



المدرسة العليا للمواصلات بتونس
Ecole Supérieure des Communications de Tunis
Higher School of Communications of Tunis



2025

RAPPORT DE STAGE

Formation humaine

Réalisé par: EZZINE Montassar

Encadré par: DEBYAOUI Haithem



Résumé

Ce document présente une vue d'ensemble détaillée du stage de formation humaine effectué au sein de l'entreprise Groupe Chimique Tunisien (GCT).

Il s'inscrit dans le cadre d'un projet de mise en place d'une solution open source pour la gestion d'accès (NAC).

Ce rapport propose une analyse approfondie de l'entreprise ainsi qu'une description complète des travaux réalisés, tant sur le plan technique que sur le plan humain, en mettant en valeur les compétences techniques acquises, ainsi que le développement des aptitudes relationnelles et organisationnelles.

Remerciements

C'est avec une profonde gratitude que j'écris ces mots pour exprimer ma reconnaissance envers toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce travail. Je leur adresse mes remerciements les plus sincères.

Je tiens tout particulièrement à remercier Monsieur Haithem DEBYAOUI, mon encadrant technique, pour m'avoir accueilli au sein de GCT, pour m'avoir offert l'opportunité de réaliser ce stage, et pour son accompagnement bienveillant tout au long de cette expérience professionnelle. Je lui suis reconnaissant pour la clarté de ses explications, la mise à disposition de toutes les ressources nécessaires, ainsi que pour les précieuses méthodes d'organisation et de documentation qu'il m'a transmises.

Je ne saurais oublier de remercier chaleureusement l'ensemble de l'équipe de GCT pour leur collaboration, leur disponibilité et leur esprit d'équipe, ainsi que toutes les personnes ayant, de près ou de loin, contribué à la réussite de ce projet.

Mes remerciements s'adressent également à l'ensemble de mes enseignants de l'École Supérieure des Communications de Tunis – SUP'COM, pour la qualité de leur enseignement et leur accompagnement tout au long de l'année académique 2024/2025.

Enfin, j'adresse ma reconnaissance aux membres du jury, en espérant que ce rapport saura répondre à leurs attentes en termes de clarté, de rigueur et de motivation.

Table des matières

Liste des abréviations	vi
Introduction générale	1
1 Cadre général du projet	3
1.1 Introduction	3
1.2 Présentation de l'organisme d'accueil	3
1.2.1 Présentation du GCT	3
1.2.2 Domaines d'activités	4
1.3 Présentation du projet	5
1.3.1 Contexte du projet	5
1.3.2 Problématique	6
1.3.3 Étude comparative des solutions NAC	6
1.3.3.1 PacketFence	6
1.3.3.2 OpenNac Enterprise	11
1.3.4 Solution proposée	13
1.4 Méthodologie de travail	15
1.4.1 Les méthodes séquentielles (en cascade)	15
1.4.2 Variantes des méthodes séquentielles	15
1.4.3 Méthode adoptée : En cascade	16
1.5 Conclusion	17
2 Analyse préliminaire et planification	18
2.1 Introduction	18

2.2	Présentation de l'équipe	18
2.3	Capture des besoins	18
2.3.1	Besoins fonctionnels	18
2.3.2	Besoins non fonctionnels	19
2.4	Analyse préliminaire des besoins	19
2.4.1	Identification des acteurs	19
2.4.2	Diagramme de cas d'utilisation global	20
2.4.3	Vue architecturale	21
2.4.3.1	Architecture physique	21
2.4.3.2	Architecture logique	23
2.5	Environnement de travail	25
2.5.1	Environnement matériel	25
2.5.2	Environnement logiciel	25
2.6	Conclusion	27
3	Intégration de PacketFence	29
3.1	Introduction	29
3.2	Sélection de la méthode d'installation de PacketFence	29
3.3	Création de l'environnement virtuel de simulation	31
3.4	Installation et configuration d'Open vSwitch	33
3.5	Installation et configuration de OpenLDAP	35
3.5.1	Test de connectivité	38
3.6	Conclusion	39
4	Configuration de PacketFence	40
4.1	Introduction	40
4.2	Configuration de base	40
4.3	Présentation de l'interface de configuration	43
4.4	intégration de Open LDAP	49
4.5	Redémarrage des services et accès à l'interface d'observation	51
4.6	Conclusion	51

Table des matièresv

Conclusion générale et perspectives	52
Nétopraphie	53

Liste des abréviations

- **2FA** : Two-Factor Authentication
- **AD** : Active Directory
- **AUP** : Acceptable Use Policy
- **BYOD** : Bring Your Own Device
- **CMDB** : Configuration Management Database
- **EAP** : Extensible Authentication Protocol
- **EAP-PEAP** : Protected EAP
- **EAP-TLS** : Transport Layer Security
- **EAP-TTLS** : Tunneled TLS
- **EDR** : Endpoint Detection and Response
- **GCT** : Groupe Chimique Tunisien
- **IDS** : Intrusion Detection System
- **IP** : Internet Protocol
- **LAN** : Local Area Network
- **LDAP** : Lightweight Directory Access Protocol
- **MAC** : Media Access Control
- **MDM** : Mobile Device Management
- **NAC** : Network Access Control
- **NGFW** : Next Generation Firewall
- **OSI** : Open Systems Interconnection
- **SGBD** : Système de Gestion des Bases de Données
- **SIEM** : Security Information and Event Management
- **VPN** : Virtual Private Network
- **WAN** : Wide Area Network
- **Wi-Fi** : Wireless Fidelity

Table des figures

1.1	Logo du Groupe Chimique Tunisien	4
1.2	Logo de Packet Fence	7
1.3	Architecture logicielle et fonctionnelle de Packet Fence	9
1.4	Logo de Packet Fence	12
2.1	Diagramme des cas d'utilisation	21
2.2	Architecture physique de déploiement de la solution PacketFence	22
2.3	Architecture logique de PacketFence	24
3.1	Architecture virtuelle de simulation	32
3.2	Configuration d'Open vSwitch	34
3.3	Ajout d'une entrée dans l'annuaire LDAP	37
3.4	Recherche dans l'annuaire LDAP	37
3.5	Succès du ping entre les VMs PacketFence et OpenLDAP	38
3.6	Succès du ping entre la VM de test et les VMs PacketFence et Open vSwitch	39
4.1	Configuration des interfaces réseau	41
4.2	Configuration des paramètres généraux	41
4.3	Création du compte administrateur	42
4.4	Création des utilisateurs nécessaires pour la base de données gérée par MariaDB	43
4.5	La section « Statut »	44
4.6	La section « Rapports »	45
4.7	La section « Audit »	46
4.8	La section « Appareils »	46

4.9	La section « Utilisateurs »	47
4.10	Section « Configuration »	48
4.11	Section « Configuration des réseaux »	48
4.12	Section « Configuration – Intégration des composants externes »	49
4.13	Configuration de l'intégration OpenLDAP dans PacketFence	50
4.14	Réussite de la configuration de l'intégration OpenLDAP dans PacketFence	50
4.15	Page de connexion de PacketFence	51

Liste des tableaux

1.1	Tableau comparatif des solutions NAC	14
1.2	Comparaison entre les méthodes séquentielles	16
2.1	Identification des intervenants du système	20
2.2	Équipements de l'environnement matériel et logiciel	25
2.3	Outils de simulation utilisés	26
2.4	Outils de test et d'observation utilisés	27
3.1	Plan d'adressage IPv4 de l'architecture de simulation	33

Introduction générale

À l'ère de la transformation numérique et de l'évolution constante des modes de travail, les entreprises adoptent de plus en plus des pratiques telles que le télétravail, le **BYOD** (Bring Your Own Device) ou encore l'accès à distance via des réseaux privés virtuels (**VPN**). Ces approches, bien qu'innovantes et bénéfiques en termes de flexibilité et de productivité, introduisent également de nouveaux défis en matière de sécurité des réseaux d'entreprise. En effet, l'ouverture croissante des systèmes d'information expose les réseaux locaux privés à des risques accrus d'intrusion et d'attaques malveillantes.

Parallèlement, la multiplication des cyberattaques et la sophistication des techniques utilisées par les attaquants mettent en évidence les limites des méthodes classiques d'authentification. Ces failles sont souvent aggravées par un manque de sensibilisation des employés aux enjeux de sécurité, rendant les réseaux vulnérables à diverses menaces internes et externes.

Dans ce contexte, il devient essentiel pour les administrateurs réseau de déployer des outils de sécurité robustes, notamment ceux destinés à la gestion des accès au réseau. Ces outils doivent permettre de contrôler, authentifier et autoriser les utilisateurs ou les équipements qui cherchent à se connecter au réseau, tout en respectant les politiques de sécurité de l'organisation.

C'est dans cette optique que l'entreprise **GCT** a fait de la sécurisation de son infrastructure réseau multisites une priorité stratégique. Le stage de perfectionnement réalisé au sein de cette entreprise s'inscrit dans le cadre d'un projet visant à concevoir et à déployer une architecture réseau sécurisée, basée sur la mise en place d'un outil open source de contrôle d'accès au réseau (**NAC**).

Ce rapport présente de manière détaillée les travaux menés durant ce stage, en exposant la démarche suivie, les choix technologiques effectués, ainsi que les résultats obtenus

à travers la mise en œuvre de l'architecture proposée.

Le premier chapitre est consacré à la présentation de l'organisme d'accueil. Il décrit son historique, ses domaines d'activité, ses services, ainsi que le contexte et les objectifs du projet mené.

Le deuxième chapitre aborde les concepts théoriques nécessaires à la bonne compréhension du projet. Il s'intéresse notamment aux principes fondamentaux du Network Access Control (NAC), aux mécanismes de sécurisation des réseaux, ainsi qu'aux normes et bonnes pratiques en matière de contrôle d'accès.

Chapitre 1

Cadre général du projet

1.1 Introduction

Ce chapitre a pour objectif de mettre le point sur la présentation de l'organisme d'accueil, l'entreprise **Groupe Chimique Tunisien (GCT)**, au sein de laquelle mon stage de formation humaine était effectué en première partie. Il met en avant la problématique ainsi que la solution proposée en deuxième partie et se focalise sur la démarche adoptée pour l'élaboration du projet en dernière partie.

1.2 Présentation de l'organisme d'accueil

Dans les sections suivantes, nous allons présenter **GCT** ainsi que ses différents départements.

1.2.1 Présentation du GCT

GCT dont le logo est présenté dans la figure 1.1 est un leader mondial dans la transformation de phosphate en Acide Phosphorique Marchand (MGA), en Phosphate d'Ammonium (DAP, MAP) , en Super Phosphate (TSP, SSP) et en Phosphate de Calcium (DCP). Sa capacité nominale annuelle est d'environ 6,5 millions de tonnes de phosphate naturel.

En outre, le GCT produit le Nitrate d'Ammonium Agricole et le Nitrate d'Ammonium Poreux destinés principalement au marché local [1].



FIGURE 1.1 – Logo du Groupe Chimique Tunisien

Le GCT dispose de 3 sites de production répartis sur 3 régions du sud tunisien :

- Gabès
- Skhira
- M'dhilla

L'entreprise emploie plus de 4200 personnes (en 2024), sa mission est définie comme suit :

- Création d'une forte valeur ajoutée à partir du phosphate tunisien.
- Production et exportation de l'Acide Phosphorique et des Engrais Solides à travers le monde.
- Création d'emplois et amélioration de la vie sociale des citoyens.

1.2.2 Domaines d'activités

Les domaines d'activités couvrent principalement les secteurs suivants :

- **Production d'acide phosphorique** : Le GCT transforme le phosphate naturel en acide phosphorique, un composant de base essentiel dans la fabrication d'engrais chimiques. L'acide est produit principalement à Gabès et à Skhira.
- **Fabrication d'engrais chimiques** : Le groupe fabrique divers types d'engrais destinés au marché national et à l'exportation, notamment :
 - DAP (Di-Ammonium Phosphate)
 - TSP (Triple Super Phosphate)
 - DCP (Di-Calcium Phosphate)
 - Ammonitrates (AN)
- **Traitement et valorisation du phosphate** : En partenariat avec la Compagnie des Phosphates de Gafsa (CPG), le GCT réceptionne le phosphate brut extrait du bassin minier de Gafsa pour le transformer dans ses différentes unités industrielles.
- **Exportation de produits chimiques** : Le GCT occupe une position de leader régional dans l'exportation de produits phosphatés, desservant des marchés tels que

l'Inde, le Bangladesh, la Turquie, le Brésil et plusieurs pays européens.

- **Partenariats industriels et projets stratégiques :** Le groupe développe des partenariats internationaux pour renforcer sa capacité de production, tels que la coentreprise pour la fabrication d'engrais complexes (NPK) ou le projet Mdhilla 2 [1].

1.3 Présentation du projet

Dans cette partie, nous nous intéressons au contexte du projet, l'étude de l'existant ainsi que la problématique. Nous présenterons par la suite la solution proposée.

1.3.1 Contexte du projet

L'évolution rapide des technologies de l'information et la généralisation de nouveaux modes de travail, tels que le télétravail, le **BYOD** ou encore les accès distants via **VPN**, ont profondément transformé l'environnement numérique des entreprises. Dans ce contexte, la sécurité des réseaux informatiques est devenue un enjeu stratégique majeur. Les menaces telles que les cyberattaques, les fuites de données ou les accès non autorisés exigent une maîtrise rigoureuse des connexions au sein du système d'information.

Face à ces défis, les solutions de contrôle d'accès au réseau (**NAC**) se présentent comme un levier indispensable pour garantir l'intégrité, la confidentialité et la disponibilité des ressources informatiques. Ces solutions permettent de contrôler, d'authentifier et de superviser les terminaux souhaitant accéder au réseau, tout en assurant une conformité avec les politiques de sécurité de l'organisation.

C'est dans cette optique que notre projet, mené au sein de l'entreprise **GCT**, vise la mise en place d'une solution open source pour la gestion d'accès réseau (**NAC**). Ce choix stratégique repose sur la flexibilité, la transparence et la maîtrise des coûts qu'offrent les logiciels libres. La solution proposée ambitionne de fournir un outil robuste, évolutif et adapté aux besoins spécifiques de **GCT**, permettant ainsi de renforcer sa posture de cybersécurité et d'assurer une gestion centralisée, efficace et automatisée des accès réseau.

1.3.2 Problématique

Au sein de l'entreprise **GCT**, la sécurité informatique est un enjeu prioritaire, en particulier dans un contexte où les flux de données sont de plus en plus sensibles et où les menaces cybernétiques se multiplient. Toutefois, il a été constaté que certains sites de l'entreprise ne disposent actuellement d'aucune solution de gestion d'accès réseau (NAC), exposant ainsi ces environnements à des risques importants.

En l'absence de mécanismes de contrôle et d'authentification des équipements connectés, il devient difficile de garantir que seuls les utilisateurs et dispositifs autorisés puissent accéder aux ressources internes du réseau. Cette situation augmente la probabilité d'intrusions, de propagation de logiciels malveillants, ou encore de violations de données, mettant en péril l'intégrité et la confidentialité des informations de l'entreprise.

