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

Université A. Mira de Béjaïa
Faculté des Sciences Exactes
Département informatique

Mémoire de Fin de Cycle
En vue de l'obtention du diplôme de Master professionnel en Informatique
Option : Administration et sécurité des réseaux

Thème

Étude et Amélioration d'une infrastructures réseau en multicouches. Cas d'étude SPA Général emballage

Réalisé par :

M^lle^ OUFELLA *Nadjet* et M^lle^ LAHBIBEN *Imane*

Soutenu le 14/09/2023 devant les jury composé de :

Président :	Mr.SAADI Mustapha	M.C.B	U.A/Mira Béjaia
Examinateur :	Mr.KHENOUS Lachemi	M.C.B	U.A/Mira Béjaia
Encadrant :	Mr. BENNAI Yani-Athman	M.C.B	U.A/Mira Béjaia
Co-Encadrant :	Mr. BERAZA Abderrahmane	Doctorant	U.A/Mira Béjaia

Promotion 2022/2023

Remerciements

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères remerciements.
Nous remercions le dieu le tout puissant de nous avoir donné la force, la volonté de donner le meilleur de nous-même et le courage de mener ce travail.
Nous tenons en premier lieu à exprimer notre profonde reconnaissance à notre encadreur **Mr. BENAI Yani-Atehman**, et notre **Co-Encadrant Mr. BERAZA Abderrahmane** pour leurs encadrements, puis pour nous avoir fait confiance, encouragé et conseillé au cours de réalisation de ce projet.
Nos profonde gratitude et sincères remerciements à notre encadrant de stage **Mr LAHLOU Mhnd Arezki** au sien de l'entreprise Général Emballage 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 ; plus précisément **Mr L. KESSOUM.**

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'espoir 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 sœurs, puisse dieu vous donner amour, bonheur et Réussite « **Latifa** » « **Mounia** » « **Sonia** » et « **Naima** » pour leur soutient et encouragement.
A tous mes professeurs, leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.

On remercie tous ceux qui ont contribués de près ou de loin à l'aboutissement de notre travail. Pour tous, merci infiniment.

Oufella nadjet

Dédicaces

Je dédie ce modeste travail
À mon cher papa, mon exemple, quoi que je fasse ou que je dise je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.

À ma très chère maman qui éclair mon chemin et m'illumine de douceur, celle qui n'a jamais dit non à mes exigences et qui s'est toujours sacrifier pour me voir réussir.
À mon adorable petite sœur Wissame, que Dieu te protège.
Mon défunt grand-père, j'aurais tant voulu que tu sois présent avec moi mais Dieu en a voulu autrement.
À ma grand-mère et grand-père à qui je souhaite une longue vie, mes oncles, mes tentes et mes cousines.

À toute ma famille ainsi que mes proches amis qui n'ont cessés de m'encourager.
À mes meilleures amis Yazid, Saliha, Wissame, Halima et Sabrina.

Lahbiben imane

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ACL Access Control List

AD DS Active Directory Domain Services

AD CA Active Directory Certification Authority

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DNS Domain Name System

GNS3 Graphical Network Simulator

GRE Generic Routing Encapsulation

HA High Availability

HSRP Host Standby Router Protocol

HTTPs Hypertext Transfer Protocol Secure

IPSec Internet Protocol Security

IPS Intrusion Prevention System

IP Internet Protocol

LACP Link Agregation Control Protocol

LAN Local Area Network

NAT Network Address translation

NPS Network policy server

OSI Open system interconnection

PEAP Protected Extensible Authentication Protocol

RADIUS Remote Access Dial In User Service.

UTM Unified threat management

VLAN Virtual Local Area Network

VM Virtual Machine

VPN virtual private network

WAN Wide Area Network

Introduction Générale

L'infrastructure réseau est le fondement sur lequel repos de nombreuses initiatives technologiques et opérationnelles des entreprise modernes. Son rôle est essentiel pour soutenir la croissance des infrastructures Réseau, la sécurité et l'agilité dans un environnement numérique. Elle a fait irruption dans le quotidien des entreprises permettent ainsi un des services qui sont offerts.

Nous projetons notre étude sur l'entreprise agroalimentaire SPA Général Emballage, nous avons pu observer que l'infrastructure réseau existante contient quelques défaillances, due 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'une infrastructure 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 Radius ceux-ci dans le but d'améliorer et de virtualiser la couche infrastructure réseau.

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

- Le premier chapitre intitulé « Généralités sur le Réseau et la sécurité informatique » comporte deux parties : la première est consacrée aux généralités sur les Réseaux informatiques. dans la seconde partie nous présentons quelque généralité sur les attaques et les mécanismes de sécurité.
- Le deuxième chapitre titré « Présentation de l'organisme d'accueil » 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 nous exposerons les problématiques ainsi que les solutions.
- Le troisième chapitre nommé « Études des solutions proposées » est consacré a la présentation des solutions proposées.
- Le quatrième chapitre intitulé « Réalisation » définit toutes les configurations nécessaires pour la mise en œuvre de notre infrastructure, Et les différentes vérifications des fonctionnalités de Fortigate, Active Directory et test fonctionnement Radius, ayant servis à l'émulation de notre implémentation, tout en expliquant les configurations établies.

Enfin, nous terminerons notre travail par une conclusion générale.

ChapitreI. Généralité sur les réseaux et la Sécurité Informatique

I.1 Introduction

L'administration de réseau est une discipline de l'informatique qui désigne plus précisément les opérations de contrôle du réseau avec la gestion des configurations et de la sécurité, Toute machine connectée à un réseau informatique peut être vulnérable aux attaques, menace, etc.

La sécurité informatique est une notion qui émerge de plus en plus dans le monde actuel, son concept est de recouvrir un ensemble des méthodes, techniques et outils de sécurisation des ressources.

Dans ce chapitre, nous essayons de donner une idée générale sur les réseaux et la sécurité informatique, en commençant par des définitions simples, nous fournirons le vocabulaire usuel utilisé dans ces domaines, puis nous expliquerons comment se protéger de ces dangers.

I.2 Les Réseaux Informatique

I.2.1 Définition d'un Réseau informatique

Un réseau informatique est constitué de nœuds autonomes, qui sont des systèmes informatiques reliés par des supports matériels et logiciels, et qui peuvent communiquer entre eux directement ou indirectement. En effet, même deux ordinateurs peuvent suffire pour former un réseau [1].

I.2.2 L'intérêt des Réseaux informatique

Les réseaux informatiques permettent de [2] :

- Outil de communication (email travail collaboratif ...)
- Partage des ressources (programme, équipement, données).
- Partage de ressources matérielles
- L'interaction avec les utilisateurs connectés.
- La garantie de l'unicité de l'information
- Réduire ses charges et mutualiser les coûts
- Commerce électronique.

I.2.3 Architectures des Réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories [3] :

— Réseau Client /serveur

Comportent en général plus de dix postes. La majorité des stations sont des « postes clients », c'est à dire des ordinateurs, utilisée par les utilisateurs, tandis que les autres stations sont réservées à une ou plusieurs taches spécialisées, ce qui les qualifie alors de serveurs.

— Réseau poste à poste

En règle générale, les réseaux poste à poste ont peu de postes, souvent moins de dix, car chaque utilisateur est responsable de l'administration de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.

I.2.4 Types de Réseaux

Nous pouvons classifier les réseaux informatiques de la manière suivante [4] :

— PAN (Personal Area Network)

Un réseau PAN relie sur quelques mètres des équipements personnels (tels que les terminaux UMTS, portables, organiseurs, Pc portable, etc.) d'un même utilisateur.

— LAN **(**Local Area Network)

Ce sont des réseaux locaux d'étendue limitée, destiné à l'échange de donnée et au partage local de ressources informatique au sein d'une entreprise.

— MAN (Métropolitain Area Network)

C'est des réseaux d'étendus de l'ordre de quelques kilomètres, utilisés pour connecter plusieurs sites équipés d'un réseau local (réseau de campus).

— WAN (Wide Area Network)

C'est des réseaux très étendus, qui assurent le transport des informations sur de longue distances entre plusieurs villes et pour interconnecter des réseaux appartenant à une même entreprise.

I.2.5 Topologies d'un Réseaux

- **Topologies physiques**

Il existe trois topologies physiques pour concevoir un réseau : bus, anneau et étoile [5] :

— Bus

La topologie en bus (support linéaire) repose sur un câblage, sur lequel viennent de connecter des nœuds (postes de travail, Equipements d'interconnexion, périphérique). Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux.

— Anneau

Cette topologie utilise une boucle fermée pour connecter les périphériques via des liaisons point à point. Chaque nœud fonctionne comme un répéteur et les trames transitent par chaque nœud.

— Etoile

Repose sur des équipements actifs qui remettent en forme et régénèrent les signaux en intégrant une fonction de répéteur. Ces équipements centraux sont appelés desconcentrateurs (hubs) et des commutateurs (Switchs). Il est possible de créer une structure hiérarchique en utilisant un nombre limité de niveaux.

- **Topologies logiques**

La topologie logique désigne la manière dont les équipements communiquent en réseau. Dans cette topologie les plus courantes sont les suivantes [6] :

— Topologie Ethernet

dans ce réseau, la communication s'effectue à l'aide d'un protocole appelé CSMA/CD, ce qui permet une surveillance minutieuse des données transmises afin d'éviter les collisions.

— Topologie Token ring

La topologie Token Ring repose sur un anneau physique (ring) et utilise la méthode d'accès au jeton (Token). Dans cette technologie, seule la station possédant le jeton a le droit de transmettre.

— Topologie FDDI

La topologie FDDI est composée de deux anneaux : un anneau principal et un anneau secondaire. L'anneau secondaire est utilisé pour compenser les erreurs sur l'anneau principal. FDDI utilise un jeton (Token ring) pour détecter et corriger les erreurs.

I.2.6 Arbre Modèle d’un Réseau hiérarchique

— Couche d’accées

Cette couche a pour rôle principal de permettre aux utilisateurs de se connecter au réseau et d'assurer un accès de première ligne aux services réseau. C'est à ce niveau que la plupartdes hôtes, y compris les serveurs et les postes de travail des utilisateurs, sont reliés au réseau [7].

— Couche distribution

La couche de distribution agit comme une interface entre la couche d'accès et la couche centrale. Sa fonction principale est de fournir le routage, le filtrage et l'accès au WAN (WideArea Network), ainsi que de déterminer comment les paquets peuvent accéder à la base si nécessaire [7].

— Couche cœur réseau

La couche cœur du réseau, quant à elle, est la couche supérieure. Son rôle est de relier les différents segments du réseau, tels que les sites distants, les LAN et les étages d'une entreprise) [7] (voir figure I.1).

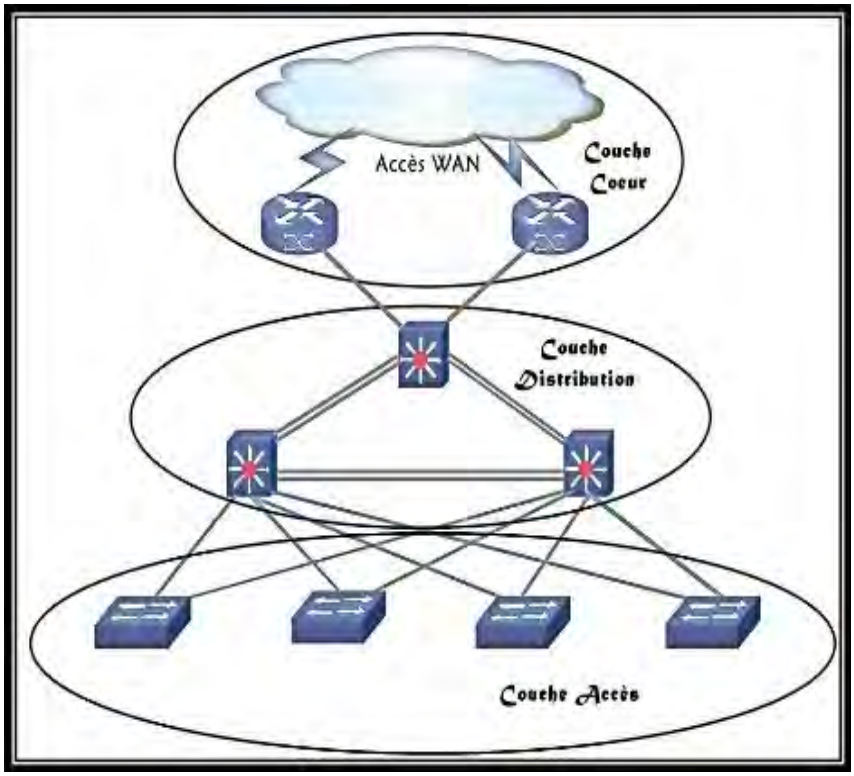


FIGURE I.1 - ARBRE Modèle d’un réseau hiérarchique.

I.2.7 Les normes de Communication

I.2.7.1 Le Modèle de Référence OSI (open système interconnexion)

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System Interconnexion OSI destiné à normaliser les échanges entre deux machines. Il définit ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques [8] (voir Figure I.2).

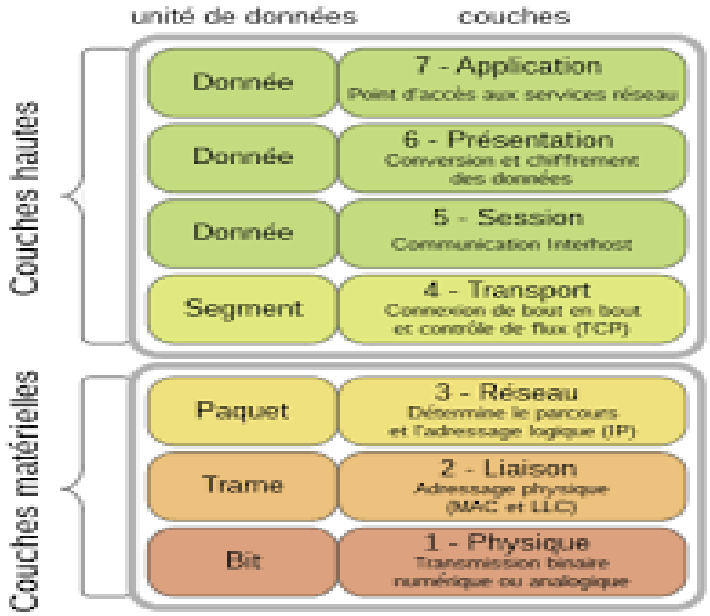


FIGURE I.2 - le modèle OSI.

— Couche physique : Cette couche assure la transmission des données binaires d'une machine à une autre. Elle définit les aspects de synchronisation et de formatage grâce auxquels les bits sont convertis en signaux transmis sur des canaux de communication.

— Liaison de donnée : Cette couche permet à deux machines connectéesphysiquement par un canal de communiquer de manière fiable et efficace en échangeant des données sous forme de trames.

— Réseaux : La couche réseau a pour mission de transporter les paquets de bout en bout, de la source à la destination, en passant par plusieurs réseaux et routeurs.

— Transport : Cette couche garantit le transport fiable des données entre une sourceet une destination, indépendamment des réseaux physiques, en s'appuyant sur la couche réseau.

— Session : La couche session permet principalement l'ouverture, la gestion et la fermeture de sessions entre deux machines communicantes.

— Présentation : Cette couche permet la présentation des données dans un format standard compréhensible par toutes les machines.

— Application : Cette couche constitue une interface d'accès au réseau pour lesapplications utilisateurs. Elle permet à ces dernières d'envoyer et de recevoir des données à travers le réseau.

I.2.7.2 La pile protocolaire TCP/IP

Le protocole TCP/IP est une suite de protocoles de communication et une pile qui prend comme modele de base OSI, utilisés pour interconnecter des périphériques réseau sur Internet. Il spécifie comment les données sont échangées sur Internet en fournissant des communications de bout en bout qui identifient comment elles doivent être divisées en paquets, adressées, transmises, acheminées et reçues destination [4] (voir Figure I.3).

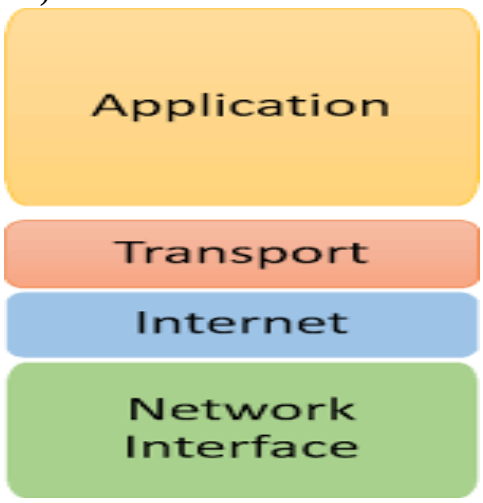


FIGURE I.3 - la pile protocolaire TCP/IP.

— Couche Accès réseau : Cette couche est regroupée les couches physique et liaison de données du modèle OSI. Elle assure la bonne gestion du médium (détection de collisions) et permet l'acheminement des informations entre émetteur et destinataire au niveau des adresses MAC.

— Couche Internet : Ce sont ici des protocoles de haut niveau de la couche réseau. IP permet le routage des informations entre réseaux, c'est ici que l'adresse IP est utilisée, ICMP est un protocole de contrôle qui offre des outils permettant de détecter les erreurs et de signaler des problèmes. Il joue un rôle essentiel et mérite une attention particulière. Nous reviendrons plus en détail sur ce protocole. Il est également important de mentionner le protocole ARP.

— Couche Transport : La couche transport permet d'identifier les applications qui communiquent en utilisant des ports de communication spécifiques à chaque application plutôt que des noms d'applications. La couche transport gère 2 protocoles de livraisondes informations : UDP est dit "sans connexion" et TCP est dit "avec connexion".

— Couche application : C'est la couche de haut niveau, elle correspond directement avec l'utilisateur, elle englobe les couches OSI d'application, de présentation et de session. Elle s'assure que les données soient correctement "empaquetées" pour qu'elles soient lisibles par la couche suivante.

I.2.8 Les supports de Transmission

Le câble à fibre optique, le câble à paire torsadée et le câble coaxial sont les trois types principaux de câbles réseau utilisés dans les systèmes de communication [2].

— Coaxial

Pour transmettre des signaux haute fréquence, des câbles coaxiaux sont nécessaires. Ils sont constitués d'un conducteur en cuivre rond entouré de trois couches d'isolation et de blindage pour limiter les interférences externes.

— La paire torsadée

Est le moyen de transmission le plus simple, utilisé pour les communications téléphoniqueset la plupart des réseaux Ethernet. Elle peut être blindée ou non-blindée et se compose d'unou plusieurs fils torsadés en spirale. Ce type de support convient à la transmission de signaux analogiques et numériques.

— La fibre Optique

C'est un type de câble Ethernet utilisés pour la transmission de données sous forme d'impulsions de lumière qui passent à travers de minuscules tubes de verre. Elle est utiliséepour des débits très élevés, mais peut être divisée en fibres monomodes (SMF) et multimodes (MMF) en fonction de la qualité de transmission requise et de l'environnement.

I.2.9 Le protocole IP

Le protocole IP (Internet Protocol) est un protocole de communication de niveau 3 dans le modèle OSI, qui permet d'envoyer des paquets de données à travers le réseau. Il est utilisé pour établir des communications entre les machines et fournit un service d'adressage unique pour toutes les machines [9].

✓ **Routage**

Le routage est une technique qui permet de diriger les informations vers leur destination dans un réseau. Cette méthode assure une stratégie fiable pour établir des itinéraires optimaux entre les nœuds du réseau, ce qui garantit une transmission continue des messages [9].

Il existe deux types de routages :

— **Routage statique :** consiste en la configuration manuelle de routes par l'administrateurréseau afin de garantir la connectivité entre deux équipements quelconques du réseau.
— **Routage dynamique :** est quant à lui automatisé et confié à un protocole qui se charge dedécouvrir les routes et de mettre à jour les tables de routage en conséquence.

I.3 La Sécurité informatique

I.3.1 La définition de la sécurité informatique

Fait référence à l'ensemble des mesures et des pratiques mises en place pour réduire la vulnérabilité d'un système informatique contre les menaces, les attaques, les accès non autorisés et les dommages potentiels. Il convient d'identifier les exigences de base de la sécurité informatique, elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité [4].

I.3.2 Objectif de la Sécurité

La sécurité informatique vise généralement à protéger les informations contre toutes divulgation, altération ou destruction, alors on peut sélectionner ces principaux objectifs de la sécurité d'un réseau [10] :

- **Authentification :** Assure l'identité d'un utilisateur, c'est á dire de garantir á chacun de correspondants que son partenaire est bien celui qu'il croit être.
- **Confidentialité :** Consiste à conserver des informations à l'abri de ceux qui ne sont pas autorisés à les connaitre.
- **Intégrité :** Lors des transferts, vérifier l'intégrité c'est assurer qu`aucune modification n'a eu lieu entre l'émetteur et le destinataire.
- **Disponibilité : L'accès** aux ressources du système doit être permanant et sans faille durant les plages d'utilisation prévues. Les services et les ressources sont accessibles rapidement et régulièrement.
- **Non répudiation :** C'est la propriété qui assure la preuve de l'authenticité d'un acte, c'est-à-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

I.3.3 Menace contre la Sécurité des Réseaux

De mauvaises habitudes lors de la configuration des aspects suivants d'un réseau peuvent augmenter le risque d'attaques [11] :

- **Architectures fragiles** : un réseau local ouvert et fiable est un point d'entrée essentiel pourles intrus. Un réseau mal configuré rend l'ensemble du réseau vulnérable aux attaques.
- **Réseaux de diffusion** : un matériel qui utilise le principe de diffusion. Lorsqu'un nœud transmet des données à un autre nœud, le routeur ou le commutateur envoie les paquets de données jusqu'à ce que le second nœud les traite.
- **Serveurs centralisés** : Les entreprises ont tendance à regrouper leurs services sur une seule machine puissante pour des raisons de rentabilité, mais cela peut présenter un risque important pour le réseau en raison du point de défaillance unique que constitue le serveur central. En effet, une compromission de ce dernier peut rendre le réseau inutilisable ou le rendre vulnérable aux manipulations et vols de données, le serveur central devenant alors une porte d'entrée pour accéder à l'ensemble du réseau.

I.3.4 Les attaques informatiques

I.3.4.1 Définition d'une Attaque

Une attaque peut être définie comme tout l'ensemble d'actions visant à exploiter une ou plusieurs vulnérabilités du système, et elle représente la concrétisation d'une menace [12].

I.3.4.2 But d'Attaque

Voici quelque but d'attaque [12] :

- Troubler le bon fonctionnement d'un service (déni de service) : Empêcher l'accès àune ressource ou prendre le contrôle d'une ressource.
- Utiliser les ressources d'un système (ex : bonne bande passante).
- Récupérer de l'information.
- Utiliser le système compromis pour attaquer un autre (rebondir).
- Obtenir un accès au système

I.3.4.3 Types d'Attaque

On distingue deux effets d'attaque qui sont les attaques passive et active [13] :

- **Attaque Passive**

Les attaques passives se limitent à écouter et analyser le trafic échangé. Ce type d'attaque est plus facile à réaliser (il suffit d'avoir le bon récepteur) et plus difficile à détecter, car l'intrus ne modifie pas les informations échangées. L'intention de l'intrus peut être la connaissance de l'information confidentielle des utilisateurs ou bien la connaissance des nœuds importants le réseau, en analysant les informations de routage, pour se préparer à une attaque active.

- **Attaque Active**

Une attaque active est une attaque informatique qui implique une modification des données ou une perturbation du fonctionnement normal du système ciblé. Les attaques actives sont plus complexes à mettre en œuvre que les attaques passives, car elles nécessitent souvent une compréhension plus approfondie du système ciblé. Les intentions de l'attaquant dans une attaque active peuvent être variées, telles que la prise de contrôle d'un système, le vol d'informations sensibles, la perturbation du service ou l'extorsion de fonds. Les attaques actives peuvent être menées à partir de l'intérieur ou de l'extérieur du système cible et peuvent prendre plusieurs formes.

