**République Algérienne Démocratique et Populaire**
**Ministère de l'Enseignement Supérieure et de la Recherche Scientifique**
**Université Abderrahmane Mira**
**Faculté de la Technologie**

**Département d'Automatique, Télécommunications et d'Electronique**

# Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

## Thème

**Mise en place d'une sécurité réseau basée sur l'utilisation des pare-feu et des liaisons virtuelles (BMT)**

**Préparé par :**

- BOURENGUITE Imane

**Dirigé par :**

- M. Diboune Abdelhani

**Examiné par :**

- M. Alliche (président)
- Mme Gherbi (examinatrice)

**Année universitaire** : **2022/2023**

# Remerciement

*Tout d'abord, je remercie le bon Dieu qui m'a donné la force et la volonté d'accomplir ce travail.*

*Je tiens à remercier* ***M. DIBOUNE*** *pour la qualité de son encadrement exceptionnelle, son aide, sa patience et sa disponibilité durent la préparation de ce projet de fin d'études.*

*Mes vifs remerciements vont aux membres de jury* ***Mr.ALLICHE*** *et* ***Mme.GHERBI*** *d'avoir accepté d'examiner mon travail.*

*Je remercie également* ***M. REGRAGE*** *pour son aide pratique pendant l'élaboration de ce travail.*

*Je profite de cette occasion pour remercier tout le personnel de l'entreprise BMT pour leurs caractères accueillants et leurs encouragements.*

*Je tiens à remercier tous les enseignants à tous les niveaux ainsi que tout le personnel de la faculté technologie de l'université de Béjaïa, particulièrement ceux du département ATE.*

# Dédicace

*Avec un énorme plaisir, je dédie ce travail :*

*À ma très chère mère Fella, Mon cher père Nourdine*

*Pour leurs soutiens, sacrifices, conseils et leurs encouragements aucun dédicace ne pourrait être à la hauteur de ce que j'ai pu recevoir de leur part.*

*Que Dieux vous garde et vous accorde longue vie.*

*À ma chère sœur Yasmine.*

*Mon petit frère Abdelmoumene.*

*Que Dieu leur donne santé, bonheur et réussite.*

*À mon cher Nassim qui m'a épaulé durant toute cette si longue période.*

*À ma grande famille,*

*Plus particulièrement à ma chère grande mère.*

*À ma chère copine Nouara.*

*À tous ceux qui m'ont aidé à réaliser ce travail*

# Table des matières

# Liste des figures

# Liste des listings

# Liste des tableaux

# Liste des abréviations

## A

| | |
|---|---|
| ACL | Access Control List |
| AD | Active Directory |
| AH | Authentification Header |
| ARPANET | Advanced Research Projects Agency Network |
| ARP | Adresse resolution protocol |
| ATM | Asynchronous Transfer Mode |

## B

| | |
|---|---|
| BMT | Béjaia Mediterranean Terminal |
| BMT Spa | Béjaia Mediterranean Terminal Société Par Action |
| BPDU | Bridge Protocol Data Units |
| BSD | Berkeley Software Distribution |

## C

| | |
|---|---|
| CHAP | Challenge Handshake Authentification Protocol |
| CTMS | Container Terminal Management System |

## D

| | |
|---|---|
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | DeMilitarized Zone |
| DNS | Domain Name System |
| DOS | Denial of Service |
| DDOS | Distributed Denial of Service |
| DTP | Dynamic Trunking Protocol |

## E

| | |
|---|---|
| EPB | Entreprise portuaire de Bejaia |
| ESP | Encapsulated Security Payload |

## F

| | |
|---|---|
| FAI | Fournisseur d'Accès Internet |
| FDDI | Fiber Distributed Data Interface |
| FHRP | First Hop Redundancy Protocole |
| FTP | File Transfer Protocol |
| FTPs | File Transfer Protocol Secure |

## G

| | |
|---|---|
| GLBP | Gateway Load Balancing Protocol |
| GNS3 | Graphical Network Simulator-3 |
| GRE | Generic Routing Encapsulation |

## H

| | |
|---|---|
| HDLC | High-Level Data Link Control |
| HSRP | Hot Standby Redundancy Protocol. |
| HTTP | Hypertext Transfer Protocol |
| HTTPs | Hypertext Transfer Protocol Secure |

## I

| | |
|---|---|
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| ISL | Inter Switch Link |
| ISO | International Stendard Organisation |
| ITU | International Telecommunication Union |

## L

| | |
|---|---|
| LACP | Link Aggregation Control Protocol |
| LAN | Local Area Network |
| LLC | Logical Link Control |
| L2F | layer 2 forwarding |

| | |
|---|---|
| L2TP | layer 2 forwarding tunneling protocol |

## M

| | |
|---|---|
| MAC | Medium Access Control |
| MAN | Metropolitan Area Network |
| MAU | Multiple Access Unit |
| MITM | Main In The Middle |
| MPLS | Multi-Protocol Label Switching |
| MPPE | Microsoft Point-to Point Encryption |

## N

| | |
|---|---|
| NAT | Network Address Translation |
| NGFW | Next Generation Firewall |
| NAS | Network Attached Storage |

## O

| | |
|---|---|
| OSI | Open Systems Interconnection |

## P

| | |
|---|---|
| PAGP | Port Aggreration Protocol |
| PAN | Personal Area Network |
| PAP | Password Authentification Protocol |
| PIN | Personal Identification Nimber |
| POP | Post Office Protocol |
| PPP | Point to Point Protocol |
| PPTP | point to point tunneling Protocol |
| PVLAN | Private Virtual local area network |

## R

| | |
|---|---|
| RFCs | Requests For Comments |
| ROAS | Router On a Stick |

## S

| | |
|---|---|
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |

| | |
|---|---|
| SQL | Structured Query Language |
| SSH | Secure Socket Shell |
| SSL | Transport Layer Security |
| STP | Spanninge Tree Protocol |
| SVI | Switch Virtual Interface |
| SYN/ACK | Synchronize, cknowledge |

## T

| | |
|---|---|
| TCI-tag | Tag control information |
| TCP | Transmission Control Protocol |
| TelNet | Terminal Network |
| TPID | Tag Protocol Identifier |

## U

| | |
|---|---|
| UDP | User Datagram Protocol |
| USB | Universal Serial Bus |
| UTM | Unified Threat Management |

## V

| | |
|---|---|
| Vlan | Virtual local area network |
| VMPS | Virtual Local Area Network Management Policy Server |
| VPN | Virtual Private Network |
| VRRP | Virtual Router Redundancy Protocol |
| VTP | VLAN Trunking Protocol |

## W

| | |
|---|---|
| WAN | Wide Area Network |
| WIFI | Wireless Fidelity |
| WIMAX | World Wide Interoperabilite for Microware Access |
| WLAN | Wireless Local Area Network |
| WPAN | Wireless Personal Area Network |

## Z

| | |
|---|---|
| ZEP | zone extra portuaire |

# Introduction générale

Aujourd'hui, la plupart des entreprises possèdent de nombreux postes informatiques reliés entre eux afin d'assurer le transport des données entre utilisateurs d'une manière fiable, sécurisée, rapide et qui permet d'assurer un bon service même dans les grandes distances entre les équipements à partir desquels les utilisateurs s'échangent des services divers.

Cela nécessite des techniques de plus en plus élaborées, une bonne connaissance des mécanismes de base et une maîtrise des technologies utilisées. Il est également recommandé de pouvoir gérer la sécurité d'un réseau informatique et de prendre des mesures contre les menaces. Pour cela, une architecture de réseau sécurisée est nécessaire afin de garantir la confidentialité des données des entreprises.

Avec le développement de l'informatique, les méthodes permettant une protection efficace des systèmes informatiques et des réseaux ne cessent de se multiplier avec la multiplication des attaques qui utilisent des différents techniques pour nuire à un réseau, de ce fait plusieurs techniques de protection des réseaux informatiques sont proposées parmi ces techniques nous citons les pare-feu, les liaisons virtuelles VLAN et VPN, l'antivirus, les serveurs proxy, les systèmes de détection d'intrusion, etc.

Dans ce cadre s'inscrit notre projet de fin d'études qui consiste à la mise en place d'une sécurité réseaux basée sur l'utilisation des pare-feu et des liaisons virtuelles au sein de l'entreprise BMT (Bejaia Mediterranean terminal).

Durant notre stage, nous avons fait une analyse détaillée de leur réseau et localisé les principales failles pour pouvoir proposer une architecture améliorée en implémentant d'autres techniques de sécurité qui sont : la configuration des VLAN et la segmentation du réseau pour pouvoir gérer les sous-réseaux d'une manière fiable et sécurisée, la reconfiguration de pare-feu pour bénéficier de ses performances et l'isolation des applications Web sur un propre réseau qui est la DMZ qui sera gérée par le pare-feu, la configuration de VPN entre les deux sites distants de l'entreprise et la mise en place d'un pare-feu secondaire pour avoir la haute disponibilité.

Pour mener à bien notre projet, nous l'avons structuré en quatre chapitres qui sont organisés comme suit :

Le premier chapitre présente les concepts de bases d'un réseau informatique, les différentes attaques qu'il subit ainsi les techniques de sécurité d'un réseau.

Le deuxième chapitre intitulé "Les pare-feu et les liaisons virtuelles " détaillera ses trois techniques de sécurité.

Le troisième chapitre concerne la présentation de l'organisme d'accueil BMT, la description de la structure de leur réseau où nous exposerons la problématique ainsi que les différentes solutions pour améliorer la sécurité de ce réseau.

Le dernier chapitre est consacré à la définition des différents outils et logiciels ayant servi à réalisation de notre implémentation, tout en expliquant les configurations établies ainsi que les tests effectués pour vérifier nos simulations.

On termine par une conclusion générale qui récapitule les points essentiels de ce travail.

# Chapitre I :

## Généralités sur les réseaux informatiques et leurs sécurités

# *Introduction*

Les réseaux informatiques sont devenus indispensables pratiquement dans tous les domaines de la vie humaine, en vue de leurs importances qui consiste principalement le partage et le transfert des données informatiques entre systèmes, il est nécessaire de protéger ses réseaux pour assurer une communication fiable et sécurisée entre les participants.

Ce chapitre est constitué de deux parties, la première est consacrée à la présentation de quelques notions de base sur le réseau informatique, ses classifications et la définition de ses modèles. Dans la deuxième partie, nous allons aborder les différentes types d'attaques qui peuvent perturber et nuire un réseau informatique et on termine par les moyens et les solutions de sécurité possibles qui permettent de faire face à ces attaques.

## 1.1 Généralités sur les réseaux informatiques

### 1.1.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements électroniques indépendants (ordinateur, commutateur, routeur, imprimante, etc.) interconnectés par des supports de transmission (filaire ou sans fil) afin de permettre à des personnes de changer et de partager des informations et des services.

Les réseaux sont différenciés et catégorisés selon leurs topologies, leurs tailles, la portée, l'usage et les services offerts.

### 1.1.2 Objective de la mise en réseau

- L'échange et le partage des données informatiques.
- La communication et la messagerie électronique.
- La transmission de fichiers de différents types.
- Les jeux vidéo multi-joueurs.
- Fournis l'accès à des bases de données.

### 1.1.3 L'étendue géographique d'un réseau

#### 1.1.3.1 Définition

L'étendue d'un réseau correspond à un ensemble de contraintes (nombre de postes reliés, leur éloignement…) que le concepteur devra prendre en compte lors de la réalisation de son réseau.

Il existe de nombreux types de réseau, on distingue généralement quatre catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau.

1.1.3.2 Catégorie du réseau selon l'étendue

a. **Personal area network (PAN)**

C'est un réseau personnel qui permet d'interconnecter sur quelques centimètres à quelques mètres, des appareils tels qu'un téléphone mobile, ordinateur, clavier, impriment, etc. qui sont proches de l'utilisateur dans le but de partager et synchroniser des données, des photos, des e-mails ou d'autres sur les deux appareils.

La connexion de ses équipements au réseau PAN peut être filaire par un FireWire ou USB pour connecter un portable à un ordinateur. Ou sans fil qui est le WPAN, grâce à des protocoles de connectivité sans fil à faible portée qui est l'IEEE.802.15 tel que Bluetooth (IEEE.802.15.1) et Zigbee (IEEE.802.15.4) pour connecter par exemple un écouteur sans fil à un smartphone.

Figure 1.2-Architecture WPAN.

Figure 1.1-Architecture WPAN.

b. **Local area network (Lan)**

Le réseau local (LAN) est composé de deux ou plusieurs équipements informatiques (ordinateurs, téléphone, serveur…) reliés entre eux par des supporte de transmission filaire (câble) ou sans fil (WLAN) afin de partager des ressources communes, d'échanger des données dans une aire géographique de quelques centaines de mètres.

Sa taille correspond par exemple à des réseaux intra-entreprise (RLE), un bâtiment ou un cybercafé.

Les débits de ces réseaux vont aujourd'hui de plusieurs centaines de mégabits à quelques mégabits par seconde grâce aux technologies Ethernet et Wi-Fi les mieux adaptés à ces réseaux.

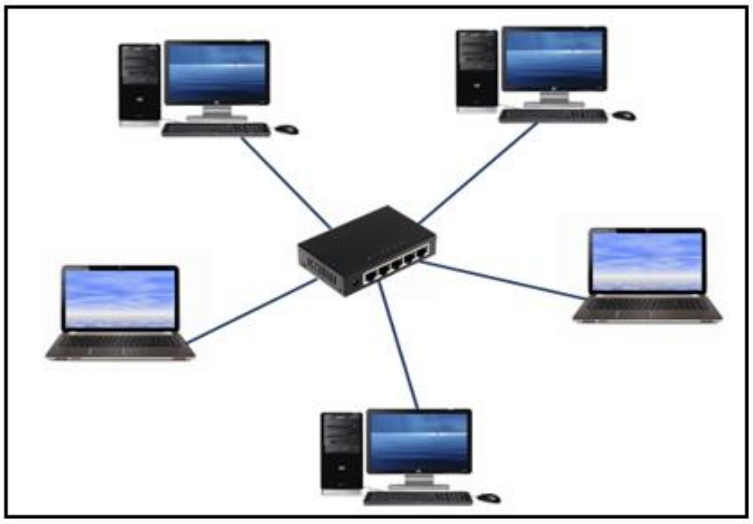


Figure 1.3-Architecture LAN.

### c. Metropolitan area network (MAN)

Le réseau métropolitain permet l'interconnexion des particuliers sur un réseau à haut débit qui est géré à l'échelle d'une ville.

Pour surmonter la limitation en distance, en nombre de machines et en débit, des réseaux locaux (proches géographiquement) ont été fédérés et interconnectés généralement par des câbles à fibre optique pour donner un réseau métropolitain nommé également réseau fédérateur pour permettre des communications sur des distances de quelques kilomètres.

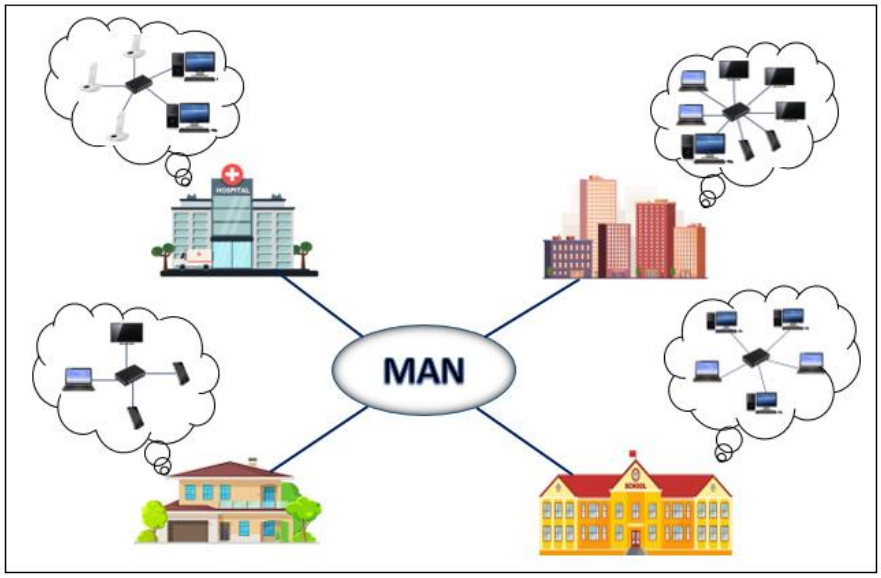



Figure 1.4-Architecture MAN.

d. **Wide area network WAN**

C'est un réseau étendu regroupe un ensemble de LAN et MAN distants géographiquement et reliés par des lignes téléphoniques à haut débit. Ces réseaux sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents.

Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellites, mais seulement pour des applications particulières à débit faible. (1)

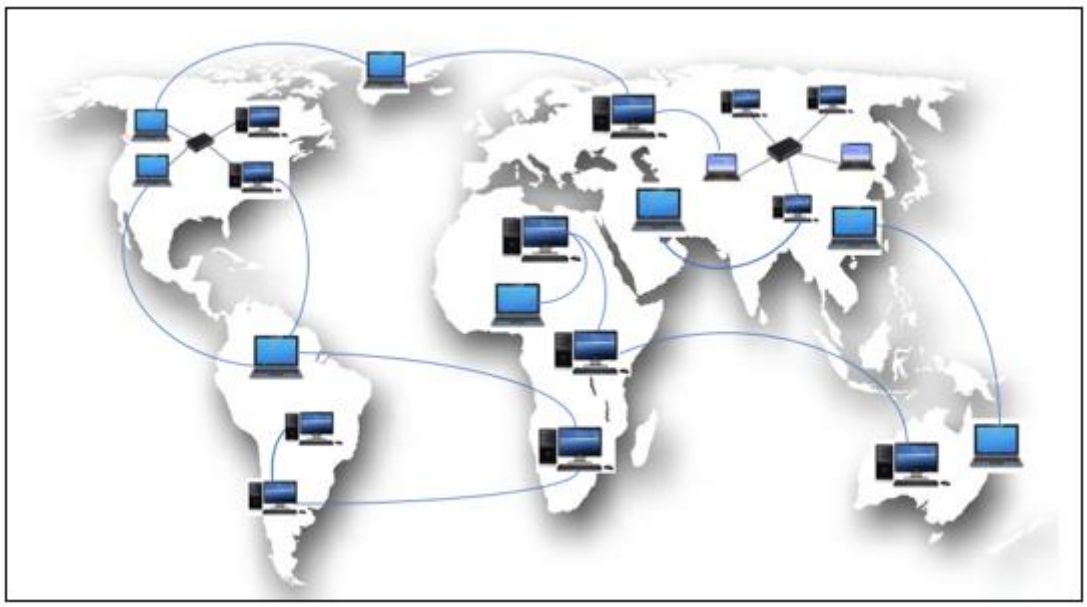


Figure 1.5-Architecture WAN

## 1.1.4 Topologie de réseau

### 1.1.4.1 Définition

La topologie physique d'un réseau correspond à son architecture physique qui décrit la manière dans les équipements (ordinateur, modem, switch, hub, routeur…) sont raccordées entre eux grâce à des supports physiques (paire torsadée, câble coaxial, fibre optique…).

Tant dite que la topologie logique renseigne sur le mode d'échange des données d'un nœud à un autre dans un réseau. Elle est basée sur les protocoles de la couche liaison du modèle OSI qui fournissent les normes utilisées et à partir de celle-ci, il est possible de définir la méthode d'accès au canal. Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI.

### 1.1.4.2 Type de topologie physique

Les réseaux utilisent les topologies de base comme le bus, l'anneau et l'étoile ou d'autre tel que maillée et arbre ou encore des combinaisons de celles-ci ce qui donne la topologie hybride.

a. **Bus :**

L'ensemble des équipements sont reliés à un câble commun généralement par des raccords type T, cette topologie est une variante de la liaison multipoint où l'information émise par une station est diffusée sur tout le réseau, ce mode est dit aussi réseau à diffusion. On désigne deux types : (2)

Bus unidirectionnel : les données ne peuvent circuler que dans un sens et la transmission entre les stations est assurée par l'intermédiaire de deux canaux séparés.

Bus bidirectionnel : les données peuvent circuler dans les deux sens, mais non simultanément, car le câble est unique, lorsqu'une station émet, le signal se propage dans les deux sens, de part et d'autre vers toutes des autres stations.

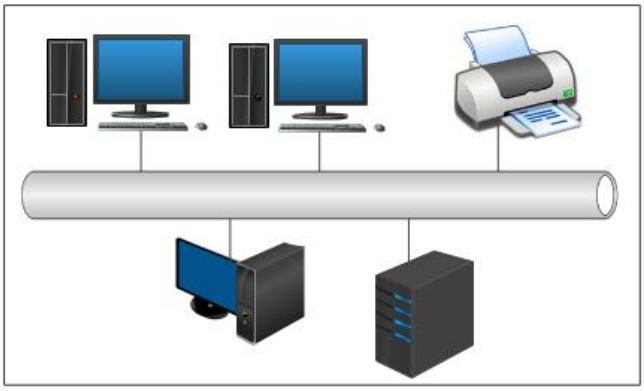


Figure 1.6-Topologie en Bus.

b. **Etoile :**

C'est une variante de la topologie en point à point où tous les nœuds du réseau sont reliés à un équipement central qui est le commutateur (avant, c'était par un concentrateur) afin d'assurer la communication entre les équipements de ce réseau.

Les grands fabricants offrent des switchs de 8, 12, 16, 32, 48 ou 96 prises ce qui permet donc de construire une étoile unique avec près de 100 ordinateurs à connecter. (3)

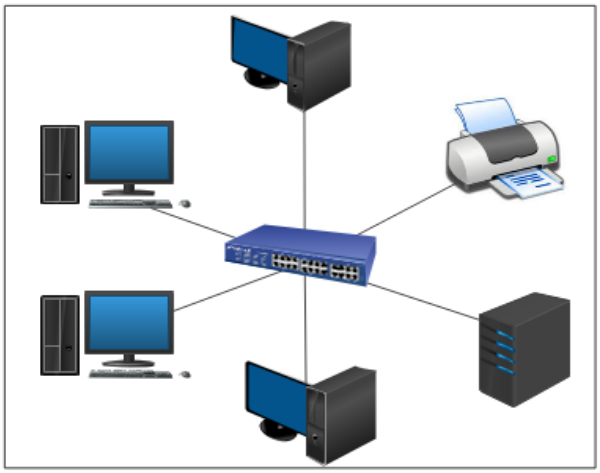


Figure 1.7-Topologie en étoile.

c. **Anneaux**

Token ring en anglais, chaque équipement est relié à deux équipements voisins de telle façon a ce que l'ensemble constitue une boucle fermée comme est illustré sur la figure (1.8).

La donnée diffusée circule tout au long de l'anneau dans une seule direction, lorsque le passage de la donnée par une station de travail, celle-ci l'accepte que si le message lui est destiné, sinon il le fait passer au nœud suivent.

Dans une topologie en anneau, chaque station participe à la diffusion du message et à sa régénération. L'arrêt d'une station interrompt ce mécanisme. Pour pallier ceci, les stations sont raccordées physiquement à un concentrateur d'accès (répartiteur MAU : Multiple Access Unit) dont le rôle est de détecter les stations hors service et de court-circuiter leur raccordement (by-pass). (4)

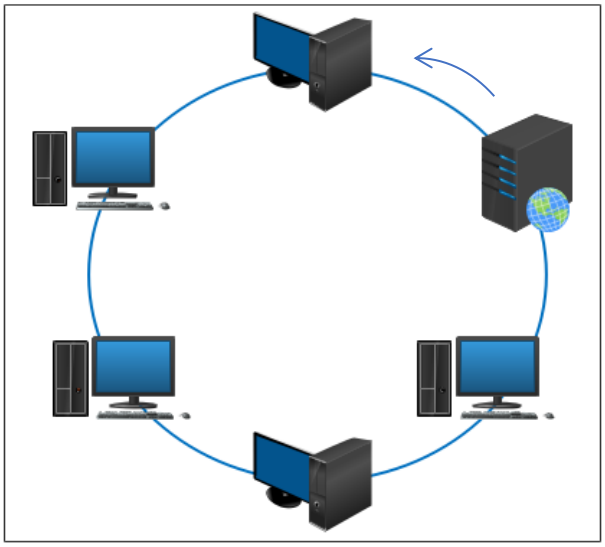


Figure 1.8-Topologie en anneaux.

## 1.2 Modèles et protocoles réseaux

Pour permettre la communication entre les différentes machines du réseau, il faut que toutes ses machines puissent se comprendre pour cela, il est nécessaire qu'elles parlent le même langage et les règles de cette langue commune de la communication réseau sont définies par les deux modèles OSI et TCP/IP.

### 1.2.1 Modèle OSI

1.2.1.1 Définition

ISO (international standard organisation) à développer un modèle de référence pour l'interconnexion des systèmes ouverts (tout équipement à interconnecter : ordinateur, terminal…) appelé OSI « Open System Interconnection » qui se traduit en français par « interconnexion des systèmes ouverts ».

Le modèle OSI est une architecture abstraite de communication, décrit dans la norme X.200 de l'ITU (International Télécommunication Union) dans le but d'assurer la communication entre les différents systèmes et de résoudre les problèmes d'interconnexion d'équipements hétérogènes. Il est composé de sept couches indépendantes, chacune remplissant une partie bien définie des fonctions permettant l'interconnexion. (5)
Ses couches sont reliées entre elles par deux types de relations :

### 1.2.1.2 Les couches de modèle OSI

Les sept couches peuvent être regroupées en trois blocs fonctionnels. (2)
Comme illustré sur la figure (1.9)

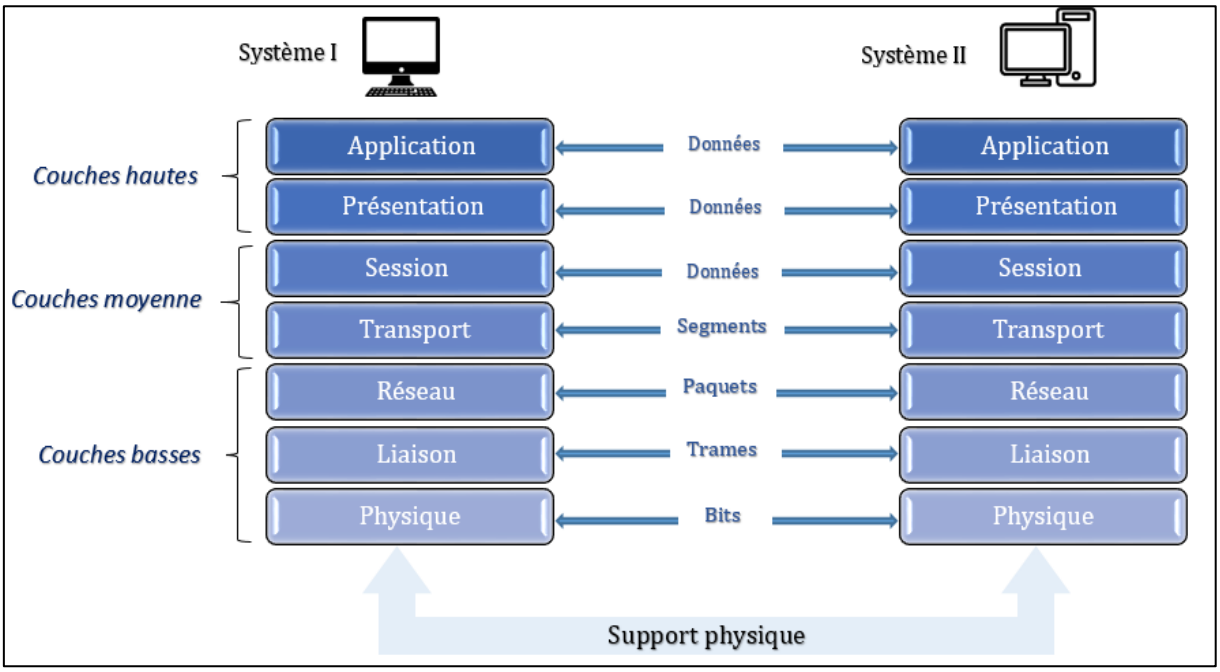



Figure 1.9-Le modèle OSI.

**Les couches basses** : regroupe les couches 1,2 et 3, elles assurent la transmission et l'acheminement des informations à travers le réseau sur le support (câble, transmission sans fil…).

La couche physique : cette couche comporte les éléments physiques appliqués dans le transfert des données, elle définit donc l'interface, les connecteurs et le câblage utilisés. L'unité de données manipulées à ce niveau est le bit.

La couche liaison : fournis les moyens d'établir et de maintenir les connexions entre les entités de réseau et les méthodes de contrôle d'accès au support (MAC) et de contrôle de liaison logique (LLC). De plus, elle détecte et elle corrige les erreurs de la couche physique. La trame est l'unité de données manipulées par cette couche.

La couche réseau : assure l'adressage et le routage des trames de données regroupées en paquets à travers le réseau, elle permet aussi l'interconnexion de réseau hétérogène.

**Les couches moyennes :** composées des deux couches 4 et 5, elles gèrent les communications et les ressources (processus et mémoire) nécessaires à l'échange des messages entre équipements terminaux.

La couche transport : responsable de la transmission des données de bout en bout, elle assure les fonctions de contrôle de flux, la résolution des pertes et le réassemblage des paquets en message.

La couche session : responsable de l'ouverture et la fermeture des sessions de communication entre les machines du réseau ainsi elle organise et synchronise le dialogue entre les systèmes d'extrémité.

**Les couches hautes :** regroupe les couches 6 et 7 et elles traitent les données échangées (exécution de commandes, mise en forme, affichage, etc.).

La couche présentation : s'occupe de la préparation et de la mise en forme des données afin qu'elles puissent être utilisées par la couche application, elle se charge aussi de la conversion, la compression de données et de la sécurité des informations (chiffrement/déchiffrement).

La couche application : c'est le point d'accès aux services réseaux (navigateur web, la messagerie électronique, etc.). Elle présente donc le niveau le plus proche des utilisateurs.

### 1.2.2 Modèle TCP/IP

#### 1.2.2.1 Définition

Le modèle TCP/IP est une architecture de communication implémentée au sein des machines, il simplifie le modèle théorique OSI en 4 couches. Son origine remonte au réseau de télécommunications ARPANET.

Ce dernier regroupe un ensemble de protocoles fonctionnant sur les différentes couches et il porte le nom des deux protocoles principaux qui le constituent : le TCP (Transmission Control Protocol) et IP (Internet Protocol). La majeure partie des informations relatives à ces protocoles sont définies dans les RFCs (Requests For Comments). Les RFCs contiennent les dernières versions des spécifications de tous les protocoles TCP/IP. (6)

#### 1.2.2.2 Les couches TCP/IP

L'architecture de protocoles TCP/IP est construite sur un modèle en couches « pile TCP/IP » qui est moins complet que la proposition de l'ISO. Quatre couches sont suffisantes pour définir l'architecture de ce protocole.

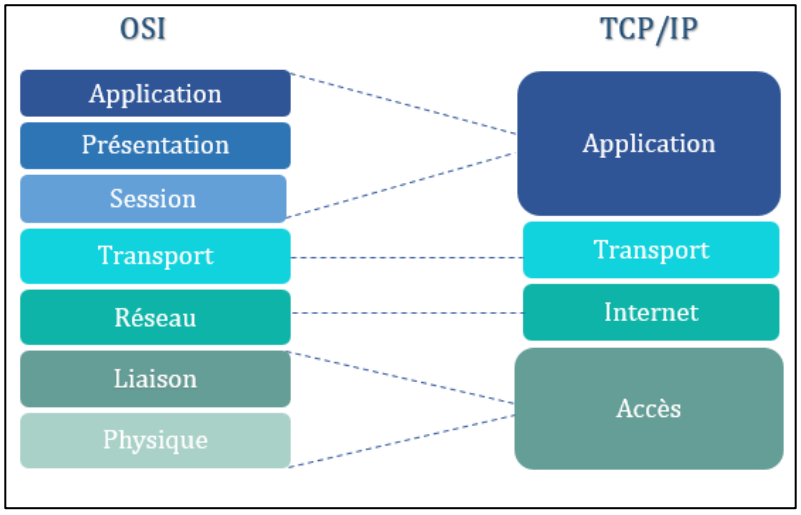



Figure 1.10-Le modèle TCP/IP.

**La couche accès réseau :** définis comment les trames IP sont transmises. La définition de ceux-ci reste indépendante de la couche réseau, ce qui leur permet de s'adapter à chaque nouvelle technologie au fur et à mesure de leur apparition.

**La couche internet :** sur celle-ci se trouve le protocole IP (Internet Protocol) qui assure la connectivité des réseaux, l'acheminement et l'adaptation de la taille des données.
Un équipement sur un réseau doit avoir une configuration IP avec au minimum :

- Une adresse IP pour le distinguer sur le réseau et pouvoir communiquer avec.
- Un masque de sous-réseau (netmask) qui indique dans quel sous-réseau il se situe.
- Une passerelle (gateway) qui permet de communiquer à l'extérieur de ce réseau.

**La couche transport** : elle assure l'acheminement des données et elle renseigne sur l'état de la transmission. On se basant sur deux types de protocoles selon les besoins des utilisateurs : le TCP (Transmission Control Protocol), qui fonctionne en mode connecté et l'UDP (User Datagram Protocol) fonctionne en mode non connecté.

**La couche application :** elle contient tous les protocoles de haut niveau, utilisés par les différents logiciels afin de communiquer entre eux. Chaque programme d'application interagit avec la couche de transport pour définir le protocole de transport à utiliser.

### 1.2.3 Les protocoles

#### 1.2.3.1 Notion de protocole

Un protocole est une méthode standard qui définit un langage commun pour toutes les machines par lequel ils doivent communiquer, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il existe plusieurs types de protocoles selon le service souhaité.

1.2.3.2 Classification des protocoles

Les différents protocoles peuvent être classer selon les couches du modèle TCP/IP :

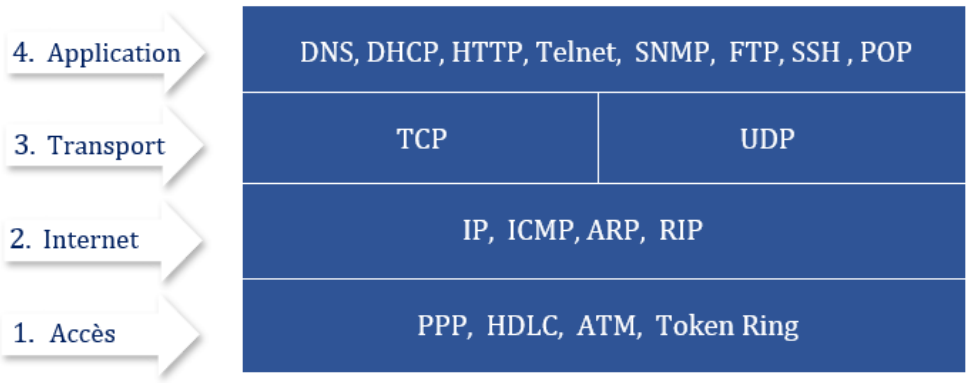



Figure 1.11-Classification des protocoles TCP/IP.

1.2.3.3 Les protocoles de redondance

Le protocole FHRP (First Hop Redundancy Protocole) fournit une redondance de passerelle par défaut par la configuration de deux routeurs : routeur actif qui prend en charge le trafic comme passerelle par défaut et routeur standby ou retour de secours pour permettre le basculement automatique de la passerelle par défaut vers le routeur secours en cas d'une panne,

Sur les équipements réseau, on ne peut avoir qu'une seule passerelle par défaut, l'intérêt de FHTP est de permettre d'avoir une passerelle par défaut « Virtuel » pour cela, il combine les routeurs pour utiliser une seule adresse IP virtuelle (VIP) et une adresse mac virtuelle (VMAC), l'utilisation de cette même correspondance VIP/VMAC donne l'impression aux terminaux qu'ils n'ont accès qu'à une seule passerelle par défaut.

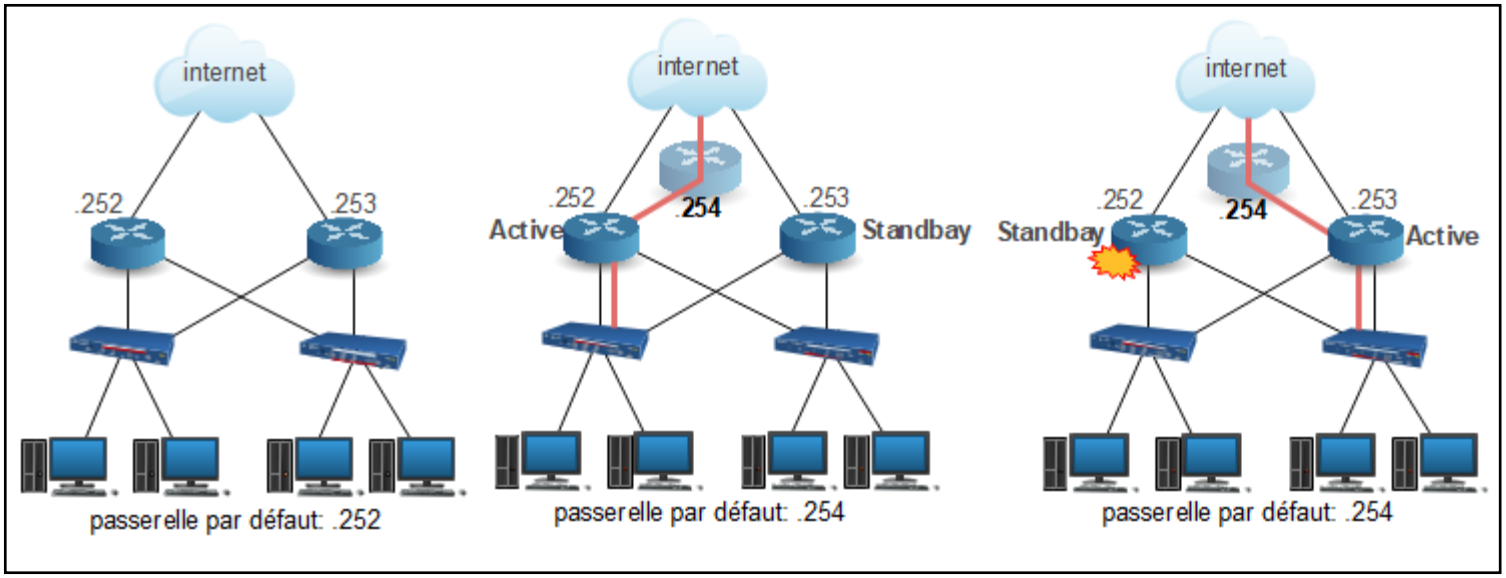



Figure 1.12-Principe de fonctionnement de protocole de redondance.

Il existe plusieurs protocoles FHRP, nous citons ces trois types suivis par leurs différentes caractéristiques.

- **HSRP :** Hot Standby Redundancy Protocol.
- **VRRP :** Virtual Router Redundancy Protocol.
- **GLBP :** Gateway Load Balancing Protocol.

Tableau 1.1-Les protocoles de redondances

| Protocol | HSRPv1 | HSRPV2 | VRRP | GLBP |
|---|---|---|---|---|
| Propriétaire | CISCO | | IEEE | CISCO |
| Support | IPv4 | IPv4/IPv6 | | |
| IP | 224.0.0.2 | 224.0.0.102 | 224.0.0.18 | 224.0.0.102 |
| Port | UDP 1985 | UDP 2029 | UDP 112 | UDP 3222 |
| Virtual MAC | 0000-0C07-Ac**xx** | 0000-0C9f-Fx**xx** | 0000-5E00-01**xx** | 0007-b4xx-xx**xx** |
| Groupe | 0-255 | 0-4095 | 0-254 | 0-1023 |
| Rôles | Active/Passive | | Master/Backup | AVG/AVF |
| priorité | 100 (Compris entre 0 &255) | | | |
| Hello timer | 3 sec | | 1sec | 3 sec |
| Hold timer | 10 sec | | 3.6 sec | 10 sec |
| Preempt | Disable | | Actif | Actif |

## 1.3 La sécurité des réseaux

### 1.3.1 Généralité sur la sécurité

1.3.1.1 Définition

La sécurité d'un réseau est l'ensemble des techniques mises en œuvre pour garantir que l'ensemble des machines du réseau fonctionnent de façon optimale et que les ressources d'un ordinateur ou d'un réseau sont utilisées uniquement par les personnes autorisées dans le but de protéger le réseau contre tout type d'attaque et de menace pouvant perturber sa fonctionnalité (modification, vol d'informations, etc.)

Pour cela, il est nécessaire d'identifier les menaces et connaître à quel endroit intervient l'attaque, il faut donc assurer :

- La sécurité des équipements.
- La sécurité des logiciels.
- La sécurité des données.
- La sécurité des télécommunications.

1.3.1.2 Services de sécurité

La sécurité informatique vise généralement cinq principaux objectifs : (7)

- **Intégrité :** garantit que les données n'ont pas été altérées durant la communication.
- **Confidentialité :** les données de la communication ne peuvent pas être connues ou accessibles par des personnes non-autorisées.
- **Authenticité :** assure et vérifie l'identité des utilisateurs grâce au contrôle d'accès (mot de passe par exemple) qui fournit l'accès à des ressources uniquement aux personnes autorisées.
- **Non-répudiation :** permet de garantir qu'aucun des correspondants ne pourra nier la réception ou la transmission d'un message.
- **Disponibilité :** garantit aux utilisateurs l'accès à un service ou à des données dans de bonnes conditions.

## 1.3.2 Les attaques réseau

1.3.2.1 Problèmes liés à la sécurité informatique :

- **Vulnérabilité :** c'est une faille ou une faiblesse dans un programme ou un système informatique, elle est due à la base à la négligence et la non prise en compte de certains aspects lors de la conception et la réalisation d'un travail, ce qui ronde ses systèmes sensibles aux attaques réseau.
- **Attaque :** une attaque réseau est une intrusion dans une infrastructure de communication afin d'obtenir un accès non autorisé à des ressources ou d'exploiter des vulnérabilités existantes. Elle est généralement constituée de deux phases : une attaque passive qui analysera, dans un premier temps, le trafic réseau pour collecter des informations sensibles, puis comme deuxième phase, une attaque active, qui consiste à nuire au réseau. (8)

1.3.2.2 Buts des attaques

Un attaquant peut avoir plusieurs objectifs qui peuvent être regroupés en quatre catégories : (9)

- **L'interruption :** vise la disponibilité des informations. (Déni de service, etc.).

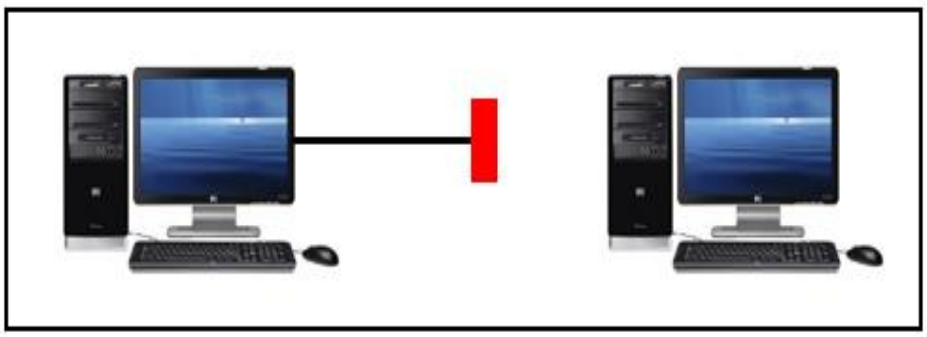


Figure 1.13-L'attaque pour l'interruption.

- **L'interception :** vise la confidentialité des informations circulant dans un réseau (capture de contenu, analyse de trafic, etc.).

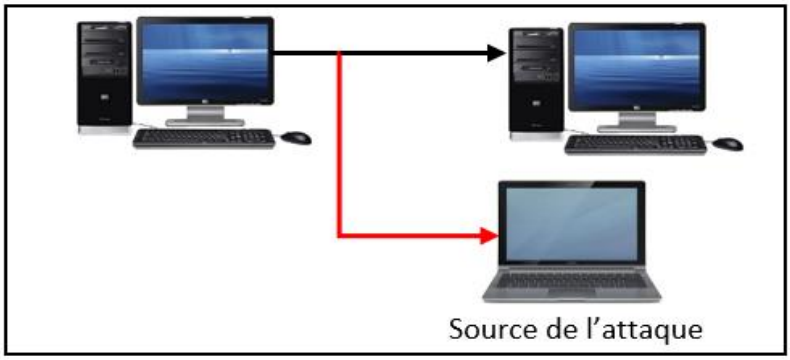



Figure 1.14-L'attaque pour l'interception.

- **La modification** : vise l'intégrité des informations (modification, rejeu, etc.).

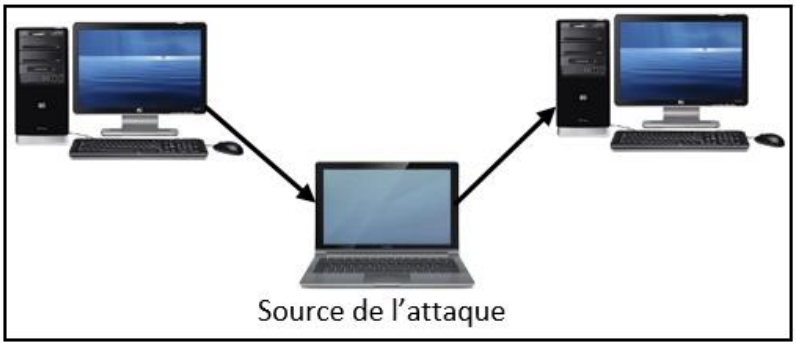



Figure 1.15-L'attaque pour la modification.

- **La fabrication :** vise l'authenticité des informations (mascarade, etc.).

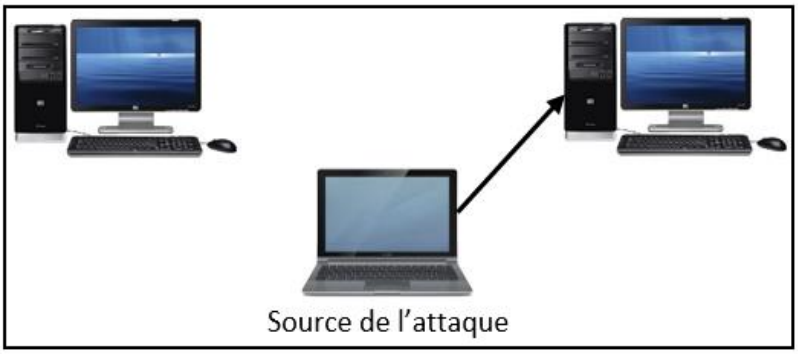



Figure 1. 16-L'attaque pour la fabrication

### 1.3.2.3 Type d'attaque réseau

Pour concevoir des solutions de sécurité des réseaux, il faut tout d'abord évaluer l'ensemble des attaques existantes et comprendre leur mode de fonctionnement. Ces attaques sont variées et elles visent les différents niveaux d'un système, pour cela, elles peuvent être classées selon les couches du modèle TCP/IP.

#### 1.3.2.3.1 **Attaques sur la couche applicative :**

##### a. **Attaque de mot de passe**

Les mots de passe sont stockés d'une manière chiffrée dans un fichier ou une base de données. Lorsqu'un pirate accède au système et récupère ce fichier, il lui est possible de tenter de casser le mot de passe d'un utilisateur.

Les deux types d'attaques les plus courantes sont :

- **Password craking** (Attaque de brute force) : le craquage d'un mot de passe consiste à trouver un mot de passe à travers des tentatives successives. L'attaquant devine et teste l'ensemble des combinaisons possibles jusqu'à trouver la bonne.

- **Attaque par dictionnaire** : cette attaque consiste à utiliser une liste de mots de passe prédéfinis dans un fichier externe, cette liste est appelée dictionnaire, la plus connue est le Rockyou dans lequel un programme crypte tous les mots un par un et les compare au mot de passe du système. (7)

##### b. **Password Sniffing**

Elle consiste à installer un renifleur de mot de passe sur une machine et analyser tout le trafic réseau entrant et sortant. Dans le but de récupérer et enregistrer les mots de passe circulant au sein d'un réseau. La raison principale de cette attaque est la faille des protocoles FTP, http, Telnet et SMTP qui est l'envoi de mots de passe et donnée en texte clair.

##### c. **Les Malware**

Ce sont des logiciels de malveillants installés sur des machines (ordinateur et serveur) dans le but d'endommager et détruire un système.

Il existe plusieurs types de malware, nous décrivons l'essentiel ci-dessous : (10)

- **Virus** : C'est un programme informatique qui a la capacité d'infecter un autre programme dans un système et qui a la possibilité de se reproduire, il peut se propager à travers tout moyen d'échange de données comme l'Internet ou encorde les disquettes, les clefs USB et les DVD.

- **Les Vers :** (worms) c'est un logiciel autonome capable de se reproduire par lui-même (il effectue ses copies en exécutant son propre code pour les envoyés à d'autres systèmes du réseau) dans le but de prendre le contrôle du système en utilisant des ressources comme la mémoire de l'ordinateur et la bande passante réseau. (11)

- **Spywares (logiciel espion)** :un spyware collecte des informations sur les victimes sans que celle-ci ne s'en rende compte notamment des mots de passe, des codes PIN ou des coordonnées bancaires en se basant sur l'enregistreur de frappe «Keylogger». (12)

- **Ransomware** : c'est l'un des malwares les plus répandus, il est basé sur le cryptage des données afin de bloquer l'accès à un système, puis l'attaquant demande à la victime d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. (13)

- **Cheval de Troie** : (Trojan horse) ce type de logiciel se présente comme étant une application ou programme attirant pour encourager les utilisateurs à l'installer, en suit, il s'exécute en arrière-plan. L'objectif de cette attaque est la préparation et l'installation d'autres types d'attaques.

d. **Buffer overflow**

Le débordement de tampon affecte généralement les programmes C pour le débordement de la mémoire tampon afin d'avoir l'accès au système, perturber l'exécution d'un programme et d'en prendre le contrôle, elle consiste à injecter des codes qui serrent stocker dans une zone de stockage temporaire (tampon) jusqu'à que la taille maximale des données dépasse la taille du tampon, ce qui écrase les informations et l'adresse de processus. (14)

e. **Injection SQL**

Cette attaque vise les bases de données. Elle est due au mal surveillance des données entrante saisie par l'utilisateur pour cela, il est possible à un pirate de modifier la requête SQL par l'injection d'un morceau de requête dans le code afin d'accéder à la base de données et d'extraire les informations.

f. **Usurpation d'identité HTTPS**

C'est l'une des techniques d'attaque Main In The Middle (MITM) qui consiste à placer une machine pirate entre le client et le serveur. De ce fait, le pirate a accès à toutes les communications sans que le client ne s'en rende compte.

Dans l'URL d'un site Web le « HTTPS » indique que ce site est sécurisé, l'attaquant peut tromper le navigateur en lui faisant croire qu'il visite un site Web sécurisé alors que ce n'est pas le cas. Dans le but de pouvoir surveiller l'interaction avec ce site Web et éventuellement voler les informations personnelles partagées. La vulnérabilité de ce protocole réside dans le manque de capacités de chiffrement, ce qui le rend moins sécurisé.

1.3.2.3.2 **Attaques sur la couche transport :**

a. **Scaning de port**

Le scan de port est une technique utilisée pour détecter les ports ouverts sur un hôte afin d'identifier les protocoles utilisés ce qui permet de déterminer le type d'attaque a utilisé, c'est une préparation à une attaque.

b. **Denial of Service (DOS)**

C'est l'attaque d'un pirate sur un serveur informatique de façon à l'empêcher d'offrir le service pour lequel il est destiné ainsi, l'accès à ce dernier devienne impossible aux clients dans le but de mettre le système en panne ou le ralentir au point de le rendre indisponible et inutilisable. (15)

Sur cette couche nous trouvons :

- **L'attaque SYN (TCP/SYN Flooding) :** c'est une attaque par saturation vise le mécanisme de poignée de main en trois temps (Three-ways handshake) du protocole TCP. Elle consiste à envoyer un grand nombre de requêtes SYN erroné au serveur (demandes successives d'ouverture de connexion TCP), ce dernier répond par le message SYN-ACK habituel, mais l'attaquant ne répond jamais par un message ACK pour achever la procédure de connexion. C'est alors une connexion semi-ouverte au bout d'un certain temps le serveur est saturé et ne peut plus accepter de connexions, car il se met dans un état d'attente infinie.

c. **Distributed Denial of Service (DDOS)**

Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de déni de service distribué (DDoS).

