**République Algérienne Démocratique et Populaire Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

Université Abderrahmane Mira-Bejaïa
Faculté des Sciences Exactes
Département d'Informatique


Mémoire de fin de cycle En vue de l'obtention du diplôme de master en Informatique, Spécialité Administration et sécurité des réseaux

## Thème

# Virtualisation de la couche infrastructure et application d'un système d'information. cas d'étude SPA Général emballage

**Réalisé par :**
HAMMOUMRAOUI Alissia
IDRI Lydia

**Soutenu le 10/10/2021 devant le jury composé de :**

| | | |
|---|---|---|
| **Président :** | Mr S.AISSANI | U.A/Mira Béjaia |
| **Examinateur :** | Mr M.MOKETFI | U.A/Mira Béjaia |
| **Encadrant :** | Mr. K.AMROUN | U.A/Mira Béjaia |
| **Co-Encadrant :** | Mr. N.ELSAKAAN | U.A/Mira Béjaia |

**Promotion 2020/2021**

# Remerciements

**On remercie en premier lieu Dieu tout puissant qui nous a doté d'une grande volonté, courage et patience pour mener à terme mon projet. Il nous est particulièrement agréable avant de présenter notre travail, d'exprimer toute notre gratitude envers les personnes qui de près ou de loin nous ont apporté leur soutien.**

**Nos profonde gratitude et sincères remerciements à notre encadrant de stage Mr LAHLOU Mhnd Arezki qui nous a inculqué une grande confiance et nous a accordé de son temps, ses conseils et nous a orienté dans le bon sens quant à l'élaboration de ce projet, ainsi nous remercions l'ensemble des employés du service Informatique ; Mr k.KHIMOUZI, Mr B.CHERID et Mr L.KESSOUM pour leurs conseils et nous a orienté dans le bon sens quant à l'élaboration de ce projet.**

**On tient à exprimer toute notre grande gratitude à Mr Ragab Nadim et aux membres de jury d'avoir accepté de juger ce travail. On remercie également nos chers parents pour tous les sacrifices consentis à notre égard et leur énorme soutien durant notre vie et notre cursus d'études.**

**Nos vifs remerciements s'adressent également à tous nos enseignants de la faculté des sciences exactes de l'université ABDERRAHMANE MIRA de Bejaia pour la formation qu'ils ont eu le soin de nous apporter tout au long de notre cursus universitaire**

## Dédicaces

je dédie ce modeste travail accompagné d'un profond amour à celle qui m'a arrosée de tendresse,et l'éspoir à ma source de bonheur ma mère,quoi que je fasse ou je dise, je ne saurai point te remercier comme il se doit. je t'aime maman.

A mon père pour ses précieux conseils qui m'ont permis d'arriver là où je suis.

A mes trés chères et adorables soeurs. puisse dieu vous donner amour,bonheur et réussite Meriem et Fatima.

A mon petit frère Azem qui nous apportent tant de joie et d'ambiance dans notre vie, Inchallah tu réussiras dans tes études mon petit ange.

A celui qui m'a soutenue tout au long de ce projet : mon fiancé Toufik, qui a cru en moi et m'as encouragé à aller de l'avant, grâce à son aide et à sa patience que ce travail a pu voir le jour. Que dieu le tout puissant nous accorde un avenir meilleur.

A la meilleure personne que je connaisse, ma soeur,mon amie,ma confidente,à toi ma chère binome qui a toujours été la pour moi dans les meilleur et les pires moment Lydia .

A Mes chers Oncles et Tantes ainsi leurs épouses, époux et enfants. J'espère que mon travail sera le témoignage de mon respect et de mes sentiments les plus sincères.

A mes chères amies Nouna, Wissam, Zahra, Lilia, Amira, qui nous ont épaulées pendant tout notre projet, je n'oublierai jamais votre aide et votre soutien, merci.

A ceux qui m'ont toujours aidé et encouragé, qui étaient toujours à mes côtés, qui m'ont accompagné durant mon chemin d'études supérieures.

A tous ceux qui compte pour moi et qui n'ont pas pu être cités ici.

*Hammoumraoui Alissia*

## Dédicaces

A mon père qui m'a toujours soutenu dans mes choix et en particulier vis-à-vis les études, qui par sa présence, son sérieux, et ses précieux conseils m'a permis d'arriver là où je suis. Papa qui est toujours là derrière moi, je ne saurais te remercier assez pour tout ce que tu fais pour moi, merci du fond du coeur.

A ma chère maman, qui ne cesse de me pousser d'avantage, qui s'est sacrifiée pour moi et a toujours su m'épauler et me soutenir dans mes moments difficiles, j'espère être à la hauteur de tes attentes maman, je t'aime.

A ma soeur Alissa que malgré la distance qui nous sépare m'a beaucoup aidés et soutenu à sa façon et reste pour moi un modèle à suivre pour l'accomplissement de mes projets professionnelles, je t'adore chère soeur.

A mes frères et soeurs qui sont également loin je vous remercie infiniment pour vos encouragements et vos conseils.

A mon fiancé Moumene, qui importe tant dans ma vie, qui a partagé tous ces moment et qui les partagera pour toute la vie Inchallah, tu as cru en moi et tu m'as encouragé à aller de l'avant surtout en cette année, Je remercie également sa famille.

A toute ma famille qui n'arrêtait pas de m'encourager aux quotidiens, je vous remercie mes oncles, tantes et cousins(es).

A ma copine et binôme Alissia, qui a toujours été auprès de moi et qui m'a soutenu dans les moments de faiblesse, et avec qui j'ai partagé cette expérience ; Le meilleur reste à venir.

A mes chères amies Faty, Mayou, Wissam, Zahra, Lilia, Amira, qui nous ont vraiment épaulées pendant tout notre projet, je n'oublierai jamais votre aide et votre soutien, merci.

*Idri Lydia*

# Table des matières

**Table des figures**

**Listes des tableaux**

**Liste des abréviations**

**Introduction Générale** **1**

**1 Les systèmes d'informations au cœur des métiers** **3**
1.1 Introduction . . . 3
1.2 Première partie : Parc informatique et ses composants . . . 3
1.2.1 Modèle d'architecture en couche des systèmes d'information . . . 4
1.2.1.1 Couche fonctionnelle . . . 4
1.2.1.2 Couche applicative . . . 4
1.2.1.3 Couche infrastructure . . . 4
1.2.1.4 Couche opérationnelle . . . 5
1.2.2 Parc matériel . . . 5
1.2.2.1 Infrastructure réseaux . . . 5
1.2.2.2 Différents dispositifs de sécurité et serveurs . . . 5
1.2.3 Parc logiciel . . . 9
1.2.3.1 Enterprise Ressource Planning . . . 10
1.2.3.2 ERP Odoo . . . 10
1.2.3.3 Gestion de la relation client . . . 12
1.3 Deuxième partie : Analyse des risques . . . 12
1.3.1 Risques et menaces sur la sécurité du système d'informations . . . 13
1.3.2 Dispositifs de sécurité dans les réseaux informatiques . . . 13
1.4 Troisième partie : virtualisation, simulation et émulation . . . 14
1.4.1 Virtualisation . . . 14
1.4.1.1 Différents types de virtualisation . . . 15
1.4.1.2 Avantages de la virtualisation . . . 15
1.4.1.3 Inconvénients de la virtualisation . . . 16
1.4.2 Simulation et émulation . . . 16
1.4.2.1 Présentation de GNS3 . . . 16
1.4.2.2 Présentation de VMware . . . 17
1.5 Conclusion . . . 18

**2 Introduction du cas d'étude** **19**
2.1 Introduction . . . 19
2.2 Première partie : Présentation de la société d'accueil . . . 19
2.2.1 Présentation de Général Emballage . . . 19
2.2.2 Historique de l'entreprise Général Emballage . . . 20
2.2.3 Evolution des effectifs . . . 22
2.2.4 Valeurs de Général emballage . . . 23
2.2.5 Plans du réseau de l'entreprise . . . 24
2.3 Deuxième partie : Etat des lieux . . . 24
2.3.1 Présentation de l'infrastructure réseau . . . 24
2.3.2 Normes ISO de General Emballage . . . 25
2.3.3 Etude du réseau de l'entreprise . . . 26
2.3.4 Analyse de l'existant . . . 28
2.3.5 Problématique . . . 32
2.3.6 Objectifs . . . 32
2.4 Conclusion . . . 33

**3 Études des solutions proposées** **34**
3.1 Introduction . . . 34
3.2 Présentation de notre infrastructure réseau . . . 34
3.3 Pare-feu FortiGate de Fortinet . . . 35
3.3.1 Importation de FortiGate sur gns3 . . . 35
3.3.2 Configuration d'accès au FortiGate . . . 37
3.3.3 Configuration des VLANs . . . 39
3.3.4 Configuration d'une liste de contrôle d'accès . . . 41
3.3.4.1 Filtrage web . . . 42
3.3.4.2 Filtrage applicatif . . . 43
3.3.5 Configuration du VPN IPsec . . . 44
3.3.5.1 Configuration VPN1 (Oran vers Akbou) . . . 44
3.3.5.2 Configuration VPN2 (Akbou vers Oran) . . . 47
3.3.6 Configuration de la haute disponibilité . . . 48
3.4 Configuration du switch L2 IOU sous GNS3 . . . 49
3.5 Les machines virtuelles sur VMware Workstation 16Pro . . . 50
3.5.1 Installation de Windows Server 2016 . . . 50
3.5.1.1 Installation de Active Directory (AD1) . . . 53
3.5.1.2 Replication de Active Directory (ADirectory2) . . . 58
3.5.2 Installation de Windows 10 Professionnel . . . 61
3.5.3 Installation de CentOS 8 . . . 64
3.6 Conclusion . . . 71

**4 Tests et Validations** **72**
4.1 Introduction . . . 72
4.2 Vérification des fonctionnalités de Fortigate . . . 72
4.2.1 Fonctionnement des VLANs . . . 72
4.2.2 Tests de fonctionnement des règles de filtrage . . . 74
4.2.3 Service VPN IPsec . . . 75
4.2.4 Haute disponibilité du Fortigate . . . 76

4.3 Test de réplication . . . . . 77
4.4 Fonctionnement Odoo13 . . . . . 77
4.5 Conclusion . . . . . 79

**Conclusion générale et perspectives** **80**

**Bibliographie** **81**

# Table des figures


1.1 Différentes couches du système d'information. . . . . 5
1.2 L'interface graphique du pare-feu Fortigate. . . . . 6
1.3 Zone Démilitarisée. . . . . 8
1.4 Fonctionnalités d'ERP. . . . . 10
1.5 L'ERP ODOO. . . . . 11
1.6 Les Taches d'un CRM. . . . . 12
1.7 L'interface graphique de GNS3. . . . . 17
1.8 L'interface graphique de VMware workstation 16. . . . . 17

2.1 SPA Général Emballage site Taharacht Akbou et son logo. . . . . 20
2.2 Plan du réseau de l'entreprise. . . . . 24
2.3 Architecture réseau LAN General Emballage Akbou. . . . . 25
2.4 Risques liés au système d'information de GE. . . . . 31

3.1 Maquette du réseau sous GNS3. . . . . 35
3.2 Importation d'appliance Fortigate 6.4.0 sur GNS3. . . . . 36
3.3 Importation d'appliance Fortigate 6.4.0 avec succès . . . . . 37
3.4 Ajout et configuration du cloud. . . . . 37
3.5 Configuarations d'appliance Fortigate 6.4.0. . . . . 38
3.6 Ping PC local vers FortiGate réussi . . . . . 38
3.7 Interface d'authentification . . . . . 39
3.8 Tableau de bord fortiGate . . . . . 39
3.9 Création et paramétrage du vlan10 . . . . . 40
3.10 Les interfaces VLANs configuées sur le port 3. . . . . 40
3.11 Creation d'une nouvelle zone et l'ajout des VLANs. . . . . 41
3.12 Configuration d'accès de la zone "inter-vlan" vers "Internet". . . . . 41
3.13 Exemple des autres ACLs crées . . . . . 42
3.14 Création d'un nouveau filtre URL "Facebook" . . . . . 42
3.15 Application du filter web sur ACL . . . . . 43
3.16 Création d'une règle de contrôle d'application "Gmail". . . . . 43
3.17 Application de la règle de contrôle d'application. . . . . 44
3.18 Creation et Authentification du tunnel VPN1 IPsec . . . . . 45
3.19 Policy and Routing VPN1 IPsec. . . . . 45
3.20 Configuration créée par VPN1. . . . . 45
3.21 L'interface VPN1 créée. . . . . 46
3.22 Adresses créées par VPN1. . . . . 46
3.23 Routes créées par VPN1. . . . . 46
3.24 ACLs créées par VPN1. . . . . 47

3.25 Configuration d'Authentification et " Policy and Routing" VPN2 IPsec. . . . . 47
3.26 Activation du tunnel VPN sur les deux site. . . . . 47
3.27 Configuration HA "fortigate-A". . . . . 48
3.28 Configuration HA "fortigate-B". . . . . 49
3.29 Configuration HA effectuée avec succès. . . . . 49
3.30 Création d'une nouvelle machine virtuelle. . . . . 51
3.31 Importation du fichier ISO. . . . . 51
3.32 Vérification des paramètres de la machine virtuelle créer. . . . . 52
3.33 Installation de Windows . . . . . 52
3.34 Configuration du mot de passe pour la machine virtuelle . . . . . 53
3.35 Installation de windows server avec succès. . . . . 53
3.36 Configuration de l'adressage du premier Serveur . . . . . 54
3.37 Ajout des rôles et des fonctionnalités . . . . . 54
3.38 Sélection des deux rôles DNS et AD DS. . . . . 55
3.39 Promotion du serveur en contrôleur de domaine. . . . . 55
3.40 Configuration de déploiement . . . . . 56
3.41 configuration des options du contrôleur de domaine. . . . . 56
3.42 Vérification des prérequis et installation contrôleur de domaine . . . . . 57
3.43 Connexion au domaine "generalemballage.local". . . . . 57
3.44 Creation d'un utilisateur sur le premier serveur Active Directory . . . . . 58
3.45 Configuration de l'adressage du deuxième Serveur . . . . . 58
3.46 Ajout du deuxième serveur à notre domaine. . . . . 59
3.47 Configuration de déploiement du deuxième serveur. . . . . 59
3.48 Vérification des prérequis et installation du contrôleur de domaine . . . . . 60
3.49 Vérification de la réplication sur le premier serveur (AD1). . . . . 60
3.50 Installation de Windows 10 professionnel. . . . . 61
3.51 Windows 10 professionnel prête à l'emploi. . . . . 62
3.52 Joindre Windows 10 professionnel au domaine. . . . . 63
3.53 Connection au domaine. . . . . 64
3.54 Paramétrages des information d'installation de centOS 8. . . . . 64
3.55 Personnalisation et installation de CentOS 8. . . . . 65
3.56 Ecran de connexion et la page d'accueil de centOS 8. . . . . 65
3.57 Ecran de configuration d'Odoo 13 . . . . . 70

4.1 Attribution adresse IP par DHCP . . . . . 73
4.2 Connectivité entre les VLANs . . . . . 73
4.3 Connectivite de la zone démilitarisée . . . . . 74
4.4 Tests d'accès a Internet. . . . . 74
4.5 Page URL "Facebook" Bloquer. . . . . 75
4.6 L'application "Gmail" bloqué. . . . . 75
4.7 Test de fonctionnement du VPN à partir du site Akbou vers Oran et inversement . 76
4.8 Test du basculement HA . . . . . 76
4.9 Vérification de la réplication sur ADirectory2. . . . . 77
4.10 Création d'une base de donnée Odoo13. . . . . 77
4.11 Interface des applications d'Odoo. . . . . 78
4.12 Gestion du pipeline client avec l'intégration Odoo CRM. . . . . 78

# Liste des tableaux

2.1 Evolution des effectifs par catégorie socioprofessionnelle. . . . . 22
2.2 Evolution des effectifs des sites de GE. . . . . 23
2.3 Questionnaire sur l'analyse de l'existant [5]. . . . . 31

# Liste des abréviations

**ACL** Access Control List

**AD DS** Active Directory Domain Services

**BDD** Base De Données

**CRM** Customer Relationship Management

**DHCP** Dynamic Host Configuration Protocol

**DMZ** zone Démilitarisée

**DNS** Domain Name System

**DSI** Directeur des systèmes d'information

**ERP** Enterprise Resource Planning

**GNS3** Graphical Network Simulator

**GRH** Gestion des Ressources Humaines

**GUI** Graphical User Interface

**HA** High Availability

**HTTPs** Hypertext Transfer Protocol Secure

**IAAA** Identification, Authentication, Authorization, Accounting - Authentification

**IMG** International Management Group

**ISO** Organisation internationale de normalisation.

**IPSec** Internet Protocol Security

**IPS** Intrusion Prevention System

**IP** Internet Protocol

**IOS** iPhone Operating System

**LAN** Local Area Network

**LDAP** Lightweight Directory Access Protocol

**MRP** Management des Ressources de Production

**NAT** Traduction D'adresse Réseau

**NIF** Numéro d'identification fiscale

**NIS** Numéro d'identification statique

**RC** Ruling Cases

**SI** Systeme d'information

**SSH** Secure Shell

**SSL** Secure Socket Layer

**SSL** Secure Socket Layer

**TLS** Transport Layer Security

**TPE/PME** Très Petite Entreprise / Petite Moyenne Entreprise

**UTM** Unified threat management

**VLAN** Virtual Local Area Network

**VM** Virtual Machine

**VPN** virtual private network

**WAN** Wide Area Network

# Introduction Générale

Le système d'information (SI) est un élément central d'une entreprise ou d'une organisation. Il permet aux différents acteurs de véhiculer des informations et de communiquer grâce à un ensemble de ressources matérielles, humaines et logicielles. Un SI permet de créer, collecter, stocker, traiter, modifier des informations sous divers formats. L'objectif d'un SI est de restituer une information à la bonne personne et au bon moment sous le format approprié.

Le SI a deux finalités, fonctionnelle et sociale. Concernant la finalité fonctionnelle, le SI est un outil de communication entre les différents services d'une entreprise et a un rôle opérationnel et stratégique. La finalité sociale quant à elle permet de se soucier de l'intégration des salariés dans l'entreprise favorisant la vie sociale, la culture d'entreprise par la diffusion de l'information.

Le SI aujourd'hui joue un rôle important au sein d'une entreprise, il est même indispensable à leur bon fonctionnement. Un SI performant permet à une entreprise d'optimiser leur processus, de sous-traiter des tâches à faible valeur ajoutée, d'améliorer la relation client, de mieux communiquer et améliorer la productivité. Lorsque vous ne savez pas de quoi est composé votre SI, que vous pensez qu'il n'est pas optimisé, ou que vous souhaitez le faire évoluer, réaliser un audit de votre SI peut s'avérer nécessaire.

Nous projetons notre étude sur l'entreprise agroalimentaire Général Emballage, nous avons pu observer que l'infrastructure réseau existante contient quelques défaillances, dus principalement à la structure réseau de ce dernier et aux extensions relatives aux demandes incessantes des utilisateurs de ce réseau, entrainants des pannes et surcharges réseaux et l'exposant donc à des attaques qui peuvent lui être nuisibles. Dans ce cadre là, nous avons opter pour un stage pratique dans lequel nous avons envisagé a virtualiser leur architecture réseau afin d'analyser les besoins réels en termes des services réseaux, faire une anatomie du réseau existant, repérer les points faibles et le point forts et construire une plate-forme de base pour concevoir la nouvelle architecture et enfin proposer nos solutions aux insuffisances constatés.

Dans ce projet de fin d'étude pour l'obtention du diplôme de Master, Notre mission est la conception d'une architecture réseau pour un parc informatique qui permet de modéliser le réseau réel à l'échelle d'un laboratoire réseau sous GNS3 pour virtualiser le fonctionnement d'un réseau LAN et WAN basé sur les protocoles TCP/IP en utilisant les IOS réels des différents équipements (pare-feu FortiGate et commutateur), des machines virtuelles crées sous l'hyperviseur VMware Workstation ainsi qu'un ERP Odoo, ceux-ci dans le but de virtualiser la couche infrastructure et d'appliquer un système d'information.

Nous avons organisé notre mémoire en quatre (4) chapitres dont le contenu est brièvement décrit dans les points suivant :

— Le premier chapitre intitulé «Les systèmes d'informations au cœur des métiers» comporte trois partie : dont la première est consacré à définir des généralités sur le parc informatique et ses composants, dans la seconde partie nous présentons quelque définition sur l'analyse des risques en dernière partie tout ce qui concerne la virtualisation et l'émulation .

— Le deuxième chapitre titré « Introduction du cas d'étude » porte en premier lieu sur la présentation de la société d'accueil Général Emballage,son état des lieux qui consiste à définir l'infrastructure réseau, étudié le réseau de l'entreprise et Risques liés au système d'information, où nous exposerons la problématique ainsi que les objectifs à atteindre.

— Le troisième chapitre nommé «Études des solutions proposées» est consacré a la présentation de notre infrastructure réseau ainsi que toutes les installations et Configurations nécessaire pour la mise en œuvre de notre labo.

— Le quatrième chapitre intitulé «Tests et Validations» définit les différentes vérifications des fonctionnalités de Fortigate, test de réplications de Active Directory et test fonctionnement d'Odoo 13 ayant servis à l'émulation de notre implémentation , tout en expliquant les configurations établies .

Enfin, nous terminerons notre travail par une conclusion générale.

# Chapitre 1

# Les systèmes d'informations au cœur des métiers

## 1.1 Introduction

Le système d'information (SI) c'est l'ensemble des ressources de l'entreprise qui permettent la gestion de l'information. Le SI est généralement associé aux technologies matérielles, logiciel et communication, aux processus qui les accompagnent, et aux hommes qui les supportent [6].

Dans ce chapitre nous allons présenter le parc informatique et ses composants, l'analyse des risques , ainsi que tout ce qui concerne la virtualisation et l'émulation de la couche infratructure.

## 1.2 Première partie : Parc informatique et ses composants

Élément indissociable de l'infrastructure d'une entreprise, le parc informatique rassemble tout le matériel, les logiciels, les ressources réseau et les services composites nécessaires à l'existence, au fonctionnement et à la gestion de l'environnement informatique de celle-ci. Ça peut désigner des ordinateurs, des équipements de connectivité de réseaux et internet, des routeurs, ainsi que les pares-feux des systèmes de sécurité. Un parc informatique prend en compte l'envergure et le type d'activité de l'entreprise. Généralement, l'administration du parc informatique est confiée à un responsable informatique ou au service DSI [8].

### 1.2.1 Modèle d'architecture en couche des systèmes d'information

Un préambule à toute démarche, est de bien différencier entre Système d'Information et Système Informatique ! Le Système d'Information doit s'inscrire dans une vision fonctionnelle et plus pérenne que l'architecture informatique .

L'objectif de l'architecture SI est d'analyser, définir et cadrer l'évolution des systèmes d'information en fonction de la stratégie d'entreprise, des processus métier et des innovations technologiques.

Dans le domaine des SI, de nombreux modèle d'architectures existent, Ces architectures sont parfaitement identifiées et sont issues du résultat des différentes phases de conception d'un SI [14]. Nous présentons plus en détails les quatre couches des système d'information :

#### 1.2.1.1 Couche fonctionnelle

Elle représente l'aspect métier, c'est à dire ce que fait l'application et la nature des données qu'elle échange avec le reste du monde. Elle traite de tout ce que fait l'application : les données manipulées et comment elle s'inscrit dans son écosystème applicatif.

#### 1.2.1.2 Couche applicative

Elle est concentré sur l'aspect logiciel : les flux (protocole, fréquence, sens), les stocks (partage de donnée...), les middlewares (base de données, serveur java. . . ) et les frameworks utilisés (.NET, Java...). L'analyse de la couche applicative est aussi l'occasion de mettre en avant différents mécanismes offerts par les middlewares : réplication de données, partage de sessions, clustering, chiffrement des données... qu'il peut être pertinent de faire apparaître afin d'expliciter comment l'architecture présentée répond aux contraintes de services. En général, ce sont les mécanismes de la couche applicative, de la couche opérationnelle et de la couche technique qui vont permettre d'y répondre [14].

#### 1.2.1.3 Couche infrastructure

Globalement, la couche infrastructure traite l'ensemble des mécanismes sous-jacents qui proposent des ressources et garantissent la performance, la disponibilité et la protection des données . On parle ici de serveurs, de réseau, de stockage, de virtualisation, de sauvegarde, d'archivage, de cloud bien sûr. Elle permet aussi de décrire les choix techniques, les serveurs (dans le cloud ou ailleurs), leur dimensionnement, l'interconnexion via les réseaux, etc .

#### 1.2.1.4 Couche opérationnelle

La partie opérations est pourtant absolument essentielle et nécessite une vraie réflexion. En effet, la façon dont un système va être supervisé, mesuré, sauvegardé et ordonnancé va faire fortement varier sa résilience et son agilité [14] .


FIGURE 1.1 – Différentes couches du système d'information.

### 1.2.2 Parc matériel

#### 1.2.2.1 Infrastructure réseaux

La mise en place d'une infrastructure réseau constitue une obligation pour toute société moderne et ambitieuse. Celle-ci s'apparente à la charpente d'une organisation informatique. Le bon fonctionnement des équipements et logiciels en dépend. Elle favorise une transmission rapide et sécurisée des données .

#### 1.2.2.2 Différents dispositifs de sécurité et serveurs

Le parc dispositifs de sécurité est indispensable dans l'entreprise, Une bonne gestion de son matériel informatique présente des enjeux considérables en matière de sécurité des données, de pérennité du matériel, mais également de confort d'utilisation pour les employés.

a) **Présentation d'un pare-feu Fortigate de Fortinet**

Le module Firewall-FortiOS du pare-feu FortiGate de Fortinet est un composant essentiel de FortiOS pour apporter de la sécurité dans toute organisation possédant un réseau informatique. Son rôle principal est de bloquer les accès non autorisés[17].

FortiOS de Fortinet implémente un module UTM ( en français gestion unifiée des menaces) de Firewall basé sur une gestion unifiée des accès avec le classique contrôle par adresses IP,par utilisateur et par machine.Il permet également très facilement d'appliquer des fonctionnalités avancées telles que l'antivirus, l'IPS, le contrôle applicatif, tout en offrant des fonctionnalités de qualité de service,de translation d'adresse etc .

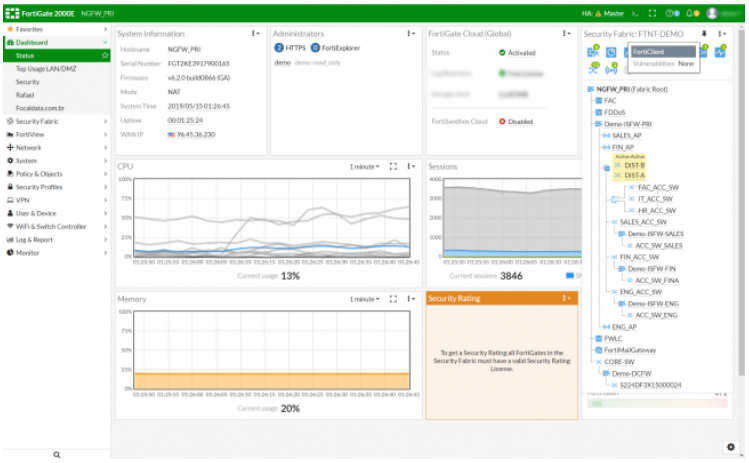

FIGURE 1.2 – L'interface graphique du pare-feu Fortigate.