I.3.4.4 Exemples d'attaque

- **Malware**

Un malware est un programme malveillant conçu pour causer des dommages, il peut infecter diverstypes de systèmes informatiques tels que des ordinateurs, des serveurs, des smartphones, des équipements réseau et des objets connectés. Cette attaque est considérée comme une attaque active [10].

Il existe plusieurs types de malwares dont les principaux sont les suivant :

— **Le virus :** un virus est un programme d'ordinateur capable d'infecter un autre programmed'ordinateur en le modifiant de façon á ce qu'il puisse á son tour se reproduire.

— **Le ver :** un ver est une catégorie de virus qui est un programme qui peut s'auto-reproduireet de se propager en utilisant les mécanismes réseaux.

— **Le Spyware :** un programme permet un espionnage sur les activités des utilisateurs et l'envoie des rapports aux adresse ou url spécifiés.

— **Le Hijacker** : un individu malintentionné qui utilise des techniques de piratage pour altérerles configurations du navigateur de sa cible et la diriger vers des pages.

- **Attaque d'accès**

Ces attaques ont pour but de récupérer des informations confidentielles, permettant à une personne d'accéder à des données auxquelles elle n'est pas autorisée à consulter. L'attaque d'accès n'est ni exclusivement passive ni exclusivement active, car elle peut impliquer à la fois des actions passives et actives [14].

On a plusieurs exemples d'attaque d'accès parmi eux :

— **Attaque par dictionnaire** : L'outil utilisé pour mener cette attaque utilise tous les mots depasse d'un dictionnaire.

— **Attaque par force brute :** elle permet de tester toutes les combinaisons possibles pour trouver le mot de passe.

— **Attaque Man in the Middle :** L'objectif principal de cette attaque est d'intercepter le trafic entre deux machines afin de pouvoir modifier, détruire ou espionner les données transmises pendant la communication.

- **Attaque par déni de service**

Ce sont des attaques dont le but est de rendre une machine, un réseau ou un service indisponible.Voici quelques attaques permettant de rendre le service indisponible [14] :

— **Attaque par réflexion (Smurf)** : Le pirate envoie un paquet ping (requêtes ICMP ECHO) en diffusion avec l'adresse IP de la victime, cette machine cible va recevoir un grand nombre de réponses et ainsi elle va se paralyser.

— **Attaque par fragmentation :** Est une attaque par saturation exploitant le principe de fragmentation du protocole IP. Elle consiste à bombarder une machine de requêtes afin qu'elle soit incapable de répondre aux requêtes réelles. Deux types d'attaques sur les fragments IP peuvent être distingués : Fragments Overlapping et Tiny Fragments.

— **Attaque SYN Flooding :** Est une méthode utilisée pour submerger un système cible en envoyant un grand nombre de demandes de connexion SYN au protocole TCP. Elle exploite le mécanisme de la poignée de main en trois temps du protocole TCP. L'attaquant envoie une multitude de demandes SYN sans répondre aux réponses SYN-ACK reçues, laissant ainsi les connexions en attente. Ces connexions en attente occupent des ressources mémoire du système, conduisant éventuellement à une saturation des ressources et à une impossibilité de traiter de nouvelles demandes légitimes (voir figure I.4).

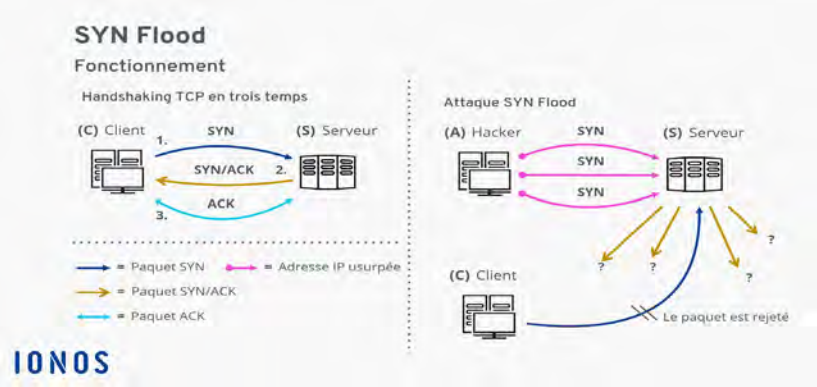


FIGURE I.4 - Attaque par SYN Flooding.

I.3.5 Mécanismes de Sécurités

- **L'Antivirus**

Un antivirus est un logiciel qui a pour but de détecter et d'éradiquer les codes malicieux présents dans un PC, et de prendre des mesures pour les empêcher de nuire. Les logiciels antivirus peuvents'installer en deux sortes d'endroits : Soit à l'entrée d'un réseau local, soit sur le poste de travail de l'utilisateur Son mode de fonctionnement est soit statique ou dynamique [12].

- **Proxy**

Proxy est un serveur intermédiaire qui agit en tant qu'intermédiaire entre un client et un serveur. Lorsqu'un client envoie une demande à travers un proxy, celui-ci transmet la demande au serveur cible au nom du client, et renvoie la réponse du serveur au client, les utilisations les plus courantes du proxy sont : l'anonymat, le contournement de restrictions, la mise en cache, filtrage du contenu, répartition de charge…etc. [15].

- **Certificat numérique**

Une personne Bob, qui veut permettre à d'autres personnes de communiquer avec lui de façon sécurisée, se rend auprès de la CA muni de sa clé publique et de sa carte d'identité et demande à être certifier, Le CA lui délivre alors un certificat et signe son hachage avec la clé privée de cet organisme [12].

- **IDS (system de détection d'intrusion)**

Les systèmes de détection d'intrusion (IDS) surveillent en continu le trafic réseau autour du pare- feu pour détecter toute activité suspecte. Si une attaque est détectée, l'IDS avertit l'administrateur pour une intervention manuelle sur le pare-feu, ou bien configure automatiquement celui-ci pour mettre en place des filtres de blocage nécessaires pour contrer l'attaque [16].

- **IPS (system de prévention d'intrusion)**

Est un outil de sécurité des systèmes d'information conçu pour protéger contre les intrusions atténuant les conséquences d'une attaque. Contrairement à un IDS passif, l'IPS agit activement en empêchant toute activité suspecte détectée au sein du système [16].

I.4 Conclusion

Dans ce chapitre, nous avons défini les notions fondamentales de réseau et sécurité informatique et décrit ses différentes fonctionnalités. Le chapitre suivant sera consacré à la présentation de l'organisme d'accueil Général Emballage et l'étude et l'analyse approfondie de son réseau.

ChapitreII. Présentions de l'organisme d'accueil

II.1 Introduction

Ce chapitre sera réservé à la présentation du Général emballage où nous effectuons notre stage, Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecteur réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

II.2 Première partie : Présentions de l'entreprise « Général Emballage »

II.2.1 Création et évolution

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 réalise des post-impressions en haute résolution jusqu'à 6 couleurs avec vernis intégral ou sélectif.

Leurs équipes maîtrisent l'ensemble des tâches de production :

- Etudes.
- 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 plus de 1200 employés et un chiffre d'affaires de 19 milliards DZD. Général Emballage est certifié conforme au système de management intégré Qualité-Santé et Sécurité au travail (S&ST) - Environnement (ISO 9001 :2015, ISO 14001 :2015, ISO 45001 :2018).

Son siège social est à ZAC Taherachet, Akbou, dans la wilaya (gouvernorat) de Béjaia.

RC N° : 06/00-0183268 B 00 du 09/01/2017

NIF : 000006018326879

Article d'imposition : 06256000300NIS: 099806250344426

II.2.2 Localisation de l'entreprise

FIGURE II.1 - Localisation de l'entreprise Général Emballage.

II.2.3 Fiche technique

Le tableau 1 ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude.

Dénomination	**Général Emballage**
Logo	GENERAL EMBALLAGE
Siège	Usine d'**Akbou** · ZAC de Taherachet, BP 63E **Akbou** 06001, Bejaia – Algérie ·
Secteurs d'activités	Emballage en carton ondulé et compact.
Numéros de Téléphone	034 19 61 90
Email	commercial@generalemballage.com
Site Internet	https://www.generalemballage.com

TABLE II.1 - dentification sur Général Emballage.

II.2.4 HISTORIQUE de Général E 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. 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 2006.
  - Le capital est porté à 150 millions de dinars.
  - Effectif : 318 employés.

- **En 2007 :**

  - Le capital est porté à 1,23 milliards de dinars.
  - Entrée en production de l'usine de Sétif.
  - Effectif : 425 employés.
  - Trophée de la Production (Euro-Développement PME).

- **En 2008**

  - Début d'exportation vers la Tunisie.
  - Entrée en exploitation de l'unité d'Oran.

- **En 2009 :**

  - 03 Juin : Augmentation du capital à 2 milliards de DA et entrée de MAGHPRIVATE EQUITY FUND II « Cyprus II » (MPEF II) avec une participation de 40%. Général Emballage devient une société de capitaux (Société par actions).
  - Effectif : 597 employés.

- **En 2010 :**

  - Effectif : 630 employés.

- **En 2011 :**

  - Effectif : 699 employés.

- Novembre : Cotation COFACE « @@@ ».

➢ **En 2012 :**

- Mars : Les capacités de production sont portées à 130.000 tonnes.
- Juin : L'usine d'Oran est transférée à la ZI Hassi-Ameur.
- Juin : Production des premiers ouvrages en Haute résolution.
- Juillet 02 : Signature d'une Convention cadre de partenariat avec l'Université de Béjaia.
- Décembre 17 : Notation COFACE « @@@ ».
- Effectif : 830 employés.

➢ **En 2013 :**

- Effectif : 960.
- Janvier 23 : Certification ISO 9001 :2008.
- Octobre 8 : Démarrage de la 1ère promotion de Licence en Emballage & Qualité à l'Université de Béjaia.

➢ **En 2014 :**

- Effectif : 1005.
- Février 22 : Signature d'un protocole d'accord de recrutement avec l'Agence Nationale de l'Emploi (ANEM).
- Octobre 30 : Début des exportations vers la Libye 2015.
- Effectif : 1100 o Avril : Entrée en production de la nouvelle usine de Sétif à ZI Ain Sfiha.
- Juin 02 : Prix d'encouragement du Trophée Export 2014 (World Trade Center (WTCA).

➢ **En 2016 :**

- Février : 1ere exportation en Espagne.
- Août : 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% du capital social.

- Septembre : 1ere exportation en Mauritanie Effectif : 1170.

- **En 2017 :**
  - Effectif : 1200.
  - Avril 19 : Notation COFACE @@@.
- **En 2018 :**
  - Effectif : 1200.
  - Avril 09 : Certification ISO 9001 Version 2015.
  - Juillet 29 : Notation COFACE @@@.
- **En 2019 :**
  - Effectif : 1201
  - Janvier 16 : Distinguée comme entreprise « inspirante » pour l'Afrique dans le Rapport « Compagnies to inspire African. 2019 » du London Stock Exchange Group (Bourse de Londres).
  - Avril 21 : Première expédition sur la Belgique.
  - Juin 13 : Prix spécial du jury du Trophée Export 2018 (World Trade Center (WTCA).
  - Juin 19 : Première exportation sur la France.
  - Juillet 25 : Notation COFACE @@@.
- **En 2020 :**
  - Effectif : 1222.
  - Janvier 25 : Certifications ISO 14001 :2015 et ISO 45001 :2018.
  - Juillet 23 : Notation COFACE @@@.

II.2.5 Evolution des effectifs par catégorie socioprofessionnelle :

UNITE	CADRE	MAITRISE	EXECUTION	TOTAL
GE DG	39	39	65	143
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%	69,19%	

FIGURE II.2 - Evolution des effectifs par catégorie.

II.2.6 Organigramme général de l'organisme d'accueil

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du Général Emballage dans lequel cet apprentissage termine le stage (voir figure II. 3) :

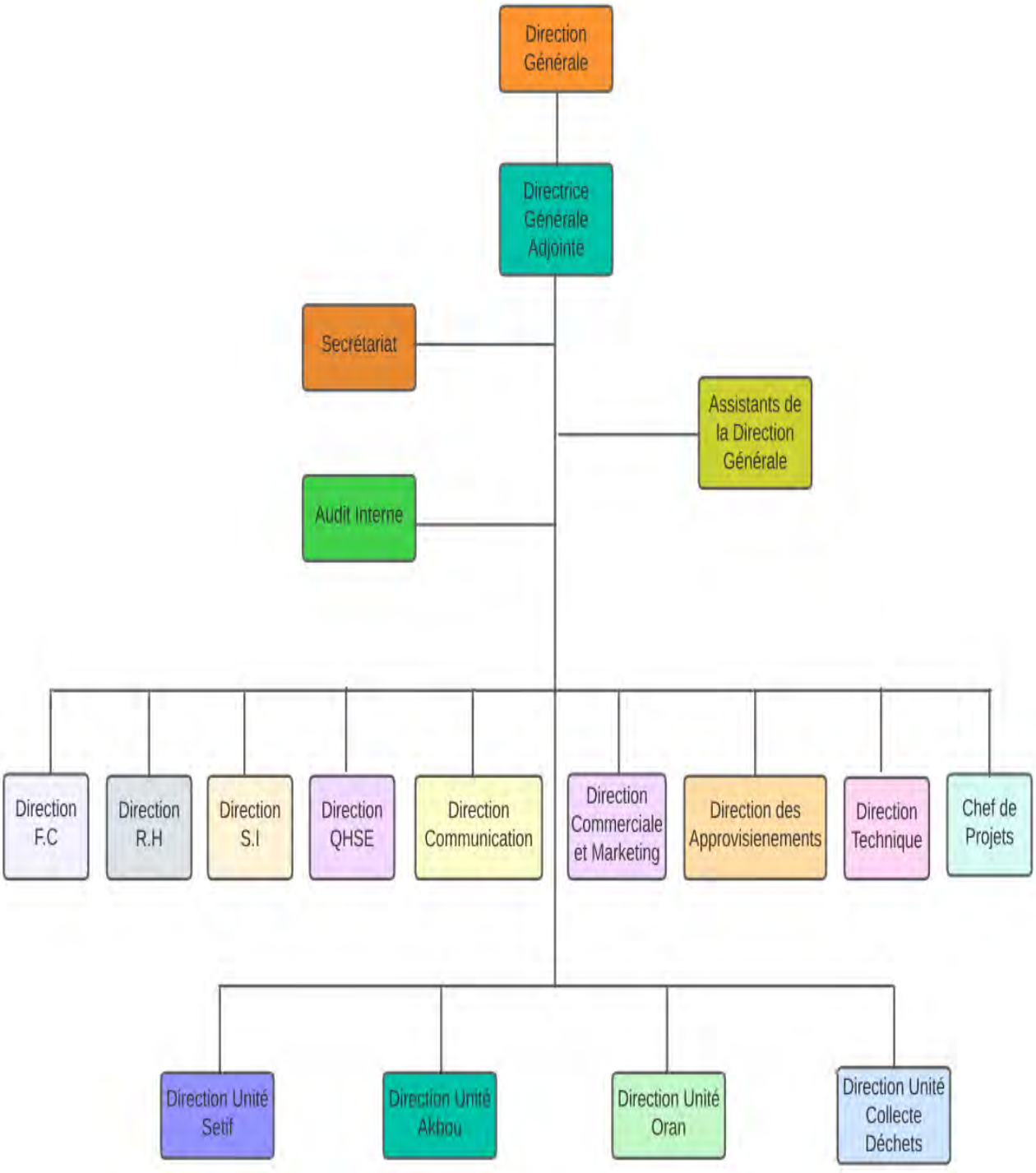


FIGURE II-3 - L'organigramme de Général Emballage.

La direction Générale :
Elle veille à l'élaboration de la politique générale de la société. Elle est chargée de coordonner et de contrôler les principales structures de la société, Ainsi que le suivi des budgets et les plans de développements.

La direction commerciale (Marketing) :
Elle assure le suivi des commandes clients et exprime les besoins de formation de chaque agent de la fonction vente. Elle étudie et suit l'évolution et les tendances des marchés et recherches de nouveaux segments de marchés et définie toutes conditions pour les satisfaire, fidéliser des nouveaux clients et posséder au recouvrement des créances.

La direction Finance et comptabilité :
Elle aide à définir les principaux objectifs de la société et veille à exécution de la politique financière de la société.

La direction de qualité et développement R.H :
La gestion des ressources humaines est la fonction organisationnelle qui s'occupe de recrutement, de la gestion, de perfectionnement et de la motivation du personnel, y compris de fournir du soutien et des système fonctionnel et spécialisé pour favoriser la participation des normes liées à l'emploi et aux droits de la personne.

La direction d'approvisionnement :
Elle assure la mission d'achat des matières nécessaires, elle assure aussi la mission de gestion des stocks des matières premières.

La direction Technique :
Elle assure le pilotage de la structure technique sous tous ses aspects : technique, production, maintenance et elle supervise l'activité de la maintenance.

La direction QHSE :
La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que : les actions de prévention des risques professionnels et de la pénibilité au travail, la mise en place d'une organisation et de moyens adaptés.

La direction de communication :
Chargé de gérer et de coordonner toutes les activités de communication interne est externe de l'entreprise, ses principales responsabilités comprennent : la stratégie de communication, les relations publiques, la communication interne, la communication de crise, le marketing et la publicité.

La direction de Service Informatique :
Elle est responsable de la gestion et de la maintenance des systèmes informatique et de l'entreprise, ses principales responsabilités comprennent : la gestion du réseau informatique, la maintenance des logiciels, la sécurité informatique, la gestion des données, et l'assistances informatique.

II.2.7 Organigramme de service d'accueil

Notre étude se focalise au niveau du Générale Emballage d'AKBOU dont nous avons effectué notre stage, dans le service de réseau informatique (voir figure II.4).

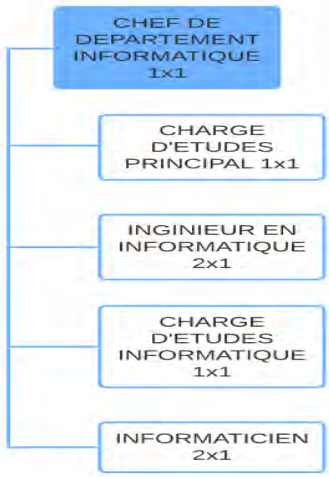


FIGURE II.4 - organigrammes de service d'accueil.

La description :
Chef de département informatique : est responsable de la direction stratégique de la gestion de l'équipe professionnels de l'informatique de l'entreprise. Il doit être capable de travailler en collaboration avec les autres départements d'entreprise pour granitaires que le système répond aux besoins de l'entreprise.
Charge d'études principale :il est responsable de la conception et de la mise en œuvre de solution informatique pour l'entreprise, parmi ses tâches principales : analyse des besoins, conception de solution, gestion de projets, développement de logiciel et fournir un support technique pour résoudre les problèmes.
Ingénieur en informatique :il est spécialisé dans la conception, le développement, la mise en ouvre de la maintenance des systèmes informatiques pour l'entreprise, il garantit que ces derniers sont efficaces et sécurisés.
Charge d'étude informatique : travaille sous la direction d'une charge d'étude principale ou d'un ingénieur en informatique pour les aidée dans leurs taches ces principales responsabilité incluent : la réalisation d'études techniques, le développement de logiciel et d'application, les tests et validation.
Informaticiens : il est responsable de développement, réalisation, intégration, installation et maintenance des systèmes et application informatique, il s'occupe aussi du matériel et des logiciels de ordinateurs individuels ou relies à un réseau ainsi que des systèmes de saisies de données, de transmission et de commandes de processus.

II.3 Deuxième Partie : Etat des lieux

II.3.1 Présentation du réseau Général Emballage :

Général Emballage dispose une architecture en couches (Core, Distribution et Access) et un réseau interne assez vaste permettant d'assurer la communication entre ses différents services, elle connecte son WAN à une connexion ADSL fournie par un fournisseur d'accès Internet, Par la segmentation de son LAN avec des Vlan configurés par Fortigate, Le réseau est composé de plusieurs équipements nous citons :

- 07 Serveurs Physique (Dell Power Edge R730, R740. . .).
- 200 Ordinateurs.
- 02 Firewalls Fortigate (Fortinet) en redondance.
- 25 Switchs CISCO (2960, 3750. . .).

Le schéma ci-dessous nous montre l'infrastructure du réseau Général Emballage (figure 5).

A. Présentation de l'infrastructure réseau existante dans l'entreprise :

Général Emballage construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustré dans la figure suivante :

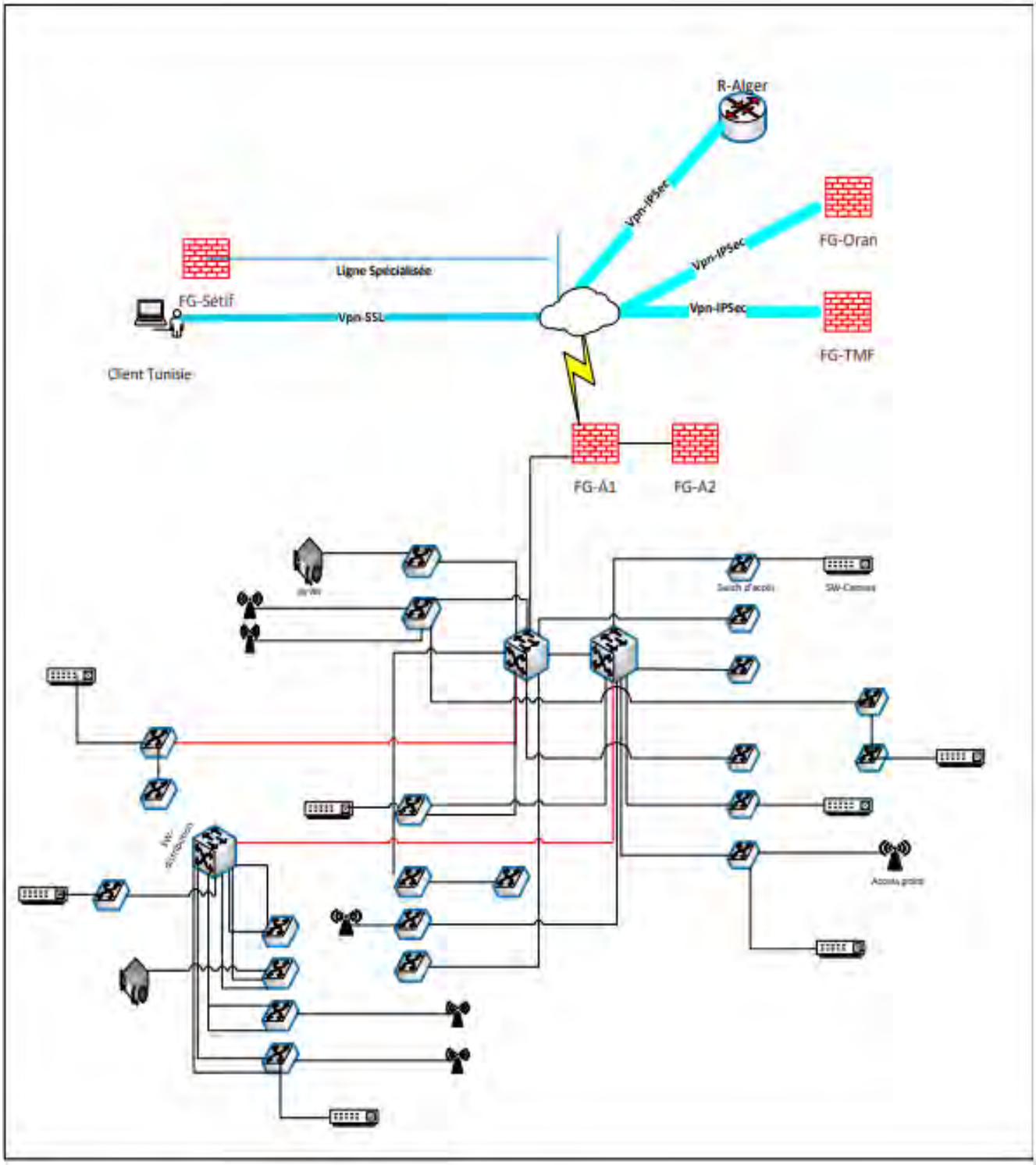


FIGURE II.5 - Architecture de réseau Général Emballage.