1.3.2.3.3 **Attaques sur la couche réseau :**

Les versions actuelles des protocoles IP ou ICMP, ne dispose pas de mécanisme d'authentification, de ce fait elles subissent des attaques qui s'appuient sur cette faiblesse. Parmi les principales attaques, on trouve :

a. **IP Spoofing**

Afin d'usurper l'adresse IP d'une autre machine, l'attaquant se place dans la communication client-serveur et falsifie son adresse IP, une fois il utilise l'adresse IP du serveur comme étant son adresse IP pour recevoir la requête de client afin d'obtenir son identité et l'autre fois il la remplace par celle de client et envoie une demande de connexion au serveur.

b. **Scanning IP**

Cette attaque lance une analyse sur une plage ou une liste d'adresses IP pour découvrir les adresses IP d'un réseau et déterminer celles qui sont activées.

c. **ICMP tunneling**

Le tunneling ICMP est une technique d'attaque de commande et de contrôle qui fait passer secrètement le trafic malveillant (établis une connexion secrète entre deux ordinateurs). Les données malveillantes passant par le tunnel sont cachées dans des requêtes d'écho et des réponses d'écho ICMP d'apparence normale. (16)

d. **Attaque de smurf**

Cette attaque est basée sur le serveur de broadcast et le Ping ICMP, dont lequel l'attaquant commence par falsifier son adresse IP pour se faire passer pour la machine cible et il envoie une requête Ping au serveur broadcast, ce dernier transmet cette requête à toutes les machines qui lui sont connectées, chaque machine envoie une réponse au serveur qui redirige l'ensemble de ses réponses vers la machine cible. Donc cette machine sera inondée et elle finira par se ralentir et se déconnecter de service.

La raison de ses deux types d'attaques est que le protocole ICMP n'a aucune mesure de vérification et de sécurité.

#### 1.3.2.3.4 Attaques sur la couche d'accès (liaison) :

a. **MAC Spoofing**

Sur un même réseau, chaque système possède une table de correspondance entre les adresses IP (couche réseau) et MAC (couche liaison) des systèmes voisins cette interface est assurée par le protocole ARP (Address Resolution Protocol), mais la faiblesse d'authentification de ce protocole permet à l'attaquant d'envoyer des requêtes ARP au système ciblé indiquant que l'adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne. C'est le même principe que l'IP Spoofing, mais elle vise la couche de liaison pour usurper l'adresse de contrôle d'accès au support (MAC).

b. **MAC Flooding**

C'est la saturation de la table d'apprentissage, elle consiste à injecter un grand nombre de paquets (ARP) au commutateur pour remplir tout l'espace de la mémoire dans le but d'inonder la table MAC du commutateur. Sachant que celle-ci associe les adresses MAC aux différents ports (Relation entre une adresse MAC et numéro de port), ce qui permet à l'attaquant d'avoir accès à toute sorte de données.

c. **Ecoutes Wi-Fi**

Cette attaque est dangereuse et facile à mettre en œuvre dans laquelle l'attaquant configure un faux réseau et une fois qu'un utilisateur se connecte, l'attaquant sera en mesure de surveiller toutes ses activités.

### 1.3.3 Mécanismes de défense et de sécurité

La sécurité informatique permet de préserver la confidentialité, l'intégrité et la disponibilité des données du réseau, pour cela de nombreux mécanismes ont été développés pour garantir la sécurité des réseaux.

Ces mécanismes fonctionnent sur les différentes couches du modèle TCP/IP selon le niveau de sécurité à fournir, certains d'eux permettant de prévenir les attaques, d'autres, moins efficaces, ne font qu'une détection ultérieure.

#### 1.3.3.1 VLAN (Virtual local area network)

Les VLAN introduisent la notion de segmentation qui permet de constituer des sous-réseaux totalement indépendants les uns des autres. Ils fonctionnent soit au niveau de la couche liaison, soit au niveau de la couche réseau du modèle TCP/IP.

Un Vlan est donc un regroupement logique des machines d'un même réseau physique.

#### 1.3.3.2 VPN (Virtual Private Network)

C'est un réseau privé consiste à créer un lien logique direct entre l'émetteur et le destinataire distant, pour acheminer les données de façon cryptées. De plus, il masque les adresses IP de l'émetteur et le récepteur pour les rendre illisibles par les personnes non autorisées.

Les VPN appartiennent à la couche liaison et la couche réseau du modèle TCP/IP selon les protocoles utilisés.

La mise en place d'un VPN permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison comme s'ils étaient sur le même réseau local.

#### 1.3.3.3 Le Pare-feu (firewall)

Les pare-feu (firewalls) sont des dispositifs physiques (matériel) ou logiques (logiciels) fonctionnent sur la couche application du modèle TCP/IP, conçus pour contrôler le trafic entre le réseau interne et le réseau externe. Quand un pare-feu reçoit un paquet, il commence par vérifier sa liste de règles de filtrages du début à la fin à la recherche d'une règle permettant d'accepter ou de rejeter le paquet. (17)

Le pare-feu propose un véritable contrôle sur le trafic réseau de l'entreprise, il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'autre part, un firewall évite la fuite non contrôlée d'informations vers l'extérieur.

#### 1.3.3.4 La DMZ (DeMilitarized Zone)

La Zone démilitarisée consiste à utiliser un pare-feu pour créer un périmètre délimité (sous réseau) isolé du réseau d'une entreprise, cette zone intermédiaire permet de définir des règles d'accès entre le réseau externe (internet) et le réseau local de l'entreprise.

Le principal avantage de cette configuration est le renforcement de niveau de sécurité du réseau local de l'entreprise de plus, c'est une solution filtrante permet le confinement de toutes les requêtes inconnues au niveau de la DMZ. Ce qui évite de les recevoir sur le réseau interne où sont stockées les ressources les plus précieuses.

La politique de sécurité mise en œuvre sur la DMZ est la suivante : (7)

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

#### 1.3.3.5 Le serveur mandataire « proxy »

Le proxy est une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et Internet, il peut être vu comme une porte sur l'extérieur pour permettre à un réseau local d'accéder de manière transparente aux sites d'Internet.

Lorsqu'un utilisateur se connecte à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy pour lui envoyer sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente souhaite joindre et lui transmettre la requête. Le serveur va ensuite envoyer une réponse au proxy, qui va à son tour la transmettre à l'application cliente. (7)

L'objective d'un proxy est la protection de l'anonymat de l'utilisateur en masquant son adresse IP, la limitation des accès à certains sites, filtré les connexions internet et enfin gardé en mémoire les pages les plus souvent visitées par les utilisateurs afin de pouvoir les leur fournir le plus rapidement possible, et cela grâce à la fonction cache qui est un espace de stockage temporaire.

#### 1.3.3.6 Le NAT (Network Address Translation)

Ce mécanisme est mis en place pour remplacer l'adresse IP privée source des machines qui font partie d'un intranet par une adresse IP publique pour pouvoir communique avec un équipement situé sur internet.

Les adresses privées sont donc invisibles de l'extérieur, cet avantage de masquage des adresses IP renforce la sécurité du réseau interne.

Il existe trois types de NAT :

- Le NAT statique : associe une adresse IP privée à une adresse IP publique routable sur internet, cette traduction se fait dans un sens et dans l'autre.
- Le NAT dynamique : partage une même adresse IP publique entre plusieurs machines, comme il est possible d'utiliser un nombre réduit d'adresses IP publiques ce qu'on appelle IP pool (pool d'adresse). Ce type de NAT permet de résoudre le problème de limitation d'adresses IP utilisées en extérieur puisqu'une seule adresse IP publique est partagée par plusieurs machines d'adresses IP privées différentes.
- Le PAT (Port Address Translation) : est un type de NAT basé sur l'utilisation des numéros de ports, ce type de translation consiste à utiliser la même adresse IP publique pour l'ensemble de machines en ajoutant le numéro de port.

1.3.3.7 Antivirus

C'est un logiciel permettant de détecter et de nettoyer une machine contre les malware (virus, ver, cheval de Troie, etc.), cet utile applique souvent des techniques de détection basées sur la reconnaissance de la signature d'un virus pour empêcher son exécution.

1.3.3.8 La cryptographie

C'est l'ensemble des techniques permettant de coder les données et les messages sur le réseau de façon de les rendre incompréhensibles pour les personnes non autorisées.

Le fait de coder un message de telle façon de le rendre secret s'appelle chiffrement et le résultat de cette opération est appelé cryptogramme (chiphertext) par opposition au message initial, appelé message en clair (plaintext). La méthode inverse, consistant à retrouver le message original, est appelée déchiffrement.

Deux techniques de cryptographie sont utilisées :

- Le chiffrement symétrique : consiste à utiliser la même clé secrète pour chiffrer et déchiffrer un message.
- Le chiffrement asymétrique : basé sur une paire de clés : une clé publique pour le chiffrement du message, et une clé privée pour le déchiffrement.

1.3.3.9 L'authentification

C'est une méthode de sécurisation des échanges dans laquelle l'identité d'utilisateur est vérifiée avant tout échange de données. Nous trouvons principalement :

**Authentification PAP :** (password Authentification Protocol) : c'est un protocole d'authentification par échange de mot de passe pour PPP (Point to Point Protocole), il consiste à envoyer le mot de passe en clair avant le transfert de données, si le mot de passe correspond l'accès est autorisé.

**Authentification CHAP :** (Challenge Handshake Authentification Protocol) ce protocole repose sur l'échange de messages cryptés selon une clé secrète, il améliore le PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau.

1.3.3.10 Le système IDS (Intrusion Detection System)

C'est un mécanisme qui alerte l'administrateur en cas de faille ou de menace de sécurité dans un réseau. Il consiste à surveiller et à écouter les trafics réseau en repérant celles qui sont anormales ou suspectes permettant ainsi de prévenir les risques d'intrusion. Il existe deux grandes familles distinctes d'IDS :

- Les N-IDS (Network Based Intrusion Detection System) : ils assurent la sécurité au niveau du réseau (la surveillance des paquets entrants et sortants d'un réseau).
- Les H-IDS (Host Based Intrusion Detection System) : ils assurent la sécurité au niveau des hôtes. Pour la détection de toute activité suspecte.

1.3.3.11 Les protocoles de sécurité

**Protocole SSH :** (Secure Socket Shell) : c'est un protocole de la couche application conçu dans le but de sécuriser les différents protocoles non chiffrés dédiés à l'accès en ligne pour s'assurer que toutes les communications vers et depuis le serveur distant se produisent de manière chiffrée et sécurisée.

**Protocole SSL :** (Transport Layer Security) il se situe entre les couches transport et application. Ce protocole repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission des données entre deux machines (un client et un serveur) après une étape d'authentification. De plus, il sécurise les transactions faites sur le Web par le protocole http, FTP et autres. (7)

**Protocole HTTPs :** (Hypertext Transfer Protocol Secure) c'est la combinaison du protocole http avec une couche de chiffrement comme SSL pour sécuriser les communications web.

**FTPS :** (FTP over SSL) permet de sécuriser les connexions FTP en utilisant des certificats SSL, tout en authentifiant l'utilisateur, à l'aide d'un username et d'un password.

**Protocole IPsec** : (Internet Protocol Security) c'est le protocole de sécurisation de la couche réseau du modèle TCP/IP, assure l'authentification et le chiffrement des paquets IP sur internet

## *Conclusion*

À travers ce chapitre, nous avons présenté les réseaux informatiques et leurs classifications par la suite nous avons vu le principe de la sécurité, ses objectifs, le but et les types d'attaques ainsi que les différentes méthodes et mécanismes appropriés à la sécurisation des réseaux.

Pour mieux comprendre l'importance de sécuriser un réseau informatique, nous allons détailler dans le prochain chapitre trois mécanismes de sécurités importants pour la mise en place d'un réseau et qui sont les liaisons virtuelles (VLAN et VPN) et les pare-feu.

# Chapitre II :

## Les pare-feu et les liaisons virtuelles

# *Introduction*

La sécurité est une fonctionnalité essentielle pour mettre en œuvre un réseau. Comme indiqué précédemment, plusieurs matériels et logiciels ont été mis à la disposition des utilisateurs pour garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle et cela nécessite parfois de combiner plusieurs types de sécurité à la fois pour atteindre le niveau de sécurité demandée sur un réseau.

Pour cela, nous allons détailler quelques solutions essentielles, nous commencerons par les liaisons virtuelles : VLAN (Virtuel Local Area Network) et les VPN (Virtuel Privat Network), qui forment un ensemble d'instruments très importants pour la gestion et le contrôle d'un réseau. Pour plus de sécurité, nous abordons une autre solution qui est les pare-feu pour comprendre leurs rôles, leurs différents types ainsi que leurs fonctionnements.

## 2.1 Virtuel Local Area Network

### **2.1.1** Définition

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est une technologie qui permet de réaliser des réseaux de façon indépendante du système de câblage et cela consiste à créer des segments logiques, dans lequel un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN.

Il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, etc.) en définissant une segmentation logique basée sur un regroupement de machines selon des critères (interfaces, adresses MAC, protocoles, adresses IP, etc.).

Le nombre de VLAN a configuré dépend de Switch utilisé, le switch Cisco prend en charge jusqu'à 1024 VLAN.

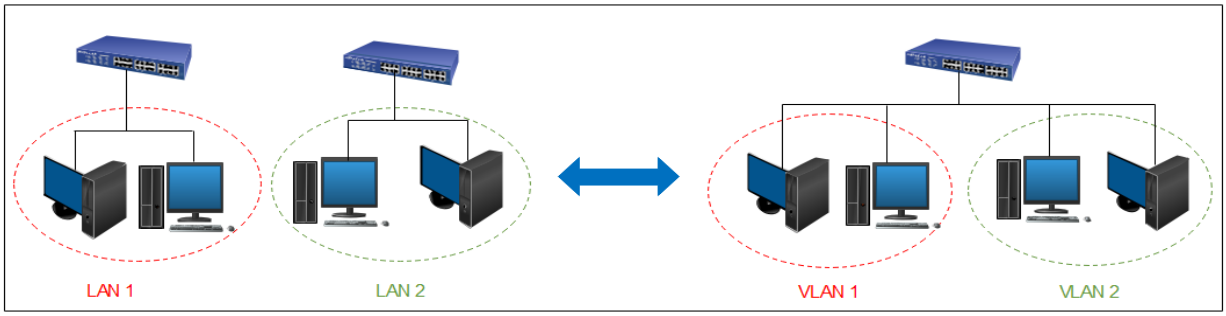



Figure 2.1-Virtual Local Area Network (VLAN).

### **2.1.2 Classification de VLAN**

Selon le principe de fonctionnement, les VLAN sont classés en 3 catégories chacun intervient à une couche particulière de modèle OSI.

2.1.2.1 VLAN niveau 1 (Port-Based VLAN) :

Le VLAN par port correspond à une configuration physique, l'apparence d'une machine à un VLAN est définie par le port de commutateur auquel elle est connectée pour cela, le commutateur est équipé d'une table « port/VLAN » remplie par l'administrateur qui précise le VLAN affecté à chaque port. Dans cette situation, toutes machines les reliées à un même port doivent appartenir au même VLAN.

Pour faire appartenir un même port à plusieurs VLAN, il est nécessaire d'utiliser un marquage de tram dans lequel les machines doivent être vlan aware et être capable de rajouter dans l'en-tête de la trame un marqueur « tag » identifiant le vlan auquel elles appartiennent. (18)

Le problème de ce mode est l'affectation statique des VLAN au port. En effet, si une machine doit changer de VLAN (déplacement logique) il faut réaffecter manuellement le port. De plus, si cette machine est physiquement déplacée et que l'on désire qu'il soit toujours dans le même VLAN, il faudra désaffecter son ancien port et réaffecter son nouveau port.

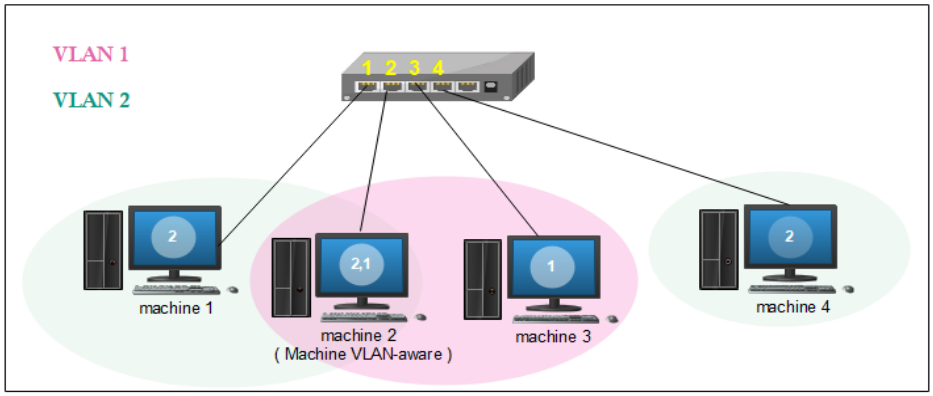



Figure 2.2-VLAN par port.

2.1.2.2 VLAN niveau 2 (MAC Address-Based VLAN) :

Sur ce niveau, L'association à un VLAN s'effectue en fonction de la table d'adresse MAC, l'administrateur saisit dans la table du commutateur le couple adresse MAC/VLAN et lorsque le commutateur découvre sur quel port est connectée la machine, il affecte dynamiquement le port au VLAN. Donc ce sont encore les ports des commutateurs qui sont affectés à des VLAN, mais d'une manière dynamique grâce à l'adresse MAC des machines.

Ce procédé est bien adapté aux équipements mobiles puisque la reconfiguration du port se fait sans intervention manuelle en cas de déplacement physique. Par contre si une machine change de VLAN, le commutateur doit réaffecter l'adresse MAC à un autre VLAN ce changement dans sa table adresse MAC/VLAN provoque une surcharge sur le réseau. De plus, dans ce type de VLAN, l'administrateur doit procéder à la saisie de toutes les adresses MAC, ce qui rend le VLAN de niveau 2 plus long et plus complexe surtout lorsque le nombre d'éléments devient important.

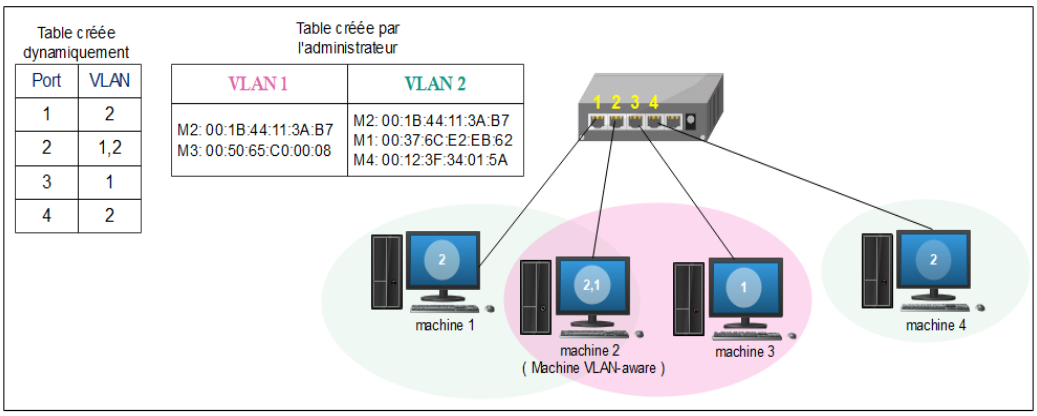



Figure 2.3-VLAN par adresse MAC.

2.1.2.3 VLAN niveau 3 (Network Address-Based VLAN)

Également appelé VLAN par sous-réseau, ce type de VLAN est associé à des sous-réseaux selon l'adresse IP des paquets. Les stations d'un VLAN de niveau 3 sont affectées dynamiquement à un VLAN, en décapsulant le paquet pour accéder à l'adresse IP. Une station peut appartenir à plusieurs VLAN par affectation statique et en cas de déplacement, la configuration de commutateur se modifie automatiquement.

La difficulté de ce type de VLAN provient de la façon d'accéder aux adresses, le commutateur est obligé de décapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel Vlan il appartient.

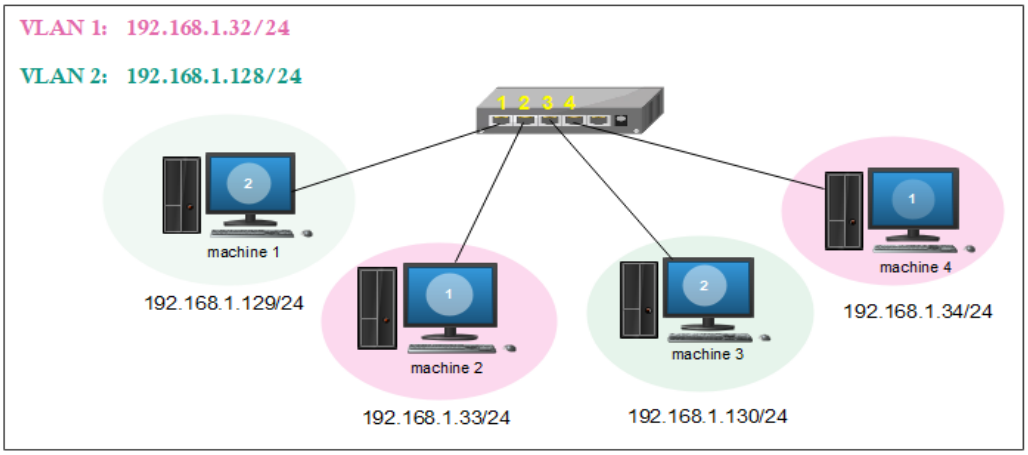



Figure 2.4-VLAN par adresse IP.

## 2.1.3 Types de VLAN

2.1.3.1 VLAN par défaut :

Le VLAN par défaut fait référence à celui auquel appartiennent tous les ports et les trames d'un périphérique lorsqu'il n'y a pas de configuration spécifique. Lors de la mise en œuvre des VLAN sur un périphérique, au moins un VLAN doit être défini, d'où la nécessité du VLAN par défaut, qui ne peut pas être renommé ou supprimé. Généralement, le VLAN par défaut est le VLAN 1.

2.1.3.2 VLAN natif :

Ce type de VLAN est configuré sur un port trunck. Lorsqu'un paquet reçu n'est pas étiqueté avec un identificateur de VLAN, il est automatiquement associé au VLAN natif, ce qui permet à un VLAN de prendre en charge des périphériques qui ne marquent pas leur trafic sur le réseau.

2.1.3.3 VLAN privé (PVLAN) :

C'est une technique de segmentation de réseau de la couche 2, permettant l'isolation des ports ou la segmentation du trafic sous le même segment IP. En appliquant le VLAN privé dans un environnement de réseau partagé, cela permet d'économiser des adresses IP et d'améliorer la sécurité des ports de commutation dans la couche 2.

- Types de PVLAN : dans un VLAN privé il existe trois types de VLAN

**VLAN primaire :** ce VLAN fait référence au VLAN d'origine, qui peut véhiculer les trames vers tous ses sous-VLAN (VLAN secondaires)

**VLAN isolé :** c'est le VLAN secondaire, le VLAN isolé ne peut prendre en charge que les ports de commutation (ports isolés) au sein du VLAN isolé qui transmettent des données aux ports promiscuous du VLAN primaire. Même dans un même VLAN isolé, les ports isolés ne peuvent pas communiquer entre eux.

**VLAN communautaire :** Le VLAN communautaire est également un type de VLAN secondaire. Les ports de commutation (ports communautaires) au sein d'un même VLAN communautaire peuvent communiquer entre eux ainsi qu'avec les ports du VLAN primaire. Mais un tel type de VLAN est également incapable de communiquer avec d'autres VLAN secondaires, y compris d'autres VLAN communautaires. (19)

- Types de port du PVLAN : Il existe trois types de port VLAN :

**Port promiscuous :** ce type de port est capable d'envoyer et de recevoir des trames de n'importe quel autre port du VLAN.

**Port isolé :** Existant dans un sous-VLAN, le port isolé se connecte à un hôte et ne peut communiquer qu'avec des ports promiscuous.

**Port communautaire :** Le port communautaire réside également dans un sous-VLAN et se connecte à un hôte. Cependant, il ne peut dialoguer qu'avec les ports promiscuous et les autres ports communautaires du même sous-réseau.

2.1.3.4 VLAN de donnée :

Également connu sous le nom de VLAN utilisateur, le VLAN de données est désigné uniquement pour l'acheminement des données générées par l'utilisateur. Ce qui permet de mieux contrôler le trafic et la sécurité des données.

2.1.3.5 VLAN de la voix :

Un Voice VLAN est un VLAN qui est spécifiquement alloué aux flux de données vocales de l'utilisateur. Il assure la qualité du trafic vocal en améliorant la priorité de transmission de celui-ci lorsqu'il est transmis avec d'autres trafics. Autrement dit, lorsque d'autres services (données, vidéo, etc.) sont transmis simultanément, le service vocal sera priorisé et transmit avec une priorité d'acheminement plus élevée. (20)

2.1.3.6 VLAN de gestion :

Un VLAN de gestion est configuré pour accéder aux fonctions de gestion d'un commutateur, la configuration de VLAN de gestion se fait tout simplement en lui attribuant une adresse IP et un masque de sous-réseau.

### 2.1.4 Protocole de VLAN

2.1.4.1 Protocole de transport

Le trunk ou liaison d'agrégation est un lien physique transportant les trames de plusieurs VLAN, nous définissons deux protocoles qui permettent de mettre en place un lien trafic :

a. **La norme IEEE 802. 1Q:** normalisée par l'IEEE, c'est une norme de réseau local qui définit une méthode de marquage des trames Ethernet. Elle ajoute pour cela un en-tête « tag » de quatre octets qui contient un identifiant de VLAN (VLAN ID) à la trame Ethernet ce qui permet aux commutateurs de regrouper les ports en fonction des VLAN.

L'en-tête rajouté à la trame Ethernet contient deux champs de 2 octets chacun TPID (Tag Protocol Identifier) et TCI-tag (Tag control information) comme indiqué ci-dessous :

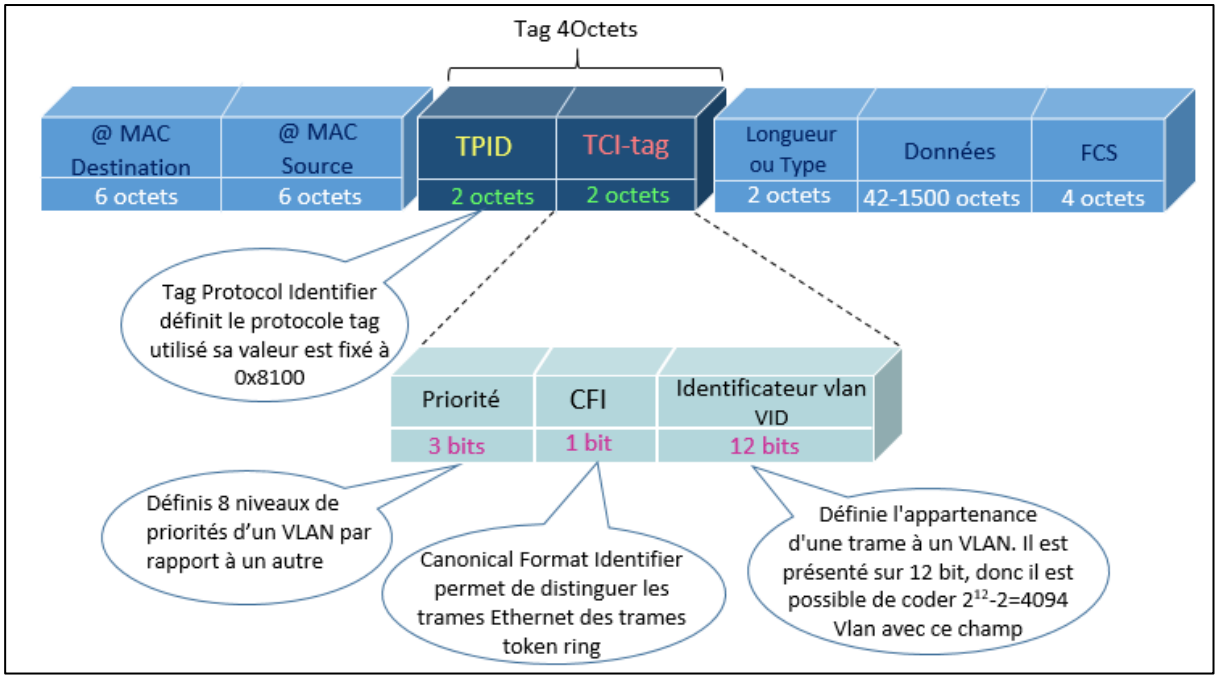



Figure 2.5-la norme IEEE 802.1Q.

b. **Protocole ISL:** (Inter Switch Link) c'est un protocole propriétaire Cisco utilisé pour l'interconnexion de plusieurs commutateurs et la maintenance des informations VLAN, son principe de fonctionnement consiste à encapsuler la totalité d'une trame Ethernet d'un VLAN dans une autre trame plus grande en ajoutant 30 octets, après sa transmission sur une connexion trunk, cette trame sera décapsulée pour que la trame d'origine soit envoyée au commutateur approprié grâce au VLAN ID.

Le protocole ISL encapsule chaque trame Ethernet entre un en-tête ISL de 26 octets et un en-queue ISL de 4 octets.

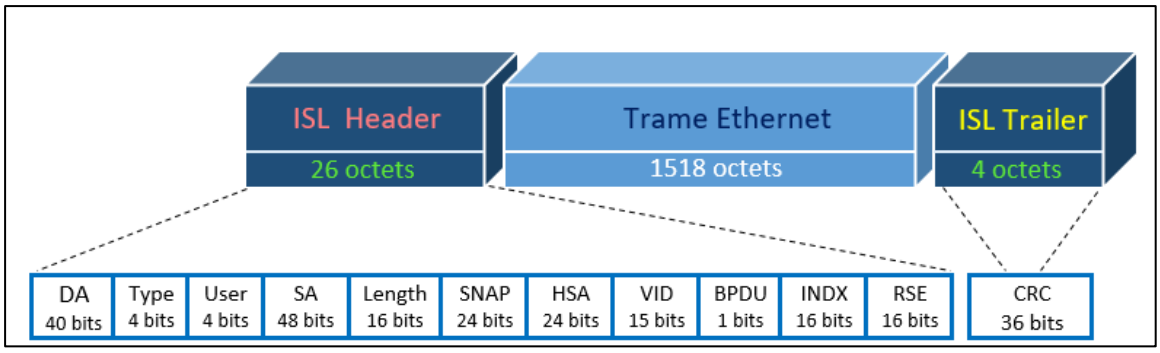



Figure 2.6-Le protocole ISL.

2.1.4.2 Protocole d'administration et de contrôle

a. **Protocole VTP :** (VLAN Trunking Protocol) c'est un protocole de niveau 2 propriétaire de Cisco, permet de propager automatiquement des VLAN configurés sur un commutateur en mode « serveur » vers les autres commutateurs configurés en mode « client » sur le même LAN réduisant ainsi le besoin de configuration manuelle des VLAN sur chaque commutateur individuel.

❖ Principe de fonctionnement :

le protocole VTP fonctionne en envoyant des messages VTP entre les commutateurs contiennent des informations sur les VLAN configurés sur le commutateur émetteur « serveur », notamment l'ID, le nom et autres attributs du VLAN, lorsqu'un VLAN est créé ou modifié, le commutateur configuré en mode serveur envoie un message VTP contient une valeur appelée RN (Révision Number) qui augmente à chaque fois qu' une modification est faite (initialement 0 puis 1 puis 2 puis 3, etc.) aux commutateurs clients qui vont comparer la nouvelle valeur RN reçu avec le RN qu'ils stockent en local, si ce dernier est plus petit, alors les commutateurs se synchronisent avec le commutateur serveur et récupèrent la nouvelle base de données des Vlan. (21)

Le protocole VTP est basé sur le protocole STP pour envoyer des messages VTP.

**Le protocole STP** :(Spanninge Tree Protocol) c'est un protocole de couche liaison de données, normalisé par IEEE 802.1D, Sa principale fonction est d'empêcher la production des boucles dans un réseau commuté redondant.
STP détecte et désactive ces boucles sur le réseau grâce aux informations contenues dans la trame de données appelée BPDU (Bridge Protocol Data Units) qui sont utilisés pour activer et désactiver les ports selon leurs adresses MAC.

❖ Mode du VTP :

Il existe trois modes VTP dans lesquels un commutateur peut être configuré :

1. VTP serveur : dans ce mode, le commutateur peut créer, modifier et supprimer des VLAN selon le besoin et les diffuser automatiquement a d'autres commutateurs du même domaine VTP.

2. VTP client : le commutateur en mode client reçoit les mises à jour, les prend en compte et les traite, mais ne permet pas à l'administrateur de faire des modifications sur les VLAN.
3. VTP transparent **:** le commutateur reçoit des annonces VTP, mais il ne les traite pas et ne met pas à jour sa propre base de données VLAN, en ce mode l'administrateur effectue tout sort de modification sur les VLAN en local uniquement, c'est-à-dire, il ne propage pas ses modifications vers tous les commutateurs du réseau.

b. **Protocole VMPS:** (Virtual Local Area Network Management Policy Server): c'est un protocole propriétaire Cisco utilisé pour attribuer dynamiquement l'appartenance au VLAN des machines connectées sur le réseau en fonction de leurs adresses MAC, c'est donc une identification de la machine connectée, adapté généralement pour les grands réseaux où la gestion manuelle du VLAN est complexe.

❖ Principe de fonctionnement :

Le protocole VMPS est basé sur l'architecture client-serveur. Le client est un commutateur de marque Cisco, tandis que le serveur est un serveur VMPS. Lorsqu'une machine se connecte au réseau, elle envoie son adresse MAC dans une trame IP au commutateur qui envoie une requête au serveur avec l'adresse MAC de la machine. Le serveur vérifie sa base de données pour déterminer dans quel VLAN placer cette machine. Une fois l'appartenance au VLAN déterminée, le serveur renvoie les informations du VLAN au commutateur qui attribue ensuite le VLAN à la machine.

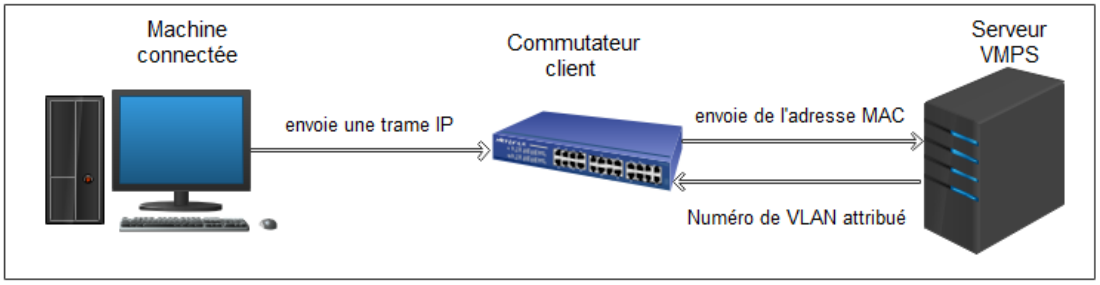



Figure 2.7-fonctionnement du protocole VMPS.

c. **Protocole DTP :** (Dynamic Trunking Protocol) c'est un protocole réseau propriétaire de Cisco Système, utilisé pour gérer dynamiquement le mode trunk d'un port sur le commutateur réseau, il fonctionne uniquement de point à point entre les périphériques réseau.

Pour ce faire, DTP utilise des différents modes qui peuvent être configurés sur les interfaces et qui sont :

- Mode access : il force la liaison à être non trunk quel que soit l'état de l'autre extrémité, c'est la désactivation du trunk en informant le commutateur voisin.
- Mode trunk : le commutateur est mis en mode trunk pour faire transiter les trames de plusieurs VLAN quel que soit l'état de l'autre extrémité.
- Mode dynamique automatique : par défaut, c'est le mode d'un port, il met l'interface prête à être un trunk si l'autre extrémité est en mode trunk ou dynamique souhaitable. Ce mode n'envoie pas de requêtes, mais répond aux requêtes d'en face.
- Mode dynamique desirable : c'est un mode actif dans lequel le lien essaie de négocier le mode trunking avec l'autre extrémité (annonce sa volonté de passer en trunk).
- Mode nonegotiate : le commutateur se met en mode trunk automatiquement sans informer le commutateur voisin.
- Off : désactivation du trunk.

Tableau 2.1-principe de fonctionnement de protocole DTP

| | Dynamic Auto | Dynamic Desirable | Trunk | Access |
|---|---|---|---|---|
| **Dynamic Auto** | Access | Trunk | Trunk | Access |
| **Dynamic Desirable** | Trunk | Trunk | Trunk | Access |
| **Trunk** | Trunk | Trunk | Trunk | |
| **Access** | Access | Access | | Access |

d. **Protocole GVRP :** (Generic VLAN Registration Protocol) développée par IEEE sur la norme 802.1Q , c'est un protocole de couche 2 permet de transférer des informations VLAN entre des périphériques réseau. Il fait le même travail que VTP, mais GVRP a été développé pour fonctionner sur différents appareils de marque.

Il existe également d'autres protocoles liés aux VLAN, tels que MVRP (Multiple VLAN Registration Protocole) et VACL (VLAN Control List), qui peuvent être utilisés pour la gestion et la configuration des VLAN.

### 2.1.5 Intérêts d'un routage inter vlan

Par défaut, les ordinateurs sur les différents VLAN sont incapables de communiquer entre eux, c'est l'intérêt de la mise en place des VLAN, mais parfois, ces ordinateurs ont besoin de communiquer pour une raison ou une autre, pour autoriser une communication entre VLAN, il est demandé de configurer le routage inter-VLAN.

❖ Principe de routage inter VLAN

Lorsqu'un hôte d'un VLAN souhaite communiquer avec un hôte d'un autre VLAN, un routage est nécessaire. Ce dernier est un processus de communication entre des réseaux LAN différents, soit par un routeur ou un commutateur de couche 3 qui est un commutateur capable d'assurer une fonction de routage en plus de ses fonctions habituelles, il existe donc deux méthodes pour faire communiquer deux VLAN :

- La méthode Switch Virtual Interface (SVI).
- La méthode Router On a Stick (ROAS) : ce type de configuration implique une connexion unique dans laquelle l'ensemble des VLAN sont regroupés d'une façon logique dans une même interface physique, il n'existe qu'une seule connexion physique avec le routeur.

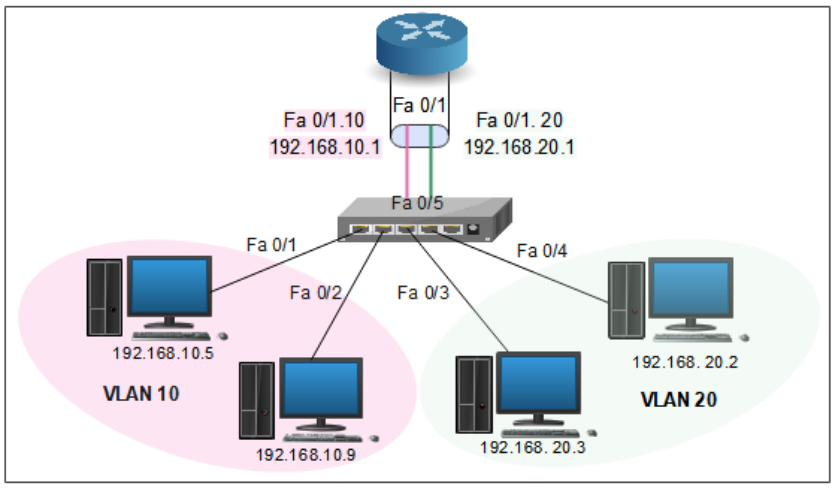



Figure 2.8-router-on-a-stick.

### 2.1.6 Avantages et inconvénients des VLAN

2.1.6.1 Les avantages :

La technologie de VLAN comporte de nombreux avantages permettant une meilleure organisation d'un réseau local. Ces avantages sont cités ci-dessous :

- ✓ La segmentation par VLAN réduit la taille des domaines de diffusion ainsi le nombre de collisions ce qui facilite le contrôle des trafics réseau.
- ✓ Augmentation de la sécurité : les Vlan permettent d'isoler des groupes d'utilisateurs en donnant l'accès à certaines ressources uniquement, ils peuvent donc être regroupés selon leurs centres d'intérêt.
- ✓ Plus de souplesse pour l'administration et la simplification de la gestion : l'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques.
- ✓ Régulation de la bande passante : il est important de pouvoir contrôler le gaspillage de capacité de trafic dans le réseau, le VLAN offre à l'administrateur les moyens de réguler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure.
- ✓ La réduction des coûts : l'utilisation des VLAN entraîne souvent la réduction du nombre de routeurs nécessaires.

2.1.6.2 Les inconvénients :

- × La mise en place d'un VLAN de niveau 1 (pare porte) peut-être complexe, en particulier pour les réseaux de grande taille.
- × Lorsqu'un VLAN de niveau 1 est configuré et une machine souhaite changer de VLAN, il faut réaffecter manuellement le port qui correspond.

## 2.2 Virtual Privat Network

Généralement les machines qui se trouvant à l'extérieur du réseau privé ne peuvent pas accéder à celui-ci. Ce n'est pas forcément vrai. La mise en place d'un réseau privé virtuel (VPN) permet de connecter tout un réseau ou des ordinateurs distants au réseau local privé.

### 2.2.1 Définition

Les VPN (Virtual privat Network) ou réseau virtuel privé est un outil informatique qui permet d'établir une communication sécurisée sur Internet afin de garantir la confidentialité des transmissions. Elle consiste à créer un tunnel sécurisé entre deux extrémités distantes par exemple un client distant et son réseau local ou encore entre deux réseaux, grâce au protocole de tunnellisation (tunneling) qui se chargera de crypter la communication de bout en bout.

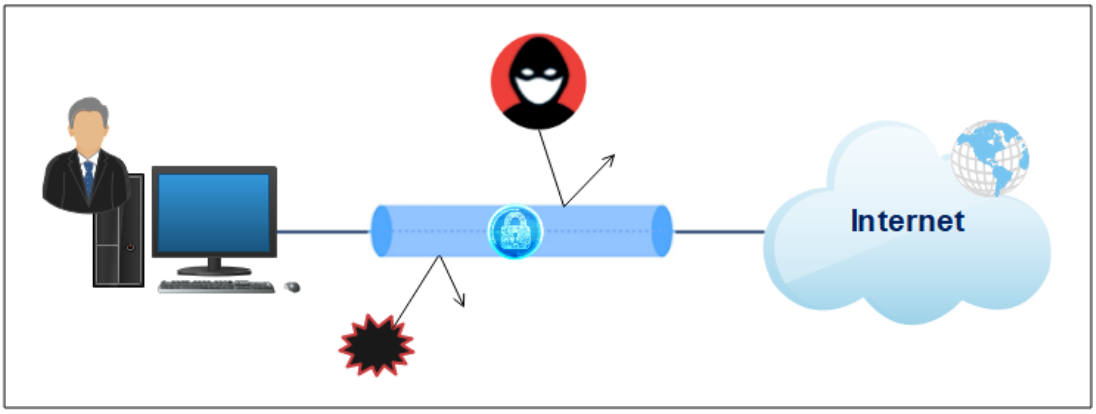



Figure 2.9-Virtual private Network (VPN).

### 2.2.2 Les composants d'un VPN

Le client VPN : initie une connexion vers un serveur VPN. Ce client peut-être :

- Une station telle qu'un client de l'extérieur qui souhaite créer un VPN avec le réseau de son entreprise.
- Un routeur : dans ce cas, toutes les stations du réseau local utiliseront le tunnel et donc la protection VPN sera effective sur tous les périphériques qui sont connectés au routeur.

Le serveur VPN : qui accepte, traite et répond aux demandes des clients VPN il fournit donc :

- Un VPN accès distant pour un poste isolé
- Un VPN routeur pour sécuriser et donner l'accès à un réseau local.

Le tunnel : c'est un lien de connexion entre le client et le serveur VPN dans lequel les paquets de données sont encapsulés.

Le client et le serveur VPN sont tous les deux capables de chiffrer et déchiffrer les données de part et d'autre du tunnel, on désigne deux modes de Tunnels :

- Tunnel obligatoire : Node To Node, est crié au niveau de deux extrémités de tunnel par exemple entre deux LAN d'une entreprise (routeur à routeur).
- Tunnel volontaire : End To End, est crié entre le client et le serveur VPN.

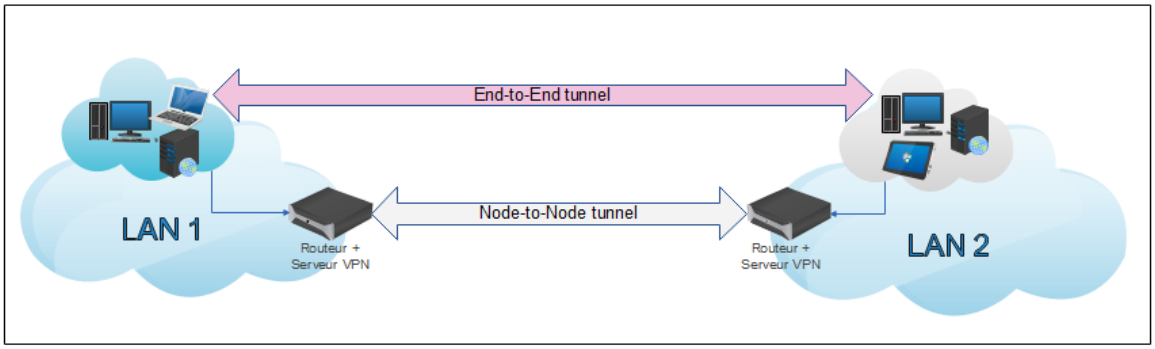



Figure 2.10-les modes de tunnel VPN.

### 2.2.3 Principe de fonctionnement

Le fonctionnement d'un VPN est basé sur l'utilisation d'un tunnel crypté qui permet de transférer des données de manière sécurisée entre le client et le serveur VPN. Pour ce faire, Le client installe un logiciel VPN sur son ordinateur ou appareil mobile et configure l'accès au serveur VPN, une fois la connexion à ce serveur VPN est établie, les données seront traitées comme suit :

- Pour que le client puisse accéder à un site web, le logiciel VPN installé sur son ordinateur chiffre le trafic de données et l'envoie (via son fournisseur d'accès à internet) au serveur VPN distant. Dans cette étape le protocole de tunneling encapsule les données en rajoutant un en-tête permettant le routage des trames dans le tunnel.
- Le serveur VPN déchiffre les données chiffrées provenant de l'ordinateur du client.
- Le serveur VPN envoie ces données sur internet et reçoit une réponse.
- Le trafic de données est à nouveau chiffré par le serveur VPN et renvoyé au client.
- Le logiciel VPN sur l'ordinateur de client déchiffre les données pour pouvoir les utiliser.

### 2.2.4 Les types de VPN

Selon les besoins, on désigne 3 type de VPN :

#### 2.2.4.1 Le VPN post à site (Host to LAN)

C'est un VPN d'accès utilisé pour permettre à des utilisateurs de se connecter à un réseau distant, et généralement pour accéder au réseau interne de l'entreprise en se basant sur deux composants :

- Serveur d'accès au réseau (NAS) : c'est un serveur dédié ou un logiciel installé sur un serveur, il est connecté au réseau interne de l'entreprise pour établir une connexion cryptée.
- Client VPN : c'est un logiciel installé sur l'ordinateur d'un utilisateur.

Ce procédé est adapté par de nombreuses entreprises afin de permettre à leurs utilisateurs distants de se connecter au réseau local de l'entreprise hors de leur lieu de travail.

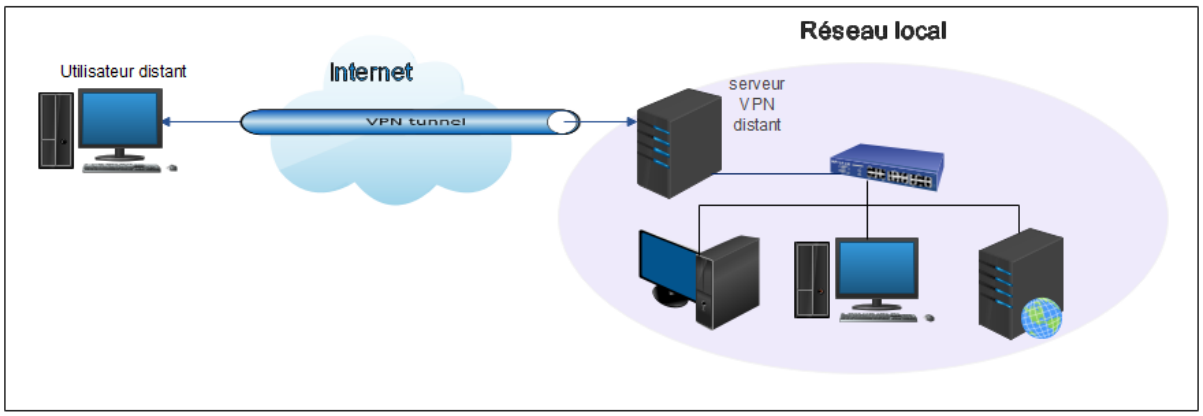



Figure 2.11-VPN post à site.

2.2.4.2 Le VPN intranet (LAN to LAN)

Ce type de VPN consiste à créer un réseau virtuel entre deux ou plusieurs sites distants d'une même entreprise ou encorde entre le site d'une entreprise et celui d'un fournisseur. De cette façon, les utilisateurs de chaque bureau peuvent accéder au réseau virtuel partagé sans besoin de client VPN.

Généralement, ce type de VPN est mis en place par l'interconnexion de deux éléments matériels (routeurs ou pare-feu) situés à la frontière entre le réseau interne et le réseau public de chaque site.

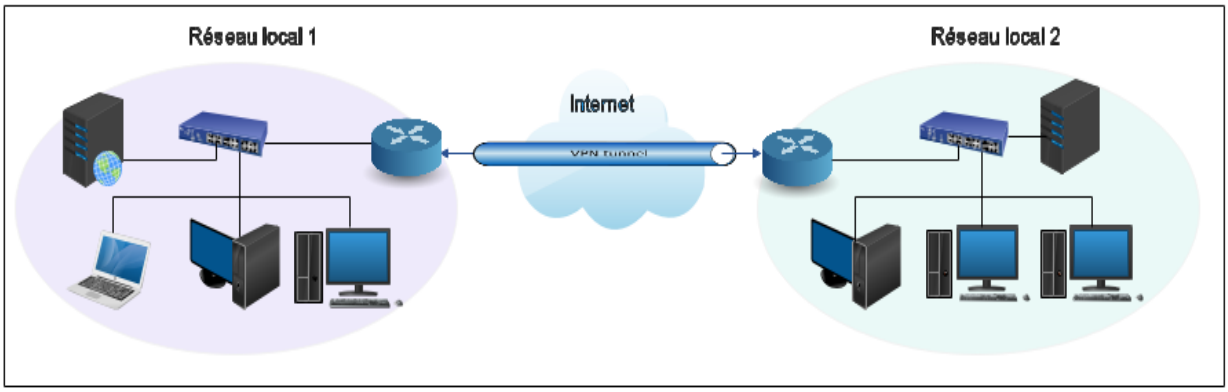



Figure 2.12-VPN site à site.

2.2.4.3 Le VPN extranet (Host to Host)

L'extranet VPN ou encorde VPN post à post est utilisé pour établir un canal sécurisé entre deux postes clients, proche ou distant par exemple, un client et son partenaire sur deux sites différents, ce qui permet au client distant de communiquer avec le poste concerné uniquement et non avec tous les postes du réseau virtuel.

Les deux postes peuvent être situés sur le même réseau ou sur deux réseaux différents reliés eux-mêmes par un VPN site à site. (22)

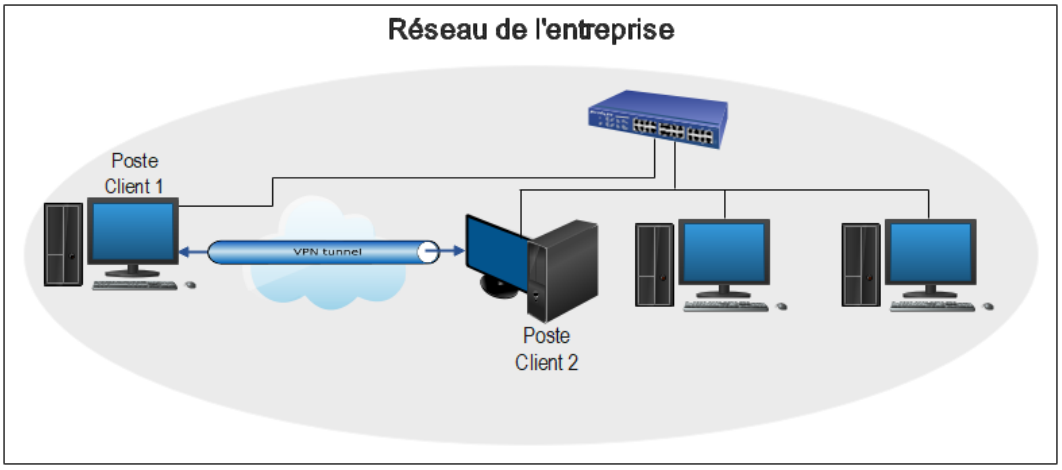



Figure 2.13-VPN post à post.