- **Fonctionnalités et avantages du pare-feu Fortigate**

  — Visibilité intégrale : L'inspection des flux chiffrés sous SSL, et TLS1.3 notamment, supprime les zones d'ombre.

  — Protection Contre Les Menaces : La sécurité la plus intégrée du marché avec une protection automatisée contre les menaces.

  — Intégration avec la Security Fabric : Assure le partage des informations sur les menaces sur l'ensemble de la surface d'attaque pour accélérer et automatiser la protection.

  — Fabric Management Center : Automatisation, orchestration et traitement analytique à partir d'une console de gestion unifiée.

  — Efficacité éprouvée de la sécurité : Une veille sur les menaces permanente et certifiée protège contre les menaces connues et inconnues.

- **Filtrage web et applicatif de Fortinet**

Le filtrage Web est un moyen de contrôler le contenu qu'un internaute est autorisé à consulter. Avec la popularité croissante des applications web le besoin de surveiller et contrôler les accès à l'Internet devient un composant clé de la gestion sécurisée des contenus incluant l'antivirus, le filtrage web et la sécurité des messages électronique [17].

Dans le filtrage de niveau applicatif, également appelé proxy, le pare-feu agit comme un filtre au niveau applicatif, c'est-à-dire au niveau 7 (couche application) du modèle OSI.

- **Zone**

Les zones sont un groupe d'une ou plusieurs interfaces FortiGate physiques ou virtuelles auxquelles des politiques de sécurité peuvent être appliquer pour contrôler le trafic entrant et sortant. Le regroupement d'interfaces et de sous-interfaces VLAN dans des zones simplifie la création de stratégies de sécurité où un certain nombre de segments de réseau peuvent utiliser les mêmes paramètres de stratégie et profils de protection [1].

- **VPN IPSec**

Parmis les principaux objectifs du VPN est la sécurité des données lorsqu'elles traversent un réseau public. Le cryptage des données est une façon de les protéger en déployant des dispositifs de chiffrement/déchiffrement sur chaque site. IPSec est une suite de protocoles qui fournit des services sécurisés sur des réseaux IP à commutation de paquets. Un VPN IPSec déployé sur l'Internet public peut représenter une économie de coûts significative pour une entreprise par rapport à un VPN en ligne louée. Les services IPSec permettent l'authentification, l'intégrité, le contrôle d'accès et la confidentialité ainsi les informations échangées entre les sites distants peuvent être cryptées et vérifiées [9].

- **Haute disponibilité**

La haute disponibilité est un terme souvent utilisé en informatique, à propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable. HA est un composant crucial de la plupart des réseaux puisque tout le trafic la traverse. Une passerelle de sécurité réseau autonome est un point de défaillance unique qui est vulnérable à un certain nombre de problèmes logiciels ou matériels qui pourraient compromettre l'appareil et arrêter tout le trafic sur le réseau.

b) **Zone démilitarisée**

Un DMZ est un emplacement sur un réseau qui est ouvert d'Internet tout en sécurisant le

réseau local derrière un Pare-feu. La séparation du réseau principal d'un seul hôte ou d'un sous-réseau entier, ou du « sous-réseau » s'assure que les gens visitant votre service tel que le jeu, la vidéoconférence, le Web, ou les serveurs de mail d'Internet par l'intermédiaire du DMZ, n'auront pas accès au réseau local [10]. Cisco offre deux méthodes d'utiliser DMZs qui est l'hôte DMZ et le matériel DMZ. L'hôte DMZ permet un hôte sur le RÉSEAU LOCAL à exposer à l'internet tandis que le matériel DMZ (sous-réseau/plage) est un sous-réseau qui est ouvert au public [10].

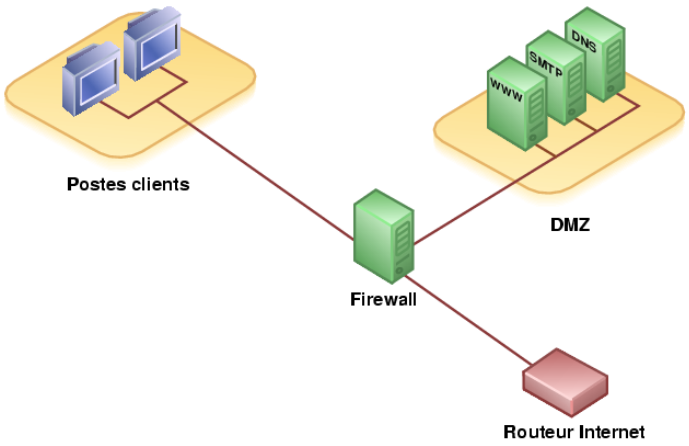


FIGURE 1.3 – Zone Démilitarisée.

c) **Serveurs Active Directory et domain name server.**

— Active Directory (AD) est un service d'annuaire destiné aux environnements Windows Server. Il s'agit d'une base de données LDAP distribuée et hiérarchisée qui partage des informations relatives à l'infrastructure permettant de localiser, de sécuriser, de gérer et d'organiser des ressources ordinateur, utilisateurs, groupes, périphériques et appareils réseau. Il fournit des protocoles d'authentification et d'autorisation intégrés et de grande ampleur [15].

— Les serveurs DNS (Domain Name System) exécutés sur des contrôleurs de domaine peuvent stocker leurs zones dans les services de domaine Active Directory (AD DS). De cette façon, il n'est pas nécessaire de configurer une topologie de réplication DNS distincte qui utilise des transferts de zone DNS ordinaires, car toutes les données de zone sont répliquées automatiquement au moyen de la réplication Active Directory [15].

d) **Commutateurs**

Un commutateur est un boîtier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier en réseau différents éléments du système informatique. Il permet notamment de créer différents circuits au sein d'un même réseau, de recevoir des informations et d'envoyer des données vers un destinataire précis en les transportant via le port adéquat. Le switch contribue à la sécurité du réseau et à la protection des données échangées via le réseau. D'autre part, il permet de connecter davantage de postes de travail sur le même réseau Ethernet.[10].

— **Virtual local area network**

Un VLAN (Virtual Local Area Network, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique. les VLANs multiplient les capacités de l'unité FortiGate et peuvent également fournir une sécurité réseau supplémentaire. Ils utilisent des balises d'identification pour séparer logiquement les périphériques d'un réseau en domaines de diffusion plus petits. Ces domaines plus petits transfèrent les paquets uniquement aux périphériques qui font partie de ce domaine VLAN. Cela réduit le trafic et augmente la sécurité du réseau.

### 1.2.3 Parc logiciel

Un logiciel spécialisé constitue une excellente solution pour faciliter la gestion d'un parc de logiciel. En effet, elle consiste dans un premier temps à réaliser un inventaire exhaustif du matériel et des programmes installés, ce qui fournit des informations pertinentes pour maintenir, protéger et faire évoluer le système informatique d'une entreprise. Un logiciel de gestion d'un parc logiciel permet de faciliter de nombreuses démarches, voire de les automatiser, afin d'avoir un matériel et des programmes constamment à jour, ce qui est essentiel pour réduire les risques et améliorer les performances.

Dans le parc logiciel on trouve :

- Les systèmes d'exploitations (Windows 7, 8, 10, XP).
- Les éditeurs de texte (Word, Excel, ...).
- Progiciel de Gestion Intégré (entreprise ressource planning).
- Les logiciels conçus pour les réseaux et même des logiciels de base de données (MySQL, SGBD, oracle, ...).

#### 1.2.3.1 Enterprise Ressource Planning

Le terme ERP «Enterprise Ressource Planning en français Progiciel de gestion intégré» se définit comme un groupe de modules relié à une base de données unique. L'ERP est un logiciel de gestion qui permet à l'entreprise d'intégrer différentes fonctionnalités telles que [18] :

— La gestion comptable et financière.

— La gestion des stocks.

— La gestion des ressources humaines.

— La gestion des fournisseurs (ERP fournisseurs grande distribution).

— La gestion de la vente.

— La gestion de la distribution.

— La gestion de commerce.

Dans la figure (1.4) nous distinguons les différentes fonctionnalités de l'ERP.


FIGURE 1.4 – Fonctionnalités d'ERP.

En complément d'un ERP et dans le cadre d'une démarche de satisfaction client, de nombreuses entreprises se dotent aussi d'un logiciel de CRM. Cet outil leur permet de mettre en commun et de maximiser la connaissance d'un client donné et ainsi de mieux comprendre, anticiper et gérer ses besoins [18].

#### 1.2.3.2 ERP Odoo

Odoo est une suite d'applications métiers open source qui couvrent tous les besoins de votre entreprise : CRM ,commerce , comptabilité, inventaire, point de vente, gestion de projet, etc. Sa proposition de valeur unique est d'être à la fois très simple d'utilisation et entièrement intégré.

Odoo existe en deux versions, une version Enterprise hébergée sur les serveurs de Odoo qui est uniquement éditable par eux, et une version Community que l'on peut installer gratuitement sur un serveur personnel et ainsi le modifier à sa guise[16]. Odoo contient entre autres les fonctionnalités suivantes :

Gestion des achats : permet de prendre en charge les achats de fournitures d'une entreprise.

Gestion des ventes : permet de prendre en charge les ventes de biens ou services de l'entreprise.

Gestion de projets : propose une gestion de projet standard

MRP : permet de gérer des lignes de production, gestion des commandes, planification des commandes

Gestion de stock : permet une gestion des fournitures d'une entreprise, peux gérer des entrepôts multiples et les mouvements entre ces entrepôts.

Points de vente : propose une interface spéciale pour simuler une caisse enregistreuse pour faire de la vente au comptoir.

Ressources Humaines : permet de gérer ce qui concerne les employés.

Comptabilité et Finance : permet de gérer les mouvements financiers, faire des rapports comptables, etc.

CRM : permet des faire de la gestion de clientèle, des prospections, des historiques d'appels, des campagnes marketings

Facturation : permet la gestion de la facturation des clients et fournisseurs.


FIGURE 1.5 – L'ERP ODOO.

#### 1.2.3.3 Gestion de la relation client

Le CRM, Customer Relationship Management ou Gestion de la Relation Client en français, est un concept préconisant la centralisation au sein d'une base de données de toutes les interactions entre une entreprise et ses clients. Cela permet de mettre en commun et de maximiser la connaissance d'un client donné et ainsi de mieux comprendre, anticiper et gérer ses besoins.


FIGURE 1.6 – Les Taches d'un CRM.

- **Les point fort du CRM**

En collectant et en organisant les données d'interaction client, en les rendant accessibles tous et en facilitant l'analyse, le CRM offre de nombreux avantages :

— Collaboration en équipe.

— Augmentation de la productivité.

— Gestion des ventes dynamisée.

— Prévisions de ventes précises.

— Meilleure satisfaction et fidélité des clients.

— Retour sur investissement marketing plus rentable.

— Meilleurs produits et services

## 1.3 Deuxième partie : Analyse des risques

L'analyse de risques et l'audit de sécurité sont deux outils complémentaires et indispensables pour sécuriser un systèmes d'information.

### 1.3.1 Risques et menaces sur la sécurité du système d'informations

Le risque informatique est devenu l'une des préoccupations principales pour la grande majorité des entreprises, quelque soient leur taille et leur secteur d'activité, dont nous citons la perte de données, Piratage de données, Phishing, et l'intrusion.

• **Perte de données :** Elle peut être le fait de la perte ou d'un vol de matériel (ordinateur, disque dur, etc.), sur lequel sont stockées des données non chiffrées d'une infiltration du pirate dans le réseau informatique via le cloud ou le wifi par exemple ; ou même du comportement des collaborateurs. Sur ce dernier point, il est évidemment primordial de prendre en compte le risque humain : mauvaises manipulations, négligences ou même malversations .

• **Piratage de données :** Il prend la forme de logiciel (malware ou spyware), de virus et de vers qui vont infecter le système informatique d'une entreprise pour en bloquer les données. Une fois les données cryptées et inaccessibles, les pirates demandent une rançon à l'entreprise pour les récupérer [13].

• **Phishing :** Le phishing est une forme de fraude dans l'environnement en ligne qui consiste à utiliser des techniques pour manipuler l'identité d'individus/organisations afin d'obtenir des avantages matériels ou des informations confidentielles. Les attaquants utilisent diverses techniques d'ingénierie sociale pour persuader les victimes de divulguer des données d'authentification. Les cibles les plus courantes sont les sites Web des institutions financières, telles que les banques [13]

• **L'intrusion :** Les failles de sécurité et les connexions non sécurisées permettent aussi au pirate de prendre connaissance de données confidentielles ou de prendre contrôle de certains appareils. Permettant ainsi l'espionnage d'informations sensibles et de conversations ou encore la manipulation des systèmes de la chaîne de production (imprimante, alimentation, commandes, etc.). [13].

### 1.3.2 Dispositifs de sécurité dans les réseaux informatiques

Toutes les sociétés, quelles que soient leur taille ou leur activité, sont confrontées à des problématiques de sécurité informatique en entreprise. De nombreuses menaces pèsent sur l'infrastructure ainsi que sur les données et nous devons mettre en œuvre tous les dispositifs nécessaires pour assurer la protection, de nombreuses solutions permettent de les éviter. Voici quelque dispositifs pour la sécurité informatique.

• **Des systèmes anti-virus et anti-spams :** La messagerie est le principal point d'entrée

des menaces informatiques. Les virus, malwares et logiciels espions se diffusent principalement par l'intermédiaire des pièces jointes et emails. D'autre part, des cybercriminels peuvent tenter des manœuvres d'ingénierie sociale pour tromper les collaborateurs et obtenir des données capitales comme des mots de passe. Nous devons impérativement sécuriser le mieux possible la messagerie d'entreprise en installant des système anti-virus et anti-spams efficaces[7].

- **Une bonne solution d'hébergement des données :** Les TPE et PME sont devenues la principale cible des cybercriminels. En effet, elles sous-estiment souvent les risques d'attaques informatiques et négligent la sécurité de leurs données [7]. Or,faut être en mesure de restaurer rapidement les données en cas d'attaque et de les protéger efficacement contre les cybercriminels et les sinistres.
- **Un système de monitoring du SI :** De nombreuses TPE subissent des attaques informatiques sans même s'en rendre compte [7]. Un système de monitoring permet de surveiller de près l'infrastructure informatique et d'assurer le bon fonctionnement des divers éléments qui la constituent. Le monitoring informatique permet de détecter toute activité inhabituelle de votre système informatique et ainsi, d'intervenir rapidement cas de problème.
- **Un technicien disponible :** Le principal élément d'une bonne sécurité informatique en entreprise est le fait de pouvoir compter sur un technicien efficace et disponible en cas de problème. Les pannes et incidents informatiques ralentissent significativement les activités de l'entreprise en cas d'attaque, nous devons pouvoir bloquer rapidement l'intrus ou empêcher la propagation du virus sur le réseau informatique[7].

## 1.4 Troisième partie : virtualisation, simulation et émulation

L'émulation et la virtualisation atteignent le même objectif : exécuter un autre système d'exploitation dans une machine virtuelle. Cependant, chacun fait cela différemment, et quand il peut être utilisé, la virtualisation est beaucoup plus rapide.

### 1.4.1 Virtualisation

La virtualisation consiste à la création d'une ou plusieurs machines virtuelles à partir d'une machine physique telle qu'un serveur ou un ordinateur. Un logiciel nommé hyperviseur est alors

chargé de faire le lien entre les propriétés de l'entité physique et celles de l'entité virtuelle. L'hyperviseur attribue des propriétés propres à chaque machine virtuelle afin de répondre au mieux aux besoins spécifiques du projet informatique [12].

#### 1.4.1.1 Différents types de virtualisation

L'environnement virtuel peut être créé à partir d'une instance unique (par exemple, un serveur virtuel peut être la copie d'un serveur physique) ou bien être le résultat de l'association de plusieurs systèmes virtuels. Voici quelques déclinaisons possibles [12].

— Virtualisation hardware ou matérielle : La virtualisation hardware est utilisée pour la gestion des applications. Elle consiste à regrouper tous les serveurs physiques transformés en serveurs virtuels en un seul serveur physique. La virtualisation hardware implique donc directement la gestion du matériel informatique. Elle permet de libérer le processeur pour le faire tourner plus vite et plus efficacement, tout en ne représentant qu'une seule entité pour les autres matériels.

— Virtualisation réseau : Elle consiste à reproduire virtuellement un réseau physique existant. Les ressources matérielles du réseau sont alors combinées en plusieurs canaux virtuels, permettant de consommer moins de bande passante. Les différentes parties créées par la virtualisation sont alors plus simples à gérer. Plus concrètement, il devient plus facile de voir comment les données sont utilisées.

— Virtualisation des serveurs : permet d'exécuter plusieurs systèmes d'exploitation sur un seul serveur physique sous forme de machines virtuelles. Elle permet une efficacité accrue, une réduction des coûts, un déploiement plus rapide des workloads, une augmentation des performances d'application, une disponibilité de serveur en hausse, et l'élimination des complications liées à la gestion de serveurs.

#### 1.4.1.2 Avantages de la virtualisation

Les différentes formes de virtualisation présentent des avantages et des inconvénients spécifiques. Voici les principaux avantages :

— La baisse de la consommation en énergie

— Plus de portabilité

— Plus de disponibilité

— La virtualisation permet de créer un environnement de test.

— Plus d'obligation de réinstaller les serveurs

#### 1.4.1.3 Inconvénients de la virtualisation

Voici quelques critères à prendre en compte avant de virtualiser un serveur, un réseau ou un espace de stockage [12].

— La nécessité de disposer d'un matériel adapté.

— Une sécurisation immatérielle.

— La nécessité de former les équipes informatiques.

— Des performances moindres en virtuel qu'en physique.

### 1.4.2 Simulation et émulation

La simulation en général est une représentation fictive de la réalité. elle revien à reproduire l'architecture d'un réseau ,Il existe plusieurs logiciels de simulation réseaux mais nous avons choisis GNS3 Comme son nom l'indique, "Graphical Network Simulator" (GNS3) c'est un simulateur réseaux graphiques et encore c'est un outil de simulation de réseaux open source, multiplateforme, gratuit. [11].

#### 1.4.2.1 Présentation de GNS3

GNS3 est un logiciel libre et gratuit qui est utilisé par des centaines de milliers d'ingénieurs réseau dans le monde entier pour émuler, configurer, concevoir et tester des réseaux virtuels et réels de toute taille sans recourir à l'infrastructure matérielle physique. Il permet d'établir avec précision la topologie d'un système d'exploitation réseau pour des fonctions avancées de routage, de pare-feu ou d'hôte, GNS3 se base sur :

— L'émulateur Dynamips pour émuler les routeurs et les commutateur cisco à travers la couche logicielle de contrôle de gestion.

— L'émulateur de processeurs QEMU pour émuler des machines virtuelles à base de différentes architectures.

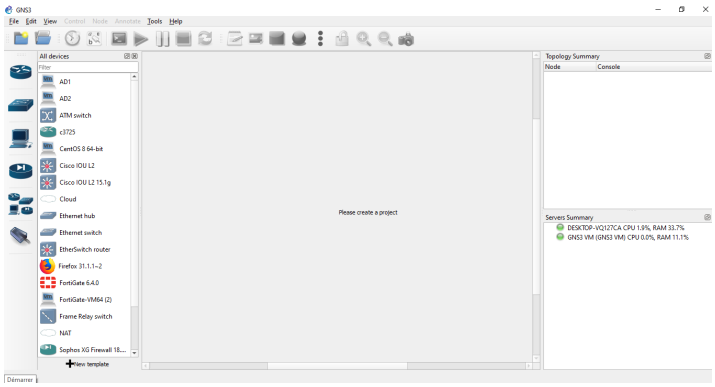


FIGURE 1.7 – L'interface graphique de GNS3.

Pour pouvoir installer n'importe quel appareil sur GNS3 et non pas seulement les équipements CISCO, il faut donc installer GNS3 VM et pour cela, nous avons besoin d'un hyperviseur qui est VMware Workstation.

L'émulation est l'imitation du comportement physique d'un matériel par un logiciel, et ne pas la confondre avec la simulation, laquelle vise à imiter un modèle abstrait. L'émulateur reproduit le comportement d'un modèle dont toutes les variables sont connues, alors que le simulateur tente de reproduire un modèle mais en devant extrapoler une partie des variables qui lui sont inconnues [11].

### 1.4.2.2 Présentation de VMware

Il permet d'émuler des systèmes d'exploitation complets c'est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique.

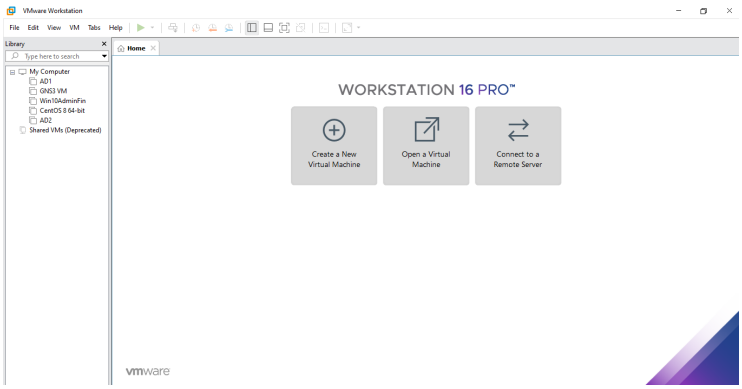


FIGURE 1.8 – L'interface graphique de VMware workstation 16.

## 1.5 Conclusion

Dans ce chapitre nous avons défini le parc informatique et ses composants ,l'anayse des risques et nous avons présenté dans la troisième partie les outils que nous allons utilisée pour la virtualisation et l'émulation de notre infrastructure réseaux.

Dans le chapitre suivant nous allons présenter la société d'accueil et parler sur l'état des lieux.

# Chapitre 2

# Introduction du cas d'étude

## 2.1 Introduction

Dans ce chapitre nous allons présenter SPA Général Emballage , nous y ferons une présentation du réseau informatique et ensuite l'état des lieux de l'entreprise dont nous allons discuter sur ses normes ISO ainsi que les risques liés au système d'information pour mieux connaitres ses objectifs. et Enfin nous allons énumérer les insuffisances et proposer des solutions qui résoudront les anomalies constatées.

## 2.2 Première partie : Présentation de la société d'accueil

### 2.2.1 Présentation de Général Emballage

Général Emballage est leader en Algérie de l'industrie du carton ondulé. Il fabrique, à la commande, des plaques double- face (cannelures B, C, E et F) et double-double (BC et BE), des emballages et des displays. Et réalisons des post-impressions en Haute résolution jusqu'à 6 couleurs avec vernis intégral ou sélectif.

Les équipes maîtrisent l'ensemble des tâches de production : études, prototypage, réalisations de formes de découpe et de films d'impression, fabrication des emballages et des displays, livraison. Entré en exploitation en 2002, Général Emballage est une Société de capitaux avec un capital social de 2.000.000.000 DZD opérant sur 3 sites industriels (Akbou, Oran et Sétif) avec près d'un millier d'employés et un chiffre d'affaire de 6 milliards DZD. Général Emballage est une entreprise certifiée ISO 9001 :2008. Son siège social est à ZAC Taharacht, Akbou, dans la wilaya (gouvernorat) de

Béjaia.

RC N° : 00 B 0183268 du 05/08/2009.

NIF : 000006018326879.

Article d'imposition : 06256000300.

NIS : 099806250344426.

FIGURE 2.1 – SPA Général Emballage site Taharacht Akbou et son logo.

### 2.2.2 Historique de l'entreprise Général Emballage

— En 2000, 1er Août Création de la SARL Général Emballage avec un capital de 32 millions de dinars dans la Zone d'activités de Taharacht (Akbou.W. de Béjaia) (décision APSI N°13051 du 06 juin 1998).

— En 2002, Entrée en production de l'usine d'Akbou avec un effectif de 83 employés

— En 2006, Le capital est porté à 150 millions de dinars et comptait un Effectif de 318 employés.

— En 2007, Le capital est porté à 1,23 milliards de dinars,l'Entrée en production de l'usine de Sétif, elle comptait un Effectif de 425 employés ainsi elle remporte le Trophée de la Production (Euro-Développement PME).

— En 2008, le Début d'exportation vers la Tunisie et l'entrée en exploitation de l'unité d'Oran.

— En 2009, L'Augmentation du capital à 2 milliards de DA et entrée de MAGHREB PRIVATE EQUITY FUND II « Cyprus II» (MPEF II) avec une participation de 40et elle devient une société de capitaux (Société par actions) avec un Effectif de 597 employés.

— En 2010, avec son chifre d'afaires elle parvenait à occuper une place parmi les 50 grandes entreprises algériennes avec un Effectif de 630 employés.

— En 2011, la capacité totale de production des trois usines d'Akbou, d'Oran et de Sétif était de 130 000 tonnes, soit 80 pour cent de la consommation algérienne et elle comptait un Effectif de 699.

— En 2012, leurs capacités de production sont portées à 130.000 tonnes, L'usine d'Oran est transférée à la ZI Hassi-Ameur, la Production des premiers ouvrages en Haute résolution, Signature d'une Convention cadre de partenariat avec l'Université de Béjaia et elle comptait un Effectif de 830 employés.

— En 2013, Général Emballage a obtenu la Certification ISO 9001 :2008, Démarrage de la 1ère promotion de Licence en Emballage et Qualité à l'Université de Bejaïa et elle comptait un Effectif de 960 employés.

— En 2014, Signature d'un protocole d'accord de recrutement avec l'Agence Nationale de l'Emploi, Début des exportations vers la Libye et elle comptait un Effectif de 1005 employés.

— En 2015, l'Entrée en production de la nouvelle usine de Sétif à ZI Ain Sfiha, elle remporte le Prix d'encouragement du Trophée Export 2014 (World Trade Center (WTCA) et elle comptait un Effectif de 1100 employés.

— En 2016, la 1ere exportation en Espagne, Sortie de Maghreb Private Equity Fund et entrée de Development Partners International (DPI) et de la Deutsche Dation Investitions und Entwicklungsgesellschaft mbH (DEG) à hauteur de 49 pour cent du capital social, 1ere exportation en Mauritanie et elle comptait un Effectif de 1170 employés.

— En 2019, cet entreprise est Distinguée comme entreprise « inspirante » pour l'Afrique dans le Rapport « Compagnies to inspire Africa 2019 » du London Stock Exchange Group (Bourse de Londres), fait sa Première expédition sur la Belgique et la Première exportation sur la France, remporte le Prix spécial du jury du Trophée Export 2018 (World Trade Center (WTCA) et elle comptait un Effectif de 1201 employés.

— En 2020, Général Emballage a obtenu Certifications ISO 14001 :2015 et ISO 45001 :2018 et et elle comptait un Effectif de 1222 employés.

