire de nombreux effets, allant du blocage d'une fonction à la destruction des ressources de l'ordinateur, comme l'efficacement de la mémoire ou du disque dur, en passant par l'émission de messages incontrôlés.

II.5 Mesure de la sécurité des réseaux

La mise en œuvre des mesures de sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information. Ainsi, la plupart du temps il est nécessaire de recourir à des applications implémentant des algorithmes cryptographiques permettant de garantir la confidentialité des échanges.

II.5.1 Dispositif de sécurité

Un dispositif de sécurité est défini comme tout instrument, appareil, équipement, pièces, mécanisme, matière ou autre organisme ou organisation utilisées seule ou en association, pour être utilisés à des fins de mise en sécurité de personnes ou de biens, et ces dispositifs sont les suivants :

II.5.1.1 Les réseaux privés virtuel

Les réseaux privés virtuels sont utilisés pour interconnecter des réseaux locaux à travers un réseau public comme Internet. Ils reposent sur le principe de création d'un tunnel virtuel dont les extrémités identifiés appartiennent à deux réseaux locaux différents, les données circulent alors dans ce tunnel après avoir était chiffrée, le principale avantage des VPN est interconnecter des réseaux à moindre coût à travers un réseau publique au lieu d'utilisation de lignes dédiées très couteuses. [11]

II.5.1.2 Liste de contrôle d'accès (ACL)

Les administrateurs réseau doivent trouver le moyen d'interdire l'accès au réseau à certains utilisateurs tout en permettant aux utilisateurs internes d'accéder aux services nécessaires, les routeurs assurent cette fonction à l'aide des listes de contrôle d'accès. Une ACL est un ensemble de conditions qui est appliqué au trafic circulant via une interface du routeur. Elle indique au routeur les types des paquets à accepter ou à rejeter. Les ACLs permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

II.5.2 La cryptographie

Il existe à l'heure actuelle deux grands principes de cryptages : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui, repose sur un codage à deux clés, une privée et l'autre publique. [9] [12]

II.5.2.1 La cryptographie symétrique

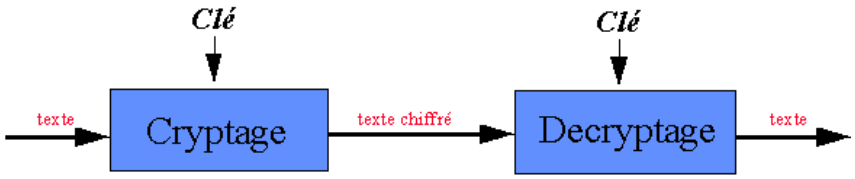


Figure I.6 – Chiffrement symétrique

Le cryptage à clé privé ou symétrique est basé sur une clé partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. L'avantage de la cryptographie symétrique est sa rapidité d'exécution car elle met en œuvre des opérations simples. Les algorithmes développés pour réalisé les opérations de cryptographie symétrique sont : DES, 3DES, AES.

II.5.2.2 La cryptographie asymétrique

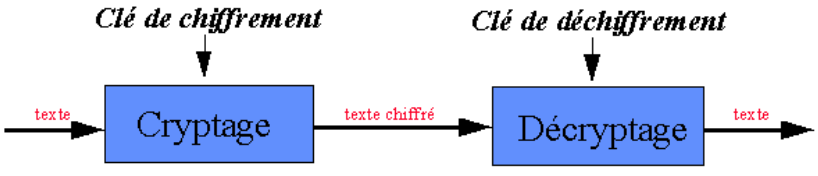


Figure I.7– Chiffrement asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est pas connue que par l'utilisateur; l'autre est publique et donc accessible par tout le monde. Les clés publique et privée correspondante. Ce message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Ce cryptage présente l'avantage de permettre la signature numérique des messages et ainsi permettre l'authentification de l'émetteur. Les algorithmes à clé publique les plus fréquemment utilisés sont : RSA, DSA, DH.

La cryptographie asymétrique et cryptographie symétrique sont donc exploitées de manière complémentaire et successive dans les protocoles cryptographique pour authentifier l'émetteur, le récepteur, énoncer la non-répudiation des interlocuteurs, et déployer les systèmes de secrets qui vont leurs permettre de se communiquer de manière sécurisé.

II.5.3 Le hachage

Le hachage est appelé aussi fonction de hachage, c'est une fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe, le résultat de cette fonction est appelée une empreinte. Une fonction de hachage qui est aussi une fonction à sens unique, c'est-à-dire il est très difficile de trouver une chaîne qui donne cette empreinte. [13]

II.5.4 La signature numérique

Une signature numérique est une empreinte (d'un document) chiffrée par la clé privée de l'auteur, cette empreinte chiffrée étant jointe au document original. La signature permet ainsi de vérifier l'intégrité du document et l'identité de l'expéditeur. Signe un document via des fonctions de hachage. [13]

Conclusion

Ce chapitre nous a permit en premier lieu de découvrir et de mieux comprendre les notions et les concepts élémentaires des réseaux informatique. Il décrit le rôle de chaque matériel de base et son importance et en deuxième lieu de comprendre le concept de la sécurité informatique (cryptographie, fonction de hachage, signature numériques…) et plus particulièrement la sécurité des réseaux ou nous avons présenté brièvement les différentes politiques sécuritaires, tel que les VPNs qu'on abordera en détails dans le chapitre suivant.

Introduction

Les réseaux locaux types LAN permettent de faire communiquer les ordinateurs d'un site ou d'une société ensemble. Ces réseaux sont relativement sûr car ils sont quasiment toujours derrière une série de pare-feu ou coupés d'Internet et le chemin emprunté par les données ne quitte pas l'entreprise et est connu.

Sur Internet, on ne sait pas par où passent les données car les chemins changent. Ces données peuvent donc être écoutées ou interceptées. Il n'est donc pas envisageable de faire connecter deux LAN entre eux par Internet sans sécuriser le cheminement des données échangées. Dans ces conditions, l'internet fournit des solutions VPN est idéale pour pouvoir exploiter au mieux les capacités de ce réseau des réseaux et relier des sites distants.

Afin de sécuriser les échanges de données entre deux LAN, on peut recourir à deux alternatives :

- Relier les deux sites par une ligne spécialisée mais hors de prix.
- Créer un réseau privé virtuel sécurisé autrement dit un VPN. On encapsule (en anglais tunneling) les données dans un tunnel crypté.

Nous nous intéresserons dans ce chapitre à la deuxième solution, ainsi nous verrons quelles sont les principales caractéristiques des VPN et les protocoles permettant leur mise en place.

II.1 Définition d'un VPN

Un VPN est un réseau virtuel permettant d'interconnecter les entités distantes en vu de faire comme si plusieurs machines faisaient partie d'un même réseau local, bien qu'elles soient en réalité situées aux plusieurs endroits géographiques différents et reliées entre elles par le réseau public tel qu'Internet d'une manière complètement sécurisée, c'est-à-dire que seules les ordinateurs des réseaux interconnectés peuvent voir les données échangées. [11]

II.2 Fonctionnement d'un VPN

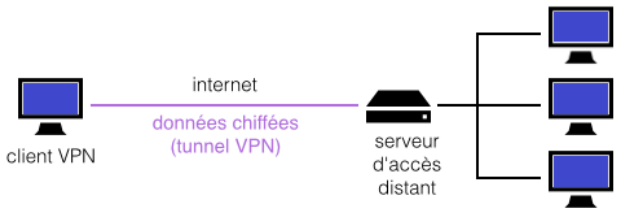


Figure II.1 – connexion VPN entre un client et un serveur

Le VPN repose sur un protocole de tunnelisation, protocole qui encapsule dans son datagramme un autre paquet de données complet utilisant un protocole de communication différent et qui permet le passage de données cryptées d'une extrémité du VPN (machine client) à l'autre (serveur) grâce à des algorithmes cryptographiques.

Le terme tunnel est employé pour symboliser le fait que les données soient cryptées et de ce fait incompréhensible pour tous les autres utilisateurs du réseau public (ceux qui ne se trouvent pas aux extrémités du VPN).

Dans le cas d'un VPN établie entre deux machines, l'une sera un client VPN (élément permettant de chiffrer de déchiffrer les données du côté utilisateur) et l'autre le serveur VPN (élément chiffrant et déchiffrant les données du côté de l'organisation). Ainsi lorsque le client nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant (le serveur) par l'intermédiaire d'une infrastructure de réseau public, puis une fois connecté au serveur il va transmettre la requête de façon chiffrée.

Au cas où le serveur VPN est connecté avec d'autre machines sur son réseau local, le client pourra alors joindre ces machines par l'intermédiaire du serveur VPN. Pour répondre au client ces machines vont alors fournir les données au serveur VPN de leur réseau local qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmise à l'utilisateur.

Pour émuler une liaison point à point, les données sont encapsulées, ou enrobée, à l'aide d'un en-tête qui contient les informations de routage pour leurs permettre de traverser le réseau partagé ou public jusqu'à leur destination finale.

Pour émuler une liaison privée, les données sont cryptées à des fins de confidentialité. Les paquets interceptés sur le réseau partagé ou public restant indéchiffrable sans clé de décryptage.

Ainsi, tous les utilisateurs passent par le même “portail“, ce qui permet de gérer la sécurité des accès, ainsi le trafic utilisé par chacun.

Le tunneling est l’ensemble des processus d’encapsulation, de transmission et de dés-encapsulation. [14]

II.3 Objectif et fonctionnalités des VPN

Un réseau privé virtuel, repose sur les principes fondamentaux de la sécurité, en assurant la mise en œuvre de diverses fonctionnalités.

- ***Confidentialité des données***

Les VPN visent à protéger le contenu des messages contre toute interception par des sources non authentifiées ou non autorisées. La confidentialité est garantie grâce à l’encapsulation et au chiffrement effectués. [16]

- ***Intégrité des données***

Pour garantir qu’aucune altération ou modification n’a été apportée aux données lors de leurs parcours entre la source et la destination, les réseaux privés virtuels utilisent des hachages. Un hachage ressemble à une somme de contrôle ou à un seau garantissant que personne n’a lu le contenu, tout en étant plus robuste. [16]

- ***Authentification***

Afin de garantir qu’un message provient d’une source authentique, que la personne avec qui la communication est établie est effectivement le destinataire escompté. Les réseaux privés virtuels peuvent utiliser des mots de passes, des certificats numériques et des cartes à puce pour vérifier l’identité des parties à l’autre extrémité du réseau. [16]

- ***Gestion des clés***

Les VPN assurant la génération, la distribution, le stockage et la suppression des clés de cryptage pour le client et pour le serveur avec différents mécanisme et protocoles. [16]

- ***Prise en charge multi protocoles***

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP. [16]

II.4 Catégories de VPN

Suivant les besoin on référence 3 types de VPN :

II.4.1 Le VPN d'accès

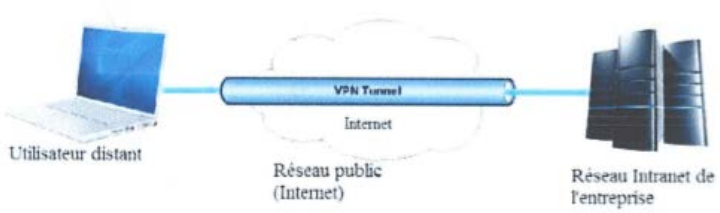


Figure II.2 – VPN d'accès

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leurs entreprises. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisé. [15]

II.4.2 L'intranet VPN

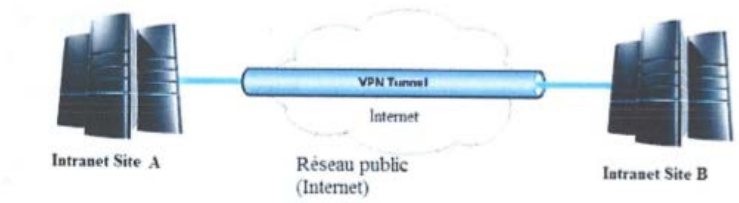


Figure II.3 – VPN intranet

Il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveur distant, etc.). [15]

II.4.3 L'extranet VPN

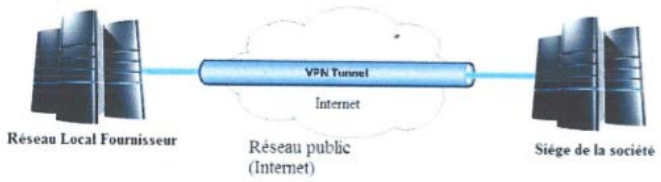


Figure II.4 – VPN extranet.

