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

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunication

Spécialité : Réseaux et Télécommunications

Thème

Etude et mise en œuvre d'une solution de sécurité réseau basée sur l'utilisation des pare-feu et les liaisons virtuels (cas :BMT).

Préparé par :

- LAOUHID Houria
- OULABAS Ines

Dirigé par :

- M.Diboune Abdelhani

Examiné par :

- Mme Zenadji (P)
- Mme K.Mammeri

Année universitaire : **2023/2024**

Remerciement

Tout d'abord, nous tennons à remercier Le bon Dieu de nous avoir donné la patience et la volonté pour accomplir ce travail.

Nos remerciements s'adressent également à notre promoteur ***M.DIBOUNE Abdelhani*** *pour ses conseils ,ses orientations pour nous avoir transmis les renseignements nécessaires à la réalisation de ce travail.*

Mes vifs remerciements vont aux membres de jury ***Mme ZENADJI (P)*** *et* ***Mme K.MAMMERIE*** *d'avoir accepté d'examiner notre travail. Nous remercions également L'organisme d'accueil BMT tout particulièrement le chef de service informatique,* ***M. BENALI Lyes****, pour avoir mis à notre disposition la place de déroulement de notre stage.*

En fin, nous remercions toutes personnes ayant contribué de près ou de loin à la réalisation de ce travail.

Dédicace

Je dédie ce mémoire :

A mes chers parents

Aux plus belles créatures que dieu a créés sur terre, a cette source de tendresse, de patience et de générosité. Aucune dédicace ne pourrait exprimer mon respect, ma considération et mes chaleureux sentiments envers mes chers parents, grâce à leurs tendres encouragements et leurs grands sacrifices, ils sont pu créer le climat affectueux et propice à la poursuite de mes études. Je prie le bon lieu de les bénir, de veiller sur eux, en espérant qu'ils soient toujours fiers de moi.

A mon cher ami et mari Mehdi

Je te remercie pour ton amour inconditionnel et ta patience tout au long de ce parcours. Tes conseils avisés et ton soutien indéfectible ont été ma bouée de sauvetage dans les moments de doute. Ce mémoire est autant le fruit de mon travail que le tien. Que dieu te garde pour moi.

A mon très cher frère Marwan et à mes adorables sœurs : Samira, Hakima, Malika et rebiha

Puisse dieu, le très haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

A tous les membre de la famille laouhid et Itim

A toutes mes copine Marwa, Samra, Lamia, nada, Sabrina, Melissa, Kenza ,djihane, Amel, Katia… merci à toutes mes amies avec qui ont partagée des moments de ma vie au fil du temps.

A ma binôme INES je te souhait une vie pleine de sante et de bonheur.

Houria

Dédicace

Je dédie ce modeste travail :

A mes très chers parents

Aucune dédicace ne saurait exprimer l'affection et l'amour que j'ai pour vous.

Je prie le bon dieu de les garder en bonne santé pour une langue vie et m'aider à être toujours leur fierté.

A mes frères A mes sœurs

A ma binôme Houria avec qui j'ai eu grand plaisir à partager cette expérience

Ines

Table des matières

Chapitre III : Présentation de l'organisme d'accueil et contexte du projet

Chapitre IV : Simulation et réalisation

Liste des tableaux

Liste des figures

Liste des listings

Liste des abréviations

A

ACL Access Control List

AH Authentification Header

B

BMT Béjaia Mediterranean Terminal

BMT Spa Béjaia Mediterranean Terminal Société Par Action

C

CDMA/CD Carrier Sense Multiple Access / Collision Detection

CDN Centre Digitalisation et Numerique

CHAP Challenge Handshake Authentification Protocol

CTMS Container Terminal Management System

D

DHCP Dynamic Host Configuration Protocol

DH Diffie-Hellman

DMZ DeMilitarized Zone

DNS Domain Name System

DOS Denial of Service

DDOS Distributed Denial of Service

E

EPB Entreprise portuaire de Bejaia

ESP Encapsulated Security Payload

F

FAI Fournisseur d'Accès Internet

FDDI Fiber Distributed Data Interface

FTP File Transfer Protocol

FTPs	File Transfer Protocol Secure

G

GNS3	Graphical Network Simulator-3
GRE	Generic Routing Encapsulation

H

SRP	Hot Standby Redundancy Protocol.
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol Secure

I

ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISO	International Stendard Organisation

L

LACP	Link Aggregation Control Protocol
LAN	Local Area Network
L2TP	layer 2 forwarding tunneling protocol

M

MAC	Medium Access Control
MAN	Metropolitan Area Network
MAU	Multiple Access Unit
MD5	Message Digest 5
MITM	Main In The Middle
MPLS	Multi-P rotocol Label Switching
MPPE	Microsoft Point-to Point Encryption

N

NAT	Network Address Translation

O

OSI	Open Systems Interconnection

P

PAN	Personal Area Network
PPP	Point to Point Protocol
PPTP	point to point tunneling Protocol
PVLAN	Private Virtual local area network

S

SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Socket Shell
SSL	Transport Layer Security
SYN/ACK	Synchronize, cknowledge

T

TCP	Transmission Control Protocol
TelNet	Terminal Network

U

UDP	User Datagram Protocol
UTM	Unified Threat Management

V

VLAN	Virtual local area network
VPN	Virtual Private Network
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

A l'aire de la numérisation et de mondialisation, les entreprises dépendent de plus en plus des réseaux informatiques pour assurer une communication rapide, fiable et sécurisé entre leurs différents unités et utilisateurs. Cette interconnectivité permet non seulement un échange efficace de données, mais également une continuité des services sur des grandes distances. Toutefois, cette dépendance accrue s'accompagne de défis majeurs en matière de sécurité. Les cybermenaces se multiplient et deviennent de plus en plus sophistiquées, nécessitant des stratégies de protection robustes et évolutives.

Les pares-feux, les réseaux privés virtuels (VPN), les VLAN, les antivirus, les serveurs proxy et les systèmes de détection d'intrusion font partie des technologies de sécurité essentielles pour protéger les réseaux de communication des attaques. Parmi ces solutions, les pares-feux jouent un rôle crucial en agissant comme une première ligne de défense, filtrant le trafic et bloquant les accès non autorises.

Dans ce contexte, notre projet de fin d'étude se concentre sur la mise en œuvre d'une sécurité réseau basée sur l'utilisation des pares-feux, avec une intégration de VPN IPSec (Internet Protocol Security), au sein de l'entreprise BMT (Bejaia Mediteranean Terminal).

Durant notre stage , nous avons réalisé une analyse approfondie du réseau de BMT afin d'identifier ses principales vulnérabilités .Sur cette base , nous avons proposé et mise en place une architecture réseau améliorer comprenant la configuration des VLAN pour une segmentation sécurisée des sous-réseaux , la reconfiguration des pare-feu pour optimiser leur performance , et l'isolement des applications web dans une zone démilitarisée (DMZ) gérée par des pare-feu .en outre nous avons implémenté un VPN IPSec pour sécuriser les communications entre les sites distants de l'entreprise et mise en place un pare-feu secondaire pour assurer une haute disponibilité.

Afin de présenter notre travail, nous avons structuré notre mémoire comme suit :

- Le premier chapitre est consacré aux généralités sur le réseau de communication en citant les différents grands piliers de ce dernier et les différentes attaques qu'il subit.
- Dans le second chapitre nous décrivant les différentes techniques de sécurité d'un réseau.

- Le troisième chapitre représente l'organisme d'accueil BMT et l'étude effectué durant notre stage au sein de cette entreprise.
- En fin le quatrième chapitre, décrira la partie pratique de notre travail ou nous avons défini les différents outils et logiciel ayant servi à réaliser notre implémentation, puis on a expliqué les configurations établies ainsi que les tests effectués pour vérifier nos simulations.

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

Chapitre I

Généralité sur les réseaux de communication et leurs attaques

Introduction

Aujourd'hui les réseaux sont omniprésents et ils dominent la vie dès L'évolution des réseaux a passé d'une simple interconnexion des terminaux avec des gros ordinateurs a une vaste interconnexion des ordinateurs personnels et des grands serveurs dispersés sur toute la planète.

Dans ce chapitre nous allons commencer par présenter des notions de base sur les réseaux decommunication dans lesquels en abordant leurs classifications et leur architecture (modèle OSIet modèle TCP/IP).

1.1. Généralités sur les réseaux de communication :

1.1.1. Définition d'un Réseau de communication :

Un réseau de communication peut être défini comme l'ensemble des ressources matériels et logiciels liées à la transmission et l'échange d'information entre différentes entités suivant leur organisation, ou architecture, les distances, les vitesses de transmission et la nature des informations transmises, les réseaux font l'objet d'un certain nombre de spécifications et de normes.

1.1.2. Utilisation des réseaux de communication :

Les moyens de communication ont révolutionné notre manière d'interagir et de communiquer à l'échelle mondiale. Ils occupent une place primordiale dans notre vie quotidienne et permettant une connectivité instantanée entre les individus, les organisations et les communautés, parmi leurs utilisations on trouve :

- Partage de ressources (logique, physique).
- Echange des données et communication entre personnes.
- Accès à des services distants.
- Permet de partager des connaissances et des expériences et pourquoi pas de se placer comme mentor.

1.1.3. Classification des réseaux :

On peut distinguer différent type de réseaux selon plusieurs critères tel que l'étendu, la topologie, et le mode de communication.

1.1.3.1. Classification selon l'étendu :

Est la classification la plus utilisée et la Plus citée qui répertorie les réseaux selon la taille géographique. Généralement, cette classification définit quatre classes de réseau.

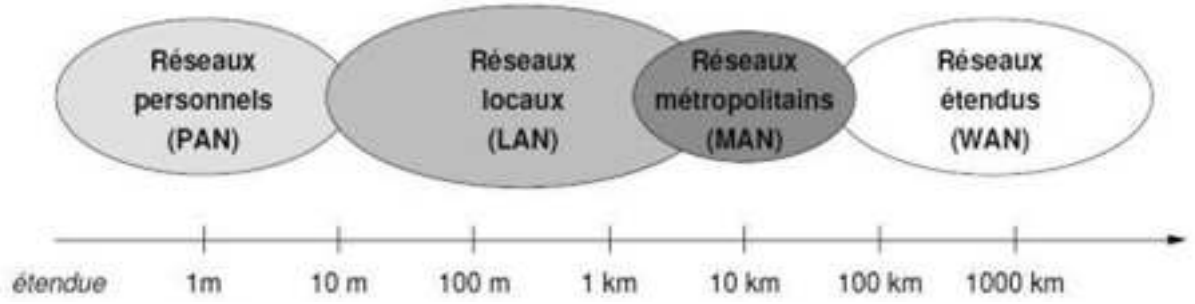


Figure 1. 1 : La taille des différentes catégories de réseau informatique [1].

a) Les réseau personnels (Personal area network : PAN) : Il désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le Personal Operating Space (POS). Deux autres appellations de ce type de réseau sont réseau individuel et réseau domestique [2].

b) Réseau local (Local Area Network :LAN) : de taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, relie entre eux des ordinateurs, des serveurs, … il est couramment utilisé pour le partage de ressources communes comme des périphériques, des données ou des applications [2].

c) Le réseau métropolitain (Metropolitan Area Network : MAN) : est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaisonprivée ou non, différents bâtiments distants de quelques dizaines de kilomètres [2].

d) Le réseau étendu (Wide Area Network : WAN) :

les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier.Le WAN le plus célèbre est le réseau public internet dont le nom provient de cette qualité ; interNetworking ou interconnexion de réseaux [2].

1.1.3.2 Classification selon la topologie :

La topologie du réseau de communication correspond à l'architecture de celui-ci, définissant les liaisons entre les équipements de réseau et une hiérarchie éventuelle entre eux. Elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau. Les topologies peuvent être classées en deux types de la manière la plus fondamentale : la topologie physique et la topologie logique.

a) La topologie physique : elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau. Les topologies classiques les plus utilisées sont présentées dans la figure suivante :

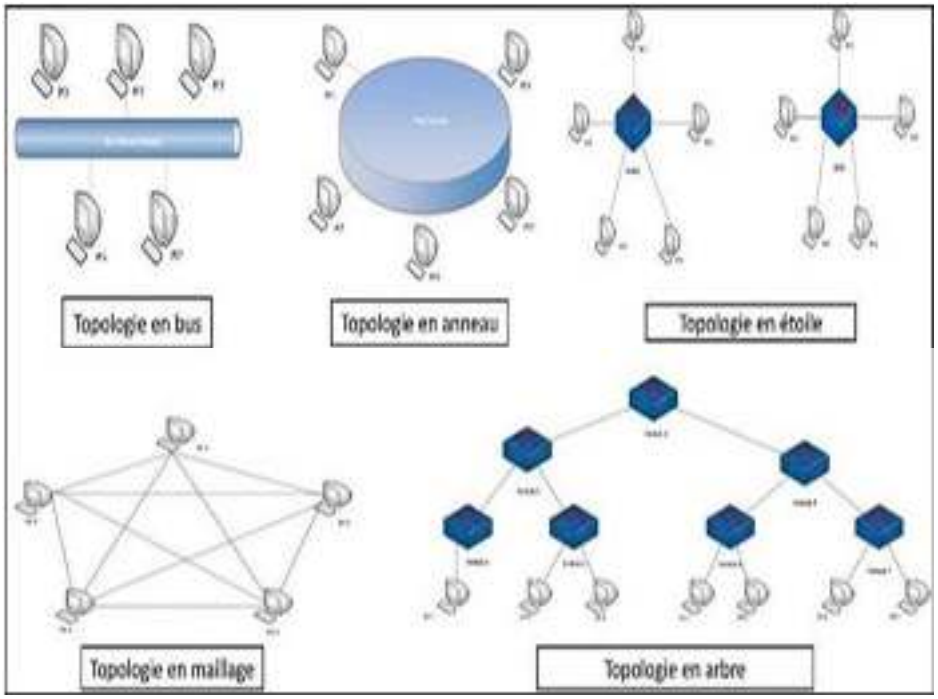


Figure 1. 2 : les topologies physiques

b) La topologie logique : Par opposition à la topologie physique, elle représente la façon dont les données transitent dans les lignes de communication. Elle gère :

- Discipline de ligne
- Notification d'erreur
- Contrôle optimal du flux

Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI .

- **La topologie Ethernet :** Ethernet (aussi connu sous le nom IEEE802.3) désigne une technologie qui permet aux dispositifs des réseaux de données câbles de communiquer entre eux. Les appareils connectés dans un réseau Ethernet peuvent former un réseau et échanger des paquets de données. De cette façon un réseau local (LAN) est créé via des connexion Ethernet. Chaque appareil d'un réseau Ethernet dispose de sa propre adresse MAC (48 bits).

Les membres de ce réseau partagé peuvent transmettre des messages à haute fréquence. Cette topologie utilise des techniques de bande de base et de multiplexage.

L'algorithme CSMA/CD (Carrier Sense Multiple Access/Collision Detection) est utilisé pour gérer l'accès au canal [3].

- **La topologie Token Ring :** le Token Ring ou anneau à jeton (norme IEEE 802.5) est une topologie de réseau associée à un protocole de réseau local qui fonctionne sur la couche « liaison » du modèle OSI (toutes les autres normes citées dans cette section fonctionnent sur les couches 1 et 2 du modèle OSI).

Le protocole utilise une trame spéciale de trois octets, appelée jeton, qui circule dans une seule direction autour d'un anneau. Les trames token ring parcourent l'anneau dans un sens qui est toujours le même [4].

- **La topologie FDDI :** est un type de réseau informatique LAN ou MAN permettant d'interconnecter plusieurs LAN à une vitesse de 100 Mbit/s de la fibre optique (ce qui lui permet d'atteindre une distance maximale de 200 km [5].

1.1.3.3. Classification selon le mode de communication :

On distingue généralement deux types de réseaux très différents en fonction de la nature des relations entre les sites, mais ils partagent des similitudes, ils sont :

a) Réseau client /serveur : Dans une architecture client-serveur des applications de machine dites clientes communiquent avec des applications de machines dite serveurs. Un exemple d'une architecture client-serveur est le navigateur Web d'un client qui envoie des requêtes http(s) à un serveur Web qui répond en envoyant la page Web demandée (voir la figure 1.3).

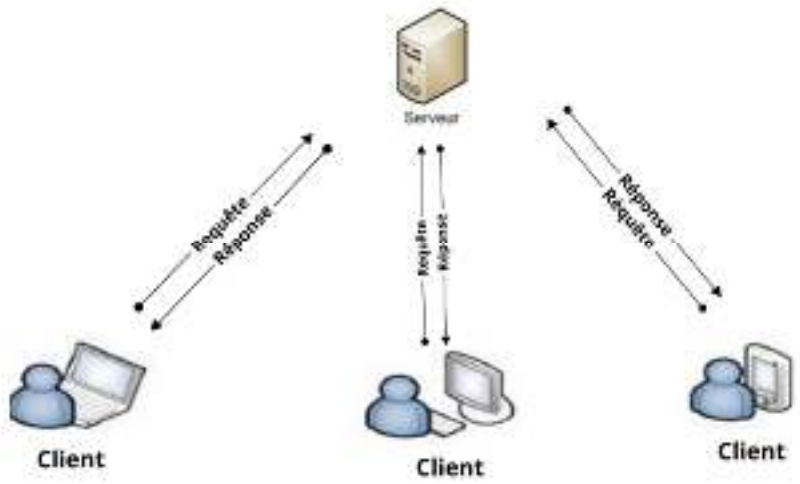


Figure 1. 3 : architecture client/serveur

b) Réseau poste à poste : une architecture réseau est dite Pair-à- Pair (Peer-to-Peer : P2P) s'il n'y a pas de serveurs dédiés, chaque nœud (machine) est à la fois client/serveur. C'est un modèle de réseau informatique ou chaque ordinateur participant agit à la fois comme clients etserveur, permettant ainsi le partage direct de fichier et de ressources entre les utilisateurs sans passer par un serveur centralisé.

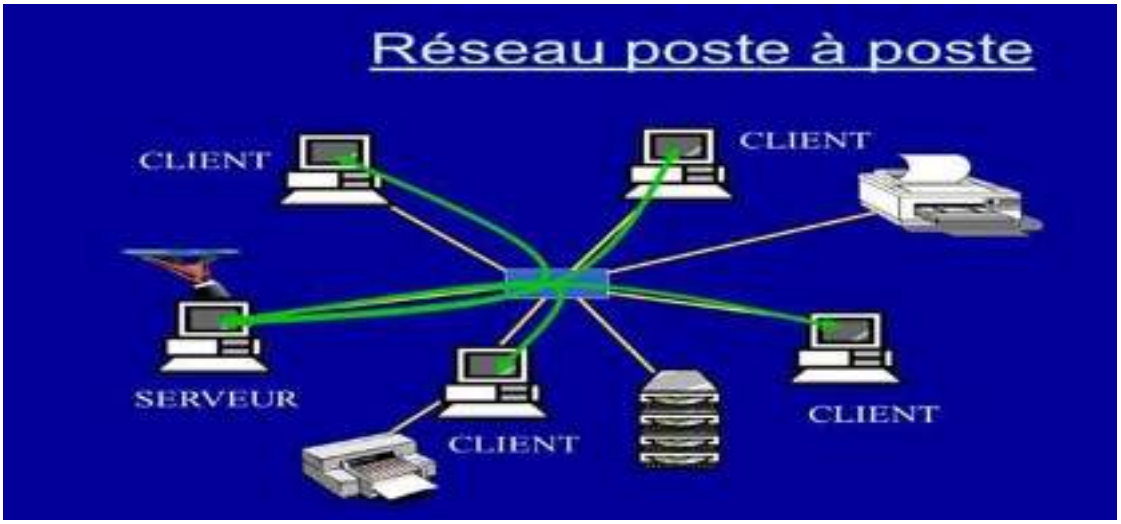


Figure 1. 4 : Architecture poste à poste

1.2. Les Modèle d'architecture réseau :

Il existe deux types de bases de modèles de réseau : le modèle de référence (OSI) et le modèle d'application (TCP/IP) :

1.2.1. Modèle OSI :

L'ISO (international Standard Organization) a développé une norme pour l'interconnexion des systèmes ouverts appelée OSI (open système interconnexion). Cette architecture hiérarchique, connue sous le nom « ISO/OSI », est composée de sept couches distinctes remplissant chacune une partie bin définie des fonctions, nécessaires à l'interconnexion.

Le modèle OSI décrit des niveaux de transmission, mais non les protocoles proprement dits. Il divise l'ensemble des protocoles en sept couches indépendantes entre lesquelles sont définis deux types de relation :

- Les relations verticales entre les couches d'un même système (interfaces).
- Les relations horizontales relatives au dialogue entre deux couches de même niveau (les protocoles).

Le rôle de ces couches est donné dans le tableau ci- dessous :

Tableau 1. 1 : les différentes couches du modèle OSI

C7 : Application	➢ Est le point d'accès aux services réseaux
C6 : Présentation	➢ La mise en forme des données, la conversion des codes, le cryptage et la compression des données.
C5 : Session	➢ Organise et synchrone les échanges entre taches distantes. ➢ Gestion des transactions entre application distantes ➢ Définition des points de reprise.
C4 : Transport	➢ Garantir l'intégrité des données. ➢ Transfert de bout en bout des informations. ➢ Assurer un transfert fiable
C3 : Réseau	➢ Gere les connexions entre les nœuds du réseau. ➢ Adressage logique ➢ Routage des paquets contrôle de congestion ➢ Adaptation des tailles des blocs aux capacite des réseaux physiques
C2 : Liaison de données	➢ Méthode d'accès au canal ➢ Délimitation de la trame ➢ Le maintien de la connexion logique, le transfert des blocs de donnée, la détection et la correction des erreurs
C1 : Physique	➢ Responsable de la transmission des Signaux. Connecteurs, câblages, Codage.

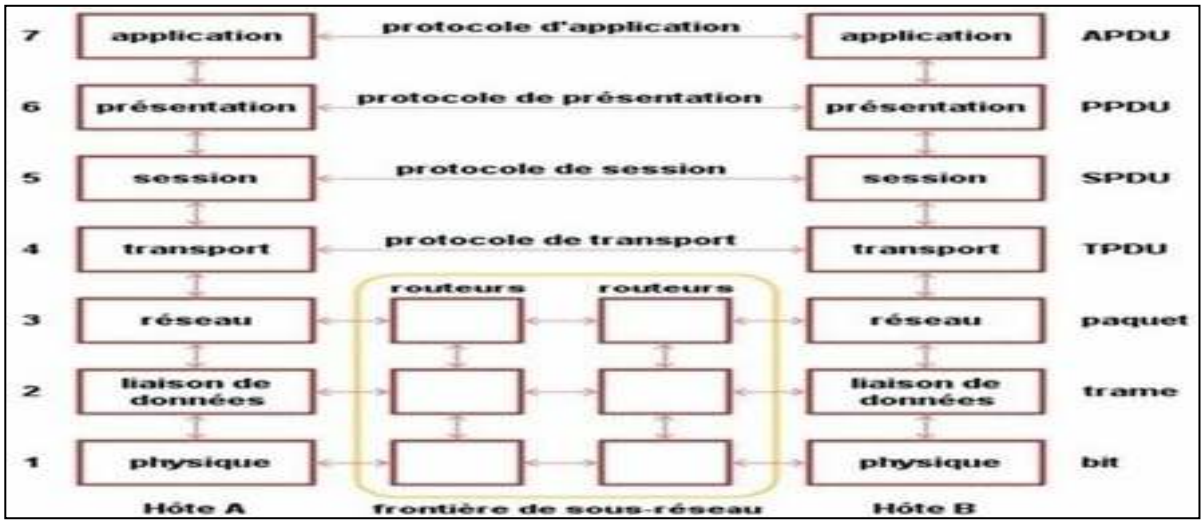


Figure 1. 5 : Le modèle OSI [6].

1.2.2. Principe architectural

Les modèles OSI (Open System Interconnexion) et TCP/IP (Transmission Control Protocol / Internet Protocol) sont deux modèles de référence pour la communication des

données en réseau. Ils définissent tous deux des couches et des protocoles qui permettent de communiquer entre les ordinateurs.

Précédant le modèle OSI, TCP en diffère fortement, non seulement par le nombre de couches, mais aussi par l'approche. Le modèle OSI spécifie des services (approche formaliste), TCP/IP des protocoles (approche pragmatique). Développé au-dessus d'un environnement existant, TCP/IP ne décrit, à l'origine, ni de couche physique ni de couche liaison de données.

Les applications s'appuient directement sur le service de transport. L'architecture TCP/IP ne comprend que 4 couches : la couche transport (TCP) et la couche inter réseau (IP). Le tableau suivant compare les deux architectures.

Tableau 1. 2 : comparaison entre modèle OSI et le modèle TCP/IP.

Modèle OSI	Modèle TCP/IP	Exemples de protocoles TCP/IP
Application Présentation Session	Application	NFS, NIS, DNS, LDAP, telnet, FTP, rlogin , rsh , rcp ,RIP,RDISC,SNMP …
Transport	Transport	TCP, UDP, SCTP
Réseau	Internet	IPv4, IPv6, ARP, ICMP
Liaison de données Physique	Accès réseau	PPP, IEEE 802.2

1.3. Sécurité des systèmes informatique SSI :

Avec l'avènement de la technologie et de l'Internet, le vol d'information numérique s'est largement répandu nous avons donc mis en place des mesures de sécurité pour protéger nos systèmes informatiques. La SSI aussi appelé cyber sécurité, est l'ensemble des mesures techniques et organisationnelles, juridiques et humaines nécessaires pour prévenir l'utilisation

non autorisée, le mauvais usage, la modification ou le détournement du système informatique. Assurer la sécurité du système informatique relève du management du système d'information.

La sécurité réseau est l'un des types de sécurité informatique. Comprends toutes les techniques de sécurité informatique pour protéger un réseau. Autrement dit est l'ensemble des moyens mise en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles .il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regarde delà sécurité [7].

1.3.1. Terminologie de la sécurité :

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

- **Vulnérabilité :**

Le terme « vulnérabilité » définit toutes les failles d'un système informatique pouvant être exploitées par des menaces à des fins malveillantes.

On peut cependant le classer dans trois catégories différentes [8] :

a) Les vulnérabilités de management : la mauvaise gestion d'un système informatique peut entraîner des vulnérabilités dans celui-ci. Ces vulnérabilités seront par la suite utilisées par des menaces pour endommager notre système.

b) Les vulnérabilités physiques : c'est à dire les accidents, les pannes ou les dégradations volontaires de matériels.

c) Les vulnérabilités technologiques : c'est la catégorie de vulnérabilités la plus conséquente, car elle comprend toutes les failles liées à l'utilisation des logiciels, des applications ainsi qu'à celle de nouveaux produits.

- **Menace :** les menaces sont susceptibles de transformer des vulnérabilités en attaques contre des systèmes informatique, des réseaux, etc. ils peuvent mettre en danger les systèmes informatiques individuels et les ordinateurs professionnels, de sorte que les vulnérabilités doivent être corriger afin que les attaquants ne puissent pas s'infiltrer dans le système et causer des dommages [9].

- **Risque :** est la probabilité qu'une menace donnée puisse exploiter une vulnérabilité au système données [10].
- **Contre mesure :** ce sont les méthodes de contrôle implémentées dans un système informatique pour diminuer ou éliminer le risque.
- **Attaque :** une attaque informatique est une action délibérée visant à exploiter les vulnérabilités d'un système, d'un réseau ou d'une application dans le but de compromettre son intégrité, sa confidentialité ou sa disponibilité.

1.3.2. Les critères de la sécurité d'un réseau :

Quelle que soit la nature du réseau, sa politique de sécurité vise à satisfaire les propriétés suivantes [11] :

- **La confidentialité des données :** est une exigence importante dans la sécurité du réseau. Elle permet d'assurer qu'une communication de données reste entre un émetteur et un destinataire.la cryptographie ou le chiffrement des données est la seule solution fiable pour sécuriser le transfert des données.
- **L'intégrité des données :** l'intégrité peut être vue comme un ensemble de mesures garantissant la protection des données contre les modification et altérations non autorisées. On peut distinguer les altérations accidentelles dues à l'environnement dur de communication, par exemple une mauvaise couverture des ondes, et les altérations volontaires d'un attaquant. Cela concerne aussi la protection contre l'injection ou a modification des paquets.
- **Disponibilités :** est un service réseau qui donne une assurance aux entités autorisées d'accéder aux ressources réseaux avec une qualité de service adéquate.
- **Non-répudiation :** mécanisme permettant de garantir d'un message a bien été envoyé par un émetteur et reçu par un destinataire, c'est à dire aucun des correspondants ne pourra nier l'envoi ou la réception du message.
- **Traçabilité :** se réfère aux mesure mises en place pour suivre et enregistrer les activités et les évènements sur un réseau informatique. Cela inclut généralement la collecte d'information sur les connexions réseau, les tentatives d'accès non autorisé, les modifications de configuration et d'autre actions susceptibles d'affecter la sécurité du réseau. La traçabilité permet de détecter les violations de sécurité, de comprendre comment elles se produisent et de prendre des mesures correctives appropriées.

1.3.3. Les attaques :

Les attaques informatiques sont devenues courantes dans le monde numérique contemporain, mettant en danger la confidentialité, la disponibilité des donné et des systèmes informatiques.

1.3.3.1. Définition d'une attaque :

Une attaque informatique est une action délibérée visant à exploiter les vulnérabilités d'un système, d'un réseau ou d'une application dans le but de compromettre son intégrité, sa confidentialité ou sa disponibilité.

1.3.3.2. Les types d'attaque :

Les risque de cybersécurité peuvent être classés en deux types généraux : les attaques passives et actives [12].

a) **Attaque passive :** lors d'une attaque passive, aucune modification de données n'a lieu et la cible n'a pas conscience qu'elle se produit, à moins qu'elle ne dispose d'un système de surveillance et de protection des identités des machines.

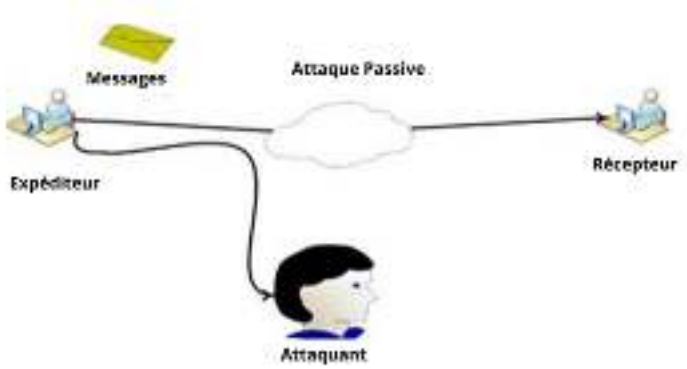


Figure 1. 6 : Attaque passive

b) **Attaque active :** lors d'une attaque active, les ressources et les données d'un système sont modifiées, voire endommagées afin d'altérer son fonctionnement normal. Bien que l'utilisateur soit susceptible de détecter ce type d'attaque, il est

difficile de déterminer leur cause première sans surveiller et protéger l'identité des personnes et des machines.

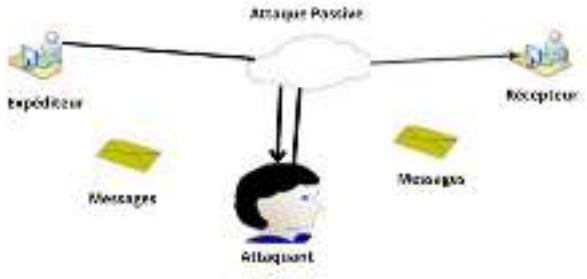


Figure 1. 7 : Attaque active

1.3.3.3. Les attaques selon la couche TCP/IP :

Afin d'élaborer des solutions de sécurité réseau efficaces, il est indispensable de comprendre en profondeur les différentes attaques qui menacent un système. Ces attaques, diverses dans leur nature, visent les différentes couches du modèle TCP/IP, ce qui nécessite une évaluation complète de leurs mécanismes. Pour mettre au point des contre- mesures robustes et adaptées à chaque niveau du réseau, il est crucial d'analyser en profondeur ces menaces [13].

1.3.3.3.1. Attaque sur la couche applicative :

a) Le craquage de mots de passe : Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide :

- D'un dictionnaire des mots de passe les plus courants (et de Leur variantes).
- Password craking (attaque de brute force) ou bien la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

b) Password sniffing : déploiement d'un dispositif de capture de mots de passe cette technique implique l'installation d'un renifleur sur une machine pour scruter l'ensemble du trafic réseau entrant et sortant.

Son objectif et d'intercepter et d'enregistrer les mots de passe circulant au sein d'un réseau. Cette attaque tire principalement avantage des vulnérabilités de protocoles tels que FTP,

http, TELNET, et SMTP, ou les mots passe et les données sont souvent transmis en texte clair, facilitant ainsi leur récupération

c) **Malwares :** on appelle malware (ou programme malveillant, maliciel) un programme ou une partie de programme destine à perturber, altérer ou détruire tout ou partie des éléments logiciels indispensables au bon fonctionnement d'un système informatique [13].