### 2.2.3 Evolution des effectifs

| ANNEE | Unité AKBOU | Unité SETIF | Unité ORAN | Unité ALGER | TOTAL GE |
|---|---|---|---|---|---|
| 2002 | 83 | / | / | / | 83 |
| 2003 | 165 | / | / | / | 165 |
| 2004 | 176 | / | / | / | 176 |
| 2005 | 185 | / | / | / | 185 |
| 2006 | 318 | / | / | / | 318 |
| 2007 | 439 | / | / | / | 439 |
| 2008 | 479 | / | / | / | 479 |
| 2009 | 189 | 56 | 40 | / | 585 |
| 2010 | 528 | 59 | 43 | / | 630 |
| 2011 | 589 | 54 | 56 | / | 699 |
| 2012 | 528 | 59 | 43 | / | 630 |
| 2013 | 812 | 87 | 61 | / | 960 |
| 2014 | 819 | 115 | 76 | / | 1010 |
| 2015 | 802 | 290 | 87 | / | 1179 |
| 2016 | 777 | 331 | 84 | / | 1192 |
| 2017 | 774 | 323 | 90 | / | 1187 |
| 2018 | 774 | 334 | 93 | / | 1201 |
| 2019 | 772 | 332 | 118 | / | 630 |
| 2020 | 771 | 348 | 135 | 25 | 1279 |

TABLE 2.1 – Evolution des effectifs par catégorie socioprofessionnelle.

- **Evolution des effectifs par catégorie socioprofessionnelle**

| UNITE | CADRE | MAITRISE | EXECUTION | TOTAL |
|---|---|---|---|---|
| GE DG | 39 | 89 | 65 | 83 |
| GE AKBOU | 33 | 149 | 446 | 628 |
| GE SETIF | 19 | 71 | 258 | 348 |
| GE RECUP/DECHET | 3 | 2 | 20 | 25 |
| GE ORAN | 8 | 31 | 96 | 135 |
| TOTAL | 102 | 292 | 885 | 1279 |
| taux | 7,97 % | 22,83% | 69,18% | / |

TABLE 2.2 – Evolution des effectifs des sites de GE.

### 2.2.4 Valeurs de Général emballage

- **Leadership :**

Les politiques d'investissement, de recrutement et de formation reposent sur deux principes fondamentaux : satisfaire la demande et anticiper sur les besoins du futurs du marché. Il en découle une mise à niveau continuelle des compétences humaines et des process technologiques.

- **Proximité :**

Ils entretiennent le rapprochement avec leurs clients pour une meilleure compréhension de leurs besoins et pour réduire les coûts et les délais d'acheminement de leurs produits et garantir le meilleur rapport qualité/prix.

- **Citoyenneté :** Général Emballage est une entreprise citoyenne qui inscrit son intérêt dans celui de la société et de l'humanité en général.

- **Développement Durable :** Général Emballage s'engage à :

— Recycler l'ensemble de ses déchets de production et de ses rejets industriels.

— A ne se fournir qu'auprès d'industries respectant les principes du Développement durable.

— A apporter sa contribution aux efforts visant la préservation de l'environnement et notamment aux actions de reforestation.

### 2.2.5 Plans du réseau de l'entreprise

La figure suivante représente les plans fournit par l'entreprise et qui détaille les différentes zones et les différents sites (Oran, Setif, Alger et Akbou qui est notre cas d'étude) définis par l'entreprise.

Nous retrouvons un pare feu FORTINET lié directement au CLOUD qui est lié par la suite aux différents sites existants, ainsi on retrouve La zone A contenant des réseaux LANs, reliés avec un Switch géré par un pare-feu Fortinet et la zone B qui est une zone démilitarisée contenant les multiples serveurs.

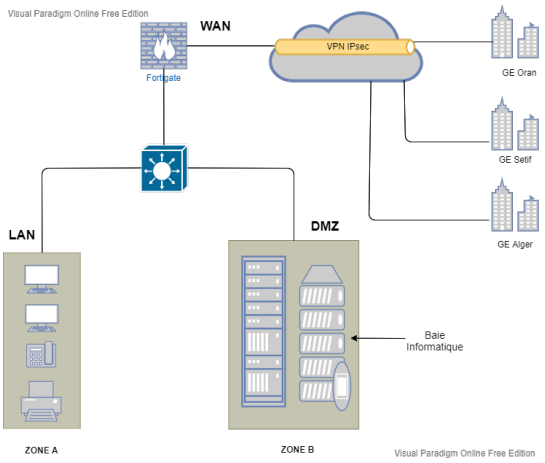


FIGURE 2.2 – Plan du réseau de l'entreprise.

## 2.3 Deuxième partie : Etat des lieux

### 2.3.1 Présentation de l'infrastructure réseau

Général emballage dispose d'un réseau interne assez vaste permettant de relier les différents bâtiments, unités de production et direction du complexe. Nous pouvons le décomposer en trois parties qui sont la partie Core, Distribution et Access. Le réseau est composé de plusieurs équipements interconnectés entre eux par fibre optique, ou cuivre ; nous citons :

— 07 Serveurs Physique (Dell Power Edge R730, R740...).

— 200 Ordinateurs.

— 02 Firewalls Fortigate (Fortinet) en redondance.

— 21 Switchs CISCO (2960, 3750... ).

- Schéma général de l'architecture réseau

La couche accès du réseau est composée de switch niveau 2, C2960, ainsi que des points d'accès Fortinet pour couvrir les zones non accessibles via le câblage Ethernet.

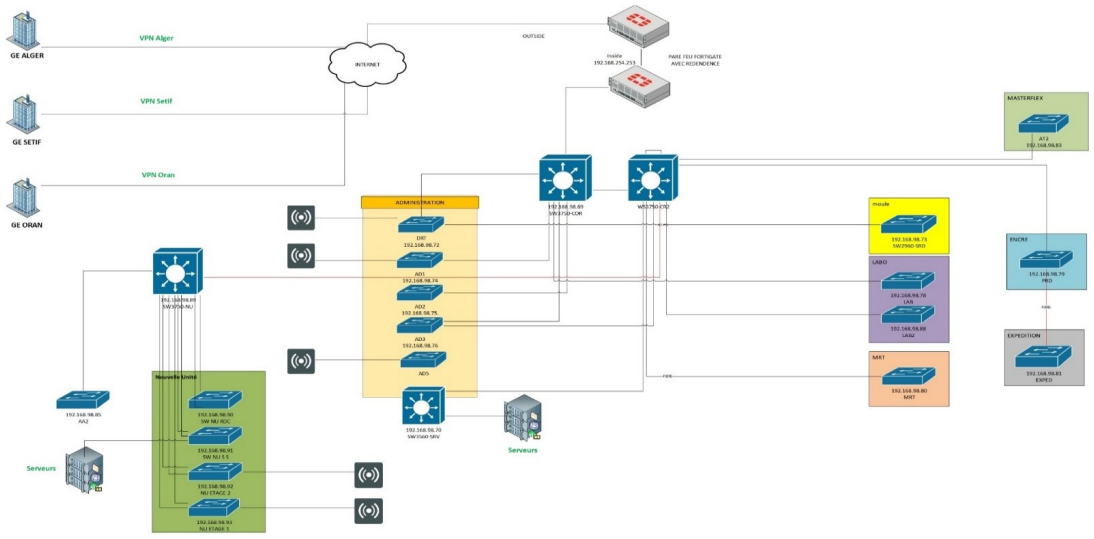


FIGURE 2.3 – Architecture réseau LAN General Emballage Akbou.

### 2.3.2 Normes ISO de General Emballage

- **ISO 9001 (MANAGEMENT DE LA QUALITÉ)**

Elle définit les critères applicables à un système de management de la qualité. Il s'agit de la seule norme de la famille ISO 9000 à pouvoir être utilisée pour la certification ; Cette norme repose sur un certain nombre de principes de management de la qualité, notamment une forte orientation client, la motivation et l'engagement de la direction, l'approche processus et l'amélioration continue[3].

- **ISO 14001 (MANAGEMENT ENVIRONEMENTAL))**

Définit les critères d'un système de management environnemental et se prête à la certification. Elle propose un cadre que les entreprises peuvent appliquer pour mettre en place un système efficace de management environnemental.

ISO 14001 établit les exigences associées à des lignes directrices de mise en œuvre de la norme dans le cadre de systèmes environnementaux. D'autres normes de cette famille sont axées sur des approches spécifiques telles que les audits, les communications, l'étiquetage et l'analyse du cycle de vie, et traitent également des défis environnementaux associés au changement climatique [3].

- **ISO 19011**

La norme ISO 19011 est une norme internationale qui établit des directives pour l'audit des systèmes de management, Elle est développée par l'Organisation internationale de normalisation [3]. Cette norme propose quatre ressources pour les organisations afin de gagner du temps, de l'effort et de l'argent :

- Une explication claire des principes d'audit des systèmes de management.
- Des lignes directrices sur la gestion des programmes d'audit.
- Des lignes directrices sur la conduite des audits internes ou externes.
- Des lignes directrices sur l'évaluation de la compétence des auditeurs.

- **ISO 45001 (SANTÉ ET SÉCURITÉ AU TRAVAIL)**

C'est la nouvelle norme ISO relative à la santé et à la sécurité au travail (SST), elle vise à fournir un lieu de travail sûr et sain pour les travailleurs et les visiteurs. Pour y parvenir, il est essentiel de maîtriser l'ensemble des facteurs susceptibles d'entraîner des maladies, des traumatismes et, dans le pire des cas, des décès, en atténuant les effets préjudiciables pour l'état physique, mental et cognitif d'une personne et ISO 45001 couvre l'ensemble de ces aspects que les organismes choisissent ou non de l'adopter.

Cette norme est appelée à s'imposer comme exigence à part entière dans les entreprises et il est important que ces dernières se tiennent informées des développements les plus récents [3].

### 2.3.3 Etude du réseau de l'entreprise

- **Equipements actifs**

**Equipements d'interconnexion**

— Equipements de sécurité Pare-feu (Fortinet) : Les pare-feu nouvelle génération de Fortinet sont équipés de processeurs SPU (Security Processing Units), et des services de sécurité des FortiGuard Labs. Le pare-feu dont dispose l'entreprise : Fortinet (Fortios 6.2.3).

— Points d'accées Les points d'accès FortiAPs existent en plusieurs modèles et a des tarifs diffèrent. Le réseau sans fil se configure et se gère via la plateforme de sécurité FortiGate.

— Routeur Cisco : C'est un périphérique intermédiaire dans un réseau informatique qui a pour rôle d'assurer le routage des paquets entre réseaux indépendants. Il aide à mettre en place un

réseau plus intelligent, plus réactif et mieux intégrées les routeurs dont dispose l'entreprise : Routeur CISCO 2801.

— Switch Cisco : Le commutateur réseau est un équipement reliant les multiples segments d'un réseau informatique et dispose de multiples services de sécurité. Les commutateurs Cisco, sont évolutifs et économiques et répondent aux besoins de toute taille d'entreprise. Le switch dont dispose l'entreprise : Switch Cisco 3750, Switch Cisco 2960.

— Switch D-Link : Les commutateurs D-Link, étaient parmi les premiers, économiques et ils accomplissent leur fonction par rapport aux besoins de l'entreprise.

**Equipements terminaux**

— serveur : C'est un equipement informatique qui fournit des services a un ou plusieurs clients. les services les plus courants sont :

- La sauvegarde de données.
- L'accées aux informations du World Wide Web .
- Le courrier électronique.
- Le partage d'imprimantes.
- Le commerce électronique.
- Le stockage en base de données.
- La gestion de l'authentifcation et du controle.
- Le jeu et la mise à disposition de logiciels applicatifs (optique software as a service).

- **Equipements passifs**

— Les câbles : pour que l'entreprise assure le cablage, elle utilise :

- La fibre optique.
- Des connecteurs RJ45.

— Armoire de brassage : BAIE informatique.

— Tiroir optique coulissant 19 pouces.

- **Equipements logiques**

— Systémes d'Exploitation Windows et Linux.

— Systemes de BACKUP sauvegarde automatique .

— Antivirus kaspersky.

— Bureautique Microsoft Once.

— Protection d'accées :active directory.

- **Equipements service de connexion**

— Connexion : ISO/CEI 8802-11 wifi.

— Messagerie : General Emballage.

— Annuaire LDAP.

### Data center

Le data center est une pièce sécurisée, l'accès y est restreint, seul les responsables et techniciens de la DSI (Direction Système d'Information) y ont accès, la température est contrôlée par un système d'air conditionné et l'alimentation électrique est doublée permettant ainsi de veiller au bon fonctionnement des équipements qui s'y trouvent. Le data center de Général emballage constitue le noyau central du réseau de l'entreprise, on y trouve :

— Les serveurs de l'entreprise.

— Le Switch cœur et les routeur

— Les pare feu.

— Le standard téléphonique

## 2.3.4 Analyse de l'existant

C'est la phase du projet qui nous permettra d'auditer les processus et les solutions informatiques existants. Elle est réalisée avant l'initialisation du changement. Elle permet de préparer l'analyse des besoins de la solution cible et de réaliser l'analyse des écarts .

| Question | Réponse |
|---|---|
| <u>Sécurité et sûreté du réseau</u> | |
| Présence d'un pare-feu ? | Aucun pare-feu sur le réseau<br>Oui mais il n'est pas mis à jour<br>**Oui mis à jour régulièrement** |
| Les appareils importants sont-ils reliés à un onduleur ? | Non<br>En partie<br>**Oui** |
| La baie serveur est-elle nettoyée ? | Non<br>**Oui, tous les mois**<br>Oui, toutes les semaines |
| Existe-t-il un plan réseau ? | Non<br>Oui mais pas mis à jour<br>**Oui tout le réseau et mis à jour Régulièrement** |
| Les deux pare-feu sont-ils directement liées a internet ? | Non<br>**un seul**<br>les deux |
| Les serveurs et autres appareils sont-ils dans des locaux sécurisés ? | Non<br>peu<br>**Oui** |

| Sécurité des SI | |
|---|---|
| Avez-vous, un jour, procédé à un audit de sécurité du système d'information de votre entreprise par une entreprise externe ? | Non<br>Une fois<br>**Régulièrement** |
| Avez-vous procédé à un inventaire des OS et logiciels, installés sur le matériel fixe et portable de l'entreprise ? | Non<br>Occasionnellement<br>**Régulièrement** |
| Votre matériel informatique fixe et portable est-il équipé de logiciels de sécurité (antivirus, firewall, etc.) ? | Non<br>Matériel portable<br>**Matériel fixe et portable** |
| Les logiciels détenus par l'entreprise sont-ils mis à jour ? | Non<br>Occasionnellement<br>**Régulièrement** |
| Avez-vous mis en place une charte d'utilisation du système d'information et de communication, et/ou une clause de reconnaissance de responsabilité, pour l'usage d'internet et d'intranet, des matériels informatiques et des logiciels de l'entreprise, signée par chaque salarié ? | Non<br>peu<br>**En fonction du poste occupé** |

| | |
|---|---|
| Avez-vous une réglementation pour l'installation de tout nouveau matériel ou logiciel sur les ordinateurs fixes et mobiles de l'entreprise ? | Non<br>peu<br>**Systématiquement** |
| Avez-vous mis en œuvre une procédure d'authentification (identification par login et mot de passe) du personnel pour accéder au système d'information ? | Non<br>Rarement<br>**Systématiquement** |
| Les mots de passe utilisés pour accéder au matériel informatique de l'entreprise sont-ils une combinaison de chiffres ou bien de lettres et de caractères spéciaux ? | Non<br>Entre 1 et 4 caractères<br>**Entre 4 et 7 caractères** |

TABLE 2.3 – Questionnaire sur l'analyse de l'existant [5].

## Risques liés au système d'information

Il existe de nombreux risques en sécurité du système d'information, qui évoluent d'année en année, Selon notre cas d'étude le service Mangement de General emballage ont identifier trois catégories de risques : la Défaillance dans serveur, le Piratage d'information et la Contamination des travailleurs par le COVID-19 ainsi ils ont spécifier leurs probabilité, gravité ainsi l'action face aux risque critiques et d'autre facteurs secondaire.

| N° | Nature du risque | La conséquence | Probabilité | Gravité | Critique | Action face aux risques critiques | Responsable de l'action | Échéance |
|---|---|---|---|---|---|---|---|---|
| **Processus système d'information (informatique)** | | | | | | | | |
| 1 | Défaillance dans serveur | - Perte des données importantes pour l'entreprise | 1 | 10 | 10 | Maintenance régulière de serveur | Directeur Système d'informations | En continu |
| 2 | Piratage d'information | - Perte de donnée,<br>- Confidentialité | 1 | 10 | 10 | Licence des logiciels utilisés (alerte pare-feu) | Directeur Système d'informations | Chaque expiration de validité |
| 3 | Contamination des travailleurs par le COVID-19 | - Propagation du virus<br>- Manque d'effectif | 3 | 5 | 15 | - Mise en place des moyens de lutte contre le virus<br>- Polyvalence | Directeur commercial | En continu |

FIGURE 2.4 – Risques liés au système d'information de GE.

### 2.3.5 Problématique

Après avoir étudier le réseau de l'entreprise Général Emballage en prenant en considération les exigences auxquelles doit répondre un réseau performant et sécurisé qui est vraiment important car les effets sont de plus en plus lourds et les systèmes d'information sont de plus en plus connectés et externalisés. Cependant malgré la présence d'un système de sécurité, d'énormes difficultés et des vulnérabilités existent entre autre on a :

— Gestion des utilisateurs et des ressources.

— Reprise sur panne.

— Contrôle d'accès (IAAA).

— Contrôle et analyse du trafic réseau.

— Centralisation du processus métier.

— L'accès distant entre les sites.

— Normalisation de processus informatique.

### 2.3.6 Objectifs

Notre projet a pour but la mise en oeuvre et la configuration d'un pare-feu, la replication de l'annuaire Active Directory ainsi la mise en place d'un ERP Odoo. Cette solution permettra de pallier les différents problèmes cités auparavant et afin d'atteindre les différents objectifs suivants :

— Gestion des utilisateurs et des ressources par la mise en place de l'annuaire Active Directory.

— Reprise sur panne Mise en place d'un pare-feu redondant.

— Contrôle et analyse du trafic réseau par la Configuration du système de filtrage Web et applicatif.

— Contrôle d'accès (IAAA) par la mise en place d'une listes de contrôle d'accès (ACL).

— Normalisation de processus informatique par la mise en place d'un ERP Odoo.

— L'accès distant entre les sites par la mise en place d'une architecture VPN IPsec.

— Centralisation du processus métier par Mettre en place d'un CRM.

## 2.4 Conclusion

Le premier point de ce chapitre est porté sur la présentation de la société "General Emballage", son historique depuis sa création, l'evolution de ses Effectifs, ses valeurs ainsi son plans réseau. Ensuite, en deuxième position vient l'état des lieux, à partir de là nous avons présenter l'infrastructure réseau de l'entreprise, ses normes ISO, l'étude de son réseau puis les risques liés au système d'information .

Et tout cela pour entamer le chapitre intitulé : "Études des solutions proposées" aura pour contenu des captures d'écrans qui schématisent toutes les installations et les configurations du pare-feu FortiGate et les machines virtuelles que nous avons utilisé ainsi que les solutions que nous avons proposés pour y remédier.

# Chapitre 3

# Études des solutions proposées

## 3.1 Introduction

Dans ce chapitre, nous allons mettre en oeuvre l'architecture réseau de l'entreprise basée sur le firewall Fortigate en utilisant le simulateur réseau GNS3 (Graphical Network Simulator) et l'hyperviseur VMware Workstation.

Pour cela nous utiliseront l'IOS réel de ce pare-feu afin de virtualiser et réaliser un système de haute disponibilité et resistant aux pannes. L'objectif est de sortir avec des connaissance suffisantes pour simuler des scénarios qu'on peut rencontrer dans la pratique et évaluer leurs faisabilités.

## 3.2 Présentation de notre infrastructure réseau

Dans notre projet nous allons emmener a faire la virtualisation de la couche infrastructure et applications d'un système d'information cas d'étude Général emballage.

Notre infrastructure se compose de deux sites qui se situe à Akbou et à Oran ; le site d'Akbou est constitué de trois couches qui sont la couche cœur, la couche distribution et la couche d'accès qui représente respectivement les deux fortiGate (maitre et esclave), le switch Core et les switches d'accès.

L'architecture du réseau que nous avons créé est illustrer dans la topologie suivante :

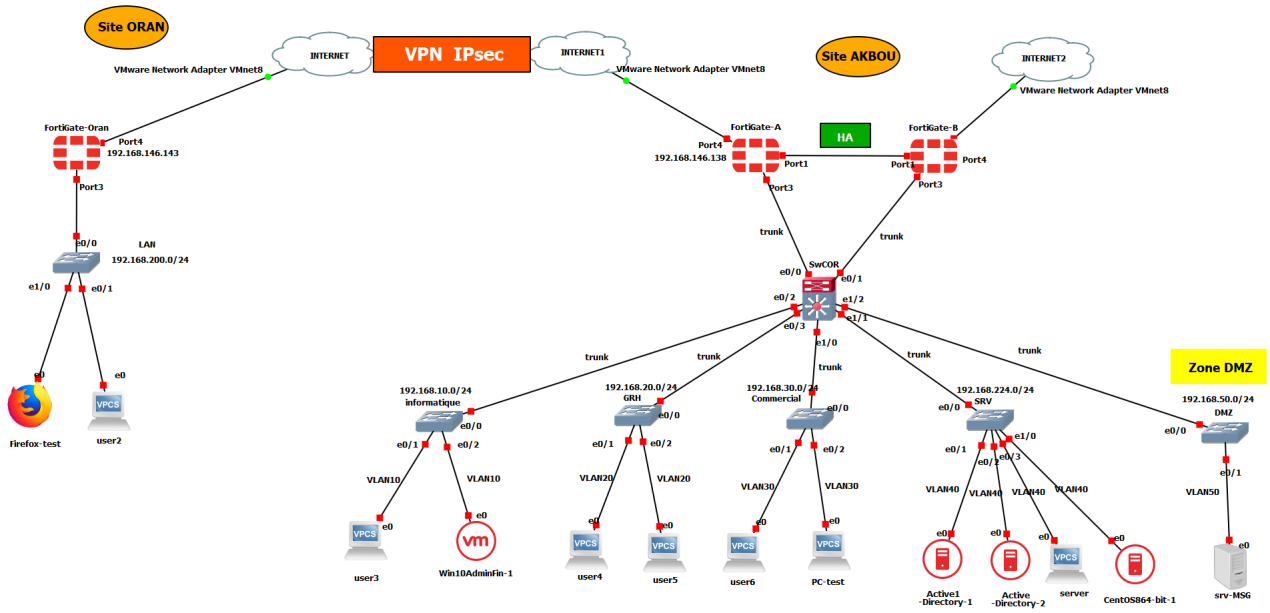


FIGURE 3.1 – Maquette du réseau sous GNS3.

Dans cette topologie, vous remarquez la présence de deux firewall Fortigate au niveau de notre site principal d'Akbou, ceci dans le but d'assurer la haute disponibilité de notre pare-feu. Concernant l'autre firewall se trouvant au niveau du site distant (Oran), nous l'avons mis en place afin de simuler un tunnel VPN .

Afin d'accéder à l'interface graphique de nos différents pare-feu nous avons mis en place une machine virtuelle sous windows 10 et un navigateur Firefox .

Dans le site principal, nous avons crées un domaine nommer "generalemballage.local", pour assurer la sécurité,la redondance et la mise à jour des objets de nos données, nous avons effectuer la replication de l'active directory. Ainsi nous avons installer CentOS 8 et configurer un ERP Odoo13 sur ce dernier.

## 3.3 Pare-feu FortiGate de Fortinet

### 3.3.1 Importation de FortiGate sur gns3

a) Tout d'abord, nous entrons dans GNS3 et nous allons créer un nouveau projet, on accède au nœud "Dispositifs" de sécurité et cliquer sur "New Template".

b) Une fois que nous avons commencé le processus d'importation de l'appliance, nous pouvons simplement continuer jusqu'à ce que nous atteignions la fenêtre où nous devons cliquer sur

"Create a new Version" pour creer une nouvelle version (6.4.0) puis spécifier les fichiers qui seront utilisés pour installer l'image logicielle.

c) Maintenant que nous en sommes à la partie des fichiers requis du processus d'importation, nous devons d'abord décider quelle version du pare-feu nous souhaitons importer. Pour notre cartographie réseau, nous téléchargerons la version 6.4.0.

d) En cliquant sur la flèche déroulante nous montrera quels fichiers sont manquants, ces fichiers seront téléchargés à partir du site de support FortiNet [4], par la suite on passe à l'étape de l'importation (voir figure 3.2).

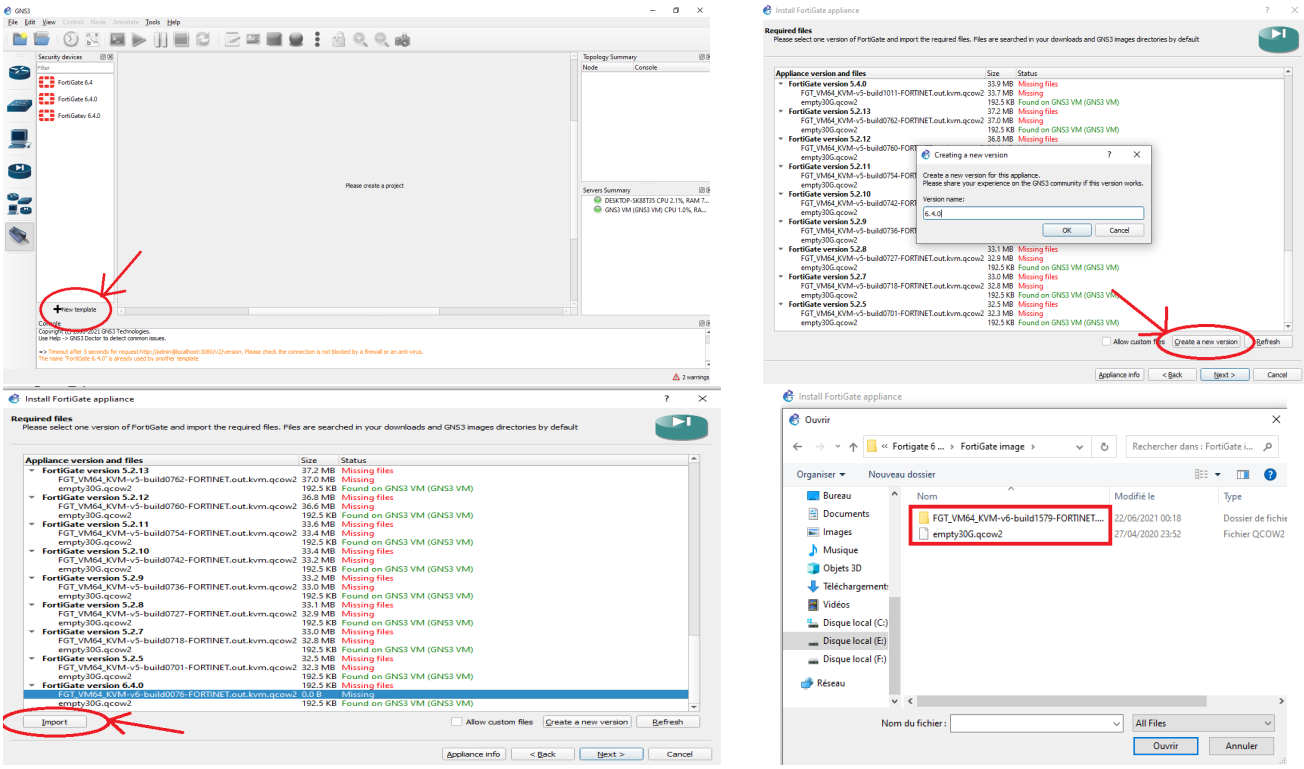


FIGURE 3.2 – Importation d'appliance Fortigate 6.4.0 sur GNS3.

e) Les prochaines cases, nous appuyons simplement sur suivant jusqu'à ce que nous arrivions à l'espace où nous terminerons l'importation et nous aurons qu'à nommer notre appareil. Nous avons maintenant importé avec succès une appliance virtuelle FortiGate.

