République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Univérsité Abderrahmane Mira - Béjaia -
Faculté des Sciences Exacte
Département d'Informatique

Mémoire de Fin de cycle

En vue de l'obtention du diplôme de MASTER professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Solution de virtualisation et supervision des réseaux pour avoir la haute disponibilité : Cas d'Etude BMT

Réalisée par :
YAHIA Rima. & TAHI Chahinez.

Devant les jurys composés de :

Président :	Dr KHENOUS Lachemi.	MCB Université de Béjaïa
Examinateur :	Dr OUYAHIA Samira.	MCB Université de Béjaïa
Encadré :	Dr YAICI Malika.	MCB Université de Béjaïa

2022 — 2023

Remerciements

Nous tonnons à remercier :

Le bon dieu de nous avoir donné la patience et la volonté pour accomplir ce travail.

Nos remerciements s'adressent également à :

Notre promoteur Madame YAICI Malika pour avoir généreusement accepté de nous encadrer. Ses conseils avisés, ses orientations précieuses et sa disponibilité tout au long de ce travail ont grandement contribué à sa réussite.

Nous remercions également :

L'organisme d'accueil BMT tout particulièrement Monsieur ZAABAR Fayssal, notre encadrant sur le lieu de stage, pour son encadrement attentif, ses suggestions pertinentes et son partage de connaissances. Sa présence et son suivi ont grandement contribué à l'enrichissement de notre expérience professionnelle.

Nous tenons également à remercier :

Les membres de jury, pour l'honneur qu'ils nous font en acceptant de juger, de lire et d'évaluer ce mémoire
Enfin, nous remercions toutes personne ayant contribué de près ou de loin à la réalisation de ce travail.

Rima & Chahinez.

Dédicace

Je tiens à dédier vivement ce modeste travail a mes très chers parents auxquels je dois ma réussite et auxquels je ne rendrai jamais assez .je leurs souhaite une longue vie,

À mes frères Yacin, Fahem, Fateh, Messaoud et Djallal,
vous êtes mes piliers, mes confidents et mes sources d'inspiration. Votre soutien indéfectible, vos encouragements sans faille et votre présence bienveillante ont joué un rôle essentiel dans mon cheminement. Cette dédicace est un témoignage de ma gratitude envers chacun de vous.

À mon fiancé Massi,
tu as été mon roc, mon soutien constant et mon moteur tout au long de cette aventure.

À ma binôme Chahinez,
nous avons formé une équipe dynamique et solidaire. Je te remercie du fond du cœur pour cette expérience enrichissante que nous avons partagée.

À mes chère copine kenza et Nihad,
Votre présence indéfectible, vos encouragements constants ont été d'une valeur inestimable.

Merci infiniment pour tout.

Mlle Rima.

Dédicace

À mes chers parents,

En ce moment de réussite professionnelle, je tiens à vous dédier ce message empli de gratitude. Votre amour inconditionnel. Je vous suis profondément reconnaissant(e) de m'avoir donné les valeurs et l'éducation qui m'ont permis d'atteindre mes objectifs professionnels. Votre amour et votre soutien ont été mon plus grand moteur, et je vous serai éternellement reconnaissant(e) pour cela.

À mes chères sœurs, Kahina et Anaïs,

Vous êtes mes sœurs adorées, mes alliées dans la vie et mes sources d'inspiration.Votre présence dans ma vie est un cadeau inestimable, et je suis reconnaissant(e) d'avoir des sœurs aussi merveilleuses que vous.

À ma binôme Rima,

Nous avons partagé tant de moments précieux pendant notre parcours académique. Ta perspicacité, ton travail acharné et notre collaboration ont été des éléments clés de notre réussite, et je te remercie pour ton soutien infaillible.

Et enfin, à mes chère copine Nihad et kenza,

Votre présence constante, votre soutien indéfectible et vos encouragements sincères ont été un pilier essentiel. Je suis infiniment reconnaissant(e).

À vous tous, ma famille et mes proches, je dédie cette déclaration avec une profonde gratitude. Votre amour, votre soutien et votre présence dans ma vie ont été des éléments essentiels de ma réussite professionnelle. Je vous remercie du fond du cœur pour tout ce que vous avez fait et continuez de faire pour moi.

Avec amour et reconnaissance ,je vous remercie infiniment

Mlle Chahinez.

Table des matières

Table des figures

Liste des tableaux

Abbreviations

ARP Address Resolution Protocol

BMT Bejaia Méditerranean Terminal

CDN Centre Digitalisation et Numérique

CPE Conseil des Participations de l'Etat

CTMS Container Terminal Management System

DHCP Dynamic Host Configuration Protocol.

DMZ Zone Démilitarisée

DNS Domain Name Server

EJB Enterprise Java Beans

EPB Entreprise Portuaire de Bejaia

ESXi7 Elastic Sky X Integrated 7

FTP File Transfer Protocol

GLBP Getway Load Balancing Protocol

GNS3 Graphical Network System 3

GRH Gestion des Ressources Humaines

IOU Ios On Unix

IP Internet Protocol

JEE Java Entreprise Edition

JPA Java Persistence API

KVM Kernel-based Virtual Machine

LACP Link Aggregation Control Protocol

LAN Local Area Network

LXC Linux Containers

MAC Media Access Control address

NAS Network Attached Storage

NVRAM non-volatile random access memory

PHP Hypertext Preprocessor

PSE PORTEK Systems and Equipment

SLA Service Level Agreement

SNMP Simple Network Management Protocol

TOS Terminal Operation System

UTM Unified Threat Management

VLAN Virtual Local Area Network

VPN Virtual Private Network

VTP Virtual Trunking Protocol

WAN Wide Area Network

ZEP Zone Extra Portuaire

Introduction Générale

La virtualisation et la supervision des réseaux sont deux domaines essentiels pour assurer une haute disponibilité des infrastructures réseau.

La virtualisation des réseaux est un processus qui consiste à créer des versions virtuelles des ressources réseau, telles que les commutateurs, les routeurs, les pare-feu et autres appareils, sur une infrastructure physique sous-jacente. Cela permet de séparer les ressources réseau logiquement et de les partager entre plusieurs utilisateurs ou applications, offrant ainsi une plus grande flexibilité et une utilisation plus efficace des ressources. La virtualisation des réseaux permet également de créer des réseaux virtuels isolés, appelés VLAN (Virtual Local Area Networks), qui permettent de segmenter le trafic et d'améliorer la sécurité.

En ce qui concerne la supervision des réseaux, il s'agit d'un processus visant à surveiller et à contrôler les performances, la disponibilité et la sécurité du réseau. La supervision des réseaux permet de collecter des informations sur les appareils réseau, les flux de trafic, les erreurs, les goulots d'étranglement et d'autres paramètres importants. Cette surveillance en temps réel permet aux administrateurs réseau de détecter rapidement les problèmes potentiels, d'identifier les causes profondes et de prendre des mesures correctives.

Pour assurer une haute disponibilité des réseaux, la virtualisation et la supervision sont souvent combinées. En virtualisant les ressources réseau, il est possible de répartir la charge de manière équilibrée entre différents appareils virtuels, ce qui contribue à éviter les points de défaillance uniques et à améliorer la disponibilité globale du réseau. De plus, la supervision en temps réel permet de détecter les pannes, les ralentissements ou les comportements anormaux, et d'agir rapidement pour les résoudre et minimiser les interruptions de service.

En résumé, la virtualisation et la supervision des réseaux sont des technologies essentielles pour garantir une haute disponibilité des infrastructures réseau. Elles offrent une flexibilité accrue, une utilisation plus efficace des ressources et une détection précoce des problèmes, ce qui contribue à maintenir les réseaux en fonctionnement optimal .

Notre travail porte sur l'étude et la mise en place d'un système de virtualisation et de supervision des réseaux pour avoir une haute disponibilité. Le thème a été proposé par l'entreprise BMT (Bejaia Méditerranean Terminal), où on a effectué notre stage et nous avons constaté que l'entreprise ne disposait pas de ce genre de solution. Notre mémoire est organisé comme suit.

Dans le premier chapitre de notre travail, on a analysé en détail l'organisme d'accueil, mettant en lumière son expertise dans le domaine des technologies de l'information et des communications.

Le deuxième chapitre a été consacré à la sécurité informatique en général. Et on a étudié les différentes menaces auxquelles les réseaux sont exposés et les stratégies de défense pour garantir la confidentialité, l'intégrité et la disponibilité des informations.

Dans le troisième chapitre, le sujet de la virtualisation et la supervision des réseaux a été abordée. Les avantages de la virtualisation,notamment en termes de flexibilité, d'évolutivité et de gestion centralisée ont été cités.on a également exploré les différentes technologies de virtualisation, telles que la virtualisation des serveurs, des réseaux et des applications, en met-

tant l'accent sur les bénéfices qu'elles apportent aux entreprises. Ensuite on a abordé le sujet de la supervision des réseaux. Les outils et les techniques de supervision utilisés pour surveiller l'état des équipements, les performances du réseau et la disponibilité des services ont été étudié.

Dans le quatrième chapitre, les solutions de haute disponibilité adaptées à l'organisme d'accueil ont été examinés. En l'occurrence les architectures redondantes, les mécanismes de basculement et de récupération après sinistre. L'objectif est d'évaluer les options disponibles et de recommander la meilleure approche pour garantir la haute disponibilité et la résilience des systèmes.

Enfin,le cinquième chapitre a été consacré à la partie pratique de notre projet, premièrement on a proposé une architecture de réseau de la BMT, puis on a expliquer les différentes étapes de simulation et les différents tests.

Ainsi, à travers ces différents chapitres, nous avons pu fournir une vision exhaustive de notre travail, que nous clôturons par une conclusion.

Chapitre I

Etude et analyse des besoins

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

I.1 Présentation générale de l'organisme d'accueil :

BMT (Bejaia Méditerranéen Terminal) est une co-entreprise(jointe venture) entre l'Entreprise Portuaire de Bejaia (EPB) et Portek Systems & Equipment (PSE) (Figure I.1). EPB est l'autorité portuaire qui gère le port de Bejaia. PSE, filiale du groupe PORTEK, est un opérateur de Terminaux à conteneurs présent dans plusieurs ports dans le monde, spécialisé dans les équipements portuaires.L'activité principale de BMT est la gestion et l'exploitation du terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients.[1]

FIGURE I.1 – Jointe venture de l'EPB et PORTEK.[1]

I.1.1 Création et évolution :

I.1.2 Création de la BMT :

BMT à été créée sur décision du Conseil des Participations de l'Etat (CPE) en Mai 2004. C'est une jointe venture entre EPB et PSE.

I.1.3 Evolution de la BMT :

Le transport maritime ainsi que la logistique de la BMT son en évolution de leur trafic depuis l'avènement d'un port à conteneur. Prenant en compte la concurrence internationale dans la conteneurisation, l'entreprise portuaire de Bejaia est une entreprise publique économique, qui s'est associée d'une manière stratégique à un spécialiste dans ce domaine, PORTEK une entreprise Singapourienne. De cette alliance est née la société BMT, qui a pour but d'organiser et d'exploiter un terminal polyvalent selon les normes internationales. La société BMT continue à investir dans ses infrastructures dans le but de développer l'activité du conteneur et d'atteindre ses objectifs. [1]

I.1.4 Situation géographique de la BMT :

L'entreprise BMT se situe au niveau du port de Bejaia, ce dernier est implanté au centre du Nord-Est du pays et jouit d'une situation géographique stratégique. Elle se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Bejaia et elle est reliée au réseau routier national qui facilite le transport des marchandises conteneurisées de toute nature vers l'ensemble des régions du pays,(**Position GPS** : L'ATTITUDE NORD : 36○ 45' 14" ; LONGITUDE EST : 05○ 05' 50").

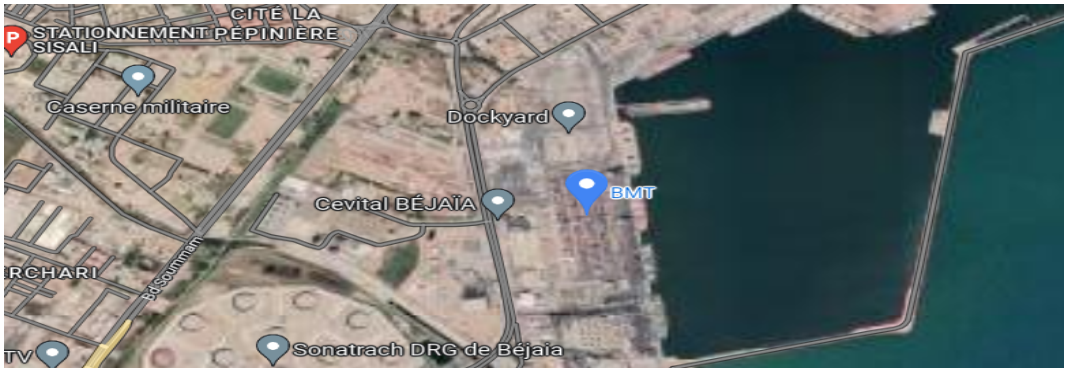

FIGURE I.2 – Capture sur la situation géographique.

I.2 L'organisation de la BMT :

La BMT est constituée de sept directions, chacune d'elles contient des départements et services à différentes tâches.

I.2.1 L'organigramme de l'entreprise :

La Figure I.3 présente l'organigramme général de la BMT donné par le service Gestion des Ressources Humaines (GRH) de l'entreprise.

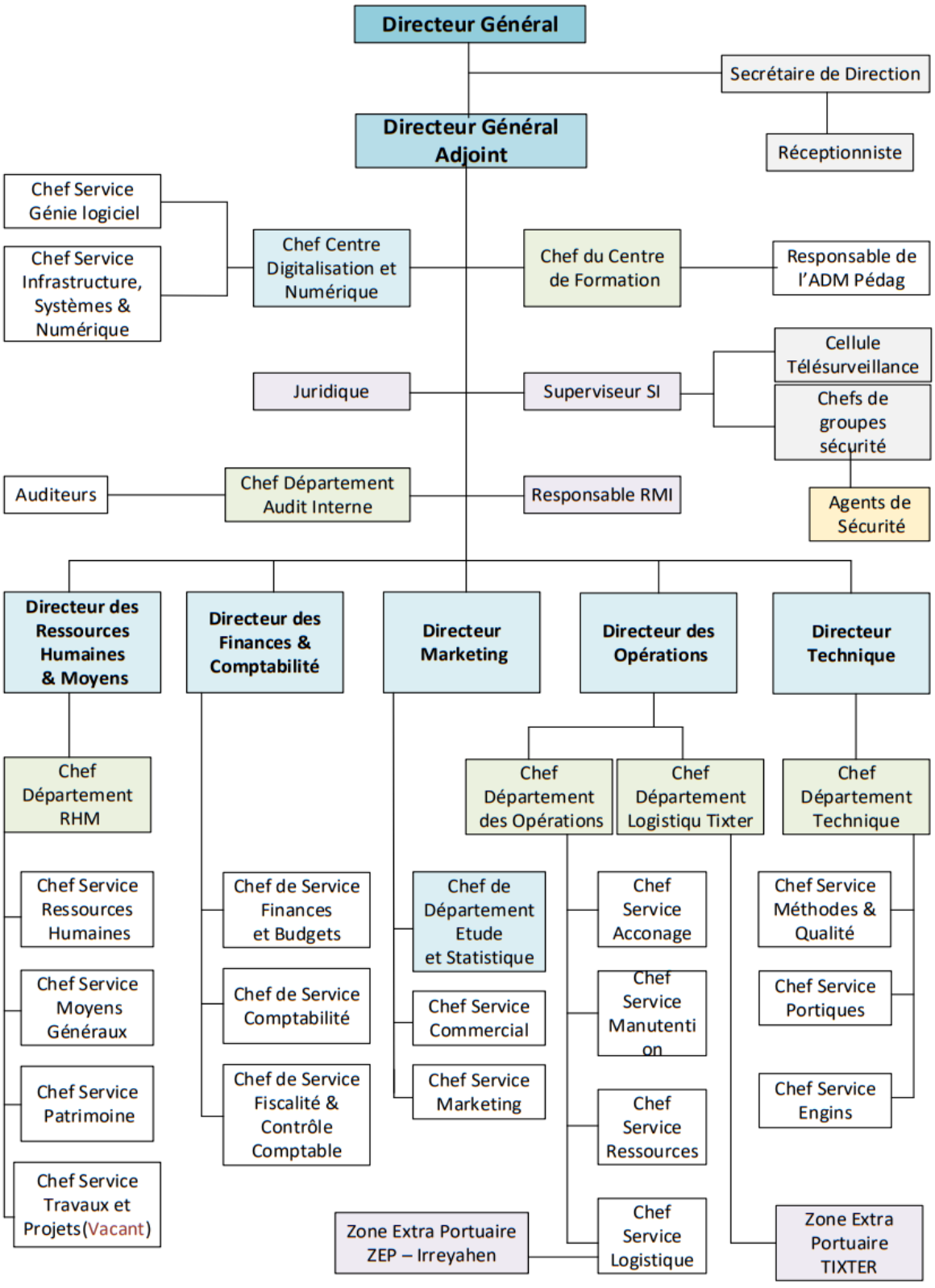

FIGURE I.3 – Organigramme Général de l'entreprise.

I.2.2 Les différentes directions :

La BMT se compose de plusieurs directions dont on peut citer[20] :

1. **Direction Générale (DG) :**
   Le directeur général (avec le DGA) qui gére l'entreprise, a le pouvoir de prendre des décisions, administrer l'entreprise, assigner des directives pour les différentes structures et faire entre les directions de l'entreprise.

2. **Direction des ressources humaines (DRH) :**

   A) **Service ressources humaines :** Il met en œuvre des systèmes de gestion intégré à la stratégie de l'entreprise et qui traduise une adéquation entre les impératifs économiques et les attentes du personnel. Pour cela, la véritable importance de cette structure réside dans la recherche de meilleur potentiel, le conserver en lui offrant les meilleurs conditions (salaire, climat de travail et environnement, formation).

   B) **Service des moyens généraux :** est chargé des achats et de la gestion des stocks de l'entreprise.

   C) **Service hygiène et sécurité :** assure la sécurité de la marchandise, du parc à conteneurs et la propreté de l'entreprise et de son environnement.

3. **Direction des opérations (DO) :**
   Direction des opérations assure la planification des escales, de parc à conteneurs (Figure I.4) et la planification des ressources (humaines et matériels). Elle prend en charge les opérations de manutentions, comme la réception des navires porte conteneurs et leurs chargement et déchargement, comme elle suit les opérations de l'acconage [1] tel que : le suivi des livraisons, dépotages [2], mise a disposition des conteneurs vides, traitement des conteneurs frigorifiques.

FIGURE I.4 – Parc à conteneurs[2].

1. Acconage :transport des marchandises d'un navire à l'aide d'un chaland (Bateau à fond plat pour le transport des marchandises).
2. Dépotages : pour le déchargement des conteneurs.

4. **Direction marketing (DM) :**
   Elle 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 auprés de ses clients. Elle améne son environnement externe à prendre conscience de l'importance des démarches qu'elle entreprend dans le développement et l'amélioration de la qualité des services.

   A) **Service commercial :** Suit la facturation, la gestion de portefeuille client et le recouvrement des créances.

   B) **Département informatique :** Assure le bon fonctionnement du Container Terminal Management System (CTMS), la maintenance du parc informatique de l'entreprise et le développement de nouvelles applications aux différentes structures.

5. **Direction des finances et de comptabilité (DFC) :**
   Elle procède à l'enregistrement de toutes les opérations effectuées par l'entreprise au cours de l'année .Elle est constituée de deux services :

   A) **Service de comptabilité :** procède au contrôle et l'enregistrement de toutes les factures d'achat, de présentation et d'investissement.

   B) **Service des finances :** procède au règlement de toutes les factures d'un coté et de l'autre à l'encaissement de toutes les créances de l'entreprise émis a la banque.

6. **Direction technique (DT) :**
   Elle assure une maintenance préventive et curative des engins du parc à conteneurs.

I.3 Présentation du service d'accueil (Centre Digitalisation et numérique) :

Il est basé sur un management de proximité, le Centre Digitalisation et Numérique (CDN) vise l'harmonisation,la cohérence,et la gouvernance des systèmes des ports. Cela nécessite une restructuration et un alignement pour perfectionner les services rendus aux client,en vue d'améliorer la compétitivité du secteur du transport maritime. L'objectif est aussi 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. Ce service contient plusieurs fonctions telles que :

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

Le chef du centre digitalisation et numérique a pour mission de uniformiser les processus en termes de digitalisation, d'automatisation d'infrastructures informatiques.

I.4 Activités de la BMT :

Bejaia Méditerranean Terminal reçoit annuellement un grand nombre de navires aux qu'elle assure les opérations de planifications, de manutention et d'acconage avec un suivi et une traçabilité des opérations.

I.4.1 Opération de planification :

- Planification des escales , programmation des accostages [3] et des postes à quai [4].
- Planification déchargement/chargement.
- Planification du parc à conteneurs (visite, dépotage, enlèvement et restitution des conteneurs vides au parc).
- Planification des ressources : Equipes et moyens matériels.

I.4.2 Opération de manutention :

La manutention est opérationnelle de jour comme de nuit, répartie en deux shifts de 07h00 à 13h00 et de 13h00 à 19h00 avec un troisième shift « over time » optionnel qui s'étale jusqu'à 07h00 du matin.

Elle comprend les opérations :

- D'embarquement, de débarquement des conteneurs.
- De réception des navires porte-conteneurs.

I.4.3 Opération d'acconage :

- Transfert des conteneurs vers les zones d'entreposage.
- Transfert des conteneurs frigorifiques vers les zones «reefers [5]».
- Suivi des visites du conteneur par les services concernés.
- Chargement de position des conteneurs.
- Suivi des livraisons et des dépotages.
- Suivi des restitutions et des mises à quai.

3. Accostage :manœuvre qui consiste, pour un navire ou une embarcation, à venir sans vitesse parallèlement à un quai ou à un autre navire afin de s'y amarrer.

4. Postes à quai (dock, quay, wharf) : structure en longueur située le long d'une voie navigable permettant aux navires de s'amarrer pour effectuer des opérations de chargement et de déchargement.

5. Reefers :Le terme reefer désigne un conteneur frigorifique.

- Mise à disposition des conteneurs vides pour empotage [6].

I.5 Objectifs de la BMT :

L'objectif de la BMT est de faire du terminal à conteneurs une infrastructure moderne tout en répondant aux exigences les plus élevées en matière de qualité dans le traitement des conteneurs et mettre à sa disposition une nouvelle technologie dans le traitement des conteneurs en vue d'assurer :

- Gain de productivité ;
- Réduction des coûts d'escale ;
- Fiabilité de l'information ;
- Meilleur service ;
- Sauvegarder la marchandise des clients ;
- Faire face aux concurrences nationales et internationales ;
- Propulser le terminal au stade international ;
- Gagner des parts du marché.

I.6 Missions de la BMT :

BMT a comme mission principale le suivi, la gestion et l'exploitation du terminal à conteneur.On peut citer :

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

• Manutention sur navire (aussi bien le chargement et le déchargement) des conteneurs et leurs entreposages dans les zones de stockage.

• Fournir les prestations de service d'acconage sur les aires spécialisées ainsi que leurs livraisons.

I.7 Etude de l'existant :

Une meilleure compréhension de l'environnement informatique aide à déterminer la portée du projet et la solution a implémenter.

6. Empotage : l'opération de chargement des marchandises à l'intérieur d'un conteneur.

I.7.1 L'aspect humain :

BMT dispose de :

- Chef de centre numérique et digitalisation (le directeur informatique).

- Ingénieur étude et développement(poste vacant).

- Ingénieur base de donnée (poste vacant).

- Administrateur réseaux (poste vacant).

- Administrateur système (poste vacant).

- 01 technicien en maintenance informatique.

I.7.2 L'aspect logiciel :

Les technologies utilisées :

- Platfrorme Java EE(JEE,EJB,JPA,Servlet et Oracle10g, entreprise Edition et Weblogic application server version 8.1).

- Platfrorme PHP et MySQL.

- Platforme NET (Internet).

Les applications existantes :

Plusieurs applications ont été développées parmi lesquelles :

- La gestion commerciale(bon de commande, facturation,...).

- La gestion des fiches navettes.

- Customer Relationship Management (CRM) : gestion de la relation client a pour objectif d'optimiser le traitement et l'analyse des données relatives aux clients et prospects.

- CTMS : système de gestion de terminal a conteneurs

- Le tableau de bord commercial.

- Gestion RH : ou gestion des ressources humaines (gestion des congés, gestion de paie, gestion des recrutements...).

- Plateforme EDI(COARRI et CODECO) : c'est une plateforme d'échange de données informatisées destinée a envoyer le rapport de chargement et déchargement des conteneurs sous format électronique.

I.7.3 Présentation du réseau de BMT :

Le réseau de BMT est un réseau ethernet, basé sur la topologie étoile. La norme de câblage utilisée est RJ45 selon les types de périphériques à connecter, et d'une liaison physique qui est la fibre optique, elle est utilisée pour transmettre des informations sur de longues distances, avec des débits binaires élevés.

I.7.4 Architecture du réseau de BMT :

Le réseau BMT est composé de quatre réseaux :

I.7.4.1 Le réseau Container Terminal Management System (CTMS) :

CTMS est un système de gestion à conteneurs propre à la BMT, utilisé par la direction d'opération ,basé sur une architecture client/serveur. Il se compose de deux serveurs de base de données hébergeant l'application CTMS exécutée sur Oracle,deux serveurs d'application TOMCAT et de deux serveurs Web Apache.
Les principales activités gérées par CTMS sont :la planification des escales qui est la mise a quai, la planification des chargements/déchargements qui nous donne virtuellement les positions des conteneurs en tenant compte de leurs poids sous format EDI(Echange de Données Informatisées),la planification du parc à conteneurs,et la planification des ressources.

I.7.4.2 Le réseau INTERNET LAN :

Le réseau LAN a un réseau sans fils et un réseau filaire. Son adresse est 192.168.10.0 avec un masque de 255.255.255.0 et disposé d'un serveur de fichiers et d'un serveur intranet pour gérer les applications de messagerie et du Web. Un serveur de caméras pour gérer les caméras de l'entreprise, un serveur Network Attached Storage (NAS) en tant que serveur de fichiers, qui stocke les données, et un réseau LAN de points d'accès connectés à un commutateur Cisco à 24 ports. Le réseau a des connexions physiques avec des fibres optiques pour distribuer les connexions aux émetteurs/récepteurs, aux routeurs Fortigate, puis cette connexion est transmise à un commutateur.

I.7.4.3 Le réseau Terminal Operation System IPROS :

Le réseau IPROS Terminal Operation System ou appelé (TOS),est un système complet de planification, d'exploitation et de surveillance des ressources qui peut être utilisé dans les terminaux à conteneurs.Il est basé sur architecture client/serveur.
Remarque : La BMT n'a pas encore mis en place le réseau IPROS.

I.7.4.4 Le réseau comptabilité :

C'est un réseau isolé avec un switch separé du reseau internet qui contient un serveur de comptabilité et un serveur de sauvegarde.

- **Architecture globale du réseau de BMT :**

Le réseau de la BMT est composé de deux parties distinctes : un réseau au niveau Ireyahane et un autre réseau situé au port de Bejaia (BMT). Ce dernier est divisé en deux sous-réseaux : l'un est situé dans l'ancien bâtiment et représente la direction des opérations, tandis que le

nouveau bâtiment représente la direction générale. Ces deux sous-réseaux sont interconnectés à l'aide d'un câble en fibre optique,la Figure I.5 ci-dessous montre l'architecture générale du réseau de la BMT :

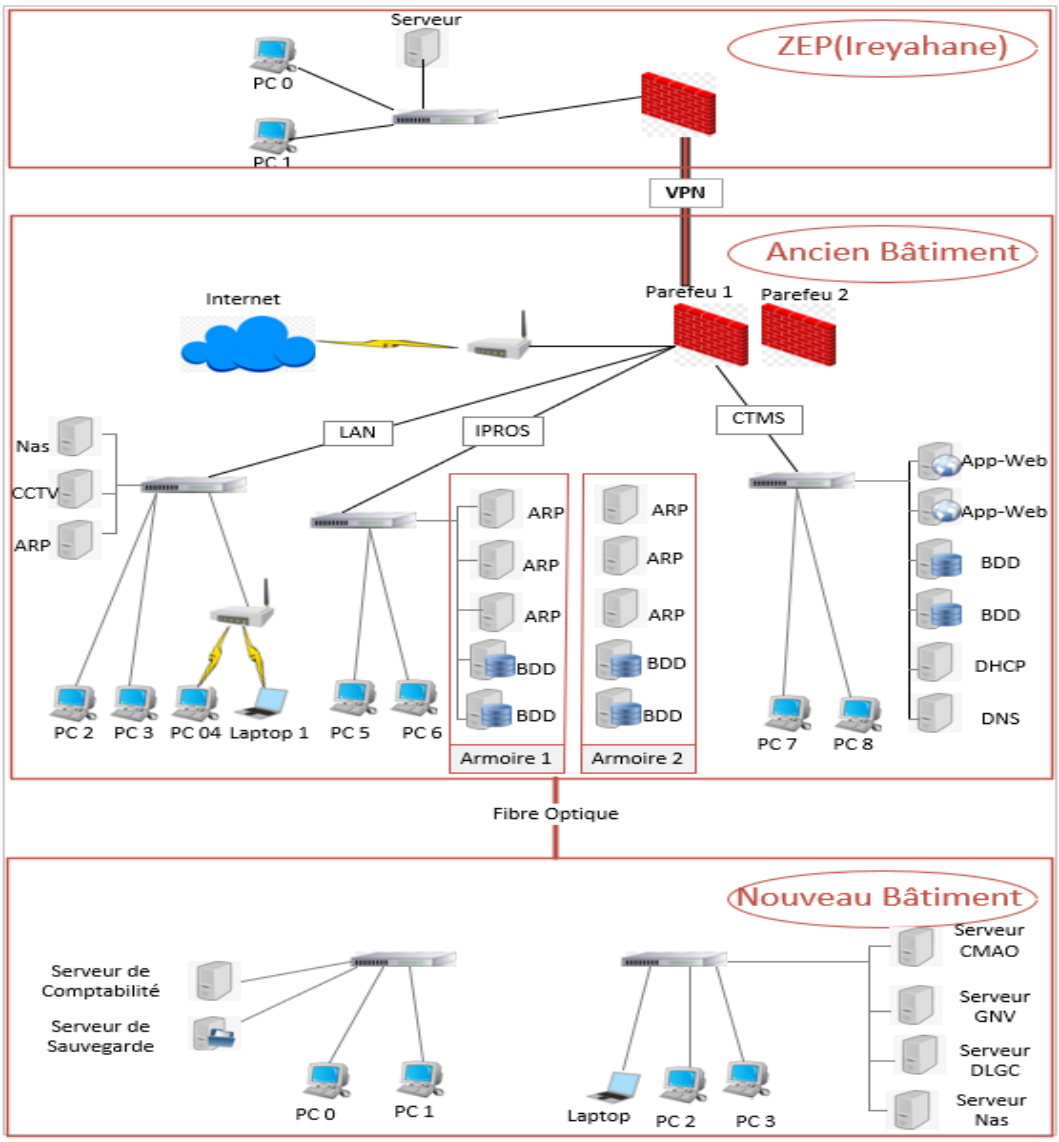

FIGURE I.5 – Architecture réseau générale de la BMT.

- Serveur GMAO : Gestion Maintenance Assisté par Ordinateur.

- Serveur GNV : Gestion d'investissement.

- Serveur DLGC : Logiciel de Gestion des stocks et Commerciale.

- Serveur NAS : Network Attached Storage ou Stockage en réseau.

- Serveur CCTV : un système de surveillance en circuits ouverts(caméras de surveillance).

I.7.5 Les caractéristiques des équipements terminaux et équipements de raccordement :

Le tableau(Table I.1) et le tableau(Table I.2) représentent respectivement les équipements de raccordement et les équipements terminaux de l'entreprise.

Équipement	Marque	Quantité	Caractéristique
Routeur	Fortinet Fortigate 100F	1	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.Slots .
Commutateur	Cisco SG200-26	15	26 ports RJ45 et 2 ports SFP.
Convertisseur	D-Link DMG-100	50	D-Link DMG-100.

Table I.1 – Les équipements de raccordement.

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
Onduleur	APC	130	\
Imprimante réseau	IPSON, CANON KY-GERA	8	\
Imprimante laser	HP	30	\
Caméra de surveillance	@Ihua	14	\
modem	ADSL	2	\

Table I.2 – Les équipements terminaux de la BMT.

I.7.6 Les services Intranet et internet de BMT :

1. **Les services Intranet :** les services intranet existant au BMT sont les suivants :

   - le courrier électronique.
   - l'accès a l'internet public.
   - l'accés aux données de l'entreprise.
   - la distribution et la publication d'informations.

- la gestion des documents.

2. **Les services Internet :** Internet offre une variété de fonctionnalités et d'avantages aux utilisateurs comme :

   - la messagerie électronique(E-mail).
   - la transfert des fichiers FTP.
   - le World Wide Web.

I.7.7 Politique de sécurité du réseau :

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

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

• **VPN virtuel et des lignes spécialisé privée :** qui relient le site distant Zone Extra Portuaire (ZEP) au BMT en utilisent les algorithmes de cryptographie.

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

• **Zone Démilitarisée (DMZ) :** la BMT dispose d'une DMZ dans son infrastructure reseau,elle est utilisée dans le but de renforcer la sécurité et de protéger les ressources sensibles de l'organisation.

I.8 Problématique :

Le réseau BMT comme n'importe quel autre réseau n'est pas sans faille en terme de sécurité réseau, à cause entre autres du nombre élevé de ses utilisateurs qui viennent de partout dans le monde.Au cours de nos visites au sein de l'entreprise, nous avons constaté des anomalies au niveau de la sécurisation du réseau de l'entreprise, nous les énumérons comme suit :

-**Remarque :** :Dans le réseau de la BMT, une infrastructure de redondance matérielle est déjà en place.

• Absence des serveurs d'administration et de gestion des compte et droits d'accés.

• Absence de la virtualisation qui permet de créer des représentations virtuelles de serveurs, de stockage, de réseaux et d'autres machines physiques.

• Absence de la haute disponibilité réseau et système.

• Un seul domaine de diffusion qui peut engendrer une surcharge réseau grâce aux tempêtes ARP.

I.9 Solution :

Nous suggérons les solutions suivantes :

• Installation des serveurs Active Directory et DHCP pour faciliter la gestion centralisée des utilisateurs et l'administration des addresses IP .

• Appliquer une solution de virtualisation.

• Appliquer le clustring et la réplication au niveau des serveurs et firewalls.

• Configuration des VLANs et private VLAN.

• Segmenter le domaine de diffusion en sous-domaines pour alléger le reseau et aporter la sécurité niveau 2 grâce à la virtualisation.

• Appliquer les protocoles de redondance comme Getway Load Balancing Protocol (GLBP) qui sert à equilbrer les charges entre deux routeurs ou switchs.

• Sécurisation de la DMZ avec des privates VLANs.

Conclusion :

A travers ce chapitre, nous avons introduit l'organisme d'accueil de BMT. Cette présentation nous a permis de mieux comprendre sa structure, ainsi que le rôle et les missions du département informatique, tout en dégageant les failles identifiées et citant les solutions proposées. Dans le chapitre suivant, nous allons présenter les objectifs de la sécurité informatique, les différentes attaques qui peuvent s'introduire ainsi quelques mécanismes de sécurité.

Chapitre II

Généralités sur la sécurité dans les réseaux informatique

Introduction

Avec le développement de l'utilisation d'internet,les entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.On parle de la securité informatique. Dans ce chapitre nous allons présenter la sécurité informatique .Pour l'objectif de bien identifier le domaine dans lequel nous souhaitons travailler.

II.1 la sécurité informatique :

II.1.1 Définition :

La sécurité informatique est l'ensemble des moyens et discipline mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces et protéger l'intégrité et la confidentialité des informations stockées dans un système informatique .
La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

II.1.2 Objectifs de la sécurité informatique :

La sécurité informatique vise généralement cinq principaux objectifs :

• **L'intégrité** qui garantit que les données sont bien celles que l'on croit être, qu'elles n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

• **La confidentialité** Assurer que l'information ne soit divulguée ou révélée qu'aux personnes autorisées. Pour obtenir ce service, on utilise généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique.[21]

• **La disponibilité** qui permet de garantir l'accès à un service ou à des ressources.

• **La non-répudiation** de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction.

• **L'authentification** qui consiste à assurer l'identité d'un utilisateur, c'est-à-dire à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple, par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.[22]

II.1.3 Terminologie de la sécurité informatique :

1. **Vulnérabilité :** c'est une faille ou un point ou le système et susceptible d'être attaqué.
2. **Les contre-mesures :** Ce sont les procédure ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

3. **Une politique de sécurité :** La politique de sécurité d'un réseau se fonde avant tout sur une analyse des risques décrivant les ressources critiques du réseau, ses vulnérabilités, les probabilités d'occurrences les menaces sur ces ressources vitales, ainsi que leurs conséquences. A partir de cette politique de sécurité, une architecture, des outils et des procédures sont définis et déployés afin de protéger les ressources critiques et de répondre aux objectifs de sécurité.

   L'établissement d'une politique de sécurité se fait selon les étapes suivantes :

   - Identification des vulnérabilités.
   - Evaluation des probabilités associées à chacune des menaces.
   - Evaluation du cout d'une intrusion réussie.
   - Choix des contres mesures.
   - Evaluation des couts des contre mesure.
   - Décision.

II.1.4 Attaques informatiques :

Les attaques sont des moyens d'exploiter des vulnérabilités qui reposent sur divers types de vulnérabilités, telles que des faiblesses de protocole, des faiblesses d'authentification, des faiblesses de mise en œuvre et des erreurs de configuration. Tous les ordinateurs en réseau sont vulnérables aux attaques. Et on peut distinguer deux catégorie d'attaques : attaque passive et attaque active. [23]

II.1.4.1 Les attaques passives :

Une attaque passive tente d'apprendre ou d'utiliser l'information du système, mais n'affecte pas ses ressources. relativement difficile à détecter, mais plus facile à prévenir .

II.1.4.2 Les attaques actives :

Une attaque active tente de modifier les ressources du système ou d'affecter leur fonctionnement Relativement difficile à éviter, mais plus facile à détecter .[?]

II.1.5 Types d'attaques :

Ci-dessous on cite quelque type d'attaques informatique qui peuvent se produire lorsque on se connecte à un réseau :

II.1.5.1 Attaque d'accès (interception) :

Une attaque d'interception est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information, et peut se produire par plusieurs techniques telles que : l'homme du milieu (Man-In-The-Middle)(Figure II.1), le sniffing, les chevaux de Troie, porte dérobée .[24]

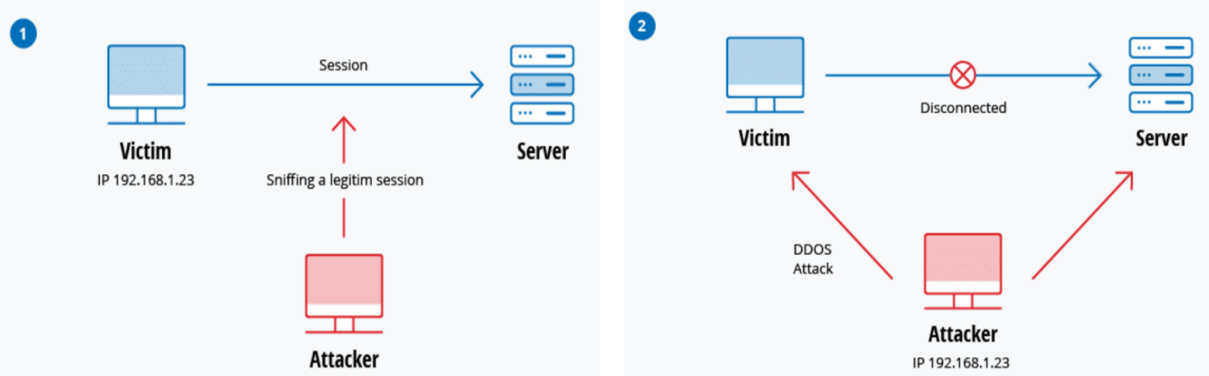

FIGURE II.1 – Attaque d'accès(l'homme du milieu).[3]

II.1.5.2 Attaque d'interruption :

Il s'agit d'une attaque sur la disponibilité, ce type d'attaque n'est pas géré directement par le mécanisme de sécurité mais par le mécanisme de rendez-vous. Ce dernier garantit la délivrance du message lors d'une communication. Si le rendez-vous échoue, le comportement actuel est de lever une exception afin d'en informer l'utilisateur .[24]

II.1.5.3 Attaque par rejeu :

L'attaquant qui a réussi à intercepter des messages les réémet dans le but d'obtenir des informations ou de perturber la cible de l'attaque. Nous considérons qu'il s'agit d'une attaque sur l'intégrité des messages.[24]

II.1.5.4 Attaque par déni de service :

Les attaques de type Denial-of-Service (Figure II.2) ont pour but de saturer un routeur ou un serveur afin de le crasher ou en préambule d'une attaque massive. Ces types d'attaque sont très faciles à mettre en place et très difficile à empêcher. Parmi les techniques utilisées pour réaliser ce type d'attaque on cite : le flooding, le débordement de tampon, le smurf.[25]

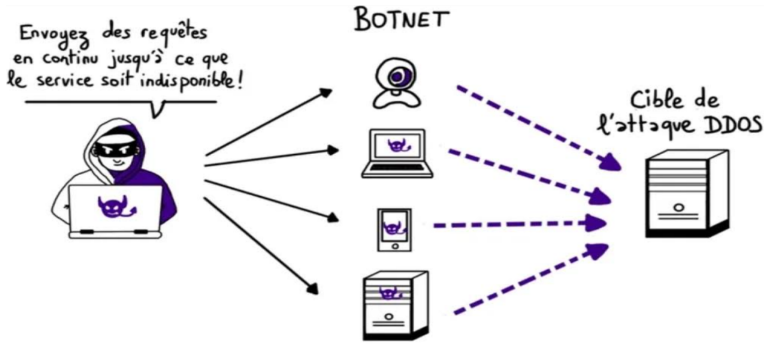

FIGURE II.2 – Attaque par déni de service.[4]

II.1.6 Les mécanismes de sécurité :

Les mécanismes de sécurité consistent en la mise en place de moyens et de dispositifs visant à protéger les systèmes d'information et à faire respecter les règles définies dans les politiques de sécurité. Parmi ces mécanismes, on peut citer :

II.1.6.1 La cryptographie :

Le chiffrement est le processus de cryptage utilisé pour rendre un document inintelligible sans la clé de décryptage. Le cryptage peut garder la signification d'un document privée, mais une communication sécurisée nécessite d'autres techniques de cryptage.

II.1.6.2 Le pare-feu :

Ensemble de divers composants matériels (physiques) et logiciels (logiques) qui contrôlent le trafic interne/externe conformément aux politiques de sécurité. Un système de pare-feu fonctionne la plupart du temps grâce à des règles de filtrage qui spécifient quelles adresses IP sont autorisées à communiquer avec les machines de votre réseau. En d'autres termes, un système de pare-feu est une passerelle de filtrage. Bien que cela soit utilisé pour empêcher les attaques et les connexions suspectes au réseau interne, les pares-feux sont souvent utilisés pour empêcher que des informations ne soient exposées sans protection. Obtenez un contrôle réel sur le trafic de votre réseau d'entreprise afin de pouvoir l'analyser, le protéger et le gérer. La (Figure II.3) ci-dessous présente un schéma d'une architecture réseau utilisant un Firewall.[26]

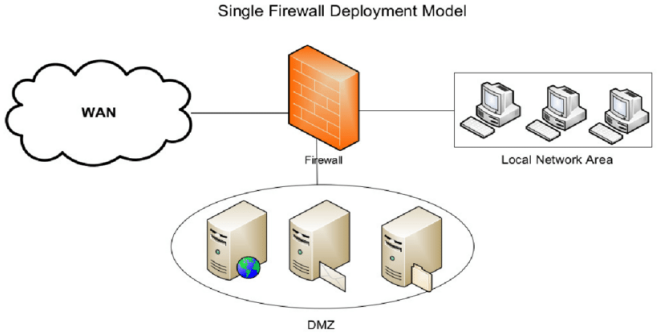

FIGURE II.3 – Schéma d'une architecture réseau utilisant un Firewall.[5]

II.1.6.3 Zone démilitarisée (DMZ) :

Une zone démilitarisée (DMZ) est une interface entre un réseau connu (le réseau interne) et un réseau externe (Internet). C'est un ensemble de règles de connectivité configurées dans le pare-feu qui fait de cette interface une zone physiquement séparée entre les deux réseaux. Cette séparation physique permet d'autoriser l'accès Internet à des serveurs situés dans la DMZ (Figure II.4) plutôt qu'à des serveurs dédiés sur un réseau privé (interne). [27]

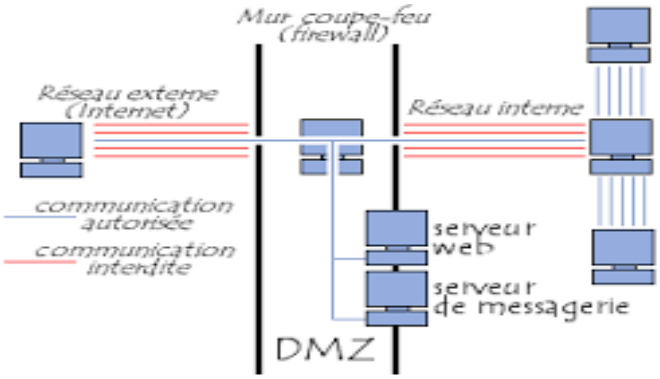

FIGURE II.4 – DMZ (zone démilitarisée).[6]

II.1.6.4 Les VPNs :

Un réseau privé virtuel (VPN) permet de créer une connexion privée sécurisée (réseau privé) sur un réseau public tel qu'Internet. Ils sont protégés par des tunnels établis entre les points d'accès VPN. Ces tunnels peuvent être protégés à l'aide de tunnels chiffrés de trames, de paquets ou de messages. Un pare-feu empêche le trafic indésirable d'entrer dans le réseau du client VPN et protège l'accès au réseau des utilisateurs. La (Figure II.5) présente le principe de fonctionnement d'un VPN.[7]

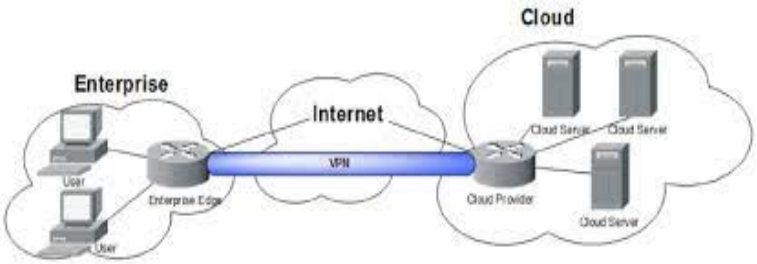

FIGURE II.5 – Principe de fonctionnement d'un VPN.[7]

Conclusion

Dans ce chapitre nous avons présenté la sécurité informatique d'une façon générale, nous avons cité les critères basiques qui montrent le rôle de la informatique, pour l'objectif de bien définir le concept d'administration et la sécurité d'un réseau au sein d'une entreprise.Dans le prochain chapitre on va aborder la virtualisation et la supervision des réseaux.