Il existe plusieurs types de malware on cite l'essentiel ci-dessous :

- **Les virus :** les virus sont des programmes malveillants qui ont pour but de se reproduire. Souvent, ils sont gênants pour l'utilisateur, puisqu'ils peuvent détruire des fichiers sur l'ordinateur [15].
- **Les vers (les Worms) :** les vers figurent parmi les plus anciennes menaces informatiques. Un ver, c'est un logiciel malveillant qui circule sur toute la planète par l'intermédiaire des connexions réseaux. Ils exploitent les failles de sécurité pour s'insérer dans une machine. Contrairement aux virus, les vers informatiques n'ont pas besoin d'être lies à un programme exécutable, ils se déplacent de façon autonome [16].
- **Ransomware :** une menace répandue parmi les malwares, se caractérise par le chiffrement des données, bloquant ainsi l'accès à un système. L'attaquant demande à la victime d'envoyer de l'argent en échanges de la clé qui permettra de les déchiffrer [13].
- **Le cheval de Troie :** (Trojan Horse) n'est ni un virus ni un ver, parce qu'il ne se reproduit pas. Il introduit sur une machine a pour but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet [13].

Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un cheval de Troie :

- Récupération des mots de passe grâce à un key logger.
- Administration illégale à distance d'un ordinateur.
- Relais utilisé par les pirates pour effectuer des attaques.
- Serveur de spam (envoi en masse des e-mails).

- **Spywares (logiciel espion) :** un mouchard ou un espiogiciel est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile. Dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données [17].

d) Buffer oveflow : le dépassement de tampon, souvent associé aux programmes écrits en langage C représente une menace majeure. Cette technique d'attaque vise à submerger la mémoire tampon d'un programme en injectant des données au-delà maximales du tampon set dépassée cela peut écraser des informations cruciales, y compris des adresses de processus, permettant de perturber l'exécution du programme, voire de prendre le contrôle du système [13].

e) L'injection SQL : est une technique d'attaque courante visant à manipuler des bases de données en exploitant les vulnérabilités des requête SQL. Les attaquants insèrent du code SQL malveillant dans les entrées utilisateurs, souvent via des formulaires web, pour compromettre la sécurité et accéder, altérer ou supprimer des données [14].

Au sein de l'URL d'un site web, la présence du protocole https indique une illusion de sécurité chez les utilisateurs. En effet, un attaquant à la capacite de tromper le navigateur, le conduisant à percevoir la visite d'un site comme étant sécurisée. Alors que ce n'est pas le cas. Cette manipulation vise à surveiller les interactions avec le site, ouvrant la porte au vol éventuel d'information personnelles partagées. La vulnérabilité de ce protocole réside dans son absence de chiffrement, le rendant ainsi moins sécurise et exposant les utilisateurs à des risques considérables.

1.3.3.3.2. Les attaque pour la couche transport :

- **Scanning de port :** Le scan de ports est une technique d'exploration informatique utilisée pour identifier les ports ouverts sur un ordinateur ou un serveur connecté à un réseau. Cette identification permet de déterminer les services en cours d'exécution et les protocoles utilisés, exposant ainsi des informations précieuses pour les attaquants potentiels [13].

- **L'attaque DDoS :** ou attaque par déni de service (Denial of service (DOS)), ne touchent pas les machines mais les sites internet. Elles consistent à envoyer d'innombrables requêtes de connexion a un site. Comme il ne peut pas les gérer,

il devient inaccessible. Les cybercriminels demandent ensuite parfois une rançon en échange du retour à la normale [16].

- **L'attaque SYN (TCP/SYN Flooding) :** c'est une attaque par saturation, ciblant le protocole TCP et exploitant le mécanisme de poignée de main en trois temps, se déploie en inondant le serveur de requête SYN erronées. Ce faisant, le serveur répond avec le message SYN-ACK habituel, mais l'attaquant omis de répondre avec un message ACK, laissant ainsi la connexion en état semi-ouvert. Au fil du temps, cette tactique engendre une saturation du serveur, le plongeant dans un état d'attente infinie, incapable d'accepter nouvelles connexions.
- **Distributed denial of service (DDOS) :** lorsqu'une attaque vise à perturber un service en ligne en mobilisant plusieurs machines simultanément, on parle alors de déni de service distribué (DDOS).

1.3.3.3.3. Attaques sur la couche réseau :

- **Attaque spoofing :** cette attaque permet l'utilisation d'adresse IP ou de MAC falsifiées pour masquer l'identité de l'attaquant et tromper les dispositifs réseau.
- **Scanning IP :** une attaque de type scan réseau consiste à effectuer une analyse sur une plage ou une liste d'adresse IP dans le but de découvrir les adresses actives au sein d'un réseau et d'identifier celles qui sont en fonctionnement [13].
- **ICMP Tunneling :** l'utilisation d'une technique de commande et de contrôle appelée « tunneling » permet de dissimuler de manière secrète le trafic malveillant, établissant ainsi une connexion discrète entre deux ordinateurs. Les données nocives transitent à travers ce « tunnel », demeurant camouflées au sein de requête d'écho et de réponses d'écho ICMP, adoptant ainsi l'apparence normale du trafic réseau [13].
- **Attaque de smurf :** est une forme d'attaque par déni de services (DoS) qui exploite la fonctionnalité de diffusion (broadcast) des protocoles Internet Contrôle Message

Protocol (ICMP). L'attaquant envoie de manière massive des requête ICMP de type « écho request » (ping) a une adresse de diffusion avec une adresse IP falsifiée [13].

- **MITM usurpation adresse IP :** l'une des techniques d'attaque Man in the middle (MITM) se matérialise par l'insertion d'une machine pirate entre le client

et le serveur. Cette manœuvre permet à l'attaquant d'intercepter toutes les communications, offrant un accès discret a l'échange d'information entre le client et le serveur sans que ce dernier ne suspecte l'intervention malveillante [13].

1.3.3.3.4. Attaques sur la couche d'accès (liaison) :

Un attaquant pratiquant le « MAC spoofing » est une entité qui falsifie délibérément l'adresse MAC (Media Access Contrôle) d'un périphérique réseau. En utilisant une adresse MAC différente de celle qui lui est attribuée, l'attaquant cherche à usurper l'identité d'un autre périphérique sur le réseau. Cela peut être utilise dans diverses attaques, telles que l'ARP spoofing, pour tromper les dispositifs réseau et compromettre la communication légitime entre les machines [13].

- **Le MAC flooding :** est une attaque réseau ou une attaque envoie un grand nombre de trames avec des adresse MAC falsifiées, saturant ainsi la table d'adresse MAC d'un commutateur. Cela peut entrainer la diffusion excessive du trafic sur le réseau, provoquant des problèmes de performance et parfois des attaques par déni de services.
- **Ecoutes-wifi :** généralement appelée « sniffing » wifi, désigne le fait d'intercepter et de capturer les données sans fil échangées sur un réseau WIFI. Les outils d'écoute wifi sont souvent utilisés à des fins de dépannage réseau légitime, mais ils peuvent également être exploités de manière malveillante pour interconnecter des informations sensibles, comme les identifiants de connexion, si le réseau n'est pas correctement sécurisé.

Conclusion :

Au terme de ce chapitre, nous avons une bonne compréhension sur les fondamentaux des réseaux informatiques qui sont essentielle dans le domaine des télécommunications. Avec une croissance continue de ces réseaux dans l'enivrement des entreprises, les risque associe augmentent également. Ainsi dans le prochain chapitre, nous explorerons les enjeux de sécurité lies au transport des données en vue de garantir l'intégrité et la confidentialité des information échangées.

Chapitre II

Les VPN et le pare-feu

Introduction

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à internet. Les réseaux sont toujours devant desmenaces.il y'a de plus en plus de techniques pour les protéger et atteindre le niveau de sécurité demandée sur un réseau.

Dans ce chapitre, nous faisons un survol des notions de sécurité informatique, et nous allons montrer les moyens et les dispositifs de sécurité utilisé pour l'assurer, nous étudierons en particulier les pares-feux et les VPN (réseau privés virtuels).

2.1. Le pare-feu

Les pares-feux sont devenus très populaires en tant qu'outils de sécurité pour les réseaux, il offre au système une protection d'un réseau interne, contre un certain nombre d'intrusions venant de l'extérieur, grâce à des techniques de filtrage rapide et intelligentes.

Aussi appelé coupe-feu est un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent .il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas) [18].

Le pare-feu a pour rôle de faire respecter la politique de sécurité du réseau préalablement définie, celle-ci énumérant quels sont les types de paquets pouvant circuler dans et à travers le réseau à protéger, ce en surveillant et contrôlant les applications et les flux de données (paquets).

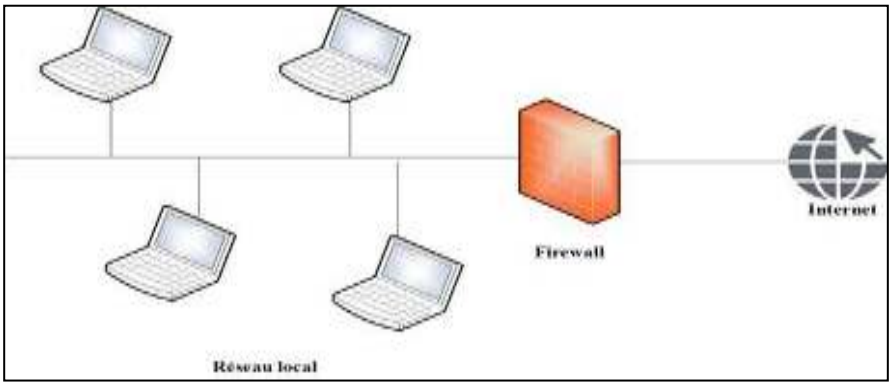


Figure 2. 1 : Pare-feu (firewall).

2.1.1. Classification des pares-feux :

Les pares-feux sont le plus vieil équipement de sécurité et comme tel, ils ont été soumis à de nombreuses évolutions. Suivant la génération des pares-feux ou leur rôle précis, on peut les classer en différents catégories [19].

2.1.1.1. Les pares-feux sans état ou filtrage simple de paquets (stateless packet inspection firewall) :

C'est le plus vieux dispositif de filtrage réseau, introduit sur les routeurs il regarde chaque paquet indépendamment des autres et le compare à une liste de règles preconfigurées.la configuration de ces dispositifs est souvent complexe et l'absence de prise en compte des machines a états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pares-feux ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation.

2.1.1.2. Les pares-feux avec état ou filtrage dynamique de paquets (stateful packet inspection firewall) :

Certains protocoles dits « à état » comme TCP introduisent une notion de connexion. Les pares-feux à état vérifient la conformité des paquets a une connexion en cours. Est à dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précèdent paquet et la réponse à un paquet dans l'autre sens.

2.1.1.3. Les pare-feu applicatif (proxy ou passerelle applicative) :

Dernière mouture de pare-feu, ils vérifient la complète conformité du paquet a un protocole attendu. Par exemple, ce type de pare-feu permet de vérifier que seul du http passe par le port TCP 80. Ce traitement est très gourmand en temps de calcul dès que le débit devient très important, il est justifié par le fait que de plus en plus de protocoles réseaux utilisent un tunnel TCP pour contourner le filtrage par ports.

2.1.2. Mode de fonctionnement d'un pare-feu :

Selon l'approche fonctionnelle, les pares-feux 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 entredeux machines.

- Les firewalls fonctionnant au niveau applicatif ou proxy : ce sont les filtres mandatés oud'application [20].

2.1.3. Les types de pare-feu :

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

2.1.3.1. Le firewall matériel :

Est un dispositif physique déployé pour renforcer les limites d'un réseau. Toutes les liaisons réseau traversant cette frontière passent par ce pare-feu, ce qui lui permet d'inspecter le trafic réseau entrant et sortant et d'appliquer des contrôles d'accès et d'autres politiques de sécurité.

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

- **Avantage :**

- Intégré au matériel réseau
- Administration relativement simple
- Bon niveau de sécurité.

- **Inconvénients :**

- Dépendant du constructeur pour les mises à jour.
- Souvent peu flexibles.

2.1.3.2. Les firewalls logiciels :

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que cers l'exhaustivité, afin de rester accessible à l'utilisateur final. [21].

- **Avantages :**

- Sécurité en bout de chaine (le poste client).
- Personnalisable assez facilement

- **Incontinents :**

- Facilement contournable
- Difficiles à départager

2.1.3.3. Les firewall bridge :

Ces firewalls se trouvent typiquement sur le switch, 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 a un autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable. Ce qui implique que le pare-feu bridge fonctionnent en mode transparent. [22].

- **Avantages** :

- Impossible de l'éviter (les paquets passeront par ses interfaces).
- Peu couteux.
- Simplifie la gestion de la sécurité réseau.

- **Incontinents :**

- Possibilité de le contourner (il suffit de passer outre ses règles)
- Configuration souvent contraignante.
- Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

2.1.4. Segmentation des zones de sécurité :

La segmentation par zone de sécurité, lorsqu'elle est associée à des zones démilitarisées (DMZ), à un réseau local (LAN) et à un réseau étendu (WAN), offre une approche complète pour sécuriser les réseaux d'entreprise complexes. Cette stratégie implique la division du réseau en segments distincts, chacun ayant ses propres politiques de sécurité et contrôles d'accès, pour limiter la propagation des cybermenaces et protéger les données sensibles.

Les rôles des différentes zones sont :

- **DMZ (zone démilitarisée) :** la DMZ agit comme un tampon entre le réseau interne (LAN) et internet public. Elle héberge des serveurs et des services accessibles depuis internet, réduisant ainsi l'exposition directe du réseau interneaux menaces externes.

- **LAN (réseau local) :** le LAN est le réseau interne privé de l'entreprise, où se trouvent les ordinateurs de bureau, les serveurs et autres appareils .il est protégé par un pare-feu interne et des contrôles d'accès strict pour limiter l'accès aux ressources internes.
- **WAN (réseau étendu) :** le WAN connecte plusieurs sites d'une entreprise ou permet l'accès à distance au réseau interne .il utilise des technologies telles que les VPN (Virtual Privat Network) pour sécuriser les communications sur les réseaux publics.

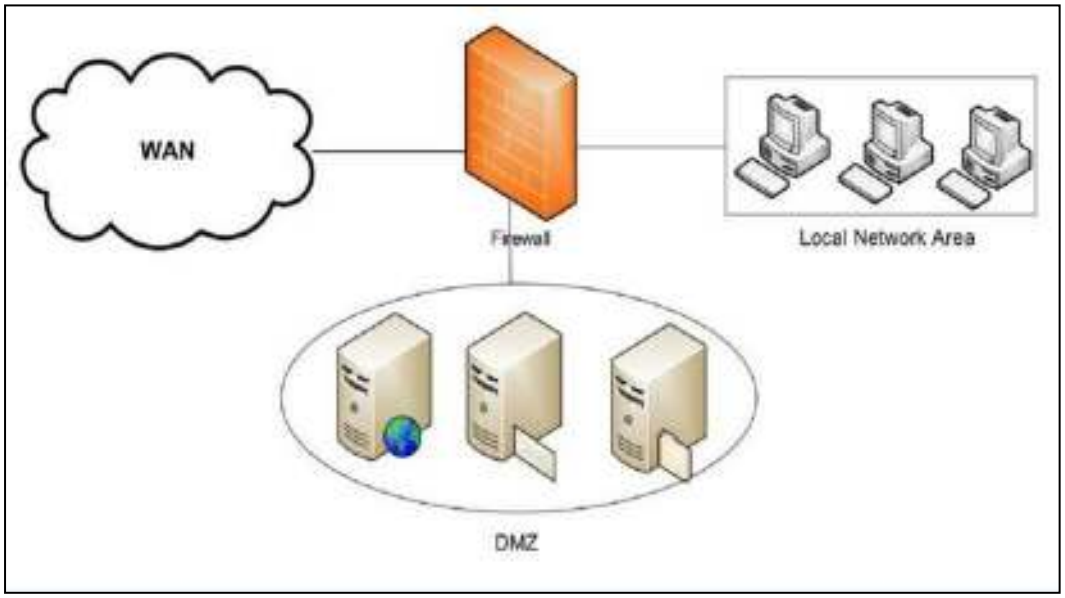


Figure 2. 2 : architecture DMZ avec un seul pare-feu

2.1.5. Politique de sécurité d'un pare-feu :

2.1.5.1. Définition de la politique de sécurité et ACL :

- **Définition de la politique de sécurité**

C'est la première phase avant de créer des règles de filtrage sur le pare feu. Elle se base sur les besoins d'entreprise en termes de connexions à internet et par la suite transformer ces besoins en règles tout en assurant non seulement la sécurité de l'entreprise mais aussi son bon fonctionnement.

Deux méthodes sont possibles [23] :

- Autoriser tout le trafic et bloquer les services dangereux.
- Bloquer tout le trafic et autoriser que les services nécessaires au bon fonctionnement del'entreprise.

- **Définition des listes de contrôles d'accès (ACL) :**

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur (figure2.3) :

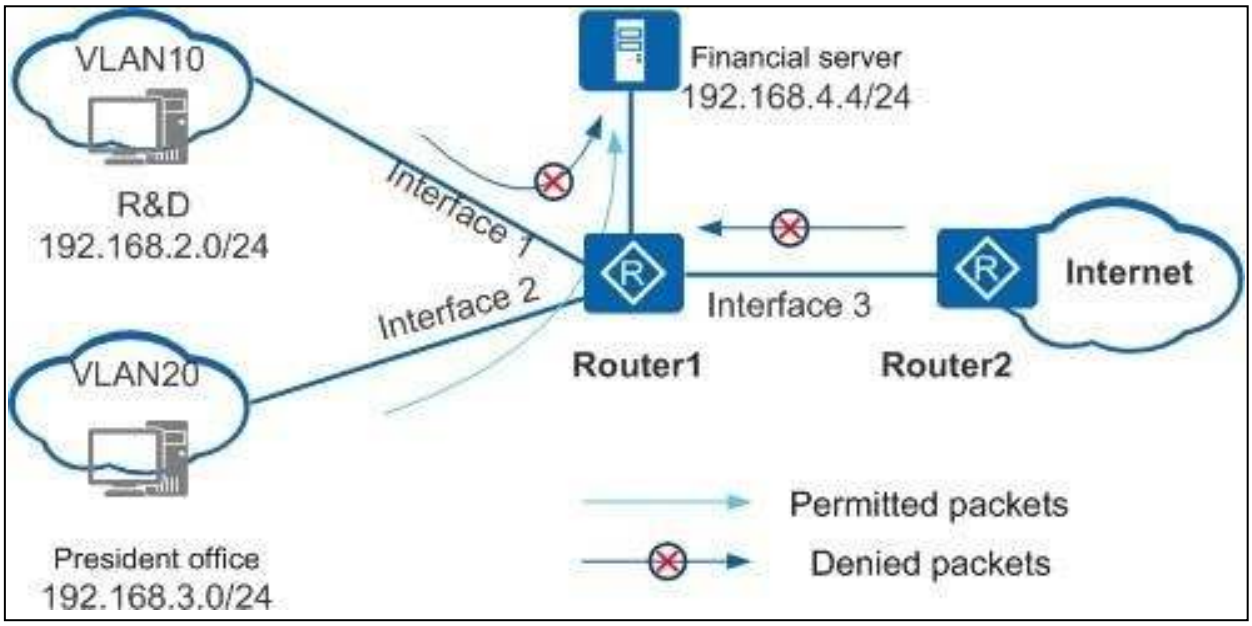


Figure 2. 3 : les ACL.

Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocole) et IPX (Inernet work packet exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau [24].

On distingue trois types des ACL :

- **ACL standard :** ils sont fondamentaux et offrent une forme simple de filtrage des paquets. Les ACL standard contrôlent le trafic en comparent l'adresse source des paquets IP aux adresse configurées dans l'ACL.
- **ACL étendues :** elles permettent un contrôle plus précis que les listes de contrôle d'accès standard. Ils peuvent filtrer le trafic en fonction du protocole, du port, de l'adresse IP source et de l'adresse IP de destination.
- **ACL dynamique :** ils sont également connus sous le nom d'ACL « lock-and-key ». Les ACL dynamique permettent aux administrateurs d'accorder aux utilisateurs un accès temporaire à certaines zones du réseau.[25].

2.1.5.2. Principes de fonctionnement :

Un system pare-feu contient un ensemble des règles prédéfinies permettant [26] :

- 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 permettent de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entreprise.

On distingue habituellement deux types de politique de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : « tout ce qui n'est pas explicitement autorisé est interdit ».
- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sure mais, elle impose toutefois une définition précise et contraignante des besoins en communication**.**

2.1.6. Transfert interzone :

Une interzone de sécurité spécifie le canal de transmission du trafic, qui est la seule « Route » entre deux zones. Si nous souhaitons détecter le trafic passant par ce canal, nous devons définis un « mot de passe » sur le canal, tel qu'une politique de sécurité de pare- feu.

- Deux zones de sécurité quelconques forment une interzone et ont une vue interzone distincte.
- Les flux de données entre les zones de sécurité sont directionnels, y compris entrants etsortants [27].

2.2. Virtual Privat Network (VPN) :

2.2.1. Définition d'un VPN :

Le VPN (Virtuel Private Network) ou réseau virtuel privé est une liaison sécurisée entre deux sites d'une organisation via un réseau public, en général internet. Il nous permet d'envoyer et de partager des données ou des ressources entre des sites distants.

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grâce à un principe de tunnel (tunneling) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées. Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles et donc inutilisables [28].

Un VPN fonctionne selon un système de tunnelisation privé, c'est à dire qu'un tunnel est créé, à l'intérieur duquel transitent toute la communication et ou toutes les données transmises qui sont cryptées.

Pour communiquer au travers du VPN, plusieurs protocoles peuvent être utilisés :

- Internet Protocol Security (IPSec)
- Layer Two Tunnelig Protocol (L2TP)
- Point-to-point Tunnelig Protocol (PPTP).

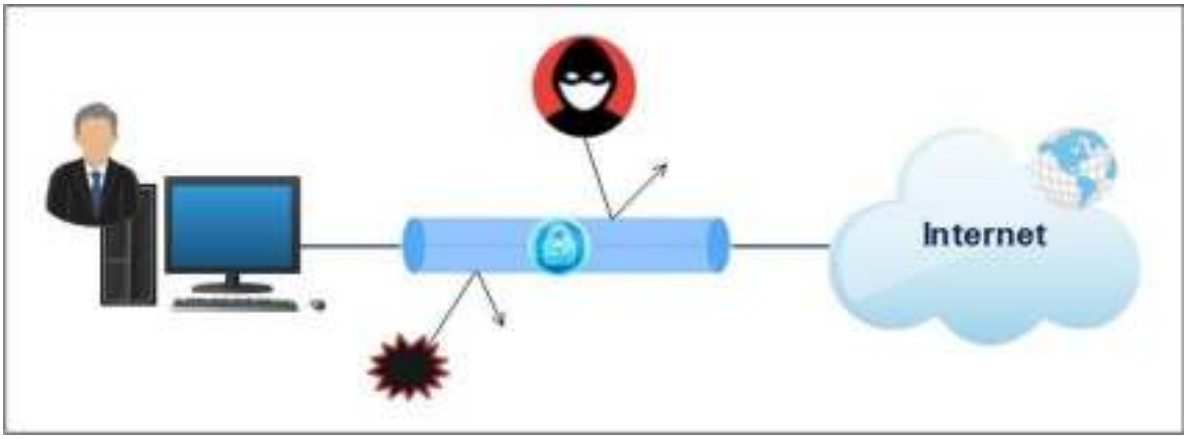


Figure 2. 4 : Virtuel Private Network.

2.2.2. Les différentes architectures des VPN :

Selon les besoins, on désigne 3 types de VPN :

a) **De poste à poste** : le VPN poste à poste est utilisé pour établir un canal sécurisé entre deux poste clients, proche ou distant par exemple, un client et son partenaire sur deux sites différents, ce qi permet au client distant de communiquer avec le poste concerne uniquement et non avec tous les postes du réseau virtuel.

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

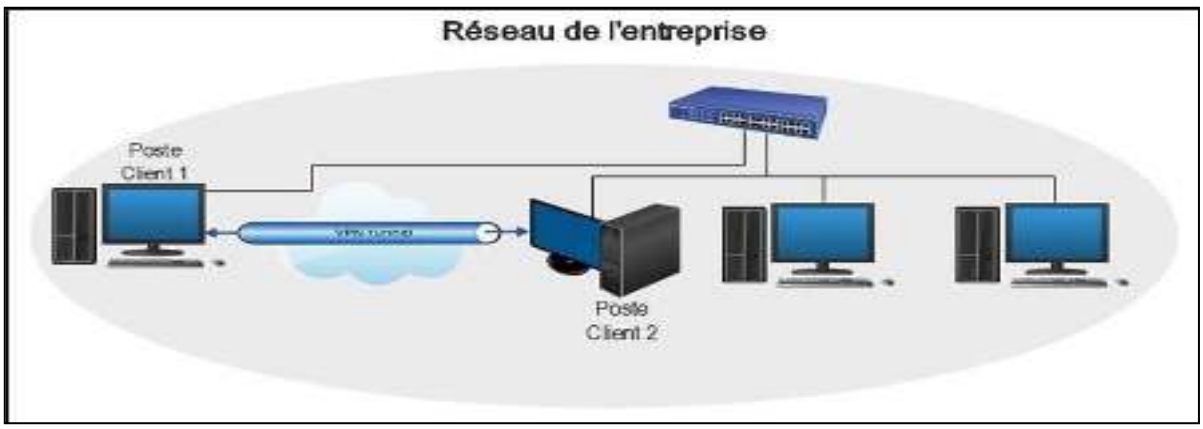


Figure 2. 5 : VPN poste à poste

b) **De poste à site** : un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion internet. Le développement de l'ADSL favorise ce genre d'utilisation.

Toutefois à interdire l'accès internet depuis le poste « localement » pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise.

Ce point est important et rejoint la réflexion la plus large de la sécurité des sites mis en relation avec VPN. Lorsque les niveaux de la sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux, s'il existe une faille de sécurité sur un site ou sur poste normale, celle-ci peut être exploitée.

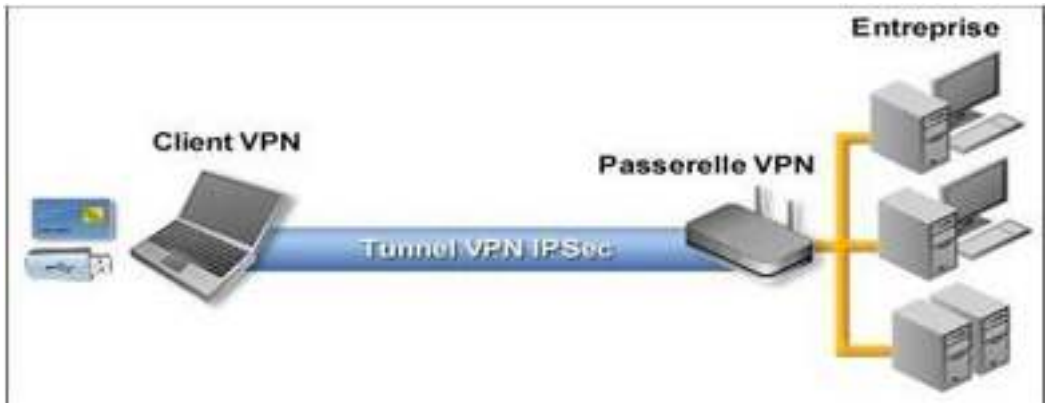


Figure 2. 6 : VPN poste à site 1

c) **De site à site :** Elle correspond à un type d'infrastructure de réseau étendu, c'est-à-dire que l'interconnexion entre les VPN remplace et améliore les réseaux privés existant. Elle est utilisée pour relier un site avec des filiales a moindre cout et en toute sécurité.

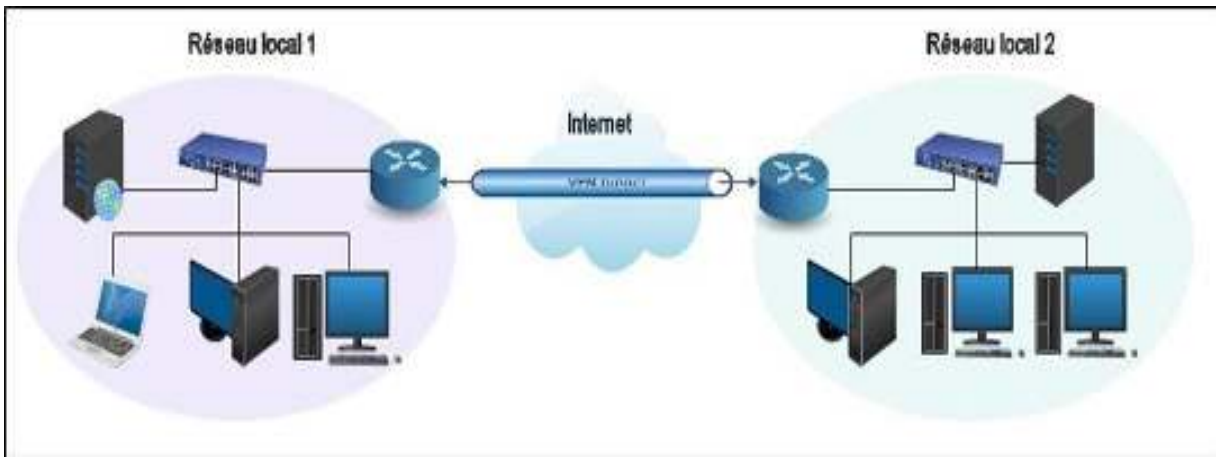


Figure 2. 7 : VPN site à site

2.2.3. Catégories des VPN :

Voici une brève description des protocoles les plus communément utilisés dans la place dans les couches OSI (open system interconnexion) mais ce classement peut se révéler arbitraire pour certains d'entre eux qui recouvrent enfait plusieurs niveaux.

Tableau 2. 1 : Catégories des VPN

Couche protocolaire	Catégories	VPN
Transport	**L4 VPN**	SSL VPN
Réseau	**L3VPN**	GRE, IPsec
Liaison de données	L2VPN	PPTP, L2TP

2.2.4. VPN de niveau 4 :

Les VPN de niveau 4, sont discrets mais performants, ils opèrent au niveau transport et s'intègrent parfaitement aux applications et protocoles existants, offrant une compatibilité accrue. Basée sur le protocole SSL.

2.2.4.1. SSL VPN

- **Définition SSL VPN (Secure Sockets Layer Virtual Private Network)** : Est un type de VPN qui fonctionne au -dessus de TLS (Transport Layer Security) et qui est accessible avec un navigateur web ou un client lourd (OpenVPN , AnyConnect), permettant des ouvertures de sessions https.il permet aux utilisateurs d'établir une Connexion sécurisée au réseau intranet depuis n'importe quel ordinateur possédant un navigateur web ou le client adéquat plusieurs fournisseurs proposent des solutions VPN SSL[29].
- **Fonctionnalité d'un SSL VPN :** Ils s'appuient sur le protocole TLS (Transport Layer Security). Ce dernier a été remplacé l'ancien protocole SSL (fonctionnent ensemble comme un seul protocole), pour sécuriser l'accès à distance. Ils permettent aux utilisateurs authentifies d'établir des connexions sécurisées aux services internes HTTPS ; via des navigateurs web standard ou des applications clientes. Ainsi, ils permettent un accès direct aux réseaux [30].

Il existe deux principaux types de VPN SSL [30] :

Le portail VPN et le tunnel VPN.

- **Le portail ou client VPN SSL :** un portail VPN SSL permet d'établir une connexion à la fois vers des sites web distants. Ainsi, les utilisateurs distants accèdent à la passerelle avec leur navigateur web après avoir été authentifies par une méthode prise en charge par la passerelle. L'accès se fait via une page web qui fait office de portail vers d'autres services.
- **Le tunnel VPN SSL :** un tunnel VPN SSL permet aux utilisateurs d'accéder en toute sécurité a plusieurs services de réseau via des navigateurs web standard, ainsi qu'à d'autres protocoles et applications qui ne sont pas bases sur le web. Le tunnel VPN est un circuit établi entre l'utilisateur distant et le serveur VPN. Le serveur peut se connecter à un ou plusieurs sites web, services de réseau ou ressources distant à la fois pour le compte du client. Aussi, le tunnel exige que le navigateur web gère le contenu actif et fournisse des fonctionnalités qui ne sont pas autrement accessibles via un portail VPN SSL.

2.2.5 VPN de niveau 3 :

Les VPN de niveau 3, sont des piliers de sécurité réseau ils opèrent au niveau du routage (paquets) et s'intègrent parfaitement à l'infrastructure existante, offrant un contrôle et une protection renforcée basée sur le protocole GRE et IPSec.

