République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER PROFESSIONNEL

En

Informatique

Option

Administration et Sécurité des Réseaux

Thème

Étude et amélioration de l'architecture réseau et sécurité des services intranet et Internet.

Cas d'étude : entreprise BMT (Bejaia Méditerranéen Terminal)

Présenté par : M^lle^. **KHERFALLAH Sara**
M^lle^. **MERZOUG Amel**

Devant le jury composé de :

Président	**Dr. L. KHENOUS**	**Maître de Conf. B**	**U. A/Mira Béjaia.**
Examinatrice	**Dr. K. HOCINI**	**Maître Assist. B**	**U. A/Mira Béjaia.**
Rapporteur	**Dr. M. MOHAMMEDI**	**Maître de Conf. A**	**U. A/Mira Béjaia.**

Béjaia, Juin 2023.

⁂ *Remerciements* ⁂

Nos premiers remerciements vont à Dieu Tout-Puissant qui, par sa bonté et sa miséricorde, nous a permis d'avoir le courage, la foi et la volonté de mener à bien ce travail.

Nous voudrons exprimer nos profondes gratitudes a notre encadrant M. MOHAMMEDI Mohamed pour sa patience, sa disponibilité et surtout ses judicieux conseils tout au long de la période du projet qui nous ont permis de réaliser ce travail, aussi, pour ses critiques constructives, sans lesquelles ce travail n'aurait pu aboutir.

Nous désirons adresser nos vifs remerciements aux membres de jury d'avoir accepté de faire partie de cette évaluation et de l'enrichir par leurs propositions. Et ainsi pour l'intérêt qu'ils portent à notre travail .

Nous tenons a remercier notre maitre de stage M. ZAABAR Fayssal pour son sérieux et ses conseils, ainsi qu'à toute l'équipe du service Informatique de l'entreprise BMT.

Nos sincères remerciements pour nos parents pour leurs soutiens, leurs encouragements et leurs sacrifices.

Nous remercions également tout le corps professionnel du département d'Informatique de l'université Abderahmane MIRA de Bejaia.

Enfin, nous tenons a remercier tous ceux qui ont contribué de prés ou de loin pour l'élaboration de ce travail.

⁕ *Dédicaces* ⁕

À mon cher père

Tu as toujours été pour moi un exemple du père respectueux, honnête, de la personne méticuleuse, je tiens à honorer l'homme que tu es. Grâce à toi papa j'ai appris le sens du travail et de la responsabilité. Je voudrais te remercier pour ton amour, ta générosité, ta compréhension... Ton soutien fut une lumière dans tout mon parcours. Aucune dédicace ne saurait exprimer l'amour l'estime et le respect que j'ai toujours eu pour toi. Ce travail est le fruit de tous les sacrifices que tu as déployés pour mon éducation et ma formation. Je t'aime papa et j'implore le tout-puissant pour qu'il t'accorde une bonne santé et une vie longue et heureuse.

À ma chère mère

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

À mes chères sœurs et mon unique frère

Lyna, Aya et Amine auxquels je souhaite toute la réussite et le bonheur du monde.

À la mémoire de mon cher et unique oncle Abdallah.

Et a toute ma famille et mes proches.

À Amel, chére amie avant d'être binôme.

A mes chére copines Yasmine, Tiziri et Yousra.

Sara

⁕ *Dédicaces* ⁕

Je dédie ce travail accompagné d'un profond amour à mes parents, pour tous leurs sacrifices, leurs soutiens, leurs encouragements et leurs amours qui ont été la raison de ma réussite. Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices qu'ils ont consentis pour mon instruction et mon bien-être. Que dieu leur présente une bonne santé et une longue vie.

À la mémoire de ma sœur qui nous a quitté trop tôt et qui a toujours voulu voir ma réussite, que dieu l'accueille dans son vaste paradis.

À ma sœur Lina mon âme sœur et ma confidente.

À ma sœur Saoussen qui ma toujours soutenu, encouragé et qui a toujours cru en moi.

À mes deux frères adorés pour leur compréhension, leur grande tendresse et leur soutien moral.

À mes neveux et mes nièces que j'aime énormément Adem, Ilèss, Izem, Mohamed, Ritadj, Manel et en particulier a ma source de joie Yakoub.

À mes beaux frères et mes belles sœurs.

À ma chère binôme et amie Sara.

À tous ceux qui ont participé du pré ou du loin à la réalisation de ce travail.

Amel

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

LISTE DES ACRONYMES

A	ADSL	Asymmetric Digital Subscriber Line.
	AVP	Serveur d'Application.
	APP	Application.
B	BMT	Bejaia Méditerranéen Terminal.
	BNC	Bayonet Neill–Concelman.
	BDD	Base de Donnée.
C	CTMS	Container Terminal Management System.
	CCTV	Closed-Circuit Télévision.
	CRM	Customer Relationship Management.
D	DHCP	Dynamic Host Configuration Protocol.
	DNS	Domain Name System.
	DMZ	Zemilitarized Zone.
E	EPB	Entreprise Portuaire de Bejaia.
	ERP	Entreprise Resource Planning.
F	FTP	File Transfer Protocol.
	FDDI	Fiber Distributed Data Interface.
G	GMAO	Gestion de Maintenance Assistée par Ordinateur.
	GRPI	Gestionnaire Libre de Parc Informatique.
I	IPROS	Opérating Systèm Terminal.
	ISO	International Standard Interconnection.
	IBM	International Business Machines.
	IP	Internet Protocol.
L	LAN	Local Area Network.
M	MAN	Métropolitain Area Network.
	MAC	Media Access Control.
N	NAS	Network Access Server.
O	OSI	Open Systems Interconnection.
P	PSE	Portek Systems and Equipement.
	PAN	Personal Area Network.
	PC	Personal Computer.

R	RJ45	Registered Jack.
T	TCP/IP	Transmission Control Protocol/Internet Protocol.
	TOMCAT	Apache Tomcat.
U	UTM	Unified Threat Management.
V	VPN	Virtual Private Network.
	VLAN	Virtual Local Area Network.
	VTP	Virtual Trunking Protocol.
W	WEB	World Wide Web.
	WAN	Wide Area Network.
Z	ZEP	Zone Extra Portuaire.

INTRODUCTION GÉNÉRALE

Aujourd'hui, les réseaux informatiques sont devenue indispensable et ils constituent des outils essentiels au succès d'une entreprise [14]. Cette dernière utilise les réseaux informatiques pour effectuer en interne des tâches quotidiennes tels que le partage de données et l'accès aux ressources. Ce qui leur permet de faire gagner le temps et diminuer les erreurs. Mais, ils restent incomplet sans sécurité, chaque entreprise a besoin de sécurité pour protéger les confidentialités de données et garantir l'intégrité, la disponibilité, l'authentification et la non répudiation de ses systèmes. Car elles sont trop souvent exposé a des défaillances techniques, des intrusions de logiciels malveillants ou tout simplement des erreurs humaines de manipulation.

Face à l'évolution rapide des réseaux informatiques, les entreprises se trouvent confronter à un marché fortement concurrentiel qui évolue rapidement [14]. Et Vu l'importance des informations qui sont souvent véhiculées dans les réseaux. Ceux-ci requièrent les entreprises à améliorer leurs architecture du réseau et avoir un certain degré de sécurité pour assurer le bon fonctionnement des services intranet et Internet. Ces derniers sont devenus des éléments essentiels pour assurer la continuité des systèmes d'information des entreprises.

Dans le monde numérique d'aujourd'hui, où les entreprises dépendent largement des services intranet et Internet pour leurs opérations quotidiennes, il est essentiel de mettre en place une architecture de sécurité robuste pour protéger les ressources et les données sensibles [14]. Cette architecture de sécurité doit couvrir à la fois les services intranet, utilisés à l'intérieur de l'entreprise, et les services Internet, qui permettent la connectivité avec des réseaux externes.

L'étude et la mise en place d'une architecture de sécurité des services intranet et Internet sont un processus continu, car les menaces évoluent constamment. Cependant, en investissant dans la conception et la mise en place d'une architecture de sécurité solide, les organisations peuvent protéger leurs ressources et leurs données critiques, réduire les risques de perturbation des activités et maintenir la confiance de leurs utilisateurs et de leurs clients.

La sécurisation des réseaux est devenue un élément essentiel pour assurer la continuité des systèmes informatiques d'une entreprise, indépendamment de son activité, de sa taille et de sa répartition géographique [14]. L'entreprise BMT (Bejaia Méditerranéen Terminal) ne fait pas exception à cette règle. Avec une communauté croissante d'utilisateurs comprenant des directeurs, des chefs de services et des employés, la nécessité de partager des données stratégiques et des services disponibles augmente, ce qui engendre également une augmentation des risques sécuritaires. La vulnérabilité du réseau actuel face aux

potentielles attaques internes et/ou externes nous pousse à mettre en place des mesures de sécurité plus robustes. Ces mesures visent à préserver l'intégrité des données sensibles, à garantir la confidentialité des informations, à prévenir les interruptions dans les opérations commerciales et à maintenir la confiance des clients de l'entreprise BMT. Ce faisant, l'entreprise BMT pourra renforcer sa résilience face aux risques sécuritaires et assurer la pérennité de ses systèmes informatiques. C'est dans ce contexte que s'inscrit notre travail, avec pour objectif principal d'effectuer une étude et de mettre en place une architecture de sécurité pour les services intranet et internet.

Ce mémoire s'articule autour de quatre principaux chapitres. Pour bien le structurer, nous avons adopté le plan suivant :

Le premier chapitre s'intitule « Prérequis théoriques sur les réseaux et la sécurité » décrit brièvement des généralités sur les réseaux et la sécurité informatique.

Le deuxième chapitre nommé « Présentation du cadre d'étude et de stage » présente l'entreprise dans laquelle nous avons effectué notre stage, une brève étude sur le réseau de BMT, la problématique, ainsi que les améliorations proposées.

Le troisième chapitre intitulé « Proposition d'une amélioration pour l'architecture de sécurité existante » est consacré aux améliorations proposées pour régler les problèmes soulevés au sein de l'entreprise BMT, ainsi que l'architecture proposée.

Enfin, un dernier chapitre nommé « Mise en oeuvre de la solution » qui consiste a présenté l'ensemble des installations et configurations nécessaires pour la mise en œuvre de notre travail, ainsi que les tests et les validations.

Nous clôturons ce manuscrit par une conclusion générale qui résume les connaissances acquises durant la réalisation de notre projet suivie de perspectives que nous souhaitons accomplir dans le futur.

CHAPITRE 1

PRÉREQUIS THÉORIQUES SUR LES RÉSEAUX ET LA SÉCURITÉ

1.1 Introduction

La sécurité des réseaux informatiques est un sujet essentiel qui favorise le développement des échanges d'information dans tous les domaines. L'expansion et l'importance grandissante des réseaux informatiques ont engendré le problème de sécurité des systèmes de communication. Dans la plupart des organisations informatisées, partager les données directement entre machines est un souci majeur. Il s'avère indispensable de renforcer les mesures de sécurités, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

Dans ce chapitre, nous allons présenter les principaux concepts liés aux réseaux et sécurité informatique qui formeront la base nécessaire a notre contribution en présentant des généralités sur les réseaux informatiques suivis de quelques notions sur la sécurité.

1.2 Les réseaux informatiques

1.2.1 Définition

Un réseau informatique est un ensemble d'équipements électroniques relié entre eux par des canaux de communication (filaire ou sans fil) permettant de circuler des données [16].

1.2.2 Types de réseau

Les réseaux informatiques peuvent être classés selon plusieurs critères qui se différencient entre eux en fonction de la distance entre les systèmes informatiques, ou encore en fonction de la technologie qui permet de les mettre en œuvre, parmi ces critères on trouve l'étendue [15].

1.2.2.1 PAN (Personal Area Network)

Désigne un type de réseau informatique restreint en termes d'équipements, ce réseau comme son nom l'indique est pour une seule personne généralement mis en œuvre dans un espace d'une dizaine de mètres [15].

1.2.2.2 LAN (Local Area Network)

Ce réseau est limité à une zone géographique réduite qui ne dépasse pas 10 km tels qu'un bâtiment, il permet l'échange de données informatiques et le partage de ressources, Le débit varie de quelques Mbps à 100 Mbps avec un nombre de stations limités à 1000 stations [15].

1.2.2.3 MAN (Metropolitain Area Network)

Ce réseau est étendu sur une dizaine de kilomètres, permet l'interconnexion de plusieurs réseaux locaux, pouvant relier des points distants de 10 à 25 km [15].

1.2.2.4 WAN (Wide Area Network)

Appelé aussi réseau longue distance, ce réseau a une couverture nationale (Transpac) ou internationale (Internet), Leurs supports de transmission sont variés (ligne téléphonique, ondes hertziennes, fibre optique, satellite, etc) [15].

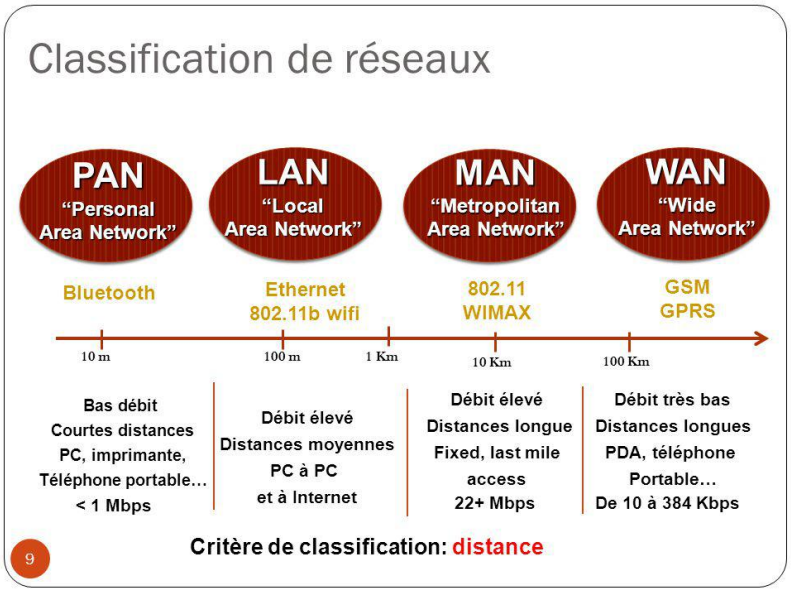

FIGURE 1.1 – Les types de réseau selon l'étendue.

1.2.3 Topologies

Une topologie caractérise la façon dont les différents équipements réseaux sont positionnés les uns par rapport aux autres. On distingue deux types de topologies [19] :

1.2.3.1 Les topologies physiques

Représente L'arrangement physique des éléments du réseau

- **Topologie en bus :** le message est envoyé simultanément à toutes les stations de travail en utilisant un seul câble pour relier toutes les stations sur la même ligne, ce type de montage est simple à mettre en œuvre et peu coûteux.
- **Topologie en étoile :** la liaison entre deux stations est établie, puis le message est envoyé, son principal avantage est que la panne n'affecte pas le reste du réseau.
- **Topologie en anneau :** c'est une topologie active, il s'agit d'un réseau local dans lequel les nœuds sont reliés en boucle fermée, Le message circule dans un seul sens et est régénéré par les stations de travail.
- **Topologie en maille :** le réseau maillé est un réseau dans lequel deux stations de travail peuvent être mises en relation par différents chemins. La connexion est effectuée à l'aide de commutateurs, ce réseau est facile a dépanné mais coûteux en câblage [19].

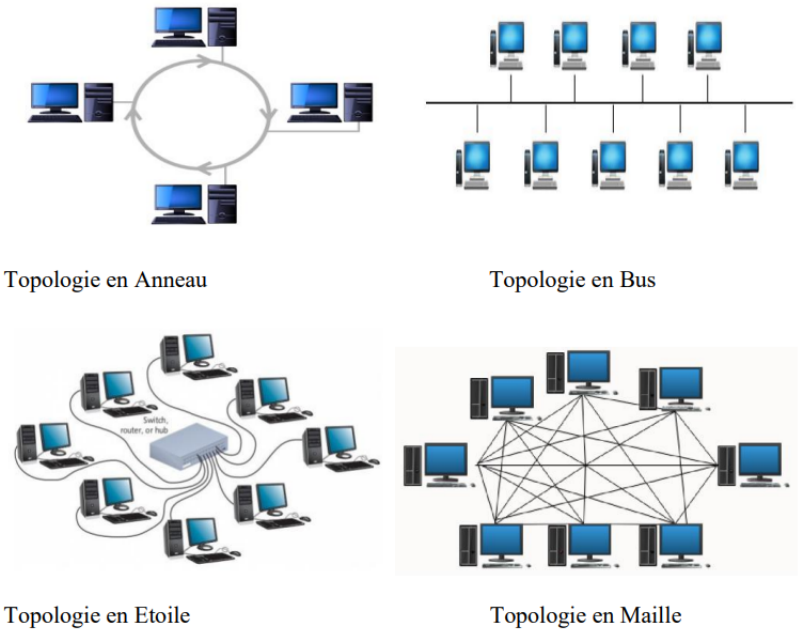

FIGURE 1.2 – Topologie des réseaux.

1.2.3.2 Les topologies logiques

Représente la façon selon laquelle les données transitent dans les câbles, les plus courantes sont : Ethernet,Token Ring et FDDI [19].

1.2.4 Les types d'architectures

1.2.4.1 Les réseaux organisés autour de serveurs (client/serveur)

Désigne un mode de communication entre plusieurs ordinateurs d'un réseau qui distingue un ou plusieurs clients du serveur, elle est utilisée surtout pour le partage de connexion internet et des logiciels,

ce type est plus facile à administrer lorsque le réseau est important l'administration est centralisée[6].

1.2.4.2 Les réseaux poste à poste (Peer to Peer/ égal à égal)

Contrairement à une architecture de réseau de type client/serveur, dans un réseau poste à poste il n'y a pas d'administrateur, chaque ordinateur joue à la fois le rôle de serveur et de client (Chaque utilisateur administre son propre poste) cela signifie notamment que chaque nœud du réseau est libre de partager ses ressources (données dans des répertoires partagés, imprimantes, cartes fax etc.) [6].

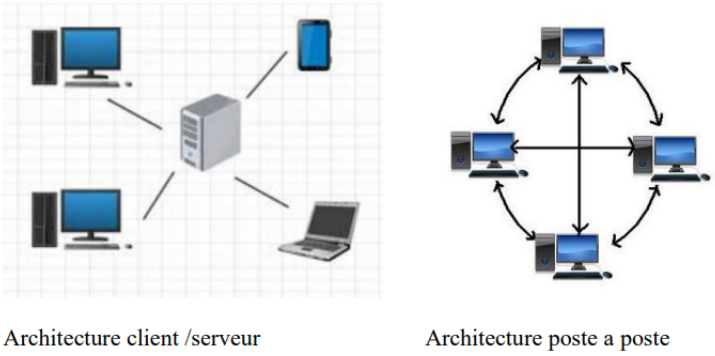

FIGURE 1.3 – Architecture des réseaux.

1.2.5 Les équipements des réseaux informatiques

1.2.5.1 Les équipements d'interconnexion

1. **Répéteur** : c'est un élément qui régénère et augmente le signal pour le transmettre d'un réseau à un autre (couche 1 du modèle OSI) [17].
2. **Concentrateur (hub)** : est un dispositif qui joue le rôle d'un répéteur multiport (lorsqu'un paquet est reçu sur un port, celui-ci est envoyé aux autres ports afin que tous les segments du réseau local puissent accéder à tous les paquets) (couche 1 du modèle OSI) [17].
3. **Pont (Bridge)** : des équipements permettant de relier des réseaux travaillant avec le même protocole (couche 2 du modèle OSI) [17].
4. **Commutateur (Switch)** : est un hub intelligent qui peut relier un segment de réseau à un ou plusieurs autres segments selon leurs adresses physiques de la couche liaison de données. Il possède une mémoire interne qui contient les informations sur le réseau commuté stocké dans une table appelée « table de commutation »(couches 2 et 3 du modèle OSI) [17].
5. **Passerelle (Gateway)** : est un système matériel et logiciel permettant de passer des informations d'un réseau à un autre en adaptant les différent couche de modèle OSI) [17].
6. **Routeur** : capable d'interconnecter plusieurs réseaux utilisant différents protocoles entre eux. Il permettant d'assurer le routage des paquets afin de déterminer le chemin qu'un paquet de données va emprunter (couche 3 du modèle OSI) [17].
7. **Fortigate** : fortigate est une gamme de boîtiers de sécurité UTM (appliance sécurité tout en un) comprenant les fonctionnalités firewall, Antivirus, système de prévention d'intrusion (IPS), VPN

(IPSec et SSL),filtrage Web, Antispam et d'autres fonctionnalités : QoS, virtualisation, compression de données [17].

1.2.5.2 Les équipements matériels

1. **Carte réseau** : est l'interface entre l'ordinateur et le réseau. Elle assure donc les échanges et les transferts des données avec les autres appareils présents sur le réseau tels que des serveurs, des imprimantes ou même des PCs. Elle est identifiée avec une adresse physique (l'adresse Mac) [19].
2. **La fibre optique** : permet de transmettre des données sous forme d'impulsions lumineuses avec un débit nettement supérieur à celui des autres supports de transmissions filaires. Elle est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice [12].
3. **La paire torsadée** : sont des câbles constitué au moins de deux brins de cuivres entrelacés en torsade et recouverts des isolants [12].
4. **Le câble coaxial** : est composé d'un fil de cuivre entouré successivement d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure [12].

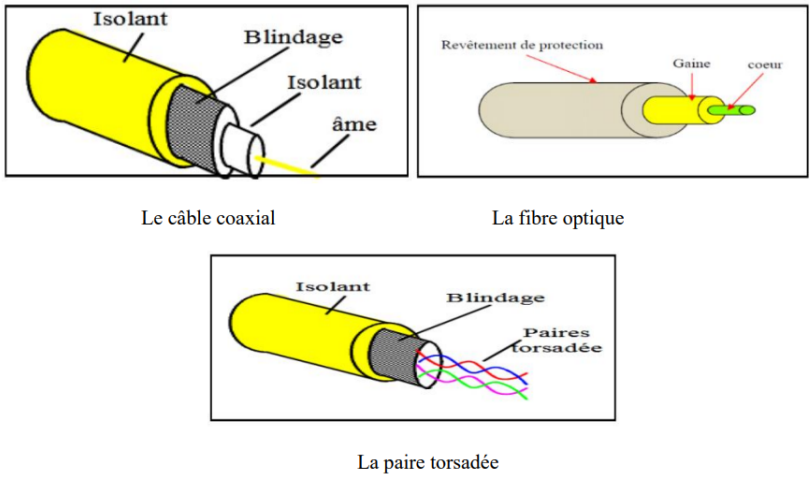

FIGURE 1.4 – Les différents types de capables.

1.2.5.3 Les connecteurs réseaux

Un connecteur est un dispositif qui termine un segment de câblage ou fournit un point d'entrée pour les dispositifs de réseau tels que les ordinateurs, les hubs et les routeurs [3].
Il existe plusieurs types différents de connecteurs

1. **Connecteur BNC** : adapter pour les câbles coaxiaux [3].
2. **Connecteur RJ45** : adapter aux câbles à paires torsadées [3].
3. **Connecteur fibre optique** : utiliser pour les fibres optiques [3].

1.2.6 Les normes de communication OSI et TCP/IP

La transmission d'information entre deux programmes informatiques sur deux noeud différentes passe par deux modèles : le modèle OSI ou le modèle TCP/IP.

1.2.6.1 Le modèle OSI

OSI (Open System Interconnection) est le modèle de base défini par ISO (International Standard Interconnections). Cette organisation revient régulièrement pour établir des normes de communication entre les ordinateurs sur les réseaux. Le modèle OSI normalisation la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau,ce modèle est organisé en sept couches successives [5].

1.2.6.2 Le modèle TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) est un ensemble de protocoles de communication utilisés pour connecter des périphériques réseau sur internet et peut également être utilisé comme protocole de communication sur les réseaux locaux (LAN) [5].
La figure 1.5 présente les couches des normes de communication OSI et TCP/IP.