Chapitre III

La virtualisation et la supervision des réseaux

Introduction

Depuis quelques années, les entreprises s'intéressent de plus en plus aux technologies de virtualisation. Bien que ce concept ne soit pas nouveau, de nombreuses solutions sont actuellement mises en œuvre autour de la virtualisation.

Conquis par les capacités apportées par les outils de virtualisation, de nombreux Responsables informatiques se tournent vers cette technologie. En effet, ce procédé permet de configurer une machine physique en y installant plusieurs machines virtuelles. Ainsi, on a la possibilité d'utiliser plusieurs systèmes d'exploitation sur une même machine. Mais c'est surtout pour les serveurs que cette technologie prend toute son importance en optimisant la capacité et la puissance.

Ensuite, nous allons définir précisément le concept du monitoring ou la supervision des réseaux, ou nous verrons le fonctionnement du protocole le plus utilise actuellement : le protocole SNMP et quelques solutions de supervision .

III.1 La virtualisation :

III.1.1 Définition :

La virtualisation est un ensemble de techniques matérielles et/ou logicielles qui autorisent l'exécution de plusieurs applications indépendantes sur une même machine hôte. Grâce à la virtualisation, il est possible d'exécuter plusieurs systèmes d'exploitation (OS invité) sur un même serveur (Figure III.1). Ainsi, il n'est plus nécessaire d'utiliser un serveur par application. On parle souvent d'environnement virtuel (Virtual Environment – VE) ou de serveur privé virtuel (Virtual Private Server – VPS) lorsqu'une machine exploite la virtualisation. Pour bénéficier de cette technologie, il suffit d'équiper une machine d'un logiciel de virtualisation permettant d'ajouter une couche de virtualisation, appelée hyperviseur. Cet hyperviseur masque les véritables ressources physiques de la machine afin de proposer des ressources différentes et spécifiques en fonction des applications qui tournent. Il y a donc une totale indépendance entre le matériel et les applications. Le logiciel de virtualisation simule autant de machines virtuelles que de systèmes d'exploitation souhaité. Chaque OS croit alors qu'il est installé seul sur une machine alors qu'en réalité, plusieurs OS peuvent fonctionner en parallèle en partageant les mêmes ressources.[8]

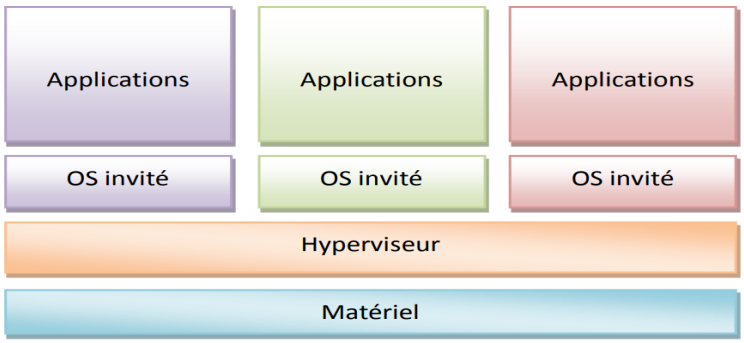

FIGURE III.1 – Les différentes couches d'un serveur virtualisé.[8]

III.1.2 Objectifs de la virtualisation

L'objectif principal de la virtualisation est l'usage efficient de ressources de calcul partagées entre plusieurs entités virtuelles : mémoire, processeur, réseau, stockage sont partagés efficacement dans la perspective d'économies d'échelle. Cet objectif correspond aux principes actuels de gestion des systèmes d'information. On a aussi la réduction des coûts. Cette réduction s'explique par la mutualisation des ressources qui permet de diminuer d'une part les besoins en matériel et de réduire d'autre part la consommation d'énergie électrique. De plus, le regroupement de plusieurs serveurs sur une même machine physique est sans perte de performance, la plupart des serveurs en entreprise n'exploitent qu'environ 10 à 15 % des ressources matérielles. La virtualisation offre également un déploiement et une migration facile des machines virtuelles d'une machine physique à une autre. L'administration des serveurs et des postes de travail devient aussi plus aisée.[8]

III.1.3 Architecture et fonctionnement de la virtualisation :

III.1.3.1 L'architecture de la virtualisation :

Il existe deux principaux types d'architecture de virtualisation : hébergée et bare-metal :

1. **Architecture hébergée :**Dans cette architecture, un système d'exploitation hôte est installé sur le matériel, suivi du logiciel. Le logiciel, qui est un hyperviseur ou un moniteur de machine virtuelle (MV), est nécessaire pour installer plusieurs systèmes d'exploitation invités ou MV sur le matériel afin de configurer l'architecture de virtualisation. Une fois l'hyperviseur en place, les applications peuvent être installées et exécutées sur les MV comme si elles étaient installées sur des machines physiques.

2. **Architecture bare-metal :**Dans cette architecture, un hyperviseur est installé directement sur le matériel plutôt qu'au-dessus d'un système d'exploitation. L'installation de l'hyperviseur et des machines virtuelles se déroule de la même manière qu'avec une architecture hébergée. Une architecture de virtualisation bare-metal convient aux applications qui fournissent un accès en temps réel ou effectuent un certain type de traitement de données.

III.1.3.2 Le fonctionnement de la virtualisation :

Le principe de la virtualisation repose sur 3 pivots majeurs que sont le système hôte, l'hyperviseur et le système invité. La combinaison de l'ensemble de ces entités permet de créer une virtualisation.

Sur le serveur utilisé, un système d'exploitation, également appelé système hôte, est installé pour assurer le fonctionnement de la machine. Il représente l'OS (operating system) principal pour accueillir les autres systèmes d'exploitation. Un logiciel de virtualisation nommé hyperviseur est alors installé sur le système hôte. Son rôle est de pouvoir créer des environnements sur lesquels d'autres systèmes d'exploitation seront hébergés. Ces derniers sont appelés systèmes invités. Chaque environnement, appelé machine virtuelle, fonctionne de manière indépendante, mais peut disposer des capacités du serveur physique en termes de ressources hardware. Les machines virtuelles bénéficient, donc, chacune d'un accès à la mémoire, au processeur ou encore à l'espace disque.

III.1.4 Les différents types de la virtualisation :

Il existe plusieurs types de virtualisation dont on peut citer [28] :

III.1.4.1 Virtualisation des serveurs :

La virtualisation des serveurs est le premier type de virtualisation rencontré. Cette technique implique la consolidation ou combinaison de plusieurs serveurs virtuels en un seul serveur physique plus grand et plus solide,à l'aide d'une couche logicielle. Chacune des machines virtuelles créée agit ensuite de manière autonome et isolée, exécutant ses propres système d'exploitation et applications.

Ce type de virtualisation repose sur le rôle de l'hyperviseur installé sur le serveur physique, qui assure la gestion des différents OS invités.

Il existe deux types d'hyperviseurs :

1. **l'hyperviseur de type 1, ou bare metal :**il opère directement sur le hardware, et devient de ce fait l'outil de contrôle du système d'exploitation. Les OS invités s'exécutent alors par dessus cet hyperviseur.
   Exemples d'hyperviseurs de type 1 : VSphere de l'éditeur VMware, ou KVM, l'hyperviseur libre pour Linux.

2. **l'hyperviseur de type 2, ou host metal :** il fonctionne à l'intérieur d'un autre système d'exploitation.
   Exemples d'hyperviseurs type 2 : VirtualBox, logiciel Open Source édité par Oracle.

III.1.4.2 Virtualisation des systèmes d'exploitation :

La virtualisation des systèmes d'exploitation, utilisée parfois à l'échelle domestique, permet d'exécuter sur une seule et même machine plusieurs OS différents, n'interférant pas les uns avec les autres.
Exemple :installer sur un même ordinateur d'un environnement Windows ,un environnement Linux.

III.1.4.3 Virtualisation des postes de travail :

Un des types de virtualisation fortement apprécié et usité en entreprise est la virtualisation des postes de travail, ou virtualisation desktop. Cette technique reproduit l'environnement d'un ordinateur, afin d'offrir la possibilité aux professionnels d'accéder à leurs fichiers et applications personnelles depuis n'importe quel poste.

Ce type de virtualisation est rendu possible grâce à l'hébergement du poste de travail virtuel sur un serveur VDI (Virtual Desktop Infrastructure) qui exécute l'ensemble de l'environnement du poste (système d'exploitation et applications).

III.1.4.4 Virtualisation des applications :

La virtualisation des applications lorsque celles-ci s'exécutent sous une forme encapsulée (regroupement des données brutes) et indépendante du système d'exploitation sous-jacent.
Exemple :utiliser une application Linux sur un environnement Windows.

III.1.4.5 Virtualisation du stockage :

La virtualisation du stockage (appelée également Software Defined Storage, ou SAN (Storage Area Network) virtuel) consiste à regrouper l'ensemble des périphériques de stockage physiques en un seul périphérique simulé. Ce dernier est géré depuis une console centrale. Une solution telle que SAN symphony, développée par DataCore,permet de placer une couche de virtualisation évolutive sur les infrastructures de stockage. De la sorte, la cohabitation entre différents matériaux de stockage est possible.

III.1.4.6 Virtualisation de réseau :

La virtualisation du réseau, (ou network virtualisation), est le processus qui reproduit un réseau physique basé sur le matériel (ports, routeurs, etc.) en un réseau basé sur le logiciel.elle permet de fournir des fonctions réseau, des ressources matérielles et des ressources logicielles indépendamment du matériel, sous la forme d'un réseau virtuel.

III.1.5 Les avantages de la virtualisation :

Faire le choix de la virtualisation pour son entreprise, c'est bénéficier de plusieurs avantages :

- **Des coûts réduits :** la virtualisation implique moins de serveurs, moins de place pour les héberger, moins de coûts de maintenance, etc. .

- **Des économies d'énergie :** moins de serveurs équivalant à moins de pollution numérique .

- **Une meilleure exploitation des ressources :** jusqu'alors souvent sous-exploitées, les capacités matérielles de l'entreprise sont fortement optimisées grâce à la virtualisation.

- **Une continuité d'activité :** en cas de sinistre ou d'interruption, la virtualisation facilite le plan de reprise d'activité.

- **Une meilleure agilité :** en permettant de s'affranchir des contraintes matérielles, la virtualisation encourage la flexibilité des processus et la mobilité des équipes.[28]

III.1.6 Les inconvénients de la virtualisation :

Comme la virtualisation a plusieurs avantages,elle a aussi des inconvénients comme :

- **Complexité :** La virtualisation ajoute une couche de complexité à l'infrastructure informatique. Cette complexité peut rendre difficile la gestion des machines virtuelles, ce qui entraîne une augmentation des coûts de gestion.

- **Sur-coût de performance :** La virtualisation introduit une surcharge de performance en raison de la couche supplémentaire de logiciel entre le matériel et le système d'exploitation. Cela peut se traduire par un ralentissement des performances de certaines applications.

• **Risques de sécurité :** La virtualisation introduit de nouveaux risques de sécurité, tels que la possibilité d'attaques par évasion de la machine virtuelle. Ces attaques peuvent compromettre la sécurité de l'ensemble de l'infrastructure virtuelle.

• **Problèmes de licence :** La virtualisation peut poser des problèmes de licence aux fournisseurs de logiciels. Certains vendeurs n'autorisent pas l'exécution de leurs logiciels dans un environnement virtualisé ou facturent des frais supplémentaires pour la virtualisation.[29]

III.1.7 Les solutions de la virtualisation :

III.1.7.1 Xen :

Xen est un logiciel libre de virtualisation.Il permet l'exécution de plusieurs systèmes d'exploitation de manière isolée sur une même machine physique. Les systèmes d'exploitation exécutés ou invités partagent les ressources de la machine hôte. Xen est un « hyperviseur de type 1 ».

III.1.7.2 Kernel-based Virtual Machine (KVM) :

(Kernel-based Virtual Machine) KVM est une solution de virtualisation open source destinée à Linux. Il est conçu pour les architectures x86 utilisant la technologie Intel VT (Virtual Technology) et est intégré au noyau Linux depuis la version 2.6.20. Contrairement à d'autres logiciels tels que VirtualBox, KVM utilise le noyau du système d'exploitation hôte pour émuler des machines virtuelles, qu'il s'agisse d'ordinateurs ou de serveurs physiques. En d'autres termes, KVM est un module de noyau chargé pour Linux qui tire parti des technologies de virtualisation matérielle. Chaque machine virtuelle créée avec KVM dispose de ses propres ressources dédiées, notamment les interfaces CPU, la mémoire RAM et les interfaces réseau.

III.1.7.3 VSphere Elastic Sky X Integrated 7 (ESXi7) :

ESXi 7 est une plateforme de virtualisation développée par VMware, un leader dans le domaine de la virtualisation des serveurs. ESXi est le composant principal de la solution VMware vSphere, qui permet de créer et de gérer des environnements de virtualisation. Il s'agit d'un hyperviseur de type 1, ce qui signifie qu'il s'exécute directement sur le matériel physique sans nécessiter de système d'exploitation hôte. Cela permet une utilisation plus efficace des ressources matérielles et une meilleure performance.

ESXi 7 offre une virtualisation complète du matériel, ce qui permet de faire fonctionner plusieurs systèmes d'exploitation et applications sur un seul serveur physique. Il prend en charge différents types de machines virtuelles, telles que les machines virtuelles Windows, Linux et d'autres systèmes d'exploitation. Il offre également des fonctionnalités avancées telles que la migration à chaud des machines virtuelles, la haute disponibilité, la gestion centralisée, la sécurité renforcée et l'automatisation. Il permet aux entreprises de consolider leurs serveurs physiques en un nombre réduit de serveurs virtuels, ce qui permet des économies de coûts et une gestion plus efficace de l'infrastructure informatique.

III.1.7.4 OpenVz :

OpenVZ est une technologie de virtualisation au niveau du système d'exploitation du noyau Linux.Il permet à plusieurs instances de s'exécuter sur un seul serveur physique, appelé Serveurs privés virtuels (VPS) ou environnement virtuel (VE). Les machines virtuelles telles

que VMware, la paravirtualisation comme Xen ou OpenVZ réduisent la flexibilité dans la sélection du système d'exploitation .Les systèmes d'exploitation invités et hôtes doivent être de type Linux (mais les distributions Linux peuvent varier d'un VE à l'autre). mais la virtualisation au niveau du système d'exploitation d'OpenVZ offre de meilleures performances : évolutivité, densité accrue et meilleure gestion dynamique des ressources.

III.1.7.5 Linux Containers (LXC) :

Le noyau Linux 2.6.24 inclut une prise en charge de conteneurisation de base pour fournir une virtualisation au niveau du système d'exploitation et permet à un seul hôte plusieurs instances Linux isolées , appelées « Conteneurs Linux ».Il est basé sur les ressources (en particulier les processeurs, la mémoire et l'accès aux E/S) sans s'appuyer sur un environnement virtuel complet sur le concept de groups (les groupes de contrôle Linux) ,chaque groupe de contrôle offre aux applications une isolation totale des ressources, et ce sans recourir à des machines virtuelles . Les conteneurs Linux fournissent également une isolation complète de l'espace de noms. Les fonctionnalités telles que le système de fichiers, l'identité du réseau et l'identité de l'utilisateur. Par conséquent, d'autres facteurs généralement associés aux systèmes d'exploitation peuvent être pris en compte.

III.1.7.6 Cloud Computing :

Le Cloud Computing est la pratique consistante à fournir des services informatiques à distance, en les hébergeant dans un ou plusieurs centres de données externes plutôt que sur des serveurs dédiés sur place. Plutôt que d'acheter et de déployer en interne les ressources numériques dont elles ont besoin, les organisations peuvent y accéder à distance via un fournisseur de services cloud. Parmi les avantages de Cloud Computing : Vitesse de déploiement,sécurité renforcée,contrôle des coûts,évolutivité,etc.La Figure III.2 ci-dessous présent une simple architecture de Coud Computing.

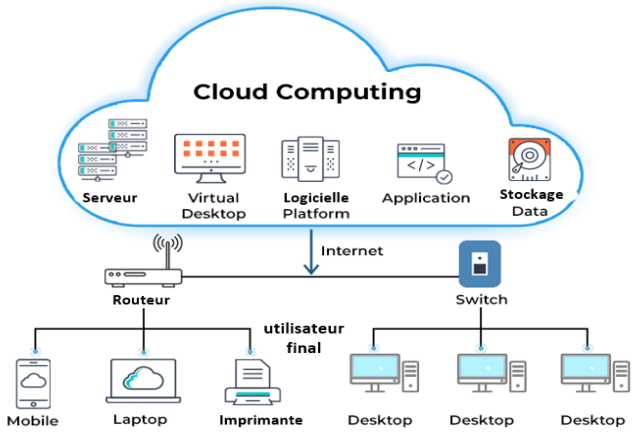

FIGURE III.2 – Architecture de Cloud Computing.[9]

III.2 La supervision des réseaux informatiques :

III.2.1 Définition :

La supervision du réseau est une exigence essentielle pour les entreprises qui dépendent fortement de l'informatique pour leurs opérations quotidiennes.De nombreuses entreprises déploient la supervision de réseau comme un moyen de réduire les problèmes d'infrastructure de réseau, d'améliorer les performances du réseau et d'augmenter la productivité des employés.La supervision du réseau est un élément essentiel pour maintenir le bon fonctionnement du réseau interne.

III.2.2 Le concept de supervision réseaux :

La supervision réseau fait référence à la surveillance du bon fonctionnement des réseaux informatiques et des services informatiques connectés sur ces réseaux.Cette dernière porte plus spécifiquement sur :

- la qualité (bande passante).
- la sécurité de la connexion Internet.
- mais aussi, par extension, à l'état des services et matériels connectés : serveurs, imprimantes, postes de travail, etc.

III.2.3 Type de supervision et actions liées :

Il existe plusieurs types de supervision des réseaux :[30]

1. **Supervision système :**
   Ce type de supervision (surveillance) couvre essentiellement toutes les ressources des différents systèmes d'exploitation : mémoire RAM, stockage de masse, système RAID, etc.
2. **Supervision réseau :**
   Ce type de supervision est basé sur le principe de surveiller le réseau et ses équipements. L'idée est de vérifier que ce réseau fonctionne , aucun port ou convertisseur d'interface gigabyte n'est défectueux et la connexion fonctionne . De plus, un contrôle continu de la disponibilité du service de fonctionnement, vitesse et sécurité , ainsi que contrôle de flux .
3. **Supervision applicative :**
   Supervision des applications (ou surveillance applicative) permet de connaître la disponibilité des machines liées aux services fournis en testant les applications hébergées sur le serveur . La surveillance des applications comprend également la mesure des flux de service appelé validation fonctionnelle.Elle se focalise sur les applications, en examinant trois points : leur disponibilité, leur performance, et l'intégrité des données.
4. **Supervision métier :**
   c'est le suivi des différents processus métiers, un emploi peut dépendre de plusieurs applications. Il est donc important de s'assurer qu'ils sont tous actifs et valides et en bon état.

III.2.4 La norme ISO du point de vue de la gestion des réseaux :

La gestion du réseau ne se limite pas à assurer le bon fonctionnement d'un matériel. L'organisation internationale de normalisation (ISO) énumère cinq facteurs clés que les services informatiques doivent prendre en compte dans leur programme de gestion de réseau.[31]

• **Gestion de performances :** Son but est d'assurer des niveaux de service acceptables dans le réseau afin d'optimiser les opérations commerciales.Recueillir des statistiques périodiques sur la qualité des services réseau. Les outils de surveillance du réseau collectent des données de performance à l'aide de diverses métriques et les transmettre aux applications de surveillance des performances. Ils produisent et analysent des statistiques sur des métriques telles que l'utilisation de la connexion, le taux de perte de paquets, le temps de réponse du réseau, etc.

• **Gestion des configurations :** Elle ne se résume pas à l'installation initiale des routeurs, commutateurs, serveurs ou autres périphériques réseau. Cela inclut la surveillance continue des modifications apportées à la configuration du système. Les problèmes de configuration sont l'une des principales causes de pannes. Les entreprises doivent donc utiliser des outils efficaces et mettre en œuvre les meilleures pratiques pour gérer tous les aspects de la gestion de la configuration.

• **Gestion de comptabilité :** Elle est destinée à collecter des informations sur l'utilisation du réseau .Elle est affectée à des fins de comptabilité, de facturation ou de suivi de la consommation de divers services ou domaines d'activité. Les facturations ne sont pas destinées aux petites entreprises qui ne sont pas organisées en plusieurs services, mais toutes les entreprises et tous les gouvernements doivent surveiller leur utilisation du réseau.

• **Gestion de la sécurité :** La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisations établies. Elle veille à ce que les utilisateurs non autorisés ne puissent accéder à certaines ressources protégées.

III.2.5 Les protocoles de supervision :

Les systèmes de supervision utilisent des protocoles, très réglementés par la DMTF (Distributed Management Task Force) depuis 2005. Parmi les principaux protocoles utilisés, on peut citer quelques uns [32] :

1. **Protocole Intelligent Platform Management Interface (IPMI) :** IPMI est largement utilisé comme l'une des interfaces les plus populaires, il concerne surtout les serveurs et cette interface intelligente de gestion de matériel permet de contrôler à distance certains composants très sensibles comme les sondes et autres ventilateurs.

2. **Protocole Java Management Interface (JMX) :** C'est l'API(application programming interface), qui permet de gérer une application en cours d'exécution. JMX est maintenant complètement intégré dans J2E à partir de la version V.

3. **Protocole Common Information Model (CIM) :** Le modèle CIM (Common Information Model) est une méthode de représentation des divers dispositifs informatiques activement utilisés associés à une entreprise. CIM est conçu et publié par le DMTF .Ce protocole vise à simplifier la tâche de gestion des différents appareils informatiques dans une entreprise.

4. **Protocole Simple Network Management Protocol (SNMP) :** C'est le protocole de communication et de gestion du réseau simplifiée . SNMP permet aux administrateurs de contrôler et de gérer tous les éléments actifs du réseau.

III.2.6 Le protocole Simple Network Management Protocol (SNMP) :

III.2.6.1 Présentation :

Proposé par l'IETF(Internet Engineering Task Force) en 1988 pour la gestion des environnements TCP/IP. SNMP est devenu le protocole de gestion de référence en raison du succès des protocoles de l'IETF (tels que IP, TCP). Cet environnement est actuellement le plus déployé et utilisé.

- Deux ports sont désignés pour l'utilisation de SNMP :

- Port 161 pour les requêtes à un agent SNMP.

- Port 162 pour l'écoute des alarmes destinées à la station d'administration. [33]

III.2.6.2 Architecture du protocole SNMP :

L'environnement de gestion SNMP est composé de plusieurs entités : la station de supervision, les éléments actifs du réseau, la MIB et un protocole (Figure III.3). Les éléments actifs du réseau sont les équipements ou les logiciels que l'on cherche à gérer. Cela va d'un poste de travail à un concentrateur, un routeur, un pont, etc. Chaque élément du réseau dispose d'une entité dite agent qui répond aux requêtes de la station de supervision[10].

• **La station de supervision :** (appelée aussi manager) exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail.

• **Les MIBs :**(Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules MIB spécifiques.

• **Le protocole :**qui permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

III.2.6.3 Fonctionnement du SNMP :

Le protocole SNMP repose sur la présence de : station de supervision (Manager), les éléments actifs du réseau, les variables MIB et des agents SNMP, les agents sont généralement des interfaces SNMP intégrées au matériel cible qui peut être géré à distance.
Le protocole SNMP dispose de plusieurs commandes telles que : [10] :

•**Get :**Cette commande, envoyée par le manageur à l'agent, a pour objectif de demander une information à l'agent. Celui-ci, dans le cas où la validité de la requête est confirmée, renvoie au manageur la valeur correspondant à l'information demandée.

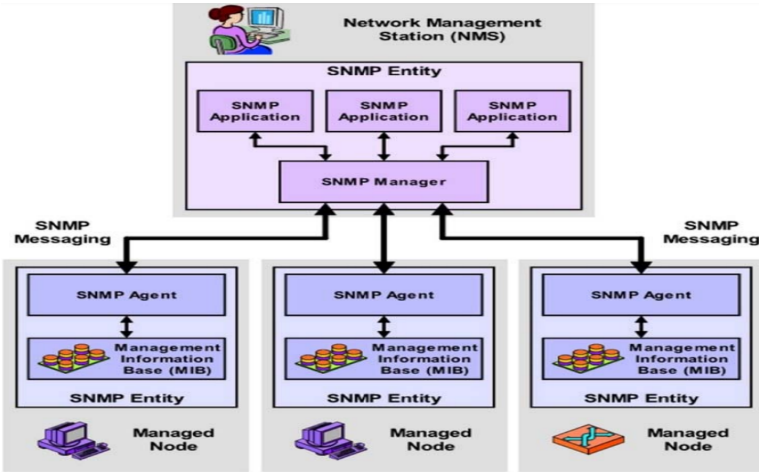

FIGURE III.3 – Architecture du protocole SNMP[10].

•**Getnext :** Cette commande, envoyée par le manageur à l'agent, a pour objectif de demander l'information suivante à l'agent : il arrive qu'il soit nécessaire de parcourir toute une liste de variables de l'agent. On utilise alors cette commande, à la suite d'une requête 'get', afin d'obtenir directement le contenu de la variable suivante.

•**Getbulk :** Cette commande, est envoyée par la manageur à l'agent pour connaître la valeur de plusieurs variables : cela évite d'effectuer plusieurs requêtes Get en série, améliorant les performances (implémenté dans SNMPv2).

•**Set :** Cette commande, envoyée par le manageur à l'agent, a pour objectif de définir la valeur d'une variable de l'agent administré. Cela permet d'effectuer des modifications sur le matériel.

•**Trap :** Lorsqu'un événement particulier survient chez l'agent (connexion, modification de la valeur d'une variable donnée, etc…), celui-ci est susceptible d'envoyer ce que l'on appelle une « trap », qui est un message d'information destiné à la station d'administration : celle-ci pourra alors la traiter et éventuellement agir en conséquence

•**Inform :** il peut être intéressant pour l'agent d'obtenir une réponse à une Trap qu'il a émise, afin d'obtenir confirmation que celle-ci a bien été reçue et analysée : c'est l'objectif d'une commande « inform ». (Implémenté dans SNMPv2).

III.2.7 Solutions de supervision :

Parmi les solutions de supervision informatique on cite[34] :

1. **NAGIOS :** Nagios est le logiciel de surveillance le plus connu.Utilisé pour la surveillance du système et du réseau. il supervise des hôtes et des services spécifiques et émet des alertes lorsque des erreurs système se produisent. Il envoie également des alertes lorsque le système revient à la normale. Le logiciel excelle à fournir des résultats dans diverses représentations visuelles et rapports.Les administrateurs système peuvent hiérarchiser les résultats et les données reçues en fonction de leurs préférences.

   Nagios fonctionne grâce à trois composants principaux (Figure III.4) :

• L'ordonnanceur qui est le cœur du logiciel. Il a pour rôle d'ordonnancer les tâches de supervision.

• L'interface web sur laquelle on peut voir les informations et les données qui concernent les éléments supervisés.

• Le plugin qui assure des missions plus spécifiques. On peut les ajouter ou les désinstaller fonction des besoins.

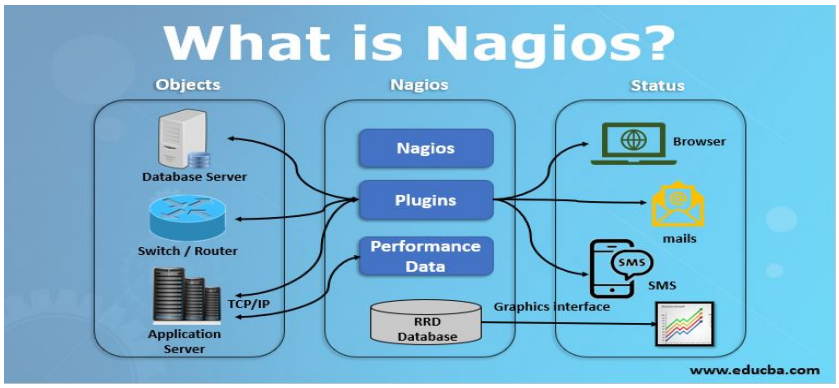

FIGURE III.4 – Architecture de nagios.[11]

2. **Zabbix :** C'est une solution de supervision réseau gratuite et open source(Figure III.5). Il utilise un modèle client-serveur dans lequel un serveur Zabbix obtient des informations de surveillance de son agent Zabbix. Les fonctionnalités fournies par Zabbix incluent la surveillance des performances, la surveillance des applications, la rapidité et la simplicité de la configuration des modèles de surveillance, la découverte automatique, des alertes et des rapports. Zabbix ne couvre pas seulement la surveillance de l'état, mais également la surveillance des performances du SI(Système d'Information).

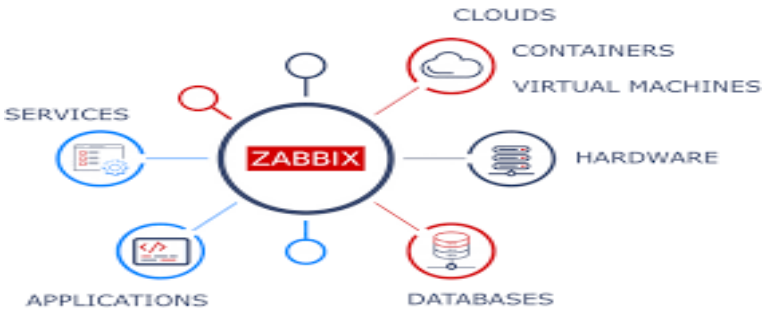

FIGURE III.5 – Solution ZABBIX.[12]

3. **CACTI :** C'est un logiciel libre qui se présente comme une solution complète de supervision de l'infrastructure informatique avec une interface Web. Il fonctionne sur Windows et Linux OS et offre plusieurs fonctionnalités comme : surveillance du serveur, cartographie réseau, alertes (SMS, e-mail), rapports, gestion de la configuration du réseau, analyse du trafic réseau. CACTI est incapable de faire la corrélation d'alertes en cas d'incident.

4. **CENTREON :** Ce logiciel supervise les SI des sites et bâtiments les plus importants comme celui du Ministère de la Justice de certains pays. À sa création, Centreon avait pour ambition de faire mieux que Nagios.

   Son tableau de bord diffuse en temps réel des informations telles que l'utilisation du processeur, de la RAM, de l'espace du disque dur, les périphériques connectés…, il permet de vérifier l'état des serveurs supervisés et la disponibilité des matériels informatiques connectés au SI. Sa vraie puissance réside aussi dans le fait qu'il offre à celui qui supervise la possibilité de faire une configuration personnalisée.

Conclusion

A travers ce chapitre, la virtualisation semble s'être imposée comme un élément incontournable au sein des entreprises et ce sont principalement les serveurs qui sont au centre de toutes les attentions, dans la deuxième partie on défini l'aspect de supervision, et aborder le protocole SNMP, et on a fini par citer quelques solutions de monitoring . Le chapitre suivant va porter sur la haute disponibilité.

Chapitre IV

La haute disponibilité

Introduction

La haute disponibilité est devenue un standard pour les entreprises, voire également un argument de vente. Vous verrez souvent marqué sur les sites de vente de service « SLA 99,99% ». SLA signifiant « Service Level Agreement », c'est l'assurance de la qualité du service fourni. Nous pourrions nous demander « Pourquoi ne pas mettre 100%, mes serveurs n'ont jamais été inaccessibles, n'ont jamais perdu la connexion au réseau ». Effectivement, dans la pratique et pour la majorité des personnes, ce taux s'approche des 100%, cependant l'informatique étant ce qu'il est, le risque zéro n'existe pas.,

Aujourd'hui, c'est un enjeu essentiel. Pour qu'une entreprise puisse se développer et fonctionner, un système d'information disponible et fiable est primordial. Auquel cas, il y a un risque de pertes de productivité, de matériels, mais également de coûts supplémentaires (liées aux pannes, aux ressources à déployer, etc.)[35]

IV.1 Définition :

La haute disponibilité (ou High Availability ou HA) permet d'assurer et de garantir le bon fonctionnement des services et applications. Cela consiste donc à mettre en place toutes les actions et dispositions techniques pour qu'une infrastructure informatique soit toujours disponible en appliquant certains principes tels que la réplication des données, la sauvegarde, la répartition de la charge, la redondance,...etc. [36]

IV.2 La nécessité de la haute disponibilité :

Pour un réseau informatique , la haute disponibilité est mesurée en termes d'expérience et d'attentes de l'utilisateur final. L'impact concret et perceptible du temps mort peut être exprimé en termes de perte d'informations, de dégâts matériels, de baisse de la productivité, ou de perte de clientèle.

La nécessité principale d'une solution de haute disponibilité est de minimiser ou d'atténuer l'impact du temps mort. Une bonne stratégie consiste à équilibrer de manière optimale les processus d'entreprise et les contrats SLA par rapport aux capacités techniques et aux coûts d'infrastructure.

Une plateforme est considérée comme hautement disponible conformément à l'accord et aux attentes des clients et des parties prenantes. La disponibilité d'un système peut être exprimée sous la forme du calcul suivant :

$$\frac{\textbf{Temps de fonctionnement réel}}{\textbf{Temps de fonctionnement attendu}} \textbf{ X 100 \%}$$

La valeur résultante est souvent exprimée en nombre de 9 fournis par la solution. Cela permet d'indiquer un nombre annuel de minutes de temps de fonctionnement possible, ou à l'inverse, un nombre de minutes de temps mort (Table IV.1).[36]

Nombre de 9	Pourcentage de disponibilité	Total de temps mort annuel
2	99 %	3 jours, 15 heures.
3	99,9 %	8 heures, 45 minutes.
4	99,99 %	52 minutes, 34 secondes.
5	99,999 %	5 minutes, 15 secondes.

TABLE IV.1 – Le Pourcentage de disponibilité paraport au nombre de 9.

IV.3 Les ressources critiques d'un système informatique :

La panne d'un système informatique peut causer une perte de productivité et d'argent, voir des pertes matérielles ou humaines dans certains cas critiques. Il est essentiel d'évaluer les risques liés à un dysfonctionnement d'une des composantes du système d'information et de prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident. Les risques de pannes d'un système informatique en réseau sont nombreux, l'origine des fautes peut être schématisée de la manière suivant.[13]

1. **Origines matérielle :**Elles peuvent être d'origine naturelle ou humaine :
   - Désastre naturel (inondation, séisme, incendie).
   - Environnement (intempéries, taux d'humidité de l'air, température).
   - Panne matérielle.
   - Panne du réseau.
   - Coupure électrique.
2. **Origines humaines :** Elles peuvent être soit intentionnelles soit fortuites :
   - Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau).
   - Sabotage.
   - Piratage.
3. **Origines opérationnelles :** Elles sont liées à un état du système à un moment donné :
   - Bogue logiciel
   - Dysfonctionnement logiciel.

IV.4 les solutions existantes :

Il existe diverses solutions disponibles pour assurer une haute disponibilité telles que :

IV.4.1 La redondance matérielle :

L'une des possibilités est d'avoir un réseau qui tient la charge sans pour autant avoir de coupure dans son utilisation, est la redondance. C'est-à-dire dupliquer de composants, d'éléments de liaisons ou de données essentielles d'un système, tout en étant au maximum transparent pour les utilisateurs. Grâce aux doublons, une entreprise peut garantir les fonctionnalités de son centre informatique dans l'éventualité ou un dysfonctionnement.

Les protocoles de redondance :

Il existe plusieurs protocoles de redondance disponibles pour assurer une meilleure disponibilité des systèmes comme :

1. **Virtual Router Redundancy Protocol (VRRP) :**
   Le protocole de redondance pour le routeur virtuel (en anglais VRRP) élimine le seul point d'échec inhérent à un environnement routé par défaut et en statique. VRRP spécifie un protocole d'élection qui assigne dynamiquement les responsabilités pour un routeur virtuel à un concentrateur VPN provenant d'un réseau LAN. Le routeur VRRP, qui contrôle les adresses IP associées est appelé maître.Quand le maître est indisponible, un back up concentrateur VPN prend la place du maître.[37]

2. **Link Aggregation Control Protocol (LACP) :**

   Le protocole LACP (Link Aggregation Control Protocol) est un protocole utilisé dans les réseaux informatiques pour agréger plusieurs liens physiques entre des commutateurs (switches) et former une liaison logique appelée agrégation de liens, trunk ou EtherChannel. LACP offre plusieurs avantages, notamment l'augmentation de la capacité de bande passante, l'amélioration de la disponibilité et la fourniture d'une redondance en cas de défaillance d'un des liens physiques. De plus, LACP fournit une redondance en cas de défaillance d'un des liens physiques. Lorsque les liens sont agrégés, LACP surveille en permanence leur état. Si l'un des liens est déconnecté ou rencontre un problème, LACP détecte cette défaillance et redirige automatiquement le trafic vers les liens restants du groupe agrégé.

3. **Gateway Load Blancing Protocol (GLBP) :**
   Le protocole GLBP (Gateway Load Balancing Protocol) est un protocole de routage qui permet de distribuer la charge de trafic entrant sur plusieurs passerelles par défaut (gateways) dans un réseau. Contrairement à d'autres protocoles de routage, tels que HSRP ou VRRP, GLBP offre une répartition de charge active-active, ce qui signifie que toutes les passerelles actives peuvent répondre aux requêtes des clients. GLBP utilise un algorithme de sélection pour choisir dynamiquement la passerelle par défaut active pour chaque client, offrant ainsi une meilleure utilisation des ressources du réseau. En cas de défaillance d'une passerelle active, GLBP peut rapidement basculer le trafic vers une autre passerelle disponible, garantissant ainsi une continuité du service et une redondance élevée dans l'environnement réseau.[13]

4. **Spanning-Tree Protocol (STP) :**
C'est un protocole réseau standardisé IEEE 802.1d qui permet de définir une topologie sans boucle dans un LAN composé de switches, STP protège des domaines d'émission de la couche 2 contre des saturations de diffusion. Il place les liens au mode standby pour empêcher des boucles dans le réseau. Pour assurer la fiabilité des liaisons entre des commutateurs du réseau, la mise en œuvre d'une topologie redondance est primordiale. si les commutateurs acheminent le trafic de diffusion et multicast par tous les ports sauf celui d'origine et si les rames Ethernet ne disposent pas de durée de vie (TTL), plusieurs problèmes peuvent s'apparaître :[38]

A) **Le " spanning tree " en trois étapes :**

Étape 1 : élection du root bridge : Le root bridge est sélectionné parmi les commutateurs du réseau. Il agit comme le commutateur principal et définit la racine du Spanning Tree.

Étape 2 : sélection des ports désignés : Chaque commutateur choisit les ports qui offrent le chemin le plus court vers le root bridge pour chaque segment du réseau. Ces ports sont désignés comme les ports préférentiels pour acheminer le trafic.

Étape 3 : désactivation des ports redondants : Les ports non sélectionnés sont désactivés ou mis en état de blocage pour éviter les boucles dans le réseau. Cela permet de créer une topologie sans boucle et d'assurer une commutation efficace et fiable.[39]

B) **Problèmes du Spanning-Tree : [13]**

i. **Tempête de diffusion :**Lorsque des trames de diffusion (broadcast) ou de multicast sont envoyées, les switchs les transfèrent par tous les ports. Les trames circulent en boucle et sont multipliées à chaque passage sur un commutateur tel que ses trames n'ayant pas de durée de vie elles vont tourner indéfiniment entre les commutateurs. La (Figure IV.1) ci-dessous présente une trame de diffusion multipliée en boucle sur tous les ports jusqu'à surcharger les liens et rendre le réseau indisponible.

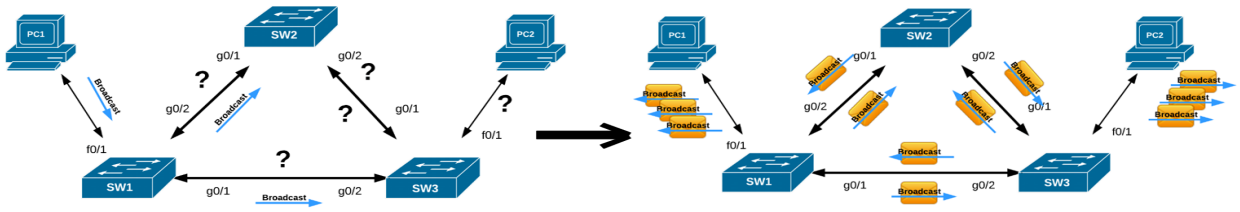

FIGURE IV.1 – Représentation de Tempête de diffusion [13].

ii. **Trames dupliquées :**Les trames peuvent être dupliquées sur certaines topologies redondantes. Ce scenario on le retrouve rarement car une tempête de diffusion va disfonctionner le réseau bien avant. La Figure IV.2 illustre que PC1 envoie une trame à PC2.elle arrive en double à sa destination.

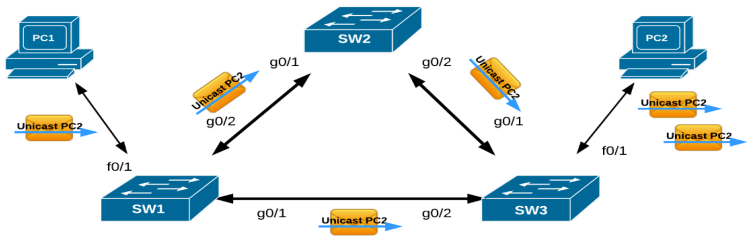

FIGURE IV.2 – Représentation de trame dupliquée [13].

STP conçu pour les commutateurs répond à la problématique de trames dupliquées dans un environnement de liaisons redondantes. Il détecte et désactive les boucles et fournit un mécanisme de liens de sauvegarde.

5. **Le protocole VTP :**
Le protocole VTP est un protocole de couche 2 propriétaire de la compagnie CISCO. Son avantage principal c'est sa capacité de propager automatiquement des VLAN configurés sur un commutateur en mode 'serveur' vers les autres commutateurs configurés en mode 'client'. Il existe 3 modes de configurations possibles d'un commutateur CISCO :

•**Mode server :**C'est le mode par défaut de tous les commutateurs niveau 2 de CISCO. Le commutateur-serveur propage les VLANs et leurs paramètres aux autres commutateurs 'client' du même domaine VTP. Le serveur-commutateur enregistre les informations des VLANs dans sa mémoire vive non volatile NVRAM. On peut créer, supprimer et renommer les VLANs tout en propageant ces changements aux autres commutateurs du réseau via des paquets 'vtp advertisement'.

•**Mode client :**On ne peut pas créer, supprimer ni renommer les VLANs au niveau du commutateur-client. Les informations des VLANs qui lui sont propagées ne sont pas enregistrées dans sa NVRAM.

•**Mode transparent :**Le commutateur en mode 'transparent' ne participe pas au protocole VTP. Il transmet les 'vtp advertisement' aux autres clients VTP. On peut créer, renommer ou supprimer des VLANs mais ils seront uniquement associés à ce commutateur.[40]

IV.4.2 Répartition de charge (Load Balancing) :

La répartition de charge est un ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe. Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs d'une façon intelligente vers les équipements (serveurs) les moins chargés, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur. Il est cependant nécessaire d'avoir une bande passante suffisamment élevée et puissante pour que cette architecture en load balancing fonctionne correctement.La figure suivante (Figure IV.3) montre que le flux entrant va être dirigé vers plusieurs serveurs.

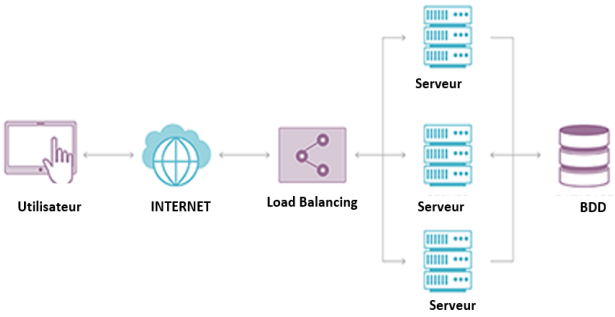

FIGURE IV.3 – Schéma illustrant le principe de répartition de charge.[14]

IV.4.3 Tolérance aux pannes (le FailOver) :

La tolérance aux pannes signifie une méthode de conception permettant à un système de continuer à fonctionner correctement même en cas de défaillance de certains de ses composants. La tolérance aux pannes désigne comment un système d'exploitation réagit et permet des dysfonctionnements et des défaillances matérielles ou logicielles. La capacité du système d'exploitation à récupérer et à tolérer les pannes peut être gérée par le biais d'un logiciel, d'un matériel ou d'une solution combinée qui exploite les équilibreurs de charge. Certains systèmes informatiques utilisent plusieurs systèmes de tolérance aux pannes en double pour gérer les pannes avec élégance, ce qu'on appelle un réseau tolérant aux pannes [41]. La figure ci-dessous (Figure IV.4) illustre qu'en fonctionnement normal, l'utilisateur sera dirigé vers le serveur disponible (en vert), les autres serveurs seront mis en attente (en jaune). Dans le cas où le serveur principal est indisponible (en rouge), un des serveurs secondaires prend le relais (L'ordre de passage en mode actif est défini dans la configuration).

