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

Mémoire de Fin d'Etude

En vue d'obtention du diplôme de Master en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Mise en place de la haute disponibilité de l'infrastructure et la virtualisation

---

Réalisé par :

Mlle. IKENI Saliha et Mlle. MAKHLOUFI Rima

Président	**Dr. GHANEM Souhila**	**U. A/Mira Béjaïa.**
Examinateur	**Dr. BOUADEM Nassima**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. KHALED Hayette**	**U. A/Mira Béjaïa.**

Année universitaire 2022/2023

Remerciements

À travers ce modeste travail, nous tenons à exprimer notre profonde gratitude à notre encadrant, Mme **KHALED Hayette**, pour ses précieux conseils, son orientation experte et son soutien constant tout au long de notre projet de fin d'étude. Nous sommes reconnaissantes envers Mme **GHANEM.S** et Mme **BOUADEM.N**, présidente et membre du jury respectivement, d'avoir acceptées d'examiner et d'évaluer notre travail avec bienveillance.

Nos remerciements s'étendent également à tous les professeurs et enseignants qui nous ont apporté leur aide et leur expertise, contribuant ainsi à la réalisation de ce travail. Nous tenons à exprimer notre sincère reconnaissance envers tous ceux qui ont participé de près ou de loin à la concrétisation de ce projet.

Nous souhaitons exprimer nos plus sincères remerciements à notre encadrant de stage, Mr. **SLIMANI Mennad**, pour sa précieuse guidance, ses conseils éclairés et son soutien inestimable tout au long de notre projet de fin d'étude. Comme nous tenons à exprimer notre profonde gratitude Mr. **DJEBBARI Yacine** pour sa patience et sa volonté de partager ses connaissances ont été inestimables qui nous ont pu approfondir notre compréhension du domaine et relever des défis passionnants.

Enfin, nous voulons adresser nos plus sincères remerciements à nos chers parents et familles, dont le soutien indéfectible, les sacrifices et les encouragements constants ont été essentiels pour nous permettre de mener à bien cette formation dans les meilleures conditions.

Dédicaces

À mon Dieu tout-puissant,

Je commence cette dédicace en te remerciant du fond de mon cœur pour ta grâce infinie et ta guidance tout au long de ma vie.

À mon cher père,

Tu es mon héro. Merci pour ton amour paternel a été une source d'inspiration pour moi. Je t'aime de tout mon cœur.

À ma chère mère,

Tu es la personne la plus aimante, attentionnée et dévouée que je connaisse. Tu as toujours été là pour moi. Je t'aime plus que les mots ne peuvent le dire.

À mon cher frère,

Tu es mon confident et mon meilleur ami. Je te remercie pour ton soutien inconditionnel et ton amour fraternel. Je t'aime énormément.

À mon fiancé bien-aimé,

Ta présence dans ma vie m'a apporté un amour pur et une joie infinie. Tu m'as soutenu dans tous mes projets et m'as encouragé à atteindre mes objectifs.

À ma future belle famille,

Mes sincères remerciements , je suis sincèrement reconnaissant de votre générosité et de votre soutien inconditionnel.

Je souhaite exprimer ma sincère reconnaissance à Tata Kahina et sa petite famille, Nassima et tonton hanafi ainsi leurs enfants et mes tantes.

À ma binôme et sa famille,

Travailler avec toi a été une expérience incroyable.Avec ton soutien ont contribué à la réussite de ce projet. Je voudrais également adresser mes remerciements à ta famille.

À mes chères copines,

Vous êtes mes amies les plus proches. Merci d'avoir été là pour moi tout au long de ce parcours. Je vous aime chéries Naima, Leticia, Lynda.

Enfin, à tous ceux qui ont contribué de près ou de loin à notre PFE.

Saliha

Dédicaces

Alhamdullilah,
Je commence cette dédicace par m'exprimer ma profonde gratitude envers ALLAH pour m'avoir accordé la force, la persévérance et la clarté d'esprit tout au long de cette étude

À mon cher papa,

Tu es ma fierté, mon pilier et ma source d'inspiration.je te remercie de ton amour inconditionnel et de ton soutien constant que tu m'apporte tout au long de mon chemin. Je t'aime très fort. .

À ma chère mama,

Tu es mon exemple, ma confidente et ma supportrice dans la vie. Je te remercie pour ton influence positive dans ma vie. Je t'aime de profond du mon cœur.

A mes chères sœurs,

Nesrine, Yasmine et Malak vous êtes mes meilleurs amies, mes complices, et mes alliées je suis très reconnaissante de vous avoir dans ma vie. je vous aime profondément mes chéries.

A mes chèrs cousins ,

Lyes, Mohand, Anis, Koceila, Bilal et Faiz, notre enfance partagée marquée par nos rires et nos moments de complicité restera gravée dans ma mémoire. Je suis trés honorée de vous avoir dans ma vie, je vous aime. Ma petite cousine Nadine, tu as déjà conquis mon cœur avec ta douceur et ta tendresse. Je t'aime ma petite.

A ma binôme et sa famille,

Je suis très honorée de partager ce moment assez spécial de ma vie avec toi. Je te remercie pour ton soutien, ta présence et tes conseils. Je voudrais également adresser mes remerciements à toute ta famille.

A mes chers amis,

Vous avez été mes partenaires de fous rires et mes compagnons d'aventure. Que nos liens d'amitié se renforcent et que nous continuions à célébrer nos réussites ensemble.

Enfin, à tous ceux qui ont contribué de près ou de loin à notre PFE.

Rima

Table des matières

Table des matières

Table des figures

Liste des tableaux

Introduction générale 1

1 Généralités sur les réseaux et la sécurité informatique **2**

1.1 Introduction 3
1.2 Définition des réseaux informatiques 5
1.3 Types des réseaux informatiques 5
1.4 Objectifs des réseaux 5
1.5 Architectures des réseaux 5
1.5.1 Poste à poste 6
1.5.2 Client/serveur 6
1.6 Topologie des réseaux 7
1.6.1 La topologie physique 7
1.6.1.1 La topologie en bus 7
1.6.1.2 La topologie en étoile 8
1.6.1.3 La topologie en anneau 8
1.6.1.4 La topologie maillée 9
1.6.1.5 La topologie en arbre 9
1.6.2 La topologie logique 10
1.7 Les modèles des réseaux 10
1.7.1 Modèle OSI 10
1.7.2 Modèle TCP/IP 10
1.8 Routage 11
1.9 Définition de la sécurité 13
1.10 Les objectifs de la sécurité 13
1.11 Terminologie de la sécurité informatique 13
1.12 Les causes de l'insécurité 14
1.13 Les attaques informatiques 14
1.13.1 Un logiciel malveillant 14
1.13.2 Attaques de reconnaissance 15
1.13.3 Attaques d'accès 15
1.13.4 Attaques par déni de service 15
1.14 L'effet d'une attaque 15
1.14.1 Attaque active 15
1.14.2 Attaque passive 16

1.15 Les mécanismes de sécurité . . . 16
1.15.1 L'antivirus . . . 17
1.15.2 Le cryptage . . . 17
1.15.3 Le pare-feu . . . 17
1.15.4 Le proxy . . . 18
1.15.5 Système de détection d'intrusion (IDS) . . . 19
1.15.6 Un système de prévention des intrusions (IPS) . . . 19
1.15.7 Les VPN . . . 19
1.15.8 Les VLANs . . . 20
1.15.9 La DMZ . . . 20
1.16 Conclusion . . . 20

2 Présentation de l'organisme d'accueil **22**
2.1 Introduction . . . 23
2.2 Les valeurs du Groupe CEVITAL . . . 25
2.3 Situation géographique . . . 25
2.4 Organigramme général de CEVITAL . . . 26
2.5 Le rôle de différentes directions de l'entreprise CEVITAL . . . 27
2.5.1 La direction Système d'informations . . . 27
2.5.2 La direction des Finances . . . 27
2.5.3 La direction commerciale . . . 27
2.5.4 La direction des Ressources Humaines . . . 27
2.6 L'organigramme de service informatique . . . 27
2.7 Le matériel informatique de l'entreprise CEVITAL . . . 28
2.7.1 Switch d'accès de type Cisco Catalyst 2960-X et 9200 . . . 28
2.7.2 Switch cœur de type Cisco 6800 . . . 28
2.7.3 Routeur de type Cisco 1900 . . . 29
2.7.4 Le pare-feu FortiGate (601E) . . . 29
2.7.5 Data Center . . . 29
2.8 VLAN de l'entreprise . . . 30
2.9 L'architecture de l'entreprise CEVITAL . . . 31
2.10 Problématique et solutions proposées . . . 31
2.10.1 Problématique . . . 31
2.10.2 Solutions Proposées . . . 31
2.10.3 Objectifs . . . 32
2.11 Conclusion . . . 32

3 La haute disponibilité **33**
3.1 Introduction . . . 34
3.2 Nécessité de haute disponibilité . . . 34
3.3 Les stratégies de la haute disponibilité . . . 34
3.3.1 La redondance . . . 34
3.3.1.1 La redondance matérielle . . . 34
3.3.1.2 La redondance logique . . . 35
3.3.2 Les protocoles de la haute disponibilité . . . 35
3.3.2.1 Le protocole Virtual Router Rendundancy (VRRP) . . . 35
3.3.2.2 Le protocole Hot Standby Router (HSRP) . . . 35
3.3.2.3 Le protocole Gateway Load Blancing (GLBP) . . . 36

3.3.2.4 Le protocole Spainning Tree (STP) . . . 36
3.3.3 Protocole de gestion de VLAN . . . 36
3.3.3.1 Le protocole Vlan Trunking (VTP) . . . 36
3.3.4 Redundant Array of Independent Disks (RAID) . . . 37
3.3.5 La répartition de charge . . . 37
3.3.5.1 L'utilité de la répartition de charge . . . 37
3.3.6 Clustering . . . 38
3.3.6.1 La mise en place de cluster . . . 38
3.3.6.2 Cluster à surveillance de répartition de charge . . . 39
3.3.6.3 Cluster à mécanisme de redondance . . . 39
3.3.6.4 Cluster aux tolérances aux pannes . . . 39
3.3.7 Le basculement automatique . . . 40
3.3.8 La sauvegarde et la récupération . . . 41
3.3.8.1 Network Attached Storage (NAS) . . . 41
3.3.8.2 Storage Area Network (SAN) . . . 42
3.3.9 La supervision et le monitoring . . . 43
3.4 Les avantages de la haute disponibilité . . . 44
3.5 Conclusion . . . 44

4 La virtualisation **45**
4.1 Introduction . . . 46
4.2 Histoire de virtualisation . . . 46
4.3 Le modèle de couches des systèmes d'informations . . . 46
4.3.1 Couche infrastructure . . . 47
4.3.2 Couche opérationnelle . . . 47
4.3.3 Couche applicative . . . 47
4.3.4 Couche décisionnelle . . . 47
4.4 Le moniteur des machines virtuelles . . . 48
4.4.1 Les hyperviseurs de type 1 . . . 48
4.4.2 Les hyperviseurs de type 2 . . . 49
4.5 Le fonctionnement de la virtualisation . . . 50
4.6 Les avantages de virtualisation . . . 50
4.7 Les meilleures pratiques de la virtualisation . . . 51
4.8 Les types de virtualisation . . . 51
4.8.1 Virtualisation de systèmes d'exploitation . . . 51
4.8.2 Virtualisation de poste de travail . . . 52
4.8.3 Virtualisation de données . . . 53
4.8.4 Virtualisation matérielle . . . 53
4.9 Les techniques de virtualisation . . . 53
4.9.1 La virtualisation complète . . . 53
4.9.2 La paravirtualisation . . . 53
4.9.3 L'isolation . . . 54
4.10 Migration de la machine virtuelle . . . 54
4.11 Consolidation, rationalisation et concentration des serveurs . . . 54
4.11.1 Consolidation des serveurs . . . 54
4.11.2 Rationalisation des serveurs . . . 55
4.11.3 Concentration des serveurs . . . 56
4.12 Conclusion . . . 57

5 Réalisation **58**
5.1 Introduction . . . 59
5.2 Architecture à réaliser . . . 59
5.3 Environnement de travail . . . 59
5.3.1 GNS3 . . . 59
5.3.1.1 Installation de GNS3 sous Windows . . . 60
5.3.2 VMware Workstation version 17.0.0 . . . 60
5.3.2.1 Installation VMware Workstation version 17pro . . . 61
5.4 Configuration des équipements . . . 61
5.4.1 La commutation . . . 61
5.4.1.1 Protocole trunk . . . 61
5.4.1.2 Protocole VTP . . . 62
5.4.1.3 Virtual Local Area Networks (VLANs) . . . 64
5.4.1.4 Configuration de protocole PAgP . . . 68
5.4.2 Le Routage . . . 69
5.4.2.1 Configuration de pare-feu . . . 69
5.4.2.2 Installation et configuration de Serveur DHCP . . . 73
5.4.3 La configuration du site distant . . . 76
5.4.3.1 Les VLANs . . . 77
5.4.3.2 Activer le routage inter-VLANs . . . 78
5.4.3.3 Configuration de mode trunk . . . 78
5.4.3.4 Configuration de protocole Link Aggregation Configuration (LACP) 80
5.4.3.5 Configuration de protocole Host Standby Router (HSRP) . . . 80
5.4.3.6 Configuration de tunnel VPN GRE . . . 81
5.5 Tester la haute disponibilité du réseau . . . 84
5.5.1 Test de l'attribution de l'adresse IP à un PC par le serveur DHCP . . . 85
5.5.2 Teste le basculement entre le serveur1 et le serveur2 . . . 85
5.5.3 Test de configuration de la HA au niveau du FortiGate-B . . . 86
5.5.4 Vérification des règles de routage configurées sur le site distant . . . 87
5.5.5 Test de PING de FortiGate-A vers le Tunnel . . . 87
5.5.6 Test de PING de FortiGate-A vers la passerelle du routeur du site distant 87
5.5.7 Test de PING de FortiGate-A vers le LAN du site distant . . . 88
5.5.8 Test de PING due site distant vers FortiGate-A . . . 88
5.5.9 Test de ping du PC management vers le Tunnel . . . 88
5.5.10 Test du Ping de PC manager vers le PC du site distant . . . 88
5.6 Conclusion . . . 89
Conclusion générale . . .

A Annexe
Annexe . . .

Bibliographie

Table des figures

1.1 L'architecture poste à poste. 6
1.2 L'architecture client serveur. 7
1.3 La topologie en bus [2]. 8
1.4 La topologie en étoile [5]. 8
1.5 La topologie en anneau [4]. 9
1.6 La topologie en maillé.[6] 9
1.7 La topologie en arbre. [8] 10
1.8 Modèle OSI [9]. 11
1.9 modèle TCP/ IP [9]. 11
1.10Une attaque active 16
1.11Une attaque passive 16
1.12La technique de cryptage[15]. 17
1.13Le pare-feu [16]. 18
1.14Le proxy [17]. 18
1.15La technique de l'IPS et l'IDS [18] 19
1.16La sécurité par la mise d'un VPN 20

2.1 Localisation de l'entreprise CEVITAL 25
2.2 L'organigramme générale de l'entreprise CEVITAL [19]. 26
2.3 L'organigramme de département DSI de CEVITAL [19]. 28
2.4 Commutateur 2600-X [20]. 28
2.5 Commutateur 9200 [20]. 28
2.6 Commutateur cœur Cisco 6800 [20]. 29
2.7 Routeur 1900 [20]. 29
2.8 Le pare-feu fortigate [20]. 30
2.9 Centre de données [20]. 30
2.10L'architcture de l'entreprise CEVITAL[19]. 31

3.1 La répartition de charge 38
3.2 La mise en place d'un cluster avec Load balancer 39
3.3 Serveur redondant [24]. 40
3.4 Les techniques de tolérances aux pannes dans les systèmes répartis [25]. . . 40
3.5 Network Attached Storage 42

4.1 Le modèle de couches des systèmes d'informations 48
4.2 Hyperviseur type 1 [29]. 49
4.3 Hyperviseur type 2 [29]. 50
4.4 virtualisation des systèmes d'exploitation de type 1 et 2 [30] 52
4.5 virtualisation des postes de travail 52

4.6 Consolidation des serveurs 55
4.7 Rationalisation des serveurs 56
4.8 Concentration des serveurs 56

5.1 Architecture de réalisation 59
5.2 Logo de GNS3. 60
5.3 L'interface principale de gns3. 60
5.4 Logo de VMWare 17pro. 61
5.5 Configuration du mode trunk sur core-A. 62
5.6 Vérification de l'interface trunk pour core-A. 62
5.7 Configuration du mode vtp server sur core-A. 63
5.8 Configuration du mode vtp client sur Swa01. 63
5.9 Verification du mode vtp serveur sur Core-A. 64
5.10Verification du mode vtp client sur Swa01. 64
5.11Creation des VLANs. 65
5.12Verification de la creation des VLANs sur core-A. 65
5.13Verification de la creation des VLANs sur Sw01. 66
5.14Configuration de VLAN natif sur Core-A. 67
5.15Verification de VLAN natif. 67
5.16Configuration de mode accès sur le Swa02 le vlan 101. 68
5.17Vérification mode accès sur le Swa02 le vlan 101. 68
5.18Configuration de protocole PAgP sur le Core-A en le mode « desirable ». . 69
5.19Vérification de protocole PAgP sur le Core-A. 69
5.20Configuration de l'interface port 2. 70
5.21Configuration de l'interface port 5. 70
5.22Configuration de l'interface port 1. 70
5.23Création de la zone. 71
5.24Configuration de HA redondant sur le FortiGate-A. 71
5.25Configuration de HA sur le pare-feu FortiGate-B. 72
5.26Vérification du configuration de HA. 72
5.27Définition la régle de routage de réseau local vers l'externe. 73
5.28Installation de serveur AD. 74
5.29Installation de serveur DHCP. 75
5.30Interface principale de serveur après la configuration de service AD et DHCP. 75
5.31Créer l'entendue 100 sur le ser01. 76
5.32Configuration de basculement de l'étendu. 76
5.33L'architecture de site distant. 77
5.34Vérification de VLAN sur S1. 77
5.35Vérification des VLANs sur S2. 78
5.36Configuration de routage inter-VLANs Core2. 78
5.37Vérification de mode trunk sur le commutateur S1. 79
5.38Vérification de mode trunk sur le commutateur S2. 79
5.39Attribution de l'adresse IP pour le PC6. 80
5.40Configuration de protocole LACP sur le commutateur S2. 80
5.41Configuration de protocole HSRP sur le Core1 en mode active. 81
5.42Configuration de protocole HSRP sur le Core2 en mode standby. 81
5.43Vérification de protocole HSRP sur le Core1 en mode active. 81
5.44Configuration de VPN GRE sur le site-dist. 82

5.45Vérification de VPN GRE sur le site-dist. 82
5.46Configuration de VPN GRE sur le FortiGate-A. 82
5.47Vérification de la création de tunnel-GRE au niveau de FortiGate-A. 83
5.48La règle 1 du pare-feu FortiGate-A. 83
5.49La règle 2 du pare-feu FortiGate-A. 84
5.50Configuration de règle de routage de site distant vers le LAN. 84
5.51Configuration de règle de routage de site distant vers le LAN. 85
5.52Tester le basculement en désactivant le serveur 1 (étape 01). 85
5.53Tester le basculement en désactivant le serveur 1(étape 02). 86
5.54Tester la HA au niveau de FortiGate-B 86
5.55Vérification des régles de routage au niveau de site distant. 87
5.56Vérication du ping de FortiGate-A vers le tunnel VPN. 87
5.57Vérication du ping de FortiGate-A vers la passerelle du routeur de site distant. 87
5.58Vérication du ping de FortiGate-A vers le LAN du site distant. 88
5.59Vérication du ping de site distant vers FortiGate-A. 88
5.60Vérication du ping de PC manager vers le tunnel. 88
5.61Vérication du ping de PC manager vers le Pc de site distant. 89

Liste des tableaux

2.1 Plan d'adressage IPv4 [19] 30

Liste des abréviations

AD	Active Directory
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FT	Fault Tolerance (Tolérance aux pannes)
FTP	File Transfer Protocol
GSLB	Global Server Load Balancing (Équilibrage de charge global et basé sur les services)
HA	High Availability (Haute disponibilité)
HP	High Performance (Haute Performance)
HTTP	HyperText Transfer Protocol
IDS	Intrusion detection System
IMS	IP multimedia subsystem
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NAS	Network Attached Storage (Stockage en réseau)
NAT	Network Address Translation
OSI	Open Systems Interconnection
P2P	peer-to-peer
SAN	Storage Area Network (Réseau de stockage)
SI	System Information
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine (Machine virtuelle)
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol (Protocole de routage de redondance virtuelle)
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

Introduction générale

À mesure que notre monde devient de plus en plus interconnecté et dépendant de la technologie, les entreprises sont confrontées à des défis croissants en ce qui concerne la disponibilité et les performances de leurs infrastructures informatiques. La panne ou l'interruption des systèmes informatiques de l'organisation peut entraîner des pertes financières considérables, une dégradation de la réputation de l'entreprise et une baisse de la satisfaction des utilisateurs. Pour faire face à ces défis, de nombreuses entreprises se tournent vers deux concepts principaux voir la haute disponibilité et la virtualisation pour garantir des services continus et fiables.

Dans le cadre de notre projet de fin d'études en Informatique, spécialisé en Administration et Sécurité des Réseaux, nous avons réalisé notre stage au sein de l'organisme d'accueil CEVITAL, qui attache une grande importance à l'acquisition de nouvelles solutions pour garantir une haute disponibilité de son réseau. Ce stage nous a offert une opportunité unique de découvrir le fonctionnement du réseau et d'approfondir nos connaissances.

L'objectif principal de notre projet de mémoire consiste à configurer et mettre en place une infrastructure à haute disponibilité, ainsi que la virtualisation, afin de permettre l'échange d'informations entre tous les équipements présents dans le réseau local et distant de CEVITAL. Ce travail contribuera à améliorer la continuité des services et renforcer la fiabilité du réseau, ce qui représente un enjeu crucial pour l'entreprise.

Afin d'atteindre notre objectif, notre mémoire est structuré en cinq chapitres principaux. Le premier chapitre aborde les généralités des réseaux et la sécurité informatique. Le deuxième chapitre est dédié à la présentation de l'organisme d'accueil, CEVITAL en mettant en avant sa structure et son environnement réseau. Dans le troisième chapitre, nous nous concentrons sur la haute disponibilité du réseau, en explorant les concepts essentiels et en présentant des solutions potentielles pour garantir une continuité des services fiables. Le quatrième chapitre traite de la virtualisation et de son importance dans l'optimisation des ressources et la flexibilité du réseau.

Enfin, dans le dernier chapitre, nous détaillons la mise en œuvre de la solution au sein de CEVITAL, en expliquant la configuration des différents protocoles et en réalisant des tests de validation pour s'assurer de l'atteinte de notre objectif.

Nous terminons avec une conclusion qui montre que l'implémentation de solutions de haute disponibilité et de virtualisation présente des avantages significatifs pour les entreprises afin q'elles peuvent garantir une disponibilité accrue de leurs systèmes et applications.

Chapitre 1

Généralités sur les réseaux et la sécurité informatique

1.1 Introduction

L'objectif de ce chapitre est de fournir un aperçu sur quelques concepts théoriques fondamentaux des réseaux informatiques et explorer leurs caractéristiques. Ensuite, nous examinerons le domaine de la sécurité des réseaux, en définissant ce terme et en présentant divers types d'attaques auxquelles les réseaux peuvent être confrontés. Enfin, nous aborderons différents mécanismes de sécurité avancés utilisés pour se protéger contre ces attaques.

Les réseaux informatiques

1.2 Définition des réseaux informatiques

Le réseau informatique est un ensemble d'équipements informatiques ou systèmes digitaux interconnectés entre eux à travers des médias d'accès vise à partager des données binaires issus d'applications ou de processus informatiques tels que les traitements de texte ou les navigateurs internet. En pratique, deux terminaux suffisent pour constituer un réseau informatique.

1.3 Types des réseaux informatiques

LAN (Local Area Network) : est un réseau privé qui relié des ordinateurs personnels et des équipements électroniques situés dans une zone géographique relativement restreinte tel qu'un bureau, un immeuble, un campus..., afin de leurs permettre d'échanger des informations et de partager des ressources. [1]

MAN (Metropolitan Area Network) : est un réseau qui connecte plusieurs réseaux locaux (LAN) entre eux. Il s'étend sur une zone géographique un plus grande telle qu'une ville (quelques dizaines de kilomètres) et il est plus petit que le réseau étendu (WAN). [1]

WAN (Wide Area Network) : est un réseau étendu qui couvre une zone géographique très importante (un pays, voire un continent). Le WAN connecte des LANs et des MANs et on trouve comme exemple Internet. [1]

1.4 Objectifs des réseaux

Il est intéressant de mettre en place un réseau informatique pour plusieurs principales raisons :

- Partage de ressources entre les utilisateurs en permettant de rendre accessible un ensemble de ressources (logiciels, bases de données, imprimantes...) indépendamment de la localisation géographique des utilisateurs.
- Augmentation de fiabilité pour limiter les pertes d'informations et dupliquer les données.
- Flexibilité de la manipulation qui donne à l'utilisateur l'accès de se connecter à un ordinateur n'importe où sur le réseau.
- Installer un système de messagerie électronique (e-mail) sur le réseau afin que tous les utilisateurs puissent envoyer et recevoir des messages, et bénéficier d'un canal de communication supplémentaire.
- Sauvegarde automatique des fichiers importants.

1.5 Architectures des réseaux

On distingue deux types d'architectures des réseaux informatique qui sont :

1.5.1 Poste à poste

Est un modèle de réseau informatique d'égal à égal entre ordinateurs d'où ils ont tous le rôle identique qui sont à la fois clients pour quelques ressources et des serveurs pour d'autres. En général, c'est un petit réseau de dizaine de postes sans un administrateur réseau. Il permet de distribuer et recevoir des données et des fichiers.

Avantages :

- Faible cout de mise en œuvre.
- Aucun système d'exploitation réseau requis.
- Administrateur réseau dédié.

Inconvénients :

- Moins sécurisé.
- Chaque utilisateur doit être formé sur les tâches administratives.
- Devient rapidement très complexe à gérer.

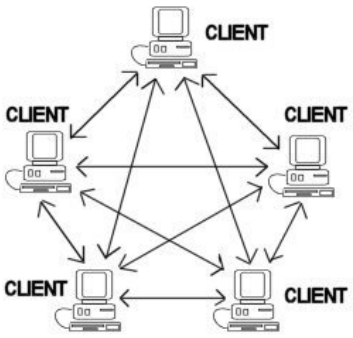


FIGURE 1.1 – L'architecture poste à poste.

1.5.2 Client/serveur

Un client est actif, il envoie des demandes au serveur, il attend à recevoir des réponses du serveur qui est initialement passif, il écoute et se prépare à répondre aux requêtes envoyées par les clients. Une fois qu'une requête lui parvient, il la traite et envoie une réponse. Ces deux éléments doivent utiliser le même protocole de communication. Un serveur est généralement capable de servir plusieurs clients en même temps. Une fois qu'un client est géré,le serveur peut en gérer un autre. Il existe des serveurs multi-clients comme les serveurs Web/http qui sont capables de gérer plusieurs clients en même temps. Il existe aussi des serveurs "non connectés", dans ce cas il n'y a pas de connexion ou de déconnexion.

Avantages :

- Les données sont centralisées sur un serveur unique, de sort qu'on a « une vérification de sécurité simplifié ».
- Les technologies prenant en charge l'architecture client/serveur sont plus mûres que les anciennes.

– L'administration va à l'échelle du serveur, toute la complexité/ puissance peut être déplacé vers les serveurs, les utilisateurs utilisant simplement un client léger.
– Etant donné que les serveurs sont centralisés, cette architecture est particulièrement adaptée et rapide pour trouver et comparer des grandes quantités d'informations (moteur de recherche sur le web).

Inconvénients :

– Avec l'augmentation de nombre des clients qui veulent établir une connexion avec un serveur simultanément, ce dernier risque un dépassement de charge contrairement au réseau P2P fonctionne mieux en ajoutant des nouveaux participants.
– La non-disponibilité du serveur mène à interrompre le fonctionnement des clients (le réseau P2P continue le fonctionnement, même les autres utilisateurs quittent le réseau).
– Un coût élevé pour mise en place de cette architecture et sa maintenance. En aucune circonstance les clients ne peuvent communiquer entre eux, ce qui donne lieu à une asymétrie de l'information en faveur des serveurs.

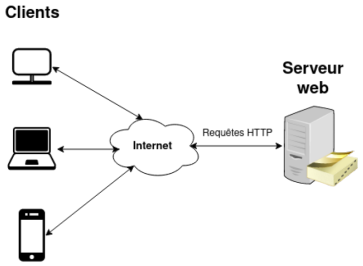


FIGURE 1.2 – L'architecture client serveur.

1.6 Topologie des réseaux

La topologie définit l'emplacement des équipements informatiques dans un réseau. Il existe deux types de topologie (physique et logique).

1.6.1 La topologie physique

Est relative au plan de réseau qui définit la façon dont les équipements sont interconnectés. Par conséquent, on trouve :

1.6.1.1 La topologie en bus

Est une topologie pour un réseau local (LAN) dans lequel tous les équipements sont reliés à un câble unique, ce dernier s'agit d'un support multipoints. Cette topologie a comme avantage qu'elle ne nécessite pas une grande quantité de câbles ainsi de points centraux. Par contre son majeur problème est du fait que si le câble est coupé, les stations ne pourront pas s'échanger des données sur le réseau [3].

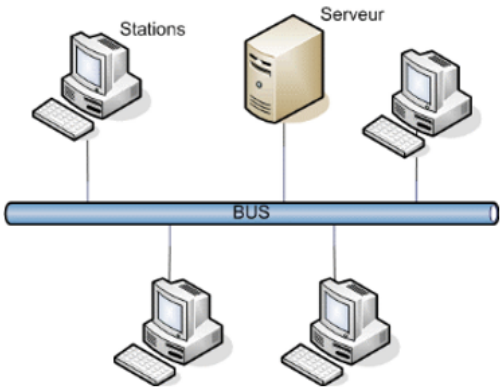


FIGURE 1.3 – La topologie en bus [2].

1.6.1.2 La topologie en étoile

Est une topologie pour un réseau local (LAN) dans lequel tous les stations sont connectées éventuellement à un point de connexion central (Hub et Switch). Elle nécessite plus de câble que celle en bus. Son principal avantage que si une station défectueuse n'affecte pas le fonctionnement le reste du réseau. Ce type de topologie est couteux et dépend du nœud central [3].

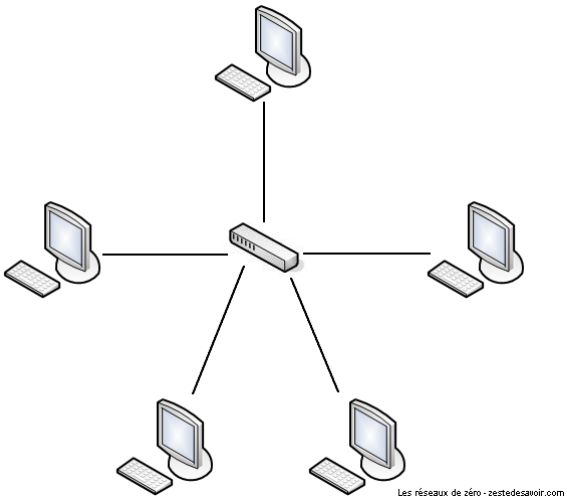


FIGURE 1.4 – La topologie en étoile [5].

1.6.1.3 La topologie en anneau

Est une topologie pour un réseau local (LAN) dont la communication repose sur une boucle fermée, constituée de liaisons point à point entre périphériques. Son mode de transmission se diffère à celui de topologie en étoile ou en bus, d'où la trame appelé jeton porte des informations sur les adresses et les données de l'émetteur, puis elle circule autour de l'anneau jusqu'à qu'elle s'arrête au destinataire. L'avantage de cette topologie qu'il n'y a pas de risques de collisions. Par contre si un câble ou un nœud est défaillant rompt la boucle et l'anneau sera défectueux [3].

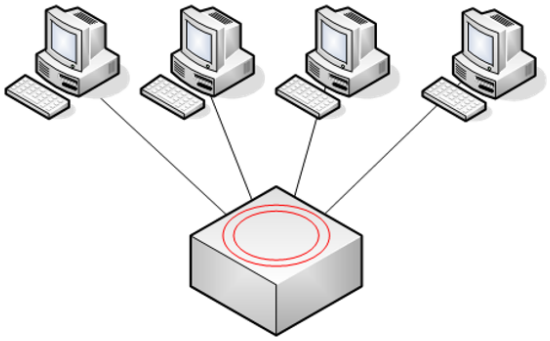


FIGURE 1.5 – La topologie en anneau [4].

1.6.1.4 La topologie maillée

Est une topologie pour un réseau étendu (WAN) dont tous les hôtes sont connectées paire à paire sans hiérarchie centrale qui utilise plusieurs chemins de transmissions entre différents périphériques, d'où chacun doit envoyer, recevoir et relier des données. Cette topologie est fiable et robuste car la défaillance d'une liaison n'indique pas la panne d'un réseau. D'autre part, le nombre de fils nécessaire pour connecter chaque système est énorme.[6]

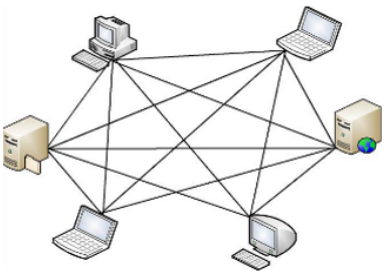


FIGURE 1.6 – La topologie en maillé.[6]

1.6.1.5 La topologie en arbre

Appelée topologie arborescente ou hiérarchique. Elle est considérée comme un ensemble de réseaux en étoile organisés hiérarchiquement[8]. Le réseau est divisé en plusieurs niveaux. Le niveau supérieur se connecte à plusieurs nœuds de niveau inférieur. Ce type de topologie est apprécié pour son évolutivité et son accessibilité pour le dépannage. Son inconvénient est qu'un système entier peut être paralysé par dysfonctionnement d'un nœud principal. Cette topologie ce divise en plusieurs couches [7] :

Couche d'accès : c'est le point d'entré qui permet aux groupes de travail et aux utilisateurs d'accéder au réseau. Elle assure l'accès au réseau de l'entreprise en utilisant des technologies WAN. Cette couche comporte des Switchs de niveau 2 qui fournissent des services de connectivité aux différents équipements : PC, Serveurs, Point d'accès,etc [7].

