**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

# Optimisation de la sécurité d'un réseau à multicouches

**Préparé par :**

- HAMANE Souhila
- KASMI Samy

**Dirigé par :**

Mr TOUAZI Djoudi

Mr. Djebari Yassine

**Examiné par :**

Mr. MEKHMOUKH Abdenour

Mme. GHERBI Meriem

**Année universitaire** : **2023/2024**

# *Remerciements*

*Avant tout, on remercie ALLAH le Tout-puissant de nous avoir donné le courage, la volonté et la patience de mener à terme ce présent travail dans des meilleures conditions.*

*On tient tout d'abord à remercier notre encadrant Mr. Touazi Djoudi, pour sa contribution et son aide qui nous ont été indispensable pour la réalisation de ce travail ainsi que toutes ces remarques constructives qui nous ont permis d'approfondir les connaissances scientifiques.*

*Nous adressons aussi nos remerciements au président et aux membres du jury qui nous ferons l'honneur en acceptant de juger notre travail.*

*Nous tenons aussi à remercier également tous les enseignants qui ont assurés notre formation durant notre cycle universitaire. Ainsi, que tout le personnel du département ATE.*

*Enfin, dans ces dernières lignes on tient à remercier nos parents, nos sœurs et nos frères, pour les conseils et les encouragements qu'ils nous ont toujours prodigues ainsi que pour leur soutien tant moral que financier. Sans eux, on n'en serait pas ou on n'en est et ce qu'on est.*

*Merci encore à tous…*

# *Dédicaces*

*Je dédie ce modeste travail, rendu possible grâce à l'aide de Dieu, le Tout-Puissant.*

*À ma chère mère, qui est la bonté même, la source de tendresse et l'exemple de dévouement. Ton soutien constant et tes prières ont toujours été mon pilier.*

*À mon cher père, rien ne vaut les efforts que tu as fournis jour et nuit pour mon éducation et mon bien-être. Ce travail est le résultat de tes sacrifices pour ma formation.*

*À vous deux, mes parents adorés, qui avez su m'encourager et me soutenir tout au long de mes études. Aucune dédicace ne saurait rendre justice aux sacrifices que vous avez faits depuis ma naissance, pendant mon enfance et jusqu'à l'âge adulte.*

*Vous êtes la lumière de ma vie et l'étoile qui guide ma réjouissance. Que Dieu vous protège.*

*A ma merveilleuse sœur, Fatima pour ta générosité et ton amour inconditionnel qui ont rendu possible ce parcours d'éducation que je chérirai toujours. Chaque succès que je célèbre est un hommage à ton sacrifice et à ta confiance en moi. Merci pour avoir investi dans mon avenir de la manière la plus précieuse qui soit.*

*À mes chères sœurs Zahia, Sarah, pour votre amour, vos conseils et vos encouragements constants. Votre gentillesse, votre sagesse et votre joie de vivre ont toujours été une source d'inspiration, et vous êtes toujours à mes côtés. Je vous en suis profondément reconnaissante.*

*A Mon petit cher frère, Lyes à qui je souhaite le succès dans sa vie.*

*A ma meilleure amie, Lydia qui était toujours là pour moi, tu es celle qui illumine mes jours avec ton amitié sincère et ton soutien indéfectible.*

*A ma meilleure cousine, sélia tu es à la fois ma partenaire de rire et mon pilier dans les épreuves ; je suis profondément reconnaissante de notre lien unique, une source constante de bonheur et de complicité.*

*A mon binôme Samy ainsi qu'à sa famille.*

*A mes chers amis, Célia, Melina, Maria, Dalia, Melissa, Nina, Thiziri, Asma, Siham, Liticia, Djida, Rania.*

*A toute la promotion RT 2023/2024.*

*Et à tous ceux qui m'aiment et qui me connaissent de proche ou de loin.*

***SOUHILA HAMANE***

# *Dédicaces*

*Avec l'expression de ma reconnaissance, je dédie ce modeste travail à ceux qui, quels que soient les termes embrassés, je n'arriverais jamais à leur exprimer mon amour sincère.*

***A ma très chère maman*** *Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit pour ton amour inconditionnel, ton soutien indéfectible et tes encouragements constants. Ta tendresse, ta patience et ta foi en moi m'ont donné la force de surmonter tous les obstacles. Ce mémoire est le reflet de tous les sacrifices que tu as faits pour moi et de ta confiance en mes capacités. Merci pour tout ce que tu as fait pour m'aider à réaliser mes rêves.*

***A mon père****, Pour ton amour inconditionnel, ton soutien sans faille et tes sages conseils. Ta force et ta détermination m'ont toujours inspiré à donner le meilleur de moi-même. Ce mémoire est le fruit de tes encouragements constants et de ta confiance en moi. Merci pour tout ce que tu as fait pour m'aider à réaliser mes rêves. Avec toute ma gratitude et mon affection.*

***A ma grande sœur****, Pour ta présence constante, ton soutien indéfectible et tes conseils avisés. Tu as toujours été là pour moi, me guidant avec amour et patience. Ta force et ta détermination m'ont inspiré à persévérer et à donner le meilleur de moi-même. Ce mémoire est le reflet de tous les encouragements et de l'affection que tu m'as offerts.*

***A mes chers cousins****, Massy, Zidane Pour votre soutien inconditionnel et les moments inoubliables partagés. Votre présence a rendu ce parcours encore plus significatif et enrichissant.*

***A mes amis*** *Ali, Hidou, Adel, Brahim, Mecipsa, Nadir, Yuba et Baderdine, vous êtes pour moi des frères et des amies sur qui je peux compter. En témoignage de l'amitié qui nous unit et des souvenirs de tous les moments que nous avons passés ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.*

***A mon binôme Souhila*** *pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.*

***A toute la promo RT 2023/2024****, pour votre soutien mutuel et votre camaraderie ont rendu cette expérience enrichissante et inoubliable.*

*Et à tous ceux qui m'aiment de proche ou de loin.*

***KASMI SAMY***

# *Sommaire*

# Table des matières

# Table des matières

## Chapitre II: La sécurité des réseaux informatiques

## Chapitre III : L'optimisation de la sécurité des réseaux informatiques

# Table des matières

# Table des matières

# Table des matières

# Liste de figures

## Liste des figures

# Liste de figures

# Liste de figures

# Liste de figures

## Liste des tableaux

# A

**ACL:** Access Control List.

**AH:** Authentication Header.

**ARP:** Address Resolution Protocol.

**AVF:** Active Virtual Forwarder.

**AVG:** Active Virtual Gateway.

# B

**BPDU:** Bridge Protocol Data Units.

# C

**CDN:** Content Delivery Network.

# D

**DHCP:** Dynamics Host Configuration Protocol.

**DMZ:** Demilitarized Zone.

**DNS:** Domaine Name System.

**DOS:** Denial Of Service.

# E

**EAP:** Extensible Authentication Protocol.

**EDR: Endpoint** Detection and Response.

**ESP: Encapsulating** Security Payload.

**ETF:** Exchange Traded Fund.

# F

**FAI :** Fournisseur d’accès à Internet.

**FTP:** File Transfer Protocol.

**FTPs:** File Transfer Protocol Secure.

# G

**Gns3:** Graphical Network Emulator.

# H

**HIDS:** Host Based Intrusion Detection System.

**HIPS:** Host based IPS.

**HTTP:** Hyper Text Transfer Protocol.

**HTTPS:** Hyper Text Transfer Protocol Secure.

**HSRP:** Host Standby Router Protocol.

# I

**IAM:** Identity and Access Management.

**ICMP:** Internet Control Message Protocol.

**IDS:** Intrusion Detection System.

**IETP: International** Test of English Proficiency

**IKE:** Internet Key Exchange.

**IOS:** International Organisation For Standardisation.

**ISO/IEC: International** Organisation For Standardisation/ International Electrotechnical Commission.

**ISP:** Internet Service Provider.

**IP:** Internet Protocol.

**IPS:** Intrusion Prévention System.

**IPSec:** Internet Protocol Security.

**IPv4:** Internet Protocol version 4.

**IPv6:** Internet Protocol version 6.

# L

**LAN:** Local Area Network.

**LDAP:** Lightweight Directory Access Protocol.

**LLC:** Logical Link Control.

**L2F:** Layer Two Forwarding.

**L2TP:** Layer Two Tunneling Protocol.

# M

**MAC: Media** Access Control.

**MAN:** Metropolitan Area Network.

**MAU:** Multistation Access Unit.

**MFA:** Multi-Factor Authentification.

## N

**NAC: Network** Access Control.

**NAT:** Network Adresse Translation.

**NBA:** Network behavior analysis.

**NBIDS:** Network-Based Intrusion Detection System.

**NIC:** Network Interface Card.

**NIPS:** Network based IPS.

**NTS:** New Technology & Solutions.

**NPS:** Network Policy Server.

## O

**OS:** Operating System.

**OSI:** Open Systems Interconnection.

## P

**PAgP :** Port Aggregation Protocol.

**PAN:** Personal Area Network.

**PoE:** Power over Ethernet.

**POP3 :** Post Office Protocol version 3.

**PPTP:** Point to Point Tunneling Protocol.

**PSSI :** Politique de sécurité du système d'information.

## R

**RARP:** Reverse Address Resolution Protocol.

**RDP:** Remote Desktop Protocol.

## S

**SA:** Security Assocation.

**SCTP:** Stream Control Transmission Protocol.

**SIEM :** Security Information and Event Management.

**SMTP:** Simple Mail Transfer Protocol.

**SOC:** Security Operations Center.

**SSH:** Secure Shell.

**SSL:** Secure Sockets Layer.

**SSO:** Single Sign-On.

**STA:** Spanning Tree Algorithm.

# T

**TCP:** Transmission Control Protocol.

**TCP/IP:** Transmission Control Protocol/Internet Protocol.

**TLS:** Transport Layer Security.

# U

**UDP:** User Datagram Protocol.

# V

**VNC:** Virtual Network Computing.

**VLAN:** Virtual Local Area Network.

**VPN:** Virtual Private Network.

**VRRP:** Virtual Router Rdundancy Protocol.

**VTP:** VLAN Trunking Protocol.

# W

**WAN:** Wide Area Network.

**WIPS:** Wireless based IPS.

# X

**XDR:** Extended Detection and Response.

# *Introduction Générale*

## Introduction Générale

L'informatique est devenue un outil essentiel pour la gestion, l'organisation, la production et la communication dans les entreprises. Le réseau informatique de l'entreprise gère, stocke et partage des données sensibles, parfois avec d'autres entreprises. Cette ouverture vers l'extérieur permet des gains de productivité et de compétitivité.

Cependant, il est impossible de renoncer complètement aux bénéfices de l'informatisation. Isoler le réseau de l'extérieur ou supprimer le caractère électronique et confidentiel des données n'est pas envisageable. Les données sensibles du système d'information sont donc exposées aux actes de malveillance comme l'augmentation du nombre de pirates informatiques et de cybercriminels.

Par conséquent, il est primordial de veiller à la sécurité de ces données, aussi bien à l'intérieur qu'à l'extérieur de l'entreprise. La protection des données sensibles est devenue un enjeu majeur.

La sécurité des réseaux informatiques est devenue une préoccupation majeure pour les organisations à l'ère numérique. Les réseaux à multicouche, par leur complexité et leur interconnectivité croissante, nécessitent une approche stratégique et intégrée pour garantir une protection efficace contre les menaces en constante évolution. Cette étude se concentre sur l'optimisation de la sécurité d'un tel réseau, structurée en quatre chapitres clés.

Notre projet de fin d'études se concentre sur la sécurisation des infrastructures réseau de l'entreprise N.T.S. Pour atteindre cet objectif, nous avons mis en place un ensemble de technologies telles que des pare-feux, des PVLAN (Réseaux Locaux Virtuels Privés) et des VPN (Réseaux Privés Virtuels).

Afin de présenter notre travail, nous avons structuré notre mémoire en quatre chapitres:

Dans le premier chapitre introductif, nous présenterons l'organisme d'accueil, son rôle dans l'écosystème numérique et les enjeux spécifiques de sécurité auxquels il est confronté. En identifiant les défis et les risques potentiels, nous explorerons également les solutions actuellement en place ou envisagées pour renforcer la sécurité du réseau multicouche.

Le deuxième chapitre examine les fondements de la sécurité des réseaux informatiques. Nous aborderons les principaux types de menaces et les vecteurs d'attaque courants auxquels les réseaux multicouches sont exposés. En comprenant les vulnérabilités potentielles, nous poserons les bases nécessaires à la conceptualisation d'une stratégie de sécurité efficace.

Le troisième chapitre se concentre sur les méthodologies et les pratiques visant à optimiser la sécurité des réseaux informatiques. Nous examinerons les techniques avancées telles que la segmentation de réseau, la surveillance proactive des menaces, et l'intégration de technologies de détection. L'objectif est de fournir des recommandations pratiques pour renforcer la résilience du réseau face aux cybermenaces.

Le dernier chapitre de notre mémoire est dédié à la conception d'une nouvelle architecture réseau sécurisée, réalisée sur le simulateur de réseau "GNS3". Ce chapitre détaille les tests effectués et les résultats obtenus pour les différentes configurations mises en place.

Enfin, nous concluons notre mémoire par une synthèse générale de notre projet et évoquons quelques perspectives d'amélioration ou d'évolution futures.

# *Chapitre I : Présentation de l'organisme d'accueil*

## I.1 Introduction

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

## I.2 Présentation de l'entreprise « Campus NTS »

### I.2.1 Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été créée en 2020à Bejaia par Yassine DJEBBARI, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- La technologie.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (targaouzamour, 17 octobre...etc.).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

### I.2.2 La localisation de l'entreprise

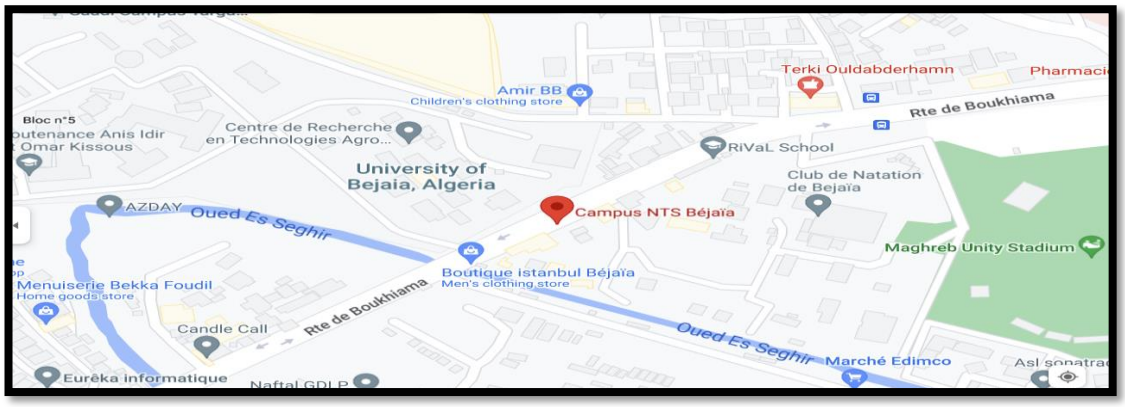



**Figure I.1 :** Localisation de l'entreprise NTS.

### I.2.3 Fiche technique

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

| **Dénomination** | **Campus NTS** |
|---|---|
| **Logo** | |
| **Siège** | Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000 |
| **Secteurs d'activités** | Informatique et télécommunication |
| **Numéros de FAX** | 044 204 400 |
| **Numéros de Téléphone** | 0770446101 |
| **Email** | contact@campus-nts.com |
| **Site Internet** | http://www.campus-nts.com/ |

**Tableau I.1** : Identification sur campus NTS.

### I.2.4 Objectifs, Missions et activités de l'Entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentées dans la figure 2 :

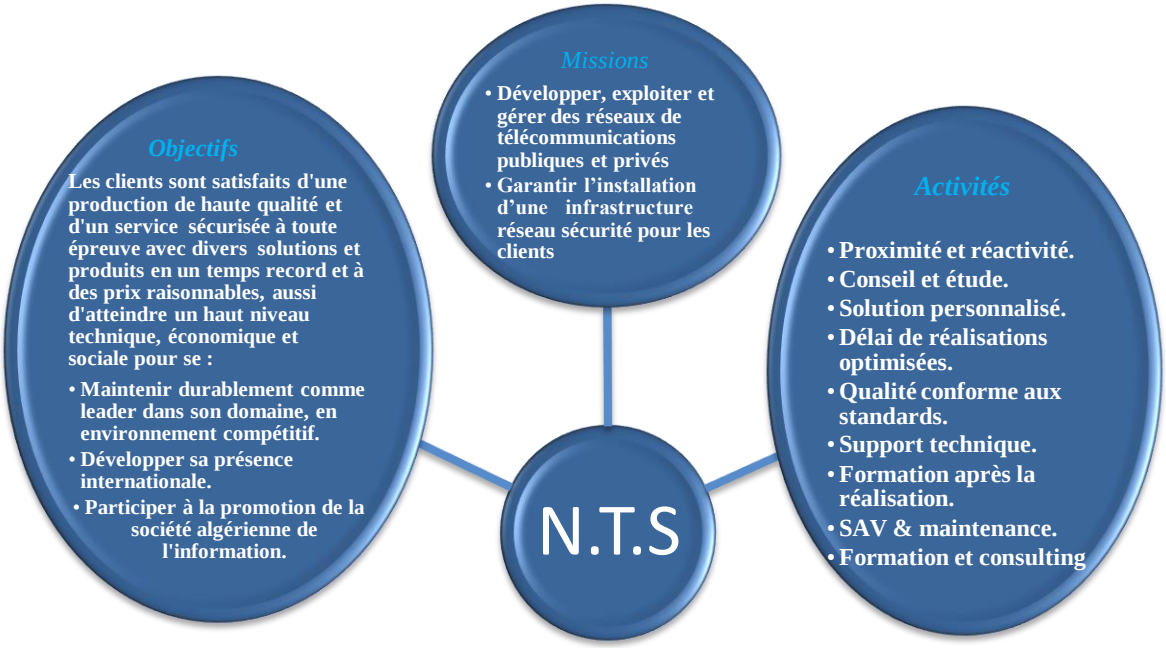



**Figure I.2 :** Objectifs, Missions et Activités de l'NTS.

### I.2.5 Organigramme général de l'organisme d'accueil

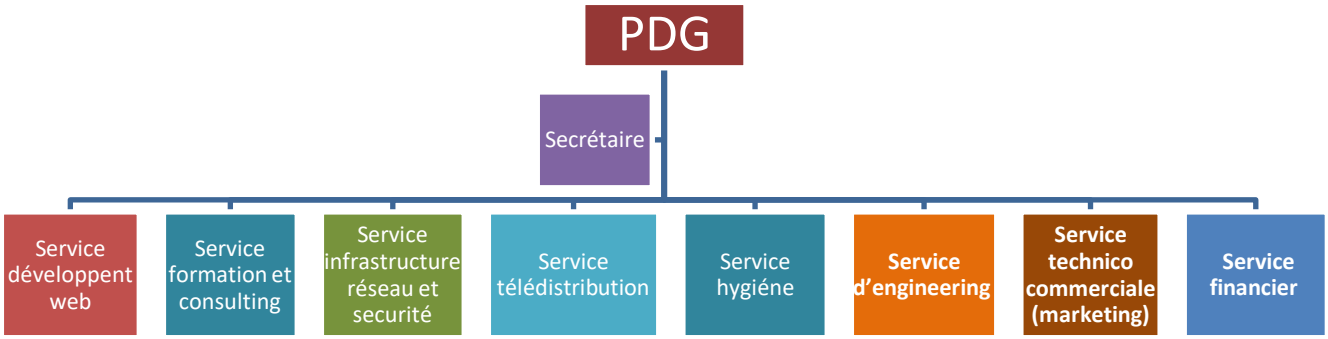



**Figure I.3** : L'organigramme de campus NTS.

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

### I.2.5.1 Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

### I.2.5.2 Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, C#, Java, Python…etc.).
- Électricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP S&R.
- Virtualisation.
- Microsoft server, SQL.
- Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

### I.2.5.3 Service d'accueil

- **Présentation de service infrastructure réseau et sécurité**

L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

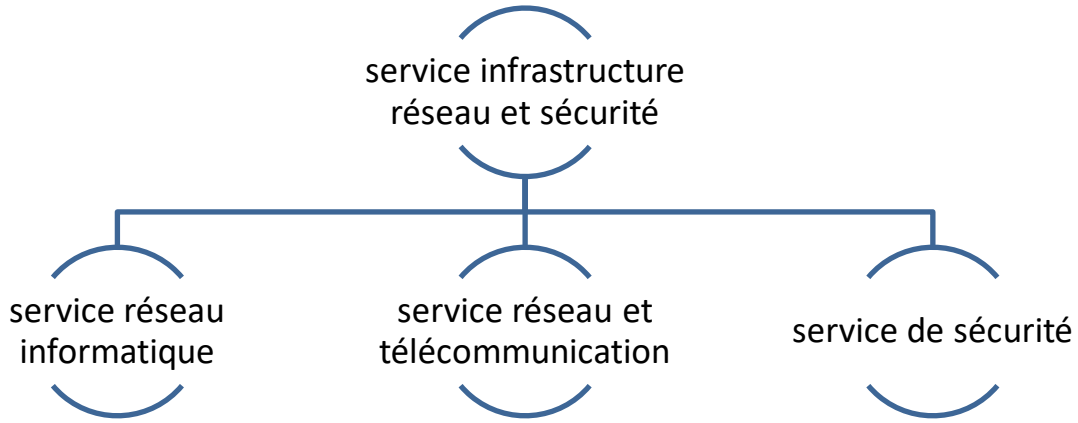



**Figure I.4 :** organigramme de service d'accueil.

- **Service réseau informatique**

Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :

Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

- **Service réseau et Télécommunication**

Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici des exemples de services d'infrastructure de télécommunications :

- Pose de fibre optique.
- Emplacement du site de la tour cellulaire.
- Test d'antenne radio.
- Installation d'équipements téléphoniques standards et réseau de données.
- Téléphonie standard

- **Service de sécurité**

Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources.

Les services qu'elle réalise sont les suivants :

- Caméras de surveillance
- Alarme anti- intrusion
- Détection incendie
- Pointeuse et Contrôles d'accès
- Vidéophonie

### I.2.5.4 Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de

télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.
- Services interactifs.
- Programmation locale.

### I.2.5.5 Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.

L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

### I.2.5.6 Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

### I.2.5.7 Service financier

Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

➢ Les tâches principales du Service des finances :

- Assurer une saine gestion des ressources financières de l'entreprise par la planification.
- La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
- La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

➢ Le rôle du service financier :

- La préparation et du suivi des budgets de fonctionnement et d'investissement.
- La préparation des états financiers.
- La gestion de la trésorerie et de des encaissements.
- La rémunération des employés, des comptes à payer.
- De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
- La réception des marchandises et du courrier.

### I.2.5.8 Service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :

- Des actions de prévention des risques professionnels et de la pénibilité au travail.
- La mise en place d'une organisation et de moyens adaptés.

## I.3 État des lieux (Client Collable)

### I.3.1 Présentation du réseau collable

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte ces vlans à une connexion L.S (Ligne Spécialisée publique symétrique) en fibre optique fournie par Algérie télécom, Le schéma ci-dessous nous montre l'infrastructure du réseau Collable :

### I.3.2 Présentation de l'architecture réseau existant dans l'entreprise

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

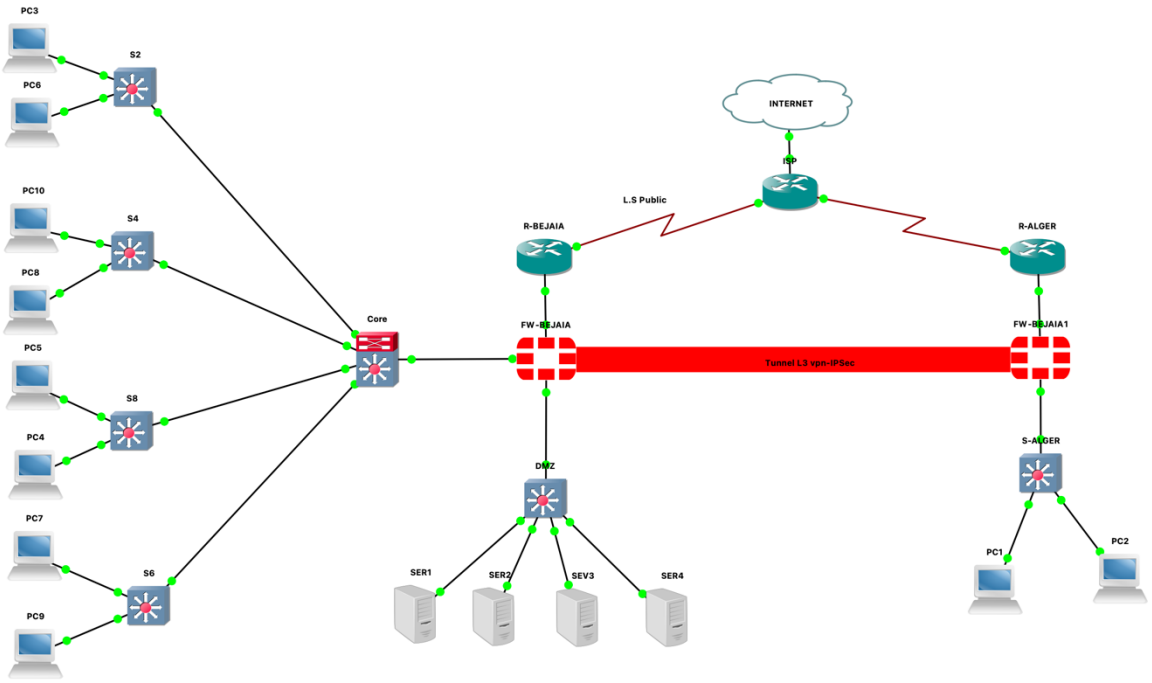



**Figure I.5 :** Architecture de réseau Collable.

### I.3.3 Analyse du parc informatique

#### I.3.3.1 Présentation d'environnement hard et soft

| Nom de l'équipement | Le hardware (hard) | Software (soft) |
|---|---|---|
| **Routeur** | ISR 4331 | IOS (International Organisation For Standardisation) |
| **Pare-feu** | PfSense | FREEBSD |
| **Switch** | • HPE 1820-24G Managed L2<br>• HPE 1920-24G Managed L3 | LINUX |
| **Server** | ESHP ProLiant DL380P génération 10 | • ESXI<br>• GOAUTODIAL<br>• SERVER WINDOWS 2022 |
| **PC portable** | Dell IAER 35 R | Windows 10 |

**Tableau I.2 :** L'environnement hardware et le software.

### I.3.3.2 Les caractéristiques des équipements par niveaux

| Nom de l'équipement | Modèle | Caractéristique |
|---|---|---|
| **Router**  | ISR 4331 | • **RAM :**4 G0 (installé) /16 GO (maximum)<br>• **Mémoire Flash :**4000 MO<br>• **Débit :**100 Mb/s<br>• **Protocole de liaison de données :** Ethernet, fast Ethernet et gigabit-ethernet |
| **Pare-feu**  | PFSENSE | • **Débit :** 4000 Mbit/s<br>• **Débit IPS :** 2700Mbit/s<br>• **Débit VPN IP sec :** 560 Mbit/s<br>• **@ IP/Numéro de port** |
| **Switch**  | **HPE 1920** | • **Ports :** 24 ports<br>• **Mémoire Flash :** 16MO<br>• **Mémoire RAM :**128MO<br>• **Capacité de commutation :** 32 Gbit/s |
| **Switch**  | **HPE 1820** | • **Ports :** 24 ports<br>• **Mémoire Flash :** 128MO<br>• **Mémoire RAM :**512MO<br>• **Capacité de commutation :** 56 Gbit/s |
| **Server**  | HP ProLiant DL380P génération 10 | • Processor Intel Xeon<br>• Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo)<br>• 16 G0 DDR4 RDIMM (1x 16 GO -12 slots) |
| **PC portable**  | Dell IAER 35 R | • **AMD core:** i5 8th génération<br>• **RAM :** 8GO<br>• **Disque :** 256GO<br>• **Écran :** UHD Graphies 620 ($1920 \times 1080 \times 32b$) |

**Tableau I.3 :** Détails des ressources disponibles de l'entreprise.

## I.4 Problématiques et Solutions proposées

### I.4.1 Problématiques

Au cours de notre stage chez l'entreprise NTS à Bejaia, nous avons observé que le réseau de leur client présentait des défaillances et un manque de sécurité, nous avons pu mettre en évidence les problèmes suivants :

- Le réseau n'est pas segmenté donc une attaque ou un malware peut se propager facilement à travers l'ensemble du réseau, compromettant tous les dispositifs connectés.
- Les données sensibles sont exposées vu que la DMZ a des attaques sur internet ainsi qu'un risque élevé de propagation des attaques au sein de la DMZ
- La complexité de la configuration, de la gestion et de la maintenance du réseau ce qui peut empenner a des pertes de données
- Le manque de stabilité du réseau en permettant la formation de boucles de commutation
- Le risque accru de formation de boucles de commutation dans un réseau, menant à des tempêtes de diffusion, à une congestion du réseau et à une vulnérabilité accrue face aux attaques réseau, compromettant ainsi la disponibilité et la sécurité des services.
- L'absence d'une redondance et de la répartition automatique de la charge entre plusieurs passerelles, augmentant ainsi le risque de pannes prolongées et de performances réseau réduites en cas de défaillance d'une passerelle principale.
- L'entreprise a des communications distantes mais sont moins sécuriser et facile à intercepter.
- Difficulté de Contrôler le Trafic entrant vers le réseau interne et d'appliquer des Politiques de Sécurité.