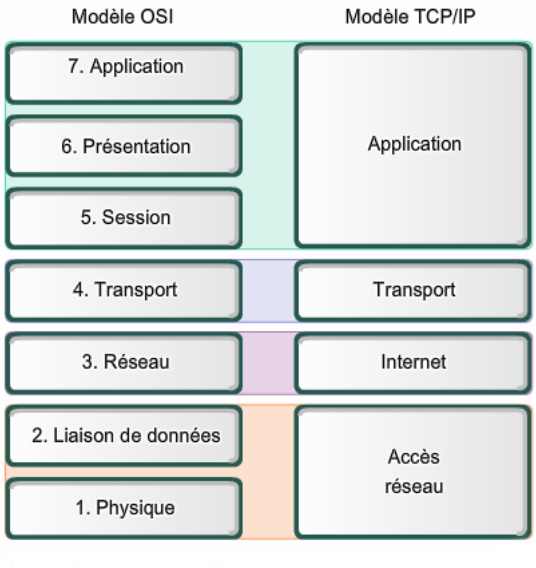

FIGURE 1.5 – Comparaison des modèles OSI et TCP/IP.

1.2.7 Les services et protocoles

Dans un réseau informatique, il existe différents protocoles et services qui sont utilisés pour permettre la communication, la gestion et la sécurité des données. ils sont essentiels pour assurer le bon fonctionnement et la sécurité des réseaux informatiques. Voici quelques-uns des protocoles et services couramment utilisés :

1.2.7.1 Les services

Il existe deux types principaux de services : les services Intranet et les services Internet.

1. **Les services intranet** Un intranet est un réseau privé similaire à internet, mais accessible uniquement à des utilisateurs spécifiques. Les entreprises utilisent intranet pour publier et stocker des informations utiles qui aident les employés dans leur travail quotidien [2], on cite : [20]

- Le courrier électronique.
- L'accès à l'Internet public.
- L'accès aux données de l'entreprise.
- La distribution et la publication d'informations.
- La gestion des documents.

2. **Les services Internet** : une série de réseaux mondiaux interconnecter qui permettent aux ordinateurs et aux serveurs de communiquer efficacement via un protocole de communication commun (IP). Ses principaux services sont : [9].

   • La messagerie électronique (e-mail) : est un service de transmission utilisé pour envoyer des messages écrits et des documents par voie électronique sur internet aux boîtes aux lettres électroniques des destinataires choisis par l'expéditeur [9].

   • Le transfert des fichiers FTP : est un protocole standard pour le transfert de fichiers entre ordinateurs sur internet via une connexion TCP/IP [9].

   • Le World Wide Web : est un système de pages web publiques interconnecter à travers l'internet [9].

   • Les groupes de discussion.

1.2.7.2 les protocoles

Les protocoles sont des règles et des normes établies qui définissent la manière dont les dispositifs et les systèmes informatiques communiquent et interagissent les uns avec les autres [3].

Le protocole DHCP : le protocole de configuration dynamique des hôtes (DHCP) est un protocole client/serveur qui automatise l'attribution d'adresses IP à des hôtes fixes et mobiles connectés avec ou sans fil [3].

Cependant, dans certaines configurations réseau, le serveur DHCP peut ne pas être directement accessible par les clients.

Le DHCP relay : facilite la communication entre les clients DHCP et le serveur DHCP, en permettant aux demandes et aux réponses DHCP de traverser des réseaux différents. Cela garantit que les clients peuvent recevoir des adresses IP et des configurations réseau appropriées, même s'ils ne sont pas directement connectés au serveur DHCP.

VTP (Virtual Trunking Protocol)

Définition

VTP est un protocole de liaison propriétaire de CISCO qui s'applique au niveau de la couche liaison de données du modèle OSI. Il est chargé de gérer les VLANs d'une manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs dans un réseau pour ajouter, modifier ou supprimer la configuration d'un appelé serveur VTP, afin de distribuer ces informations de configuration VLAN d'un bout à l'autre du réseau commuté. Ce protocole réduit les délais d'administration et de maintenance des réseaux VLAN [3].

Principe de fonctionnement

Le protocole VTP définit la notion de domaine VTP où ce dernier est composé d'un ou plusieurs équipements interconnectés qui partagent le même nom. Il regroupe des commutateurs pour échanger leurs informations de configurations envoyées par le serveur VTP de chaque domaine concerné et plus dans un environnement VTP, un commutateur peut assurer un des trois rôles qui définissent les trois

modes de fonctionnement suivants :

• Mode serveur VTP : Un commutateur en mode serveur est chargé de diffuser la configuration aux commutateurs du domaine VTP en envoyant des messages connus sous le nom « trames VTP », c'est le seul commutateur du domaine capable d'ajouter, supprimer ou renommer des VLAN dans le domaine VTP concerné [3].

• Mode client VTP : Un commutateur en mode client est chargé d'appliquer la configuration émise par un commutateur en mode serveur, ce mode ne donne pas la possibilité de créer, modifier Ou supprimer des informations VLAN. Donc, il faut d'abord appliquer la modification au sein du serveur VTP pour qu'elle se propage aux différents commutateurs en mode client du même domaine VTP [3].

• Mode transparent VTP : Un commutateur en mode transparent ne fait que diffuser les annonces VTP et les configurations du domaine VTP auquel il appartient à travers ses ports de liaison sans prendre en compte leurs contenus [3].

La figure 1.6 illustre le fonctionnement du protocole VTP

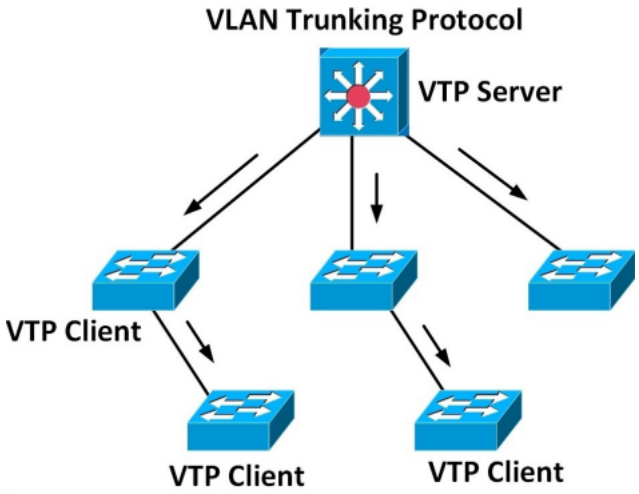

FIGURE 1.6 – Le protocole VTP.

1.3 La sécurité informatique

1.3.1 Définition

La sécurité informatique est un terme utilisé pour décrire l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement d'un système [11].

1.3.2 La sécurité, la sûreté et la sûreté de fonctionnement

— **La sécurité** : La protection contre les actions intentionnelles malveillantes [22].
— **La sûreté** : Est la protection contre les actions non intentionnelles [22].
— **La sûreté de fonctionnement** : Est un domaine d'activité qui propose des moyens pour augmenter la fiabilité et la sûreté des systèmes dans des délais et avec des coûts raisonnables [8].

1.3.3 Les objectifs de la sécurité

La sécurité informatique vise généralement cinq principaux objectifs

1. **La confidentialité :** empêcher la divulgation d'informations à des entités (sites, organisations, personnes, etc.) non autorisée.
2. **L'intégrité :** assurer que les informations n'ont pas été altérées par des entités non autorisées ou inconnues.
3. **L'authentification :** prouver qu'une information provient de la source annoncée.
4. **La disponibilité :** assurer l'accès et la continuité d'un service afin de préserver le bon fonctionnement du système.
5. **Non répudiation :** empêcher le démenti(nier) d'engagements ou d'actions précédentes [11].

1.3.4 Terminologies de la sécurité informatique

1. **Les menaces** : la possibilité qu'une vulnérabilité soit exploitée accidentellement ou par un agent malicieux [11].
2. **Les vulnérabilités** : représente les failles de la sécurité dans un système [11].
3. **Les risques** : une mesure de l'importance dans laquelle une entité est menacée par une circonstance ou un événement potentiel [11].
4. **Les attaques** : est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant du système et généralement préjudiciable [11].
5. **Les contre-mesures** : ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique [11].

1.3.5 La politique de sécurité

Une politique de sécurité est considérée comme un ensemble de règles spécifiques destinées à décrire comment les informations et autres ressources sensibles sont gérées, protégées et distribuées au sein d'un système informatique [10].

1.3.5.1 Les éléments clés d'une politique de sécurité contre les intrusions informatiques

— L'identification des enjeux, des risques et des techniques de piratage utilisées [10].
— Les mesures de sécurité dans un réseau : pour pouvoir se défendre contre les dangers omniprésents [10].
— L'authentification des utilisateurs, leurs droits d'accès, les ports et les services, les outils de sécurité, les audits et les sauvegardes seront abordés [10].
— Les principales opérations à effectuer avant et/ou après les attaques [10].

1.3.5.2 Les types de politiques de sécurité

Une politique de sécurité couvre les éléments suivants [10]

— **Sécurité de l'infrastructure :** il inclut la sécurité logique et physique des périphériques et des connexions réseau.

— **Sécurité des accès :** cela inclut la sécurité logique de l'accès local et distant aux ressources de l'entreprise, ainsi que l'administration des utilisateurs et les droits d'accès des utilisateurs aux systèmes d'information de l'entreprise.
— **Sécurité de l'intranet face à Internet :** il intègre la protection logique de l'accès aux ressources de l'entreprise (intranet) et de l'accès aux ressources externes (Internet).

1.3.6 Les attaques informatiques

Une attaque est un moyen d'exploiter une (ou plusieurs) vulnérabilités d'un système pour violer une ou plusieurs exigences de sécurité [4].

1.3.6.1 Catégorie d'attaques

Il existe quatre catégorie d'attaques : interruption, interception, modification, fabrication.
— **Interception** : une tentative par une personne non autorisée d'accéder à des informations. Ce type d'attaque impacte la confidentialité des informations [13].
— **Interruption** : un attaquant non autorisé tente de se faire passer pour une autre entité. Il s'agit d'une attaque contre la disponibilité des ressources [13].
— **Modification** : contient des modifications au message d'origine.c'est-à-dire un troisième personne non autorisée intercepte et modifie les données avant de les divulguer au destinataire. Il s'agit d'une attaque contre l'intégrité de l'information [13].
— **Fabrication** : cela peut impliquer l'insertion de fausses données dans les communications de l'application, de faux messages sur le réseau ou l'ajout d'enregistrements dans des fichiers. Il s'agit d'une attaque contre l'authentification [13].

1.3.6.2 Les différentes étapes d'une attaque

— **Identification de la cible :** permet de récolter un maximum de renseignements sur la cible, ces informations peuvent être techniques tel que les adresses IP des serveurs accessibles de l'extérieur ou sociales [4].
— **Le scanning :** c'est une phase importante son objectif est de compléter les informations réunies sur une cible visées [4].
— **Exploitation des failles :** cette étape permet d'exploiter les failles identifiées sur les éléments de la cible, l'attaque peut se faire par l'injection de code malveillant au sein du système d'exploitation ou de l'application, peut aussi viser la disponibilité du système [4].
— **La progression :** le pirate va vouloir mettre en place des accès pour se reconnecter plus facilement plus tard lors d'une prochaine attaque [4].
— **Effacement des traces :** représente la dernière étape d'une attaque, consiste a effacer toutes les traces a fin que l'attaque passe complètement inaperçue et ne puisse jamais être découvert [4].

1.3.6.3 Classification des attaques selon l'interaction avec le système cible

La figure 1.7 montre la classification des attaques selon l'interaction avec le système cible.

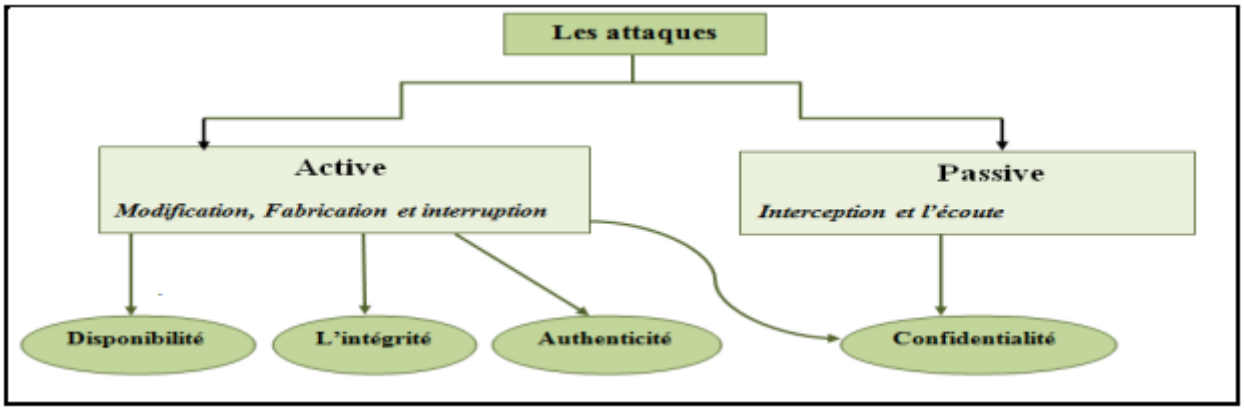

FIGURE 1.7 – Classification des attaques selon l'interaction avec le système cible[4].

1.3.7 Mécanismes de sécurité

À cause des menaces provenant des logiciels malveillants,il faut mettre en place des mécanismes pour assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer

1. **Antivirus** : les antivirus sont des programmes de sécurité capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci(supprimer le virus du fichier sans l'endommager) dans la mesure du possible si jamais un ou plusieurs virus sont trouvés. Mais, parfois ce nettoyage simple n'est pas possible [21].
2. **Chiffrement** : le cryptage est un processus cryptographique conçu pour rendre les documents inintelligibles à ceux qui ne possèdent pas les clés de cryptage et de décryptage. Ce principe est généralement lié au principe d'accès conditionnel [18].
3. **Pare-feu** : un ensemble de divers composants matériels et logiciels qui contrôlent le trafic intérieur et extérieur conformément aux politiques de sécurité. D'une part, il garantit que les attaques et les connexions suspectes se voient refuser l'accès à votre réseau interne. D'autre part, les pare-feu sont souvent utilisés pour empêcher la fuite d'informations non protégées vers l'extérieur [18].
4. **Réseaux privés virtuels (VPN)** : un réseau privé virtuel permet aux utilisateurs de créer un chemin virtuel sécurisé entre une source et une destination. Grâce au principe de tunneling (Tunneling) où les deux extrémités sont identifiées, les données sont transmises sous forme cryptée.Le but d'un VPN est de créer un réseau privé à moindre coût. En cryptant les données tout se fait comme si la connexion se faisait de l'extérieur d'Internet [21].
5. **Zone démilitarisée** : une DMZ (anglais :De-Militarized Zone), ou « zone démilitarisée » est une partie du réseau local dont l'objectif est d'être accessible depuis l'extérieur du réseau local, avec ou sans authentification préalable [7].
6. **EtherChannel** : l'etherchannel qui est aussi connu sous l'appellation d'agrégation de liens est une technologie qui permet de regrouper plusieurs liens physiques en un seul lien logique. L'agrégation

des liens (EtherChannel) a pour objectif d'augmenter la vitesse de la bande passante, il est possible de regrouper jusqu'à 8 interfaces physiques, la seule condition est que les types de ports doivent être identiques sur ce même lien, par exemple, il n'est pas possible de regrouper deux ports FastEthernet et deux ports Gigabit Ethernet dans un EtherChannel.

1.4 Conclusion

Dans ce chapitre nous avons illustré quelques termes en relation avec notre thème sur les réseaux informatiques, leurs types, leurs topologies et leurs différents composants ainsi que quelques notions sur la sécurité informatique tels que ses objectifs,les terminologies liées a cette dernière et quelques notions sur les attaques, ce baguage théorique nous permettra de bien munir le développement de notre thème.

Dans le chapitre suivant, nous aborderons la présentation de l'organisme d'accueil.

CHAPITRE 2

PRÉSENTATION DU CADRE D'ÉTUDE ET DE STAGE

2.1 Introduction

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

Nous commençons par une brève présentation de l'entreprise BMT, puis décrivons la structure générale de son organisation et de ses différents départements, notamment département d'Informatique, ainsi que ses objectifs. Ensuite, Nous évaluerons les problèmes soulevés et proposerons des solutions.

2.2 Présentation générale de BMT

BMT ou Bejaia Méditerranéen Terminal est une société par action (SPA) qui fournit des services de la gestion et l'exploitation du Terminal à conteneurs dans les meilleurs délais, coûts et fiabilité. Cette dernière s'agit d'une coentreprise entre L'EPB (Entreprise Portuaire de Bejaia) qui est l'autorité portuaire qui gère le port de Bejaia et PSE (Portek Systems and Équipement) qui est un opérateur de Terminaux à conteneurs présent dans plusieurs ports a travers le monde. Afin d'offrir des services de qualités elle s'est disposée des équipements performants et de systèmes informatiques pour atteindre ses objectifs [1].

La figure 2.1 illustre la jointe venture de l'EPB et PORTEK.

FIGURE 2.1 – Jointe venture de l'EPB et PORTEK.

2.2.1 Création et évolution

Suite au besoin de l'EPB d'établir un partenariat pour la gestion et l'exploitation du terminal à conteneurs au port de bejaia, l'entreprise portuaire de bejaia à sélectionné le groupe PORTEK spécialisé dans le domaine de la gestion des terminaux à conteneurs. Le projet a été soumis au conseil des participations de l'État (CPE) en février 2004 et le CPE a approuvé le projet en mai 2004.
Donc, BMT a été créé sur une décision du conseil des participations de l'État (CPE) avec la joint-venture de l'EPB à 51 % et PORTEK à 49 % [1].

2.2.2 Situation géographique de BMT

BMT se trouve au port de bejaia stratégiquement situé au cœur de la méditerranée dans le nord du continent africain, elle occupe une situation géographique importante et stratégique, dispose des voies de communication reliant l'ensemble des routes du pays, des voies ferroviaires et à proximité d'un aéroport international ce qui facilite le transport de toutes sortes de marchandises conteneurisées.
Position GPS : Attitude Nord : 36 45 24 Longitude est : 05 05 50

La figure 2.2 donne un aperçu sur la situation géographique de BMT.

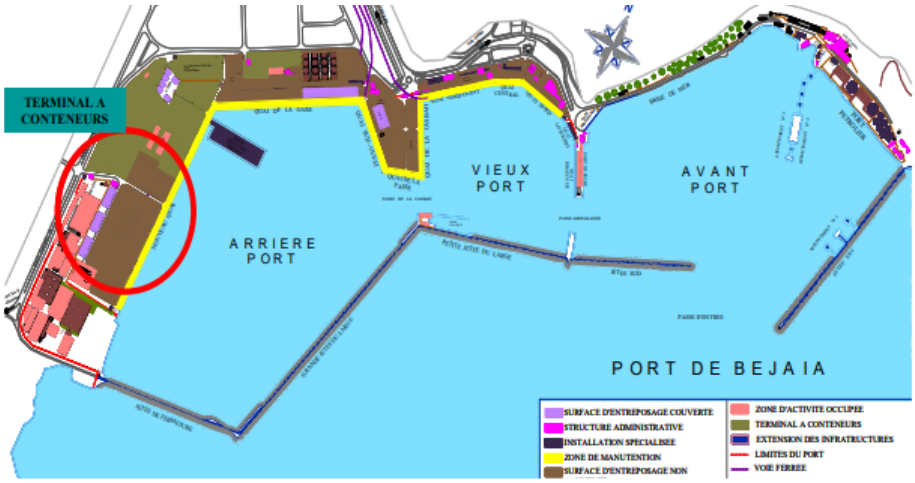

FIGURE 2.2 – La situation géographique de BMT.

2.2.3 La structure de l'entreprise BMT

BMT est divisé en plusieurs directions :
• Direction générale (DG) : à sa tête, le directeur général qui gère l'entreprise. Il a le pouvoir de décision, d'administrer l'entreprise et d'assigner des directives pour les différentes structures et fait la liaison entre les directions d'entreprise, composé des départements suivants :

— Département Audit interne : assure l'audit des procédures et mesure leur efficacité.
— Centre de Digitalisation et du Numérique (CDN) : basé sur un management de proximité, le C D N vise l'harmonisation, la cohérence, et la gouvernance des systèmes des ports, ce qui nécessite une restructuration et un alignement pour perfectionner les services rendus aux clients, en vue d'améliorer la compétitivité du secteur du transport maritime et de mettre en place une plateforme d'échange de données, dématérialisée et interactive entièrement dédiée à la fluidification

des passages portuaires et à la facilitation du commerce et d'offrir un service global au profit des acteurs portuaires.
— Centre de formation [1].

• Direction des ressources humains et moyens : assure la coordination et le suivi des services de la DRHM et le suivi des projets, elle possède les services suivants.
— Le service patrimoine : assure la gestion des stocks et des immobilisations.
— Service moyens généraux : satisfaire les besoins des différentes structures en produits et prestations de services.
— Service ressources humaines : assure la gestion administrative du personnel et le développement des compétences [1].

• Direction des finances et de comptabilité (DFC) : assure l'élaboration des bilans et des situations financières de la société. Elle est constituée de deux services
— Service comptabilité : procède au contrôle et à l'enregistrement de toutes les opérations de la société (achat, vente, investissement.etc).
— Service finances et budget : assure le suivi de l'exécution du budget de la société et de la comptabilité analytique et aussi la gestion de la trésorerie.
— Service fiscalité et contrôle comptable [1].

• Direction marketing : veille à la marque de l'entreprise en se préoccupant en permanence d'entretenir des relations avec les clients. Elle vise à faire connaître ses missions, ses programmes, ses orientations et ses performances auprès de ses clients. En outre, Elle amène son environnement externe à prendre conscience de l'importance des démarches qu'elle entreprend dans le développement et l'amélioration de la qualité de ces services. Elle se compose de deux services
— Service commercial : suivent la facturation, la gestion de portefeuille client et le recouvrement des créances.
— Service Marketing : assure la promotion de l'image de marque de l'entreprise et la mise en œuvre du plan marketing et commercial [1].

• Direction des opérations : assure la planification des escales, de parc à conteneurs et la planification des ressources (humaines et matérielles). Elle prend en charge les opérations de manutentions, comme la réception des navires porte-conteneurs et leurs chargements et déchargements. De plus, elle suit les opérations de l'acconage tel que : le suivi des livraisons, dépotages, mise à disposition des conteneurs vides, traitement des conteneurs frigorifiques [1].

• Direction technique (DT) : assure la maintenance préventive et curative des engins de la société [1].

2.2.4 Organigramme de l'entreprise

La figure 2.3 présente les différentes directions de l'entreprise de BMT.