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et partenaires. Elle ouvre alors son réseau local à ces derniers, dans ce cas il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus en plus, seule une partie des ressources sera partagée, ce qui signifie une gestion rigoureuse des espaces d'échange. [15]

II.5 Avantages des VPN

Les réseaux privés virtuels offrent les avantages suivants : [15]

1. **Économie**

Les organisations peuvent utiliser un transport Internet tiers et rentable pour connecter les bureaux et les particuliers à distance au siège, à la différence des liaisons dédiées de réseau étendu qui est une solution très couteuse. Grâce à la large bande, les réseaux privés virtuels réduisent les coûts de connectivité en augmentant la bande passante de connexions distantes.

2. **Sécurité**

Les protocoles de chiffrement et d'authentification avancés protègent les données contre tout accès non autorisé.

3. **Évolutivité**

Les réseaux privés virtuels utilisent l'infrastructure Internet dont les FAI et les opérateurs, facilitant l'ajout de nouveaux utilisateurs pour les entreprises. Ces dernières, quelle que soit leur taille, peuvent augmenter leurs capacités sans élargir sensiblement leur infrastructure.

4. **Simplicité**

Utilise le circuit de télécommunication classique.

Les protocoles utilisés dans le cadre d'un VPN sont de deux types, suivant le niveau de la couche OSI auquel ils travaillent. Le protocole qui nous intéresse ici est l'IPSec qui est la technique la plus employée lorsqu'il s'agit de mettre en œuvre une liaison site à site sur un réseau public dont nous allons donner une description détaillée :

II.6 Le protocole IPSEC

IPSec est un protocole défini par l'IETF (RFC 2401) permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir des services de sécurité comme la confidentialité, l'intégrité et l'authenticité de données échangées. [17]

- **Authentification des extrémités** : cette authentification mutuelle permet à chacun de s'assurer de l'identité de son interlocuteur. Rappelons tout de même qu'IPSec est un protocole de niveau 3 et qu'il ne fournit donc qu'une authentification de niveau égale, c'est-à-dire une authentification des machines mettant en œuvre le protocole plutôt que des personnes utilisant réellement la machine.
- **Confidentialité des données échangées** : IPSec permet si on le désire de chiffrer le contenu de chaque paquet IP pour éviter que quiconque ne le site.
- **Authenticité des données** : IPSec permet de s'assurer, pour chaque paquet échangé, qu'il a bien été émis par la bonne machine et qu'il est bien à destination de la seconde machine.
- **Intégrité des données échangées** : IPSec permet de s'assurer qu'aucun paquet n'a subit de modification quelconque (attaque dite active) durant son trajet.
- **Protection contre les écoutes et analyses de trafic** : IPSec permet de chiffrer les adresses IP réelles de la source et de la destination, ainsi que tout l'en-tête IP correspondant. C'est le mode de tunneling, qui empêche tout attaquant à l'écoute d'inférer des informations sur les identités réelles des extrémités du tunnel, sur les protocoles utilisés au-dessus d'IPSec, sur l'application utilisant le tunnel (timing-attacks et autres)...
- **Protection contre le rejeu** : IPSec permet de se prémunir contre les attaques consistant à capturer un ou plusieurs paquets dans le but de les envoyer à nouveau (sans pour autant les avoir déchiffrés) pour bénéficier des mêmes avantages que l'envoyeur initial.

II.6.1 Protocoles liée au traitement des paquets d'IPSec

Les services de sécurité fournis par IPsec reposent principalement sur deux protocoles qui sont :

- AH : “Authentification Header“ (protocole numéro51) dont la version la plus récente est normalisée par la RFC 4302. Il permet d’assurer l’intégrité, l’authentification et la protection contre le rejeu, mais ne gère pas la confidentialité, c’est pour ça qu’il est moins utiliser qu’ESP.
- ESP : “Encapsulation Security Payload“ (protocole numéro 50) dont la version la plus récente est normalisée par la RFC 4303. Il permet 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 et justifie donc l’abandon d’AH). [17]

Indépendamment du choix entre AH et ESP, il est possible d’utiliser IPsec dans deux modes distincts : le mode tunnel et le mode transport. [17]

1. Le mode transport

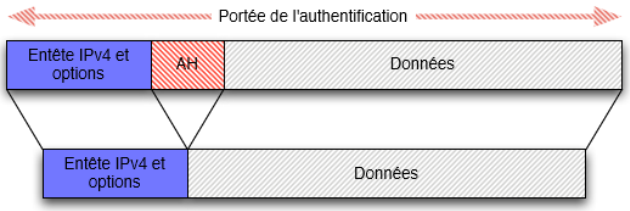


Figure II.5 – Utilisation d’AH en mode transport

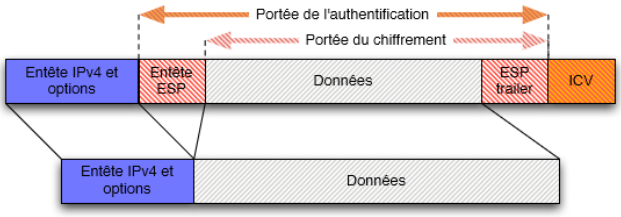


Figure II.6– Utilisation d’ESP en mode transport

Dans le mode transport, les données associées à AH ou à ESP viennent se greffer sur le paquet IP initial. Le paquet IP résultant contient un paquet AH ou ESP qui contient lui-même le contenu du paquet initial (un segment TCP par exemple). [17]

2. **Le mode tunnel**

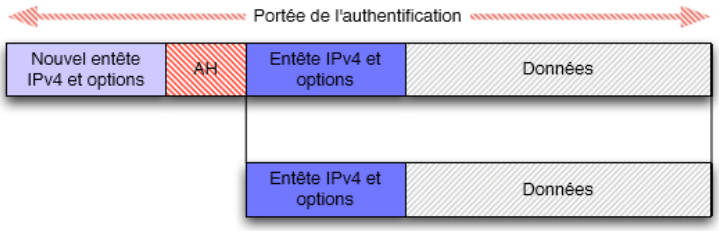


Figure II.7– Utilisation d'AH en mode tunnel

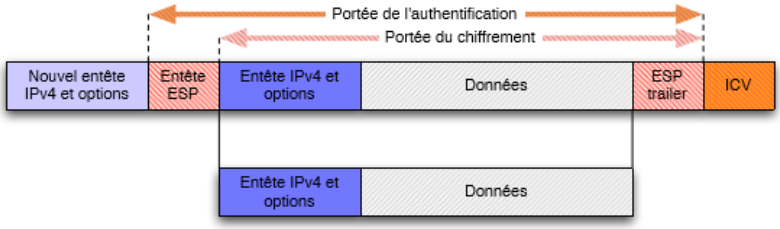


Figure II.8 – Utilisation d'ESP en mode tunnel. ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité

Dans le mode tunnel, un nouveau paquet IP est généré pour contenir un paquet AH ou ESP qui contient lui-même le paquet IP initial sans modification. Il y a donc deux en-têtes IP. L'en-tête externe sera 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). [17]

Les protocoles offertes par IPSec sont basées sur des choix définis par l'administrateur du réseau par le biais de politique de sécurité, c'est donc par elles que se fait la configuration d'IPSec. L'établissement de ces politiques de sécurité est associés à plusieurs mécanismes (SA, SAD, SPD) qui font appel à la cryptographie et utilisent donc un certain nombre de paramètres (échange préalables d'algorithmes utilisés, échange de clés, mécanismes sélectionnés…), ces échanges préalables sont gérés automatiquement par le protocole IKE, qui est un protocole développé spécifiquement pour IPSec. [17]

II.6.2 Détails du protocole

Le mécanisme interne d'IPSec est complexe. Le fait que ce protocole soit hautement configurable introduit des notions de gestion et configuration inconnues du monde IP.

II.6.2.1 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 les lois suivantes. [16]

a) **Security Policy :** Une SP définit ce qui doit être traité sur un flux et la manière dont nous voulons transformer un paquet. Il y sera indiqué pour un flux donné :

- Les adresses IP de l'émetteur et du récepteur (unicast, multicast ou brodcast).
- Par quel protocole il devra être traité (AH ou ESP).
- Le mode IPSec à utiliser (tunnel ou transport).
- Le sens de liaison (entrant ou sortant).

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

b) **Security Association :** Une SA définit la manière dont 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 donnée contenant les informations suivantes :

- 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.

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 (Security Parameter Index).

Une SA ne sera associée qu'un seul des protocoles AH ou ESP. Si nous voulons protéger un flux avec ces deux protocoles, deux SA devront être créés.

- **SPI :** Est une indice (ou ID) sur 32 bits attribué au SA lors de sa création. Nous verrons plus loin que 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.

c) **Base de données SPD et SAD :** Tout système implémentant IPSec possède donc deux bases de données distinctes dans laquelle ils stockent leurs SP (ici, SPDatabase) et leurs SA (ici, SADatabase).

- **SAD (Security Association Dtabase) :** Stocke les SA afin de savoir comment traiter les paquets arrivant ou sortant. Elles sont identifiées par de triplets :

- Adresse de destination des paquets.
- Identifiant du protocole AH ou ESP utilisé.
- Un index des paramètres de sécurité (Security parameter index) qui est un champ de 32 bits envoyé en clair dans les paquets.

- **SPD (Security Policy Database) :** Est la base de configuration de IPSec. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé passer ou rejeté. C'est à sa charge de savoir avec quel SA fait-il le traitement.

II.6.3 Protocole de gestion et d'échange de clés IPSec [16]

La présence de mécanisme de chiffrement implique la prise en compte des problématiques de gestion de clés et leur distribution à l'ensemble des systèmes destinés à être source et/ou destination d'une communication IPSec.

Pour la gestion de distribution des clés, on peut, soit opter pour une gestion manuelle dans le cas de petites infrastructures, soit pour une gestion automatique. Pour cela le protocole IKE (Internet Key Exchange), défini dans la RFC 2409, a été défini comme protocole par défaut pour la gestion et la distribution des clés. IKE est un protocole qui combine des éléments, des définitions et des fonctionnalités issu de protocoles tel que ISAKMP, SKEME et Oakley pour la gestion et l'échange de clés ou de SA.

Le protocole ISAKMP (Internet Security Association and Key Management Protocol), défini dans la RFC 2408, apporte une infrastructure permettant de définir et d'administrer des SA

enter deux ordinateurs devant communiquer de manière sécurisée. ISAKMP a un DOI (Domain of Iterpretation) défini pour être utilisé avec IPSec. Ce DOI permet de spécifier les formats et les conditions requises lorsqu'ISAKMP est appliqué à IPSec.

Le protocole IKE utilise l'infrastructure du protocole ISAKMP pour échanger des clés et définir des SA entre deux machines. IKE utilise également le protocole Oakley pour la création des clés et le protocole SKEME pour les échanger.

II.6.4 Fonctionnement d'IPSec [16]

Le schéma ci-dessous représente tous les éléments présentés ci-dessus (en bleu), leurs positions et leurs interactions

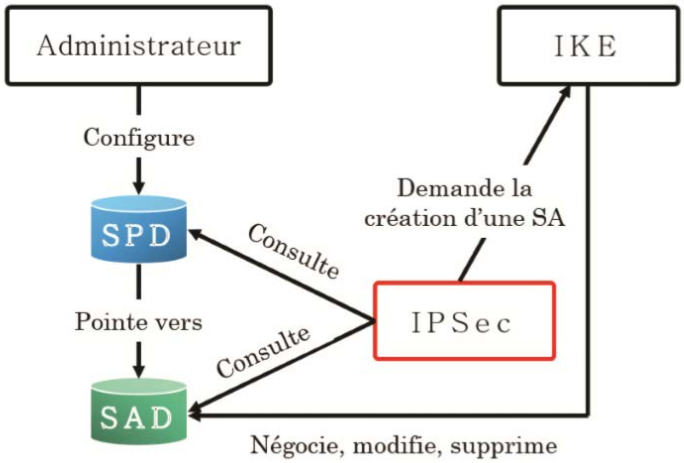


Figure II.9 – Principe de fonctionnement d'IPSec.

Pour bien comprendre le fonctionnement d'IPSec, nous allons voir comment est traité le trafic sortant et le trafic entrant.

- Trafic sortant

Lorsqu'on veut envoyer un paquet IP vers l'extérieur du réseau local et que le protocole IPSec est activé, notre système décidera la démarche à suivre de ce paquet. Il peut le détruire, l'envoyer tel quel ou le sécuriser en appliquant les règles propres à IPSec. Pour savoir ce qu'il doit faire de ce paquet, IPSec consulte la base de données SPD (Security Policy Database) créée par l'administrateur du système. Cette dernière contient les règles et les stratégies de sécurité

auxquelles IPSec détermine les paramètres qui seront utilisé pour la protection du paquet. Pour déterminer ces paramètres, IPSec doit consulter la SA associé au paquet dans la base SPD.

- Trafic entrant

Imaginons qu'un paquet protégé par le protocole IPSec vienne d'arriver. IPSec va déterminer la SA associé au paquet entrant. Les SA se trouvent dans la base de données SA (SAD) stockée sur la machine destinataire et comprend les éléments suivant : le SPI, l'adresse IP de destination et le protocole IPSec de manipulation de données (AH ou ESP).