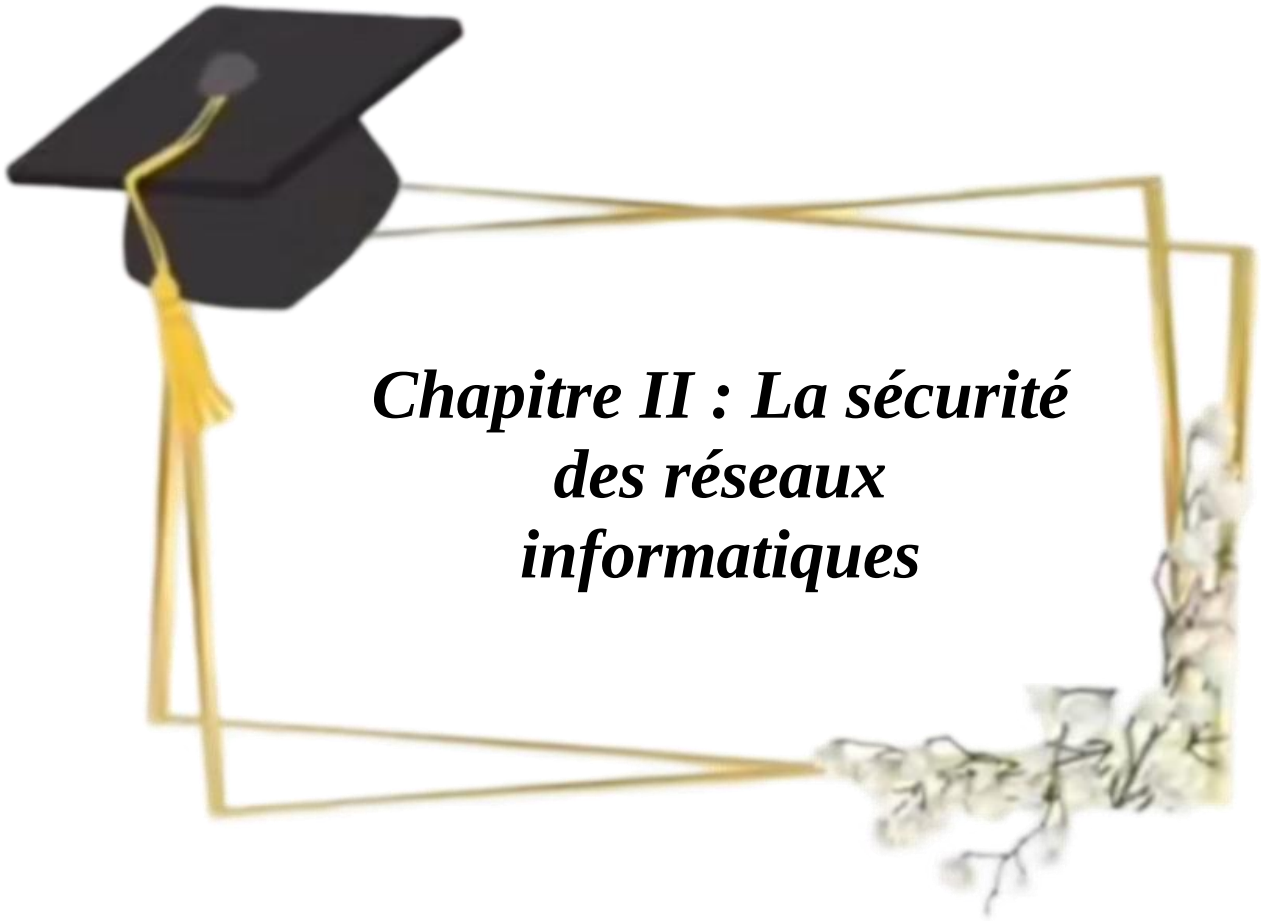
### I.4.2 Solutions proposées

On a relevé le défi d'optimiser la sécurité de cette infrastructure réseau a multicouches afin de faire face aux vulnérabilités et éventuelles attaques ou vol d'informations. Pour cela, nous avons proposé différentes solutions pour les problèmes que nous avons déjà mentionnés :

- Les VLANs offrent une solution efficace pour segmenter et isoler le trafic réseau, permettant ainsi de renforcer la sécurité en limitant l'accès aux ressources spécifiques aux utilisateurs autorisés et en réduisant la propagation des problèmes de sécurité à travers le réseau.
- Le VTP propose une solution de gestion et de distribution cohérente des configurations de VLAN à travers les switches réseau, simplifiant ainsi l'administration et assurant la cohérence des VLANs à travers l'infrastructure.
- Les PVLANs au sein d'une DMZ renforcent la sécurité en segmentant les serveurs et périphériques sensibles, limitant ainsi la communication directe entre eux et réduisant la surface d'attaque.
- Implémentation du protocol PAGP qui permet d'agréger plusieurs liens physiques en un seul lien logique, améliorant ainsi la redondance et la bande passante disponibles. Cette configuration réduit également la complexité de gestion tout en renforçant la fiabilité du réseau
- Implémentation du Protocol STP pour éviter les boucles de commutation dans l'architecture en désactivant sélectivement les chemins redondants, assurant ainsi la stabilité et la fiabilité du réseau
- Implémentation du Protocol (GLBP) pour avoir une redondance active-active des passerelles, permettant à plusieurs routeurs de fonctionner simultanément pour distribuer la charge de trafic entrant. Cette approche augmente la disponibilité des services tout en optimisant l'utilisation des ressources réseau.
- Configuration d'un tunnel VPN site-to-site pour chiffrer le trafic entre le site de BEJAIA et le site d'ALGER, assurant ainsi la confidentialité et l'intégrité des données transitant sur des réseaux publics comme Internet.
- Mettre le pare-feu comme première ligne de défense du réseau pour contrôler le trafic entrant et sortant des réseaux d'entreprise grâce à un ensemble de règles de sécurité

## I.5 Conclusion

Dans ce chapitre, nous avons donné un aperçu de l'infrastructure de client collable du fournisseur de solution IT campus NTS, puis nous avons découvert les problèmes qui nous ont amenés à rechercher et à mettre en œuvre une nouvelle architecture de réseau sécurisée en employant des technologies et des outils de sécurité. Enfin, l'application de la solution proposée fera l'objet de notre 4 ème chapitre.



# *Chapitre II : La sécurité des réseaux informatiques*

## II.1 Introduction

Un réseau informatique est constitué d'un ensemble de systèmes informatiques interconnectés les uns avec les autres grâce à des équipements et supports de communications.

Les entreprises, qu'elles soient petites ou grandes, font face à une menace constante d'attaquesinformatiques. Plus elles détiennent des informations sensibles, plus elles sont susceptiblesd'êtreciblées. Cependant, il est possible de renforcer la sécurité des systèmes en mettant en œuvre descontre-mesures pour réduire les risques d'attaques et de compromission des données.

La sécurité des systèmes d'information représente aujourd'hui une tâche de fond à prendre en comptepar toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent etassurent la gouvernance de son système d'information. Ainsi plusieurs méthodes d'analyse dessystèmes informatiques proposent des démarches de certification afin de garantir une image pérenneaux entreprises intégrant les processus de sécurité dans la liste de leur préoccupation managériale.

Ce chapitre présente dans sa globalité des généralités sur les réseaux informatique et la sécurité informatique.

## Section 1 : Généralités sur les réseaux informatiques

Dans un monde interconnecté, les réseaux informatiques constituent l'épine dorsale de la société numérique. Leur omniprésence transcende les frontières physiques, reliant les individus, les entreprises et les institutions à travers le globe. Ce tissu complexe de données et de communications façonne notre quotidien, facilitant l'échange d'informations et propulsant l'innovation à une vitesse vertigineuse.

### II.2 Définition d'un réseau informatique

C'est un ensemble d'équipement reliés entre eux pour échanger des données et des ressources permettant la communication et le partage d'informations entre différents utilisateurs.

#### II.2.1 Objectifs des réseaux informatiques

L'objectif principal d'un réseau informatique est de faciliter la communication et l'échange dedonnées entre les différents dispositifs connectés.

### II.2.2 Types de réseaux informatiques

Les réseaux sont classifiés selon leur taille, topologie et mode de commutation

#### II.2.2.1 Classifications selon leur taille

- **PAN (Personal Area Network) :** Réseau pour une seule personne.
- **LAN (Local Area Network) :** Réseau d'entreprise dans un bâtiment ou un campus.
- **MAN (Metropolitan Area Network) :** Couvre une ville.
- **WAN (Wide Area Network) :** Couvre un pays, un continent.

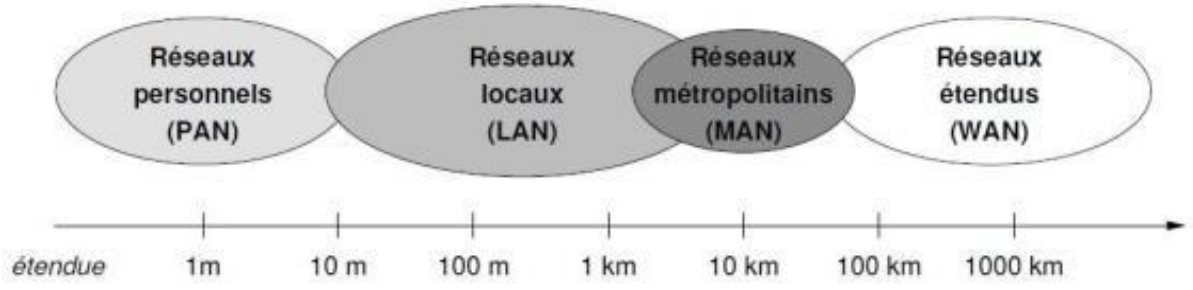



**Figure II.1 :**type des réseaux informatique.

### II.2.3 Modèle hiérarchique

Cisco a défini un modèle hiérarchique de réseaux. Ce modèle qui simplifie la tâche de construire un réseau d'interconnexion fiable, évolutif et moins coûteux. Comme le montre la figure ci-dessous, ce modèle est décomposé en trois couches distinctes qui sont en grande partie basées sur la répartition des rôles entre routage et commutation [1]. (Voir annexe A)

### II.2.4 Modèles de référence pour les réseaux informatiques

On retrouve deux modèles :

#### II.2.4.1 Modèle OSI (Open Systems Interconnection)

Le modèle de référence OSI (Open System Interconnexion) définit une sorte de langage commun. Ce modèle a été mis au point par l'ISO (Organisation Internationale des Standards) et il est devenu le socle de référence pour tout système de traitement de communications. Il

repartit les questions relatives au domaine des communications informatiques selon sept couches classées par ordre d'abstraction croissant. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace. [2] (Voir annexe A)

### II.2.4.2 Modèle TCP/IP (Transmission Control Protocol/ Internet Protocol)

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais il contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application [2][3]. (Voir annexe A)

Les principaux protocoles et applications de l'environnement TCP/IP sont :

- **Http** : *HyperText Transport Protocol*, assure le transfert de fichiers hypertextes entre un serveur Web et un client Web ;
- **FTP** : *File Transfer Protocol*, est un système de manipulation de fichiers à distance (transfert, suppression, création...) ;
- **TELNET** : *TELety pewriter NETwork protocol* (ARPA) ou *TERminaL NETwork protocol*, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes.
- **SMTP** : *Simple Mail Transfer Protocol*, offre un service de courrier électronique.
- **TFTP** : *Trivial FTP*, est une version allégée du protocole FTP.
- **DNS** : *Domain Name System*, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse Internet (adresse IP).
- **SNMP :** *Simple Network Management Protocol*, est devenu le standard des protocoles d'administration de réseau.
- **ICMP :** *Internet Control and error Message Protocol*, permet la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit... Il est utilisé par l'utilitaire Ping qui permet de tester la présence d'une station sur le réseau.

## Section 2 : Sécurité des réseaux informatiques

# II.3 Les principes de la sécurité informatique

### II.3.1 Objectifs de la sécurité informatique

La sécurité informatique, d'une vue générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.
La sécurité vise généralement ses objectifs :

- **La confidentialité :** Protection de données émises sur le réseau compréhensibles seulement par des entités autorisées.
- **Disponibilité :** Garantir qu'un système reste en permanence utilisable par les personnes autorisées.
- **Intégrité :** Garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau.
- **Authentification :** Garantie que les données reçues proviennent bien de l'entité émettrice.
- **Non répudiation** : C'est la propriété qui assure la preuve de l'authenticité d'un acte.

### II.3.2 Politique de sécurité

#### II.3.2.1 Définition

Une politique de sécurité est constituée par l'ensemble des lois, règles, et pratiques qui régissent le traitement des informations sensibles et l'utilisation des ressources par le matériel et le logiciel d'un système.

#### II.3.2.2 Les types de politique de sécurité

- **La politique qui interdit tout par défaut :** dans cette approche, tout ce qui n'est pas explicitement permis est interdit. Elle consiste à définir les services à autoriser (SMTP pour l'hôte serveur de courrier, http pour l'hôte devant accéder au web) et définir les droits de chaque utilisateur.

- **La politique qui autorise tout par défaut :** dans cette approche, tout est permis sauf ce qui est considéré comme dangereux donc tout ce qui n'est pas explicitement interdit est autorisé. Elle consiste à analyser les différents risques d'application qui doivent

s'exécuter, en déduire les interdictions à appliquer et autoriser tous les restes [4].

### II.3.3 Les attaques informatiques [5]

#### II.3.3.1 Définition

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une attaque est l'exploitation d'une faille (vulnérabilité ou brèche) d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

#### II.3.3.2 Types d'attaques

Il est ainsi possible de catégoriser les risques de la manière suivante :

- **Accès physique :** il s'agit d'un cas où l'attaquant a accès aux locaux, éventuellementmême aux machines :
    - Coupure de l'électricité, Extinction manuelle de l'ordinateur, Vandalisme, Ouverture du boitier de l'ordinateur et vol de disque dur, Écoute du trafic sur le réseau et ajout d'éléments (clé USB, point d'accès Wifi.....).
- **Interception de communications :** Vol de session, Usurpationd'identité etdétournement ou altération de messages.
- **Deni de service :** il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
    - Exploitation de faiblesses des protocoles TCP/IP,
    - Exploitation de vulnérabilité des logiciels serveurs.
- **Intrusions :**
    - Balayage de ports, Élévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application et maliciels : (virus, vers, et chevaux de Troie).

- **Ingénierie sociale :** dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! en effet, c'est souvent lui qui, par méconnaissance ou par duperie, va ouvrir une brèche dans le système, en donnant des informations (mot de passe par exemple) au pirate informatique.
- **Trappes :** il s'agit d'une porte dérobéedissimulée dans un logiciel, permettant un accèsultérieur à son concepteur.

### II.3.4 Les malwares

Un malware est un logiciel développé dans le but de nuire à un système informatique. Il existe plusieurs familles de malwares. On va définir les plus intéressants [6] :

#### II.3.4.1 Virus

C'est un programme malveillant introduit à l'insu des utilisateurs dans un système, il possède la capacité de se dupliquer (s'auto reproduire).

#### II.3.4.2 Cheval de Troie

Un cheval de Troie (*Trojan horse*) est un programme qui exécute des instructions sans l'autorisation de l'utilisateur. Ces instructions sont généralement nuisibles à l'utilisateur, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses.

#### II.3.4.3 Ver

Un ver informatique est un programme qui peut s'auto reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.) pour se propager.

### II.3.5 les outils de la sécurité

#### II.3.5.1 Antivirus

Un antivirus est un logiciel permettant de protéger une machine contre les programmes/logiciels néfastes ou les fichiers potentiellement exécutables. De nos jours, les antivirus sont aussi des anti- malwares c'est-à-dire ils protègent aussi les machines contre tous les autres types de malwares à savoir les vers et les chevaux de Troie. Il consiste à chercher les codes malveillants dans les logiciels infectes. Cependant, un antivirus ne protège pas le réseau

contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitimeaccédantà une ressource alors qu'il n'est pas autorisé à le faire. [7]

### II.3.5.2 IDS/IPS (Intrusion Detection System/ Intrusion Prevention System)

#### II.3.5.2.1 Les systèmes de détection d'intrusions (IDS)

Un système peut subir plusieurs attaques, il est donc nécessaire d'avoir un logiciel spécialisé capable de surveiller les données qui transitent sur ce système, et qui peut réagir si des données semblent suspectes. Les systèmes de détection d'intrusions (IDS) conviennent parfaitement pour réaliser cette tâche. [8]

- **Les différentes sortes d'IDS**

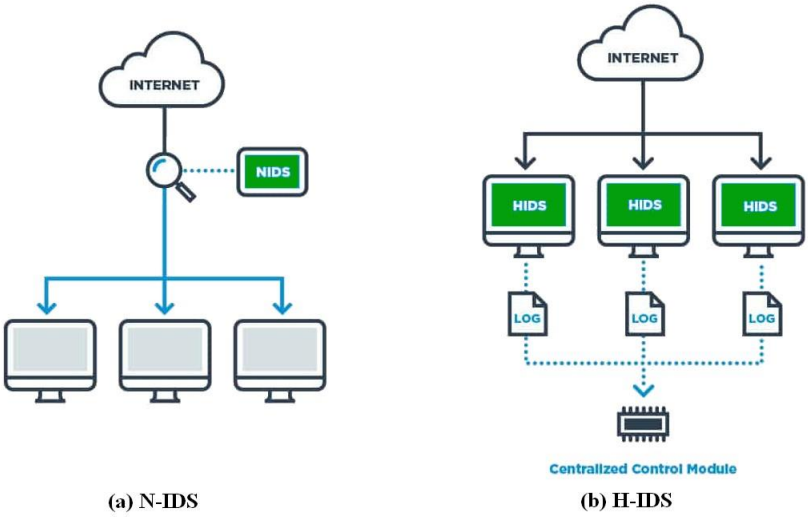
Les IDS se caractérisent par leur domaine de surveillance. Celui-ci peut se situer au niveau d'un réseau d'entreprise, d'une machine hôte, d'une application…, il existe trois sortes distinctes d'IDS :

**a. La Détection d'Intrusion Réseau (N-IDS)** *(Network Based Intrusion Detection System)*

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau. Les N-IDS assurent la sécurité au niveau du réseau en utilisant principalement des capteurs qui sont souvent des hôtes dont leur seule tâche est l'analyse du trafic réseau et d'envoyer une alerte à une console sécurisée. Ils agissent de manière invisible ce qui les rend difficile à localiser et à atteindre par un attaquant. Les capteurs peuvent être placés avant ou après le pare-feu, ou encore dans une zone sensible que l'on veut protéger spécialement.

**b. La détection d'Intrusion basée sur l'hôte H-IDS** (*Host Based Intrusion Detection System)*

Ils analysent seulement l'information concernant cet hôte. Ces systèmes n'ont pas à contrôler le trafic du réseau mais uniquement les activités d'un hôte donné, ce qui leur donne une grande précision sur les types d'attaques subies. [9]




**FigureII.2 :** Architectures des N-IDS et H-IDS

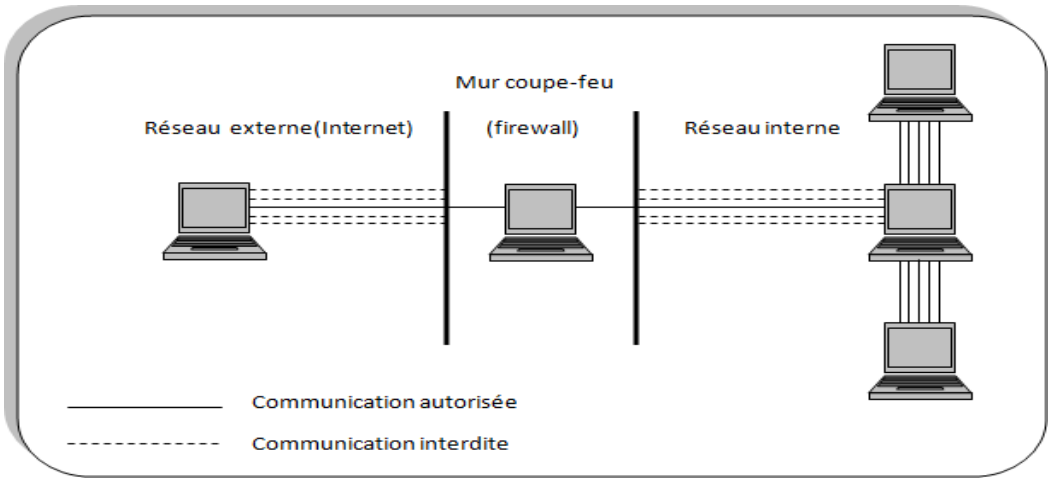
#### II.3.5.2.2 Système de prévention d'intrusion (IPS)

Un système de prévention d'intrusion est un dispositif capable de détecter des attaques, connues et inconnues, et de les empêcher d'êtreréussies. L'IPS n'est pas un observateur : il fait partie intégrante du réseau. Il est placé en ligne et examine tous les paquets entrants ou sortants. [6]

### II.3.5.3 Les pare-feu (firewall)

Un pare-feu (appelé aussi *coupe-feu* ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs, des intrusions provenant d'un réseau tiers (notamment Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivantes :

- Une interface pour le réseau a protégé (réseau interne).
- Une interface pour le réseau externe.[5]




**FigureII.3 :** Pare-feu.

Le système pare-feu est un système logiciel, reposant parfois sur un matériel réseau dédie, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu n'importe quel système pourvu que :

-Lamachine soit suffisamment puissante pour traiter le trafic,
-Lesystèmesoitsécurisé,
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Dans le cas où le système Pare-feu est fourni dans une boite noire <<clé en main>>, on utilise le terme d'Appliance. [8]

- **Principe de fonctionnement**

  Un système pare-feu contient un ensemble de règlesprédéfinies permettant :

  - D'autoriser la connexion (allow) ;
  - De bloquer la connexion (deny) ;
  - De rejeter la demande de connexion sans avertir l'émetteur (drop). [5]

- **Classifications de pare-feu**

Plusieurs classifications existent pour catégoriser les types de pare-feu. En effet, en termes de filtrage, on distingue principalement deux types de pare-feu : [7]

**_ Pare-feu « réseau » (ou filtrage de paquets) :** fonctionnant au niveau des couches Internet et Transport du modèle TCP/IP, en se basant sur le filtrage de paquets, c'est-à-dire autoriser un

paquet ou le refuser en fonction de son entête IP (Adresses IP source et destination, numéro de port et protocole TCP/UDP), sans accéder à son contenu ce qui ne permet pas de reconnaître l'identité de l'émetteur du paquet. Dans ce type de pare-feu, on distingue deux types de filtrage :

**Filtrage simple de paquet (Stateless) :** La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. C'est la méthode de filtrage la plus simple, car elle consiste à autoriser ou à refuser le passage de paquets d'un réseau à un autre en se basant sur l'entête IP du paquet (Adresses IP source et destination, numéro de port et protocole TCP/UDP). Cela nécessite de configurer le pare-feu par des règles de filtrages, généralement appelées des ACL (Access Control Lists).
Parmi les limites du filtrage simple, ce dernier requiert une configuration poussée pour être efficace, en plus de ralentir le débit de la bande passante qui le traverse. Par ailleurs, il ne résiste pas à certaines attaques de type IP Spoofing/IP Flooding, la déformation de paquet, ou encore certaines attaques de type DoS.

**Filtrage de paquet avec état (Stateful) :** La différence de ce filtrage par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au pare-feu. Ce dernier prend ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. En outre, ce filtrage permet aussi de se protéger face à certaines attaques de type DoS. En effet, les connexions Internet sont contrôlées en n'autorisant que celles qui sont à la demande, et dans le cas des protocoles UDP et ICMP, un certain délai est défini pour autoriser les réponses légitimes aux paquets envoyés. Cependant, dès lors que l'accès à un service est autorisé par ce type de pare-feu, il n'y aurait aucun contrôle effectué sur le flux qui concerne ce service.

**_Pare-feu applicatif (ou filtre d'application) :** permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modelé OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des applications présente sur le réseau, et notamment de la manière dont les données sont échangées (port,etc..). Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. [5]

Le principe de ce pare-feu est identique à celui d'un proxy, c'est-à-dire, quand un utilisateur veut se connecter à un serveur externe, il se connecte d'abord au programme mandataire, qui lui va relayer le flux vers le serveur demandé. Par exemple, la connexion à

internet à travers certains réseaux Wi-Fi d'entreprises exige une authentification au préalable sur un pare-feu mandataire permettant à l'utilisateur de surfer mais passant toujours à travers le proxy. Avec ce genre de filtre, une seule machine (le serveur mandataire) envoie des requêtes vers l'extérieur en gardant trace du trafic. Ce type de pare-feu est plus efficace car le contenu des paquets est analysé, ce qui permet au filtre de laisser passer ou non suivant des règles applicables au contenu. [7]

- **Types de pare-feu**

On distingue :

**-Les firewalls bridge**

Ces derniers sont relativement répandus. Ils agissent comme de vrais câblesréseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règlesprédéfinies. En effet, quand une requête ARP est émise sur le câbleréseau, le firewall ne répond jamais et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles. Toute attaque devra donc faire avec ses règles, et essayer de les contourner. [10]

**-Le firewall logiciel**

Il est mis en œuvre sur un simple PC avec plusieurs interfaces réseau, embarquant un OS généraliste (Linux, ou un autre UNIX). Les fonctions du pare-feu sont implémentées à l'aide d'un logiciel adapté (Ipchains ou Netfilter sous Linux ; PacketFilter sous OpenBSD).

**-Le firewall matériel**

Il se présente sous la forme d'un boîtier spécialisé embarquant un OS souvent minimaliste (routeurs ou équipements dédiés).

- **Zone démilitarisée (DMZ)**

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes.

C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feu permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de cloisonnement des réseaux (le terme isolation est parfois également utilisé).

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, serveur de messagerie,serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.

On parle ainsi de zone démilitarisée (notée DMZ, DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

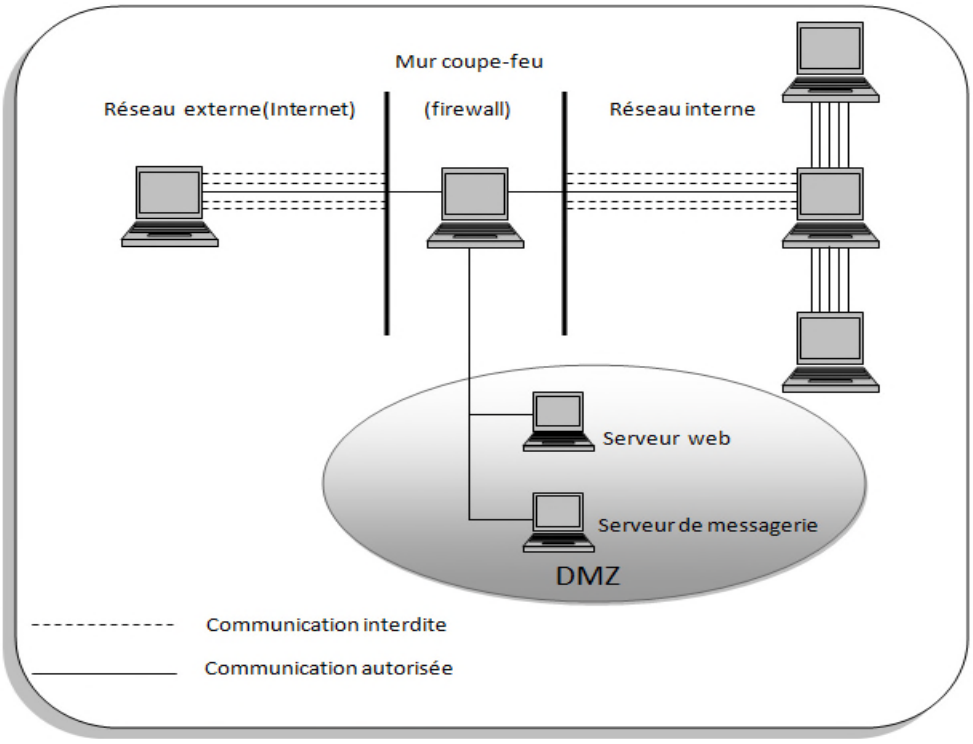



**Figure II.4 :** Exemple d'une zone démilitarisée (DMZ).

Les serveurs situés dans la DMZ sont appelés bastions en raison de leur position d'avant-poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- trafic du réseau externe vers la DMZ autorisé,
- trafic du réseau externe vers le réseau interne interdit,
- trafic du réseau interne vers la DMZ autorisé,
- trafic du réseau interne vers le réseau externe autorisé,
- trafic de la DMZ vers le réseau interne interdit,
- trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise. [5]

### II.3.5.4 Serveurs mandataires (Proxy)

Un serveur Proxy, appelé aussi serveur mandataire est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local, utilisant parfois des protocoles autre que le protocole TCP/IP et Internet.

La plupart du temps le serveur Proxy est utilisé pour le web, il s'agit alors d'un Proxy HTTP. Toutefois il peut exister des serveurs Proxy pour chaque protocole applicatif (FTP, etc.) [5].

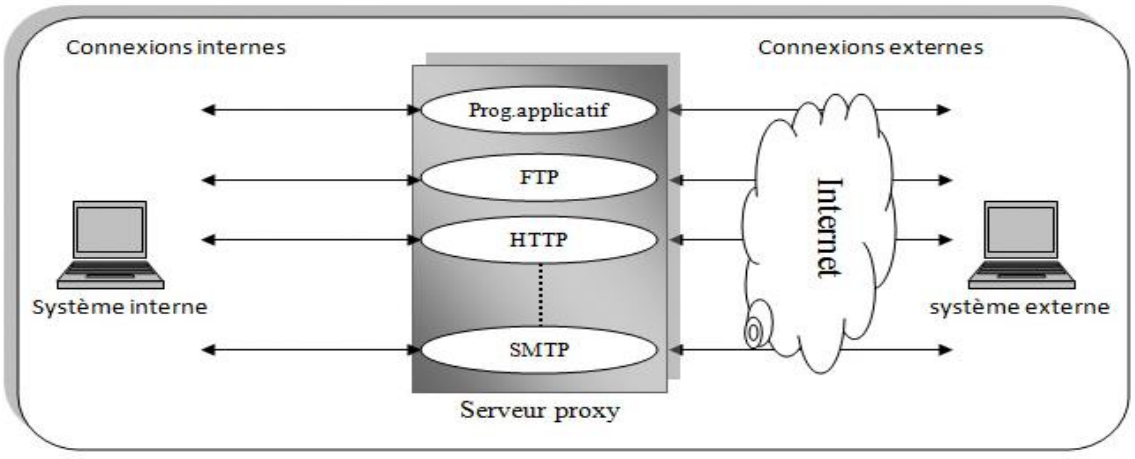



**Figure II.5 :** Architecture d'un Proxy.

- **Principe de fonctionnement**

Le principe de fonctionnement d'un serveur Proxy est assez simple : il établit en lieu et place de l'utilisateur le service invoqué par celui-ci (FTP, etc.). Ainsi lorsqu'un utilisateur se connecte à l'aide d'une application cliente configurée pour utiliser un serveur Proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur Proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête (le serveur Proxy contacte le serveur externe sollicité sur internet avec sa propre adresse ou une adresse issue d'un pool d'adresses IP libres). Le serveur va ensuite donner sa réponse au Proxy, qui va à son tour la transmettre à l'application cliente [5]. Le Proxy cache de la sorte toute l'infrastructure du réseau local et ne dévoile en aucun cas les adresses des machines internes (masquage d'adresse).

- **La NAT (network Address Translation)**

Son principe consiste à modifier l'adresse IP source ou destination, dans l'en-tête d'un datagramme IP lorsque le paquet transite dans le Pare-feu (Proxy) en fonction de l'adresse source ou destination et du port source ou destination.

Lors de cette opération, le Pare-feu garde en mémoire l'information lui permettant d'appliquer la transformation inverse sur le paquet de retour. La traduction d'adresse permet de masquer le plan d'adressage interne (non routable) à l'entreprise par une ou plusieurs adresses routables sur le réseau externe ou sur Internet. Cette technologie permet donc de cacher le schéma d'adressage réseauprésent dans une entreprise derrière un environnement protègé. [11]

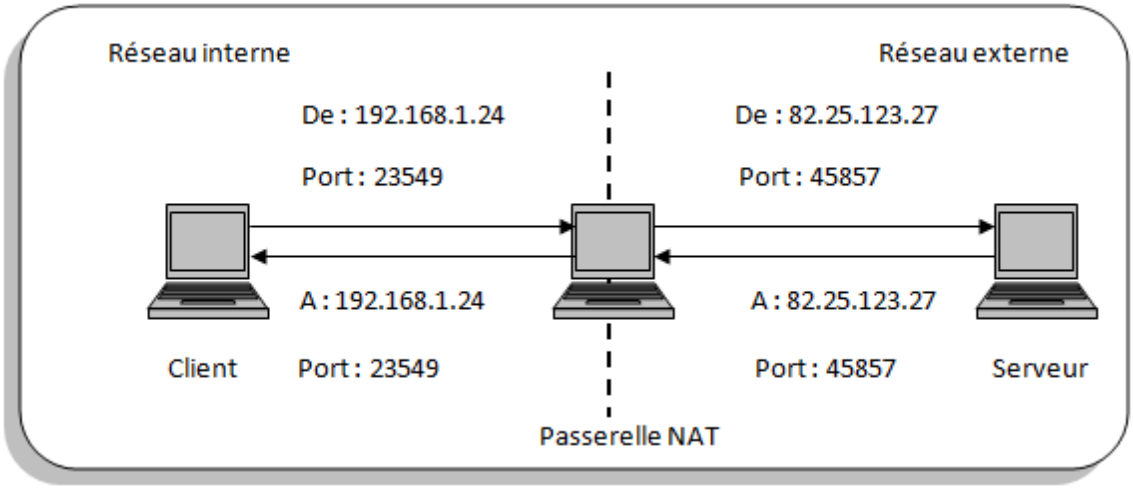



**Figure II.6 :** Translation d'adresses (NAT).

### II.3.5.5 Réseau virtuel privé (VPN)

Un Réseau virtuel privé « VPN » (pour Virtuel Private Network), fait référence à l'usage du protocole IPSec afin de créer un canal de communication sécurisé à usage privé, dans un réseau public non sécurisé. Souvent mis en œuvre par une organisation, pour connecter ses différents sites via Internet afin d'assurer la confidentialité des données échangées [12].

- **Fonctionnement d'un VPN**

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling, c'est- à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'êtresécurisées par des algorithmes de cryptographie.

L'expression tunnel chiffré est utilisée pour symboliser le fait qu'entre l'entrée et la sortie du VPN, les données sont chiffrées (cryptées) et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du coté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du coté de l'organisation.