Couche distribution : fournit la connectivité basée sur des stratégies et des règles ou politiques d'accès. La couche distribution comporte des routeurs ou des Switchs de niveau 3 pour assurer la segmentation du réseau et limiter les domaines de diffusion [7].

Couche cœur réseau : C'est la couche dorsale ou backbone du réseau. Elle comporte des équipements de hautes performances. Elle est conçue pour assurer le transport rapide des paquets et interconnecter les différents composants de l'infrastructure : Les modules de la couche distribution, modules de service, Data Center, Sites distants (WAN) [7].

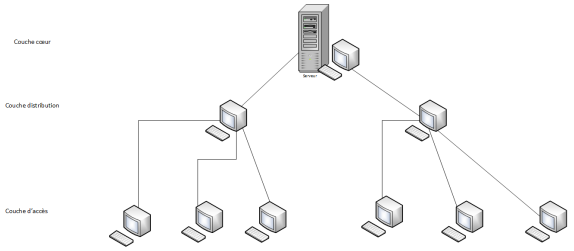


FIGURE 1.7 – La topologie en arbre. [8]

1.6.2 La topologie logique

La topologie logique représente le chemin emprunté. Elle désigne la manière dont un réseau transfère les trames d'un nœud à l'autre. Cette configuration est composée de connexions virtuelles entre les nœuds d'un réseau. Ces chemins de signaux logiques sont définis par les protocoles de couche liaison de données. La topologie logique des liaisons point à point est relativement simple tandis que les supports partagés proposent des méthodes de contrôle d'accès au support déterministes et non déterministes.

1.7 Les modèles des réseaux

On distingue deux grandes familles d'architecture de réseau :

1.7.1 Modèle OSI

Le modèle OSI (Open System Interconnexion) est un modèle conceptuel créé par l'ISO (International Standard Organisation), il repose sur l'empilement de sept couches pouvant de se communiquer verticalement, chaque couche assure un rôle particulier. Ce modèle permet à divers systèmes de s'échanger des données à l'aide des protocoles standards [9].

1.7.2 Modèle TCP/IP

Le modèle définit par la défense américaine (DOD), pour but de connecter plusieurs réseaux utilisant des protocoles de communication différents et incompatibles. Il représente un ensemble de règles de communication sur internet et se base sur la notion d'adressage IP, en fournissant une adresse IP a chaque machine de réseau afin de pouvoir acheminer des paquets de données [9].

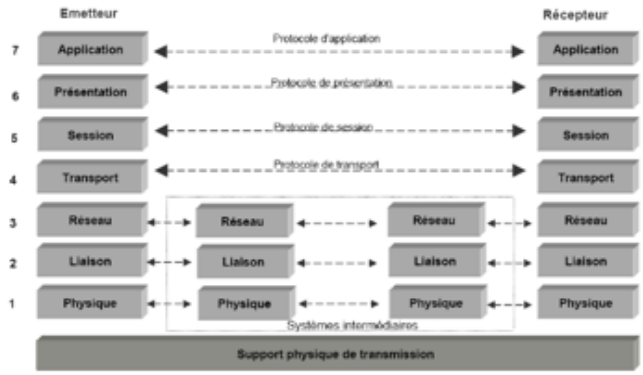


FIGURE 1.8 – Modèle OSI [9].

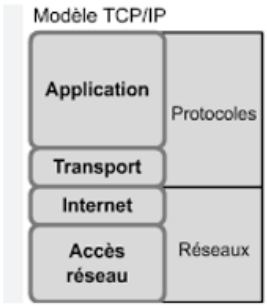


FIGURE 1.9 – modèle TCP/ IP [9].

1.8 Routage

Le routage est un processus qui permet de transmettre les données entre les différents appareils d'un réseau informatique, tels que les ordinateurs les commutateurs, les routeurs, etc, entre des réseaux différents. Il implique l'utilisation de protocoles de routage pour déterminer la meilleure route à emprunter par les données afin d'arriver à la destination [10].

Le routage est une étape cruciale dans la mise en réseau, notamment sur Internet, car il permet de connecter des réseaux distincts et de faire passer les données d'un réseau à un autre. Lorsqu'un appareil dans un réseau envoie des données à un autre appareil situé dans un réseau différent, les données sont divisées en paquets et acheminées à travers les appareils de routage le long du chemin le plus efficace jusqu'à ce qu'ils atteignent leur destination [10].

Sécurité informatique

1.9 Définition de la sécurité

La sécurité informatique est l'ensemble de moyens mis en œuvre pour éviter et/ou minimiser les défaillances naturelles dues à l'environnement ou au défaut du système d'informations et les attaques malveillantes intentionnelles dont les conséquences sont catastrophiques. La sécurité d'un réseau est un niveau de garantie que les ordinateurs du réseau fonctionnent de façon optimale et que les utilisateurs possèdent uniquement les droits qui leurs ont été octroyés.

1.10 Les objectifs de la sécurité

La sécurité informatique a pour objectif de s'assurer que les ressources matérielles ou logicielles d'une entreprise sont uniquement utilisées par les personnes autorisées. Elle vise généralement à préserver cinq principaux services de sécurité [11] :

- **La confidentialité** : est le principe que l'information n'appartient pas à tout le monde et que les personnes autorisées ont le droit d'y accéder, en empêchant de divulguer l'information aux non-autorisées et de la lire. Les services utilisés pour garantir cet objectif sont le chiffrement et le contrôle d'accès.
- **L'authentification** : consiste à limiter l'accès aux personnes autorisées, et de vérifier que le message provient de la source réelle du message. Les techniques utilisées pour assurer cet objectif : un mot de passe, une carte à puce et une empreinte digitale.
- **L'intégrité** : ce service consiste à assurer que les données transmises n'ont pas été altérées, c'est-à-dire garantir que le message reçu est bien celui qui a été envoyé, et qu'il n'a pas été modifié ou fabriqué. Parmi les mécanismes utilisés, on trouve le chiffrement, la signature numérique, le contrôle d'accès et le contrôle d'intégrité.
- **La non-répudiation** : permet de garantir l'identité des deux parties autrement dit vérifier que l'émetteur et le récepteur sont bien les parties qui ont respectivement envoyé ou reçu le message. Cela se fait par le biais de certificats numériques grâce à une clé privée. [5]
- **La disponibilité** : permet de maintenir le bon fonctionnement du système en fournissant de l'information aux personnes autorisées aux moments où elles en ont besoin, grâce aux mécanismes de sauvegarde et de partage de charge.

1.11 Terminologie de la sécurité informatique

La terminologie de sécurité informatique comprend un ensemble de termes et d'expressions utilisés dans le domaine de la sécurité informatique. Voici quelques termes les plus fréquents :

La vulnérabilité : désigne toute faiblesse d'un système informatique, telle qu'une application Web, qui permettrait à une personne potentiellement malveillante d'altérer le fonctionnement normal du système ou d'accéder à des données non autorisées.

Les menaces : sont susceptibles de traduire les vulnérabilités en attaques contre les systèmes informatiques, les réseaux, etc. Ils peuvent compromettre les systèmes informatiques personnels ainsi que les ordinateurs professionnels, de sorte que les vulnérabilités

doivent être corrigées afin que les attaquants ne puissent pas pénétrer dans le système et causer des dommages.

Les contre-mesures : sont des actions ou des méthodes utilisées pour prévenir, éviter ou réduire les menaces potentielles contre les ordinateurs, les serveurs, les réseaux, les systèmes d'exploitation (OS) ou les systèmes d'information (IS). Les outils de contre-mesure comprennent un logiciel antivirus et des pares-feux.

1.12 Les causes de l'insécurité

L'insécurité informatique peut avoir de nombreuses causes. Voici les plus courantes [12] :

1. Les attaques de logiciels malveillants : Les logiciels malveillants (tels que les virus, les vers, les chevaux de Troie, les ransomwares, etc.) peuvent infecter un système informatique et causer des dommages importants
2. Les vulnérabilités de logiciels et systèmes d'exploitation : Les vulnérabilités peuvent permettre aux cybercriminels d'exploiter les faiblesses des logiciels et des systèmes d'exploitation pour accéder aux données sensibles.
3. Le manque de mises à jour de sécurité : Les mises à jour de sécurité sont essentielles pour protéger les systèmes informatiques contre les vulnérabilités connues. Si les mises à jour ne sont pas effectuées régulièrement, les systèmes peuvent devenir vulnérables aux attaques.
4. Les erreurs humaines : Les erreurs humaines, telles que l'utilisation de mots de passe faibles ou le partage de données sensibles, peuvent contribuer à l'insécurité informatique.
5. L'ingénierie sociale : Les cybercriminels peuvent utiliser des techniques d'ingénierie sociale pour tromper les utilisateurs et obtenir des informations sensibles, telles que des identifiants de connexion ou des informations bancaires.

1.13 Les attaques informatiques

Une attaque informatique est une tentative d'accès non autorisée à un système ou un réseau informatique. Elle vise à désactiver, perturber ou contrôler des réseaux informatiques ou à modifier, supprimer, manipuler ou voler les données circulées dans ces réseaux. On peut classifier les attaques en deux classes principales : les attaques passives et les attaques actives.

1.13.1 Un logiciel malveillant

Est un type de programme ou logiciel conçue pour exploiter ou endommager un ordinateur ou un réseau informatique, sans que les utilisateurs finaux s'en aperçoivent. Et parmi ces programmes on trouve :

— Un virus : est un programme malveillant qui se propage dans des ordinateurs afin de perturber le bon fonctionnement et la destruction de ses ressources comme la mémoire et le disque dur.

— Un ver : est un type de logiciel malveillant qui a la particularité de circuler d'un ordinateur à un autre à l'aide d'une connexion réseau en utilisant des ressources du réseau.

— Un cheval de Troie : la catégorie de logiciels malveillants la plus fréquente, utilisée pour prendre le contrôle de l'appareil affecté, exfiltrer les données utilisateur et les envoyer à l'attaquant, télécharger et exécuter d'autres logiciels malveillants sur le système affecté [13].

1.13.2 Attaques de reconnaissance

Est la découverte non autorisée de systèmes, de leurs adresses et de leurs services ou encore la découverte de leurs vulnérabilités. Il s'agit d'une collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque [13].

1.13.3 Attaques d'accès

L'accès au système est la possibilité pour un intrus d'accéder à un périphérique pour lequel il ne dispose pas d'un compte ou d'un mot de passe. Les attaques d'accès exploitent des vulnérabilités connues dans les services d'authentification, les services FTP et les services Web.

1.13.4 Attaques par déni de service

Est la forme d'attaque la plus répandue et aussi la plus difficile à éliminer. Elle vise à rendre un ordinateur indisponible pour ses utilisateurs prévus en interrompant le fonctionnement normal de la machine. Une attaque DoS se caractérise par l'utilisation d'un seul ordinateur pour lancer l'attaque. [13]

1.14 L'effet d'une attaque

Dans le domaine de la sécurité informatique, une attaque peut avoir des conséquences importantes sur les systèmes, les données et les utilisateurs concernés. On distingue deux catégories :

1.14.1 Attaque active

Une attaque active est une attaque dans laquelle l'attaquant tente de modifier des informations ou de créer de fausses nouvelles. La prévention de ces attaques est difficile en raison des nombreuses vulnérabilités physiques, réseau et logicielles. Plutôt que la prévention, il met l'accent sur la détection des attaques et la récupération de toute perturbation ou retard causé par celles-ci. Les attaques actives nécessitent généralement plus d'efforts et sont souvent plus dangereuses, lorsque l'agresseur essaie d'attaquer. Les attaques actives prennent la forme d'interruption, de modification et de fabrication.

– Une interruption d'où un attaquant non autorisé essayant de se faire passer pour une autre entité.

– La modification implique l'édition du message d'origine dans une autre manière différente.
– La fabrication peut conduire à une attaque par déni de service (DOS), dans laquelle un attaquant tente d'empêcher les utilisateurs d'accéder à certains services.

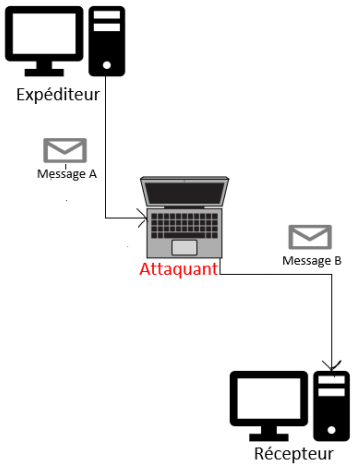


FIGURE 1.10 – Une attaque active

1.14.2 Attaque passive

Une attaque passive est une attaque dans laquelle l'attaquant écoute et surveille simplement la transmission ou la collecte d'informations. Les indiscrets n'apporteront aucune modification aux données ou aux systèmes. Les attaques passives sont difficiles à détecter car elles n'impliquent pas de modification des données ou des ressources système. Par conséquent, l'entité attaquée n'a aucune idée de l'attaque. Cependant, cela peut être évité en utilisant des méthodes de cryptage où les données sont d'abord codées dans une langue inintelligible du côté de l'expéditeur, puis reconverties en langage humain compréhensible du côté du destinataire.

FIGURE 1.11 – Une attaque passive

1.15 Les mécanismes de sécurité

La sécurité du réseau permet la communication assurée d'un système à l'autre, tant que sa sécurité se base sur des mécanismes qu'évitent les intrusions. Un tel mécanisme : mot de passe qui protège contre les intrusions à partir d'un réseau, ainsi d'autres méthodes de sécurité matérielle et biométrie.

1.15.1 L'antivirus

Un logiciel antivirus est un logiciel qui détecte les virus informatiques, les détruit, supprime aussi répare les fichiers infectés sans les endommager. Ils utilisent un certain nombre de techniques pour cela, notamment :

- Contrôle global des systèmes informatiques.
- Surveiller les lecteurs de médias amovibles, il est généralement recommandé d'utiliser un logiciel antivirus sous licence de tenir à jour, car cela permet la correction des défauts détectés par l'utilisateur ou par les concepteurs de ces systèmes d'information [14].

1.15.2 Le cryptage

Le chiffrement est un processus de cryptage par lequel le document soit incompréhensible pour quiconque sans la clé de cryptage (déchiffrée). Ce principe est souvent associé au principe d'accès conditionnel. Alors que le chiffrement peut garder la signification des documents privés, d'autres chiffrements sont nécessaires pour communiquer en toute sécurité [15].

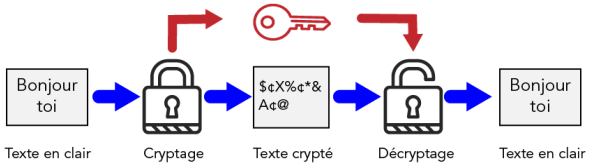


FIGURE 1.12 – La technique de cryptage[15].

1.15.3 Le pare-feu

Il s'agit d'un ensemble de différents composants matériels (physiques) et logiciels (logiques) qui contrôlent le trafic interne/externe conformément aux politiques de sécurité. Les règles de filtrage indiquant les adresses IP pour lesquelles il est autorisé, le système de pare-feu fonctionne la plupart du temps et constitue donc une passerelle de filtrage. Communiquant avec les machines sur le réseau, il permet d'une part d'empêcher les attaques ou les connexions suspectes d'accéder au réseau interne. D'autre part, dans de nombreux cas, les pares-feux sont également utilisés pour empêcher la fuite incontrôlée d'informations vers l'extérieur. Il offre un véritable contrôle sur le trafic du réseau d'entreprise afin qu'il puisse être analysé, sécurisé et géré[14].

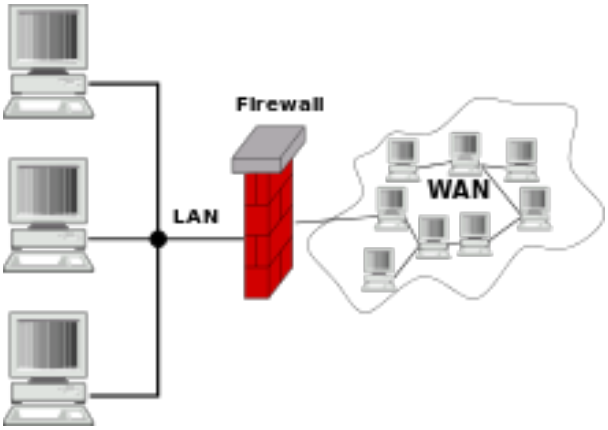


FIGURE 1.13 – Le pare-feu [16].

1.15.4 Le proxy

Les agents de proxy fonctionnent au niveau de l'application. Il est utilisé comme mandataire par des machines présentes sur le réseau, n'ayant pas un accès direct à l'extérieur et souhaitant s'y connecter pour une application donnée. Pour les routeurs, le nom du serveur proxy doit être configuré sur le poste client pour chaque type d'application. Ensuite, il peut s'agir de HTTP, FTP, proxy ARP. Cependant, des options lui sont généralement associées, en voici quelques-unes :

Proxy-Cache qui est une mémoire installée sur un proxy lui permet de conserver dans sa propre mémoire le contenu des requêtes qu'il a faites.

Proxy-Authentification permet de ne donner accès à Internet qu'à certaines personnes autorisées auxquelles sont attribués des identifiants et des mots de passe.

Proxy anonyme utilisé pour permettre la protection de la vie privée. En fait, lorsqu'une connexion Internet se produit, des informations sur le système sont fournies au site Web. Les informations peuvent ensuite être utilisées pour suivre les déplacements des internautes. Pour éviter de dévoiler sa vie privée.

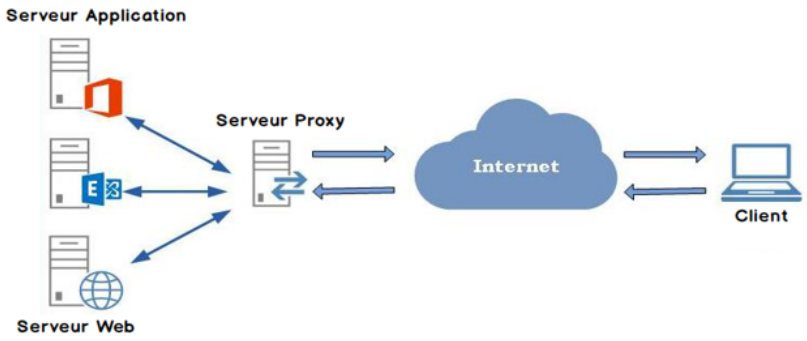


FIGURE 1.14 – Le proxy [17].

1.15.5 Système de détection d'intrusion (IDS)

Intrusion Detection System IDS (ou IDS : Intrusion Detection System) est un mécanisme destiné à détecter une activité anormale ou suspecte sur une cible d'analyse (réseau ou hôte). Par conséquent, il peut connaître les tentatives d'intrusion réussies et échouées. Deux aspects du fonctionnement de l'IDS doivent être distingués : les modes utilisés et les réponses apportées par l'IDS lorsqu'une intrusion est détectée. Les IDS se classifier selon la cible qu'ils vont surveiller, les systèmes de détection d'intrusion réseau et les systèmes de détection d'intrusion hôte [14].

1.15.6 Un système de prévention des intrusions (IPS)

Un système de prévention des intrusions (ou IPS, Intrusion Prevention System) est un outil similaire à un IDS, sauf que le système prend des mesures pour réduire Risque d'impact d'attaque. C'est un IDS actif qui détecte que l'IPS peut automatiquement bloquer l'auto scan du port.

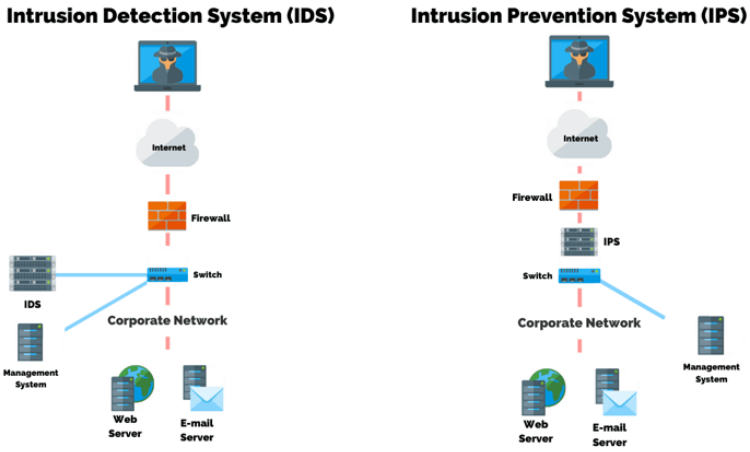


FIGURE 1.15 – La technique de l'IPS et l'IDS [18]

1.15.7 Les VPN

Un réseau privé virtuel en anglais Virtual Private Network, VPN en abrégé dans des réseaux informatiques est considéré comme une extension d'un réseau local, qui prend en charge la sécurité du réseau. Il correspond en fait à l'interconnexion des réseaux locaux grâce à la technologie du tunneling.

Lorsqu'une organisation interconnecte ses sites via une infrastructure partagée avec d'autres organisations, on appelle cela un VPN, il comprend deux types de ces infrastructures partagées : les infrastructures « publiques » (comme internet) et les infrastructures privées établies par les opérateurs pour fournir des services VPN aux entreprises. La technologie « Tunnel » est développée sur Internet et IP.

FIGURE 1.16 – La sécurité par la mise d'un VPN

1.15.8 Les VLANs

Virtual Local Networks sont des réseaux locaux virtuels qui permettent de diviser un réseau physique en plusieurs sous-réseaux logiques. Les VLANs sont créés en regroupant des ports de commutation réseau en fonction de critères tels que le département, la fonction ou l'emplacement géographiques des utilisateurs. Les avantages des VLANs incluent :

- Sécurité : les VLANs peuvent isoler les flux de données pour éviter que les utilisateurs non autorisés ne puissent accéder aux informations.
- Gestion de la bande passante : Les VLANs peuvent segmenter le trafic en groupes logiques, permettant aux administrateurs réseaux de mieux contrôler la bande passante allouée à chaque groupe.
- Flexibilité : Les VLANs permettent aux administrateurs de réorganiser facilement les ports de commutation sans avoir à modifier la configuration physique de leur réseau.

Il existe plusieurs types de VLAN, tels que les VLANs basés sur le port, les VLANs basés sur le protocole, les VLANs basés sur la couche réseau et autres sur la couche applicative. Les VLANs sont largement utilisés dans les entreprises pour améliorer la sécurité et la gestion du réseau. [10]

1.15.9 La DMZ

Appelée aussi une zone démilitarisée qui est un sous réseau qui se situe entre l'internet public et les réseaux privés, afin de protéger les réseaux locaux internes contre le trafic non sécurisé. Son principal rôle est de permettre à une organisation d'accéder à des sites non sécurisés, tels qu'Internet, tout en garantissant la sécurité de son réseau local et privé.

Les réseaux DMZ sont essentiels à la sécurisation des réseaux d'entreprise depuis la création des pares-feux. Ils protègent les données, les systèmes et les ressources sensibles des entreprises en maintenant les réseaux internes séparés des systèmes qui pourraient être la cible d'assaillants. Les DMZ permettent également aux entreprises de contrôler et de réduire les niveaux d'accès aux systèmes sensibles.

1.16 Conclusion

En conclusion, ce chapitre sur les réseaux et la sécurité informatique souligne l'importance cruciale de ces domaines dans le contexte technologique actuel. Assurer La protection des réseaux et des données est un défi permanent et en constante évolution, qui

nécessite une compréhension approfondie des concepts, des techniques et des meilleures pratiques en matière de sécurité telles que le cryptage et la sauvegarde régulière de données de l'entreprise. Grâce à la connaissance de ces deux piliers fondamentaux de l'informatique, il est possible de développer des stratégies efficaces pour prévenir les attaques, protéger les informations sensibles de l'entreprise et assurer un fonctionnement sécurisé de son réseau informatique.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

CEVITAL est l'une des entreprises algériennes d'industrie agro-alimentaire qui ont vu le jour dès l'entrée de notre pays en économie de marché en 1998. Elle se constitue de plusieurs unités de production telles que : raffinerie d'huile, raffinerie de sucre, margarinerie, unité de conditionnement d'eau minérale, unité de fabrication et de conditionnement de boisson rafraichissante, conserverie, silos portuaires ainsi qu'un terminal de déchargement portuaire. Dans ce chapitre nous présentons sans la première note l'organisme CEVITAL en exposant ses différentes ressources physiques et organisationnelles et dans la deuxième partie, nous allons citer les problèmes rencontrés dans cette entreprise afin de proposer des solutions sur lesquelles tournera notre mémoire.

Présentation de l'entreprise

2.2 Les valeurs du Groupe CEVITAL

Les quatre règles de valeur (IRIS) à respecter à l'intérieure de l'entreprise [19] :

— **Initiative** : L'employé utilise ses connaissances sur le terrain pour anticiper les problèmes potentiels et proposer des solutions innovantes.

— **Respect** : Le principe de respect doit prévaloir entre collègues et dans les interactions avec partenaires internes et externes.

— **Intégrité** : C'est une valeur fondamentale qui impose aux collaborateurs d'adopter une éthique professionnelle irréprochable.

— **La solidarité** : est également cruciale, car les employés doivent se soutenir mutuellement, partager leurs connaissances et leur expérience et travailler ensemble vers des objectifs communs.

Dans l'ensemble, ces valeurs favorisent une culture d'intégrité, de professionnalisme et de collaboration au sein de l'organisation.

2.3 Situation géographique

Le complexe agro-industrie CEVITAL s'étends sur 45 000 mètres carrés et est considéré comme le plus grand complexe privé d'Algérie, il est situé à la proximité de nouveau quai du port de Bejaia, à proximité de la route nationale N° 09 et N°26 ; Le complexe a été construit sur un terrain auparavant inhabitable qui a été récupéré et rendu viable grâce à l'utilisation de la dernière technologie de consolidation des sols utilisant des colonnes lestées (337 km de colonnes ballastées de 18M chacune ont été réalisées) ainsi qu'une partie à gagner sur la mer. L'entreprise a beaucoup bénéficié de cette situation qui lui donne un avantage de proximité économique car se trouve proche du port et de l'aéroport.

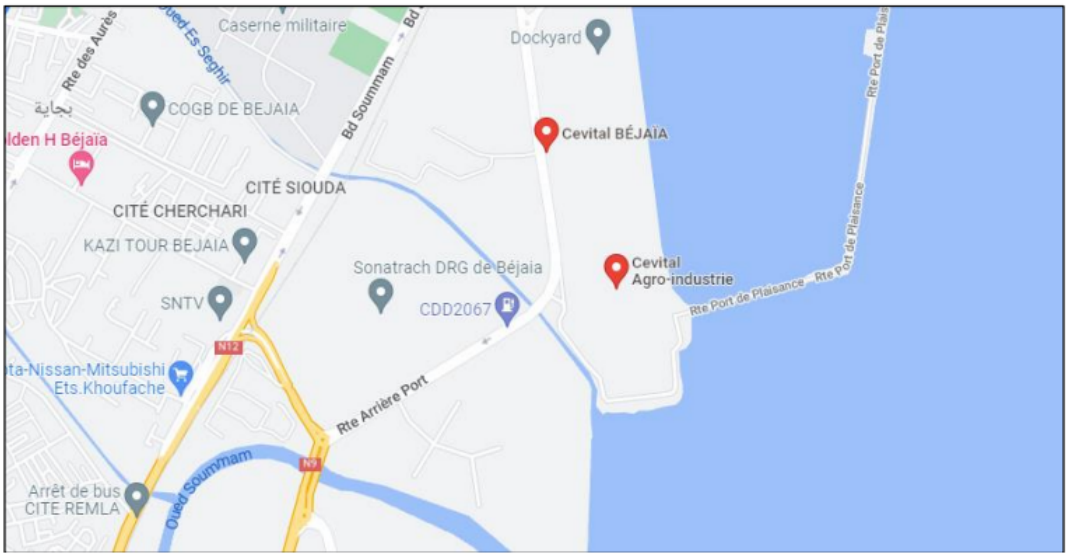


FIGURE 2.1 – Localisation de l'entreprise CEVITAL

2.4 Organigramme général de CEVITAL

Le schéma ci-dessous représente l'organigramme de CEVITAL, qui est constitué de plusieurs directions principales, neuf directions chaque un est responsable afin d'assurer de l'exécution de ses tâches pour garantir le bon fonctionnement de l'ensemble du complexe CEVITAL.

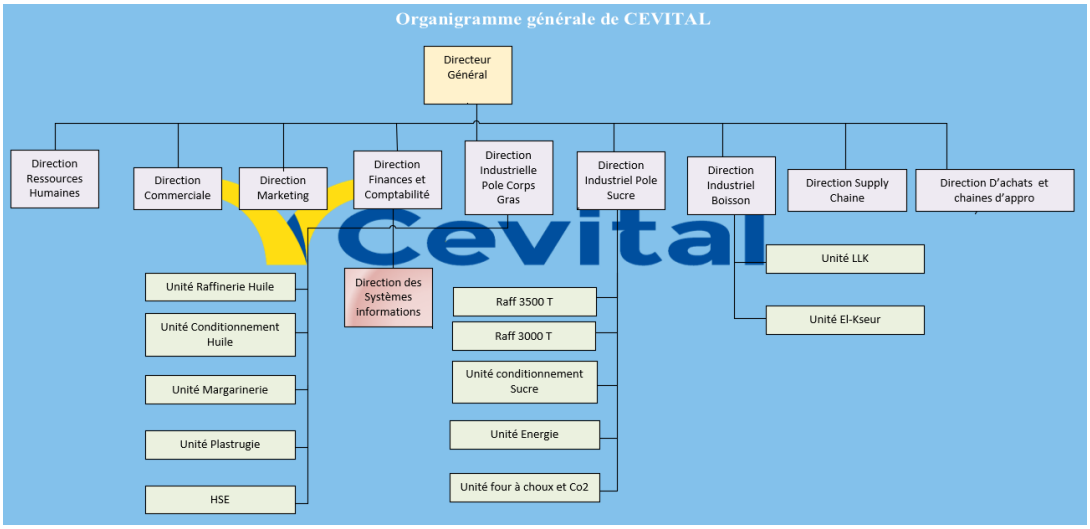


FIGURE 2.2 – L'organigramme générale de l'entreprise CEVITAL [19].

2.5 Le rôle de différentes directions de l'entreprise CEVITAL

2.5.1 La direction Système d'informations

Elle assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise. Présentation de L'organisme d'accueil Elle doit ainsi veiller à la cohérence des moyens informatiques et de communication mis à la disposition des utilisateurs, à leur mise à niveau, à leur maîtrise technique et à leur disponibilité et opérationnalité Elle définit, également, dans le cadre des plans pluriannuels les évolutions nécessaires en fonction des objectifs de l'entreprise et des nouvelles technologies.

2.5.2 La direction des Finances

Le rôle de cette direction est de préparer et mettre à jour les budgets, tenir la comptabilité et préparer les états comptables et financiers selon les normes et pratiquer le contrôle de gestion.

2.5.3 La direction commerciale

Elle a en charge de commercialiser toutes les gammes des produits et le développement du Fichier clients de l'entreprise, au moyen d'actions de détection ou de promotion de projets à base de hautes technologies. En relation directe avec la clientèle, elle possède des qualités relationnelles pour susciter l'intérêt des prospects.

2.5.4 La direction des Ressources Humaines

Cette direction a pour rôle de définir et proposer à la direction générale les principes de Gestion ressources humaines en support avec les objectifs du business. Elle assure le recrutement et la gestion des carrières. Elle se charge de la formation du personnel et participe avec la direction générale à l'élaboration de la politique de communication afin de développer l'adhésion du personnel aux objectifs fixés par l'organisation.

2.6 L'organigramme de service informatique

Le stage a été effectué au sein du département Réseau et Télécom de la direction des systèmes d'information (DSI), dont la mission consiste à mettre en place les outils et technologies informatiques nécessaires pour améliorer l'activité, la stratégie et la performance de l'entreprise. La DSI doit garantir la cohérence et la disponibilité des moyens de communication et informatiques, ainsi que leur maîtrise technique et leur sécurité. La figure suivante présente l'organigramme du système d'information.

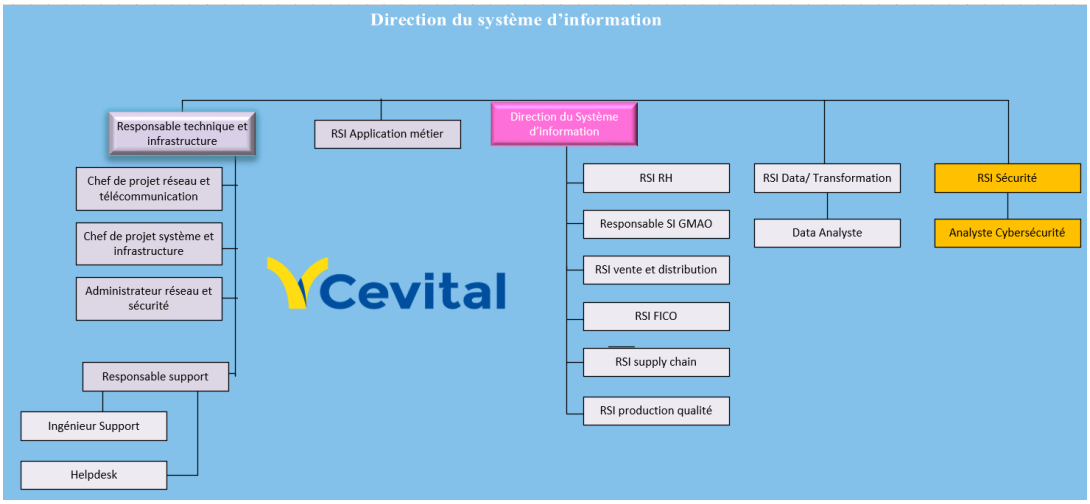


FIGURE 2.3 – L'organigramme de département DSI de CEVITAL [19].