Par ailleurs, l'absence d'un système **NAC** centralisé complexifie la gestion des accès, notamment dans un environnement multi-sites. Cela rend plus difficile l'application uniforme des politiques de sécurité, le suivi des connexions, ainsi que l'adaptation rapide aux nouvelles menaces.

Face à cette problématique, il devient impératif de mettre en place une solution de gestion des accès réseau, fiable, flexible et adaptée aux besoins de l'entreprise, afin de sécuriser les différents sites et garantir une politique de sécurité cohérente à l'échelle de l'organisation.

1.3.3 Étude comparative des solutions NAC

L'étude comparative constitue une étape essentielle dans la mise en œuvre de notre projet. Elle vise à analyser les forces et les faiblesses des principales solutions open source existantes, afin d'identifier celles qui répondent le mieux à nos besoins. Cette analyse permet également de définir avec précision les fonctionnalités à intégrer dans la solution envisagée.

Il existe de nombreux outils répondant aux mêmes objectifs que ceux que nous poursuivons. Dans ce qui suit, nous présentons les solutions qui nous semblent les plus pertinentes pour notre cas d'usage.

1.3.3.1 PacketFence

Les informations présentées dans cette section sont principalement issues du site officiel de PacketFence [2].

PacketFence est une solution NAC libre, gratuite, fiable et entièrement prise en charge. Elle offre un ensemble impressionnant de fonctionnalités, notamment :

- Un portail captif pour l'enregistrement et la remédiation
- Une gestion centralisée des accès filaires et sans fil
- La prise en charge de la norme 802.1X
- L'isolation en couche 2 des équipements posant problème
- L'intégration avec le système de détection d'intrusion Snort et l'outil de détection de vulnérabilités Nessus

Grâce à cela, PacketFence permet de sécuriser efficacement des réseaux, qu'ils soient petits ou très grands, homogènes ou hétérogènes.

La figure suivante, 1.2, représente le logo de la solution de contrôle d'accès réseau "PacketFence".



FIGURE 1.2 – Logo de Packet Fence

— **Déploiement en mode "Out-of-band" :**

Le fonctionnement de PacketFence est entièrement hors bande (out-of-band), ce qui permet à la solution d'être hautement évolutive géographiquement et plus résistante aux pannes. En utilisant les technologies adéquates (comme la sécurité de port), un seul serveur PacketFence peut sécuriser des centaines de commutateurs et des milliers de terminaux connectés.

— **Déploiement en mode "Inline" :**

Bien que le mode hors bande soit recommandé, PacketFence supporte également un mode « inline », utile notamment pour les équipements filaires ou sans fil non administrables. Ce mode peut être mis en place en quelques minutes seulement et coexiste parfaitement avec un déploiement out-of-band.

— Vue d'ensemble des composants et intégrations de PacketFence :

La figure 1.3 illustre l'architecture logicielle et fonctionnelle de PacketFence. Il met en évidence :

- Modules de base utilisés par PacketFence (à gauche)
 - **FreeRADIUS** : pour l'authentification via 802.1X (filaire et sans fil)
 - **Apache** : pour l'interface web (portail captif et administration)
 - **Netdata** : pour la surveillance de la performance système
 - **MariaDB** : base de données relationnelle pour stocker les informations (utilisateurs, équipements, événements...)
 - **Redis** : base de données clé-valeur en mémoire pour améliorer les performances (caching, sessions)
- Fonctionnalités principales de PacketFence (au centre)
 - **Authentication** : Gestion des méthodes d'authentification des utilisateurs
 - **Compliance** : Vérification de la conformité des postes
 - **Device Management** : Gestion des appareils (avec ou sans agent)
 - **Firewall** : Intégration avec des pare-feu pour appliquer des politiques réseau
 - **IDS** : base de données relationnelle pour stocker les informations (utilisateurs, équipements, événements)
 - **Profiling and Fingerprinting** : Identification du type d'équipement grâce à Fingerbank
- Outils et technologies externes compatibles (à droite)

Chaque fonctionnalité peut s'intégrer avec des outils ou services tiers :

 - **Authentication** : LDAP / Active Directory / RADIUS / Google / Facebook / Email / SMS
 - **Compliance** : Nessus / OpenVAS / WMI
 - **Device Management** : Symantec, OPSWAT, MobileIron, PacketFence mobile (Apple/Android)
 - **Firewall** : Palo Alto, Fortigate, Barracuda, Checkpoint, Watchguard
 - **IDS** : Snort, Suricata, Tipping Point
 - **Profiling and Fingerprinting** : Utilisation de Fingerbank pour reconnaître automatiquement les types d'appareils. grâce à Fingerbank
- Communication avec les équipements réseau (en bas)
 - PacketFence peut communiquer avec de nombreux équipements réseau (switches, points d'accès...) via différents protocoles (SNMP, SSH, TELNET, RADIUS).
 - Les constructeurs mentionnés : ARUBA/HP, AEROHIVE, XIRRUS, DELL, RUCKUS, CISCO, BROCADE.

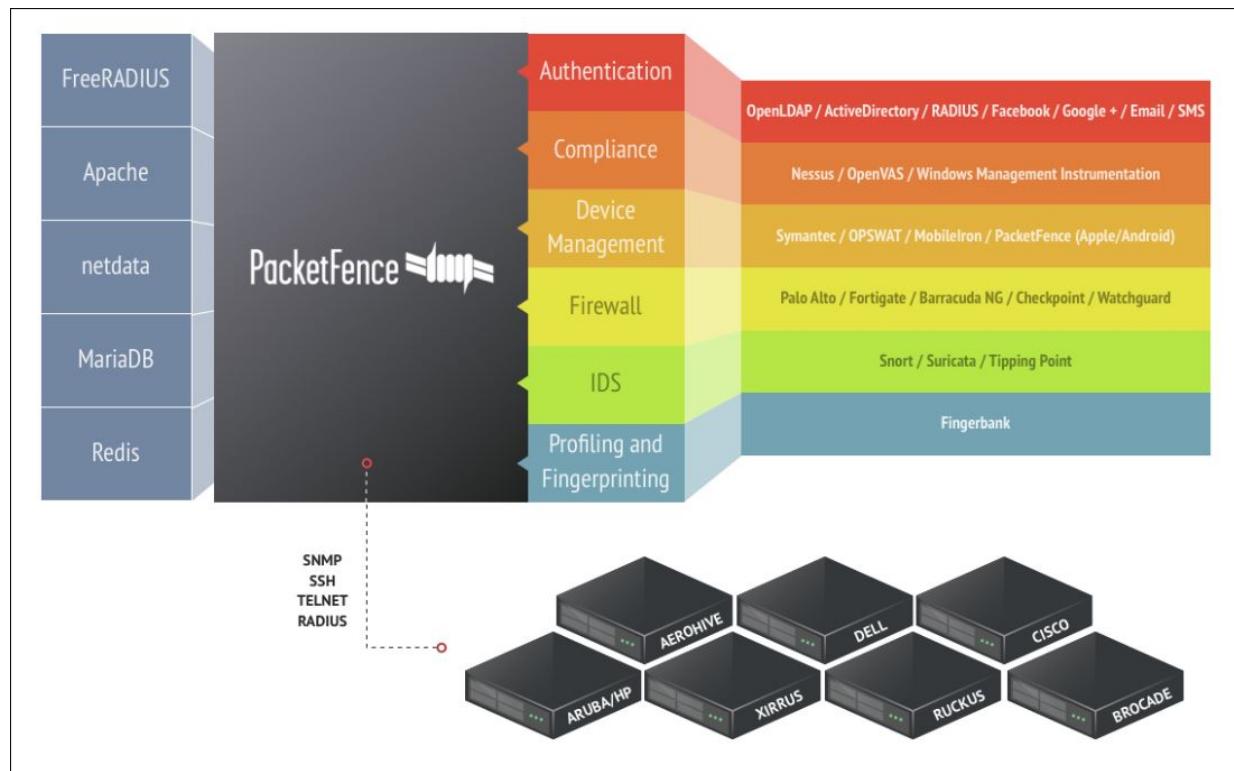


FIGURE 1.3 – Architecture logicielle et fonctionnelle de Packet Fence

— Prise en charge de la norme 802.1X :

- Il prend en charge l'authentification réseau basée sur la norme IEEE 802.1X, qui constitue une méthode standard pour contrôler l'accès aux réseaux filaires et sans fil. Cette norme permet une authentification sécurisée des utilisateurs et des appareils avant qu'ils n'accèdent au réseau.
- Grâce à l'intégration du module FreeRADIUS, PacketFence peut gérer efficacement les requêtes d'authentification envoyées par les équipements réseau (comme les commutateurs et les points d'accès Wi-Fi). Il prend en charge une variété de protocoles d'authentification EAP, notamment :
 - **EAP-TLS** : Une méthode très sécurisée reposant sur des certificats numériques pour authentifier à la fois le client et le serveur.
 - **EAP-PEAP** : Encapsule le protocole EAP dans une session TLS sécurisée, souvent utilisé avec des identifiants de type nom d'utilisateur/mot de passe.
 - **EAP-TTLS** : Semblable à PEAP mais plus flexible dans le choix des protocoles d'authentification internes.

Ce support étendu permet à PacketFence de s'adapter à divers environnements d'entreprise avec des exigences variées en matière de sécurité, tout en assurant une compatibilité avec un large éventail d'appareils et de systèmes d'exploitation. En appliquant la norme 802.1X, PacketFence renforce significativement la sécurité du réseau en autorisant uniquement les utilisateurs et dispositifs authentifiés à s'y connecter.

— **Enregistrement des équipements**

PacketFence propose un mécanisme d'enregistrement optionnel similaire aux portails captifs. Contrairement à la plupart des solutions de ce type, PacketFence mémorise les utilisateurs ayant déjà été enregistrés et leur redonne automatiquement l'accès sans nécessiter une nouvelle authentification, bien entendu, ce comportement est configurable. Un accord d'utilisation (AUP) peut aussi être défini pour obliger l'utilisateur à l'accepter avant d'obtenir un accès au réseau.

— **Intégration aux réseaux sans fil**

Grâce au module FreeRADIUS, PacketFence s'intègre parfaitement aux réseaux Wi-Fi. Cela permet de sécuriser les accès filaire et sans fil de manière unifiée, en utilisant la même base d'utilisateurs et le même portail captif, garantissant une expérience cohérente. La solution est également compatible avec plusieurs fournisseurs de points d'accès (AP) et de contrôleurs sans fil.

— **Prise en charge de la VoIP**

PacketFence prend en charge la téléphonie sur IP (VoIP), y compris dans les environnements hétérogènes. Il est compatible avec de nombreux fournisseurs de commutateurs, tels que : Cisco, Edge-Core, HP, LinkSys, Nortel Networks, etc.

— **Détection des activités réseau anormales**

Les comportements anormaux sur le réseau (virus, vers, logiciels espions, trafic interdit par la politique de sécurité, etc.) peuvent être détectés grâce à Snort, Suricata ou des capteurs commerciaux, en local ou à distance. Avec Suricata, une inspection de contenu est également possible. Au-delà de la simple détection, PacketFence propose un système de notifications et de réponses personnalisées à chaque type d'alerte, avec des actions configurables pour chaque type de violation.

— **Analyses de vulnérabilités proactives**

Des analyses de vulnérabilités avec Nessus ou OpenVAS peuvent être lancées à l'enregistrement d'un terminal, de manière planifiée ou ponctuelle. PacketFence corrèle les

identifiants de vulnérabilités détectées avec ses règles internes et redirige l'utilisateur vers une page web explicative sur les failles détectées sur son poste.

— **Intégration avec des agents de sécurité**

PacketFence s'intègre avec plusieurs solutions de sécurité, comme Microsoft Intune, SentinelOne, etc. La solution peut vérifier que l'agent de sécurité est bien installé avant d'autoriser l'accès au réseau. Elle peut aussi évaluer la conformité de l'équipement et l'isoler automatiquement en cas de non-conformité.

— **Remédiation via portail captif**

Une fois intercepté, tout le trafic réseau d'un poste passe par PacketFence. Selon l'état du terminal (non enregistré, en violation, etc.), l'utilisateur est redirigé vers l'URL appropriée. En cas de violation, un message d'instructions personnalisées est affiché, réduisant ainsi les sollicitations du support technique.

— **Isolation des appareils problématiques**

PacketFence prend en charge plusieurs techniques d'isolation des équipements suspects, y compris l'isolation VLAN avec prise en charge VoIP, même dans les environnements multi-fournisseurs.

— **Interface de gestion Web et ligne de commande**

- Toutes les tâches d'administration peuvent être réalisées via une interface web ou en ligne de commande.
- L'interface web prend en charge différents niveaux d'autorisation et l'authentification via LDAP ou Active Directory.

1.3.3.2 OpenNac Enterprise

Les informations présentées dans cette section sont principalement issues du site officiel de OpenNac Enterprise [3]

OpenNAC Enterprise est une solution logicielle de contrôle d'accès réseau (NAC) conçue pour les environnements LAN et WAN. Elle offre aux entreprises la possibilité d'authentifier, autoriser et auditer les connexions réseau en fonction de règles prédefinies. Principalement adaptée aux grandes structures, elle vise à renforcer la visibilité et le contrôle des appareils et utilisateurs connectés, qu'ils accèdent au réseau via câble, Wi-Fi ou VPN.

Ce qui distingue OpenNAC, c'est son approche modulaire : les organisations peuvent activer uniquement les fonctionnalités dont elles ont besoin, facilitant ainsi un déploiement progressif et maîtrisé.

La figure 1.4 représente le logo de la solution de contrôle d'accès réseau "OpenNac".



FIGURE 1.4 – Logo de Packet Fence

— Fonctionnalités clés

OpenNAC propose un éventail complet de fonctionnalités :

- **Authentification** : Via des certificats, AD/LDAP, adresse MAC ou encore portail captif
- **Autorisation** : Attribution de VLAN dynamique selon l'identité ou l'état du poste
- **Audit** : Historisation des connexions et tentatives d'accès
- **Inventaire (CMDB)** : Dynamique des identités connectées
- **Profiling et Posture** : Vérification de la conformité des équipements (OS, antivirus, correctifs)
- **Rémédiation** : Isolation automatique en cas de non-conformité
- **Double authentification (2FA)** : Renforcement de la sécurité (Google Authenticator)
- **Agent natif multi-plateforme** : (Windows, Linux, Mac) pour une réponse rapide aux anomalies
- **Intégration avec** : Des SIEM tiers, NGFW, MDM, antivirus, etc
- **Détection de comportements anormaux** : Via des capteurs réseau (Couche 7 du modèle OSI)
- **Support étendu des équipements réseau** : Quelle que soit la marque.

— Vue d'ensemble de l'architecture

L'architecture logicielle principale d'openNAC comprend différentes technologies et modules. Ces modules sont les suivants :

- **Apache** : C'est un serveur web, utilisé par le portail d'administration, l'agent openNAC, le portail captif et l'accès via API.