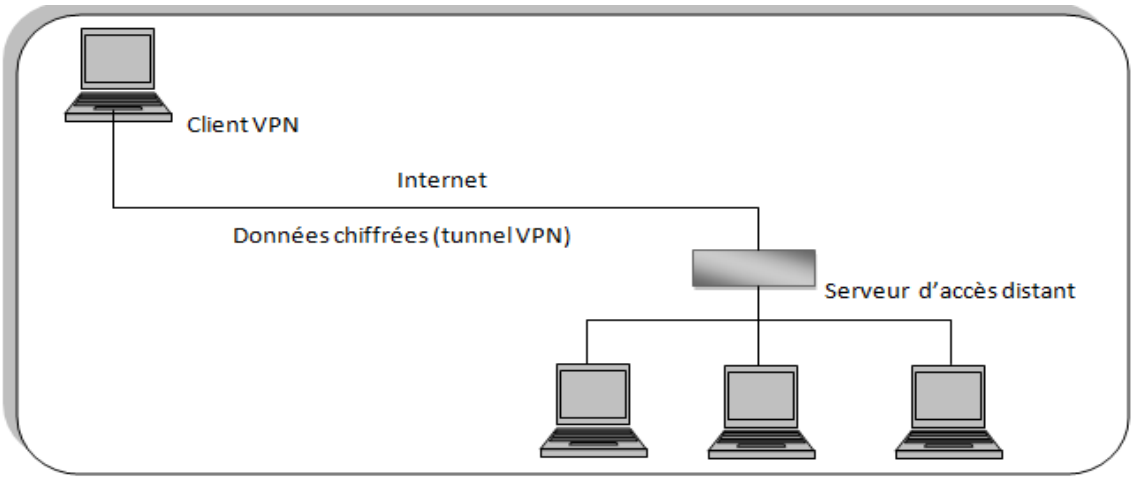



**Figure II.7 :** Réseau privé virtuel (VPN).

De cette façon, lorsqu'un utilisateur a besoin d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façonchiffrée.

L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façonchiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur [5].

## ➢ Protocoles de tunneling

Les principaux protocoles de tunneling sont les suivants :

- **PPTP** (point-to-point tunneling Protocol) est un protocole de niveau 2 développé parMicrosoft, 3 Com, Ascend, US Robotics et ECI Telematics,
- **L2F** (Layer TwoForwarding) est un protocole de niveau 2 développé par Cisco, NorthernTelecom et Shiva. Il est désormais quasi obsolète,
- **L2TP** (Layer Two Tunneling Protocole) est l'aboutissement des travaux de l'IETF (RFC2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2,
- **IPsec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporterdes données chiffrées pour les réseaux IP [5].

- **Modes d'utilisation d'un VPN**

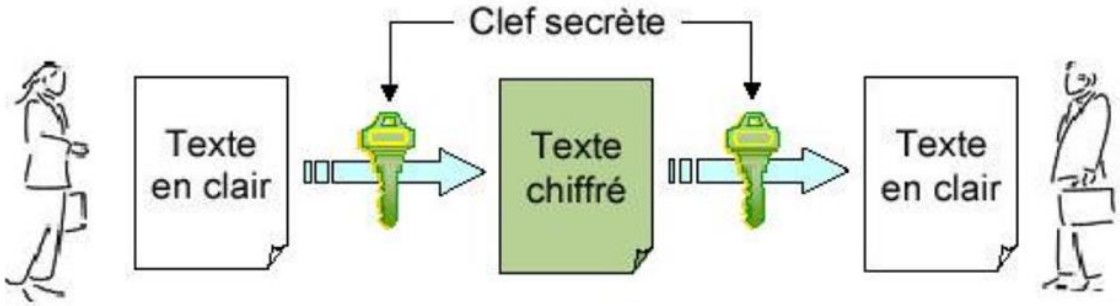
Un réseau privé virtuel peut être utilisé de deux façons : [13]

- **L'intranet ou l'extranet VPN (LAN-to-LAN) :** permet de relier deux réseaux LAN. L'extranet permet, par exemple, de relier une entreprise avec ses collaborateurs ou clients. Quant à l'intranet VPN, il permet, par exemple, de relier deux serveurs distants d'une même entreprise de façon sécurisée.
- **Le VPN d'accès (Host-to-LAN) :** permet par exemple à un télétravailleur de se connecter au réseau local de son entreprise à distance pour travailler, pour accéder à des données privées, ou pour communiquer avec ses collègues de travail qui à leur tour peuvent être connectés en VPN.
  Nécessite un code d'accès pour chaque connexion au VPN.

### II.3.5.6 Cryptographie

La cryptographie est l'étude des méthodes de chiffrement et de déchiffrement, elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des données.

- **Cryptographie symétrique :** Elle est basée sur une clé prive unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypté les messages.




**FigureII.8 :** Cryptographie symétrique.

- **Cryptographie Asymétrique :** Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : une est privée et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde.

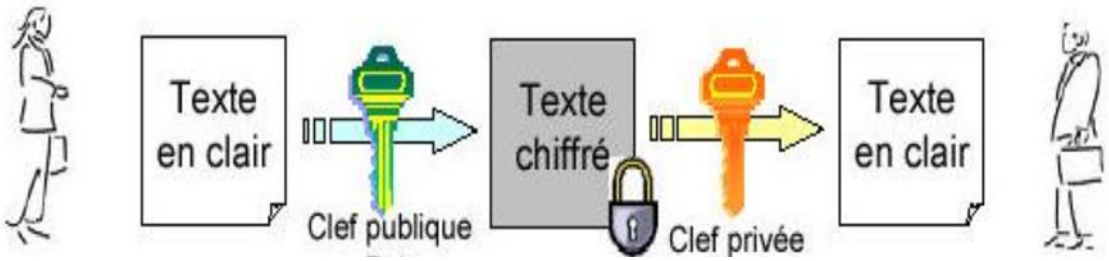



**Figure II.9:** Cryptographie asymétrique.

### II.3.5.7 La haute disponibilité

La haute disponibilité est un terme souvent utilisé en informatique, à propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable, cette dernière concerne de plus en plus d'entreprises comme de particuliers. En Anglais, la « haute disponibilité » est appelée « High availability » (HA) toutes les dispositions visant à garantir la disponibilité d'un service, c'est-à-dire assurer le bon fonctionnement de ce dernier.

## II.3.6 Implémentation des règles de sécurité dans les dispositifs à filtrage

### II.3.6.1 Les ACL

Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole). Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny). Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output). Une ACL est analysée par l'IOS de manière séquentielle. Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé. Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.

- **Rôles des listes d'accès**

Les listes d'accès sont utilisées à des fins multiples, et voici les principales raisons pour lesquelles il est nécessaire de les créer : [11]

- Limiter le trafic réseau pour augmenter les performances,
- Déterminer quel type de trafic sera acheminé ou bloqué au niveau des interfaces du routeur,

- Capacité à contrôler les zones d'un accès client.

➢ **Les types d'ACL [14]**

Il existe plusieurs types d'ACL. Les listes d'accès Cisco sont soit standards, soit étendues :

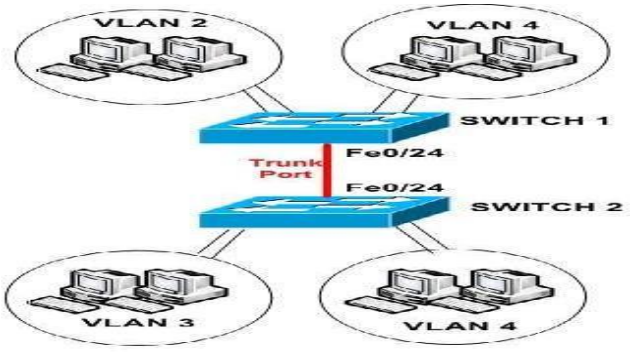
♠**ACL standards (IP standard accesslist) :** permettent d'autoriser ou de refuser le trafic selon les adresses IP source (le seul critère de filtrage est l'adresse IP source). ♠**ACL étendues (IP extendedaccesslist) :** permettent de filtrer les paquets IP enfonction de plusieurs attributs, le type de protocole, l'adresse IP source, l'adresse IP destination, les ports TCP/UDP source et destination.

**Remarque :** Chaque ACL est identifiée avec un numéro unique d'une plage précise valable pour le protocole. Tel que :

- ACLs standards : les plages de numéros assignes sont <**1-99**>, et <**1300-1999**>
- ACLsétendues : les plages de numéros sont <**100-199**>, et <**2000-2699**>

### II.3.6.2 Les VLAN (réseaux locaux virtuels)

Un VLAN est un réseau regroupant les machines de manière logique et non plus physique. Sur un Switch, un VLAN est un groupe de ports, les machines connectées É ces ports (même identifiant VLAN) peuvent communiquer entre elles librement. En revanche, toute communication est impossible avec un port étranger au VLAN, ces communications inter-VLAN doivent transiter par un routeur. En fait, les VLAN introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques selon des critèresprédéfinis (ports, adresses MAC, adresses réseau...). [15]




**FigureII.10 :** Exemple de VLAN.

Les VLANs optimisent l'utilisation de la bande passante car ils limitent les domaines de diffusion, et autorisent une répartition et un partage optimal des ressources de l'entreprise. En plus des nouvelles exigences de sécurité qui découlent de l'utilisation de ceux-ci.

- **Caractéristiques d'un VLAN**

- Un VLAN supprime les contraintes physiques relatives aux communications d'un groupe de travail,
- Un VLAN peut couvrir tout un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN),
- Une station peut appartenir à plusieurs VLAN simultanément.

- **Les types de VLAN**

Il existe plusieurs méthodes de construction de VLAN : [16]

- **VLAN par port** : il est défini en associant chaque VLAN à un port du commutateur. Son avantage, c'est qu'il est facile d'emploi. L'inconvénient est qu'on ne définit qu'un seul VLAN par port.
- **VLAN basée sur l'adressage MAC** : il s'agit de dire quelles adresses MAC (adresses physiques) appartiennent à tel VLAN. L'avantage est que des stations sur un même port peuvent être sur des VLAN différents. L'inconvénient, c'est la difficulté de manipulation des adresses MAC.
- **VLAN par Protocole** : est obtenu en associant un réseau virtuel par type de protocole du réseau (par exemple TCP/IP), regroupant ainsi toutes les machines utilisant le même protocole dans un même VLAN.

- **Les protocoles utilisés**

1. **Le protocole VTP (VLAN Trunking Protocol)**

Il permet de gérer les VLANs de manière centralisée selon un modèle maître/esclave, ce qui permet de configurer un switch pour qu'il propage les configurations VLAN aux autres switches du domaine. Les configurations VLAN sont stockées dans la base de données VLAN des switches (vlan.dat). Un domaine VTP se compose de switches interconnectés. Pour échanger les configurations entre ces switches, des annonces ou informations VTP sont utilisées via des liens trunk. Par défaut, la configuration VTP d'un switch inclut : une version VTP de 1, un nom de domaine VTP nul, un mode VTP serveur, et tous les ports dans le VLAN1. [17]

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [18] :

- **Le mode serveur**

– L'information est stockée dans la NVRAM.
– Il définit le nom de domaine VTP.
– Il peut ajouter, modifier ou supprimer un VLAN.
– Il stocke la liste des VLANs du domaine VTP.

- **Le mode client**

– Il possède un nom de domaine.
– Il stocke une liste de VLANs non modifiable.

- **Le mode transparent**

– Il ne participe pas aux domaines VTP du réseau.
– Il transmet les paquets VTP via ses liens trunk.
– Il possède sa propre liste de VLANs qu'il est possible de modifier.

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :

– Il faut assigner le même nom de domaine de VTP à chaque commutateur.
– L'option trunk pour l'interconnexion des commutateurs doit être activée [18].

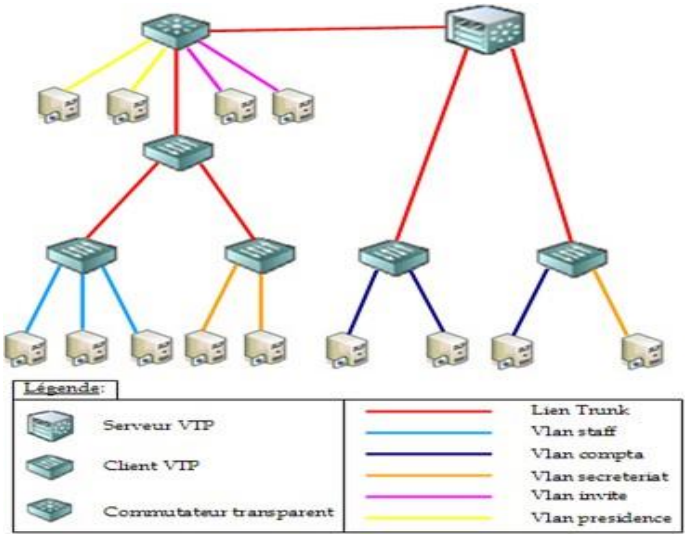



**Figure II.11 :** Le protocole VTP.

## 2. Le protocole STP (Spanning-Tree Protocol)

- **Définition**

Le protocole STP est un protocole de couche 2 qui fonctionnent sur des ponts et des commutateurs. La spécification des protocoles STP est IEEE 802.1. L'objectif principale 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.

- **Concept du protocole STP**

Le protocole STP utilise l'Algorithme SpanningTree (STA) pour déterminer quels ports de commutateurs doivent être bloqués afin d'éviter les boucles réseau. L'algorithme sélectionne un commutateur comme pont racine, qui sert de référence pour le calcul des chemins. Les commutateurs échangent des trames BPDU pour identifier le commutateur avec l'identificateur de pont (BID) le plus faible, qui devient alors le pont racine. Chaque trame BPDU contient un identificateur de pont composé d'une valeur de priorité, de l'adresse MAC du commutateur émetteur et éventuellement d'un ID système étendu. Après avoir désigné le pont racine, l'algorithme STA attribue des rôles spécifiques aux ports des commutateurs pour réguler le trafic [18].

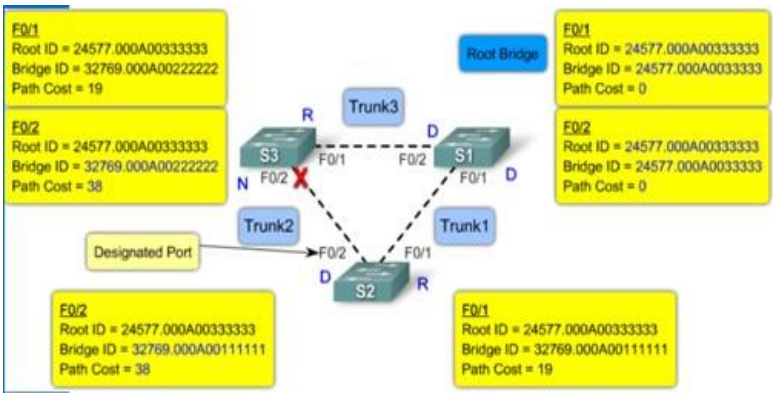



**Figure II.12 :** Exemple du concept du protocole STP.

## 3. GLBP (Gateway Load Balancing Protocol)

- **Définition**

Gateway Load Balancing Protocol est un protocole propriétaire Cisco qui permet de

faire de la redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, mais plusieurs adresses MAC virtuelles.

Le protocole GLBP élit un Active Virtual Gateway (AVG) qui va répondre aux requêtes ARP pour l'adresse IP virtuelle. GLBP permet de donner un poids variable à chacun des routeurs participants pour la répartition de la charge entre ces routeurs. La charge est donc répartie par hôte dans le sous-réseau.

- **Fonctionnement du GLBP**

Le protocole GLBP a dans son fonctionnement les mêmes concepts de bases que HSRP et VRRP. Plus concrètement, à l'intérieur du groupe GLBP, le routeur ayant la plus haute priorité ou la plus haute adresse IP du groupe prendra le statut de « AVG » (Active Virtual Gateway). Ce routeur va intercepter toutes les requêtes ARP effectuées par les clients pour avoir l'adresse MAC de la passerelle par défaut, et grâce à l'algorithme d'équilibrage de charge préalablement configuré, il va renvoyer l'adresse MAC virtuelle d'un des routeurs du groupe GLBP. C'est d'ailleurs le Routeur AVG qui va assigner les adresses MAC virtuelles aux routeurs du groupe, Ainsi ils ont le statut « AVF » (Active Virtual Forwarder). Un maximum de 4 adresses MAC virtuelle est défini par groupe, les autres routeurs ayant des rôles de backup en cas de défaillance des AVF.

Toutefois, en dépit du fait que ce protocole reprend les concepts de base de HSRP et VRRP, il convient de noter que contrairement à ces deux protocoles, dans le fonctionnementdu GBLP, tous les routeurs du groupe GLBP participent activement au routage ce qui n'est pas le cas de VRRP ou HSRP, il n'y en a qu'un qui est en mode actif, tandis que les autres sont en attentes (standby).

Au-delà des possibilités de redondances, tolérance aux pannes ainsi que la continuité des services que nous offre le protocole GBLP, sa particularité est qu'il est capable d'effectuer l'équilibrage des charges entre routeurs qu'on désigne par « Load Balancing » [19].

### 4. Protocole d’agrégation des ports PAgP

- **Définition**

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 et est considéré

comme port unique [20].

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.

- **Mode de PAgP**

PAgP utilise les modes suivants :

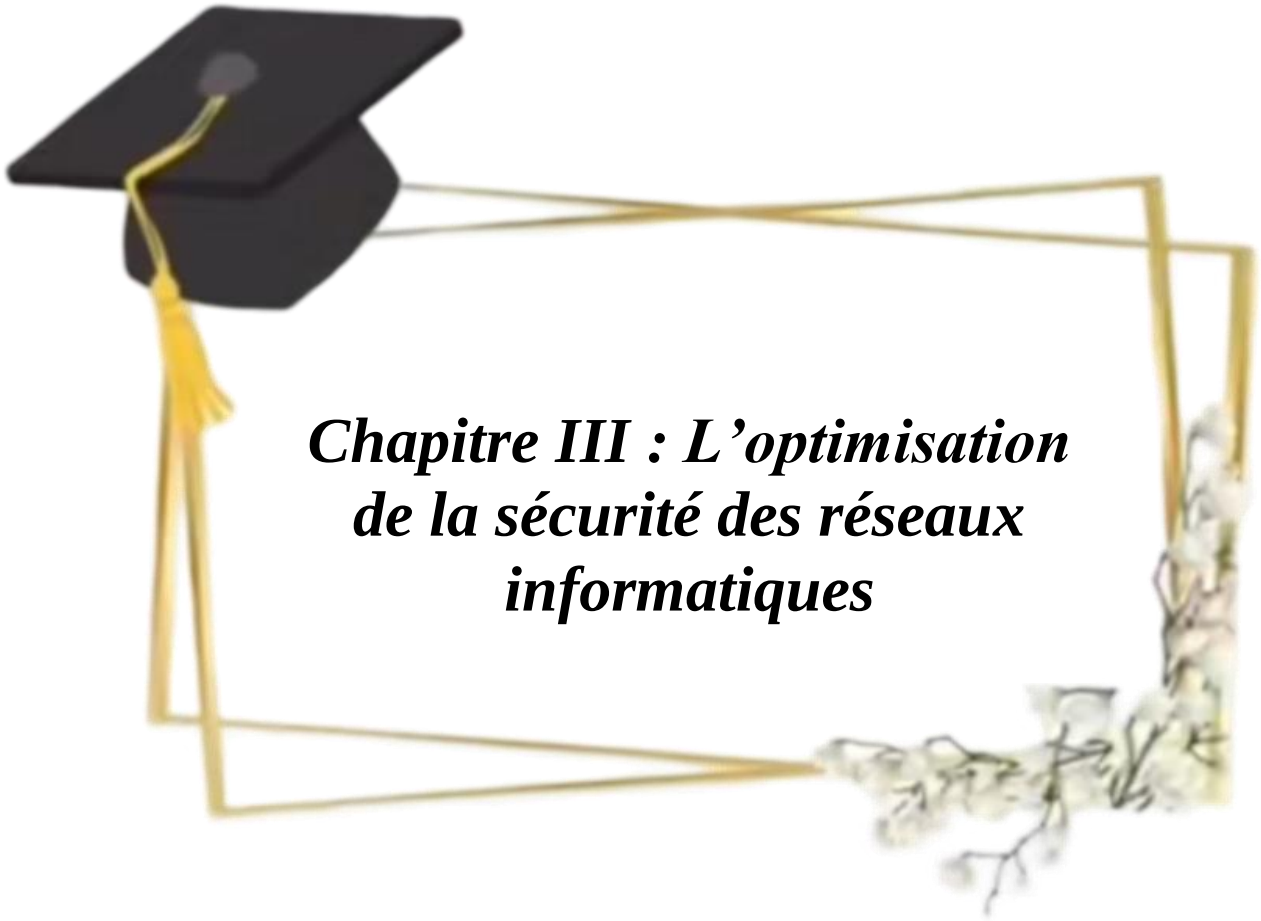
▪ **On :** Ce mode force l'interface à établir un canal sans PAgP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets PAgP.

▪ **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.

▪ **Auto :** Ce mode PAgP 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 PAgP.

## II.4 Conclusion

La sécurité des réseaux informatiques est un enjeu crucial à l'heure actuelle, notamment en raison de la nature ouverte et complexe d'Internet. Pour renforcer la sécurité, divers outils comme les pare-feu, les proxys et les réseaux privés virtuels sont utilisés. Cependant, afin de garantir une protection efficace, il est indispensable de définir clairement les objectifs de sécurité.



# *Chapitre III : L'optimisation de la sécurité des réseaux informatiques*

## III.1 Introduction

L'optimisation de la sécurité d'une infrastructure réseau est un aspect crucial dans le domaine de la sécurité informatique. Dans le contexte actuel, où les réseaux informatiques sont au cœur de nombreuses activités professionnelles, gouvernementales et personnelles, la protection de ces infrastructures contre les menaces cybernétiques est devenue une priorité absolue.

Ce chapitre va se concentrer sur l'examen approfondi des stratégies, des technologies et des meilleures pratiques visant à optimiser la sécurité des infrastructures réseau.

### III.1.1 Définition de l'optimisation de la sécurité réseau

la mise en place d'une stratégie à but de renforcer la protection des infrastructures informatiques en identifiant les vulnérabilités, évaluant les risques et mettant en place des mesures pour atténuer ces risques, assurant ainsi la sécurité des données et des services.

L'optimisation de la sécurité des réseaux vise à atteindre plusieurs objectifs essentiels pour garantir la protection des informations, la continuité des opérations, et la confidentialité des utilisateurs.

## III.2 Evaluation de la sécurité réseau existante

Elle consiste à analyser et mesurer l'efficacité des mesures de sécurité mises en place pour protéger le réseau contre les menaces et les vulnérabilités. Cette évaluation comprend plusieurs aspects clés :

### III.2.1 Audit de sécurité réseau

C'est une démarche, censée être périodique, qui permet de connaître le niveau de sécurité global de votre système d'information, et d'évaluer le degré de sa conformité par rapport à votre politique de sécurité,

L'audit de sécurité informatique garantit ainsi la disponibilité du système d'information, l'intégrité de vos données, la confidentialité des accès, et permet de déceler les vulnérabilités du SI afin d'en maitriser les risques.

- **Un audit de sécurité doit permettre d'atteindre les objectifs suivants :**

  - évaluer le niveau de maturité du SI (analyse de l'architecture réseau, configuration, contrôle des accès, sécurité des ressources humaines et des communications, cryptographie, etc.) ;
  - tester la résistance du SI face à une attaque ;
  - tester l'efficacité de la politique de sécurité du SI (PSSI) ;
  - vérifier la conformité du SI.
  - Tester l'intégration d'un nouvel équipement.

Après l'audit de sécurité, vient le temps des résultats restitués dans un rapport d'audit qui vous recommandera les optimisations prioritaires à faire pour assurer la sécurité de votre Système d'Information.

Ce document compile l'ensemble des failles de sécurité constatées et apporte les recommandations, classées par ordre de priorité, à mettre en œuvre pour les corriger [21].

### III.2.2 Identification des vulnérabilités et des points faibles

Pour l'identification on s'appuie sur un test de vulnérabilité

- **Test de vulnérabilité :**

Un test de vulnérabilité est une évaluation systématique des points faibles potentiels dans les systèmes informatiques, les réseaux ou les applications d'une entreprise. Il vise à identifier les vulnérabilités de sécurité spécifiques qui pourraient être exploitées par des attaquants pour compromettre la confidentialité, l'intégrité ou la disponibilité des données.

- **Déroulement d'un test de vulnérabilité :** il se fait principalement en 5 étapes

1. **La reconnaissance :** est l'une des étapes clés dans le processus de test de vulnérabilité. Elle consiste à collecter des informations sur la cible (système, réseau ou application) pour en savoir plus sur son fonctionnement, son architecture, ses points d'entrée et ses vulnérabilités potentielles

La reconnaissance peut être effectuée de manière active ou passive. La reconnaissance passive consiste à collecter des informations disponibles publiquement, comme les informations sur le site web. La reconnaissance active, en revanche, consiste à envoyer des requêtes à la cible pour collecter des informations sur les ports ouverts, les services en cours d'exécution, les versions

de logiciels utilisés et autres informations qui pourraient être utiles pour identifier les vulnérabilités.

2. **Analyse de vulnérabilités :** Elle consiste à examiner les résultats de la reconnaissance et à identifier les vulnérabilités potentielles dans le système ou le réseau testée**.**

   Cette analyse peut être effectuée manuellement ou à l'aide d'outils automatisés qui peuvent détecter des vulnérabilités connues dans les logiciels et les systèmes d'exploitation. Les vulnérabilités susceptibles d'inclure des failles de sécurité dans le code, des erreurs de configuration, des erreurs de conception, des vulnérabilités dans les protocoles de communication, et bien plus encore.

3. **Exploitation des vulnérabilités** : est une étape du test de vulnérabilité qui consiste à utiliser les vulnérabilités protégées pour prévenir leur impact potentiel sur le système, le réseau ou l'application testée.

   L'exploitation des vulnérabilités peut être effectuée de manière manuelle ou automatisée, selon les vulnérabilités et les outils disponibles. L'objectif est de déterminer si les vulnérabilités sont effectivement exploitables, quel est l'impact de leur exploitation sur la sécurité du système, et si des données sensibles peuvent être compromises.

4. **Post exploitation :** est une étape du test de vulnérabilité qui convient à l'exploitation des vulnérabilités. Elle consiste à effectuer des actions supplémentaires sur le système, le réseau ou l'application testée pour limiter l'étendue des dommages qu'un attaquant pourrait causer s'il parvenait à exploiter une vulnérabilité.

   La post-exploitation peut inclure la collecte de données supplémentaires, l'escalade de privilèges, la persistance, la création d'une porte dérobée ou l'installation de logiciels malveillants. L'objectif est de supprimer que les vulnérabilités infectées peuvent être utilisées pour compromettre la sécurité du système testé de manière plus avancée.

5. **Génération de rapport :** Les rapports de test de vulnérabilité doivent fournir une analyse détaillée de toutes les vulnérabilités signalées, de leur impact potentiel sur la sécurité du système testé, ainsi que des recommandations pour les corriger et améliorer la sécurité globale du système.

   Les rapports de test de vulnérabilité doivent également fournir des preuves concrètes de toutes les vulnérabilités prouvées, y compris des captures d'écran, des journaux d'exploitation, des exemples de code et d'autres éléments qui fournissent les résultats du test. Les rapports doivent être complets, organisés et faciles à suivre [22].

### III.2.3 Analyse des risques associés à l'infrastructure réseau

C'est une étape préalable à la sécurisation du système d'information, et permet d'évaluer les éventualités et les conséquences plausibles de multiples risques, avant de décider des actions à mener et de leur ordonnancement. Cela permet de réduire ces risques à un niveau acceptable. Chaque risque est identifié, quantifié, qualifié et priorisé par rapport aux critères de son évaluation et à ses impacts sur le réseau**.**

Différentes méthodes existent pour l'analyse des risques liés à la sécurité de l'information ; nous nous référons à la méthode d'Ebios (Expression des Besoins et Identification des Objectifs de Sécurité) de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ainsi qu'à la norme ISO 27005.

- **Méthode d'Ebios :** est maintenue par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Elle a été revue en 2018 et s'intitule EBIOS Risk Manager.

La méthode EBIOS Risk Manager adopte une approche de management du risque qui part du plus haut niveau (grandes missions de l'objet étudié) pour s'intéresser progressivement aux éléments métier et techniques, en étudiant les chemins d'attaque possibles. Elle vise à obtenir une synthèse entre conformité et scénarios par le repositionnement de ces deux approches complémentaires là où elles apportent le plus de valeur ajoutée.

La méthode repose sur cinq ateliers ayant chacun un objectif.

1. **Cadrage et socle de sécurité**, reposant sur les principes de base en termes de sécurité et le cadre réglementaire et normatif.
2. **Identification des sources de risques**, c'est à dire un élément, une personne, un groupe de personnes ou une organisation susceptible d'engendrer un risque, et caractérisé par sa motivation, ses ressources, ses compétences, et ses modes opératoires.
3. **Définition des scénarios stratégiques**, qui sont des chemins d'attaque allant d'une source de risque à un objectif visé, en passant par l'écosystème et les valeurs métier de l'objet étudié.
4. **Définition des scénarios opérationnels**, définis comme des enchaînements d'actions élémentaires portées sur les biens supports de l'objet étudié ou de son écosystème.
5. **Recensement des mesures de sécurité appropriées** dans un plan d'amélioration continue de la sécurité.

- **La norme ISO 27005 :** L'ISO 27005 définit un cadre et des exigences en matière de gestion du risque pour la mise en place d'un système de management de la sécurité de l'information. Elle s'inscrit dans une logique d'amélioration continue PDCA (Plan, Do, Check, Act). Le risque est défini comme l'effet de l'incertitude sur l'atteinte des objectifs.[23]

## III.3 Planification et conception de l'optimisation de la sécurité réseau

### III.3.1 Les stratégies de sécurité réseau

Après avoir défini les objectifs et les différents types de politiques de sécurité réseau, nous détaillons à présent les stratégies de sécurité à adopter pour mettre en œuvre une telle politique. La conception de stratégies de sécurité exige de prendre en compte l'historique de l'entreprise, l'étendue de son réseau, le nombre d'employés, la sous-traitance avec des tierces parties, le nombre de serveurs, l'organisation du réseau, etc.

#### III.3.1.1 Méthodologie pour élaborer une politique de sécurité réseau

Diverses méthodes permettent d'élaborer des stratégies de sécurité. Nous décrivons ici la méthodologie générique à savoir :

- **Prédiction des attaques potentielles et analyse de risque**

La première étape consiste à déterminer les menaces qui pèsent sur les biens de l'entreprise, ainsi que les impacts de ces menaces sur l'activité de l'entreprise si elles devaient se concrétiser. Le rapprochement entre les ressources critiques de l'entreprise et les risques de sécurité associés, déterminés par le triptyque menace/vulnérabilité/conséquence, permet de définir la stratégie sécurité de l'entreprise. Afin de protéger ses biens critiques des menaces identifiées, l'entreprise doit aussi analyser les techniques d'attaque utilisées pour enfreindre les contrôles de sécurité ou tirer parti des vulnérabilités. Ce deuxième niveau d'analyse permet de définir des stratégies de sécurité proactives, visant à diminuer les probabilités d'occurrence des menaces.

- **Analyse des résultats et amélioration des stratégies de sécurité**

Les différentes simulations sont l'occasion d'améliorer les contre-mesures de sécurité, voire de les remettre en question. Par exemple, si l'on constate que certains types d'attaques ne sont pas détectés par un pare-feu, les règles de filtrage définies ou le pare-feu lui-même doivent être remis en cause. Il faut aussi valider l'efficacité des stratégies de sécurité mises en place face aux simulations exécutées. Enfin, dans la mesure où la stratégie existante n'a pas apporté de résolution satisfaisante, il est nécessaire de la modifier ou d'en créer une nouvelle.

- **Règles élémentaires d'une stratégie de sécurité réseau :** Lors de la conception d'une stratégie de sécurité, il faut toujours garder à l'esprit quelques règles ou principes élémentaires afin de se prémunir des erreurs possibles dans le choix de contre-mesures. Voici quelques-uns :

- **Simplicité :** Plus une stratégie n'est complexe, plus il est difficile de l'appliquer, de la maintenir dans le temps ou de la faire évoluer. La simplicité et le pragmatisme sont des critères de réussite d'une stratégie de sécurité ;
- **Le maillon le plus faible :** Un réseau est composé d'un ensemble d'équipements, ayant ou non une fonction de sécurité implémentée. Pour qu'une stratégie de sécurité recouvre le périmètre de l'entreprise, il faut s'assurer que toutes les méthodes d'accès fournissent un même niveau de sécurité, faute de quoi le maillon le plus faible sera privilégié pour attaquer le réseau d'entreprise ;
- **Variété des protections** : La variété des solutions mises en place pour assurer la sécurité ne doit pas se fonder sur un seul type de logiciel de pare-feu ou de détection d'intrusion ;
- **L'implémentation en profondeur des mécanismes de sécurité** : La sécurité ne doit jamais reposer sur un seul mécanisme de sécurité. Une imbrication de mécanismes offre une garantie de sécurité bien supérieure, pour peu que le premier élément de sécurité vienne à faillir. L'implémentation de mécanismes de sécurité en profondeur doit être comprise et perçue comme une assurance de sécurité à plusieurs niveaux. Plus le système à protéger est critique, plus le nombre de mécanismes de sécurité ne doit être important [8].

