République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et télécommunications.

Thème

Étude et mise en œuvre des politiques de sécurité approfondie sur une infrastructure de virtualisation.

Préparé par :

- M.BOUKHEMAL Elhocine
- M.BOUAKIL Zineddine

Dirigé par :

M.BELLAHSENE Hocine

M.LATRECHE Sofiane

M. LAHLOU Mohand Arezki

Examiné par :

Mme. MEZHOUD

M. BESSAAD

Année universitaire : **2022/2023**

Remerciements

Au terme de ce mémoire, nous tenons à remercier tout naturellement en premier lieu le Dieu tout-puissant, qui nous dotait d'une forte volonté et suffisamment de connaissance pour mener à bien ce modeste travail.

Nous remercions notre encadrant M. Hocine BELLAHSENE ainsi que notre co-encadrant M. Sofiane LATRECHE pour leur inspiration, leur aide ainsi le temps qui nous a consacrés.

Un grand merci pour l'organisme d'accueil du " Général Emballage " et on tient particulièrement à adresser nos remerciements pour Monsieur Mohand Arezki LAHLOU pour toute l'aide qu'ils ont pu nous procurer, et pour la transmission de son savoir-faire qui nous a été d'une aide précieuse.

Nos remerciements s'adressent également aux membres de jurys d'avoir accepté d'assister à cette soutenance et d'évaluer notre travail.

Nous tenons à exprimer notre plus sincère gratitude à ceux qui nous ont aidés et contribués au développement de ce travail, et à la réussite de cette année universitaire.

Notre reconnaissance s'adresse à nos familles qui ont su nous apporter, sans relâche, leurs soutiens durant toutes ces longues années d'études.

Enfin, nous tenons à exprimer notre plus sincère gratitude à tous les amis et à toute personne qui nous ont soutenu et encouragé lors de la préparation de ce mémoire.

Table des matières

Listes des abréeviations

AD : Active Directory
DHCP : Dynamic Host Configuration Protocol
DMZ : Demilitarized Zone
DNS : Domain Name System
DRP : Disaster Recovery Plan
ERP : Enterprise Resource Planning
FTP : File Transfer Protocol
GNS3 : Graphical Network Simulator 3
GRE : Generic Routing Encapsulation
HSRP : Hot Standby Router Protocol
HTTP : Hypertext Transfer Protocol
IDS : Intrusion Detection System
IP : Internet Protocol
IEEE : Institute of Electrical and Electronics Engineers
IOS : Internetwork Operating System
IPS : Intrusion Prevention System
IPsec : Internet Protocol Security
LACP : Link Aggregation Control Protocol
LAN : Local Area Network
LS : Ligne spécialisée
MAC : Media Access Control
MAN : Metropolitan Area Network
NAT : Network Address Translation
NFV : Network Functions Virtualization
OSI : Open Systems Interconnection
PAgP : Port Aggregation Protocol
PVLAN : Private Virtual Local Area Network
QoS : Quality of Service
SD-WAN : Software-Defined Wide Area Network
SPA : Société Par Actions
STP : Spanning Tree Protocol
TCP : Transmission Control Protocol
VLAN : Virtual Local Area Network
VoIP : Voice over Internet Protocol
VPN : Virtual Private Network
VRRP : Virtual Router Redundancy Protocol
VTP : Virtuel Trunking Protocole
WAN : Wide Area Network

Introduction générale

Dans ces temps modernes, les entreprises ont largement adopté les réseaux informatiques, qui constituent des ensembles de ressources essentielles pour offrir une multitude de services. L'évolution rapide des services et du trafic a conduit à un développement technologique permettant d'augmenter la capacité et les fonctionnalités de ces réseaux. Cependant, cette évolution a également engendré de nouveaux défis, notamment en matière de sécurité et de redondance.

D'une part, la sécurité est devenue un enjeu majeur dans les réseaux informatiques. Les entreprises doivent faire face à une multitude de menaces, tant internes qu'externes, qui cherchent à exploiter les vulnérabilités du réseau pour accéder à des informations sensibles, perturber les opérations ou causer des dommages. La protection des données et des ressources est donc primordiale, nécessitant la mise en place de politiques et de mesures de sécurité appropriées.

D'autre part, la redondance joue un rôle crucial dans la continuité des services au sein des réseaux. Les pannes matérielles, les erreurs humaines ou les catastrophes naturelles peuvent entraîner des interruptions de service coûteuses pour les entreprises. La redondance permet de mettre en place des systèmes de secours et des mécanismes de récupération qui garantissent la disponibilité continue des services, même en cas de défaillance d'un élément critique.

Ainsi l'entreprise général emballage ne fait pas exception à cette règle car la nécessité de protéger les données stratégiques, les services disponibles et la fragilité du réseau actuel aux différentes attaques internes et externes est primordiale. Ainsi, il nous a été confié la tâche d'améliorer et de mettre en œuvre une architecture réseau qui réponde à ces exigences au sein de l'entreprise. Notre objectif est de concevoir un réseau robuste et hautement disponible, capable de maintenir les opérations critiques en toutes circonstances. En mettant en place des mécanismes de redondance et de récupération en cas de défaillance, nous assurerons la continuité des services et réduirons les risques d'interruption. Grâce à cette architecture, Général Emballage pourra renforcer sa position en tant qu'entreprise fiable et performante, prête à faire face aux défis technologiques actuels et futurs.

Tout d'abord nous donnerons un aperçu sur les réseaux informatique, ensuite dans le deuxième chapitre l'objet de notre étude va se porter sur la présentation de général emballage et nous concentrerons aussi notre attention sur les critiques des parties réseau et sécurité de l'architecture existante et nous proposerons d'une éventuelle solution et pour le troisième chapitre aborde l'administration et la sécurité avancées des réseaux informatiques, Puis le quatrième chapitre sera consacré à la mise en œuvre de quelques améliorations, et enfin nous terminerons notre mémoire par une conclusion générale.

Chapitre 1

Généralités sur les réseaux informatiques.

1.1 Introduction

De nos jours, le monde est de plus en plus connecté, et les réseaux informatiques jouent un rôle essentiel dans cette connectivité. Que ce soit pour accéder aux données ou de communiquer avec d'autre appareils. Les réseaux informatiques sont omniprésents et essentiels pour le fonctionnement de nombreux aspects de notre vie quotidienne. Dans ce chapitre. Nous allons explorer les généralités des réseaux informatiques. Nous allons nous concentrer sur les aspects clés qui permettent de comprendre leur fonctionnement et leur utilité. Nous verrons comment les réseaux informatiques sont conçus pour permettre la communication entre les différents appareils. Nous allons également les déférents types des réseaux informatiques, ainsi que les alternatives de raccordements et les topologies couramment utilisées dans les réseaux informatiques.

1.2 Un réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et de périphériques reliés entre eux qui communiquent les uns avec les autres pour partager des ressources, notamment des fichiers, des imprimantes, des bases de données et des applications, ainsi que pour échanger des données. Les réseaux informatiques permettent de connecter des ordinateurs géographiquement séparés et de partager efficacement des informations. Ils peuvent être utilisés dans des environnements résidentiels, commerciaux et industriels et peuvent être constitués d'une variété de technologies, y compris le câblage en cuivre, les câbles en fibre optique, les réseaux sans fil et les téléphones cellulaires. Les réseaux informatiques peuvent être utilisés pour diverses applications, telles que le partage de fichiers, le partage de périphériques, la communication en temps réel, l'accès à distance, la collaboration en ligne, le commerce électronique, entre autres.[1]

1.3 Classifications des réseaux informatiques

Il existe plusieurs type des réseaux informatiques qu'on peut les classifier selon la portée ces derniers comme suite[2] :

1.3.1 LAN (Local Area Network)

est un réseau local permettant de relier des équipements qui se situe à proximité.

1.3.2 MAN (Metropolitan Area Network)

est un réseau qui peut contenir plusieurs réseaux locaux (LAN) géographiquement à proximité.

1.3.3 WAN (Wide Area Network)

est un réseau étendu couvrant une large zone géographique à l'échelle d'un pays.

1.4 Les normes de communications réseau

1.4.1 Le Modèle OSI (Open Systems Interconnection)

est un modèle théorique apparait en 1984 dont le but est de définir des normes de communications entre différents systèmes informatiques. Le modèle OSI se compose de 7 couches[3] :

FIGURE 1.1 – Les sept couches du modèle OSI .

La couche physique

c'est la première couche dans le modèle OSI, elle s'occupe de la transmission des bits de façon brute sur le canal de transmission, cette couche doit garantir la parfaite transmission des données.

La couche liaison de données

son principal rôle est d'acheminer les données entre deux stations directement connectées au même support physique.

La couche réseau

c'est la couche qui permet de relier des sous-réseaux, le routage de paquets et l'interconnexion dans ces sous-réseaux.

La couche transport

cette couche est responsable du bon acheminement des messages complets au destinataire, ainsi que l'optimisation des ressources de réseau. La couche transport est aussi responsable de type de services à fournir pour la couche session. C'est l'une des couches les plus importantes car elle fournit le service de base de l'utilisateur.

La couche session

cette couche se charge de l'organisation et la synchronisation entre tâches distantes, elle établit le lien entre les adresses logiques et les adresses physique des tâches réparties.

La couche présentation

cette couche s'occupe de la syntaxe et la sémantique des données transmises, cette couche peut convertir les données, les reformater, les crypter et les compresser.

La couche application

c'est la dernière couche de modèle OSI, elle représente le point de contacte entre l'utilisateur et le réseau, donc c'est cette couche qui va apporter à l'utilisateur les services de base offerts par le réseau.

1.4.2 Le modèle TCP/IP

ce modèle est développé par le département de la défense des Etats-Unis pour assurer une transmission précise et adéquate des données entre les équipements. Il divise le message en paquet afin d'éviter d'avoir à renvoyer l'intégralité du message en cas de problème de transmission. Le modèle TCP/IP peut être décrit comme une architecture réseau à 4 couches [3] :

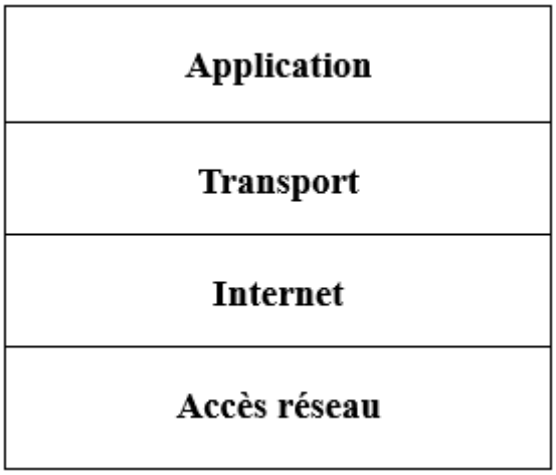

FIGURE 1.2 – Les couches du modèle TCP/IP .

La couche accès réseau

c'est la couche qui définit la manière d'envoie des données, elle gère l'acte physique d'envoie et la réception de données, ainsi qu'elle assure la transmission des données entre les périphériques dans un réseau.

La couche Internet

c'est la couche qui permet l'envoie et le contrôle des données dans un réseau en fournissant des fonctions et des procédures de transfert des séquences de données entre les applications et les périphériques sur les réseaux.

La couche transport

c'est la couche qui garantie la fiabilité et la qualité d'une connexion de données, c'est dans ce niveau que les données sont divisées en paquets et numérotées pour créer une séquence.

La couche application

c'est à ce niveau que les utilisateurs interagissent généralement, cette couche combine les couches session, présentation et application du modèle OSI.

1.5 Architecture réseau

1.5.1 Architecture poste à poste

L'architecture poste à poste appelée aussi point à point, ou en anglais peer to peer, ne comportent d'habitue qu'un nombre minimal de postes car chaque utilisateur est considéré comme administrateur de sa propre machine, autrement dit qu'il n'y a pas d'administrateur central, ni de la hiérarchie entre les postes. Dans un réseau poste à poste, chaque utilisateur est à la fois un client et serveur, toutes les stations ont le même rôle, il n'y a pas de statut privilégié pour l'une des stations. Les réseaux point à point sont déployés pour des petits réseaux ce qui permet le travaille en groupe.[4]

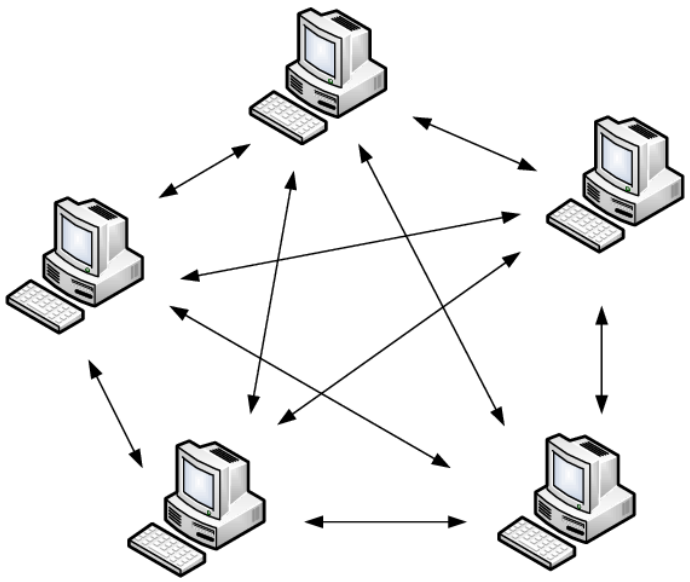

FIGURE 1.3 – Une architecture poste à poste [5].

1.5.2 Architecture client/serveur

Une architecture client/serveur est un modèle de conception informatique dans lequel les tâches sont réparties entre deux types de programmes : client et serveur. Le client est généralement le périphérique qui demande des services ou des ressources auprès des serveurs, qui sont des programmes ou équipements centralisés qui s'occupent de la gestion et la distribution des services et des ressources demandées par les clients. Les postes serveurs en général se dispose des machines puissantes et performantes, qui peuvent être dédiées à une certaine tâche qu'on peut citer [4] :

- Les serveurs d'application (application de base de données et application bureautique)
- Les serveurs de messagerie
- Les serveurs PROXY pour accéder à internet
- Les serveurs web

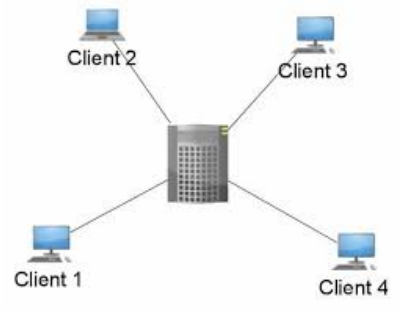

FIGURE 1.4 – Une architecture client/serveur[6].

1.6 Topologie physique

La topologie physique c'est la façon dont les périphériques ou les équipements sont reliés entre eux dans un réseau informatique, elle décrit la manière dont les câbles sont utilisés pour connecter les différents équipements tels que les commutateurs, les pares-feux et les routeurs. Il existe plusieurs topologies physiques dans un réseau informatique[7] :

1.6.1 Topologie en bus

Tous les équipements du réseau sont reliés à un câble unique appelé le bus, les données sont transmises dans ce câble et reçus par tous les équipements qui partagent une seule bande passante. Cette topologie est simple et peu coûteuse, mais elle n'est pas fiable car si le câble tombe en panne, tout le réseau sera affecté ainsi que les données sont envoyées à tous les périphériques ce qui peut rendre les données vulnérables aux attaques malveillantes. La topologie en bus est illustrée dans la figure 1.9 [7] :

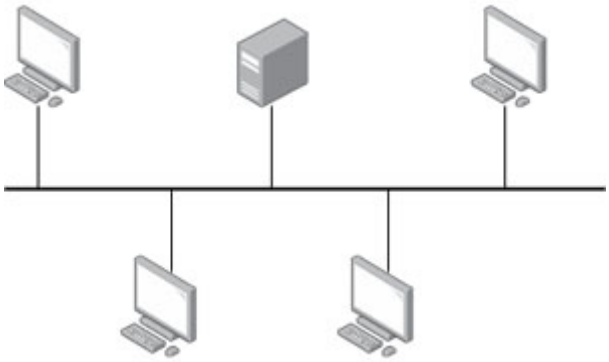

FIGURE 1.5 – La topologie en bus [8].

1.6.2 Topologie en étoile

tous les terminaux sont connectés à un commutateur central, dans cette configuration, chaque périphérique est relié directement au concentrateur et les communications entre périphériques passent par le concentrateur. Dans un réseau de topologie en étoile, si un périphérique échoue, cela n'affecte pas les autres périphériques du réseau. Cependant, la topologie en étoile peut être plus coûteuse que la topologie bus, car elle nécessite plus de câblage et plus de commutateurs pour connecter un grand nombre de périphériques. En outre, si le commutateur tombe en panne, tout le réseau peut être affecté. La topologie en étoile est illustrée dans la figure 1.10[7] :

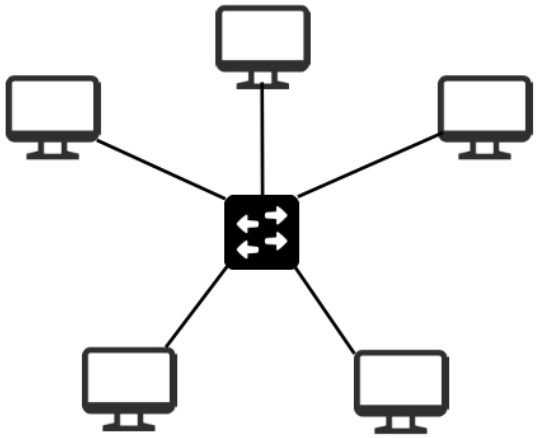

FIGURE 1.6 – La topologie en étoile [9].

1.6.3 Topologie en anneau

tous les équipements sont connectés en série pour former une boucle, chaque périphérique est connecté à deux autres périphériques de sorte de créer un anneau. Les données circulent dans un seul sens autour de l'anneau, de périphérique en périphérique, jusqu'à ce qu'elles atteignent leur destination. Chaque périphérique examine les données qui circulent sur l'anneau et les transmet à leur destination ou les passe simplement au périphérique suivant s'ils ne sont pas destinés à eux. La topologie

en anneau peut avoir des problèmes de bande passante, car chaque équipement doit attendre son tour pour transmettre sur l'anneau, de plus, la topologie n'est pas fiable, car un équipement malveillant peut intercepter les données qui circulent dans l'anneau, la topologie en anneau est exhibée dans la figure 1.11[7] :

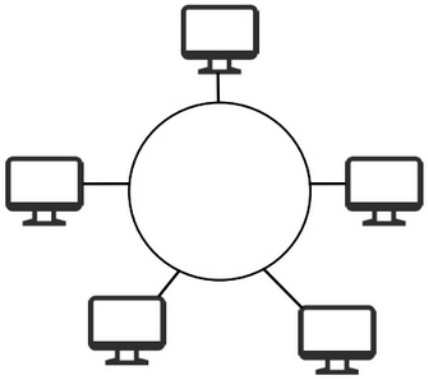

FIGURE 1.7 – La topologie en anneau [9].

1.6.4 Topologie maillée

chaque périphérique du réseau informatique est relié à tous les autres périphériques, créant ainsi un maillage de connexion, dans cette topologie chaque périphérique peut directement communiquer avec tous les autres périphériques, ceux qui rend le réseau résistant aux pannes. Cependant, la topologie maillée est trop coûteuse à mettre en place car elle nécessite un grand nombre de câble, ainsi la configuration et la maintenance du réseau peuvent être compliquées en raison du grand nombre de connexions à gérer. La topologie maillée est illustrée dans la figure 1.12 [7] :

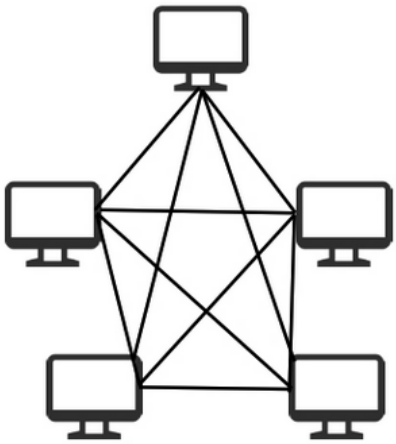

FIGURE 1.8 – La topologie maillée[9] .

1.7 Conclusion

En conclusion, ce chapitre à couvert les généralités des réseaux informatique en expliquant leurs utilités et les types de réseaux informatiques, les normes de communications ainsi que les différentes topologies souvent utilisées dans les réseaux informatiques. Ce chapitre est conçu pour mieux comprendre les avantages et les défis associés à leur utilisation et pour prendre des décisions éclairées en matière de conception, de mise en œuvre et de gestion de réseaux informatiques. Le chapitre suivant sera consacré à l'étude d'existant de l'infrastructure réseau de l'entreprise SPA Général Emballage afin de s'en soulever les problématiques de cette dernière, ainsi de définir nos objectifs pour apporter les solutions nécessaires.

Chapitre 2

Présentation de l'organisme d'étude :problématique et solutions.

2.1 Introduction

L'architecture réseau et la mise en disponibilité sont deux éléments clé dans le bon fonctionnement d'une entreprise moderne. Dans le cadre de notre étude, nous allons nous intéresser à la société Général Emballage, spécialisée dans la production d'emballages pour les entreprises alimentaires et pharmaceutiques. Pour garantir une production efficace et une gestion optimale de leurs processus, il est primordial que leur architecture réseau soit bien conçue et que leur infrastructure soit disponible en permanence. Dans ce chapitre, nous allons donc nous pencher sur l'étude de l'architecture réseau de Général Emballage ainsi que sur les mesures prises pour assurer la mise en disponibilité de leur système.

2.2 Présentation de Général Emballage :

Général Emballage est une entreprise algérienne spécialisée dans la fabrication et la transformation de carton ondulé. Créer par RAMDANE BATOUCHE en 2000 qui assure aujourd'hui les fonctions PDG de l'entreprise. Général Emballage est un leader en Algérie de l'industrie du carton ondulé, elle fabrique à la commande, des plaques double-face (cannelure B, C, E et F) et double-double (BC et BE) des emballages et des displays. Et réalisons des post-impressions en haute résolution jusqu'à 6 couleurs avec vernis intégral ou sélectif. L'équipe équipes hautement qualifiée maîtrise toutes les étapes de la production, de l'étude et prototypage à la fabrication et à la livraison.

Depuis son entrée en exploitation en 2002, General Emballage a connu une croissance rapide et dispose actuellement de trois sites industriels à Akbou, Oran et Sétif avec plus de 1200 employés. Ils sont fiers d'être certifiés conforme au système de management intégré Qualité-Santé et Sécurité au travail (S et ST) - Environnement (ISO 9001 :2015, ISO 14001 :2015, ISO 45001 :2018), témoignant ainsi de leur engagement envers la qualité de leur produits et la sécurité de leurs employés.

2.3 Organigramme de l'entreprise :

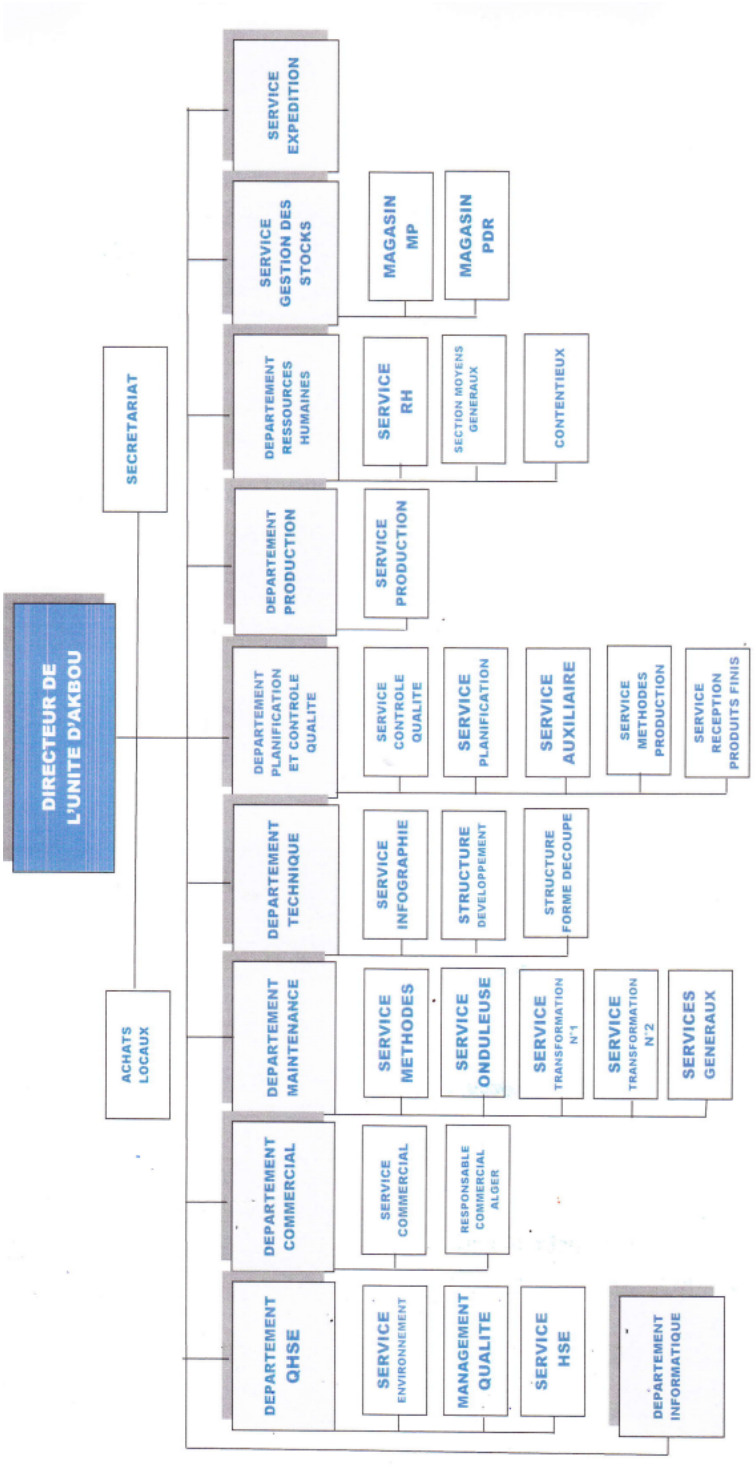

FIGURE 2.1 – Organigramme de l'entreprise [10].