- **FreeRADIUS** : Prend en charge les services AAAA (Authentification, Autorisation, Comptabilisation, Audit).
- **MySQL** : C'est un SGBD qui permet de stocker la configuration et les données collectées.
- **Redis** : C'est une mémoire rapide en temps réel qui offre un accès très rapide aux événements et aux processus internes tels que les workers, le lecteur DHCP, les traps SNMP, etc.
- **Gearman Queues** : Système de files d'attente utilisé pour les tâches asynchrones. Il transmet les tâches à exécuter aux workers.
- **Workers** : Agents d'exécution des tâches en arrière-plan, responsables du traitement asynchrone (exécution de plugins, alertes, etc.).
- **Collectd** : Outil de collecte de métriques système. Il surveille la santé et les performances d'openNAC (CPU, RAM, trafic, nombre d'événements, etc.) et crée des tableaux de bord dynamiques et visuels pour les administrateurs (trending dashboards).

— Points d'attention

Bien qu'OpenNAC Enterprise soit riche en fonctionnalités, il est important de souligner :

- **Sa complexité d'architecture** : Peut exiger des compétences avancées et un accompagnement technique poussé
- **Le modèle modulaire** : Bien que flexible, peut impliquer plusieurs déploiements progressifs, ce qui allonge le temps de mise en production
- **Utilité variable de certains modules** : Certaines fonctionnalités clés (par exemple l'analyse de flux réseau ou les intégrations avancées) reposent fortement sur des modules spécifiques non toujours nécessaires dans des contextes classiques
- **Fonctionnalités sous licence** : Le modèle "Enterprise" d'OpenNAC n'est pas intégralement open source : certaines fonctionnalités peuvent dépendre de souscriptions, de services professionnels ou de licences spécifiques
- **Visibilité communautaire limitée** : Moins répandue que d'autres solutions dans les communautés open source, ce qui réduit la disponibilité de ressources communautaires, de retours d'expérience ou d'exemples concrets.

1.3.4 Solution proposée

Certaines solutions NAC open source, telles que FreeNAC et Netpass, ne disposent pas de documentation officielle, ce qui a rendu l'étude comparative plus complexe. Pour sur-

monter cette difficulté, nous nous sommes appuyés sur des vidéos disponibles sur YouTube ainsi que sur des échanges avec des outils de discussion basés sur l'intelligence artificielle. Par ailleurs, bien que FreeRADIUS soit une solution NAC à part entière, elle est déjà intégrée dans l'architecture de solutions plus complètes comme PacketFence et OpenNAC. Sur cette base, nous avons pu construire le tableau comparatif suivant :

TABLE 1.1 – Tableau comparatif des solutions NAC

Critères	PacketFence	OpenNAC Enterprise	FreeRadius
Licence	GPLv2	GPLv2	GPLv2
Développement actif	Forte communauté	Faible activité	Peu de MAJ
Authentification	Certifs, AD, LDAP, MAC, portail captif	Certifs, LDAP, portail captif	Intégration avec d'autres outils
Autorisation dynamique	VLANs dynamiques	Partiel	Non
Détection d'anomalies	IDS/IPS via Snort/Suricata	Non	Non
Gestion BYOD	Intégrée	Limitée	Non
Posture et conformité	Oui	Non	Non
Portail captif avancé	Personnalisable et multi-usage	Basique	Nécessite un frontend
Support 802.1X	Complet	Partiel	Oui
Facilité de déploiement	Complexe (documentation riche)	Simple	Configuration avancée

Au terme de cette analyse comparative des principales solutions **NAC open source**, à savoir **PacketFence**, **OpenNAC Enterprise** et **FreeRadius**, il apparaît clairement que **PacketFence** se distingue comme la solution la plus complète et la plus aboutie. Elle bénéficie d'une documentation officielle riche, d'une communauté active qui facilite la résolution des problèmes et le partage de bonnes pratiques, ainsi que d'une intégration fluide avec de nombreux outils (IDS/IPS, AD/LDAP, certificats, etc). De plus, elle propose un portail captif personnalisable, une interface web conviviale, une prise en charge complète du protocole 802.1X et une gestion efficace des appareils BYOD. Ces caractéristiques font de **PacketFence** une solution robuste, évolutive et adaptée aux besoins de sécurisation des réseaux modernes. Par conséquent, notre choix se porte sur **PacketFence** comme **solution NAC à adopter**.

1.4 Méthodologie de travail

Les méthodologies de travail, aussi appelées méthodes de gestion de projet, sont des approches structurées permettant de planifier, exécuter et finaliser efficacement un projet. Elles facilitent la coordination des tâches, la gestion des ressources, le suivi des délais, ainsi que la collaboration entre les parties prenantes.

Dans le cadre de projets techniques clairement définis, à périmètre fixe et objectifs stables, comme **la mise en place d'une solution open source pour la gestion d'accès réseau (NAC)**, les approches dites séquentielles, notamment la méthode en cascade et ses variantes, s'avèrent particulièrement adaptées.

Contrairement aux approches agiles, qui sont orientées vers le développement logiciel avec une forte adaptabilité aux changements, les méthodes séquentielles sont conçues pour les projets où les besoins sont bien établis dès le départ et où la rigueur de la planification est essentielle. Cela correspond parfaitement aux caractéristiques d'un projet d'intégration et de configuration d'une solution existante.

1.4.1 Les méthodes séquentielles (en cascade)

Les méthodes dites en cascade sont historiquement les premières approches structurées de gestion de projet. Elles sont particulièrement adaptées aux projets techniques avec des objectifs clairs et des étapes bien identifiées, comme c'est le cas dans le déploiement de la solution **PacketFence**.

Cette approche repose sur une succession de phases linéaires, chaque phase produisant des livrables validés avant de passer à la suivante.

Cette logique linéaire favorise une bonne traçabilité, une documentation rigoureuse et une planification fiable, ce qui est essentiel lorsqu'on intègre une solution tierce dans un environnement informatique existant.

1.4.2 Variantes des méthodes séquentielles

Plusieurs variantes ont été conçues à partir du modèle en cascade classique, afin de renforcer certains aspects comme la validation ou la gestion des risques. Voici les deux principales :

- **Modèle en V** : Ce modèle conserve une progression linéaire mais accorde une importance particulière à la validation. Chaque phase de conception a une phase de test correspondante. Ce modèle est souvent utilisé dans les projets techniques où la qualité et la sécurité sont critiques (ex. systèmes réseau, embarqués).
- **Modèle en spirale** : Il intègre une logique de cycles successifs avec une forte gestion

des risques à chaque itération. Moins utilisé pour les projets à périmètre fixe, il peut cependant convenir dans les environnements incertains ou les projets évolutifs.

Le tableau suivant présente une comparaison synthétique de ces trois modèles, appliqués au contexte des projets techniques tels que l'intégration d'une solution NAC.

TABLE 1.2 – Comparaison entre les méthodes séquentielles

Critères	Méthode en cascade	Méthode en V	Méthode en spirale
Structure	Séquentielle, chaque phase suit la précédente	Extension de la méthode en cascade, avec validation et test à chaque étape	Cycle itératif combinant conception et analyse des risques
Phases clés	Analyse, conception, implémentation, tests, déploiement	Idem que la cascade + phase de validation systématique	Définition des objectifs, évaluation des risques, développement et planification
Flexibilité	Faible	Faible à moyenne	Élevée, adaptée aux projets évolutifs
Gestion des risques	Non intégrée explicitement	Présente uniquement en phase de validation	Intégrée dès le début
Complexité du projet	Moyenne	Moyenne à élevée	Élevée
Documentation	Forte documentation à chaque étape	Documentation rigoureuse + traçabilité des tests	Documentation moins rigide mais centrée sur les risques
Coût et délais	Moins coûteuse si les besoins sont bien définis	Coût modéré avec bonne gestion des erreurs	Plus coûteuse à cause des itérations multiples

1.4.3 Méthode adoptée : En cascade

Dans le cadre de ce projet, il ne s'agit pas de développer une solution logicielle à partir de zéro, mais de mettre en place et configurer une solution open source existante, en

l'occurrence PacketFence. Cela implique des étapes bien définies, comme :

- L'installation de PacketFence,
- La configuration des services (DHCP, RADIUS, VLAN..),
- Les tests de fonctionnement et la validation.

Ce type de projet ne nécessite pas d'itérations fréquentes ni d'ajustements constants, comme dans les méthodes agiles. En revanche, une planification rigoureuse, une documentation claire et un suivi étape par étape sont essentiels.

Ainsi, la méthode en cascade s'avère la plus appropriée pour ce projet. Elle permet de structurer le travail en phases successives et cohérentes, ce qui correspond parfaitement à la démarche d'installation et de configuration d'un système.

1.5 Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil le **Groupe Chimique Tunisie (GCT)**. Nous avons ensuite défini le cadre du projet en détaillant l'analyse et l'étude comparative des solutions disponibles sur le marché, la problématique ainsi que la solution proposée. Enfin nous nous sommes penchés sur le choix de la méthodologie de travail.

Dans le chapitre suivant, nous aborderons la phase de planification de notre projet.

Chapitre 2

Analyse préliminaire et planification

2.1 Introduction

Dans le cadre de la mise en place d'une solution open source de gestion d'accès réseau NAC, une phase d'analyse préliminaire est indispensable pour bien cerner les exigences du projet, identifier les acteurs, définir l'architecture cible et planifier les différentes étapes du projet. Ce chapitre présente les fondements de cette phase, en s'appuyant sur une méthodologie structurée intégrant à la fois une compréhension fine du besoin et une planification rigoureuse.

2.2 Présentation de l'équipe

Le projet est réalisé par moi-même, Ezzine Montassar, en tant que stagiaire ingénieur, sous la supervision de M. Haithem Debyaoui, qui occupe le rôle d'encadrant technique.

2.3 Capture des besoins

La capture des besoins consiste à identifier, dans un premier temps, les besoins fonctionnels du projet. Ensuite, elle permet de spécifier les exigences non fonctionnelles attendues par les utilisateurs.

2.3.1 Besoins fonctionnels

Les besoins fonctionnels décrivent les services que doit rendre la solution NAC. Ils incluent notamment :

- Authentifier les utilisateurs et les équipements accédant au réseau
- Appliquer des politiques d'accès selon le rôle ou le type de l'utilisateur
- Isoler les postes non conformes (machines infectées, non mises à jour, etc)
- Fournir une interface d'administration centralisée
- Générer des rapports de connexion et des alertes de sécurité
- Intégration avec des systèmes d'annuaire (LDAP / Active Directory).

2.3.2 Besoins non fonctionnels

Les besoins non fonctionnels regroupent les exigences techniques et ergonomiques que la solution doit respecter afin de garantir sa fiabilité, sa qualité et la satisfaction des utilisateurs. Parmi ces besoins, on peut citer :

- **Fiabilité** : disponibilité continue du service
- **Scalabilité** : adaptation à l'augmentation du nombre d'utilisateurs
- **Sécurité** : protection des données sensibles, journalisation sécurisée
- **Interopérabilité** : compatibilité avec l'infrastructure existante (switchs, firewalls, OS)
- **Open source** : l'ensemble des composants utilisés doit être librement accessible.

2.4 Analyse préliminaire des besoins

Dans cette section, nous allons identifier les acteurs de notre système, présenter le diagramme de cas d'utilisation global et explorer sa vue architecturale.

2.4.1 Identification des acteurs

Le tableau 2.1 répertorie les acteurs impliqués dans notre projet.

TABLE 2.1 – Identification des intervenants du système

Acteurs	Rôle
Administrateur réseau	Gère les règles NAC, supervise les alertes, applique les politiques.
Utilisateur final	Tente de se connecter au réseau (authentifié ou invité).
Système d'annuaire	Fournit les identifiants des utilisateurs pour l'authentification.
Système NAC	Applique les règles d'accès et contrôle le trafic réseau.

2.4.2 Diagramme de cas d'utilisation global

Le diagramme de cas d'utilisation global et l'architecture globale du projet sont présentés dans cette section, suite à une première analyse préliminaire de ce projet.

La Figure 2.1 présente le diagramme de cas d'utilisation global qui met en évidence les fonctionnalités générales attendues de notre solution.

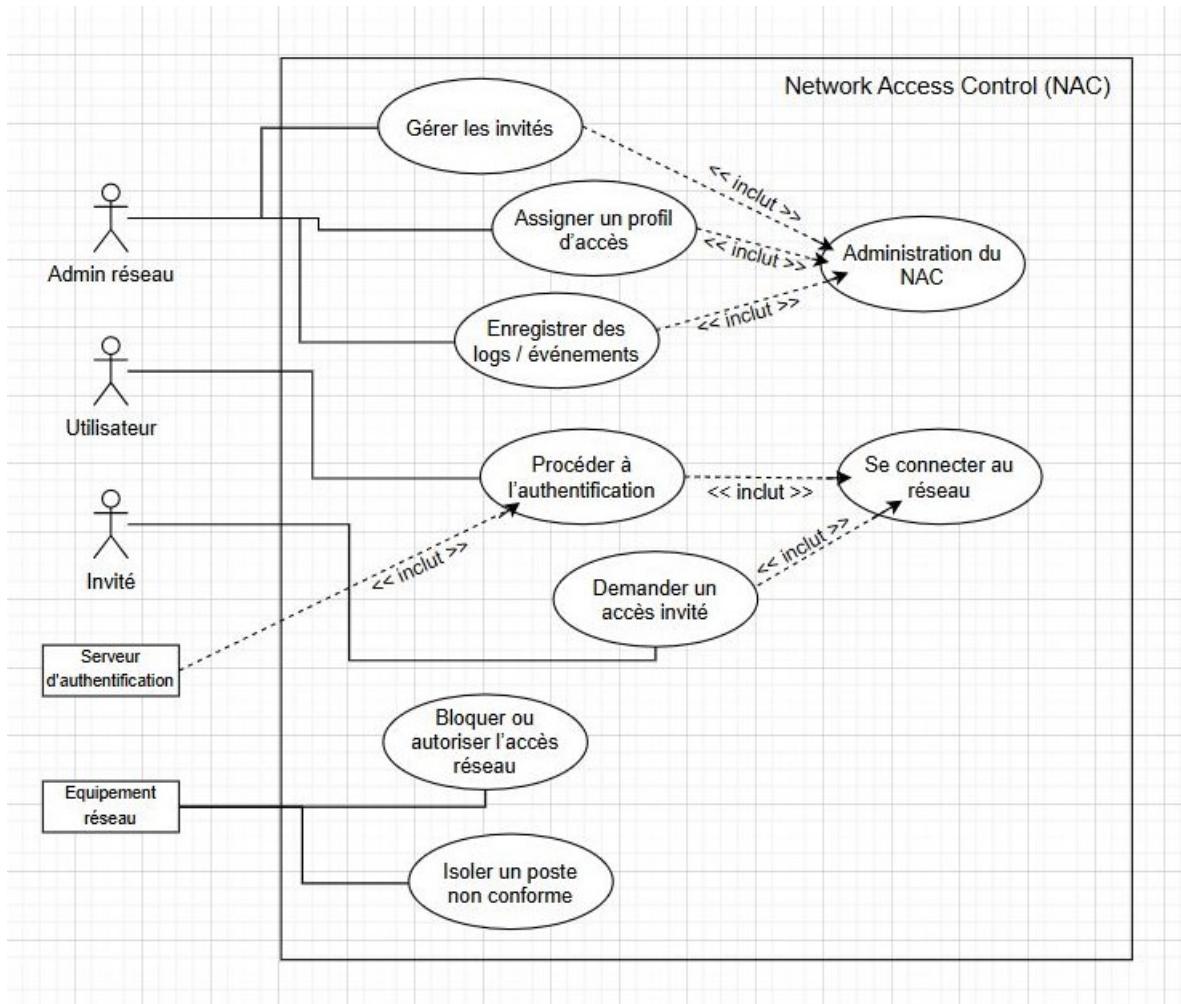


FIGURE 2.1 – Diagramme des cas d'utilisation

2.4.3 Vue architecturale

Il est essentiel de sélectionner l'architecture de la solution appropriée pour chaque système informatique afin de garantir un bon fonctionnement et des performances optimales. Nous exposons dans cette section les structures physiques et logiques de notre système.