## III.3.2 Choix des technologies et des solutions de sécurité adaptées

L'un des aspects les plus importants de la sécurité des réseaux est le choix, l'utilisation d'outils et de technologies de sécurité. Ces outils et technologies sont conçus pour faire face a de nombreux problèmes comme [24] :

-Les cybercriminels exploitent souvent les failles des systèmes d'authentification. Pour cela on recommande les solutions suivantes :

1. **MFA (Multi-Factor Authentification) :** Pour une sécurité renforcée, combinez un mot de passe avec un code unique.

2. **SSO (Single Sign-On) :** Simplifiez la gestion des mots de passe tout en maintenant une sécurité robuste.

3. **IAM (Identity and Access Management) :** Assurez-vous que chaque employé n'accède qu'aux informations nécessaires à sa fonction.

-Les attaques réseau peuvent paralyser une entreprise. Pour éviter ça, on a choisi les solutions suivantes :

1. **Firewall :** Filtre le trafic suspect pour protéger votre réseau.

2. **IPS/IDS :** Surveille le réseau pour détecter et bloquer les activités malveillantes.

3. **VPN :** Assure une connexion sécurisée pour les employés à distance.

4. **NAC (Network Access Control) :** Contrôle les dispositifs pouvant se connecter à votre réseau.

5. **CDN (Content Delivery Network) :** Protège contre les attaques DDoS et accélère la distribution du contenu.

-Les dispositifs connectés peuvent être la porte d'entrée des cyberattaques. Pour les éviter, on recommande ces solutions :

1. **EDR (Endpoint Detection and Response) :** Surveille les comportements suspects sur les appareils.

2. **Antivirus et antimalware :** Détecte et supprime les logiciels malveillants.

-Les menaces évoluent constamment, et une détection rapide est cruciale. On recommande comme solutions les suivantes :

1. **XDR (Extended Detection and Response) :** Offre une vue consolidée des menaces.

2. **SOC (Security Operations Center) :** Une équipe dédiée pour surveiller et répondre aux menaces.

3. **SIEM :** Centralise la surveillance en collectant et analysant les journaux et événements de sécurité.

- Les données non protégées peuvent être interceptées ou modifiées. Pour cela, on recommande les solutions suivantes :

1. **Chiffrement :** Assure que seules les personnes autorisées peuvent lire les données.

2. **Gestion des clés de chiffrement :** Stocke et gère en toute sécurité les clés.

3. **Signature numérique :** Confirme l'authenticité d'un message ou d'un document.

-Sans évaluation, vous ne pouvez pas connaître les faiblesses de votre système. Les solutions suivantes aident à reconnaitre ces faiblesses :

1. **Scanners de vulnérabilité** : Identifie les faiblesses potentielles.

2. **Tests d'intrusion :** Simule des attaques pour évaluer la robustesse de votre système.

3. **Audits de sécurité (pentest) :** Réalise une évaluation complète de votre posture de sécurité.

## III.4 Renforcement de la sécurité des périphériques réseau

Le renforcement de la sécurité des périphériques réseau consiste à appliquer des mesures et des technologies visant à protéger ces dispositifs contre les attaques et les intrusions. Cela inclut la configuration sécurisée, les mises à jour régulières, l'authentification renforcée, et la surveillance continue pour détecter toute activité suspecte.

### III.4.1 Configuration sécurisée des routeurs et des commutateurs

La sécurisation des routeurs et des commutateurs est essentielle pour protéger les réseaux. Cela inclut la sécurisation des accès physiques et distants, l'utilisation de mots de passe complexes et chiffrés, et la désactivation des interfaces inutilisées. Il est crucial de maintenir les dispositifs à jour, de segmenter le réseau avec des VLANs, d'utiliser des ACLs pour filtrer le trafic, et de configurer la journalisation et la surveillance centralisées. L'utilisation d'IPSec pour les communications et la documentation des configurations sont également indispensables pour une sécurité optimale.

### III.4.2 Filtrage de listes de contrôle d'accés (ACL)

#### III.4.3.1 Définition

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

En général Les ACL assurent les tâches suivantes : Elles limitent les trafics réseaux pour accroître les performances réseaux, elle contrôle les flux de trafic, elles fournissent un niveau de sécurité de base pour l'accès de réseau, elles filtrent les hôtes pour autoriser ou refuser l'accès au service sur le réseau [25].

## III.4.3.2 Le fonctionnement des listes de contrôles d'accès

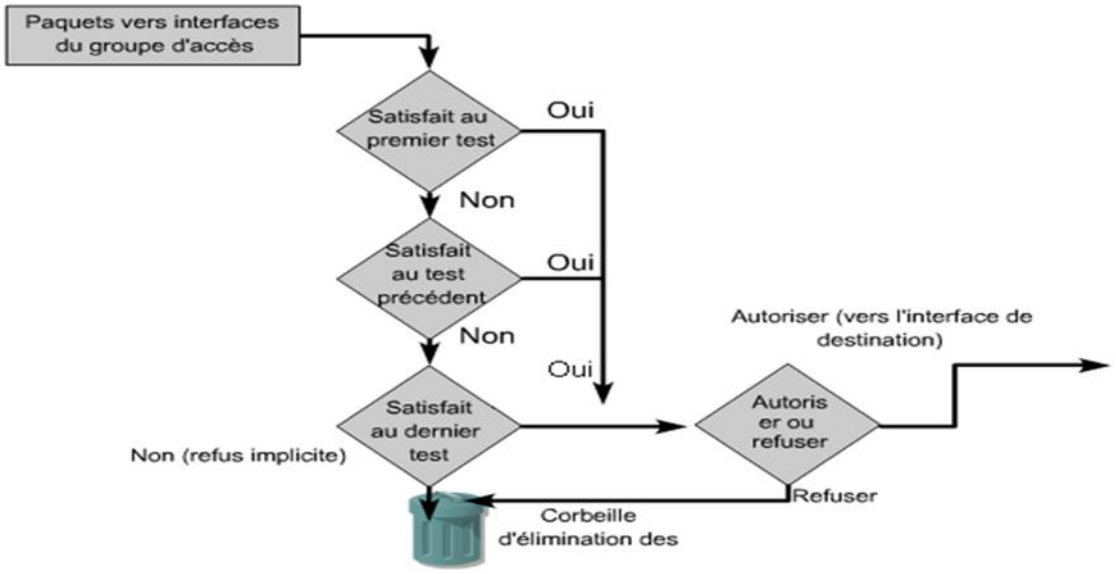



**Figure III.1 :** fonctionnement des listes de contrôles.

Une liste de contrôle d'accès est un groupe d'instructions qui définissent si les paquets sont acceptés ou rejetés au niveau des interfaces d'entrée et de sortie. Pour prendre ces décisions, les paquets sont comparés avec une instruction de condition d'une liste d'accès, puis acceptés ou rejetés selon l'action définie dans l'instruction.

L'ordre des instructions ACL est important. La plate-forme logicielle Cisco IOS teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin. Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées. Si une instruction de condition autorisant l'accès à tout le trafic est située en haut de la liste, aucune instruction ajoutée en dessous ne sera vérifiée.

Pour ajouter des instructions de condition supplémentaires dans une liste d'accès, vous devez supprimer toute la liste et en recréer une avec les nouvelles instructions. Pour faciliter le processus de révision d'une liste de contrôle d'accès, il est préférable d'utiliser un éditeur de texte comme le Bloc-notes et de coller la liste dans la configuration du routeur [38].

## III.5 Sécurisation des communications réseau

### III.5.1 Chiffrement des données en transit

Les données sont considérées comme étant en transit lorsqu'elles circulent entre des appareils, comme au sein de réseaux privés ou sur Internet. Pendant le transfert, les données sont plus exposées en raison de la nécessité de déchiffrement avant le transfert et des vulnérabilités de la méthode de transfert elle-même. Le fait de chiffrer les données pendant le transfert, ou chiffrement de bout en bout, garantit leur confidentialité même si elles sont interceptées [26].

## III.5.2 Implémentation de protocoles de sécurité robustes (IPsec, SSL/TLS,etc)

### III.5.2.1 Le protocole IPSec (Internet Protocol Security) [5]

IPsec est un protocole défini par l'ETF permettant de sécuriser les échanges au niveau de la couche réseau.

Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Le protocole IPSec est basé sur trois modules :

- IP Authentification Header (AH) concernant l'intégrité, l'authentification et la protection contre le rejet des paquets à encapsuler.
- Encapsulating Security Payload (ESP) définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejet.
- Security Assocation (SA) définissant l'échange des clés et des paramètres de sécurité. Les SA rassemblent ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP (les protocoles AH et/ou ESP, mode tunnel ou transport, les algorithmes de sécurité utilisés par les proto-coles, les clés utilisées...). L'échange des clés se fait soit de manière manuelle soit avec le protocole d'échange IKE (la plupart du temps), qui permet aux deux parties de s'entendre sur les SA.

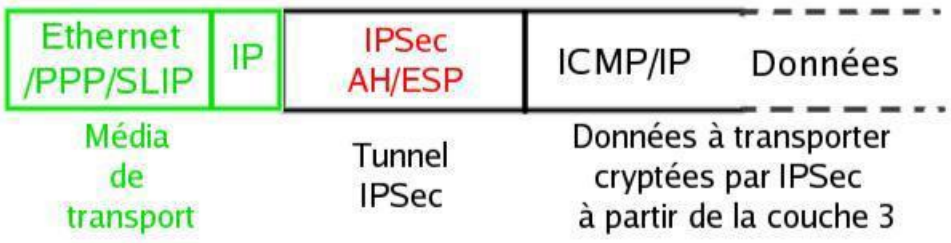


**Figure III.2 :** IPsec.

#### III.5.2.2 Implémentation de SSL/TLS

Comme SSL/TLS est un protocole situé entre la couche Application et la couche Transport, tous les protocoles applicatifs utilisant TCP peuvent l'exploiter pour sécuriser leurs échanges, comme HTTPS (pour sécuriser HTTP) ou FTPS (pour sécuriser FTP).

Généralement, un protocole applicatif basé sur SSL/TLS obtient un nouveau numéro de port par l'IANA. Par exemple, HTTPS est associé au port 443. Dans certains cas, le même port est utiliséavec et sans SSL/TLS, où la connexion est initiée en mode non chiffré, ensuite un tunnel sera mis enplace au moyen du mécanisme StartTLS, c'est le cas par exemple des protocoles IMAP, SMTP ou LDAP [7].

## III.6 Surveillance et détection des menaces

### III.6.1 Journalisation et surveillance de la sécurité réseau

- **Journalisation :** consiste à collecter des données sur les activités, les événements, les erreurs, et l'état général d'un système d'information ou d'un réseau. Son but est de recueillir des informations pertinentes pour la sécurité afin d'aider les administrateurs à comprendre le comportement des systèmes et à enquêter sur des incidents de sécurité potentiels [27].
- **Surveillance :** implique l'observation des données collectées à partir de diverses sources, comme les dispositifs réseau, serveurs, applications et bases de données, pour détecter des changements et des anomalies. Elle vise à identifier des signes d'attaques connues, des comportements inhabituels ou des activités non autorisées. Cette tâche doit être réalisée par des analystes de sécurité ou une équipe dédiée, et non par les administrateurs système responsables de la configuration des systèmes [27].

### III.6.3 Utilisation de solutions de gestion des informations et des évènements de sécurité (SIEM)

#### III.6.3.1 Définition

La gestion des informations et des événements liés à la sécurité (SIEM) est une solution de gestion des journaux et des événements qui connaît un certain succès et qui a fait ses preuves. La SIEM consiste essentiellement à recueillir un maximum d'informations sur les journaux provenant de tous les secteurs de l'entreprise.

### III.6.3.2 Fonctionnalités SIEM et cas d'utilisation

Les SIEM (Security Information and Event Management) sont des systèmes qui offrent différentes fonctionnalités et peuvent être utilisés dans divers cas :

- **Gestion des journaux :** Les SIEM collectent et centralisent les données, puis les organisent pour détecter les signes de menaces, d'attaques ou de violations de sécurité.
- **Corrélation des événements :** Les données sont analysées pour identifier les relations et les schémas afin de détecter rapidement les menaces potentielles.
- **Surveillance et réponse aux incidents :** Les SIEM surveillent les incidents de sécurité sur le réseau d'une organisation, fournissant des alertes et des audits pour toutes les activités liées à ces incidents [28].

Les systèmes SIEM offrent diverses fonctionnalités permettant de réduire les risques liés à la cybersécurité. Ils peuvent être utilisés pour détecter les activités suspectes des utilisateurs, surveiller leurs comportements, limiter les tentatives d'accès non autorisées et générer des rapports de conformité. Ces cas d'utilisation contribuent à renforcer la sécurité des systèmes informatiques et à prévenir les incidents de sécurité.

## III.7 Conclusion

L'optimisation de la sécurité des réseaux informatiques est essentielle pour se protéger contre les menaces. Cela commence par une évaluation approfondie des vulnérabilités, suivie de la planification de stratégies de renforcement, comme la sécurisation des accès et l'utilisation de mots de passe complexes. La sécurité des communications est assurée par des protocoles comme SSH et IPSec. Enfin, une surveillance proactive et la détection des menaces permettent de réagir rapidement aux incidents. Ces mesures garantissent une protection robuste et adaptative des réseaux.

# *Chapitre IV:*
# *Réalisation*

# IV.1 Introduction

Ce chapitre explore la mise en place et la configuration d'un environnement de travail réseau en utilisant des outils et logiciels spécifiques. Nous aborderons notamment l'utilisation des logiciels GNS3 et VMware Workstation 17 Pro pour la simulation et la gestion de réseaux virtuels, ainsi que l'implémentation de machines virtuelles pour divers systèmes d'exploitation. L'objectif est de fournir une architecture réseau robuste et efficace, répondant aux besoins du campus NTS et permettant la mise en œuvre la solution proposée en Chapitre 1. Tout en assurant la sécurité et la fiabilité des communications.

# IV.2 Environnement de travail

## IV.2.1 Présentation de logiciel de simulation

### IV.2.1.1 GNS3

Gns3 (Graphical Network Emulator) est un émulateur de réseau graphique multiplateforme àsavoir Windows, Linux et MacOs. L'un des avantages majeurs du logiciel est qu'il est open source et gratuit que vous pouvez télécharger sur http://gns3.com. Il est utilisé par les ingénieurs réseau du monde entier pour simuler, configurer, tester et dépanner des réseaux virtuels et réels car il permet de connecter des hyperviseurs à partir de VMware ou VirtualBox.

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 le logo de GNS3.

**Figure IV.1 :** Logo de GNS3.

### IV.2.1.2 VMwareWorkstation17 pro

VMware Workstation est un logiciel de machine virtuelle (VM) qui permet aux utilisateursd'exécuter plusieurs machines virtuelles sur une seule machine physique. Elle se réalise sur sonpropre système d'exploitation (OS, Operating System), tel que : Linux, MacOs, Windows, etbénéficiedes mêmeséquipements qu'une machine physique : CPU, mémoireRAM, disque duret carte réseau. VMware simplifie la gestion et offre un meilleur contrôle sur

l'infrastructure informatique.

Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation en suivant les étapes d'installations jusqu'à la fin puis cliquer sur le bouton « terminer ». La figure 4.2 présente L'interface graphique de VMware Workstation 17.

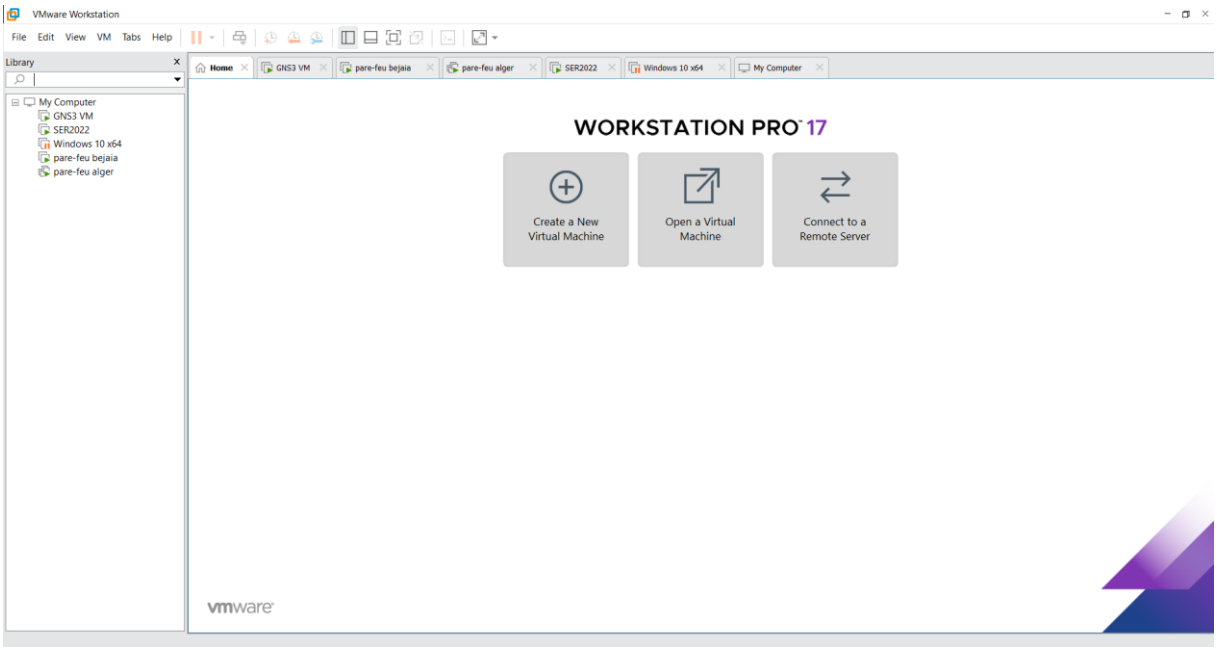



**Figure IV.2 :** Interface graphique de VMware Workstation 17.

### IV.2.2 Les machines virtuelles

Une machine virtuelle (VM) est une simulation logicielle d'un système d'exploitation complet, qui fonctionne sur un ordinateur physique. Elle est exécutée grâce à un logiciel appelé hyperviseur, comme VMware. Le système d'exploitation installé dans la machine virtuelle est stocké sous forme de fichiers sur le disque dur de l'ordinateur hôte. L'objectif principal des machines virtuelles est de permettre à plusieurs systèmes d'exploitation de fonctionner simultanément sans avoir besoin de matériel physique supplémentaire.

#### IV.2.2.1 PfSense

PfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. PfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

**Figure IV.3 :** logo pfSense.

### IV.2.2.2 Windows serveur 2022

Windows Server 2022 est la version actuelle du système d'exploitation de Microsoft destinée aux serveurs. Ce système propose une sécurité multicouche avancée, des fonctionnalités hybrides avec Azure et une plateforme d'application flexible.

Après avoir installé VMware Workstation 17 Pro, ou les informations sur les comptes d'utilisateurs, comme les noms, les mots de passe sont stockés. Nous allons installer le systèmed'exploitation Windows Server. Pour créer cette nouvelle machine virtuelle, nous allons ouvrir VMware et cliquer sur "Nouvelle machine virtuelle" dans le menu "Fichier". Ensuite, nous allons suivre les étapes jusqu'à ce que nous terminions l'installation. Nous arrivons sur la fenêtre ci-dessous :

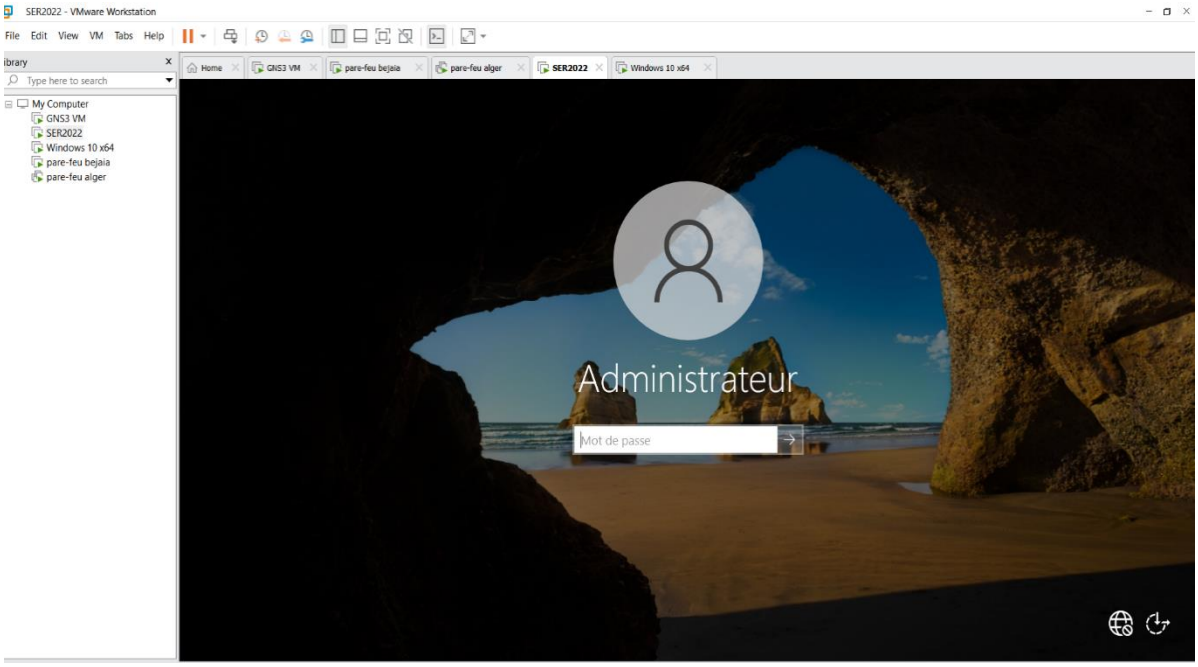



**Figure IV.4:** La page d'accueil de Windows server 2022.

#### IV.2.2.3 Windows 10

Windows 10 est un système d'exploitation de la famille Windows NT développé par la société américaine Microsoft.

## IV.3 La nouvelle architecture proposée

Nous avions initialement prévu de créer une topologie uniquement avec des switchs fédérateurs directement reliés au pare-feu. Cependant, nos PC ne sont pas assez puissants pour les supporter et nous craignions des bugs. Par conséquent, nous avons opté pour une autre solution : utiliser deux routeurs dans la couche cœur et deux switchs dans la couche d'accès. Ces équipements vont assumer les fonctions que nous avions prévues pour les switchs fédérateurs. Les routeurs assureront le routage inter-VLAN, tandis que les switchs se chargeront du switching.

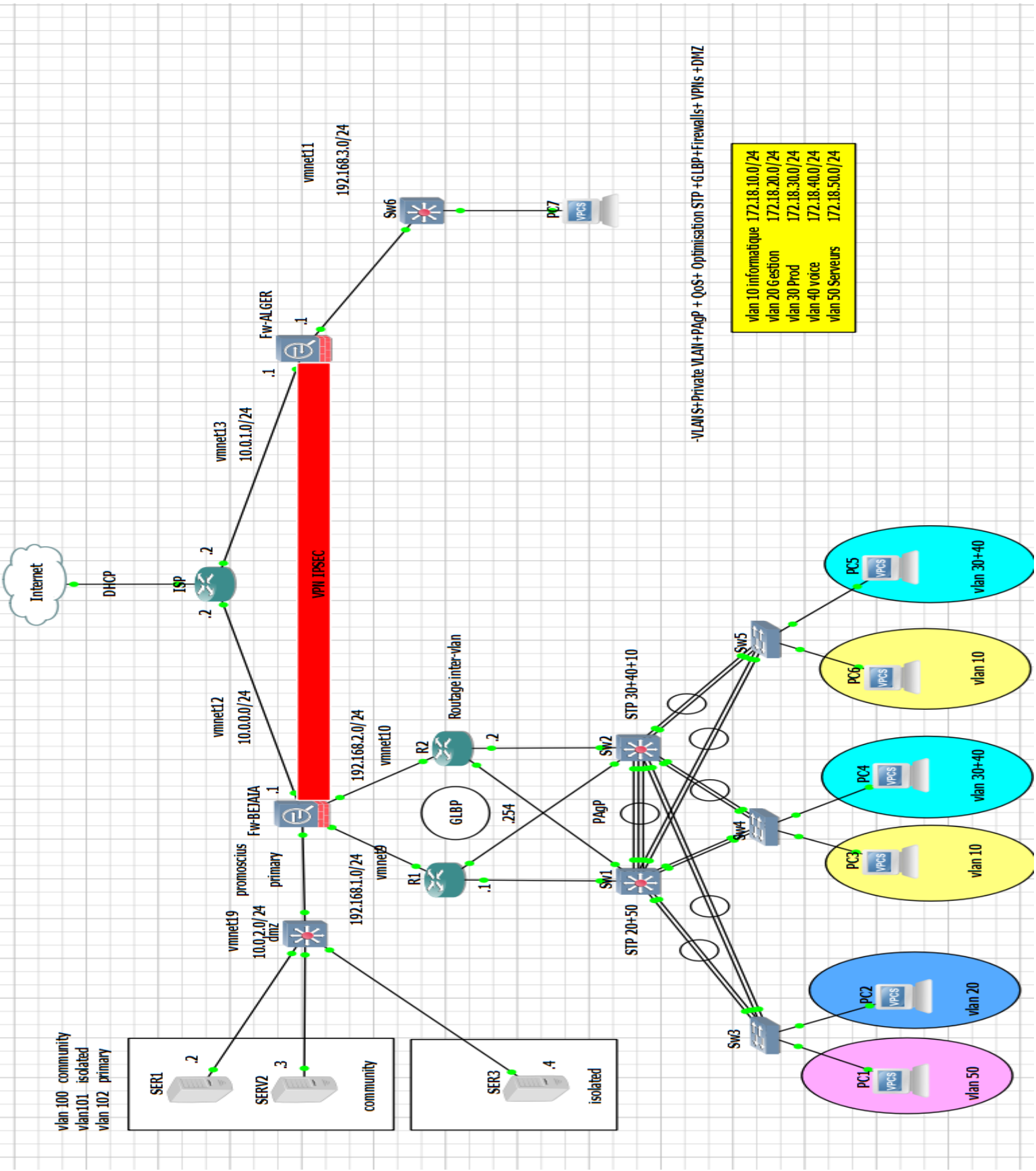

-VLANS+Private VLAN+PAgP + QoS+ Optimisation STP +GLBP+Firewalls+ VPNs +DMZ
vlan 10 informatique 172.18.10.0/24
vlan 20 Gestion 172.18.20.0/24
vlan 30 Prod 172.18.30.0/24
vlan 40 voice 172.18.40.0/24
vlan 50 Serveurs 172.18.50.0/24
Internet
DHCP
ISP
VPN IPSEC
Fw-ALGER
Fw-BEJAIA
promoscius
primary
Sw6
PC7
vmnet11
192.168.3.0/24
vmnet13
10.0.1.0/24
vmnet12
10.0.0.0/24
192.168.2.0/24
vmnet10
Routage inter-vlan
R2
R1
GLBP
.254
PAgP
SW1
SW2
STP 30+40+10
STP 20+50
Sw5
Sw4
Sw3
PC5
PC6
PC4
PC3
PC2
PC1
vlan 30+40
vlan 10
vlan 30+40
vlan 10
vlan 20
vlan 50
vmnet19
10.0.2.0/24
dmz
192.168.1.0/24
vmnet9
SER1
SERV2
SER3
community
isolated
vlan 100 community
vlan101 isolated
vlan 102 primary

**Figure IV.5 :** Architecture du réseau proposé.

### IV.3.1 Le plan d'adressage des sous réseaux « VLANs »

| Nom de VLAN | ID de VLAN | Adresse du sous-réseau | Passerelle du sous-réseau |
|---|---|---|---|
| VLAN Informatique | 10 | 172.18.10.0/24 | 172.18.10.1 |
| VLAN Gestion | 20 | 172.18.20.0/24 | 172.18.20.1 |
| VLAN Prod | 30 | 172.18.30.0/24 | 172.18.30.1 |
| VLAN Voice | 40 | 172.18.40.0/24 | 172.18.40.1 |
| VLAN Serveurs | 50 | 172.18.50.0/24 | 172.18.50.1 |

**Tableau IV.1 :** Plan d'adressage des VLANs.

### IV.3.2 Plan d'adressage des Privates VLANs et ports associés

| **Nom du VLAN** | **ID du VLAN** | **Portshosts** | **Ports promis cuousmapping** | **Adresse Private VLAN** |
|---|---|---|---|---|
| **SECONDARY COMMU-NITY** | 100 | 100 102 | 100101,102 | 10.0.2.2/24 10.0.2.3/24 |
| **SECONDARY ISOLATED** | 101 | 101 102 | 100101,102 | 10.0.2.4/24 |
| **PRIMARY** | 102 | / | 100101,102 | 10.0.2.1/24 |

**Tableau IV.2 :** Plan d'adressage des (sous-réseaux) Private VLAN.

### IV.3.3 Plan d'adressage des équipements d'interconnexion

| Equipements | Interface réseau | Adresse IP |
|---|---|---|
| Pare-feu Bejaia | External (WAN)<br>DMZ<br>Internal LAN1<br>Internal LAN2 | 10.0.0.1/24<br>10.0.2.1/24<br>192.168.1.1/24<br>192.168.2.1/24 |
| Pare-feu Alger | WAN<br>Internal LAN | 192.168.3.0/24<br>10.0.1.0/24 |
| Router 1 | Ethernet 0/0<br>Ethernet 0/1 | Utilisé pour le routage inter-vlan et GLBP 192.168.1.1/24<br>192.168.1.254/24 |
| Router 2 | Ethernet 0/0<br>Ethernet 0/1 | Utilisé pour le routage inter-vlan et GLBP 192.168.2.2/24<br>192.168.2.254/24 |
| Sw-access3 | Vlan 20 gestions<br>Vlan 50 serveurs | 172.18.20.0/24<br>172.18.50.0/24 |
| Sw-access4 | Vlan 10 informatiques<br>Vlan 30 prod<br>Vlan 40 voice | 172.18.10.0/24<br>172.18.30.0/24<br>172.18.40.0/24 |
| Sw-access5 | Vlan 10 informatiques<br>Vlan 30 prod<br>Vlan 40 voice | 172.18.10.0/24<br>172.18.30.0/24<br>172.18.40.0/24 |
| Router ISP | WAN (Bejaia)<br>WAN (Alger)<br>Internet | 10.0.0.2/24<br>10.0.1.0/24<br>DHCP |

**Tableau IV.3 :** Plan d'adressage des équipements d'interconnexion.

### IV.3.4 Tableau de routage inter-vlan

| Equipements | Interface | Adresse IP | Machine virtuelle |
|---|---|---|---|
| Router1 | e0/0 | / | / |
| | e0/0.10 | 172.18.10.1 | 172.18.10.254 |
| | e0/0.20 | 172.18.20.1 | 172.18.20.254 |
| | e0/0.30 | 172.18.30.1 | 172.18.30.254 |
| | e0/0.40 | 172.18.40.1 | 172.18.40.254 |
| | e0/0.50 | 172.18.50.1 | 172.18.50.254 |
| Router2 | e0/0.10 | 172.18.10.2 | 172.18.10.254 |
| | e0/0.20 | 172.18.20.2 | 172.18.20.254 |
| | e0/0.30 | 172.18.30.2 | 172.18.30.254 |
| | e0/0.40 | 172.18.40.2 | 172.18.40.254 |
| | e0/0.50 | 172.18.50.2 | 172.18.50.254 |

**Tableau IV.4 :** Tableau de routage inter-vlan.

## IV.4 Configuration du routeur ISP

- **Vers Internet**

```
ISP(config)#interface ethernet0/0
ISP(config-if)#description // interface vers internet //
ISP(config-if)#ip address dhcp
ISP(config-if)#
*Jun 22 11:29:56.118: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP a
ddress 192.168.122.116, mask 255.255.255.0, hostname ISP

ISP(config-if)#ip nat outside
ISP(config-if)#ip virtual-reassembly in
ISP(config-if)#end
```

**Figure IV.6 :** configuration de l'interface vers Internet.

- **Vers les deux sites BEJAIA et ALGER**

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#interface ethernet 0/1
ISP(config-if)#description // interface vers BEJAIA //
ISP(config-if)#ip address 10.0.0.2 255.255.255.0
ISP(config-if)#ip nat inside
ISP(config-if)#ip virtual-reassembly in
ISP(config-if)#exit
ISP(config)#do wr
Building configuration...
[OK]
ISP(config)#interface ethernet 0/2
ISP(config-if)#description // interface vers ALGER //
ISP(config-if)#ip add 10.0.1.2 255.255.255.0
ISP(config-if)#ip nat inside
ISP(config-if)#ip virtual-reassembly in
ISP(config-if)#exit
ISP(config)#do wr
Building configuration...
[OK]
```

**Figure IV.7 :** Configuration des interfaces vers les deux sites (Bejaia et Alger).

## IV.5 Configuration de DHCP

Pour créer un pool d'adresse pour chaque vlan.

