Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation
Université Cadi Ayyad
École Nationale des Sciences Appliquées de Marrakech
Ingénierie de la Cyberdéfense et des Systèmes de Télécommunications Embarqués

rapport : Déploiement d'un système NAC (Network Access Control) pour contrôler l'accès des postes

Réalisé par :

HIBA LAZZOUZI
IKRAM LAABOUKI
SOUKAINA BACHIR
KAOUTAR ELKISSANY
OUSSAMA BAGY

Encadré par :

Pr. ALI AZOUGAGHE

Année universitaire 2025-2026

REMERCIEMENTS

Nous tenons à exprimer notre sincère gratitude à toutes les personnes qui ont apporté, de manière directe ou indirecte, leur aide à la réalisation de ce projet. Mené dans le cadre du module Protocoles de Sécurité et Sécurité des Réseaux et des Communications, ce travail n'aurait pas abouti sans le soutien constant et l'implication de nombreux contributeurs.

Nous exprimons notre reconnaissance la plus profonde à Monsieur le Professeur Ali Azougaghe, encadrant de ce projet. Sa disponibilité, la précision de ses remarques et la qualité de son accompagnement ont été déterminantes dans l'avancement de notre étude. Grâce à sa vision claire, ses explications toujours pertinentes et son exigence scientifique, nous avons pu aborder sereinement les aspects techniques et théoriques les plus complexes.

Nos remerciements s'adressent également à l'ensemble des enseignants du département Génie Cyberdéfense et Systèmes de Télécommunications Embarqués (GCDSTE). Leur engagement, leur expertise et leur sens du partage ont fortement contribué au développement de nos compétences et à l'enrichissement de notre formation. Nous remercions aussi le personnel administratif de l'ENSA de Marrakech pour son efficacité et son soutien dans les différentes démarches liées au projet.

Nous souhaitons également saluer nos camarades et collègues de promotion. Leurs échanges, leur esprit d'entraide et la dynamique collaborative qui a animé nos travaux ont grandement facilité la progression du projet. Les discussions, les idées partagées et la solidarité dont chacun a fait preuve ont représenté un véritable atout tout au long de cette expérience.

Enfin, nous adressons une pensée particulière à nos familles et à toutes les personnes qui nous ont soutenus moralement. Leur patience, leur encouragement et leur confiance ont été une source précieuse de motivation, nous accompagnant durant toute la durée de ce travail

À toutes celles et ceux qui ont, de près ou de loin, contribué à la réussite de ce projet, nous exprimons notre profonde reconnaissance. Leur appui a constitué un environnement propice à l'apprentissage, au dépassement de soi et à la réussite de ce travail académique.

RÉSUMÉ

Dans le cadre de ce projet, nous avons conçu et déployé une solution de contrôle d'accès réseau (Network Access Control – NAC) afin de renforcer la sécurité du réseau et de maîtriser l'accès des utilisateurs ainsi que des équipements. Le NAC constitue aujourd'hui un élément essentiel pour les organisations, car il permet de limiter les connexions non autorisées, de détecter les équipements potentiellement compromis et d'appliquer des politiques de sécurité basées sur le niveau de conformité des machines.

Pour mettre en œuvre cette architecture, nous avons utilisé PacketFence, une solution NAC open-source intégrant des services clés tels que DHCP, DNS et RADIUS. L'ensemble de l'environnement a été déployé dans GNS3 à l'aide de machines virtuelles sous VMware, permettant de reproduire une infrastructure réseau réaliste. Trois VLANs ont été définis afin d'assurer une segmentation fonctionnelle du réseau : un VLAN Registration réservé aux nouveaux appareils, un VLAN Isolation pour les machines non conformes ou présentant un risque, et un VLAN Production dédié aux postes approuvés et autorisés.

La topologie du projet repose sur un switch d'accès, un switch core, un serveur PacketFence ainsi que plusieurs machines clientes, dont un PC utilisateur, deux postes Kali Linux et un scanner réseau. Cette organisation offre une structure claire et segmentée facilitant l'application des politiques NAC. PacketFence interagit avec les équipements réseau et les outils de sécurité afin d'évaluer le statut des machines et de contrôler leur accès en fonction de leur niveau de conformité.

Pour la vérification de conformité, nous avons intégré Nessus, un outil d'analyse de vulnérabilités, permettant d'évaluer l'état de sécurité des postes clients. Les scénarios de test réalisés ont notamment permis d'observer le comportement du système face à une machine inconnue, une machine non conforme ou un poste approuvé.

Les résultats obtenus démontrent l'efficacité de la solution mise en place. L'architecture NAC déployée assure une gestion intelligente de l'authentification et la vérification de letat de les appareils essayent de se connecter au réseau. Ce projet a permis de valider la pertinence de l'utilisation d'un NAC associé à un outil de conformité, tout en offrant une compréhension approfondie du fonctionnement des solutions de contrôle d'accès réseau professionnelles.

ABSTRACT

As part of this project, we designed and deployed a Network Access Control (NAC) solution to strengthen network security and manage access for both users and devices. NAC is now an essential component for organizations, as it helps limit unauthorized connections, detect potentially compromised devices, and apply security policies based on the compliance level of machines.

To implement this architecture, we used PacketFence, an open-source NAC solution that integrates key services such as DHCP, DNS, and RADIUS. The entire environment was deployed in GNS3 using virtual machines on VMware, allowing us to reproduce a realistic network infrastructure. Three VLANs were defined to ensure functional network segmentation: a Registration VLAN dedicated to new devices, an Isolation VLAN for non-compliant or risky machines, and a Production VLAN for approved and authorized endpoints.

The project topology is based on an access switch, a core switch, a PacketFence server, and several client machines, including a user PC, two Kali Linux systems, and a network scanner. This organization provides a clear and segmented structure that facilitates the application of NAC policies. PacketFence interacts with the network equipment and security tools to evaluate the status of devices and control their access according to their compliance level.

For compliance verification, we integrated Nessus, a vulnerability scanning tool that assesses the security state of client machines. The test scenarios performed allowed us to observe how the system behaves when facing an unknown device, a non-compliant machine, or an approved workstation.

The results obtained demonstrate the effectiveness of the implemented solution. The deployed NAC architecture ensures intelligent authentication management and verification of the state of devices attempting to connect to the network. This project validated the relevance of using a NAC combined with a compliance tool, while providing an in-depth understanding of how professional network access control solutions operate.

TABLE DE MATIERE

TABLE DE FIGURES

Glossaire

- **AAA (Authentication, Authorization, Accounting) :** Ensemble de mécanismes permettant d'authentifier un utilisateur, d'autoriser ses actions et d'enregistrer son activité sur le réseau.
- **MAC (Media Access Control)** : Identifiant unique attribué à chaque interface réseau. Souvent utilisée dans les mécanismes de contrôle d'accès (MAC Authentication).
- **NAC(Network Access Control)** : permettant de contrôler l'accès au réseau.
- DHCP (Dynamic Host Configuration Protocol) : Protocole permettant d'attribuer automatiquement une adresse IP et d'autres paramètres réseau aux clients.
- **DNS (Domain Name System)** : Système de résolution de noms permettant de traduire des noms de domaine en adresses IP.
- **RADIUS (Remote Authentication Dial-In User Service)**: Protocole d'authentification utilisé par PacketFence pour valider les utilisateurs et contrôler l'accès au réseau.
- **IP (Internet Protocol)**: Identifiant unique d'un appareil sur le réseau (ex : 192.168.1.10), permet la communication entre les machines.
- **SNMP (Simple Network Management Protocol)** : Protocole utilisé pour gérer et monitorer les équipements réseau (switch, AP…).
- **EAP (Extensible Authentication Protocol)**: Méthodes d'auth 802.1X (PEAP, EAP-TLS…).
- **PEAP (Protected Extensible Authentication Protocol):** est une méthode d'authentification utilisée dans le 802.1X pour sécuriser l'accès réseau (WiFi ou filaire).
- **TLS (Transport Layer Security)** : est un protocole de chiffrement utilisé pour sécuriser les communications sur un réseau.
- **SVI (Switched Virtual Interface)** : une SVI est une interface virtuelle créée sur un switch pour permettre la communication entre les VLANs.
- **CoA (Change of Authorization)** : est une fonction RADIUS qui permet à PacketFence (ou tout serveur NAC) de changer dynamiquement les droits d'un utilisateur déjà connecté sans qu'il ne débranche son câble ni ne se reconnecte.
- **OVF (Open Virtualization Format):** est un format standard de fichier utilisé pour distribuer et déployer des machines virtuelles.
- **API (Application Programming Interface) :** est une interface qui permet à deux applications ou systèmes de communiquer automatiquement entre eux, sans intervention humaine.
- **MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2)** : est une méthode d'authentification basée sur un challenge/réponse qui permet à un utilisateur de s'authentifier avec un nom d'utilisateur et un mot de passe. Elle est souvent utilisée à l'intérieur de PEAP dans les environnements 802.1X.

INTRODUCTION GÉNÉRALE

La cybersécurité occupe aujourd'hui une place essentielle dans les infrastructures informatiques. Avec la multiplication des attaques, des appareils personnels, et des connexions non contrôlées, les réseaux d'entreprise sont exposés à des risques croissants. Dans ce contexte, le Network Access Control (NAC) est devenu un mécanisme incontournable pour garantir que seuls les utilisateurs et équipements autorisés, conformes et fiables puissent accéder aux ressources internes. Le NAC permet de contrôler, surveiller et sécuriser l'accès réseau, en appliquant des politiques de sécurité strictes basées sur l'authentification, la conformité et la segmentation.

L'objectif principal de ce projet est de mettre en place une solution NAC opérationnelle en utilisant PacketFence, une plateforme open-source largement adoptée pour la gestion centralisée du contrôle d'accès réseau. Pour assurer une segmentation efficace et un contrôle optimal du trafic, l'infrastructure repose sur la gestion des VLANs et des règles de filtrage configurées directement au niveau du switch et du serveur PacketFence. L'environnement est complété par un switch L2, une machine Kali Linux simulant un poste client, ainsi qu'un scanner de vulnérabilités permettant d'évaluer l'état de conformité des machines au sein du réseau.

Ce projet s'inscrit dans une démarche pédagogique visant à comprendre le fonctionnement global d'un système NAC, ses composants, ses contraintes et ses scénarios d'application. Il permet de visualiser concrètement comment un appareil inconnu est détecté, isolé, authentifié et éventuellement autorisé, grâce à l'interaction entre PacketFence et les équipements réseau configurés pour appliquer les règles d'accès et de segmentation.

La méthodologie suivie comprend :

- L'analyse des besoins du NAC ;
- La conception d'une topologie basée sur les VLANs ;
- L'implémentation, incluant l'installation de PacketFence et la configuration du switch ;
- Les tests, réalisés sur plusieurs scénarios.

Ce rapport est structuré de manière à présenter d'abord les concepts fondamentaux du NAC, puis les technologies utilisées dans notre projet. Ensuite, une large partie est consacrée à la réalisation pratique, à la configuration détaillée des différents composants et à l'analyse des résultats obtenus. Enfin, une conclusion générale met en évidence les apports, les limites et les perspectives d'amélioration du système mis en place.

Chapitre I:
Contexte Général

1.1 Introduction

Ce chapitre expose le cadre général dans lequel s'inscrit notre projet. Il présente d'abord l'environnement d'accueil, à travers l'établissement et la filière, avant d'aborder la problématique à laquelle répond notre travail. Enfin, il met en lumière les objectifs et la solution envisagée pour répondre aux besoins identifiés.

1.2 Présentation de l'ENSA

L'École Nationale des Sciences Appliquées (ENSA) de Marrakech, fondée en 2000, est un établissement d'enseignement supérieur d'ingénierie relevant de l'Université Cadi Ayyad (UCA). Elle a pour mission de former des cadres ingénieurs hautement qualifiés, en s'appuyant sur une pédagogie innovante et orientée vers l'ouverture professionnelle, internationale et culturelle.

L'ENSA Marrakech occupe une place stratégique dans le paysage marocain de la formation d'ingénieurs. Elle contribue de manière significative au développement de compétences techniques et managériales, grâce à un environnement éducatif fondé sur la rigueur, l'excellence et la collaboration. L'établissement met également un point d'honneur à instaurer un climat de confiance entre étudiants, enseignants et personnel administratif, favorisant ainsi une dynamique d'apprentissage harmonieuse et efficace.

L'école propose cinq filières d'ingénierie majeures :

- Génie Informatique ;
- Génie Industriel et Logistique ;
- Génie Réseaux, Systèmes et Services Programmables ;
- Génie Systèmes Électroniques Embarqués et Commande des Systèmes ;
- Génie Cyber-Défense et Systèmes de Télécommunication Embarqués.

Figure 1: logo de ENSA MARRAKECH

1.3 Présentation de GCDSTE

La filière Génie Cyberdéfense et Système de Télécommunications Embarquée (GCDSTE) de l'ENSA-M a pour objectif de former des ingénieurs compétents dotés de solides connaissances scientifiques. Cette formation intègre des méthodes et des techniques avancées pour assurer la sécurité et gérer les risques liés aux systèmes d'information. De plus, elle vise à habiliter les étudiants à concevoir des systèmes de télécommunications embarqués. L'accent est mis sur la préparation de chaque élève ingénieur aux méthodes et outils nécessaires pour contrer la cybercriminalité, résoudre les failles des systèmes

Figure 2: logo de GCDSTE

1.4 Présentation du projet:

1.4.1.Problématique:

La sécurisation des réseaux informatiques est devenue un enjeu majeur dans le contexte actuel, où la multiplication des appareils connectés et des utilisateurs augmente les risques d'intrusion et de compromission des systèmes. Dans de nombreuses organisations, les réseaux sont accessibles à différents types d'appareils, tels que des ordinateurs portables, smartphones, tablettes ou objets connectés, qui ne sont pas toujours conformes aux normes de sécurité. Cette diversité rend la gestion des accès et la protection des données particulièrement complexes.

De plus, les méthodes traditionnelles de contrôle d'accès, basées uniquement sur des mots de passe ou des permissions statiques, ne permettent pas de détecter les appareils compromis ni de réagir en temps réel face aux menaces. Un utilisateur ou un appareil infecté peut ainsi se connecter au réseau, propager des logiciels malveillants, accéder à des informations sensibles ou perturber le fonctionnement des systèmes. Cette situation met en évidence la nécessité d'une solution capable de contrôler et sécuriser les accès réseau de manière dynamique et intelligente.

Enfin, le défi réside dans la mise en place d'un mécanisme qui puisse authentifier, évaluer et contrôler l'accès de chaque appareil ou utilisateur avant qu'il ne rejoigne le réseau. Il s'agit de combiner la vérification de la conformité aux politiques de sécurité, la surveillance en temps réel et la gestion automatique des autorisations pour réduire les risques d'intrusion et assurer la continuité des services. La problématique centrale du projet est donc : comment sécuriser efficacement un réseau tout en permettant un accès contrôlé et fluide aux utilisateurs légitimes ?

1.4.2.Solution proposée:

Le projet propose la mise en place d'une solution NAC pour sécuriser l'accès au réseau de manière dynamique et automatisée. Cette solution permet de :

- Identifier et authentifier chaque appareil ou utilisateur tentant d'accéder au réseau.
- Vérifier que l'appareil respecte les politiques de sécurité (antivirus à jour, correctifs installés, configuration conforme).

Grâce à cette approche, le réseau est protégé contre les accès non autorisés, tout en garantissant un environnement sûr et contrôlé pour les utilisateurs légitimes. La solution NAC mise en œuvre dans le projet illustre ainsi une stratégie proactive pour renforcer la sécurité des infrastructures réseau.

1.4.3 Objectifs du projet

Le projet a pour principal objectif de renforcer la sécurité des réseaux en mettant en place une solution NAC (Network Access Control) adaptée aux besoins d'une organisation. Plus précisément, les objectifs sont :

- Authentifier chaque appareil : garantir que seuls les utilisateurs et équipements autorisés puissent accéder au réseau.
- Évaluer la conformité des dispositifs : vérifier que chaque appareil respecte les politiques de sécurité définies (antivirus à jour, correctifs appliqués, configuration sécurisée).

1.4.4 Structure du rapport

Le rapport est organisé pour présenter le projet NAC de manière progressive et claire :

- Chapitre I : Contexte Général – Présentation de l'ENSA, de l'encadrant, du projet, de la problématique, de la solution et des objectifs.
- Chapitre II : Notions Théoriques – Concepts des réseaux et de la sécurité, architecture NAC, PacketFence, rôle du switch et tests préliminaires.
- Chapitre III : Implémentation et réalisation
- Conclusion Générale et Perspectives – Synthèse des travaux et recommandations pour l'avenir.

Cette structure permet au lecteur de suivre le projet du contexte général à la mise en œuvre pratique, de manière logique et concise.

1.4.5 Conclusion

Ce chapitre a permis de poser les bases du projet en présentant le contexte général, l'encadrant, la problématique rencontrée, la solution NAC envisagée ainsi que les objectifs poursuivis. Il met en évidence l'importance d'un contrôle d'accès réseau efficace pour sécuriser les infrastructures informatiques et prévenir les risques liés aux accès non autorisés.

La compréhension de ces éléments constitue un préalable essentiel avant de passer à l'étude approfondie des concepts de NAC et à l'implémentation pratique de la solution, qui seront détaillés dans les chapitres suivants.

Chapitre II : Notions Théoriques

2.1 Introduction

Le contrôle d'accès réseau (NAC) repose sur un ensemble de concepts et de technologies fondamentales issues des domaines des réseaux informatiques et de la sécurité. Ce chapitre a pour objectif de détailler ces notions théoriques essentielles, permettant de contextualiser le choix et le fonctionnement de notre solution, PacketFence. Nous aborderons les bases des réseaux, les principes de la sécurité, l'architecture globale d'un système NAC, et le rôle crucial de composants spécifiques comme les VLANs, RADIUS, et le rôle du switch. La compréhension de ces concepts est indispensable pour appréhender les choix de conception et de configuration qui seront présentés dans les chapitres suivants.

2.2 Introduction aux notions fondamentales des réseaux

La mise en œuvre d'une solution NAC nécessite une solide compréhension des concepts de base des réseaux informatiques, en particulier ceux qui régissent la connectivité et la segmentation.

2.2.1 Le Modèle OSI

Le Network Access Control opère principalement sur les couches basses du modèle OSI (Open Systems Interconnection) :

- **Couche 1 (Physique) :** Gère la transmission physique des données (câbles, signaux). Le NAC se déclenche lorsque le support physique est connecté.
- **Couche 2 (Liaison de Données) :** Utilise les adresses MAC (Media Access Control) pour l'adressage local. Le NAC utilise l'adresse MAC pour identifier l'équipement et la technologie VLAN (Virtual Local Area Network) pour segmenter le réseau logiquement à ce niveau.
- **Couche 3 (Réseau) :** Utilise les adresses IP pour le routage et l'adressage global. L'attribution dynamique d'adresses IP (via DHCP) à partir d'un pool dépendant du VLAN est une conséquence directe de la politique NAC.

2.2.2 Le Rôle de la Commutation (Switching)

Le switch (commutateur) est l'élément central pour la mise en œuvre du NAC :

- **Passerelle d'Accès :** Le switch agit comme le point d'entrée pour les dispositifs filaires, ce qui en fait l'endroit idéal pour appliquer la politique de contrôle d'accès.
- **Support du 802.1X :** La capacité du switch à supporter la norme IEEE 802.1X est fondamentale. Cette norme permet d'ouvrir ou de bloquer l'accès à un port en fonction du résultat d'une authentification. Il est l'Authenticator dans l'architecture NAC.

- **VLAN Dynamique :** Les switches modernes doivent être capables d'attribuer dynamiquement un VLAN à un port une fois l'authentification validée par le serveur RADIUS (PacketFence). Ceci permet de garantir que, qu'il soit authentifié ou en quarantaine, le client est placé dans le segment réseau approprié.

2.2.3 Adressage et Segmentation Logique

La gestion des adresses IP et la segmentation sont vitales pour l'isolation et l'application des politiques :

- **DHCP (Dynamic Host Configuration Protocol) :** Le serveur DHCP est souvent géré par PacketFence ou est en interaction étroite avec lui. L'adresse IP attribuée à un client estdéterminée par le VLAN dans lequel il est placé par le NAC.
- **Segmentation par VLAN :** Les VLANs permettent de diviser un réseau physique unique en plusieurs domaines de diffusion logiques. Par exemple, le VLAN 10 sera dédié auxutilisateurs validés, et le VLAN 20 à la quarantaine. Cette isolation logique est la base dela remédiation sécurisée.

2.3 Notion de sécurité réseau

La sécurité réseau est un domaine critique visant à protéger les ressources et les données contre les accès non autorisés, les modifications, et la destruction. Le Network Access Control (NAC) est une composante essentielle de la stratégie de sécurité moderne, car il ne se contente pas d'appliquer la sécurité au périmètre, mais l'étend à l'intérieur même du réseau.

2.3.1 Le Modèle AAA (Authentification, Autorisation, Comptabilité)

Le NAC est la mise en œuvre pratique du modèle AAA, un pilier fondamental de la sécurité d'accès. Ce modèle définit les trois phases par lesquelles un utilisateur ou un dispositif doit passer pour se connecter au réseau :

1. **Authentification (Authentication) :**

- Objectif : Vérifier l'identité de l'entité qui tente d'accéder au réseau (l'utilisateur ou la machine).
- Méthodes : Utilisation de 802.1X (certificats ou identifiants), portail captif (identifiants web), ou adresse MAC (pour certains appareils IOT/legacy). PacketFence agit comme le serveur qui valide ces identités, souvent en interrogeant un annuaire externe (comme un Active Directory simulé dans notre cas).