2.4.3.1 Architecture physique

Cette architecture met en œuvre PacketFence, une solution NAC basée sur des VLANs, pour gérer dynamiquement les connexions des hôtes selon leur statut : enregistrement, isolement ou accès autorisé.

La figure 2.2 présente le principe de cette architecture.

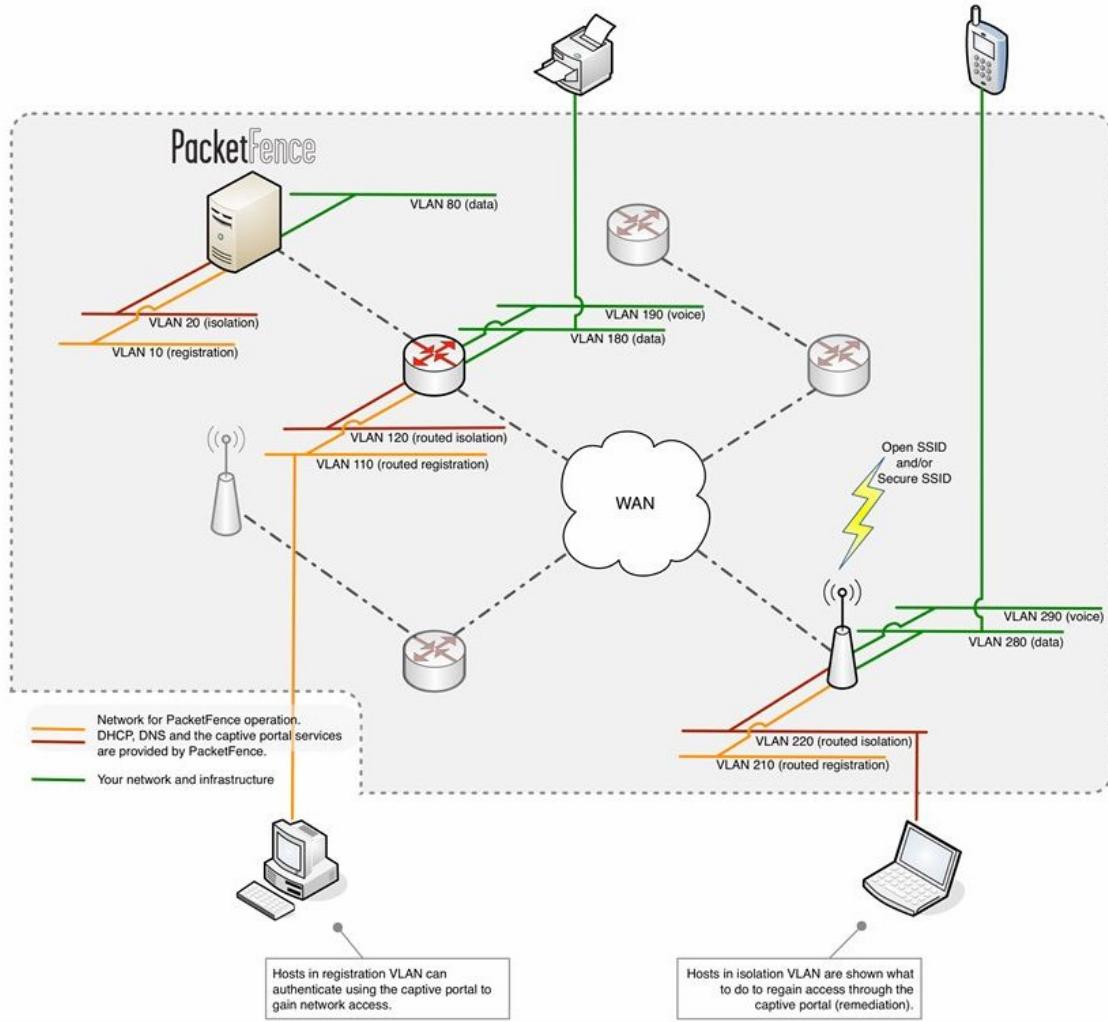


FIGURE 2.2 – Architecture physique de déploiement de la solution PacketFence

Dans cette architecture, PacketFence est déployé comme une solution NAC concrète et opérationnelle, reposant principalement sur une segmentation réseau via des VLANs. Au cœur du système, le serveur PacketFence joue un rôle central en assurant des services essentiels tels que le DHCP, le DNS, la gestion du portail captif, ainsi que la détection et la mise en quarantaine des postes non conformes. Ce serveur est connecté à plusieurs VLANs dédiés, à savoir : le VLAN 10 pour l'enregistrement initial des hôtes, le VLAN 20 pour l'isolement des machines jugées non conformes, et le VLAN 80 pour l'accès aux données, réservé aux hôtes validés.

L'architecture repose sur une logique claire de séparation du trafic. Les VLANs 10, 110 et 210 sont utilisés pour l'enregistrement, redirigeant les nouveaux hôtes vers un portail captif où ils doivent s'authentifier. Les VLANs 20, 120 et 220 sont dédiés à l'isolement des équipements présentant un comportement suspect ou ne respectant pas les politiques de sécurité. Dans ces VLANs, les utilisateurs reçoivent des instructions de remédiation via une page dédiée. Une fois authentifiés et validés, les utilisateurs sont redirigés vers les VLANs 80, 180 ou 280 pour un accès normal aux ressources réseau. En parallèle, les VLANs 190 et 290 sont réservés au trafic voix, notamment pour les équipements VoIP, garantissant ainsi la séparation du trafic critique.

Les équipements réseau (commutateurs, routeurs, points d'accès Wi-Fi) jouent un rôle essentiel dans le basculement dynamique des VLANs, en fonction de l'état de chaque utilisateur. Les bornes Wi-Fi, quant à elles, diffusent des SSID ouverts ou sécurisés permettant une gestion fine des connexions sans fil. Enfin, l'accès au WAN (réseau étendu ou Internet) n'est autorisé qu'aux hôtes ayant été validés, assurant ainsi un niveau de sécurité élevé. Cette architecture illustre de manière concrète la capacité de PacketFence à isoler, contrôler et sécuriser dynamiquement le trafic réseau selon des règles d'accès bien définies.

2.4.3.2 Architecture logique

La figure 2.3 illustre l'architecture logique de PacketFence. Elle met en évidence son intégration fluide avec divers composants du réseau, tels que les sources d'authentification (OpenLDAP, Active Directory, eDirectory, RADIUS), les équipements réseau (commutateurs, points d'accès, contrôleurs), ainsi que des outils de sécurité comme Snort (détection d'intrusion), Nessus (analyse de conformité des postes), ou encore NetFlow/IPFIX (contrôle de la conformité aux politiques d'accès). Le serveur Apache permet la gestion du portail captif et de l'interface d'administration, tandis que FreeRADIUS assure l'authentification filaire et sans fil via le protocole 802.1X. Cette architecture illustre la capacité de PacketFence à centraliser le contrôle d'accès, renforcer la sécurité et garantir la conformité dans des environnements réseau hétérogènes.

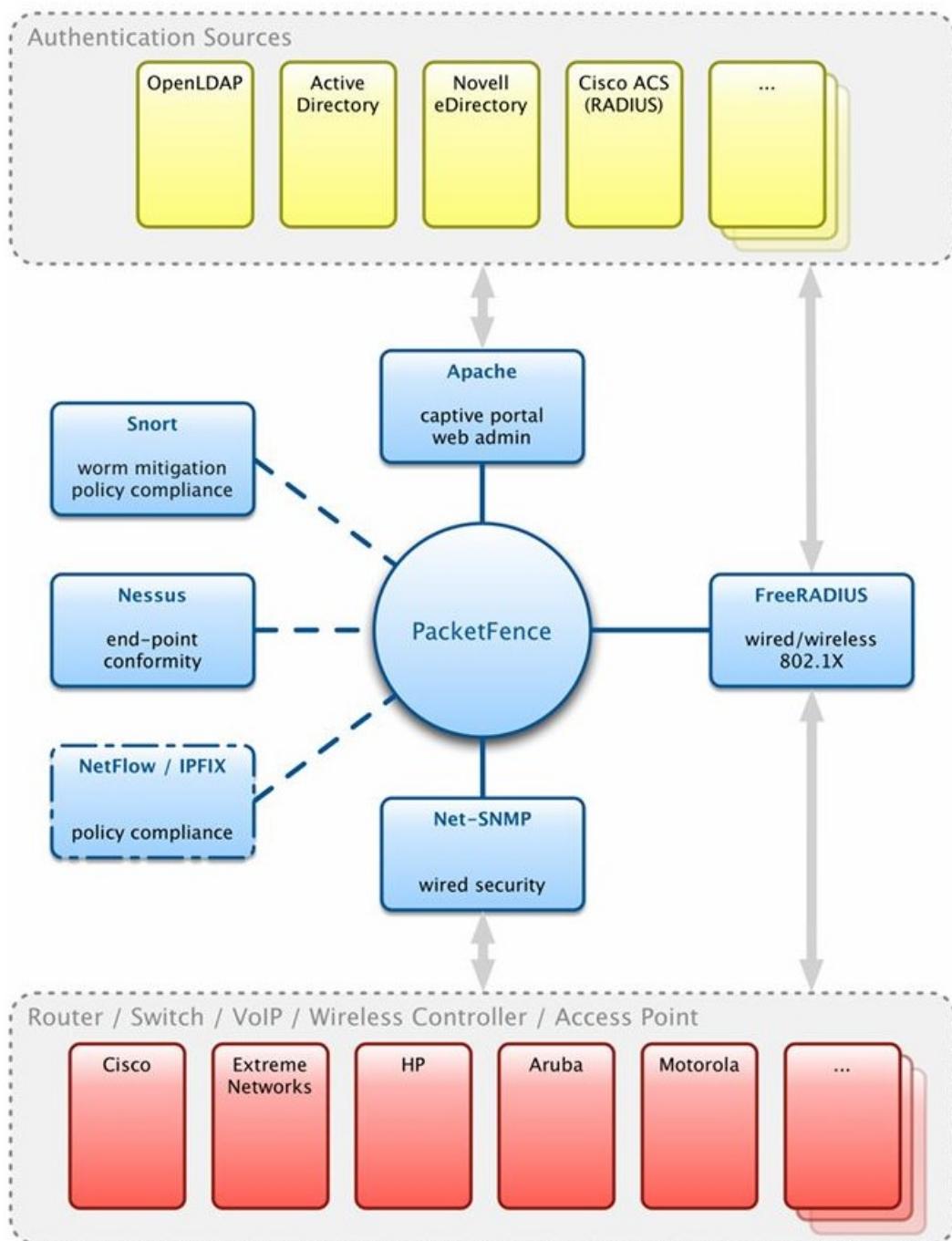


FIGURE 2.3 – Architecture logique de PacketFence

2.5 Environnement de travail

L'environnement professionnel est composé de deux éléments : l'environnement matériel et l'environnement logiciel.

2.5.1 Environnement matériel

Le tableau 2.2 présente les différents équipements matériels et logiciels utilisés dans le cadre du projet, ainsi que leur rôle dans l'architecture de test.

TABLE 2.2 – Équipements de l'environnement matériel et logiciel

Équipement	Rôle / Description
VM Debian 12	Machine virtuelle utilisée pour héberger l'environnement PacketFence.
PC HP	Poste physique d'administration et de configuration, utilisé pour accéder aux VM, lancer les tests et gérer la topologie.
Câblage	Câbles Ethernet RJ45 (droit/croisé selon besoin) pour les liaisons physiques et câble console (USB-RJ45) pour l'accès initial aux équipements si nécessaire.

2.5.2 Environnement logiciel

Dans cette partie, nous présentons les outils de simulation et d'observation, puis nous terminons par les outils de test et de vérification.

Les tableaux 2.3 et 2.4 présentent les outils utilisés dans ce projet.

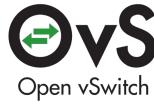
Outil	Description
	VMware Workstation Pro 17 est un hyperviseur de type 2 (hosted hypervisor) développé par VMware, qui permet de créer et gérer plusieurs machines virtuelles (Linux, Windows, BSD, MS-DOS, etc..) sur un ordinateur Windows ou Linux hôte. Chaque machine virtuelle fonctionne indépendamment tout en partageant les ressources du système physique [4].
 VM	PacketFence-VM sur Debian 12 est une appliance virtuelle complète de contrôle d'accès au réseau (NAC), basée sur Debian 12, développée par la communauté PacketFence (supervisée par Inverse Inc.). Elle intègre de nombreuses fonctionnalités : portail captif pour l'enregistrement et la remédiation, gestion centralisée des accès filaires et sans fil, prise en charge du standard 802.1X, isolation au niveau couche 2 pour les appareils problématiques, ainsi qu'une intégration avec des systèmes IDS, scanners de vulnérabilités et pare-feu. Déployée sous forme d'image ISO ou OVF prête à l'emploi, elle peut être déployée rapidement dans des environnements virtualisés (VMware ESXi, Proxmox, VirtualBox...), avec des exigences matérielles standardisées [2].
	EVE-NG est une plateforme de simulation réseau multivendeur qui permet aux professionnels, étudiants et formateurs de concevoir, tester et valider des topologies réseau complexes dans un environnement virtuel. Son interface web intuitive facilite l'accès et l'interaction avec les dispositifs simulés [5].
	Open vSwitch (OVS) sur Debian 12 est un commutateur virtuel multilayer open-source, sous licence Apache 2.0, conçu pour les environnements virtualisés. Il permet une automatisation réseau avancée via des interfaces de gestion standard (CLI, sFlow, NetFlow, IPFIX, RSPAN, LACP...) et supporte les extensions programmatiques. [6].
	OpenLDAP est une implémentation libre et open source du protocole Lightweight Directory Access Protocol (LDAP), développée par le projet OpenLDAP et distribuée sous sa propre licence de style BSD (OpenLDAP Public License). C'est une suite logicielle robuste, disponible pour de nombreux systèmes (Linux, BSD, AIX, macOS, Windows, etc.). Cette solution est idéale comme annuaire hiérarchisé pour gérer un grand volume d'utilisateurs ou de services, et peut très bien être installée dans une machine virtuelle Debian 12 [7].

