République Algérienne Démocratique et Populaire
Ministre de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira-Bejaia

Faculté des Sciences et Technologies
Département A.T.E

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Mémoire fin d'étude

Filière : Télécommunications

Specialite : Reseaux et telecommunications

THÈME

Étude et mise en place des liaisons virtuelles (VLAN,VPN)

Presente par :

- **BRAHMI** *Ilhem*
- **GUENANE** *Anaïs*

Les jury :

- Président : **Mr** ***BESSAAD***
- Examinateur : **Mr** ***AZNI***
- Encadrant : **Mr** ***A. DIBOUNE***

Annee universitaire : 2021/2022

Remerciement

Avant d'entamer ce projet de fin d'étude, nous tenons à traduire notre immense gratitude envers tous ceux qui ont contribué de près ou de loin au bon déroulement de notre travail.

Nous adressons ainsi notre grande reconnaissance envers nos parents et à toutes nos familles qui ont été d'un grand soutien. Leurs encouragements et leur suivi avec patience, nous a donné la force de mener à terme notre travail.

Nous tenons à remercier vivement notre promoteur Monsieur ***A. DIBOUNE*** , d'avoir accepté de diriger notre travail, pour sa disponibilité, son aide et ses précieux conseils.

Nous tenons aussi à remercier tous les membres de la commission du jury **M^r^** ***BESSAAD*** et **M^r^** ***AZNI*** qui évalueront notre travail.

Un profond merci pour Monsieur ***Y. DJEBBARI*** , pour l'accueil chaleureux auquel nous avons eu droit au sein de son entreprise, pour ses précieux conseils et tous les moyens qui nous ont été offert pour mener à bien notre projet.

Nous remercions également tous les membres du département ***ATE*** ainsi que tous nos enseignants qui ont pris part à notre formation universitaire.

Merci à toutes et à tous.

Dédicaces

Je dédie ce mémoire à :

Mes très chers parents qui m'ont toujours soutenue tout au long de mes études et qui ont contribué à ma réussite, que dieu les bénisse et leur donne une longue vie.

Mon frère ***Lotfi*** *et mes deux chères sœurs* ***Cylia*** *et* ***Dalal*** *que j'aime beaucoup et à qui je souhaite une bonne réussite dans leurs études et dans leur vie.*

Toute ma famille ***BRAHMI****.*

Ma binôme ***Anaïs****, avec qui j'ai partagé de belles années d'études, ainsi que toute sa famille.*

Mes chers copines et amis.

Ilhem.

Je dédie ce modeste travail à :

Mes très chers parents, auxquels nulle dédicaces peut exprimer ma profonde gratitude envers tous les sacrifices et le soutiens qu'ils m'ont apportés durant toute mon existance faisant de moi la personne que je suis aujourd'hui.

Mon frère ***Yanis****, qui a toujours été un model et une source inépuisable d'inspiration et de force.*

Mes petites sœurs de cœur ***Léa*** *et* ***Tania****, pour lesquelles je porte une immense affection.*

Toute ma famille.

Ma binôme ***Ilhem****, qui a rendu ces années mémorables, ainsi que toute sa famille.*

Tous mes amis (es).

Anaïs.

Table des matieres

Table des figures

Liste des tableaux

Glossaire

D

DHCP : *Dynamic host configuration protcol.*
DTP : *Dynamic Trunking Protocol.*

G

GRE : *Generic Routing Encapsulation.*
GVRP : *Generic VLAN Register Protocol.*

I

IEEE : *Institute of Electrical and Electronics Engineers.*
IGP : *Interior Gateway Protocol.*
IGPR : *Interior Gateway Routing Protocol.*
IP : *Internet Protocol.*
IPSec : *Internet Protocol Security.*
IS-IS : *Intermediate system to intermediate system.*
ISL : *Inter-Switch Link.*

L

LAN : *Local Area Network.*

M

MAN : *Métropolitain Area Network.*

O

OSPF : *Open Shortest Path First.*

P

PAN : *Personnel Area Network.*

PPP : *PPoint to Point Protocol.*

PPTP : *Point-to-Point Tunneling Protocol.*

R

RFC : *Request For Comments..*

RIP : *Routing Information Protocol.*

S

STP : *Spannig Tree Protocol.*

V

VLAN : *Virtual Local Area Network.*

VPN : *Virtual Private Network.*

VTP : *VLAN Trunking Protocol.*

W

WAN : *Wide Area Network.*

Introduction générale

De nos jours à l'aire du « tout disponible partout et à tout moment », les réseaux informatiques sont la base de toute entreprise aussi petite soit-elle, et leurs croissances exponentielles les rend de plus en plus ouvert sur Internet, qui est considéré comme la plus grande source d'information qui existe au monde. Cette ouverture sur Internet fait donc d'un réseau détenteur de divers informations privés, néanmoins constitue un problème majeur en termes de sécurité. En effet c'est aussi une ouverture à partir d'internet vers le réseau informatique d'un particulier ou d'une entreprise, qui constitue une brèche à partir de laquelle une cyberattaque de quelque nature qu'elle soit et pour quelconque intension.

Internet constitue donc un danger, dans la mesure où chacun a un accès au réseau où de plus en plus d'information circule via ce media menaçant l'intégrité, la confidentialité et la disponibilité de l'information.

Nous sommes face non seulement à une augmentation de la qualité des réseaux informatiques mais aussi et surtout à l'augmentation des risques sur la donnée.

Il est évident que la sécurité informatique se place actuellement au premier plan dans la mise en place et l'administration des réseaux, afin d'éviter les risques d'attaques et de garantir la sécurité du réseau de l'entreprise et de le rendre moins vulnérable sans pour autant le privé d'un accès vers internet, qui est la source primaire des attaques.

Source primaire, mais pas unique. En effet les attaques peuvent provenir de l'intérieure même de l'organisme. Il est primordial pour chaque entreprise d'instaurer une politique de sécurité adaptée.

L'évolution des réseaux a aboutit à une progression logique et virtuelle de ces derniers, palliant à certaines contraintes observées au sein du réseau de l'entreprise.

L'objectif de notre projet consiste, à améliorer les performances d'un réseau et à implémenter des mécanismes sûrs en s'aidant des liaisons virtuels (VLAN et VPN) qui permettront

par la suite une exploitation optimale des ressources du réseau et des communication sûre et confidentielles entre les utilisateurs.

Nous avons divisé notre mémoire en trois chapitres comme suit :

Le premier chapitre sera dédié aux généralités sur les réseaux informatiques en citant les différents grands piliers de ces derniers, mais aussi sur la sécurité informatique et l'importance de celle-ci.

Le deuxième chapitre portera sur les liaisons virtuelles, où nous verrons plus explicitement lesconcepts de VLAN et VPN, nous présenterons par la suite l'organisme d'accueil : Campus NTS,et l'étude effectué durant notre stage au sein de cette entreprise.

Enfin le troisième chapitre, décrira la partie pratique de notre travail, où nous présenterons l'environnement de travail puis la mise en place des liaisons virtuelles.

Nous terminerons notre travail par une conclusion générale, qui résumera les connaissances acquises durant la réalisation du projet et quelques perspectives futures.

I

Généralites sur les reseaux et la sécurite informatique

Introduction

L'apparition des réseaux informatiques a révolutionné le quotidien de l'homme, c'est devenu un outil indispensable pour lui, c'est pour ça qu'il se doit de le protéger.

Dans ce chapitre, nous allons commencer par voir des notions de base sur les réseaux, puis nous introduirons quelques concepts sur la sécurité informatique, afin de cerner au mieux le sujet.

1 Généralités sur les réseaux informatiques

1.1 Définition d'un réseau informatique

Un réseau informatique est une interconnexion de plusieurs machines entre elles dans l'intérêt d'échanger des informations [1]. Remarquons qu'on a parlé de machines et non d'ordinateurs, car en plus de ces derniers un réseau peut également connecter d'autres équipements comme des imprimantes, des tablettes, des téléphones portables et même des automates au sein d'une usine.

Figure I.1 – Représentation d'un réseau informatique [15].

1.2 Intérêt d'un réseau informatique

L'une des principales raisons d'une interconnexion de machines est le transfert de fichiers et l'accès aux fichiers distants ; c'est-à-dire que des utilisateurs d'un réseau peuvent accéder à des fichiers sur d'autres périphériques de ce réseau et ce simultanément, c'est donc un gain de temps non négligeable, mais aussi un gain d'espace de stockage, dans la mesure où un seul ordinateur peut très vite tomber à court de mémoire tandis que dans un réseau la mémoire est partagée. Toutefois pour de grandes entreprises un serveur de stockage serait plus judicieux. [1]

Autre atout qu'on peut associer à un réseau informatique est le partage des ressources, où plusieurs utilisateurs peuvent accéder à une seule et même ressource comme par exemple une imprimante, au lieu d'attribuer à chaque poste une propre à lui, c'est ici une réduction considérable en coût de matériels.

1.3 Architecture des réseaux

Il existe deux types d'architecture : [12]

1.3.1 Client/Serveur

Pour établir une communication dans un réseau, il faudra au minimum deux machines, une qui demande un service et l'autre qui en offre un, on parlera ici de clients et de serveur. On aura donc des applications de types clientes qui communiquent (Requête, Réponse) avec des applications de type serveur.

Un exemple très courant est un navigateur web (client) qui demande (requête) à un serveur web (serveur) le contenue d'une page web (réponse).

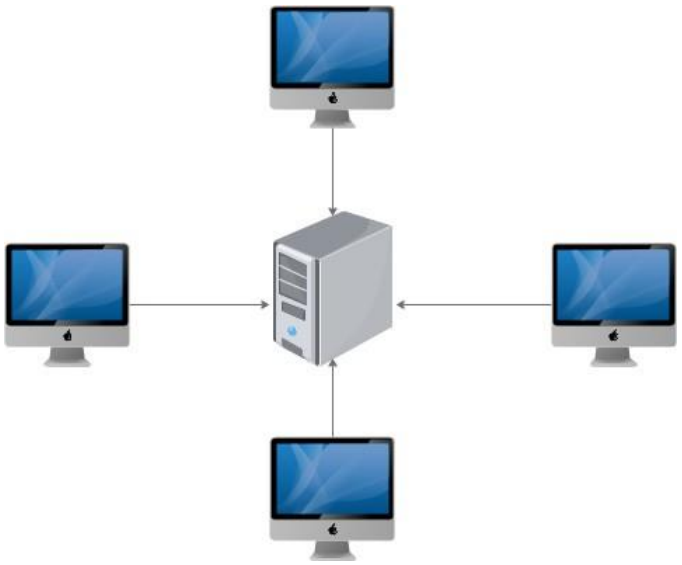

Figure I.2 – Architecture client/serveur

1.3.2 Peer-to-peer

D'un certain point de vue, toutes les applications réseau sont des applications client/serveur et ce tant qu'il y a une demande et une offre de service, dans ce genre d'architecture plusieurs clients communiquent avec un serveur centralisé.

Une architecture peer-to-peer consiste à décentraliser les demandes de services dans le sens où un poste peut à la fois être client et serveur, réduisant ainsi la charge de travail sur un seul équipement.

Nous pouvons citer comme exemple d'application peer-to-peer : BitTorrent, conçu pour le partage de fichier entre utilisateurs où il est possible de demander ou de fournir un fichier à d'autres utilisateurs.

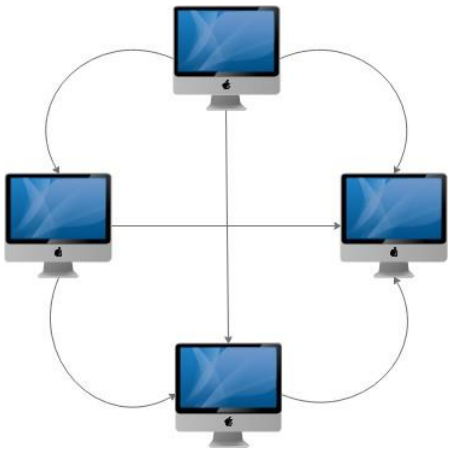

Figure I.3 – Architecture Peer to Peer

1.4 Types des réseaux

En fonction de la localisation, la distance, la taille (le nombre de machines) et le débit, les réseaux sont classés en quatre catégories. Nous pouvons faire une première classification des réseaux de données à l'aide de leur taille : [10]

Figure I.4 – Types de réseaux en fonction de l'étendu

1.4.1 PAN

Un réseau personnel désigne un réseau informatique limité en équipement, et généralement mis en œuvre dans un espace d'une dizaine de mètres, également appelé réseau domestique ou réseau individuel. Ce type de réseau est utilisé pour connecter des périphériques tels que des imprimantes, téléphones portables, appareils électroménagers, etc.

Figure I.5 – Représentation d'un PAN

1.4.2 LAN

Un réseau local est un réseau permettant d'interconnecter les ordinateurs d'une entreprise ou d'une organisation. Ces réseaux sont privés (on ne peut pas y accéder de l'extérieur), la vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet) et 1 Gbps (en FDDI ou Gigabit Ethernet), la distance sur laquelle s'étend un LAN ne dépasse généralement pas les 1000 mètres.

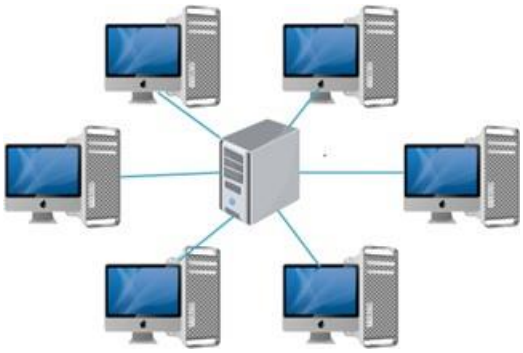

Figure I.6 – Représentation d'un LAN

1.4.3 MAN

Un Réseau métropolitain est un réseau de données haut débit connectant plusieurs réseaux locaux couvrant une zone géographiquement proche (au maximum quelques dizaines de kilomètres), telle qu'un village ou une ville. Un MAN est plus vaste qu'un LAN, permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local par le biais de commutateurs (switch) et de routeurs.

Figure I.7 – Représentation d'un MAN

1.4.4 WAN

Un réseau étendu WAN est un réseau généralement public qui interconnecte différents réseaux locaux au sein d'un même pays ou d'une vaste zone géographique dans le monde. Les WAN fonctionnent grâce à des routeurs, qui dirigent les données pour atteindre les nœuds du réseau, le support utilisé peut être terrestre ou hertzien.

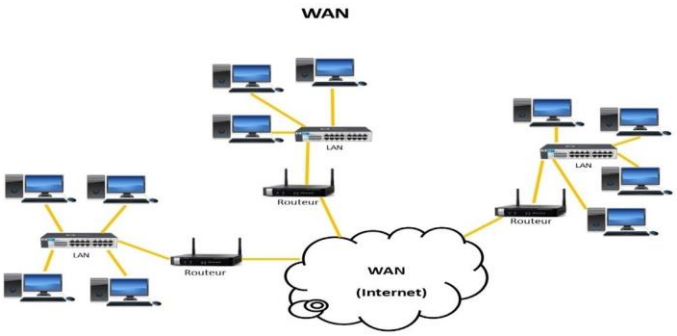

Figure I.8 – Représentation d'un WAN

1.5 Types de topologies

Nous en énumérons deux types [7] :

1.5.1 Topologie physique

La Topologie physique nous montre comment les machines sont connectées, c'est-à-dire l'emplacement physique de ces derniers ainsi que la manière dont elles sont interconnectées (câblage). A titre d'exemple nous avons : la topologie en bus, en étoile, en anneau, maillée, etc.

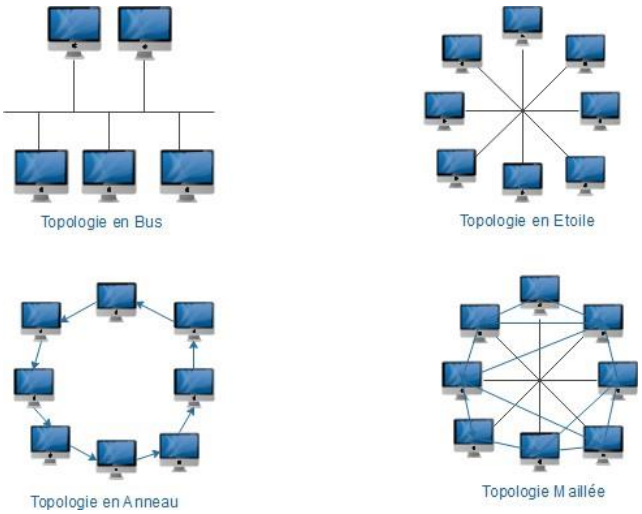

Figure I.9 – Types de topologies physiques

1.5.2 Topologie logique

Cette fois-ci la topologie logique nous montre la façon dont l'information circule et ce indépendamment du câblage. Il en existe deux modes :

1.5.2.1 Mode multipoints (broadcast)

Chaque équipement peut à tout moment envoyer un message sur le support partagé après avoir écouté au préalable si la voie est libre, et ce message est reçu par tous les autres équipements. Ce principe s'applique à la topologie en bus et en anneau.

1.5.2.2 Mode point à point (point-to-point)

Seulement deux équipements voulant communiquer sont relié par le support de transmission. Ce principe est adapté pour une topologie en étoile ou encore une topologie maillée.

1.6 Les modèles d'architecture réseau

Il existe deux types de base de modèles de réseau : le modèle de référence (OSI) et le modèle d'Application (TCP/IP) : [10]

1.6.1 Modèle OSI

Pour faciliter l'interconnexion des systèmes, un modèle appelé interconnexion des systèmes ouvert, également appelé OSI (Open System Interconnections) a été défini par l'ISO (Organisation internationale de normalisation).

Le modèle OSI est une représentation abstraite en couches utilisée comme guide pour la conception de protocoles réseau. Il divise le processus réseau en sept couches logiques, chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes. Même si le modèle OSI est très peu implémenté, il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant réseau.

Afin de connaitre les services de chaque couche nous allons les présenter ci-dessous l'une après l'autre :

1.6.1.1 Couche physique

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication sous la forme électrique, optique ou fréquences radioélectriques (suivant le type de support).

La couche physique est la première couche du modèle d'interconnexion des systèmes ouverts (modèle OSI). Elle gère les transferts au niveau du bit entre différents appareils et prend en charge les interfaces électriques ou mécaniques avec le support physique pour une communication synchrone.

1.6.1.2 Couche liaison de données

La couche liaison de donnés est la deuxième couche du modèle OSI, cette couche assure le transfert de données entre deux nœuds directement connectés, elle est devisée en deux sous-couches :

- **Contrôle de liaison logique (LLC) :** Cette sous-couche supérieure définit les processus logiciels qui fournissent des services aux protocoles de la couche réseau. Elle place des informations dans la trame indiquant le protocole de couche réseau utilisé pour la trame. Ces informations permettent à plusieurs protocoles de couche 3 (tels que IPv4 et IPv6) d'utiliser la même interface réseau et les mêmes supports.
- **Contrôle d'accès au support (MAC) :** Cette sous-couche inférieure définit le processus d'accès au support effectué par le matériel. Elle fournit l'adressage de la couche liaison de données et la délimitation des données en fonction des exigences de signalisation physique du support et du type de protocole de couche liaison de données utilisé. Les objets échangés sont souvent appelés trames.

1.6.1.3 Couche réseau

La couche réseau est la troisième couche du modèle OSI, cette couche garantit que les données sont transmises sur le réseau. C'est là qu'intervient le concept de routage, permettant l'interconnexion de différent réseau, plus du routage cette couche assure la gestion des congestions. Parmi les protocoles principaux de communication de la couche réseau on trouve : IP version 4 et IP version 6.

1.6.1.4 Couche transport

La couche de transport assure une livraison fiable des messages et fournit des mécanismes de vérification des erreurs et un contrôle du flux de données. Cette couche fournit des services de transport en mode « connexion » ou « sans connexion ». Les deux protocoles de cette couche sont les protocoles TCP et UDP. Les objets échangés sont souvent appelés segments.

1.6.1.5 Couche session

La couche session permet de gérer les connexions et déconnexions et la synchronisation entre deux processus.

1.6.1.6 Couche présentation

La couche de présentation est responsable de la traduction, du chiffrement et de la compression des données.

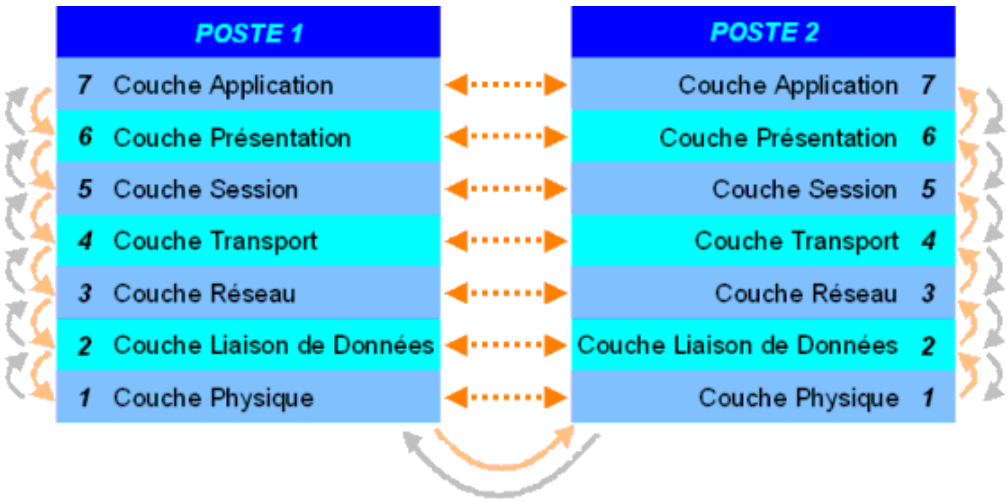

Figure I.10 – Modèle de référence OSI

1.6.1.7 Couche application

La couche 7 est la couche utilisée par les utilisateurs. C'est au niveau de cette couche que sont implémentées toutes les fonctions utilisateur : commandes permettant la gestion de la communication, terminaux virtuels, détermination des ressources disponibles, disponibilité des partenaires de communication, etc.

1.6.2 Modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP n'est pas né d'une implémentation mais il est inspiré du modèle OSI, il désigne en fait deux protocoles étroitement liés un protocole de transport TCP (Transmission contrôle protocole) et un protocole réseau IP (internet protocole), le modèle TCP/IP est en fait une architecture réseau a quatre couches :

1.6.2.1 Couche accès au réseau

Cette couche regroupe les couche physique et liaison de données du modèle OSI, elle permet à un hôte d'envoyer des paquets IP sur le réseau.

1.6.2.2 Couche internet

Le rôle de la couche Internet consiste à envoyer des paquets sources à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et

des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol).

L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

1.6.2.3 Couche transport

Chargée de fournir un moyen de communication de bout en bout entre deux programmes d'application. Agit en mode connecté TCP et en mode non connecté UDP.

1.6.2.4 Couche application

Cette couche regroupe les trois couches supérieures du modèle OSI : application, présentation et session.

1.6.3 Comparaison

La figure suivante montre la correspondance entre le modèle OSI et TCP/IP :

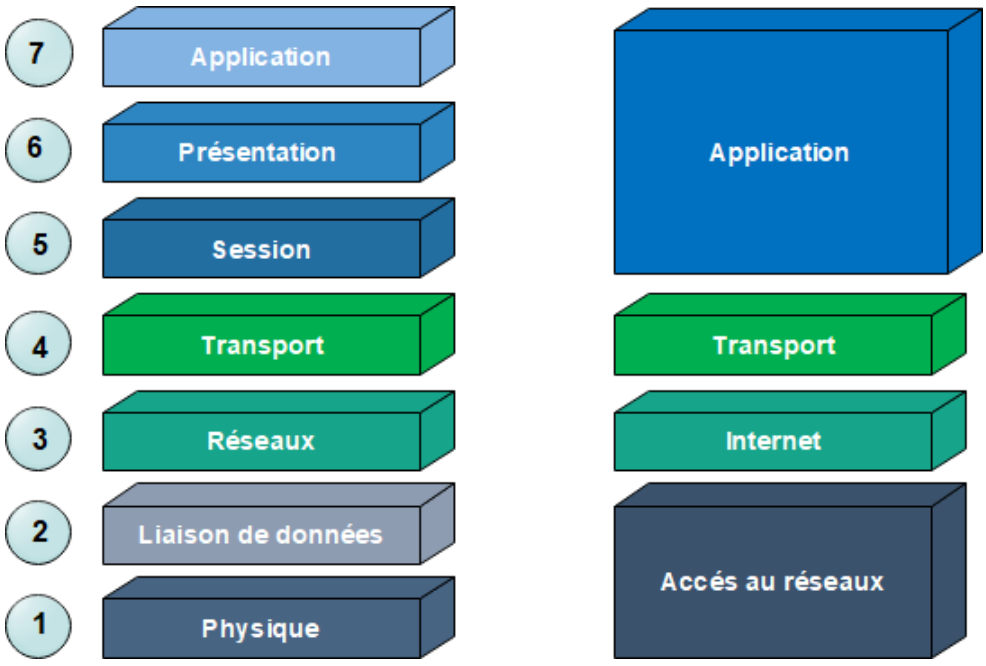

Figure I.11 – Comparaison entre les couches du modèle OSI et TCP/IP

1.6.4 Encapsulations et désencapsulations de données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information qui garantit la transmission de données est ajoutée au paquet de données, il s'agit d'un en-tête (encapsulation). Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, traité puis supprimé (désencapsulations).

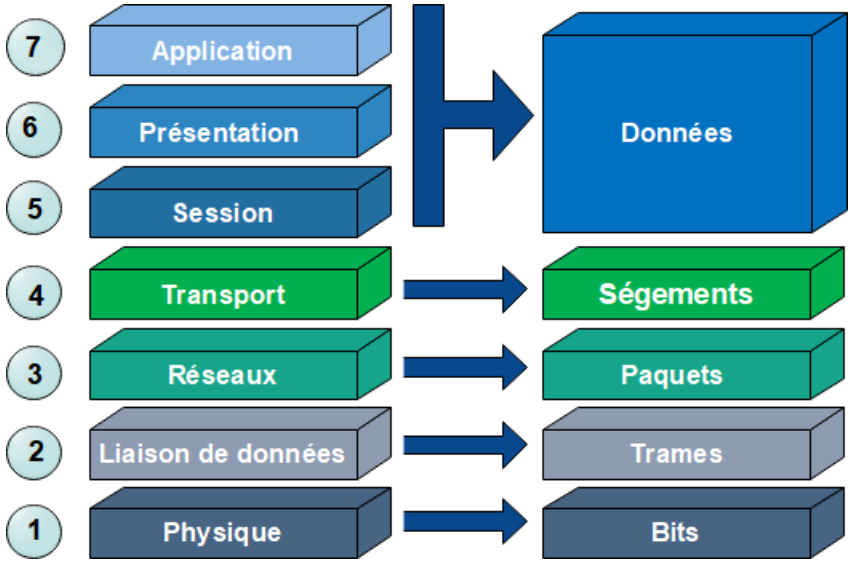

Figure I.12 – Format de l'information à travers les couches

1.7 Adressage IP

Nous savons que le but ultime d'un réseau est d'interconnecter des machines entre elles et permettre ainsi un échange d'informations entre ces dernières. Pour ce faire il faut que ces machines aient un moyen de se reconnaitre entre elles, cela se fait par le biais des adresses IP.

1.7.1 Le protocole IP

Le protocole IP (Internet Protocol) est un protocole réseau de niveau 3, qui permet à deux équipements de dialoguer et ce en émettant des paquets tout en indiquant l'adresse source et l'adresse de destination. Ce protocole est dit sans connexion, car peu fiable et ne fournit pas de garantie de livraison des paquets, ce paramètre est assuré par la couche transport.

Les adresses IP sont attribuées de deux manières différentes : soit de manière statique, c'est-à-dire que l'administrateur réseau les implémente manuellement une à une ; soit de manière dynamique où cette fois-ci un serveur DHCP qui les attribue dynamiquement aux périphériques du réseau [4].

1.7.2 Formats des adresses IP

1.7.2.1 IPv4

Une adresse IPv4 est une adresse à 32 bits (4 octets) qui se compose d'une partie réseau qui identifie le réseau auquel appartient la machine et d'une partie hôte qui identifie la machine elle-même.

- **Masque de sous-réseau :**

Afin de déterminer les deux parties composant l'adresse IPv4, un masque de sous-réseau y est adjoint. En effectuant un ET logique entre l'adresse IPv4 d'un périphérique et le masque de sous-réseau, on obtient l'adresse du réseau auquel il appartient.

- **Passerelle par défaut (Default Gateway) :**

La passerelle par défaut est une adresse nécessaire pour atteindre les réseaux distants. Elle constitue une porte de sortie du réseau local.

➢ **Types d'adresses IPv4 :**

- **Monodiffusion (Unicast) :** est une adresse qui identifie un périphérique IPv4 de manière unique.
- **Diffusion (Broadcast) :** est une adresse dont tous les bits de la partie hôte sont à 1. Un paquet IPv4 dont l'adresse destination est une adresse de diffusion indique qu'il doit être transmis à tous les périphériques du réseau local.
- **Multidiffusion (Multicast) :** est une adresse attribuée à un groupe d'hôtes, permettant ainsi de réduire le volume du trafic. IPv4 a réservé les adresses 224.0.0.0 à 239.255.255.255 comme plage de multidiffusion.