2.7 Le matériel informatique de l'entreprise CEVITAL

Le réseau est composé de plusieurs dispositifs dont la plupart sont de marque Cisco (Switch Catalyst, Routeur) interconnectés entre eux grâce à la fibre optique, ou paire de cuivre torsadée.

2.7.1 Switch d'accès de type Cisco Catalyst 2960-X et 9200

Un commutateurs Ethernet à configuration fixe, qui fournit aux postes de travail une connectivité Fast Ethernet et Gigabit Ethernet et permet la mise en œuvre de services LAN avancés au sein des réseaux d'entreprise et des réseaux d'agences.

FIGURE 2.4 – Commutateur 2600-X [20].

FIGURE 2.5 – Commutateur 9200 [20].

2.7.2 Switch cœur de type Cisco 6800

Le commutateur central est un commutateur reliant les commutateurs d'accès, les pares-feux, les serveurs et les routeurs du réseau de CEVITAL. Il est d'une grande capacité placée habituellement au cœur physique du réseau ou du cœur de réseau. Il fonctionne

comme une porte d'entrée au réseau étendu (WAN) ou à Internet en constituant le point de convergence final du réseau et en permettant à plusieurs modules d'agrégation de travailler ensemble ainsi il s'occupe du routage inter-Vlan (Virtuel Lan).

FIGURE 2.6 – Commutateur cœur Cisco 6800 [20].

2.7.3 Routeur de type Cisco 1900

Tous les routeurs de la gamme à services intégrés Cisco 1900 intègrent l'accélération matérielle des fonctions de chiffrement, des slots pour DSP compatibles voix et vidéo, un pare-feu facultatif, la prévention des intrusions, le traitement des appels, la messagerie vocale et des services d'applications. En outre, ces plates-formes prennent en charge l'éventail le plus complet du marché en termes de connectivité filaire et sans fil, telles que T1/E1, T3/E3, xDSL et Gigabit Ethernet cuivre ou fibres optiques.

FIGURE 2.7 – Routeur 1900 [20].

2.7.4 Le pare-feu FortiGate (601E)

Le pare-feu peut protéger tout le trafic réseau et est capable d'identifier et d'empêcher le trafic indésirable. Une version reformulée possible pourrait être : "Le pare-feu offre une protection complète du trafic réseau, car il peut détecter et empêcher toute communication indésirable." Le pare-feu FortiGate se caractérise par sa protection contre les menaces de sécurité, il utilise une combinaison de technologies de sécurité telles que l'inspection des paquets, la détection et la prévention d'intrusion, le filtrage web ainsi l'analyse de contenu pour empêcher les cyberattaques et les menaces qui cause le WAN.

2.7.5 Data Center

"Data Center" en français "centre de données", est une infrastructure physique ou logique qui sert à stocker, traiter, diffuser les données numériques. Le data center est

FIGURE 2.8 – Le pare-feu fortigate [20].

adopté dans les entreprises afin d'héberger leurs serveurs, sites web, applications, etc. Il est utilisé dans le but de garantir une disponibilité de données et la sécurité des systèmes informatiques qu'il héberge.

FIGURE 2.9 – Centre de données [20].

2.8 VLAN de l'entreprise

Nom du VLAN	Id du VLAN	Adress ip	masque	passerelle
RH	Vlan100	10.1.100.0	255.255.255.0	10.1.100.1
Marketing	Vlan101	10.1.101.0	255.255.255.0	10.1.101.1
DSI	Vlan102	10.1.102.0	255.255.255.0	10.1.102.1
Manager	Vlan103	10.1.103.0	255.255.255.0	10.1.103.1
Serveur	Vlan104	10.1.104.0	255.255.255.0	10.1.104.1
Voice	Vlan105	10.1.105.0	255.255.255.0	10.1.105.1
PROD1	Vlan200	172.16.200.0	255.255.255.0	172.16.200.1
PROD2	Vlan201	172.16.201.0	255.255.255.0	172.16.201.1

TABLE 2.1 – Plan d'adressage IPv4 [19]

2.9 L'architecture de l'entreprise CEVITAL

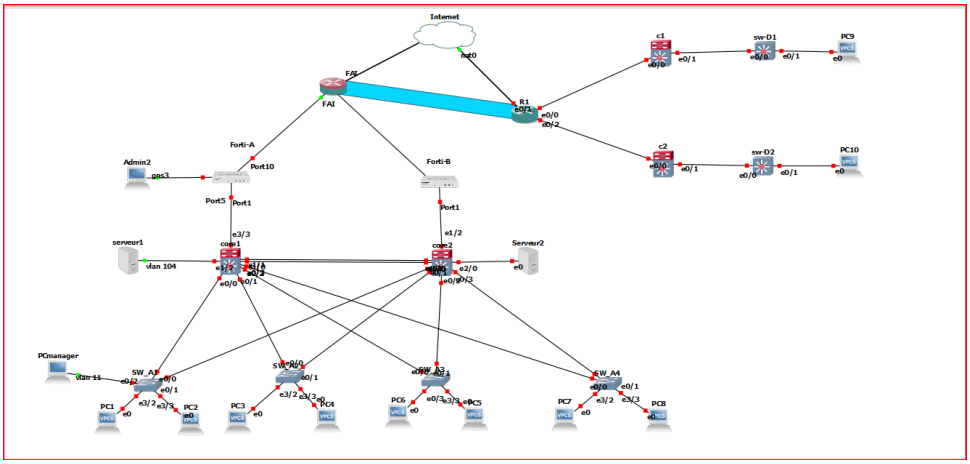


FIGURE 2.10 – L'architcture de l'entreprise CEVITAL[19].

2.10 Problématique et solutions proposées

2.10.1 Problématique

Après avoir étudier l'état de réseau de notre entreprise d'accueil CEVITAL, nous avons soulevé les problèmes suivants :

• L'entreprise CEVITAL est exposée à des risques tels que la vulnérabilité de la sécurité qui causera une interruption avec un temps d'arrêt prolongé en provoquant l'indisponibilité de systèmes.

• Chaque équipement physique de sauvegarde est en risque de défaillance alors la récupération de ses données est presque impossible sauf si on bascule sur une autre solution matérielle qui entraine des coûts élevés.

2.10.2 Solutions Proposées

Afin de remédier au premier problème cité dans la problématique, nous proposons de mettre en œuvre un ensemble de solutions de la haute disponibilité afin d'assurer la continuité du système et en minimisant le temps d'arrêt. Pour cela on doit inclure :

1. La redondance des serveurs de secours pour assurer la reprise automatique de système en cas de panne de serveur principal.
2. La mise en place d'une solution tolérente aux pannes au niveau des pares-feux en synchronisant ses règles afin d'améliorer leurs fonctionnement.
3. L'activation du basculement automatique au niveau des serveurs afin d'éviter un temps d'arrêt élevé.
4. La réplication des données qui assure la disponibilité de données en cas de défaillance de serveur principal.

Pour le deuxième problème nous mettons en disposition la virtualisation qui a pour but d'optimiser les ressources matérielles et de faciliter la gestion, nous proposons :

1. Intégrer un logiciel virtuel afin d'optimiser notre solution de la haute disponibilité.

2.10.3 Objectifs

Les configurations que nous sommes sur le point de mettre en place doivent utiliser différents processus liés au réseau LAN du client ainsi en rajoutant les outils fonctionnels afin d'optimiser le réseau existant, le futur système doit répondre aux critères suivants :

1. Assurer la haute disponibilité des services et de données.
2. Utiliser les différents protocoles de sécurité afin d'atteindre ses objectifs.
3. Réduire les risques de conflits ou d'interférences entre les différents logiciels et applications.
4. Réduire le coût, la consommation d'énergie en consolidant plusieurs serveurs physiques en une seule machine physique.

2.11 Conclusion

La première partie de ce chapitre nous a permis de bien comprendre less divers services offerts par l'entreprise CEVITAL et parmi eux le service direction de système information où nous avons effectué notre stage pratique, qui est le noyau des services de l'entreprise. Nous avons affiné notre sujet en identifiant les deux problématique remarquées au niveau de cette entreprise puis nous avons proposé des solutions aux problématiques qui se focalise sur la mise en place de la haute disponibilité et de la virtualisation de l'infrastructure.

Chapitre 3

La haute disponibilité

3.1 Introduction

La haute disponibilité d'un système informatique désigne un ensemble d'actions et de mesures prises en cas de défaillances matérielles et logicielles qui peuvent causer un ralentissement ou un arrêt de la productivité et de l'activité de l'entreprise.

Ce chapitre présente les différentes stratégies et solutions de la haute disponibilité telles que la redondance des composants, le clustering, la répartition de charge et le basculement automatique qui servent à éviter les pertes de productivité financière et les failles de sécurité afin de garantir une disponibilité maximale de services pour les utilisateurs de l'entreprise.

3.2 Nécessité de haute disponibilité

La haute disponibilité informatique est une notion importante pour assurer la performance de des entreprises. En fait, la numérisation augmente la productivité des employés, ce qui améliore les performances de l'entreprise. Si le système informatique tombe en panne, la chaîne de productivité sera sévèrement affectée, voire complètement paralysée. La haute disponibilité informatique présente plusieurs enjeux dans les entreprises numériques [12] :

- Gérer les pannes pour assurer un fonctionnement ininterrompu des activités.
- Améliorer la rentabilité en minimisant l'impact financier des défaillances.
- Maintenir leur image de marque.

3.3 Les stratégies de la haute disponibilité

3.3.1 La redondance

3.3.1.1 La redondance matérielle

En générale, une architecture tolérante aux pannes réplique le matériel dans le but d'augmenter la fiabilité, qu'il s'agisse d'un ordinateur, d'un composant (processeur, mémoire, disque dur), voire d'une partie d'un composant (cœur de processeur, unités de calcul) : si un composant tombe en panne, les autres permettre au système de fonctionner. Par exemple, vous pouvez utiliser plusieurs ordinateurs identiques qui font les mêmes fonctions en parallèle : si un ordinateur tombe en panne, les autre prendre le relais. Comme autre exemple, plusieurs processeurs peuvent être utilisés ou des unités de calcul dans un processeur peuvent être dupliquées.
Les techniques de redondance matérielle se classent en trois :

• **La redondance active** ne manque pas les défaillances comme le fait la redondance passive. Il détectera les défauts et transmettra les relais des composants défectueux aux composants fonctionnels.

• **La redondance passive** tous les composants fonctionnent en parallèle : ils reçoivent les données d'entrée, les traitent et fournissent des résultats plus en moins simultanément. La sortie du composant est reliée à un système qui se chargera de corriger les erreurs ou

défaillances de la sortie, mais pas de les détecter.
• **La redondance hybride** mélange les techniques vues plus haut. Il existe trois principales méthodes :
La redondance passive avec composants de réserve.
La redondance passive auto-correctrice.
La redondance à triple duplex.

3.3.1.2 La redondance logique

Les protocoles réseaux ont le rôle des transporteurs des données des applications à travers le réseau interne de l'entreprise. Ces protocoles comptent sur l'architecture hiérarchie, ainsi tous les équipements composent les adresses et leurs informations. Le routeur multi-protocole approvisionne toutes ces informations.

3.3.2 Les protocoles de la haute disponibilité

Les protocoles de haute disponibilité sont des mécanismes qui permettent d'atteindre cet objectif en fournissant des fonctionnalités de redondance, de basculement et de répartition de charge. Ces protocoles sont utilisés pour gérer des configurations complexes d'équipements réseau, de serveurs et d'applications afin de garantir la continuité des services essentiels.

Parmi les protocoles de haute disponibilité les plus utilisés, on trouve [21] :

3.3.2.1 Le protocole Virtual Router Rendundancy (VRRP)

Est un protocole de redondance de routeurs qui permet de créer des groupes de routeurs virtuels. Une adresse IP virtuelle unique est associée pour ces groupes de routeurs virtuels qui est utilisé comme adresse de passerelle par défaut pour les stations de réseau. VRRP améliore la fiabilité et les performances du réseau hôte en permettant à un routeur virtuel d'agir comme passerelle par défaut pour ce réseau.
Les routeurs du groupe VRRP communiquent entre eux à l'aide de protocole multidiffusion pour déterminer le routeur actif (maitre), et les routeurs de secours (esclaves). Si le routeur maitre tombe en panne, un autre routeur de secours prend automatiquement le relais afin de garantir la continuité du service et la disponibilité de la passerelle par défaut pour les stations du réseau.

3.3.2.2 Le protocole Hot Standby Router (HSRP)

Le HSRP est un protocole Cisco permettant d'obtenir une continuité de service LAN sur les routeurs en permettant à un routeur d'être le secours d'un autre routeur situé sur le même réseau Ethernet. Ce protocole est inspiré du protocole VRRP.
Le principe de son fonctionnement est que tous les routeurs contiennent une adresses IP virtuelle qui sera utilisée comme passerelle. Le routeur actif sera déterminé après que chacun configure son protocole HSRP avec un niveau de priorité.

3.3.2.3 Le protocole Gateway Load Blancing (GLBP)

Est un protocole propriétaire Cisco qui reprend les concepts de base de HSRP et VRRP, son principe est que tous les routeur virtuels GLBP participent activement au routage, le routeur de groupe GLBP ayant la haute priorité ou la plus haute adresse IP du groupe prendra la statut de « AVG » qui veut dire Active Virtual Gateway, ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP et il va assigner les adresses MAC virtuelles aux routeurs du groupes qui vont avoir la statut « AVF » qui veut dire Active Virtual Forwarder ; un autre groupe de routeurs ayant le rôle de backup en cas de panne des AVF.
Le GLBP permet une utilisation complète de la bande passante dédiée à tous les routeurs. Il permet la gestion des différentes défaillances sans pour autant arrêter le service de réseau.

3.3.2.4 Le protocole Spainning Tree (STP)

Est un protocole de réseau de niveau 2(liaison des données du modèle OSI) conçu pour les commutateurs afin d'empêcher les boucles de commutation qui peuvent se produire lorsque plusieurs chemins sont disponibles entre eux dans des réseaux Ethernet.
STP sert à créer un arbre de diffusion sans boucle afin de garantir que chaque commutateur dispose d'un unique chemin actif vers le réseau. Le protocole répond a la problématique de trames dupliquées dans un environnement de liaison redondantes. Il fonctionne en sélectionnant un commutateur racine (root) pour calculer les plus courts chemins vers ce dernier.
Il existe cinq états de port de commutation STP , Il s'agit de :

- **Désactivé (Disabled) :** Le résultat d'une commande administrative qui désactivera le port.
- **Blocage (blocking) :** Lorsqu'un périphérique est connecté, le port entre d'abord dans l'état de blocage.
- **Écoute (Listening) :** Le commutateur écoutera et enverra des BPDU.
- **Apprentissage (Learning) :** Le commutateur recevra une BPDU supérieure, cessera d'envoyer ses propres BPDU et relaiera les BPDU supérieures.
- **Transfert (Forwarding) :** Le port transfère le trafic.

3.3.3 Protocole de gestion de VLAN

Réduit la gestion dans un réseau commuté qui est :

3.3.3.1 Le protocole Vlan Trunking (VTP)

Est un protocole de couche 2 sert à simplifier la configuration et la gestion des VLANs sur les switches Cisco. VTP propose trois modes de fonctionnement :

- Le mode serveur : permet de créer, modifier et supprimer des VLANs et de les propager aux autres commutateurs.

— Le mode client : permet de recevoir les informations VLAN du mode serveur, mais ne peut pas les modifier.
— Le mode transparent : permet de transférer les trames de VLAN entre les commutateurs, mais ne participe pas à la propagation des informations VLAN.

Le VTP fonctionne qu'avec des liens de trunk entre les commutateurs donc il est important de configurer ces paramètres afin d'éviter les conflits et les perturbations sur le réseau. On peut dire aussi qu'il n'est pas un transporteur des données.

3.3.4 Redundant Array of Independent Disks (RAID)

est une technologie de stockage de données qui combine plusieurs disques durs indépendants pour améliorer les performances, la disponibilité et la fiabilité des données stockées. Les disques sont combinés dans une matrice logique, de sorte que les données sont réparties sur eux pour améliorer les performances de lecture et d'écriture. De plus, RAID protège les données en cas de panne d'un ou plusieurs disques en utilisant des techniques de redondance telles que la duplication des données sur plusieurs disques ou la distribution des données à l'aide de bits de parité. Cela minimise le risque de perte de données et garantit une disponibilité maximale du système de stockage. Il existe plusieurs niveaux de RAID, chacun offrant des avantages spécifiques en termes de performances, de redondance et de coût.

3.3.5 La répartition de charge

Appelé aussi « Load balancing » qui est une stratégie d'équilibrer le trafic entre un groupe de serveurs ou ressources informatiques, ainsi fournit une solution de secours en cas de panne. C'est là que les équilibreurs de charge entrent en jeu dans le but de maintenir la capacité à des niveaux optimaux. L'équilibrage de charge fait référence au processus de distribution des requêtes à différents serveurs en arrière-plan sans les utilisateurs ne s'en aperçoivent. Les équilibreurs de charge utilisés peuvent être implémentés dans le matériel ou le logiciel.L'équilibrage de charge est effectué avec un algorithme basé sur le DNS (Domain Name System). Les utilisateurs accèdent aux sites Web via des URL associées à leurs adresses IP. Ce dernier se connecte à l'équilibreur de charge et transmet les requêtes aux serveurs. La distribution dépend du type d'algorithme utilisé. Les quatre plus populaires sont Round Robin, Weighted Round Robin, Least Connections et Weighted Least Connections. [22]
Un logiciel de répartition de charge peut être installé sur des machines virtuelles. Il prend alors la forme d'un Application Delivery Controller (ADC). La version virtuelle rend l'équilibreur de charge plus flexible.

3.3.5.1 L'utilité de la répartition de charge

Le principe de répartition de charge est de réduire la charge entre les serveurs ainsi optimiser une performance de système en répartisse la charge entre eux, il peut se mettre en place avec plusieurs manières en exemple comme l'utilisation des algorithmes de répartition de charge qui se base sur la charge maximale du serveur, disponibilité des ressources et la latence de réseau.
Voici quelques exemples d'utilisations courantes du Load balancing :

— Optimiser le temps de réponse et éviter une défaillance due à la surcharge de trafic en répartir la charge entre les serveurs web.

— Améliorer la performance des requêtes ainsi éviter une défaillance due à la surcharge de requête en répartir la charge entre les serveurs Data Bases

— optimiser la disponibilité et assurer la fiabilité des applications en répartissaient la charge entre les serveurs qui les prend en charge.

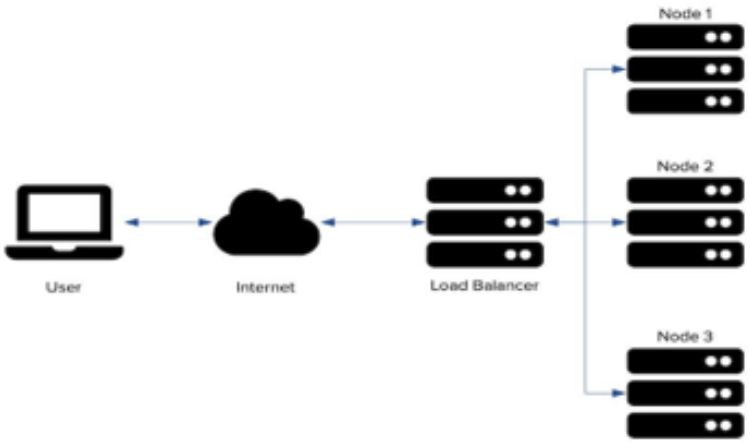


FIGURE 3.1 – La répartition de charge

3.3.6 Clustering

3.3.6.1 La mise en place de cluster

Le clustering dans l'environnement de la haute disponibilité est une méthode qui fournit une disponibilité élevée de plusieurs services : données, réseaux ; en se basant sur la création de groupes de périphériques pour fonctionner comme un système unique et puissant en partageant l'ensemble des tâches pour assurer la continuité de ces services ; en cas l'un de ces périphériques tombe en panne les autres prennent le relais sans interruption de service pour l'utilisateur final [23].
La configuration des clusters peut s'effectuer avec différentes manières suivant l'objectif et l'architecture de système. Les deux principales méthodes de mise en cluster sont :

• **Le clustering à haute disponibilité (HA)** : C'est la mise en place un nombre de serveurs pour assurer la continuité des données en cas de panne d'un serveur en répartissant la charges entre eux.

• **Le clustering à haute performance (HP)** : répartir la charge entre plusieurs serveurs qui sont configurés en mode actif-actif d'où chaque serveur gère une partie des tâches pour augmenter les performances du système. Cette méthode de clustering est exploitée dans les environnements à forte demande de traitement, comme les centres donnés, les applications d'entreprise, de calcul intensif et les services cloud.

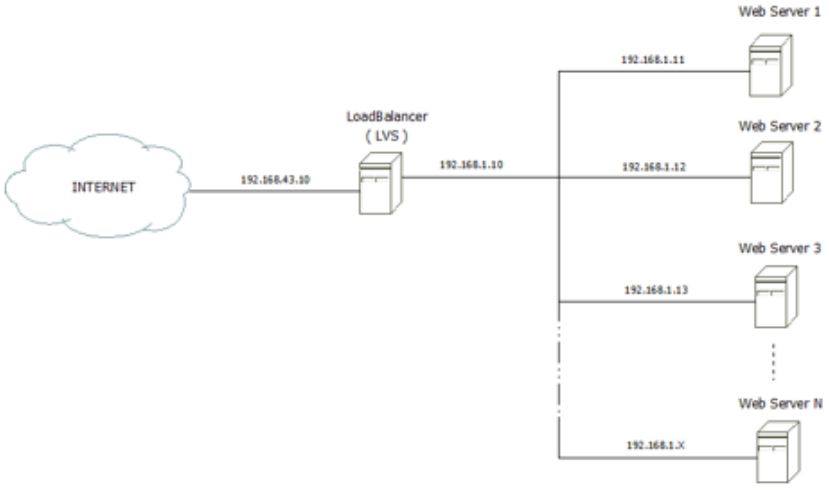


FIGURE 3.2 – La mise en place d'un cluster avec Load balancer

3.3.6.2 Cluster à surveillance de répartition de charge

est un ensemble de serveurs interconnectés et configurée de façon à distribuer la charge des requêtes venant des clients. Son principal rôle est l'acheminement de trafic vers le serveur approprié selon de charge et de l'état de serveur. Le processus de surveillance envoie des demandes à tous les serveurs pour vérifier qu'ils sont en ligne et peuvent répondre à ces requêtes. Le choix d'une technologie de la surveillance de répartition de charge dépend des besoins de l'application et des exigences de l'entreprise.
L'augmentation de la disponibilité du service est un avantage de surveillance de répartition de charge ainsi une réduction du temps de réponse et amélioration la capacité de traitement globales de système. Les charges peuvent être réparties entre les serveurs de manière dynamique et l'adaptation aux fluctuations du trafic [23].

3.3.6.3 Cluster à mécanisme de redondance

Un groupe de serveurs informatiques représente un cluster à mécanisme de redondance qui travaille en parallèle pour garantir un service haute disponibilité et tolère aux défaillances. Ce mécanisme consiste à exécuter des tâches similaires sur chaque serveur et les résultats sont comparés pour assurer leur cohérence. Autres serveurs prennent en charge les tâches du serveur défaillant. Dans ce cas, le cluster peut offrir une disponibilité élevée et une résilience aux pannes. Les clusters à mécanisme de redondance sont utilisés dans les systèmes de bases de données, les applications Web, les réseaux de stockage et d'autres applications critiques [23].

3.3.6.4 Cluster aux tolérances aux pannes

Appelé aussi cluster haute disponibilité qui est un système informatique constitué de nombreux serveurs interconnectés pour garantir la disponibilité de service en cas de panne d'un ou plusieurs de ces serveurs. Les clusters tolérants aux pannes utilisent nombreuses techniques, comme la réplication de données, la redondance de matériel et de logiciel,

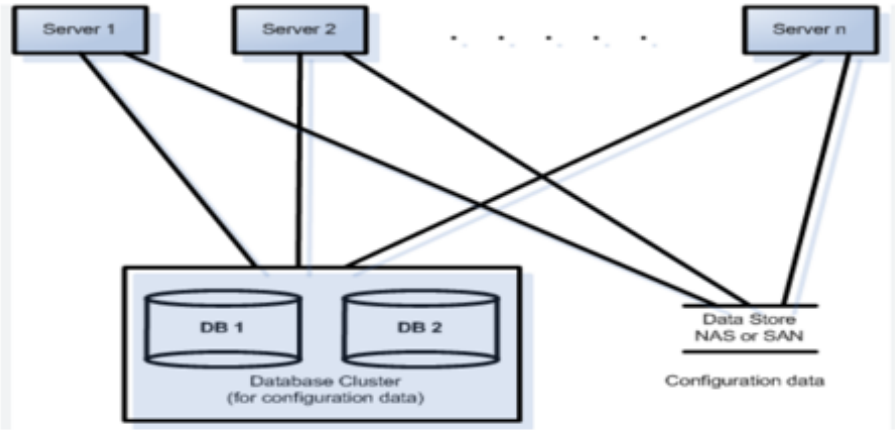


FIGURE 3.3 – Serveur redondant [24].

la reprise automatique après sinistre, la détection de panne. En cas d'une défaillance, le cluster bascule automatiquement le trafic vers les serveurs restants, en assurant une transition transparente pour les utilisateurs. Ce type de cluster est éventuellement utilisé dans les environnements de production pour des applications critiques telles que les serveurs de base de données, les serveurs de messagerie, les serveurs web, les systèmes de stockage, pour qu'ils offrent une disponibilité élevée, une évolutivité horizontale et une résilience aux pannes, qui sont obligatoire pour garantir la disponibilité des activités de l'entreprise.[24]

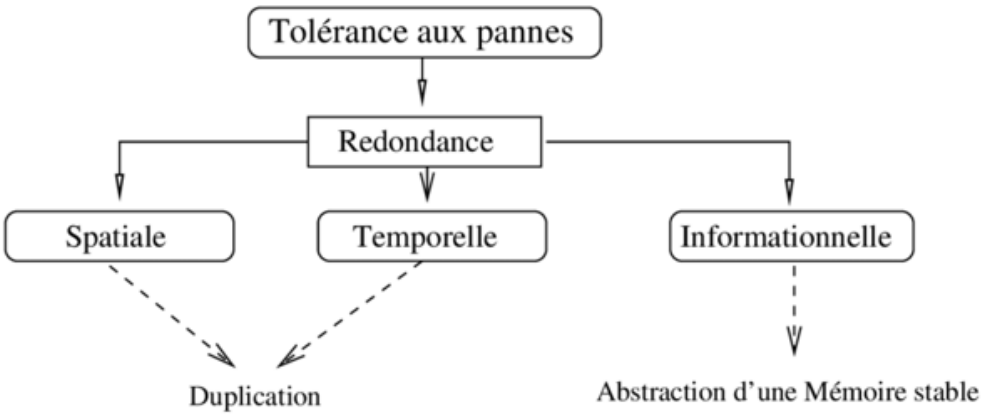


FIGURE 3.4 – Les techniques de tolérances aux pannes dans les systèmes répartis [25].

3.3.7 Le basculement automatique

Appelé aussi « Failover » qui est la solution de secours en cas de panne de la solution principale, sa mise en œuvre est dans les systèmes critiques et les systèmes de stockage de données. Le failover autorise au système de basculer automatiquement sans aucune

interruption vers la solution de secours lors d'une panne. Les deux systèmes que le fonctionnement de failover implique sont : un système principal qui est toujours actif et traite les requêtes des utilisateurs dans le temps réel, et un système de secours met en veille, reste à la disposition en cas de besoin. Le failover permet donc de garantir une disponibilité de service en cas de panne, tout en minimisant l'impact sur l'utilisateur final.

3.3.8 La sauvegarde et la récupération

La sauvegarde un processus qui protège contre la perte définitive des données en les réservant sur un support de stockage, car une erreur de système ou une attaque de sécurité peut endommager toutes les activités qui cause l'indisponibilité des données. Les différents supports de stockage servent à sauvegarder les données tels que des disques durs externes, des clés USB, des bandes magnétiques ou des serveurs de stockage en nuage (cloud), la sauvegarde des données s'automatise idéalement et régulièrement.
Voici deux types exemplaires de stockage informatiques les plus utiliser en moment actuel

3.3.8.1 Network Attached Storage (NAS)

Egalement connu sous le nom de stockage connecté en réseau, est un ensemble de fichiers qui est connecté à un réseau informatique pour que les utilisateurs puissent accéder à ces fichiers partagés directement. Ce dispositif se compose de nombreux disques durs configurés en un tableau RAID et il se connecte à un réseau avec une connexion Wi-Fi ou Ethernet. Les dispositifs NAS fournissent un moyen simple et rentable de stocker et de partager des données sur un réseau. Le NAS est un système de stockage qui est généralement connecté à un réseau local (LAN) et accessible à partir de différents ordinateurs et appareils connectés au même réseau [26].
L'architecture d'un NAS se compose généralement des éléments suivants :
1. Le matériel physique : il s'agit du boîtier du NAS, qui contient les disques durs, une carte réseau, un processeur et de la mémoire vive (RAM) traiter des requêtes.
2. Le système d'exploitation : le système d'exploitation d'un NAS se base sur un système d'exploitation open source comme Linux ou FreeBSD qui permet la gestion des disques durs, de sauvegarde et de synchronisation des données, de fournir des services de partage de fichiers.
3. Les protocoles de partage de fichiers : tels que SMB (Server Message Block), NFS (Network File System) et AFP (Apple Filing Protocol), permettant aux utilisateurs de se connecter et d'accéder aux fichiers stockés sur le NAS.
4. Les services de sauvegarde et de synchronisation : tels que la sauvegarde automatique des fichiers, la synchronisation des fichiers entre différents appareils et la récupération de fichiers supprimés.

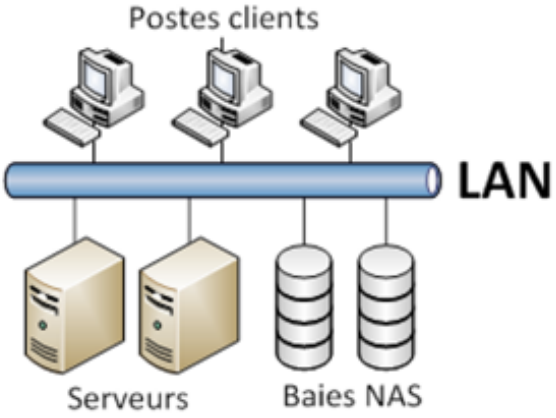


FIGURE 3.5 – Network Attached Storage

Les avantages d'un NAS (Network Attached Storage) incluent :

— Le NAS permet de centraliser le stockage de données pour tous les utilisateurs d'un réseau local, il évite la duplication des données sur les équipements.

— Les fichiers stockés sur le NAS ont un accès facile à partir de n'importe quel terminal connecté au réseau local, ce qui simplifie la gestion des données.

— Facilité le partage des fichiers entre utilisateurs de même réseau local.

— La sauvegarde automatique des données est une fonctionnalité de NAS ainsi la récupération des fichiers supprimés ou modifiés accidentellement.

3.3.8.2 Storage Area Network (SAN)

Il est également coûteux, surtout par rapport à des solutions de stockage plus simples telles que le stockage directement attaché (DAS).Est un réseau à haute vitesse qui fournit un stockage en bloc. Il permet un accès à un pool de dispositifs de stockage partagés pour plusieurs serveurs, tels que des matrices de disques ou des bibliothèques de bandes, comme s'ils étaient locaux à chaque serveur. Le SAN utilise généralement la technologie Fibre Channel pour fournir des taux de transfert de données élevés et offre plusieurs avantages, notamment la gestion centralisée du stockage, une disponibilité et une fiabilité accrues des données, des performances améliorées et une évolutivité.Il est également coûteux, surtout par rapport à des solutions de stockage plus simples telles que le stockage directement attaché (DAS) [26].
Les principes de base de l'architecture SAN incluent :
1. Fibre Channel (FC) est un protocole de transfert de données à haute vitesse pour faire une connectivité entre les serveurs.
2. Les commutateurs permettent une connectivité point à point et une interconnexion de commutateurs pour créer des réseaux de stockage plus grands.
3. Les baies de stockage offrent une capacité de stockage évolutive, une haute disponibilité et des fonctionnalités de gestion avancées.

Les avantages de l'architecture SAN (Storage Area Network) sont nombreux, voici quelques-uns des principaux :

— Haute disponibilité et performance.
— Grande capacité de stockage et sécurité de données.
— Gestion centralisée.
— Economies de coûts.

La récupération est le processus de restauration des données sauvegardées en cas de défaillance de données ou de corruption de fichiers. La récupération s'effectuée à partir d'une sauvegarde récente, afin de restaurer les données manquantes ou endommagées. La récupération peut être effectuée manuellement ou automatiquement, en fonction des paramètres de sauvegarde et de récupération.
En résumé, la sauvegarde et la récupération sont deux processus complémentaires qui base sur la protection des données et de garantir la continuité des activités en cas de sinistre ou de défaillance du système.

3.3.9 La supervision et le monitoring

La supervision permet la détection des problèmes, des pannes, les anomalies en surveillant un système en temps réel. La supervision sert à surveiller l'état de différents composants, notamment les serveurs, les réseaux, les applications, les bases de données, les systèmes de stockage, etc. Elle s'effectuée de manière manuelle ou automatisée en utilisant des logiciels de supervision qui collectent les données, les analysent et les présentent sous forme de graphiques ou de tableaux de bord.
Les types de supervision, on trouve :
1. Supervision système : tels que les serveurs, les pares-feux, etc.
2. Supervision des applications : telles que mes logiciels comptabilités, les applications web, etc.
3. Supervision du réseau : tels que les LAN, les WAN, les VPN, etc.
4. Supervision de la sécurité : surveiller les activités suspectes ou malveillantes sur les systèmes, les réseaux ou les applications.
5. Supervision des bases de données : telles que MySQL, Oracle, SQL Server, etc.