2. Autorisation (Authorization) :

- Objectif : Déterminer le niveau d'accès accordé à l'entité authentifiée en fonction des politiques de sécurité.
- Rôle du NAC : C'est le cœur du NAC. L'autorisation est dynamique : si la machine est conforme (patchée, avec antivirus), elle reçoit un accès complet (VLAN d'accès). Sielle est non-conforme, elle est autorisée à un accès restreint (VLAN de quarantaine). L'autorisation est transmise au switch via les attributs RADIUS.

3. Comptabilité (Accounting) :

- Objectif : Enregistrer les informations relatives à l'utilisation des ressources réseau par l'entité (heure de connexion/déconnexion, durée, volume de données).
- Rôle de PacketFence : PacketFence maintient ces journaux, qui sont cruciaux pourl'audit de sécurité, le traçage d'activité et l'analyse post-incident.

2.4 Architecture NAC (Network Access Control)

L'architecture de contrôle d'accès réseau (NAC) repose sur un modèle d'interaction à trois entités. Ce modèle permet de centraliser la prise de décision tout en déléguant l'exécution du contrôle d'accès au niveau du point d'entrée réseau.

2.4.1 Les Trois Rôles de l'Architecture NAC

L'interaction du NAC s'articule autour de ces trois éléments :

1. Le Supplicant (Client) :

- Définition : C'est l'entité qui demande l'accès au réseau. Il s'agit de tout appareil connecté (PC portable, smartphone, imprimante, etc.).
- Rôle : Il est responsable de fournir les informations d'identification (identifiant/mot de passe, certificat) nécessaires à l'authentification. Dans le contexte du 802.1X, le Supplicant exécute un client logiciel pour communiquer avec l'Authenticator.

2. L'Authenticator (Point d'Accès) :

- Définition : C'est le dispositif qui contrôle l'accès au réseau physique. Dans notre cas, il s'agit du switch de niveau 2 ou 3.
- Rôle : Il sert d'intermédiaire transparent entre le Supplicant et le Serveur de Politique. Il reçoit la demande d'accès du Supplicant et la transmet au Serveur de Politique. Suite à la réponse reçue, il est chargé d'appliquer la décision, par exemple en ouvrant le port ou en attribuant un VLAN spécifique.

3. Le Serveur de Politique (Serveur NAC) :

- Définition : C'est le cœur intelligent du système, le cerveau de la solution. Dans notre projet, ce rôle est tenu par PacketFence.
- Rôle : Il est le serveur RADIUS (Remote Authentication Dial-In User Service) qui exécute les fonctions AAA. Il vérifie l'identité, évalue la posture de sécurité du client (Health Check), prend la décision finale d'accès (autoriser, rejeter, mettre en quarantaine) et renvoie les attributs de politique (comme le nom du VLAN) à l'Authenticator.

2.4.2 Flux de Communication

Le processus type de connexion s'effectue comme suit :

- Le Supplicant se connecte au port du Switch (Authenticator).
- L'Authenticator bloque le port et envoie une requête d'identité au Supplicant.
- Le Supplicant fournit les identifiants.
- L'Authenticator encapsule ces identifiants et les envoie au Serveur NAC/RADIUS pour vérification.
- Le Serveur NAC vérifie l'identité et la conformité, puis renvoie la décision (Access-Accept ou Access-Reject) et le VLAN approprié.
- L'Authenticator applique la décision en ouvrant le port et en changeant dynamiquement le VLAN si nécessaire.

2.5 Concepts autour de PacketFence : VLAN, RADIUS, portail captif

PacketFence est une solution de Network Access Control (NAC) open-source qui agrège et coordonne plusieurs technologies standard pour effectuer le contrôle d'accès dynamique. Le fonctionnement de PacketFence est intrinsèquement lié à l'utilisation du protocole RADIUS, des VLANs et du concept de portail captif.

2.5.1 RADIUS (Remote Authentication Dial-In User Service)

RADIUS est le protocole standard (IETF) pour le service AAA (Authentification, Autorisation, Comptabilité) dans les environnements réseau.

- **Rôle dans le NAC :** PacketFence agit comme le serveur RADIUS. Il reçoit les requêtes d'accès (Access-Request) du switch (Authenticator) contenant les informations du client. Après avoir validé l'identité et la posture, il envoie une réponse (Access-Accept, Access- Reject ou Access-Challenge).

- **Attributs de Réponse :** Le pouvoir de PacketFence réside dans l'utilisation des attributs VSA (Vendor-Specific Attributes) de la réponse Access-Accept. Ces attributs sont utilisés pour t ransmettre au switch des instructions spécifiques, notamment le nom ou l'ID du VLAN à attribuer au client.

2.5.2 VLAN (Virtual Local Area Network)

Le VLAN est le mécanisme d'exécution de la politique de segmentation du NAC.

- **Segmentation Dynamique :** Au lieu d'avoir des ports de switch configurés statiquement pour un seul VLAN, PacketFence utilise l'attribution dynamique de VLAN (Dynamic VLAN Assignment).
  - VLAN de Quarantaine : Utilisé pour les clients non authentifiés ou non-conformes. Il restreint l'accès uniquement à PacketFence (pour le portail captif ou la remédiation).
  - VLAN d'Accès : Attribué aux clients authentifiés et jugés conformes, leur accordant un accès complet au réseau.
- **Fonctionnement :** Lorsqu'un client se connecte, le switch le place initialement dans un VLAN de "démarrage" ou de "non-authentifié". Une fois que PacketFence prend une décision, il ordonne au switch de déplacer le client vers le VLAN cible approprié.

2.5.3 Portail Captif (Captive Portal)

Le portail captif est une méthode d'authentification web flexible, souvent utilisée comme mécanisme de secours ou pour les invités.

- **Scénario d'Usage :** Il est privilégié pour les dispositifs qui ne supportent pas l'authentification 802.1X (comme certains smartphones ou les invités).
- **Mécanisme de Redirection :** Lorsqu'un client se connecte et n'est pas authentifié par RADIUS, PacketFence utilise son module de portail captif pour intercepter le trafic HTTP/HTTPS et le rediriger vers une page web d'authentification hébergée sur le serveur.
- **Enregistrement :** Une fois que l'utilisateur entre ses identifiants sur le portail captif, PacketFence les valide (via LDAP ou sa base de données interne) et envoie la commande de re-authentification au switch, qui applique alors le VLAN d'accès.

En combinant le protocole RADIUS pour la décision, les VLANs pour l'isolation et le portail captif pour la flexibilité, PacketFence fournit une solution complète pour un contrôle d'accès réseau granulaire et efficace.

2.6 Rôle du switch dans la solution NAC

Si PacketF ence est le "cerveau" qui prend les décisions d'accès, le switch de réseau (ou point d'accès sans fil) est l'"organe d'exécution" qui applique ces décisions. Il est l'Authenticator du modèle NAC. La réussite de l'implémentation du NAC dépend directement des capacités et de la configuration du switch.

2.6.1 Fonction de Point de Contrôle

Le switch est le premier et le dernier point de défense contre l'accès physique non autorisé.

- **Contrôle d'Accès Basé sur les Ports (802.1X) :** Le switch est configuré pour exiger une authentification sur chaque port. Tant que l'authentification n'est pas validée, le port reste dans un état non autorisé, ne permettant que le trafic EAP (Extensible Authentication Protocol) entre le Supplicant et l'Authenticator.
- **Support RADIUS :** Le switch doit être configuré pour communiquer de manière sécurisée (via une clé secrète partagée) avec le serveur RADIUS (PacketFence). Il envoie les requêtes d'authentification et attend la réponse pour savoir quelle action entreprendre.

2.6.2 Application de la Politique Dynamique

Le rôle le plus critique du switch est d'appliquer les politiques d'accès que lui dicte le serveur PacketFence.

- **Attribution Dynamique de VLAN (Dynamic VLAN Assignment) :** Après une authentification réussie ou échouée, PacketFence envoie une réponse RADIUS (Access- Accept ou Access-Reject) contenant les attributs spécifiques du fournisseur (VSA) qui précisent l'ID ou le nom du VLAN à attribuer au port. Le switch modifie alors la configuration de son port en temps réel pour placer le client dans le VLAN spécifié (Accès, Quarantaine, Invité).
- **Contrôle d'Accès Basé sur l'Adresse MAC (MAB) :** Pour les dispositifs qui ne supportent pas le 802.1X (ex: caméras IP, certaines imprimantes), le switch peut utiliser le MAB. Il envoie l'adresse MAC du dispositif à PacketFence, qui décide de l'accès en fonction d'une liste blanche ou d'une politique de profilage, avant d'appliquer l'attribution de VLAN dynamique.

2.6.3 Interconnexion et Supervision

Le switch est également vital pour la topologie générale :

- **Détection d'Événements :** Il est capable de signaler les événements de connexion/ déconnexion à PacketFence (via RADIUS Accounting ou des mécanismes SNMP/Trap), permettant au serveur de maintenir une vision en temps réel de l'état du réseau.
- **Isolation :** En appliquant les VLANs de quarantaine, le switch assure l'isolation stricte des paquets, empêchant la communication des clients non-conformes avec les segments sensibles du réseau.

2.7 Conclusion

Ce chapitre a permis d'établir les fondations théoriques indispensables à la compréhension de notre projet NAC (Network Access Control). Nous avons détaillé le rôle des couches basses des réseaux, souligné l'importance du modèle AAA (Authentification, Autorisation, Comptabilité) dans la stratégie de sécurité, et décrit l'architecture fondamentale du NAC.
En nous focalisant sur les outils de notre solution, nous avons explicité le fonctionnement du protocole RADIUS et le mécanisme d'isolation par VLAN dynamique par PacketFence.
Forts de ces connaissances, nous sommes maintenant prêts à passer au chapitre suivant : Implémentation et Réalisation, où ces concepts théoriques seront traduits en une topologie réseau concrète et des diagrammes de fonctionnement précis.

Chapitre III: Implémentation et Réalisation

1. Introduction

Ce chapitre marque la transition cruciale de la phase de conception à l'étape de réalisation pratique. Il a pour objectif de détailler l'ensemble des procédures et configurations techniques qui ont permis de mettre en œuvre l'architecture réseau et la solution de sécurité définies précédemment. Nous allons présenter la méthodologie utilisée pour déployer les équipements, configurer les composants clés (tels que le pare-feu, les commutateurs et les serveurs), et établir la connectivité et la segmentation logique souhaitées. La réalisation inclut non seulement la configuration initiale de l'infrastructure, mais aussi les tests de validation pour s'assurer que les exigences de performance, de disponibilité et, surtout, de sécurité du système sont pleinement satisfaites.

2. Architecture

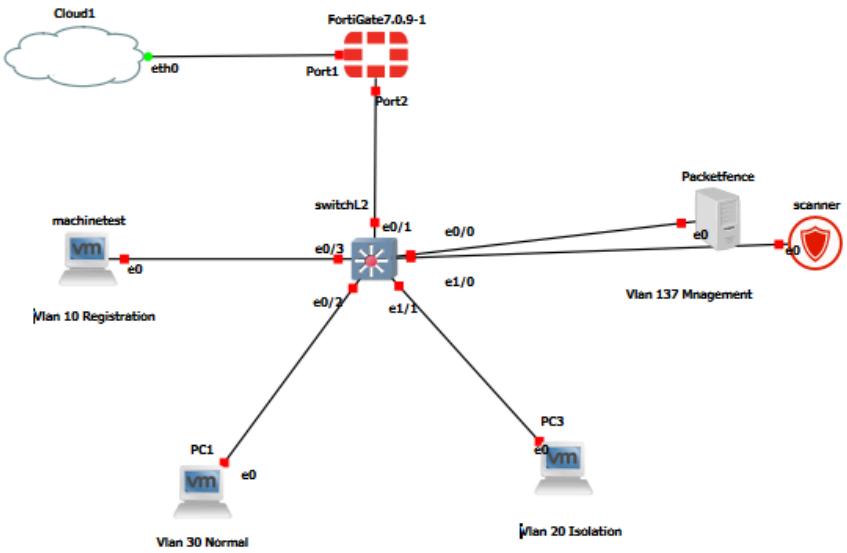


Figure 3: topologie du projet

La maquette a été conçue pour reproduire une architecture de sécurité centrée sur le Contrôle d'Accès Réseau (NAC) et la micro-segmentest composée des éléments suivants :

FortiGate 7.0.9-1 (Pare-feu) : Joue le rôle de point d'application des politiques de sécurité. Ses fonctions incluent le filtrage du trafic, la segmentation (routage inter-VLANs) et l'action de relais RADIUS ou de Network Access Device (NAD) pour interroger le serveur d'authentification. Il assure la passerelle vers l'extérieur (Cloud1).
SwitchL2 (Commutateur) : Point de convergence du réseau interne, gérant la couche 2. Il est configuré pour supporter la segmentation via VLANs (VLAN 10 Registration, VLAN 20 Isolation, VLAN 30 Normal, VLAN 137 Management) et pour effectuer le changement dynamique de port lors de la réussite de l'authentification (NAC).

Packetfence (Serveur/Appliance NAC) : Représenté dans le VLAN 137 Management, cet élément est le cœur de la solution AAA. Il gère les fonctions de serveur RADIUS, évalue les politiques d'accès, et orchestre le contrôle d'accès des machines clientes.

Machines Clientes (VMs) :

- machinetest (VLAN 10 Registration) : Machine cliente clé pour tester le processus initial d'accès et d'authentification (simulant un poste non connu).
- PC1 (VLAN 30 Normal) : Machine cliente représentant un poste authentifié et standard pour valider les accès normaux.
- PC3 (VLAN 20 Isolation) : Machine cliente utilisée pour simuler un état de quarantaine ou d'isolement suite à un échec ou un non-respect de politique.

3. Environnements de travail & composants utilisés

3.1. Outil de virtualisation VMware workstation

Figure 4: Logo de vmware

VMware Workstation est un Hyperviseur de bureau (Desktop Hypervisor) qui permet l'exécution fluide de machines virtuelles (VM), de conteneurs, et de clusters Kubernetes. Il est un outil polyvalent qui offre des fonctionnalités organisationnelles avancées, notamment le dossier d'inventaire, qui facilite la gestion (activation/désactivation) d'un nombre illimité de VMs comme une seule entité. Cette capacité est essentielle pour les tests de scénarios complexes de type client-serveur. De plus, Workstation permet de superviser les déploiements vSphere, offrant une visibilité dans les environnements hybrides.

VMware Server est une autre solution de virtualisation qui excelle spécifiquement dans la création, l'édition et l'exécution de machines virtuelles.

VMware Server est une autre solution de virtualisation qui excelle spécifiquement dans la création, l'édition et l'exécution de machines virtuelles.

3. 2 Logiciel de simulation GNS3

Figure 5: Logo de GNS3

GNS3 (Graphical Network Simulator-3) est un logiciel d'émulation et de simulation de réseau gratuit et open source. Il permet aux professionnels des réseaux, aux ingénieurs et aux étudiants de concevoir, construire et tester des réseaux complexes dans un environnement virtuel, sans nécessiter d'équipement physique coûteux.

3.3. FortiGate

Le FortiGate, développé par Fortinet, ne se contente pas d'être un simple pare-feu. Il s'agit d'une appliance de sécurité de type Pare-feu de Nouvelle Génération (NGFW) qui assure une protection complète et multicouche des réseaux informatiques.

Figure 6: Logo de Fortigate

3.4. Packetfence

Figure 7: Logo de Packetfence

PacketFence est une solution de Network Access Control (NAC) utilisée pour gérer, contrôler et sécuriser l'accès au réseau au sein d'une organisation.
Son rôle principal est de vérifier l'identité et la conformité des appareils avant de les autoriser à accéder au réseau interne.

Il fonctionne comme un système centralisé qui collecte les informations des équipements connectés, les authentifie et applique des règles de sécurité (rôles, VLAN, restrictions…). PacketFence permet de bloquer, isoler, ou autoriser un appareil en fonction de son statut ou de son niveau de conformité.
La solution s'intègre à un environnement réseau existant (switches, points d'accès WiFi, serveurs RADIUS, scanners de vulnérabilités…) et gère automatiquement les changements de VLAN ou les redirections vers un portail captif. PacketFence peut être déployé sur un serveur physique ou virtuel et offre une administration entièrement web, permettant une gestion centralisée des utilisateurs, des appareils et des politiques d'accès.

3.5. Nessus

Figure 8: Logo de Nessus

Nessus est un outil professionnel d'analyse de vulnérabilités conçu pour identifier les failles de sécurité présentes dans les systèmes, les serveurs, les réseaux et les applications d'une organisation. Développé par Tenable, il est largement utilisé dans le domaine de la cybersécurité pour renforcer la protection des infrastructures informatiques.

3.6. Kali linux

Figure 9: Logo de Kali

Kali Linux est une distribution Linux spécialisée dans la cybersécurité et le pentesting, conçue pour effectuer des tests d'intrusion, des audits de sécurité et l'analyse des vulnérabilités d'un système ou d'un réseau. Elle est développée et maintenue par Offensive Security.

4. **Configurations**:

4.1. Installation et configuration de PacketFence

La première étape de l'installation de PacketFence consiste à récupérer l'appliance virtuelle officielle fournie par les développeurs. L'image que nous utilisons montre précisément cette phase de téléchargement, essentielle pour préparer le déploiement de la solution dans notre environnement virtualisé.

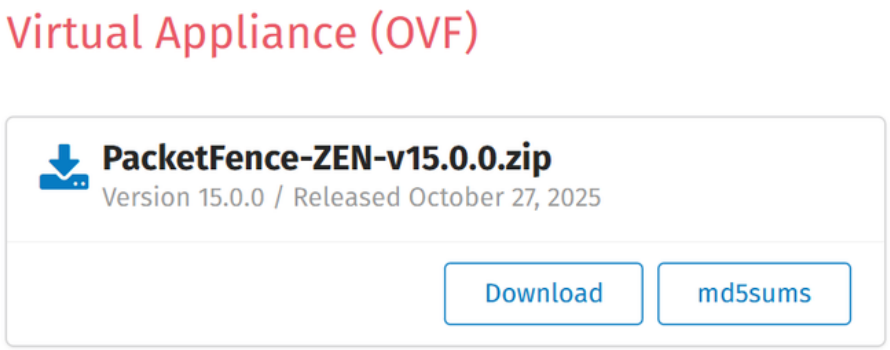


Figure 10: Appliance virtuelle

L'image illustre le téléchargement du fichier PacketFence-ZEN-v15.0.0.zip, qui correspond à l'appliance virtuelle prête à être importée dans un hyperviseur (par exemple VMware Workstation).

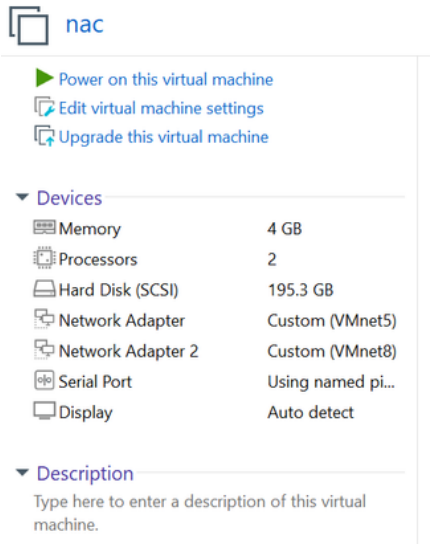


Figure 11: la configuration matérielle attribuée à la machine virtuelle.

Après l'importation de l'appliance PacketFence dans VMware Workstation, l'image ci-dessous présente la configuration matérielle initiale attribuée à la machine virtuelle. Ces paramètres définissent les ressources et les interfaces réseau nécessaires au bon fonctionnement du serveur NAC.

Après le téléchargement et l'importation du fichier OVF de l'appliance virtuelle Packetfence dans notre environnement de virtualisation, l'étape suivante consiste à démarrer la machine virtuelle et à se connecter à sa console. Une fois que le système d'exploitation basé sur Debian a terminé son initialisation, le message de bienvenue s'affiche immédiatement, nous fournissant l'information essentielle pour la suite : l'adresse IP de gestion du serveur. Dans notre cas, nous récupérons l'adresse 192.168.137.132 (sur le port 1443). On va ensuite utiliser cette URL (https://192.168.137.132:1443) à partir d'un navigateur sur une machine cliente (ou le poste de gestion) pour accéder à l'interface d'administration web de Packetfence, où l'ensemble des configurations logicielles du Contrôle d'Accès Réseau sera effectué.

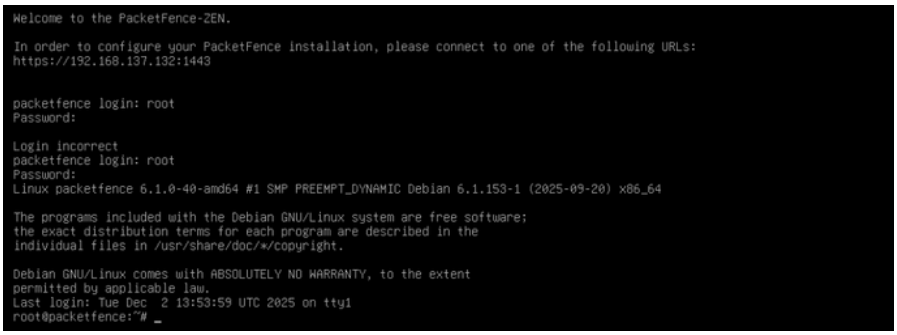


Figure 12: CLI de Packetfence

Une fois l'adresse IP de gestion 192.168.137.132 récupérée via la console, nous avons accédé à l'interface d'administration web sécurisée de Packetfence sur le port 1443 (https://192.168.137.132:1443). L'écran affiché représente l'étape 1 de l'assistant de configuration, dédiée aux Interfaces & Réseaux.