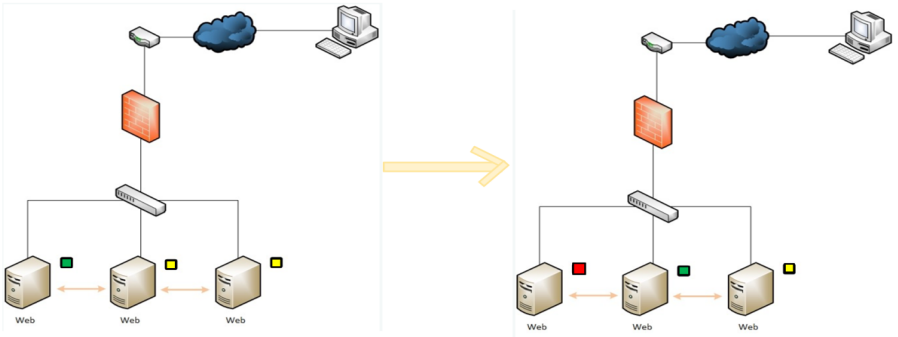

FIGURE IV.4 – Schéma illustratif sur le principe tolérance aux pannes.[13]

IV.4.4 La réplication des données :

Une combinaison d'équilibrage de charge et de technologie de basculement garantit une haute disponibilité de l'infrastructure informatique et fonctionnement en continu des services. Il existe également un risque de perte de données si une organisation est confrontée à un incendie, une catastrophe naturelle ou tout autre événement entraînant une perte d'équipement.Pour cela il faut effectuer des sauvegardes régulières pour réduire ce risque. La réplication permet de synchroniser en toute sécurité les données sur plusieurs serveurs. . Cette technologie est utilisée pour créer des sauvegardes et autoriser plusieurs versions du même

fichier. La deuxième option est la synchronisation bidirectionnelle. Cela signifie que les données ne sont pas seulement répliquées entre deux ou plusieurs serveurs, mais peuvent être consultées et modifiées en temps réel. L'implémentation d'un système de verrouillage et de temporisation empêche deux clients d'écrire dans le même fichier en même temps.[42]

IV.4.5 RAID (Redundant Array of Independent Disks) :

Le RAID (Redundant Array of Independent Disks) permet de mixer des disques durs "classiques" dans une matrice qui sera plus performante (plus d'espace, plus rapide, plus sécurisée)et aussi désigne l'action de créer une matrice contenant un minimum de deux solutions de stockage différentes et formant un seul grand disque logique. Les systèmes RAID sont régis par un principe de base, à savoir le stockage redondant de données, qui garantit l'intégrité et la fonctionnalité de l'ensemble de la matrice en cas de panne au niveau des disques durs individuels.[15]

1. **Le RAID 0 (volume agrégé par bandes) :** Les matrices de disques durs exécutés sous l'appellation RAID 0 ne sont pas considérées comme étant des systèmes RAID, car leur stockage n'est pas basé sur le principe de redondance.l'objectif de ce modèle d'accélérer l'accès aux données en combinant au moins deux disques durs de manière à former un seul grand disque logique. les données sont organisées en blocs successifs et réparties uniformément sur les différents supports.Si cette matrice offre une plus grande capacité de stockage et davantage de débit, elle a également pour effet de compromettre automatiquement la sécurité : si un disque dur tombe en panne, cela peut causer une perte de l'ensemble des données. la (Figure IV.5)ci-dessus montre le concept du RAID 0.

FIGURE IV.5 – Graphique illustrant l'ensemble du concept RAID 0 [15].

2. **Le RAID 1 (disques en miroir) :** Le niveau RAID 1 est associé au « mirroring »,illustré par la(Figure IV.6),en français c'est« mise en miroir ». Tous les disques durs intégrés à cette matrice possèdent à tout moment le même ensemble de données ; cette dernière assure une redondance complète, ce qui lui permet de garder le contrôle sans aucun problème en cas de panne de l'une des solutions de stockage individuelles. Par conséquent, la capacité totale du système RAID ne peut jamais excéder la capacité du plus petit disque dur impliqué.Dans un système RAID 1, la vitesse d'écriture est comparable à celle obtenue avec un seul disque.

FIGURE IV.6 – Graphique illustrant l'ensemble du concept RAID 1 [15].

3. **Le RAID 5 (volume agrégé par bandes à parité répartie) :** Le niveau RAID 5 désigne une matrice d'au moins trois disques durs (ce nombre est généralement impair : trois, cinq, sept, etc.). Cette méthode de stockage utilise le concept de « striping » et organise les données sous forme de blocs avant de les répartir sur les différents supports. Grâce aux blocs de données, les informations de parité sont réparties uniformément sur les disques durs appartenant à la matrice. Ceux-ci peuvent ensuite être utilisés pour restaurer les données perdues si l'un des supports de stockage tombe en panne.Le niveau RAID 5 (Figure IV.7) offre ainsi une meilleure vitesse de lecture et une sécurité accrue par rapport à un seul disque.

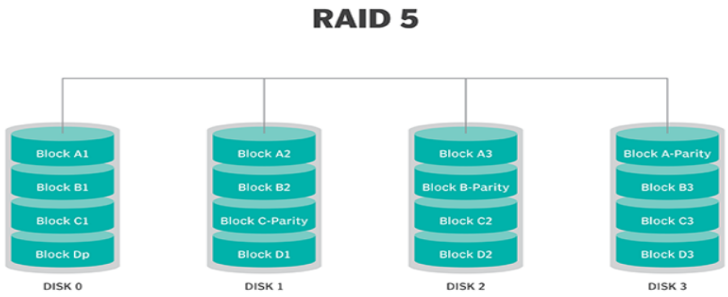

FIGURE IV.7 – Graphique illustrant l'ensemble du concept RAID 5 [15].

4. **Le RAID 10 :** Le système RAID 10, ou RAID 1 + 0, combine les propriétés du niveau RAID 0 à celles du niveau RAID 1 : cela confère aux données un débit de transfert plus élevé et davantage de sécurité. Pour y parvenir, il suffit de combiner plusieurs systèmes RAID 1 dans une matrice RAID 0 ; il est nécessaire d'utiliser au moins quatre disques durs.

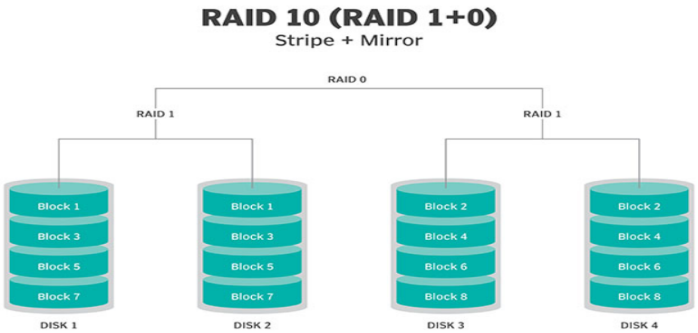

FIGURE IV.8 – Graphique illustrant l'ensemble du concept RAID 10 [15].

IV.4.6 La mise en cluster :

La mise en cluster,appelée clustering, est une technique largement utilisée dans les environnements informatiques pour améliorer la disponibilité, la redondance et les performances des applications et des services. Elle consiste à regrouper plusieurs serveurs physiques ou virtuels en un seul groupe cohérent, où ils travaillent de manière collaborative pour fournir des services de manière transparente. Lorsqu'un système est configuré en cluster, les serveurs membres partagent des ressources, tels que le stockage, la puissance de calcul et les connexions réseau. Cela permet d'assurer une haute disponibilité, car si l'un des serveurs du cluster tombe en panne, les autres membres du cluster peuvent prendre le relais et assurer la continuité des services sans interruption. La mise en cluster offre également une meilleure évolutivité et une répartition de charge efficace. Les charges de travail peuvent être réparties entre les différents membres du cluster, ce qui permet d'optimiser l'utilisation des ressources disponibles et d'améliorer les performances globales du système.[43]

IV.4.7 Le stockage en réseau :

1. **Network attached storage (NAS) :** Le stockage en réseau (NAS) repose sur une architecture de stockage en mode fichier qui rend les données stockées plus accessibles aux périphériques réseau. Le NAS, le SAN (réseau de stockage) et le DAS (stockage en attachement direct) constituent les trois principales architectures de stockage. Le NAS offre aux réseaux un point d'accès unique pour le stockage qui intègre des fonctionnalités de sécurité, de gestion et de tolérance aux pannes.

   Le NAS peut être configuré comme une option de stockage compatible avec les conteneurs, dans laquelle le système de stockage est exposé à un ou plusieurs conteneurs.Les conteneurs désignent une technologie hautement flexible qui apporte un niveau d'évolutivité considérable à la distribution des applications et des ressources de stockage.

Avantages :

- **Évolutivité :** pour augmenter la capacité de stockage d'un NAS, il suffit d'y ajouter des disques durs. Pas besoin de mettre à niveau ni de remplacer des serveurs, et encore moins de désactiver le réseau.

- **Performances :** comme le NAS est un système de fichiers, les autres périphériques du réseau n'ont pas besoin de se charger du partage des fichiers. De plus, le NAS est souvent configuré pour une utilisation bien précise (stockage de Big Data ou de contenus multimédias, par exemple), ce qui permet d'obtenir de meilleures performances.

- **Configuration simple :** les architectures NAS sont souvent accompagnées de scripts simples ou encore fournies sous la forme d'appliances préinstallées avec un système d'exploitation rationalisé, ce qui réduit considérablement le temps de configuration et de gestion du système.

- **Accessibilité :** tous les périphériques en réseau ont accès au NAS.

- **Tolérance aux pannes :** il est possible de formater le NAS de sorte qu'il prenne en charge des disques répliqués, un système RAID afin d'assurer l'intégrité des données.

2. **Storage Area Network (SAN)** Un réseau de stockage (SAN) permet le stockage en mode bloc. Le stockage en mode bloc sépare les volumes de stockage (tels que les disques durs, les nœuds de stockage virtuels ou les pools de stockage dans le cloud) afin d'obtenir des volumes plus petits nommés blocs, qui peuvent être adaptés aux formats de divers protocoles. Par exemple, il est possible d'adapter un bloc au format du protocole NFS (Network File System), un autre au format du protocole AFP (Apple Filing Protocol) et un troisième au format du protocole SMB(Server Message Block). Cette option offre une plus grande flexibilité aux utilisateurs, mais complique la navigation parmi les ressources, car le stockage en mode bloc rassemble les données de manière arbitraire.

3. **La différence entre le NAS et SAN :** Le NAS et le SAN sont tous deux des systèmes de stockage en réseau. Ils mettent en commun la capacité de stockage et la partagent avec les serveurs d'applications sur un réseau à haut débit. La principale différence entre eux est la manière dont l'utilisateur les perçoit. Pour les clients, le NAS fonctionne comme un système de fichiers et le SAN comme un système d'exploitation. Le NAS traite les demandes de fichiers individuelles, mais le SAN gère les demandes de blocs de données contigus. Les NAS et les SAN utilisent également des protocoles et des technologies sous-jacents différents. Le SAN est plus flexible pour les utilisateurs, mais il peut coûter plus cher à configurer et à gérer.

Conclusion

Ce chapitre est consacré à la définition des notions de base et à des généralités sur la haute disponibilité des réseaux informatique, ansi que ses différents protocoles qu'on a utilisé dans notre projet afin et comprendre le fonctionnement de chacun ainsi que les avantages qu'ils présentent au réseau.

Chapitre V

Proposition, simulation et test

Introduction

Dans ce chapitre, nous décrirons la phase de mise en œuvre de ce projet. Cette section est le corps principal de ce mémoire, où nous montrons les conditions préalables et les étapes de configuration et les différentes solutions choisies. Une annexe a été ajoutée pour l'installation des certains softwares

V.1 Architecture proposée :

Notre architecture a trois objectifs essentiels : la virtualisation, la supervision et la haute disponibilité.

Notre proposition d'architecture reseau pour l'entreprise doit répondre aux différents besoins en matière de connectivité et de partage ressources. Nous proposons la mise en place d'un reseau local câblé basé sur Ethernet pour assurer une connectivité stable et rapide entre les différents postes de travails, serveurs et périphériques réseaux .

Pour garantir une sécurité optimale, nous suggérons la mise en place d'un pare-feu de nouvelle génération (Fortigate)qui protégera leur reseau contre les menaces externes et internes. L'utilisation de la segmentation du reseau en VLANs permettra de séparer les différents départements et de limiter l'accès aux ressources sensibles.

Nous proposons également l'intégration des serveurs Windows 2019 comme contrôleur de domaine pour la gestion centralisée des utilisateurs, ce serveur pourra également fournir des services tels que la messagerie électronique, le partage de fichier et l'hébergement de services Web internes.

Pour la virtualisation et supervision nous avons fait le choix d'installer VMware ESXi, nous avons mis en place un protocole de LACP-LB entre les switches dist01 et dist02.

Pour la haute disponibilité, nous avons configuré un cluster CLUSTER-AH entre FG-BMT1 et FG-BMT2, ainsi qu'un cluster entre les serveurs serveur01 et serveur02. nous avons mis en place le protocole GLBP-LB entre R-ZEP1 et R-ZEP2, ainsi que le protocole PAGP-LB entre SW-ZEP et SW-ZEP2. Ces mesures nous permettent d'assurer une redondance, une répartition de charge et une disponibilité élevée dans notre infrastructure.

Pour garantir une connectivité sécurisée, nous avons configuré un VPN entre FG-BMT1 et FG-ZEP.En ce qui concerne la haute disponibilité, nous avons mis en place le protocole GLBP-LB entre R-ZEP1 et R-ZEP2, ainsi que le protocole PAGP-LB entre SW-ZEP et SW-ZEP2. Ces mesures nous permettent d'assurer une redondance, une répartition de charge et une disponibilité élevée dans notre infrastructure.

Notre proposition d'architecture est illustrée dans la Figure V.1.

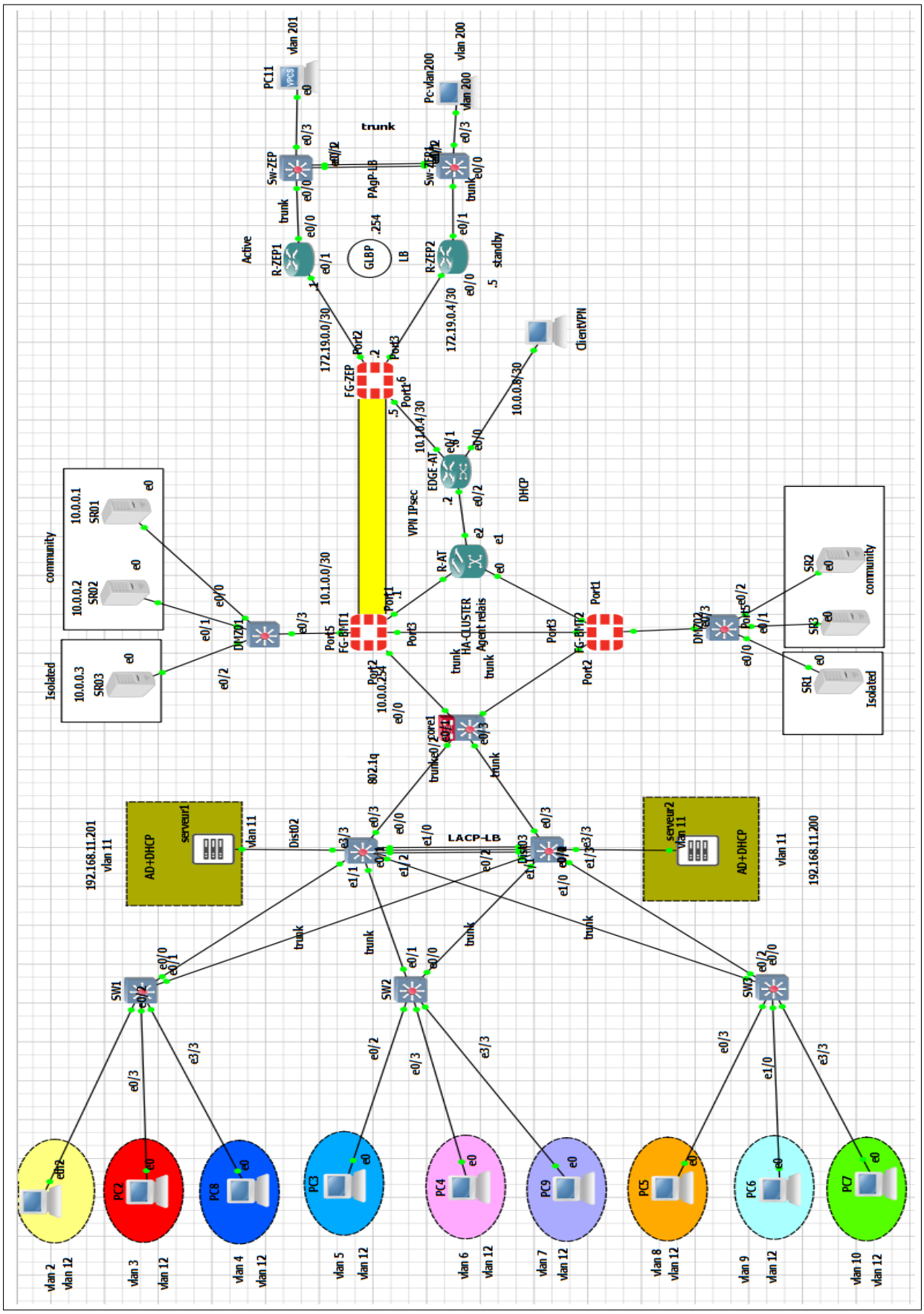

FIGURE V.1 – Architecture proposée.

V.2 Environnement de travail :

Afin de garantir une mise en œuvre optimale de notre architecture proposée, nous comptons sur des environnements de travail tels que GNS3, VMware et ESXi7. Ces outils essentiels nous permettent de concrétiser notre architecture en mettant en place les configurations nécessaires.

V.2.1 GNS3 sous windows :

Est l'abréviation de "Graphical Network Simulator-3". Il s'agit d'une interface graphique et d'une plateforme de contrôle écrites en Python qui permet de simuler des infrastructures informatiques. GNS3 utilise diverses technologies de virtualisation telles que Dynamips [1], VMWare Workstation/ESXi, VirtualBox, KVM, etc. Ces technologies permettent d'émuler le comportement des équipements réseau, tels que les routeurs, les commutateurs et les pare-feu, en utilisant des images de systèmes d'exploitation réels. Ainsi, On a choisi GNS3 pour la simulation de notre architecture car il offre une solution puissante pour la conception, la configuration, l'apprentissage et le dépannage des réseaux, sans avoir besoin d'un matériel physique coûteux. la Figure V.2 représente logo de GNS3.[44]

FIGURE V.2 – GNS3.[16]

V.2.2 VMware Workstation version 17 :

VMware est la plate-forme de virtualisation leader pour la création d'infrastructures de Cloud Computing. Elle permet aux utilisateurs d'exécuter leurs applications métier stratégiques en toute sécurité et de répondre plus rapidement aux besoins de l'activité[45]. On a choisi vmware pour sa simplicité de la gestion et son contrôle sur les infrastructures informatiques.la Figure V.3 représente logo de VMware Workstation.

FIGURE V.3 – VMware Workstation.[17]

1. Dynamips (2005) est un émulateur de routeur Cisco écrit par Christophe fillot. Il émule les plateformes matérielles C2691, C3620, C3640, C3660, C3725, C3745 et C7206 en faisant fonctionner de véritables images Cisco IOS. Dynagen et Dynagui sont deux autres projets qui s'interfacent avec Dynamips.

V.2.3 IOU Cisco :

Cisco IOS On UNIX (IOU) est une version entièrement fonctionnelle d'IOS (Internetwork Operating System) qui s'exécute en tant que processus UNIX (Solaris) en mode utilisateur. IOU est construit comme une image Solaris native et s'exécute comme n'importe quel autre programme. IOU prend en charge tous les protocoles et fonctionnalités indépendants de la plate-forme.

En ce qui concerne les fonctionnalités, il est très similaire à GNS3 mais il ne nécessite pas les ressources que nécessitent plusieurs routeurs virtuels fonctionnant sous dynamips. La Figure V.4 montre les modèles d'appareils IOU d'un routeur et d'un switch [46]

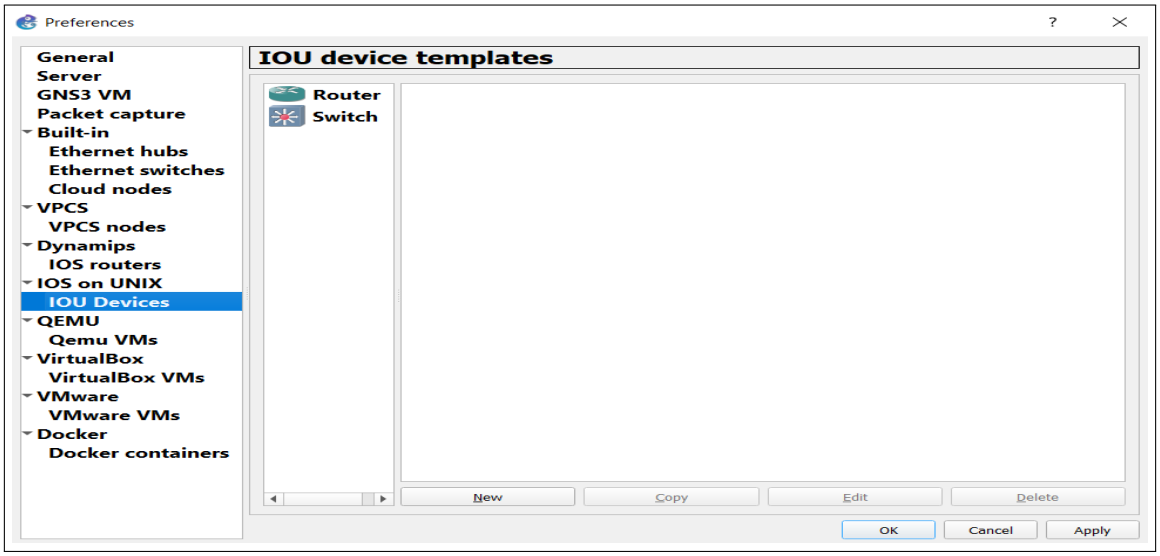

FIGURE V.4 – Modèles d'appareils IOU.

V.3 Les machines virtuelles :

V.3.1 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.[47].On a choisi l'installation de cette version sur nos machines virtuelles, car elle est la première à fonctionner sur toutes les plateformes existantes : ordinateurs de bureau et portables, smartphones, tablettes et montres connectées. L'interface de s'adapte automatiquement au format et au mode de saisie (tactile ou bien clavier et souris).

V.3.2 Windows Server :

Windows Server est un système d'exploitation pour serveur par Microsoft. Basé sur l'architecture Windows NT, il fournit toutes les capacités, fonctionnalités des mécanismes de fonctionnement d'un OS pour serveur standard [48]. On a choisi windows server 2019 car ce nouveau système d'exploitation permet la mise à jour à partir d'un OS déjà installé(Windows Server 2016, par exemple), sans éliminer les données qui figuraient dans le serveur.

V.3.3 Fortigate :

FortiGate NGFW est le pare-feu réseau le plus déployé au monde, offrant des performances de sécurité et une veille sur les menaces inégalées misant sur l'IA, ainsi qu'une visibilité complète et une convergence de la sécurité et du réseau[49].On a choisi ce par-feu car la BMT se dispose de ce type de parfeu.

FIGURE V.5 – Fortigate logo.[18]

V.3.4 Elastic Sky X Integrated (ESXI) :

VMware ESXi est un hyperviseur de type 1, ou un « hyperviseur bare metal » selon le langage courant, qui peut être installé directement sur un serveur physique et qui peut être utilisé indépendamment du système d'exploitation. Le logiciel vSphere est utilisé pour l'administration. ESXi est basé sur le VMkernel et renonce à un système d'exploitation de console en propre, ce qui permet à l'hyperviseur de nécessiter beaucoup moins d'espace disque que les autres options.[50]. On a choisi l'installation de ESXI pour nous offrir un environnement de virtualisation et supervision.

FIGURE V.6 – Logo de ESXi 7.[19]

V.4 Installation et configuration de l'Active Directory (AD) +DNS sur Serveur1 et Serveur2 :

Pour installer AD+DNS, on a suivie les étapes ci-dessous dans l'ordre pour effectuer la configuration.

1. **Installation AD+DNS :**
   Pour installer Active Directory, on doit d'abord déployer un serveur Windows et configurer une adresse IP statique. Ensuite, on peut utiliser l'Assistant Configuration du serveur pour installer les rôles et les fonctionnalités nécessaires. Une fois Active Directory installé, on pourra créer un nouveau domaine ou rejoindre un domaine existant.

   L'installation de Domain Name Server (DNS) peut être effectuée conjointement avec l'installation d'Active Directory (Figure V.7).

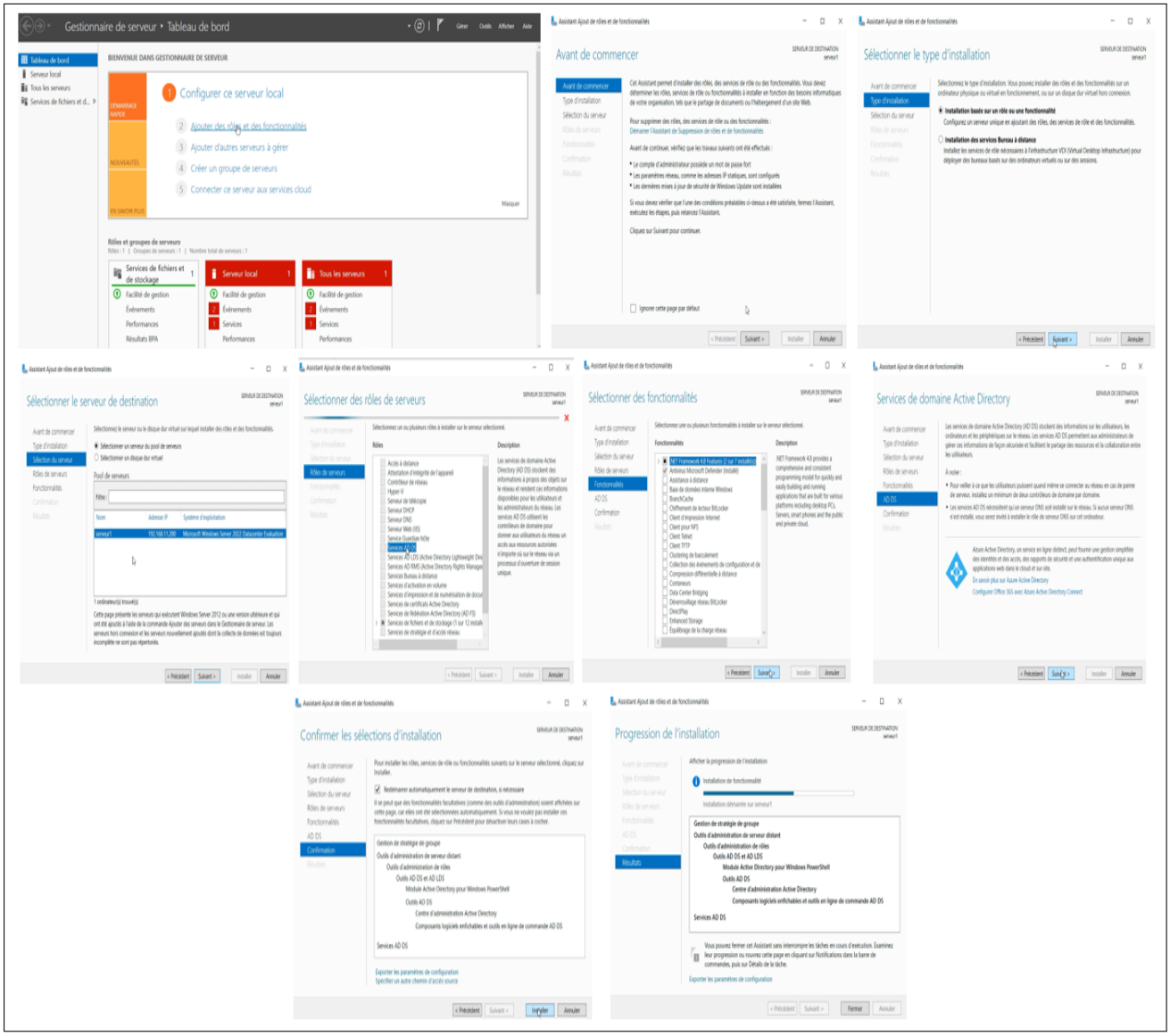

FIGURE V.7 – Installation et configuration de l'Active Directory (AD)+DNS.

2. **Créer un contrôleur du Domain :**
   Une fois notre Active Directory installé, nous commencerons à le configurer (Figure V.8). La première étape consiste à ajouter une nouvelle forêt [2] appelée bmt.local. Windows de-

2. Fait référence à la création d'une nouvelle structure hiérarchique de domaine Active Directory (AD). Une forêt AD est une collection de domaines qui partagent une relation d'approbation et une structure d'arborescence commune.

mande ensuit de sélectionner le niveau fonctionnel de la nouvelle forêt Active Directory. Dans notre cas, nous avons placé un niveau de fonctionnalité de 2016. Windows donne alors des options supplémentaires à installer, comme un serveur DNS compatible avec notre Active Directory. Après avoir configuré et installé le service, le système nécessitera un redémarrage.

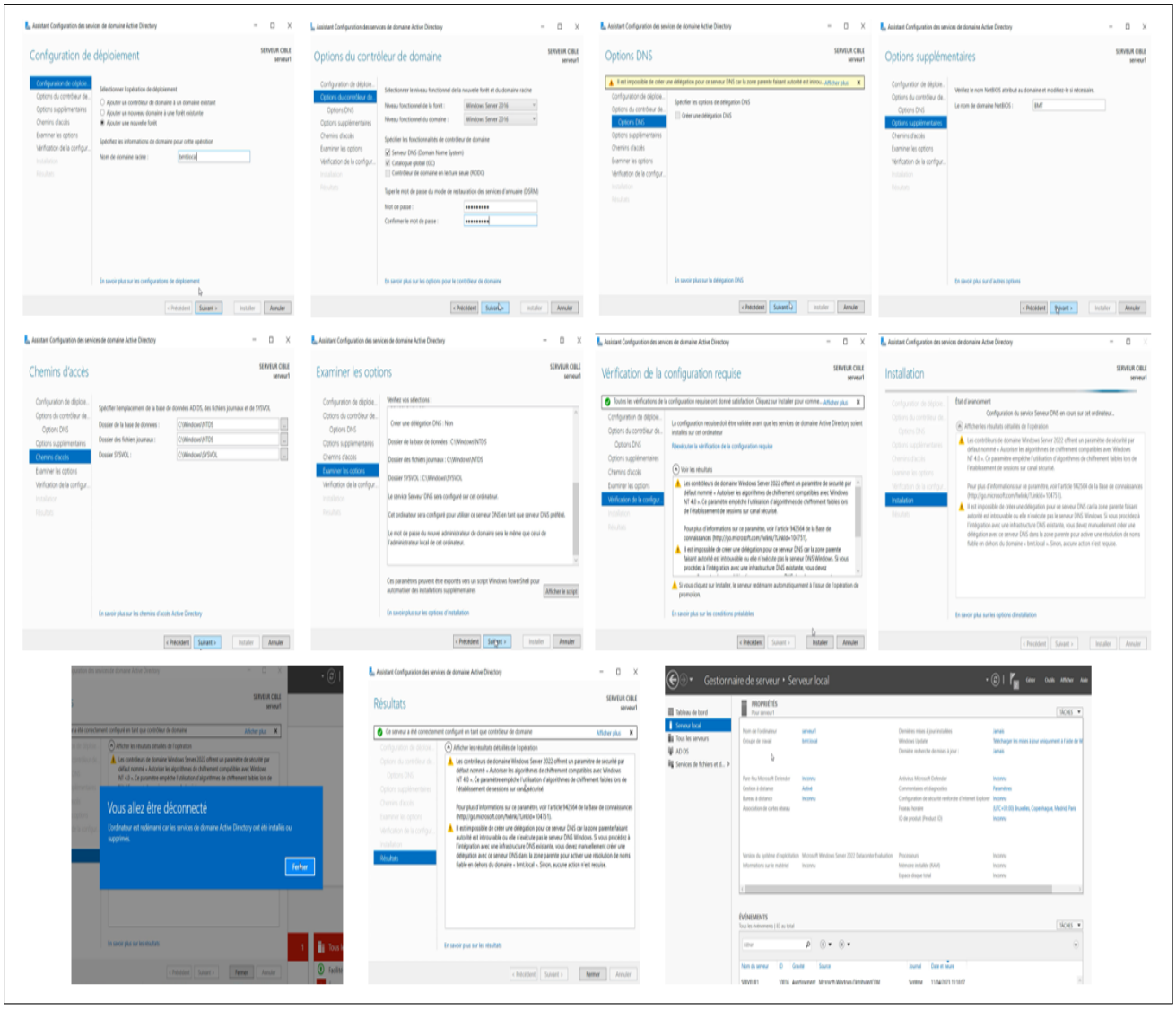

FIGURE V.8 – Création d'un contrôleur du Domaine.

3. **Ajouter le serveur2 au domaine :**
   Une fois le domaine est crée on doit ajouter le deuxième serveur (serveur2) au domaine "bmt.local" pour avoir la haute disponibilité, la Figure V.9 montre les deux étapes a suivre pour l'ajout.

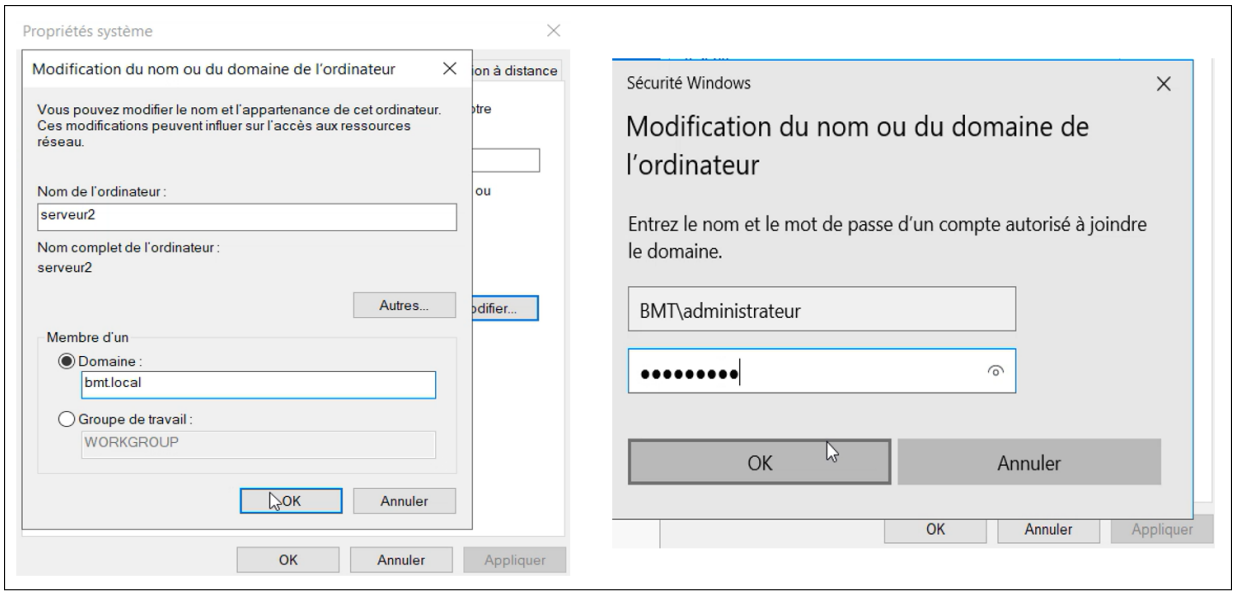

FIGURE V.9 – Ajouter le serveur2 au domaine « bmt.local ».

4. **clustering des serveur :**
   Avant de passer au cluternig des deux serveurs, on passera un ping au domaine ”bmt.local” pour Vérifier la connectivité réseau et la résolution DNS, ensuit on ping entre serveur1 et serveurs2 pour vérifier si les deux serveurs peuvent se rejoindre sur le réseau. La Figure V.10 montre que la connectivité entre les deux serveurs est établie.

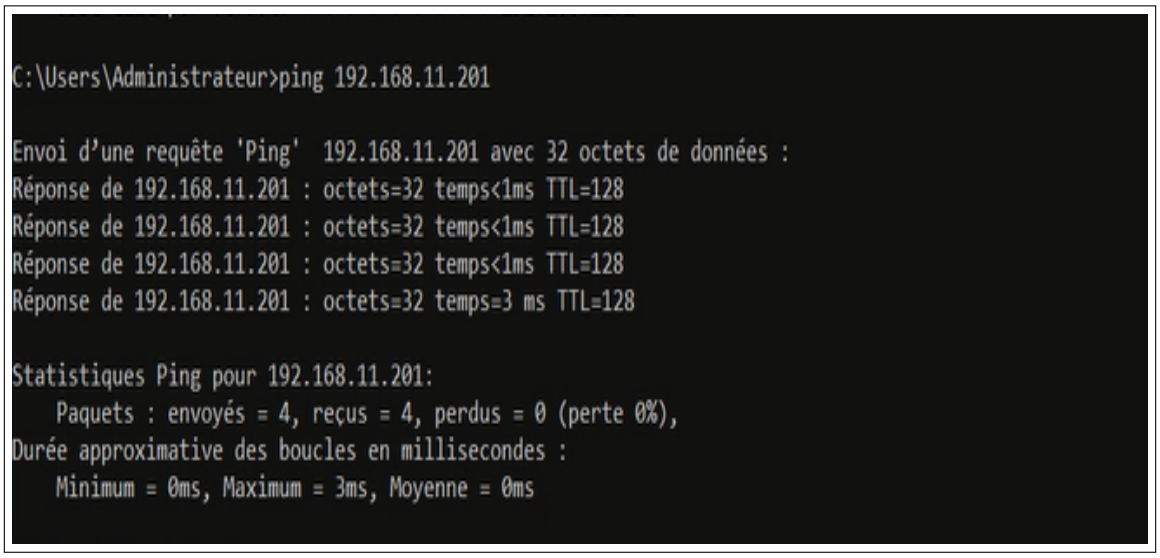

FIGURE V.10 – Ping du serveur01 vers serveur02.

Une fois que le serveur2 est ajouté au domaine "bmt.local", il est nécessaire d'effectuer la synchronisation entre les deux serveurs et de permettre la gestion du serveur2 en tant que serveur esclave à partir du serveur1, qui est le serveur maître. Pour ce faire, les étapes illustrées dans la Figure V.11 ci-dessous doivent être suivies.

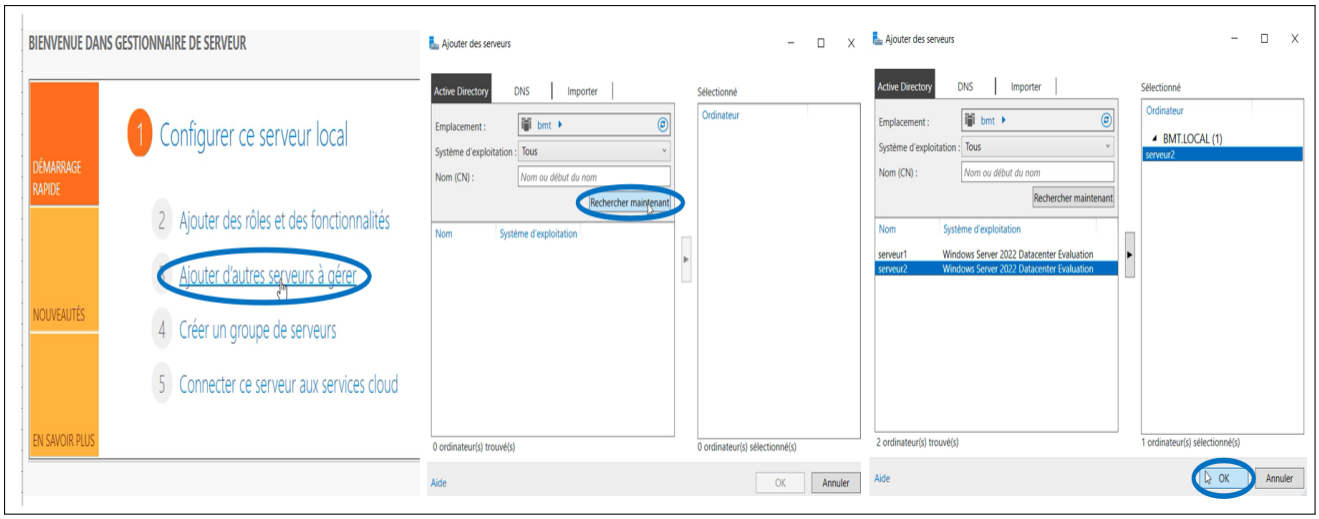

FIGURE V.11 – Synchronisation de serveur2.

5. **Créer des Unités d'organisation OU et des comptes utilisateur :**
Maintenant qu'on a les deux rôles AD et DNS installés on commence la création d'une nouvelle unité d'organisation OU [3], puis la création des comptes utilisateur comme le montre la Figure V.12.

- Il suffit d'aller vers outils ;

- Utilisateurs et ordinateurs AD ;

- clique sur le bouton droit de la souris sur bmt.local ;

- On sélectionne nouveau ;

- Unité d'organisation ;

- Puis on entre le nom de notre unité d'organisation qui est « bmt users ».

Dans l'unité « bmt users » qu'on a déjà crée on va créer des comptes pour les utilisateurs pour cela :
- On clique sur le bouton droit sur l'unité « bmt users » ;

- On choisir nouveau utilisateur ;

- Remplir les informations correspondantes à l'utilisateur ainsi le mot de passe d'ouverture de sa session ;

- Valider.

3. Fait référence à la création de conteneurs logiques dans Active Directory (AD) pour organiser et hiérarchiser les objets, tels que les utilisateurs, les groupes et les ordinateurs, en fonction de la structure organisationnelle de l'entreprise.

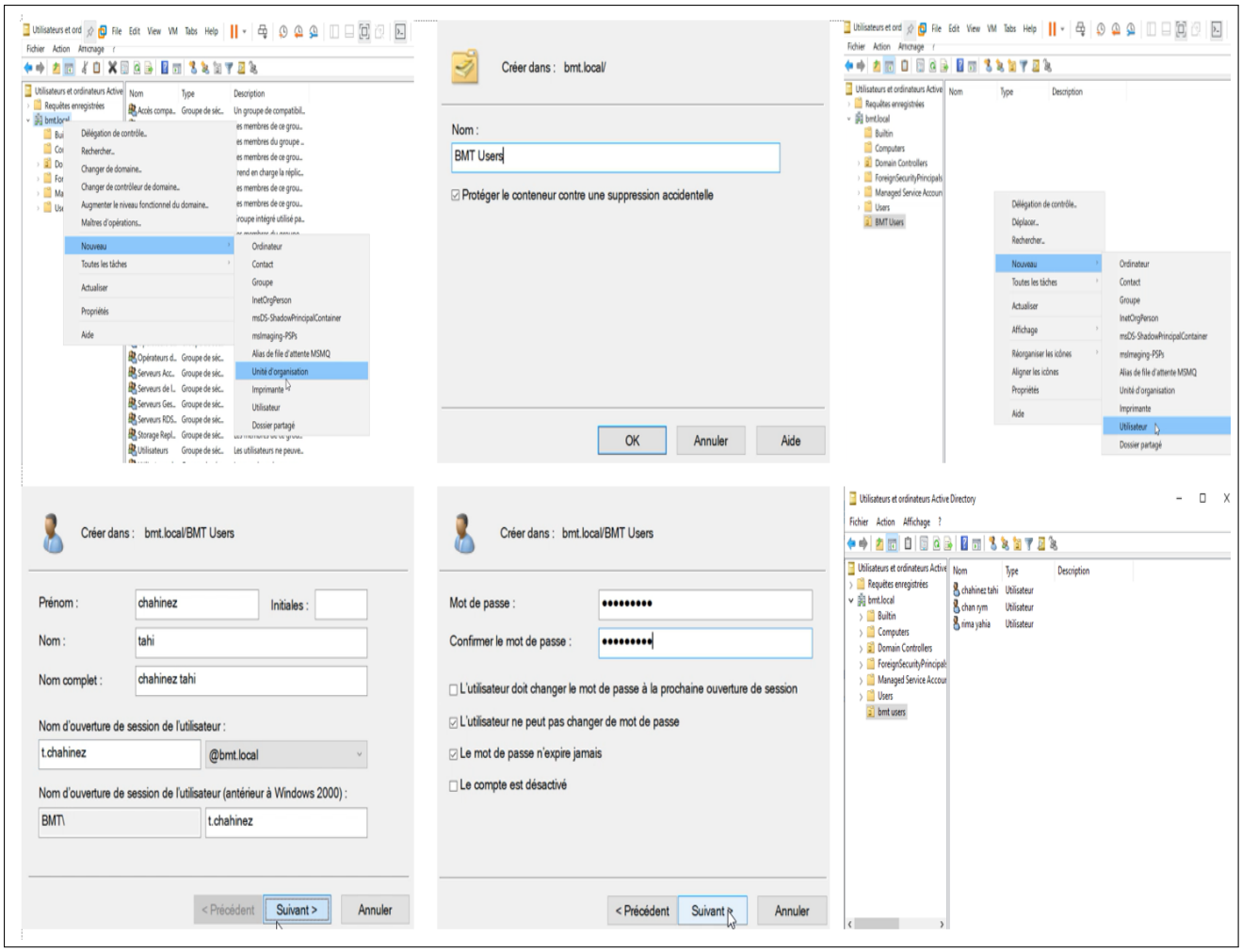

FIGURE V.12 – Création des Unités d'organisation OU et les utilisateurs.