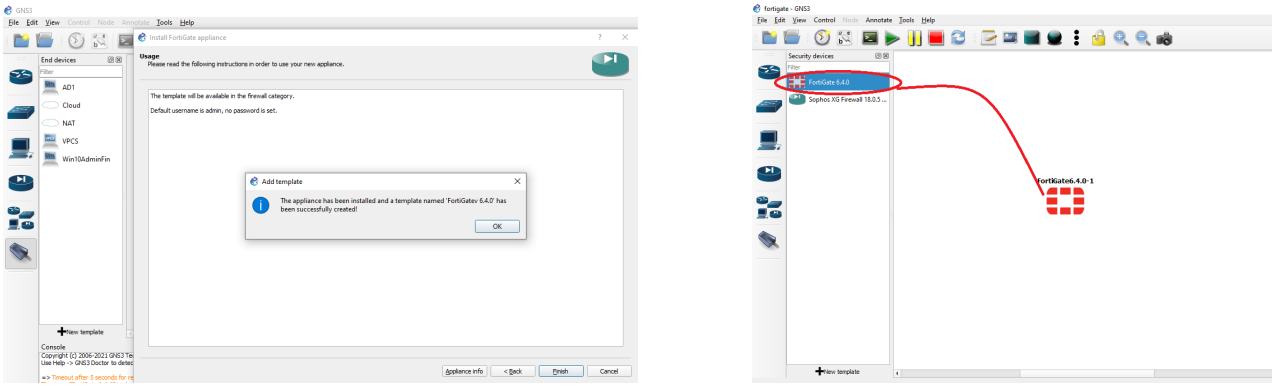

FIGURE 3.3 – Importation d'appliance Fortigate 6.4.0 avec succès .

### 3.3.2 Configuration d'accès au FortiGate

Une fois que nous avons importé avec succès notre pare-feu FortiGate virtuel dans GNS3 on va faire glisser un périphérique cloud depuis le nœud des périphériques finaux, nous devrions maintenant configurer notre cloud et lui ajouter l'interface VMnet8, ensuite faire passer un câble de notre adaptateur VMnet8 du cloud au fortiGate sur le port1 (voir Figure 3.4).

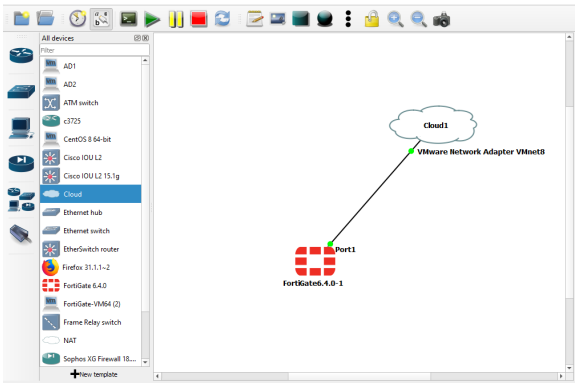


FIGURE 3.4 – Ajout et configuration du cloud.

ll nous reste plus qu'à configurer notre Pare-feu FortiGate,donc nous allons dans la configuration de l'interface en tapant "config system interface" puis allez dans l'interface que nous voulons changer qui est le port1 en tapant "edit port1". Maintenant, il nous suffit de donner une adresse IP à l'interface en tapant "set ip 192.168.146.138/24" et en définissant également l'accès autorisé qui ouvre essentiellement les ports de gestion sur l'interface, nous allons ouvrir la plupart d'entre eux en tapant "set allowaccess ping http https ssh" afin que nous puissions accéder au pare-feu sur tous ces ports. Pour enregistrer les modifications, tapez simplement « next » suivi de « end » (voir Figure 3.5).


FIGURE 3.5 – Configuarations d'appliance Fortigate 6.4.0.

Nous allons dans l'invite de commande sur notre ordinateur local et on va essayer de pinguer l'adresse 192.168.146.138, On remarque qu'on obtient une réponse car nous avons défini le ping dans la configuration d'accès autorisé sur le port1.

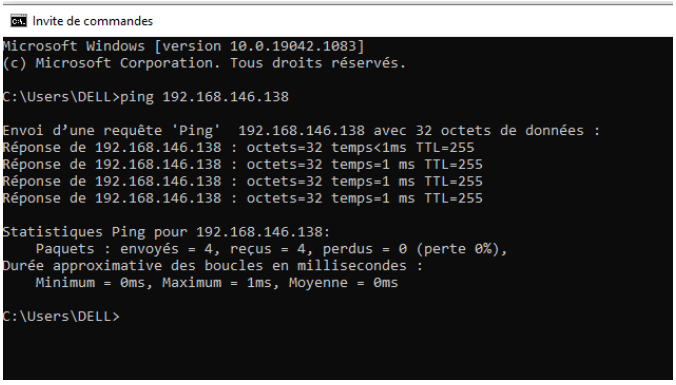


FIGURE 3.6 – Ping PC local vers FortiGate réussi .

Le ping réussi vers FortiGate implique que nous pouvons y accéder via l'interface graphique. Grâce au navigateur (Google Chrome) on tape "192.168.146.138" ou l'adresse IP que nous utilisons pour la gestion. Nous remarquons que le navigateur charge maintenant la page de connexion pour le FortiGate, On se connecte avec admin et un mot de passe (Voir Figure 3.7 ). Une fois connecté, on sera placé dans le tableau de bord (Voir Figure 3.8).

NB : Juste un rappel que l'OS fonctionnera sur une licence d'essai de 15 jours sur cette instance de l'Appliance.

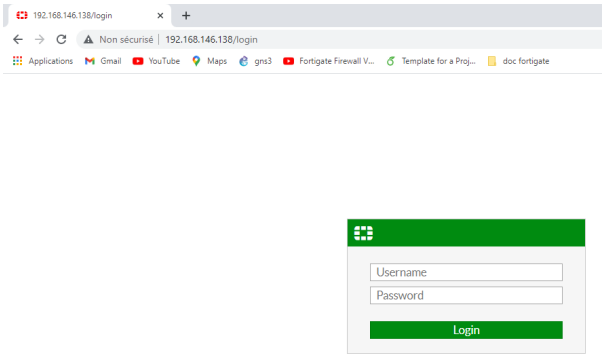


FIGURE 3.7 – Interface d'authentification .

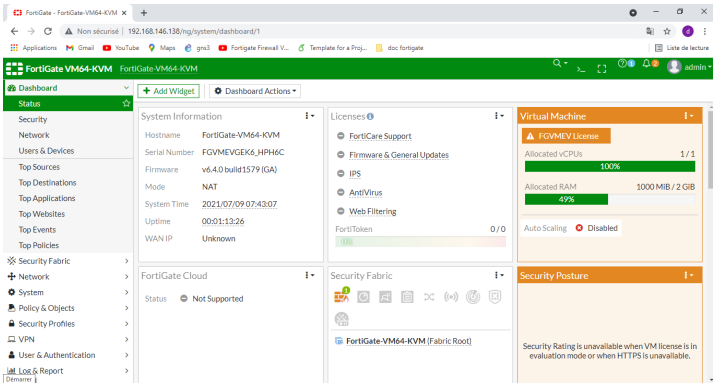


FIGURE 3.8 – Tableau de bord fortiGate .

### 3.3.3 Configuration des VLANs

a) Nous allons nous connecter au pare-feu via le Web avec l'adresse ip 192.168.146.138,puis on va accéder à [System Management] -> [Network] -> [Interfaces], on clique sur [Create New], voir ( Figure 3.9).

b) Nous allons Afficher la fenêtre de création d'interface, et remplir les informations suivante :

**Nom de l'interface :** Nous pouvons le nommer arbitrairement, mais le but est d'identifier de manière unique l'interface ; pour notre cas nous avons choisis de le nommer "INFO".

**Types :** Ici, le type d'interface doit sélectionner l'interface VLAN.

**Interface :** Nous avons sélectionner le port physique 3 pour configurer la sous-interface VLAN dans la liste déroulante.

**ID VLAN :** L'ID doit correspondre à l'ID VLAN configuré dans le commutateur, pour notre exemple VLAN ID=10.

**Adresse IP/masque de sous-réseau :**Nous avons attribuer une adresse IP 192.168.10.1/255.255.255.0 à notre interface.

**Accès de gestion :** Nous avons coché certains protocoles (PING,HTTPS,SSH,FTM,FMG-Access) pour activer le type d'accès.

**Serveur DHCP :** Nous avons Activé le Protocole DHCP sur un intervalle d'adresse 192.168.10.1 192.168.10.254 .

c) Une fois que nous avons terminer la saisie, on clique sur "OK" pour terminer la configuration.

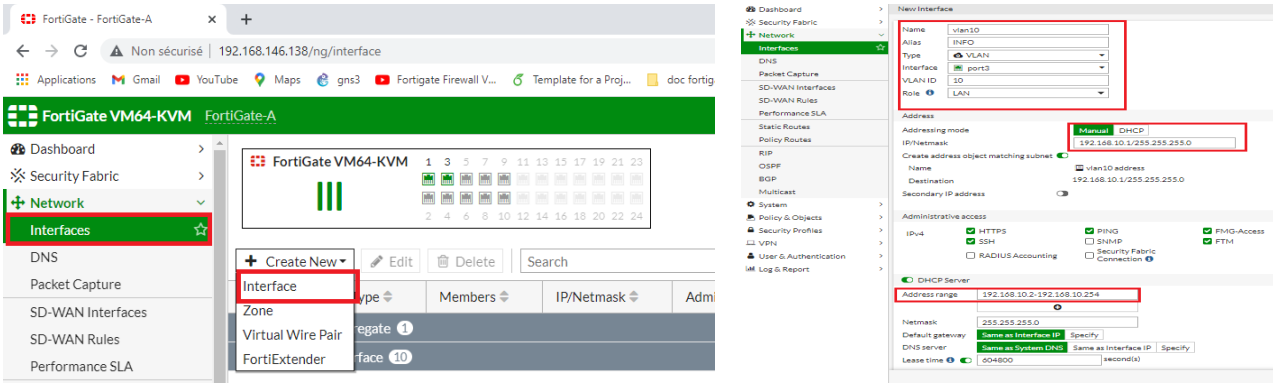


FIGURE 3.9 – Création et paramétrage du vlan10 .

d) Nous allons répéter les étapes ci-dessus pour configurer les autres interfaces VLANs, une fois que nous avons terminer la configuration, on aura cette interface, (voir Figure 3.10).

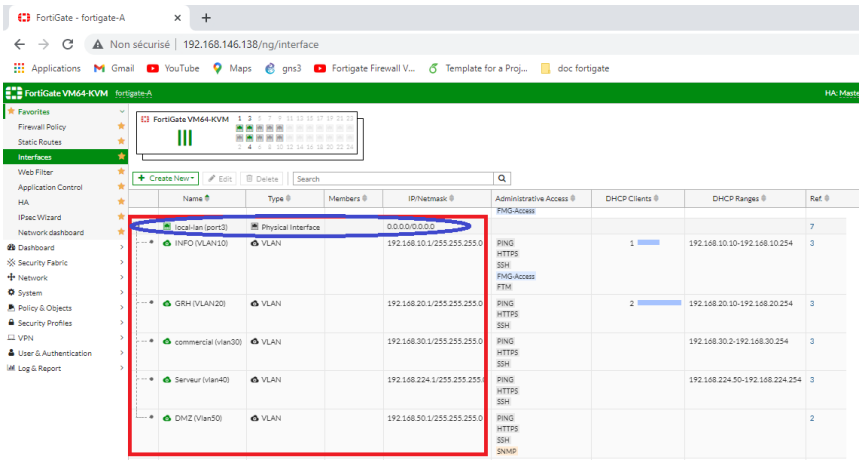


FIGURE 3.10 – Les interfaces VLANs configuées sur le port 3.

**Remarques :**

- l'interface physique 3 sur laquelle nos VLANs sont connectés ne nécessite aucun paramètre d'adresse IP (voir la partie entourée en bleu sur la Figure 3.10).
- une fois une interface VLAN créée, cette interface est soumise aux mêmes règles que les interfaces physiques. Des stratégies de pare-feu doivent être définies pour autoriser/refuser le trafic vers/depuis cette interface, et d'autres objets communs comme l'adresse de pare-feu peuvent lui être assignés.

e) <u>Creation d'une zone</u>

Pour faciliter la gestion et la maintenance des politiques à l'avenir, nous pouvons configurer l'interface VLAN en fonction de la zone.

Dans [Network] -> [Zone], nous cliquons sur "Create New", l'interface de création de zone apparaît ( voir figure 3.11).

Puis nous allons Configuré le nom ; pour notre cas c'est "inter-vlan" et enfin nous ajoutons les membres de l' interface (vlan 10,20,30 et 40) (voir figure ci-dessous).

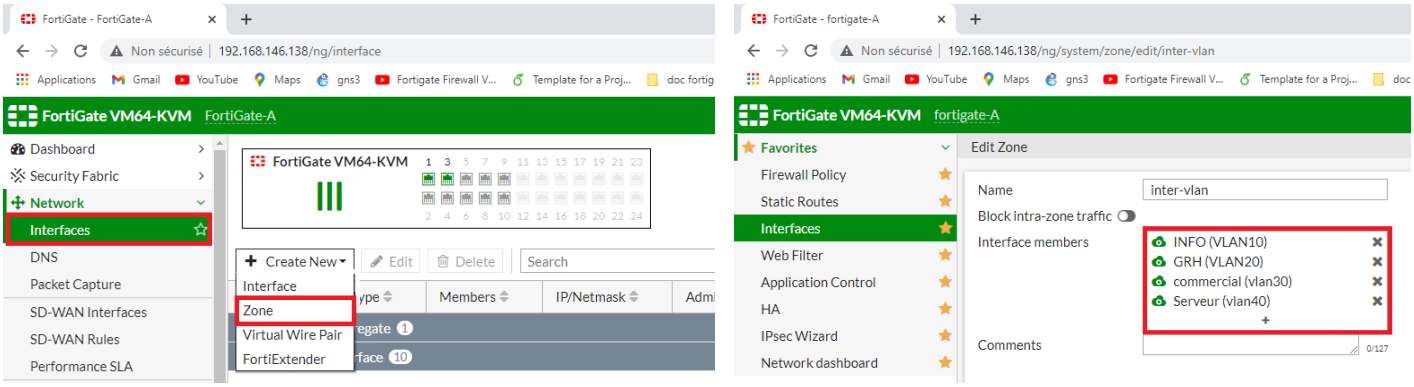


FIGURE 3.11 – Creation d'une nouvelle zone et l'ajout des VLANs.

### 3.3.4 Configuration d'une liste de contrôle d'accès

Une liste de contrôle d'accès (ACL) est une liste de blocage/accès ciblée et granulaire qui est utilisée pour bloquer/autoriser les paquets IPv4 et IPv6 sur une interface spécifiée en fonction des critères configurés dans la stratégie ACL.

Afin de configurer l'accès de la zone "inter-vlan" vers "Internet" ; nous allons Accéder à [Policy and Objects1] > [Firewall Policy] , par la suite nous allons cliquer sur "Create New" et définir les paramètres des champs (voir Figure 3.12) .

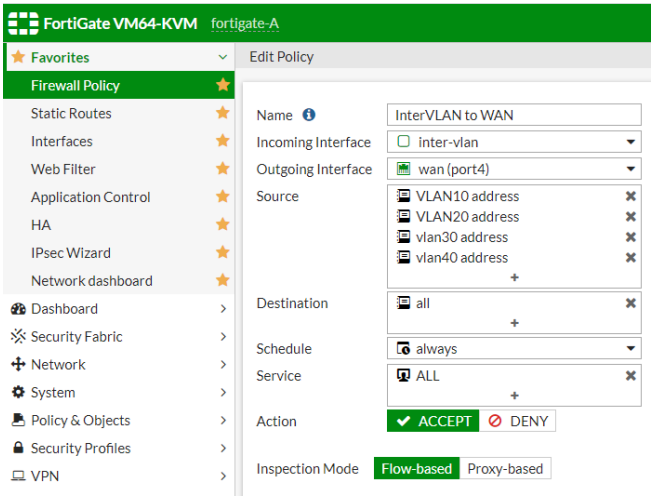


FIGURE 3.12 – Configuration d'accès de la zone "inter-vlan" vers "Internet".

En suivant les mêmes étapes nous allons créer les autres règles du pare-feu (voir Figure 3.13) .

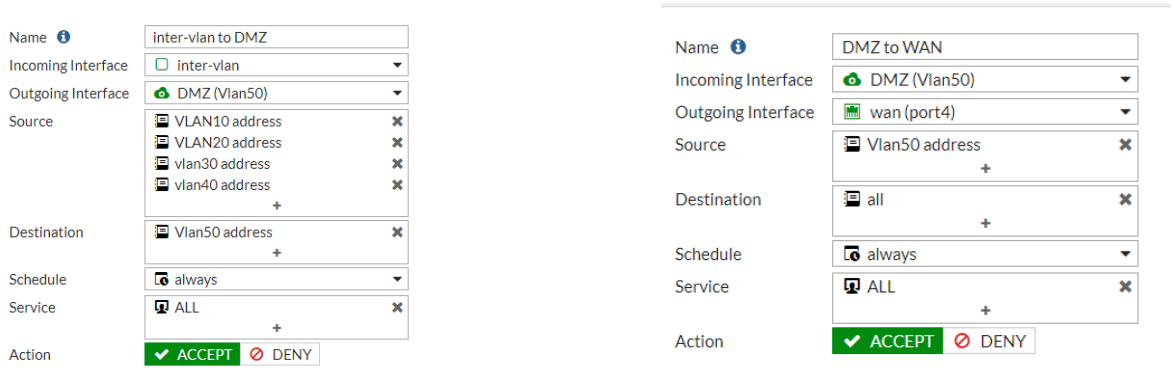


FIGURE 3.13 – Exemple des autres ACLs crées .

**Remarque :** Cette licence de fortigate 6.4.0 limite le nombre d'ACLs (Access Control Lists) à 5. cette erreur s'affiche dés que nous créons une 6-ème ACL : "Échec de l'enregistrement de certaines modifications : le nombre maximum d'entrées a été atteint".

### 3.3.4.1 Filtrage web

Précédemment tout les utilisateurs ont accès a internet sans rien bloquer, pour cela nous allons utiliser le filtrage web pour surveiller et contrôler l'accès au WAN.

a) Nous allons dans [Security Profiles] -> [Web Filter] et cliquons sur "Create New" par la suite mettre le nom de la règle de blocage (Block-Facebook) ,dans l'exemple suivant nous avons choisis de bloquer l'accès au "facebook".

b) Dans la partie "Static URL Filter" nous allons créer un nouveau Filtre d'URL, nous choisissons comme type "Wildcard" ie mettre le mot que nous souhaitons bloquer si l'utilisateur le tape dans la barre d'adresse (voir Figure 3.14).

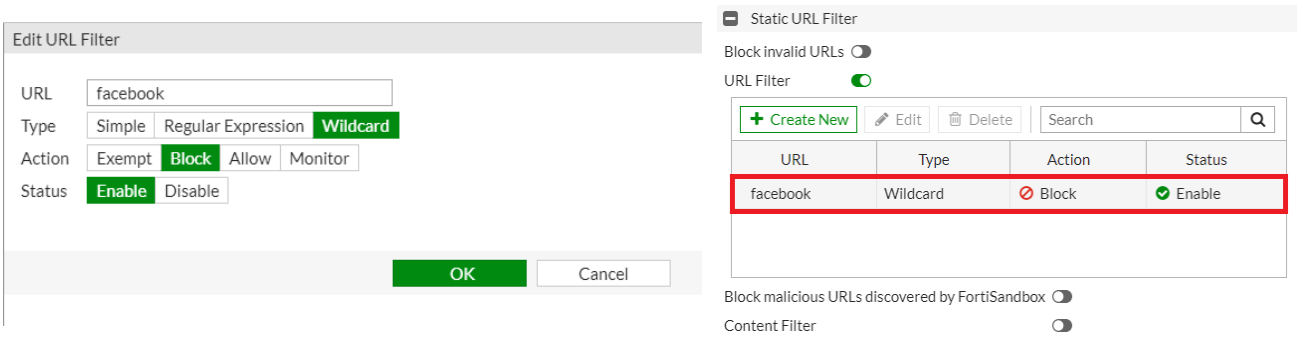


FIGURE 3.14 – Création d'un nouveau filtre URL "Facebook" .

c) Dans cette étape nous allons prendre une ACL parmi les ACLs crées auparavant, puis activer le "web filtre" dans la partie "Security Profiles " en choisissant le filtre web crée.

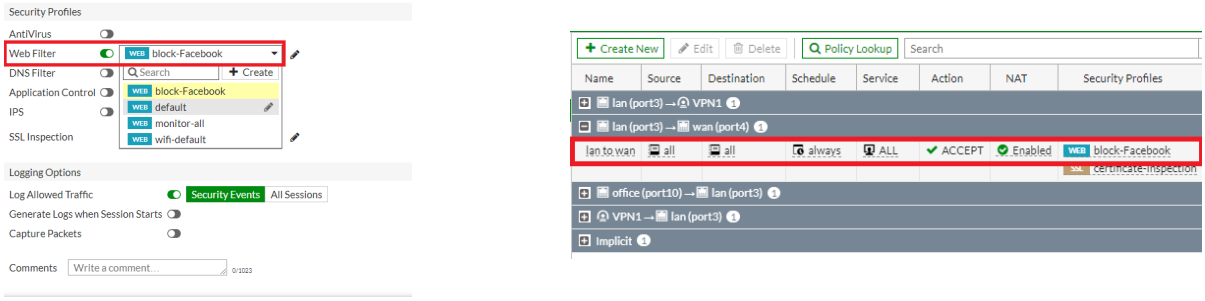


FIGURE 3.15 – Application du filter web sur ACL .

Nous allons suivre les même étapes pour bloquer les autres URL (Google,wikipedia,...).

### 3.3.4.2 Filtrage applicatif

Dans le Filtrage Applicatif nous allons bloquer l'accès à certaines applications (Nous prendrons Gmail comme exemple ) .

a) Nous allons dans [Security Profiles] -> [Application Control] et cliquons sur "Create New" par la suite mettons le nom de la règle de blocage (Block-app-gmail).

b) Dans la partie "Application and Filter Overrides" nous allons créer une nouvelle dérogation, nous choisissons comme type "Application" et selectionnons Gmail puis "OK" (voir Figure 3.16).

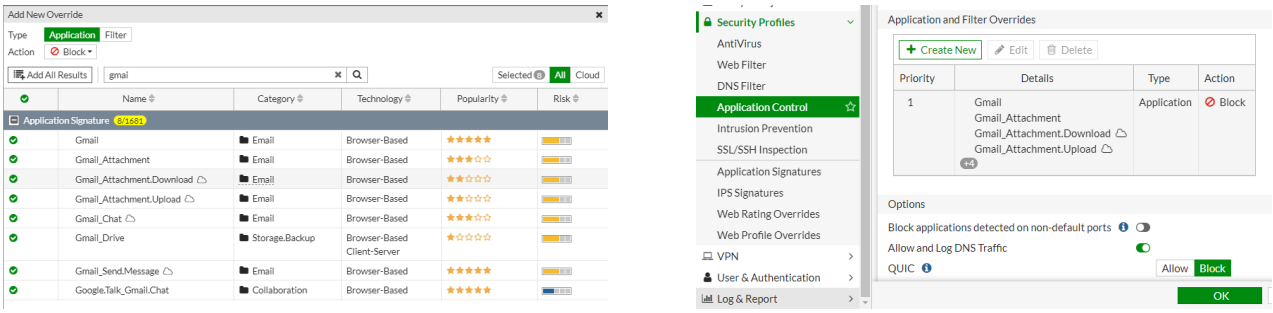


FIGURE 3.16 – Création d'une règle de contrôle d'application "Gmail".

c) Dans cette étape nous allons prendre une ACL parmi les ACLs crées auparavant, puis activer le "Application Control" dans la partie "Security Profiles" en choisissant le controle d'application crée .

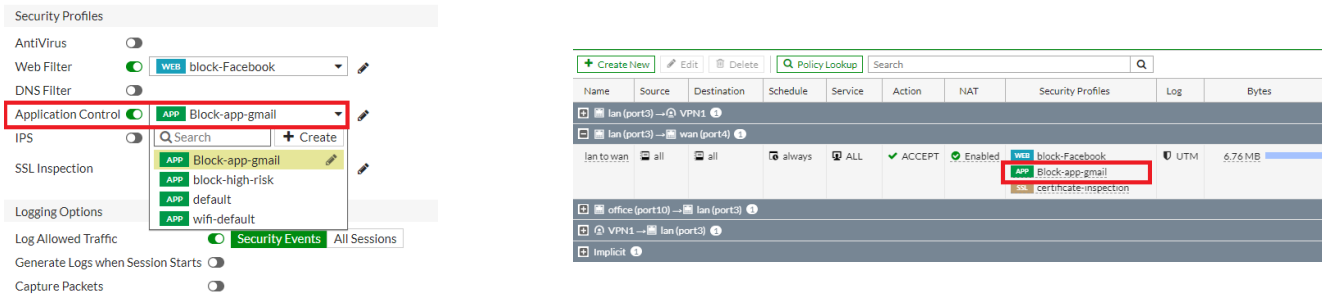


FIGURE 3.17 – Application de la règle de contrôle d'application.

Nous allons suivre les même étapes pour bloquer les autres Applications (Viber, whatsapp, yahoo,...).

### 3.3.5 Configuration du VPN IPsec

Dans cette partie nous allons creer deux VPN IPsec sur notre FortiGate qui sont : le VPN1 (Oran vers Akbou) et le VPN2 (Akbou vers Oran) ; On note que les adresses IP des sites Akbou et Oran sont respectivemet 192.168.146.138 et 192.168.146.143.

#### 3.3.5.1 Configuration VPN1 (Oran vers Akbou)

a) Afin de créer un tunnel VPN IPsec sur le pare-feu FortiGate, On selectionne [VPN] -> [IPSec Wizard] et saisir le nom du tunnel (VPN1), type de modèle c'est "site à site" et celui de périphérique distant est un pare-feu FortiGate ensuite nous allons sélectionner NAT Configuration comme" No NAT between sites".

b) Dans l'étape Authentification, on va définir l'adresse IP WAN du FortiGate Akbou distant (192.168.146.138).

Une fois l'adresse IP WAN saisie, l'assistant attribue automatiquement une interface en tant qu'interface sortante. Par la suite nous définissons une clé pré-partagée sécurisée (PSK),le site Akbou distant peut également être authentifié via un certificat .