2.4 Présentation de service d'accueil (département informatique)

La dimension de département informatique a un impact considérable sur les opérations de l'entreprise, car il est très présent et visible dans la communication, la gestion et la maintenance des données et des informations au sein de l'entreprise.

2.4.1 Rôle de département informatique

Le département informatique joue un rôle essentiel dans une entreprise. Voici quelques-unes de ses fonctions principales :

• Gestion des systèmes informatiques : le département informatique est responsable de la gestion des systèmes informatiques de l'entreprise, y compris les serveurs, les réseaux, les bases de données et les applications.

• Sécurité informatique : le département informatique est chargé de protéger les données et les systèmes de l'entreprise contre les menaces internes et externes, notamment les virus, les hackers, les tentatives de phishing et les fuites de données.

• Support technique : le département informatique fournit un support technique aux employés de l'entreprise pour résoudre les problèmes informatiques tels que les pannes de matériel et de logiciel, les problèmes de réseau et les problèmes de sécurité.

• Développement d'applications : le département informatique peut être chargé de développer des applications personnalisées pour répondre aux besoins spécifiques de l'entreprise.

• Gestion de projet : le département informatique peut être impliqué dans la gestion de projets informatiques de grande envergure, tels que la mise en place d'un nouveau système ERP ou la migration vers le cloud.

• Gestion de données : le département informatique est responsable de la gestion des données de l'entreprise, y compris la sauvegarde, l'archivage et la récupération en cas de catastrophe.

• Planification et budgétisation : le département informatique est impliqué dans la planification stratégique de l'entreprise et élabore un budget pour les projets informatiques, l'achat de matériel et la formation du personnel.

En résumé, le département informatique est responsable de la gestion, de la sécurité et de l'optimisation des systèmes informatiques de l'entreprise afin de garantir une disponibilité, une performance et une sécurité optimales.

2.5 Étude de l'existant

L'étude d'existant dans une entreprise est une étape cruciale pour comprendre l'état actuel de son infrastructure informatique. Dans le cas de l'étude de l'architecture réseau de l'entreprise, il s'agit d'analyser les différents éléments du réseau tels que les serveurs, les postes de travail, les commutateurs, les pare-feu, les équipements de téléphonie, etc. Cette analyse permet de déterminer la topologie du réseau, de repérer les éventuelles failles de sécurité, de mesurer les performances, d'identifier les zones à risque et d'évaluer les besoins futurs en matière d'investissements et de mises à niveau. L'étude d'existant est donc une étape incontournable pour toute

entreprise souhaitant améliorer son infrastructure réseau et garantir un niveau de sécurité optimal.

2.5.1 Présentation du réseau informatique de Général Emballage

Général Emballage dispose d'un grand réseau interne qui permet de relier les différentes unités a la direction. L'entreprise se base sur l'architecture hiérarchique dont on trouve des équipements de marque FORTINET telle que les pares-feux et aussi CISCO pour les switchs. La figure 2.2 illustre le schéma du réseau informatique de Général Emballage.

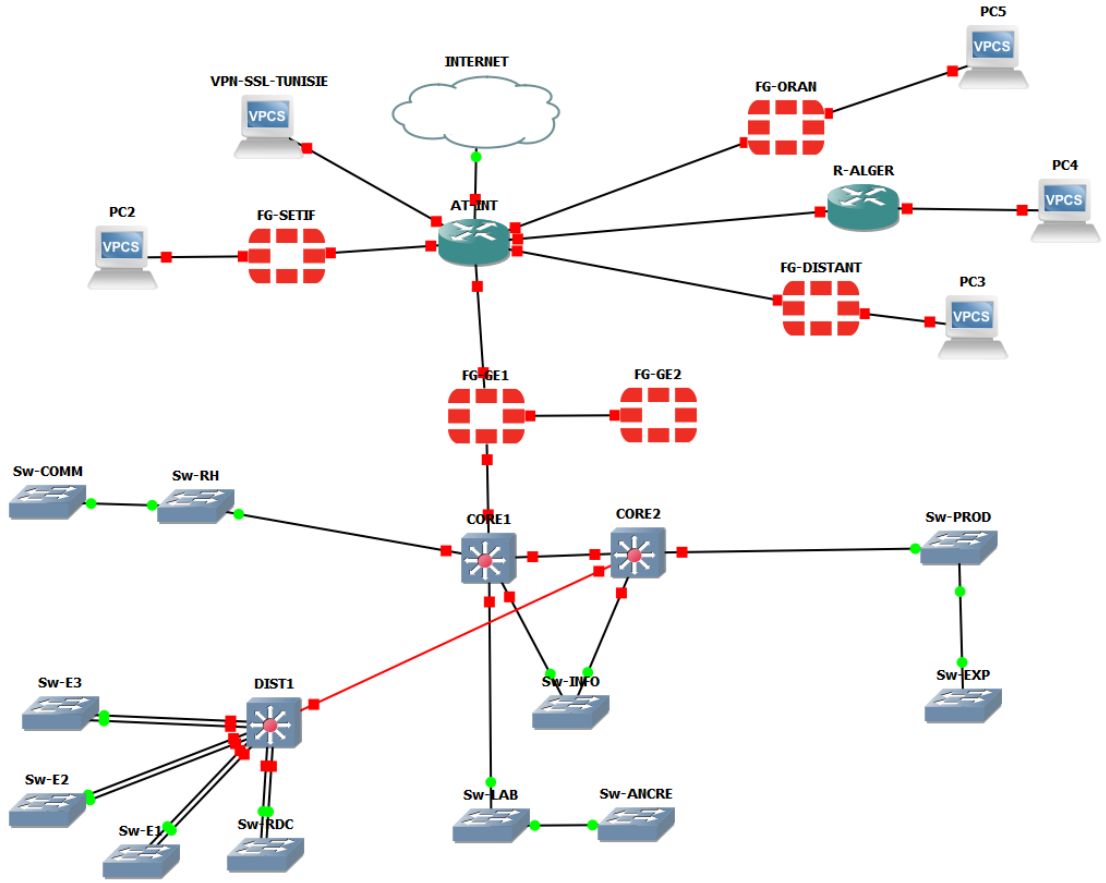

FIGURE 2.2 – Architecture réseau de Général Emballage.

2.5.2 Matériels utilisés dans l'architecture

• Pare-feu FortiGate

un dispositif de sécurité informatique qui permet de contrôler les échanges de données entre un réseau informatique et Internet, ou entre différents réseaux informatiques. Son rôle est de filtrer les connexions entrantes et sortantes en fonction de règles de sécurité prédéfinies, afin de protéger le réseau contre les attaques provenant d'Internet ou d'autres réseaux. Et dans notre cas, SPA Général emballage utilise le pare-feu FortiGate 501E exhibé dans la figure 2.3 :

FIGURE 2.3 – Pare-feu FortiGate[11] .

• Switch Cisco Catalyst 3750

est un type de commutateur réseau haut de gamme, généralement utilisé dans les grandes entreprises et les centres de données pour interconnecter différents réseaux et fournir une bande passante élevée et une faible latence. Le rôle principal d'un switch core est de fournir un accès rapide et efficace à des ressources réseau tell que des serveurs, des applications et des dispositifs de stockage en réseau. Il peut également fournir des services de qualité de service (QoS) pour garantir une bande passante appropriée pour des applications spécifiques et des niveaux de priorité de trafic. Le switch Cisco 3750 est illustré dans la figure 2.4.

FIGURE 2.4 – Switch CORE Cisco Catalyst 3750 [12].

• Switch d'accès Cisco 2960

est un dispositif de réseau local (LAN) qui permet de connecter différents périphériques réseaux tels que des ordinateurs, des imprimantes, des téléphones IP, des caméras de surveillance et d'autres équipements réseau. Il est généralement installé dans les armoires de câblage, les bureaux et les salles informatiques pour fournir une connectivité réseau local. Le rôle d'un switch d'accès est de fournir une connectivité

réseau local aux différents périphériques du réseau, de segmenter le trafic réseau, de prioriser les applications et les données importantes et d'offrir des fonctionnalités de gestion de réseau avancées. Le switch Cisco Catalyst 2960 est exhibé dans la figure 2.5.

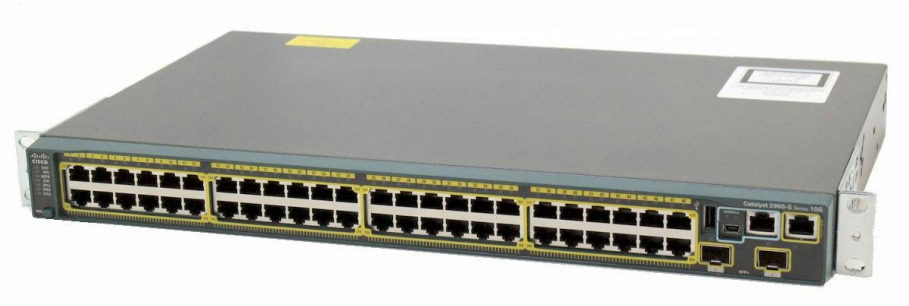

FIGURE 2.5 – Switch d'accès Cisco Catalyst 2960[13] .

2.6 Critique de l'architecture actuelle de l'entreprise

Durant notre stage au sein de SPA Général Emballage, l'étude que nous avons menée sur l'architecture nous a permis de détecter les faiblesses réseaux suivantes :

• Certains switches sont reliés en cascade, ce type de liaison est problématique car s'il y a :

— Augmentation de risque de perte de données : si l'un des switches rencontre un problème, cela provoque une perte de données pour les switches connectés à la chaine.

— Augmentation de temps de latence : lorsqu'un paquet de données doit traverser plusieurs switches en cascade, cela peut entraîner une augmentation du temps de latence, ce qui peut affecter les performances du réseau.

— Augmentation de la charge de broadcast : Les émissions de broadcast se propagent à travers tous les switches en cascade, ce qui peut augmenter la charge de broadcast sur le réseau.

• L'absence de liens et d'équipements en redondance crée plusieurs points vulnérables dans l'architecture du réseau. En effet, en cas de défaillance d'un composant, cela peut entraîner une interruption de service et une panne du réseau, car il n'y a pas de dispositif de secours pour prendre le relais.

• Fin de support pour les équipements (switch d'accès) qui signifie que les équipements ne reçoivent pas de mise à jour, cela peut avoir des implications sur la sécurité, la fiabilité et la compatibilité des équipements.

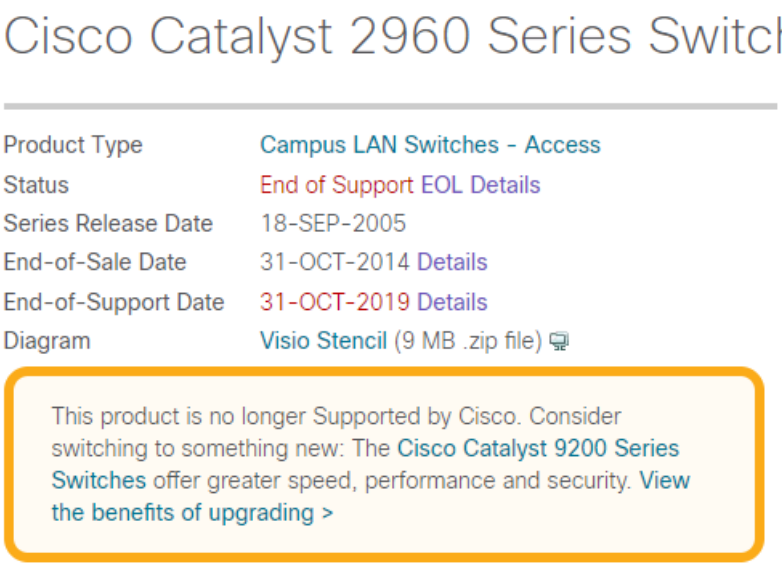

FIGURE 2.6 – Annonce de fin de prise en charge par Cisco[14] .

• Exposition de l'entreprise à un large éventail de menaces potentielles telles que les attaques par injection, les tentatives d'accès non autorisées et les attaques de déni de service.

2.7 Planification d'une solution adaptée

Après avoir effectué une étude approfondie du réseau de l'entreprise SPA Général Emballage, nous avons identifié la nécessité d'améliorer la sécurité et la performance du système. Par conséquent, nous prévoyons de mettre en place une nouvelle architecture basée sur une politique de sécurité robuste et durable.

Lors du choix de cette solution, nous prendrons en compte plusieurs critères essentiels. Nous évaluerons la capacité de la nouvelle architecture à assurer la redondance et la disponibilité du réseau, en garantissant la continuité des services en cas de défaillance d'équipements ou de liens de communication. Nous accorderons une attention particulière à la simplification de la gestion et de la configuration du réseau, afin de faciliter les opérations tout en maintenant des performances élevées.

La sécurité sera un critère majeur, avec l'utilisation de pare-feu, la segmentation du réseau et la création de zones démilitarisées (DMZ) distinctes pour protéger les données et réduire les risques d'intrusion malveillante.

Enfin, nous veillerons à ce que la nouvelle architecture soit évolutive et capable de tirer parti des dernières avancées technologiques en matière de traitement, de stockage et de communication de l'information.Par la suite, nous mettrons en œuvre cette politique de sécurité robuste et cette nouvelle architecture pour répondre aux besoins spécifiques de SPA Général Emballage.

2.8 Conclusion

Tout au long de ce chapitre, nous avons présenté la société Général Emballage, son réseau ainsi que les équipements dont cette dernière dispose, et par la suite nous avons exposé notre problématique et la solution envisagée.

Cette dernière se résume principalement à l'amélioration de l'ancienne architecture du réseau de générale emballage en une nouvelle architecture qui assure plus de disponibilité et de fiabilité. Le chapitre suivant sera dédié à la réalisation et le test de notre solution en présentant les d'efférents protocoles utilisés et leur configuration qui nous permettra d'avoir un réseau d'une haute disponibilité.

Chapitre 3

Ensemble des techniques utilisées lors de la mise en place de la solution envisagée.

3.1 Introduction

Dans le monde numérique, l'administration des réseaux informatique implique la gestion, la configuration et le contrôle des différents équipement du réseau. Une administration efficace garantit une performance optimale du réseau, une gestion des ressources efficace et une résolution rapide des problèmes.

Ce chapitre aborde l'administration et la sécurité avancées des réseaux informatiques. Dans le monde numérique d'aujourd'hui, où les réseaux jouent un rôle essentiel dans la connectivité, la communication et le partage d'informations, il est crucial de mettre en place des mesures robustes pour administrer et protéger ces réseaux.

Dans ce chapitre nous allons illustrer les architecture réseaux à plusieurs niveaux, ainsi que les réseaux locaux virtuels, leurs types et les avantages de ces derniers. Nous allons aussi définir les différents protocoles souvent utilisés pour la sécurité et la gestion des réseaux informatique pour une meilleur fiabilité et efficacité de ces derniers,avant de proposer la nouvelle topologie.

3.2 Architecture réseau à plusieurs niveaux : Modèles à deux couches et à trois couches

3.2.1 Architecture réseau à deux couches

Une architecture réseau à deux couches, notamment appelé architecture à deux niveaux, est une approche de conception utilisées dans les infrastructures réseaux. Cette architecture est basée sur la segmentation de réseau à deux couche distinctes : couche coeur-distribution combinée et couche accès[15].

Couche coeur-distribution

c'est la couche responsable de la commutation et du routage du trafic dans tout le réseau, il relie les différents sites, les réseaux internes et externes de l'organisation et assure une connectivité à haut débit entre eux. Cette couche est généralement composée des commutateurs et des routeurs haut de gamme, pour gérer le trafic élevé qui circule dans le réseau et fournir des performances optimales.

Couche accès

cette couche se situe en dessous de la couche coeur-distribution, elle se compose généralement des commutateurs d'accès qui permettent au équipements finaux de se connecter au réseau de l'organisation, tels que des ordinateurs, des imprimantes. Cette couche peut également inclure des points d'accès sans fil pour prendre en charge la connectivité Wi-Fi.

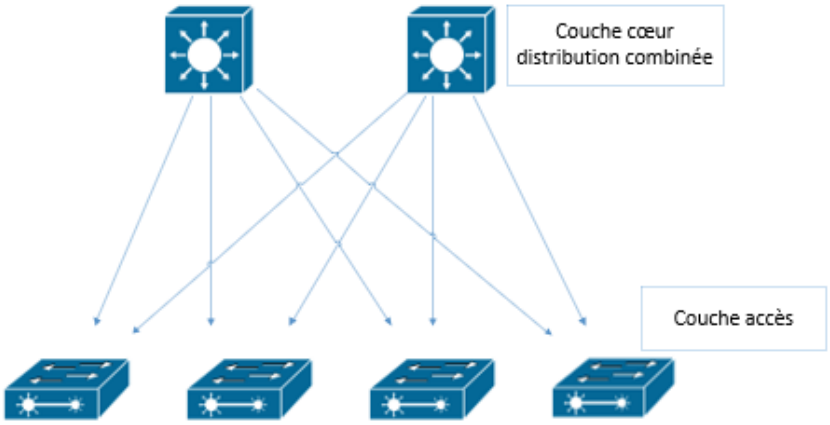

FIGURE 3.1 – Architecture réseau à deux couches.

3.2.2 Architecture réseau à trois couches

Également appelé architecture à trois niveaux, l'architecture à trois couches est une approche de conception dans laquelle le réseau est segmenté en trois couches distinctes : la couche coeur, la couche distribution et la couche d'accès. Cette architecture est souvent utilisée dans les environnements d'entreprise où des exigences de performance, de sécurité et de gestion sophistiquées sont nécessaires[15].

Couche coeur

La couche coeur est responsable de la connectivité des équipement de la couche distribution, ainsi que c'est le portail de réseau interne vers d'autres réseaux externes. La couche coeur se compose des équipements haut de gamme, car elle permet de transportée un gros volume de trafic du réseau.

Couche distribution

Cette couche prend le rôle d'intermédiaire entre la couche coeur et la couche d'accès, elle est responsable de la distribution du trafic provenant du niveau coeur vers sous-réseaux du réseaux, ainsi qu'elle assure la connectivité entre les différents départements, sites et groupes d'utilisateurs.

Couche accès

C'est le niveau inférieur de l'architecture réseau à trois couches, cette couche comprend des commutateurs d'accès qui permettent au terminaux de se connecter au réseau de l'organisation

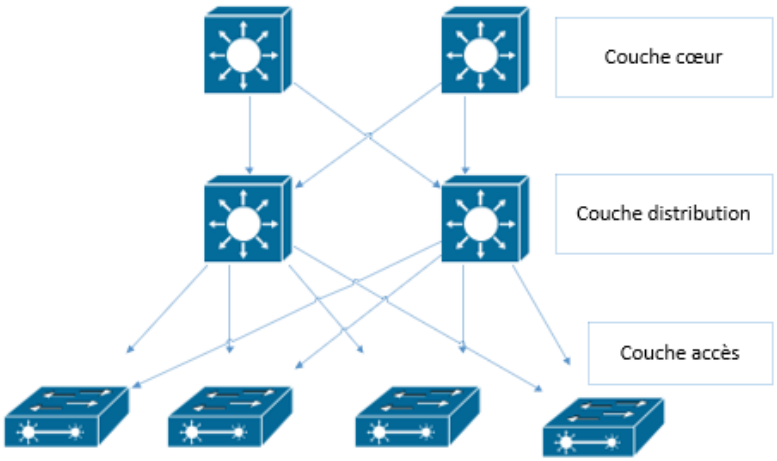

FIGURE 3.2 – Architecture réseau à trois couches

3.3 Services d'administration et gestion réseau

Les services d'administration et de gestion réseau englobent différentes fonctionnalités et services pour assurer le contrôle, l'optimisation et l'organisation des ressources réseau. Parmi ces services, on trouve [16] :

3.3.1 Domain Name System (DNS)

Plutôt que retenir des adresses IP par des humaines n'est pas si facile, il est vite devenu plus simple de travailler avec des nom. C'est pour cela que le DNS est inventé,il permet de traduire les noms de domaines conviviaux par les utilisateurs en des adresses IP compréhensibles par des machine informatique[16].

3.3.2 Dynamic Host Configuration Protocol (DHCP)

c'est un protocole de gestion des réseaux informatiques qui permet d'attribuer des adresses IP automatiquement aux clients du réseau, le DHCP permet de simplifier la gestion des adresses IP en fournissant une allocation dynamique, ainsi qu'il évite les conflits d'adresses IP et facilite la gestion des équipement réseau[17].

3.3.3 Active Directory (AD)

C'est un service principalement utilisé dans les environnements Windows, il permet de centraliser et de gérer les informations sur les utilisateurs, les groupes, les ordinateurs et les ressources du réseau. AD fournit également des services d'authentification et d'autorisation, facilitant ainsi l'accès sécurisé aux ressources du réseau[17].

3.4 Les réseaux locaux virtuels (VLAN)

Le VLAN est un groupe réseau local regroupant un groupe de machines de façon logique et non physique, ces stations pourront communiquer comme si elles étaient dans un même segment. Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs[18].

3.5 Type de VLAN

Il existe plusieurs types de réseaux locaux virtuels, parmi eux on trouve[18] :

3.5.1 VLAN de niveau 1

Appelé aussi des VLAN par ports, c'est une méthode consiste à attribuer des VLAN spécifiques à des ports physiques sur un commutateur réseau, cela permet de segmenter le réseau en fonction des emplacements physiques des périphériques connectés[18].

3.5.2 VLAN de niveau 2

Nommé également des VLAN par adresses Mac, c'est une méthode basée à l'attribution des VLAN par des adresses MAC des équipements. Ce type de VLAN est plus souple que les VLAN par ports, car il est totalement indépendant de la localisation de la station[18].

3.5.3 VLAN de niveau 3

on distingue plusieurs type de VLAN de niveau 3 :

— **VLAN par sous-réseau** associe des sous-réseau selon l'adresse IP de datagrammes, il offre une configuration automatique des VLAN en fonction des déplacements des stations, simplifiant ainsi la gestion du réseau[18].

— **VLAN par protocole** permettant de créer des réseaux virtuels par type de protocole, regroupant ainsi toute les machines utilisant le même protocole au seins d'un même réseau[18].

3.5.4 VLAN natif

Il s'agit d'un VLAN par défaut sur des commutateurs réseaux où les trames sont pas marquées avec des étiquettes VLAN, il est généralement utilisé dans les commutateurs qui ne prennent pas en charge les l'étiquetage VLAN[19].

3.5.5 VLAN isolé

Nommé aussi isolated VLAN en anglais, est un type de VLAN configuré de manière que les dispositifs qui y sont connectés ne puissent pas communiquer entre

eux, où chaque port est isolé, créant ainsi des segments distincts. Cela permet de restreindre la diffusion des données et d'améliorer la sécurité[19].

3.5.6 VLAN communautaire

Ce type de vlan est configuré de façon que les équipements qui appartient à ce VLAN peuvent se communiquer entre eux, mais pas avec les ports d'autres VLANs, à moins qu'ils ne soient explicitement autorisés[19].

3.6 La gestion des VLAN

3.6.1 VLAN voix

C'est un type de VLAN utilisé pour séparer et prioriser la voix de différents autres données du réseau, c'est un VLAN utilisé dans des organisation exploitant la téléphonie dans leur réseau. Il assure une qualité de service optimale concernant les communications vocaux[19].

3.6.2 VLAN data

Il s'agit d'un VLAN dédié spécifiquement pour le transport de données informatiques, tels que les e-mails, le transfert de fichiers, la navigation sur Internet. Il permet de séparer le données des autres types de trafics, comme la voix et la vidéo. afin d'assurer une qualité de service adaptée à chaque type de trafic et de garantir une gestion efficace des ressources réseau[19].

3.6.3 VLAN management

C'est un type de VLAN utilisé pour la gestion et l'administration des équipements réseaux tels que les commutateurs, les routeurs. Il est utilisé pour séparer le trafic de gestion du reste de trafic.Le VLAN management facilite la configuration, la surveillance et la maintenance de ces équipements[19].

3.7 Les VLANs privés

Le VLAN privé (PVLAN), également connu sous le nom d'isolation de port, est une technologie de segmentation de réseau pour les réseaux de couche 2 qui permet l'isolation des ports ou la segmentation du trafic sous le même segment IP.

En appliquant le VLAN privé dans un environnement de réseau partagé, cela permet d'économiser des adresses IP et d'améliorer la sécurité des ports de commutation dans la couche 2. Les VLAN privés ont plusieurs avantages, tels que la facilitation de la gestion des adresses IP et la configuration des équipements réseau, en évitant les conflits d'adresses et en simplifiant le routage du trafic.

De plus, ils peuvent aider à maintenir une sécurité accrue en limitant le trafic autorisé entre différents ports d'un même VLAN privé.

Cependant, la configuration des VLAN privés peut être complexe et nécessite une bonne connaissance des protocoles de réseau et des équipements. Il est donc important de planifier soigneusement la configuration des VLAN privés et de documenter la procédure pour éviter les erreurs et les problèmes de sécurité[20].

3.8 Les avantages des VLANs

• Augmentation des performances : La segmentation créée par les VLAN réduit la taille des domaines de broadcast et de ce fait le nombre de collisions sur ces domaines. De plus, les VLAN se basent sur la commutation (et non le routage) pour segmenter les domaines de diffusion ce qui permet un traitement bien plus rapide[18].

• Formation de groupes virtuels : Il est courant de retrouver, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, composés de membres qui viennent de différents départements (production, vente, etc.). Ces groupes sont souvent formés pour un temps défini et à courte durée. Dans ce cas de figure, un VLAN pourrait être implémenté (sans avoir à déplacer les individus) pour les besoins ponctuels de ce groupe et ce pour plusieurs[18].

• Meilleure sécurité : Les VLAN permettent de limiter l'accès aux ressources réseau en fonction des besoins, ce qui réduit les risques de sécurité liés à des accès non autorisés[18].

• Réduction des coûts : L'utilisation de VLAN permet de simplifier l'administration du réseau. A chaque fois qu'un utilisateur change de LAN, il faut modifier l'adresse du poste et certains paramètres des routeurs. Tandis que si un utilisateur change de lieu physique mais pas de VLAN, il peut ne pas y avoir de modifications à faire (sous réserve de disposer de bons outils de gestion des VLAN). De plus, l'utilisation des VLAN entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches[18].