Rappelons que le SPI est un nombre de 32 bits, servant d'index à la base des SA de la machine destinataire. Ces trois éléments sont extraits de l'en-tête du paquet reçu. Une fois que la SA a été identifié, le système effectue les opérations d'authentification et décryptage. Cela permettra de vérifier l'identité de l'expéditeur et d'extraire les données encapsulées.

L'extraction des données avant la vérification de la base SPD s'impose car le paquet peut contenir un en-tête TCP encrypté. Les informations contenues dans ce dernier (par exemple le numéro de port) peuvent être nécessaires pour déterminer les règles SPD applicables, ce qui explique qu'il faut d'abord le décrypter.

Une fois les données décryptées, IPSec consulte la base SPD dont l'entrée concernée est trouvée en utilisant la référence contenue dans la SA. Le paquet peut être alors relayé vers une autre destination, détruit ou remis à la couche transport.

Conclusion

Au cours de cette étude, nous avons pu comprendre la notion et le principe de fonctionnement de VPN a travers la définition de ses fonctionnalités et ses principaux d'avantages, ainsi que les différents possibilités permettant son déploiement particulièrement la solution qui représente IPSec, sur qui est porté notre choix.

Introduction

Afin de nous familiariser avec l'environnement de l'entreprise SOUMMAM COMPUTER SYSTEM (SCS), nous avons en premier lieu pris connaissance de celle-ci, des différents services, mission et activités qui la constituent. En second lieu, nous commencerons par une présentation globale du réseau de l'entreprise SCS qui est l'infrastructure réseaux sur laquelle nous réaliserons notre projet, en suite nous verrons la problématique, l'objectif de notre projet et la solution proposée.

III.1. Présentation générale

SOUMMAM COMPUTER SYSTEM (SCS) est l'une des premières entreprises spécialisées de la fourniture et la maintenance des équipements et réseaux informatiques afin de répondre à une démarche accrue du marché de l'informatique en Algérie. Depuis, la société s'est spécialisés dans l'importation, la distribution et la vente des produits informatiques, bureautiques et multimédias. Elle est aujourd'hui un acteur majeur de la commercialisation et de la distribution informatique en Algérie. Elle répond à l'ensemble des besoins des entreprises et des particuliers en matière d'importation, de distribution et de vente des produits informatiques, bureautiques et multimédias. Grace à son sérieux, son dynamisme, la qualité de ses prestations et de ses produits, elle est devenue aujourd'hui un acteur incontournable dans ce secteur.

II.2 Organigramme général de Soummam Computer System (SCS)

Voici le schéma général du groupe SCS dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe comme le montre la figure III.1

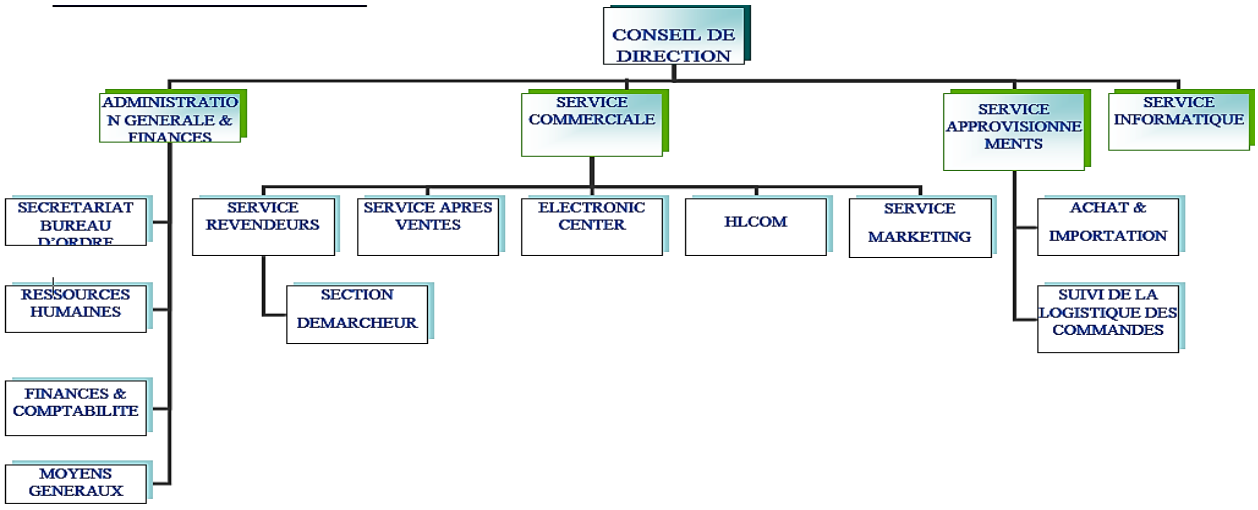


Figure III.1 – Organigramme de S.C.S

II.3 structure hiérarchique du groupe

Un label qui ne cesse d'accaparer des parts dans un marché caractérisé par une rude SCS dispose de ses propres moyens logistiques, des ses propres showrooms répartis sur tous les grands centres urbains et fait du rapprochement du service après-vente du client final une priorité.

III.1.2 Situation géographique

Soummam Computer System, dans le souci d'accomplir sa mission, dispose de plusieurs localités :

- Un centre de distribution en gros dans la zone industrielle de quatre chemins, le personnel technique est chargé des différentes opérations de maintenance en informatique, électronique et bureautique.
- L'électronique centre, centre commercial sur trois niveaux à Sidi Ahmed.
- Service après-vente situé à Ihaddaden.
- SCS Mobiliers Shows room et vente de divers mobiliers situé à proximité du siège social à Sidi Ahmed, le showroom permet à la clientèle une approche de diverses gammes de produits de mobiliers domestique et équipement de bureau.
- Centre Maxi Power Showroom à Quartier Sghir.

Hormis la wilaya de Bejaia, SCS s'est répartis sur plusieurs endroits sur le territoire Algérien tels que : Batna, Oran, Mostaganem, El Eulma.

- Atelier de maintenance qui assure à leur clientèle un service après vente de qualité, situé à rue Saint Charles KOUBA, Alger.

III.4 L'informatique dans SCS

Le service informatique est subdivisé en deux sous service dont le service réseau et le service marketing.

Le service réseau est composé de quatre administrateurs réseau parmi lesquels on dispose d'un chef de service, ils sont chargés de :

- Installer et maintenir les équipements réseaux.
- Administrer les différents serveurs (domaine, base de données, partage, proxy).

III.2 organigramme de la direction système d'informatique

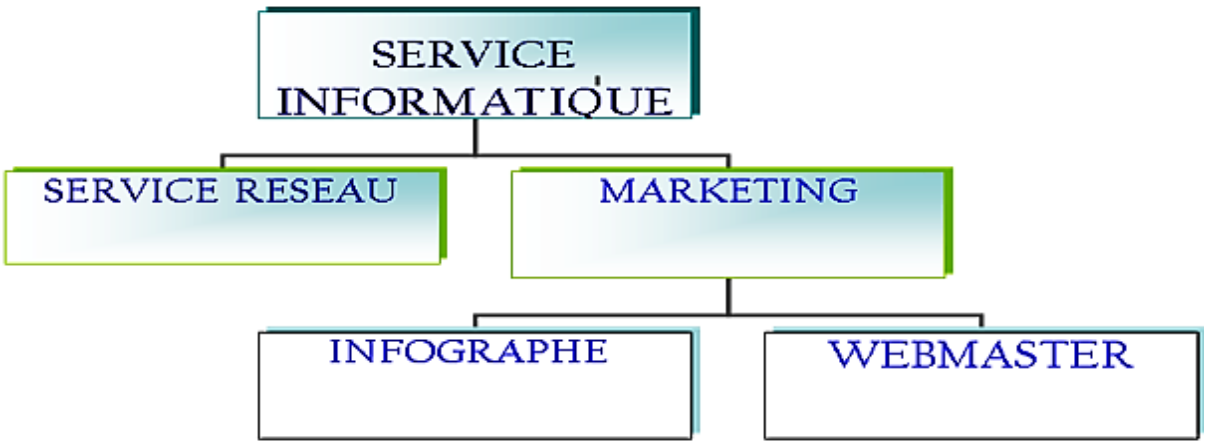


Figure III.2 – Organigramme du service d'accueil

Le service informatique est subdivisé en deux sous service dont le service réseau et le service marketing.

Le service réseau est composé de quatre administrateurs réseau parmi lesquels on dispose d'un chef de service, ils sont chargés de :

- Installer et maintenir les équipements réseaux.

- Administrer les différents serveurs (domaine, base de données, partage, proxy).

Quant au service marketing, il est constitué d'un infographe qui est en étroite collaboration avec le service commerciale afin de réaliser les publicités sur les produits, et d'un webmaster qui s'occupe de la conception et de la mise à jour des pages web de l'entreprise. Tous deux sont sous la directive d'un chef de service.

III.6.1 Problématique

Les réseaux informatique sont de plus en plus répandus et complexe. L'implantation d'un réseau et de logiciel doit être sûre pour diminuer les risques d'intrusion. SOUMMAM COMPUTER SYSTEM est une entreprise composée de plusieurs sites distants qui souhaite en tirer les avantages d'une liaison Internet entre ses sites pour d'éventuelles taches d'administration à distances et parmi ces derniers on distingue le centre de distribution en gros à Bejaia et l'atelier de maintenance à Alger ce qui est demandé est de pouvoir interconnecter ces deux sites en intégrants une connexion site à site.

Les questions qui se posent alors sont :

- ✓ comment pouvons-nous relier les différents sites de l'entreprise toute en assurant la sécurité des données ?
- ✓ comment assurer la sécurité des échanges de données entre les services dans un réseau local LAN?

III.6.2 Objectif de projet

L'objectif de notre projet est la mise en place d'un modèle type de configuration d'un réseau dans le but de faciliter la préparation et la réalisation des projets de la société. Ce modèle est basé sur deux réseaux locaux au niveau de deux sites distants, ainsi qu'une interconnexion de ces derniers grâce à une liaison Internet.

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

III.6.3 Solution proposée

L'interconnexion de deux sites d'une entreprise par la liaison spécialisée garantissant un débit de communication suffisant présente un certain nombre de limites liées au coût très élevés, mais le débit est garanti. Ainsi, la liaison entre deux sites d'une entreprise passant par Internet est trop vulnérable aux attaques des pirates. C'est-à-dire les données transitant par Internet sont trop exposées aux attaques de n'importe quel genre. Cela constitue un risque potentiel pour les entreprises.

Un VPN est particulièrement bien adapté à l'interconnexion de différents sites. Il permet un partage sécurisé des données. Il protège la confidentialité des données échangées via un canal télécom extérieur public, qui risque d'être intercepté et piraté.

Nous pouvons utiliser IPSec pour une solution complète VPN ou comme simple méthode de protection de communication réseau par l'utilisation de techniques d'encryptions. IPSec permet à l'entreprise ou à l'administration de réaliser une extension de son périmètre de sécurité à l'aide de tunnels VPN et de pouvoir exercer les taches administratives à distance.

Le VLAN permet de créer un ensemble logique isolé pour améliorer la sécurité des réseaux locaux (LANs). C'est pour cela qu'on découpera le LAN en plusieurs VLANs.

Conclusion

Ce chapitre nous a permis une bonne compréhension des différents services de l'entreprise SCS dont nous avons effectués notre étude. Nous avons éclairci notre thème en mettant en avant une problématique bien précise ce qui nous a conduit logiquement à la proposition d'une solution qui se résume la création de VPNs site à site pour interconnecter les sites distants.

Introduction

Dans ce chapitre nous allons passer à la dernière étape qui est la réalisation. Cette dernière est une étape cruciale pour la mise en œuvre de notre projet, dans le but de mettre en évidence l'efficacité de notre solution, nous commencerons par la présentation du simulateur utilisé, en suite nous allons présenter les différentes étapes de la configuration qui ont permis la réalisation de notre solution proposée.

VI.1 Présentation du simulateur Cisco GNS3

VI.1.1 Définition

GNS3 (Graphical Network Simulator) est un simulateur graphique de réseaux qui permet de créer des topologies du réseau complexes et d'en établir des simulations. Ce logiciel est un excellent outil pour l'administration des réseaux Cisco. Il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou pour tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment Open Source et multi-plates-formes. [18]

VI.1.2 Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à :[19]

- **Dynamips :** un émulateur d'image d'IOS qui permet de lancer des images binaires IOS provenant de Cisco systèmes.
- **Dynagen :** interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.
- **Qemu :** Emulateur du système.
- **VMware:** est un programme qui permet la création d'une ou plusieurs machines virtuelles au sein d'une même système d'exploitation, ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement).
- **Wireshark :** est un logiciel pour analyser les trames :

  –le design de topologies réseaux de haute qualité et complexes.