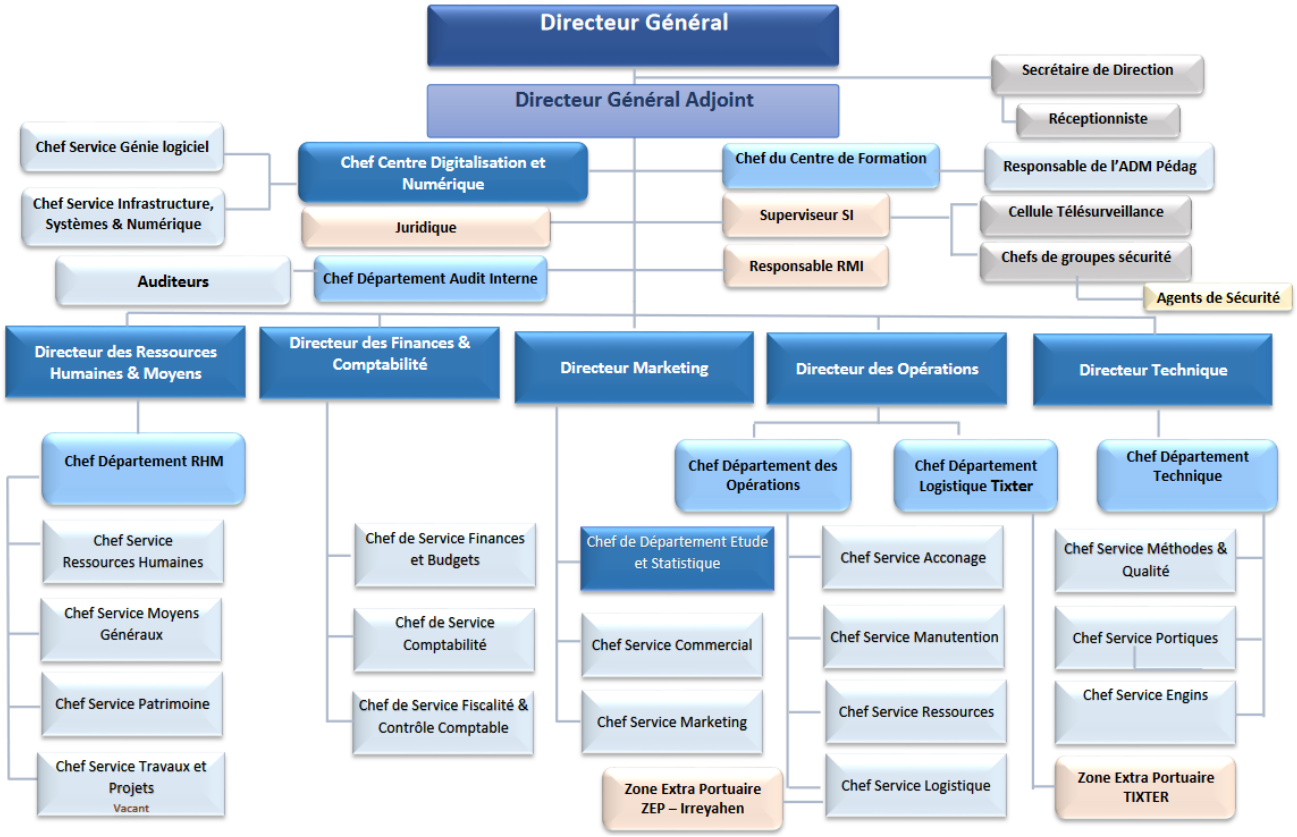

FIGURE 2.3 – Organigramme Général de BMT.

2.2.5 Les activités et les objectifs de BMT

L'activité principale de l'entreprise BMT est le suivi, la gestion et l'exploitation du terminal à conteneurs. Elle a pour mission et objectifs de

• Traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des navires porte conteneurs et des conteneurs.

• La manutention sur navire aussi bien le chargement et le déchargement des conteneurs et leurs entreposages dans les zones de stockage.

• Le service d'aconage sur les aires spécialisées ainsi que leurs livraisons.

• Faire du terminal à conteneurs de BMT une infrastructure moderne et même de répondre aux exigences les plus sévères, en matière de qualité, dans le traitement des conteneurs.

• La mise à disposition d'une nouvelle technologie dans le traitement des conteneurs pour

- Un gain de productivité.
- Une réduction des coûts d'escale.
- Une fiabilité de l'information.
- Un meilleur service.
- Sauvegarder la marchandise des clients.

— Faire face à la concurrence nationale et internationale.
— Propulser le terminal au stade international.
— Gagner des parts du marché.

• La création et la gestion d'un centre de formation.

2.3 Présentation du service d'accueil (Centre de digitalisation et numérique)

2.3.1 Organisation

L'organigramme suivant 2.4 nous illustre les différentes sections du centre de digitalisation et numérique)

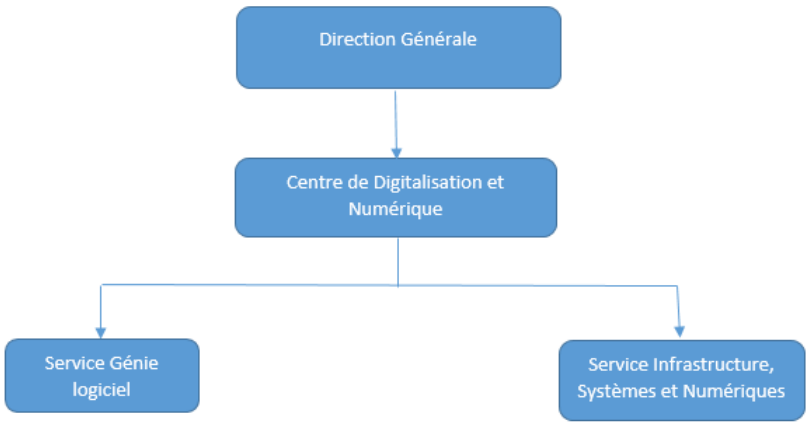

FIGURE 2.4 – L'organigramme du centre de digitalisation et numérique.

2.3.2 Activité du centre de digitalisation et numérique

C'est un service qui appartient à la direction générale. Ses principales fonctions sont :

• Le 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.
• Le développement de nouvelles applications aux différentes structures.

2.3.3 Étude de l'existant

Afin de pouvoir récolter toutes les informations nécessaires pour proposer une solution adéquate qui répond aux besoins des utilisateurs, nous avons besoin d'apporter une lumière sur l'étude de l'existant qui est une phase importante dans le développement d'un projet informatique.

2.3.3.1 Présentation du réseau de BMT

Le réseau de BMT est un réseau ethernet, basé sur une topologie en étoile, pour la diffusion de ses données il utilise le mode poste a posté avec une liaison point a point, la norme de câblage utilisé est la fibre optique avec un débit égal à 30 Mbit/s et une connexion internet ADSL.
Il se base sur le principe de redondances d'équipements en basculant manuellement en cas de panne avec une synchronisation en temps réelle.
Le réseau de BMT possède 300 utilisateurs dont 120 utilisent l'internet.

2.3.3.2 Architecture du réseau de BMT

La Figure 2.5 illustre l'architecture actuelle du réseau de l'entreprise BMT.

Le réseau BMT est composé de deux réseaux a savoir le nouveau et l'ancien bloc relier avec une fibre optique.

• Ancien bloc : Il contient trois réseaux :

- Le réseau CTMS (Container Terminal Management System) : est un système de gestion des terminaux à conteneurs, se présente sous l'architecture client/serveur, composé de deux serveurs IBM (International Business Machines) pour les applications et web, deux serveurs de base de données qui tourne sur oracle, un serveur DHCP (Dynamic Host Configuration Protocol) et un serveur DNS (Domain Name System).
- Le réseau LAN (Local Area Network) connecté sur internet : a un réseau wifi et un réseau filaire, il a un serveur NAS (Network Access Server) qui est un serveur de fichiers, il stocke des données, un serveur de caméra CCTV (Closed-Circuit Télévision) qui gère les caméras de l'entreprise et un serveur AVP (serveur d'application) pour la facturation. Les serveurs web sont reliés à un Switch auquel sont branchés les postes de travail pour solliciter ces derniers.
- Le réseau IPROS (Opérating Systèm Terminal) : se présente sous l'architecture client/serveur. Il est composé de deux serveurs de bases de données sur lesquels est hébergée l'application ipros qui tourne sous Oracle, et de trois serveurs d'application Apache Tomcat, ces derniers utilisent linux comme système d'exploitation (les serveurs de ce réseau sont en redondance).
- Le réseau BMT dispose d'un site distant appelé ZEP (Zone extra-portuaire) relié avec un VPN (Virtual Private Network) et des lignes spécialisé privées avec une adresse IP (Internet Protocol) fixe.

• Le Nouveau bloc contient un seul réseau LAN (Local Area Network) qui a un réseau wifi et un réseau filaire, il a un serveur pour la gestion des stocks, serveur de gestion d'investissement, serveur de vidéosurveillance et un serveur GMAO (Gestion de Maintenance Assistée par Ordinateur) qui contient l'application GRPI (Gestionnaire Libre de Parc Informatique) qui permet la gestion des pannes.

Remarque : il existe un autre réseau au niveau de l'ancien bloc qui n'est pas relié au réseau principal qui est le réseau comptabilité administré et géré d'une manière manuelle.

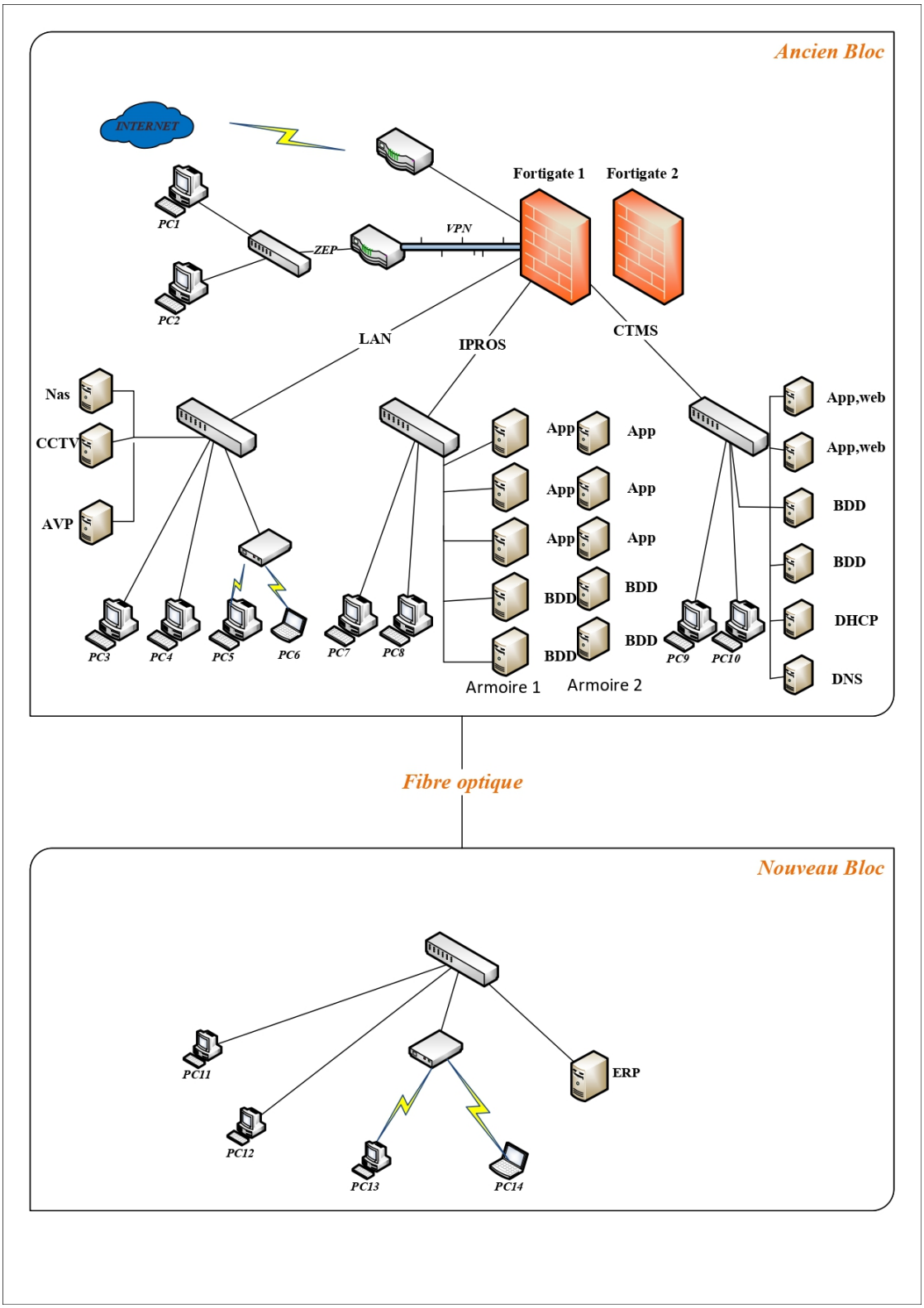

FIGURE 2.5 – Architecture actuelle du réseau de BMT.

2.3.3.3 Les différents équipements qui existent dans le réseau

1. **Les équipements de raccordement**

   Le tableau 2.1 illustre les équipements de raccordement utilisés pour établir des connexions physiques ou logiques entre les différents éléments du réseau de l'entreprise BMT.

Équipement	**Marque**	**Quantité**	**Caractéristique**
Routeur	Fortinet Fortigate 100F	2	1 port USB, 1 port console, 2 ports DMZ, 2 ports WAN, 2 ports HA, 12 ports RJ45, 2 ports SFP+ Forti-Link, 4 ports SFP Slots et 4 ports RJ45/ SFP shared Medias Pairs.
Commutateur	Cisco SG200-26	15	26 ports RJ45 et 2 ports SFP
Convertisseur	D-Link DMC-1000	50	peut contenir jusqu'à 16 convertisseurs de média

TABLE 2.1 – Les équipements de raccordement de BMT.

2. **Les équipements terminaux**

   Le tableau 2.2 présente les équipements terminaux utilisés par les utilisateurs pour accéder et interagir avec le réseau de l'entreprise BMT.

Équipement	**Marque**	**Quantité**	**IOS**
PC bureau	HP,Lenovo	130	Windows 10
PC portable	HP ,Lenovo	30	Windows 10
Serveur	Proliant DL380 Gen 9	14	Linux/Windows
Enduleur	APC	130	/
Imprimante réseau	IPSON, CANON KYCERA	8	/
Imprimante laser	HP	30	/
Caméra de surveillance	@lhua	14	/
modem	ADSL	2	/

TABLE 2.2 – Les équipements terminaux de BMT.

3. **Les supports de transmission**

Pour relier les différents équipements qui sont utilisés dans le réseau de l'entreprise, BMT opte pour un seul type de média qu'est la fibre optique.

Les différents logiciels de l'entreprise

• ERP (Entreprise Resource Planning) : est un logiciel de gestion intégrant de nombreuses fonctionnalités. Un ERP permet de gérer l'ensemble des services de l'entreprise comme la gestion des stocks, la gestion de la production, le CRM (Customer Relationship Management), la comptabilité ou la qualité. Les applications existantes au BMT, sont les suivantes :

— Application de gestion de comptabilité.
— Application de gestion de la paye.
— Application de gestion des stocks.
— Application de gestion des investissements.
— Application de gestion de temps de pointage.
— Application de gestion de maintenance d'équipements.
— Application de gestion de terminal CTMS.
— Application de gestion commerciale (facturation et recouvrement).
— Application de gestion des bons de commande.
— Application AnyDesk pour l'accès à distance.

• Antivirus Kaspersky version entreprise.
• Logiciels d'exploitation

— Windows Server 2012.
— Le pack Ms office 2013 et 2016.
— Windows 8 et 10 pour les utilisateurs.

2.3.3.4 Service intranet et Internet de BMT

1. Les services internet

   Internet offre une variété de ressources ou de services. Les services existants au BMT sont les suivants :

   • La messagerie électronique (e-mail).
   • Le transfert des fichiers FTP.
   • Le World Wide Web.

2. Les services intranet

   Les services intranet existant au BMT sont les suivants :

   • Le courrier électronique.
   • L'accès à l'Internet public.
   • L'accès aux données de l'entreprise.
   • La distribution et la publication d'informations.
   • La gestion des documents.

2.3.3.5 Politique de sécurité du réseau en place

• Par-feu fortigate : fournit des solutions de sécurité réseau robustes conçues pour protéger les réseaux, les utilisateurs et les données contre l'évolution des menaces, fortinet est aujourd'hui le leader reconnu sur le marché des firewalls UTM (Unified Threat Management).

• Antivirus Kaspersky : se classe parmi les premiers scanneurs de virus, il offre une protection contre les logiciels espions, les virus, autres vers et chevaux de Trois ainsi qu'une défense proactive et plusieurs autres avantages.

• Algorithme cryptographique RSA : est un algorithme de chiffrement asymétrique utilisé pour échanger des données confidentielles sur Internet.

• VPN physique et des lignes spécialisé privé qui relient le site distant ZEP au BMT en utilisant les algorithmes cryptographiques suivants dans la phase d'échange de clés.

— SHA256.
— SHA256-RSA.
— RSA (2048 bits).
— IKEv2.

• Filtrage par adresse MAC : permet de contrôler l'accès au sein du réseau local.

2.4 Problématique

Lors de l'étude du réseau de l'entreprise BMT, de nombreuses lacunes ont été découvertes, ce qui nous a permis de définir un grand nombre de contraintes pouvant dégrader leurs performances. C'est pourquoi, nous remarquons a partir de la figure 2.5 :

La présence des serveurs en redondance du réseau IPROS dans le même site qui est l'ancien bloc provoque un arrêt de tous les services de l'entreprise en cas de risque.

Architecture plate : Absence des VLANs peut entraîner une utilisation inefficace de la bande passante, une mauvaise segmentation du réseau, une complexité accrue de la gestion et une sécurité compromise.

L'architecture point à point utilisé ne supporte pas plusieurs machines, peut devenir difficile à administrer et n'est pas aussi sécurisée.

Absence des serveurs en redondances au niveau des réseaux LAN et CTMS peut entraîner une perte de données et une augmentation des risques de sécurité.

• Bascule des équipements en redondance telle que le routeur et les serveurs au niveau du réseau IPROS d'une façon manuelle conduit a une perte du temps en cas de panne et vise la disponibilité des informations de l'entreprise BMT.

• Le réseau sans fil est peut sécurisé.

• L'entreprise utilise des switchs cisco programmable au niveau de ses trois réseaux, ces derniers ne sont pas programmés.

2.5 Améliorations proposées

Afin de remédier à des problèmes identifiés lors de notre stage au sein de BMT, nous proposons les améliorations suivantes :

1. L'utilisation de cluster offre de meilleures performances en matière de disponibilité, de répartition des charges.
2. Mise en place des VLANs afin d'augmenter les performances du réseau, réduire les coûts et améliorer la sécurité.
3. Amélioration de la sécurité :
   • Architecture client/serveur : à travers cette architecture le réseau peut supporter plusieurs machines, peut ajouter ou retirer un poste client sans perturber le réseau et renforce la sécurité du réseau.
   • la sécurisation filaire et sans fil.
   • Étude des trafics VPN.
   • Authentification des ports physiques filaire et sans fil.
   • Filtrage réseau et ports logiques.
   • Virtualiser les serveurs logiques des réseaux LAN (ancien et nouveau bloc) et CTMS dans les serveurs physiques car c'est inutile de multiplier le nombre de serveurs physiques.

2.6 Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil de BMT, ce qui nous a permis de mieux comprendre ses service. En étudiant l'existant, nous nous sommes familiarisés avec le réseau actuel de l'entreprise BMT, nous avons approfondi notre compréhension de son fonctionnement et de ses différents services, et nous avons identifié ses lacunes et ses problèmes. Sur la base de ces constatations, nous avons formulé des solutions pour remédier à ces problèmes.

Dans le chapitre suivant nous allons présenter une proposition d'une amélioration pour l'architecture de sécurité existante.

CHAPITRE 3

PROPOSITION D'UNE AMÉLIORATION POUR L'ARCHITECTURE DE SÉCURITÉ EXISTANTE

3.1 Introduction

L'importance d'une bonne architecture réseau dans une entreprise est cruciale pour garantir une connectivité fluide, une communication efficace et une collaboration transparente entre les systèmes et les utilisateurs. De plus, une architecture bien conçue renforce la sécurité en mettant en place des mesures de protection adéquates. Elle permet également une évolutivité et une flexibilité optimales pour s'adapter aux besoins changeants de l'entreprise. Enfin, une architecture réseau solide assure la continuité des activités en réduisant les temps d'arrêt et en maintenant la disponibilité des services. Dans le contexte spécifique du BMT, ce chapitre se concentrera sur les améliorations proposées pour remédier aux problèmes identifiés, en présentant les motivations, le contexte du projet, le cahier des charges et l'architecture proposée. Une conclusion synthétisera les points clés.

3.2 Motivation

L'amélioration d'une architecture réseau réduit les problèmes potentiels et les limitations qui peuvent entraver le bon fonctionnement d'une entreprise. Une architecture réseau optimisée permet d'obtenir une connectivité fluide et fiable entre les systèmes et les utilisateurs, ce qui réduit les interruptions et les temps d'arrêt. Elle renforce également la sécurité en mettant en place des mesures de protection appropriées, ce qui réduit les risques d'attaques et de violations de données. De plus, une architecture réseau améliorée offre une plus grande flexibilité et évolutivité, permettant à l'entreprise de s'adapter rapidement aux changements technologiques et aux besoins croissants. Cela réduit les coûts liés à la maintenance et à l'expansion du réseau. Enfin, une architecture réseau optimisée facilite la gestion et l'administration du réseau, ce qui réduit la charge de travail et améliore l'efficacité opérationnelle de l'entreprise. Dans l'ensemble, l'amélioration d'une architecture réseau réduit les problèmes potentiels, améliore la sécurité, favorise la flexibilité et facilite la gestion, ce qui contribue à un fonctionnement plus efficace et performant de l'entreprise, aucune entreprise n'échappe pas à cette nécessité à savoir

L'entreprise Bejaia Mediterranean Terminal (BMT).

Après avoir étudié le réseau de l'entreprise BMT, plusieurs lacunes ont été identifiées. Afin de remédier à ces problèmes, il est essentiel de mettre en place une architecture réseau améliorée et sécurisée pour l'entreprise Bejaia Mediterranean Terminal (BMT). Cette décision revêt une grande importance pour protéger les données stratégiques de l'entreprise, garantir la disponibilité des services et renforcer la résistance du réseau aux attaques internes et externes au réseau de l'entreprise BMT.

Pour l'entreprise BMT, l'implémentation d'un serveur Active Directory présente plusieurs motivations :

— Confidentialité, intégrité et authentification : L'utilisation d'Active Directory permet de lier les utilisateurs aux ressources réseau dont ils ont besoin tout en garantissant la confidentialité des données, leur intégrité et l'authentification des utilisateurs.
— Protection contre les pannes et la perte de données : Active Directory offre des mécanismes de sauvegarde et de récupération qui permettent de protéger les données et de minimiser les pertes en cas de panne ou d'incident.
— Administration centralisée : Avec Active Directory, l'administration du réseau est centralisée, ce qui permet de réduire les coûts et les tâches liées à la gestion des utilisateurs et des ressources. Il est possible de définir des règles et des droits pour chaque élément du réseau, facilitant ainsi la gestion et le contrôle des ressources.
— Architecture hiérarchique : Une architecture Active Directory hiérarchique offre une adaptabilité aux topologies en évolution rapide, une administration simplifiée, une sécurisation des données et des accès au plus près de la source, ainsi qu'une redondance en cas de défaillances réseau.

Pour assurer la fiabilité et la haute disponibilité des composants en double (serveurs, Fortigate, etc.), il est recommandé d'utiliser des clusters qui permettent de répartir la charge de manière transparente d'un serveur à un autre et de résoudre les problèmes de défaillance du système.

La mise en place de VLANs (Virtual Local Area Networks) offre une bonne gestion et une souplesse lors de l'administration du réseau. Les VLANs permettent à l'administrateur réseau d'organiser le LAN de manière logique plutôt que physique, ce qui facilite le déplacement, l'ajout et la modification des stations de travail, le contrôle du trafic réseau et l'amélioration de la sécurité.

Enfin, l'implémentation d'une zone démilitarisée (DMZ) est souvent nécessaire lorsque certaines machines du réseau interne doivent être accessibles depuis l'extérieur. La DMZ permet de créer une interface distincte accessible à la fois depuis le réseau interne et le réseau externe, tout en préservant la sécurité de l'entreprise.

Ces choix et motivations témoignent de l'importance accordée à la sécurité, à la flexibilité et à la gestion efficace du réseau au sein de l'entreprise Bejaia Mediterranean Terminal (BMT).

3.3 Contexte du projet à réaliser

Notre travail consiste à mettre en oeuvre des améliorations à l'architecture actuelle de BMT pour assurer un meilleur fonctionnement des services intranet et Internet.

3.3.1 Présentation du projet à réaliser

Après avoir effectué une étude approfondie du réseau de l'entreprise Bejaia Méditerranéen Terminal (BMT), il a été constaté que des améliorations sont nécessaires. Dans le cadre de ce projet, nous proposerons plusieurs modifications visant à améliorer le fonctionnement des services intranet et internet du réseau, à renforcer la sécurité du réseau de BMT et à améliorer sa gestion, pour cela :

• Nous devons transformer l'architecture de BMT en une structure hiérarchique pour assurer la simplicité et la clarté des rapports hiérarchiques au sein de chaque service de l'entreprise.

• Nous devons mettre en place des VLANs afin d'augmenter les performances du réseau, réduire les coûts, améliorer la sécurité et assurer une gestion simplifiée de projets et d'applications.

• Afin de gérer les ressources du réseau de manière simple et centralisée il nous faudra également l'Active Directory.