- **GRE : Définition GRE**

(Generic Routing Encapsulation) ou encapsulation générique de routage : est un protocole réseau qui permet d'encapsuler différents types de paquets pour les faire transiter au sein d'un autre protocole. Conçu par Cisco, il sert principalement à créer des tunnels point-a-point, c'est à dire des connexions directes entre deux points du réseau [31].

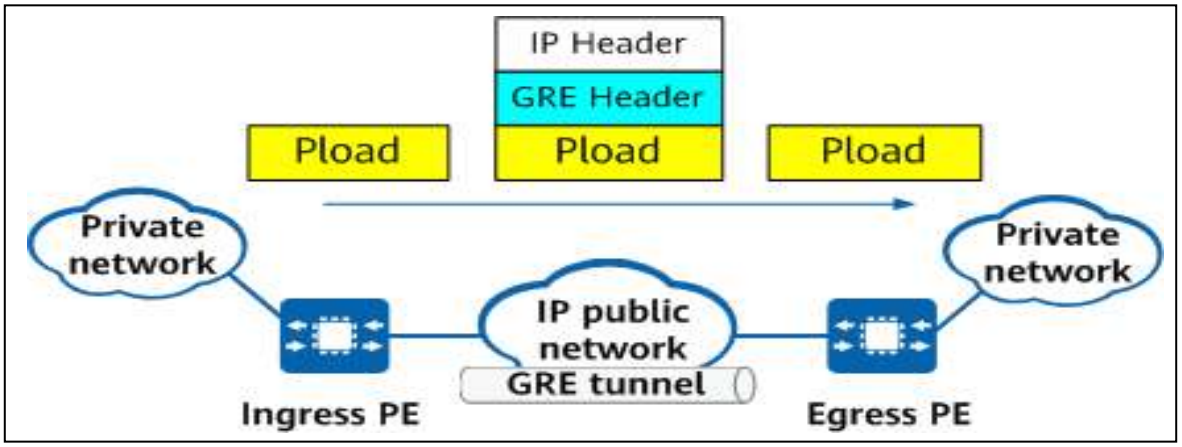


Figure 2. 8 : VPN GRE

- **Le but du tunnel GRE :** est de faciliter le transport de paquets au sein de réseaux non compatibles. Pour cela, il encapsule les paquets en ajoutant un nouvel entête (header) aux données. Grâce à cette entête supplémentaire, les paquets peuvent traverser des réseaux intermédiaires sans d'être modifies ni altérés, jusqu'à atteindre leur destination finale où ils seront désencapsulés et retrouveront leur format initial [31].

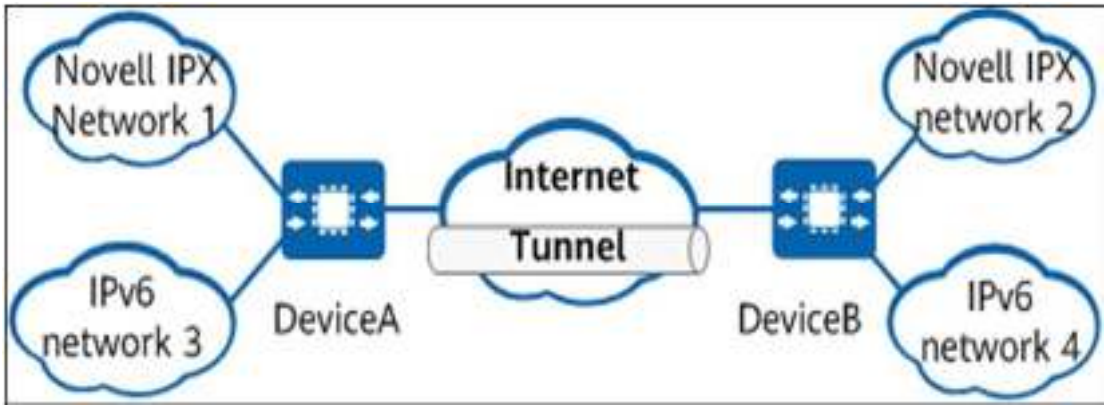


Figure 2. 9 : réseau GRE

a) **Protocole IPSec :** Est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait, d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin, de garantir la confidentialité, l'intégrité et l'authentification des échanges. Sa position dans les couches basses du modèle OSI lui permet donc de sécuriser tous type d'applications et protocoles réseaux bases sur IP sans destination. IPsec est très largement utilise pour le déploiement de réseau VPN à travers Internet a petite et grande échelle [32]. Dans le cadre de ce PFE , c'est la solution adoptée pour le tunneling.

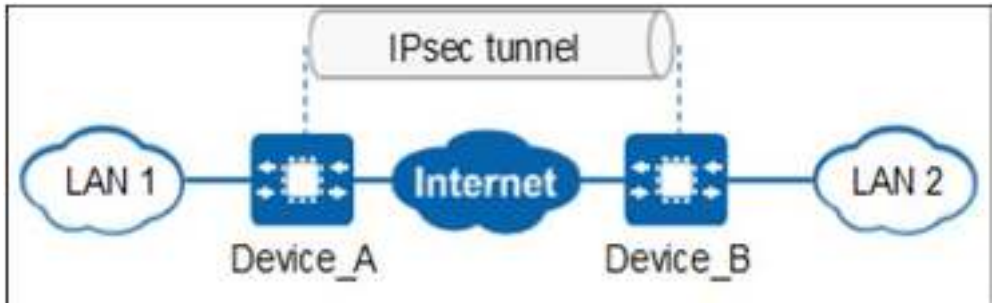


Figure 2. 10 : VPN IPSec.

2.2.6. VPN de niveau 2

Ces VPN encapsulent les données dans des trames et ce sont ces trames que va véhiculer le tunnel dans une communication point à point. Nous sommes donc bien niveau 2 du modèle OSI. La plupart des protocoles situes ici sont progressivement délaissés au profit de protocoles plus souples comme peuvent l'être ceux des niveaux 3 à 7.

a) Le protocole PPTP :

- **Définition du protocole PPTP (Point To Point Tunneling Protocol) :** ce protocole fortement soutenu par Microsoft est très simple mais assez limité. En principe, il permet de créer des trames sous le protocole PPP et les encapsuler dans un datagramme IP.
- **Principe de PPTP :** le principe du protocole PPTP est de crées des trames avec le protocole PPP et de les crypter puis de les encapsuler dans un paquet IP. Cela permet de relier les deux réseaux par une connexion point-à-point virtuelle acheminée par une connexion IP sur internet. Cela fait croire aux deux réseaux qu'ils sont reliés par une ligne directe. On garde, ainsi les adresses des réseaux physiques dans la trame PPP cryptées et cette trame est acheminée normalement sur internet vers l'autre réseau.

Il permet les opérations suivantes :

- L'authentification se fait par le protocole MS-CHAP (Challenge Handshake Authentification Protocol) version 2 ou avec le protocole PAP (Password Authentification Protocol).
- L'encryptions se fait par le protocole MPPE (Microsoft Point-to-point Encryption). Cela crée un tunnel de niveau 3 (réseau) gère par le protocole GRE (Generic Routing Encapsulation). La compression peut se faire avec le protocole MPPC (Microsoft point to point compression).

Une trame PPTP est constituée de :

- Paquets IP qui contient les données et les adresses IP de la machine.
- Entête PPP nécessaire pour toute connexion point à point
- Entête GRE (Generic Routing Encapsulation) qui gère l'encapsulation
- Entête IP contient les adresses IP sources et de destination qui correspond au client et au serveur VPN [33].

b) Protocole L2TP

- **Définition du protocole L2TP (Layer Two Tunneling Protocol)** : L2TP (Layer Two Tunneling Protocol) : L2TP est issu de la convergence des protocoles PPTP et L2F.Il est actuellement développé et évalué conjointement par Cisco Système, Microsoft...etc. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (liaison de données) et 3 (réseau). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur internet. L2TP repose sur deux concepts : les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator) et les serveurs réseau L2TP (LNS : L2TP network server).
- **Principe de L2TP : le protocole L2TP utilise une combinaison de deux protocoles de niveau 2 :** L2F (Layer 2 Forwarding Protocol) de Cisco et PPTP (Point-to-Point Tunneling Protocol) de Microsoft. L2TP utilise PPTP pour le chiffrement des données et L2F pour la gestion des sessions. Lorsqu'un utilisateur se connecte à un VPN via L2TP, un tunnel est créé entre et le serveur VPN. Les données sont alors encapsulées dans des paquets et envoyées à travers le tunnel. Le protocole L2TP utilise des clés de chiffrement pour garantir la sécurité des données pendant le transport [34].

2.2.7. IPSec :

2.2.7.1. Présentation

Ce protocole est développé par l'IETF, est un protocole standard qui garantit la sécurité de transmission et l'authentification des utilisateurs sur les réseaux publics, il fonctionne dans la couche réseau de systèmes OSI, par conséquent, il peut être mis en œuvre indépendamment des applications qui s'exécutent sur le réseau. IPSec offre la confidentialité des données, en utilisant le chiffrement pour protéger les données contre les tentatives d'écoute. Des algorithmes de chiffrement utilisés comprenant DES, 3DES et AES.

Dans le cadre de ce PFE on opte pour une solution basée sur IPSec :

IPSec est un protocole de sécurité de niveau 3 ce qui le rend plus sécurisant que les protocoles de niveau 2 (L2TP et PPTP) qui ne sont d'ailleurs utilisés que dans les réseaux IP privés (et non dans un réseau ouvert comme internet).

- Implémenté au-dessus du protocole IP, IPSec peut sécuriser toutes les couches de services au-dessus de IP.
- Flexible, modulaire.

2.2.7.2. Mode de fonctionnement

IPSec fonctionne selon deux modes différents avec des degrés de protection divers [35] :

- **Le mode tunnel** : le mode tunnel IPSec est adapté au transfert des données sur les réseaux publics, car il renforce la protection des données contre les parties non autorisées. L'ordinateur chiffre toutes les données, notamment la charge utile et l'en-tête, et y ajoute un nouvel en-tête.
- **Le mode transport** : le mode transport IPSec chiffre uniquement la charge utile du paquet de données et laisse l'en- tête IP sous sa forme d'origine. L'en- tête de paquet non chiffre permet aux routeurs d'identifier l'adresse de destination de chaque paquet de données. Par conséquent, le transport IPSec est utilisé dansun réseau étroit et de confiance, tel que la sécurisation d'une connexion directe entre deux ordinateurs. Le protocole IPsec offre une solution de sécurité complète pour les communications internet.

Les fonctionnalités principales assurées par IPsec pour la protection des données sont :

a) Cryptographie :

La cryptographie est une science permettant de convertir des informations « en clair » en informations chiffrées, c'est-à-dire non compréhensibles, puis à partir de ces informations codées de restituer les informations originales. Il existe deux grandes familles d'algorithmes cryptographiques à base de clef [36] :

- **Cryptage symétrique :** dans la cryptographie symétrique, les clés de chiffrement sont identiques, c'est la clé secrète, l'émetteur et le récepteur doivent posséder et utiliser la même clé secrète pour rendre confidentielles des données et pour pouvoir les comprendre.

- **Cryptage asymétrique :** un système de chiffrement asymétrique est basé sur l'usage d'un couple unique de deux clés complémentaires (clé publique ,clé privée), calculées l'une par rapport à l'autre. La cryptographie asymétrique utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est distribuée librement et la clé privée quantà elle, n'est jamais distribuée et doit être gardée secrète.

b) L'authentification :

La protection des accès est devenue une priorité absolue. Les protocoles d'authentification jouent un rôle essentiel en garantissant que seuls les utilisateurs autorisés peuvent accéder aux systèmes, aux réseaux et aux ressources. Parmi ces protocoles on trouve :

- **SHA** (secure hash algorithme) : est un algorithme de hachage utilise dans les connexions sécurisées pour prouver l'intégrité et l'authenticité d'un message au destinataire. L'algorithme SHA est l'algorithme de hachage par défaut défini dans les certificats SSL.il y a deux types sont [37] :
- **SHA-1** : est un algorithme produisant une empreinte digitale de 160 bits lorsqu'il est utilisé sur un message.
- **SHA-2** : est un ensemble de fonctions de hachage, notamment SHA-224 et SHA-256, SHA-384, SHA- 512/224 et SHA-512/256.
- **MD5** (Message Digest 5) : est une fonction de hachage cryptographique qui permet d'obtenir l'empreinte numérique d'un fichier (on parle souvent de message) [38].
- **SM3** : est un algorithme de hachage cryptographique de 256bits dérivé de SHA-2 conçu par la NSA, il a été conçu par Xiaoyan Wang, responsable de la découverte des attaques contre de nombreuses fonctions de hachage cryptographique, notamment MD5 et SHA-1[39].

c) Echange de clé

- **IKE :** IPSec utilise le protocole IKE pour négocier et établir des tunnels sécurisés de réseau privé virtuel (VPN) de site a site ou d'accès distant. Le protocole IKE est également appelé protocole ISAKMP (Internet Security Association and key Management Protocole) (uniquement chez Cisco) [40].

- **ISAKMP (Internet Security Association and key Management Protocol) :** est un protocole de gestion des clés et des associations de sécurité pour internet : est défini comme un cadre générique pour établir ,négocier, modifier et supprimer des SA entre deux parties. En centralisant la gestion des SA, ISAKMP réduit la quantité de fonctionnalité reproduite dans chaque protocole de sécurité.
- **L'algorithme DH(Diffie-Hellman) :** est un des algorithmes les plus utilisés dans le cadre de la première étape : l'échange de clé. L'objectif de Diffie-Hellman est de permettre l'établissement d'une clé privée entre deux parties, via l'échange de message sur un canal non autorisé. Lors de l'établissement d'une clé avec Diffie- Hellman, les messages sont en effet envoyés en clair sur le réseau, et toute personne qui intercepte les messages transmis ne doit pas pouvoir en déduire la clé générée [41].

2.2.8. IPSec SA

Une association de sécurité IPSec (SA) est essentiellement un ensemble de paramètres de sécurité qui définissent comment deux appareils communiqueront en toute sécurité a laide d'IPSec c'est comme un contrat qui établit les règles de chiffrement, d'authentification et d'autre mesures de sécurité pour une connexion spécifique les SA sont créées pour sécuriser la communication entre les appareils utilisant IPSec.

2.2.9. Les services de sécurité fournis par l'IPSec

Les services de sécurité fournis par IPsec reposent sur deux protocoles différents qui constituent le cœur de la technologie IPsec, ces deux protocoles peuvent être utilisés indépendamment ou, plus rarement, de manière combinée.

a) Le protocole AH (Authentification header) :

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

- ✓ **L'encapsulation AH :**

Tableau 2. 2 : l'encapsulation AH

IP Header	AH Header	TCP Header	Données

b) Le protocole ESP (encapsulation Security Payload) :

Il permet quant à lui d'assurer la confidentialité, l'intégrité et employé avec IKE, l'authentification des données echangees.il garantit aussi une protection contre le rejeu.il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH) [42].

- ✓ **Encapsulation ESP**

Tableau 2. 3 : l'encapsulation ESP

IP Header	ESP Header	TCP Header	Data	ESP Tail	ESP Auth Data

- ✓ **Encapsulation AH-ESP**

Tableau 2. 4 : l'encapsulation AH-ESP

IP Header	**AH Header**	**ESP Header**	**TCP Header**	**Data**	**ESP Tail**	**ESP Auth Data**

c) **IKE SA (internet key exchange Security association) :** est une association de sécurité établie lors de la phase 1 du protocole IKE. Elle permet aux périphériques de négocier en toute sécurité les paramètres nécessaires pour créer des IPSec SA (Security Associations), qui définissent comment les données seront chiffrées et authentifiées pendant la communication.

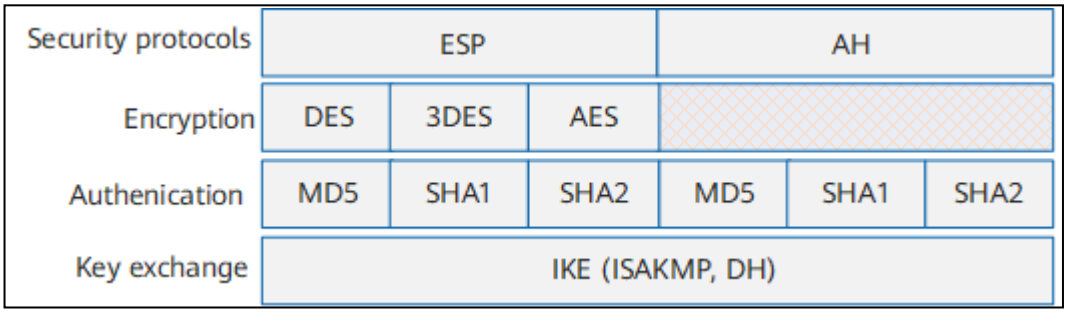


Figure 2. 11 : Les différents protocole de l'IPSec

2.3. Virtuel Local Area Network (VLAN)

La technologie de réseau local virtuel (VLAN) divise logiquement un réseau local physique en plusieurs domaines de diffusion, chacun étant appelé VLAN. Chaque VLAN fonctionne comme un domaine de diffusion distinct, les périphériques du même VLAN pouvant communiquer directement entre eux, contrairement à ceux des différents VLAN. En conséquence, les paquets de diffusion sont confinés dans un seul VLAN.

2.3.1. Définition

Un Virtual Local Area Network (VLAN) est un sous-réseau logique créé à l'intérieur d'un réseau physique. Contrairement à un réseau local traditionnel ou tous les appareils sont sur le même segment de réseau, un vlan permet de regrouper des appareils en fonction de critères comme la fonction, le département ou la sécurité.

Chaque VLAN est indépendant des autres. Ceci permet de les configurer ou de les gérer de manière séparée.

L'un des principaux avantages des vlan est la sécurité renforcer offerte par cette technologie. L'isolation des données sensibles dans des réseaux virtuels distincts empêche en effet les utilisateurs non autorisés d'y accéder.

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

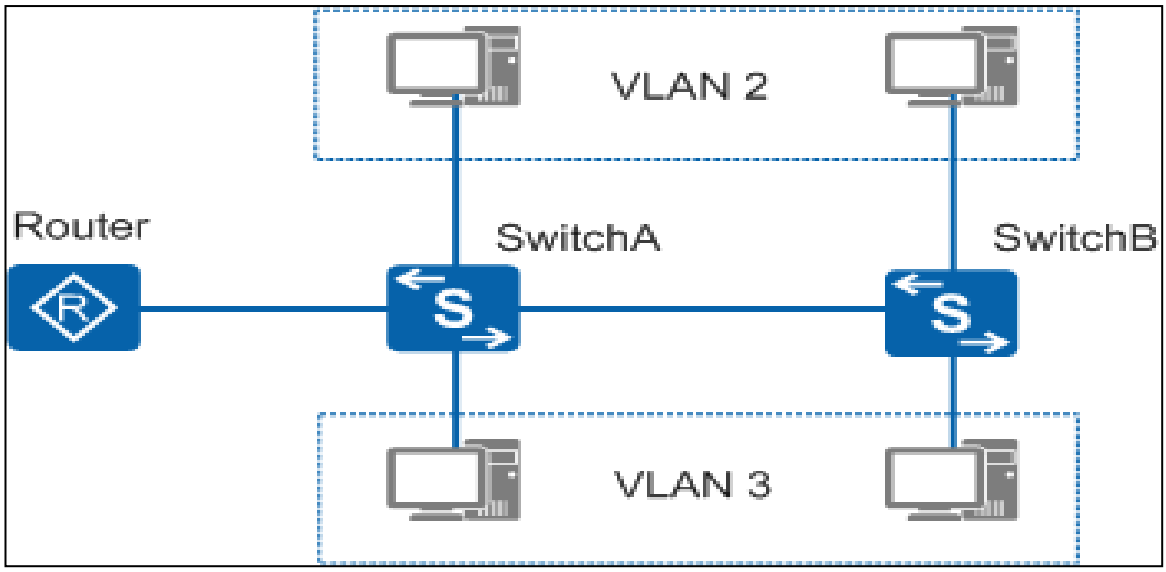


Figure 2. 12 : Virtual Local Area Network (VLAN).

2.3.2. Types de VLAN

Il existe plusieurs types e vlan utilisés dans les réseaux modernes. Certains types de VLAN sont définis par les classes de trafic. D'autre types de VLAN sont définis par leur fonction spécifique.

1. **Les VLAN par défaut :** est le VLAN auquel sont par défaut, associées les trames et les ports s'il ni a pas de configuration spécifique sur le matériel, lorsque la mise en œuvre des VLAN est réalisée. Généralement le VLAN par défaut est le VLAN 1. Lors de la mise en œuvre des VLAN sur un matériel au moins un VLAN doit être définit, d'où la nécessité du VLAN par défaut.
2. **VLAN natif :** ce type de VLAN est configuré sur un port trunk. 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.
3. **VLAN privé (PVLAN) :** les VLAN privé divisent un VLAN (dit primaire) en plusieurs sous-VLAN (secondaire). Un VLAN ordinaire forme un seul domaine de diffusion, alors que les VLAN privés forment des domaines de diffusion plus petits. En d'autres mots, un VLAN privé est un VLAN primaire découpe en plusieurs VLAN secondaires.

Dans un VLAN privé il existe trois types de VLAN :

VLAN primaire : simplement le VLAN d'origine. Ce VLAN est utilisé pour envoyer les trames (descendantes) vers tous les VLAN secondaires.

VLAN secondaire : ils possèdent aussi un numéro de VLAN. Ils appartiennent à un des types suivants :

- ✓ **Isolé :** les ports du VLAN isolé peuvent atteindre le VLAN primaire, mais aucun autre VLAN secondaire.de plus, les hôtes du même VLAN isolé ne peuvent pas communiquer entre eux .il n'est possible d'avoir qu'un seul VLAN isolé au sein d'un VLAN privé.
- ✓ **Communauté :** les ports d'un même VLAN communautaire peuvent communiquer entre eux et avec le VLAN primaire. Ils ne peuvent pas communiquer avec d'autres VLA N secondaire .il peut y avoir plusieurs VLAN communautaires au sein d'un VLAN privé.

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

Types de port du PVLAN : il existe trois types de port VLAN :

- ✓ **Port prmiscuous :** 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 promiscues et les autres ports communautaires du même sous-réseau.

Vlan de gestion : un vlan de gestion est configurer pour accéder aux fonctions de gestion d'un commutateur, la configuration de VLAN de gestion se fait tout simplement en lui attribuant une adresses IP et un masque de sous-réseau.

Les VLAN de données (VLAN utilisateur) : est configuré pour ne transporter que le trafic généré par l'utilisateur. L'importance de la séparation des données utilisateur a partir de tout autre type de VLAN est la gestion du commutateur et un contrôle adéquats.

VLAN de la voix : les VLAN voix isolent le trafic vocal sur un réseau commuté, améliorant ainsi la qualité des appels VoIP. En priorisant le trafic vocal et en le protégeant des autres données, les VLAN voix réduisent les interruptions et les retards, garantissant une communication claire.

VLAN de management : L**e** VLAN de management est utilisé par les matériels réseaux pour échanger leurs trames de contrôle et de management (OSPF, RIP, VTP…etc.). C'est aussi le VLAN par lequel les administrateurs peuvent se connecter sur les équipements afin de les administrer.

2.3.3. Avantage et inconvénients des VLAN

2.3.3.1. Les avantage :

La technologie de VLAN comporte de nombreux avantages permettant une meilleure organisation d'un réseau local. Parmi ces avantages on trouve :

- ✓ La segmentation des VLAN réduit la taille des domaines de diffusion ainsi le nombre de collision 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 ;
- ✓ Régulation de la bande passante ;
- ✓ La rédaction des couts.

2.3.3.2. Inconvénients :

- ✓ La mise en place d'un VLAN de niveau 1 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.

- ✓ La configuration et la gestion des VLAN peuvent être plus complexes surtout dans les grands réseaux avec de nombreux VLAN.

Conclusion

Dans ce chapitre, nous avons expliqué en détail la partie théorique de notre projet. Nous avons présenté les méthodes de sécurité telles que les VPN, les VLAN et les pares-feux et leurs protocoles, qui sont utilisés par de nombreuse entreprises pour assurer leur sécurité. Cette étude nous aidera dans la partie pratique que nous réaliserons dans les prochains chapitres.

Chapitre III

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

Introduction :

Dans ce chapitre, nous allons présenter l'entreprise dans laquelle nous avons effectué notrestage pour la réalisation de notre projet de fin de cycle.

Nous commençons d'abord par une brève présentation de la BMT Bejaïa, puis nous introduisons la structure générale d son organisation avec ses différentes directions et en particulier sa direction informatique, ainsi que ces objectifs. Ensuite, nous ferons le point sur la problématique posée et la solution proposée.

3.1. Présentation de l'organisme d'accueil :

3.1.1. L'historique de la BMT :

Dans le plan de développement 2004-2006, l'entreprise portuaire de Bejaïa (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 Bejaïa.

Dès lors l'EPB s'est lancées 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 présente au conseil de participation de l'état (CPU) 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) a 51% et PORTEK une société singapourienne a 49%, PORTEK est un opérateur de terminaux spécialisé dans les équipements portuaires il est présent dans plusieurs ports dans le monde.

En 2011 PORTEK System and Equipment, a été racheté par le groupe Japonais MITSUL.

Figure 3. 1 : Les partenaires de la BMT (Ressource externe)

3.1.2. Présentation de BMT Spa :

BMT – SPA est une jointe venture entre l'Entreprise Portuaire de Bejaia (EPG) et Portk Systèmes & Equipement L'EPB est l'autorité portuaire qui gère le port de Bejaia. PORTEK Systèmes and Equipment, 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 por+tuaires.

BMT Spa est une société par action, c'est une entreprise prestataire de service spécialisées dans le fonctionnement, l'exploitation et la gestion du terminal a conteneur pour atteindre son objectif, elle s'est dotée d'un personnel compétant particulièrement former dans l'opération de gestion des terminaux à conteneurs. Elle dispose d'équipements d'exploitation des plus perfectionnées 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 couts compétitifs. BMT Spa offre ses prestations sur la base 24H/7j.

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

- **Raison social, statuts juridique et capital social de BMT Spa** :

BMT est érigée sous forme de SPA (Société Par Actions), son social d'élève à 500000000 da repartis à raison de 51% pour l'EPB et 49% pour PORTEK (Mitsui).

Figure 3. 2 : Le rôle de la BMT (Ressource externe)

3.1.3. Situation géographique :

Bejaia Méditerranéen Terminal SPA est localisée au nouveau quai, dans le bassin sud du portde Bejaïa, ce dernier dessert un hinterland important et très vaste par des infrastructures routières reliant l'ensemble des villes du pays, des voix ferroviaires et d'un aéroport international. Se situant au centre de l'Algérie, sa position géographique est privilégiée, car elle bénéfice d'une baie des plusdétritée en méditerranée, afin de servir la région centre ainsi que les hauts plateaux.

BMT SPA se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Bejaïa, reliée au réseau routier national qui facilite le transport de marchandises conteneurisées detoute 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

3.1.4. Département informatique :

C'est un service qui appartient à la direction générale, sesprincipales fonctions sont :

- Suivi des applications de gestion.
- La maintenance du parc informatique de l'entreprise.
- Audit et amélioration du système d'information.
- Sauvegarde et contrôle des données de l'entreprise.
- Développement de nouvelles applications aux différentes structures.

3.2. Mission, valeurs et objectifs de BMT SPA :

3.2.1. Mission de BMT SPA :

L'activité principale de BMT est la gestion et l'exploitation du terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de couts et de sécurité ,l'ensemble des opérations qui ont rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performances 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.

3.2.2. Les valeurs de BMT SPA :

BMT veille au développement et à la gestion de son terminal à conteneurs ou l'intégrité, la productivité, l'innovation, la courtoisie, et la sécurité sont rigueur BMT est constamment soucieuse des intérêts de ses clients avec lesquels elle partage le souci de performance et de cout. Elle met à la disposition de ses clients des ressources humaines et des moyens nécessaires pour optimiser sa productivité et atteindre des niveaux de performances concurrentielle.

- **Intégrité** : Intégrité, en esprit et en forme, est notre règle de conduire et d'engagement. Nous œuvrerons, en toute circonstance et à tout moment, avec le respect absolu de l'intégrité et de l'honnêteté dans notre environnement de travail. Mentir, voler, décevoir, soudoyer, accepter des faveurs, ou faire du favoritisme vont à l'encontre de l'intégrité. L'intégrité est notre Guide et Centre de Gravite.
- **Innovation :** Montrer de la curiosité et stimuler les nouvelles idées et la créativité. Rechercher de nouvelles opportunités d'affaires. Avoir le courage de remettre en cause les vérités établies et oserexplorer de nouveaux champs et horizons. Comprendre et gérer les risques.
- **Performance :** Toujours rechercher les solutions les plus appropriées et partager son expérience. Développer l'expertise de manière continue et ciblée. Faire preuve de compétence commerciale et d'orientation clientèle. Rechercher la simplification. La clarté et éviter les activités qui n'ajoutent pas de valeur promouvoir la diversité.

- **Ténacité :** Fixer des objectifs ambitieux et respecter ses engagements. Prendre des décisions et s'assurer de leur réalisation. Travailler en équipe, éliminer les barrières et s'imposer des exigences constructives mutuelles. Montrer de la persévérance jusqu'à l'aboutissement et se concentrer sur les points importants.
- **Sécurité :** Contribuer à la protection de la sante, à l'amélioration de la sécurité et des conditions de travail dans notre entreprise. Veiller à l'application des règles relatives à la protection des employés, des clients, et des visiteurs. Protéger et agrémenter l'environnement de travail et respecter la protection de l'environnement et les directives HSE. Assurer la sécurité des biens de nos clients.
- **Courtoisie :** Le client est la raison d'être de notre simple existence. Lui montrer qu'il est le centrede notre souci et l'objet de notre entreprise. Montrer du respect à l'égard des services, de l'autorité, de la hiérarchie et des règlements établis. Respecter l'éthique du professionnalisme etde la décence sociale. Respect en tout temps ses collègues.

3.2.3. Les objectifs de BMT SPA :

La BMT a pour objectif de faire du terminal a conteneur de BMT une infrastructure moderne a même de répondre aux exigences les plus sévères en matière de qualité dans le traitement du conteneur.

La mise à disposition d'une nouvelle technologie dans le traitement du conteneur pour :

1. Un gain de productivité.
2. Une réduction de cout d'escale.3- Une fiabilité de l'information. 4- Un meilleur service des clients.

- Sauvegarder la marchandise des clients.
- Faire face à la concurrence national et international.
- Gagner des parts importantes de marché.

3.3. Activités et performances de BMT SPA :

3.3.1. Activités de BMT SPA :

L'activité principale de BMT SPA est la gestion et l'exploitation du terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de couts et de sécurité, l'ensemble des opérations qui ont 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.

3.3.2. Les opérations du terminal

3.3.2.1. Operations planification :

- Planification des escales : programmation des accostages et des postées à quai.
- Planification déchargement/chargement
- Planification du parc à conteneurs (visite, dépotage, enlèvement et restitution des conteneurs vides au pare).
- Planification des ressources : équipes et moyens matériels

3.3.2.2. Operations de manutention :

Elle comprend les opérations :

- Le déchargement des conteneurs du navire.
- La préparation des conteneurs pour chargement au navire.

3.3.2.3. Opération d'acconage :

- Transfert des conteneurs vers les zones d'entreposage.
- Transfert des conteneurs frigorifiques vers la zone « REEFERS ».
- Mise à disposition des conteneurs pour visite des services de contrôle aux frontières.
- Mise à disposition des conteneurs vides pour empotage.
- Suivi des livraisons et des dépotages.

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

3.3.3. Les équipements de la productivité de BMT

BMT avait procédé à la définition et à l'achat de produits, équipements et de systèmes de gestion du terminal permettant d'atteindre une très bonne productivité dans l'exploitation et une efficacité dans les opérations de traitements des conteneurs et un système de télésurveillance pour assurer la sécurité de la marchandise les systèmes en question sont :

- Un système logiciel pour la gestion des opérations du terminal.
- Un système de communication de données se terrain en temps.
- Un système de positionnement des transporteurs et de conducteur.
- Un système de supervision des équipements et des infrastructures.
- Une télé surveillance du par cet de ses périmètres.