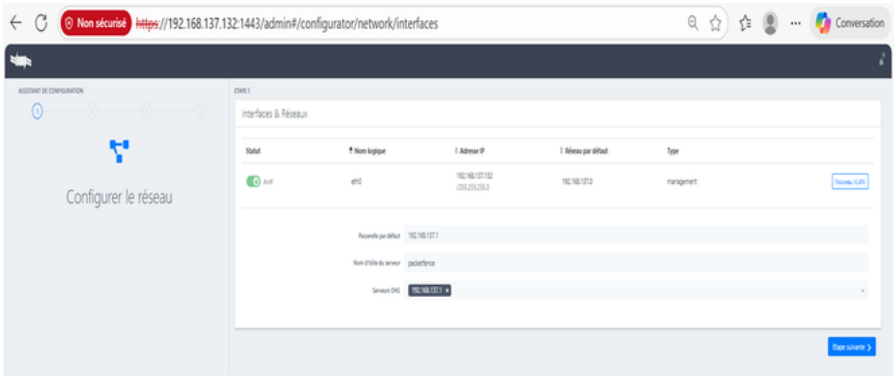


Figure 13: Interface virtuelle de Management

Une fois la vérification de la configuration réseau et de la passerelle (Étape 1) validée, on va ensuite passer à l'Étape 2 : Configurer Packetfence . Cette phase cruciale permet de finaliser l'installation logicielle et de définir les paramètres fondamentaux du serveur NAC avant de déclarer les équipements de la topologie.
Cette étape implique :

Base de Données : L'option de configuration automatique est sélectionnée pour initialiser une base de données MySQL locale, essentielle au fonctionnement du service et à la gestion des utilisateurs et des politiques.
Paramètres Généraux : Définition du nom d'hôte (packetfence) et des paramètres du système.

Administration et Sécurité : Le point le plus important est la création du compte Administrateur et l'attribution de son Mot de passe sécurisé. Ces identifiants sont le code d'accès qui sera utilisé pour toutes les modifications ultérieures des politiques de sécurité.

Après avoir défini tous les paramètres de base dans l'Étape 2, l'assistant de configuration de Packetfence passe à l'Étape 3 (Confirmation) pour récapituler et valider les mots de passe générés ou définis. Cette étape est essentielle pour la sécurité et la traçabilité.

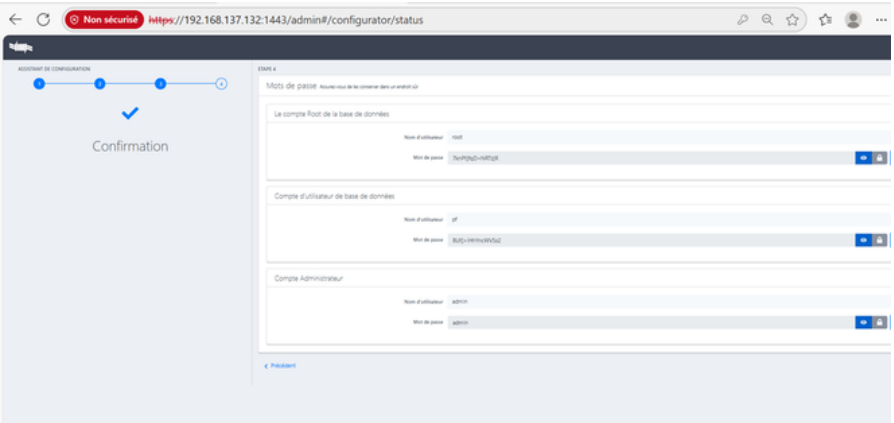


Figure 14: Validation des codes

Après la complétion des étapes d'installation et la définition du compte administrateur, l'accès à la plateforme de Contrôle d'Accès Réseau (NAC) se fait via la page de Connexion à l'administration de Packetfence. Nous utilisons l'URL sécurisée (https://192.168.137.132:1443/admin#/login) pour accéder à l'interface web. Il est alors nécessaire d'entrer le Nom d'utilisateur et le Mot de passe de l'administrateur, définis lors de l'Étape 3.

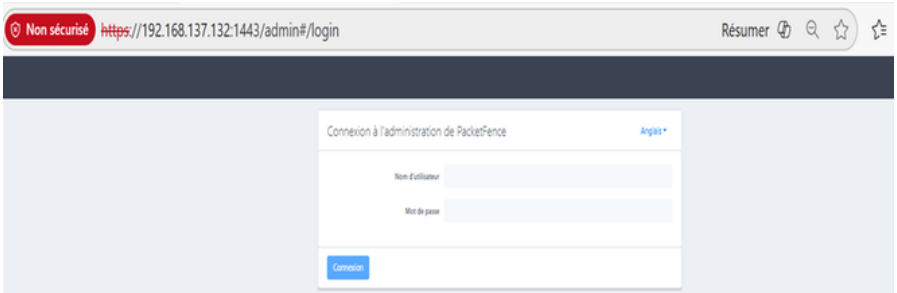


Figure 15: Page de connexion

4.1.1.Configuration des Interfaces et Réseaux dans Packetfence

Après s'être connecté à l'interface d'administration, la première étape logique dans la configuration du NAC est de déclarer les réseaux que Packetfence va contrôler. Cette étape est cruciale car elle permet à Packetfence de comprendre la segmentation de votre architecture.

- On crée l'interface de vlan 10 c'est vlan de Registration(vlan d'attente):

L'interface VLAN 10 est désignée comme Registration (ou VLAN d'attente). Son rôle est de servir de zone de pré-authentification pour toute machine (comme machinetest) qui se connecte pour la première fois ou qui n'est pas encore authentifiée.
Cette interface est donc la porte d'entrée où le processus d'authentification et de posture (vérification de conformité) est initialisé, avant que Packetfence ne décide du changement dynamique de VLAN vers la zone Isolation (VLAN 20) ou Normal (VLAN 30).

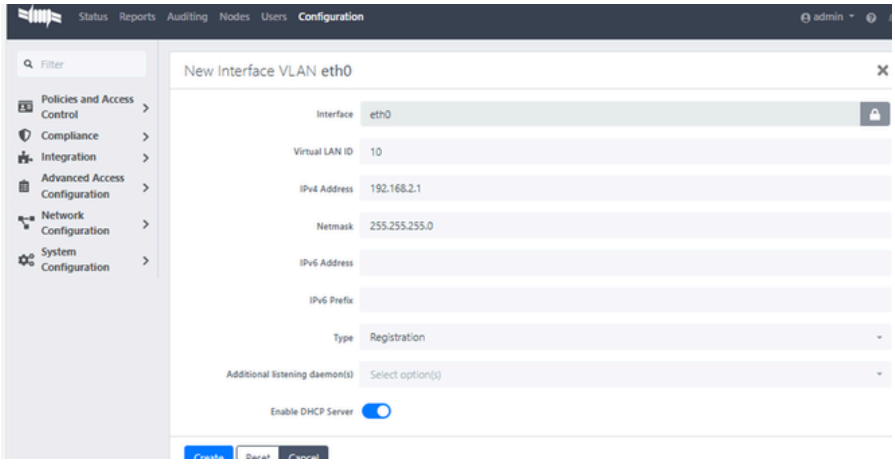


Figure 16: Création de l'interface vlan de Registration

- On crée l'interface de vlan 30 c'est Vlan de Normal:

L'interface VLAN 30 est la zone d'accès normal du réseau. Son rôle est de servir de zone post-authentification pour toute machine (comme PC1 et machinetest après validation) qui a réussi le processus de contrôle d'accès. Lorsqu'un poste est placé dans ce VLAN, il bénéficie de l'accès complet au réseau interne, y compris les ressources partagées.
Cette interface est donc la destination finale pour un poste qui est jugé sûr et authentifié par Packetfence, confirmant que le processus NAC a réussi et que l'accès normal peut être accordé.

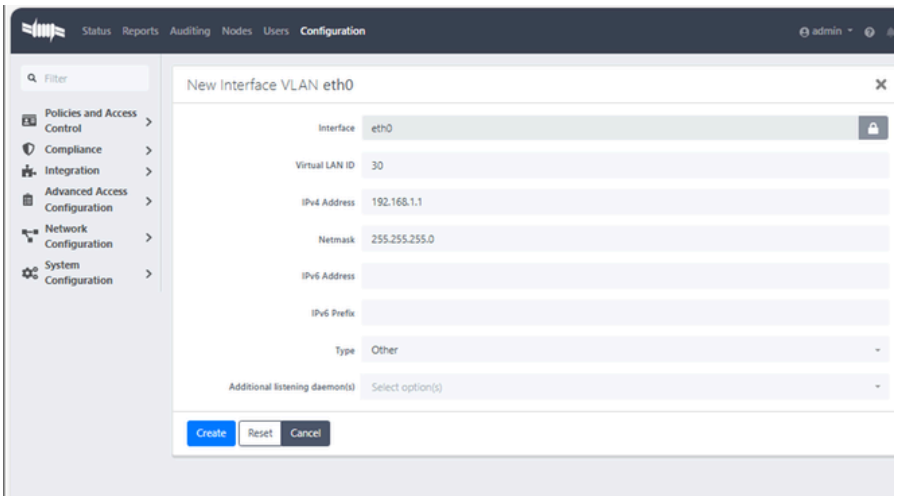


Figure 17: L'interface de vlan Normal

- On crée l'interface de vlan 20 c'est vlan Isolation:

Le VLAN 20 est le segment Isolation (ou VLAN de Quarantaine). Son rôle est de servir de zone de confinement pour les postes clients (comme PC3 dans votre topologie, ou toute machine non conforme).

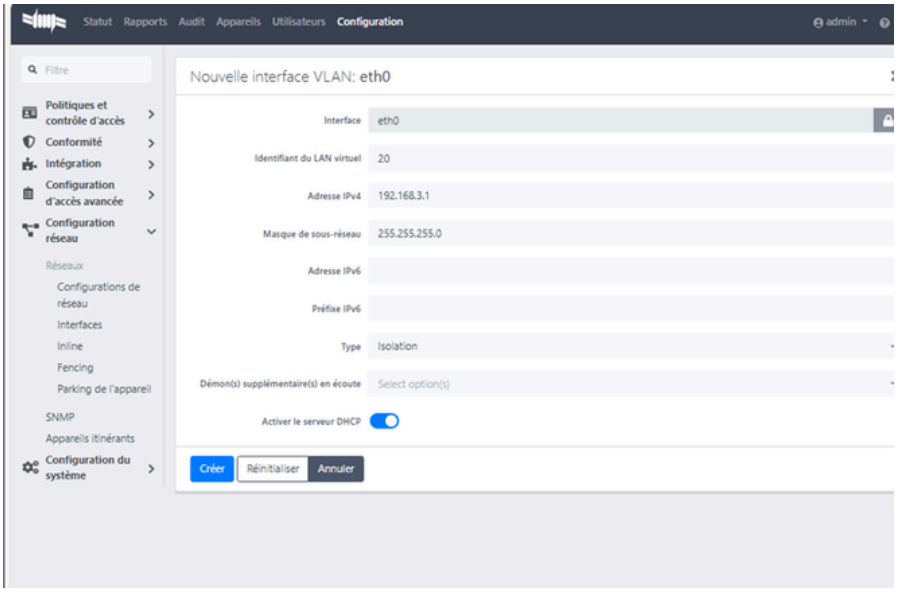


Figure 18: L'interface de vlan Isolation

- **La vérification de la création:**

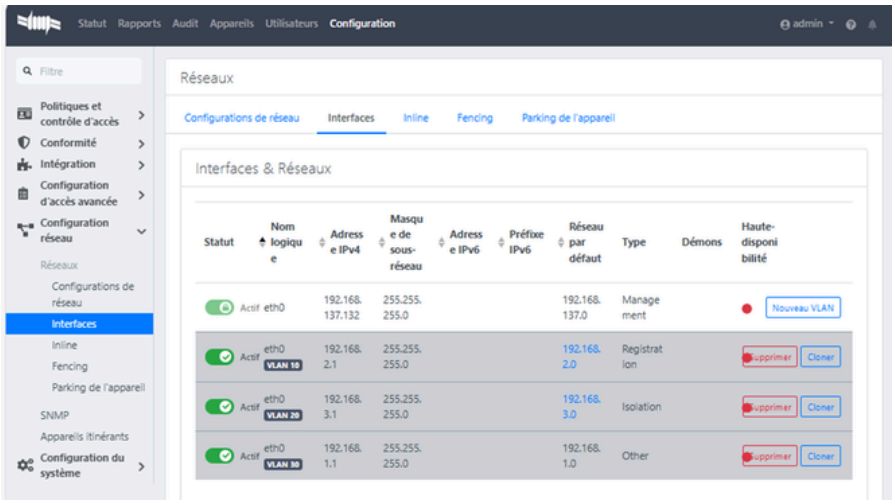


Figure 19: Affichage des interfaces vlans crées

4.1.2. Création et Définition des Rôles:

- Rôle : Registration (VLAN d'Attente)

L'image montre la création du rôle initial :
Nom du Rôle : Registration
Description : Rôle d'attente
Ce rôle est attribué par défaut à tout nouvel appareil se connectant au réseau. Lorsque le SwitchL2 place l'appareil dans ce rôle (VLAN 10), l'accès est limité aux ressources nécessaires à l'authentification (serveur Packetfence) et à l'enregistrement.

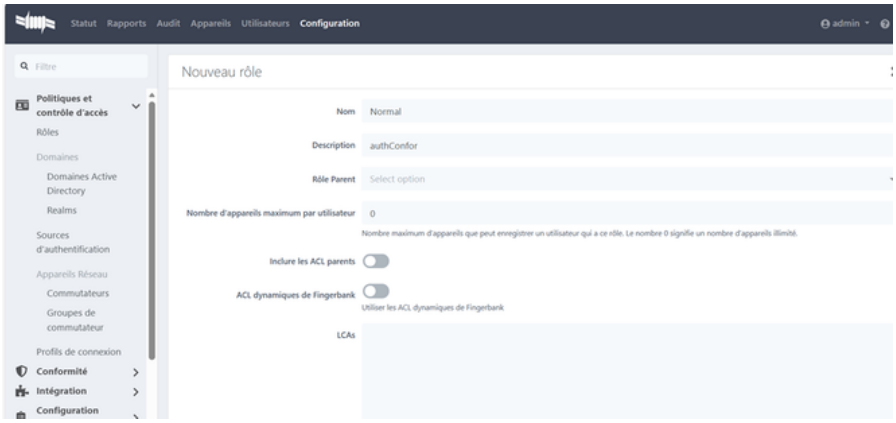


Figure 20: Création de rôle Registration

- Rôle : Normal

L'image montre la création du rôle pour l'accès complet :
Nom du Rôle : Normal
Description : authConfor (Authentifié et Conforme)
Ce rôle est attribué par Packetfence après que l'utilisateur ou le poste client a réussi l'authentification et est jugé conforme aux politiques de sécurité. L'attribution de ce rôle entraîne l'envoi d'un attribut RADIUS au SwitchL2, ordonnant le changement dynamique de VLAN du poste vers le VLAN 30 (Normal).

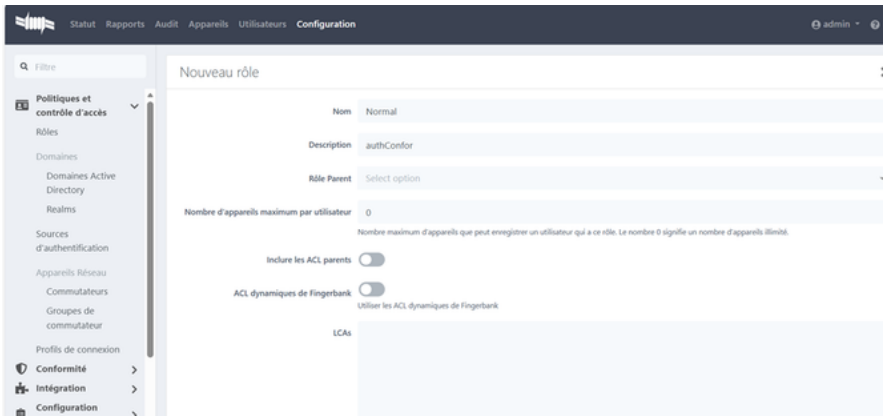


Figure 21: Création de rôle Normal

- Rôle : Isolation (VLAN de Quarantaine)

L'image montre la création du rôle de confinement :
Nom du Rôle : Isolation
Description : Poste malveillant (ou non conforme)
Ce rôle est attribué aux postes qui échouent à l'authentification ou sont détectés comme non conformes (ex: sans antivirus à jour, ou infecté). L'attribution de ce rôle dirige l'appareil vers le VLAN 20 (Isolation), où il est isolé du réseau principal.

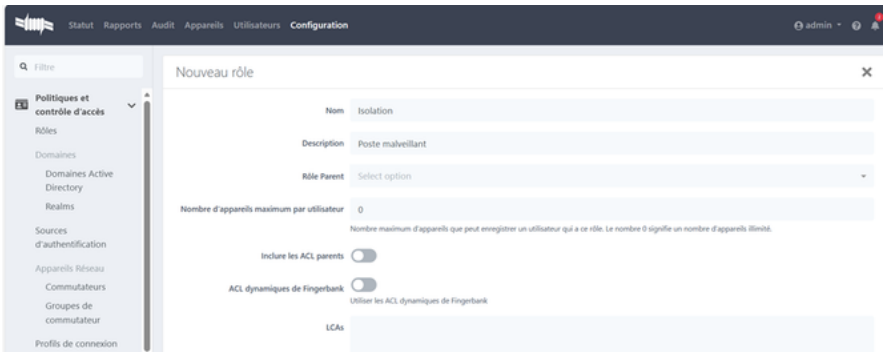


Figure 22: Création de rôle Isolation

4.1.3. Configuration du SwitchL2 dans packetfence:

Après avoir installé et démarré PacketFence, l'une des étapes essentielles est l'intégration des équipements réseau. L'image présentée montre la configuration d'un switch Cisco dans l'interface d'administration de PacketFence, au niveau du menu : Configuration → Network Devices → Switches
Cette section permet à PacketFence de reconnaître le switch, de communiquer avec lui, et d'appliquer les politiques NAC (802.1X, VLANs dynamiques, CoA…).

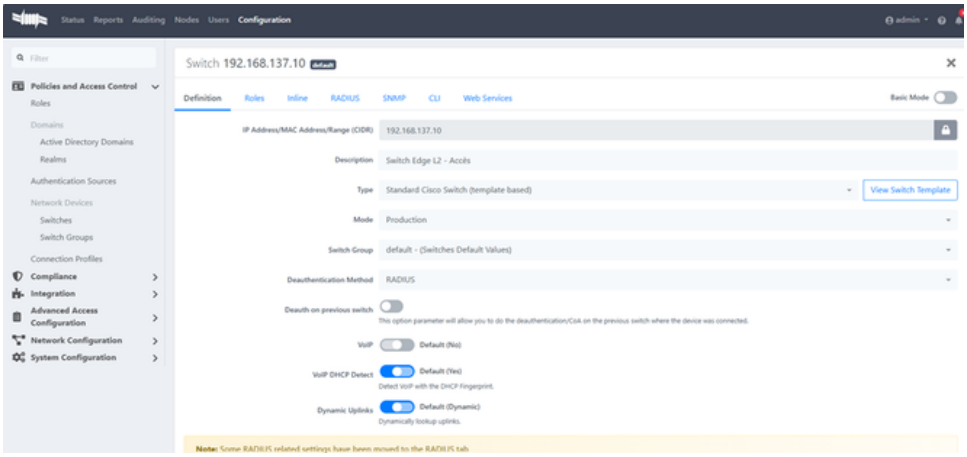


Figure 23: Configuration de Switch dans packetfence

nous déclarons le SwitchL2 en utilisant son adresse IP de gestion (192.168.137.10). Cette configuration est vitale pour le Contrôle d'Accès Réseau (NAC). Le Switch est reconnu comme un Standard Cisco Switch fonctionnant en mode Production, et est paramétré pour utiliser la méthode RADIUS pour le Change of Authorization (CoA). Cela permet à Packetfence, après une décision d'accès, d'envoyer des commandes au Switch (hors bande du trafic de données) pour modifier dynamiquement le VLAN du poste client. Cette étape établit la confiance et la communication sécurisée nécessaires entre le serveur NAC et le point d'application physique des politiques.

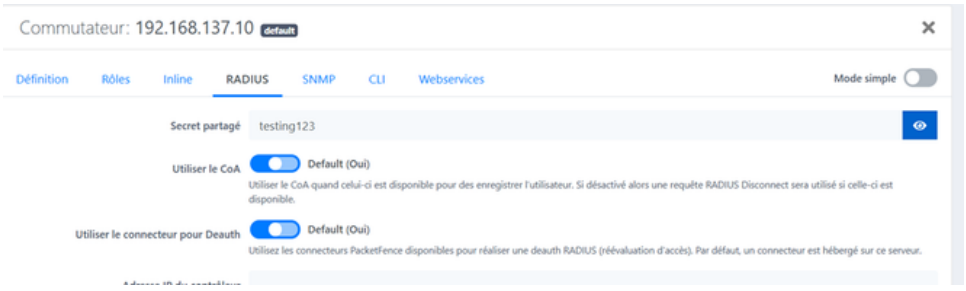


Figure 24: Définition de la Clé Secrète

Dans les paramètres du SwitchL2, définit la Clé Secrète (testing123). Cette clé doit être rigoureusement la même que celle configurée sur le SwitchL2 pour établir la communication RADIUS sécurisée et l'utilisation du mécanisme CoA (Change of Authorization).

- **Principe du Mappage de Rôle**

Packetfence attribue un Rôle interne à un utilisateur (comme registration, isolation, ou normal). Pour que le SwitchL2 comprenne cette décision et puisse appliquer le changement de segment, ce rôle doit être traduit en un ID VLAN numérique.