• Nous devons mettre en place une zone démilitarisée DMZ afin de minimiser les dommages au réseau protégé interne au cas où un de ces serveurs serait compromis.

• Enfin, nous utilisons le Clustering afin d'assurer une disponibilité et une stabilité élevées des ressources publiées, atteignant quasiment 100, tout en garantissant une absence totale de défaillances matérielles ou logicielles.

3.3.2 Contraintes

En réalisant les améliorations proposées pour remédier le réseau de BMT, nous devons assurer la continuité des services du réseau et répondre aux besoins des utilisateurs pendant et après la mise en place du projet. Les performances du réseau ne doivent pas non plus être altérées, En outre l'utilisateur ne doit pas être au courant des modifications apportées au réseau.

3.3.3 Cahier des charges

• Transformer l'architecture de BMT en modèle hiérarchique afin de facilité son administration, ce dernier est un outil pour la conception d'une infrastructure de réseau fiable et organisée, divisé en couches distinctes chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau local

— Couche d'accès : C'est le point d'entrée qui permet à un utilisateur final d'accéder aux périphériques réseau.

— Couche de distribution ou agrégation : Fournit une connectivité basée sur des règles ou politiques d'accès pour assurer la segmentation du réseau, elle comporte des routeurs ou des switchs de niveau 3.

— Couche cœur de réseau : Le cœur de réseau étant un élément essentiel pour la connectivité, comporte des équipements de hautes performances, il doit fournir une disponibilité élevée et s'adapter très rapidement aux changements et commuter les paquets le plus rapidement possible et interconnecter les différents composants de l'infrastructure.

• Mise en place d'un serveur Active directory qui est un service d'annuaire [1] créé par Microsoft en 1996 et destiné à être installé sur les Windows Server 2000, 2003, 2008, 2012 et 2016. En stockant dans une base de données les renseignements relatifs aux ressources réseau d'un domaine, Active Directory a pour premier objectif de centraliser l'identification et l'authentification d'un réseau de postes Windows. Ses fonctions additionnelles permettent aux administrateurs de gérer efficacement une stratégie de groupe, ainsi que l'installation des logiciels et des mises à jour sur les stations du réseau.
Le rôle de base d'AD a été regrouper tous les objets dans un arbre dont :

— La racine est le domaine (DNS).

— Les branches sont les unités d'organisation (pas d'objets).

— Les feuilles sont les objets (utilisateurs, groupes, ordinateurs, etc.).

• Segmenter le réseau en VLANs pour alléger et assurer la fluidité du réseau, un VLAN est un réseau local regroupant un ensemble de stations de façon logique et non physique, Ces stations pourront communiquer comme si elles étaient sur le même segment. La technologie VLAN apporte de nouvelles solutions dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances.

Les VLANs différent selon les informations utilisées pour regrouper les stations. Il en existe généralement quatre modèles, respectivement basés sur le port, sur l'adresse Mac, sur le protocole et l'adresse réseau.

Parmi les protocoles utilisés nous trouvons le VTP (Virtual Private Network) qui est un protocole de niveau deux (2) utilisé pour configurer et administrer les VLAN sur les périphériques, Il permet d'ajouter, renommer ou supprimer un ou plusieurs VLANs sur le seul Switch maître et dans un domaine VTP. Celui-ci propagera la modification de la configuration aux Switchs clients du réseau.

Les VLANs sont distribués sur différents équipements via des liaisons dédiées entre-eux appelées trunk. [2], la configuration de lien Trunk s'effectue sur les liens entre Switchs.

Il existe plusieurs types de VLAN selon le critère de commutation tels que le VLAN utilisateur ou de données, VLAN de gestion qui est utilisé pour accéder à l'interface utilisateur de gestion du commutateur, VLAN native qui est le vlan dans lequel sont véhiculées les trames non taguées dot1q et VLAN voice qui prend en charge la voix IP.

• Utilisation de la technologie de clustering pour assurer la haute disponibilité et une tolérance zéro pour les pannes matérielles ou logicielles. Le cluster est un ensemble de moyens de calcul interconnectés qui pourra réaliser des opérations communes (parallèles) en utilisant des logiciels standards et si possible OpenSource.

• Mettre en place une zone démilitarisée DMZ pour permettre à une entreprise d'accéder à des réseaux non sécurisés, tels qu'Internet, tout en garantissant la sécurité de son réseau privé ou LAN, Une zone démilitarisée (DMZ) est un réseau périphérique qui protège le réseau local (LAN) interne d'une organisation contre le trafic non sécurisé.

3.3.4 Architecture proposée pour le réseau de BMT

Nous pouvons regrouper les améliorations proposées dans la figure 3.1 comme suit :

1. Un annuaire permet de stocker des données légèrement typées, organisées selon des classes particulières et présentées dans un arbre
2. Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels

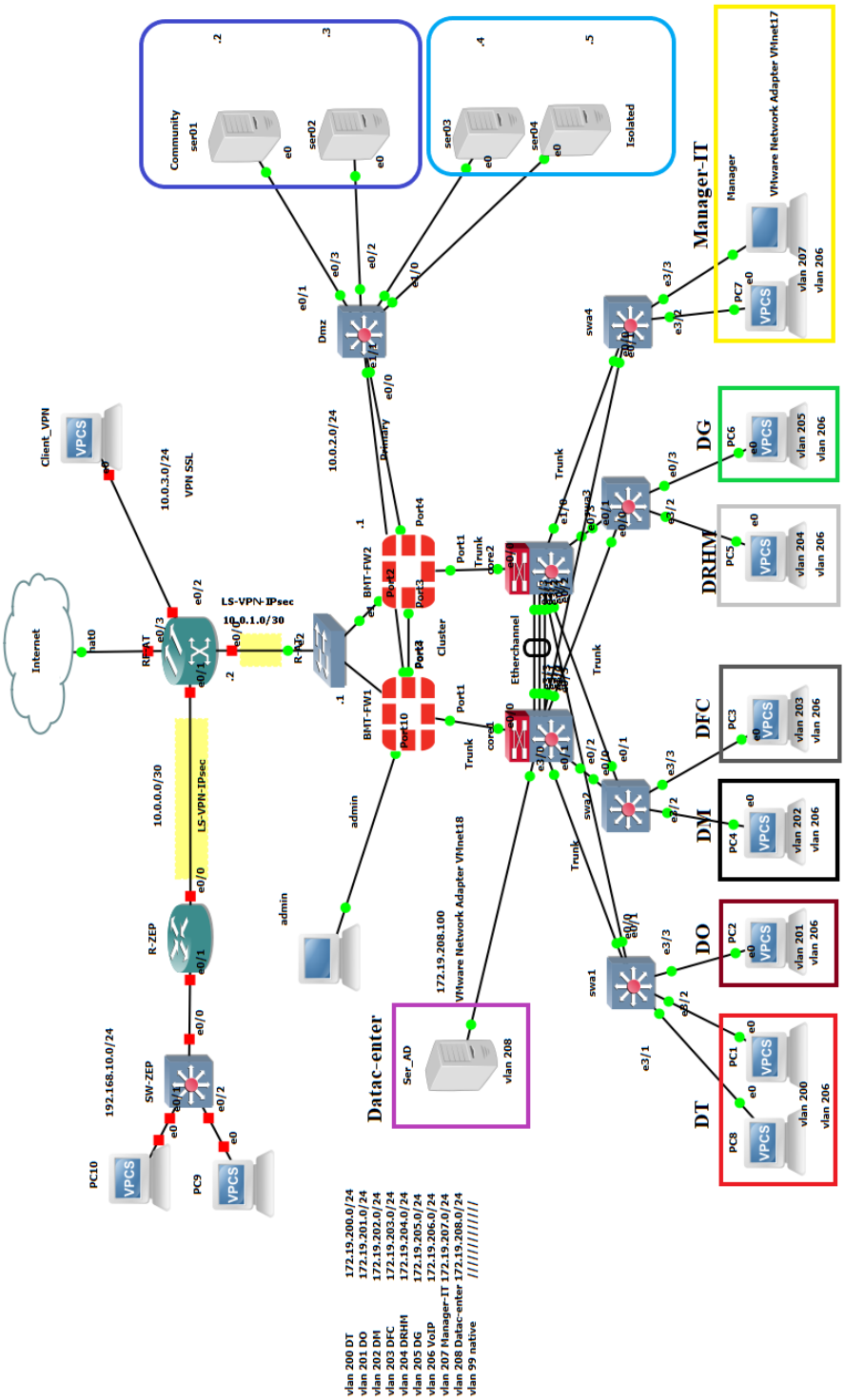

FIGURE 3.1 – Architecture proposée pour le réseau de BMT.

Dans cette configuration, nous pouvons observer la transformation d'une architecture physique en une architecture hiérarchique, cela signifie le passage d'une structure basée sur des composants matériels vers une structure organisée en couches ou en niveaux avec des rôles et des responsabilités clairement définis à chaque niveau. Cette architecture est composée de deux niveaux : la couche cœur et la couche de distribution combinée, ainsi qu'une couche d'accès.

Pour mettre en place cette architecture réseau, il est nécessaire d'utiliser 4 commutateurs d'accès, auxquels les différents hôtes seront connectés. De plus, 2 commutateurs de niveau cœur exécutent des fonctionnalités de niveau de distribution en assurant une connectivité montante pour les commutateurs de la couche d'accès. La connexion entre les commutateurs de distribution est mise en œuvre via trois liens, sur lesquels nous avons utilisé la technologie EtherChannel pour l'agrégation de liens. Cette technologie permet de regrouper plusieurs liens Ethernet physiques identiques en un seul lien logique.

Pour assurer la segmentation du réseau, nous avons défini dix (10) VLANs répartis comme suit :

1. VLAN DT (Direction Technique) : VLAN 200.
2. VLAN DO (Direction des Opérations) : VLAN 201.
3. VLAN DM (Direction Marketing) : VLAN 202.
4. VLAN DFC (Direction des Finances et Comptabilité) : VLAN 203.
5. VLAN DRHM (Direction des Ressources Humaines et Moyens) : VLAN 204.
6. VLAN DG (Direction Générale) : VLAN 205.
7. VLAN VOIP (Voix IP) : VLAN 206.
8. VLAN Manager-IT : VLAN 207.
9. VLAN Data center : VLAN 208.
10. VLAN Native : VLAN 99.

Chaque direction a été attribuée un VLAN dédié, permettant ainsi de les isoler les uns des autres sur le réseau. De plus, un VLAN Voix IP a été spécifiquement assigné à chacune de ces directions pour gérer les communications vocales. Cette segmentation par VLANs permet de mieux organiser le réseau en fonction des différentes entités et de garantir une gestion efficace des flux de données.

Dans cette topologie, nous avons mis en évidence la présence de deux pare-feu Fortigate au niveau de notre site principal. Cette redondance vise à assurer une haute disponibilité, et pour renforcer cette fiabilité, nous avons mis en place un clustering entre les deux pare-feu Fortigate.

Pour accéder à l'interface graphique de nos pare-feu, nous avons configuré une machine virtuelle sous Windows 10 avec le navigateur Firefox.

Dans le but de garantir une protection contre les pannes et la perte de données, ainsi que de simplifier la gestion des ressources réseau, nous avons mis en place un serveur d'annuaire actif (Active Directory).

Nous avons créé un domaine appelé "bmt.local" pour garantir la sécurité, la redondance et la mise à jour des objets de nos données.

En vue de renforcer la sécurité, nous avons également créé une zone démilitarisée (DMZ) avec un VLAN privé. Ce VLAN se compose d'un VLAN principal et d'un VLAN secondaire. Le VLAN secondaire comprend deux serveurs isolés, où les membres de ce VLAN ne peuvent pas communiquer entre eux. De plus, nous avons configuré deux autres serveurs dans un VLAN communautaire, permettant aux membres de ce VLAN de communiquer entre eux.

3.4 Conclusion

Au cours de ce chapitre, nous avons examiné en profondeur les solutions destinées à améliorer l'architecture de sécurité existante chez BMT et à résoudre les problèmes identifiés. Nous avons rigoureusement examiné et analysé les défis spécifiques auxquels l'entreprise est confrontée et proposé des mesures adaptées pour renforcer la sécurité de son infrastructure.

Dans le prochain chapitre, nous détaillerons les simulateurs utilisés ainsi que les configurations requises pour mettre en œuvre ces solutions. Nous présenterons également les tests et les vérifications réalisés pour évaluer l'efficacité de l'architecture de sécurité améliorée.

CHAPITRE 4

MISE EN OEUVRE DE LA SOLUTION

4.1 Introduction

Dans ce chapitre, nous abordons la dernière étape essentielle qui est la mise en œuvre. Cette phase revêt une grande importance pour concrétiser les solutions préalablement proposées. Nous débutons par une présentation des simulateurs utilisés, suivi de la description détaillée des configurations nécessaires à mettre en place sur le réseau de BMT. Enfin, nous procédons à des tests et des vérifications rigoureuses afin de confirmer le bon fonctionnement de toutes les configurations mises en œuvre.

4.2 Présentation de l'environnement de travail

L'environnement de travail désigne l'ensemble de conditions matérielles et humaines qui composent le cadre du travail.

4.2.1 Partie hardware

• Les équipements utilisés dans l'architecture ce sont des équipements existant dans l'entreprise.

4.2.2 Partie software

Présentation du simulateur GNS 3 (Graphical Network Simulator)

GNS3 est un émulateur de matériel réseau, il est la suite logique de Packet Tracer. Contrairement aux autres émulateurs GNS 3 utilise un véritable IOS entièrement fonctionnel. On y retrouve toutes les commandes réelles du matériel, mais surtout il donne la possibilité de mettre ses éléments (virtuels) dans le même réseau que les équipements réels de notre réseau (Machines, Switch, téléphones IP, etc.).

Présentation de VMWARE

VMware Workstation est une solution logicielle professionnelle, puissante et complète qui vous permet de gérer toutes les machines virtuelles localement ou sur le réseau. C'est la solution de virtualisation ultime pour émuler et gérer plusieurs systèmes d'exploitation (la version utiliser est 17).

Windows server 2022

Windows Server 2022 est une version du système d'exploitation Microsoft destiné aux serveurs, sortie en août 2021. Le système offre une sécurité multicouche avancée et une plateforme d'application flexible.

Windows 10

Windows 10 est un système d'exploitation de Microsoft sorti le 29 juillet 2015. Il succède à Windows 7 et Windows 8.1. Cette nouvelle version introduit plusieurs changements importants. Tout d'abord, elle est la première à fonctionner sur toutes les plateformes existantes : ordinateurs de bureau et portables, smartphones, tablettes et montres connectées. L'interface de l'OS s'adapte automatiquement au format et au mode de saisie (tactile ou bien clavier et souris).

4.3 Configuration d'Active Directory

La première étape consiste à configurer le nom de la machine et l'@ IPv4 du serveur local (Voir Figure 4.1).

- Nom de la machine est SER-AD1.
- L'adresse IPv4 c'est une adresse statique de classe C : 172.19.208.100.

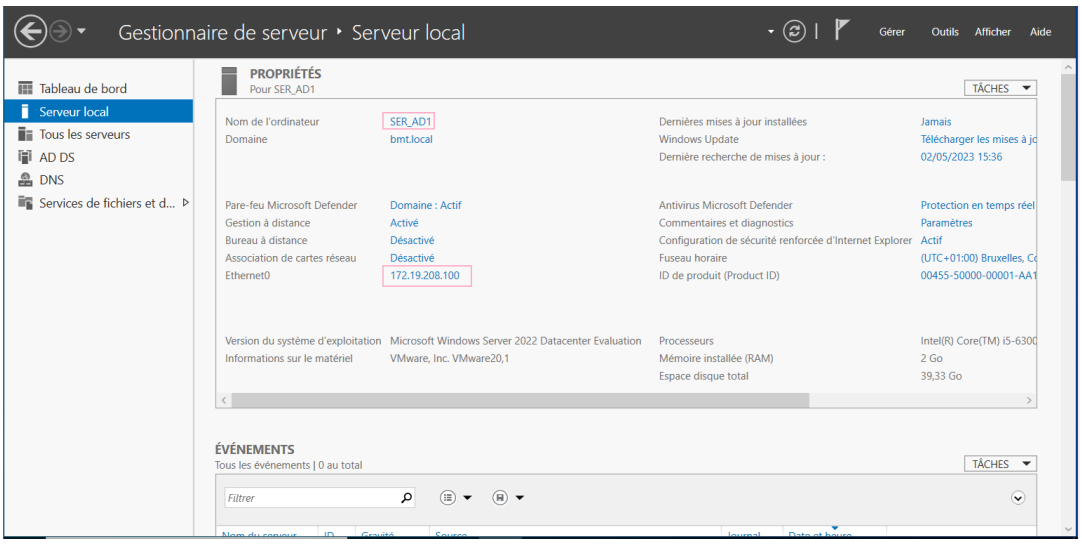

FIGURE 4.1 – Configuration du serveur local.

La deuxième étape comprend l'ajout du rôle d'Active Directory au serveur local, pour cela nous allons suivre les étapes suivantes : (Voir Figure 4.2)

- Depuis le gestionnaire de serveur, cliquer sur ajouter des rôles et fonctionnalités.
- Sélectionner le type d'installation " installation basée sur un rôle ou fonctionnalité ".
- Notre serveur et le seul du réseau, le choisir dans le pool de serveurs.
- Cocher le rôle service AD DS (Active Directory Domain Service).

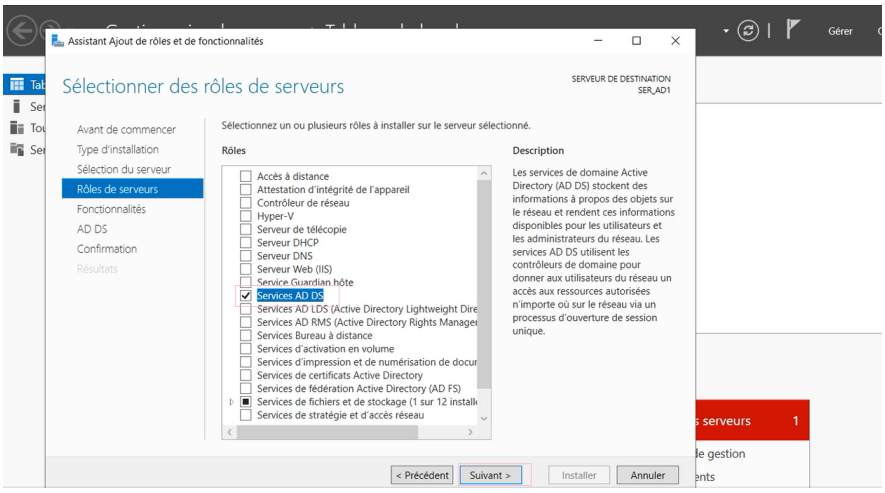

FIGURE 4.2 – Ajout du rôle AD DS.

Après l'installation d'Active Directory Domain Service, le système va redémarrer automatiquement.

Dans la troisième étape, nous devons promouvoir ce serveur en tant que contrôleur de domaine sinon le domaine ne sera pas créé (Voir la Figure 4.3).

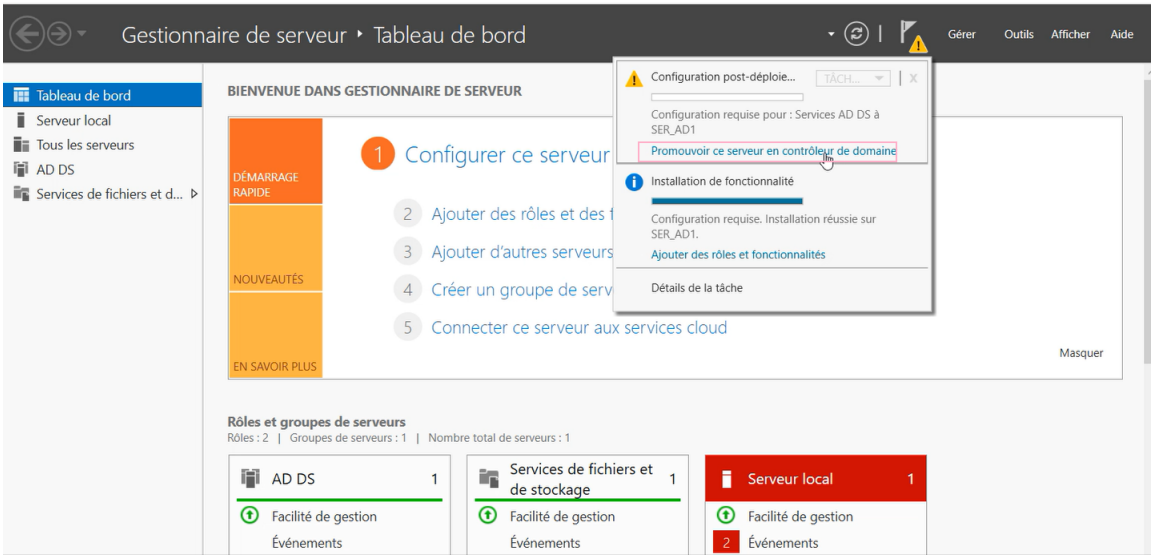

FIGURE 4.3 – Promouvoir le serveur en contrôleur de domaine.

Après avoir cliqué sur "promouvoir ce serveur en contrôleur de domaine ", l'assistant nous demande de créer une nouvelle forêt sous le nom "bmt.local "(Voir la Figure 4.4).

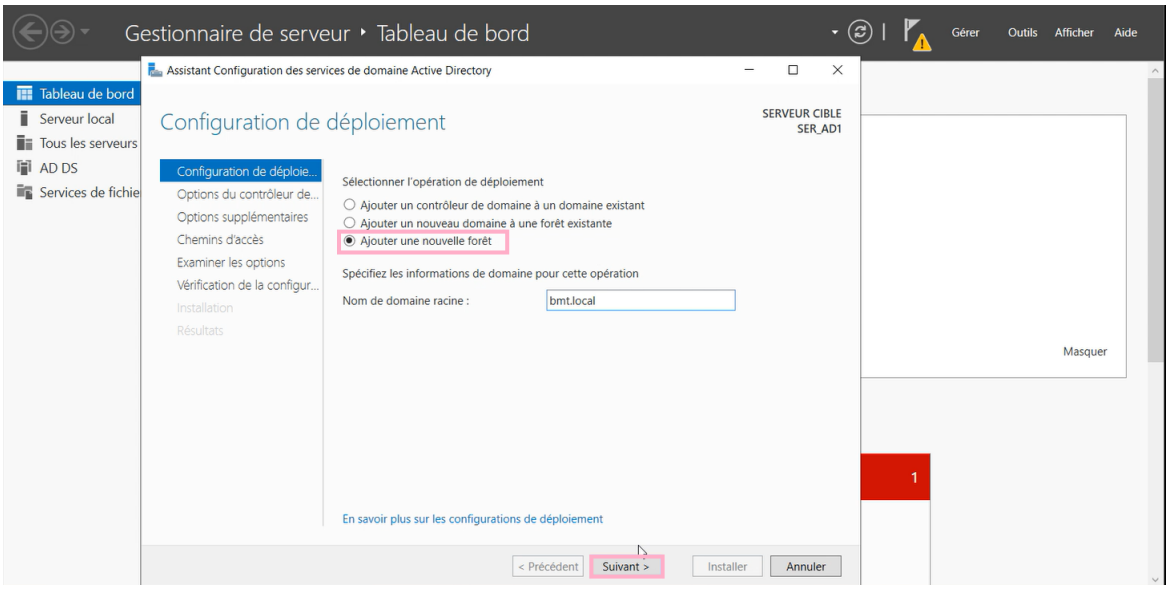

FIGURE 4.4 – Ajout d'une nouvelle forêt.

Lorsque la forêt et le domaine seront créés, le niveau fonctionnel de la nouvelle forêt est sélectionné par défaut, et nous laissons cocher l'ajout de la fonctionnalité du serveur DNS. Puis, insérer le mot de passe du mode de restauration du service d'annuaire (Voir la Figure 4.5).