TABLE 2.3 – Outils de simulation utilisés

La phase de simulation repose sur l'utilisation d'un environnement virtuel permettant d'installer et de configurer PacketFence en tant que solution NAC, OpenLDAP en tant qu'annuaire, et Open vSwitch en tant que commutateur virtuel, afin d'assurer le bon fonctionnement de PacketFence. Nous avons utilisé VMware Workstation Pro 17 comme hyperviseur pour créer les machines virtuelles dédiées à chacun des outils mentionnés. De plus, une machine EVE-NG a été déployée pour ses fonctionnalités avancées en conception et en administration des architectures réseaux. Ainsi, nous avons mis en place un environnement virtuel interactif permettant de tester le fonctionnement et les scénarios d'intégration de PacketFence dans un contexte professionnel d'entreprise.

Outil	Description
	Wireshark est un analyseur de paquets réseau open source et gratuit, largement reconnu dans l'informatique et la cybersécurité. Il permet la capture de trafic en temps réel ou l'analyse de fichiers enregistrés, avec une interface graphique intuitive à trois volets, des filtres d'affichage puissants, un codage couleur pour identifier facilement les types de trafic, et la prise en charge de centaines, voire des milliers, de protocoles [8].
	Ntopng est un outil open source de surveillance et d'analyse du trafic réseau, accessible via une interface web conviviale. Né comme version "next generation" de l'outil ntop créé en 1998. Il peut capturer le trafic via libpcap ou PF-RING, ou collecter des flux via NetFlow, sFlow ou IPFIX, notamment avec l'aide de nProbe [9].

TABLE 2.4 – Outils de test et d’observation utilisés

Wireshark et Ntopng offrent des fonctionnalités avancées d'analyse et de surveillance du trafic réseau, et sont utilisés pour vérifier la bonne configuration des différents équipements de l'architecture.

2.6 Conclusion

Grâce à ce chapitre, nous avons pu identifier les différents besoins fonctionnels et non fonctionnels du projet. Nous avons également présenté les acteurs impliqués ainsi qu'un diagramme de cas d'utilisation. Par la suite, nous avons décrit l'architecture physique de déploiement de PacketFence, suivie de son architecture logicielle. Enfin, nous avons conclu ce chapitre en détaillant l'environnement matériel et logiciel utilisé. Le chapitre suivant

portera sur la phase de l'installation de la solution NAC open source, PacketFence.

Chapitre 3

Intégration de PacketFence

3.1 Introduction

Dans ce chapitre, nous allons présenter la phase de mise en place de l'environnement virtuel de simulation ainsi que l'intégration de la solution PacketFence. Nous poursuivrons ensuite avec l'intégration des autres outils : OpenLDAP et Open vSwitch. La création de cet environnement virtuel nous offre l'opportunité de mettre en pratique les concepts avancés liés à notre solution.

3.2 Sélection de la méthode d'installation de PacketFence

La sélection du système d'exploitation sur lequel nous souhaitons installer la solution est indispensable, tout comme le choix entre une installation à partir de zéro ou l'installation sur une machine virtuelle contenant la solution PacketFence, qui est également très important. En effet, deux méthodes principales sont disponibles :

— Installation de PacketFence via RPMs/DEBs

Cette méthode consiste à installer PacketFence directement sur un système d'exploitation. Les paquets nécessaires sont disponibles sous forme de RPM ou DEB et peuvent être téléchargés depuis le site officiel de PacketFence [2]. Cette approche permet une installation native et une configuration complète sur les systèmes RHEL 8 et Debian 12.

Les RPMs (Red Hat Package Manager) sont un format de paquets utilisé par les distributions Linux dérivées de Red Hat, telles que RHEL, CentOS, AlmaLinux, Rocky Linux ou encore Fedora. Un paquet RPM contient non seulement les fichiers binaires

nécessaires au fonctionnement d'un logiciel, mais aussi des informations de métadonnées (version, dépendances, scripts de configuration, etc.). L'installation et la gestion de ces paquets se font généralement via les gestionnaires de paquets yum ou dnf, qui facilitent la résolution des dépendances et la mise à jour du système. Ce format est particulièrement adapté aux environnements professionnels, où la stabilité et la compatibilité avec l'écosystème Red Hat sont essentielles.

Les DEBs (Debian Software Packages) sont le format de paquets utilisé par Debian et ses dérivés, tels que Ubuntu, Linux Mint et bien d'autres. Chaque fichier DEB contient, de manière similaire aux RPMs, les binaires du logiciel, les scripts d'installation et les informations nécessaires à sa gestion. Sous Debian et Ubuntu, la gestion des paquets DEB se fait principalement avec les outils apt et dpkg, qui assurent l'installation, la suppression, la mise à jour et la résolution automatique des dépendances. Ce format est largement répandu dans l'écosystème open-source et apprécié pour sa simplicité et sa compatibilité avec un grand nombre de distributions communautaires et serveurs.

- **Installation de PacketFence sur RHEL 8 :**

- **sudo dnf update -y** : Mise à jour du système
- **sudo dnf install -y epel-release yum-utils** : Installer les utilitaires nécessaires
- **sudo curl -o /etc/yum.repos.d/packetfence.repo https://inverse.ca/downloads/PacketFence/RHEL8/packetfence.repo** : Ajouter le dépôt PacketFence
- **sudo dnf install -y packetfence** : Installer PacketFence
- **sudo systemctl enable --now packetfence** : Démarrer les services

- **Installation de PacketFence sur Debian 12 :**

- **sudo apt update sudo apt upgrade -y** : Mise à jour du système
- **sudo echo "deb http://inverse.ca/downloads/PacketFence/debian/14.0 bookworm main" | sudo tee /etc/apt/sources.list.d/packetfence.list** : Ajouter le dépôt PacketFence (Debian 12 = bookworm)
- **curl https://inverse.ca/downloads/GPG_KEY | sudo apt-key add -** : Ajouter la clé GPG
- **sudo apt update sudo apt install -y packetfence** : Installer PacketFence
- **sudo systemctl enable --now packetfence** : Démarrer les services

- **Installation d'une VM Debian 12 préconfigurée avec PacketFence :**

PacketFence propose également une version pré-intégrée dans une machine virtuelle De-

bian 12. Cette option est pratique pour tester ou déployer rapidement la solution sans passer par une installation complète depuis zéro. À noter que cette version VM n'est officiellement disponible que pour Debian 12 et inclut tous les composants nécessaires au fonctionnement de PacketFence [2].

Après avoir étudié les deux méthodes d'installation disponibles, nous avons retenu l'option consistant à utiliser une machine virtuelle Debian 12 préconfigurée avec PacketFence. Ce choix se justifie par plusieurs arguments :

- **Facilité de déploiement** : La VM Debian 12 pré-intégrée contient déjà tous les composants nécessaires à PacketFence, ce qui permet de gagner du temps par rapport à une installation complète sur RHEL9 depuis les RPMs.
- **Environnement isolé** : L'installation dans une VM permet de tester et de configurer PacketFence sans impacter le système hôte, réduisant ainsi les risques d'erreurs ou de conflits avec d'autres services.
- **Portabilité et sauvegarde** : Une VM peut être facilement copiée, déplacée ou restaurée, ce qui simplifie la gestion des environnements de test ou de production.
- **Compatibilité garantie** : La version VM est officiellement disponible uniquement pour Debian 12, ce qui assure que tous les composants sont compatibles et fonctionnels dès l'installation.

En résumé, le déploiement de PacketFence sur une VM Debian 12 préconfigurée allie rapidité, sécurité et fiabilité, ce qui en fait l'approche la plus adaptée à notre projet.

Nous avons donc téléchargé l'image ISO de Debian 12 contenant la solution PacketFence depuis la page officielle de téléchargement de PacketFence [10], puis nous avons créé la machine virtuelle, attribué les ressources nécessaires et configuré celle-ci correctement.

3.3 Cr éation de l'environnement virtuel de simulation

Nous avons poursuivi la mise en place de l'environnement virtuel de test en configurant les machines virtuelles intégrant OpenLDAP et Open vSwitch, afin de reproduire fidèlement le fonctionnement de PacketFence.

La figure 3.1 illustre l'architecture virtuelle à créer.

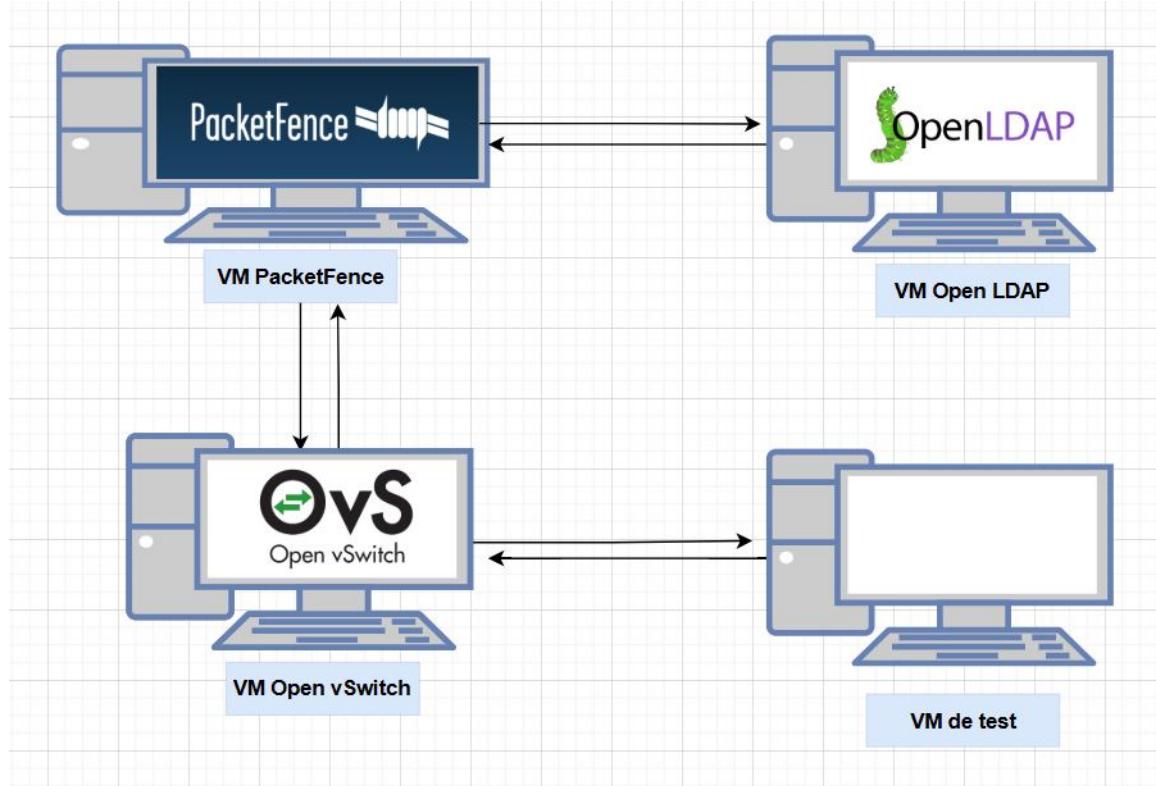


FIGURE 3.1 – Architecture virtuelle de simulation

Pour mettre en place cette architecture, nous avons dû créer des réseaux virtuels sous VMware Workstation. Nous avons défini plusieurs réseaux virtuels de type LAN Segment, nommés port1 à port5, afin de les attribuer aux interfaces physiques de la machine virtuelle Open vSwitch ainsi qu'aux équipements qui y sont connectés. Un autre réseau virtuel, nommé LDAP Connection, a également été créé pour assurer la communication entre les machines virtuelles PacketFence et OpenLDAP.

Nous sommes ensuite passés à la phase d'attribution des adresses IPv4.

Le tableau 3.1 présente le plan d'adressage adopté pour l'architecture de simulation. Il définit les adresses IP attribuées à chaque machine, garantissant une communication claire et sans chevauchement.

TABLE 3.1 – Plan d’adressage IPv4 de l’architecture de simulation

Machine	Interface	Adresse
VM PacketFence	eth0	192.168.1.254
	eth1	192.168.2.254
VM Open LDAP	ens33	192.168.2.100
VM Open vSwitch	br0	192.168.1.100
VM de test	ens33	192.168.1.50

Nous avons attribué deux sous-réseaux, 192.168.1.0/24 et 192.168.2.0/24, afin d’assurer l’invisibilité totale de la connexion entre les VMs PacketFence et OpenLDAP, et de maintenir cette dernière cachée.

3.4 Installation et configuration d’Open vSwitch

L’outil a été installé avec la commande suivante :

```
sudo apt install openvswitch-switch -y
```

Ensuite, nous avons activé le service `openvswitch-switch`. À partir de ce moment, il est possible de créer et configurer des commutateurs virtuels (*bridges*).

- **Création et configuration du bridge br0**

Nous avons créé une interface logique de type **bridge** appelée **br0**. Cette interface agit comme un commutateur virtuel et permet de regrouper plusieurs interfaces physiques.

Ainsi, toutes les machines connectées à ce bridge peuvent communiquer entre elles comme si elles étaient reliées à un switch physique.

La configuration est réalisée à l’aide des commandes suivantes :

- Crée le bridge **br0** :

```
sudo ovs-vsctl add-br br0
```

- Ajouter les interfaces physiques (adaptateurs réseau de la VM) au bridge :

```
sudo ovs-vsctl add-port br0 ens33    # ens33 = port1
sudo ovs-vsctl add-port br0 ens37    # ens37 = port2
sudo ovs-vsctl add-port br0 ens38    # ens38 = port3
```

```
sudo ovs-vsctl add-port br0 ens39    # ens39 = port4
sudo ovs-vsctl add-port br0 ens40    # ens40 = port5
```

— Attribuer une adresse IP au bridge (et non aux interfaces physiques) :

```
sudo ip addr add 192.168.1.100/24 dev br0
```

— Activer le bridge :

```
sudo ip link set br0 up
```

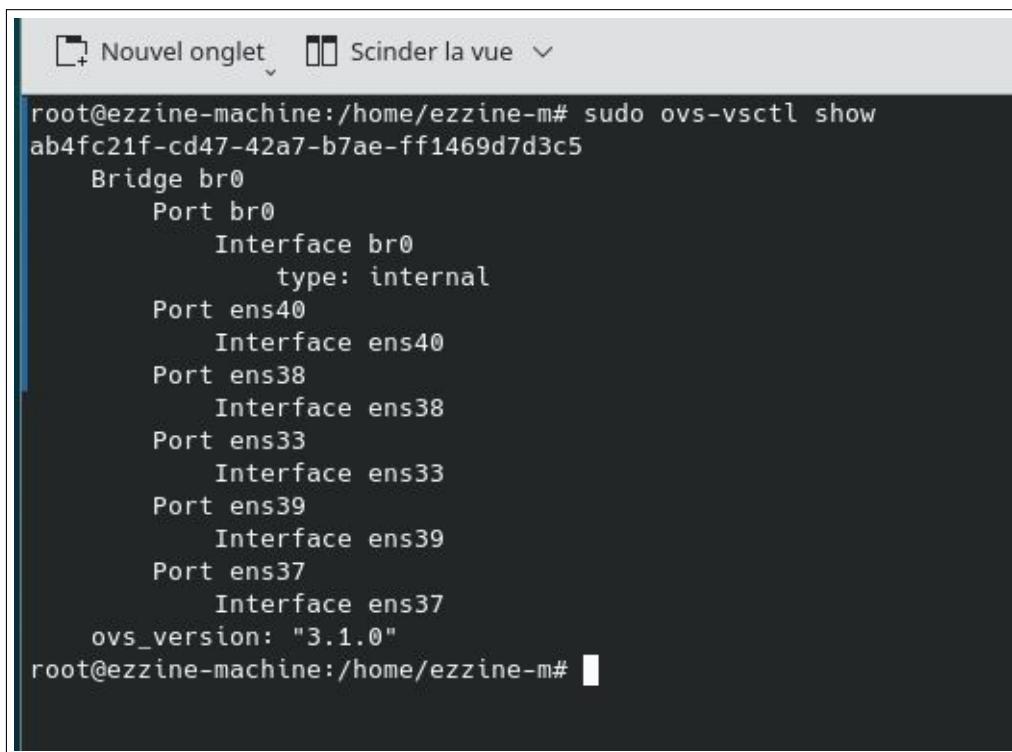
• Vérification de la configuration

Il est possible de vérifier l'état du bridge et des ports avec la commande :

```
sudo ovs-vsctl show
```

Cette commande affiche la liste des bridges créés, les ports associés et leur état.