Le monitoring en français [suivi]permet la collection des données concernant les performances d'un système sur une période de temps, il est un processus passif, généralement il fonctionne à des fins d'analyse et de rapport. Le monitoring peut être effectué à l'aide de différents outils de surveillance, tels que les capteurs, les compteurs, les enregistreurs de données, les journaux, etc. Les données collectées sont pour évaluer la performance globale d'un système, identifier les tendances, établir des comparaisons, prévoir les besoins futurs en ressources, etc.
Il se trouve différents types de monitoring, voici quelques exemples :
1. Monitoring de disponibilité : permet d'alerter l'équipe de support lors d'un dysfonctionnement ou d'une panne de système qui surveille en temps réel.
2. Monitoring de sécurité : permet la surveillance des actes suspects en détectant les attaques de sécurité, les violations des données.
3. Monitoring de performance : permet la surveillance la performance de système en temps réel en détectant les problèmes de latence, les temps de réponses lents.

En résumé, la supervision est un processus actif de contrôle en temps réel, alors que le monitoring est un processus passif de collecte de données sur une période de temps donnée. Il est nécessaire de comprendre leurs différences pour bien choisie entre eux en

fonction des besoins de surveillance et de suivi des systèmes informatiques, des réseaux et applications.

3.4 Les avantages de la haute disponibilité

La haute disponibilité (HA) est une mesure de la fiabilité d'un système informatique. Les avantages de la haute disponibilité incluent [27] :

- La redondance et la répartition de charge permettent de réduire le temps d'arrêt en basculant automatiquement sur la solution du secours.
- La haute disponibilité assure la continuité des services dans l'entreprise en maintenant leurs activités en cas de panne ou de défaillance d'un équipement [28].
- Minimisation de pertes de données en cas de panne, les données sont répliquées en temps réel ce qui permet d'obtenir une meilleure performance.
- Les solutions de la haute disponibilité garantissent une disponibilité continue pour les utilisateurs, ce qui assure le renforcement de la réputation de l'entreprise.

3.5 Conclusion

Ce chapitre met en évidence l'importance de la haute disponibilité dans le domaine informatique et son utilité majeur dans les entreprises. Nous avons compris qu'elle vise à assurer la continuité des services et des systèmes afin d'éviter les pertes financières en maintenir la productivité. Il est donc nécessaire pour l'entreprise CEVITAL de mettre en place les mesures appropriées de ce domaine afin de garantir la continuité des opérations critiques et cela en investissant dans les infrastructures nécessaires est ça par l'acquisition de serveurs et de systèmes de stockage redondants essentielles et l'investissement dans des plateforme de virtualisation qui offre des avantages significatifs en haute disponibilité en configurant des clusters virtuels afin de permettre la migration et le basculement rapides des machines virtuelles.

Chapitre 4

La virtualisation

4.1 Introduction

La virtualisation recouvre un ensemble de techniques matérielles et/ou logicielles qui consiste à créer une version virtuelle d'un dispositif ou d'une ressource informatique, comme un ordinateur, un serveur, un périphérique de stockage ou des ressources réseau. Elle permet également de faire fonctionner sur une seule machine hôte plusieurs systèmes d'exploitation, plusieurs instances différentes et cloisonnées d'un même système ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.
Dans ce chapitre, nous plongerons dans les concepts fondamentaux de la virtualisation et son importance dans le monde informatique ensuite nous aborderons ces types et ses meilleurs pratiques dans le domaine numérique.

4.2 Histoire de virtualisation

La virtualisation est une technologie qui a commencé à apparaitre dans les années 1960. A l'époque, les mainframes étaient très coûteux et les utilisateurs ne pouvaient pas se permettre d'en acheter un chacun. Pour résoudre ce problème, les chercheurs ont pensé à l'idée de partage de ressources entre plusieurs utilisateurs tout en assurant la sécurité informatique.
Dans les années 1970, l'une des premières formes de virtualisation a été la création de machines virtuelles (VM), sont des machines simulées qui peuvent être exécutées sur un hôte physique. Elles permettent à plusieurs systèmes d'exploitation de s'exécuter simultanément et d'accéder à un même système informatique sur un seul ordinateur physique.
Dans les années 1990, la virtualisation a été utilisée pour créer des environnements de développement et de test isolés, ainsi que pour fournir un environnement d'exécution pour les applications. Cela a conduit à l'émergence de la virtualisation d'application, qui permettait aux applications de s'exécuter dans des environnements isolés et sécurisés.
Au début des années 2000, la virtualisation est devenue de plus en plus populaire grâce aux avancées technologiques telles que les processeurs x86 et la virtualisation assistée par matériel. Ces avancées ont rendu la virtualisation plus accessible et plus facile à utiliser, ce qui a conduit à une adoption plus large de la technologie dans les entreprises et les centres de données.
Aujourd'hui, la virtualisation est devenue une technologie importante pour les grandes entreprises. Elle les permet de réduire leurs coûts et d'améliorer leur rendement et leur agilité, et de simplifier la gestion de leurs infrastructures informatiques.

4.3 Le modèle de couches des systèmes d'informations

Le modèle de couches des systèmes d'informations est une approche qui organise les différentes composantes d'un système informatique en couches logiques, où chaque couche offre des fonctionnalités spécifiques et communique avec les couches adjacentes. Dans le contexte du modèle de couches des systèmes d'informations, la virtualisation peut être utilisée pour créer des environnements isolés et indépendants au sein de chaque couche.
Il est constitué de quatre principales couche sont :

4.3.1 Couche infrastructure

La couche infrastructure informatique fait référence à la base technique sur laquelle repose un système informatique. Elle regroupe un ensemble des éléments matériels tels que les serveurs, les routeurs, les commutateurs, les baies de stockage, ainsi que les logiciels nécessaires pour gérer ce matériel, tels que les systèmes d'exploitation, les logiciels de virtualisation, les programmes de sécurité, etc. cette couche est pour but d'assurer le bon fonctionnement, la disponibilité des systèmes et une sécurité accrue de données. Elle est souvent gérée par des administrateurs et les ingénieurs réseau.

4.3.2 Couche opérationnelle

La couche opérationnelle appelé aussi « couche physique » comprend les composants tels que les câbles, les adaptateurs réseau, etc. elle fait référence au niveau le plus bas d'un système informatique, qui est le responsable de la communication avec le matériel. Elle permet également de fournir une interface pour les couches supérieures su système pour effectuer des taches plus complexes. Ainsi, la couche opérationnelle est responsable de la transmission de données entre les appareils et les appareils connectés à un réseau et elle assure une communication de données efficace.

4.3.3 Couche applicative

La couche applicative est responsable du développement, de la maintenance et de la gestion des applications de l'entreprise. Elle détermine un ensemble de protocoles et des règles de syntaxe des données au niveau application. Elle représente les données aux utilisateurs et elle offert des mécanismes de communication et de dialogue aux applications de l'utilisateur. En point de vue de modèle, la couche applicative représente le point d'accès aux réseaux.

4.3.4 Couche décisionnelle

Cette couche gère les systèmes et responsable de la collecte, de l'analyse et la présentation des données pour une prise de décisions stratégiques dans l'entreprise. Elle désigne les moyens et les outils qui permettent de collecter et de consolider des informations matérielles ou immatérielles d'une entreprise afin d'offrir une aide à la décision et de permettre à un décideur de prendre des décisions éclairées d'avoir une idée d'ensemble de l'activité traitée.

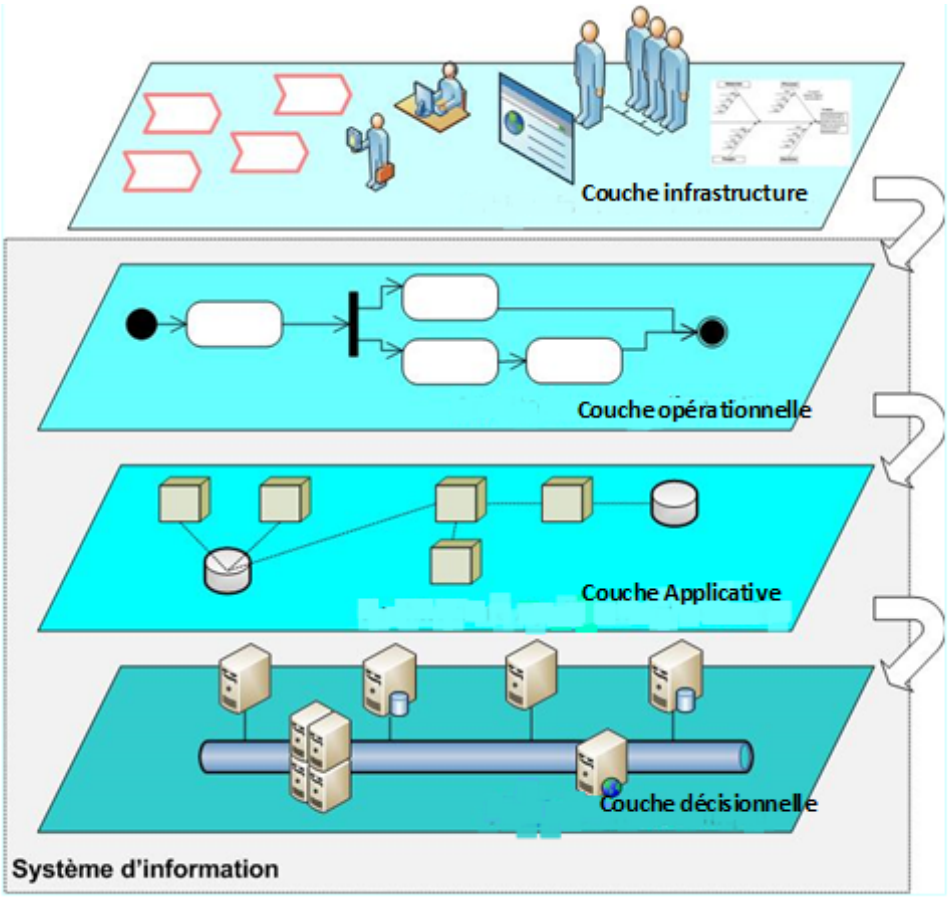


FIGURE 4.1 – Le modèle de couches des systèmes d'informations

4.4 Le moniteur des machines virtuelles

Appelés aussi hyperviseur son rôle crucial dans la virtualisation est de représenter la couche logicielle qui coordonne les machines virtuelles sur un seul ordinateur hôte. Il permet d'optimiser l'utilisation des ressources matérielles, fournir des environnements isolés pour exécuter différents OS ou application sur un même matériel physique et il autorise à une machine physique de prendre en charge plusieurs machines virtuelles invitées en partageant virtuellement ses ressources critiques tels que le processeur, le disque dur et le stockage [33].
On distingue deux types d'hyperviseurs :

4.4.1 Les hyperviseurs de type 1

Appelés aussi hyperviseurs natifs ou bare-metal sont des logiciels d'Hypervision qui s'exécutent directement sur le matériel de l'hôte pour gérer les systèmes d'exploitation invités. Au démarrage d'une machine physique, ces hyperviseurs prennent directement le contrôle de matériel. VMware ESXI, Microsoft Hyper-V et Citrix Hypervisor (anciennement XenServer) sont des exemples de ce type d'hyperviseur [33].

Avantages :

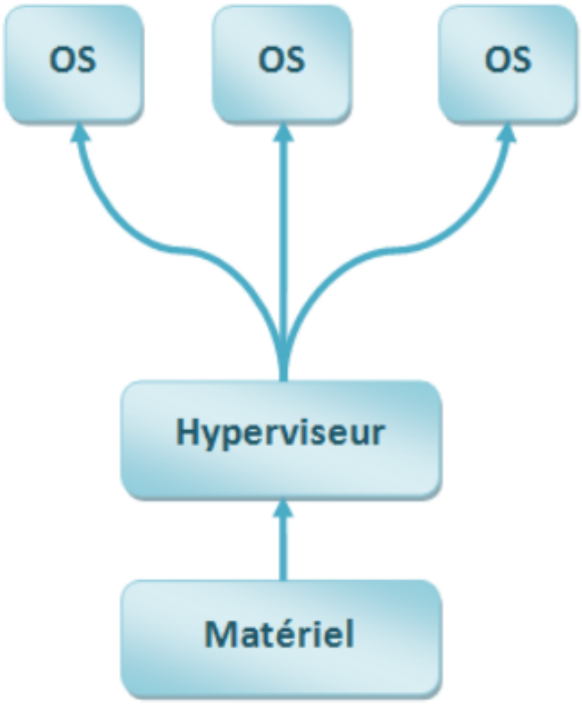


FIGURE 4.2 – Hyperviseur type 1 [29].

— La performance : Les hyperviseurs de type 1 sont très performants, car ils ont un accès direct au matériel physique.

— La sécurité : ces hyperviseurs sont protégés des failles et des vulnérabilités liées au système d'exploitation.

— La vitesse : l'accès direct au matériel entraine une latence moindre.

4.4.2 Les hyperviseurs de type 2

Appelés aussi Hyperviseurs hébergés ou hosted sont des logicielq qui s'installent et s'exécutent sur un système d'exploitation déjà en place tel que Windows ou Linux. Un hyperviseur hébergé ajoute une couche logicielle distincte au-dessus du système d'exploitation hôte, et le système d'exploitation invité devient un troisième niveau logiciel au-dessus du matériel. Les exemples d'hyperviseurs de type 2 sont Oracle VirtualBox, VMWare Workstation et Parallèles Desktop pour Mac [33].

Avantages

— La gestion simple : ce type d'hyperviseur est très facile à paramétrer, et il est compatible avec un plus grand nombre de machines car il ne s'installe pas directement sur la couche matérielle.

— L'utilité à des fins de test : ils sont utilisés pour les tests de nouveaux logiciels et développement d'application.

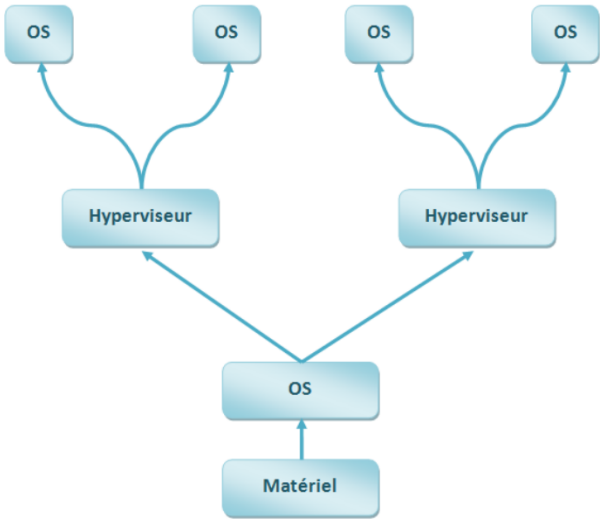


FIGURE 4.3 – Hyperviseur type 2 [29].

4.5 Le fonctionnement de la virtualisation

Le fonctionnement de la virtualisation est basé sur l'utilisation d'un logiciel appelé hyperviseur (ou VMM, Virtual Machine Manager). L'hyperviseur est responsable de la gestion des ressources physiques de la machine (processeur, mémoire, stockage, réseau, etc.) et de leur allocation aux machines virtuelles qui s'exécutent sur la machine physique. Lorsque l'hyperviseur est lancé, il crée un environnement virtuel disposant de plusieurs machines virtuelles (VM) en utilisant les ressources physiques de la machine hôte. Chaque VM dispose de son propre système d'exploitation et de ses propres applications, sans interférer les unes aux autres grâce à la couche qui est entre les VMs et le matériel physique appelé couche d'abstraction.
La machine virtuelle peut être transférée d'un ordinateur à un autre et de fonctionner de la même manière sur les deux machines physiques grâce à l'hyperviseur, appelé migration de VM, ce qui permet une gestion plus efficace des ressources informatiques.
Il existe plusieurs types de virtualisation, y compris la virtualisation de serveurs, la virtualisation de postes de travail, la virtualisation de stockage, et la virtualisation de réseaux. Chacune de ces technologies utilise l'hyperviseur de manière différente pour permettre l'exécution de plusieurs machines virtuelles sur une seule machine physique.

4.6 Les avantages de virtualisation

Les avantages de la virtualisation sont nombreux et incluent :

- Réduction de coûts : la virtualisation de serveurs permet de réduire les coûts liés à l'achat et à la maintenance de plusieurs serveurs physiques, en les remplaçant par un seul serveur physique qui peut exécuter plusieurs machines virtuelles.
- Assurer la haute disponibilité du système : la virtualisation permet le déplacement d'une machine virtuelle d'un serveur physique vers un autre, ce qui permet l'amélioration de taux de disponibilité de services. Au cas de panne d'un serveur, les machines vont directement basculer sur l'autre serveur.

— Flexibilité : la virtualisation, selon le besoin, permet de déployer de nouvelles machines sans avoir à acheter du matériel. Cela permet de déplacer plusieurs machines virtuelles entre différents serveurs physiques, offrant ainsi une grande flexibilité pour la gestion des ressources.

— Optimisation de ressources : la virtualisation permet d'allouer dynamiquement les ressources informatiques selon les besoins de chaque machine virtuelle, et de les utiliser de manière plus efficace. Cela permet de maximiser les ressources.

— Réduction du temps d'arrêt : Les machines virtuelles peuvent être sauvegardées et restaurées rapidement en cas de panne ou d'interruption du système, ce qui réduit le temps d'arrêt et améliore la disponibilité des applications.

4.7 Les meilleures pratiques de la virtualisation

— Planification et conception : Avant de mettre en place une machine virtuelle, il est crucial de planifier et d'estimer la quantité de ressources critiques dont elle aura besoin, telles que la RAM, la processeur et l'espace de stockage. Si ces ressources sont surutilisées, cela peut entraîner des ralentissements dans les temps de réponse et une baisse des performances.

— Sécurité et conformité : la sécurité doit être considérée comme une préoccupation majeure pour toute technologie, y compris les machines virtuelles. Ainsi, il est crucial de prendre des mesures de sécurité pour protéger les VM, les données et les applications qu'elles hébergent. Cela peut englober l'implémentation de pare-feu, d'antivirus et la mise en place de politiques de sécurité rigoureuses.

— Surveillance et gestion : surveiller les performances de VM est essentiel pour détecter les ralentissements et les problèmes de performance potentiels. Pour cela, il est recommandé d'utiliser des outils de surveillance de performances qui permettent de surveiller l'utilisation de la CPU, de la RAM et du stockage.

4.8 Les types de virtualisation

Il existe plusieurs types de virtualisation, chacun offrant différents niveaux d'isolation et d'abstraction du matériel physique.

4.8.1 Virtualisation de systèmes d'exploitation

Est une technique qui permet de lancer plusieurs applications et systèmes d'exploitation simultanément sur une seule machine physique, en utilisant une couche logicielle intermédiaire appelée hyperviseur. Cette technique permet de maximiser l'utilisation des ressources machine et de faciliter la gestion des ressources informatique. Ce type de virtualisation est utilisé dans de nombreux domaines tels que les grandes entreprises, les centres de données, les logiciels, les laboratoires de recherche... afin de consolider leurs infrastructures et de faciliter la gestion de leurs ressources informatiques.

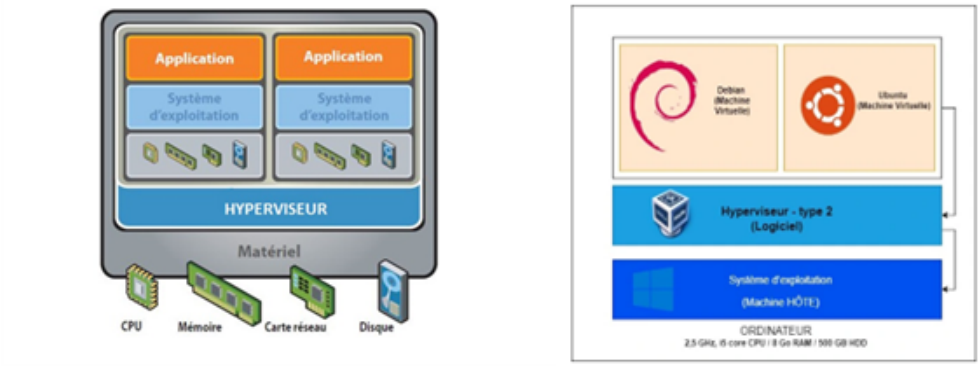


FIGURE 4.4 – virtualisation des systèmes d'exploitation de type 1 et 2 [30]

4.8.2 Virtualisation de poste de travail

Appelé aussi virtualisation desktop est une technique qui consiste à créer des stations de travail virtuelles exécutant des différents systèmes d'exploitation (Windows, Linux ou IOS) et à rendre ses stations accessibles depuis un terminal connecté au réseau, comme un ordinateur portable, une tablette ou un smartphone. Cela permet de déployer ces machines virtuelles avec des applications et des paramètres depuis un serveur centralisé. Cette technique offre plusieurs avantages, notamment le contrôle facile des mises à jour, une meilleure sécurité des données, une grande flexibilité et une réduction de coûts.

FIGURE 4.5 – virtualisation des postes de travail

4.8.3 Virtualisation de données

Est une technique qui consiste à fournir une couche d'abstraction, entre le stockage physique des données et les terminaux, qui masque les détails techniques liés à la donnée, tels que sa structure et sa localisation sur le disque dur ou la base de données, etc. la virtualisation de données permet aux utilisateurs d'accéder et d'utiliser les données provenant de diverses sources comme si elles provenaient d'une seule et même source. Ce type de virtualisation est utilisé dans les entreprises pour améliorer la qualité de données, réduire la complexité et gérer leurs ressources.

4.8.4 Virtualisation matérielle

Appelé aussi virtualisation hardware est une technologie qui est pour but de virtualiser la partie matérielle d'un ordinateur (processeur, mémoire, réseau, etc.). Elle permet de faire fonctionner de différents systèmes d'exploitation et applications dans un seul ordinateur en partageant ses ressources physiques. Ce type de virtualisation est largement utilisé dans des environnements informatiques professionnels pour des raisons de sécurité, la gestion des ressources et aussi la réduction de coûts en consolidant plusieurs machines virtuelles dans une seule machine physique.

4.9 Les techniques de virtualisation

4.9.1 La virtualisation complète

Appelé aussi la virtualisation de la machine entière est une technique qui consiste à créer des machines virtuelles autonomes et isolées qui ont leur propre système d'exploitation et leurs propres ressources matérielles. Elle fonctionne en émulant du matériel virtuel, ce qui permet d'exécuter différents systèmes d'exploitation ou des versions différentes du même système sur un même ordinateur physique. Cette méthode est particulièrement utile pour la consolidation de serveurs, l'exécution d'applications sur des plates-formes multiples et pour la mise à l'échelle des environnements de test [33].

4.9.2 La paravirtualisation

La paravirtualisation est une technique de virtualisation qui permet aux machines virtuelles de communiquer avec le matériel sous-jacent de manière plus efficace. Contrairement à la virtualisation complète où l'hyperviseur virtualise tous les composants matériels, la paravirtualisation fournit une interface logicielle similaire au matériel, permettant aux machines virtuelles de s'exécuter plus efficacement. Cette méthode est généralement plus simple et plus légère que la virtualisation complète, mais elle nécessite que le système d'exploitation invité soit spécialement modifié pour utiliser l'interface paravirtualisée et que le matériel sous-jacent prenne en charge la paravirtualisation. Les avantages de la paravirtualisation sont une meilleure performance des machines virtuelles et une réduction des coûts d'overhead de virtualisation [33].

4.9.3 L'isolation

Egalement appelée conteneurisation, permet de créer plusieurs environnements isolés sur un seul système d'exploitation (OS). Contrairement à la virtualisation traditionnelle, où chaque machine virtuelle (VM) possède son propre système d'exploitation, la virtualisation par isolation utilise une seule instance du système d'exploitation hôte pour exécuter plusieurs conteneurs qui partagent les mêmes ressources système. Chaque conteneur est une instance isolée d'un environnement d'exécution qui contient une application, ses dépendances et les bibliothèques nécessaires à son fonctionnement. Les conteneurs partagent le même noyau de système d'exploitation que l'hôte, mais ont leur propre espace utilisateur, ce qui leur permet de fonctionner indépendamment les uns des autres. Cette technique est largement utilisée dans les centres de données et les environnements de production, car elle utilise les ressources système plus efficacement que la virtualisation traditionnelle, tout en offrant une isolation plus légère et une meilleure densité d'applications.[33]

4.10 Migration de la machine virtuelle

La migration de machines virtuelles implique le transfert de l'état, des fichiers et d'autres éléments d'une machine virtuelle d'un hôte à une infrastructure physiques.
Elle peut être effectuée pour diverses raisons, telles que l'équilibrage de charge, la maintenance matérielle ou la reprise après sinistre. Il existe différents types de migration de machine virtuelle, y compris la migration dynamique qui permet la migration alors que la machine virtuelle est encore en cours d'exécution, et la migration à froid qui nécessite l'arrêt de la machine virtuelle avant que la migration puisse avoir lieu. Certaines ressources fournissent des informations détaillées sur des outils spécifiques qui peuvent être utilisés pour la migration de machines virtuelles, tels que VMware vSphere et PowerVC. Il convient de noter que le clonage ou la copie d'une machine virtuelle dans le même vCenter Server n'est pas considéré comme une forme de migration. Dans l'ensemble, la migration des machines virtuelles est un processus important dans la virtualisation qui permet une plus grande flexibilité et efficacité dans la gestion des environnements virtualisés.

4.11 Consolidation, rationalisation et concentration des serveurs

4.11.1 Consolidation des serveurs

La consolidation dans la technique de la virtualisation c'est le regroupement plusieurs machines virtuelles sur un seul serveur physique voir (Figure 4.6) les créant sur les environnements informatiques isolée est que chaque machine peut exécuter un système d'exploitation et des applications indépendamment des autres VM installées sur le même serveur. Cela permet une meilleure utilisation pour les ressources matérielles comme la puissance de calcul, la mémoire, le stockage et la bande passante réseau.

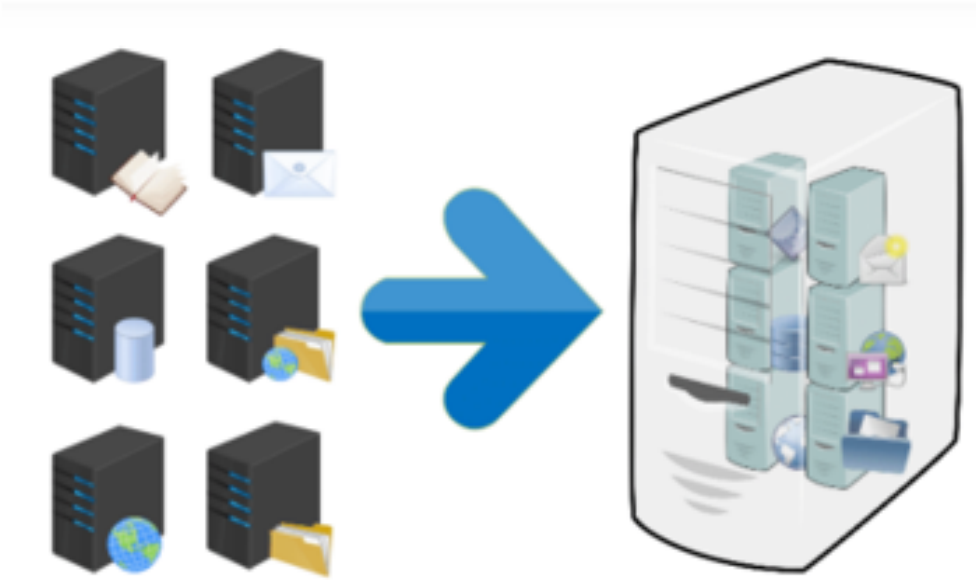


FIGURE 4.6 – Consolidation des serveurs

4.11.2 Rationalisation des serveurs

La rationalisation dans la virtualisation consiste à optimiser l'infrastructure virtuelle en éliminant les équipements redondants sans utilité, en simplifiant les processus et améliorant l'efficacité opérationnelle, la cause que à chaque foie le nombre de VM augmente, il y aura des complexités de la gestion, parmi un de ses avantages est la réduction importante de la gestion de ces équipements afin d'éviter la perte de productivité.

-

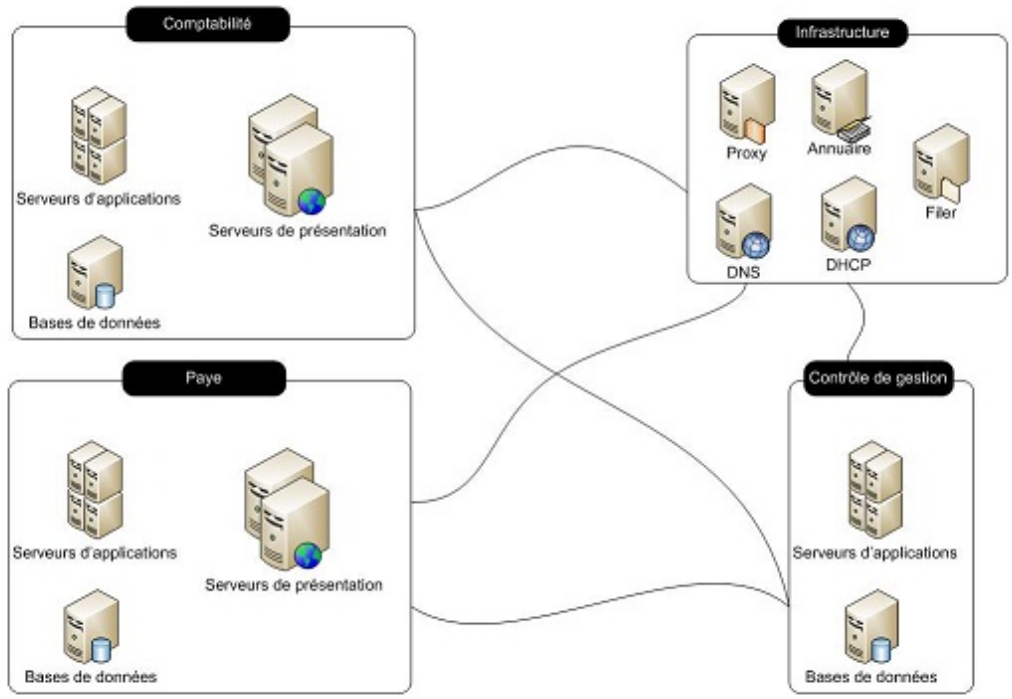


FIGURE 4.7 – Rationalisation des serveurs

4.11.3 Concentration des serveurs

La concentration c'est de regrouper physiquement plusieurs serveurs sur un même centre de données afin de réaliser des économies en termes de coûts d'exploitation, ainsi une gestion et supervision de l'infrastructure facile car la surveillance l'état serveurs, d'appliquer les mises à jour de sécurité telles que les contrôles d'accès et les systèmes de surveillance.

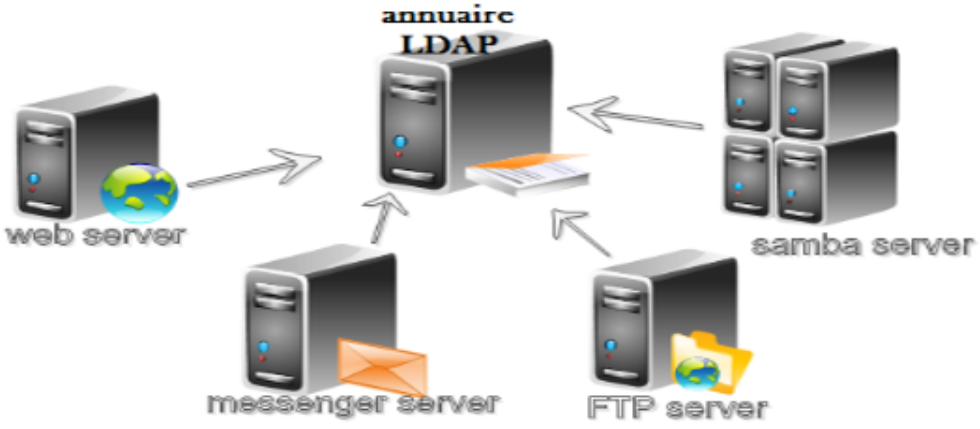


FIGURE 4.8 – Concentration des serveurs

4.12 Conclusion

Pour conclure, la virtualisation est une technologie révolutionnaire dans le monde de l'informatique moderne et apporte de nombreux avantages significatifs aux utilisateurs et aux entreprises qui l'adoptent. Grace à cette technologie, il est possible d'optimiser des ressources matérielles, d'améliorer l'efficacité énergétique, de réduire les coûts d'exploitation et de simplifier la gestion des systèmes informatiques. La virtualisation a pour objectif de créer des environnements isolés, sécurisés, agiles et performants permettant aux organisations de répondre aux besoins changeants du monde numérique. Ainsi, la virtualisation reste un élément clé dans le domaine informatique contemporain. Son développement continu et les progrès technologiques qui l'accompagnent continueront d'influencer notre manière de concevoir, de gérer et d'utiliser les systèmes informatiques.

Chapitre 5

Réalisation

5.1 Introduction

Dans ce chapitre, nous aborderons la mise en œuvre de ce projet, qui constituera la partie la plus importante de ce projet. Nous décrirons les étapes préalables ainsi que la configuration requise pour installer les différents logiciels et systèmes. Des captures d'écran accompagneront ces explications pour une meilleure compréhension.

5.2 Architecture à réaliser

L'élément clé de notre architecture proposée pour l'entreprise CEVITAL (Figure 5.1) est l'implémentation d'une infrastructure de virtualisation haute disponibilité. Cela implique la mise en place de redondance de serveurs physiques, et l'utilisation des machines virtuelles qui seront réparties de manière équilibrée et tolérante aux pannes afin de permettre une gestion flexible et évolutive des ressources informatiques. Cette approche permettra à l'entreprise de bénéficier d'une infrastructure hautement disponible, capable de gérer des charges de travail élevées de manière efficace et de répondre aux exigences de performance de l'entreprise.