```
R2#show running-config | section dhcp
ip dhcp pool vlan 10
 network 172.18.10.0 255.255.255.0
 default-router 172.18.10.254
 dns-server 8.8.8.8
 lease 15
R2#
```

```
R1#show running-config | section dhcp
ip dhcp excluded-address 172.18.50.1 172.18.50.10
ip dhcp excluded-address 172.18.20.1 172.18.20.10
ip dhcp excluded-address 172.18.40.1 172.18.40.10
ip dhcp excluded-address 172.18.30.1 172.18.30.10
ip dhcp pool vlan50
 network 172.18.50.0 255.255.255.0
 default-router 172.18.50.254
 dns-server 8.8.8.8
 lease 15
ip dhcp pool vlan20
 network 172.18.20.0 255.255.255.0
 default-router 172.18.20.254
 dns-server 8.8.8.8
ip dhcp pool vlan30
 network 172.18.0.0 255.255.0.0
 default-router 172.18.30.1
 dns-server 8.8.8.8
 lease 15
ip dhcp pool vlan40
 network 172.18.40.0 255.255.255.0
 default-router 172.18.40.1
 dns-server 8.8.8.8
 lease 15
 --More--
```

**Figure IV.8 :** Configuration DHCP.

## IV.6 Configuration des équipements

Nous allons maintenant présenter une vue d'ensemble de la configuration des équipements nécessaires à la mise en place de la nouvelle architecture proposée.

### IV.6.1 Configuration des commutateurs

Commençons par détailler la configuration des commutateurs chargés d'interconnecter les divers réseaux hétérogènes.

### IV.6.2 Configuration des interfaces trunk

Un trunk désigne une liaison physique permettant de transporter le trafic de plusieurs VLANs. Pour configurer ces interfaces trunk entre deux commutateurs, on procède de la manière suivante :

Vu le nombre d'interface à configurer, on utilisera la même configuration.

```
Sw1(config)#interface ethernet0/0
Sw1(config-if)#switchport trunk encapsulation dot1q
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#exit
```

**Figure IV.9:** Configuration trunk sur le switch distribution Sw1.

```
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#interface ethernet 0/1
Sw3(config-if)#switchport trunk encapsulation dot1q
Sw3(config-if)#switchport mode trunk
Sw3(config-if)#exit
```

**Figure IV.10:** Configuration trunk sur le switch d'accès Sw3.

### IV.6.3 Configuration d'un domaine VTP

Le protocole VTP (VLAN Trunking Protocol) permet la gestion des VLANs. Dans notre cas, nous avons configuré les commutateurs de distribution en mode VTP server, tandis que les commutateurs d'accès sont paramétrés en mode VTP client.

```
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vtp mode server
Device mode already VTP Server for VLANS.
Sw1(config)#vtp domain vtp.collable
Domain name already set to vtp.collable.
Sw1(config)# vtp password cisco
Password already set to cisco
Sw1(config)#vtp version 2
VTP version is already in V2.
Sw1(config)#vtp pruning
Pruning already switched on
Sw1(config)#exit
```

**Figure IV.11:** Configuration VTP serveur sur le switch distribution Sw1.

```
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#vtp mode client
Device mode already VTP Client for VLANS.
Sw3(config)#vtp domain vtp.collable
Domain name already set to vtp.collable.
Sw3(config)#vtp password cisco
Password already set to cisco
Sw3(config)#vtp version 3
```

**Figure IV.12 :** Configuration VTP client sur le switch d'accès Sw3.

Vérification après avoir configurer le VTP sur les switchs.

```
Sw1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : vtp.collable
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 5-22-24 18:46:38
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 10
Configuration Revision            : 8
MD5 digest                        : 0x42 0x7A 0xD2 0x3F 0xD4 0xE3 0xC7 0x95
                                    0xD5 0xB6 0xD9 0x0F 0xB7 0x50 0x79 0x0B
Sw1#
```

```
Sw3#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : vtp.collable
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0500
Configuration last modified by 0.0.0.0 at 6-12-24 00:42:01

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 10
Configuration Revision            : 9
MD5 digest                        : 0xEA 0x51 0x47 0xB3 0x27 0xB6 0x72 0x28
                                    0x1A 0xAD 0xE4 0xBE 0x81 0xB0 0xDC 0xC9
```

**Figure IV.13:** vérification de la configuration VTP sur les switchs Sw1, Sw3.

### IV.6.4 Création des VLANs

La création de VLANs permet d'une part de regrouper logiquement les différents équipements, et d'autre part d'administrer individuellement les droits et les priorités d'accès des utilisateurs. Dans le cadre de notre déploiement, nous avons défini cinq VLANs distincts, chacun étant associé à un service spécifique.

```
Sw1#
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#vlan 10
Sw1(config-vlan)#name informatique
Sw1(config-vlan)#vlan 20
Sw1(config-vlan)#name gestion
Sw1(config-vlan)#vlan 30
Sw1(config-vlan)#name prod
Sw1(config-vlan)#vlan 40
Sw1(config-vlan)#name voice
Sw1(config-vlan)#vlan 50
Sw1(config-vlan)#name serveurs
Sw1(config-vlan)#end
Sw1#
```

**Figure IV.14 :** Création des VLANs sur le switch Sw1.

```
Sw1#
*Jun 13 12:03:29.387: %SYS-5-CONFIG_I: Configured from console by console
Sw1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/3, Et1/1, Et1/2, Et1/3
                                                 Et2/0, Et2/1
10   informatique                      active
20   gestion                           active
30   prod                              active
40   voice                             active
50   serveurs                          active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

**Figure IV.15 :** vérification.

### IV.6.5 Affectation des ports au vlans

```
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#interface ethernet 3/0
Sw3(config-if)#switchport mode access
Sw3(config-if)#switchport access vlan 20
Sw3(config-if)#end
Sw3#
*Jun 19 22:17:27.515: %SYS-5-CONFIG_I: Configured from console by console
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#interface ethernet 2/3
Sw3(config-if)#switchport mode access
Sw3(config-if)#switchport access vlan 50
Sw3(config-if)#end
Sw3#
```

**Figure IV.16 :** Affectation des ports au vlan 20 et 50.

### IV.6.6 Configuration des interfaces au mode d'accès vlan

```
Sw4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw4(config)#interface ethernet2/3
Sw4(config-if)#switchport access vlan 30
Sw4(config-if)#switchport mode access
Sw4(config-if)#switchport voice vlan 40
Sw4(config-if)#end
Sw4#
```

**Figure IV. 17 :** Configuration Access sur le sw4 access.

### IV.6.7 Configuration du protocole PAgP

Pour configurer un port channel sur notre switch, nous devons assigner toutes les interfaces qui composeront notre lien logique au même channel-group. Nous avons créé trois liens logiques entre les deux switches de distribution et configuré EtherChannel en mode désirable sur le switch de distribution 1 et sur le switch de distribution 2.

```
Sw1#
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#interface range ethernet 3/1-3
Sw1(config-if-range)#channel-group 1 mode desirable
Sw1(config-if-range)#exit
Sw1(config)#port-channel load-balance src-dst-mac
Sw1(config)#end

Sw1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

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

        A - formed by Auto LAG


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Et3/1(P)    Et3/2(P)    Et3/3(P)
```

**Figure IV.18:** Configuration du protocole PAgP et vérification.

### IV.6.8 Qos (Quality of Service) / STP (Spanning Tree Protocol)

Le protocole STP (Spanning Tree Protocol) permet d'assurer une topologie réseau stable en évitant les boucles ce qui contribue à maintenir la prévisibilité de chemin de transmission pour la Qos. Une fois la topologie stabilisée par STP, la QoS peut alors efficacement prioriser et gérer le trafic selon le besoin assurant ainsi une meilleure

performance du réseau.

On a configuré STP et QoS sur le deux switchs de distribution :

*

```
Sw1#
Sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw1(config)#spanning-tree mode rapid-pvst
Sw1(config)#spanning-tree vlan 20 root primary
Sw1(config)#spanning-tree vlan 50 root primary
Sw1(config)#spanning-tree vlan 30 root secondary
Sw1(config)#spanning-tree vlan 40 root secondary
Sw1(config)#spanning-tree vlan 10 root secondary
Sw1(config)#end
Sw1#
```

```
Sw2#
Sw2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw2(config)#spanning-tree mode rapid-pvst
Sw2(config)#spanning-tree vlan 10 root primary
Sw2(config)#
*Jun 20 12:31:09.068: %IP-4-DUPADDR: Duplicate address 172.18.10.1 on Vlan10, sourc
ed by aabb.cc00.0100
Sw2(config)#spanning-tree vlan 30 root primary
Sw2(config)#spanning-tree vlan 40 root primary
Sw2(config)#spanning-tree vlan 20 root secondary
Sw2(config)#spanning-tree vlan 50 root secondary
Sw2(config)#end
Sw2#
```

**Figure IV.19 :** Configuration stp et Qos sur les deux switchs de distribution Sw1 et Sw2.

### IV.6.9 Configuration des VLANs privées pour notre réseau DMZ

Les VLANs privés sont une technologie de segmentation du réseau de couche 2 qui permet d'isoler ou de segmenter le trafic au sein d'un même segment IP. Cette technologie repose sur deux types de VLANs :

1. **Le VLAN primaire**

Il s'agit du VLAN d'origine utilisé pour envoyer les trames de liaison descendante à tous les sous-VLANs (VLANs secondaires).

2. **Les VLANs secondaires**

- **VLAN isolé :** les ports d'un même VLAN isolé ne peuvent pas communiquer entre eux.
- **VLAN communauté :** les ports du même VLAN communauté peuvent communiquer entre eux et avec le VLAN primaire, mais pas avec d'autres VLANs secondaires.

**Etape 1 : Configuration VTP mode transparent**

```
dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#vtp mode transparent
Device mode already VTP Transparent for VLANS.
```

**Figure IV.20 :** Configuration du mode VTP transparent sur le Switch DMZ.

**Etape 2 : Création du private vlan community**

```
dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#vlan 100
dmz(config-vlan)#private-vlan community
dmz(config-vlan)#end
dmz#
```

**Figure IV.21 :** Création du PVLAN Community sur le Switch DMZ.

**Etape 3 : Création du private vlan isolated**

```
dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#vlan 101
dmz(config-vlan)#private-vlan isolated
dmz(config-vlan)#end
dmz#
```

**Figure IV.22 :** Création du PVLAN isolated sur le Switch DMZ.

**Etape 4 : Création des privates vlans primary**

```
dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#vlan 102
dmz(config-vlan)#private-vlan primary
dmz(config-vlan)#private-vlan association 100-101
dmz(config-vlan)#end
dmz#
```

**Figure IV.23 :** Création des PVLANS primary sur le Switch DMZ.

**Etape 5 : Affectation des ports aux privates VLANs sur le switch DMZ**

```
dmz#
dmz#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
dmz(config)#interface range ethernet 0/0-1
dmz(config-if-range)#switchport mode private-vlan host
dmz(config-if-range)#switchport private-vlan host-association 102 100
dmz(config-if-range)#exit
dmz(config)#interface ethernet 0/2
dmz(config-if)#switchport mode private-vlan host
dmz(config-if)#switchport private-vlan host-association 102 101
dmz(config-if)#exit
dmz(config)#interface ethernet 0/3
dmz(config-if)#switchport mode private-vlan promiscuous
dmz(config-if)#switchport private-vlan mapping 102 101-100
Command Rejected: invalid VLAN list

dmz(config-if)#switchport private-vlan mapping 102 101,100
dmz(config-if)#end
dmz#
```

**Figure IV. 24 :** Affectation des ports aux PVLANs sur le Switch DMZ.

### IV.6.10 Configuration des routeurs

#### IV.6.10.1 Routage inter vlans

Le routage inter-VLAN permet de transférer du trafic réseau d'un VLAN à un autre en utilisant un équipement de couche 3 comme un routeur. Pour configurer cette fonctionnalité, vous allez devoir configurer chacune des interfaces réseau du routeur.

Le principe de configuration est toujours le même, quelle que soit l'interface réseau du routeur que vous souhaitez configurer pour le routage inter-VLAN.

### IV.6.11 Configuration du routage passerelle par défaut

On a routé du réseau 0.0.0.0 vers n'importe quel réseau 0.0.0.0 par la passerelle de sortie du routeur.

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
```

**Figure IV.25 :** Le routage sur le routeur1.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.1
      172.18.0.0/16 is variably subnetted, 10 subnets, 2 masks
C        172.18.10.0/24 is directly connected, Ethernet0/0.10
L        172.18.10.1/32 is directly connected, Ethernet0/0.10
C        172.18.20.0/24 is directly connected, Ethernet0/0.20
L        172.18.20.1/32 is directly connected, Ethernet0/0.20
C        172.18.30.0/24 is directly connected, Ethernet0/0.30
L        172.18.30.1/32 is directly connected, Ethernet0/0.30
```

**Figure IV.26 :** Vérification de routage sur le routeur1.

### IV.6.12 Configuration du protocole GLBP

#### IV.6.12.1 Le protocole GLBP (Gateway Load Balancing Protocol)

GLBP est un protocole qui permet de distribuer la charge de trafic réseau parmi plusieurs routeurs, tout en assurant la redondance de la passerelle par défaut pour une haute disponibilité. Il améliore ainsi l'efficacité et la fiabilité du réseau.

On va configurer le GLBP sur les deux routeurs :

```
interface Ethernet0/0
 no ip address
!
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 172.18.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 glbp 10 ip 172.18.10.254
 glbp 10 priority 150
 glbp 10 preempt
!
interface Ethernet0/0.20
 encapsulation dot1Q 20
 ip address 172.18.20.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 glbp 20 ip 172.18.20.254
 glbp 20 priority 150
 glbp 20 preempt

 interface Ethernet0/0.30
  encapsulation dot1Q 30
  ip address 172.18.30.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
  glbp 30 ip 172.18.30.254
  glbp 30 priority 150
  glbp 30 preempt
 !
 interface Ethernet0/0.40
  encapsulation dot1Q 40
  ip address 172.18.40.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
  glbp 40 ip 172.18.40.254
  glbp 40 priority 150
  glbp 40 preempt
 !
 interface Ethernet0/0.50
  encapsulation dot1Q 50
  ip address 172.18.50.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly in
  glbp 50 ip 172.18.50.254
  glbp 50 priority 150
```

**Figure IV.27 :** Configuration de GLBP sur le routeur 1.

## IV.7 Configuration du Pare-feu PfSense

### IV.7.1 Création des interfaces « DMZ, LAN1, LAN2, WAN » pour le site de Bejaia

Afin que le site Bejaia puisse communiquer avec l'extérieur Alger, on doit créer quatre interfaces, une externe WAN et deux pour le réseau LAN, la dernière pour la DMZ. Et pour le pare-feu d'Alger, deux interfaces unes pour le réseau interne LAN et l'autre pour le réseau externe WAN. Pour la communication réussie entre les deux sites :

#### IV.7.1.1 Pour le site Bejaia

On a d'abord commencéà configurer l'interface LAN sur Pfsense ce qui nous a permis d'avoir un lien http sur un navigateur web

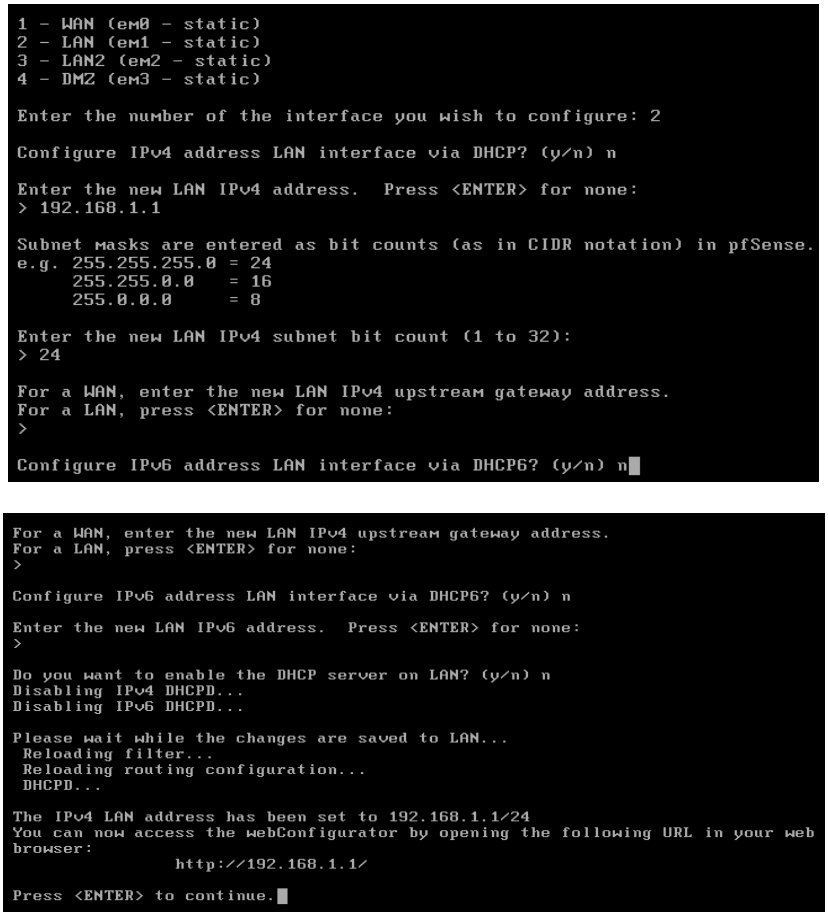



**Figure IV.28 :** Configuration de la première interface LAN.

Maintenant on va pouvoir accéder aux paramètres du pare-feu directement sur le Web à l'aide de l'adresse IP du réseau qu'on a configuré.

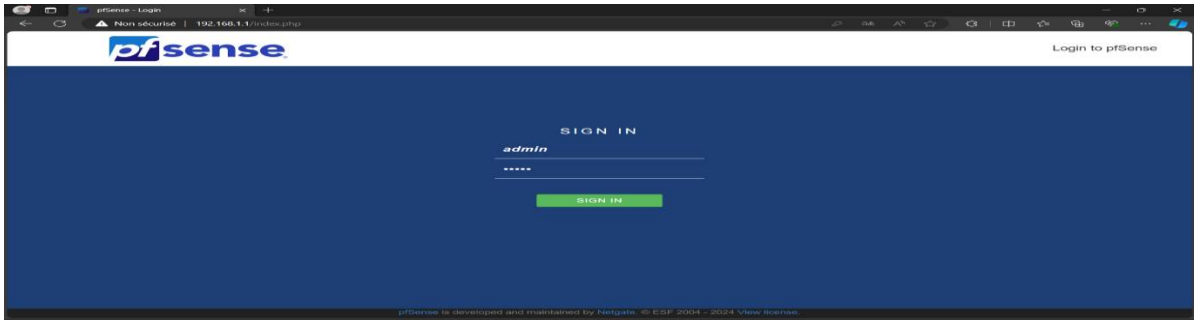



**Figure IV.29 :** Connexion au compte PFsense (site BEJAIA).

Une fois accéder au compte on va suivre ces étapes :

Tout d'abord on va cliquer sur **Interface** en suite sur **Assignements** c'est là où on va pouvoir configurer nos ports avec leur interfaces respectives.

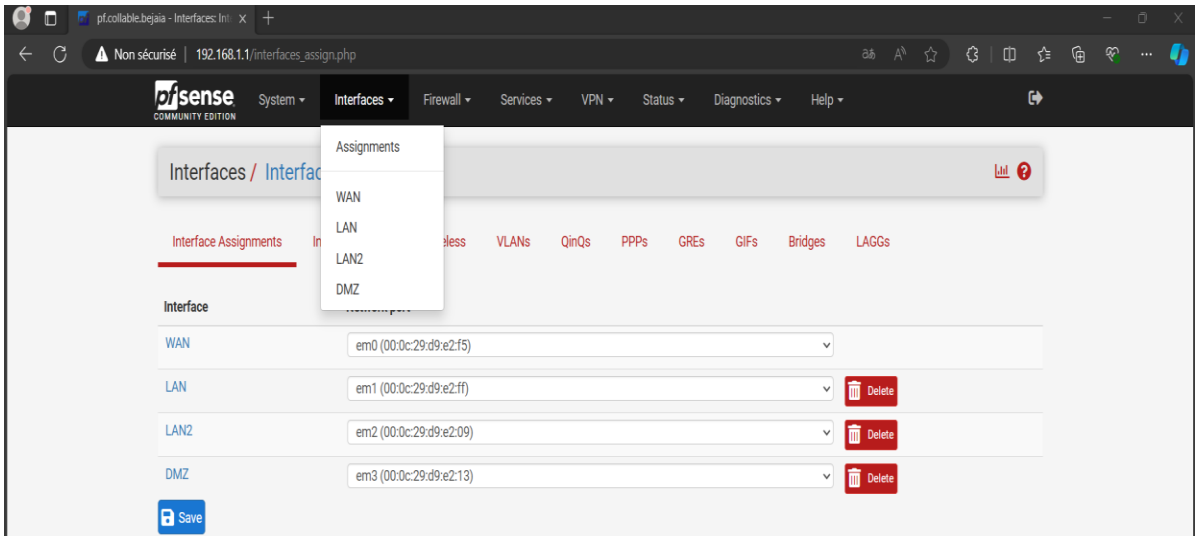



**Figure IV.30 :** Affectations des ports aux interfaces.

- Configuration des interfaces WAN, LAN1, LAN2, DMZ

En cliquant sur **Interfaces** on aura nos 4 interfaces, puis on va choisir l'interface qu'on souhaite configurer en cliquant dessus.

- **Pour l'interface WAN**

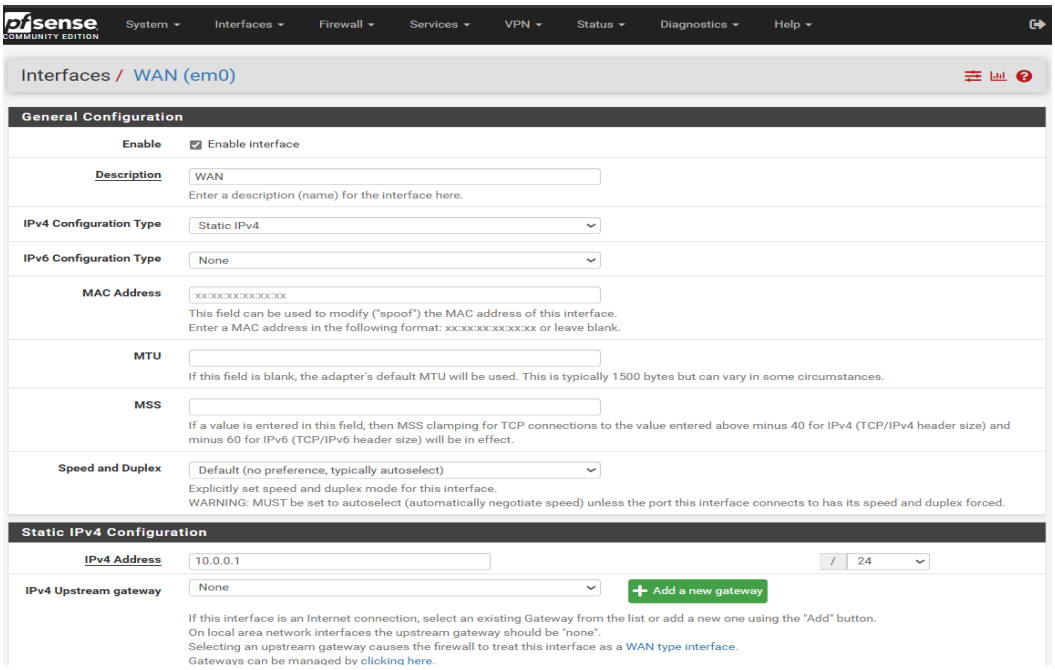



**Figure IV.31 :** Configuration de l'interface WAN (Site Bejaia).

- **Pour l'interface LAN**

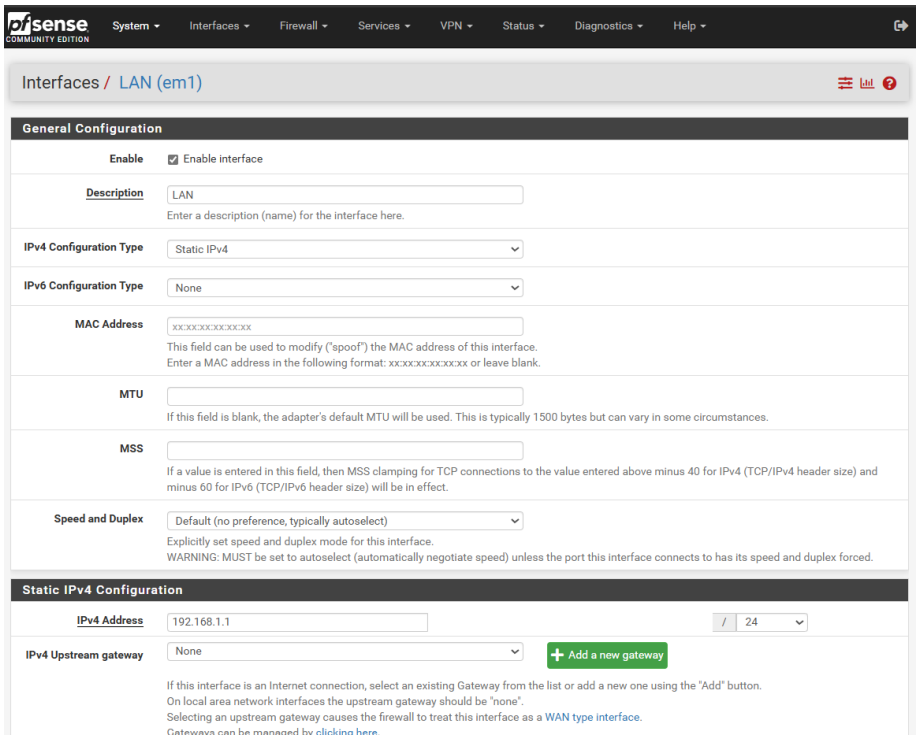



**Figure IV.32 :** configuration de l'interface LAN (Site Bejaia).

- **Pour la 2eme interface LAN2**

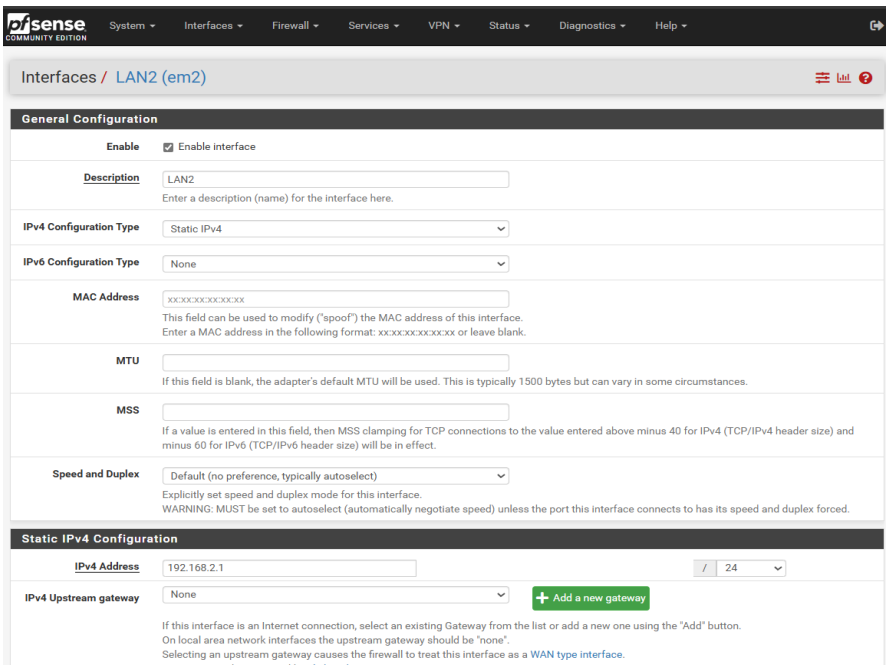



**Figure IV.33 :** configuration de l'interfaces LAN2 (Site Bejaia).

- **Pour l'interface de la DMZ**

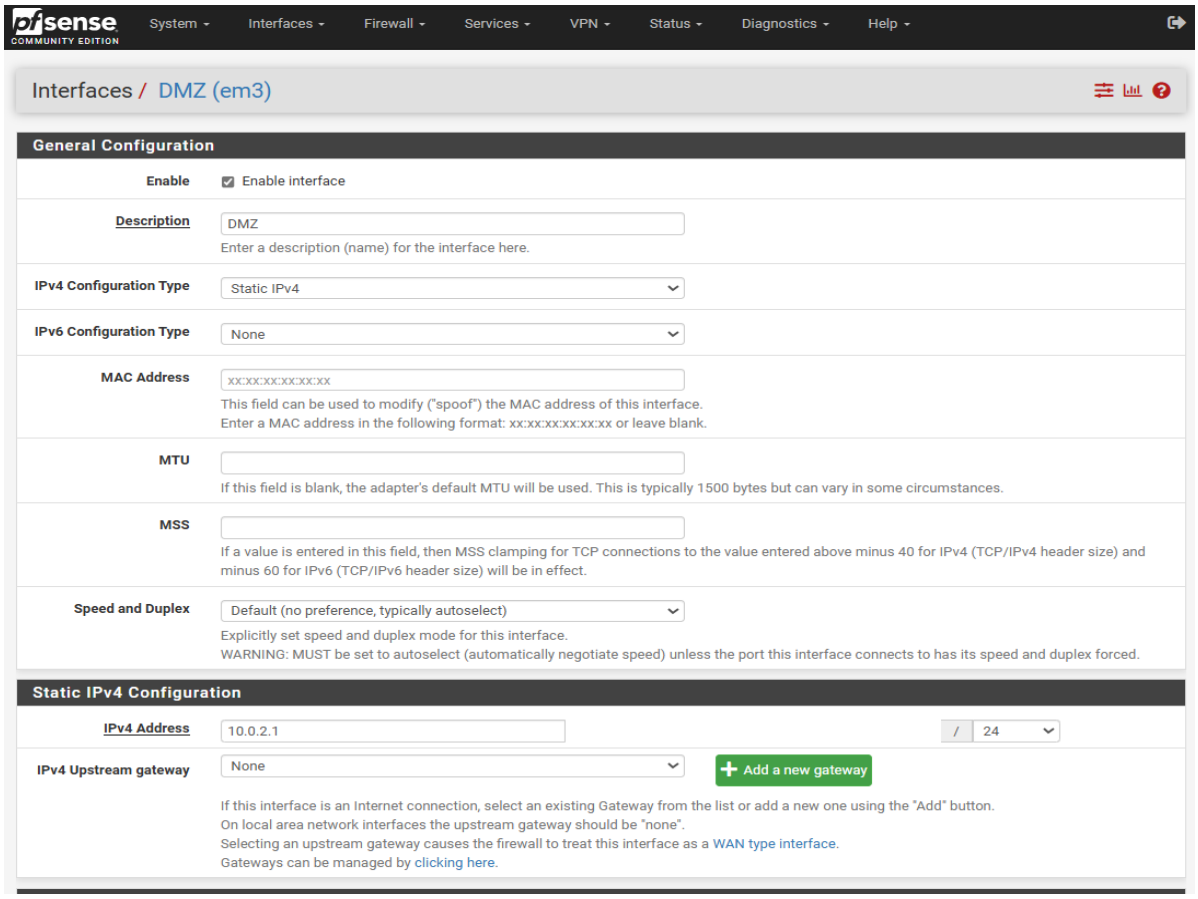



**Figure IV.34 :** Configuration de l'interface de la DMZ (Site Bejaia).

### IV.7.1.2 Pour le site d'Alger

On a d'abord commencéà configurer l'interface LAN sur Pfsense (comme pour le site de Bejaia) ce qui nous a permis d'avoir un lien http sur un navigateur web

On y accède grâce à l'adresse IP du réseau LAN 192.168.3.1.