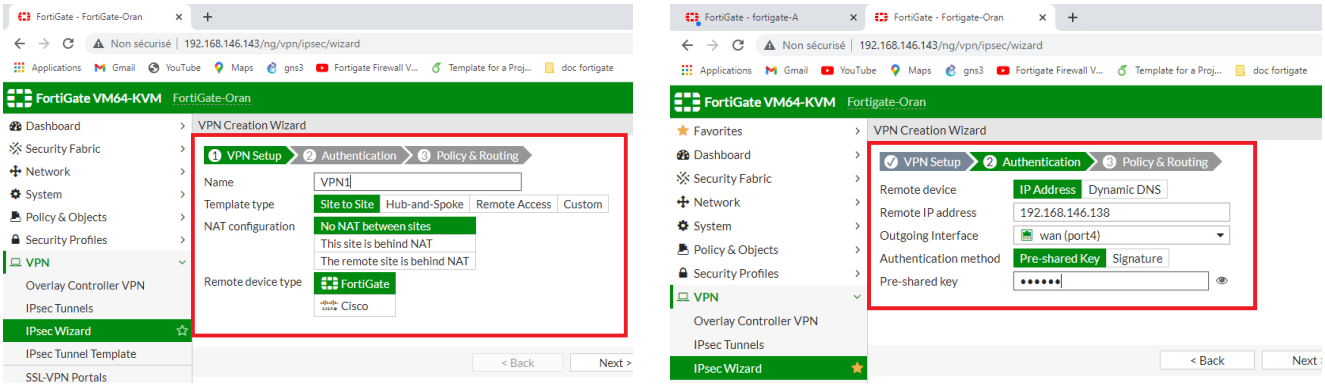


FIGURE 3.18 – Creation et Authentification du tunnel VPN1 IPsec .

c) Dans l'étape Policy and Routing, nous allons définir l'interface locale sur LAN, l'assistant ajoute automatiquement le sous-réseau local. Par la suite Nous allons définir la zone crée précédemment (inter-Vlan).

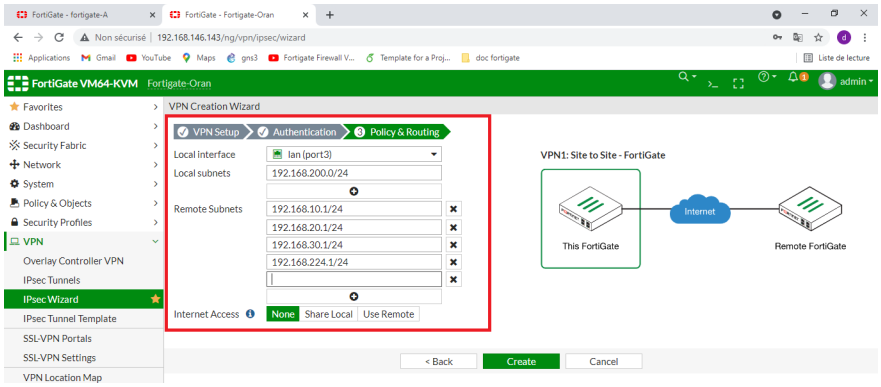


FIGURE 3.19 – Policy and Routing VPN1 IPsec.

d) Une page récapitulative affiche la configuration créée par l'assistant, y compris les interfaces, les adresses de pare-feu, les routes et les politiques.

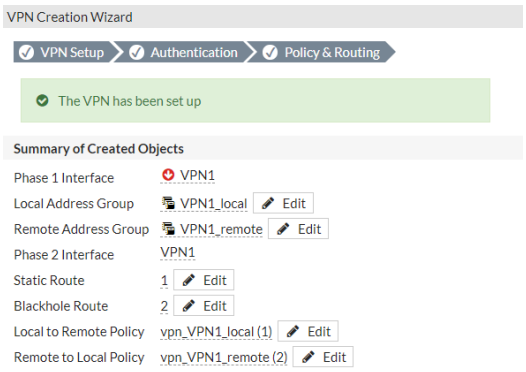


FIGURE 3.20 – Configuration créée par VPN1.

e) Pour afficher l'interface VPN créée par l'assistant, nous allons accéder à [Network] -> [Interfaces]

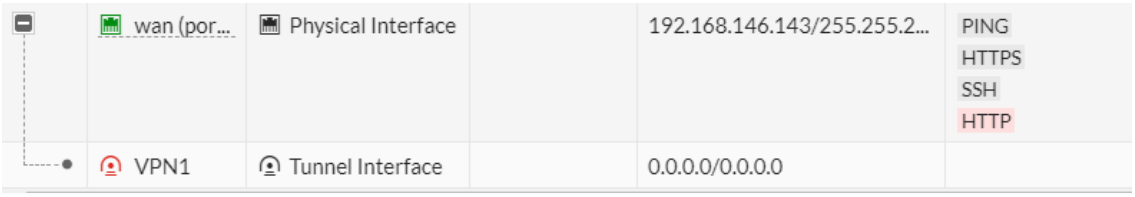


FIGURE 3.21 – L'interface VPN1 créée.

f) Pour afficher les adresses de pare-feu créées par l'assistant, nous allons accéder à [Policy Objects] -> [Addresses].

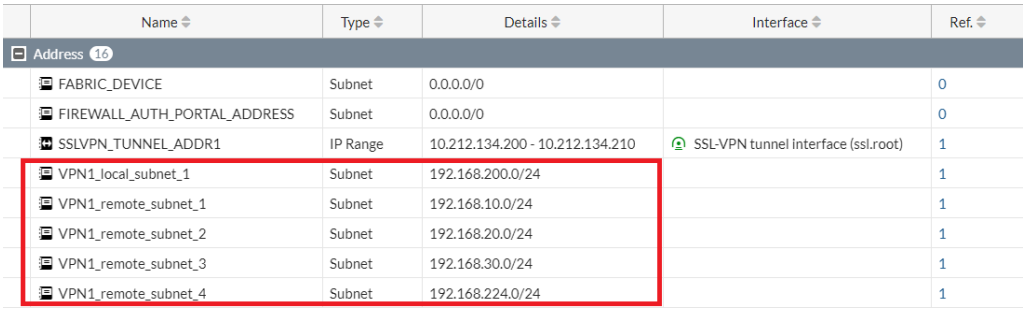


FIGURE 3.22 – Adresses créées par VPN1.

g) Pour afficher les routes créées par l'assistant, nous allons accéder à [Network] -> [Static Routes].

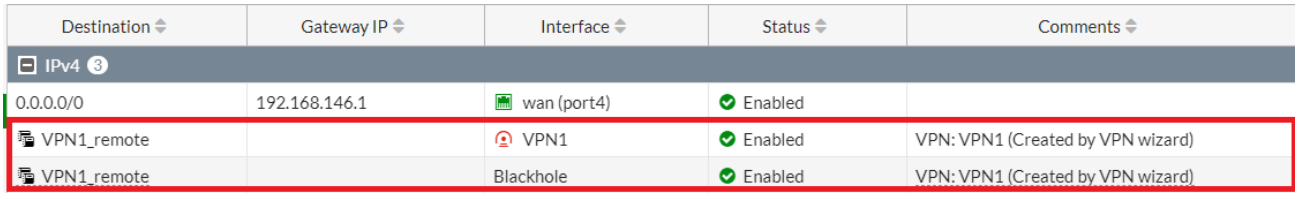


FIGURE 3.23 – Routes créées par VPN1.

h) Pour afficher les stratégies créées par l'assistant, nous allons accéder à [Policy and Objects] -> [IPv4 Policy].

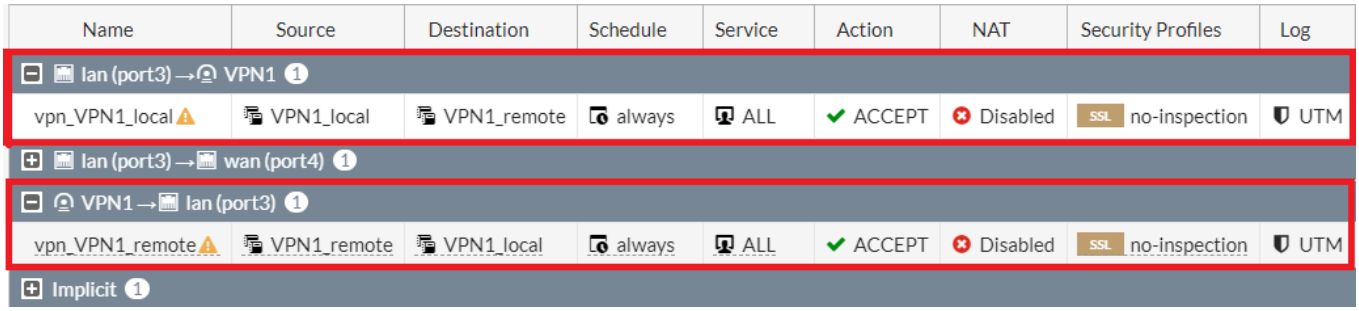


FIGURE 3.24 – ACLs créées par VPN1.

### 3.3.5.2 Configuration VPN2 (Akbou vers Oran)

Concernant la configuration du VPN2, nous avons suivis les mêmes étapes que la configuration du VPN1 (voir Figure 3.25).

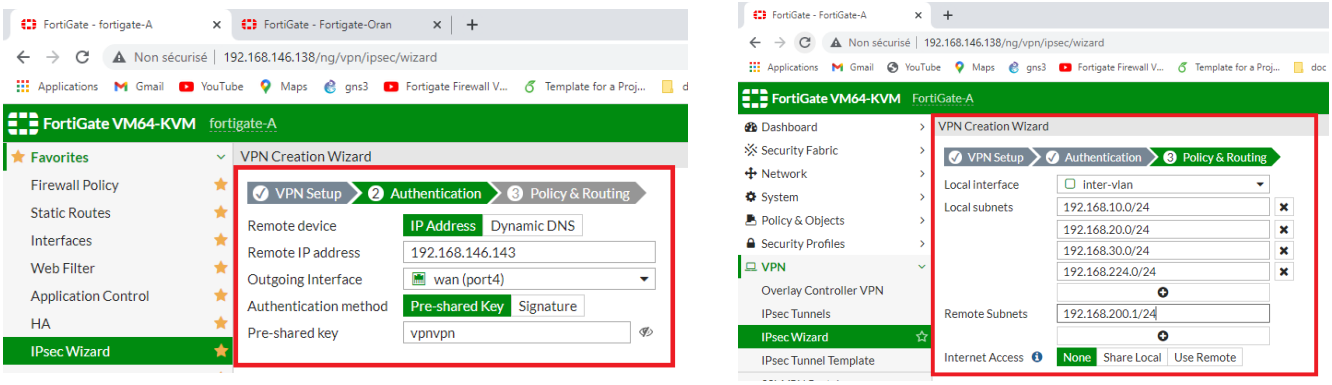


FIGURE 3.25 – Configuration d'Authentification et " Policy and Routing" VPN2 IPsec.

Pour Activer le tunnel VPN, nous avons accédé à [Dashboard] -> [Network] -> [IPsec Monitor] de VPN1 et celui de VPN2. puis on selectionne « Statut » et on clique sur "bring up" .

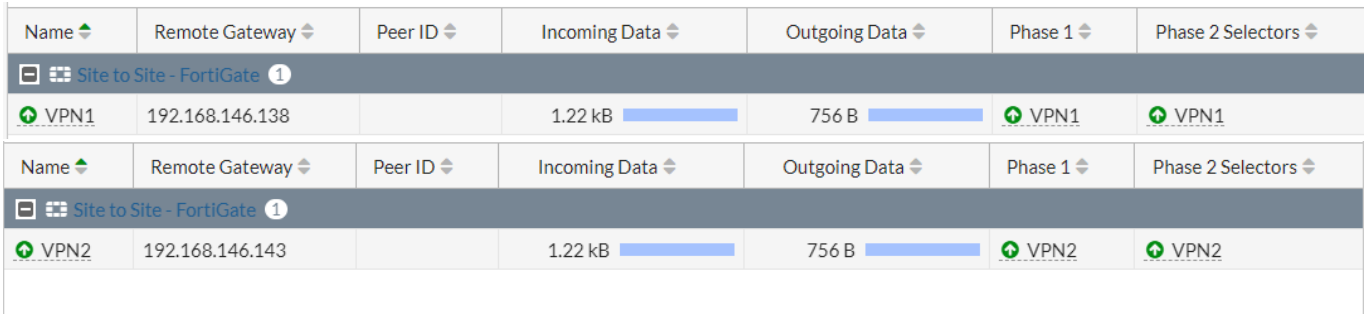


FIGURE 3.26 – Activation du tunnel VPN sur les deux site.

### 3.3.6 Configuration de la haute disponibilité

Nous allons configurer la haute disponibilité (en anglais High Availability (HA)) active-passive sur les deux pare-feu FortiGate."fortigate-A" agira en tant que maître et "fortigate-B" en tant qu'esclave. En cas d'erreur du maître l'esclave fonctionnera jusqu'à ce que le maître soit traité.

Nous allons dans [Système] -> [HA] ,puis nous allons remplir les champs suivant (voir Figure 3.27) :

— En Mode : Nous avons choisi Actif-Passif .

— Priorité du pare-feu :Nous avons défini la priorité la plus élevé sur le maitre(fortigate-A) ,pare-feu avec une priorité inférieure sera l' esclave (fortigate-B).

— Nom du groupe : Nous avons entré le nom du groupe "HA-group" sur les deux fortigates.

— Mot de passe : Nous avons défini le mot de passe pour authentifier les membres du "HA-group".

— Interfaces Heartbeat : nous avons sélectionné le port réseau pour lequel nous souhaitons configurer le HA afin que les deux fortigates se synchronisent entre eux (ici nous choisissons le port 1).

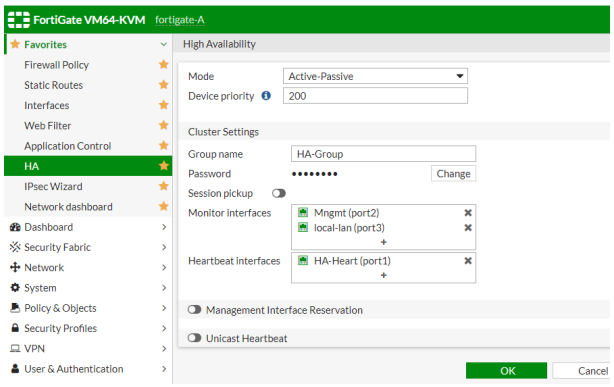


FIGURE 3.27 – Configuration HA "fortigate-A".

Nous effectuons une Configuration similaire pour le pare-feu esclave (fortigate-B), avec des paramètres de priorité inférieurs a celles du maître (voir Figure 3.28).

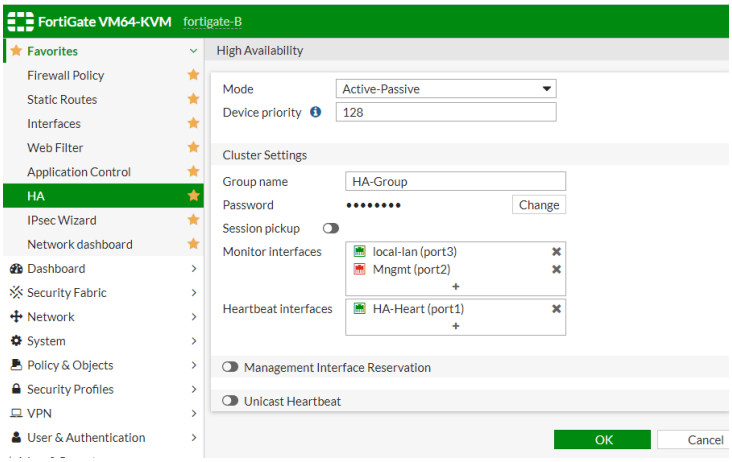


FIGURE 3.28 – Configuration HA "fortigate-B".

Ci-dessous le résultat du HA configuré sur les deux Fortigate .

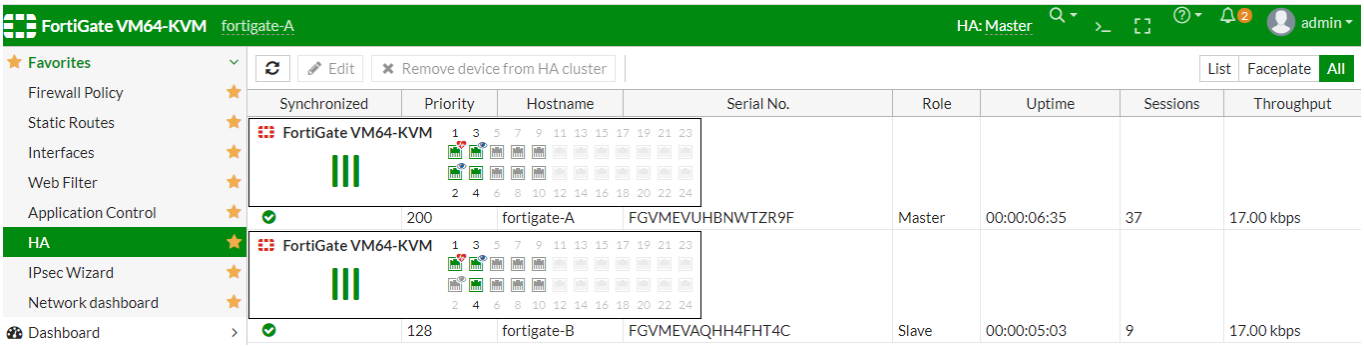


FIGURE 3.29 – Configuration HA effectuée avec succès.

## 3.4 Configuration du switch L2 IOU sous GNS3

a) **Attribution des noms aux périphériques**

Avant toute configuration nous allons attribuer un nom aux switchs, en tapant la commande ci-dessous.

```
IOU1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#hostname SW-CORE
SW-CORE(config)#
```

b) **Sécuriser l'accès aux équipements et au mode privilégié**

L'accès à la console et au mode privilégié sont les premiers points d'entrée des administrateurs. Voici les commandes pour restreindre l'accès via un mot de passe .

```
SW-CORE(config)#enable secret CoreGE
SW-CORE(config)#line console 0
SW-CORE(config-line)#password ConsGE
SW-CORE(config-line)#login
```

c) **Configuration des SVIs**

La configuration des SVIs s'éffectue au niveau des commutateurs de couche d'accès (informatique,GRH,Commercial,SRV et DMZ) en affectant les VLAN (10,20,30,40 et 50) aux ports Ethernets liées aux terminaux. Nous prendrons comme exemple le switch du service informatique en lui affectant le VLAN 10 au port Ethernet 0/2.

```
SW-Informatique(config)#interface e 0/2
SW-Informatique(config-if)#switchport mode access
SW-Informatique(config-if)#switchport access vlan 10
SW-Informatique(config-if)#
```

d) **Configuration des Trunks**

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

```
SW-CORE(config)#interface e 0/2
SW-CORE(config-if)#switchport trunk encapsulation dot1q
SW-CORE(config-if)#switchport mode trunk
```

## 3.5 Les machines virtuelles sur VMware Workstation 16Pro

### 3.5.1 Installation de Windows Server 2016

Pour installer Windows Server 2016, nous devons d'abord en avoir un fichier image ISO et nous assurer également d'avoir planifié le choix de l'édition de Windows Server 2016 et d'avoir rempli la configuration système requise .

a) Pour utiliser cette technique, nous allons sur l'assistant de création de machines virtuelles [File] -> [New Virtual Machine], Ensuite nous choisissons : Typical (recommended).

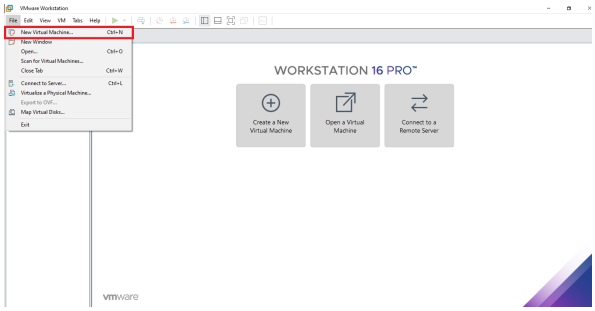


FIGURE 3.30 – Création d'une nouvelle machine virtuelle.

b) Ici, nous devons ajouter une image d'installation dans la machine virtuelle.Nous allons Sélectionner l'option Fichier image disque d'installation (ISO) et cliquer sur le bouton Parcourir, puis spécifier le chemin du fichier iso et l'importer, nous Cliquons ensuite sur le bouton "Next" .

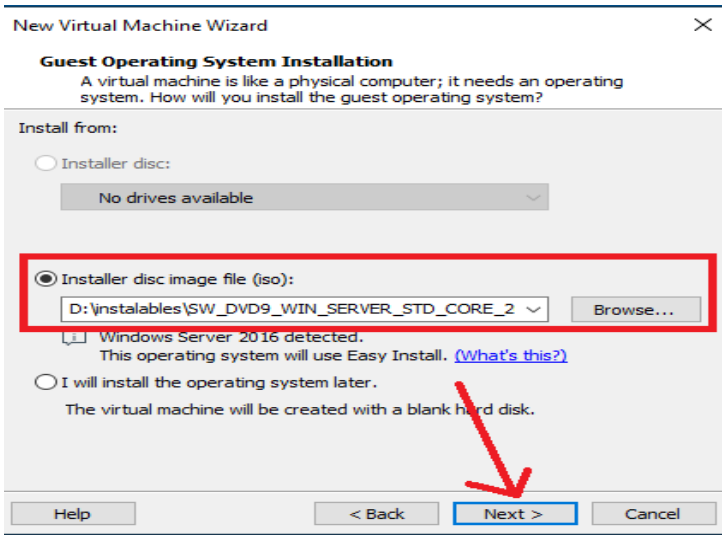


FIGURE 3.31 – Importation du fichier ISO.

c) Nous allons saisir un nom pour la machine virtuelle (AD1) et rechercher un emplacement où stocker les fichiers d'installation. Pour cela, nous allons cliquer sur le bouton Parcourir et spécifions le lieu. Une fois terminé, cliquons sur le bouton "Next" .

Puis Spécifier la quantité de disque en tapant la taille du disque (recommandé 60 Go) et cliquons sur le bouton "Next" .

d) Par la suite nous allons vérifier les paramètres que nous avons défini ou nous pouvons les personnaliser puis cliquons sur "Finish" ,la machine virtuelle démarre automatiquement.

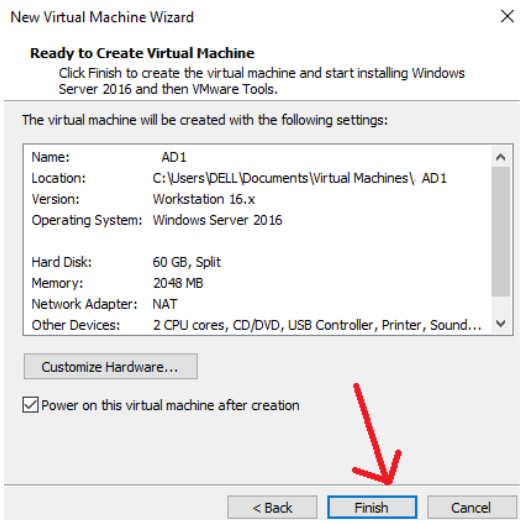


FIGURE 3.32 – Vérification des paramètres de la machine virtuelle créer.

e) Maintenant, le serveur copie tous les fichiers sur le disque, prépare les fichiers à partir de l'image Windows, installe les fonctionnalités, les mises à jour, cela prendra donc du temps et une fois terminé, il redémarrera.

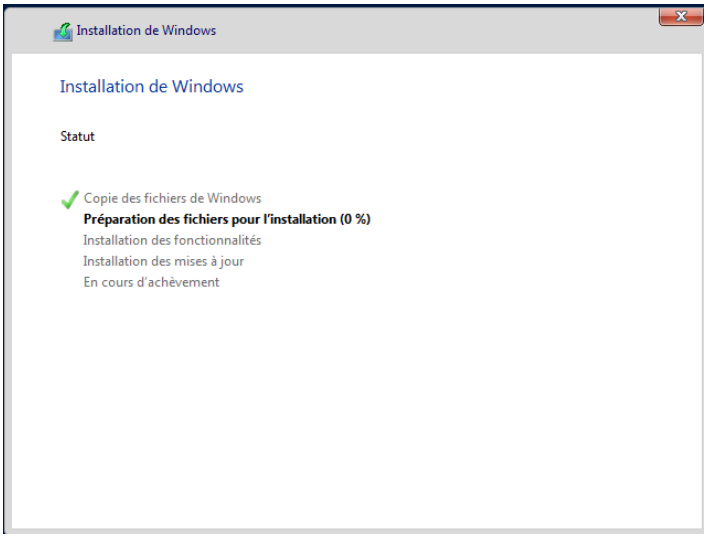


FIGURE 3.33 – Installation de Windows .

f) Après le redémarrage, nous allons taper un mot de passe complexe composé de (majuscules, minuscules, symboles et chiffres).

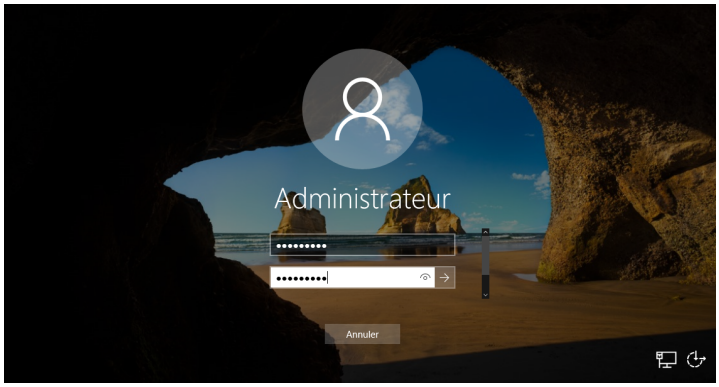


FIGURE 3.34 – Configuration du mot de passe pour la machine virtuelle .

g) Une fois que nous avons terminer la personnalisation ,nous devons maintenant nous connecter,en cliquant d'abord sur le bouton composé de ( ctrl+alt+del ) et nous connectons vers Windows Server.

Et voilà, une fois que nous sommes connectés, l'installation de notre serveur Windows est terminée comme sur la figure ci-dessous.

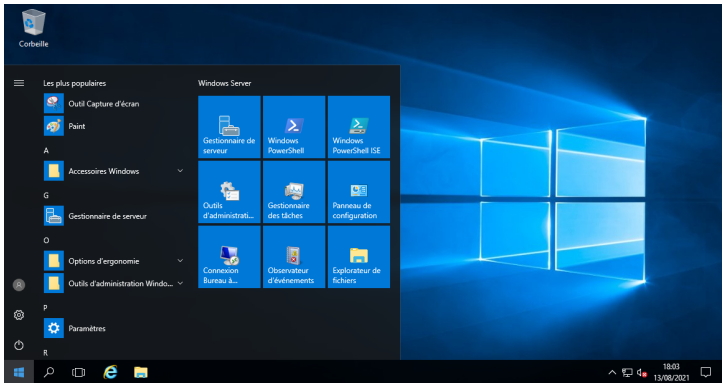


FIGURE 3.35 – Installation de windows server avec succès.

#### 3.5.1.1 Installation de Active Directory (AD1)

Dans cette partie nous allons installer le service de domaine Active Directory sur Windows Server 2016, En Suivant les étapes ci-dessous.

a) Tout d'abord, nous allons configurer la carte réseau du premier serveur ,en attribuant une adresse IP fixe 192.168.224.10/24 ,adresse du DNS (192.168.224.10/24).