## 2.2.5 Les principaux protocoles de VPN

Les protocoles de tunnellisation sont basés sur les principes de cryptage et d'authentification ce qui permet de mettre en place des solutions de sécurité pour différentes architectures de réseau, ses protocoles intervenant à différents niveaux du modèle TCP/IP, pour cela, on désigne :

2.2.5.1 **VPN de niveau 2 :**

Repose sur les protocoles de la couche liaison :

a. **Le protocole PPTP :** Le point to point tunneling Protocol est conçu par Microsoft, il est basé sur le mode point à point pour permettre la transmission des connexions point to point protocol (ppp) en créant un tunnel crypté entre le client distant et le serveur privé.
Le protocole PPTP chiffre les données avec MPPE (Microsoft Point-to Point Encryption) et en utilisant un cryptage de 128 bits ce qui le rend faible en terme de sécurité.

❖ Le principe du protocole PPTP :

Les données du réseau local ainsi que les adresses des machines présentes dans l'en-tête du message sont encapsulées dans une trame PPP, qui est elle-même encapsulée dans un datagramme IP.
Une trame PPTP est constituée de :

- Paquet IP qui contient les données et les adresses IP de la machine.
- Entête PPP nécessaire pour toute connexion point à point.
- En-tête GRE (Generic Routing Encapsulation) qui gère l'encapsulation.
- En-tête IP contient les adresses IP sources et de destination qui correspond au client et au serveur VPN. (18)

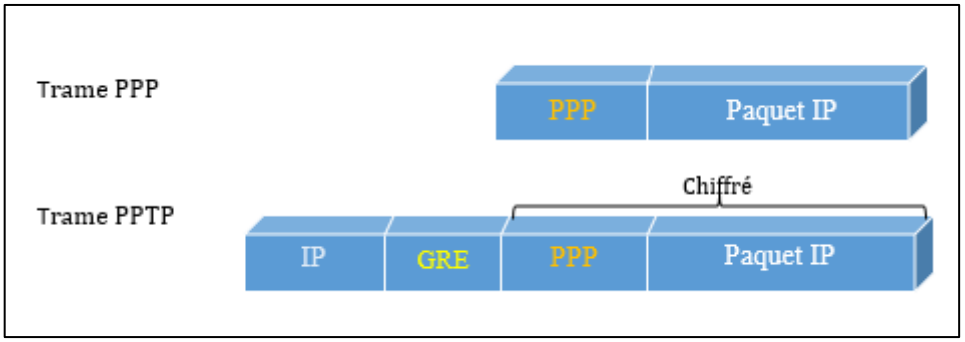



Figure 2.14-La trame de protocole PPTP.

b. **Le protocole L2F :** (layer 2 forwarding) ce protocole VPN a été développé par Cisco, son fonctionnement est basé sur le même principe que le protocole PPTP.

c. **Le protocole L2TP :** (layer 2 forwarding tunneling protocol) ce protocole a été proposé pour la première fois en 1999 comme amélioration des protocoles L2F et PPTP, il est similaire au PPTP, du fait de leur manque de chiffrement, et de leur fonctionnement avec un protocole PPP. Contrairement à PPTP, L2TP consiste à protéger la confidentialité et l'intégrité des données, il est généralement associé avec IPsec, de plus il chiffre les données en utilisant un cryptage de 256 bits ce qui le rend plus sécurisé que PPTP. (8)

2.2.5.2 **VPN de niveau 3**

Basé sur les protocoles de la couche réseau :

a. **Le protocole IPsec :** (internet Protocol Security) défini par l'IETF (Internet Engineering Task Force) afin d'offrir des services de chiffrement et d'authentification des données sur les réseaux IP.

Ce protocole offre une solution de sécurité complète pour les communications internet.
Les deux fonctionnalités principales assurées par IPsec pour la protection des données sont :

- L'authentification : assuré par l'en-tête d'authentification AH (Authentification Header) qui englobe tous les paramètres relatifs aux algorithmes d'authentifications ainsi que leurs clés associées.

La structure d'un paquet IPsec du type AH est donnée par :

- L'en-tête AH.
- Paquet IP constitué de données à transmettre et de l'en-tête IP.
- Nouveau en-tête IP composé des champs suivent : source, destination, protocole, version…

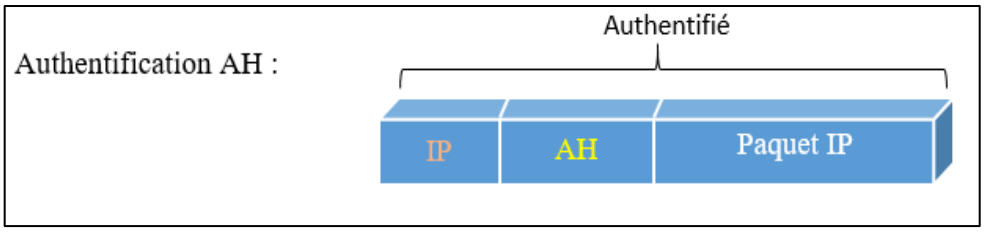



Figure 2.15-structure du paquet IPsec de type AH.

- Le chiffrement : assuré par l'entête d'encapsulation des informations de sécurité ESP (Encapsulated securityPayload) afin d'assurer la confidentialité des données, tout en garantissant leurs authentifications, ainsi La structure d'un paquet IPsec du type ESP est donnée par :

- L'en-tête (header).
- Les données chiffrées.
- Une queue.
- Des données supplémentaires d'authentification optionnelles.

Le chiffrement ne porte que sur les données encapsulées et le trailer par contre l'authentification porte sur l'en-tête ESP et tout ce qui suit, mais pas sur l'en-tête IP. (18)

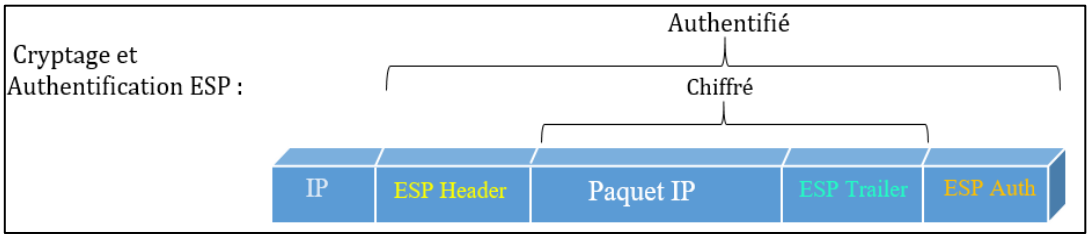



Figure 2.16-structure du paquet IPsec de type ESP.

De plus l'IPsec utilise le protocole IKE (Internet Key Exchange) pour la gestion et l'établissement d'une connexion sécurisée.
L'IPsec peut fonctionner selon 2 modes :

- Mode transport : il est utilisé pour sécuriser les données entre deux hôtes, sur ce mode, uniquement les données transférées qui sont chiffrées et authentifiées, le reste du paquet IP est inchangé.
- Mode tunnel : ce mode est utilisé pour sécuriser les données échangées entre deux réseaux, c'est la totalité du paquet IP qui est chiffré et authentifié pour qu'il soit encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP.

b. **Le protocole MPLS :** (Multi-Protocol Label Switching) c'est un protocole de commutation de paquets basé sur l'ajoute d'une étiquette (label) à chaque paquet, ce qui permet aux routeurs de transférer des paquets en fonction de l'étiquette au lieu de l'adresse IP. Cette approche de routage est beaucoup plus rapide et plus efficace que les méthodes de routage basées sur la table de routage.

#### 2.2.5.3 **VPN de niveau 4 :**

a. **Le protocole SSL/TLS :** (Secure Sockets Layer/Transport Layer Security) ce protocole est principalement utilisé par des fournisseurs de services tels que les sites de vente en ligne pour offrir une session sécurisée entre le client (le navigateur Web) et le serveur (le site Web). Il est généralement intégré par défaut dans tous les navigateurs Web en maintenant à jour ses différentes versions sans l'intervention de l'utilisateur. (23)

b. **Open VPN :** développé en 2001, c'est le protocole VPN le plus populaire et très conseillé, car il est open source, gratuit et il offre une meilleure sécurité.

Open VPN utilise la bibliothèque Open SSL, ce qui signifie qu'il supporte de nombreux types d'algorithmes de chiffrement, de plus il fournit un cryptage allant jusqu'à 256.

### 2.2.6 Avantages et inconvénients des VPN

#### 2.2.6.1 Avantage

Les principaux avantages d'un VPN sont :

- ✓ Les VPN offrent aux utilisateurs un accès à distance au réseau local de l'entreprise et de façon sécurisée.
- ✓ La confidentialité : le VPN cache l'adresse IP et l'emplacement de ses utilisateurs (garantit l'anonymat).
- ✓ Les VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites d'accéder à distance à un serveur ou la base de données de l'entreprise.
- ✓ Les connexions VPN permettent de partager des fichiers et des informations de manière sécurisées entre une machine locale et une machine distante.
- ✓ Simple a installé et a utilisé.
- ✓ L'usage d'un VPN renforce également la sécurité et la confidentialité des données

2.2.6.2 Inconvénient

Parmi les inconvénients du VPN :

- × Ralentissement de la connexion à cause du temps supplémentaire nécessaire pour chiffrer et déchiffrer les données
- × Service payant : la majorité des VPN sont payants et les VPN gratuits n'offrent pas les mêmes fonctionnalités et les mêmes niveaux de sécurité que les VPN payants.
- × Certains VPN ne sont pas compatibles avec tous les appareils ou systèmes d'exploitation.

## 2.3 Les pare-feu

Quels que soient les mécanismes de sécurité apporter à un ordinateur pour protéger ces données, cela reste insuffisant pour établir une communication sécurisée avec d'autres ordinateurs que ce soit à partir d'un réseau local ou d'un réseau externe, ce qui demande l'augmentation du niveau de sécurité en utilisant les systèmes « pare-feu ».

### 2.3.1 Définition

Le pare-feu ou coupe-feu, firewall en anglais est un dispositif séparateur conçu pour protéger un ordinateur ou un réseau des intrusions extérieures, il peut être un ordinateur, un routeur ou encore une combinaison d'éléments matériels et logiciels.

Un pare-feu est basé sur le filtrage des paquets pour garantir la sécurité et le contrôle des flux de données qui le traversent, il permet d'examiner, bloquer ou autoriser les échanges de données entre réseaux selon un ensemble de règles de sécurité prédéfinies.

le pare-feu comporte donc au minimum deux interfaces réseau une interface pour le réseau interne et l'autre pour le réseau externe.

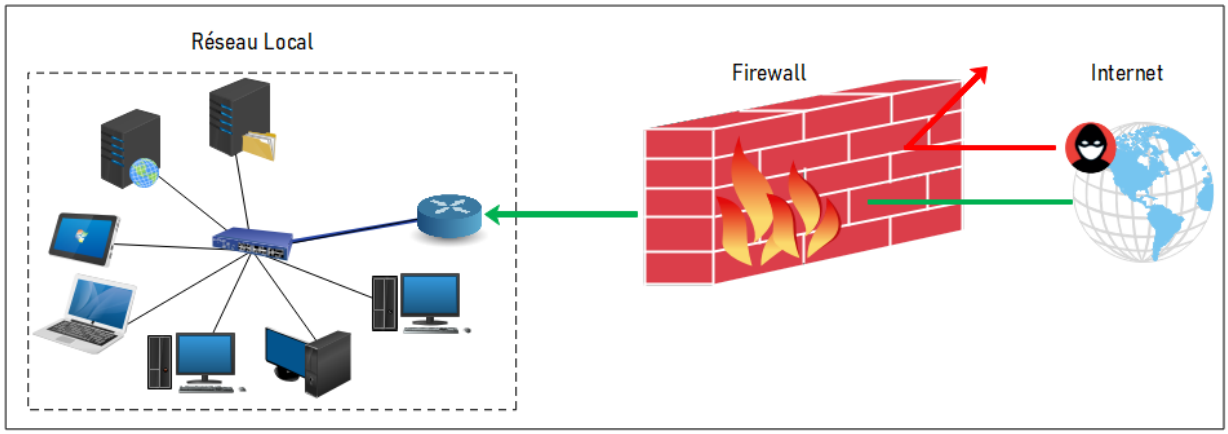



Figure 2.17-Pare-feu (Firewall).

Un pare-feu est installé le plus souvent en périphérie du réseau local de l'entreprise ce qui lui permet de contrôler l'accès aux ressources externes depuis l'intérieur, mais également entre les entités éloignées de l'entreprise. Ces dispositifs filtrent les trames des différentes couches du modèle OSI afin d'empêcher l'accès non autorisé à l'ensemble des machines du réseau de l'entreprise.

### 2.3.2 Principe de fonctionnement

Le système pare-feu interconnecte deux réseaux ou plus de niveaux de sécurité différents, par exemple entre le réseau interne de l'entreprise qui est une zone réseau de confiance forte et internet qui est une zone de confiance faible.

Pour sécuriser la communication, le firewall contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow)
- De bloquer la connexion (deny)
- De rejeter la demande de connexion sans avertir l'émetteur (drop)

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépend de la politique de sécurité adoptée par l'entreprise. On distingue habituellement deux types de politiques de sécurité permettant :

- Interdire tout par défaut : ce qui implique que tout ce qui n'est pas explicitement permis est interdit. Pour la mise en œuvre de tel politique, l'administrateur doit :
  - Analyser les services utilisés par les utilisateurs.
  - Définir les droits autorisés (la définition de la politique de sécurité).
  - Attribuer les droits autorisés dans un outil appliquant la politique et la suppression de tous les autres droits.

  Cette solution est la plus sécuritaire et la plus confortable pour l'administrateur de la sécurité, mais elle limite considérablement les droits des usagers.

- Autorisé tout par défaut : cette politique permet tout sauf ce qui est considéré comme dangereux, c'est-à-dire, tout ce qui n'est pas explicitement interdit est autorisé. Pour sa mise en œuvre il suffit donc d'analyse les différents risques des applications qui doivent s'exécuter pour déduire les interdictions à appliquer et autoriser tout le reste.

  Cette solution est inconfortable pour l'administrateur de la sécurité, car elle est moins sécurisée, mais c'est une solution qui facilite l'accès des usagers au réseau. (24)

### 2.3.3 Le filtrage pour les pare-feu

Selon l'approche fonctionnelle, les pare-feu sont basés sur le principe de filtrage, et cela peut se faire de différentes manières.

On distingue deux grands types de firewall :

- Les firewalls fonctionnant au niveau de la couche réseau : par le filtrage des paquets IP, c'est-à-dire sur l'analyse des en-têtes des paquets IP échangés entre deux machines.
- Les firewalls fonctionnant au niveau applicatif ou proxy : ce sont les filtres mandatés ou d'application. (25)

#### 2.3.3.1 Filtrage simple de paquet

a. **Principe**

Stateless packet inspection Firewall en anglais, ces types de firewalls sont les plus anciens, mais surtout les plus basiques, ils interviennent sur les couches réseau et transport de modèle OSI.

Ces firewalls sont introduits sur les routeurs pour réaliser le contrôle de l'en-tête de chaque paquet indépendamment des autres en se basant sur une liste de règles de filtrages prédéfinies par l'administrateur appelées (Access Control List). (26)

Les règles de filtrages s'appliquent alors par rapport à :

- L'adresse IP source/destination.
- Le protocole utilisé : IP pour la couche réseau ou TCP/UDP pour la couche transport.
- Le numéro de port source/destination.

b. **Les limites**

Pour la création d'un firewall, il est demandé d'ajouter les règles permettant de choisir les flux que l'administrateur souhaite laisser passer, pour cela, il suffit d'autoriser l'ouverture des ports des serveurs pour qu'ils soient accessibles depuis l'extérieur ce qui demande d'ouvrir tous les ports supérieurs à 1024 et cela pose des problèmes de sécurité.

De plus, ce type de filtrage ne résiste pas à certaines attaques du type IP-Spoofing ou SYN flood, car les règles de ses firewalls sont basées seulement sur les adresses IP. (26)

#### 2.3.3.2 Filtrage de paquet avec état

a. **Principe**

En anglais, Stateful packet inspection firewall et également appelé filtrage de connexion, c'est une évolution de firewall Stateless la différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés.

Contrairement au filtrage simple qui examine chaque paquet individuellement, le filtrage avec état ajoute la capacité de conserver les informations des requêtes et des connexions dans des tables d'états internes, c'est-à-dire, il prend en compte les trafics précédents pour garder en mémoire les différents attribues de chaque connexion. Ce qui permet de traiter les paquets non seulement suivent les règles de filtrage, mais aussi selon l'état de la session qui sont :

- New : Un client envoie sa première requête.
- Established : Connexion déjà initiée. Elle suit une connexion NEW.
- Related : Peut-être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- Invalid : correspond à un paquet qui n'est pas valide. (27)

b. **Les limites**

Le pare-feu à état est limité à garder un suivi de l'état de connexion, c'est-à-dire, une fois que l'accès à un service a été autorisé il n'y a aucun contrôle effectué sur les requêtes et les réponses des clients et serveurs.

Pour une protection complète contre les menaces, il est important de compléter ces pare-feu avec d'autres solutions de sécurité, telles que les systèmes de détection d'intrusion et les antivirus.

#### 2.3.3.3 Filtrage applicatif

a. **Principe**

Le filtrage applicatif opère au niveau 7 (couche application) de modèle OSI. Contrairement au pare-feu à filtrage de paquet, le pare-feu applicatif suppose une connaissance des protocoles utilisés par chaque application, il peut donc filtrer les trafics non seulement en fonction des en-têtes IP, mais aussi en fonction des protocoles adaptés.

Dans ce type de filtrage, les requêtes sont traitées par des processus dédiés, par exemple, une requête du type FTP sera filtrée par un processus FTP, le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole utilisé.

Le filtrage d'application est réalisé grâce au programme mandataire « proxy » qui sert à relais entre deux réseaux pour contrôler l'accès à chaque application. Le principe de ce pare-feu est identique à celui d'un proxy, c'est-à-dire, quand un utilisateur veut se connecter à un serveur externe, il se connecte d'abord au programme mandataire, qui lui va relayer le flux vers le serveur demandé. (8)

b. **Les limites**

La principale limitation de ce type de filtrage réside sur le fait qu'ils doivent connaître toutes les règles des protocoles à filtrer c'est-à-dire, qu'ils doivent être en mesure de traiter une vaste gamme de protocoles et connaître aussi leurs failles, ce qui rend difficile de réaliser un filtrage qui ne laisse rien passer, vu le nombre important de protocoles de niveau 7.

### 2.3.4 Type de pare-feu

Il existe différents types de pare-feu en fonction de la nature de l'analyse et de traitement effectués :

#### 2.3.4.1 Les firewalls matériels

Ce sont des dispositifs physiques utilisés pour protéger le réseau, positionnés entre le réseau interne et le réseau externe et, ils sont généralement intégrés dans d'autres équipements, le plus souvent dans des routeurs.

Les pare-feu matériels sont souvent adaptés par les grandes organisations, car ils offrent une sécurité robuste, par exemple : les pare-feu ASA de Cisco, Fortigate ou les pare-feu SRX de JUNIPER.

**Avantages**

- ✓ La mise à jour et la mise à niveau de protection simultanée pour tous les équipements du réseau
- ✓ Contrôle réseau à dispositif unique : un seul firewall installé permet de protéger tous les ordinateurs du réseau réduisant ainsi l'espace et le temps d'installation.

- ✓ Offre un bon niveau de sécurité : ces pare-feu sont plus fiables, car ils sont conçus pour gérer uniquement les tâches liées à la sécurité.

**Inconvénients**

- × Coût élevé : nécessite l'achat d'un matériel spécifique pour les mettre en place.
- × Plus difficile à configurer par rapport au pare-feu logiciel.
- × Risque de défaillance matériel.

2.3.4.2 Les firewalls logiciels

Ce sont des programmes informatiques installés au niveau des hôtes, tels que les pare-feu de Linux et Windows. Ils ont pour but de sécuriser un ordinateur particulier ou un serveur et non un groupe d'ordinateurs à la fois, un pare-feu personnel par exemple.

**Avantages**

- ✓ Économique pour un petit bureau avec des systèmes limités, car il ne nécessite pas un matériel supplémentaire.
- ✓ Facile à configurer et à gérer et offre une meilleure flexibilité.
- ✓ La personnalisation : le pare-feu logiciel peut être configuré selon les besoins spécifiques de l'utilisateur.

**Inconvénients**

- × Consomme plus de ressources, mémoire et l'espace disque, ce qui peut affecter et ralentir les performances du système.
- × Nécessite une administration et une mise à jour régulière.

2.3.4.3 Les firewall bridge

Ces firewalls se trouvent typiquement sur les Switchs, ils agissent comme des câbles réseau avec la fonction de filtrage en plus, leurs interfaces ne possèdent pas d'adresse IP et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable. Ce qui implique que les pare-feu bridge fonctionnent en mode transparent. (28)

**Avantages**

- ✓ Impossible de les éviter : tous les paquets passeront par ses passerelles.
- ✓ Peu coûteux.
- ✓ Simplifie la gestion de la sécurité du réseau.

**Inconvénients**

- × Ces fonctionnalités sont très basiques (filtrage en Stateless).
- × Complexité de configuration pour les réseaux hétérogènes.
- × Le pare-feu ne peut pas fournir une sécurité complète, car il n'identifie pas les adresses IP et les ports des paquets, de plus il ne contrôle pas l'accès au réseau.

### 2.3.5 Les pare-feu et la zone démilitarisée

La mise en place d'un pare-feu permet de créer un sous-réseau séparé et isolé du réseau local et Internet, ce sous-réseau est appelé la DMZ pour DeMilitarized Zone ou zone démilitarisée en français qui est moins sécurisée que le réseau local.

La DMZ contient les machines étant susceptibles d'être accédées depuis Internet par exemple un serveur SMTP le pare-feu bloque alors les accès au réseau local pour garantir sa sécurité et en cas de compromission d'un des services dans la DMZ le pirate n'aura accès qu'aux machines du DMZ et non au réseau local puisqu'il n'y a pas de trafic direct entre le réseau interne et l'extérieur.

En termes d'architecture, il existe deux façons de concevoir un réseau avec des DMZ :

- La première méthode est d'utiliser un seul firewall avec 3 l'interface réseau à créer :
  - La première interface entre le FAI (Fournisseur d'Accès Internet) et le firewall ce qui représente le réseau externe.
  - Le réseau interne est formé à partir de la deuxième interface réseau avec le firewall.
  - La troisième interface est entre la DMZ et le firewall.

  Cette architecture permet de contrôler le trafic entre Internet et la DMZ et entre le LAN et la DMZ le principal inconvénient de cette architecture et que si cet unique firewall est compromis, cette architecture tombe.

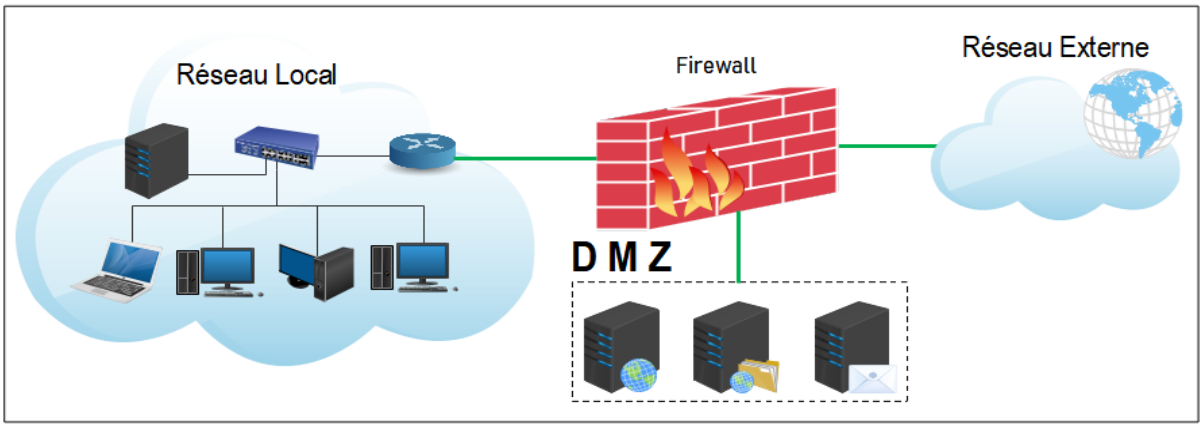



Figure 2.18-Architecture de DMZ avec un seul pare-feu.

- La deuxième méthode présente une architecture plus sécurisée consiste à utiliser deux firewalls pour créer une DMZ le premier firewall interne autorise le trafic entre la DMZ et les machines de réseau interne uniquement, tant dite que le secondaire filtre le trafic entre le monde extérieur et la DMZ.

  Cette architecture à deux firewalls est plus sécurisée puisqu'un pirate devra compromettre les deux pare-feu, ainsi que la DMZ pour accéder au réseau externe.

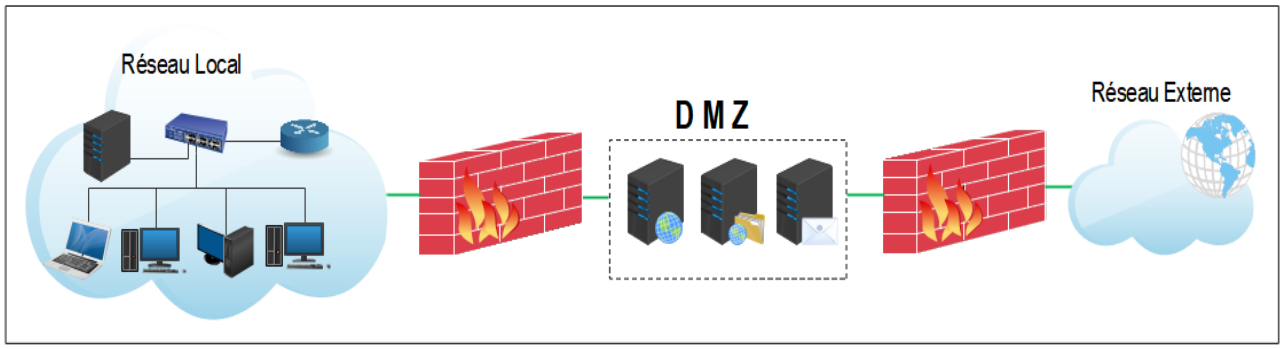



Figure 2.19-Architecture de DMZ avec deux pare-feu.

### 2.3.6 Intérêts et limites des pare-feu

2.3.6.1 Avantages

- ✓ Contrôle de l'accès au réseau : le pare-feu permet de définir des règles pour autoriser ou bloquer l'accès au réseau.
- ✓ Protection contre les attaques externes : le pare-feu permet de filtrer les connexions entrantes et sortantes pour prévenir les attaques.
- ✓ La surveillance du trafic réseau en temps réel ce qui permet d'identifier les activités suspectes ou non autorisées.
- ✓ Protégé la confidentialité des données et masque les adresses des machines clientes.

2.3.6.2 Limites des pare-feu

- × Les pare-feu, parfois ne bloquent pas tout le trafic, car ils ne protègent pas contre les attaques qui ne les traversent pas.
- × Les pare-feu sont généralement configurés pour gérer les connexions entrantes et sortantes depuis et vers le réseau externe (Internet), mais ils ne peuvent pas empêcher les attaques internes provoquées par un utilisateur par exemple.
- × Ils ne protègent pas contre les fichiers infectés par les virus, d'où l'utilité d'installer un antivirus sur les machines.
- × Ils peuvent bloquer des tentatives de propagation de virus et d'accès par différents programmes malveillants, mais ne peuvent jamais les supprimer.

## *Conclusion*

Tout au long de ce chapitre, nous avons détaillé l'aspect théorique de notre projet, nous avons présenté les méthodes de sécurité par les pare-feu et les liaisons virtuelles VLAN et VPN qui forment une stratégie de sécurité adoptée par divers entrepris. Cette étude facilite la partie réalisation que nous allons effectuer dans les prochains chapitres.

# Chapitre III :

## Présentation de l'organisme d'accueil et du contexte du projet

# *Introduction*

Au cours de ce chapitre, nous allons présenter l'entreprise d'accueil qui est la BMT (Béjaia Mediterranean terminal) au sein duquel nous avons effectué notre stage, nous allons voir sa structure, ses différentes directions ainsi que ses objectifs, par la suite, nous allons nous intéresser au Centre digitalisation et Numérique pour étudier le réseau de la BMT et on termine par la problématique suivie de la solution proposée.

## 3.1 Présentation de l'organisme d'accueil

### 3.1.1 Historique de la BMT

Dans son plan de développement 2004-2006, l'entreprise portuaire de Bejaia (EPB) avait inscrit à l'ordre du jour le besoin d'établir un partenariat pour la conception, le financement, l'exploitation et l'entretien d'un terminal à conteneurs au port de Bejaia.

Dès lors, l'EPB s'est lancé dans la tâche d'identifier les partenaires potentiels et a arrêté son choix sur le groupe PORTEK qui est spécialisé dans le domaine de la gestion des terminaux à conteneurs. Le projet a été présenté au conseil de participation de l'état (CPE) en février 2004. Le CPE a donné son accord au projet en mai 2004.

Sur accord du gouvernement, Bejaia Méditerranéen Terminal Spa « BMT Spa » a vu le jour avec la jointe venture de l'entreprise portuaire de Bejaia (EPB) à 51% et PORTEK une société Singapourienne à 49%.

En 2011 PORTECK Systems and Equipment, a été racheté par le groupe Japonais MITSUI.


Figure 3.1-Les partenaires de la BMT

(Ressource externe)

### 3.1.2 Présentation de BMT

BMT (Béjaia Mediterranean Terminal) est une jointe venture entre l'entreprise Portuaire de Bejaia et Portek Systems & Equipment. EPB est l'autorité portuaire qui gère le port de Béjaia. PORTEK Systems and Equipment, c'est une filiale du groupe PORTEK qui est un opérateur de terminaux à conteneurs présent dans plusieurs ports dans le monde et également spécialisé dans les équipements portuaires.

BMT Spa « société par actions », c'est une entreprise prestataire de services spécialisée dans le fonctionnement, l'exploitation, et la gestion du terminal à conteneurs du port de Bejaia. Pour atteindre son objectif, elle s'est doté d'un personnel compétent particulièrement formé dans l'opération de gestion des terminaux à conteneurs. Elle dispose d'équipements d'exploitation des plus perfectionnés pour les opérations de manutention et d'acconage afin d'offrir des prestations de services de qualité, d'efficacité et de fiabilité en des temps records et a des coûts compétitifs. BMT Spa offre ses prestations sur la base 24H/7j.

Le niveau de la technique mis en place et la qualité des infrastructures et équipements performants (portiques de quai, portiques gerbeurs) font aujourd'hui du port de Bejaia et de BMT Spa, le premier terminal moderne d'Algérie avec une plate- forme portuaire très performante.

Figure 3.2-Le rôle de la BMT

(Ressource externe)

### 3.1.3 Situation géographique

La BMT est localisée au nouveau quai, dans le bassin sud du port de Béjaia, cette dernière fournie des services vastes et importants par des infrastructures routières reliant l'ensemble des villes du pays, des voies ferroviaires et d'un aéroport international.

Au niveau national, BMT est située au centre du Nord-est de l'Algérie, sa position géographique est privilégiée, car elle bénéficie de l'une des baies les des plus importantes en méditerranée.

BMT SPA se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Béjaïa, reliée à la route nationale ce qui facilite le transport de marchandises conteneurisées de toute nature vers l'arrière-pays et vers d'autres destinations telles que la banlieue d'Alger.

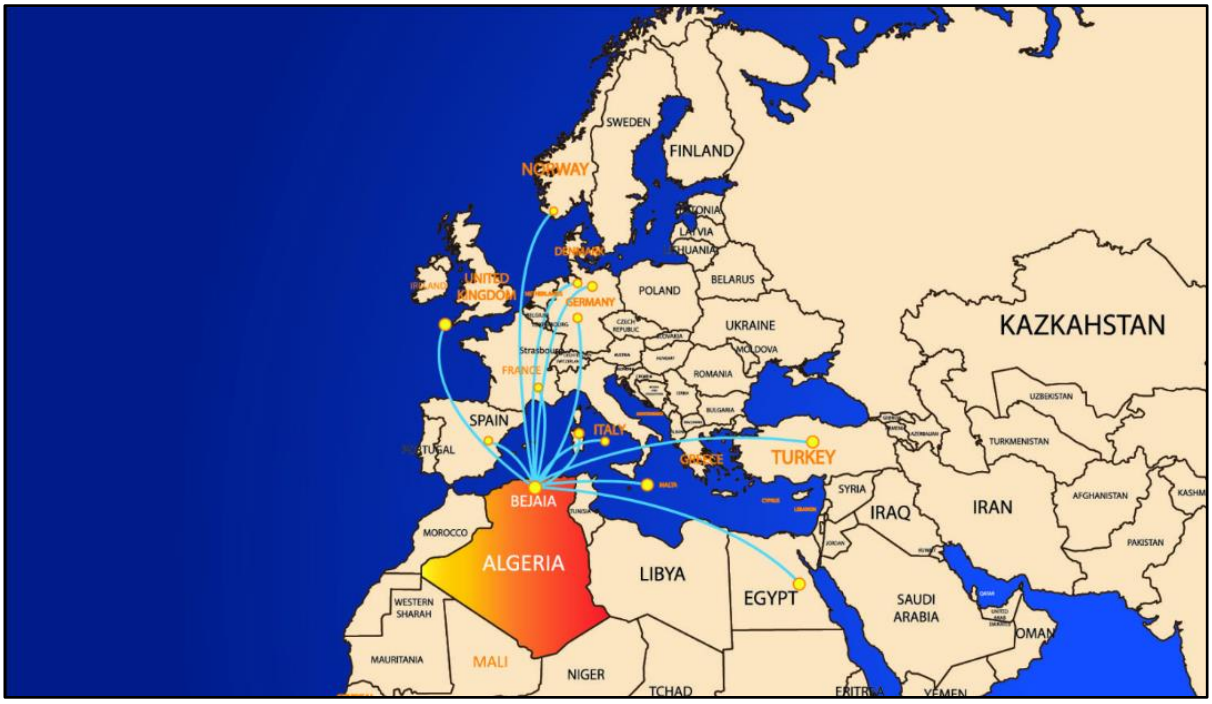



Figure 3.3-La localisation de l'entreprise BMT

(Ressource externe)

### 3.1.4 Structure et organigramme de la BMT

Comme toutes les entreprises, Béjaïa Méditerranéen Terminal dispose un organigramme bien structuré composé d'une direction générale qui se divise en plusieurs sous-directions de différents services comme illustré par Figure 3.4 :

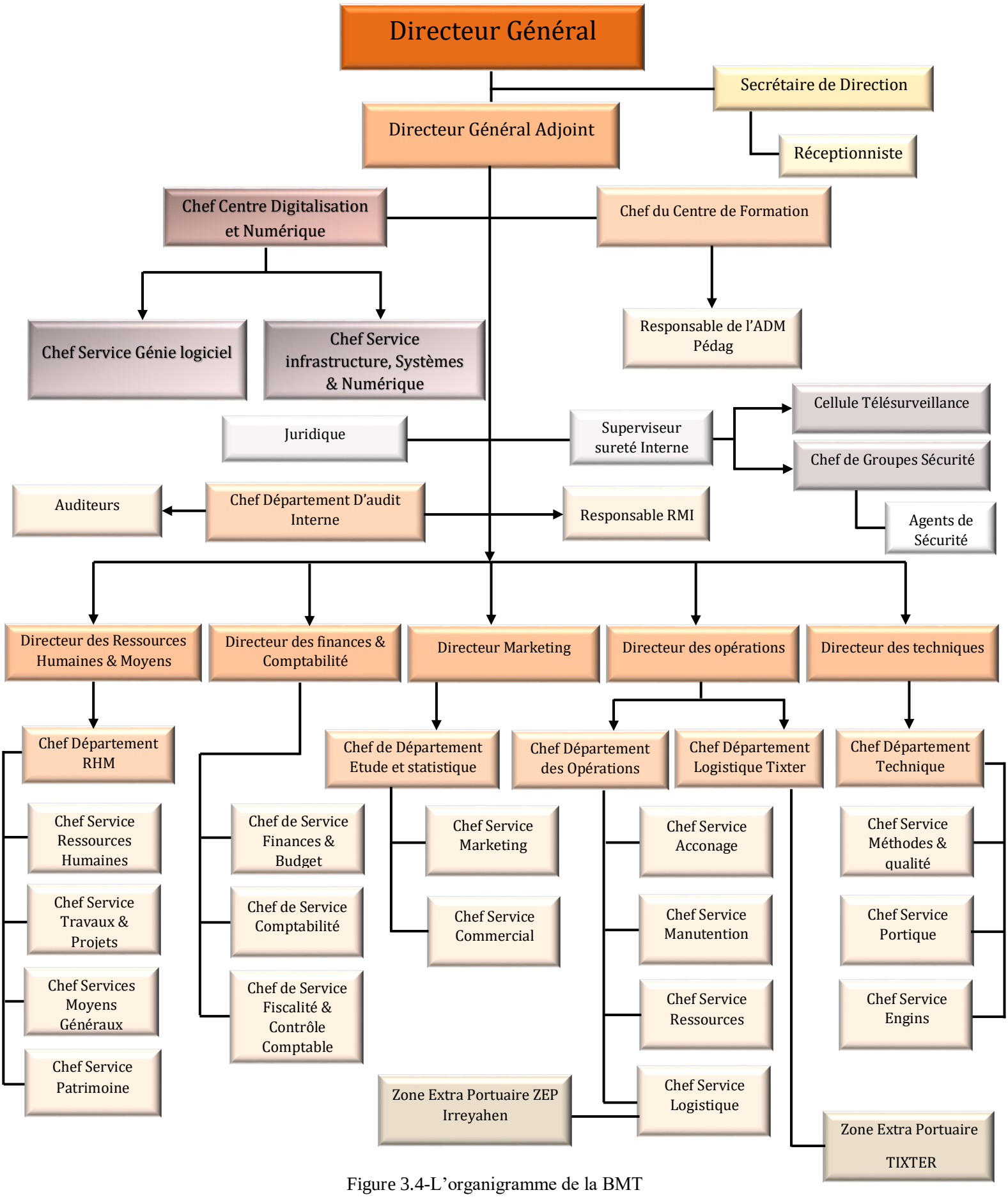



Figure 3.4-L'organigramme de la BMT

**Direction générale (DG) :**

À sa tête le Directeur Général qui gère la société « BMT-spa », il a pour rôle de définir et de piloter la stratégie globale de l'entreprise et il assigne des directives au Directeur Général Adjoint qui fait la liaison et coordonne entre les différentes directions de l'entreprise.

Les deux éléments suivants font partie à la direction générale :

- Le département audit interne : assure l'audit des procédures et mesure leur efficacité.
- Le centre de digitalisation et numérique (CDN) : mettre en place un schéma directeur informatique et uniformise les processus en termes de digitalisation, d'automatisation d'infrastructures informatiques

❖ **Direction des ressources humaines et moyens (DRHM) :**

Elle est directement rattachée à la direction générale, sa mission est de mettre en œuvre des systèmes de gestion intégrés à la stratégie de BMT pour atteindre ses objectifs et qui traduisent une adéquation entre les impératifs économiques et les attentes du personnel. L'importance de cette structure réside dans la recherche de meilleurs potentiels, les conserver on leur offrant les meilleurs conditions (climat de travail, environnement, développement des compétences et formations adéquates).

Cette direction se compose de quatre principaux services qui sont :

- Le Service Ressources Humaines : assure la gestion administrative du personnel et le développement des compétences.
- Le Service Moyens Généraux : satisfaire les besoins des différentes structures en produits et prestations de services.
- Le Service de Patrimoine : assure la gestion des stocks et des immobilisations.
- Le Service Projet et Travaux : assure la réalisation et la gestion des travaux et le suivi des projets.

❖ **Direction des finances et comptabilités (DFC) :**

La direction des finances et de la comptabilité est le domaine de la finance relatif aux décisions financières d'une entreprise. Elle a pour principal rôle : établir et suivre les budgets et les plans de financement. Déterminer, rechercher et négocier les financements les plus appropriés en relation avec les établissements concernés. Élaborer le bilan et autres états financiers et comptables et établir et analyser le bilan de fin d'année.

Cette direction est composée de deux services essentiels :

- Le Service Chargé des Finances et Budget : assure la gestion de la trésorerie et le suivi de l'exécution du budget de la société et de la Comptabilité analytique.
- Le Service Chargé de la Comptabilité : procède au contrôle et à l'enregistrement de toutes les opérations de la société (achat, vente, investissement, etc.).

❖ **Direction marketing (DM) :**

La direction Marketing est restructurée récemment après la jonction des trois départements (commercial + Marketing + Informatique). Elle a pour rôle, l'analyse du marché, les produits et le service demandé par les clients. Cette direction est chargée d'étudier, d'analyser et d'évaluer les offres de la concurrence et de la date de l'arrivée des nouveaux produits sur le marché. Cependant, la direction marketing se compose de :

- Service Marketing : assure la promotion de l'image de marque de l'entreprise et la mise en œuvre du plan marketing et commercial.
- Service Commercial : procède à la facturation des prestations fournies et le recouvrement des créances.

❖ **Direction des opérations (DO) :**

Appelée aussi direction du management des activités. Elle assure la planification des escales, du parc à conteneurs et la planification des ressources et des équipements. Elle prend en charge les opérations de manutention, comme la réception des navires porte-conteneurs, leurs chargements et déchargements. De plus, elle suit les opérations de l'acconage tel que : le suivi des livraisons, dépotages, restitutions du vide et le traitement des conteneurs frigorifiques.

Elle se compose de quatre services :

- Le Service Ressources : assure une meilleure affectation des ressources humaines et matérielles.
- Le Service Logistique : assure le suivi des moyens logistiques ainsi que la prestation logistique globale.
- Le Service Acconage : assure la gestion des opérations au niveau du terminal.
- Le Service Manutention : assure la gestion des opérations aux navires.

❖ **Direction des techniques (DT) :**

C'est la direction qui s'occupe de la stratégie industrielle, sa mission principale est la programmation des équipements. La mise en place des programmes sur un plan technique. La recherche et l'amélioration de qualité de travail et d'exploitation des équipements.

Elle se compose de :

- Service Portique : assure la maintenance des portiques de quai et des grues mobiles.
- Service Engins : assure la maintenance des portiques de quai et des grues mobiles.
- Service Méthodes et Qualité : assure la mise en œuvre du plan de maintenance des équipements.

### 3.1.5 Objectifs de la BMT

- ✓ Faire du terminal à conteneur de BMT une infrastructure moderne et de répondre aux exigences les plus sévères en matière de qualité dans le traitement du conteneur.
- ✓ La mise à disposition d'une nouvelle technique dans le traitement du conteneur pour :
    - Un gain de productivité.
    - Une réduction du coût d'escale.
    - Une fiabilité de l'information.
    - Un meilleur service des clients.
    - Faire face aux concurrences nationales et internationales.
    - Gagner des parts du marché.

- ✓ Sauvegarder la marchandise des clients.
- ✓ Faire face à la concurrence nationale et internationale.
- ✓ Gagner des parts de marché importantes.

### 3.1.6 Les opérations de la BMT

L'activité principale de la BMT est la gestion et l'exploitation du terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont un rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients.

Bejaia Méditerranéen Terminal reçoit annuellement un grand nombre de navires pour lesquels elle assure les opérations de planification, de manutention et d'acconage avec un suivi et une traçabilité des opérations.

- ❖ <u>Opérations de planification</u>
    - ✓ Planification des escales.
    - ✓ Planification déchargement/chargement.
    - ✓ Planification du parc à conteneurs.
    - ✓ Planification des ressources : équipes et moyens matériels.

- ❖ <u>Opérations de manutention</u>
    - ✓ La réception des navires porte-conteneurs.
    - ✓ Le déchargement des conteneurs du navire.
    - ✓ La préparation des conteneurs à embarquer.
    - ✓ Le chargement des conteneurs du navire.

- ❖ <u>Opérations d'acconage</u>
    - ✓ Transfert des conteneurs vers les zones d'entreposage.
    - ✓ Transfert des conteneurs frigorifiques vers la zone « reefers ».
    - ✓ Mise à disposition des conteneurs aux services de contrôle aux frontières.
    - ✓ Mise à disposition des conteneurs vides.

- ✓ Suivi des livraisons et des dépotages.
- ✓ Suivi des restitutions et des mises à quai pour embarquement.
- ✓ Gestion des conteneurs dans les zones de stockage.
- ✓ Sécurité absolue sur le terminal.

## 3.2 Présentation du service d'accueil (Centre Digitalisation et Numérique)

### 3.2.1 Présentation et Organisation

Lorsque la création de l'entreprise, le service informatique faisait partie à la direction marketing. Quelques années plus tard, l'entreprise a créé un département d'informatique indépendant de la direction marketing et composé de deux sections : section d'étude et développement et section d'exploitation.
En 2021, le département informatique a été remplacé par le centre digitalisation et numérique qui est composé de deux services :

- Service génie logiciel.
- Service infrastructure, système et numérique.

Le centre digitalisation et numérique est un service qui appartient à la direction générale, il met à la disposition des acteurs de BMT les moyens informatiques (matériels, logiciels) permettant la mise en œuvre du système d'information et la gestion des ressources informatique de l'entreprise. De plus, il assure la maintenance du parc informatique et le développement de nouvelles applications aux différentes structures.

### 3.2.2 Missions et objectives de centre digitalisation et numérique

Parmi les principales missions des deux services, nous citons :

**Service génie logiciel :** a comme fonctions:

- ✓ Étude, conception et développement des applications informatiques.
- ✓ Suivi des évolutions des applications de gestion existante.
- ✓ Maintenance des logiciels de gestion existante.
- ✓ Sécurité des systèmes d'information de l'entreprise.
- ✓ Assurer l'évolution de système d'information.
- ✓ Sauvegarde et contrôle des données de l'entreprise.
- ✓ Administration des serveurs de messagerie et du site web.

**Service infrastructure Systèmes et Numérique :** a comme tâches :

- ✓ Installation et la mise à niveau des systèmes d'exploitation des équipements informatiques.
- ✓ Assure l'implémentation des nouveaux systèmes ou des nouvelles versions.

- ✓ Garantit le bon fonctionnement des systèmes informatiques et assure la maintenance des équipements.
- ✓ Gère le réseau informatique et veille à son évolution et à son optimisation.
- ✓ Offre les éléments nécessaires à la sécurité pour l'accès aux données de l'entreprise.
- ✓ Garantit la qualité de service (optimisation des performances informatiques, haut taux disponibilité des applications et systèmes d'exploitation).
- ✓ Gère l'administration de l'infrastructure logicielle en surveillant les performances et en apportant les solutions correctives nécessaires.

## 3.3 Étude de l'existant

### 3.3.1 Présentation du réseau de la BMT

Le réseau de la BMTspa est un réseau Ethernet qui relie les différents équipements d'un réseau LAN en se basant sur la topologie étoile. La norme de câblage utilisé est T568B selon les types de périphériques à connecter.

Afin de se connecter au réseau Internet, la BMT s'appuie sur le standard de transmission de données sans fil WIMAX (World Wide Interoperabilite for Microware Access) pour assurer la transmission des données à haut débit (70Mbit/s) par voie hertzienne en utilisant une fréquence radio privée et sécurisée.

### 3.3.2 Infrastructure réseau

L'entreprise générale possède deux sites physiques : la BMT qui se trouve au niveau du port de Bejaia et la ZEP (zone extra-portuaire) sur la rue d'Irriyahen Bejaia.

La BMT possède un grand parc informatique composé de trois (03) réseaux :

i. **Réseau Local (LAN) :** c'est un réseau Wi-fi et filaire relie les sites distants par une fibre optique. Il est composé par :
   - Un serveur de fichier : assure le transfert des données à travers un réseau.
   - Un serveur d'intranet : gère les applications de messageries et d'internet.
   - Un serveur de caméra : gère les caméras de surveillance de l'entreprise.
   - Un serveur NAS : contient plusieurs baies de stockage accessible depuis les postes clients pour le stockage des données.
   - Les postes de travail.
   - Un switch a 24 ports : les serveurs web sont reliés à un Switch auquel sont branchés les postes de travail.

   Le réseau LAN possède un point d'accès relié au switch pour permettre aux appareils sans fil de se connecter à un réseau filaire.

ii. **Réseau de production CTMS** (Container Terminal Management System) : c'est un système de gestion du terminal à conteneurs développés par un prestataire de services.

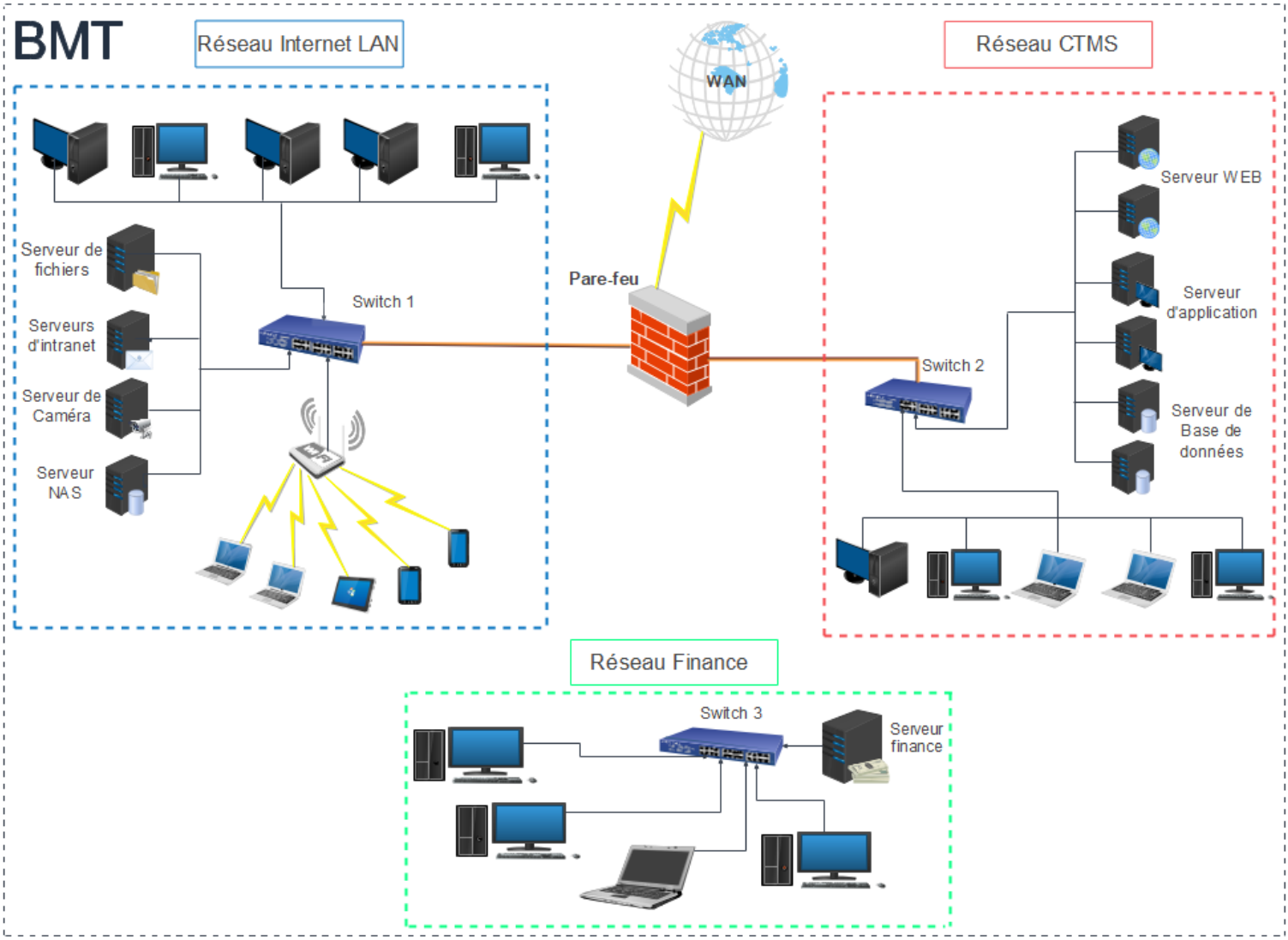
Ce réseau est basé sur l'architecture client-serveur qui assure la gestion des activités opérationnelles (regroupe les domaines navires, conteneurs, etc.) et fonctionnelles (tout ce qui concerne la gestion des ressources humaines, et du parc auto).
Ce réseau principal de l'entreprise est composé de :

- Deux serveurs de bases de données Oracle.
- Deux serveurs d'applications TOMCAT.
- Deux serveurs web Apache.
- Les postes de travail.
- Un Switch : auxquels sont bronchés les postes de travail et les serveurs.

iii. **Réseau finance :** c'est un réseau privé et sensible pour cela, il est complètement isolé de l'internet, et utilisé que pour le service fiance et comptabilité. Ce réseau offre l'accès à une dizaine de personnes uniquement pour garantir la confidentialité des données. Il est composé de :

- Un switch.
- Un serveur des finances.
- Les Postes de travail.