La figure 3.2 illustre la configuration réalisée avec Open vSwitch.



```
Nouvel onglet Scinder la vue
root@ezzine-machine:/home/ezzine-m# sudo ovs-vsctl show
ab4fc21f-cd47-42a7-b7ae-ff1469d7d3c5
    Bridge br0
        Port br0
            Interface br0
                type: internal
        Port ens40
            Interface ens40
        Port ens38
            Interface ens38
        Port ens33
            Interface ens33
        Port ens39
            Interface ens39
        Port ens37
            Interface ens37
    ovs_version: "3.1.0"
root@ezzine-machine:/home/ezzine-m#
```

FIGURE 3.2 – Configuration d’Open vSwitch

• **Création des VLANs nécessaires** Dans le cadre de l’intégration d’Open vSwitch (OVS) avec PacketFence, la configuration des VLANs est réalisée à l’aide des commandes suivantes :

- sudo ovs-vsctl add-port br0 vlan10 tag=10 – set interface vlan10 type=internal
- sudo ovs-vsctl add-port br0 vlan20 tag=20 – set interface vlan20 type=internal
- sudo ovs-vsctl add-port br0 vlan30 tag=30 – set interface vlan30 type=internal

Chaque VLAN est ajouté comme un port interne au bridge principal br0 en lui attribuant un identifiant (tag) correspondant. Ainsi, les interfaces vlan10, vlan20 et vlan30 sont respectivement associées aux VLANs 10, 20 et 30 à travers les instructions ovs-vsctl. L'option type=internal permet de créer des interfaces logiques internes au système, ce qui facilite leur gestion et leur utilisation par PacketFence pour l'application des politiques de contrôle d'accès. Enfin, les commandes sudo ip link set vlan10 up, sudo ip link set vlan20 up et sudo ip link set vlan30 up activent les interfaces VLAN nouvellement créées, les rendant opérationnelles pour le traitement du trafic réseau au sein de l'infrastructure.

- **Port trunk**

- **sudo ovs-vsctl set port ens33 trunks=1-4094**

La configuration du port trunk via la commande précédente joue un rôle essentiel dans le bon fonctionnement du système. Cette instruction permet à l'interface ens33 de transporter simultanément le trafic de l'ensemble des VLANs (de 1 à 4094) sur une seule liaison physique, garantissant ainsi une interconnexion efficace entre le switch virtuel et l'infrastructure réseau. Grâce à ce paramétrage, ens33 n'est plus restreint à un VLAN unique, mais devient capable de véhiculer toutes les trames étiquetées issues de différents segments logiques. Cette approche assure une centralisation optimale et une flexibilité accrue dans la gestion des flux, tout en permettant à PacketFence d'appliquer des politiques de sécurité adaptées à chaque VLAN. Le port trunk configuré de cette manière constitue donc un élément clé pour la segmentation, l'isolation et le contrôle dynamique des accès dans le réseau.

3.5 Installation et configuration de OpenLDAP

Nous avons ensuite procédé à l'installation et à la configuration d'**OpenLDAP**. LDAP (Lightweight Directory Access Protocol) est un annuaire, c'est-à-dire une base de données hiérarchique optimisée pour la lecture. Il permet de **centraliser l'authentification** et les informations relatives aux utilisateurs, groupes, machines, imprimantes, etc.

- **Notions clés**

Avant son installation, il est important de comprendre quelques notions fondamentales :

- **Entry (entrée)** : Chaque objet (un utilisateur, une machine, un groupe) est une entrée dans l'annuaire.
- **DN (Distinguished Name)** : identifiant unique d'une entrée dans l'annuaire.

- Exemple : uid=john, ou=people, dc=example, dc=com
- **RDN (Relative Distinguished Name)** : partie unique du DN. Ici : uid=john.
 - **Attribute (attribut)** : les champs composant une entrée (nom, email, mot de passe, etc.).
 - **Schema** : définit les attributs et types d'objets autorisés (par ex. inetOrgPerson).
 - **DIT (Directory Information Tree)** : structure hiérarchique des données. Exemple :

```
dc=example,dc=com
    ou=people
    ou=groups
```

• Étape 1 – Installation

```
sudo apt update
sudo apt install slapd ldap-utils -y
```

• Étape 2 – Reconfiguration

Dans certains cas, l'installation ne déclenche pas la configuration interactive. Pour y accéder :

```
sudo dpkg-reconfigure slapd
```

Répondre aux questions :

- Omit OpenLDAP server configuration ? → No
 - DNS domain name : gct.tn
 - Organization name : Groupe Chimique Tunisien
 - Administrator password : montassar
 - Database backend : MDB (par défaut, recommandé)
 - Remove database when slapd is purged ? → No
- Cela crée une base de type : dc=gct,dc=tn.

• Étape 3 – Vérification

```
sudo systemctl status slapd
```

• Étape 4 – Ajout d'un utilisateur

Pour ajouter un utilisateur, il faut créer un fichier LDIF. Exemple pour l'utilisateur **montassar** :

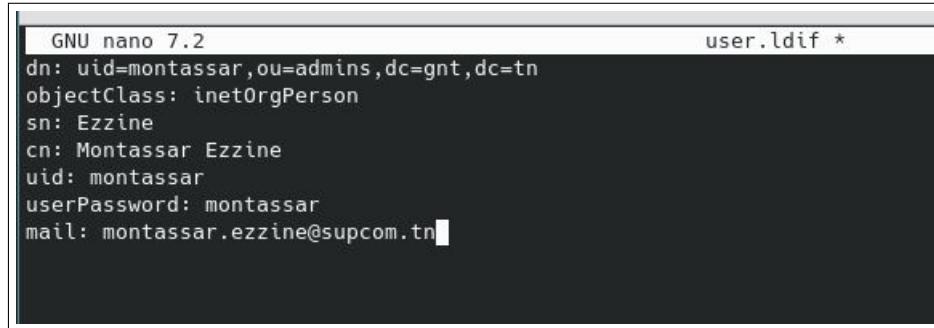
```
dn : uid=montassar,ou=admins,dc=gct,dc=tn
objectClass : inetOrgPerson
```

```
uid : montassar
sn : Ezzine
cn : Montassar Ezzine
mail : montassar.ezzine@supcom.tn
userPassword : montassar
```

Ajout dans l'annuaire :

```
ldapadd -x -D "cn=admin,dc=gct,dc=tn" -W -f user.ldif
```

La figure 3.3 illustre la phase d'ajout d'une entrée dans l'annuaire LDAP.



The screenshot shows a terminal window with the title 'user.ldif *'. The file contains the following LDAP entry definition:

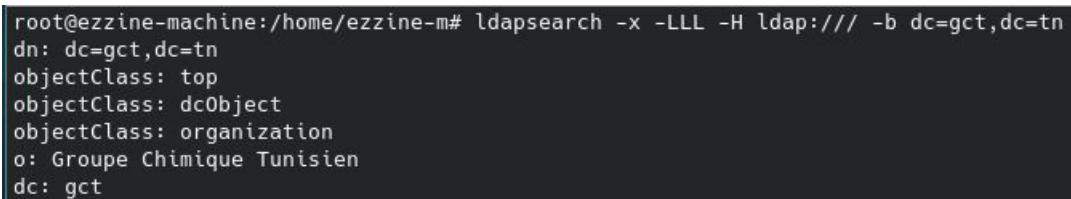
```
GNU nano 7.2
dn: uid=montassar,ou=admins,dc=gct,dc=tn
objectClass: inetOrgPerson
sn: Ezzine
cn: Montassar Ezzine
uid: montassar
userPassword: montassar
mail: montassar.ezzine@supcom.tn
```

FIGURE 3.3 – Ajout d'une entrée dans l'annuaire LDAP

• Étape 5 – Recherche dans l'annuaire

La figure 3.4 illustre la vérification de la bonne configuration de LDAP à travers une recherche dans l'annuaire en exécutant la commande :

```
ldapsearch -x -LLL -H ldap:/// -b dc=gct,dc=tn
```



The screenshot shows a terminal window with the title 'root@ezzine-machine:/home/ezzine-m#'. The command 'ldapsearch -x -LLL -H ldap:/// -b dc=gct,dc=tn' was run, and the output shows the structure of the root node:

```
root@ezzine-machine:/home/ezzine-m# ldapsearch -x -LLL -H ldap:/// -b dc=gct,dc=tn
dn: dc=gct,dc=tn
objectClass: top
objectClass: dcObject
objectClass: organization
o: Groupe Chimique Tunisien
dc: gct
```

FIGURE 3.4 – Recherche dans l'annuaire LDAP

3.5.1 Test de connectivité

Passons maintenant à la phase de vérification de la connectivité entre les différentes machines de notre architecture de test. La figure 3.5 illustre le succès du ping entre les VMs PacketFence et OpenLDAP.

```
root@packetfence:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e3:4d:9f brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname ens33
    inet 192.168.1.254/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee3:4d9f/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e3:4d:a9 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    altname ens37
    inet 192.168.2.254/24 brd 192.168.2.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee3:4da9/64 scope link
        valid_lft forever preferred_lft forever
root@packetfence:~# ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=64 time=0.340 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=64 time=0.300 ms
^C
--- 192.168.2.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.300/0.326/0.340/0.018 ms
root@packetfence:~# -
```

FIGURE 3.5 – Succès du ping entre les VMs PacketFence et OpenLDAP

La figure 3.6 illustre le succès du ping entre la VM de test et les VMs PacketFence et Open vSwitch, ce qui confirme le bon fonctionnement du switch virtuel.

```

root@ezzine-machine:/home/ezzine-m# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 brd 0.0.0.0 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: ens33: <NOARP,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:3f:3a:c3 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 192.168.1.50/24 brd 192.168.1.255 scope global ens33
            valid_lft forever preferred_lft forever
        inet6 fe80::250:56ff:fe3f:3ac3/64 scope link
            valid_lft forever preferred_lft forever
3: ens37: <NOARP,BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:00:c2:9d:3c:c3 brd ff:ff:ff:ff:ff:ff
        altname enp2s5
root@ezzine-machine:/home/ezzine-m# ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.380 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.313 ms
^C
--- 192.168.1.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.313/0.346/0.380/0.033 ms
root@ezzine-machine:/home/ezzine-m# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.823 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.507 ms
^C
--- 192.168.1.254 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.507/0.665/0.823/0.158 ms
root@ezzine-machine:/home/ezzine-m#

```

FIGURE 3.6 – Succès du ping entre la VM de test et les VMs PacketFence et Open vSwitch

3.6 Conclusion

Dans ce chapitre, nous avons présenté le choix de l’installation de la solution NAC open source PacketFence, ainsi que la création de l’environnement virtuel de simulation, composé de la VM PacketFence, d’une VM OpenLDAP utilisée comme annuaire, d’une VM Open vSwitch jouant le rôle de switch virtuel et d’une autre VM destinée aux tests. Nous avons également créé les réseaux virtuels nécessaires afin d’assurer une communication la plus proche possible de la réalité.

Dans le chapitre suivant, nous aborderons la configuration de la solution PacketFence afin de garantir son bon fonctionnement.

Chapitre 4

Configuration de PacketFence

4.1 Introduction

Après avoir vérifié la bonne installation de PacketFence ainsi que son intégration dans une architecture comprenant un switch virtuel et un annuaire, nous présentons dans ce chapitre la phase de configuration de la solution PacketFence. Cette dernière propose une interface web de configuration accessible à l'adresse : https://@de_vm_depacketfence:1443. L'interface utilise le protocole HTTPS (HTTP sécurisé) et le port 1443 pour l'échange des données."

4.2 Configuration de base

Dans cette phase, nous allons configurer les paramètres de base de PacketFence, définir le rôle de chaque interface, ainsi que le mot de passe du compte "Admin", etc.

La figure 4.1 illustre la configuration des interfaces réseau de notre VM PacketFence. L'interface ens38 est configurée comme interface de management afin de permettre l'accès à l'interface web de configuration. L'interface ens37, reliée à la VM OpenLDAP, est utilisée comme interface de connexion avec le serveur LDAP, tandis que l'interface ens33 est dédiée aux clients tentant d'accéder au réseau.

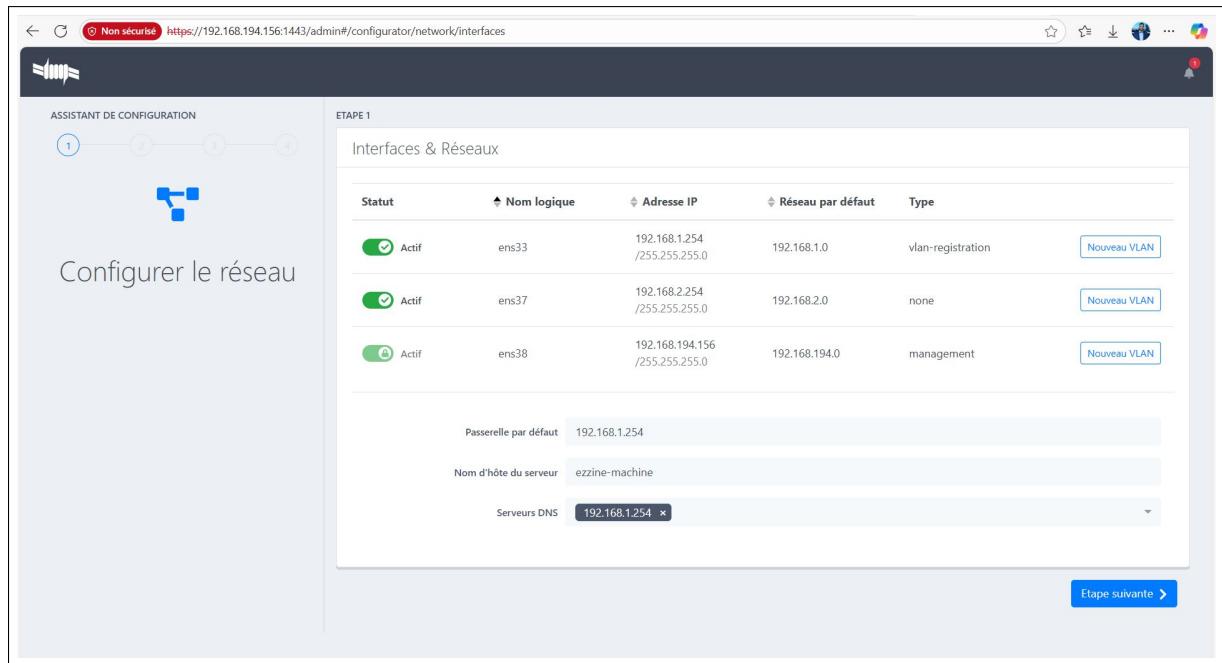


FIGURE 4.1 – Configuration des interfaces réseau

La figure 4.2 illustre la configuration d'autres paramètres de base, tels que le nom de domaine et le nom de l'hôte.

