République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. Mira Béjaïa
Faculté Des Sciences Exactes
Département Informatique

Mémoire de fin de Cycle

En vue de l'obtention du diplôme de Master Professionnel en Informatique.
Option : Administration et Sécurité des Réseaux

THÈME

Étude et mise en place d'une nouvelle installation réseau sécurisée cas de client ngtmeziani

Présenté par :

Mlle : REDOUANE Nihad & *Mlle* : SAADOUNE Dyhia

Soutenu devant le jury composé de :

Présidente :	Mme : ALLOUI Soraya.	Université A. MIRA de Béjaïa.
Examinateur :	Mr : BEDJOU Khaled	Université A. MIRA de Béjaïa.
Examinateur :	Mr : DJEBARI Yassine	Campus NTS Bejaia.
Encadrant :	Mr : MEHAOUED Kamal.	Université A. MIRA de Béjaïa.

Promotion 2022/2023

Remerciements

Tout d'abord, le grand et l'infini remerciement au bon dieu ALLAH, le tout puissant de nous avoir illuminé et ouvert les portes du savoir et nous avoir donné lavolonté, la santé et le courage pour effectuer ce travail.

Nous souhaitons adresser nos remerciements aux personnes qui nous ont aidéesdans la réalisation de notre mémoire de fin d'études.

En premier lieu, nous remercions notre promoteur ***Mr MEHAOUED Kamal*** *d'avoir accepté de nous encadrer, orienté, pour notre projet, ainsi que pour sa confiance, ses encouragements, ses corrections et pour les conseils qu'il apporté.*

Nous tenons également à remercier l'ensemble des membres de jury de nousavoir honorés en acceptant d'évaluer notre travail, ainsi que pour d'éventuelles suggestions.

Et de manière spéciale nous exprimons nos chaleureux remerciements pour notre encadrant de stage ***Mr DJEBARI Yassine*** *qui nous a donné l'opportunité de nous familiariser avec le milieu de travail, nous avoir aidé avec toute sa patience et quinous a ouvert les horizons par ses idées, ses propositions et ses ambitions et qui nous asoutenus jusqu'au bout.*

Nous tenons également à remercier toutes nos familles, nos ami(e), nos collègues étudiants et tous ceux qui ont participés de près ou de loin à la réalisation de ce travail

Nous profitons aussi cette occasion pour exprimer nos plus vifs remerciementsenvers tous les enseignants du département Informatique, de la Faculté des Sciences Exacte, d'Université Abd Rahman Mira de Bejaia qui nous ont apportés du soutien durant nos études.

Dédicace

Je dédie ce modeste travail à :

Ma mère, qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

A mes frères qui a tout fait pour m'encourager durant toutes mes études.

Aux êtres chers auxquelles je ne saurais exprimer ma gratitude et ma reconnaissance, mes sœurs Noura et Soraya, Dalila, Khoumissa,Lydia, Feyrouze et leurs maris.

A toute ma famille, la fierté d'être l'une des leurs amis(e)

Et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

SAADOUNE Dyhia

Dédicace

Je souhaite dédier ce travail à mes parents bien-aimés, avec une affection particulière envers ma mère qui occupe une place spéciale dans mon cœur, ainsi qu'à mes frères et sœurs, Faten, Nadjet et son mari Samir, Hamza, Walid et Nadjim, qui ont constamment soutenu et encouragé mes études tout au long de mon parcours.

Je tiens également à mentionner mes neveux, Ayoub, Yacer, Younes et Lokmane.

A mon oncle et mes tantes, en particulier ma tante Rahima

A mes cousins et cousines et à toute ma famille.

A mes chers amis avec une mention spéciale pour Emilia qui est bien plus qu'une simple amie, mais une sœur

Ainsi qu'à toutes les personnes qui ont entendu mes embêtements et à ceux qui m'ont conseillé et soutenu tout au long de cette période.

A tous ceux qui m'aiment et à tous ceux qui occupent une place dans mon cœur.

A tous ceux qui m'ont aidé durant ma vie universitaire.

REDOUANE Nihad

Table des matières

Chapitre IV : Réalisation et Test

Table des figures

Liste des tableaux

Liste des abréviations

A

AAA	Authentication, Authorization, Accounting/Auditing
ACL	Access Control List
AD	Active Directory
ARP	Adresse Resolution Protocol

B

BGP	Border Gateway Protocol

C

CDP	Cisco Discovery Protocol

D

DARPA	Defense Advanced Research projects agency
DMZ	DeMilitarized Zone
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
DOD	Department of Defense
DTP	Dynamic Trunking Protocol

E

EGP	Exterior Gateway Protocol

F

FDDI	Fiber Distributed Data Interface
FHRP	First Hop Redundancy Protocol
FTP	File Transfert Protocol

G

GLBP	Gateway Load Balancing Protocol
GRE	Generic Routing Encapsulation

H

HSRP	Hot Standby Router Protocol
HTTP	Hyper Text Transfer Protocol

I

ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IGP	Interior Gateway Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IP	Internet Protocol

L

LACP	Link Aggregation Control Protocol
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol

M

MAC	Media Access Control
MAU	Multistation Access Unit
MAN	Métropolitains Area Network
MPLS	Multi Protocol Label Switching

O

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

P

PAgP	Port Aggregation Protocol

Q

QOS	Quality of service
RIP	Routing information protocol

S

SMTP	Simple Mail Transport Protocol

SSH	Secure Shell
SVI	Switch Virtual Interface

T

TELNET	TELecommunication NETwork
TCP	Transmission Control Protocol

V

VLAN	Virtuel Local Area Network
VTP	Vlan Trunking Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

W

WAN	Wide Area Network

Introduction générale

Introduction générale

De nos jours, les réseaux informatiques jouent un rôle essentiel dans le fonctionnement des entreprises, des institutions et même des foyers. La connectivité est devenue un aspect fondamental pour faciliter la communication, l'échange d'informations et l'accès aux ressources. Cependant, avec l'augmentation des cybermenaces et des attaques informatiques, la sécurité des réseaux est devenue une préoccupation majeure.

La mise en place d'une nouvelle installation réseau sécurisée vise à protéger les données, les systèmes et les utilisateurs contre les menaces potentielles. Cela implique la conception, la configuration et le déploiement d'une architecture réseau solide, accompagnée de mesures de sécurité appropriées.

L'un des éléments clés d'une installation réseau sécurisée est la mise en place de **pare-feu et monitoring (Zabbix)**, de mécanismes de détection d'intrusion et de prévention, ainsi que de systèmes de gestion des vulnérabilités. Ces outils aident à identifier et à bloquer les tentatives d'intrusion, à filtrer le trafic malveillant et à prévenir les attaques. Parallèlement, il est essentiel de mettre en œuvre des politiques de sécurité robustes, telles que l'authentification forte, l'accès basé sur les rôles et les privilèges, la segmentation du réseau, le chiffrement des données sensibles et la surveillance continue du réseau.

De plus, la sensibilisation des utilisateurs aux bonnes pratiques en matière de sécurité informatique est également un aspect crucial pour renforcer la sécurité du réseau. La mise en place d'une nouvelle installation réseau sécurisée doit être réalisée de manière méthodique et bien planifiée, en tenant compte des besoins spécifiques de l'organisation, des réglementations en vigueur et des meilleures pratiques de sécurité. Cela peut nécessiter l'expertise de professionnels en sécurité informatique, tels que des ingénieurs réseau et des consultants en sécurité, afin de garantir une mise en place efficace et fiable.

Le stage que nous avons effectué au l'entreprise de campus nts à Bejaia, nous a permis de découvrir son réseau et de comprendre son fonctionnement. Le but de notre travail est de proposer une architecture réseau sécurisée de l'entreprise campus nts (Nous étudierons l'architecteur réseau de son client **« ngtmeziani »)** et de mettre des mécanismes de sécurisation des échanges de données. Afin de réaliser les objectifs visés, nous avons organisé ce travail en quatre chapitres :

- Le premier chapitre est consacré aux généralités sur les réseaux, la sécurité informatique et les dispositifs de sécurité.

- Le deuxième chapitre nommé « Présentation de l'organisme d'accueil » aura pour objectif de mieux comprendre l'organisme et sa structure hiérarchique, nous allons donc évoquer les différentes problématiques rencontrés et la solution que nous pensons la plus adéquate.

- Le troisième chapitre est focalisé sur l'administration et sécurité des réseaux avancé : nous avons examiné les modèles d'architectures sécurisées, les différents équipements et interfaces sécurisés, les stratégies et techniques de sécurisation avant d'en concevoir une.

- Le quatrième chapitre : Implémentation de l'architecture sécurisée, dans ce chapitre nous avons d'abord conçu l'architecture, puis implémenté sur **GNS3** toutes les fonctionnalités de sécurité.

Chapitre I

Généralités sur les réseaux et la sécurité informatique

***Chapitre I** : Notions de base sur les réseaux et sécurité informatique*

Introduction

Les réseaux et la sécurité sont deux domaines interconnectés essentiels dans le monde numérique d'aujourd'hui. Les réseaux font référence à l'infrastructure qui permet la communication et l'échange de données entre les différents appareils connectés, tels que les ordinateurs, les smartphones et les serveurs.

D'autre part, la sécurité vise à protéger ces réseaux et les informations qui y circulent contre les menaces potentielles. Avec la multiplication des cyberattaques et des violations de données, il est essentiel de mettre en place des mesures de sécurité pour préserver la confidentialité, l'intégrité et la disponibilité des informations.

Ce chapitre examine deux sections essentielles, la première décrit d'une manière générale les réseaux informatiques, la deuxième énumère la terminologie, les politiques et les différentes attaques réseau. Ensuite, nous discuterons des éléments à sécuriser dans un réseau, et enfin, nous étudierons les mécanismes de défense tels que les pare-feux, les ACLs et les DMZ, IPSec et nous terminons ce chapitre par une conclusion.

Partie I : introduction aux réseaux informatique

I.1 Définition et intérêt

I.1.1. Réseaux informatiques

Les réseaux informatiques sont constitués d'un groupe d'ordinateurs interconnectés par des câbles physiques, qui leur permettent d'échange des informations sous forme de données numériques, facilitant ainsi la communication et la collaboration entre les utilisateurs. Les réseaux peuvent être locaux (LAN) ou étendus (WAN), et peuvent être câblés ou sans fil. [1]

I.1.2. Intérêts des réseaux informatiques

Voici quelques exemples d'intérêts des réseaux informatiques :

- **Communication efficace (personnes, processus…) :** les réseaux informatiques permettent une communication rapide et efficace entre les utilisateurs, qu'ils soient proches ou éloignés géographiquement.
- **Partage de ressources (fichiers, applications, matériels…) :** les réseaux permettent le partage de ressources, ce qui permet d'optimiser l'utilisation des ressources disponibles et de réduire les couts.

- **Collaboration :** Les réseaux favorisent la collaboration entre les individus et les équipes en permettant le travail simultané sur des projets, le partage d'idées, de connaissances et de compétences, et la coordination des activités.
- **Accès à distance :** Les réseaux informatiques permettent l'accès à distance aux systèmes et aux données, ce qui offre une flexibilité aux utilisateurs qui peuvent accéder à leurs informations et effectuer leur travail à partir de différents endroits.
- **Accès à l'information :** Les réseaux facilitent l'accès à l'information en permettant la recherche et la récupération rapide de données à partir de diverses sources, qu'il s'agisse de ressources en ligne, de bases de données ou de système d'information internes.
- **Centralisation de contrôle :** Les réseaux permettent une gestion centralisée des ressources, des utilisateurs et des politiques de sécurité, ce qui facilite la supervision et la maintenance des systèmes informatiques. [1]

I.2 Supports de transmission

Un support de transmission transporte des données sous forme de signaux, entre les interfaces réseau tels que : La paire torsadée, le câble coaxial et la fibre optique (Multimode, Monomode).

I.2.1 Cable à paire torsadée

Est un câble composé de deux fils de cuivre isolés torsadés ensemble pour former une paire, c'est le support de transmission le plus courant, le plus simple et le plus économique. Il existe deux types de paires torsadées ; la paire torsadée non blindée UTP (peut atteindre 100 mètres) et la paire torsadée blindée STP (prend en charge des débits plus élevés, sur des distances légèrement plus importantes)

Les principaux types de connecteurs pour la paire torsadée :

RJ-11 : câble téléphonique à 2 paires torsadées.

RJ-14 : câble téléphonique à 3 paires torsadées.

RJ-45 : câble téléphonique à 4 paires torsadées. [10] [11]

I.2.2 Le câble coaxial

Est composé de de deux conducteurs cylindriques de même axe séparés par un isolant. Le câble coaxial est principalement utilisé pour la transmission de signaux audio, vidéo et de données à haute fréquence. Il offre une bonne protection contre les interférences électromagnétiques et permet des transmissions fiables sur de longues distances. [10]

I.2.3 La fibre optique : La fibre optique se compose de fils de verre extrêmement fins et transparents, elle comprend un cœur dans lequel se propage la lumière et une gaine externe de protection qui maintient la lumière à l'intérieur du cœur. Ces fils ont la capacité de transmettre des signaux lumineux à une vitesse très élevée, offrant ainsi une qualité de transmission exceptionnelle sur de longues distances. [9] [10]

I.3 Classe des réseaux

Les réseaux informatiques sont essentiels pour connecter des appareils et faciliter la communication et l'échange de données. Il existe différents types de réseaux, adaptés à des besoins spécifiques et différentes échelles géographiques.

I.3.1 LAN (Local Area Network)

C'est un réseau interne à une entreprise dans un bâtiment ou un campus (dans une zone géographique limitée), la notion de réseau local englobe un ensemble de techniques allant de celles nécessaires à la communication de plusieurs centaines de machines d'un même établissement d'une entreprise à celles beaucoup plus simples mises en œuvre par un particulier pour relier son ordinateur et son imprimante à sa connexion internet. Les réseaux locaux sont des réseaux privés dont la taille ne dépasse pas quelques kilomètres. [2]

I.3.2 MAN (Metropolitan Area Network)

D'une étendue de l'ordre d'une centaine de kilomètres, les MAN sont généralement utilisés pour fédérer les réseaux locaux ou assurer la desserte informatique de circonscriptions géographiques importantes. Le MAN est essentiellement un gros réseau LAN, qui couvre une ville. [2]

I.3.3 WAN (Wide Area Network)

Réseaux géographiquement distants connectés entre eux, (couvre un pays) ex : Internet, ces réseaux assurent l'acheminement des informations sur de grandes distances. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance. [2]

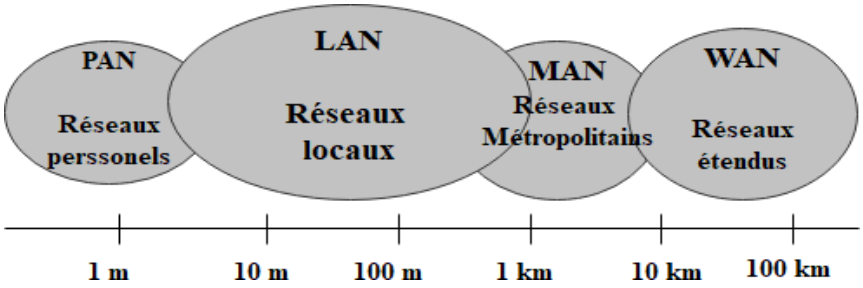


Figure I.1 : Les classes des réseaux.

I.4 Topologies des réseaux

La topologie d'un réseau fait référence à la manière dont ses différents composants sont interconnectés et interagissent entre eux.

I.4.1 La topologie logique

Désigne la manière dont les données circulent à travers les lignes de communication. Elle est établie grâce à un protocole d'accès. Les topologies logiques les plus répandues comprennent Ethernet, Token ring et FDDI.

I.4.2 La topologie physique

La topologie d'un réseau correspond à son architecture physique. On peut retenir les principales topologies suivantes : en bus, en étoile, en anneau, et en arbre

- **La topologie en bus**

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

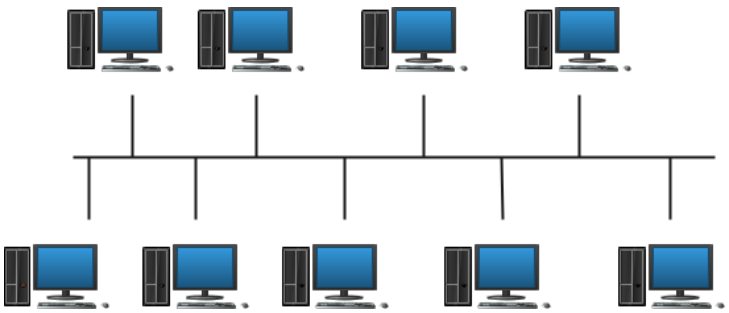


Figure I.2 : Topologie en bus.

Elle a pour avantages d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est très vulnérable car si l'une des connexions est défectueuse, l'ensemble du

réseau en est affecté. De plus, la vitesse de transmission est faible puisque le câble est commun [3].

- **Topologie en anneau**

Dans un réseau en anneau, toutes les entités sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique, d'une entité à la suivante. A un instant donné, un seul nœud peut émettre sur le réseau et il ne peut pas se produire de collision entre deux messages, contrairement au cas du réseau de type bus. Cette topologie est utilisée par les réseaux Token Ring et FDDI. [3]

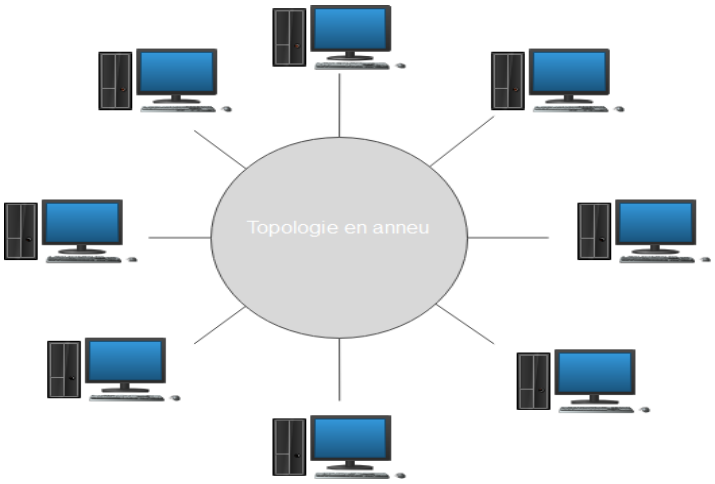


Figure I.3 : Topologie en anneau.

- **Topologie en étoile**

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système concentrateur central (hub ou switch). Les réseaux ayant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Mais toute communication devient impossible si l'élément central ne fonctionne plus. C'est un type de réseau relativement efficace et économique. La plupart des petits réseaux locaux fonctionnent sur ce principe. [3]

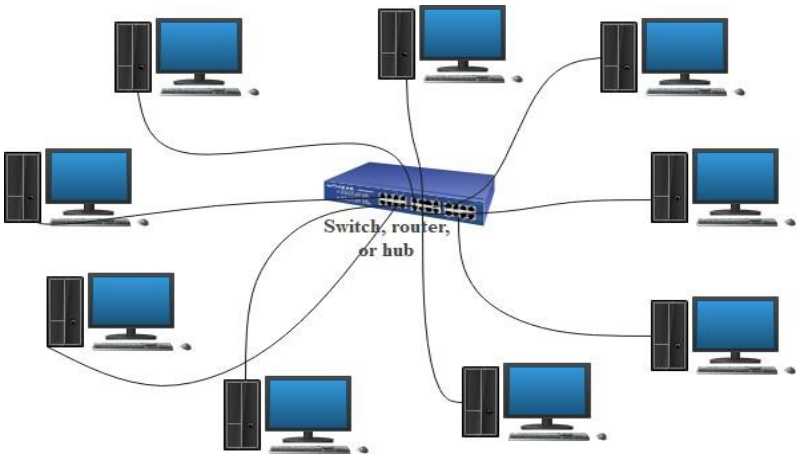


Figure I.4: Topologie en étoile.

- **Topologie en arbre**

Dans une topologie hiérarchique (topologie en arbre), le réseau est divisé en niveaux. Le sommet est connecté à plusieurs nœuds de niveau inférieur dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le point faible de ce type de topologie réside dans l'ordinateur « père » de la hiérarchie qui s'il tombe en panne, paralyse la moitié du réseau. [3]

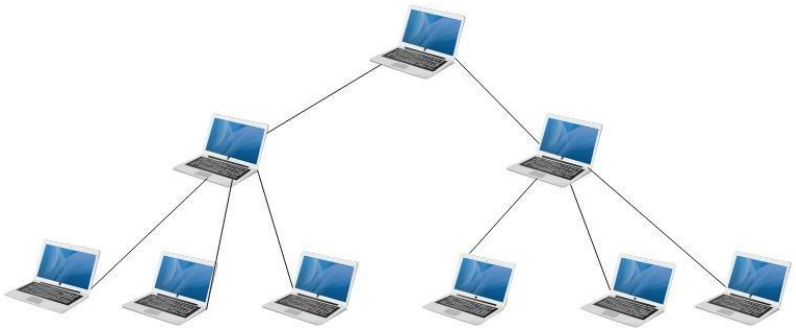


Figure I.5: Topologie en arbre.

I.5 Type de réseau

I.5.1 Internet

L'internet est un réseau mondial composé de nombreux ordinateurs interconnectés, qui utilisent le protocole TCP/IP. Il s'agit d'un service qui permet aux utilisateurs d'accéder à une vaste gamme de médias de communication et de serveurs, leur offrant ainsi la possibilité de partager des informations, de rechercher des sujets, d'échanger des messages et des fichiers via des courriers électroniques. [4]

I.5.2 Intranet

L'intranet est une section sécurisée d'un réseau informatique qu'il s'agisse d'une entreprise ou d'une organisation, qui utilise les mêmes technologies que l'Internet (protocoles de communication TCP/IP, serveur, navigateur, e-mail, etc.). Son but est de faciliter l'échange et le partage d'informations entre des programmes et/ou des utilisateurs identifiés et autorisés. Généralement, l'intranet connecté au réseau Internet afin de permettre la communication avec le monde extérieur. [4]

I.5.3 Extranet

Un extranet est une extension du système d'information d'une entreprise, permettant de partager des informations avec des partenaires situés en dehors de son réseau. L'accès à l'extranet doit être sécurisé, car il donne aux personnes extérieures à l'entreprise un accès au système d'information. Cette sécurité peut être assurée par une authentification simple (nom d'utilisateur et mot de passe) ou une authentification forte (certificat). Il est recommandé d'utiliser le protocole HTTPS pour toutes les pages web consultées depuis l'extérieur, afin de sécuriser le transfert des requêtes et des réponses HTTP, et de prévenir la divulgation en clair du mot de passe sur le réseau. [4]

I.6 Architecture réseau

Il existe 2 modes de fonctionnement des réseaux :

- **"client/serveur",** dans lequel un ordinateur central fournit des services réseaux aux utilisateurs,
- **"poste à poste" ou "égal à égal" (en anglais Peer to Peer),** dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire

I.6.1 Client/serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. [5]

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique). [5]

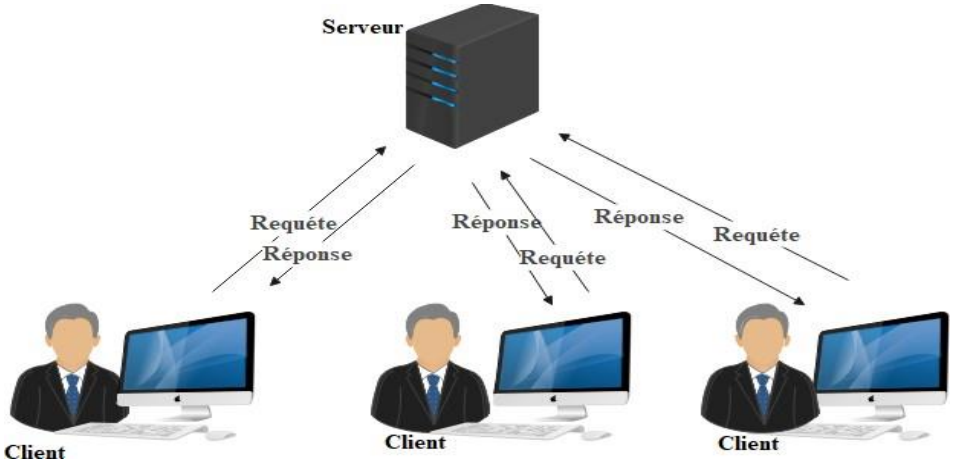


Figure I.6: Architecture client-serveur.

- **Fonctionnement d'un système client/serveur**

Un système client/serveur fonctionne selon le schéma suivant :

- Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port. [5]

I.6.2 Poste à poste

Contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources.

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.

Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste. Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.). [5]

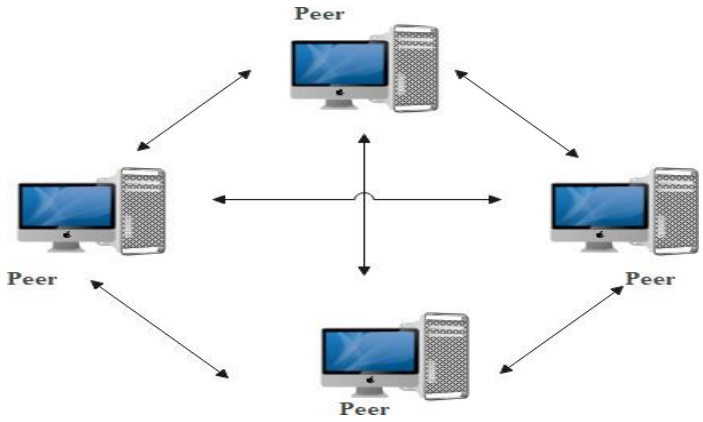


Figure I.7: Poste à poste.

- **Fonctionnement d'un système Peer to Peer**

La mise en œuvre d'une telle architecture réseau repose sur des solutions standards : Placer les ordinateurs sur le bureau des utilisateurs. Chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité Pour les connexions, on utilise un système de câblage simple et apparent

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- Moins de 10-30 utilisateurs
- Tous les utilisateurs sont situés dans une même zone géographique
- La sécurité n'est pas un problème crucial
- Ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir. [5]

I.7 Les normes de communication

I.7.1. Modèle OSI

Un aspect important dans l'ouverture des réseaux a été la mise en place d'un modèle de référence, le modèle OSI. Celui-ci définit un modèle en sept couches réseau, présentes sur chaque station qui désire transmettre.

Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes, chaque couche va donc avoir un rôle à accomplir, et l'ensemble de ces rôles va permettre de communiquer d'un ordinateur à un autre. Même si le modèle OSI est très peu complémenté, il sert toujours de référence pour identifier le niveau de fonctionnement d'un composant réseau. Ainsi, paradoxalement aujourd'hui, TCP/IP est mis en œuvre partout et même lorsque l'on parle de ce protocole on l'associe aux couches du modèle OSI. [6]

- **Principe**

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System Interconnection (OSI) destiné à normaliser les échanges entre deux machines. Il définit ainsi ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques.

Ce modèle définit précisément les fonctions associées à chaque couche. Chacun d'entre elles se comporte comme un prestataire de service pour la couche immédiatement supérieure. Pour qu'une couche puisse envoyer une commande ou des données au niveau équivalent du correspondant, elle doit constituer une information et lui faire traverser toutes les couches inferieures, chacune d'elles ajoutant un en-tête spécifique à ce qui devient une sorte de train (encapsulation). A l'arrivée, cette information est décodée, la commande ou les données sont libérées (des-encapsulation). [6]

I.7.2 TCP/IP

L'architecture TCP/IP a été développée dans le milieu des années 1970 par la DARPA (Defense Advanced Research Projets Agency – Etats Unis) pour les besoins de communication et d'interfonctionnement des applications entre les systèmes informatiques militaires (DoD, Department of Defense). Pour cela, il fallait définir un format d'échange des données commun à tous les systèmes tout en préservant l'existant, c'est-à-dire sans modifier les réseaux existants. En fait, TCP/IP masque aux applications les sous-réseaux réels de transport utilisées.

TCP/IP, du nom de ses deux protocoles principaux (TCP, Transmission Control Protocol et IP, Internet Protocol), est un ensemble de protocoles permettant de résoudre les problèmes d'interconnexion en milieu hétérogène. A cet effet, TCP/IP décrit un réseau logique (réseau IP) au-dessus du ou des réseaux physiques réels qui réalisent le transport effectif des données et auxquels sont effectivement connectés les ordinateurs. [2]

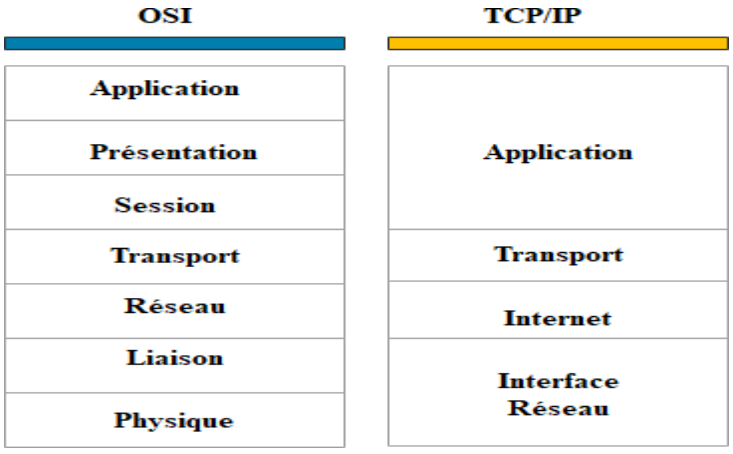


Figure I.8: Modèle OSI et architecture TCP/IP.

I.8 Adressage

I.8.1 L'adressage physique et logique

Il existe deux types d'adresses dans un réseau : une adresse physique et une adresse logique.

- **L'adresse physique de niveau 2 appelée adresse MAC** est indépendante des autres adresses physiques du réseau. Chaque interface réseau possède une seule adresse physique, ce qui signifie qu'il est impossible de trouver deux adresses physiques identiques dans le monde.
- **Une adresse logique** est liée à un plan d'adressage logique spécifique au réseau de l'entreprise. L'identification d'une station se fait d'abord grâce à la partie réseau de l'adresse logique, qui identifie un réseau ou un sous-réseau, puis grâce à l'adresse hôte, qui identifie de manière unique une station sur ce réseau ou sous-réseau. [7]

I.8.2 L'adresse IP

L'adresse IP est une référence unique utilisée par le protocole Internet pour identifier un équipement, comme un ordinateur ou une imprimante, dans un réseau interne ou externe. Elle est essentielle au fonctionnement d'internet. Parfois, une adresse IP peut représenter un groupe d'appareils, notamment lors de diffusions broadcast ou multicast. Bien qu'un même ordinateur puisse avoir plusieurs adresses IP, chaque adresse ne peut être utilisée qu'une fois simultanément dans un réseau. Les adresses IP sont vérifiées en utilisant les outils TCP/IP comme Ping, Traceroute et Telnet. [7]

L'adressage IP est divisé en cinq classes

A : [0,127] : peu de réseaux et plusieurs utilisateurs

B : [128,191] : nombre équilibré de réseaux et de machines

C : [192,223] : plus de réseaux et moins des utilisateurs (la plus utilisée chez nous)

D : [224,239] : sont réservées à la diffusion de groupe (multicast)

E : [240,255] : sont réservée pour utilisation future.

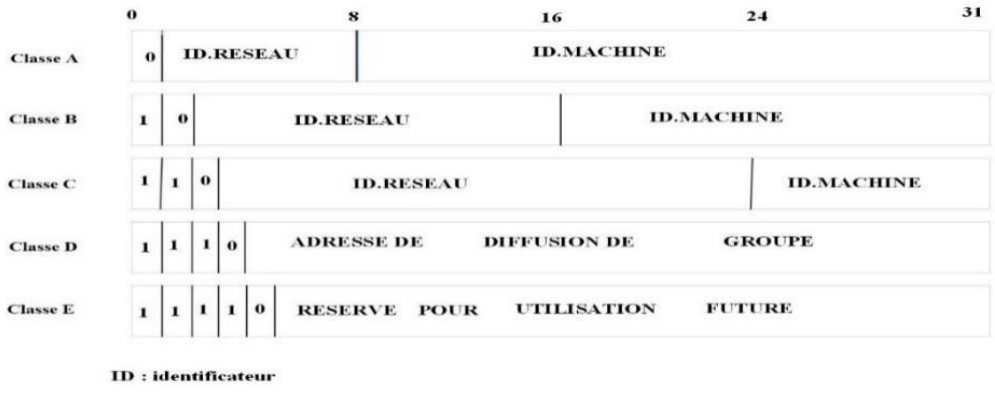


Figure I.9: Classe d'adresse.