B. 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 Unit), 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**

Le serveur c'est un équipement 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'authentification et du contrôle.

— 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 câblage, elle utilise :

• La fibre optique.

• Des connecteurs RJ45.

— Armoire de brassage : BAIE informatique.

— Tiroir optique coulissant 19 pouces.

- **Equipements logiques**

— Systèmes d'Exploitation Windows et Linux.

— Systèmes 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 le routeur.

— Les pare feu.

— Le standard téléphonique

C. Analyse de l'existant

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

Question	Réponse
Quel le pare-feu utilisé dans votre entreprise pour assurer la sécurité du réseau ?	Fortigate
Pourquoi Fortigate ?	Il répond aux besoins de l'entreprise
Pourquoi vous avez configurer une LS (ligne spécialisée) Algérie télécom de Akbou à Sétif ?	Pour garantir une connexion rapide et stable. Assurer la sécurité de leurs communications. Éviter toute interruption de service
Quel est le type de vlan utilisée au sein de votre entreprise ?	Département **Service** Sous réseau
Le type de supervision ?	**Utilisateur** Administrateur
Votre entreprise utilise elle un type quelconque connexion de par ligne fixe à internet ?	**ADSL** FTTH (fibre optique) 4G
Quelles sont les mesures de sauvegarde et de récupération en cas de défaillance ou d'autre incident ?	Basculement physique entre le firewall
Existe-t-il un plan réseau ?	Non Oui mais pas mis à jour Oui tout le réseau et mis à jour Régulièrement
	Non

Les deux pares-feux sont-ils directement liés à internet ?	**Un seul** Les deux
Les serveurs et autres appareils sont-ils dans des locaux sécurisés ?	Non **Peu** Oui
Avez-vous déjà fait évaluer la sécurité du système informatique de votre entreprise par une entreprise externe à travers un audit de sécurité (examen méthodique) ?	Non Une fois **Régulièrement**
Votre matériel informatique fixe et portable est-il équipé de logiciels de sécurité (antivirus, firewall, etc.) ?	Non Matériel portable **Matériel fixe et portable**
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 Rarement **Systématiquement**

TABLE II.2 - Questionnaire sur l'analyse de l'existant.

II.4 Troisième partie : Problématiques et Solutions proposées

Problématiques

Lors de notre stage à Akbou Général Emballage, nous avons constaté qu'il dispose d'un réseau local de diverses plates-formes, de différents services, nous avons été en mesure de détecter des problèmes de réseau, tel que :

- Basculement physique des liens de connexion sur les firewalls.
- Divers problèmes rencontrés dans la haute disponibilité
- Problème de détection des pannes.
- Mauvaise configuration des accées à distances.
- Politiques de filtrage sécurité aléatoire.

Solutions

Le principal défi d'une architecture de réseau sécurisée est de pouvoir réguler l'accès aux ressources réseau.
Tous ces problèmes cités auparavant constituent un obstacle pour l'entreprise qui peut affecter son réseau, Notre projet a pour but la mise en œuvre et la configuration d'un pare-feu au profit de l'entreprise, qui est perçue comme une nécessité dans la sécurité de son réseau. Cette solution permettra de pallier les différents problèmes cités. Pour cela, nous avons proposé différentes solutions :

- Mise en place d'un cluster.
- L'implémentation de l'infrastructure en se basant sur un modèle hiérarchique.
- Mise en place de la haute disponibilité d'équipement et liens.
- Proposition d'un autre type de tunneling.
- Contrôle et analyse du trafic réseau par la Configuration du système de filtrage Web et applicatif et l'implémentation d'un profil de sécurité.

II.5 Conclusion

Le premier point de ce chapitre est porté sur la présentation de la société "General Emballage", son historique depuis sa création, l'évolution de ses Effectifs, ses valeurs ainsi son plans réseau. Ensuite, en deuxième position vient l'état des lieux, à partir de là nous avons présenté l'infrastructure réseau de l'entreprise, et son étude détaille. Les solutions que nous avons proposées pour y remédier et même " des généralités sur les firewalls et les Vlans".

ChapitreIII. Etude et solution proposée

III.1 Introduction

Ce chapitre offre un aperçu sur l'architecture étudié, ou on va proposer des améliorations et des solutions aux faiblesses cités auparavant et répondre aux problèmes existés dans le chapitre précédent, afin d'avoir une sécurité robuste.

III.2 Première partie : Étude de l'architecture existante

III.2.1 Les Pares-feux

III.2.1.1 Définition d'un Pare-feu

Un pare-feu est un système logiciel ou matériel placé entre un réseau local (privé) et un réseau externe. Il a pour objectif de filtrer et de bloquer tout trafic non désiré qui tente de traverser la limite du pare-feu. Pour ce faire, un pare-feu doit respecter certaines recommandations tels que : la résistance aux attaques, l'unicité de point de passage entre deux réseaux et l'assurance d'application de la stratégie de contrôle d'accès de l'organisation [3].

III.2.1.2 Principe de Fonctionnements d'un Pare-feu

Principe de fonctionnement d'un pare-feu repose sur le filtrage des paquets, il comprend un ensemble de règles préétablies qui permettent [11] :

- De filtrer et autoriser la connexion que sous certaines conditions (adresse IP et port), avec la commande [Allow].
- De bloquer la connexion et empêcher toute intrusion dans le réseau à l'aide de commandes [Deny, Reject].
- De rejeter la demande de connexion sans avertir l'émetteur en utilisant la commande [drop].

III.2.1.3 Les Différentes catégories des Pares-feux

Les pares-feux ce sont des dispositifs de sécurité essentiels, sont classés en différentes catégories pour répondre aux besoins spécifiques des réseaux et des environnements [11] :

— **Le pare-feu Bridge**

Le pare-feu bridge inspecte le trafic réseau en analysant les trames Ethernet qui passent à travers lui, il peut filtrer et contrôler le trafic en se basant sur des critères tels que les adresses MAC source et destination. Son avantage est qu'il peut être transparent pour les dispositifs du réseau, car il ne modifie pas les adresses IP et ne nécessite pas de reconfiguration des dispositifs connectés ce qui permet la non perturbation du fonctionnement du réseau.

— **Le pare-feu traditionnel**

Le pare-feu traditionnel contrôle le trafic entrant et sortant d'un réseau en fonction de l'adresse IP source ou destination, Cependant, ces fonctionnalités peuvent présenter des limites dans la capacité à détecter et à bloquer les nouvelles cyberattaques. Il est recommandé de les compléter avec d'autres technologies de sécurité plus avancées pour assurer une protection plus robuste contre les menaces émergentes.

— **Le pare-feu UTM**

Le pare-feu UTM dispose d'un grand nombre d'outils permettant de protéger le réseau et de minimiser les éventuelles cyberattaques, particulièrement adaptés aux petites et moyennes entreprises (PME) car il permet de consolider plusieurs systèmes indépendants en un seul. Parmi les pares-feux UTM on site : Fortigate, Sophos UTM.

— **Le pare-feu Next génération**

Ce genre de pare-feu est constitué de divers composants, chacun fournissant des fonctionnalités distinctes, ce qui améliore la capacité de traitement et assure une continuité de fonctionnement en cas de défaillance d'un des services. Parmi les pares-feux de next génération les plus connus on trouve : ASA CISCO XG.

III.2.1.4 Présentation de Pare-feu Fortigate de Fortinet :

Le module pare-feu -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.
FortiOS de Fortinet implémente un module UTM (en français gestion unifiée des menaces) du pare-feu 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 [17] (voir figure III.1).

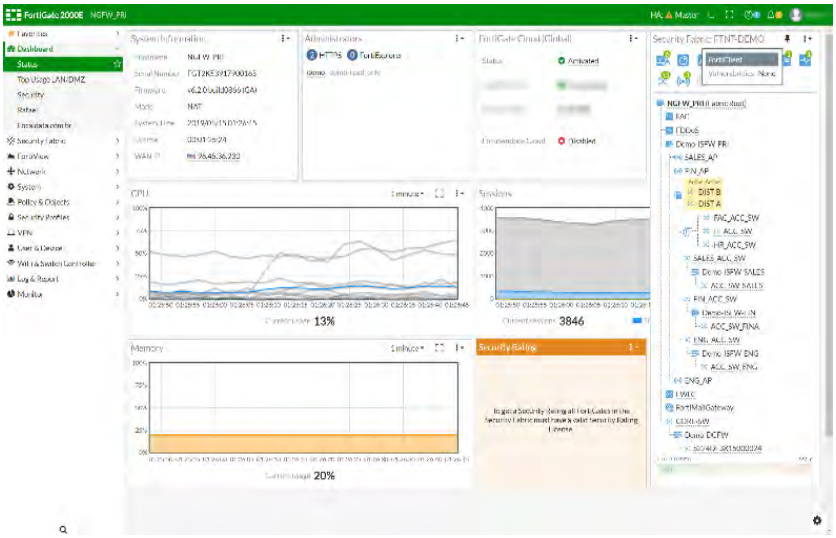


FIGURE III.1 - L'interface graphique du pare-feu Fortigate.

- **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.

III.2.2 Zone démilitarisée (DMZ)

Définition de la DMZ

En utilisant un pare-feu avec zone démilitarisée, les systèmes dans la DMZ peuvent être protégés de manière plus efficace. Le pare-feu est configuré pour permettre un accès limité aux systèmes de la DMZ, tout en bloquant l'accès direct au réseau interne. Cela crée une couche de sécurité supplémentaire en empêchant les attaquants d'accéder directement aux systèmes critiques du réseau interne [15] (voir Figure III.2).

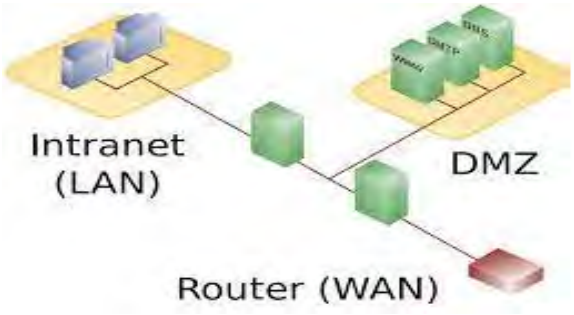


FIGURE III.2 - Fonctionnement de la DMZ.

— **Fonctionnement de la DMZ**

La zone démilitarisée s'appuie sur deux importantes zones qui sont les suivantes [18] :

La DMZ communautaire : est une configuration où plusieurs organisations ou entités partagent une même zone démilitarisée. Cela permet aux différentes entités de bénéficier d'une infrastructure commune tout en maintenant une isolation logique entre elles pour des raisons de sécurité et de confidentialité.

La DMZ isolée : est une configuration où une organisation dispose d'une zone démilitarisée dédiée exclusivement à ses propres services et ressources. Cela permet à l'organisation de bénéficier d'un niveau de contrôle et d'isolation supplémentaire pour ses systèmes sensibles ou stratégiques.

— **Serveurs installés sur la DMZ**

La DMZ permet de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles sur ces serveurs [19] :

- Les serveurs Web (http),
- Les serveurs de fichiers (ftp),
- Les serveurs d'e-mails (SMTP),
- Les serveurs de noms (DNS)

III.2.3 Les Vpns

Les réseaux privés virtuels, ou VPN (Virtual Private Networks), sont des connexions sécurisées et cryptées établies entre deux réseaux ou entre un utilisateur individuel et un réseau. Ils offrent la possibilité de protéger l'identité en ligne, en acheminant le trafic Internet à travers un tunnel chiffré qui empêche toute observation par des pirates informatiques, des gouvernements ou même votre fournisseur d'accès Internet [4] (voir figure III.3).

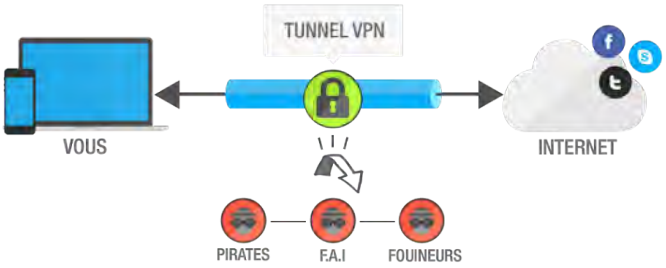


FIGURE III.3 - le Fonctionnement de VPN.

III.2.3.1 Les différents types de Vpn

Il existe 3 types standard d'utilisation des VPN [20] :

— Vpn client to site (Vpn d'accès)

Le VPN d'accès : est une solution qui permet aux utilisateurs distants d'accéder à un réseau privé en utilisant une connexion Internet. L'utilisateur se connecte au réseau privé via une connexion VPN sécurisée établie à travers Internet.

— Vpn site to site (L'intranet)

L'intranet VPN : est une solution utilisée pour connecter plusieurs intranets entre eux. C'est particulièrement utile pour les entreprises qui ont plusieurs sites distants. L'objectif principal de ce type de réseau est d'assurer la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (ex : base de données clients, informations financières, etc…).

— Vpn client to client (L'extranet)

L'extranet VPN : ce type de VPN, permet à une entreprise de communiquer avec ses clients et partenaires en ouvrant son réseau local à ces derniers. Dans ce contexte, il est essentiel que l'administrateur du VPN puisse surveiller les clients sur le réseau et gérer leurs droits d'accès. Cela garantit un contrôle approprié et sécurisé des connexions et des ressources partagées entre l'entreprise et ses partenaires

III.2.4 Les VLANs (Virtual local area network)

III.2.4.1 Définition des Réseau Virtuels

Un réseau local virtuel (VLAN) est un réseau logique de niveau 2 qui permet de regrouper des stations de travail de manière logique, même si elles ne sont pas physiquement proches les unes des autres. Par exemple, un logiciel développé pour le service financier ne concerne pas les personnes du département des ressources humaines. De la même manière, certaines ressources ne doivent pas être accessibles à tous les employés de l'entreprise. Les VLANs ont été normalisés selon la spécification IEEE 802.1Q, mais il peut y avoir des variations d'implémentation entre les fabricants de matériel [2] (voir figure III.4).

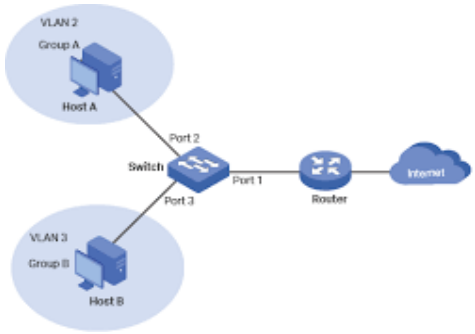


FIGURE III.4 - Le Fonctionnement des VLANs.

III.2.4.2 Les Intérêt des VlANs

Les Vlans présentent les intérêts suivants [21] :

- Diminuer le domaine de défusion (Broadcast).
- Peut couvrir tout un bâtiment, connecter plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN).
- Optimise la bande passante.
- Améliorer la gestion du réseau.
- Séparer les flux.
- Permettent de créer des groupes logiques isolés afin d'améliorer la sécurité.

III.2.4.3 Types des réseaux locaux virtuels (VLANs)

Il existe différents types de VLAN. Et chaque type est défini en fonction du type de trafic réseau qu'il porte ou de la fonction spécifique qu'il remplit. Voici une description des types de VLAN les plus courants [22].

— **VLAN de données**

Un VLAN de données, parfois appelé VLAN utilisateur, est créé pour transporter uniquement le trafic généré par les utilisateurs. La séparation des données utilisateur dans ce type de VLAN est importante pour assurer une gestion efficace du commutateur et un contrôle approprié.

— **VLAN par défaut**

Le VLAN par défaut est automatiquement assigné aux trames et aux ports lorsqu'aucune configuration spécifique n'est effectuée sur le matériel lors de la mise en place des VLAN. En général, le VLAN par défaut est le VLAN 1. Lors de la configuration des VLAN sur un équipement, au moins un VLAN doit être défini, d'où l'importance du VLAN par défaut.

— **VLAN natif**

Le VLAN natif est utilisé lorsqu'on associe des VLAN à des ports trunk. Il correspond au PVID (Port VLAN ID) sur un port trunk. Lorsqu'une trame non taguée arrive sur un port trunk, elle est attribuée à un VLAN en fonction du PVID du port. On dit alors qu'elle est associée au VLAN natif du port. Autrement dit, le VLAN natif identifie et surveille le trafic provenant des différentes extrémités du lien trunk.

— **VLAN de gestion (Management)**

Un VLAN de gestion est un VLAN spécialement configuré pour accéder aux fonctions de gestion d'un commutateur. Pour le configurer, en lui attribue une adresse IP et un masque de sous-réseau. Sur un commutateur VLAN, n'importe quel port peut être configuré comme port de gestion VLAN si aucune spécification VLAN est dédié à cet effet. Dans certains cas, un administrateur réseau peut proactivement définir le VLAN 1 comme VLAN de gestion, ce qui crée une option de secours pour empêcher toute connexion non autorisée à un commutateur.

— **VLAN voix**

Un VLAN voix est configurée pour transporter le trafic voix. Les réseaux virtuels vocaux sont principalement la priorité de transmission sur d'autres types de trafic réseau. La communication sur le réseau n'est pas complète sans des appels téléphoniques. Les appels sont plus effectués sur le réseau que les autres formes de transmission de message. L’envoi de courriers électroniques et des messages texte sont aussi des formes de l'interrelation, mais l'écoute d'une vraie voix donne de la légitimité et de l'assurance. Il est considéré parmi les administrateurs de réseau pour concevoir un réseau qui prenne en charge VOIP avec une bande passante assurée pour assurer la qualité de la voix, et la capacité d'être acheminés vers les zones congestionnées sur le réseau avec des retards minimes (150-180 millisecondes).

III.2.4.4 Protocoles de transport des VLANs

Voici quelques protocoles des réseaux locaux virtuels [22] :

- **Notion du TRUNK**.

Un trunk est une connexion physique unique sur laquelle on transmit le trafic de plusieurs réseaux virtuels, les trunks peuvent être utilisés :

— Entre deux commutateurs

C'est le mode de distribution des réseaux locaux le plus courant. C'est la solution du second problème énoncé.

— Entre un commutateur et un hôte

C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le Trunking a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.

— Entre un commutateur et un routeur

C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

- **La norme 802.1Q**

Le protocole IEEE 802.1Q est un protocole normalisé par L'IEEE (il fonctionne sur tous les équipements.). Il est de nos jours le protocole le plus utilisé pour faire du Trunking.

III.2.4.5 Protocoles de gestion des VLANs

- **Protocole VTP**

Afin d'éviter la nécessité de configurer tous les VLAN existants sur chaque commutateur, Cisco a créé un protocole appelé VTP (VLAN Trunking protocole). Ce protocole utilise la norme 802.1Q. Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [22]:

— Mode serveur : dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.

— Mode client VTP : dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.

— Mode transparent : dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

- **Protocole VMPS**

Est un service crée par Cisco, charger de faire une correspondre un vlan a une (ou plusieurs) Address Mac.

III.2.5 Les services

— **Service Active directory (AD)**

Est un service d'annuaire conçu pour les environnements Windows Server. Il fonctionne comme une base de données LDAP distribuée et hiérarchisée, permettant le partage d'informations relatives à l'infrastructure. Son rôle est de localiser, sécuriser, gérer et organiser les ressources telles que les ordinateurs, les utilisateurs, les groupes, les périphériques et les appareils réseau. AD fournit également des protocoles d'authentification et d'autorisation intégrés et évolutifs [17].

— **Service DNS (Domain Name System)**

Exécutés sur les contrôleurs de domaine ont la possibilité de stocker leurs zones dans les services de domaine Active Directory (AD DS). Cela élimine la nécessité de configurer une topologie de réplication DNS distincte utilisant des transferts de zone DNS traditionnels, car toutes les données de zone sont répliquées automatiquement via la réplication Active Directory [17].

— **Service DHCP (Dynamic Host Configuration Protocol)**

Le DHCP (Dynamic Host Configuration Protocol) est un protocole qui permet à un ordinateur connecté à un réseau local d'obtenir automatiquement sa configuration IP de manière dynamique. Son objectif principal est de simplifier l'administration d'un réseau. Bien que le protocole DHCP soit souvent considéré comme un distributeur d'adresses IP, il a été initialement conçu comme un complément au protocole BOOTP (Bootstrap Protocol), utilisé notamment lors de l'installation d'une machine à travers un réseau. Cette fonctionnalité est particulièrement utile pour la maintenance de grands parcs de machines. Les serveurs DHCP actuels prennent en charge IPv4 [23].

III.2.6 Filtrage Web et Filtrage Applicatif

- **Filtrage web**

Le filtrage Web est un outil permettant de contrôler le contenu accessible aux internautes. Avec la popularité croissante des applications web, il est essentiel de surveiller et de contrôler les accès à Internet pour garantir une gestion sécurisée des contenus, incluant l'antivirus, le filtrage Web et la sécurité des messages électroniques.

Le filtrage de niveau applicatif, également appelé proxy, s'effectue au niveau de l'application, soit la septième couche du modèle OSI [17].

- **Filtrage applicatif**

Le filtrage applicatif est une méthode de contrôle de sécurité informatique qui permet de réguler le trafic réseau en fonction des applications spécifiques utilisées par les utilisateurs, plutôt que des ports ou protocoles. Il permet de bloquer, autoriser ou limiter l'accès à certaines applications pour renforcer la sécurité du réseau et protéger les données sensibles [17].

III.3 Amélioration et solutions proposées

Après avoir analyser et traiter le réseau, nous allons proposer une amélioration de l'architecture par niveau pour répondre aux exigences spécifiques de l'entreprise afin d'avoir une infrastructure réseau robuste et adaptable par la mise en place d'une solution redondante qui se base sur la notion du HA (haute disponibilité) qui est de niveau quatre (couche transport) de Modèle OSI ,puis nous allons aussi proposer un système de tunneling GRE (Generic Routing encapsulation) de niveau trois (couche réseau) qui est le mieux adapté par rapport aux entreprises qui n'ont pas l'autorisation de chiffrer leurs données, ensuit nous mettant en œuvre un système d'authentification Radius de niveau deux (couche liaison de donnée) afin d'authentifier les utilisateurs.
Dans ce qui suit nous allons expliquer et détailler toutes les solutions proposées.

III.3.1 Première Solution : la Haute disponibilité (HA) d'équipements

Définition de HA :
La haute disponibilité est un terme couramment utilisé dans le domaine de l'informatique pour décrire une architecture système ou un service qui présente un taux de disponibilité adéquat. Il s'agit d'un élément essentiel de la plupart des réseaux, car tout le trafic y transite. Il fait référence à la capacité d'un system à fonctionner de manière continue et sans faille pendant une longue période, son principal objectif et de maintenir le réseau en état de fonctionnement 24H /24H en limitant la fréquence et la durée des interruptions [17].

Comment et assurer le HA entre les deux pares-feux dans notre solution :
Pour garantir une haute disponibilité de notre système, nous mettons en œuvre des mécanismes essentiels tels que le clustering, le basculement automatique :

— Clustering

Le clustering entre deux pares-feux est une méthode de configuration où deux pares-feux (ou plus) sont reliés pour travailler ensemble en tant qu'entité unique. Cette approche permet d'améliorer la redondance, la disponibilité et la fiabilité du pare-feu, en assurant une continuité de service même en cas de défaillance d'un des pares-feux.

- Configuration en cluster

Les deux pares-feux sont configurés en tant que cluster, où ils fonctionnent en parallèle et partagent une adresse IP virtuelle (VIP). Le VIP est l'adresse IP à la quelles le trafic réseau est dirigé.

- Synchronisation des états

Les pares-feux en cluster synchronisent en permanence leurs états de connexion et leurs règles de filtrage afin que les deux appareils aient une vue cohérente de c réseau. Cela garantit que les connexions établies ne sont pas interrompues lorsqu'un pare-feu bascule en mode actif ou passif.

— Basculement automatique

En cas de défaillance d'un pare-feu, le deuxième pare-feu prend automatiquement le relais et assume le rôle d'actif, sans interruption. Le basculement peut être déclenché par des mécanisme

de détection des pannes ou de surveillance, ou il peut être déclenché manuellement par administrateur réseau.