3.9 Le protocole VTP (Virtuel Trunking Protocole)

Le protocole VTP est un protocole propriétaire de Cisco. Il permet la gestion des VLANs dans un réseau informatique de manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs pour ajouter, modifier ou supprimer la configuration d'un VLAN[21].

3.9.1 Fonctionnement du VTP

Le protocole VTP définit la notion de domaine VTP. Un domaine VTP est composé d'un ou plusieurs équipements interconnectés qui partagent le même nom. Il regroupe des commutateurs pour qu'ils échangent leurs informations de configurations envoyées par le serveur VTP de chaque domaine concerné et plusieurs domaines VTP peuvent cohabiter dans le même réseau local. Dans un environnement VTP, un commutateur peut assurer un des trois rôles qui définissent les trois modes de fonctionnement suivants :

• Mode serveur VTP Un commutateur en mode serveur est chargé de diffuser la configuration aux commutateurs du domaine VTP en envoyant des messages connus

sous le nom « trames VTP », c'est le seul commutateur du domaine capable d'ajouter, supprimer ou renommer des VLAN dans le domaine VTP concerné. Le serveur VTP indique régulièrement le nom de domaine VTP et toutes les informations de configuration VLAN enregistrées dans la mémoire NVRAM du commutateur, y compris le dernier numéro de révision de la configuration VLAN.

• Mode client VTP Un commutateur en mode client est chargé d'appliquer la configuration émise par un commutateur en mode serveur, ce mode ne donne pas la possibilité de créer, modifier ou supprimer des informations VLAN. Donc, il faut d'abord appliquer la modification au sein du serveur VTP pour qu'elle se propage aux différents commutateurs en mode client du même domaine VTP. Contrairement aux serveurs VTP, les informations de configuration VLAN sont totalement perdues lors de la réinitialisation de la mémoire NVRAM du commutateur client.

• Mode transparent VTP Un commutateur en mode transparent ne fait que diffuser les annonces VTP et les configurations du domaine VTP auquel il appartient à travers ses ports de liaison sans prendre en comptes leurs contenus. Donc, le commutateur transparent joue le rôle d'un intermédiaire de communication pour permettre aux clients VTP d'échanger les informations de configuration VLAN avec le serveur VTP[21].

Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci- dessous :

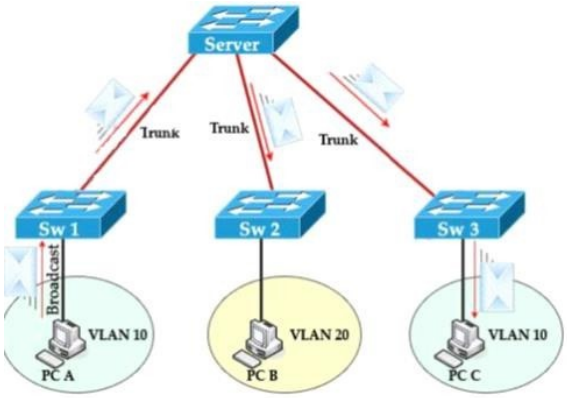

FIGURE 3.3 – Fonctionnement du protocole VTP[22].

3.10 Les réseaux privés virtuels (VPN)

VPN (Virtual Private Network) est une méthode qui assure une communication sécurisée entre des postes distants. Il crée un environnement de communication contrôlé, limitant l'accès aux membres d'une communauté spécifique.

Les VPN utilisent diverses technologies telles que le GRE (Generic Routing Encapsulation), qui permet d'encapsuler les données réseau et crée des tunnels virtuels entre les points distants, offrant ainsi un moyen de transport sécurisé pour les données , ainsi que l'IPsec (Internet Protocol Security), qui assure le chiffrement et l'authentification des paquets IP. De plus, les lignes spécialisées (LS) fournissent une connectivité fiable entre les sites distants. En combinant ces éléments, les VPN offrent des communications sécurisées et fiables pour les postes distants. [23].

Un VPN assure divers objectives, et se caractérise par :

• Étanchéité du trafic entre les différents réseaux privés virtuels.

• La sécurité des communications qui est assurée à travers l'authentification des utilisateurs ou des données, ainsi que la confidentialité à travers le chiffrement effectué entre les données échangées.

• La mise en place d'une liaison VPN réduit les coûts liés à l'infrastructure réseau des entreprises.

• La mise en place d'une liaison VPN assure la qualité de service.

3.10.1 Les types des VPN

Selon le mode d'utilisation, on distingue trois types d'architecture VPN [24] :

• VPN d'accès (host to LAN)

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur distant se sert d'une connexion Internet pour établir la connexion VPN, il sera connecté logiquement au réseau LAN de l'entreprise comme s'il l'était physiquement[24].

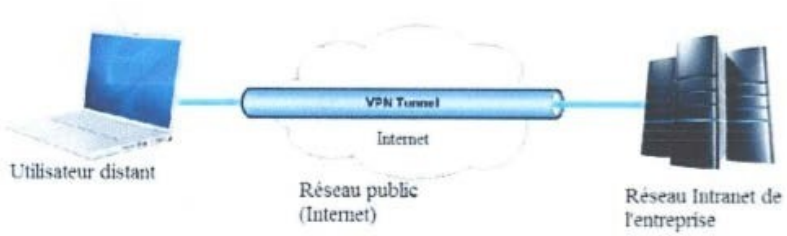

FIGURE 3.4 – VPN d'accès[34] .

• Intranet VPN (LAN to LAN)

L'intranet VPN est utilisé pour relier deux ou plusieurs intranets d'une même Entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants)[24].

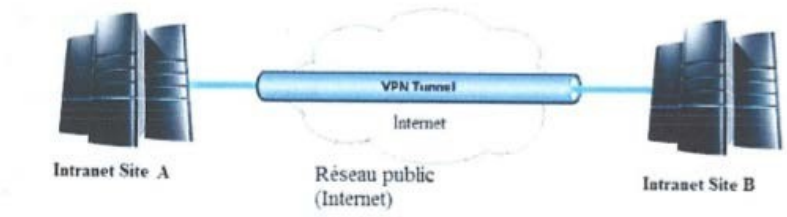

FIGURE 3.5 – VPN intranet [34].

• **Extranet VPN (host to host)**

C'est le cas d'utilisation le plus simple. Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de bases de données entre deux serveurs d'une entreprise disposant de chaque côté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation[24].

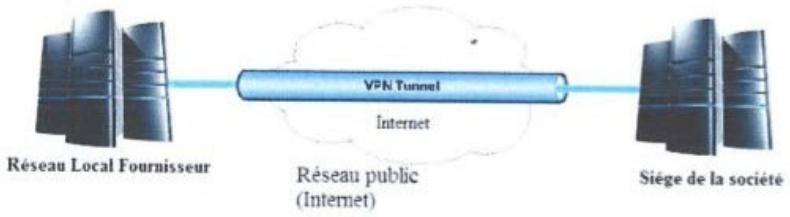

FIGURE 3.6 – VPN extranet[34] .

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

3.10.2 Les avantages de VPN

Les VPN sont une option populaire pour les entreprises qui ont besoin d'une connexion sécurisée et fiable entre différents sites ou pour les travailleurs distants qui doivent accéder aux ressources de l'entreprise de n'importe où dans le monde. Les VPN offrent une sécurité élevée, sont évolutifs et relativement faciles à utiliser et à maintenir[24]

• **Économique**

Sont généralement moins chers que la location de lignes privées pour les connexions à distance, car ils utilisent des réseaux publics pour transmettre les données.

• **Sécurité**

Offrent un niveau élevé de sécurité pour les données en transit. Les données sont chiffrées et authentifiées pour empêcher les accès non autorisés.

• **Évolutivité**

Sont très évolutifs et permettent d'ajouter facilement de nouveaux utilisateurs et de nouveaux sites sans avoir à ajouter de nouvelles lignes privées ou de nouveaux équipements.

• **Simplicité**

Sont relativement faciles à configurer et à maintenir, ce qui les rend accessibles aux entreprises de toutes tailles.

3.11 L'agrégation des liens

L'agrégation de liens est le regroupement de plusieurs interfaces physiques distinctes en une interface logique. Elle a pour objectifs :

• D'assurer une tolérance aux pannes en cas de perte d'un lien ou de problèmes sur une interface.

• D'augmenter la bande passante entre deux équipements interconnectés. L'agrégation de liens consiste à regrouper plusieurs connexions réseau en un seul lien pour augmenter la vitesse et la fiabilité du réseau. Il existe plusieurs façons de le faire, mais cela dépend des équipements utilisés[25].

3.11.1 Le protocole PAGP (Port Aggregation Protocol) :

Le protocole PAGP est un protocole propriétaire de Cisco qui facilite la création automatique de liaisons EtherChannel. Quand une liaison EtherChannel est configurée grâce à PAGP, des paquets PAGP sont envoyés entre les ports compatibles EtherChannel pour négocier la formation d'un canal. Quand PAGP identifie des liaisons Ethernet associées, il groupe les liaisons dans un EtherChannel. L'EtherChannel est ensuite ajouté à l'arbre recouvrant comme port unique.

S'il est activé, PAGP gère également l'EtherChannel. Les paquets PAGP sont envoyés toutes les 30 secondes. PAGP vérifie la cohérence de la configuration et gère les ajouts de liaison et les défaillances entre deux commutateurs. Il garantit que tous les ports ont le même type de configuration quand un EtherChannel est créé.

PAGP permet de créer la liaison EtherChannel en détectant la configuration de chaque côté et en assurant la compatibilité des liaisons, afin que la liaison EtherChannel puisse être activée si besoin[25]. La table illustre les modes pour PAGP :

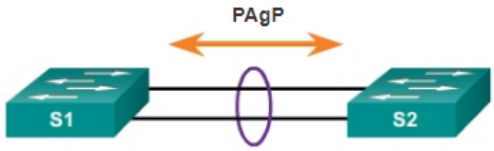

FIGURE 3.7 – Protocole PAGP[26] .

Switch 1	**Switch 2**	**Etablissement de canal**
On	On	Oui
Auto/Désirable	Désirable	Oui
On/Auto/Désirable	Non configure	Non
On	Désirable	Non
Auto	On	Auto

TABLE 3.1 – Table des mode pour PAGP.

On

Ce mode force l'interface à établir un canal sans PAGP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets PAGP.

PAGP desirable

Ce mode PAGP place une interface dans un état de négociation actif, dans lequel l'interface entame des négociations avec d'autres interfaces en envoyant des paquets PAGP.

PAGP auto

ce mode place une interface dans un état de négociation passif, dans lequel l'interface répond aux paquets PAGP qu'elle reçoit mais n'entame pas de négociation.

3.11.2 Le protocole LACP (Link Aggregation Control Protocol)

LACP est un protocole de contrôle de liaison qui permet de gérer l'agrégation de liens Ethernet conformément à la norme 802.3ad qui permet de regrouper plusieurs ports physiques pour former un seul canal logique. LACP permet à un commutateur de négocier un regroupement automatique en envoyant des paquets LACP à l'homologue. Il assure une fonction semblable à celle de PAGP avec Cisco EtherChannel.

LACP étant une norme IEEE, il peut être utilisé pour faciliter les EtherChannel dans des environnements multifournisseurs. Sur les périphériques Cisco, les deux protocoles sont pris en charge.

LACP offre les mêmes avantages en matière de négociation que PAGP. LACP permet de créer la liaison EtherChannel en détectant les configurations de chacun des côtés et en assurant leur compatibilité, afin que la liaison EtherChannel puisse être activée au besoin[25].

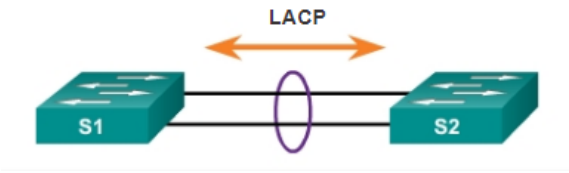

FIGURE 3.8 – Protocole LACP[26] .

La table illustre les modes pour LACP :

Switch 1	**Switch 2**	**Etablissement de canal**
On	On	Oui
Active/Passive	Active	Oui
On/Active/Passive	Non configure	Non
On	Active	Non
Passive/On	Passive	Non

TABLE 3.2 – Table des mode pour LACP.

On

Ce mode force l'interface à établir un canal sans LACP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets LACP.

LACP active

Ce mode LACP place un port dans un état de négociation actif. Dans cet état, le port entame des négociations avec d'autres ports en envoyant des paquets LACP.

LACP passive

Ce mode LACP place un port dans un état de négociation passif. Dans cet état, le port répond aux paquets LACP qu'il reçoit, mais n'entame pas de négociation par paquet LACP.

3.12 Le protocole STP (Spanning Tree Protocol)

Le protocole STP est un protocole de couche 2 qui fonctionne sur des ponts et des commutateurs. La spécification du protocole STP est IEEE 802.1. L'objectif principal de ce protocole est de vérifier qu'aucune boucle n'est créée lorsqu'il y'a des chemins redondants dans le réseau car ces dernières sont fatales[27].

3.12.1 Fonctionnement du STP

Le fonctionnement du Spanning Tree Protocol (STP) repose sur la sélection d'un commutateur principal appelé "Root" et sur le calcul des chemins les plus courts vers ce commutateur. Les ports des commutateurs peuvent se trouver dans cinq états différents, dont le "Blocking" (bloquant) qui empêche le transfert de trames de données, et le "Forwarding" (transfert) qui permet le transfert des trames de données. STP échange régulièrement des informations appelées BPDU (Bridge Protocol Data Unit) entre les commutateurs afin de détecter toute modification potentielle de la topologie du réseau et d'adapter le réseau en conséquence, évitant ainsi les boucles.

Bien que le STP soit conçu pour empêcher les boucles, en théorie, il ne peut pas y en avoir aux points de terminaison du réseau. Pour remédier à cela, Cisco a développé les fonctionnalités PortFast et BPDU ,PortFast elle permet de réduire le temps nécessaire pour qu'un équipement en bout de chaîne puisse accéder à l'état de transfert, tandis que BPDU permet de détecter les informations BPDU provenant de ports qui ne devraient normalement pas les envoyer, évitant ainsi les boucles potentielles[28] .

3.13 Qos(Qualite De Service)

La QoS est la description ou la mesure de la performance globale d'un service, tel qu'un réseau téléphonique ou informatique ou un service, elle permet de prioriser le trafic important, comme la voix ou les données critiques, tout en limitant le trafic moins important, comme les téléchargements ou la navigation web.

La QoS permet de garantir une performance optimale pour les applications et les utilisateurs qui en ont le plus besoin, tout en évitant les goulets d'étranglement et la congestion du réseau.

En outre, la QoS peut également permettre une meilleure utilisation des ressources réseau, en réservant une bande passante suffisante pour les applications critiques et en évitant les perturbations de trafic. Enfin, la mise en place d'une QoS peut améliorer la fiabilité et la disponibilité du réseau, en garantissant que les applications critiques peuvent toujours fonctionner même lorsque le réseau est chargé.

En somme, la QoS est une composante essentielle pour améliorer la performance et la disponibilité des architectures réseaux[29].

3.14 La haute disponibilité

La haute disponibilité fait référence à la capacité d'un système informatique à fonctionner sans interruption même en cas de défaillance d'une partie du système, l'objectif de la haute disponibilité consiste à minimiser le temps d'arrêt et d'assurer la continuité des opérations. Pour atteindre la haute disponibilité, plusieurs techniques sont mises on oeuvre, tels que la redondance, la répartition des charges, la mise en cluster[30].

3.14.1 La redondance au premier saut

Ce que les entreprises recherchent avant tout, c'est un réseau fiable et disponible à tout moment. La mise en place d'un tel réseau peut être difficile et coûteuse. C'est pourquoi la redondance est une solution populaire.

La redondance du premier saut, également connue sous le nom de redondance de la passerelle, est une forme de redondance qui permet de garantir une connectivité réseau continue en cas de défaillance d'un commutateur ou d'une passerelle. L'idée est d'avoir une deuxième passerelle configurée en parallèle avec la première, qui sera utilisée en cas de panne de la première.

Les commutateurs sont configurés pour envoyer des trames à la passerelle principale, mais s'ils ne peuvent pas être envoyés, les trames seront envoyées à la passerelle

de secours. La redondance du premier saut peut être mise en place à l'aide de protocoles tels que VRRP (Virtual Router Redundancy Protocol) ou HSRP (Hot Standby Router Protocol) .

Cela permet une continuité de service ininterrompue pour les utilisateurs finaux et garantit que les applications critiques continuent de fonctionner en cas de défaillance de la passerelle principale [31].

3.14.2 Load balancing

La répartition de charge, ou load balancing en anglais, est une technique utilisée pour équilibrer les charges de travail sur plusieurs serveurs ou ressources informatiques, dans le but d'optimiser les performances, la fiabilité et la capacité du réseau.

Pour ce faire, on utilise un équipement dédié, une appliance physique ou virtuelle, qui identifie en temps réel quel serveur au sein d'un pool répond le mieux à une demande donnée du client, tout en veillant à ne pas surcharger un seul et même serveur.

La répartition de charge permet également d'assurer une fonctionnalité de basculement, ou failover, en cas de panne d'un serveur. Ainsi, le load balancer redirige immédiatement les charges de travail vers un serveur de secours pour minimiser les conséquences de la panne sur les utilisateurs.

Il existe deux types de répartition de charge : celle de la couche 4, qui se base sur les données de transport telles que les adresses IP et les numéros de port TCP, et celle de la couche 7, qui prend en compte des caractéristiques des applications telles que les informations d'en-tête HTTP et le contenu du message. Les répartiteurs de charge de la couche 7 sont les plus couramment utilisés, mais ceux de la couche 4 restent prisés, surtout pour les déploiements périphériques[32].

3.14.3 Cluster

Le cluster est une technique utilisée pour regrouper des ressources physique en une seule entité logique qui travaillent de manière coordonnée, il est pour objectif de garantir la haute disponibilité, la tolérance aux pannes ainsi que la répartition des charges[32].

Il existe plusieurs architecture du clustering :

Clustering Actif-passif

un noeud principal traite les requêtes, un deuxième noeud reste en veille et prends le relais en cas de défaillance du noeud principal.

Clustering Actif-Actif

tous les noeuds sont actifs, ils partagent la charge et chaque noeud traite des requêtes, en offrant ainsi une meilleur performance et une disponibilité continue.

Clustering à basculement

un noeud principal actif, tandis que le reste restent en veille prêt à basculer en cas de besoin.

3.15 DMZ (demilitarized zone)

Une zone démilitarisée (DMZ) est un sous-réseau situé entre l'internet public et les réseaux privés qui protège le réseau local (LAN) interne d'une organisation contre le trafic non sécurisé.

Son rôle principal est d'exposer les services externes à des réseaux non fiables tout en ajoutant une couche de sécurité supplémentaire pour protéger les données sensibles stockées sur les réseaux internes.

La DMZ permet à une entreprise d'accéder à des réseaux non sécurisés comme Internet tout en garantissant la sécurité de son réseau privé. Elle abrite généralement des services et des ressources externes tels que des serveurs DNS, FTP, messagerie, proxy, VoIP et web. Ces serveurs et ressources sont isolés et ont un accès limité au LAN, ce qui les rend accessibles via Internet mais pas depuis le réseau LAN interne. En conséquence, une approche DMZ rend plus difficile pour les hackers d'accéder directement aux données et aux serveurs internes d'une entreprise via Internet[33].

3.16 La zone mixte

La zone mixte est un élément crucial au sein d'une architecture réseau d'entreprise. Elle assure une protection supplémentaire en séparant la zone interne des ressources sensibles et la DMZ, qui est accessible publiquement. Elle crée un sous-réseau distinct qui facilite la segmentation logique du réseau, renforce la sécurité globale et simplifie la gestion des politiques de sécurité. Elle offre un accès contrôlé aux ressources sensibles et simplifie la configuration et la gestion de la DMZ, en établissant une zone intermédiaire entre la zone interne et la DMZ, la zone mixte renforce la protection des actifs internes en empêchant les accès non autorisés.

Elle permet également un contrôle précis du flux de trafic, isolant efficacement les ressources sensibles tout en offrant un accès restreint aux utilisateurs autorisés. Grâce à la zone mixte, les entreprises peuvent améliorer la sécurité de leurs infrastructures réseau, prévenir les attaques potentielles et assurer une gestion plus efficace des ressources sensibles[33] .

3.17 Solutions proposées

En effet des faiblesses et les failles trouvées dans le réseau actuelle de l'entreprise SPA Général emballage, nous proposons une nouvelle architecture représentée en figure 3.9 et qui porte les améliorations suivantes :

• La duplication des câbles entre les switches de distributions et les switches d'accès, cela sert à assurer une redondance dans l'architecture réseau de l'entreprise. Cela signifie que si un des câbles échoue, il existe un autre câble qui prend le relais pour assurer la communication entre les deux équipements.

• Élimination des liaisons en cascade, cela permet de réduire les risques de pannes et d'interruption de service, ainsi que d'améliorer les performances de réseau et simplifier la gestion et la configuration du réseau.

• Utilisation des protocoles de redondance qui permettent de détecter rapidement les pannes sur un équipement ou un lien de communication dans un réseau informatique. En cas de panne, ils permettent de basculer automatiquement sur un

équipement ou un lien de secours pour maintenir la disponibilité et la continuité des services. Cela permet de réduire l'impact des pannes sur l'activité de l'entreprise et d'optimiser les performances du réseau.

• Installation d'un switch pour relier les deux pares-feux avec le réseau extérieur, ce switch permet une répartition équitable de la charge de trafic sur les deux pares-feux. En cas de panne de l'un des pares-feux, le switch bascule automatiquement la charge de trafic sur le pare-feu opérationnel, cella garantit la continuité de service dans le réseau en cas de panne.

• Remplacement des équipements fin de support avec d'autres plus récents pour bénéficier des dernières avancées technologiques en matière de traitement, stockage et communication de l'information. Cela peut entraîner des gains d'efficacité et de productivité pour l'entreprise, en réduisant les temps de traitement et d'accès à l'information, en améliorant la qualité des données traitées et en permettant une meilleure coordination entre les différents services et collaborateurs.

• Création de deux DMZ distinctes, l'entreprise peut mieux protéger ses données et réduire les chances d'intrusions malveillantes.

La figure 3.9 représente la nouvelle architecture proposée.

3.18 Conclusion

Dans ce chapitre nous avons illustré les différentes architectures à plusieurs niveaux, nous avons défini les VLANs ainsi que les VPNs, la haute disponibilité et l'équilibre des charges de ces réseaux. La définition des différents protocoles qu'on a utilisé durant notre projet et comprendre le fonctionnement de chacun ainsi que les avantages qu'ils présentent au réseau. La démonstration de l'implémentation de notre projet fera l'objet du chapitre 4.

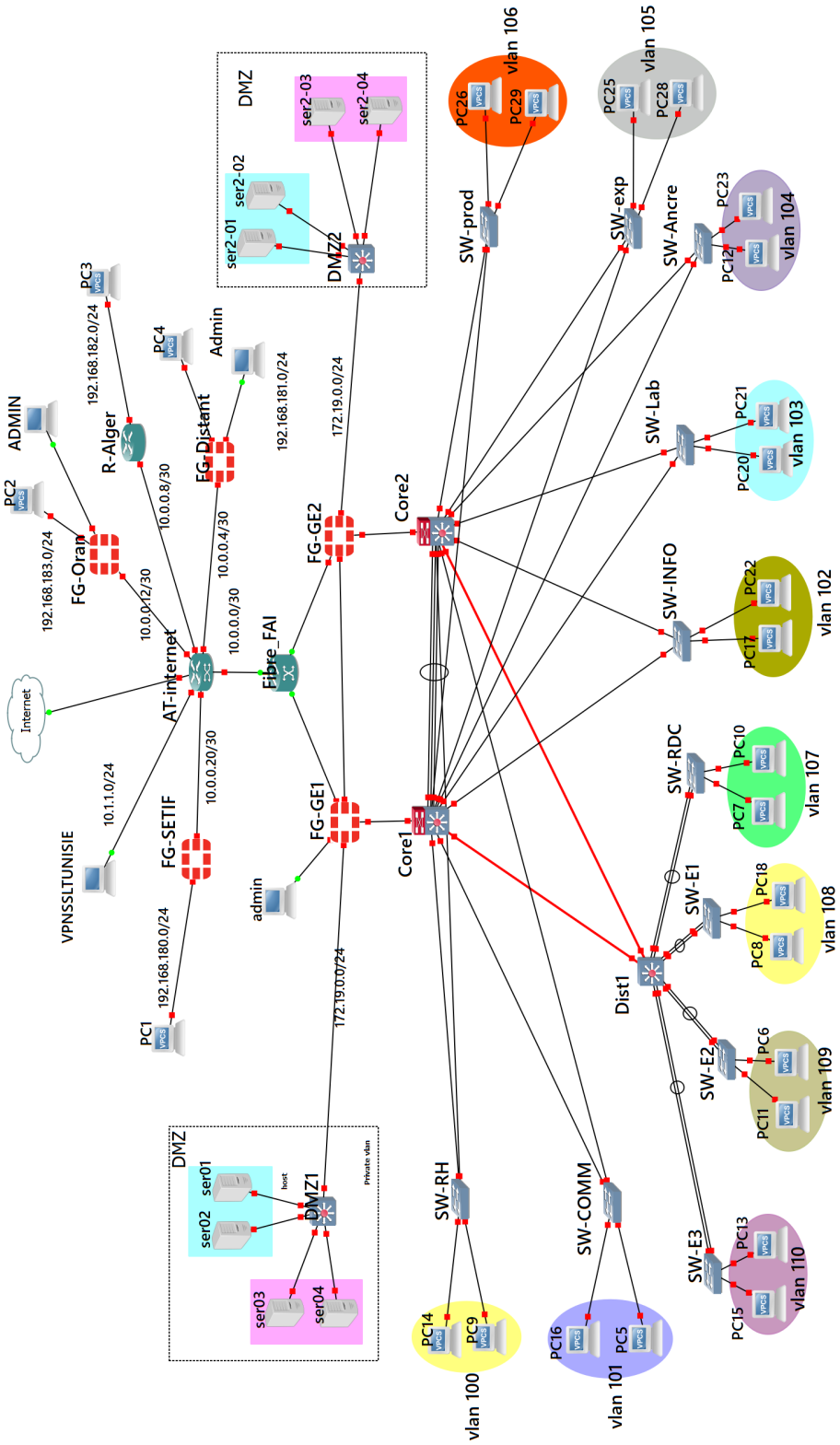

FIGURE 3.9 – Nouvelle architecture proposée.