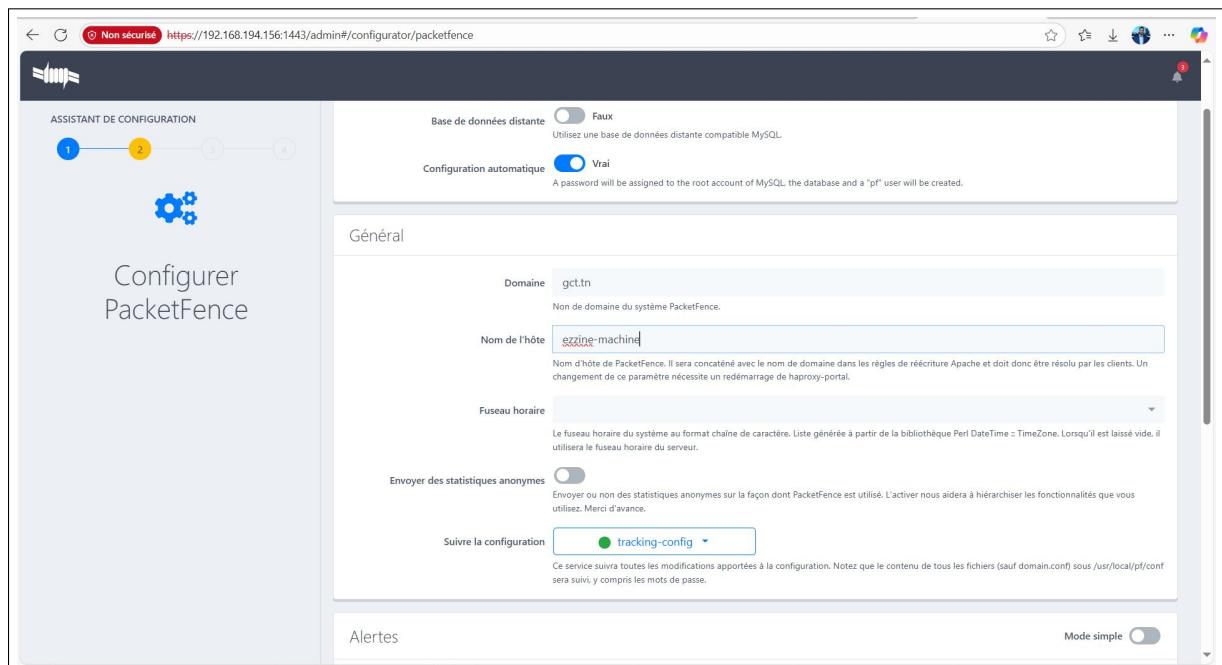


FIGURE 4.2 – Configuration des paramètres généraux

La figure 4.3 illustre la création du compte administrateur ainsi que la définition de son mot de passe.

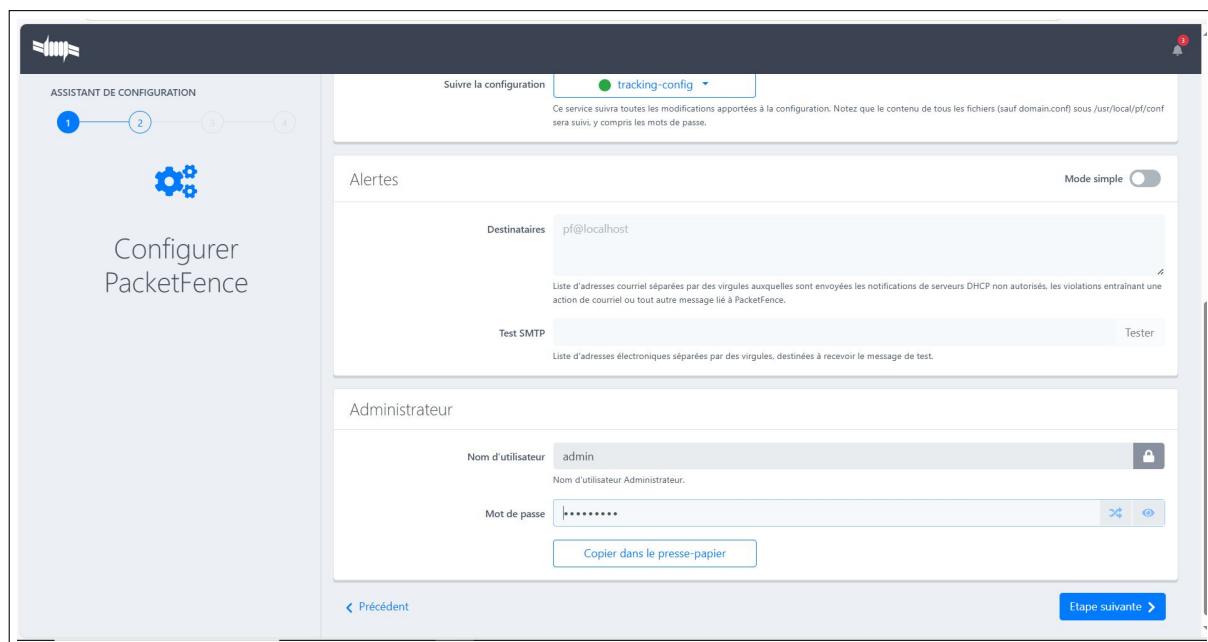


FIGURE 4.3 – Création du compte administrateur

La figure 4.4 illustre la création des comptes requis pour la base de données.

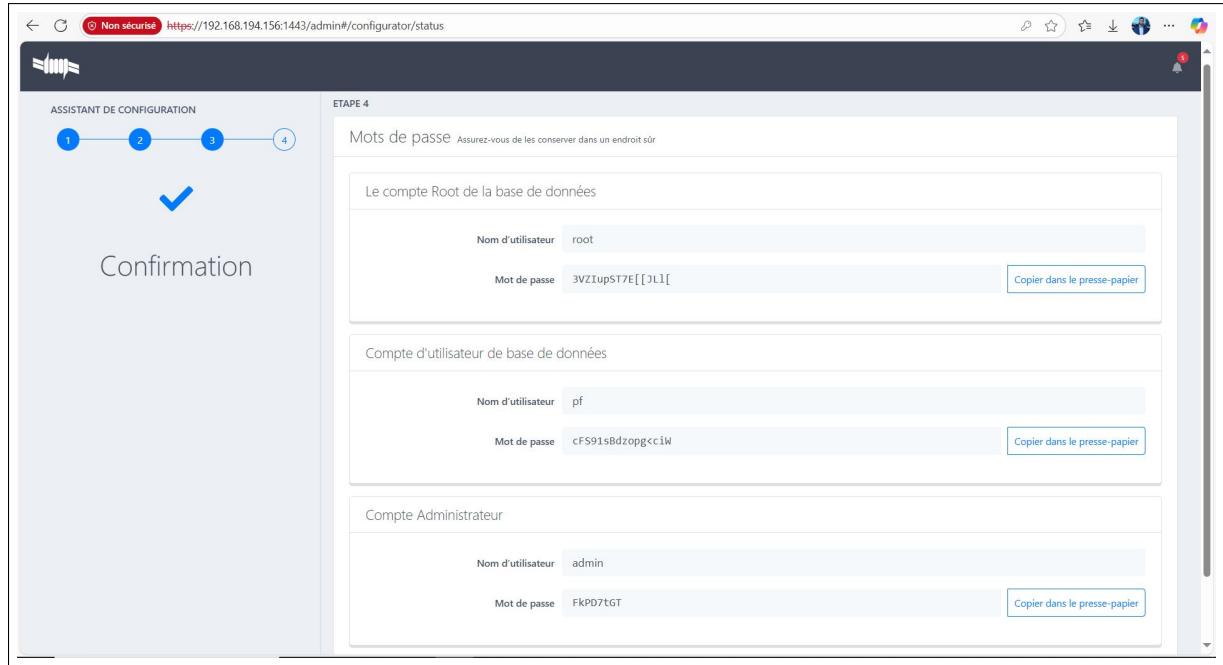


FIGURE 4.4 – Création des utilisateurs nécessaires pour la base de données gérée par MariaDB

4.3 Présentation de l'interface de configuration

L'interface web de PacketFence constitue l'outil central de gestion et de supervision de l'infrastructure réseau. Elle est conçue pour offrir un accès intuitif et structuré aux différentes fonctionnalités nécessaires à l'administration du système, tout en permettant le suivi et le contrôle des flux réseau. Cette interface se compose de plusieurs pages principales, chacune dédiée à un aspect spécifique de la gestion réseau.

La figure 4.5 présente la section "Statut" qui fournit une vue d'ensemble de l'état actuel du système. Elle permet de visualiser les services actifs, l'état des VLANs et des interfaces, ainsi que les connexions des clients en temps réel. Le tableau de bord offre une synthèse immédiate permettant de détecter rapidement toute anomalie ou interruption dans le réseau.

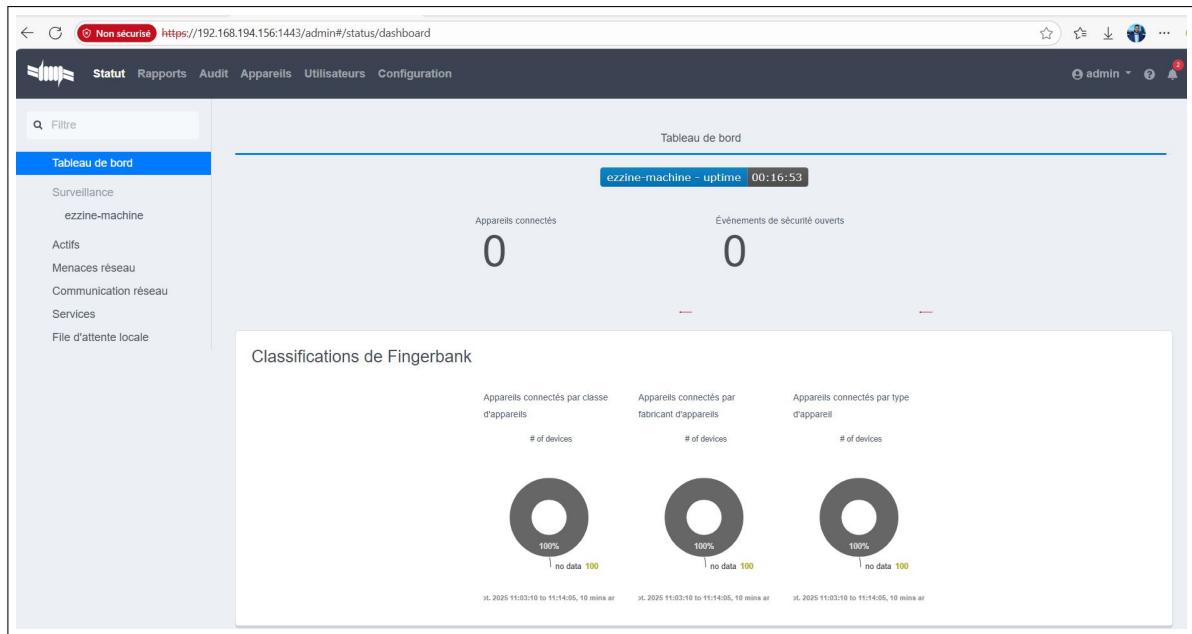


FIGURE 4.5 – La section « Statut »

La figure 4.6 présente la section "Rapports". Cette page centralise les données statistiques et historiques sur l'activité réseau. Les administrateurs peuvent générer des rapports détaillés sur l'usage des VLANs, les tentatives d'accès, ou les événements de sécurité. Ces informations sont essentielles pour l'analyse des performances du réseau et la planification d'éventuelles améliorations.

The screenshot shows the PacketFence web interface with the URL <https://192.168.194.156:1443/admin#/reports/Accounting%3A%3ABandwidth>. The top navigation bar includes links for Status, Reports (which is highlighted), Audit, Appareils, Utilisateurs, and Configuration. A user 'admin' is logged in. On the left, a sidebar menu under 'Accounting' has 'Bandwidth' selected. The main content area is titled 'Accounting / Bandwidth' and displays 'Total accounting bandwidth'. It shows a chart placeholder with the message 'Aucun résultat à afficher' (No results to display). Below the chart is a search bar and a table header for 'time_bucket', 'bytes_in', 'bytes_out', and 'bytes_total'. A search message 'Aucun résultat trouvé' (No results found) is displayed below the table.

FIGURE 4.6 – La section « Rapports »

La figure 4.7 présente la section "Audit" qui assure le suivi des événements de sécurité et des actions effectuées sur le système. Elle permet de vérifier la conformité aux politiques internes et de tracer les modifications apportées, offrant ainsi un historique précis des opérations pour des besoins de contrôle et de vérification.

FIGURE 4.7 – La section « Audit »

La figure 4.8 présente la section "Appareils". Cette page recense tous les équipements connectés au réseau, qu'il s'agisse de clients authentifiés, d'équipements inconnus ou d'appareils en quarantaine. Elle permet de gérer l'état de chaque appareil, de visualiser ses informations réseau, et d'appliquer des politiques de filtrage ou de blocage si nécessaire.

FIGURE 4.8 – La section « Appareils »

La figure 4.9 présente la section "Utilisateurs" qui centralise la gestion des comptes clients et administrateurs. Elle permet de créer, modifier ou supprimer des utilisateurs, d'assigner des rôles, et de contrôler leurs droits d'accès. Cette page est essentielle pour la mise en œuvre de la sécurité basée sur l'identification et l'authentification des utilisateurs.