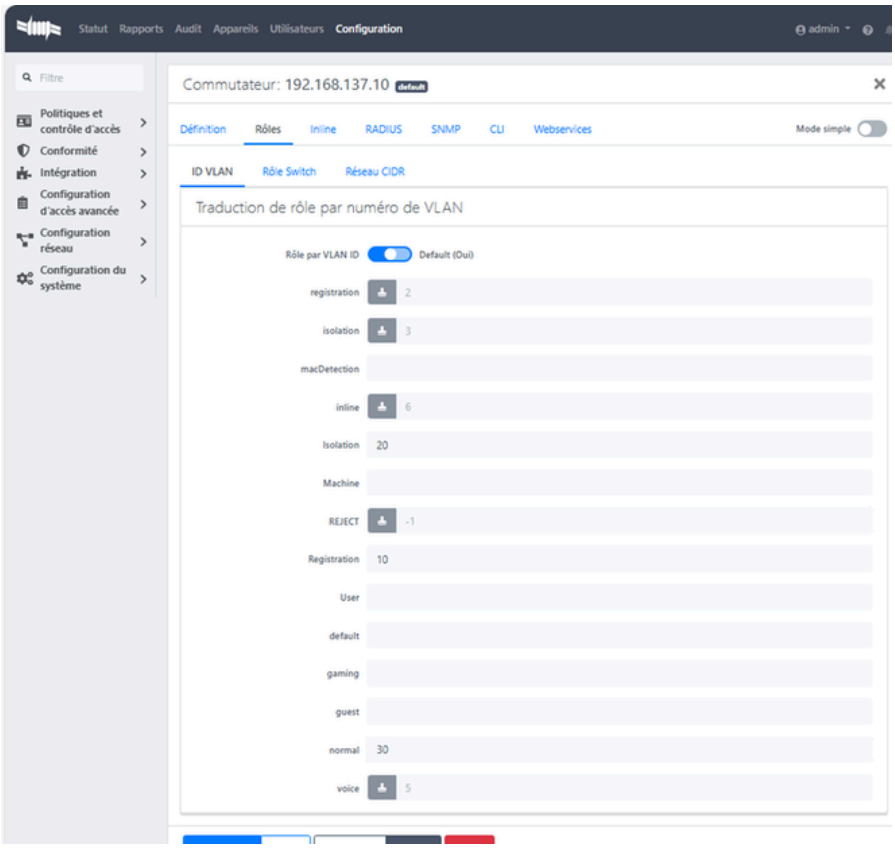


Figure 25: Mappage de rôle

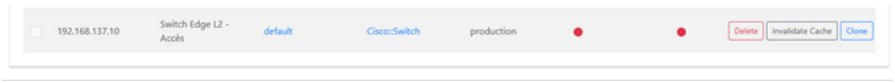


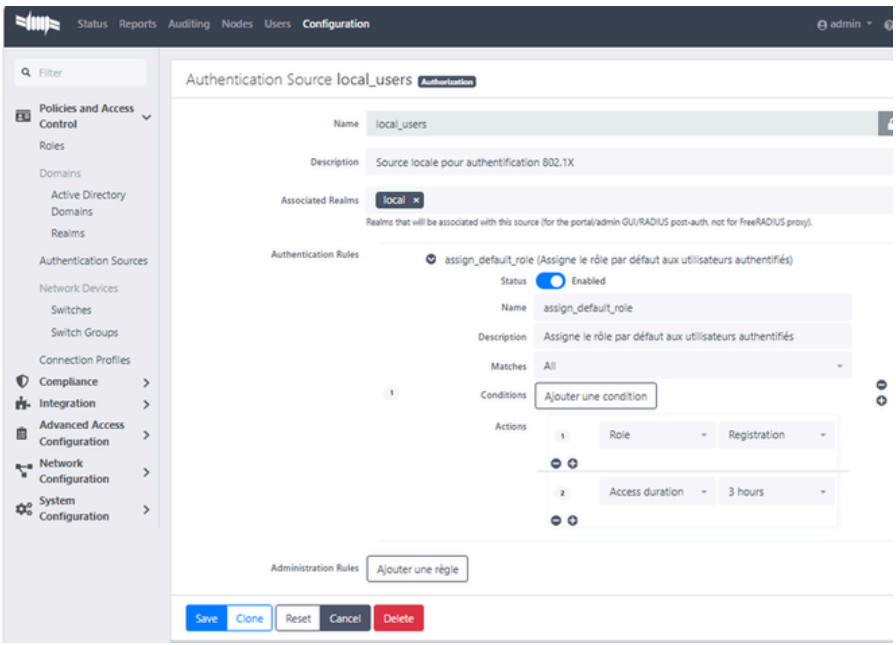
Figure 26: Vérification de création de switch

4.1.4. configuration radius dans packetfence

- Configuration de la Source d'Authentification RADIUS

La source d'authentification "local_users" est un système d'authentification autonome qui utilise une base de données locale intégrée à PacketFence pour vérifier les identités des utilisateurs lors des connexions 802.1X. Contrairement aux sources externes comme Active Directory ou LDAP, cette source stocke directement les credentials (noms d'utilisateur et mots de passe) dans PacketFence.

Lorsqu'un utilisateur tente de se connecter, le serveur RADIUS PacketFence interroge sa base locale, compare les credentials fournis avec ceux enregistrés, et valide ou refuse l'authentification en conséquence. Cette source est associée au realm "local", ce qui permet à PacketFence de router automatiquement les requêtes d'authentification portant ce domaine vers cette source spécifique



Figur 27: Création de la source locale de l'authentification

4.1.5. Profil de Connexion "profileauth":

Cette source d'authentification (local_users) sera ensuite associée au Profil de Connexion (Connection Profile) principal, qui est l'étape finale liant les règles d'accès au protocole 802.1X. C'est le Profil de Connexion qui ordonnera à Packetfence d'utiliser cette source d'utilisateurs locaux pour valider les tentatives de connexion provenant du SwitchL2.

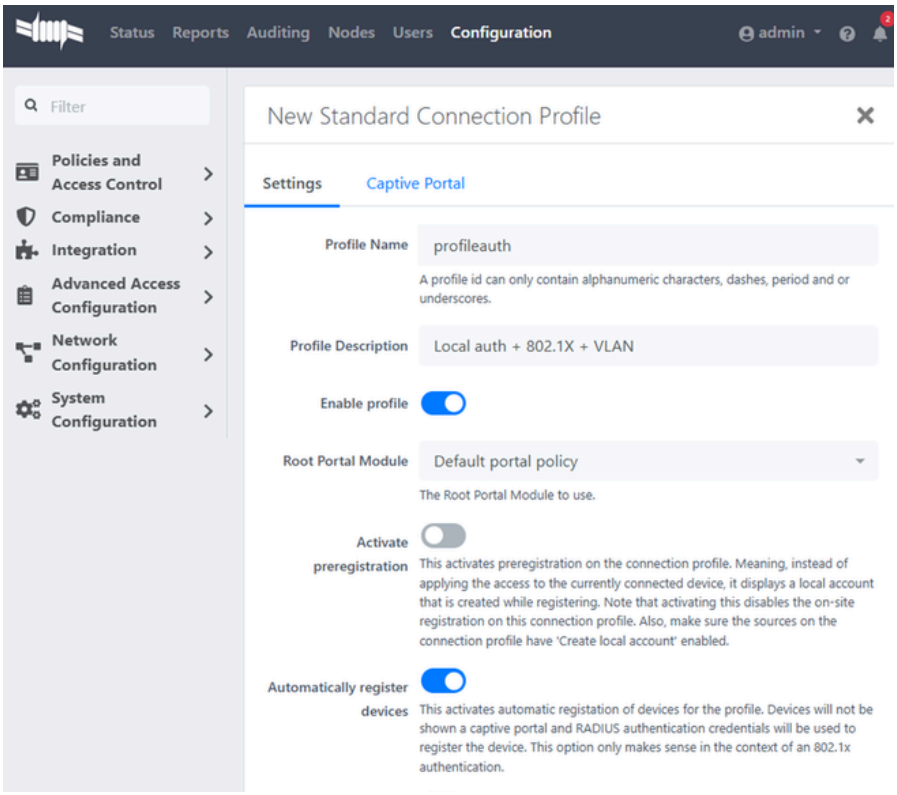


Figure 28: la configuration de profil de connexion

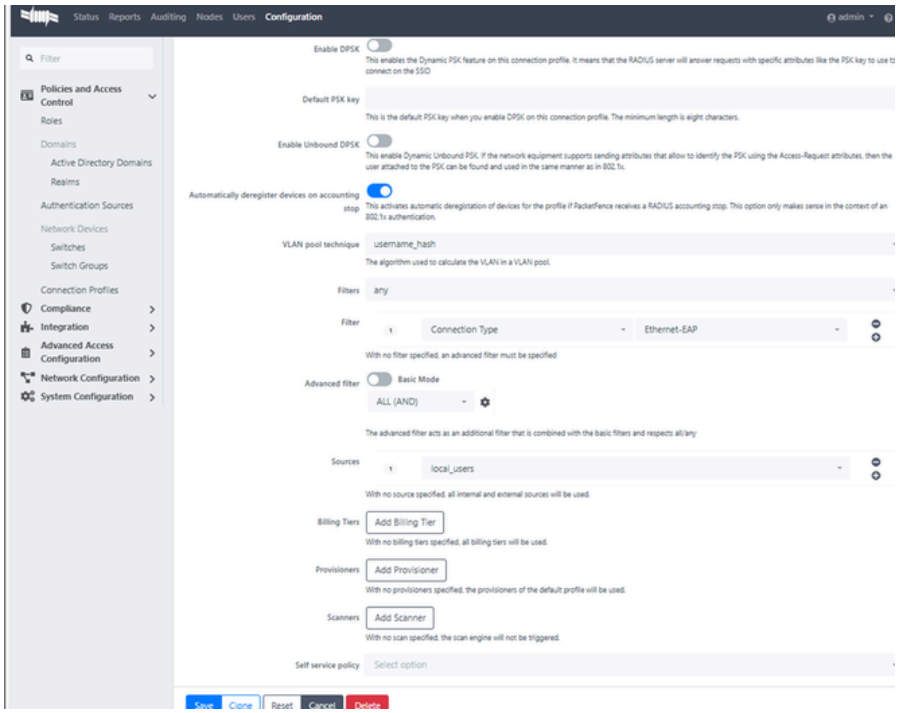


Figure 29: la suite de configuration de profil de connexion

4.1.6. Vérification de activation de services radius dans packetfence

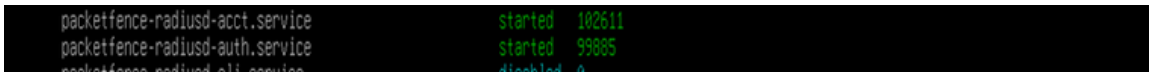


Figure 30: la vérification d'activation des services

Les deux services PacketFence sont actifs :
packetfence-radiusd-acct.service (port 102611) : Gère la comptabilité RADIUS (accounting) - enregistre les sessions utilisateurs, durées de connexion, etc.
packetfence-radiusd-auth.service (port 99865) : Gère l'authentification RADIUS - vérifie les identités des utilisateurs

4.1.7. Configuration Générale RADIUS

Cette interface configure les paramètres globaux du serveur RADIUS PacketFence.
Options activées :
Record accounting in SQL tables : Enregistre toutes les données de comptabilité RADIUS (sessions utilisateurs, durées de connexion, volumes de données) dans les tables SQL pour assurer la traçabilité et permettre l'analyse ultérieure des connexions
Use RADIUS filters in packetfence authorize : Active l'utilisation de filtres RADIUS lors de la phase d'autorisation, permettant d'appliquer des règles spécifiques avant d'accorder l'accès réseau aux utilisateurs
Use RADIUS filters in packetfence accounting : Active les filtres lors de la réception des paquets RADIUS Accounting (Start, Stop, Interim-Update) pour personnaliser le traitement des informations de session

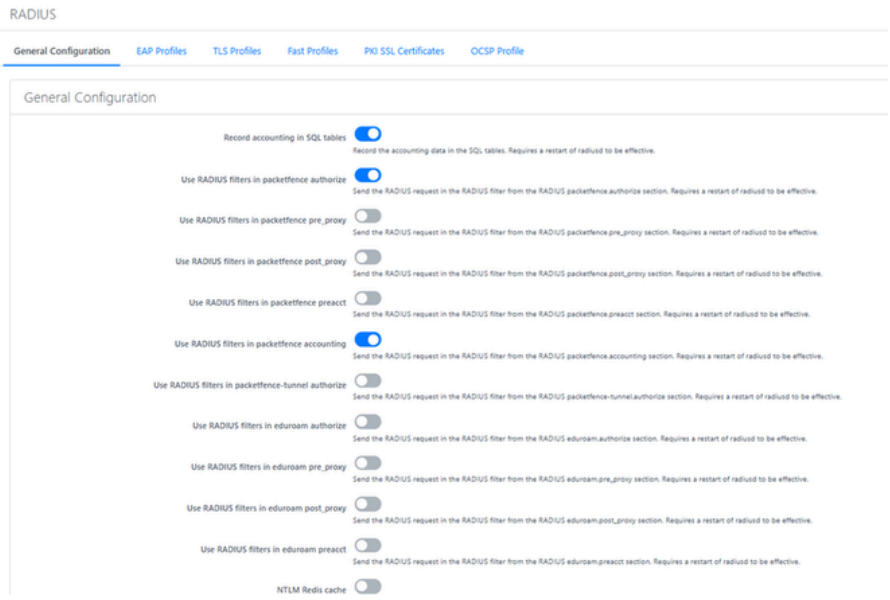


Figure 31: La configuration générale de Radius

Ces paramètres définissent comment le serveur RADIUS traite, filtre et enregistre les requêtes d'authentification et de comptabilité.

4.1.8.Profil EAP "default"

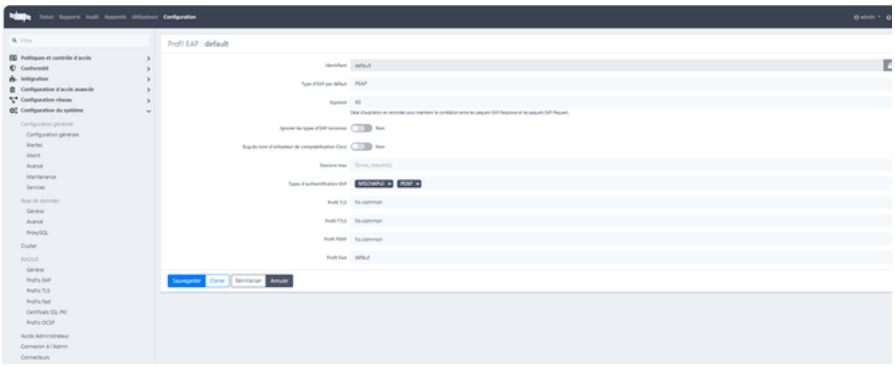


Figure 32: Profile EAP

Cette uniformisation des profils TLS vers "tls-common" permet une gestion centralisée des paramètres de sécurité (versions TLS, cipher suites, validation certificats) pour tous les types d'authentification EAP. Le profil EAP détermine comment le serveur RADIUS négocie les credentials avec les clients 802.1X.
PEAP (Protected Extensible Authentication Protocol) - crée un tunnel TLS sécurisé pour protéger l'authentification

4.1.9.TLS Profiles

Ce profil TLS centralise tous les paramètres de sécurité cryptographique pour l'authentification EAP. La restriction à TLS 1.2 exclut les versions obsolètes et vulnérables (SSL 3.0, TLS 1.0, TLS 1.1) tout en garantissant la compatibilité avec la majorité des équipements. La courbe elliptique prime256v1 offre un excellent équilibre entre sécurité et performance pour les échanges de clés cryptographiques.

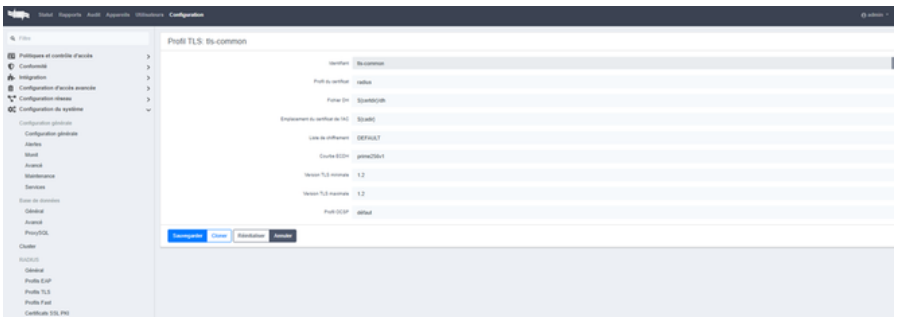


Figure 33: Profile TLS

4.1.10. Vérification de ports :

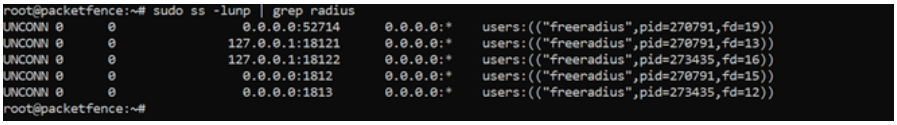


Figure 34: Vérification des ports

La commande ss -lunp | grep radius confirme que les services FreeRADIUS (le moteur RADIUS de Packetfence) sont bien démarrés et écoutent sur les ports standards

4.1.11. Création d'utilisateur de test :

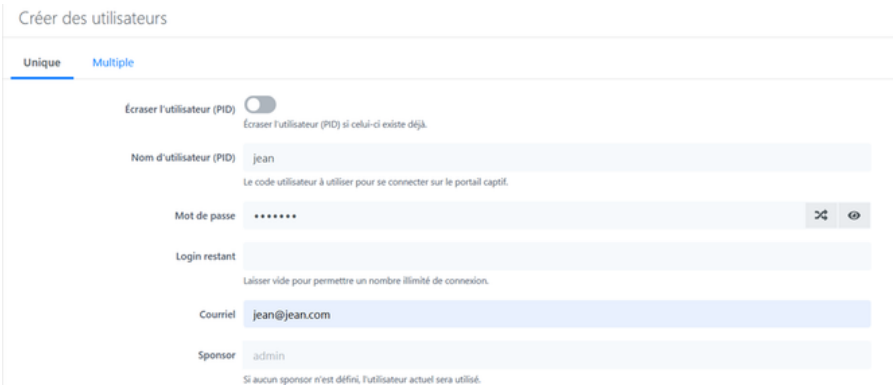


Figure 35: Règle de vlan 20 vers l'Internet

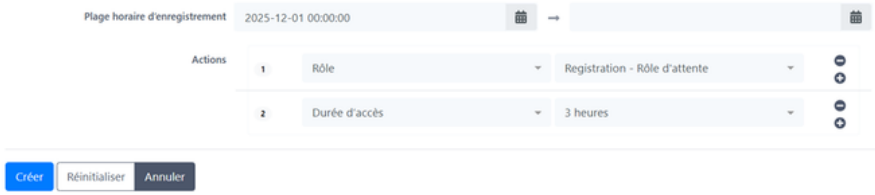


Figure 36: Règle de vlan 20 vers l'Internet

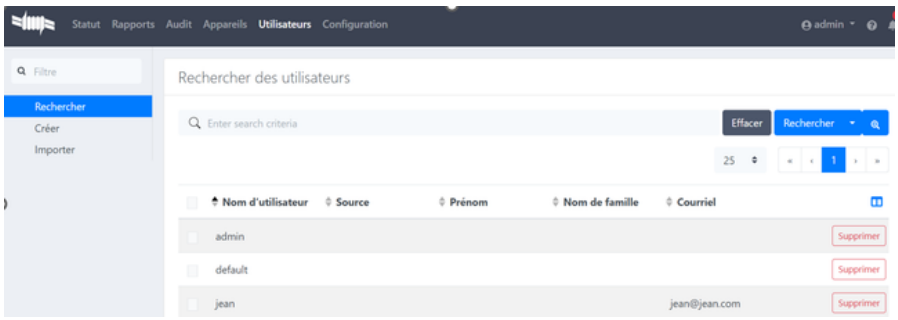


Figure 37: Affichage des utilisateurs dans packetfence

4.1.12. Gestion des Plages d'Adresses DHCP:

Cette image nous montre où Packetfence est configuré pour donner des adresses IP aux postes clients lorsqu'ils se connectent pour la première fois. C'est le service DHCP interne de Packetfence.

C'est une étape importante pour deux zones :

1. Le VLAN 10 (Registration) : Les postes qui viennent d'être branchés (comme machinetest) reçoivent une adresse IP dans la plage 192.168.2.x. Cela leur permet d'atteindre le serveur Packetfence pour s'authentifier.
2. Le VLAN 20 (Isolation) : Les postes qui sont en quarantaine reçoivent une adresse IP dans la plage 192.168.3.x. Cela leur donne accès uniquement aux serveurs de mise à jour ou de correction.

4.2. Configuration des equipements:

4.2.1 La configuration de switchs L2

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#aaa authorization network default group radius
Switch(config)#aaa accounting dot1x default start-stop group radius
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#dot1x system-auth-control
```

Figure 38: configuration de switch

Dans cette première configuration, nous activons tout d'abord le modèle AAA avec la commande aaa new-model, indispensable pour permettre au switch d'utiliser un serveur d'authentification externe. Nous configurons ensuite l'authentification, l'autorisation et l'accounting 802.1X afin que toutes les demandes soient envoyées vers PacketFence, qui intègre son propre serveur RADIUS et gère entièrement le processus d'authentification des utilisateurs. La commande dot1x system-auth-control active globalement le protocole 802.1X sur le switch, permettant aux ports configurés d'exiger une identité avant d'accorder l'accès au réseau. Cette configuration prépare le switch à déléguer toutes les décisions d'accès à PacketFence, qui applique les rôles et les VLAN selon l'état de conformité des machines.