Chapitre 4

Mise en place de la nouvelle topologie et discussion des résultats.

4.1 Introduction

Après l'étude théorique vue au chapitres précèdent nous allons terminer ce mémoire par la réalisation pratique en concrétisant la solution proposée. Ce présent chapitre, nous expliquons en détail le test de notre solution et nous illustrons les différentes configurations qui permettent d'avoir un réseau a haute disponibilité. Nous commençons par la configurations des Vlans, les protocoles STP, le VTP, le PAGP, et enfin le LACP et nous avons configuré des connexions VPN sécurisées,tout donnons des explications nécessaires pour chaque étapes de configuration .Finalement ,nous testons la fiabilités de notre solution. Pour visualiser l'efficacité de notre travail et mettre en évidence l'efficacité de notre solution, nous avons utilisé le simulateur GNS3 version 0.8.6 qui est un logiciel très pratique open source pour maquetter un réseau. Il pourra nous servir à reproduire une architecture physique ou logique complète avant la mise en production

4.2 Les outils utilisés pour la réalisation de nos solution

Pour la réalisation de notre solution proposée, il est nécessaire d'utiliser plusieurs outils, et on citera :

4.2.1 Le simulateur GNS3

GNS3 (Graphical Network Simulator) est un simulateur graphique de réseaux qui permet de créer des topologies du réseau complexes et d'en établir des simulations. Ce logiciel est un excellent outil pour l'administration des réseaux Cisco. Il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou pour tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment Open Source et multi-plates-formes. Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton « Finish ». La figure suivante représente l'interface de GNS3.

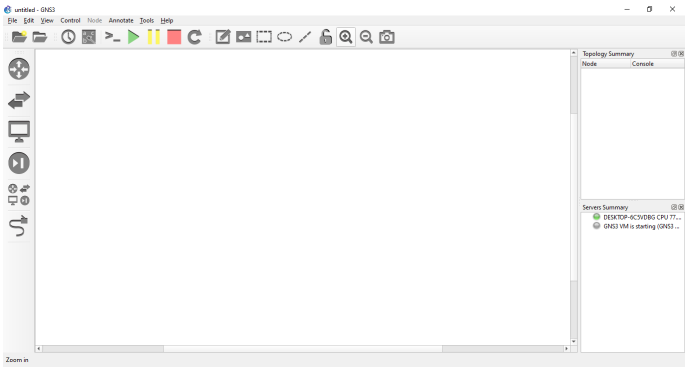

FIGURE 4.1 – Interface d'accueil GNS3

4.2.2 VMware Workstation version 16.1.2

VMware Workstation est un logiciel qui permet de créer des machines virtuelles sur le même ordinateur, ceux-ci peuvent être reliés au réseau local avec une adresse différente, tout en étant sur la même machine physique, et il est possible de faire fonctionner plusieurs machines virtuelles en même temps.Après l'installation de VMware une page d'accueil apparaîtra :

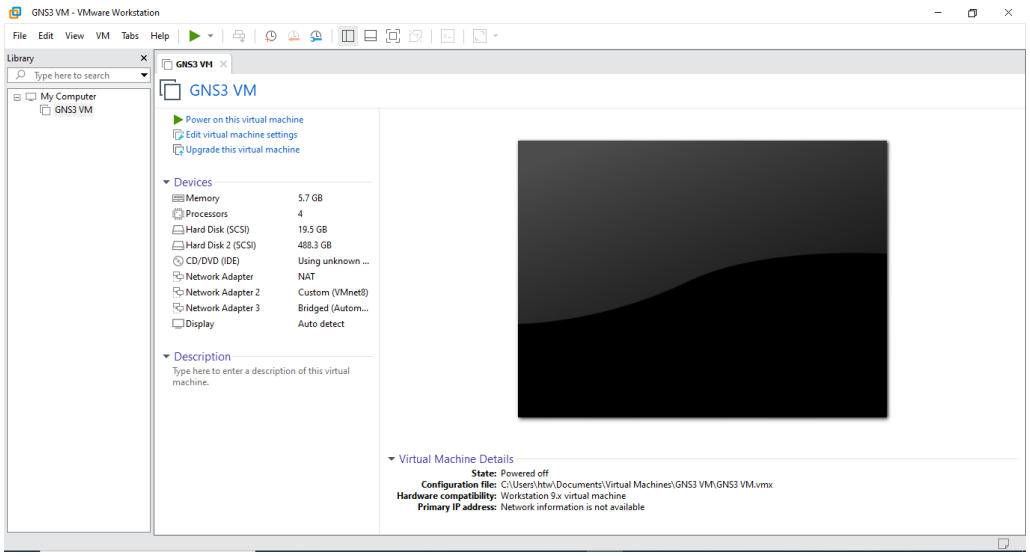

FIGURE 4.2 – Page d'accueil de VMware Workstation 16.1.2

4.2.3 FortiClient VPN

FortiClient VPN est une fonctionnalité spécifique de FortiClient qui permet d'établir une connexion sécurisée et chiffrée à un réseau privé à distance. Cela permet aux utilisateurs de se connecter en toute sécurité à des ressources réseau situées dans un réseau d'entreprise ou une infrastructure sécurisée, même lorsqu'ils sont en dehors de l'emplacement physique du réseau

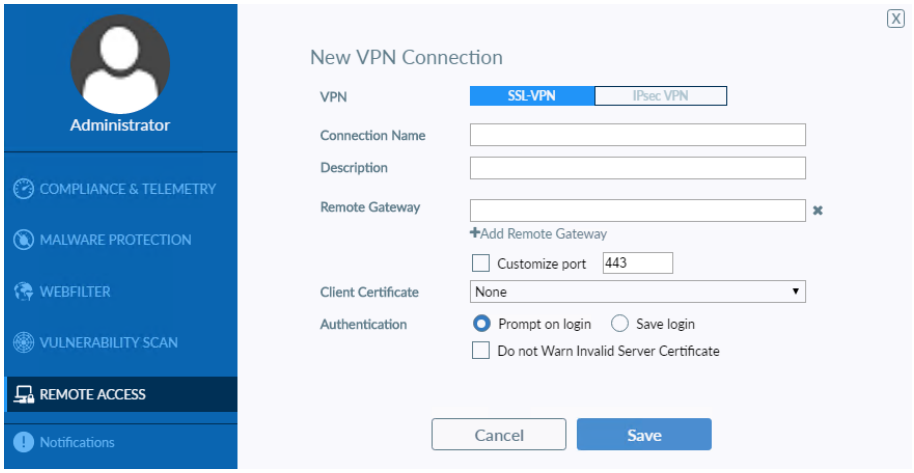

FIGURE 4.3 – Interface FortiClient.

4.3 Adressage

4.3.1 Adressage des interfaces

ÉQUIPEMENT	INTERFACE	ADRESSE	MASQUE	PASSERELLE
Router AT	Ethernet 0/0	10.0.0.2	255.255.255.252	/
Router AT	Ethernet 0/2	10.0.0.13	255.255.255.252	/
Router AT	Ethernet 0/3	10.0.0.9	255.255.255.252	/
Router AT	Ethernet 1/0	10.0.0.21	255.255.255.252	/
Router AT	Ethernet 1/1	10.1.1.1	255.255.255.252	/
Router AT	Ethernet 1/2	10.0.0.5	255.255.255.252	/
Router R-Alger	Ethernet 0/0	10.0.0.10	255.255.255.252	10.0.0.9
Router R-Alger	Ethernet 0/1	192.168.182.1	255.255.255.0	/
FG-GE1	port1	10.0.0.1	255.255.255.252	10.0.0.2
FG-GE1	port4	172.19.0.1	255.255.255.0	/
FG-GE1	port10	192.168.171.10	255.255.255.0	/
FG-Distant	port1	10.0.0.6	255.255.255.252	10.0.0.5
FG-Distant	port2	192.168.181.1	255.255.255.0	/
FG-Distant	port3	192.168.171.12	255.255.255.0	/
FG-Oran	port1	10.0.0.14	255.255.255.252	10.0.0.13
FG-Oran	port2	192.168.183.1	255.255.255.0	/
FG-Oran	port3	192.168.171.13	255.255.255.0	/
FG-Setif	port1	10.0.0.22	255.255.255.252	10.0.0.21
FG-Setif	port2	192.168.180.1	255.255.255.0	/
FG-Setif	port3	192.168.171.11	255.255.255.0	/
ser01	ethernet 0	172.19.0.2	255.255.255.0	172.19.0.1
ser02	ethernet 0	172.19.0.3	255.255.255.0	172.19.0.1
ser03	ethernet 0	172.19.0.4	255.255.255.0	172.19.0.1
ser04	ethernet 0	172.19.0.5	255.255.255.0	172.19.0.1

TABLE 4.1 – Table d'adressage des interfaces.

4.3.2 Vlans utilisés

ID	NOM	DESCRIPTION	ADRESSE
100	RH	RESSOURCE HUMAIN	192.168.100.0/24
101	COMM	COMMERCE	192.168.101.0/24
102	INFO	INFORMATIQUE	192.168.102.0/24
103	LAB	LABORATOIRE	192.168.103.0/24
104	ANCRE	ANCRE	192.168.104.0/24
105	EXPD	EXPÉDITION	192.168.105.0/24
106	PROD	PRODUCTION	192.168.106.0/24
107	RDC	REZ-DE-CHAUSSÉE	192.168.107.0/24
108	E1	ÉTAGE 1	192.168.108.0/24
109	E2	ÉTAGE 2	192.168.109.0/24
110	E3	ÉTAGE 3	192.168.110.0/24
111	VOICE	VOIX	192.168.111.0/24
112	DMZ1	DMZ1	192.168.112.0/24
113	DMZ2	DMZ2	192.168.113.0/24

TABLE 4.2 – Table des Vlans utilisés.

4.4 Configuration de base

4.4.1 Configuration des équipement Cisco

Comme premier pas dans notre travail nous allons changer le nom de chaque équipement en donnant des noms significatifs et facile à reconnaître. Voici un exemple illustratif la nomination de l'un des Switches coeur <Core1> :

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#hostname Core1
Core1(config)#
```

FIGURE 4.4 – Configuration de hostname.

4.4.2 Configuration de base FortiGate

Une fois le pare-feu est démarré, il vient avec une configuration de système tels que le nom d'utilisateur est « admin » et sans mot de passe, après il nous demande d'insérer un nouveau mot de passe et le confirmer, dans notre cas on a mis « admin » comme mot de passe. Une fois confirmer ça apparait le message « Welcome ! » indiquant qu'on a accédé au paramètre du pare-feu comme l'indique la figure suivante :

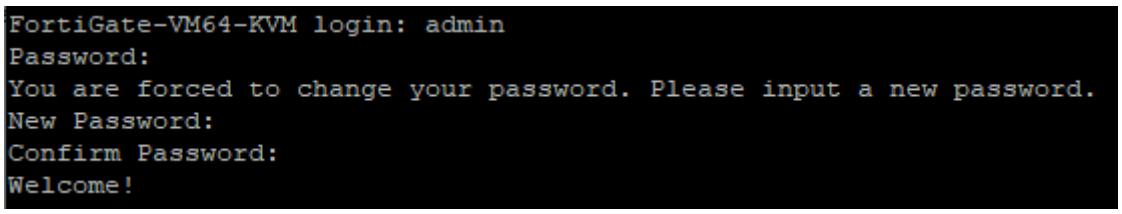

FIGURE 4.5 – Configuration mot de passe de FortiGate.

Pour changer du nom au pare-feu FortiGate on doit d'abord accéder aux configurations globales avec la commande « config system global », ensuite on va lui attribuer un nom commença par la commande « set hostname », dans notre cas on configurer les deux pares-feux, le premier on lui attribuant « FG-GE1 » et le deuxième « FG-GE2 », la figure ci-dessous montre la configuration du premier pare-feu :

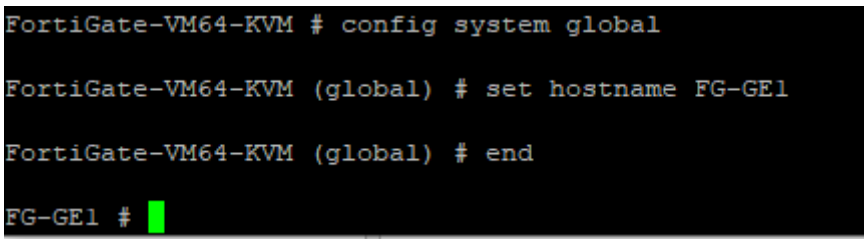

FIGURE 4.6 – Configuration hostname FortiGate.

4.4.3 Configuration des interfaces FortiGate

Pour configure les interfaces, on doit d'abord accéder au configuration système des interfaces par la commande « config sys int », ensuite on configure le port connecter toute en commençant par la commande « edit ». Les ports sont de base en mode dynamique, donc pour pouvoir attribuer des adresses manuellement, on est obligé de rendre en mode statique par la commande « set mode static », après on va attribuer l'adresse et son masque commençant par la commande « set ip », ainsi que d'attribuer les autorisations selon le besoin avec la commande « set allowaccess ». La figure suivante illustre toutes les configurations nécessaires pour pouvoir configurer les interfaces :

```
FG-GE1 # config sys int

FG-GE1 (interface) # edit port10

FG-GE1 (port10) # set mode static

FG-GE1 (port10) # set ip 192.168.171.10/24

FG-GE1 (port10) # set allowaccess https http ping ssh

FG-GE1 (port10) # end
```

FIGURE 4.7 – Configuration des interfaces FortiGate.

Une fois l'interface connecté à internet est configurée, on accède au paramètre de pare-feu depuis le navigateur WEB, toute en insérant l'adresse affectée au port.

Ça nous dirige vers une interface de connexion qui demande d'insérer le nom d'utilisateur et le mot de passe, c'est le même qu'on a déjà insérer au début de la configuration.La figure suivante montre l'interface :

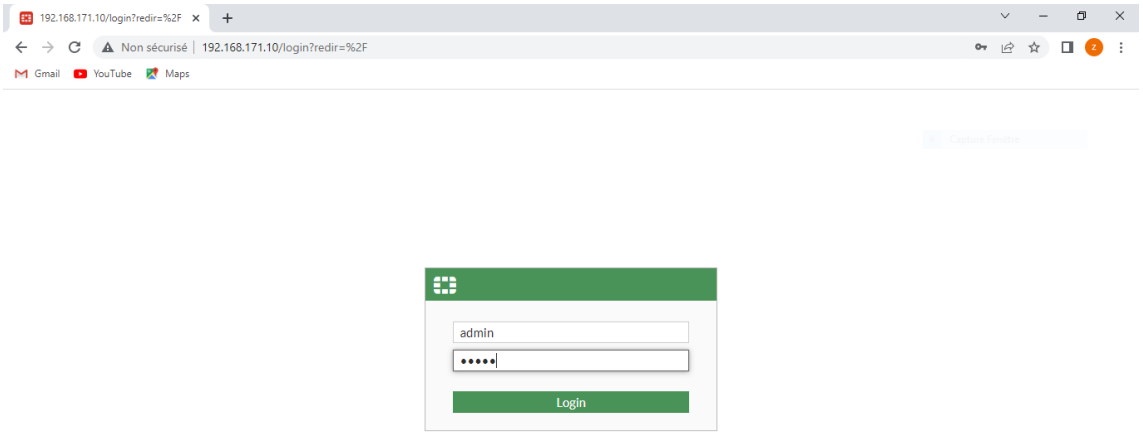

FIGURE 4.8 – Interface de connexion FortiGate.

Une fois le nom d'utilisateur et le mot de passe sont confirmer, on accède au page d'accueil de pare-feu comme l'illustre la figure suivante :

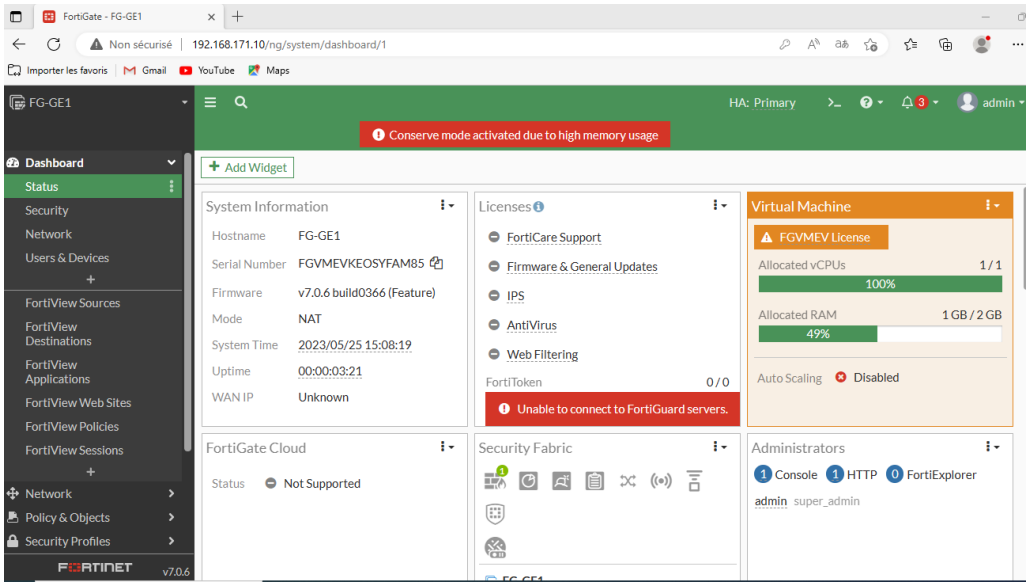

FIGURE 4.9 – Interface d'accueil FortiGate.

4.4.4 Création des Vlans dans FortiGate

Une fois l'interface connecté à internet est configurée, on accède au paramètre de pare-feu depuis le navigateur WEB, toute en insérant l'adresse affectée au port.

Ça nous dirige vers une interface de connexion qui demande d'insérer le nom d'utilisateur et le mot de passe, c'est le même qu'on a déjà insérer au début de la configuration.La figure suivante montre l'interface :

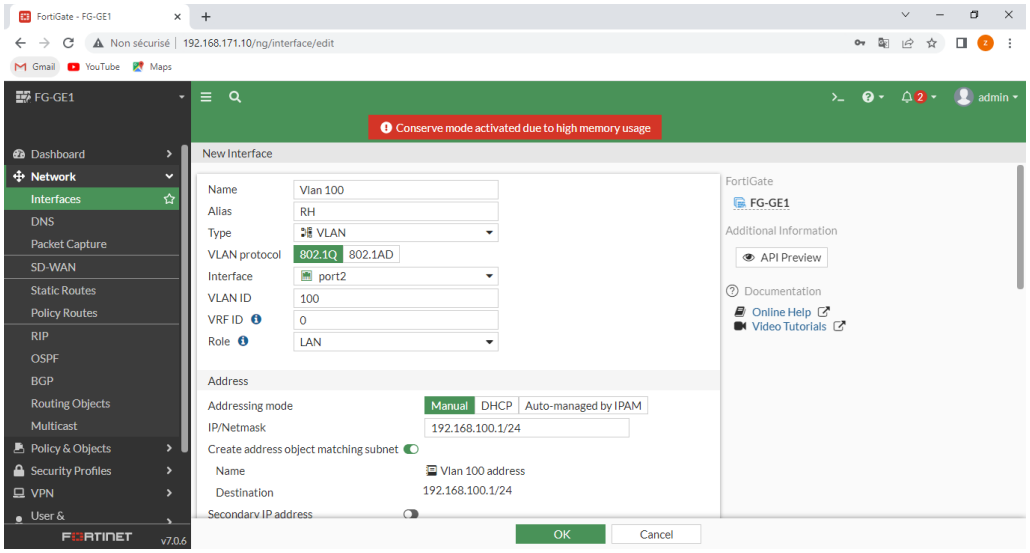

FIGURE 4.10 – Création vlan dans FortiGate.

Ensuite on va coucher les services qu'on a besoin et autoriser le service de DHCP et insérer la plage d'adresse qu'on veut attribuer à l'équipement connectés dans le Vlan comme l'illustre la figure ci-dessous :

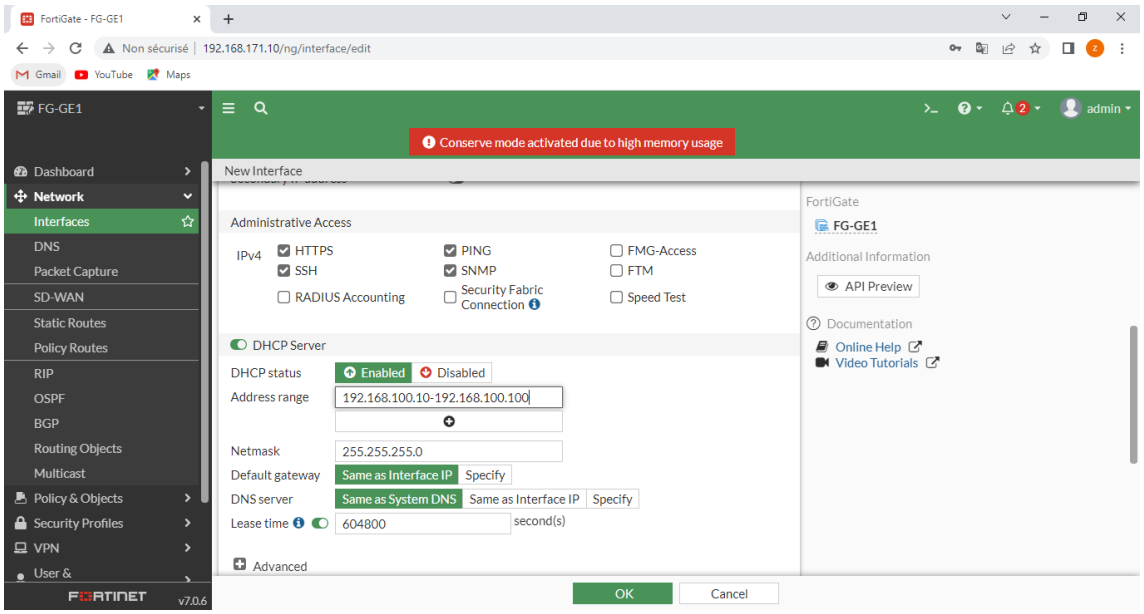

FIGURE 4.11 – Autorisation des services de vlan.

Une fois tout est configurer, on clique sur « OK » et aura l'interface ajoutée dans le tableau des interfaces comme suite :

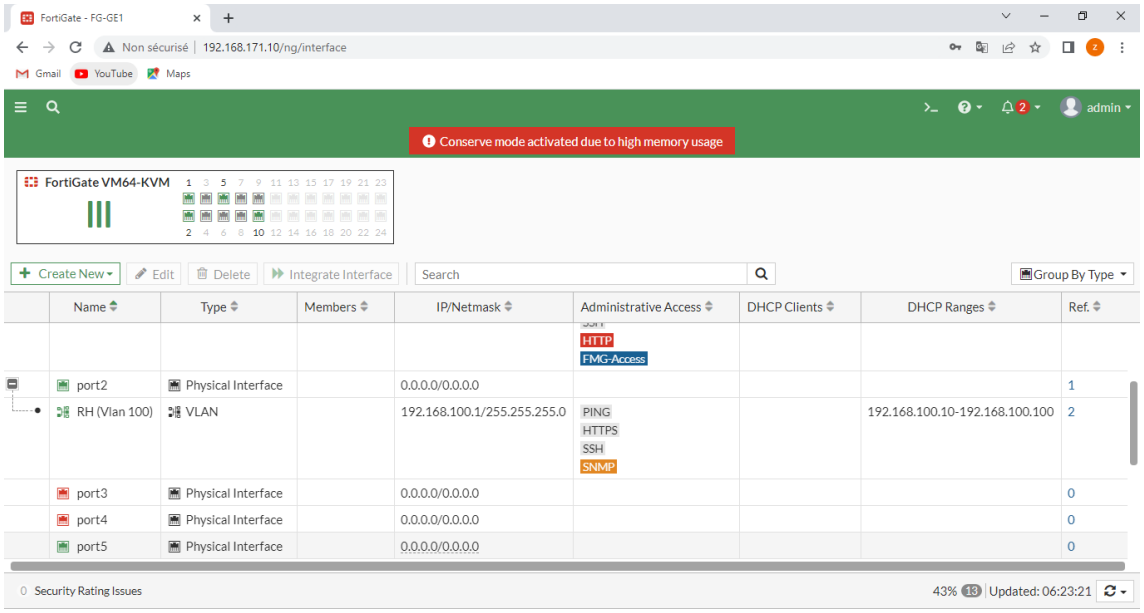

FIGURE 4.12 – Visualisation des interfaces.

4.5 Configuration du protocole VTP (VLAN Trunking Protocol)

Maintenant nous allons configurer le protocole VTP : Nous allons configurer les deux switches Core1 et Core2 en mode serveur (voir l'annexe D) :

```
Core1(config)#vtp mode server
Device mode already VTP Server for VLANS.
Core1(config)#vtp domain Gemb.2023
Domain name already set to Gemb.2023.
Core1(config)#vtp password pfe2023
Password already set to pfe2023
Core1(config)#vtp version 2
VTP version is already in V2.
Core1(config)#vtp pruning
Pruning already switched on
Core1(config)#
```

FIGURE 4.13 – Configuration du vtp en mode server1.

Concernant les switches d'accès on va les configurer en mode client, voici un exemple pour le switch RH :

```
SW-RH(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW-RH(config)#vtp domain Gemb.2023
Changing VTP domain name from NULL to Gemb.2023
SW-RH(config)#vtp password pfe2023
Setting device VTP password to pfe2023
SW-RH(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SW-RH(config)#
```

FIGURE 4.14 – Configuration du vtp en mode client.

4.5.1 Création des Vlans

Nous allons créer les différents VLANs de l'entreprise et tant qu'on a configure le protocole VTP , on va créer les Vlans que dans le switch de distribution Core1 et ensuite la configuration sera transférée pour les autres équipements.

La création des Vlans dans le core1 se fait comme suite :