The screenshot shows the 'Utilisateurs' (Users) section of the PacketFence web interface. At the top, there is a navigation bar with links for Statut, Rapports, Audit, Appareils, Utilisateurs (which is highlighted in blue), and Configuration. On the far right of the header, there is a user icon labeled 'admin' and some notification icons. Below the header, on the left, is a sidebar with a 'Filtre' button, a search input field, and two buttons: 'Rechercher' (highlighted in blue) and 'Créer'. Underneath these are 'Importer' and 'Supprimer' buttons. The main content area has a title 'Rechercher des utilisateurs' and a search input field with placeholder text 'Enter search criteria'. To the right of the search field are 'Effacer', 'Rechercher', and a magnifying glass icon. Below the search area is a table header with columns: Nom d'utilisateur, Source, Prénom, Nom de famille, and Courriel. The table contains two rows: 'admin' and 'default'. Each row has a 'Supprimer' button to its right. At the bottom of the table area, there are navigation buttons for page number (1) and other controls. The overall interface is clean and modern, using a dark header and light body colors with blue highlights for active buttons.

FIGURE 4.9 – La section « Utilisateurs »

Les figures 4.10, 4.11 et 4.12 illustrent la section de configuration avancée, qui offre l'ensemble des paramètres nécessaires pour adapter PacketFence aux besoins de l'organisation. Elle inclut la gestion des VLANs, des ports de switch, des stratégies d'accès, des serveurs externes (LDAP, RADIUS), ainsi que les paramètres généraux du système. Cette section constitue le cœur de la personnalisation et de l'optimisation de l'infrastructure réseau.

The screenshot shows the 'Configuration' tab selected in the top navigation bar. On the left, a sidebar menu includes 'Politiques et contrôle d'accès', 'Conformité', 'Intégration', 'Configuration d'accès avancée', 'Configuration réseau', and 'Configuration du système'. The main content area is titled 'Politiques et contrôle d'accès' and contains sections for 'Rôles', 'Domaines', 'Sources', 'Commutateurs', and 'Profils de connexion', each with detailed explanatory text.

FIGURE 4.10 – Section « Configuration »

The screenshot shows the 'Réseaux' section within the 'Configurations de réseau' tab. It includes tabs for 'Interfaces', 'Inline', 'Fencing', and 'Parking de l'appareil'. The 'Réseau' tab is active, displaying settings for 'DéTECTEUR DHCP', 'Limitation du débit du détecteur DHCP', 'DéTECTION DHCP non fiable', 'Interval illégal', 'DéTECTER les changements de nom d'hôte', and 'DéTECTER les changements dans le type de connexion MAC'. A sidebar on the left lists 'Politiques et contrôle d'accès', 'Conformité', 'Intégration', 'Configuration d'accès avancée', 'Configuration réseau', and 'Réseaux' (which is expanded to show 'Configurations de réseau', 'Interfaces', 'Inline', 'Fencing', 'Parking de l'appareil').

FIGURE 4.11 – Section « Configuration des réseaux »

The screenshot shows the 'Configuration' tab selected in the top navigation bar. The left sidebar has a 'Filtre' search field and a tree view of configuration modules. The 'Intégration' module is expanded, showing sub-options: 'Gestionnaire d'événements', 'Pare-feu SSO', 'Web Services', 'Modèle de commutateur', 'Renvoi Syslog', 'WRIX', and 'ICP'. Each option has a brief description below it.

FIGURE 4.12 – Section « Configuration – Intégration des composants externes »

4.4 intégration de Open LDAP

Puis, nous sommes passés à l'intégration du serveur OpenLDAP dans notre architecture. À travers l'interface de configuration de PacketFence, nous avons renseigné les données nécessaires à la connexion avec OpenLDAP, comme illustré dans la figure 4.13. La figure 4.14 présente quant à elle la réussite du test de connexion avec le serveur LDAP.

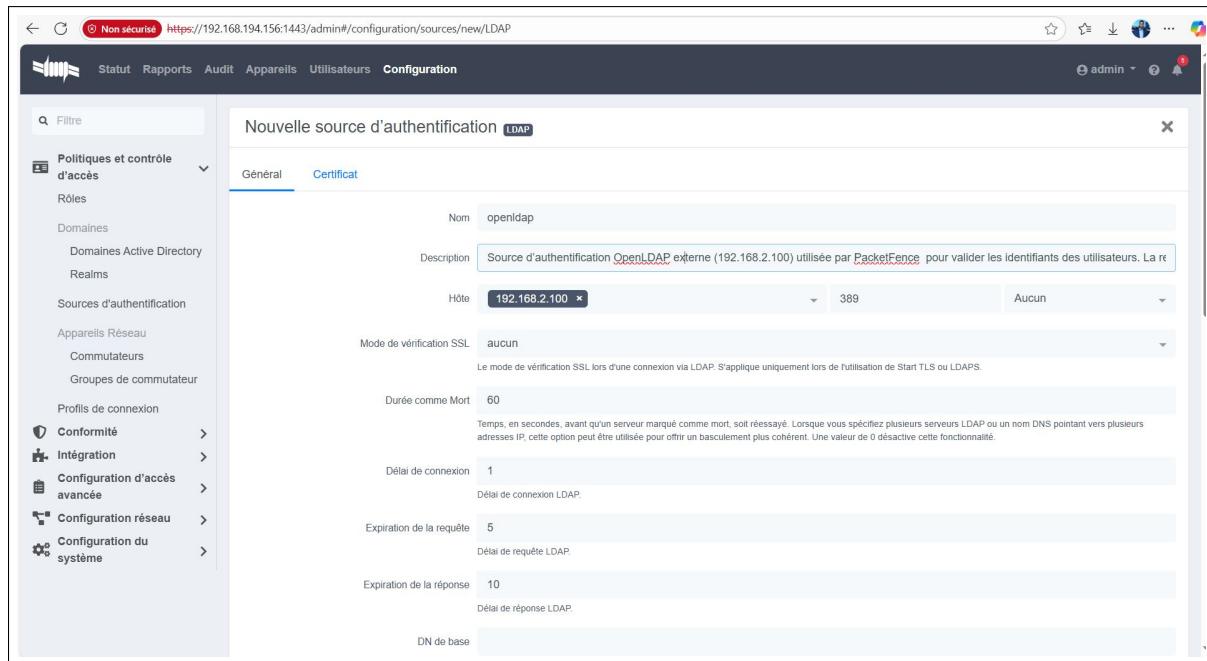


FIGURE 4.13 – Configuration de l'intégration OpenLDAP dans PacketFence

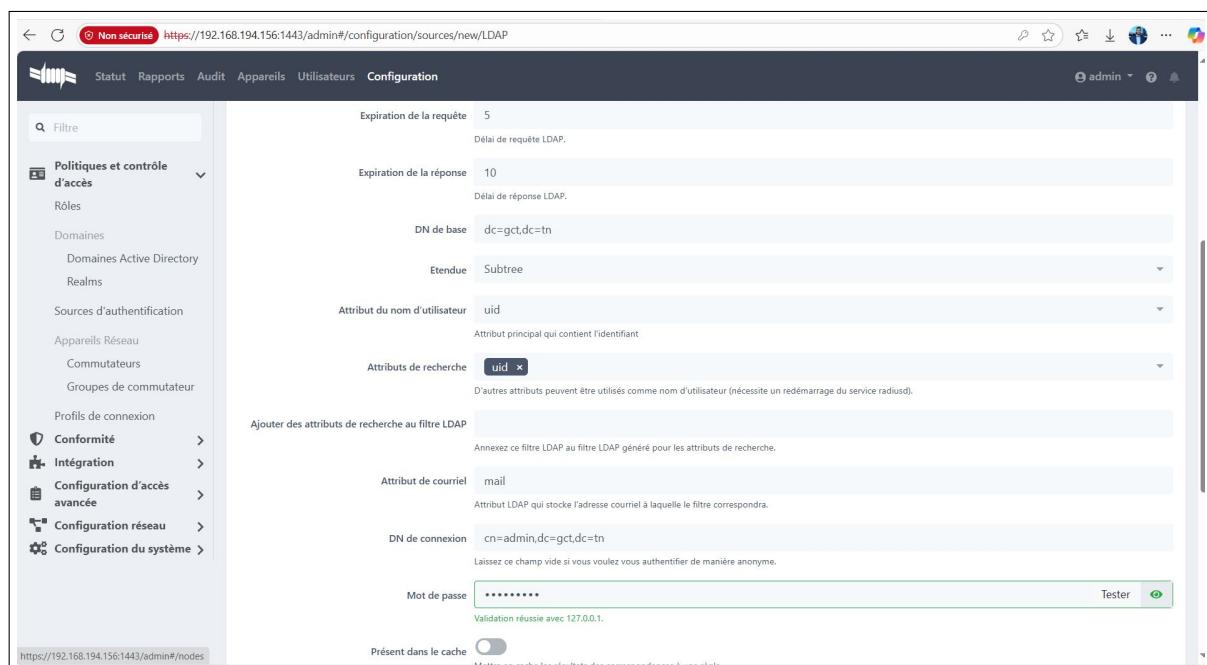


FIGURE 4.14 – Réussite de la configuration de l'intégration OpenLDAP dans PacketFence

4.5 Redémarrage des services et accès à l'interface d'observation

Une fois la configuration de base de PacketFence terminée, nous avons redémarré le service via la commande :

— sudo systemctl restart packetfence

Ensuite, nous avons de nouveau accédé à l'interface web de configuration, et cette fois la page de connexion s'est affichée. La figure 4.15 présente cette page de connexion, affichée avant de permettre à l'administrateur de se connecter à l'interface.

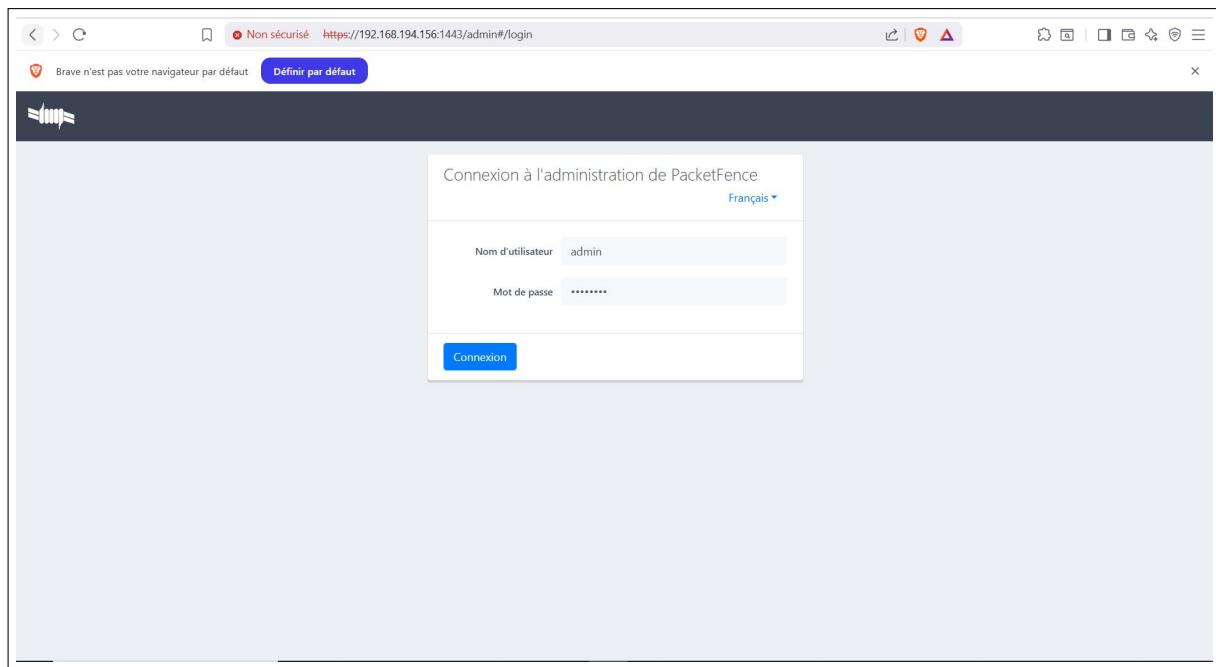


FIGURE 4.15 – Page de connexion de PacketFence

4.6 Conclusion

Dans ce chapitre, nous avons présenté la phase de configuration de la solution PacketFence à travers son interface web. Toutes les étapes, qu'il s'agisse de l'intégration de l'annuaire ou de la création des utilisateurs, y sont clairement détaillées. Dans le chapitre suivant, nous aborderons la phase de test du fonctionnement de la solution PacketFence ainsi que l'observation de son intervention lors de la tentative de connexion d'une nouvelle machine au réseau.

Conclusion générale et perspectives

En synthèse, ce rapport de stage de formation humaine met en lumière l'importance croissante de la gestion de l'accès au réseau local des entreprises, en particulier à travers les solutions NAC (Network Access Control).

Par ailleurs, la recrudescence des cyberattaques visant les organisations impose la mise en place de solutions robustes, capables de sécuriser efficacement cet accès.

À travers l'étude de cas du Groupe Chimique Tunisien, ce rapport a détaillé les différentes phases de l'installation et de l'intégration de la solution NAC open source Packet-Fence. Chaque chapitre a contribué à une compréhension approfondie des étapes critiques, allant de l'analyse préliminaire et la planification, jusqu'à la mise en œuvre technique et la configuration spécifique des diverses composantes de la solution proposée.

Il est indéniable que nous avons rencontré des obstacles techniques et conceptuels au cours de notre stage, mais ces difficultés ont également constitué une opportunité précieuse d'immersion dans le monde professionnel. Nous avons ainsi pu développer des compétences solides en administration des réseaux et des systèmes informatiques, ainsi qu'une meilleure maîtrise des systèmes d'exploitation basés sur le noyau Linux.

Enfin, pour l'avenir, plusieurs axes d'amélioration peuvent être envisagés, notamment l'intégration de nouvelles technologies basées sur l'intelligence artificielle. Celles-ci permettraient de renforcer les processus de contrôle d'accès au réseau, d'optimiser les mécanismes d'authentification et d'améliorer l'identification des différents acteurs du réseau.

Nétographie

- [1] Site officiel de GCT, disponible sur : <http://www.gct.com.tn>, consulté le 21 juillet 2025.
- [2] Site officiel de Packet Fence, disponible sur : <https://www.packetfence.org>, consulté le 22 juillet 2025.
- [3] Site officiel de OpenNac Enterprise, disponible sur : <https://doc-opennac.opencloudfactory.com>, consulté le 24 juillet 2025.
- [4] Site officiel de VMWare, disponible sur : <https://www.vmware.com>, consulté le 28 juillet 2025.
- [5] Site officiel de EVE-NG, disponible sur : <https://www.eve-ng.net>, consulté le 31 juillet 2025.
- [6] Site officiel de Open vSwitch, disponible sur : <https://www.openvswitch.org>, consulté le 2 août 2025.
- [7] Site officiel de Open LDAP, disponible sur : <https://www.openldap.org>, consulté le 2 août 2025.
- [8] Site officiel de Wireshark, disponible sur : <https://www.wireshark.org>, consulté le 2 août 2025.
- [9] Site officiel de Ntop, disponible sur : <https://www.ntop.org>, consulté le 2 août 2025.
- [10] Page officielle de l'installation de PacketFence », disponible sur : <https://www.packetfence.org/download.html>, consulté le 4 août 2025.

RAPPORT DE STAGE

Mise en place d'une solution open source pour la gestion d'accès réseau (NAC).

EEZZINE MONTASSAR
FORMATION HUMAINE
21/07/25 - 31/08/25