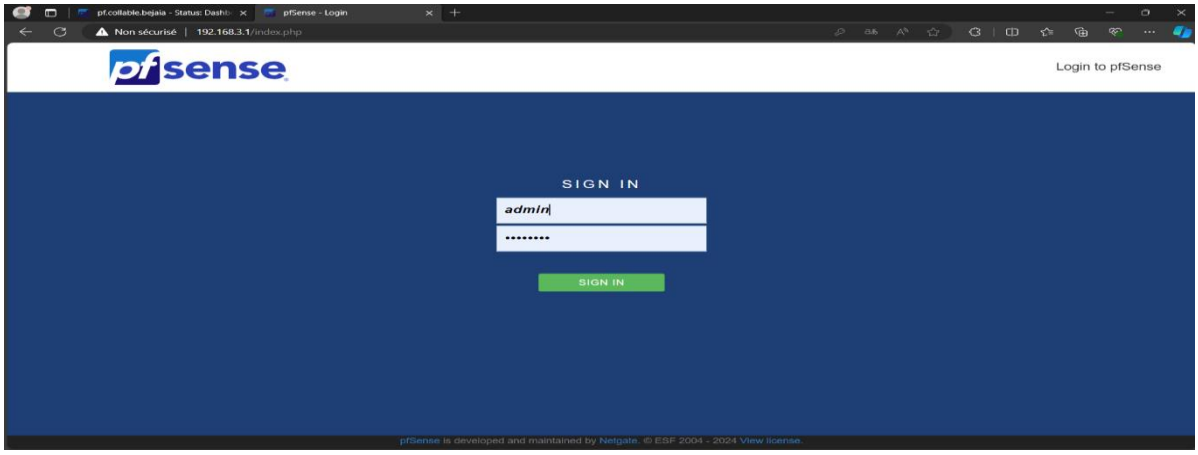



**Figure IV.35 :** Connexion au compte PFsense (site Alger).

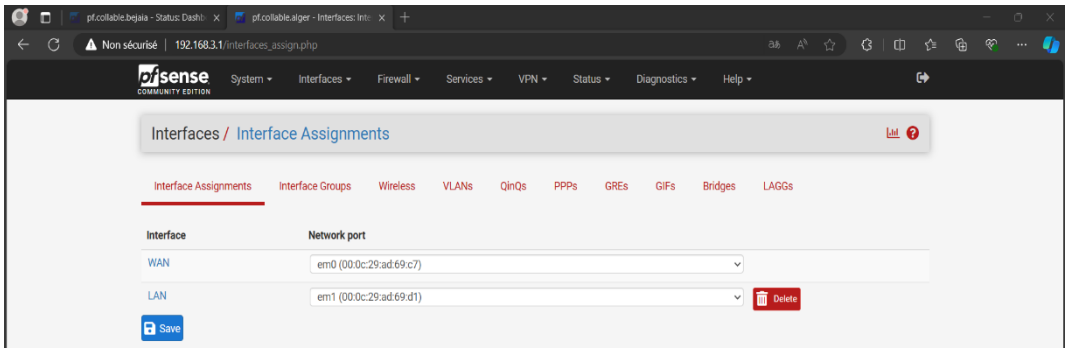



**Figure IV.36 :** Affectations des ports aux interfaces (Site Alger).

- **Configuration des interfaces WAN, LAN**
- **Pour l'interface WAN**

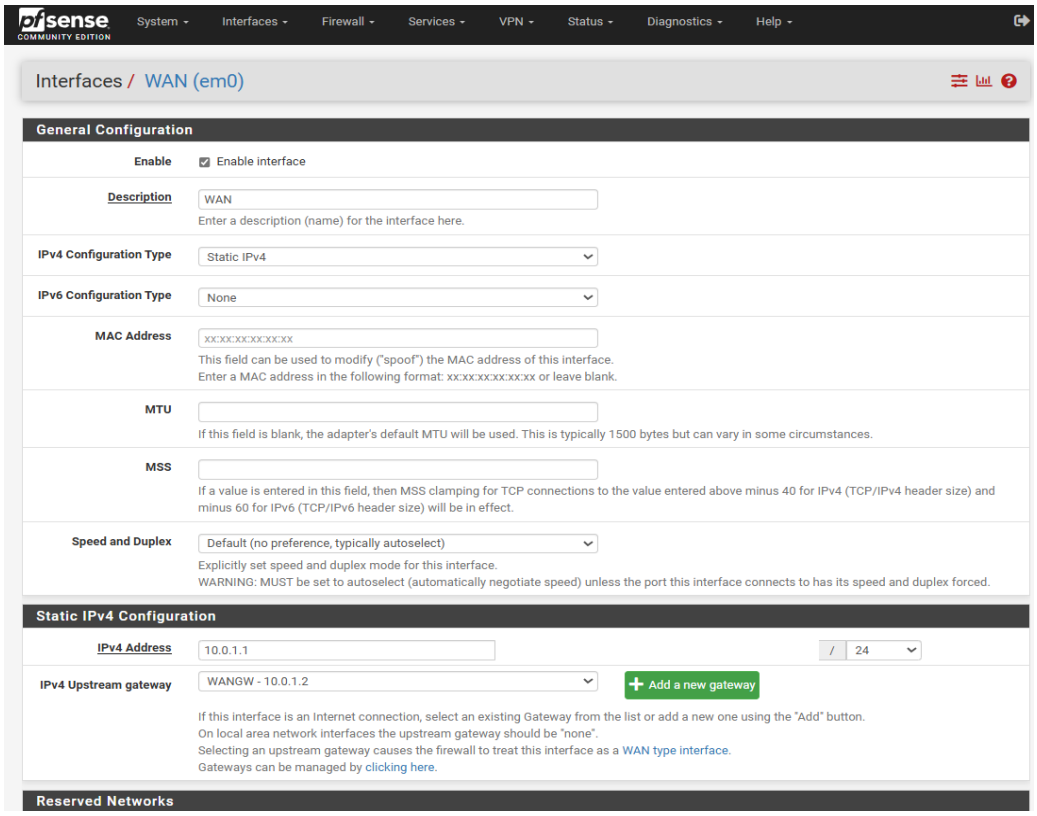



**Figure IV.37 :** Configuration de l'interface WAN (Site Alger).

- **Pour l'interface LAN**

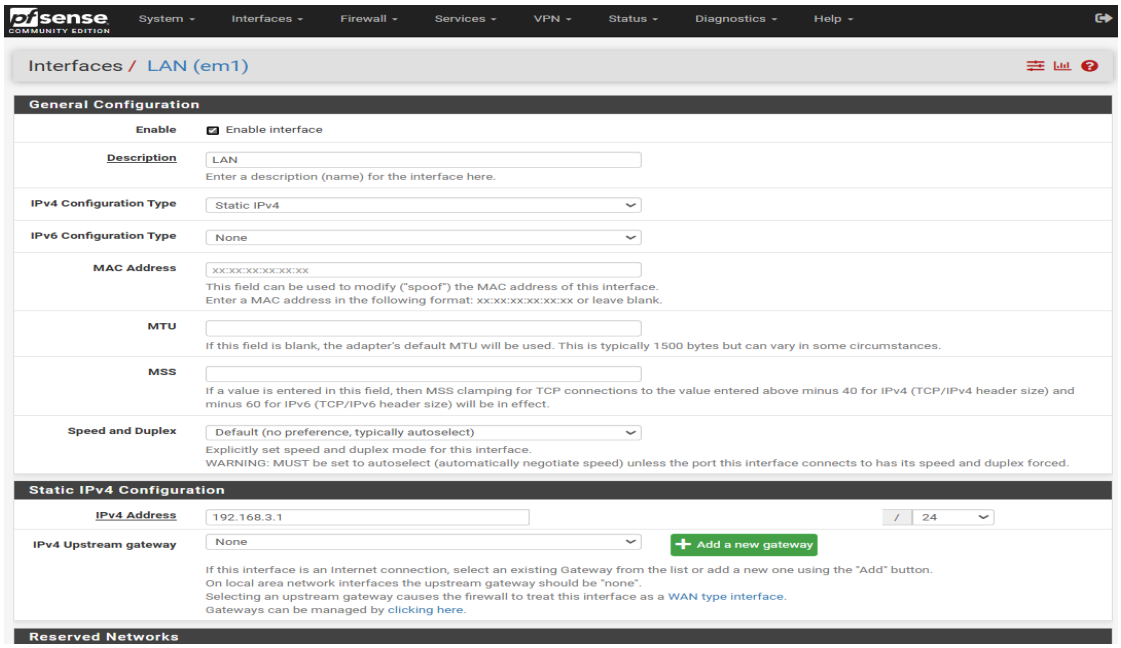



**Figure IV.38 :** Configuration de l'interface LAN (Site Alger)

### IV.7.2 Filtrage sur Pare-feu

#### IV.7.2.1 Création des ACL's sur le site Bejaia

En premier lieu on clique sur firewall ensuite RULES et on aura nos 4 interfaces.

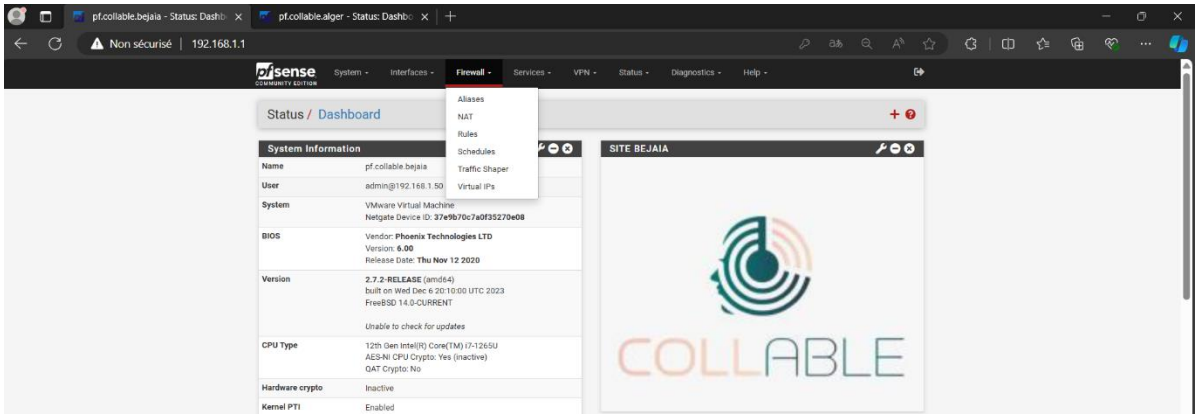



**Figure IV.39 :** Configuration ACL.

- **Pour l'interface WAN**

On a décrit une règle qui permet tout le trafic ICMP entrant sur l'interface WAN provenant de n'importe quelle source et destiné à l'adresse IP de l'interface WAN du pare-feu.

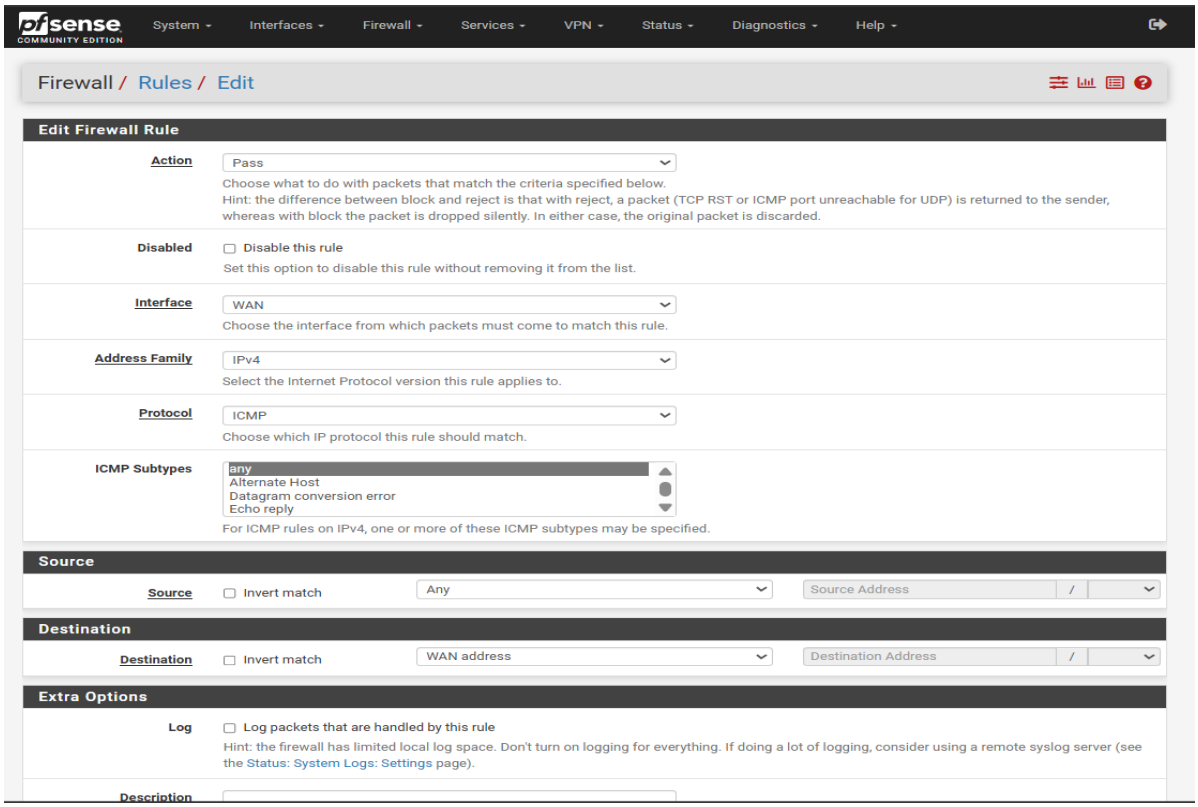
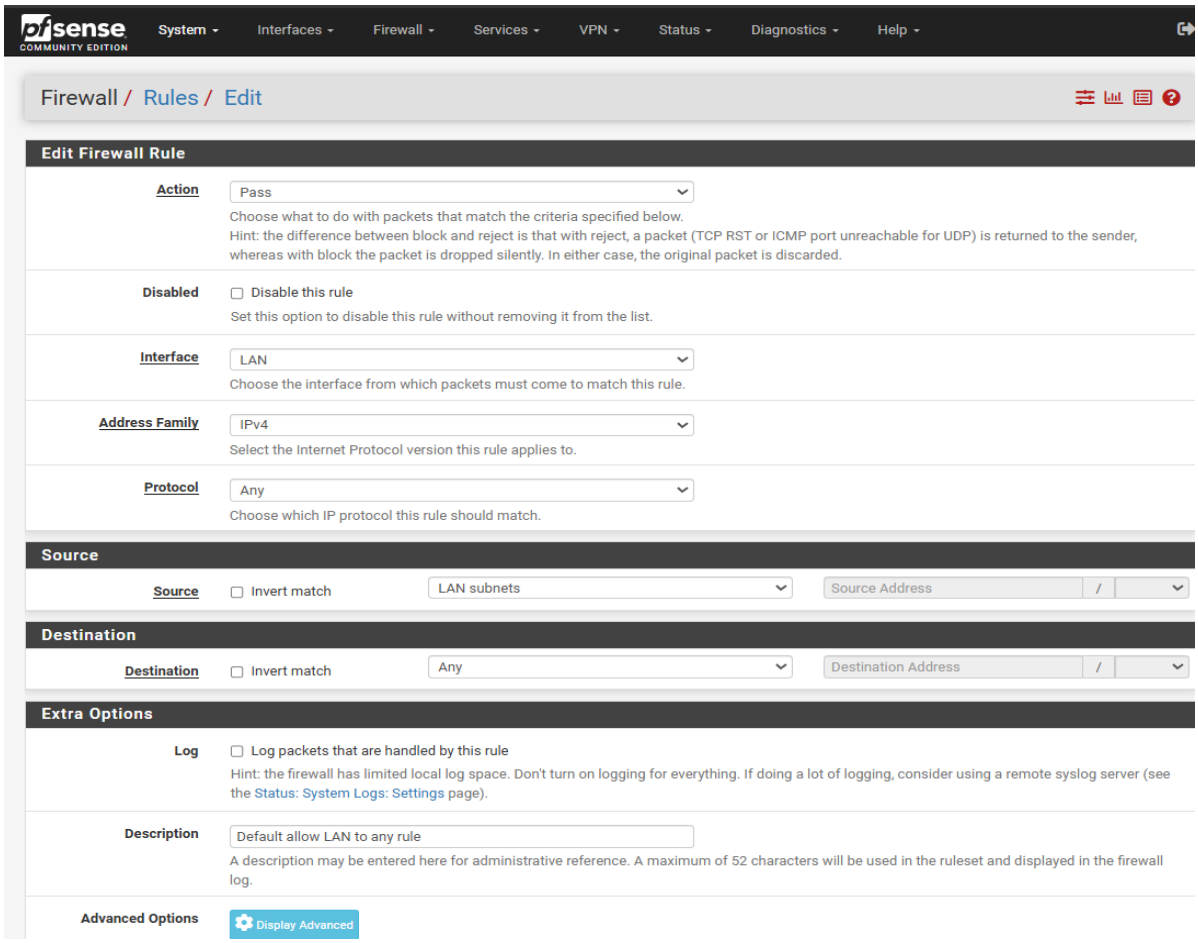



**Figure IV.40 :** Configuration d'une ACL sur l'interface WAN (Site Bejaia).

- **Pour l'interface LAN**

Sur cette interface on a d'abord configuré la règle anti-lockout qui est conçue pour garantir que l'administrateur réseau ne perd pas l'accès à l'interface de gestion du pare-feu.

Ensuite on a décrit une règle qui permet tout le trafic entrant sur l'interface LAN, sans restriction sur le protocole ou la destination, mais limitée aux sous-réseaux locaux en tant que source.



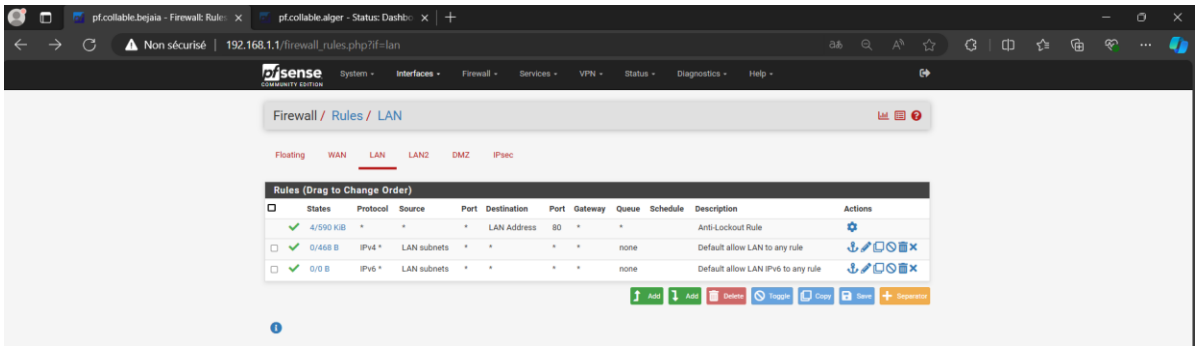




**Figure IV. 41 :** Configuration des ACL's sur l'interface LAN (Site Bejaia).

- **Pour l'interface LAN2**

On a décrit une règle qui permet tout le trafic IPv4 entrant et sortant sans aucune restriction, cela signifie que tous les protocoles et toutes les adresses source et destination sont autorisés.

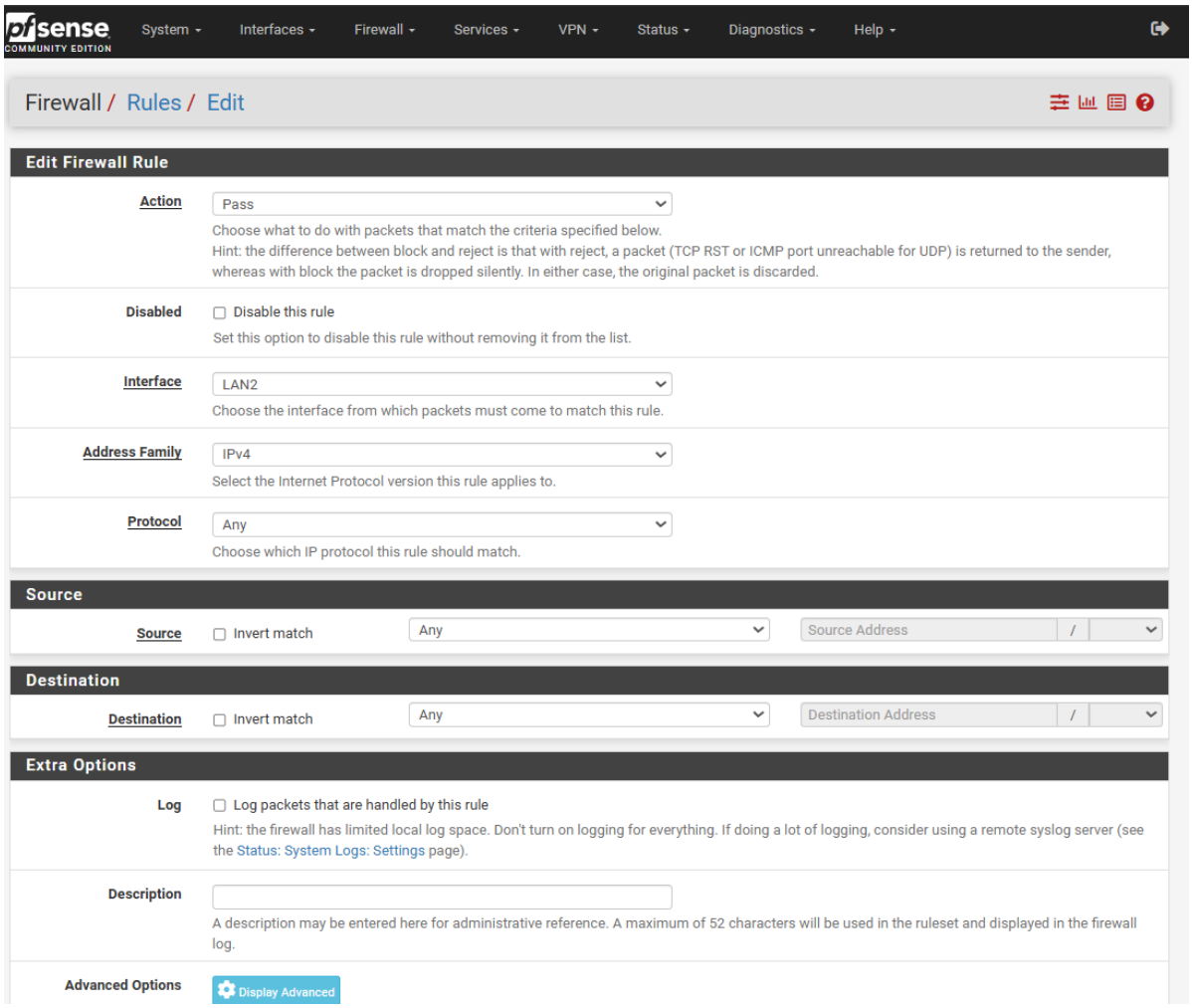



**Figure IV.42 :** Configuration d'une ACL sur l'interface LAN 2 (Site Bejaia).

- **Pour l'interface DMZ**

On a permis tout le trafic provenant des sous réseaux de la DMZ à destination de n'importe quelle adresse IP.

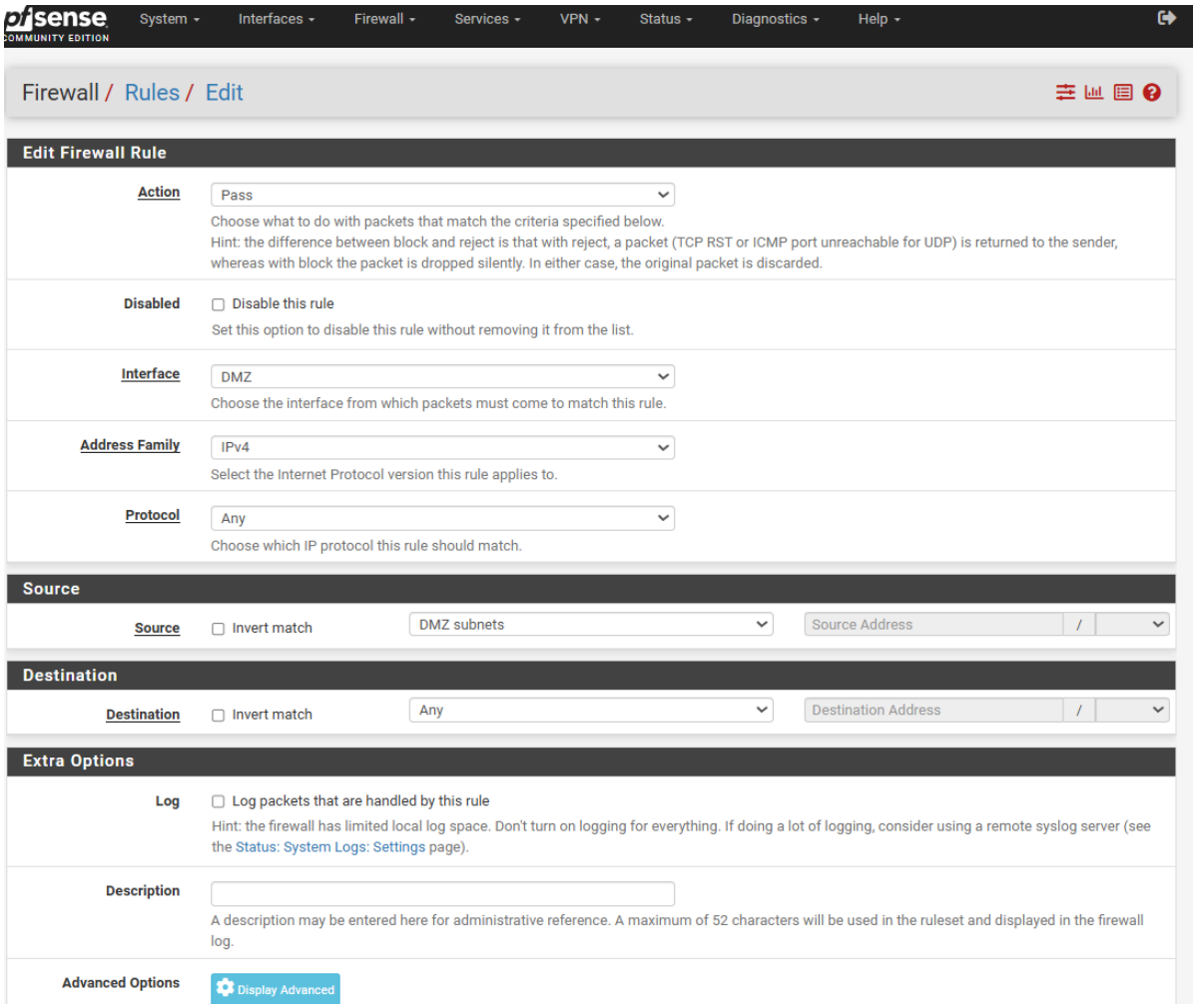



**Figure IV.43 :** Configuration d'une ACL sur l'interface DMZ (Site Bejaia).

### IV.7.2.2 Création des ACL's sur le site d'ALGER

- **Sur l'interface WAN**

On a décrit une règle qui permet à tout le trafic ICMP d'entrer sur l'interface WAN, incluant tous les sous-types ICMP et autorise le trafic provenant de n'importe quelle source vers l'adresse IP de l'interface WAN.

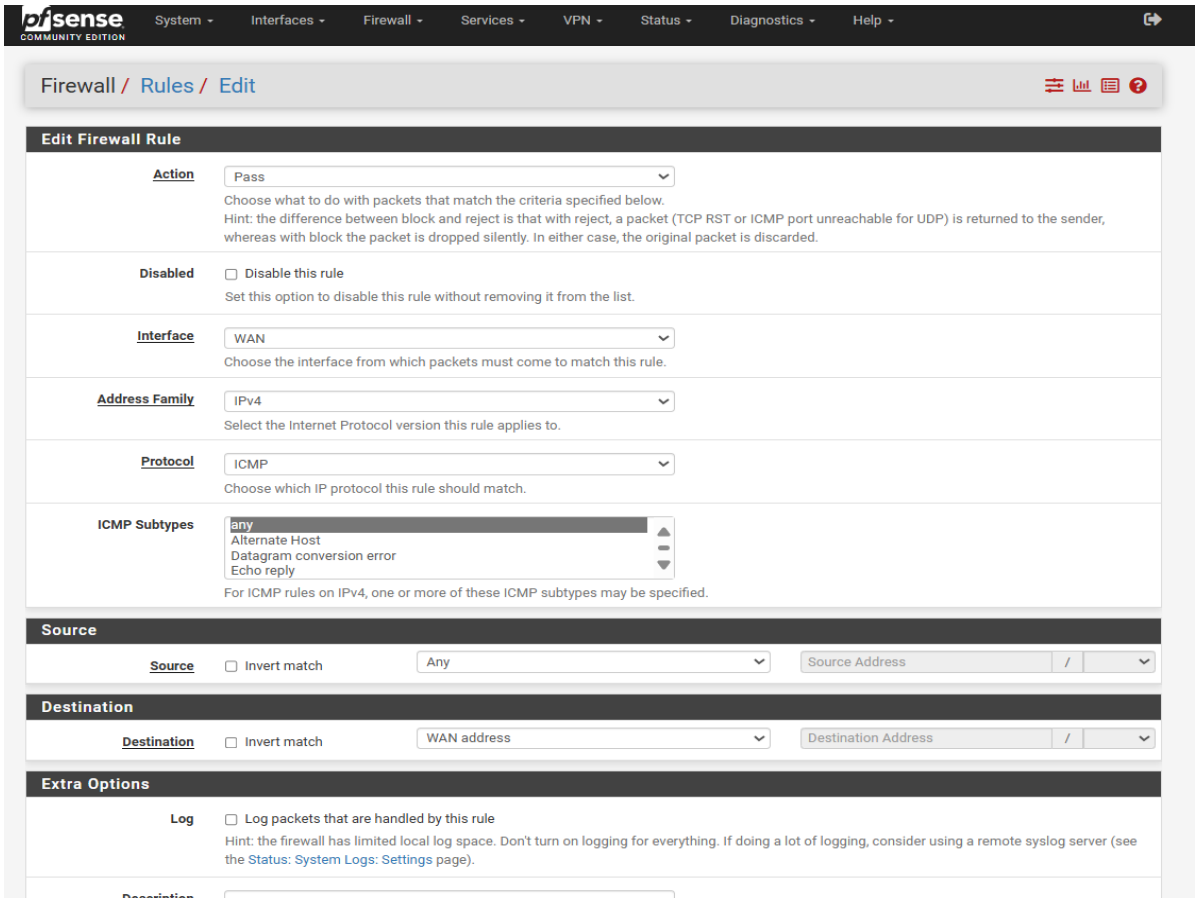



**Figure IV.44 :** Configuration d'une ACL sur l'interface WAN (Site Alger).

- **Sur l'interface LAN**

Sur cette interface on a d'abord configuré la règle anti-lockout qui est conçue pour garantir que l'administrateur réseau ne perd pas l'accès à l'interface de gestion du pare-feu

Ensuite on a décrit une règle qui permet tout le trafic entrant sur l'interface LAN, sans restriction sur le protocole ou la destination, mais limitée aux sous-réseaux locaux en tant que source

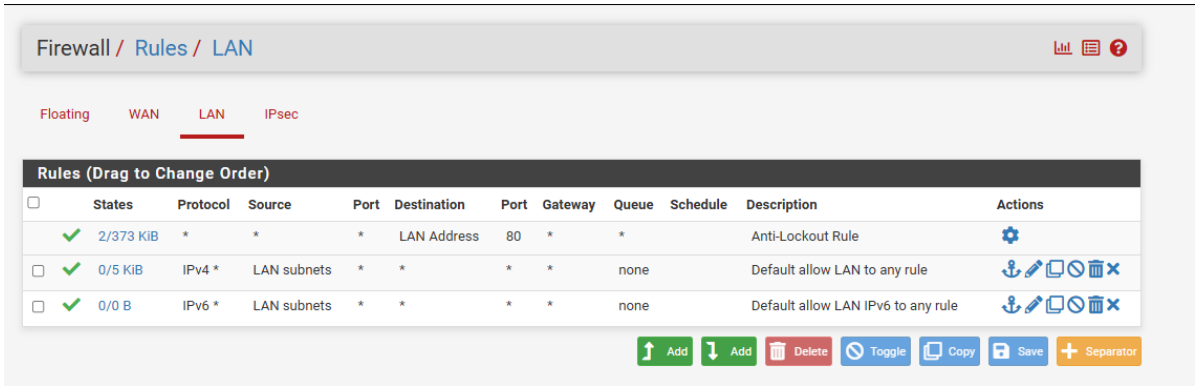



**Figure IV.45 :** Configuration des ACL's sur l'interface LAN (Site Alger)

### IV.7.3 Configuration des passerelles sur les pares-feux

#### IV.7.3.1 Sur le pare-feu ALGER

On a configuré une passerelle qui relie le réseau LAN à internet.