- **Adresse IPv4 (les adresses de moment) :** est une version spécifique d'une adresse IP utilisé pour identifier les appareils connectés à Internet. Elle est codée sur quatre octets, elle est représentée en notation décimale pointée, (192.168.0.1). Chaque octet peut contenir des nombres de 0 à 255. Toutefois, en raison de la croissance rapide d'Internet, le nombre d'adresses IPv4 disponibles est devenu limité, ce qui a conduit à L'introduction d'IPv6 offrant un espace d'adressage beaucoup plus vaste. [8]
- **Adresse IPv6 (les adresses de l'avenir) :** les adresses IPv6 sont une nouvelle génération d'adresses IP. Elle est codée sur seize octets, elle est composée de huit groupes de chiffres hexadécimaux, séparés par des deux-points (2001:0db8:85a3:0000:8a2e:0370:7334), les adresses IPv6 répondent aux besoins croissants d'Internet. [8]

I.8.3 Le routage

Le routage est le processus principal utilisé par des systèmes intermédiaires permettant de trouver le meilleur chemin pour livrer des paquets de la station source a la station destinataire.

Dans le réseau IP, un modèle de routage par saut est employé, cela signifie que chaque hôte ou routeur qui traite un paquet examine l'adresse de destination dans l'en-tête IP, calcule le prochain saut qui rapprochera le paquet de sa destination finale, puis le transmet au relais ou à la passerelle, où le processus se répète. Pour accomplir cette tâche, deux choses sont nécessaires :

Tout d'abord, des tables de routage (contenant des informations sur les réseaux et les routes disponibles) qui associent les adresses de destination aux prochains relais, et ensuite, des protocoles de routage qui mettent à jour ces tables.

Le routage IP assure une connectivité efficace entre les réseaux d'Internet, garantissant ainsi un acheminement fiable des données. [7]

Type de routage

Le routage dans les réseaux informatiques comprend plusieurs types :

Le routage statique ou fixe implique une configuration manuelle des routes par un administrateur réseau, tandis que le routage dynamique utilise des protocoles pour échanger automatiquement des informations de routage entre les routeurs (tels que RIP, OSPF et BGP). Le routage par défaut envoie les paquets vers une route générique lorsque la destination n'est pas spécifiée dans la table de routage.

Un protocole de routage résout essentiellement trois problèmes : il découvre les autres routeurs du réseau, il construit les tables de routage, il maintient les tables de routage à jour.
Le routage interne IGP est utilisé pour acheminer les paquets à l'intérieur d'un réseau local, tel qu'un réseau d'entreprise, (les protocoles de routage interne IGP, comme RIP et OSPF), tandis que le routage externe EGP est utilisé pour acheminer les paquets vers des destinations en dehors du réseau local, les protocoles de routage externe EGP, tels que BGP. [2]

Partie II : La sécurité dans les réseaux

I.9 Définition

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité. [12]

I.10Objectifs de la sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique vise généralement cinq principaux objectifs :

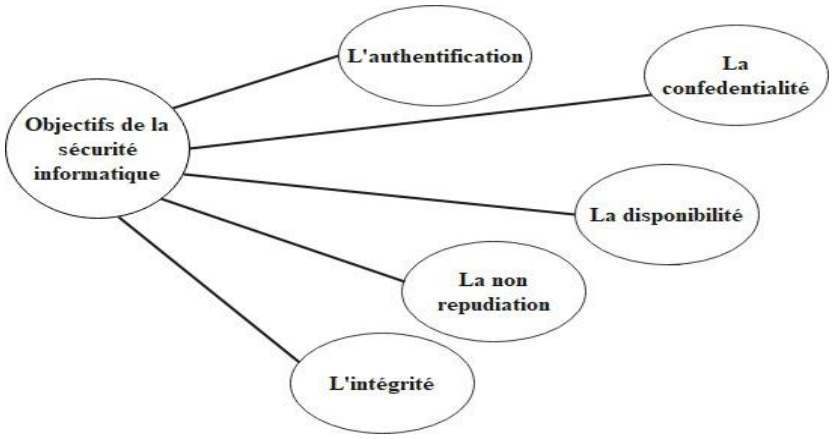


Figure I.10: Les objectifs de la sécurité informatique.

I.10.1 Intégrité : le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction. [13]

I.10.2 Confidentialité : la confidentialité des données peut être définie comme la protection des données contre une divulgation non autorisée. Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- Limiter et contrôler leurs accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
- Les rendre incompréhensibles en les chiffrant de telle sorte que seules les personnes ayant les moyens de déchiffrement puissent y accéder. [13]

I.10.3 Disponibilité : le bon fonctionnement des services, systèmes et données doivent être accessibles aux ayants droits en continu sans interruption, sans retard, ni dégradation.

I.10.4 Non-répudiation : c'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (actions, transactions) a eu lieu. A ce critère de sécurité peuvent être liées les notions suivantes :

- L'imputabilité est l'attribution d'une action (un événement) à une entité déterminée (ressources ou personnes).
- La traçabilité permet de grader une trace numérique de tout événement (message électronique, transfert de données…).
- L'auditabilité définie la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement (courant ou exceptionnel) effectué dans le cadre de procédure de contrôle spécifique et d'audit.

I.10.5 Authentification : doit permettre de vérifier l'identité d'une entité pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources.

I.11 Terminologies de la sécurité informatique

Parmi les mots-clés de la sécurité qui sont largement repris dans la littérature informatique nous trouvons :

- **Vulnérabilité :** c'est une faille de sécurité le plus souvent cachée touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de

configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial. [13]

- **Risque :** c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter.
- **Attaque :** elle représente le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Contre-mesure :** c'est la procédure ou technique permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
- **Menace :** c'est un adversaire déterminé capable de monter une attaque exploitant unevulnérabilité.

I.12 Politique de sécurité

Définition

La politique de sécurité définit un certain nombre de règles, de procédures et une bonne pratique permettant d'assurer un niveau de sécurité conforme au besoin de l'organisation. Elle a pour objectif :

- D'identifier les besoins en temps de sécurité, les risques informatiques et leurs éventuelles conséquences.
- D'élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiées.
- De surveiller et détecter les vulnérabilités du système d'information et se tenir informer des failles sur les applications et matériels utilisés.
- De définir les actions à entreprendre et les personnes à contacter on cas de détection d'une menace. [13]

I.13 Les attaques informatiques

Définition

Chaque ordinateur connecté à un réseau informatique présente une vulnérabilité potentielle face aux attaques. La plupart de ces attaques sont déclenchées automatiquement à partir de machines infectées, à l'insu de leurs propriétaires. Dans certains cas plus rares, il peut s'agir d'actions anticipées par des pirates informatiques (hackers ou crackers).

En d'autres termes, une attaque consiste à exploiter une faille dans un système informatique par le biais d'actions qui peuvent être accidentelles, malveillantes ou intentionnelles. [14]

Dans ce qui suit, nous présenterons les différentes étapes, les types et Quelques techniques d'attaque.

I.13.1 Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma [I.11] :

- **Identification de la cible :** Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS1, ... :
- **Le scanning :** L'objectif est de compléter les informations réunies sur une cible visées, il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall. . .). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entrainer la défaillance de certains systèmes.
- **L'exploitation :** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.
- **La progression :** Il est temps pour l'attaquant de réaliser ce pourquoi il a franchi les précédentes étapes. Le but ultime étant d'élever ses droits vers root (administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces, . . .)

I.13.2 Les différents types d'attaques

Il existe trois types d'attaques [15] :

- **Attaque directe :** C'est la plus simple des attaques. Le hacker attaque directementsa victime à partir de son propre ordinateur. La figure 1 illustre l'attaque directe.

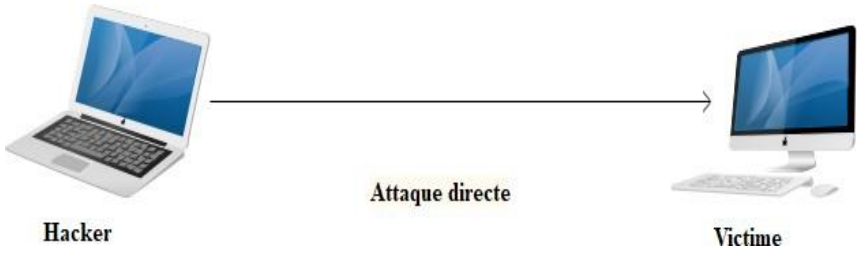


Figure I.11: Attaque directe.

- **Attaque indirecte par rebond :** Cette attaque est très prise des hackers, car le principe est simple, les paquets d'attaques sont envoyés à l'ordinateur intermédiaire, qui récupère l'attaque vers la victime. D'où le terme de rebond qui permet de :

- Masquer l'identité (l'adresse IP) du hacker.
- Utiliser éventuellement les ressources de l'ordinateur intermédiaire, car il est plus puissant pour l'attaque.

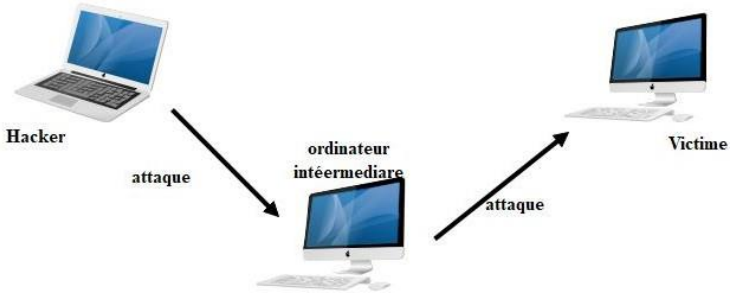


Figure I.12: Attaque indirecte par rebond.

- **Attaque indirecte par réponse :** Cette attaque est dérivée de l'attaque par rebond. Cependant au lieu d'envoyer une attaque à la machine intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête, cette dernière va être envoyée à la machine.

Figure I.13: Attaque indirecte par réponse.

I.13.3 Quelques techniques d'attaque

Les attaques réseau sont si effectuées de nos jours qu'il serait impossible de prétendre toutes les descriptions. Elles utilisent généralement les trois éléments essentiels d'un système :

- La couche réseau,
- Le système d'exploitation et la couche applicative, dès qu'une vulnérabilité exploitable est présente.

Voici quelques-unes des attaques les plus couramment utilisées [2] :

- **Le Flooding** consiste à envoyer à une machine de nombreux paquets IP de grosse taille, la machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.
- **Le smurf** est une attaque basée sur l'utilisation du ping (Packet Internet Groper) et des serveurs de diffusion. Dans cette attaque, on commence par falsifier notre adresse IP afin de se faire passer pour la machine cible. Ensuite, on envoie un ping vers un serveur de diffusion, qui le redistribuera à toutes les machines connectées, et chacune d'entre elles renverra un "pong" au serveur, qui le fera parvenir à la machine cible. En conséquence, la machine cible sera submergée par un grand nombre de paquets et finira par se déconnecter.
- **Man-in-The-middle** consiste à faire passer les échanges réseaux entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant parfaitement à chaque acteur de l'échange la réalité de son interlocuteur.
- **Le craquage de mots de passe** consiste à faire de nombreux essais pour trouver le bon mot de passe, soit en essayant toutes les possibilités qui sont faites dans l'ordre pour trouver la bonne solution (la méthode brute), soit en testant un mot pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci.

I.14Les éléments à sécuriser dans un réseau

Les réseaux sont composés d'une variété d'équipements d'un côté, et de connexions filaires ou sans fil qui les relient de l'autre. Certains de ces équipements peuvent être gérés par des logiciels spécifiques, et différentes sortes de données y sont considérables. Certaines de ces données peuvent être masquées en utilisant des protocoles connus sous le nom de protocoles de réseau.

Dans ce contexte, la sécurité englobe la protection du matériel, des logiciels, des données et des protocoles Avant de réaliser un système de sécurité, il faut spécifier d'abord les éléments à protéger. [15]

On dénombre trois types essentiels qui sont :

- **Matériel :** Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaires comme les répéteurs, commutateurs (switch), routeurs, serveur, modems, firewalls, etc. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble.
- **Programme :** les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels programmes gérant les différents mécanismes de réseaux. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là de services réseau tels que : DHCP, DNS, FTP, etc.
- **Données :** On distingue deux sortes de données, celles qui servent au fonctionnement du réseau comme les tables de routage, les bases de données de clients, les fichiers relatifs aux droits d'accès, etc. On trouve aussi des données qui ne sont pas en rapport avec le fonctionnement du réseau tels que : les documents et les archives

I.15 Les mécanismes de défense et de sécurité

La mise en œuvre des mesures de sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité. De nombreux mécanismes ont été développés pour assurer la sécurité, qu'il est souvent indispensable de combiner pour atteindre un niveau de sécurité suffisant, parmi lesquelles nous trouvons :

I.15.1 Firewalls (pare-feux)

Définition

Un pare-feu est un composant essentiel d'un réseau informatique, qu'il soit logiciel, matériel ou les deux, et joue un rôle indispensable dans la sécurité de tout système informatique. Son objectif est de protéger le réseau contre les intrusions provenant de l'extérieur. Ces dispositifs filtrent les paquets de données des différentes couches du modèle TCP/IP afin de contrôler leur flux et de les bloquer en cas d'attaques, qui peuvent se présenter sous différentes formes. Le filtrage réalisé par le pare-feu constitue le premier rempart de la protection du système d'information. Il est installé le plus souvent en périphérie du réseau local de l'entreprise

ce qui lui permet de contrôler l'accès des ressources externes vers l'intérieur mais également entre entités éloignés de l'entreprise mais reliées par un réseau de type extranet.

Leur utilisation permet de contrôler la connectivité des communications, une entreprise peut empêcher des accès non autorisés aux ressources et systèmes de son réseau local et plus précisément pour ses environnements les plus sensibles. [4]

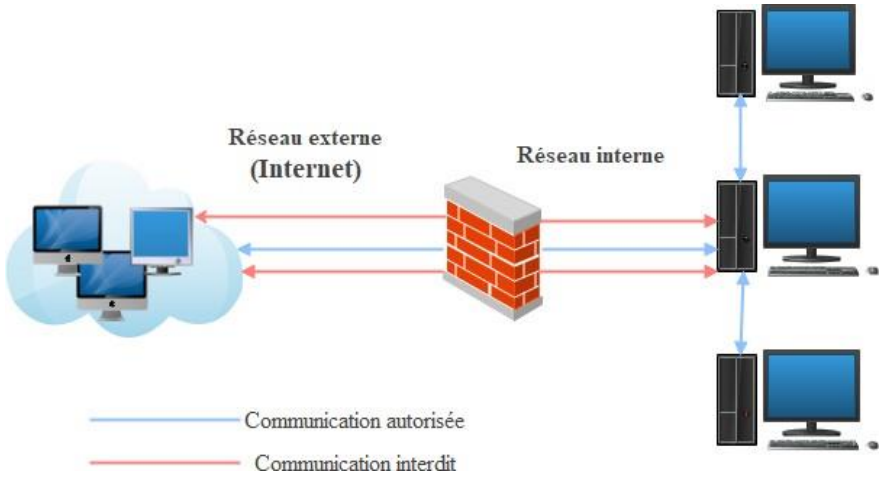


Figure I.14: Pare-feux.

Principe de fonctionnement

- **Le filtrage statique :** c'est le filtrage le plus simple. Un pare-feu qui fonctionne selon ce mode de filtrage inspecte les entêtes de chaque paquet qui le traverse et décide selon la politique de sécurité de le laisser passer ou de le supprimer et ce sans tenir compte des autres paquets.
- **Le filtrage applicatif :** Cette technique a été proposée pour palier à certaines limites de pare-feux utilisant le filtrage simple. L'idée est de conserver les traces de sessions et de connexions dans les tables d'états internes aux pare-feux. Ces traces seront également prises en considération par les pare-feux lors de prises de décisions. Ces informations augmentent considérablement les capacités des pare-feux à détecter des attaques sophistiquées.
- **Le filtrage dynamique :** est souvent associé à un type de pare-feu appelé passerelle applicative ou proxy. Un serveur proxy agit comme un intermédiaire au niveau des applications, rendant les machines internes invisibles depuis l'extérieur. Il permet la suppression des en-têtes précédant le message applicatif, ce qui offre un niveau supplémentaire de sécurité. Bien que les serveurs proxy soient le plus souvent utilisés pour le web (comme les proxys HTTP), il existe également des serveurs proxy adaptés à chaque protocole applicatif spécifique.

I.15.2 La DMZ

La DMZ (DeMilitarized Zone) est un environnement de sous-réseau positionné entre un réseau interne de confiance et un réseau externe non sécurisé. Les serveurs installés dans la partie externe de la DMZ permettent de fournir des services aux réseaux externes, tout en protégeant le réseau interne contre des intrusions possibles.

La figure (II.14) ci-après montre l'exemple d'un environnement composé d'une DMZ interne et externe avec plusieurs serveurs et des périphériques de détection d'intrusion. Dans cet exemple, le serveur VPN est combiné avec le pare accessibles de l'extérieur sont positionnés aussi sur la DMZ externe. Tous les autres serveurs internes sont situés dans la DMZ interne, protégés à la fois des menaces internes et externes. [16]

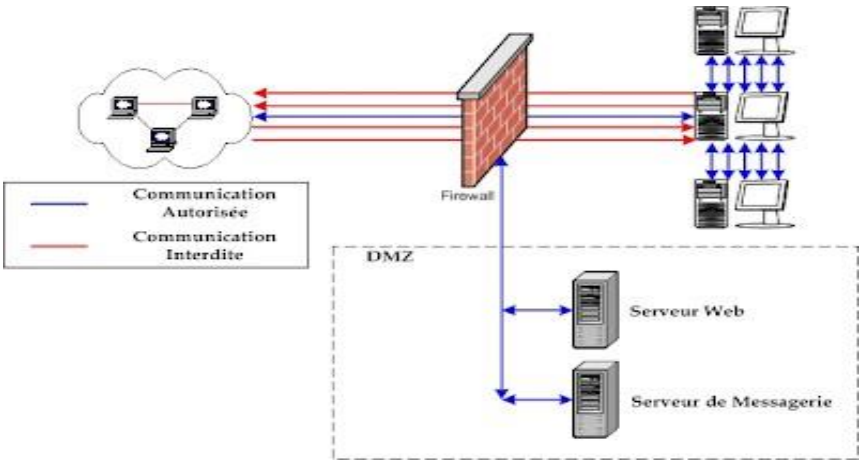


Figure I.15: La DMZ.

I.15.3 La technologie AAA

Nous évoluons dans un environnement où la protection est essentielle, que vous occupiez un poste d'administrateur système, de responsable, d'ingénieur réseau ou que vous soyez étudiant. Lorsque nous nous connectons à un réseau, nous sommes constamment exposés à ces trois aspects. [17]

- **Authentification :** il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assurée au moyen d'un secret partagé ou d'un logiciel approuvé.
- **Autorisation :** elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assure qu'il est autorisé à accomplir les actions qu'il demande, tels que l'accès à des fichiers, le droit d'écrire, etc. l'autorisation est gérée au moyen de liste ACL ou de stratégie.
- **Traçabilité :** elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

I.15.4 Les VLANs ACL

Définition

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

- L'adresse d'origine -L'adresse de destination.
- Le numéro de port.
- Les protocoles de couches supérieures.
- D'autres paramètres (horaires par exemple). Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers.

Elles sont ainsi associées à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certaines conditions faisant partie de la liste de contrôle d'accès. [16]

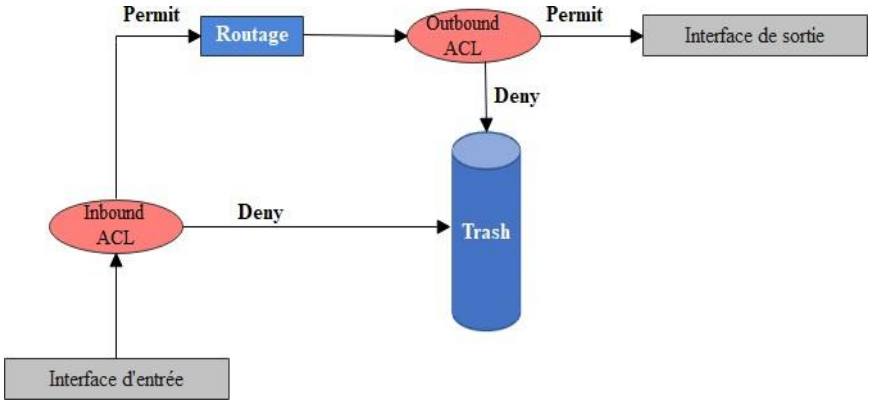


Figure I.16: Principe de fonctionnement des ACLs.

Les différents types d'ACL

Il existe 3 types de liste de contrôle d'accès : les ACLs standards, les ACLs étendues et les ACLs nommées.

- **Les ACLs standards** utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole. Les ACLs standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.
- **Les ACLs étendues** utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis. Les ACLs étendues sont à appliquer le plus proche possible de la source.
- **Les ACLs nommées** peuvent être soit standards, soit étendues ; elles n'ont pour but que de faciliter la compréhension et de connaître la finalité de l'ACL.

I.15.5 Proxy

Un système mandataire (Proxy) (Figure I.16) repose sur un accès à l'internet par une machine dédiée : le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales, et exécute les requêtes pour le compte de ces dernières.

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (http, FTP, SMTP, etc.) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, etc.).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés

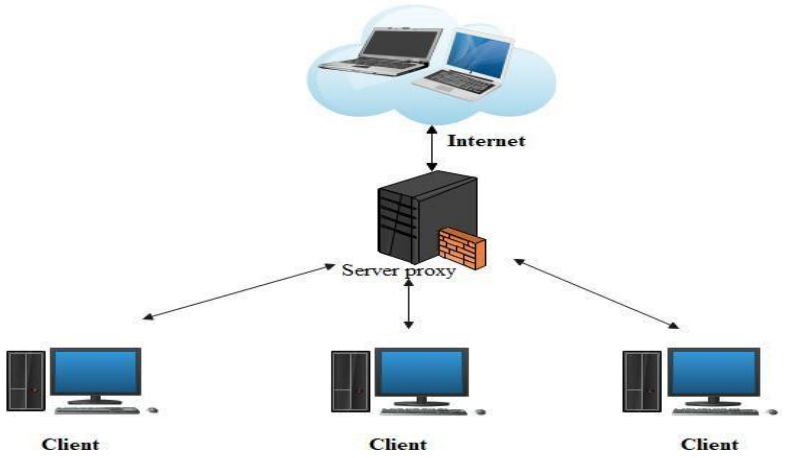


Figure I.17: Proxy**.**

I.15.6 Le Protocol IPSec

IPSec (Internet Protocole Security) est un protocole de niveau 3. Il est très utilisé lors de la création de réseaux privés virtuels et pour la sécurisation des accès distants à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour les échanges de données. IPSec s'insère dans la pile de protocoles TCP/IP au niveau d'IP. Ceci présente l'avantage de le rendre exploitable par les niveaux supérieurs et d'offrir un moyen de protection unique pour toutes les applications. [4]

IPSec distingue deux niveaux de protection à travers deux protocoles :

- **Authentification Header (AH)** qui ne prend en charge que l'authentification, le contrôle d'intégrité et l'anti-rejeu. Le rejeu est une technique, utilisable par un intrus, qui consiste à renvoyer des paquets capturés lors d'une communication réseau légale.
- **Encapsulating Security Payload (ESP)** qui ajoute la fonction de confidentialité.

I.15.7 Système de détection d'intrusion (IDS)

Les outils de détection d'intrusion viennent compléter les fonctions du pare-feu. Au travers d'une surveillance de l'identité des requêtes en circulation sur le réseau, ces outils sont à même de repérer les requêtes malintentionnées, de repérer les intrus dans le flot du trafic courant transitant par les ports de communication laissés ouverts par le pare-feu.

Les systèmes de détection sont conçus pour informer des accès non autorisés ou des intrusions dans les réseaux. Les pare-feux qui opèrent avec les systèmes de détection d'intrusion sont capable de détecter automatiquement les menaces venant de l'extérieur, plus rapidement qu'une vérification par un opérateur.

Il existe deux types de détection d'intrusion :

- Le premier système, basé sur l'hôte, doit être installé sur chaque machine à protéger. Il est, en général, intégré au système d'exploitation qu'il protège. Ce types d'IDS sont prévus pour la détection des menaces à un haut niveau de sécurité.
- Le premier système, basé sur le réseau, est implémenté en tant qu'analyseur intelligent de protocole. Ses composants surveillent le trafic réseau au niveau physique. [4]

Conclusion

En conclusion, les réseaux et la sécurité sont deux éléments indissociables dans notre monde numérique en constante évolution. La sécurisation des réseaux est essentielle pour protéger les informations sensibles, prévenir les attaques et maintenir la confiance des utilisateurs. En adoptant des mesures de sécurité appropriées, en restant à jour sur les meilleures pratiques et en sensibilisant les utilisateurs aux risques, nous pouvons créer un environnement numérique plus sûr et fiable. La collaboration continue entre les professionnels de la sécurité, les entreprises et les utilisateurs est cruciale pour faire face aux défis et garantir la protection des réseaux dans le futur.

Après avoir discuté les principaux points de ce chapitre, nous allons passer à une autre partie « Présentation de l'organisme d'accueil », où nous présentons l'entreprise de Campus-NTS, son créations et situation géographique, son organisation et ses équipements.

Chapitre II
Présentation de l’organisme d’accueil

***Chapitre II** : Présentation de l'organisme d'accueil*

Introduction

Ce chapitre sera réservé à la présentation du campus NTS (New Technology § Solutions) où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecteur réseau de son client « ngtmeziani » et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

Partie 1 : Présentions de l'entreprise « Campus NTS »

II.1 Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été créé en 2020 à Bejaia par Yassine djebbari, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- La technologie.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (targa ouzamour, 17 octobre...etc).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

II.2 La localisation de l'entreprise

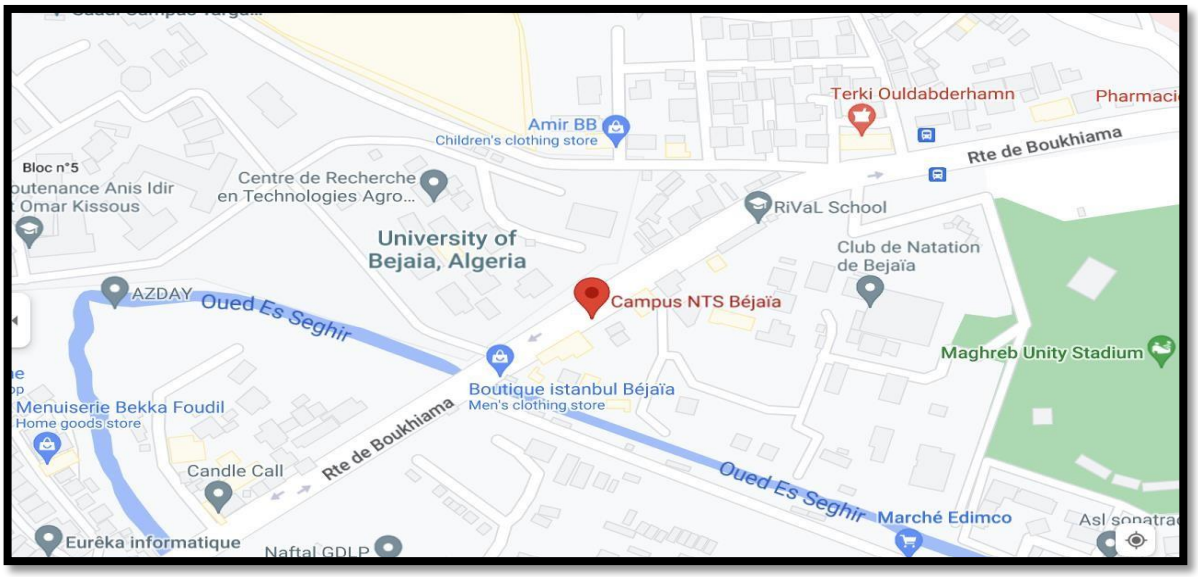


Figure II.1 : Localisation de l'entreprise NTS. [32]

II.3 Fiche technique

Le tableau 1 ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude.

Dénomination	**Campus NTS**
Logo	
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http://www.campus-nts.com/

Tableau II.1 : Identification sur campus NTS. [32]

II.1 Objectifs, Missions et activités de l'Entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentées dans la figure 2 :

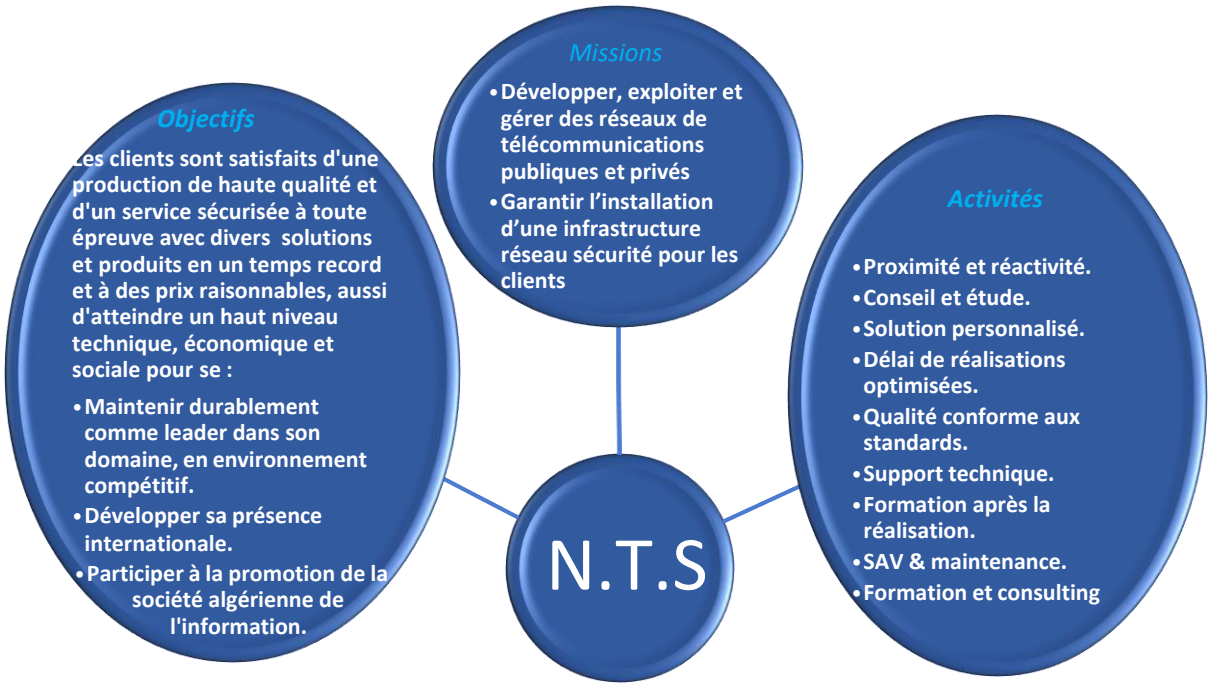


Figure II.2 : Objectifs, Missions et Activités de l'NTS. [32]

II.2 Organigramme général de l'organisme d'accueil

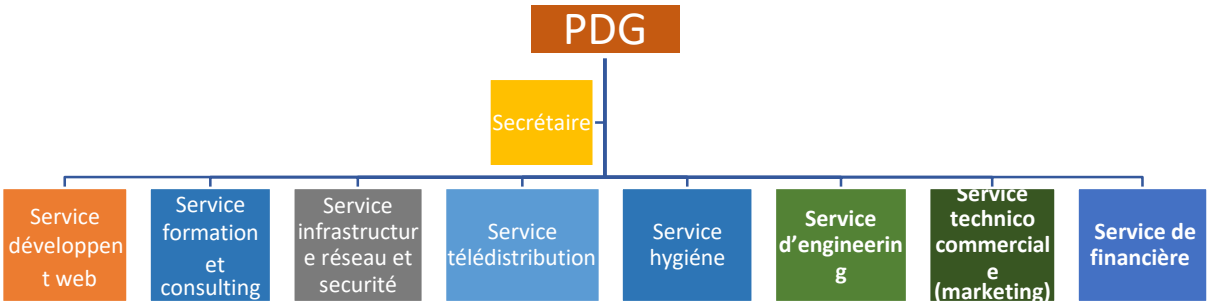


Figure II.3 : L'organigramme de campus NTS. [32]

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS (voir la figure 3) dans lequel cet apprentissage termine le stage :

A. Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des

langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

B. Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, C#, Java, Python…etc.).
- Electricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP S&R.
- Virtualisation.
- Microsoft server, SQL.
- Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

C. Service d'accueil

❖ **Présentation de service infrastructure réseau et sécurité**

L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de

l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

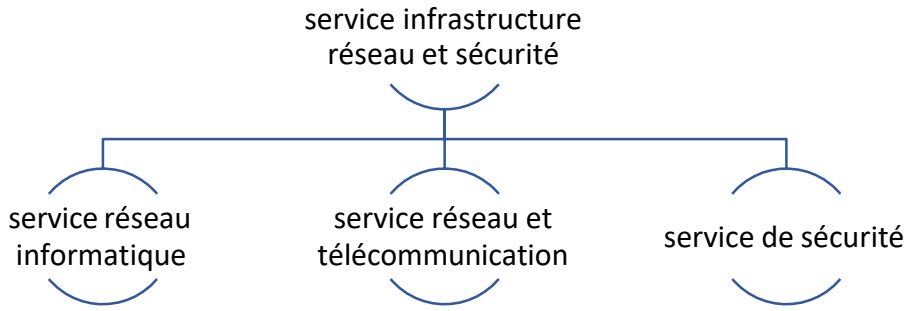


Figure II.4 : Organigramme de service d'accueil. [32]

❖ **Service réseau informatique :**

Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :

Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

❖ **Service réseau et Télécommunication :**

Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici des exemples de services d'infrastructure de télécommunications :

- Pose de fibre optique.
- Emplacement du site de la tour cellulaire.
- Test d'antenne radio.
- Installation d'équipements téléphoniques standards et réseau de données.
- Téléphonie standard

❖ **Service de sécurité**

Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources.