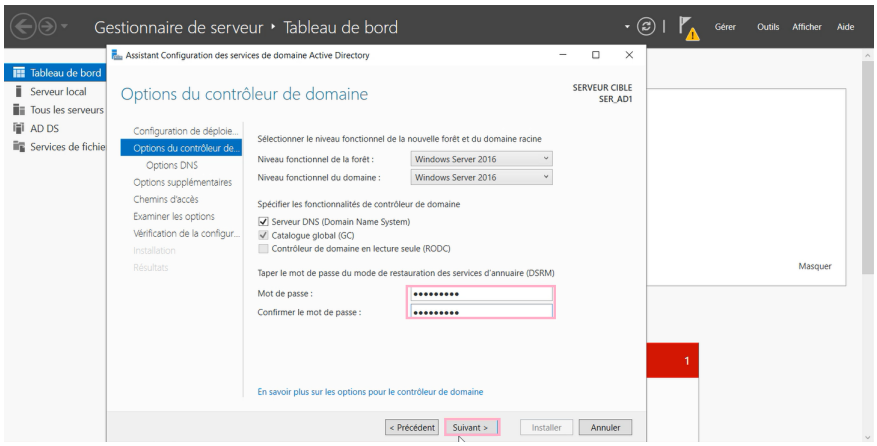

FIGURE 4.5 – Options de contrôleur de domaine.

Une erreur apparaît sur l'écran suivant, ce message survient car aucun serveur DNS n'est installé sur la machine, nous cliquons simplement sur suivant pour le créer automatiquement, car c'est grâce à lui que les clients (postes utilisateurs ou serveurs membres du domaine) vont pouvoir trouver le serveur AD.

Après la configuration, le serveur redémarre automatiquement. À présent, les outils de gestion d'Active Directory sont présents dans le menu outils, notre domaine est crée et l'ouverture d'une

session s'effectue avec le compte d'administrateur du domaine BMT/Administrateur comme la figure 4.6 l'illustre.

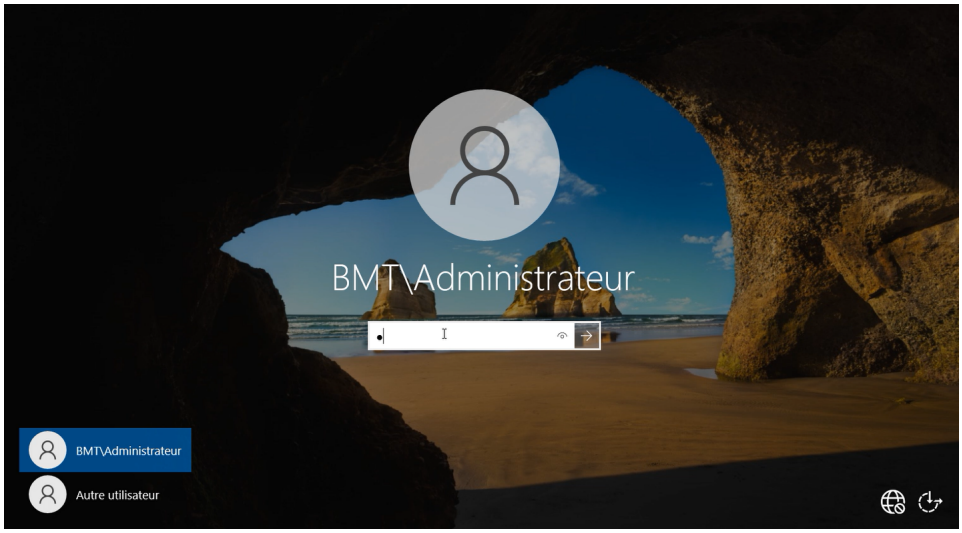

FIGURE 4.6 – Ouverture de la session Administrateur.

Organisation des clients AD en unités organisationnelle

Nous allons commencer à peupler notre Active Directory. Pour ce faire, nous devons lancer la console Utilisateur et ordinateur Active Directory. Nous pouvons la lancer depuis le gestionnaire de serveur puis sous la rubrique AD DS.

Nous allons créer une unité organisationnelle afin d'y mettre l'ensemble des utilisateurs et groupes, pour cela on se place dans l'arbre à la hauteur de notre domaine "bmt.local" et sur le menu, nous choisissons l'option Unité d'organisation (Voir la Figure 4.7).

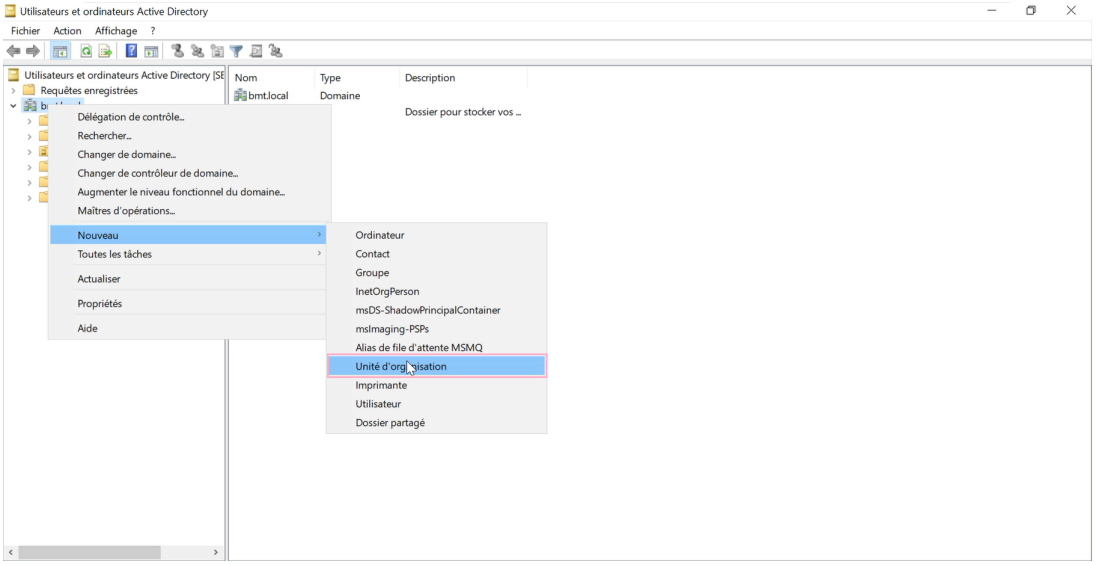

FIGURE 4.7 – Création d'une unité d'organisation.

Cette procédure nous permet de regrouper des ordinateurs ou des utilisateurs dans une seule unité

afin de pouvoir leur appliquer des procédures et des stratégies des groupes. Après avoir créé les unités organisationnelles relatives à notre entreprise, nous pouvons créer les premiers utilisateurs et commencer à peupler nos unités. Nous répétons la même procédure pour tous les nouveaux utilisateurs (Voir la Figure 4.8).

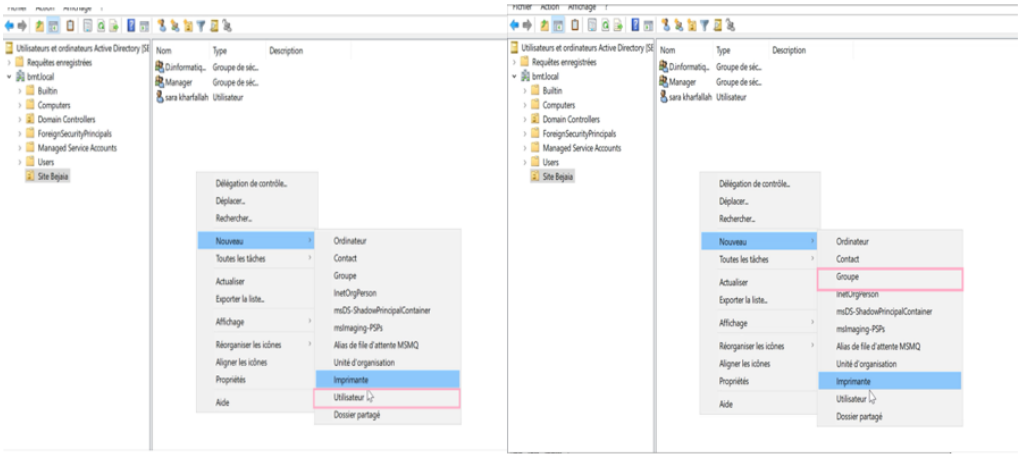

FIGURE 4.8 – Ajout des utilisateurs et groupes.

• Chaque utilisateur aura un compte avec un identifiant unique de la forme N.prenom@bmt.local et un mot de passe (Voir la Figure 4.9).

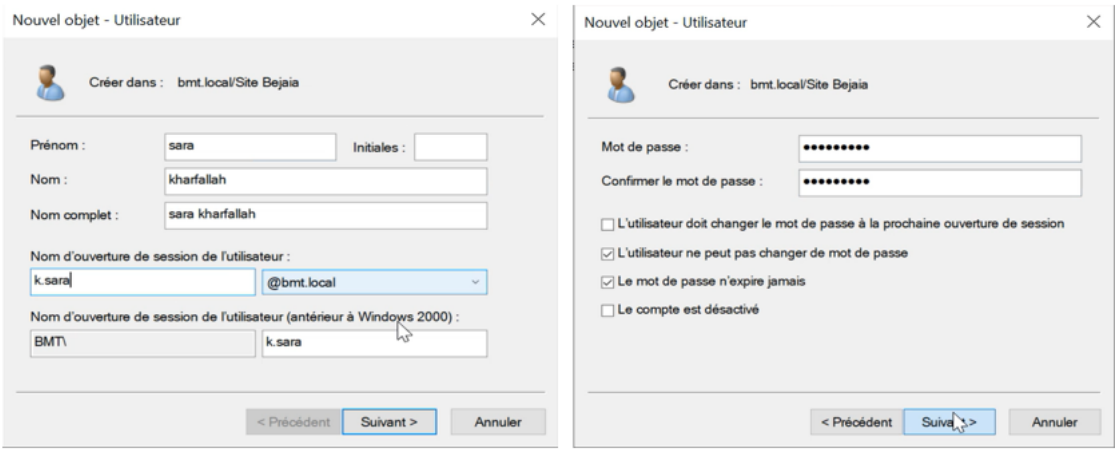

FIGURE 4.9 – Création des sessions utilisateur.

• Chaque département aura son propre groupe avec un identifiant unique de la forme qui est son nom en lui même (Voir la Figure 4.10).

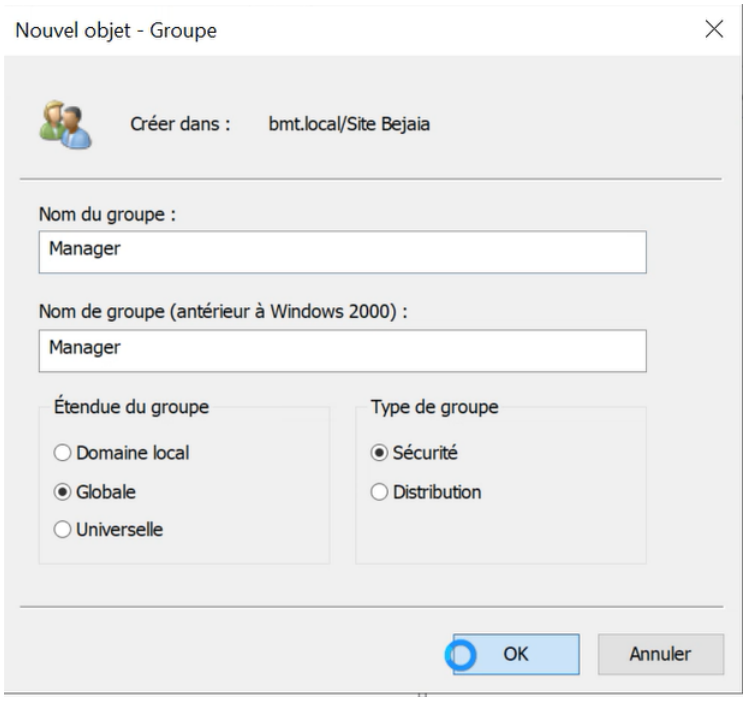

FIGURE 4.10 – Forme du groupe.

• Chaque employé doit être affecté à son département "chaque utilisateur a son groupe" (Voir la Figure 4.11).

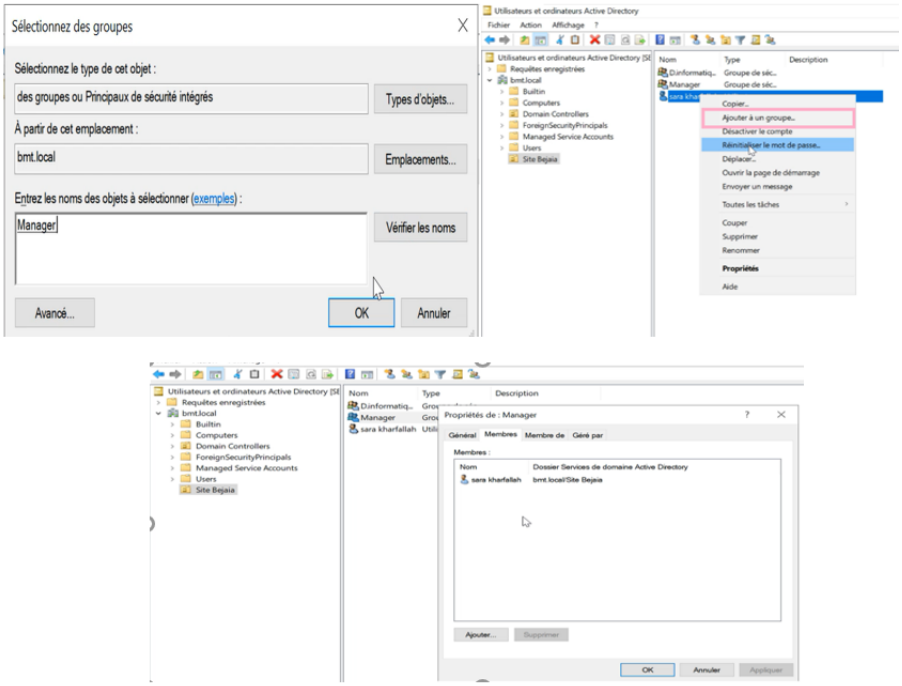

FIGURE 4.11 – Ajout d'un utilisateur a un groupe.

Mise en œuvre des Group Policy Organisation (GPO)

Les stratégies de groupe sont des outils de configuration permettant de modifier un ensemble de paramètres s'appliquant à des configurations utilisateur ou à des configurations ordinateur membres d'un domaine Active Directory (AD DS), ils présentent plusieurs avantages dont : la réduction des coûts, le contrôle des configurations, la conservation des utilisateurs productifs, le renforcement de la sécurité et la gestion des droits d'accès aux ressources.

Après avoir installé Active Directory, mis en place notre domaine dans une nouvelle forêt et crée nos unités d'organisation, nous allons mettre en place nos GPO.

La première étape consiste à modifier le "default domaine Policy" dans le menu" Gestion de stratégie de groupe" celle-ci représente la GPO par défaut de notre domaine, il suffit de faire un clic droit et de modifier (Voir la Figure 4.12).

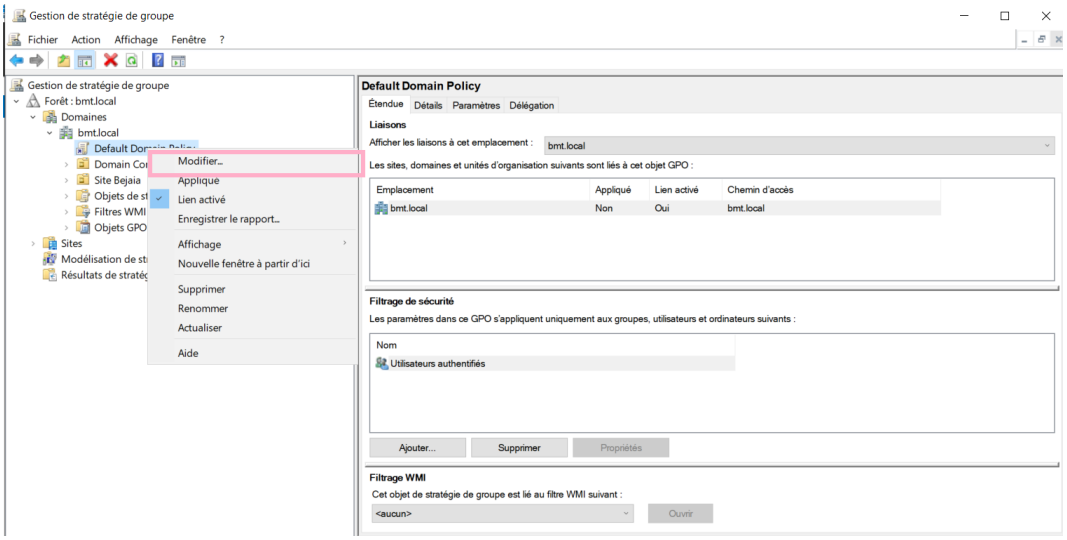

FIGURE 4.12 – Modification de la stratégie de groupe par défaut.

La stratégie des groupes n'est pas applicable pour tout le monde juste pour les concerné, pour cela on doit créer des nouvelles stratégies pour les utilisateurs ainsi pour ordinateurs.

Pour les crées, nous allons sur le menu" Gestion de stratégie de groupe" , clic droit puis nous choisissons "nouveau" (Voir la Figure 4.13).

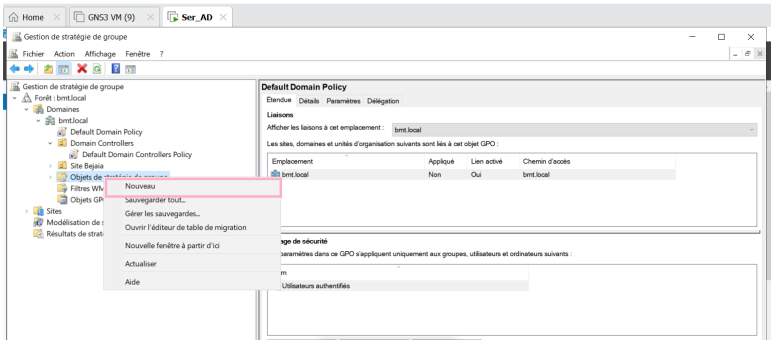

FIGURE 4.13 – Création d'un nouveau GPO.

Dans la figure 4.14, nous illustrons la nomination de chaque stratégie .

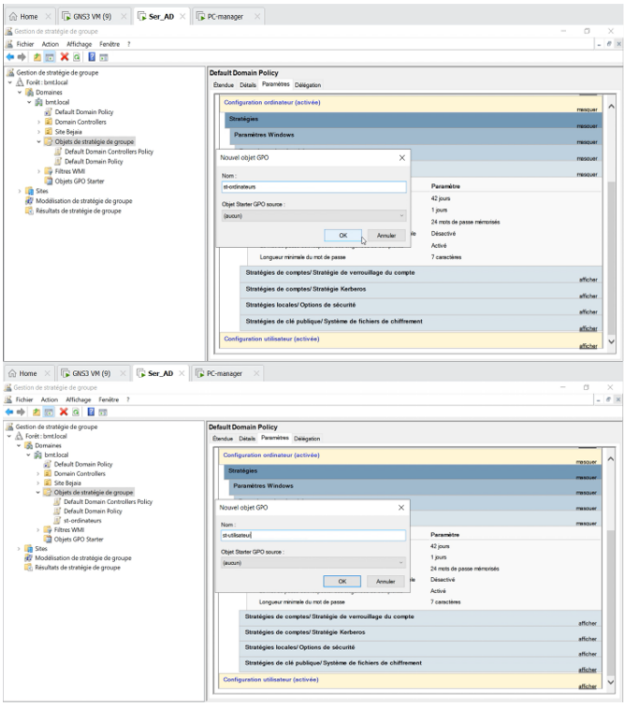

FIGURE 4.14 – Nomination des stratégies.

Pour la configuration des stratégies elle fait comme suit :

• La configuration ordinateur s'applique au démarrage et est valable pour tous les utilisateurs qui ouvrent une session.

• La configuration utilisateur s'applique à l'ouverture de session et "suit" l'utilisateur quelque soit l'ordinateur sur lequel il se connecte (Voir la Figure 4.15).

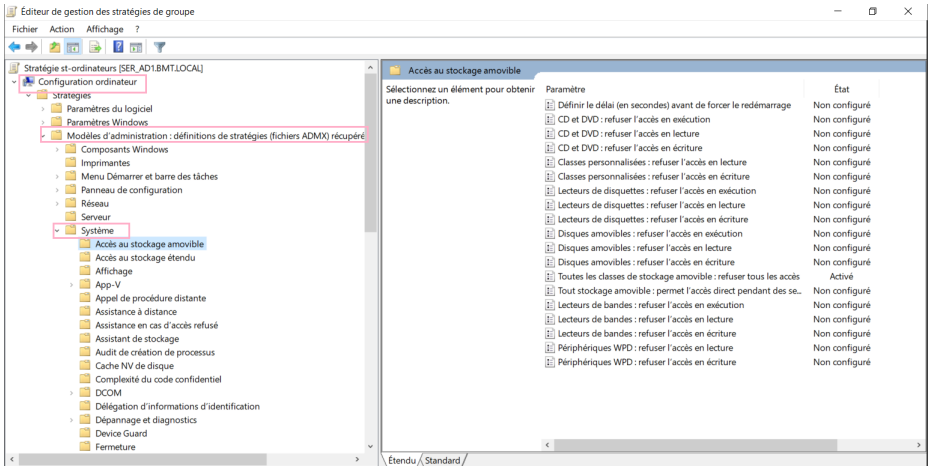

FIGURE 4.15 – Configuration d'une GPO.

Nous pouvons faire différents paramétrages liés aux utilisateurs et aux ordinateurs, comme interdire

l'accès au panneau de configuration, interdire la suppression des imprimantes, désactivé les disques amovibles et bien d'autres.

4.4 Configuration et création des VLANs

Les performances réseau jouent un rôle crucial dans la productivité des entreprises. L'une des technologies permettant d'améliorer ces performances est la segmentation des vastes domaines de diffusion en domaines plus petits. Dans un réseau commuté, les VLAN (Virtual Local Area Networks) offrent une solution pour cette segmentation, ce qui permet ainsi une flexibilité dans l'organisation du réseau. Les VLAN regroupent des périphériques au sein d'un même LAN, leur permettant de communiquer comme s'ils étaient connectés au même câble. Contrairement aux connexions physiques, les VLAN reposent sur des connexions logiques.

4.4.1 Plan d'adressage des VLANs

Le tableau suivant illustre les noms et les adresses affecter au VLANs

Nom du VLAN	**ID du VLAN**	**Adresse IP**	**Masque**
VLAN 200 DT	200	172.19.200.0	255.255.255.0
VLAN 201 DO	201	172.19.201.0	255.255.255.0
VLAN 202 DM	202	172.19.202.0	255.255.255.0
VLAN 203 DFC	203	172.19.203.0	255.255.255.0
VLAN 204 DRHM	204	172.19.204.0	255.255.255.0
VLAN 205 DG	205	172.19.205.0	255.255.255.0
VLAN 206 VOIP	206	172.19.206.0	255.255.255.0
VLAN 207 Manager-IT	207	172.19.207.0	255.255.255.0
VLAN 208 Data-Center	208	172.19.208.0	255.255.255.0
VLAN native	99	/////	/////

TABLE 4.1 – Plan d'adressage des VLANs.

4.4.2 Configuration du mode trunks

Les interfaces des équipements d'interconnexion à configurer en mode trunk, sont toutes les interfaces existantes entre l'ensemble des commutateurs distributions-accès et distributions-cœur.

4.4.2.1 Configuration des liens Trunks au niveau de la couche cœur

Les liens trunks au niveau de la couche coeur sont configurées comme le montre la Figure 4.16.

```
core1(config)#interface  range ethernet 3/1-3, ethernet 0/1-3, ethernet  1/0
core1(config-if-range)#swt
core1(config-if-range)#sw
core1(config-if-range)#switchport t
core1(config-if-range)#switchport trunk en
core1(config-if-range)#switchport trunk encapsulation do
core1(config-if-range)#switchport trunk encapsulation dot1q
core1(config-if-range)#sw
```

```
core1(config-if-range)#switchport trunk native vlan 99
core1(config-if-range)#sw
core1(config-if-range)#switchport all
core1(config-if-range)#switchport t
core1(config-if-range)#switchport trunk all
core1(config-if-range)#switchport trunk allowed vl
core1(config-if-range)#switchport trunk allowed vlan 200-208,99
core1(config-if-range)#end
core1#
core1#
core1#wr
```

FIGURE 4.16 – Configuration des liens Trunks au niveau du switch cœur "core1".