L'intérêt d'assurer le HA sur notre infrastructure :

En raison de problème de basculement physique entre les deux pares-feux , plusieurs inconvénients et risques se présentent : perte de données, temps d'arrêt prolongé, erreurs humaines, complexité de gestion, incohérence de configuration et perte de connexions actives, Afin de remédier à cela, nous proposons de mettre en place un clustering entre les deux pares-feux Fortigate avec basculement automatique et synchronisation des états qui offre une haute disponibilité, une continuité de service, une répartition de charge, une gestion simplifiée et une sécurité renforcée ce qui permet à l'entreprise de maintenir un réseau robuste et fiable.

III.3.2 Deuxième Solution : Tunneling GRE

Définition de GRE :

GRE (Generic Routing Encapsulation) c'est un protocole de tunneling qui permet d'acheminer des paquets de données d'un réseau à un autre. Il est utilisé pour créer des tunnels VPN (Virtual Private Network) ou des tunnels de communication entre des réseaux distants. Le protocole GRE peut également être utilisé pour encapsuler des protocoles de routage tels que OSPF et EIGRP, pour les faire passer à travers des réseaux qui ne prennent pas en charge ces protocoles [24].

La déférence entre les différents protocoles : IPSec vs GRE

Voici une comparaison entre IPSec (Internet Protocol Security) et GRE (Generic Routing Encapsulation) sous forme de tableau [24] :

	IPsec	**GRE**
Protocole	Protocole de sécurité utilisé pour établir des connexions VPN sécurisées	Protocole de tunneling utilisé pour encapsuler différents protocoles réseau
Sécurité	Offre une sécurité de bout en bout en chiffrant et authentifiant les données	Ne fournit pas de sécurité par lui-même, mais peut être utilisé en conjonction avec IPsec pour créer un tunnel sécurisé
Fonctionnement	Fonctionne au niveau du réseau (couche 3 du modèle OSI)	Fonctionne au niveau du réseau (couche 3 du modèle OSI)
Tunneling	Crée des tunnels VPN pour le transport sécurisé des données entre les sites distants	Crée des tunnels pour encapsuler des paquets de protocole réseau dans un autre réseau
Performance	Peut entraîner une légère surcharge en raison du chiffrement et de l'authentification	Aucune surcharge supplémentaire, car il ne fournit pas de sécurité directe

TABLE III.1- Comparaison entre IPSec et GRE.

L’intérêt d’utiliser le tunneling GRE sur notre infrastructure :
En proposant le tunneling GRE pour les entreprises qui n’ont pas une autorisation délivrée par l’ARPCE (Autorité de Régulation de la poste et des communications électroniques) pour chiffrer leurs données, de plus GRE dispose de deux tunnels prive (local) et publique où le NAT (Network Address translation) vers internet est assurer dans le tunnel priver pour ne pas perturber le tunnel public ce qu’est y n’est pas assuré dans le tunnel public de l’IPSec.

III.3.3 Troisième Solution : la haute disponibilité des liens

Définition d’équilibrage de charge :
Appelé aussi répartition de charge, est une méthode utilisée pour distribuer la charge de travail entre plusieurs ordinateurs d'un groupe. Son objectif est de répondre à une charge excessive en répartissant intelligemment le travail sur les équipements (switches, serveurs …etc) [25].

Comment est assurer le HA entre les deux switches dans notre solution :
Définition de protocole LACP

Il existe une spécification de l'IEEE qui permet de regrouper plusieurs ports physiques en un seul canal logique. Cette spécification est connue sous le nom de protocole de contrôle de l’agrégation des liens LACP, il permet à un commutateur de négocier un regroupement automatique en envoyant des paquets LACP à l'homologue. Les modes LACP sont on, LACP active et LACP passive.

L’intérêt d’utiliser la HA entre les deux switches :
En utilisant LACP cela permet :

- D’exploiter de manière flexible les ports de commutation en les regroupant pour former un groupe agrégé unique.
- Offre une redondance en considérant la liaison globale comme une seule connexion logique. En cas de perte d'une liaison physique au sein du groupe agrégé, la topologie du réseau n'est pas modifiée, ce qui garantit la continuité de la connectivité et minimise les interruptions potentielles. Cela permet d'améliorer la résilience du réseau en évitant les perturbations dues à la défaillance d'un lien individuel.

III.3.4 Quatrième Solution : Serveur d’authentification Radius

Définition de serveur d’authentification Radius :
Radius est un protocole utilisé pour authentifier les postes de travail sur les réseaux locaux, qu’ils Soient filaires ou sans fil. Le protocole Radius est un système client/serveur qui permet de sécuriser des réseaux contre des accès à distance non autorisé, il peut également configurer des stratégies et des certificats réseau pour autoriser les demandes de connexion et gérer la norme 802.1X pour vérifier l’authentification avant la connexion d’un ordinateur au réseau [15].

Comment est assurer l'authentification RADIUS dans notre solution :
Pour garantir l'authentification RADIUS de notre système, nous procédons comme suit :

- Configuration d'un serveur RADIUS dédié et sécurisé afin de suivre les meilleures pratiques de sécurité pour le système d'exploitation et le logiciel RADIUS.
- Configuration des équipements réseau (tels que les commutateurs, les routeurs) en tant que clients RADIUS pour assurer que les informations de configuration (adresse IP, clé partagée) sont correctes.
- Application des mesures de sécurité recommandées pour le serveur RADIUS lui-même, telles que la mise à jour régulière, la gestion des accès physiques, et la configuration des règles de pare-feu pour limiter les accès non autorisés.

L'intérêt d'utiliser Radius dans notre solution :

- L'utilisation d'un certificat Radius permet de demander à toute personne souhaitant se connecter au réseau de s'authentifier, il consiste à faire présenter un certificat électronique dont la validité sera vérifiée par le serveur.
- La méthode d'authentification par certificat est très fiable Radius permet de centraliser des données d'authentification.

III.4 Conclusion

Ce chapitre nous a permis de prendre connaissance des différents concepts et généralités, associés aux pares-feux, Vlan et aux VPN…etc, et de comprendre l'intérêt qu'ils y apportent, et nous avons introduit les solutions proposées.
Dans le chapitre suivant nous allons présenter les différentes configurations de notre infrastructure réseau proposée avec l'utilisation du simulateur GNS3 (Graphical Network Simulator), ainsi que les tests de validation de ces configurations.

ChapitreIV. Réalisation

IV.1 Introduction

Dans ce chapitre, nous allons mettre en œuvre l'architecture réseau de l'entreprise basée sur le pare-feu 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 résistant aux pannes. L'objectif est de sortir avec des connaissances suffisantes pour simuler des scénarios qu'on peut rencontrer dans la pratique et évaluer leurs faisabilités.

IV.2 Présentation d'outil de travail GNS3

Simulation et émulation

La simulation en général est une représentation fictive de la réalité. Elle revient 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.

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.

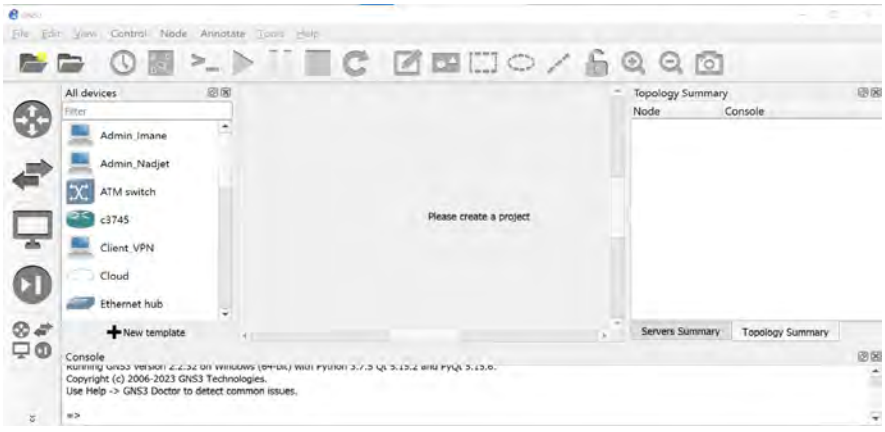


FIGURE IV.1 - L'interface graphique de GNS3.

IV.3 Présentation de notre infrastructure réseau réaliser

Dans notre projet nous allons emmener à faire l'amélioration de l'infrastructure de réseau en s'appuyant sur les principes d'un modèle hiérarchique, cas d'étude SPA Général emballage.
Notre infrastructure se compose de quatre sites qui se situe à Akbou, Oran, Tunisie et Alger : le site d'Akbou est constitué de trois couches qui sont la couche cœur et distribution et la couche d'accès qui représente respectivement les switches Cores 1et 2, et les switches d'accès.
Pour les sites distants on a le Vpn site à site (ORAN/AKBOU), on a un autre Vpn site à site (ALGER/AKBOU), et un autre Vpn client à site (AKBOU/TUNISIE).

L'architecture du réseau que nous avons créé est illustrer dans la topologie suivante :
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. Concernant le routeur qui se trouvant au niveau du site distant (Alger), nous l'avons mis en place afin de simuler un autre tunnel VPN. Concernant la machine cliente qui se trouvant au niveau du site distant (Tunisie), nous l'avons mis en place afin de d'accéder à distance au site d'Akbou par l'installation de Forticlient sur la machine afin d'accéder à l'interface graphique de nos différents pares-feux. Sur le serveur, nous avons créés un domaine nommer "ge.local", pour assurer la sécurité ,gérer les comptes et les utilisateurs (voir figure IV.2).

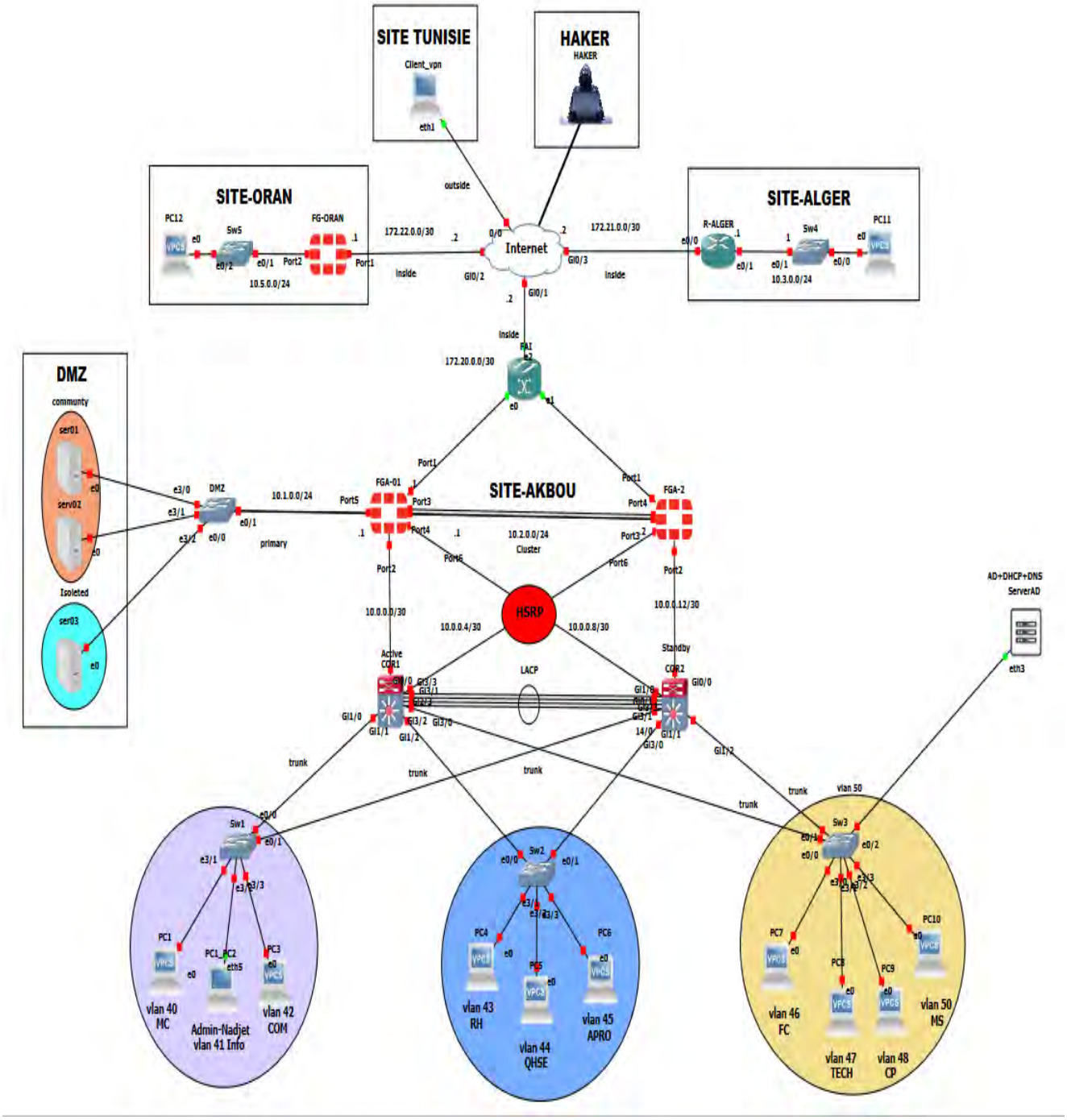


FIGURE IV.2 - L’infrastructure Réseau Proposée.

IV.4 Le diagramme qui représente notre Méthodologie de configuration

La Figure suivante représente les configurations réaliser sur GNS et la VM :

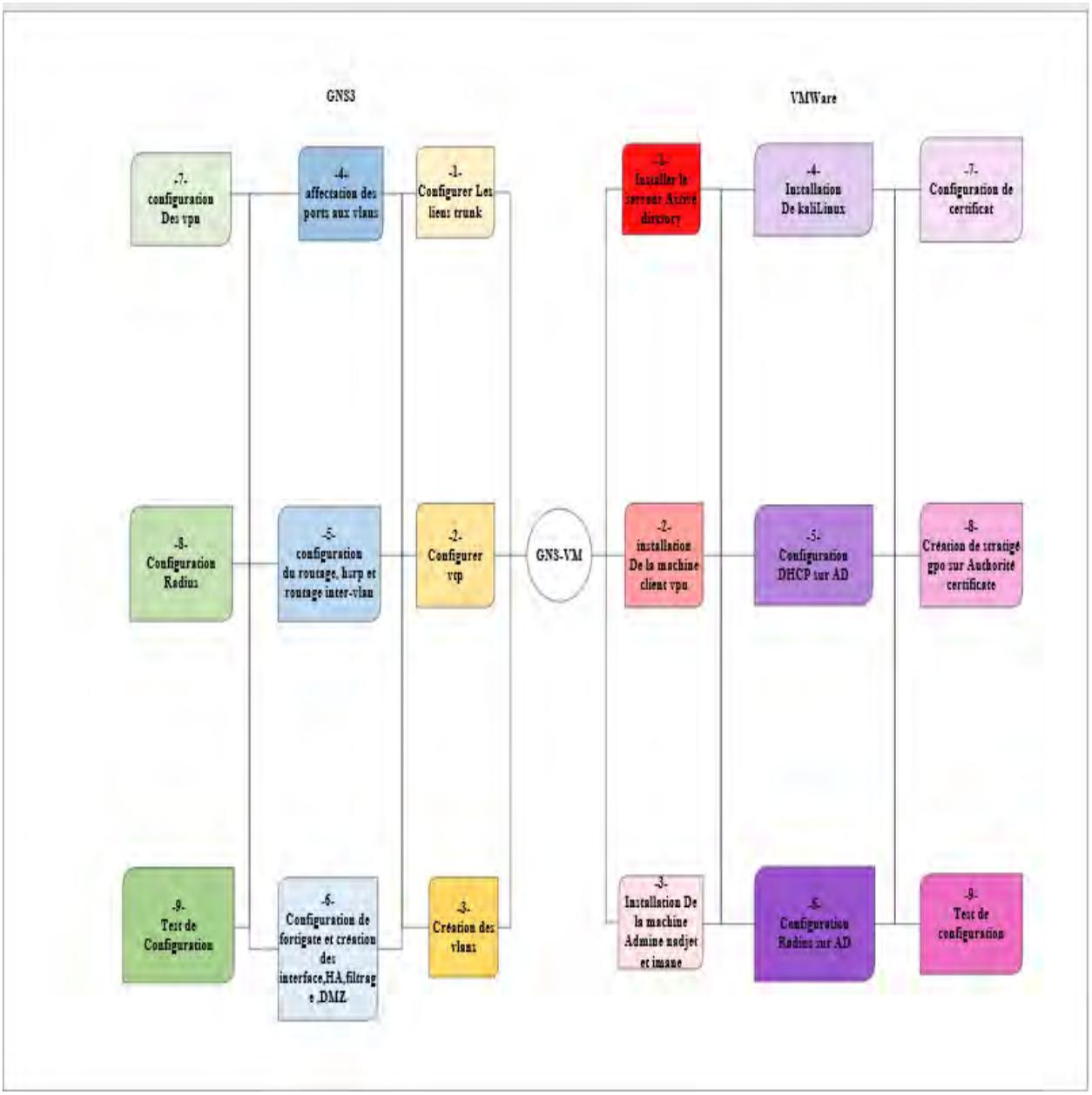


FIGURE IV.3 - la Méthodologie de la configuration.

IV.5 Nomination des VLAN

Le tableau suivant représente la liste des VLAN :

Nom de Vlan	ID Vlan	Default Gateway	Adresse IP	Masque
MC	40	192.168.40.1	192.168.40.0	255.255.255.0
INFO	41	192.168.41.1	192.168.41.0	255.255.255.0
COM	42	192.168.42.1	192.168.42.0	255.255.255.0
RH	43	192.168.43.1	192.168.43.0	255.255.255.0
QHSE	44	192.168.44.1	192.168.44.0	255.255.255.0
APPR	45	192.168.45.1	192.168.45.0	255.255.255.0
FC	46	192.168.46.1	192.168.46.0	255.255.255.0
TECH	47	192.168.47.1	192.168.47.0	255.255.255.0
CP	48	192.168.48.1	192.168.48.0	255.255.255.0
VOICE	49	192.168.49.1	192.168.49.0	255.255.255.0
MS	50	192.168.50.1	192.168.50.0	255.255.255.0

TABLE IV.1- Liste des VLANs.

IV.6 Le tableau d'adressage général

Le tableau suivant représente le tableau d'adressage général :

Les équipements	Les interfaces	L'@ IP/Masque	La passerelle
FGA-Oran (Version 7.0.12/ qemu).	Port1 Port2	172.23.0.1/30 10.5.0.1/24	/
R-Alger	Eth0/0 Eth0/1	172.21.0.1/30 10.3.0.1/24	10.11.12.2
Internet	Eth0/0 Eth1/0 Eth0/1 Eth0/3	192.168.189.130/24 172.20.0.2/30 172.22.0.2/30 172.21.0.2/30	/
FGA-1/ FGA-2 (Version 7.0.12/ qemu).	Port1 (WAN) Port2 (LAN1) Port3 (Cluster1) Port4 (Cluster2) Port5 (DMZ) Port6 (LAN2)	172.20.0.1/30 10.0.0.2/30 / / 10.1.0.1/24 10.0.0.10/30	/
COR1 (SW Cisco LOSvL2/ qemu)	Gi0/0 Gi2/3 Gi3/0-3 (Trunk)	10.0.0.1/30 10.0.0.5/30 /	/

COR2 (SW Cisco LOSvL2/ qemu)	Gi0/0 Gi2/3 Gi3/0-3 (Trunk)	10.0.0.13/30 10.0.0.9/30 /	/
Server	Eth3 (vlan 50)	192.168.50.100/24	192.168.50.1
PC1	Carte Réseau	192.168.40.250/24	192.168.40.1
PC2	Carte Réseau	192.168.41.250/24	192.168.41.1
PC3	Carte Réseau	192.168.42.250/24	192.168.42.1

TABLE IV.2- Tableau d’adressage général.

IV.7 La configuration de base

Configuration des liens Trunk

Nous allons configurer les liaisons entre ses commutateurs en mode trunk. La figure suivante illustre les configurations faites:

```
COR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR1(config)#$itEthernet 0/2-3, gigabitEthernet 2/3, gigabitEthernet 3/0-3
COR1(config-if-range)#switchport trunk encapsulation dot1q
COR1(config-if-range)#switchport mode  trunk
COR1(config-if-range)#end
```

```
COR2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR2(config)#$tethernet 3/0-3,gigabitethernet 1/0,gigabitethernet 0/2-3
COR2(config-if-range)#switchport trunk encapsulation dot1q
COR2(config-if-range)#switchport  mode trunk
COR2(config-if-range)#end
```

Configuration de VTP (Vlan Trunking Protocol)

Durant la phase de déploiement, nous allons configurer les switches cœur en mode 'VTP server' tandis que les autres switches (switches d'accès) seront configurés en mode 'VTP client'. Pour cela nous allons procéder comme suit :

Configuration du VTP serveur :

```
COR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR1(config)#vtp mode server
Device mode already VTP Server for VLANS.
COR1(config)#vtp domain ge.vtp
Domain name already set to ge.vtp.
COR1(config)#vtp password ge2023
Password already set to ge2023
COR1(config)#vtp version 2
VTP version is already in V2.
COR1(config)#vtp pruning
Pruning already switched on
COR1(config)#end
```

```
COR2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR2(config)#vtp mode server
Device mode already VTP Server for VLANS.
COR2(config)#vtp domain ge.vtp
Domain name already set to ge.vtp.
COR2(config)#vtp password ge2023
Password already set to ge2023
COR2(config)#vtp version 2
VTP version is already in V2.
COR2(config)#END
```

Configuration du VTP client :

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vtp mode client
Device mode already VTP Client for VLANS.
Sw1(config)#vtp domain ge.vtp
Domain name already set to ge.vtp.
Sw1(config)#vtp password ge2023
Password already set to ge2023
Sw1(config)#vtp versio 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
Sw1(config)#end
```

Création des vlans

La création des VLANs pour tous les services de l'entreprise est faite au niveau du commutateur Core1 qui va propager automatiquement aux autres switches reliés, elle est illustrée dans la figure suivante :

```
Core1(config)#Vlan 40
Core1(config-vlan)#NAME MC
Core1(config-vlan)#Vlan 41
Core1(config-vlan)#NAME Info
Core1(config-vlan)#Vlan 42
Core1(config-vlan)#NAME COM
Core1(config-vlan)#Vlan 43
Core1(config-vlan)#NAME RH
Core1(config-vlan)#Vlan 44
Core1(config-vlan)#NAME QHSE
Core1(config-vlan)#Vlan 45
Core1(config-vlan)#NAME APRO
Core1(config-vlan)#Vlan 46
Core1(config-vlan)#NAME FC
Core1(config-vlan)#Vlan 47
Core1(config-vlan)#NAME TECH
Core1(config-vlan)#Vlan 48
Core1(config-vlan)#NAME CP
Core1(config-vlan)#Vlan 50
Core1(config-vlan)#NAME MS
Core1(config-vlan)#Vlan 99
Core1(config-vlan)#NAME native
Core1(config-vlan)#end
```

Affectation des ports aux VLANs

Dans cette étape nous allons assigner des ports aux Vlans au niveau des switches d'accès avec les commandes citées dans la figure ci-dessous :

```
Sw1(config)#interface eth 0/2
Sw1(config-if)#switchport mode Access
Sw1(config-if)#switchport Access Vlan 40
Sw1(config-if)#EXIT
Sw1(config)#interface eth 0/3
Sw1(config-if)#switchport mode Access
Sw1(config-if)#switchport Access Vlan 41
Sw1(config-if)#EXIT
Sw1(config)#interface eth 1/0
Sw1(config-if)#switchport mode Access
Sw1(config-if)#switchport Access Vlan 42
```

Configuration du VLAN native

Le VLAN 99 dit VLAN native : nous avons configuré ce dernier sur tous les Switch de, la figure suivante montre comment configurer le VLAN native sur le Sw2:

```
Sw2(config)#interface rang eth 0/0-1
Sw2(config-if-range)#switchport trunk native vlan 99
Sw2(config-if-range)#switchport trunk allowed vlan 40-50,99
Sw2(config-if-range)#END
```

Configuration de haute disponibilité des liens entre les deux Switches cor par LACP
Dans l'architecture, nous avons opté pour une agrégation des liens gigabitethernet entre les deux switches de distribution Core1 et Core2, on a donc mis les ports gigabitethernet dans un groupe en précisant le mode Active comme la figure ci-dessous le montre :

```
COR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR1(config)#interface range gigabitethernet 3/0-3
COR1(config-if-range)#channel-group 30 MODE Active
COR1(config-if-range)#exit
COR1(config)#port-channel load-balance src-dst-mac
COR1(config)#end
```

Configuration du routage Inter-VLAN :
Pour configurer le routage Inter-VLAN il faut d'abord activer la fonction de routage des switches Cœurs et configuré un DHCP relay avec l'adresse du notre serveur DHCP, comme la figure ci-dessous le montre :

```
COR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR1(config)#ip routing
COR1(config)#interface vlan 40
COR1(config-if)#no shutdown
COR1(config-if)# ip address 192.168.40.1 255.255.255.0
COR1(config-if)#ip helper-address 192.168.50.100
COR1(config-if)#exit
```

```
COR2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR2(config)#ip routing
COR2(config)#interface vlan 40
COR2(config-if)#no shutdown
COR2(config-if)#ip address 192.168.40.2 255.255.255.0
COR2(config-if)#ip helper-address 192.168.50.100
COR2(config-if)#end
```

Configuration HSRP
Nous allons d'abord attribuer une adresses IP virtuel pour chaque vlan sur les deux switches de distribution Core1 et Core2, puis on définit une priorité « standby priority 150 » la plus élevée pour le commutateur Core1 et de la préemption « standby preempt » comme monter ci-dessus :

```
COR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR1(config)#interface vlan 40
COR1(config-if)#standby version 2
COR1(config-if)#standby 40 ip 192.168.40.250
COR1(config-if)#standby 40 priority 150
COR1(config-if)#standby 40 preempt
COR1(config-if)#end
COR1#wr
Building configuration...
```

```
COR2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR2(config)#interface vlan 40
COR2(config-if)#standby version 2
COR2(config-if)#standby 40 ip 192.168.40.250
COR2(config-if)#end
```

Configuration du routage

Nous allons tout d'abord convertir les ports de couche 2 en des ports de couche 3 et les faire fonctionner comme des interfaces de routeur, puis on attribue une adresse IP et un masque de réseau pour chacun des ports routés comme la figure ci-dessus montre

```
COR1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR1(config)#interface gigabitEthernet 0/0
COR1(config-if)#no switchport
COR1(config-if)#ip address 10.0.0.1 255.255.255.252
COR1(config-if)#no shutdown
COR1(config-if)#exit
COR1(config)#interface gigabitEthernet 2/3
COR1(config-if)#no switchport
COR1(config-if)#ip address 10.0.0.5 255.255.255.252
COR1(config-if)#no shutdown
COR1(config-if)#end
```

```
COR2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
COR2(config)#interface gigabitEthernet 2/3
COR2(config-if)#no switchport
COR2(config-if)#ip address 10.0.0.9 255.255.255.252
COR2(config-if)#no shutdown
COR2(config-if)#exit
COR2(config)#interface gigabitEthernet 0/0
COR2(config-if)#no switchport
COR2(config-if)#ip address 10.0.0.13 255.255.255.252
COR2(config-if)#no shutdown
COR2(config-if)#end
```

Ensuite nous allons créer deux routes statiques sur chaque switches distribution en utilisant l'adresse du prochain saut dont la métrique du deuxième chemin est à 2 comme on a procédé ci-dessus:

```
COR1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
COR1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.6 2
COR1(config)#end
```

```
COR2(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.10
COR2(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.14 2
COR2(config)#end
```

Configuration des interfaces de l'internet

Configuration de l'interface 0/0 outside qui aura une adresse DHCP fourni par le FAI :

```
Internet#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet(config)#interface gigabitethernet 0/0
Internet(config-if)#no shutdown
Internet(config-if)#ip address dhcp
Internet(config-if)#exit
```

Configuration des l'interfaces Inside 0/1, 0/2 et 0/3 vers les sites Akbou Oran Alger respectivement :

```
Internet(config)#interface gigabitethernet 0/1
Internet(config-if)#ip address 172.20.0.2 255.255.255.252
Internet(config-if)#no shutdown
Internet(config-if)#exit
Internet(config)#interface gigabitethernet 0/2
Internet(config-if)#ip address 172.22.0.2 255.255.255.252
Internet(config-if)#no shutdown
Internet(config-if)#exit
Internet(config)#interface gigabitethernet 0/3
Internet(config-if)#ip address 172.21.0.2 255.255.255.252
Internet(config-if)#no shutdown
Internet(config-if)#exit
```

IV.8 Pare-feu FortiGate de Fortinet

Importation de FortiGate sur « GNS3 » V 7.0.12

L'importation d'Appliance virtuelle Fortigate en utilisant L'émulateur de processeurs QEMU de GNS3, sur "New Template" ensuite "Create a new Version" pour créer une nouvelle version (7.0.12) puis spécifier les fichiers qui seront utilisés pour installer l'image logicielle, Maintenant téléchargerons cette version à partir du site de support Fortinet, par la suite on passe à l'étape de l'importation. (Voir figure IV.4)

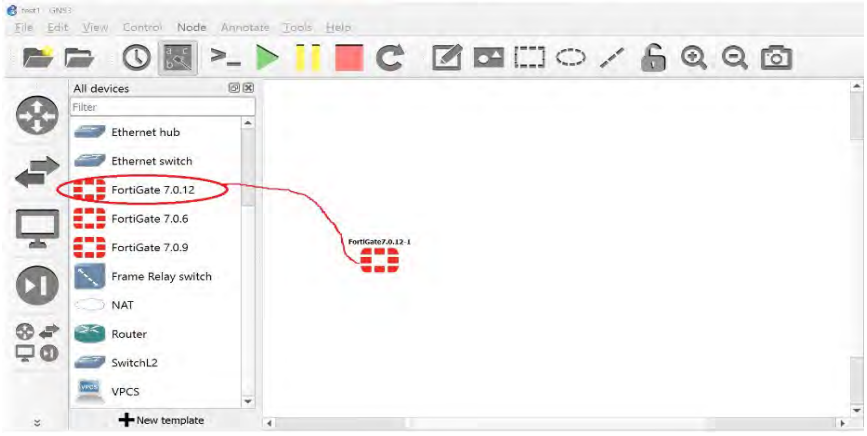


FIGURE IV.4 - Importation d'Appliance Fortigate 7.0.12 avec succès.

Configuration d'accès au FortiGate

ll nous reste plus qu'à configurer notre Pare-feu FortiGate, donc nous allons dans la configuration de l'interface , pour accéder à l'interface graphique. Grâce au navigateur (Google Chrome) on tape "10.0.0.2", On se connecte avec admin et un mot de passe 'Admin'. (Voir figure IV.5).

```
FGA-02 # config system interface

FGA-02 (interface) # edit port2

FGA-02 (port2) # set mode static

FGA-02 (port2) # set ip 10.0.0.2/30

FGA-02 (port2) # set allowaccess ping http https
```

FIGURE IV.5 - configuration de pare-feu.

IV.8.1 Configuration de HA la haute disponibilité Entre les deux pares-feux

Nous allons configurer la haute disponibilité (en anglais High Availability (HA)) active-active sur les deux pare-feu FortiGate. “FGA-01" agira en tant que maître (primary par priority) et "FGA-02" en tant qu’esclave. En cas d’erreur du maître l’esclave devient maître automatiquement c’est à dire qu’il devient lui primary et fonctionnera jusqu’à ce que le maître soit traité. Nous allons dans [Système] -> [HA], puis nous allons remplir les champs suivant (voir Figure) :

— En Mode : Nous avons choisi Actif-Actif.

— Priorité du pare-feu : Nous avons défini la priorité la plus élevé sur le maître (FGA-01), pare-feu avec une priorité inférieure sera l’esclave (FGA-0).

— Nom du groupe : Nous avons entré le nom du groupe "HA-Group1" sur les deux fortigates.

— Mot de passe : Nous avons défini le mot de passe pour authentifier les membres du "ge2023".

— 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 3 et le port 4).

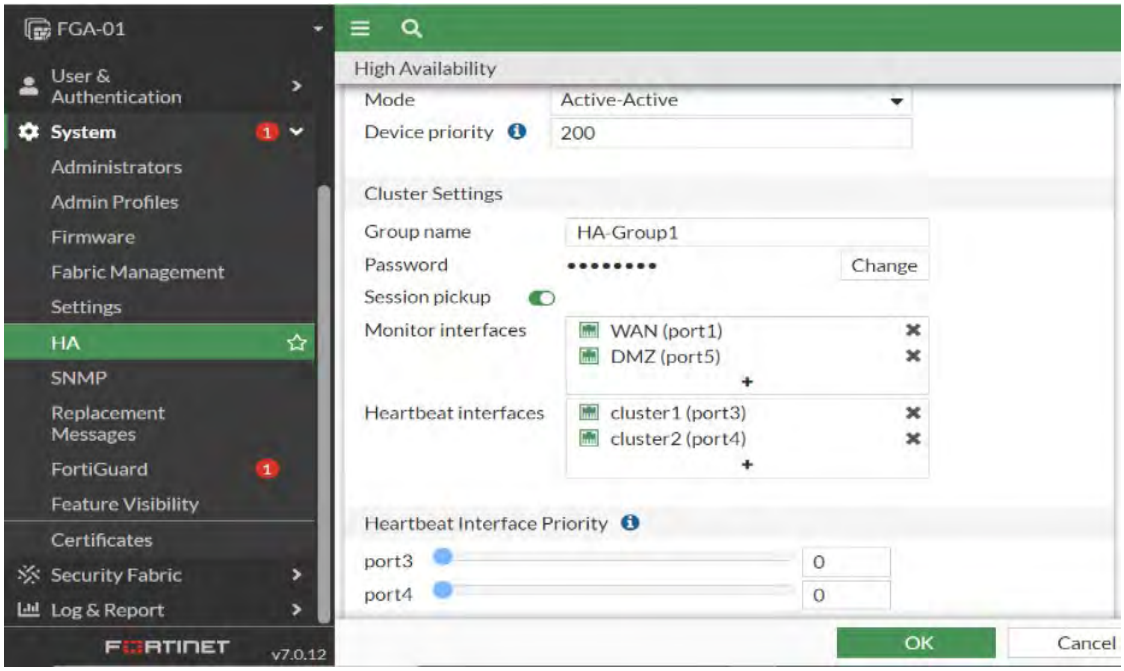


FIGURE IV.6 - Configuration HA "FGA-01 ".

Nous effectuons une Configuration similaire pour le pare-feu esclave (FGA-02), avec des paramètres de priorité inférieurs à celles du maître.

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

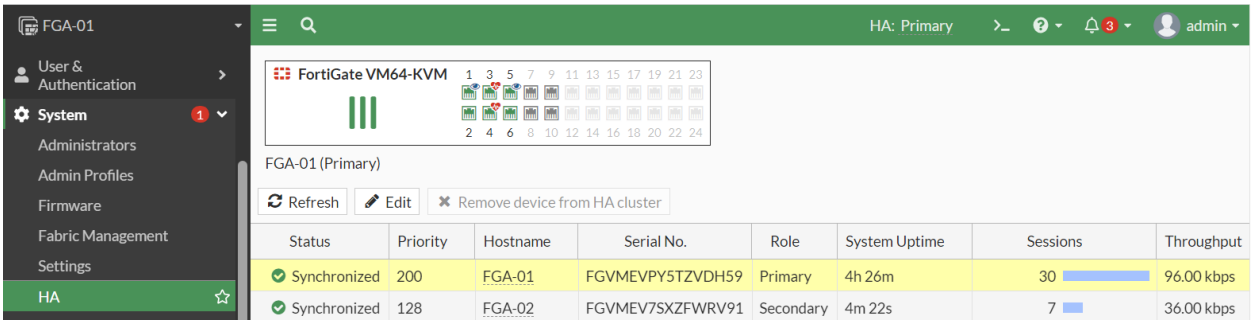


FIGURE IV.7 - Configuration HA effectuée avec succès.

IV.8.2 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 " DMZ " vers "Internet ou WAN" ; 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 IV.8).

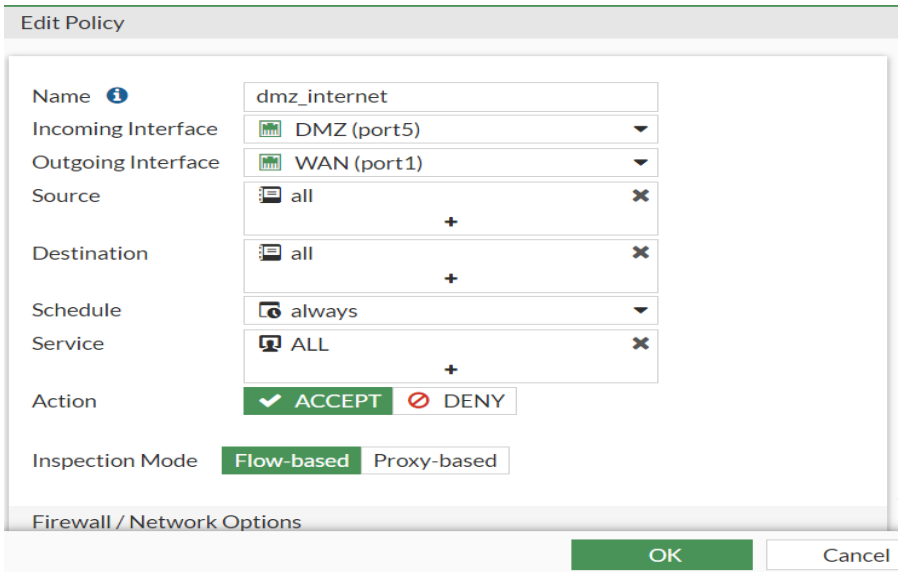


FIGURE IV.8 - Exemple de Configuration d'accès de la zone "dmz" vers "Internet".

Filtrage Web

Précédemment tous les utilisateurs ont accès à 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 IV.9).

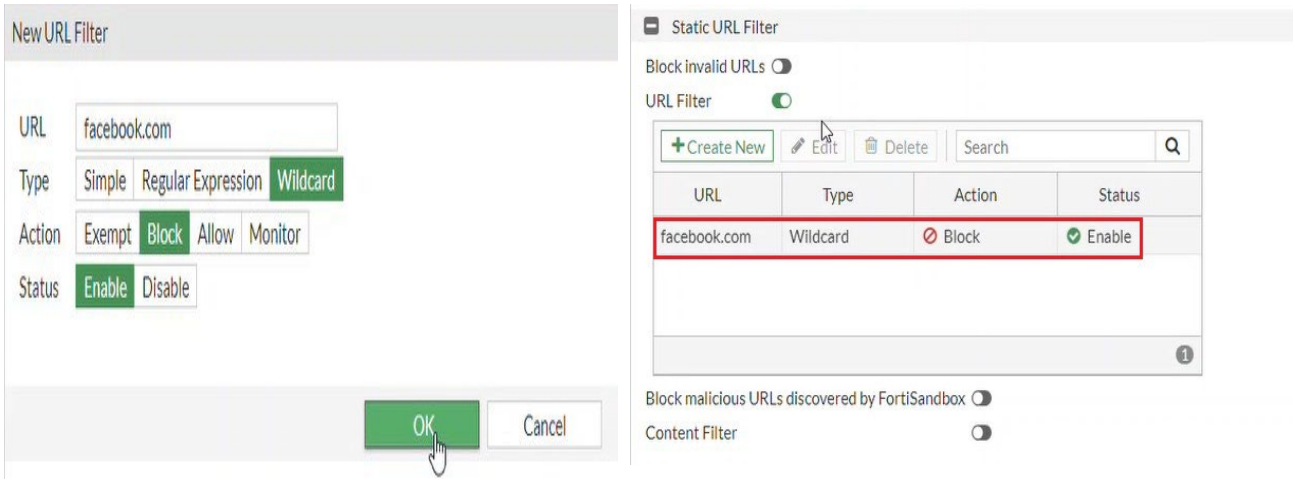


FIGURE IV.9 - Création d'un nouveau filtre URL "Facebook".

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. (Voir figure IV.10).

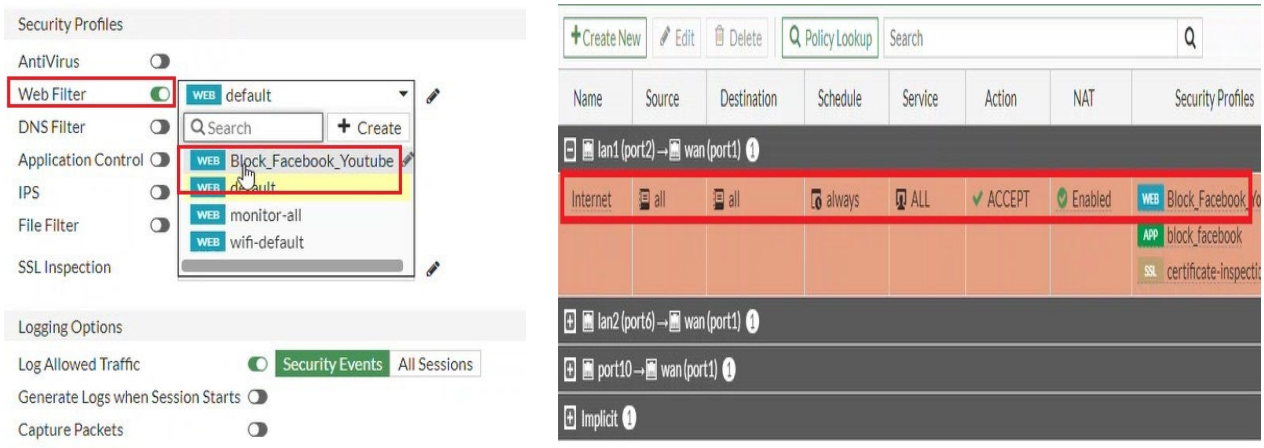


FIGURE IV.10 - Application du filter web sur ACL.

Filtrage applicatif

Dans le Filtrage Applicatif nous allons bloquer l'accès à certaines applications (Nous prendrons YouTube 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-youtube).

b) Dans la partie "Application and Filter Overrides" nous allons créer une nouvelle dérogation, nous choisissons comme type "Application" et selectionnons YouTube puis "OK" (voir Figure IV.11).

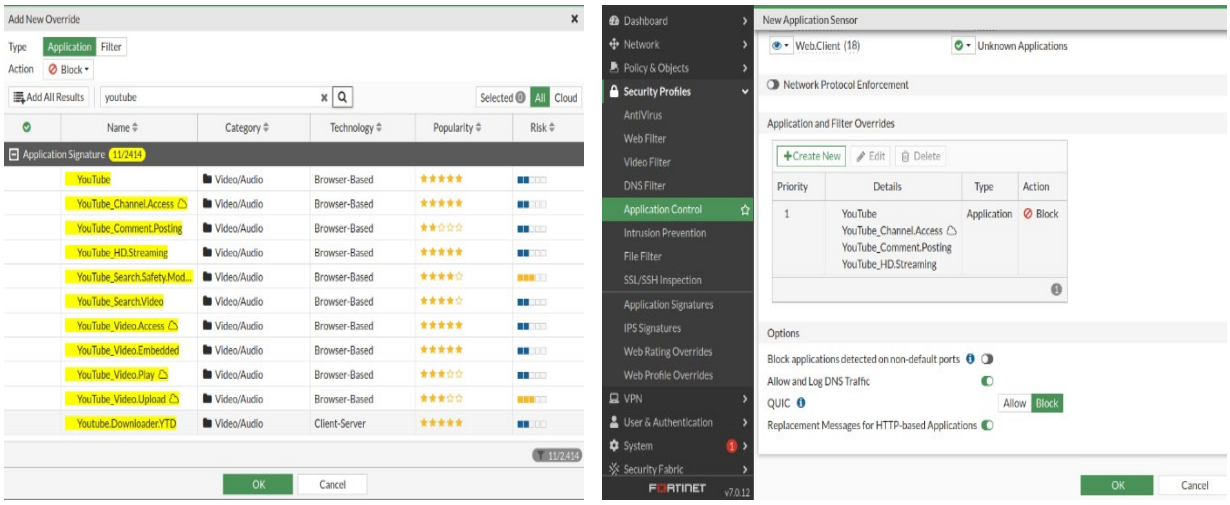


FIGURE IV.11Création d'une règle de contrôle d'application "YouTube".

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 (voir Figure IV.12).

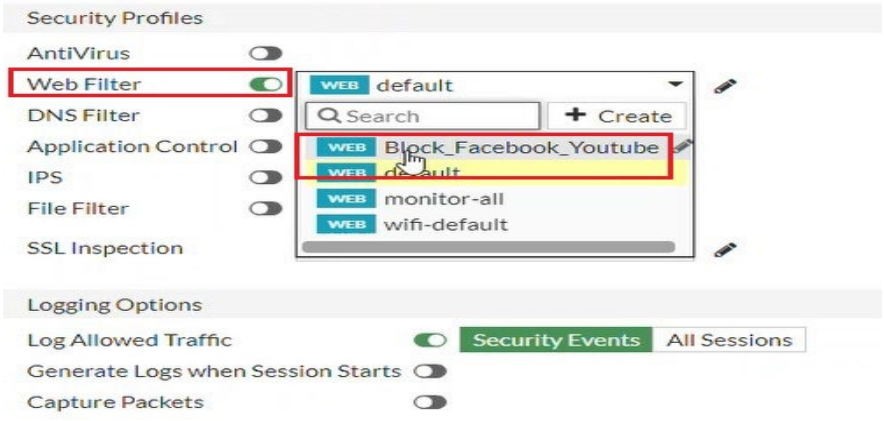


FIGURE IV.12 - Application de la règle de contrôle d'application.

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

IV.8.3 Configuration des Vpn

IV.8.3.1 Configuration du VPN IPsec (site à site)

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 respectivement 172.20.0.1 et 172.22.0.2

Configuration vpn1 (Akbou vers ORAN)

a) Afin de créer un tunnel VPN IPsec sur le pare-feu FortiGate, On selectionne [VPN] -> [IPSec Wizard] et saisir le nom du tunnel (AKBOU_ORAN), 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 ORAN distant (172.22.0.1).

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 ORAN distant peut également être authentifié via un certificat (voir Figure IV.13).

.

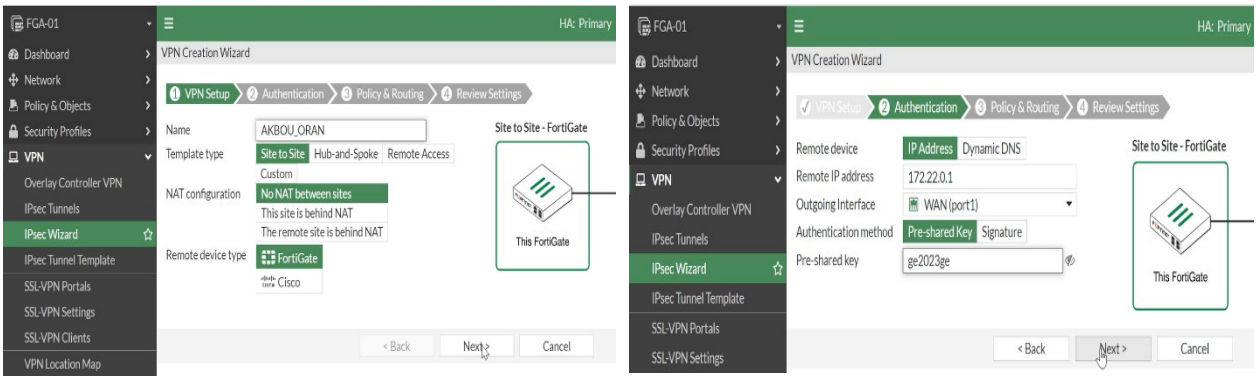


FIGURE IV.13 - Création et Authentification du tunnel Akbou-Oran IPsec.

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 le vlan 40 et 50 qu'on a autoriser pour les faire sortir vers l'extérieurs (voir Figure IV.14).

.

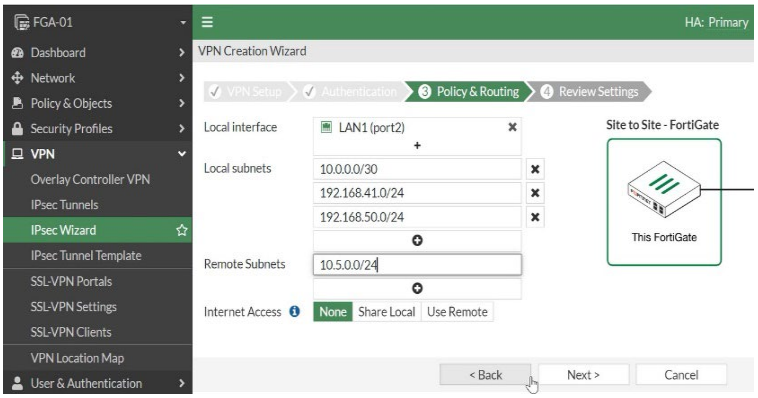


FIGURE IV.14 - Policy and Routing Akbou-Oran IPsec.

d) Une page récapitulative affiche la configuration créée, y compris les interfaces, les adresses de pare-feu, les routes et les politiques (voir Figure IV.15).
.

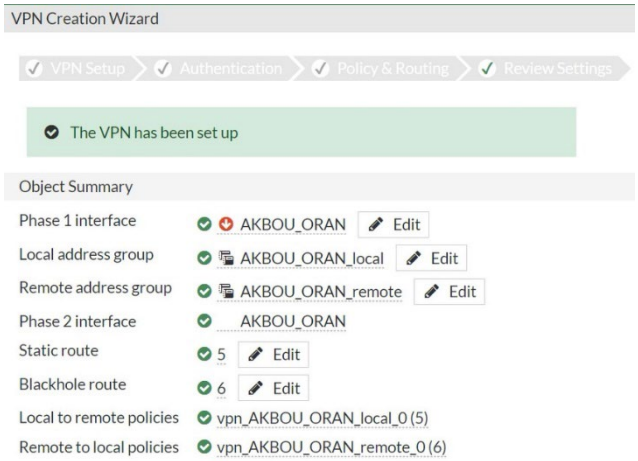


FIGURE IV.15 - Configuration créée par Akbou-Oran.

e) Pour afficher l'interface VPN créée par l'assistant, nous allons accéder à [Network] -> [Interfaces] (voir Figure IV.16).

FIGURE IV.16 - L'interface Akbou-Oran créée.

f) Pour afficher les routes créées par l'assistant, nous allons accéder à [Network] -> [Static Routes] (voir Figure IV.17).
.

Destination	Gateway IP	Interface	Status	Comments
IPv4 4				
Akbou-Oran_remote	172.23.0.1	Akbou-Oran	Enabled	VPN: Akbou-Oran (Created by VPN wizard)
Akbou-Oran_remote		Blackhole	Enabled	VPN: Akbou-Oran (Created by VPN wizard)
0.0.0.0/0	172.20.0.2	WAN (port1)	Enabled	

FIGURE IV.17 - Routes créées par Akbou-Oran.

Configuration vpn2 (ORAN vers Akbou)

Concernant la configuration du VPN2, nous avons suivis les mêmes étapes que la configuration du VPN1 (voir Figure IV.18).

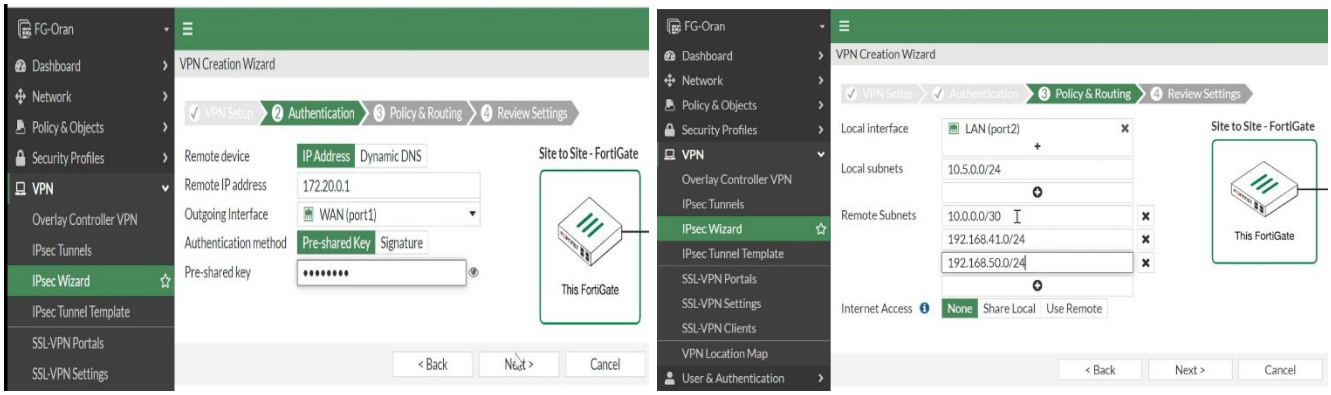


FIGURE IV.18 - Configuration d'Authentification et " Policy and Routing" ORAN_AKBOU IPsec.

Pour Activer le tunnel VPN, nous avons accédé à [Dashboard] -> [Network] -> [IPsec Monitor] de VPN1 et celui de VPN2. Puis on sélectionne « Statut » et on clique sur "bring up" (voir Figure IV.19).

.

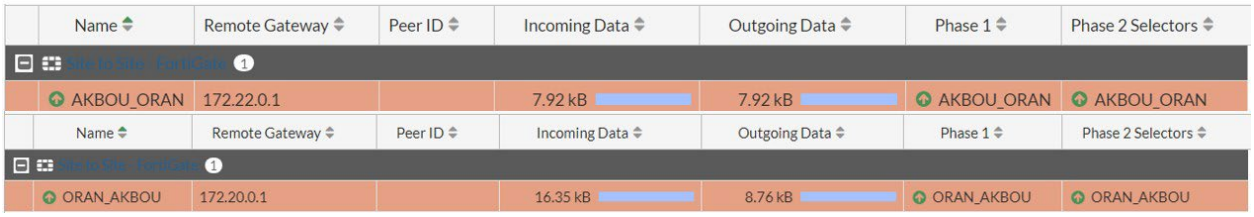


FIGURE IV.19 - Activation du tunnel VPN sur les deux sites.

IV.8.3.2 Configuration du VPN GRE (site à site)

Dans cette partie nous allons creer un tunnel GRE sur notre FortiGate qui sont : le IN_GRE (Alger vers Akbou) et le OUT_GRE (Akbou vers Alger) ; On note que les adresses IP des sites Akbou et Alger sont respectivement 172.20.0.1 et 172.21.0.2

Configuration de GRE au niveau du « R_ALGER »

Par la configuration des interface eth0/0 et eth0/1 et la création de l'interface tunnel nommé « tunnel 1 » et la création des routes statique pour les vlan 41 et 50 pour autoriser l'accès au Wan, voici les commandes utiliser (voir Figure IV.20):