Les services qu'elle réalise sont les suivants :

- Caméras de surveillance
- Alarme anti- intrusion
- Détection incendie
- Pointeuse et Contrôles d'accès
- Vidéophonie

D. Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.
- Services interactifs.
- Programmation locale.

E. Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.

L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

F. Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

G. Service de financière

Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

- **Les tâches principales du Service des finances :**

- Assurer une saine gestion des ressources financières de l'entreprise par la planification.
- La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
- La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

- **Le rôle du service financier :**

- La préparation et du suivi des budgets de fonctionnement et d'investissement.
- La préparation des états financiers.
- La gestion de la trésorerie et de des encaissements.
- La rémunération des employés, des comptes à payer.
- De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
- La réception des marchandises et du courrier.

H. Service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :

- Des actions de prévention des risques professionnels et de la pénibilité au travail.
- La mise en place d'une organisation et de moyens adaptés.

Partie 2 : Etude des lieux du client « ngtmeziani »

ngtmeziani est une entreprise blessée à Alger spécialisé dans la distribution des systèmes, des vidéos survivance et alarmes.

II.3 Présentation du réseau « ngtmeziani »

Afin de bien comprendre les domaines dans lesquels un service informatique souhaite améliorer ses capacités et les besoins et contraintes d'information à respecter, nous examinerons un ensemble de spécifications pour l'infrastructure informatique et technique dont le service a besoin. Cette section contient tous les détails sur l'infrastructure réseau et matérielle.

II.4 Architecture réseau « ngtmeziani »

Le service informatique ngtmeziani a mis en place son réseau en choisissant une topologie en étoile pour relier ses différents équipements et ces sites distant comme le montre la figure suivante :

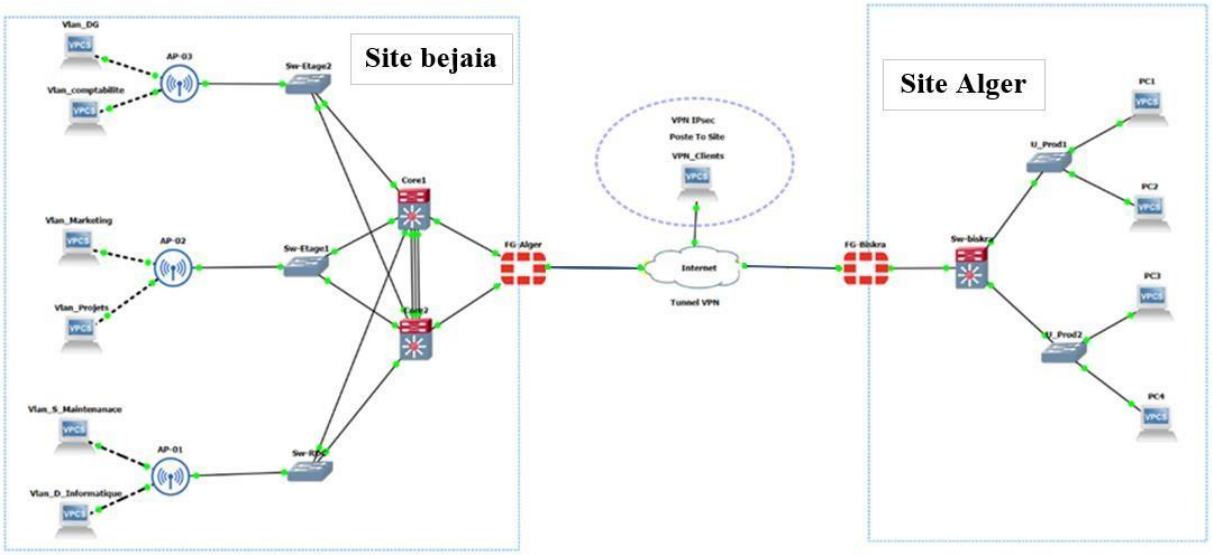


Figure II.5 : Architecture actuelle de réseau ngtmeziani.

A. Analyse du parc informatique

Les périphériques connectés dans sont : les ordinateurs, téléphones et les imprimantes

Le tableau suivant contient les statistiques des périphériques par service :

Services	Nombre d'hôtes	Type de connexion
Informatique	25	RJ45 ET WIFI
Maintenance ET SAV	08	RJ45 ET WIFI
Projets	10	RJ 45 ET WIFI
Marketing	18	RJ45 ET WIFI
Comptabilité	12	RJ45 ET WIFI
Direction Générale	04	WIFI

Tableau II.2 : Nombre de périphérique par service

❖ **Matériel utilisé :**

Les matériels utilisé dans le réseau sont :

- Firewall
- Switches Multicouche
- Switches d'accès
- Les Points d'accès
- Les ordinateurs et imprimantes
- Serveurs
- Prises RJ45
- Câbles à paire torsadée
- Câble à fibre optique pour les armoires

La figure suivante contient précisément le type de chaque équipement utilisé dans le réseau :

Nom de l'équipement	Le hardware (hard)	Software (soft)
Firewall 	FortiGate 1800F Series	FortiOS (Fortinet *Operating System)*
Switches Multicouche 	Cisco MDS 9000	IOS (*Internetwork Operating System)*
Switches d'accès Stackable (Empilable) 	Catalyst 9200 multigigabit 48 ports	IOS (*Internetwork Operating System)*
Les ordinateurs (Bureau et Portable) 	DELL PC Bureau : Optiplex 7080 MT PC portable : DELL LATITUDE 5300	Windows 10 et 11
Serveurs 	Serveur HPE ProLiant DL380 Gen10	ESXi Server Windows Server 2021 Linux server
Point d'accès 	***TENDA AC6***	unix

Tableau II.3 : L'environnement hardware et le software.

Partie 3 : Problématiques et Solutions proposées

II.8 Problématiques

Durant le stage effectué au niveau de service projet réseau et sécurité informatique pour le client « ngtmeziani », nous avons pu constater que ce client « ngtmeziani » possèdent de nombreux postes informatiques reliés entre eux par un réseau local filaire et sans fils.

Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et aussi de se connecter à l'internet.

- La plupart des ports de commutateur se trouvent sur le VLAN natif, ce qui risque d'augmenter les domaines de diffusion et de compromettre la sécurité. Contredit, l'objectif de l'utilisation des VLAN, qui est de micro-segmenter le réseau en petits domaines de diffusion.
- Les adresses IP changées entre les sites de l'entreprises ne sont pas masquées.
- La société s'étend à des sites distants et à plusieurs centres de distribution. Il dispose donc d'un réseau important et nécessite une interconnexion permanente fiable et privée entre ces différents sites.
- Leur réseau manque de plusieurs configurations et technologies :
    1. Technologie d'agrégation de liens pour augmenter la bande passante.
    2. Technologie de redondance a premier saut.
    3. L'équilibrage de charge et clustering.
- L'absence de supervision donc on peut avoir des pannes

II.9 Solutions

L'objectif principal de notre étude est la mise en œuvre d'une solution d'administration et d'authentification qui nous permet de mieux gérer et sécuriser l'accès aux services réseaux de « ngtmeziani », pour cela nous avons opté pour les solutions suivantes : à savoir :

- Les VLANs réduisent les domaines de diffusion et améliorent la sécurité du réseau.
- VLAN privé sont de fournir une nouvelle méthode pour bloquer le trafic entre les ports du même VLAN. Les utilisateurs n'ont pas besoin d'activer l'isolation des ports pour atteindre l'objectif, qui est de sécuriser le réseau sur le site.
- Mettre en place une solution de pare-feu grâce à sa fonction de configuration, selon les besoins d'accès et de filtrage au réseau Internet, les utilisateurs sont répartis en groupes.

Ports sécurisés, utilisés pour filtrer et limiter le nombre d'adresses MAC autorisées à se connecter aux ports des commutateurs Cisco. Établir un lien VPN entre les sites de Béjaïa et d'Alger.

- Placez une zone démilitarisée (DMZ) qui aidera les entreprises à détecter et à corriger les failles de sécurité avant qu'elles n'atteignent le réseau interne où sont stockées les ressources les plus précieuses.
- Le protocole HSRP intégré, fournit une redondance pour tous les périphériques réseau, c'est-à-dire que si le chemin actif rencontre une erreur, un autre chemin sera ouvert.
- Mise en œuvre de la technologie Etherchannel conçue pour augmenter la vitesse et tolérance aux pannes entre les commutateurs, les routeurs et les serveurs.
- Surveillance de bon fonctionnement des équipements, de système et d'activités en utilisant Zabbix

Conclusion

Dans ce chapitre, nous avons donné un aperçu général de l'entreprise du campus NTS et son Client ngtmeziani, puis nous avons découvert un problème qui nous a amenés à rechercher de mettre en œuvre une architecture qui puisse améliorer la sécurité des réseaux sans fil.

Dans le chapitre suivant, nous allons présenter le service de l'administration et sécurité des réseaux avancé, pour gérer les comptes utilisateurs et sécuriser en générale le réseau de l'entreprise.

Chapitre III
Administration et sécurité des réseaux avancé

***Chapitre III** : Administration et sécurité des réseaux avancé*

Introduction

L'administration des réseaux avancés implique la mise en place, la configuration et la gestion de l'ensemble du réseau. Cela comprend des tâches telles que la planification de l'architecture du réseau, l'installation de matériel et de logiciels, la configuration des équipements réseau (routeurs, commutateurs, pare-feu), ainsi que la gestion des adresses IP et des noms de domaine. Les administrateurs réseau sont responsables de la surveillance des performances du réseau, de la résolution des problèmes de connectivité et de la mise en œuvre des mesures pour améliorer l'efficacité et la fiabilité globale du réseau.

Ce chapitre se concentre sur la sécurité des réseaux avancé. Nous examinerons d'abord l'architecture hiérarchisé des réseaux, puis nous examinerons les Vlans, les types et la gestion vlan. Ensuite, nous discuterons sur le protocol VTP et le réseau VPN, et enfin, nous étudierons l'agrégation des liens, la redondance en première saut, monitoring et nous terminons ce chapitre par une conclusion.

III.1 Modèle Campus

III.1.1 Modèle à deux couches Core-distribution, Access

L'architecture de distribution de noyau effondrée, présentée dans la figure 1, convient davantage aux réseaux de campus de petite à moyenne taille. Idéalement, elle est appropriée pour interconnecter jusqu'à trois blocs d'interruption fonctionnelle. Dans cette conception, les fonctions de base et de distribution sont combinées en une seule couche, offrant une solution efficace et pratique. [18]

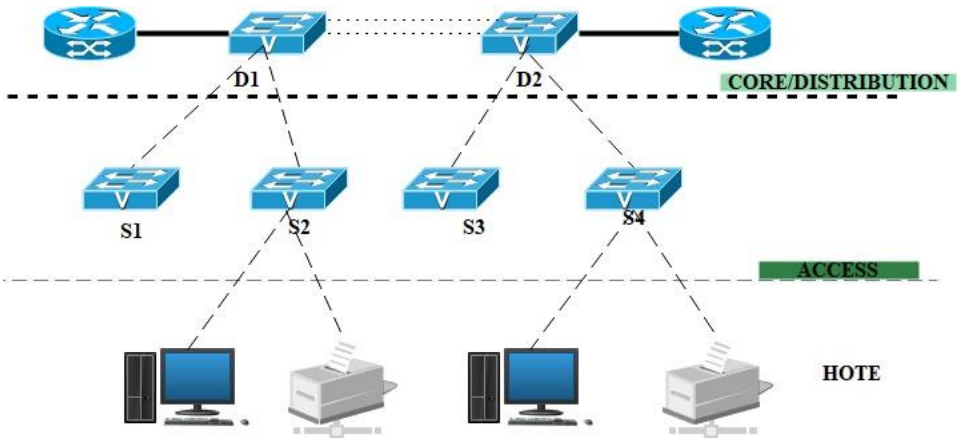


Figure III.1 : Modèle de conception de réseau à deux niveaux.

III.1.2 Modèle à trois couches Core, distribution, Access

Le modèle réseau hiérarchique le plus couramment utilisé de nos jours, que ce soit pour les réseaux locaux (LAN) ou étendus (WAN), est connu sous le nom de modèle à trois couches (noyau, distribution, accès), également appelé modèle hiérarchique en trois couches. Ce modèle, largement répandu grâce à Cisco, a été conçu pour offrir une structure organisée et efficace.

Le principe de ce modèle est simple : il consiste à créer un réseau avec une structure en trois couches, chacune ayant un rôle spécifique et impliquant des différences en termes de matériel, de performances et d'outils [18]. Les trois couches principales sont les suivantes :

- La couche cœur, « Coré layer »
- La couche distribution, « Distribution layer ».
- La couche accès, « Access layer ».

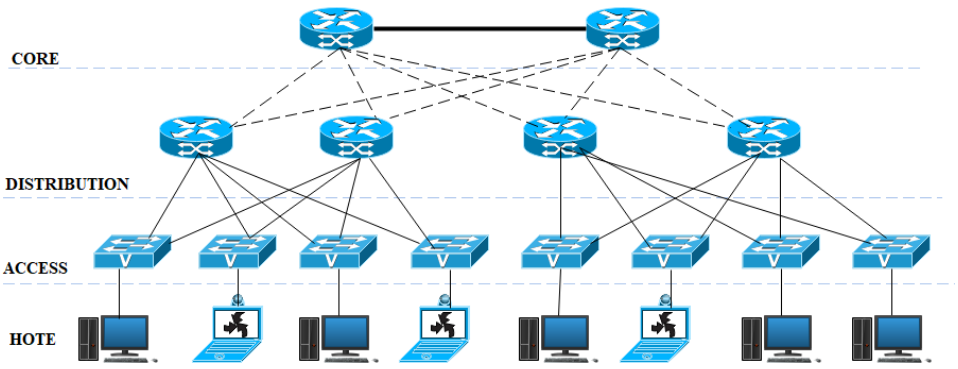


Figure III.2 : Architecture hiérarchisée en trois couches. [18]

A. Couche cœur :

C'est la couche supérieure. Son rôle est simple : relier entre les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société.

Nous trouvons généralement les routeurs ou des switches niveau à ce niveau. Le Core est aussi appelé Back Bône.

B. Couche distribution

Une fois nos routeurs/switches de la couche Core choisis et mis en place dans notre architecture, le designer s'intéresse à la couche Distribution.

Son rôle est simple : filtrer, router, autoriser ou non les paquets… Nous sommes entre la couche Core et la couche Access, c'est-à-dire entre la partie « liaison » et la partie « utilisateurs ». Ici, on commence à diviser le réseau en segment, en ajoutant plusieurs

routeurs/switches de distribution, chacun étant connecté au Core d'un côté, et à la couche Access de l'autre.

Ces routeurs de distribution vont s'occuper de router les paquets, d'y appliquer des ACLs, d'assurer la tolérance de panne, de délimiter les domaines de broadcast, etc…

C. Couche accès

C'est la dernière couche de notre modèle. Son rôle est simple mais très important : connecter les périphériques « end-users » au réseau.

Mais aussi, assurer la sécurité d'accès au réseau !

Ici, pas de routeur. Seuls des Switch, ou hubs parfois, sont implémentés. C'est normal, puisque tout le travail des routeurs est déjà effectué au niveau de la Distribution ou du Core.

Résultat, on ne s'occupe que de connecter nos end-users au réseau, que ce soit en Wi-Fi, Ethernet ou autre. Et si possible, on le fait de manière sécurisée, c'est-à-dire en utilisant switch port sur nos switches, en désactivant les interfaces non utilisées, etc…

III.1.3 Principes du modèle de réseau hiérarchique

Pour mettre en place correctement un réseau hiérarchique, il faut commencer par étudier la couche d'accès et définir les périphériques finaux. Pour les autres couches, il faut étudier ces éléments :

- **Les liens agrégés :** il faut identifier les ports permettant la liaison entre les commutateurs de chaque couche et surtout estimer les débits nécessaires et disponibles pour mettre en place les liens agrégés permettant d'augmenter la bande passante disponible.
- **Les liens redondants :** en plus des liens agrégés, il faut prévoir des liens redondants permettant d'assurer la continuité de service sur la couche de distribution et la couche cœur de réseau en cas de défaillance d'un commutateur sur ces couches. [19]

III.2 Centralisation

La centralisation d'une prestation implique la fourniture d'un service à l'ensemble de l'entreprise depuis un seul point central. En général, cela signifie que l'équipe responsable de la prestation opère exclusivement à un emplacement stratégique, tandis que les autres sites bénéficient du service à distance, par le biais du téléphone, d'une connexion Internet ou même, dans certains cas, par courrier postal. [19]

III.3 Active Directory et DNS, DHCP

III.3.1 Active Directory

Un Active directory est un rôle1 disponible sur Windows Server qui permet la mise en place d'un service d'annuaire (d'utilisateurs, d'ordinateurs, etc.), et de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows (ex : création de session individuelles), il permet également l'attribution et l'application de stratégies de groupe (Interdiction : de changer de fond d'écran, d'installation d'applications ou de paramétrage en tout genre). [20]

Active directory s'appuie sur le protocole le plus connu du domaine LDAP (Lightweight Directory Access Protocol) pour l'interrogation des bases de données Active Directory. Ce protocole fonctionnant en TCP/IP, Microsoft a dû utiliser cette pile de protocoles en standard et faire reculer au second plan ses protocoles historiques : NetBIOS, WINS, etc.

Les domaines qui utilisent les services Active Directory sont nommés domaines Active Directory. Si les domaines Active Directory ne peuvent fonctionner qu'avec un contrôleur de domaine, il convient de configurer plusieurs contrôleurs pour le domaine. Si un contrôleur tombe en panne, les autres prennent le relais pour gérer l'authentification et les autres tâches critiques. [21]

III.3.2 Active Directory et DNS

Il est indispensable pour un contrôleur de domaine Active Directory de pouvoir contacter un serveur DNS compatible. Lorsqu'un serveur Windows est transformé en contrôleur de domaine, il doit avoir un serveur DNS à sa disposition. Si aucun serveur DNS n'est pas trouvé sur le réseau, le service DNS est installé par défaut sur le nouveau contrôleur de domaine.

Pour Active Directory, l'importance de service DNS se situe à deux niveaux :

a) Pour qu'un client puisse se connecter à Active Directory, le DNS doit être disponible pour localiser le contrôleur de domaine. Le service NetLogon nécessite la présence d'un serveur DNS prenant en charge les RR SRV, ces derniers servant à enregistrer et à identifier les contrôleurs de domaine dans l'espace de noms DNS.

b) L'annuaire Active Directory peut stocker les informations de zone DNS et les propager dans l'entreprise. [20]

III.3.3 Active Directory et DHCP

Le service Serveur DHCP est intégrer dans Active Directory pour fournir l'autorisation pour les serveurs DHCP. Un serveur DHCP contrôleur de domaine ou membre d'un domaine Active Directory interroge Active Directory pour obtenir la liste des serveurs autorisés (identifiés par leur adresse IP). Si sa propre adresse IP ne figure pas dans la liste des serveurs DHCP autorisés, le service Serveur DHCP ne termine pas sa séquence de démarrage et se ferme automatiquement. [20]

III.4 Les Liaisons Virtuelles

III.4.1 Les réseaux locaux virtuels (VLAN)

Les VLANs offrent une solution efficace pour segmenter les réseaux locaux en plusieurs réseaux logiques, améliorant ainsi la sécurité, les performances et la gestion globale du réseau.

- **Définition**

Un VLAN (Virtual Local Area Network ou réseau local virtuel) est une méthode qui regroupe un ensemble de machines utilisant la technologie Ethernet au sein d'un même réseau local. Il permet de regrouper les éléments du réseau (utilisateurs, périphériques, etc.) en fonction de critères logiques tels que la fonction, le partage de ressources ou l'appartenance à un département, sans être limité par des contraintes physiques telles que la dispersion des ordinateurs ou un câblage informatique inapproprié. [22]

- **Type des VLANs**

On distingue généralement trois techniques pour construire des VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI

VLAN de niveau 1 ou VLAN par port

Chaque port des commutateurs est assigné à un VLAN. Ainsi, les ports sont statiquement attribués à un VLAN spécifique. Lorsqu'une station est déplacée physiquement, il est nécessaire de désaffecter son port du VLAN initial et d'assigner le nouveau port de connexion de la station au VLAN approprié.

De même, lorsqu'une station est déplacée logiquement (c'est-à-dire lorsqu'on souhaite la déplacer vers un autre VLAN), il est nécessaire de modifier l'affectation du port au VLAN correspondant. [22]

VLAN de niveau 2 ou VLAN MAC

Chaque adresse MAC est associée à un VLAN. En réalité, il s'agit d'affecter dynamiquement les ports des commutateurs à chaque VLAN en fonction de l'adresse MAC de

l'hôte qui émet à travers ce port. L'avantage principal de ce type de VLAN réside dans son indépendance par rapport à la localisation géographique.

Ainsi, si une station est déplacée physiquement sur le réseau, sa configuration MAC reste inchangée, ce qui lui permet de continuer à appartenir au même VLAN. Ce fonctionnement est particulièrement adapté à l'utilisation de machines portables. [22]

VLAN de niveau 3 ou VLAN d'adresses réseaux

Les VLANs sont attribués à des adresses de niveau 3. Ainsi, l'appartenance d'une trame à un VLAN est déterminée par l'adresse de niveau 3 (ou supérieur) qu'elle contient. En utilisant l'association adresse de niveau 3/VLAN, les ports des commutateurs sont affectés dynamiquement à chaque VLAN.

Dans ce type de VLAN, les commutateurs acquièrent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Cependant, ce mode de fonctionnement est moins rapide que celui du VLAN de niveau 2. On peut distinguer deux types de VLAN :

- **VLAN par protocole :** Le VLAN par protocole (en anglais Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.
- **VLAN par sous réseaux :** Les VLANs de niveau 3 permettent de regrouper plusieurs machines suivant le sous- réseau auquel elles appartiennent. La mise en place de VLAN de niveau 3 est conditionnée par l'utilisation d'un protocole routable (IP, autres protocoles propriétaires ...). L'attribution des VLANs se fait de manière automatique en décapsulant le paquet jusqu'à l'adresse source. Cette adresse va déterminer à quel VLAN appartient la machine (voir la figure ci-dessous).

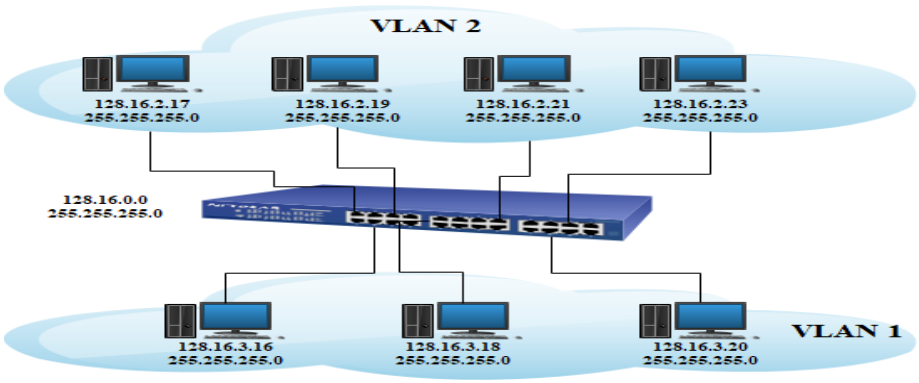


Figure III.3 : VLAN par adresse IP. [23]

Le tableau suivant montre quelques différences entre les trois techniques :

Types de VLANs	Description.
VLAN niveau 1 Basé sur le port	▪ Configuration la plus courante. ▪ Ports affectés individuellement à un ou plusieurs VLANs. ▪ Facile à mettre en place. ▪ Les interfaces de gestion des Switchs permettent une configuration facile.
VLAN niveau 2 Basé sur l'adresse MAC	▪ Rarement utilisé ▪ Difficile à administrer, à dépanner et à gérer.
VLAN niveau 3 Basé sur le protocole	▪ L'adresse IP (sous-réseau) détermine l'appartenance à un VLAN. ▪ Fréquence d'utilisation et simplicité la compliexité de mise en oeuvre.

Tableau III.1 : comparaison entre les 3 techniques.

- **Gestion des VLANs**

Il existe différents types de VLAN. Le type de trafic du réseau qu'ils portent définit un type particulier de réseau local virtuel et d'autre tirent leurs noms en raison de la nature ou une fonction spécifique du VLAN effectue. La section suivante d'écrit VLAN commun :

❖ **Vlan par défaut :**

Le VLAN 1 est un VLAN spécial qui joue un rôle particulier. Il est le VLAN par défaut pour tous les ports, y compris l'interface de gestion (SVI). De plus, plusieurs protocoles de couche 2 tels que CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol) et DTP (Dynamic Trunking Protocol) doivent obligatoirement transiter à travers ce VLAN spécifique. En raison de ces deux raisons, le VLAN 1 ne peut jamais être supprimé, il existe automatiquement et est essentiel au fonctionnement du réseau [24].

❖ **Vlan utilisateur :**

Ce type de VLAN est considéré comme un VLAN "normal" car il est configuré pour assurer une segmentation logique du commutateur dans le contexte de l'utilisation des VLAN. La numérotation des VLAN est disponible sur 12 bits, ce qui permet de créer et de gérer un

certain nombre de VLAN. Cependant, chaque modèle de commutateur a ses propres limites en termes de nombre total de VLAN pouvant être créés et gérés.

❖ **Vlan de gestion :**

Le VLAN de gestion est un VLAN spécifique assigné aux commutateurs afin de les rendre accessibles via une adresse IP. Cela permet d'utiliser des protocoles tels que ICMP, Telnet, SNMP et HTTP pour accéder aux commutateurs. Même s'il n'y a pas d'interface physique spécifiquement dédiée au VLAN de gestion, on peut toujours accéder au commutateur via une interface virtuelle (SVI) de type VLAN x, en utilisant son adresse IP.

❖ **Vlan natif :**

La notion de VLAN natif intervient uniquement lors de la configuration d'un port en mode trunk. Lorsqu'un port est configuré en tant que trunk, le commutateur étiquette les trames avec le numéro de VLAN approprié. Toutes les trames qui passent par un port trunk sont ainsi étiquetées, à l'exception des trames appartenant au VLAN natif. Par défaut, le VLAN natif est le VLAN 1 et ses trames ne sont pas étiquetées [24].

Ce VLAN natif est utilisé pour assurer l'interopérabilité avec le trafic qui ne prend pas en charge l'étiquetage (tagging). De plus, les protocoles de contrôle tels que CDP, VTP, PAgP et DTP sont toujours transmis via le VLAN natif. Si l'identifiant du VLAN natif est modifié, cette modification doit être effectuée sur tous les liens trunk, voire sur toute la topologie du réseau. [A]

❖ **Vlan Voice :**

Pour assurer une qualité de service (QoS) des communications vocales, le Vlan Voice se configure sur un port Access et crée une sorte de mini-trunk vers un téléphone IP. [A]

- **Les avantages des VLANs**

Ce mode de segmentation des réseaux locaux modifie entièrement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages. Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment :

❖ **Augmentation des performances :** La segmentation créée par les VLAN réduit la taille des domaines de broadcast et de ce fait le nombre de collisions sur ces domaines. De plus, les VLAN se basent sur la commutation (et non le routage) pour segmenter les domaines de diffusion ce qui permet un traitement bien plus rapide.

❖ **Réduction des coûts :** L'utilisation de VLAN permet de simplifier l'administration du réseau. A chaque fois qu'un utilisateur change de LAN, il faut modifier l'adresse du poste et certains paramètres des routeurs. Tandis que si un utilisateur change de lieu

physique mais pas de VLAN, il peut ne pas y avoir de modifications à faire (sous réserve de disposer de bons outils de gestion des VLAN). De plus, l'utilisation des VLAN entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches.

- **Formation de groupes virtuels :** Il est courant de retrouver, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, composés de membres qui viennent de différents départements (production, vente, etc.). Ces groupes sont souvent formés pour un temps défini et à courte durée. Dans ce cas de figure, un VLAN pourrait être implémenté (sans avoir à déplacer les individus) pour les besoins ponctuels de ce groupe et ce pour plusieurs groupes différents dans l'entreprise. Ce qui permet de créer des groupes de travail de manière transparente vis-à-vis de l'architecture physique du réseau.
- **Gain de sécurité :** Périodiquement, des données sensibles sont envoyées en broadcast sur le réseau par les machines (et plus particulièrement les serveurs). Les VLANs permettent d'isoler les serveurs dans un même domaine de broadcast et de les isoler par service. Les VLANs apportent donc une grande flexibilité dans la gestion des réseaux ; les utilisateurs pourront être regroupés selon leur centre d'intérêt. Les VLANs sont réalisés sur une architecture commutée et le concept de VLAN est applicable dans un même bâtiment, entre plusieurs bâtiments ou sur un réseau WAN. [26]

III.4.2 Les réseaux privés virtuels (VPN)

- **Définition**

Les VPNs est une technique permettant à un ou plusieurs postes distants de communiquer de manière sûre, tout en empruntant les infrastructures publiques, ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites et ce de façon simple et économique.

En d'autres termes, c'est un tunnel sécurisé permettent la communication entre deux entités y compris au travers des réseaux peu surs comme peut l'être le réseau Internet. Les VPNs ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics. [11]

- **Principe de fonctionnement**

Un VPN fonctionne selon un système de tunnelisation privé, c'est-à-dire qu'un tunnel est créé, à l'intérieur du quel transitent toute la communication et ou toutes les données transmises qui sont cryptées. Un VPN est très fermé, un utilisateur non autorisé, ne peut en

aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables.

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN. Ce sont ces protocoles qui sécurisent les données au moyen d'algorithmes de cryptographie, et qui leurs permettent de circuler en toute sécurité d'un bout à l'autre. [27]

- **Les types de VPNS [16]**

On peut dénombrer trois types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie :

- **VPN d'accès :** il permet à un utilisateur isolé de se connecter dans un réseau local interne. De ce cas, il peut avoir son propre client VPN afin de se connecter directement au réseau.

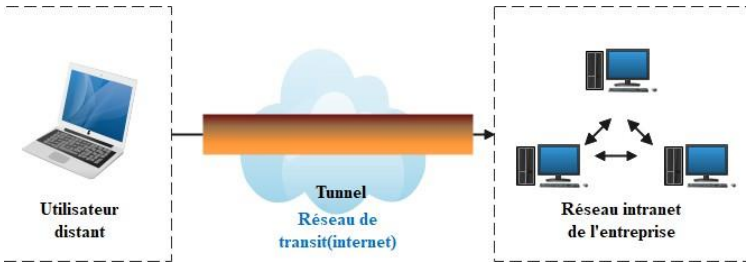


Figure III.4 : VPN d'accès.

- **Intranet VPN :** est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

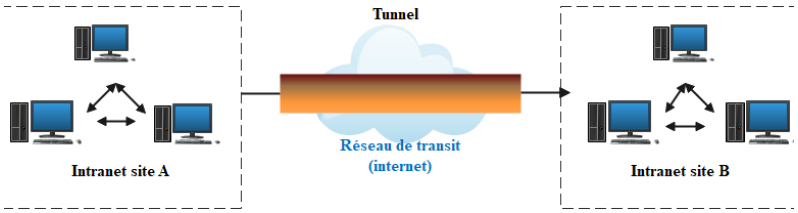


Figure III.5 : Intranet VPN.

- **Extranet VPN :** une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il

nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès.

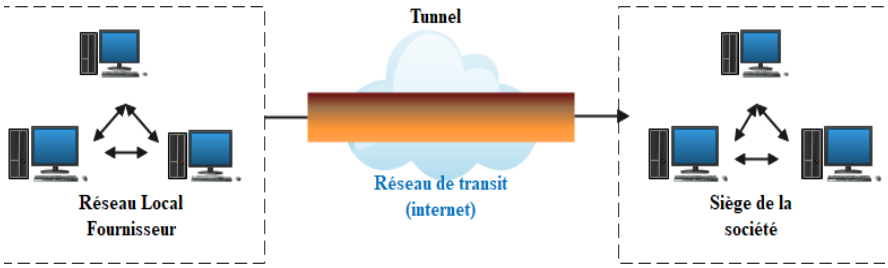


Figure III.6 : Extranet VPN.