4.4.2.2 Configuration des liens Trunks au niveau de la couche d'accès

Les liens trunks au niveau de la couche d'accès sont configurés comme le montre la Figure 4.17.

```
swa2(config-if-range)#switchport trunk encapsulation dot1q
swa2(config-if-range)#sw
swa2(config-if-range)#switchport mo
swa2(config-if-range)#switchport mode  tr
swa2(config-if-range)#switchport mode  trunk
swa2(config-if-range)#sw
swa2(config-if-range)#switchport tr
swa2(config-if-range)#switchport trunk n
swa2(config-if-range)#switchport trunk native vl
swa2(config-if-range)#switchport trunk native vlan  99
swa2(config-if-range)#sw
```

```
swa2(config-if-range)#switchport trunk allowed vlan 200-208,99
swa2(config-if-range)#
swa2(config-if-range)#end
swa2#
swa2#wr
```

FIGURE 4.17 – Configuration des liens Trunks au niveau du switch d'accès"swa2".

4.4.3 Configuration d'EtherChannel

Nous avons configuré l'etherChannel en ajoutant toutes les interfaces qui doivent composer notre lien logique dans le même channel-group. Nous avons créé un lien logique entre les deux switchs coeurs et nous avons configuré etherChannel en mode ON sur les deux switch core (Voir la Figure 4.18).

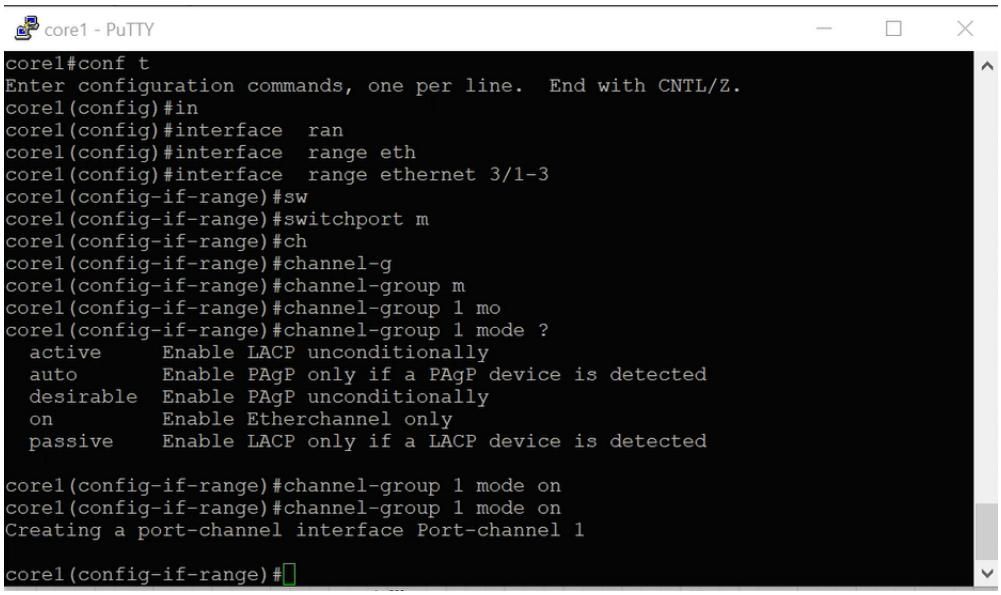

FIGURE 4.18 – Configuration d'EtherChannel sur le switch "core1".

4.4.4 Configuration du protocole VTP

4.4.4.1 Configuration du serveur VTP

Le mode serveur VTP sera réalisé au niveau des deux switchs coeurs (Voir Figure4.19).

```
core1(config)#vtp mode server
Device mode already VTP Server for VLANS.
core1(config)#vtp dom
core1(config)#vtp domain bmt?
WORD

core1(config)#vtp domain bmt.vpt
Changing VTP domain name from NULL to bmt.vpt
core1(config)#vtp domain bmt.vtp
Changing VTP domain name from bmt.vpt to bmt.vtp
core1(config)#
core1(config)#
core1(config)#
core1(config)#vtp pass
core1(config)#vtp password bmt06
Setting device VTP password to bmt06
core1(config)#vtp ve
core1(config)#vtp version 2
core1(config)#vtp pru
core1(config)#vtp pruning
Pruning switched on
```

FIGURE 4.19 – Configuration du serveur VTP.

4.4.4.2 Configuration du client VTP

Nous avons associé aussi le mode Client pour tous les switchs de la couche accès (Voir Figure 4.20).

```
swa1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
swa1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
swa1(config)#vtp password bmt06
Setting device VTP password to bmt06
swa1(config)#vtp domain bmt.vtp
Changing VTP domain name from bmt.vpt to bmt.vtp
swa1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
swa1(config)#do wr
Building configuration...
Compressed configuration from 1632 bytes to 967 bytes[OK]
```

FIGURE 4.20 – Configuration du client VTP.

4.4.5 Création des VLANs

La création des VLANs est faite au niveau du switch coeur du réseau (Voir Figure 4.21).

```
core1(config)#vlan 200
core1(config-vlan)#
*May  2 14:34:29.453: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch d
ed on Ethernet1/0 (99), with Dist4 Ethernet0/1 (1).
core1(config-vlan)#name DT
core1(config-vlan)#vlan 201
core1(config-vlan)#name DO
core1(config-vlan)#vlan 202
core1(config-vlan)#name DM
core1(config-vlan)#vlan 203
core1(config-vlan)#name DFC
core1(config-vlan)#vlan 204
core1(config-vlan)#name DRHM
core1(config-vlan)#vlan 205
core1(config-vlan)#name DG
core1(config-vlan)#vlan 206
core1(config-vlan)#
*May  2 14:35:24.330: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch d
ed on Ethernet1/0 (99), with Dist4 Ethernet0/1 (1).
core1(config-vlan)#name VoIP
core1(config-vlan)#vlan 207
core1(config-vlan)#name ManagerIT
core1(config-vlan)#vlan 208
core1(config-vlan)#name Data_center
core1(config-vlan)#vlan 99
core1(config-vlan)#name native
core1(config-vlan)#
core1(config-vlan)#END
core1#
core1#
core1#WR
Building configuration...
Compressed configuration from 2374 bytes to 1195 bytes[OK]
```

FIGURE 4.21 – Création des VLANs.

4.4.6 Affectation des ports aux VLANs

L'affectation des ports aux VLANs se fait au niveau des switchs d'accès.
Nous avons affecté pour chaque port un VLAN data ainsi qu'un VLAN voice (Voir Figure 4.22).

```
swal(config)#interface  ethernet 3/3
swal(config-if)#switchport mode access
swal(config-if)#switchport access vlan 201
swal(config-if)#switchport voice vlan 206
swal(config-if)#
swal(config-if)#end
swal#
swal#
swal#wr
Building configuration...
Compressed configuration from 1790 bytes to 1029 bytes[OK]
```

FIGURE 4.22 – Affectation des VLANs 201 et 206 au port fastEhernet 3/3.

4.4.7 Configuration des VLANs

La première étape consiste à attribuer une adresse à l'interface admin : Pour cela nous allons accéder au Panneau de configuration -> Réseau et internet -> connexions réseau, on clique sur admin puis propriété et enfin protocoles internet version 4 (Voir Figure 4.23).

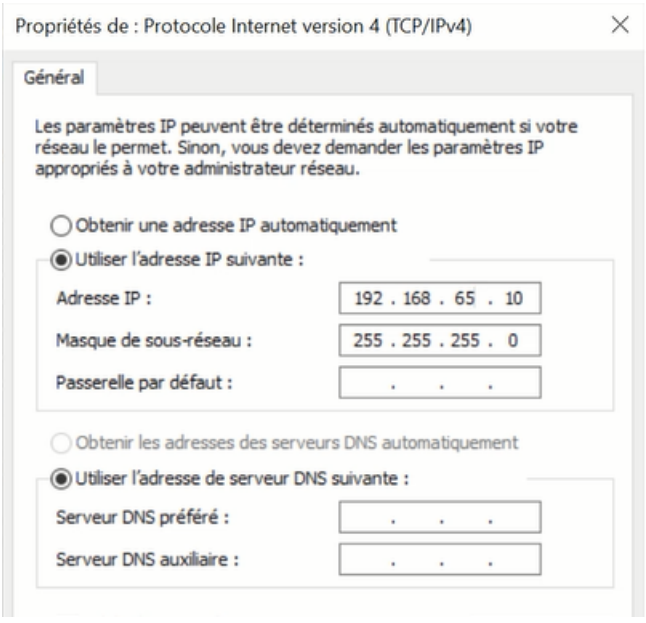

FIGURE 4.23 – Écran de configuration de la carte réseau admin.

La deuxième étape consiste à configurer le pare-feu fortiget en suivant les étapes suivantes : (voir Figure 4.24).

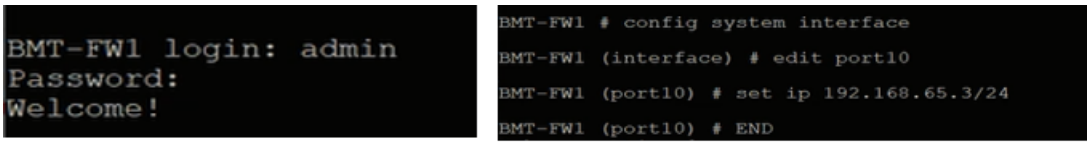

FIGURE 4.24 – Configuration du firewall fortiget.

4.4.8 Routage Inter-VLAN

Nous allons nous connecter au pare-feu via le Web avec l'adresse IP 192.168.65.10, une interface d'authentification s'affichera. Après nous allons introduire le login ainsi que le password (Voir Figure 4.25).

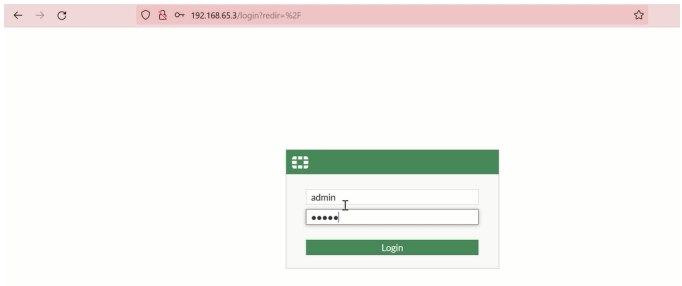

FIGURE 4.25 – Interface d'authentification.

Une fois connecté, on sera placé dans le tableau de bord, puis nous allons accéder à [System Management] -> [Network] -> [Interfaces] et on configure l'interface WAN sur le port 2 (Voir Figure 4.26).

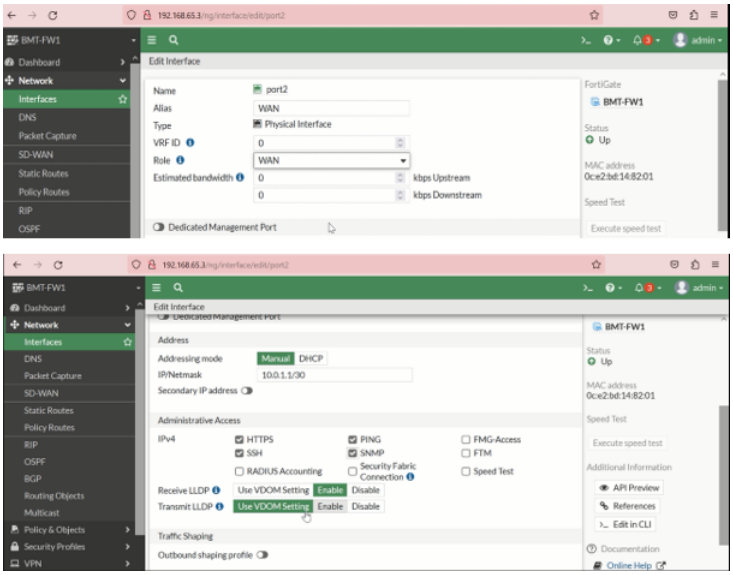

FIGURE 4.26 – Configuration du port 2.

Les interfaces VLANs seront configurées sur le port 1 car c'est l'interface physique sur laquelle nos VLANs sont connectés, elle ne nécessite aucun paramètre d'adresse IP.

Afin de créer des interfaces, on clique sur port1 puis on va créer une interface nommée inter-VLAN (Voir Figure 4.27).

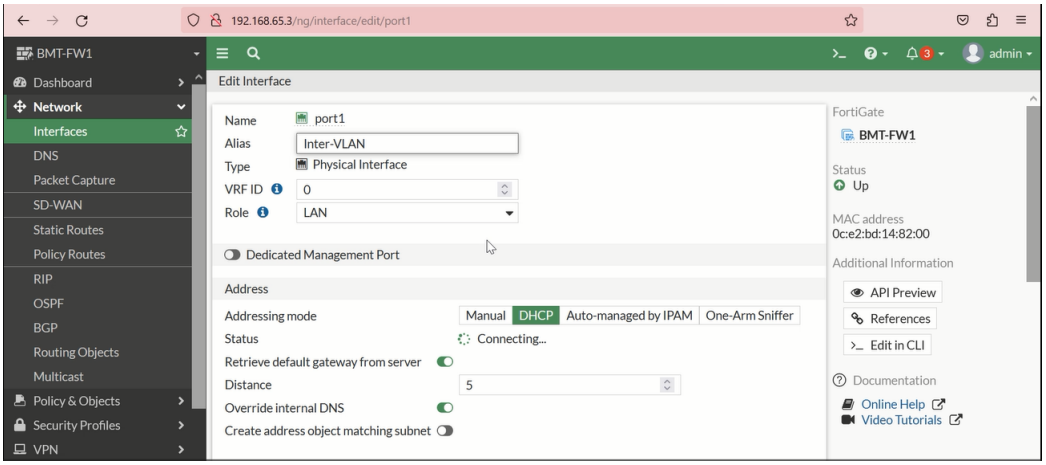

FIGURE 4.27 – Création de l'interface Inter-VLAN.

Dans cette interface nous allons créer des interfaces VLANs, pour cela nous cliquons sur [Create New] puis nous allons afficher la fenêtre de création des interfaces, et remplir les informations suivantes : nom de l'interface, type, interface, ID VLAN, adresse IP/masque de sous-réseau, Accès de gestion et serveur DHCP relay comme illustré sur la figure 4.28.

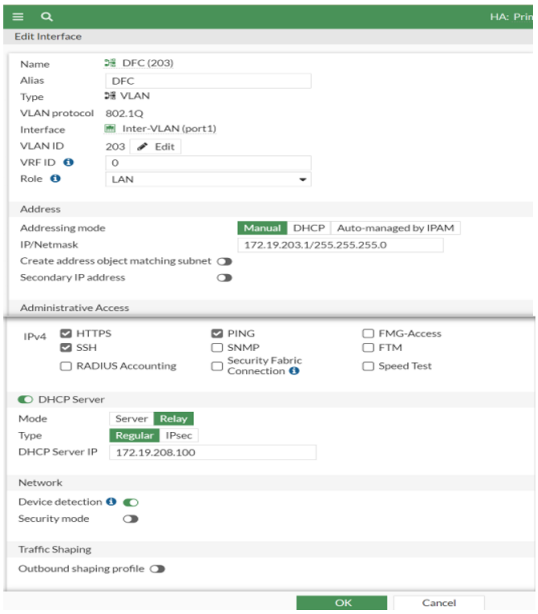

FIGURE 4.28 – Création du VLAN 203.

4.4.8.1 Création d'une zone

La création d'une zone permet de faciliter la gestion et la maintenance des politiques à l'avenir.

Pour cela nous allons sur [Network] -> [Zone], nous cliquons sur "Create New".

Une fois l'interface de création d'une zone apparaît, nous allons introduire le nom puis nous ajoutons les membres de l'interface (VLAN 200, 201, 202, 203, 204, 205, 206, 207 et 208) comme le montre la figure 4.29.

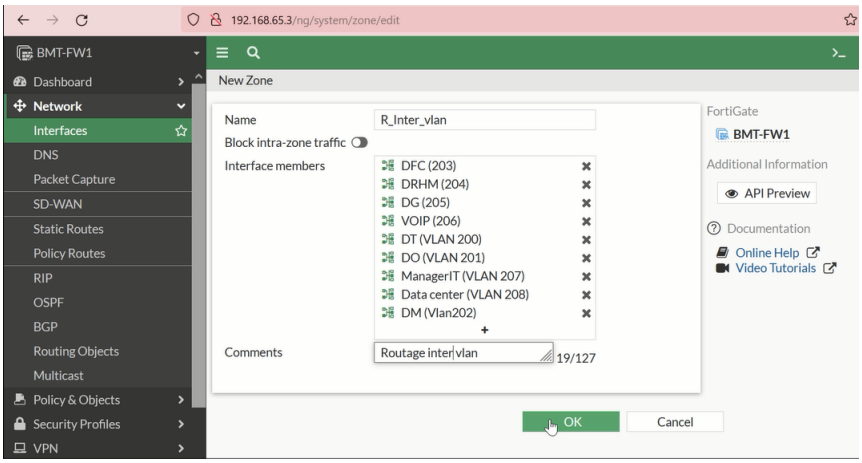

FIGURE 4.29 – Création d'une zone.

4.4.8.2 Routage des VLANs vers Internet

D'abord, nous allons créer une route par défaut vers Internet en allant sur [Static Routes], puis nous cliquons sur "Create New", puis nous allons introduire l'adresse de la passerelle "10.0.1.2" ainsi que l'interface (port2) (Voir Figure 4.30).

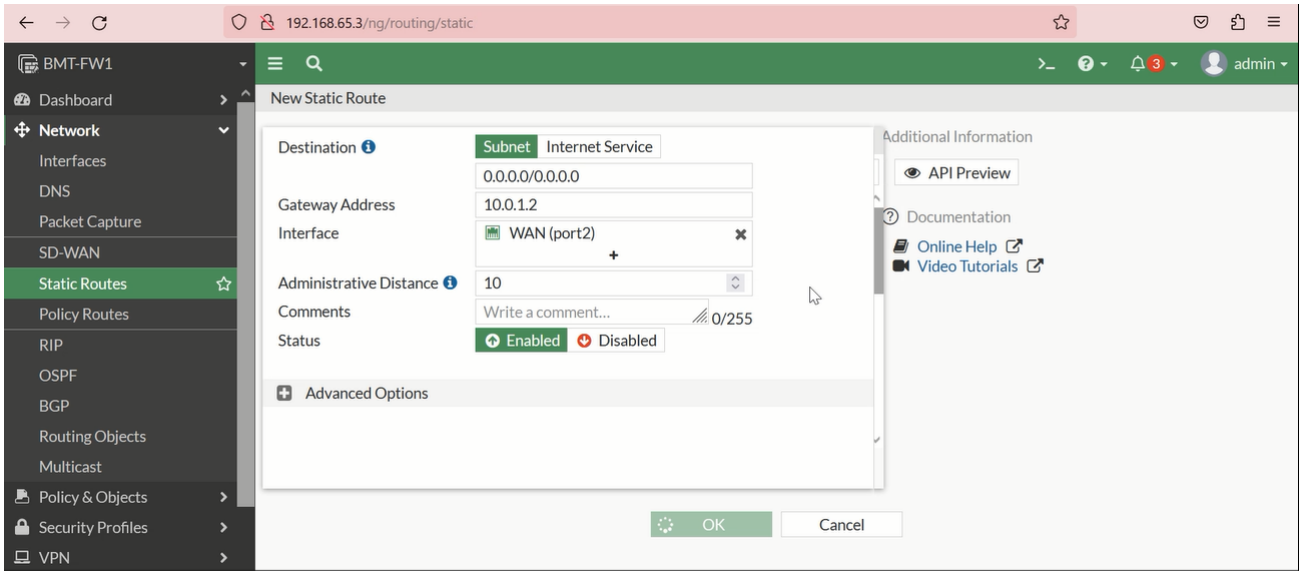

FIGURE 4.30 – Création d'une route par défaut vers internet.

4.4.8.3 Autorisation de la connexion des VLANs vers Internet

Pour configurer l'autorisation de la connexion des VLANs vers internet, nous allons accéder à [Policy and Objects] -> [Firewall Policy], puis nous allons cliquer sur "Create New" puis nous allons introduire le nom, l'interface d'entrée, de sortie, la source, la destination ainsi que les services (Voir Figure 4.31).

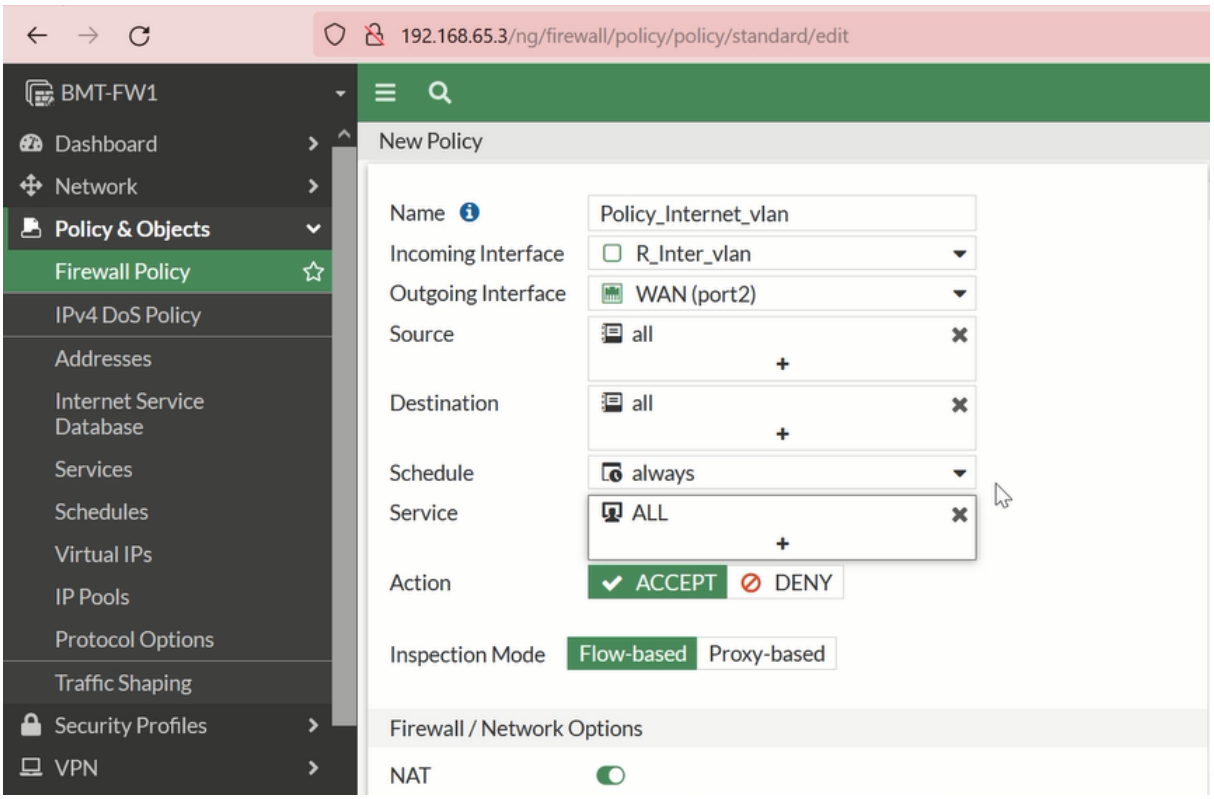

FIGURE 4.31 – Autorisation de la connexion des VLANs vers internet.

4.5 Configuration du Cluster

Nous allons configurer le cluster active-active sur les deux pare-feu FortiGate afin que les charges de travail soient distribuée sur au moins deux nœuds pour préserver la sécurité et la disponibilité de vos données en cas de panne inattendue, le premier firewall va être configuré autant qu'un maître sur l'interface graphique en introduisant des paramètres de priorité supérieurs a celles du deuxième, tandis que le deuxième firewall va être configuré sur l'interface de ligne de commande autant qu'un esclave.

La première étape consiste à configurer le premier firewall en suivant les étapes suivantes :

D'abord nous devons s'authentifier sur l'interface d'authentification de notre firewall en introduisant le login et le password (Voir Figure 4.25).