```
R-ALGER#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-ALGER(config)#interface ethernet 0/0
R-ALGER(config-if)#no shutdown
R-ALGER(config-if)#ip address 172.21.0.1  255.255.255.252
R-ALGER(config-if)#EXIT
R-ALGER(config)#interface ethernet 0/1
R-ALGER(config-if)#no shutdown
R-ALGER(config-if)#ip address 10.3.0.1  255.255.255.0
R-ALGER(config-if)#EXIT
R-ALGER(config)#interface tunnel 1
R-ALGER(config-if)#ip address 10.11.12.1  255.255.255.252
R-ALGER(config-if)#ip mtu 1400
R-ALGER(config-if)#ip tcp adjust-mss 1360
R-ALGER(config-if)#tunnel source 172.21.0.1
R-ALGER(config-if)#tunnel destination 172.20.0.1
R-ALGER(config-if)#ip route 0.0.0.0 0.0.0.0 172.21.0.2
R-ALGER(config)#ip route 192.168.41.0 255.255.255.0 10.11.12.2
R-ALGER(config)#ip route 192.168.50.0 255.255.255.0 10.11.12.2
R-ALGER(config)#END
```

FIGURE IV.20 - configurations de GRE au niveau de router Alger.

Configuration de GRE au niveau du pare-feu « FAG-01 »

a) Afin de créer un tunnel VPN GRE sur le pare-feu FortiGate, On crée des deux règle entrant et sortant [Firewall policy] -> [new poliy] et saisir le nom règle (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" (voir Figure IV.21).

.

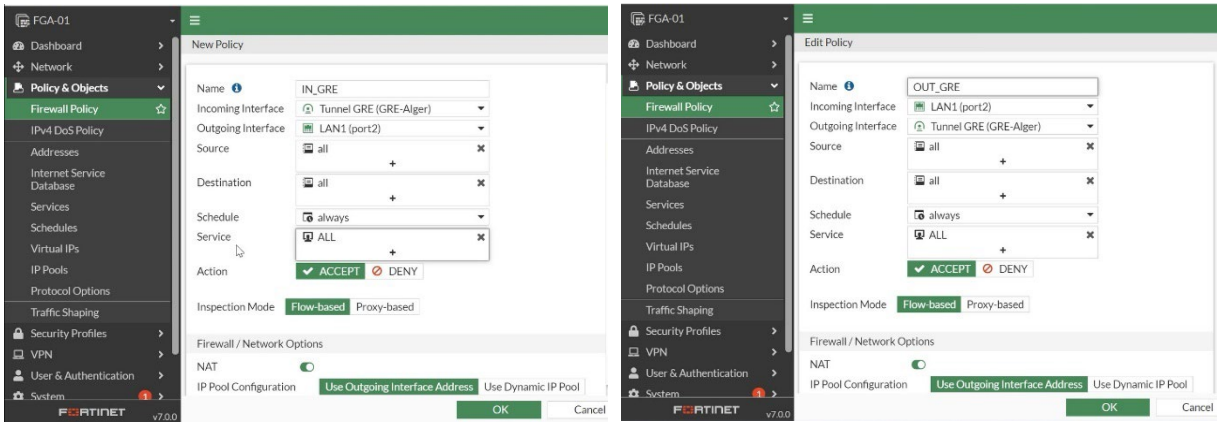


FIGURE IV.21 - créations de règle de filtrage entrant et sortant.

b) Création de la route statique Akbou vers Alger et Policy route :

Dans l'étape Policy and Routing, nous allons définir l'interface Tunnel GRE (GRE-Alger), l'assistant ajoute automatiquement le sous-réseau local et la route statice crée (voir Figure IV.22).

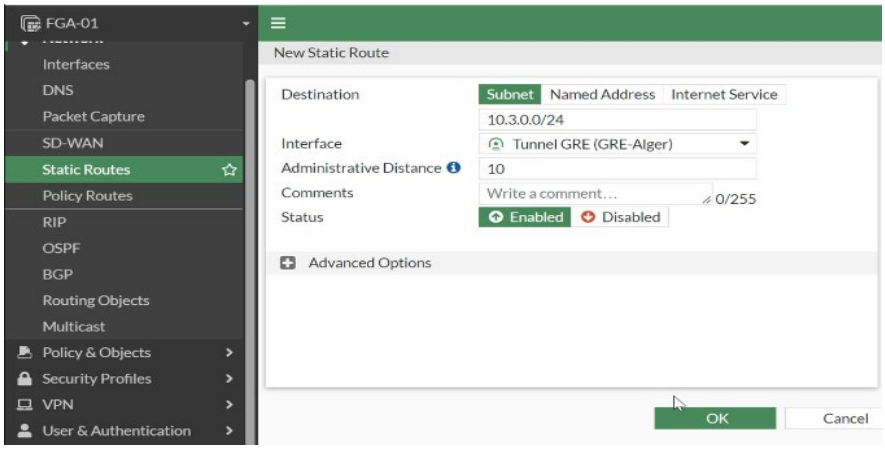


FIGURE IV.22 - créations d'une Policy route et une route statice vers Alger.

d) Configuration GRE sur le FGA-01, voici les commandes effectuées :

```
FGA-01 (gre-tunnel) # edit GRE-Alger

FGA-01 (GRE-Alger) # set interface port1

FGA-01 (GRE-Alger) # set remote-gw 172.21.0.1

FGA-01 (GRE-Alger) # set local-gw 172.20.0.1
```

```
FGA-01 (interface) # edit GRE-Alger
FGA-01 (GRE-Alger) # set vdom root
FGA-01 (GRE-Alger) # set ip 10.11.12.2 255.255.255.255
FGA-01 (GRE-Alger) # set allowaccess ping
FGA-01 (GRE-Alger) # set type tunnel
FGA-01 (GRE-Alger) # set remote-ip 10.11.12.1 255.255.255.255
FGA-01 (GRE-Alger) # set snmp-index  62
FGA-01 (GRE-Alger) # set interfeace port 1
```

FIGURE IV.23 - création et configuration de GRE Alger.

IV.8.3.3 Configuration du VPN IPsec (client à site)

a) Afin de créer un tunnel VPN IPsec sur le pare-feu FortiGate, On selectionne [VPN] -> [IPSec Wizard] et saisir le nom du tunnel (vpnCtoS), type de modèle c'est "client à site" et celui de périphérique distant est une machine virtuelle windows 10 nommé 'clint_vpn', ensuite nous allons sélectionner NAT Configuration comme" No NAT between sites".

b) Dans l'étape Authentification, on va définir incoming interface wan(port1), Par la suite nous définissons une clé pré-partagée sécurisée (PSK) « ge2023 » (voir Figure IV.24).

.

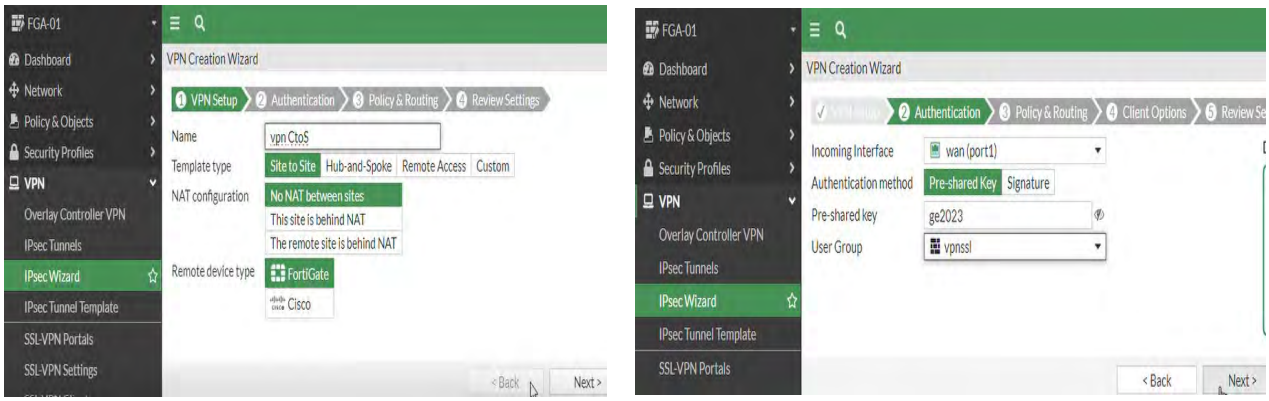


FIGURE IV.24 - Création et Authentification du tunnel Client Vpn IPsec.

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 le vlan 40 et 50 qu'on a autoriser pour les faire sortir vers l'extérieurs (voir figure IV.25)

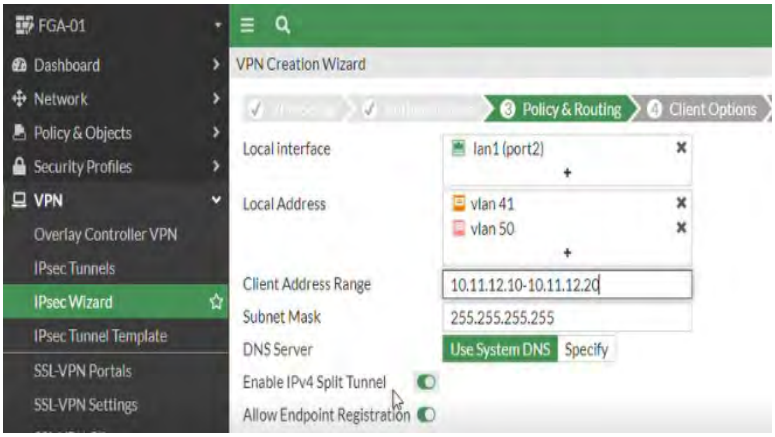


FIGURE IV.25 - Policy and Routing client IPSec.

d) Une page récapitulative affiche la configuration créée, y compris les interfaces, les adresses de pare-feu, les routes et les politiques (voir Figure IV.26).

.

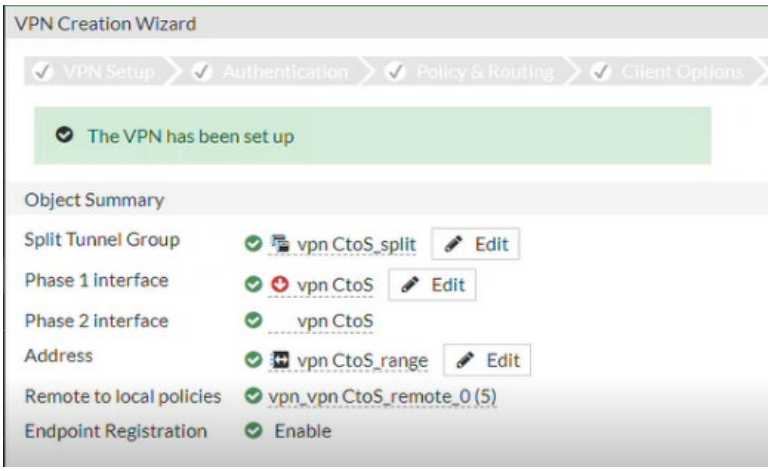


FIGURE IV.26 - Configuration créée par Vpn CtoS.

e) Ensuite on modifie les protocoles de cryptage de la clé partagée nécessaires pour le tunnel VPN, cette étape est faite en deux phase 1 et 2, (voir Figure IV.27).

.

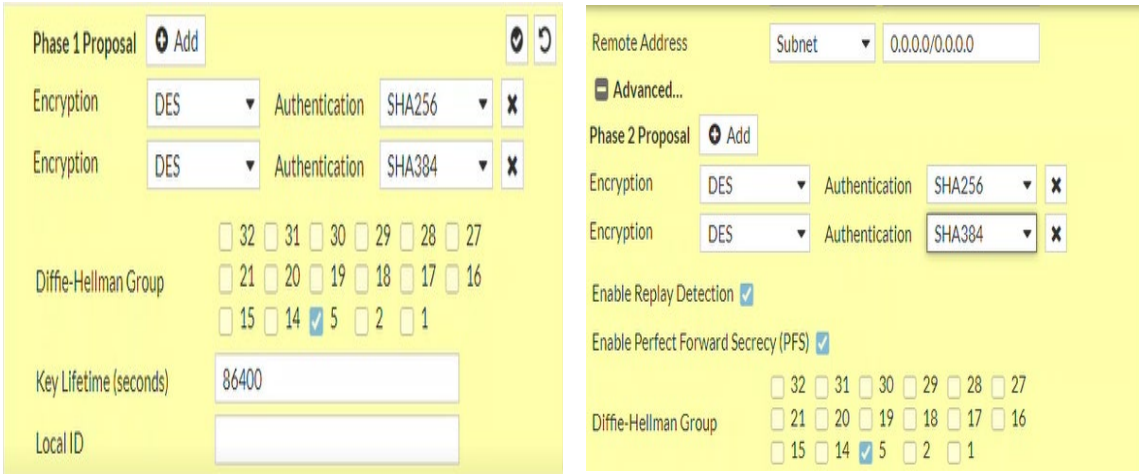


FIGURE IV.27 - les protocoles de cryptage utiliser pour de la clé.

Connexion au niveau d'application Forticlient

a) Tout d'abord on acréé une nouvelle connexion VPN dont on a saisie l'adresse de la passerelle distante et le mot de passe de la clé partagé.

b) Ensuite on a paramétré la phase 1 et 2 avec les mêmes algorithmes qu'on a défini avant sur le pare-feu (voir Figure IV.28).

.

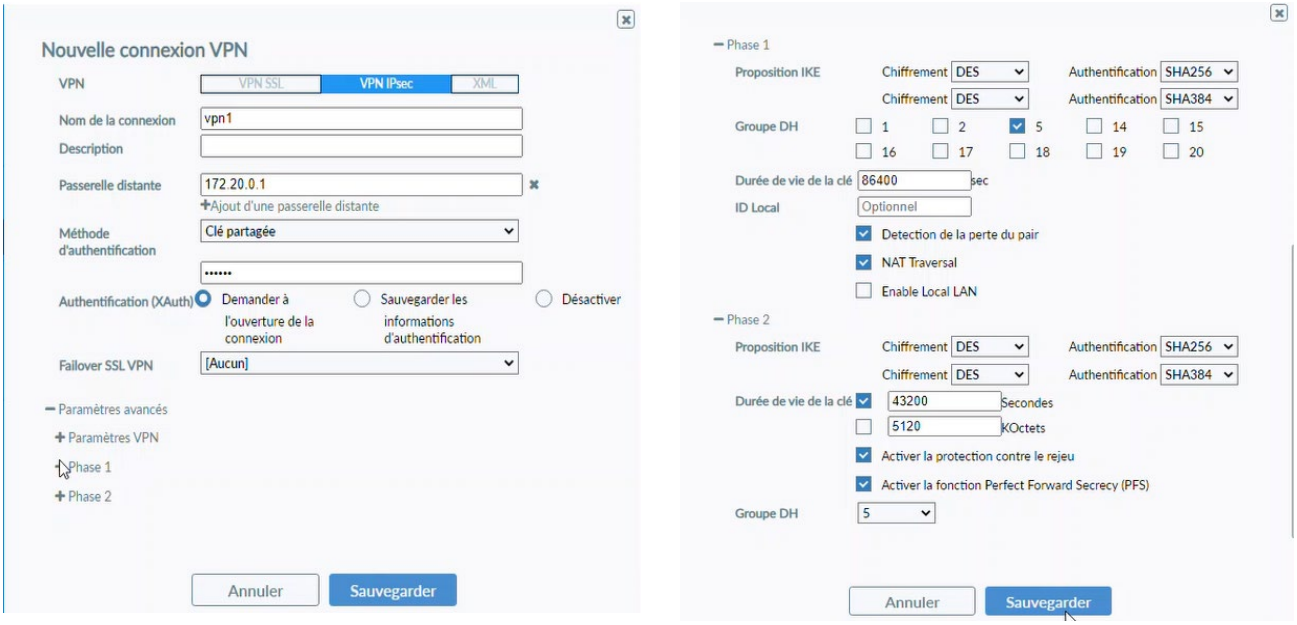


FIGURE IV.28 - Création d'une nouvelle connexion.

c) Puis nous allons saisir le nom d'utilisateur ainsi que son mot de passe comme respectivement « nadjetimane » et « 123456 »
d) Enfin la figure suivante nous montre que la connexion a été établie avec succès (voir Figure IV.29).

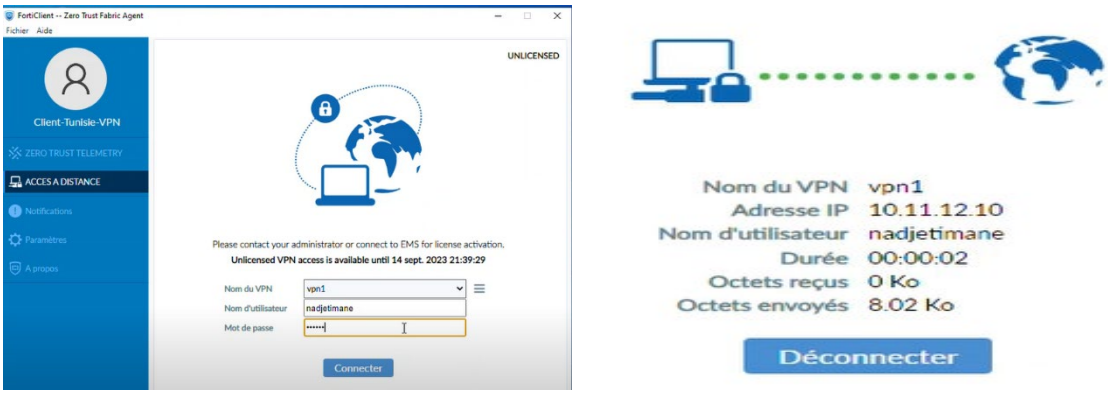


FIGURE IV.29 - Connexion VPN établie avec succès.

IV.8.4 Configuration de la DMZ

Configuration vlan Community 100 et isolated 101et vlan primary 102 et associer le primary avec isoleted voici les commandes effectuées :