```
Core1(config)#vlan 100
Core1(config-vlan)#name RH
Core1(config-vlan)#vlan 101
Core1(config-vlan)#name COMM
```

FIGURE 4.15 – Créations des vlans.

Pour la vérification de statut de VTP et la création des Vlans, on utilise la commande « show vtp status » et on obtient le résultat suivant pour le Core1 (voir l'annexe D pour le Core2) :

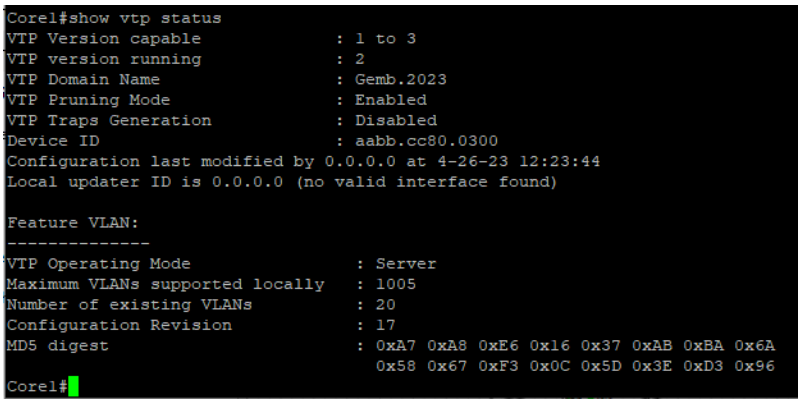

FIGURE 4.16 – Vérification du vtp core1.

On remarque que mode vtp est server et la version est 2 comme on a configuré ainsi que le nombre de Vlans,on fait de même pour les autres switches et obtient le même résultat.

Pour voir si les Vlans sont bien créer, on utilise la commande « show vlan » ,et on voit bien que c'est bien les vlan qu'on vient de créer dans le Core1 qui s'apparait dans le Core2, ce résultat est exhibé dans la figure suivante :

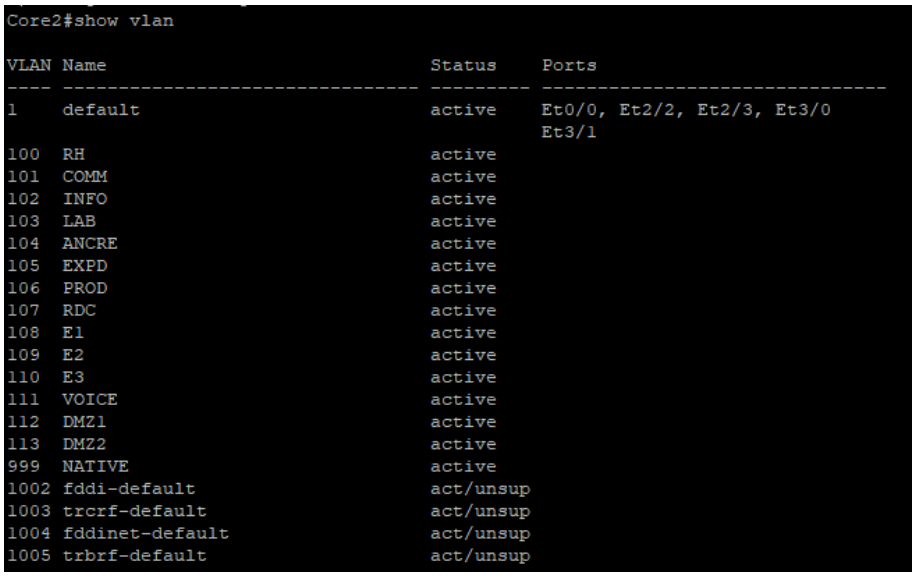

FIGURE 4.17 – Vérification des vlans core2.

On fait de mêmes étapes dans le switch d'accès qu'on a configurer en tant que client et on obtient les résultats suivants :

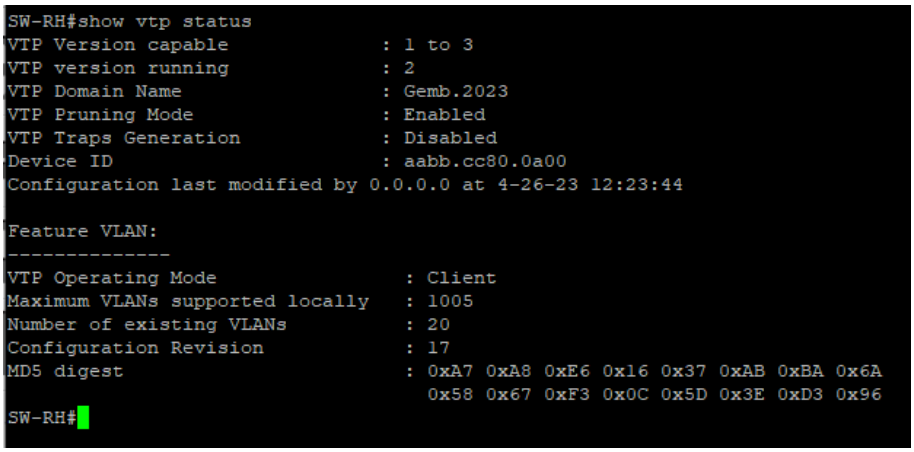

FIGURE 4.18 – Vérification du vtp SW-RH.

Pour vérifier que les Vlans sont bien créer, on utilise la commande « show vlan » et on remarque qu'on a bien les même Vlans qu'on a créé dans le Core1, la figure suivante montre le résultat :

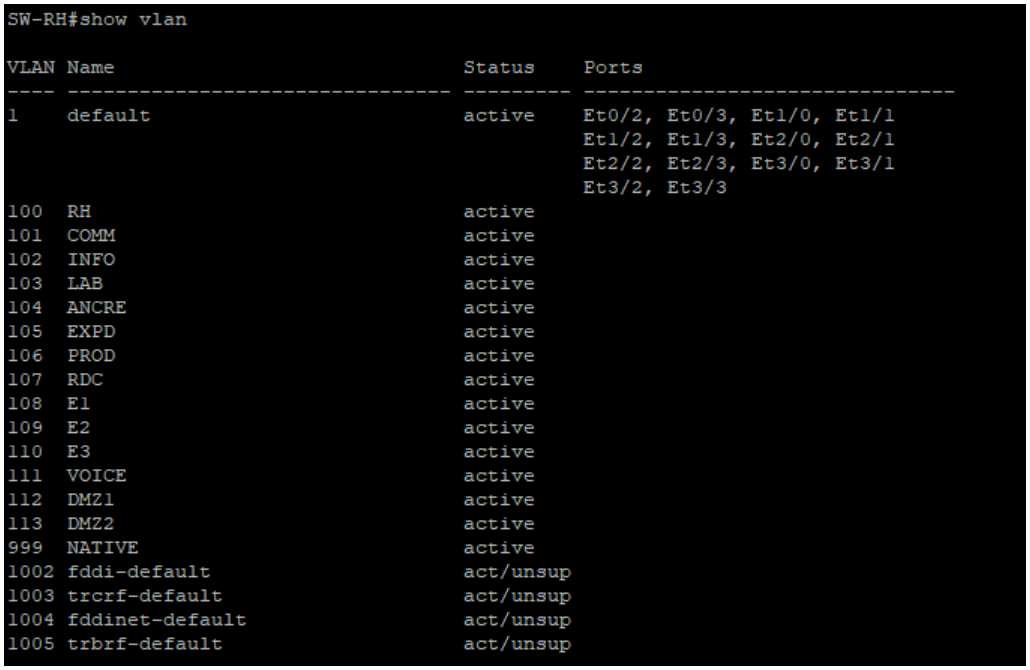

FIGURE 4.19 – Vérification des vlans SW-RH.

4.6 Configuration des liens trunk

Dans cette section, nous allons configurer les liaisons entre les switches de distribution et les switches d'accès (niveau 2) en mode trunk afin que ses derniers communiquent et transmettent entre eux les Vlans configurés dans les switches de distribution.

Premièrement on utilise la commande show cdp neighbors pour voir les interfaces connectées dans notre équipement :

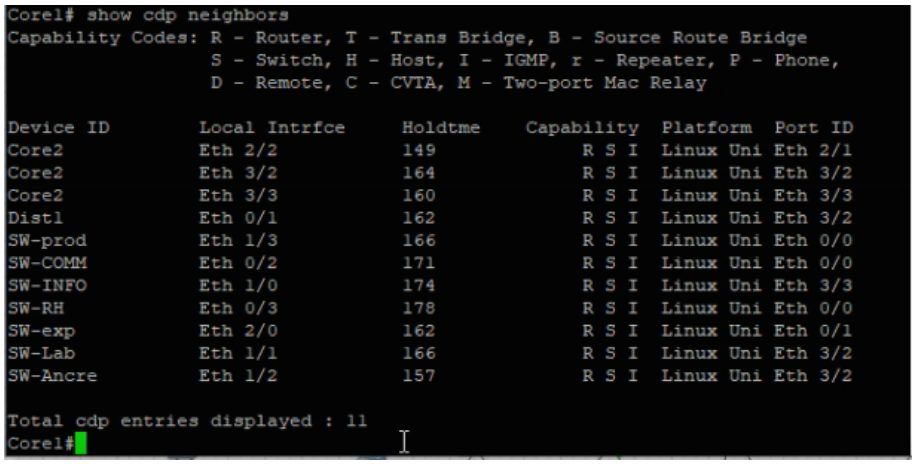

FIGURE 4.20 – Vérification des interfaces connecte.

Ensuite, on choisit les interfaces pour les configurer en mode trunk ainsi que configurer le Vlan native qui est dans notre cas le Vlan 999, comme la montre la figure 4.22,on va faire la même configurations pour les switchs d'accès :

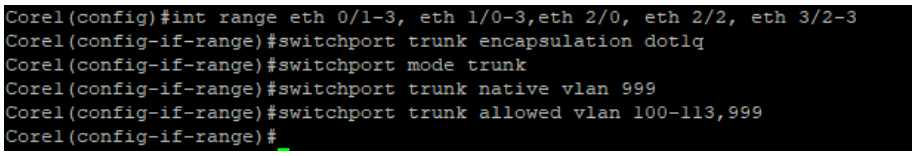

FIGURE 4.21 – Configuration des lien trunk et le vlan native.

Afin de vérifier cette configuration, on vérifie l'état des interfaces avec la commande «show interface trunk ».

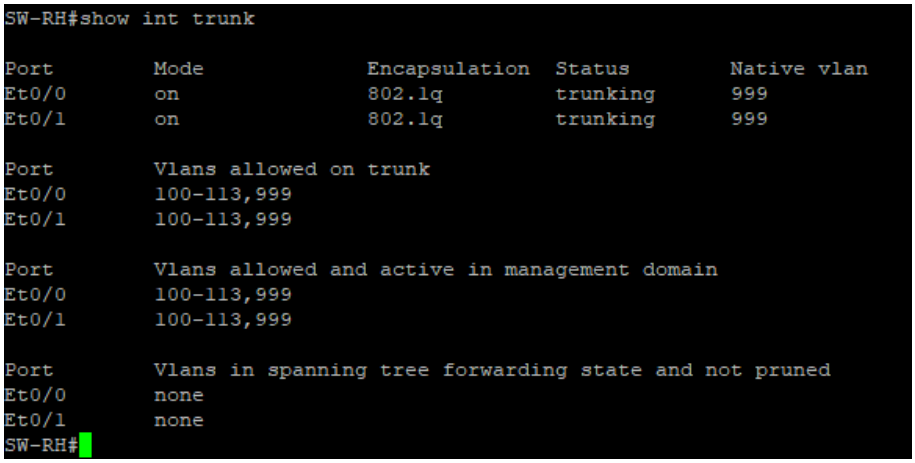

FIGURE 4.22 – Vérification de la configuration.

4.7 Configuration du protocole STP(Spanning Tree Protocol)

Pour faciliter la mise en place d'un chemin logique sans boucle sur l'ensemble du domaine de diffusion nous allons configurer le protocole STP.

On commence par l'activation du rapid spanning-tree en tapant la commande « spanning- tree mode rapid-pvst » :

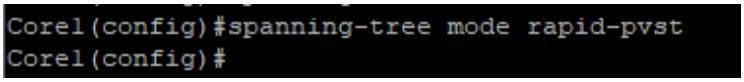

FIGURE 4.23 – L'activation du rapid spanning-tree.

Pour choisir les priorités on doit choisir des valeurs suivantes :

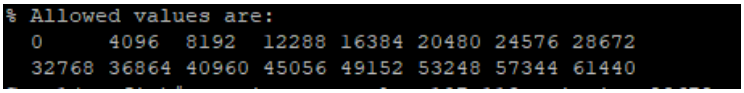

FIGURE 4.24 – Choisir les priorités.

Configuration de stp dans le Core1 :

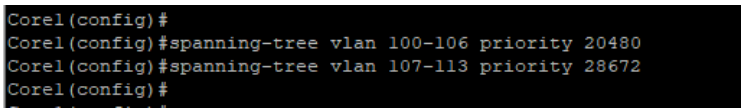

FIGURE 4.25 – La configuration du STP core1.

Configuration de stp dans le Core2 :

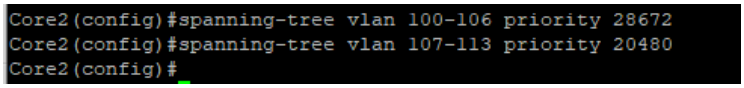

FIGURE 4.26 – La configuration du STP core2.

(voir l'annexe D pour la vérification du protocole)

4.8 Configurations du LACP (Link Aggregation Control Protocol) :

La configuration du protocole LACP implique plusieurs étapes. Tout d'abord, il est nécessaire d'activer les interfaces qui relient les switches, c'est-à-dire les ports physiques que l'on souhaite agréger. Une fois les interfaces activées en exécute la commande «channel-groupe 2 mode active». Elle indique que le protocole LACP est configuré en mode actif, ce qui signifie que le port émet et reçoit ,et pour la commande «port-channel load-balance src-dst-mac» elle spécifie que la répartition de la charge doit être basée sur les adresses sources et de destination MAC des paquets.

Configuration du Core1, (voir l'annexe D pour la configuration de Core2) :

```
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#interface range eth3/2-3, eth2/2
Core1(config-if-range)#channel-group 2 mode active
Core1(config-if-range)#exit
Core1(config)#port-ch
Core1(config)#port-channel lo
Core1(config)#port-channel load-balance src-dst-mac
Core1(config)#end
Core1#w
*May 15 11:08:57.064: %SYS-5-CONFIG_I: Configured from console by consoler
Core1#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1513 bytes to 904 bytes[OK]
Core1#
```

FIGURE 4.27 – Configuration du protocle LACP core1.

• Vérification de la configuration de LACP en utilisant la commande « show etherchannel summary »

```
Core1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Et2/2(P)    Et3/2(P)    Et3/3(P)

Core1#
```

FIGURE 4.28 – Vérification de la configuration du LACP.

En remarque que dans le port-channel on trouve po2(SU), la lettre S décrit le niveau 2 (layer 2) et la lettre U veut dire que le protocole est en marche (in use).

4.9 Configuration PAgP (Port Aggregation Protocol)

Switch	Groupe
RDC	1
E1	3
E2	2
E3	4

TABLE 4.3 – Table des Vlans utilisés.

Configuration du DIST1 :

La figure suivante illustre la configuration du protocole PAgP dans le switch DIST1 en créant un groupe 4 pour l'étage 3 :

```
Dist1(config)#
Dist1(config)#interface range eth 1/0, eth 0/1
Dist1(config-if-range)#channel-group 4 mode desirable
Creating a port-channel interface Port-channel 4

Dist1(config-if-range)#exit
*May 15 11:34:58.014: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to down
*May 15 11:34:58.016: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
*May 15 11:34:59.025: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to up
*May 15 11:34:59.026: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to up
Dist1(config-if-range)#exit
Dist1(config)#port-ch
Dist1(config)#port-channel lo
Dist1(config)#port-channel load-balance src-dst-mac
Dist1(config)#end
Dist1#
*May 15 11:35:23.770: %SYS-5-CONFIG_I: Configured from console by console
Dist1#
```

FIGURE 4.29 – Configuration du protocole PAGP DIST1.

Configuration du PAGP dans le switch d'accès, la figure suivante illustre la configuration de protocole PAGP dans le switch E3 (voir l'annexe D pour la vérification) :

```
SW-E3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-E3(config)#interface range eth 0/0-1
SW-E3(config-if-range)#channel-group 4 mode desirable
SW-E3(config-if-range)#exit
SW-E3(config)#port-channel load-balance src-dst-mac
SW-E3(config)#end
SW-E3#wr
*May 15 11:48:53.411: %SYS-5-CONFIG_I: Configured from console by console
SW-E3#wr
Building configuration...
Compressed configuration from 2062 bytes to 1160 bytes[OK]
SW-E3#
```

FIGURE 4.30 – Configuration du PAGP E3.

Après la configuration des autres liens, on vérifie qu'ils ont étaient bien configurés on utilisant la commande « show etherchannel summary »

```
Dist1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG


Number of channel-groups in use: 4
Number of aggregators:           4

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)         PAgP      Et0/3(I)    Et2/3(I)
2      Po2(SD)         PAgP      Et0/0(I)    Et3/1(I)
3      Po3(SU)         PAgP      Et0/2(P)    Et3/0(P)
4      Po4(SD)         PAgP      Et0/1(I)    Et1/0(I)

Dist1#
```

FIGURE 4.31 – Vérification de la configuration du PAGP DIST1.

4.10 Configuration de la DMZ

Configuration de VTP mode transparent et création du vlan primary :

```
DMZ2(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
DMZ2(config)#vlan 200
DMZ2(config-vlan)#private-vlan primary
DMZ2(config-vlan)#private-vlan association 201,202
DMZ2(config-vlan)#
```

FIGURE 4.32 – Configuration de VTP mode transparent et création du vlan primary.

Création des vlan community et isolated :

```
DMZ2(config)#vlan 201
DMZ2(config-vlan)#private-vlan community
DMZ2(config-vlan)#exit
DMZ2(config)#vlan 202
DMZ2(config-vlan)#private-vlan isolated
DMZ2(config-vlan)#exit
DMZ2(config)#
```

FIGURE 4.33 – Création des vlan community et isolated.

Configuration de lien promiscuous dans la connexion reliant le pare-feu et le switch DMZ :

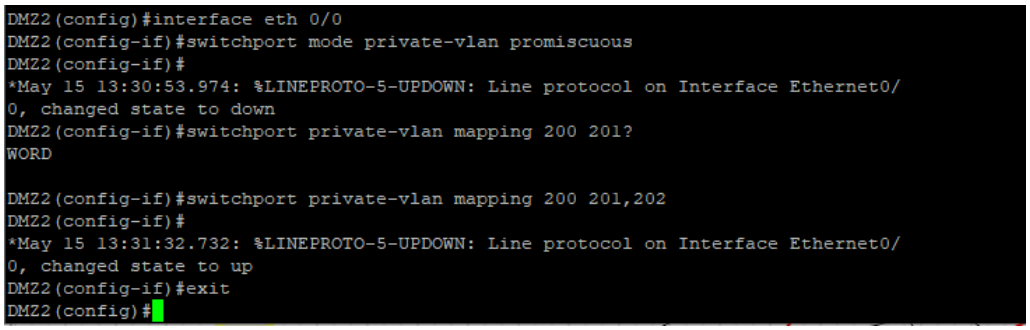

FIGURE 4.34 – Configuration de lien promiscuous .

Configuration de lien host pour la partie communication :

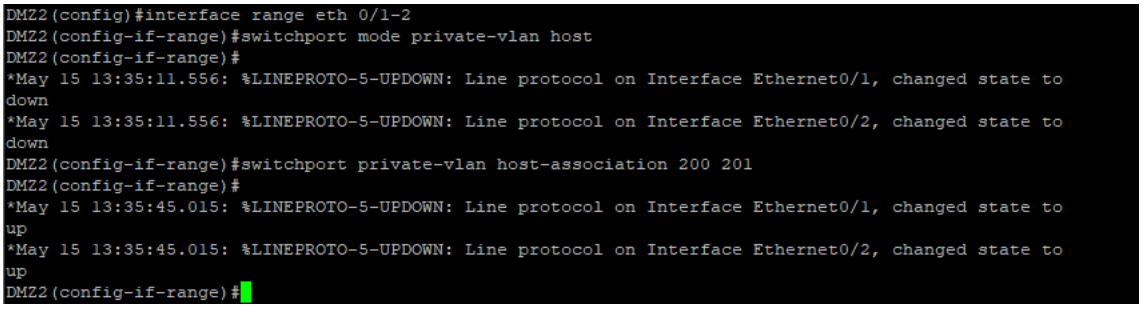

FIGURE 4.35 – Configuration de lien host pour la partie communication.

Configuration de lien host pour la partie isolation :

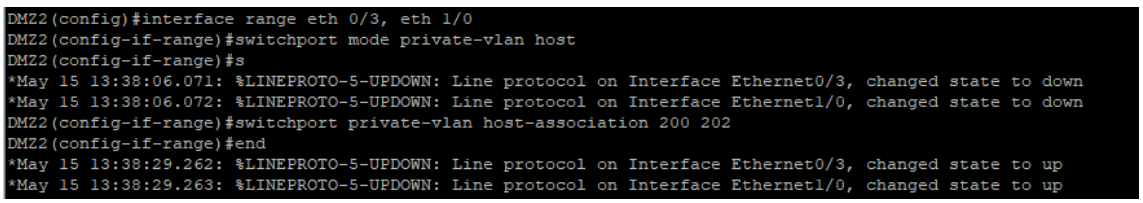

FIGURE 4.36 – Configuration de lien host pour la partie isolation.

Création d'une politique qui permet la connexion vers internet :

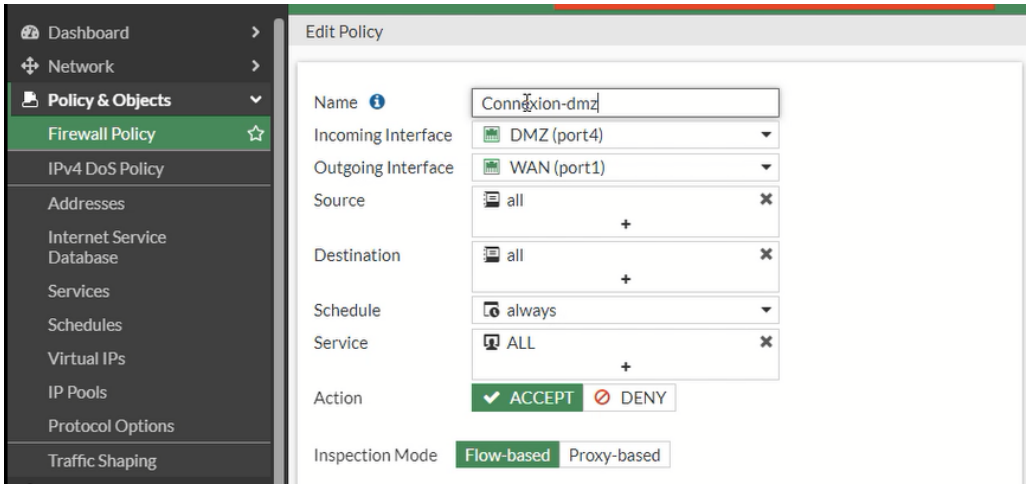

FIGURE 4.37 – Création d'une politique qui permet la connexion vers internet.

- **Test de connectivité entre différents équipements**
  - Du serveur 2 au serveur 1 :

```
ser2-02> ping 172.19.0.2

84 bytes from 172.19.0.2 icmp_seq=1 ttl=64 time=1.847 ms
84 bytes from 172.19.0.2 icmp_seq=2 ttl=64 time=0.996 ms
84 bytes from 172.19.0.2 icmp_seq=3 ttl=64 time=1.529 ms
84 bytes from 172.19.0.2 icmp_seq=4 ttl=64 time=1.506 ms
84 bytes from 172.19.0.2 icmp_seq=5 ttl=64 time=2.301 ms
```

FIGURE 4.38 – Test de connectivité Du serveur 2 au serveur 1.

  - Du serveurs 2 au serveur 3 :

```
ser2-02> ping 172.19.0.4

host (172.19.0.4) not reachable
```

FIGURE 4.39 – Test de connectivité Du serveurs 2 au serveur 3 .

  - Du serveurs 3 au serveur 2 :