3.3.4. Les différentes structure et l'Organisation de BMT :

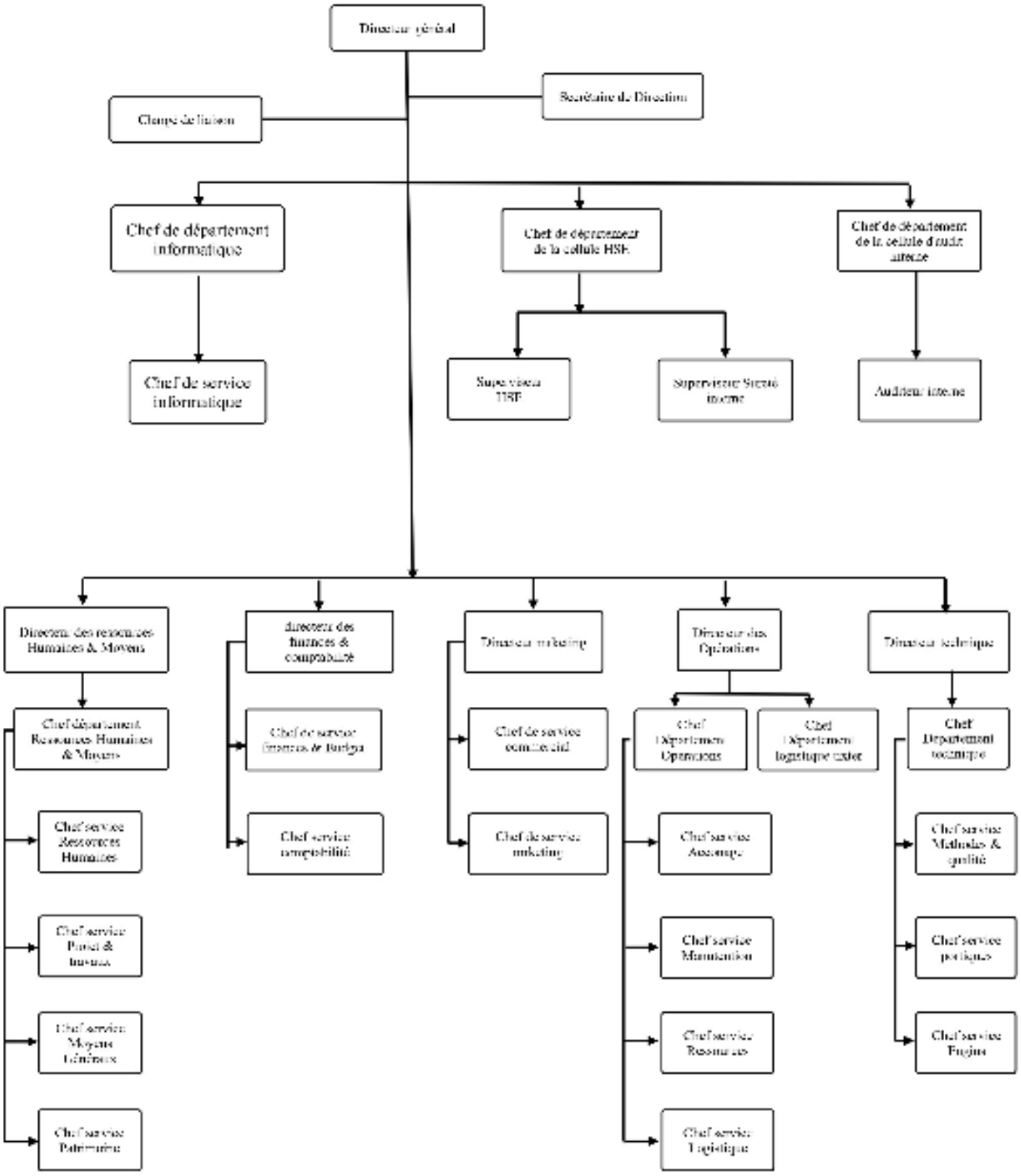


Figure 3. 4 : l'organigramme de la BMT

- **Direction générale (DG) :**

Décision, administre l'entreprise, assigne des directives au directeur générale à sa tête le directeur général qui gère la société BMP SPA, a le pouvoir d'adjoint qui fait la liaison et coordonne entre les différentes directions de BMT.

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

La direction des ressources humaines et moyens est assuré par le DRHM .la DRHM est placé sous l'autorité directe de directeur générale.sa mission est de mettre en œuvres des systèmes de gestion intégrées à la stratégie de BMT p Our atteindre ses objectifs et qui traduisent une adéquation entre les impératifs économiques et les attentes du personnel.

- **Direction des finances et comptabilité (DFC) :**

La mission de la Direction des Finances et Comptabilité est :

- Veiller à l'adéquation de la politique financière de l'entreprise avec les objectifs globaux
- Coordonner et suivre les relations avec les institutions financières
- Assurer les relations avec les banques et les administrations fiscales et parafiscales
- Assurer le recouvrement des créances de toute nature
- Etablir et suivre les budgets et les plans de financement
- Elaborer et rechercher et négocier les financements les plus appropriés en relation avec les établissements concernes
- Veiller à l'application des règles comptables et à la tenue correcte des livres au sein de la société
- Elaborer le bilan et autres états financiers et comptables
- Etablir et analyser le bilan de fin d'année.

- **Direction Marketing (DM) :**

La Direction Marketing restructurée récemment après la jonction des trois départements (Commercial +Marketing + Informatique) sa mission est de :

- Elaboration une politique commerciale et tarifaire
- Elaboration le plan marketing
- Coordonner et veiller à la bonne exécution des actions marketing

- Assumer le rôle de représentation de l'entreprise en Algérie et à l'étranger.
- Participer à l'élaboration du Business Plan
- Assurer la veiller technologique en matière de la communication et de l'information
- Elaboration des plans d'action de l'entreprise en termes d'efficacité de facturation de recouvrement et d'amélioration de la relation client
- Administration du système logiciel CTMS.

- **Direction des Operations (DO) :**

La mission de la Direction des Opération est de :

- Assurer la planification des escales, de parc à conteneurs et la planification des ressources, équipes et équipements.
- Prendre en charge les opérations de manutention, comme la réception des navires porte-conteneurs et leurs chargements et déchargement.
- Suivre les opérations de l'acconage tel que : le suivi des livraisons, dépotages, restitution duvide et le traitement des conteneurs frigorifiques.

- **Direction Technique (DT) :**

La mission de la Direction Technique est d'assurer une maintenance préventive et curative des engins du parc à conteneurs.

3.4. Présentation du service d'accueil (Centre Digitalisation et Numérique)

3.4.1. Présentation et organisation :

Au départ, le service informatique de BMT était intégré à la direction marketing. Cependant, l'entreprise a rapidement compris la nécessite d'une gestion informatique indépendante et a créé un département informatique dédie. Ce département, compose de deux sections (étude et développement et exploitation), était charge de gérer l'ensemble des systèmes informatique de l'entreprise.

En 2021, BMT a franchi une nouvelle étape en créant le centre digitalisation et numérique. Ce centre, placé sous la responsabilité direction générale, regroupe deux services :

- Le service génie logiciel
- Le service infrastructure, système et numérique.

Le centre digitalisation et numérique joue un rôle central dans la transformation digitale de BMT .il met à la disposition des collaborateurs les outils informatiques nécessaires à leur travail quotidien, assure la maintenance du parc informatique et développe de nouvelle application répondant aux besoins spécifiques de l'entreprise.

En résumé, l'évolution du service informatique de BMT illustre l'importance croissante accordée aux technologies numériques par l'entreprise.

3.4.2. Mission et objectives de Centre Digitalisation et Numérique :

Parmi les principales missions des deux services, nous citons :

3.4.2.1. Service génie logiciel :

A comme fonction :

1- Développement applicatif :

- Conception et réalisation d'application répondant aux besoins métiers de l'entreprise.
- Évolution et maintenance des applications existantes.

2- Gestion du système d'information :

- Assurer la sécurité et la pérennité du système d'information.
- Sauvegarder et contrôler les données stratégiques de l'entreprise.
- Administrer les serveurs de messagerie et le site web.

3.4.2.2. Service infrastructure système et numérique :

1. Gestion du parc informatique :

- Installer, configurer et mettre à niveau les systèmes d'exploitation des équipements informatiques.
- Déployer et maintenir les nouveaux systèmes et logiciels
- Garantir le bon fonctionnement du parc informatique et assurer la maintenance des équipements.

2. Administration réseau :

- Gérer le réseau informatique et veiller à son évolution et a son optimisation.
- Mettre en place les solutions de sécurité nécessaires pour protéger le réseau et les données.

3. Optimisation des performances :

- Garantir la qualité de service en optimisant les performances des systèmes informatiques.
- Assurer un haut taux de disponibilité des applications et des systèmes d'exploitation.

4. Administration logicielle :

- Surveiller les performances de l'infrastructure logicielle et apporter les correctifs nécessaires.
- Gérer les licences et le mise à jour des logiciels.

Les deux services travaillent en étroite collaboration pour assurer le bon fonctionnement dusystème d'information de l'entreprise.

Les missions des deux servies sont complémentaires et essentielles pour la réussite de l'entreprise.

3.5. Étude de l'existant

3.5.1. Présentation du réseau de la BMT :

Le réseau de la BMT SPA est un réseau Ethernet qui relie les différents équipements d'un réseau LAN en se basant sur la topologie étoile .la norme de câblage utilisée est T568B, adaptée aux différents types de périphériques connectés.

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 (70 Mbit/s) par voie hertzienne en utilisant une fréquence radio privée et sécurisée.

3.5.2. Infrastructure réseau :

La BMTSpa possède deux sites physiques :

- Le port de Bejaia
- La ZEP (zone extra-portuaire).

1. Réseau local (LAN) :

Ce réseau combine WI-FI et câble et relie les sites distants par fibre optique, il comprend les éléments suivants :

- Un serveur de fichier pour le transfert de données sur le réseau.
- Un serveur d'intranet pour les applications de messagerie et d'internet.
- Un serveur de camera pour la surveillance de l'entreprise.
- Un serveur NAS pour le stockage des données accessible depuis les postes clients.
- Des postes de travail.
- Un switch à 24 ports reliant les serveurs web, les postes de travail et un pont d'accès Wi-Fi.

2. Réseau de production CTMS (Container Terminal Management System) :

Ce réseau est basé sur l'architecture client-serveur développé par un prestataire externe gère les activités opérationnelles (regroupe les domaines navires, conteneurs, etc.) et fonctionnelles (tout ce qui concerne la gestion des ressources humaines, parc automobile).

Il est composé de :

- Deux serveurs de bases de données Oracle.
- Deux serveurs d'applications TOMCAT.
- Deux serveur web Apache.
- Des postes de travail.
- Un switch reliant les postes de travail et les serveurs.

3. Réseau financier :

C'est un réseau privé et sensible pour cela, il est complètement isolé de l'internet, et utilisé quepour le service finance et comptabilité, il offre un accès restreint à une dizaine d'utilisateurs pour garantir la confidentialité des données.

Il est composé de :

- Un switch
- Un serveur financier
- Des postes de travail

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

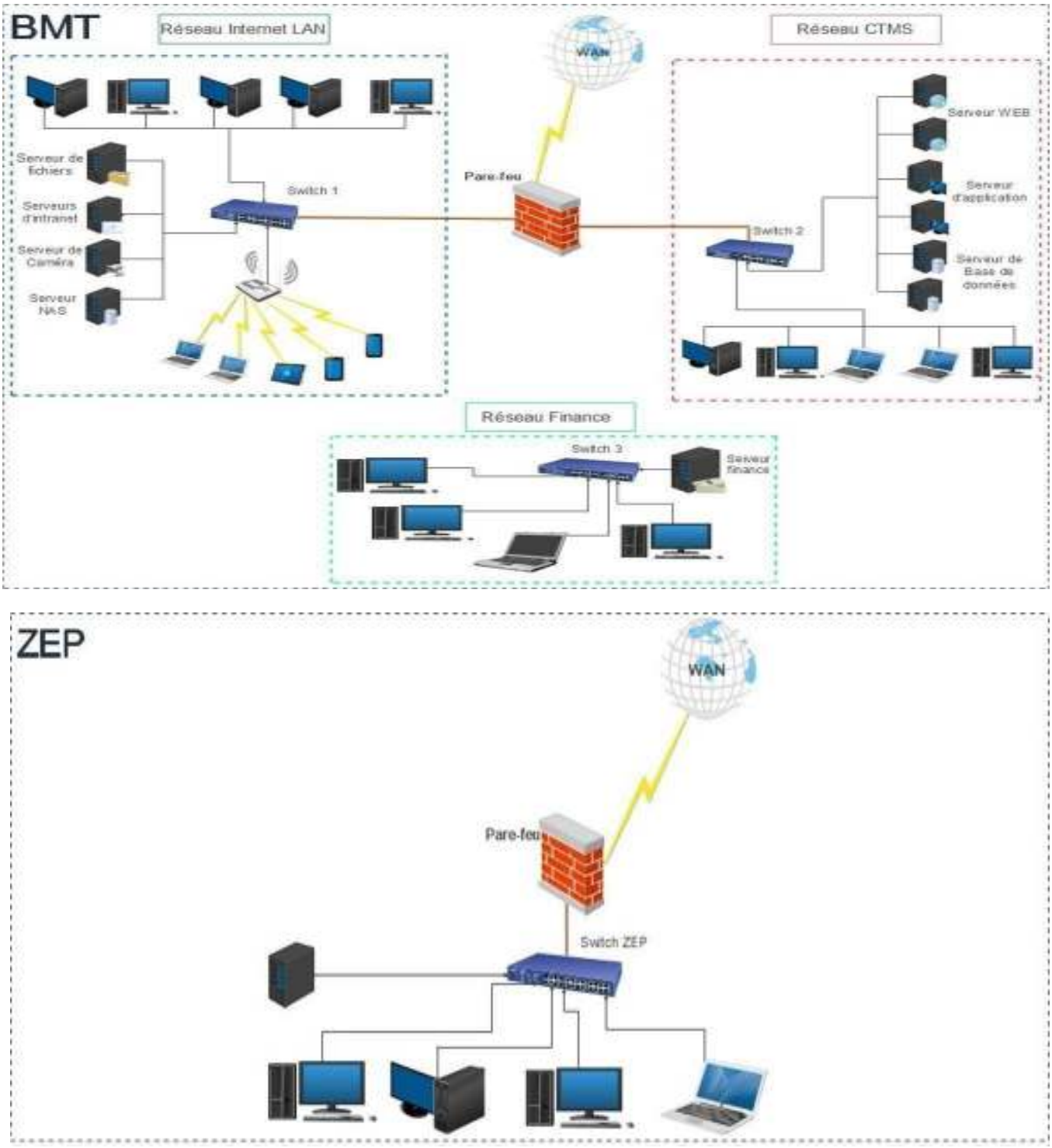


Figure 3. 5 : Architecture réseau de l'entreprise BMT

3.5.3. 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** :20Gbps -**Débit de protection contre lesmenaces** : 700 Mbps-1Gbps
Switch	Cisco sg200-26	-**RAM** :128Mo -**Mémoire Flash** :16Mo -**Performances :** (capacité de commutation) 52 Gbps -**Performance de transfert** (taillede paquet 64 octets) :38.69Mpps port :24 port
Serveur	HP Proliant DL380PGénération 10	-Processeur Intel Xeon Silver 4110(Octo-core 2.1 GHz/3.0 GHz Turbo-16 threads-Cache 11 Mo) Alimentation :500 Watts Adaptateur ethernet HPE 1 Gb 331i4 ports Eth Gigabit 10/10/1000 Mbit/s
Laptop	ASUS X409F	-**Processeur Core** : Intel i5 10 th Génération -**RAM** :16 Go -**SSD** :512 Go -**Processeur Graphique :** NVIDIAMX250

- **Le pare feu fortigate :** le pare feu de nouvelle génération (NGFW) fortigate de fortinet offre une solution de sécurité réseau complète de type Unified Threat Management (UTM) pour protéger les entreprises contre les menaces sophistiquées , bénéficiant de l'inspection approfondie des paquets , d'un filtrage Web avancé , d'une protection contre les intrusions robuste , d'un VPN SSL sécurisé , d'une protection antivirus et anti-malware efficace , d'un contrôle granulaire des applications et d'outils de gestion du réseau performants , le FortigateNGFW se distingue par ses performances élevées, sa facilite d'administration et sa compatibilité étendue avec les protocoles de sécurité standard , faisant de lui un choix idéal pour les entreprises de toutes tailles qui cherchent à sécuriser leur réseau.

Figure 3. 6 : le pare -feu Fortigate de Fortinet 1

3.6. Présentation de projet à réaliser :

L'analyse approfondie de l'architecture réseau de l'entreprise BMT est essentielle pour identifier les failles de sécurité et mettre en place des améliorations concrètes.

Notre mission consiste à déceler les lacunes en matière de sécurité et à proposer des solutions adéquates pour renforcer la protection du réseau et garantir son bon fonctionnement.

3.6.1. Problématiques :

Le réseau BMT comme n'importe quel autre réseau n'est pas sans faille en termes de sécurité réseau, à cause entre autres du nombre élevé de ses utilisateurs qui viennent de partout dans le monde.

Au cours de nos visites au sein de l'entreprise, nous avons constaté des anomalies au niveau de la sécurisation du réseau de l'entreprise, nous les énumérons comme suite :

- Absence d'un Fortigate qui doit filtrer les connexions entrantes et sortantes de l'infrastructure et bloquer les accès non autorisés.
- Absence d'une zone démilitarisée (DMZ) qui doit être accessibles de l'extérieur.
- L'absence de la redondance et de la haute disponibilité dans les réseaux de la BMT.

3.6.2. Solution proposée :

Le projet est de créer une passerelle entre le réseau interne et le réseau internet. La finalité est de pouvoir déployer la solution dans toutes les structures de nos problématiques au niveau de l'entreprise BMT. C'est dans le but qu'il nous a été demandé de mettre en place un firewall pour pouvoir gérer la connexion sortante à partir du réseau local, protéger le réseau interne des intrusions venant de l'extérieur et surveiller/tracer le trafic entre le réseau local et internet.

On a apporté quelques améliorations consistant à :

- ✓ Configurer les VLAN sur le réseau LAN 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.
- ✓ 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 pares-feux 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 site 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.

Assurer la disponibilité du réseau par la configuration de protocole de redondance HSRP sur le réseau LAN.

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

3.6.3. 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 :

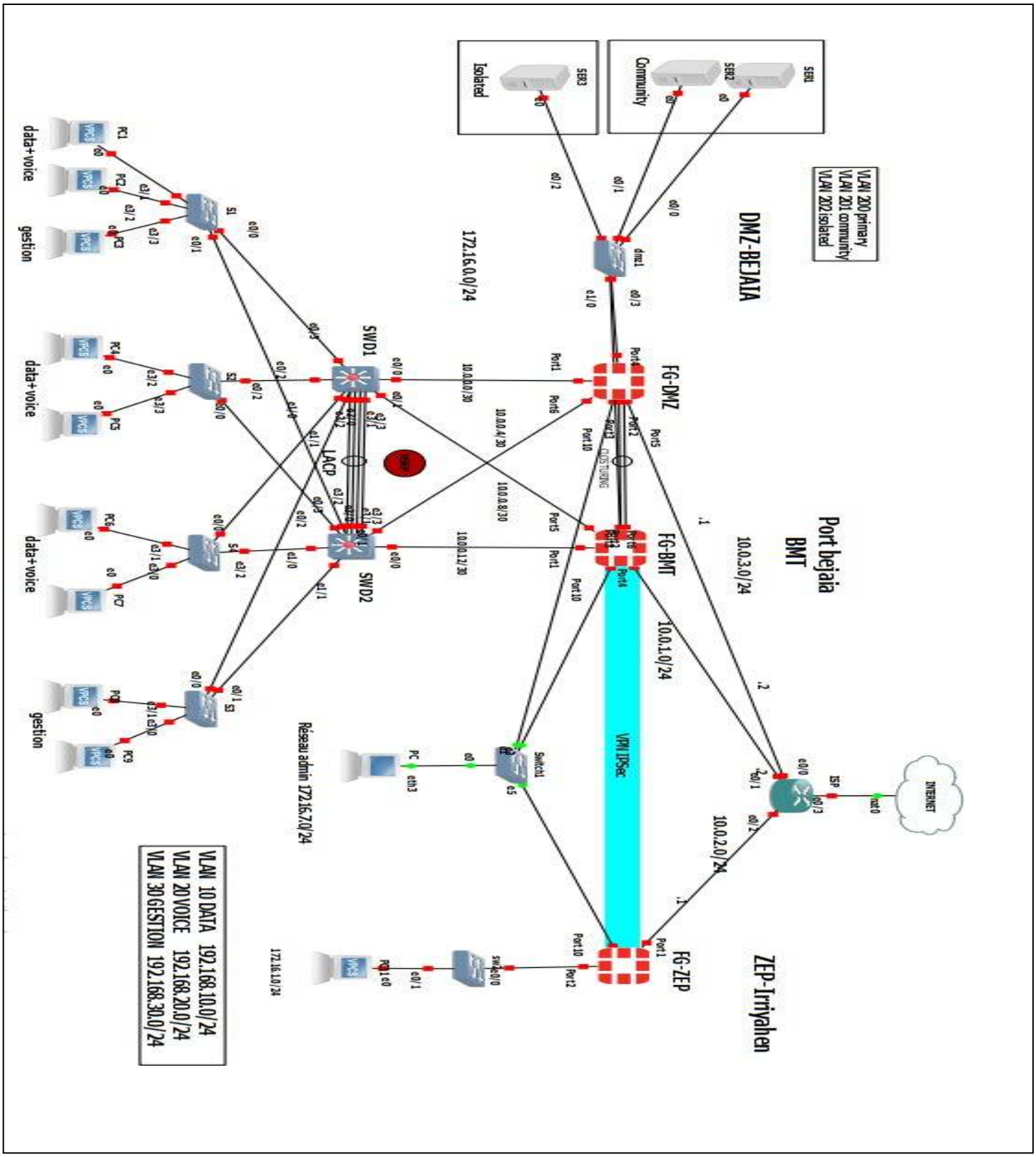


Figure 3. 7 : Nouvelle architecture réseau proposée.

Conclusion :

Dans ce chapitre nous avons présenté l'organisme d'accueil BMTSpa, précisément nous avons détaillé les missions du centre digitalisation et numérique ou notre stage s'est déroulé, notamment la compréhension de l'installation, de la construction et de l'utilité des différentes entités du réseau.

Des failles et faiblesses ont été identifiées, conduisant à la proposition de solution d'amélioration visant à optimiser la performance, la sécurité et la fiabilité du réseau.

Ces solution, détaillées dans le prochain chapitre, permettront à la BMTSpa de bénéficier d'un réseau informatique plus performant et sécurisé, répondant ainsi aux besoins croissants de l'entreprise.

Chapitre IV

Simulation et réalisation

Introduction

Ce chapitre propose une méthodologie rigoureuse pour optimiser l'architecture du réseau BMT, s'appuyant sur des outils de simulation et des tests approfondis.

La première étape consiste à sélectionner des outils de simulation adaptés, tels que VMware Workstation et GNS3, permettant de créer un environnement virtuel fidèle au réseau BMT. Ensuite, un processus détaillé de simulation et de configuration du réseau BMT amélioré est décrit, incluant la création du modèle e réseau virtuel, sa configuration minutieuse et l'intégration des améliorations proposées.

Enfin, des tests rigoureux sont menés pour évaluer les performances, la sécurité et la stabilité du réseau reconfiguré, répondant aux besoinscroissants de l'entreprise et le préparant aux défis futurs.

4.1. Présentations de l'environnement de travail

4.1.1. Présentation des logiciels utilisés

4.1.1.1. Logiciel la VMware Workstation :

Pour l'émulation de notre réseau, nous avons choisi la VMware Workstation. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être relies au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique.

Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs poste de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web.

Figure 4. 1 : VMware Workstation.

4.1.1.2. Graphical Network Simulator-3(GNS3) :

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau, nous avons opté pour l'utilisation de GNS3.un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il limite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel.

Figure 4. 2 : Graphical Network Simulator-3.

4.1.2. Présentation des équipements utilisés :

- **Windows server 2022 :** est la dernière version du système d'exploitation serveur de Microsoft, conçu pour les serveurs physiques et virtuels, il assure la protection des données critiques, simplifier la gestion de l'infrastructure informatique, améliorer les performances et garantit une compatibilité étendue. Windows server 2022 constitue une plateforme idéale pour exécuter des applications critiques et moderne avec une efficacité, une sécurité et une évolutivité accrues.

- **Windows 10 :** est un système d'exploitation conçu par Microsoft, il s'agit de la dernière version du système d'exploitation Windows NT et sorti en 2015. Il est également doté de fonctionnalités de sécurité renforcées et d'applications universelles qui fonctionnent sur tous les appareils Windows 10.
- **IOS Cisco :** est un système d'exploitation propriétaire développé par Cisco pour ses routeurs et commutateurs réseau. Il permet de gérer des réseaux complexes avec une efficacité redoutable, garantissant une connectivité stable et sécurisée pour les applications critiques. IOS dispose d'un ensemble de fonction de routage, de commutation et d'interconnexion de réseau.
- **Putty :** est une application open source qui établit des sessions à distance sur des ordinateurs à l'aide des protocoles réseaux tels que SSH, Telnet et login.
- **Wireshark :** est un analyseur de paquets réseau open source reconnu pour sa puissance et sa polyvalence .il permet de capturer le trafic réseau en temps réel sur une interface réseau, puis de l'analyser en détail pour identifier d'éventuels problèmes, diagnostiquer des pannes de réseau, comprendre les protocoles réseau et même décoder les données échangées.

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
SWD1 (routeur1)	Ethernet 0/0 Ethernet 0/1	10.0.0.0/30 10.0.0.8/30
SWD2 (routeur2)	Ethernet 0/0 Ethernet 0/1	10.0.0.12/30 10.0.0.4/30
FW1	Port 1(LAN) Port 6(LAN) Port 5 (ISP)	10.0.0.0/30 10.0.0.4/30 10.0.3.0/24
FW2	Port 1(LAN) Port 4(ZEP) Port 5(LAN)	10.0.0.12/30 10.0.1.0/24 10.0.0.8/30
FW3	Port 1(ISP)	10.0.2.0/24

4.2.2. La table d'adressage des VLAN

4.2.2.1. Réseau LAN

Tableau 4. 2 : la table d'adressage des VLAN du réseau LAN

Nom des VLAN	ID du VLAN	Passerelle (LAN)	Passerelle HSRP
VLAN Data	10	192.168.10.253/24 192.168.10.254/24	192.168.10.252/24
VLAN Voice	20	192.168.20.253/24 192.168.20.254/24	192.168.20.252/24
VLAN Gestion	30	192.168.30.253/24 192.168.30.254/24	192.168.30.252/24

4.2.2.2. La DMZ-Bejaia

Tableau 4. 3 : La table d'adressage des VLAN de la DMZ-Bejaia

Nom des PVLAN	ID du PVLAN	Adresse de PVLAN
Primary VLAN	200	172.16.0.2/24
Community VLAN	201	172.16.0.3/24
Isolated VLAN	202	172.16.0.4/24

4.3. Configuration de réseau LAN

4.3.1. Configuration des VLAN

4.3.1.1. Configuration des commutateurs de distribution en mode trunk

Nous allons configurer les portes des Switch distribution et accès en mode trunk pour faire passer les différents VLAN sur le réseau, les interfaces à configurer dans ce cas sont celles entre les commutateurs de la couche d'accès et les commutateurs de la couche distribution.

```
SWD1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#interface range ethernet 3/0-3 , ethernet 1/0-1 , ethernet 0/2-3
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#exit
SWD1(config)#
```

Listing 4. 1 : Configuration des commutateurs de distribution en mode trunk

4.3.1.2. Configuration des commutateurs d'accès en mode trunk

```
S1(config)#interface range ethernet 3/0-1
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#switchport voice vlan 20
S1(config-if-range)#exit
```

Listing 4. 2 : configuration des commutateurs d'accès en mode trunk

4.3.1.3. Activation de protocole VTP (VLAN Trunking Protocol)

Il est nécessaire de l'utiliser pour simplifier et faciliter la gestion des VLAN sur un réseau commuté CISCO, il permet de centraliser la configuration et la synchronisation des VLAN, réduisant ainsi le temps et les efforts nécessaires à la gestion manuelle de chaque commutateur individuel. Parmi ses avantages :

- Configurer les VLAN sur un seul commutateur et propagez-les automatiquement à tous les autres.
- Eliminer la configuration manuelle de chaque VLAN sur chaque commutateur.
- Assurer une configuration VLAN uniforme sur l'ensemble du réseau.

a) La configuration des commutateurs de distribution en mode serveur VTP

```
SWD1(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD1(config)#vtp domain bmt-vtp
Changing VTP domain name from NULL to bmt-vtp
SWD1(config)#vtp password cisco
Setting device VTP password to cisco
SWD1(config)#vtp version 2
SWD1(config)#vtp pruning
Pruning switched on
```

Listing 4. 3 : configuration de VTP serveur.

b) La configuration des commutateurs d'accès en mode client VTP

```
S1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
S1(config)#vtp domain bmt-vtp
Domain name already set to bmt-vtp.
S1(config)#vtp password cisco
Setting device VTP password to cisco
S1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
```

Listing 4. 4 : la configuration de VTP client.

4.3.1.4. Création des VLAN au niveau des commutateurs de distribution

Nous allons crées les VLAN sur le SWD1 qui est configurer en mode VTP serveur pour diffuser ses VLAN sur tous les autres commutateurs :

```
SWD1(config)#vlan 10
SWD1(config-vlan)#name data
SWD1(config-vlan)#vlan 20
SWD1(config-vlan)#name voice
SWD1(config-vlan)#vlan 30
SWD1(config-vlan)#name gestion
SWD1(config-vlan)#end
```

```
SWD1#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et0/0, Et0/1, Et1/2, Et1/3
                                                   Et2/0, Et2/1, Et2/2, Et2/3
10   data                                active
20   voice                               active
30   gestion                             active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
```

Listing 4. 5 : Création des VLAN.

4.3.1.5. Affectation des portes de commutateurs accès au VLAN correspond

Nous allons configurer chaque port de commutateur avec le VLAN selon la table d'adressagedes VLAN du réseau LAN :

```
S1(config)#interface range ethernet 3/0-1
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#switchport voice vlan 20
S1(config-if-range)#exit
```

```
S1#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------
------
1    default                             active    Et0/2, Et0/3, Et1/0, Et1/
1
                                                   Et1/2, Et1/3, Et2/0, Et2/
1
                                                   Et2/2, Et3/2, Et3/3
10   data                                active    Et3/0, Et3/1
20   voice                               active    Et3/0, Et3/1
30   gestion                             active    Et2/3
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
```

Listing 4. 6 : Configuration de VLAN sur le commtateur d'accès.

4.3.2. Configuration de protocole LACP

Link Agrégation Control Protocol est un protocole standard (EtherChannel) défini par IEEE 802.3 il permet de regrouper plusieurs liens logiques en un seul lien physique. La principale de LACP est améliorée la disponibilité et la bande passante d'une connexion réseau en utilisant plusieurs ports en tant qu'un seul grand port.

Pour ce faire, nous allons crées un channel groupe qui regroupe toutes les interfaces reliant les deux switches distributeurs. La configuration de ce protocole est montrée ci-dessous

```
SWD1#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#interface range ethernet 3/0-3
SWD1(config-if-range)#channel-group 1 mode active
Creating a port-channel interface Port-channel 1
```

Listing 4. 7 : Configuration de protocole LACP.

4.3.3. Configuration de routeur

4.3.3.1. Création de routage inter-VLAN :

```
SWD1(config)#interface vlan 10
SWD1(config-if)#ip address 192.168.10.253 255.255.255.0
SWD1(config-if)#EXIT
SWD1(config)#interface vlan 20
SWD1(config-if)#ip address 192.168.20.253 255.255.255.0
SWD1(config-if)#EXIT
SWD1(config)#interface vlan 30
SWD1(config-if)#ip address 192.168.30.253 255.255.255.0
SWD1(config-if)#EXIT
```

```
SWD2(config)#interface vlan 10
SWD2(config-if)#ip address 192.168.10.254 255.255.255.0
SWD2(config-if)#EXIT
SWD2(config)#interface vlan 20
SWD2(config-if)#ip address 192.168.20.254 255.255.255.0
SWD2(config-if)#EXIT
SWD2(config)#interface vlan 30
SWD2(config-if)#ip address 192.168.30.254 255.255.255.0
SWD2(config-if)#EXIT
```

Listing 4. 8 : configuration de routage inter-VLAN.

4.3.3.2. Configuration de protocole HSRP :

Pour la mise en place de protocole HSRP, nous allons configurer les interfaces de SWD1(routeur 1) en mode active, tandis que celles du SWD2(routeur 2) seront en mode standby.

Pour ce faire nous allons ajouter les deux commandes suivantes à la configuration des interfaces de SWD1(routeur 1) :

- **Standby X priority 150 :** par 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 :

```
SWD1(config)#interface vlan10
SWD1(config-if)#standby version 2
SWD1(config-if)#standby 10 ip 192.168.10.252
SWD1(config-if)#standby 10 priority 150
SWD1(config-if)#standby 10 preempt
SWD1(config-if)#exit
```

```
SWD2(config)#interface vlan 10
SWD2(config-if)#standby version 2
SWD2(config-if)#standby 10 ip 192.168.10.252
SWD2(config-if)#exit
```

Listing 4. 9 : configuration de protocole HSRP.