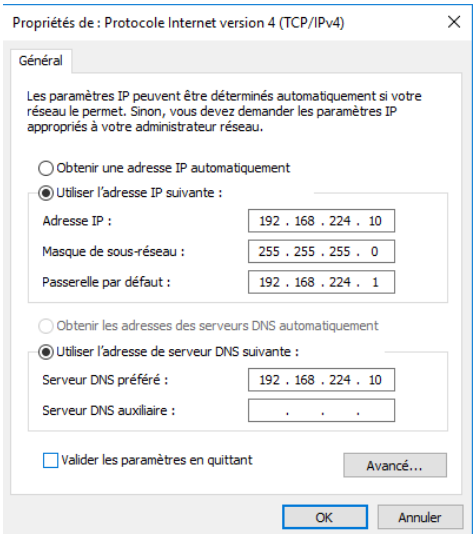


FIGURE 3.36 – Configuration de l'adressage du premier Serveur .

b) Une fois que nous avons terminer la configuration, nous allons nous connecter en tant qu'administrateur et appuyer sur le bouton du [menu Démarrer] et cliquer sur l'icône [Gestionnaire de serveur] qui est l'outil de gestion de Windows Server 2016.

c) Les services de domaine Active Directory sont un rôle Windows Server. Nous allons cliquer sur l'option [Ajouter des rôles et des fonctionnalités] pour installer le rôle.

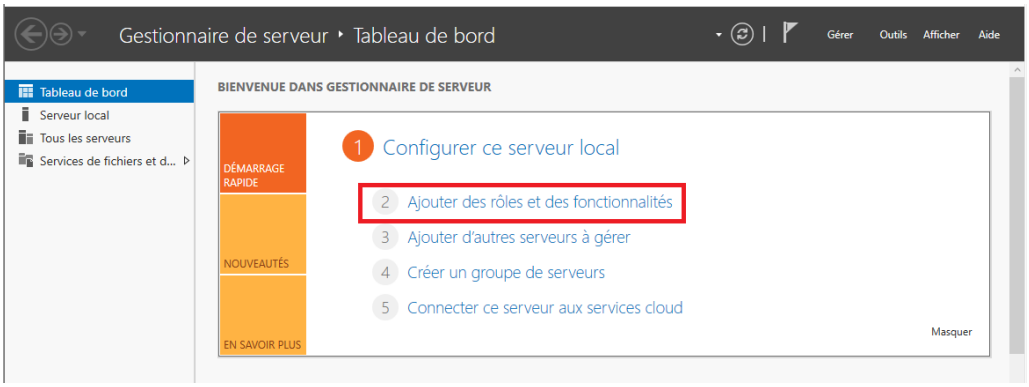


FIGURE 3.37 – Ajout des rôles et des fonctionnalités .

d) Ensuite, il ouvre l'assistant d'ajout de rôles et de fonctionnalités.Dans le "Avant de commencer", le "Type d'installation" et la "Sélection du serveur",nous allons conserver les valeurs par défaut.

e) Dans la fenêtre suivante à partir des rôles, nous allons cocher les deux cases, les services de domaine Active Directory et serveur de nom de domaine. Ensuite,nous Cliquons sur "Ajouter des fonctionnalités" pour les ajouter.

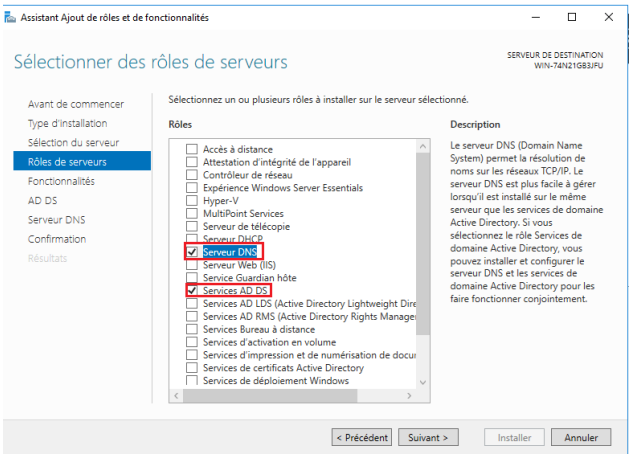


FIGURE 3.38 – Sélection des deux rôles DNS et AD DS.

f) La page des fonctionnalités,nous allons la conserver par défaut, puis dans les fenêtres suivantes, il nous donne une brève description du service AD DS et DNS .

g) Ensuite il nous donnera la confirmation de l'installation, nous cliquons sur "installer" pour démarrer le processus d'installation du rôle. Une fois l'installation terminée, nous cliquons sur l'option promouvoir ce serveur en contrôleur de domaine (voir Figure 3.39).

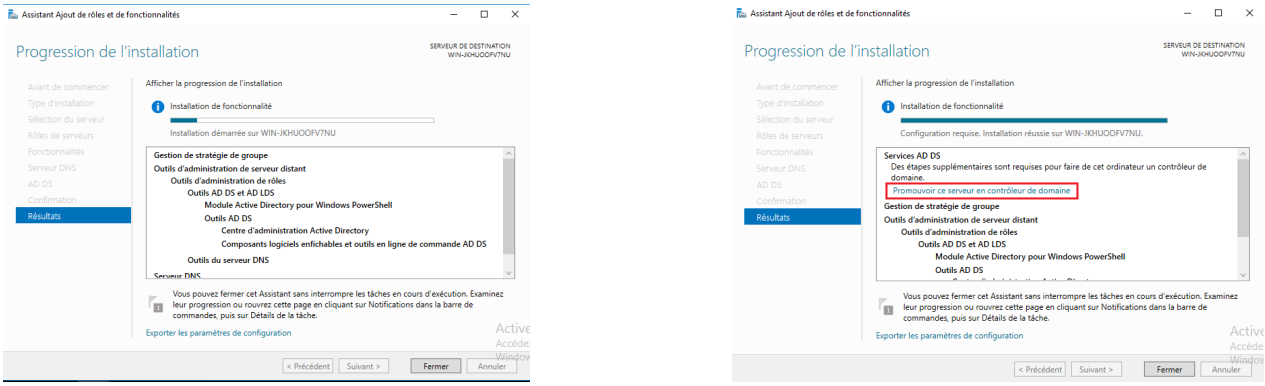


FIGURE 3.39 – Promotion du serveur en contrôleur de domaine.

h) Par la suite il ouvrira l'assistant de configuration d'Active Directory. Nous allons sélectionner la troisième option pour ajouter une nouvelle forêt puis Entrer un nom de domaine racine "generalemballage.local" (voir figure 3.40).

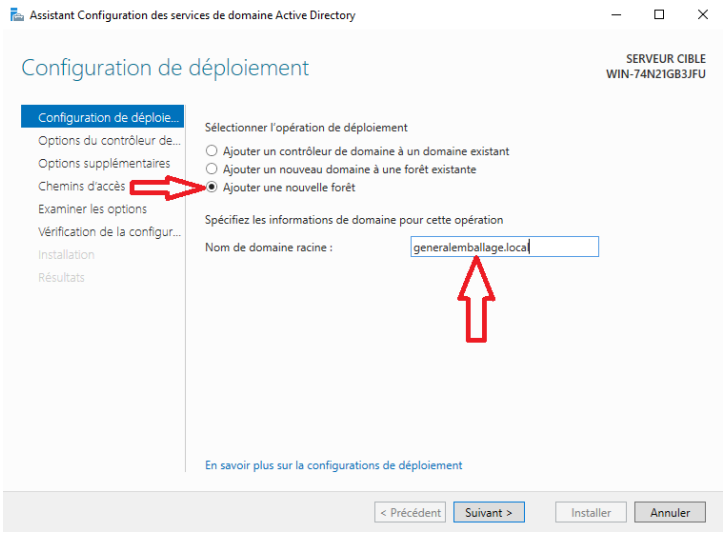


FIGURE 3.40 – Configuration de déploiement .

i) Dans la page suivante, nous allons sélectionner les niveaux fonctionnels du domaine et de la forêt. Ensuite tapons un mot de passe pour DSRM.

Cliquons ensuite sur "suivant",Pour le nom NETBIOS,nous allons garder la valeur par défaut (GENERALEMBALLAG).

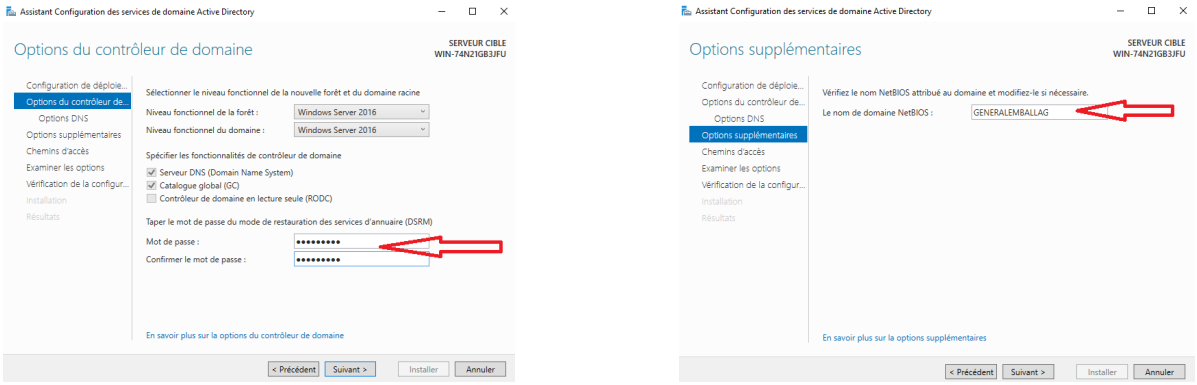


FIGURE 3.41 – configuration des options du contrôleur de domaine.

j) Dans la prochaine fenêtre, il effectuera une vérification des prérequis. Si toutes les conditions sont aquises, l'option d'installation sera activée. Cliquons sur installer pour commencer le processus d'installation.

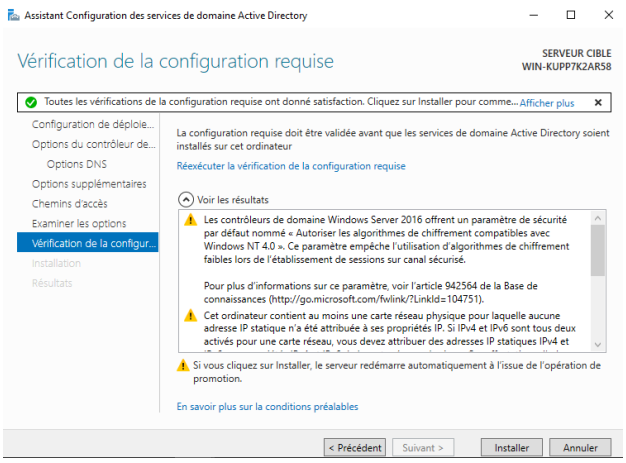


FIGURE 3.42 – Vérification des prérequis et installation contrôleur de domaine .

k) Une fois le redémarrage terminé,nous allons nous connecter avec le compte Administrateur du domaine qui correspond à l'administrateur local de ce serveur.
Dans le gestionnaire de serveur, nous verrons que le rôle "AD DS" est installé sur notre serveur (voir Figure 3.43).

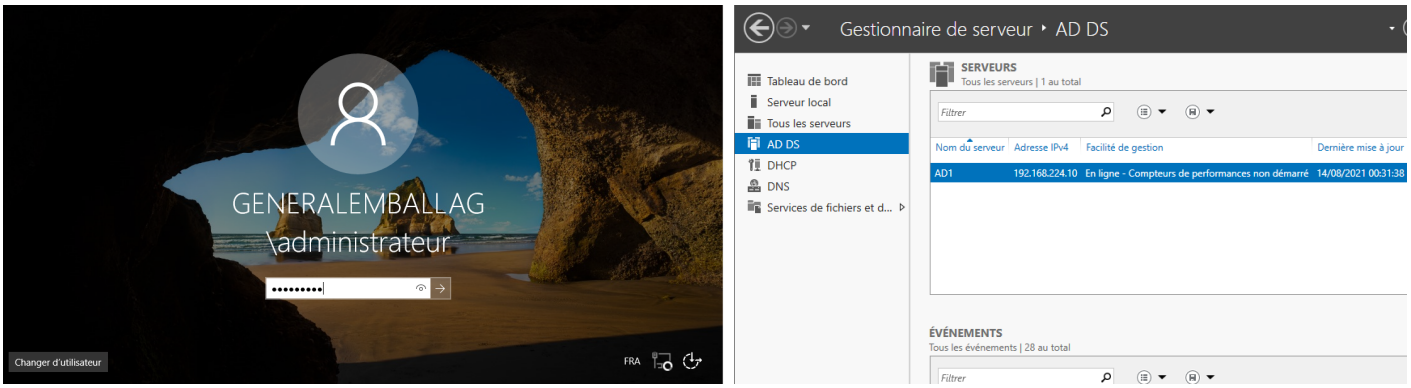


FIGURE 3.43 – Connexion au domaine "generalemballage.local".

**Création d'un utilisateur dans le domaine**

1. Cliquons sur [Démarrer] -> [Gestionnaire de serveur] -> [Outils] -> [Utilisateurs et ordinateurs Active Directory] ensuite nous allons cliquer sur le nom de domaine.
2. Cliquons sur Utilisateurs avec le bouton droit de la souris puis sélectionnons [Nouveau] > [Utilisateur],Dans les zones Nom d'utilisateur et Nom d'ouverture de session, nous allons entrer un nom "testuser".

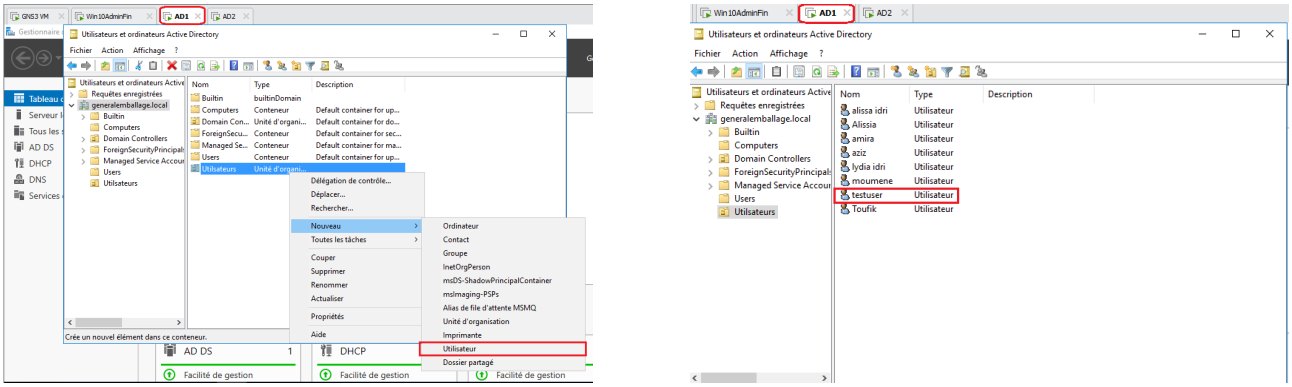

FIGURE 3.44 – Creation d'un utilisateur sur le premier serveur Active Directory .

### 3.5.1.2 Replication de Active Directory (ADirectory2)

Après avoir crée le domaine generalemballage.local, nous allons passer à la replication de Active Directory sur un autre Windows Server 2016, en Suivant les étapes suivantes :

a) Tout d'abord, nous Configurons les adresses du deuxième serveur on va mettre notre serveur en adresse IP fixe et nous allons rester sur le même réseau et lui attribuer l'adresse suivante : 192.168.224.11/24 ainsi dans la partie DNS nous attribuons l'adresse du AD1 (192.168.224.10/24) voir la figure ci-dessous.

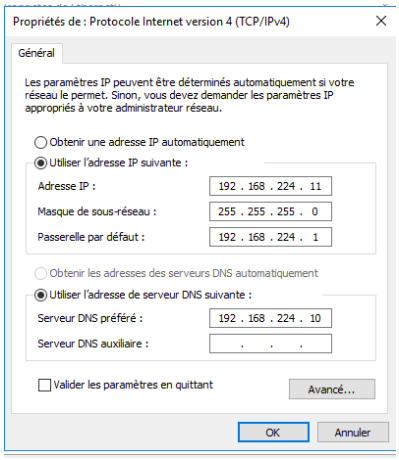


FIGURE 3.45 – Configuration de l'adressage du deuxième Serveur .

b) Comme notre premier serveur a un contrôleur de domaine et une forêt nous allons ajouter notre deuxième serveur a ce domaine. nous allons dans [Gestionnaire de Serveur] -> [Serveur local] -> [Nom de l'ordinateur],le renommer et l'ajouter dans notre domaine en saisissant les authentifications, enfin redemmarer le serveur et s'authentifier sur le domaine (voir figure 3.46).

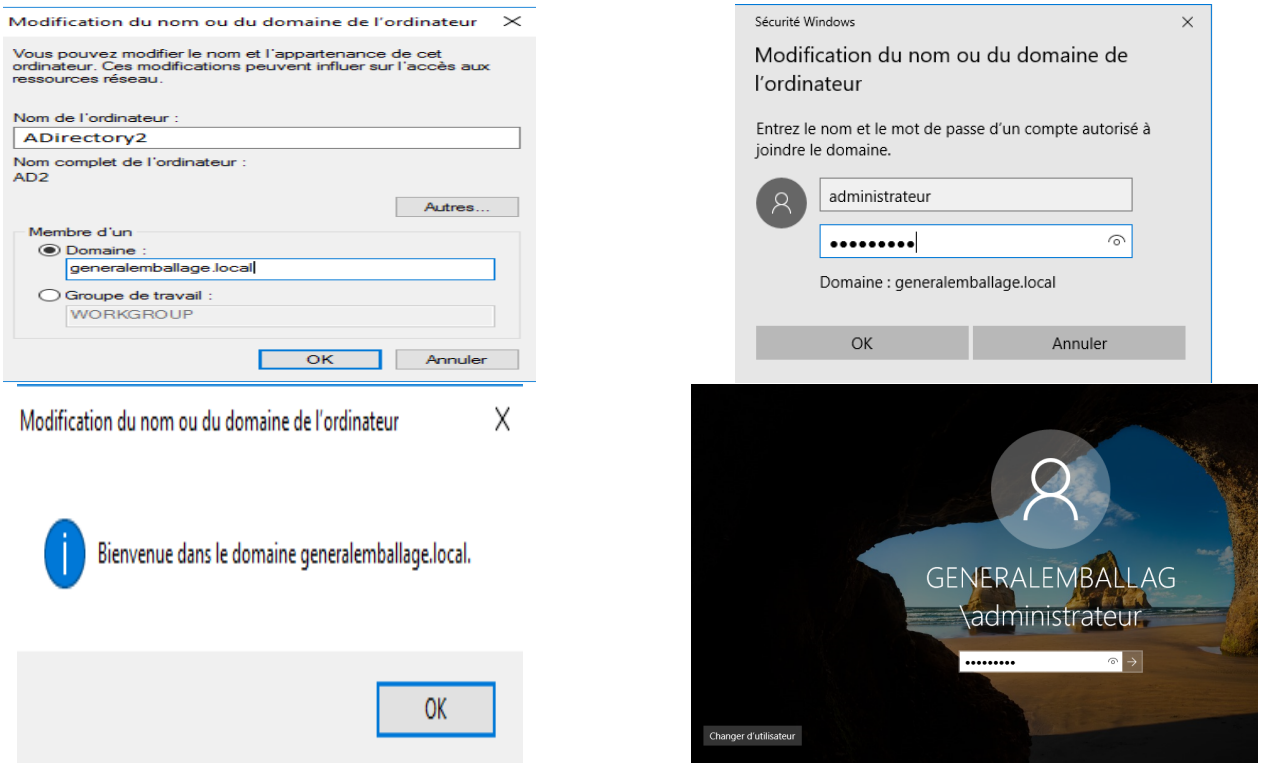


FIGURE 3.46 – Ajout du deuxième serveur à notre domaine.

c) Parmis les Prérequis de la replication du AD1 est l'installation du rôle AD DS sur ce deuxieme serveur en suivant les mêmes étapes expliquées auparavant (a-g).

d) Par la suite on effectuera la configuration de déploiement et nous allons sélectionner la première option pour ajouter un contrôleur de domaine à un domaine existant puis cliquer sur [modifier] et s'authentifier .

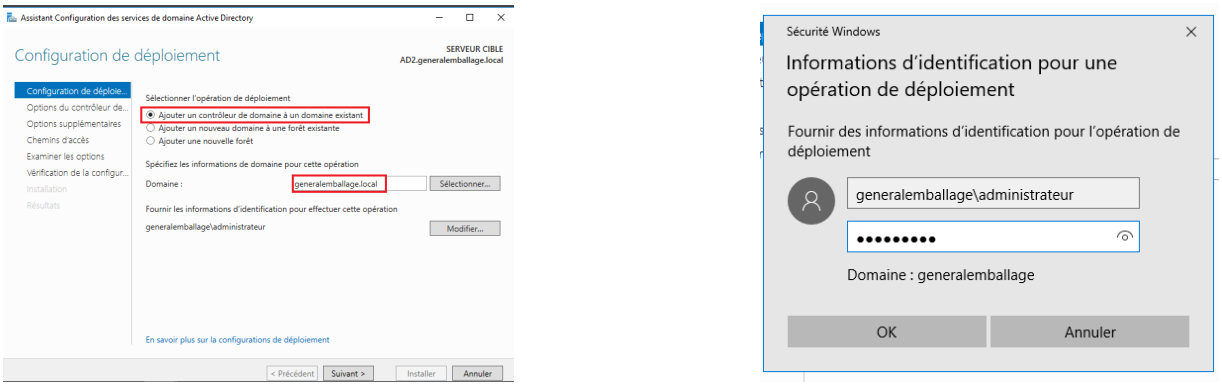


FIGURE 3.47 – Configuration de déploiement du deuxième serveur.

e) Nous allons indiquer un mot de passe de restauration, en mettant le même mot de passe que celui d'administrateur pour éviter tout problèmes, concernant les paramétrages suivants on les garde par défaut.

f) Pour les options supplémentaires ; concernant la case "Répliquer depuis" nous allons indiquer que la réplication se fait depuis le premier serveur (voir figure 3.48) puis passer à la vérification de la configuration requise et commencer l'installation.

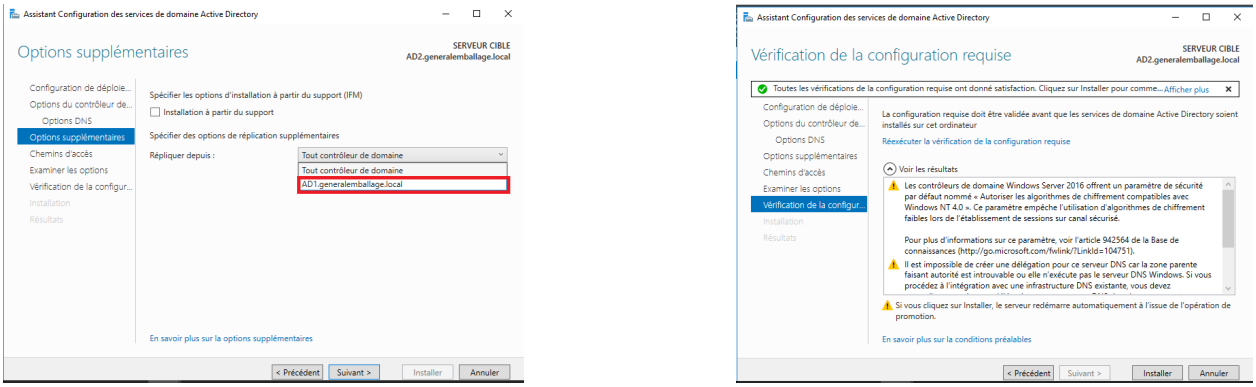


FIGURE 3.48 – Vérification des prérequis et installation du contrôleur de domaine .

g) A la fin de la procédure de réplication ,le serveur se redémarre automatiquement. Ensuite, la réplication se met en place et on remarque qu'après le lancement du gestionnaire de serveur que la partie AD DS est apparue sur le deuxième serveur.

h) Maintenant nous allons sur le premier serveur dans "Outils" -> "Utilisateurs et Ordinateurs Active Directory", sur notre foret "generalemballage.local" -> "Domain Controllers" , on remarque que y a le premier serveur (AD1) et le deuxième serveurs (ADirectory2).

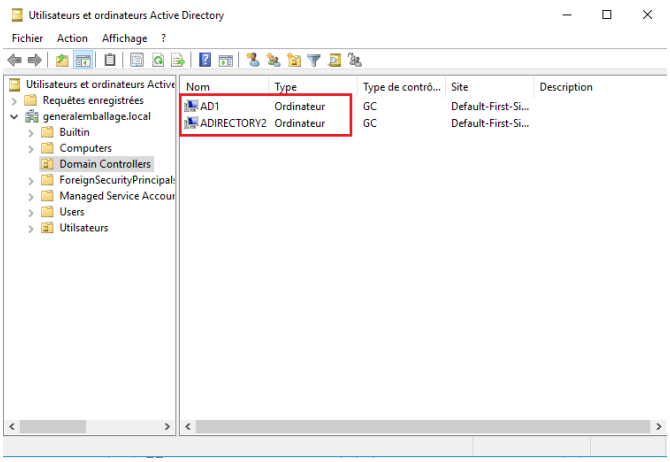


FIGURE 3.49 – Vérification de la réplication sur le premier serveur (AD1).

### 3.5.2 Installation de Windows 10 Professionnel

Pour installer Windows 10 professionnel, nous devons d'abord en avoir un fichier image ISO et nous assurer également d'avoir planifié le choix de l'édition de Windows 10 et d'avoir rempli la configuration système requise.

a) Tout d'abord, pour utiliser cette technique, nous allons sur l'assistant de création de machines virtuelles [File] -> [New Virtual Machine],nous choisissons : Typical (recommended).

b) Ensuite, nous devons ajouter une image d'installation dans la machine virtuelle, Sélectionner l'option Fichier image disque d'installation (ISO) en spécifiant le chemin du fichier ISO et l'importer.

c) Nous allons saisir un nom pour la machine virtuelle (Windows 10),rechercher un emplacement où stocker les fichiers d'installation.et spécifier la quantité de disque (recommandé 60 Go).

d) Dans la fenêtre suivante, nous allons vérifier les paramètres définis puis cliquons sur "Finish"et la machine virtuelle démarre automatiquement.