➢ **Classe d'adresse IP :**

Classe	Bits de départ	Plage d'adresses	Masque de sous-réseau
A	0	0.0.0.0 à 127.255.255.255	255.0.0.0 (/8)
B	10	128.0.0.0 à 191.255.255.255	255.255.0.0 (/16)
C	110	192.0.0.0 à 223.255.255.255	255.255.255.0 (/24)
D	1110	239.0.0.0 à 127.255.255.255	Non définie
E	11110	240.0.0.0 à 255.255.255.255	Non définie

TABLE I.1 – Classes d'adresses IP

1.7.2.2 IPv6

L'IPv4 est théoriquement limité à 4.3 milliards d'adresses et avec la croissance explosive du nombre d'utilisateurs, une pénurie d'adresses IPv4 fut rapidement atteinte, c'est pour cela qu'il est envisagé de transiter vers un autre format d'adressage qui est l'IPv6. Une adresse IPv6 possède un espace d'adressage de 128 bits, or 16 octets pour un total de 340 unidécillions ($340x10^{36}$) adresses disponibles. Elle se présente sous forme de chaine de valeurs hexadécimales, chaque groupe de 4 bits est représenté par un caractère hexadécimal pour un total de 32 caractères séparés par deux points (:) comme le montre la figure suivante :

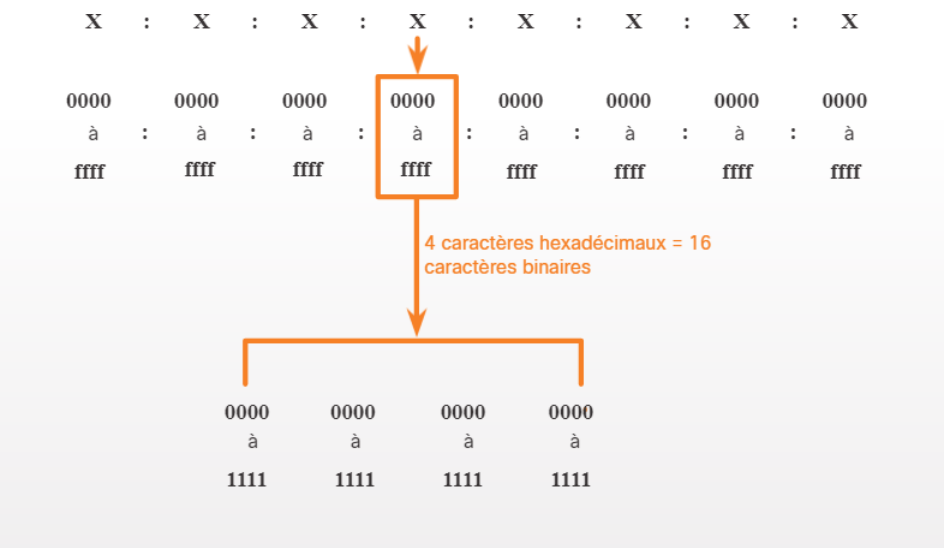

Figure I.13 – Structure d'une adresse IPv6

Il est possible de réduire la taille de l'adresse IPv6 en s'aidant de deux règles qui sont les suivantes :

- **Règle 1 :** omettre les zéros en début et uniquement en début de chaque segment.
- **Règle 2 :** remplacer une seule suite de zéros sur un ou plusieurs segments successifs par deux points (:).

Exemple 1.1

Adresse complète : *2001 :0db8 :0000 :1111 :0000 :0000 :0000 :0200.*

Etape 1 : *2001 :db8 :0 :1111 :0 :0 :0 :200*

Etape 2 : *2001 :db8 :0 : 1111 : : 200*

➢ **Types d'adresses IPv6 :**

- **Monodiffusion :** est une adresse de monodiffusion qui identifie une interface sur un périphérique IPv6 de façon unique.
  Contrairement à un périphérique IPv4 qui a une seule adresse, les périphériques IPv6 ont généralement deux adresses de monodiffusion :
  - ✓ **Adresse de monodiffusion globale (GUA) :** Similaire à une adresse IPv4 publique, ces adresses sont uniques au monde et routable sur internet.
  - ✓ **Adresse Link-Local (LLA) :** Utilisé pour communiquer avec d'autres équipements sur le même réseau local.
- **Multidiffusion (Multicast) :** Utilisée pour l'envoi d'un seul paquet IPv6 vers plusieurs destinataires.
- **Anycast :** est une adresse IPv6 de monodiffusion pouvant être attribuée à plusieurs périphériques. Un paquet IPv6 ayant comme adresse de destination une adresse anycast, sera acheminé vers la machine la plus proche possédant cette adresse.

1.8 Les différents dispositifs de la connectivité

Les équipements réseau sont des périphériques physiques nécessaires à la communication et l'interconnexion entre les appareils d'un réseau, nous en distinguons :

1.8.1 Le Répéteur

Un répéteur est un équipement qui intervient au niveau 1 du modèle OSI. Il sert à prolonger la longueur des supports de transmission qui relient tous les périphériques du réseau, un répéteur a deux rôles importants : le filtrage des distorsions et des parasites afin d'éviter les interférences et l'amplification du signal reçu.

1.8.2 Le concentrateur

Est un équipement qui survient au niveau de la couche 1 du modèle OSI, permet la connexion de plusieurs machines disposées en étoile, on distingue 2 types :

- ➢ Les concentrateurs dits « actifs » : ils sont alimentés électriquement et permettant de régénérer le signal sur les différents port.
- ➢ Les concentrateurs dits « passifs » : ils ne permettent que de diffuser les hôtes connectés.

1.8.3 Le commutateur

Est un équipement du niveau 2 qui relie plusieurs segments dans un réseau, il permet de créer des circuits virtuels et de diriger les informations vers une destination précise sur le réseau, il existe cependant des switches de niveau 3 appelées switches multicouches.

1.8.4 Le Routeur

Un routeur est un dispositif d'interconnexion de réseaux informatiques qui intervient au niveau de la couche 3, utilisé pour assurer le routage des paquets de données entre deux ou plusieurs réseaux afin de déterminer le chemin que les paquets de données emprunteront.

1.8.5 Le Pont

C'est un équipement qui opère au niveau 2 de la couche OSI, qui assure l'interconnexion avec d'autres réseaux en utilisant des protocoles identiques.

1.8.6 La passerelle

Une passerelle est un équipement recouvrant les 7 couches du modèle OSI, qui permet de relier des réseaux de types différents n'utilisant pas les mêmes protocoles.

2 La sécurité dans les réseaux

2.1 Définition

Un système information est une entité qui définit l'intégralité des ressources matérielles et logicielles d'une entreprise, il constitue donc la valeur et le cœur de celle-ci. Il est donc plus que nécessaire de le protéger de toutes menaces de quelque nature qu'elle soit [5].

2.2 Enjeux de la sécurité informatique

Un système d'information est constamment exposé aux menaces, c'est-à-dire à toutes les actions susceptibles de nuire à ce dernier, le rendant vulnérable et exploitable par de tierces personnes ou organisations malveillantes à des fins non connues. Il est indispensable d'identifier les menaces et les risques potentiels, de connaitre son ennemi et ses motivations, afin de mettre en place une politique de sécurité.

La sécurité d'un système d'information est fondée sur cinq principes majeurs :

2.2.1 La confidentialité

Seules les personnes adhérentes et agréées ont le droit d'accès aux données.

2.2.2 L'intégrité

Est le fait de garantir que les données qui affluent sont bien celles supposées, qu'il n'y a pas eu altération volontaire ou pas lors de la communication.

2.2.3 L'authentification

Procédé permettant de restreindre l'accès aux ressources, où seules les personnes autorisées y ont le droit.

2.2.4 La disponibilité

Assure le bon fonctionnement des ressources et ce à tout moment.

2.2.5 La non répudiation

Les données transitant de bout en bout de la communication ne peuvent pas être reniées par les deux correspondants.

2.3 Estimation des risques

Afin d'adopter la meilleure stratégie de sécurité pour son entreprise, il en convient de connaitre les menaces qui peuvent nuire au bon fonctionnement du système d'information. [9]

Parmi les menaces les plus communes, nous pouvons en citer les suivantes :

2.3.1 Erreurs et omissions

Souvent d'origine humaine, elle représente une menace pour l'intégrité du système, elles peuvent être dues à des erreurs de manipulation de données ou de programmation.

2.3.2 Fraude et vol

Pouvant être interne ou externe à l'entreprise, c'est-à-dire commis par des personnes possédant des accès privilégiés aux ressources, ou pas. Un employé de l'entreprise a une meilleure position qu'une personne externe pour un éventuel sabotage.

2.3.3 Les hackers

Terme définissant tout individu non autorisé s'introduisant dans le système d'information, et ce pour des raisons diverses comme le vol de données ou encore leurs destructions.

2.3.4 Espionnage commercial ou industriel

Consiste en la récupération illégale de données confidentielles (Données clients, brevets industriels, etc.) d'une entreprise, dans le cadre d'une concurrence économique ou industrielle.

2.3.5 Programmes malveillants

Un logiciel malveillant est un type de programme conçu pour endommager ou exploiter des équipements, des réseaux programmables, ainsi des services. Parmi les types de logiciels malveillants on trouve :

2.3.5.1 Virus

Un virus est un programme logiciel malveillant qui se propage d'un ordinateur à un autre, lorsque des fichiers infectés sont envoyés, il se réplique en ajoutant son code à un autre programme, le but d'un virus est d'endommager les systèmes sur lesquels il réside.

2.3.5.2 Ver

Un ver est un type de logiciel malveillant qui se réplique sur plusieurs ordinateurs à l'aide d'un réseau informatique tel qu'internet, contrairement au virus les vers informatiques peuvent se propager sans être attachés à un hôte.

2.3.5.3 Cheval de trois (Trojans)

Un cheval de trois est un logiciel légitime, qui semble utile mais une fois téléchargé et installé, il modifie l'ordinateur et il affecte des activités malveillantes.

2.3.5.4 Spyware

Est un logiciel espion qui s'installe sur un ordinateur avec ou sans permission dans le but de rassembler des informations sur l'utilisateur et de les envoyer à un autre utilisateur distant.

2.3.5.5 Rootkit

Est un logiciel malveillant qui permet aux attaquants d'installer une série d'outils afin d'accéder à distance a l'ordinateur et de le contrôler.

2.3.5.6 Ransomwares (Rançongiciel)

Un rançongiciel est un logiciel malveillant qui bloque l'accès à un ordinateur ou à des fichiers en les cryptant et qui exige le paiement d'une rançon de la part de la victime pour y accéder à nouveau. Les machines peuvent être infectées en ouvrant des pièces jointes ou en cliquant sur des liens malveillants reçus dans des e-mails.

2.4 Techniques d'attaques [5]

2.4.1 Attaque par déni de service (DOS)

Est une attaque informatique qui vise à perturber et détruire le fonctionnement d'un service en empêchant ses utilisateurs de l'utiliser durant une certaine période.

2.4.2 Attaque par l'homme du milieu (man in the middle)

Une attaque par l'homme du milieu est une attaque conçue pour intercepter les communications TCP entre deux machines, aucune des machines ne peut soupçonner que le canal de communication entre elles a été compromis.

2.4.3 Attaque par force brute (craquage de mot de passe)

Une attaque par force brute est une méthode qui consiste à trouver le mot de passe ou la clé de chiffrement d'une personne en testant successivement toutes les combinaisons possibles afin de pouvoir accéder à un service en ligne, à des données personnelles ou à un ordinateur.

2.4.4 Attaque par débordement de tampon (buffer overflow)

La mémoire tampon est utilisée pour stocker temporairement des données dans la mémoire vive ou sur le disque dur de l'ordinateur, un débordement de mémoire tampon se produit l'lorsque un programme tente de stocker dans la mémoire tampon plus de données que ce qu'elle a été conçue pour contenir, cela provoque un débordement d'informations supplémentaires dans la mémoire tampon adjacente, ce qui peut corrompre ou écraser les données valides.

2.4.5 Attaque spoofing (l'usurpation d'identité)

L'usurpation d'identité est le déguisement d'une communication ou d'une identité afin qu'elle semble être associé à une source fiable et autorisée, l'usurpation d'identité peut s'appliquer aux emails, aux appels téléphoniques aux sites web, elle peut aussi être plus technique, comme des ordinateurs usurpant des adresses IP.

2.4.6 Attaque sniffing (reniflement de paquet)

Le reniflage est une technique de surveillance et de capture de tous les paquets d'un réseau a laide d'outil logiciels ou matériels, il permet également aux attaquants d'observer et d'accéder à tout le trafic réseau ciblé, et de collecter des informations sur le trafic route messagerie, la configuration des routeurs, le trafic DNS et les sessions de chats.

2.4.7 Attaque phishing (hameçonnage)

Est une technique utilisée par un attaquant pour récupérer des informations, l'hameçonnage consiste à envoyer des emails ou d'autres communications conçues pour tromper les victimes, le message semble provenir d'une personne de confiance, mais cache toutefois une ruse, où il sera demandé à la victime de fournir des informations personnelles, souvent confidentielles (coordonnées bancaires), généralement sur un site web frauduleux.

2.5 Motivation des attaques [6]

- Intrusion dans le système.
- Vol d'informations industrielles telles que les brevets, personnelles telles que les codes bancaires, commerciales ou encore organisationnels.
- Trouble le bon fonctionnement d'un service, le rendant inexploitable par les utilisateurs (attaque DOS).
- Utiliser les ressources d'un système comme une bonne bande passante et ce sans y être autorisé.
- Atteinte à la vie privée.
- Usurpation d'identité.

2.6 Outils de sécurité

2.6.1 Proxy

Un proxy est un serveur intermédiaire entre un client et un serveur web, permet de protéger et d'améliorer l'accès à certaines pages web en stockant des copies (ou en les mettant en cache), et en filtrant certains contenus web et logiciels malveillants.

2.6.2 Pare-feu

Un pare-feu est un outil ou un logiciel qui fait l'intermédiaire entre le réseau local (privé) et le réseau externe, conçue pour protéger un réseau local des intrusions extérieures, il permet de sécuriser les informations du réseau en filtrant les entrées et en contrôlant les sorties selon des règles définis par l'administrateur.

2.6.3 DMZ (Demilitarized zone)

La DMZ est un sous réseau isolé à la fois du réseau local et d'internet, sert à protéger le réseau local tout en permettant la communication entre les deux zones de façon sécurisée grâce à des règles de filtrage, DMZ sert généralement des services accessibles aux utilisateurs depuis un réseau externe tel que : les serveurs web, les serveurs de messagerie. [13]

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Traffic du réseau externe vers la DMZ autorisé.
- Traffic du réseau externe vers le réseau interne interdit.
- Traffic du réseau interne vers la DMZ autorisé.
- Traffic du réseau interne vers le réseau externe autorisé.
- Traffic de la DMZ vers le réseau interne interdit.
- Traffic de la DMZ vers le réseau externe refusé.

Il existe de multiples façons de concevoir un réseau intégrant une zone démilitarisée. Deux méthodes sont fréquemment employées : l'utilisation d'un pare-feu unique (appelé pare-feu à trois interfaces) et l'utilisation de deux pare-feux.

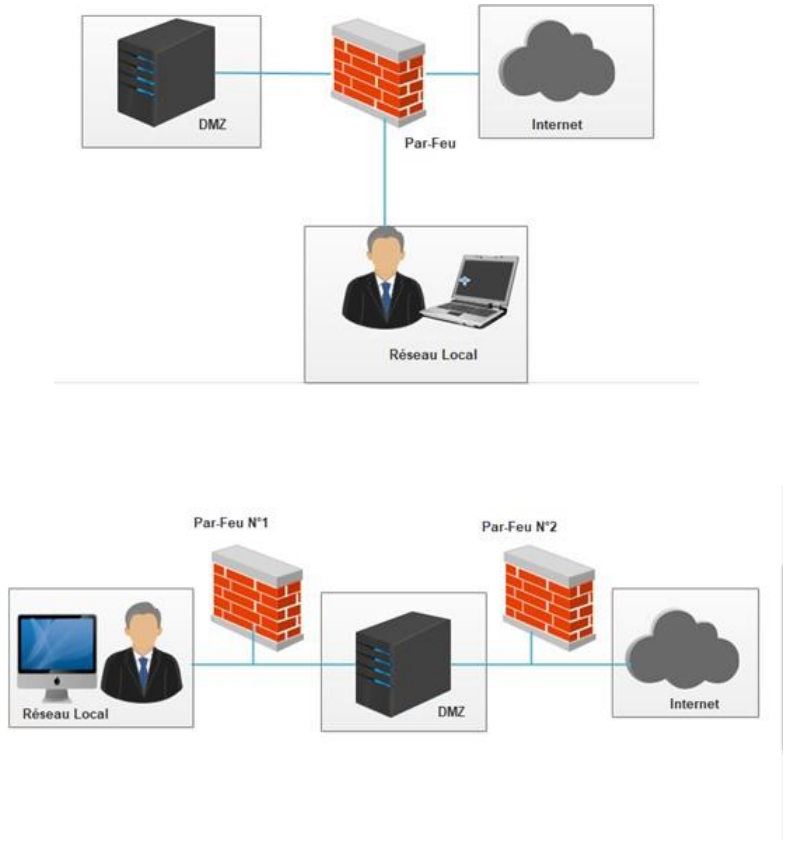

Figure I.14 – Architecture avec un seul et avec deux pare-feux

2.6.4 Antivirus

C'est un logiciel qui peut s'installer soit à l'entrée d'un réseau local, là où arrivent les flux en provenance d'internet, soit sur le poste de travail de l'utilisateur. Il peut être utilisé en mode statique, c'est-à-dire que le logiciel est activé uniquement sur ordre de l'utilisateur, ou alors en mode dynamique, où le logiciel est actif de façon permanente, ce mode offre une meilleure détection, bien qu'il consomme plus de ressources. L'antivirus repose sur deux méthodes de fonctionnement, qui sont respectivement : la recherche de signature et l'analyse comportementale.

La première consiste à répertorier tous les codes malveillants ainsi que leurs signatures (suite de bits caractéristiques) et de rechercher cette dernière dans les flux de données reçues. Quant à la seconde méthode, elle consiste à étudier le comportement d'un logiciel et de déceler de potentielles actions malveillantes. [13]

2.6.5 ACL (Access Control List)

Les listes de contrôles d'accès sont des moyens employés dans un réseau informatique pour superviser les accès des utilisateurs à certaines ressources, en autorisant ou interdisant les paquets sortants ou entrants. L'avantage principal des ACLs et qu'elles fournissent une sécurité au réseau en filtrant le trafic, néanmoins c'est un traitement supplémentaire à effectuer pour chaque paquet entrant et sortant du routeur. [14]

2.6.6 IDS (Intrusion Detection System)

Le système de détection d'intrusion, et un mécanisme pouvant repérer tout type de trafic et activité s'éloignant de la norme et pouvant être malveillants, en surveillant une cible qui peut être un réseau ou un hôte, et ce en analysant une copie du trafic, nous pouvons trouver deux sortes des IDS en fonction de cette cible :

Le NIDS (Network IDS) ou IDS Réseau, se situe sur un réseau isolé et ne dialogue pas avec le réseau à surveiller, il est donc passif et se contente uniquement de superviser le trafic et lancer une alerte en cas de détection de malveillances afin d'agir en conséquence.

Le HIDS (Host IDS), autrement appelé IDS système, se charge de la surveillance d'un hôte, et ce en analysant les activités de la machine (nombre d'utilisateurs, ressources consommées…) Ou en analysant les activités de l'utilisateur (horaires et durée de connexion, programmes activés…). [14]

2.6.7 IPS (Intrusion Prevention System)

Le système de prévention d'intrusion, analyse la donnée elle-même, contrairement à l'IDS qui lui analyse une copie de celle-ci. L'IPS réagit donc en temps réel en bloquant les ports de provenance du trafic suspect. Tout comme IDS, nous distinguons deux types d'IPS selon la cible à surveiller (réseaux ou hôte).

NIPS (Network IPS), analyse le trafic réseau en s'appuyant sur une base de données de signatures d'attaques, et bloque les flux malveillants en cas de leurs détections.

HIPS (Host IPS), qui analyse les machines hôtes, en surveillant différents éléments de la machine et en bloquant les activités suspectes. [14]

Conclusion

Au terme de ce chapitre, nous avons pu sillonner l'environnement des réseaux informatiques, en définissant dans les grandes lignes les principaux axes de ces derniers et en soulignant leurs valeurs, les risques auxquels ils peuvent faire face ainsi que la nécessité de les préserver de tout crime allant à l'encontre de leurs principes et pratiques.

II

Introductions aux liaisons virtuelles et etude de l'existant

Introduction

Le plus souvent des cas lorsque nous abordons la sécurité informatique, il nous vient à l'esprit la prévention des attaques en provenance de l'extérieur, or négliger la provenance de l'intérieur par le réseau local, serait un danger pour l'intégrité de l'entreprise, de sorte qu'un utilisateur mal intentionné de ce réseau dispose d'un moyen d'accéder à des ressources qui ne lui sont pas destinées.

Ou dans le cas d'utilisateurs distants du réseau local de son entreprise, souhaitant accéder à distance aux ressources de celles-ci, et le faire via internet est totalement possible, mais rend la communication vulnérable vis-à-vis des attaques. Dans ces deux cas, deux solutions nous est proposées : les VLANs (Virtual local Area network) et les VPNs (Virtual private network), que nous allons voir plus explicitement au cours de ce chapitre.

1 Introduction aux liaisons virtuelles (VLAN/VPN)

1.1 VLAN

Apparu en 1995, un VLAN pour réseau local virtuel en français, est un réseau local regroupant un ensemble de machines de façon logique et non physique, c'est-à-dire indépendamment du système de câblage. Il est réalisé en intervenant par voie logiciel sur le commutateur.

Ce n'est qu'en 1998 que les VLANs sont normalisés par la norme 802.1q, qui a impliqué la modification du format de la trame, et ce en ajoutant une étiquette (tag), destinée à identifier le VLAN auquel appartient la trame. [13]

1.1.1 Avantages

Les VLANs offrent plusieurs avantages parmi lesquels nous pouvant citer :

- ➢ Suppression de la contrainte physique, où l'appartenance à un VLAN est indépendante de la position géographique de la machine.
- ➢ Amoindrissement du trafic en segmentant les domaines de diffusion, augmentant de ce fait la bande passante.
- ➢ Centralisation et simplification d'administration.
- ➢ Gain en sécurité, car les informations sont encapsulées dans un niveau supplémentaire.

1.1.2 Types de VLAN

Différents types de VLAN sont utilisés dans les réseaux modernes. Certains types de VLAN sont définis par des classes de trafic. D'autres types de VLAN sont définis par leurs capacités spécifiques, qui sont les suivants : [15]

1.1.2.1 VLAN par défaut

Le VLAN par défaut est le VLAN auquel les trames et les ports sont associés par défaut sans configuration sur le matériel, lorsque l'implémentation du VLAN est menée à bien. Lors de la mise en œuvre du VLAN au moins un VLAN doit être d définis sur le matériel. Globalement sur le commutateur Cisco, le VLAN par défaut est le VLAN 1.

1.1.2.2 VLAN natif

Le VLAN natif est le VLAN qui transmet les trames non étiquetées 802.1q, si le switch reçoit une trame Ethernet standard sur l'interface trunk, il la mettra dans ce VLAN natif. Le concept de VLAN natif n'entre en jeu que lors de la configuration des ports en mode trunk, ce type de VLAN existe pour assurer une inter¬opérabilité avec le trafic qui ne prend pas en charge l'étiquetage.

1.1.2.3 VLAN de données

Un VLAN de données (appelé utilisateur de VLAN) est un réseau local virtuel configuré pour acheminer le trafic généré par l'utilisateur. L'importance de séparer les données utilisateurs de tout autre type de communication réside dans la gestion et le contrôle approprié.

1.1.2.4 VLAN de la voix

Un VLAN voix est un VLAN qui est exclusivement affecté au trafic voix des utilisateurs. Il assure la qualité du trafic vocal en priorisant sa transmission lorsqu'il est transmis avec d'autres trafics. C'est-à-dire que lorsque d'autres services (données, vidéo, etc.) sont transmis simultanément, le service vocal sera prioritaire et sera transmis avec la priorité de routage la plus élevée.

1.1.2.5 VLAN de gestion

Un VLAN de gestion est utilisé pour accéder à l'interface utilisateur de gestion des commutateurs, la configuration de la gestion du VLAN se fait en lui attribuant une adresse IP est un masque sous réseau, généralement le VLAN de gestion par défaut est le VLAN 1.

1.1.2.6 VLAN privé

Un VLAN privé est également appelé port isolé ou port d'accès, devise un domaine vlan standard en deux ou plusieurs sous-domaines, chaque sous domaine est représenté par les vlan primaire et secondaire, un VLAN privé est identifié par son id vlan principal, ce dernier est le même pour tous les sous-domaine appartenant au VLAN privé , les ID de VLAN secondaire distinguent les sous-domaines les uns des autres et fournissent une isolation de couche 2 entre les ports sur le même VLAN Il existe trois types de vlan pour construire une infrastructure de vlan privé [17] :

- **VLAN principal :** Est définit à l'aide d'une balise 802.1Q (ID VLAN), il transfert le trafic des ports promiscuous en aval vers des port isolés, des ports de communauté et d'autre port promiscuous dans le même VLAN privé. Un VLAN principal peut contenir plusieurs VLAN secondaire (isolée et communautaire). Un seul VLAN principal peut être configuré par VLAN privé.
- **VLAN communautaire :** Est un VLAN secondaire qui dirige le trafic entre les ports appartenant à la même communauté et les ports promiscuité, Il peut y avoir plusieurs VLAN communautaires par VLAN privé. Une interface au sein d'un VLAN de communauté spécifique peut établir une communication de couche 2 avec n'importe quelle autre interface au sein du même VLAN de communauté. Une interface au sein du VLAN communautaire peut également communiquer avec un port proche ou un port ISL.

- **VLAN isolé :** Est un VLAN secondaire. Il transfère le trafic de ports isolés vers des ports promiscuité ou des ports ISL, une interface isolée ne peut ni émettre ni recevoir de paquets d'une autre interface isolée. Un seul VLAN isolé peut être configuré par un VLAN privé.

Il existe trois types d'attributions de ports dans les VLAN privés :

- **Port promiscue :** appartient à un VLAN principal et peut communiquer avec toutes les interfaces du VLAN privé, y compris les autres ports promiscuité, les ports communautaires et les ports isolés.
- **Ports de communauté :** Ces ports peuvent communiquer avec d'autres ports de communauté et des ports de promiscuité.
- **Ports isolés :** peuvent uniquement communiquer avec des ports promiscuité.
- **Port ISL :** Est un port d'agrégation qui connecte plusieurs commutateurs dans un VLAN privé.

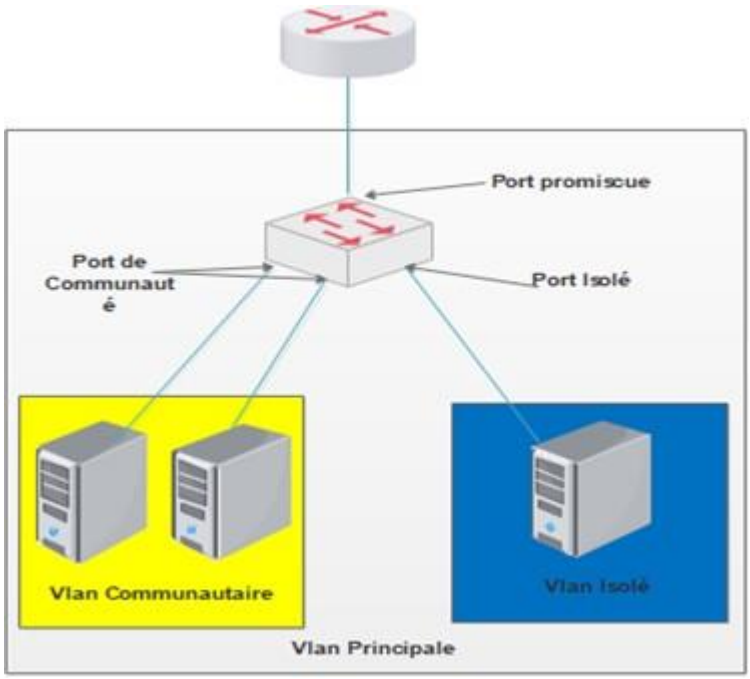

Figure II.1 – Représentation VLAN Privé

❖ **Plages d'ID de VLAN**

Les réseaux locaux virtuels d'accès sont divisés selon une plage normale ou une plage étendue.

✓ **Réseaux locaux virtuels à plage normale :**

Utilisés dans les réseaux de petites, moyennes et grandes entreprises.

Identifiés par un ID de VLAN compris entre 1 et 1005.

Les ID de 1002 à 1005 sont réservés aux VLAN Token Ring et aux VLAN à interface de données distribuées sur fibre (FDDI).

Les ID 1 et 1002 à 1005 sont automatiquement créés et ne peuvent pas être supprimés.

✓ **Réseaux locaux virtuels à plage étendue :**

Permettent aux fournisseurs de services d'étendre leur infrastructure à un plus grand nombre de clients. Certaines multinationales peuvent être suffisamment grandes pour avoir besoin d'une plage étendue d'ID de VLAN.

Sont identifiés par un ID de VLAN compris entre 1006 et 4094.

Prennent en charge moins de fonctionnalités VLAN que les VLAN à plage normale.

1.1.3 Classification de VLAN

Nous pouvons classer les VLANs selon le regroupement effectué et ce comme suit :

1.1.3.1 VLAN de niveau 1 (Port based VLAN)

Le VLAN par port est un type de VLAN associé à la couche physique, car il s'agit d'affecter chaque port d'un switch à un VLAN et la machine raccordée à ce port est automatiquement associé au VLAN du port. Dans le cas où un hub est raccordé à ce port, toutes les machine relier à ce hub appartiennent à ce même VLAN. Toutefois il ne permet pas de traiter les commutateurs en cascade.

La configuration est statique, ce qui implique qu'un périphérique qui change de port changera automatiquement de VLAN, ce qui rend l'administration de ce VLAN fastidieuse car en cas de déménagement de stations une reconfiguration ou un brassage est nécessaire. C'est pourquoi il est rarement utilisé.[9]

Ci-dessous un exemple de table de commutation pour un VLAN de niveau 1 :

PORT	VLAN
Fa0/1	10
Fa0/2	10
Fa0/10	20
Fa0/11	20
Fa0/12	20
Fa0/15	30

TABLe II.1 – Classification des VLAN par port

❖ **Mode de fonctionnement des ports d'un commutateur :** [16]

Sur les ports d'un switch Cisco, on distingue plusieurs modes de fonctionnements qui sont les suivants : le mode Access et le mode Trunk, qui détermine si le port peut faire transiter un seul ou plusieurs VLANs sur le lien et les modes Dynamic Auto et Dynamic Desirable, qui eux ont pour but de négocier un trunk à l'aide du protocole DTP.