```
Switch(config)#radius server Packetfence
Switch(config-radius-server)#$4 192.168.137.132 auth-port 1812 acct-port 1813
Switch(config-radius-server)#key testing123
Switch(config-radius-server)#timeout 30
Switch(config-radius-server)# retransmit 3
Switch(config-radius-server)#exit
```

Figure 39: la déclaration du serveur RADIUS et la clé secrète

La deuxième image montre la déclaration du serveur RADIUS intégré à PacketFence, qui est responsable de l'authentification et du contrôle d'accès des terminaux. On y configure l'adresse IP de PacketFence ainsi que les ports RADIUS standard, à savoir 1812 pour l'authentification et 1813 pour l'accounting, permettant au switch d'échanger correctement avec le NAC. La clé secrète définie doit être identique sur PacketFence et sur le switch afin de sécuriser toutes les communications RADIUS. Les paramètres timeout et retransmit déterminent le nombre de tentatives et le délai d'attente en cas d'absence de réponse du serveur, assurant ainsi une communication fiable. Grâce à cette configuration, le switch redirige toute la logique d'accès réseau vers PacketFence, qui applique les rôles, VLANs et politiques de sécurité adaptés.

```
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#client 192.168.137.132 server-key testing123
Switch(config-locsvr-da-radius)# auth-type any
Switch(config-locsvr-da-radius)#exit
```

Figure 40: Configuration du RADIUS Dynamic Authorization (CoA)

Configure le commutateur pour qu'il agisse comme un client de Dynamic Authorization (Client de Changement d'Autorisation ou CoA/PoD). Elle initialise la fonction aaa server radius dynamic-author pour désigner l'équipement comme récepteur. Ensuite, elle autorise spécifiquement le serveur RADIUS à l'adresse 192.168.137.132 à envoyer des requêtes de changement de politique (par exemple, pour déconnecter un utilisateur ou lui changer son accès réseau) au commutateur. La clé secrète testing123 est définie pour assurer que ces requêtes proviennent bien d'un serveur RADIUS de confiance, et la commande auth-type any garantit que le commutateur appliquera ces changements d'autorisation.

```
switchL2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switchL2(config)#vlan 10
switchL2(config-vlan)#name Registration
switchL2(config-vlan)#exit
switchL2(config)#vlan 20
switchL2(config-vlan)#name Isolation
switchL2(config-vlan)#exit
switchL2(config)#vlan 30
switchL2(config-vlan)#name Normal
switchL2(config-vlan)#exit
switchL2(config)#vlan 137
switchL2(config-vlan)#name management
switchL2(config-vlan)#exit
```

Figure 41: Création de vlans

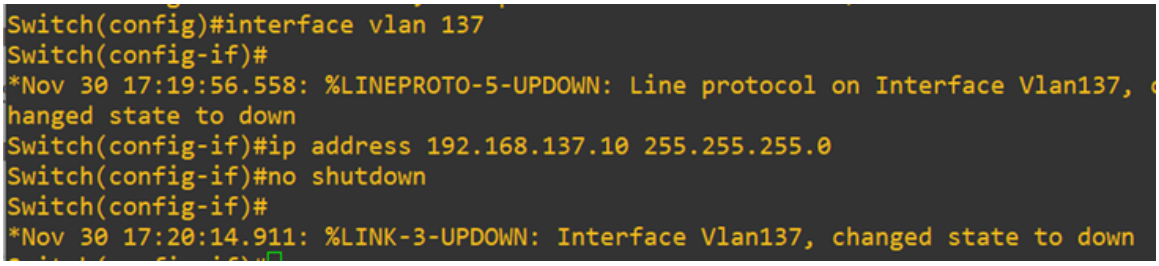


Figure 42: Attribution une adresse IP au commutateur

la configuration d'une interface VLAN (SVI – Switched Virtual Interface) pour le VLAN 137.
attribue une adresse IP au commutateur dans ce VLAN. Cette IP joue généralement le rôle de passerelle par défaut pour tous les hôtes du VLAN 137. Elle est indispensable pour permettre le routage inter-VLAN, c'est-à-dire la communication entre les appareils du VLAN 137 et ceux d'autres VLAN ou réseaux.

- La Configuration des interfaces Access et Trunk

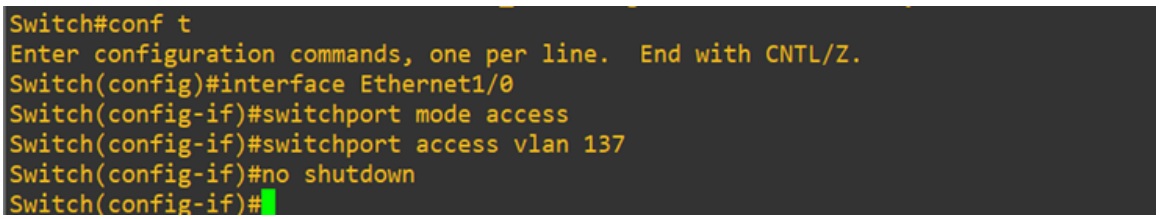


Figure 43: la configuration de l'interface liée a scanner

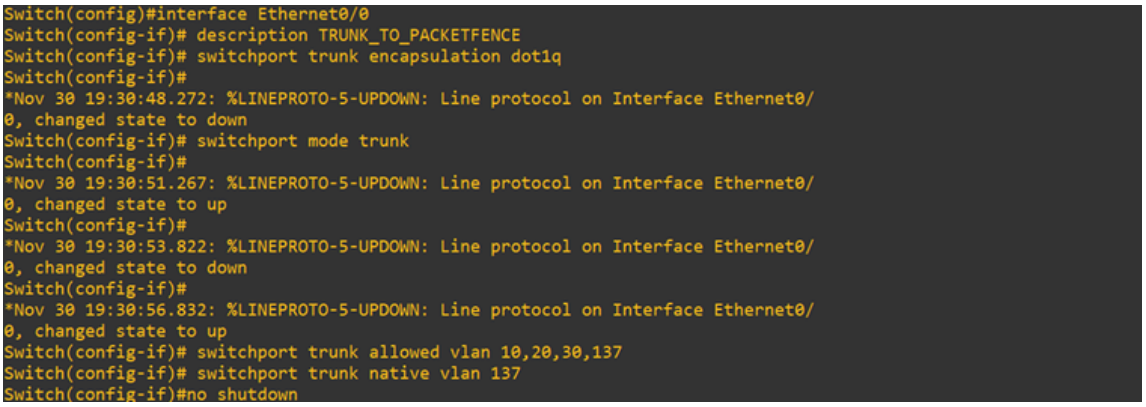


Figure 44: la configuration de l'interface liée a Packetfence

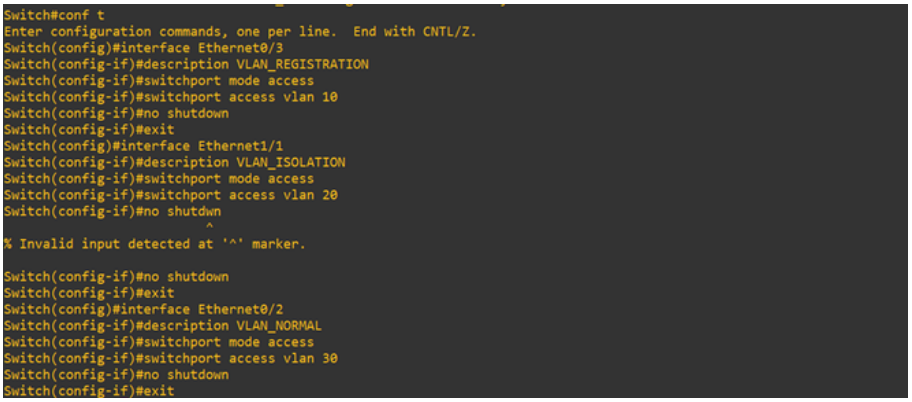


Figure 45: la configuration de l'interface liée au vlans

La configuration des interfaces Access sur un switch Cisco permet d'attribuer chaque port physique à un VLAN spécifique géré par PacketFence. Chaque port est défini en mode Access, transportant un seul VLAN non taggé. Par exemple :

- Ethernet0/3 → VLAN 10 (VLAN_REGISTRATION) : pour les nouveaux équipements non authentifiés.
- Ethernet0/1 → VLAN 20 (VLAN_ISOLATION) : pour les équipements en quarantaine ou en violation de sécurité.
- Ethernet0/2 → VLAN 30 (VLAN_NORMAL) : pour les utilisateurs authentifiés avec accès complet au réseau.

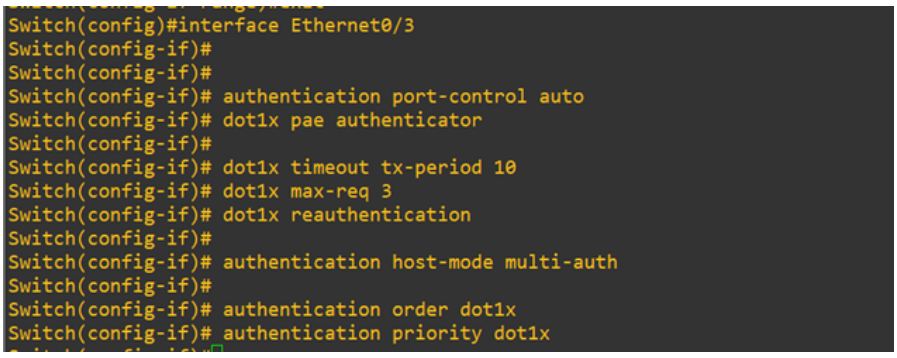


Figure 46 :Contrôle d'Accès Sécurisé (802.1X)

Le port Ethernet0/3 (VLAN Registration) est configuré pour l'authentification 802.1X (dot1x) :

La commande **authentication port-control auto** force le port à rester bloqué jusqu'à ce que l'authentification (via un serveur RADIUS externe) réussisse.

Le commutateur est défini comme l'authenticator (gérant la session d'authentification).

a**uthentication host-mode multi-auth** permet à plusieurs périphériques connectés au même port d'être authentifiés individuellement.
Des paramètres de temporisation (dot1x timeout) et de tentatives (dot1x max-req) sont ajustés pour optimiser le processus d'authentification.

- **Verification de ping de switch vers packetfence :**

```
Switch#ping 192.168.137.132
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.137.132, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
Switch#
```

Figure 47: ping réussie

4.2.2 La configuration de firewall

```
FortiGate-VM64-KVM (interface) # edit "VLAN10"

FortiGate-VM64-KVM (VLAN10) # set vdom "root"

FortiGate-VM64-KVM (VLAN10) # set interface "port2"

FortiGate-VM64-KVM (VLAN10) # set vlanid 10

FortiGate-VM64-KVM (VLAN10) # set ip 192.168.10.1/24

FortiGate-VM64-KVM (VLAN10) # next

FortiGate-VM64-KVM (interface) # edit "VLAN20"
new entry 'VLAN20' added

FortiGate-VM64-KVM (VLAN20) # set vdom "root"

FortiGate-VM64-KVM (VLAN20) # set interface "port2"

FortiGate-VM64-KVM (VLAN20) # set vlanid 20

FortiGate-VM64-KVM (VLAN20) # set ip 192.168.20.1/24

FortiGate-VM64-KVM (VLAN20) # next

FortiGate-VM64-KVM (interface) # edit "VLAN30"
new entry 'VLAN30' added

FortiGate-VM64-KVM (VLAN30) # set vdom "root"

FortiGate-VM64-KVM (VLAN30) # set interface "port2"

FortiGate-VM64-KVM (VLAN30) # set vlanid 30

FortiGate-VM64-KVM (VLAN30) # set ip 192.168.30.1/24

FortiGate-VM64-KVM (VLAN30) # next

FortiGate-VM64-KVM (interface) # end
```

Figure 48: Création des interfaces dans pare-feu

Cette configuration sur le pare-feu FortiGate a pour but de centraliser le routage inter-VLAN et d'appliquer une sécurité stricte. En créant des sous-interfaces pour les VLANs 10, 20 et 30 sur son port physique port2, et en leur attribuant des adresses IP (ex: $192.168.10.1$ pour le VLAN 10), le FortiGate devient la passerelle par défaut pour ces segments. Par conséquent, tout le trafic qui doit circuler entre les différents VLANs (Registration, Isolation, Normal) ou sortir vers l'extérieur doit impérativement passer par le pare-feu. Cette architecture garantit que le FortiGate peut inspecter, filtrer et contrôler chaque flux de données, assurant ainsi une isolation efficace et une application rigoureuse des politiques de sécurité entre les différentes zones du réseau.

```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 30
new entry '30' added

FortiGate-VM64-KVM (30) # set default-gateway 192.168.30.1

FortiGate-VM64-KVM (30) # set netmask 255.255.255.0

FortiGate-VM64-KVM (30) #  set interface "VLAN30"

FortiGate-VM64-KVM (30) # config ip-range

FortiGate-VM64-KVM (ip-range) #
FortiGate-VM64-KVM (ip-range) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set start-ip 192.168.30.10

FortiGate-VM64-KVM (1) # set end-ip 192.168.30.200

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (ip-range) # end

FortiGate-VM64-KVM (30) # set dns-server1 8.8.8.8

FortiGate-VM64-KVM (30) # next

FortiGate-VM64-KVM (server) # end
```

Figure 49: DHCP pour le VLAN 30 sur FortiGate

Cette configuration sur le FortiGate établit un serveur DHCP pour le VLAN 30 (le segment "Normal"), dont l'objectif est d'automatiser l'attribution des adresses IP aux clients. Le serveur est lié à la sous-interface virtuelle VLAN30 et attribue des adresses IP dans la plage allant de 192.168.30.10 à 192.168.30.200. Les clients recevront 192.168.30.1 comme passerelle par défaut, confirmant le rôle du FortiGate comme routeur de ce segment, ainsi que l'adresse DNS 8.8.8.8. Cette configuration est cruciale pour l'opérabilité du réseau, permettant aux périphériques de ce VLAN d'obtenir leur configuration réseau de manière dynamique et de communiquer efficacement en passant par le pare-feu.

Configuration des politiques du pare feu:

Les règles actuelles autorisent un accès complet (srcaddr "all", dstaddr "all", set service "ALL") du VLAN 137 (Management) vers tous les autres VLANs (10, 20, 30). Cela garantit que l'équipe d'administration peut gérer et surveiller tous les segments.

```
FortiGate-VM64-KVM (policy) #     edit 1
new entry '1' added

FortiGate-VM64-KVM (1) #         set srcintf "VLAN137"

FortiGate-VM64-KVM (1) #         set dstintf "VLAN10"     # \742\606\620 change ici
si n\703\651cessaire
node_check_object fail! for name #

value parse error before '#'
Command fail. Return code -651

FortiGate-VM64-KVM (1) #         set srcaddr "all"

FortiGate-VM64-KVM (1) #         set dstaddr "all"

FortiGate-VM64-KVM (1) #         set action accept

FortiGate-VM64-KVM (1) #         set schedule "always"

FortiGate-VM64-KVM (1) #         set service "ALL"
```

Figure 50: Règle du vlan 137 vers vlan 10

```
FortiGate-VM64-KVM (policy) #     edit 2
new entry '2' added

FortiGate-VM64-KVM (2) #         set srcintf "VLAN137"

FortiGate-VM64-KVM (2) #         set dstintf "VLAN20"

FortiGate-VM64-KVM (2) #         set srcaddr "all"

FortiGate-VM64-KVM (2) #         set dstaddr "all"

FortiGate-VM64-KVM (2) #         set action accept

FortiGate-VM64-KVM (2) #         set schedule "always"

FortiGate-VM64-KVM (2) #         set service "ALL"

FortiGate-VM64-KVM (2) #     next
```

Figure 51: Règle du vlan 137 vers vlan 20

```
FortiGate-VM64-KVM (policy) #     edit 3
new entry '3' added

FortiGate-VM64-KVM (3) #         set srcintf "VLAN137"

FortiGate-VM64-KVM (3) #         set dstintf "VLAN30"

FortiGate-VM64-KVM (3) #         set srcaddr "all"

FortiGate-VM64-KVM (3) #         set dstaddr "all"

FortiGate-VM64-KVM (3) #         set action accept

FortiGate-VM64-KVM (3) #         set schedule "always"

FortiGate-VM64-KVM (3) #         set service "ALL"

FortiGate-VM64-KVM (3) #     next
```

Figure 52: Règle du vlan 137 vers vlan 30

```
FortiGate-VM64-KVM # config firewall policy

FortiGate-VM64-KVM (policy) #     edit 0
new entry '0' added

FortiGate-VM64-KVM (0) #         set name "VLAN20-to-Internet"

FortiGate-VM64-KVM (0) #         set srcintf "VLAN20"

FortiGate-VM64-KVM (0) #         set dstintf "port1"

FortiGate-VM64-KVM (0) #         set srcaddr "all"

FortiGate-VM64-KVM (0) #         set dstaddr "all"

FortiGate-VM64-KVM (0) #         set action accept

FortiGate-VM64-KVM (0) #         set schedule "always"

FortiGate-VM64-KVM (0) #         set service "ALL"

FortiGate-VM64-KVM (0) #         set nat enable

FortiGate-VM64-KVM (0) #     next
```

Figure 53: Règle de vlan 20 vers l'Internet

```
FortiGate-VM64-KVM # config firewall policy
FortiGate-VM64-KVM (policy) #     edit 0
new entry '0' added
FortiGate-VM64-KVM (0) #         set name "Deny-VLAN20-to-VLAN30"
FortiGate-VM64-KVM (0) #         set srcintf "VLAN20"
FortiGate-VM64-KVM (0) #         set dstintf "VLAN30"
FortiGate-VM64-KVM (0) #         set srcaddr "all"
FortiGate-VM64-KVM (0) #         set dstaddr "all"
FortiGate-VM64-KVM (0) #         set action deny
FortiGate-VM64-KVM (0) #         set schedule "always"
FortiGate-VM64-KVM (0) #         set service "ALL"
FortiGate-VM64-KVM (0) #     next
```

Figure 54: Règle du vlan 20 vers vlan 30

4.3. La configuration de base de donnees de Packetfence:

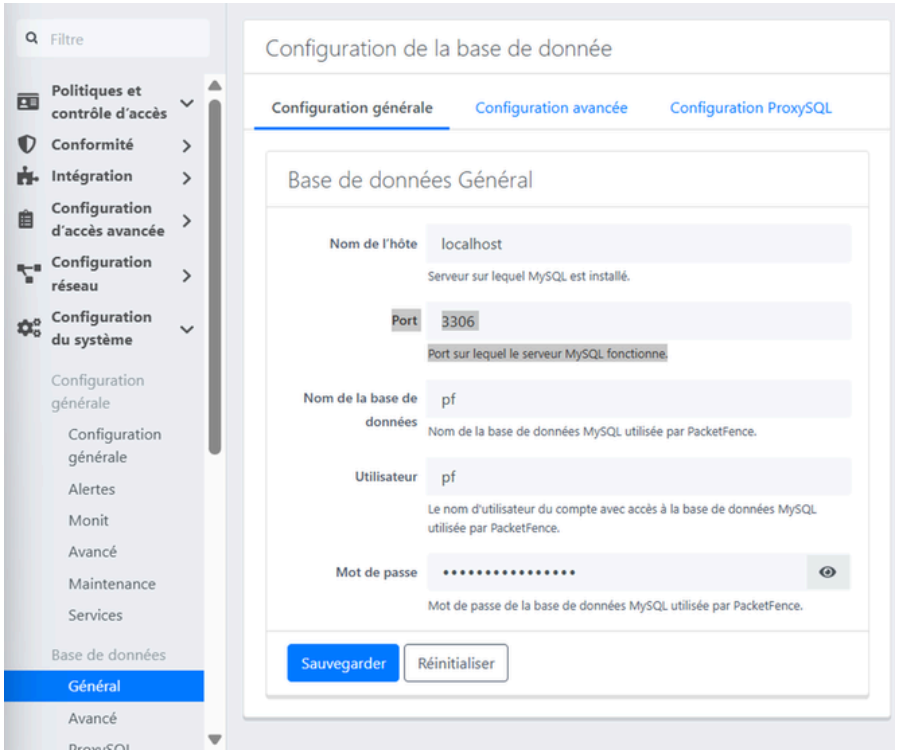


Figure 55: Configuration générale de la base de donnée

Cette interface permet de configurer les paramètres de connexion à la base de données MySQL utilisée par PacketFence pour stocker toutes ses informations (utilisateurs, équipements réseau, logs, politiques d'accès, etc.).

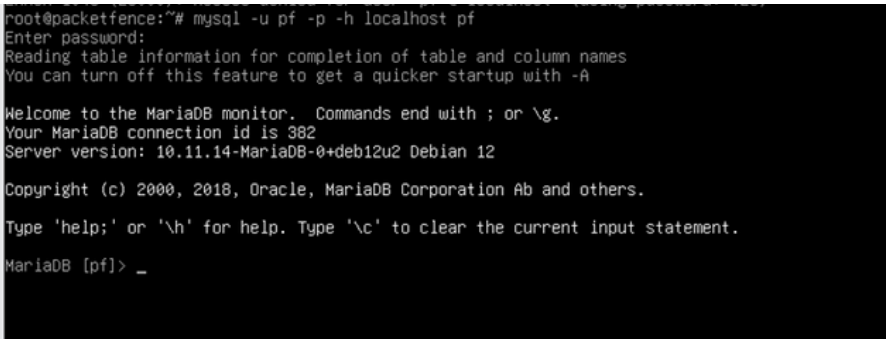


Figure 56: Connexion à la base de donnée autant qu'utilisateur

Cette image montre la connexion réussie à la base de données MySQL de PacketFence via la ligne de commande. La commande mysql -u pf -p -h localhost pf permet de se connecter en utilisant l'utilisateur "pf" sur le serveur local à la base de données "pf". Après avoir saisi le mot de passe, le système affiche les informations de connexion confirmant que le serveur MariaDB version 10.11.14 fonctionne correctement sur Debian 12. L'identifiant de connexion 302 est attribué à cette session, et l'invite de commande "MariaDB [pf]>" indique que la base de données est prête à recevoir des requêtes SQL.

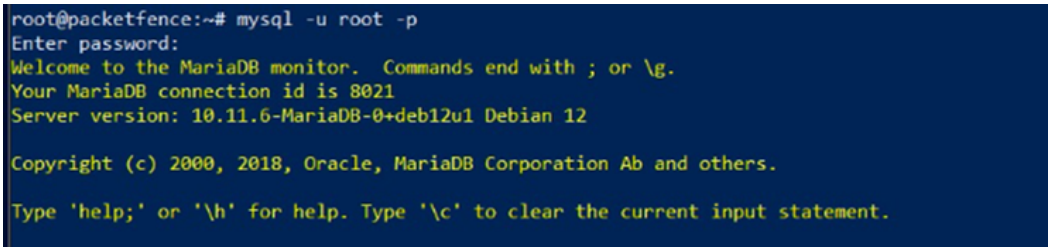


Figure 57: Connexion a la base de donnée autant que root

Cette capture montre une connexion à la base de données MariaDB en tant qu'utilisateur root (super-administrateur) via la commande mysql -u root -p. Contrairement à la connexion précédente avec l'utilisateur "pf" qui avait des privilèges limités à la base PacketFence,

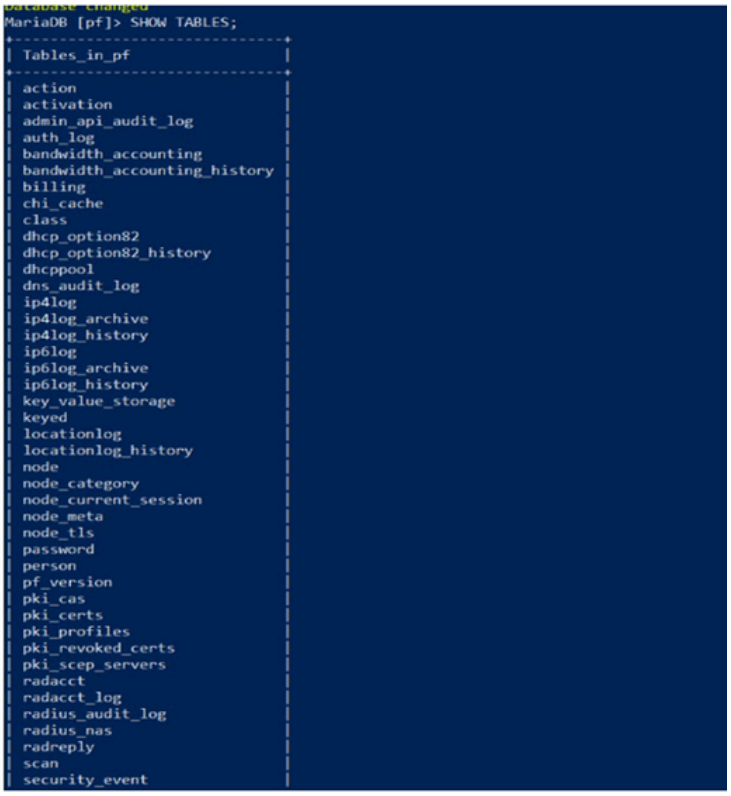


Figure 58: Les tables de base de donnée de Packetfence

Cette commande SHOW TABLES; liste toutes les tables présentes dans la base de données PacketFence, révélant ainsi la structure complète du système de stockage. On remarque l'existence de la table person qui stocke les informations des utilisateurs enregistrés dans le système. Parmi les autres tables importantes, on trouve node pour les équipements connectés, locationlog pour l'historique des connexions réseau, ip4log et ip6log pour le traçage des adresses IP, auth_log pour les tentatives d'authentification, radacct pour la comptabilité RADIUS, et dhcp_option82 pour la gestion DHCP. Les tables avec suffixe "_history" conservent l'historique des modifications pour l'audit et l'analyse. Cette architecture de base de données permet à PacketFence de gérer efficacement l'authentification, le contrôle d'accès et la traçabilité des connexions sur l'ensemble du réseau.