- **Les avantage des VPN**

Les VPN présentent essentiellement deux avantages

✓ Les économies sur les budgets alloués à la connectivité. Ces économies sont obtenues en remplaçant les connexions longues distances via des lignes louées privées par une connexion unique à Internet sur laquelle on implémente des tunnels VPN afin de réaliser un réseau privé à travers Internet

✓ La flexibilité. Dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN d'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.

III.4.3 Les VLANs privée (Private Vlan)

Le Private VLAN a été inventé afin d'isoler les hôtes au niveau 2, Vous me direz que les VLAN standards font déjà cela, et vous aurez raison. Mais parfois, l'utilisation des VLAN devient abusive.

Imaginons le cas où nous avons 10 serveurs à connecter au réseau, et que ces serveurs ne doivent pas pouvoir discuter entre eux (cas typique d'une DMZ).

Ou encore que nous souhaitions faire un réseau invité, ou les machines ne peuvent joindre que la passerelle. Il nous faudrait alors 1 VLAN par machine. Il en découlera alors une création de très nombreux sous réseau, et un gaspillage d'adresse relativement important.

L'idéal serait d'avoir un VLAN (et donc un sous réseau), dans lequel les utilisateurs ne peuvent pas discuter.

C'est ce que permettent les PVLAN. PVLAN se compose d'une association de VLAN :

- Un VLAN **Primary**
- Un ou plusieurs VLAN **Secondary**

Le VLAN Secondary peut être de deux types :

- **Isolated :** les membres de ce VLAN ne peuvent pas communiquer entre eux.
- **Community :** les membres de ce VLAN peuvent communiquer entre eux.

Enfin, le port d'un switch peut fonctionner dans l'un des deux modes suivants :

- **Host :** Le port à un comportement qui découle du type de PVLAN auquel il est associé (Isolated ou Community).
- **Promiscuous :** le port peut communiquer avec les ports membres du même VLAN.

Voici un schéma représentant cela :

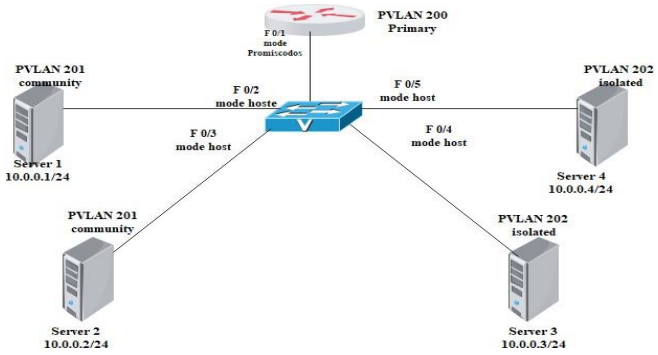


Figure III.7 : Private VLAN.

Commençons par le routeur. Il est dans le PVLAN primaire, et le port auquel il est connecté est en mode Promiscuous. Tout le monde sera donc capable de communiquer avec le routeur.

Les serveurs 1 et 2 sont dans un PVLAN du type Community et les ports auxquels ils sont connectés en mode Host.

Ces deux serveurs seront donc capables de communiquer entre eux, ainsi qu'avec le routeur.

Les serveurs 3 et 4 sont dans un PVLAN du type Isolated, et les ports auxquels ils sont connectés en mode Host.

Les deux serveurs ne pourront donc pas communiquer entre eux, mais seulement avec le routeur.

De plus, vous remarquerez que toutes les machines sont dans le même sous réseau. [26]

III.4.4 La redondance au premier saut

FHRP est un acronyme Cisco pour désigner les protocoles de redondance du premier saut (passerelle par défaut).

Les solutions de ce type permettent de combler le point unique de rupture que constitue la passerelle par défaut dans les réseaux locaux.

Les protocoles qui offrent ce service sont les suivants :

HSRP (propriétaire Cisco), VRRP (standard IETF similaire à HSRP), GLBP (propriétaire Cisco). [D]

Les protocoles de redondance offrent un mécanisme pour identifier le routeur qui doit prendre en charge le transfert du trafic et déterminer le moment auquel ce rôle doit être assumé par un routeur de secours. Le protocole HSRP définit un groupe de routeurs de secours, dont l'un est désigné comme routeur actif. VRRP est un protocole normalisé qui offre des fonctionnalités similaires. Le protocole GLBP est une solution Cisco propriétaire permettant la sélection automatique et l'utilisation simultanée de plusieurs passerelles disponibles. Il assure également le basculement automatique entre ces passerelles. [E]

- **HSRP ET VRRP, GLBP**

Tous les trois sont des protocoles de redondance du premier saut et des protocoles de couche réseau et sont utilisés pour fournir une redondance dans le réseau. La principale différence est que VRRP et HSRP sont des normes de l'industrie tandis que GLBP est un protocole propriétaire de Cisco. VRRP et HSRP ciblent un seul commutateur Ethernet de couche 3 ou un routeur pour qu'il soit actif dans un groupe, tandis que GLBP peut répartir la responsabilité entre jusqu'à quatre routeurs en configurant des schémas d'équilibrage de charge.

Il est principalement recommandé d'utiliser GLBP dans une configuration à quatre routeurs où l'équilibrage de charge est requis, le reste partout ailleurs HSRP ou VRRP est plus que suffisant pour faire fonctionne les choses. GLBP dispose également d'un mécanisme de pondération afin que le routeur principal obtienne la majorité du trafic, tandis que les autres routeurs équilibreront la charge. En fin de compte, cela dépend du support de votre fabricant. Si vous utilisez un routeur Cisco, vous pouvez configurer VRRP, HSRP ou GLBP, mais si vous avez un périphérique de fournisseur différent, vous êtes principalement bloqué avec HSRP ou bien VRRP dans ce cas. [F]

- **HSRP :** est un protocole standard permettant d'assurer la haute disponibilité de la passerelle d'un réseau. Ce protocole peut être mis en place sur un routeur ou un switch de niveau 3. Le but est qu'une éventuelle panne du routeur ne perturbe pas le routage. Le principe d'HSRP est relativement simple. Nous avons un groupe de routeur (en général 2), dans l'un d'eux est le routeur Actif. Le routeur de secours sera en Standby. Les autres en mode Listen. Le routeur actif assure le rôle de passerelle par défaut pour le sous-réseau. S'il vient à tomber en panne, le routeur standby prendra le relai. Puis un des routeurs Listen deviendra le nouveau Standby.
- **VRRP :** Remplit une fonction similaire à celle du HSRP, VRRP, cependant est une norme ouverte et définie dans la RFC 2338 de l'IETF. Comme HSRP, VRRP a des stations terminales qui utilisent un routeur virtuel comme passerelle par défaut. VRRP

est pris en charge pour les types de médias Ethernet ainsi que dans les VLANs et les VPN MPLS. [C]

- **GLBP :** Est un protocole propriétaire de Cisco. L'une des imitations de HSRP et VRRP est qu'un seul routeur du groupe HSRP est actif et peut transférer le trafic pour le groupe, le reste des routeurs restent inactif. Cisco a conçu GLBP pour résoudre ce problème. GLBP permet l'attribution dynamique d'un groupe d'adresses virtuelles à des stations terminales. [29]

III.5 Les protocoles de transport des VLANs

III.5.1 La norme 802.1Q et le Trunk des VLANs

La norme 802.1q date de décembre 1998. C'est un protocole Standardisé et interopérable. Le standard supporte les technologies IEEE 802.3 (Ethernet), IEEE 802.11 (WIFI), IEEE 802.5 (Token-Ring), etc., en tant que protocole de « pontage » (bridging, IEEE 802.1).

- **Etiquette 802.1q**

IEEE 802.1q ajoute une étiquette dans l'en-tête de la trame (un ensemble de champs juste après le champ d'adresse MAC d'origine). Cette étiquette a une taille de 4 octets ou 32 bits dont 12 bits sont consacrés au numéro de VLAN. Vu que la trame sera modifiée, le commutateur recalculera la valeur du champ CRC/FCS. [24]

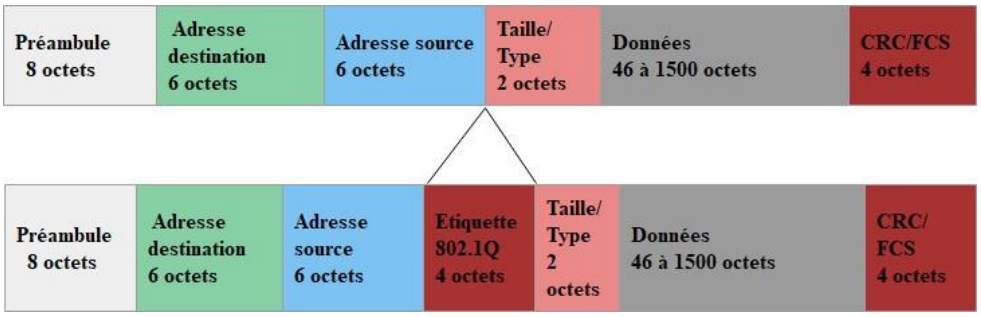


Figure III.8 : Etiquette 802.1q

La norme définit trois types de trames :

- **Les trames non étiquetées (untagged frame) :** une trame non étiquetée est une trame qui ne contient aucune information sur son appartenance à un Vlan.
- **Les trames étiquetées (tagged frame) :** une trame étiquetée est une trame qui contient un entête supplémentaire. Cet entête modifie le format standard d'une trame, notamment de la trame 802.3.
- Les trames étiquetées par une priorité (priority-tagged frame)

Le format de cette étiquette est illustré dans la figure 3.5 :

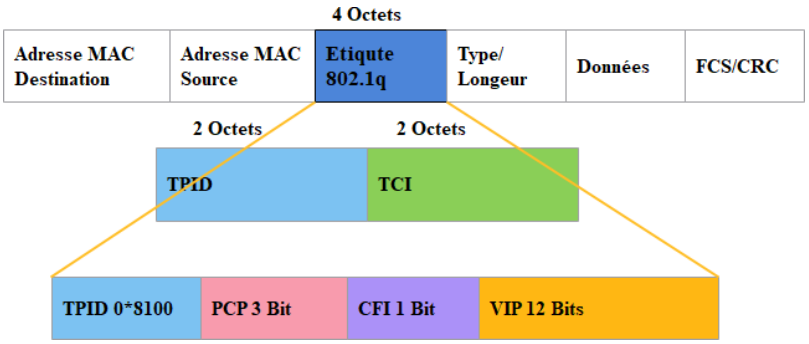


Figure III.9 : Format de l'étiquette 802.1q

Le champ Ethertype ou Tag Protocol Identifier (TPID), sur 16 bits, est utilisé pour identifier le type de la balise insérée. Pour le 802.1q la valeur est fixée à 0x8100.

Le champ TCI (Tag Control Identifier) de 16 bits est utilisé pour l'identification d'un control de l'étiquette. Il est comporte :

- Un champ priorité ou PCP (Priority Code Point) de 3 bits, qui est utilisé pour coder 8 niveaux de priorités d'un VLAN par rapport à l'autre.
- Un champ CFI (Canonical Format Indicator) sur 1 bit pour la compatibilité entre les adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe ce champ à 0 (si 1 la trame n'est pas propagée).
- Un champ VID (VLAN Identifier) sur 12 bits. Ce champ permet de définir l'appartenance d'une trame à un VLAN, la valeur maximale est de 4095 (Vlan 0 signifie que la trame n'appartient à aucun vlan).

III.5.2 La notion des trunks

Pour distribuer le réseau local virtuel on utilise des trunks. Un trunk est en fait la connexion physique sur laquelle transitent les trames de plusieurs VLANs. Ces trames sont identifiées par le VID afin d'arriver à bon port. On peut placer un trunk entre deux commutateurs, entre un commutateur et un hôte supportant le trunking et enfin entre un commutateur et un routeur pour effectuer un routage inter-VLAN. Il ne faut pas oublier que les VLANs transitant sur un même trunk se partagent la bande passante, c'est pourquoi il est recommandé d'utiliser des connexions à débit important, comme du Gigabit Ethernet ou de la fibre optique dans le meilleur des cas. Ce schéma ci-dessous (Figure 3.6) nous illustre la liaison de trunk entre deux commutateurs

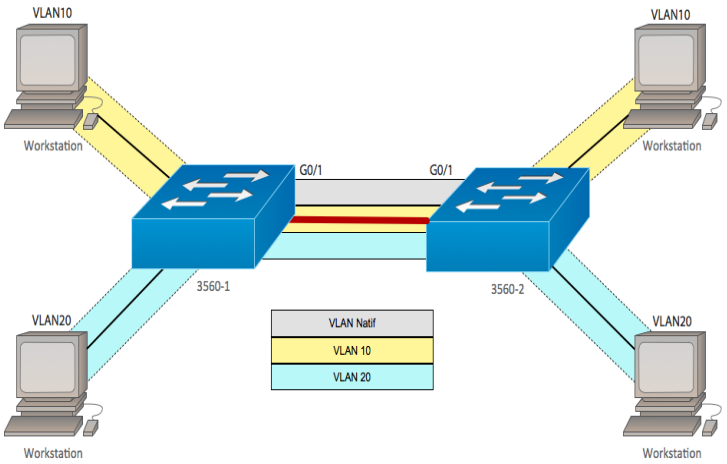


Figure III.10 : Utilisation du trunk entre deux commutateurs.

III.6 Quelques protocoles d'administration et de gestion des VLANs

III.6.1 Le protocole VTP (VLAN Trunking Protocol)

Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP. Ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs. [25]

- **Comprendre le VTP (VLAN Trunking Protocol)**

Un commutateur doit alors être déclare en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifie ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créent sur le commutateur serveur.

La mise en place d'un domaine VTP permet de centraliser la gestion des VLANs, ce qui peut s'avérer plus que plaisant dans un environnement abondamment commuté et comprenant de multiples VLANs. Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

- **Mode serveur :** dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.
- **Mode client VTP :** dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.
- **Mode transparent,** dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci-dessous.

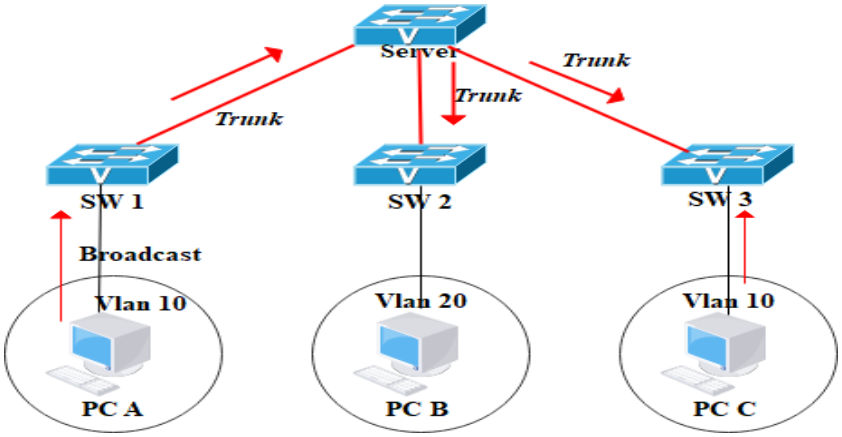


Figure III.11 : Fonctionnement du protocole VTP [14].

Les administrateurs peuvent changer les informations des VLAN sur les switchs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées `a tout le domaine VTP au travers des liens ”trunk”. En mode transparent, les modifications sont locales mais non distribuées. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP. Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée. Quand un nouveau switch est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

III.7 L’agrégation des liens et IEEE 802.3ad

III.7.1 L’agrégation des liens

La redondance et l’agrégation sont deux techniques essentielles en environnement SAN. La première technique vous donnera la continuité d’accès au stockage malgré la perte d’un élément du réseau tandis que la deuxième multipliera la vitesse des liens agrégés.

Il existe plusieurs protocoles dans le monde des réseaux Ethernet comme le LACP-norme IEEE 802.3ad, EthernetChannel chez Cisco et le Trunking qui peuvent grandement optimiser et sécuriser les environnements iSCSI au niveau des commutateurs.

L’agrégation des liens permet à plusieurs liens distincts d’être vu comme un seul et même lien et permet d’obtenir une bande passante démultipliée mais aussi une redondance et une répartition de charge sur ce groupe de liens. Généralement le Trunking (configuration statique) est couplé à LACP. [28]

III.7.2 IEEE 802.3ad

IEEE 802.3ad est une standardisée d'agrégation de liens qui permet de combiner plusieurs cartes Ethernet en un seul adaptateur virtuel, fonctionnant de manière similaire à EtherChannel. Cette agrégation de liens offre une capacité de bande passante accrue et une redondance en cas de défaillance.

Prenons l'exemple d'une agrégation de liens IEE 802.3ad dans laquelle les interfaces ent0 et ent1 sont regroupées pour former une seule interface appelée ent3. L'interface ent3 est ensuite configurée avec une adresse IP. Le système traite ces adaptateurs agrégés comme s'ils formaient un unique adaptateur, ce qui permet de configurer une adresse IP sur eux de même manière que sur n'importe quelle carte Ethernet individuelle.

Le commutateur doit prendre en charge la norme IEEE 802.3ad pour permettre son utilisation. [C]

III.8 Les Protocoles de négociation EtherChannel

- **LACP ET PAgP**

PAgP offre les mêmes avantages de négociation que LACP. Les paquets LACP et PAgP sont échangés entre les commutateurs sur des ports compatibles avec EtherChannel. La principale différence réside dans leur prise en charge par les fabricants. LACP est un standard ouvert soutenu par la plupart des fabricants, tandis que PAgP est une fonctionnalité propre à Cisco et utilisée exclusivement entre les appareils Cisco.

Les protocoles LACP et PAgP sont similaires, mais ils diffèrent dans le mode de configuration et le mécanisme d'agrégation. LACP étant un protocole conforme à L'IEEE, est plus souvent utilisé pour regrouper les liens afin d'obtenir un débit maximal entre les armoires de câblage et les centres de données. Cependant, PAgP est également sollicité lorsque des équipements Cisco sont intégrés à votre réseau et que votre architecture réseau peut prendre en charge la négociation PAgP. [C]

LACP et PAgP prennent en charge deux modes de canal configurables par l'utilisateur comme indiqué dans le tableau :

Table PAgP et LACP Modes		
Mode	**Protocol**	**Description**
On	**Les deux**	**Le port est configuré pour faire partie du canal et n'envoie pas de trames PAgP ou LACP**
Auto	**PAgP**	**Un port devient membre d'un canal si l'autre commutateur l'initie. C'est le mode par défaut**
Désirable	**PAgP**	**Un port cherche activement à devenir membre d'un canal en envoyant des trames PAgP**
Passive	**LACP**	**Un port devient membre d'un canal si l'autre commutateur l'initie**
Active	**LACP**	**Un port cherche activement à devenir membre d'un canal en envoyant des trames LACP**

Tableau III.2 : Tableau de Modes PAgP et LACP

III.9 Load balancing (équilibrage de charges)

L'équilibrage de charge (parfois appelé répartition de charge ou en anglais load balancing) consiste à distribuer une tâche à un pool de machines ou de périphériques afin :

- ✓ De lisser le trafic réseau, c'est-à-dire de répartir la charge globale vers différents équipements.
- ✓ De s'assurer de la disponibilité des équipements, en n'envoyant des données qu'aux équipements en mesure de répondre, voire à ceux offrant le meilleur temps de réponse.

Ce type de mécanisme s'appuie sur un élément, appelé répartiteur de charge (en anglais load balancer) chargé de distribuer le travail entre différentes machines.

Il existe plusieurs façons de mettre en œuvre le load balancing :

- Grâce à un commutateur de niveau 4,
- Grâce à un serveur utilisant un algorithme de type Round-Robin. [30]

III.10 ZABBIX

Zabbix est une application libre de supervision des systèmes et des infrastructures IT. Elle permet de superviser les équipements réseau, les serveurs, les systèmes et les applications et les logiciels (il fait la supervision technique et applicative).

L'architecture se compose de trois éléments :

- ❖ **Le premier,** un serveur représentant le cœur de l'application Zabbix, centralise les données ainsi que toutes les informations de configuration et permet d'alerter les administrateurs en cas de problème.
- ❖ **Le deuxième** est une interface web permettant la visualisation des informations stockées dans la base, mais également la configuration des objets de supervision.

- **Le troisième** élément et qui tournent en arrière-plan, et communiquent régulièrement avec le serveur Zabbix. [31]

Conclusion

L'administration et la sécurité des réseaux avancés sont des éléments clés pour garantir la protection et le bon fonctionnement des systèmes informatiques. Les administrateurs de réseaux ont pour responsabilité de mettre en place et de maintenir des mesures de sécurité pour protéger les données sensibles et les systèmes informatiques contre les menaces malveillantes. Ils doivent également surveiller les activités du réseau pour détecter les vulnérabilités et les attaques potentielles.

En outre, la gestion efficace des réseaux permet d'assurer la disponibilité et la performance des systèmes informatiques, ce qui est crucial pour les entreprises et les organisations.

Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

Chapitre IV
Réalisation et Test

***Chapitre 4** : Réalisation et Test*

Introduction

Dans ce chapitre, nous procéderons à la présentation des divers outils à utiliser et à l'environnement de travail requis. Nous aborderons également les exigences relatives à l'installation et à la configuration. En outre, nous examinerons les différentes étapes essentielles pour mettre en œuvre la solution proposée dans le chapitre 2.

IV.1 L'architecture proposée

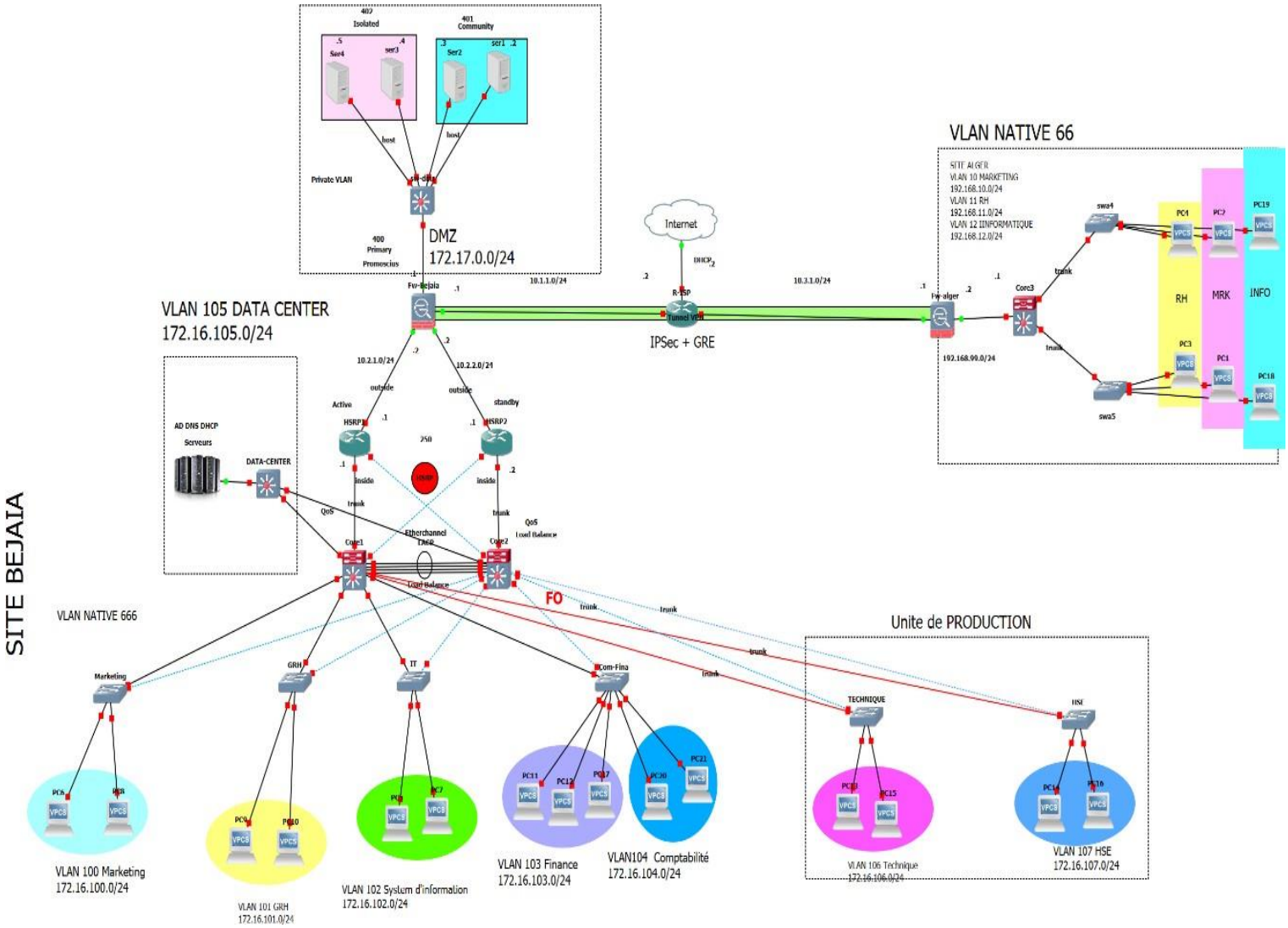


Figure IV.1 : Architecture proposée pour le client « ngtmeziani »

IV.1.1 Tableau d'adressage des équipements

Equipments	Interfaces réseau	Adresse IP
Pare feu Bejaia	WAN	10.1.1.1/24
	LAN1	10.2.1.2/24
	LAN2	10.2.2.2/24
	DMZ	172.17.0.1/24
Pare feu Alger	WAN	10.3.1.1/24
	LAN	192.168.99.2/24
Routeur HSRP1	Ethernet 0/0	
	Ethernet 0/2	10.2.1.1/24
Routeur HSRP2	Ethernet 0/0	
	Ethernet 0/2	10.2.2.1/24

Table IV.1 : Tableau d'adressage des équipements

4.1.1 Tableau d'adressage des VLANs et routage inter vlan :

Nom du VLAN	**ID du VLAN**	**Adresse du sous-réseau**	**Passerelle du sous-réseau (HSRP1)**	**Passerelle du sous-réseau (HSRP2)**	**Passerelle virtuelle**
VLAN Marketing	100	172.16.100.0 /24	172.16.100.1	172.16.100.2/24	172.16.100.250
VLAN GRH	101	172.16.101.0 /24	172.16.101.1	172.16.101.2/24	172.16.101.250
VLAN System d'nformation	102	172.16.102.0 /24	172.16.102.1	172.16.102.2/24	172.16.102.250
VLAN Finance	103	172.16.103.0 /24	172.16.103.1	172.16.103.2/24	172.16.103.250
VLAN Comptabilité	104	172.16.104.0 /24	172.16.104.1	172.16.104.2/24	172.16.104.250
VLAN DATA-CENTER	105	172.16.105.0 /24	172.16.105.1	172.16.105.2/24	172.16.105.250

VLAN Technique	106	172.16.106.0 /24	172.16.106.1	172.16.106.2/24	172.16.106.250
VLAN HSE	107	172.16.107.0 /24	172.16.107.1/24	172.16.107.2/24	172.16.107.250
VLAN NATIVE	666	…	…	…	…

Table IV.2 : Plan d'adressage des VLANs et routage inter vlan.

4.1.2 Tableau d'adressage de VLANs privé et ports associés

Nom du VLAN	**ID du VLAN**	**Ports hosts**	**Ports promiscuous mapping**	**Adresses Private VLAN**
Primary	400	/	Ethernet 1/0	172.17.0.1/24
Community	401	Ethernet 0/0 Ethernet 0/1	Ethernet 1/0	172.17.0.2/24 172.17.0.3/24
Isolated	402	Ethernet 0/2 Ethernet 0/3	Ethernet 1/0	172.17.0.4/24 172.17.0.5/24

Table IV.3 : Plan d'adressage des sous(sous-réseaux) Private VLAN.

IV.2 Installation et configuration Active directory AD DS et DNS, DHCP

IV.2.1 Installation des rôles AD et DNS, DHCP

Pour ajouter des rôles, dans le tableau de bord on va cliquer sur Ajouter des rôles et des fonctionnalités, on va sélectionner le type d'installation puis on va choisir le serveur, en suite on va installer le serveur DHCP, DNS et Active Directory.

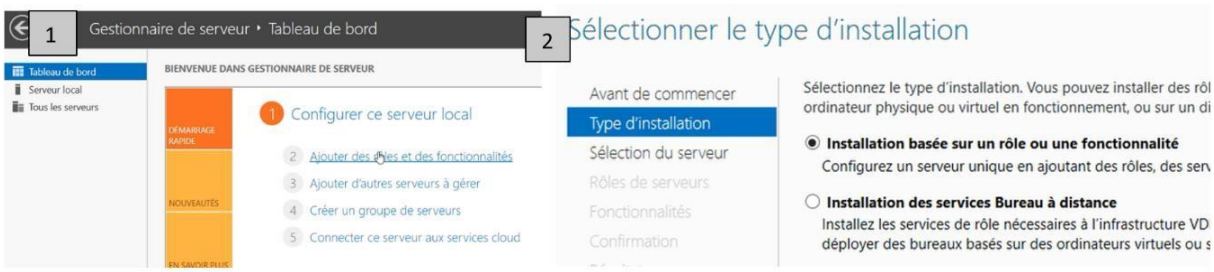


Figure IV.2 : Etapes d'installation des rôles (1)

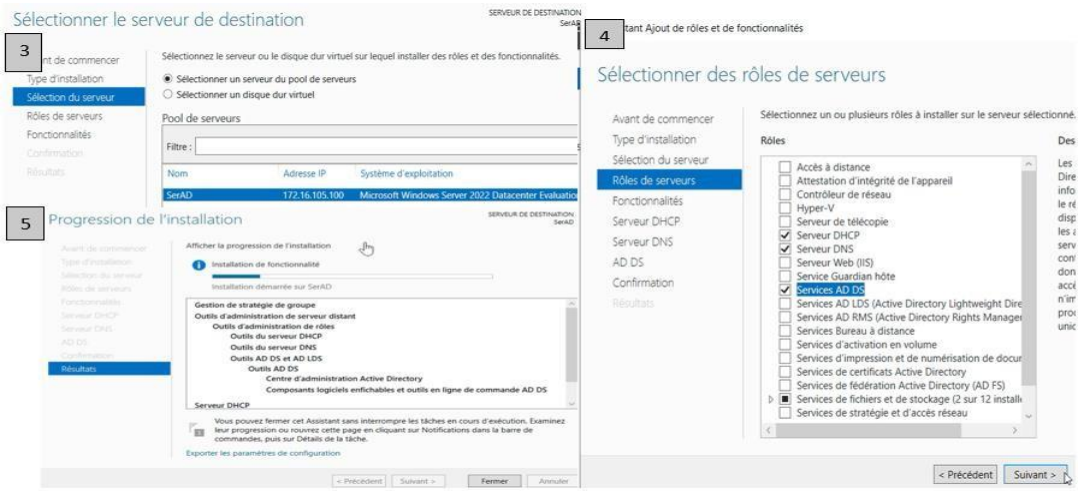


Figure IV.3 : Etapes d'installation des rôles (2)

Installation DHCP

On va finaliser l'installation du rôle DHCP aussi

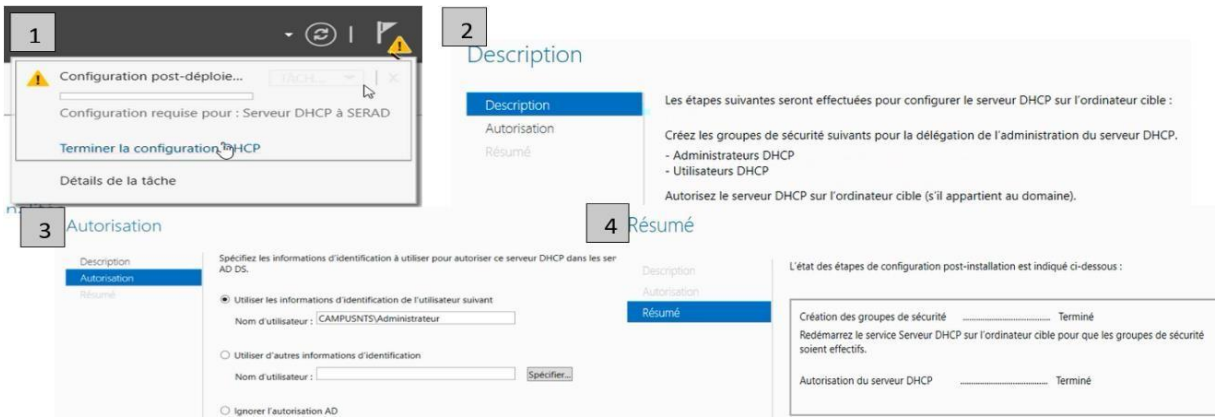


Figure IV.4 : Installation DHCP

IV.2.2 Configuration Active Directory et DNS

Pour promouvoir ce serveur en contrôleur de domaine donc on va créer une nouvelle forêt sous le nom de **campusnts.local**, après on va donner un mot de passe, il va faire une petite vérification en fin on va lancer l'installation donc il va installer DNS et appliqué les configurations qu'on a mis sur l'active directory, (afin de l'installation il a redémarré)

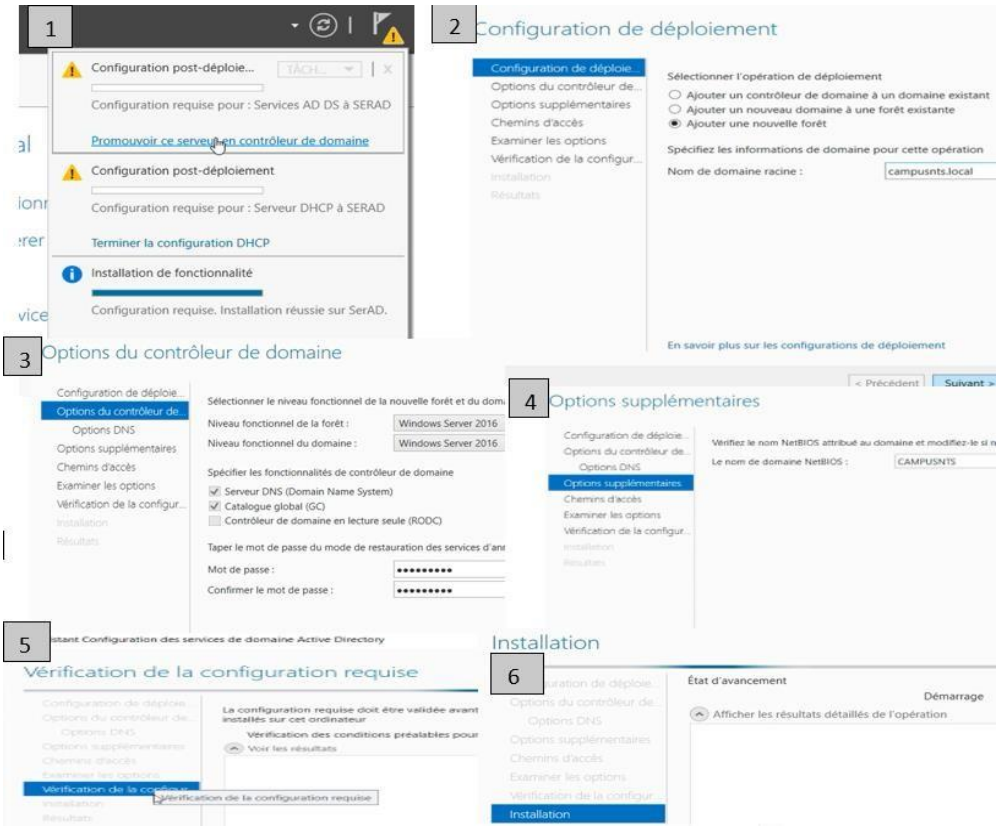


Figure IV.5 : Configuration AD et DNS

Nous sommes désormais en mesure de créer des utilisateurs, et nous allons donc commencer par créer des unités d'organisations.