✓ **Mode Access :**

Par défaut un port de commutateur est en mode access et est attribué au VLAN 1. Un port en mode access est un port qui fait transiter les trames d'un seul et unique VLAN et ces trames ne portent aucune étiquette, ce type servira à connecter un switch à des périphériques finaux tels que des ordinateurs, serveurs, imprimantes, etc.

✓ **Mode trunk :**

Contrairement à un port en mode access, le mode trunk li a la possibilité de faire transiter les trames de plusieurs VLAN, sachant que des étiquettes sont ajoutées aux trames permettant de distinguer le VLAN d'appartenance. Seul le VLAN Natif ne comporte pas d'étiquette ajoutée sur le port du trunk. Le port trunk connecte un commutateur à un router ou à un autre commutateur.

✓ **Mode Dynamic Auto (DA) :**

Un port d'un switch est par défaut en mode DA, ce port pourra être convertis en mode trunk si l'interface voisine est définie sur le mode trunk ou DD. En mode DD, le switch ne génèrera pas de messages DTP, mais ne fera qu'écouter ceux des interfaces voisines pour se mettre ou pas en mode trunk.

✓ **Mode Dynamic Desirable :**

Quand le port d'un switch est configuré en mode DD, il tendra inlassablement à passer en mode trunk, si ces interfaces voisines sont en mode DA, trunk ou DD et l'interface générera également des messages DTP pour informer les autres interfaces.

Afin de mieux visualiser le procédé des négociations voici un tableau qui résume cela :

	DA	**DD**	**Trunk**	**Access**
DA	Access	Trunk	Trunk	Access
DD	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	✗
Access	Access	Trunk	✗	Access

TABLe II.2 – Mode de fonctionnement des ports

1.1.3.2 VLAN de niveau 2 (Mac Address based VLAN)

Ce type de VLAN, où c'est l'adresse Mac du périphérique qui détermine le VLAN auquel il appartient, est associé à la couche 2 du modèle de référence OSI. Dans ce cas de figure, même si deux différentes stations sont raccordées à un même port du switch, elles peuvent appartenir à des VLAN différents, permettant de traiter des switchs en cascade. Il offre donc plus de souplesse que le VLAN de niveau 1 car dynamique, ici c'est le port qui détermine le VLAN d'appartenance en fonction de l'adresse Mac de la station. En cas de déménagement de stations, toute reconfiguration est inutile.

Sachant qu'une station peut appartenir à plusieurs VLAN, il est donc nécessaire de maintenir un fichier de correspondance entre adresses Mac et VLAN à jour et éventuellement en cas de changement de carte réseau sur les stations. [9]

Le tableau suivant montre un exemple de table de commutation qui associe des adresses Mac à des VLAN :

Adresse Mac	VLAN
0000.5E00.0101	10
0000.4B01.1000	10
AAE0.FBA0.0365	20
BAD0.0404.1999	20
CD00.1997.1309	20
ABB0.CE01.0258	30

TABLE II.3 – Classification des VLAN par port

1.1.3.3 VLAN de niveau 3

Associé à la couche Réseau, les VLANs de niveau 3 sont réalisables de la manière suivante :[9]

✓ **Par protocole :** (Protocole based VLAN)

Permet de regrouper les machines dynamiquement par type de protocoles en un réseau virtuel, ce qui implique que la communication peut s'établir uniquement entre les périphériques utilisant les mêmes protocoles. Comme suit :

Protocole	VLAN
TCP/IP	10
IPX	20
AppleTalk	30

TABLE II.4 – Classification des VLAN par protocole

✓ **Par application :** (numéro de port TCP)

L'appartenance dans ce cas de figure à un VLAN est déterminée selon l'application que la station utilise, la constitution des VLAN est alors dynamique.

N° de port TCP	Application	VLAN
53	DNS	10
80	HTTP	10
110	POP 3	20
161	SNMP	30

TABLE II.5 – Classification des VLAN par application

✓ **Par sous-réseau :** (Network address based VLAN)

Le regroupement se fait en fonction des adresses réseaux des périphériques. On associera un VLAN à une plage d'adresses, il est donc dynamique. Cependant un périphérique peut appartenir à plusieurs VLAN par affectation statique.

Sous-réseau	VLAN
192.168.1.32 /27	10
192.168.1.96 /27	20
192.168.1.128 /28	30
192.168.1.144 /28	40

TABLE II.6 – Classification des VLAN par sous-réseau

1.1.4 Routage inter-VLANs

Bien que les VLANs proposent divers avantages de sorte qu'ils réduisent le domaine de diffusion et définissent des sous réseaux logiques en dessus d'une topologie connue isolant le trafic, ils présentent un léger souci, tel que des machines n'appartenant pas à un même VLAN ne peuvent pas communiquer entre elles, à moins qu'un routage soit effectué soit par un routeur soit par un switch de niveau 3 et ce de deux manières différentes :

✓ **Une liaison physique :** c'est-à-dire une interface physique distincte par VLAN, sauf que cela revient à gaspiller des interfaces en particulier si le réseau possède un grand nombre de VLAN, ce serait un coût en plus.

✓ **Une liaison logique :** le principe est le même que le précèdent, hormis qu'il existe un seul lien physique regroupant de façon logique plusieurs VLAN, ce principe d'agrégation de VLAN sur une seule interface physique s'appelle « Router-On-a-Stick ».

Une communication inter-VLAN, passe donc par ce lien multi-VLAN, en traversant d'abord par le backbone de couche 2 ; le router remplit sa fonction de routage en renvoyant par ce même lien le trafic vers le VLAN de destination. Ce flux se nomme « out to the router and back ».

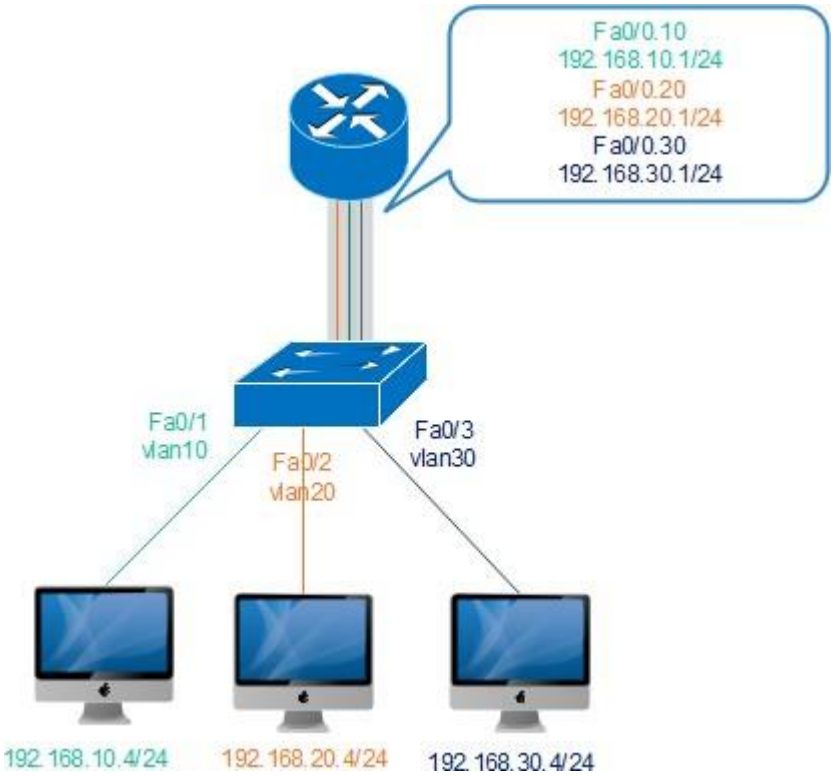

Figure II.2 – Représentation du principe du Router-On-Stick

1.1.5 Protocoles utilisés

1.1.5.1 Protocoles de transport

1.1.5.1.1 Protocole ISL

Protocole ISL est la méthode d'identification VLAN ou les informations VLAN sont explicitement marqué sur la trame Ethernet, ISL est le Protocol propriétaire Cisco est pris en charge uniquement sur les commutateurs de la gamme Cisco 1900, il fonctionne au niveau de la couche 2 en encapsulant la trame de donnée avec un en-tête de 26 octets et effectuant une nouvelle redondance cyclique (CRC) de 4 octets d'où un total de 30 octets de surcharge, ISL prend en charge jusqu'à 1000 VLAN. Le concept de VLAN natif n'est pas important pour ISL car toutes les trames, y compris celles du VLAN natif, sont étiquetées.

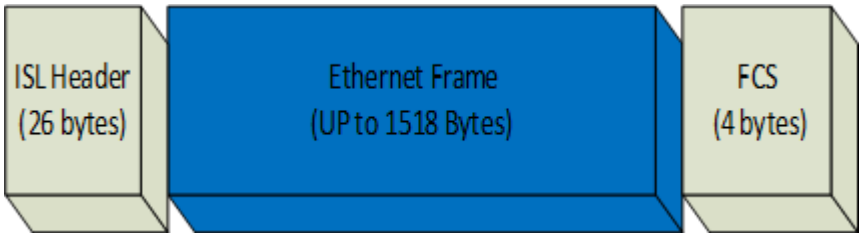

Figure II.3 – Trame Ethernet ISL

1.1.5.1.2 Norme 802.1q

Pour répondre à des besoins d'interopérabilité entre les constructeurs que le protocole ISL ne fournissait pas, une autre méthode de marquage de trame standardisée est apparue et qui est la 802.1Q, il s'agit d'ajouter à la trame qui initialement atteignait une taille de 1518 octets, un champ de 4 octets passant ainsi à un maximum de 1522 octets, un recalcule de la séquence de contrôle de trame (FCS) est nécessaire avant que le périphérique envoie la trame sur le lien trunk, car le marquage n'est pas effectué sur les trames circulant sur un lien Access [12].

La figure II.4 illustre le format de la trame obtenue :

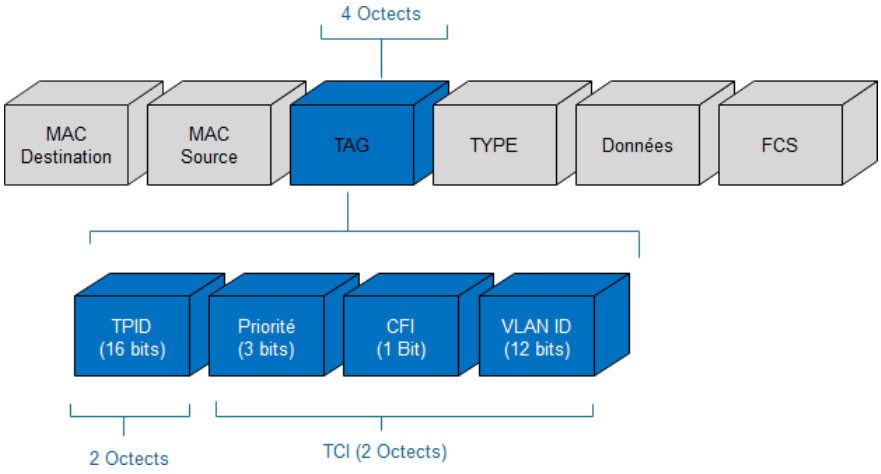

Figure II.4 – Trame Ethernet 802.1q

Ce champ de 4 octets se compose de :

- **TPID (Tag Protocol ID) :** Ce champ de 2 octets, fixer à 0x8100 définis le type donc capsulation et indique qu'elle suit la norme 802.1Q.

- **TCI (Tag Control Information) :** Également à 2 octets il comporte trois informations qui sont les suivantes :

  - **User Priority :**
    Sur 3 bits, définis 8 niveaux de priorités d'un VLAN par rapport à un autre.
  - **CFI (Canonical format Indicator) :**
    Sur 1 bit et la valeur du bit permet de distinguer les trames Ethernet (bit à 0) des trames Token Ring (bit à 1).
  - **VLAN-ID :**
    Sur 12 bits, indique le numéro du VLAN auquel appartient à la trame, il est possible de coder $12^{12} - 2 = 4094$ VLANs avec ce champ.

1.1.5.2 Protocoles de contrôle

1.1.5.2.1 Protocole VTP

Le protocole VTP est un protocole de niveau 2 utiliser pour configurer et administrer les VLAN sur des commutateur Cisco. Son avantage principal c'est sa capacité à propager automatiquement des VLAN configurés sur un commutateur en mode « server » vers les autres commutateurs configurés en mode « client », VTP utilise des liens TRUNK pour annoncer les informations VLAN aux autres commutateurs. Dans un réseau complexe contenant plusieurs commutateurs, VTP évite également toute incohérence dans la configuration VLAN par l'ensemble de réseau local.

Dans un domaine VTP, on distingue une hiérarchie comprenant trois modes de fonctionnement :

✓ VTP mode server :

C'est le mode par défaut de tous les commutateurs de niveau 2, il permet à l'administrateur d'apporter d'éventuelle modification au VLAN et de propager automatiquement les modifications à tous les commutateurs réseau du même domaine VTP et les enregistre dans la NVRAM.

✓ VTP mode client :

Les commutateurs en mode client ne permettent pas aux administrateurs de modifier les VLAN, ils envoient/transmettent des annonces VTP et synchronisent les informations de configuration VLAN avec d'autres commutateurs, ils stockent également les informations VLAN dans son fichier VLAN.dat.

✓ VTP mode Transparent :

Un commutateur en mode transparent permet à l'administrateur d'apporter des modifications au VLAN uniquement localement. Les commutateurs transparents VTP n'annoncent pas leur configuration VLAN et ne synchronisent pas leur configuration VLAN en fonction des annonces reçues, mais les commutateurs transparents transmettent les annonces VTP qu'ils reçoivent sur leurs ports de jonction VTP.

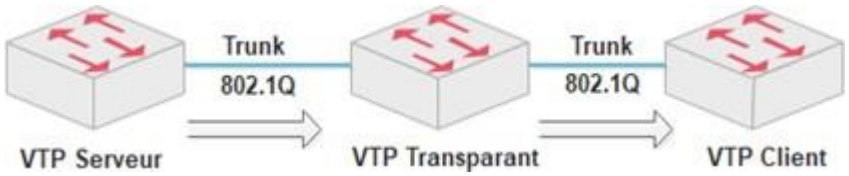

Figure II.5 – Différents modes du VTP

❖ **Synchronisation VTP :**

À chaque fois qu'un VLAN est créé/supprimé/modifié, une variable appelée RN (Révision Number) est incrémentée (initialement 0, puis 1, puis 2, puis 3...), le switch server envoie un message VTP avec la nouvelle valeur RN. Les autres commutateurs comparent le RN reçu du commutateur serveur avec leur RN stocké localement, et si ce dernier est plus petit, le commutateur se synchronise avec le serveur et récupère la nouvelle base de données VLAN. Par défaut, le RN est envoyé automatiquement une fois qu'un VLAN est créé/supprimé/modifié, puis toutes les 5 minutes.

❖ **Commande VTP :**

- **Numéro de révision :**

  Le numéro de révision de configuration est un nombre de 32 bits qui représente le niveau de révision du paquet VTP. Chaque commutateur suit ce numéro de configuration pour déterminer si les informations reçues sont plus récentes que la version actuelle.

  Il existe 3 RN :

  V1 : Les commutateurs Cisco utilisent VTP v1 par défaut. VTP v1 prend en charge les numéros de VLAN de 1 à 1005.

  V2 : prend également en charge les numéros de VLAN de 1 à 1005 VTP V2 n'est pas très différent de VTP V1. La principale différence est que VTP V2 introduit la prise en charge des VLAN Token Ring.

  V3 : prend en charge tous les VLAN de 1 à 4094.

- **VTP Prunning :**

  Le prunning VTP optimise l'utilisation de la bande passante du réseau en limitant le trafic inondant les ports de jonctions qui peuvent atteindre tous les périphériques réseaux actifs. Lors de l'utilisation de ce protocole, un port de jonction ne recevra pas de trafic inondé destiné à un VLAN spécifique. Supposons qu'un commutateur reçoive les VLAN 1 et 2, mais qu'aucune de ses interfaces n'appartienne au VLAN 2. Lorsqu'un commutateur adjacent lui envoie des trames à partir du VLAN 2, le commutateur les abandonne car aucune de ses interfaces n'appartient à ce VLAN. Il est donc inutile que le switch voisin lui envoie du trafic VLAN 2. On active alors la fonction VTP pruning pour avertir le switch voisin de ne pas lui envoyer de trafic pour ce VLAN. La fonction s'active à partir du switch Server.

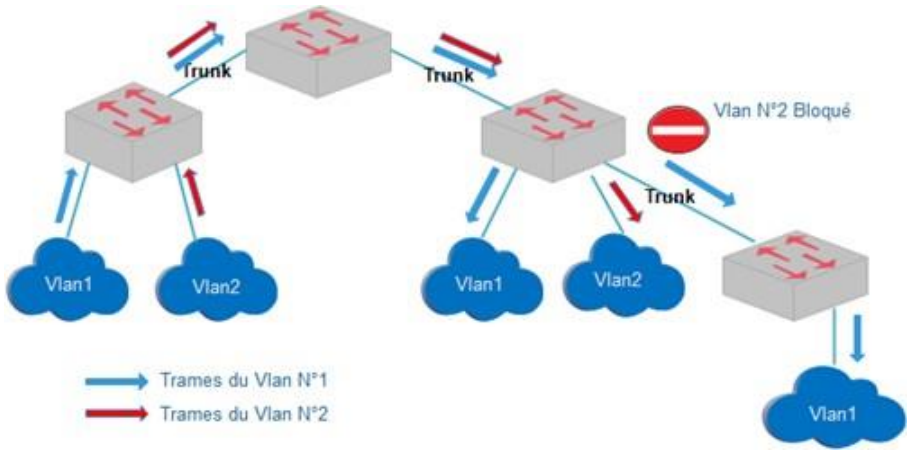

Figure II.6 – Principe du VTP prunning

- **Mot de passe VTP :**
  Les mots de passe doivent être configurés sur tous les commutateurs domaine VTP. Il doit être le même sur tous les commutateurs.

1.1.5.2.2 Protocole GVRP (Generic VLAN Registration Protocol)

GVRP Est un protocole développé par l'IEEE sous la norme 802.1Q. Il nous permet de transmettre des informations VLAN entre des périphériques réseau. GVRP utilise le mécanisme de fonctionnement du GARP (Generic Attribute Registration Protocol), GARP fournit une propagation dynamique des informations VLAN et est utilisé pour l'enregistrement et le désenregistrement de différents attributs VLAN, GVRP fonctionne de la même manière que VTP, mais a été développé pour fonctionner sur différentes marques d'appareils. Les ports exécutant GVRP sont appelés participants GVRP, ils sont automatiquement affectés ou supprimés du VLAN. Avec GVRP, les VLAN configurés sur un ou plusieurs commutateurs sont propagés sans intervention de configuration manuelle de la part de l'administrateur. Le processus d'attribution et de suppression de VLAN est appelé enregistrement de VLAN et désenregistrement de VLAN. Lorsqu'un VLAN reçoit une déclaration d'attribut, les informations VLAN ici sont affectées à ce port, ou lorsqu'un VLAN reçoit une déclaration de suppression, les informations VLAN ici sont supprimées de ce port. [18]

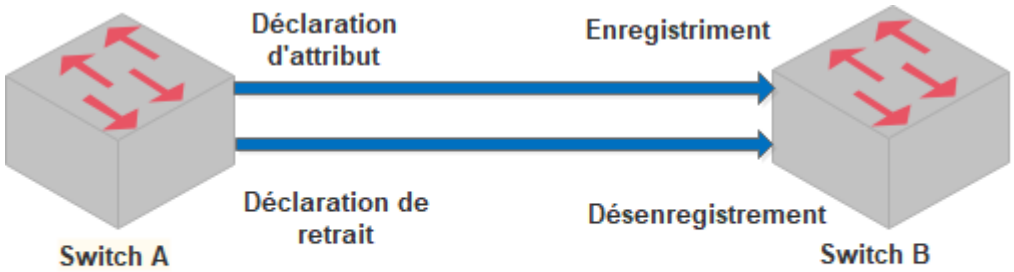

Figure II.7 – Principe GVRP

1.1.5.2.3 Protocole DTP (Dynamic Trunking Protocol)

Le protocole DTP est un protocole propriétaire de Cisco de couches liaison de données, il est par défaut activé et utiliser pour la négociation d'un trunk entre deux commutateurs et détermine le type d'encapsulation à effectuer sur la trame (802.1Q ou ISL).

1.1.5.2.4 Protocole DHCP (Dynamic Host Configuration Protocole)

Est un protocole qui permet à des périphériques se connectant sur un réseau local, d'obtenir dynamiquement sa configuration IP, c'est-à-dire sans une intervention humaine sur les périphériques, réduisant voir supprimant les erreurs dû à l'adressage. Il offre une administration beaucoup plus simple, particulièrement lorsque le réseau local est devisé en VLANs, où il attribue automatiquement des adresse IP aux machines en fonction de leurs VLAN d'appartenance.

Le protocole DHCP est basé sur une architecture client-serveur, où le serveur joue le rôle central dans l'attribution des adresses IP, il reçoit les requêtes d'hôtes désirant accéder au réseau et y répond.

1.1.5.2.5 EtherChannel

Le besoin en bande passante ne cesse de croitre, spécialement avec des applications telles que la messagerie instantanée ou la vidéo, il est donc nécessaire de recourir à diverses méthodes afin d'améliorer cette dernière. Il a été envisagé d'utiliser des liens plus rapides, sauf que c'est un coût en plus, ou alors utiliser plusieurs liens physiques entre les switches, mais le protocole STP bloquera tous les liens pour en laisser qu'un seul ce qui est donc non bénéfique en termes de bande passante.

Cisco est venue par la suite avec une technique qui consiste à réunir plusieurs liens physiques en un seul lien logique trompant ainsi STP qui le considérera comme étant un seul lien, c'est la technique d'agrégation de liens communément appelée EtherChannel.

Tous les ports qui composent le lien EtherChannel sont actifs, ce qui induit à une augmentation de la bande passante. Un regroupement doit se faire entre des ports identiques sur le lien qui comportera au maximum 8 ports pour un maximum de 6 liens EtherChannels par switch.

Cette technologie fournie également une redondance, dans la mesure où si un lien physique appartenant à un même lien logique vient à tomber en panne, cela n'affectera pas la topologie et ce tant qu'il reste au moins un lien physique fonctionnel, en revanche ça affectera la bande passante où elle se trouvera réduite. Il existe deux manières pour crée une agrégation de liens, soit en la forçant (mode ON) or l'interface est membre de l'agrégation sans aucune négociation, soit en utilisant un protocole de négociations d'agrégations dont on en distingue deux qui sont les suivants [14] :

❖ **PAgP (Port Agregation Protocol) :**

Est un protocole de négociation propriétaire Cisco, permettant de configurer dynamiquement un lien Etherchannel et possède deux statuts :

1. **auto :** le port attend une requête du port voisin, si celui-ci est en mode Desirable une agrégation est créée, s'il est en mode Auto alors aucune agrégation n'est créée.
2. **Desirable :** le port configuré en mode Desirable négocie avec le port voisin, dans les deux cas : qu'il soit en mode Desirable également ou en mode Auto une agrégation est créée.

Le tableau suivant illustre le procédé des négociations :

PAgP	**ON**	**Desirable**	**Desirable**
ON	Compatible	Non compatible	Non compatible
Desirable	Non compatible	Compatible	Compatible
Desirable	Non compatible	Compatible	Non compatible

TABLE II.7 – Etablissement des agrégations en utilisant PAgP

❖ **LACP (Link Agregation Control Protocol) :**

Est un protocole standard (802.3ad), similaire à PAgP et dont les statuts de port peuvent être :

1. **Passive :** le port attend les paquets LACP du port voisin pour y répondre, et créer une agrégation si le port voisin est en mode Active.
2. **Active :** le port négocie avec le port voisin et établie une agrégation que ce dernier soit en mode active ou en mode passive.

Comme illustré dans le tableau ci-dessous :

LACP	**ON**	**Passive**	**Active**
ON	Compatible	Non compatible	Non compatible
Passive	Non compatible	Non compatible	Compatible
Active	Non compatible	Compatible	Compatible

TABLe II.8 – Etablissement des agrégations en utilisant LACP

1.1.5.2.6 Protocole FHRP (First Hop Redondancy Protocols)

Désigne les protocoles de redondance du premier saut, qui offre des solutions aux limites des passerelles par défauts. Imaginons que nous disposions d'un seul router connectant notre réseau local au réseau externe, l'interface raccordée à notre LAN constitue notre passerelle par défaut, si maintenant ce lien vient à se rompre le LAN tout entier se retrouve isolé des réseaux externes, utiliser deux passerelles paraitrait être une solution à cela, autrement dit si la première passerelle est inutilisable on basculerait vers la deuxième sauf que pour ce faire, il va falloir reconfigurer tous les équipements du réseau en changeant sur chacun d'eux le paramètre Default Gateway et ce serait fastidieux si on est en présence d'un réseau de moyenne ou grande taille.

Les protocoles FHRP remédient à ce problème et ce en proposant de virtualiser une passerelle donnant l'impression que les deux sont une seule et même passerelle par défaut, qui sera ensuite configuré sue nos périphériques ; un des routeurs sera Routeur de transfert qui acheminera le trafic, quant à l'autre sera en Veil et en cas de panne du premier deviendra à son tour Routeur de transfert [14].

Plusieurs protocoles offrent ce service :

❖ **GLBP (Gateway Load Balancing Protocol) :**

Qui est un protocole de redondance du premier saut propriétaire Cisco, où dans une telle topologie, le trafic vers la passerelle est partagé entre les routeurs réels, offrant ainsi un équilibrage de charge. Il existe deux versions : GLBP pour IPv4 et GLBP pour IPv6.

❖ **VRRP (Virtual Redondancy Protocol) :**

Qui est défini par le standard IETF, VRRP élit un routeur principal qui achemine le trafic et des routeurs de secondaire ; le routeur virtuel se verra attribuer une adresse IP et une adresse MAC virtuelles constituant la passerelle. Il existe en deux versions VRRPv2 pour IPv4 et VRRPv3 pour IPv4 et IPv6.

❖ **HSRP (Host Standby Router Protocol) :**

Est un protocole propriétaire Cisco, où un routeur principal est élu, on dit qu'il est en mode active et les autres seront en mode standby c'est-à-dire en écoute et un routeur virtuel aura une adresse IP et une adresse MAC virtuelles également. Existe en deux versions : pour IPv4 et IPv6.

1.1.5.3 Protocoles de routage

1.1.5.3.1 STP (Spanning Tree Protocol)

Normalisé par le comité IEEE 802.1, STP un mécanisme de routage sur réseaux locaux qui travaille au niveau de la couche 2 du modèle OSI. Il consiste à représenter la topologie du réseau en arbre qui recouvre cette dernière et par lequel chaque nœud du réseau est accessible, il existe donc plusieurs chemins possibles vers un nœud de ce dit réseau.

Le protocole élit un commutateur central appelé « root bridge », puis calcule la longueur du chemin « port's cost » entre ce commutateur ainsi que tous les autres nœuds du réseau. Le meilleur chemin, c'est-à-dire celui qui possède le port's cost le plus petit sera retenue comme chemin actif (mode forwarding), quant aux autres ils seront fermés (mode blocking).

Les ponts s'échangent entre eux des messages, et en cas de changement dans la topologie, le switch racine recalcule donc cette valeur et s'il en trouve une inférieure à celle désignée avant, il garde cette nouvelle valeur et change de chemin actif (passage du mode forwarding au mode blocking et vis vers ça) [14][15].

1.1.5.3.2 IGP (Interior Gateway Protocol)

Est un groupe de protocoles de routage dynamique destiné à l'acheminement de paquets au sein d'un réseau d'entreprise, qu'il soit LAN (un seul site) ou WAN (plusieurs sites). Il comprend les protocoles suivants : [10]

• RIP (Routing Information Protocol) :

Est un protocole dit à vecteur de distance, qui existe en trois versions ; RIP version 1, RIP version 2 et RIPpng, dont la première est obsolète. Il permet à un router ou un switch de niveau 3 de déterminer le meilleur chemin et ce en utilisant une métrique qui est le nombre de sauts, qui enfaite est le nombre de routeurs rencontrés en cours de chemin, avec un nombre de sauts max équivaut à 15 et considérant 16 comme un réseau inaccessible, sachant que le nombre le plus petit de sauts sera retenue comme étant le meilleur chemin. Le protocole permet au router de mettre à jour sa table de routage toutes les 30 secondes et l'envoie à tous les autres routeurs du réseau, ce qui est inutile à moins que la topologie change, il est donc inadapté pour les réseaux de moyenne et grande taille.

• IGRP (Interior Gateway Routing Protocol) :

Est un protocole propriétaire Cisco, similaire à RIP mais qui a été remplacé par EIGRP car obsolète.

• EIGRP (Enhanced IGRP) :

Créé par Cisco, c'est un protocole de routage dynamique de couche 3 (Router et switch de niveau 3), fonctionne sur la base du Distance-Vector-Routing, autrement dit, il calcule le nombre de sauts qui est représenté par la valeur AD (Administrative Distance) entre un nœud du réseau et un autre. Le router construit alors une table de routage et la met à jour en prenant soin de garder la valeur AD la plus petite à chaque fois et partage cette table avec les routeurs voisins uniquement.

• OSPF (Open Shortest Path First) :

Est un protocole normalisé, c'est-à-dire opérable sur des périphériques de niveau 3 de différents fabricants d'équipements réseaux. On dit qu'il est à état de liaison, contrairement à RIP et EIGRP qui sont à vecteur de distance, où le nombre de sauts (AD) est le facteur qui détermine le meilleur chemin. Le protocole OSPF lui en revanche découpe le réseau en zones (Area) regroupant plusieurs routeurs (pas plus de 15), un routeur OSPF peut être :

- Backbone Router : sont tous les routeurs appartenant à la zone 0.
- Internal Router : dont toutes les interfaces sont dans la même zone.
- Routeur ABR (Area Border Router) : est un routeur qui a des interfaces dans plus d'une zone.
- Routeur ASBR (Area Summary Border Router) : est un routeur qui connecte un réseau OSPF à d'autres domaines de routage.