La cartographie ci-dessous montre l'architecture réseau de la BMT :



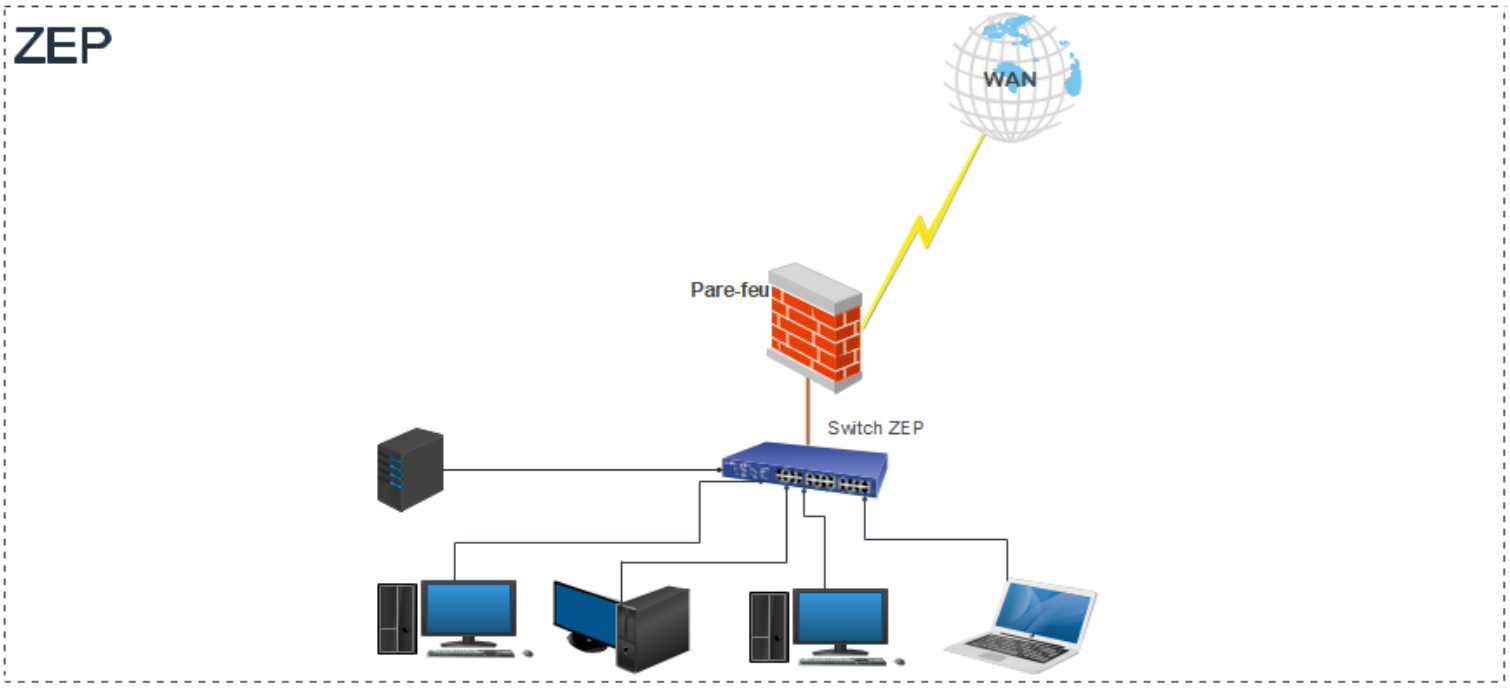




Figure 3.5-Architecture réseau de l'entreprise BMT

### 3.3.3 Présentation et caractéristiques des équipements du réseau

Tableau 3.1 décrit les différents équipements informatiques existant au niveau de l'entreprise BMT.

Tableau 3.1-les équipements du réseau BMT

| Nom de l'équipement | Modèle | Caractéristique |
|---|---|---|
| **Pare-feu** | Fortigate 100F | - **Débit :**20 Gbps<br>- **Débit de protection contre les menace** : 700 Mbps- 1Gbps<br>- **Fréquence :** 5GHz<br>- **Debit VPN :**11,5 Gbps |
| **Switch** | Cisco sg200-26 | - **RAM :** 128 Mo<br>- **Mémoire Flash :** 16Mo<br>- **Performances :** (capacité de commutation) 52 Gbps<br>- **Performance de transfert** (taille de paquet 64 octets) : 38,69Mpps<br>Port :24 port |
| **Serveur** | HP Proliant DL380P génération 10 | - Processeur Intel Xeon Silver 4110 (Octo-core 2.1 GHz/3.0 GHz Turbo-16 threads-Cache 11 Mo)<br>Alimentation :500 Watts<br>Adaptateur ethernet HPE 1 Gb 331i 4 ports Eth Gigabit 10/10/1000 Mbit/S |
| **Laptop** | ASUS X409F | - **Processeur Core :** intel i5 10 th Génération<br>- **RAM :** 16Go<br>- **SSD :**512 Go<br>- **Processeur Graphique :** NVIDIAMX250 |

- **Le Pare-feu Fortigate :** le pare-feu de nouvelle génération (NGFW) Fortigate est une solution Unified Threat Management (UTM) société de cybersécurité, développé par la société Fortinet qui offre des fonctionnalités de sécurité avancées pour protéger les réseaux d'entreprise contre les menaces et les attaques.

  Fortigate utilise une variété de technique telle que la détection et la prévention des intrusions, la sécurité et le filtrage web, l'analyse de contenu ainsi que les systèmes d'antivirus, anti-malwares, VPN…

  Ce pare-feu est très performant et facile à administrer de plus, il est compatible avec les protocoles de sécurité tels que le VPN, IP sec, SSL, FTPS, et d'autre : SNMP, DNS, DHCP, etc. Ce qui facilite son intégration avec d'autres équipements de sécurité.


Figure 3.6-le pare-feu Fortigate de Fortinet

## 3.4 Présentation de projet à réaliser

L'analyse et l'étude de la situation de la sécurité au sein d'entreprise représentent une étape très importante pour pouvoir définir les manques et apporter des améliorations compatibles avec le réseau de l'entreprise.

Notre travail consiste à présenter les lacunes constatées durant l'étude effectuée sur l'architecture réseau de l'entreprise BMT, afin de mettre en œuvre des améliorations à cette architecture pour un meilleur fonctionnement et pour pallier le manque de sécurité.

### 3.4.1 Problématiques

L'étude du réseau de BMT nous a permet de découvrir plusieurs manques et contraintes qui peuvent réduire la qualité de ce réseau.

- L'absence de la segmentation du réseau ce qui implique une surcharge du trafic.
- Le réseau finance est complètement isolé des autres réseaux alors que ses utilisateurs ont parfois besoin d'accéder aux ressources et aux données des autres réseaux.
- L'absence de la zone démilitarisée
- L'absence d'une liaison fiable et sécurisée entre les deux sites de l'entreprise BMT pour avoir l'accès à distance.
- Une mauvaise gestion et attribution d'adresse IP sur le réseau CTMS (configuration d'adresse IP manuellement).
- Manque de mécanisme de gestion et d'organisation des utilisateurs et des ressources.
- L'absence de la redondance et de la haute disponibilité dans les réseaux de la BMT.

### 3.4.2 Solution proposée

Pour renforcer la sécurité du réseau nous allons modifier l'architecture du réseau et apporter quelques améliorations consistant à :

- Configurer les VLAN sur les deux réseaux LAN et CTMS selon les services et les missions des départements de l'entreprise, cette segmentation du réseau en plusieurs sous réseau permet d'ajouter un niveau de sécurité et facilite la gestion des postes de travail.
- Relier le réseau finance au réseau local de l'entreprise et le séparé logiquement par la configuration de VLAN.
- Création de la DMZ pour regrouper l'ensemble des serveurs accessible depuis l'extérieur pour améliorer la sécurité de réseau
- Protéger les DMZ de l'entreprise en créant des VLAN privés.
- Améliorer la configuration des pare-feu par la mise en place d'une liste de contrôle d'accès selon les besoins d'accès, du NAT pour renforcer la sécurité. Et implémenter ses interfaces pour augmenter la redondance.
- La mise en place d'un pare-feu secondaire pour assurer la haute disponibilité du réseau en cas de panne.
- La BMT est composée de deux sites distants, pour relier ses pôles tout en assurant une connexion fiable et sécurisée, nous allons mettre en place la solution VPN Site à site qui sera implémenté entre les deux pare-feu Fortigate en utilisant le protocole IPsec.
- La configuration d'un Serveur DHCP sur le réseau CTMS de l'entreprise : c'est plus efficace vu le nombre élever des utilisateurs.
- Améliorer l'architecture réseau en utilisant le modèle hiérarchique en couches.
- La mise en place de l'annuaire Active directory pour organiser la gestion des utilisateurs et des ressources.
- Assurer la disponibilité du réseau par la configuration des Protocoles de redondance HSRP et GLBP sur les deux réseaux LAN et CTMS.

La mise en place de la technologie EtherChannel pour augmenter la bande passante du réseau.

### 3.4.3 Nouvelle architecture proposée

La figure suivante illustre une nouvelle architecture améliorée du réseau de l'entreprise BMT que nous allons configurer dans ce qui suit :

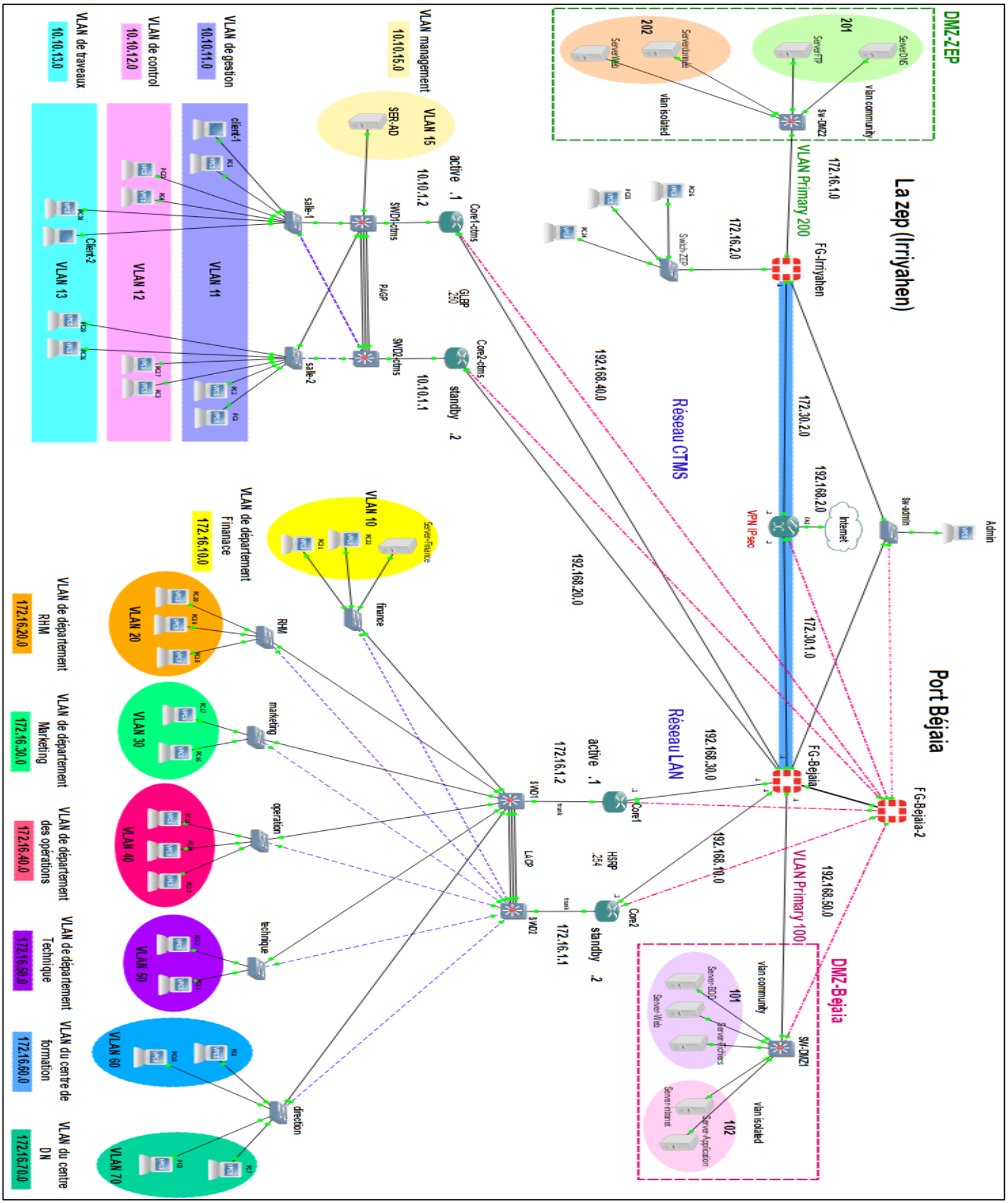



Figure 3.7-Nouvelle architecture réseau proposée

## *Conclusion*

À travers ce chapitre, nous avons présenté l'organisme d'accueil BMT-spa. Afin de comprendre ses objectives, sa structure, ainsi le fonctionnement de ces différentes directions, précisément nous avons détaillé les missions du centre digitalisation et Numérique où notre stage s'est déroulé dans le but de se familiariser avec le réseau de la BMT, de comprendre son installation, sa construction et l'utilité de ses entités, ce qui nous a permis de déterminer ses failles et ses faiblesses.

L'étude de ses failles nous a conduits à proposer des améliorations pour pallier ses dernières. Le prochain chapitre est consacré à la description et à la réalisation des solutions citées précédemment, à savoir l'installation du matériel et des logiciels ainsi que les configurations des équipements concernés.

# Chapitre IV :

## Simulation et réalisation

# *Introduction*

Ce chapitre représente le corps essentiel de ce mémoire à travers lequel nous allons expliquer et réaliser nos améliorations de l'architecture du réseau BMT proposées dans le chapitre présidant.

Dans la première partie, nous allons décrire les outils adaptés à la réalisation de notre projet (VMware Workstation, Graphical Network Simulator-3…), la deuxième partie est consacrée à la simulation et à la présentation des étapes suivies pour la configuration du réseau et on termine par les tests nécessaires à la vérification de travail réalisé.

## 4.1 Présentation de l'environnement de travail

### 4.1.1 Présentation des logiciels utilisés

#### 4.1.1.1 Logiciel VMware Workstation :

Le VMware Workstation est un logiciel utilisé pour la création d'une ou de plusieurs machines virtuelles, il permet donc à un PC physique d'exécuter simultanément plusieurs systèmes d'exploitation. Ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

Le VMware Workstation est installé généralement sur les systèmes d'exploitation Windows, Linux, Solaris et BSD (Berkeley Software Distribution). Il offre les avantages de plusieurs ordinateurs sans les coûts supplémentaires, la configuration physique et la maintenance.

Figure 4.1-VMware Workstation.

#### 4.1.1.2 Graphical Network Simulator-3

GNS3 l'abréviation de Graphical Network Simulator-3 est un logiciel libre et open source écrit en Python et lancée pour la première fois en 2008. Il permet aux utilisateurs de simuler des infrastructures informatiques. Sa dernière version est 2.2.38 (28 février 2023).

Ce logiciel est largement utilisé dans l'industrie des réseaux, car il est fiable et gratuit de plus, il offre les moyennes de créer, simuler, tester et résoudre les problèmes des topologies de réseau complexe.

Grâce à GNS3, les utilisateurs peuvent créer des réseaux virtuels en connectant sur des machines virtuelles. Les technologies de virtualisation utilisées par GNS3 sont Dynamips, VPCS,

VMWare Workstation/ESXi, VirtualBox, QEMU/KVM, Docker, et il peut être utilisé sur les systèmes d'exploitation Windows, Linux, Microsoft et Mac OS.


Figure 4.2-Graphical Network Simulator-3.

### 4.1.2 Présentation des équipements utilisés

- **Commutateur :** le switch ou commutateur réseau est un dispositif d'interconnexion de niveau 2 du modèle OSI, il permet la communication entre deux ou plusieurs appareils informatiques tels que des ordinateurs**.**
- **Serveur :** c'est un dispositif informatique qui offre des services aux clients pour assurer le partage des fichiers, le sauvgarde des données…
- **Commutateur de niveau 3 :** c'est un équipement multicouche qui assure à la fois les fonctions de switching habituelles c'est-à-dire les tache d'un switch de niveau 2 et les fonctions de routeur
- **Routeur :** c'est un équipement réseau informatique de la couche 3 du modèle OSI qui relie deux ou plusieurs réseaux ou sous-réseau pour faire transiter des paquets d'une interface vers une autre.
- **Windows Serveur 2022 :** c'est la dernière version de système d'exploitation commercialisé par Microsoft, sortie en août 2022 et destinée aux serveurs. Windows Server 2022 inclut une sécurité multicouche avancée, des fonctionnalités hybrides avec Azure et une plateforme d'applications flexible.
- **Windows 10 :** c'est un système d'exploitation de la famille Windows NT développé par la société américaine Microsoft et publier en juillet 2015.
- **IOS Cisco :** (abréviation de internetwork Operating System) c'est un système d'exploitation propriétaire Cisco utilisé par la plupart des équipements. IOS dispose d'un ensemble de fonctions de routage, de commutation et d'interconnexion de réseau.
- **Wireshark** : c'est un analyseur de paquets libre et gratuit. Permet de visualiser et de capturer les trames et les paquets qui circulent au sein d'un réseau.

## 4.2 Table d'adressage

### 4.2.1 La table d'adressage des équipements

Tableau 4.1-La table d'adressage des équipements

| Equipement | Interface réseau | Adresse IP |
|---|---|---|
| Routeur 1 LAN (Core 1-LAN) | Ethernet 0/0<br>Ethernet 0/1 | Encapsulation dot1Q<br>192.168.10.2 |
| Routeur 2 LAN (Core 2-LAN) | Ethernet 0/0<br>Ethernet 0/1 | Encapsulation dot1Q<br>192.168.30.2 |
| Routeur 1 CTMS (Core 1-CTMS) | Ethernet 0/0<br>Ethernet 0/1 | Encapsulation dot1Q<br>192.168.20.2 |
| Routeur 2 CTMS (Core 2-CTMS) | Ethernet 0/0<br>Ethernet 0/1 | Encapsulation dot1Q<br>192.168.40.2 |
| Routeur FAI | Ethernet 0/1<br>Ethernet 0/2 | 172.30.2.2<br>172.30.1.2 |
| Fortigate Bejaia | Port 1 (WAN)<br>Port 2 (DMZ)<br>Port 3 (LAN 1)<br>Port 4 (LAN 2)<br>Port 5 (CTMS 1)<br>Port 6 (CTMS 2) | 172.30.1.1<br>192.168.50.1<br>192.168.10.1<br>192.168.30.1<br>192.168.20.1<br>192.168.40.1 |
| Fortigate Irriyahen(ZEP) | Port1 (WAN)<br>Port 2 (LAN de Irriyahen)<br>Port 3 (DMZ) | 172.30.2.1<br>172.16.2.2<br>172.16.2.1 |

### 4.2.2 La table d'adressage des VLAN

#### 4.2.2.1 Réseau CTMS

Tableau 4.2-La table d'adressage des VLAN du réseau CTMS

| Nom du VLAN | ID du VLAN | Adresse IP CTMS 1 (Active) | Adresse IP CTMS 2 (Standby) |
|---|---|---|---|
| VLAN de gestion | 11 | 10.10.11.1 | 10.10.11.2 |
| VLAN de control | 12 | 10.10.12.1 | 10.10.12.2 |
| VLAN de travaux | 13 | 10.10.13.1 | 10.10.13.2 |
| VLAN Voice | 14 | 10.10.14.1 | 10.10.14.2 |
| VLAN Server | 15 | 10.10.15.1 | 10.10.15.2 |
| Vlan native | 99 | / | / |

#### 4.2.2.2 Réseau LAN

Tableau 4.3-La table d'adressage des VLAN du réseau LAN

| Nom du VLAN | ID du VLAN | Adresse IP LAN1 (Active) | Adresse IP LAN2 (Standby) |
|---|---|---|---|
| VLAN finance | 10 | 172.16.10.1 | 172.16.10.2 |
| VLAN RHM | 20 | 172.16.20.1 | 172.16.20.2 |
| VLAN Marketing | 30 | 172.16.30.1 | 172.16.30.2 |
| VLAN opération | 40 | 172.16.40.1 | 172.16.40.2 |
| VLAN Technique | 50 | 172.16.50.1 | 172.16.50.2 |
| VLAN Formation | 60 | 172.16.60.1 | 172.16.60.2 |
| VLAN DN | 70 | 172.16.70.1 | 172.16.70.2 |
| | | | |
| VLAN Voice | 80 | 172.16.80.1 | 172.16.80.2 |
| VLAN native | 99 | / | / |

#### 4.2.2.3 La DMZ-Bejaia

Tableau 4.4-La table d'adressage des VLAN de la DMZ-Bejaia

| Nom du PVLAN | ID du PVLAN | Adresse de PVLAN |
|---|---|---|
| Primary VLAN | 100 | / |
| Community VLAN | 101 | 192.16.50.2/24<br>192.16.50.3/24<br>192.168.50.4/24 |
| Isolated VLAN | 102 | 192.16.50.5/24<br>192.168.50.6/24 |

#### 4.2.2.4 La DMZ-Irriyahen

Tableau 4.5-La table d'adressage des VLAN de la DMZ-Irriyahen

| Nom du PVLAN | ID du PVLAN | Adresse de PVLAN |
|---|---|---|
| Primary VLAN | 200 | / |
| Community VLAN | 201 | 172.16.1.2/24<br>172.16.1.3/24 |
| Isolated VLAN | 202 | 172.16.1.4/24<br>172.16.1.5/24 |

### 4.2.3 La table d'adressage de routage inter-VLAN

#### 4.2.3.1 Réseau CTMS

Tableau 4.6-La table de routage-inter VLAN du réseau CTMS

| Interface | Adresse IP Core1 (CTMS) | Adresse IP Core2 (CTMS) | Passerelle HSRP |
|---|---|---|---|
| Ethernet 0/0.11 | 10.10.11.1/24 | 10.10.11.2/24 | 10.10.11.250 |
| Ethernet 0/0.12 | 10.10.12.1/24 | 10.10.12.2/24 | 10.10.12.250 |
| Ethernet 0/0.13 | 10.10.13.1/24 | 10.10.12.2/24 | 10.10.13.250 |
| Ethernet 0/0.14 | 10.10.14.1/24 | 10.10.14.2/24 | 10.10.14.250 |
| Ethernet 0/0.15 | 10.10.15.1/24 | 10.10.15.2/24 | 10.10.15.250 |

#### 4.2.3.2 Réseau LAN

Tableau 4.7-La table de routage inter-VLAN du réseau LAN

| Interface | Adresse IP Core1 (LAN) | Adresse IP Core2 (LAN) | Passerelle HSRP |
|---|---|---|---|
| Ethernet 0/0.10 | 192.168.10.1/24 | 192.168.10.2/24 | 192.168.10.254 |
| Ethernet 0/0.20 | 192.168.20.1/24 | 192.168.20.2/24 | 192.168.20.254 |
| Ethernet 0/0.30 | 192.168.30.1/24 | 192.168.30.2/24 | 192.168.30.254 |
| Ethernet 0/0.40 | 192.168.40.1/24 | 192.168.40.2/24 | 192.168.40.254 |
| Ethernet 0/0.50 | 192.168.50.1/24 | 192.168.50.2/24 | 192.168.50.254 |
| Ethernet 0/0.60 | 192.168.60.1/24 | 192.168.60.2/24 | 192.168.60.254 |
| Ethernet 0/0.70 | 192.168.70.1/24 | 192.168.70.2/24 | 192.168.70.254 |
| Ethernet 0/0.80 | 192.168.80.1/24 | 192.168.80.2/24 | 192.168.80.254 |

## 4.3 Configuration de réseau LAN

### 4.3.1 Configuration des VLAN

#### 4.3.1.1 Configuration des Switch en mode trunk

Pour faire passer les différents VLAN sur le réseau nous allons configurer les portes des Switch distribution et accès en mode Trunk, de plus nous allons créer un VLAN natif (VLAN 99) pour prendre en charge les trames non étiquetées.

Les interfaces à configurer dans ce cas sont celles entre les commutateurs de la couche d'accès et le commutateur distribution et les interfaces entre le commutateur distribution et le routeur pour pouvoir router les différent VLAN vers l'extérieure.

❖ Configuration des Switches distribution en mode trunk

```
SWD1 (config)# interface range ethernet 0/1-3, ethernet 1/0-2, ethernet 3/1-3
SWD1 (config-if-range)# switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99
SWD1 (config-if-range)# switchport trunk native vlan 99
SWD1 (config-if-range)# switchport trunk encapsulation dot1q
SWD1 (config-if-range)# switchport mode trunk
SWD1 (config-if-range)# exite
SWD1 (config) # interface ethernet 0/0
SWD1 (config-if-range)# switchport trunk encapsulation dot1q
SWD1 (config-if-range)# switchport mode trunk
```

Listing 4.1-Configuration de Switch distribution en mode trunk.

❖ Configuration de mode Trunk sur les Switch d'accès

```
Direction (config) # interface range ethernet 0/0, ethernet 0/1
Direction (config-if-range)# switchport trunk allowed vlan 10,20,30,40,50,60,70,80,99
Direction (config-if-range)# switchport trunk native vlan 99
Direction (config-if-range)# switchport trunk encapsulation dot1q
Direction (config-if-range)# switchport mode trunk
```

Listing 4.2-Configuration de Switch acces en mode trunk.

#### 4.3.1.2 Activation de protocole VTP

Il est nécessaire d'activer le protocole VTP pour simplifier et faciliter la gestion des VLAN.

Le serveur VTP diffuse les configurations de ses VLAN, tandis que le client VTP met à jour sa configuration de VLAN selon les informations reçues du serveur VTP.

❖ La configuration des switch distributeur en mode serveur VTP

```
SWD1 (config)# vtp mode server
Setting device to VTP Server mode for VLANS.
SWD1 (config)# vtp domain bmt.vtp
Domain name already det to bmt.vtp .
SWD1 (config)# vtp password bmt123
Password already set to bmt123
SWD1 (config)# vtp version2
SWD1 (config)#  vtp pruning
```

```
SWD2 (config)# vtp mode server
Setting device to VTP Server mode for VLANS.
SWD2 (config)# vtp domain bmt.vtp
Domain name already det to bmt.vtp .
SWD2 (config)# vtp password bmt123
Password already set to bmt123
SWD2 (config)# vtp version2
```

Listing 4.3-Configuration de VTP serveur.

❖ La configuration des switch d'accès en mode client VTP

```
Direction (config)# vtp mode client
Setting device to VTP Client mode for VLANS.
Direction (config)# vtp domain bmt.vtp
Changing VTP domain name from NULL to bmt.vtp
Direction (config)# vtp password bmt123
Setting device VTP password to bmt123
Direction (config)# vtp version2
```

Listing 4.4-Configuration de VTP client.

#### 4.3.1.3 Création des VLAN sur le Switch distribution

Nous allons créer les VLAN sur le SWD1 qui est configurer en mode VTP Serveur pour diffuser ses VLAN sur tous les autres Switch :

```
SWD1 (config)# vlan 10
SWD1 (config-vlan)# name  Finance
SWD1 (config-vlan)# vlan 20
SWD1 (config-vlan)# name RHM
SWD1 (config-vlan)# vlan 30
SWD1 (config-vlan)# name Marketing
SWD1 (config-vlan)# vlan 40
SWD1 (config-vlan)# name operation
SWD1 (config-vlan)# vlan 50
SWD1 (config-vlan)# name Technique
SWD1 (config-vlan)# vlan 60
SWD1 (config-vlan)# name formation
SWD1 (config-vlan)# vlan 70
SWD1 (config-vlan)# name DN
SWD1 (config-vlan)# vlan 80
SWD1 (config-vlan)# name VoIP
```

```
SWD1# show vlan brief

VLAN Name                    Status    Ports
------- -------------------------- --------- ---------------------

1    default                 active    Et1/3, Et2/0, Et2/1
                                       Et2/2, Et2/3, Et3/0
10   Finance                 active
20   RHM                     active
30   Marketing               active
40   Operation               active
50   Technique               active
60   formation               active
70   DN                      active
80   VoIP                    active
```

Listing 4.5-Création des VLAN.

#### 4.3.1.4 Affectation des portes de Switch accès au VLAN correspond

Nous allons configurer chaque port de switch avec le VLAN selon la Table d'adressage des VLAN du réseau LAN :

```
Technique (config)# interface range ethernet 0/1-2
Technique (config-if-range)# switchport mode access
Technique (config-if-range)# switchport access vlan 50
Technique (config-if-range)# switchport access vlan 80
```

```
Technique# show vlan brief
VLAN Name                       Status    Ports
------ -------------------------------- ---------- -------------------------------------------------------------
1    default                    active    Et1/0, Et1/1, Et1/2, Et1/3, Et2/0, Et2/1
                                          Et2/2, Et2/3, Et3/0, Et3/1, Et3/2, Et3/3
10   Finance                    active
20   RHM                        active
30   Marketing                  active
40   Operation                  active
50   Technique                  active    Et0/1, Et0/2
60   formation                  active
70   DN                         active
80   VoIP                       active    Et0/1, Et0/2
```

Listing 4.6-Configuration de VLAN sur le Switch accès.

### 4.3.2 Configuration de protocole LACP

Link Aggregation Control Protocol est un protocole EtherChannel IEEE 802.3ad permet de regrouper plusieurs ports physiques en une seule voie logique pour avoir la tolérance aux pannes et augmenter la bande passante.

Pour ce faire, nous allons créer un Channel groupe qui regroupe toutes les interfaces reliant les deux Switches Distributeurs. La configuration de ce protocole est montrée ci-dessous :

```
SWD1 (config)# interface range ethernet 3/1-3
SWD1 (config-if-range)# channel-group 2 mode active
SWD1 (config-if-range)# exite
SWD1 (config)# port-channel load-balance src-dst-mac
```

Listing 4.7-Configuration de protocole LACP.

### 4.3.3 Configuration de routeur

#### 4.3.3.1 Configuration de routage inter-VLAN

Chaque interface logique d'un routeur peut être divisée en plusieurs sous-interfaces virtuelles (la création des sous-réseaux). Comme indiqué dans Listing 4.8.

Et de même pour les VLAN 20-70

```
Core1 (config)# interface ethernet 0/0
Core1 (config-if)# no shutdown
Core1 (config)# interface ethernet 0/0.10
Core1 (config-subif)# encapsulation dot1q 10
Core1 (config-subif)# ip address 172.16.10.1 /24
```

```
Core2 (config)# interface ethernet 0/0
Core2 (config-if)# no shutdown
Core2 (config)# interface ethernet 0/0.10
Core2 (config-subif)# encapsulation dot1q 10
Core2 (config-subif)# ip address 172.16.10.2 /24
```

Listing 4.8-Configuration de routage inter VLAN sur le réseau LAN.

#### 4.3.3.2 La configuration de protocole de la redondance HSRP

Pour la mise en place de protocole HSRP. Nous allons configurer les sous-interfaces de Core 1 (Router1) en mode active, tandis que celles du Core 2 seront en mode standby.

Pour ce faire nous allons ajouter les deux commandes suivantes à la configuration des sous-interfaces de Core 1 :

- **Standby X priority 150** : pare défaut la valeur de priority est 100, pour éviter le conflit entre les deux routeurs nous allons augmenter cette valeur a 150.
- **Standby X preempt :** pour spécifier le routeur actif.

La configuration de protocole HSRP est donnée par :

```
Core1 (config)# interface ethernet 0/0.10
Core1 (config-subif)# standby version 2
Core1 (config-subif)# standby 10 ip 172.16.10.254
Core1 (config-subif)# standby 10 priority 150
Core1 (config-subif)# standby 10 preempt
```

```
Core2 (config)# interface ethernet 0/0.10
Core2 (config-subif)# standby version 2
Core2 (config-subif)# standby 10 ip 172.16.10.254
```

Listing 4.9-Configuration de protocole HSRP.

Et de même pour les sous-interfaces 0/0.20-80.

#### 4.3.3.3 La connectivité de réseau LAN vers internet

Pour connecter le réseau LAN vers le réseau interne, nous allons attribuer les adresses IP et les masques aux interfaces des routeurs connectés au pare-feu, ensuite nous allons configurer le routage statique par défaut vers le prochain saut suivant l'interface de sortie de routeur.

La configuration des interfaces des routeurs est donnée par les commandes suivantes :

```
Core1 (config)# interface ethernet 0/1
Core1 (config-if)# no shutdown
Core1 (config-if)# ip address 192.168.30.2  255.255.255.0
Core1 (config-if)# exit
Core1 (config-if)# ip route 0.0.0.0  0.0.0.0  192.168.30.1
```

Listing 4.10-Configuration de la route par défaut.

#### 4.3.3.4 Configuration de protocole DHCP

Le protocole réseau DHCP (Dynamic Host Configuration Protocol) assure la configuration automatique des paramètres IP d'une station (adresse IP, masque de sous-réseau et la passerelle par défaut.

Nous allons configurer le DHCP sur le VLAN 10-70 pour permettre l'attribution automatique des adresses IP et de même pour le routeur Core2.

```
Core1 (config)# ip dhcp excluded-address 172.16.10.1 172.16.10.10
Core1 (config)# ip dhcp pool vlan10
Core1 (dhcp-config)# network 172.16.10.0 255.255.255.0
Core1 (dhcp-config)#default-router 172.16.10.254
Core1 (dhcp-config)#dns-server 1.1.1.1
```

Listing 4.11-Configuration de protocole DHCP.

#### 4.3.3.5 Configuration de NAT sur les routeurs de réseau LAN

La translation d'IP est généralement effectuée par un routeur ou un pare-feu, sur ce qui suit, nous allons configurer le routeur comme étant un agent entre son réseau local et internet, donc seule son adresse (adresse IP publique) qui sera utilisée en externe pour présenter tous les sous-réseaux, les VLAN et les équipements internes.

Pour la configuration de NAT, nous allons créer une liste d'accès qui contient les adresses des réseaux VLAN par la suite, nous allons spécifier les interfaces d'entrées et de sortie.

La configuration de NAT pour le VLAN 20 est donnée par les commandes suivantes

```
Core1 (config)# ip access-list standard NAT-WAN
Core1 (config-std-nacl)# permit 172.16.20.0  0.0.0.255
Core1 (config-std-nacl)#exit
Core1 (config)# interface ethernet 0/1
Core1 (config-if)# ip nat outside
Core1 (config-if)# exit
Core1 (config)# interface ethernet 0/0.20
Core1 (config-subif)# ip nat inside
Core1 (config-subif)# exit
Core1 (config)# ip nat inside source list NaT-WAN interface ethernet 0/1 overload
```

Listing 4.12-Configuration de NAT.

Et de même pour les sous-réseaux 0.30-0.80

## 4.4 Configuration du réseau CTMS

### 4.4.1 Configuration des VLAN sur le réseau CTMS

#### 4.4.1.1 Configuration des Switches du réseau CTMS en mode trunk

```
SWD1-ctms (config)# interface range ethernet 0/1-2, ethernet 3/1-3
SWD1-ctms (config-if-range)# switchport trunk encapsulation dot1q
SWD1-ctms (config-if-range)# switchport mode trunk
SWD1-ctms (config-if-range)# switchport trunk allowed vlan 11,12,13,14,99
SWD1-ctms (config-if-range)# switchport trunk native vlan 99
SWD1-ctms (config-if-range)# exite
SWD1-ctms (config)# interface ethernet 0/0
SWD1-ctms (config-if)# switchport trunk encapsulation dot1q
SWD1-ctms (config-if)# switchport mode trunk
```

Listing 4.13-Configuration de switch distribution de réseau CTMS en mode trunk.

Nous allons créer le VLAN 15 pour le serveur qui sera configuré en mode access.

```
SWD1-ctms (config)# interface ethernet 0/3
SWD1-ctms (config-if)# switchport mode access
SWD1-ctms (config-if)# switchport access vlan15
```

Listing 4.14-Configuration de l'interface relié au VLAN serveur en mode acces.

❖ Configuration de Switch d'accès CTMS en mode Trunk

```
Salle1 (config)# interface range ethernet 0/0, ethernet 1/0
Salle1 (config-if-range)# switchport trunk allowed vlan 11,12,13,14,15,99
Salle1 (config-if-range)# switchport trunk encapsulation dot1q
Salle1 (config-if-range)# switchport trunk native vlan 99
Salle1 (config-if-range)# switchport mode trunk
```

Listing 4.15-Configuration de switch accès de réseau CTMS en mode trunk.

#### 4.4.1.2 Activation de protocole VTP sur les Switch de réseau CTMS

Nous avons utilisé la même configuration effectuée sur les switches de réseau LAN pour activer Le protocole VTP sur le réseau CTMS

#### 4.4.1.3 Création des VLAN sur le Switch distribution CTMS

```
SWD1-ctms (config)# vlan 11
SWD1-ctms (config-vlan)# name Gestion
SWD1-ctms (config-vlan)# vlan 12
SWD1-ctms (config-vlan)# name Control
SWD1-ctms (config-vlan)# vlan 13
SWD1-ctms (config-vlan)# name Traveaux
SWD1-ctms (config-vlan)# vlan 14
SWD1-ctms (config-vlan)# name VoIP
SWD1-ctms (config-vlan)# vlan 15
SWD1-ctms (config-vlan)# name Server
```

```
SWD1-ctms# show vlan brief
VLAN Name                        Status    Ports
---- ----------------------------- --------- -------------------------------
1    default                     active    Et1/0, Et1/1, Et1/2
                                           Et1/3, Et2/0, Et2/1
                                           Et2/2, Et2/3
11   Gstion                      active
12   Control                     active
13   Traveaux                    active
14   VoIP                        active
15   Server                      active    Et0/3
```

Listing 4.16-Création des VLAN sur réseau CTMS.

#### 4.4.1.4 Attribution des ports de Switch accès CTMS au VLAN

Nous allons attribuer les VLAN aux interfaces de Switch des deux salles, chaque Switch sera configuré par tous les VLAN (11, 12, 13, 14) selon les ports qui corrompent.

```
Salle1 (config)# interface range ethernet 1/1-2
Salle1 (config-if-range)# switchport mode access
Salle1 (config-if-range)# switchport access vlan 11
Salle1 (config-if-range)# switchport voice vlan 14
Salle1 (config-if-range)# exit

Salle1 # show vlan brief
VLAN Name                    Status  Ports
------- ------------------------- --------- -------------------------------------------------------------------------
1   default                      active    Et2/0, Et2/1, Et2/2, Et2/3, Et3/0, Et3/1, Et3/2, Et3/3
11  Gestion                  active    Et1/1, Et1/2
12  Control                          active    Et0/3, Et1/0
13  Traveaux                 active    Et0/1, Et0/2
14  VoIP                         active    Et0/1, Et0/2, Et0/3, Et1/0, Et1/1, Et1/2
15  server                       active
```

Listing 4.17-Configuration des VLAN sur les Switch d'accès de réseau CTMS.

### 4.4.2 Configuration de protocole PAGP

Nous allons configurer le protocole PAgP (Port Aggregation Protocol) propriétaire Cisco pour créer la liaison EtherChannel afin d'assurer l'agrégation de plusieurs liens physiques.

Le PAgP sera activé en mode désirable qui sera compatible sur les deux Switches distribution.

```
SWD1-ctms(config)# interface range ethernet 3/1-3
SWD1-ctms(config-if-range)# channel-group 1 mode desirable
SWD1-ctms(config-if-range)# exite
SWD1-ctms(config)# port-channel load-balance src-dst-mac
```

Listing 4.18-Configuration de protocole PAGP.

### 4.4.3 Configuration de routeur CTMS

#### 4.4.3.1 Configuration de routage inter-VLAN

```
Core1-ctms (config)# interface ethernet 0/0.11
Core1-ctms (config-subif)# encapsulation dot1q 11
Core1-ctms (config-subif)# ip address 10.10.11.1 255.255.255.0
```

```
Core2-ctms (config)#interface ethernet 0/0.10
Core2-ctms (config-subif)#encapsulation dot1q 10
Core2-ctms (config-subif)#ip address 172.16.10.2  255.255.255.0
```

Listing 4.19-Configuration de routage inter VLAN sur le réseau CTMS.

#### 4.4.3.2 Configuration de protocole GLBP

Le protocole GLBP assure la redondance et il est configuré de la même manière que HSRP.

```
Core1-ctms (config)# interface ethernet 0/0.11
Core1-ctms (config-subif)# glbp 11 ip 10.10.11.250
Core1-ctms (config-subif)# glbp 11 priority 150
Core1-ctms (config-subif)# glbp 11 preempt
Core1-ctms (config-subif)# glbp 11 load-balancing
```

```
Core2-ctms (config)# interface ethernet 0/0.11
Core2-ctms (config-subif)# glbp 11 ip 10.10.11.250
Core2-ctms (config-subif)# glbp 11 load-balancing
```

Listing 4.20-Configuration de protocole GLBP.

#### 4.4.3.3 Configuration de relais DHCP

La configuration d'un relais DHCP se fait au niveau d'un routeur pour permettre la communication et le transfert des configurations DHCP entre les hôtes et le serveur DHCP distant.

Pour ce faire, nous allons attribuer aux sous-interfaces de chaque routeur le DHCP relais c'est-à-dire, on indique pour chaque sous-interface qui est l'agent DHCP en utilisant la commande « ip helper server » suivie par l'adresse du serveur, comme indiqué sur la figure suivante :

```
Core1-ctms (config)# interface ethernet 0/0.11
Core1-ctms (config-subif)# ip helper server 10.10.15.100

Core1-ctms (config)# interface ethernet 0/0.12
Core1-ctms (config-subif)# ip helper server 10.10.15.100
```

Listing 4.21-Configuration de relai DHCP.

#### 4.4.3.4 Connectivité de réseau CTMS vers internet

Nous allons configurer l'interface de routeur ainsi que la route par défaut vers le prochain saut pour permettre la connectivité de réseau CTMS sur internet.

```
Core1-ctms (config)# interface ethernet 0/1
Core1-ctms (config-if)# no shutdown
Core1-ctms(config-if)# ip address 192.168.40.2  255.255.255.0
Core1-ctms (config-if)# exit
Core1-ctms (config-if)#ip route 0.0.0.0  0.0.0.0  192.168.40.1
```

Listing 4.22-Configuration de la route par défaut sur le réseau CTMS.

#### 4.4.3.5 Configuration de NAT sur le réseau CTMS

Vu le nombre élever des VLAN (VLAN du réseau LAN et CTMS) et pour faciliter leur gestion au niveau de Pare-feu, nous allons configurer le NAT pour éviter l'encombrement des adresses au niveau de Fortigate.

```
Core1-ctms (config)# ip access-list standard NAT-WAN
Core1-ctms (config-std-nacl)# permit permit 10.10.11.0 0.0.0.255
Core1-ctms (config-std-nacl)#exit
Core1-ctms (config)# interface ethernet 0/1
Core1-ctms (config-if)# ip nat outside
Core1-ctms (config-if)# exit
Core1-ctms (config)# interface ethernet 0/0.11
Core1-ctms (config-subif)# ip nat inside
Core1-ctms (config-subif)# exit
Core1-ctms (config)# ip nat inside source list NaT-WAN interface ethernet 0/1 overload
```

Listing 4.23-Configuration de NAT sur le réseau CTMS.

## 4.5 Configuration des DMZ sur les deux sites de la BMT

Dans cette partie, nous allons configurer le Privat VLAN pour sécuriser les serveurs de la zone démilitarisée, pour cela, nous allons créer le VLAN Primary pour faire passer les deux VLAN secondaires VLAN communicat et le VLAN isolated.

Sur le Switch de la DMZ nous allons :

- Configurer le VTP mode transparent pour permettre à l'administrateur de faire toute modification sur les VLAN en local uniquement.
- Créer le VLAN Primariy.
- Créer les VLAN community et isolated.
- Affecter les ports de switch au VLAN.

La configuration de PVLAN sur la DMZ de Bejaia est donnée ci-dessous :

```
SW-DMZ1 (config)# vtp mode transparent
Setting device to VTP Transparent mode for VLANS.

SW-DMZ1 (config)# vlan 100
SW-DMZ1 (config-vlan)# private-vlan primary
SW-DMZ1 (config-vlan)# private-vlan association 101,102
SW-DMZ1 (config-vlan)# exit

SW-DMZ1 (config)# vlan 101
SW-DMZ1 (config-vlan)# private-vlan community
SW-DMZ1 (config-vlan)# exit

SW-DMZ1 (config)# vlan 102
SW-DMZ1 (config-vlan)# private-vlan isolated
SW-DMZ1 (config-vlan)# exit
```

Listing 4.24-La création des VLAN privés

```
SW-DMZ1 (config)# interface range ethernet 0/1-3
SW-DMZ1 (config-if-range)# switchport mode private-vlan host
SW-DMZ1 (config-if-range)# switchport private-vlan host-association 100 101
SW-DMZ1 (config-if-range)# exit

SW-DMZ1 (config) # interface range ethernet 1/0-1
SW-DMZ1 (config-if-range)# switchport mode private-vlan host
SW-DMZ1 (config-if-range)# switchport private-vlan host-association 100 102
SW-DMZ1 (config-if-range)# exit

SW-DMZ1 (config) # interface ethernet 0/0
SW-DMZ1 (config-if)# switchport mode private-vlan promiscuous
SW-DMZ1 (config-if)# switchport private-vlan mapping 100 101,102
```

Listing 4.25-Configuration de VLAN privé sur le Switch de la DMZ.

De même nous allons configurer le switch de la DMZ de site irriyahen (SW-DMZ2) avec les ID Vlan suivante

- VLAN Primariy 200
- VLAN community 201
- VLAN isolated 202

## 4.6 Configuration de l'active directory

Active Directory (AD) est un ensemble de services d'annuaire destiné aux environnements Windows Server. La fonction principale de cette base de données consiste à permettre aux administrateurs de gérer et contrôler l'accès aux ressources du réseau, ce qui facilite la sécurité dans une entreprise.

Une fois l'installation est terminée, nous allons redémarrer le serveur pour nous connecter avec le compte Administrateur et voir les rôles ajoutés.

### 4.6.1 Création des étendus

Nous allons créer pour chaque VLAN son propre étendu de DHCP basé sur l'adresse de VLAN, pour se faire, sur le serveur on clique sur « outil » pour choisir « DHCP ».

Pour ajouter un nouveau étendu, nous allons suivre les étapes suivantes :

Cliquez sur serveur « Ser-AD » ensuite sur « IPv4 », une clique droite permet d'afficher une liste de plusieurs services, nous allons choisir « nouvelle étendue », par la suite on ajoute le nom et la description de la nouvelle étendue.

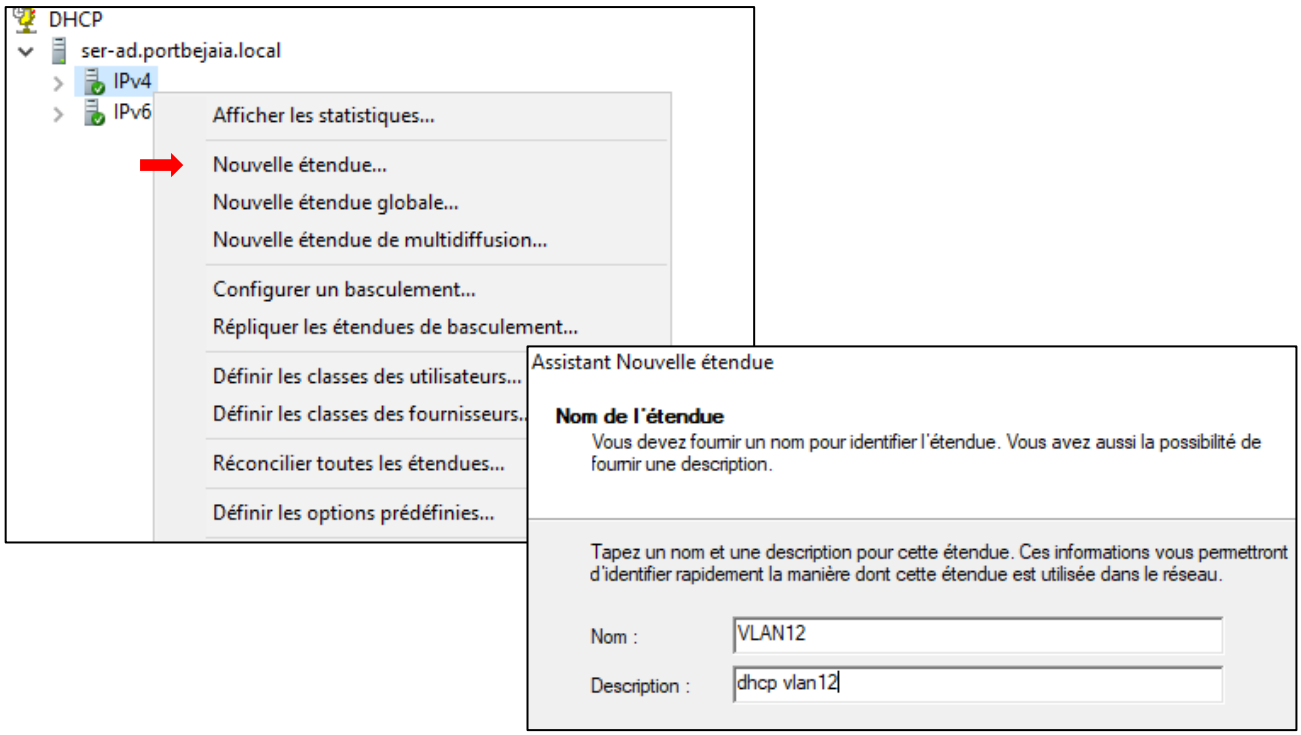



Figure 4.3-Création d'une nouvelle étendue.