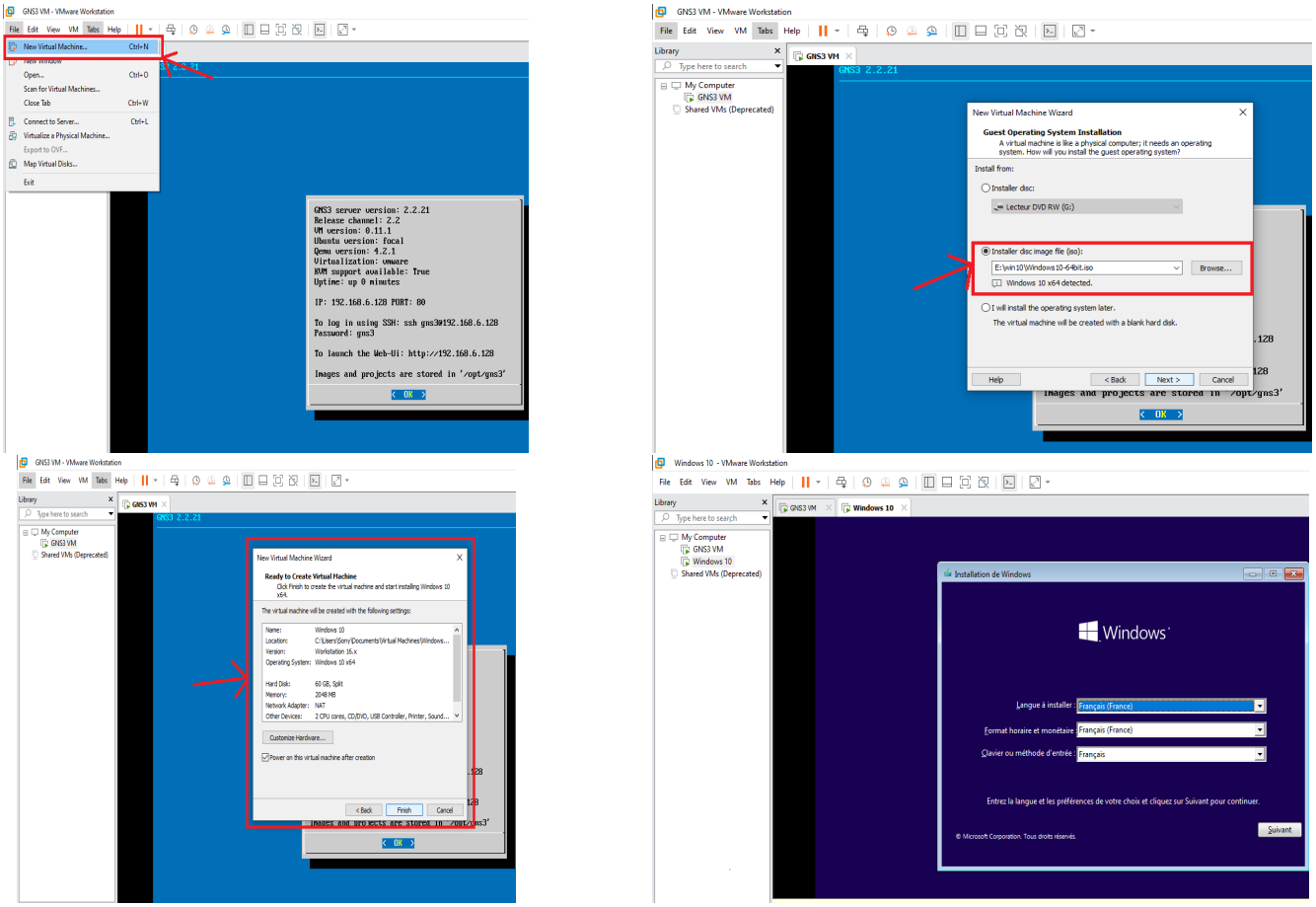


FIGURE 3.50 – Installation de Windows 10 professionnel.

e) L'installation de VMware Tools démarrera automatiquement, Plusieurs étapes d'installation de Windows 10 s'enchaînent avec plusieurs redémarrage de la VM.

f) La machine virtuelle VMware Workstation 16 en Windows 10 est alors démarrée et prête à l'emploi.

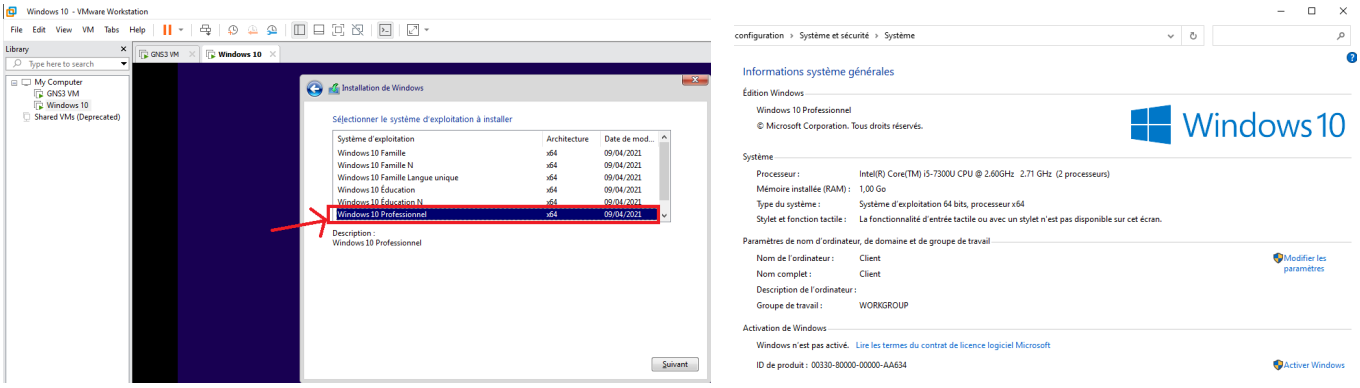


FIGURE 3.51 – Windows 10 professionnel prête à l'emploi.

- **Joindre pc Windows 10 professionnel au domaine Active Directory**

Notre réseau est basé sur un domaine "generalemballage.lacal" qui nous permet de centraliser notre réseau entier à partir d'un seul ordinateur appelé serveur. Ce domaine permet à un seul utilisateur de se connecter à partir de n'importe quel ordinateur en réseau dans le périmètre de notre réseau.

a) Tout d'abord, nous allons Sur le PC Windows 10, [Paramètres] -> [Système] > [À propos], puis nous cliquons sur "Rejoindre un domaine" et entrer le nom de notre domaine (generalemballage.local).

b) Dans la fenêtre suivante, nous entrerons les informations de compte qui est utilisées pour nous authentifier sur le domaine.

c) Une fois que notre ordinateur est authentifié sur le domaine on clique sur "OK".
Ensuite, nous devrons redémarrer pour terminer le processus,le PC devient membre du réseau et que la session utilisateur soit déjà préparée.

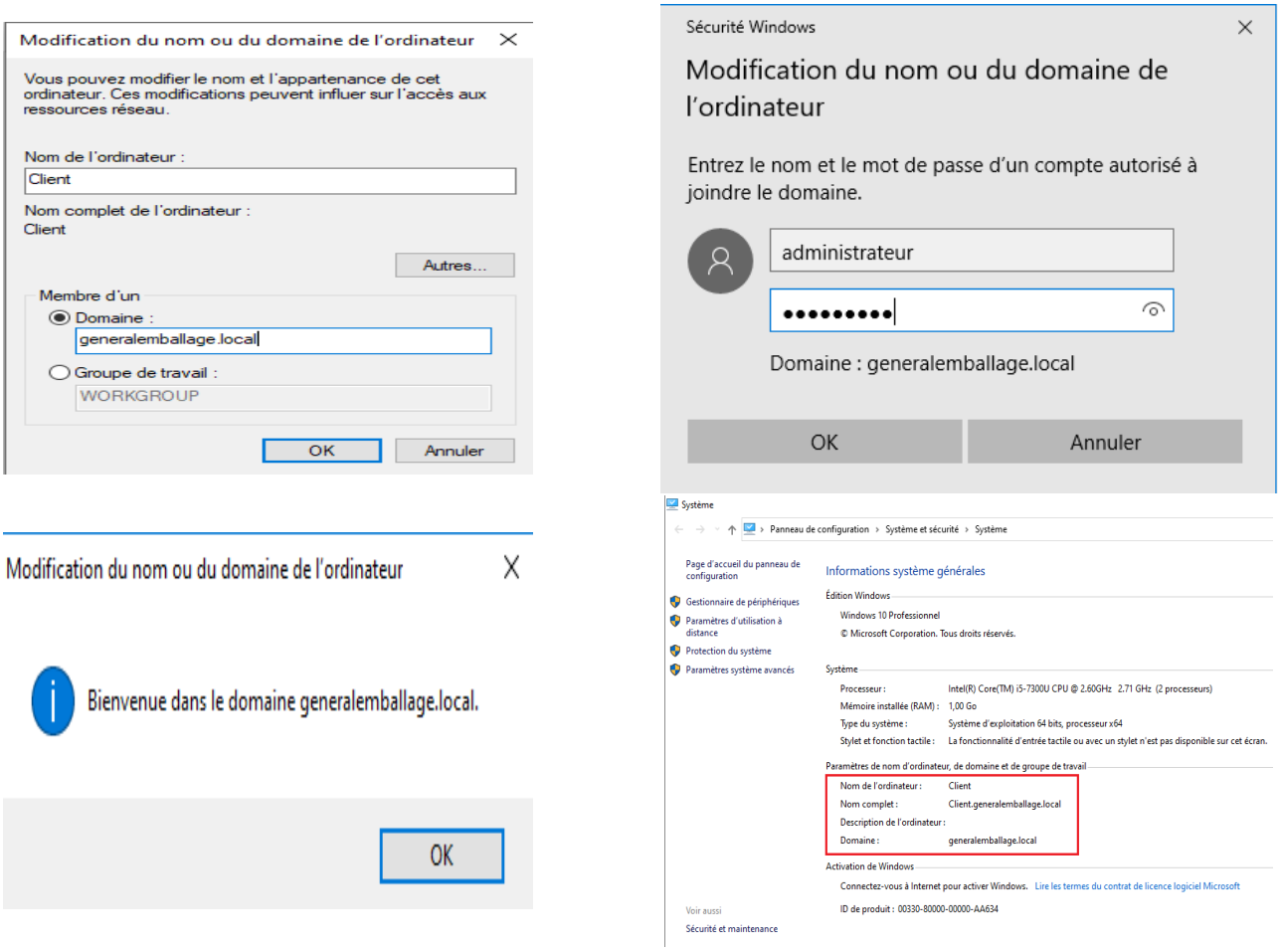


FIGURE 3.52 – Joindre Windows 10 professionnel au domaine.

d) Lorsque l'écran d'identification apparaît, nous remarquons que le compte "GENERALEMBALLAG/Administrateur" est affiché. Nous allons Entrer le mot de passe et nous serons alors connecté au domaine (generalemballage.local).

e) En dernier lieu, nous remarquons qu'une fois on est connecté au domaine (generalemballage.local), notre paramètre "À propos" n'affiche plus les options qui étaient présentées auparavant. Cela s'explique par le fait que notre ordinateur est géré de manière centralisée par le serveur.

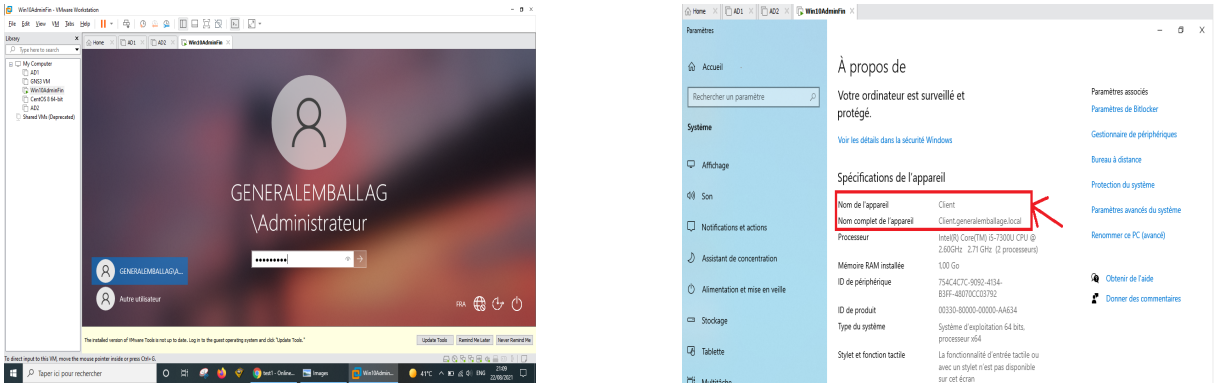


FIGURE 3.53 – Connection au domaine.

### 3.5.3 Installation de CentOS 8

Pour installer Centos 8 sur VMware Workstation 16 Pro,nous devons Tout d'abord, télécharger l'image du système d'exploitation CentOS 8 disponible sur le site officiel [2].

a) Nous allons sur l'assistant de création de machines virtuelles [File] -> [New Virtual Machine],nous choisissons : Typical (recommended).

b) Ensuite, nous devons ajouter l'image d'installation dans la machine virtuelle en sélectionnant l'option Fichier image disque d'installation (ISO).

c) Maintenant, nous définissons les informations de l'utilisateur avec les informations d'identification.

d) Par la suite, nous l'avons nommer CentOS8 64-bit et pour l'emplacement on la laisser par défaut.

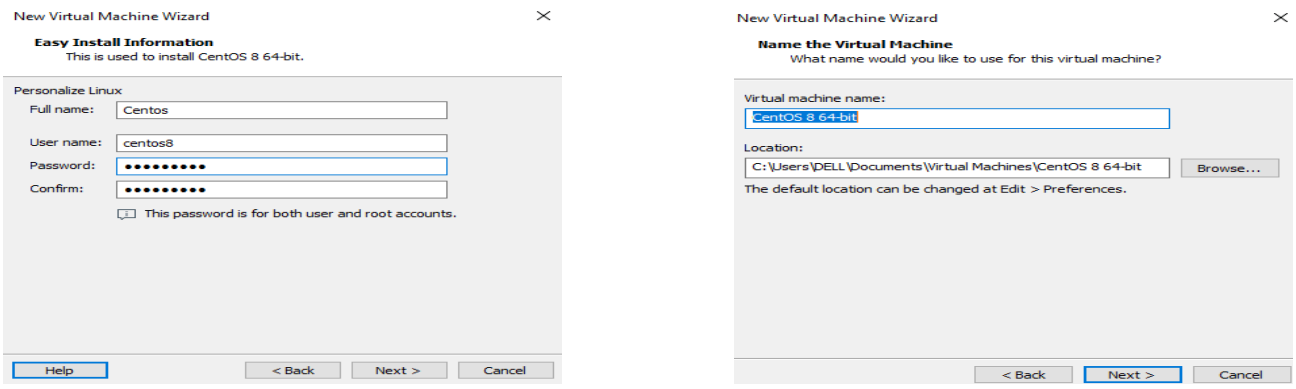


FIGURE 3.54 – Paramétrages des information d'installation de centOS 8.

e) Dans la fenêtre "Spécifier la capacité du disque", nous laissons tout par défaut, y compris la taille de stockage de 20 Go.

f) Dans la personnalisation du matériel, nous pouvons modifier de nombreux paramètres (mémoire, processeur), Une fois que nous avons terminé la personnalisation du matériel, on clique sur Terminer.Le processus d'installation commence et peut prendre un certain temps .

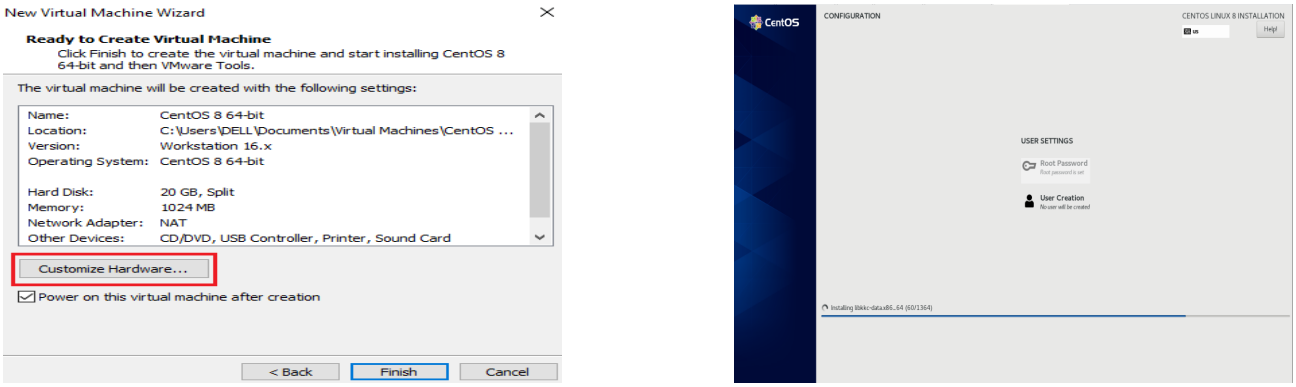


FIGURE 3.55 – Personnalisation et installation de CentOS 8.

g) Une fois l'installation terminée, nous pouvons continuer et redémarrer la machine en cliquant sur redémarrer et enfin l' écran de connexion s'affichera.

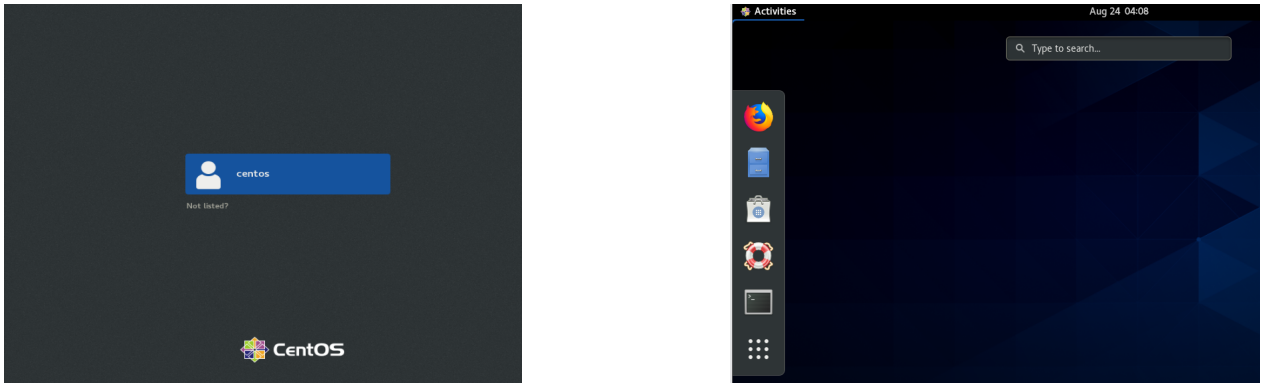


FIGURE 3.56 – Ecran de connexion et la page d'accueil de centOS 8.

- **Installation de Odoo13** Dans cette partie, nous allons montrer comment installer Odoo 13 sur une Machine virtuelle CentOS 8 . En premier lieu, nous allons connecter notre serveur en tant qu'utilisateur root.

a) **Mise à jour le système**

Nous allons mettre à jour le serveur avec la commande suivante :

```
[root@localhost centos8]# dnf update
CentOS-8 - AppStream100% [====================]
CentOS-8 - AppStream 98% [====================-]
```

Une fois que cette opération terminée, nous installons le référentiel EPEL en tapant :

```
Is this ok [y/N]: Operation aborted.
[root@localhost centos8]# dnf install epel-release
```

b) **Installation des packages Python et des dépendances d'Odoo**

Dans cette étape, nous allons installer Python 3 en exécutant la commande suivante :

```
Complete!
[root@localhost centos8]# dnf install python36 python36-devel
Extra Packages for E  5% [=                   ]  15 kB/s | 3.0 kB     00:03 ETA
```

Par la suite, nous installons tous les outils et dépendances dont nous aurons besoin pour construire le dernier Odoo 13 en tapant :

```
[root@localhost centos8]# dnf install git gcc wget nodejs libxslt-devel bzip2-devel openldap-
devel libjpeg-devel freetype-devel
Last metadata expiration check: 0:05:33 ago on Sun 27 Jun 2021 07:30:23 AM PDT.
Package gcc-8.3.1-4.5.el8.x86_64 is already installed.
Package wget-1.19.5-7.el8_0.1.x86_64 is already installed.
Dependencies resolved.
```

c) **Création d'un utilisateur Odoo**

Nous allons créer un nouvel utilisateur système et un groupe dont nous aurons besoin pour exécuter le service Odoo. Le répertoire personnel que nous définirons dans le /opt/odoo répertoire .

```
Complete!
[root@localhost centos8]# useradd -m -U -r -d /opt/odoo -s /bin/bash odoo
[root@localhost centos8]#
```

d) **Installation et configuration de PostgreSQL**

Installez PostgreSQL en exécutant :

```
[root@localhost centos8]# dnf install postgresql postgresql-server postgresql-contrib
CentOS-8 - AppStream                                            7.0 kB/s | 4.3 kB     00:00
CentOS-8 - Base                                                 5.7 kB/s | 3.9 kB     00:00
CentOS-8 - Extras                                               3.3 kB/s | 1.5 kB     00:00
Extra Packages for Enterprise Linux Modular 8 - x86_64           28 kB/s |  60 kB     00:02
Extra Packages for Enterprise Linux 8 - x86_ 59% [=======================          ]  48 kB/s |  32 kB     00:00 ETA
```

Ensuite, nous initialisons la base de données

```
Installed:
  postgresql-10.17-1.module_el8.4.0+823+f0dbe136.x86_64         postgresql-contrib-10.17-1.module_el8.4.0+823+f0dbe136.x86_64
  postgresql-server-10.17-1.module_el8.4.0+823+f0dbe136.x86_64  libpq-13.3-1.el8_4.x86_64
  uuid-1.6.2-43.el8.x86_64

Complete!
[root@localhost centos8]# /usr/bin/postgresql-setup initdb
```

Une fois cela fait, nous pouvons démarrer le processus PostgreSQL . Puis, nous allons créer un nouvel utilisateur PostgreSQL avec le même nom que le système utilisateur Odoo .

```
[root@localhost centos8]# systemctl start postgresql
[root@localhost centos8]# systemctl enable postgresql
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql.service → /usr/lib/systemd/system/
[root@localhost centos8]# su - postgres -c "createuser -s odoo"
[root@localhost centos8]#
```

e) **Installation de Wkhtmltopdf**

Odoo nécessite le wkhtmltopdfpackage, qui est un outil open source qui convertit le format HTML en PDF afin qu'Odoo puisse imprimer des rapports PDF. Nous allons installer la version 0.12.6 .

```
[root@localhost centos8]#
[root@localhost centos8]# sudo yum -y install wget
```

```
[root@localhost centos8]#
[root@localhost centos8]#
[root@localhost centos8]# wget https://github.com/wkhtmltopdf/packaging/releases/download/0.12.6-1/wkhtmltox-0.12.6-1.centos8.x
86_64.rpm
--2021-06-25 07:27:31--  https://github.com/wkhtmltopdf/packaging/releases/download/0.12.6-1/wkhtmltox-0.12.6-1.centos8.x86_64.
rpm
```

```
[root@localhost centos8]#
[root@localhost centos8]# sudo dnf localinstall wkhtmltox-0.12.6-1.centos8.x86_64.rpm
```

f) **Installation et configuration d'Odoo 13**

Dans cette étape, nous allons cloner la branche d'Odoo 13.0 sur le serveur. Mais d'abord, nous allons passer à l'utilisateur Odoo que nous avons créé dans les étapes précédentes.

```
[root@localhost centos8]# su - odoo
Last login: Sun Jun 27 09:18:48 PDT 2021 on pts/0
Last failed login: Mon Jun 28 05:15:42 PDT 2021 on pts/0
There were 7 failed login attempts since the last successful login.
[odoo@localhost ~]$ git clone https://www.github.com/odoo/odoo --depth 1 --branch 13.0 /opt/odoo/odoo13
```

Nous pouvons commencer par l'installation des modules Python requis pour l'installation d'Odoo :

```
[root@localhost odoo13]# pip3 install Babel==2.6.0
WARNING: Running pip install with root privileges is generally not a good idea. Try `pip3 install --user` instead.
Collecting Babel==2.6.0
  Downloading https://files.pythonhosted.org/packages/b8/ad/c6f60602d3ee3d92fbed87675b6fb6a6f9a38c223343ababdb44ba201f1
/Babel-2.6.0-py2.py3-none-any.whl (8.1MB)
    100% |                                | 8.1MB 21kB/s
```

Les commandes suivantes créeront un fichier journal pour la nouvelle installation d'Odoo et changeront sa propriété en l'utilisateur « odoo » :

```
[odoo@localhost odoo13]$
[odoo@localhost odoo13]$ mkdir /var/log/odoo13 && touchez /var/log/odoo13/odoo.log
mkdir: cannot create directory '/var/log/odoo13': File exists
[odoo@localhost odoo13]$ chown -R odoo: /var/log/odoo13/
```

L'étape suivante consiste à créer un fichier de configuration pour la nouvelle instance Odoo.

```
[odoo@localhost odoo13]$ nano /etc/odoo.conf
[odoo@localhost odoo13]$
```

Une fois le fichier ouvert, nous allons taper la configuration ci-dessous,nous enregistrons et fermons le fichier, ceci termine l'installation d'Odoo sur notre système.

```
[options]
; This is the password that allows database operations:
admin_passwd = Serveur16
db_host = False
db_port = False
db_user = odoo
db_password = False
xmlrpc_port = 8069
; longpolling_port = 8072
logfile = /var/log/odoo13/odoo.log
logrotate = True
addons_path = /opt/odoo/odoo13/addons,/opt/odoo/odoo13-custom-addons
```

g) **Création d'un fichier Unit File**

Maintenant que notre installation d'Odoo est terminée, nous allons créer un fichier d'unité de service afin que nous puissions exécuter Odoo en tant que service en tapant :

```
[odoo@localhost odoo13]$
[odoo@localhost odoo13]$ nano /etc/systemd/system/odoo13.service
[odoo@localhost odoo13]$
```

Une fois le fichier ouvert, nous allons taper la configuration ci-dessous :

```
[Unit]
Description=Odoo13
#Requires=postgresql-10.6.service
#After=network.target postgresql-10.6.service

[Service]
Type=simple
SyslogIdentifier=odoo13
PermissionsStartOnly=true
User=odoo
Group=odoo
ExecStart=python3 /opt/odoo/odoo13/odoo-bin -c /etc/odoo.conf
StandardOutput=journal+console

[Install]
WantedBy=multi-user.target
```

Une fois le fichier enregistré et fermé, nous rechargerons le démon en tapant :

```
[odoo@localhost odoo13]$
[odoo@localhost odoo13]$ systemctl daemon-reload
```

Enfin, nous pouvons utiliser les commandes suivantes pour démarrer et activer au démarrage notre nouvelle instance Odoo.

```
[odoo@localhost odoo13]$ systemctl start odoo13
[odoo@localhost odoo13]$ systemctl enable odoo13
```

Nous pouvons exécuter la commande status afin de vérifier si la nouvelle instance Odoo est active et en cours d'exécution.

```
[root@localhost ~]# systemctl status odoo13.service
● odoo13.service - Odoo13
   Loaded: loaded (/etc/systemd/system/odoo13.service; enabled; vendor preset: >
   Active: active (running) since Tue 2021-06-29 04:04:18 PDT; 4min 6s ago
 Main PID: 911 (python3)
    Tasks: 4 (limit: 4892)
   Memory: 3.5M
   CGroup: /system.slice/odoo13.service
           └─911 /usr/bin/python3 /opt/odoo/odoo13/odoo-bin -c /etc/odoo.conf

Jun 29 04:04:18 localhost.localdomain systemd[1]: Started Odoo13.
```

h) **Accés à l'instance Odoo**

Maintenant que nous avons terminé l'installation d'Odoo est qu'elle est activée et en cours d'exécution sur le serveur, nous pouvons y accéder via le navigateur en tapant "http ://127.0.0.1 :8069/web". Nous pourrons voir l'écran de configuration d'Odoo comme indiqué ci-dessous.

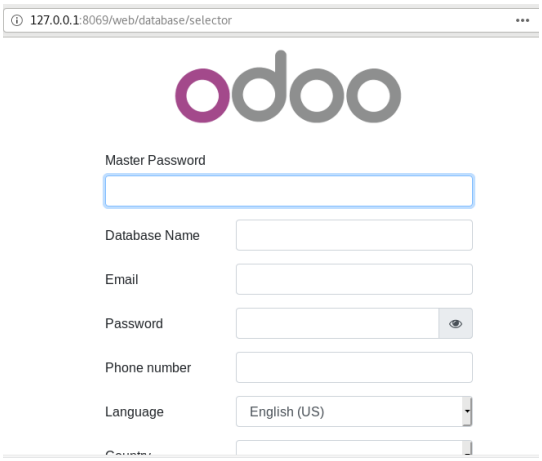


FIGURE 3.57 – Ecran de configuration d'Odoo 13

Nous pouvons maintenant créer notre première base de données et commencer à utiliser le dernier Odoo 13.