Ce découpage en zone permet de réduire la charge CPU des routeurs, car l'échange de paquets de reconnaissance (Hello) et l'algorithme de calcul des routes (Algorithme de Dijkstra) s'exécute uniquement dans la même aire OSPF. Grace aux paquets Hello le routeur recueille des informations sur ces voisins et ces données appelées LSA (Link State Advertissement) seront stocké dans la LSDB (Link State Data Base). Elles seront ensuite utilisées afin de trouver le meilleur chemin vers d'autres réseaux en utilisant l'algorithme.

Une métrique est ensuite déterminée pour chaque liaison avec la formule « 100/Débit », qui représente le coût (cost) de celle-ci et plus le résultat de la métrique sera faible, meilleur sera le chemin.

• IS-IS (Intermediate system to Intermediate system) :

Tout comme OSPF, IS-IS est un protocole de routage dynamique normalisé à état de lien utilisant le même algorithme pour sélectionner le chemin à l'aide des paquets Hello et construisant une base de données qui sera ensuite partagée. Toute fois IS-IS est plus simple d'utilisation qu'OSPF car comprennent moins de fonctionnalités.

1.2 VPN (Virtual Private Network)

De nos jours, grâce au développement des technologies et aux performances des réseaux qui deviennent de plus en plus importantes, les ressources d'un réseau réel peuvent être partagées à tout moment entre un ou plusieurs réseaux disjoints, donnant l'impression d'appartenir à une seule et même infrastructure physique. C'est un atout non négligeable en particulier pour des organisations s'étendant sur de grandes distances géographiques, il est donc opportun de bien maîtriser un tel mécanisme et de protéger un tel flux pour assurer son intégrité, sa confidentialité et son authentification. D'où l'apparition des VPN.

Un VPN, ou réseau privé virtuel est l'ensemble des ressources pouvant être partagées, il offre un moyen de chiffrer le trafic des données et requiert une forte authentification, proposant ainsi un accès à distance sécurisé. [2]

1.2.1 Avantages

- ➢ Un VPN est désormais un outil faisant partie du quotidien de la quasi-totalité des utilisateurs, dans la mesure où il permet de se protéger des potentiels pirates en offrant une navigation et un téléchargement anonymes et un accès à des plateformes de streaming et des sites pouvant être non accessibles dans de certaines zones géographiques.
- ➢ Il offre une sécurité de bout en bout due à l'utilisation de protocoles de chiffrements et d'authentifications.

- ➢ Il se trouve être économique, car utilise internet pour le transport et ne nécessite pas la mise en place d'une connexion physique comme une ligne dédiée qui par exemple connectera plusieurs sites d'une entreprise entre eux sur de longues distances, c'est donc un coût en moins pour l'entreprise en question.
- ➢ Un VPN est une technologie évolutive, où le medium est internet, ce qui fait que l'infrastructure physique est supervisée par les opérateurs et FAIs, rendant l'ajout ou la suppression d'autres utilisateurs possibles sans être influencer par l'infrastructure.

1.2.2 Principe

Un réseau VPN, utilise un processus appelé « Tunneling » afin d'étendre un réseau privé sur un réseau publique qui est Internet, l'idée est de crée un chemin virtuel entre la source et la destination et d'y faire transiter les données chiffrées en assurant leurs confidentialités et leurs intégrités, via le medium public. Toutefois dans la réalité il n'est pas question de tunnel physique à proprement parler, mais s'agit plutôt d'encapsulation et de cryptage des données pour une livraison en toute sécurité.

L'encapsulation isole le paquet de données des autres données circulant sur le même réseau, quant au cryptage il rend les données illisibles pour une personne autre que le destinataire légitime. [2]

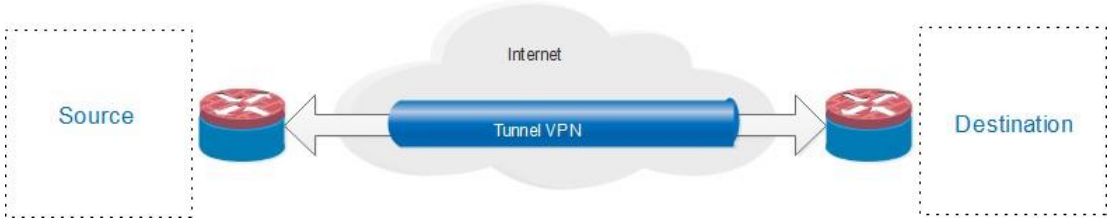

Figure II.8 – Principe d'un tunnel VPN

1.2.3 Types de VPN

1.2.3.1 VPN d'accès

Le VPN d'accès à distance est le type de VPN le plus populaire aujourd'hui. Connecte les utilisateurs à un réseau privé via un serveur distant sécurisé. L'accès à distance VPN fonctionne en acheminant les données de l'utilisateur via un tunnel virtuel entre l'appareil de l'utilisateur et le réseau privé. [13]

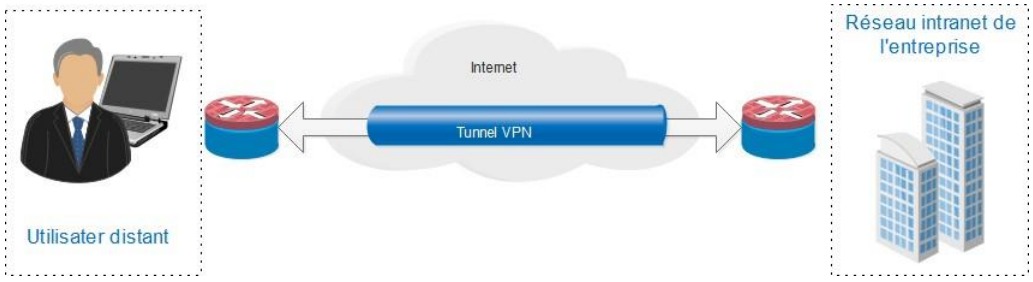

Figure II.9 – VPN d'accès

1.2.3.2 VPN site à site

Les VPN de site à site sont souvent utilisés dans les grandes entreprises où plusieurs utilisateurs situés à différents endroits doivent accéder à des ressources partagées. Les organisations ayant des succursales dans de nombreux endroits s'appuient sur des VPN de site à site pour connecter le réseau d'une succursale à une autre.

Il existe différents types de VPN de site à site : [13]

1.2.3.2.1 Intranet

Un VPN intranet est utilisé pour relier deux ou plusieurs intranets. Ce type de réseau est particulièrement utile dans les entreprises disposant de plusieurs sites distants. Dans ce type de réseau, le plus important est de garantir la sécurité et l'intégrité des données.

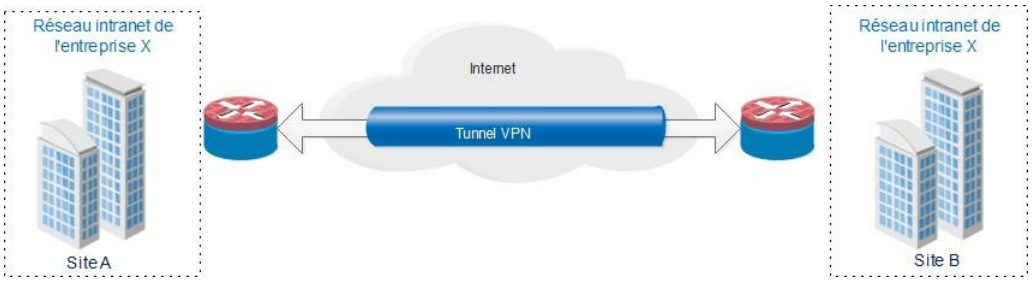

Figure II.10 – VPN intranet

1.2.3.2.2 Extranet

Un extranet VPN est utilisé dans une entreprise pour établir la communication entre les clients et ses partenaires.

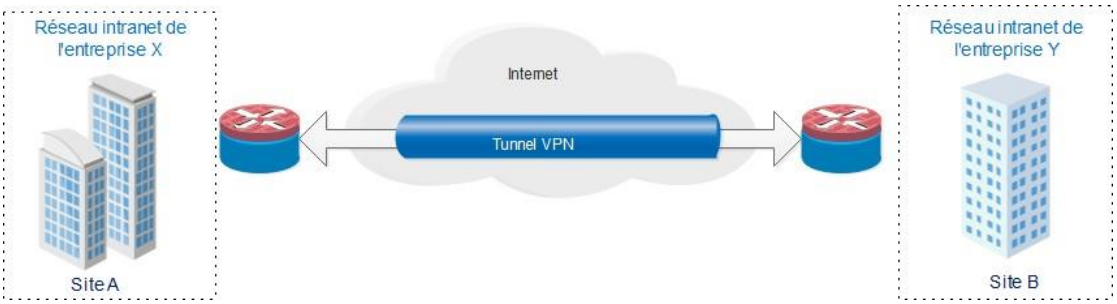

Figure II.11 – VPN extranet

1.2.4 Protocoles utilisés

1.2.4.1 Protocole PPP (Point to Point Protocol)

Est un protocole de transport de couche liaison de données (couche 2 du modèle de référence OSI), basé sur HDLC, permettant le transfert de données sur des liaisons point à point synchrone ou asynchrone, et est full duplex et garantit l'ordre d'arrivée des paquets entre deux hôtes. Il est défini par le standard RFC 1661, et permet d'encapsuler des paquets IP, IPX et NetBEUI dans des trames PPP et de les acheminer au travers de la liaison point à point.

Le protocole d'encapsulation de paquet PPP est lui-même composé de sous protocoles chargés du réseau de liaison ou NCP (Network Control Protocol) qui comporte des protocoles tels que : ACP-AppleTalk, ECP-DES, triple DES, PPP-LEX-LAN et bien d'autre encore ; mais aussi de protocoles chargés du contrôle de la liaison LCP (Link Control Protocol) comme : PAP (Password Authentification Protocol), CHAP (Challenge-Handshake Authentification Protocol), EAP (Extensible Authentification Protocol), etc [11].

1.2.4.2 Protocole PPTP (Point to Point Tunneling Protocol)

Créé par Microsoft en collaboration avec Ascend et 3Com et défini par la RFC 2637, PPTP est un protocole de niveau 2 qui permet de créer un réseau privé virtuel en étant pris en charge par des protocoles tels que IP, IPX et NetBEUI.

Paracerque Microsoft y a implémenté ses propre algorithmes, PPTP est intégré à son système d'exploitation, faisant de lui un outil largement utilisé dans les produits VPN Commerciaux.

Par le biais d'un tunnel, le protocole PPTP encapsule les paquets IP qui eux même sont encapsulés dans des paquets PPP, et ce en utilisant le protocole GRE pour la création de ce tunnel de niveau 3.

PPTP s'appuie sur plusieurs protocoles : ainsi la fonction d'authentification est assurée par les protocoles PAP ou MS-CHAP, le chiffrement par les fonctions de MPPE et enfin la compression par MPPC [11][2].

1.2.4.3 Protocole L2TP (Layer 2 Tunneling Protocol)

L2TP est un protocole de niveau 2 basé sur PPP et permettant la création d'un tunnel. Ce protocole assure uniquement le transport et l'intégrité des données, pas la confidentialité. Par conséquent, les données transitant par ce protocole ne sont pas cryptées.

1.2.4.4 Protocole MPLS (Multi Protocol Label Switch)

Est une technologie conçue pour augmenter la vitesse et l'efficacité du transfert de données au sein d'un WAN ou d'un site informatique en périphérie. Il fonctionne au sein d'un réseau privé virtuel (VPN) et s'intègre aux infrastructures sous-jacentes telles que les réseaux IP (Internet Protocol), Ethernet, FR (Frame Relay) et ATM (Asynchronous Transfer Mode).

1.2.4.5 Protocole GRE (Generic Routing Protocol)

Est un protocole de tunnelisation permettant à deux routeurs de construire un tunnel virtuel entre eux, au-dessus du réseau physique et d'y faire transiter des paquets d'un bout à l'autre du tunnel, qui seront encapsulés grâce au protocole GRE ; une fois le tunnel créé une adresse IP source et une adresse IP destination sera attribuer à ses deux extrémités, comme le montre la figure suivante :

Figure II.12 – Principe du tunnel GRE

Un routage est ensuite nécessaire, soit statique soit par l'utilisation de protocoles de routage. Cependant le protocole GRE ne fournit pas de sécurité pour le tunnel, et pour ce faire il faudra utiliser le protocole IPSec qui lui est sécurisé. Mais alors pourquoi utiliser GRE puisqu'il ne nous offre pas de sécurité ? Et bien tout simplement que GRE contrairement à IPSec a la capacité de supporter les paquets multicast ainsi que les protocoles de routage.

1.2.4.6 Protocole IPSec (Internet Protocole Security)

IPSec est conçu pour protéger le trafic réseau de la couche réseau, par conséquent, il peut protéger tous les types d'applications et de protocoles réseau basés sur IP. Il a été conçu de manière à être supporté par Ipv4 et a été intégré dans le protocole Ipv6 par la suite. Le protocole IPSec est un complément du protocole IP, il intègre donc les concepts de base de la sécurité des datagrammes IP qui garantiront l'intégrité, l'authentification et la confidentialité.

1.2.5 Présentation de l'IPSec

IPsec est un protocole de sécurité développé par l'IETF (RFC 2401) en 1995, c'est un protocole de couche 3 du modèle OSI (couche réseau) qui fait référence à un ensemble de mécanismes de protection du trafic au niveau IP (IPv4 ou IPv6). L'intérêt principal d'IPsec reste sans aucun doute son soi-disant mode tunnel, c'est-à-dire l'encapsulation IP, qui lui permet entre autres de créer un VPN. IPSec Permet une connexion entre les deux des systèmes informatiques, entièrement sécurisés, utilisant le réseau existant. Facultatif dans IPv4, IPsec est obligatoire pour toute implémentation IPv6. [3]

1.2.5.1 Mécanismes de sécurité de IPSec

IPsec utilise deux mécanismes de sécurité pour le trafic IP, les protocoles AH et ESP, ajoutés à la gestion IP classique.

1.2.5.1.1 En-tête d'authentification (AH)

Conçu pour garantir l'intégrité et l'authentification des datagrammes IP sans cryptage des données (c'est-à-dire sans confidentialité). Le principe de HA est d'ajouter un champ supplémentaire aux datagrammes IP classiques qui permet un accusé de réception permettant et de vérifier l'authenticité des données contenues dans le datagramme.

1.2.5.1.2 Encapsulating Security Payload (ESP)

À pour rôle premier d'assurer la confidentialité, mais il peut aussi garantir l'authenticité des données. Le principe de l'ESP est de générer un datagramme IP classique, un nouveau datagramme où les données et l'en-tête d'origine étaient probablement cryptés.

1.2.5.2 Mode de fonctionnement

IPSec fonctionne selon deux modes différents.

1.2.5.2.1 En mode transport

Dans le mode transport, IPSec intervient entre le niveau transport (TCP) et le niveau réseau (IP) du modèle OSI : le PDU de la couche transport se voit appliqué les mécanismes de signature et de chiffrement puis le résultat passe à la couche réseau (encapsulation IP). Ce mode ne résout pas un problème majeur en matière de sécurité : l'en-tête du paquet est inchangé puisque produit par la couche IP. Il n'y a donc ni masquage d'adresse ni protection des options IP. Cependant ce mode est relativement aisé à mettre en œuvre. En mode transport, seules les données en provenance du protocole de niveau supérieur et transportées par le datagramme IP sont protégées. Ce mode n'est utilisable que sur des équipements terminaux ; en effet, en cas d'utilisation sur des équipements intermédiaires, on courrait des risques, suivant les aléas du routage, que le paquet atteigne sa destination finale sans avoir traversé la passerelle censée le déchiffrer.

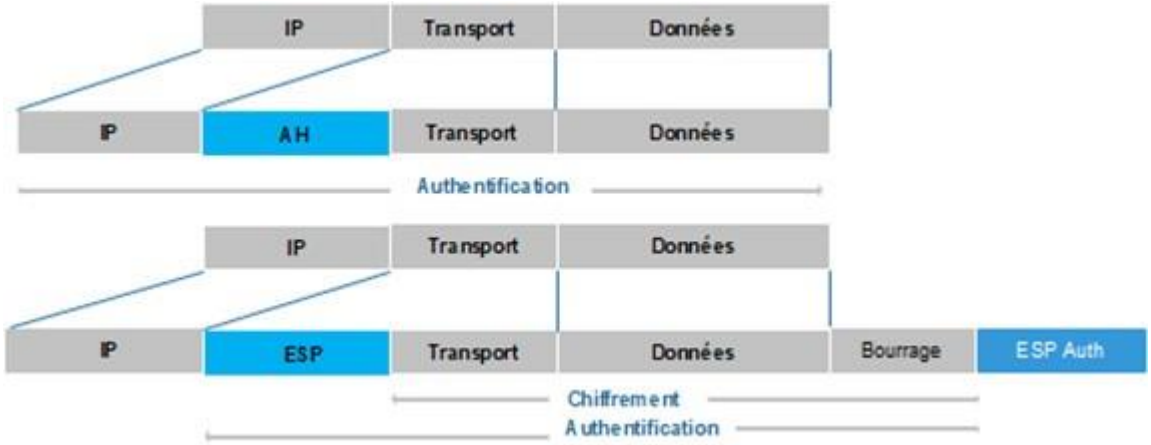

Figure II.13 – Encapsulation en mode transport

1.2.5.2.2 En mode tunel

IPSec fonctionne directement après l'encapsulation IP. Le paquet IP entier est encapsulé dans un paquet IPSec sécurisé. Dans ce cas, l'en-tête IP d'origine est protégé et l'adresse est masquée. Ce mode est largement utilisé pour configurer des VPN. En mode tunnel, les en-têtes IP sont également protégés (authentification, intégrité et/ou confidentialité) et remplacés par le nouveau titre. Ce nouvel en-tête est utilisé pour transmettre des paquets à tunnel, où l'en-tête d'origine est restauré. Ainsi, le mode tunnel peut être utilisé pour les deux terminaux et passerelles de sécurité. Ce mode assure une meilleure protection contre l'analyse du trafic car elle masque les adresses expéditrices et destinataire final.

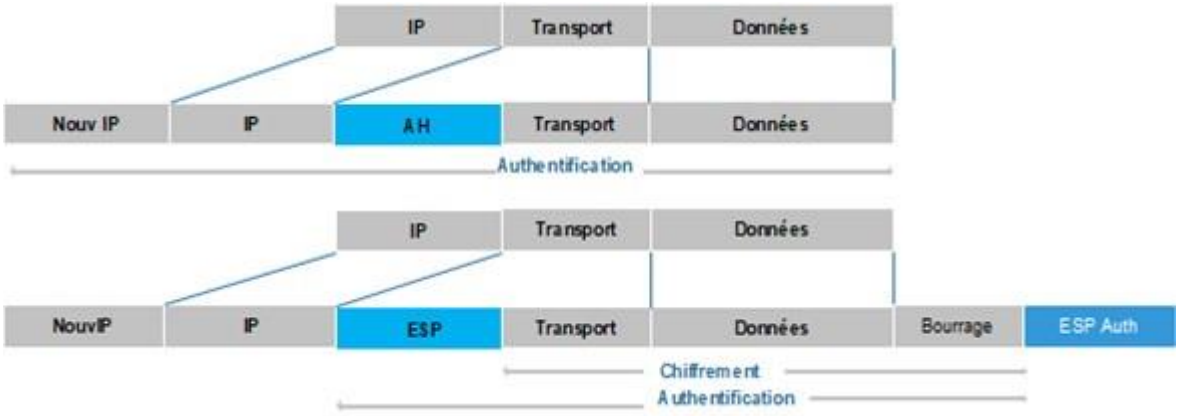

Figure II.14 – Encapsulation en mode Tunnel

1.2.5.3 Les négociations VPN IPSec

La négociation VPN est un processus qui consiste à créer un tunnel VPN, pour cela deux terminaux agissant en tant que pairs IPsec échangent une série de messages liés au cryptage et à l'authentification, puis essayant de s'entendre sur de nombreuses questions d'installation. Pour gérer la négociation entre deux routeurs (PC, firewall), IPsec utilise le protocole IKE (Internet Key Exchange), qui gère la connexion entre deux routeurs en deux phases : Phase 1 et phase2.

1.2.5.4 Les gestions de clés

Comme nous l'avons vu précédemment, IPSec offre une intégrité, authentification et confidentialité des données, ce qui nécessite des mécanismes de chiffrement impliquant la mise en place de gestion de clés ainsi que leurs distributions aux acteurs d'une communication IPSec.

Pour cela le protocole IKE (Internet Key Exchange) est utilisé pour une gestion et distributions automatique des clés, c'est un moyen sûr de s'échanger des clés afin de chiffrer les données transitant à travers un tunnel VPN entre deux réseaux locaux où entre un client et un réseau local. IKE permet à travers cet échange de clés d'authentifier les deux extrémités utilisant la connexion VPN, il permet également de déterminer le protocole de chiffrement à utiliser.

IKE est un protocole qui existe en deux versions : IKE version 1 (IKEv1), défini dans la RFC 2409 et IKE version 2 (IKEv2) défini dans la RFC 5996. Il combine des éléments et des fonctionnalités issues de protocoles tels que : ISAKMP, SKEME, et Oakley.

Défini dans la RFC 2408 ISAKMP (Internet Security Association And Key Management Protocol) est un protocole apportant une infrastructure sur laquelle est basé IKE et qui permet de définir et d'administrer des SA entre deux machines.

Il y a souvent ambiguïté pour ce qu'il s'agit de différencier IKE et ISAKMP, car les deux termes sont souvent interchangeables, c'est d'ailleurs le cas dans les platforms Cisco.

1.2.5.5 Les bases de données SPD et SAD

Un système de communication utilisant IPSec possède deux bases de données où sont stockés SP et SA qui sont respectivement SPD et SAD. Sachant que SP (Security Policy) définit ce qui doit être traité sur un flux de sécurité, et SA (Security Association) définit la manière avec laquelle sera traité le paquet en fonction de sa SP.

1.2.5.5.1 SPD (Security Policy Database)

Est une base de données qui permet de déterminer comment appliquer les traitements nécessaires sur les paquets et s'ils seront ou non autorisés, elle est mise en place par un administrateur ou un utilisateur quelconque.

1.2.5.5.2 SAD (Security Association Database)

Est la base de données propre à SA, contenant tous les paramètres relatifs à chaque association de sécurité. Elle est consultée pour déterminer quel mécanisme sera appliqué sur chaque paquet reçu ou à émettre.

1.2.5.6 Principe de fonctionnement

La figure ci-dessous, représente tous les éléments présentés ci-dessus (en bleu), leurs positions et leurs interactions.

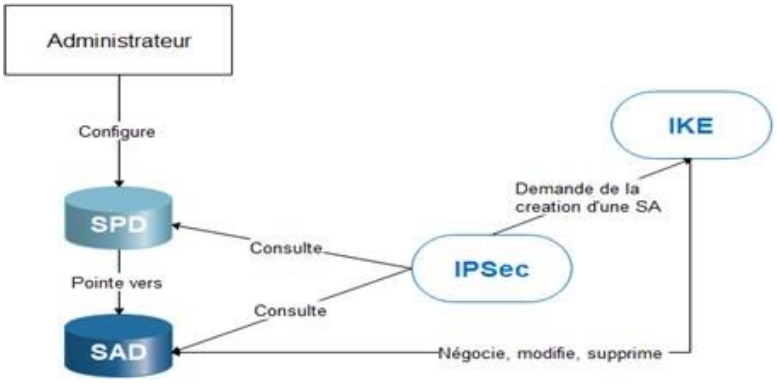

Figure II.15 – Schéma global de IPSec

On distingue deux situations

Trafic sortant :

Lorsque la couche IPSec reçoit des données à envoyer, elle consulte d'abord la base de données de politique de sécurité (SPD) sur la manière dont ces données sont traitées. Si cette base lui indique que le trafic doit appliquer un mécanisme de sécurité, elle récupère les caractéristiques requises de la SA correspondante et interroge la base de données de SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPsec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

Trafic entrant :

Lorsque la couche IPSec reçoit un paquet du réseau, elle examine l'en-tête du paquet pour savoir si un ou plusieurs services IPsec ont été appliqués à ce paquet, et si oui, quelles sont les références de la SA. Il consulte ensuite le SAD pour savoir quels validation et/ou déchiffrement de paquets. Une fois le paquet authentifié et/ou déchiffré, le SPD est interrogé pour voir si l'association de sécurité appliquée au paquet correspond. Si le paquet reçu est un paquet IP classique, le SPD permet de savoir s'il a encore le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont gérés par IKE qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

2 Présentation de l'organisme d'accueil, problématiques et solutions proposées

Dans cette section, afin de nous familiariser avec l'environnement de l'entreprise, à savoir CAMPUS NTS, nous allons l'introduire en présentant d'abord un bref historique, ses différentes branches, les différents services qui compose l'entreprise, puis ses secteurs d'activité ainsi que les services qu'elle propose et enfin nous étudierons un cas qui constituera notre projet où nous établirons un diagnostic qui soulèvera la problématique et enfin nous proposerons une solution pour ce cas.

2.1 Présentation générale

2.1.1 Situation géographique

CAMPUS NTS se situe dans la ville de BEJAIA, au lieu-dit « Targa Ouzamour », face à l'université de BEJAIA.

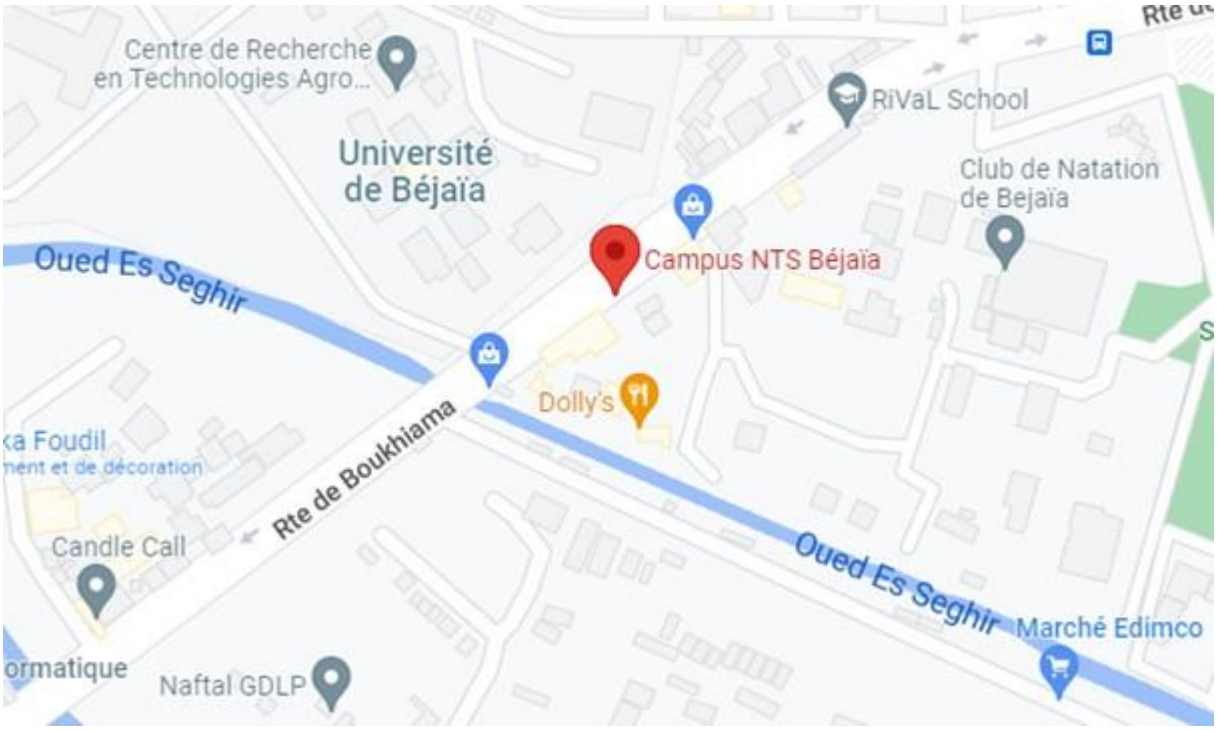

Figure II.16 – Localisation de l'entreprise CAMPUS NTS.

2.1.2 Historique

L'entreprise CAMPUS NTS a été fondée en 2020, elle est spécialisée dans l'étude, la conception et la réalisation de solutions ainsi que l'intégration de systèmes de sécurité, offrant à d'autres entreprises ou des particuliers des solutions intelligentes, innovantes et efficaces, mais pas que ; CAMPUS NTS offre aussi un large choix de formations pour toute personne désireuse d'en apprendre davantage sur le monde des réseaux.

2.1.3 Structure et organigramme

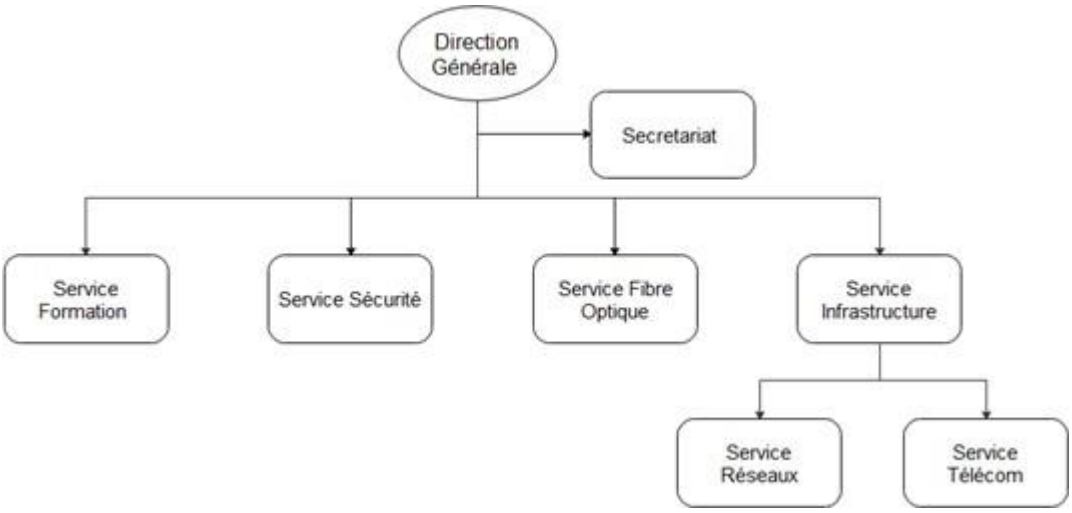

Figure II.17 – Organigramme de l'entreprise CAMPUS NTS.