On spécifie la plage d'adressage pour cette étendu et on exclue les dix premières adresse

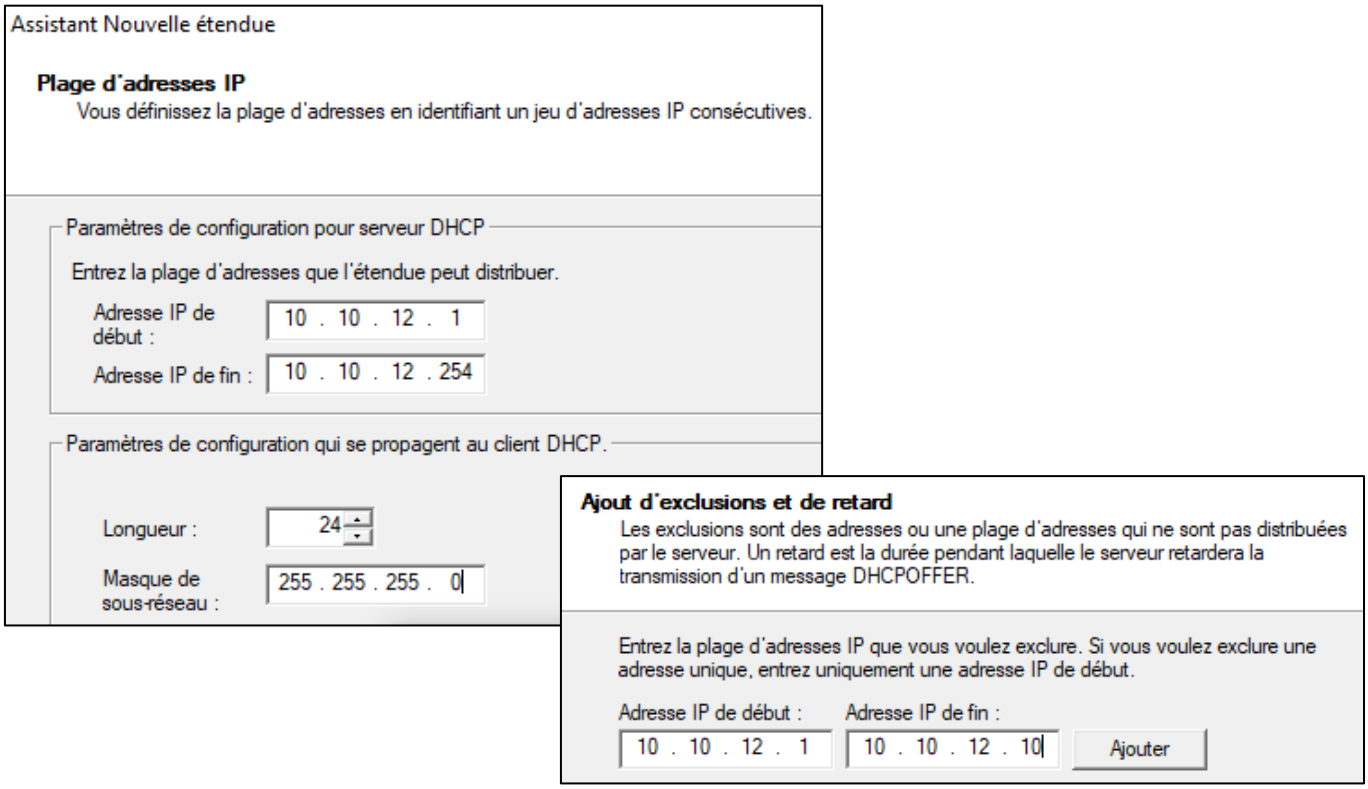



Figure 4.4-Configuration des paramètres d'adressage de serveur DHCP.

On ajoute la passerelle par défaut et l'adresse IP pour permettre l'accès à internet.

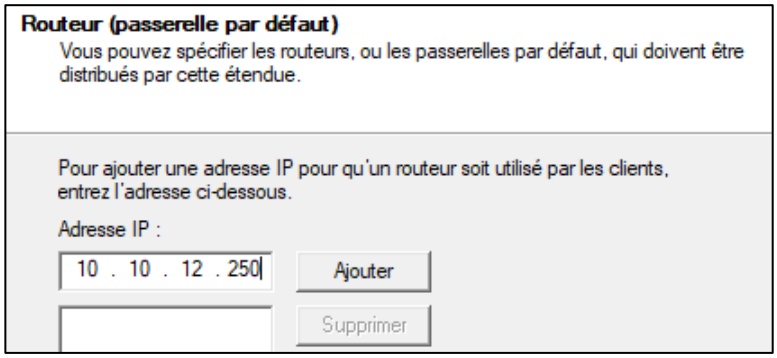



Figure 4.5-Configuration de la passerelle par défaut de serveur DHCP.

On spécifie l'adresse IP de serveur DNS (Domain Name System) et le serveur WINS (Windows Internet Naming Service) qui est un serveur de nom et de service pour les ordinateurs utilisant le NetBIOS (Network Basic d'Entrées et de Sorties Réseau)

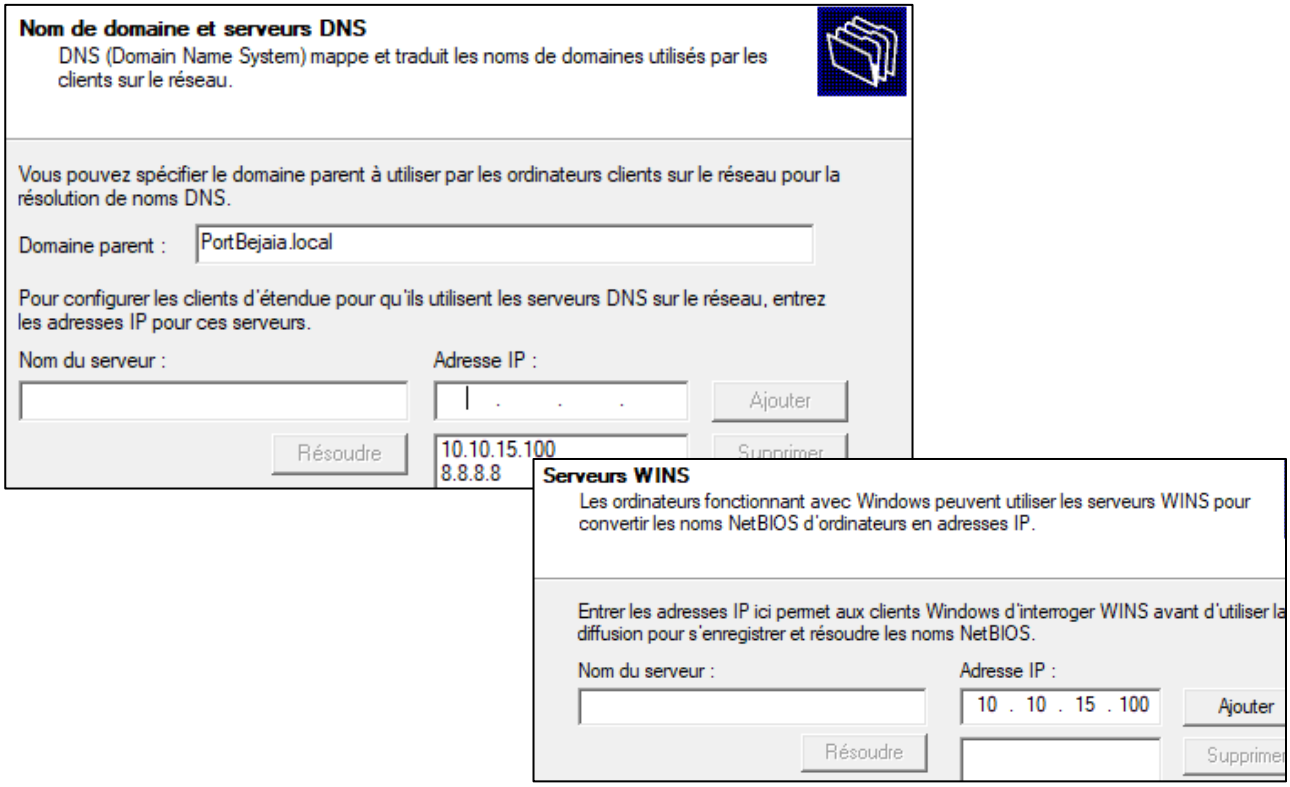



Figure 4.6-Configuration des serveur DNS et WINS.

Nous allons refaire les mêmes étapes pour créer l'entendue des autres VLAN comme indiqué sur la figure suivante :

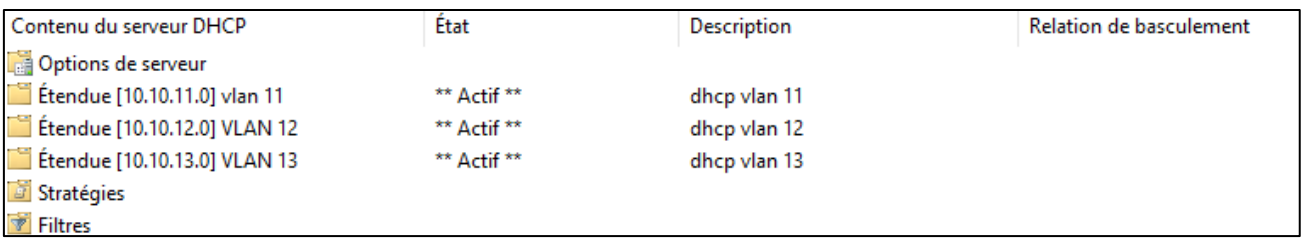



Figure 4.7-Le contenu de serveur DHCP.

### 4.6.2 Création des groupes et des clients

Sur l'annuaire Active directory, nous allons créer des groupes de clients et leurs ordinateurs, pour faciliter et organiser la gestion des utilisateurs selon les VLAN auquel ils appartiennent.

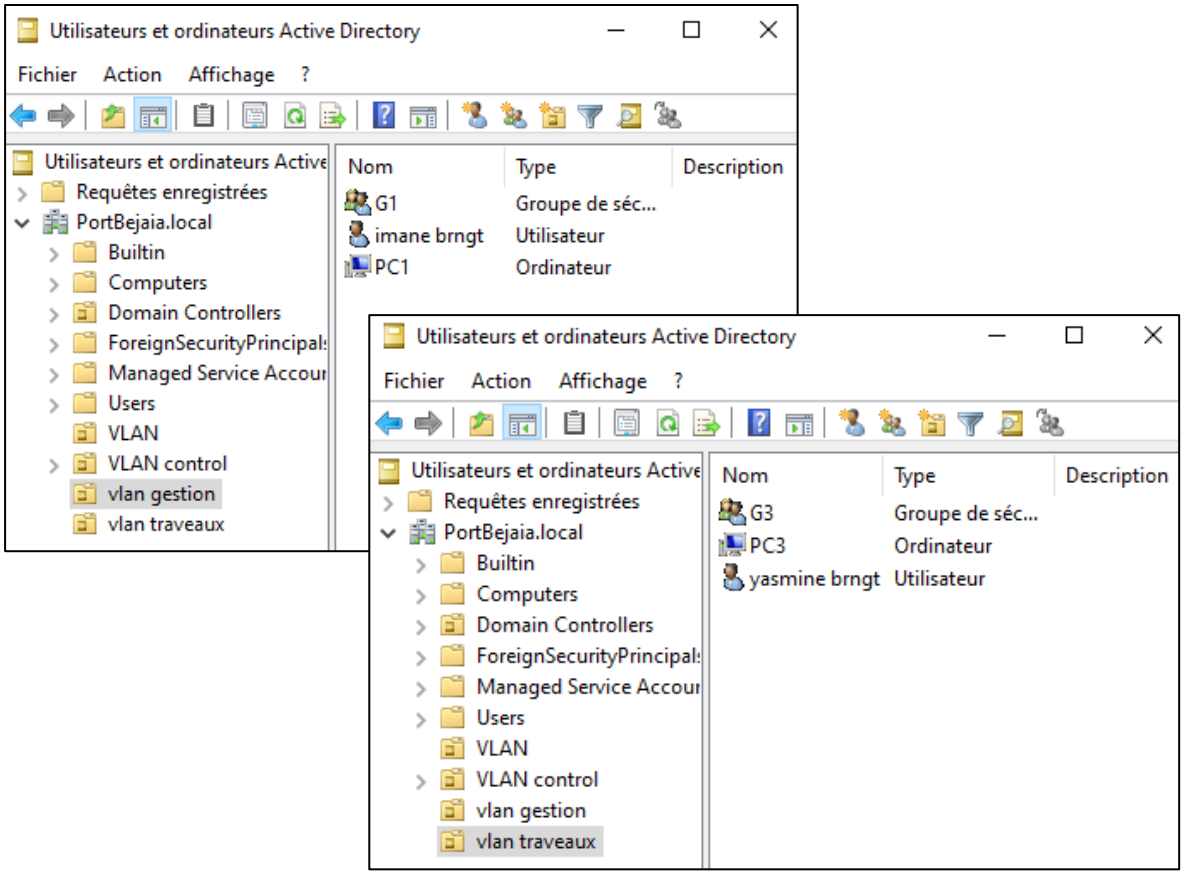



Figure 4.8-Création des groupes et des utilisateurs.

## 4.7 Configuration de Windows 10

Après l'installation de deux machines virtuelles Windows 10 « client BMT1 » et « client BMT2 », nous allons configurer la carte réseau de chaque machine selon l'emplacement de VLAN :

Client BMT 1 ➔ VLAN 11 ➔ VMnet5 ➔ 10.10.11.55

Client BMT 2 ➔ VLAN 13 ➔ VMnet4 ➔ 10.10.13.53

Par la suite, le serveur attribue une adresse aux machines virtuelles selon les adresses de VLAN configurées et il devient possible de configurer le Windows 10 pour créer des comptes utilisateur sur le domaine **PortBejaia.local** afin de se connecter à un PC réel.

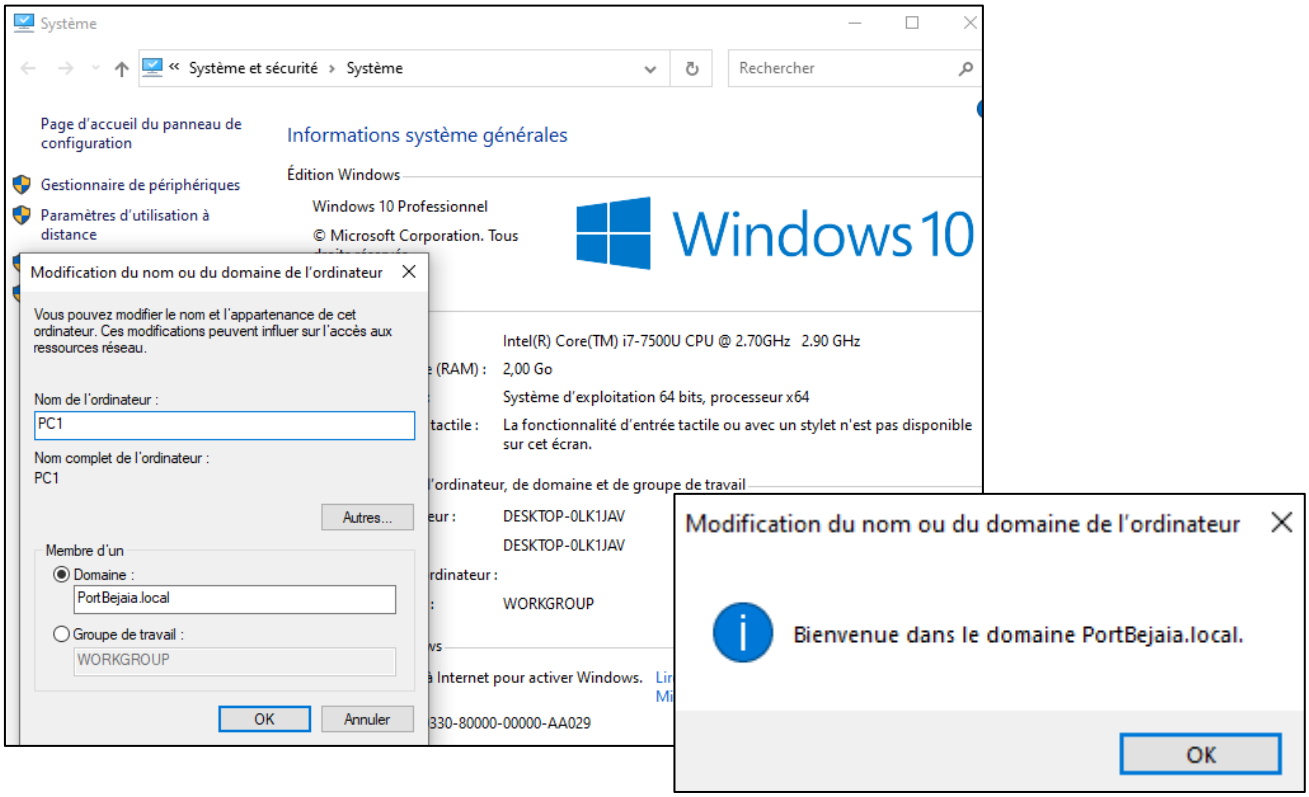



Figure 4.9-Configuration de la machine Windows.

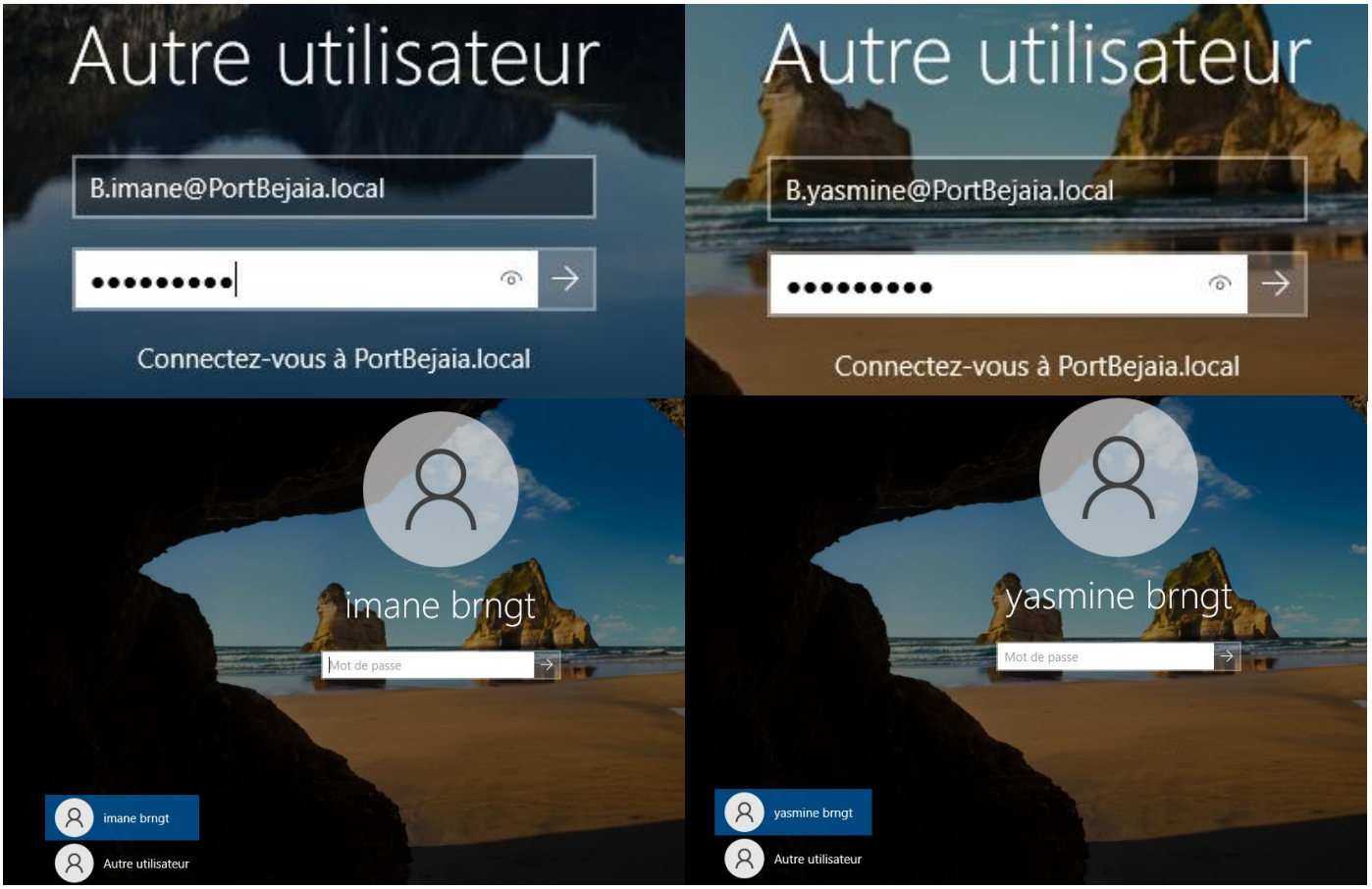



Figure 4.10-l'interface des machines clients après la configuration de Windows.

## 4.8 Configuration de Routeur FAI

Ce routeur est mis en place par Algérie Telecom pour données l'accès vers internet.

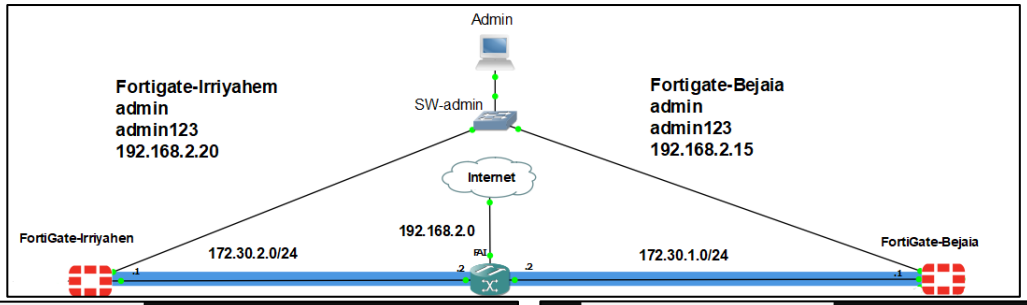
```
FAI(config-if)# interface ethernet 0/2
FAI(config-if)# no shutdown
FAI(config-if)# ip address 172.30.1.2 255.255.255.0
FAI(config-if)# interface ethernet 0/1
FAI(config-if)# no shutdown
FAI(config-if)# ip address 172.30.2.2 255.255.255.0

FAI#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            192.168.2.146   YES DHCP   up                    up
Ethernet0/1            172.30.2.2      YES NVRAM  up                    up
Ethernet0/2            172.30.1.2      YES NVRAM  up                    up
```

Listing 4.26-Configuration de Routeur FAI.

## 4.9 Configuration des pare-feu Fortigate Bejaia et Fortigate-Irriyahen

### 4.9.1 Configuration d'accès au pare-feu

Pour avoir l'accès au pare-feu, nous allons ajouter un cloud qui sera configuré autant qu'un ordinateur admin pour donner l'accès au pare-feu, ce cloud sera configuré sur l'interface VMnet8 d'adresse 192.168.2.0.




FortiGate-Bejaiia

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FG-Bejaia
FortiGate-VM64-KVM (global) # end
FG-Bejaia # config system interface
FG-Bejaia (interface) # edit port10
FG-Bejaia (port10) # set mode static
FG-Bejaia (port10) # set ip 192.168.2.15/24
FG-Bejaia (port10) # set allowaccess ping https http
```

Figure 4.11-Configuration de l'accès au Fortigate de Bejaia.

FortiGate-Iriyahen

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FG-Irriyahen
FortiGate-VM64-KVM (global) # end
FG-Irriyahen # config system interface
FG-Irriyahen (interface) # edit port10
FG-Irriyahen (port10) # set mode static
FG-Irriyahen (port10) # set ip 192.168.2.20/24
FG-Irriyahen (port10) # set allowaccess ping https http
```

Figure 4.12-Configuratin de l'accès au Fortigate d'Irriyahen.

**NB:** la commande « set allowaccess ping https http » permet l'accès au pare-feu sur tous les ports.

Nous pouvons maintenant y accéder au pare-feu grâce au navigateur « Google Chrome », on ajoute l'adresse de pare-feu, par la suite le navigateur charge la page de connexion de Fortigate et on se connecte avec admin et le mot de passe configurer ci-dessus.

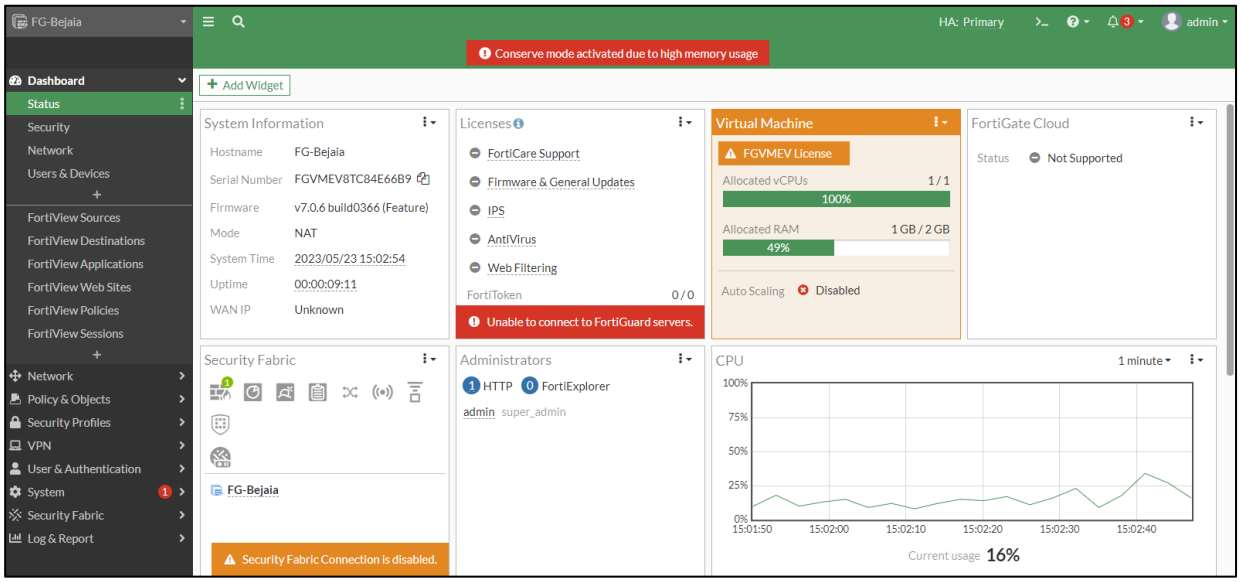



Figure 4.13-Interface d'accueil du pare-feu Fortigate.

### 4.9.2 Configuration des interfaces des pare-feu

Pour configurer les interfaces de chaque Pare-feu, nous allons suivre les étapes suivantes :


Par la suite, nous allons configurer chaque interface en lui attribuant l'Alias, le type du réseau (LAN, WAN ou DMZ), l'adresse IP de l'interface de ce réseau, et nous allons autoriser l'accès aux services essentiels pour ouvrir les ports de gestion sur l'interface.

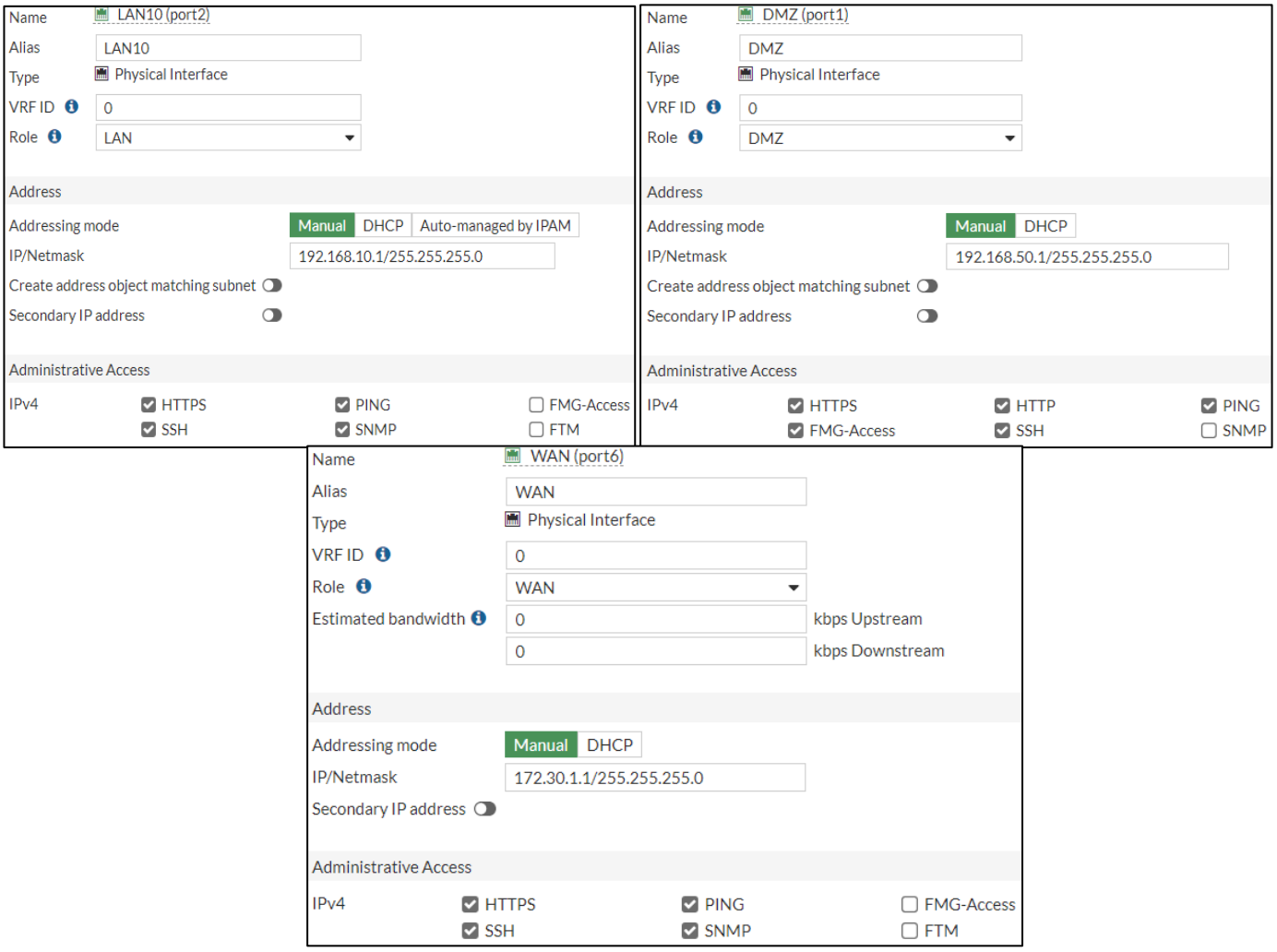



Figure 4.14-Configuration des interfaces de pare-feu.

### 4.9.3 Configuration de routage statique vers Internet

Pour permettre l'acheminement des paquets entre les différents réseaux nous allons créer une route statique par défaut au niveau des pare-feu suivant les étapes :

Fortigate → Network → static route → Create New

- FG-Bejaia

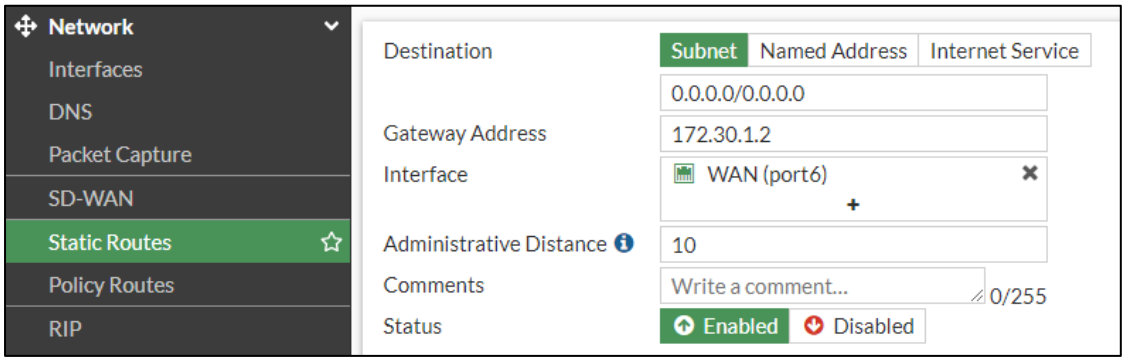



Figure 4.15-Configuration de routage statique dur FG-Bejaia.

- FG-Irriyahen

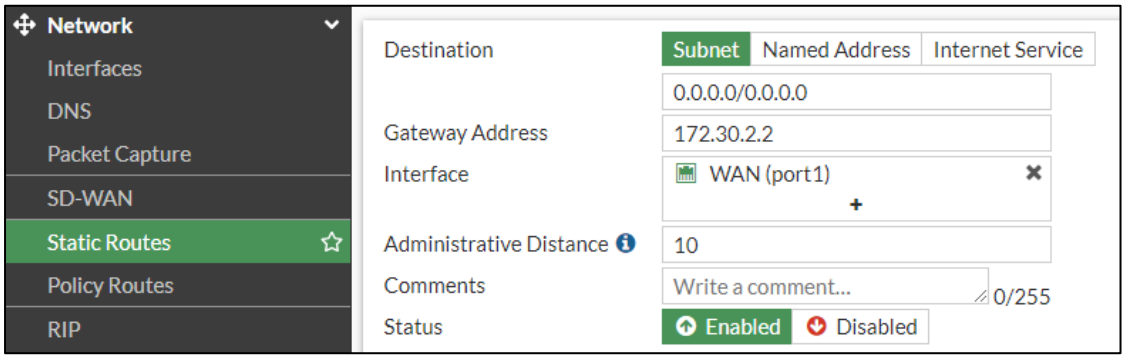



Figure 4.16-Configuration de routage statique sur FG-Irriyahen.

### 4.9.4 Création d'une liste de contrôles d'accès

Afin de contrôler l'accès des différents réseaux (LAN, WAN, DMZ) vers internet nous allons créer une liste de contrôle d'accès (ACL) qui permet de bloquer ou d'autoriser les paquets IP échangés sur les différentes interfaces selon des critères configurés dans cette liste.

La création de ACL est faite suivant ces étapes :


Après avoir créé une nouvelle Policy, nous allons ajouter le nom et spécifier l'interface d'entrée et de sortie du réseau, la destination et les services autorisés, nous avons autorisé tous les réseaux et les services.

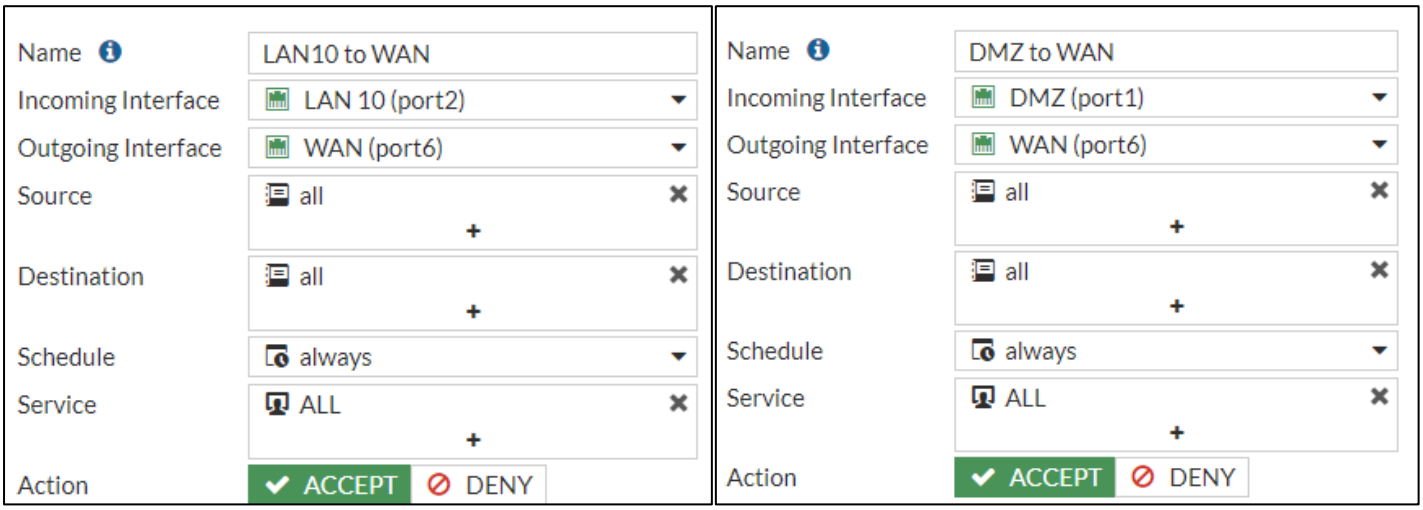



Figure 4.17-Création de la liste de contrôle d'accès sur le pare-feu.

### 4.9.5 Configuration de NAT sur le pare-feu

Parmi les avantages de Fortigate est que nous pouvons définir la politique NAT directement dans la politique de sécurité. Il suffit d'activer le NAT, le Fortigate prend en charge tout la configuration.

Il existe deux méthodes pour la configuration de NAT sur Fortigate

1. Utilisé une seule adresse IP publique pour l'ensemble des machines, c'est la méthode que nous allons utiliser pour configurer le NAT sur nos réseau LAN et DMZ, il suffit d'activer le NAT pour les Policy configurés et choisir « Use Outgoing Interface Address ».

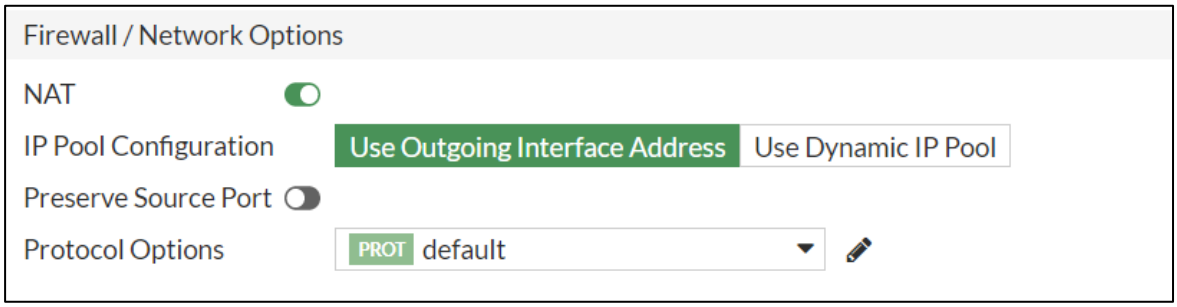



Figure 4.18-Activation du NAT sur Fortigate.

2. La deuxième méthode consiste à créer une Pool d'adresse, il faut choisir « Use Dynamics IP Pool » et créer une nouvelle plage pour le IP Pool.

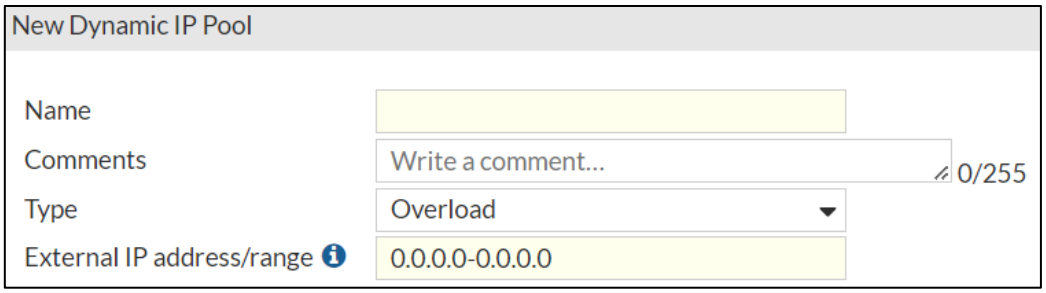



Figure 4.19-Illustration de la fenêtre Dynamic IP Pool.

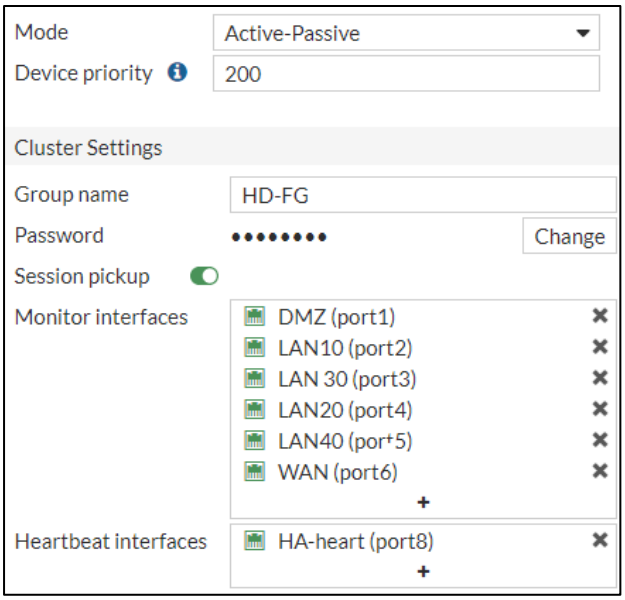
### 4.9.6 Configuration de la haute disponibilité

Dans le but de garder le bon fonctionnement de nos réseaux, nous allons configurer la haute disponibilité (en anglais High Availability (HA) sur deux pare-feu. En cas d'une panne du pare-feu principal, le secondaire prendra le relais et fonctionnera jusqu'à ce que le principal soit traité.

Cette HA sera configurée en mode active-passive sur les deux pare-feu « FG-Bejaia » et « FG-Bejaia-2 », le premier agira en tant que maître il aura donc une propriété de périphérique élevée et le deuxième en tant qu'esclave, nous allons créer le groupe de HA avec un mot de passe et on spécifier les interfaces que le pare-feu esclave doit prend en charge ainsi que l'interface Heatbeat qui relie les deux pare-feu.

❖ Configuration de FG-Bejaia

FG-Bejaia → System → HA




❖ Configuration de FG-Bejaia-2

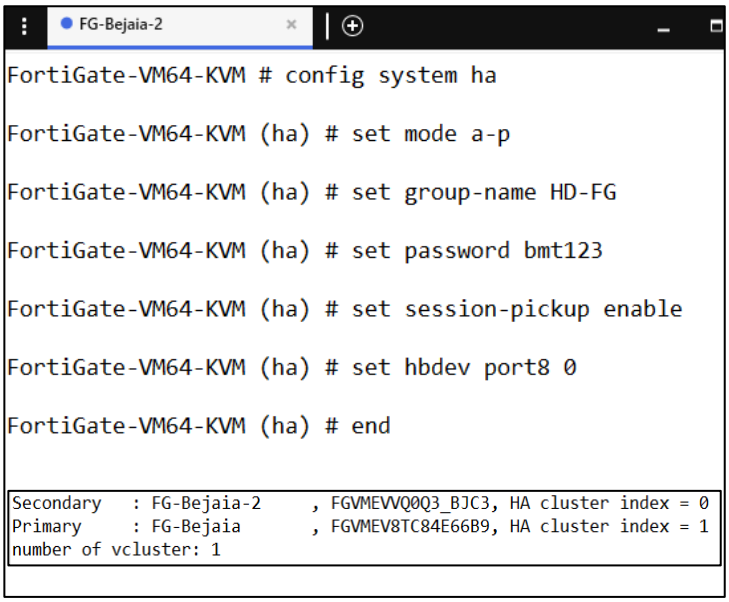



Figure 4.20-Configuration de la haute disponibilité sur les FG Bejaia /2.

Le résultat de la synchronisation des deux pare-feu est illustré par la figure ci-dessous

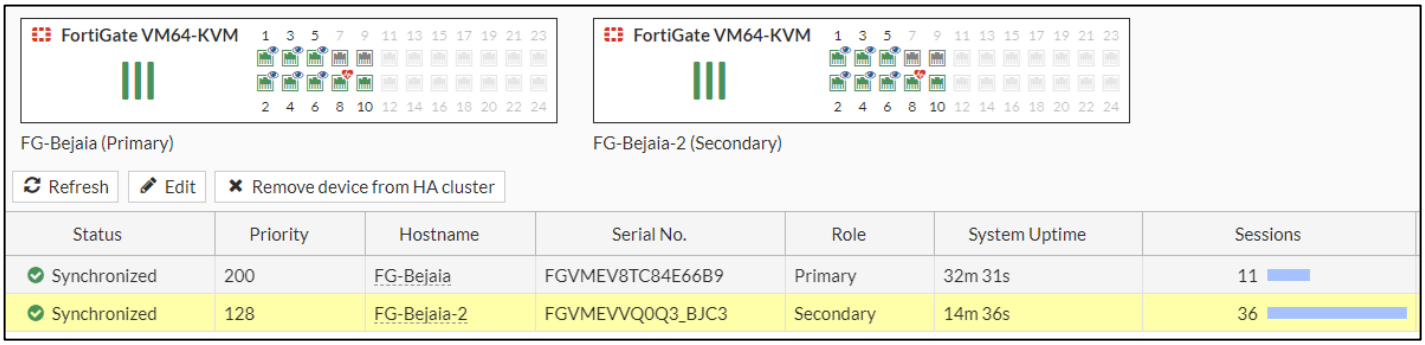



Figure 4.21-Synchronisation des pare-feu FG-Bejaia/2.

## 4.10 Configuration de VPN site a site

Dans cette partie, nous allons expliquer la création d'un tunnel VPN site à site sur nos pare-feu tels que :

- VPN (Bejaia-Irriyahen) sur FG-Bejaia de site Port Bejaia.
- VPN (Irriyahen-Bejaia) sur FG-Irriyahen de site Irriyahen.

### 4.10.1 Au niveau de Fortigate Bejaia

Pour la création d'un nouveau tunnel, nous allons suivre les étapes suivantes :

FG-Bejaia → VPN → IPsec Tunnels → Create New → IPsec Tunnel

Par la suite, nous allons configurer notre VPN tunnel. Les différentes étapes sont expliquées ci-dessous :

- Nous commençons par attribuer le nom de VPN et spécifier sont type ainsi que le type de périphérique distant avec lequel se VPN sera créer.

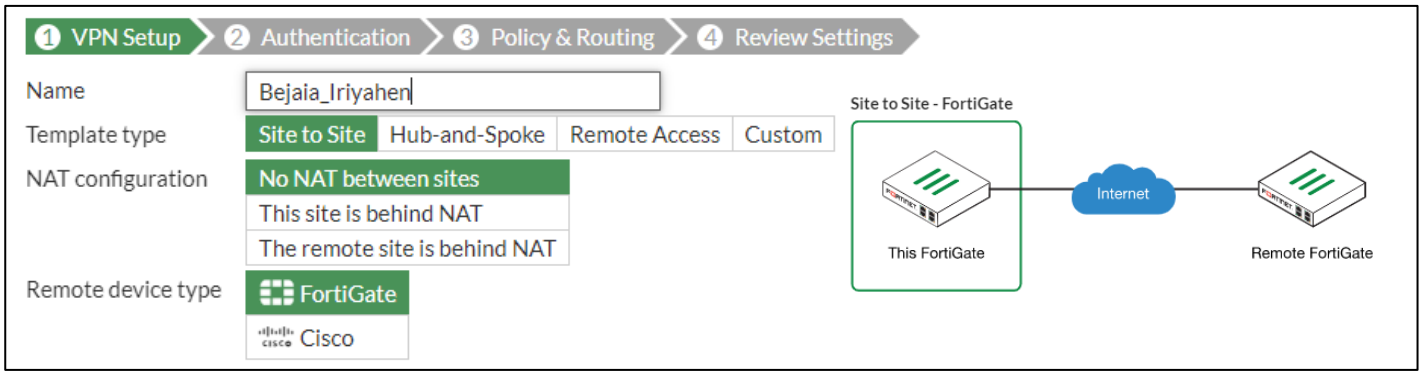



Figure 4.22-Création de VPN IPsec Bejaia-Irriyahen.

- Par la suite nous allons définir l'adresse de l'interface WAN de pare-feu, l'assistant attribue automatiquement le port de l'interface sortante, nous définissons aussi la clé pré-partagée sécurisée (PSK) sur le tunnel entre les deux sites.


Figure 4.23-Authentification de VPN Bejaia-Irriyahen.

- Sur ce qui suit nous allons sélectionner les réseaux locaux LAN et les réseaux distants pour donner l'accès à distance, nous allons autoriser uniquement le réseau CTMS à circuler dans le tunnel.

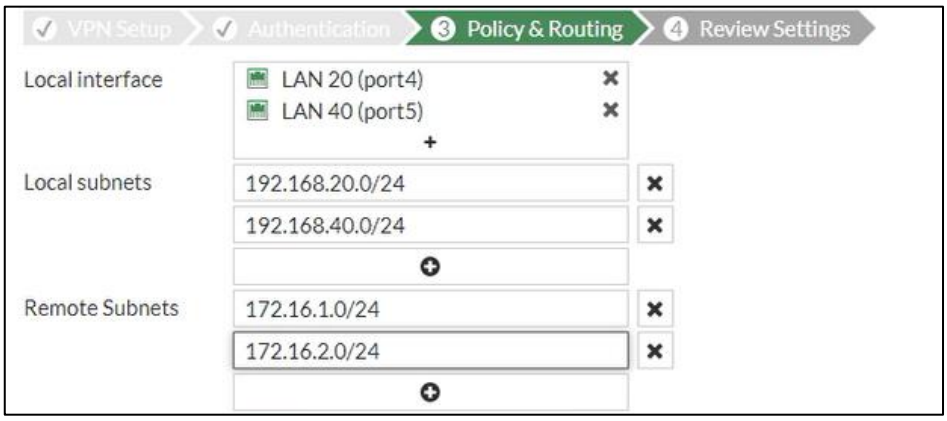



Figure 4.24-Les interfaces de Policy et de routage sur le VPN Béjaia-Irriyahen.

Une page récapitulative sera affichée à la fin de la configuration pour finaliser la création du tunnel.

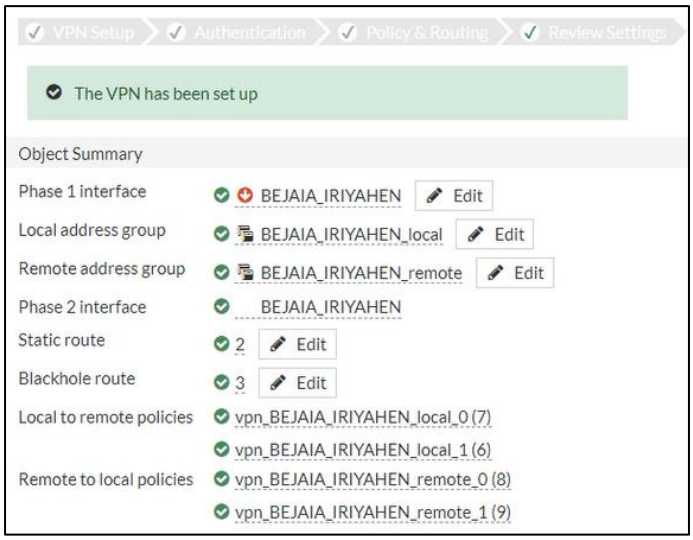



Figure 4.25-Finalisation de la création de VPN Bejaia-Irriyahen.

- La négociation et partage des clés : pour assurer la négociation et la gestion de la clé utilisée entre les deux pare-feu, IPsec utilise le protocole IKE (Internet Key Exchange) basé sur ISAKMP (Internet Security Association and Key Management Protocole) pour établir une connexion sécurisée entre les deux extrémités du tunnel.

  La configuration doit être identique dans les deux extrémités, la négociation est faite en deux phases :

  - **Phase 1 :** pour crypter les données nous allons utiliser l'algorithme de chiffrement DES**)** qui est un algorithme de chiffrement symétrique basé sur le chiffrement par bloc en utilisant des clés de 56 bits et on définit le SHA256 comme méthode d'authentification de message haché, par la suite un groupe de Diffie-Hellman 5 sera défini ce qui permet de crypter 1024 bits.
  - **Phase 2 :** cette phase permet de définir les algorithmes de chiffrement et d'authentification à utiliser pour le reste de la session.

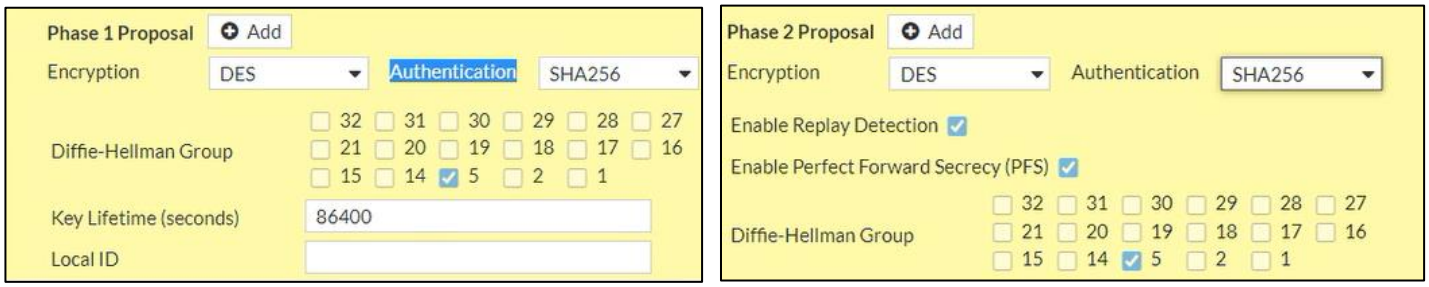



Figure 4.26-La modification des paramètres de cryptage de VPN Bejaia-Irriyahen.