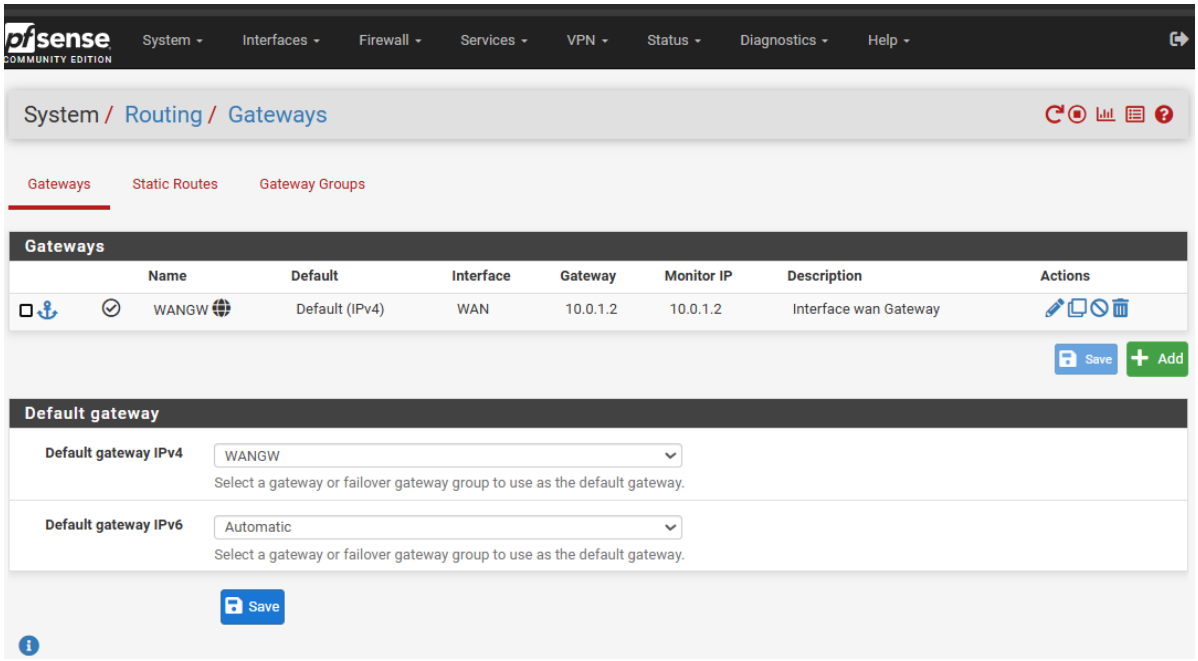



**Figure IV.46 :** Configuration de la passerelle sur le pare-feu Alger.

#### IV.7.3.2 Sur le pare-feu BEJAIA

On a configuré deux passerelles, une qui relie le réseau LAN à internet, et une deuxième pour l'interface LAN.

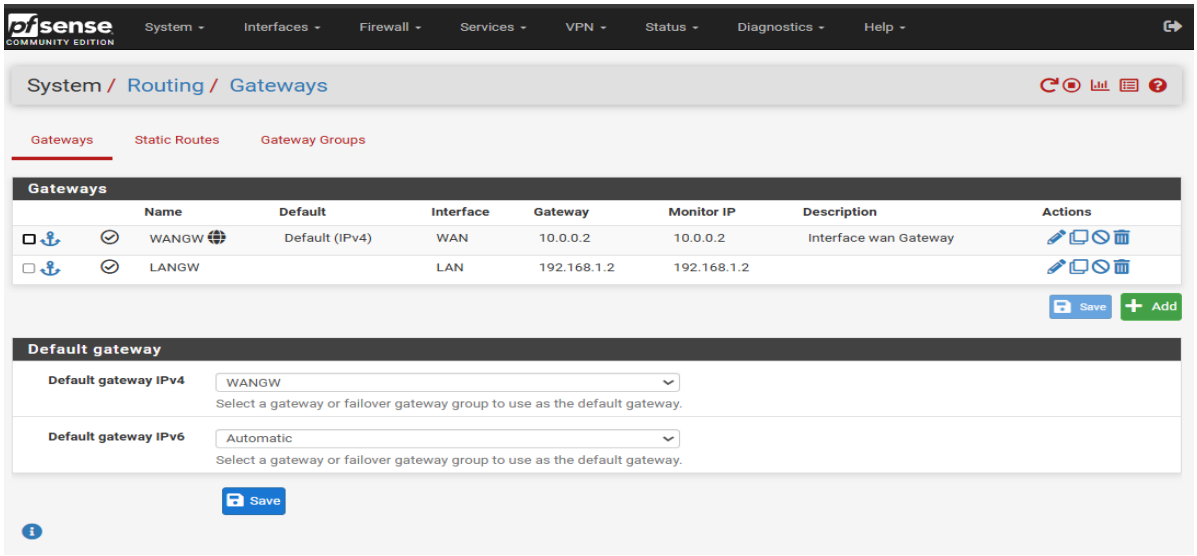



**Figure IV.47 :** Configuration de la passerelle sur le pare-feu Bejaia.

- **Routage statique**

Le routage statique est une méthode où l'administrateur réseau configure manuellement les chemins de données, offrant un contrôle précis des itinéraires.

Dans ce cas, tout le trafic entrant provenant de l'extérieur sera routé pour bénéficier d'une connexion internet, puis identifié lors de la création de notre tunnel VPN site à site.

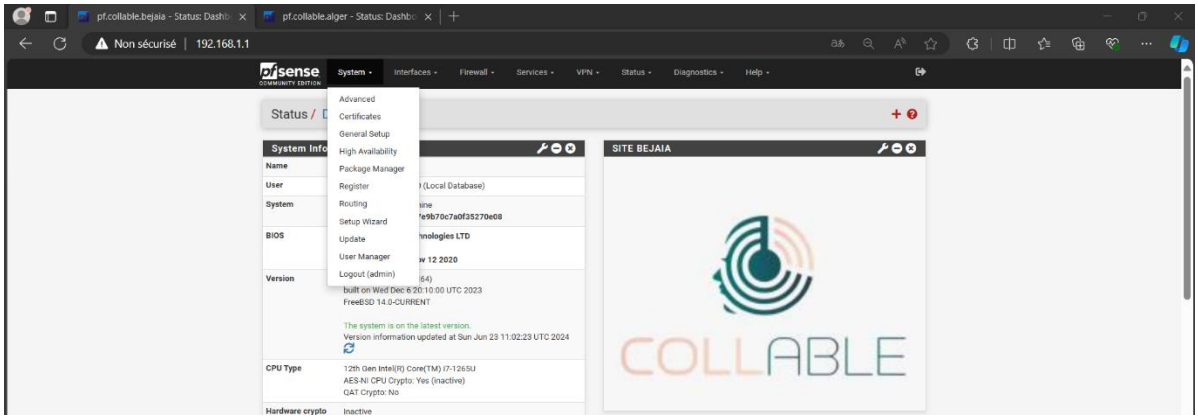



**Figure IV.48 :** Routage statique (Site Bejaia).

On a créé une route statique de réseau LAN vers VLAN50 avec une passerelle 192.168.1.2.

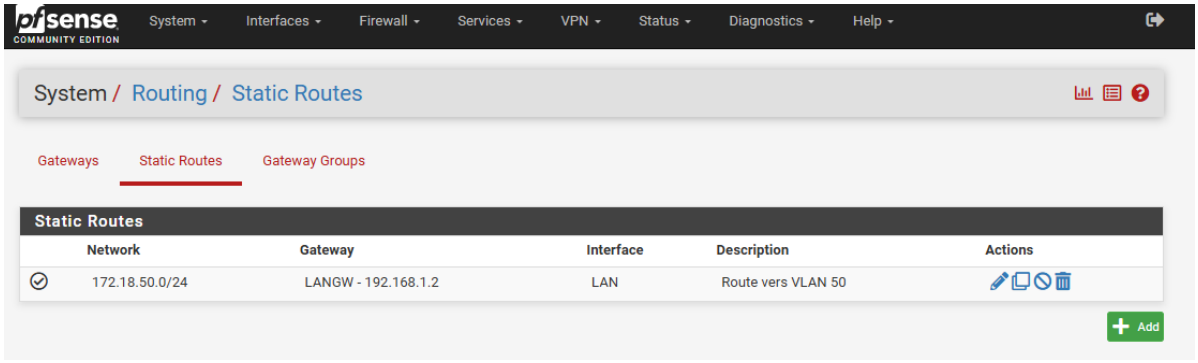



**Figure IV.49 :** Routage statique vers vlan50 (Site Bejaia).

- **VPN**

Un VPN IPsec site-à-site est une connexion sécurisée entre deux réseaux distincts via Internet, utilisant le protocole IPsec pour chiffrer et authentifier les données échangées. Il permet aux ressources des deux réseaux de communiquer comme s'ils étaient sur le même réseau local, malgré la distance physique.

### IV.7.4 Configuration du VPN site à site IPSec

Tout d'abord pour accéder aux paramètres de VPN on suit les étapes suivantes :

On clique sur VPN puis IPSec.

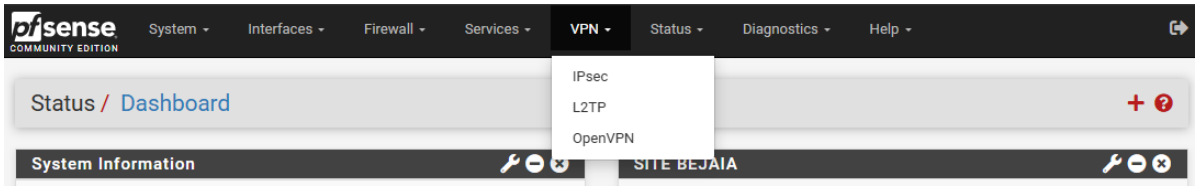



**Figure IV.50 :** Accéder aux paramètres de VPN IPsec.

- **Sur le site de Bejaia**

On va créerun tunnel sur le pare-feu vers le pare-feu d'Alger qu'on va nommer Connexion IPSEC BEJAIA ----> ALGER, on va configurer les informations requises comme le nom de la passerelle, son type, la clé partagée sur le tunnel et ce qui suit.

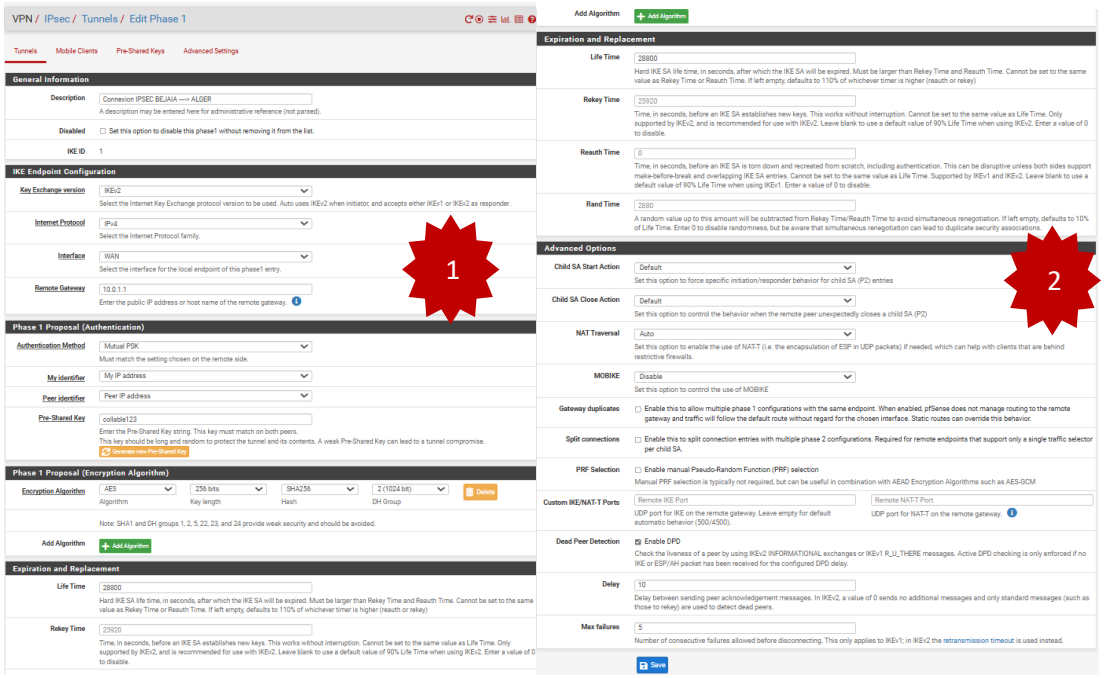



**Figure IV.51 :** Configuration IPSEC BEJAIA ----> ALGER.

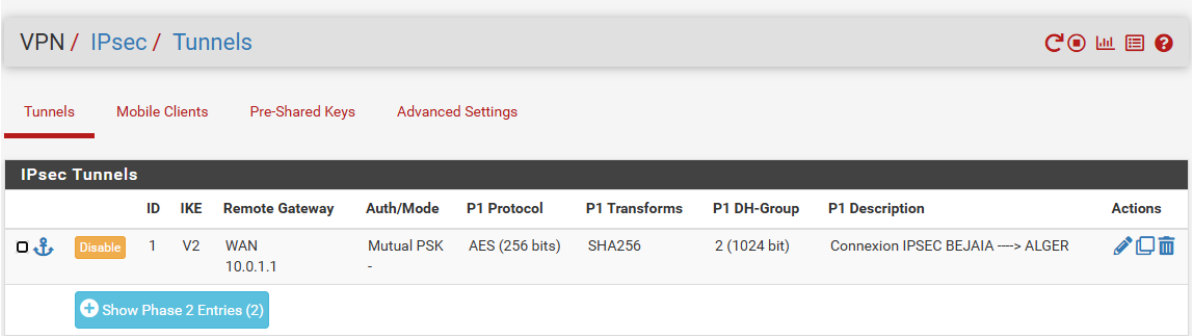



**Figure IV.52** : IPSEC tunnel BEJAIA ----> ALGER.

**Explication du tunnel IPSec**

1. **ID** : Un identifiant unique pour la connexion IPsec. Ici, c'est "1".
2. **IKE** : Indique la version du protocole Internet Key Exchange utilisée. "V2" signifie que IKEv2 est utilisé.
3. **Passerelle distante** : L'adresse IP de la passerelle distante. Ici, c'est "10.0.1.1".
4. **Authentification/Mode** : La méthode d'authentification et le mode utilisés pour établir la connexion. "PSK Mutuel" signifie que les deux extrémités de la connexion utilisent une clé pré-partagée pour l'authentification.
5. **Protocole P1** : Le protocole utilisé en Phase 1. Non explicitement listé ici, mais généralement c'est IKE.
6. **Transformations P1** : Les algorithmes de chiffrement et de hachage utilisés en Phase 1. Ici, "AES (256 bits)" est l'algorithme de chiffrement et "SHA256" est l'algorithme de hachage.
7. **Groupe DH P1** : Le groupe Diffie-Hellman utilisé en Phase 1. "2 (1024 bits)" indique l'utilisation du Groupe 2, qui est un groupe de 1024 bits.
8. **Description P1** : Une description de la configuration de la Phase 1. "Connexion IPSEC BEJAIA ----> ALGER" décrit le but ou les points de terminaison de la connexion, suggérant une connexion de Bejaia à Alger.

- **Sur le site d'Alger**

On va suivre les mêmes étapes et les mêmes configurations en changeant la passerelle 10.0.0.1

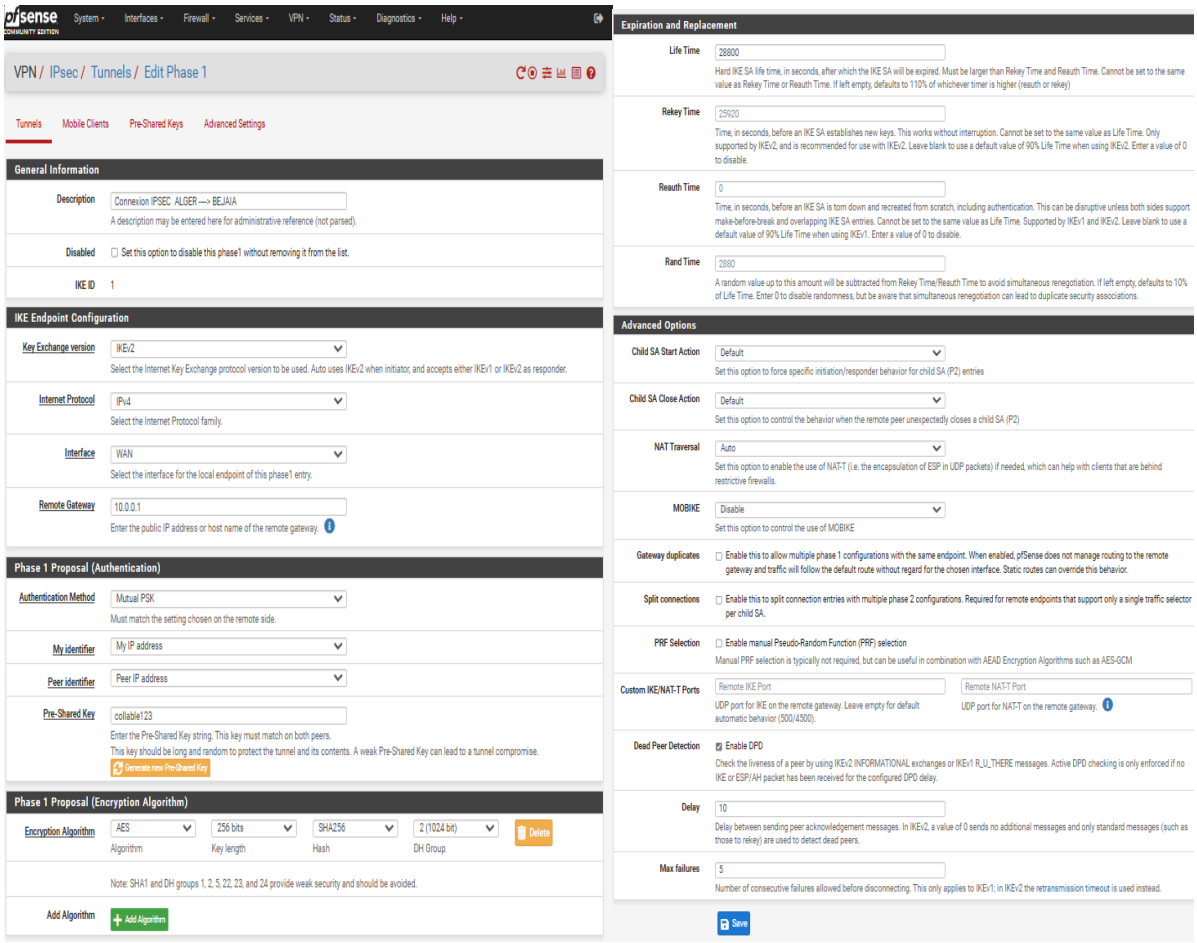



**Figure IV.53** : Configuration IPSEC ALGER ----> BEJAIA

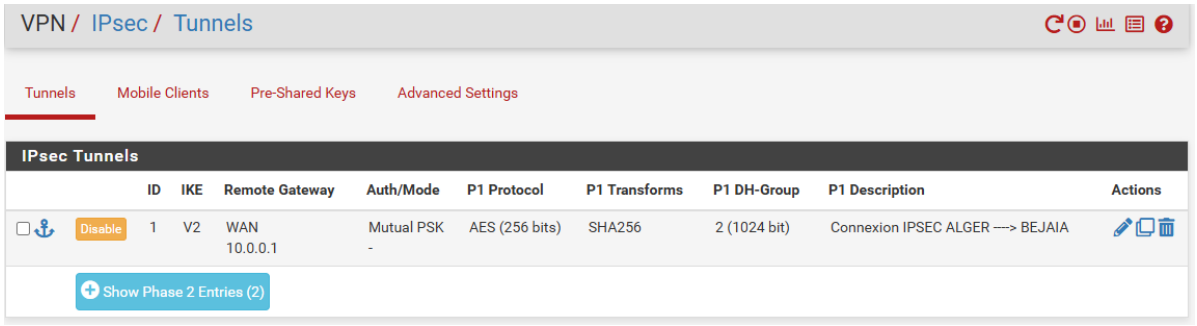



**Figure IV.54** : IPSEC tunnel ALGER ----> BEJAIA.

### Explication de l'IPsec tunnel

1. **ID** : Un identifiant unique pour la connexion IPsec. Ici, c'est "1".
2. **IKE** : Indique la version du protocole Internet Key Exchange utilisée. "V2" signifie que IKEv2 est utilisé.
3. **Passerelle distante** : L'adresse IP de la passerelle distante. Ici, c'est "10.0.0.1".

4. **Authentification/Mode** : La méthode d'authentification et le mode utilisés pour établir la connexion. "PSK Mutuel" signifie que les deux extrémités de la connexion utilisent une clé pré-partagée pour l'authentification.
5. **Protocole P1** : Le protocole utilisé en Phase 1. Non explicitement listé ici, mais généralement c'est IKE.
6. **Transformations P1** : Les algorithmes de chiffrement et de hachage utilisés en Phase 1. Ici, "AES (256 bits)" est l'algorithme de chiffrement et "SHA256" est l'algorithme de hachage.
7. **Groupe DH P1** : Le groupe Diffie-Hellman utilisé en Phase 1. "2 (1024 bits)" indique l'utilisation du Groupe 2, qui est un groupe de 1024 bits.
8. **Description P1** : Une description de la configuration de la Phase 1. "Connexion IPSEC ALGER ----> BEJAIA" décrit le but ou les points de terminaison de la connexion, suggérant une connexion d'Alger à Bejaia.

- **Sur le site de Bejaia**

On met en place 2 connexion VPN IP sec vers le réseau situé à Alger en provenance du réseau DMZ et le sous-réseau 172.18.50.0/24 (Bejaia).

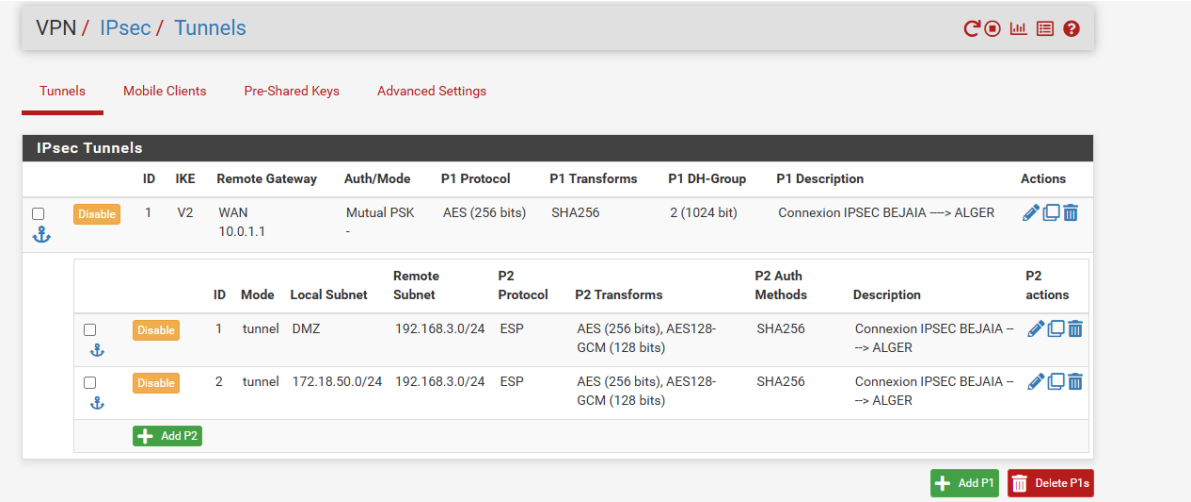



**Figure IV.55 :** Mise en place de deux connexions IPSEC tunnel BEJAIA ----> ALGER.

- **Explication de la connexion DMZ vers le réseau situé à Alger**

1. **ID** : Un identifiant unique pour la connexion IPsec Phase 2. Ici, c'est "1".
2. **Mode** : Le mode de la connexion. Ici, c'est "tunnel".

3. **Sous-réseau Local** : Le sous-réseau local protégé par cette connexion. Ici, c'est "DMZ", représentant la zone démilitarisée.
4. **Sous-réseau Distant** : Le sous-réseau distant protégé par cette connexion. Ici, c'est "192.168.3.0/24".
5. **Protocole P2** : Le protocole utilisé en Phase 2. Ici, "ESP" (Encapsulating Security Payload) est utilisée.
6. **Transformations P2** : Les algorithmes de chiffrement utilisés en Phase 2. Ici, "AES (256 bits)" et "AES128-GCM (128 bits)".
7. **Méthodes d'authentification P2** : Les algorithmes de hachage utilisés en Phase 2. Ici, c'est "SHA256".
8. **Description P2** : Une description de la configuration de la Phase 2. "Connexion IPSEC BEJAIA ----> ALGER" décrit le but ou les points de terminaison de la connexion, suggérant une connexion de Bejaia à Alger.

**Remarque :** pour la connexion IPsec sur tunnel entre le réseau 172.18.50.0 /24 et le réseau situé à Alger c'est la même explication que la DMZ sauf que le sous réseau local va devenir 172.18.50.0 mais le réseau local reste le même

- **Sur le site d'Alger**

On à configurer 2 connexions IPsec Alger →Bejaia, similaire à celle configurer sur le site de Bejaia sauf que cette fois le réseau local c'est le réseau d'Alger 192.168.3.0 /24 pour les 2 connexions, les sites distants sont le réseau DMZ 10.0.2.0/24 (Bejaia) et le réseau 172.18.50.0/24 (Bejaia).

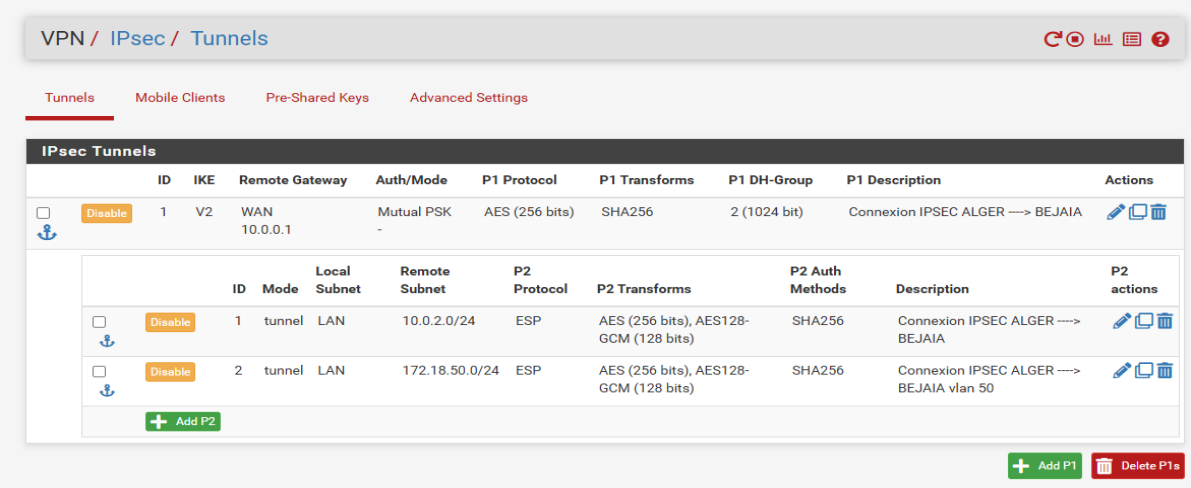



**Figure IV.56 :** Mise en place de deux connexions IPSEC tunnel ALGER ----> BEJAIA.

### Création d'une ACL sur les deux pares-feux

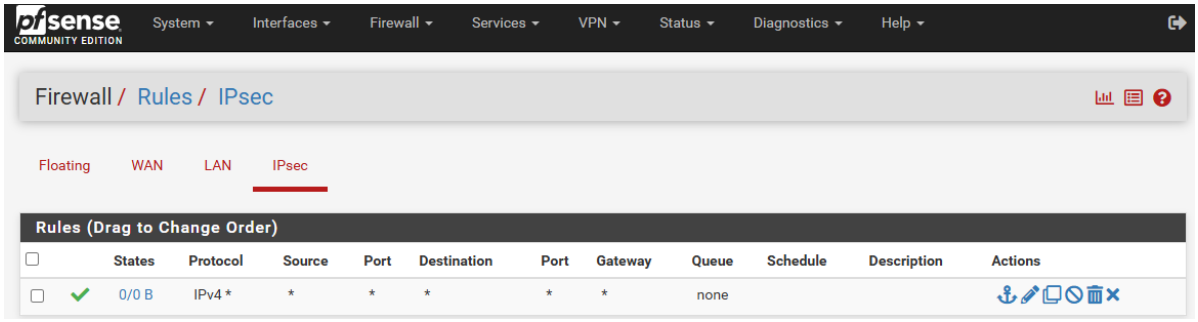



**Figure IV.57 :** ACL IPsec (ALGER).

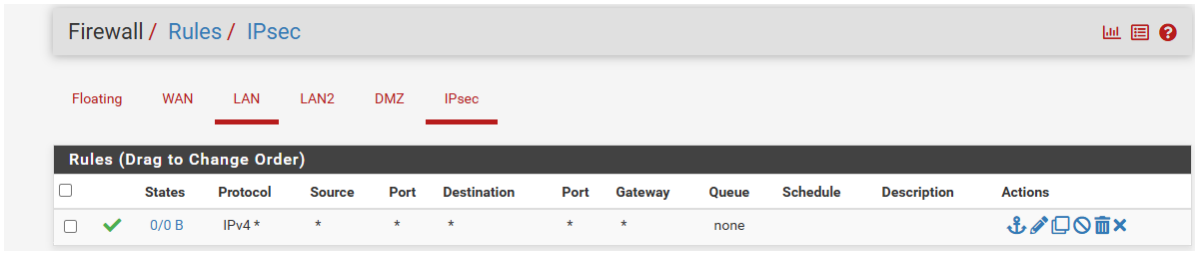



**Figure IV.58** : ACL IPsec (BEJAIA).

**Explication :**

Cette règle autorise tout le trafic IPv4 à travers le pare-feu sans filtrage spécifique basé sur la source, la destination, les ports, ou d'autres critères.

Elle est utilisée pour permettre le trafic IPsec de passer à travers le pare-feu sans restriction, bien que les détails spécifiques de la configuration soient faits lors de la configuration des tunnels.

## IV.8 Tests

Nous allons finaliser notre travail par des tests aux configurations déjà faites et qui sont présentées dans la partie configuration pour s'assurer que le réseau est bien sécurisé.