2.2 Description des services

2.2.1 Service formation

CAMPUS NTS propose à ses clients des formations certifiées qui sont les suivantes :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et systèmes.
- Installation et configuration des firewalls (Pfsense, Sophos, fortigate, palo alto. . .).
- Installation et configuration des réseaux sans fil professionnelle.
- Installation et configuration des cameras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTx.
- Création des sites web.
- Programmation (C, C#, C++, java, python. . .).
- Electricité bâtiments et industriels.
- Formation Cisco CCNA, CCNP, S&R.
- Virtualization.
- Microsoft Server, SQL.
- Cybersecurity.

2.2.2 Service réseaux et télécom

Ce service a pour objectif la mise en place et la configuration du réseau informatique de l'entreprise, il assure :

- ✓ La pose du câblage informatique.
- ✓ La configuration des postes utilisateurs.
- ✓ La gestion des domaines, des groupes et des ressources.
- ✓ La maintenance des équipements.
- ✓ Analyses et corrections des pannes.

2.3 Domaine d'activité

CAMPUS NTS exerce dans les domaines suivants :

- Ondulation et protection électrique et énergie solaire.
- Vidéo surveillance.
- Vidéophone et interphone.
- Réseaux informatiques.
- Contrôle d'accès et pointeuse.
- Détection d'incendies et anti-intrusion.
- Domotique.
- Formation et consulting.
- Télédistribution.
- Wifi-professionnel.
- Standard téléphonique.
- Fibre optique.

2.4 Services et produits proposés

2.4.1 Services proposés

CAMPUS NTS offre à ses clients les services suivants :

- Une expertise certaine dans le domaine de la sécurité.
- Une gamme étendue pouvant aller du haut de gamme à la gamme standard afin de toujours satisfaire une cible large et diversifiée.
- Une augmentation des avantages perçus par le client, de par les offres personnalisées.
- Un réseau complet de collaborateurs assurant la réalisation et le suivi des projets d'installation de systèmes de sécurité de A à Z.

2.4.2 Produits proposés

L'entreprise offre une large gamme de produits dont les suivants :

- Produits de réseaux et data center armoire, panneaux, câblage, prises, Converter, goulotte, cordon, système d'aération, onduleurs et protection électrique, serveurs, load balancing…
- Éléments actifs de réseau : hubs, switches, routeurs, firewall, proxy…
- Éléments passifs : tous types de câblage réseau et télécoms, coaxial, pairs torsadée, fibre optique…
- Équipements informatique et bureautique.
- Équipements de téléphonie et télécom.
- Équipements d'ondulation et protection électrique.
- Installation d'énergie solaire.
- Équipements de sécurité physique.

3 Problématique

Au cours de notre période de stage au sein de l'entreprise CAMPUS NTS nous avons remarquées certaines contraintes pouvant réduire les performances du réseau de l'entreprise mais surtout porter atteinte à sa sécurité, où on note :

- Un seul et unique domaine de diffusion.
- Une gestion d'adressage peu optimale, utilisant un adressage statique.
- Une liaison non sécurisée via Internet entre ses partenaires.

Ce qui soulève les questions suivantes :

➢ Comment assurer la sécurité des échanges de données entre les services du réseau local de CAMPUS NTS ?

➢ Comment nous est-il possible de relier le réseau local de l'entreprise sise à Bejaia avec le réseau local d'un partenaire se trouvant à Alger ?

4 Solutions

L'objectif de notre travail est de corriger les contraintes exposées en problématique précédemment et ainsi optimiser les ressources de l'entreprise notamment en bande passante, mais surtout sécuriser les échanges via Internet, pour cela, nous proposons d'organiser les service composant CAMPUS NTS en groupe logique (VLAN) afin de faciliter la gestion du réseau et mettre en place un VPN en utilisant IPSec pour sécuriser les flux de données qui passeront par Internet.

Voici donc l'architecture proposée :

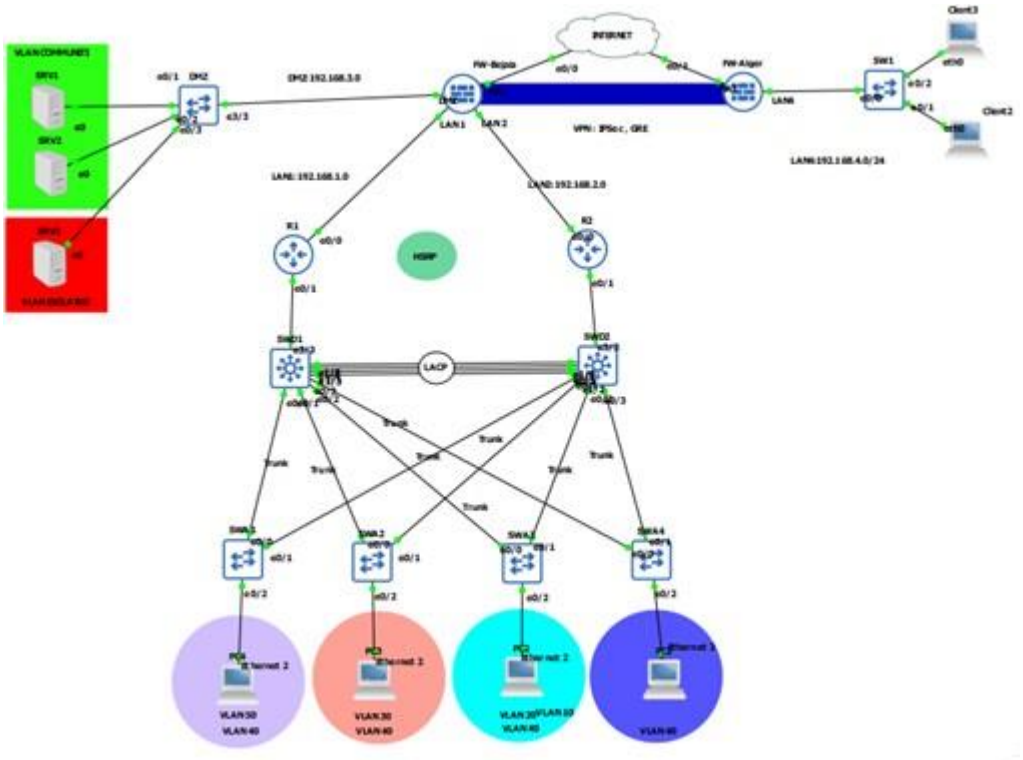

Figure II.18 – Nouvelle architecture proposé.

Conclusion

Au cours de ce chapitre, nous avons introduit les liaisons virtuelles à savoir les VLANs et les VPNs, où nous avons pu pour chacun d'eux poser une définition, leurs principes ainsi que leurs caractéristiques et leurs importances dans un système informatique. Par la suite nous avons présenté l'organisme d'accueil CAMPUS NTS, qui après un diagnostic du réseau nous avons mis le point sur quelques failles du réseau auquel nous avons proposé des solutions.

III

Simulation et resultats

Introduction

Dans ce chapitre, afin de mettre en œuvre tout ce qui a été traité dans la partie théorique de notre travail et afin de répondre à la problématique posée précédemment, nous allons simuler nos solutions proposées pour le réseau de l'entreprise Campus NTS Bejaia. Nous commençons par présenter le logiciel utilisé pour la réalisation de notre projet, puis nous énumérons tous les étapes effectuées pour y parvenir ; enfin nous terminons par les tests et résultats obtenus.

1 Outils de réalisation

1.1 GNS3

GNS3 est un simulateur de réseau permettant la simulation et l'émulation des réseaux en général et les équipements Cisco en particulier tels que les routeurs et les commutateurs.

1.2 VMware Workstation

VMware Workstation est un hyperviseur géré qui s'exécute sur les versions x64 des systèmes d'exploitation Windows et Linux, il permet aux utilisateurs de configurer des machines virtuelles (VM) sur une seule machine physique et les utiliser simultanément avec l'hôte

1.3 Windows 7

Windows 7 est un système d'exploitation de la société Microsoft, sorti le 22 octobre 2009 et successeur de Windows Vista.

1.4 Windows server 2016

Windows Server 2016 est le système d'exploitation orienté serveur de Microsoft. Basé sur l'architecture Windows NT, il connecte l'environnement sur site avec Azure. Il ajoute une nouvelle couche de sécurité tout en aidant à moderniser vos applications et infrastructures. Par conséquent, il fournit divers services orientés serveur tels qu'héberger des sites Web, gérer les ressources entre différents utilisateurs et applications, ainsi que des fonctionnalités de messagerie et de sécurité.

1.5 Wireshark

Wireshark est un analyseur de protocole réseau gratuit et open source qui permet aux utilisateurs de visualiser de manière interactive le trafic de données sur un réseau informatique. Le projet de développement a débuté sous le nom d'Ethereal, mais a été renommé Wireshark en 2006.

2 Environement de travail

2.1 Installation de GNS3

Après avoir téléchargé le fichier GNS3 nous allons l'exécuter et suivre les étapes d'installation jusqu'à la fin.

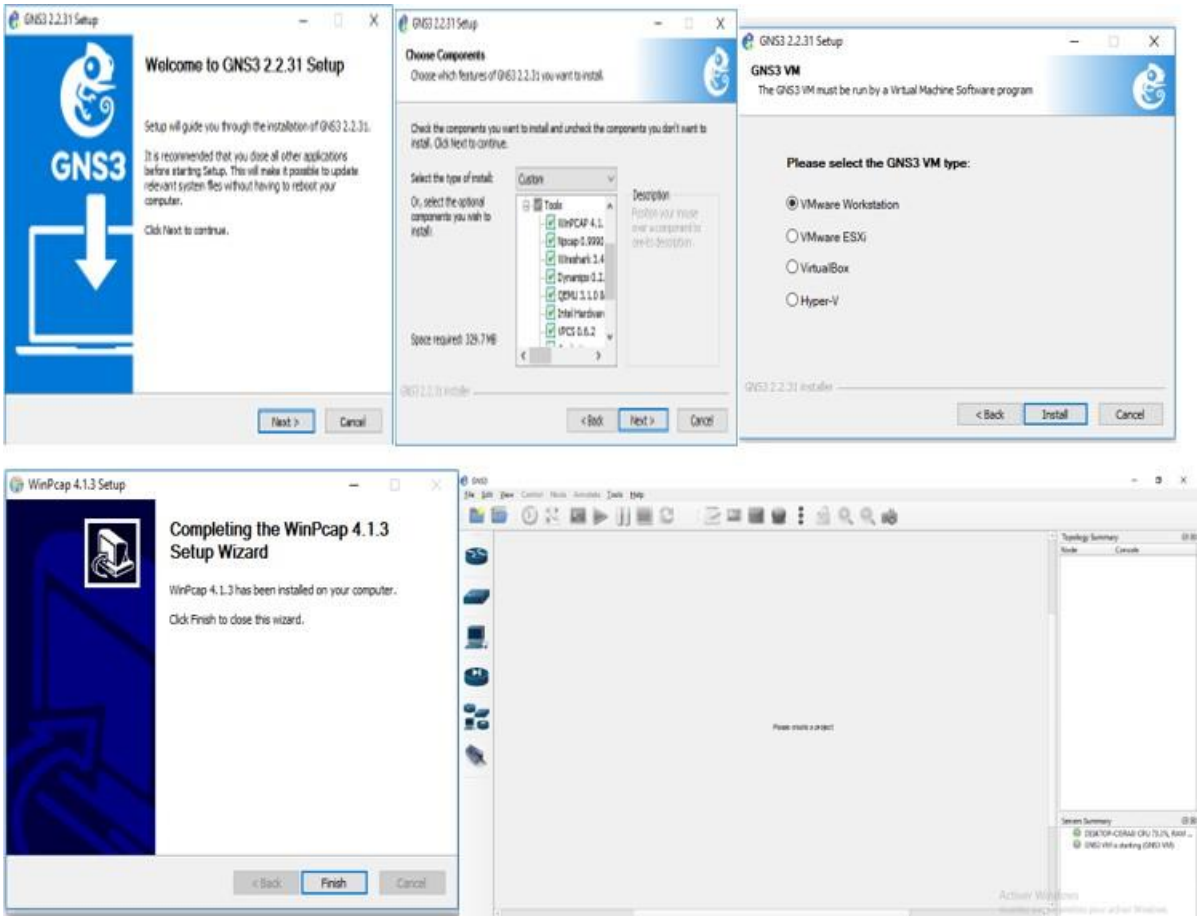

Figure III.1 – Étapes d'installation de GNS3

2.2 Installation de VMWare Workstation

Pour que nous puissions créer des machines virtuelles, nous aurons besoin d'installer VMware Workstation et ce en suivant les étapes d'installation.

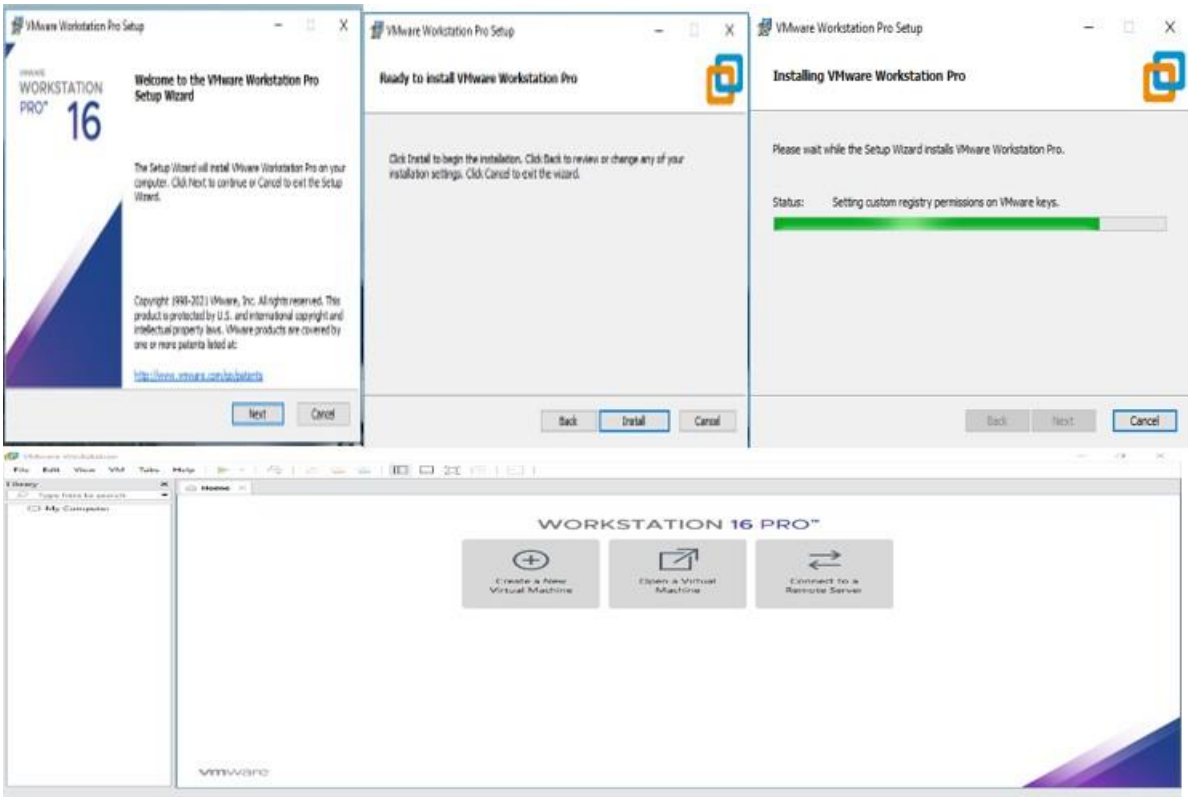

Figure III.2 – Étapes d'installation de VMware Workstation

2.3 Création et installation des machines virtuelles

2.3.1 GNS3 VM

Avant toute chose, nous allons d'abord créer la machine virtuelle de GNS3 et ce en allant sur VMware Workstation et en cliquant sur File > Open, puis en suivant les étapes indiquées, on importe le fichier GNS3 VM tel qu'il est illustré dans la Figure III.3 :

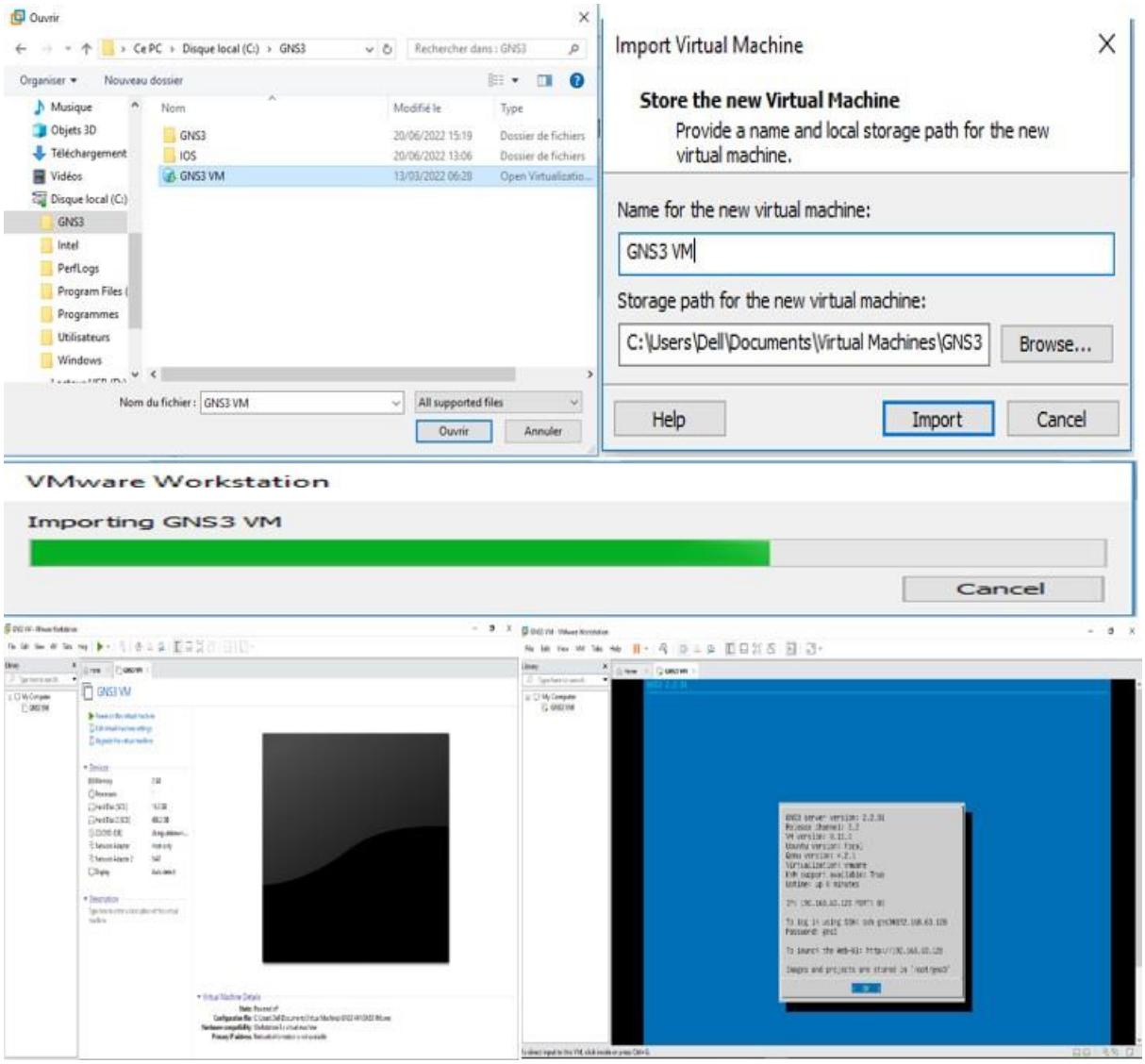

Figure III.3 – Installation de la machine virtuelle GNS3.

2.3.2 Les deux machines clientes

Pour créer une nouvelle machine virtuelle, nous allons cliquer sur file >New Virtual machine, puis suivre les étapes indiquées. Une fois la machine créée nous passerons à son installation :

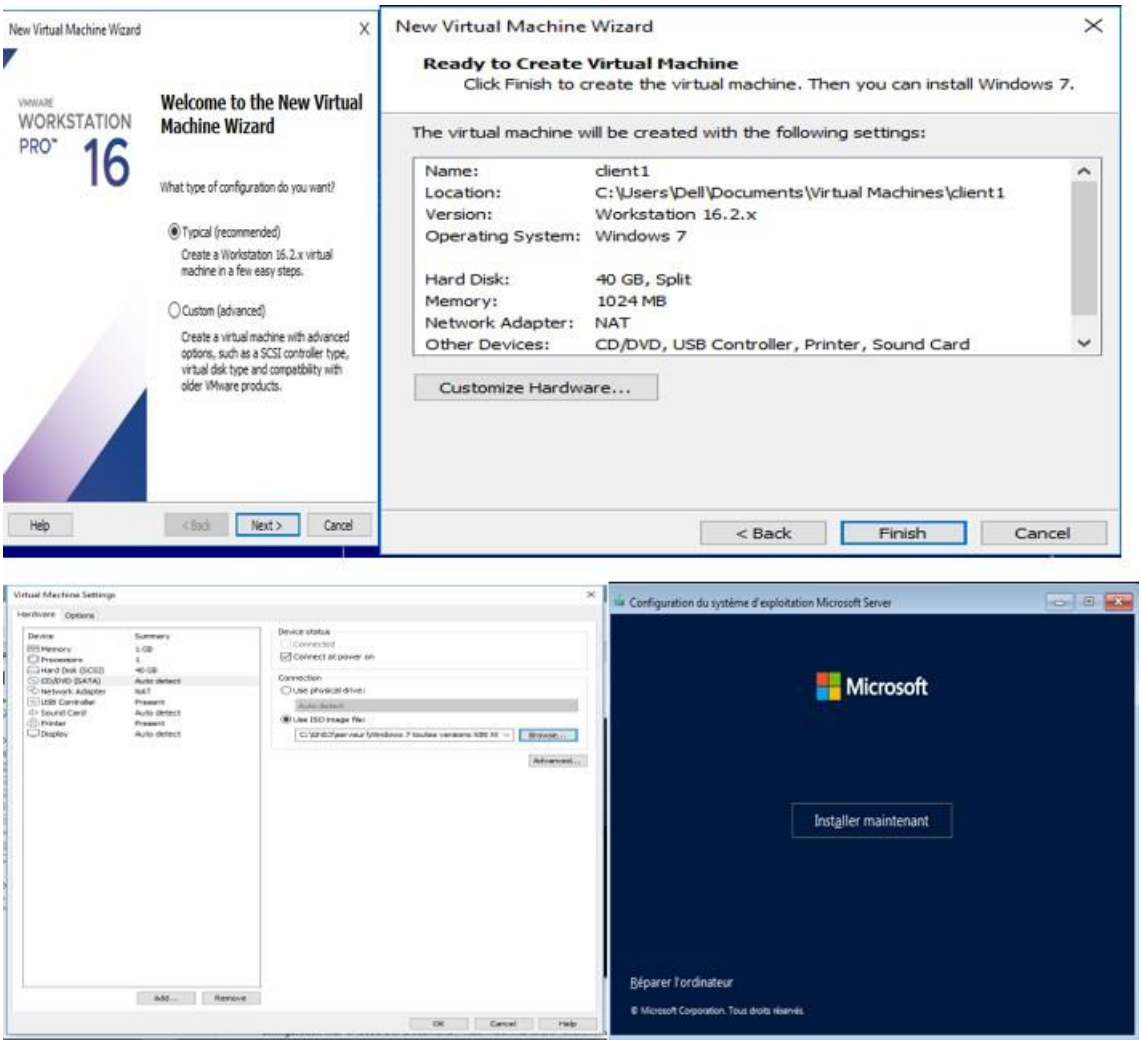

Figure III.4 – Création et installation de la machine virtuelle Client1.

Une fois la machine virtuelle client 1 installé nous aurons besoin d'une autre machine cliente (Client 2) que nous clonerons à partir de la première, et ce par une clique droite sur la fenêtre machine client1 >Manage>clone.

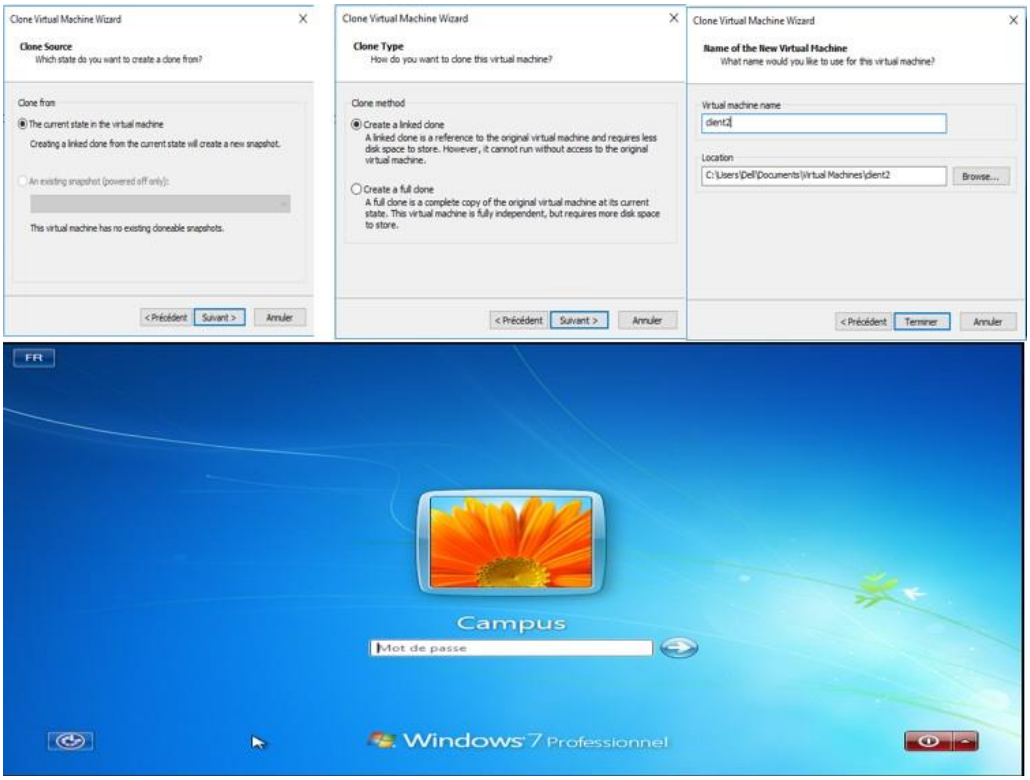

Figure III.5 – Clonage de la machine virtuelle Client2.

2.3.3 Serveur AD

Nous allons à présent créer et installer une machine virtuelle Windows server 2019 :

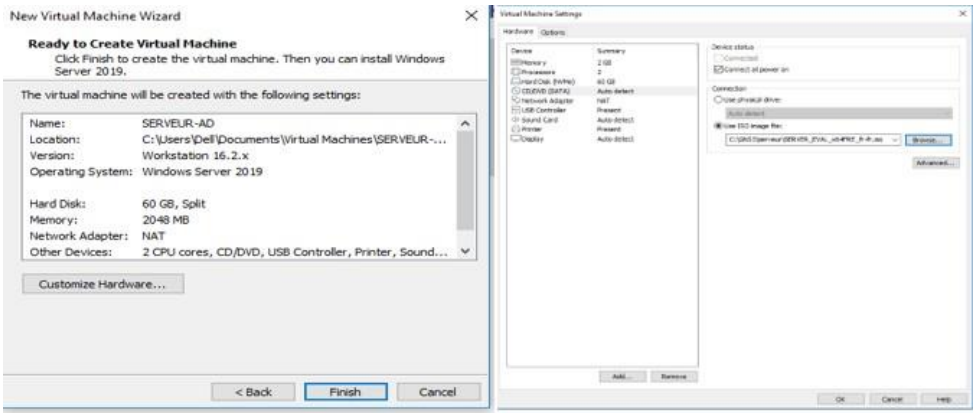

Figure III.6 – Création et installation de la machine virtuelle Windows server 2019.

2.4 Les deux Firewalls

De la même manière nous allons créer deux autres machines virtuelles destinées à représenter nos deux Firewalls et ce en important l'image IOS adéquate.