- **<u>Créations d'unité d'organisation :</u>**

D'abord on a créé l'unité d'organisation sous le nom (service informatique) :

Cliquant sur outils, on va choisir « Utilisateurs et ordinateurs Active Directory », sur **campusnts.local** on va cliquer sur Nouveau>>Unité d'organisation et on va la donner un nom (service informatique), La figure ci-dessous montre les étapes de la création de l'unité.

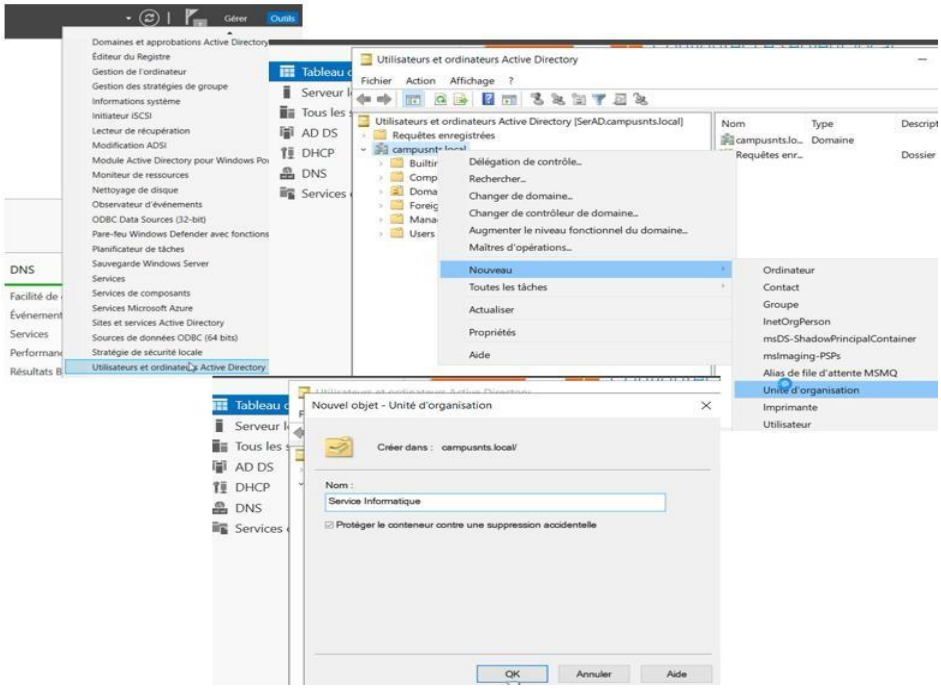


Figure IV.6 : Création d'unité d'organisation

Nous allons maintenant procéder à la création des groupes au sein de l'unité d'organisation.

- **<u>Création des groupes :</u>**

On a créé deux groupes, groupe réseau et groupe GL,

Cliquant sur l'unité d'organisation qu'on a créé (service informatique)>>Nouveau>>Groupe, enfin on va donner un nom au groupe. La figure ci-dessous montre les étapes de la création de groupe.

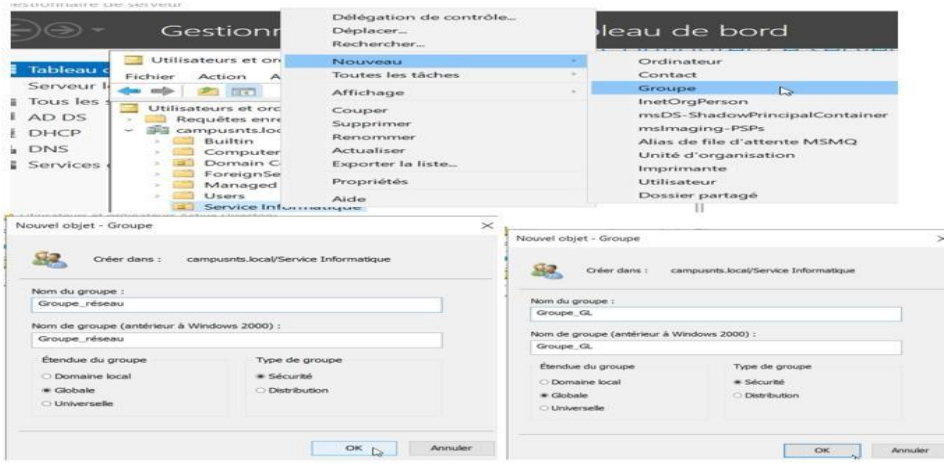


Figure IV.7 : Création des groupes (réseau et GL)

Ensuite, On va passer à la création des utilisateurs

- **Création des utilisateurs :**

Cliquant sur l'unité d'organisation qu'on a créé>> Nouveau>>Utilisateur, on va compléter les cases (Prénom, mot de passe…) comme la figure illustre.

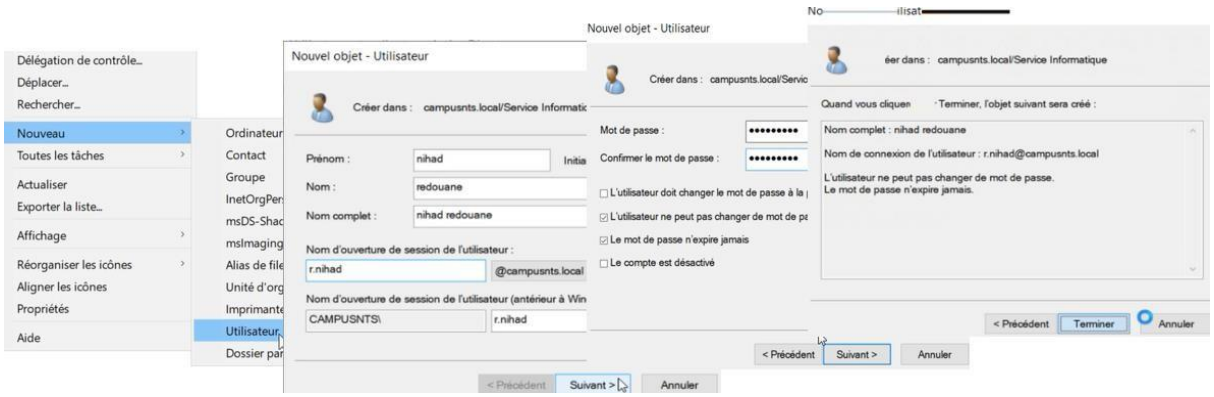


Figure IV.8 : Création utilisateur redouane nihad.

De la même façon on va créer l'utilisateur saadoune dyhia

Maintenant nous allons ajouter ces utilisateurs au groupe : On va accéder au groupe réseau, sur membres on va mettre ajouter, et on va ajouter l'utilisateur saadoune dyhia

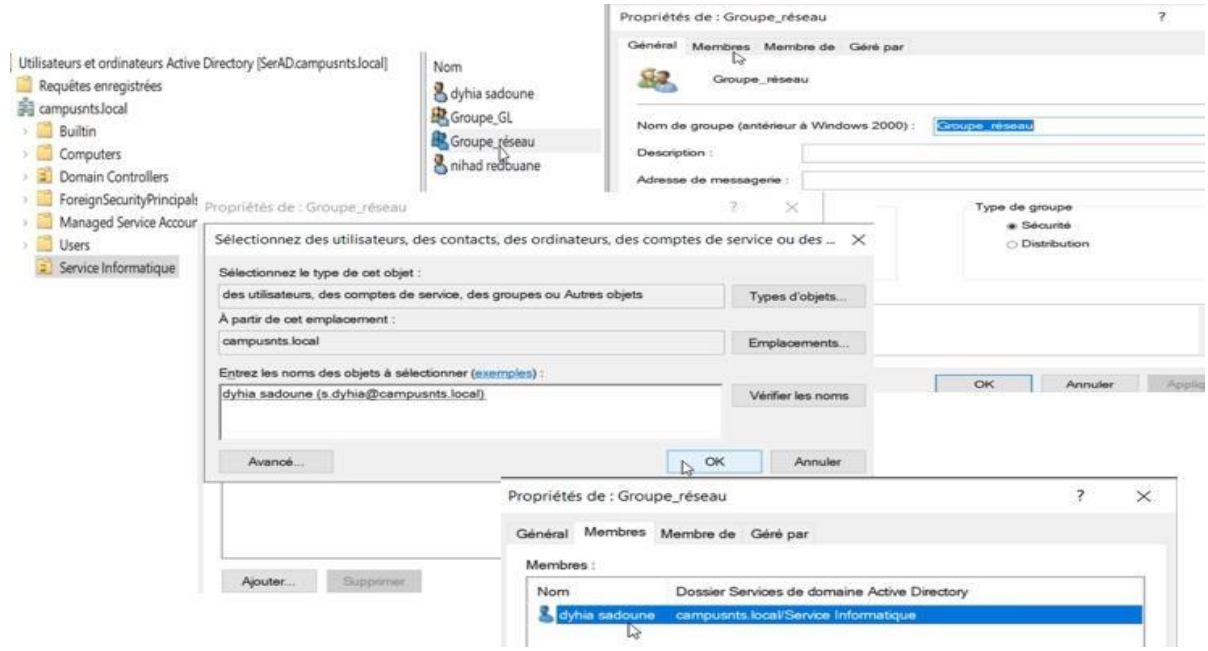


Figure IV.9 : L'ajout d'utilisateur saadoune dyhia au groupe réseau

De la même façon on va ajouter l'utilisateur redouane nihad au groupe GL

IV.2.3 Configuration DHCP

- **Création des étendues :**

Sur DHCP nous allons créer une étendue pour chaque VLAN,

En cliquant sur outils, on va choisir DHCP, sur IPv4 on va cliquer sur Nouvelle étendue, on va donner un nom (ici on a pris l'exemple de VLAN 105)>> après on va donner la plage d'adresse>>on va exclure les premières adresses>>ajouter la passerelle>>ajouter l'adresse IP sur serveur WINS qui fait la conversion des noms NetBIOS en adresses IP

Les figures ci-dessous montre les étapes de la création d'étendue.

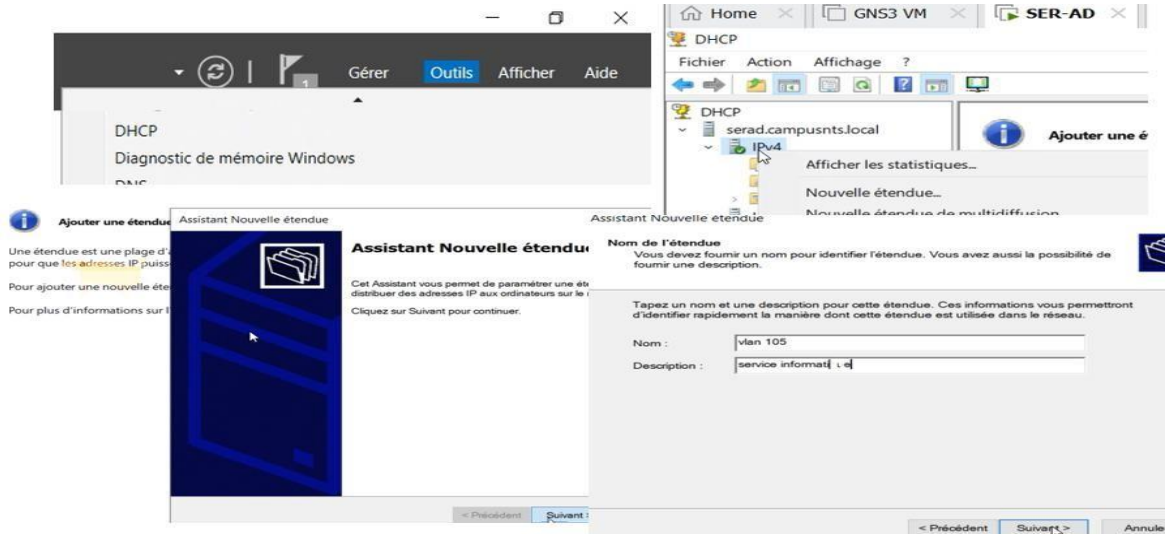


Figure IV.10 : Etape de création d'étendu (1)

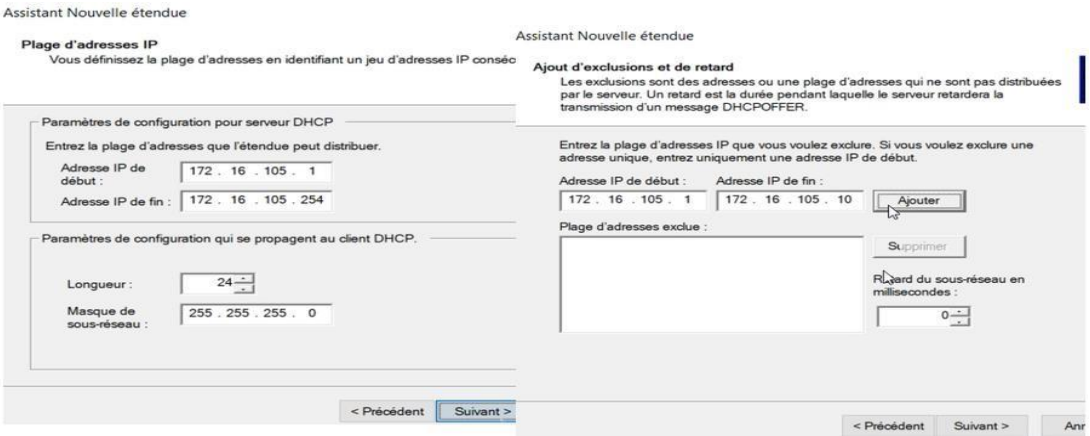


Figure IV.11 : Etape de création d'étendu (2)

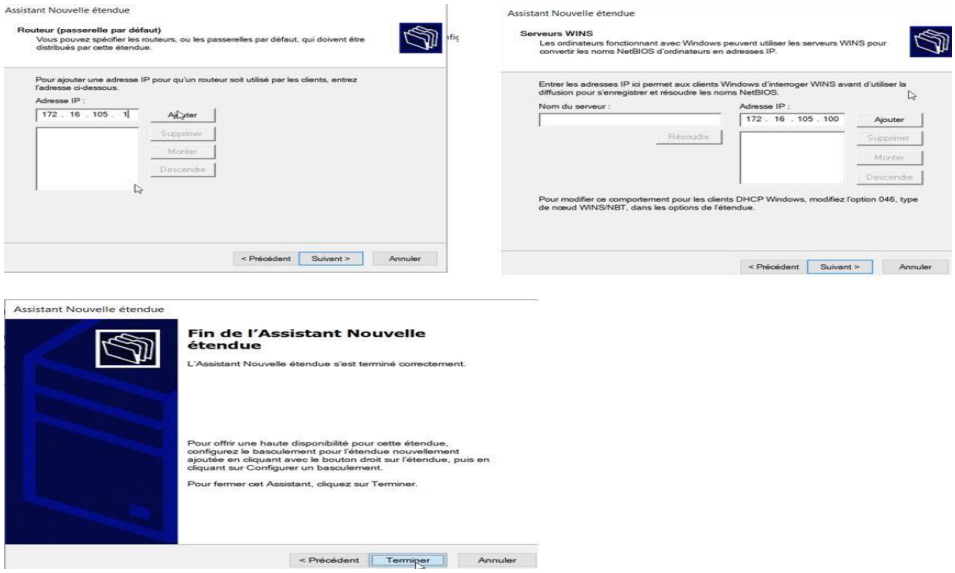


Figure IV.12 : Etape de création d'étendu (3)

IV.2.4 Teste AD

Comment joindre un domaine via un utilisateur (redouane nihad)

Il faut d'abord se connecter sur domaine

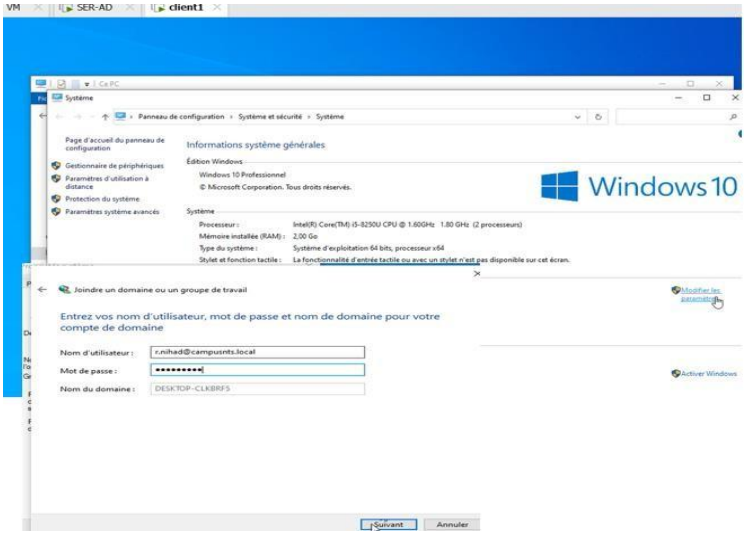


Figure IV.13 : Se connecter sur le domaine (1)

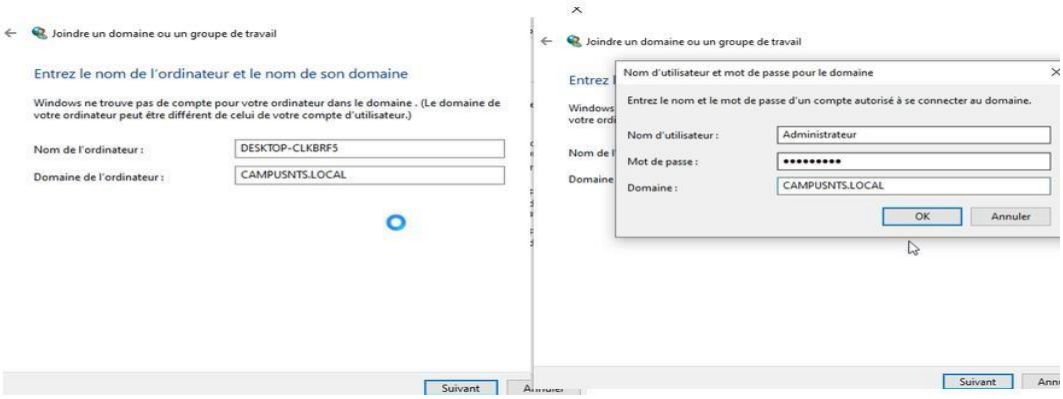


Figure IV.14 : Se connecter sur le domaine (2)

De cette façon l'utilisateur redouane nihad peut se connecter avec sa session sur le domaine AD.

Figure IV.15 : L'utilisateur redouane nihad joindre le domaine

L'ordinateur est dans le domaine, donc on n'a pas besoin de se connecter au domaine

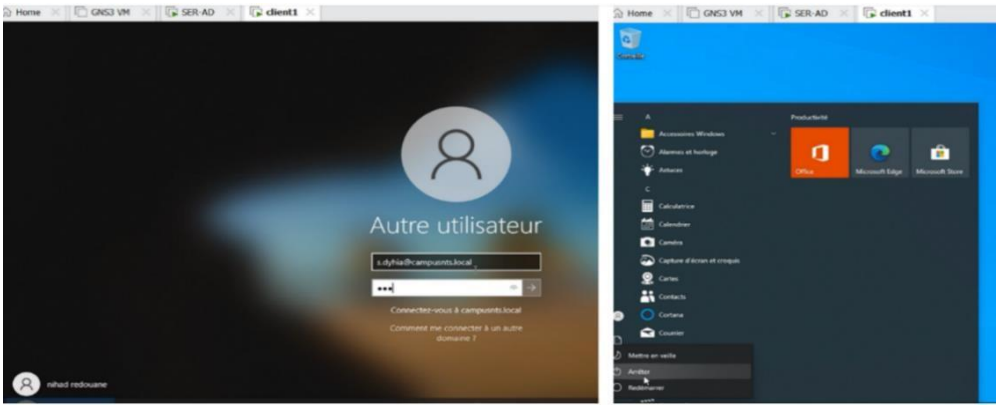


Figure IV.16 : L'utilisateur saadoune dyhia joindre le domaine

- Test AD réussi

IV.2.5 Test DHCP

Comme la figure montre on va vérifier si DHCP a donné l'adresse auswitch DATA-CENTER,

Sur la carte réseau de client1 on a trouvé que le serveur a donné l'adresse 172.16.105.11 au switch DATA-CENTER

Et sur le serveur SER-AD, cliquant sur l'entendue de VLAN 105, puis sur baux d'adresse, on a trouvé que DHCP a donné l'adresse 172.16.105.11 au switch DATA-CENTER,

Donc DHCP est bien configuré (test DHCP réussi).

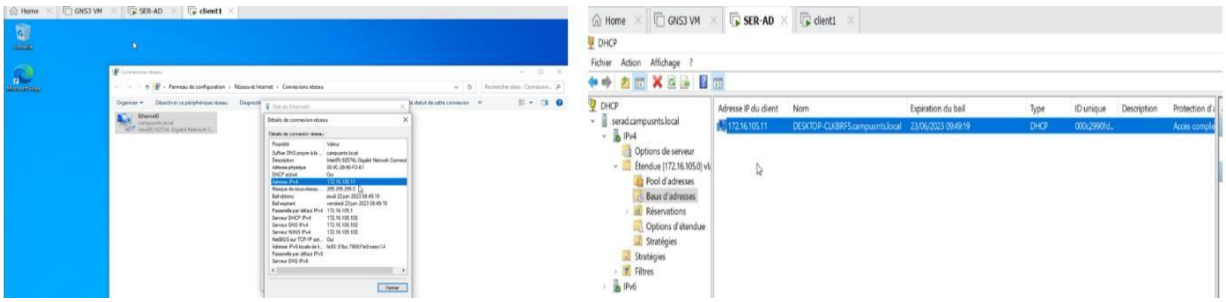


Figure IV.17 : Test DHCP

Il est maintenant possible d'effectuer un ping vers l'adresse du serveur.

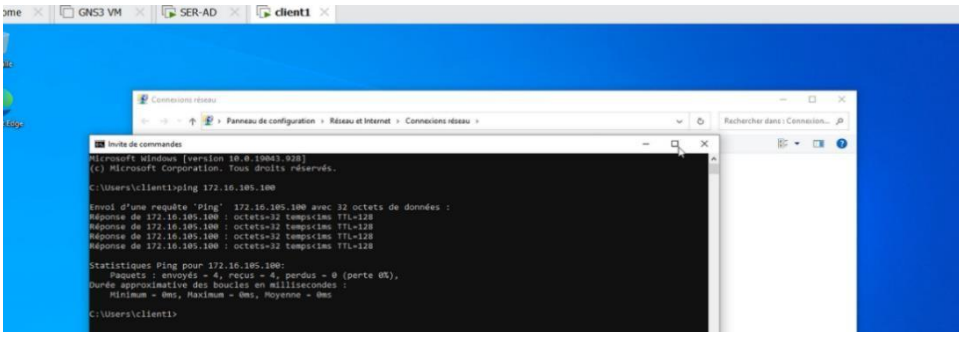


Figure IV.18 : Ping réussi depuis client1 vers l'adresse de serveur

IV.3 Configuration Zabbix

- **<u>Création des hôtes :</u>**

Cliquer sur créer un hôte pour créer l'hôte data-center-sw, après on va ajouter le modèle Cisco IOS by SNMP dont la Template est Network devices, on va donner l'adresse IP, enfin on a ajouté la communauté data-center, et on va valider

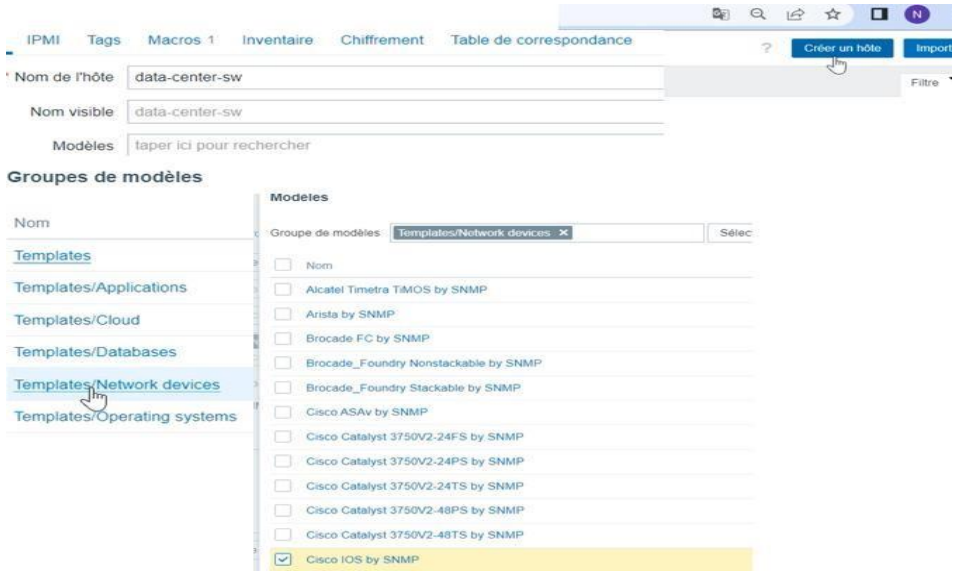


Figure IV.19 : Etapes de création d'hôte data-center-sw (1)

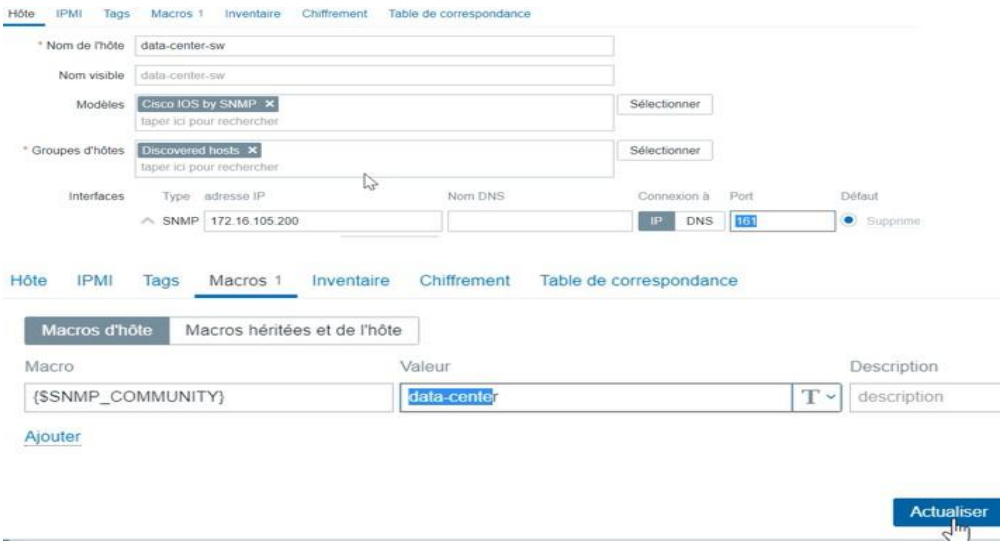


Figure IV.20 : Etapes de création d'hôte data-center-sw (2)

Par la suite, nous allons configurer l'adresse IP de l'hôte (switch data center) et le nom de la communauté

```
DATA-CENTER(config)#interface  vlan 105
DATA-CENTER(config-if)#ip address 172.16.105.200 255.255.255.0
DATA-CENTER(config-if)#no shutdown
```

```
DATA-CENTER#show running-config | include snmp
snmp-server community data-center RO
```

Figure IV.21 : Configuration d'interface VLAN 105 et communauté sur le switch data center

Pour tester, on va effectuer un ping depuis le server zabbix vers le client snmp (switch data center), le ping marche très bien (test réussi)

Figure IV.22 : Ping vers l'hôte à partir de Zabbix

Afin de mettre en place un hôte Windows Server, il est nécessaire d'utiliser l'agent Zabbix. Nous avons procédé au téléchargement de cet agent, puis à son installation sur le serveur. Ensuite, nous devrons accepter les termes du contrat de licence.

Figure IV.23 : Installation d'agent Zabbix

Une fois l'agent installé, nous procéderons à la création de l'hôte Windows Server.

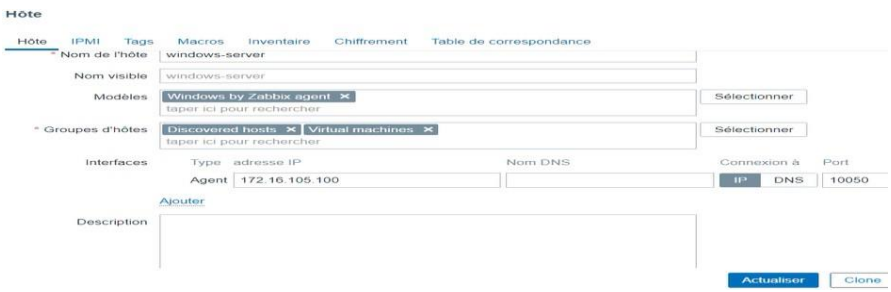


Figure IV.24 : Etapes de création d'hôte Windows Server

Nous voyons dans cette figure que les hottes sont bien créées

Figure IV.25 : Les hôtes sont créés

IV.3.1 Tests monitoring

Nous allons cliquer sur Surveillance, puis sur Hôtes, À partir de là, nous pourrons récupérer les graphiques et vérifier s'il y a des problèmes ou non.