De même pour les vlan 20 et 30

4.3.3.3. Configuration de protocole DHCP

Le protocole réseau DHCP (Dynamic Host Configuration Protocol) assure la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau.

Nous allons configurer le DHCP sur le 10-30 pour permettre l'attribution automatique des adresses IP et de même pour le SWD2(routeur 2).

```
SWD1(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
SWD1(config)#ip dhcp pool vlan30
SWD1(dhcp-config)#network 192.168.30.0 255.255.255.0
SWD1(dhcp-config)#default-router 192.168.30.252
SWD1(dhcp-config)#dns-server 8.8.8.8
SWD1(dhcp-config)#exit
```

Listing 4. 10 : Configuration de protocole DHCP.

4.3.3.4. Configurations de protocole OSPF (Open Shortest Path First) au niveau des routeur (SWD1 et SWD2) :

Est un protocole de routage conçu pour trouver le chemin le plus court entre deux points d'un réseau en minimisant le nombre de sauts entre les routeurs (SWD1et SWD2).

```
SWD1(config)#router ospf 1
SWD1(config-router)#network 10.0.0.0 252.0.0.0 area 0
SWD1(config-router)#network 10.0.0.8 252.0.0.0 area 0
SWD1(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
SWD1(config)#EXIT
```

```
SWD2(config)#router ospf 1
SWD2(config-router)#network 10.0.0.4 252.0.0.0 area 0
SWD2(config-router)#network 10.0.0.12 252.0.0.0 area 0
SWD2(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
SWD2(config)#EXIT
```

Listing 4. 11 : Configuration de protocole OSPF au niveau des routeurs (SWD1 et SWD2)

4.3.3.5. Création des VALN sur la DMZ :

Pour configurer les VLAN sur le switch DMZ il faut d'abord désactiver le mode VTP (ou bien VTP en mode transparent).

```
dmz(config)#vlan 200
dmz(config-vlan)#private-vlan primary
dmz(config-vlan)#private-vlan association 201,202
dmz(config-vlan)#exit
dmz(config)#vlan 201
dmz(config-vlan)#private-vlan community
dmz(config-vlan)#exit
dmz(config)#vlan 202
dmz(config-vlan)#private-vlan isolated
dmz(config-vlan)#exit
```

Listing 4. 12 : création des PVLAN au niveau de la DMZ.

De même nous allons configurer le switch de la DMZ avec les ID VLAN suivante :

- VLAN primary 200
- VLAN community 201
- VLAN isolated 202

4.3.3.6. Affectation des portes sur la DMZ au PVLAN correspond

```
dmz(config)#interface range ethernet 0/0-1
dmz(config-if-range)#switchport mode private-vlan host
dmz(config-if-range)#switchport private-vlan host-association 200 201
dmz(config-if-range)#exit
dmz(config)#interface ethernet 0/2
dmz(config-if)#switchport mode private-vlan host
dmz(config-if)#switchport private-vlan host-association 200 202
dmz(config-if)#exit
dmz(config)#interface range ethernet 0/3 , ethernet 1/0
dmz(config-if-range)#switchport mode private-vlan promiscuous
dmz(config-if-range)#switchport private-vlan mapping 200 201,202
dmz(config-if-range)#exit
```

Listing 4. 13 : affectation des ports du Switch DMZ au PVLAN.

4.3.3.7. Configuration de NAT sur le routeur :

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

La configuration de NAT est donnée par les commandes suivantes :

```
ISP(config)#ip access-list standard NAT
ISP(config-std-nacl)#permit 10.0.1.0 0.0.0.255
ISP(config-std-nacl)#permit 10.0.2.0 0.0.0.255
ISP(config-std-nacl)#permit 10.0.3.0 0.0.0.255
ISP(config-std-nacl)#exit
ISP(config)#interface range ethernet 0/0-2
ISP(config-if-range)#ip nat inside
ISP(config-if-range)#exit
ISP(config)#interface ethernet 0/3
ISP(config-if)#ip nat outside
ISP(config-if)#exit
ISP(config)#ip nat inside source list nat interface ethernet 0/3 overload
ISP(config)#exit
```

Listing 4. 14 : Configuration de NAT.

4.3.3.8. Configuration de protocole OSPF au niveau de routeur ISP

```
ISP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#router ospf 1
ISP(config-router)#network 10.0.3.0 0.0.0.255 area 0
ISP(config-router)#network 10.0.2.0 0.0.0.255 area 0
ISP(config-router)#network 10.0.1.0 0.0.0.255 area 0
ISP(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
ISP(config)#exit
```

Listing 4. 15 : Configuration de protocole OSPF au niveau du routeur ISP.

4.4. Configuration des pare-feu FG-BMT et FG-ZEP

4.4.1. Configurer l'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'adresse d'interface 172.16.7.0/24.

```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname FG-BMT

FortiGate-VM64-KVM (global) # end

FG-BMT # config system interface

FG-BMT (interface) # edit port10

FG-BMT (port10) # set mode static

FG-BMT (port10) # set ip 172.16.7.20/24

FG-BMT (port10) # set allowaccess ping https http
```

Figure 4. 3 : configuration de l'accès au Fortigate de BMT.

```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname FG-ZEP

FortiGate-VM64-KVM (global) # end

FG-ZEP # config system interface

FG-ZEP (interface) # edit port10

FG-ZEP (port10) # set mode static

FG-ZEP (port10) # set ip 172.16.7.15/24

FG-ZEP (port10) # set allowaccess ping https http
```

Figure 4. 4 : configuration de l'accès au fortigate ZEP.

NB : La commande « set allow access ping https http » permet l'accès au pare-feu sur tous les ports.

Pour se connecter à l'interface d'administrateur de fortigate, nous accédant à google chrome, nous saisissons l'adresse IP du pare-feu dans la barre d'adresse, appuyer sur entrée, connecter vous «admin » et le mot de passe configurer, une fois connecter, vous aurez accès à toutes les fonctionnalités d'administration.

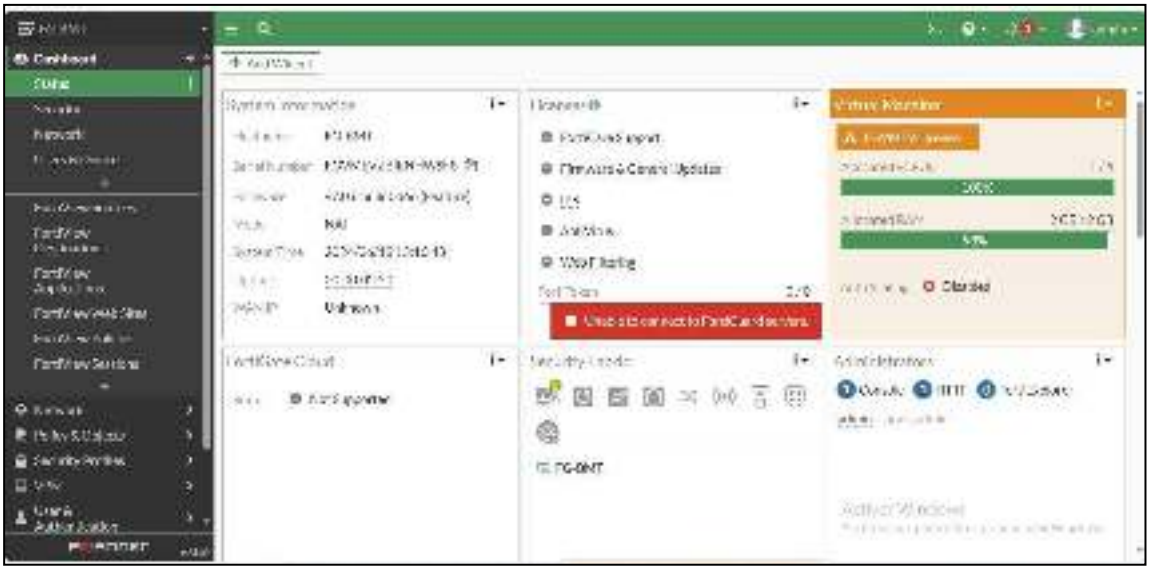
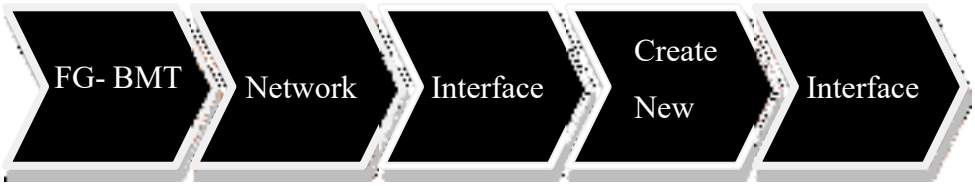


Figure 4. 5 : interface d'accueil du pare-feu fortigate (BMT).

Figure 4. 6 : interface d'accueil du pare-feu fortigate (ZEP).

4.4.2. 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.

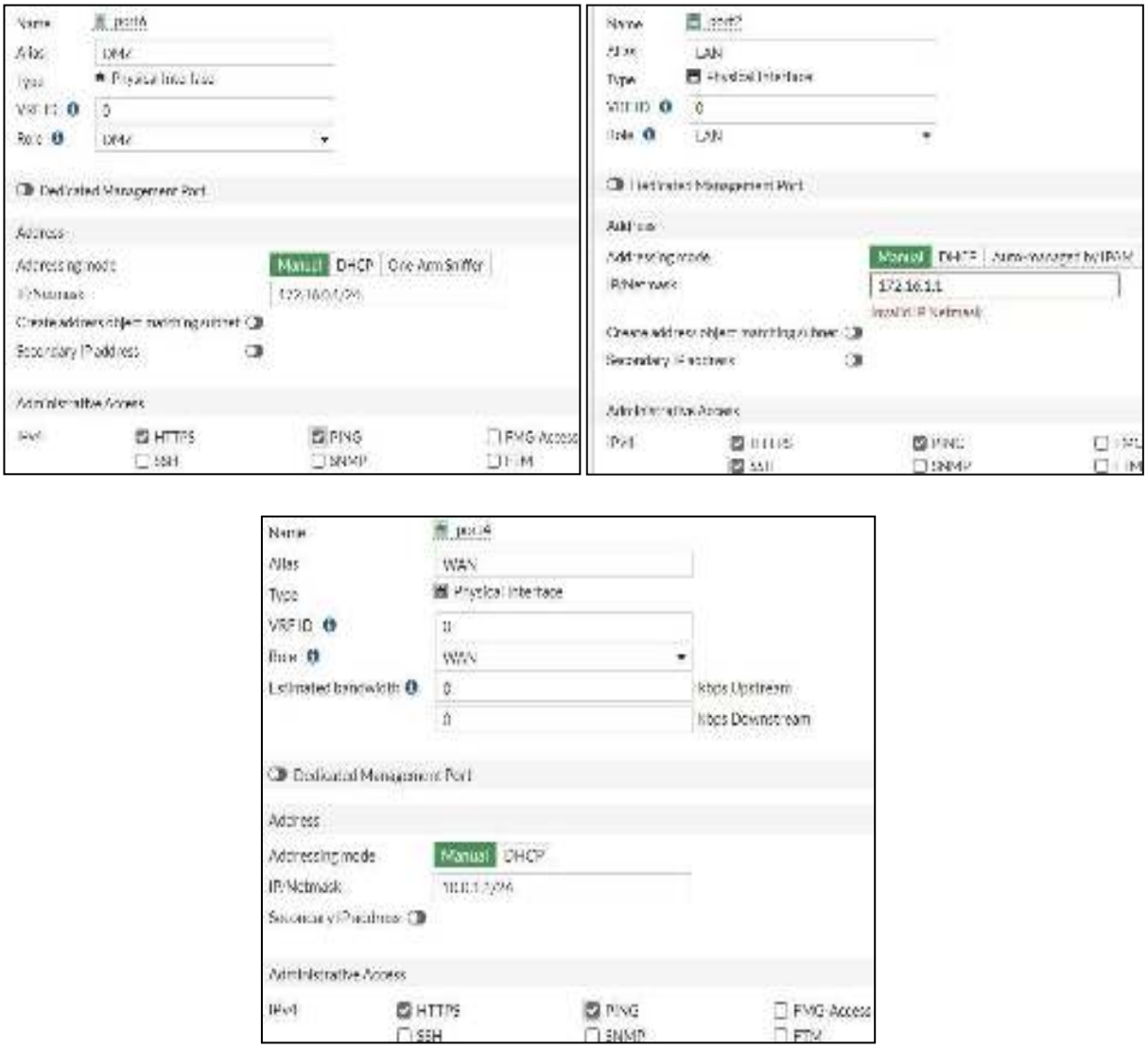
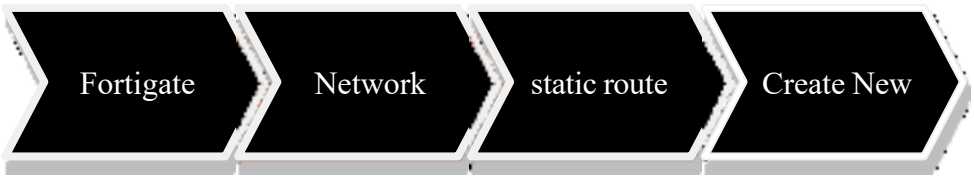


Figure 4. 7 : configuration des interfaces de pare-feu.

4.4.3. 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 :



FG-BMT :

Figure 4. 8 : configuration de routage statique du FG-BMT.

FG-ZEP

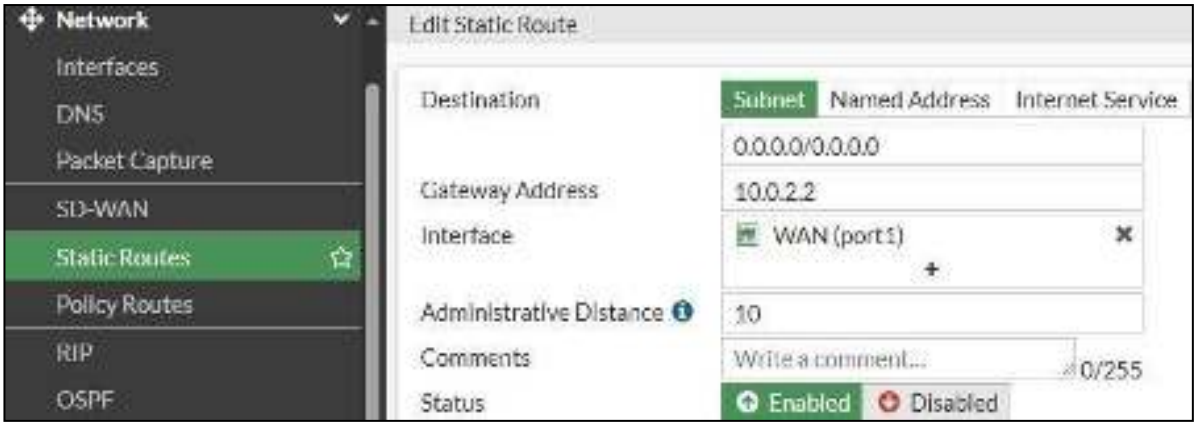


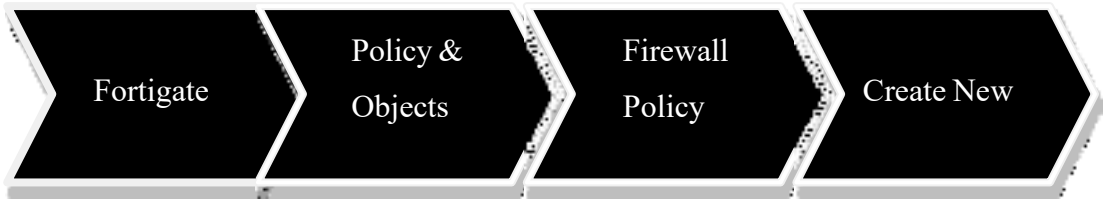
Figure 4. 9 : configuration de routage statique du FG-ZEP.

4.4.4. Création d'une liste de contrôle d'accès :

Pour sécuriser l'accès des réseaux (LAN, WAN, DMZ) à l'internet, une liste de contrôle d'accès (ACL) est implémentée. Cette liste définit des règles pour filtrer les paquets IP selon des critères spécifiques (adresses IP, protocoles, ports).

L'ACL agit comme un gardien, analysant chaque paquet et déterminant son sort (blocage ou autorisation) en fonction des règles définies. Cela permet de bloquer les intrusions, de restreindre l'accès aux services et de prioriser le trafic, garantissant ainsi la sécurité et une utilisation efficace de la bande passante.

La création des 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.

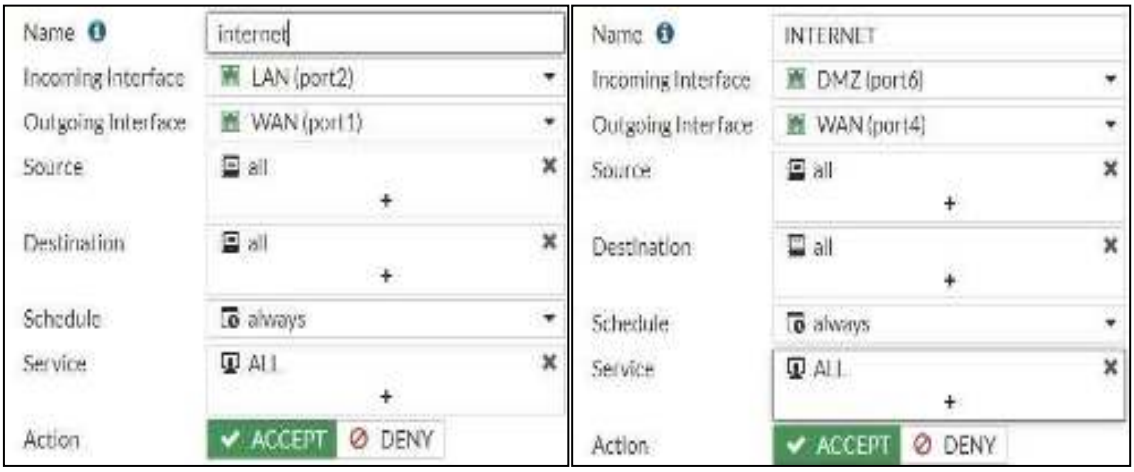


Figure 4. 10 : Création de la liste de contrôle d'accès sur le pare-feu

4.4.5. 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 toute la configuration.

Il existe deux méthodes pour la configuration de NAT sur fotigate :

1. L'utilisation d'une seule adresse IP publique pour l'ensemble des machines, c'est la méthode que nous avons utilisée pour configurer le NAT sur nos réseaux LAN et DMZ, il suffit d'activer le NAT pour les Policy configurés et choisir « use Outgoing Interface Address ».

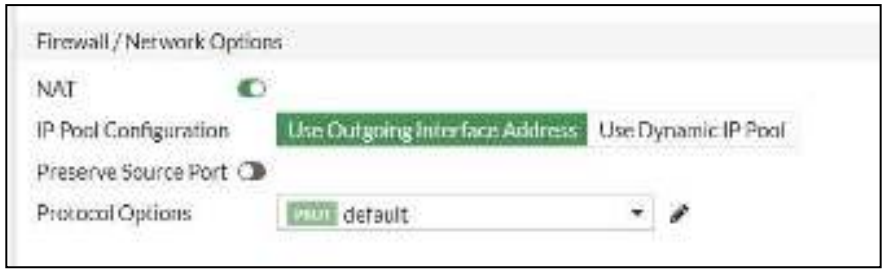


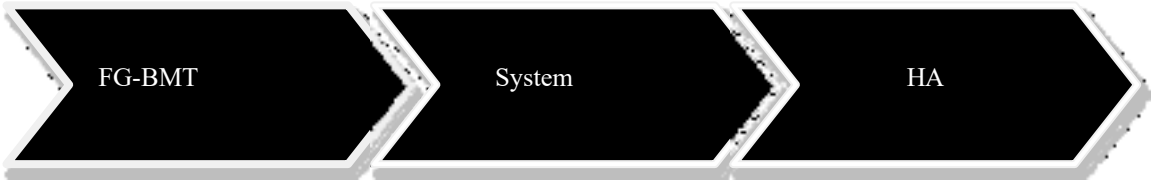
Figure 4. 11 : activation du NAT sur fortigate

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.

4.4.6 Configuration de la haute disponibilité :

Afin de garantir un fonctionnement continu de nos réseaux, nous allons configurer la haute disponibilité (en anglais High Availability (HA) sur deux pares-feux. En cas de panne du pare-feu principal, le pare-feu secondaire basculera de manière transparente en mode actif, garantissant une protection réseau continue jusqu'à la remise en service du pare-feu principal.

Cette (HA) sera configurer en mode active-active, le premier pare-feu principal, désigne comme maitre, fonctionnera activement, tandis que le pare-feu secondaire, en tant qu'esclave, restera en veille. Nous allons créer le groupe de HA avec un mot de passe et on spécifier les interfaces que le pare-feu esclave doit prendre en charge ainsi que l'interface Heatbeat qui relie les deux pares-feux.



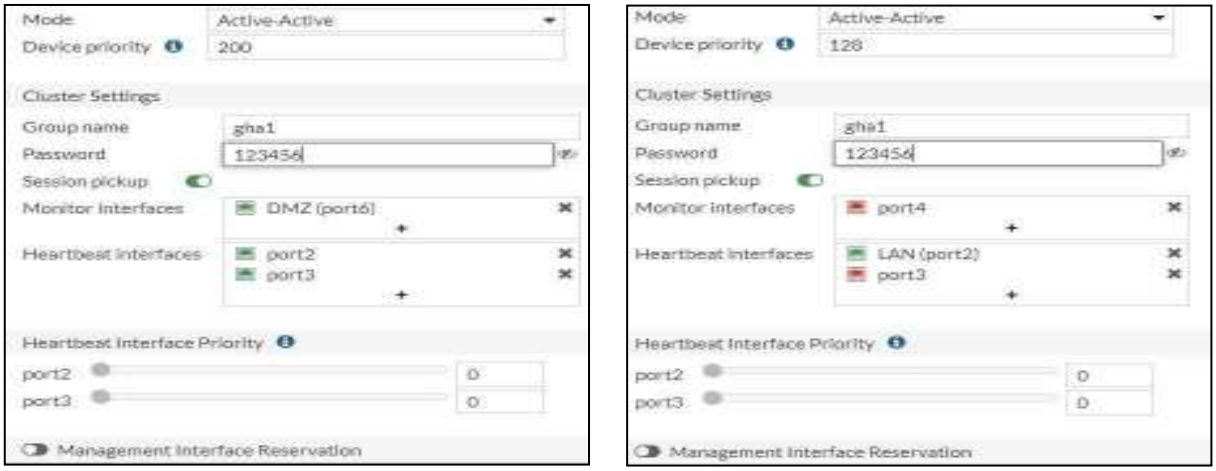


Figure 4. 12 : Configuration de la haute disponibilité sur les FG-BMT et FG-DMZ.

Le résultat de la synchronisation des deux pares-feux est illustre par la figure ci-dessous.

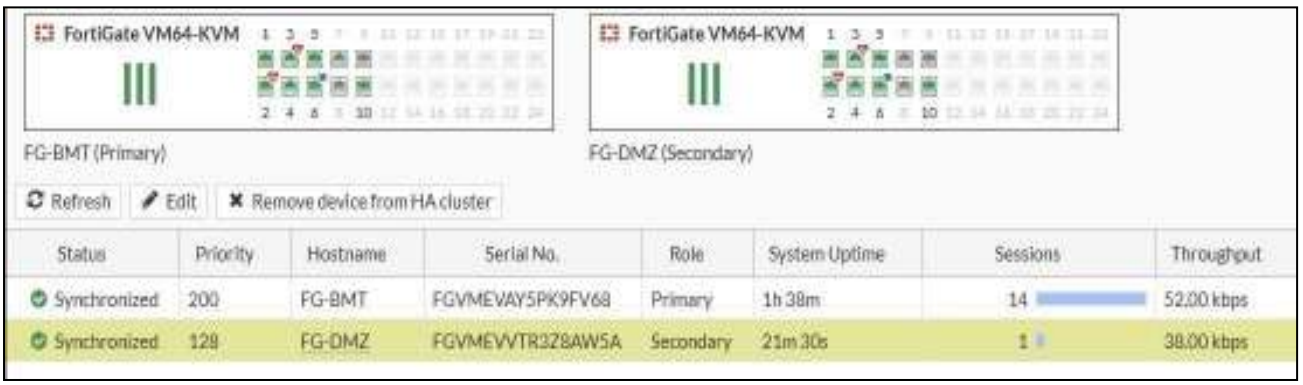


Figure 4. 13 : Synchronisation des pare-feu FG-BMT et FG-DMZ.

4.5. Configuration de VPN site à site :

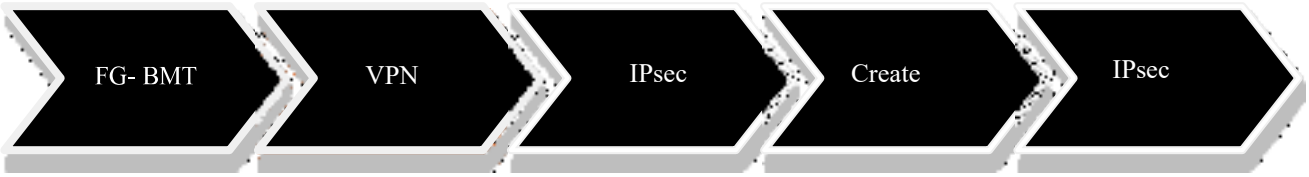
Dans cette partie, nous allons expliquer la création d'un tunnel VPN site à site sur nos pares-feux tels que :

- VPN (BMT-ZEP) sur FG-BMT de site port Bejaia
- VPN (ZEP-BMT) sur FG-ZEP de site irriyahen

4.5.1. Au niveau de fortigate Bejaia :

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

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 son type ainsi que le type de périphérique distant avec lequel ce VPN sera créé.

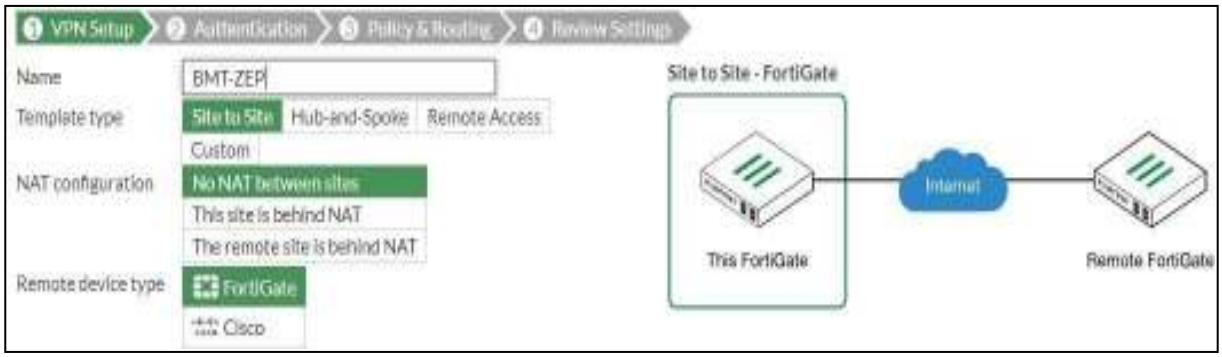


Figure 4. 14 : création de VPN IPsec BMT-ZEP.

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.

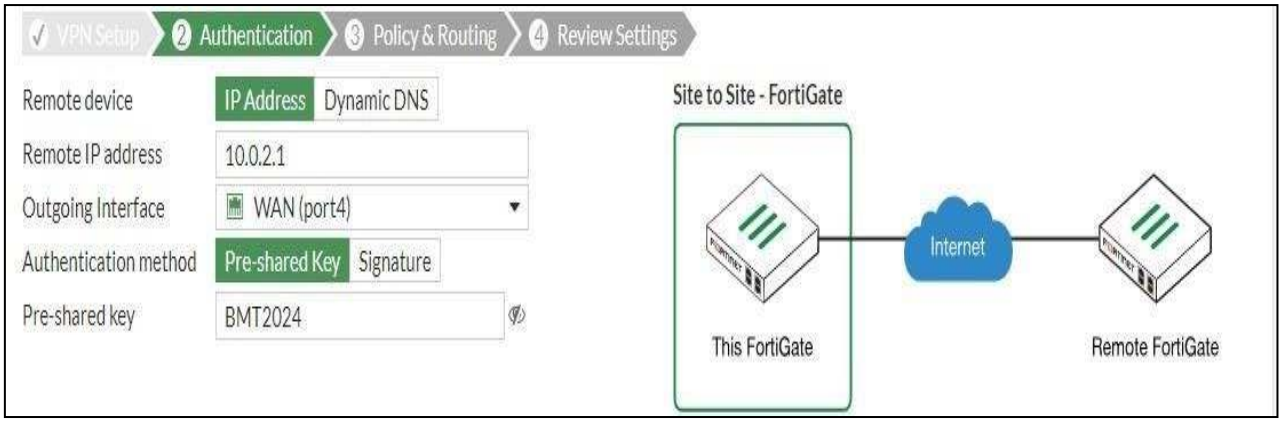


Figure 4. 15 : authentification de VPN BMT-ZEP.

Dans cette étape nous allons sélectionner les réseaux locaux LAN et les réseaux distants pour donner l'accès à distance.

Figure 4. 16 : les interfaces de Policy et de routage sur le VPN BMT-ZEP.

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

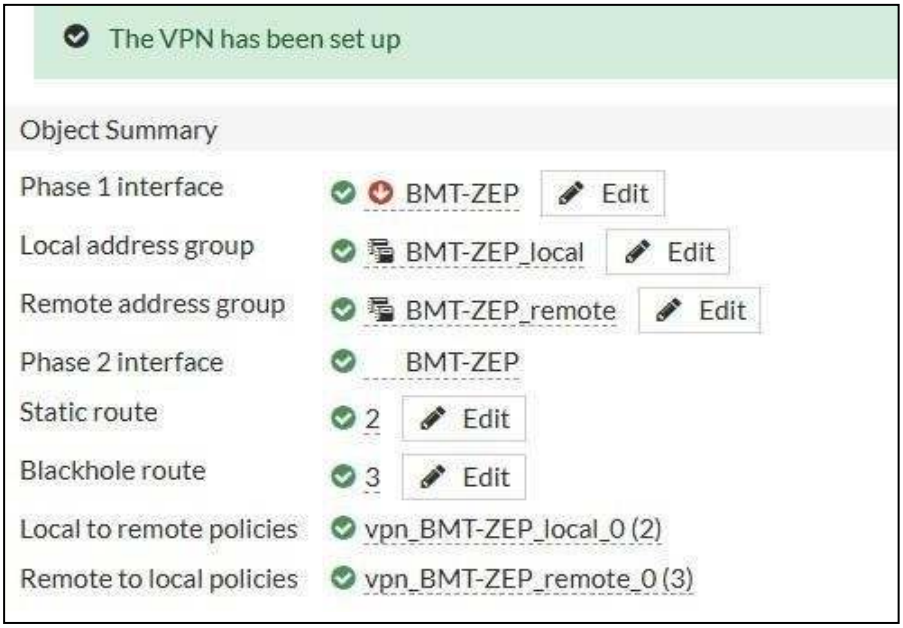


Figure 4. 17 : finalisation de la création de VPN BMT-ZEP.