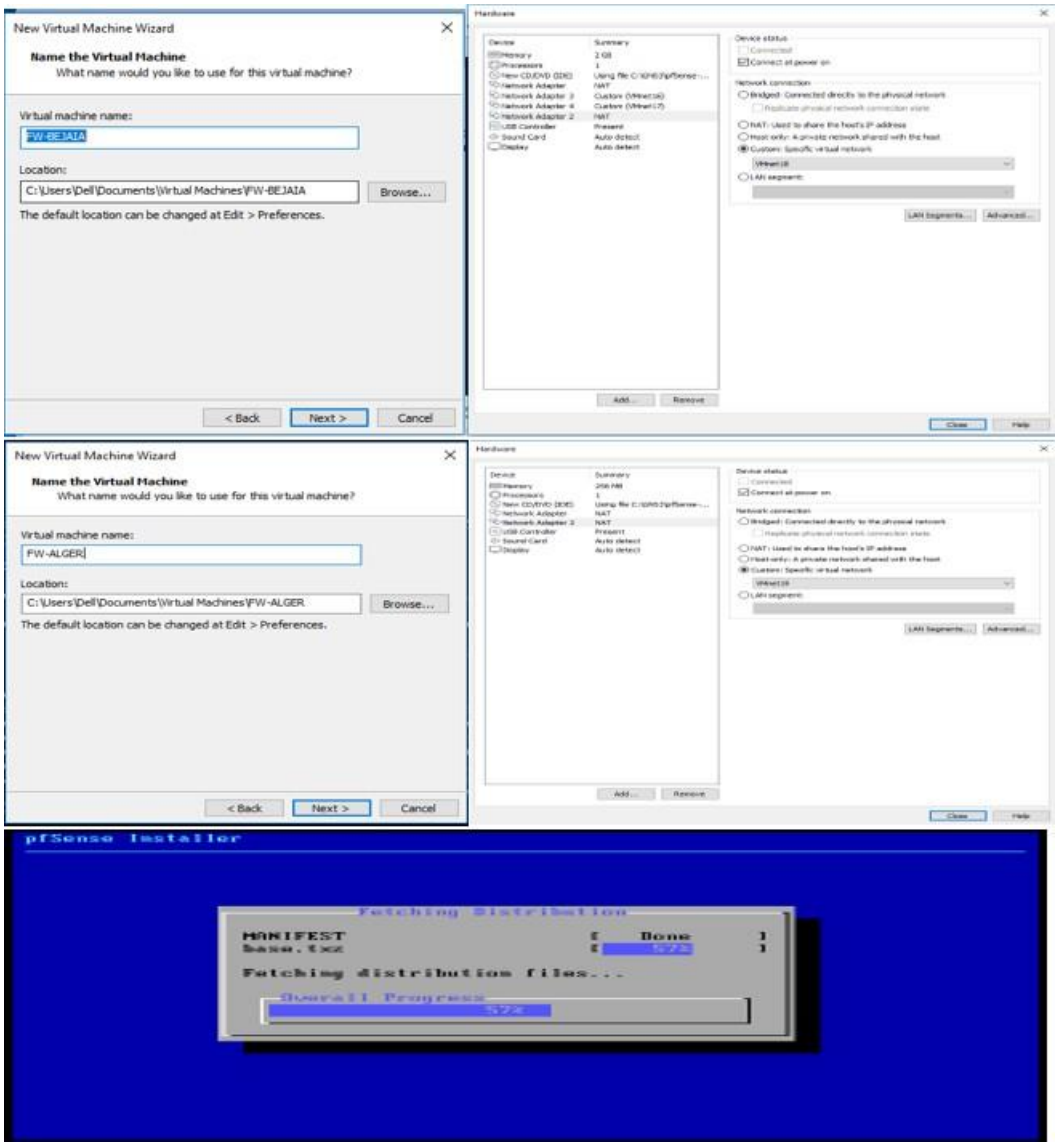

Figure III.7 – Création et installation des machines virtuelles pfsense.

3 Créations des cartes réseaux

Cartes réseaux	Nom de la carte	L'adresse IP	Masque sous réseau
VMnet10	VLAN 10	10.0.10.0	255.255.255.0
VMnet11	VLAN 20	10.0.20.0	255.255.255.0
VMnet12	VLAN 30	10.0.30.0	255.255.255.0
VMnet13	VLAN 50	10.0.50.0	255.255.255.0
VMnet16	LAN 1	192.168.1.0	255.255.255.0
VMnet17	LAN 2	192.168.2.0	255.255.255.0
VMnet18	LAN 3	192.168.3.0	255.255.255.0
VMnet19	LAN 4	192.168.4.0	255.255.255.0

TABLe III.1 – Plan de création des cartes réseaux.

4 Configuration de l'AD

4.1 Configuration de base

Nous allons entamer la configuration de base de notre Active-directory (Nom de l'ordinateur, domaine, Bureau à distance, etc).

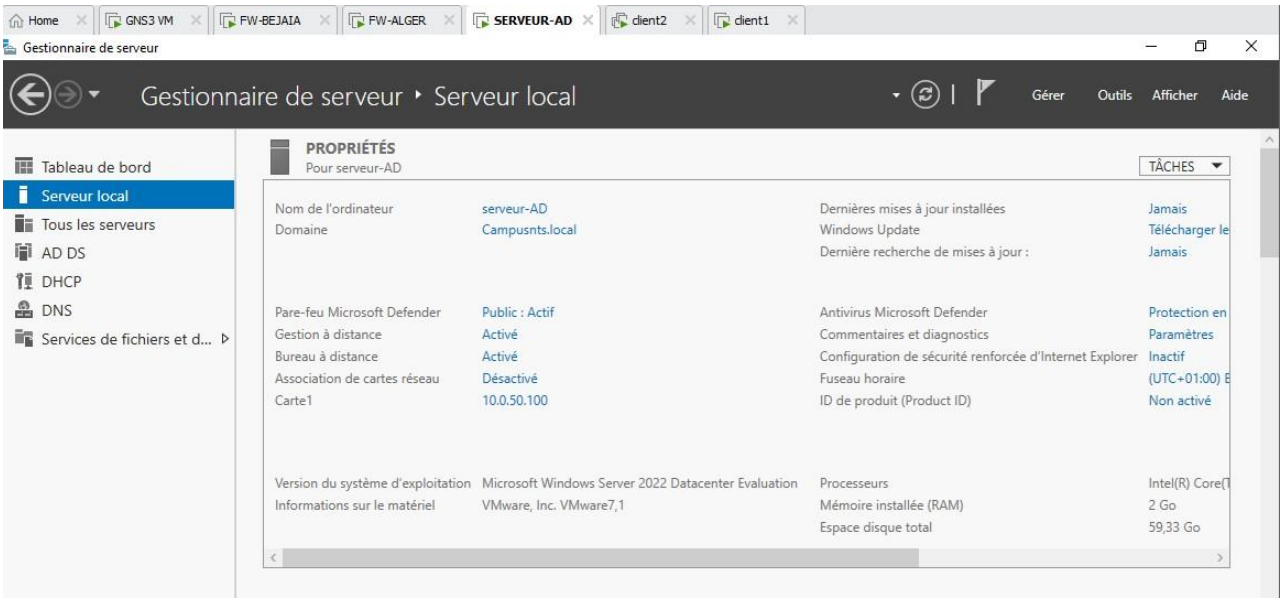

Figure III.8 – Configuration de base du serveur.

4.2 Ajouts des rôles et fonctionnalités

4.2.1 Service AD DS

Une fois cela fait, nous allons ajouter des rôles et fonctionnalités à notre serveur à commencer par les services AD DS, qui permet de stocker des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs du domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisé n'importe où sur le réseau via un processus d'ouverture de session unique.

Nous allons créer une nouvelle forêt « Campusnts.local » puis Windows nous demande de choisir le niveau fonctionnel de notre forêt, nous choisirons un niveau fonctionnel 2016, il nous propose également d'installer des fonctions supplémentaires telles que DNS, nous introduirons ensuite un mot de passe.

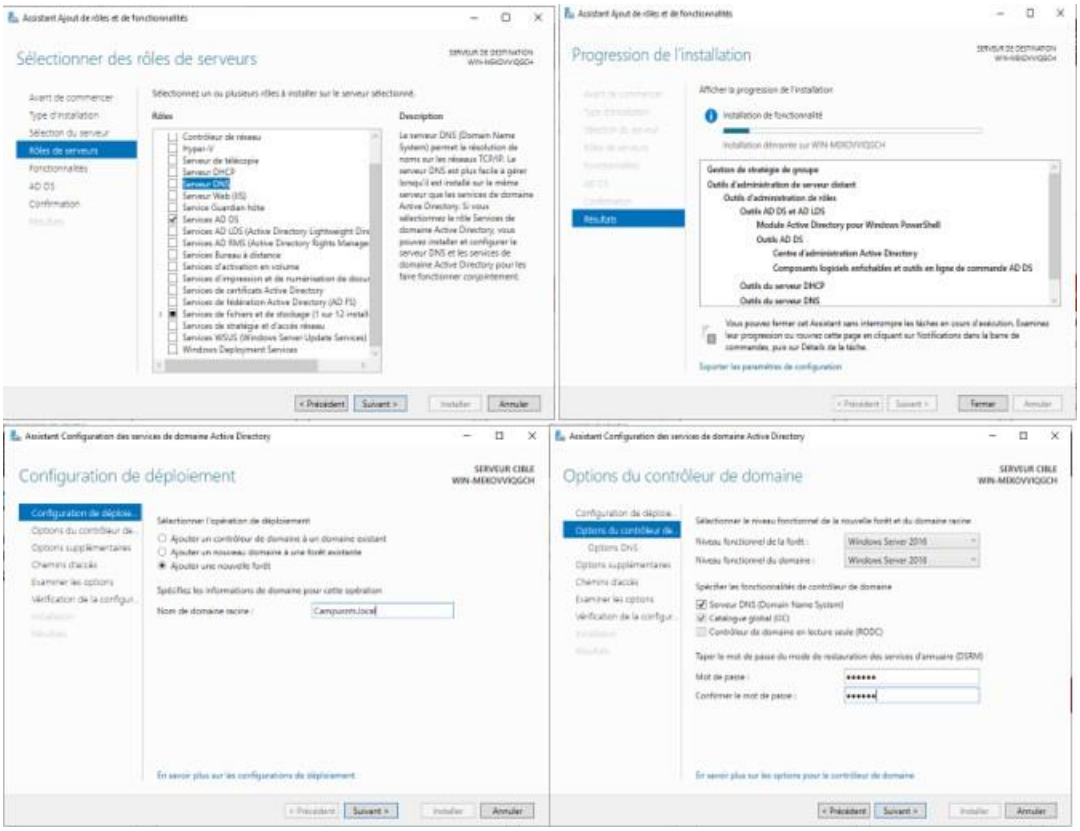

Figure III.9 – Ajout du rôle AD DS au serveur.

Maintenant nous allons créer une unité d'organisation par un clic droit sur le nom de domaine >nouveau >Unité d'organisation dont le nom est « Unité de Bejaïa ». Puis nous passons à la création des utilisateurs et des ordinateurs et des groupes de la même manière.

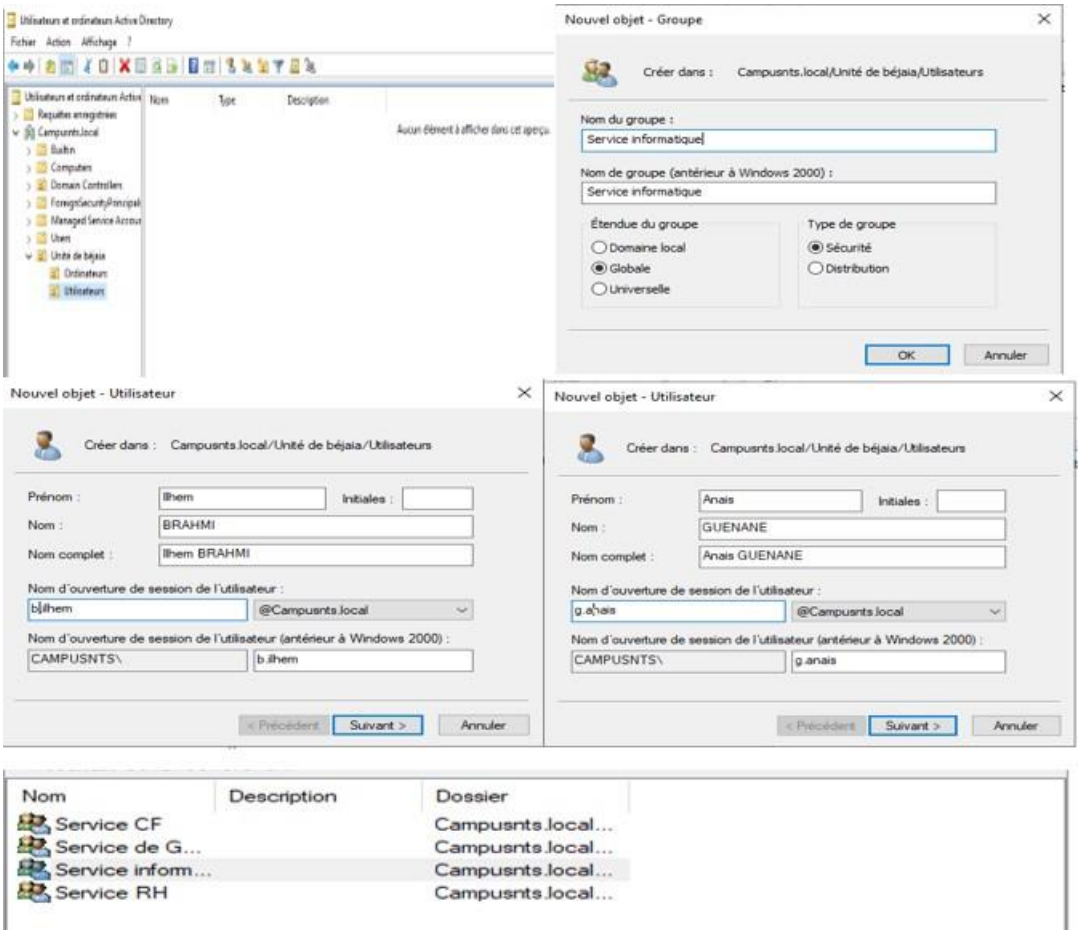

Figure III.10 – Création des groupes et utilisateur.

4.2.2 Service DHCP

Nous ajoutons un autre service à notre serveur qui est un service DHCP en suivant les étapes indiquées.

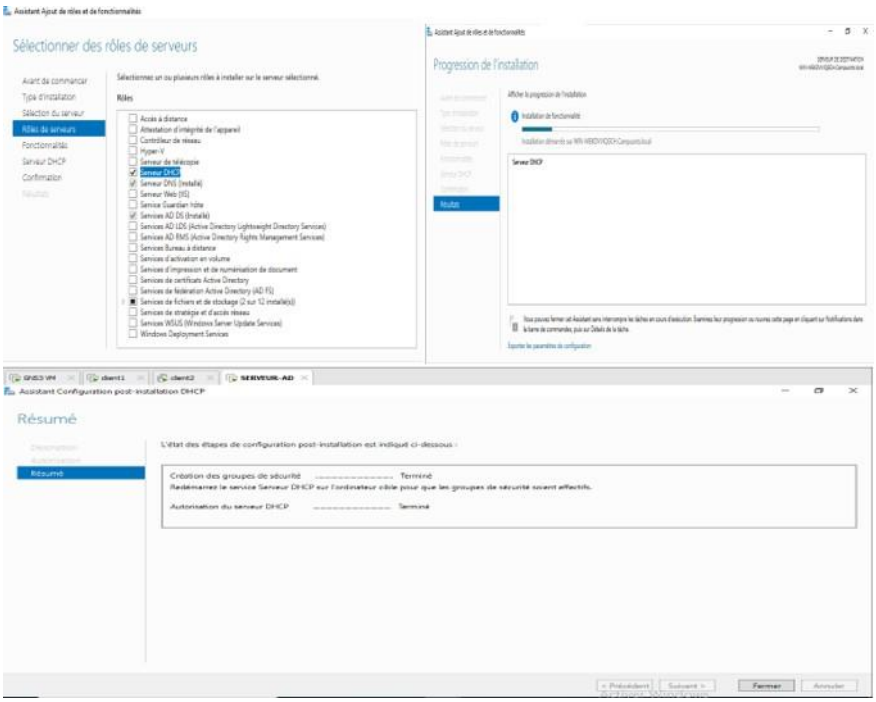

Figure III.11 – Ajout du Servie DHCP au serveur.

A présent nous allons créer les étendues pour chaque VLAN comme le montre la figure III.12 suivante :

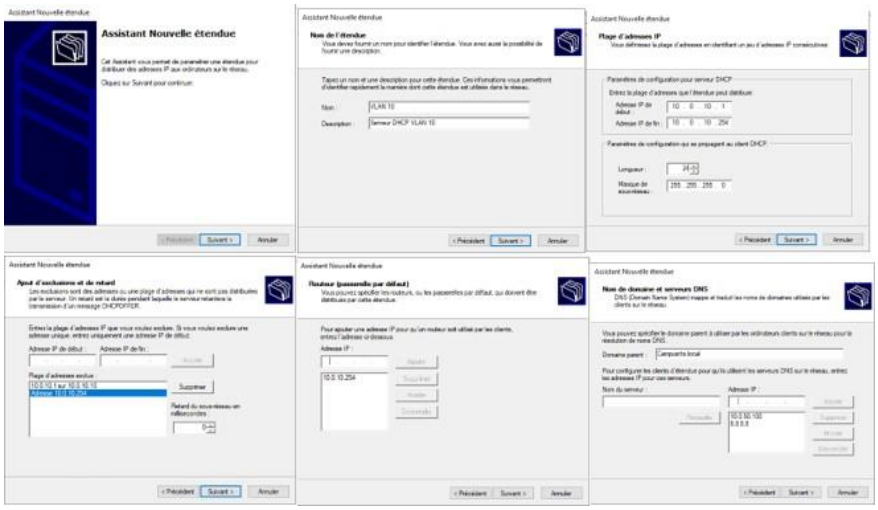

Figure III.12 – Configuration de l'étendu du VLAN 10.

La figure III.12 montre le processus de création de l'étendu pour le VLAN 10, où nous avons indiqué le nom et une description, la plage d'adresses IP ainsi que le masque, puis nous avons exclue l'adresse qui sera celle de la passerelle du sous réseau (10.0.10.254) et les dix premières adresses, c'est-à-dire la plage allant de 10.0.10.1 à 10.0.10.10 et ce pour une utilisation en statique pour des périphériques tels que les imprimantes, puis nous introduirons la passerelle et enfin l'adresse du DNS qui se trouve être celle du serveur que nous avons créé. Le processus sera le même pour ce qui est des autres VLAN restants (20,30,40).

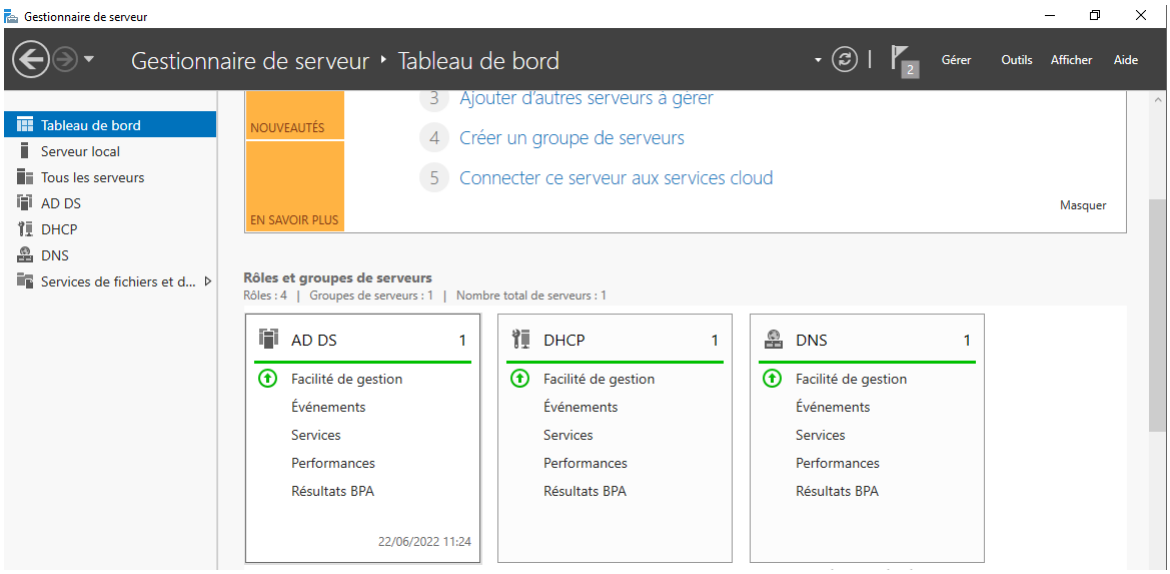

Figure III.13 – Configuration de l'étendu du VLAN 10.

5 Configuration des Firewalls

5.1 Configuration de base

Une fois l'installation des pare-feux terminer nous allons y accéder, afin d'appliquer la configuration de base, sachant que par défaut le nom d'utilisateur est « admin » et le mot de passe « pfsense », que nous modifierons par la suite :

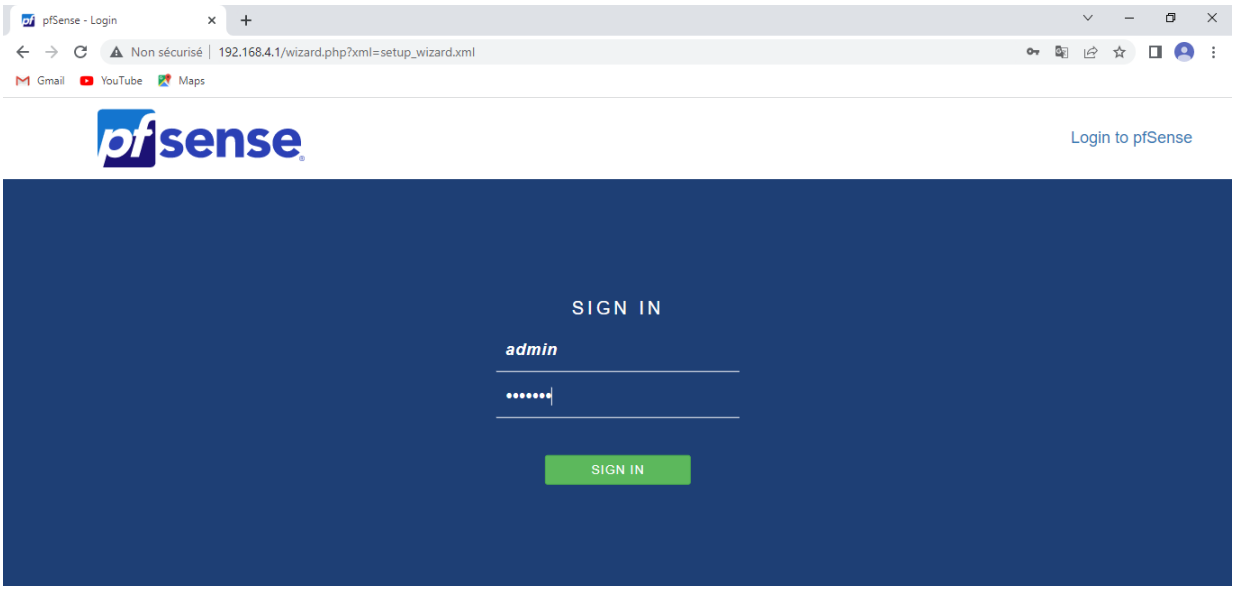

Figure III.14 – Configuration de l'étendu du VLAN 10.

Une fois la configuration de base effectuée c'est-à-dire le nom d'utilisateur, le mot de passe, le domaine et les interfaces. La page d'accueil sera comme suit :

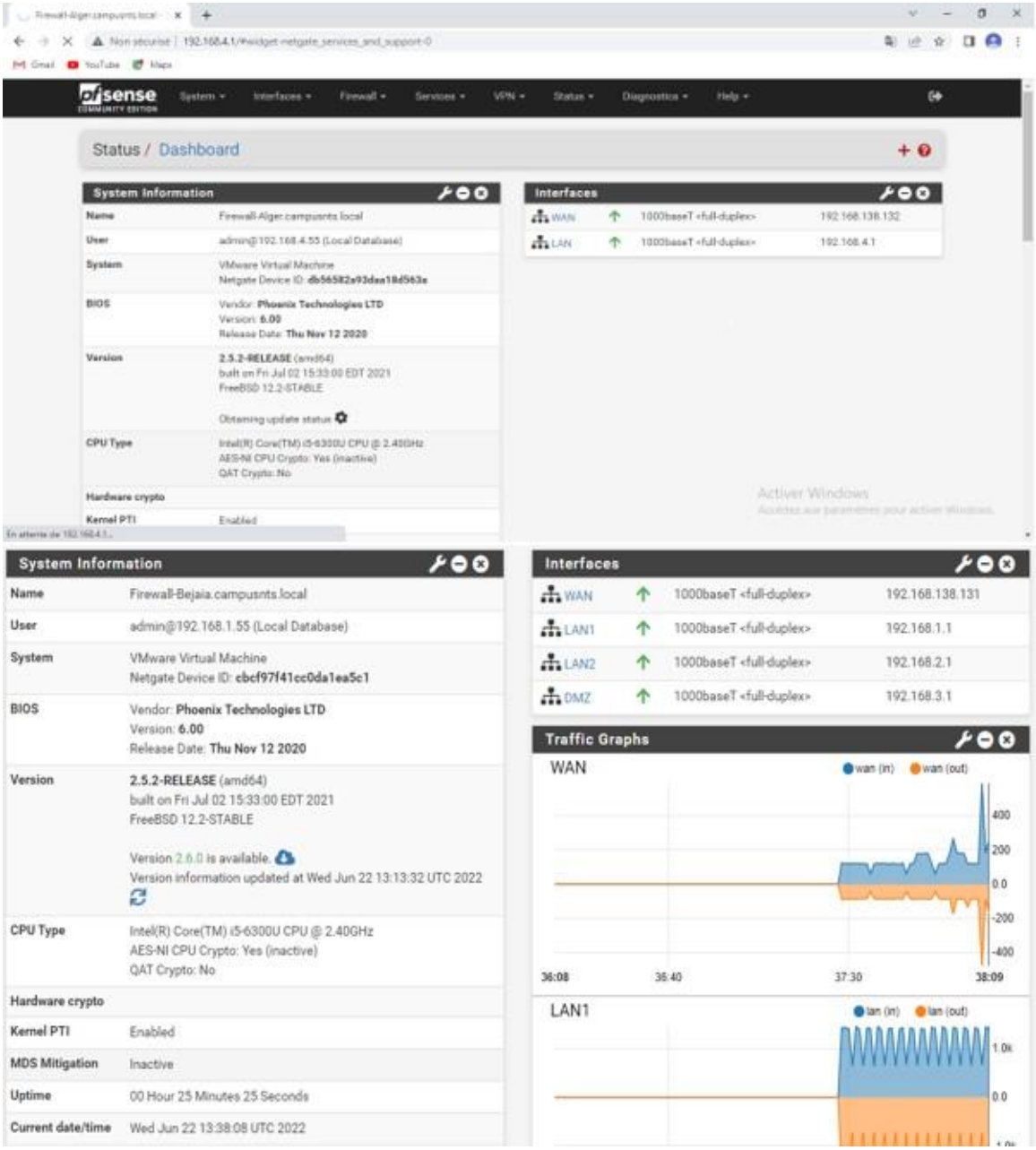

Figure III.15 – Page principale des Pare-feux de Bejaia et de Alger.

5.2 Configuration du routage

Afin que notre réseau local ait un accès vers l'extérieur nous allons effectuer un routage sur le firewall de Bejaia :

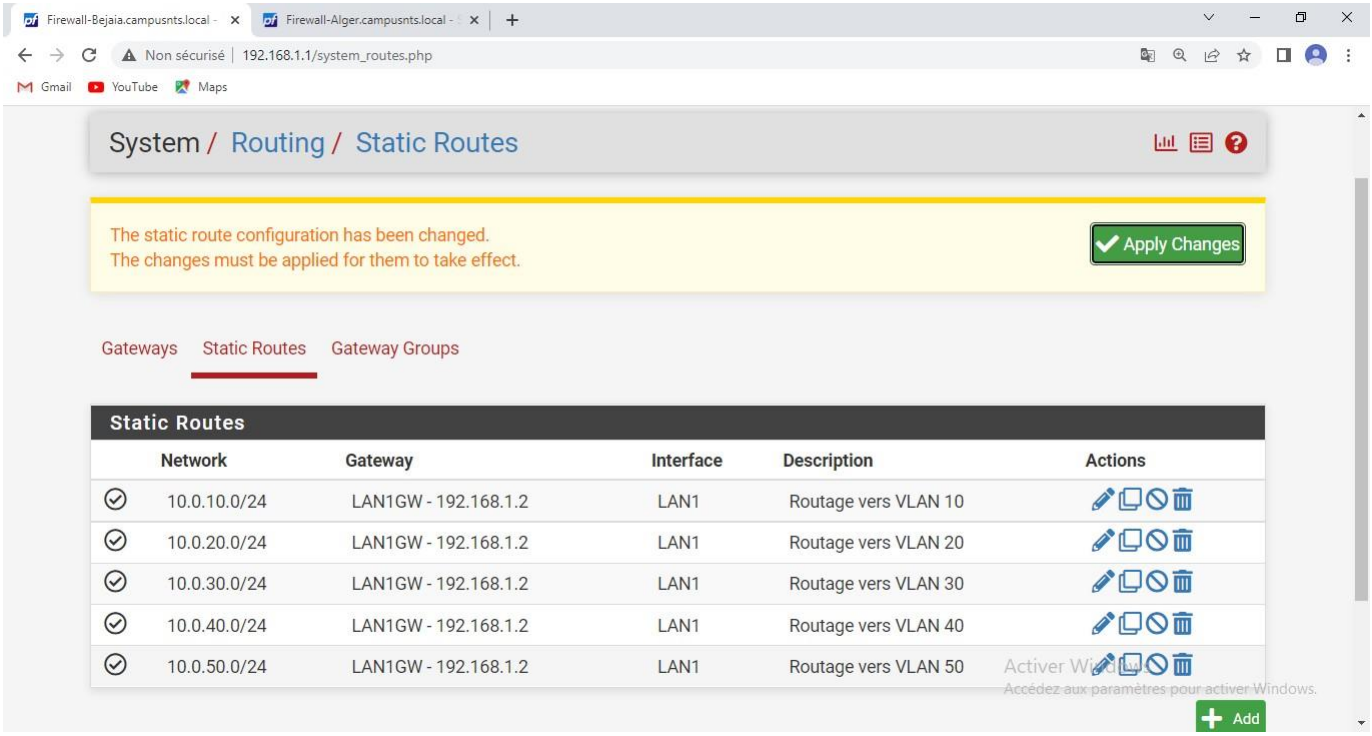

Figure III.16 – Configuration du routage statique sur le Firewall de Bejaia.

5.3 Configuration des tunnel VPN site to site (IPSec)

5.3.1 Configuration de la phase 1

Pour configurer les VPN Site to site IPSec nous allons sur VPN>IPSec et nous allons configurer la première phase qui a pour but de mettre en place un canal chiffré et sécurisé par l'intermédiaire duquel deux paires peuvent négocier la phase 2, en cliquant sur « Add P1 » et nous appliquerons les configurations indiquées ci-dessous, sachant que les mêmes paramètres doivent être appliqué sur les deux pare-feux en respectant l'adressage.