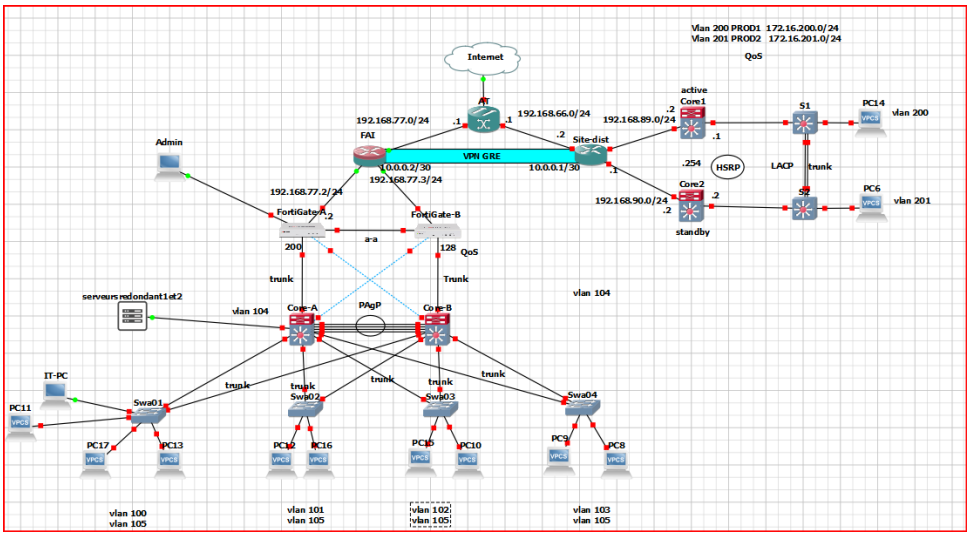


FIGURE 5.1 – Architecture de réalisation

5.3 Environnement de travail

Nous avons réaliser notre travail avec :

5.3.1 GNS3

GNS3 (Graphical Network Simulator) est un logiciel open source permettant aux utilisateurs de créer des topologies de réseau virtuelles afin de les simuler avant de les mettre en production.

FIGURE 5.2 – Logo de GNS3.

5.3.1.1 Installation de GNS3 sous Windows

Pour installer GNS3, il est nécessaire de télécharger le fichier exécutable et de le lancer pour commencer le processus d'installation jusqu'à la fin puis cliquez sur le bouton « Finish ». Une fois l'installation terminée, on peut accéder à l'interface de GNS3 qui est illustrée par la figure suivante :

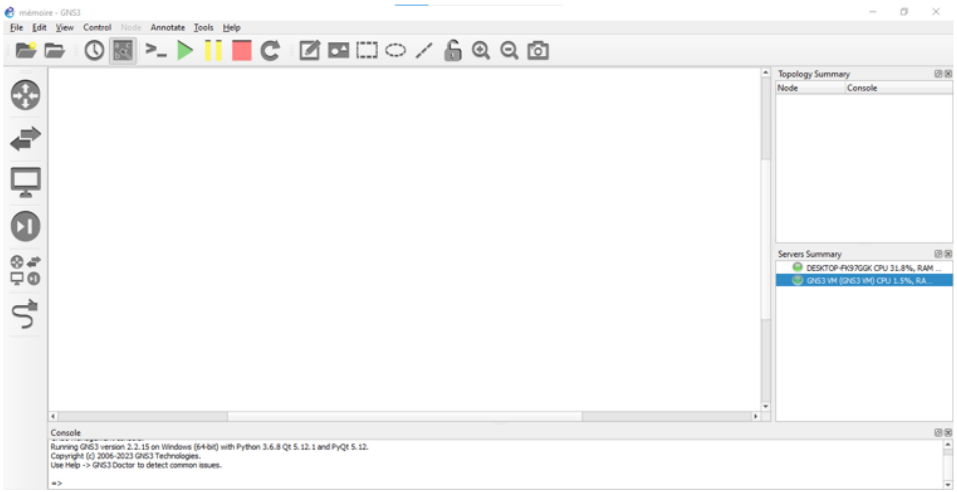


FIGURE 5.3 – L'interface principale de gns3.

5.3.2 VMware Workstation version 17.0.0

VMware Workstation est un logiciel de virtualisation d'infrastructures réseau qui permet aux utilisateurs de créer et de gérer des machines virtuelles sur leurs ordinateurs. La version installée de VMware Workstation est toujours compatible avec l'OS de la machine physique et avec les spécifications de ses machines virtuelles. Avant de télécharger

et d'installer la version choisie, il est recommandé de vérifier certaines exigences système pour éviter les problèmes de compatibilité.

FIGURE 5.4 – Logo de VMWare 17pro.

5.3.2.1 Installation VMware Workstation version 17pro

VMware Workstation est un outil qui permet aux utilisateurs de créer des machines virtuelles au sein d'un seul PC [31].

5.4 Configuration des équipements

5.4.1 La commutation

Dans cette partie nous allons entamer la partie commutation d'où nous adapterons les techniques de commutation dans les réseaux LAN pour connecter plusieurs périphériques (ordinateurs, serveurs, etc) afin de transférer les données entre leurs connexions physiques en se concentrant sur la gestion des vlans, la configuration des ports, et l'implémentation de quelques protocoles pour assurer le fonctionnement global du réseau.

5.4.1.1 Protocole trunk

la fonction principale du protocol trunk est de permettre la commutation entre plusieurs switches, ainsi que le transporter du le trafic de plusieurs vlans sur un seul port physique, dans notre cas nous avons utilisé la version 802.1Q du protocole trunk.

Configuration de trunk

Afin de configurer le protocole trunk nous suivons les commandes montrées sur la figure (Figure 5.5) effectuée sur le commutateur core-A interface ethernet 3/2 et ethernet 3/3. Nous précisons que nous avons effectué les mêmes étapes sur les autres commutateurs de notre réseaux à savoir le deuxième commutateur Core-B et les quatre commutateurs d'accès (swa01, swa02, swa03, swa04).

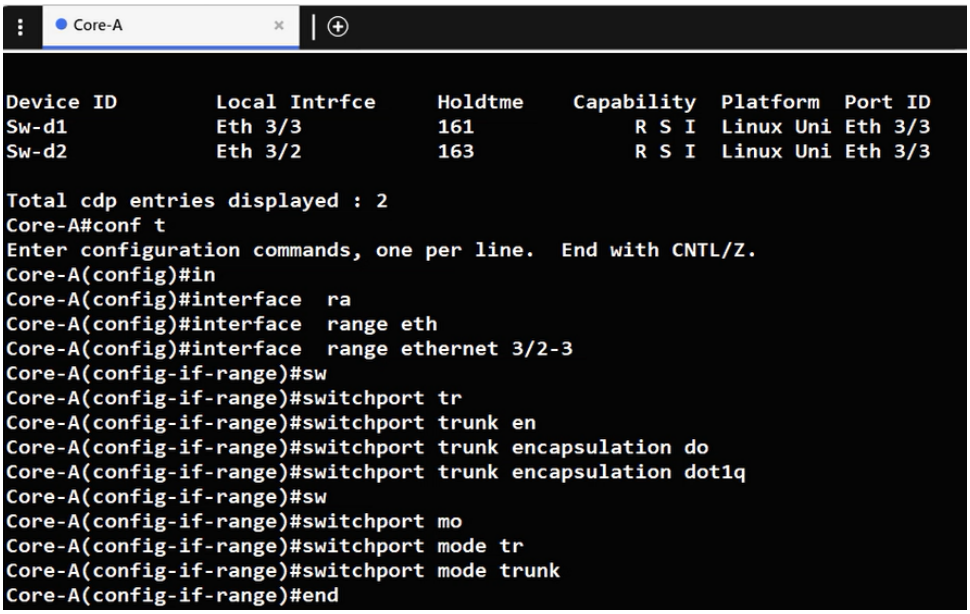


FIGURE 5.5 – Configuration du mode trunk sur core-A.

La figure suivante montre les deux interfaces que nous venons de configurer sont mises en mode trunk.

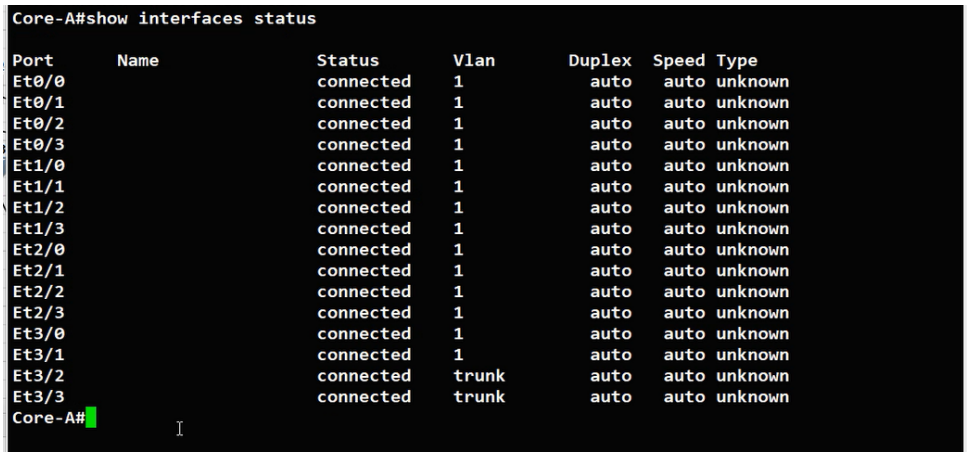


FIGURE 5.6 – Vérification de l'interface trunk pour core-A.

5.4.1.2 Protocole VTP

Le VTP joue sert à la gestion des en synchronisante leurs informations et faciliter la création et la suppression des VLANs en permettant la distribution automatique du domaine VTP aux commutateurs. Le VTP définit trois modes de fonctionnement : serveur, client, transparent.

Configuration du VTP

Nous configurons le protocole VTP (Figure 5.7) en mode serveur pour les commutateurs Core-A, Core-B ; en mode client (Figure 5.8) pour les commutateurs d'accès (swa01, swa02, swa03 et, swa04) comme montré sur les figures suivantes :

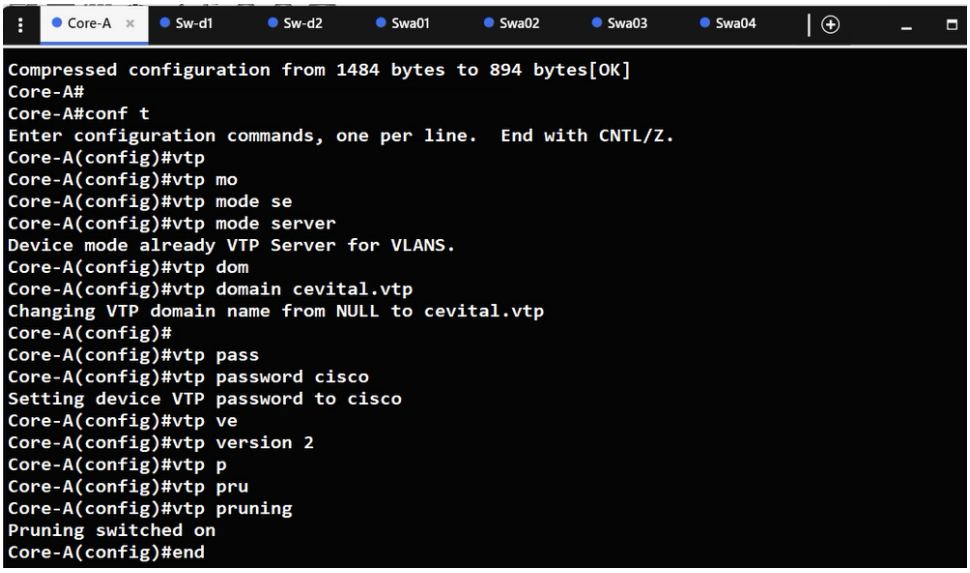


FIGURE 5.7 – Configuration du mode vtp server sur core-A.

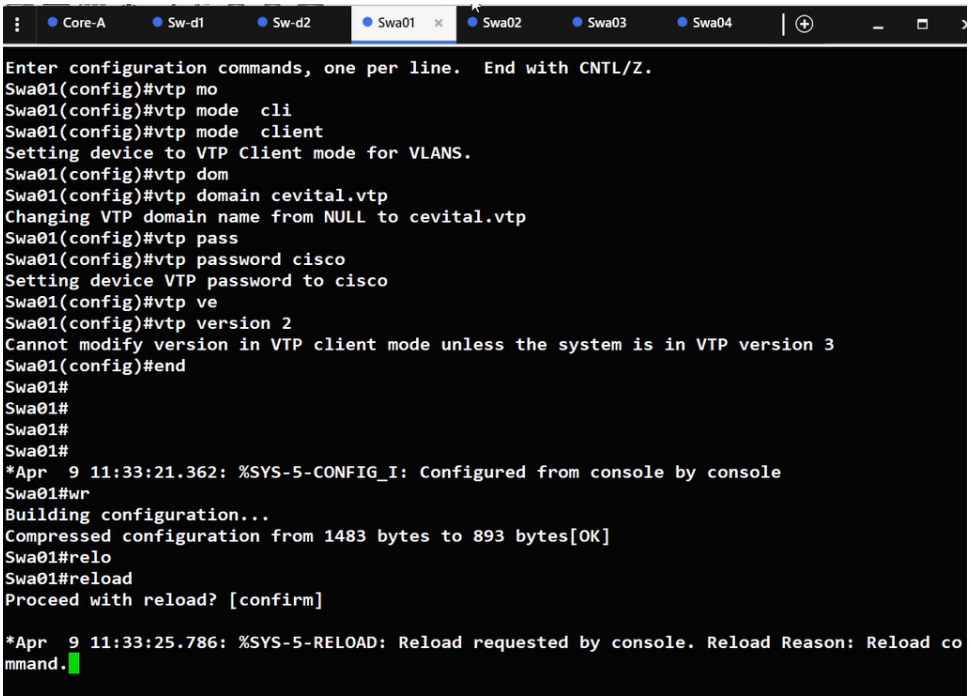


FIGURE 5.8 – Configuration du mode vtp client sur Swa01.

Une fois que nous avons terminé la configuration du VTP nous effectuons la vérification comme montré sur la figures suivantes :

FIGURE 5.9 – Verification du mode vtp serveur sur Core-A.

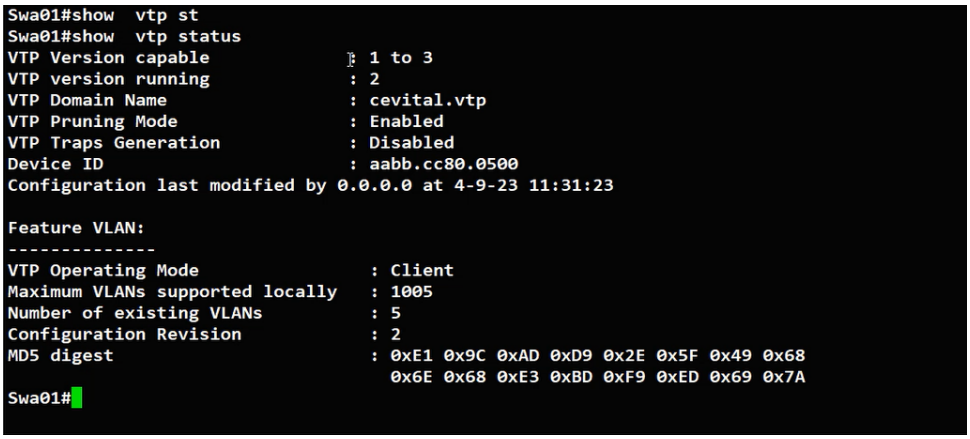


FIGURE 5.10 – Verification du mode vtp client sur Swa01.

5.4.1.3 Virtual Local Area Networks (VLANs)

La création des VLANs implique l'attribution des ports spécifiques à ces derniers et leurs assigner un identificateur (ID) unique. Dans notre cas, grâce au protocole VTP ça nous a suffi de créer les VLANs au niveau de l'un des commutateurs configurés au mode serveur la figure suivante montre l'exemple de core-A(Figure 5.11) afin de les avoir sur tous les commutateurs. La vérification est montrée sur les figures (Figure 5.12 et Figure 5.13).

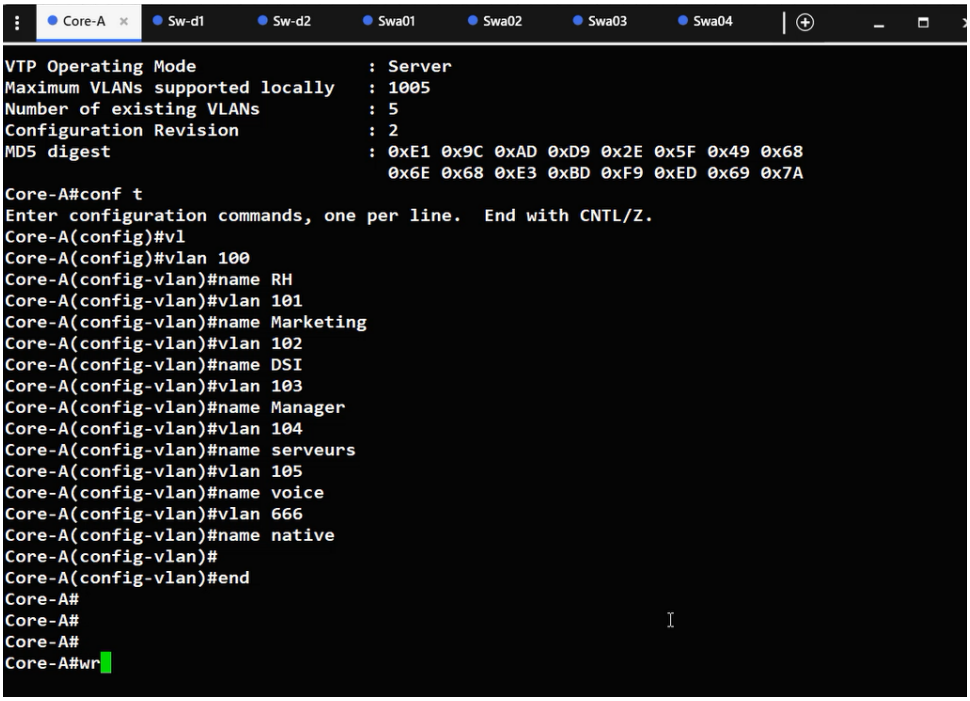


FIGURE 5.11 – Creation des VLANs.

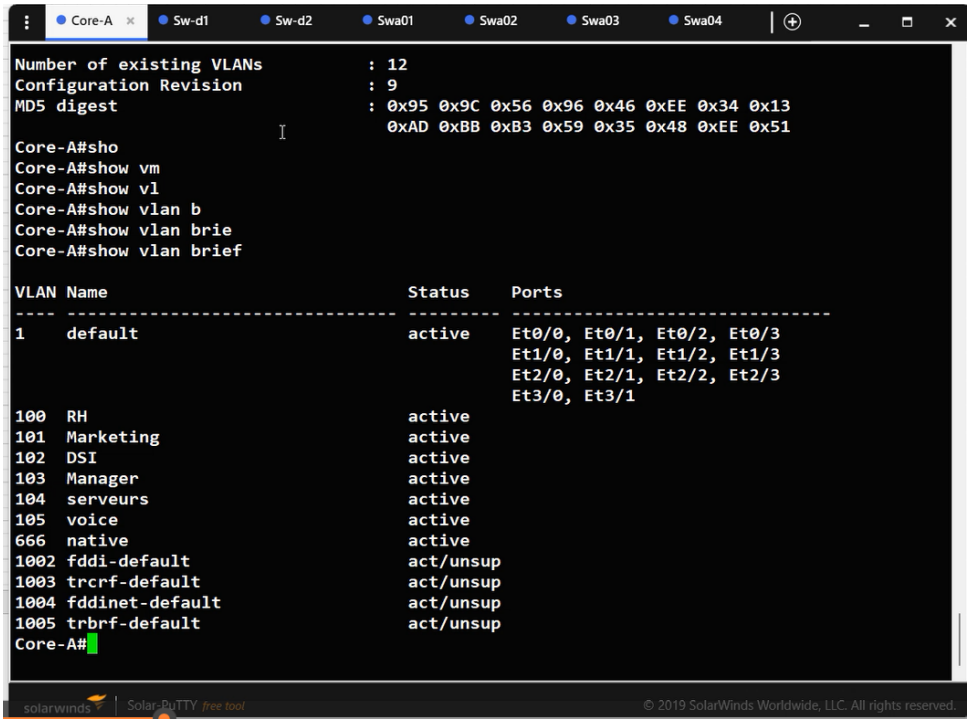


FIGURE 5.12 – Verification de la creation des VLANs sur core-A.

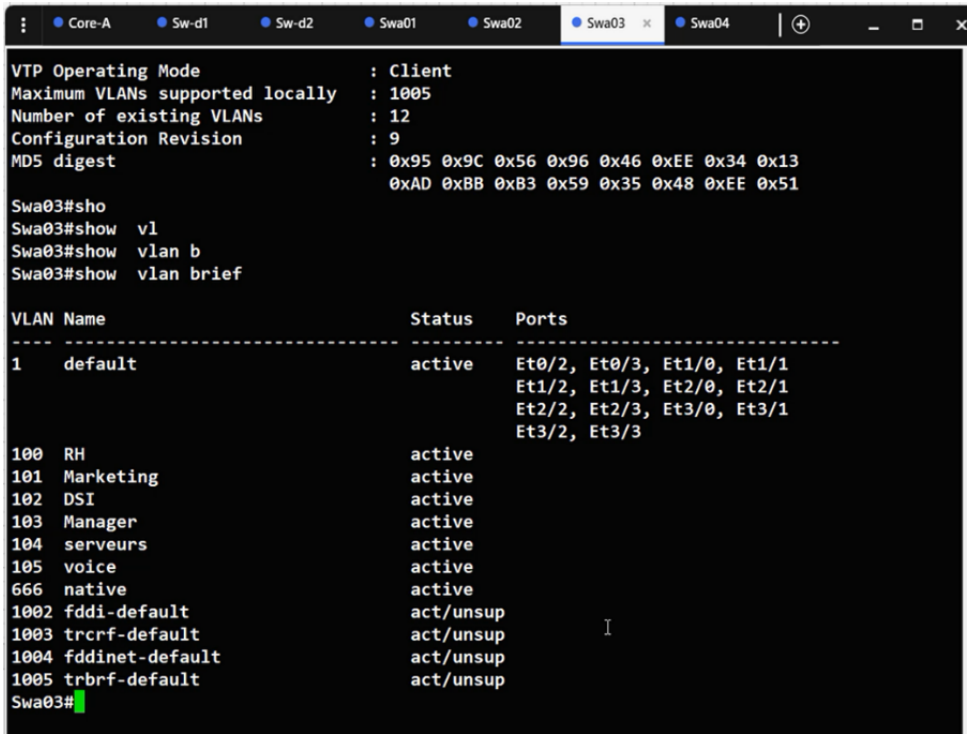


FIGURE 5.13 – Verification de la creation des VLANs sur Sw01.

Configurer VLAN Natif

Lorsque nous avons configuré le trunk entre les commutateurs (Figure 5.14), ça a permis aux trames de transir sur les liaisons marquées qu'avec des tags VLAN ce qui risque l'utilisation des VLANs ou la gestion du réseau par l'utilisateur malveillant.

Afin d'éviter cela, nous attribuons le VLAN natif pour les interfaces des commutateurs Core-A, Core-B, Swa01, Swa02, Swa03 et Swa04 voir (Figure 5.14) qui autorisent la gestion des VLANs déjà créés. La vérification de vlan natif est indiquée sur la figure(Figure 5.15).

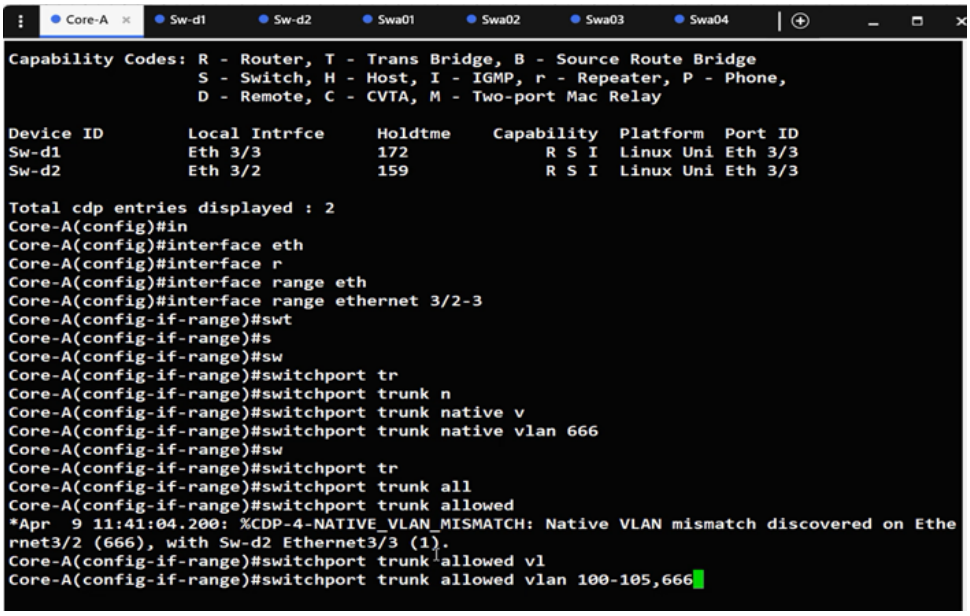


FIGURE 5.14 – Configuration de VLAN natif sur Core-A.

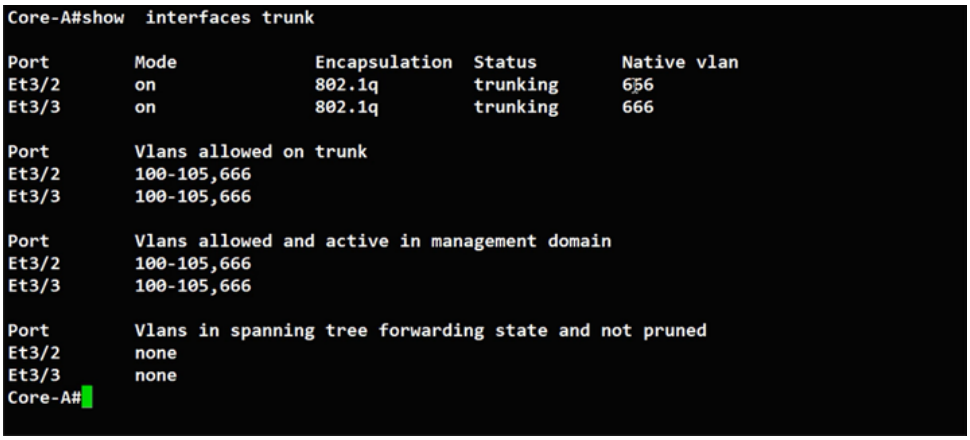


FIGURE 5.15 – Verification de VLAN natif.

Configuration de mode Access

Nous avons configuré le mode Access (voir Figure 5.16) sur les ports des commutateurs de notre architecture afin de fournir la connectivité aux appareils qui seront assignés à un VLAN spécifique ce qui limite le trafic entrant et sortant. Le résultat est montré sur la figure (Figure 5.17).

```
Swa02(config)#interface  range ethernet 0/2-3
Swa02(config-if-range)#sw
Swa02(config-if-range)#switchport mo
Swa02(config-if-range)#switchport mode  acc
Swa02(config-if-range)#switchport mode  access
Swa02(config-if-range)#
Swa02(config-if-range)#sww
Swa02(config-if-range)#sw
Swa02(config-if-range)#switchport acc
Swa02(config-if-range)#switchport access vl
Swa02(config-if-range)#switchport access vlan 101
Swa02(config-if-range)#sw
Swa02(config-if-range)#switchport voi
Swa02(config-if-range)#switchport voice vl
Swa02(config-if-range)#switchport voice vlan 105
Swa02(config-if-range)#end
Swa02#
Swa02#
Swa02#wr
Building configuration...
```

FIGURE 5.16 – Configuration de mode accès sur le Swa02 le vlan 101.

```
Swa03#show  vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
100  RH                               active
101  Marketing                        active
102  DSI                              active    Et0/2, Et0/3
103  Manager                          active
104  serveurs                         active
105  voice                            active    Et0/2, Et0/3
666  native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

FIGURE 5.17 – Vérification mode accès sur le Swa02 le vlan 101.

5.4.1.4 Configuration de protocole PAgP

Nous présentons la configuration du protocole PAgP, qui est du niveau 2 du modèle TCP/IP afin de l'utiliser pour agréger les liens physiques entre le Core-A (Figure 5.18) et le Core-B, pour former un lien logique de plus grande capacité et de redondance. Le PAgP va nous permettre de créer un groupe de ports qui est « port channel-group 1 » en combinant les 4 interfaces reliant les commutateurs Core-A et Core-B.

```
Core-A(config)#interface r
Core-A(config)#interface range eth
Core-A(config)#interface range ethernet 0/0-3
Core-A(config-if-range)#chann
Core-A(config-if-range)#channel-g
Core-A(config-if-range)#channel-group 1 mode de
Core-A(config-if-range)#channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
```

FIGURE 5.18 – Configuration de protocole PAgP sur le Core-A en le mode « desirable ».

Pour s'assurer que ce mode est activé, il est nécessaire de vérifier comme suite :

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

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

        A - formed by Auto LAG


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Et0/0(P)    Et0/1(P)    Et0/2(P)
                                 Et0/3(P)
```

FIGURE 5.19 – Vérification de protocole PAgP sur le Core-A.

5.4.2 Le Routage

La mise en place de routage efficace pour notre réseau est fondamentale afin d'avoir une connectivité entre les différents réseaux. Dans cette partie, nous aborderons la configuration du routage dans notre infrastructure réseau, en mettaent l'accent sur les meilleurs pratiques et conceptions.

5.4.2.1 Configuration de pare-feu

Pour configurer le pare-feu nous avons trois étapes détaillées dans ce qui suit :

Configuration des interfaces

Afin de configurer le pare-feu primaire de type FortiGate, nous commençons par la configuration des interfaces du port de ce dernier (Figure 5.20, Figure 5.21 et Figure 5.22) qui seront utilisées pour le routage, ensuite nous le configurons en tant que passerelle par défaut voir toujours (Figure 5.20, Figure 5.21 et Figure 5.22) pour les périphériques du réseau interne et attribuer les adresses IP statiques pour ces interfaces. Cela permettra au

trafic provenant des périphériques internes d'être acheminés via le pare-feu pour accéder à des réseaux externes.

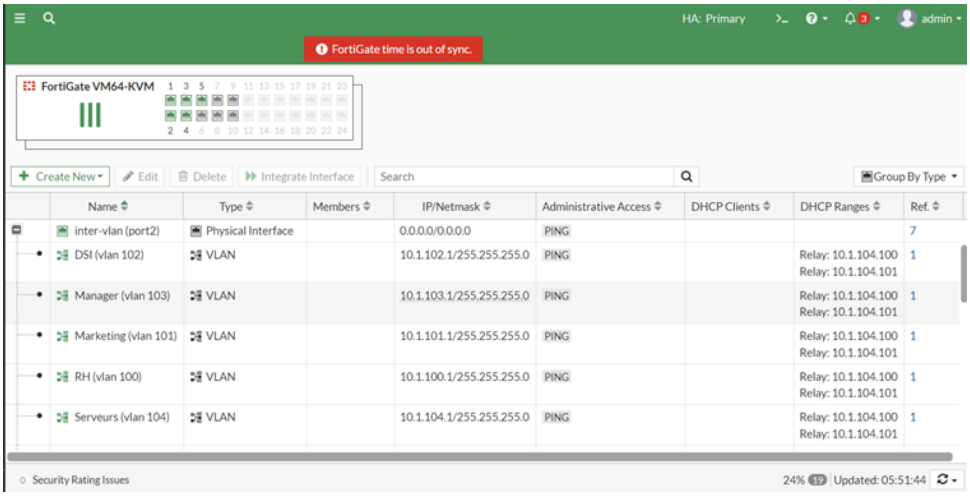


FIGURE 5.20 – Configuration de l'interface port 2.

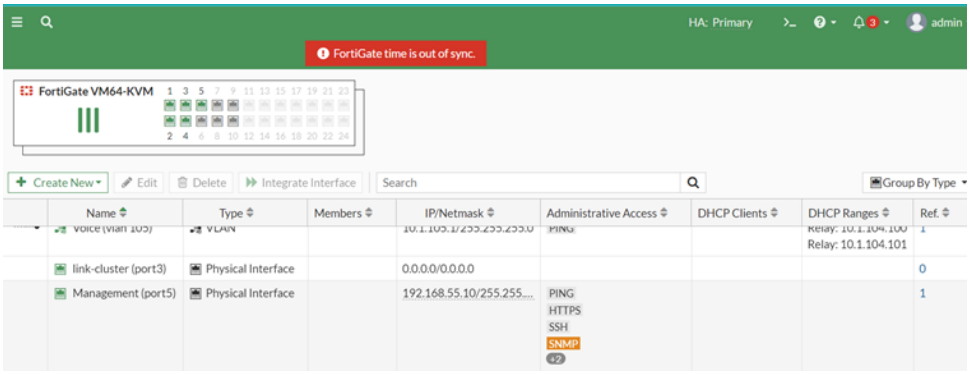


FIGURE 5.21 – Configuration de l'interface port 5.