4.5.2. Au niveau de fortigate ZEP :

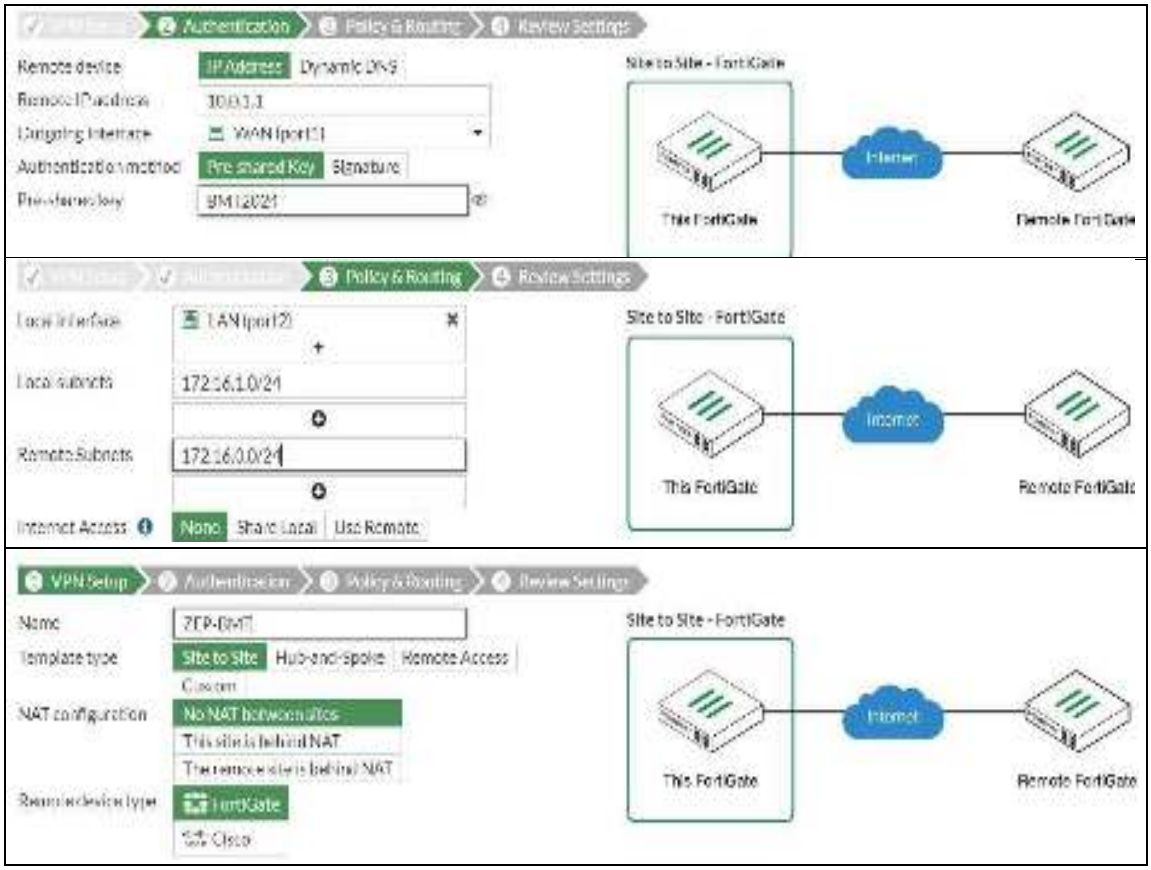


Figure 4. 18 : création de VPN IPSec ZEP-BMT.

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 a la création de :

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

FG-BMT

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.0.2.2	WAN (port1)	Enabled	
ZEP-BMT_remote	10.0.1.1	ZEP-BMT	Enabled	VPN: ZEP-BMT (Created by VPN wizard)
ZEP-BMT_remote		Blackhole	Enabled	VPN: ZEP-BMT (Created by VPN wizard)

FG-ZEP

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.0.1.2	WAN (port4)	Enabled	
BMT-ZEP_remote	10.0.2.1	BMT-ZEP	Enabled	VPN: BMT-ZEP (Created by VPN wizard)
BMT-ZEP_remote		Blackhole	Enabled	VPN: BMT-ZEP (Created by VPN wizard)

Figure 4. 19 : Routes statique créées par les VPN configurés.

Des adresses locales et distantes

FG-BMT

Name	Details
IP Range/Subnet 7	
BMT-ZEP_local_subnet_1	172.16.0.0/24
BMT-ZEP_remote_subnet_1	172.16.1.0/24
FABRIC_DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
all	0.0.0.0/0
none	0.0.0.0/32

FG-ZEP

Name	Details
IP Range/Subnet 7	
FABRIC_DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
ZEP-BMT_local_subnet_1	172.16.1.0/24
ZEP-BMT_remote_subnet_1	172.16.0.0/24
all	0.0.0.0/0
none	0.0.0.0/32

Figure 4. 20 : Adresses local et distantes créées par les VPN configurés.

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

FG-BMT

Name	Source	Destination	Schedule	Service	Action
BMT-ZEP → DMZ (port6) 1					
DMZ (port6) → BMT-ZEP 1					
DMZ (port6) → WAN (port4) 1					

FG-ZEP

Name	Source	Destination	Schedule	Service	Action
LAN (port2) → WAN (port1) 1					
internet	all	all	always	ALL	ACCEPT
LAN (port2) → ZEP-BMT 1					
ZEP-BMT → LAN (port2) 1					

Figure 4. 21 : Listes de contrôles d'accès créés par les VPN configurés.

4.5.3. Etablissement du tunnel VPN

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

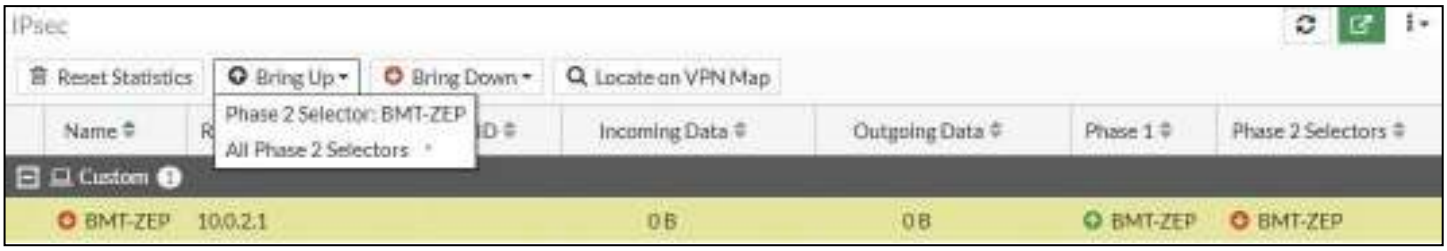


Figure 4. 22 : Etablissement de tunnel VPN site à site

4.6. Test et Vérification

4.6.1 Vérification de la configuration

❖ **Vérification de protocole LACP**

```
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
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et3/0(P)    Et3/1(P)    Et3/2(P)
```

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

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

        A - formed by Auto LAG


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et3/0(P)    Et3/1(P)    Et3/2(P)
```

Figure 4. 23 : Vérification du protocole LACP.

❖ **Vérification de protocole HSRP**

```
SWD1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   150 P Active  local           192.168.10.254  192.168.10.252
Vl20        20   150 P Active  local           192.168.20.254  192.168.20.252
Vl30        30   150 P Active  local           192.168.30.254  192.168.30.252
```

```
SWD2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   100   Standby 192.168.10.253  local           192.168.10.252
Vl20        20   100   Standby 192.168.20.253  local           192.168.20.252
Vl30        30   100   Standby 192.168.30.253  local           192.168.30.252
```

Figure 4. 24 : Vérification du protocole HSRP.

❖ **Vérification de protocole OSPF**

```
SWD1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.30.254    1   FULL/DR         00:00:39    192.168.30.254  Vlan30
192.168.30.254    1   FULL/DR         00:00:39    192.168.20.254  Vlan20
192.168.30.254    1   FULL/DR         00:00:38    192.168.10.254  Vlan10
```

```
SWD2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.30.253    1   FULL/BDR        00:00:37    192.168.30.253  Vlan30
192.168.30.253    1   FULL/BDR        00:00:34    192.168.20.253  Vlan20
192.168.30.253    1   FULL/BDR        00:00:34    192.168.10.253  Vlan10
```

Figure 4. 25 : Vérification de protocole OSPF

❖ **Vérification de routage statique du réseau LAN**

```
SWD1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.253/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.253/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.253/32 is directly connected, Vlan30
```

```
SWD2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.254/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.254/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.254/32 is directly connected, Vlan30
```

Figure 4. 26 : Vérification de routage sur le réseau LAN.

4.6.2 Test de routage inter VLAN du réseau LAN

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

```
PC1> ip dhcp
DDORA IP 192.168.10.11/24 GW 192.168.10.252
```

```
PC2> ip dhcp
DDORA IP 192.168.10.12/24 GW 192.168.10.252
```

```
PC3> ip dhcp
DDORA IP 192.168.30.11/24 GW 192.168.30.252
```

Figure 4. 27 : Attribution des adresses IP par le protocole DHCP.

❖ **Test de routage inter VLAN du réseau LAN**.

```
PC1> ping 192.168.10.253
84 bytes from 192.168.10.253 icmp_seq=1 ttl=255 time=1.167 ms
84 bytes from 192.168.10.253 icmp_seq=2 ttl=255 time=1.343 ms
84 bytes from 192.168.10.253 icmp_seq=3 ttl=255 time=1.467 ms
84 bytes from 192.168.10.253 icmp_seq=4 ttl=255 time=1.616 ms
84 bytes from 192.168.10.253 icmp_seq=5 ttl=255 time=1.246 ms

PC1> ping 192.168.20.253
84 bytes from 192.168.20.253 icmp_seq=1 ttl=255 time=1.281 ms
84 bytes from 192.168.20.253 icmp_seq=2 ttl=255 time=1.106 ms
84 bytes from 192.168.20.253 icmp_seq=3 ttl=255 time=1.285 ms
84 bytes from 192.168.20.253 icmp_seq=4 ttl=255 time=1.862 ms
84 bytes from 192.168.20.253 icmp_seq=5 ttl=255 time=2.362 ms

PC1> ping 192.168.30.253
84 bytes from 192.168.30.253 icmp_seq=1 ttl=255 time=1.674 ms
84 bytes from 192.168.30.253 icmp_seq=2 ttl=255 time=1.159 ms
84 bytes from 192.168.30.253 icmp_seq=3 ttl=255 time=1.412 ms
84 bytes from 192.168.30.253 icmp_seq=4 ttl=255 time=1.425 ms
84 bytes from 192.168.30.253 icmp_seq=5 ttl=255 time=1.696 ms
```

```
PC1> ping 192.168.10.254
84 bytes from 192.168.10.254 icmp_seq=1 ttl=255 time=2.490 ms
84 bytes from 192.168.10.254 icmp_seq=2 ttl=255 time=1.592 ms
84 bytes from 192.168.10.254 icmp_seq=3 ttl=255 time=1.764 ms
84 bytes from 192.168.10.254 icmp_seq=4 ttl=255 time=1.675 ms
84 bytes from 192.168.10.254 icmp_seq=5 ttl=255 time=1.610 ms

PC1> ping 192.168.20.254
84 bytes from 192.168.20.254 icmp_seq=1 ttl=255 time=1.998 ms
84 bytes from 192.168.20.254 icmp_seq=2 ttl=255 time=1.495 ms
84 bytes from 192.168.20.254 icmp_seq=3 ttl=255 time=1.780 ms
84 bytes from 192.168.20.254 icmp_seq=4 ttl=255 time=1.653 ms
84 bytes from 192.168.20.254 icmp_seq=5 ttl=255 time=1.367 ms

PC1> ping 192.168.30.254
84 bytes from 192.168.30.254 icmp_seq=1 ttl=255 time=2.274 ms
84 bytes from 192.168.30.254 icmp_seq=2 ttl=255 time=2.828 ms
84 bytes from 192.168.30.254 icmp_seq=3 ttl=255 time=1.447 ms
84 bytes from 192.168.30.254 icmp_seq=4 ttl=255 time=1.782 ms
84 bytes from 192.168.30.254 icmp_seq=5 ttl=255 time=1.217 ms
```

Figure 4. 28 : Connectivite réussie entre les VLAN de réseau LAN.

❖ **Test DMZ** :

Ping à partir d'un hôte du VLAN community

```
SER1> ip 172.16.0.2/24 172.16.0.1
Checking for duplicate address...
SER1 : 172.16.0.2 255.255.255.0 gateway 172.16.0.1

SER1> ping 172.16.0.3

84 bytes from 172.16.0.3 icmp_seq=1 ttl=64 time=0.337 ms
84 bytes from 172.16.0.3 icmp_seq=2 ttl=64 time=0.776 ms
84 bytes from 172.16.0.3 icmp_seq=3 ttl=64 time=0.731 ms
84 bytes from 172.16.0.3 icmp_seq=4 ttl=64 time=0.736 ms
84 bytes from 172.16.0.3 icmp_seq=5 ttl=64 time=0.713 ms

SER1> ping 172.16.0.4

host (172.16.0.4) not reachable
```

```
SER2> ip 172.16.0.3/24 172.16.0.1
Checking for duplicate address...
SER2 : 172.16.0.3 255.255.255.0 gateway 172.16.0.1

SER2> ping 172.16.0.2

84 bytes from 172.16.0.2 icmp_seq=1 ttl=64 time=0.337 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=64 time=0.689 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=64 time=0.716 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=64 time=0.670 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=64 time=0.638 ms

SER2> ping 172.16.0.4

host (172.16.0.4) not reachable
```

Figure 4. 29 : Test DMZ (Ping à partir d'un hôte du VLAN community).

❖ **Ping à partir d'un hôte du VLAN isolated**

```
SER3> ip 172.16.0.4/24 172.16.0.1
Checking for duplicate address...
SER3 : 172.16.0.4 255.255.255.0 gateway 172.16.0.1

SER3> ping 172.16.0.2

host (172.16.0.2) not reachable

SER3> ping 172.16.0.3

host (172.16.0.3) not reachable
```

Figure 4. 30 : Test DMZ (Ping à partir d'un hôte du VLAN isolated)

4.6.3. 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 pares-feux.

```
FG-ZEP # execute ping-option source 172.16.7.15

FG-ZEP # execute ping 172.16.7.20
PING 172.16.7.20 (172.16.7.20): 56 data bytes
64 bytes from 172.16.7.20: icmp_seq=0 ttl=255 time=3.2 ms
64 bytes from 172.16.7.20: icmp_seq=1 ttl=255 time=2.1 ms
64 bytes from 172.16.7.20: icmp_seq=2 ttl=255 time=1.6 ms
64 bytes from 172.16.7.20: icmp_seq=3 ttl=255 time=1.1 ms
64 bytes from 172.16.7.20: icmp_seq=4 ttl=255 time=1.5 ms

--- 172.16.7.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.9/3.2 ms
```

Figure 4. 31 : Ping réussi entre les interfaces des pare-feu FG-ZEP vers FG-BMT.

4.6.4. Test de NAT

Nous allons envoyer un Ping à partir de serveur de la DMZ d'adresse 172.16.0.1/24 vers le routeur ISP qui se trouve sur internet.

```
SER1> ip 172.16.0.2/24 172.16.0.1
Checking for duplicate address...
SER1 : 172.16.0.2 255.255.255.0 gateway 172.16.0.1