Ici il a détecté un problème de mémoire

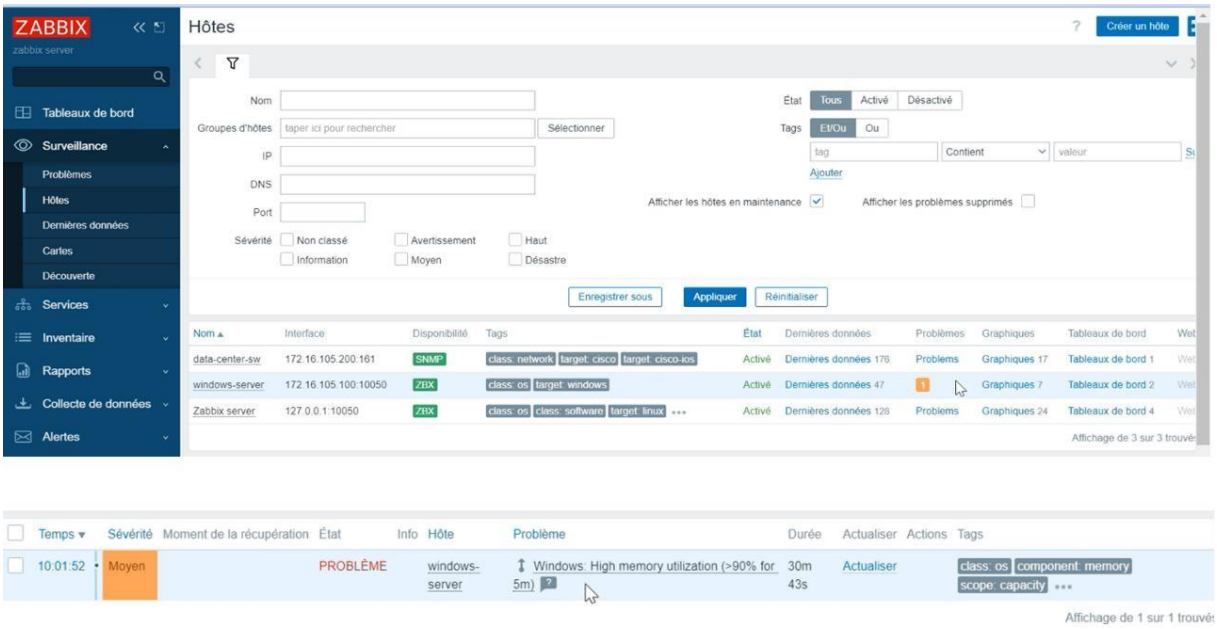


Figure IV.26 : Détection de problème

Nous avons la possibilité de visualiser les graphiques qui fournissent des informations pertinentes. En cliquant sur "Graphiques", nous pourrons les afficher à l'écran.

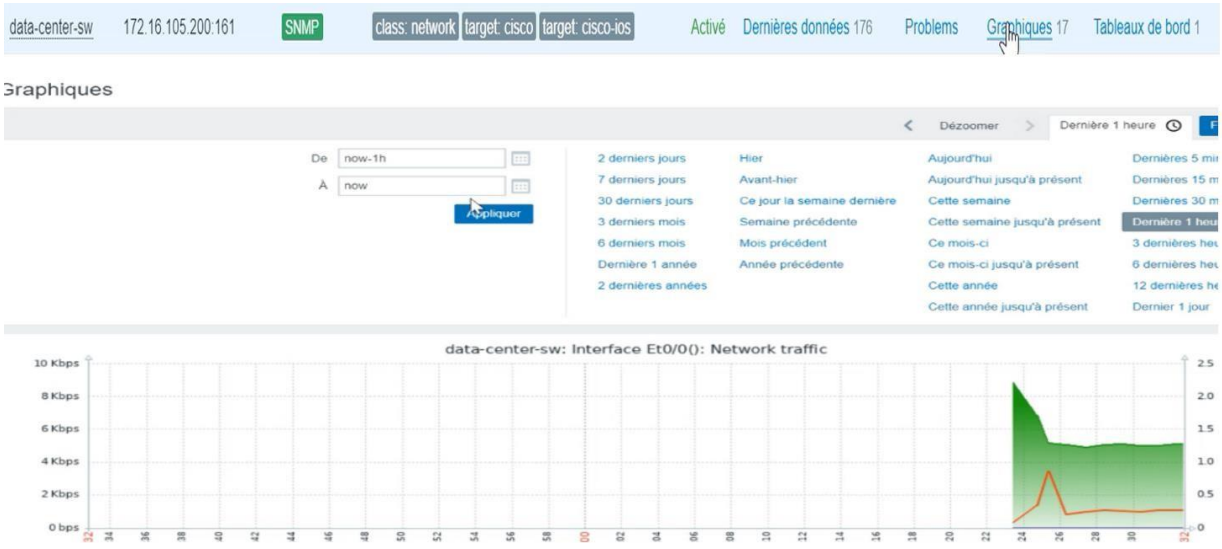


Figure IV.27 : Affichage de graphe

Test supervision réussi.

IV.4 Configuration des VLANs

IV.4.1 Configuration des liaisons trunk

Mettre le switch Core1 en mode Trunk : Interface core1 en mode trunk pour que les VLANs peuvent sortir vers l'extérieur.

Mettre les interfaces en mode trunk pour core1, et sécurisé le trunk avec native. Et allouer les VLANs pour vlan native 666.

```
Core1(config)#interface Ethernet1/0
Core1(config-if)# switchport trunk allowed vlan 100-107,666
Core1(config-if)# switchport trunk encapsulation dot1q
Core1(config-if)# switchport trunk native vlan 666
Core1(config-if)# switchport mode trunk
Core1(config-if)#exit
```

Figure IV.28 : Mettre le switch Core en mode Trunk.

De la même façon nous allons mettre les interfaces en mode trunk pour Core2 :

```
Core2(config)#$rnet 3/0-3, ethernet 0/2-3, ethernet 1/0-1, ethernet 2/3
Core2(config-if-range)#
*May 18 08:42:39.873: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discov
ore1 Ethernet3/2 (666).
Core2(config-if-range)# switchport trunk allowed vlan 100-107,666
Core2(config-if-range)# switchport trunk encapsulation dot1q
Core2(config-if-range)# switchport trunk native vlan 666
Core2(config-if-range)# switchport mode trunk
Core2(config-if-range)#
```

Figure IV.29 : Mode trunk pour core2.

IV.4.2 Configuration VTP

Utilisant le protocole VTP pour faciliter la tâche (d'automatisation de configuration des VLANs),

VTP mode server pour core1 et core2, les VLANs pourront être propagés vers les switches d'accès,

```
Core2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core2(config)#vtp mode server
Device mode already VTP Server for VLANS.
Core2(config)#vtp domain ngtmeziani.vtp
Changing VTP domain name from NULL to ngtmeziani.vtp
Core2(config)#vtp password cisco
Password already set to cisco
Core2(config)#vtp version 2
VTP version is already in V2.
Core2(config)#vtp pruning
Pruning already switched on
Core2(config)#
Core2(config)#end
```

Figure IV.30 : VTP mode server pour core2

VTP mode client pour tous switches d'accès

```
DATA-CENTER(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
DATA-CENTER(config)#vtp domain ngtmeziani.vtp
Changing VTP domain name from NULL to ngtmeziani.vtp
DATA-CENTER(config)#vtp password cisco
Setting device VTP password to cisco
DATA-CENTER(config)#vtp version 2
```

Figure IV.31 : VTP mode client pour switch DATA-CENTER

- **Vérification :** Affichage de statut VTP pour le switch DATA-CENTER

```
DATA-CENTER#show  vtp st
DATA-CENTER#show  vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : ngtmeziani.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.1200
Configuration last modified by 0.0.0.0 at 5-18-23 10:48:15

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 2
MD5 digest                        : 0x00 0xE4 0xC9 0xD2 0x20 0xE0 0xAD 0x7F
                                    0xAE 0x2C 0x50 0x5E 0x9A 0x58 0x1E 0xD1
```

Figure IV.32 : Statut vtp pour le switch DATA-CENTER

IV.4.3 Création des VLANs

Création des VLANs dans core1, on a créé neuf VLANs, chacun est associé à son service de plus on a créé le VLAN native

```
Core1(config)#vlan 100
Core1(config-vlan)# name Marketing
Core1(config-vlan)#vlan 101
Core1(config-vlan)#name GRH
Core1(config-vlan)#vlan 102
Core1(config-vlan)#name SI
Core1(config-vlan)#vlan 103
Core1(config-vlan)#name Finance
Core1(config-vlan)#vlan 104
Core1(config-vlan)#name comptabilite
Core1(config-vlan)#vlan 105
Core1(config-vlan)#name data centre
Core1(config-vlan)#vlan 106
Core1(config-vlan)#name Technique
Core1(config-vlan)#vlan 107
Core1(config-vlan)#name HSE
Core1(config-vlan)#vlan 666
Core1(config-vlan)#name native
```

Figure IV.33 : Création des VLANs dans core1

- **Vérification :** affichage des

VLANsLes VLANs sont créés dans core1

```
Core1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et1/2, Et1/3, Et2/0
                                                Et3/0, Et3/1, Et3/2, Et3/3
100  Marketing                        active
101  GRH                              active
102  SI                               active
103  Finance                          active
104  comptabilite                     active
105  data centre                      active
106  Technique                        active
107  HSE                              active
666  native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Figure IV.34 : Affichage des VLANs sur core1

- **Vérification :** Affichage des vlans sur le switch (Com-Fina) :

```
Com-Fina#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/2, Et1/0, Et1/1, Et1/2
                                                 Et1/3, Et2/0, Et2/1, Et2/2
                                                 Et3/0
100  Marketing                         active
101  GRH                               active
102  SI                                active
103  Finance                           active    Et3/1, Et3/2, Et3/3
104  comptabilite                      active    Et0/3, Et2/3
105  data centre                       active
106  Technique                         active
107  HSE                               active
666  native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

Figure IV.35 : Affichage des VLANs sur le switch Com-Fina

IV.4.4 Affectation des ports aux VLANs

On va affecter les ports au VLANs (de 100 jusqu'à 107)

On prend l'exemple de VLAN 101 (GRH)

```
GRH#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GRH(config)#int
GRH(config)#interface range eth
GRH(config)#interface range ethernet 0/2-3
GRH(config-if-range)#swi
GRH(config-if-range)#switchport mode acc
GRH(config-if-range)#switchport mode access
GRH(config-if-range)#sw
GRH(config-if-range)#switchport acce
GRH(config-if-range)#switchport access vlan 101
GRH(config-if-range)#end
```

Figure IV.36 : Affectation des ports au VLAN 101

IV.5 L'équilibrage de charge

Agrégation des liens LACP : l'agrégation des liens pour avoir la tolérance au panne (même si y a une panne dans un câble toujours le réseau est disponible), en plus on va multiplier le débitvirtuellement,

Donc on a utilisé l'équilibrage de charge pour avoir la haute-disponibilité, pour utiliser les quatre ports au même temps, en utilisant protocole LACP

Dans core1 et même chose pour core2

```
Core1(config)#interface range ethernet 3/0-3
Core1(config-if-range)#ch
Core1(config-if-range)#channel-g
Core1(config-if-range)#channel-group 7 MO
Core1(config-if-range)#channel-group 7 MOde ?
  active      Enable LACP unconditionally
  auto        Enable PAgP only if a PAgP device is detected
  desirable   Enable PAgP unconditionally
  on          Enable Etherchannel only
  passive     Enable LACP only if a LACP device is detected

Core1(config-if-range)#channel-group 7 MOde ac
Core1(config-if-range)#channel-group 7 MOde active
Creating a port-channel interface Port-channel 7
```

Figure IV.37 : Configuration d'équilibrage de charge (1)

```
Core1(config)#port-channel lo
Core1(config)#port-channel load-balance ?
  dst-ip          Dst IP Addr
  dst-mac         Dst Mac Addr
  src-dst-ip      Src XOR Dst IP Addr
  src-dst-mac     Src XOR Dst Mac Addr
  src-ip          Src IP Addr
  src-mac         Src Mac Addr

Core1(config)#port-channel load-balance
*May 18 12:52:31.169: %EC-5-L3DONTBNDL2: Et3/3 suspen
*May 18 12:52:31.607: %EC-5-L3DONTBNDL2: Et3/1 suspen
*May 18 12:52:31.778: %EC-5-L3DONTBNDL2: Et3/2 suspen
*May 18 12:52:31.783: %EC-5-L3DONTBNDL2: Et3/0 suspen
Core1(config)#port-channel load-balance  src-dst-mac
Core1(config)#end
```

Figure IV.38 : Configuration d'équilibrage de charge (2)

- **Vérification :** affichage de résumé d'EtherChannel

```
Core1#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
------+-------------+-----------+-----------------------------------------------
7      Po7(SU)         LACP      Et3/0(P)    Et3/1(P)    Et3/2(P)
                                 Et3/3(P)
```

Figure IV.39 : Affichage EtherChannel sur CORE1

IV.6 Routage inter vlan

Activer l'interface HSRP1 (même chose pour HSRP2)

```
HSRP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HSRP1(config)#in
HSRP1(config)#interface  eth
HSRP1(config)#interface  ethernet 0/0
HSRP1(config-if)#no shu
HSRP1(config-if)#no shutdown
HSRP1(config-if)#
HSRP1(config-if)#exit
```

Figure IV.40 : Activer l'interface HSRP1

Créer les sous-interfaces pour chaque vlan (100 jusqu'à 107), sur HSRP1 et HSRP2 :

```
HSRP1(config)#interface ethernet 0/0.100
HSRP1(config-subif)#encapsulation dot1Q 100
HSRP1(config-subif)#ip address 172.16.100.1 255.255.255.0
HSRP1(config-subif)#
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.100
HSRP1(config-subif)#encapsulation dot1Q 100
HSRP1(config-subif)#ip address 172.16.100.1 255.255.255.0
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.101
HSRP1(config-subif)#encapsulation dot1Q 101
HSRP1(config-subif)#ip address 172.16.101.1 255.255.255.0
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.102
HSRP1(config-subif)#encapsulation dot1Q 102
HSRP1(config-subif)#ip address 172.16.102.1 255.255.255.0
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.103
HSRP1(config-subif)#encapsulation dot1Q 103
HSRP1(config-subif)#ip address 172.16.103.1 255.255.255.0
HSRP1(config-subif)#exit
```

```
HSRP1(config)#interface ethernet 0/0.104
HSRP1(config-subif)#encapsulation dot1Q 104
HSRP1(config-subif)#ip address 172.16.104.1 255.255.255.0
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.105
HSRP1(config-subif)#encapsulation dot1Q 105
HSRP1(config-subif)#ip address 172.16.105.1 255.255.255.0
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.106
HSRP1(config-subif)#encapsulation dot1Q 106
HSRP1(config-subif)#ip address 172.16.106.1 255.255.255.0
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.107
HSRP1(config-subif)#encapsulation dot1Q 107
HSRP1(config-subif)#ip address 172.16.107.1 255.255.255.0
HSRP1(config-subif)#exit
```

Figure IV.41 : Routage inter vlan sur routeur HSRP1

```
HSRP2(config)#interface ethernet 0/0.100
HSRP2(config-subif)#encapsulation dot1Q 100
HSRP2(config-subif)#ip address 172.16.100.2 255.255.255.0
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.101
HSRP2(config-subif)#encapsulation dot1Q 101
HSRP2(config-subif)#ip address 172.16.101.2 255.255.255.0
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.102
HSRP2(config-subif)#encapsulation dot1Q 102
HSRP2(config-subif)#ip address 172.16.102.2 255.255.255.0
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.103
HSRP2(config-subif)#encapsulation dot1Q 103
HSRP2(config-subif)#ip address 172.16.103.2 255.255.255.0
HSRP2(config-subif)#exit
```

```
HSRP2(config)#interface ethernet 0/0.104
HSRP2(config-subif)#encapsulation dot1Q 104
HSRP2(config-subif)#ip address 172.16.104.2 255.255.255.0
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.105
HSRP2(config-subif)#encapsulation dot1Q 105
HSRP2(config-subif)#ip address 172.16.105.2 255.255.255.0
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.106
HSRP2(config-subif)#encapsulation dot1Q 106
HSRP2(config-subif)#ip address 172.16.106.2 255.255.255.0
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.107
HSRP2(config-subif)#encapsulation dot1Q 107
HSRP2(config-subif)#ip address 172.16.107.2 255.255.255.0
```

Figure IV.42 : Routage inter vlan sur routeur HSRP2

IV.7 La redondance a premier saut

Configurer HSRP : (création HSRP pour chaque sous-interface 100-107) ; configurer l'adresse virtuelle (passerelle HSRP qui va surveiller les 2 routeurs HSRP1 et HSRP2)

Si HSRP1 ne marche pas ils vont basculer sur HSRP2, avec la passerelle virtuelle (250) pour les 2 routeurs (HSRP1 et HSRP2), sauf que HSRP1 est priorisé par rapport à HSRP2

On a utilisé priority dans HSRP1 qui est le prioritaire, et preempt dans HSRP1 pour savoir qu'il est actif par apport a HSRP2 (HSRP1 qui gère HSRP2)

```
HSRP1(config)#interface ethernet 0/0.100
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 100 ip 172.16.100.250
HSRP1(config-subif)#standby 100 priority 150
HSRP1(config-subif)#standby 100 preempt
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.101
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 101 ip 172.16.101.250
HSRP1(config-subif)#standby 101 priority 150
HSRP1(config-subif)#standby 101 preempt
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.102
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 102 ip 172.16.102.250
HSRP1(config-subif)#standby 102 priority 150
HSRP1(config-subif)#standby 102 preempt
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.103
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 103 ip 172.16.103.250
HSRP1(config-subif)#standby 103 priority 150
HSRP1(config-subif)#standby 103 preempt
HSRP1(config-subif)#exit
```

```
HSRP1(config)#interface ethernet 0/0.104
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 104 ip 172.16.104.250
HSRP1(config-subif)#standby 104 priority 150
HSRP1(config-subif)#standby 104 preempt
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.105
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 105 ip 172.16.105.250
HSRP1(config-subif)#standby 105 priority 150
HSRP1(config-subif)#
HSRP1(config-subif)#standby 105 preempt
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.106
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 106 ip 172.16.106.250
HSRP1(config-subif)#standby 106 priority 150
HSRP1(config-subif)#standby 106 preempt
HSRP1(config-subif)#exit
HSRP1(config)#interface ethernet 0/0.107
HSRP1(config-subif)#standby version 2
HSRP1(config-subif)#standby 107 ip 172.16.107.250
HSRP1(config-subif)#standby 107 priority 150
HSRP1(config-subif)#standby 107 preempt
HSRP1(config-subif)#
```

Figure IV.43 : Configuration de redondance sur HSRP1

```
HSRP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HSRP2(config)#interface ethernet 0/0.100
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 100 ip 172.16.100.250
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.101
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 101 ip 172.16.101.250
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.102
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 102 ip 172.16.102.250
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.103
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 103 ip 172.16.103.250
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.104
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 104 ip 172.16.104.250
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.105
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 105 ip 172.16.105.250
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.106
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 106 ip 172.16.106.250
HSRP2(config-subif)#
HSRP2(config-subif)#exit
HSRP2(config)#interface ethernet 0/0.107
HSRP2(config-subif)#
HSRP2(config-subif)#standby version 2
HSRP2(config-subif)#standby 107 ip 172.16.107.250
```

Figure IV.44 : Configuration de redondance sur HSRP2

- **Vérification :** affichage de status des routeurs HSRP1 et HSRP2

```
HSRP1#show  standby brief
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.100   100  150 P Active  local           172.16.100.2    172.16.100.250
Et0/0.101   101  150 P Active  local           172.16.101.2    172.16.101.250
```

```
HSRP2#show  standby  brief
                    P indicates configured to preempt.
                    |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.100   100  100   Standby 172.16.100.1    local           172.16.100.250
Et0/0.101   101  100   Standby 172.16.101.1    local           172.16.101.250
```

Figure IV.45 : Affichage status de routeur (HSRP1 et HSRP2)

IV.7.1 Test HSRP

```
HSRP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HSRP1(config)#in
HSRP1(config)#interface  eth
HSRP1(config)#interface  ethernet 0/0
HSRP1(config-if)#shu
HSRP1(config-if)#shutdown
```

```
HSRP2#
*May 18 13:27:26.203: %HSRP-5-STATECHANGE: Ethernet0/0.100 Grp 100 state Standby -> Active
*May 18 13:27:26.204: %HSRP-5-STATECHANGE: Ethernet0/0.101 Grp 101 state Standby -> Active
*May 18 13:27:26.206: %HSRP-5-STATECHANGE: Ethernet0/0.102 Grp 102 state Standby -> Active
*May 18 13:27:26.208: %HSRP-5-STATECHANGE: Ethernet0/0.103 Grp 103 state Standby -> Active
*May 18 13:27:26.209: %HSRP-5-STATECHANGE: Ethernet0/0.104 Grp 104 state Standby -> Active
```

Figure IV.46 : Test de redondance HSRP

IV.8 Configuration DMZ

IV.8.1 Switch DMZ en mode transparent : pour configurer le private VLAN, d'abord ilfaut mettre le switch en mode transparent vtp (off), car par default VTP est activé en mode serveur sur les switches

```
sw-dmz(config)#vtp mode  transparent
Device mode already VTP Transparent for VLANS.
sw-dmz(config)#end
```

Figure IV.47 : sw-dmz en mode transparent

- **Affichage :** on va vérifier si le sw-dmz est en mode transparent (en utilisant lacommande show vtp status)

```
sw-dmz#show  vtp status
VTP Version capable                 : 1 to 3
VTP version running                 : 1
VTP Domain Name                     :
VTP Pruning Mode                    : Disabled
VTP Traps Generation                : Disabled
Device ID                           : aabb.cc80.0600
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                  : Transparent
Maximum VLANs supported locally     : 1005
Number of existing VLANs            : 5
Configuration Revision              : 0
```

Figure IV.48 : Affichage de sw-dmz mode transparent

IV.8.2 Création des VLANs : VLAN primary (VLAN 400), VLAN community (VLAN 401) et VLAN isolated (VLAN 402), et associer les 2 VLANs community et isolated dansprimary, donc primary va faire passer les deux VLANs vers l'extérieur.

```
sw-dmz(config)#vlan
sw-dmz(config)#vlan 400
sw-dmz(config-vlan)#pri
sw-dmz(config-vlan)#private-vlan pri
sw-dmz(config-vlan)#private-vlan primary
```

Figure IV.49 : Création VLAN primary

```
sw-dmz(config-vlan)#private-vlan association 401,402
sw-dmz(config-vlan)#exit
```

Figure IV.50 : Associer les deux VLANs dans primary

```
sw-dmz(config)#vlan 401
sw-dmz(config-vlan)#pri
sw-dmz(config-vlan)#private-vlan co
sw-dmz(config-vlan)#private-vlan community
sw-dmz(config-vlan)#exit
sw-dmz(config)#vl
sw-dmz(config)#vlan 402
sw-dmz(config-vlan)#pri
sw-dmz(config-vlan)#private-vlan i
sw-dmz(config-vlan)#private-vlan isolated
sw-dmz(config-vlan)#exit
```

Figure IV.51 : Création VLANs community et isolated

IV.8.3 Affectation des ports aux VLANs

```
sw-dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-dmz(config)#interface range ethernet 0/0-1
sw-dmz(config-if-range)#switchport mode private-vlan host
sw-dmz(config-if-range)#switchport private-vlan host-association 400 401
sw-dmz(config-if-range)#exit
sw-dmz(config)#interface range ethernet 0/2-3
sw-dmz(config-if-range)#switchport mode private-vlan host
sw-dmz(config-if-range)#switchport private-vlan host-association 400 402
sw-dmz(config-if-range)#exit
```

Figure IV.52 : Affectation des ports aux VLANs sur switch sw-dmz

Le mode promiscuous permet de faire passer tous les VLANs secondaires

```
sw-dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-dmz(config)#interface range ethernet 1/0
sw-dmz(config-if-range)#switchport mode private-vlan promiscuous
sw-dmz(config-if-range)#switchport private-vlan mappi
sw-dmz(config-if-range)#switchport private-vlan mapping 400 401,402
sw-dmz(config-if-range)#end
```

Figure IV.53 : Sw-dmz en mode promiscuous

- **Vérification :** Affichage des interfaces

```
sw-dmz#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  up                    up
Ethernet3/3            unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

Figure IV.54 : Les interfaces du switch DMZ sont activées

IV.8.4 Donner les adresses aux serveurs

```
ser1> ip 172.17.0.2/24 172.17.0.1
Checking for duplicate address...
ser1 : 172.17.0.2 255.255.255.0 gateway 172.17.0.1

ser1> save
Saving startup configuration to startup.vpc
.  done
```

Figure IV.55 : Adresse de serveur ser1

```
Ser2> ip 172.17.0.3/24 172.17.0.1
Checking for duplicate address...
Ser2 : 172.17.0.3 255.255.255.0 gateway 172.17.0.1

Ser2> save
Saving startup configuration to startup.vpc
.  done
```

Figure IV.56 : Adresse de serveur ser2

```
ser3> ip 172.17.0.4/24 172.17.0.1
Checking for duplicate address...
ser3 : 172.17.0.4 255.255.255.0 gateway 172.17.0.1

ser3> save
Saving startup configuration to startup.vpc
.  done
```

Figure IV.57 : Adresse de serveur ser3

```
Ser4> ip 172.17.0.5/24 172.17.0.1
Checking for duplicate address...
Ser4 : 172.17.0.5 255.255.255.0 gateway 172.17.0.1

Ser4> save
Saving startup configuration to startup.vpc
.  done
```

Figure IV.58 : Adresse de serveur ser4**.**

IV.8.5 Les tests de ping DMZ

- Ping de ser1 community vers isolated ça ne marche pas

```
ser1> ping 172.17.0.4
host (172.17.0.4) not reachable
ser1> ping 172.17.0.5
host (172.17.0.5) not reachable
```

Figure IV.59 : Ping de ser1 vers les deux serveurs ser3 et ser4

- Ping entre community ça marche

```
ser1> ping 172.17.0.3

84 bytes from 172.17.0.3 icmp_seq=1 ttl=64 time=0.532 ms
84 bytes from 172.17.0.3 icmp_seq=2 ttl=64 time=0.433 ms
84 bytes from 172.17.0.3 icmp_seq=3 ttl=64 time=1.114 ms
84 bytes from 172.17.0.3 icmp_seq=4 ttl=64 time=8.036 ms
84 bytes from 172.17.0.3 icmp_seq=5 ttl=64 time=1.900 ms
```

Figure IV.60 : Ping de ser1 vers ser2

- Ping entre isolated ça ne marche pas

```
ser3> ping 172.17.0.5
host (172.17.0.5) not reachable
```

Figure IV.61 : Ping de ser3 vers ser4

- Ping de ser3 isolated vers community ça ne marche pas