6. **Créer des groupes :**
   Une fois les comptes sont crées on passe à la création des groupes et des ordinateurs pour les utilisateurs déjà crée (Figure V.13).

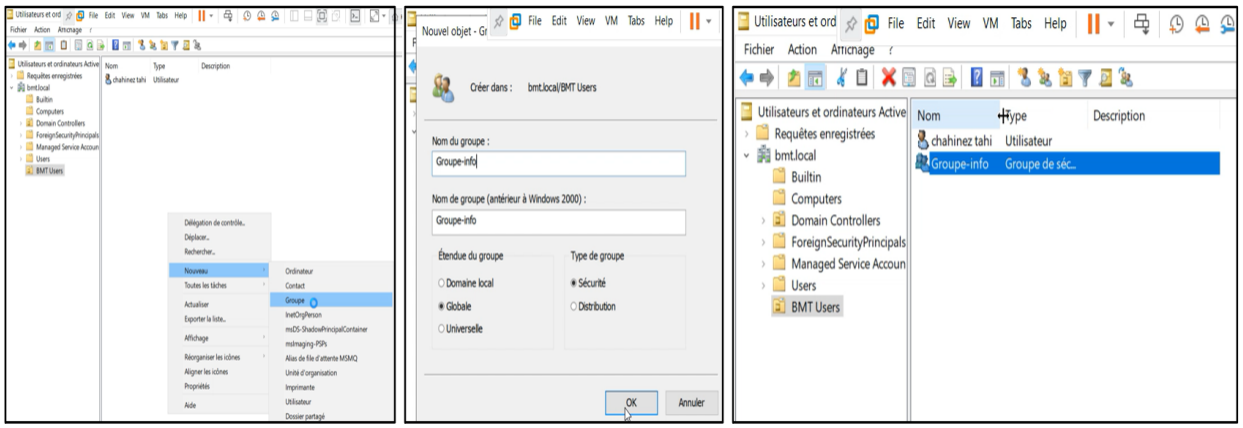

FIGURE V.13 – Création de groupe « group-info » .

7. **Tester AD+DNS depuis un PC :**
   Nous avons commencé par les commandes ping suivantes : ping du serveur vers la passerelle et vers le nom de domaine, ainsi que du PC vers le serveur et vers le nom de domaine (Figure V.14).

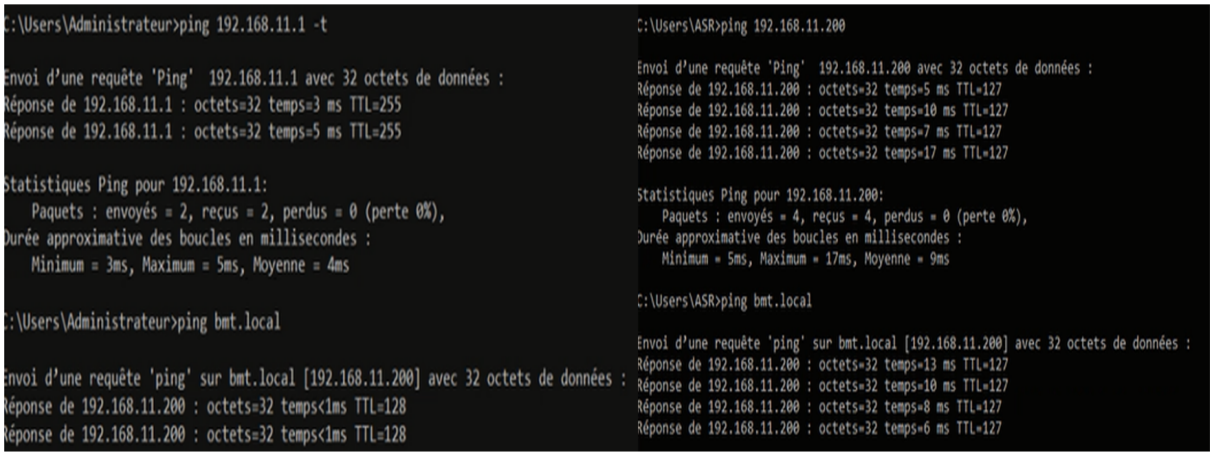

FIGURE V.14 – Pings du serveur et PC vers la passerelle et le domaine.

Pour tester AD+DNS on a besoin d'un compte utilisateur, pour cela premièrement on ajoute un PC dans le domaine bmt.local, pour cela nous allons essayer d'ajouter un compte utilisateur déjà créé au domaine en suivant les étapes illustrées dans la Figure V.15 :

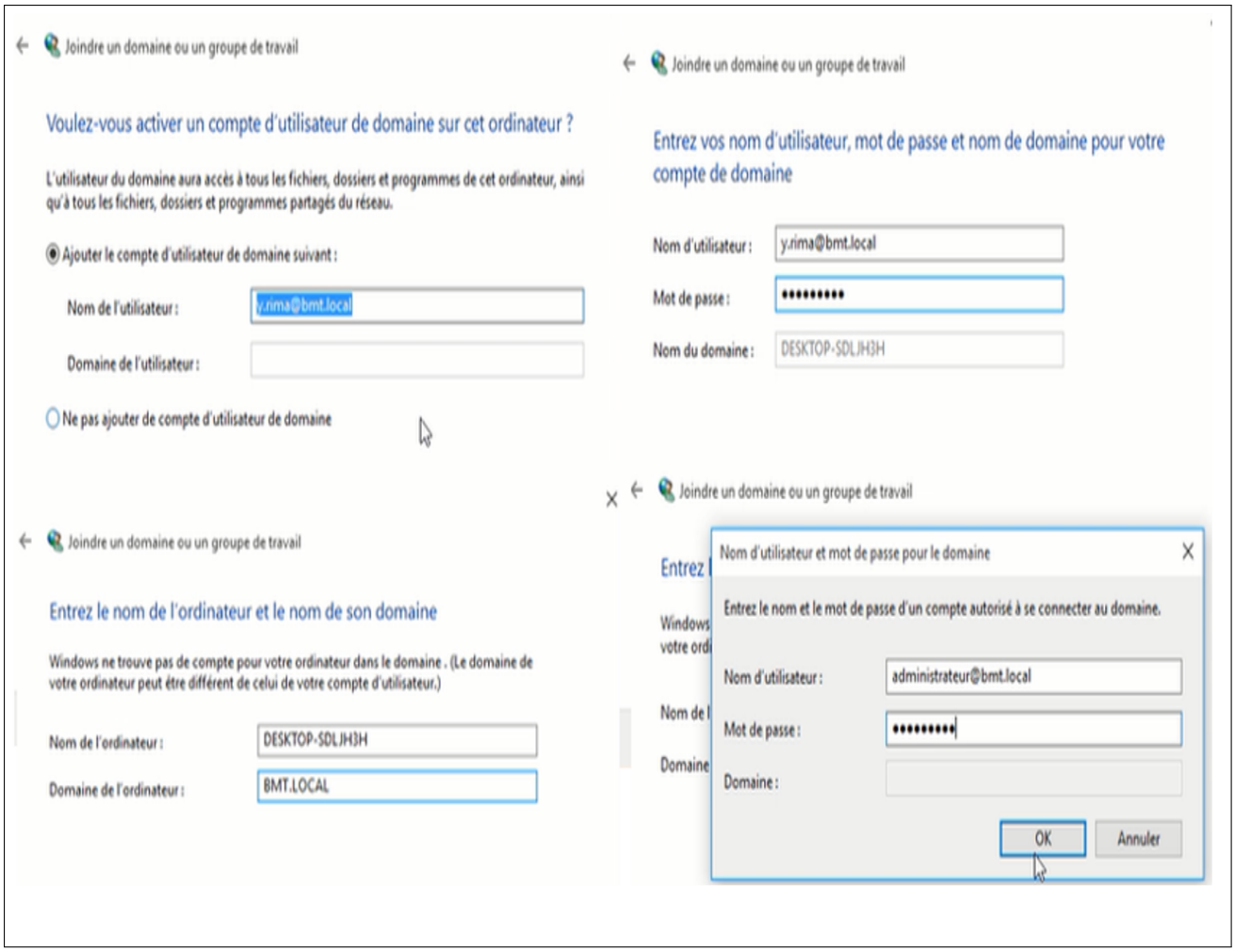

FIGURE V.15 – Ajout d'un compte utilisateur au domaine.

Une fois que le compte utilisateur "y.rima@bmt.local" est ajouté avec succès, cette fenêtre s'affichera (Figure V.16) :

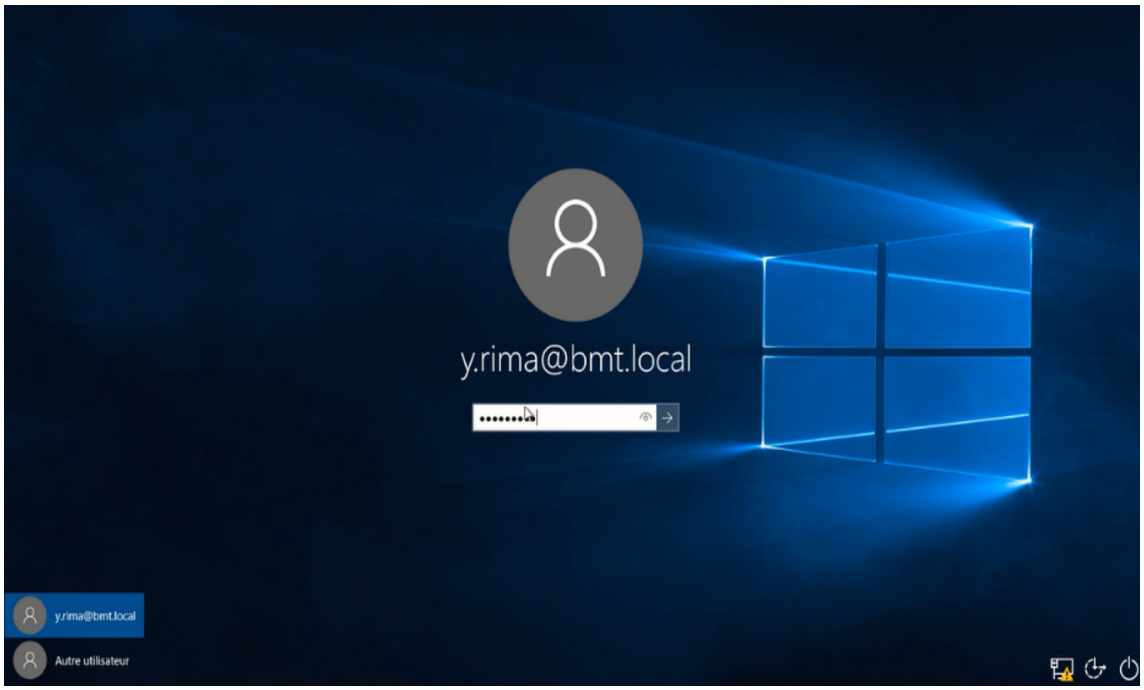

FIGURE V.16 – Écran administrateur" y.rima".

V.5 Installation et configuration de Dynamic Host Configuration Protocol (DHCP) :

Afin de permettre l'attribution automatique des adresses IP aux machines, il est nécessaire d'installer le service DHCP. Pour cela, il est recommandé de suivre les étapes suivantes pour configurer correctement le service DHCP.

1. **Installation de service DHCP :**
   Nous allons installer DHCP sur serveur1 et serveur2 de la même façon et pour commencer l'installation, il va falloir ajouter le Service de DHCP. Puis, lancer l'installation et ajouter les fonctionnalités nécessaires (Figure V.17).

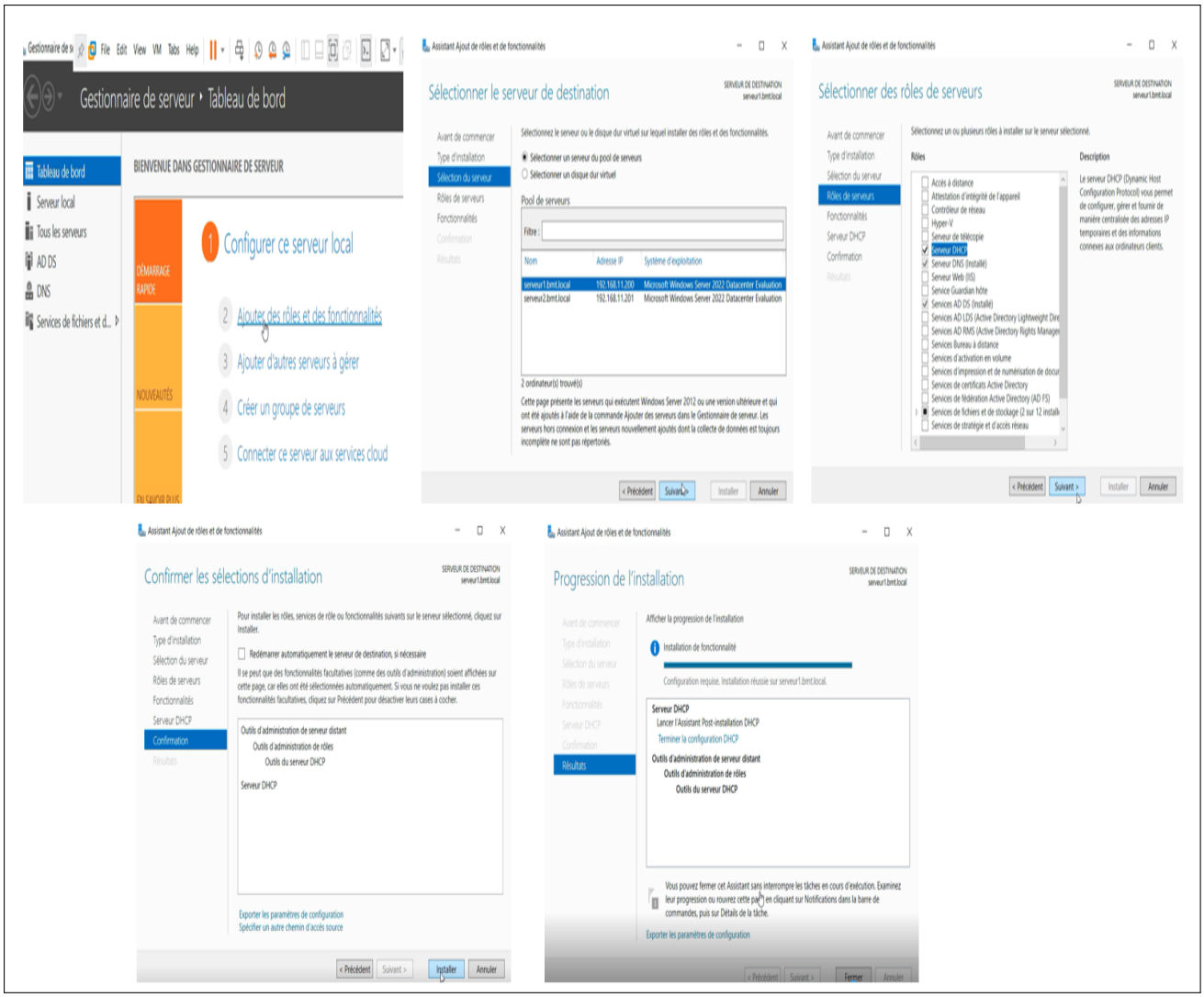

FIGURE V.17 – Installation DHCP.

2. **Relier DHCP avec AD :**
   La Figure V.18 montre comment relier DHCP avec AD et les informations d'identification a utiliser pour autoriser le serveur DHCP dans le service AD.

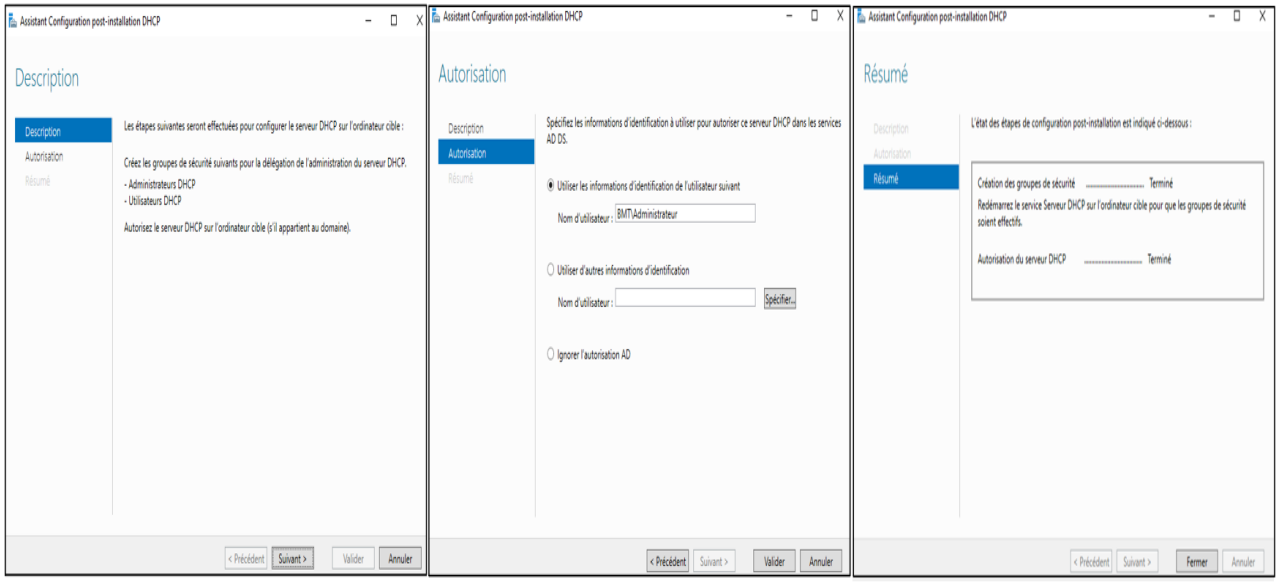

FIGURE V.18 – Relier DHCP avec AD.

3. **Création des étendus pour chaque vlan :**
   Nous allons commencer par créer des étendus [4] pour chaque vlan :

   - Nous allons dans Outils ;

   - DHCP ;

   - Serveur1.bmt.local ;

   - Clique droit dans ipv4 ;

   - Nouvelle étendue.

   comme le montre la (Figure V.19) suivante :

4. Créer une étendue dans AD signifie configurer un pool d'adresses IP disponibles pour l'attribution automatique aux clients du réseau via le service DHCP. Cela facilite la gestion des adresses IP et garantit une allocation efficace des adresses aux clients.

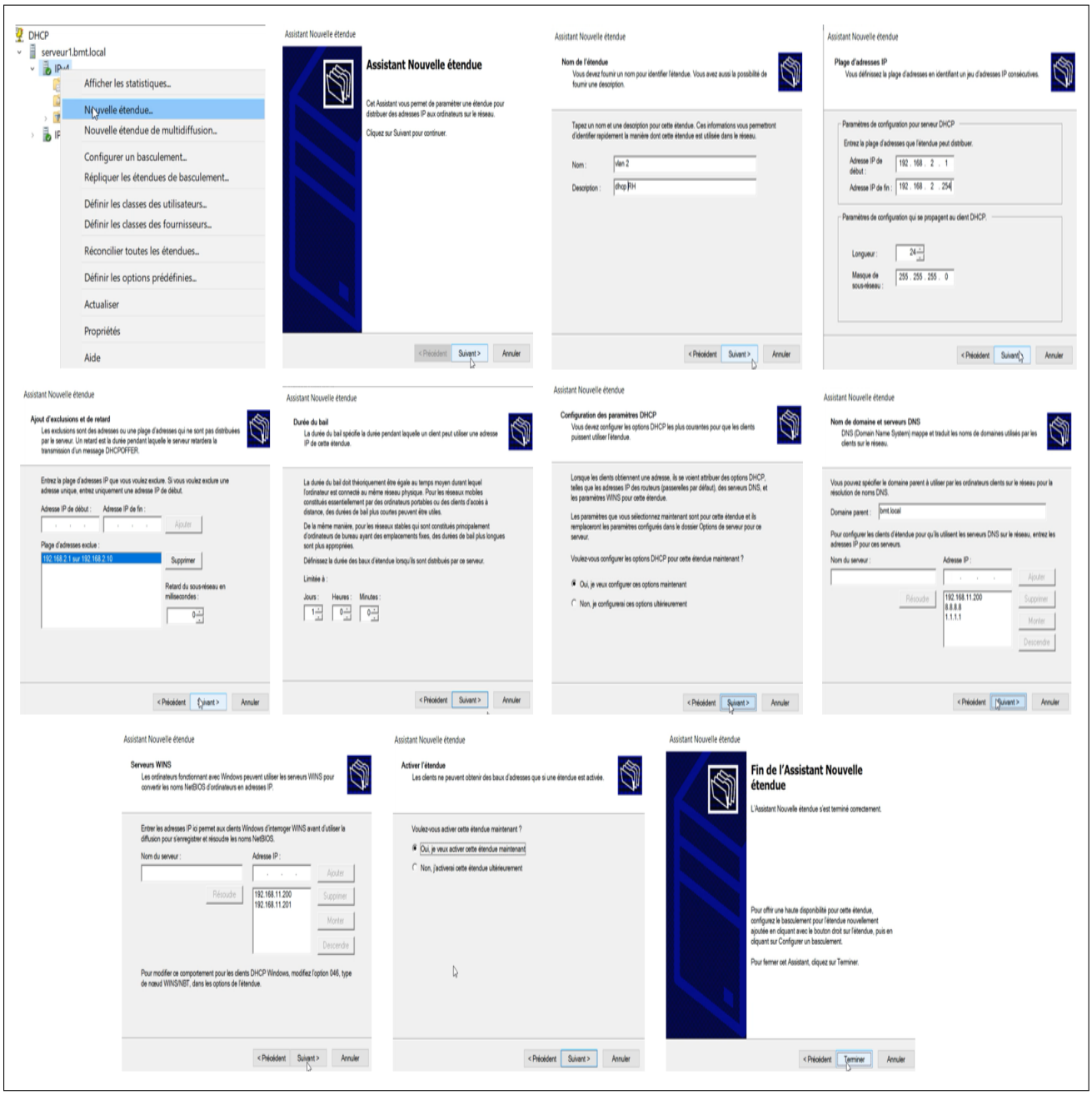

FIGURE V.19 – Création de l'étendue vlan 2 « RH ».

la Figure V.20 ci-dessous montre toutes les étendus qu'on a crée.

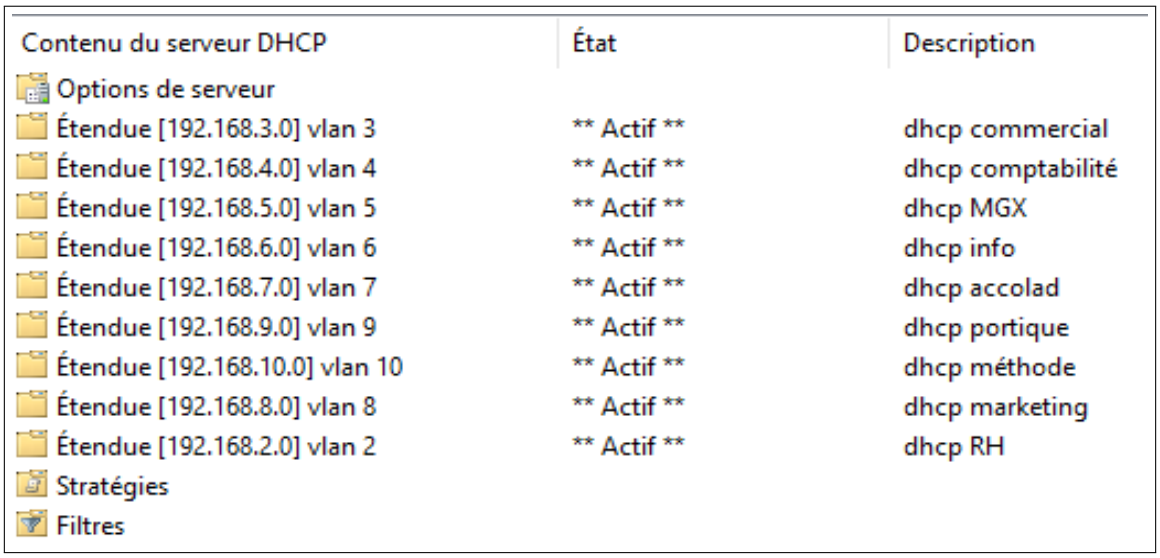

FIGURE V.20 – Liste des étendus crées.

4. **Réplication de chaque étendu dans serveur2 :**
   Pour assurer une synchronisation efficace et fiable du serveur2, on doit d'abord autoriser le serveur1 de gérer le serveur2, pour cela :

   - On clique droit sur DHCP ;

   - Gérer les serveurs autorisés ;

   - Sélectionner serveur2.bmt.local ;

   - OK.

   Par la suite, pour transférer les étendus au serveur2, les étapes à suivre sont illustrées dans la Figure V.21.

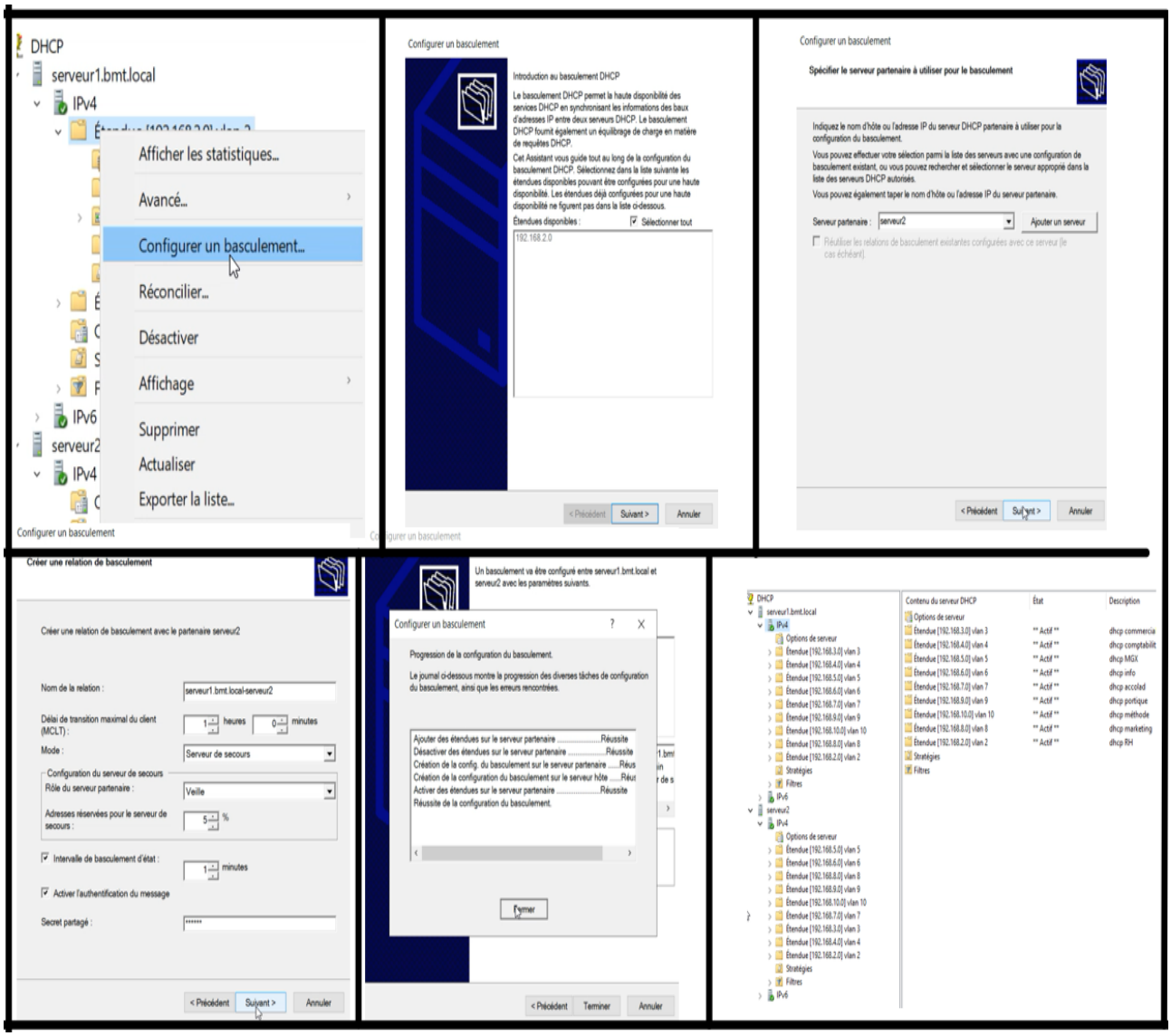

FIGURE V.21 – Réplication de l'étendu « vlan 2 » dans serveur2.

5. **Tester DHCP depuis un PC :**
   On vérifie l'obtention de l'adresse IP pour n'importe quel pc des vlans créé. dans notre cas on va tester dans le vlan 2 depuis le PC1 comme le montre la Figure V.22, en cas d'une panne de serveur1 le serveur2 prendra le relais pour distribuer les adresses IP aux machines.

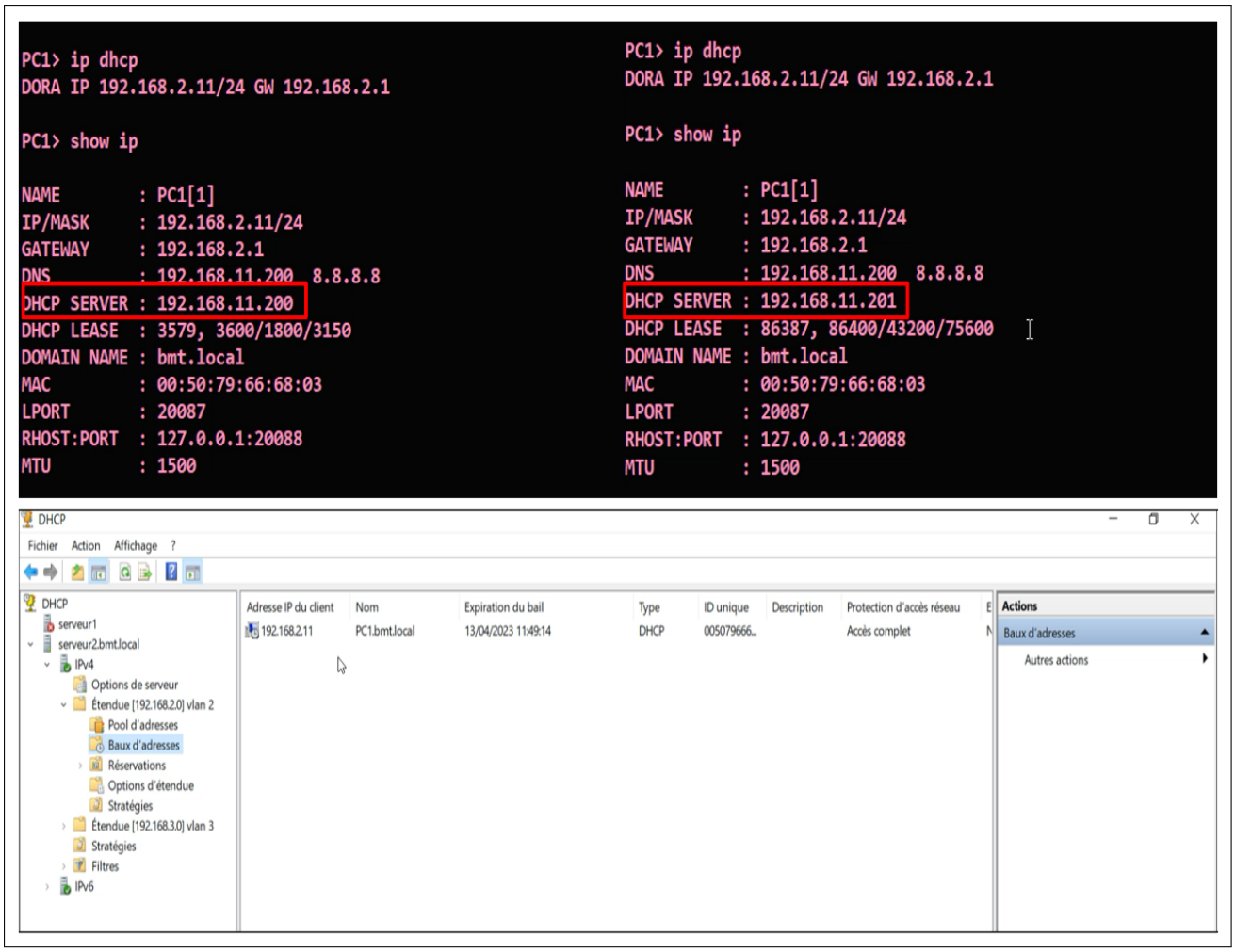

FIGURE V.22 – Obtention de l'adresse IP du PC1 de vlan 2.

V.6 Les configuration au niveu de fortigate :

1. **Exportation de l'image Fortigate sur Gns3 :**
   On a exporté l'image de FortiGate en suivant les étapes indiqué dans GNS3, en sélectionnant le fichier d'image et en configurant les paramètres appropriés pour créer un appareil FortiGate virtuel fonctionnel.

2. **Configuration de l'interface du FortiGate :**
   Après avoir installé l'image de FortiGate dans GNS3, on a configuré notre FortiGate en définissant les paramètres tels que les adresses IP comme la (Figure V.23) le montre.

   Remarque : notre topologie se compose de trois fortigate (version 7), et c'est les mêmes étapes a suivre pour configurer chacun des parfeus (firewalls).

   - L'adresse du FG-BMT1 192.168.11.1.
   - L'adresse du FG-BMT2 192.168.11.1.
   - L'adresse du FG-ZEP 10.1.0.5.

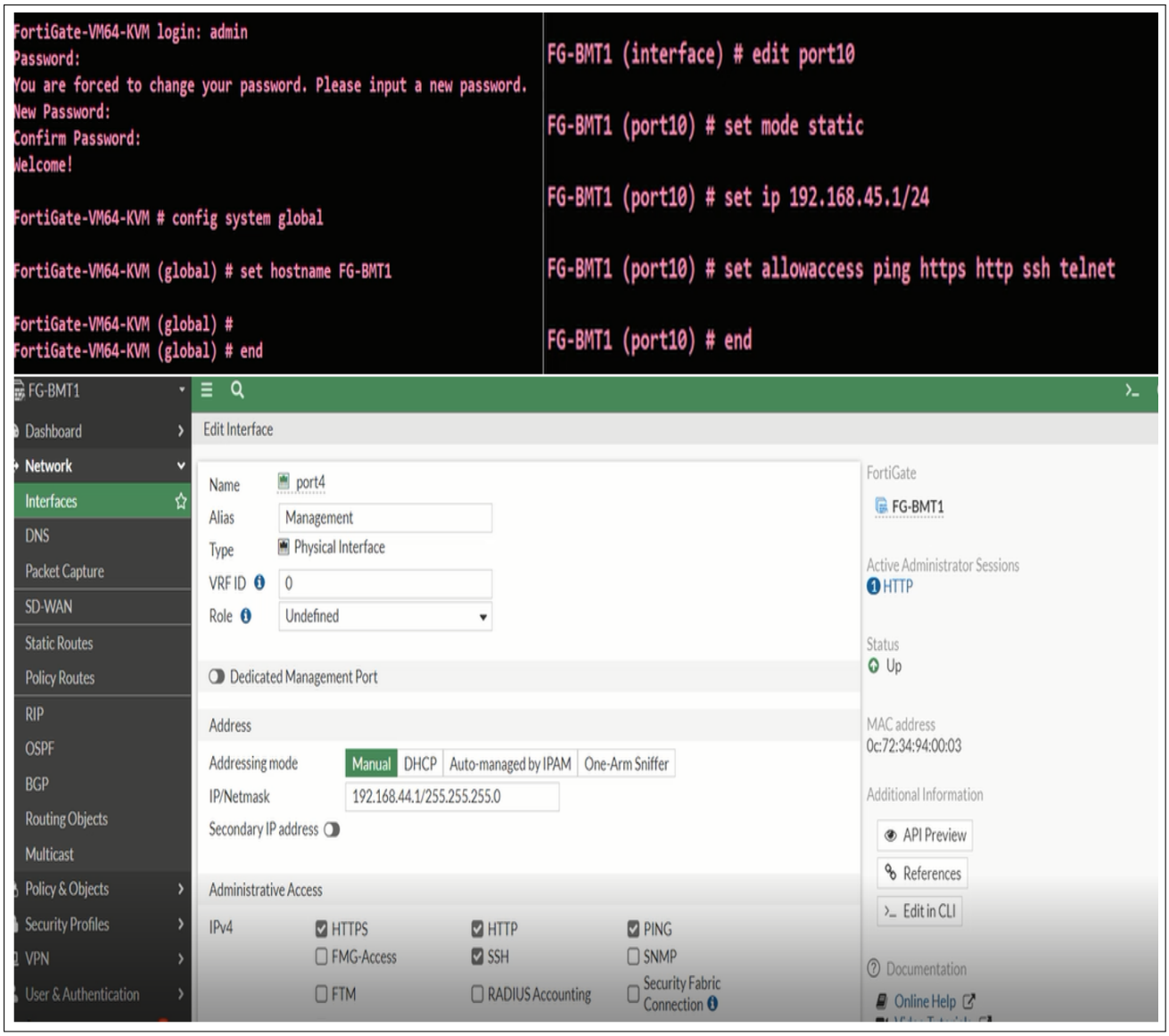

FIGURE V.23 – Configuration de l'interface du fortigate FG-BMT1.

3. **Création des VLANs :**
   Pour créer des VLAN (Figure V.24), on a configuré appareil FortiGate en définissant des interfaces virtuelles (VLAN) avec des identifiants uniques, puis on a attribué ces interfaces à des ports physiques spécifiques.

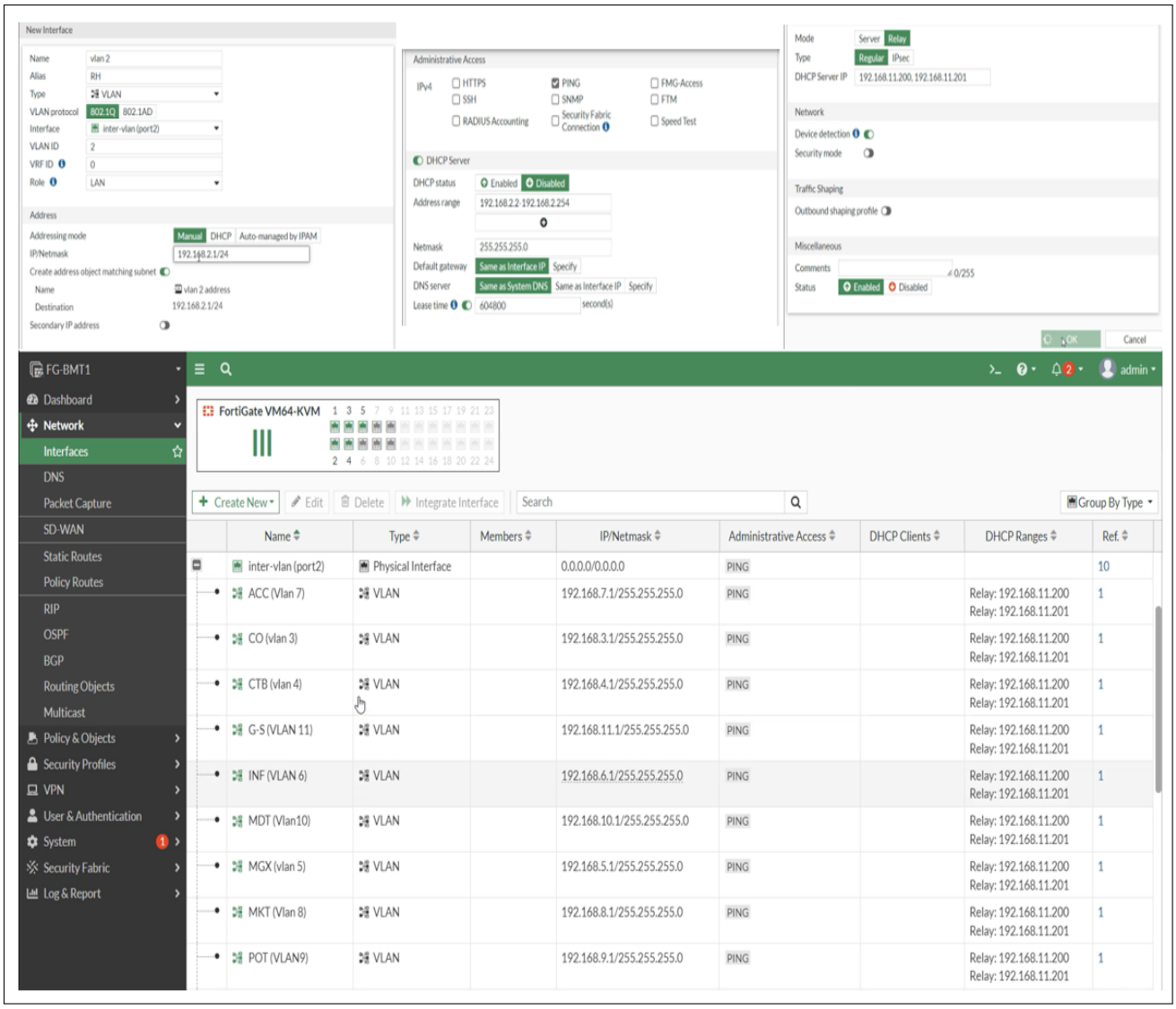

FIGURE V.24 – La création des VLANs dans Fortigate.

4. **Création de l'interface inter-vlan :**
   Pour créer une interface inter-VLAN sur FortiGate, on a configuré une interface physique (port 2) pour servir de lien de communication entre différents VLANs créés. On a attribué à cette interface les VLANs, et on a configuré les paramètres de routage appropriés ,montré dans la Figure V.25, tels que les adresses IP et les règles de routage, pour permettre le trafic entre les VLANs et assurer la connectivité inter-VLAN au sein de l'appareil FortiGate.

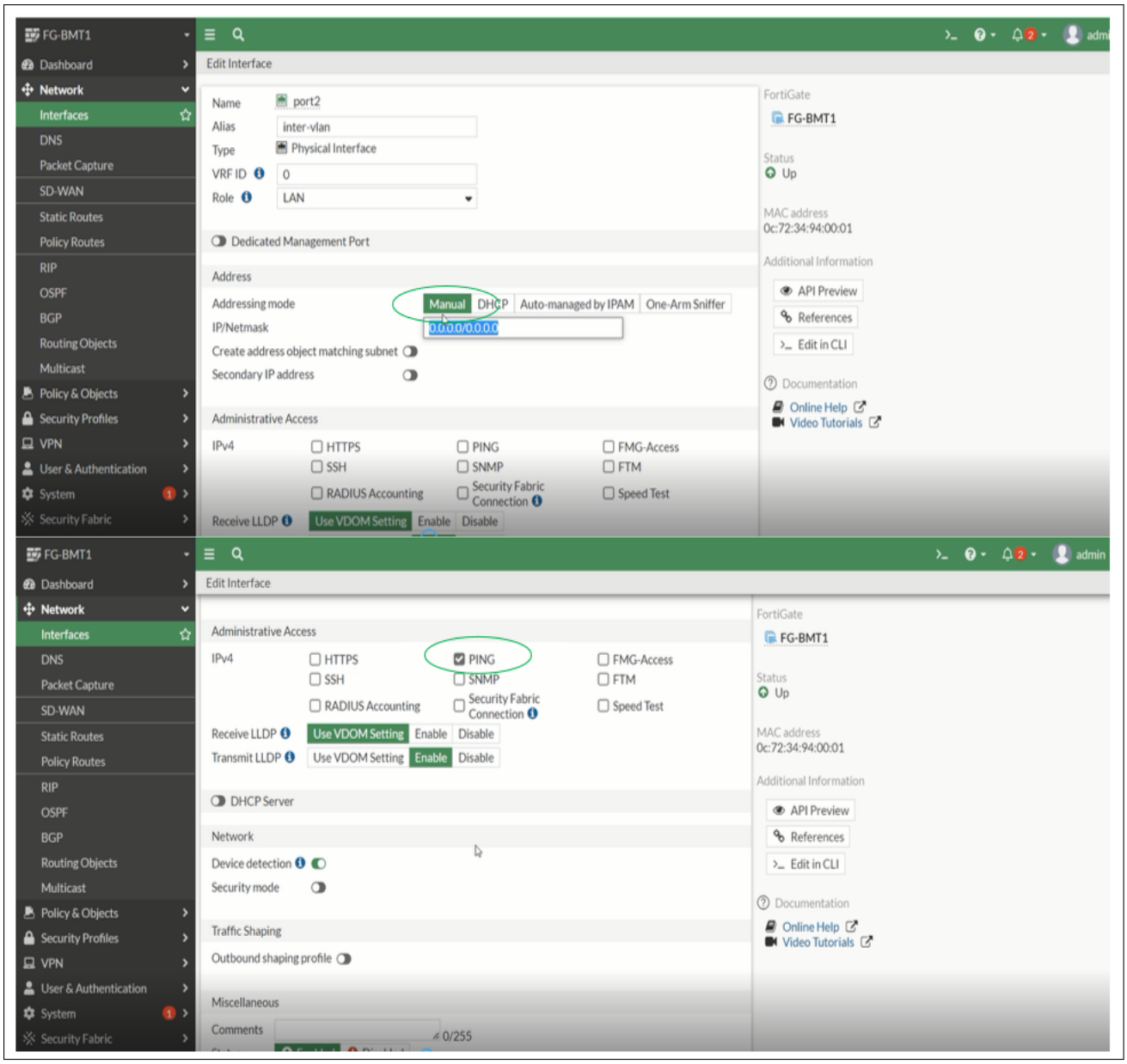

FIGURE V.25 – Création de l'interface inter-vlan.

5. **Configuration du routage inter-vlan :**
   Sur fortigate on a créé une nouvelle zone appelée inter-vlan ou on lui a attribué toutes les sous interfaces VLANs qu'on a établis , montré dans la Figure V.26.