Puis nous allons dans [Système] -> [HA], et nous allons remplir les champs suivants (Voir Figure 4.32).

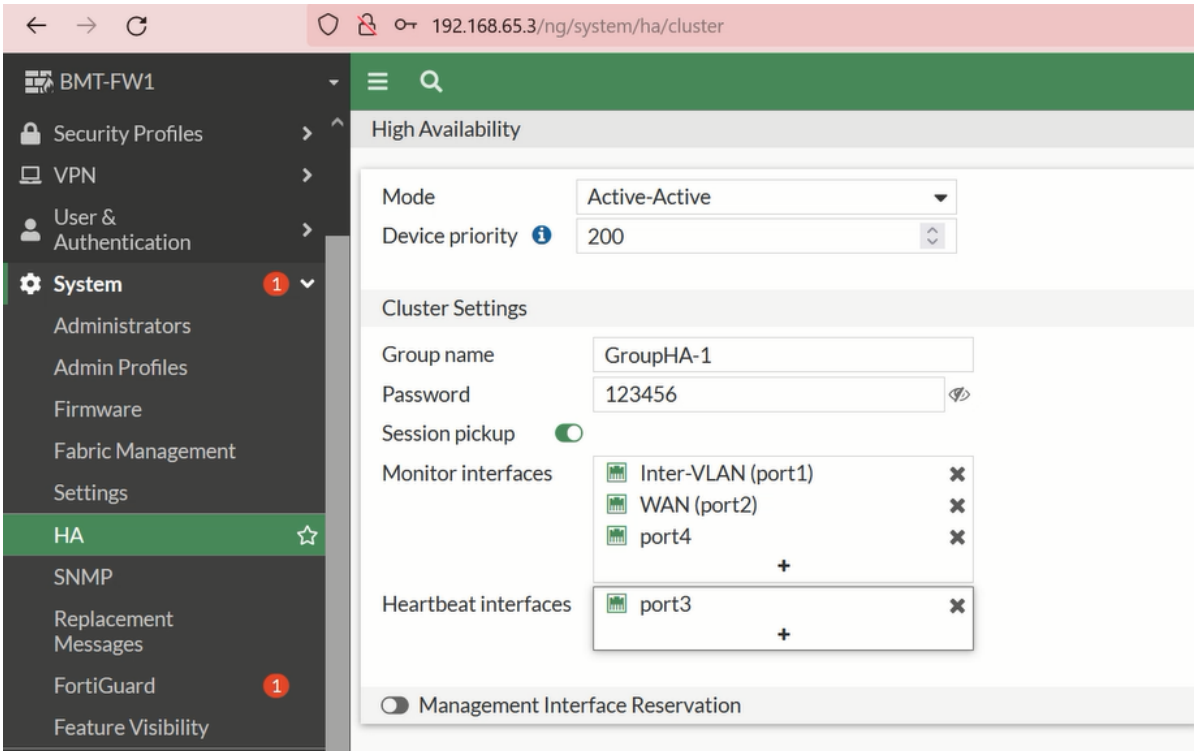

FIGURE 4.32 – Configuration HA sur le premier firewall.

La deuxième étape consiste à configurer le deuxième firewall sur l'interface de ligne de commande (Voir Figure 4.33).

```
BMT-FW2 # config system ha
BMT-FW2 (ha) # set group-name GroupHA-1
BMT-FW2 (ha) # set mode a-a
BMT-FW2 (ha) # set password 123456
BMT-FW2 (ha) # set session-pickup enable
BMT-FW2 (ha) # set hbdev port3 0
BMT-FW2 (ha) # end
```

FIGURE 4.33 – Configuration HA sur le deuxième firewall.

Le résultat du cluster configuré sur les deux Fortigates est le suivant : (Voir Figure 4.34).

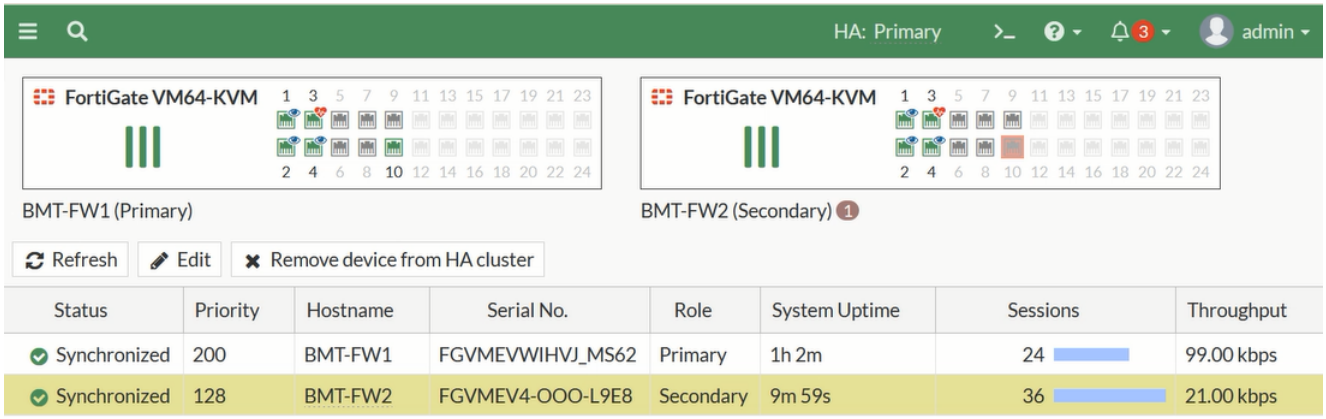

FIGURE 4.34 – Configuration HA effectué avec succès.

4.6 Configuration de la DMZ

(Zemilitarized Zone) est similaire au LAN (Local Area Network), tandis que le réseau LAN utilise principalement l'accès sortant du LAN vers Internet. Dans le cas de la DMZ, le trafic sera entrant d'Internet vers le côté DMZ, ou du côté LAN vers la DMZ. Il faut toujours conserver les serveurs connectés à Internet sur la DMZ. Il peut s'agir de serveurs Web, de serveurs de messagerie, de serveurs FTP/SFTP, etc.

4.6.1 Création du mode VTP transparent

La première étape consiste à activer le mode VTP transparent pour faire toute modification sur les VLANs en local uniquement et donc ne propage pas ses modifications vers tous les switchs du réseau, comme la Figure 4.35 l'illustre.

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

FIGURE 4.35 – Création du mode VTP transparent.

4.6.2 Création des privates VLANs

La deuxième étape consiste a créer un private VLAN primary (VLAN 100) et lui associer deux private VLAN secondaire 101 et 102 le premier est communautaire et le second est isolé (Voir la Figure 4.36).

```
Dmz(config)#vlan 100
Dmz(config-vlan)#pri
Dmz(config-vlan)#private-vlan pri
Dmz(config-vlan)#private-vlan primary
Dmz(config-vlan)#pri
Dmz(config-vlan)#private-vlan as
Dmz(config-vlan)#private-vlan association 101,102
Dmz(config-vlan)#exit
Dmz(config)#vlan 101
Dmz(config-vlan)#pri
Dmz(config-vlan)#private-vlan co
Dmz(config-vlan)#private-vlan community
Dmz(config-vlan)#exit
Dmz(config)#vlan 102
Dmz(config-vlan)#pri
Dmz(config-vlan)#private-vlan i
Dmz(config-vlan)#private-vlan isolated
Dmz(config-vlan)#exit
```

FIGURE 4.36 – Création des privates VLANs.

4.6.3 Association des ports aux Private VLAN

Nous avons associé le port 0/1 et le port 0/3 au primary VLAN 100 et au private VLAN 101 comme le montre la Figure 4.37. Ainsi, que nous avons associé l'interface 0/2 et 1/0 au VLAN primary 100 et au private VLAN 102 en mode host.

```
Dmz(config)#interface  range ethernet 0/1, ethernet 0/3
Dmz(config-if-range)#sw
Dmz(config-if-range)#switchport mo
Dmz(config-if-range)#switchport mode pri
Dmz(config-if-range)#switchport mode private-vlan h
Dmz(config-if-range)#switchport mode private-vlan host
Dmz(config-if-range)#sw
Dmz(config-if-range)#switchport p
*May  2 15:31:25.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
*May  2 15:31:25.216: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
Dmz(config-if-range)#switchport pri
Dmz(config-if-range)#switchport private-vlan h
Dmz(config-if-range)#switchport private-vlan host-association 100 101
Dmz(config-if-range)#exit
```

FIGURE 4.37 – Association des ports 0/1 et 0/3 aux Private VLAN 100 et 101.

La dernière étape consiste a configuré le port 0/0 en mode promiscuous pour communiquer avec les ports membres du même VLAN(Voir la Figure 4.38).

```
Dmz(config)#interface  ethernet 0/0
Dmz(config-if)#sw
Dmz(config-if)#switchport m
Dmz(config-if)#switchport mode pri
Dmz(config-if)#switchport mode private-vlan p
Dmz(config-if)#switchport mode private-vlan promiscuous
Dmz(config-if)#
*May  2 15:33:54.619: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Dmz(config-if)#sw
Dmz(config-if)#switchport pri
Dmz(config-if)#switchport private-vlan m
Dmz(config-if)#switchport private-vlan mapping 100 101,102
Dmz(config-if)#end
```

FIGURE 4.38 – Association du port 0/0 aux Private VLAN.

4.7 Tests et Vérifications

Dans cette partie, l'ensemble des tests consiste à vérifier la validation des configurations en utilisant les commandes "Show" qui affichent selon la commande utilisée les différentes configurations effectuées sur les équipements, et une autre phase qui consiste a vérifier les communications entre quelques équipements en utilisant la commande " Ping ".

4.7.1 Vérification des configurations

4.7.1.1 Vérification de l'active directory

Nous avons créer une stratégie de groupe d'où on a interdit l'accès au panneau de configuration et désactivé les disque amovible. A partir du pc manager nous essayons d'accéder au disque amovible (Voir la Figure 4.39).

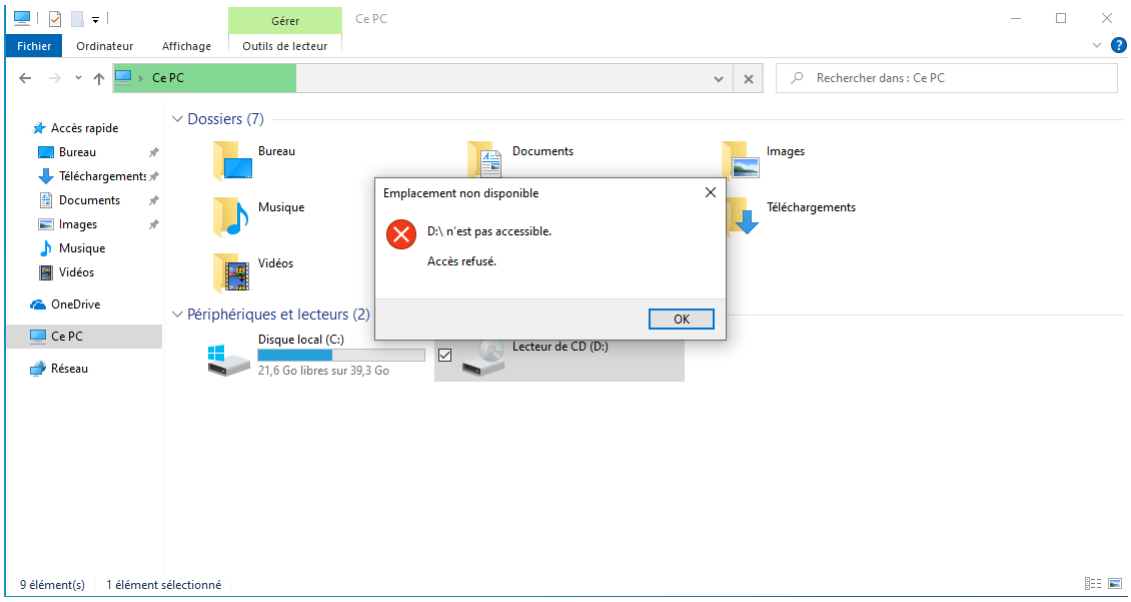

FIGURE 4.39 – Disque amovible désactivé.

A partir du pc manager on essaye d'accéder au panneau de configuration (Voir la Figure 4.40).

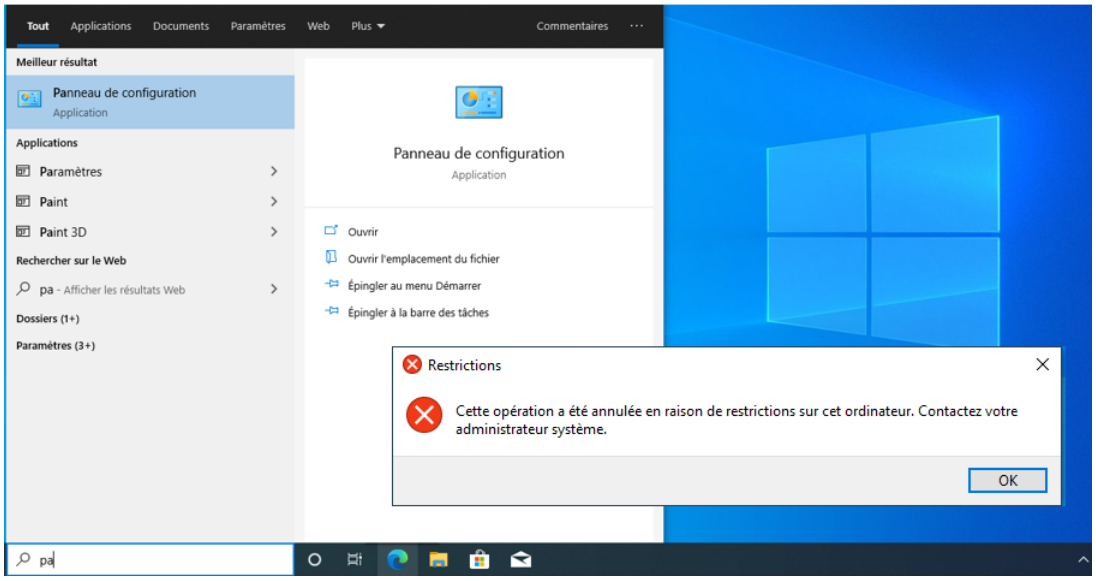

FIGURE 4.40 – Accès interdit au panneau de configuration.

4.7.1.2 Vérification de la configuration du protocole VTP

Nous vérifions l'activation du protocole VTP avec la commande "Show vtp status" sur le switch core. VTP mode serveur (Voir la Figure 4.41).

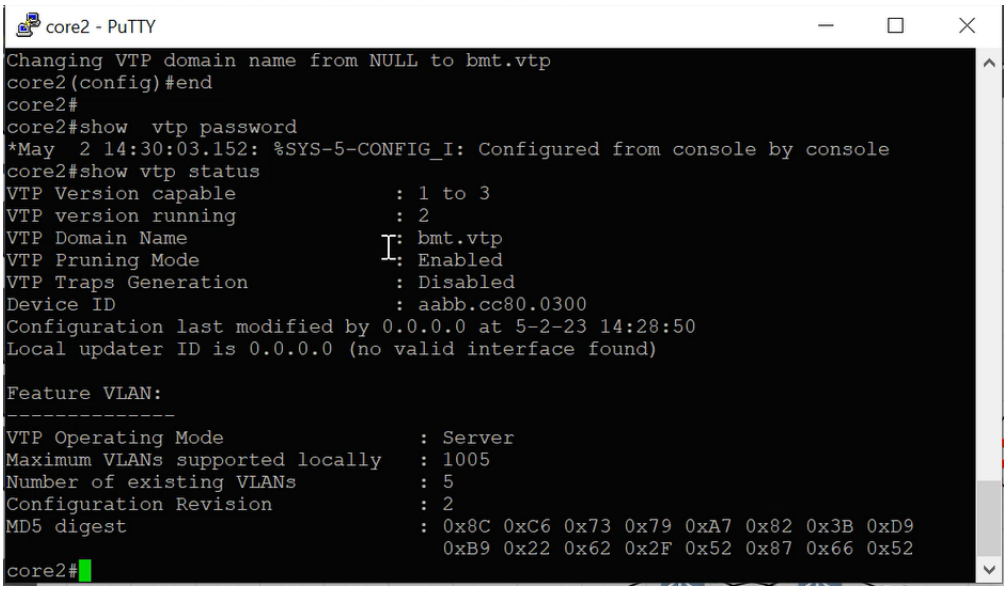

FIGURE 4.41 – Vérification du protocole VTP en mode serveur.

VTP mode client (Voir la Figure 4.42).

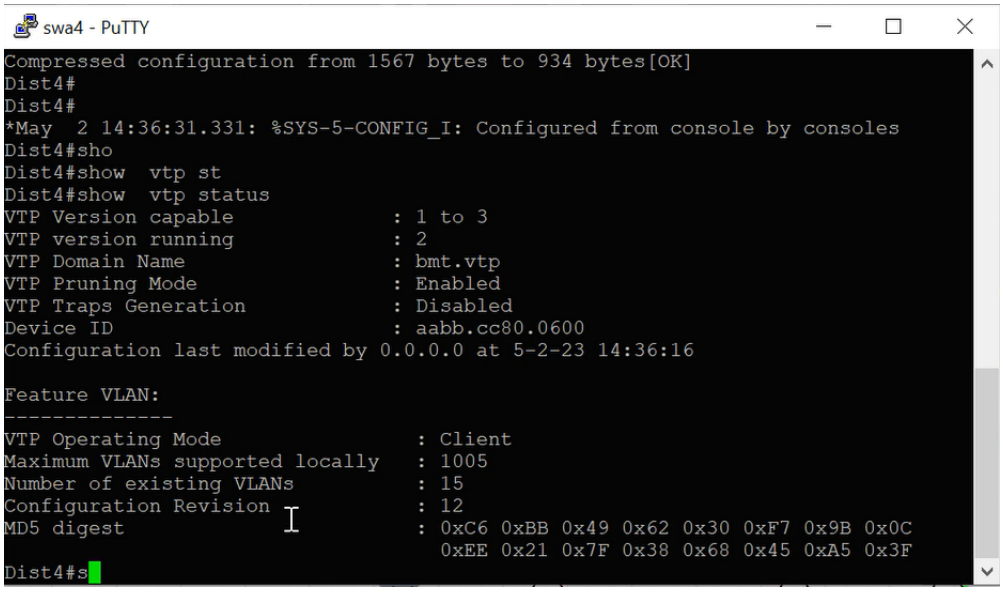

FIGURE 4.42 – Vérification du protocole VTP en mode client.

4.7.1.3 Vérification de la création des VLANs

Pour vérifier que les VLANs sont bien créés, on lance la commande "show vlan brief" sur les commutateurs de la couche coeur et accès (Voir la Figure 4.43).

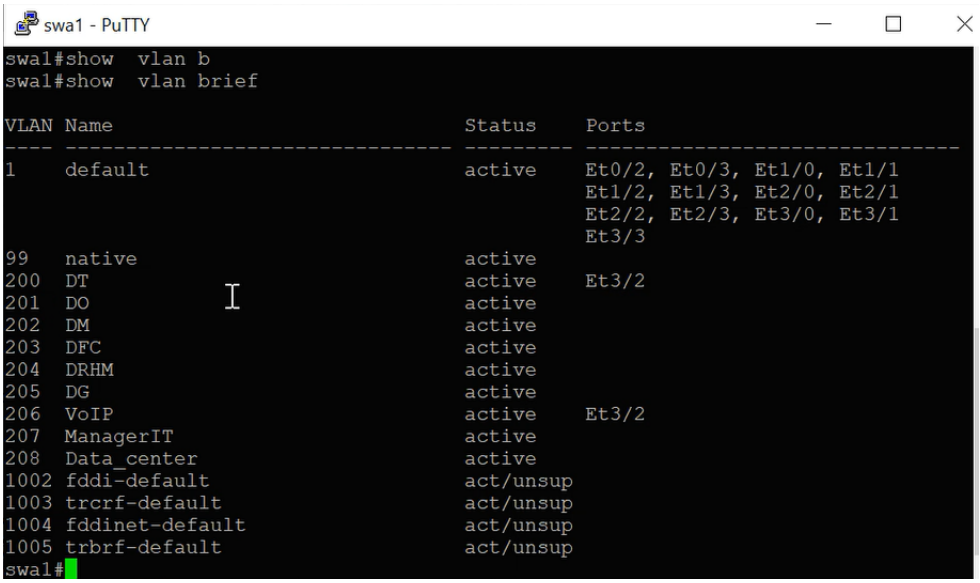

FIGURE 4.43 – Vérification de la création des VLANs.

4.7.1.4 Vérification d'EtherChannel

Nous vérifions la création d'EtherChannel et son fonctionnement en utilisant la commande "show etherchannel summary" sur la console des switchs core (Voir la Figure 4.44).

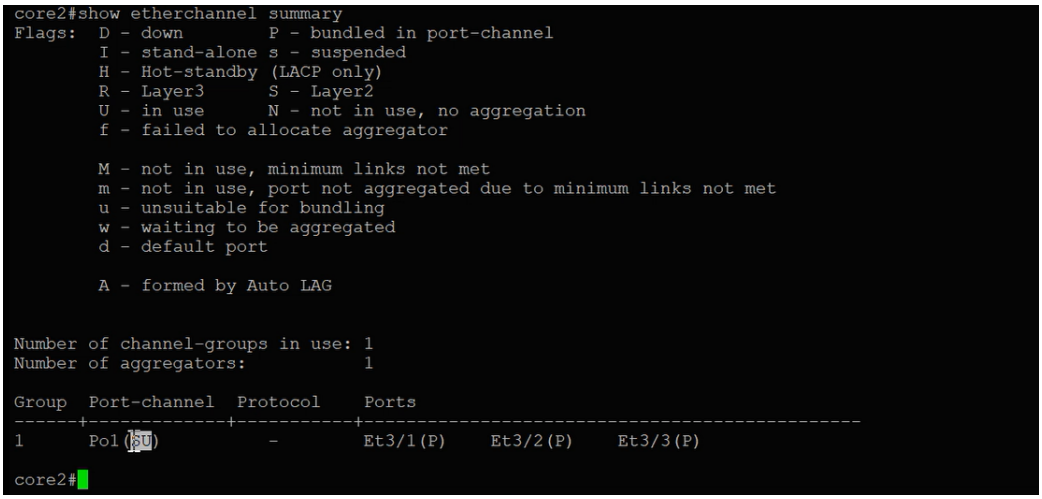

FIGURE 4.44 – Vérification de la configuration d'etherchannel sur le switch core.

4.7.1.5 Vérification de cluster

La Figure 4.45 montre que le FW1 est en primary et le FW2 est en secondary a l'aide de la commande "get system ha status", pour vérifier le basculement automatique nous éteignons le FW1 a l'aide de la commande "execute shutdown" comme la Figure 4.46 l'illustre.

Après avoir éteigniez le FW1, le FW2 va devenir primary (Voir la Figure 4.47).

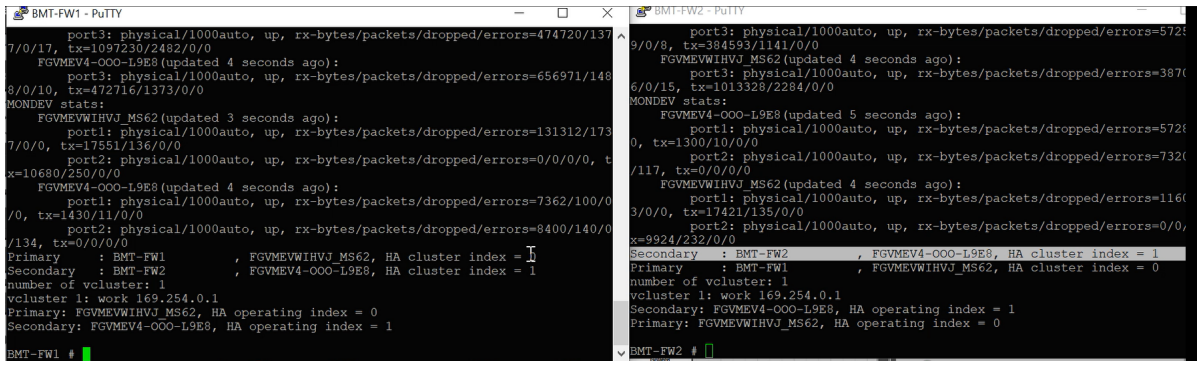

FIGURE 4.45 – Les priorités des clusters.