```
ser2-03> ping 172.19.0.3

host (172.19.0.3) not reachable
```

FIGURE 4.40 – Test de connectivité Du serveurs 3 au serveur 2 .

• Du serveur 3 au serveur 4 :

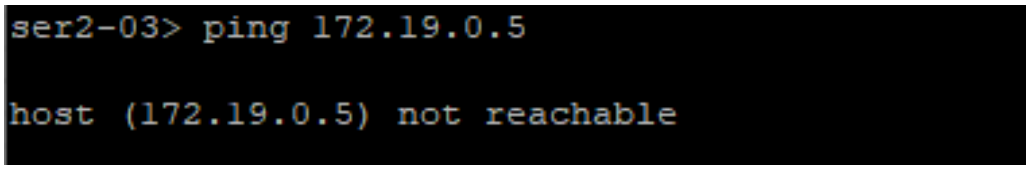

FIGURE 4.41 – Test de connectivité Du serveur 3 au serveur 4 .

On remarque que la connectivité entre le serveur 2 et le serveur 1 est établie, contrairement aux autres serveurs. Cela est dû au type de vlan, le vlan isolated ne permet pas de se communiquer avec d'autres équipements que se soit dans le même vlan ou d'un autre, par contre le vlan community permet la communication entre les machines dans le même vlan.

4.11 Configuration du Clustering

Configuration de FG-GE1

Dans la configuration de clustering, on va accéder au paramètre système et dans la session HA (High Availability) qui sert pour effectuer la configuration.

Dans notre cas, on va configure le mode Active-Active, on va choisir une priorité de 200 pour le que ce pare-feu FG-GE1 soit le principal dans le réseau, on va choisir un nom de groupe : Group1-HA, et un mot de passe : 1234567.

On va activer le Session Pickup pour synchroniser les sessions, pour les interfaces monitoring sont les interfaces connectées dans le réseau qu'on veut synchroniser dans le deuxième pare-feu, HeartBeat Interface désigne le port du clustering, qui est dans notre cas le port3.

toute la configuration est illustrée dans la figure suivante :

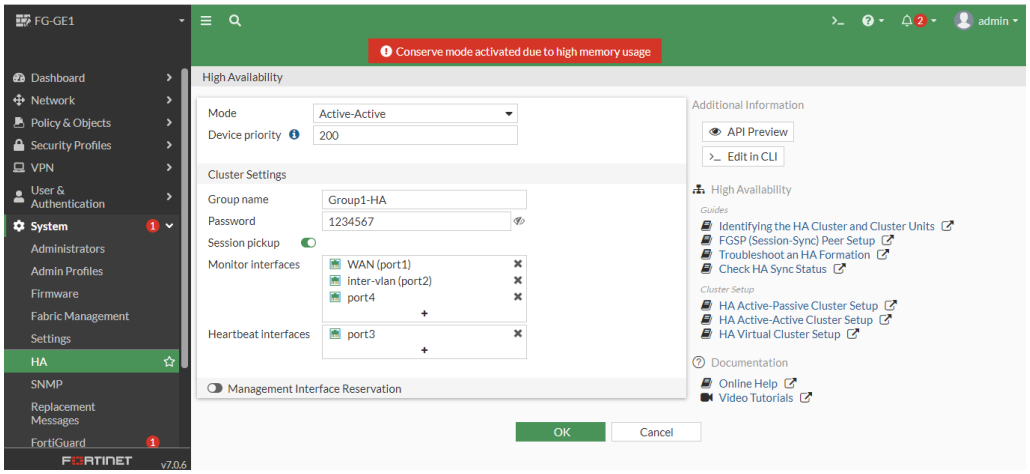

FIGURE 4.42 – Configuration du système HA.

• Une fois terminer on clique sur « OK » pour activer l'interface :

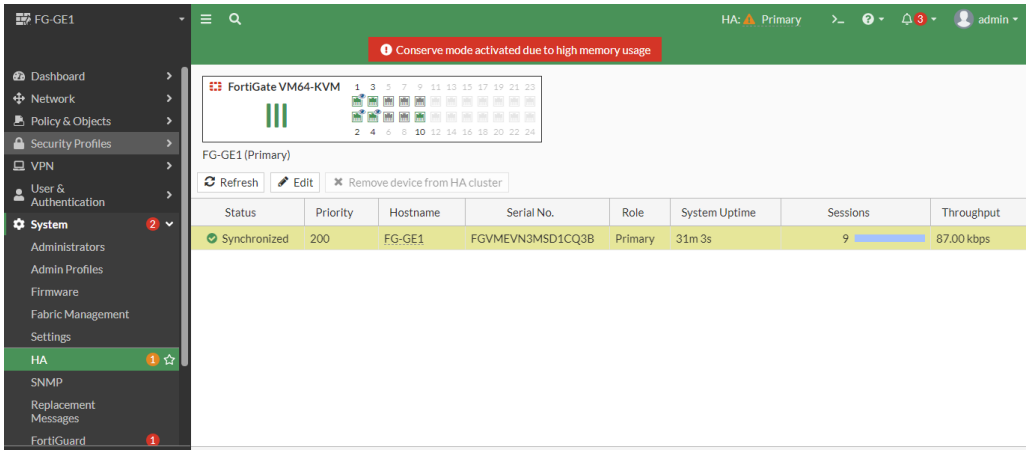

FIGURE 4.43 – Vérification de l'interface.

• On vérifie la configuration dans ce pare-feu avec la commande « show system ha » :

```
FG-GE1 # show system ha
config system ha
    set group-name "Group1-HA"
    set mode a-a
    set password ENC p1J7Kx4qKhErMnzbfqkNIjugcNiaK/KLLRCfnetsHLLyVja/rlNTm6XuTa/
pYhsTH4ZpqZi8CiJ+3JMjsvSc9bj5u/T0Iou3+zff5L2nCloolAm25MPjV716aWr7ExYR+QPj/lOqc+L
UrSjyVDcaohs+54AkpdX2CIJ4uKCvzAHOudkxW3ZDlAXGmOGTsOKDFrcJwQ==
    set hbdev "port3" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1" "port2" "port4"
end

FG-GE1 #
```

FIGURE 4.44 – Vérification de la configuration du pare-feu FG-GE1.

on voit que toute la configuration est illustrée dans le résultat.

Configuration de FG-GE2

En premier lieu, on vérifie la configuration de la haute disponibilité dans ce pare-feu avec la commande « show system ha », et on remarque qu'il n'y a aucune configuration :

```
FG-GE2 # show system ha
config system ha
    set override disable
end

FG-GE2 #
```

FIGURE 4.45 – Vérification de la configuration du pare-feu FG-GE2 .

• Nous allons configurer ce pare-feu en effectuant la même configuration du premier pare-feu :

```
FG-GE2 # config system ha

FG-GE2 (ha) # set group-name Group1-HA

FG-GE2 (ha) # set mode a-a

FG-GE2 (ha) # set password 1234567

FG-GE2 (ha) # set hbdev port3 0

FG-GE2 (ha) # set session-pickup enable

FG-GE2 (ha) # set monitor port1 port2 port4

FG-GE2 (ha) # end

FG-GE2 #
```

FIGURE 4.46 – Configuration du pare-feu FG-GE2.

• On va ensuite télécharger la configuration du clustering avec la commande « get system ha » :

```
FG-GE2 # get system ha
group-id              : 0
group-name            : Group1-HA
mode                  : a-a
sync-packet-balance   : disable
password              : *
hbdev                 : "port3" 0
session-sync-dev      :
route-ttl             : 10
route-wait            : 0
route-hold            : 10
multicast-ttl         : 600
sync-config           : enable
encryption            : disable
authentication        : disable
hb-interval           : 2
hb-interval-in-milliseconds: 100ms
```

FIGURE 4.47 – Téléchargement de la configuration du clustering.

• On utilisant la commande « get system ha status », on obtient le statut des deux pares-feux :

```
Secondary   : FG-GE2          , FGVMEVWXUIUJ-340, HA cluster index = 0
Primary     : FG-GE1          , FGVMEVN3MSD1CQ3B, HA cluster index = 1
```

FIGURE 4.48 – Vérifications des statuts des deux pares-feux.

Comme l'indique la figure, le pare-feu FG-GE1 est le principal, le pare-feu FG-GE2 est secondaire.

• Pour vérifier que la configuration est effectuée, nous allons dans la session HA du premier pare-feu, et on trouve cette configuration du deuxième pare-feu avec une priorité inférieure comme la montre la figure suivante :

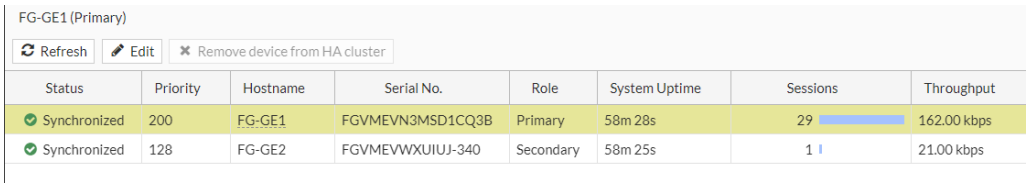

FIGURE 4.49 – Vérification de la configuration du clustering.

4.12 Configuration de VPN :

4.12.1 Configuration d'une LS (ligne spécialisée)

Pour la configuration d'une LS entre le site AKBOU et site de Setif, nous allons premièrement configurer les interfaces du routeur, comme l'illustre la figure suivante :

```
AT-internet#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AT-internet(config)#in
AT-internet(config)#interface  eth
AT-internet(config)#interface  ethernet 0/2
AT-internet(config-if)#in
AT-internet(config-if)#ip add
AT-internet(config-if)#ip address 10.0.0.13 255.255.255.252
AT-internet(config-if)#no shu
AT-internet(config-if)#no shutdown
AT-internet(config-if)#exit
```

FIGURE 4.50 – Configuration des interfaces routeur.

Ainsi on va configurer une route statique par défaut :

```
R-Alger(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.9
R-Alger(config)#
```

FIGURE 4.51 – Route statique par défaut.

Ensuite on va configurer le pare-feu FG-SETIF, la configuration est basée sur les routes statiques permettant d'atteindre le réseau voulu dans le site Béjaia, prenant exemple du Vlan 100 RH :

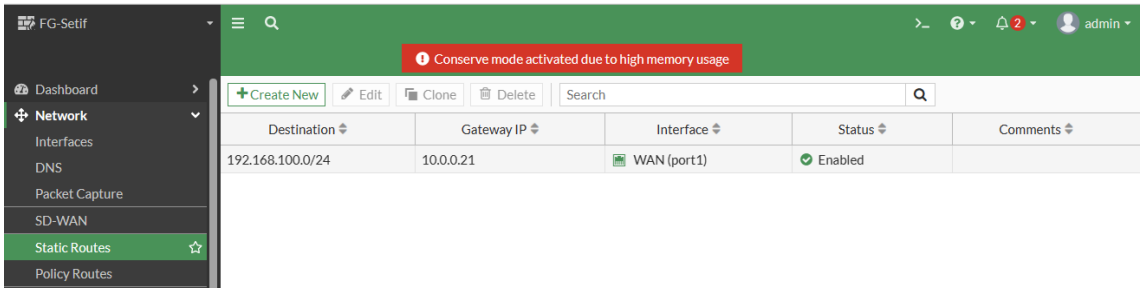

FIGURE 4.52 – Route statique dans le pare-feu

Après avoir configurer toutes les interfaces ainsi que la route statique vers internet, on va créer une politique pour le trafic traversant la liaison spécialisée, qui sort vers les autres réseaux par l'interface WAN (port 1) :

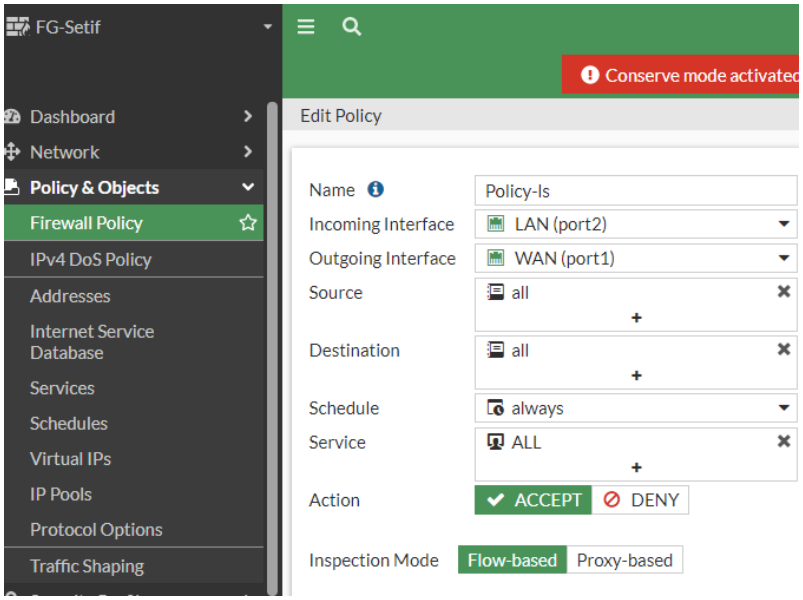

FIGURE 4.53 – Politique Sortante LS.

• Ensuite on va créer une autre politique qui permet la connexion des autres interfaces vers le réseau de site Sétif, par l'interface LAN (port 2) :

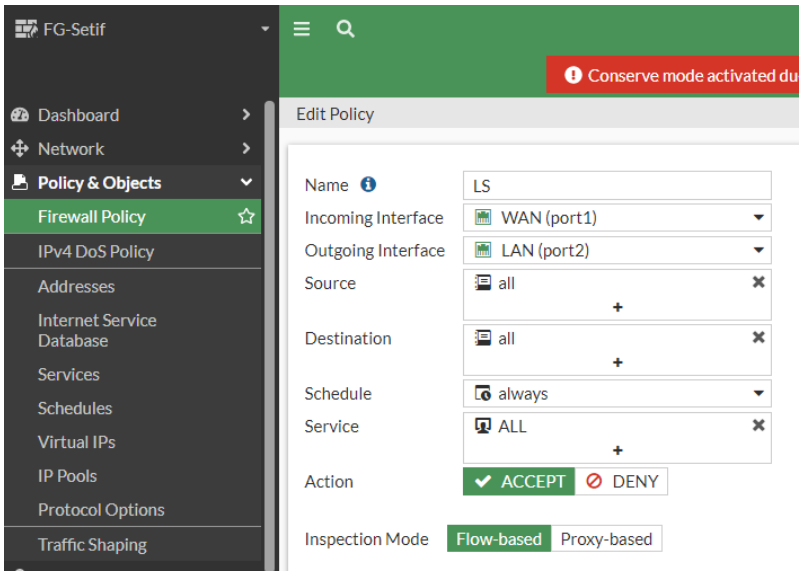

FIGURE 4.54 – Politique entrante LS.

4.12.2 Configuration de VPN IPsec(Internet Protocol Security)

Dans notre simulation, nous allons configurer des tunnels IPsec entre le site Béjaia et le site Distant, ainsi que le site Béjaia et site Oran. c'est la même configuration pour les deux tunnels.

Tout d'abord on va accéder au pare-feu de Béjaia, dans les paramètres de VPN, on accède au paramètre de tunnel IPsec Tunnels, et en va créer un nouveau tunnel, on va choisir le type de tunnel tant que site à site et on choisit le type d'équipement dans le réseau de Distant qui est FortiGate comme montre la figure suivante :

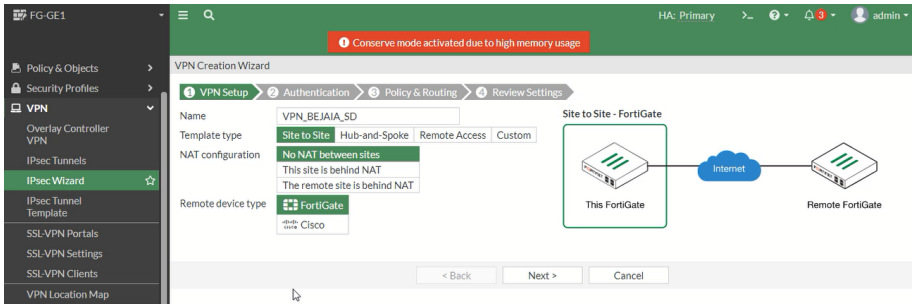

FIGURE 4.55 – Nomination du tunnel.

Ensuite, nous allons insérer la passerelle voulu attendre ainsi que l'interface de sortie. Nous allons aussi lui attribuer un mot de passe qui est dans notre cas « ge2023 » :

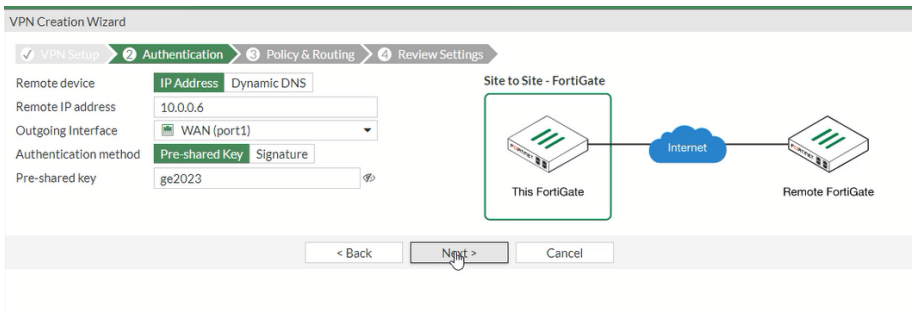

FIGURE 4.56 – Passerelle IPsec.

Après on va insérer l'interface locale du réseau Béjaia, ainsi que l'adresse réseau local du réseau distant qui est le site Distant :

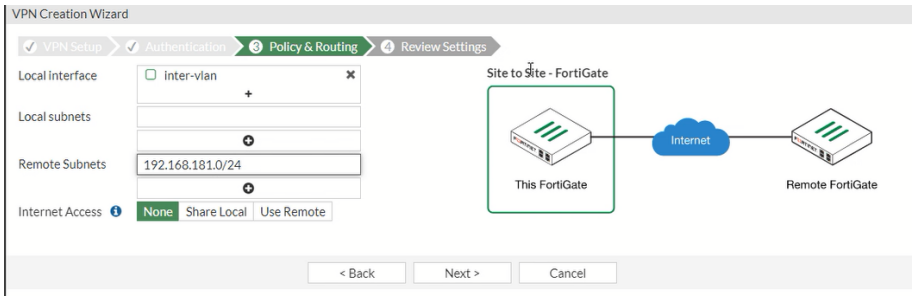

FIGURE 4.57 – Adresses IPsec.

Ensuite on va vérifier la configuration, une fois confirmer on va créer le tunnel :

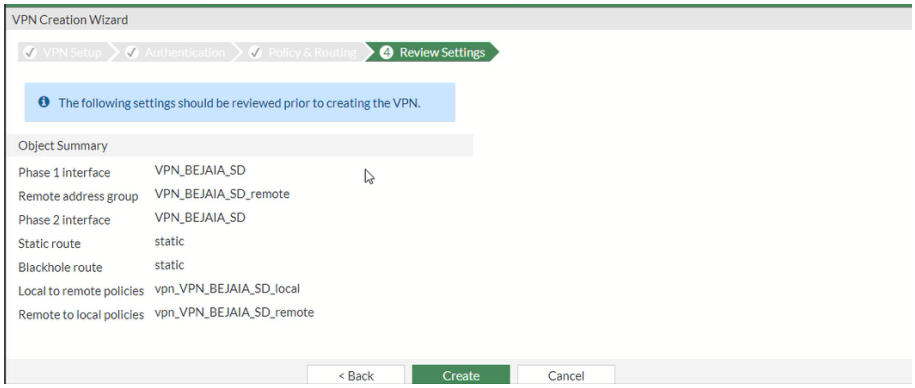

FIGURE 4.58 – Confirmation des informations.

Une fois le tunnel est créé on va de même créer un autre tunnel de site Distant vers Béjaia :

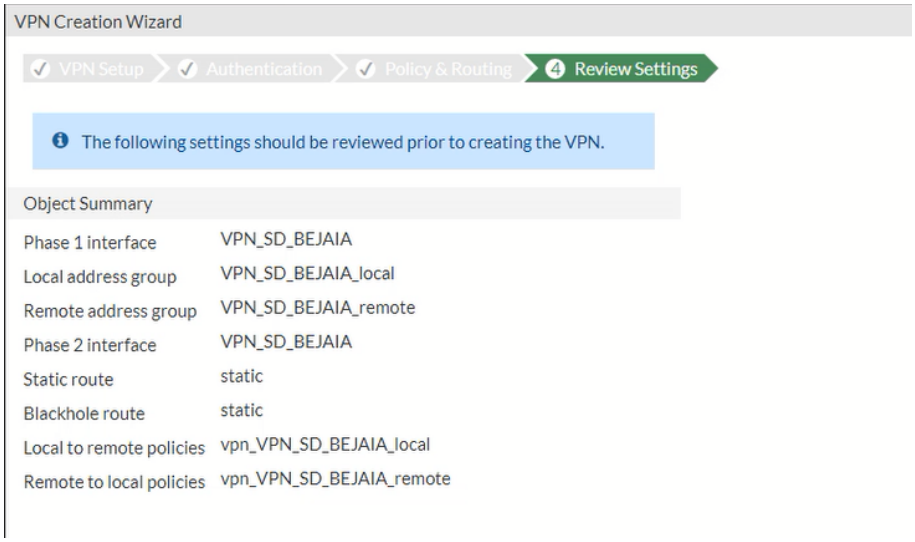

FIGURE 4.59 – IPsec Distant vers Béjaia.

Après avoir créer tous les tunnels.Dans le pare-feu Distant, on va créer des route statiques qui permettent d'atteindre les réseau du site Béjaia, la figure suivante illustre les routes créée :

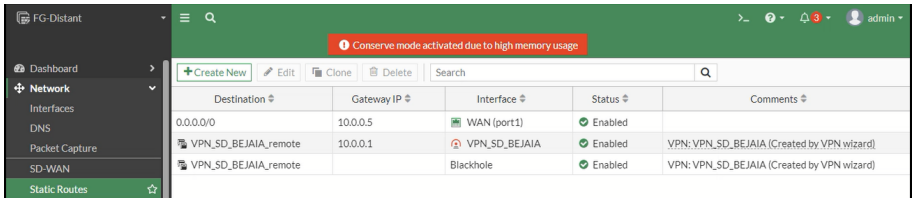

FIGURE 4.60 – Routes statiques de pare-feu Distant.

On fais de même dans le pare-feu FG-GE1, on va créer des routes permettant de connecter au réseau de site Distant :

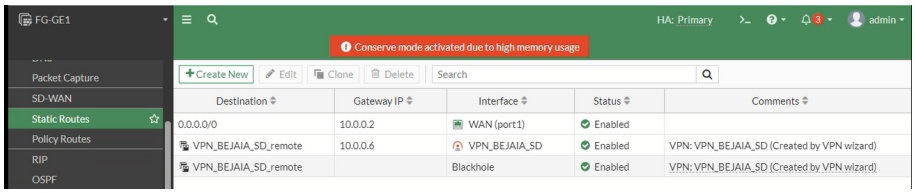

FIGURE 4.61 – Route statique de pare-feu FG-GE1

4.12.3 Configuration de protocole GRE (Generic Routing Encapsulation)

Tout d'abord on va créer une interface tunnel qu'on vas la nommé tunnel 1, et on va lui attribuer une adresse 172.16.0.1/30, ensuite on va fixer la taille de trame à 1400 pour éviter la charge en utilisant la commande « ip mtu 1400 », après on ajuste la taille maximum des segments tcp en utilisant la commande « ip tcp adjust-mss 1360 », on va insérer l'adresse source du tunnel qui est 10.0.0.10, et l'adresse destination qui est 10.0.0.1, la figure suivante illustre toute la configuration :

```
R-Alger#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-Alger(config)#interface tunnel 1
R-Alger(config-if)#ip add 172.16.0.1 255.255.255.252
R-Alger(config-if)#ip mtu 1400
R-Alger(config-if)#ip tcp adjust-mss 1360
R-Alger(config-if)#tunnel source 10.0.0.10
R-Alger(config-if)#tunnel destination 10.0.0.1
R-Alger(config-if)#exit
```

FIGURE 4.62 – Configuration de tunnel GRE dans le routeur.

Après avoir configurer le protocole GRE, on va créer des routes statiques envers les réseaux qu'on veut accéder, la figure suivante exhibe toutes les adresses :

```
R-Alger(config)#ip route 192.168.100.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.101.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.102.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.103.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.104.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.105.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.106.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.107.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.108.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.109.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.110.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.111.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.112.0 255.255.255.0 172.16.0.2
R-Alger(config)#ip route 192.168.113.0 255.255.255.0 172.16.0.2
R-Alger(config)#
R-Alger(config)#end
```

FIGURE 4.63 – Routes statiques GRE dans le router.

Après on va configurer le protocole dans le pare-feu, tout d'abord on va créer une interface tunnel qu'on va nommer « GRE-ALGER », et on va l'affecter au port de sortie qui est dans notre cas le port 1, ensuite on va insérer les passerelles de sortie et d'entrer comme illustre la figure suivante :

```
FG-GE1 # config sys gre-tunnel

FG-GE1 (gre-tunnel) # edit GRE-ALGER
new entry 'GRE-ALGER' added

FG-GE1 (GRE-ALGER) # set interface port1

FG-GE1 (GRE-ALGER) # set remote-gw 10.0.0.10

FG-GE1 (GRE-ALGER) # set local-gw 10.0.0.1

FG-GE1 (GRE-ALGER) # next

FG-GE1 (gre-tunnel) # end
```

FIGURE 4.64 – Création du tunnel GRE dans le pare-feu.

Une fois l'interface est créée, on va la configurer on lui effectuant l'adresse IP, ainsi qu'on va autoriser le ping dans le tunnel comme le montre la figure suivante :

```
FG-GE1 # config sys int

FG-GE1 (interface) # edit GRE-ALGER

FG-GE1 (GRE-ALGER) # set vdom root

FG-GE1 (GRE-ALGER) # set ip 172.16.0.2 255
<class_ip&net_netmask>    IP address and subnet mask (syntax = 1.1.1.1/24).