SER1> ping 172.16.0.1

84 bytes from 172.16.0.1 icmp_seq=1 ttl=255 time=3.176 ms
84 bytes from 172.16.0.1 icmp_seq=2 ttl=255 time=62.328 ms
84 bytes from 172.16.0.1 icmp_seq=3 ttl=255 time=5.270 ms
84 bytes from 172.16.0.1 icmp_seq=4 ttl=255 time=2.154 ms
84 bytes from 172.16.0.1 icmp_seq=5 ttl=255 time=2.585 ms
```

Figure 4. 32 : 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.

4.6.5. Test de la haute disponibilité

❖ **Vérification de la configuration :**

Comme nous voyons après la configuration de HA, les interfaces de FG-BMT vont être configurer automatiquement sur FG-DMZ.

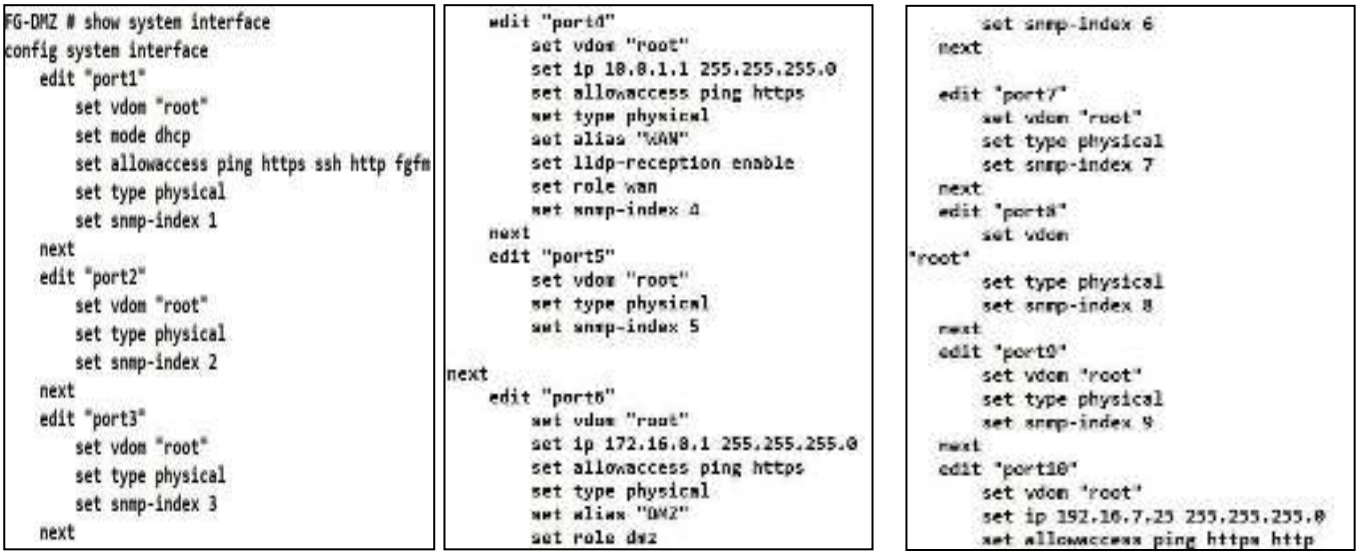


Figure 4. 33 : Interface de pare-feu FG-DMZ.

❖ **Test d'établissement des données au niveau de tunnel VPN**

Figure 4. 34 : Tunnel VPN établi au niveau de FG-BMT.

Figure 4. 35 : Tunnel VPN établi au niveau de FG-ZEP.

Conclusion

Dans le but de renforcer la sécurité des connexions entre les différents réseaux de l'entreprise BMT, des améliorations ont été mises en place conformément à un ensemble de politiques de sécurité définies antérieurement. Ces améliorations, rigoureusement testées pour en garantir le bon fonctionnement, ont permis d'établir une connexion sécurisée entre les réseaux, répondant ainsi aux exigences de sécurité établies.

Conclusion générale

L'objectifs principale de notre projet de fin d'études était de proposer et de mettre en œuvre une nouvelle infrastructure réseau sécurisée pour l'entreprise BMT, en utilisant diverses technologies telles que les VLAN et la segmentation du réseau pour contrer les potentilles attaques interne. Nous avons configuré le pare-feu Fortigate en établissant une liste de contrôle d'accès pour autoriser ou bloquer les communications entre ses différentes interfaces, protégeant ainsi le réseau contre les attaques externes. Parallèlement, nous avons mis en place un VPN IPSec reliant les sites de BMT et ZEP, assurant un accès distant sécurisé aux ressources de l'entreprise.

Pour renforcer la sécurité des réseaux locaux, nous avons créé une DMZ afin de séparer ces réseaux des éléments accessibles depuis internet.de plus, pour garantir la disponibilité et la continuité des services, nous avons configuré divers éléments supplémentaires tels que des routeurs et les protocoles HSRP pour une tolérance aux pannes.

Les simulations effectuées sur GNS3 ont confirmé le bon fonctionnement des technologies configurées, améliorant ainsi la disponibilité et la sécurité des données échangées au sein de l'entreprise.

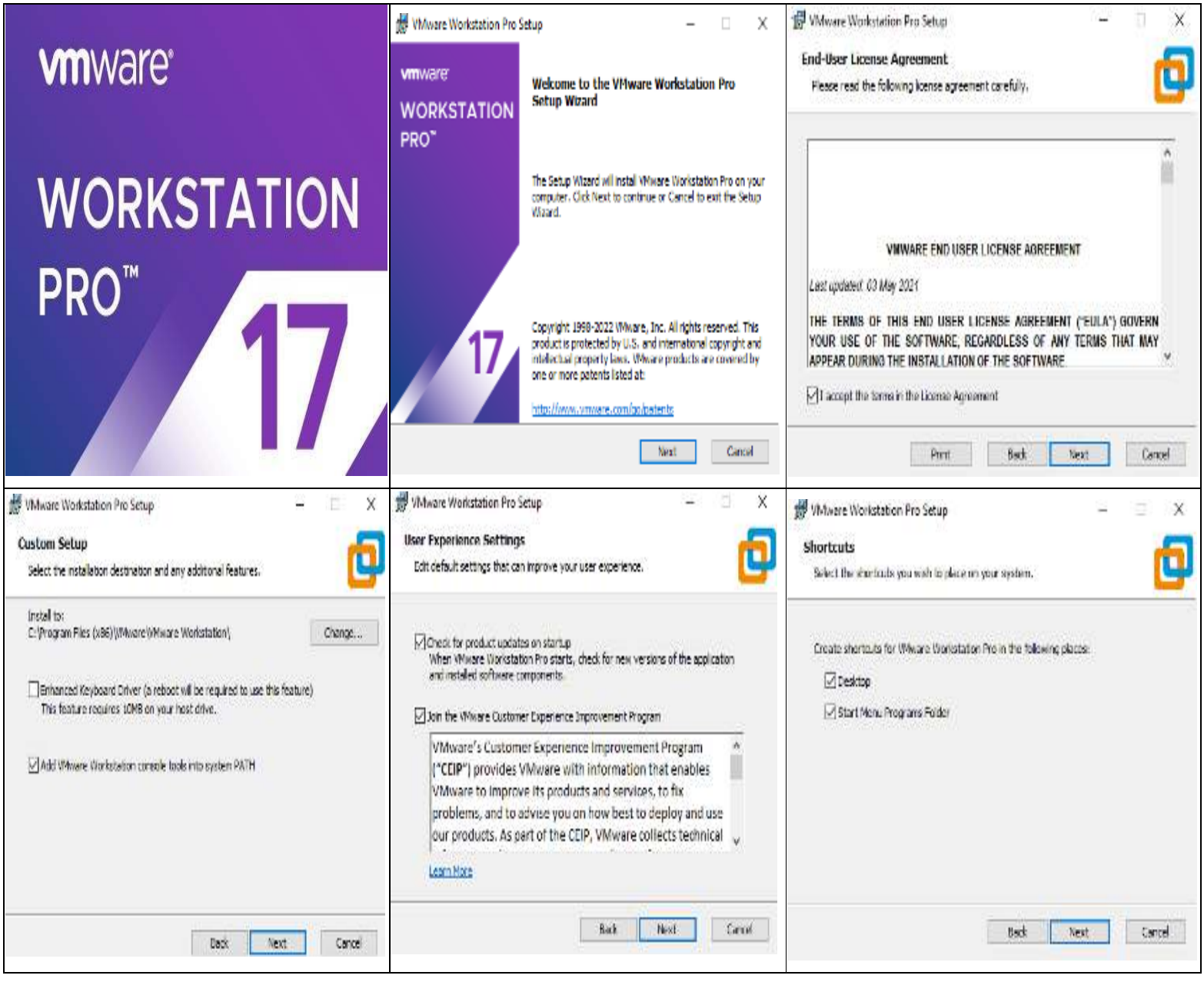
Ce projet nous a permis d'enrichir nos compétences en administration et en sécurité des réseaux de communication. Il nous a également donne l'opportunité de découvrir et de maitriser des logiciels de simulation avances tels que VMware Workstation 17 pro et Windows Server 2022. Ce travail constitue une base solide pour de futures innovations et améliorations dans le domaine de la sécurité des réseaux.

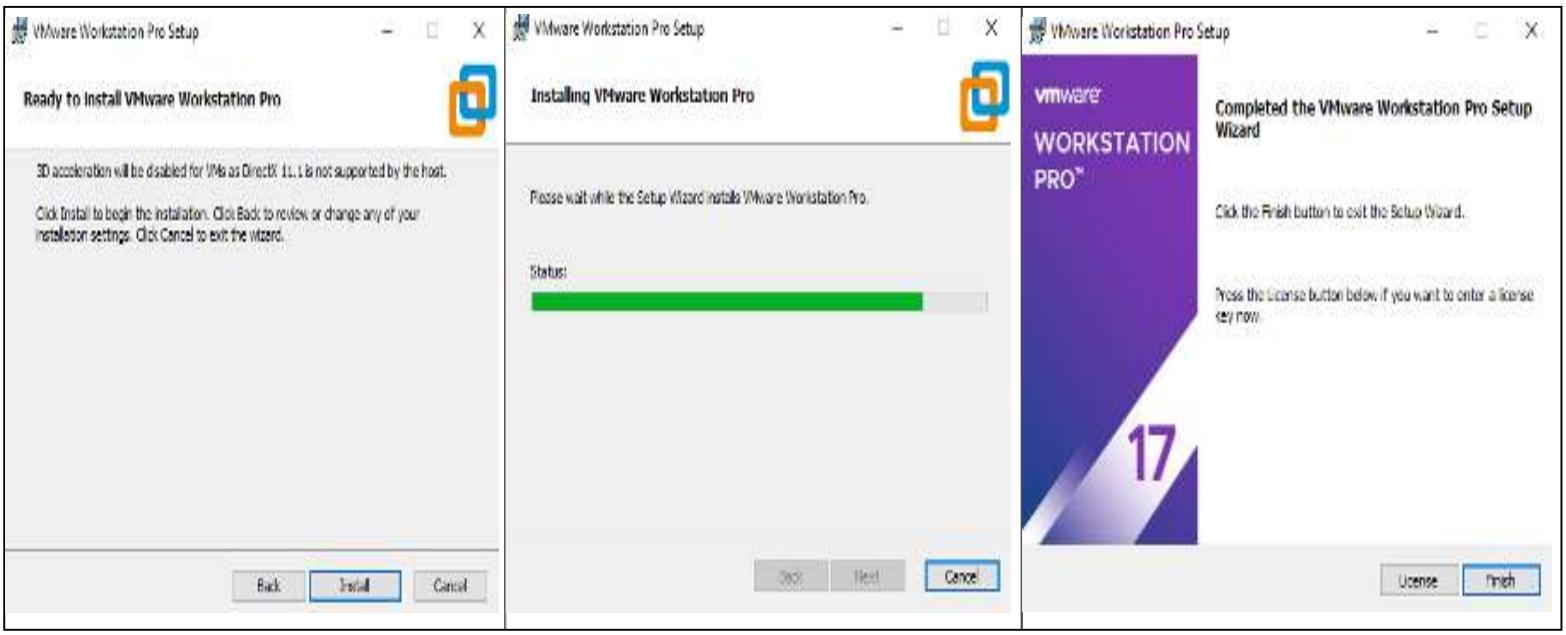
Annexes

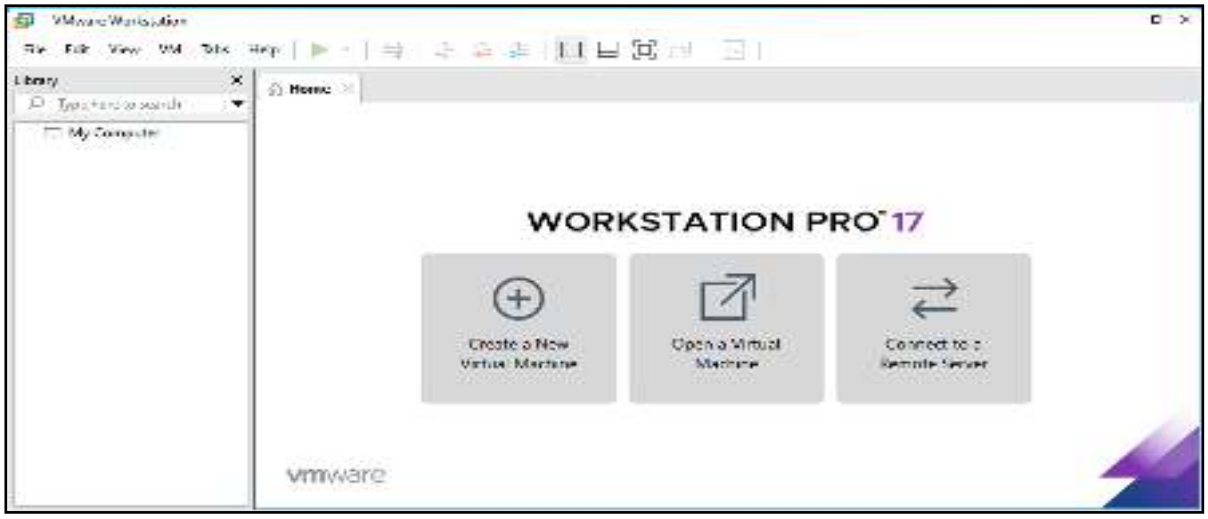
Annexe 1 : Installation de VMware Workstation version 17.0.0

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 :





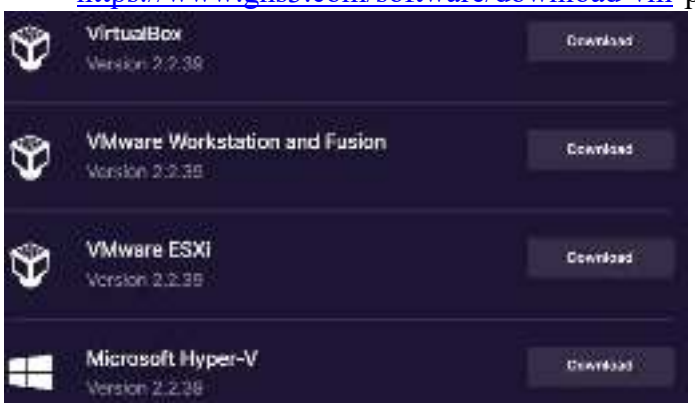


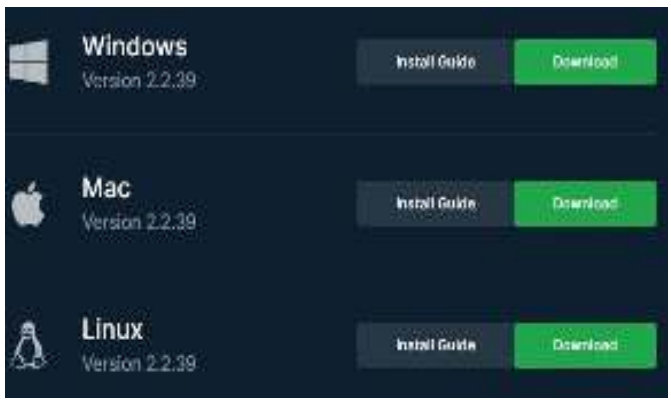
Annexe 2 : Installation de GNS3

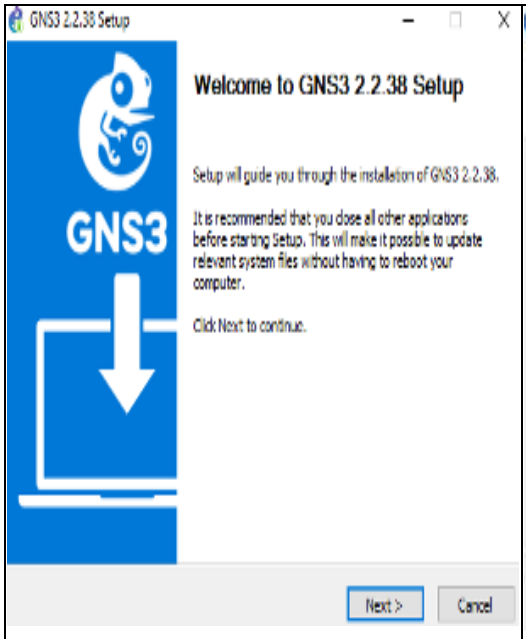
La version de GNS3 utilisé est 2.2.38 qui est disponible sur le lien

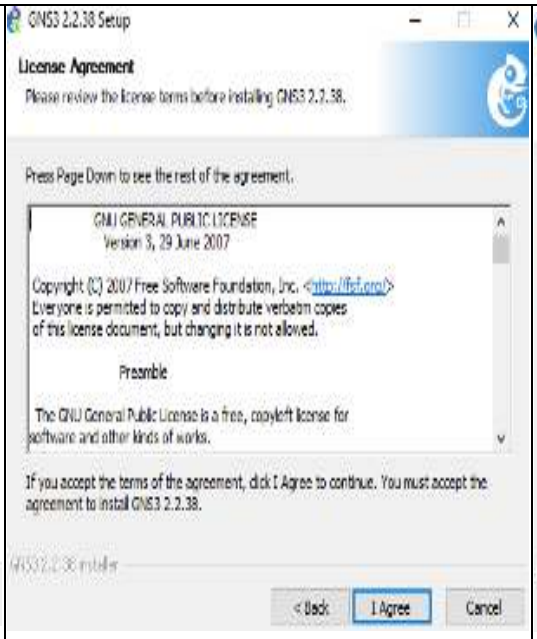
https://www.gns3.com/software/download pour GNS3 et

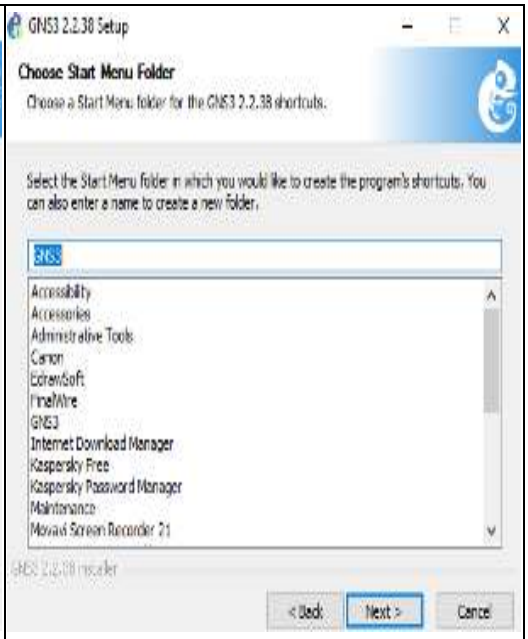
https://www.gns3.com/software/download-vm pour GNS3 VM

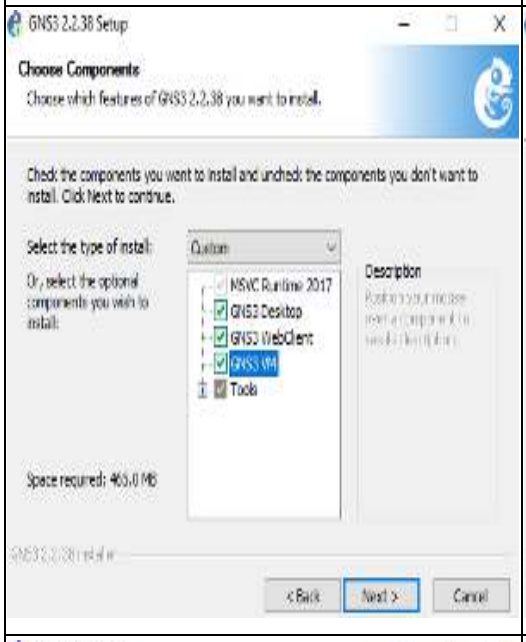


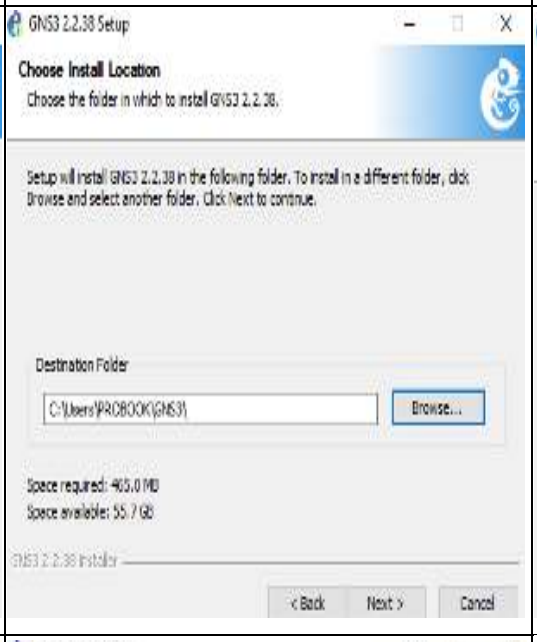


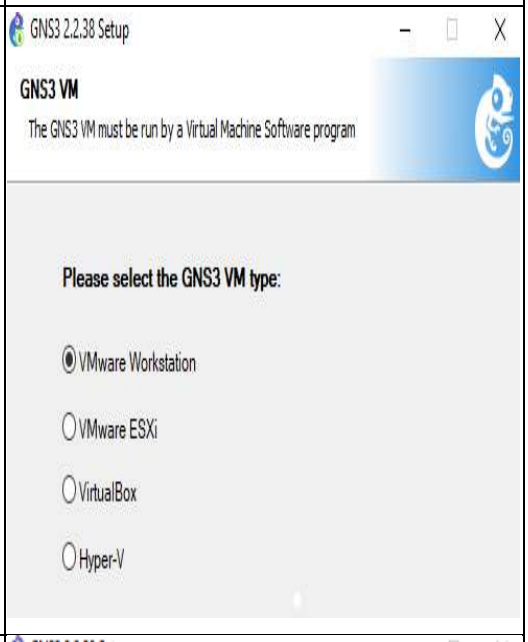

GNS3 2.2.38 Setup
Welcome to GNS3 2.2.38 Setup
Setup will guide you through the installation of GNS3 2.2.38.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to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

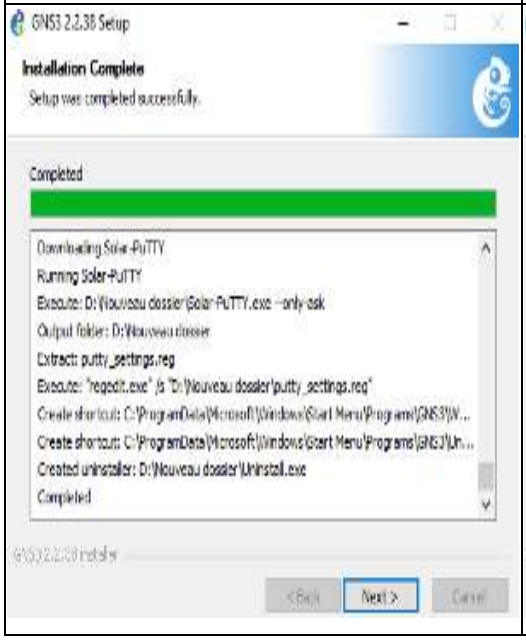

GNS3 2.2.38 Setup
License Agreement
Please review the license terms before installing GNS3 2.2.38.
Press Page Down to see the rest of the agreement.
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007
Copyright (C) 2007 Free Software Foundation, Inc.
Everyone is permitted to copy and distribute verbatim 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.
< 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
EaseUsSoft
FinalWire
GNS3
Internet Download Manager
Kaspersky Free
Kaspersky Password Manager
Maintenance
Movavi Screen Recorder 21
< Back
Next >
Cancel

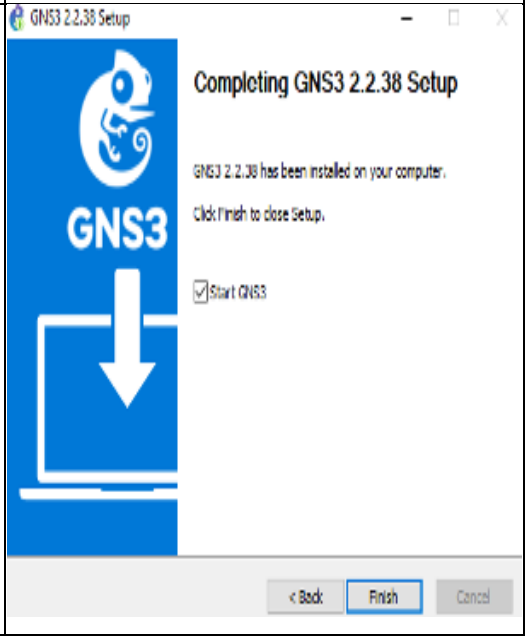

GNS3 2.2.38 Setup
Choose Components
Choose which features of GNS3 2.2.38 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Custom
Or, select the optional components you wish to install: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

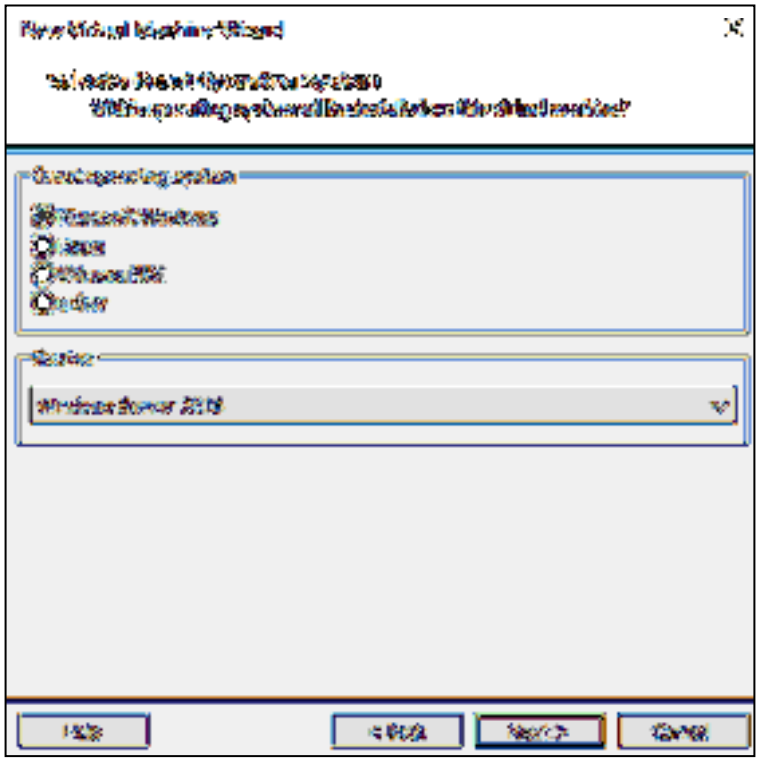

GNS3 2.2.38 Setup
GNS3 VM
The GNS3 VM must be run by a Virtual Machine Software program
Please select the GNS3 VM type:
VMware Workstation
VMware ESXi
VirtualBox
Hyper-V

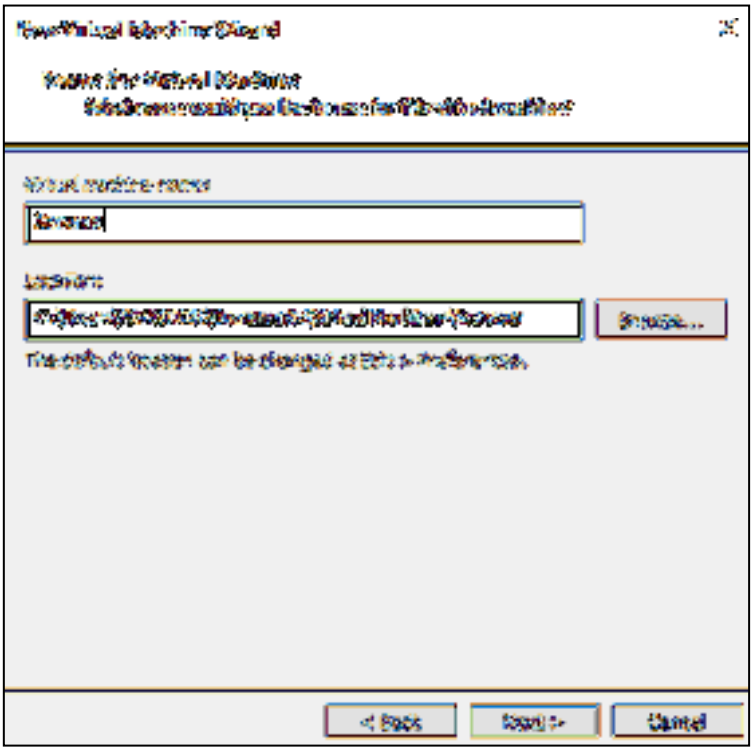

GNS3 2.2.38 Setup
Installation Complete
Setup was completed successfully.
Completed
Downloading Solar-PuTTY
Running Solar-PuTTY
Execute: D:\Nouveau dossier\Solar-PuTTY.exe --only-ask
Output folder: D:\Nouveau dossier
Extract: putty_settings.reg
Execute: "regedit.exe" /s "D:\Nouveau dossier\putty_settings.reg"
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
Next >
Cancel

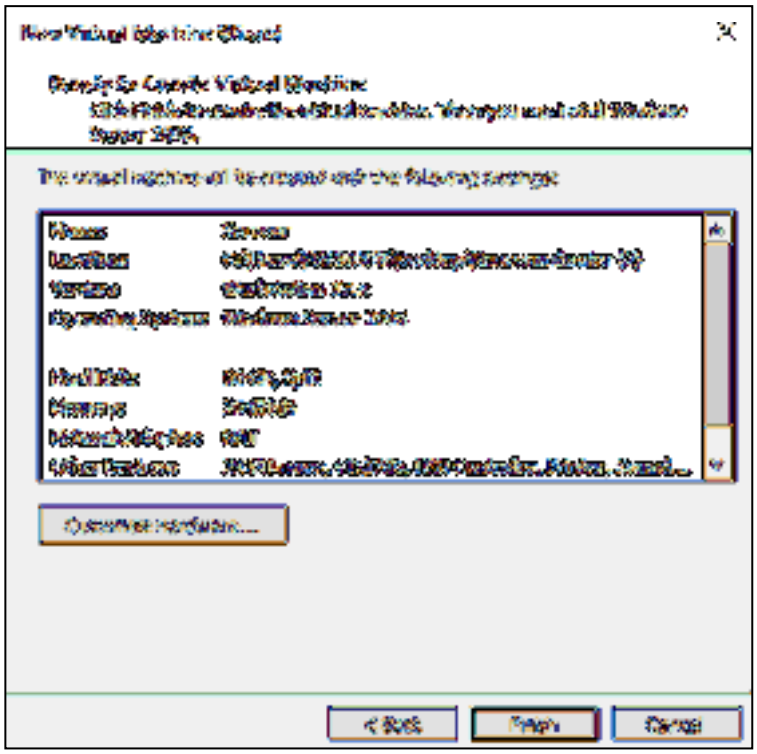

GNS3 2.2.38 Setup
Solarwinds Standard Toolset
Exclusive for GNS3 users
Would you like to get your free license of Solarwinds Standard Toolset? ($200 value)
Yes
No
Toolset F.A.Q
Next >
Cancel

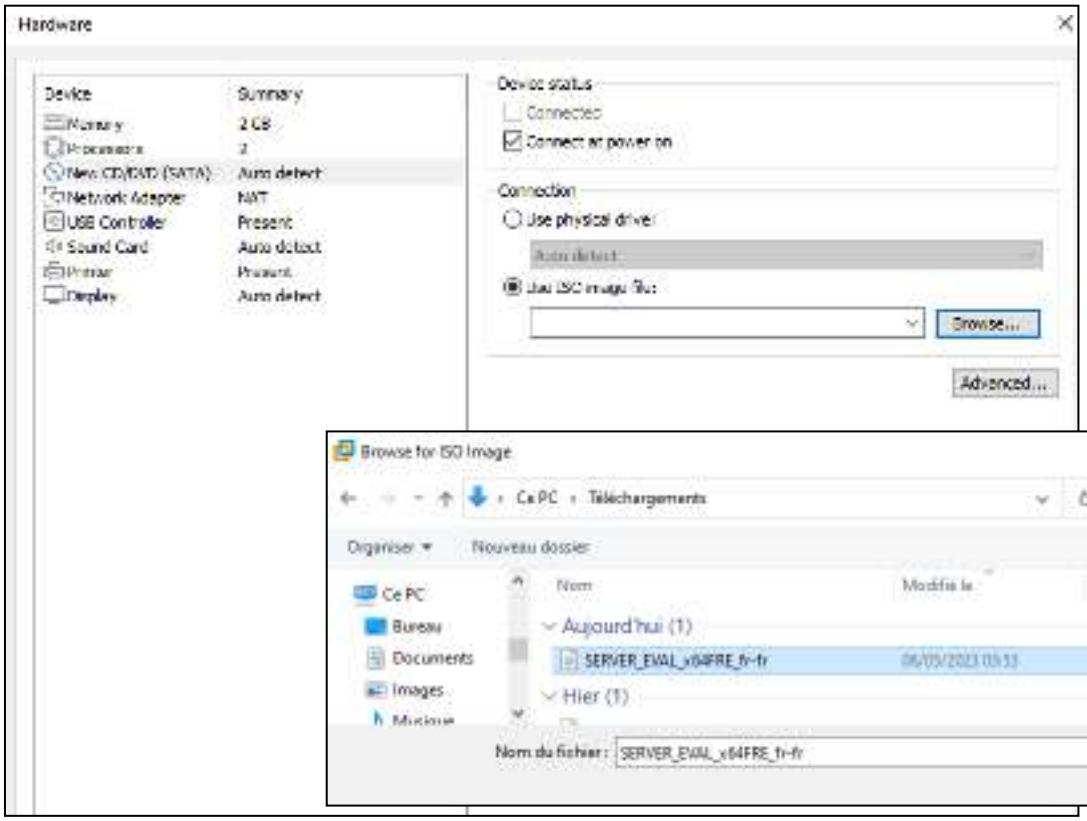

GNS3 2.2.38 Setup
Completing GNS3 2.2.38 Setup
GNS3 2.2.38 has been installed on your computer.
Click Finish to close Setup.
Start GNS3
GNS3
< Back
Finish
Cancel

Annexe 3 : installation de Windows serveur 2022

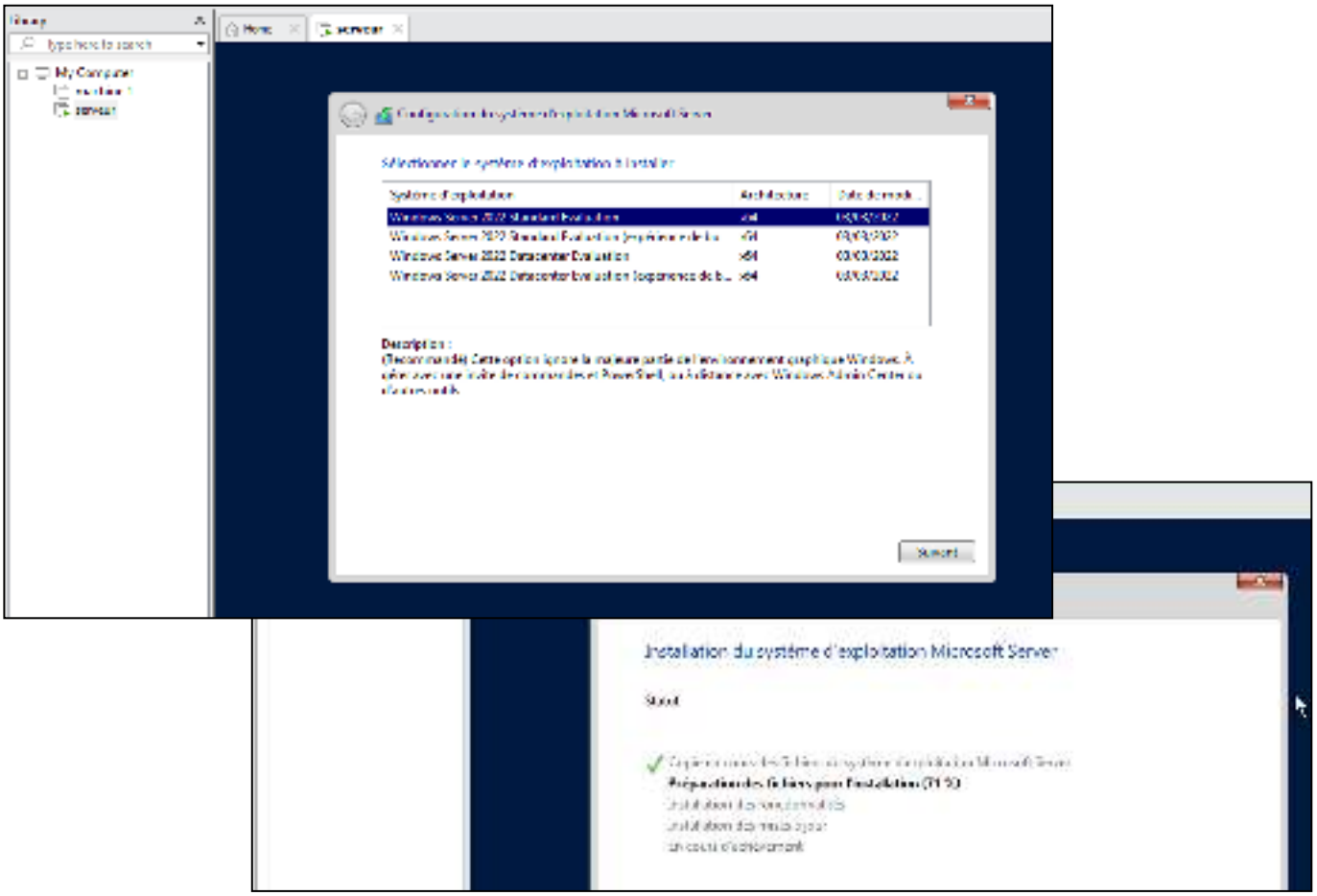


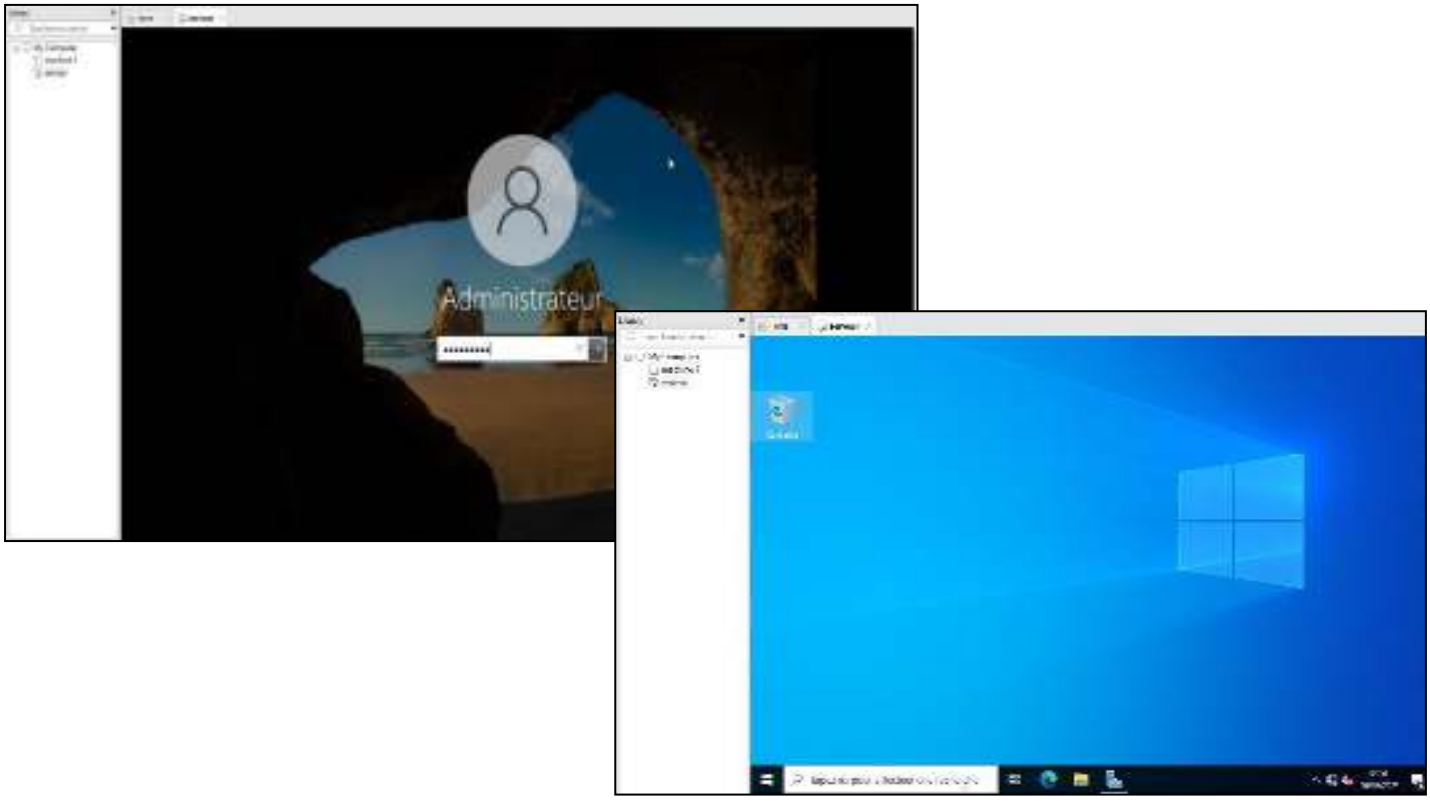




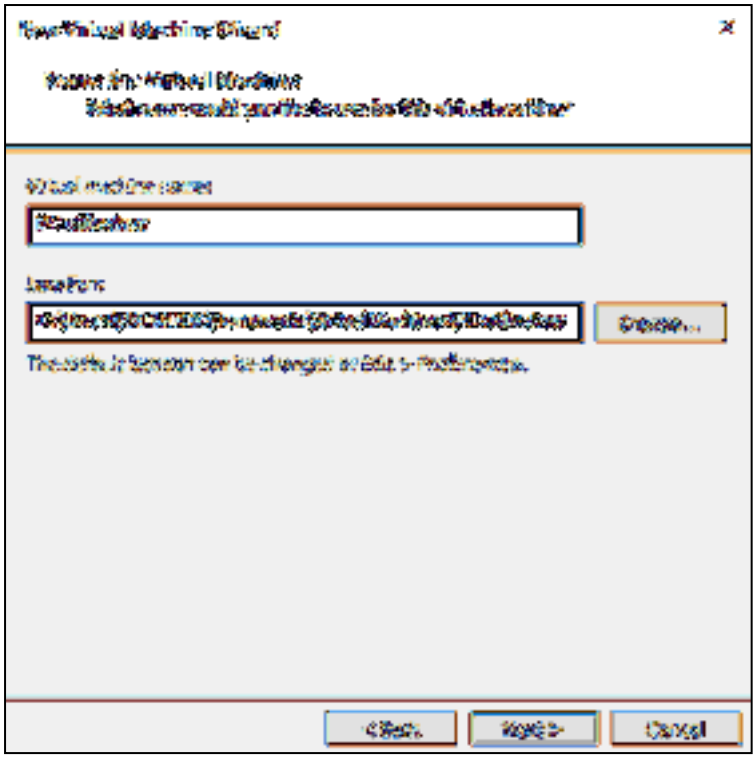

Hardware
Device
Summary
Memory
2 GB
Processors
2
New CD/DVD (SATA)
Auto detect
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Printer
Present
Display
Auto detect
Device status
Connected
Connect at power on
Connection
Use physical drive:
Auto detect
Use ISO image file:
Browse...
Advanced...

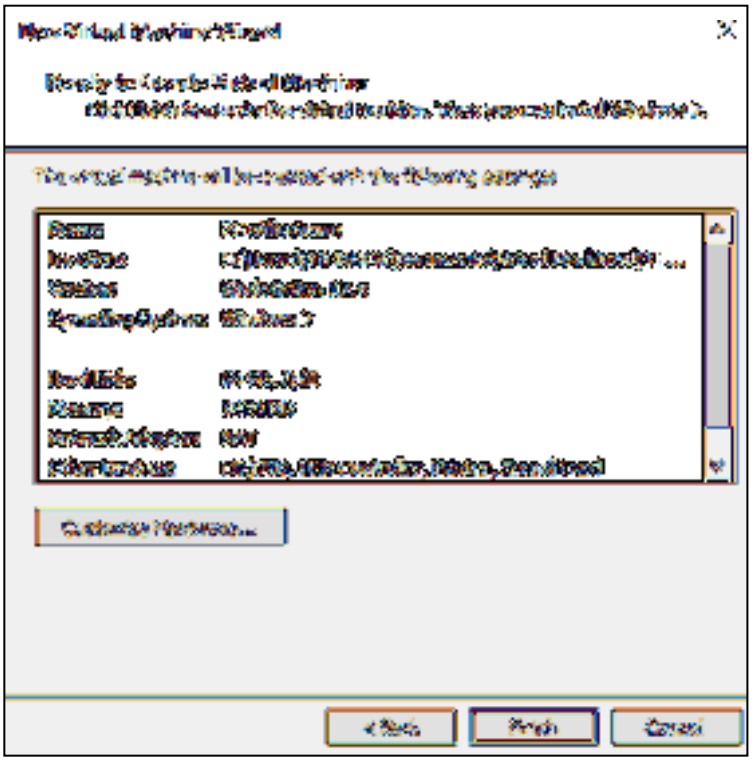
Browse for ISO Image
Ce PC
Téléchargements
Rechercher dans : Téléchar...
Organiser
Nouveau dossier
Ce PC
Bureau
Documents
Images
Nom
Modifié le
Type
Taille
Aujourd'hui (1)
SERVER_EVAL_x64FRE_fr-fr
Fichier d'image di...
Hier (1)
Nom du fichier :
SERVER_EVAL_x64FRE_fr-fr
CD-ROM images (*.iso)
Ouvrir
Annuler

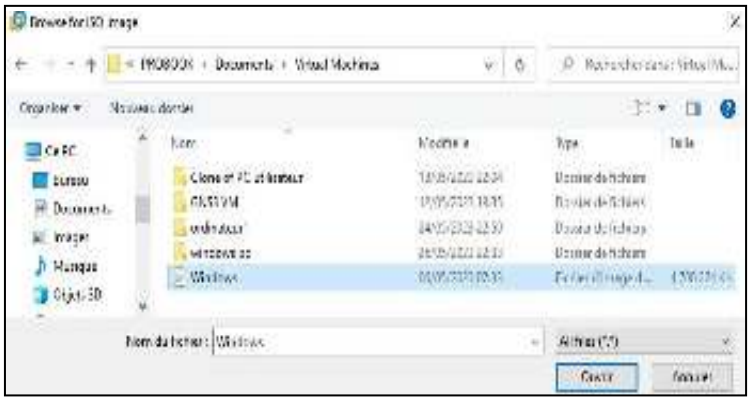

Installation du système d'exploitation Microsoft Server

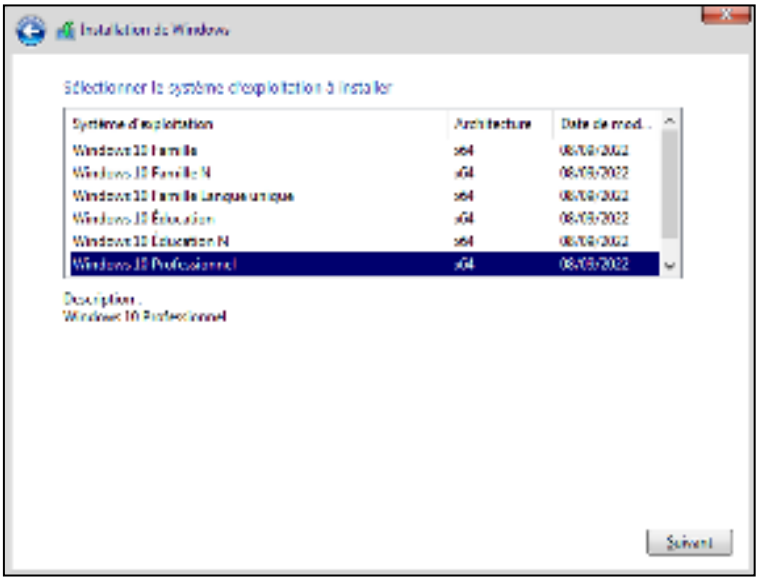

Administrateur

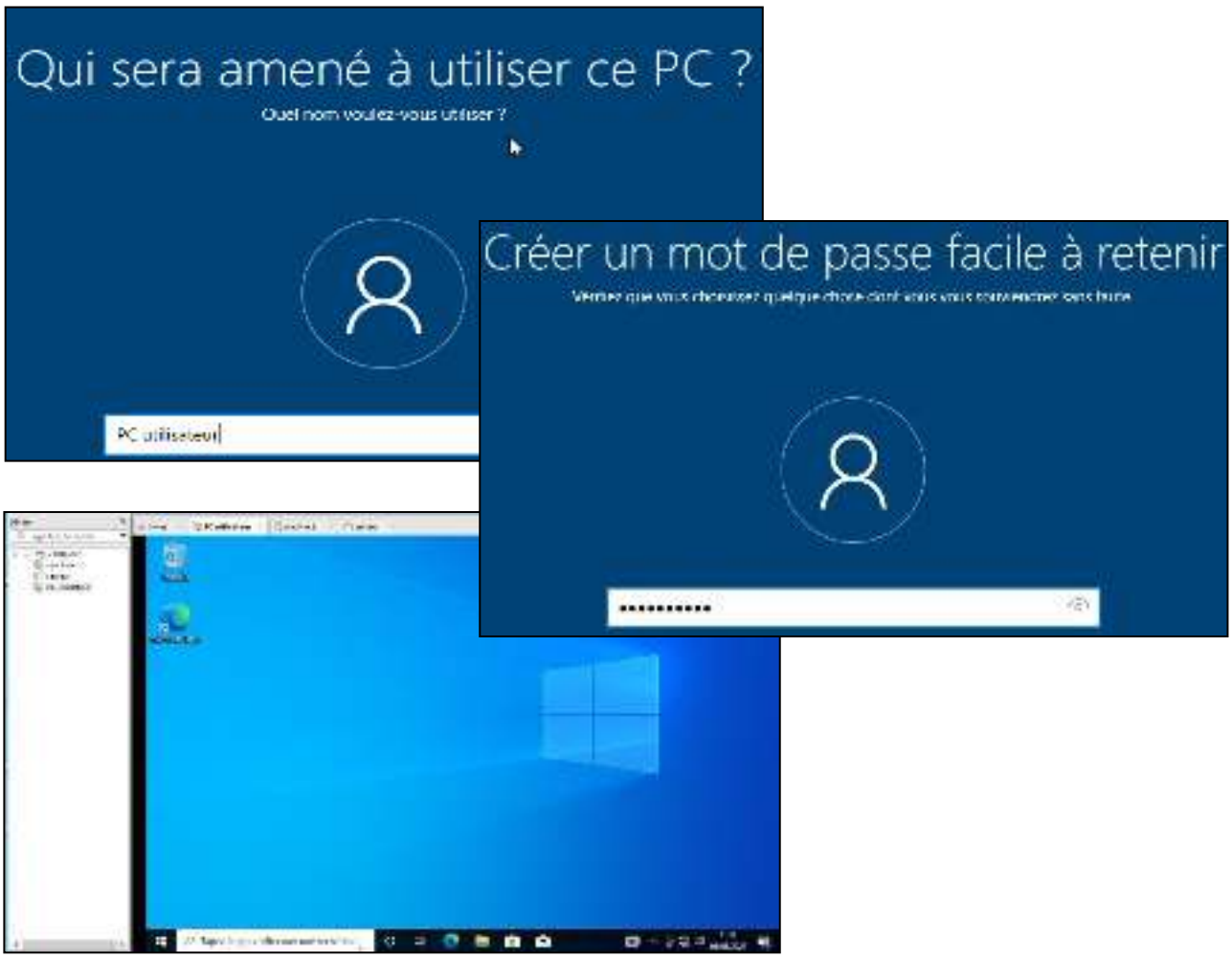
Annexe 4 : installation de Windows 2010





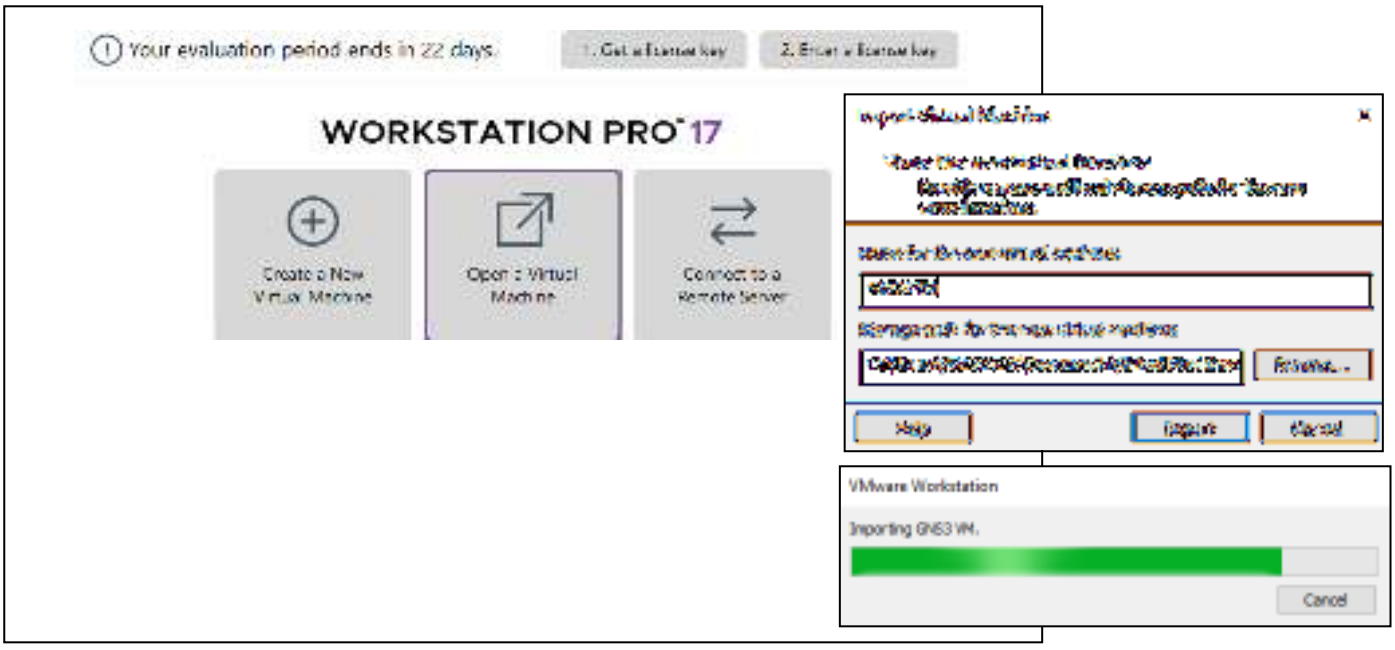




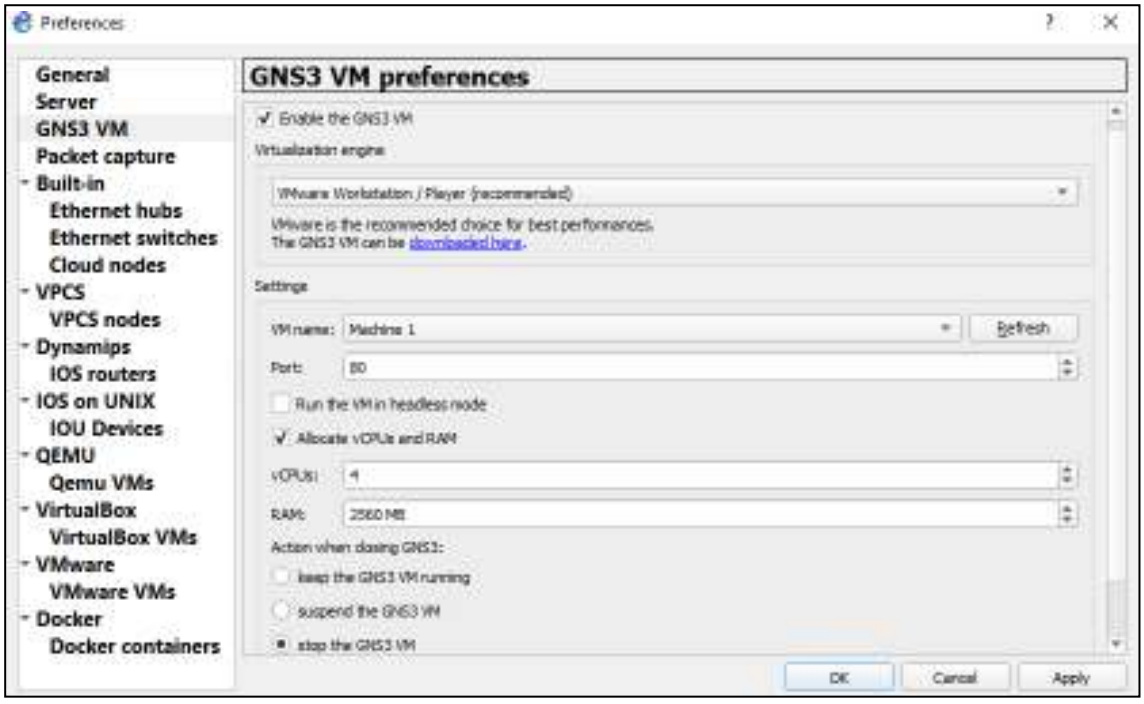


Annexe 5 : Importation de GNS3 VM sur VMware Workstation

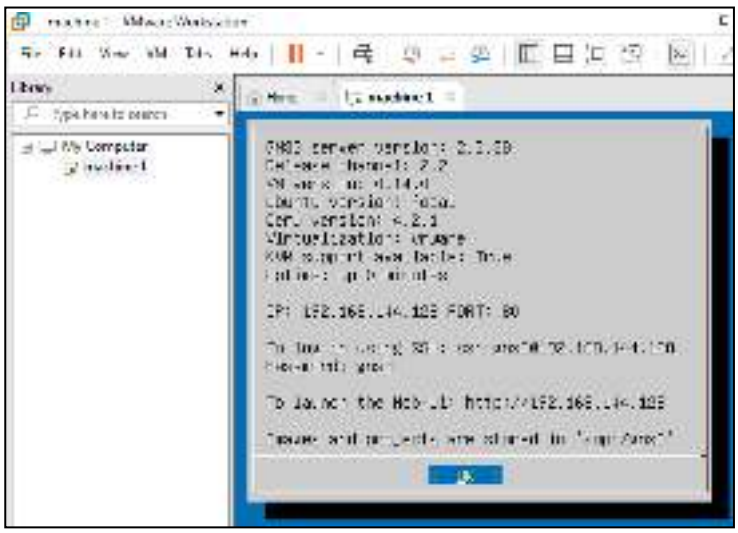