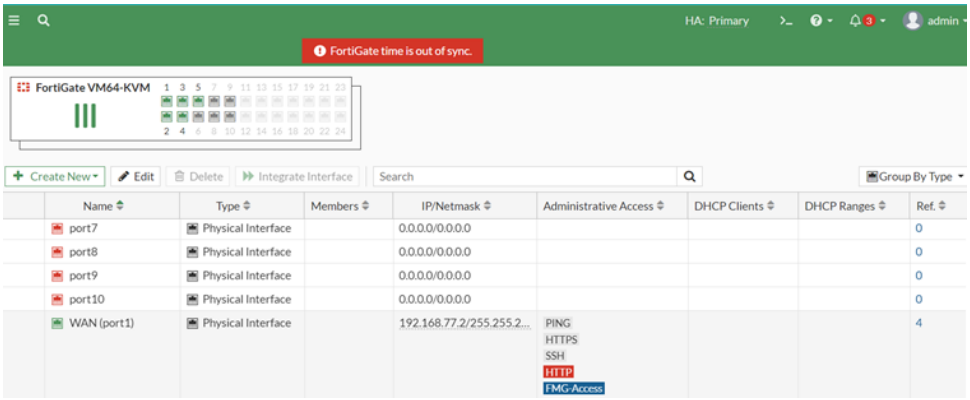


FIGURE 5.22 – Configuration de l'interface port 1.

En troisième lieu, nous englobons les VLANs créés dans les interfaces du pare-feu primaire dans une même zone dont le but est d'assurer le routage inter-VLAN de notre réseau interne.

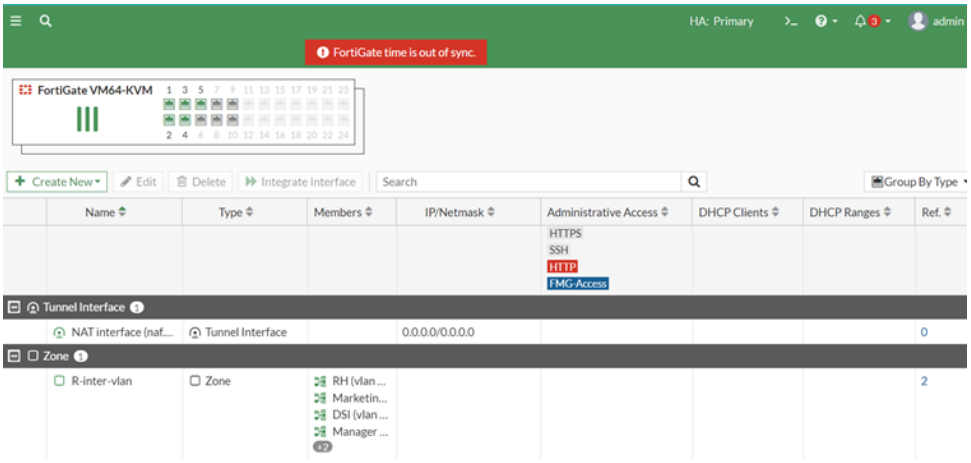


FIGURE 5.23 – Création de la zone.

Configuration de High Availability (HA) sur les deux pare-feu

Dans cette étape, nous intéressons au déploiement d'un deuxième pare-feu FortiGate-B qui sera considérer comme secondaire, afin de former une paire de pare-feu actif-actif (Figure 5.24, Figure 5.25), pour qu'ils puissent fonctionner ensemble et de fournir une redondance et une résilience, garantissant le trafic réseau qui peut toujours être filtré et sécurisé, même en cas de défaillance du pare-feu FortiGate-A qui est d'une priorité élevée que celle par défaut afin de déterminer qu'il est prioritaire.

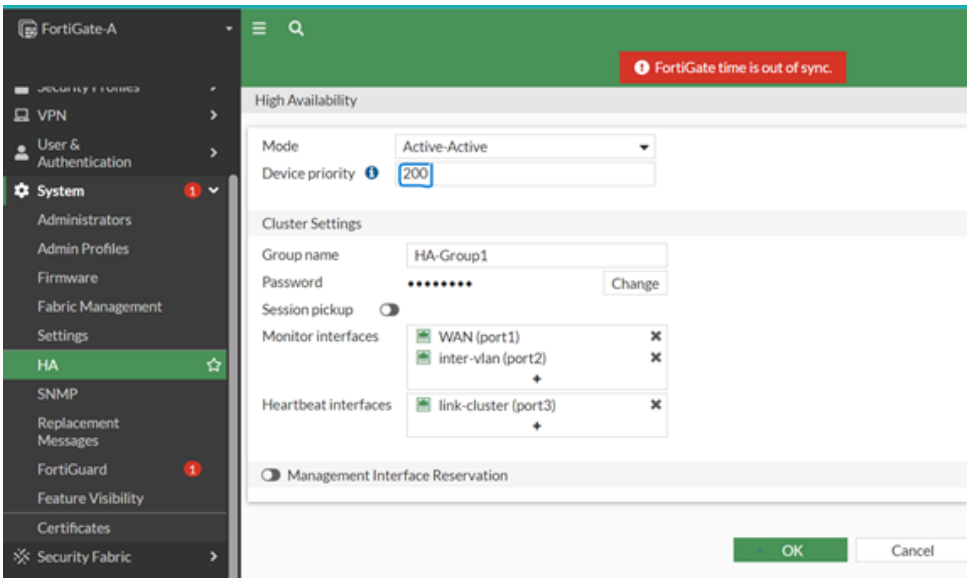


FIGURE 5.24 – Configuration de HA redondant sur le FortiGate-A.

```
FortiGate-B # config system ha

FortiGate-B (ha) # set mode a-a

FortiGate-B (ha) # set group-name HA-Group1

FortiGate-B (ha) # set password 123456

FortiGate-B (ha) # set session pi
ambiguous command before 'session'

FortiGate-B (ha) # set session-pickup enable

FortiGate-B (ha) # set hbdev port3 0

FortiGate-B (ha) # end

FortiGate-B #
```

FIGURE 5.25 – Configuration de HA sur le pare-feu FortiGate-B.

La figure ci-dessous montre la réussite de la configuration de HA :

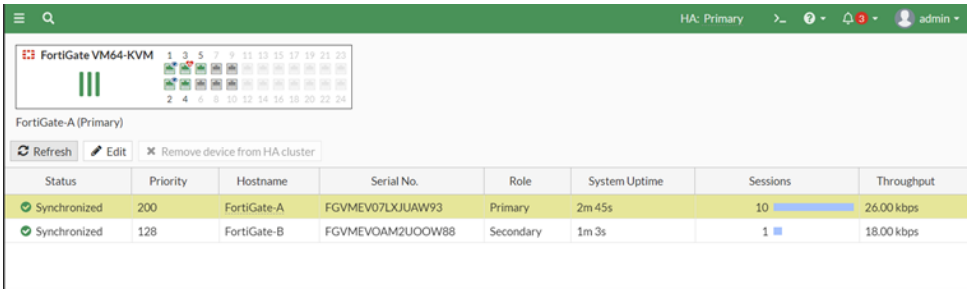


FIGURE 5.26 – Vérification du configuration de HA.

Création des règles de pare-feu

Nous configurons les règles de routage sur notre pare-feu, afin de contrôler précisément le flux de trafic réseau, en déterminant les chemins empruntés par les paquets de données. Cela nous permet de diriger le trafic vers les destinations appropriées, de bloquer les communications non autorisées et de garantir la sécurité de notre réseau selon nos propres politiques définies.

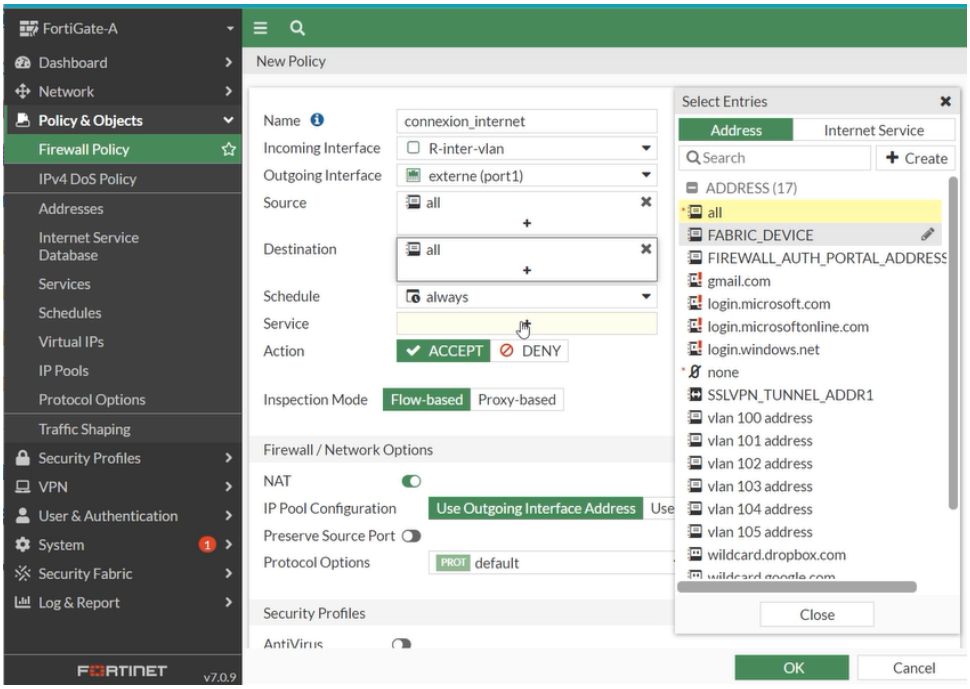


FIGURE 5.27 – Définition la régle de routage de réseau local vers l'externe.

5.4.2.2 Installation et configuration de Serveur DHCP

Nous installons le serveur DHCP (Figure 5.29), qui permet d'attribuer automatiquement des adresses IP aux clients de réseau. Cela évite la nécessité de configurer manuellement chaque appareil avec une adresse IP statique en définissant les plages d'adresses IP disponibles. Préalablement à cela, il est recommandé d'intégrer un contrôleur de domaine (Figure 5.28), dans ce serveur DHCP afin d'offrir une intégration plus étroite avec l'infrastructure Active Directory pour une authentification centralisée des clients DHCP cela simplifier la gestion du réseau et renforce la sécurité et la stabilité de notre LAN.

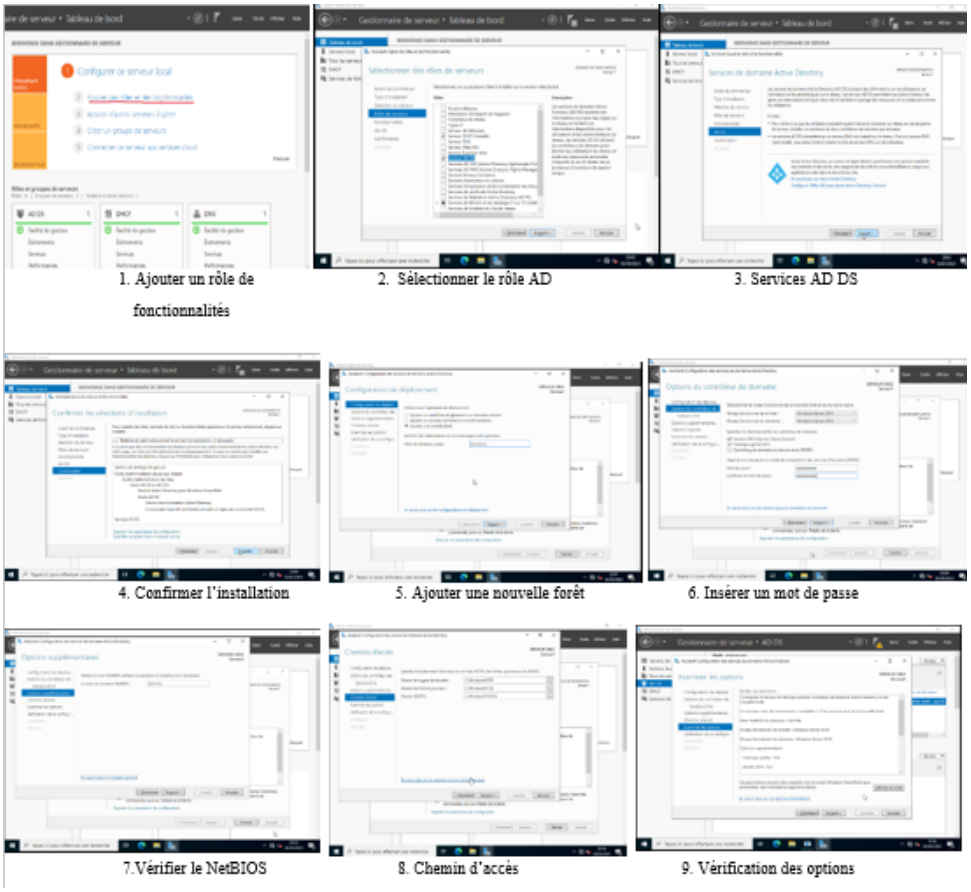
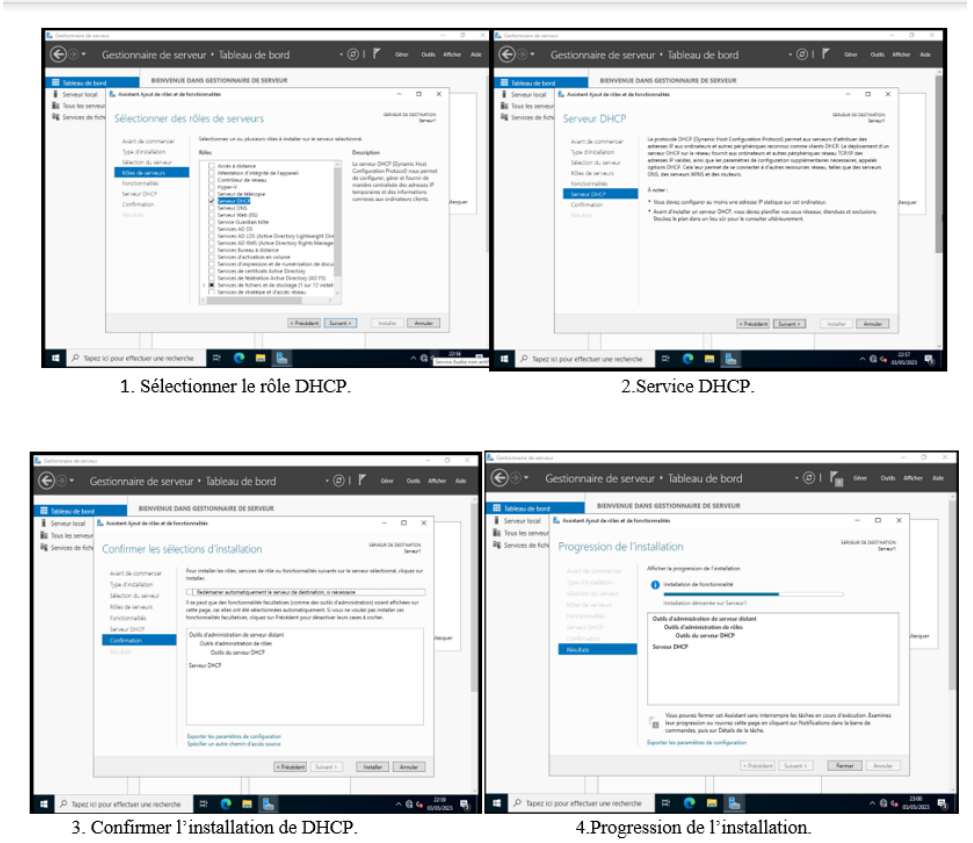


FIGURE 5.28 – Installation de serveur AD.



1. Sélectionner le rôle DHCP. 2.Service DHCP.

3. Confirmer l'installation de DHCP. 4.Progression de l'installation.

FIGURE 5.29 – Installation de serveur DHCP.

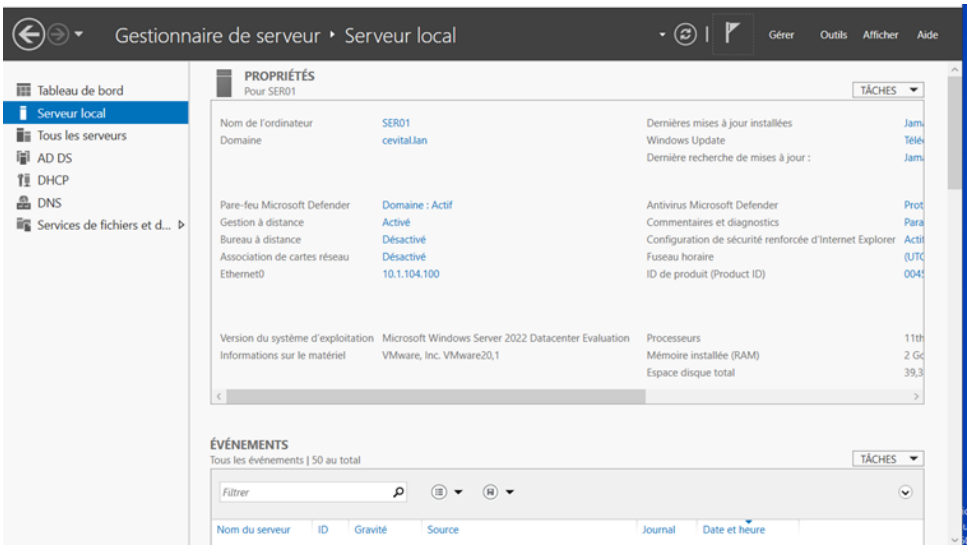


FIGURE 5.30 – Interface principale de serveur après la configuration de service AD et DHCP.

Nous définissons les étendus d'adresses IP disponibles pour les clients DHCP en spécifiant l'adresse de début et l'adresse de fin du l'étendue, ainsi que d'autres options telles que la durée de bail (lease duration) pour les adresses IP (Figure 5.31).

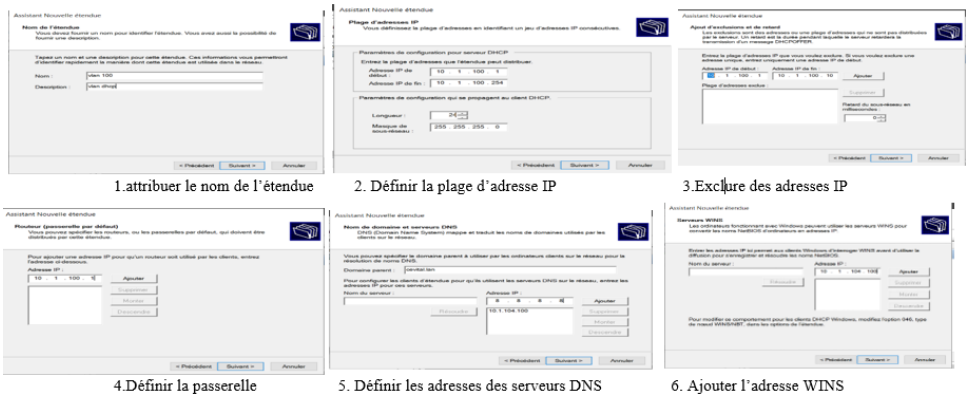


FIGURE 5.31 – Créer l'entendue 100 sur le ser01.

Configuration du basculement sur le serveur DHCP :

Dans notre environnement, il est important d'avoir une redondance du serveur DHCP pour assurer la continuité de ses services en cas de panne. Nous pouvons configurer une architecture de basculement actif-passif, où le deuxième serveur DHCP travaille ensemble avec le premier pour fournir des adresses IP aux clients.

Configuration de la synchronisation des données :

Afin de s'assurer que les données DHCP, y compris les baux d'adresses IP et les options de configuration, sont synchronisées entre les deux serveurs DHCP redondants il est nécessaire de configurer le basculement de chaque étendue en ajoutant le mode de basculement soit serveur de secours ou bien équilibrage de charge (Figure 5.32) ainsi cela il est indiqué avec un ajout de l'adresse IP de deuxième serveur, cette opération garantit que ces serveurs DHCP ont les mêmes informations et peuvent répondre aux demandes des clients de manière cohérente.

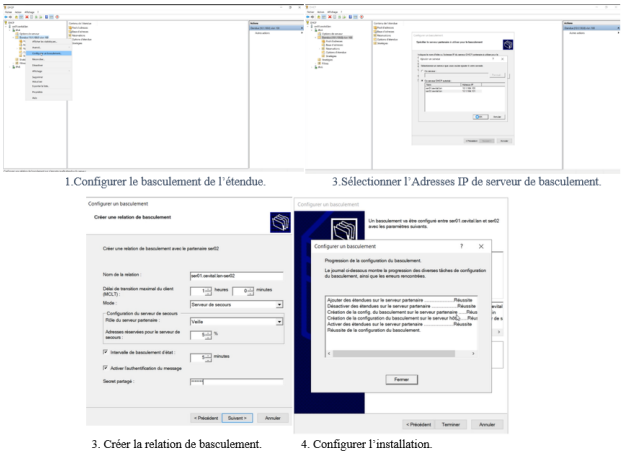


FIGURE 5.32 – Configuration de basculement de l'étendu.

5.4.3 La configuration du site distant

Dans le cadre de notre déploiement d'infrastructure réseau, la configuration d'un deuxième site (Figure 5.33) est d'une importance cruciale pour étendre nos capacités

et assurer la redondance de nos services. En ajoutant un deuxième site, nous sommes en mesure d'améliorer la disponibilité de nos services, de garantir la continuité de nos activités et de répartir la charge entre nos différentes localisations.

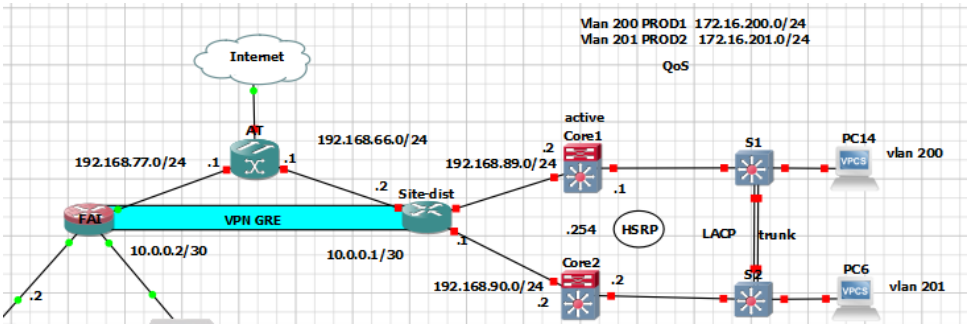


FIGURE 5.33 – L'architecture de site distant.

La configuration de site distant suit pratiquement les mêmes étapes que celles de la configuration du LAN du site précédent à la différence des protocoles de redondance.

5.4.3.1 Les VLANs

A chaque VLAN nous avons attribué un identifiant numérique ainsi qu'un nom distinct, favorisant ainsi une gestion efficace de notre réseau. Voici les deux VLANs configurés (Figure 5.34 et Figure 5.35) :

— VLAN 200 - VLAN PROD1
- Numéro d'identification : 200.
- Nom : PROD1.

— VLAN 201 - VLAN PROD2
- Numéro d'identification : 201.
- Nom : PROD2.

```
S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
200  PROD1                            active    Et0/0
201  PROD2                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1#
```

FIGURE 5.34 – Vérification de VLAN sur S1.

```
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
200  PROD1                            active
201  PROD2                            active    Et0/0
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S2#
```

FIGURE 5.35 – Vérification des VLANs sur S2.

5.4.3.2 Activer le routage inter-VLANs

Cette fonctionnalité permettra aux deux VLANs de communiquer entre eux, facilitant ainsi le partage des ressources et des services au sein de notre infrastructure en activant le routage inter-VLAN sur le core1 et le core2 (Figure 5.36) :

```
Core1  Core2  S1  S2  PC14  PC6
*Apr 10 09:51:04.500: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Apr 10 09:51:04.500: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname core2
core2(config)#interface Ethernet0/1
core2(config-if)# ip address 192.168.89.2 255.255.255.0
core2(config-if)#interface Ethernet0/0
core2(config-if)#no shutdown
core2(config-if)#interface Ethernet0/0.200
core2(config-subif)# encapsulation dot1Q 200
core2(config-subif)# ip address 172.16.200.2 255.255.255.0
core2(config-subif)# shutdown
core2(config-subif)#
core2(config-subif)#interface Ethernet0/0.201
core2(config-subif)# encapsulation dot1Q 201
core2(config-subif)# ip address 172.16.201.2 255.255.255.0
core2(config-subif)#
core2(config-subif)#ip route 0.0.0.0 0.0.0.0 192.168.90.1
core2(config)#
core2(config)#
core2(config)#end
core2#
core2#
core2#
core2#
*Apr 10 09:51:37.124: %SYS-5-CONFIG_I: Configured from console by console
core2#w
```

FIGURE 5.36 – Configuration de routage inter-VLANs Core2.

5.4.3.3 Configuration de mode trunk

Nous avons entrepris de configurer le mode trunk (Figure 5.37 et Figure 5.38) sur nos équipements réseau. En utilisant les instructions de configuration spécifiques que nous avons déjà mis en place lors de configuration de LAN, nous avons établi des liens de

trunk entre nos deux commutateurs, permettant ainsi le transport simultané de VLANs (PROD1 et PROD2) sur une seule interface physique.

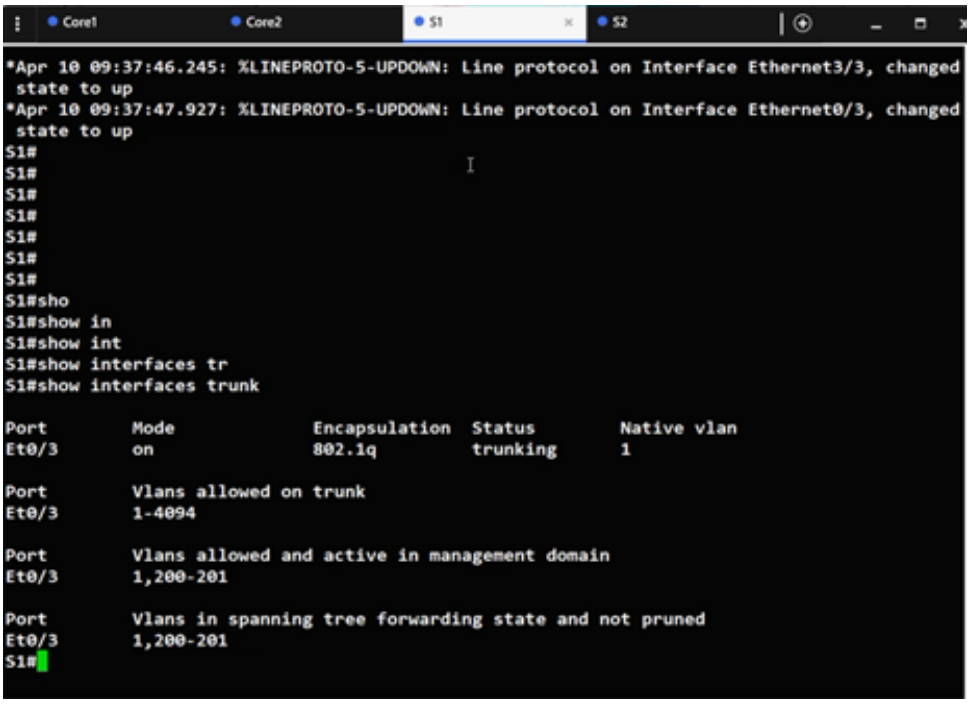


FIGURE 5.37 – Vérification de mode trunk sur le commutateur S1.

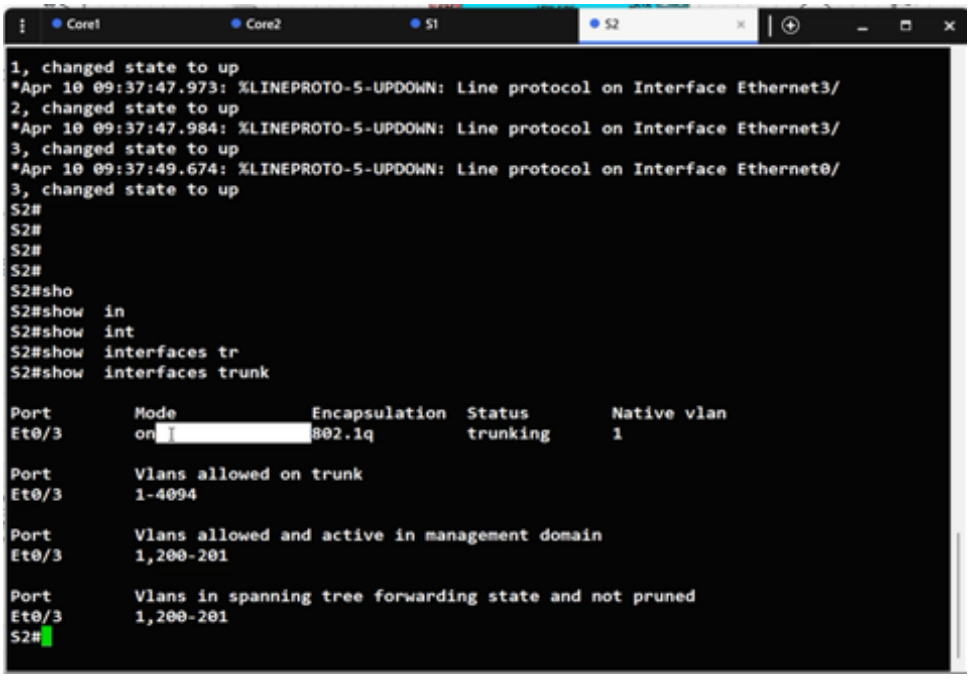


FIGURE 5.38 – Vérification de mode trunk sur le commutateur S2.

Nous allons attribués une adresses IP pour le P6 de VLAN 201 (Figure 5.39)

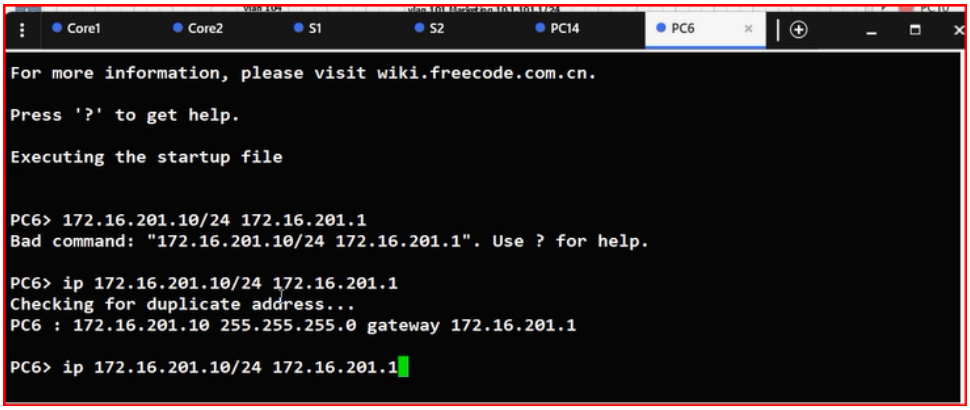


FIGURE 5.39 – Attribution de l'adresse IP pour le PC6.

5.4.3.4 Configuration de protocole Link Aggregation Configuration (LACP)

En configurant le protocole LACP (Figure 5.40) sur les deux commutateurs (S1 et S2), nous pouvons combiner plusieurs liens physiques pour former un seul lien logique à plus grande capacité. Cela permet d'augmenter la bande passante disponible et d'améliorer les performances du réseau.
LACP joue un rôle essentiel dans la prévention des boucles de commutation et dans l'amélioration de la résilience du réseau, en particulier en relation avec le Spanning Tree Protocol (STP).

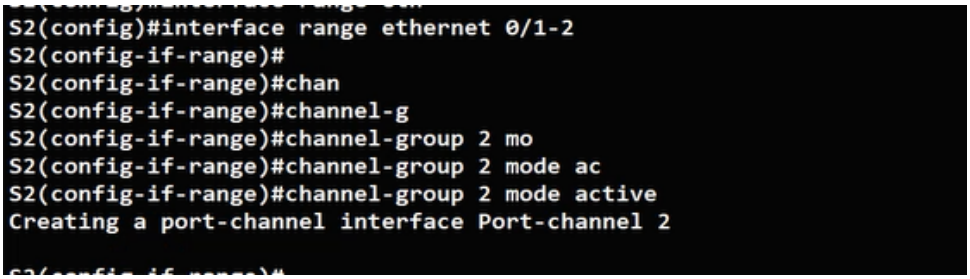


FIGURE 5.40 – Configuration de protocole LACP sur le commutateur S2.

5.4.3.5 Configuration de protocole Host Standby Router (HSRP)

En configurant le protocole HSRP (Hot Standby Router Protocol), nous mettons en place une solution de redondance de passerelles par défaut pour assurer une haute disponibilité et la fiabilité en fournissant une redondance de passerelle par défaut, le basculement automatique et la répartition de charge de notre réseau.
Le protocole HSRP nous permet de créer un groupe virtuel de commutateur niveau 3 de modèle TCP/IP, où commutateur Core1 est désigné actif (Active) (Figure 5.41) et le Core2 comme un commutateur de secours (Standby) (figure 5.42). Le Core1 actif répondra aux requêtes des hôtes du réseau et sera utilisé comme passerelle par défaut (172.16.200.254/24, 172.16.201.254/24) tandis que les routeurs de secours resteront en attente, prêts à prendre le relais en cas de défaillance du routeur actif.

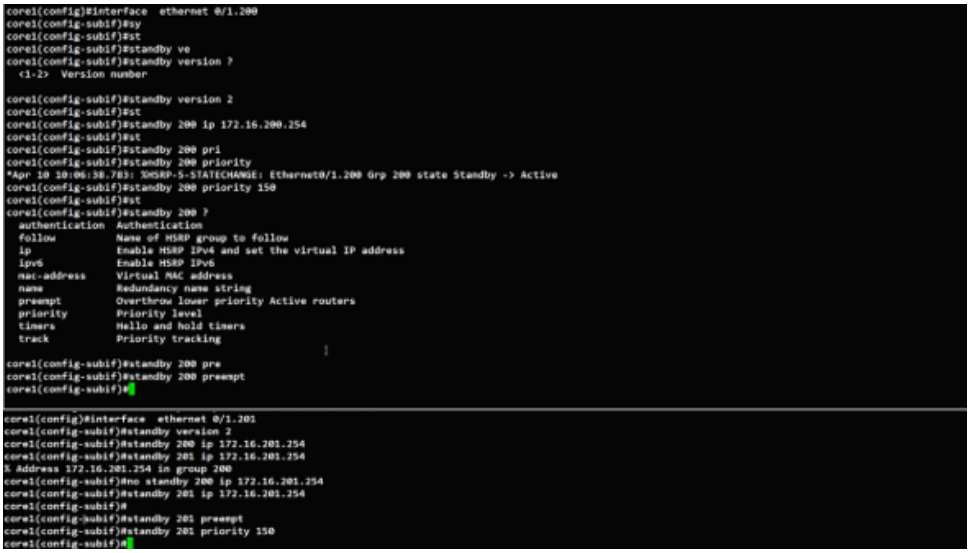


FIGURE 5.41 – Configuration de protocole HSRP sur le Core1 en mode active.