FG-GE1 (GRE-ALGER) # set ip 172.16.0.2 255.255.255.255

FG-GE1 (GRE-ALGER) # set allowaccess ping

FG-GE1 (GRE-ALGER) # set type tunnel

FG-GE1 (GRE-ALGER) # set remote-ip 172.16.0.1 255.255.255.255

FG-GE1 (GRE-ALGER) # set snmp-index 62

FG-GE1 (GRE-ALGER) # set interface port1

FG-GE1 (GRE-ALGER) # end
```

FIGURE 4.65 – configuration du tunnel créé dans le pare-feu.

Ensuite on va créer une route statique dans les paramètres de pare-feu :

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.0.0.2	WAN (port1)	Enabled	
0.0.0.0/0		Blackhole	Enabled	VPN: VPN_BEJAIA_SD (Created by VPN wizard)
192.168.182.0/24	172.16.0.1	GRE-FGA-RA (GRE-ALGER)	Enabled	
VPN_BEJAIA_ORAN_remote	10.0.0.14	VPN_BEJAIA_ORAN	Enabled	
VPN_BEJAIA_ORAN_remote		Blackhole	Enabled	
VPN_BEJAIA_SD_remote	10.0.0.6	VPN_BEJAIA_SD	Enabled	VPN:VPN_BEJAIA_SD(Created by VPN Wizard)
VPN_BEJAIA_SD_remote		Blackhole	Enabled	VPN:VPN_BEJAIA_SD(Created by VPN Wizard)

FIGURE 4.66 – Routes statiques GRE dans le pare-feu.

Et de même on va créer deux politiques de sécurité qui permet la rentrée et la sortie du trafic comme l'indique la figure suivante :

FIGURE 4.67 – politique de sécurité GRE dans le pare-feu.

4.12.4 Configuration VPN client to site

Dans le pare-feu FG-GE1 nous allons accéder aux paramètres du VPN, et nous dirigerons vers « SSL-VPN Settings »,on va générer un certificat qu'on va nommer « vpn-ssl » :

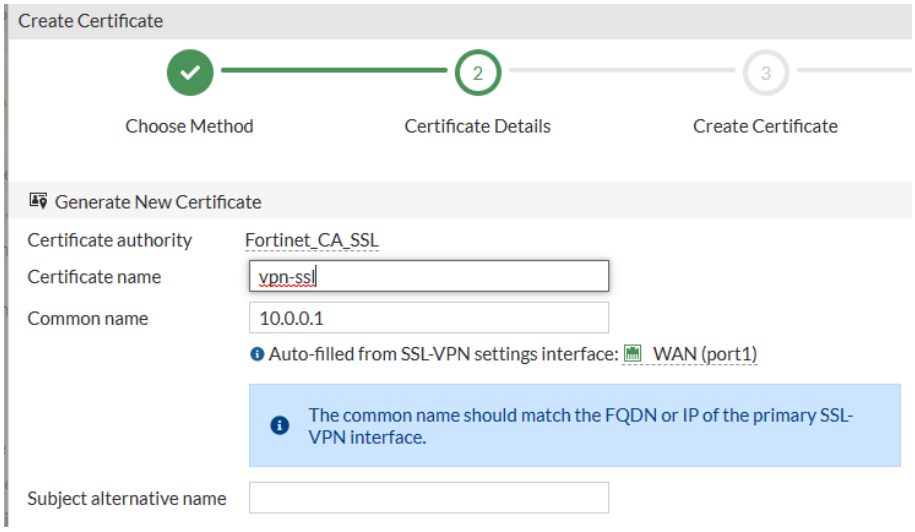

FIGURE 4.68 – Création d'un certificat.

Ensuite, on va choisir l'interface dans laquelle les clients vont rentrer a notre réseau qui est dans notre cas l'interface port1, et on va choisir le port 4444 :

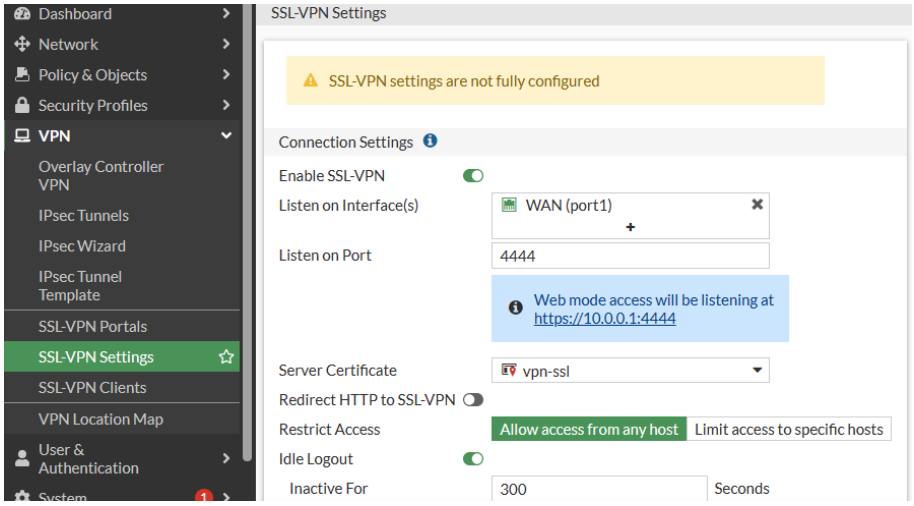

FIGURE 4.69 – Choix interface et port SSL.

On va créer des agents qui peuvent se connecter à notre réseau, le premier « agent1 » avec un mot de passe « 123456 » et un deuxième « agent2 » avec un mot de passe « 56789 » :

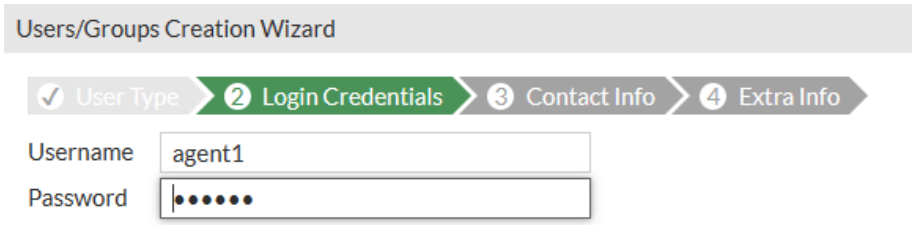

FIGURE 4.70 – Création agent1.

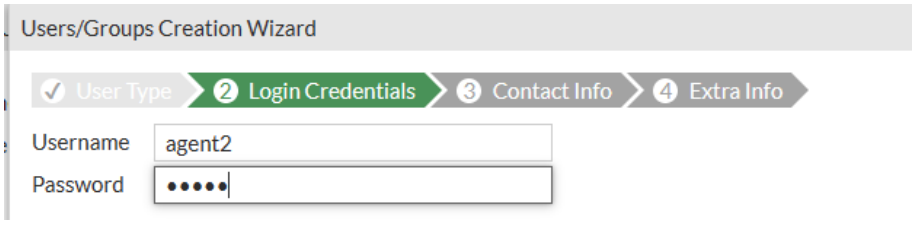

FIGURE 4.71 – Création agent2.

Ensuite on va créer un groupe des utilisateurs comme illustre les figures suivantes :

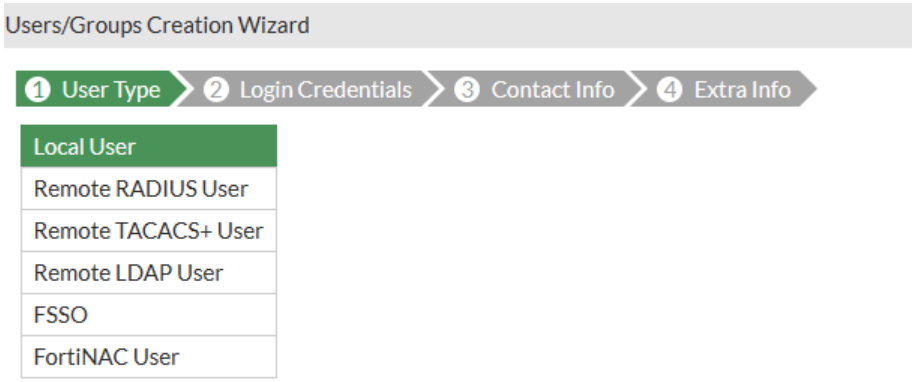

FIGURE 4.72 – Création d'un groupe.

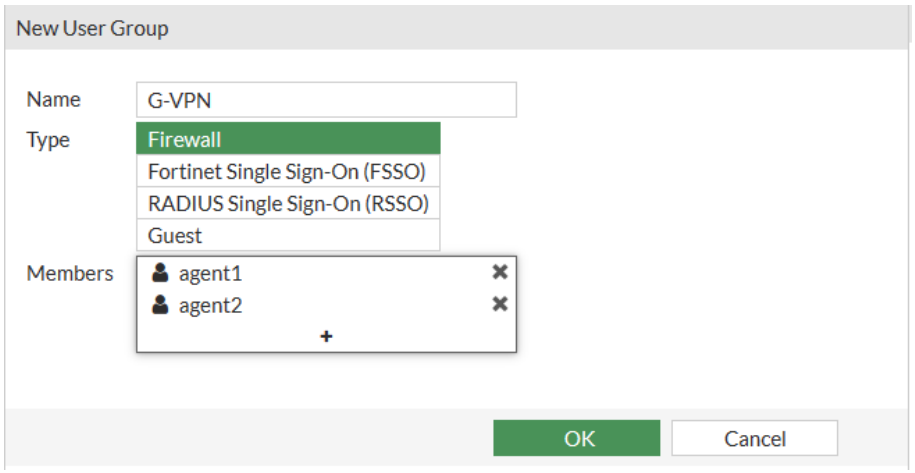

FIGURE 4.73 – Sélection des membres de groupe.

Dans l'authentification on va autoriser au groupe qu'on a créé d'accéder au réseau par full-access :

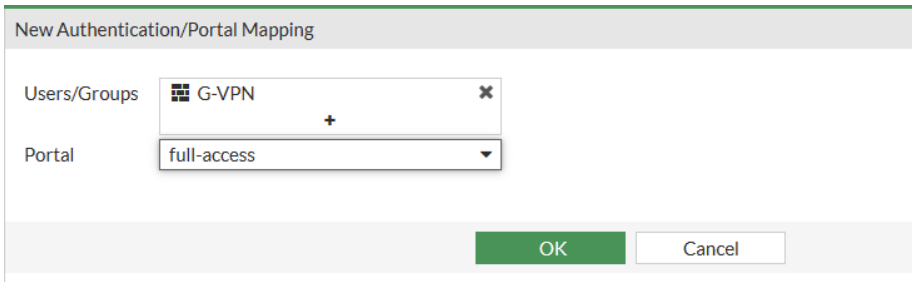

FIGURE 4.74 – Création d'une nouvelle authentification.

Une fois terminer on trouve tous les autorisations effectuer comme illustre la figure suivante :

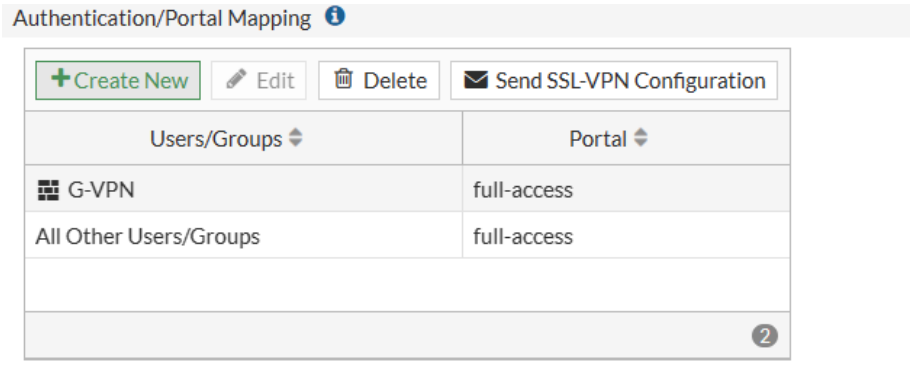

FIGURE 4.75 – Groupe des authentifications.

Une fois terminer, on doit créer une politique de sécurité qui permet aux utilisateurs à distant de se connecter à notre réseau comme montre la figure suivante :

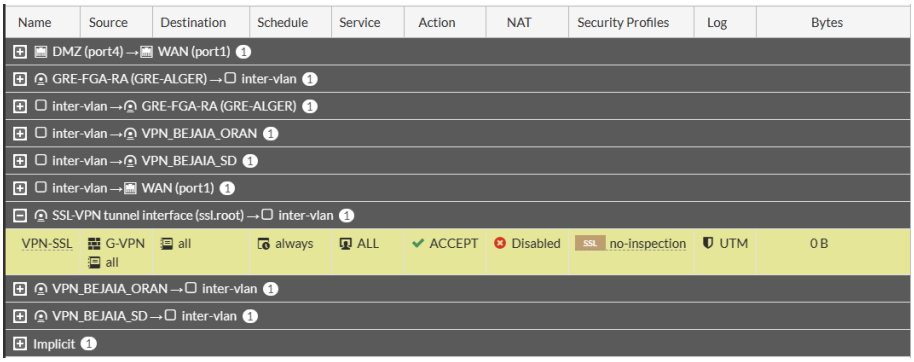

FIGURE 4.76 – Politique de sécurité SSL

4.13 Tests de validation des configurations

Dans cette partie, nous allons tester la validation des configurations effectuer dans ce chapitre à l'aide de la commande ping qui test la réponse d'un équipement dans le réseau, la commande ping permet d'envoyer des paquets de données d'un équipement vers un autre, si l'équipement à la réception reçois les paquets cela implique que la connexion est établie, sinon la connexion est échouée.

4.13.1 Ping inter-Vlan

pour tester la connectivité entre des Vlans différents, nous allons envoyer des paquets de données du PC16 qui appartient au Vlan 101 vers le PC14 appartenant au Vlan 100, la figure suivante illustre le résultat du test :

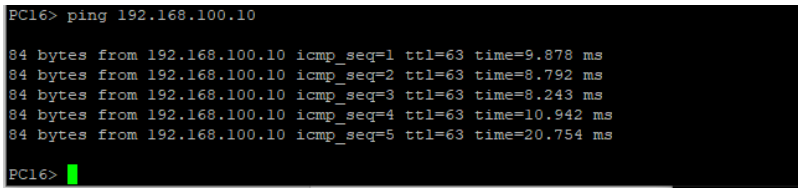

FIGURE 4.77 – Ping entre PC16 et PC14.

Pour vérifier la disponibilité de réseau en cas de panne, nous avons éteint la switch Core1 et on a vérifié la connectivité entre les deux PC26 appartenant au VLAN 106 avec le PC14 qui appartient vlan 100 :

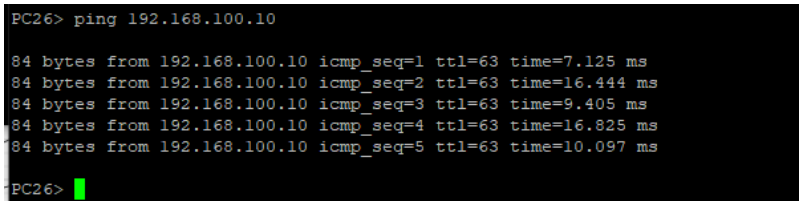

FIGURE 4.78 – Ping entre PC26 et PC14.

4.13.2 Test de VPN

Tout d'abord, nous allons tester la connectivité entre le PC4 appartenant au site Distant vers le PC14 de Vlan 100 de site AKBOU pour verifier la validité de la configuration VPN IPsec effectuée précédemment :

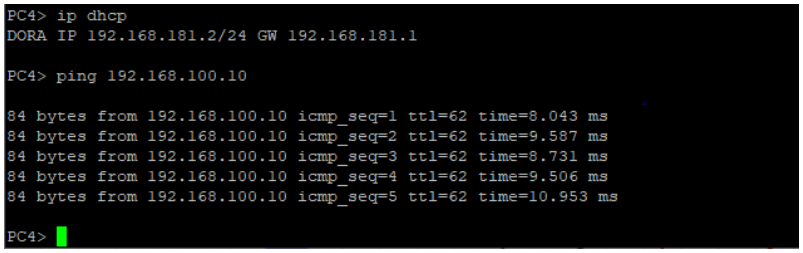

FIGURE 4.79 – Ping de PC4 vers PC14.

Pour vérifier la validation de Clustering Active-Active, nous allons éteindre la pare-feu FG-GE1 et tester à nouveau :

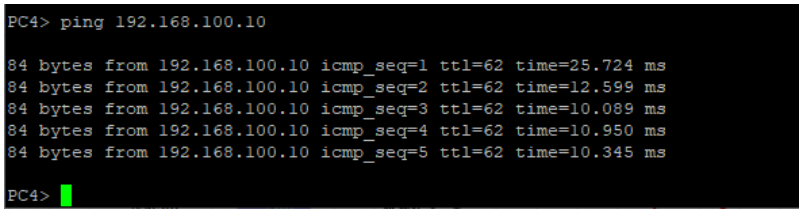

FIGURE 4.80 – Ping avec FG-GE1 éteint.

Nous constatons que le Ping est réussi, cella implique que le pare-feu FG-GE2 à pris le relais et devenu le pare-feu principal :

```
Primary     : FG-GE2          , FGVMEVWTPPNL_MDB, HA cluster index = 0
```

FIGURE 4.81 – Statut de FG-GE2.

Nous allons également tester la connectivité du PC4 vers PC14 tout en éteignant le FG-GE1 et le Core1 :

```
PC4> ping 192.168.100.10

84 bytes from 192.168.100.10 icmp_seq=1 ttl=62 time=7.138 ms
84 bytes from 192.168.100.10 icmp_seq=2 ttl=62 time=11.995 ms
84 bytes from 192.168.100.10 icmp_seq=3 ttl=62 time=12.941 ms
84 bytes from 192.168.100.10 icmp_seq=4 ttl=62 time=7.626 ms
84 bytes from 192.168.100.10 icmp_seq=5 ttl=62 time=12.300 ms

PC4>
```

FIGURE 4.82 – Ping avec FG-GE1 et Core1

Nous constatons que la connexion est établie même on éteignant le FG-GE1 et le Core1, ceci implique que le FG-GE2 et le Core2 ont pris le relais tout en garantissant le continuité de service.

4.13.3 Test de connectivité GRE

On va tester la connectivité du PC3 situé dans le site ALGER vers le PC14 situé dans le vlan 100 de site AKBOU :

```
PC3> ping 192.168.100.1

84 bytes from 192.168.100.1 icmp_seq=1 ttl=254 time=5.517 ms
84 bytes from 192.168.100.1 icmp_seq=2 ttl=254 time=4.163 ms
84 bytes from 192.168.100.1 icmp_seq=3 ttl=254 time=3.844 ms
84 bytes from 192.168.100.1 icmp_seq=4 ttl=254 time=4.103 ms
84 bytes from 192.168.100.1 icmp_seq=5 ttl=254 time=3.885 ms

PC3> ping 192.168.100.10

84 bytes from 192.168.100.10 icmp_seq=1 ttl=62 time=12.972 ms
84 bytes from 192.168.100.10 icmp_seq=2 ttl=62 time=8.235 ms
84 bytes from 192.168.100.10 icmp_seq=3 ttl=62 time=8.029 ms
84 bytes from 192.168.100.10 icmp_seq=4 ttl=62 time=7.750 ms
84 bytes from 192.168.100.10 icmp_seq=5 ttl=62 time=6.433 ms