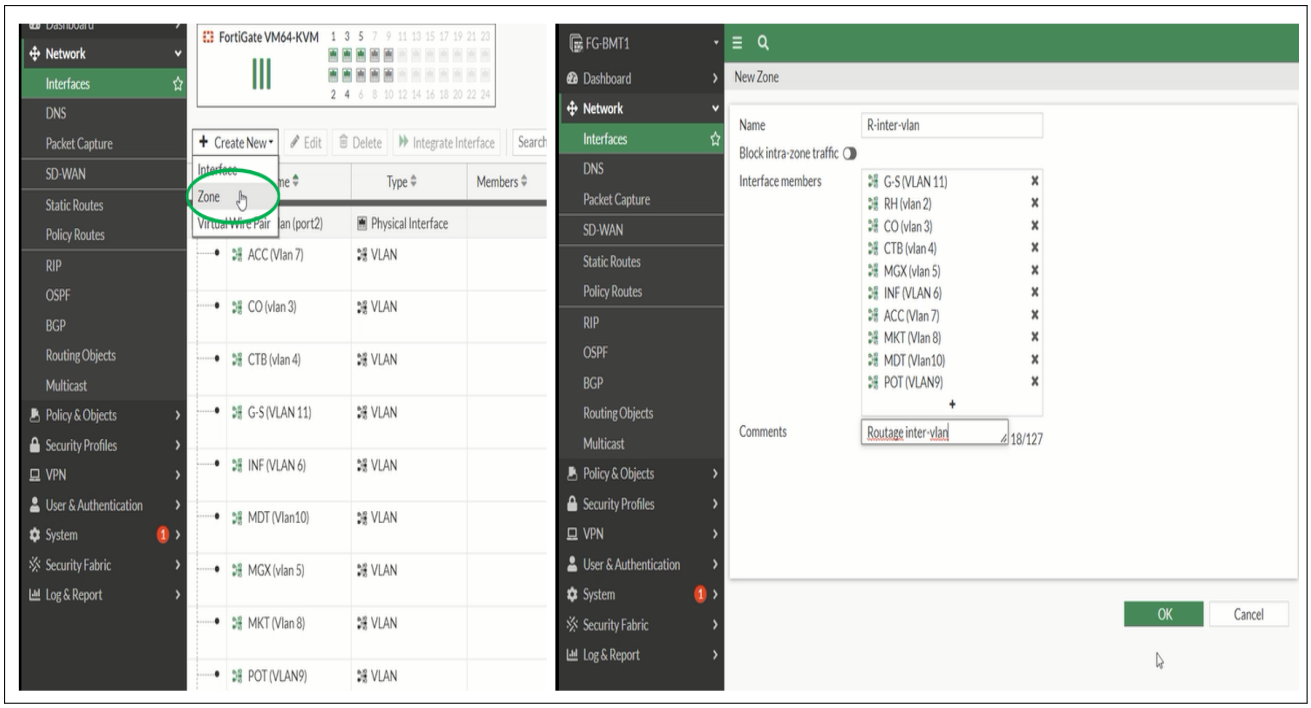

FIGURE V.26 – Configuration du routage inter-vlan.

6. **Création de la règle connexion internet sur fortigate :**
   La règle de connexion Internet permet d'appliquer des politiques de sécurité pour protéger notre réseau interne contre les menaces potentielles provenant d'Internet. La Figure V.27 illustre les etapes de la création de la règle Internet au niveau de FG-BMT1, cette derniére sera automatiquement crée dans le FG-BMT2 grace au cluster entre les deux pare-feu.Ce processus permet de synchroniser les règles de connexion entre eux (Firewalls).

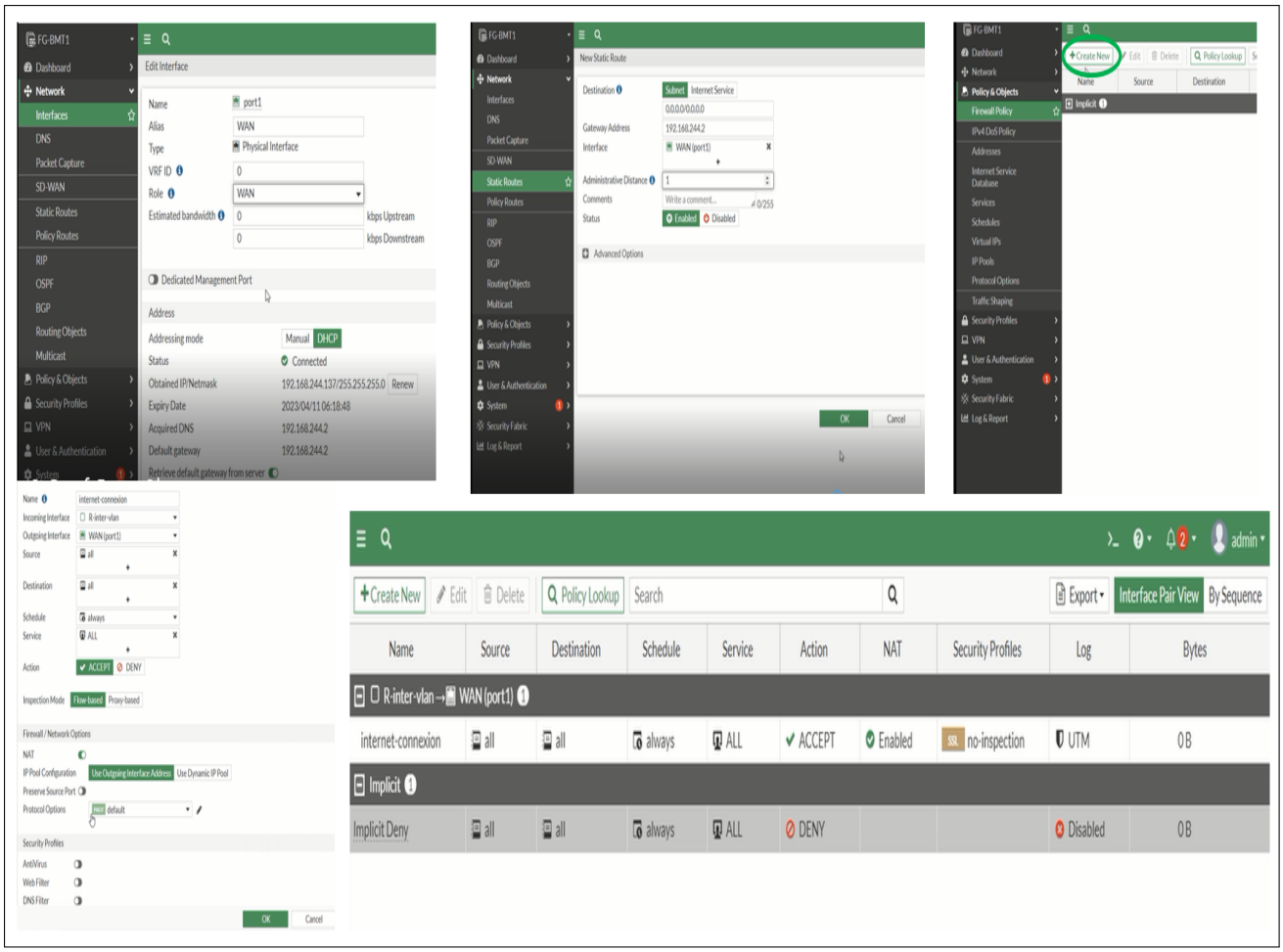

FIGURE V.27 – Création d'une règle connexion internet sur fortigate..

7. **Configuration de la haute disponibilité (HA) :**
   La configuration de la haute disponibilité (HA) sur FortiGate consiste à mettre en place un système redondant afin d'assurer la continuité des services en cas de défaillance d'un appareil. On a configuré l'interface (port3) de FB-BMT1, en mode HA actif-actif. montré dans la Figure V.28.

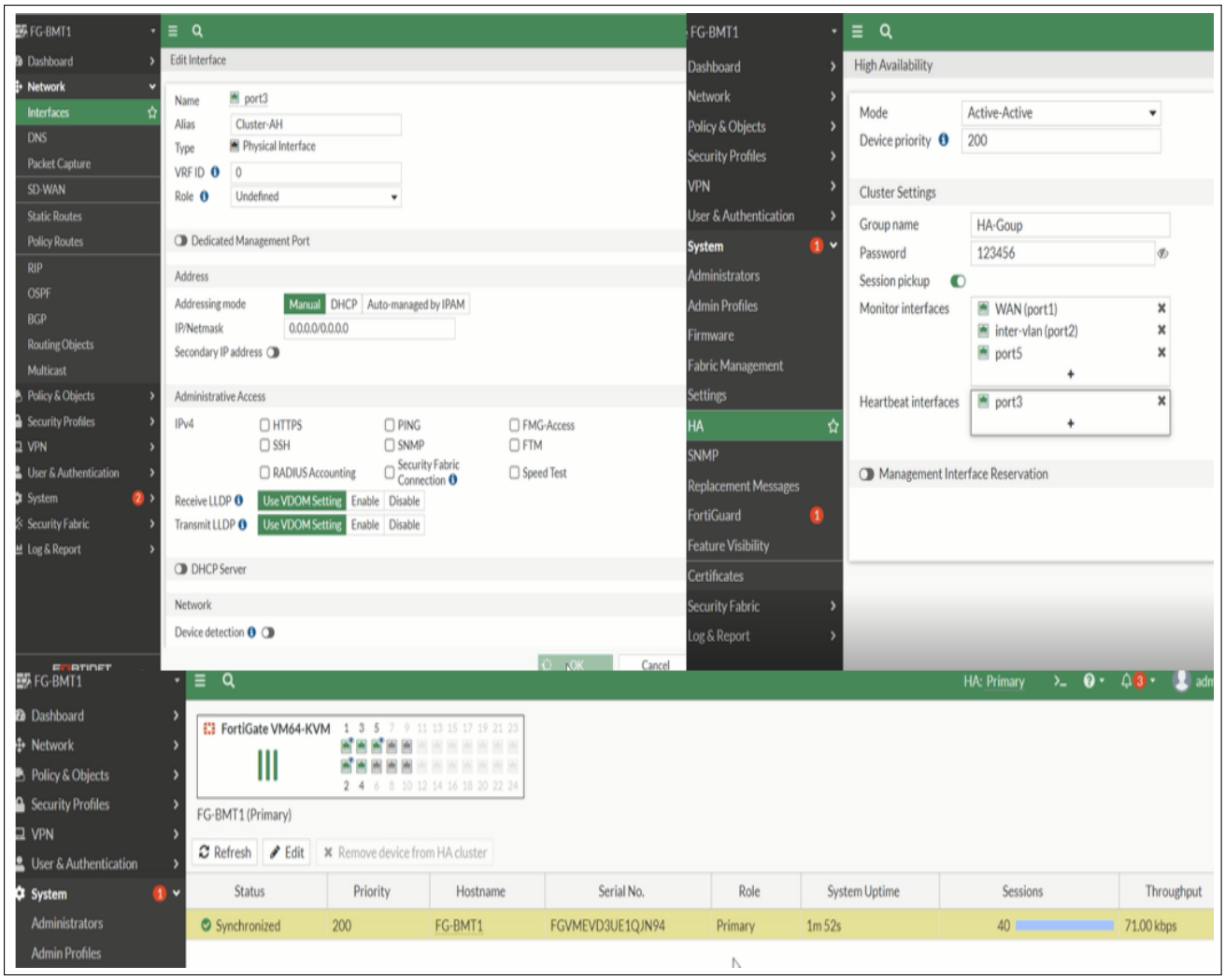

Figure V.28 – Configuration HA dans FB-BMT1.

Ensuite , on a synchronisé les configurations et les connexions (clustering) dans le deuxième fortigate (FG-BMT2), de sorte que si l'appareil principal tombe en panne, l'appareil de secours prend automatiquement le relais, minimisant ainsi les temps d'arrêt et assurant une disponibilité élevée du réseau, présenté dans la Figure V.29.

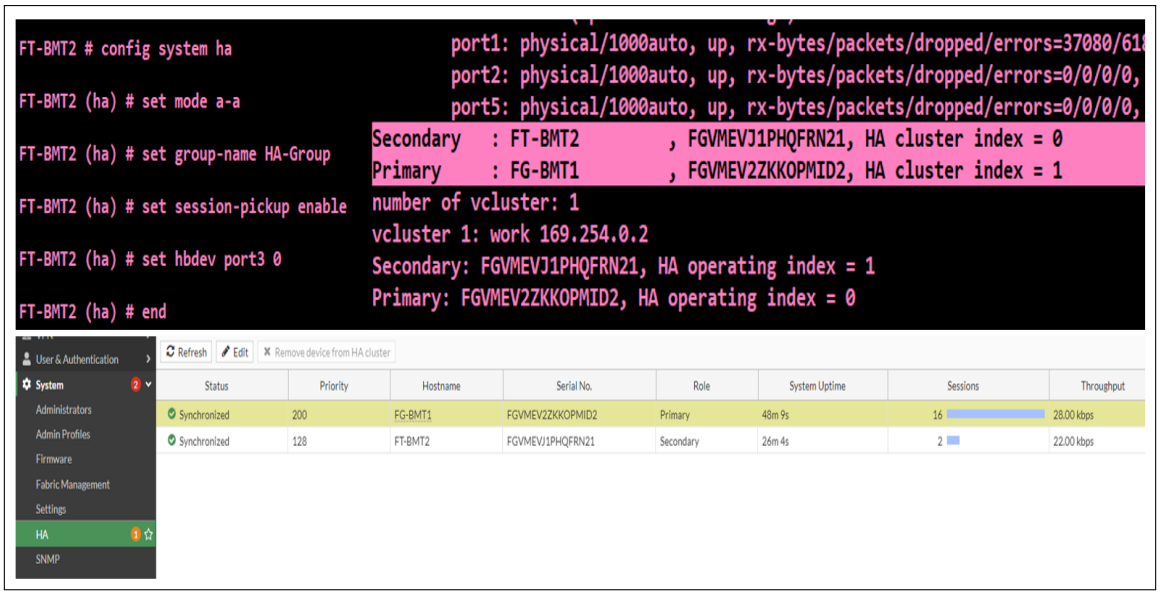

FIGURE V.29 – Synchronisation des deux fortigates.

8. **Test du cluster entre FG-BMT1 et FG-BMT2 :**
   Pour effectuer un test sur le cluster(Figure V.30), il est nécessaire d'éteindre le pare-feu principal, FG-BMT1. En faisant cela, on pourra observer que le deuxième pare-feu prendra automatiquement le relais et deviendra le pare-feu primaire.

FIGURE V.30 – Test du cluster entre FG-BMT1 et FG-BMT2.

9. **Connectivité des deux fortigates FG-BMT1 et FG-ZEP :**
   Une fois les adresses des routeurs intermédiaires configurées et le routage mis en place, la connectivité entre les deux FortiGates de BMT et de Zep est établie, permettant ainsi un flux de données sécurisé et une communication efficace entre les réseaux des deux entités comme la Figure V.31 le montre.

FIGURE V.31 – Routage des deux fortigates FG-BMT1 et FG-ZEP.

10. **Test sur Connectivité des deux fortigates FG-BMT1 et FG-ZEP :**
Afin de vérifier la connectivité entre les deux FortiGates et s'assurer que le routage est correctement configuré, on effectue un test de ping (Figure V.32).

```
FG-BMT1 # execute ping 10.1.0.5
PING 10.1.0.5 (10.1.0.5): 56 data bytes
64 bytes from 10.1.0.5: icmp_seq=0 ttl=254 time=4.1 ms
64 bytes from 10.1.0.5: icmp_seq=1 ttl=254 time=3.1 ms
64 bytes from 10.1.0.5: icmp_seq=2 ttl=254 time=3.0 ms
64 bytes from 10.1.0.5: icmp_seq=3 ttl=254 time=7.7 ms
64 bytes from 10.1.0.5: icmp_seq=4 ttl=254 time=7.3 ms

--- 10.1.0.5 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.0/5.0/7.7 ms

FG-ZEP # execute ping 10.1.0.1
PING 10.1.0.1 (10.1.0.1): 56 data bytes
64 bytes from 10.1.0.1: icmp_seq=3 ttl=254 time=5.8 ms
64 bytes from 10.1.0.1: icmp_seq=4 ttl=254 time=4.0 ms

--- 10.1.0.1 ping statistics ---
5 packets transmitted, 2 packets received, 60% packet loss
round-trip min/avg/max = 4.0/4.9/5.8 ms
```

FIGURE V.32 – Test de ping entre FB-BMT1 et FG-ZEP.

11. **La configuration des deux interfaces Port1 et Port3 du Fortigate ZEP :**
Les interfaces du FortiGate de Zep on les configurées pour assurer une connectivité efficace et sécurisée. Le port1 a été configuré pour le WAN, afin de permettre la mise en place de la règle Internet. Quant au port3, on les configuré pour le LAN2, dans le but de mettre en place un routage statique (Figure V.33).

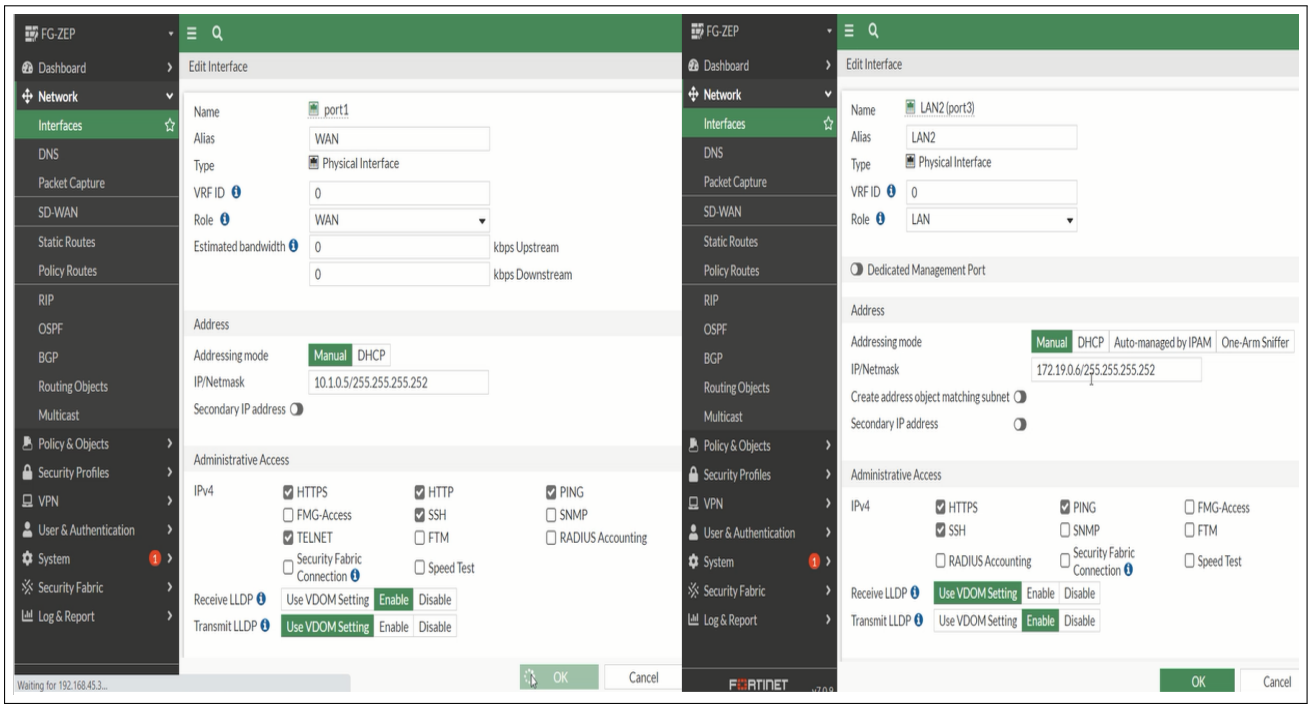

FIGURE V.33 – La configuration des interfaces Port1 et Port3.

12. **La création d'une règle internet sur Fortigate ZEP :**
Vu que nos deux fortigates (FG-BMT1 et FG-ZEP) doivent communiquer entre eux une règle internet doit être crée, présenté dans la Figure V.34 suivante.

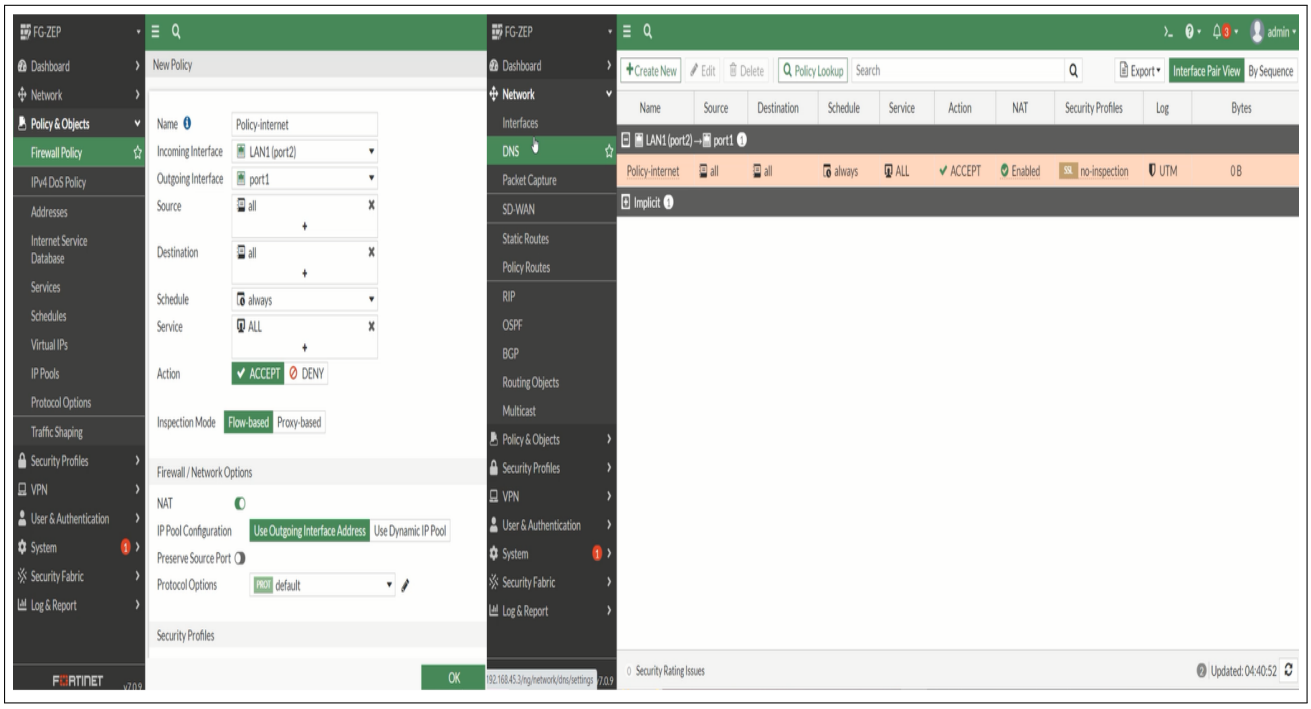

FIGURE V.34 – La création d'une règle internet.

13. **Configuration VPN :**
Dans la section VPN de notre projet, nous allons configurer deux types de VPN. Le VPN site to site permettra de connecter de manière sécurisée deux réseaux locaux distincts, à savoir le réseau de la BMT et le réseau de ZEP, et le VPN client to site qui permet aux utilisateurs externes de se connecter de manière sécurisée au réseau de l'entreprise BMT.

A) **VPN site to site :**
Pour configurer un VPN site to site on suit les étapes suivantes :

- **Configuration des interfaces :** on doit s'assurer que les interfaces appropriées sur chaque FortiGate sont configurées avec les adresses IP correctes et qu'elles sont reliées aux réseaux locaux respectifs (Figure V.35).

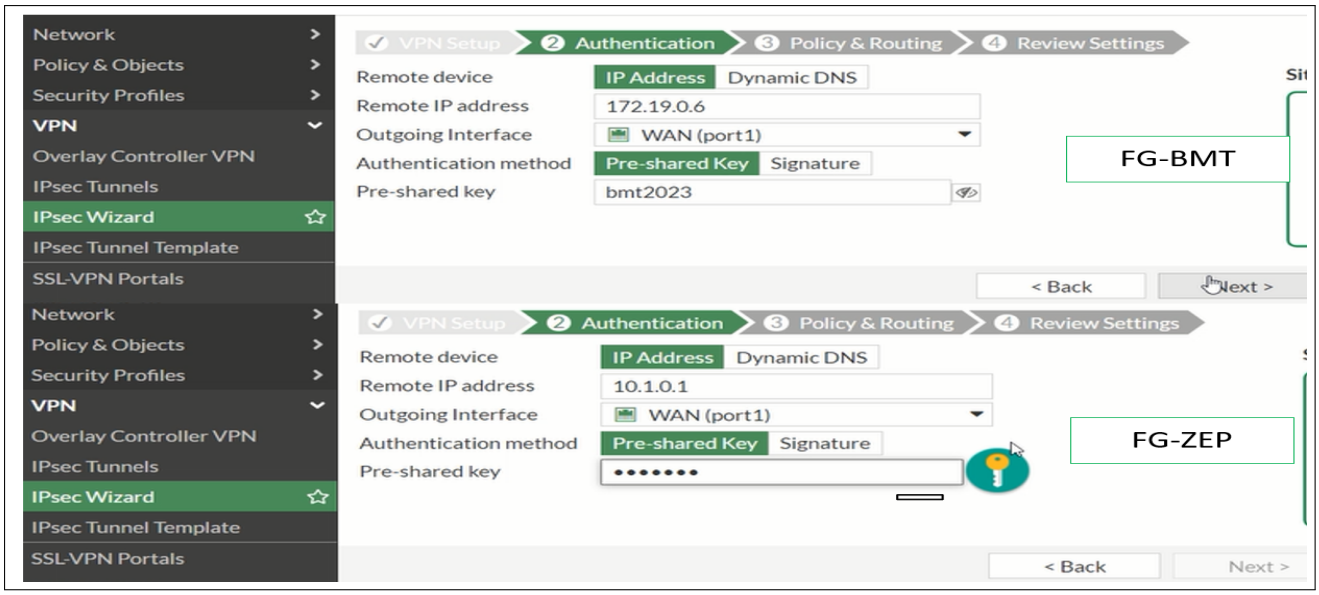

FIGURE V.35 – Configuration des interfaces appropries.

Configuration des politiques de sécurité : on doit créer des politiques de sécurité sur chaque FortiGate pour autoriser le trafic entre les réseaux locaux et distants. Ces politiques doivent spécifier les adresses IP source et de destination, ainsi que les services et protocoles autorisés (Figure V.36).

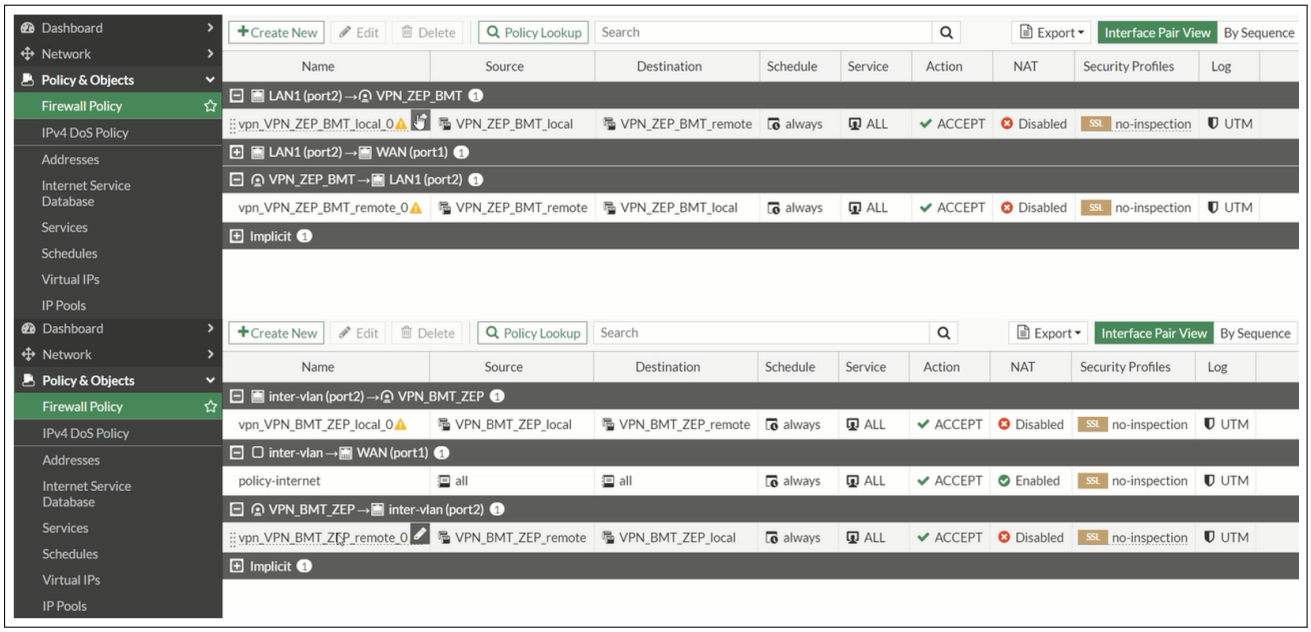

FIGURE V.36 – Création des politiques de sécurité.

- **Création du tunnel VPN :** on va configurer un tunnel VPN sur chaque FortiGate (Figure V.37). On doit spécifier les paramètres de chiffrement, les clés partagées et les adresses IP des passerelles VPN de chaque côté.

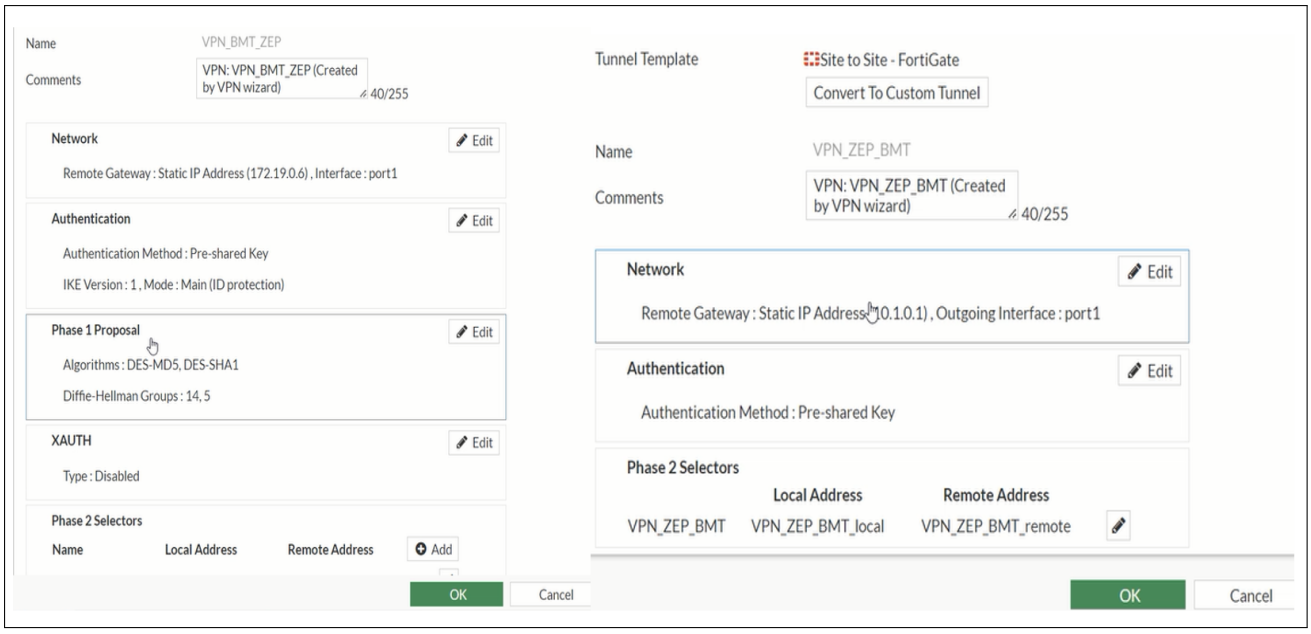

FIGURE V.37 – Configuration des algorithmes de chiffrements sur les deux fortigates.

- **Configuration des routes :** on ajoute des routes statiques sur chaque FortiGate pour diriger le trafic du réseau local vers le tunnel VPN (Figure V.38).

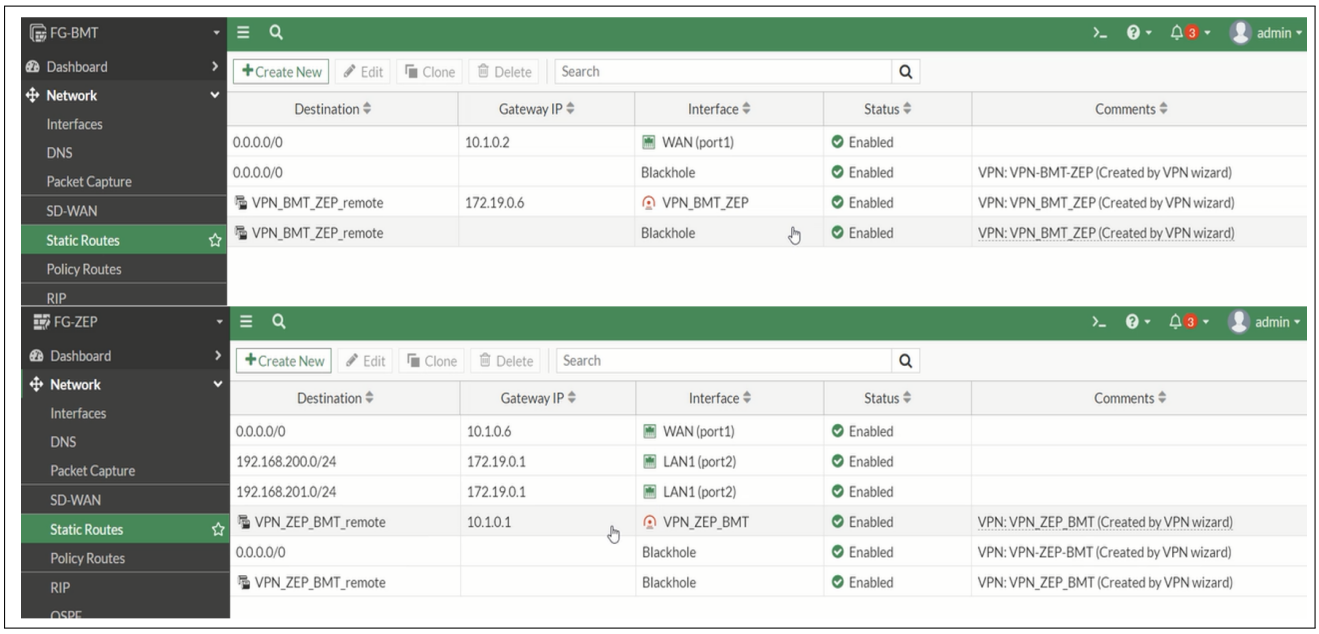

FIGURE V.38 – Configuration des routes statiques sur les deux fortigates.

Après avoir suivi ces étapes on aura le résultat représenté dans la Figure V.39 :

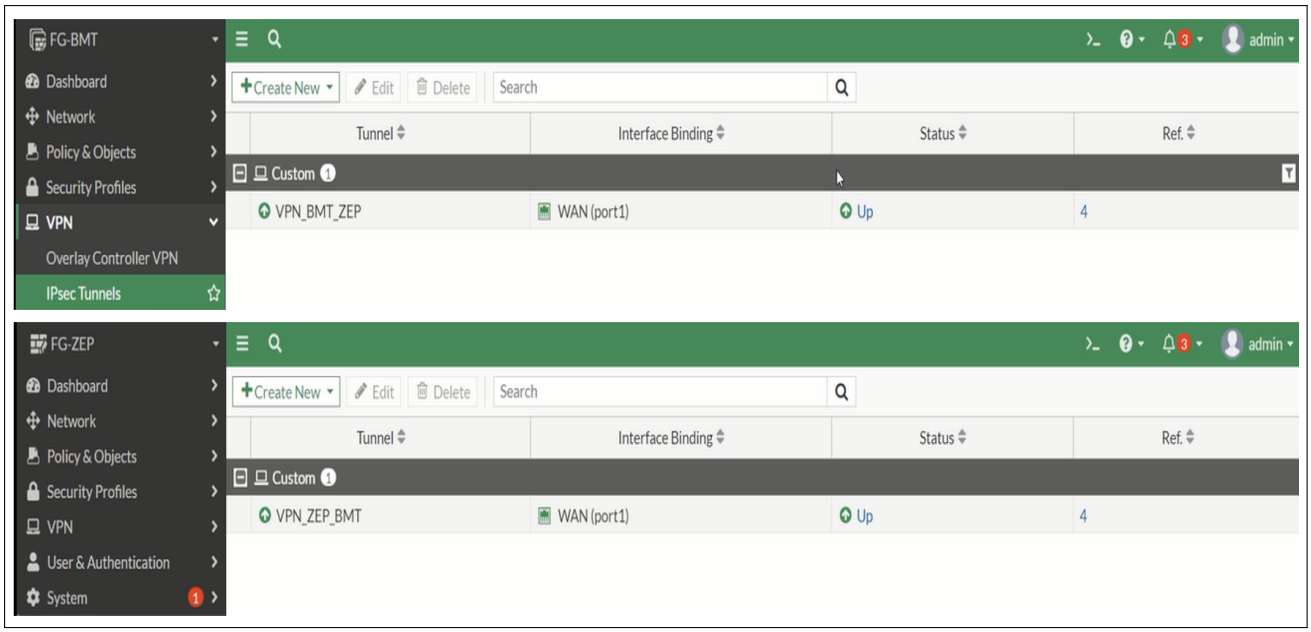

FIGURE V.39 – Les deux tunnels VPN sur les deux fortigates.

- **Test et vérification de la négociation entre les deux fortigates :** Une fois que le VPN site-to-site est configuré, on accède à :
Log&Report ensuite Events après VPN Events on obtient le résultat présenté dans la Figure V.40 suivante.

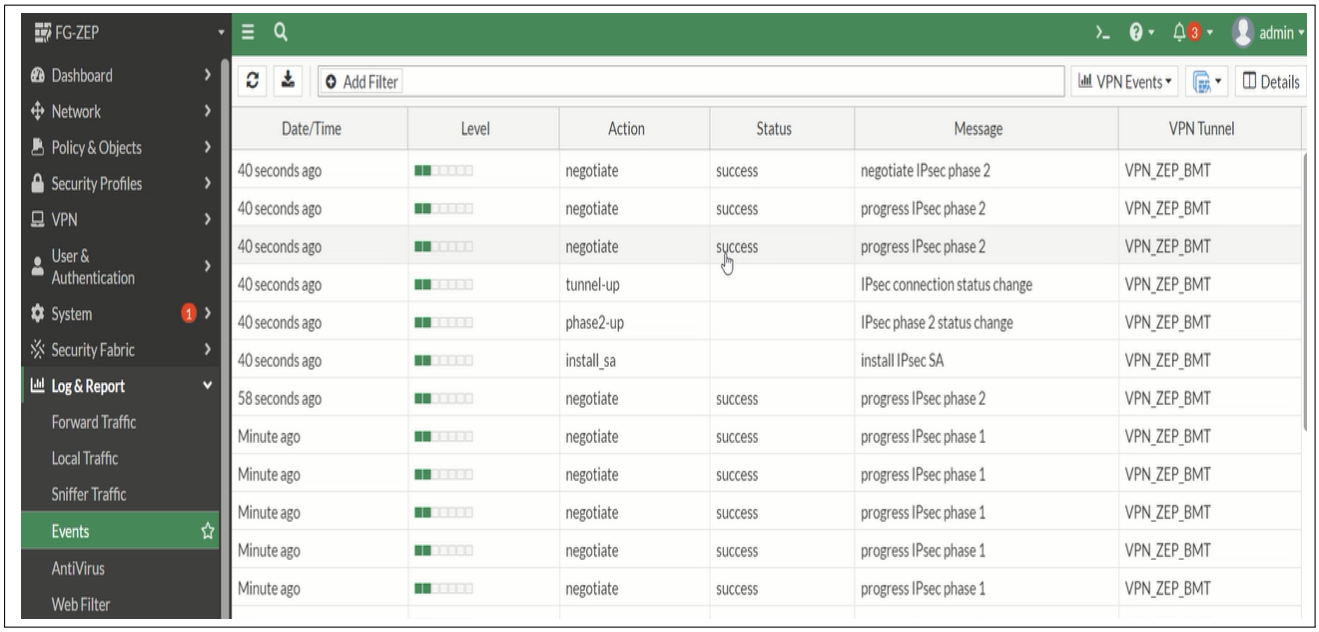

FIGURE V.40 – Résultat de négociation entre les deux fortigates.

B) **Configuration du VPN Client-to-site :**
Pour configurer un VPN Client-to-Site on suit l'ensemble des étapes suivantes :

• **Configuration des adresses IP :**La première étape consiste à configurer les adresses au niveau du routeur intermédiaire. Ensuite, nous accédons à la machine virtuelle Client VPN et configurons la connexion réseau en accédant à la carte réseau Ethernet 0,

- Au niveau du routeur EDGE-AT L'adresse est : 172.168.10.1, avec un masque de 255.255.0.0.
- Au niveau de la carte réseau Ethernet0 l'adresse est :172.168.10.10, avec un masque de 255.255.0.0.

• **Création du VPN :** Pour mettre en place un VPN, il est nécessaire de suivre plusieurs étapes. Tout d'abord, il faut créer une adresse IP locale spécifique au réseau, puis configurer les règles de firewalling pour renforcer la sécurité. Ensuite, il est essentiel de créer les utilisateurs et les groupes associés qui auront accès au VPN et aux ressources internes du réseau.

i. **Création d'une adresse IP locale :**Pour identifier et router le trafic de l'ordinateur distant à travers le VPN vers les ressources internes du réseau ,une adresse IP locale sera crée comme la Figure V.41 le montre :

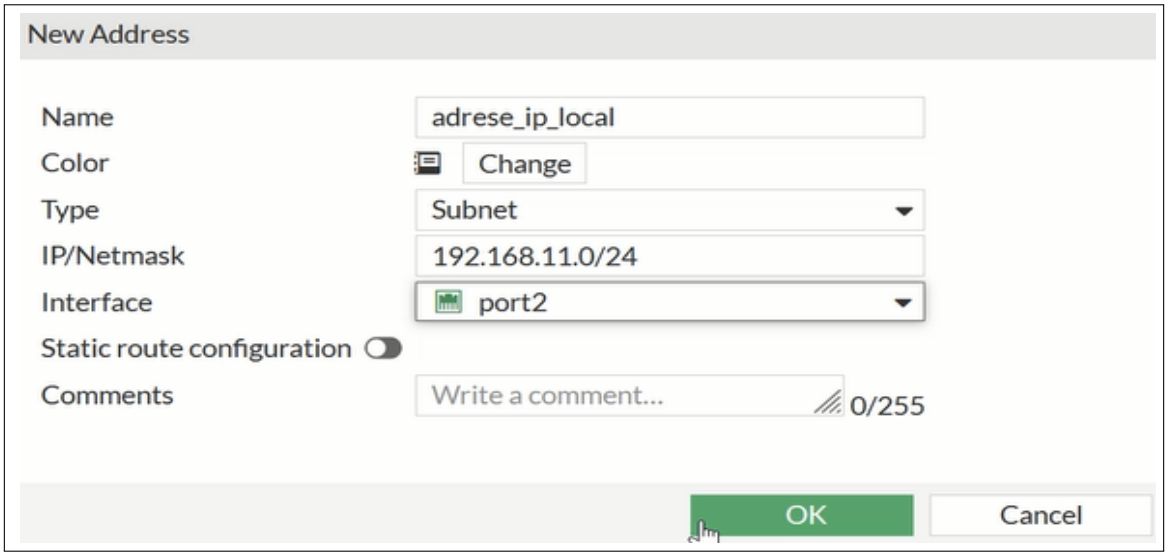

FIGURE V.41 – Création d'une adresse IP locale.

ii. **Création d'une régle firwalling :** Après avoir créé une adresse IP locale dans un VPN client-to-site, on met en place une règle firewalling pour renforcer la sécurité du réseau, elle permet de contrôler et de filtrer le trafic entrant et sortant du réseau ,illustré dans la Figure V.42 ci-dessous :

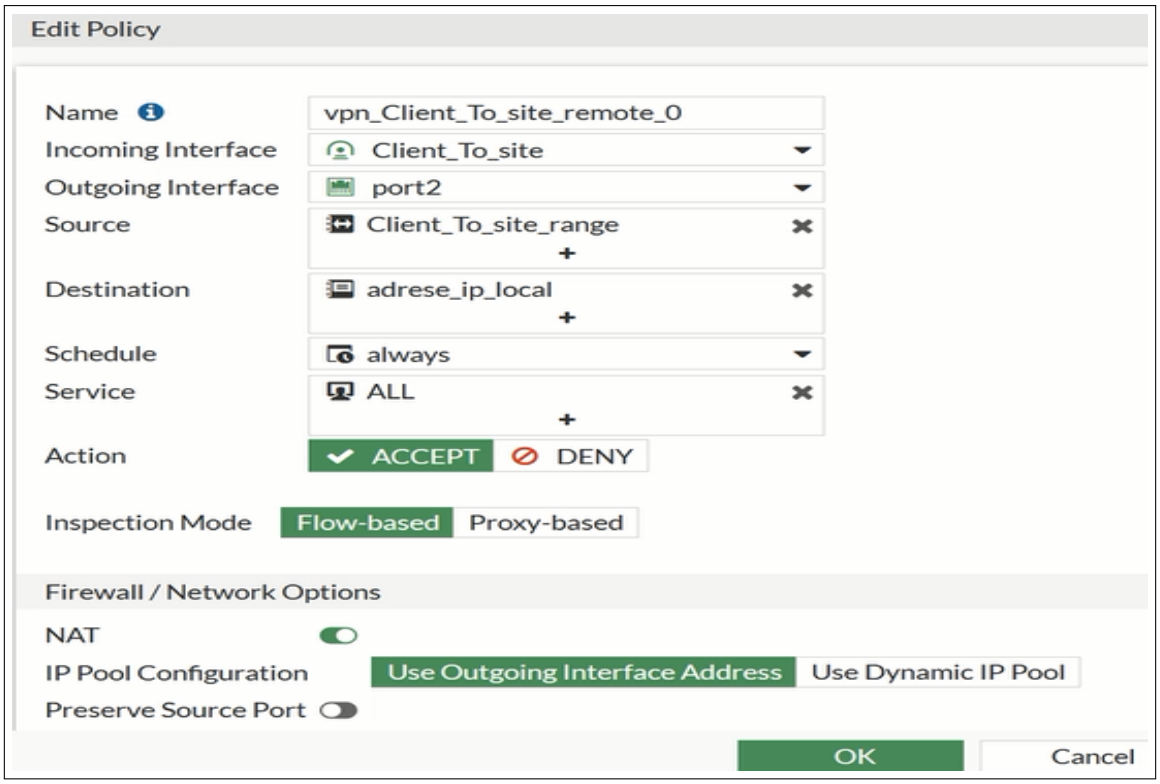

Figure V.42 – Création d'une régle firewalling.

iii. **Création des comptes utilisateurs :**Afin de permettre aux utilisateurs d'une organisation, tels que les employés de l'entreprise BMT, de se connecter de manière sécurisée, il est nécessaire de créer manuellement ces utilisateurs lors de la configuration du VPN. Pour créer un compte utilisateur, on peut suivre les étapes illustrées dans la Figure V.43 ci-dessous.