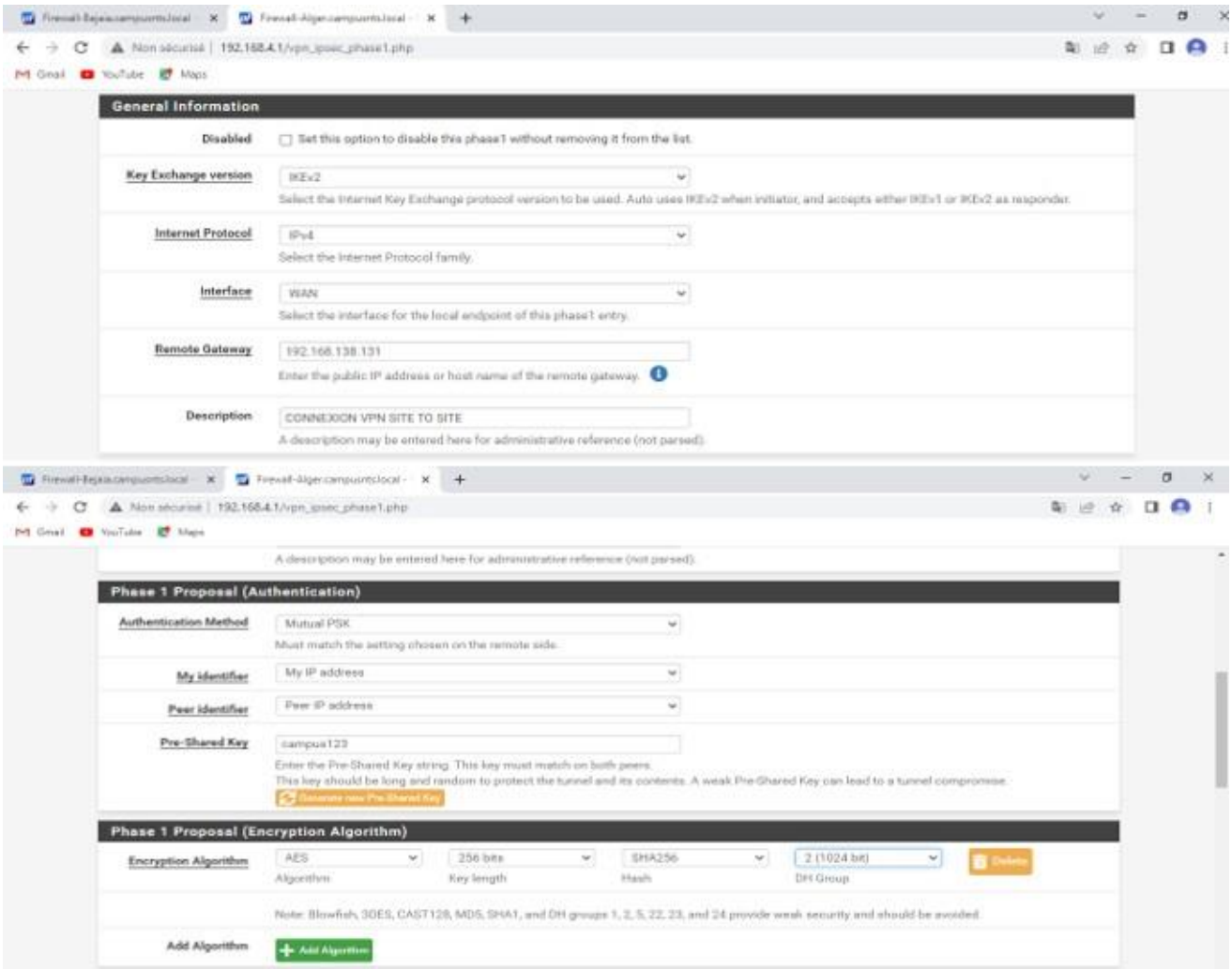

Figure III.17 – Configuration de la phase 1 du tunnel IPSec sur le firewall d'Alger.

5.3.2 Configuration de la phase 2

Nous configurerons par la suite la phase 2 dont l'objectif est que les deux paires s'accordent sur un ensemble de paramètres qui définira le type de trafic pouvant ou pas passer par le tunnel et la manière de le chiffrer.

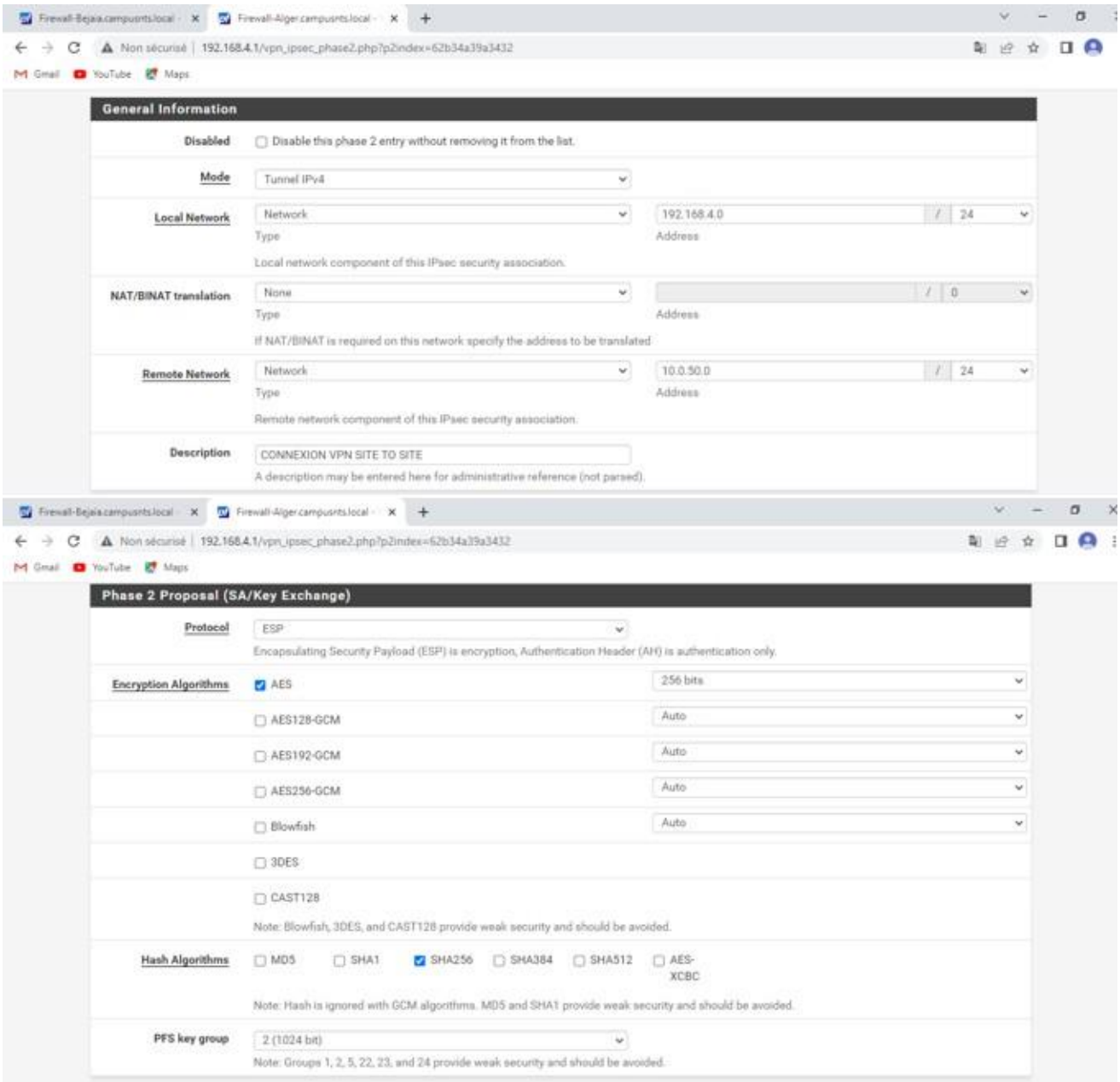

Figure III.18 – Configuration de la phase 2 du tunnel IPSec sur le firewall d'Alger.

Nous enregistrerons par la suite la configuration faite puis nous activerons le VPN et nous obtiendrons :

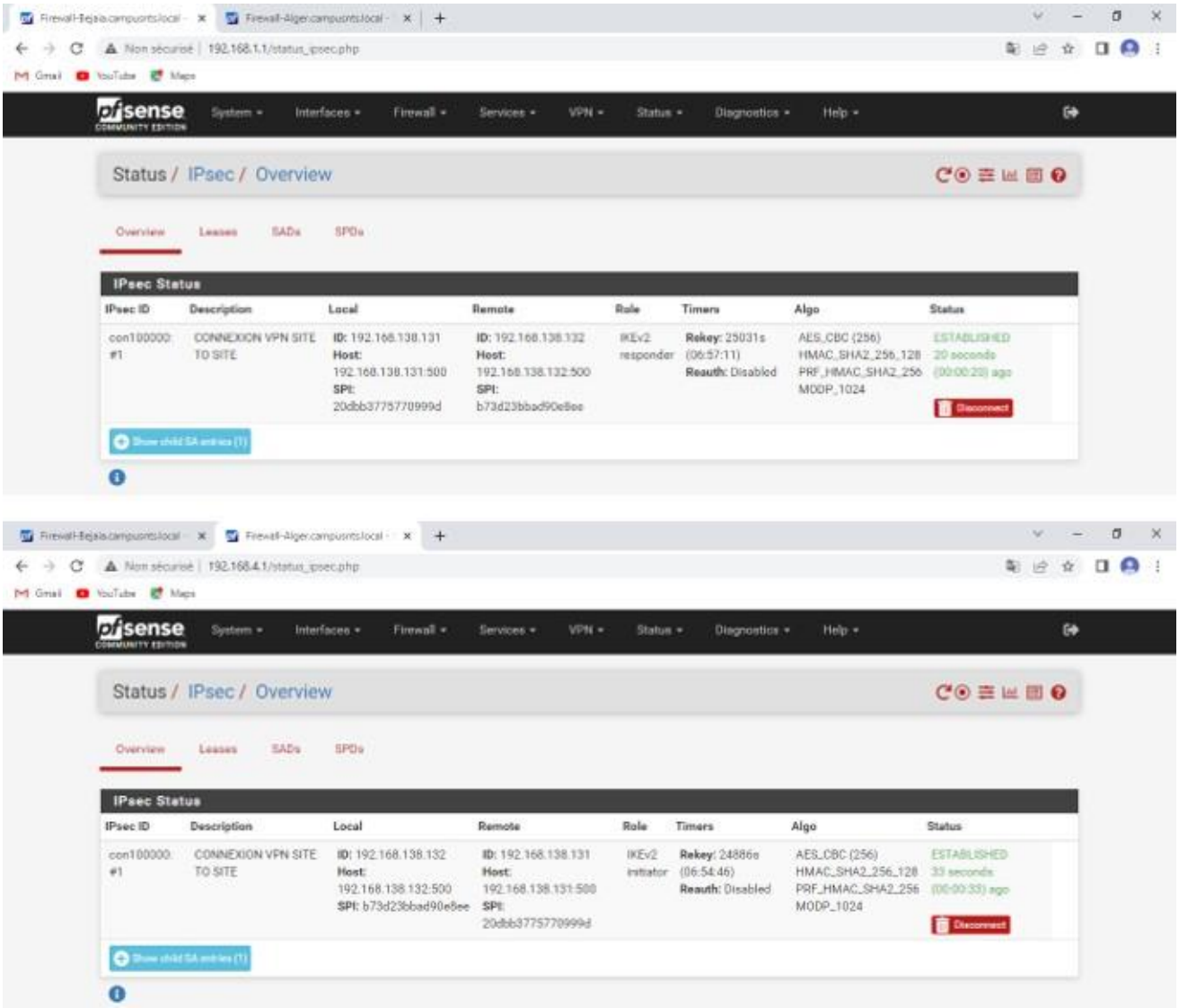

Figure III.19 – Activation du VPN sur les deux Firewalls.

6 Configuration des équipements

6.1 Plan d'adressage des VLANs

Nom du VLAN	ID du VLAN	Adresse du sous-réseau	Passerelle du sous-réseau
VLAN RH	10	10.0.10.0 /24	10.0.10.254
VLAN FC	20	10.0.20.0 /24	10.0.20.254
VLAN INFO	30	10.0.30.0 /24	10.0.30.254
VLAN VOICE	40	10.0.40.0 /24	10.0.40.254
VLAN GESTION	50	10.0.50.0 /24	10.0.50.254
VLAN NATIVE	99	/	/

TABLe III.2 – Plan d'adressage des VLANs.

6.2 Plan d'adressage des PVLANs

Nom	ID du PVLAN	Adressage	Passerelle
Serveur 1	101	192.168.3.10	192.168.3.1
Serveur 2	101	192.168.3.11	192.168.3.1
Serveur 3	102	192.168.3.12	192.168.3.1
Primary	100	/	/

TABLe III.3 – Plan d'adressage du Private VLAN.

6.3 L'encapsulation dot1q

Nom du routeur	Interface	Adressage	Passerelle
R1	Ethernet 0/1.10	10.0.10.1	10.0.10.254
	Ethernet 0/1.20	10.0.20.1	10.0.20.254
	Ethernet 0/1.30	10.0.300.1	10.0.30.254
	Ethernet 0/1.40	10.0.400.1	10.0.40.254
	Ethernet 0/1.50	10.0.500.1	10.0.50.254
R2	Ethernet 0/1.10	10.0.10.2	10.0.10.254
	Ethernet 0/1.20	10.0.20.2	10.0.20.254
	Ethernet 0/1.30	10.0.30.2	10.0.30.254
	Ethernet 0/1.40	10.0.40.2	10.0.40.254
	Ethernet 0/1.50	10.0.50.2	10.0.50.254

TABLe III.4 – Plan d'adressage du Private VLAN.

6.4 Plan d'adressage des Private VLAN

Equipement	Interface	Adressage
FW-BEJAIA	DMZ	192.168.3.1
	LAN 1	192.168.1.1
	LAN 2	192.168.2.1
	WAN	192.168.138.131
FW-ALGER	LAN 4	192.168.4.1
	WAN	192.168.138.132
R1	Ethernet 0/0	192.168.1.2
	Ethernet 0/1	Encapsulation dot1q
R2	Ethernet 0/0	192.168.2.2
	Ethernet 0/1	Encapsulation dot1q
Serveur 1	/	192.168.3.10
Serveur 2	/	192.168.3.11
Serveur 3	/	192.168.3.12
Serveur-AD	/	10.0.50.100

TABLe III.5 – Plan d'adressage du Private VLAN.

6.5 Configurations des commutateurs

Nous commencerons par la configuration des commutateurs qui permettra l'interconnexion des différents segments.

6.5.1 Configuration des interfaces trunk

Pour cela nous avons utilisé la configuration suivante sur les deux switches distribution (SWD1, SWD2) ainsi que les switches Access (SWA1, SWA2, SWA3, SWA4) :

```
SWD2(config)#interface range ethernet 0/0-3
SWD2(config-if-range)#switchport trunk encapsulation dot1q
SWD2(config-if-range)#switchport mode trunk
SWD2(config-if-range)#exit
SWD2(config)#interface range ethernet 1/0-3
SWD2(config-if-range)#switchport trunk encapsulation dot1q
SWD2(config-if-range)#switchport mode trunk
SWD2(config-if-range)#exit
SWD2(config)#interface ethernet 3/3
SWD2(config-if)#switchport trunk encapsulation dot1q
SWD2(config-if)#switchport mode trunk
SWD2(config-if)#end
```

Figure III.20 – Configuration du Trunk sur SWD1.

```
SWA1(config)#interface range ethernet 0/0-1
SWA1(config-if-range)#switchport trunk encapsulation dot1q
SWA1(config-if-range)#switchport mode trunk
SWA1(config-if-range)#end
```

Figure III.21 – Configuration du trunk sur SWA1.

6.5.2 Configuration du VTP

Afin d'ajouter, de renommer ou de supprimer un ou plusieurs VLANs, où un seul commutateur propagera la nouvelle configuration aux autres commutateurs du réseau, nous allons configurer le VTP Serveur sur les switches distribution et le VTP Client sur les switches Access :

```
SWD1(config)#vtp domain CampusNTS.vtp
Changing VTP domain name from NULL to CampusNTS.vtp
SWD1(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD1(config)#vtp domain CampusNTS.vtp
Domain name already set to CampusNTS.vtp.
SWD1(config)#vtp password campus123
Setting device VTP password to campus123
SWD1(config)#vtp version 2
SWD1(config)#vtp pruning
Pruning switched on
SWD1(config)#exit
```

Figure III.22 – Configuration du domaine VTP sur SWD1.

```
SWD2(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD2(config)#vtp domain CampusNTS.vtp
Changing VTP domain name from NULL to CampusNTS.vtp
SWD2(config)#vtp password campus123
Setting device VTP password to campus123
SWD2(config)#vtp version 2
SWD2(config)#end
SWD2#wr
```

Figure III.23 – Configuration du domaine VTP sur SWD2.

```
SWA1(config)#vtp mode client                SWA2(config)#vtp mode client
Device mode already VTP Client for VLANS.   Setting device to VTP Client mode for VLANS.
SWA1(config)#vtp domain CampusNTS.vtp       SWA2(config)#vtp domain CampusNTS.vtp
Domain name already set to CampusNTS.vtp.   Changing VTP domain name from NULL to CampusNTS.vtp
SWA1(config)#vtp password campus123         SWA2(config)#vtp password campus123
Password already set to campus123           Setting device VTP password to campus123
SWA1(config)#vtp version 2                  SWA2(config)#vtp version 2

SWA3(config)#vtp mode client                SWA4(config)#vtp mode client
Setting device to VTP Client mode for VLANS.  Setting device to VTP Client mode for VLANS.
SWA3(config)#vtp domain CampusNTS.vtp       SWA4(config)#vtp domain CampusNTS.vtp
Changing VTP domain name from NULL to CampusNTS.vtp Changing VTP domain name from NULL to CampusNTS.vtp
SWA3(config)#vtp password campus123         SWA4(config)#vtp password campus123
Setting device VTP password to campus123    Setting device VTP password to campus123
SWA3(config)#vtp version 2                  SWA4(config)#vtp version 2
```

Figure III.24 – Configuration du domaine VTP sur les SWA.

```
SWA1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : CampusNTS.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 6-21-22 09:43:56

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 2
```

Figure III.25 – Vérification du VTP sur SWA1.

6.5.3 Créations des VLANs

Nous allons à présents créer les VLANs à savoir :

```
SWD1(config)#vlan 10
SWD1(config-vlan)#name RH
SWD1(config-vlan)#vlan 20
SWD1(config-vlan)#name FC
SWD1(config-vlan)#vlan 30
SWD1(config-vlan)#name INFO
SWD1(config-vlan)#vlan 40
SWD1(config-vlan)#name VOICE
SWD1(config-vlan)#vlan 50
SWD1(config-vlan)#name GESTION
SWD1(config-vlan)#vlan 99
SWD1(config-vlan)#name NATIVE
SWD1(config-vlan)#end
SWD1#
SWD1#wr
```

Figure III.26 – Création des VLANs sur le SDW1.

6.5.4 Affectations des ports mode Access

```
SWA1(config)#interface ethernet 0/2
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport access vlan 50
SWA1(config-if)#switchport voicE vlan 40
SWA1(config-if)#end
```

```
SWA2(config)#interface ethernet 0/2
SWA2(config-if)#switchport mode access
SWA2(config-if)#switchport access vlan 30
SWA2(config-if)#switchport voice vlan 40
SWA2(config-if)#end
```

```
SWA3(config)#interface ethernet 0/2
SWA3(config-if)#switchport mode acces
SWA3(config-if)#switchport acces vlan 20
SWA3(config-if)#switchport voice vlan 40
SWA3(config-if)#end
```

```
SWA4(config)#interface ethernet 0/2
SWA4(config-if)#switchport mode access
SWA4(config-if)#switchport access vlan 10
SWA4(config-if)#switchport voice vlan 40
SWA4(config-if)#end
SWA4#wr
```

Figure III.27 – Configuration des ports mode Access.

6.5.5 Configuration du VLAN native

Nous allons maintenant modifier le VLAN native qui est par défaut le VLAN1, par le VLAN 99 qu'on a précédemment créé, et ce sur tous les switches.

```
SWD1(config)#interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 3/0-3
SWD1(config-if-range)#switchport trunk native vlan 99
SWD1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,99
SWD1(config-if-range)#end

SWD2(config)#interface range ethernet 0/0-3, ethernet 1/0-3, ethernet 3/0-3
SWD2(config-if-range)#switchport trunk native vlan 99
SWD2(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,99
SWD2(config-if-range)#END
```

Figure III.28 – Configuration du VLAN native sur les switches Distributions.

```
SWA1(config)#interface range ethernet 0/0-1
SWA1(config-if-range)#switchport trunk native vlan 99
SWA1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,99
SWA1(config-if-range)#end

SWA2(config)#interface range ethernet 0/0-1
SWA2(config-if-range)#switchport trunk native vlan 99
SWA2(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60,99
SWA2(config-if-range)#END

SWA3(config-if-range)#interface range ethernet 0/0-1
SWA3(config-if-range)#switchport trunk native vlan 99
SWA3(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,99
SWA3(config-if-range)#end

SWA4(config)#interface range ethernet 0/0-1
SWA4(config-if-range)#switchport trunk native vlan 99
SWA4(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,99
SWA4(config-if-range)#end
```

Figure III.29 – Configuration du VLAN native sur les switches Access.

```
SWA1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      99
Et0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Et0/0       10,20,30,40,50,99
Et0/1       10,20,30,40,50,99

Port        Vlans allowed and active in management domain
Et0/0       10,20,30,40,50,99
Et0/1       10,20,30,40,50,99

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       10,20,30,40,50,99
Et0/1       10,20,30,40,50,99
```

Figure III.30 – Vérification des configurations sur SWA1.

6.5.6 Configuration des ports EtherChannel

Pour cela nous allons assigner tous les ports qui composeront notre lien logique entre les deux switches distribution au même Channel-Groupe, en configurant EtherChannel en mode active sur SWD1 et en mode passive sur SWD2.

```
SWD1(config)#interface range ethernet 1/0-3
SWD1(config-if-range)#channel-group 1 mode active
SWD1(config-if-range)#exit
SWD1(config)#interface port-channel 1
SWD1(config-if)#switchport trunk native vlan 99
SWD1(config-if)#switchport trunk allowed vlan 10,20,30,40,50,99
SWD1(config-if)#end

SWD2(config)#interface range ethernet 1/0-3
SWD2(config-if-range)#channel-group 1 mode passive
SWD2(config-if-range)#exit
SWD2(config)#interface port-channel 1
SWD2(config-if)#switchport trunk native vlan 99
SWD2(config-if)#switchport trunk allowed vlan 10,20,30,40,50,99
SWD2(config-if)#END
```

Figure III.31 – Configuration des ports EtherChannel.

```
SWD2#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      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

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

Figure III.32 – Vérification de la configuration de l'EtherChannel.

6.5.7 Configuration des Private-VLAN

Nous passerons maintenant à la configuration de la DMZ, dans laquelle nous créerons différents VLANs.

Tout d'abord nous allons commencer par configurer le VTP sur le switch DMZ en mode transparent pour qu'il ne participe pas au processus VTP.

```
DMZ(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
```

Figure III.33 – Configuration du VTP sur le switch DMZ.

Nous passerons à la création des VLANs, à commencer par le VLAN privé de type Community, où les équipements de ce VLAN sont capables de communiquer. Puis le VLAN privé de type Isolated qui contrairement au VLAN Community, les équipements de ce même VLAN ne communiqueront pas entre eux. Enfin nous terminerons par créer le VLAN privé de type Primay qui lui englobera les deux autres VLANs et pouvant communiquer avec les deux précédents.

```
DMZ(config)#vlan 101
DMZ(config-vlan)#private-vlan community
DMZ(config-vlan)#exit
DMZ(config)#vlan 102
DMZ(config-vlan)#private-vlan isolated
DMZ(config-vlan)#exit
DMZ(config)#vlan 100
DMZ(config-vlan)#private-vlan primary
DMZ(config-vlan)#private-vlan association 101,102
DMZ(config-vlan)#exit
```

Figure III.34 – Création des VLANs privés.

Après cela nous allons associer chaque port au VLAN approprié.

```
DMZ(config)#interface ethernet 3/3
DMZ(config-if)#switchport mode private-vlan promiscuous
DMZ(config-if)#switchport private-vlan mapping 100 101,102
DMZ(config-if)#EXIT

DMZ(config)#interface range ethernet 0/1-2
DMZ(config-if-range)#switchport mode private-vlan host
DMZ(config-if-range)#switchport private-vlan host-association 100 101
DMZ(config-if-range)#EXIT

DMZ(config)#interface ethernet 0/3
DMZ(config-if)#switchport mode private-vlan host
DMZ(config-if)#switchport private-vlan host-association 100 102
DMZ(config-if)#exit
DMZ(config)#
```

Figure III.35 – Association des ports au VLANs.

6.6 Configuration des routeurs

6.6.1 Routage Inter-VLAN

Nous allons maintenant effectuer un routage inter-VLAN afin de router les paquets des différents VLANs et ce en utilisant le principe du routeur-on-stick a fin de créé plusieurs sous interfaces, chacune d'elle subira une encapsulation dot1Q qui précisera l'ID du VLAN, une adresse et un masque sous réseau lui sera attribué ainsi qu'un DHCP Relay qui n'est autre que notre serveur DHCP se trouvant sur le VLAN 50.

```
R1(config)#interface ethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 10.0.10.1 255.255.255.0
R1(config-subif)#ip helper-address 10.0.50.100
R1(config-subif)#exit
R1(config)#interface ethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 10.0.20.1 255.255.255.0
R1(config-subif)#ip helper-address 10.0.50.100
R1(config-subif)#exit
```

```
R1(config)#interface ethernet 0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 10.0.30.1 255.255.255.0
R1(config-subif)#ip helper-address 10.0.50.100
R1(config-subif)#EXIT
R1(config)#interface ethernet 0/1.40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 10.0.40.1 255.255.255.0
R1(config-subif)#ip helper-address 10.0.50.100
R1(config-subif)#EXIT
R1(config)#interface ethernet 0/1.50
R1(config-subif)#encapsulation dot1q 50
R1(config-subif)#ip address 10.0.50.1 255.255.255.0
R1(config-subif)#ip helper-address 10.0.50.100
R1(config-subif)#EXIT
```

Figure III.36 – Configuration du routeur-On-stick sur R1.

```
R2(config-subif)#interface ethernet 0/1.10
R2(config-subif)#encapsulation dot1q 10
R2(config-subif)#Ip address 10.0.10.2 255.255.255.0
R2(config-subif)#ip helper-address 10.0.50.100
R2(config-subif)#exit
R2(config)#interface ethernet 0/1.20
R2(config-subif)#encapsulation dot1q 20
R2(config-subif)#Ip address 10.0.20.2 255.255.255.0
R2(config-subif)#ip helper-address 10.0.50.100
R2(config-subif)#exit
R2(config)#interface ethernet 0/1.30
R2(config-subif)#encapsulation dot1q 30
R2(config-subif)#Ip address 10.0.30.2 255.255.255.0
R2(config-subif)#ip helper-address 10.0.50.100
R2(config-subif)#exit
R2(config-subif)#interface ethernet 0/1.40
R2(config-subif)#encapsulation dot1q 40
R2(config-subif)#Ip address 10.0.40.2 255.255.255.0
R2(config-subif)#ip helper-address 10.0.50.100
R2(config-subif)#exit
R2(config)#interface ethernet 0/1.50
R2(config-subif)#encapsulation dot1q 50
R2(config-subif)#Ip address 10.0.50.2 255.255.255.0
R2(config-subif)#ip helper-address 10.0.50.100
R2(config-subif)#exit
```

Figure III.37 – Configuration du Routeur-On-Stick sur R2.

6.6.2 Configuration des routes statiques

Afin de router le trafic de notre réseau local vers l'extérieur nous allons effectuer un routage statique, et ce en créant une route du n'importe quel réseau (0.0.0.0) vers n'importe quel réseau (0.0.0.0) via la passerelle de sortie.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R2(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Figure III.38 – Configuration des routes statiques sur R1 et R2.

6.6.3 Configuration du protocole HSRP

Nous allons finaliser la configuration de nos routeurs par la mise en place du protocole HSRP, où nous allons définir sur les deux routeurs une adresse IP qui sera celle du routeur virtuel. R1 sera en mode active tandis que R2 sera en mode standby, c'est-à-dire que R1 assurera le rôle de passerelle par défaut et basculera vers R2 uniquement en cas de panne du routeur actif.

```
R1(config)#interface ethernet 0/1.10
R1(config-subif)#standby version 2
R1(config-subif)#standby 10 ip 10.0.10.254
R1(config-subif)#standby 10 priorit
*Jun 27 11:17:10.180: %HSRP-5-STATECHANGE:
R1(config-subif)#standby 10 priority 110
R1(config-subif)#standby 10 preempt
R1(config-subif)#exit
R1(config)#interface ethernet 0/1.20
R1(config-subif)#standby version 2
R1(config-subif)#standby 20 ip 10.0.20.254
R1(config-subif)#standby 20 priority 110
R1(config-subif)#standby 20 preempt
*Jun 27 11:19:32.147: %HSRP-5-STATECHANGE:
R1(config-subif)#standby 20 preempt
R1(config-subif)#exit
R1(config)#interface ethernet 0/1.30
R1(config-subif)#standby version 2
R1(config-subif)#standby 30 ip 10.0.30.254
R1(config-subif)#standby 30 priority 110
R1(config-subif)#standby 30 preempt
R1(config-subif)#exit
```

```
R1(config)#interface ethernet 0/1.40
R1(config-subif)#standby version 2
R1(config-subif)#standby 40 ip 10.0.30.254
*Jun 27 11:20:39.231: %HSRP-5-STATECHANGE:
R1(config-subif)#standby 40 ip 10.0.40.254
R1(config-subif)#standby 40 priority 110
R1(config-subif)#standby 40 preempt
R1(config-subif)#exit
R1(config)#standby 40 priority 110
*Jun 27 11:21:04.257: %HSRP-5-STATECHANGE:
R1(config)#interface ethernet 0/1.50
R1(config-subif)#standby version 2
R1(config-subif)#standby 50 ip 10.0.50.254
R1(config-subif)#standby 50 priority 110
R1(config-subif)#standby 50 preempt
R1(config-subif)#exit
```

Figure III.39 – Configuration du HSRP sur R1.