  –Emulation de plusieurs plate-forme de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.

  – Simulation de switches Ethernet, ATM et Frame Relay.

  – Connexion de réseaux simulés au monde réel.

  – Capture de paquets grâce à Wireshark.

VI.1.3 L'objectif de GNS3

L'objectif de GNS3 est d'apporter aux étudiants et aux professionnels travaillant dans le domaine d'administration des systèmes et réseaux des nouvelles technologies de communication. C'est un outil pour virtualiser et modéliser fidèlement des réseaux informatiques.

Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations avant de les mettre en place physiquement. [18]

V1.2.4 Configuration de GNS3

Lors du lancement du logiciel une fenêtre similaire à celle-ci apparait, c'est l'espace de travail de GNS3.

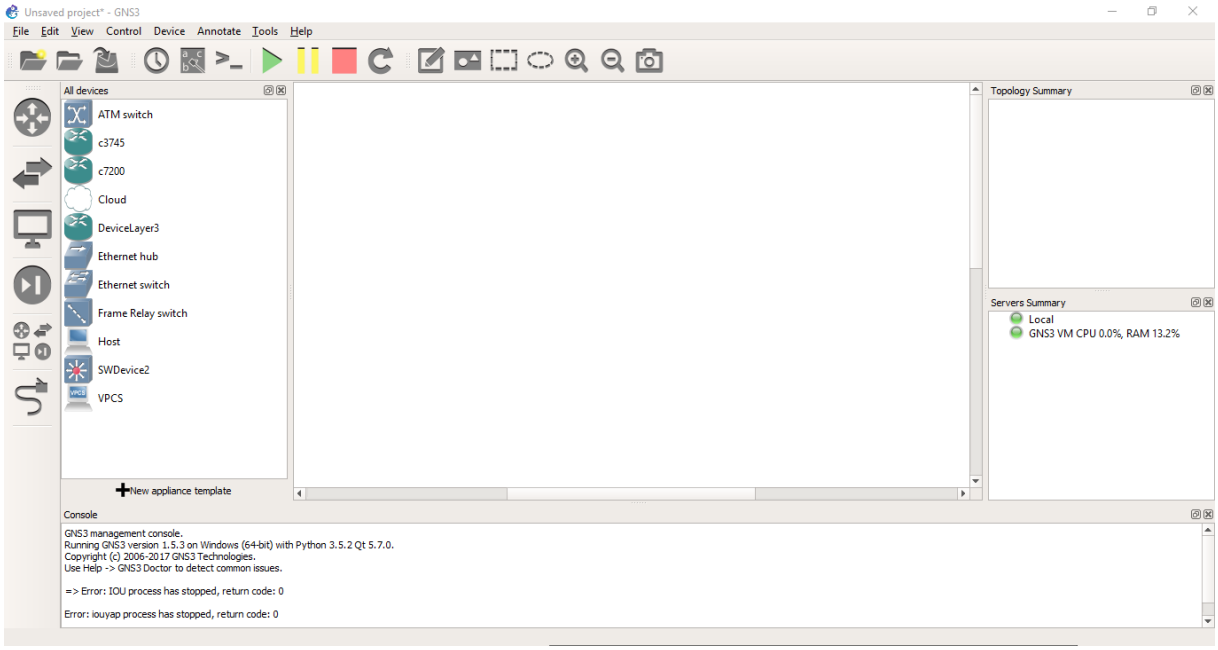


Figure VI.1– L'espace de travail GNS3

L'interface de GNS3 est divisée en trois parties, la partie gauche affiche la liste des équipements matériels disponibles que nous pouvons ajouter dans notre topologie, la partie droite affiche la liste des éléments actifs et au milieu c'est l'espace de travail.

V1.2.5Configuration de VMware

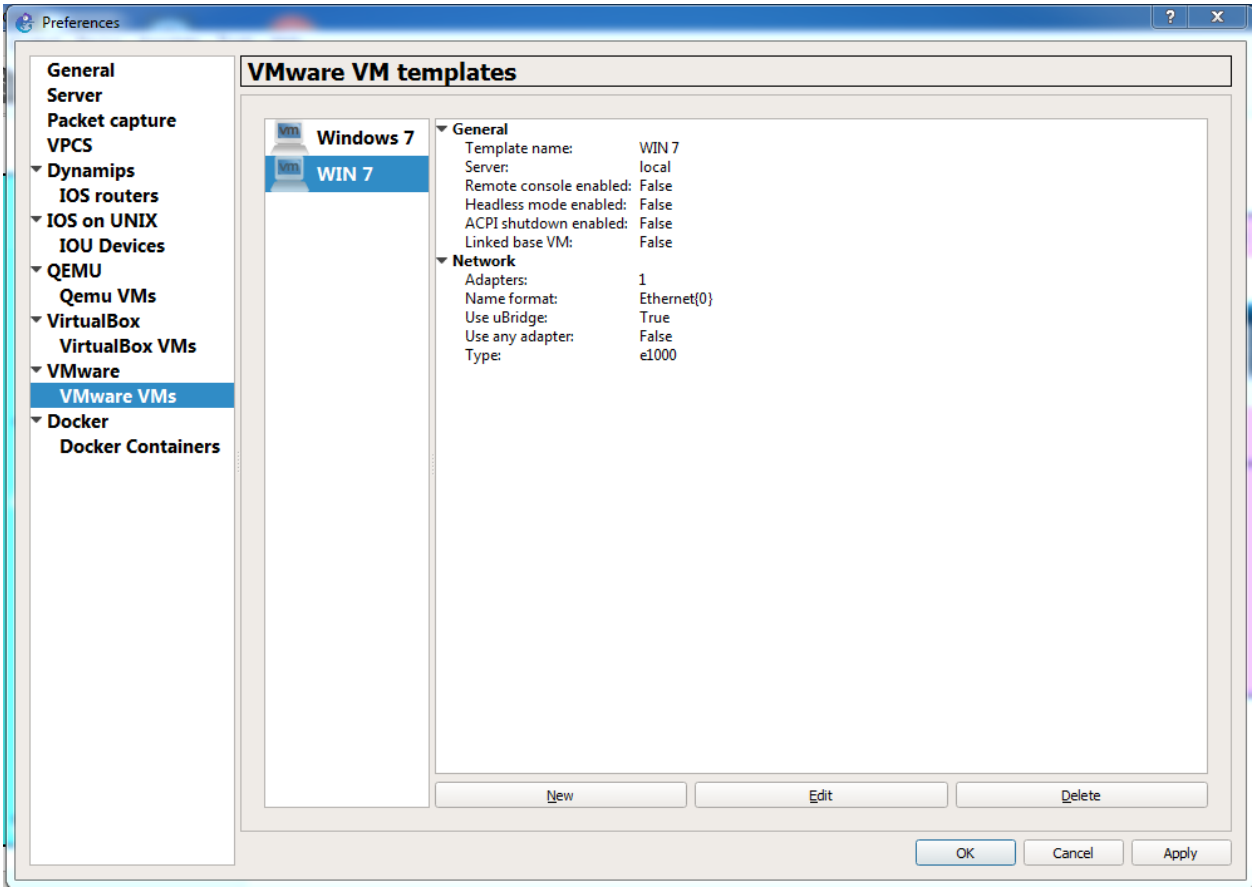


Figure VI.2– L'espace de travail de VMware

VI.2 Présentation générale et principe de la solution proposée

VI.2.1 Description de la maquette à configurer

Avant d'entamer la mise en œuvre de la solution proposée, il est essentiel de définir l'architecture réseaux utilisée. Pour cela, nous utiliserons la maquette du réseau WAN ci-dessous, constitué de 2 sites distants (LAN de Béjaïa et le LAN de Alger), possédant chacun :

- Un routeur Cisco, avec un IOS supportant les fonctions de cryptage (modules d'accélération de cryptage matériel).
- Une connexion Internet avec des adresses IP fixes.

-	Interface / IP Locale	Interface / IP
Site-BEJAIA	FastEthernet 0/0 192.168.1.1/24	Serial 2/0 1.1.1.2/30
Site-ALGER	FastEthernet 0/0 172.16.1.1/24	Serial 2/0 2.2.2.2/30

Table VI.1– Caractéristiques des deux routeurs

VI.2.2 Principe de mise en place

Dans la réalité il est évidement impossible de connecter directement les 2 routeurs, puisque le but premier du VPN est justement de se passer d'une ligne spécialisée. Ce lien sera donc créé grâce à un tunnel crypté, qui permettra aux 2 sites de communiquer entre eux de manière sécurisée. Pour cela, nous allons réaliser la configuration d'IPSec sur les deux routeurs : en mode automatique avec un secret pré-partagé via le protocole ISAKMP.

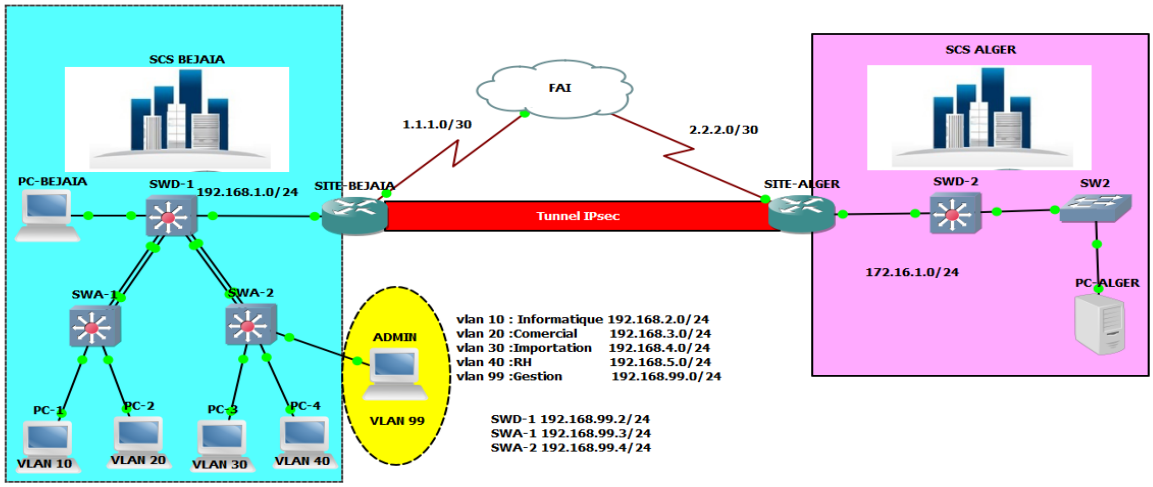


Figure VI.3 – Schéma illustrant la connexion entre deux sites par un tunel IPsec

Les critères de configuration d'IPSec à mettre en place seront :

– Chiffrement et authentification avec le protocole ESP.

– Authentification avec le protocole AH.

– Mode tunnel.

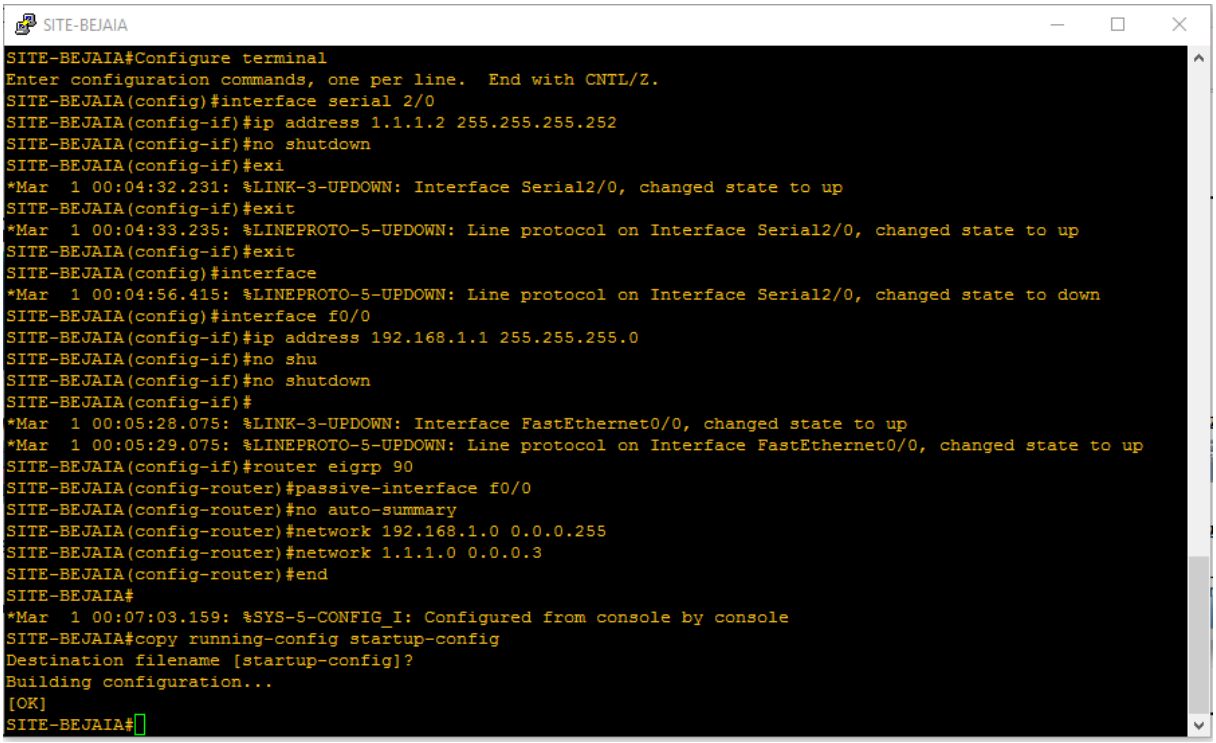
– Les algorithmes de chiffrement et d'authentification sont AES et SHA.