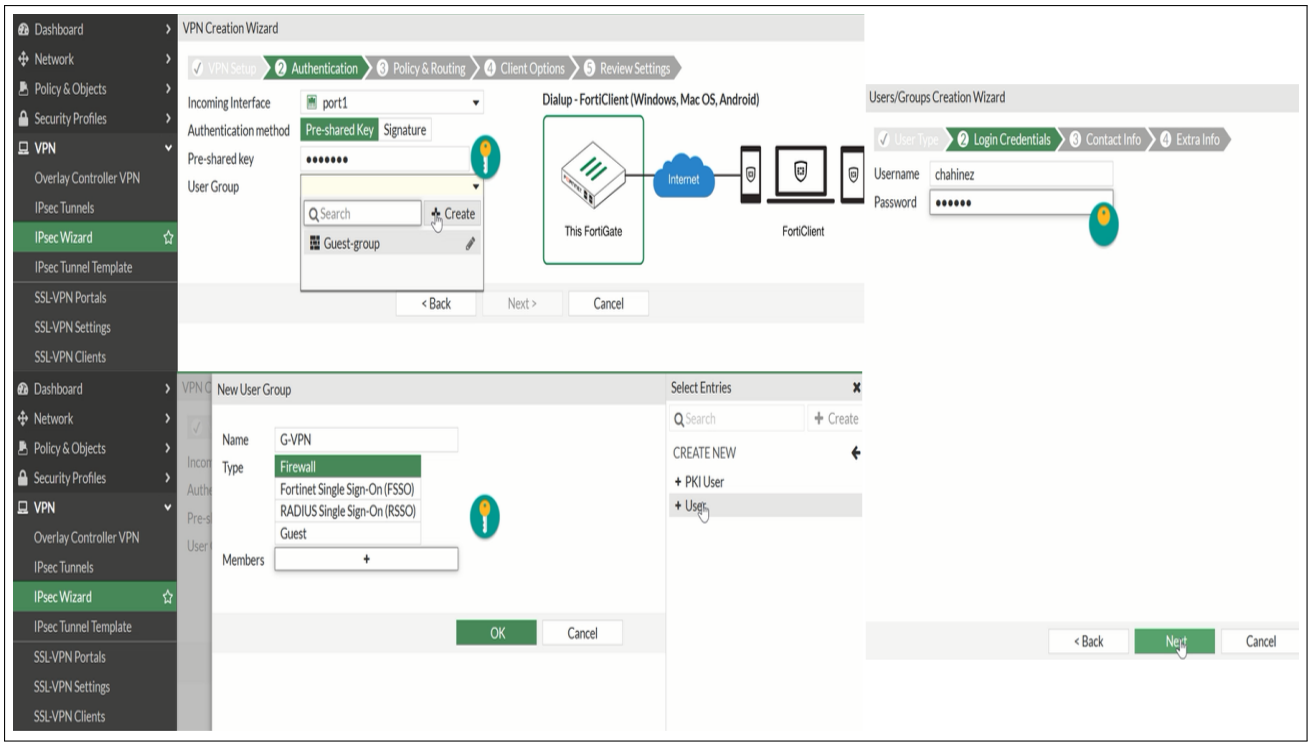

FIGURE V.43 – Création d'un utilisateur.

iv. **Création d'un groupe :**Pour regrouper les utilisateurs crées ayant des besoins et des paramètres similaires, on peut suivre les étapes montrées dans la Figure V.44 suivante :

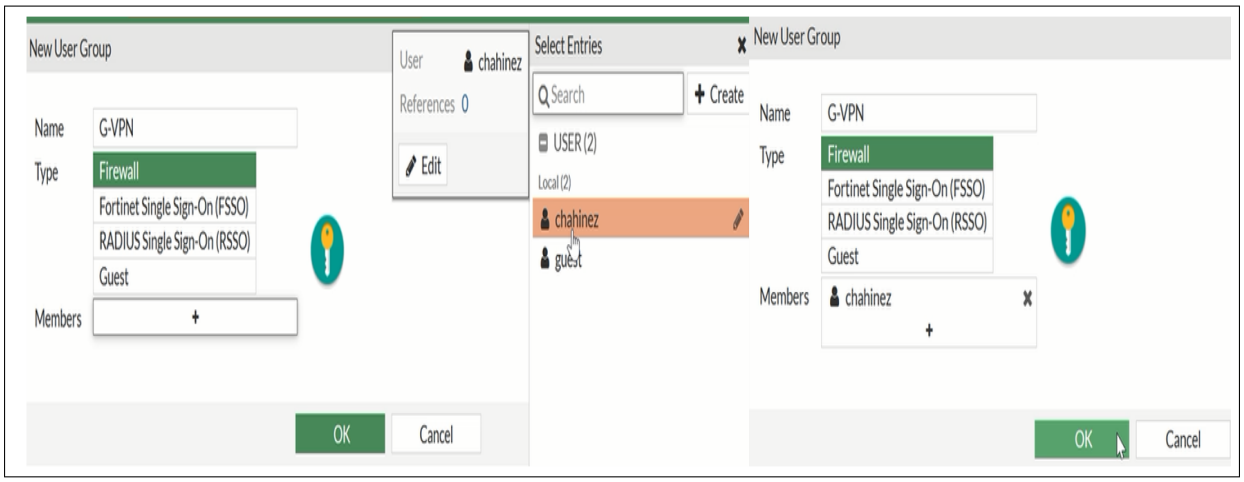

FIGURE V.44 – Création d'un groupe.

Après avoir créer les utilisateurs et les groupes, on peut maintenant continuer la création de notre VPN en suivant les étapes illustrées dans la Figure V.45 ci-dessous :

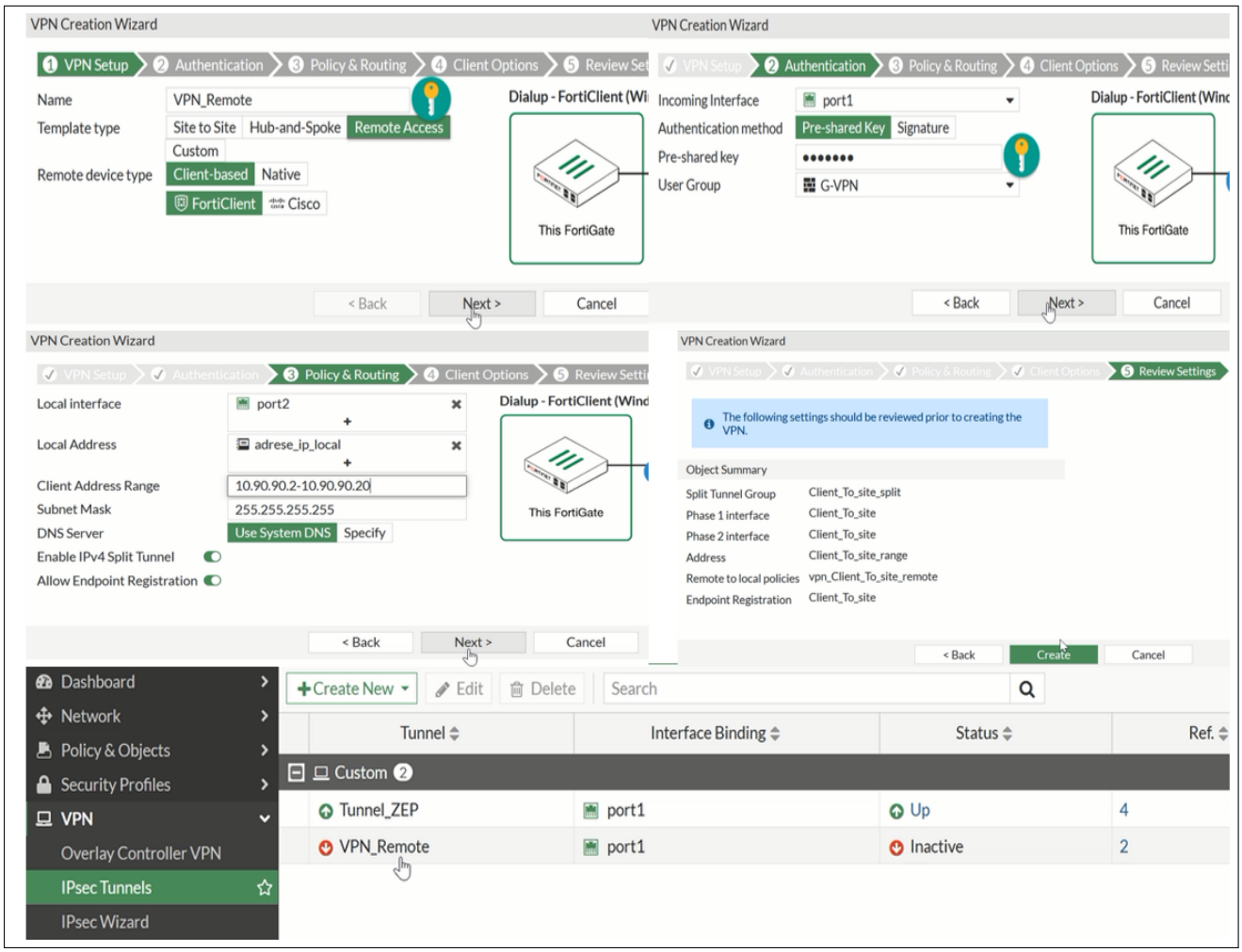

FIGURE V.45 – Création du VPN.

• **Configuration des algorithmes de chiffrement du tunnel VPN :** Avant de lancer le VPN que nous avons créé, il est essentiel de procéder à la vérification et à la configuration des algorithmes de chiffrement et d'authentification. Cette étape permet d'assurer la confidentialité des données, l'intégrité des informations et l'authenticité des échanges. En configurant les algorithmes appropriés, on pourra garantir que seules les parties autorisées peuvent accéder aux données échangées, détecter toute altération ou modification indésirable et maintenir la sécurité des informations transitant à travers le VPN montrée dans la Figure V.46 :

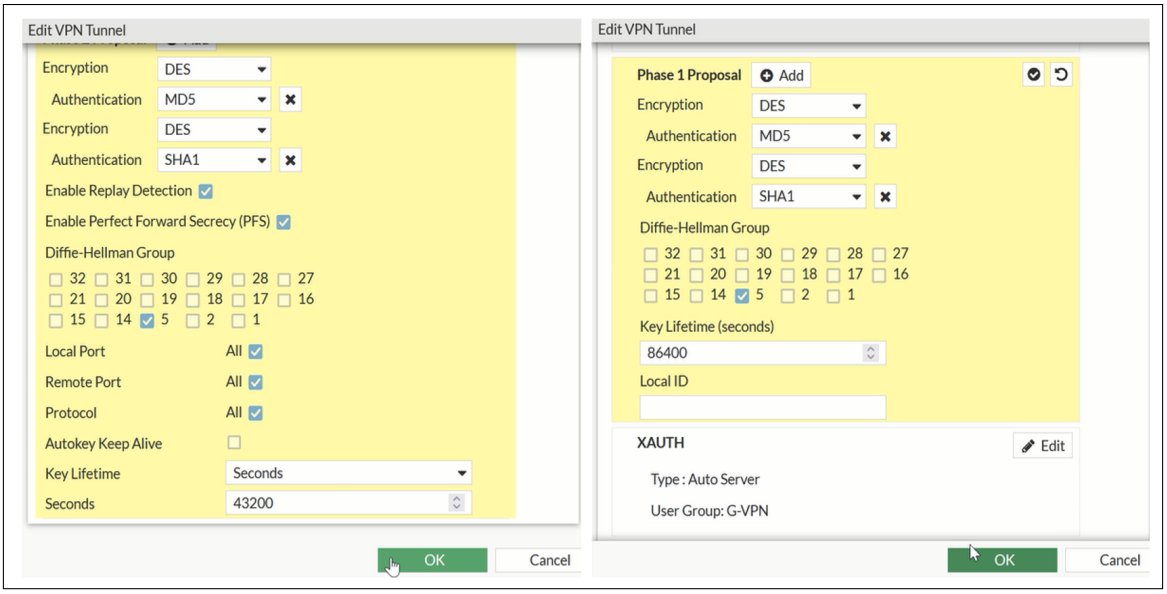

FIGURE V.46 – Configuration des algorithmes de chiffrement.

• **La configuration de FortiClient VPN :** La configuration de FortiClient dans un VPN client-to-site implique plusieurs étapes essentielles pour permettre aux utilisateurs distants de se connecter de manière sécurisée au réseau de l'entreprise.

- La première étape consiste à installer FortiClient sur l'ordinateur distant. Une fois installé, il est nécessaire de configurer les paramètres de connexion du VPN. Cela inclut la spécification de l'adresse IP ou du nom de domaine du serveur VPN, ainsi que les informations d'identification nécessaires, telles que le nom d'utilisateur et le mot de passe et la passerelle IP, illustré dans la Figure V.47 ci-dessous :

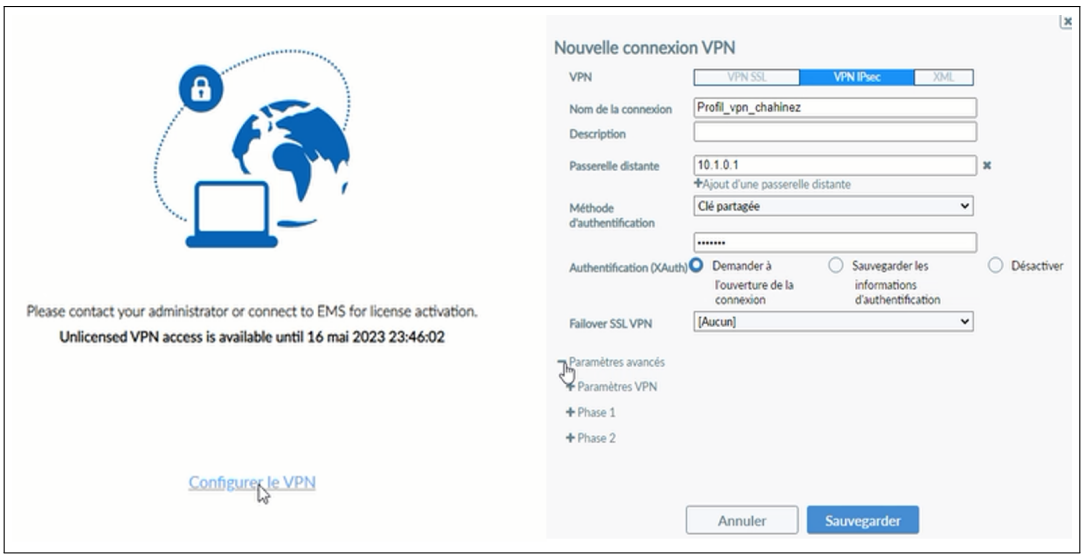

FIGURE V.47 – Configuration d'une connexion VPN.

- Ensuite, il faut configurer les paramètres de sécurité du VPN, tels que les protocoles de chiffrement et d'authentification, présenté dans la Figure V.48.

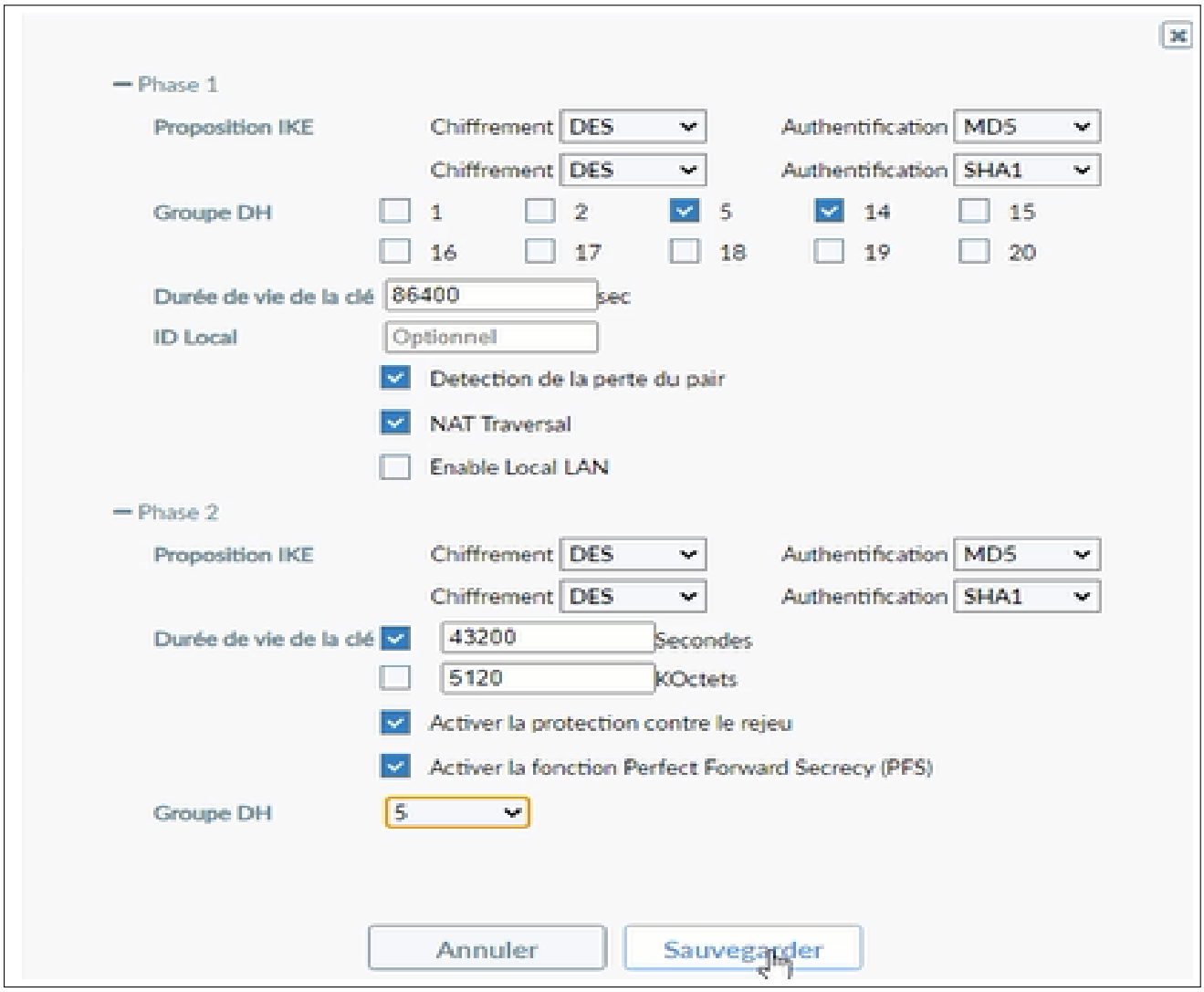

Figure V.48 – Configuration des paramètres de sécurité VPN.

- Une fois la configuration terminée, l'utilisateur peut lancer FortiClient et établir la connexion VPN. FortiClient créera alors un tunnel sécurisé entre l'ordinateur distant et le réseau de l'entreprise, permettant à l'utilisateur d'accéder aux ressources internes, comme les fichiers partagés, les applications et les services, de manière sécurisée, montré dans la Figure V.49.

FIGURE V.49 – Lancement d'une connexion VPN.

• **Test de l'état du tunnel VPN après avoir lancer une connexion :** La connexion est établie entre le client distant et le réseau de l'entreprise via un protocole de numérotation (dial-up), comme la Figure V.50 le montre :

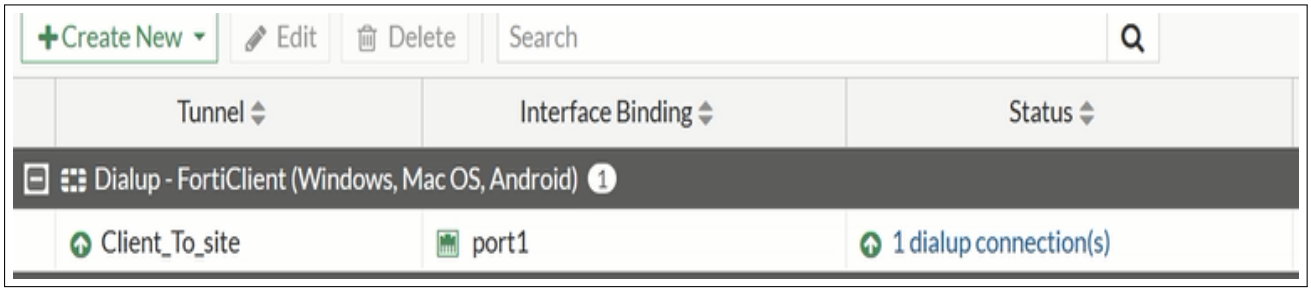

FIGURE V.50 – Établissement d'une connexion entre client distant et le réseau.

• **Test du ping de la machine ClientVPN vers les VLANs :** Après avoir configurer la machine ClientVPN, on va effectuer des pings(Figure V.51) vers les VLANs du coté de FG-BMT1.

```
C:\Users\ASR>ping 192.168.2.1

Envoi d'une requête 'Ping'  192.168.2.1 avec 32 octets de données :
Réponse de 192.168.2.1 : octets=32 temps=24 ms TTL=255
Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.2.1 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 192.168.2.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 24ms, Moyenne = 7ms

C:\Users\ASR>ping 192.168.3.1

Envoi d'une requête 'Ping'  192.168.3.1 avec 32 octets de données :
Réponse de 192.168.3.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.3.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.3.1 : octets=32 temps=3 ms TTL=255
Réponse de 192.168.3.1 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 192.168.3.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\ASR>ping 192.168.4.1

Envoi d'une requête 'Ping'  192.168.4.1 avec 32 octets de données :
Réponse de 192.168.4.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.4.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.4.1 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.4.1 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 192.168.4.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
```

FIGURE V.51 – Ping de la machine clientVPN vers l'ensemble des VLANs.

V.7 Configuration de ESXI :

Pour bien configurer ESXI et pouvoir ensuite installer nos deux serveurs, on doit suivre les étapes suivantes :

1. **Création d'un commutateur virtuel :**
   Premièrement on doit crée un commutateur vSphere standard pour assurer la connectivité réseau des hôtes et des machines virtuelles et pour gérer le trafic (Figure V.52).

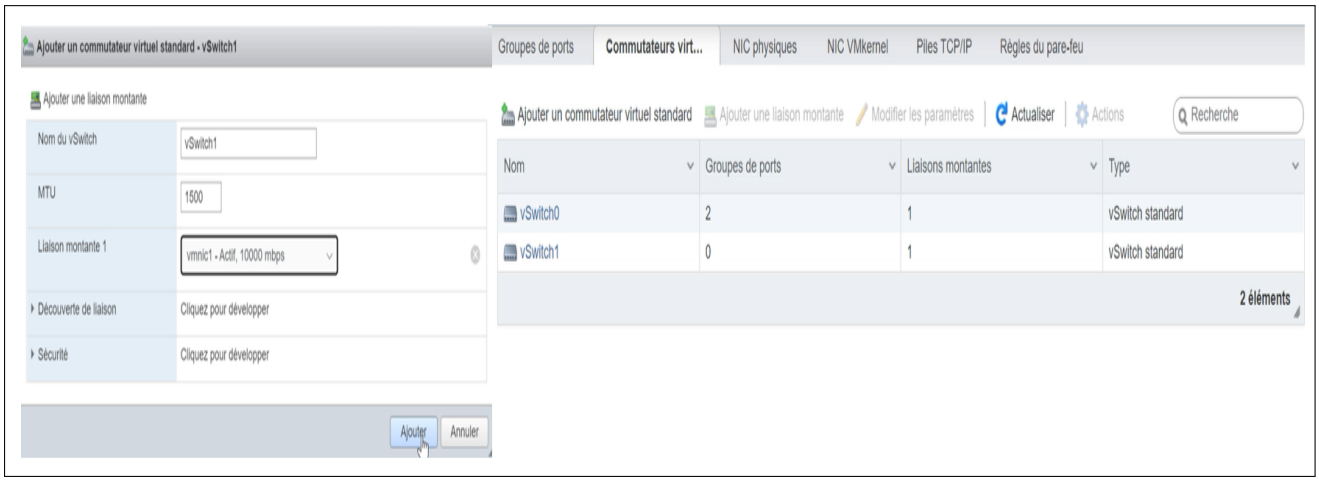

FIGURE V.52 – Création d'un vSwitch.

2. **Création d'un group de port :**
   Pour faciliter la gestion et la configuration des ports réseau au sein de l'hyperviseur ESXi, on va crée un groupe de port. On suit les étapes de la Figure V.53 :

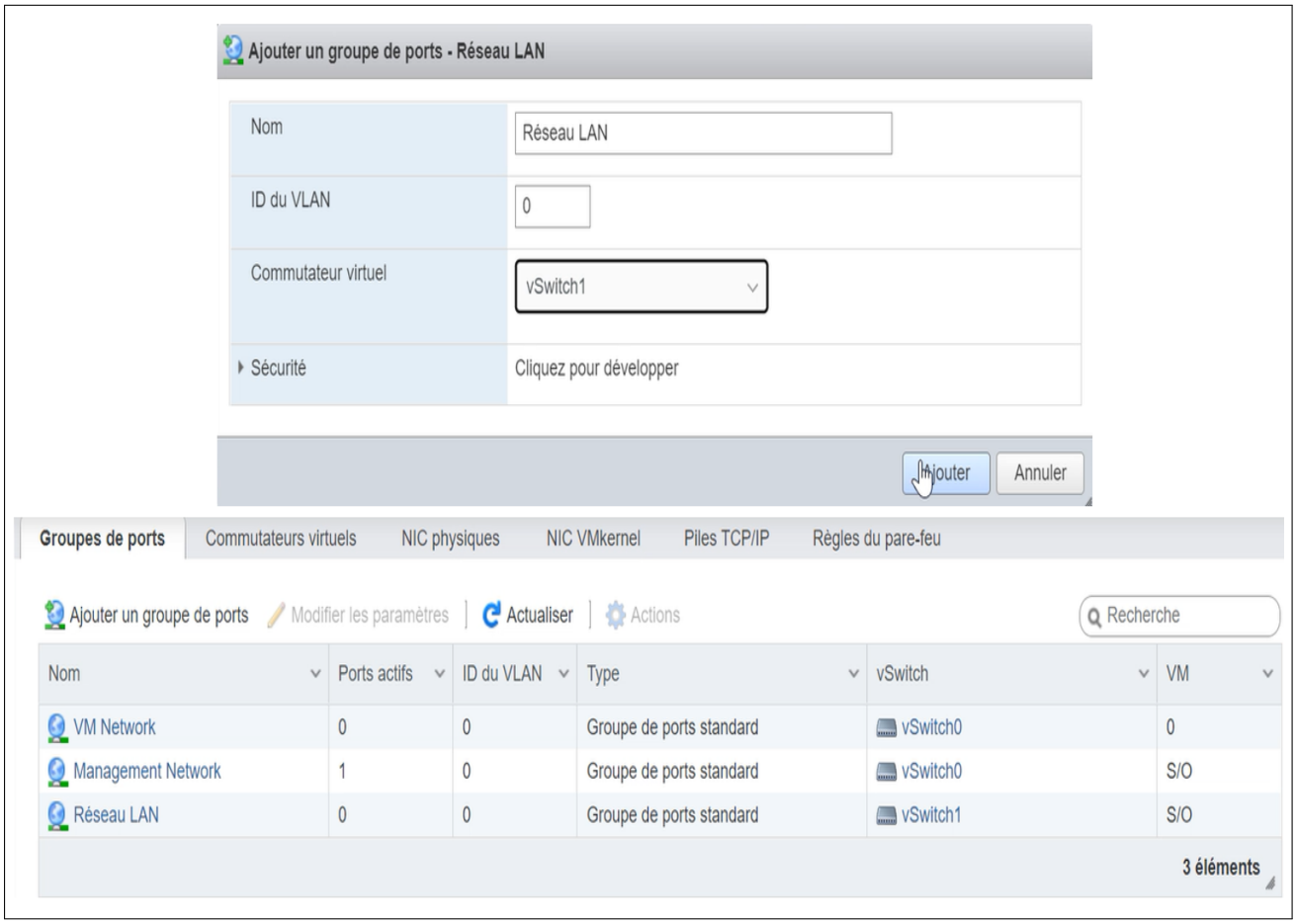

FIGURE V.53 – Création du Réseau LAN.

3. **Ajouter un disque :**
   Pour permettre d'étendre la capacité de stockage disponible pour la machine virtuelle, offrant ainsi davantage d'espace pour le stockage des données et des fichiers,cela consiste d'ajouter un disk comme la figure V.54 le montre.

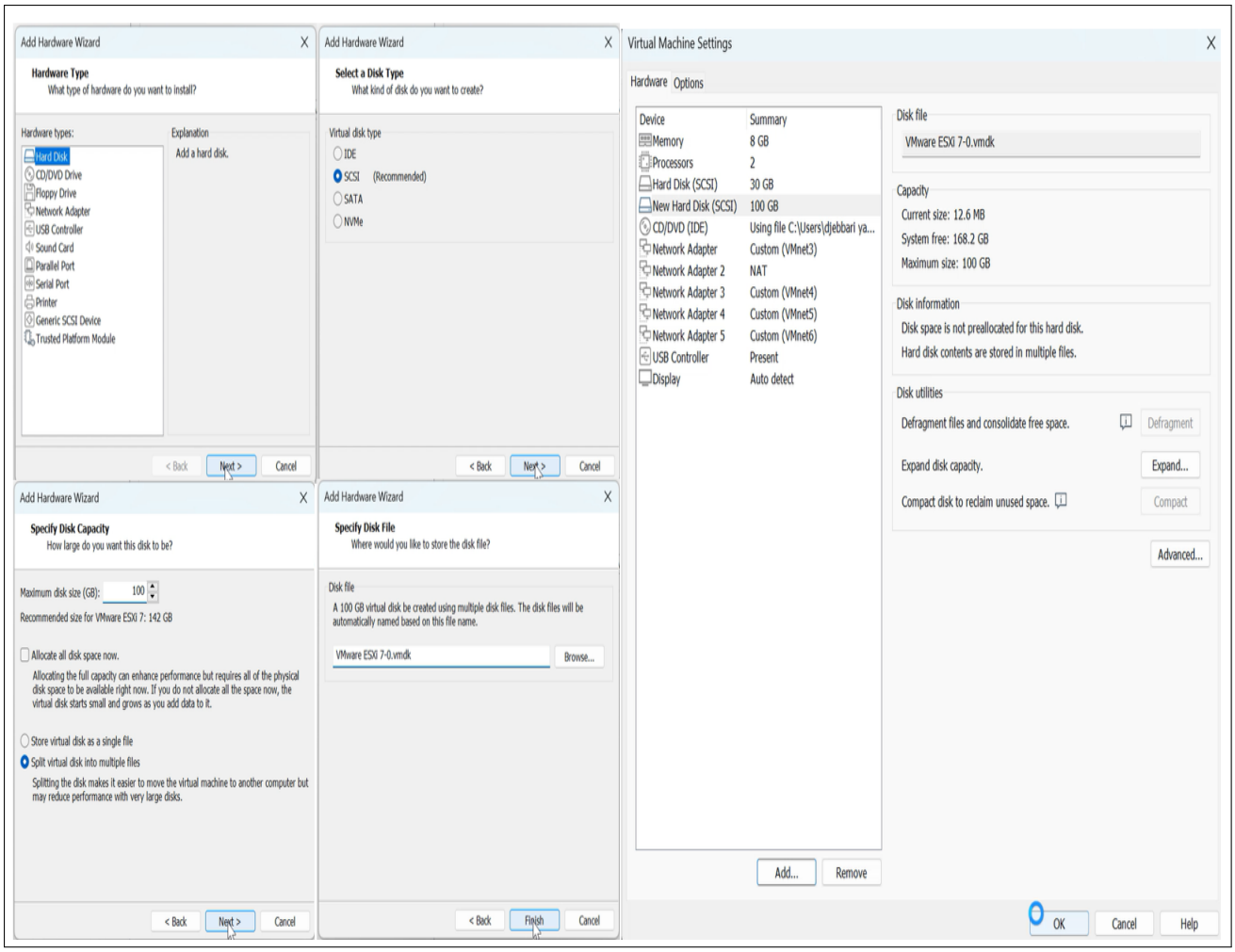

FIGURE V.54 – Ajouter un disque.

4. **Création d'une banque de donnée :**
   ESXi nécessite une banque de données [5] (Figure V.55)pour stocker et organiser les données du serveur, pour cela on doit la crée :

5. Une banque de données (ou datastore en anglais) est un espace de stockage logique utilisé pour héberger les fichiers de machines virtuelles, les modèles, les fichiers ISO et d'autres données associées à l'environnement ESXi.

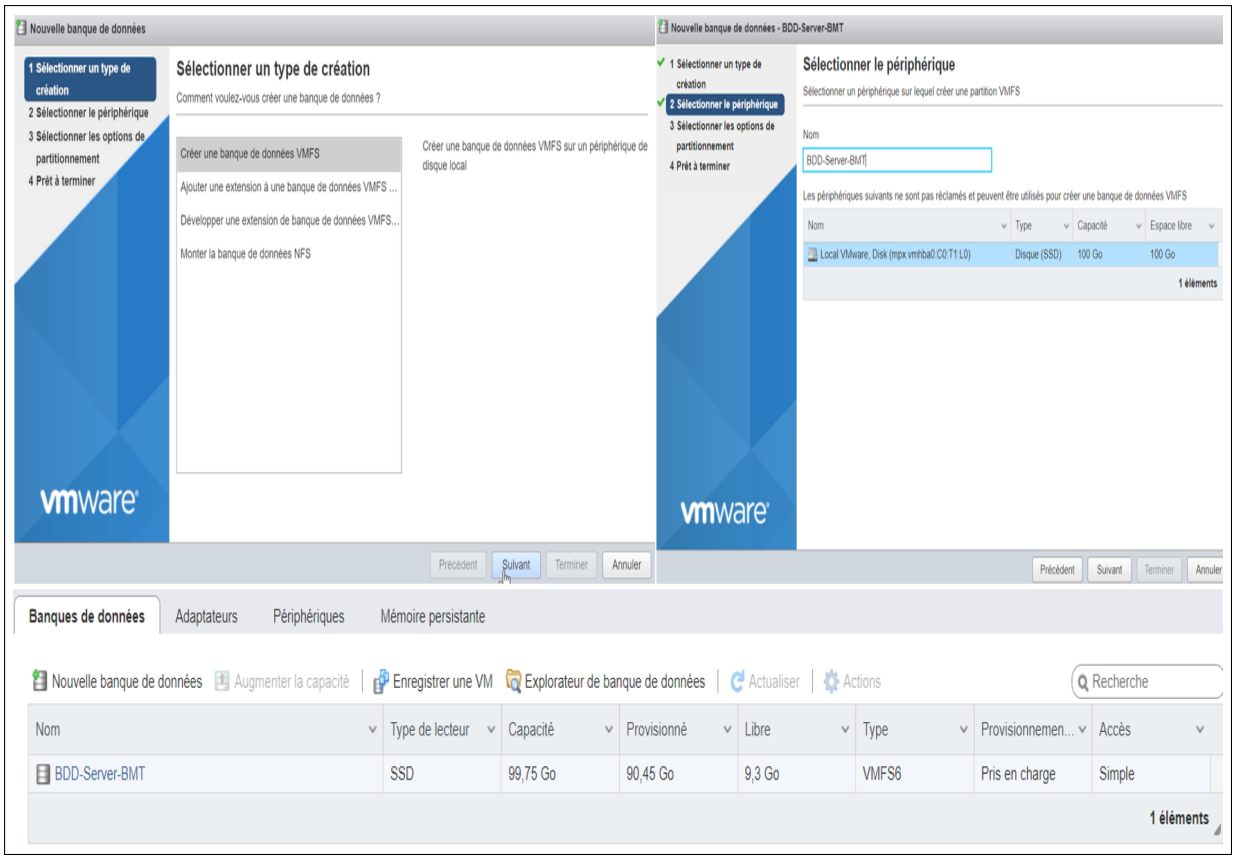

FIGURE V.55 – Création d'une banque de donnée "BDD-Serveur-BMT".

5. **Installation des deux serveurs sur ESXi7 :**
   Pour installer les serveurs sur ESXI on suit les etapes illustrées dans la Figure V.56 ci-dessous

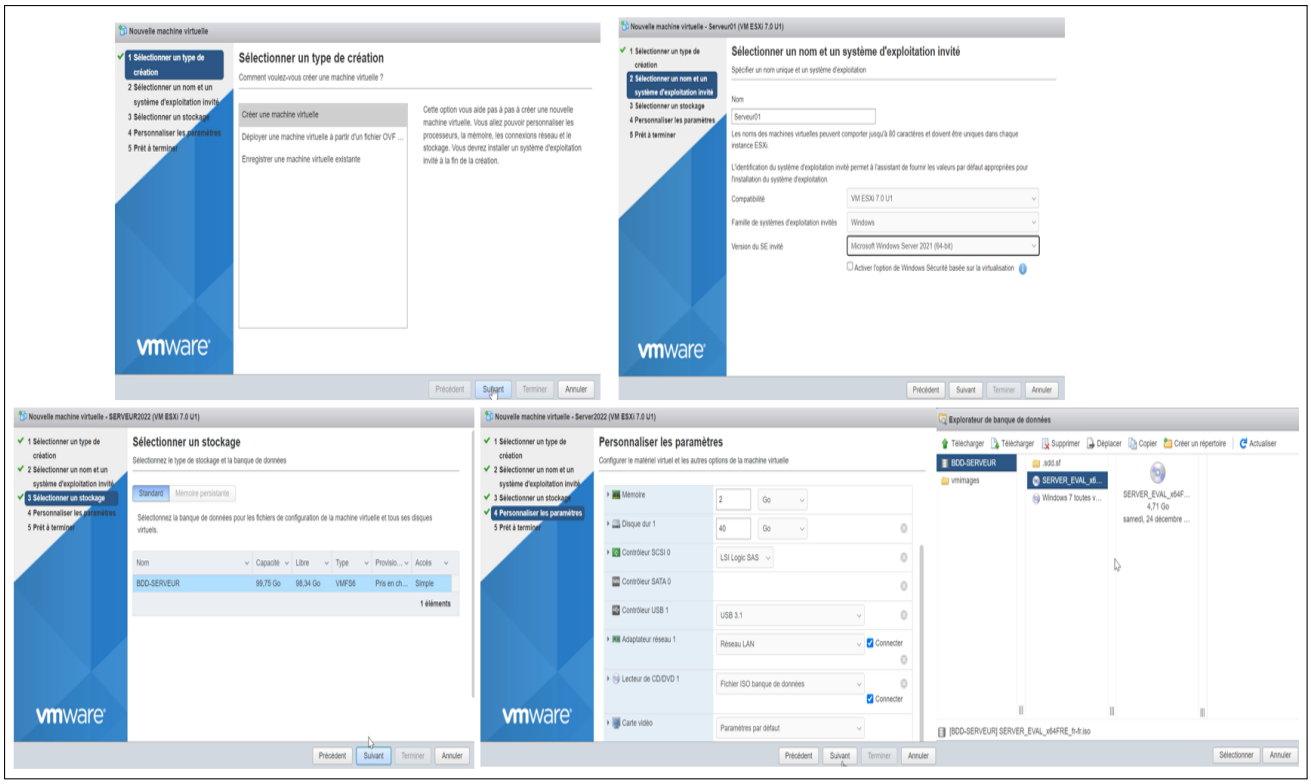

FIGURE V.56 – Les étape de l'installation de Serveur01 .

Une fois que l'installation des deux serveurs est termine, cette interface s'affichera (Figure V.57) :

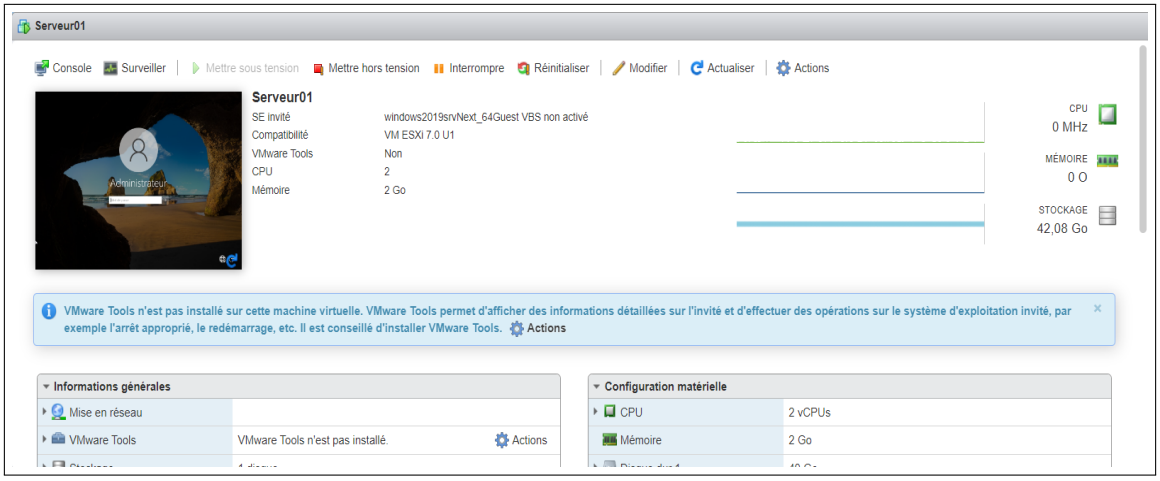

FIGURE V.57 – Interface de Serveur01 sur VMware ESXi 7 .

V.8 La supervision sur VMware ESXi 7 :

La supervision sur VMware ESXi 7 est un processus essentiel pour surveiller, gérer et diagnostiquer l'état et les performances de l'hôte ESXi, des machines virtuelles et des ressources associées.

Les Figure V.58-63 illustrent la surveillance qui se déroule dans VMware ESXi 7 des deux serveurs Serveur01 et Serveur02 pour la surveillance de Chacun des métriques CPU, la mémoire, le réseau et le disque.

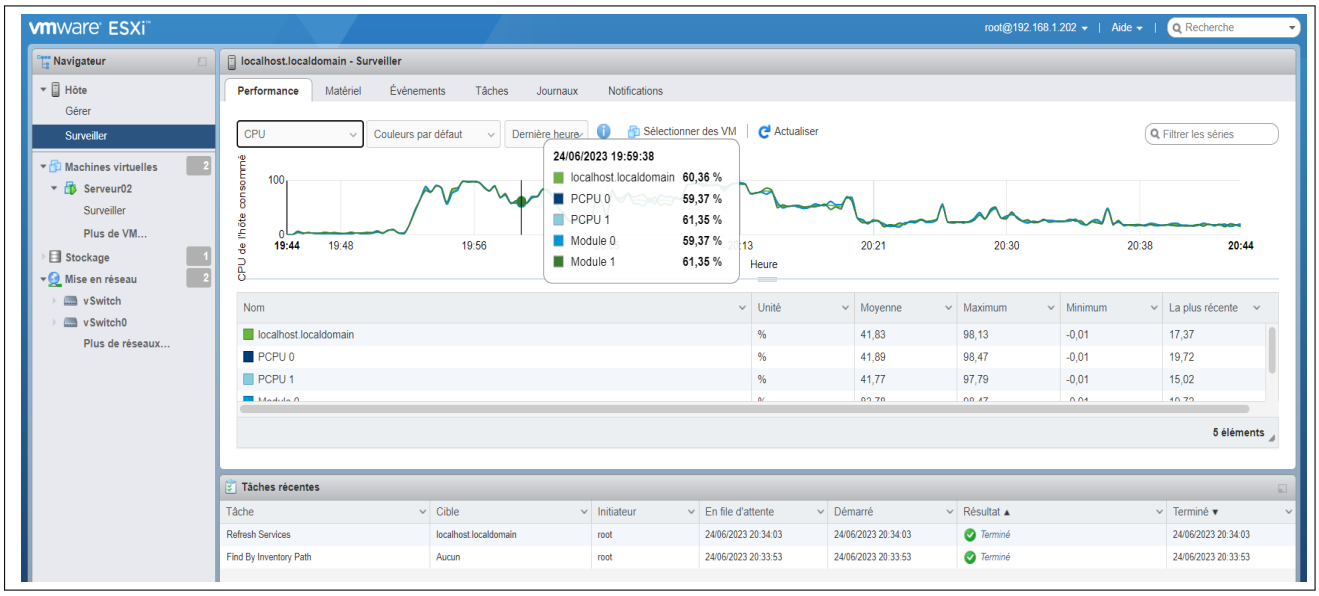

FIGURE V.58 – La surveillance des CPU.