```
MariaDB [pf]> DESCRIBE person;
+-------------------+--------------+------+-----+---------+-------+
| Field             | Type         | Null | Key | Default | Extra |
+-------------------+--------------+------+-----+---------+-------+
| pid               | varchar(255) | NO   | PRI | NULL    |       |
| firstname         | varchar(255) | YES  |     | NULL    |       |
| lastname          | varchar(255) | YES  |     | NULL    |       |
| email             | varchar(255) | YES  |     | NULL    |       |
| telephone         | varchar(255) | YES  |     | NULL    |       |
| company           | varchar(255) | YES  |     | NULL    |       |
| address           | varchar(255) | YES  |     | NULL    |       |
| notes             | varchar(255) | YES  |     | NULL    |       |
| sponsor           | varchar(255) | YES  |     | NULL    |       |
| anniversary       | varchar(255) | YES  |     | NULL    |       |
| birthday          | varchar(255) | YES  |     | NULL    |       |
| gender            | char(1)      | YES  |     | NULL    |       |
| lang              | varchar(255) | YES  |     | NULL    |       |
| nickname          | varchar(255) | YES  |     | NULL    |       |
| cell_phone        | varchar(255) | YES  |     | NULL    |       |
| work_phone        | varchar(255) | YES  |     | NULL    |       |
| title             | varchar(255) | YES  |     | NULL    |       |
| building_number   | varchar(255) | YES  |     | NULL    |       |
| apartment_number  | varchar(255) | YES  |     | NULL    |       |
| room_number       | varchar(255) | YES  |     | NULL    |       |
| custom_field_1    | varchar(255) | YES  |     | NULL    |       |
| custom_field_2    | varchar(255) | YES  |     | NULL    |       |
| custom_field_3    | varchar(255) | YES  |     | NULL    |       |
| custom_field_4    | varchar(255) | YES  |     | NULL    |       |
| custom_field_5    | varchar(255) | YES  |     | NULL    |       |
| custom_field_6    | varchar(255) | YES  |     | NULL    |       |
| custom_field_7    | varchar(255) | YES  |     | NULL    |       |
| custom_field_8    | varchar(255) | YES  |     | NULL    |       |
| custom_field_9    | varchar(255) | YES  |     | NULL    |       |
| portal            | varchar(255) | YES  |     | NULL    |       |
```

Figure 59: La structure de la table person

Affiche la structure détaillée de la table "person" dans la base de données PacketFence. Cette table est essentielle car elle stocke toutes les informations relatives aux utilisateurs enregistrés dans le système.

- Création d'un utilisateur test1 créer depuis l'interface de packetfence et vérifier si il est ajouté vraiment a la base de donnée.

```
MariaDB [pf]> SELECT * FROM person WHERE pid = 'test1';
| pid   | firstname | lastname | email         | telephone | company | address | notes | sponsor | anni
versary | birthday | gender | lang | nickname | cell_phone | work_phone | title | building_number | apa
rtment_number | room_number | custom_field_1 | custom_field_2 | custom_field_3 | custom_field_4 | custo
m_field_5 | custom_field_6 | custom_field_7 | custom_field_8 | custom_field_9 | portal | source | psk
| potd | otp  | sponsored_date |
| test1 |           |          | test@test.com |           |         |         |       | admin   |
        |          |        | NULL |          |            |            |       |                 |
              |             |                |                |                |                |
          |                |                |                |                |         | NULL   | NULL   |
| no   | NULL | NULL           |
1 row in set (0.002 sec)

MariaDB [pf]>
```

Figure 60: Vérification de la création d'un utilisateur test1 dans la base de donnée

Nous avons effectué l'ensemble des configurations nécessaires pour tester notre système d'authentification, qui constitue le premier pilier du NAC. Différents scénarios de tests ont été mis en œuvre pour valider le processus d'authentification des utilisateurs et des équipements sur le réseau.

Tests d'authentification:

- Cas 1 – Utilisateur Jean (présent en base)

L'utilisateur Jean est présent dans la base de données locale de PacketFence. Lorsqu'il se connecte au port configuré en 802.1X, le client Kali envoie ses identifiants via EAP-PEAP. PacketFence valide les identifiants et renvoie un Access-Accept.
Le switch place alors le port en état Authorized

Pour commencer, nous avons installé l'outil wpa_supplicant en utilisant la commande « sudo apt install wpa-supplicant ». Cette installation est indispensable, car wpa_supplicant est le client officiel permettant à une machine Linux d'effectuer une authentification 802.1X sur un réseau filaire. Sans lui, le poste ne serait pas capable d'échanger les messages EAPOL avec le switch, et donc aucune authentification PEAP ou MSCHAPv2 ne pourrait être initiée. Cette étape constitue la base nécessaire pour que Kali puisse dialoguer avec PacketFence à travers le switch.

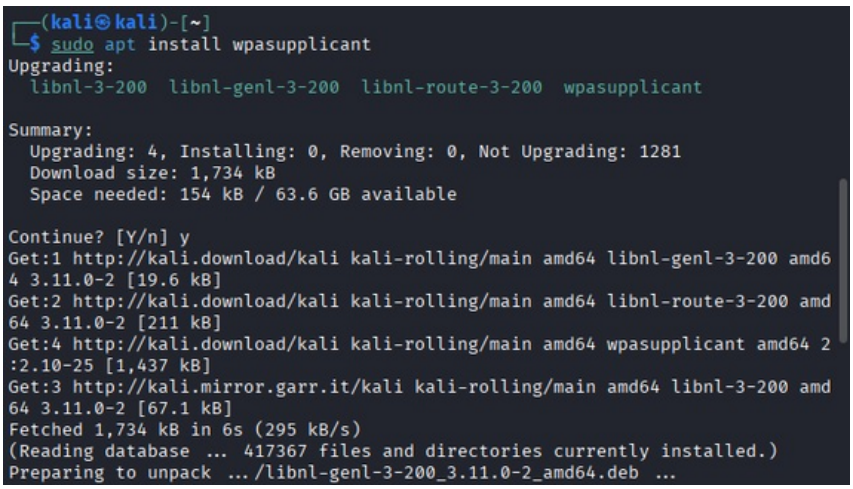


Figure 61: Installation de wpa_supplicant

Après l'installation, nous avons configuré un fichier personnalisé, par exemple « /etc/wpa_supplicant/wissong.conf », qui contient les paramètres d'authentification EAP utilisés lors de la connexion 802.1X. Dans ce fichier, nous avons défini « key_mgmt=IEEE8021X », ce qui active le mode d'authentification EAPOL sur câble Ethernet. Nous avons choisi l'EAP de type PEAP. À l'intérieur du tunnel PEAP, l'authentification interne se fait en MSCHAPv2 grâce au paramètre « phase2=auth=MSCHAPV2 ». Enfin, l'option « eapol_flags=0 » permet d'utiliser un échange EAPOL standard. L'ensemble de ces options permet à Kali d'envoyer correctement ses identifiants au switch via un tunnel chiffré PEAP.

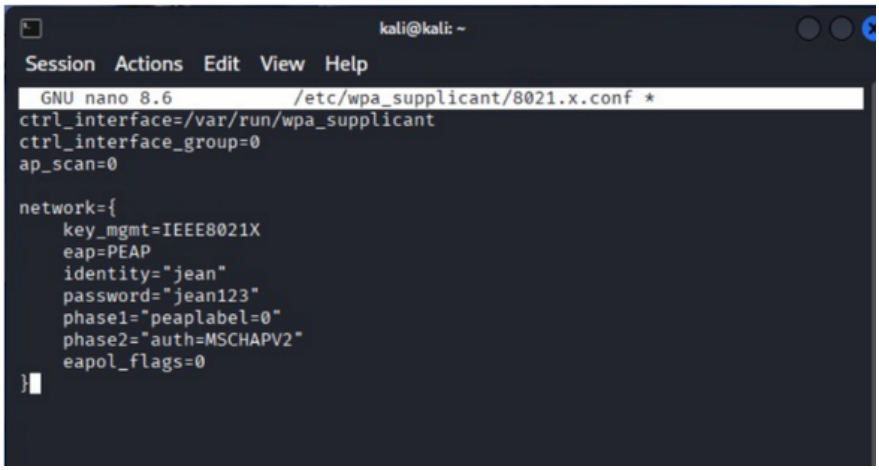


Figure 62: Configuration du fichier 802.1X

Une fois le fichier de configuration prêt, nous avons lancé l'authentification 802.1X en exécutant la commande « sudo wpa_supplicant -D wired -i eth0 -c /etc/wpa_supplicant/wissong.conf -d ». Cette commande permet au poste Kali de s'authentifier en EAP/PEAP via l'interface eth0, en utilisant l'identité « jean ». Le mode debug affiche en direct les échanges EAPOL et montre clairement si l'authentification est acceptée ou non par PacketFence. Lorsque les informations de jean sont correctes, wpa_supplicant affiche un message de réussite de type « EAP-SUCCESS ».

Figure 63: Lancement de l'authentification 802.1X

Pour confirmer le résultat, nous avons vérifié l'état du port sur le switch à l'aide de la commande « show authentication sessions interface ». Le switch affiche alors l'adresse MAC de la machine, l'utilisateur authentifié « jean » et l'adresse IP obtenue dans le VLAN registration.

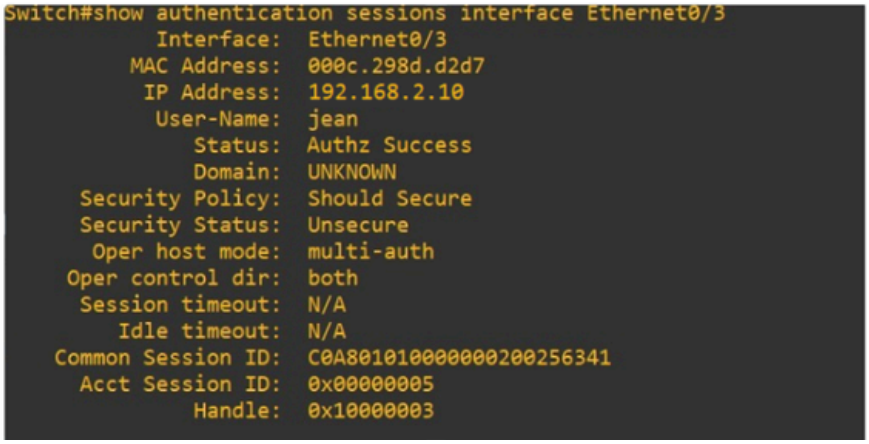


Figure 64: Vérification de l'authentification sur le switch

- Cas 2 – Utilisateur Marie (absent de la base)

Nous avons configuré wpa_supplicant dans la même machine Kali avec l'identité « Marie » et le mot de passe « Marie123 » en PEAP/MSCHAPv2. Comme Marie n'existe pas dans la base PacketFence, l'authentification échoue et wpa_supplicant affiche un message de rejet.

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0

ap_scan=0
eapol_version=1

network={
    key_mgmt=IEEE8021X
    eap=PEAP
    identity="marie"
    password="marie123"
    phase1="peapver=0"
    phase2="auth=MSCHAPV2"
    eapol_flags=0
}
```

Figure 65: Authentification 802.1X avec Marie

L'utilisateur Marie ne figure pas dans la base de données. Lorsque Kali tente de s'authentifier avec son identité, PacketFence renvoie un Access-Reject.
Le switch marque donc la session comme Failed

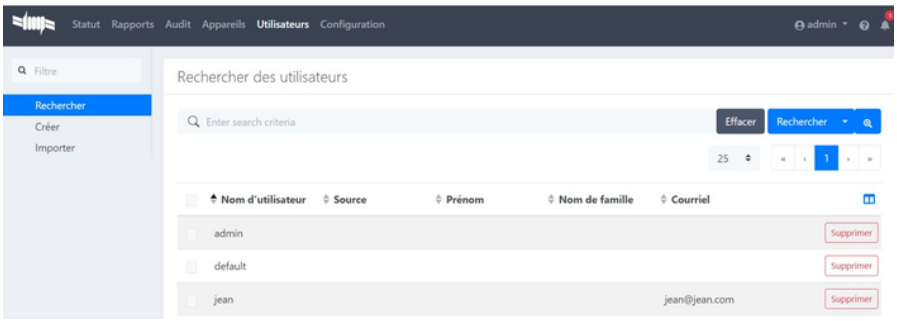


Figure 66: Base d'utilisateurs PacketFence

La commande « show authentication sessions interface » montre que le switch a détecté l'adresse MAC et l'adresse IP renouvelée de la machine. Le statut est « auth failed » puisque Mary n'est pas enregistrée dans PacketFence.

Figure 67: Authentification échouée pour utilisateur Marie

Suite à la validation réussie du premier pilier d'authentification, nous passons maintenant au deuxième pilier du NAC : la conformité. Ce pilier permet de vérifier que les équipements connectés au réseau respectent les politiques de sécurité définies par l'organisation, telles que la présence d'un antivirus à jour, l'installation des correctifs de sécurité, et la conformité aux standards de configuration imposés.

Dans notre cas, nous avons utilisé le scanner de vulnérabilités Nessus Essentials (version gratuite sans licence commerciale) pour évaluer la conformité des équipements connectés au réseau. Nessus effectue un scan automatisé des postes de travail pour détecter les vulnérabilités de sécurité, vérifier l'absence de correctifs critiques, identifier les logiciels obsolètes, et contrôler les configurations non sécurisées.

5. Installation et configuration de Nessus:

5.1 Installation de Nessus:

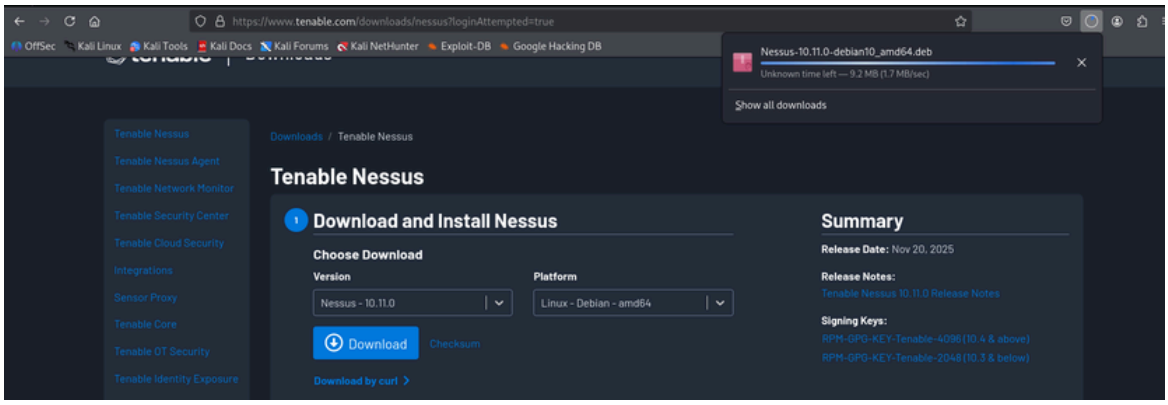


Figure 68: Interface de Téléchargement Tenable Nessus

L'interface web officielle de Tenable pour télécharger Nessus. On y voit la section "Download and Install Nessus" avec les options de sélection de la plateforme (Linux, Debian, et architecture all/amd64)

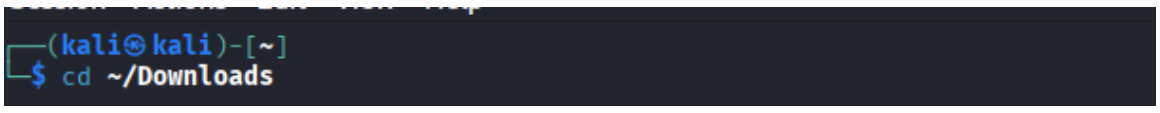


Figure 69: Navigation vers le Répertoire de Téléchargement

cd ~/Downloads exécutée dans le terminal Linux pour accéder au répertoire où le fichier d'installation de Nessus a été téléchargé.

Figure 70: package Nessus installé

Le changement de répertoire est confirmé par le prompt qui affiche maintenant ~/Downloads, indiquant que l'utilisateur se trouve dans le dossier de téléchargements et peut maintenant procéder à l'installation du package Nessus.

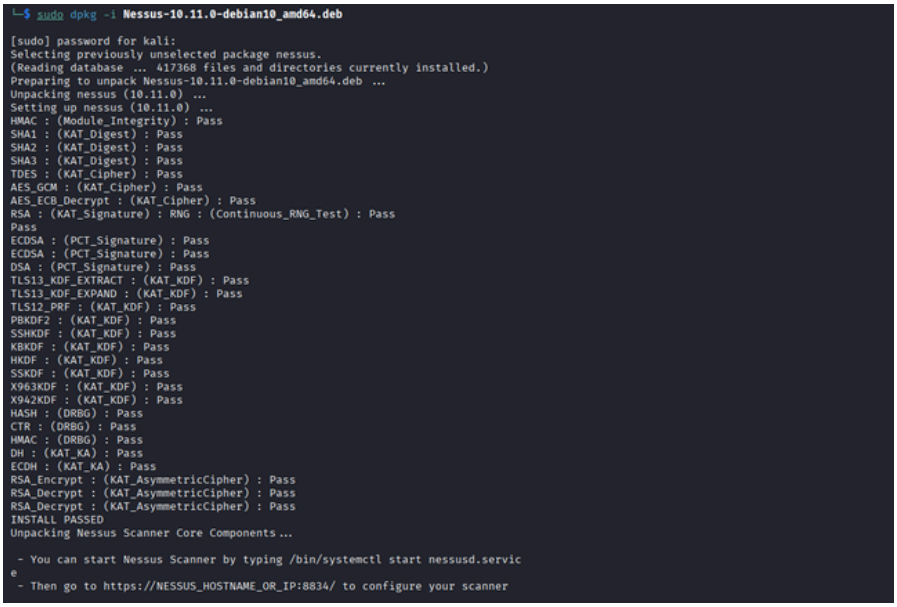


Figure 71: Installation du Package Nessus

la commande **dpkg -i Nessus-10.8.3-debian10_amd64.deb** utilisée pour installer le package Debian de Nessus. La commande dpkg -i (Debian Package) permet d'installer le fichier .deb téléchargé. Le fichier Nessus-10.8.3-debian10_amd64.deb correspond à la version 10.8.3 de Nessus compilée pour Debian 10 en architecture 64 bits. Cette installation déploie le scanner de vulnérabilités sur le système qui sera ensuite intégré avec PacketFence pour la vérification de conformité des équipements réseau.