## 3.6 Conclusion

Dans ce chapitre nous avons présenter toutes les installations des VMs faites avec succès , qui nous ont servi pour la réalisation et la mise en oeuvre de notre maquette tout en respectant l'architecture de l'entreprise. Ainsi, nous avons configuré divers services primordiaux à la sécurité du réseau.

Dans le prochain chapitre, nous allons faire des tests et validation afin d'affirmer le bon fonctionnement de toutes les configuration mise en oeuvre.

# Chapitre 4

# Tests et Validations

## 4.1 Introduction

Après avoir Installer les machines virtuelles et configurer les principales fonctionnalités de notre firewall Fortigate proposées dans le chapitre précédent, nous réaliserons dans ce dernier chapitre des tests de validation pour l'affirmation du bon fonctionnement de chaque service.

## 4.2 Vérification des fonctionnalités de Fortigate

Les tests de vérification visent ainsi à vérifier que les services mis en place dans notre système Fortigate sont fonctionnels. Nous allons effectuer dans ce qui suit différents types de tests pour la validation et la confirmation de nos différentes configurations.

### 4.2.1 Fonctionnement des VLANs

Comme nous remarquons dans cette figure le fortigate a attribuer une adresse IP "192.168.10.11" au terminal qui est dans le service "Informatique" après avoir activé le DHCP ; ce qui signifie le bon fonctionnement du DHCP configuré sur le VLAN 10, Nous allons faire la même chose pour les autres PCs des autres services.

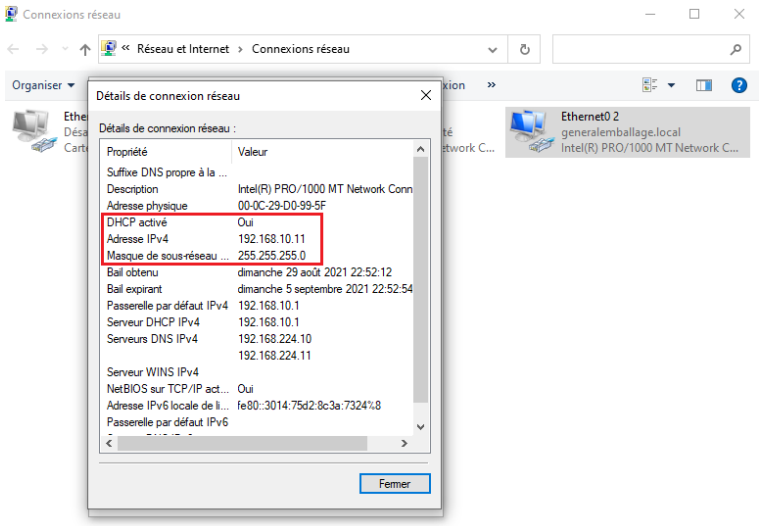


FIGURE 4.1 – Attribution adresse IP par DHCP .

- **Connectivité entre les VLANs** Nous allons faire des ping à partir d'un utilisateur (user3) du service Informatique vers tous les autres services (GRH et Commercial), Serveurs ainsi que la zone démilitarisée .

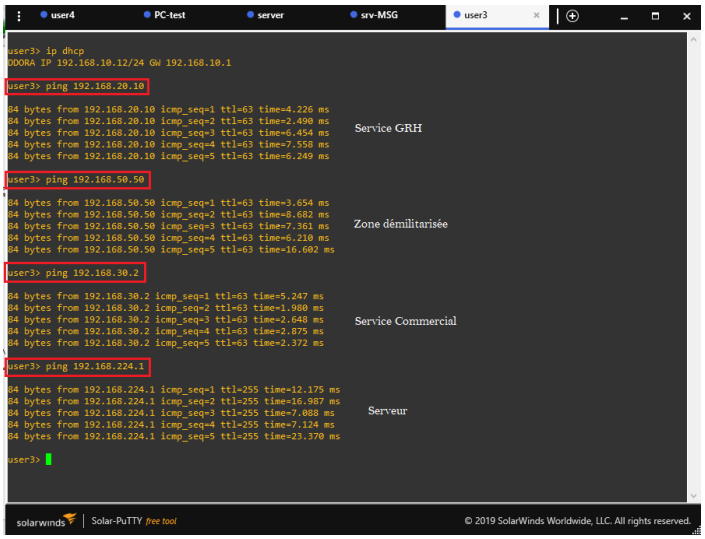


FIGURE 4.2 – Connectivité entre les VLANs .

Nous allons tester la connectivite de la zone démilitarisée vers le WAN ainsi que la zone "inter-Vlan", où nous allons constater un ping échoué vers le service Informatique ; Cette configuration dote le réseau de l'entreprise d'un niveau de sécurité supplémentaire, en empêchant les pirates d'accéder directement aux serveurs et aux données internes via Internet.

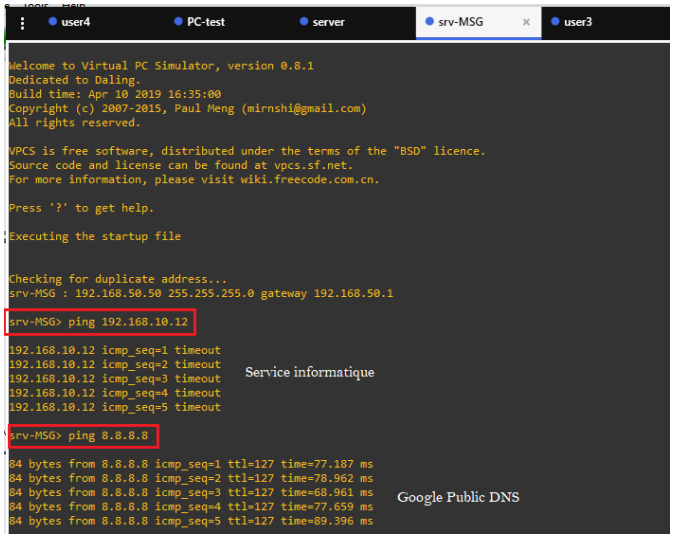


FIGURE 4.3 – Connectivite de la zone démilitarisée .

### 4.2.2 Tests de fonctionnement des règles de filtrage

- **Connexion à Internet**

Nous allons tester la connectivité Internet des différents services des deux sites (Akbou,Oran).

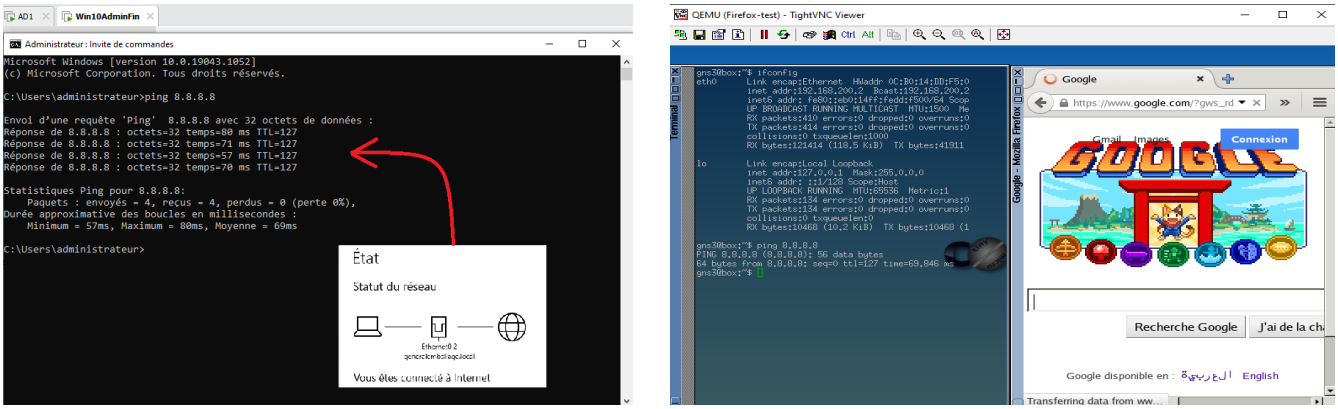


FIGURE 4.4 – Tests d'accès a Internet.

- **Filtrage Web**

Nous testons l'accès à l'URL "facebook" qu'on avais bloquer précédemment. En visitant : "http ://facebook.com " comme notre policy est configuré, nous verrons une page bloquée.

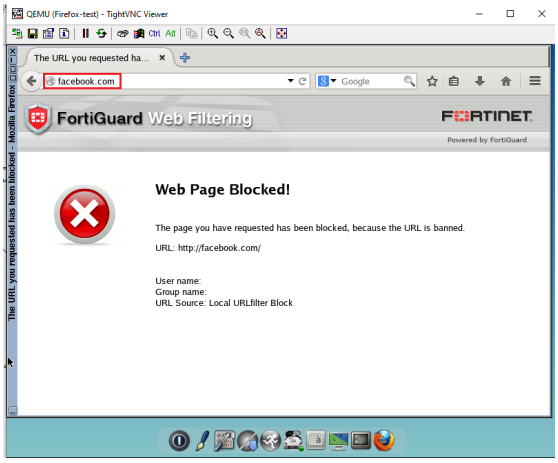


FIGURE 4.5 – Page URL "Facebook" Bloquer.

- **Filtrage Applicatif**

La figure ci-dessous illustre parfaitement à partir du PC Windows10 qui est dans le service informatique, le test réalisé pour accéder a l'application "Gmail" est bloquée.

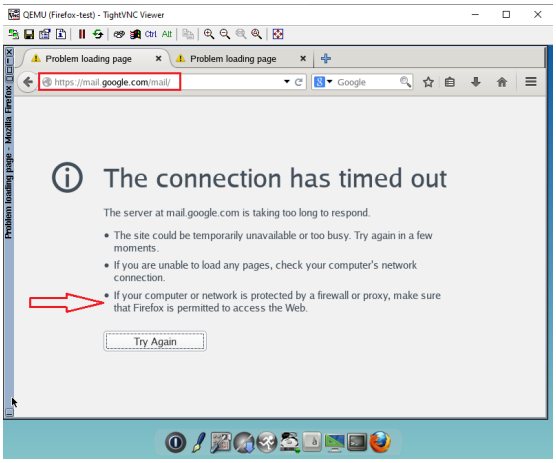


FIGURE 4.6 – L'application "Gmail" bloqué.

### 4.2.3 Service VPN IPsec

Afin de tester l'état de fonctionnement du service de notre VPN . Nous allons faire un Ping à partir du réseau d'Akbou vers le réseau distant d'Oran et inversement.

Dans cet exemple nous choisissons de réaliser notre test dans le service informatique afin de joindre un hôte du réseau distant d'Oran Comme vous pouvez le voir sur la Figure 4.7, l'hôte 192.168.10.11 (Informatique) arrive à pinguer l'hôte 192.168.200.1 du réseau distant d'Oran .

Nous pouvons aussi vérifier si notre test fonctionne dans le sens inverse. En essayant de pinguer depuis le site d'Oran un hôte se situant sur le site principale d'Akbou (nous garderons le même exemple précédent). Le test est illustré à travers la deuxieme capture suivante :

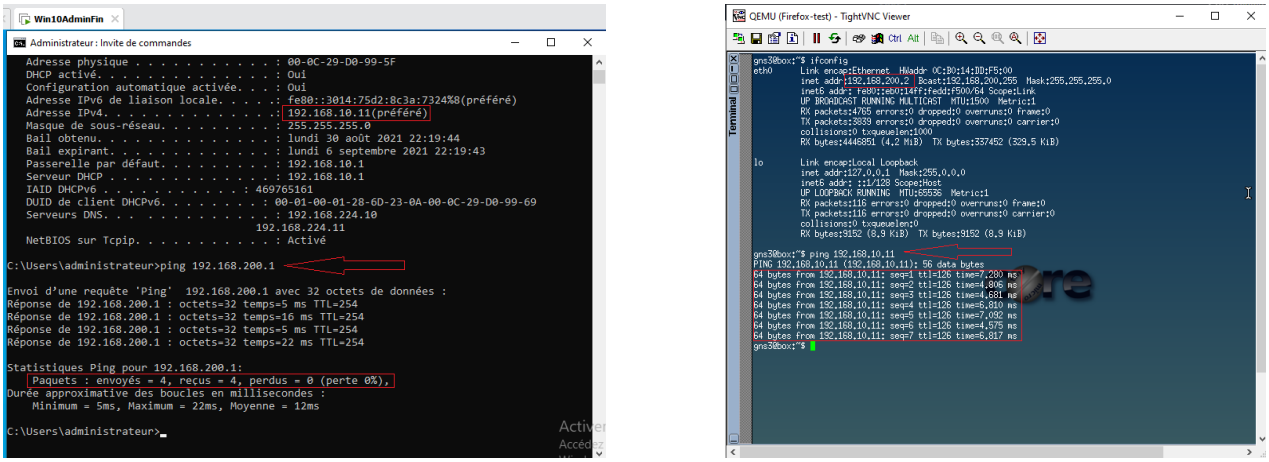


FIGURE 4.7 – Test de fonctionnement du VPN à partir du site Akbou vers Oran et inversement .

### 4.2.4 Haute disponibilité du Fortigate

Afin de vérifié la qualité du traitement des transactions et de flux nous allons faire un test sur la haute-disponibilité en provoquant une panne volontairement.

Nous allons lancer un ping continu "ping 192.168.30.1 -t" sur le fortigate-A (le maitre) après un moment en rafale nous allons l'arrêter ou débrancher le câble réseau de l'interface WAN. nous remarquons que le fortigate-B (l'esclave) bascule du secondaire vers le primaire et reprend le relais pour assurer la continuité du service.

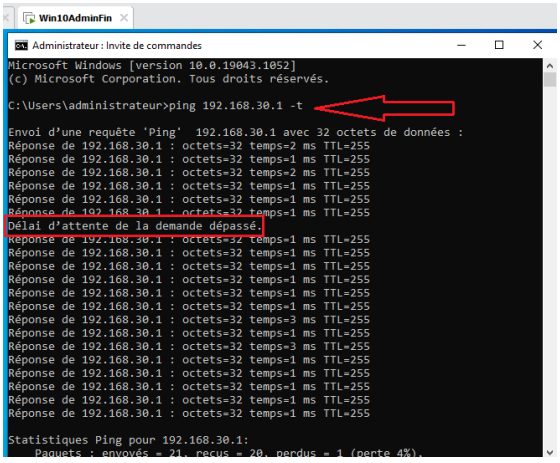


FIGURE 4.8 – Test du basculement HA .

## 4.3 Test de réplication

Maintenant nous allons vérifier si la réplication entre les contrôleurs de domaine (AD1 et ADirectory2) est automatiquement générée, en vérifiant sur le serveur ADirectory2 si une copie de l'utilisateur crée auparavant (testuser) a été créer (voir figure 4.9).

Nous pouvons aussi aller dans Invite de commandes et taper "set" et vérifier que LOGONSERVER est bien sur le serveur ADirectory2.

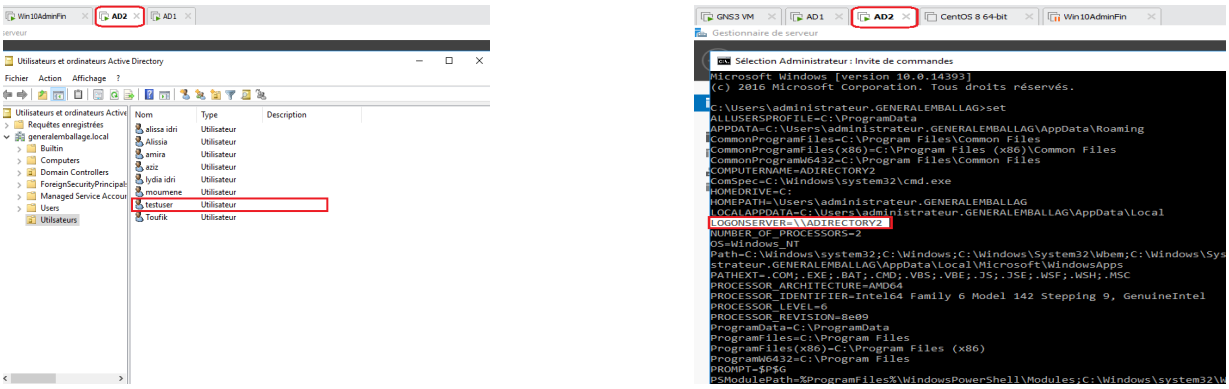


FIGURE 4.9 – Vérification de la réplication sur ADirectory2.

## 4.4 Fonctionnement Odoo13

Après avoir installée odoo13, nous allons crée une base de donnée (Demo data) en remplissant le formulaire ci-dessous :

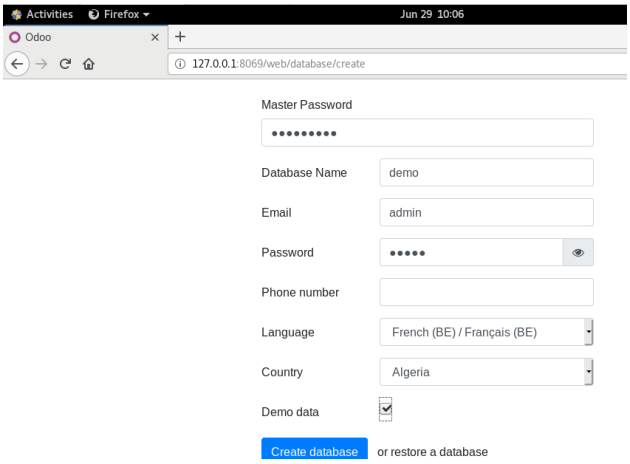


FIGURE 4.10 – Création d'une base de donnée Odoo13.

L'interface ci-dessous représente les différentes applications qui peuvent être installée selon le besoin de l'entreprise.

Maintenant il nous reste plus qu'à implémenter une application de vente, prenons comme exemple le module CRM dans l'éditeur gratuit Odoo 13.

ci-dessous l'nterface des applications d'Odoo :

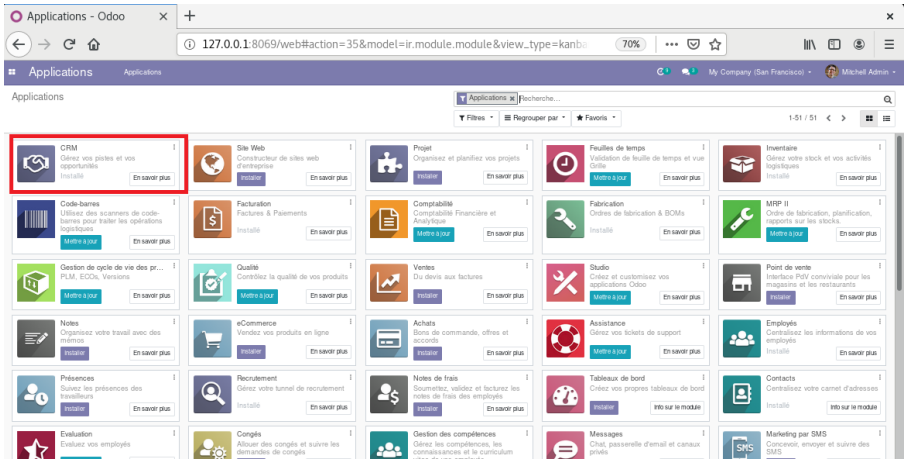


FIGURE 4.11 – Interface des applications d'Odoo.

La figure ci-dessous représente un exemple de pipeline qui est une représentation visuelle des clients potentiels, du stade où ils trouvent dans le processus d'achat, donnent également un aperçu des prévision établies pour le compte d'un compte d'un commercial et ce qu'il lui reste à parcourir pour atteindre son quota.

Un pipeline permet aussi de savoir où se situe l'équipe commerciale dans son ensemble par rapport aux objectifs globaux fixés.

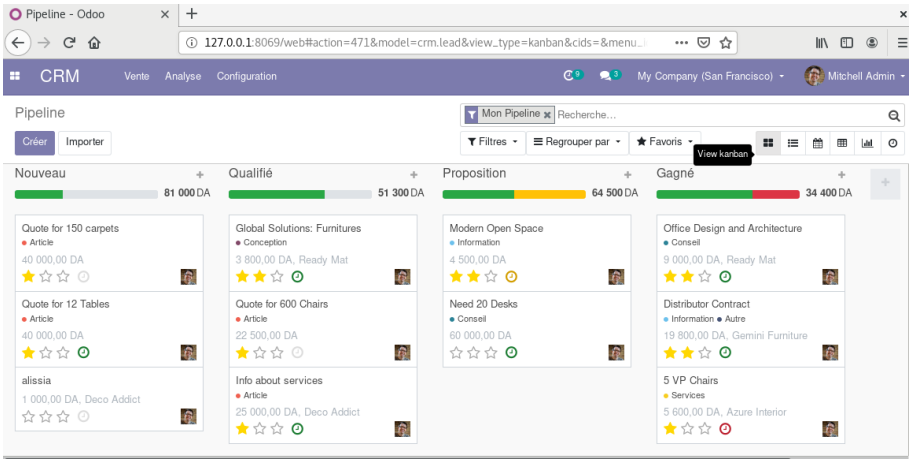


FIGURE 4.12 – Gestion du pipeline client avec l'intégration Odoo CRM.

## 4.5 Conclusion

Durant ce dernier chapitre, nous avons mis en évidence divers tests de fonctionnement de chaque service configuré auparavant, où nous avons constaté leurs bons fonctionnements. Cette étape nous a permis de valider et d'atteindre les différents objectifs de notre solution .

# Conclusion générale et perspectives

Ce travail nous a permis d'acquérir une expérience personnelle et professionnelle intéressante. Nous avons amélioré nos connaissances et compétences en terme de configuration dans un environnement virtuel qui est Vmware. De plus nous avons perfectionné nos connaissances dans le domaine de la sécurité d'un réseau d'entreprise grâce à l'implémentation d'un réseau virtuel privé, ainsi que d'un pare-feu Fortigate .

Au terme de ce projet, nous avons pu exploiter nos connaissances théoriques et pratiques acquises durant notre cycle universitaire, pour la mise en place d'un firewall open source FortiGate au profit de l'entreprise Général Emballage.

Dans un premier temps, nous avons présenté l'architecture existante du réseau de l'entreprise et quelques généralités. Dans un second temps nous avons présenté notre infrastructure réseau sous GNS3 ainsi que toutes les installations et Configurations faîtes sur le pare-feu FortiaGate nous avons configurer sur ce dernier les VLANs pour segmenter le réseau de l'entreprise Général Emballage puis le filtrage du flux de données entrant/sortant à l'aide de règles de pare-feu ACL, et enfin l'implémentation d'une politique de sécurité pour l'interconnexion des différents site d'Akbou ainsi deux VPN configurer ...

En dernier lieux, nous avons réalisé une simulation du réseau de l'entreprise sous GNS3 afin d'effectuer divers tests de validations des configurations et services réalisés, qui ont été décrits dans le dernier chapitre consacré aux tests de fonctionnements.

Suite aux travaux effectués, plusieurs points restent à développer et à améliorer. Parmi lesquels citons :

- Intégration d'autres applications comme la facturation, la gestion de transport pour l'ERP.
- Ajout des VPN client à site pour que le personnel puisse travailler a distance .
- Mise en place des stratégies de groupe et des politique d'authentification.

# Bibliographie


[1] Bibliothèque de documents fortinet. https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/116821/zone. Page consultée le 29 juin 2021.

[2] Centos8. http://isoredirect.centos.org/centos/8/isos/x86_64/. Page consultée le 20 juin 2021.

[3] Iso/iec norme managment de sécurité l'information. //https://www.iso.org/fr/home.html. Page consultée le 26 juin 2021.

[4] The one-stop networking shop for gns3 network pros. https://www.gns3.com/marketplace/featured/fortigate. Page consultée le 2 juillet 2021.

[5] Questionnaire risque cyber. https://riskat.fr/public/questionnaires/cyber.php. Page consultée le 15 juin 2021.

[6] systeme d'information. https://www.syloe.com/glossaire/systeme-dinformation/. Page consultée le 20 mai 2021.

[7] k. D. Alexnder Pierre. Dispositifs de securite informatique. *Nowteam*, 20 aout 2018.

[8] M. Ameur et al. *Gestion du parc informatique a base d'un logiciel libre*. PhD thesis, Université Virtuelle de Tunis, 2017.

[9] V. Bollapragada, M. Khalid, and S. Wainner. *IPSec VPN Design*. Cisco Press, 2005.

[10] Cisco. Configuration de dmz. https://www.cisco.com/c/fr_ca/support/docs/smb/routers/cisco-rv-series-small-business-routers/Configuring_DMZ_on_the_RV34x_Series_Router.html. Page consultée le 2 juin 2021.

[11] Encyclopédie. l'emulation en informatique. 11 octobre 2020.

[12] E. GALL. la virtualisation en informatique. 201, 27 octobre 2020.

[13] V. GURANDA. La cyber-sécurité. 2021.

[14] J. Lefebvre. Concervez l'architecture d'un systeme. https://openclassrooms.com/fr/courses/1372996-concevez-larchitecture-dun-systeme/5670259-decrivez-la-couche-operationnelle. Page consultée le 20 mai 2020.

[15] Microsoft. Active directory-integrated dns zones. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/active-directory-integrated-dns-zones. Page consultée le 3 juin 2021.

[16] B. V. Patz Michel. Alignement business-it : le cas de l'erp odoo, 2017.

[17] E. sécurité Informatique. sécuriser son réseau avec un pare-feu fortigate de fortinet. *newsletter*, 2019.

[18] T. Vasiljeva and E. Berezkina. Determining project management practices for enterprise resource planning system projects. *Journal of Enterprise Resource Planning Studies*, 2018, 2018.

# Résumé

Ce présent ouvrage pourtant sur notre projet de fin de cycle Master fait état de l'étude portée sur l'entreprise Général Emballage de Akbou.

Notre travail consiste à simuler et émuler une architecture réseau sécurisé sous GNS3 en prenant en compte les différentes faiblesses et vulnérabilités qui peuvent être exploité par un attaquant.

Durant notre travail, nous avons réalisé différentes configurations sur le firewall FortiGate à savoir la mise en place de deux tunnels VPN sécurisé ; entre les différents sites distants de l'entreprise, une haute disponibilité, une liste de contrôle d'accès ainsi que diverses fonctionnalités.



**Mots clés :** GNS3, FortiGate, Général Emballage, VLANs, VPN, HA, AD, ACL, Odoo, ...


---


# Abstract

This book, however, on our end-of-master's cycle project, reports on the study carried out on the Akbou General Emballage company.

Our work consists in simulating and emulating a secure network architecture under GNS3 by taking into account the various weaknesses and vulnerabilities which can be exploited by an attacker.

During our work, we carried out various configurations on the FortiGate firewall, namely the establishment of two secure VPN tunnels ; between the various remote sites of the company, high availability, an access control list as well as various Features.



**Keywords :** GNS3, FortiGate, General Emballage , VLANs, VPN, HA, AD, ACL, Odoo, ...