```
ser3> ping 172.17.0.2
host (172.17.0.2) not reachable
ser3> ping 172.17.0.3
host (172.17.0.3) not reachable
```

Figure IV.62 : Ping de ser3 vers les deux serveurs ser1 et ser2.

IV.9 Config VPN (Tunnel)

IV.9.1 Config GRE

Sur site Bejaia on va aller sur interfaces >> Assignments >> GREs, on va cliquer sur Add pour créer le tunnel qu'il doit sortir avec l'interface WAN au site distant (10.3.1.1 est l'adresse de site distant), et on va créer un réseau local virtuel, en fin on va créer une route vers site distant, et on va sauvegarder.

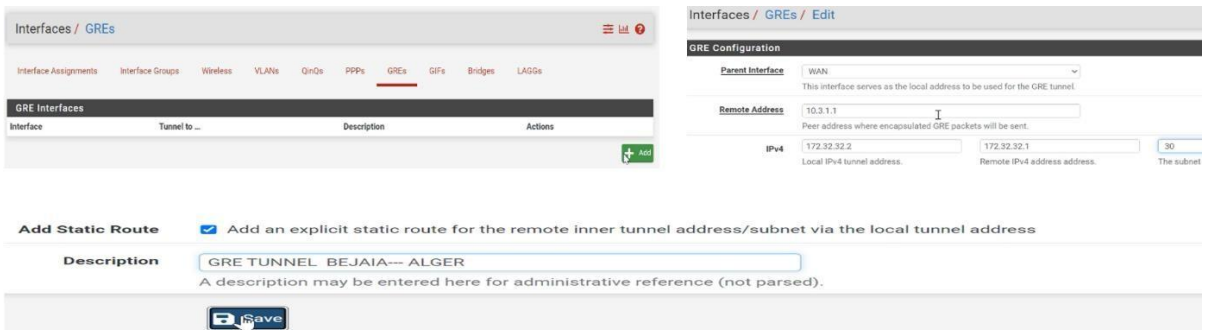


Figure IV.63 : Création de tunnel sur site Bejaia

Figure IV.64 : Le tunnel est bien créé sur site Bejaia

La même chose sur l'autre coté (site d'Alger)

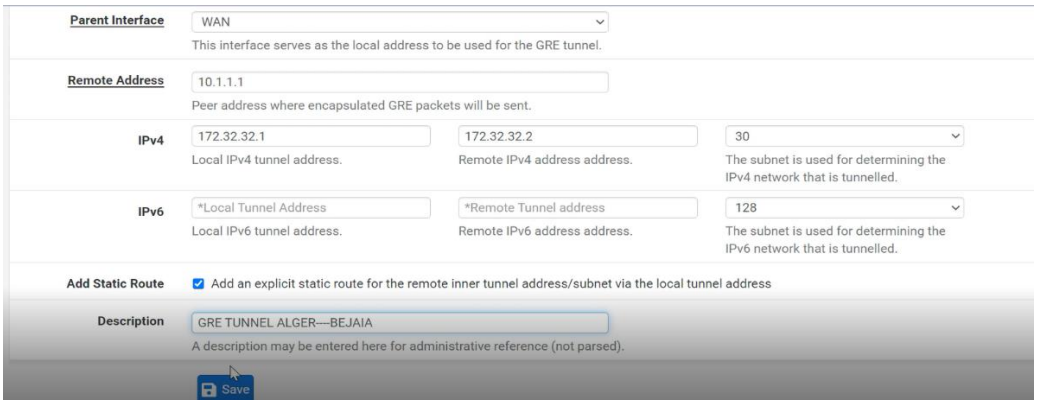


Figure IV.65 : Création de tunnel sur site Alger

Figure IV.66 : Le tunnel est bien créé sur site Alger

IV.9.2 Créer interface GRE

Sur Interfaces du site Bejaia >> Assignments, cliquant sur Add pour créer l'interface GRE, et on va sauvegarder

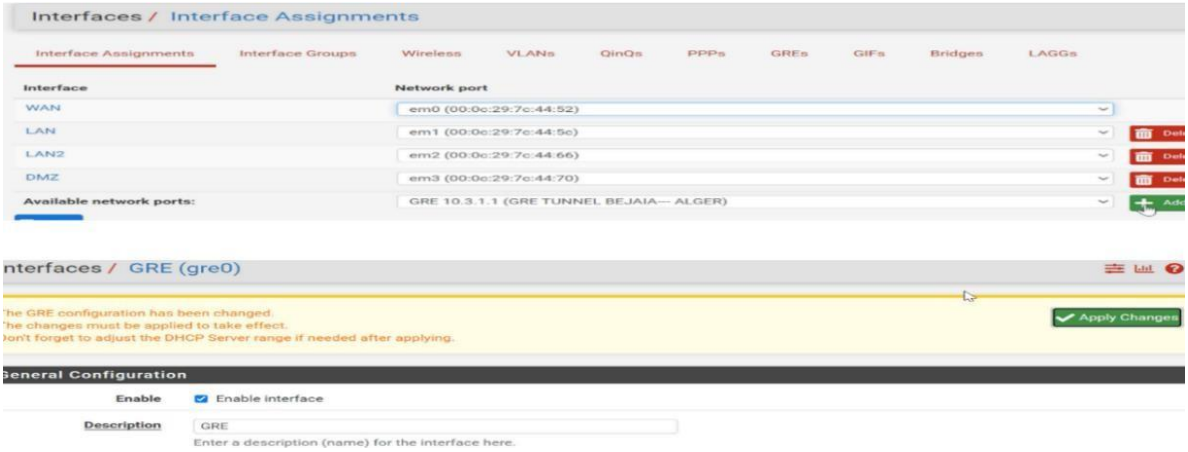


Figure IV.67 : Création interface GRE.

Même chose pour site d'Alger.

- **Vérification de l'état de GRE :** active

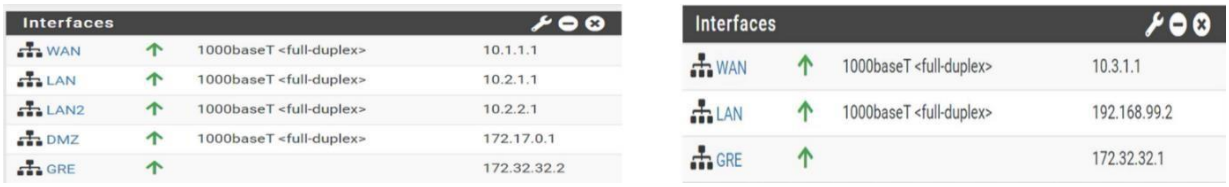


Figure IV.68 : L'état de GRE pour les deux sites

Mais pas de chiffrement, donc on active le chiffrement avec IPSec

IV.9.3 IPSec

La négociation dans le tunnel VPN se fait en deux phases :

Phase 1 : Dans cette phase, on fait les échanges des clés sécurisées avec IKE afin que lesutilisateurs puissent négocier dans le tunnel secrètement et c'est la deuxième phase.

Phase 2 : C'est là où on fait la négociation avec les deux protocoles suivants :

- **Le protocole ESP** (Encapsulating Security Payload) Fournit des services d'authentifications optionnels pour garantir l'intégrité des paquets protégés.
- **Le protocole AH** (Authentication Header) Garantit l'authenticité des paquets échangés en saisissant une somme de contrôle chiffrée (de l'en-tête IP jusqu'à la fin du paquet)

Sure site Bejaia on va cliquer sur VPN >> IPSec >> on va donner description, choisissant l'interface GRE, on va donner l'adresse de site distant, on va utiliser la même clé privée pour les deux sites, les mêmes algorithmes, et on va sauvegarder.

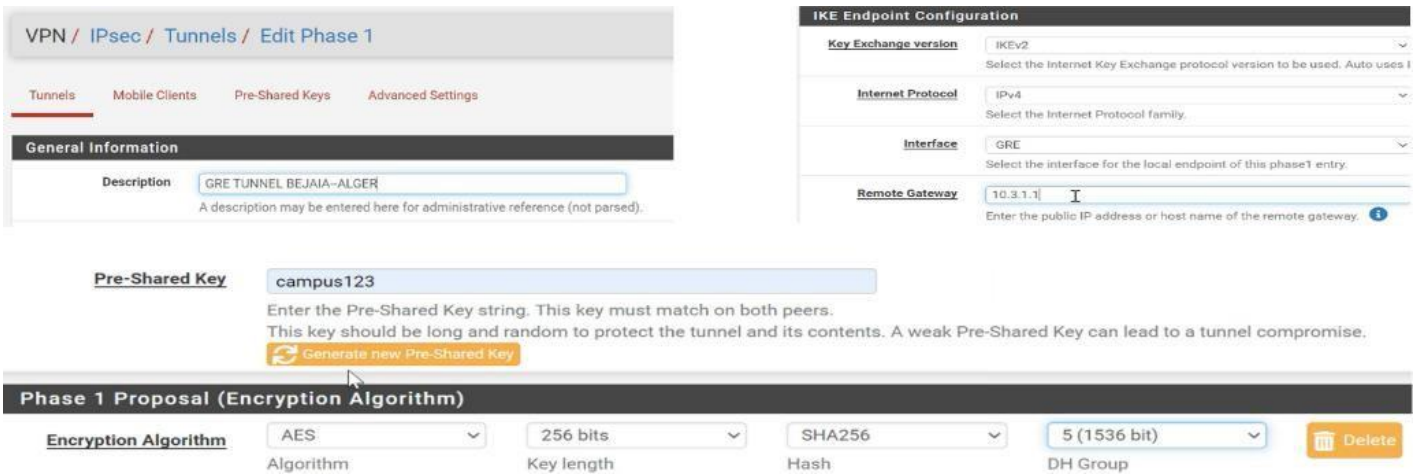


Figure IV.69 : Phase1

Figure IV.70 : Première phase est créée

Même chose pour le site d'Alger.

On va passer à la deuxième phase pour ajouter une adresse dans le tunnel, cliquant sur Add P2,on va donner description, on va laisser le réseau LAN à connecter, on va donner l'adresse de réseau distant, ESP qui va chiffrer, choisissant l'algorithme AES,

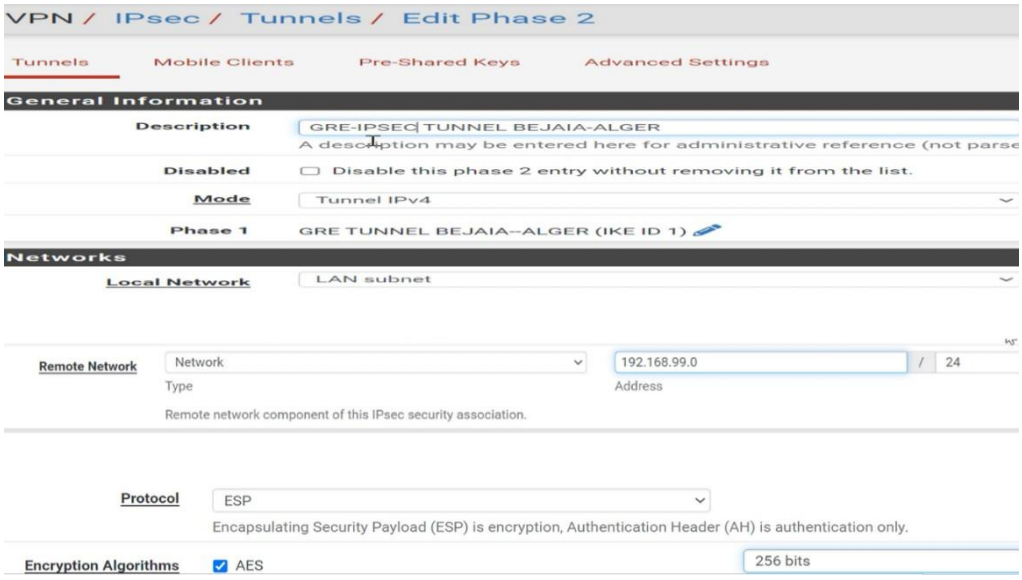


Figure IV.71 : Phase2

On a mentionné les réseaux qui vont se connecter entre eux, (on a autorisé le réseau de site Alger dans fw-Bejaia), la même chose dans l'autre coté (pour le site d'Alger)

Donc le trafic passe par le tunnel qui utilise GRE et IPSec,

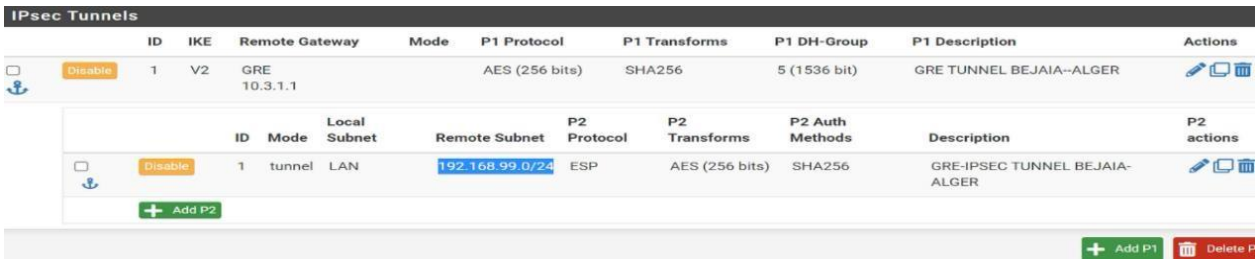


Figure IV.72 : Deuxième phase est créée

Même chose pour le site d'Alger.

- **Autorisation de trafic à l'intérieur de GRE et IPSec :** on va autoriser tout le trafic àl'intérieur de GRE et IPSec dans fw-Bejaia (la même chose pour fw-Alger) :

Nous allons vers Rules, dans GRE on autorise tous le trafic

Figure IV.73 : Autoriser le trafic dans GRE

Dans IPSec aussi on autorise le trafic

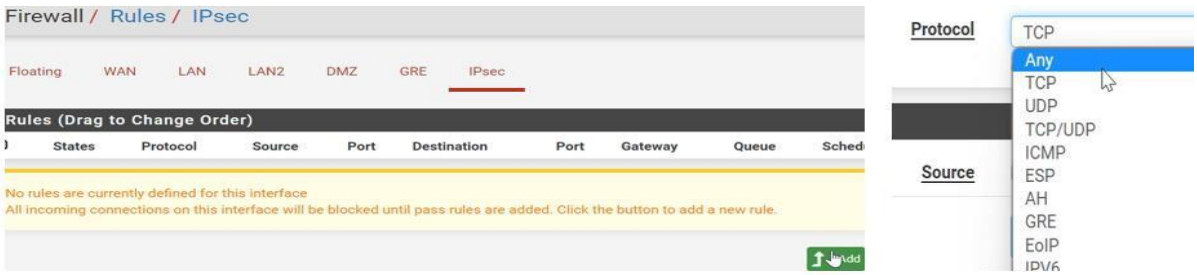


Figure IV.74 : Autoriser le trafic dans IPSec

IV.9.4 Test de ping VPN (test tunnel)

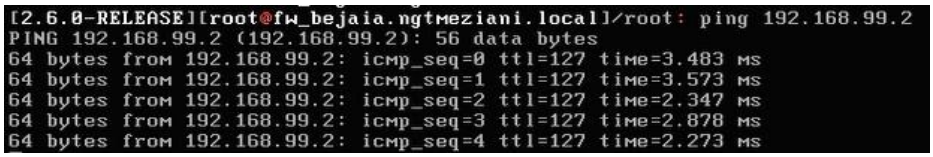


Figure IV.75 : Ping de fw-Bejaia vers 192.168.99.2

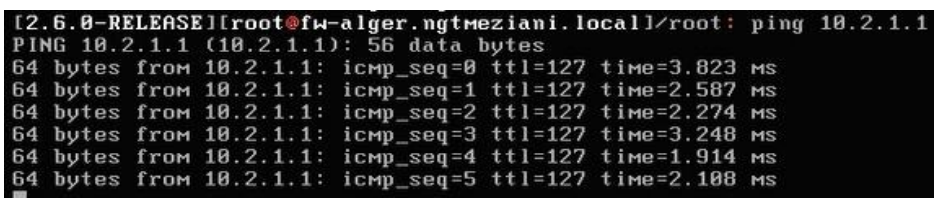


Figure IV.76 : Ping de fw-Alger vers 10.2.1.1

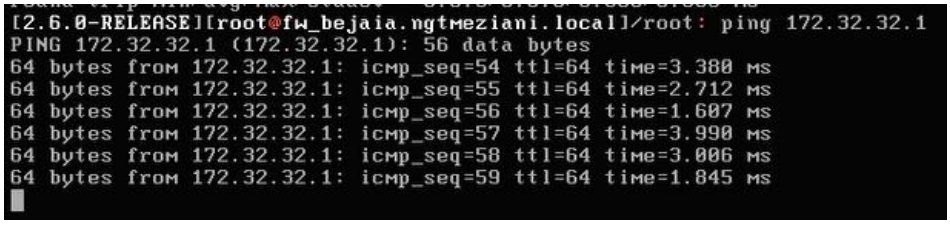


Figure IV.77 : Ping à l'intérieur du tunnel

IV.9.5 Capture wireshark

Les informations sont cryptées par IPSec

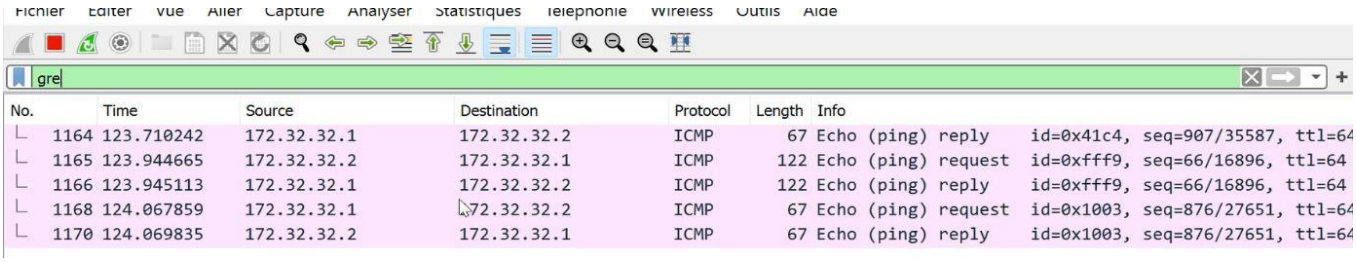


Figure IV.78 : Capture wireshark du protocole GRE

Conclusion

Ce chapitre se focalise sur la pratique, en mettant l'accent sur la mise en œuvre et la sécurité de l'architecture réseau que nous avons précédemment exposé.

Conclusion générale

Conclusion générale

Le travail que nous avons accompli a pour principal objectif la proposition d'une nouvelle architecture réseau sécurisée pour **« ngtmeziani »** d'alger. Ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde sur la sécurité des réseaux. Dans ce mémoire, nous avons présenté quelques généralités sur les réseaux, la sécurité informatique ainsi que les principales caractéristiques des réseaux privés virtuels et leur principe de fonctionnement.

Nous avons ensuite étudié cette architecture du réseau et ces différentes zones où nous avons expliqué l'ensembles de techniques (méthodes), afin d'aider à construire et à faire fonctionner une infrastructure réseau protégée par : **Firewalls, VPN et VLAN, Active Directory, Port Security** contre ces différentes menaces et attaques.

Dans cette nouvelle architecture, nous avons proposé de diviser le réseau en deux réseaux indépendants à savoir **BEJAIA, ALGER** pour une meilleure fluidité du trafic, qui devient de plus en plus important et de moins surcharger le firewall, ces deux réseaux seront ensuite reliés par un tunnel sécurisé.

La réalisation de ce projet a été bénéfique et fructueuse pour nous dans le sens où il nous a permis d'apporter une contribution à **« ngtmeziani »**de alger, mais aussi d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles et déterministes pour nous à l'avenir.

Partie : Annex

Annex1 : Installation de GNS3 sous windows :

Définition

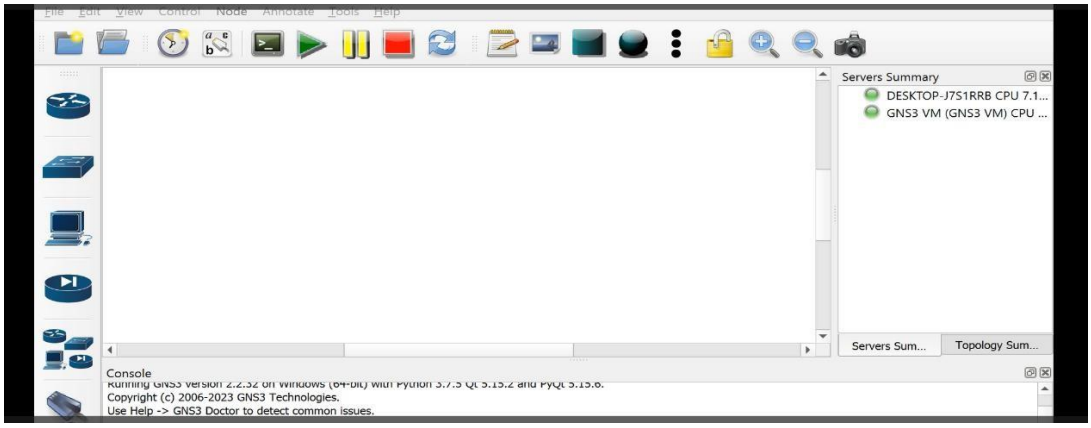
GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.

GNS3

Installation de GNS3 sous Windows

Afin d'installer GNS3, il est nécessaire de procéder en suivant ces étapes : télécharger d'abord le fichier exécutable, puis le lancer et suivre les instructions d'installation jusqu'à leur terme.
Enfin, il suffit de cliquer sur le bouton "Finish" pour finaliser le processus.

La capture d'écran ci-dessous illustre l'interface de GNS3.



Interface d'accueil GNS3

Annex2 : Installation de VMware Workstation version 17 pro

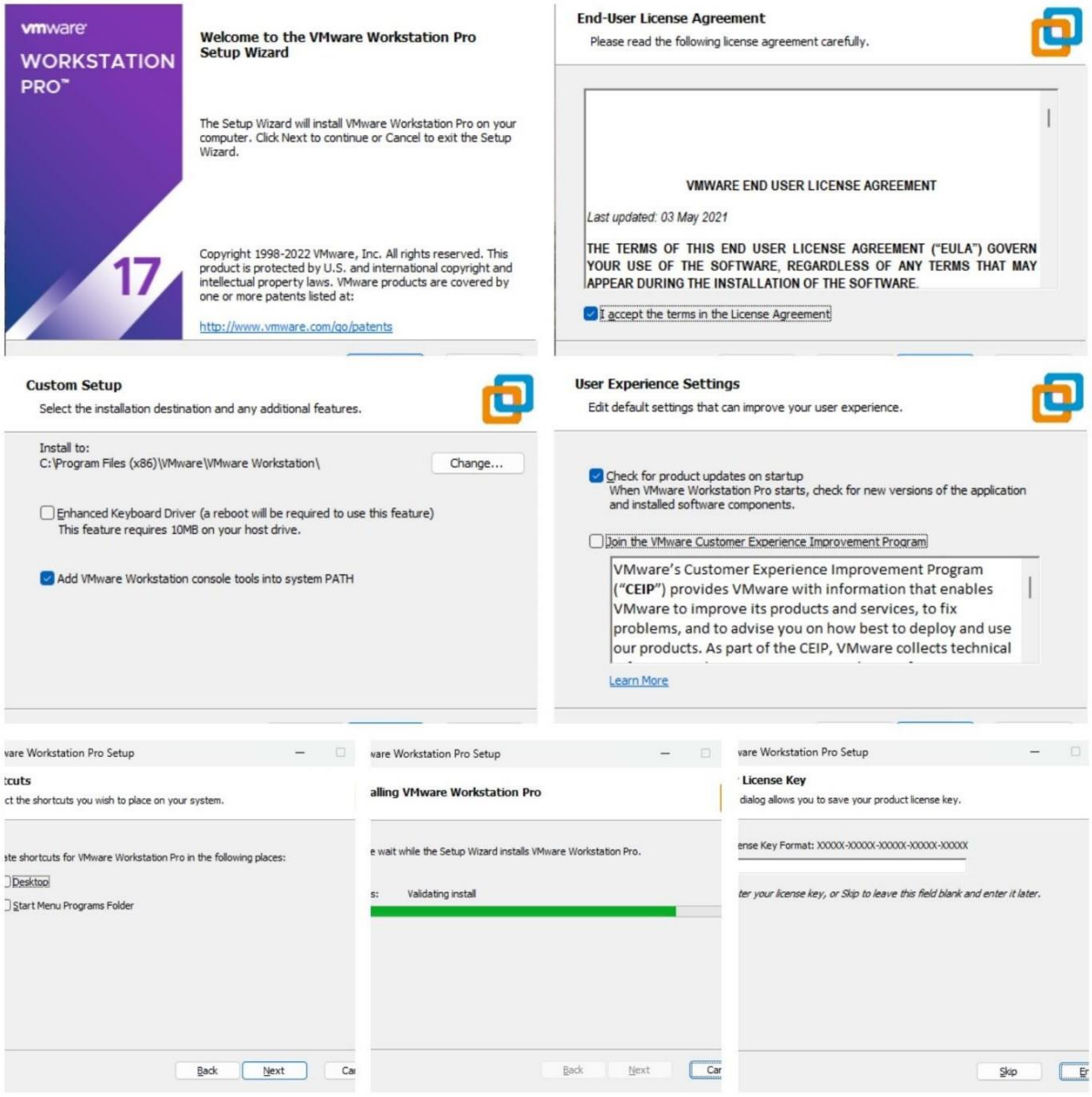
Définition

Il s'agit d'un logiciel de machine virtuelle de VMWare Inc. Il permet plusieurs copies du même système d'exploitation ou il peut y avoir plusieurs systèmes d'exploitation différents qui peuvent s'exécuter simultanément sur la même machine x86. Il prend en charge plusieurs systèmes d'exploitation exécutés sur un PC Windows ou Linux. Il dispose également d'outils de déploiement comme VMWare ACE. Le bureau d'un utilisateur peut être stocké sur une clé USB pour le transport. Il s'agit du processus de création d'un logiciel ou d'une représentation virtuelle qui inclut des serveurs, du stockage et différents réseaux. Il agit efficacement comme une solution pour réduire les dépenses informatiques et augmenter l'efficacité et l'agilité.[1]

VMware Workstation

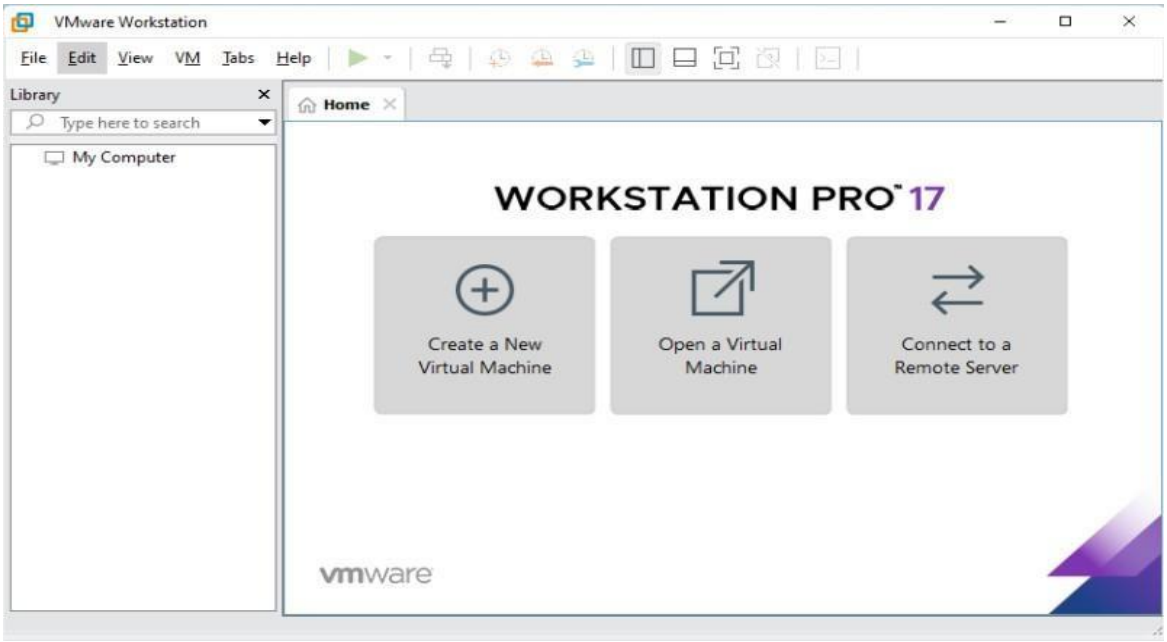
Installation de la VMware Workstation 17pro

Afin d'installer VMware Workstation 17 pro, il est nécessaire de procéder en suivant ces étapes : télécharger d'abord le fichier exécutable, puis le lancer et suivre les étapes de la figure ci-dessous :



Installation de VMware workstation

Après avoir installé VMware, vous serez accueilli par une page d'accueil. Cette page d'accueil peut fournir diverses options et fonctionnalités pour vous permettre de gérer vos machines virtuelles.

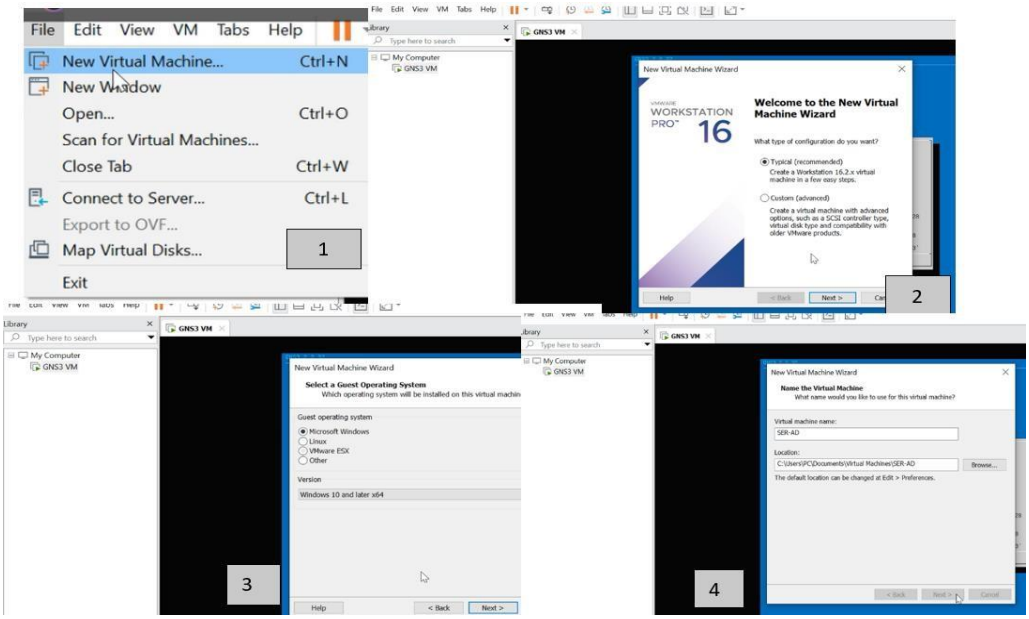


Page d'accueil de VMware Workstation

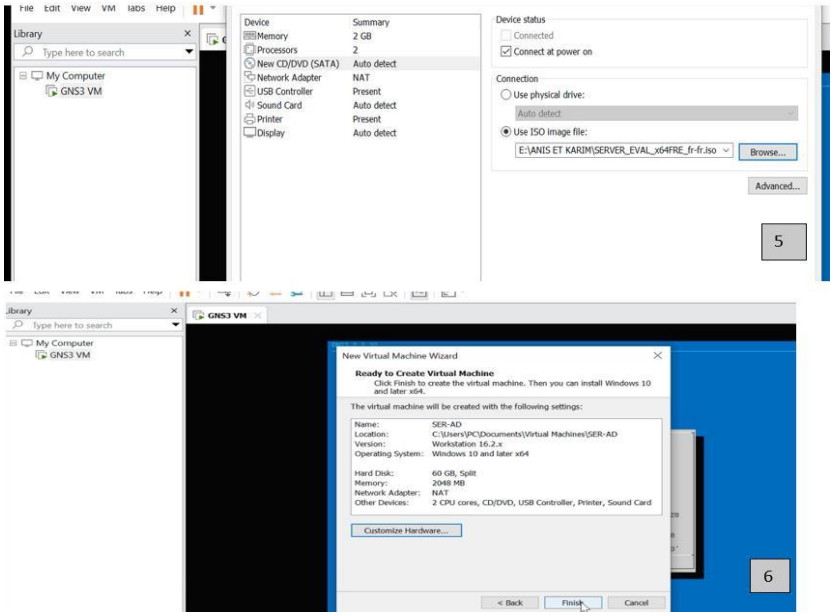
Annex3 : **Installation des serveurs**

Installation du Windows server 2022

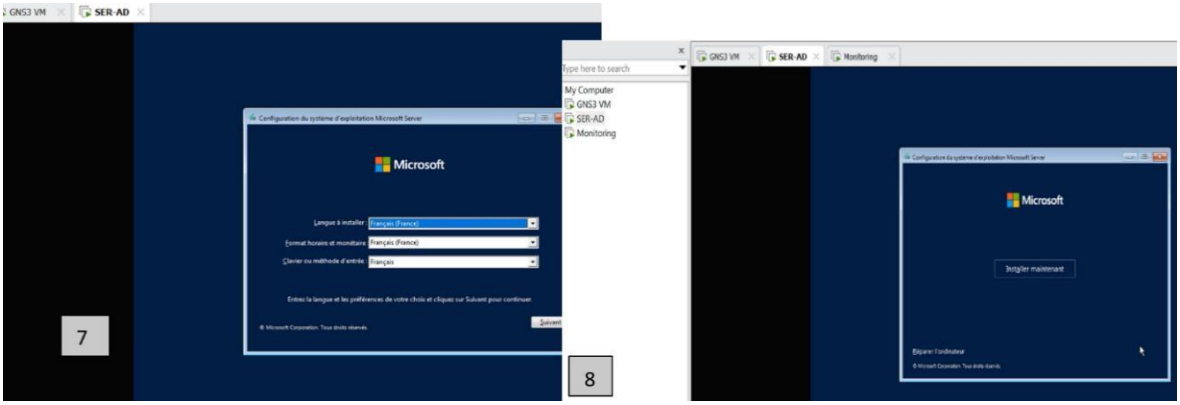
Dans cette partie nous allons voir les différentes étapes d'installations du Windows Server 2022.



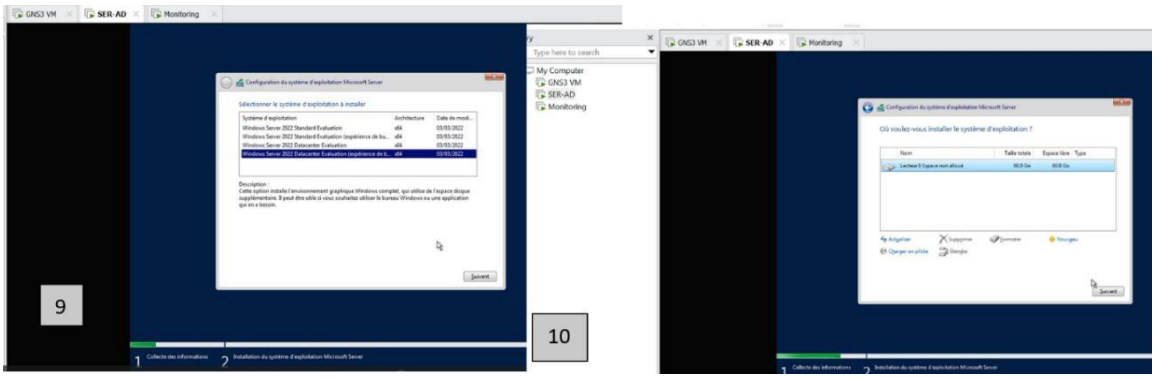
Etapes d'installation de serveur AD (1)



Etapes d'installation de serveur AD (2)

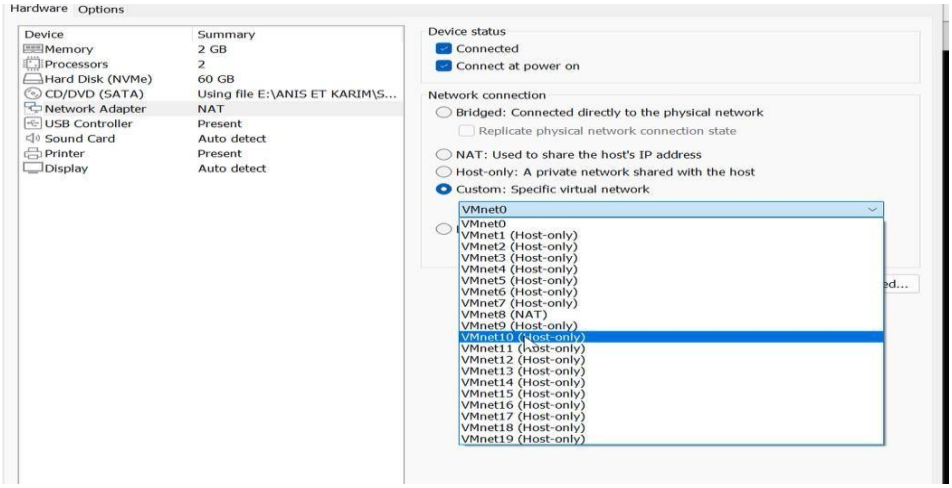


Etapes d'installation de serveur AD (3)



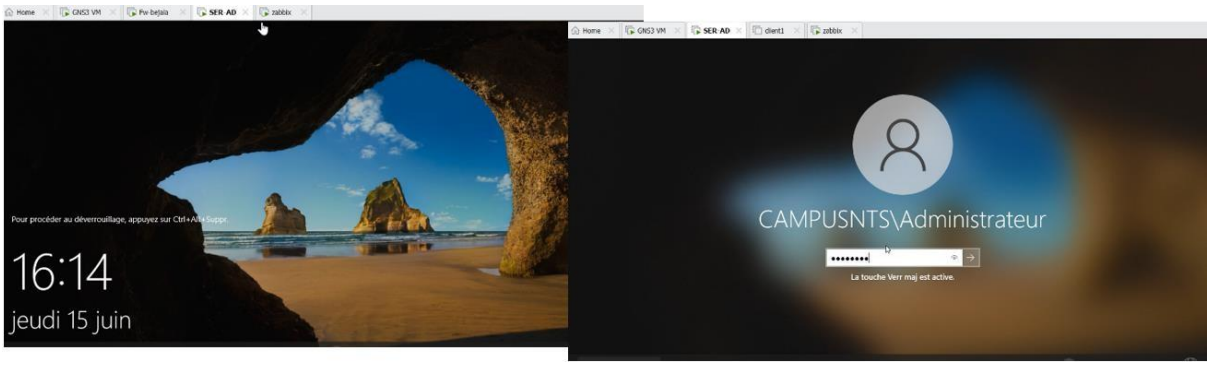
Etapes d'installation de serveur AD (4)

La figure illustre que l'interface du serveur a été placée dans la VMNET 10



Interface de serveur dans la VMNET10

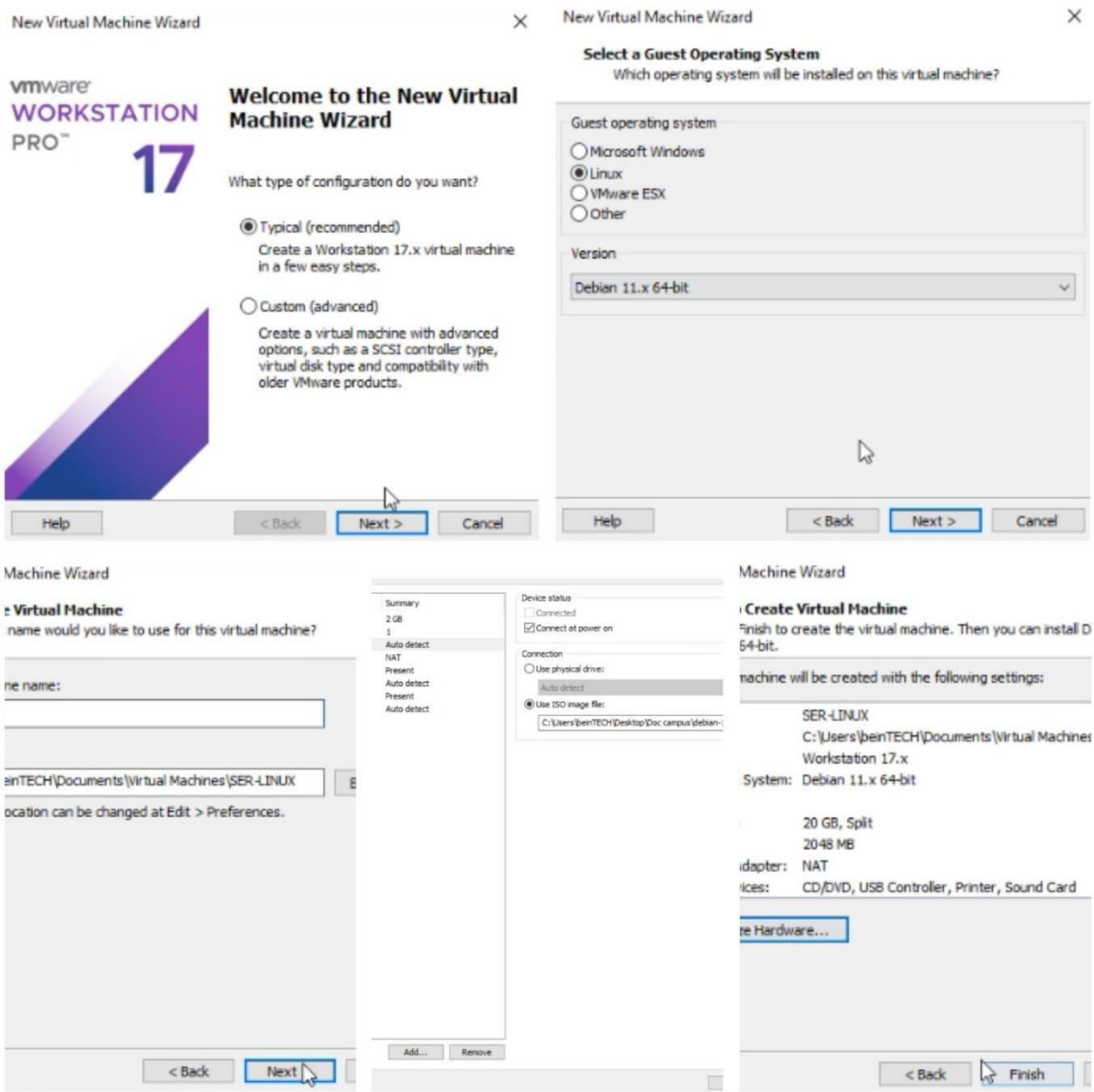
On voit que le serveur est bien installé,



SER-AD est installé

Annex4 : Installation du Linux server " Debian 11.X 64 bit" :

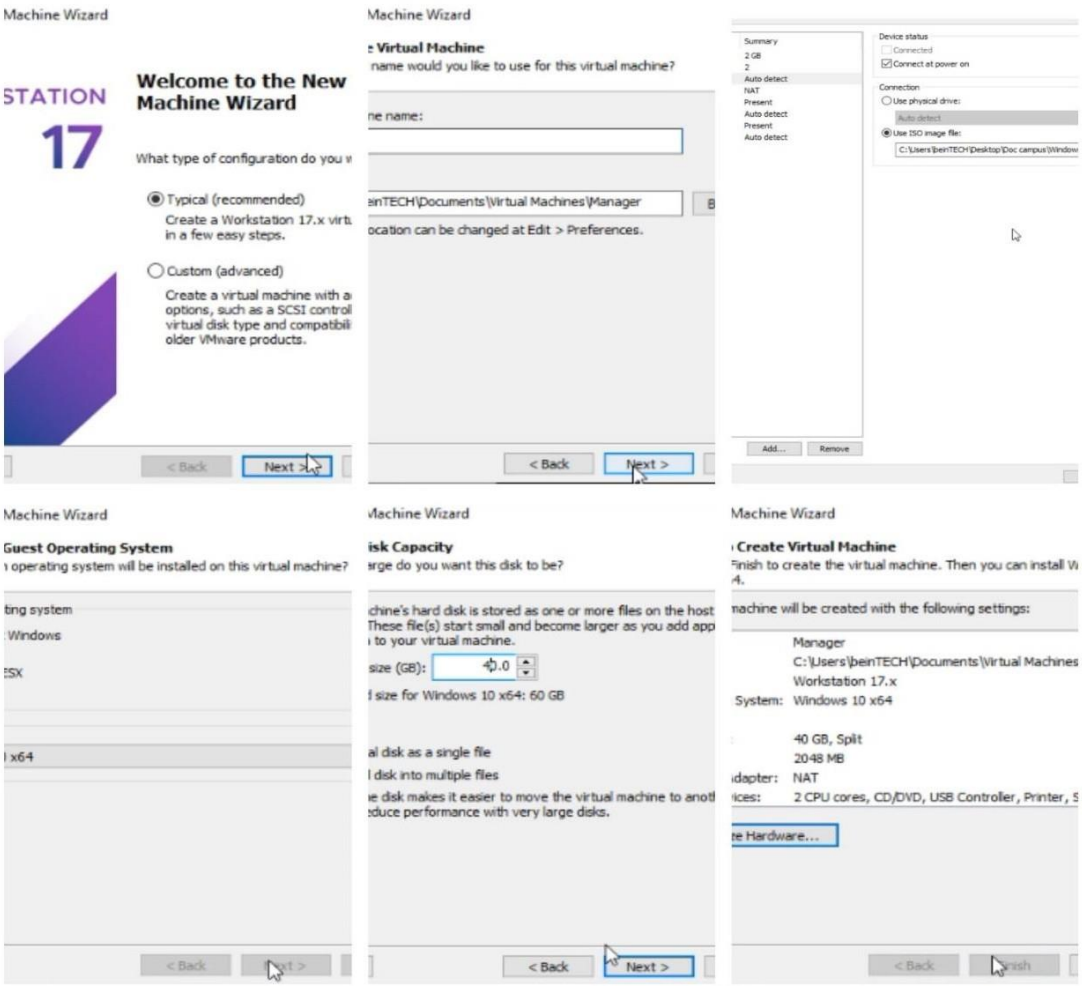
Dans cette partie nous allons voir les différentes étapes d'installations du Linux server " Debian 11.X64bit".



Les étapes d'installation Linux server " Debian 11.X 64 bit"

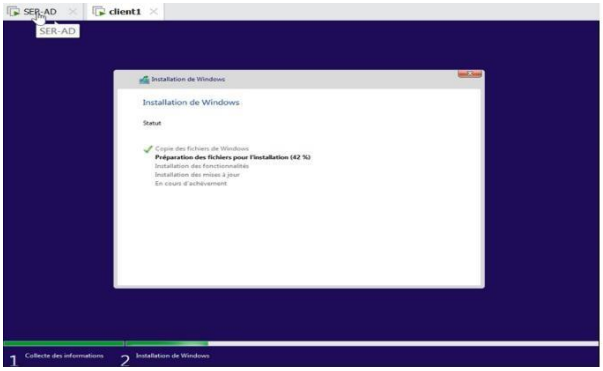
Annex5 : Installation Client Windows 10 " client1 "