Une fois le tunnel IPSec mis en place, nous lancerons un *Ping* entre les deux machines (PCBejaia et PCAlger), et visualiser les SA établies ainsi que certaines informations sur le trafic échangé.

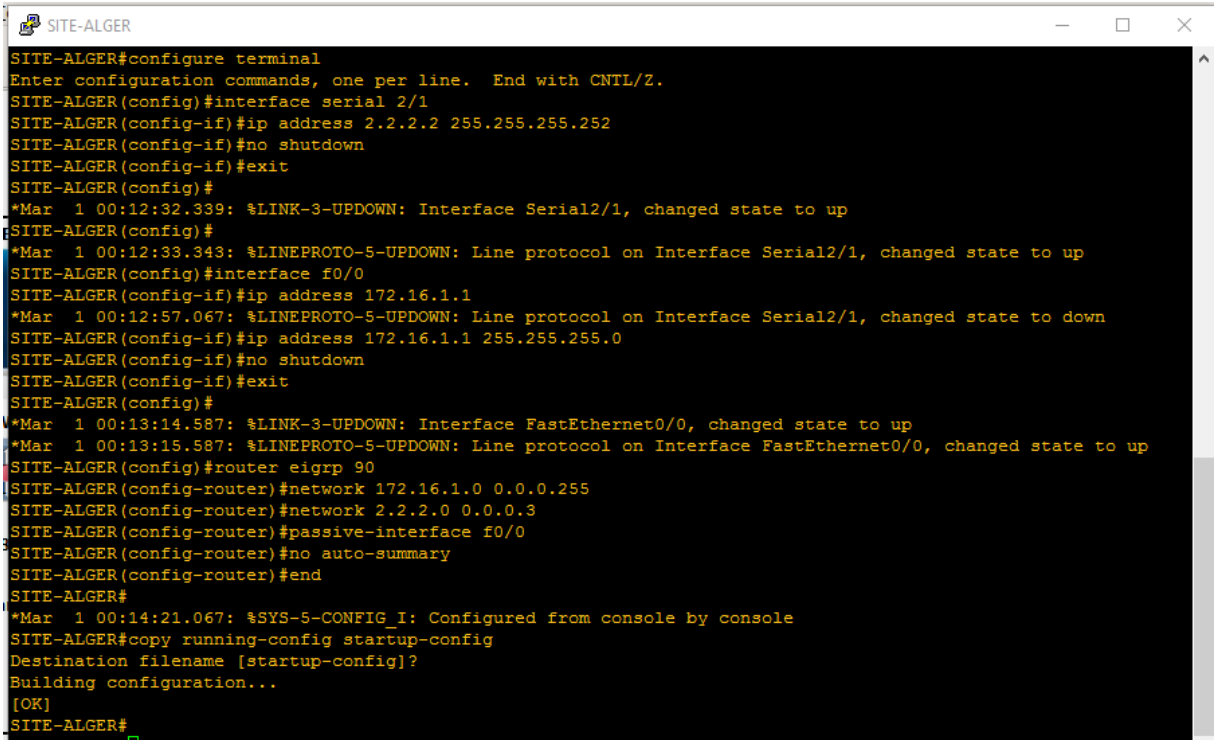
VI.3 Configuration (En ligne de commandes)

VI.3.1 Configuration des routeurs

Pour commencer, nous allons configurer les deux routeurs (SITE-BEJAI et SITE-ALGER), en indiquant les adresses IP des interfaces associés à chacun d'entre eux, ainsi que le protocole de routage utilisé par chaque routeur.



De même, nous allons effectuer la même configuration pour le routeur 2 :



Pour vérifier le bon fonctionnement du réseau créé, nous allons envoyer un *Ping* depuis la machine PC-BEJAIA vers la machine PC-ALGER. Une analyse du trafic à l'aide de Wireshark au niveau de l'interface Internet de routeur SITE-ALGER nous a donnée le résultat suivant :

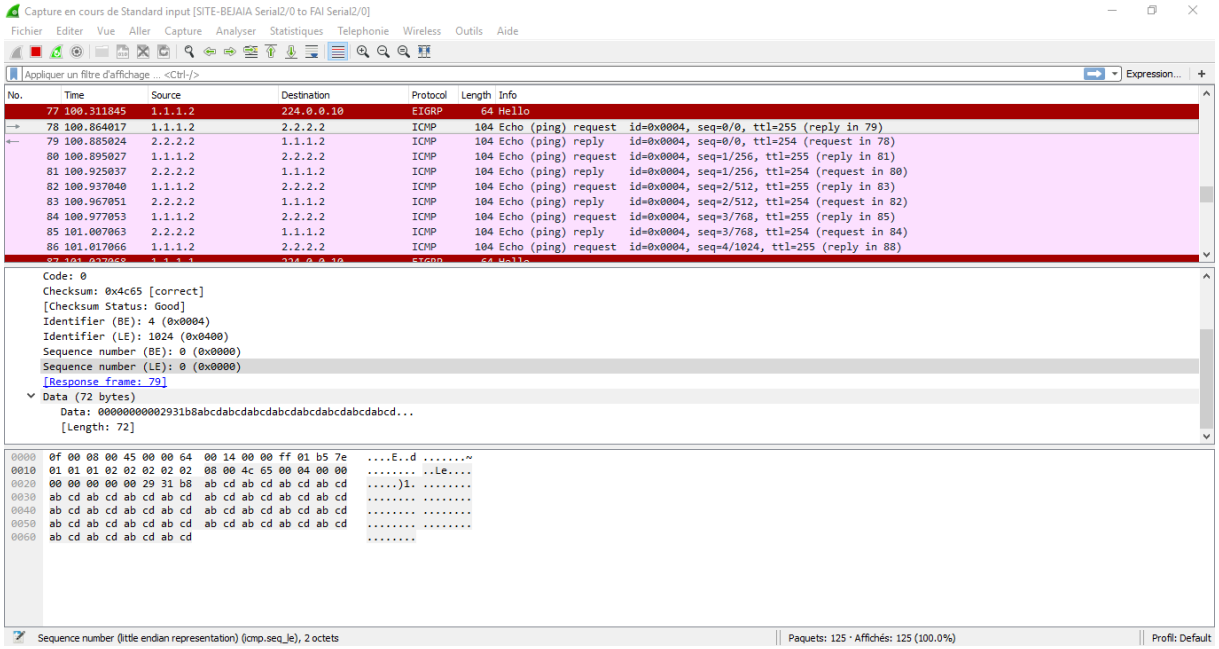


Figure VI.4–Capture d'un échange de données non sécurisé entre SITE-BEJAIAet SITE-Am8LGER

Nous remarquons que des informations importantes et détaillées ainsi que des adresses du réseau local, sont transportées en claire, cela présente une vulnérabilité, car un utililisateur malveillant, en possession de ces informations peut anticiper plusieurs types d'attaques.

VI.3.2 configuration du protocole IPSec

La configuration d'IPSec s'effectue généralement en suivant les étapes ci-dessous :

1. Configuration de la politique d'ISAKMP de la phase 1 du protocole IKE : algorithmes, clés, durée de vie du tunnel ISAKMP qui se trouveront à la suite de la ligne de configuration commençant par crypto isakmp.

2. Configuration de la SA IPSec de la phase 2 du protocole IKE (protocoles AH/ESP, algorithmes, durée de vie du tunnel IPSec) se trouveront à la suite de la ligne de configuration commençant par crypto ipsec.

3. Description d'une carte de cryptage (crypto map) rassemblant les paramètres des deux phases, l'extrémité du tunnel et la définition du trafic à sécuriser se trouvera à la suite de la ligne de configuration commençant par crypto map.

Il est très important de faire attention à ce que les configurations des deux routeurs soient cohérentes et symétriques, l'une par rapport à l'autre.

VI.3.3 Configuration d'IKE

Pour configurer le protocole IKE, nous allons réaliser les taches suivantes :

- Activation du protocole IKE.
- Configuration de la politique d'IKE (phase 1).
- Configuration de l'authentification mutuelle par clé pré-partagée.

VI.3.3.1 Activation du protocole IKE

Le mécanisme IKE est activé par défaut sur la plupart des IOS Cisco. Il est validé globalement pour toutes les interfaces sur un routeur Cisco. Pour s'assurer, nous allons exécuter les commandes suivantes sur les deux routeurs :

```
SITE-BEJAIA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-BEJAIA(config)#no crypto isakmp enable
SITE-BEJAIA(config)#
*Mar  1 00:48:08.131: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
SITE-BEJAIA(config)# crypto isakmp enable
SITE-BEJAIA(config)#
*Mar  1 00:48:15.855: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
SITE-BEJAIA(config)#
```

De même pour le routeur SITE-ALGER :

```
SITE-ALGER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-ALGER(config)#no crypto isakmp enable
SITE-ALGER(config)#no crypto isakmp enable
*Mar  1 00:51:04.663: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
SITE-ALGER(config)# crypto isakmp enable
SITE-ALGER(config)#
*Mar  1 00:51:10.327: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
SITE-ALGER(config)#
```

VI.3.3.2 Configuration des paramètres de la SA ISAKMP (IKE phase 1)

Dans cette étape nous allons créer une politique pour le mécanisme IKE sur chaque routeur, cette politique se définit par une combinaison des paramètres de sécurité à employer, le tableau ci-dessous indique la liste de ces paramètres.

Paramètre	Valeurs acceptées	Mot-clé	Par défaut
algorithme d'encryption	DES 56-bit	Des	DES 56-bit
	DES 168-bit	3des	DES 168-bit
	AES 128-bit	aes-128	AES 128-bit
	AES 256-bit	aes-256	
algorithme de hachage	SHA1 (HMAC variant)	Sha	SHA1
	MD5 (HMAC variant)	md5	
Méthode d'authentification	Signatures RSA	rsa-sig	RSA signatures
	Chiffrement RSA	rsa-encr	
	Clés pré-partagées	pre-share	
groupe Diffie-Hellman	D-H 768-bit	1	D-H 768-bit
	D-H 1024-bit	2	
durée de vie de la SA	Spécifier une valeur	–	86400 seconds

Table VI.2 –Liste des paramètres de sécurité pour IKE

Une politique définie indique quels paramètres de sécurité seront employés pour protéger les négociations suivantes et précise également comment les deux routeurs seront mutuellement authentifiés.

Pour la configuration des paramètres relatifs à la SA ISAKMP, nous allons procéder comme suit :

```
SITE-BEJAIA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-BEJAIA(config)#crypto isakmp policy 10
SITE-BEJAIA(config-isakmp)#encryption aes 256
SITE-BEJAIA(config-isakmp)#authentication pre-share
SITE-BEJAIA(config-isakmp)#group 5
SITE-BEJAIA(config-isakmp)#lifetime 3600
SITE-BEJAIA(config-isakmp)#
```

La même SA, avec les mêmes commandes seront implémentées sur le routeur SITE-ALGER

```
SITE-ALGER#
SITE-ALGER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-ALGER(config)#crypto isakmp policy 10
SITE-ALGER(config-isakmp)#encryption aes 256
SITE-ALGER(config-isakmp)#authentication pre-share
SITE-ALGER(config-isakmp)#group 5
SITE-ALGER(config-isakmp)#lifetime 3600
SITE-ALGER(config-isakmp)#
```

À l'issue de cette négociation, un tunnel sécurisé (phase 1 du protocole IKE) est établi entre les deux routeurs SITE-BEJAIA et SITE-ALGER. Désormais, la politique de sécurité

de phase 2 (SA IPSec) sera négociée à travers ce tunnel ISAKMP pour ces deux derniers.

VI.3.3.3 Configuration de l'authentification par clé pré-partagée

Dans cette étape nous allons configurer les clés pré-partagées que doit utiliser chaque hôte IPSec dans sa politique d'IKE en mode de configuration globale.