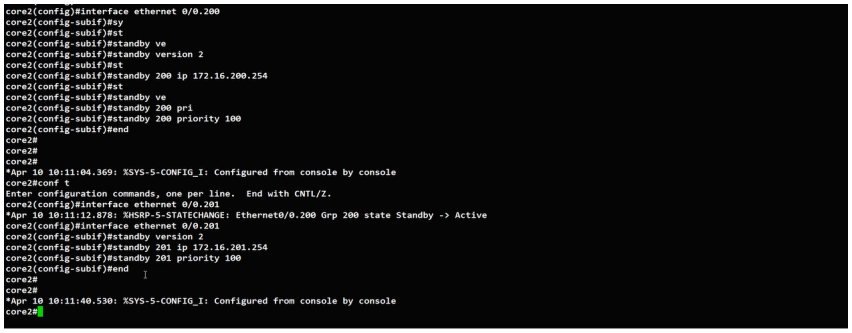


FIGURE 5.42 – Configuration de protocole HSRP sur le Core2 en mode standby.

Nous allons vérifier le mode de core-A voir la figure (Figure 5. 43)

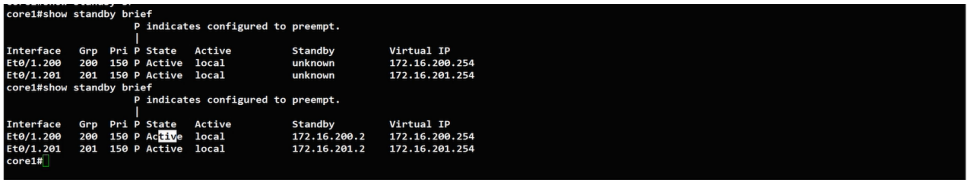


FIGURE 5.43 – Vérification de protocole HSRP sur le Core1 en mode active.

5.4.3.6 Configuration de tunnel VPN GRE

Lorsque nous configurons un tunnel VPN GRE (Generic Routing Encapsulation), nous mettons en place une connexion virtuelle entre deux sites distants de notre réseau. Cette configuration nous permet de créer une interface tunnel (Figure 5.44) qui encapsule les paquets IP ainsi les mêmes configurations pour l'autre router, permettant ainsi le transit sécurisé de données entre les sites, nous allons vérifier création de l'interface voir (Figure 5.45). Pour configurer le VPN GRE, nous suivons les étapes suivantes :

```
site-dist(config)#interface Tunnel1
site-dist(config-if)#tunnel mode gre ip
site-dist(config-if)#ip address 10.0.0.1 255.255.255.252
site-dist(config-if)#tunnel sour
site-dist(config-if)#tunnel source 192.168.66.2
site-dist(config-if)#tunnel des
site-dist(config-if)#tunnel destination 192.168.77.2
site-dist(config-if)#do wr
```

FIGURE 5.44 – Configuration de VPN GRE sur le site-dist.

```
interface Tunnel1
 ip address 10.0.0.1 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 192.168.66.2
 tunnel destination 192.168.77.2
!
interface Ethernet0/0
 ip address 192.168.66.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/1
 ip address 192.168.89.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet0/2
 ip address 192.168.90.1 255.255.255.0
!
 --More--
```

FIGURE 5.45 – Vérification de VPN GRE sur le site-dist.

Après Avoir créé notre interface tunnel sur le routeur site-dist il est sûr que la création sera réalisée au niveau de pare-feu par les instructions voir la figure (Figure 5.46) puis la vérification de création du tunnel comme la montre la figure (5.47) :

```
FortiGate-A # config system gre-tunnel

FortiGate-A (gre-tunnel) # edit GRE-SITEDIST
new entry 'GRE-SITEDIST' added

FortiGate-A (GRE-SITEDIST) # set interface port1

FortiGate-A (GRE-SITEDIST) # set  remote-gw 192.168.66.2

FortiGate-A (GRE-SITEDIST) # set local-gw 192.168.77.2

FortiGate-A (GRE-SITEDIST) # next

FortiGate-A (gre-tunnel) # end

FortiGate-A # config system interface

FortiGate-A (interface) # edit GRE-SITEDIST

FortiGate-A (GRE-SITEDIST) # set vdom root

FortiGate-A (GRE-SITEDIST) # set ip 10.0.0.2 255.255.255.255

FortiGate-A (GRE-SITEDIST) # set allowaccess ping

FortiGate-A (GRE-SITEDIST) #
FortiGate-A (GRE-SITEDIST) # set  snmp-index 88

FortiGate-A (GRE-SITEDIST) # set interface port1
```

FIGURE 5.46 – Configuration de VPN GRE sur le FortiGate-A.

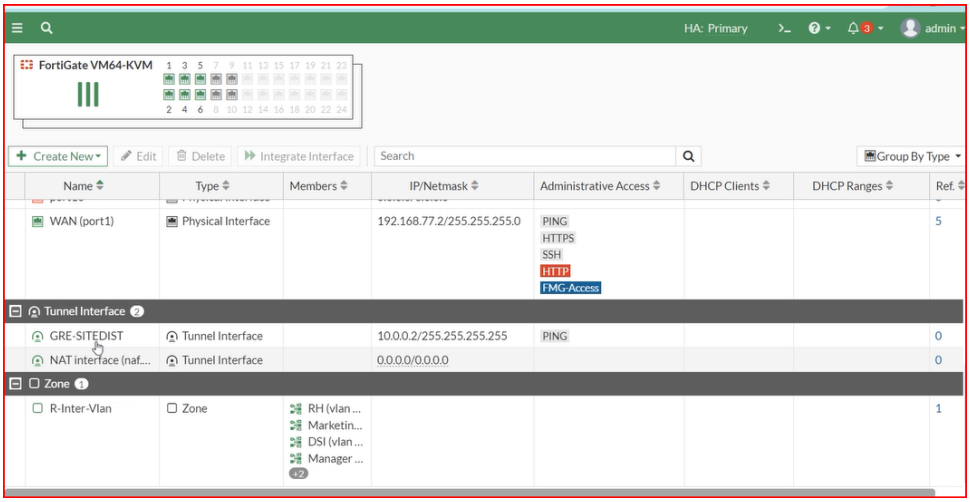


FIGURE 5.47 – Vérification de la création de tunnel-GRE au niveau de FortiGate-A.

Lorsque nous créons un tunnel GRE, nous devons prendre en compte les règles de pare-feu et le routage statistique. Pour garantir la sécurité et le bon fonctionnement du tunnel, il est essentiel de configurer les règles de pare-feu de manière appropriée. Nous devons définir des régles de sécurité qui autorisent spécifiquement le trafic à travers le tunnel GRE (Figure 5.48 et Figure 5.49), tout en bloquant les paquets indésirables. Cela permet de contrôler et de filtrer le trafic entrant et sortant du tunnel.

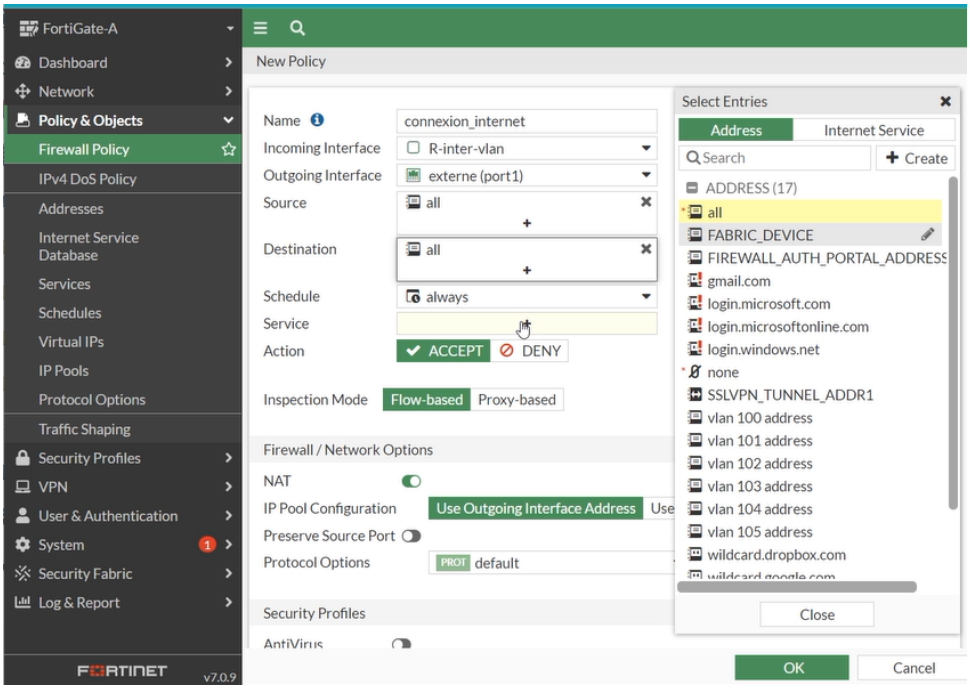


FIGURE 5.48 – La règle 1 du pare-feu FortiGate-A.

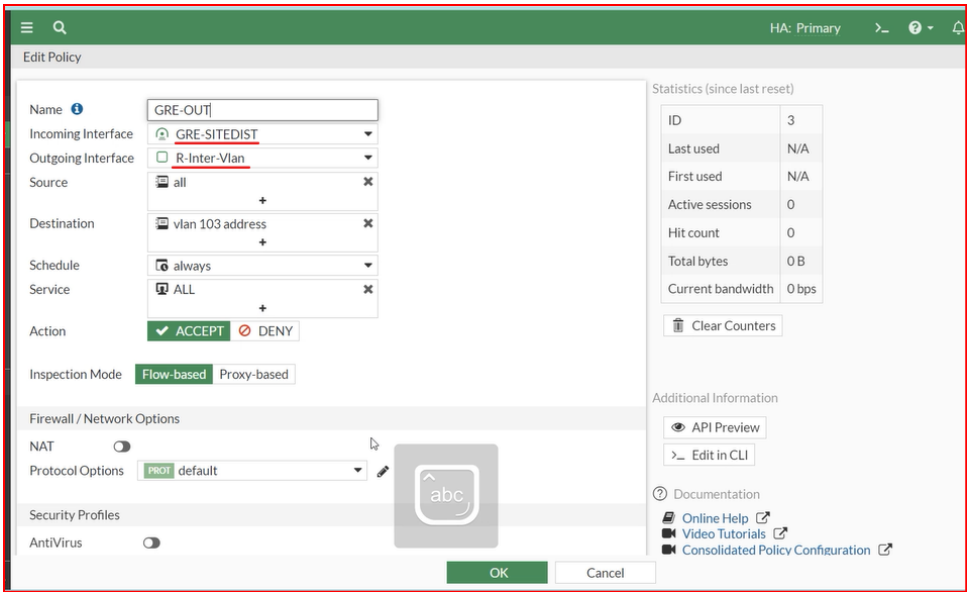


FIGURE 5.49 – La règle 2 du pare-feu FortiGate-A.

De plus, nous devons configurer le routage statistique (Figure 5.50) pour déterminer le chemin optimal pour acheminer les paquets à travers le réseau. Cette fonctionnalité nous permet de prendre en compte les différentes métriques et conditions de réseau pour garantir une transmission efficace des données à travers le tunnel GRE. En combinant la configuration adéquate des règles de pare-feu et du routage statistique, nous assurons la sécurité, la fiabilité et les performances optimales du tunnel GRE. Nous avons aussi augmenté la priorité de cette route statique vers 2 afin qu'il y'aura pas un décalage de la priorité de la route par défaut.

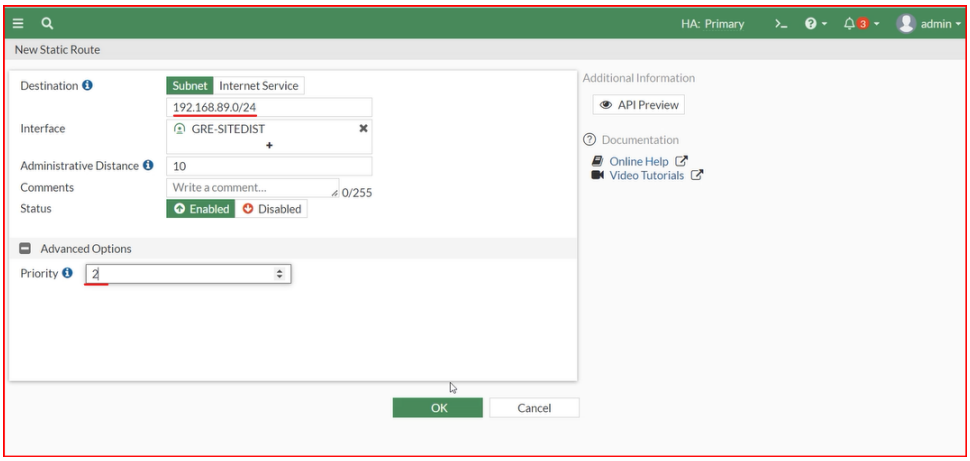


FIGURE 5.50 – Configuration de règle de routage de site distant vers le LAN.

5.5 Tester la haute disponibilité du réseau

Afin de tester le bon fonctionnement de notre réseau LAN et de s'assurer qu'il est opérationnel, nous allons simuler un ping continu de l'un des VLANs vers une autre interface :

5.5.1 Test de l'attribution de l'adresse IP à un PC par le serveur DHCP

L'attribution des adresses IP aux machines de l'organisme se fait d'une manière dynamique grâce au serveur DHCP, comme le montre la figure (Figure 5.51) :

```
PC13> ip dhcp
DORA IP 10.1.100.11/24 GW 10.1.100.1

PC13> show ip

NAME        : PC13[1]
IP/MASK     : 10.1.100.11/24
GATEWAY     : 10.1.100.1
DNS         : 10.1.104.100  8.8.8.8
DHCP SERVER : 10.1.104.100
DHCP LEASE  : 86382, 86400/43200/75600
DOMAIN NAME : cevital.lan
MAC         : 00:50:79:66:68:0b
LPORT       : 20113
RHOST:PORT  : 127.0.0.1:20114
MTU         : 1500
```

FIGURE 5.51 – Configuration de règle de routage de site distant vers le LAN.

5.5.2 Teste le basculement entre le serveur1 et le serveur2

Lorsque nous désactivons le serveur1 DHCP voir la figure(Figure 5.52), le service DHCP peut se basculer vers l'autre serveur disponible (Figure 5.53)

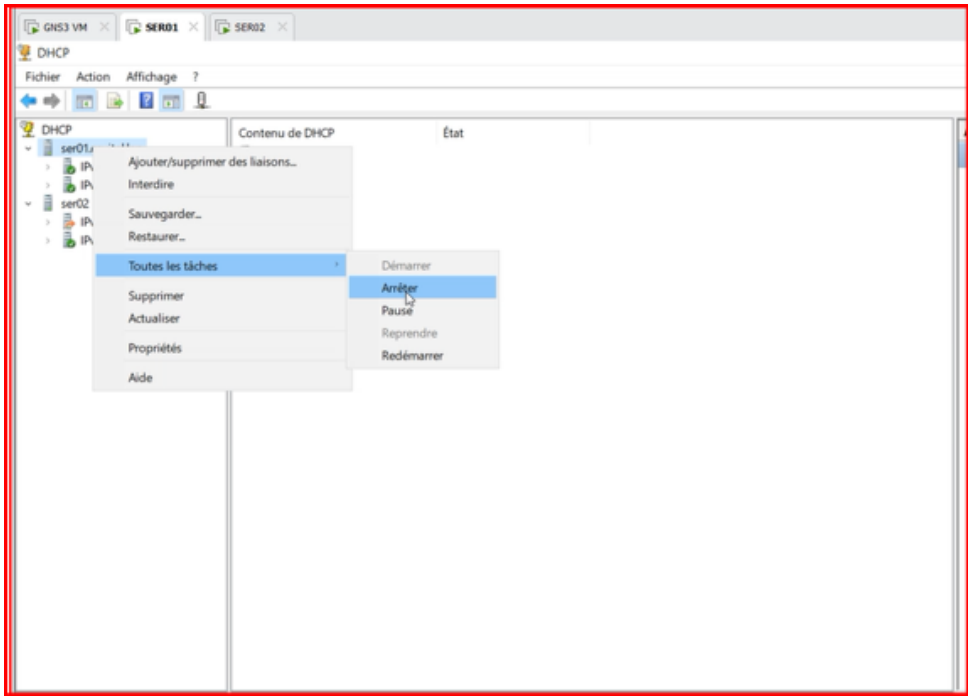


FIGURE 5.52 – Tester le basculement en désactivant le serveur 1 (étape 01).

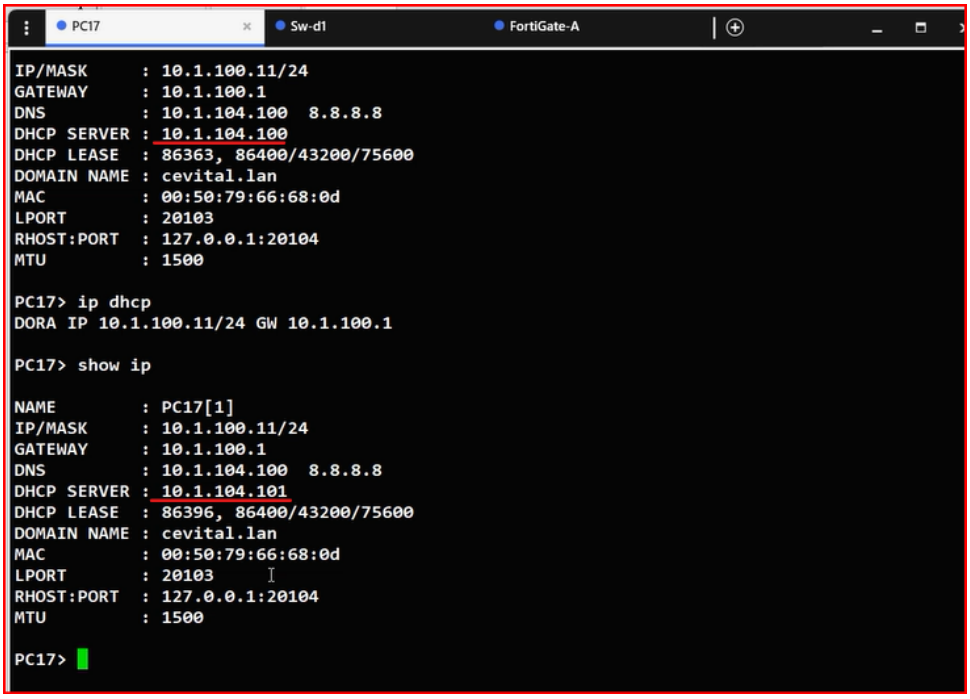


FIGURE 5.53 – Tester le basculement en désactivant le serveur 1(étape 02).

5.5.3 Test de configuration de la HA au niveau du FortiGate-B

On observe qu'après la désactivation du FortiGate-A, le fonctionnement se basculera sur le FortiGate-B qui ensuite deviendra primaire (Figure 5.54)

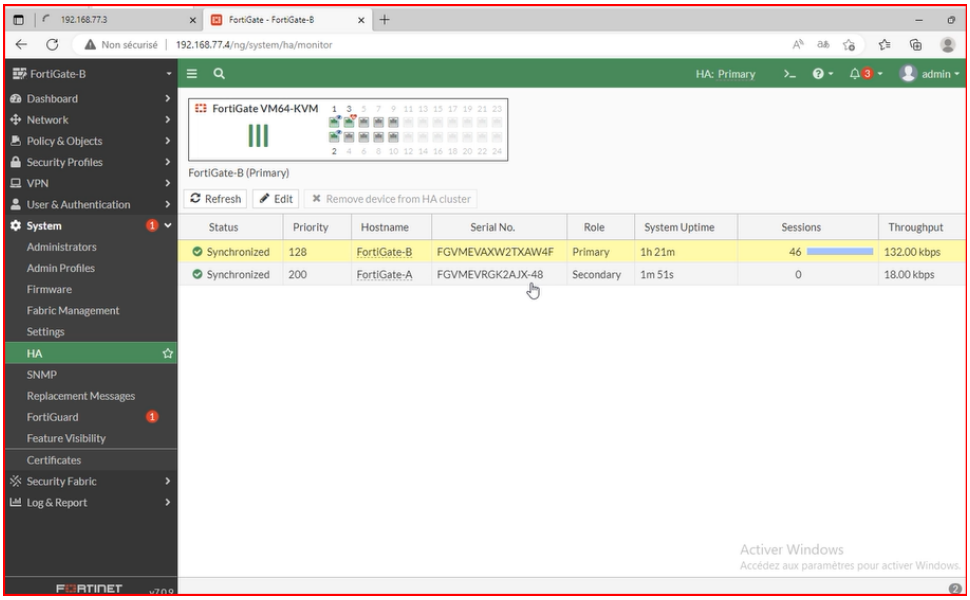


FIGURE 5.54 – Tester la HA au niveau de FortiGate-B .

5.5.4 Vérification des règles de routage configurées sur le site distant

Cette étape sert précisément à configurer la règle de routage du VLAN management vers le site distant comme la figure ci-dessous l'explique :

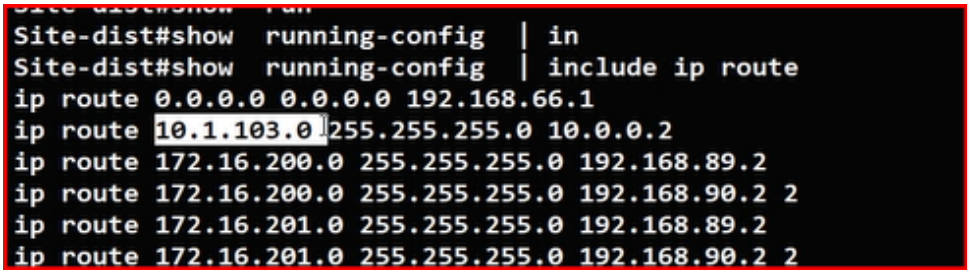


FIGURE 5.55 – Vérification des régles de routage au niveau de site distant.

5.5.5 Test de PING de FortiGate-A vers le Tunnel

Ce test sert à vérifier la connectivité du FortiGate-A vers l'adresse IP du l'interface Tunnel GRE du site distant, comme la figure (Figure...) le montre la figure (Figure 5.56) :

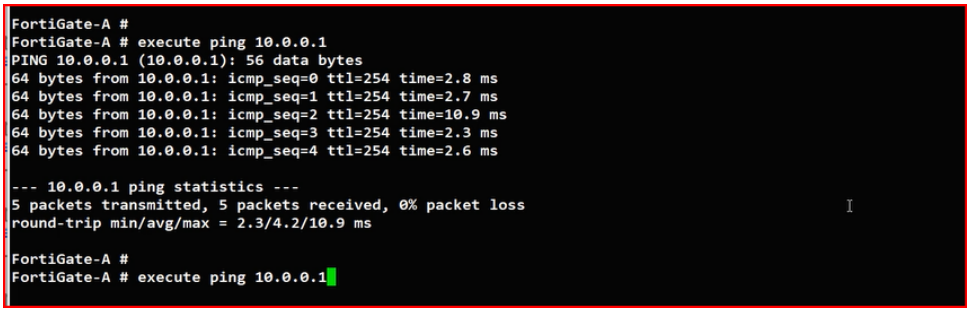


FIGURE 5.56 – Vérication du ping de FortiGate-A vers le tunnel VPN.

5.5.6 Test de PING de FortiGate-A vers la passerelle du routeur du site distant

Après la réussite de connectivité du FortiGate-A vers le Tunnel, on teste de pinger à partir du pare-feu vers l'adresse IP public du routeur du site distant (Figure 5.57) :

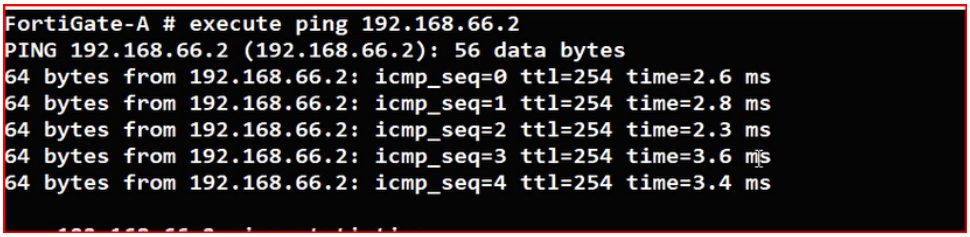


FIGURE 5.57 – Vérication du ping de FortiGate-A vers la passerelle du routeur de site distant.

5.5.7 Test de PING de FortiGate-A vers le LAN du site distant

Ensuite on continuera les tests de connectivité vers le LAN due site distant à partir du FortiGate-A, comme montrée dans la figure (Figure 5.58) ci-dessous :

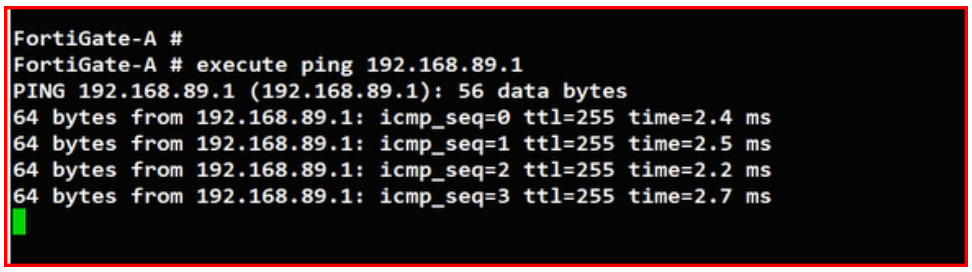


FIGURE 5.58 – Vérication du ping de FortiGate-A vers le LAN du site distant.

5.5.8 Test de PING due site distant vers FortiGate-A

Comme on a testé la connectivité du FortiGate-A vers le site distant, on teste de manière inverse, du site distant vers le FortiGate-A, (Figure 5.59)

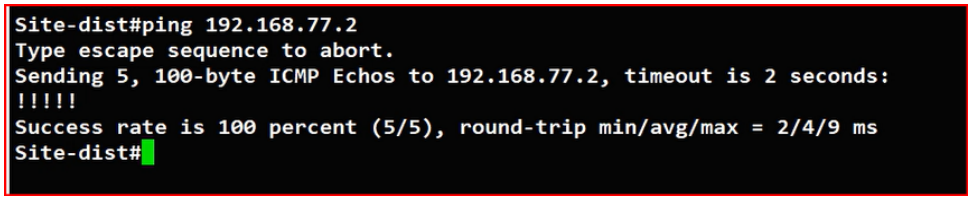


FIGURE 5.59 – Vérication du ping de site distant vers FortiGate-A.

5.5.9 Test de ping du PC management vers le Tunnel

Dans la figure (Figure 5.60), on teste la connectivité de PC management vers l'adresse de Tunnel indiquée dans le FortiGate-A avec la commande PING

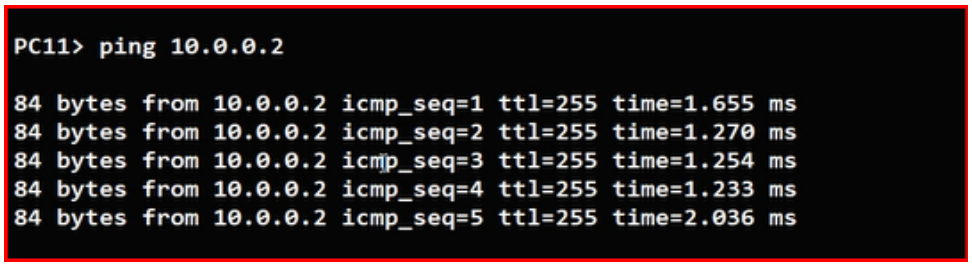


FIGURE 5.60 – Vérication du ping de PC manager vers le tunnel.

5.5.10 Test du Ping de PC manager vers le PC du site distant

On test la connectivité de PC manager par un ping vers le VLAN 200 (10.1.200.10) voir (Figure 5.61) :

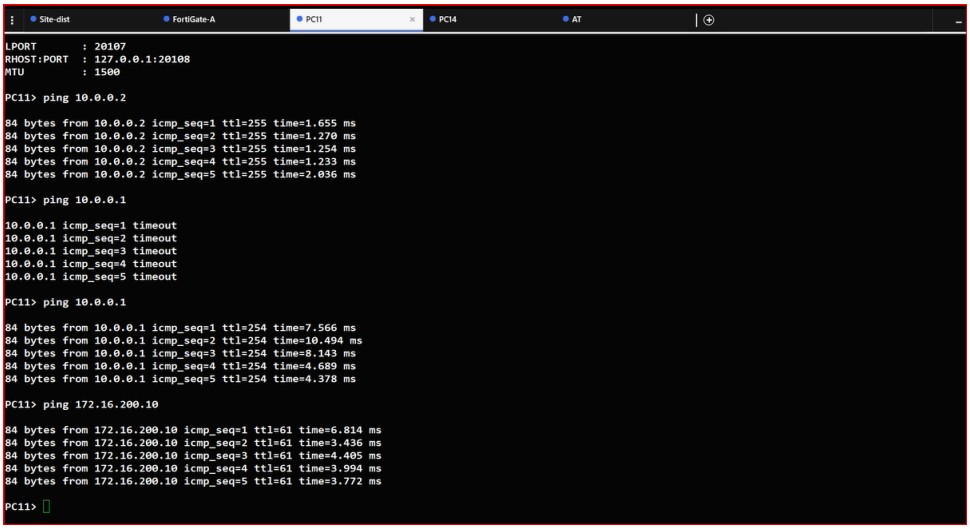


FIGURE 5.61 – Vérication du ping de PC manager vers le Pc de site distant.

5.6 Conclusion

Tout au long de ce chapitre, nous avons présenté notre environnement de travail, comme nous avons montré la configuration de base de notre architecture proposé, ensuite nous avons simulé les protocoles de la haute disponibilité ainsi ses techeniques après une connection avec un site distant afin d'assurer que les données se transmisent.

Conclusion générale

En conclusion générale, ce mémoire nous a permis d'approfondir nos connaissances sur le thème de la haute disponibilité de l'infrastructure et de la virtualisation. Nous avons réalisé l'importance de garantir une disponibilité optimale des systèmes et des services dans un environnement informatique critique.

Nous avons appris que la haute disponibilité repose sur la mise en place de mesures techniques et organisationnelles visant à minimiser les interruptions de service. Cela peut inclure l'utilisation de technologies telles que la redondance matérielle, les systèmes de secours, les clusters et la répartition de charge.

La virtualisation s'est révélée être un élément clé pour atteindre la haute disponibilité. En créant des machines virtuelles et des environnements isolés, nous avons pu garantir une meilleure résilience et une reprise rapide en cas de défaillance d'un système physique.

Au cours de notre période de stage, nous avons également appris à concevoir des architectures hautement disponibles, en tenant compte des exigences spécifiques de l'entreprise, de la redondance des composants critiques et de la mise en place de plans de continuité des activités.

Enfin, ce mémoire nous a permis de comprendre l'importance de la haute disponibilité de l'infrastructure et de la virtualisation dans le contexte des systèmes informatiques d'entreprise. Nous avons acquis des compétences pratiques précieuses pour concevoir, mettre en œuvre et maintenir des environnements hautement disponibles, ce qui est essentiel pour assurer la continuité des activités et garantir la satisfaction des utilisateurs finaux.