Figure 72: Démarrage et Activation du Service Nessus

La première commande **sudo systemctl start nessusd** démarre immédiatement le service Nessus après avoir saisi le mot de passe sudo, permettant ainsi au scanner de vulnérabilités de fonctionner en arrière-plan. La seconde commande **sudo systemctl enable nessusd** active le démarrage automatique du service Nessus au boot du système.

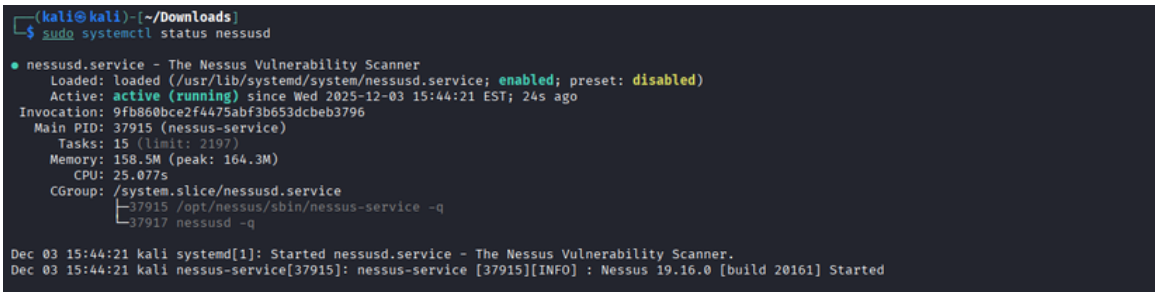


Figure 73: Vérification du Statut du Service Nessus

la commande **sudo systemctl status nessusd** qui permet de vérifier l'état du service Nessus après son démarrage. Le service "nessusd.service - The Nessus Vulnerability Scanner" apparaît comme loaded (chargé) et enabled (activé au démarrage automatique), avec un statut active (running) en vert confirmant que le scanner fonctionne correctement

- On accéde à l'interface web:

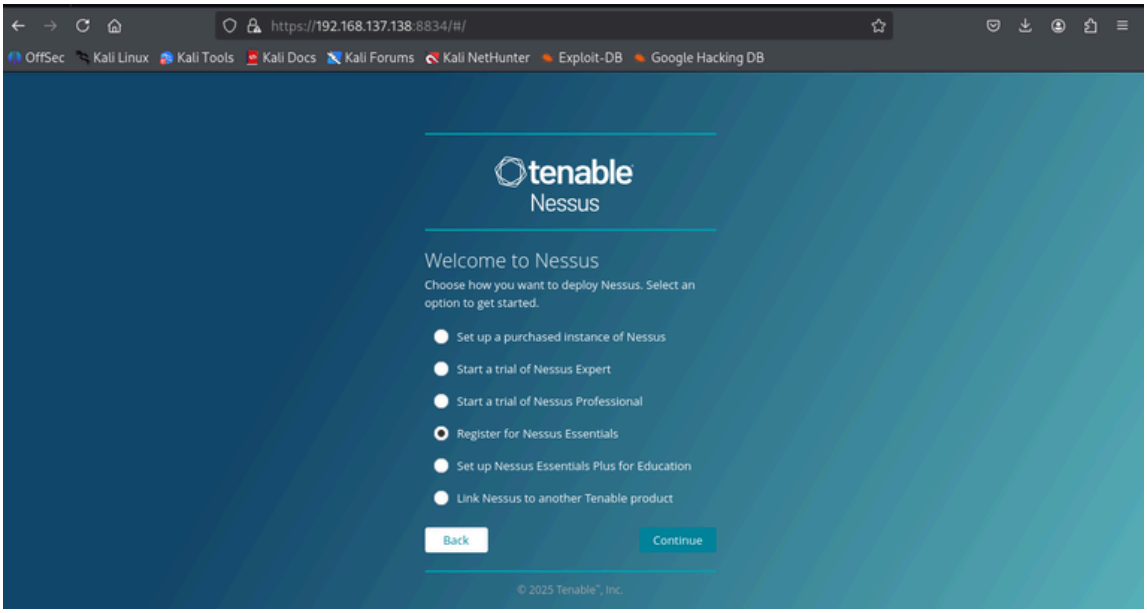


Figure 74: L'interface web de Nessus

L'interface web de bienvenue de Nessus est accessible à l'adresse https://192.168.137.138:8834. La page propose différentes options de déploiement, et nous avons sélectionné "Register for Nessus Essentials", qui est la version gratuite permettant de scanner jusqu'à 16 adresses IP sans licence commerciale. Cette option est idéale pour notre environnement de test PacketFence car elle offre les fonctionnalités essentielles de détection de vulnérabilités nécessaires pour la vérification de conformité des équipements réseau.

Après avoir cliqué sur "Continue", nous pourrons créer un compte administrateur et obtenir un code d'activation gratuit pour finaliser la configuration du scanner.

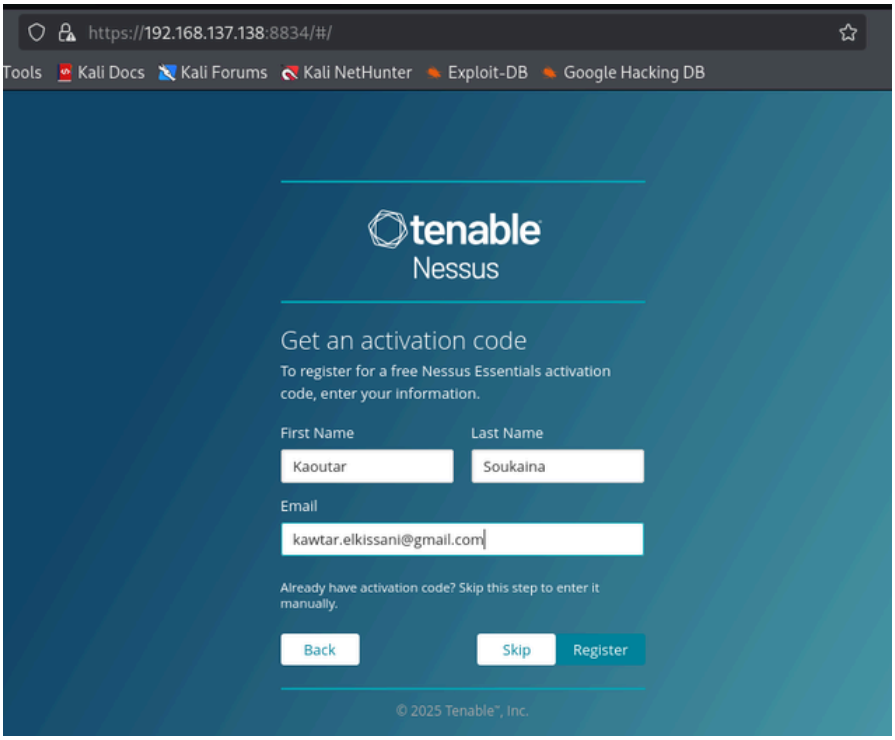


Figure 75: Création de compte administrateur

Après clique sur Registrer une page "License Information" de Nessus s'affiche avec le code d'activation NBJN-QM2Z-3BC5-VX3J-FMS3, qui est généré automatiquement par Tenable après l'enregistrement d'un compte gratuit Nessus Essentials. Ce code unique permet d'activer la version gratuite du scanner de vulnérabilités.

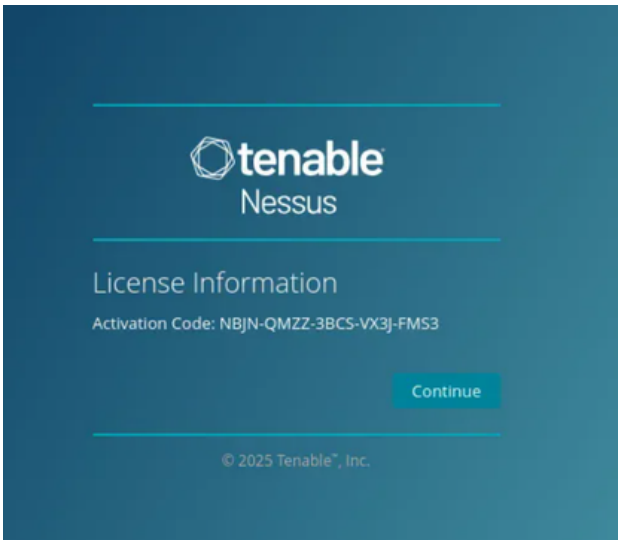


Figure 76 : Code d'Activation de Nessus Essentials

Après avoir cliqué sur "Submit", l'interface affiche la page d'initialisation de Nessus avec le message "Please wait while Nessus is initializing" (Veuillez patienter pendant l'initialisation de Nessus). Une barre de progression indique "Downloading plugins..." montrant le téléchargement en cours des plugins de détection de vulnérabilités. Cette étape est essentielle car Nessus télécharge sa base de données complète de plugins qui contient des milliers de tests de sécurité pour identifier les vulnérabilités, les mauvaises configurations et les failles dans les systèmes.

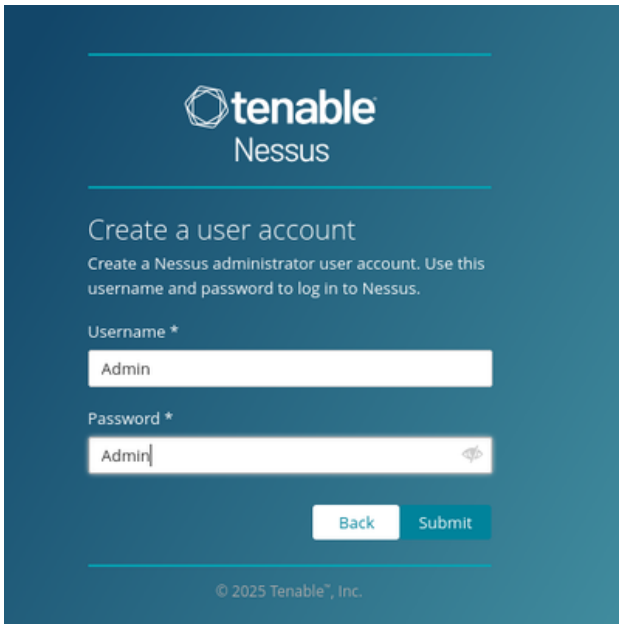


Figure 77: Création du compte administrateur pour accéder a Nessus

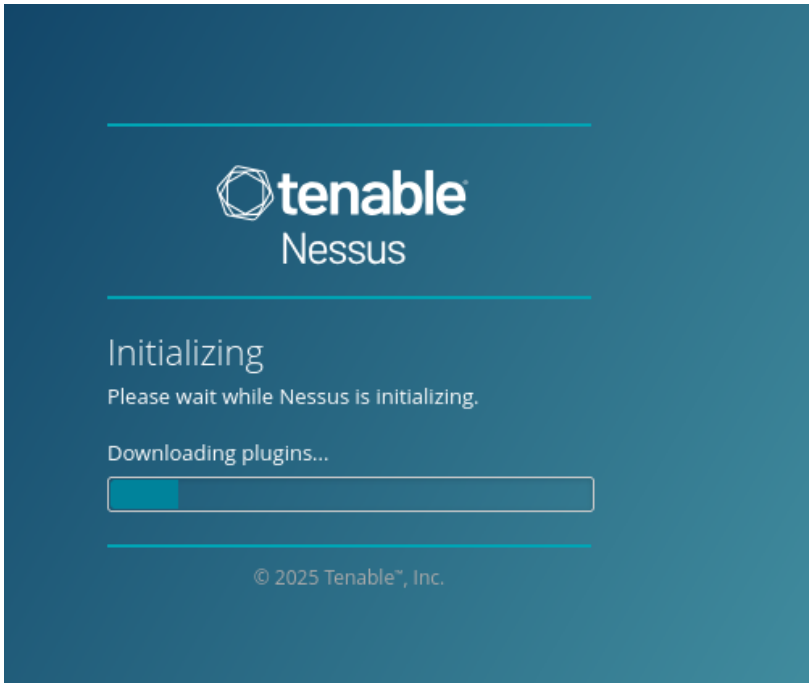


Figure 78 : Initialisation de Nessus

5.2 Activer l'API de Nessus:

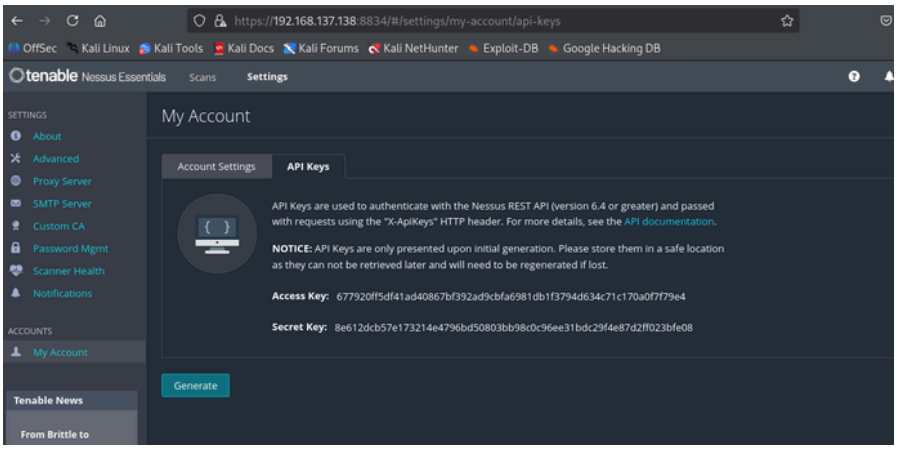


Figure 79 : Génération des Clés API Nessus

L'interface de configuration Nessus affiche maintenant la section "My Account" dans l'onglet "API Keys" accessible via le menu Settings. Les clés API (Application Programming Interface) sont utilisées pour authentifier les requêtes auprès de l'API REST de Nessus (version 6.4 ou supérieure) en utilisant l'en-tête HTTP "X-ApiKeys".

Ces clés API permettent à PacketFence de communiquer automatiquement avec Nessus pour lancer des scans de vulnérabilités, récupérer les résultats, et intégrer les informations de conformité dans le système NAC sans intervention manuelle. Le bouton "Generate" permet de créer de nouvelles clés si nécessaire.

5.3. Création d'une Policy::

L'interface Nessus affiche la page "Policies" qui permet de gérer les modèles de scan de vulnérabilités.
Une policy définit comment Nessus va scanner les équipements : quels tests effectuer, quelle profondeur d'analyse, et quels types de vulnérabilités rechercher. Pour créer notre première policy, nous cliquons sur le bouton "New Policy" qui nous permettra de configurer un modèle de scan adapté à nos besoins de vérification de conformité pour PacketFence.

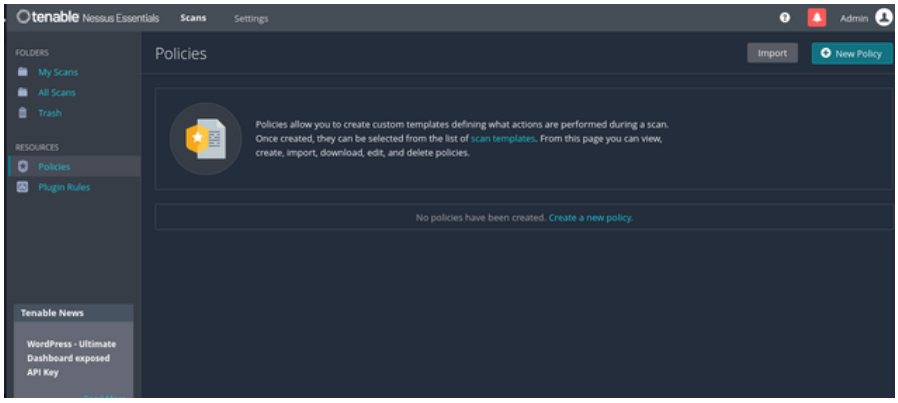


Figure 80 : Création d'une Policy

Nessus propose plusieurs modèles de scan préconfigurés selon différents objectifs. Les modèles de découverte comme "Host Discovery" permettent de détecter les équipements actifs sur le réseau. Les modèles de vulnérabilités comme "Basic Network Scan" effectuent un scan rapide des failles courantes, tandis que "Credentialed Patch Audit" vérifie si les mises à jour de sécurité sont installées en s'authentifiant sur les machines. "Advanced Scan" offre plus d'options de personnalisation pour des analyses approfondies. Pour notre intégration avec PacketFence, nous choisissons généralement "Basic Network Scan" ou "Credentialed Patch Audit" selon le niveau de contrôle souhaité pour vérifier la conformité des équipements avant de leur autoriser l'accès au réseau.

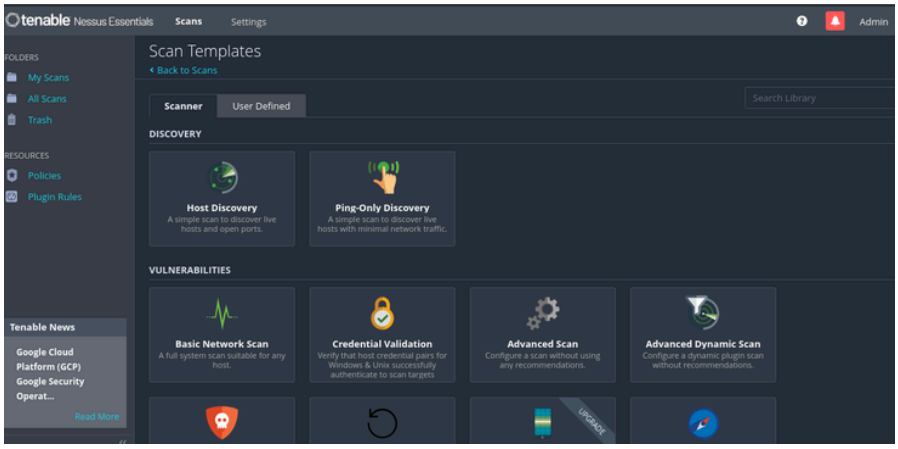


Figure 81 : Sélection des Modèles de Policy

L'interface de configuration affiche l'onglet "Settings" avec un menu latéral contenant cinq catégories : BASIC, DISCOVERY (actuellement sélectionné), ASSESSMENT, REPORT et ADVANCED.
Nous configurons une nouvelle policy nommée "Basic Network Scan" dans l'onglet "Settings".

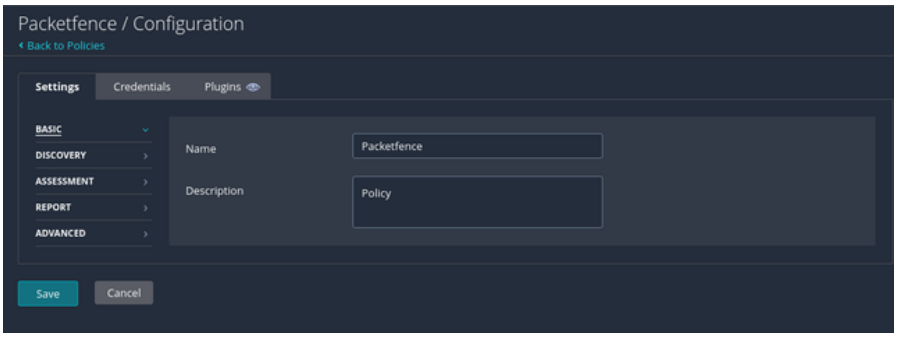


Figure 82: Informations Générales de la Policy

Dans la section Discovery, le Scan Type est configuré sur "Port scan (all ports)" pour analyser l'ensemble des 65535 ports TCP/UDP disponibles. Les General Settings activent deux options : "Always test the local Nessus host" pour scanner également le serveur Nessus lui-même, et "Use fast network discovery" pour accélérer la détection des hôtes. Les Port Scanner Settings définissent que tous les ports (1-65535) seront scannés, que netstat sera utilisé si des identifiants sont fournis pour obtenir la liste des ports ouverts directement depuis le système, et que le scanner SYN sera utilisé si nécessaire pour détecter les ports ouverts de manière furtive. Enfin, la section Ping hosts using liste les méthodes utilisées pour vérifier si un hôte est actif avant de le scanner : TCP pour les connexions TCP, ARP pour la résolution d'adresses au niveau liaison, et ICMP avec 2 tentatives pour les requêtes ping classiques.

- Onglet Assessment

La section Assessment configure l'analyse approfondie des vulnérabilités web. Le type de scan est réglé sur "Scan for all web vulnerabilities (complex)", ce qui permet une évaluation complète. Les options générales activées permettent de réduire les fausses alertes, d'analyser les scripts CGI et d'effectuer des tests approfondis. Pour les applications web, Nessus commence le scan depuis la racine /, explore jusqu'à 1000 pages et 6 répertoires, teste les vulnérabilités web connues, exécute chaque test pendant 10 minutes maximum, utilise toutes les méthodes HTTP et tente de détecter les attaques de type HTTP Parameter Pollution (tentative de détection des injections de paramètres HTTP).