Pour le routeur SITE-BEJAIA nous indiquons "SCS-06000" comme clé pré-partagée :

```
SITE-BEJAIA(config)#crypto isakmp key 0 SCS-06000 address 2.2.2.2
SITE-BEJAIA(config)#
```

La même commande doit être saisie pour le routeur SITE-ALGER :

```
SITE-ALGER(config)#crypto isakmp key 0 SCS-06000 address 1.1.1.2
SITE-ALGER(config)#
```

VI.3.4 Configuration des paramètres IPSec (transform-set)

Une fois la négociation de la phase 1 faite, nous devons configurer les paramètres de négociation pour la phase 2.

Il s'agit de définir une transformation qui explicite les algorithmes IPSec (AH et/ou ESP) nécessaires pour la mise en œuvre du tunnel IPSec. Le tableau ci-dessous définit la liste des transformations disponibles. Le nom de la transformation est suivi de la commande crypto ipsec transform-set. Les transform-sets doivent être identiques aux deux paires.

Paramètre	Transform	Description
AH Transform	ah-md5-hmac	AH avec authentification MD5
	ah-sha-hmac	AH avec authentification SHA
ESP Encryption-Transform	esp-des	ESP avec cryptage DES
	esp-3des	ESP avec cryptage 3DES
	esp-aes	ESP avec cryptage AES
	esp-null	ESP sans cryptage
ESP Authentification -Transform	esp-md5-hmac	ESP avec authentification MD5
	esp-sha-hmac	ESP avec authentification SHA

Table VI.3 –Liste des transformations disponibles.

Pour la mise en place de notre transformation, nous allons taper la commande suivante sur le routeur SITE-BEJAIA :

```
SITE-BEJAIA(config)#crypto ipsec security-association lifetime seconds 1800
SITE-BEJAIA(config)#crypto ipsec transform-set SCSTRANS ah-sha-hmac esp-aes esp-sha-hmac
```

La même commande sur le routeur SITE-ALGER :

```
SITE-ALGER(config)#crypto ipsec security-association lifetime seconds 1800
SITE-ALGER(config)#crypto ipsec transform-set SCSTRANS ah-sha-hmac esp-aes esp-sha-hmac
```

VI.3.5 Configuration des listes d'accès

Il faut configurer une liste d'accès qui définit le trafic à sécuriser. Ces listes d'accès sont différentes des ACLs qui déterminent quel trafic à expédier ou bloquer sur une interface. C'est l'entrée de la crypto map référençant la liste d'accès qui décide si le traitement d'IPSec est appliqué au trafic en fonction de l'action (permit et/ou deny) définie dans la liste d'accès.

Pour le routeur SITE-BEJAIA nous allons procéder comme suit :

```
SITE-BEJAIA(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

De même, nous allons définir l'ACL associée au SITE-ALGER :

```
SITE-ALGER(config)#access-list 101 permit ip  172.16.1.0 0.0.0.255 192.168.1.0 0.0.0.255
```

VI.3.6 Configuration de la carte de cryptage (crypto map)

La carte de cryptage (ou crypto map) permet de lier les SA négociées et la politique de sécurité (SP : *Security Policy*). En d'autres termes, elle permet de renseigner :

1. Quel trafic devrait être protégé par IPSec.
2. L'autre extrémité du tunnel vers lequel le trafic IPSec devrait être envoyé.
3. L'adresse locale à employer pour le trafic d'IPSec.
4. Quelle sécurité d'IPSec devrait être appliquée à ce trafic (transform-set).

Pour créer les différentes entrées de la carte de cryptage, qui emploieront IKE pour établir les associations de sécurité, nous allons procéder comme suit en suivant les étapes ci-dessous.

```
SITE-BEJAIA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-BEJAIA(config)#cryp
SITE-BEJAIA(config)#crypto m
SITE-BEJAIA(config)#crypto map SCSMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
SITE-BEJAIA(config-crypto-map)#set peer 2.2.2.2
SITE-BEJAIA(config-crypto-map)#set pfs group5
SITE-BEJAIA(config-crypto-map)#set security-association lifetime seconds 900
SITE-BEJAIA(config-crypto-map)#set transform-set scstrans
ERROR: transform set with tag "scstrans" does not exist.

SITE-BEJAIA(config-crypto-map)#set transform-set SCSTRANS
SITE-BEJAIA(config-crypto-map)#match address 101
SITE-BEJAIA(config-crypto-map)#
```

Les mêmes commandes seront implémentées sur le routeur SITE-ALGER :

```
SITE-ALGER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-ALGER(config)#crypto map SCSMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
SITE-ALGER(config-crypto-map)#set peer 1.1.1.2
SITE-ALGER(config-crypto-map)#set pfs group5
SITE-ALGER(config-crypto-map)#set security-association lifetime seconds 900
SITE-ALGER(config-crypto-map)#set transform-set SCSTRANS
SITE-ALGER(config-crypto-map)#match address 101
SITE-ALGER(config-crypto-map)#
```

VI.3.7 Application des crypto map aux interfaces

Il faut lier la crypto map ainsi définie à une interface du routeur par laquelle le trafic d'IPSec passera. Tout trafic arrivant ou sortant de cette interface est comparé avec le trafic à sécuriser défini dans une liste d'accès : s'il y a correspondance ce dernier est chiffré.

Pour appliquer la crypto map SCSMAP à l'interface Internet sur SITE-BEJAIA, nous allons procéder comme suit :

```
SITE-BEJAIA#
SITE-BEJAIA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-BEJAIA(config)#in
SITE-BEJAIA(config)#interface S 2/0
SITE-BEJAIA(config-if)#crypto map SCSMAP
SITE-BEJAIA(config-if)#
*Mar  1 01:33:54.539: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
SITE-BEJAIA(config-if)#
```

La même chose pour le routeur SITE-ALGER:

```
SITE-ALGER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SITE-ALGER(config)#in
SITE-ALGER(config)#interface S 2/1
SITE-ALGER(config-if)#crypto map SCSMAP
SITE-ALGER(config-if)#
*Mar  1 01:35:08.699: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
SITE-ALGER(config-if)#
```

VI.4 tests de fonctionnement

Nous allons faire un ping entre le PC de Bejaia vers le PC de Alger ping ‘’172.16.1.10 ‘’.

```
C:\Windows\system32>ipconfig

Configuration IP de Windows


Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::75e1:6dd7:2ac4:9655%11
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.10
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.1.1

Carte Tunnel isatap.{1E0DC054-195F-4D64-91CE-8C0C1443A290} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Tunnel isatap.{724ADA5C-002D-4C1D-ACBF-D749F6108369} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Windows\system32>ping 172.16.1.10

Envoi d'une requête 'Ping'  172.16.1.10 avec 32 octets de données :
Réponse de 172.16.1.10 : octets=32 temps=34 ms TTL=254
Réponse de 172.16.1.10 : octets=32 temps=40 ms TTL=254
Réponse de 172.16.1.10 : octets=32 temps=54 ms TTL=254
Réponse de 172.16.1.10 : octets=32 temps=41 ms TTL=254

Statistiques Ping pour 172.16.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 34ms, Maximum = 54ms, Moyenne = 42ms
```

Afin de vérifier le bon fonctionnement du VPN, plusieurs commandes sont à notre disposition en mode privilégié.

- La commande "show crypto engine connections active" nous permet de voir les connexions cryptées actives :

```
Packet sent with a source address of 192.168.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/31/40 ms
SITE-BEJAIA#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   1 Serial2/0            1.1.1.2         set    HMAC_SHA+AES_256_C        0        0
2001 Serial2/0            1.1.1.2         set    SHA+AES+SHA               0        4
2002 Serial2/0            1.1.1.2         set    SHA+AES+SHA               4        0

SITE-BEJAIA#
```

- La commande "show crypto ipsec transform-set" nous permet de voir les différents types d'encodage actifs.

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

- La commande "show crypto ipsec sa" fourni une version plus détaillé que les deux commandes citées plus haut.

```
SITE-BEJAIA#show crypto  ipsec sa

interface: Serial2/0
    Crypto map tag: SCSMAP, local addr 1.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
   current_peer 2.2.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #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.: 1.1.1.2, remote crypto endpt.: 2.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
     current outbound spi: 0xF3F7FCBD(4093115581)

     inbound esp sas:
      spi: 0x652653FA(1697010682)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: SCSMAP
        sa timing: remaining key lifetime (k/sec): (4480661/708)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
      spi: 0x9D014475(2634105973)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: SCSMAP
        sa timing: remaining key lifetime (k/sec): (4480661/705)
        replay detection support: Y
        Status: ACTIVE

     inbound pcp sas:

     outbound esp sas:
 --More--
```

- La commande "show crypto isakmp sa" fourni des informations sur l'association de sécurité d'ISAKMP.

```
SITE-BEJAIA#show crypto isakmp sa
dst             src             state          conn-id slot status
2.2.2.2         1.1.1.2         QM_IDLE              1    0 ACTIVE

SITE-BEJAIA#
```

- La commande "show crypto map sa" nous permet de visionner des informations relatives aux cartes de cryptage crées.

```
SITE-BEJAIA#show crypto map
Crypto Map "SCSMAP" 10 ipsec-isakmp
        Peer = 2.2.2.2
        Extended IP access list 101
            access-list 101 permit ip 192.168.1.0 0.0.0.255 172.16.1.0 0.0.0.255
        Current peer: 2.2.2.2
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={
                SCSTRANS,
        }
        Interfaces using crypto map SCSMAP:
                Serial2/0

SITE-BEJAIA#
```

- En fin, nous allons effectuer un *sniffing* à l'aide de Wireshark pour visionner le trafic échangés entre les deux sites. Un "Ping 172.16.1.10" de PCBejaia vers PCAlger nous donne le résultat suivant :

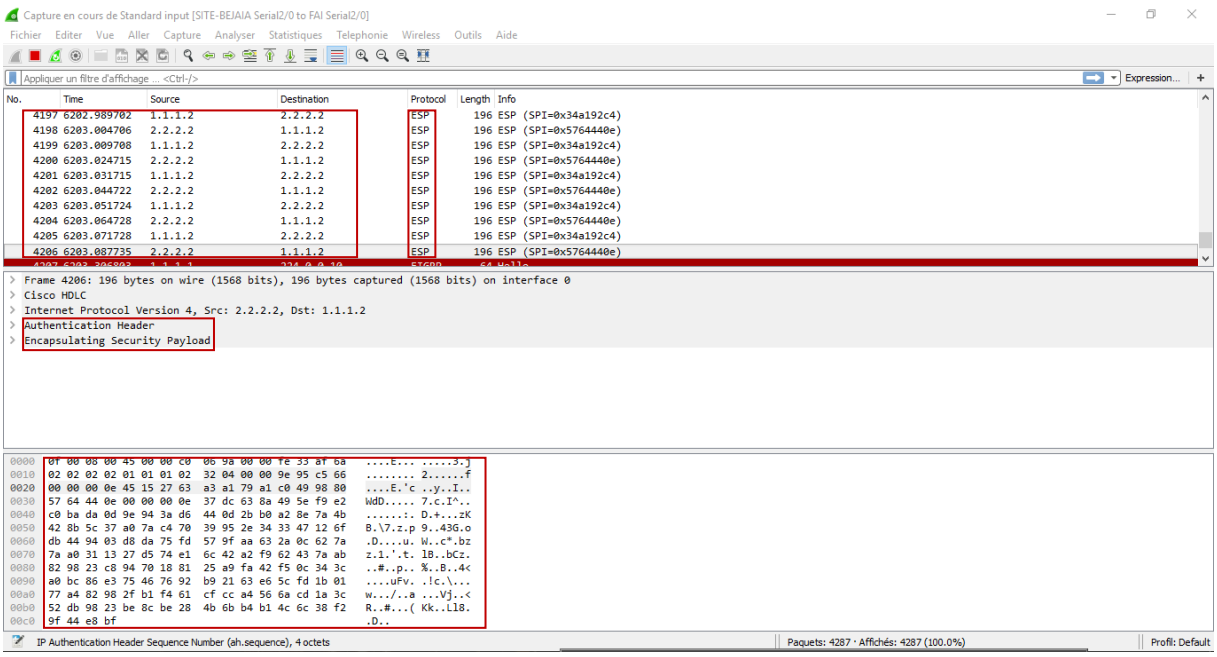


Figure VI.4– Capture d'un échange de données sécurisé entre SITE-BEJAIA et SITE-ALGER

Nous remarquons très bien que le flux d'informations circulant entre les deux LANs est crypté, et que les adresses machine (sources et/ou destinations) n'apparaissent pas, cela confirme que le VPN fonctionne parfaitement.

VI.5 La partie LAN

VI.5.1 Présentation des VLAN utilisés

Les VLAN permettant de créer des réseaux logiques au sein de commutateurs et routeurs physiquement raccordés au même réseau. Ils permettent de regrouper les utilisateurs par fonction dans l'entreprise (commerciaux, techniciens, assistants,…), par niveau de droits (administrateurs, utilisateurs,…) ou autre. Il s'agit d'une conception pleinement logique, sans tenir compte de la localisation géographique de l'utilisateur dans l'entreprise.

Les VLAN représentés dans notre projet sont les suivants :

- VLAN Informatique.
- VLAN Commercial.
- VLAN Importation.
- VLAN RH.
- VLAN gestion.

Les noms et les identificateurs des VLAN à implémenter ainsi leur adressage seront représentés comme suit :

Nom du VLAN	VLAN-ID	Description	Adresse VLAN
Informatique	10	Informatique	192.168.2.0/24
Commercial	20	Commercial	192.168.3.0/24
Importation	30	Importation	192.168.4.0/24
RH	40	Ressources Humaine	192.168.5.0/24
Gestion	99	Gestion	192.168.99.0/24

1) Configuration du mode trunk sur les interfaces

Nous allons configurer les liens trunk. Les interfaces a configuré en mode trunk sont au niveau des commutateurs distributeur et accès, on utilisera la commande «range » pour réunir toutes les interfaces en une seule fois.

- pour le switch distributeur