la figure ci-dessous montre les étapes à suivre dans l'ordre pour Installer Windows 10



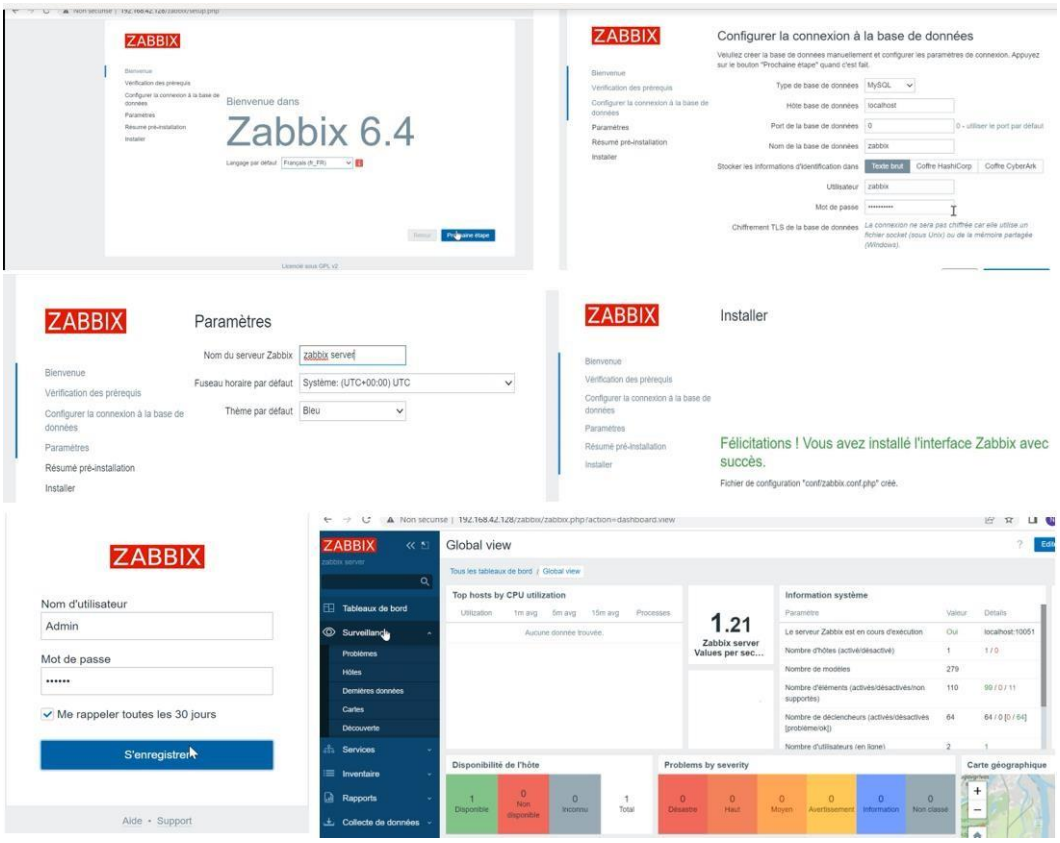
Les étapes d'installation Windows 10

Le client est bien instalée



Le client est instalé

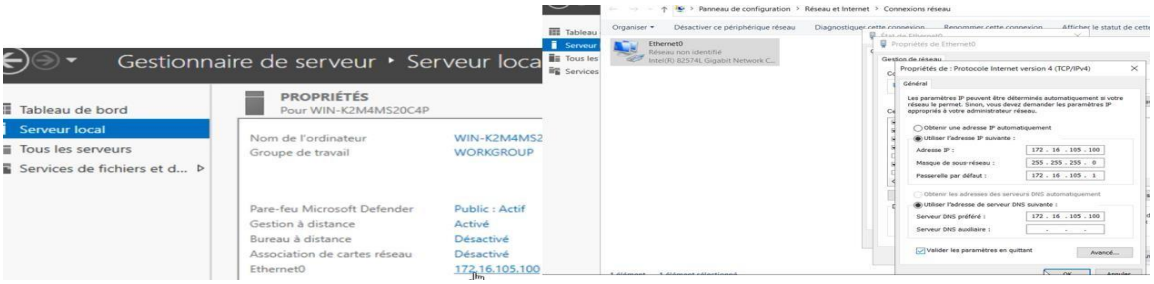
Annex6 : Installation Zabbix :



Les étapes d'installation Zabbix

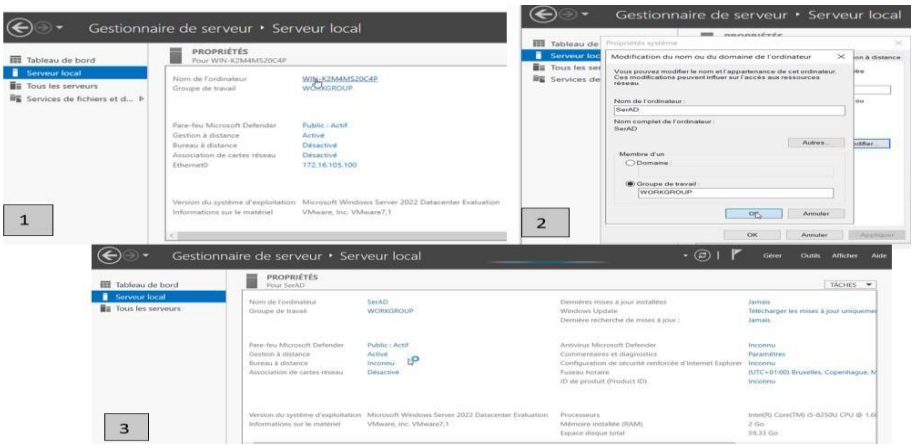
Annex7 : Configuration de base du serveur ;

Attribution d’une adresse ip pour le serveur :



Configuration de l’adresse de serveur

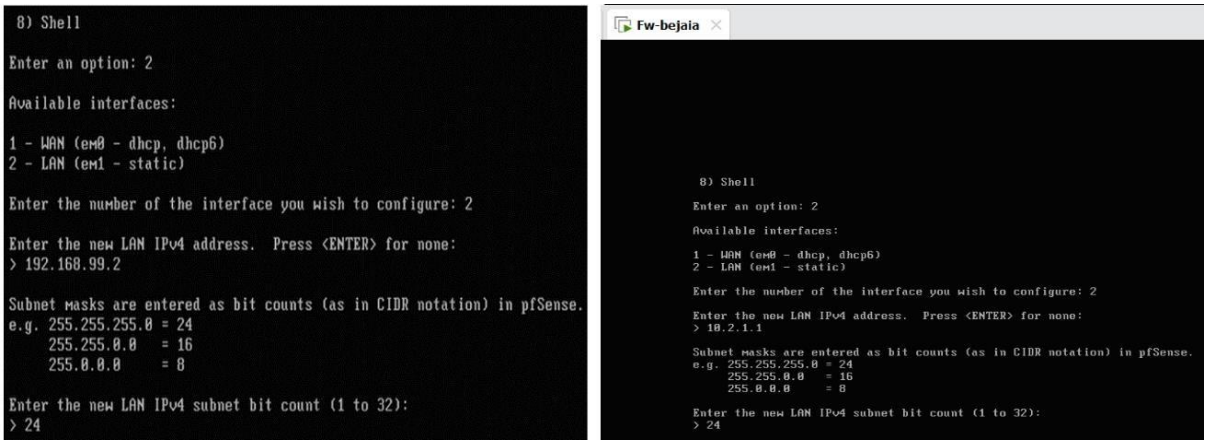
Configuration du nom du serveur :



Configuration du nom de serveur

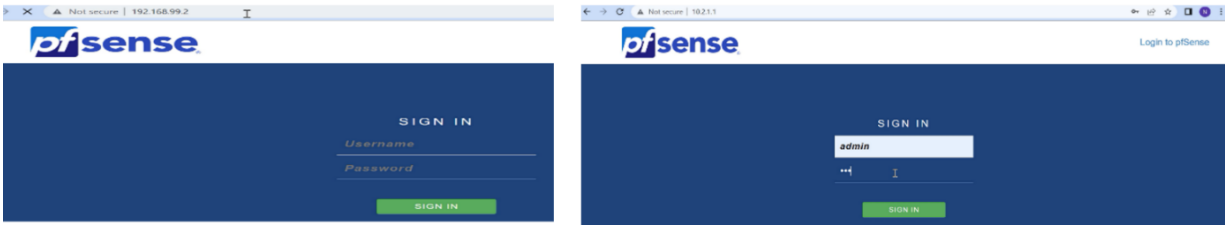
Annex8 : Configuration pfsense Alger et Bejaia :

Donner l'adresse au firewall Alger et Bejaia :



Donner l'adresse au firewall Alger et Bejaia

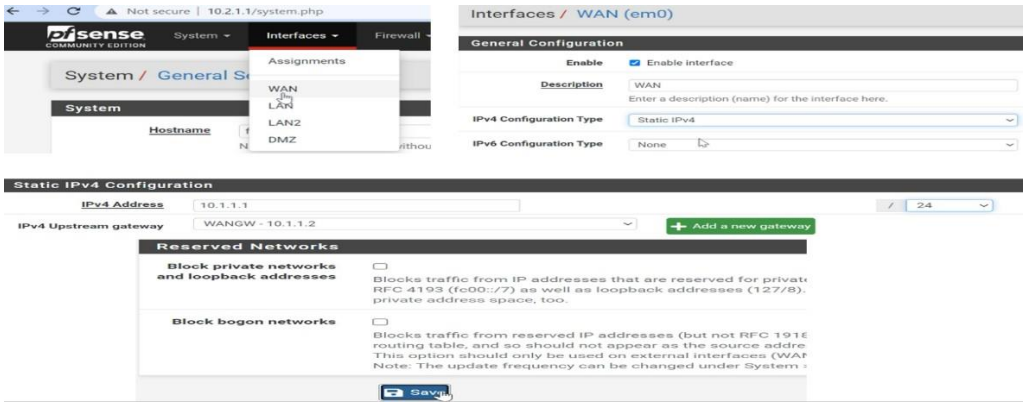
Accéder au pfsense : Alger (adresse est 192.168.99.2) et pfsense Bejaia (adresse est 10.2.1.1)



Accéder au pfsense (Alger et Bejaia)

Connecter le pfsense Bejaia à l'internet :

Sur Interfaces, on va cliquer sur WAN et effacer l'ipv6 et le DHCP, ensuite on va donner l'adresses à l'interface WAN de fw-bejaia (10.1.1.1) et donner adresse de Gateway (10.1.1.2), et il faut décocher les deux dernières lignes pour permettre utiliser les @ privées, en fin on va sauvegarder.



Interface WAN fw-bejaia

L'interface LAN :

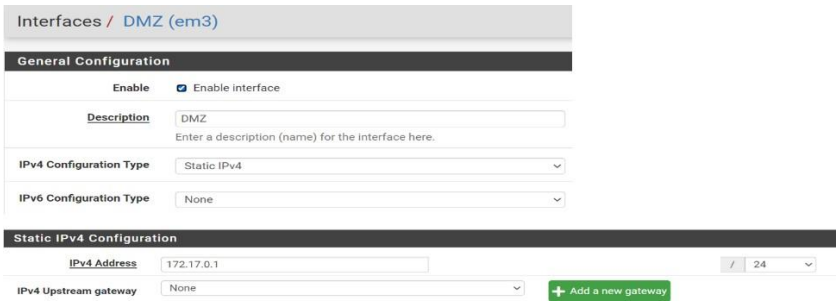
De la même façon on va configurer l'interface LAN, et on va donner l'dresse à l'interface LAN de fw-Bejaia (10.2.1.1),

Interface LAN fw-bejaia

L'interface LAN2 et DMZ :

De la même façon pour LAN2 et DMZ

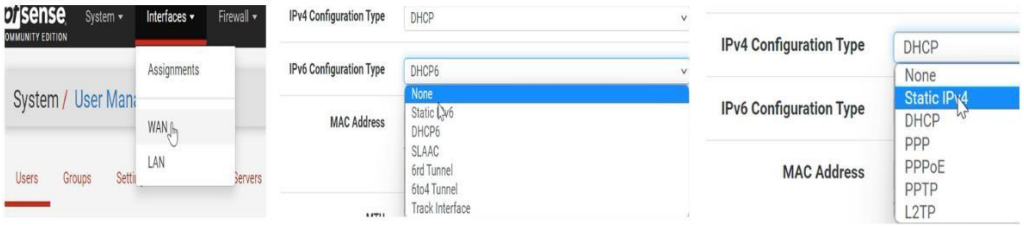
Interface LAN2 fw-bejaia



Interface DMZ fw-bejaia

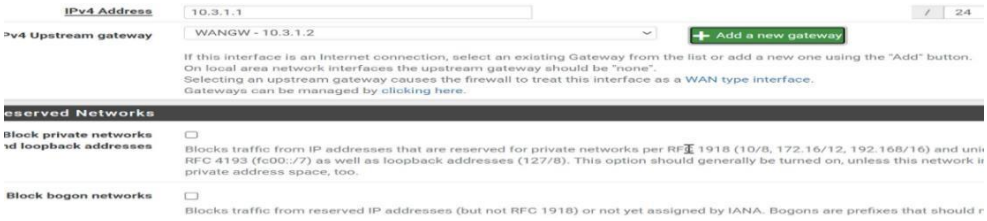
Connecter le pfsense Alger à l'internet :

Cliquant sur Interfaces, aller au WAN et enlevé l'ipv6 et le DHCP,



Interface WAN fw-alger (1)

Apres on va donner les adresses à l'interface WAN de fw-alger (10.3.1.1) et donner adresse de Gateway (10.3.1.2), décocher les deux dernières lignes pour permettre utiliser les @ privées, et on va sauvegarder.

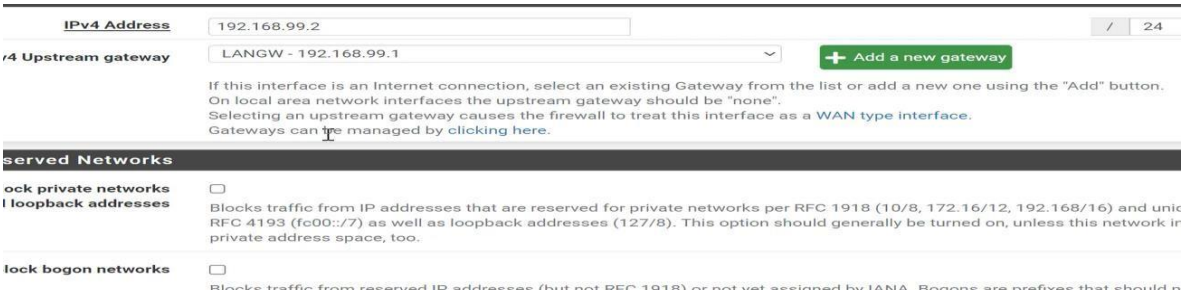


Interface WAN fw-alger (2)

Interface LAN :

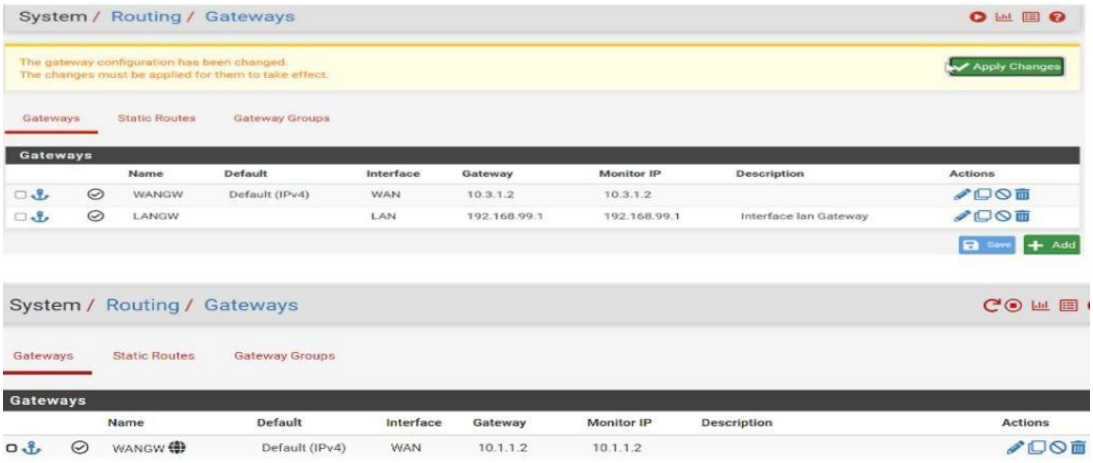
Pour LAN la même chose

Donc on va donner les adresses à l'interface LAN de fw-Alger (192.168.99.2) et donner adresse de Gateway (192.168.99.1), et décocher les deux dernières lignes pour permettre utiliser les @ privées, puis on va sauvegarder.



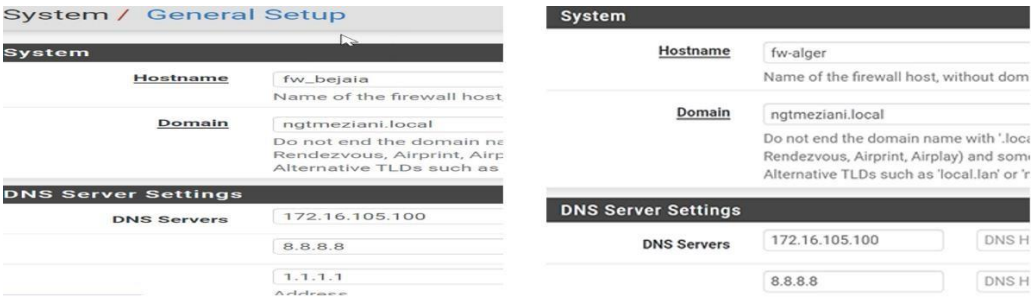
Interface LAN fws-alger

Le résultat : en haut on trouve le résultat de fw-alger, en bas c'est le résultat de fw-bejaia,



Changer nom et adresse DNS :

On va aller vers system, on va cliquer sur General Setup ensuite on va changer le nom et on va donner l'adresse de serveur distant DNS



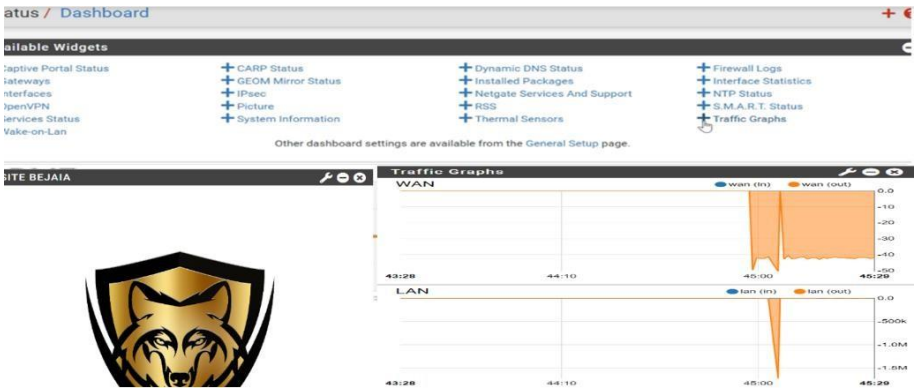
Changer le nom et donner l'adresse DNS (pour chaque pfsense)

Afficher les graphes et la photo :

Sur le tableau de bord de site Bejaia en va cliquer sur Traffic Graphs pour ajouter les graphes (trafic graphe pour afficher le graphe entrant et sortant),

Et on va ajouter une photo à partir de Picture.

De la même façon pour site Alger,



L'ajout de trafic graphe et la photo (fw-bejaia)

Bibliographie

[1] PDF, Cours de Réseaux, Université Lumière Lyon 2

[2] Réseaux et Télécoms, Dunod 4e édition, Paris,2013, Claude Servin.

[3] Voyage au cœur de l'informatique : Technologies, usages, enjeux, édition ISTE, grande Bretagne, 2021, Jean-Loïc Delhaye.

[4] Initiation-aux-réseaux, Eyrolles 7éme édition, 2011, Guy Pujolle.

[5] PDF, Université Nice SOPHIA ANTIPOLICE

[6] TCP/IP et les protocoles Internet, ENI 2e édition, Décembre 2006, Philippe Atelin, José Dordoigne

[7] CISCO interconnexion des réseaux à l'aide des routeurs et commutateurs, Edition ENI, novembre 2003, Djillali SEBA

[8] Les technologies IPv4 et IPv6 protocoles et transitions, LAVOISIER 2012, André Pérez

[9] CISCO Installation, Configuration et maintenance de réseaux, Editions ENI, Octobre 2003, Djilali SEBA

[10] Les autoroutes de l'information, Un produit de la convergence, Presse de l'Université du Québec, 1995, par Jean-Guy Lacroix et Gaëtan Tremblay

[11] Network+ notions fondamentales sur les réseaux locaux et étendus, Editions ENI, José Dordoigne

[12] ACISSI, sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre, (3ème édition) Broché – 12 septembre 2012

[13] Solange Ghernouatu-Hélie, sécurité informatique et réseaux, Dunod, 2008.

[14] : Michèle Germain, Introduction aux réseaux, Livre blanc Forum ATENA.

[15] Lourent Bloch-Christophe Wolfhugel. EYROLLES, 2éme édition. 2005

[16] : Cédric Lorens, Informatique et Réseau d'un opérateur de télécommunication, édition

[17] : Jean-Luc, Réseaux d'entreprise par la pratique, EYROLLES.

[18] : PORTE, L. Topologie réseau : le modèle hiérarchique en 3 couches. Disponible sur bibabox:, (2011, août 3).

[19]: Edwards, Wade. CCNP Complete Study Guide (642-801, 642-811, 642-821, 642-831). Sybex. © 2005

[20] : CRAFT.M, Active Directory pour Windows 2000 Server, Edition EYROLLES, Paris, 2002.

[21] : William.R. S, Guide de l'administrateur Windows server 2012, Edition Dunod, 2007.

[22] : KOUASSI T. ingénieur en conception informatique, Centre d'expertise et de perfectionnement en informatique, Etude et optimisation du réseau local,2007

[23] I. GADOUCHE H. BABA HAMED, Installation mise en place des VLANs sécurisation des ports,

[24] F. Emmanuel, « Technologies VLAN » http://cisco.goffinet.org. Février 2013

[25] F. Nolot. Cours5-VTP. Académie Cisco, 2007

[26] NetworkLab, sécurité niveau 2, available : https://www.networklab.fr/securite-deniveau-2/

[27] : Gerardo RUBINO et Laurent TOUTAIN, Réseaux locaux, Ecoule Nationale Supérieure des télécommunications de Bretagne, Campus de rennes.

[28] BONNES PRATIQUES, PLANIFICATION ET DIMENSIONNEMENT DES INFRASTRUCTURES DE STOCKAGE ET DE SERVEUR EN ENVIRONNEMENT VIRTUEL, Books on Demand, France, 2011, Cédric GEORGEOT.

[29] BCMSN Exam Cram 2, Que Publishing, 2004, Richard A. Deal.

[30] PDF, Université de Nouvelle-Galles du Sud, Université en Australie

[31] Intégration des infrastructures réseaux et systèmes, conception, implémentation, sécurité et supervision, ISTE Editions Ltd, Great Britain, 2021, Saida HELALI.

[32] Document officiel, campus NTS, 2020.

Webographie

[A] http://reussirsonccna.fr/. Comment-separer-son-reseau-avec-les-vlan, Mars 2013 ; Consulté en Juin 2023

[B] type de vlan, URL http://www-igm.univ-mlv.fr ; Consulté en Juin 2023

[C]https://www.ibm.com/docs/fr/aix/7.3?topic=teaming-ieee-8023ad-link-aggregation-configuration ; Consulté en Juin 2023

[D] https://cisco.goffinet.org/ccna/disponibilite-lan/redondance-de-passerelle-host-standby-router-protocol-hsrp/#:~:text=1.1.-,First%20Hop%20Redundancy%20Protocols,d%C3%A9faut%20dans%20les%20r%C3%A9seaux%20locaux ; Consulté en Juin 2023

[E] https://slideplayer.fr/slide/9511942/ ; Consulté en Juin 2023

[F] https://afrozahmad.com/blog/hsrp-vs-vrrp-vs-glbp/ ; Consulté en Juin 2023

Résumer

L'étude et la mise en place d'une nouvelle installation réseau sécurisée sont essentielles pour protéger les données et le réseau d'une organisation contre les cyberattaques, les intrusions et les fuites d'informations. L'étude implique d'évaluer les besoins en sécurité, d'analyser les risques et les vulnérabilités. Ensuite, la mise en place comprend la sélection et la configuration d'équipements de sécurité appropriés, tels que le pare-feu, les systèmes de détection d'intrusion (IDS) et les protocoles de sécurité IPSec. La sensibilisation et la formation des utilisateurs sont également importantes pour minimiser les risques liés à une utilisation inappropriée du réseau. En somme, ces processus complexes permettent de mettre en œuvre des mesures techniques et organisationnelles afin d'assurer une protection solide contre les cybermenaces.

Mots Clés : cyberattaques, intrusion, fuites d'information, IDS, protocoles de sécurité, cybermenaces.

Abstract

The study and implementation of a new secure network installation are essential to protect an organization's data and network from cyberattacks, intrusions, and information leaks. The study involves assessing security needs, analyzing risks, and vulnerabilities. Subsequently, the implementation includes selecting and configuring appropriate security equipment, such as firewalls, intrusion detection systems (IDS), and security protocols (expl : IPSEC). Raising awareness and providing user training are also important to minimize risks associated with improper network usage. In summary, these complex processes enable the implementation of technical and organizational measures to ensure robust protection against cyber threats.

Keywords : cyberattacks, intrusions, information leaks, IDS, security protocols, cyber threats