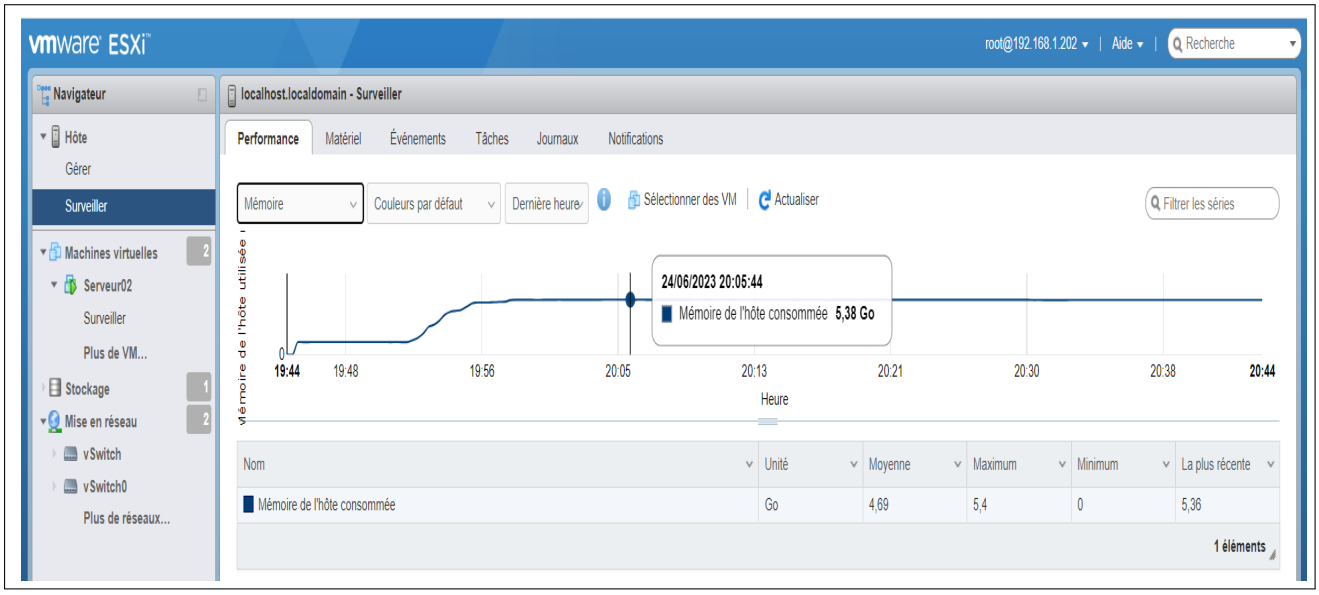

FIGURE V.59 – La surveillance des memoires.

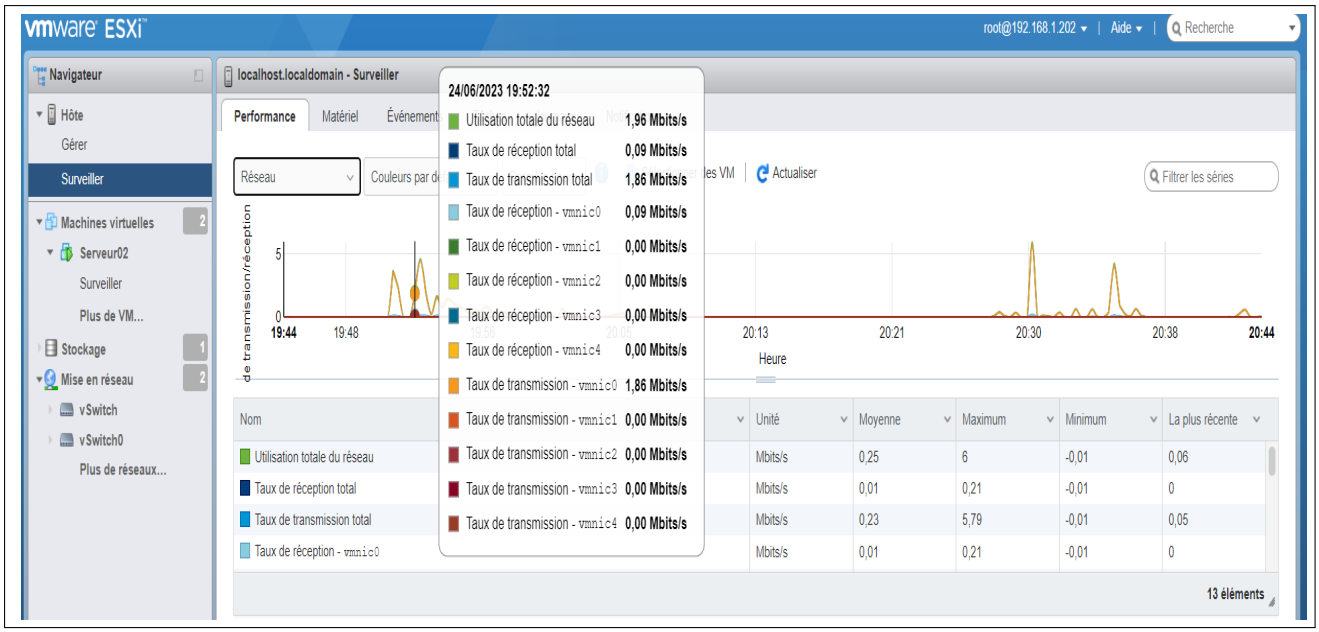

FIGURE V.60 – La surveillance des réseau.

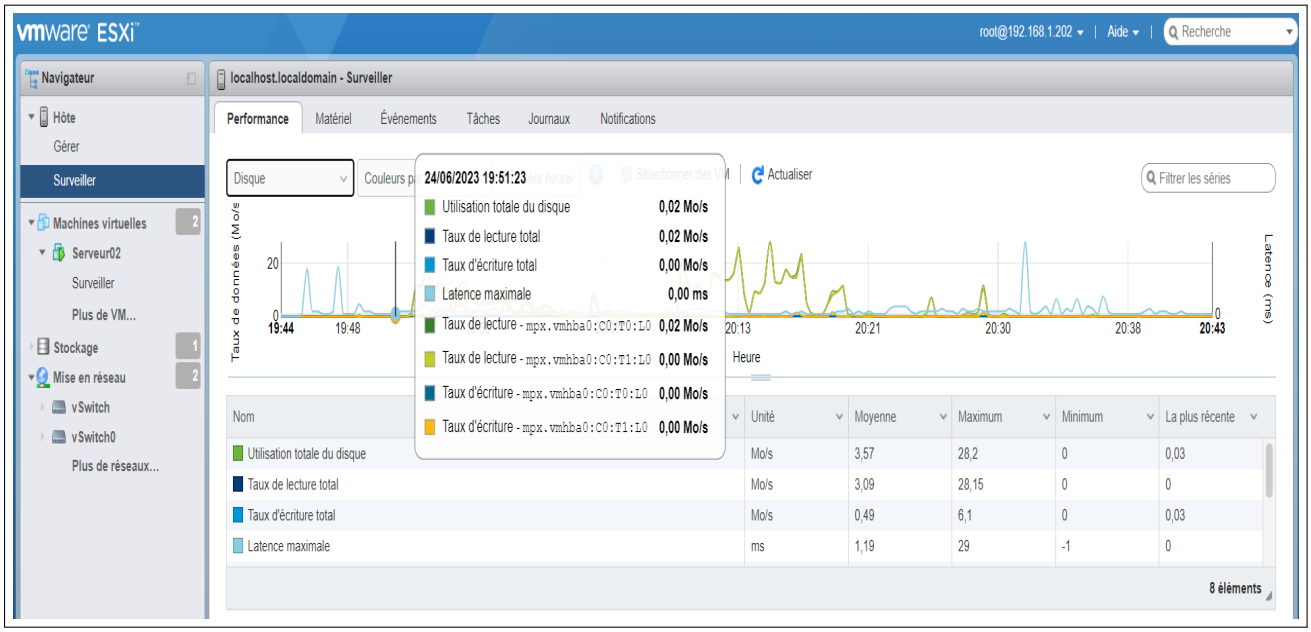

FIGURE V.61 – La surveillance des disques.

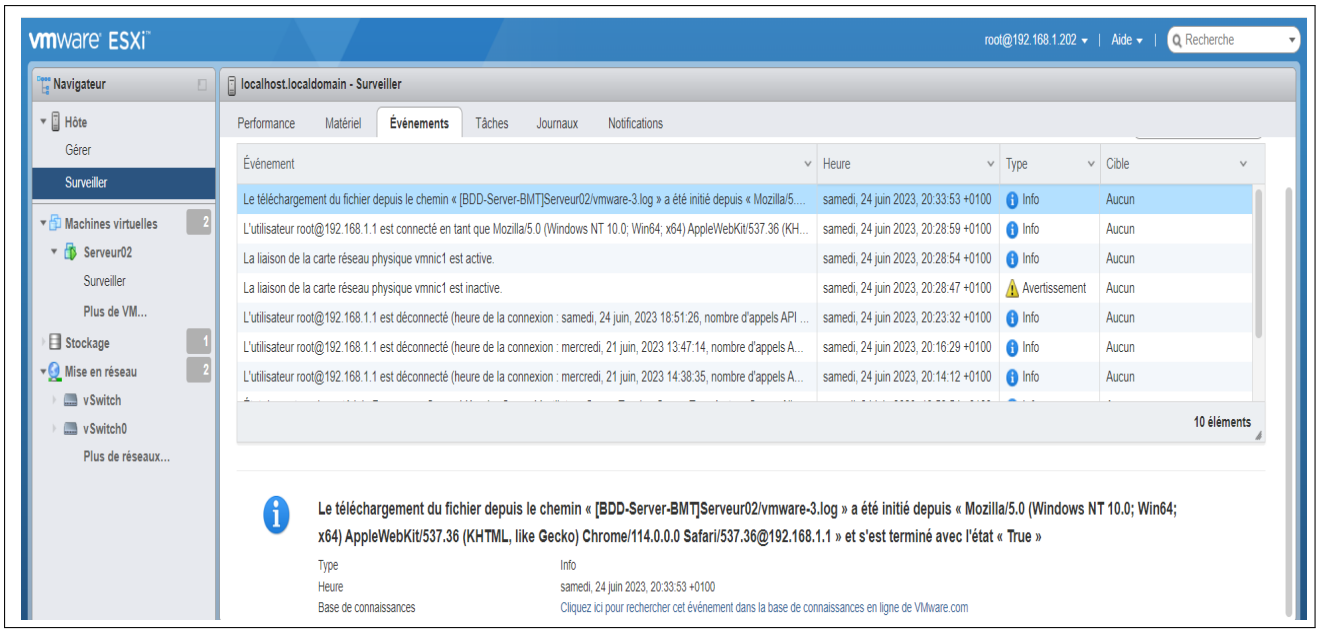

FIGURE V.62 – Les événements.

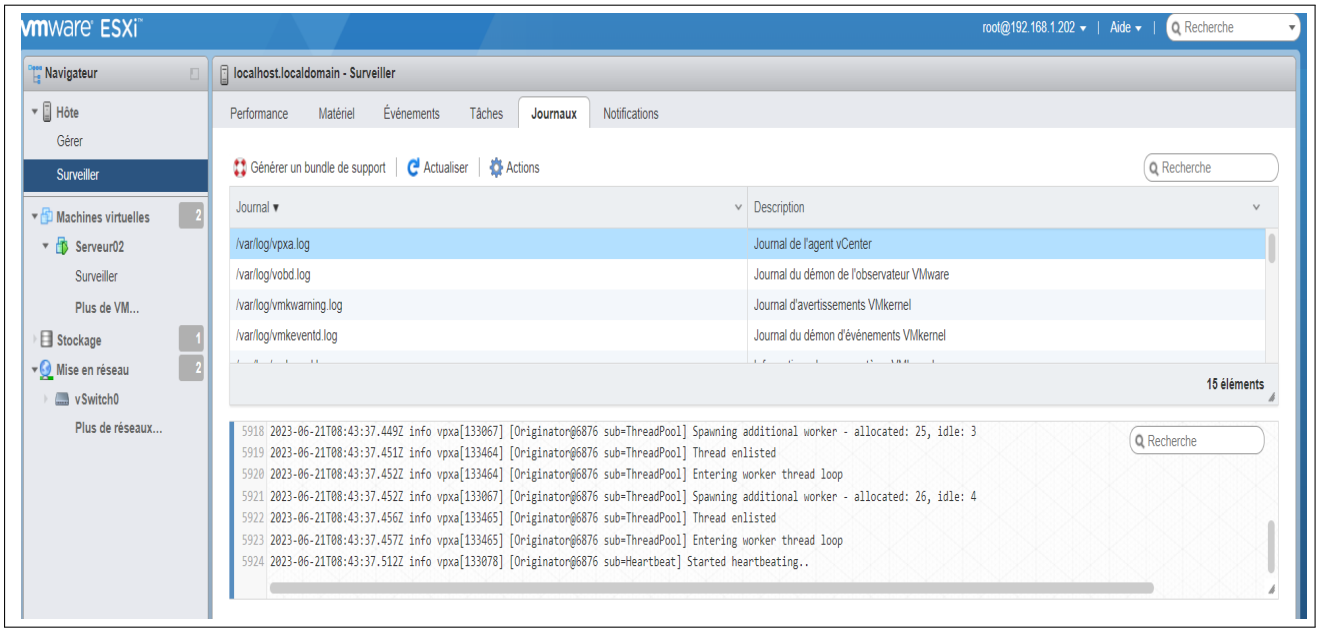

FIGURE V.63 – Les journaux.

En cas de mise hors tension ou de panne de l'un des serveurs, les alertes correspondantes sont immédiatement signalées sur VMware ESXi 7 comme le montre la Figure V.64. Ces alertes permettent aux administrateurs de réagir rapidement en prenant des mesures appropriées et en mettant en place des actions correctives pour garantir la continuité des opérations et minimiser les interruptions de service.

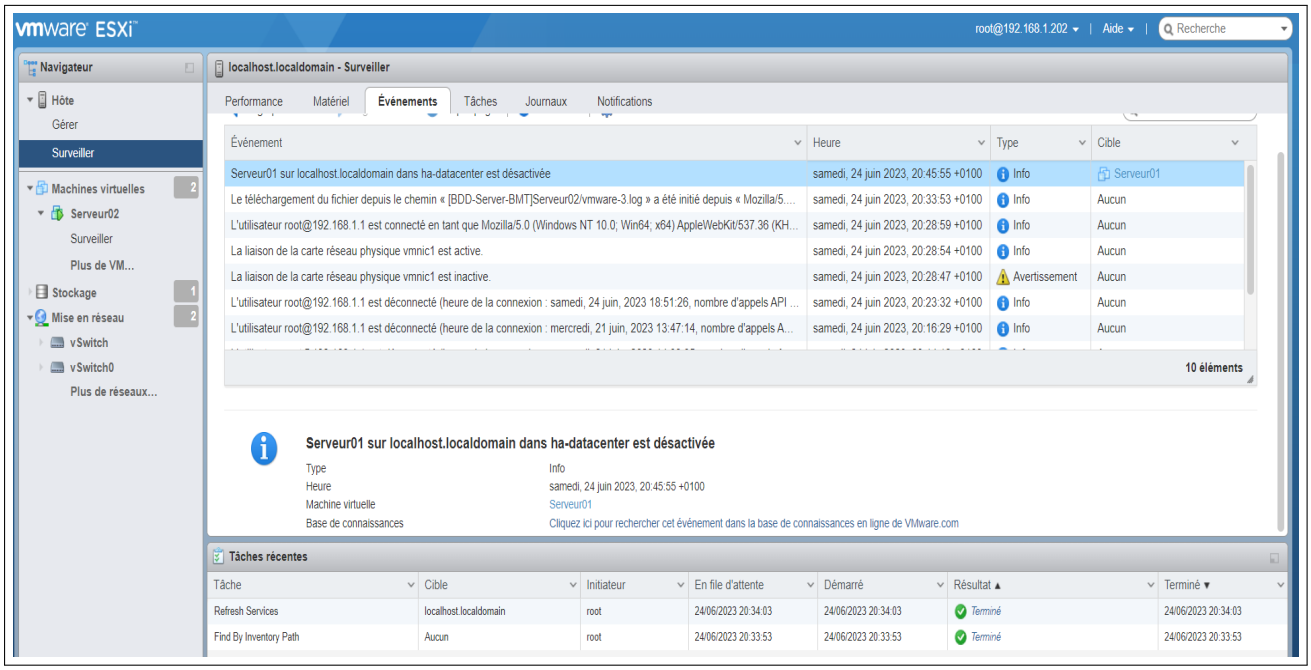

FIGURE V.64 – Le Serveur01 est éteint.

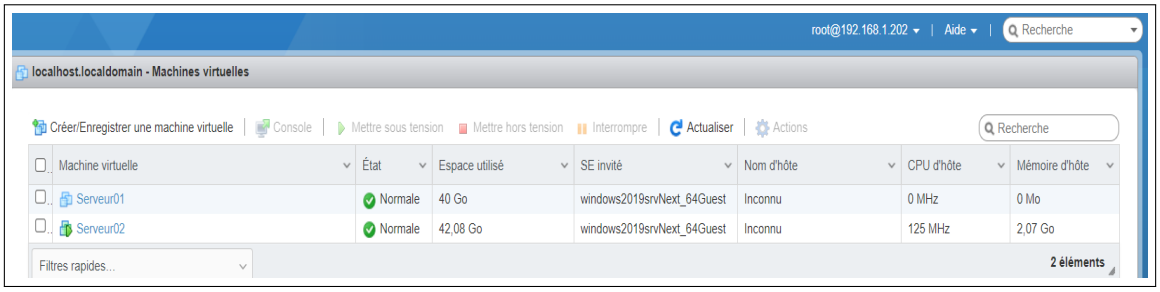

FIGURE V.65 – Le Serveur01 a été signalé hors tension.

V.9 Configuration des équipements :

Dans cette partie,nous allons présenter la configuration en générale des équipements qui vont nous permettre de mettre en place la nouvelle architecture proposée.

V.9.1 Plan d'adressage :

A) **Des VLANs :**

Nom de VLAN	ID VLAN	Adresse de sous réseau	passerelle de sous réseau
RH	vlan 2	192.168.2.0	192.168.11.200 192.168.11.201
Commerciale	vlan 3	192.168.3.0	192.168.11.200 192.168.11.201
Comptabilité	vlan 4	192.168.4.0	192.168.11.200 192.168.11.201
MGX	vlan 5	192.168.5.0	192.168.11.200 192.168.11.201
Informatique	vlan 6	192.168.6.0	192.168.11.200 192.168.11.201
Accolade	vlan 7	192.168.7.0	192.168.11.200 192.168.11.201
Marketing	vlan 8	192.168.8.0	192.168.11.200 192.168.11.201
Portique	vlan 9	192.168.9.0	192.168.11.200 192.168.11.201
Méthode	vlan 10	192.168.10.0	192.168.11.200 192.168.11.201
Management	vlan 11	192.168.11.0	192.168.11.200 192.168.11.201
Voice	vlan 12	\\	\\
Native	vlan 66	\\	\\

Table V.1 – Plan d'adressage des VLANs.

B) **L'encapsulation dot1Q sur les deux routeur :**

Nom de l'équipement	Interface	Passerelle virtuelle
R-ZEP1	ethernet 0/0.200 ethernet 0/0.201 Ethernet0/1	192.168.200.1 192.168.201.1 172.19.0.1
R-ZEP2	Ethernet0/0 ethernet 0/0.200 ethernet 0/1.201	172.19.0.5 192.168.200.2 192.168.201.2

Table V.2 – Plan d'adressage des équipements.

C) **L'adressage des équipements :**

Équipement	Adressage
FG-BMT1 FG-BMT2	192.168.1.1
FG-ZEP	10.0.1.5
Server1	192.168.11.200
Serveur2	192.168.11.201
EDGE-AT	172.168.10.1

TABLE V.3 – Plan d'adressage des équipements.

V.9.2 Configuration des commutateurs :

1. Configuration des interfaces trunk :

Le trunk est utilisé pour transporter des trames provenant de différents VLAN. Afin de configurer les interfaces trunk entre deux commutateurs, on suit les commandes suivantes (Figure V.66) sur les switchs « core1 », « Dist02 » et « Dist03 ».

```
core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
core1(config)#interface range ethernet 0/2-3
core1(config-if-range)#switchport trunk encapsulation dot1q
core1(config-if-range)#switchport mode trunk
core1(config-if-range)#switchport trunk native vlan 66
core1(config-if-range)#switchport trunk allowed vlan 2-12,66
core1(config-if-range)#end
core1# show interfaces trunk

Port         Mode             Encapsulation  Status        Native vlan
Et0/0        on               802.1q         trunking      1
Et0/1        on               802.1q         trunking      1
Et0/2        on               802.1q         trunking      66
Et0/3        on               802.1q         trunking      66

Port         Vlans allowed on trunk
Et0/0        1-4094
Et0/1        1-4094
Et0/2        2-12,66
Et0/3        2-12,66

Port         Vlans allowed and active in management domain
Et0/0        1-12,66
Et0/1        1-12,66
Et0/2        2-12,66
Et0/3        2-12,66

Port         Vlans in spanning tree forwarding state and not pruned
Et0/0        1-12,66
Et0/1        1-12,66
Et0/2        2-12,66
Et0/3        2-12,66
```

FIGURE V.66 – Configuration trunk sur le switch distribution « core1 » et vérification.

2. Configuration d'un domaine VTP :

Dans cette étape on va configurer le protocole VTP comme suit :

- Configurer les commutateurs de distribution « core1 », « Dist02 » et « Dist03 » en mode vtp srver pour propager les VLANs créés et leurs paramètres aux autres commutateurs clients (Figure V.67).

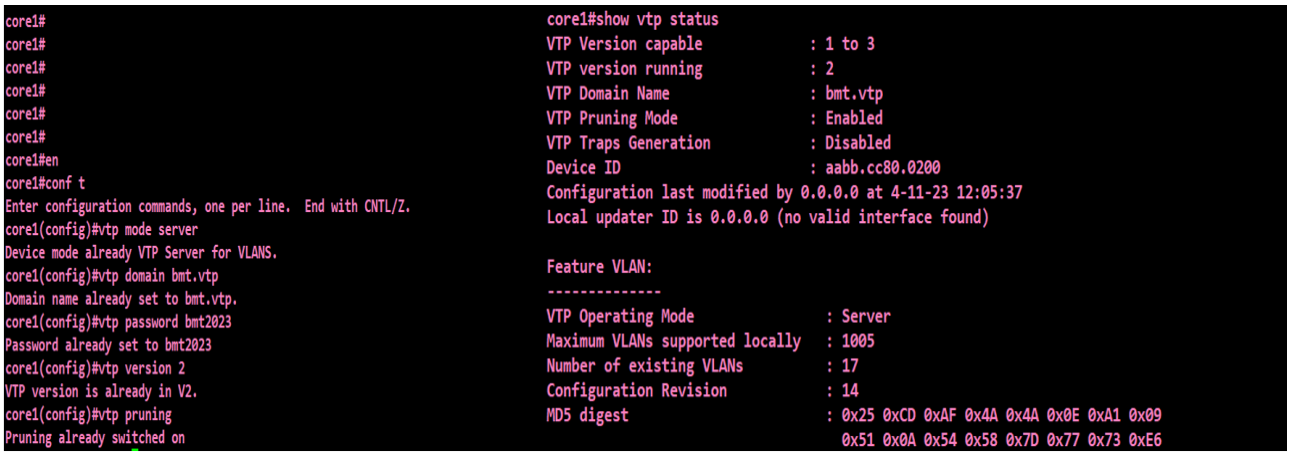

FIGURE V.67 – Configuration VTP serveur sur le switch distribution « core1 » et vérification.

- Configurer les Switchs d'accès « SW1 »,« SW2 » et « SW3 » en mode vtp client pour recevoir les informations des VLANs qui leurs sont propagés (Figure V.68).

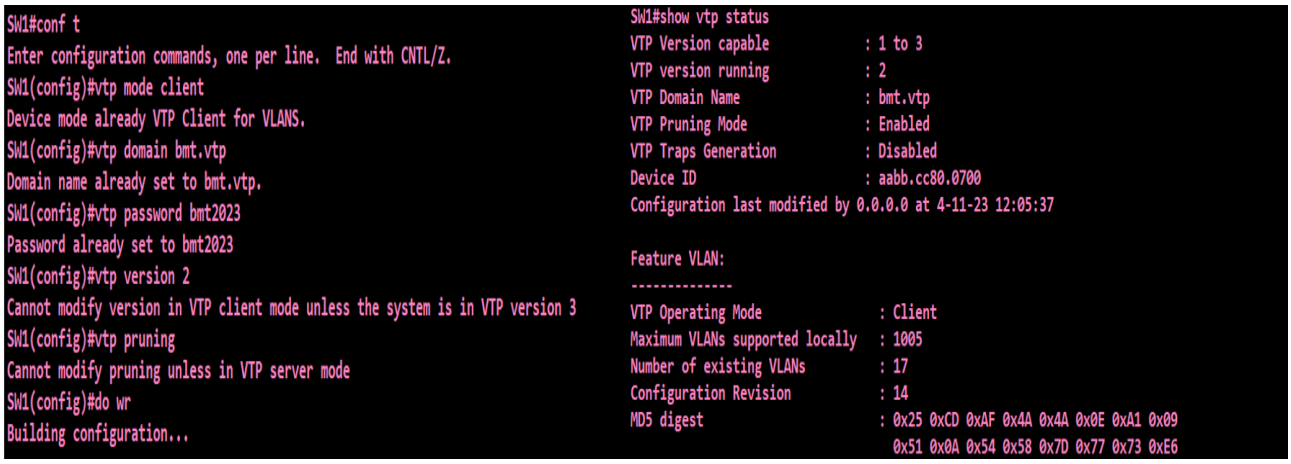

FIGURE V.68 – Configuration VTP Client sur le switch distribution « SW1 » et vérification.

- Configurer les Switchs d'accès « DMZ01 » et « DMZ02 » en mode vtp transparent pour désactiver la diffusion des informations de configuration VTP aux autres commutateurs du réseau. (Figure V.69).

```
DMZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DMZ(config)#vtp mode transparent
Device mode already VTP Transparent for VLANS.
DMZ(config)#do wr
Building configuration...
Compressed configuration from 1862 bytes to 1057 bytes[OK]
DMZ(config)#end
DMZ#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
--------------
VTP Operating Mode                : Transparent
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 8
Configuration Revision            : 0
MD5 digest                        : 0x2C 0x4B 0x04 0x0A 0x98 0x9D 0x8F 0xBB
                                    0x85 0x3A 0x5E 0x20 0x75 0x74 0x7B 0x4C
```

FIGURE V.69 – Configuration VTP transparent sur le switch distribution « DMZ01 » et vérification.

3.Création des VLANs :

On a crée nos VLANs dans le switch «core» comme la Figure V.70 le montre :

```
Enter configuration commands, one per line.  End with CNTL/Z.
core1(config)#vln
core1(config)#vl
core1(config)#vlan 2
core1(config-vlan)#name RH
core1(config-vlan)#vlan 3
core1(config-vlan)#name CTB
core1(config-vlan)#name CO
core1(config-vlan)#
core1(config-vlan)#vlan 4
core1(config-vlan)#name CTB
core1(config-vlan)#vlan 5
core1(config-vlan)#name MGX
core1(config-vlan)#vlan 6
core1(config-vlan)#name INF
core1(config-vlan)#vlan 7
core1(config-vlan)#name ACC
core1(config-vlan)#vlan 8
core1(config-vlan)#name MKT
core1(config-vlan)#vlan 9
core1(config-vlan)#name POT
core1(config-vlan)#vlan 10
core1(config-vlan)#name MDT
core1(config-vlan)#vlan 11
core1(config-vlan)#name G-S
core1(config-vlan)#vlan 12
core1(config-vlan)#name voice
core1(config-vlan)#
core1(config-vlan)#vlan 66
core1(config-vlan)#name native
```

```
core1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
2    RH                               active
3    CO                               active
4    CTB                              active
5    MGX                              active
6    INF                              active
7    ACC                              active
8    MKT                              active
9    POT                              active
10   MDT                              active
11   G-S                              active
12   voice                            active
66   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
core1#
```

FIGURE V.70 – Création des VLANs dans le switch «core» .

4.Affectation des ports aux VLANs dans les switchs SW1,SW2 et SW3 :

Grâce aux VTP crée dans le switch «core», nos VLANs sont automatiquement crée dans les trois switchs et on a directement affecter les ports aux vlan illustré dans les Figure V.71-73.

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface ethernet 0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#switchport voice vlan 12
SW1(config-if)#exit
SW1(config)#interface ethernet 0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 3
SW1(config-if)#switchport voice vlan 12
SW1(config-if)#exit
SW1(config)#interface ethernet 3/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 4
SW1(config-if)#switchport voice vlan 12
SW1(config-if)#exit
SW1(config)#end
SW1#
*Jun  9 14:02:58.677: %SYS-5-CONFIG_I: Configured from console by console
SW1#wr
Building configuration...
Compressed configuration from 1853 bytes to 1048 bytes[OK]
```

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2
2    RH                               active    Et0/2
3    CO                               active    Et0/3
4    CTB                              active    Et3/3
5    MGX                              active
6    INF                              active
7    ACC                              active
8    MKT                              active
9    POT                              active
10   MDT                              active
11   G-S                              active
12   voice                            active    Et0/2, Et0/3, Et3/3
66   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SW1#
```

FIGURE V.71 – Affectation des ports aux VLANs dans le switch SW1.

```
SW2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW2(config)#interface ethernet 0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 5
SW2(config-if)#switchport voice vlan 12
SW2(config-if)#exit
SW2(config)#interface ethernet 0/3
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 6
SW2(config-if)#switchport voice vlan 12
SW2(config-if)#exit
SW2(config)#interface ethernet 3/3
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 7
SW2(config-if)#switchport voice vlan 12
SW2(config-if)#exit
SW2(config)#end
SW2#w
*Jun 19 17:01:02.599: %SYS-5-CONFIG_I: Configured from console by console
SW2#wr
Building configuration...
Compressed configuration from 1854 bytes to 1051 bytes[OK]
```

```
SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2
2    RH                               active
3    CO                               active
4    CTB                              active
5    MGX                              active    Et0/2
6    INF                              active    Et0/3
7    ACC                              active    Et3/3
8    MKT                              active
9    POT                              active
10   MDT                              active
11   G-S                              active
12   voice                            active    Et0/2, Et0/3, Et3/3
66   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SW2#
```

FIGURE V.72 – Affectation des ports aux VLANs dans le switch SW2.

```
SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#interface ethernet 0/3
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 8
SW3(config-if)#switchport voice vlan 12
SW3(config-if)#exit
SW3(config)#interface ethernet 1/0
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 9
SW3(config-if)#switchport voice vlan 12
SW3(config-if)#exit
SW3(config)#interface ethernet 3/3
SW3(config-if)#switchport mode access
SW3(config-if)#switchport access vlan 10
SW3(config-if)#switchport voice vlan 12
SW3(config-if)#exitt
                  ^
```

```
SW3#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2
2    RH                               active
3    CO                               active
4    CTB                              active
5    MGX                              active
6    INF                              active
7    ACC                              active
8    MKT                              active    Et0/3
9    POT                              active    Et1/0
10   MDT                              active    Et3/3
11   G-S                              active
12   voice                            active    Et0/3, Et1/0, Et3/3
66   native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SW3#
```

FIGURE V.73 – Affectation des ports aux VLANs dans le switch SW3.

5. Test des VLANs :

Nous avons effectué un test sur un PC faisant partie du VLAN2 avec l'adresse IP 192.168.2.1. Ensuite, nous avons accédé au PC dans VMware et avons activé la configuration d'obtention automatique d'adresse IP. Comme résultat, le PC était ajouté au réseau bmt.local. En vérifiant l'adresse IP du PC, nous avons confirmé qu'elle appartenait bien à la même plage d'adresses que le VLAN. Comme le montre la Figure V.74.

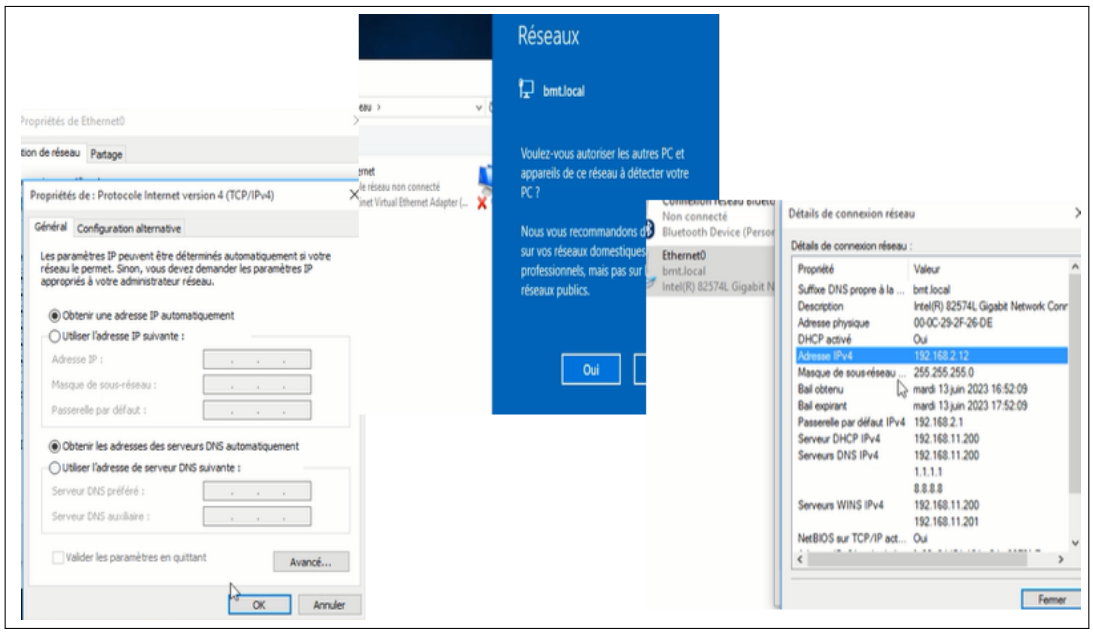

FIGURE V.74 – Test effectué sur les VLANs.

V.9.2.1 Création des VLANs sur SW-ZEP et SW-ZEP1 :

Sur les deux switches SW-ZEP1 et SW-ZEP2, nous avons réalisé la configuration de deux VLANs distincts : "vlan manager" et "vlan prod" (Figure V.75). Cette configuration permet de séparer le trafic réseau en fonction des besoins spécifiques de chaque VLAN, facilitant ainsi la gestion et l'organisation du réseau.

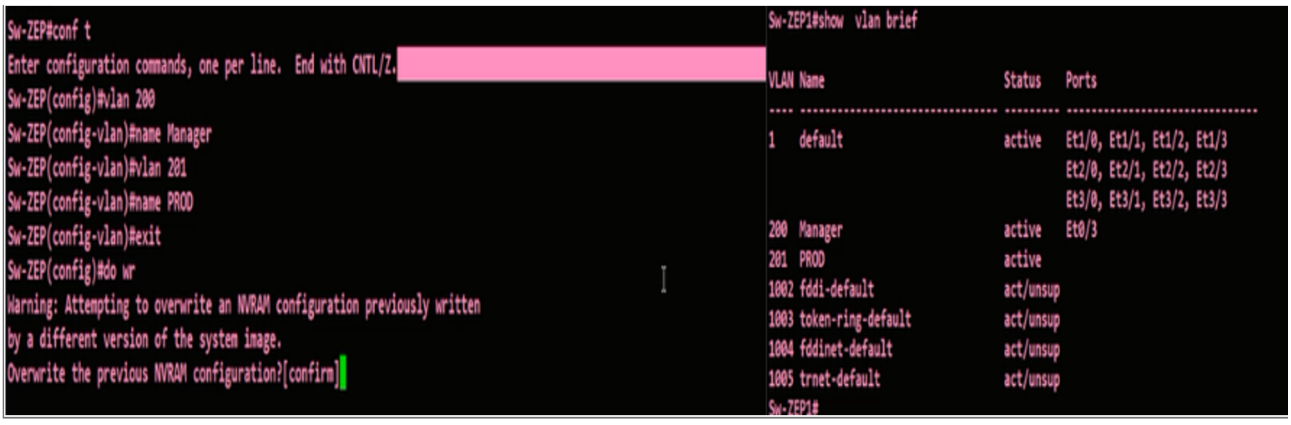

FIGURE V.75 – Création des VLANs manager et PROD.

On a configuré le trunk, sur les deux switchs, ensuite on a activé le protocole (Figure V.76). Cette configuration permet une agrégation de liens entre les switches, favorisant une meilleure utilisation de la bande passante et une répartition équilibrée du trafic entre les ports physiques.

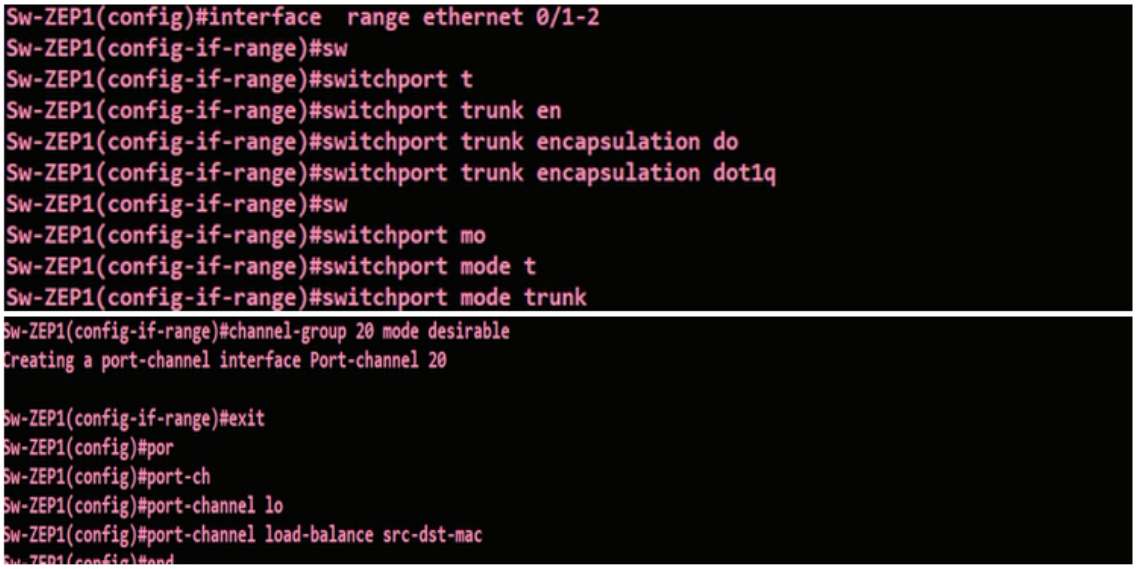

Figure V.76 – Configuration du Trunk et activation du protocole Pagp-LB.

V.9.2.2 Configuration de GLBP-LB :

On a configuré le protocole GLBP entre le routeur ZEP1 et le routeur ZEP2 afin de permettre une répartition équilibrée du trafic entre ces deux équipements.

Les deux routeurs sont équipés de deux interfaces chacun, et la configuration du protocole GLBP sera appliquée aux deux interfaces de chaque routeur pour assurer une répartition équilibrée du trafic. (Figure V.77).

- R-ZEP1 : ethernet 0/0.200 ethernet 0/1.200.
- R-ZEP2 : ethernet 0/0.201 ethernet 0/1.201.

```
R-ZEP1(config)#interface ethernet 0/0.201
R-ZEP1(config-subif)#glbp 201 ip 192.168.201.254
R-ZEP1(config-subif)#glbp 201 load-balancing round-robin
R-ZEP1(config-subif)#glbp 201 preempt
R-ZEP1(config-subif)#glbp 201 load-balancing round-robin
*Apr 17 08:58:32.144: %GLBP-6-STATECHANGE: Ethernet0/0.201 Grp 201 state Speak -> Active
R-ZEP1(config-subif)#glbp 201 priority 200
R-ZEP1(config-subif)#end
*Apr 17 08:58:43.220: %GLBP-6-FWDSTATECHANGE: Ethernet0/0.201 Grp 201 Fwd 1 state Listen -> Active
R-ZEP1(config-subif)#end
```

```
R-ZEP2(config)#interface ethernet 0/1.201
R-ZEP2(config-subif)#glbp 201 ip 192.168.201.254
R-ZEP2(config-subif)#glbp 201 priority 150
R-ZEP2(config-subif)#glbp 201 preempt
R-ZEP2(config-subif)#glbp 201 load-balancing round-robin
*Apr 17 09:00:20.295: %GLBP-6-FWDSTATECHANGE: Ethernet0/1.201 Grp 201 Fwd 2 state Listen -> Active
R-ZEP2(config-subif)#glbp 201 load-balancing round-robin
R-ZEP2(config-subif)#end
```

Figure V.77 – Configuration du protocole glbp-LB.

Après avoir configuré GLBP, on va exécuter de la commande "show glbp brief" (Figure V.78). En analysant les résultats, on peut observer l'état de chaque interface associée au groupe GLBP. L'état "Active" indique que l'interface est actuellement utilisée pour la répartition du trafic, ce qui signifie qu'elle reçoit et traite les requêtes des clients.

L'état "Standby" indique que l'interface est en attente et prête à prendre en charge le trafic en cas de défaillance de l'interface active. Cela garantit une redondance et une haute disponibilité du réseau.

De plus, la commande "show glbp brief" affiche également l'adresse IP virtuelle partagée par les membres du groupe GLBP. Cette adresse est utilisée comme passerelle par défaut pour les clients, leur permettant d'accéder au réseau.

```
R-ZEP1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Et0/0.200   200  -   200 Active   192.168.200.254 local           192.168.200.2
Et0/0.200   200  1   -   Active   0007.b400.c801  local           -
Et0/0.200   200  2   -   Listen   0007.b400.c802  192.168.200.2   -
Et0/0.201   201  -   200 Active   192.168.201.254 local           192.168.201.2
Et0/0.201   201  1   -   Active   0007.b400.c901  local           -
Et0/0.201   201  2   -   Listen   0007.b400.c902  192.168.201.2   -
```

Figure V.78 – Le résultat de l'exécution de la commande "show glbp brief ".

Pour vérifier le bon fonctionnement du protocole GLBP, on a attribué aux PC11 et PC12 des adresses IP ainsi que la passerelle virtuelle créée lors de la configuration du protocole GLBP (Figure V.79), cela permettra aux clients d'utiliser la passerelle virtuelle pour accéder au réseau et d'établir une communication avec d'autres ressources.

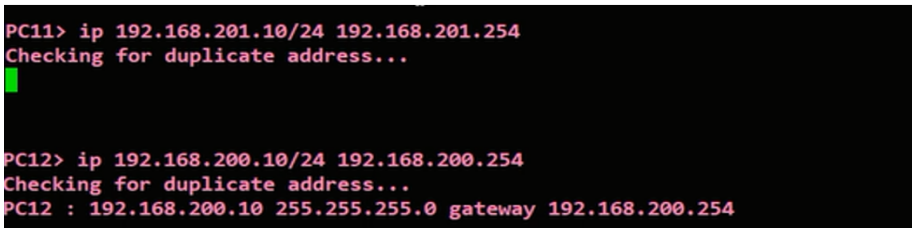

FIGURE V.79 – Configuration des adresses IP et la passerelle virtuelle des PC11 et PC12.

Ensuite on va tester le ping entre PC11 et PC12 comme la Figure V.80 le montre :

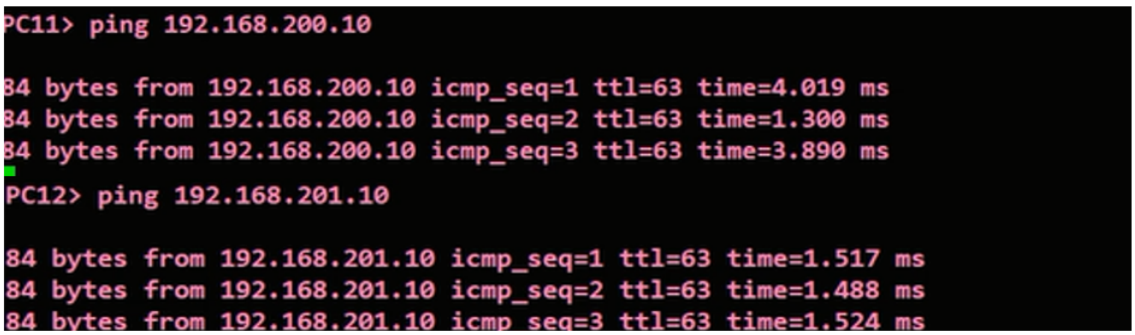

FIGURE V.80 – Ping entre PC11 et PC12.

V.9.2.3 Configuration de LACP-LB :

Nous avons configuré le protocole LACP (Figure V.81) avec équilibrage de charge entre les commutateurs "dist1" et "dist2" .

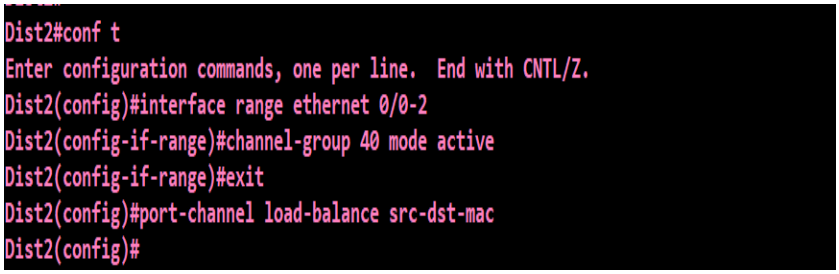

FIGURE V.81 – Configuration du protocole LACP-LB.

Et pour le load balancing on a utilisé l'algorithme round roubin pour équilibrer la charge entre les liens agrégés (Figure V.82).

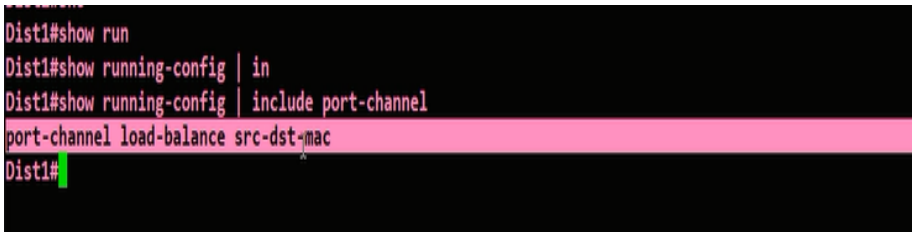

FIGURE V.82 – Affichage du port channel configuré.