```
R2(config-subif)#interface ethernet 0/1.10
R2(config-subif)#standby version 2
R2(config-subif)#standby 10 ip 10.0.10.254
R2(config-subif)#standby 10 priority 100
R2(config-subif)#exit
R2(config)#interface ethernet 0/1.20
R2(config-subif)#standby version 2
R2(config-subif)#standby 20 ip 10.0.20.254
R2(config-subif)#standby 20 priority 100
R2(config-subif)#exit
R2(config)#interface ethernet 0/1.30
R2(config-subif)#standby version 2
R2(config-subif)#standby 30 ip 10.0.30.254
R2(config-subif)#standby 30 priority 100
R2(config-subif)#exit
```

```
R2(config-subif)#interface ethernet 0/1.40
R2(config-subif)#standby version 2
R2(config-subif)#standby 40 ip 10.0.40.254
R2(config-subif)#standby 40 priority 100
R2(config-subif)#exit
R2(config)#interface ethernet 0/1.50
R2(config-subif)#standby version 2
R2(config-subif)#standby 50 ip 10.0.50.254
R2(config-subif)#standby 50 priority 100
R2(config-subif)#exit
```

Figure III.40 – Configuration du HSRP sur R2.

7 Tests

7.1 Test sur le serveur

Le premier test que nous effectuerons sera sur le serveur en vérifiant son adresse et sa passerelle par défaut par le biais de la commande « ipconfig » :

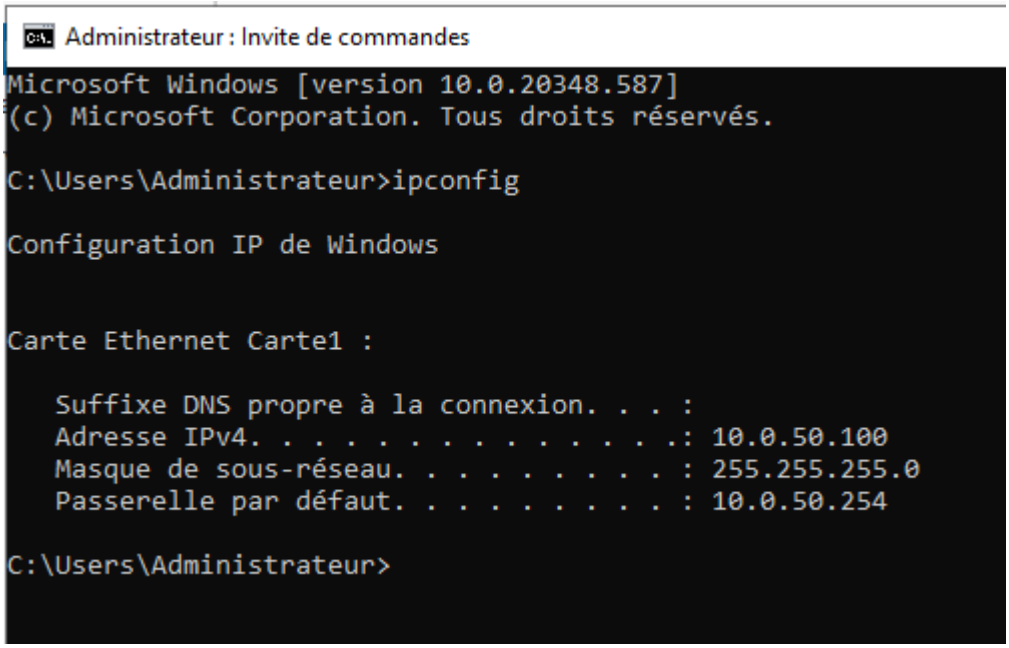

Figure III.41 – Configuration réussite sur le serveur.

Toujours sur le serveur nous allons tester sa passerelle par defaut par un ping :

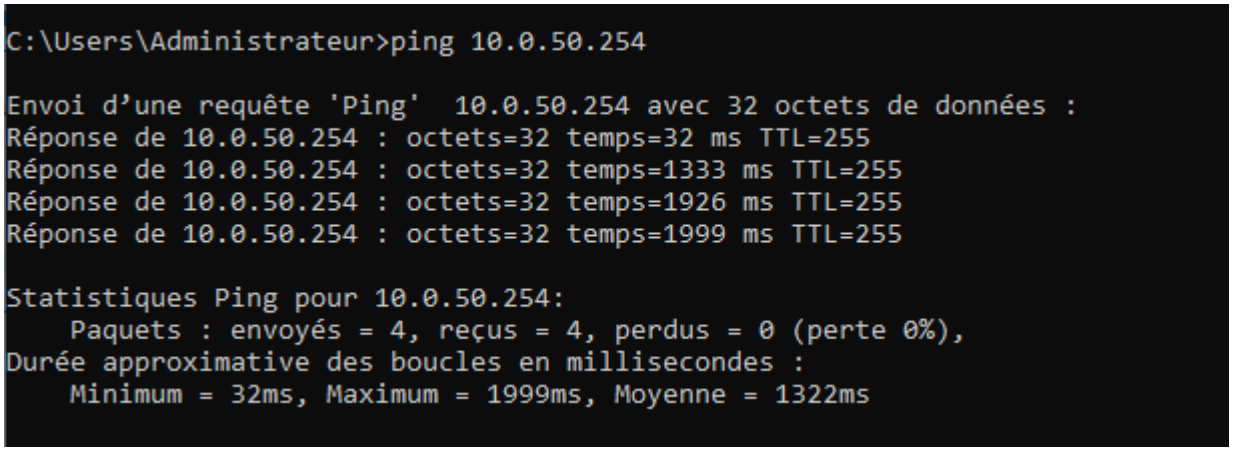

Figure III.42 – Ping vers la passerelle réussi sur le server.

Puis pour tester la connectivité entre le serveur les différents Vlans nous allons envoyer des requêtes Ping à leurs passerelles respectives :

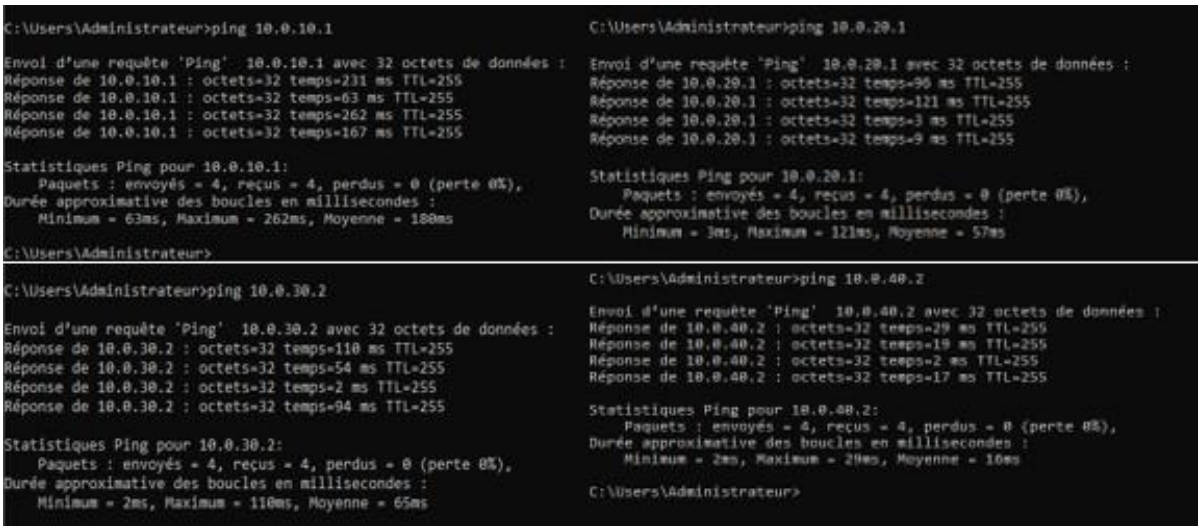

Figure III.43 – Ping vers les VLANs réussi sur le serveur.

7.2 Tests sur les PC clients

7.2.1 Sur Client1

On vérifiera d'abord le bon adressage du Client 1 se trouvant sur le VLAN 10 :

Figure III.44 – Configuration IP reussite sur la machine Client 1.

Une fois la vérification faite, nous allons tenter d'envoyer une requête ping à sa passerelle par défaut :

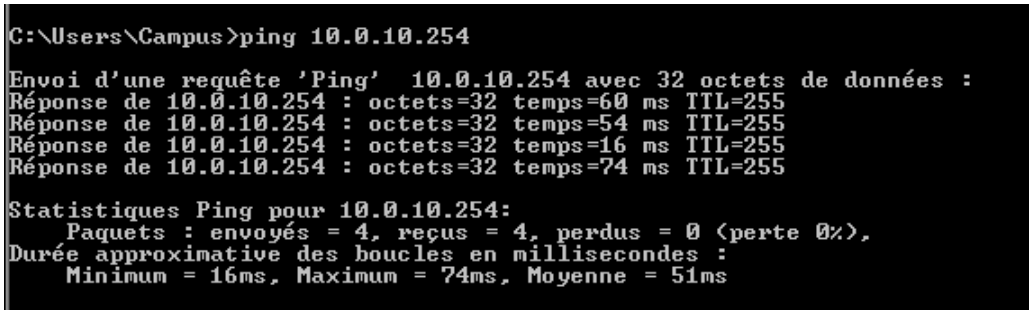

Figure III.45 – Ping vers la passerelle reussi sur la machine Client 1.

À partir du Client 1 qui se trouve toujours sur le VLAN 10, nous allons tester la connectivité avec le serveur se trouvant sur le VLAN 50 :

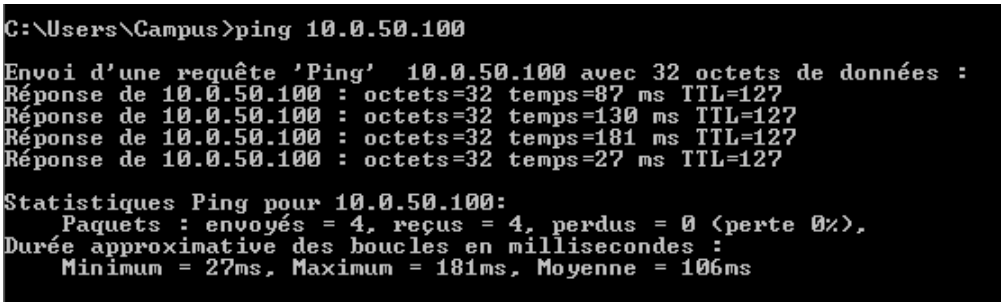

Figure III.46 – Ping vers le serveur reussi sur le Client 1.

De la même manière nous allons envoyer une requête Ping du Client 1 (VLAN 10) vers les autres VLAN afin de vérifier le routage-inter-VLAN :

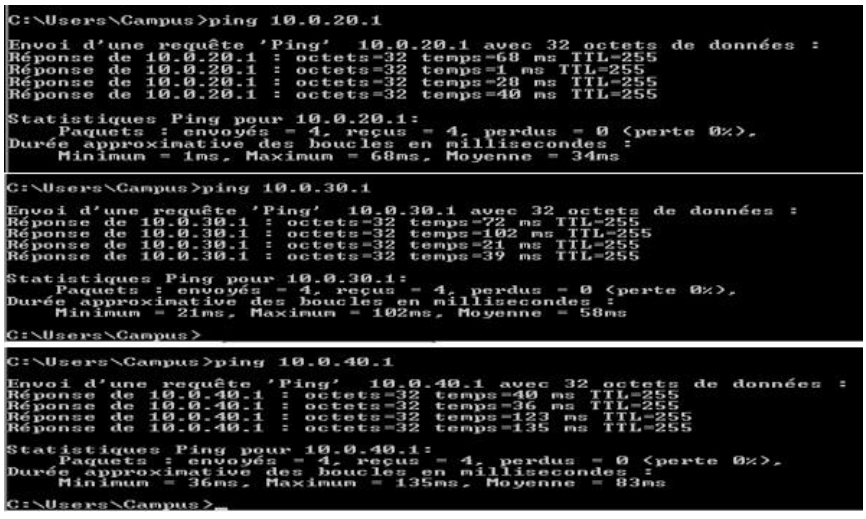

Figure III.47 – Pings reussis vers les VLANs.

7.2.2 Sur Client2

Tout d'abord nous allons vérifier la configuration IP du client 2 :

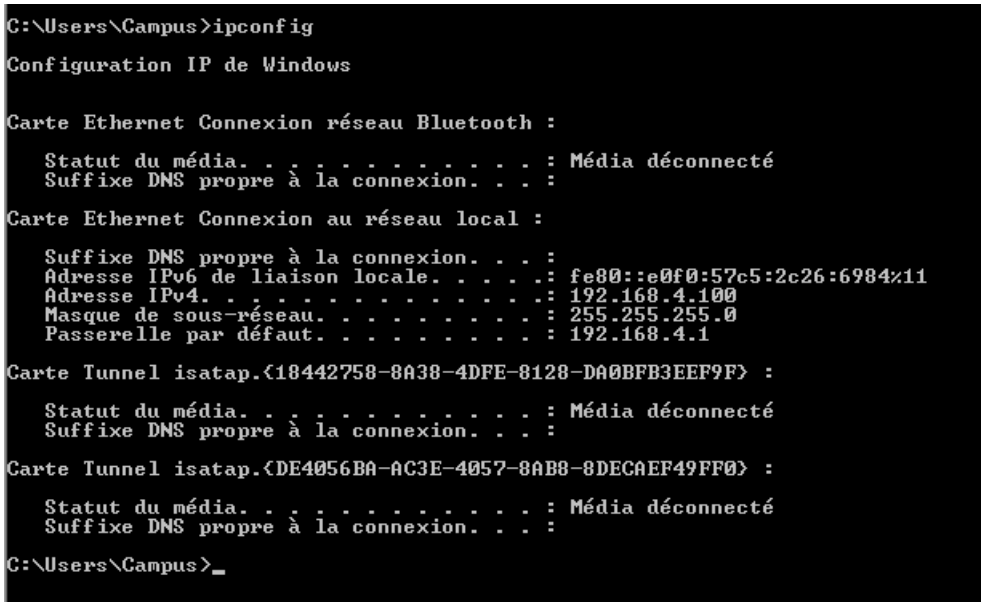

Figure III.48 – Configuration IP reussite sur la machine Client 2.

Puis nous testerons par un ping sa passerelle par défaut :

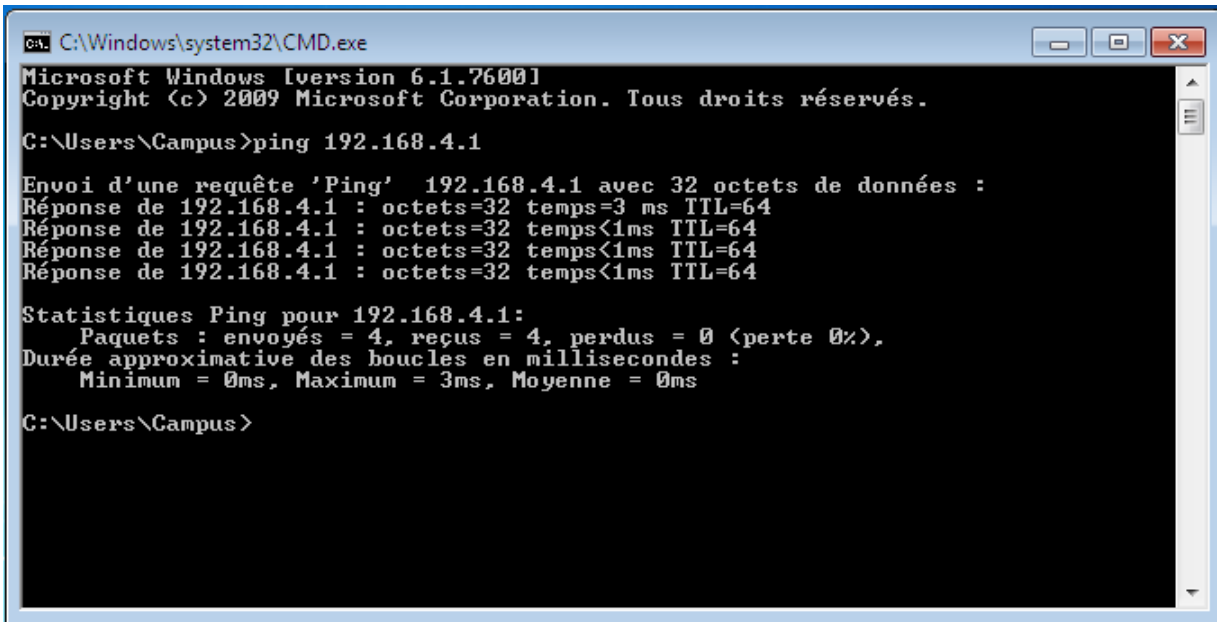

Figure III.49 – Ping reussi vers la passerelle sur le Client 2.

Par la suite nous allons envoyer une requête Ping vers le pare-feu de Bejaia :

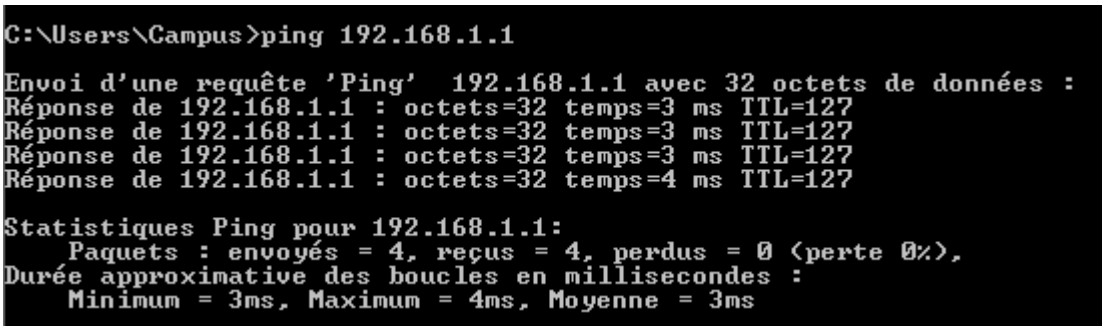

Figure III.50 – Ping reussi vers le pare-feu de Bejaia.

7.3 Tests sur la DMZ

Nous allons envoyer une requête Ping du Serveur 1 (community) Vers le Serveur 2 (Community) puis vers le Serveur 3 (Isolated) :

```
SRV1> ping 192.168.3.11

84 bytes from 192.168.3.11 icmp_seq=1 ttl=64 time=0.362 ms
84 bytes from 192.168.3.11 icmp_seq=2 ttl=64 time=0.857 ms
84 bytes from 192.168.3.11 icmp_seq=3 ttl=64 time=0.396 ms
84 bytes from 192.168.3.11 icmp_seq=4 ttl=64 time=0.935 ms
84 bytes from 192.168.3.11 icmp_seq=5 ttl=64 time=0.724 ms

SRV1> ping 192.168.3.12

host (192.168.3.12) not reachable
```

Figure III.51 – Ping reussi sur le Serveur 1.

Par la suite nous allons faire de même sur Serveur 2 :

```
SRV2> ping 192.168.3.10

84 bytes from 192.168.3.10 icmp_seq=1 ttl=64 time=0.691 ms
84 bytes from 192.168.3.10 icmp_seq=2 ttl=64 time=0.490 ms
84 bytes from 192.168.3.10 icmp_seq=3 ttl=64 time=0.609 ms
84 bytes from 192.168.3.10 icmp_seq=4 ttl=64 time=48.757 ms
84 bytes from 192.168.3.10 icmp_seq=5 ttl=64 time=0.766 ms

SRV2> ping 192.168.3.12

host (192.168.3.12) not reachable
```

Figure III.52 – Ping réussi sur Serveur 2.

7.4 L'accès à distance

Nous allons maintenant essayer d'accéder au poste du Client 2 se trouvant sur le LAN distant à Alger (LAN4). Dans la barre de recherche du menu démarrage, nous allons entrer la recherche « RDC » ou alors « Connexion bureau à distance ». Nous introduisant l'adresse IP de l'hôte auquel on souhaite accéder, dans notre cas l'adresse IP du Client 2 qui est 192.168.4.100, puis une autre fenêtre apparait demandant le nom d'utilisateur ainsi que le mot de passe de l'ordinateur comme l'indique la figure III.53.

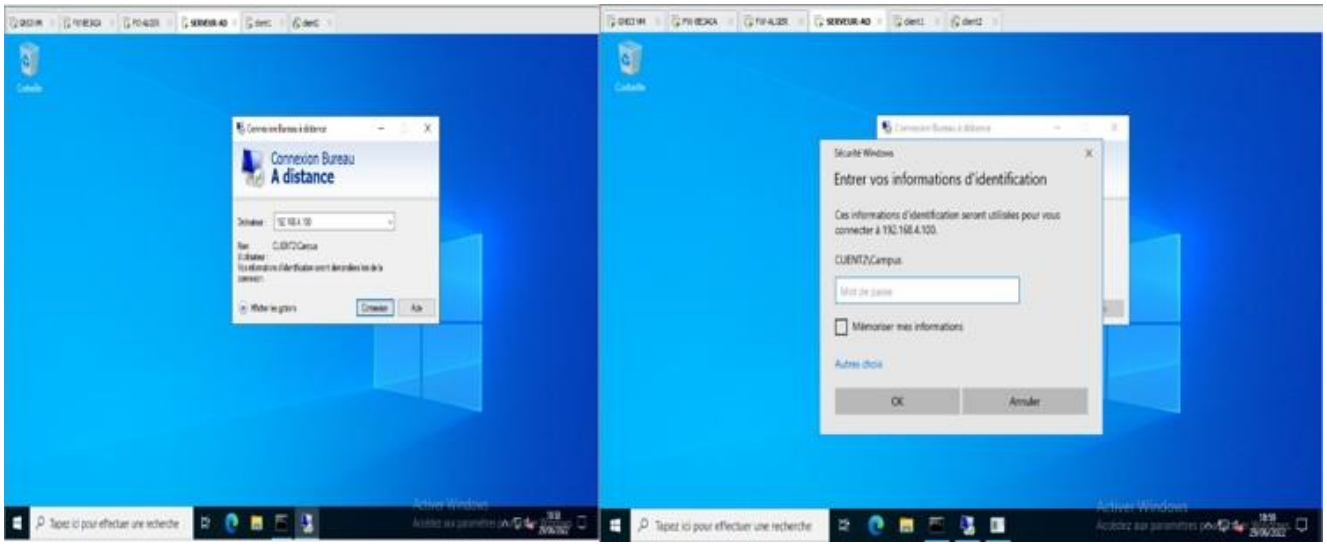

Figure III.53 – Demande d'accès à distance.

Une fois cela fait un accès au poste du Client 2 nous ai possible, comme suit :

Figure III.54 – Interface du poste client 2.

Afin de capture le trafic circulant entre les deux pares-feux nous utiliserons Wireshark comme suit :

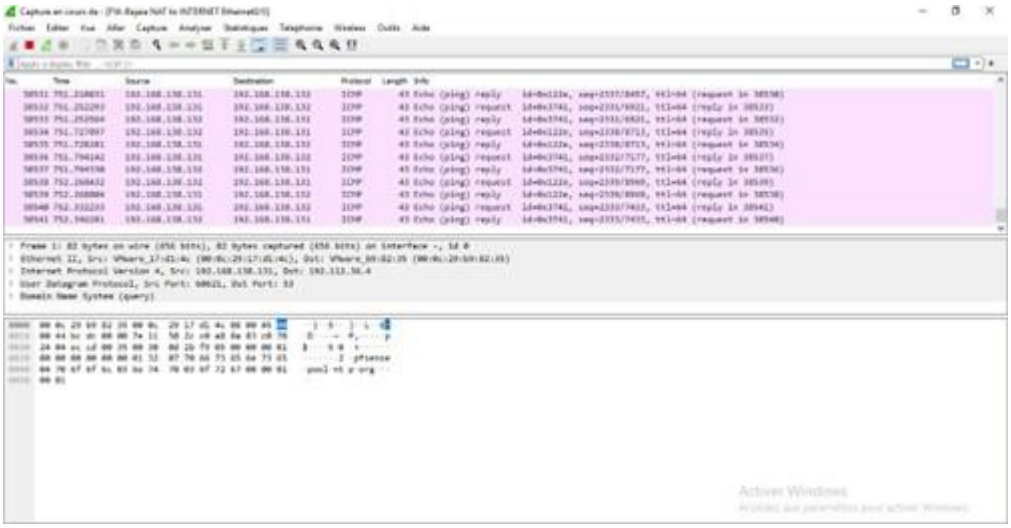

Figure III.55 – Capture du trafic entre les deux pares-feux.

Conclusion

Dans ce chapitre, nous avons simulé la nouvelle architecture proposée pour Campus NTS Bejaia, où nous avons organiser les différents services composant l'entreprise dans des réseaux virtuels relativement à leurs fonctionnalités, puis nous avons mis en place une liaison virtuelle avec un partenaire distant se trouvant à Alger en utilisant un VPN pour un accès à distance plus simple et sécurisé et à moindre coût.

Conclusion générale

La diversité de menaces qui pèse sur un système d'information pousse les ingénieurs réseaux à redoubler de créativité et à sans cesse trouver des solutions efficaces mais surtout durables pour la sécurisation des réseaux informatiques.

Le présent travaille nous a permis de faire un état des résultats de la segmentation d'un réseau local en VLAN qui rappelons le, offre une flexibilité et une facilité d'administration par le biais d'utilisation de protocoles tel que VTP, et une sécurité en plus du fait de de l'encapsulation à des niveaux supérieures. Puis la mise en place d'un VPN site-to-site entre l'entreprise Campus NTS se trouvant à Bejaia et un partenaire distant se trouvant à Alger. Grace à cette technologie un accès à distance totalement sûr a pût être mis en place via l'utilisation du protocole IPSec qui offre une sécurisation de la communication.

Notre travail a été partagée en deux parties, la première étant l'approche théorique, où nous avons abordées les bases des réseaux informatique et l'impartibilité de la mise en place d'une politique de sécurité efficace en fonctions des besoins et de l'envergure de l'organisme mais surtout en fonction des pratiques non éthiques qui constitue un danger pour le système d'information et qui ne cesse de progresser. La seconde partie quant à elle porte sur l'application des notions développées dans la première partie pour mettre en place les liaisons virtuelles (VLAN et VPN).

Nous avons ainsi pu apporter notre contribution à l'entreprise et acquérir de nouvelles connaissances et une expérience personnelle et professionnelle, nous donnant une occasion de nous familiariser avec l'environnement de travail, qui fut plus que bénéfique pour nous.

Bibliographie

[1] G. PUJOLLE, Les Réseaux, 5ème édition. Paris : Editions EYROLLES, 2006, 1124 p.

[2] M.E. WHITMAN, H.J. MATTORD, A. GREEN, Guide to firewalls & VPN, 3ème édition. Boston : Cengage Learning, 2011, 370 p.

[3] Bartlett, Graham, IKEv2 IPsec Virtual private network, 1ère édition. Indiana : Cisco Press, 2017, 608 p.

[4] A. VARDY, CISCO CCNA networking for beginners, 1ère édition. South Carolina : CreateSpace Independent Publishing, 2015, 90 p.

[5] F. EBEL, S. BAUDRU, R. CROFERT, D. PUCHE, J. HENNECART, S. LARSSON, M. AGE, Sécurité informatique Ethical Hacking, 1ère édition. Saint-Herblain : Edition ENI, 2009, 359 p.

[6] ANSSI, Guide d'Informatique, 2nd édition. Paris : Agence Nationale de la Sécurité des Systèmes Informatique, 2017, 72 p.

[7] P. ATELIN, Réseaux Informatiques, 3ème édition. Saint-Herblain : Edition ENI, 2009, 409 p.

[8] C. WELSH, GNS3 Network Simulation Guide, 1ère édition. Birmingham : Packet Publishing Ltd, 2013, 155 p.

[9] J-F. CARPENTIER, La sécurité informatique dans la petite entreprise Etat de l'art et bonne pratique, 3éme édition. Saint-Herblain : Edition ENI, 2016, 444 p.

[10] P. JAQUET, « Les Réseaux Informatiques », cours, 2015.

[11] C. LLORENS, L. LEVIER, D. VALOIS, O. SALVATORI, Tableau de bord de la sécurité réseaux, 2ème édition. Paris : Editions EYROLLES, 583 p.

[12] C. Severin, Réseaux & Télécom, 2ème édition. Paris : Edition DUNOD, 2006, 938 p.

[13] C. Wolfhugel, L. Bloch, Sécurité Informatique Principes et méthodes à l'usage des DSI, RSSI et administrateurs, 2ème édition. Paris : Editions EYROLLES, 2009, 292 p.

[14] F. Goffinet. (2021). [En ligne]. https ://cisco.goffinet.org

[15] V. Weber (2014). [En ligne]. https ://www.networklab.fr

[16] https ://formip.com

[17] https ://networklessons.com

[18] https ://forum.huawei.com/enterprise/fr/index.html

Résume

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 mettre en œuvre une amélioration de l'architecture du réseau de CAMPUS NTS, afin de gérer et sécuriser d'une bonne manière le transfert de données entre les services du réseaulocal et entre 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 modern times, computer security is essential for the proper functioning of any network due to its extreme importance. For this reason, corporate network engineers need to develop more robust and effective management and security mechanisms and protocols to protect their networks. The objective of this project is to implement an improvement of CAMPUS NTS's network architecture, in order to manage and secure data transfer between local network services and between two remote sites in a good way. To this end, we organized all the network users into VLANs according to their functions or categories, and then we configured a secure VPN between the two local networks linking BEJAIA and ALGIERS with GNS3. During our internship, we were able to improve the services that can be provided by the use of communication and security networks essential in our daily lives.

Keywords : VLAN, VPN, GNS3.