Annexe A

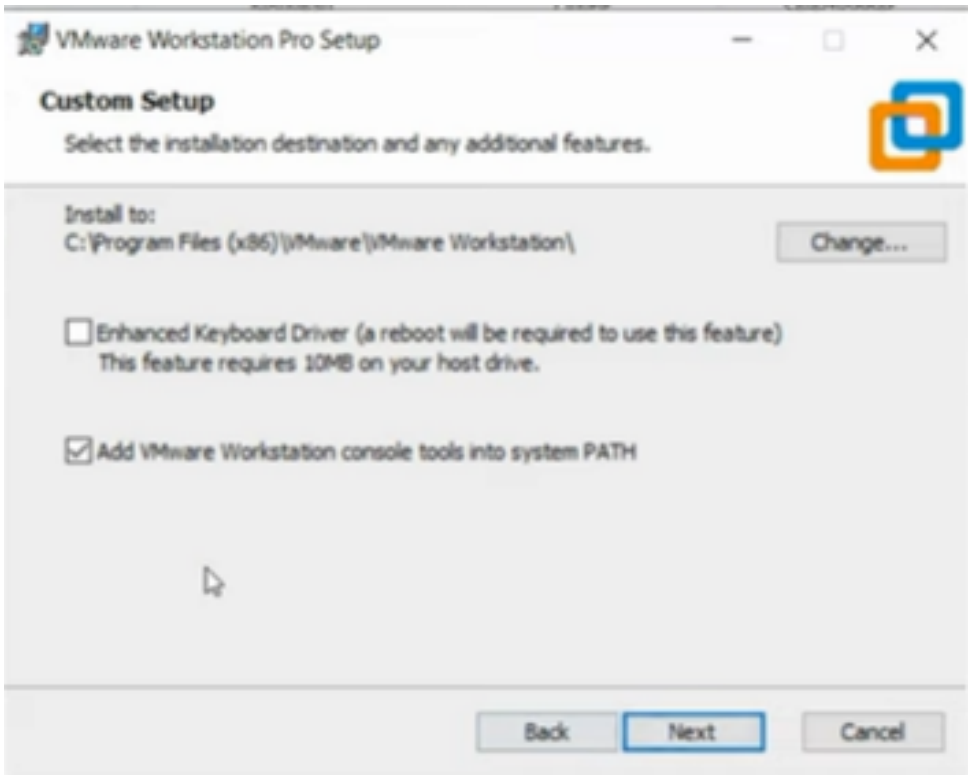
Annexe

Installation de VMware workstation 17

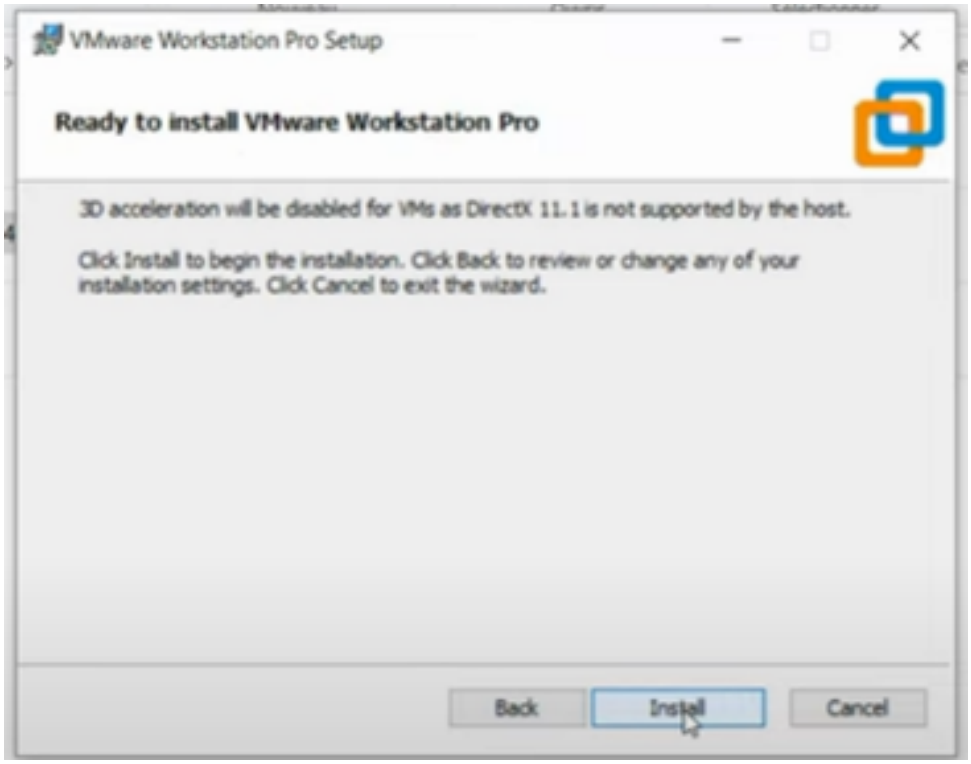
1. Exécution du programme d'installation : Une fois le téléchargement terminé, exécutez le fichier d'installation en double-cliquant dessus, acceptez et continuez.

2. Contrat de licence : Acceptez les termes du contrat de licence et continuez.

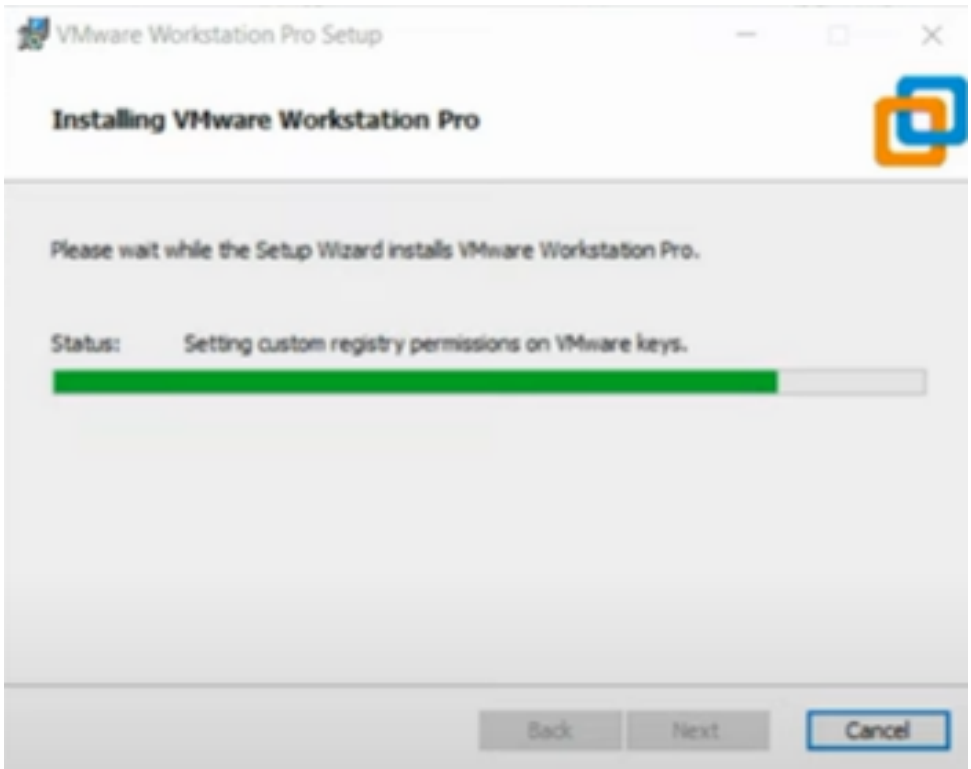
3. Emplacement d'installation : Sélectionnez l'emplacement où vous souhaitez installer VMware Workstation 17 Pro ou utilisez l'emplacement par défaut.



4. Installation : Cliquez sur le bouton "Installer" pour commencer l'installation. Patientez pendant que le programme d'installation extrait les fichiers et configure les composants.

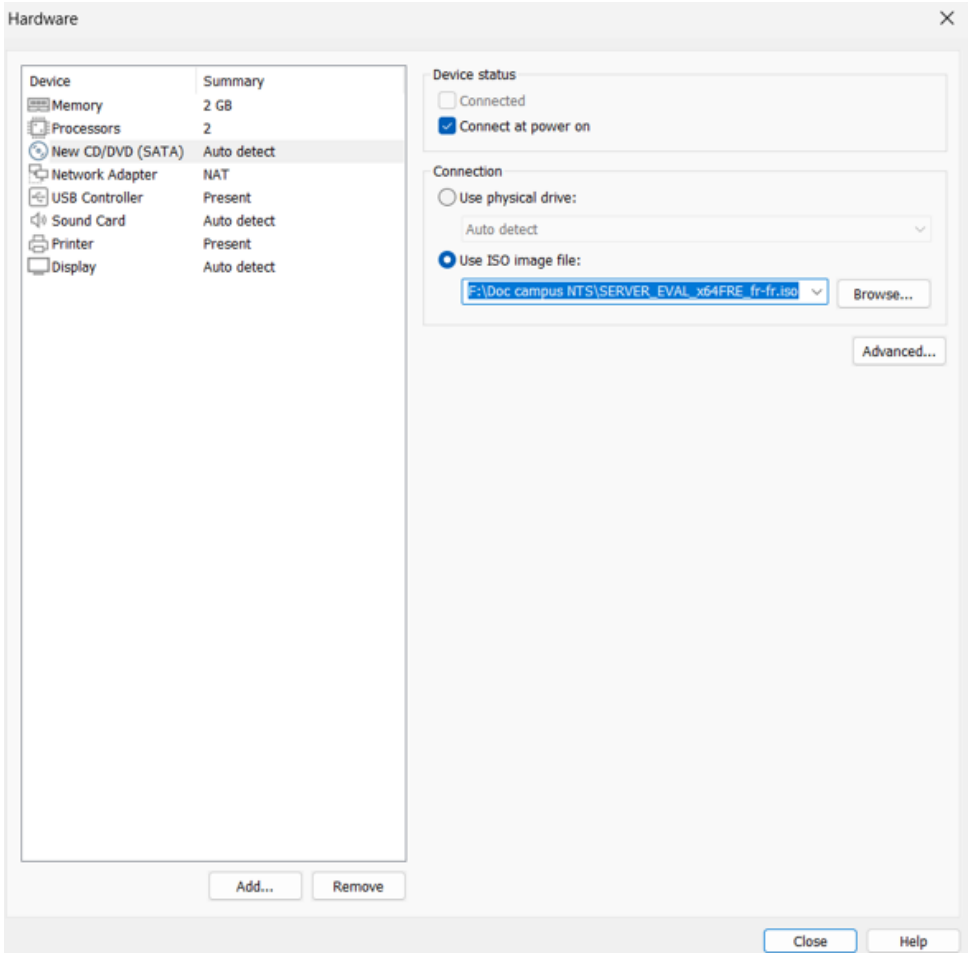


5. Terminer l'installation : Une fois l'installation terminée, vous pouvez choisir de lancer VMware Workstation 17 Pro immédiatement ou de le lancer ultérieurement.

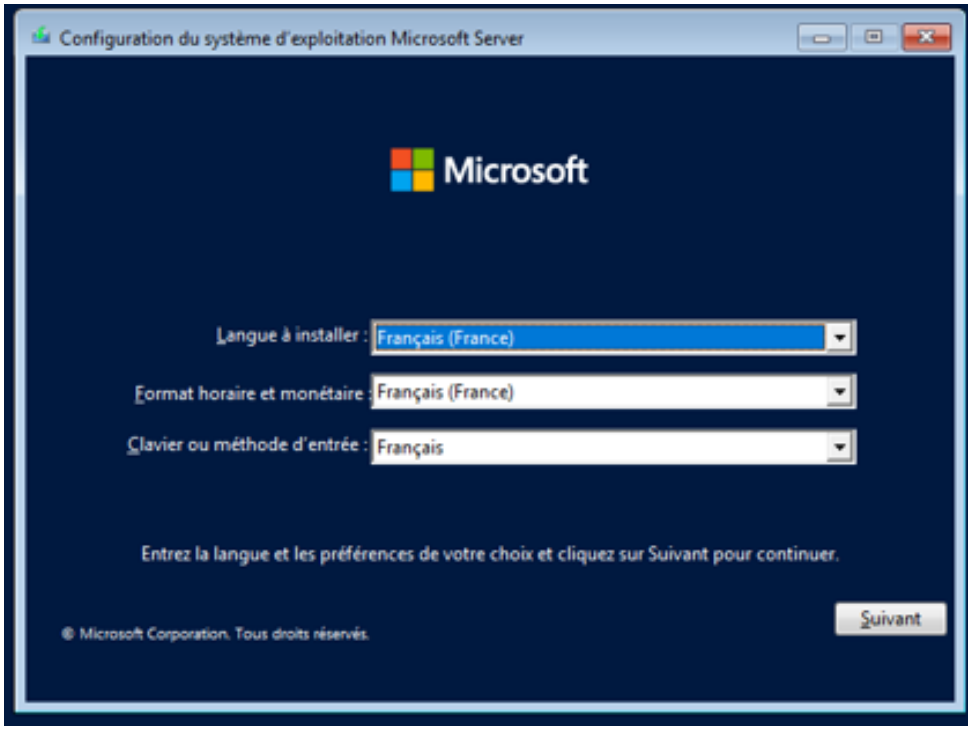


Installation de serveur

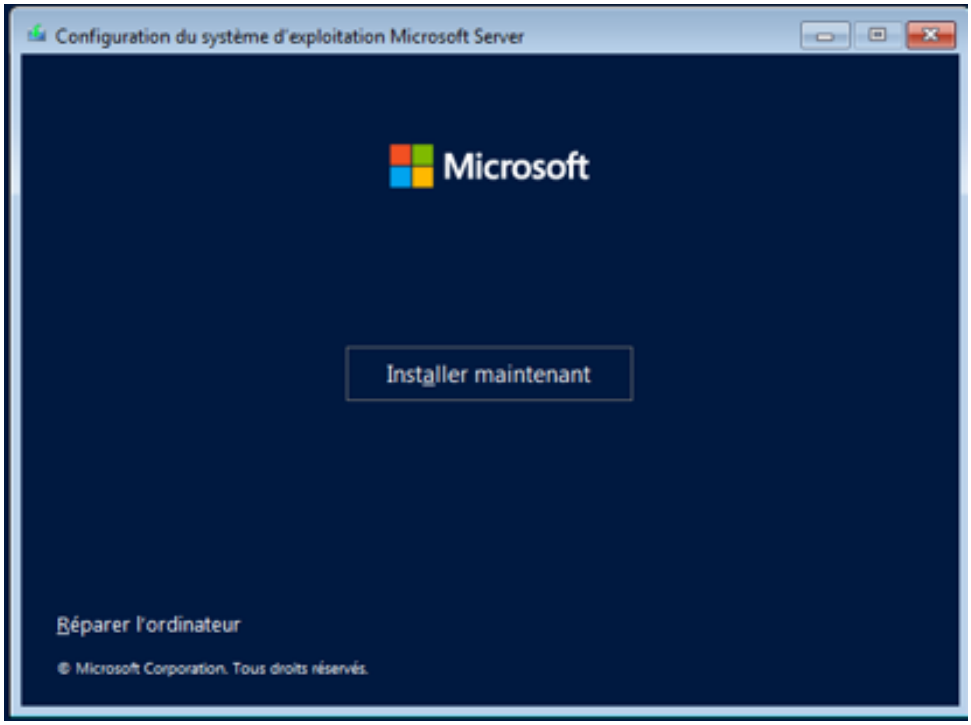
1. Démarrage à partir du support d'installation : Insérez le DVD ou la clé USB dans l'ordinateur où vous souhaitez installer Windows Server 2022. Redémarrez l'ordinateur et assurez-vous que le démarrage à partir du DVD ou de la clé USB est configuré dans le BIOS ou l'UEFI.



2. Sélection de la langue et du clavier : Lorsque l'installation démarre, sélectionnez la langue d'installation et le paramètre de clavier appropriés, puis cliquez sur "Suivant".

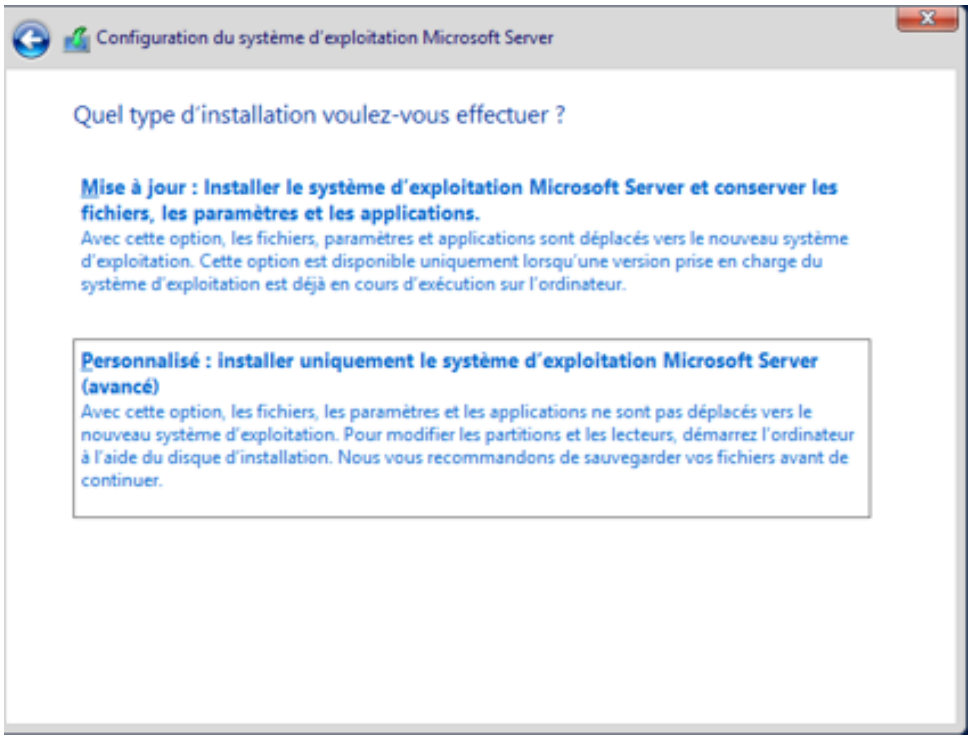


3. Installation : Cliquez sur "Installer maintenant" pour démarrer l'installation de Windows Server 2022.

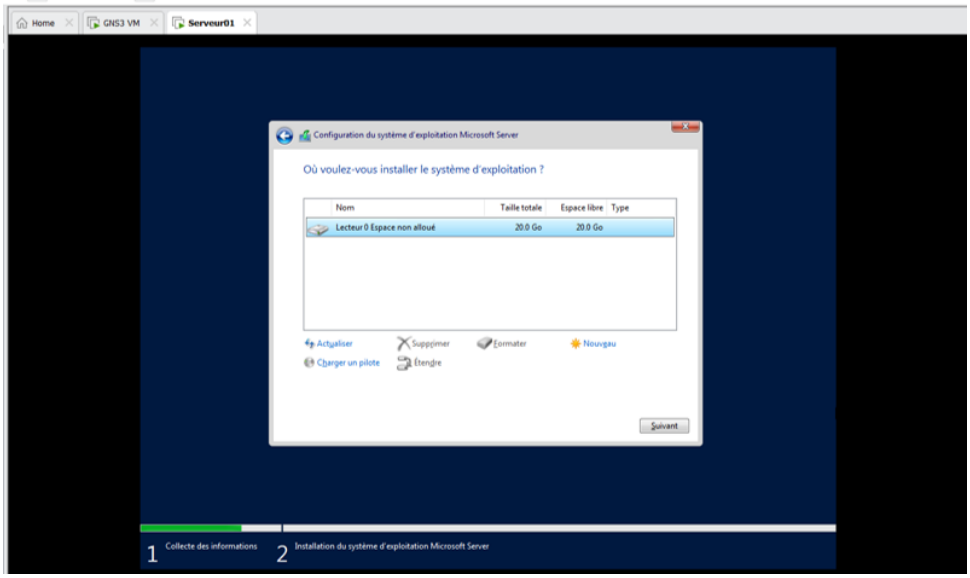


4. Acceptation des termes de licence : Lisez attentivement les termes de licence de Microsoft et acceptez-les pour continuer.

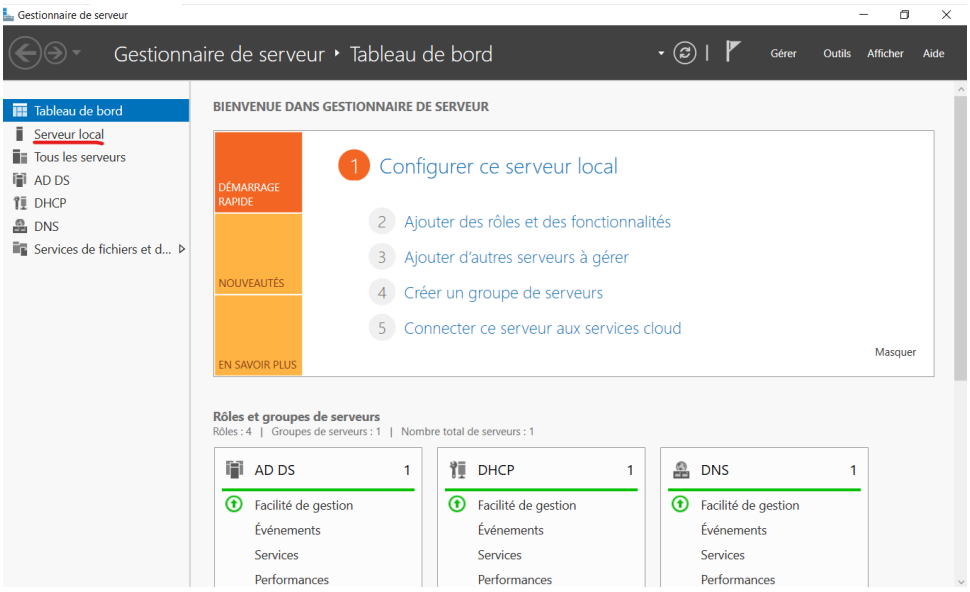
5. Sélection du type d'installation : Choisissez le type d'installation souhaité, par exemple, "Personnalisée : Installer uniquement Windows" ou "Mise à niveau : Installer Windows et conserver les fichiers, paramètres et applications existants".



6. Installation en cours : L'installation de Windows Server 2022 va maintenant commencer. Attendez que les fichiers soient copiés et que les composants soient installés.



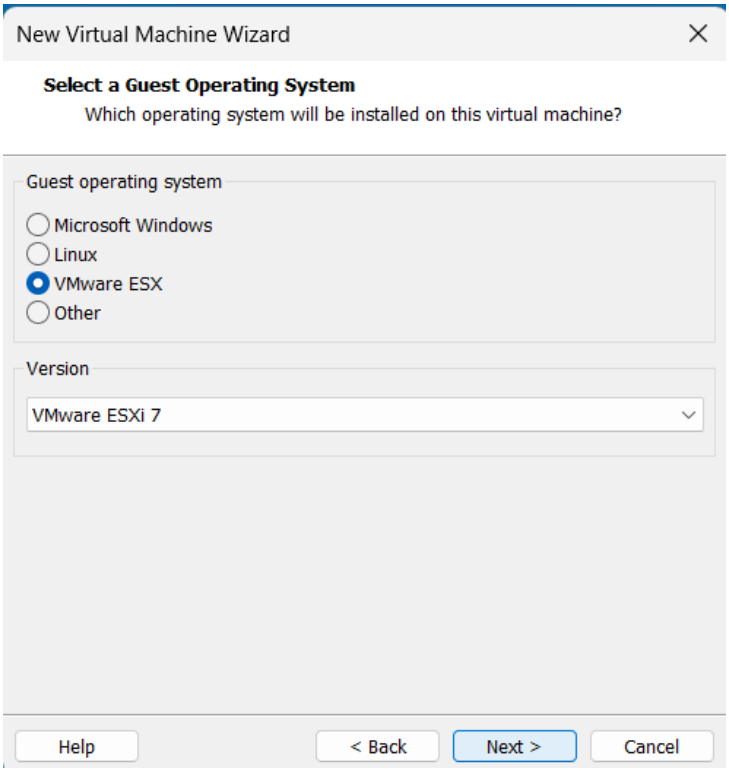
7. Configuration initiale : Suivez les instructions à l'écran pour configurer des paramètres tels que le nom d'ordinateur, le mot de passe administrateur, les mises à jour automatiques, le fuseau horaire, etc.



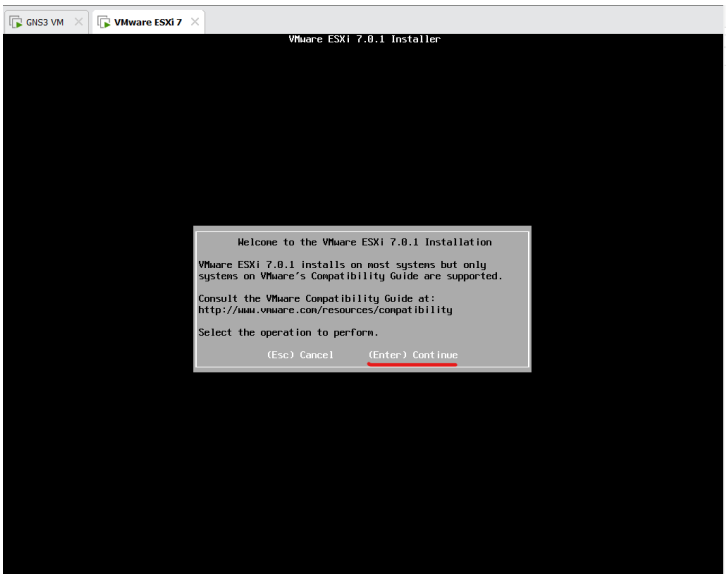
‘

Installation de VMWare ESXI 7

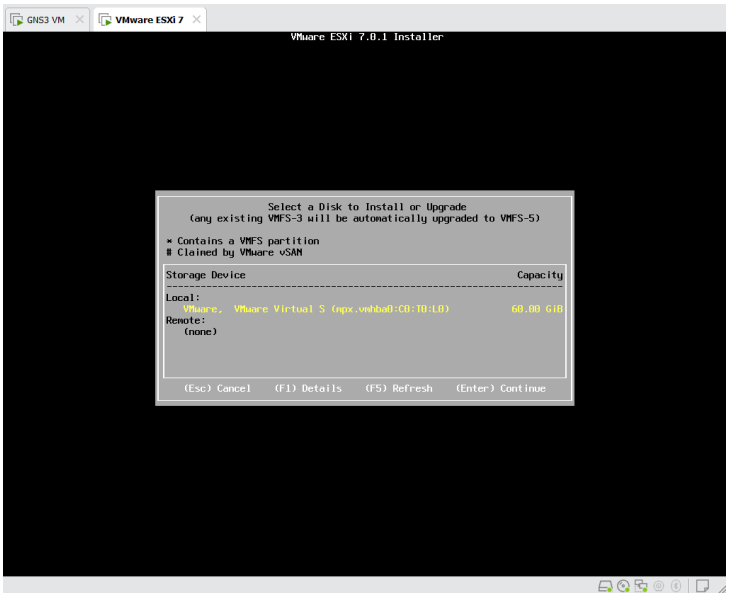
1. Lorsque le programme d'amorçage apparaît, on sélectionne l'option d'installation d'ESXi. Nous pouvons également choisir d'exécuter des tests de mémoire et de matériel avant l'installation pour assurer que tout fonctionne correctement.



2. l'acceptation de contrat de licence de VMware ESXi.

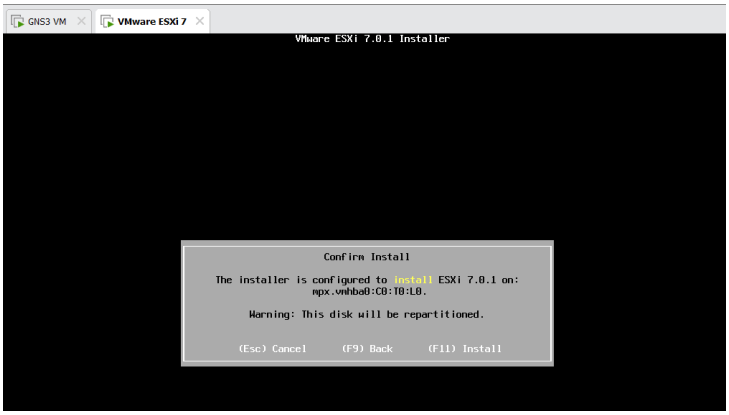


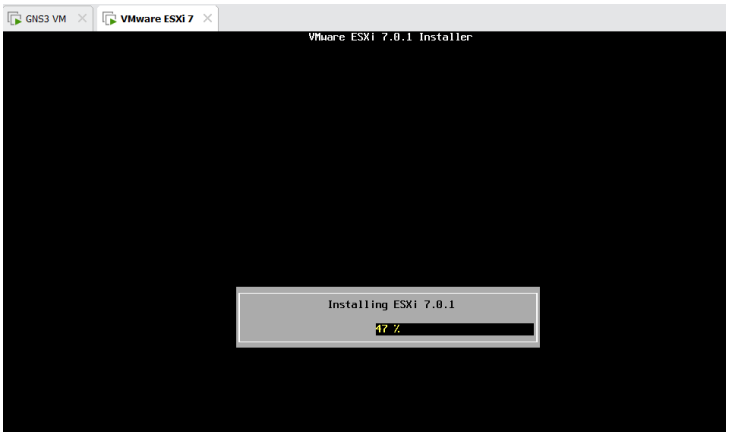
3. En sélectionnant le lecteur ou la partition sur lequel l'installation de VMware ESXi se réalisera,après le choix d'un lecteur approprié et à prendre en compte l'espace disponible nécessaire pour les machines virtuelles et les fichiers de données.



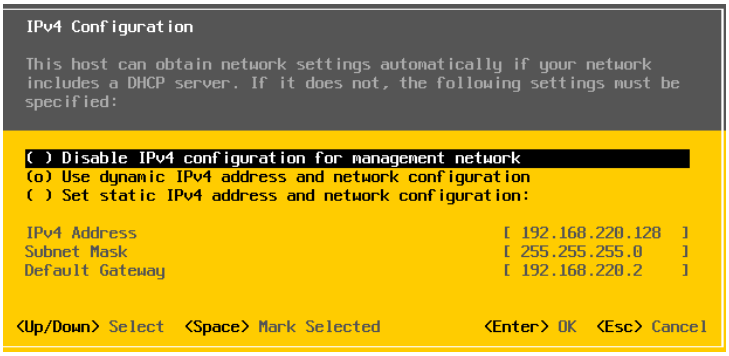
4. La configuration de mot de passe administrateur pour le serveur VMware ESXi. Ce mot de passe sera utilisé pour accéder à l'interface de gestion.

5. Une fois qu'on termine la configuration, l'installation de VMware ESXi commencera. Cela peut prendre quelques minutes.





6. Une fois que le serveur a redémarré, vous pouvez accéder à l'interface de gestion de VMware ESXi en utilisant un navigateur web et en saisissant l'adresse IP qui a été attribuée au serveur.



Bibliographie

[1] J. DORDOIGNE, Les réseaux informatiques notions fondamentales (Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IPV6), 6 éme éd., ENI.

[2] "https ://www.patshtecno.com/grandes-lignes-sur-les-reseaux-informatiques/. [Accès le 25 02 2023].

[3] "Available : https ://sti.ac-versailles.fr/IMG/pdf/reseau.pdf,cours : : ARCHITECTURE D'UN RÉSEAU INFORMATIQUE. [Accès le 04 02 2023].

[4] https ://reussirsonccna.fr/topologie-des-reseaux/.[Accès le 04 02 2023]

[5] https ://zestedesavoir.com/tutoriels/2789/les-reseaux-de-zero/le-concept-et-les-bases/les-topologies/ [Accès le 09 02 2023]

[6] https ://www.memoireonline.com/09/19/11026/mtude-d-une-solution-d-un-reseau-d-acces-optique-dans-les-systemes-de-communication16.html,[Accès le 25 02 2023]

[7] https ://http ://bits-genius.com/topologie-reseau/[Accès le 18 03 2023]

[8] vulgarisation-informatique.com/topologie-reseau.php[Accès le 18 03 2023]

[9] Andrew Tanenbaum Nick Feamster David Wethrall, 6 éme éd, Prearson.

[10] https ://www.cloudflare.com/fr-fr/learning/network-layer/what-is-routing/[Accès le 20 03 2023]

[11] https ://web.maths.unsw.edu.au/ lafaye/CCM/secu/secuintro.htm [Accès le 22 03 2023]

[12] https ://www.techno-science.net/glossaire-definition/Insecurite-du-systeme-d-information.html [Accès le 22 03 2023]

[13] https ://www.axis-solutions.fr/cyberattaques-les-5-types-les-plus-courants/ [Accès le 22 03 2023]

[14] amazonaws/Security-Mechanisms/pdf.

[15] https ://parlonssciences.ca/ressources-pedagogiques/documents-dinformation/protection-des-donnees-introduction-au-cryptage [Accès le 23 03 2023]

[16] https ://fr.wikipedia.org/wiki/Pare-feu [Accès le 23 03 2023]

[17] https ://waytolearnx.com/2018/09/difference-entre-proxy-et-firewall.html[Accès le 23 03 2023]

[18] https ://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/[Accès le 23 03 2023]

[19] Les ressources internes de l'entreprise CEVITAL

[20] https ://www.google.com/imghp ?hl=EN

[21] https ://www.networklab.fr/ [Accès le 28 03 2023]

[22] https ://www.ionos.fr/digitalguide/serveur/know-how/load-balancer-repartition-de-charge-sur-un-serveur/[Accès le 29 01 2023]

[23] microapp.com/contenus-propres/fiches-produits/extraits-livres/1095/extrait.pdf

[24] https ://www.aimetis.com/webhelp/Symphony/6.13/fr/Serveur redondant.htm [Accès le 08 03 2023]

[25] https ://www.researchgate.net/figure/Les-techniques-de-tolerance-aux-pannes-dans-les-systemes-repartis[Accès le 01 04 2023]

[26] Marie GALEZ, galez@cines.fr, LE SAN ET LE NAS : LE RESEAU AU SERVICE DES DONNEES, pdf.

[27] https ://web.maths.unsw.edu.au/ lafaye/CCM/surete-fonctionnement/haute-disponibilite.htm [Accès 15 02 2023 jusqu'a 24 03 2023]

[28] https ://appmaster.io/fr/blog/quest-ce-que-la-haute-disponibilite [Accès le 16 02 2023].

[29] https ://www.it-connect.fr/les-types-dhyperviseurs/ [Accès le 16 04 2023].

[30] https ://www.developpez.net/forums/d1592745/systemes/virtualisation/vos-hyperviseurs-preferes-faire-virtualisation-serveurs-pourquoi/[Accès le 16 04 2023].

[31] https ://www.youtube.com/watch ?v=3tgcAvV7dt8 installation vmware workstation 17pro

[32] https ://fr.wikipedia.org/wiki/Wikip

[33] Virtualisation Cloud Principes, mise en oeuvre et outils open source, pdf.

Résumé

De nos jours, la haute disponibilité est devenue un élément crucial pour garantir le fonctionnement optimal de tout réseau informatique. Dans le cadre de cette étude, notre objectif principal était de mettre en place une solution de haute disponibilité en utilisant les mécanismes de redondance matérielle et logicielle des services au sein du réseau Cevital-Béjaia. Pour atteindre cet objectif, nous avons explorer la technique de basculement et de redondance des données pour assurer la continuité des services. Nous avons utilisé VMWare Workstation pour virtualiser plusieurs machines, ce qui nous a permis de bénéficier d'une meilleure flexibilité et d'une gestion simplifiée des ressources.

Mots clés : Haute Disponibilité, Virtualisation, Redondance, DHCP.

Abstract

Nowadays, high availability has become a crucial element to ensure the optimal functioning of many computer networks. In this study, our main objective was to implement a high availability solution using the redundancy mechanisms of hardware and software services within the Cevital Bejaia network. To achieve this objective, we explored the techniques of failover and data redundancy to ensure service continuity. We utilized VMWare Workstation to virtualize multiple machines, enabling us to gain better flexibility and simplified resource management.

Key words : High Availability, Virtualization, Redundancy, DHCP.