```
SWD-1(config)#interface range eth 0/1, eth 0/3, eth 0/2, eth 1/1, eth 1/0
SWD-1(config-if-range)#switchport trunk  encapsulation Dot1q
SWD-1(config-if-range)#switchport mode trunk
SWD-1(config-if-range)#
*Jun 13 15:27:58.902: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
SWD-1(config-if-range)#
```

- pour le switch client 1

```
SWA-1(config)#interface range eth 0/2, eth 0/3
SWA-1(config-if-range)#switchport trunk encapsulation Dot1q
SWA-1(config-if-range)#
*Jun 13 15:30:31.660: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/2 TDR=0, TRC=0
SWA-1(config-if-range)#switchport mode trunk
```

- Pour le switch client 2

```
SWA-2(config)#INTerface range eth 1/0, eth 1/1
SWA-2(config-if-range)#switchport trunk encapsulation
*Jun 13 15:32:32.325: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SWA-2(config-if-range)#switchport trunk encapsulation Dot1q
SWA-2(config-if-range)#switchport mode trunk
SWA-2(config-if-range)#no sh
SWA-2(config-if-range)#
```

- Interface mode trunk 99

```
SWD-1(config)#interface VLan 99
SWD-1(config-if)#ip address 192.168.99.2 255.255.255.0
SWD-1(config-if)#no shutdown
```

2) Configuration du protocole VTP et les sécurités sur les commutateurs

Les tâches de configuration VTP courantes consistent à paramétrer le mode de fonctionnement, le domaine et le mot de passe.

Le commutateur server déclare en mode serveur, on lui attribut également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié et supprimé. Ainsi chaque commutateur client (client1, client2) présent dans le domaine hériteront automatiquement de nouveaux VLAN crées sur le commutateur serveur.

- Création de VTP mode serveur

```
SWD-1(config)#vtp password cisco
Password already set to cisco
SWD-1(config)#vtp domain SCS
Domain name already set to SCS.
SWD-1(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD-1(config)#vtp version 3
VTP version is already in V3.
SWD-1(config)#vtp pruning
Pruning already switched on
```

- Affichage de VTP mode serveur

```
SWD-1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : SCS
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0100

Feature VLAN:
--------------
VTP Operating Mode                : Server
Number of existing VLANs          : 10
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 4096
Configuration Revision            : 0
Primary ID                        : 0000.0000.0000
Primary Description               :
MD5 digest                        :
```

- Création de VTP mode client1 même configuration pour le client 2

```
SWA-1(config)#vtp password cisco
Setting device VTP password to cisco
SWA-1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SWA-1(config)#
```

- Affichage de VTP mode client

```
SWA-1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : SCS
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0200
Configuration last modified by 0.0.0.0 at 6-16-17 20:32:35

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 10
Configuration Revision            : 6
MD5 digest                        : 0x7A 0x10 0xDF 0xC6 0x40 0x63 0x6B 0xF8
                                    0xB9 0x20 0x66 0x44 0x73 0x85 0xD9 0xA0
```

3) Création et affichage des VLANs

Pour configurer nos VLAN sur le commutateur il faut d'abord créer ces VLAN, Les commandes **enable** et **configure terminal** permettent de passer en mode privilégié pour la gestion et la configuration du commutateur.

- Creation des VLANs SWD

```
SWD-1(config)#vtp password cisco
Password already set to cisco
SWD-1(config)#vtp domain SCS
Domain name already set to SCS.
SWD-1(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD-1(config)#vtp version 3
VTP version is already in V3.
SWD-1(config)#vtp pruning
Pruning already switched on
```

- Creation des VLANs SWA 1

```
SWA-1(config)#vtp password cisco
Setting device VTP password to cisco
SWA-1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SWA-1(config)#
```

- Affichage des vlans vtp client

```
SWA-1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : SCS
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0200
Configuration last modified by 0.0.0.0 at 6-16-17 20:32:35

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 10
Configuration Revision            : 6
MD5 digest                        : 0x7A 0x10 0xDF 0xC6 0x40 0x63 0x6B 0xF8
                                    0xB9 0x20 0x66 0x44 0x73 0x85 0xD9 0xA0
```

4) Affectation et affichage des ports aux vlans

- Affectation des ports pour le VLAN 10

```
SWA-1(config)#interface eth 0/2
SWA-1(config-if)#switchport mode access
SWA-1(config-if)#switchport access vlan 10
SWA-1(config-if)#
```

- Affectation des ports pour le VLAN 20

```
SWA-1(config-if)#interface eth 3/3
SWA-1(config-if)#switchport mode access
SWA-1(config-if)#switchport access vlan 20
SWA-1(config-if)#
```

- Affectation des ports pour le VLAN 30

```
SWA-2(config)#interface eth 1/1
SWA-2(config-if)#switchport mode access
SWA-2(config-if)#switchport access vlan
*Jun 13 15:44:56.088: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SWA-2(config-if)#switchport access vlan 30
```

- Affectation des ports pour le VLAN 40

```
SWA-2(config)#interface eth 1/0
SWA-2(config-if)#switchport mode access
SWA-2(config-if)#switchport access vlan 40
SWA-2(config-if)#
```

- Affectation des ports pour le VLAN 99

```
SWA-2(config)#interface eth 1/2
SWA-2(config-if)#switchport mode access
SWA-2(config-if)#switchport access vlan 99
```

- affichage des ports au vlan du SWA2

```
SWA-2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/3, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
                                                Et3/1, Et3/2, Et3/3
10   Informatique                     active
20   Comercial                        active
30   Importation                      active    Et1/1
40   RH                               active    Et1/0
99   Gestion                          active    Et1/2
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

5) Affectation des ports au Vlan native

- Pour le switch distributeur

```
SWA-1(config)#interface range eth0/2 ,eth0/3
SWA-1(config-if-range)#switchport trunk native vlan 99
SWA-1(config-if-range)#
```

```
SWD-1(config-if-range)#interface range eth0/2, eth0/3 ,eth 1/1 ,eth 1/0
SWD-1(config-if-range)#switchport trunk native vlan 99
SWD-1(config-if-range)#
```

- Pour le SWA1

```
SWA-1(config)#interface eth0/0
SWA-1(config-if)#switchport mode access
SWA-1(config-if)#switchport access vlan 10
SWA-1(config-if)#
*Jun 16 20:45:53.269: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SWA-1(config-if)#interface eth0/1
SWA-1(config-if)#switchport mode access
SWA-1(config-if)#switchport access vlan 20
SWA-1(config-if)#
```

- Pour le SWA2

```
SWA-2(config)#interface eth 0/0
SWA-2(config-if)#switchport mode access
SWA-2(config-if)#switchport access vlan 30
SWA-2(config-if)#interface eth 0/1
SWA-2(config-if)#switchport mode access
SWA-2(config-if)#switchport access vlan 40
*Jun 16 20:53:49.083: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SWA-2(config-if)#switchport access vlan 40
SWA-2(config-if)#interface eth 0/2
SWA-2(config-if)#switchport mode access
SWA-2(config-if)#switchport access vlan 99
```

6) Création des interfaces VLAN natives sur tout les switchs

- Sur le switch distributeur

```
SWD-1(config)#interface  vlan 99
SWD-1(config-if)#ip address 192.168.99.1 255.255.255.0
SWD-1(config-if)#no sh
```

- Sur le switch d'accès 1

```
SWA-1(config)#interface  vlan 99
SWA-1(config-if)#ip address  192.168.99.3 255.255.255.0
*Jun 16 21:58:16.892: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SWA-1(config-if)#ip address  192.168.99.3 255.255.255.0
SWA-1(config-if)#no sh
```

- Sur le switch d'accès 2

```
SWA-2(config)#interface vlan 99
SWA-2(config-if)#ip address 192.168.99.2 255.255.255.0
SWA-2(config-if)#no shu
SWA-2(config-if)#
```

7) Permutation d'accès pour les VLANs native

- permutation des vlan 10, 20, 40, 99 sur le SWA-1

```
SWD-1(config)#interface range eth0/2,eth0/3 ,eth 1/0 ,eth1/1 ,eth0/1
SWD-1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,99
SWD-1(config-if-range)#
```

- permutation des vlan 10, 20, 30, 40, 99 sur le SWA-2

```
SWA-2(config-if-range)#interface range eth 0/2 , eth0/3
SWA-2(config-if-range)#switchport trunk allowed vlan 10,20,30,40,99
SWA-2(config-if-range)#
```

8) Configuration et affichage d'etherchannel 'redondance LAN '

Dans notre cas on a utilisé le protocole LACP qui est standard qui fonctionne entre les équipements cisco et non cisco.

- Pour le switch distributeur

```
SWD-1(config)#interface range eth0/2, eth0/3
*Jun 16 21:21:47.330: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
SWD-1(config)#interface range eth0/2, eth0/3
SWD-1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1

SWD-1(config-if-range)#exit
SWD-1(config)#interface range eth0/2, eth0/3
*Jun 16 21:22:29.182: %EC-5-L3DONTBNDL2: Et0/3 suspended: LACP currently not enabled on the remo
*Jun 16 21:22:29.692: %EC-5-L3DONTBNDL2: Et0/2 suspended: LACP currently not enabled on the remo
SWD-1(config)#interface range eth0, eth0/3
*Jun 16 21:22:31.983: %AMDP2_FE-6-EXCESSCOLL: Ethernet1/1 TDR=0, TRC=0
SWD-1(config)#interface range eth1/1, eth1/0
SWD-1(config-if-range)#channel-group 2  mode active
Creating a port-channel interface Port-channel 2
```

- Pour le switch accès 1

```
SWA-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA-1(config)#interface range
*Jun 16 21:25:01.261: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SWA-1(config)#interface range eth 0/2 ,eth 0/3
SWA-1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
```

- le switch accès 2

```
SWA-2(config)#interface range eth1/0 ,eth 1/1
SWA-2(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2
```

- Affichage d'etherchannel

```
SWD-1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/2(P)    Et0/3(P)
2      Po2(SU)         LACP      Et1/0(P)    Et1/1(P)
```