```
vlan 100
  private-vlan community
!
vlan 101
  private-vlan isolated
!
vlan 102
  private-vlan primary
  private-vlan association 100-101
```

Configuration 0/1 en mapping

```
interface Ethernet0/1
 switchport private-vlan mapping 102 100-101
 switchport mode private-vlan promiscuous
```

Configuration de l'interface 3/0 et 3/1 en associant le vlan primary avec community
Configuration de l'interface 3/2 en associant le vlan primary avec isolated

```
interface Ethernet3/0
 switchport private-vlan host-association 102 100
 switchport mode private-vlan host
!
interface Ethernet3/1
 switchport private-vlan host-association 102 100
 switchport mode private-vlan host
!
interface Ethernet3/2
 switchport private-vlan host-association 102 101
 switchport mode private-vlan host
```

Configuration de dmz sur le pare-feu « FGA-01 »

Par la création d'un regel [firewall policy] sur l'interface de DMZ (port5) vers le WAN (port1) (Voir Figure IV.30).

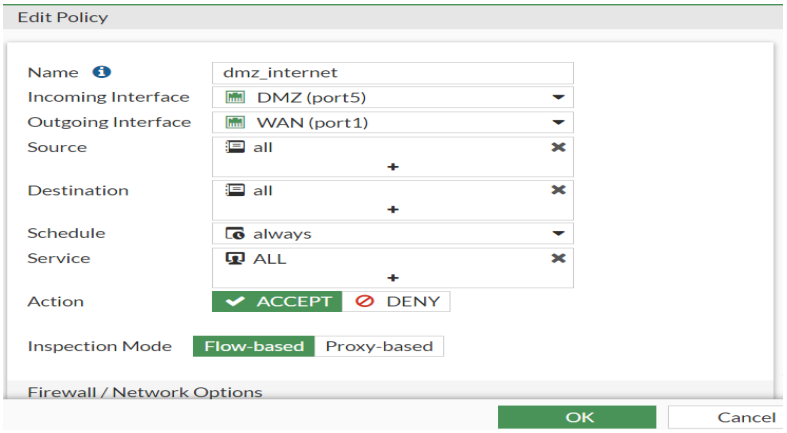


FIGURE IV.30 – Connexion de DMZ vers Internet.

IV.9 Les machines virtuelles sur VMware Workstation 17 Pro

IV.9.1 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 (Voir Figure IV.31).

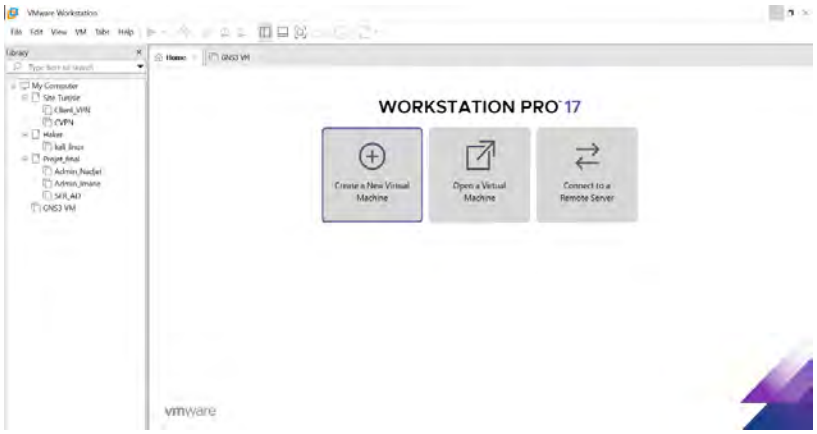


FIGURE IV.31 - L'interface graphique de VMware Workstation 17pro.

IV.9.2 Installation de la machine Windows serveur 2022

Installation des rôles et des fonctionnalités sur la machine Windows serveur 2022

a) Ajout des rôles de fonctionnalité : (DNS, AD DS, DHCP)

b) Nous avons sélectionné les rôles Active Directory domaine service, DNS et DHCP en cochant les cases correspondantes puis on clique sur suivant, à ce stade, une fenêtre apparait, on clique sur installer pour commencer l'installation.

c)Une fois que l'installation est achevée, une autre fenêtre va apparaitre, on clique sur fermer pour terminer.

d) Une fois les fonctionnalités d'AD DS installées. Nous devons promouvoir ce serveur en tant que contrôleur de domaine, sinon le domaine ne sera pas créé.

e) Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en cochant sur Ajouter une nouvelle forêt et en spécifiant le nom de domaine « ge. local »

f) L'étape suivante consiste à choisir le niveau fonctionnel de la forêt et du domaine ainsi pour éviter les restaurations non souhaitées d'Active Directory, il est demandé de saisir un mot de passe de restauration, L'assistant suivant montre le nom NetBIOS de domaine (Voir Figure IV.32).

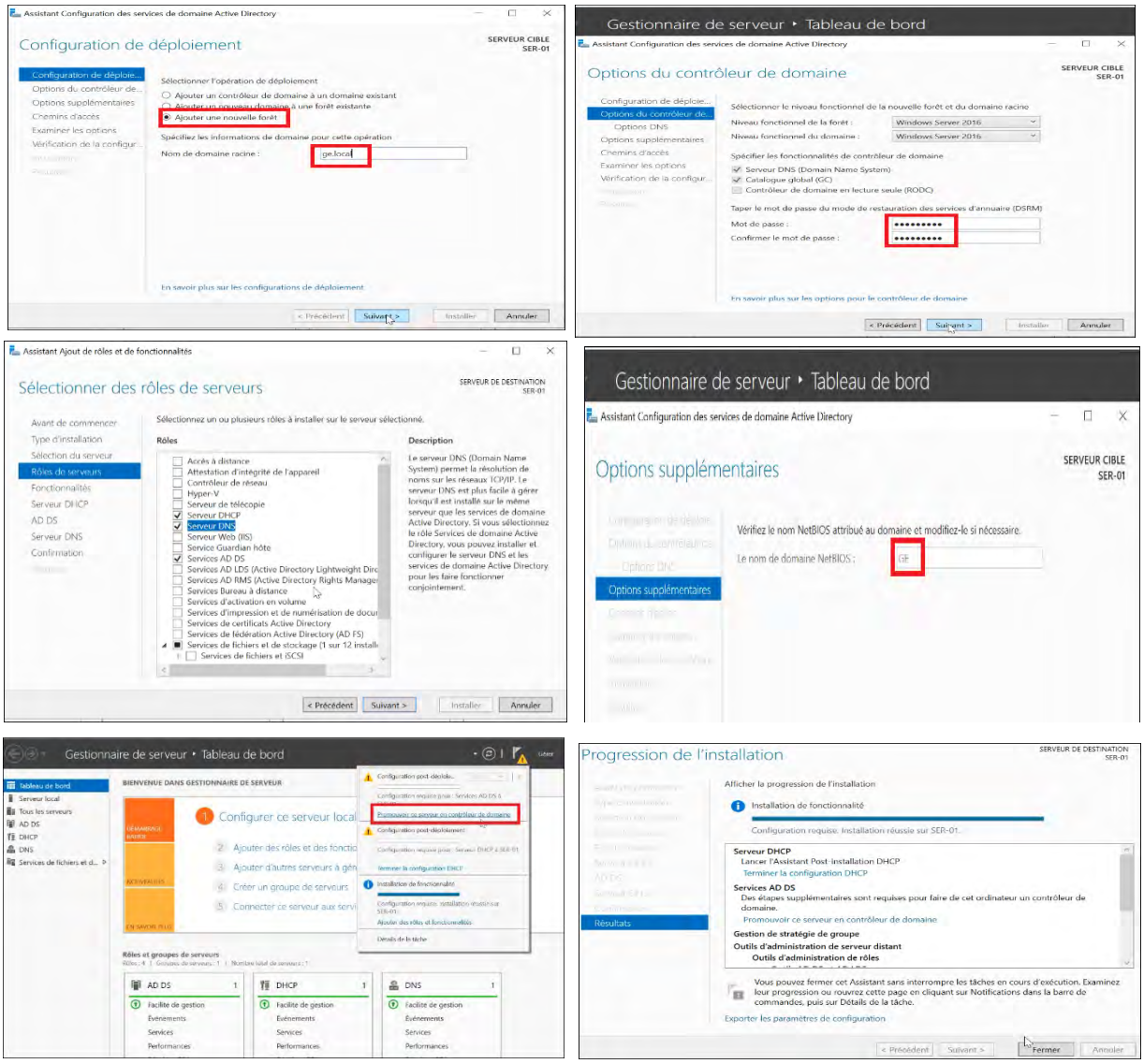


FIGURE IV.32 - étapes d'installations d'AD, DHCP, DNS.

IV.9.2.1 Configuration DHCP

Dans cette étape, nous avons créé des étendues pour chaque VLAN avec un simple clic droit, puis on a choisi Nouvelle étendue, Ensuite nous allons attribuer un nom à notre étendu que nous voulons créer puis introduisons la plage d'adresse à cet étendu c'est elle qui définis le nombre maximal d'adresses que nous pouvons distribuer aux ordinateurs, En suit nous définissons une plage d'adresses qui ne seront pas distribuer par le serveur, Ensuite on rajoute une passerelle par défaut puis Nous rajoutons l'adresse de serveur DNS et nous spécifions le nom de domaine, Enfin on ajoute l'adresse de notre serveur (Voir Figure IV.33).

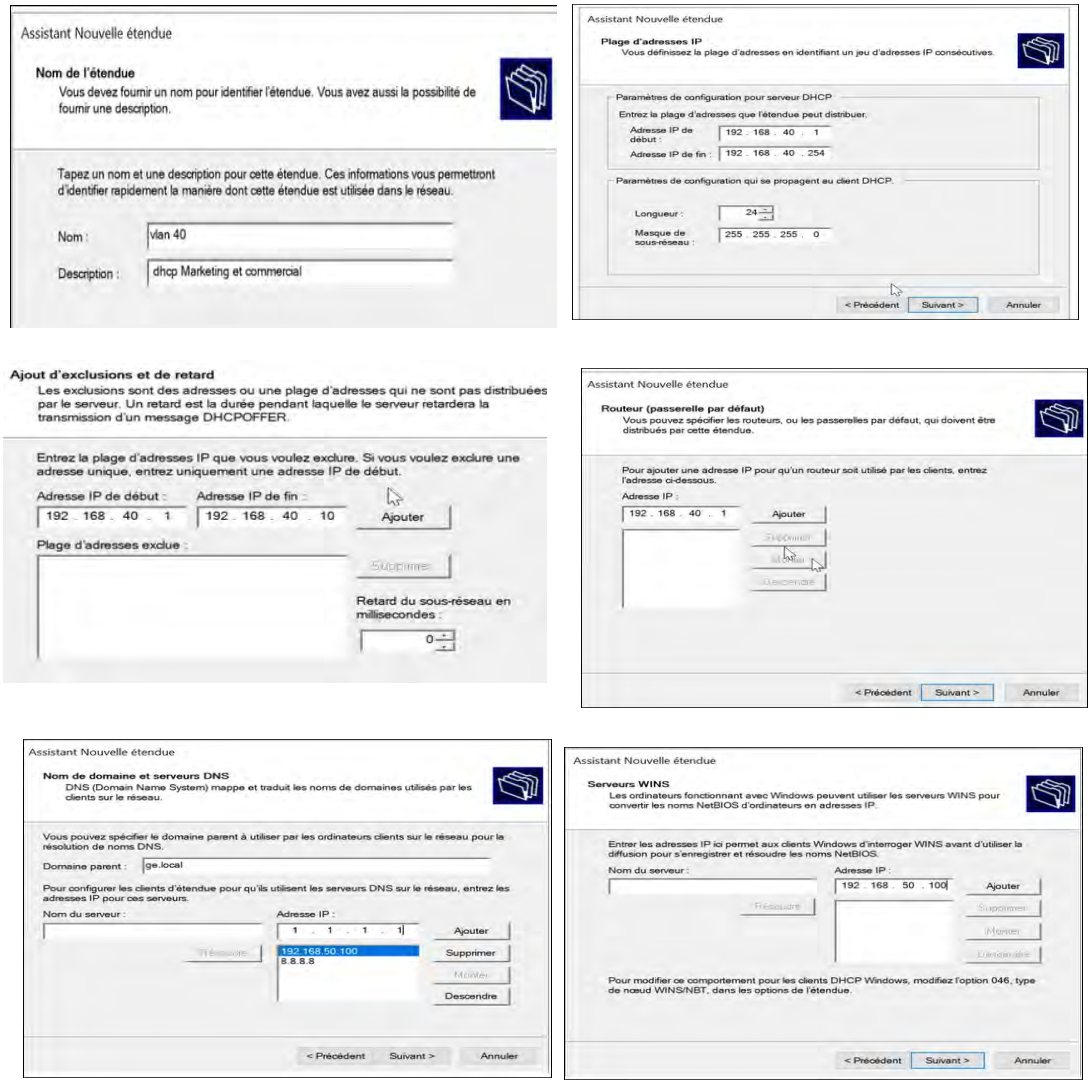


FIGURE IV.33 - étapes de configuration DHCP pour le vlan 40.

IV.9.3 Installation Windows 10 professionnel qui est la machine cliente

Ensuit Cloner Admin_Nadjet et Amin_Imane.

IV.9.3.1 Installation de l'application Forticlient sur cette machine cliente

FortiClient est un l'agent de sécurité qui offre protection, conformité et accès sécurisé dans un client léger unique et modulaire. Un agent de sécurité est un peu de logiciel de endpoint qui s'exécute sur un endpoint, tel qu'un ordinateur portable ou un appareil mobile et communique avec la Security Fabric de Fortinet pour fournir des informations, une visibilité et un contrôle à cet appareil [26]. (Voir Figure IV.34).

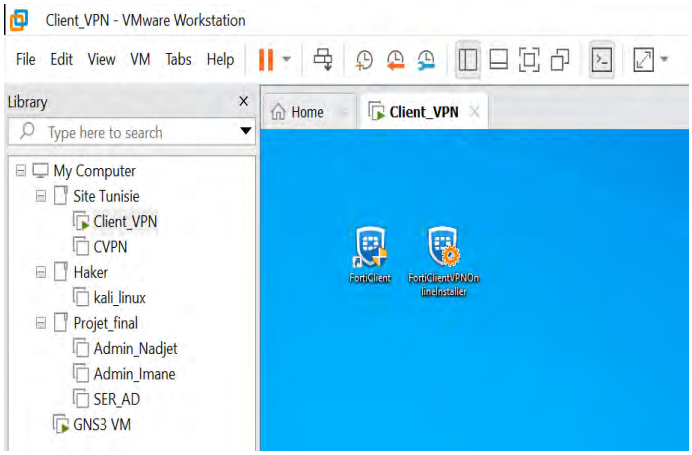


FIGURE IV.34 - l'application Forticlient installé sur la machine Client_Vpn.

IV.9.4 Installation de kali linux

Kali Linux est une distribution Linux open source largement utilisée pour les tests d'intrusion, le piratage et les tâches liées à la cybersécurité. Il est développé et maintenu par Offensive Security. Kali Linux est connu pour sa vaste collection d'outils et de ressources qui aident les professionnels et les passionnés de sécurité à tester, analyser et sécuriser les systèmes et réseaux informatiques (Voir Figure IV.35).

FIGURE IV.35 - L'interface graphique de Kalilinux.

Authentification avec nom d'utilisateurs : haker, mot de passe : 1.

FIGURE IV.36 - Authentification.

IV.9.4.1 Configuration de IPS

a) Sur le pare-feu « FGA-01 » Nous allons dans [Security Profiles] > [Intrusion Prévention] on crée une nouvelle règle Nommée « IPSGE » et on ajoute la signature log bloque (Voir Figure IV.37).

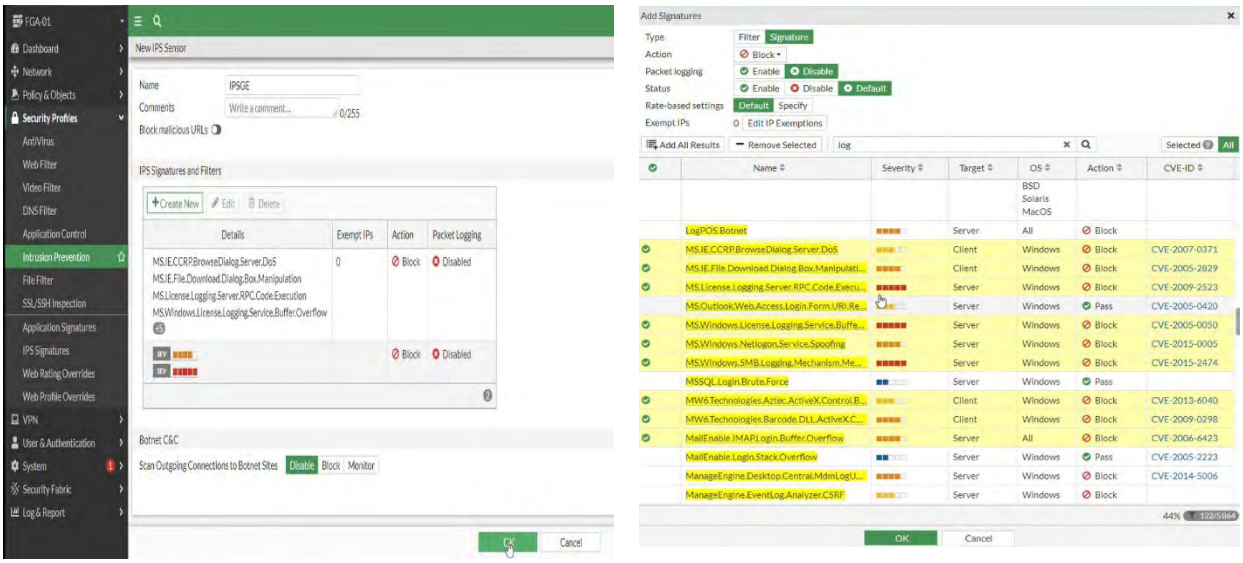


FIGURE IV.37- Création d'une règle de prévention d'intrusion IPSGE.

b) Dans cette étape nous allons prendre une ACL parmi les ACLs crées auparavant et applique le règle « IPSGE » (Voir Figure IV.38).

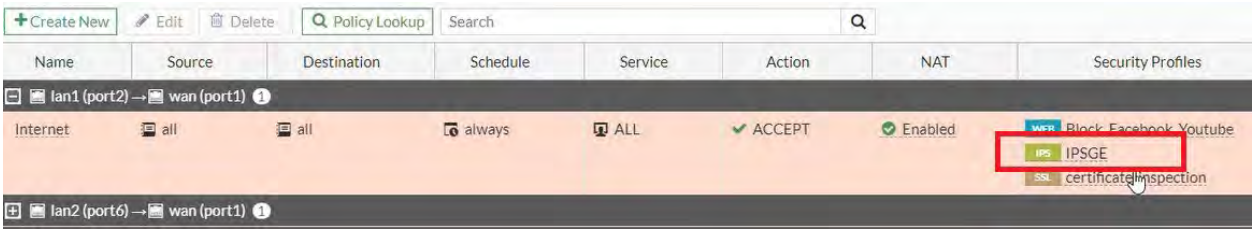


FIGURE IV.38 - Application de la règle de prévention d'intrusion IPSGE.

IV.9.5 Mise en œuvre de l'autorité de certification Active et le server NPS

a) Installation et configuration de server de certificat

Après avoir installé et configure le serveur de certificats sur « SER-01.ge.local » (Voir Figure IV.39).

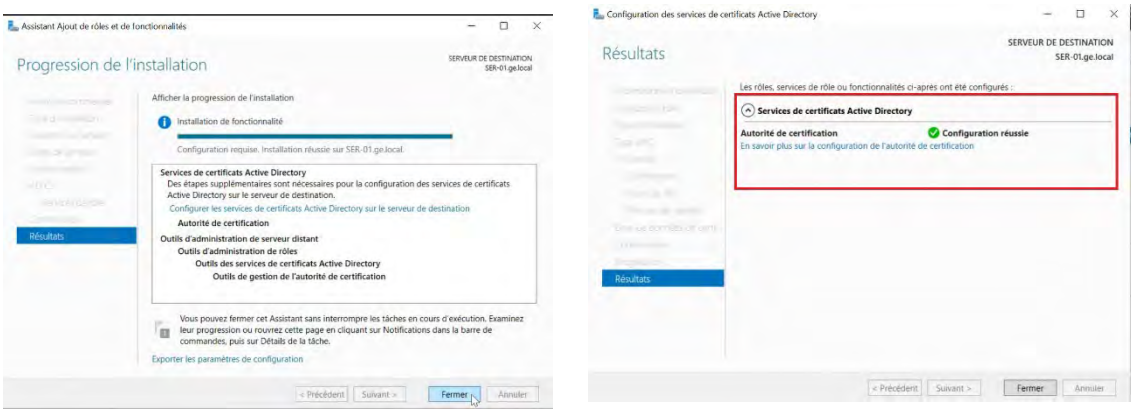


FIGURE IV.39 - Installation et configuration de service de certificat sur le AD.

b) Création des unités d'organisation

nous allons créer une unité d'organisation nommée 'Site Akbou', sur cette unité 'Site Akbou' on va encore créer des autres unités d'organisation pour chacun de nos VLANs, par la suite dans l'unité 'Service Informatique' nous allons créer deux autres unités : une unité 'ordinateurs' où on a associé deux nouveaux ordinateurs 'PC 1' et 'PC2' et une autre 'utilisateurs' où on a associé ces groupes 'G certificat serveur', 'G certificat clients' et 'G vlan 41 informatique', ensuite on va créer deux nouveaux utilisateurs avec un mot de passe pour chacun dans 'Service informatique' puis on les ajoutera au 'G vlan 41 informatique'(voir figure IV.40) .

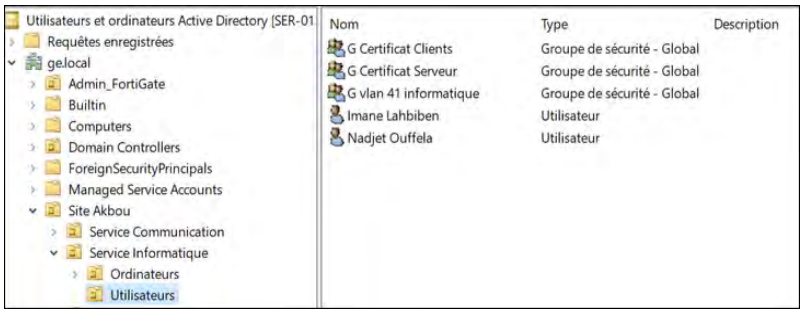


FIGURE IV.40 - Création des unités d'organisation.

c) **Création des Modèles de certificat**

Sur Outil ensuite autorité de certificat on ajoute les deux modèles de certificat crée un pour la certification des serveurs « Serveurs GE authentification certificat » et l'autre pour les clients « Authentification SDT GE », (SDT : station de travail). (Voir figure IV.41)

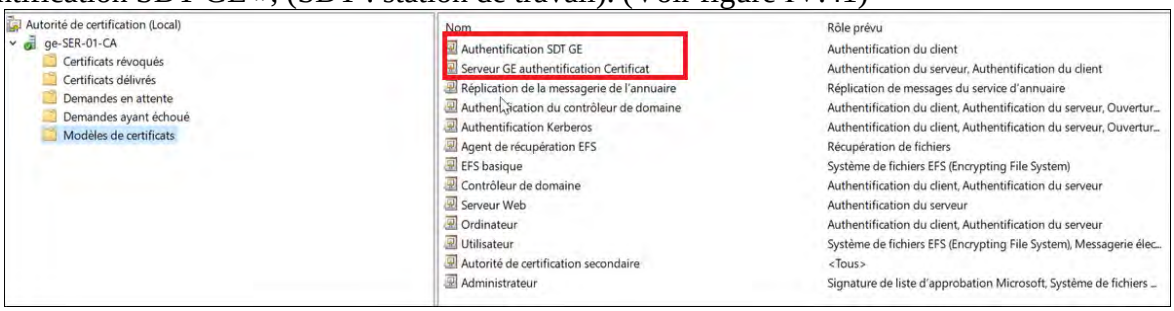


FIGURE IV.41 - Création de modèle de certificat.

d) Configuration de Stratégie

1) Configuration d'une stratégie globale

Une stratégie globale qui s'applique sur les utilisateurs et les ordinateurs qui permet de les centraliser.
Sur outil ⇒nouveau gestion de stratégies du groupe ⇒ge.local ⇒stratégie global ⇒cliquer sur modifier afin d'appliquer cette stratégie sur les ordinateur.
Puis sur paramètre Windows ⇒ paramètre de sécurité⇒ stratégie clé publique ⇒client des services de certificats et on configure comme montre ci-dessus (Voir Figure IV.42).

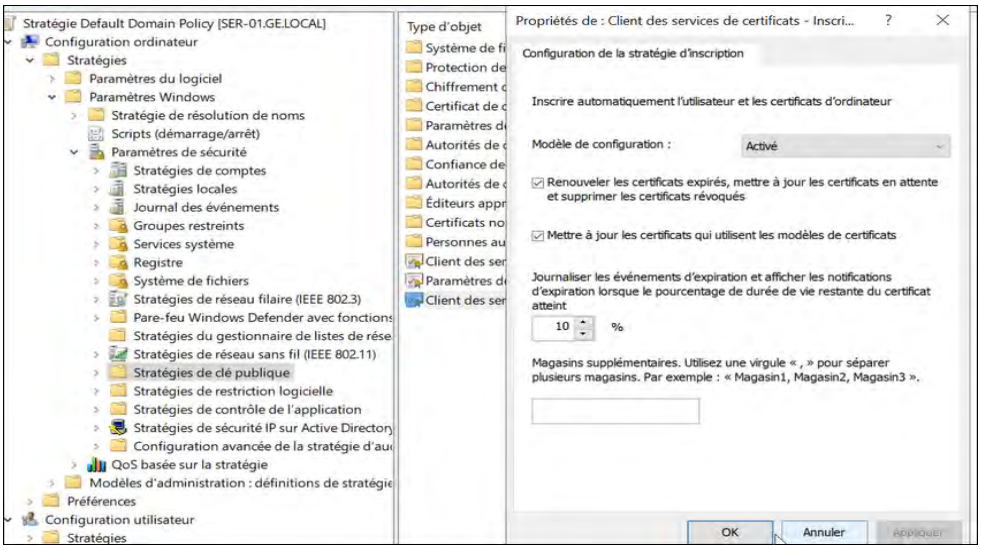


FIGURE IV.42 - Configuration d'une stratégie globale.

2) Création d'une nouvelle stratégie

Sur objets ⇒stratégie de groupe ⇒nouveau stratégie nommer 'ST-RADIUS' ⇒ modifier (car par défaut elle est vide) ⇒ configurer ordinateur ⇒ stratégies ⇒ paramètre Windows ⇒ paramètre de sécurité ⇒ services système afin d'activer la 802.1X (pour chaque ordinateur qui se connecte cette stratégie sera appliquer automatiquement pour lui car on veut certifier le physique) (voir figure IV.43)

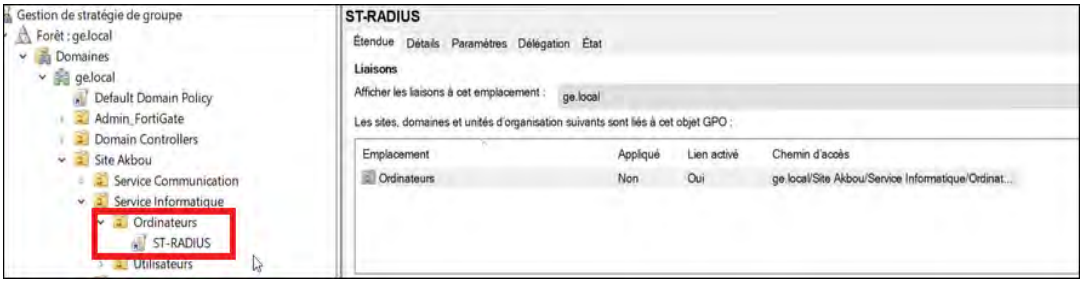


FIGURE IV.43 - Application de la stratégie sur les ordinateurs.

e) Configuration du serveur NPS (Network Policy Server)

Apre avoir relié notre serveur NPS dans Active Directory

1) Nous allons créer une nouvelle politique 802.1x pour authentifier les utilisateurs lors de la connexion à notre commutateur. Pour cela on configure 802.1x , (Voir Figure IV.44).

FIGURE IV.44 - Sélection d'un scénario de configuration.

2) On ajoute notre client Radius ”Client-Radius”, l’authentificateur est le commutateur. Lorsque l’utilisateur est connecté à un port sur le commutateur, le commutateur nécessite une authentification de l’utilisateur (voir figure IV.45)

Figure IV.45 - Ajout de client Radius.

3) Après avoir choisi une méthode d’authentification ‘Microsoft : Protected EAP (PEAP)’, on va effectuer l’authentification avec les utilisateurs du groupe ”G vlan 41 informatique” (voir figure IV.46)

FIGURE IV.46 - Spécification de groupe d’utilisateurs pour la connexion.

IV.10 Les Tests de Connectivité

Test de DHCP