### 4.10.2 Au niveau de Fortigate Irriyahen

Selon les mêmes règles, nous allons configurer le VPN Irriyahen-Bejaia sur le FG-Irriyahen :

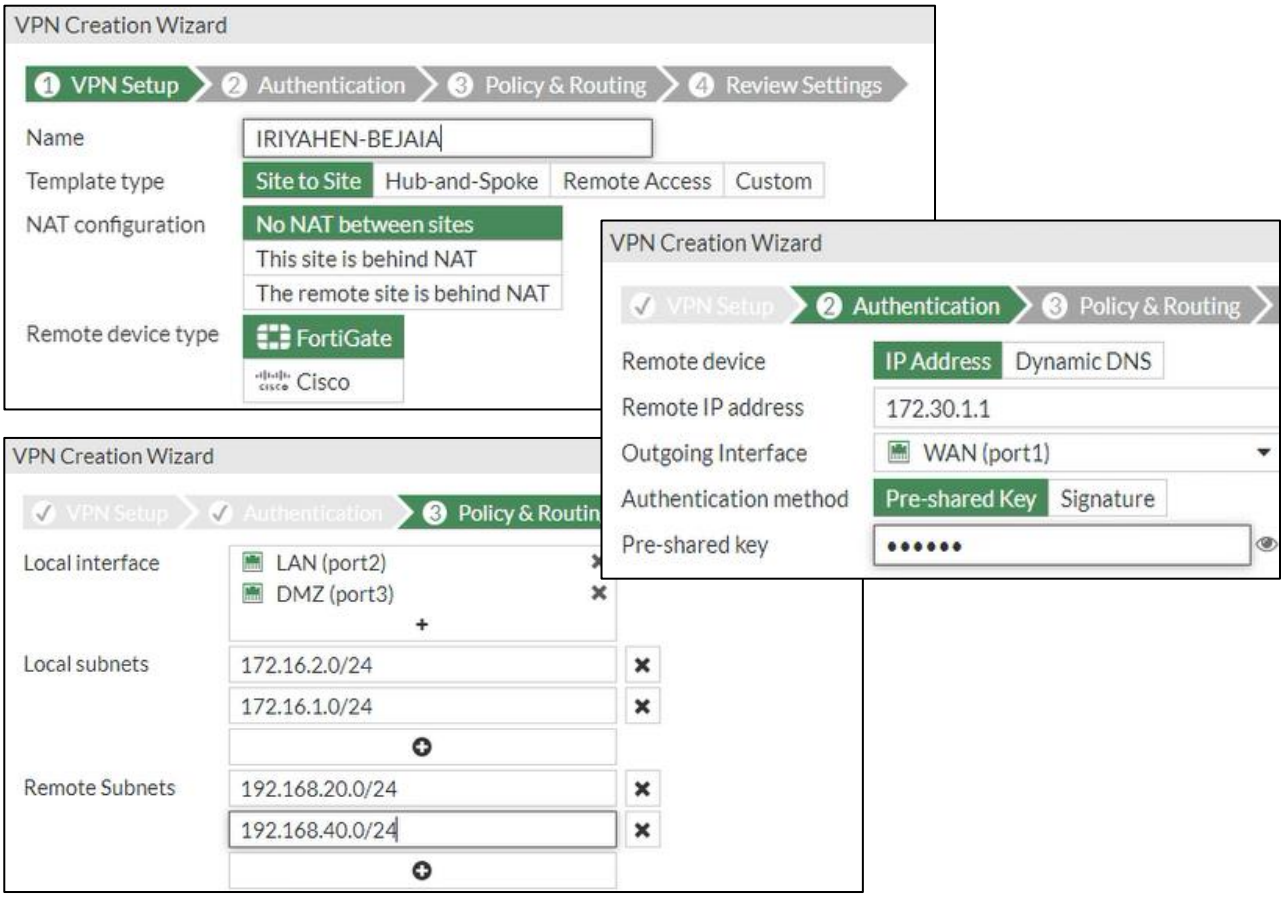



Figure 4.27-Création de VPN IPsec Irriyahen-Bejaia.

Les paramètres d'authentification et de négociation des clés seront configurés de la même manière pour les deux VPN.

⇨ **Résultat**

La configuration d'un tunnel VPN mène à la création de :

- Une route statique à l'intérieur du tunnel sur chaque pare-feu

FG-Bejaia

| Destination | Gateway IP | Interface | Status | Comments |
|---|---|---|---|---|
| 0.0.0.0/0 | 172.30.1.2 | WAN (port6) | Enabled | |
| BEJAIA_IRIYAHEN_remote | 172.30.2.1 | BEJAIA_IRIYAHEN | Enabled | VPN: BEJAIA_IRIYAHEN (Created by VPN wizard) |
| BEJAIA_IRIYAHEN_remote | | Blackhole | Enabled | VPN: BEJAIA_IRIYAHEN (Created by VPN wizard) |

FG-Irriyahen

| Destination | Gateway IP | Interface | Status | Comments |
|---|---|---|---|---|
| 0.0.0.0/0 | 172.30.2.2 | WAN (port1) | Enabled | |
| IRIYAHEN-BEJAIA_remote | 172.30.1.1 | IRIYAHEN-BEJAIA | Enabled | VPN: IRIYAHEN-BEJAIA (Created by VPN wizard) |
| IRIYAHEN-BEJAIA_remote | | Blackhole | Enabled | VPN: IRIYAHEN-BEJAIA (Created by VPN wizard) |

Figure 4.28-Routes statiques créées par les VPN configurés.

- Des adresses locales et distantes

FG-Bejaia

| Name | Details |
|---|---|
| BEJAIA_IRIYAHEN_local_subnet_1 | 192.168.20.0/24 |
| BEJAIA_IRIYAHEN_local_subnet_2 | 192.168.40.0/24 |
| BEJAIA_IRIYAHEN_remote_subnet_1 | 172.16.2.0/24 |
| BEJAIA_IRIYAHEN_remote_subnet_2 | 172.16.1.0/24 |

FG-Irriyahen

| Name | Details |
|---|---|
| IRIYAHEN_BEJAIA_local_subnet_1 | 172.16.2.0/24 |
| IRIYAHEN_BEJAIA_local_subnet_2 | 172.16.1.0/24 |
| IRIYAHEN_BEJAIA_remote_subnet_1 | 192.168.20.0/24 |
| IRIYAHEN_BEJAIA_remote_subnet_2 | 192.168.40.0/24 |

Figure 4.29-Adresses locales et distantes créées par les VPN configurés.

- Deux types de Policy entrant et sortant sur chaque pare-feu

FG-Beiaia

| Name | Source | Destination | Schedule | Service | Action |
|---|---|---|---|---|---|
| BEJAIA_IRIYAHEN → LAN 20 (port4) 1 | | | | | |
| BEJAIA_IRIYAHEN → LAN 40 (port5) 1 | | | | | |
| DMZ (port1) → WAN (port6) 1 | | | | | |
| LAN 10 (port2) → WAN (port6) 1 | | | | | |
| LAN 20 (port4) → BEJAIA_IRIYAHEN 1 | | | | | |
| LAN 20 (port4) → WAN (port6) 1 | | | | | |
| LAN 30 (port3) → WAN (port6) 1 | | | | | |
| LAN 40 (port5) → BEJAIA_IRIYAHEN 1 | | | | | |

FG-Irriyahen

| Name | Source | Destination | Schedule | Service | Action |
|---|---|---|---|---|---|
| DMZ (port3) → IRIYAHEN-BEJAIA 1 | | | | | |
| DMZ (port3) → WAN (port1) 1 | | | | | |
| IRIYAHEN-BEJAIA → DMZ (port3) 1 | | | | | |
| IRIYAHEN-BEJAIA → LAN (port2) 1 | | | | | |
| LAN (port2) → IRIYAHEN-BEJAIA 1 | | | | | |

Figure 4.30-Listes de contrôles d'accès créées par les VPN configurés.

### 4.10.3 Etablissement du tunnel VPN

Pour établir le tunnel VPN entre les de sites, nous allons activer les deux phases authentification et de négociation.

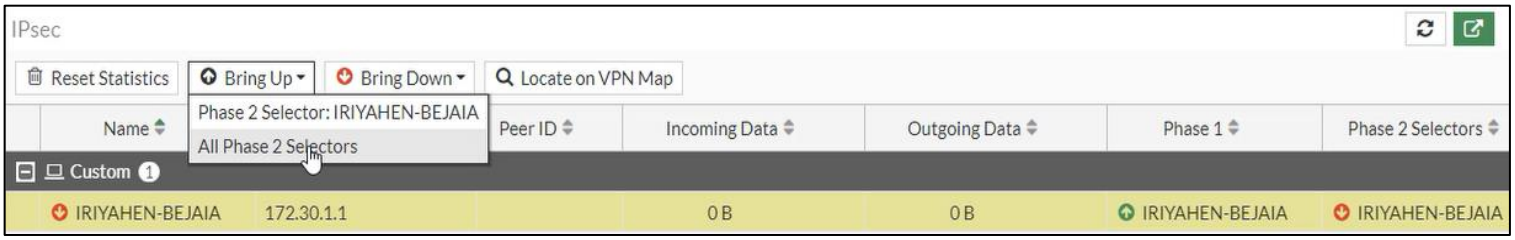



Figure 4.31-Etablissement de tunnel VPN site à site.

## 4.11 Test et vérification

### 4.11.1 Vérification de la configuration

- Vérification de protocole LACP

SWD1

```
SWD1#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
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Et3/1(P)    Et3/2(P)    Et3/3(P)
```

SWD2

```
SWD2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Et3/1(P)    Et3/2(P)    Et3/3(P)
```

Figure 4.32-Vérification de la configuration du protocole LACP.

- Vérification de protocole PAGP

SWD1-ctms

```
SWD1ctms#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Et3/1(P)    Et3/2(P)    Et3/3(P)
```

SWD2-ctms

```
SWD2ctms#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG

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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Et3/1(P)    Et3/2(P)    Et3/3(P)
```

Figure 4.33-Vérification de la configuration du protocole PAGP.

❖ Vérification de protocole HSRP

Core1

```
core1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.10    10   150 P Active  local           172.16.10.2     172.16.10.254
Et0/0.20    20   150 P Active  local           172.16.20.2     172.16.20.254
Et0/0.30    30   150 P Active  local           172.16.30.2     172.16.30.254
Et0/0.40    40   150 P Active  local           172.16.40.2     172.16.40.254
Et0/0.50    50   150 P Active  local           172.16.50.2     172.16.50.254
Et0/0.60    60   150 P Active  local           172.16.60.2     172.16.60.254
Et0/0.70    70   150   Active  local           172.16.70.2     172.16.70.254
Et0/0.80    80   150 P Active  local           172.16.80.2     172.16.80.254
```

Core2

```
core2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.10    10   100   Standby 172.16.10.1     local           172.16.10.254
Et0/0.20    20   100   Standby 172.16.20.1     local           172.16.20.254
Et0/0.30    30   100   Standby 172.16.30.1     local           172.16.30.254
Et0/0.40    40   100   Standby 172.16.40.1     local           172.16.40.254
Et0/0.50    50   100   Standby 172.16.50.1     local           172.16.50.254
Et0/0.60    60   100   Standby 172.16.60.1     local           172.16.60.254
Et0/0.70    70   100   Standby 172.16.70.1     local           172.16.70.254
Et0/0.80    80   100   Standby 172.16.80.1     local           172.16.80.254
```

Figure 4.34-Vérification de la configuration de protocole HSRP.

Nous allons éteindre le routeur actif (Core1) pour voir le comportement de routeurs standby (Core2), ce dernier passe de mode standby au mode active et prend la relave pour continuer le fonctionnement de réseau.

Core2 Core1

```
*May 22 17:06:46.544: %HSRP-5-STATECHANGE: Ethernet0/0.50 Grp 50 state Standby -> Active
*May 22 17:06:47.133: %HSRP-5-STATECHANGE: Ethernet0/0.80 Grp 80 state Standby -> Active
*May 22 17:06:47.195: %HSRP-5-STATECHANGE: Ethernet0/0.20 Grp 20 state Standby -> Active
*May 22 17:06:48.249: %HSRP-5-STATECHANGE: Ethernet0/0.30 Grp 30 state Standby -> Active
*May 22 17:06:49.075: %HSRP-5-STATECHANGE: Ethernet0/0.10 Grp 10 state Standby -> Active
*May 22 17:06:49.445: %HSRP-5-STATECHANGE: Ethernet0/0.70 Grp 70 state Standby -> Active
*May 22 17:06:49.958: %HSRP-5-STATECHANGE: Ethernet0/0.40 Grp 40 state Standby -> Active
*May 22 17:07:01.400: %HSRP-5-STATECHANGE: Ethernet0/0.60 Grp 60 state Standby -> Active
```

Figure 4.35-Vérification de fonctionnement de routeur Standby du réseau LAN.

❖ Vérification de protocole GLBP

Core1-ctms

```
core1ctms#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Et0/0.11    11   -   150 Active   10.10.11.250    local           10.10.11.2
Et0/0.11    11   1   -   Active   0007.b400.0b01  local           -
Et0/0.11    11   2   -   Listen   0007.b400.0b02  10.10.11.2      -
Et0/0.12    12   -   150 Active   10.10.12.250    local           10.10.12.2
Et0/0.12    12   1   -   Active   0007.b400.0c01  local           -
Et0/0.12    12   2   -   Listen   0007.b400.0c02  10.10.12.2      -
Et0/0.13    13   -   150 Active   10.10.13.250    local           10.10.13.2
Et0/0.13    13   1   -   Active   0007.b400.0d01  local           -
Et0/0.13    13   2   -   Listen   0007.b400.0d02  10.10.13.2      -
Et0/0.14    14   -   150 Active   10.10.14.250    local           10.10.14.2
Et0/0.14    14   1   -   Active   0007.b400.0e01  local           -
Et0/0.14    14   2   -   Listen   0007.b400.0e02  10.10.14.2      -
Et0/0.15    15   -   150 Active   10.10.15.250    local           10.10.15.2
Et0/0.15    15   1   -   Active   0007.b400.0f01  local           -
Et0/0.15    15   2   -   Listen   0007.b400.0f02  10.10.15.2      -
```

Core2-ctms

```
Core2ctms#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Et0/0.11    11   -   100 Standby  10.10.11.250    10.10.11.1      local
Et0/0.11    11   1   -   Listen   0007.b400.0b01  10.10.11.1      -
Et0/0.11    11   2   -   Active   0007.b400.0b02  local           -
Et0/0.12    12   -   100 Standby  10.10.12.250    10.10.12.1      local
Et0/0.12    12   1   -   Listen   0007.b400.0c01  10.10.12.1      -
Et0/0.12    12   2   -   Active   0007.b400.0c02  local           -
Et0/0.13    13   -   100 Standby  10.10.13.250    10.10.13.1      local
Et0/0.13    13   1   -   Listen   0007.b400.0d01  10.10.13.1      -
Et0/0.13    13   2   -   Active   0007.b400.0d02  local           -
Et0/0.14    14   -   100 Standby  10.10.14.250    10.10.14.1      local
Et0/0.14    14   1   -   Listen   0007.b400.0e01  10.10.14.1      -
Et0/0.14    14   2   -   Active   0007.b400.0e02  local           -
Et0/0.15    15   -   100 Standby  10.10.15.250    10.10.15.1      local
Et0/0.15    15   1   -   Listen   0007.b400.0f01  10.10.15.1      -
Et0/0.15    15   2   -   Active   0007.b400.0f02  local           -
```

Figure 4.36-Vérification de la configuration du protocole GLBP.

Nous allons éteindre le Routeur 1 de réseau CTMS (Core1-CTMS) pour voir le comportement de routeur 2 (Core2-CTMS)

Core2-ctms | Core1-ctms

```
*May 24 12:25:13.742: %GLBP-6-STATECHANGE: Ethernet0/0.15 Grp 15 state Standby -> Active
*May 24 12:25:14.724: %GLBP-6-FWDSTATECHANGE: Ethernet0/0.15 Grp 15 Fwd 2 state Listen -> Active
*May 24 12:25:15.401: %GLBP-6-FWDSTATECHANGE: Ethernet0/0.12 Grp 12 Fwd 2 state Listen -> Active
*May 24 12:25:15.477: %GLBP-6-STATECHANGE: Ethernet0/0.13 Grp 13 state Standby -> Active
*May 24 12:25:15.668: %GLBP-6-FWDSTATECHANGE: Ethernet0/0.13 Grp 13 Fwd 2 state Listen -> Active
*May 24 12:25:15.743: %GLBP-6-STATECHANGE: Ethernet0/0.14 Grp 14 state Standby -> Active
*May 24 12:25:15.891: %GLBP-6-FWDSTATECHANGE: Ethernet0/0.11 Grp 11 Fwd 2 state Listen -> Active
*May 24 12:25:15.995: %GLBP-6-STATECHANGE: Ethernet0/0.11 Grp 11 state Standby -> Active
*May 24 12:25:16.409: %GLBP-6-FWDSTATECHANGE: Ethernet0/0.14 Grp 14 Fwd 2 state Listen -> Active
*May 24 12:25:16.521: %GLBP-6-STATECHANGE: Ethernet0/0.12 Grp 12 state Standby -> Active
```

Figure 4.37-Vérification de fonctionnement de routeur standby du réseau CTMS.

❖ Vérification de routage statique par défaut du réseau LAN

Core1

```
core1#show ip route
Gateway of last resort is 192.168.30.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.30.1
      172.16.0.0/16 is variably subnetted, 16 subnets, 2 masks
C        172.16.10.0/24 is directly connected, Ethernet0/0.10
L        172.16.10.1/32 is directly connected, Ethernet0/0.10
C        172.16.20.0/24 is directly connected, Ethernet0/0.20
L        172.16.20.1/32 is directly connected, Ethernet0/0.20
C        172.16.30.0/24 is directly connected, Ethernet0/0.30
L        172.16.30.1/32 is directly connected, Ethernet0/0.30
C        172.16.40.0/24 is directly connected, Ethernet0/0.40
L        172.16.40.1/32 is directly connected, Ethernet0/0.40
C        172.16.50.0/24 is directly connected, Ethernet0/0.50
L        172.16.50.1/32 is directly connected, Ethernet0/0.50
C        172.16.60.0/24 is directly connected, Ethernet0/0.60
L        172.16.60.1/32 is directly connected, Ethernet0/0.60
C        172.16.70.0/24 is directly connected, Ethernet0/0.70
L        172.16.70.1/32 is directly connected, Ethernet0/0.70
C        172.16.80.0/24 is directly connected, Ethernet0/0.80
L        172.16.80.1/32 is directly connected, Ethernet0/0.80
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Ethernet0/1
L        192.168.30.2/32 is directly connected, Ethernet0/1
```

Core2

```
core2#show ip route
Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      172.16.0.0/16 is variably subnetted, 16 subnets, 2 masks
C        172.16.10.0/24 is directly connected, Ethernet0/0.10
L        172.16.10.2/32 is directly connected, Ethernet0/0.10
C        172.16.20.0/24 is directly connected, Ethernet0/0.20
L        172.16.20.2/32 is directly connected, Ethernet0/0.20
C        172.16.30.0/24 is directly connected, Ethernet0/0.30
L        172.16.30.2/32 is directly connected, Ethernet0/0.30
C        172.16.40.0/24 is directly connected, Ethernet0/0.40
L        172.16.40.2/32 is directly connected, Ethernet0/0.40
C        172.16.50.0/24 is directly connected, Ethernet0/0.50
L        172.16.50.2/32 is directly connected, Ethernet0/0.50
C        172.16.60.0/24 is directly connected, Ethernet0/0.60
L        172.16.60.2/32 is directly connected, Ethernet0/0.60
C        172.16.70.0/24 is directly connected, Ethernet0/0.70
L        172.16.70.2/32 is directly connected, Ethernet0/0.70
C        172.16.80.0/24 is directly connected, Ethernet0/0.80
L        172.16.80.2/32 is directly connected, Ethernet0/0.80
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Ethernet0/1
L        192.168.10.2/32 is directly connected, Ethernet0/1
```

Figure 4.38-Vérification de routage sur le réseau LAN.

❖ Vérification de routage statique par défaut du réseau CTMS

Core1-ctms

```
core1ctms#show ip route
Gateway of last resort is 192.168.40.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.40.1
      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C        10.10.11.0/24 is directly connected, Ethernet0/0.11
L        10.10.11.1/32 is directly connected, Ethernet0/0.11
C        10.10.12.0/24 is directly connected, Ethernet0/0.12
L        10.10.12.1/32 is directly connected, Ethernet0/0.12
C        10.10.13.0/24 is directly connected, Ethernet0/0.13
L        10.10.13.1/32 is directly connected, Ethernet0/0.13
C        10.10.14.0/24 is directly connected, Ethernet0/0.14
L        10.10.14.1/32 is directly connected, Ethernet0/0.14
C        10.10.15.0/24 is directly connected, Ethernet0/0.15
L        10.10.15.1/32 is directly connected, Ethernet0/0.15
      192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.40.0/24 is directly connected, Ethernet0/1
L        192.168.40.2/32 is directly connected, Ethernet0/1
```

Core2-ctms

```
Core2ctms#show ip route
Gateway of last resort is 192.168.20.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.20.1
      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C        10.10.11.0/24 is directly connected, Ethernet0/0.11
L        10.10.11.2/32 is directly connected, Ethernet0/0.11
C        10.10.12.0/24 is directly connected, Ethernet0/0.12
L        10.10.12.2/32 is directly connected, Ethernet0/0.12
C        10.10.13.0/24 is directly connected, Ethernet0/0.13
L        10.10.13.2/32 is directly connected, Ethernet0/0.13
C        10.10.14.0/24 is directly connected, Ethernet0/0.14
L        10.10.14.2/32 is directly connected, Ethernet0/0.14
C        10.10.15.0/24 is directly connected, Ethernet0/0.15
L        10.10.15.2/32 is directly connected, Ethernet0/0.15
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Ethernet0/1
L        192.168.20.2/32 is directly connected, Ethernet0/1
```

Figure 4.39-Vérification de routage sur le réseau CTMS.

❖ Vérification de la connectivité des machines utilisateurs au serveur DHCP

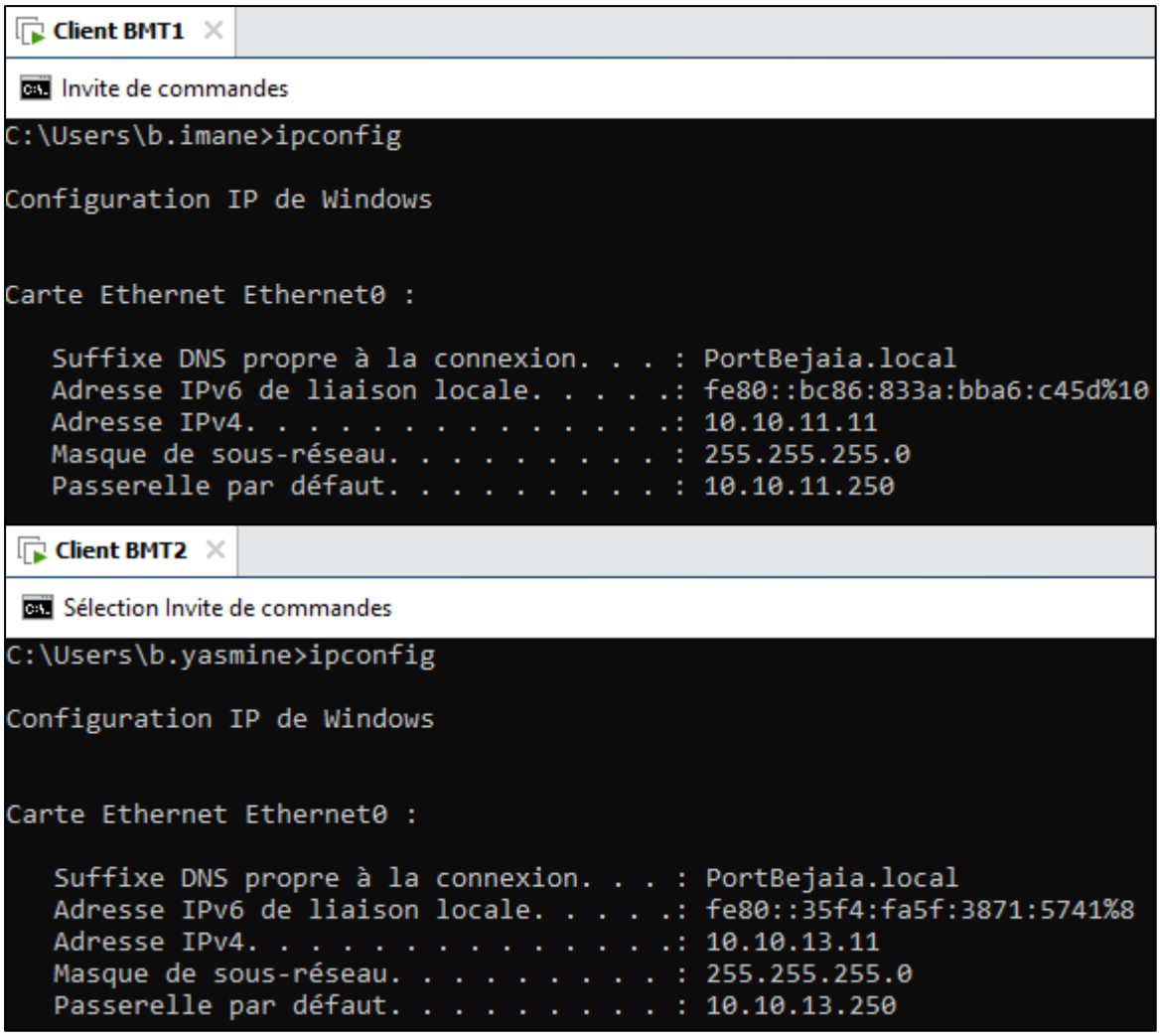



Figure 4.40-Vérification de la connectivité des machines Windows au serveur DHCP.

### 4.11.2 Test de routage inter VLAN du réseau LAN

❖ Test de protocole DHCP : l'attribution dynamique des adresses IP est réussie.


Figure 4.41-Attribution des adresses IP par le protocole DHCP.

❖ Test de routage inter VLAN du réseau LAN Bejaia

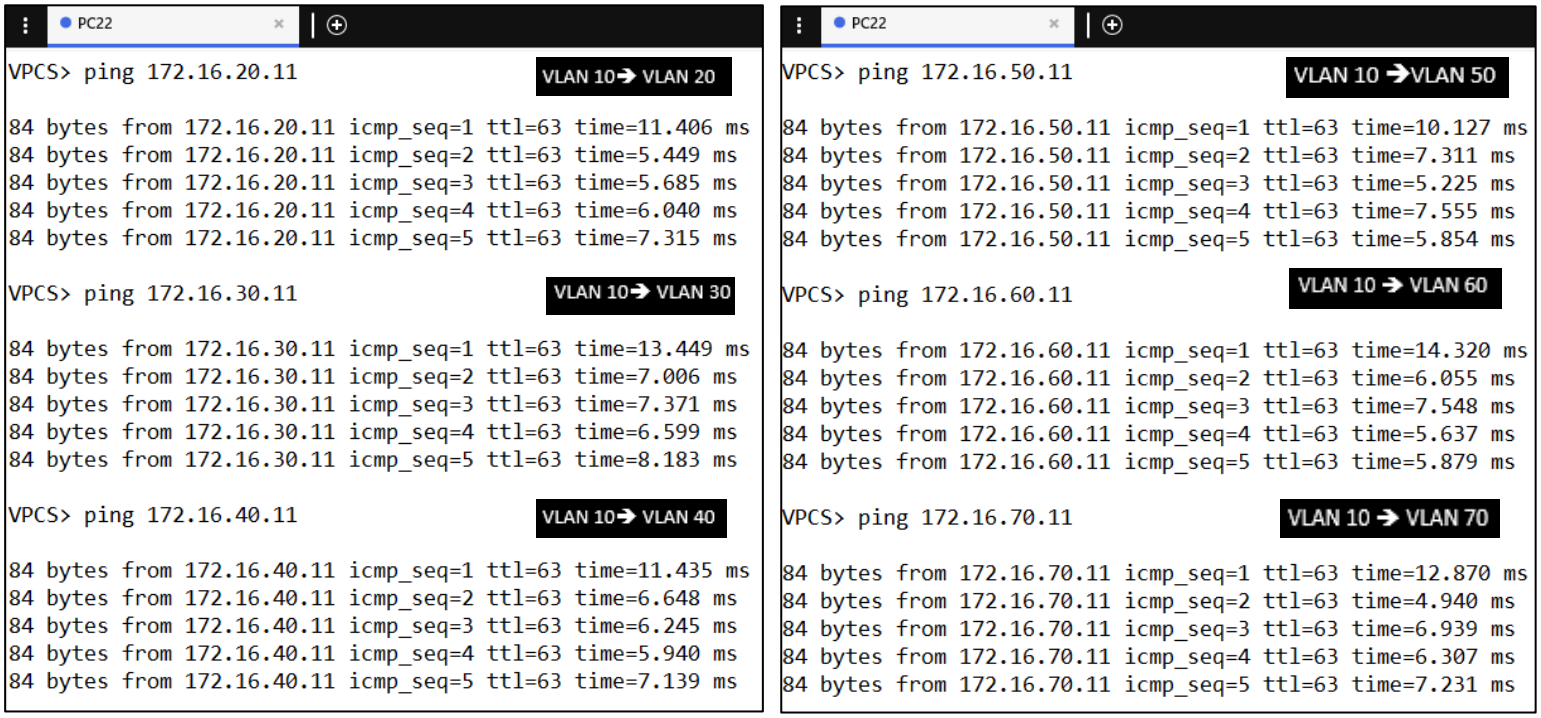
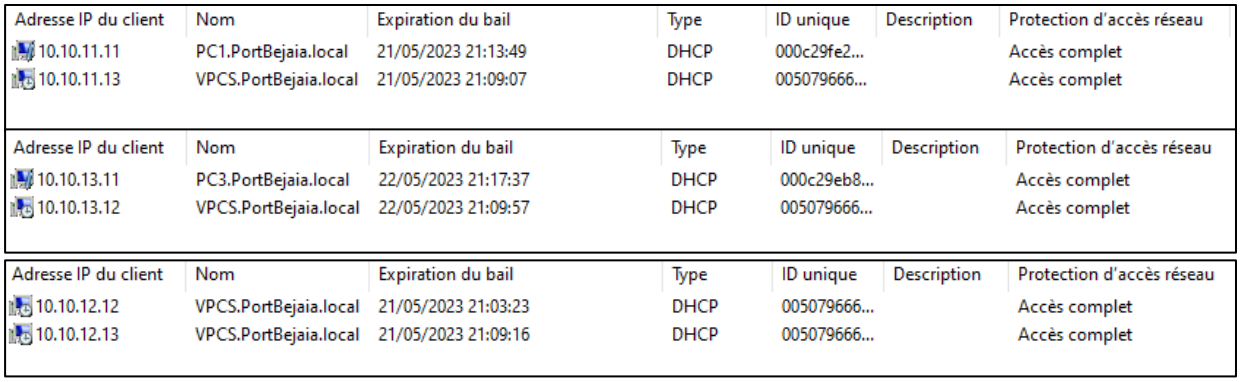



Figure 4.42-Connectivité réussie entre les VLAN de réseau LAN.

### 4.11.3 Test de serveur DHCP et routage inter VLAN du réseau CTMS

Nous pouvons voir sur le serveur Windows le fonctionnement de DHCP et l'attribution dynamique des adresse IP aux différentes machines sur l'étendue de chaque VLAN.



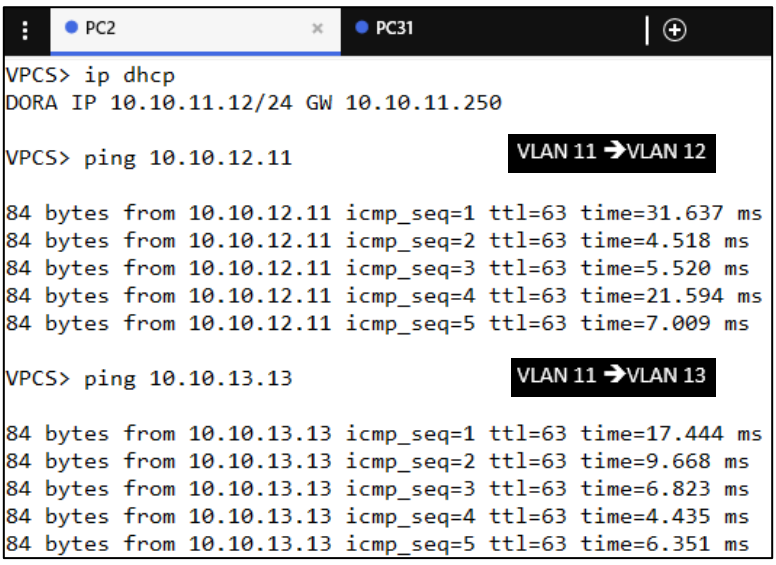
| Adresse IP du client | Nom | Expiration du bail | Type | ID unique | Description | Protection d'accès réseau |
|---|---|---|---|---|---|---|
| 10.10.11.11 | PC1.PortBejaia.local | 21/05/2023 21:13:49 | DHCP | 000c29fe2... | | Accès complet |
| 10.10.11.13 | VPCS.PortBejaia.local | 21/05/2023 21:09:07 | DHCP | 005079666... | | Accès complet |

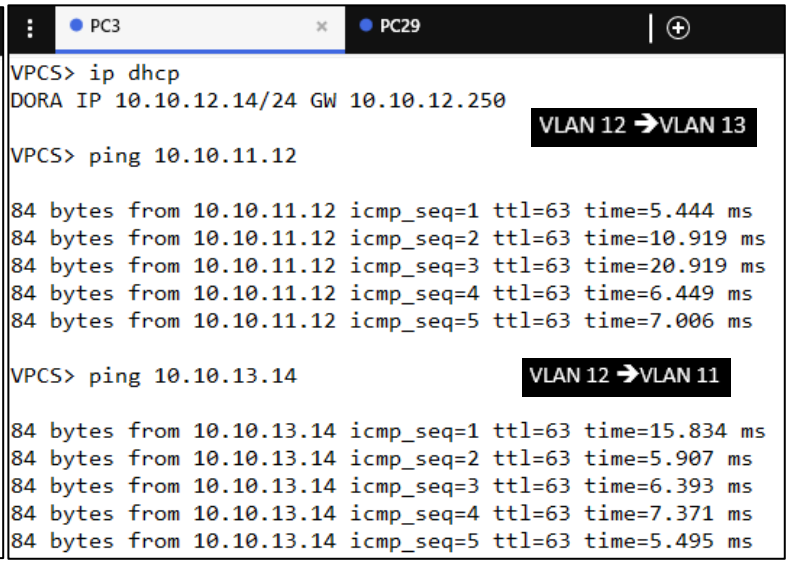
| Adresse IP du client | Nom | Expiration du bail | Type | ID unique | Description | Protection d'accès réseau |
|---|---|---|---|---|---|---|
| 10.10.13.11 | PC3.PortBejaia.local | 22/05/2023 21:17:37 | DHCP | 000c29eb8... | | Accès complet |
| 10.10.13.12 | VPCS.PortBejaia.local | 22/05/2023 21:09:57 | DHCP | 005079666... | | Accès complet |

| Adresse IP du client | Nom | Expiration du bail | Type | ID unique | Description | Protection d'accès réseau |
|---|---|---|---|---|---|---|
| 10.10.12.12 | VPCS.PortBejaia.local | 21/05/2023 21:03:23 | DHCP | 005079666... | | Accès complet |
| 10.10.12.13 | VPCS.PortBejaia.local | 21/05/2023 21:09:16 | DHCP | 005079666... | | Accès complet |

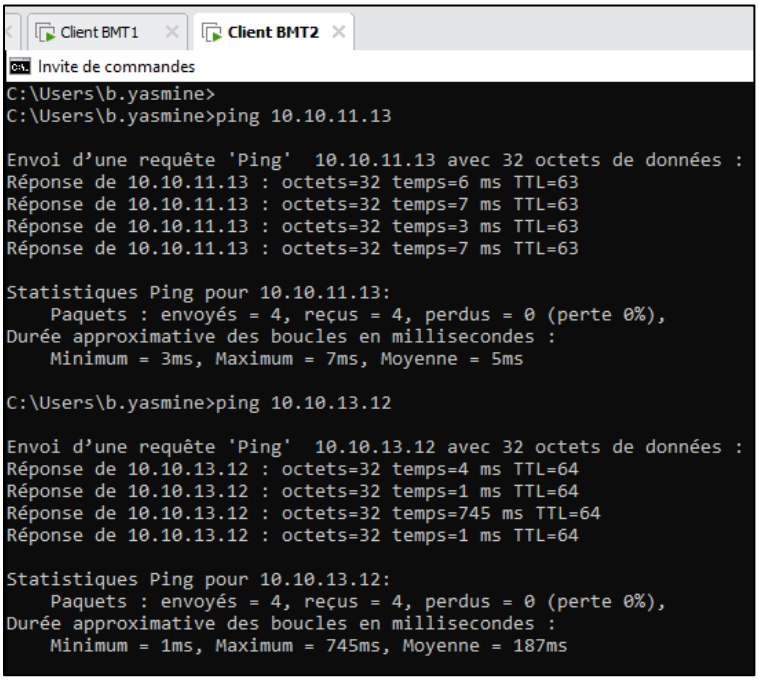
Figure 4.43-Attribution des adresses au hôte de réseau CTMS par le serveur DHCP.

Pour tester le routage inter VLAN sur le réseau CTMS, nous allons pinger entre les hôtes des différents VLAN, après l'attribution dynamique des adresses IP, par la suite nous allons éteindre le routeur Core1 pour basculer au Core2 et vérifier la continuité de fonctionnement de réseau.




De même, nous allons pinger partir des machines Windows 10 vers les hôtes du réseau, le routage inter VLAN est réussi.



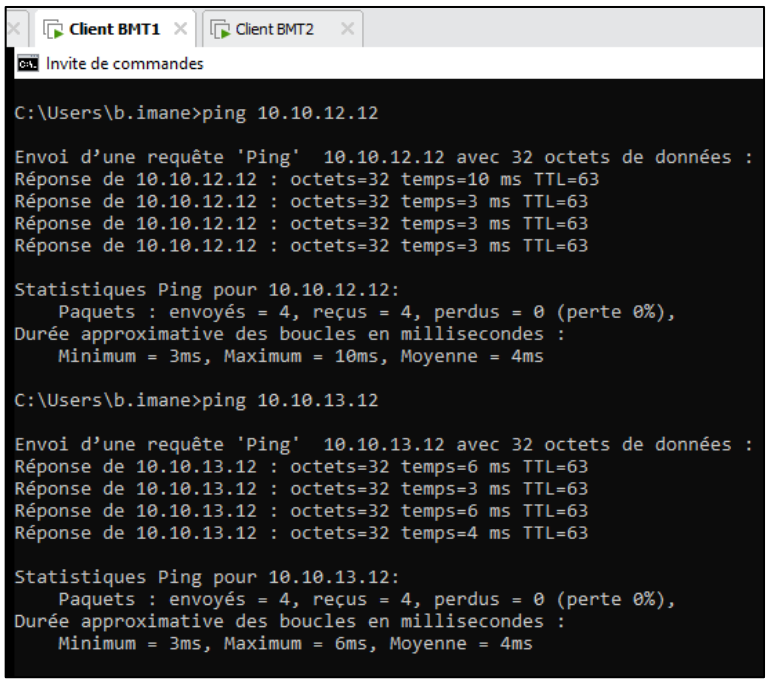




Figure 4.44-Connectivité réussie entre les VLAN de réseau CTMS.

### 4.11.4 Test DMZ-Bejaia

❖ Ping à partir d'un hôte du VLAN community

❖ Ping à partir d'un hôte du VLAN isolated

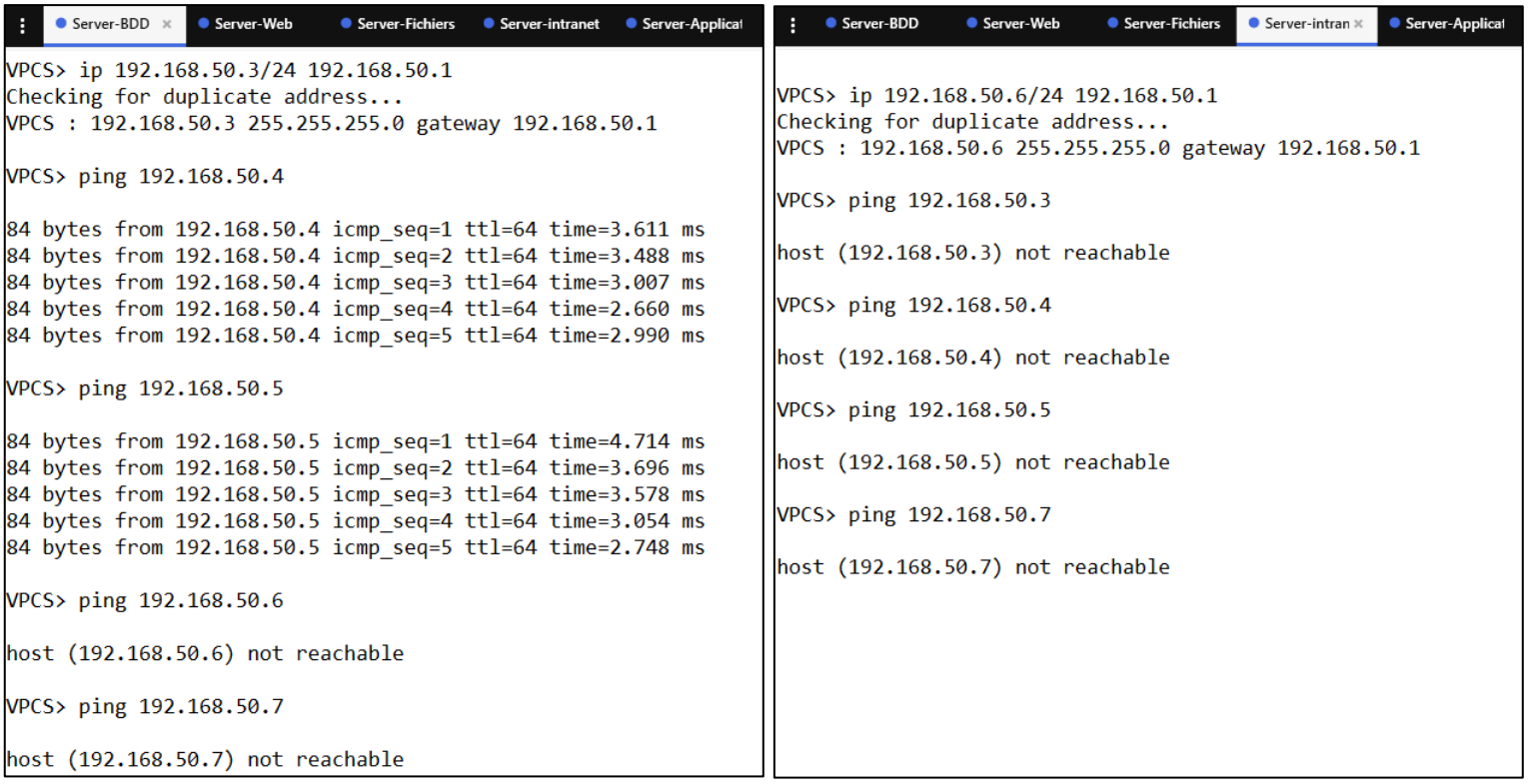



Figure 4.45-Test DMZ Bejaia.

### 4.11.5 Test DMZ-ZEP

❖ Ping à partir d'un hôte du VLAN community

❖ Ping à partir d'un hôte du VLAN isolated

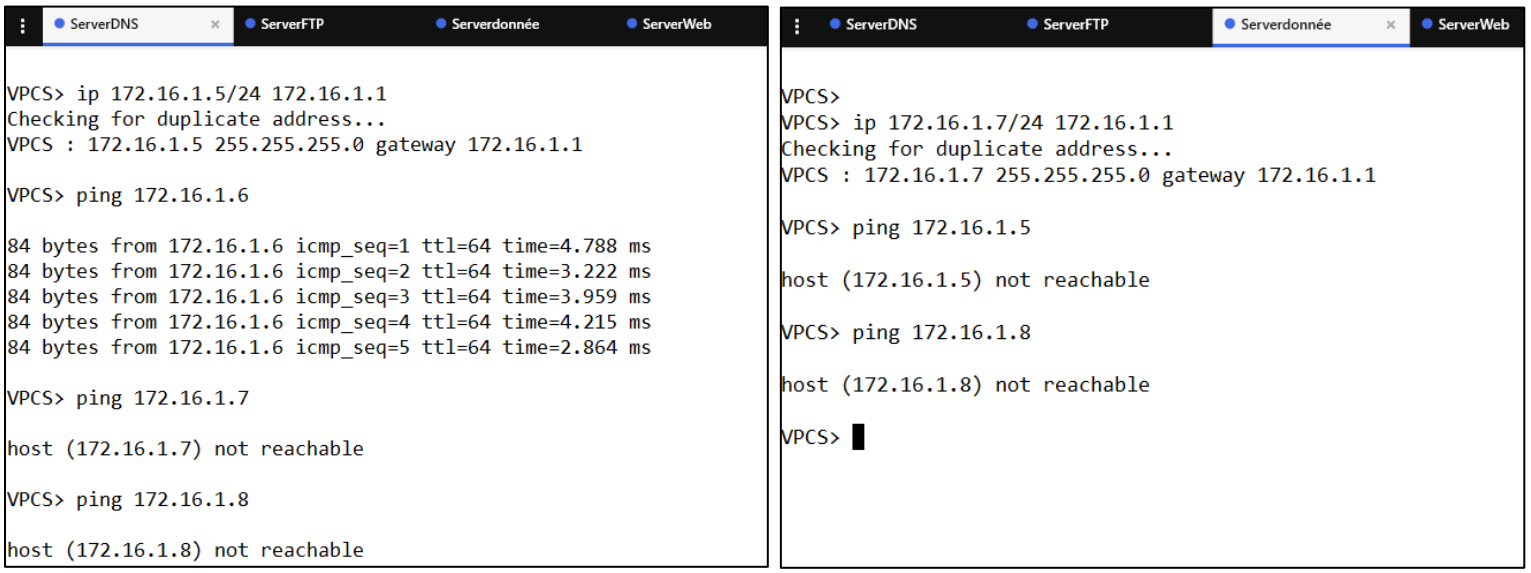



Figure 4.46-Test DMZ Irriyahen.

### 4.11.6 Test des interfaces des pare-feu

Sur le CLI de chaque pare-feu, nous allons pinger entre les différentes interfaces pour tester la connectivité des pare-feu.

❖ FG-Bejaia

```
FG-Bejaia # execute ping-options source 192.168.10.1
                                                    LAN1➔ LAN2
FG-Bejaia # execute ping 172.30.1.1
PING 172.30.1.1 (172.30.1.1): 56 data bytes
64 bytes from 172.30.1.1: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 172.30.1.1: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 172.30.1.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 172.30.1.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 172.30.1.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 172.30.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.1/0.5 ms

FG-Bejaia #
FG-Bejaia # execute ping-options source 192.168.40.1
                                                    CTMS1➔ ZEP
FG-Bejaia # execute ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1): 56 data bytes
64 bytes from 192.168.50.1: icmp_seq=0 ttl=255 time=1.2 ms
64 bytes from 192.168.50.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 192.168.50.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.2/1.2 ms
```

❖ FG-Irriyahen

```
FG-Irriyahen # execute ping-options source 172.16.1.1
                                                    DMZ-zep➔ CTMS2
FG-Irriyahen # execute ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1): 56 data bytes
64 bytes from 192.168.20.1: icmp_seq=0 ttl=255 time=7.2 ms
64 bytes from 192.168.20.1: icmp_seq=1 ttl=255 time=5.2 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=255 time=6.8 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=255 time=5.5 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=255 time=5.3 ms

--- 192.168.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.2/6.0/7.2 ms

FG-Irriyahen # execute ping-options source 172.16.2.1
                                                    LAN➔ DMZ-zep
FG-Irriyahen # execute ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1): 56 data bytes
64 bytes from 172.16.1.1: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 172.16.1.1: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 172.16.1.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 172.16.1.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 172.16.1.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 172.16.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.4 ms
```

Figure 4.47-Ping réussi entre les interfaces des pare-feu.

### 4.11.7 Test de NAT

Nous allons envoyer un ping à partir de serveur de la DMZ-Bejaia d'adresse 192.168.50.4/24 vers le routeur FAI qui se trouve sur internet, sur ce dernier nous allons activer la commande « debug ip icmp » pour afficher les informations sur les messages ICMP envoyés et reçus par le routeur.

```
Server-Web
VPCS> ip 192.168.50.4/24 192.168.50.1
Checking for duplicate address...
VPCS : 192.168.50.4 255.255.255.0 gateway 192.168.50.1

VPCS> ping 172.30.2.2

84 bytes from 172.30.2.2 icmp_seq=1 ttl=254 time=7.334 ms
84 bytes from 172.30.2.2 icmp_seq=2 ttl=254 time=7.789 ms
84 bytes from 172.30.2.2 icmp_seq=3 ttl=254 time=5.377 ms
84 bytes from 172.30.2.2 icmp_seq=4 ttl=254 time=10.449 ms
84 bytes from 172.30.2.2 icmp_seq=5 ttl=254 time=4.061 ms
```

```
FAI                Server-Web
FAI#debug ip icmp
ICMP packet debugging is on
FAI#
*Jun  5 15:17:29.864: ICMP: echo reply sent, src 172.30.2.2, dst 172.30.1.1
FAI#
*Jun  5 15:17:30.874: ICMP: echo reply sent, src 172.30.2.2, dst 172.30.1.1
FAI#
*Jun  5 15:17:31.881: ICMP: echo reply sent, src 172.30.2.2, dst 172.30.1.1
*Jun  5 15:17:32.891: ICMP: echo reply sent, src 172.30.2.2, dst 172.30.1.1
FAI#
*Jun  5 15:17:33.899: ICMP: echo reply sent, src 172.30.2.2, dst 172.30.1.1
```

Figure 4.48-Test de la configuration du NAT sur Fortigate.

Le résultat indique que la requête envoyée par le serveur est reçue avec une autre adresse qui est l'adresse de l'interface WAN de Fortigate.

### 4.11.8 Test de la haute disponibilité

❖ Vérification de la configuration :

Comme nous voyons après la configuration de HA, les interfaces de FG-Bejaia vont être configurées automatiquement sur FG-Bejaia-2.

FG-Bejaia-2

```
FG-Bejaia-2 # show system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.50.1 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set type physical
        set alias "DMZ"
        set role dmz
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp
        set type physical
        set alias "LAN10"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 2
    next
```

```
edit "port3"
    set vdom "root"
    set ip 192.168.30.1 255.255.255.0
    set allowaccess ping https ssh snmp
    set type physical
    set alias "LAN 30"
    set device-identification enable
    set lldp-transmission enable
    set role lan
    set snmp-index 3
next
edit "port4"
    set vdom "root"
    set ip 192.168.20.1 255.255.255.0
    set allowaccess ping https ssh snmp
    set type physical
    set alias "LAN20"
    set device-identification enable
    set lldp-transmission enable
    set role lan
    set snmp-index 4
next
```

```
edit "port6"
    set vdom "root"
    set ip 172.30.1.1 255.255.255.0
    set allowaccess ping https ssh snmp
    set type physical
    set alias "WAN"
    set lldp-reception enable
    set role wan
    set snmp-index 6
next
edit "port7"
    set vdom "root"
    set type physical
    set snmp-index 7
next
edit "port8"
    set vdom "root"
    set type physical
    set alias "HA-heart"
    set snmp-index 8
next
```

Figure 4.49-Interfaces de pare-feu FG-Bejaia-2.

❖ Test :

Afin de tester la configuration de AH nous allons envoyer un Ping au FG-Bejaia suivie de **-t** pour ne pas arrêter l'affichage de résultat.

Une fois le Ping est envoyé et réussi, nous allons éteindre le FG-Bejaia pour provoquer la panne, nous remarquons que le FG-Bejaia-2 prend le relais et bascule du secondaire vers primaire pour assurer la continuité de fonctionnement du réseau.

Invite de commandes

```
Microsoft Windows [version 10.0.19045.2965]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\PROBOOK>ping 192.168.2.15 -t

Envoi d'une requête 'Ping'  192.168.2.15 avec 32 octets de données :
Réponse de 192.168.2.15 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=4 ms TTL=255
Délai d'attente de la demande dépassé.
Réponse de 192.168.2.15 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=4 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.2.15 : octets=32 temps=3 ms TTL=255
```

Figure 4.50-Test de la haute disponibilité réussi.

### 4.11.9 Test de VPN site à site

Afin de tester l'état du tunnel VPN établi entre les deux pare-feu FG-Bejaia et FG-Irriyahen, un Ping sera envoyé de réseau CTMS de Bejaia vers le réseau ZEP de Irriyahen et inversement en utilisant la capture Wireshark dans l'interface de sortie du pare-feu.

- Test de Ping de réseau CTMS Bejaia vers le réseau ZEP Irriyahen
  Puisque le NAT est configuré sur le réseau CTMS, nous allons utiliser le routeur pour pinger vers l'hôte du réseau Irriyahen.