### IV.8.1 Test DHCP

```
PC1> ip dhcp
DORA IP 172.18.50.11/24 GW 172.18.50.254

PC1>
```

**Figure IV.59 :** Test DHCP.

### IV.8.2 Ping PC1 vers la passerelle et PC2

```
PC1> ping 172.18.50.1

84 bytes from 172.18.50.1 icmp_seq=1 ttl=255 time=1.680 ms
84 bytes from 172.18.50.1 icmp_seq=2 ttl=255 time=1.791 ms
84 bytes from 172.18.50.1 icmp_seq=3 ttl=255 time=1.565 ms
84 bytes from 172.18.50.1 icmp_seq=4 ttl=255 time=2.216 ms

84 bytes from 172.18.50.1 icmp_seq=5 ttl=255 time=2.563 ms

PC1>
PC1> ping 172.18.20.11

84 bytes from 172.18.20.11 icmp_seq=1 ttl=63 time=5.827 ms
84 bytes from 172.18.20.11 icmp_seq=2 ttl=63 time=3.031 ms
84 bytes from 172.18.20.11 icmp_seq=3 ttl=63 time=3.390 ms
84 bytes from 172.18.20.11 icmp_seq=4 ttl=63 time=4.939 ms
84 bytes from 172.18.20.11 icmp_seq=5 ttl=63 time=3.727 ms
```

**Figure IV.60 :** Ping PC1 vers la passerelle et PC2.

### IV.8.3 Ping PC1 vers les interfaces du R1.

```
PC1> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=63 time=2.790 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=63 time=3.572 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=63 time=3.110 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=63 time=3.066 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=63 time=4.319 ms

PC1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=255 time=1.973 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=255 time=2.014 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=255 time=1.346 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=255 time=1.575 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=255 time=2.284 ms
```

**Figure IV.61 :** Ping PC1 vers les interfaces du R1.

### IV.8.4 Ping PC1 vers internet

```
PC1> ping 1.1.1.1

84 bytes from 1.1.1.1 icmp_seq=1 ttl=124 time=91.101 ms
84 bytes from 1.1.1.1 icmp_seq=2 ttl=124 time=241.528 ms
84 bytes from 1.1.1.1 icmp_seq=3 ttl=124 time=51.800 ms
84 bytes from 1.1.1.1 icmp_seq=4 ttl=124 time=85.503 ms
84 bytes from 1.1.1.1 icmp_seq=5 ttl=124 time=150.516 ms
```

**Figure IV.62 :** Ping PC1 vers internet.

### IV.8.5 Ping PC7 vers PC1

```
PC7> ping 172.18.50.11

84 bytes from 172.18.50.11 icmp_seq=1 ttl=61 time=37.917 ms
84 bytes from 172.18.50.11 icmp_seq=2 ttl=61 time=22.725 ms
84 bytes from 172.18.50.11 icmp_seq=3 ttl=61 time=20.986 ms
84 bytes from 172.18.50.11 icmp_seq=4 ttl=61 time=21.950 ms
84 bytes from 172.18.50.11 icmp_seq=5 ttl=61 time=22.731 ms
```

**Figure IV.63 :** ping PC7 vers PC1.

### IV.8.6 Ping PC7 vers ISP

```
PC7> ping 10.0.1.1

84 bytes from 10.0.1.1 icmp_seq=1 ttl=64 time=4.962 ms
84 bytes from 10.0.1.1 icmp_seq=2 ttl=64 time=4.296 ms
84 bytes from 10.0.1.1 icmp_seq=3 ttl=64 time=4.220 ms
84 bytes from 10.0.1.1 icmp_seq=4 ttl=64 time=4.312 ms
84 bytes from 10.0.1.1 icmp_seq=5 ttl=64 time=3.671 ms

PC7> ping 10.0.1.2

84 bytes from 10.0.1.2 icmp_seq=1 ttl=254 time=12.223 ms
84 bytes from 10.0.1.2 icmp_seq=2 ttl=254 time=8.710 ms
84 bytes from 10.0.1.2 icmp_seq=3 ttl=254 time=10.001 ms
84 bytes from 10.0.1.2 icmp_seq=4 ttl=254 time=15.034 ms
84 bytes from 10.0.1.2 icmp_seq=5 ttl=254 time=13.670 ms
```

**Figure IV. 64 :** Ping PC7 vers ISP.

### IV.8.7 Ping PC7 vers Internet

```
PC7> ping 1.1.1.1

84 bytes from 1.1.1.1 icmp_seq=1 ttl=125 time=98.321 ms
84 bytes from 1.1.1.1 icmp_seq=2 ttl=125 time=78.215 ms
84 bytes from 1.1.1.1 icmp_seq=3 ttl=125 time=92.552 ms
84 bytes from 1.1.1.1 icmp_seq=4 ttl=125 time=113.047 ms
```

**Figure IV. 65:** Ping PC7 vers Internet.

### IV.8.8 Ping serv1 vers la passerelle et serv2

```
SER1> ping 10.0.2.1

84 bytes from 10.0.2.1 icmp_seq=1 ttl=64 time=3.208 ms
84 bytes from 10.0.2.1 icmp_seq=2 ttl=64 time=3.951 ms
84 bytes from 10.0.2.1 icmp_seq=3 ttl=64 time=2.317 ms
84 bytes from 10.0.2.1 icmp_seq=4 ttl=64 time=2.538 ms
84 bytes from 10.0.2.1 icmp_seq=5 ttl=64 time=3.021 ms

SER1> ping 10.0.2.5

84 bytes from 10.0.2.5 icmp_seq=1 ttl=64 time=3.318 ms
84 bytes from 10.0.2.5 icmp_seq=2 ttl=64 time=1.582 ms
84 bytes from 10.0.2.5 icmp_seq=3 ttl=64 time=1.612 ms
84 bytes from 10.0.2.5 icmp_seq=4 ttl=64 time=2.811 ms
84 bytes from 10.0.2.5 icmp_seq=5 ttl=64 time=1.211 ms
```

**Figure IV.66 :** Ping serv1 vers serv2 et la passerelle.

### IV.8.9 Ping serv1 vers PC7

```
SER1>
SER1> ping 192.168.3.1

84 bytes from 192.168.3.1 icmp_seq=1 ttl=63 time=27.042 ms
84 bytes from 192.168.3.1 icmp_seq=2 ttl=63 time=47.949 ms
84 bytes from 192.168.3.1 icmp_seq=3 ttl=63 time=21.241 ms
84 bytes from 192.168.3.1 icmp_seq=4 ttl=63 time=70.012 ms
84 bytes from 192.168.3.1 icmp_seq=5 ttl=63 time=13.580 ms

SER1> ping 192.168.3.10

84 bytes from 192.168.3.10 icmp_seq=1 ttl=62 time=29.071 ms
84 bytes from 192.168.3.10 icmp_seq=2 ttl=62 time=14.609 ms
84 bytes from 192.168.3.10 icmp_seq=3 ttl=62 time=14.399 ms
84 bytes from 192.168.3.10 icmp_seq=4 ttl=62 time=13.714 ms
```

**Figure IV.67 :** Ping serv1 vers PC7.

### IV.8.10 Ping pare-feu Bejaia vers Internet

```
[2.7.2-RELEASE][root@pf.collable.bejaia]/root: ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: icmp_seq=0 ttl=126 time=82.434 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=126 time=144.736 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=126 time=109.975 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=126 time=59.321 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=126 time=63.468 ms
^C
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 59.321/91.987/144.736/31.867 ms
[2.7.2-RELEASE][root@pf.collable.bejaia]/root:
```

**Figure IV.68 :** Ping pare-feu Bejaia vers Internet.

### IV.8.11 Ping pare-feu Alger vers Internet

```
[2.7.2-RELEASE][root@pf.collable.alger]/root: ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: icmp_seq=0 ttl=126 time=72.452 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=126 time=31.003 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=126 time=53.666 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=126 time=33.450 ms
c64 bytes from 1.1.1.1: icmp_seq=4 ttl=126 time=54.818 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=126 time=32.108 ms
^C
--- 1.1.1.1 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 31.003/46.250/72.452/15.337 ms
[2.7.2-RELEASE][root@pf.collable.alger]/root:
```

**Figure IV.69 :** Ping pare-feu Alger vers Internet.

## IV.9 Vérification du tunnel VPN

La négociation dans le tunnel VPN, ça se passe bien donc il est bien réussi. Et elle se fait en deux phases :

**Phase 1 :** Dans cette phase, on fait les échanges des clés sécurisées avec IKE afin que les utilisateurs puissent négocier dans le tunnel secrètement et c'est la deuxième phase.

**Phase 2 :** C'est là où on fait la négociation avec le protocole suivant :
- **Le protocole ESP** (Encapsulating Security Payload) Fournit des services d'authentifications optionnels pour garantir l'intégrité des paquets protégés.

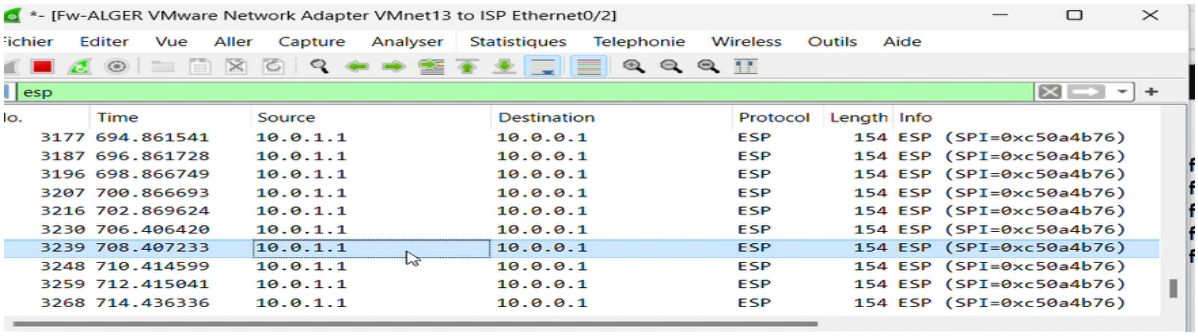



**Figure IV.70 :** Capture WireShark qui montre la négociation ESP du tunnel vpn.

- **Explication de Wireshark**

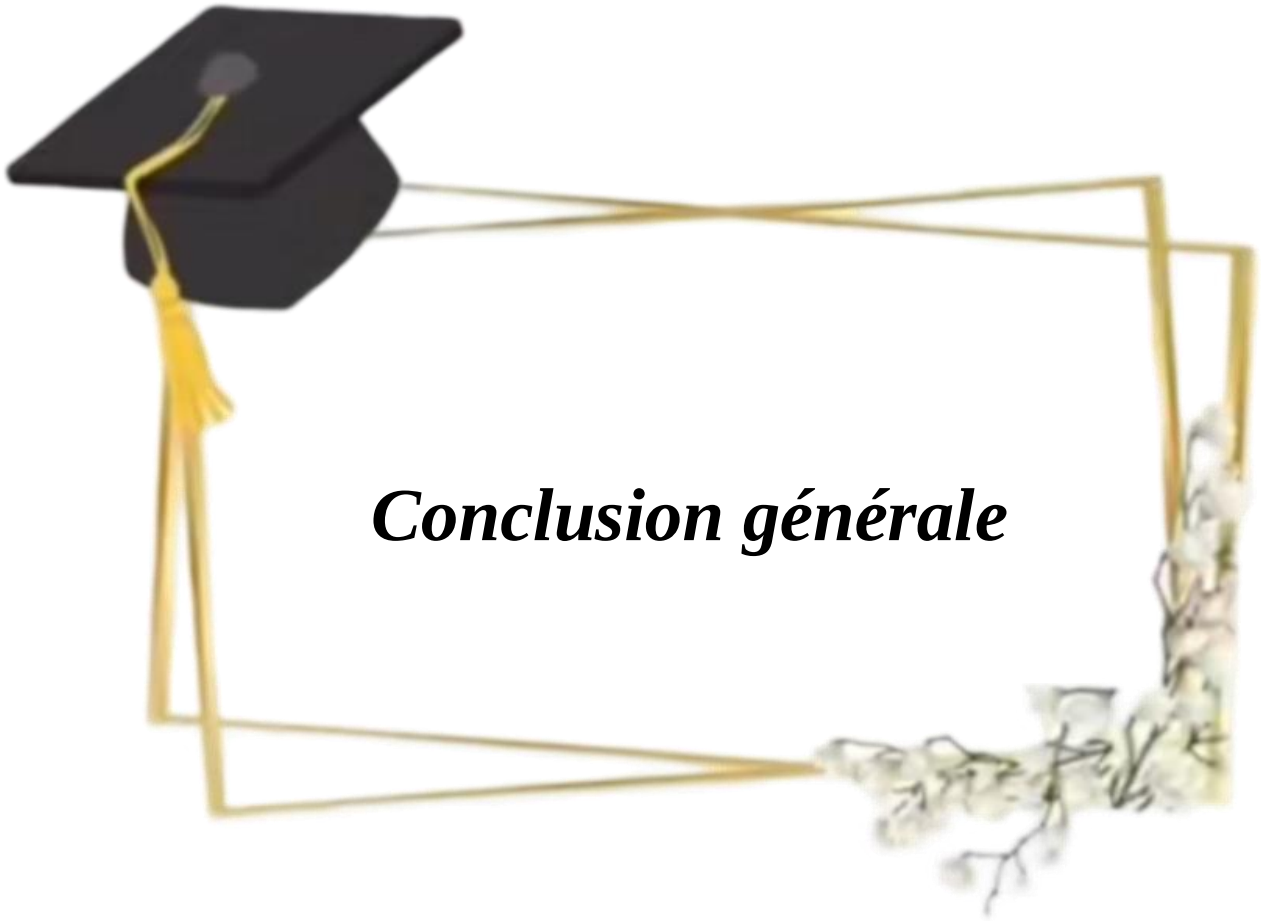
Le screenshot semble montrer un outil de surveillance réseau, probablement Wireshark, qui analyse des paquets sur un réseau. Voici une explication des colonnes clés : 1. **No.**: Numéro du paquet dans le fichier de capture. 2. **Time**: Horodatage montrant quand chaque paquet a été capturé. 3. **Source**: Adresse IP de l'expéditeur du paquet. 4. **Destination**: Adresse IP du destinataire du paquet. 5. **Protocol**: Le protocole utilisé dans le paquet, dans ce cas, ESP (Encapsulating Security Payload). 6. **Length**: Taille du paquet en octets. 7. **Info**: Informations supplémentaires sur le paquet, y compris l'Index des Paramètres de Sécurité (SPI) qui aide à identifier l'association de sécurité pour le paquet. ESP (Encapsulating Security Payload) fait partie de la suite de protocoles IPsec, utilisée pour fournir la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données. Les paquets répertoriés utilisent tous le même SPI (0xc50a4b76), ce qui indique qu'ils appartiennent à la même association de sécurité IPsec. Dans ce contexte, tous les paquets voyagent entre les mêmes adresses source (10.0.1.1) et destination (10.0.0.1) en utilisant le protocole ESP, ce qui suggère une communication chiffrée entre ces deux adresses IP.

## IV.10 Conclusion

Au terme de ce chapitre, nous pouvons affirmer que les objectifs fixés ont été atteints avec succès.

Notre étude sur l’optimisation de la sécurité d’un réseau à multicouche a permis de mettre en place les solutions proposées qui sont composé de différents protocoles et équipements.

Ces solutions ont non seulement renforcé la sécurité de l’infrastructure réseau, mais ont également amélioré sa performance et sa résilience. Le client de l’entreprise NTS bénéficie désormais d’un réseau plus robuste, mieux protégé contre les attaques et les pannes, offrant une plus grande stabilité et une meilleure gestion des ressources.



# *Conclusion générale*

## Conclusion générale

La sécurité d'un réseau se définit comme un ensemble de mesures destinées à protéger l'intégrité, la confidentialité et la disponibilité des données transitant par les réseaux. Pour cela nous avons était mis au défi d'optimiser la sécurité du réseau client de NTS après avoir identifié les problèmes de sécurité auxquelles il est confronté.

Pour mettre en place notre solution, on a utilisé un logiciel de simulation de réseaux informatiques GNS3 et un outil de virtualisation qui est VMware. Cette solution se base sur l'implémentation de nombreux protocoles et outils indispensable pour renforcer la sécurité. Les implémentations pratiques ont été documentées, démontrant comment les théories et les solutions ont été appliquées dans l'environnement.

Après la mise en place de nos solutions, on a présenté les résultats obtenus suite à ces optimisations, montrant une amélioration significative de la sécurité globale du réseau contre les menaces et les attaques, tout en assurant la continuité et l'efficacité des opérations.

En conclusion, ce mémoire a permis d'optimiser de manière significative la sécurité du réseau multicouche du client de NTS, fournissant une base solide pour des améliorations continues et une meilleure protection contre les menaces informatiques. Les découvertes réalisées soulignent l'importance d'une approche proactive et intégrée en matière de sécurité réseau, et offrent des perspectives prometteuses pour de futures recherches et applications pratiques.

# Annexe A

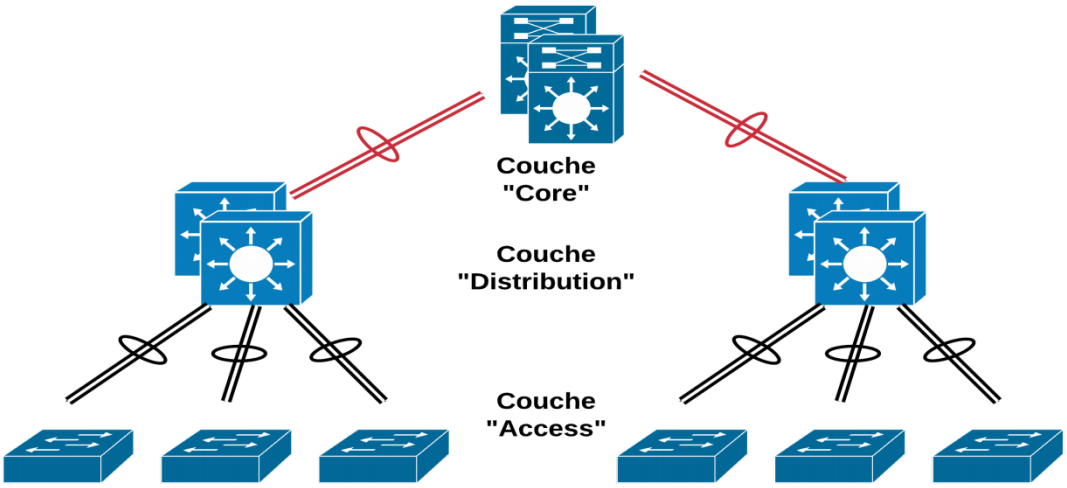



**Figure A.1 :**modèle hiérarchique.

- **La couche Cœur (CORE Layer)**

Cette couche correspond à la dorsale du réseau de l'entreprise qui relie entre eux les blocs fonctionnels d'équipements. Les objectifs à ce niveau sont les performances, la stabilité et le moins de complexité possible. C'est la raison pour laquelle on ne trouve généralement que deux routeurs redondants à ce niveau.

Le débit binaire utile est le critère de dimensionnement d'un routeur qui conditionne les performances. Par débit binaire utile, on entend la transmission de flux réseau classifiés, routés et filtrés.

- **La couche Distribution (Distribution Layer)**

Cette couche repose sur la convergence, l'équilibrage de charge, la qualité de service et la haute disponibilité. On y trouve l'isolation vis-à-vis de la couche accès avec le moins de commutation de circuits (ou d'adresses MAC) possible. Vue de la couche accès, c'est à ce niveau que l'on offre la redondance des passerelles réseau par défaut des hôtes.

- **La couche Accès (Access Layer)**

Plus les usages réseau évoluent, plus cette couche doit être riche en fonctionnalités diverses. Elle ne se limite plus à fournir des ports de commutateur en vis-à-vis de postes de travail fixes qui utilisent tous le même système. On y trouve maintenant des fonctions de gestion de l'alimentation des équipements raccordés au commutateur (téléphones, points

d'accès Wifi, etc.) via la technologie PoE (Power over Ethernet). On y trouve aussi les fonctions d'authentification de ces mêmes hôtes ou équipements raccordés à l'aide du protocole IEEE 802.1X.

**Modèle OSI (Open Systems Interconnection)**

Décrivons succinctement le rôle de chaque couche : [5]

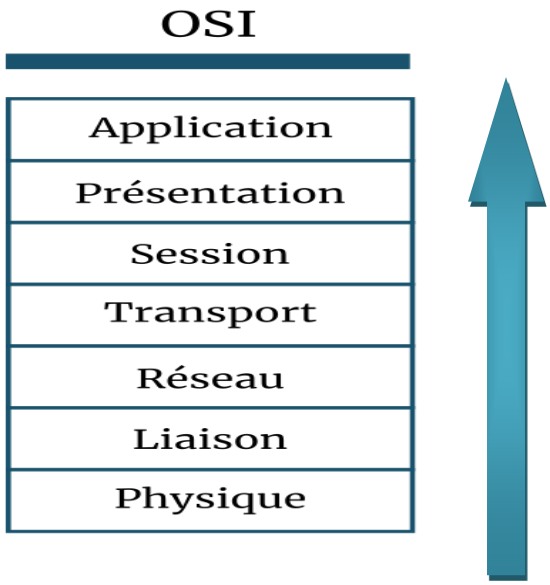



**Figure A.2 :** Modèle OSI.

- **La couche physique :** Elle convertit les signaux électriques en bits de données et inverse- ment, selon qu'elle transmet ou reçoit les informations à la couche liaison.
- **La couche de liaison de données :** Elle est divisée en deux sous-couches : -La couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux.

  -La couche LLC qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels des couches supérieures.

- **La couche réseau :**Renvoie à des concepts tels que le routage, le transfert et l'adressage sur un réseau dispersé ou plusieurs réseaux connectés de nœuds ou de machines. La couche réseau peut également gérer le contrôle du flux. Sur Internet, les protocoles Internet v4 (IPv4) et IPv6 constituent les principaux protocoles de couche réseau.

- **La couche Transport :** Elle segmente les données de la couche session, prépare et contrôle les tâches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport.
- **La couche session :** Son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.)
- **La couche présentation :** Elle convertit les données en information compréhensible par les applications et les utilisateurs : syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression.
- **La couche d'application :** Elle renvoie au type spécifique d'application lui-même et à ses méthodes de communication normalisées. Par exemple, les navigateurs peuvent communiquer à l'aide du protocole HTTPS (HyperText Transfer Protocol Secure), et les clients HTTP et de messagerie via POP3 (Post Office Protocol version 3) et SMTP (Simple Mail Transfer Protocol).

**Modèle TCP/IP (Transmission Control Protocol/ Internet Protocol)**

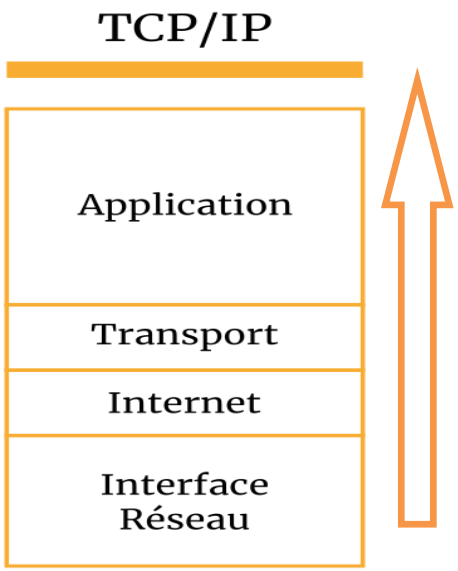



**Figure A.3 :** modèle TCP/IP.

- **Couche interface réseau :** elle semble regrouper les couches physiques et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule

contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau.

- **Couche Internet** : Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination**.**
- **Couche transport :** Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.
- **Couche application :** définit les services Internet standard et les applications réseau à la disposition des utilisateurs. Ces services fonctionnent conjointement avec la couche transport pour assurer l'envoi et la réception de données. Il existe de nombreux protocoles de couche d'application comme http, DNS, FTP et etc.

# ***Références bibliographiques***

[1] Latu, P. *«inetdoc.net,»* Interconnexion réseau et Logiciel Libre, p. modèle hiérarchique, 25 mars 2024.

[2] Pierre Erny. « Les réseaux informatiques d'entreprise ». 1998.

[3] Jean-François Pillou. *« Tout sur les réseaux et Internet »*, DUNOD 2006.

[4] MIHOUBI, M, MEDJANI, N, Mémoire de fin d'études en Master 2 réseaux et Télécommunications : *« Sécurisation d'une infrastructure LAN/WAN A base d'équipement Cisco »*, UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU, 2015.

[5] Jean-François Pillou et Jean-Philippe Bay. « *Sécurité informatique »*.3ième édition, Dunod, Paris 2013.

[6] BENDELLA, Z.Mémoire de fin d'études en Master 2 Informatique : *« Gestion de la sécurité d'une application Web à l'aide d'un IDS comportemental optimisé par l'algorithme des K-means »*. Université Abou Bekr Belkaid, Tlemcen**,** 2012-2013.

[7] Boukharrou, R. 2019-2020.Support du cours *« Sécurité des réseaux »*. Destiné aux étudiants 1ère Année Master réseaux et systèmes distribués. Université Abdelhamid Mehri - Constantine 2.

[8] OGUNGBEMI, H. Mémoire en licence professionnelle en Maintenance et Réseaux Informatiques : *« Etude pour la sécurisation d'un réseau par la mise en place d'un pare-feu open source: cas de C.A.F.E. informatique & télécommunications »*. Université de Lomé, 2019.

[9] TURKI, H. Mémoire Ingénieurs en Télécommunications :*« Gestion de la sécurité dans les réseaux TCP/IP : « SATAN » »*, École supérieure des communications de Tunis, 2004/2005.

[10] Amakou M'BATA, Olivier PERSENT, Firewall, pare-feu, Mur de feu, 2006.

[11] Jean- François Carpentier. *« La sécurité informatique dans la petite entreprise »*. 2ième édition, copyright-Edition ENI- Décembre 2012.

[12] BELALIA, MC, MAACHE, K. Projet de fin d'étude en Master 2 en Réseaux et Télécommunications :*« Étude et conception d'un Firewall »*. UNIVERSITÉ SAAD DAHLEB DE BLIDA, 2010-2011.

[13] KHERNANE, N. 2021-2022. Support du cours cyber sécurité 1 : *« les réseaux Privés Virtuels (VPN) »*. Destiné aux étudiants Master 1 ISIDS, Université Batna 2.

[14] BELHADJ, N. Mémoire de fin d'études en Master 2 réseaux et télécommunications : *« Etude et conception d'une plateforme de réseaux informatique couplant entre sécurité et supervision pour l'entreprise ENIEM »*.UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU, 2012-2013.

[15] DROMARD Danièle, Dominique SERET, Architecture des Réseaux, PEARSON France, 2013, ISBN : 978-2-7440-7664-0.

[16] DAVOU, M. Mémoire d'ingénieur de conception en informatique : **«** Mise en place d'un Intranet au Ministère de l'Économie et des Finances ». Université Polytechnique Bobo-Dioulasso, Janvier 2001.

[17] REMAZEILLES Vincent, *« La sécurité des réseaux avec CISCO »*. Edition eni.

[18] BOUBEKRI, S, MEBARKI, R. projet fin d'étude : « La haute disponibilité des réseaux campus. Cas d'étude : Sonatrach ». Université A/Mira de Béjaïa, 2015/2016.

[19] Albert, M. Mémoire en licence en ingénieur Système et Réseaux : *« Approche de design et implémentation d'un lan hiérarchique redondant pour la haute disponibilité d'une infrastructure réseau. Cas réseau de la drkat/Lubumbashi* ». Université Méthodiste au Katanga / Mulungwishi,2015.

[20] HAMRANI, A. Mémoire de fin d'études de Master 2 Automatique des systèmes : *« Amélioration des performances des réseaux industriels : Étude du protocole d'agrégation de liens EtherChannel »*. Université YAHIA FARES DE MEDEA, 2020.

[21] *« Audit de sécurité informatique : ce que vous devez savoir »*. (2024). Récupéré sur Oo2 Consulting&formations & Consulting: https://www.oo2.fr/consulting/audit-securite-informatique-ce-que-vous-devez-savoir. [Accès le 20 mai 2024].

[22] Axido. *« Test de vulnérabilité : Comment s'y prendre. Axido ».* [En ligne] https://www.axido.fr/faille-de-securite-informatique/test-de-vulnerabilite/. [Accès le 20 mai 2024].

[23] Algosecure. Spécialistes en sécurité informatique et pentests à Lyon, *«Analyse du risque cybersécurité»*. 2024. [En ligne]. Available: https://www.algosecure.fr/conseil/analyse-de-risques. [Accès le 20 mai 2024].

[24] Foxeet. *«Stratégie de Sécurité Informatique en Entreprise»*. Linked in, p. Étape 3 : Mise en Place de Mesures de Protection Conformément aux Bonnes Pratiques en Sécurité Informatique, 26 septembre 2023.

[25] CCNA 2 : Notions de Base sur les routeurs et le routage. Chapitre 11 : Listes de contrôle d'accès (ACL), p 194-195.

[26] *« Qu'est-ce que le chiffrement des données ? Définition et explication. (s.d.) »*. Récupéré sur Kaspersky: https://www.kaspersky.fr/resource-center/definitions/encryption.

[27] Centre de la sécurité des télécommunications. (2022, décembre). *« Journalisation et surveillance de la sécurité de réseau - ITSAP.80.085 »*. Récupéré sur gouvernement du canada : https://www.cyber.gc.ca/fr/orientation/journalisation-surveillance-securite-reseau-itsap80085.

[28] *« Qu'est-ce qu'un système SIEM ? »*. (2024). Récupéré sur Microsoft: https://www.microsoft.com/fr-fr/security/business/security-101/what-is-siem.

[29] http://technet.microsoft.com.

[30] https://www.memoireonline.com.

# Résumé

**Résumé**

La sécurité informatique est désormais essentielle en raison de la diversité croissante des attaques informatiques actuelles. Les réseaux des entreprises, des institutions et des gouvernements nécessitent particulièrement cette protection, car ils sont fréquemment ciblés.

Ce mémoire a été rédigé en s'appuyant sur le réseau d'un client de l'entreprise Campus NTS (Nouvelle Technologie et Solution) afin de créer le nôtre. L'objectif était de modéliser et simuler une architecture sécurisée et l'optimiser en utilisant un logiciel libre permettant la simulation de réseaux informatiques qui est GNS3 et un outil de virtualisation qui est VMware Workstation.

La solution est appliquée sur des équipements de base tels que les pare-feux, les commutateurs, les routeurs et les serveurs. Toutes les étapes d'installation, de configuration et de test sont présentées et expliquées dans ce mémoire.

**Mots clés** : Sécurité informatique, attaques informatiques, vulnérabilités, pares-feux, Gns3, VMware.

**Summary**

Computer security is now essential due to the increasing diversity of today's computer attacks. Business, institutional and government networks particularly require this protection, as they are frequently targeted.

This dissertation was written using the network of a client of the company Campus NTS (New Technology and Solution) in order to create our own. The objective was to model and simulate a secure architecture and optimize it using free software allowing the simulation of computer networks which is GNS3 and a virtualization tool which is VMware Workstation.

The solution is applied on basic equipment such as firewalls, switches, routers and servers. All installation, configuration and testing steps are presented and explained in this dissertation.

**Keywords:** Computer Security, computer attacks, vulnerabilities, firewalls, Gns3, VMware.

# Résumé


ملخص

أصبح أمان الكمبيوتر الآن ضروريًا نظرًا للتنوع المتزايد لهجمات الكمبيوتر اليوم. وتتطلب الشبكات التجارية والمؤسساتية والحكومية هذه الحماية بشكل خاص، لأنها مستهدفة بشكل متكرر

التكنولوجيا الجديدة والحلول) من أجل إنشاء ) Campus NTS تمت كتابة هذه الأطروحة باستخدام شبكة عميل شركة شبكة خاصة بنا. كان الهدف هو تصميم ومحاكاة بنية آمنة وتحسينها باستخدام برامج مجانية تسمح بمحاكاة شبكات VMware Workstation. وأداة المحاكاة الافتراضية وهي GNS3 الكمبيوتر وهي

يتم تطبيق الحل على المعدات الأساسية مثل جدران الحماية والمحولات وأجهزة التوجيه والخوادم. يتم عرض وشرح جميع خطوات التثبيت والتكوين والاختبار في هذه الأطروحة.



الكلمات المفتاحية: أمن الحاسوب، هجمات الحاسوب، نقاط الضعف، جدران الحماية، VMware، Gns3.