1.Test du protocole LACP-LB :

Afin de tester le protocole LACP, nous allons désactiver l'une des interfaces physiques dans la laison agrégée connectées entre les deux commutateurs (Figure V.83). Dans notre exemple, nous avons éteint l'interface Ethernet 0/3. Et nous constatons que le port channel associé reste actif et fonctionne. Cette observation démontre l'efficacité du LACP dans la gestion des défaillances de liens.

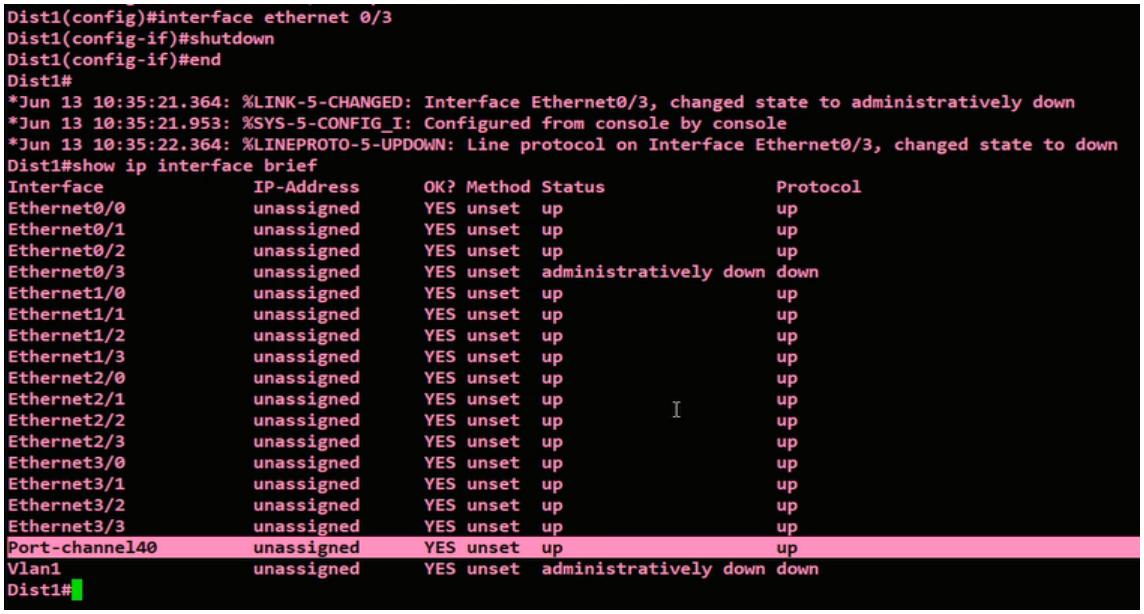

FIGURE V.83 – Test du protocole LACP-LB.

V.9.2.4 Configuration de la DMZ :

1. Création des private VLANs :

Notre DMZ est composée de trois switches. Les serveurs S01 et S02 sont configurés dans le VLAN "community", tandis que le switch S03 est dans le VLAN "isolated". Cette configuration permet une communication bidirectionnelle entre S01 et S02, mais ils ne peuvent pas communiquer avec S03 comme la Figure V.84 le montre. De plus, S03 est isolé et ne peut pas établir de communication avec S01 et S02. Cette segmentation garantit une séparation claire entre les réseaux pour des raisons de sécurité et de contrôle d'accès.

```
DMZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
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
DMZ(config)#vl
DMZ(config)#vlan 100
DMZ(config-vlan)#pr
DMZ(config-vlan)#private-vlan p
DMZ(config-vlan)#private-vlan primary
DMZ(config-vlan)#pr
DMZ(config-vlan)#private-vlan as
DMZ(config-vlan)#private-vlan association 101,102
DMZ(config-vlan)#exit
DMZ(config)#
```

FIGURE V.84 – Création des private VLANs.

2.Affectation des ports aux PVLANs :

Aprés la creation des VLANs on va le effectuer les ports aux PVLANs crées (Figure V.85).

```
MZ(config-if-range)#switchport private-vlan h
MZ(config-if-range)#switchport private-vlan host-association 100 101
MZ(config-if-range)#exit
MZ(config)#
*Apr 11 14:40:12.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
*Apr 11 14:40:12.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
MZ(config)#interface ethernet 0/2
MZ(config-if)#sw
MZ(config-if)#switchport mo
MZ(config-if)#switchport mode pri
MZ(config-if)#switchport mode private-vlan h
MZ(config-if)#switchport mode private-vlan host
MZ(config-if)#sw
MZ(config-if)#switchport pr
*Apr 11 14:40:41.177: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
MZ(config-if)#switchport pri
MZ(config-if)#switchport private-vlan h
MZ(config-if)#switchport private-vlan host-association 100 102
DMZ(config)#interface ethernet 0/3
DMZ(config-if)#s
DMZ(config-if)#sw
DMZ(config-if)#switchport mo
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)#sw
DMZ(config-if)#switchport
*Apr 11 14:41:19.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
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
DMZ#
```

FIGURE V.85 – Affectation des ports aux PVLANs .

3. Configuration de l'interface port5 du FG-BMT1 :

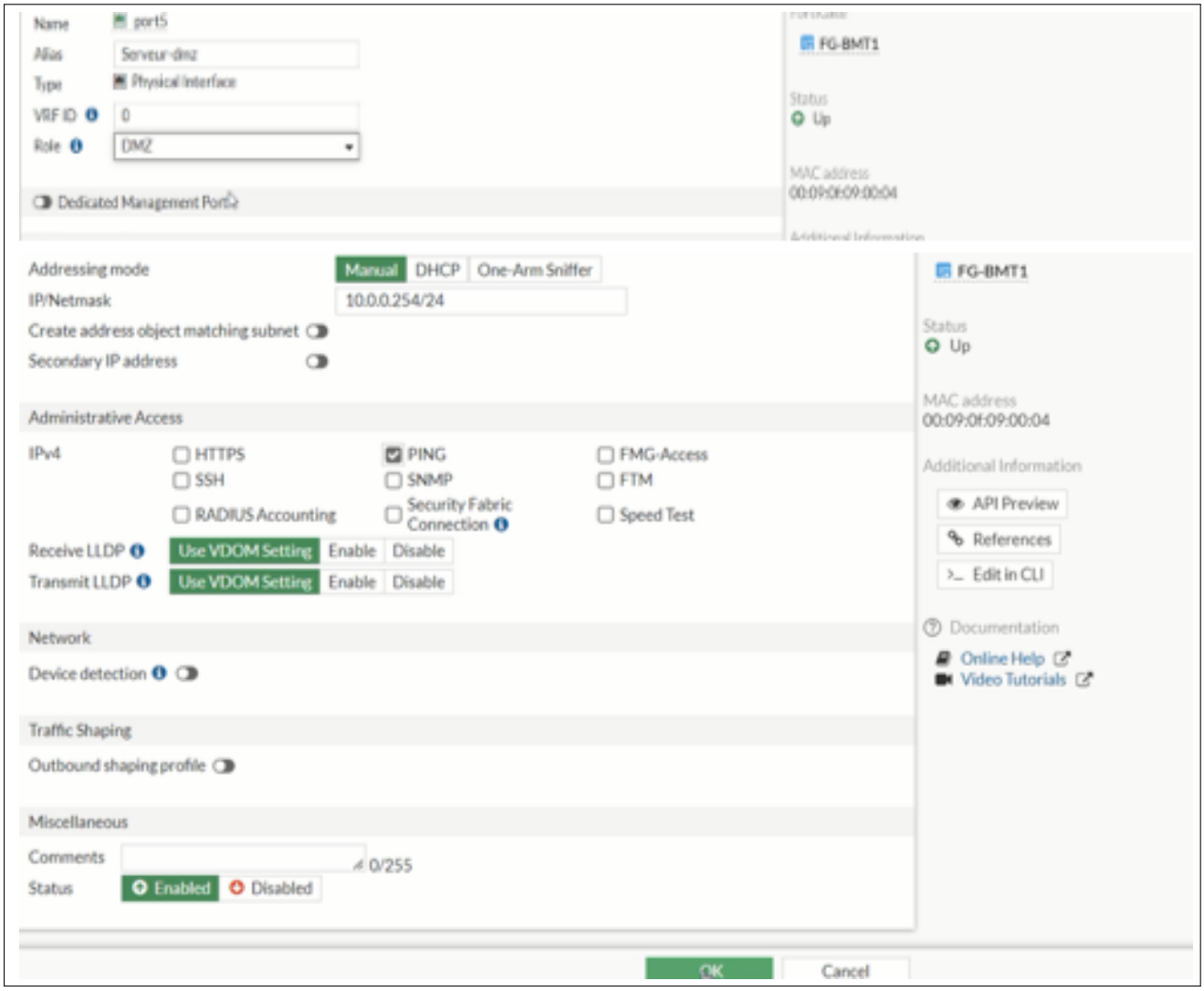

FIGURE V.86 – Configuration de l'interface port5 du FG-BMT1.

4.Test sur les PVLANs :

Afin de vérifier le bon fonctionnement de la zone démilitarisée (DMZ), nous allons procéder à des tests de connectivité en utilisant des pings (Figure V.87)entre les serveurs. La communication sera autorisée entre S01 et S02, tandis qu'ils ne pourront pas établir de communication avec S03.

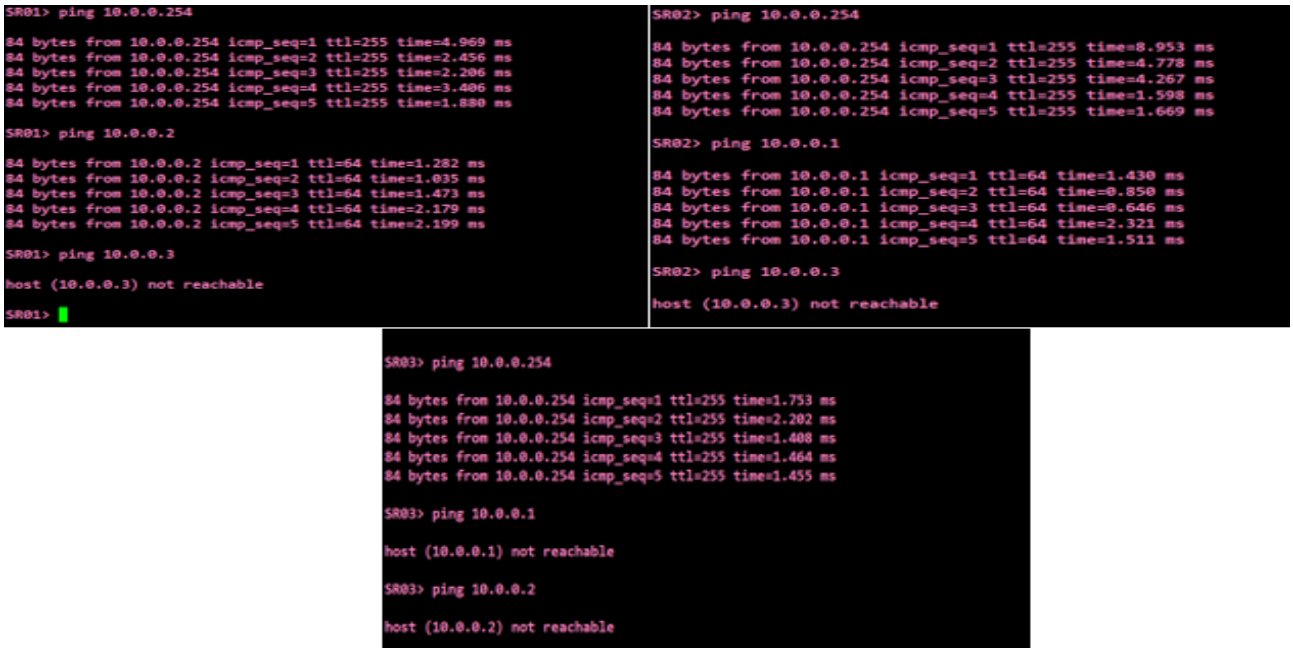

FIGURE V.87 – Test sur les PVLANs.

Conclusion

Ce chapitre est une simulation de l'architecture réseau proposée à la BMT, nous avons inclut les solutions de virtualisation et la supervision des réseaux pour obtenir une haute disponibilité étudié dans les chapitre précédents.Nous l'avons débuté par les composantes et les outils nécessaires, après nous avons décrit les étapes de sa réalisation avec des précision sur la configuration de chaque équipement et serveurs de l'architecture réseau qu'on a simulé avec GNS3.

Conclusion Générale

En conclusion, ce projet met en évidence l'importance de la virtualisation et de la supervision des réseaux pour garantir une haute disponibilité, en se basant sur l'étude de cas de BMT. La virtualisation permet de maximiser l'utilisation des ressources matérielles, d'améliorer l'évolutivité et de réduire les coûts liés à la gestion des infrastructures.

De plus, la supervision des réseaux assure une surveillance proactive, une détection précoce des problèmes et une résolution rapide des incidents, contribuant ainsi à maintenir les services essentiels opérationnels en tout temps.

Dans ce projet, nous avons proposé une nouvelle architecture réseau pour BMT, visant à améliorer sa robustesse et sa sécurité. Et pour la mise en œuvre d'une solution de virtualisation et de supervision des réseaux, adaptée aux besoins spécifiques de BMT, a permis d'optimiser la performance, la fiabilité et la sécurité de leur infrastructure, garantissant ainsi une expérience utilisateur optimale. Cette étude souligne l'importance cruciale de ces technologies dans un monde de plus en plus connecté et dépendant des systèmes informatiques, offrant des avantages significatifs pour les entreprises qui cherchent à assurer une haute disponibilité de leurs services.

Notre travail s'est d'abord concentré sur l'étude du contexte de la virtualisation, ainsi que sur les différentes solutions existantes dans ce domaine, tout en examinant également la partie de la supervision des réseaux et ses différentes approches.

Ensuite, nous avons proposé et simulé une nouvelle architecture pour l'infrastructure réseau de BMT. Nous avons configuré l'ensemble des équipements en utilisant différents protocoles garantissant la haute disponibilité, qui était l'objectif principal du projet.

Ce projet nous a permis d'acquérir de nombreuses connaissances dans un vaste domaine couvrant diverses technologies de virtualisation et de supervision pour assurer une haute disponibilité des équipements réseau.

Dans l'ensemble, nous avons atteint la plupart de nos objectifs fixés.

A travers les resultats de la simulation, nous avons pu monter la robustesse de l'architecture réseau proposée par rapport aux pannes, et la garentie d'une haute disponibilité grace aux solutions de virtualisation et suoervision utilisées

Cependant, vu la taille importante du projet et la limitation du temps, plusieurs améliorations peuvent être encore envisagées, en perspective, une possibilité d'utilisation du cloud pour une meilleure prise en charge de la securité.

Bibliographie

[1] http://www.bejaiamed.com. consulté le 2 mars 2023.

[2] https://bejaiamed.com/services/. consulté le 21 mars 2023.

[3] https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les/. consulté le 25 Mai 2023.

[4] https://arnaquesetpiratages.wordpress.com/attaques-par-deni-de-service/. consulté le 25 Mai 2023.

[5] https://www.researchgate.net/figure/Architecture/-de-pare-feu-simple-BULLET-Architecture-de-pare-feu-Distribue-ce-modele_fig1_278827782. consulté le 25 Mai 2023.

[6] https://web.maths.unsw.edu.au/~lafaye/CCM/protect/dmz-cloisonnement.htm. consulté le 25 Mai 2023.

[7] PUJOLLE, G.: *" Les réseaux ",6ème édition.* Eyrolles, 2008..

[8] GERVAISEr, David GELIBERT Farid SMILI Jérôme DEROCK Loïc RATSIHORIMANANA Mickaël DREYER Thomas: *La sécurité et la virtualisation.* Veille Technologique Livre Blanc, Mai 2012.

[9] https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/. consulté le 25 Mai 2023.

[10] https://philpetitpa.pagesperso-orange.fr/SNMP.pdf. consulté le 1 Mai 2023.

[11] https://www.educba.com/what-is-nagios/. consulté le 20 Avril 2023.

[12] https://www.axelit.fr/technologies/zabbix/. consulté le 20 Avril 2023.

[13] ALOUACHE Lynda, KEMACHA Habiba et: *"La Haute Disponibilité des Réseaux (HSRP) Cas d'étude : Réseau LAN de CEVITAL Agro-industrie".* Université Abderrahmane Mira, Bejaïa, 2021/2022.

[14] https://www.lemagit.fr/definition/Load-balancer-repartition-de-charge. consulté le 20 Avril 2023.

[15] https://www.ionos.fr/digitalguide/serveur/securite/raid/. consulté le 25 Avril 2023.

[16] https://www.computernetworkingnotes.com/ccna-study-guide/differences-between-packet-tracer-gns3-and-cisco-virl.html. consulté le 19 Mai 2023.

[17] https://logos.fandom.com/wiki/VMware_Workstation_Pro?file=VMware_Workstation_logo.jpg. consulté le 16 juin 2023.

[18] https://nds.id/cara-renewal-license-fortigate/. consulté le 16 juin 2023.

[19] https://www.laintimes.com/esxi-explication-sur-la-gestion-du-reseau/esxi-logo-laintimes/. consulté le 16 juin 2023.

[20] https://bejaiamed.com/organisation/. consulté le 2 mars 2023.

[21] HAJJEH, I.: *" Conception et validation d'un nouveau protocole pour la sécurisation des échanges. ".* thèse doctorat, Ecole Nationale Supérieure des Télécommunication, Paris, décembre 2004.

[22] Jean-François PILLOU, Jean Philippe BAY: *Tout sur la sécurité informatique.* DUNOD Paris, 2016.

[23] J. Ben-Othman, S. Bouam et: *protocole de sécurisation des données à base de routage dans les réseaux AD HOC*. thèse doctorat, Université des Sciences et de la Technologie Houari Boumédiene. Faculté d'Electronique et Informatique, Alger, 2004.

[24] CONTES, A.: *" Une Architecture De Sécurité Hiérarchique, Adaptable Et Dynamique Pour La Grille "*. thèse doctorat, Université de Nice - Sophia Antipolis, Septembre 2005.

[25] *Les attaques en déni de service(DDoS).* https://www.cybermalveillance.gouv.fr/tousnos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos.

[26] *Pare-feux('Firewalls') Cours de sécurité – Cnam.* http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours_parefeux.pdf.

[27] Jabou Chaouki, Schillings Michaël et Hantach Anis: *" TER Détection d'anomalies sur le réseau "*. Rapport de projet, Université Paris Descartes, 2009.

[28] https://www.appvizer.fr/magazine/services-informatiques/virtualisation/type-virtualisation. consulté le 20 mars 2023.

[29] https://commentouvrir.com/info/avantages-et-inconvenients-de-la-virtualisation/ consulté le 2 Mai 2023.

[30] https://www.lemagit.fr/essentialguide/Les-astuces-de-ladministrateur/-reseau-en-2023. consulté le 1 Mai 2023.

[31] https://www.lemagit.fr/essentialguide/Les-astuces-de-ladministrateur-reseau-en- consulté le 25 Avril 2023.

[32] https://fr.theastrologypage.com/common-information-model. consulté le 25 Avril 2023.

[33] Méré, Aurélien: *"Les réseaux - Les protocoles de gestion réseau - Le protocole SNMP"*. 2005.

[34] https://supervision-clever.fr/meilleures-solutions-de-supervision-informatique/ consulté le 1 Mai 2023.

[35] https://www.syloe.com/glossaire/haute-disponibilite/. consulté le 3 mars 2023.

[36] https://learn.microsoft.com/fr-fr/sharepoint/administration/high-availability-and-disaster-recovery-concepts. consulté le 2 Avril 2023.

[37] Https://support.huawei.com/enterprise/en/doc/EDOC1100055104/a5b057b1/overview-of-vrrp. consulté le 25 Avril 2023.

[38] https://www.cisco.com/c/fr_ca/support/docs/smb/switches/cisco-250-series-smart-switches/smb5303-configure-spanning-tree-protocol-stp-o pdf. consulté le 2 Mai 2023.

[39] http://www.fsr.ac.ma/DOC/cours/informatique/benaini/Cours2-AdminReseaux.pdf. consulté le 2 Mai 2023.

[40] https://www.connecthostproject.com/vtp.html. consulté le 2 Mai 2023.

[41] https://www.bitwarsoft.com/fr/a-brief-introduction-to-fault-tolerance.html. consulté le 23 Mai 2023.

[42] https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco. consulté le 24 Mai 2023.

[43] https://www.lebigdata.fr/cluster-definition. consulté le 25 Mai 2023.

[44] https://cisco.goffinet.org/ccna/cisco-ios-cli/installer-et-configurer-gns3/#11-pr. consulté le 20 juin 2023.

[45] https://www.vmware.com/content/dam/digitalmarketing/vmware/fr/pdf/VMware-vSphere-Standard-Edition.pdf. consulté le 20 juin 2023.

[46] https://learningnetwork.cisco.com/s/question/0D53i00000KsOb9CAF/cisco-iou. consulté le 16 juin 2023.

[47] https://www.futura-sciences.com/tech/definitions/informatique-windows-10-15093/, consulté le 20 juin 2023.

[48] https://www.ikoula.com/fr/systeme-d-exploitation-windows-server-2019#:~:text=Le", consulté le 20 juin 2023.

[49] https://www.fortinet.com/fr/products/next-generation-firewall#:~:text=FortiGate, consulté le 20 juin 2023.

[50] https://www.ionos.fr/digitalguide/serveur/know-how/esxi, consulté le 20 juin 2023.

Annexe : Etapes d'installation des environnements.

Installation de GNS3 sous Windows :

Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton «Finish». La Figure V.88 suivante représente l'interface de GNS3.

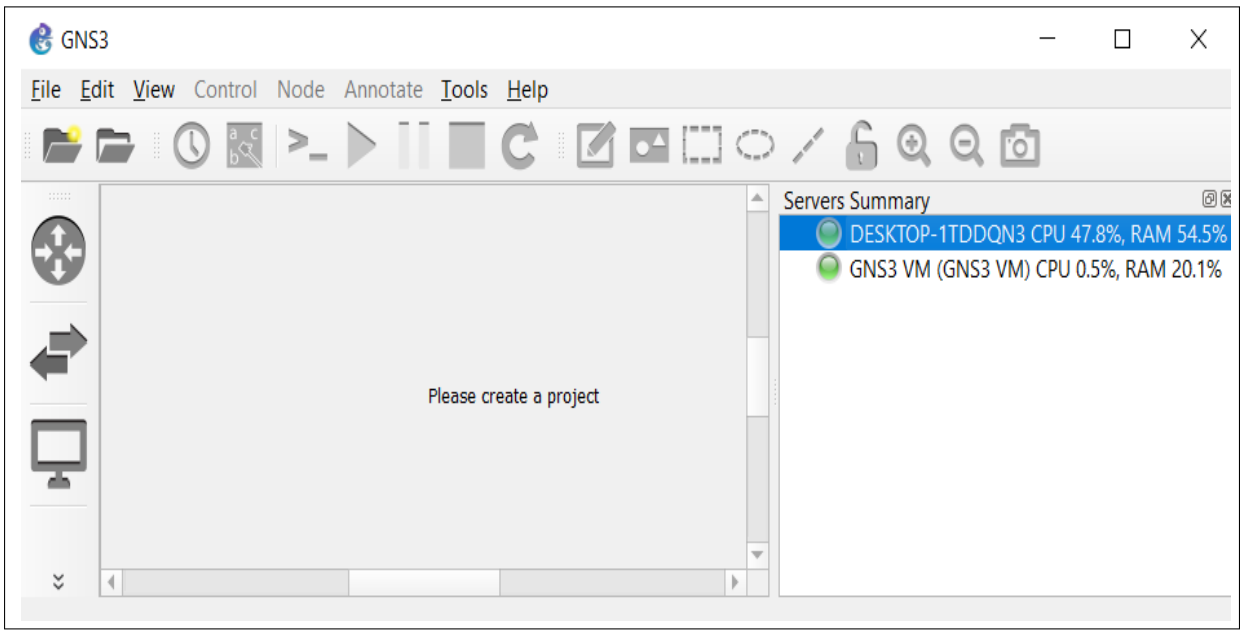

FIGURE V.88 – Interface d'accueil GNS3.

Installation de la VMware Workstation 17pro :

Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation en suivant les étapes de la Figure V.89 ci-dessous :

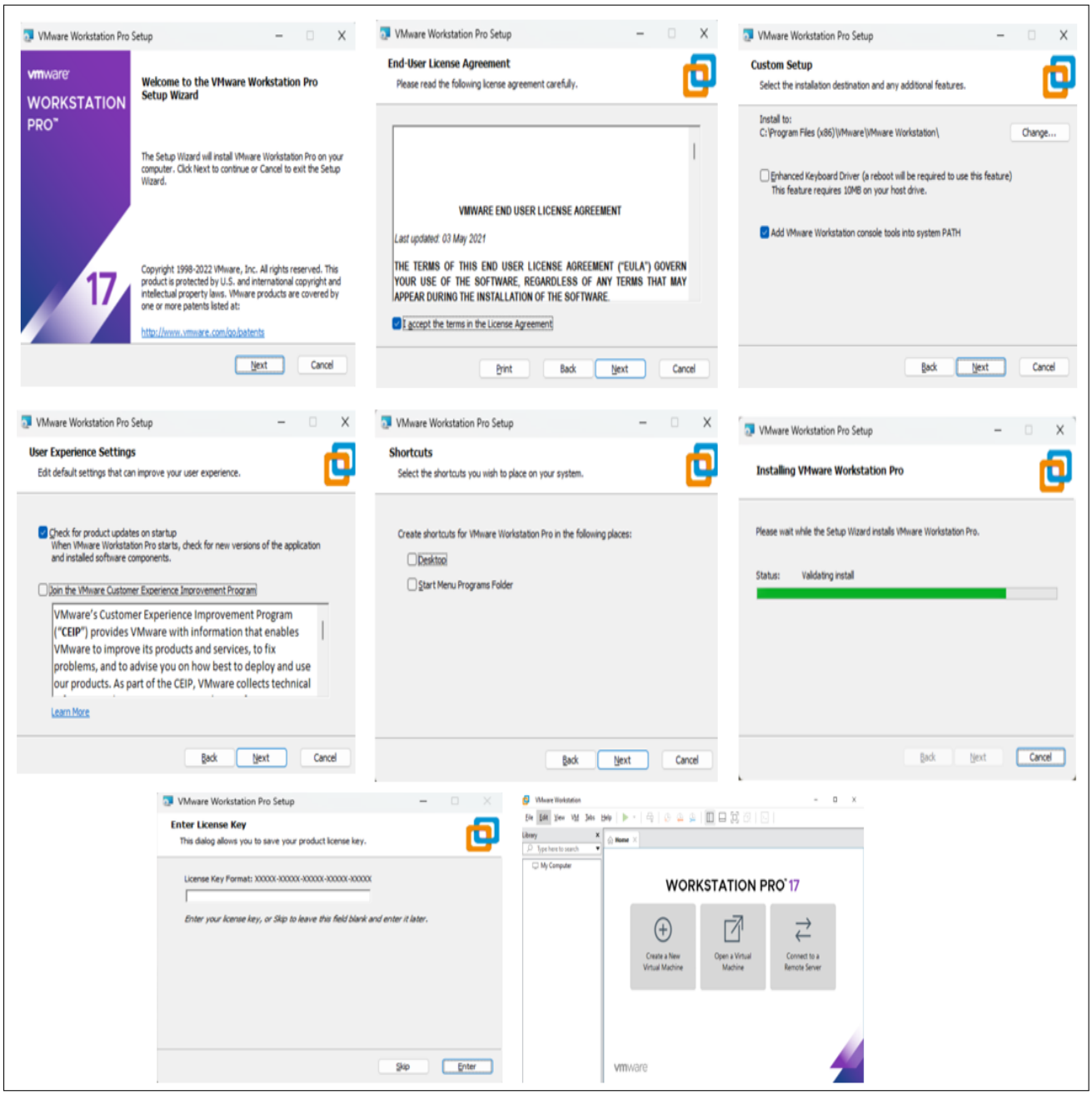

FIGURE V.89 – Installation de VMware workstation.

Après l'installation de VMware une page d'accueil (Figure V.90) apparaîtra :

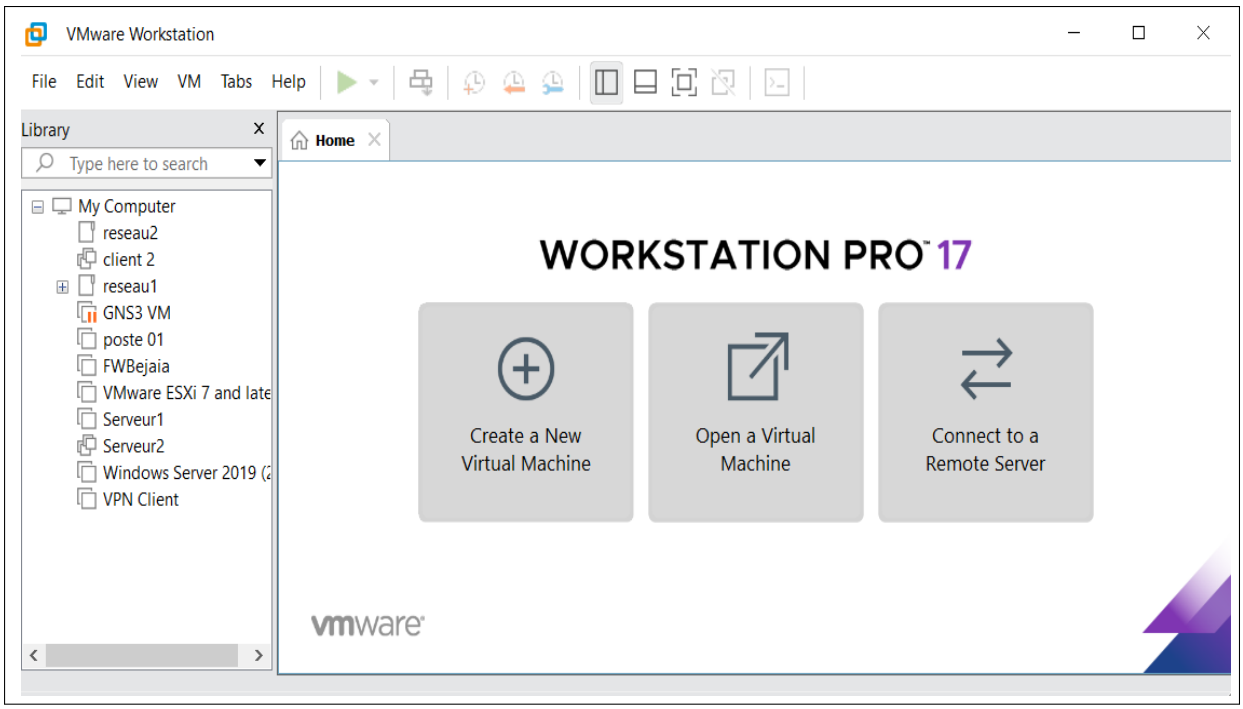

FIGURE V.90 – Interface d'accueil de VMware Workstation.

Installation du Windows 10 sous VMwar Workstation :

Nous avons créé une machine après avoir ajouté l'image de Windows 10 sur VMware à qui on a attribué les caractéristiques suivantes Figure V.91 :

- Allocation de la mémoire pour la machine fixé à 2GB .

- Deux processeurs .

- Disque dur 60GB.

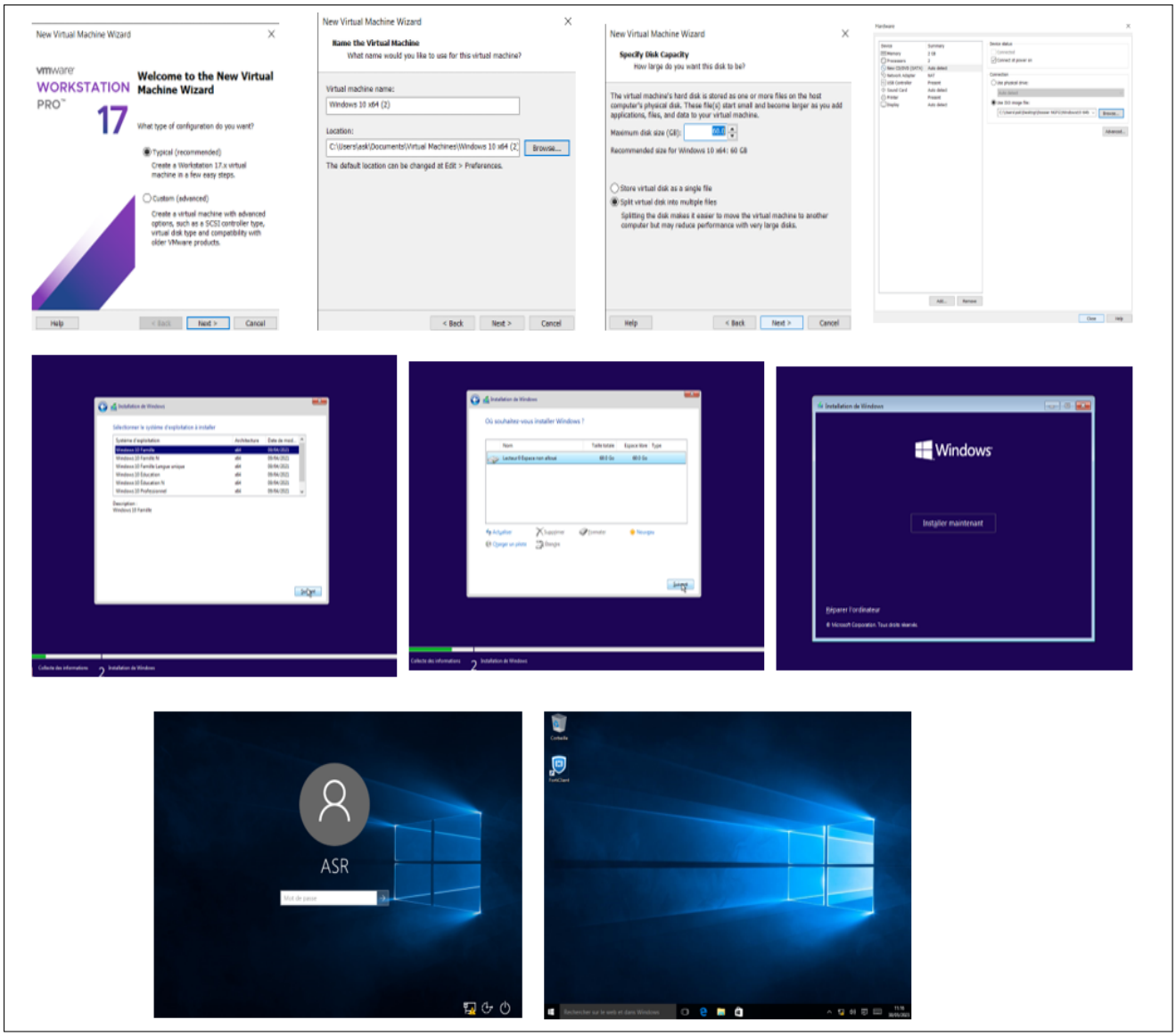

FIGURE V.91 – Installation du Windows 10 sous VMwar Workstation.

Instalation Windows Server 2019 :

Dans cette partie nous allons voir les différentes étapes d'installations de Windows Server 2022 (Figure V.92).

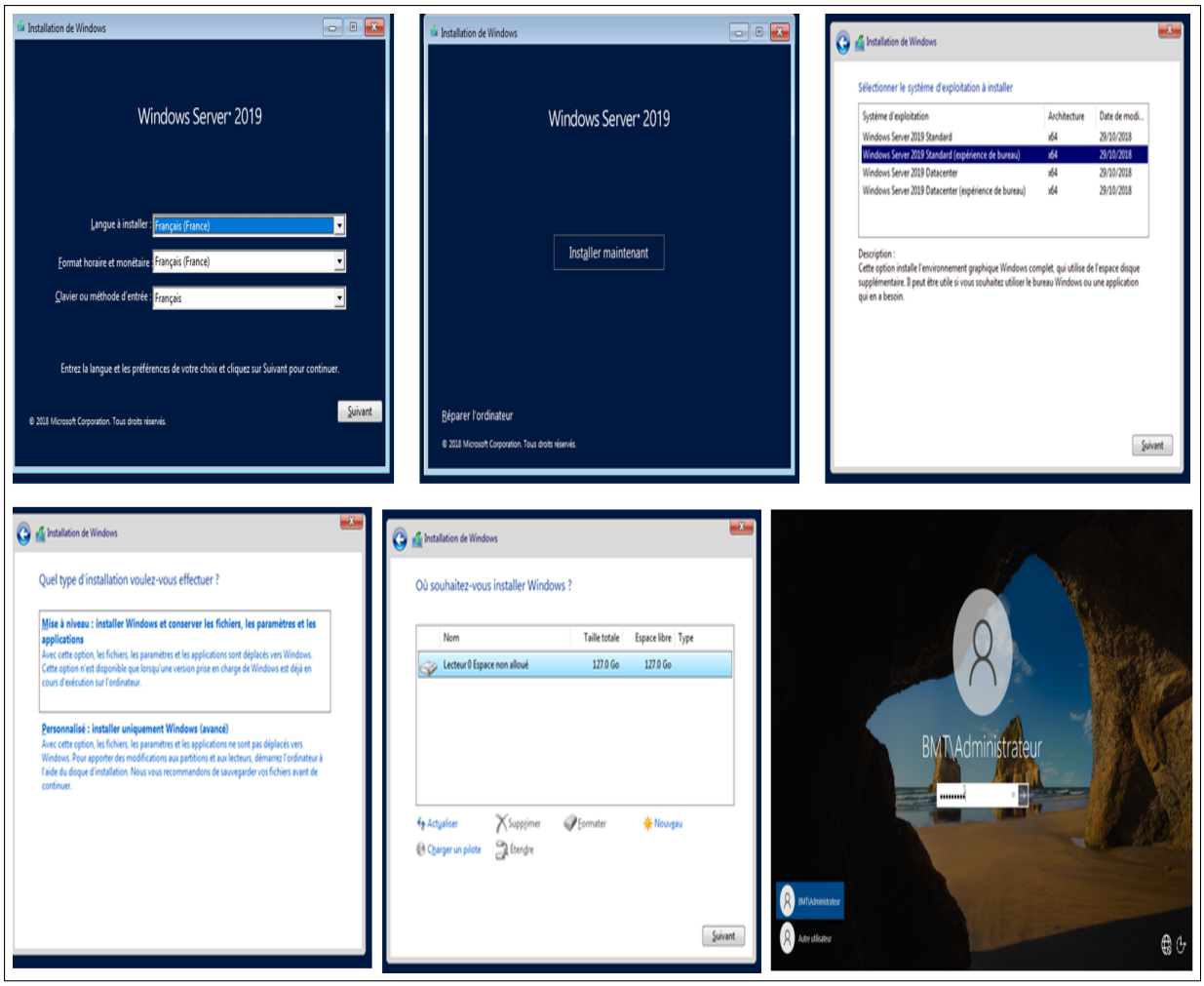

FIGURE V.92 – Installation du Windows 10 sous VMwar Workstation.

Installation de serveur ESXi 7.0.1 :

Premièrement on va crée une machine virtuelle ESXi 7 sous VMware et on lance l'installation, puis on lui affecte une adresse IP statique 192.168.1.202/24 (Figure V.93) :

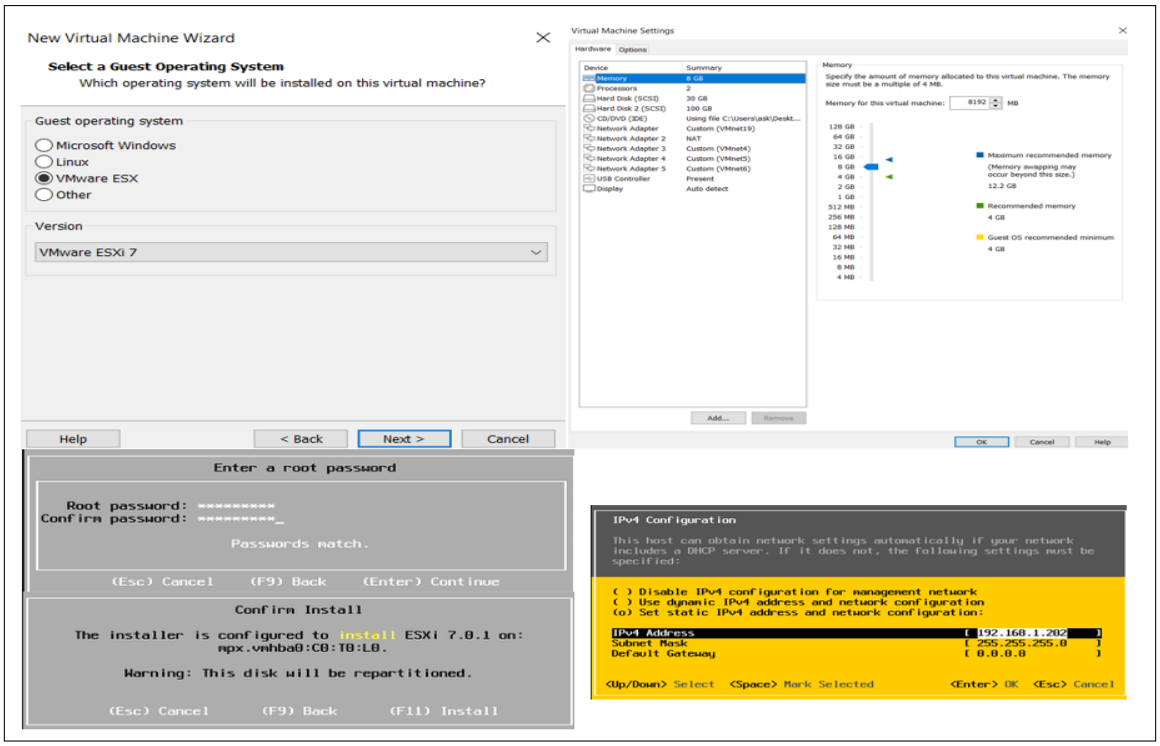

FIGURE V.93 – Installation et configuration de serveur ESXi 7 sur VMware.

Après avoir fini l'installation, on se dirige vers le navigateur web pour se connecter à l'interface Web de configuration de ESXi. Pour cela on utilise l'adresse IP de l'interface LAN https ://192.168.1.202 . La Figure V.94 montre la page d'identification et l'interface d'accueil après avoir introduit le mot de passe et le nom d'utilisateur(s'authentifier) .

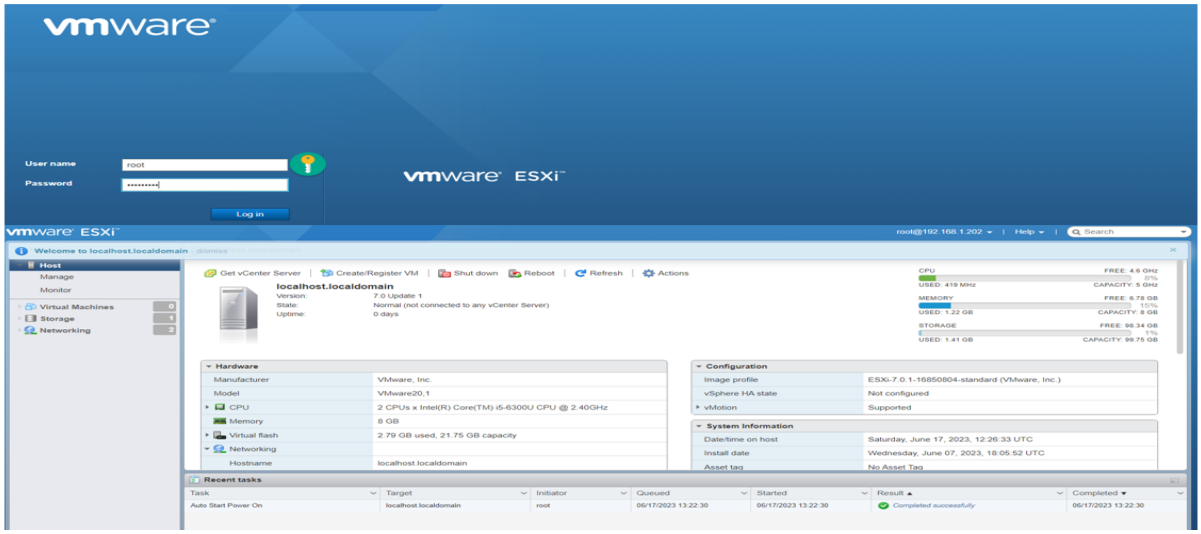

FIGURE V.94 – Page d'accueil ESXi 7.

Resumé

La combinaison de la virtualisation et de la supervision réseau offre une solution efficace pour assurer une haute disponibilité dans un réseau. La virtualisation permet le déploiement flexible de machines virtuelles qui peuvent être déplacées en cas de panne ou de maintenance. En parallèle, la supervision réseau assure une surveillance constante des performances et de la santé des équipements, permettant une détection proactive des problèmes et une intervention rapide pour minimiser les interruptions de service. Notre projet consiste à proposer une nouvelle architecture réseau de l'entreprise BMT. L'objectif est d'assurer une disponibilité élevée et une gestion efficace des infrastructures réseau. Pour ce faire, nous avons opté pour Gns3 et VMware pour la proposition et la simulation de notre architecture.

Mots clés : virtualisation, supervision, haute disponibilité, Gns3, BMT.

Abstract

The combination of virtualization and network monitoring offers an effective solution to ensure high availability in a network. Virtualization allows the flexible deployment of virtual machines that can be moved in the event of failure or maintenance. At the same time, network monitoring provides constant monitoring of device performance and health, enabling proactive problem detection and rapid response to minimize downtime. Our project consists in proposing a new network architecture of the company BMT. The objective is to ensure high availability and efficient management of network infrastructures. To do this, we opted for Gns3 and VMware for the proposal and simulation of our architecture.

Key words : virtualization, monitoring, high availability, Gns3, BMT.