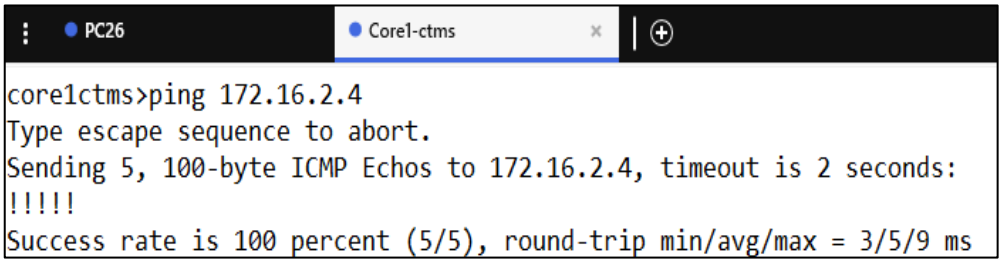



Figure 4.51- Ping réussi de réseau CTMS vers réseau ZEP.

- Test de Ping de réseau ZEP Irriyahen vers réseau CTMS Bejaia

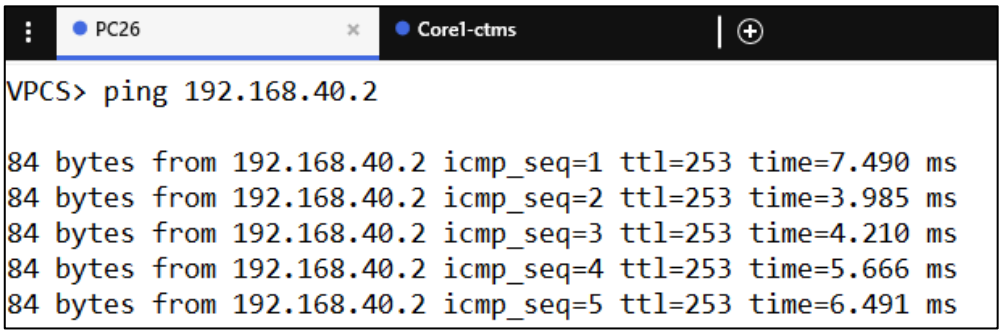



Figure 4.52-Ping réussi de réseau ZEP vers réseau ZEP.

- Test d'établissement et de cryptage des données au niveau de tunnel VPN

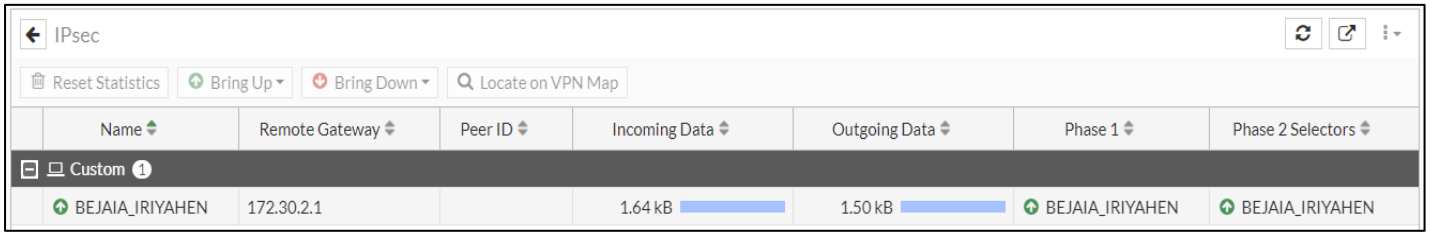



Figure 4.53-Tunnel VPN établi au niveau de FG-Bejaia.

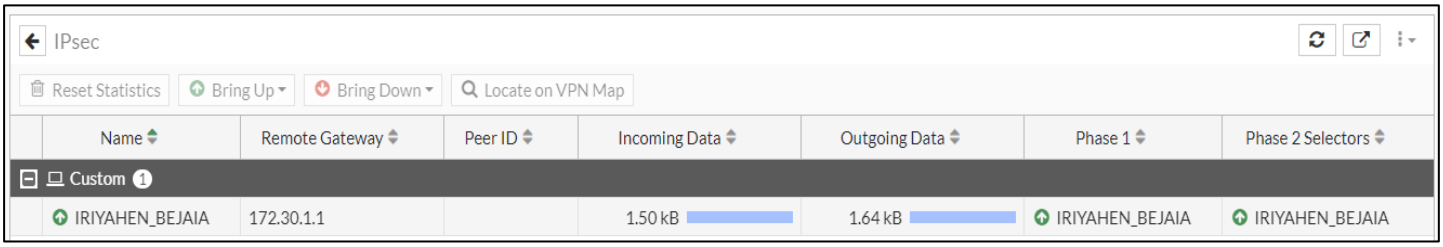



Figure 4.54-Tunnel VPN établi au niveau de FG-Irriyahen.

On lance une capture wireshark sur le lien reliant les deux sites CTMS de Béjaia et la ZEP pour observer le cryptage de trafic dans le tunnel VPN.

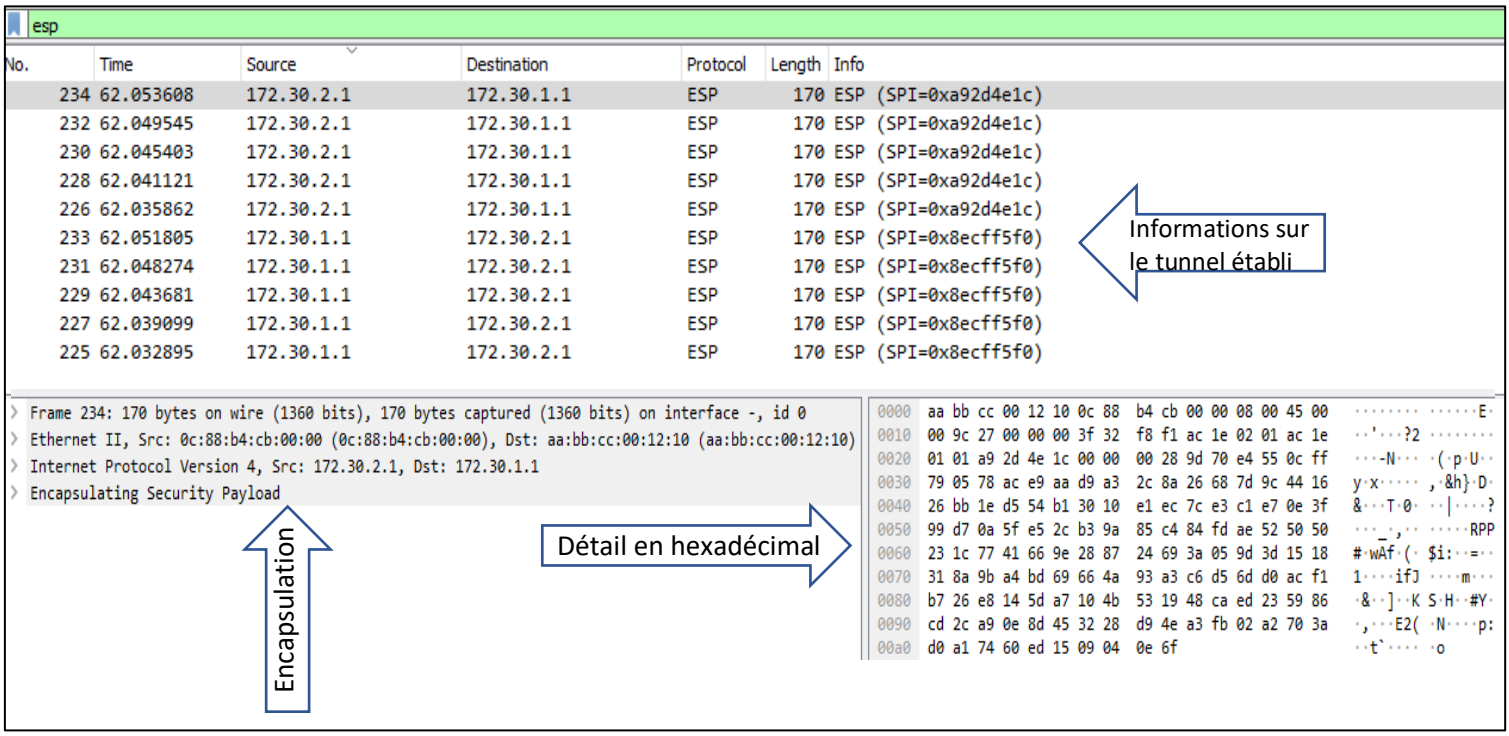



Figure 4.55-Capture des données cryptés sur Wireshark.

## *Conclusion*

Notre objectif était d'apporter des améliorations au réseau selon un ensemble de politique de sécurité que nous avons abordé auparavant pour avoir une connexion sécurisée entre les différents réseaux de l'entreprise BMT. Nous avons pu atteindre cet objectif et valider notre solution grâce à des tests effectués pour vérifier le fonctionnement de chaque configuration mise en œuvre.

# Conclusion générale

L'objectif de notre projet de fin d'études est de proposer une nouvelle infrastructure pour le réseau de l'entreprise d'accueil et de réaliser un système de sécurité basé sur plusieurs technologies en utilisant les liaisons virtuelles VLAN de niveau 3 et segmenter le réseau pour remédier aux attaques qui peuvent se produire à l'intérieur de l'entreprise. Nous avons configuré le pare-feu Fortigate en créant une liste de contrôle d'accès et autorisé/bloqué la communication entre ses différentes interfaces pour protéger le réseau des attaques externes, nous avons également configuré un VPN IPsec qui relie entre les deux sites de l'entreprise, site de Bejaia et le site de Irriyahen, afin d'assurer l'accès à distance aux ressources et l'échange de données de manière sécurisée.

Pour renforcer la sécurité de nos réseaux locaux, nous avons créé une Zone Démilitarisée (DMZ) dans le but de séparer ces réseaux de tout ce qui est accessible depuis l'internet.

Afin d'assurer la disponibilité et la continuité de fonctionnement des services, nous avons mis en place un pare-feu Fortigate secondaire et nous avons configuré d'autres éléments (routeur, protocole HSPR et GLBP) pour avoir la tolérance aux pannes. De plus nous avons configuré l'annuaire Active Directory pour faciliter la gestion des utilisateurs et des services réseaux.

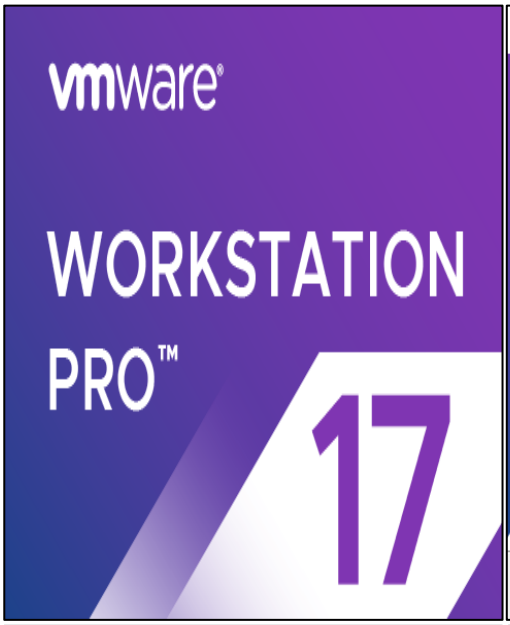
Les résultats obtenus lors des simulations effectuées sur GNS-3 ont montré le bon fonctionnement des technologies configurées au sein de l'entreprise permettant ainsi l'amélioration des problèmes relatifs à la disponibilité et à la sécurisation des données échangées entre les différentes entités du réseau.

Ce projet nous a permis d'enrichir, améliorer et approfondir nos connaissances sur l'administration et la sécurité des réseaux informatiques. Il nous a également permis de découvrir d'autres logiciels de simulation tels que VMware Workstation 17 pro, Windows server 2022 et service d'annuaire Active Directory.

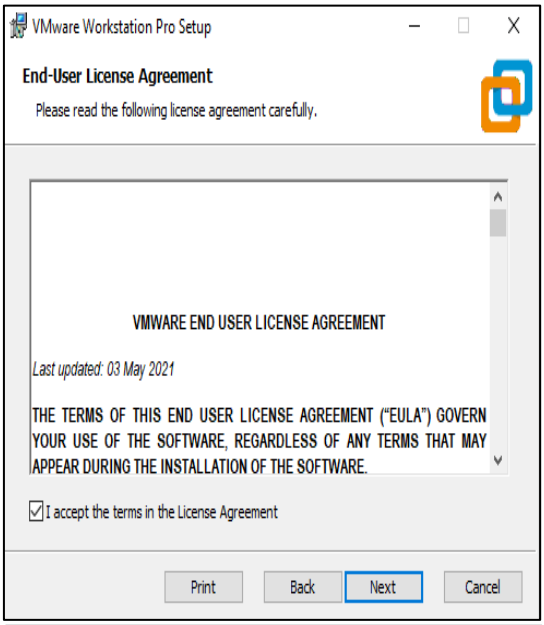
# Annexes

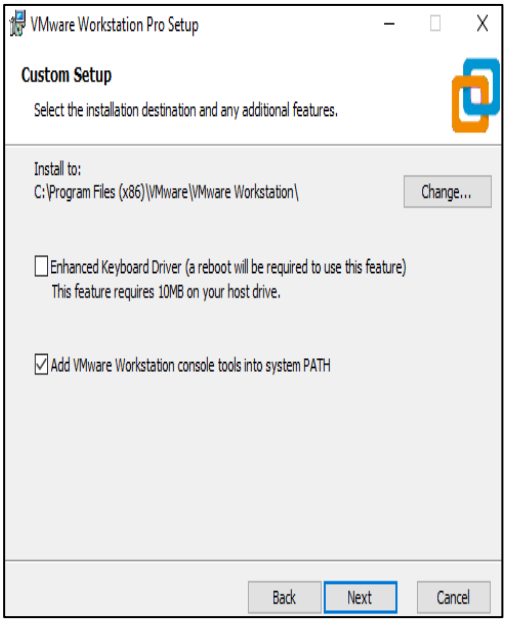
**Annexe 1 :** Installation de VMware Workstation version 17.0.0

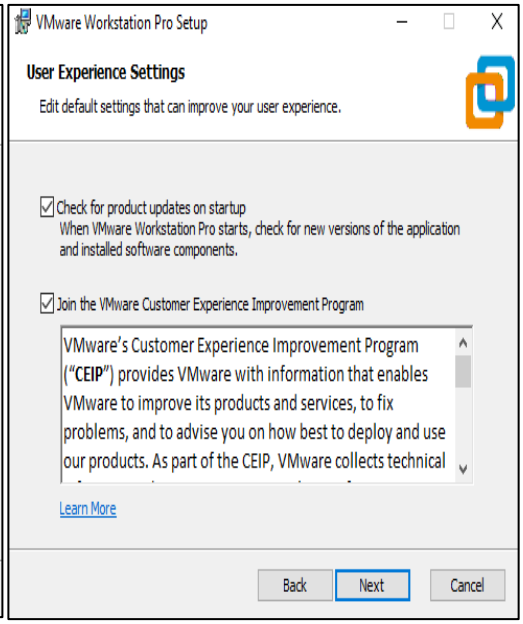
Afin de pouvoir créer plusieurs machines virtuelles au sein d'un même ordinateur, nous sommes appelés à installer VMware Workstation 17.0.0 sur Windows 10
Disponible sur le lien :
https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html
Les figures suivantes représentent les différentes étapes pour son installation :

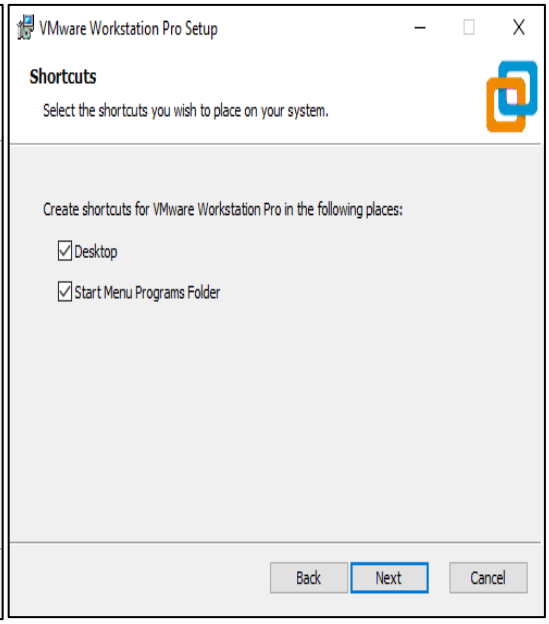


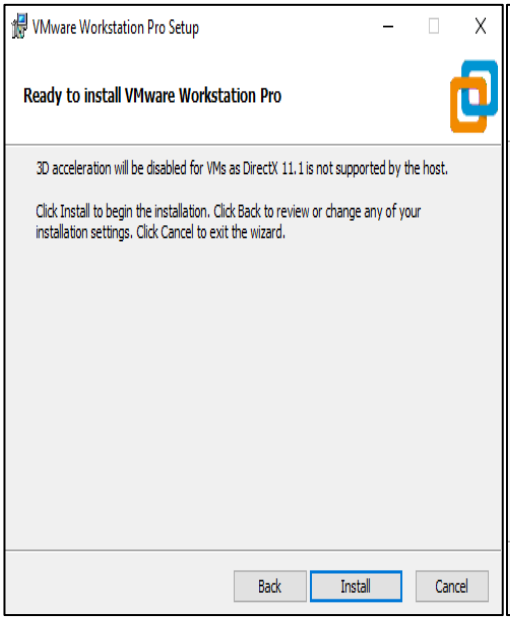


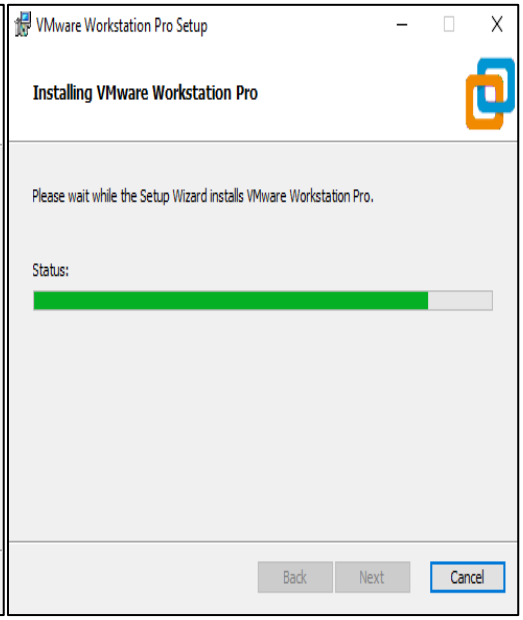


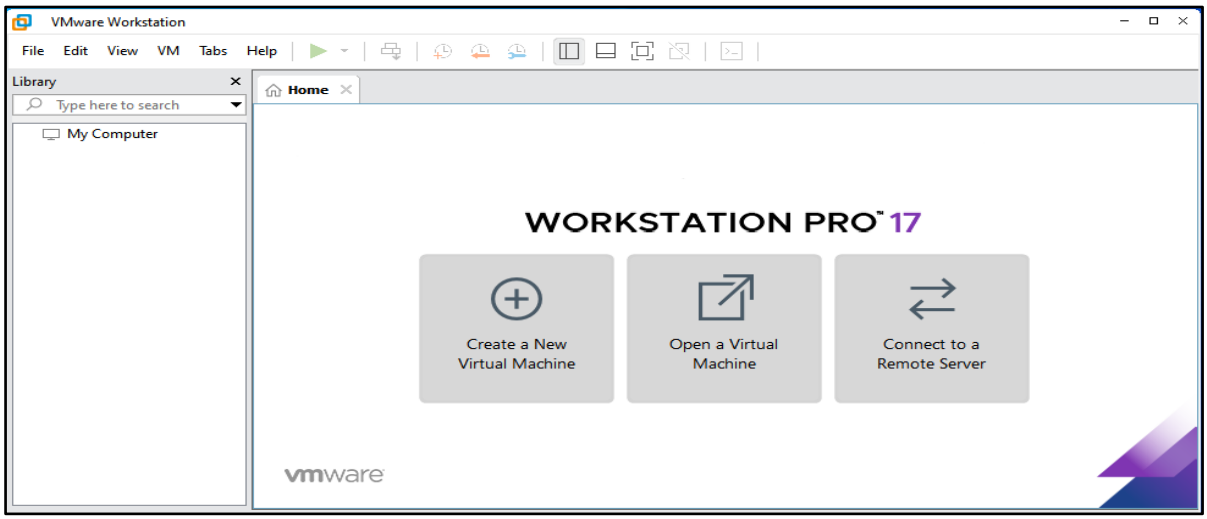





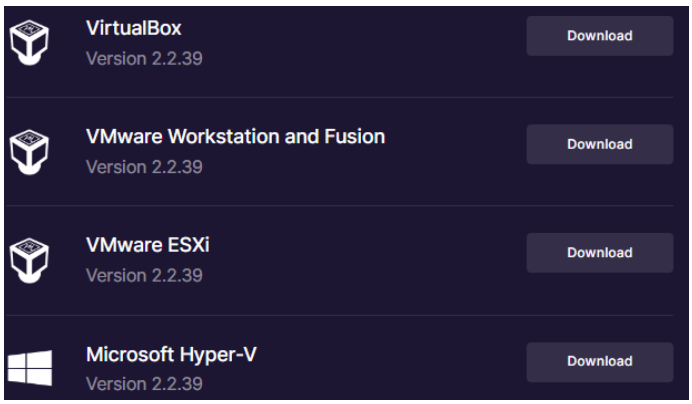



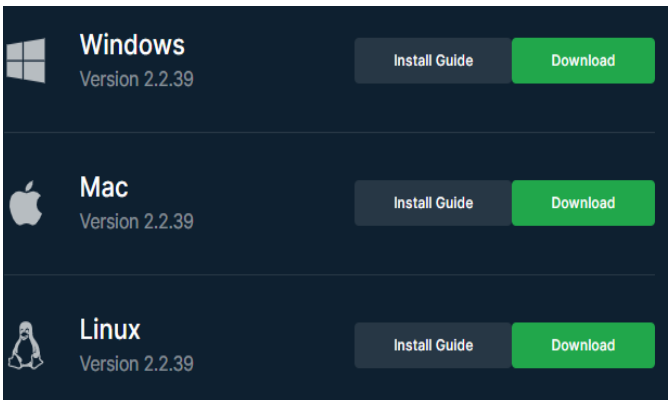


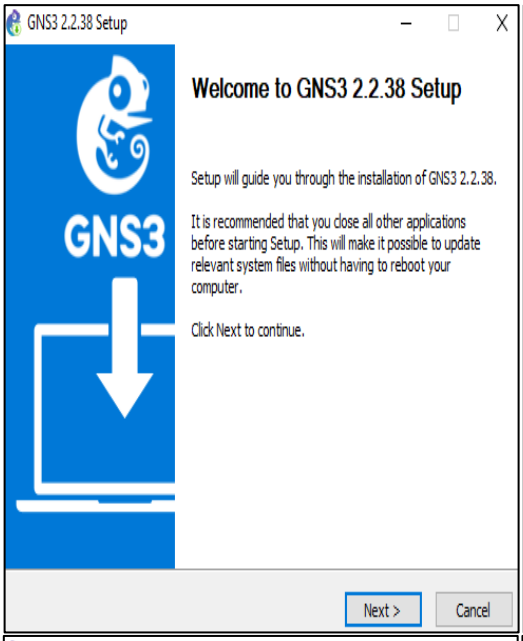


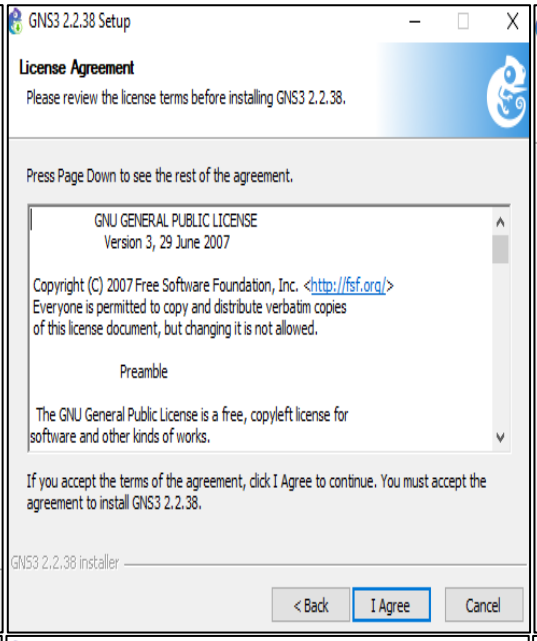

**Annexe 2 :** Installation de GNS3

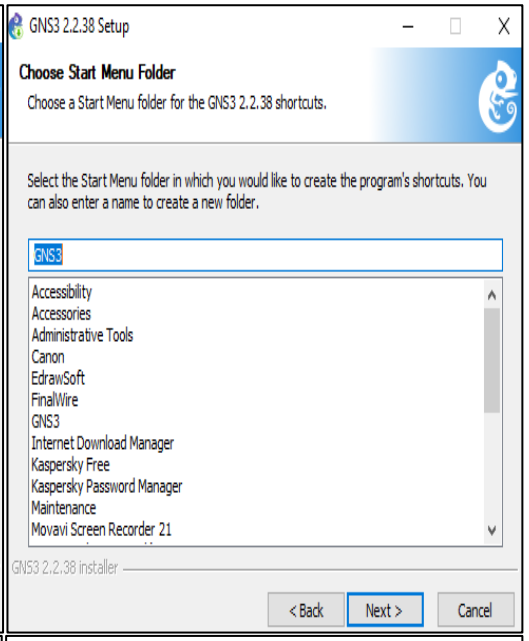
La version de GNS3 utilisé est 2.2.38 qui est disponible sur le lien https://www.gns3.com/software/download pour GNS3 et https://www.gns3.com/software/download-vm pour GNS3 VM

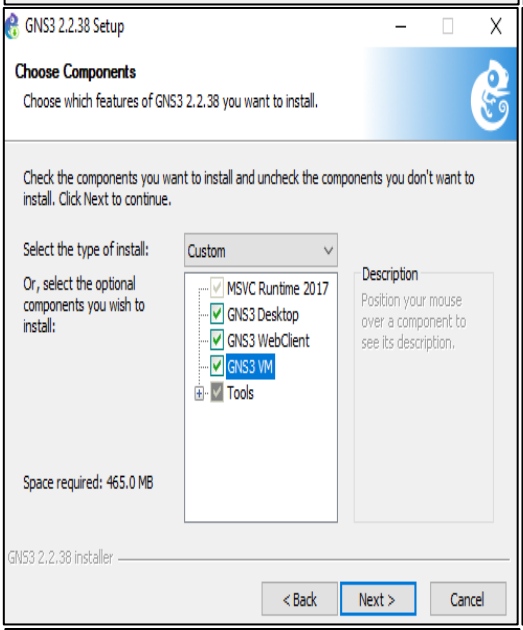


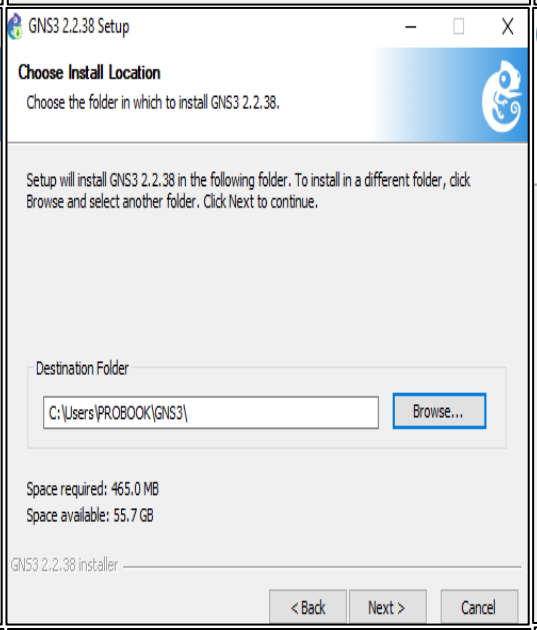



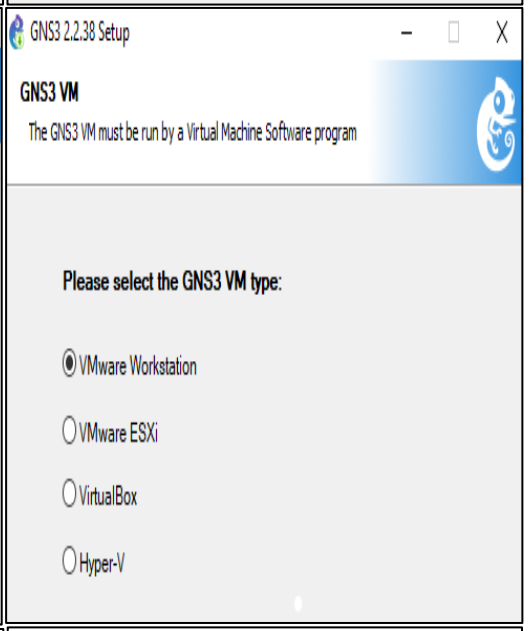

GNS3 2.2.38 Setup
Welcome to GNS3 2.2.38 Setup
Setup will guide you through the installation of GNS3 2.2.38.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel

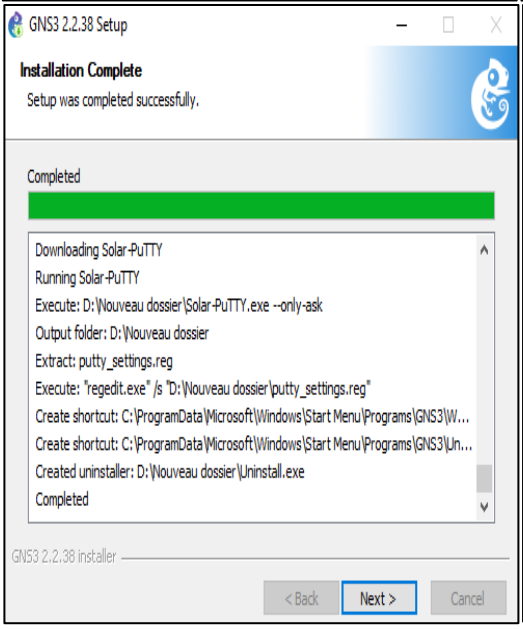

GNS3 2.2.38 Setup
License Agreement
Please review the license terms before installing GNS3 2.2.38.
Press Page Down to see the rest of the agreement.
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007
Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Preamble
The GNU General Public License is a free, copyleft license for software and other kinds of works.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install GNS3 2.2.38.
GNS3 2.2.38 installer
< Back
I Agree
Cancel


GNS3 2.2.38 Setup
Choose Start Menu Folder
Choose a Start Menu folder for the GNS3 2.2.38 shortcuts.
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.
GNS3
Accessibility
Accessories
Administrative Tools
Canon
EdrawSoft
FinalWire
GNS3
Internet Download Manager
Kaspersky Free
Kaspersky Password Manager
Maintenance
Movavi Screen Recorder 21
GNS3 2.2.38 installer
< Back
Next >
Cancel

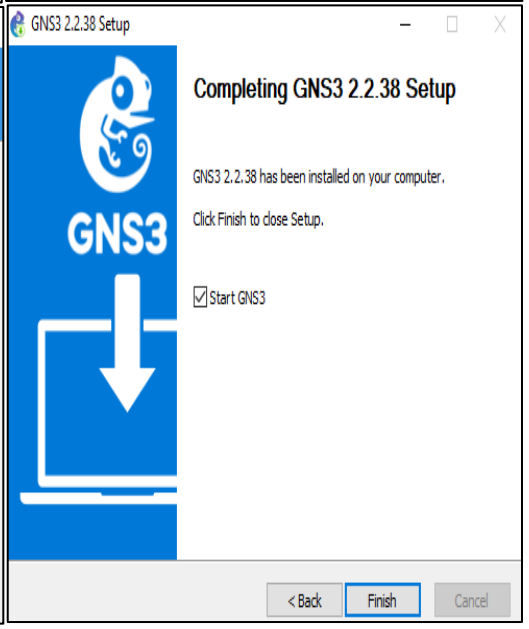

GNS3 2.2.38 Setup
Choose Components
Choose which features of GNS3 2.2.38 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Custom
Or, select the optional components you wish to install:
MSVC Runtime 2017
GNS3 Desktop
GNS3 WebClient
GNS3 VM
Tools
Description
Position your mouse over a component to see its description.
Space required: 465.0 MB
GNS3 2.2.38 installer
< Back
Next >
Cancel

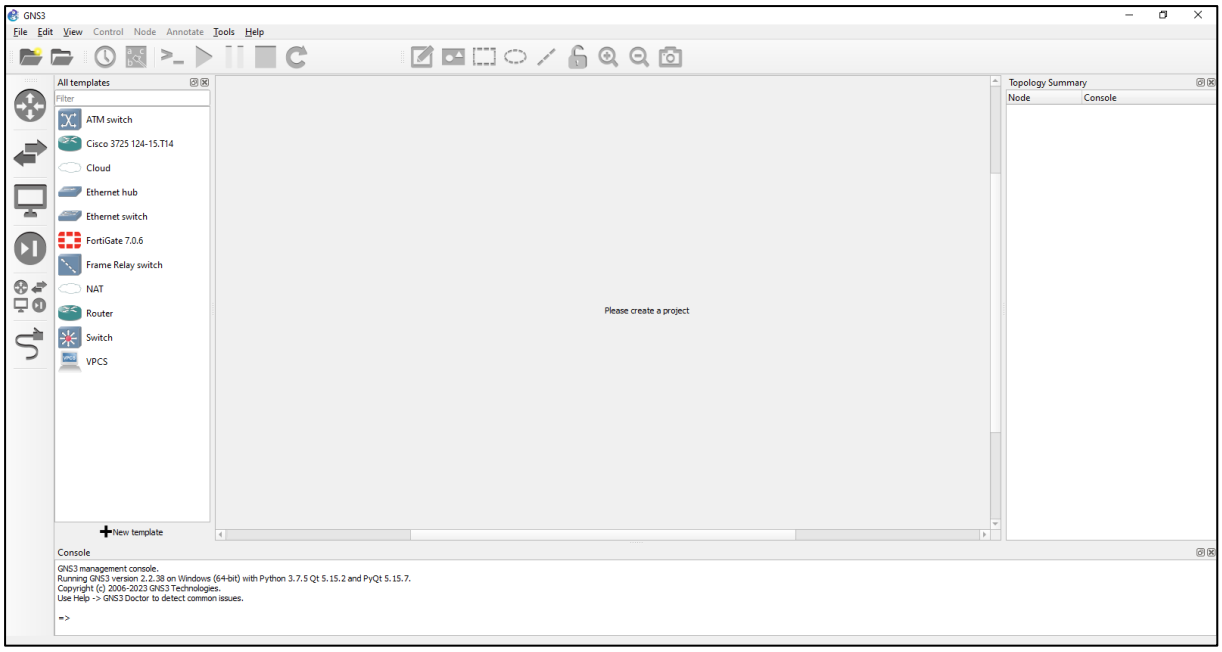

GNS3 2.2.38 Setup
Choose Install Location
Choose the folder in which to install GNS3 2.2.38.
Setup will install GNS3 2.2.38 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Users\PROBOOK\GNS3\
Browse...
Space required: 465.0 MB
Space available: 55.7 GB
GNS3 2.2.38 installer
< Back
Next >
Cancel


GNS3 2.2.38 Setup
GNS3 VM
The GNS3 VM must be run by a Virtual Machine Software program
Please select the GNS3 VM type:
VMware Workstation
VMware ESXi
VirtualBox
Hyper-V

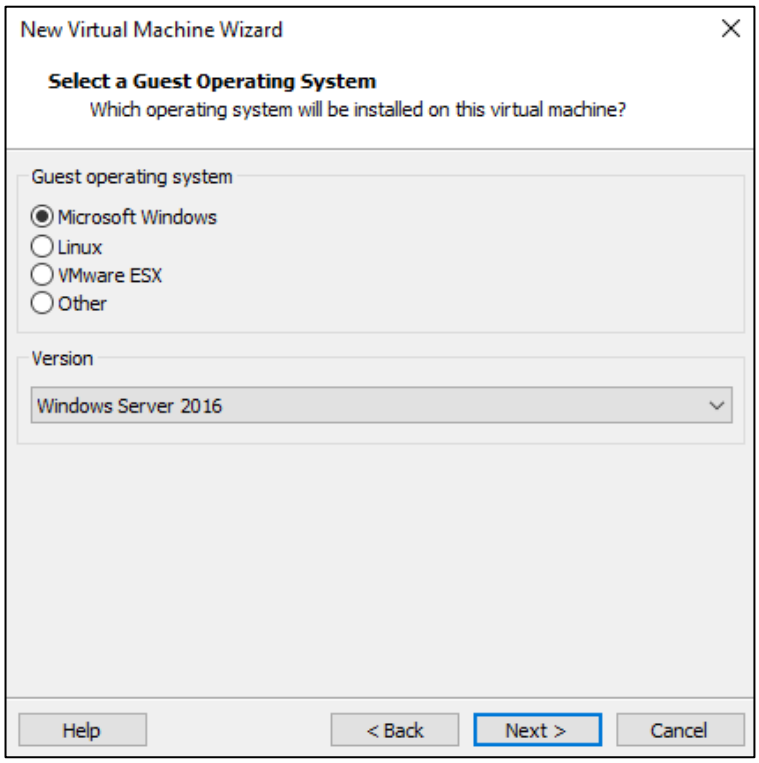

GNS3 2.2.38 Setup
Installation Complete
Setup was completed successfully.
Completed
Downloading Solar-PuTTY
Running Solar-PuTTY
Execute: D:\Nouveau dossier\Solar-PuTTY.exe --only-ask
Output folder: D:\Nouveau dossier
Extract: putty_settings.reg
Execute: "regedit.exe" /s "D:\Nouveau dossier\putty_settings.reg"
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\GNS3\W...
Create shortcut: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\GNS3\Un...
Created uninstaller: D:\Nouveau dossier\Uninstall.exe
Completed
GNS3 2.2.38 installer
< Back
Next >
Cancel

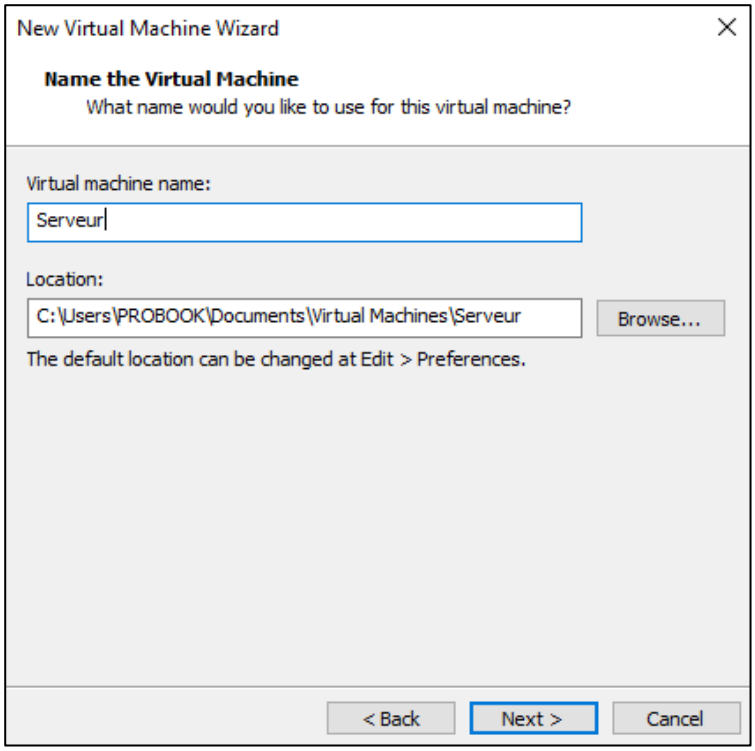

GNS3 2.2.38 Setup
Solarwinds Standard Toolset
Exclusive for GNS3 users
Would you like to get your free license of Solarwinds Standard Toolset? ($200 value)
Yes
No
Toolset F.A.Q
GNS3 2.2.38 installer
< Back
Next >
Cancel

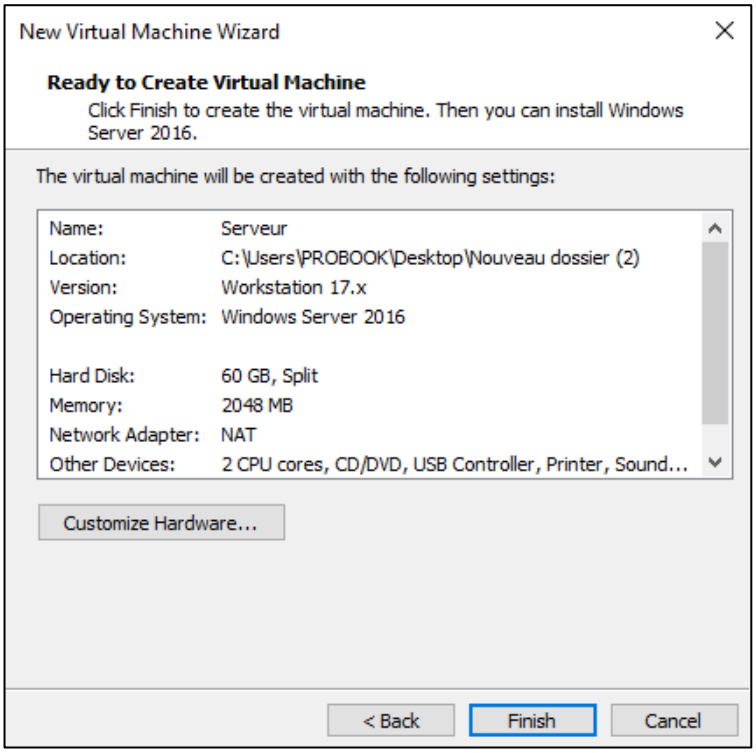

GNS3 2.2.38 Setup
Completing GNS3 2.2.38 Setup
GNS3 2.2.38 has been installed on your computer.
Click Finish to close Setup.
Start GNS3
< Back
Finish
Cancel

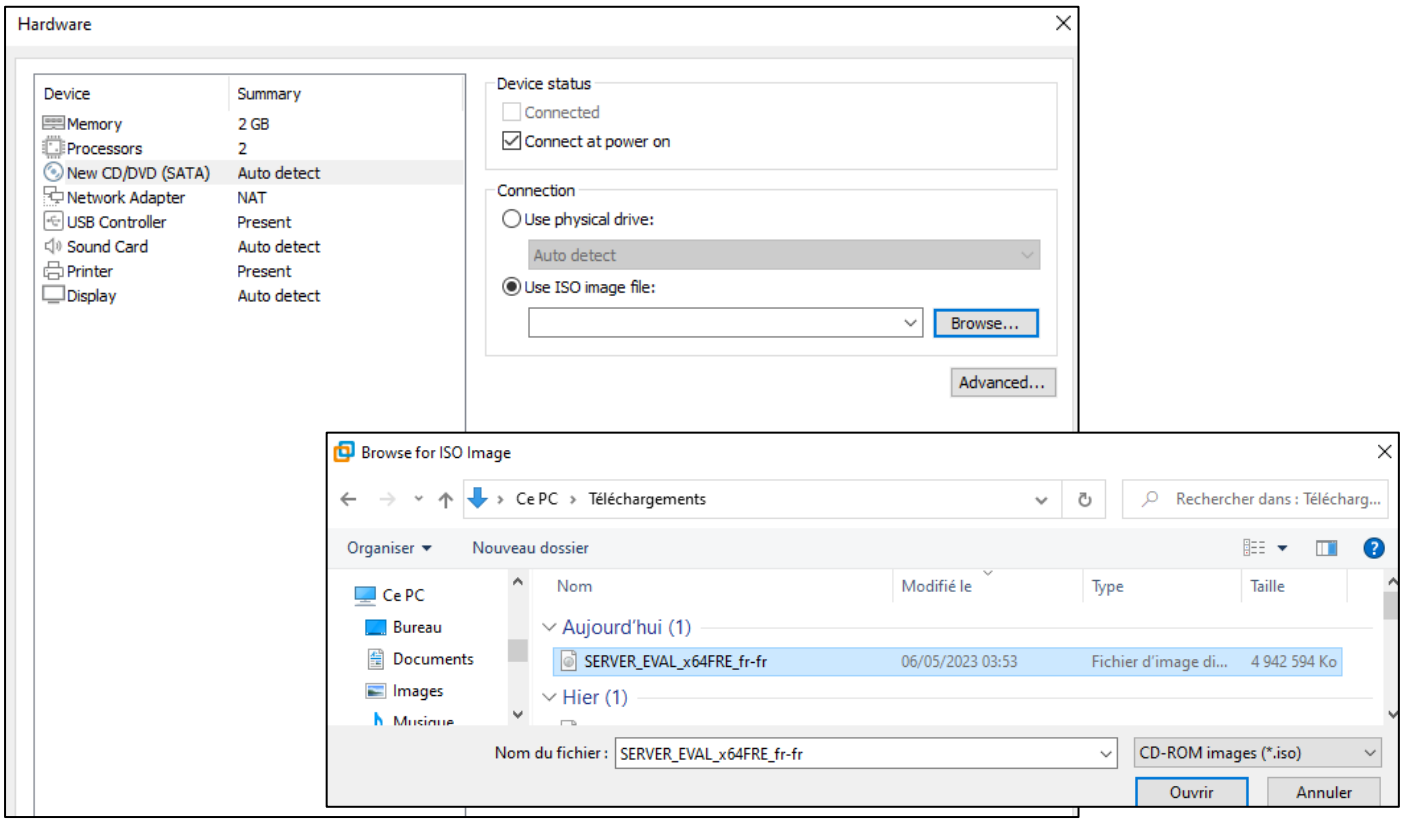


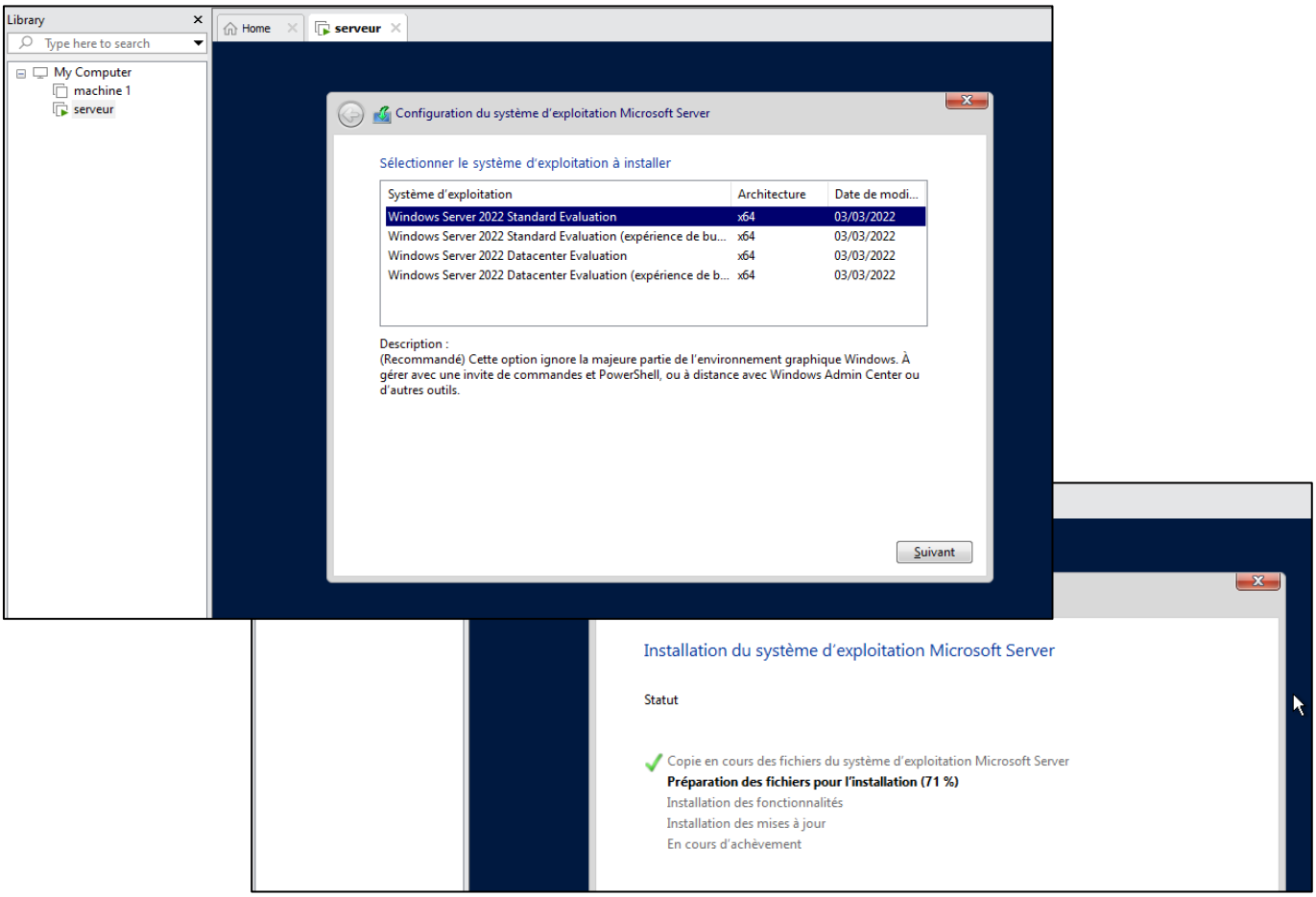

**Annexe 3** : installation de Windows serveur 2022

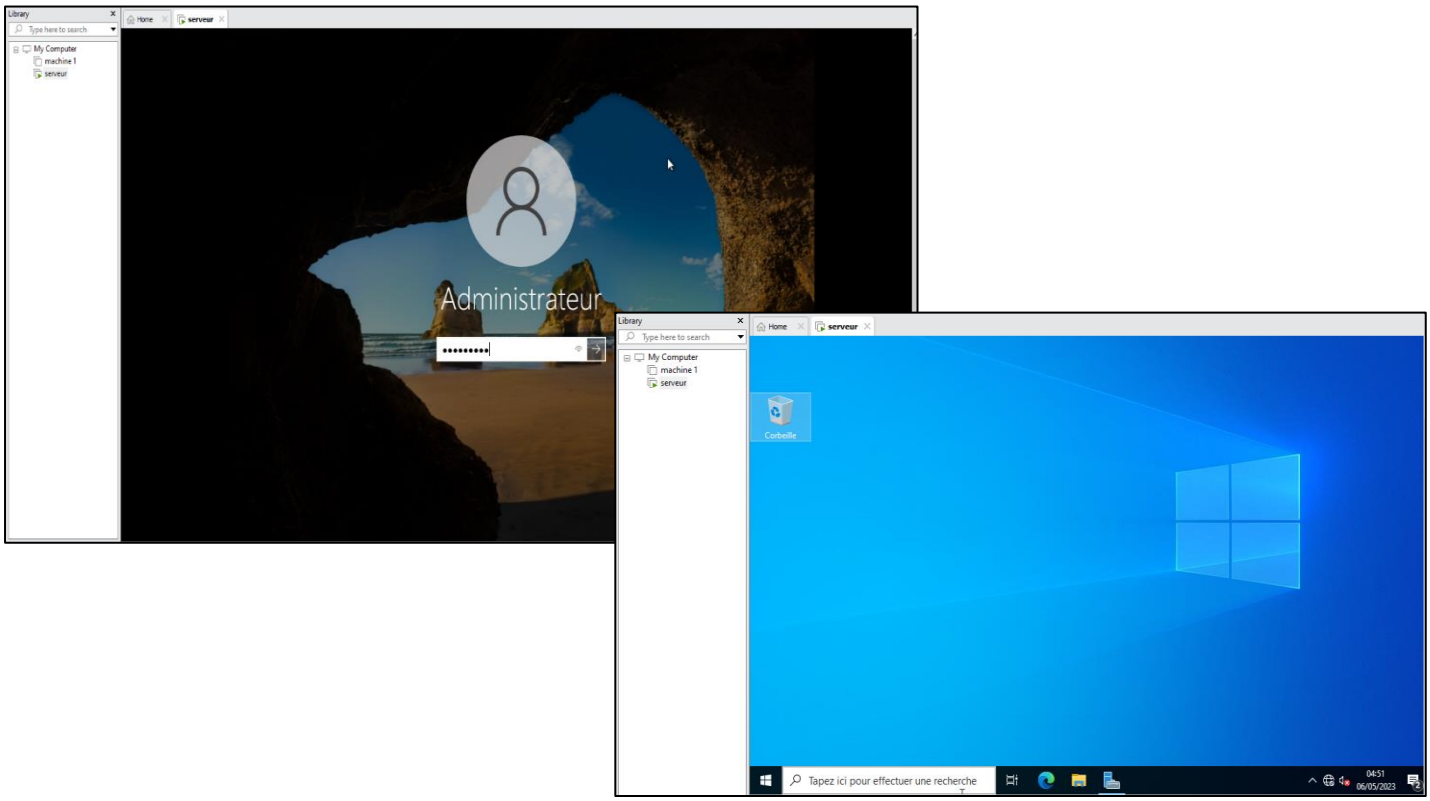




New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
Serveur
Location:
C:\Users\PROBOOK\Documents\Virtual Machines\Serveur
Browse...
The default location can be changed at Edit > Preferences.
< Back
Next >
Cancel