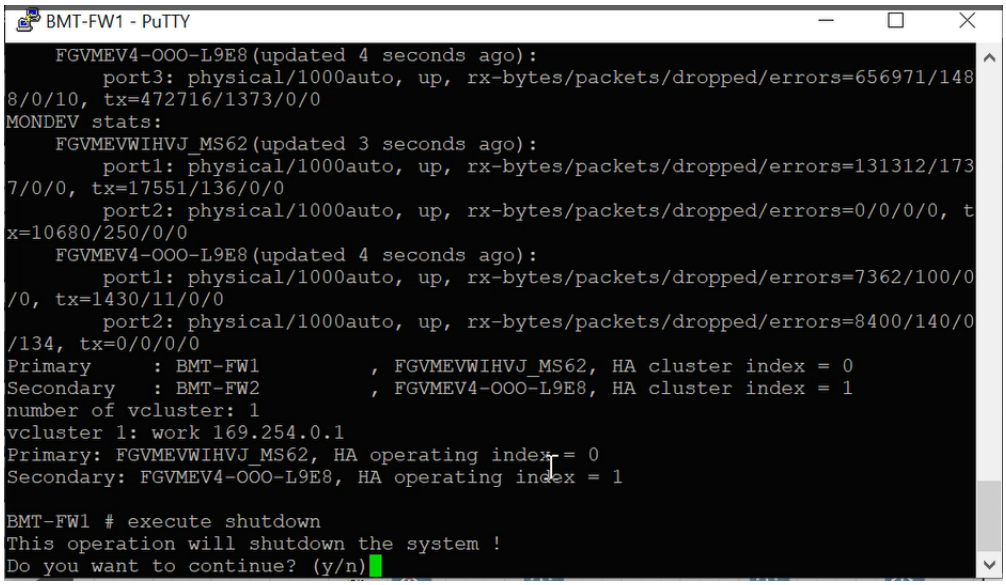

FIGURE 4.46 – Éteindre le FW1.

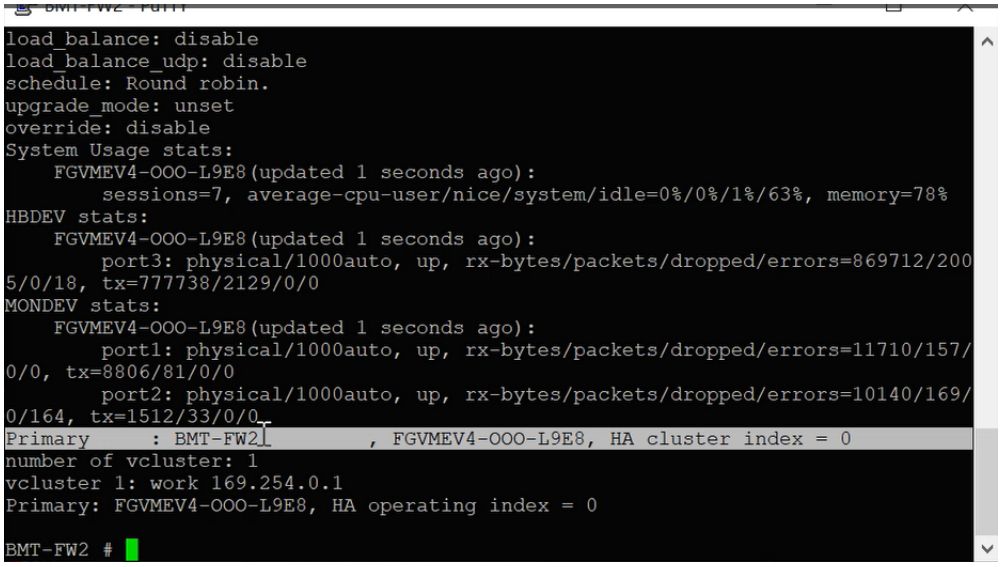

FIGURE 4.47 – Basculement de FW2.

4.7.1.6 Attribution des adresses aux PC par DHCP

Nous vérifions l'affectation des adresses IP aux ordinateurs du réseau par le protocole DHCP avec la commande "ip dhcp" lancé à partir des consoles des PCs (Voir la Figure 4.48).

FIGURE 4.48 – Attribution des adresses au PC1 par DHCP.

4.7.2 Tests

4.7.2.1 Connectivité des serveurs community

Nous avons effectué un ping entre les deux serveurs de la zone community (Voir la Figure 4.49).

```
ser01> ping 10.0.2.3
84 bytes from 10.0.2.3 icmp_seq=1 ttl=64 time=1.863 ms
84 bytes from 10.0.2.3 icmp_seq=2 ttl=64 time=4.664 ms
84 bytes from 10.0.2.3 icmp_seq=3 ttl=64 time=4.152 ms
84 bytes from 10.0.2.3 icmp_seq=4 ttl=64 time=3.754 ms
84 bytes from 10.0.2.3 icmp_seq=5 ttl=64 time=3.534 ms
```

FIGURE 4.49 – Connectivité des serveurs community 1 et 2.

4.7.2.2 Non connectivité des serveurs isolated

Nous avons effectué un ping entre le serveur 1 de la zone community et les deux serveurs de la zone isolated (Voir la Figure 4.50).

```
ser01> ping 10.0.2.4
host (10.0.2.4) not reachable

ser01> ping 10.0.2.5
host (10.0.2.5) not reachable
```

FIGURE 4.50 – Non connectivité du serveur 1 avec les serveurs isolated 3 et 4.

4.7.2.3 Test inter-VLANs

Nous vérifions la communication entre les équipements de VLANs différents, en effectuant un test « ping» entre le PC8 qui se trouve dans le VLAN 200 le PC2 avec l'adresse IP «172.19.201.10 » qui se trouve dans le VLAN 201 au commutateur (Voir la Figure 4.51).

```
PC8> ping 172.19.201.10
84 bytes from 172.19.201.10 icmp_seq=1 ttl=63 time=26.731 ms
84 bytes from 172.19.201.10 icmp_seq=2 ttl=63 time=24.553 ms
84 bytes from 172.19.201.10 icmp_seq=3 ttl=63 time=27.502 ms
84 bytes from 172.19.201.10 icmp_seq=4 ttl=63 time=14.176 ms
84 bytes from 172.19.201.10 icmp_seq=5 ttl=63 time=12.121 ms

PC8>
```

FIGURE 4.51 – Test ping inter-VLANs.

4.7.2.4 Test intra-VLANs

Nous vérifions la communication entre les équipements situés en même VLAN, nous effectuons un test « ping » entre le PC8 et le PC1 avec l'adresse IP «172.19.200.12 », tels que les deux se trouve dans

le même VLAN 200 (Voir la Figure 4.52).

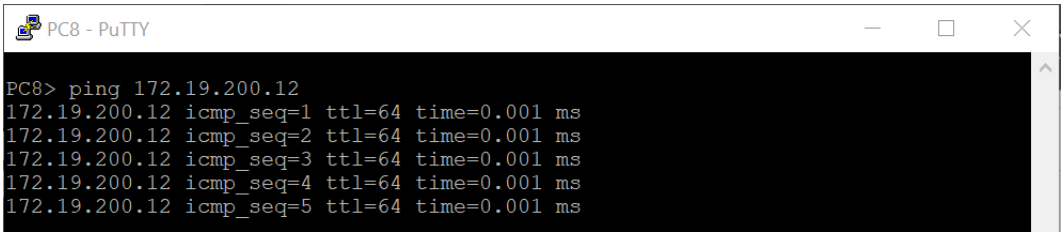

FIGURE 4.52 – Test ping intra-VLANs.

4.7.2.5 Test connexion vers internet

Nous vérifions la connexion vers internet en effectuant un ping à partir de PC manager avec l'adresse IP «1.1.1.1» (Voir la Figure4.53).

FIGURE 4.53 – Test ping vers internet.

4.8 Conclusion

Dans ce chapitre, nous avons abordé la phase de mise en œuvre de notre projet. Nous avons débuté par présenter les outils que nous avons utilisés, à savoir GNS3 et VMWARE, pour créer notre environnement de travail. Ensuite, nous avons détaillé les différentes étapes de configuration des solutions proposées, en mettant l'accent sur les aspects liés à la sécurité. Enfin, nous avons effectué des tests de vérification afin de s'assurer du bon fonctionnement de nos configurations.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

À l'issue de ce projet, nous avons pu mettre à profit nos connaissances théoriques et pratiques pour étudier en profondeur l'architecture réseau de l'entreprise Bejaia Mediterranean Terminal (BMT) et proposer des améliorations significatives. Après avoir présenté le projet et réalisé une analyse approfondie de l'architecture réseau existante de BMT, nous avons élaboré une solution visant à mieux répondre aux besoins spécifiques de l'entreprise et à garantir un niveau élevé de sécurité des services Internet et intranet.

Dans le cadre de notre proposition d'amélioration, nous avons mis en place plusieurs composants clés qui ont été intégrés avec succès dans l'architecture réseau de BMT. Tout d'abord, nous avons déployé un serveur "Active Directory", permettant ainsi la centralisation des données utilisateurs et des équipements informatiques. Cela a contribué à renforcer la sécurité en offrant aux administrateurs la possibilité de définir précisément les autorisations d'accès aux ressources et aux logiciels, et de gérer efficacement les installations et les mises à jour sur l'ensemble du réseau.

Ensuite, nous avons procédé à la segmentation du réseau en mettant en place des réseaux locaux virtuels (VLAN). Cette approche a permis d'améliorer les performances globales du réseau en réduisant le trafic et en isolant les différents groupes de périphériques en fonction de leurs besoins et de leurs niveaux de sécurité. Par conséquent, cela a renforcé la protection contre les attaques internes en limitant la propagation des menaces potentielles.

Pour garantir une haute disponibilité et la tolérance aux pannes, nous avons préconisé la conception d'un cluster. Cette configuration redondante des composants critiques du réseau a éliminé les points de défaillance uniques, assurant ainsi une continuité de service optimale et réduisant les interruptions potentielles.

En ce qui concerne la sécurité contre les attaques externes, nous avons mis en œuvre des zones démilitarisées (DMZ) pour isoler et protéger les systèmes sensibles de l'entreprise. En contrôlant strictement le trafic entre les différents segments du réseau, nous avons renforcé la résistance aux attaques et amélioré la sécurité globale de l'infrastructure.

Pour implémenter ce projet, nous avons utilisé des outils tels que GNS3 et VMWare Workstation Pro 17 pour simuler et valider notre proposition d'architecture. Ces outils nous ont permis de tester les différentes configurations et de vérifier leur bon fonctionnement avant leur déploiement dans l'environnement réel de l'entreprise.

En termes de perspectives futures, nous envisageons d'approfondir encore notre solution en mettant en place un réseau privé virtuel (VPN) afin de renforcer d'avantage la sécurité des communications et d'accroître la confidentialité des données échangées. De plus, nous prévoyons de configurer des listes de contrôle d'accès (ACL) pour filtrer de manière granulaire le trafic entrant et sortant, afin de renforcer les mécanismes de défense de l'entreprise contre les menaces potentielles. Enfin, nous envisageons d'implémenter la fonctionnalité de BranchCache pour optimiser les performances des applications locales et réduire la consommation.

BIBLIOGRAPHIE

[1] Bejaia mediterrannean terminal, 2020. `https://bejaiamed.com/`.

[2] A.Hakka. "l'intranet dans les entreprises :effet de mode ou reponse a des besoins reels ". *université d'Oran*, 2017.

[3] C.Fluke. Fllike networks, 2006. `https://www.fluKenetworks.com`.

[4] A.Hantach C.Jabou, M.Schillings. "ter détection d'anomalies sur le réseau". *Université Paris Descartes*, 2008/2009.

[5] CN.Pascla. "cours de réseau maîtrise d'informatique". *Université d'angers*, 2000.

[6] D.Zouatine. "outage multicast à travers un backbone maillé sans fil". *Université Larbi Ben M'hidi, Oum El Bouaghi*, 2017.

[7] G.Hamzata. "mise en place d'un ids en utilisant snort. etudes supérieur en informatique et réseau". *Diplôme Européen*, 2011.

[8] L.Aggabou. "cour sur la sûreté de fonctionnement". *Université BATNA 2*, 2019/2020.

[9] M.Landréa. "internet et le world wide web". *Formation des Professeurs aux outils informatiques du multimédia et de l'Internet*, juin 1998.

[10] N.Medjani M.Mihoubi. "sécurisation d'une infrastructure lan/wan a base d'équipement cisco". *Université Mouloud Mammeri de TIZI-OUZOU*, 2015.

[11] N.Battat. "cours sur les systèmes de sécurité". *Université Abderrahmane Mira, Béjaïa*, 2022/2023.

[12] C.Arkoub N.Belaid. "services d'accélération des applications et optimisation des liens wan (waas : Wide area application services) au niveau de la cnas d'alger.". *Université Mouloud Mammeri, TIZI-OUZOU*, 2010/2011.

[13] N.Labraoui. "sécurité informatique.chapitre 1 : Notions fondamentales". *Master 1 Réseaux et systèmes distribués*, 2020.

[14] P.Florian. Arcan security, 2021. `https://arcansecurity.com/securiser-reseau-entreprise/`.

[15] P.jean-francois. Comment Ça marche.net, 2007. `https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/types.htm`.

[16] Réal Rodrigue. "les réseaux informatiques". *Documentation et bibliothèques*, 41(1) :5–11, 1995.

[17] S.Mongo. Les Équipements réseaux informatiques, 2021. https://www.mongosukulu.com/index.php/contenu/informatique-et-reseaux/reseaux-informatiques/639-les-equipements-reseaux-informatiques.

[18] S.Rabehi. "mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11". *université Abou Bekr Belkaid,Tlemcen*, 2010/2011.

[19] A.Saoud S.Saoud. "etude et amélioration de l'architecture et sécurité du réseaude l'epb". *Université Abderrahmane Mira, Béjaïa*, 2015/2016.

[20] W.Achim. Ionos sarl, 2018. https://www.ionos.fr/startupguide/productivite/intranet/.

[21] Z.Bendella. "gestion de la sécurité d'une application web a l'aide d'un ids comportemental optimisé par l'algorithme des k-means". Mémoire de master, université Abou Bekr Belkaid, Tlemcen, 2012/2013.

[22] Z.Farah. "cour sur la sécurité informatique". *Université Abderrahmane Mira, Béjaïa*, 2020/2021.

ANNEXE A

ANNEXE

A.1 Configuration des interfaces des VLANs sous Windows Server 2022

La première étape consiste à ajouter le rôle DHCP (Dynamic Host Configuration Protocol) au serveur local comme nous l'avons déjà fait pour AD (Voir Figure A.1).

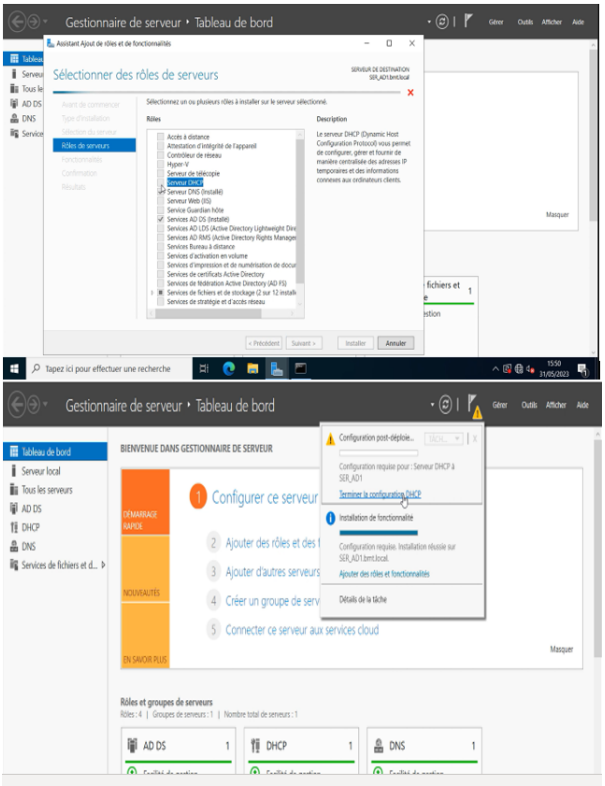

FIGURE A.1 – Ajout du role DHCP.

Pour la deuxième étape on va créer des étendues pour chaque VLAN comme la figure A.3 l'illustre.

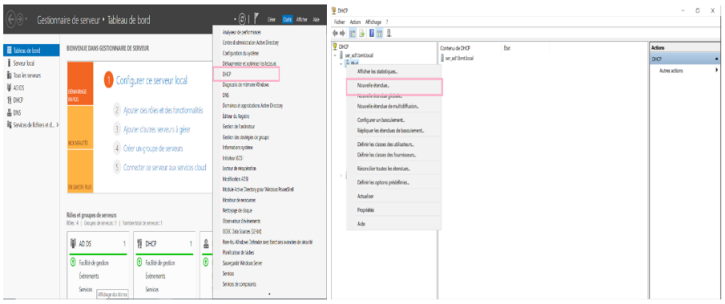

FIGURE A.2 – Création de l'étendue des VLANs au niveau du Windows Server 2022.

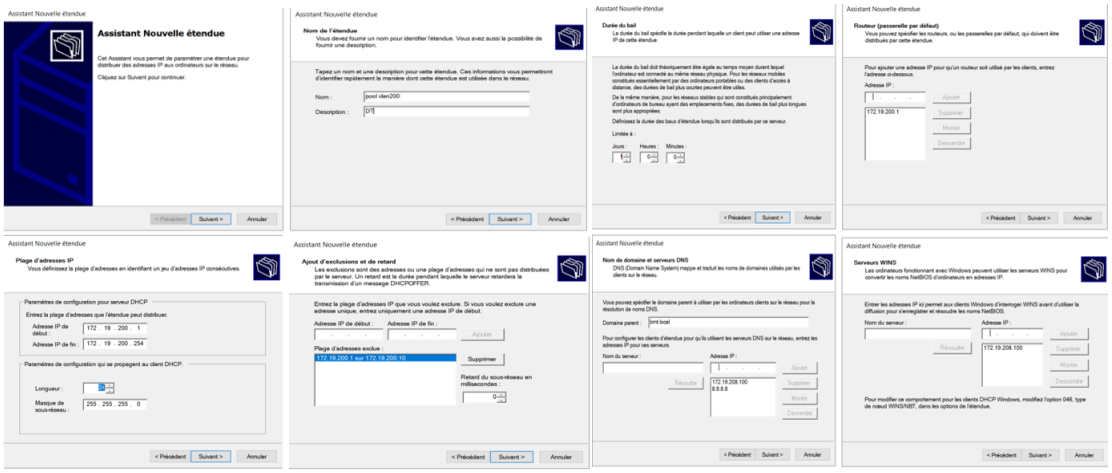

FIGURE A.3 – Création de l'étendue des VLANs au niveau du Windows Server 2022.

La figure A.4 ci-dessous montre toutes les étendues que nous avons créées.

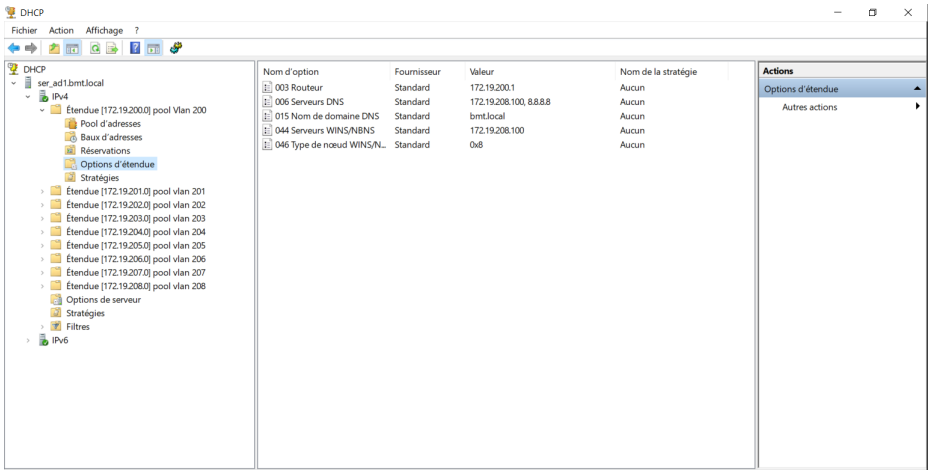

FIGURE A.4 – Vérification des étendues crée au niveau du Windows Server 2022.

A.2 Configuration du DHCP relay

Nous avons mis en place un relais DHCP en utilisant l'adresse de notre serveur DHCP afin de garantir que seul le serveur DHCP du VLAN 208 attribue les adresses IP aux ordinateurs. La configuration se fait au niveau du fortigate pour chaque VLAN.

Activation de DHCP server ,choisir le mode relay puis indiquer l'adresse du serveur DHCP qui est "172.19.208.100" (Voir Figure A.5)

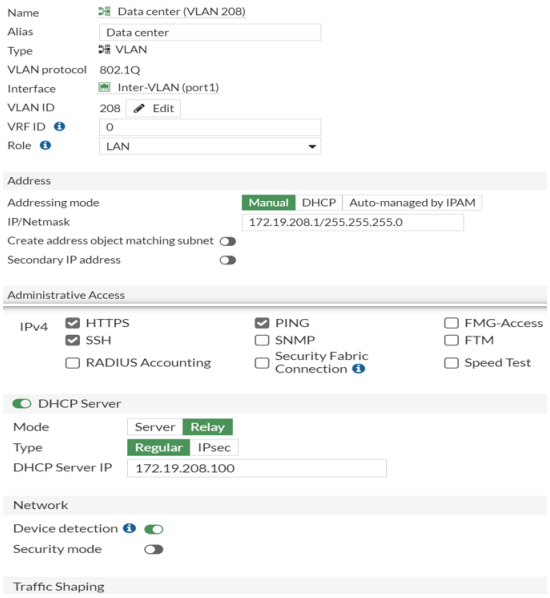

FIGURE A.5 – Activation du DHCP relay au niveau du fortigate.

RÉSUMÉ

Le réseau informatique est le cœur de l'entreprise, quel que soit son secteur d'activité. Pour cela, les problèmes de sécurité doivent être réduits au minimum afin d'assurer l'activité de cette dernière. Notre travail consiste en une étude et proposition d'une architecture réseau et sécurité des services Internet et intranet pour le réseau informatique de L'entreprise Bejaia Mediterranean Terminal (BMT).

Notre travail a consisté en l'installation d'un serveur Active Directory pour une gestion centralisée du réseau, la segmentation du réseau en utilisant des VLANs, la configuration d'un cluster pour assurer la tolérance aux pannes, et la mise en place d'une zone démilitarisée (DMZ) pour prévenir les accès indésirables. En utilisant le simulateur GNS3 et VMWARE, nous avons pu tester et valider notre architecture avant son déploiement dans l'environnement réel de l'entreprise. Ces améliorations garantiront une meilleure gestion du réseau, une protection renforcée contre les attaques et une continuité des activités de l'entreprise et les services Internet et intranet. Ainsi, nous avons intégré certains protocoles de sécurité tel que DHCP ET VTP.

Mots clés : BMT, VLAN, Cluster, DMZ, GNS3, VMWARE, réseaux informatiques, sécurité.

ABSTRACT

The computer network is the heart of the company, whatever its sector of activity. For this, security issues must be minimized to ensure the activity of the latter. Our work consists of a study and proposal of a network architecture and security of Internet and intranet services for the computer network of the company Bejaia Mediterranean Terminal (BMT).

Our work consisted of installing an Active Directory server for centralized network management, network segmentation using VLANs, configuring a cluster to ensure fault tolerance, and setting up a demilitarized zone (DMZ) to prevent unwanted access. By using the GNS3 simulator and VMWARE, we were able to test and validate our architecture before its deployment in the real environment of the company. These enhancements will ensure better network management, enhanced attack protection, and business continuity for Internet and intranet services. Thus, we have integrated certain security protocols such as DHCP AND VTP.

Key words : BMT, VLAN, Cluster, DMZ, GNS3, VMWARE, Computer Networks, Security.