```
PC1> ip dhcp
DORA IP 192.168.40.11/24 GW 192.168.40.250

PC3> ip dhcp
DORA IP 192.168.42.11/24 GW 192.168.42.250

PC8> ip dhcp
DORA IP 192.168.47.11/24 GW 192.168.47.250
```

Test de Routage inter-vlan

```
PC1> ping 192.168.42.11

84 bytes from 192.168.42.11 icmp_seq=1 ttl=63 time=34.830 ms
84 bytes from 192.168.42.11 icmp_seq=2 ttl=63 time=15.119 ms
84 bytes from 192.168.42.11 icmp_seq=3 ttl=63 time=18.411 ms
84 bytes from 192.168.42.11 icmp_seq=4 ttl=63 time=16.406 ms
84 bytes from 192.168.42.11 icmp_seq=5 ttl=63 time=17.119 ms

PC1>
PC1> ping 192.168.50.100

84 bytes from 192.168.50.100 icmp_seq=1 ttl=127 time=15.145 ms
84 bytes from 192.168.50.100 icmp_seq=2 ttl=127 time=13.361 ms
84 bytes from 192.168.50.100 icmp_seq=3 ttl=127 time=15.846 ms
84 bytes from 192.168.50.100 icmp_seq=4 ttl=127 time=16.929 ms
84 bytes from 192.168.50.100 icmp_seq=5 ttl=127 time=10.209 ms

PC1> ping 192.168.48.11

84 bytes from 192.168.48.11 icmp_seq=1 ttl=63 time=44.648 ms
84 bytes from 192.168.48.11 icmp_seq=2 ttl=63 time=10.448 ms
84 bytes from 192.168.48.11 icmp_seq=3 ttl=63 time=21.449 ms
84 bytes from 192.168.48.11 icmp_seq=4 ttl=63 time=12.517 ms
84 bytes from 192.168.48.11 icmp_seq=5 ttl=63 time=11.051 ms
```

Service communication

Serveur

Service CP (chef de projet)

Test de DMZ

```
ser01>
ser01> ping 10.1.0.4

host (10.1.0.4) not reachable
```

Community vers Isolated ne dervait pas ping

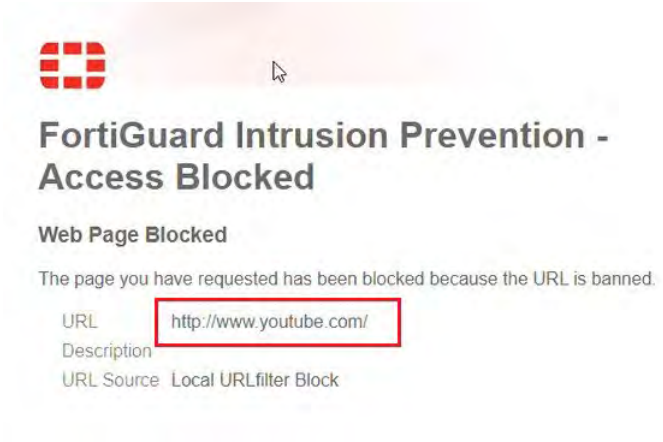
Test filtrage web et applicatif

Filtrage web

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

Filtrage Applicatif

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



Test Vpn GRE

Ping de R_Alger vers LAN Akbou

```
R-ALGER#ping 10.11.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.11.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
```

Ping de LAN Akbou vers R_Alger

```
FGA-01 # execute ping 10.11.12.1
PING 10.11.12.1 (10.11.12.1): 56 data bytes
64 bytes from 10.11.12.1: icmp_seq=0 ttl=255 time=3.9 ms
64 bytes from 10.11.12.1: icmp_seq=1 ttl=255 time=2.9 ms
64 bytes from 10.11.12.1: icmp_seq=2 ttl=255 time=2.1 ms
64 bytes from 10.11.12.1: icmp_seq=3 ttl=255 time=2.4 ms
64 bytes from 10.11.12.1: icmp_seq=4 ttl=255 time=3.0 ms

--- 10.11.12.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.1/2.8/3.9 ms
```

Test vpn Oran

Ping de pare-feu « FGA-01 » vers « FG-Oran »

```
FGA-01 # execute ping 172.22.0.1
PING 172.22.0.1 (172.22.0.1): 56 data bytes
64 bytes from 172.22.0.1: icmp_seq=0 ttl=254 time=7.2 ms
64 bytes from 172.22.0.1: icmp_seq=1 ttl=254 time=6.0 ms
64 bytes from 172.22.0.1: icmp_seq=2 ttl=254 time=4.2 ms
64 bytes from 172.22.0.1: icmp_seq=3 ttl=254 time=6.8 ms
64 bytes from 172.22.0.1: icmp_seq=4 ttl=254 time=4.8 ms

--- 172.22.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.2/5.8/7.2 ms
```

Ping de pare-feu « FG-Oran » vers « FGA-01 »

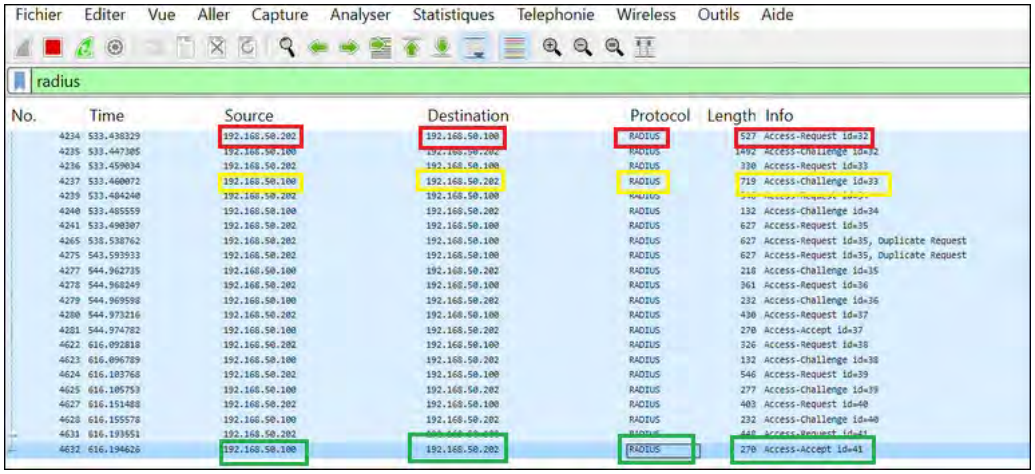
```
FG-Oran # execute ping 172.20.0.1
PING 172.20.0.1 (172.20.0.1): 56 data bytes
64 bytes from 172.20.0.1: icmp_seq=0 ttl=254 time=9.5 ms
64 bytes from 172.20.0.1: icmp_seq=1 ttl=254 time=5.8 ms
64 bytes from 172.20.0.1: icmp_seq=2 ttl=254 time=8.6 ms
64 bytes from 172.20.0.1: icmp_seq=3 ttl=254 time=4.6 ms
64 bytes from 172.20.0.1: icmp_seq=4 ttl=254 time=5.8 ms

--- 172.20.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.6/6.8/9.5 ms
```

Test radius

```
Sw1#show authentication sessions interface ethernet 3/2 details
            Interface:  Ethernet3/2
          MAC Address:  000c.29c2.f3c0
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.41.13
            User-Name:  host/PC1.ge.local
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  C0A832CA0000000C00006B80
     Acct Session ID:  Unknown
               Handle:  0x12000001
      Current Policy:  POLICY_Et3/2

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:
          Vlan Group:  Vlan: 41

Method status list:
       Method           State
       dot1x            Authc Success
```

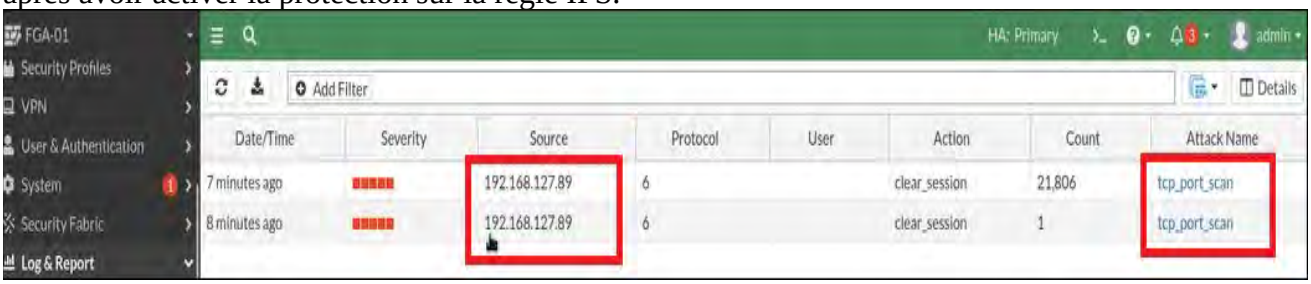
Authentification du VLAN 41

Analyse de la conversation entre switch et serveur



Traçabilité de l'utilisateur connecté au serveur Radius
Sur le serveur Radius on vérifie qui s'est connecté au serveur.

Test d'attaque « Déni de service » sur le system Ubuntu Kali Linux
la réaction du pare-feu face à l'attaque en détectant l'adresse de l'hôte qui a lancé cette attaque, après avoir activer la protection sur la règle IPS.



IV.11 Conclusion

Durant ce dernier chapitre, nous avons réalisé l'ensemble de configuration et mettre en évidence divers tests de fonctionnement de chaque service configuré auparavant, où nous avons constaté leurs bons fonctionnements. Cette étape nous a permis d'atteindre les objectifs visés au début de ce travail.

Conclusion générale

Ce projet de fin de cycle consiste à étudier et améliorer une infrastructure réseau en multicouche, en mettant en pratique les connaissances théoriques à travers des méthodes professionnelles utilisées dans l'entreprise Général Emballage.

Notre stage nous a permis de mieux comprendre le domaine de l'administration et sécurité des réseaux au sein de l'entreprise, et perfectionné nos connaissances grâce à l'implémentation d'un réseau virtuel, ainsi qu'un pare-feu Fortigate.

Au terme de ce mémoire, dans un premier temps, nous avons présenté quelques généralités sur les réseaux et la sécurité informatique puis l'architecture existante du réseau de l'entreprise. Dans un second temps nous avons étudier et améliorer le réseau et proposer nos solutions ensuite nous avons proposé notre infrastructure réseau sous GNS3, ainsi que toutes les installations, et les configurations faîte sur le pare-feu FortiGate, nous avons configurer sur ce dernier la haut disponibilité HA, et crée plusieurs règles de filtrage (politique de sécurité) pour les Vpns afin d'interconnecter les différents sites distants, ainsi que la DMZ le Filtrage Web et Applicatif…etc. Ensuite nous avons appliqué l'authentification Radius sur différents équipements de notre réseau afin de renforcer la sécurité des utilisateurs.

La réalisation de ce modeste travail nous a mené à atteindre nos objectifs fixés dès le début, nous a permis d'enrichir et développer nos connaissances et compétences en réseaux et sécurité informatiques, et s'habituer à régler les problèmes et les difficultés de la simulation et de la réalisation des projets. De plus, cela nous a permis de nous familiariser avec l'environnement de travail et aussi la vie professionnelle, tout en essayant de satisfaire notre besoin pour intégrer dans le travail de l'entreprise.

En perspective, nous souhaitons enrichir notre infrastructure, en lui rajoutant plus de fonctionnalités, aussi enrichir nos connaissances et nos compétences en vue de s'intégrer prochainement dans le milieu professionnel.

Bibilographie

[1] BOUBEKRI Sara et MEBARKI Ryma, 2016, La haute disponibilité des réseaux campus. Casd'étude : Sonatrach, Mémoire de Master, Informatique, Béjaia : Université de A. Mira de Béjaia.

[2] ADJED NOURIA et KISRI TASSADIT,2020, Optimisation du fonctionnement du réseau informatique de l l'entreprise Candia, Mémoire de Master, Informatique, Béjaia : Université de A.Mira de Béjaia.

[3] BENNACER Yasmina et MOKRANI Yasmine,2021, Les outils d'administration et sécurité des réseaux informatiques cas d'étude Sonatrach, Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[4] BELAID Nassima et ARKOUB Chabha, 2011, Services d'accélération des applications et optimisation des liens WAN (WAAS : Wide Area Application services) au niveau de la CNAS d'Alger, Mémoire de master, électronique, TIZI-OUZOU : Université Mouloud Mammeri.

[5] DAHMANI Hanane et YAKOUBEN Roza,2017, Proposition d'une configuration sécurisée d'un réseau local avec les VLANs Cas d'étude : Entreprise Bejaia Méditerranéen Terminal (BMT), Mémoire de Master, informatique, Béjaia : Université de A. Mira de Béjaia.

[6] CHABANE CHAOUCHE nadjet et TAMOURT Yacine, Conception Et Déploiement D'un Réseau Informatique Pour La Transmission Des Données, Mémoire fin d'étude, Université Akli Mohand Oulhaj Bouira.

[7] OUSSALAH Bilal et REDOUANE Salim,2012, Proposition et mise en œuvre d'une solution de segmentation et de routage du réseau LAN étendu de la RTC (Région Transport Centre) Sonatrach BEJAIA, Mémoire d e Master, informatique, Béjaia : Université de A. Mira de Béjaia.

[8] Mehaoued Kamal, 2021/2022, Réseaux informatiques [support de cours]. Béjaia : Université de A. Mira de Béjaia

[9] Mohand YAZID , 2022-2023, Administration des Réseaux [support de cours] Bejaia : Université Abderrahmane Mira Bejaia.

[11] AOUES Ouerdia. Implémentation d'une solution de sécurité en utilisant un firewall de la nouvelle génération Cas Algérie poste de Tizi-Ouzou Mémoire fin d'étude. Réseaux, Mobilités et Systèmes Embarqués Tizi-Ouzou: Université Mouloud Mammeri Tizi-Ouzou, 2022. 96 p.

[13] BOUNOUNI Sara. MECHEROUH Katia. Simulation d'un pare-feu d'entreprise Cas de SONATRACH de Béjaïa. Mémoire fin de cycle. Bejaia : Université Abderrahmane MiraBejaia, 2016. [Consulté le 12 janvier 2023].59 p

[14] Bennai Yani Athmane, BOUAM Amnay. Ethical Hacking : Étude et réalisation de tests de Vulnérabilité. Mémoire fin d'étude. Bejaia. Administration et sécurité des réseaux. Université Abderrahmane Mira Bejaia, 2017. 70 p.

[15] FERROUDJ Nadjet , GOUJIL Nabila . proposition d'une solution sécurisée de réseau intranet d'aire Algérie. Mémoire fin de cycle .Béjaia : Université Abderrahmane Mira Bejaia, 2021.

[16] BELKHATMI Keltouma, BENAMARA Ouarda. Mise en place d'un système de détection etde prévention d'intrusion. Mémoire fin d'étude. Bejaia : Université Abderrahmane MiraBejaia, 2016. [Consulté le 25 janvier 2023].75 p.

[17] HAMMOUMRAOUI Alissia et IDRI Lydia,2021, Virtualisation de la couche infrastructure et application d'un système d'information. Cas d'étude SPA Général emballage, Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[18] William Stallings. Chapitre 11: Firewalls. In Network Security Essentials: Applications and Standards. 4ème édition. Les États-Unis d'Amérique : Pearson, 2011. P 374-397.

[19] MERAD Kenza et MERNACHE Razik, 2015, Techniques de Sécurité pour les Réseaux Locaux d'Entreprise Cas "Amimer Energie", Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[20] SENA Samy et SKLAB Madjid,2017, Installation et configuration d'un VPN pour l'entreprise « Adel Computers », Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[21] Atmani Walid et Ait Atman Faouzi,2015, Etude et simulation des VLAN et d'un pare-feu (pfsens) cas EPB (entreprise portaire Béjaia), Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[22] SIDHOUM Rima et LALAM Kaissa,2020, Configuration et Simulation des VLANs Cas d'étude : AGRANA. Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[23] REDOUANE Idir et AMAOUCHE Youva,2016, Proposition d'une nouvelle architecture LAN et implémentation d'une solution VLAN Cas : SARL « ifri », Mémoire de master, informatique, Béjaia : Université de A. Mira de Béjaia.

[24] Todd Lammle. Chapitre 11: VLANs and Inter-VLAN Routing. In CCNA Routing and Switching complete study guide. 2 ème édition. Les États-Unis d'Amérique : Sybex, 2016. p 424-457.

[25] kemache habiba et Alouache Lynda. La Haute disponibilité des réseaux (HSRP) cas d'étude : réseaux LAN de

Webographie

[10] Tanenbaum Andrew, Feamster Nick, Wetherall David. Chapitre 8 : Sécurité des réseaux. In :Réseaux. 6ème édition. Paris Pearson, 2022. P 783-916. [Consulter le 15 mars 2023]. Disponible à l'adresse : https://www.pearson.fr.

[12] KRVT05-INFORMATIQUE, QU'EST-CE QUE UN RESEAU INFORMATIQUE ? 9 mai 2021 [consulté le 10 février 20223] ; Disponible sur le lien : https://www.cyberuniversity.com/.

[26] https://www.fortinet.com/ [Consulter le 08 septembre 2023].

Résumé

Ce présent mémoire porte sur notre projet de fin cycle master sur l'amélioration de l'infrastructure réseau fait état de l'étude porté sur l'entreprise SPA Général Emballage.

Notre travail consiste à étudier et améliorer une architecture réseau sécurisé par la simulation et l'émulation 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 des tunnels VPN sécurisé ; entre les différents sites distants de l'entreprise, une haute disponibilité, une liste de contrôle d'accès, Authentification des utilisateurs ainsi que diverses fonctionnalités.

Mots clés : GNS3, FortiGate, Général Emballage, VLANs, VPN, HA, AD, Radius, ...

Abstract

This present memory, concerns our end-of-cycle master's project on improving network infrastructure and reports on the study carried out on the company SPA Général Emballage.

Our work is to study and improve a secure network architecture by simulation et emulation 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, Radius, …