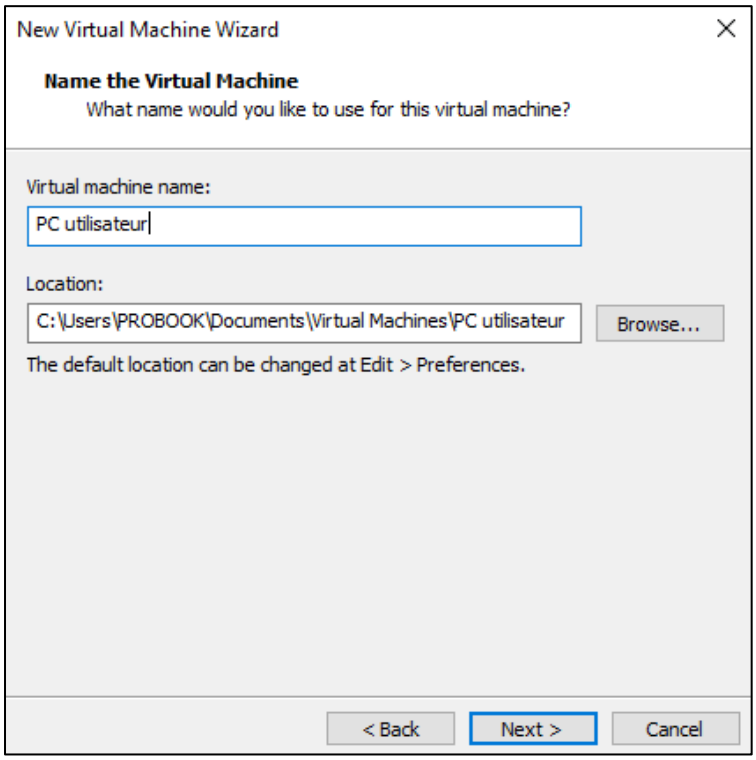

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install Windows Server 2016.
The virtual machine will be created with the following settings:
Name: Serveur
Location: C:\Users\PROBOOK\Desktop\Nouveau dossier (2)
Version: Workstation 17.x
Operating System: Windows Server 2016
Hard Disk: 60 GB, Split
Memory: 2048 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Printer, Sound...
Customize Hardware...
< Back
Finish
Cancel

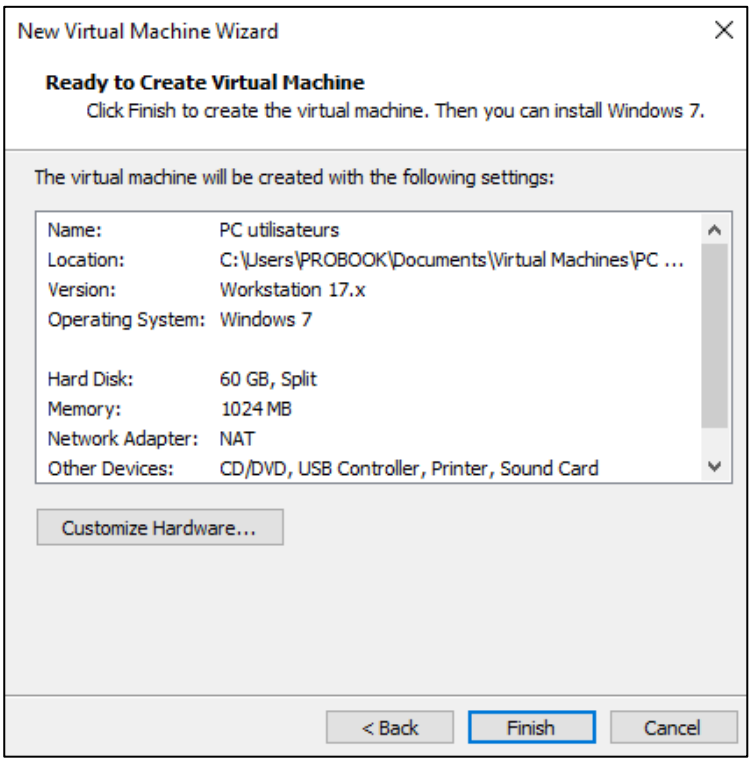

Hardware
Device
Summary
Memory
2 GB
Processors
2
New CD/DVD (SATA)
Auto detect
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Printer
Present
Display
Auto detect
Device status
Connected
Connect at power on
Connection
Use physical drive:
Auto detect
Use ISO image file:
Browse...
Advanced...
Browse for ISO Image
Ce PC › Téléchargements
Rechercher dans : Télécharg...
Organiser
Nouveau dossier
Ce PC
Bureau
Documents
Images
Nom
Modifié le
Type
Taille
Aujourd'hui (1)
SERVER_EVAL_x64FRE_fr-fr
06/05/2023 03:53
Fichier d'image di...
4 942 594 Ko
Hier (1)
Nom du fichier :
SERVER_EVAL_x64FRE_fr-fr
CD-ROM images (*.iso)
Ouvrir
Annuler

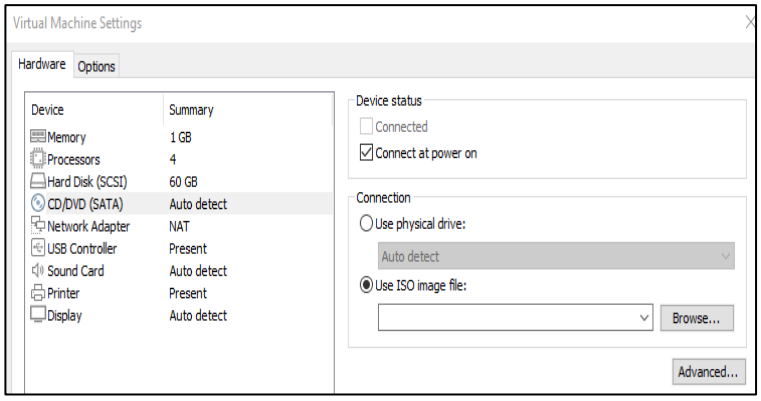

Library
Type here to search
My Computer
machine 1
serveur
Home
serveur
Configuration du système d'exploitation Microsoft Server
Sélectionner le système d'exploitation à installer
Système d'exploitation
Architecture
Date de modi...
Windows Server 2022 Standard Evaluation
x64
03/03/2022
Windows Server 2022 Standard Evaluation (expérience de bu...
x64
03/03/2022
Windows Server 2022 Datacenter Evaluation
x64
03/03/2022
Windows Server 2022 Datacenter Evaluation (expérience de b...
x64
03/03/2022
Description :
(Recommandé) Cette option ignore la majeure partie de l'environnement graphique Windows. À gérer avec une invite de commandes et PowerShell, ou à distance avec Windows Admin Center ou d'autres outils.
Suivant
Installation du système d'exploitation Microsoft Server
Statut
Copie en cours des fichiers du système d'exploitation Microsoft Server
Préparation des fichiers pour l'installation (71 %)
Installation des fonctionnalités
Installation des mises à jour
En cours d'achèvement

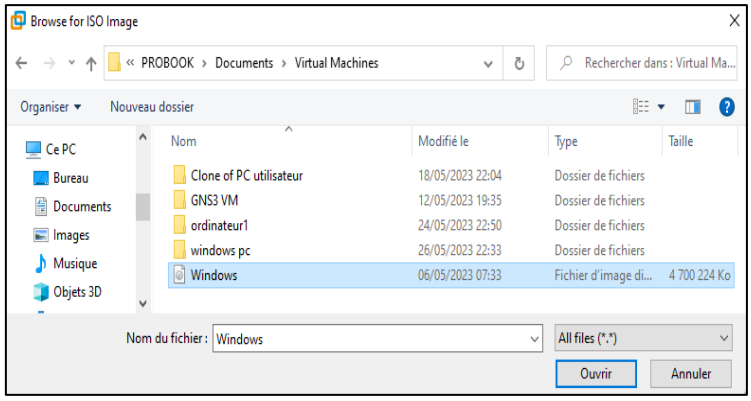

Administrateur
Corbeille
Tapez ici pour effectuer une recherche

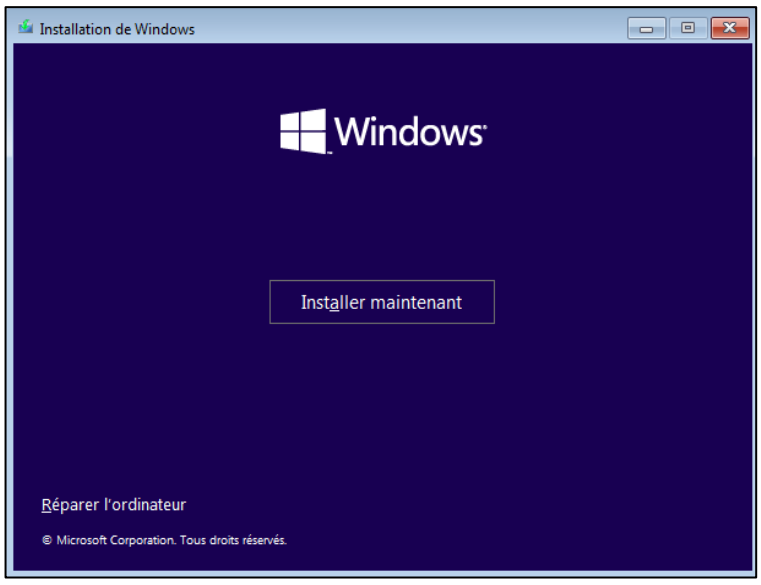
**Annexe 4:** installation de Windows 2010

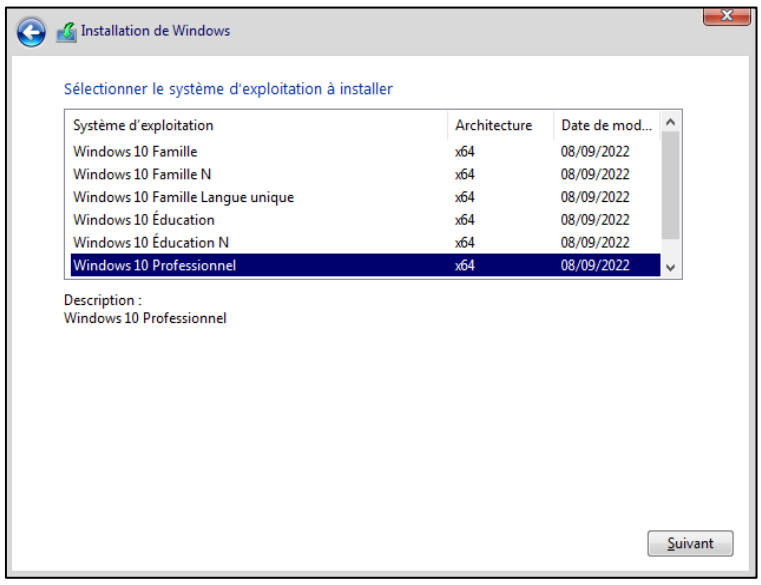


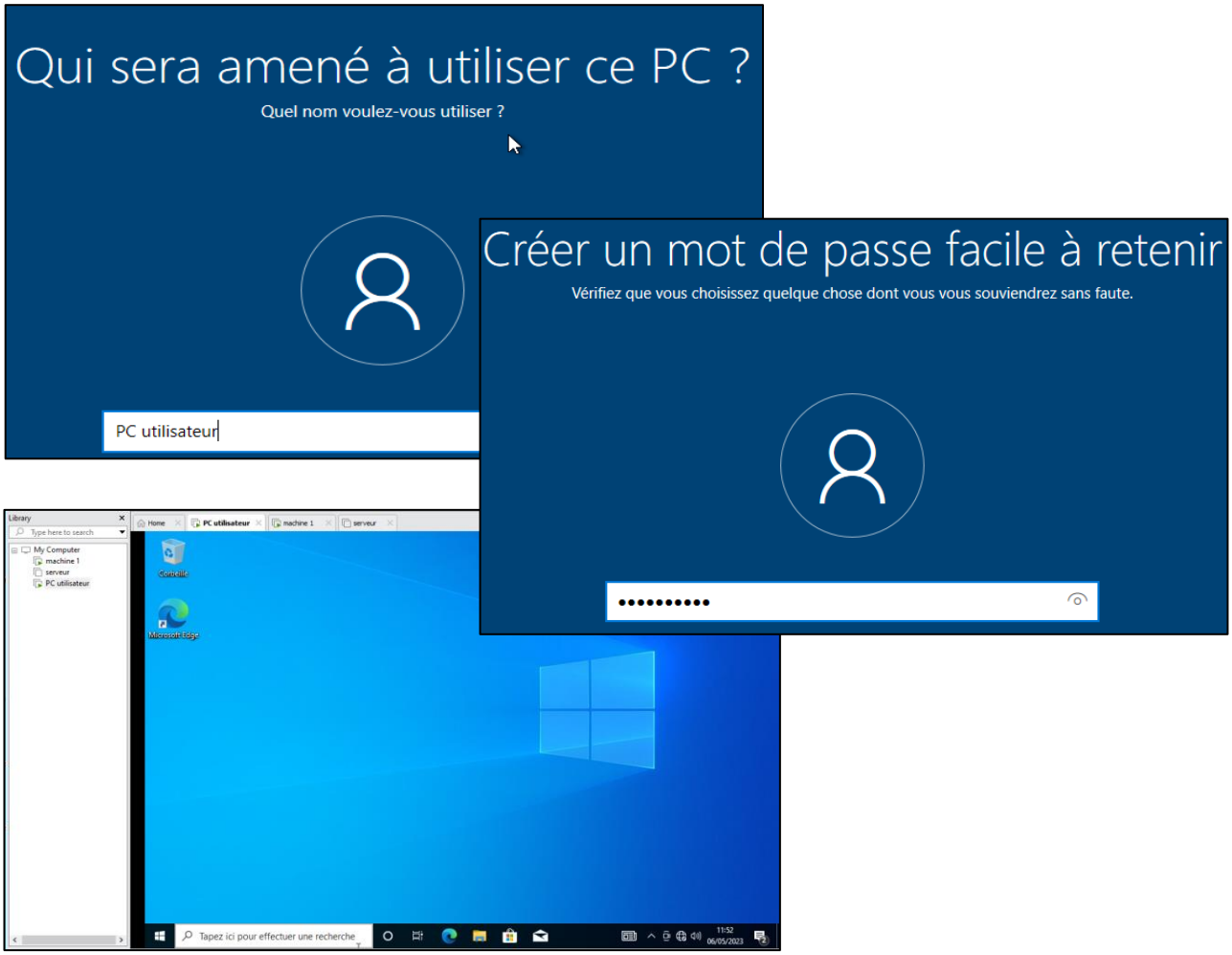



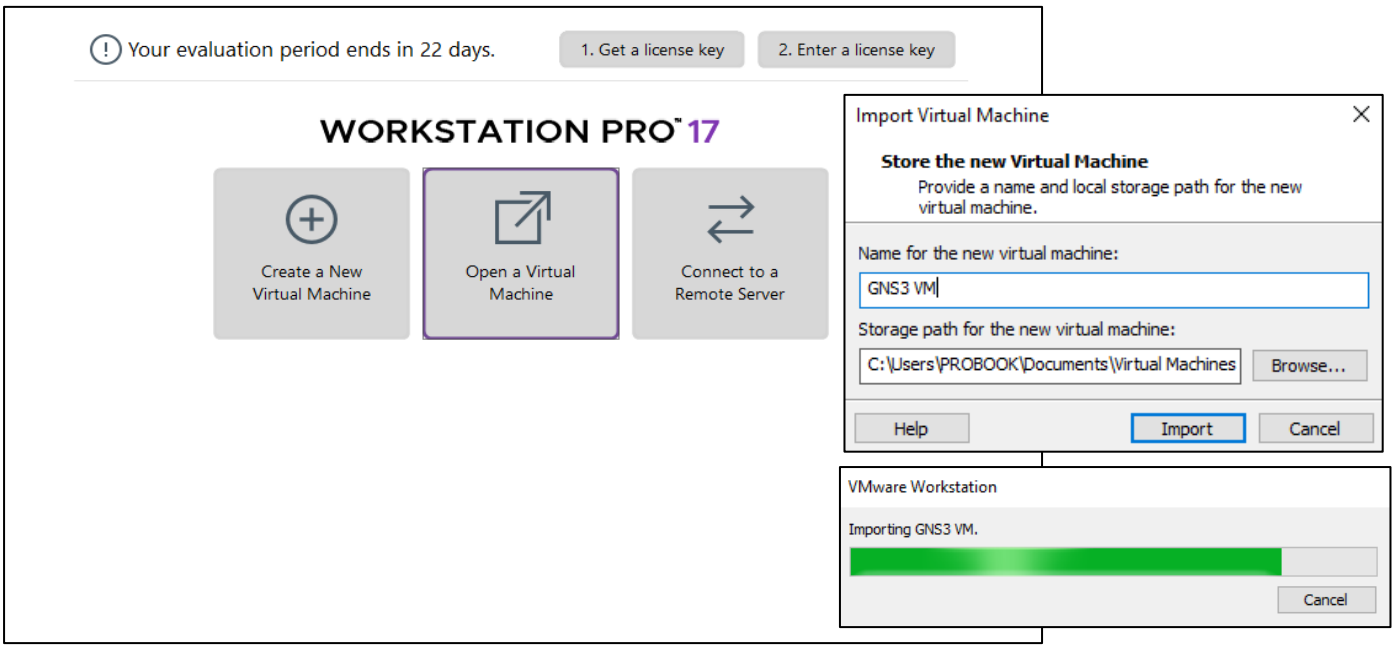



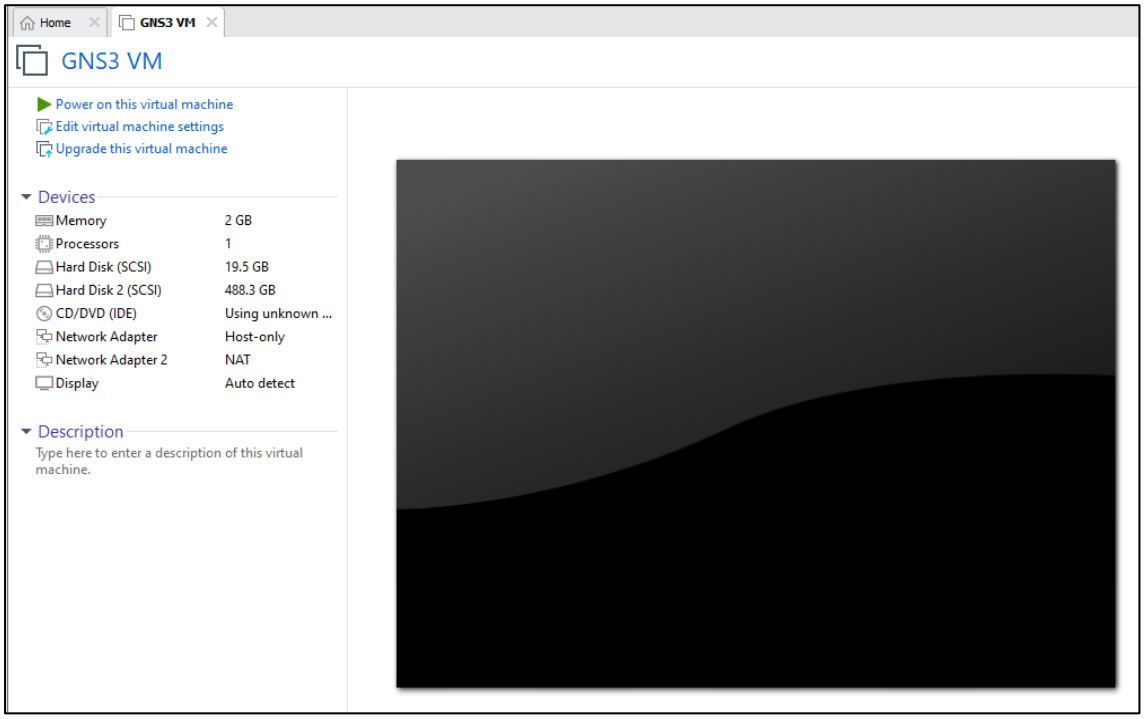






**Annexe 5 :** Importation de GNS3 VM sur VMware Workstation

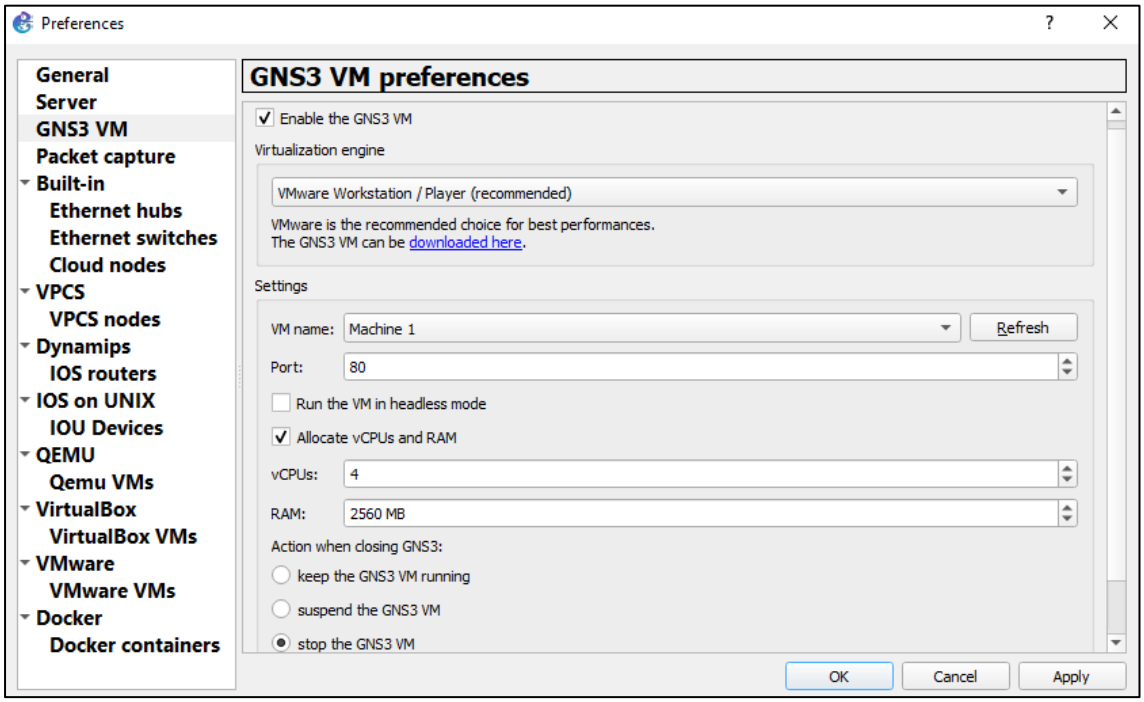
Sur la page d'accueil de VMware « home » on clique sur « open a virtual machine » pour ouvrir le GNS3 VM afin de créer une nouvelle machine virtuelle.



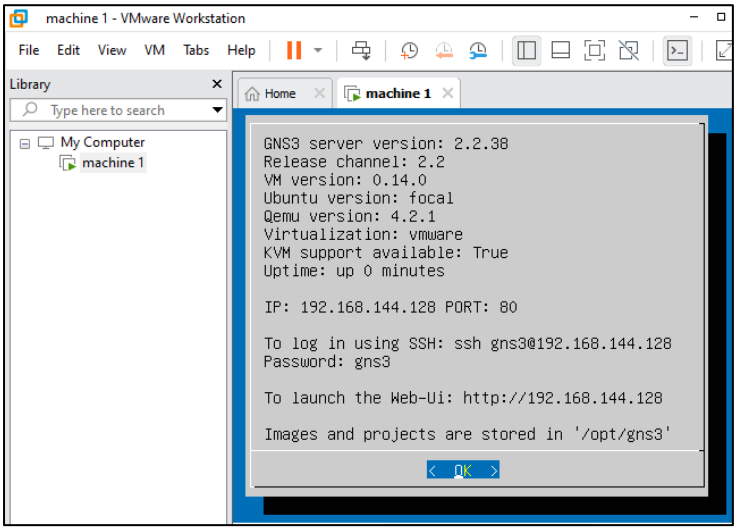


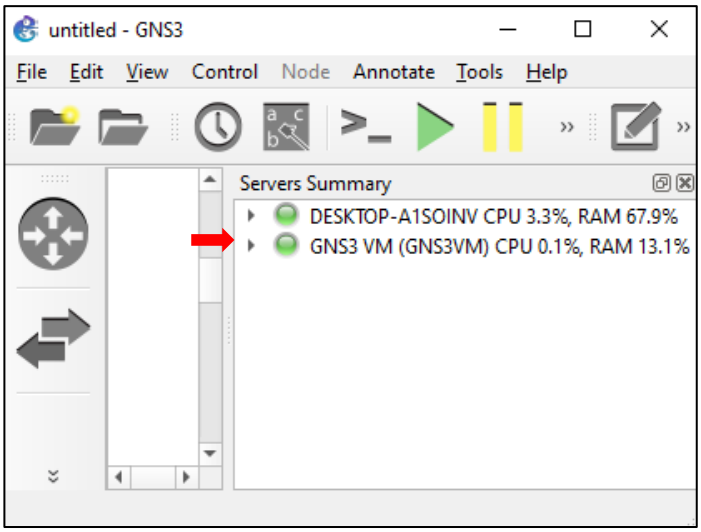

## **Annexe 6 :** Relier GNS3 au GNS3 VM importé sur VMware workstation

Sur GNS3 on clique sur « Edit » ensuite sur « Preferences » pour choisir GNS3 VM.




Lorsque on clique sur « applay » le programme GNS3 VM commence à fonctionner avec le GNS3.



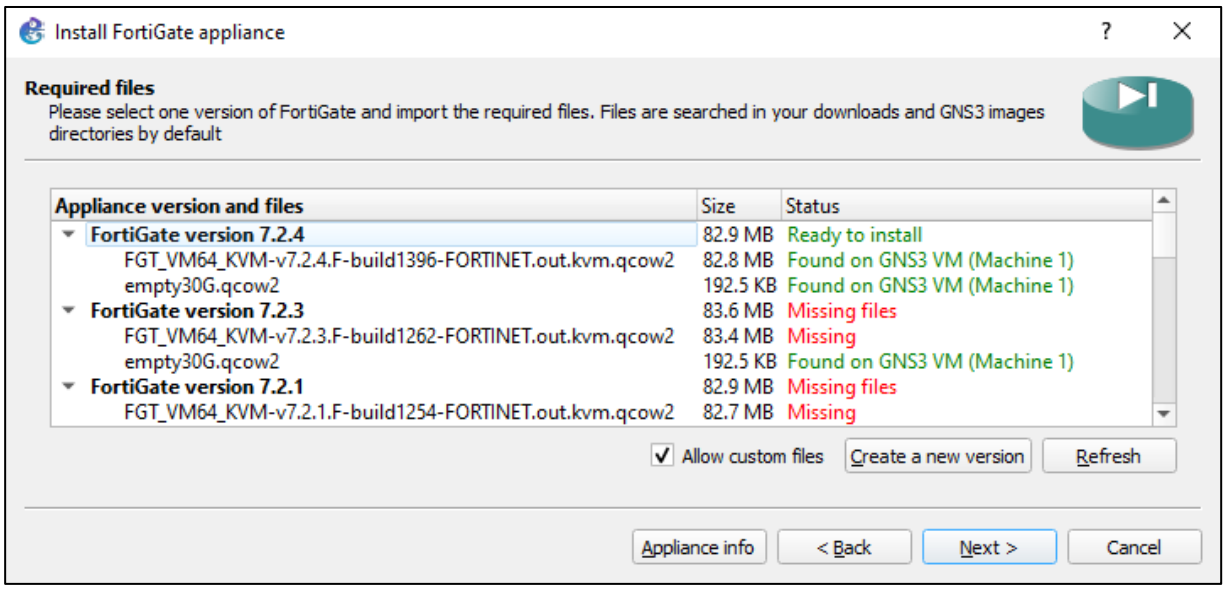



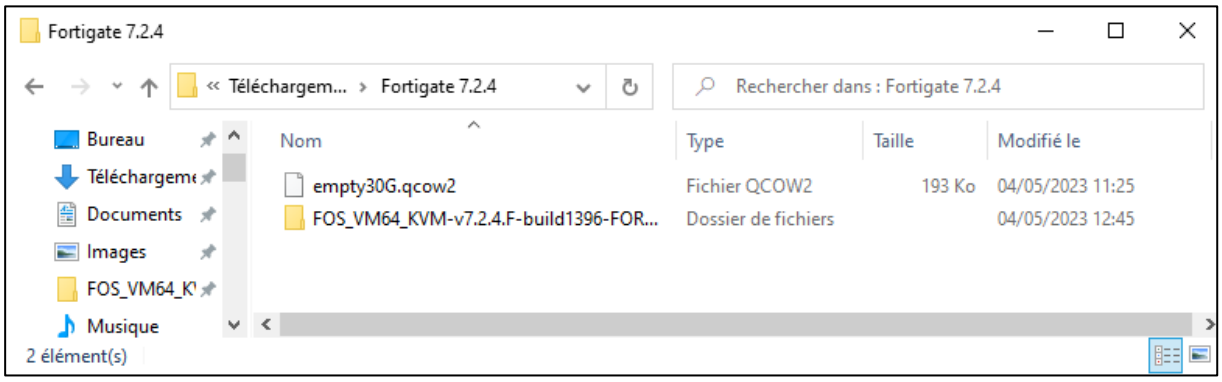

## **Annexe 7 :** Importation de pare-feu Fortigate 7.2.4 sur GNS3

L'image ISO de Fortigate est disponible sur les liens ci-dessous :

https://www.fortinet.com

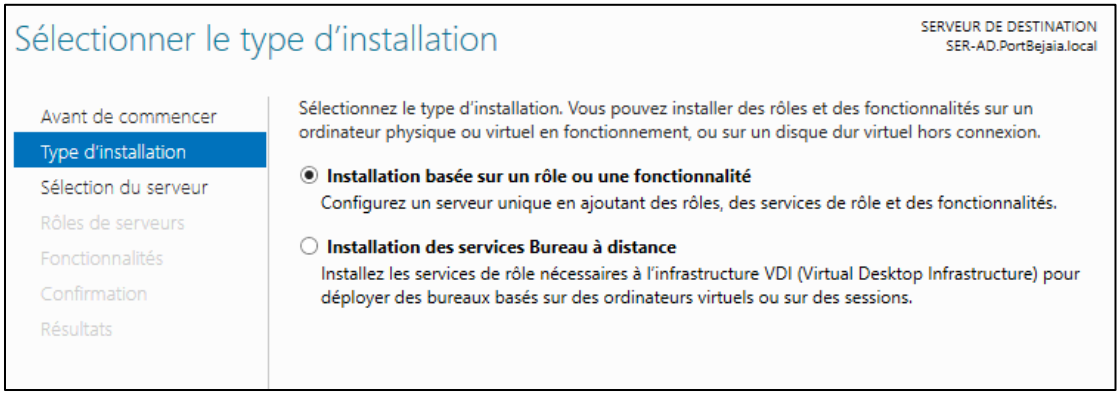
https://gns3.com/marketplace/appliances/fortigate

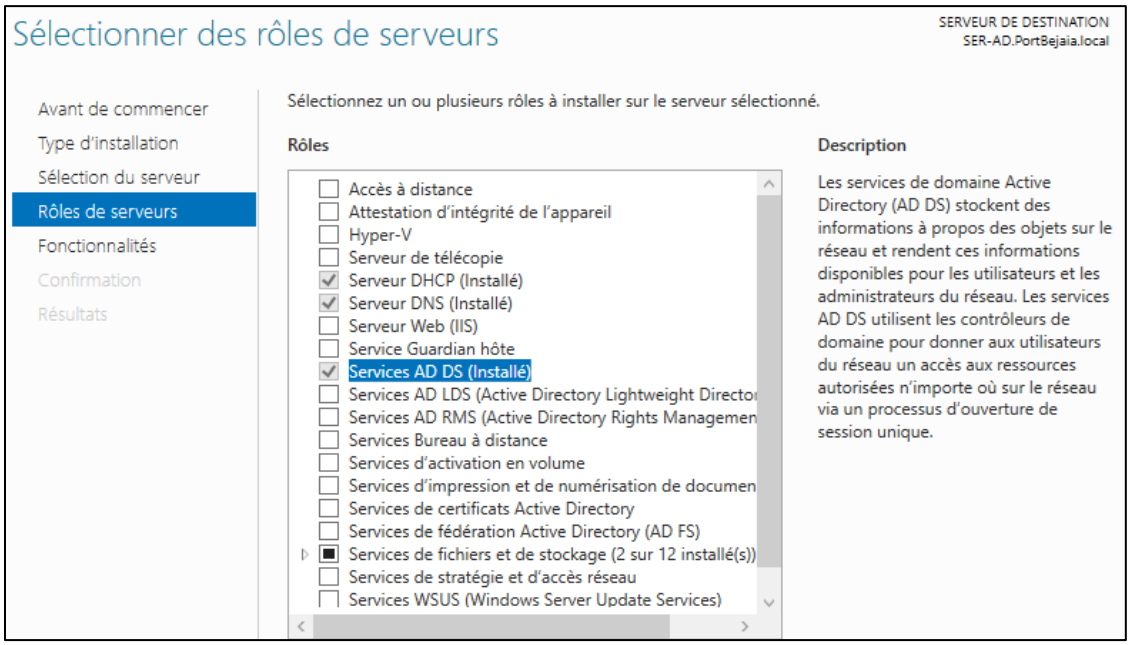


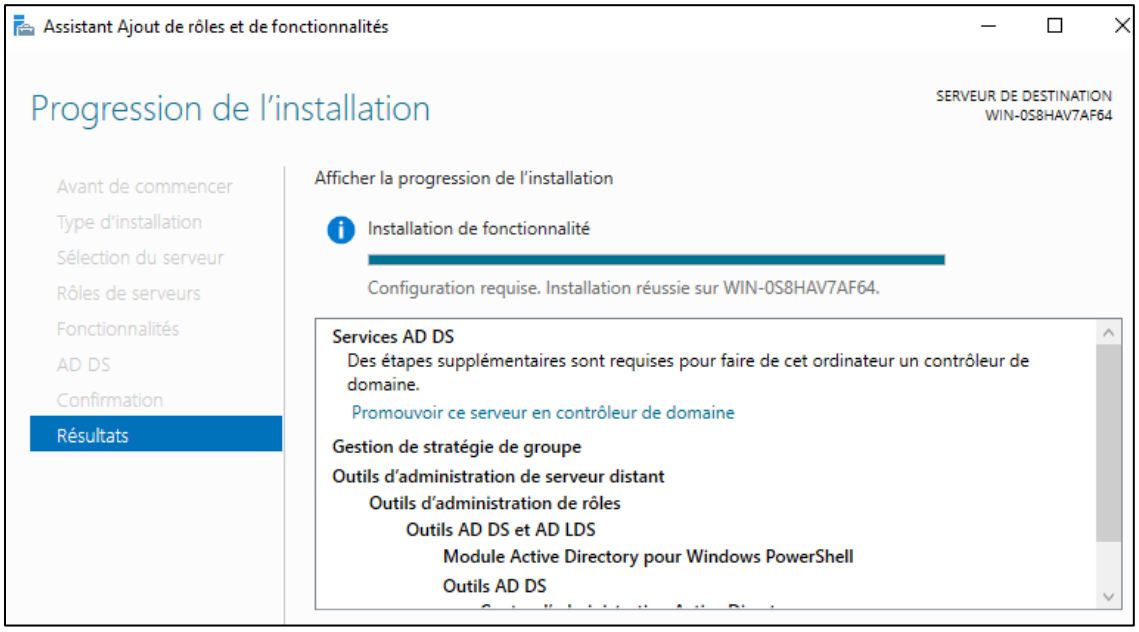



**Annexe 8 :** Installation de l'active directory

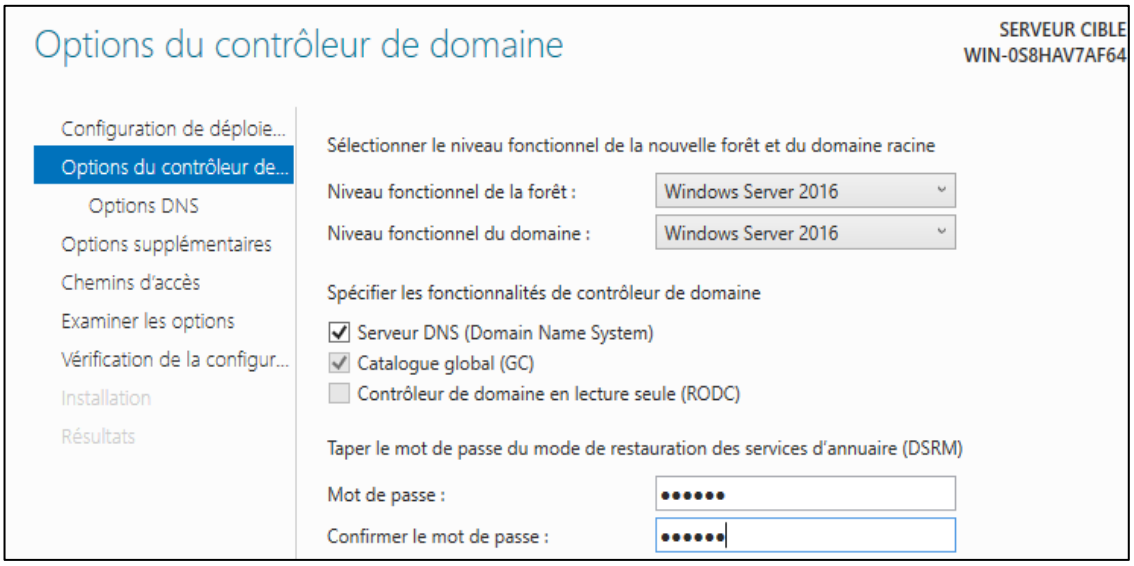
Nous allons suivre les étapes suivantes pour installer le service de domaine Active Directory sur Windows server 2022.

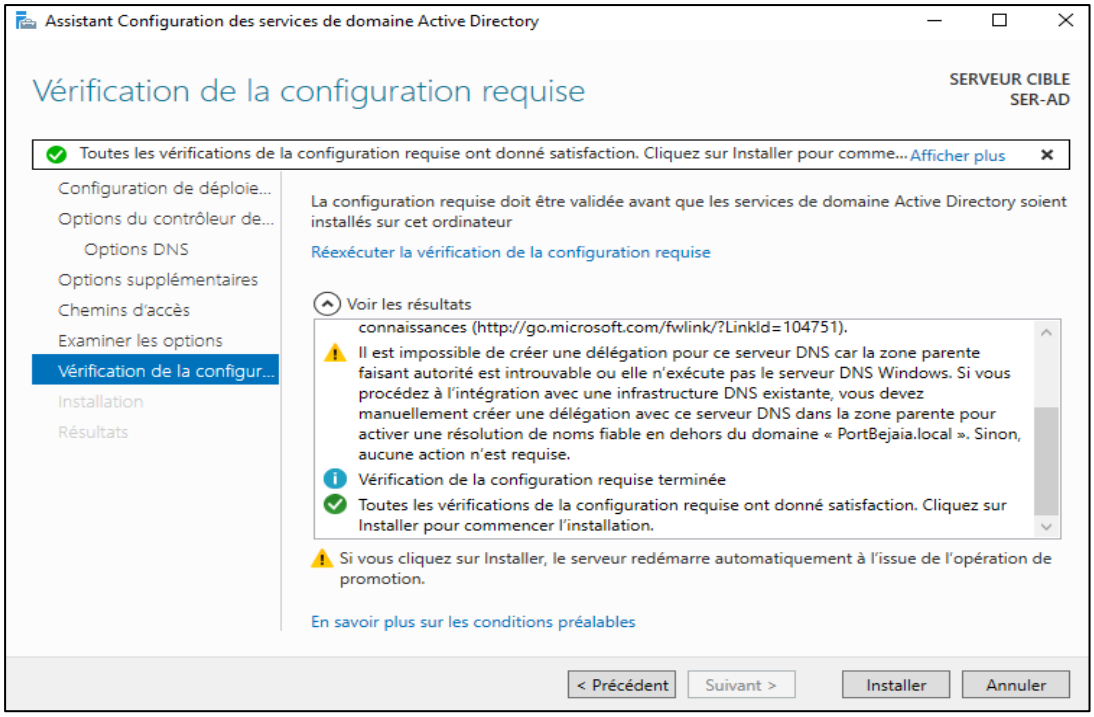



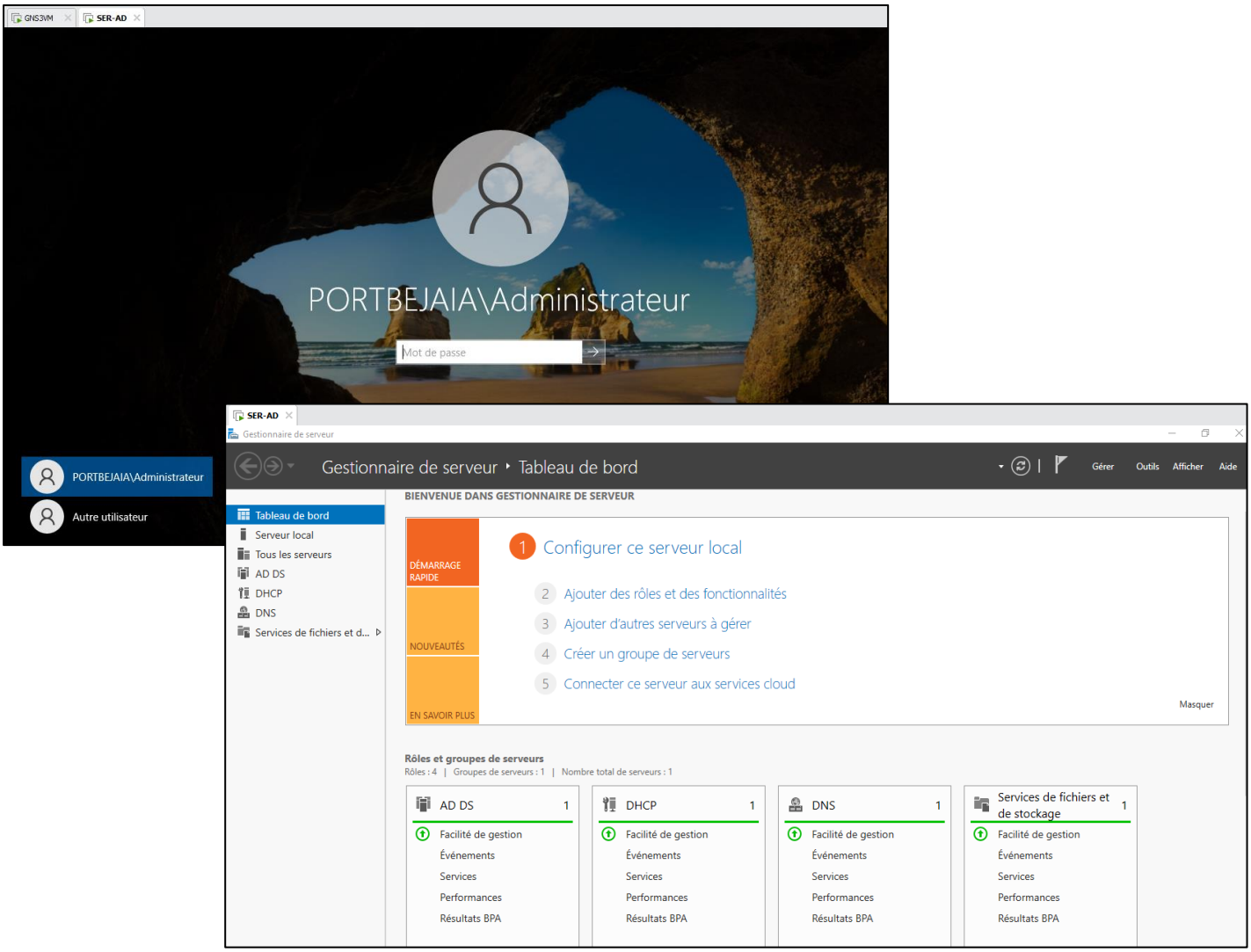




Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DESTINATION
WIN-0S8HAV7AF64
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats
Afficher la progression de l'installation
Installation de fonctionnalité
Configuration requise. Installation réussie sur WIN-0S8HAV7AF64.
Services AD DS
Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.
Promouvoir ce serveur en contrôleur de domaine
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS


Configuration de déploiement
SERVEUR CIBLE
WIN-0S8HAV7AF64
Configuration de déploie...
Options du contrôleur de...
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner l'opération de déploiement
Ajouter un contrôleur de domaine à un domaine existant
Ajouter un nouveau domaine à une forêt existante
Ajouter une nouvelle forêt
Spécifiez les informations de domaine pour cette opération
Nom de domaine racine :
PortBejaia.local


Options du contrôleur de domaine
SERVEUR CIBLE
WIN-0S8HAV7AF64
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine
Niveau fonctionnel de la forêt :
Windows Server 2016
Niveau fonctionnel du domaine :
Windows Server 2016
Spécifier les fonctionnalités de contrôleur de domaine
Serveur DNS (Domain Name System)
Catalogue global (GC)
Contrôleur de domaine en lecture seule (RODC)
Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)
Mot de passe :
Confirmer le mot de passe :


Assistant Configuration des services de domaine Active Directory
Vérification de la configuration requise
SERVEUR CIBLE
SER-AD
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
Installation
Résultats
La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Réexécuter la vérification de la configuration requise
Voir les résultats
connaissances (http://go.microsoft.com/fwlink/?LinkId=104751).
Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « PortBejaia.local ». Sinon, aucune action n'est requise.
Vérification de la configuration requise terminée
Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.
Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.
En savoir plus sur les conditions préalables
< Précédent
Suivant >
Installer
Annuler


GNS3VM
SER-AD
PORTBEJAIA\Administrateur
Mot de passe
PORTBEJAIA\Administrateur
Autre utilisateur
SER-AD
Gestionnaire de serveur
Gestionnaire de serveur ‣ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
DHCP
DNS
Services de fichiers et d...
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
1 Configurer ce serveur local
2 Ajouter des rôles et des fonctionnalités
3 Ajouter d'autres serveurs à gérer
4 Créer un groupe de serveurs
5 Connecter ce serveur aux services cloud
Masquer
Rôles et groupes de serveurs
Rôles : 4 | Groupes de serveurs : 1 | Nombre total de serveurs : 1
AD DS 1
DHCP 1
DNS 1
Services de fichiers et de stockage 1
Facilité de gestion
Événements
Services
Performances
Résultats BPA

# Bibliographie


1. Pujolle, G. Les réseaux. France : Eyrolles, 2014. p. 780.

2. Lohier, S et Present, D. Réseaux et transmission. France : Dunod, 2016. p. 328.

3. Jaquet, P. Les réseaux informatiques. 2015. p. 133.

4. Servin, C. Réseaux et télécommunications. 4. France : Dunod, 2013. p. 800.

5. Dromard, D et Seret, D. Architecture des réseaux. France : Pearson, 2009. p. 258.

6. Laissus, F. Introduction a TCP/IP. 2005. p. 282.

7. Philippe, J et Pillou, J-F. Tout sur la sécurité informatique. 4. France : Dunod, 2016. p. 271.

8. Boukharrou, R. Sécurité des réseaux. Constantine : s.n.

9. Guermouche, A. Les attaqueq. Sécurité des réseaux. 2019.

10. Aycock, J. Computer virus and malware. Amérique : Springer publishing, 2006. p. 248.

11. Goyal, M et Sharma, A. Survey on different kinds of malware and their detection. 2015.

12. Dufour, F. Clubic.com. qu'est-ce qu'un spyware et comment s'en protéger avec un antivirus. [En ligne] 2022.

13. Robert, J-M. Logiciels malveillants. Canada : s.n.

14. Roulot et Méjane. Le piratage de A à Z. France : Edigo Multimédia, 2010. p. 142.

15. Salem, O. Protection contre les attaques de déni de service dans les réseaux IP. ECTEI Parise : s.n.

16. https://www.ingecom.net/pt/blog/179/what-is-icmp-tunneling-and-how-to-protect-against-it/ . [En ligne]

17. Deswarte, Y et Mé, L. sécurité des réseaux et système répartis. s.l. : Eyrolles, 2002.

18. Lohier, S et Quidelleur, A. Le réseau internet des services aux infrastructures. Paris : Dunod, 2010. p. 376.

19. Howard. Qu'est-ce qu'un VLAN Privé et Comment Fonctionne-t-il . https://community.fs.com/fr/blog/what-is-private-vlan-and-how-it-works.html. [En ligne] 2022.

20. —. Explication du Voice VLAN : Base, Configuration et Question Fréquentes. https://community.fs.com/fr/blog/voice-vlan-configuration-guidelines-on-ethernet-switches.html. [En ligne] 2021.

21. https://www.cisco.com/c/fr_ca/support/docs/lan-switching/vtp/10558-21.html. [En ligne] Comprendre le protocole VTP, 2022.

22. Les VPN. http : //perso.modulonet.fr/placurie/ressources/bts2-amsi/chap8-lesvpn.pdf. [En ligne]

23. Steinberg, J. SSL VPN accès web et extranets sécurisés. s.l. : Eyrolles, 2006.

24. Florin, G. Cours de sécurité par-feux (firewall).

25. Postair, J-C et Aubel, A. Présentation de différent types d'architectures de Firewall.

26. Pronzato, M. Informatique et Réseaux : Les Firewalls. 2000.

27. Liu, A. Firewall design and analysis. 4. s.l. : World Scientific, 2011. p. 124.

28. Jacquemin, A et Mercier, A. https://www.fichier-pdf.fr/2014/07/29/les-firewalls/? Les Firewall. [En ligne] 2014.

# Résumé

Avec l'évolution des technologies Internet, les réseaux informatiques sont devenus un levier de croissance et de développement indispensable pour les entreprises.

Face à cette évolution et la multiplication des points d'accès au réseau, la sécurité devient de plus en plus importante pour le bon fonctionnement d'un réseau informatique, pour cela plusieurs mécanismes de sécurité ont été mis à la disposition des administrateurs afin de renforcer la sécurité de leur réseau

Notre travail consiste à la mise en place d'une architecture réseau sécurisée simulée sous GNS-3 pour l'entreprise Bejaia Mediterranean Terminal (BMT).

Afin de fournir un partage efficace de données, nous avons segmenté les réseaux en VLAN et nous avons réalisé différentes configurations sur le firewall FortiGate à savoir la mise en place de deux tunnels VPN basés sur le protocole IP sec, une haute disponibilité, une liste de contrôle d'accès, une zone démilitarisée et nous avons intégré les différends protocoles (HSRP, GLBP, PAGP, LACP, DHCP, VTP...) pour configurer nos réseaux.

**Mots clés :** sécurité réseau, BMT, LAN, CTMS, pare-feu, VLAN, VPN, IPsec, Fortigate, DMZ, HA, GNS3, VMware.

# Abstract

With the evolution of the Internet technologies, computer networks became an essential lever of growth and development for companies.

Faced to this development and the proliferation of network access points, security is becoming more important for the good functioning of the network, for this, several security mechanisms have been made available to administrators in order to strengthen the security of their network.

Our work consists in setting up a secure network architecture simulated under GNS-3 for the Mediterranean terminal company of Béjaïa.

To provide an excellent data sharing, we have segmented the network on VLAN, and we have made different configurations on Firewall Fortigate namely the establishment of the two VPN tunnels based on protocol IP sec, high availability, an access control list, a demilitarized zone, and we have integrated the different protocols (HSRP, GLBP, PAGP, LACP, DHCP, VTP …) to configure our networks.

**Keywords :** network security, BMT, LAN, CTMS, Firewall, VLAN, VPN, IPsec, Fortigate, DMZ, HA, GNS3, VMware.