9) Routage inter vlan

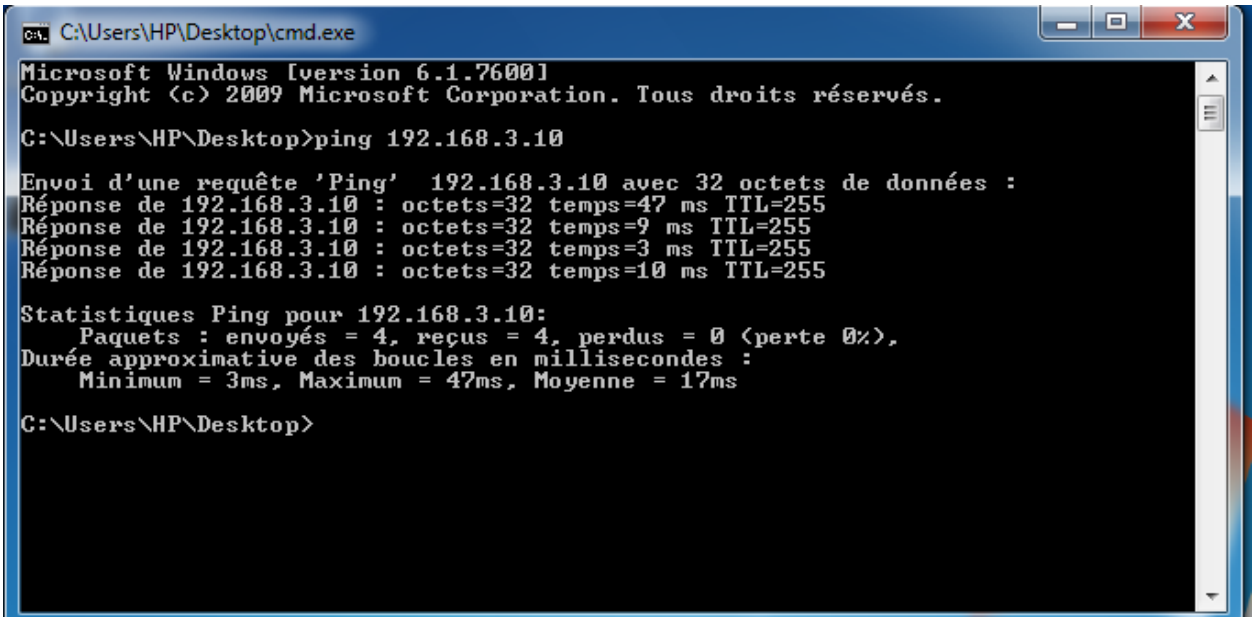
Une fois la configuration de notre commutateur effectué, il va falloir acheminer le trafic de nos VLANs et les permettre de communiquer entre eux.

```
SITE-BEJAIA(config)#interface fastEthernet 0/0
SITE-BEJAIA(config-if)#no sh
SITE-BEJAIA(config-if)#interface fastEthernet 0/0.10
SITE-BEJAIA(config-subif)#encapsulation dot1Q 10
SITE-BEJAIA(config-subif)#ip address 192.168.2.254 255.255.255.0
SITE-BEJAIA(config-subif)#interface fastEthernet 0/0.20
SITE-BEJAIA(config-subif)#ip address 192.168.3.254 255.255.255.0
SITE-BEJAIA(config-subif)#encapsulation dot1Q 20
SITE-BEJAIA(config-subif)#interface fastEthernet 0/0.30
SITE-BEJAIA(config-subif)#encapsulation dot1Q 30
SITE-BEJAIA(config-subif)#ip address 192.168.4.254 255.255.255.0
SITE-BEJAIA(config-subif)#interface fastEthernet 0/0.40
SITE-BEJAIA(config-subif)#encapsulation dot1Q 40
SITE-BEJAIA(config-subif)#ip address 192.168.5.254 255.255.255.0
SITE-BEJAIA(config-subif)#interface fastEthernet 0/0.99
SITE-BEJAIA(config-subif)#encapsulation dot1Q 99
SITE-BEJAIA(config-subif)#ip address 192.168.99.254 255.255.255.0
```

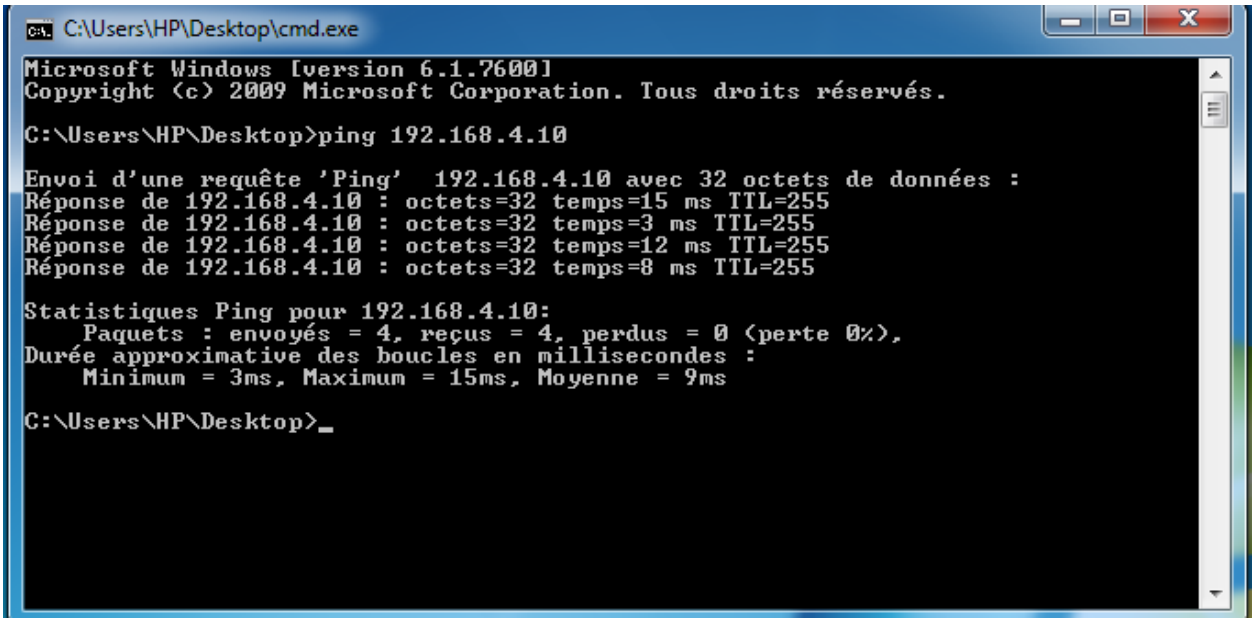
VI.5.3 Test entre Vlans

Dans cette étape on vérifie la communication entres les VLANs crées au niveau de site de Bejaia, en utilisant la commande ping.

- Ping entre VLAN 10 et VLAN 20



- Ping entre VLAN 10 et VLAN 30



Conclusion

Pour clôturer notre projet, nous avons commencé par introduire l'émulateur GNS3, nous l'avons par la suite utilisé pour la configuration de la liaison VPN site-à-site sécurisé grâce au protocole IPSec, ainsi que la segmentation de réseau local par la création des VLANs.

Conclusion générale

Le domaine de la sécurité informatique est considéré comme difficile pour sa complexité de mettre en œuvre une solution durable qui répond parfaitement aux besoins et exigences ressentis dans une entreprise, ce qui pousse les ingénieurs réseau à travailler sans relâche à fin d'arriver à une solution permettant l'amélioration de la sécurité de leur réseau.

Nous avons constaté après notre étude consacrée au mécanisme de sécurisation, son avantage qui concerne la sécurité des données et leurs échanges entre deux sites distants.

Le présent travail fait était les résultats obtenus lors de la mise en place d'un réseau VPN site-à-site à l'entreprise SCS. Nous avons en effet grâce a cette nouvelle technologie permis aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPN, ce partage était possible en internet pour les utilisateurs du réseau local de l'entreprise.

La mise en place de VPN site-à- site placés dans une entreprise permet aux réseaux privés de se relier et de s'étendre entre eux a travers internet en toute sécurité ainsi que la réduction du coût des infrastructures réseaux.

La technologie VPN basée sur le protocole IPSec est considérée comme l'un des facteurs clés de réussite qui est en constante évolution.

En conséquence, nous avons exposé un travail divisé en deux grandes parties, à savoir l'approche théorique qui était subdivisé en deux chapitres : le premier a porté sur les généralités à propos des réseaux informatiques, le second est dédié au VPN où nous avons basé de façon claire sur les notions, le fonctionnement ainsi que les différents protocoles utilisés pour la mise en œuvre de réseau VPN, et quant à la deuxième partie, elle est consacrée à la finalisation du projet, qui était aussi subdivisé en deux chapitres dont le premier a maintenu l'étude préalable dans laquelle nous avons présenté l'entreprise et exposé la problématique, laquelle nous avons solutionné par une solution VPN site-à-site qui consiste à mettre au point une liaison permanente, distante et sécurisée entre sites du SCS à savoir Béjaia et Alger et aussi on a segmenté le réseau local en plusieurs LAN virtuels, pour réduire les domaines de collisions et éviter les congestions. Ce qui permet de renforcer la sécurité au niveau du réseau local.

Le second est le dernier chapitré à été consacré à la réalisation du projet, où nous avons introduit les outils et logiciels ayant servi à l'élaboration du projet, à savoir GNS3 tout en expliquant les configurations, nous avons par la suite implémenté la solution VPN grâce au protocole IPSec.

En fin, la concrétisation de ce projet, nous a permis d'apporter une contribution à l'entreprise SCS et aussi d'acquérir de nouvelles connaissances sur le protocole IPSec grâce à une étude détaillée sur son fonctionnement, ses principes et les protocoles qu'il utilise.

Ainsi que, cette recherche nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour notre groupe de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nous connaissances sur l'administration et sécurité des réseaux informatiques.

Webliographie

[16] : Agence nationale de la sécurité des systèmes d'information, "Recommandations de sécurité relatives à IPSec", Note technique, disponible sur : www.ssi.gov.fr/uploads/2012/09/NT_IPSec.pdf, Avril 2017.

[11] : Denis de REYNAL, "Présentation sur les VPN", Rapport d'exposé, disponible sur http://igm.univ-mlv.fr/~duris/NTREZO/20032004/DeReynal-DeRorthais-Tan-VPN.pdf. mars 2017.

18] : GNS3, disponible sur : http://www.noplay.net/GNS3.html, juin 2017.

[17] "IPSec Présentation Technique", cour, disponible sur : http://www.univ-tebessa.dz/fichiers/master/master_1499.pdf, Mai 2017.

[1] : http://www.institut-numerique.org/chapitre-ii-generalite-sur-le-reseau-informatique-, mars 2017

[3] : http://www.cisco.com/web/learning/netocad/index.html, Avril 2017.

[15] : " Les VPN ", cour, disponible sur : http://perso.modulonet.fr/placuire/Ressource/BTS2-AMSI/Chap-8-Les-VPN.pdf, Avril 2017.

Bibliographie

[2]: Arnaud S. et Guillaume D, "Les VLANs: les protocoles de trasport et de controle", 2006.

[6] : Aurélien Géron, "WIFI Professionnel La norme 802.11, le déploiement, la sécurité ", DUNDO 3 ème édition, Paris, 2004, 2006, 2009. OSI.

[12] : Guy PUJOLLE, "Les réseaux", Eyrolles édition 2014.

[13] : Guillaume Desgeorge, « La sécurité des réseaux », Cour, 2000.

[14] : Jean-paul ARCHIER, « Les VPN fonctionnement, mise en œuvre et maintenance des Réseaux privés virtuel », Editions ENI, Juin 2010.

[4] : José DORDOIGNE, "Réseau Informatique", ENI 6 ème édition, Mars 2015.

[19] : Ksiks A, “Etude et simulation sue GNS3 du service MP-BGP/VPN-IP”, 2011.

[8] : Khelfa M, “ Introduction à la sécurité Informatique “, Laboratoire des logiciels de Base Session en France, 2002.

[9] : Mannuel S, lic.phil.I, collaborateur scientifique, center for Security Studies (CSS), ETH Zurich, aout 2006.

[7] : Mr RIAHLA, “Introduction a la sécurité Informatique“, Département de physique/Infotronique IT/S6, Université de limoge France, 2008/2009.

[10] : Rodrigue M, “Mise en place d’un système de sécurité basé sur l’authentification dans un réseau IP “, mémoire en Master, Université Lyon, 2011.

[5] : Romain LEGRAND & André VAUCAMPS, “CISCO : Notions de base sur les réseaux“, Editions ENI, Décembre 2014.TCP/IP

Résumé :

En ces temps modernes, la sécurité informatique est indispensable pour le bon fonctionnement de n'importe quel réseau informatique vu son extrême importance. C'est pour cette raison que les ingénieurs réseau d'entreprise doivent échafauder des mécanismes et des protocoles de gestion et de sécurité plus robustes et efficaces afin de protéger leurs réseaux.

L'objectif du travail accompli est de réussir à mettre en œuvre une amélioration de l'architecture de réseau de SCS, afin de gérer et sécuriser d'une bonne manière le transfert de données entre les services de deux sites distants. A cet effet, nous avons organisé l'ensemble des utilisateurs du réseau en VLANs selon leurs fonctions ou catégories, puis nous avons configuré un VPN sécurisé entre les deux réseaux locaux reliant BEJAIA et ALGER avec GNS3.

Au cours de notre stage, nous avons pu apporter une amélioration des services que peut fournir l'utilisation des moyens de communication et de sécurité réseaux indispensable dans notre vie quotidienne.

Mots-clés : VLAN, VPN, GNS3.

Abstract :

In these modern times, computer security is essential for the proper functioning of any computer network given its extreme importance. For this reason, enterprise network engineers need to build more robust and efficient mechanisms and management and security protocols to protect their networks.

The goal of the work is to successfully implement an enhanced SCS network architecture to manage and securely transfer data between the services of two remote sites. For this purpose, we have organized all the users of the network in VLANs according to their functions or categories, then we have configured a secure VPN between the two local networks connecting BEJAIA and ALGER with GNS3.

During our internship, we were able to provide an improvement of the services that can provide the use of the means of communication and security networks indispensable in our daily life.

Keywords : VLAN, VPN, GNS3.