Sur la page d'accueil de VMware « home » on clique sur « open a virtual machine » pour ouvrir leGNS3 VM afin de créer une nouvelle machine virtuelle.

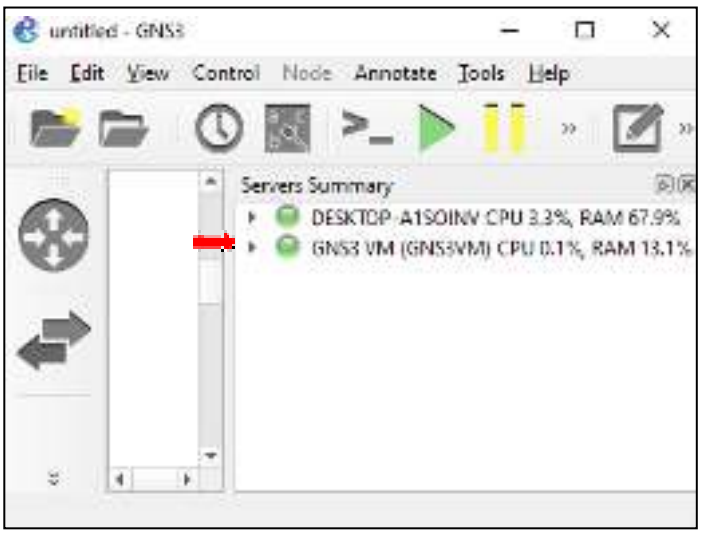


Annexe 6 : Relier GNS3 au GNS3 VM importé sur VMware workstation sur GNS3 on clique sur « Edit » ensuite sur « Preferences » pour choisir GNS3 VM.



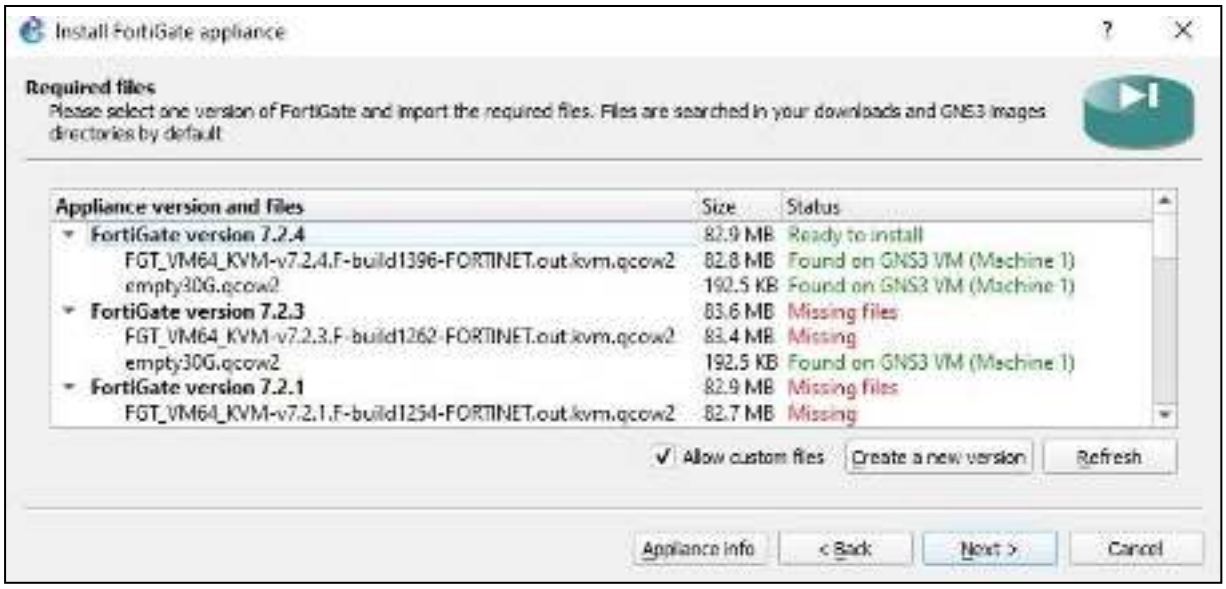
Lorsque on clique sur « applay » le programme GNS3 VM commence à fonctionner avec le GNS3.

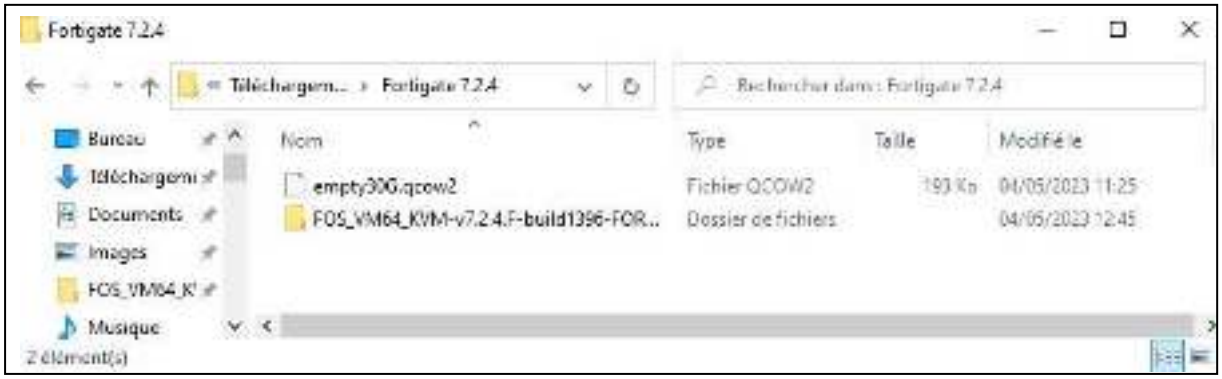




Annexe 7 : Importation de pare-feu Fortigate 7.2.4 sur GNS3 L'image ISO de Fortigate est disponible sur les liens ci-dessous : https://www.fortinet.com

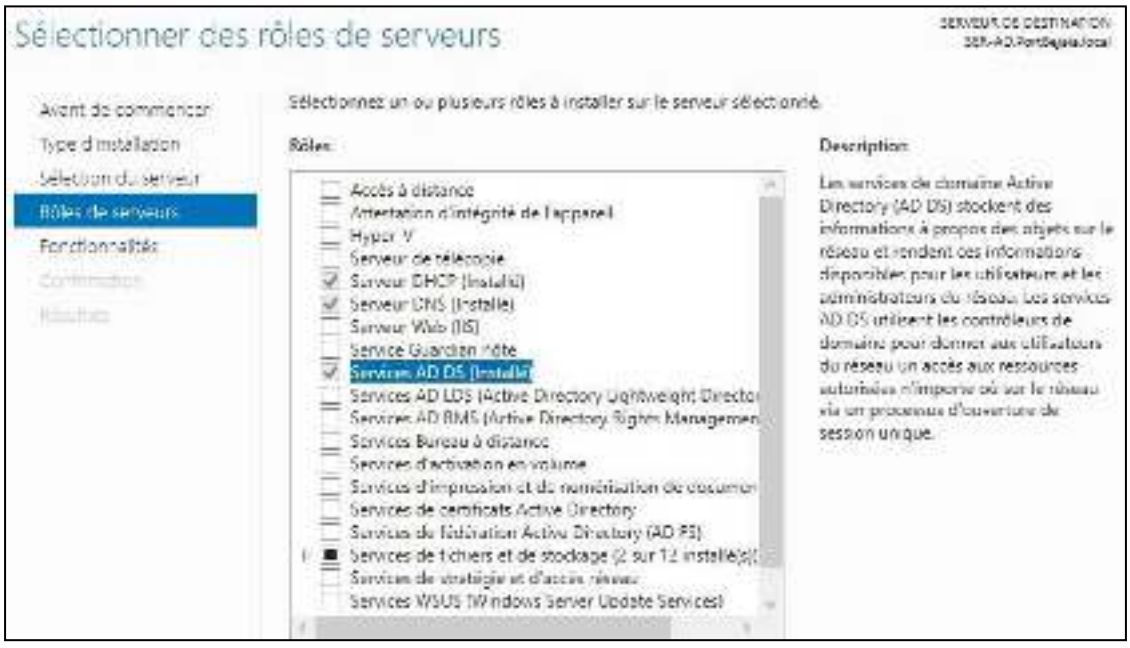
https://gns3.com/marketplace/appliances/fortigate

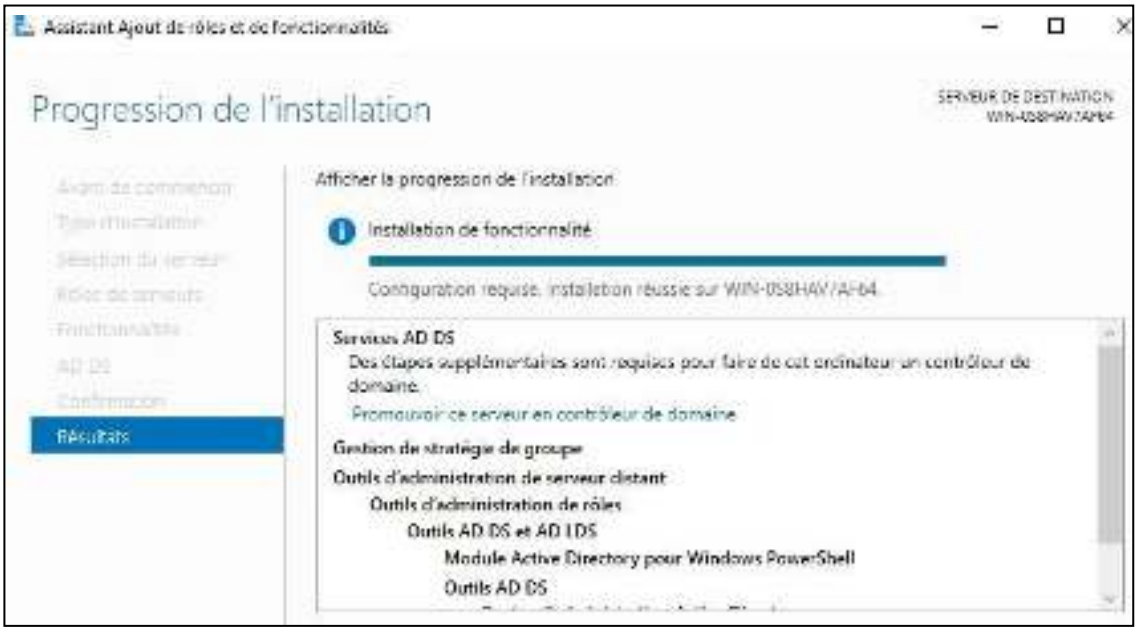




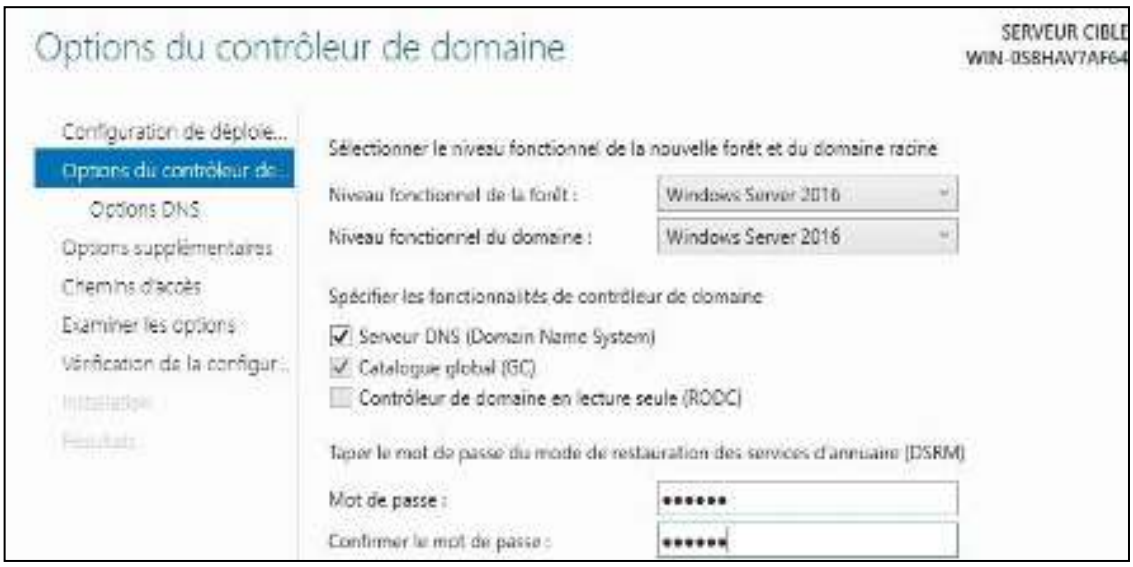
Annexe 8 : Installation de l'active directory

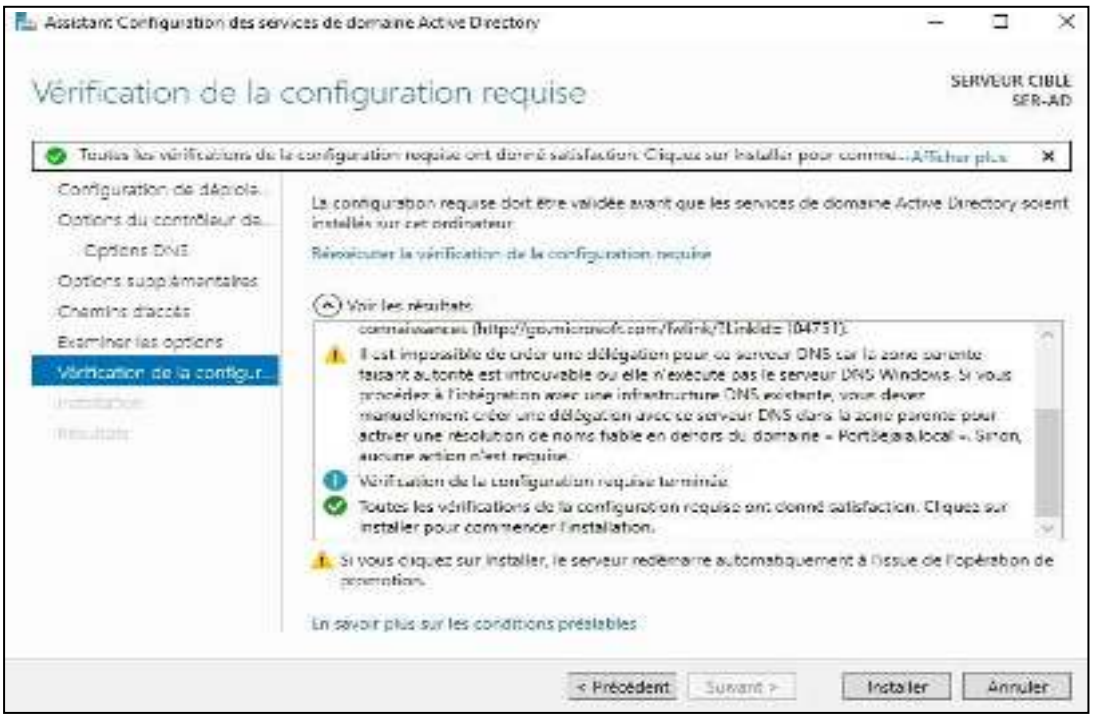
Nous allons suivre les étapes suivantes pour installer le service de domaine Active Directory sur Windows server 2022.

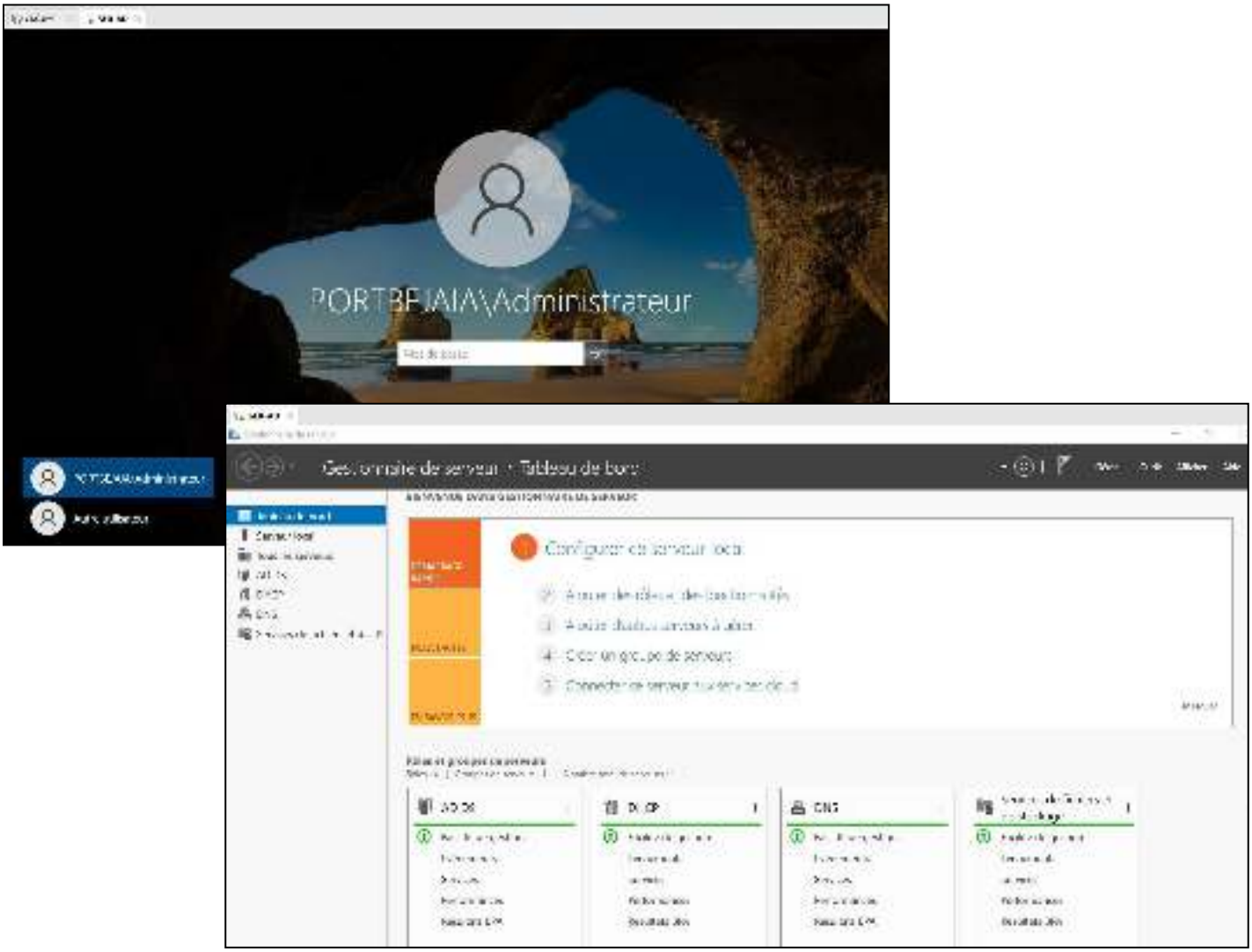



Assistant Ajout de rôles et de fonctionnalités
Progression de l'installation
SERVEUR DE DEST NATION
Afficher la progression de l'installation
Installation de fonctionnalité
Configuration requise. Installation réussie sur WIN-0S8HAV7AF64.
Résultats
Services AD DS
Des étapes supplémentaires sont requises 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 commen... Afficher plus
Configuration de déploie...
Options du contrôleur de...
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configur...
La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Relancer la vérification de la configuration requise
Voir les résultats
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 « Portbeja.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


PORTBEJAIA\Administrateur
Gestionnaire de serveur • Tableau de bord
Configurer ce serveur local
AD DS
DHCP
DNS

Bibliographie

[1] https://btssri13.wordpress.com/wp-content/uploads/2013/04/terminologie-des-rc3a9seaux.pdf

[2] José DORDOIGNE, Editions ENI ; 6eme Edition (11mars 2015), réseaux informatiques, page 37

[3] https://www.ionos.fr/digitalguide/serveur/know-how/ethernet.com

[4] https://fr.wikipedia.org/wiki/token_ring.com

[5] https://fr.m.wikipedia.org

[6] PUJOLLE.G, « les réseaux »,France, Édition 2014.

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

[8] V.REMAZEILLES , « la sécurité des réseaux avec CISCO », Edition ENI,2009.

[9] https://fr.theastrologypage.com

[10] M.Ali Sadiqui , sécurité des réseaux informatique, collection informatique , Ttd 2019,265pages.

[11] C.Liorens et L.Levier, « Tableau de bord de la sécurité réseau »,Eyrolles,Paris-France,2003.

[12] https ://securityboulevard.com/2019/03/quelle-est-la-fiffernce-entre-une-attaque-active-et-une-attaque-passive

[13] Jean-Francois Pillou et Jean-Phillipe Bay. « Tous sur la sécurité informatique ».4eme édition, Dunod, Paris 2016.

[14] Clarke-Salt, J. (2009). SQL injection attacks and defense. Elsevier.

[15] Roulot,' le piratage de A à Z ', Edition Edigo,2010.

[16] www.ipe.fr a été indexe par google il y a plus de 10ans

[17] https://fr.wikipedia.org/wiki/Logiciel_espion

[18] Mickel Choisnard, Réseaux et Sécurité informatique, Université De Bourgogne, Cours MIGS, novembre 2015,In :https://blog.u-bourgogne.fr/migs/wp content/uploads/sites/7/2016/01/ Réseaux-et-Sécurité.pdf.

[19] http : //www.tele.ucl.ac.be/EDU/ELEC/1997/firewall/Firewalls.html

[20] Postair, J-C et Aubel, A. Présentation de différents types d'architectures de Firewall.

[21] Davis chapman , « firewalls-la securité sur internet », edition O'Reilly , 1997.

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

[23] https://memoire.univ-batna2.dz

[24] http://www.linux-france.org ACL Dernier accès Juillet 2018

[25] http://www.ninjaone.com

[26] JF.pillou,JPH.Bay.tout sur la sécurité informatique .4éme édition Dunod ,2005.2009.2013.2016.

[27] https://forum.huawei.com/entreprise/fr/principes-de-base-du-pare-feu-politique- de-securite.

[28] : Franck Huet-Christian Verhille, GNU/Linux Fedora : Sécurité du système, sécurité des données, pare-feu, chiffrement, authentification, ENI, France, juin 2007.

[29] https://fr.wikipedia.org/wiki/SSL_VPN

[30] https://www.fibre-pro.fr/von-ssl/

[31] https://www.tutos-informatique.com/tunnel-gre-explications/

[32] https://www.hsc.fr/ressources/articles/ipsec-intro/ipsec-intro.pdf

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

[34] https://airmob.net/protocole-l2tp-fonctionnement/

[35] https://aws.amazon.com/fr/what-is/ipsec/

[36] http://www-img.univ-mlv.fr type de vlan dernier accès septembre 2018.

[37] https://datacampus.fr

[38] https://fr.wikipedia.org

[39] https://tinycrypt.wordpress.com

[40] https://www.cisco.com.security-vpn

[41] https://medium.com/@antoine.ansel/l-algorithme-d-echange-de-clés-diffie-hellman

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

Résumé

A l'heure où les technologies internet stimulent la croissance des entreprises, la sécurité des réseaux devient un enjeu crucial. Pour BMT, la protection des données stratégiques et la fluidité des échanges passent par une architecture réseau sécurisée, conçue et optimisée sous GNS-3.

Notre travail consiste à la mise en place d'une architecture réseau sécurisé simulée sous GNS-3 pour l'entreprise (BMT), cet outil permet de tester et d'optimiser cette architecture, assurant à Bejaia Mediterranean Terminal (BMT) une sécurité réseau robuste.

Afin de garantir un partage des données sécurisé et performant, nous avons segmenté le réseau en VLAN et configuré le pare-feu Fortigate. Cela s'est traduit par la mise en place de deux tunnels VPN IPSec, d'une infrastructure haute disponibilité, d'une liste de contrôle d'accès, d'une zone démilitarisée et l'intégration de divers protocoles (HSRP, LACP, DHCP, VTP). Ces actions ont permis de créer un réseau robuste et flexible qui répond aux besoins exigeants de l'entreprise en matière sécurité et de partage d'information.

Mots clés : sécurité réseau, BMT, LAN, pare-feu, VLAN, VPN, IPSec, fortigate, DMZ, HA, GNS3, VMware.

Abstract

In today's internet driven business landscape, network security has become a critical issue. For BMT, protecting strategic data and ensuring seamless communication requires a secure networl architecture, designed and optimized using GNS-3.

Our work involved implementing a simulated secure network architecture for BMT using GNS-3. this tool enables to us and optimize the architecture, providing Bejaia Mediterranean Terminal (BMT) with robust network security.

To ensure secure and efficient data sharing, we segmented the network into VLANs and configured the fortigate firewall. This involved setting up two IPSec vpn tunnel, a high-viability infrastructure, an access control list, a demilitarized zone (DMZ), and integrating various protocols (HSRP, LACP, DHCP, VTP). These actions resulted in a robust and flexible network that meets the company's demanding security and information sharing needs.

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