PC3>
```

FIGURE 4.83 – Ping entre PC3 et PC14.

Nous remarquons que la ping est réussi entre les deux site Alger et site Akbou, ce qui implique la validité du tunnel créé.

4.13.4 Test de validation de VPN client to site

Nous allons se rendre sur le VMware et on lance l'application FortiClient, on va sur accès à distance ainsi sur VPN SSL, on va insérer un nom pour notre connexion, ensuite on va indiquer la passerelle qui permet de se connecter au réseau ainsi que le port et on clique sur sauvegarde comme illustre la figure suivante :

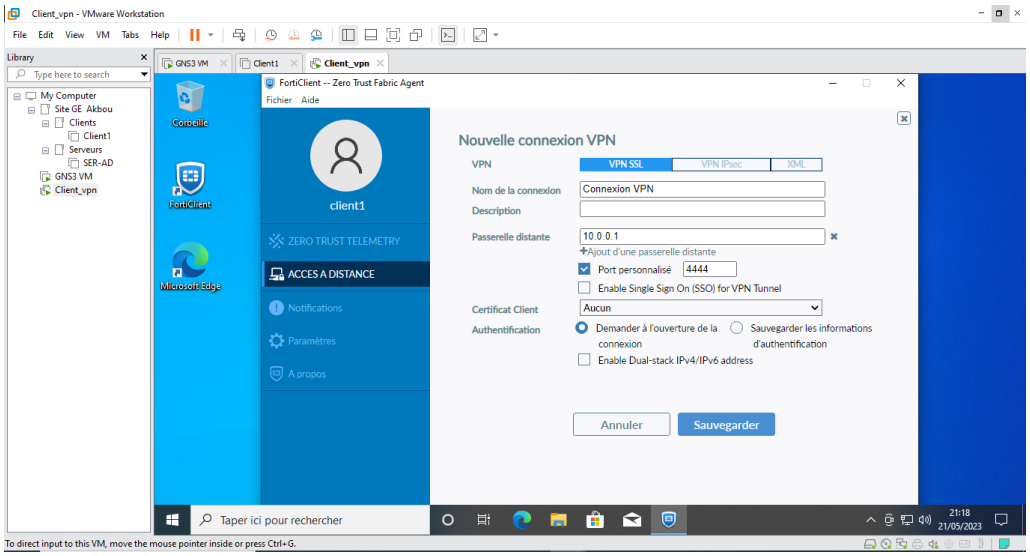

FIGURE 4.84 – Création d'une nouvelle connexion VPN.

Ensuite on va insérer les informations concernant notre agent, dans notre cas « agent1 » avec un mot de passe « 123456 », après on clique sur connecter :

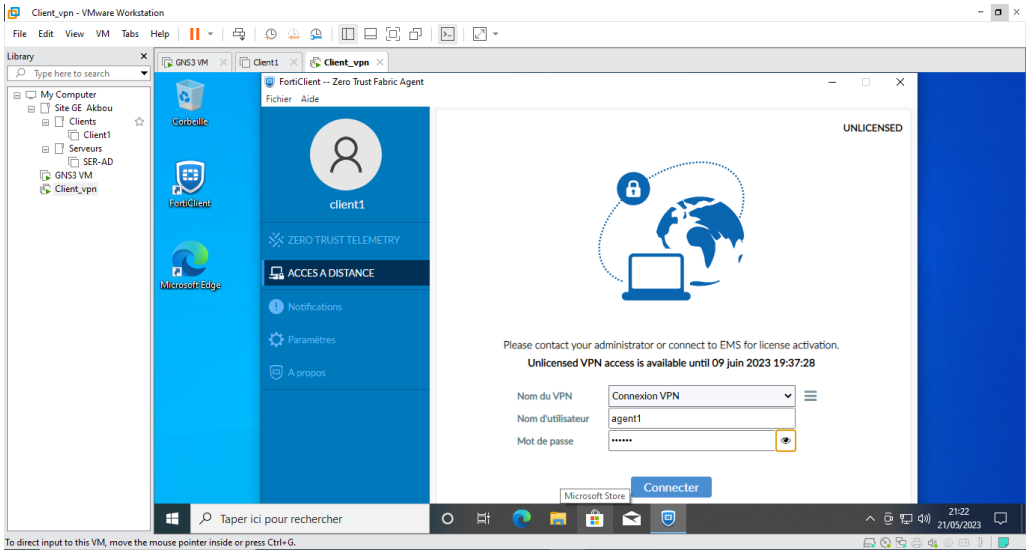

FIGURE 4.85 – Se connecter au VPN.

Une fois le nom d'utilisateur et le mot de passe sont confirmés, l'agent connecte et accède au réseau comme la montre la figure suivante :

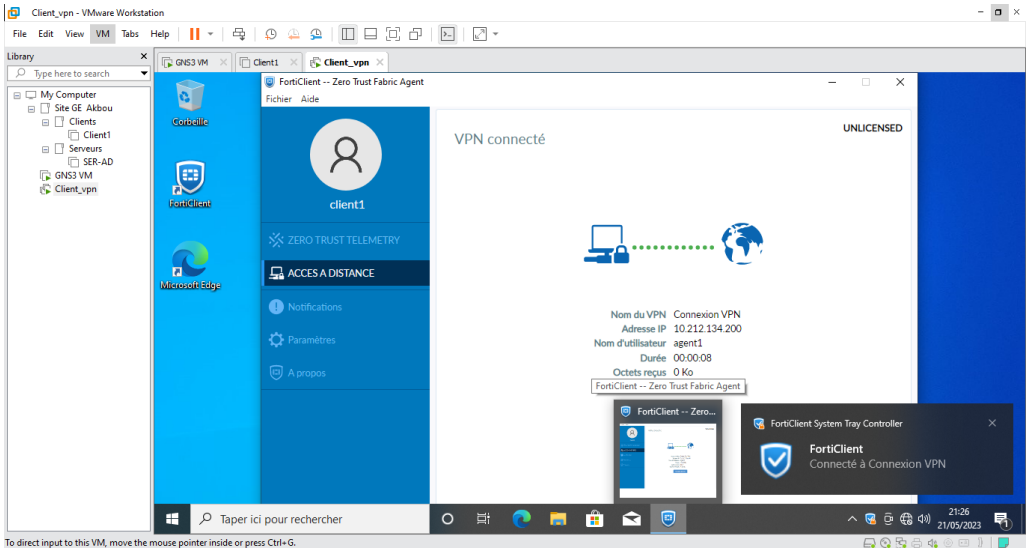

FIGURE 4.86 – Connexion établie VPN.

4.14 Conclusion

Dans ce chapitre, nous avons configuré notre réseau de manière à le rendre plus efficace, sécurisé et accessible. Nous avons utilisé des VLANs pour diviser le réseau en segments distincts, facilitant ainsi la gestion du trafic. Nous avons également mis en place des protocoles de regroupement de liens (LACP et PAGP) pour optimiser l'utilisation de la bande passante et augmenter la résilience en cas de défaillance.

Pour renforcer la sécurité, nous avons créer deux zone DMZ qui permettent d'offrir une approche stratégique pour héberger différents types de services, nous avons également mis en place un cluster Active-Active, assurant ainsi une haute disponibilité des services. Enfin, nous avons configuré des connexions VPN sécurisées, y compris l'IPsec, le GRE et le Client-to-Site, permettant aux utilisateurs distants de se connecter à notre réseau de manière sécurisée depuis n'importe quel endroit. En conclusion, ces mesures de configuration réseau, telles que l'utilisation des VLANs, la création d'une DMZ, la mise en place d'un cluster Active-Active et la configuration de connexions VPN sécurisées, contribuent à améliorer la performance, la sécurité et l'accessibilité de notre réseau.

Conclusion générale

En conclusion de notre projet de fin d'études portant sur l'étude et l'amélioration du réseau de SPA Générale Emballage, nous avons réalisé une étude supervision du réseau en place, approfondie de l'existant et identifié les failles potentielles. Notre objectif principal était de proposer une solution pour améliorer la haute disponibilité du réseau tout en le sécurisant. Pour atteindre cet objectif, nous avons mis en place plusieurs protocoles et technologies clés. Tout d'abord, nous avons configuré les protocoles STP et VTP pour assurer une meilleure gestion des boucles et une gestion efficace des VLAN, garantissant ainsi une meilleure disponibilité du réseau. Ensuite, nous avons mis en œuvre les VPN IPsec et GRE ainsi que le client-to-site VPN. Ces solutions de connectivité sécurisée nous ont permis de créer des tunnels chiffrés pour relier de manière sécurisée les utilisateurs distants au réseau de SPA Générale Emballage, renforçant ainsi la sécurité et l'accessibilité. Pour augmenter la capacité et la résilience du réseau, nous avons configuré les protocoles LACP et PAGP. Ces protocoles de regroupement de liens nous ont permis de combiner plusieurs liens physiques en une seule agrégation logique, améliorant ainsi les performances et la disponibilité du réseau.

Enfin, nous avons mis en place un clustering active-active pour assurer une haute disponibilité et une répartition de charge optimale. Ce mode de clustering nous a permis de fournir une redondance et une continuité de service en cas de panne d'un nœud, en répartissant les charges de manière équilibrée sur les nœuds actifs.

Dans l'ensemble, notre projet a permis d'améliorer significativement la disponibilité du réseau de SPA Général Emballage en identifiant les failles, en proposant des solutions adaptées et en mettant en œuvre les protocoles et technologies appropriés. Ces efforts contribuent à garantir un réseau plus fiable, sécurisé et performant, soutenant ainsi les activités de l'entreprise et assurant une meilleure expérience utilisateur.

Dans le cadre de l'amélioration de la haute disponibilité du réseau de SPA Générale Emballage, plusieurs perspectives professionnelles peuvent être envisagées. Tout d'abord, l'adoption de la technologie SD-WAN offre des possibilités de gestion avancée du trafic, permettant une optimisation dynamique des chemins et une résilience accrue en cas de défaillance de lien. Ensuite, la virtualisation des fonctions réseau (NFV) offre des avantages en termes de flexibilité et d'évolutivité, permettant une gestion plus efficiente des ressources réseau. Parallèlement, la mise en place de systèmes de détection et de prévention des intrusions (IDS/IPS) renforce la sécurité en identifiant rapidement les attaques potentielles et en prenant des mesures de protection. Enfin, l'élaboration d'un plan de reprise après sinistre (DRP) garantit la continuité des activités en cas de catastrophe en définissant des procédures de sauvegarde, de restauration et de reprise des services essentiels. Ces initiatives permettront à SPA Générale Emballage de renforcer la fiabilité, la sécurité et la disponibilité de son réseau, soutenant ainsi ses opérations et offrant une meilleure expérience à ses utilisateurs.

Annexe A

La sécurité informatique

La sécurité informatique est le domaine de l'informatique qui analyse les propriétés de sécurité des systèmes informatiques. Elle consiste à protéger les données ainsi que les ressources matérielles et logicielles telles que les ordinateurs, les serveurs, les appareilles mobiles, les réseaux et les données contre les attaques malveillantes en utilisant des mécanismes de contrôle. Ces derniers permettant d'assurer le bon fonctionnement du système. Les critères de la sécurité informatique

• La confidentialité des données informatiques

La confidentialité fait référence aux efforts d'une organisation pour garder ses données privées ou secrètes. En pratique, il s'agit de contrôler l'accès aux données pour empêcher leur divulgation non autorisée.

• L'intégrité des données

L'intégrité consiste à s'assurer que les données n'ont pas été falsifiées et qu'elles sont donc correctes, authentiques et fiables.

•La disponibilité des données informatiques

La disponibilité signifie que les réseaux, les systèmes et les applications sont opérationnels. Il garantit que les utilisateurs autorisés disposent d'un accès rapide et fiable aux ressources en cas de besoin.

• La non-répudiation

Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

• L'authentification

L'authentification vise à vérifier l'identité d'un processus communicant. Plusieurs solutions simples sont mises en œuvre pour cela, comme l'utilisation de l'identifiant et de mots de passe. Les dimensions de la sécurité informatique

La sécurité physique

Elle concerne tous les aspects liés à l'environnement dans lequel les systèmes se trouvent. C'est la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, postes de travail des personnels, alimentation électrique, climatisation, etc

• Mesures pour la sécurité physique :

– Respect de normes de sécurité.

– Protection de l'environnement contre les accidents (incendie, température, humidité, ...).

– Protection des accès physiques.

– Application de la redondance physique.

– Mise en œuvre d'un plan de maintenance préventive (ex. test) et corrective (ex. pièce de rechange), etc. La sécurité d'exploitation Elle concerne la sensibilisation des utilisateurs aux problèmes de sécurité. Elle vise le bon fonctionnement des systèmes.

Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.

• Mesures pour la sécurité d'exploitation :

– Mise en œuvre d'un plan de sauvegarde, de secours, de continuité et de tests.

– Application des inventaires réguliers et si possible dynamiques.

– Gestion du parc informatique, des configurations et des mises à jour.

– Contrôle et suivit de l'exploitation.

La sécurité logique

Elle concerne la sécurité au niveau des données, notamment les données du système d'information, les applications ou encore les systèmes d'exploitation. Elle fait référence à la réalisation de mécanismes de sécurité par logiciel.

• Mesures pour la sécurité logique :

– Mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation.

– Mise en place des dispositifs pour garantir la confidentialité, dont la cryptographie.

– Gestion efficace des mots de passe et des procédures d'authentification.

– Mise en place des mesures antivirus et de sauvegarde d'informations sensibles, etc.

La sécurité applicative

Ses objectifs se concernent sur la protection des applications informatique contre les vulnérabilités et les attaques potentielles, et d'éviter les ‹ bugs › dans les applications.

• Mesures pour la sécurité applicative :

– Application d'une méthodologie de développement des applications.

– Assurance de la robustesse des applications.

– Réalisation de contrôles programmés et des jeux de test.

– Mise en œuvre d'un plan de migration d'applications critiques.

– Mise en œuvre d'un plan d'assurance de sécurité, etc.

La sécurité des télécommunications

Elle concerne les technologies réseau, les serveurs de l'infrastructure, les réseaux d'accès, etc. Elle permet d'offrir à l'utilisateur final une connectivité fiable et de qualité de « bout en bout ».

• Mesures pour la sécurité télécommunications :

– La mise en œuvre d'un canal de communication fiable entre les correspondants, quels que soit le nombre et la nature des éléments intermédiaires. Cela implique la réalisation d'une infrastructure réseau sécurisé au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements.

Annexe B

Vulnérabilités

Une vulnérabilité est simplement une faiblesse qui peut être exploitée par un attaquant pour effectuer des actions non autorisées au sein d'un ordinateur ou d'un système réseau.

Il existe des différentes catégories pour placer les vulnérabilités, on trouve notamment :

• Vulnérabilités liées aux domaines physiques :

- Manque de redondance et de ressource au niveau équipement.

- Accès aux salles informatiques non sécurisées.

-Absence ou mauvaise stratégie de sauvegarde des données.

• Vulnérabilités liées aux domaines organisationnels :

- Manque de Ressources humaines, de personnels qualifiés et de communications.

-Absence de Contrôles périodiques, Documents de procédures adaptées à l'entreprise.

• Vulnérabilités liées aux domaines technologiques :

- Pas de mises à jour des systèmes d'exploitation et des correctifs.

- Pas de contrôle suffisant sur les logiciels malveillants.

- Récurrence des failles et absence de supervision des événements.

- Réseaux complexes, non protégés.

Les types d'attaques

Une attaque est une tentative délibérée de pénétrer un système informatique pour accéder, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé.

Il existe un grand nombre d'attaques cependant, dans le cadre de ce mémoire, nous concentrons sur une brève description de certaines d'entre elles :

Man in the middle

dite en français l'homme au milieu, c'est une attaque d'interception, consiste d'intercepter les communications entre deux entités sans que l'une ni l'autre ne puisse se douter que le canal de communication est compromis, l'objectif de l'attaquant est d'intercepter, de lire ou de manipuler toute communication entre la victime et sa ressource sans se faire remarquer.

Virus

un programme malveillant conçu pour endommager ou perturber le fonctionnement d'un système informatique.

Les virus peuvent contaminer une machine de plusieurs manières :

• Téléchargement de logiciel puis exécution de celui-ci sans précautions.

• Ouverture sans précautions de documents contenant des macros,

• Pièce jointe de courrier électronique (exécutable, script type vbs...).

• Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier (normalement, JavaScript est sans danger).

• Exploitation d'un bug du logiciel de courrier (effectuer régulièrement les mises à jour) Les virus peuvent causer des dommages mineurs tels que des ralentissements du système ou des problèmes de connectivite, ou des dommages majeurs tels que la perte de donnes ou la corruption du système.

Déni de service (Dos)

est une attaque dont le but n'est pas de voler des informations à distance sur une machine, mais plutôt de rendre un service ou un réseau complet complètement paralysé. Cette attaque a pour conséquence que les utilisateurs ne peuvent plus accéder aux ressources de services ou du réseau concerne.

Cheval de Troie

une technique d'attaque informatique, sous forme d'un logiciel malveillant qui se présente comme un programme légitime, utile même attrayante. Mais une fois installer ils exécutent des actions caches et nuisibles, et ils peuvent effectuer des taches tels que voler des informations sensibles, ou d'installer d'autres logiciels malveillants.

Annexe C

Les mécanismes de défense et de sécurité

Un mécanisme est un moyen pour appliquer une politique de donnes. Pour assurer une sécurité optimale, il déconseillait de compter sur un seul mécanisme de sécurité. En effet, la combinaison de plusieurs mécanismes permet d'offrir une sécurité plus fiable et efficace.

Les antivirus

Des logiciels conçus pour identifier, détecter et supprimer les virus et les logiciels malveillants. Il joue également un rôle préventif en empêchant les virus d'infecter les systèmes informatiques et de leur nuire. Il y a essentiellement deux modes de fonctionnement des logiciels antivirus :

• Mode statique : le logiciel est activé uniquement sur ordre de l'utilisateur, par exemple pour déclencher une inspection du disque dur.

• Mode dynamique : le logiciel est actif en permanence, et il scrute certains événements qui surviennent dans le système, ce qui induit une consommation non-négligeable de ressources telles que temps de processeur et mémoire, mais permet une meilleure détection des attaques, notamment par analyse comportementale des logiciels suspects d'être contaminés.

Le cryptage

Le cryptage (ou le chiffrement) est une technique de codage qui permet de protéger la confidentialité des données en les transformant en une forme illisible pour les personnes qui n'ont pas la clé de déchiffrement.

Il existe deux déférents type de cryptage :

• Cryptage symétrique : Ou chiffrement à clé secrète, utilise la même clé pour le chiffrement et le déchiffrement des données et la clé doit être partagée secrètement avec le destinataire.

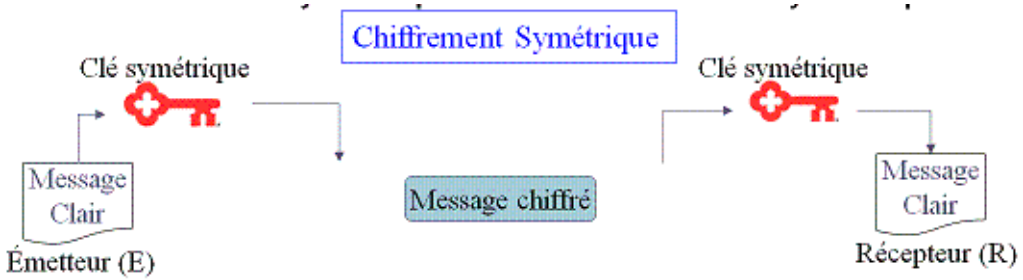

FIGURE 4.87 – Chiffrement Symétrique.

• Cryptage asymétrique : Ce chiffrement est aussi appelé chiffrement à clés publiques, utilise une paire composée d'une clé publique pour le chiffrement, et d'une clé privée pour le déchiffrement.

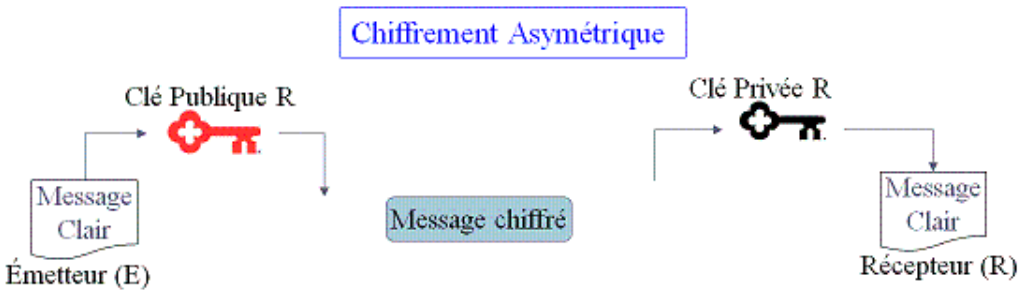

FIGURE 4.88 – Chiffrement Asymétrique .

Les pares-feux

Sont des systèmes de sécurité du réseau logiciel ou matériels qui filtrent le trafic réseaux entrant et sortant, en appliquant des règles de sécurité prédéfinis pour protéger les réseaux contre les attaques malveillantes et empêchent les connexions non autorisées.

Le fonctionnement d'un pare-feu : le fonctionnement d'un pare-feu repose sur un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).
- Autoriser uniquement les communications ayant été explicitement autorisées : « Tout ce qui n'est pas explicitement autorisé est interdit ».
- D'empêcher les échanges qui ont été explicitement interdits.

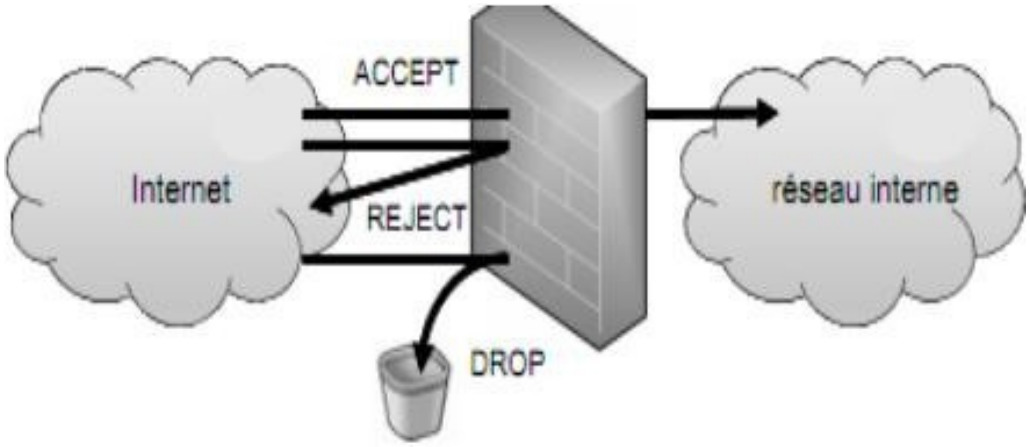

FIGURE 4.89 – fonctionnement d'un pare-feu .

Segmentation

La segmentation est une technique couramment utilisée pour atténuer la congestion d'un réseau. Cette technique consiste à diviser l'architecture du réseau en sections afin de réduire la taille des domaines de diffusion (broadcast) et ainsi d'augmenter l'efficacité du réseau. Cette technique peut aussi être utilisée pour augmenter la sécurité d'un réseau. En effet, elle permet d'implémenter des dispositifs de sécurité entre les frontières des différents segments. Ce qui permet de mieux contrôler le trafic en destination des ressources critiques.

La segmentation peut s'effectuer de plusieurs façons :

• Segmentation par séparation physique : La séparation physique des sous-réseaux est probablement la méthode de segmentation la plus sécurisée, mais elle est également la plus coûteuse en termes de cartes réseau, d'infrastructures de commutations additionnelles et intensifie l'administration.

• Segmentation avec des VLANs : Un VLAN (Virtual Local Area Network ou Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique. Il s'agit d'un dispositif de la couche 2 (liaison de données) qui fait ce que les VPNs font au niveau de la couche 3 (réseau). Les équipements connectés à un vlan ne peuvent pas communiquer directement avec les équipements connecte à un autre vlan, à moins qu'un routeur ne soit utilisé pour connecter les deux vlans. Cependant la sécurité d'un vlan dépend en partie de la configuration des commutateurs qui relient les différents segments, car la bonne assignation des ports est essentielle pour éviter tout accès non autorisé et prévenir les failles de sécurité.

• Segmentation en fonction des services : une autre technique de segmentation est de considérer les services fournis par les différentes ressources et segmenter le réseau en conséquence. Chaque segment est alors défini selon le service fourni par ses ressources. Cette approche permet un contrôle très rigoureux entre les différents segments du réseau, mais elle peut mener à un grand nombre de segments dépendamment des services disponibles. Ce qui nécessite également des dispositifs de sécurité additionnels.

• Segmentation utilisant une DMZ : Les administrateurs réseau se considèrent en guerre contre les attaquants et les utilisateurs même de leurs systèmes. Il n'est pas surprenant qu'ils empruntent alors des termes militaires comme DMZ (De Militarized Zone). La DMZ est une méthode de sécurité qui permet de séparer les ressources publiques et privées d'un réseau en créant une zone tampon intermédiaire. La DMZ est un réseau qui se situe entre l'internet et le réseau prive, contenant des serveurs et des applications accessibles depuis l'internet, comme des serveurs Web ou des serveurs de messagerie, tout en isolant le réseau prive qui contient les ressources sensibles.

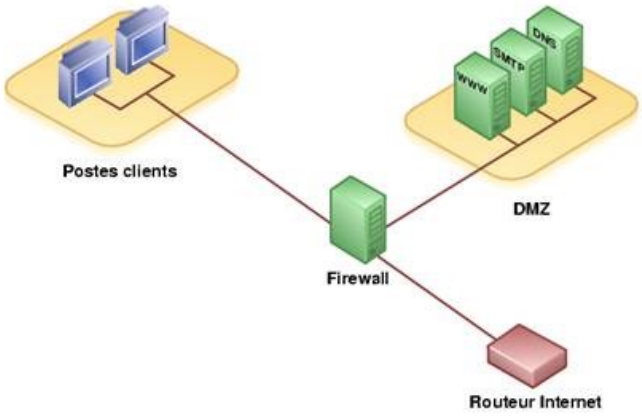

FIGURE 4.90 – exemple d'un réseau segmente avec une Dmz.

Les avantages de la DMZ

• Facilite le contrôle d'accès : en permettant la mise en place de règles strictes de filtrage pour autoriser uniquement les connexions nécessaires aux services et ressources exposés. Cela renforce la sécurité en limitant l'exposition du réseau interne

aux connexions non autorisées.

• Empêcher la reconnaissance du réseau : elle réduit la visibilité et la reconnaissance potentielles du réseau interne par des acteurs malveillants. Cela complique leur tâche pour obtenir des informations sur les systèmes internes de l'organisation.

• Elle utilise des mécanismes de traduction d'adresses réseau (NAT) pour masquer les adresses IP internes et utiliser des adresses publiques pour les services de la DMZ. Cela empêche les attaquants d'utiliser une adresse IP interne pour accéder ou perturber le réseau.

Annexe D

Configuration de VTP dans le Core2 est illusté dans la figure suivante :

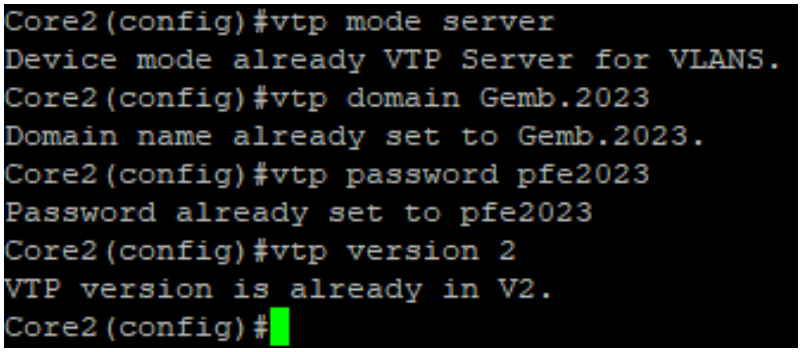

FIGURE 4.91 – configuration du vtp en mode server2

Vérification de la création des Vlans dans le switch Core2 est monté dans la figure suivante :

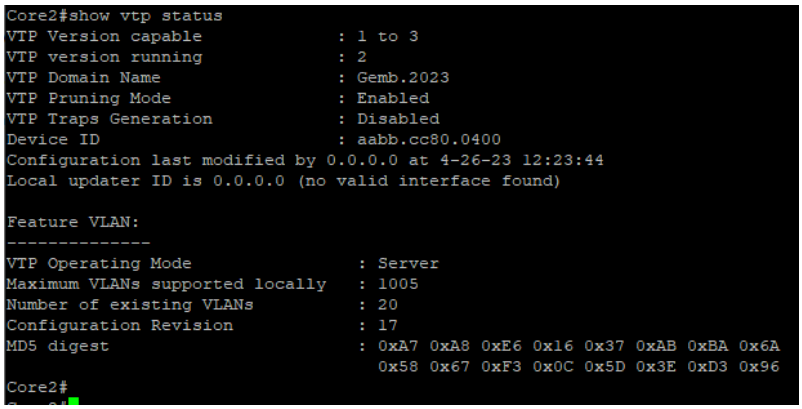

FIGURE 4.92 – vérification du vtp core2

Vérification du protocole STP en utilisant la commande « show running-config » :

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100-106 priority 20480
spanning-tree vlan 107-113 priority 28672
!
```

FIGURE 4.93 – vérification de la configuration du STP core1.

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 100-106 priority 28672
spanning-tree vlan 107-113 priority 20480
!
```

FIGURE 4.94 – vérification de la configuration du STP core2.

Configuration du protocole LACP dans le Core2 :

```
Core2(config)#interface range ethernet 3/2-3, ethernet 2/1
Core2(config-if-range)#channel-group 2 mode active
Core2(config-if-range)#exit
Core2(config)#port-channel load-balance src-dst-mac
Core2(config)#end
Core2#wr
*May 15 11:14:20.977: %SYS-5-CONFIG_I: Configured from console by console
Core2#wr
Building configuration...
Compressed configuration from 1513 bytes to 899 bytes[OK]
Core2#
```

FIGURE 4.95 – configuration du protocle LACP core2.

La vérification de la configuration du protocole PAGP dans le switch d'accès E3 :

```
SW-E3#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
4      Po4(SU)         PAgP      Et0/0(P)    Et0/1(P)

SW-E3#
```

FIGURE 4.96 – vérification de la configuration du PAGP E3.

Bibliographie

[1] Dordoigne,José. Réseaux informatiques. 9. France, Editions ENI, 2022.

[2] P.Guy. Initiation-aux-réseaux, Eyrolles 8ème édition,2014.

[3] ATELIN, Philippe et DORDOIGNE, José. TCP/IP et les protocoles Internet. Editions ENI, 2006.

[4] MONTAGNIER, Jean-Luc. Construire son réseau d'entreprise. Eyrolles, 2001.

[7] Kim-Loan Thai, Véronique Vèque, Simon Znaty. Architecture des réseux haut débit.Hermès - Lavoisier, 1995.

[10] Document interne de Général Emballage.

[15] Pérez, André. Architecture des réseaux fixes.Hermès - Lavoisier, 2011.

[16] Dordoigne, José. Les réseaux : entraînez-vous à l'administration d'un réseau. France, Editions ENI, 2004.

[17] Pignet, François. Réseaux informatiques : supervision et administration. France, Editions ENI, 2007.

[18] TOUTAIN, Laurent. Réseaux locaux et Internet. Hermès, 2003.

[19] Jarray Belgacem. Réseaux informatiques. Edition Ellipses, 2015.

[20] HOMCHAUDHURI, S. et FOSCHIANO, M. Cisco Systems' Private VLANs : Scalable Security in a Multi-Client Environment. 2010.

[21] Le grand livre de sécuritéinfo, http :// www.sécuritéinfo.com, consulté le 23 Mars 2016.

[22] F. Nolot, "Cours5-VTP", Académie Cisco, 2007.

[23] CARPENTIER, Jean-François. La sécurité informatique dans la petite entreprise : état de l'art et bonnes pratiques. Editions ENI, 2009.

[24] LASSERRE Xavier et KLEIN Thomas : Réseaux Privés Virtuels - Vpn, 2014.

[25] Helali, Saida. Intégration des infrastructures réseaux et systèmes : conception, implémentation, sécurité et supervision. Royaume-Uni, Iste editions., 2021.

[27] VAUCAMPS A. , "cisco CCNA", ENI édition, 2010.

[29] FIDÉLIS, RAMANANTSALAMA Nanah. Mise à jour de l'infrastructure informatique d'InnovaCall en matière de haute disponibilité et de sécurité. Thèse de doctorat. Paris 7.

[30] Jean-François Pillou. Tout sur les réseaux et internet. 4e-edition .2015.

[31] AOUDJIT, Rachida. 1. Thèse de doctorat. Université Mouloud Mammeri..

[32] G. PUJOLLE. Les réseaux. 5e-edition Septembre .2004.

[33] RAHOUAL, Malek et SIARRY, Patrick. Réseaux informatiques : conception et optimisation. Technip, 2006.

Webographie

[5] https ://featherbear.cc/UNSW-COMP3331-0/post/peer-to-peer-architecture /(consulté le 23 avril 2023).

[6] https ://www.malekal.com/le-modele-ou-architecture-client-serveur/ (consulté le 23 avril 2023).

[8] https ://cablage-informatique.com/topologie-en-bus-reseau-etoile-avantages-inconvenients/(consulté le 25 avril 2023).

[9] https ://www.proconcept-service.com/installation-reseau/ (consulté le 25 avril 2023).

[11] https ://initone.dz/pare-feu/fortinet-fortigate/ (consulté le 1 mai 2023).

[12] https ://www.cisco.com/c/support/switches/catalyst-3750v2-48ps-switch/model.html/ (consulté le 1 mai 2023).

[13] https ://www.cisco.com/c/support/switches/catalyst-2960s-48lps-l-switch/model.html/ (consulté le 1 mai 2023).

[14] https ://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/-series.html/(consulté le 1 mai 2023).

[26] http ://cisco.ofppt.info/ccna3/course/module3/3.1.2.2/3.1.2.2.html/ (consulté le 8 mai 2023) .

[28] Https ://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/, (consulté le 10 mai 2023)

[34] http ://www.frameip.com/vpn/(consulté le 1 mai 2023).

Résumé

De nos jours, la haute disponibilité est quasi-indispensable pour le bon fonctionnement de n'importe quel réseau informatique. Pour cela, la présente étude consiste à désigner une politique de sécurité approfondie au niveau de réseau informatique de Général Emballage, cette politique de sécurité consiste à mettre en place une redondance et une disponibilité dans le réseau. A l'aide du simulateur GNS3, une architecture hiérarchique interconnectant différent équipements est proposée assurant ainsi la haute disponibilité permettant à Général Emballage d'avoir un réseau plus fiable, sécurisé et performant.

Abstract

Nowadays, high availability is almost essential for the proper functioning of any computer network. Therefore, this study aims to establish a comprehensive security policy for the Général Emballage computer network. This security policy focuses on implementing redundancy and availability within the network. Using the GNS3 simulator, a hierarchical architecture that interconnects various devices is proposed, ensuring high availability and enabling Général Emballage to have a more reliable, secure, and efficient network.