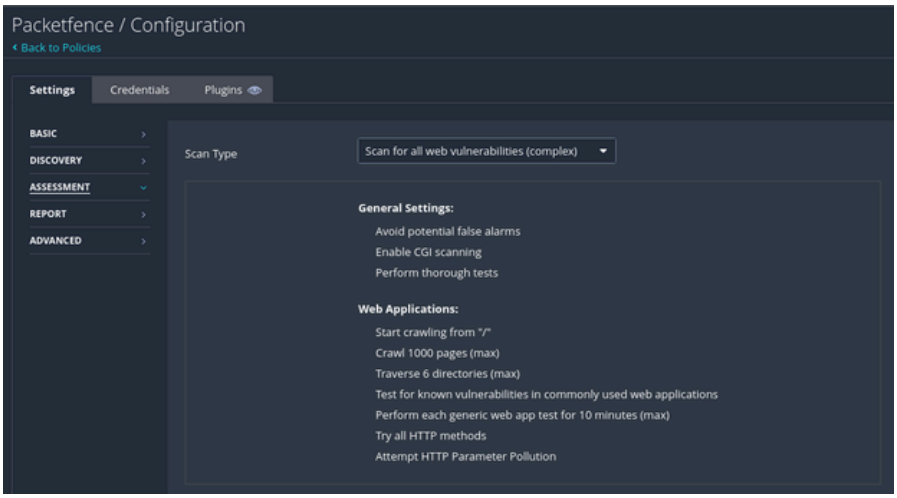


Figure 83: Configuration de la Section Assessment de la Policy

- Onglet Advenced:

L'interface affiche la section ADVANCED qui permet de configurer les options de performance du scan.
Scan Type : Configuré sur "Default" pour utiliser les paramètres standard de Nessus.
Performance options : Trois paramètres optimisent la vitesse et l'efficacité du scan - "30 simultaneous hosts (max)" permet de scanner jusqu'à 30 équipements en parallèle pour accélérer le processus, "4 simultaneous checks per host (max)" autorise l'exécution de 4 tests simultanés sur chaque hôte, et "5 second network read timeout" définit un délai d'attente de 5 secondes pour les réponses réseau avant de considérer qu'un test a échoué.

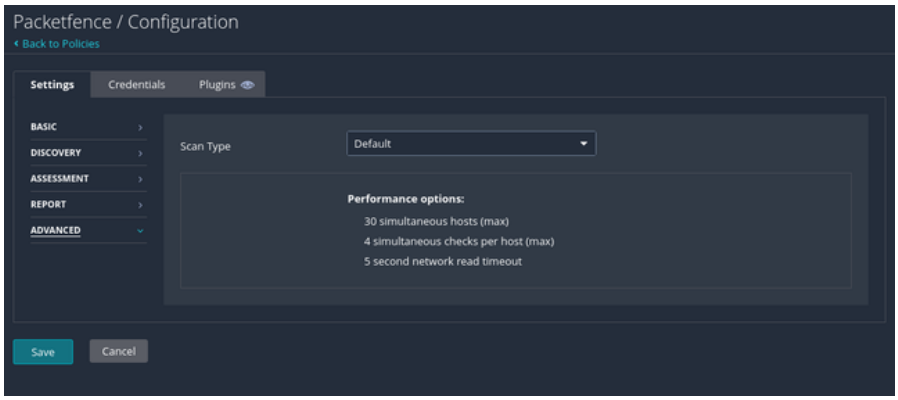


Figure 84: Configuration de la Section Advanced de la Policy

5.4. Creation de scanner dans Packetfence

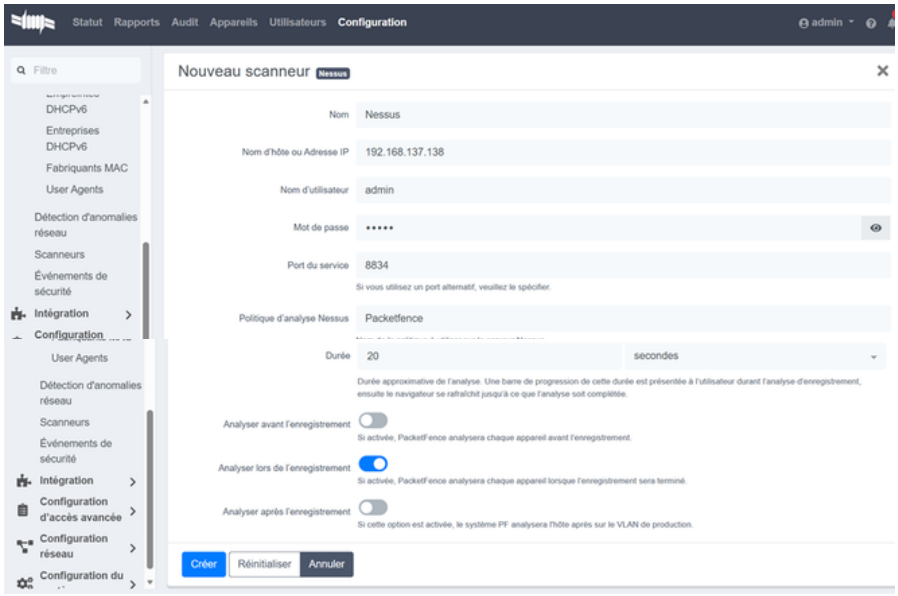


Figure 85: Configuration du Scanner Nessus dans PacketFence

PacketFence est configuré pour se connecter au scanner Nessus via l'adresse IP 192.168.137.138 sur le port 8834 en utilisant le compte administrateur. La policy de scan Nessus créée précédemment est sélectionnée pour définir les tests de vulnérabilités à effectuer. L'option "Analyser lors de l'enregistrement" est activée, ce qui signifie que chaque équipement sera automatiquement scanné par Nessus au moment de son enregistrement sur le réseau.

5.5. Ajout de scanner dans Profil d'authentification:

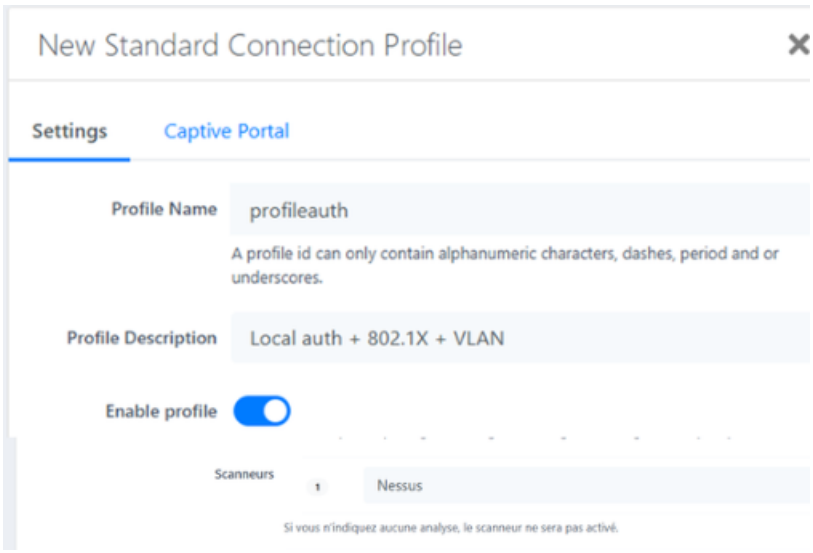


Figure 86: Ajout de scanner dans le profil dauthentification

5.6. Création automatique d'un évènement de sécurité:

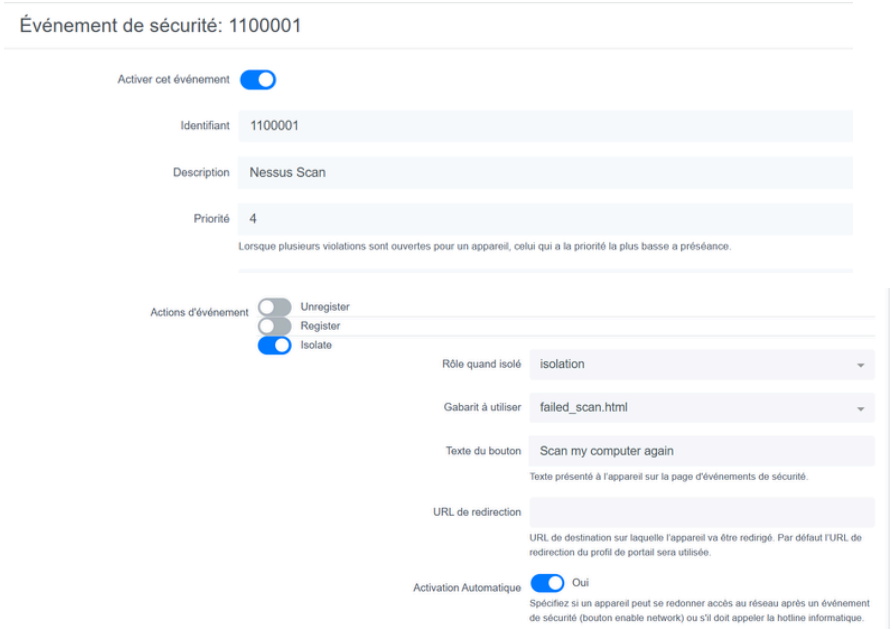


Figure 87: Événement de Sécurité Nessus dans PacketFence

Cette image présente l'interface de configuration d'un événement de sécurité Nessus dans PacketFence. En résumé, il s'agit d'une règle de sécurité automatique qui intervient lorsqu'un scan Nessus détecte une vulnérabilité sur un appareil connecté au réseau.

Les éléments clés de cette configuration sont :

- Identifiant 1100001 : numéro unique de l'événement.
- Description : "Nessus Scan" : indique que la détection se base sur les résultats d'analyse de Nessus.
- Priorité 4 : niveau de gravité modéré.
- Actions associées à l'événement : lorsqu'il se déclenche, le système :
  - Isole l'appareil concerné (quarantaine réseau)
  - Change son rôle vers "failed_scan.html"
  - Affiche un bouton "Scan my computer again" pour inviter l'utilisateur à relancer l'analyse

L'objectif est simple : dès qu'une vulnérabilité est détectée sur un poste, PacketFence isole automatiquement l'appareil et demande à l'utilisateur de résoudre le problème avant de rétablir l'accès normal au réseau. C'est un exemple concret de mécanisme NAC (Network Access Control) basé sur l'état de sécurité des terminaux.

Test de Conformite :

Après l'authentification réussie de la machine Kali de l'utilisateur Jean, nous allons procéder au test de conformité de cette machine. Tout d'abord, il est important de montrer que PacketFence a correctement détecté notre machine.

Dans l'interface Search Nodes de PacketFence, on peut constater que l'appliance a identifié la machine Kali. Le nœud correspondant s'affiche avec son adresse MAC, son adresse IP et le statut actif associé. On remarque également que le propriétaire est défini sur Registration et que le rôle appliqué est également Default, ce qui confirme que PacketFence a bien reconnu la machine Kali.

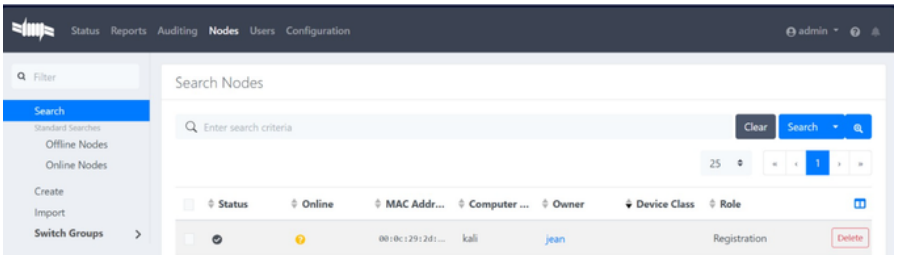


Figure 88 : Détection du poste Kali dans PacketFence (Search Nodes)

Nous avons accédé au tableau de bord (Dashboard) de PacketFence afin d'obtenir une vue d'ensemble des événements de sécurité en cours. Le Dashboard présente plusieurs indicateurs essentiels pour la supervision du réseau, notamment les statistiques des nœuds enregistrés, les événements de sécurité ouverts (Open Security Events), ainsi que les tendances d'activité réseau. Cette interface centralisée offre une visibilité en temps réel sur l'état de conformité des équipements connectés et permet d'identifier rapidement toute anomalie ou alerte de sécurité concernant les nœuds détectés, incluant notre machine Kali sous test. Grâce à cette vue synthétique, les administrateurs peuvent assurer un contrôle proactif et une supervision efficace de l'ensemble des postes intégrés dans l'architecture de contrôle d'accès réseau (NAC), facilitant ainsi la détection précoce des incidents de sécurité et la mise en conformité des appareils avant leur accès complet aux ressources du réseau.

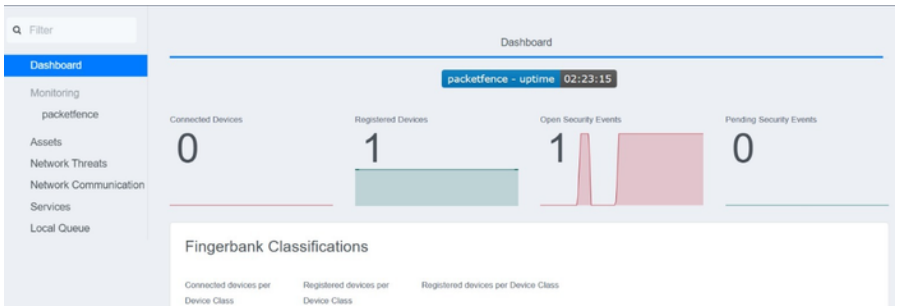


Figure 89 : Vue du Dashboard PacketFence

- **Verifcation de la connectivite entre packetfence et Nessus**

PacketFence utilise une intégration native avec les scanners de vulnérabilités tels que Nessus pour effectuer des contrôles de conformité sur les équipements du réseau. Lorsqu'un poste se connecte, PacketFence identifie son adresse IP via DHCP, ARP ou RADIUS. Ensuite, PacketFence envoie une requête via l'API REST de Nessus afin de déclencher un scan ciblé de cette adresse IP. La communication se fait en HTTPS (port 8834), ce qui garantit la sécurité des échanges. Nessus exécute alors l'analyse en utilisant la politique de scan prédéfinie par l'administrateur. Une fois le scan terminé, PacketFence interroge à nouveau l'API du scanner pour récupérer les résultats.

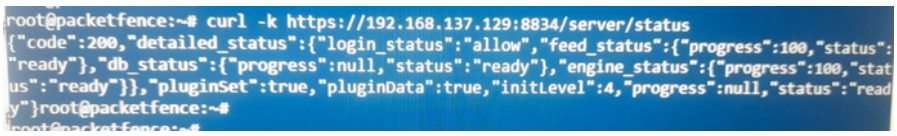


Figure 90: commande curl exécutée depuis le serveur PacketFence

Cette commande est une vérification essentielle : elle confirme que Nessus est fonctionnel, accessible depuis PacketFence et prêt à recevoir les requêtes API pour lancer les scans de conformité. Ce test valide donc la connectivité du serveur et l'état du scanner avant l'intégration avec PacketFence.

- **Configuration d'un événement de sécurité associé au scan Nessus dans PacketFence**

Dans PacketFence, un Security Event (événement de sécurité) est une action déclenchée automatiquement suite à une anomalie détectée : non-conformité, violation de politique d'accès, tentative d'accès non autorisée, détection d'un service suspect ou non-respect d'une règle réseau. Chaque événement est associé à un endpoint via son adresse MAC, et PacketFence peut appliquer des mesures telles que l'isolation, le blocage temporaire ou la redirection vers un portail de remédiation.

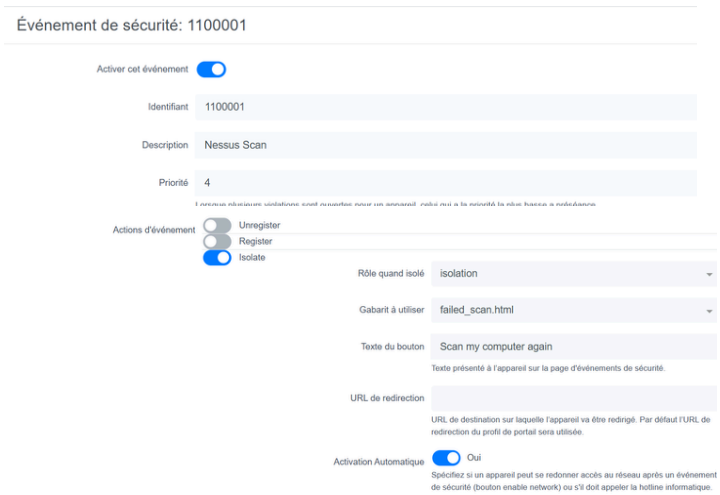


Figure 91: Configuration d'un événement de sécurité associé au scan Nessus dans PacketFence

Une fois l'événement de sécurité configuré dans PacketFence, nous avons procédé à l'exécution effective du scan de vulnérabilités sur la machine Kali via le scanner Nessus. Cette étape constitue le cœur du processus de vérification de conformité, permettant d'évaluer l'état de sécurité du poste avant de lui accorder un accès complet aux ressources du réseau. Le scan Nessus a été lancé en ciblant spécifiquement l'adresse IP assignée à la machine Kali détectée précédemment par PacketFence. L'analyse de vulnérabilités examine de manière exhaustive différentes facettes de la sécurité du système : les ports ouverts, les services exposés, les versions de logiciels installés, les correctifs de sécurité manquants, ainsi que les configurations potentiellement dangereuses. Les résultats de ce scan détermineront si la machine respecte les politiques de sécurité définies et si l'événement de sécurité 1100001 doit être déclenché.

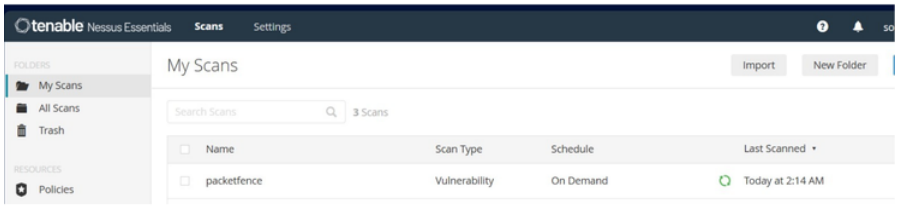


Figure 92 : Résultats des scans Nessus pour le nœud Kali

Cette vue synthétique affiche les informations essentielles pour l'évaluation de la conformité : le nombre total de vulnérabilités détectées, catégorisées par niveau de sévérité (Critical, High, Medium, Low, Info) et représentées visuellement par un graphique circulaire. Les détails complémentaires incluent la politique de scan appliquée, l'horodatage de l'exécution, le type de scanner utilisé (CVSS v3.0) ainsi que sa localisation (Local Scanner).

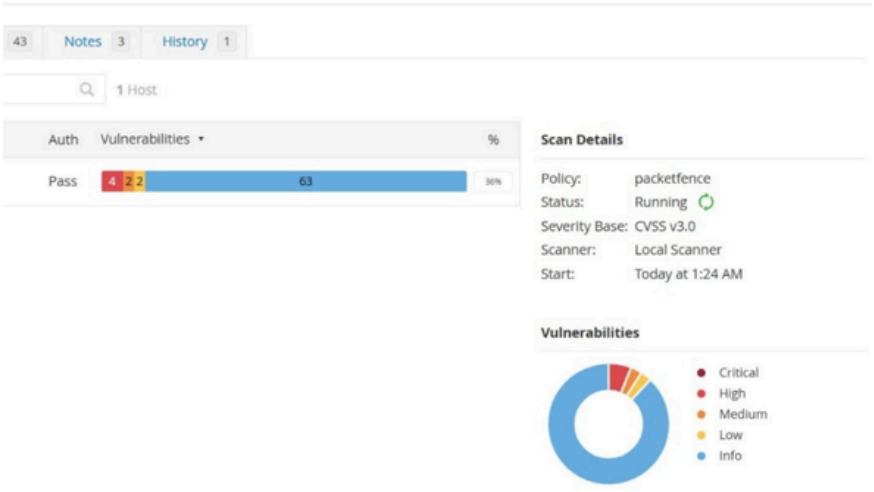


Figure 93 : Détail et classification des vulnérabilités détectées par Nessus

Suite à l'exécution du scan Nessus et à la détection de vulnérabilités sur la machine Kali, PacketFence a automatiquement déclenché les événements de sécurité correspondants conformément aux règles préalablement configurées. Pour vérifier l'application effective de ces mécanismes de contrôle, nous avons consulté l'onglet "Security Events" associé au nœud de la machine Kali (adresse MAC : 00:0c:29:2d:d7:5e).

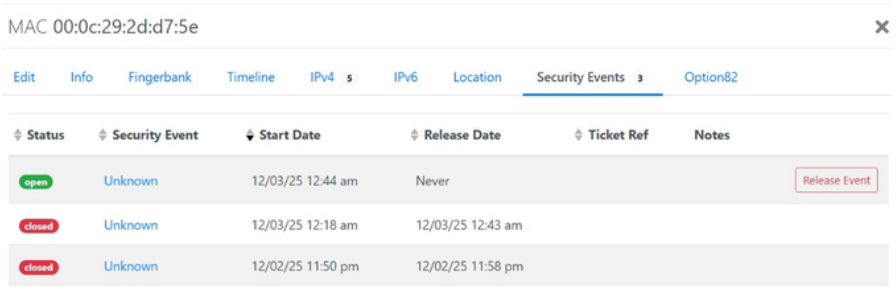


Figure 94: Security Events pour le nœud Kali dans PacketFence

6. Conclusion:

Ce chapitre consacré à la mise en œuvre de PacketFence a permis de concrétiser l'approche théorique du contrôle d'accès réseau (NAC) appliquée à une infrastructure réseau universitaire. En partant du déploiement d'une architecture réseau segmentée avec des VLANs dédiés (registration, isolation, normal) et contrôlée par l'authentification 802.1X, nous avons pu établir un système de contrôle d'accès dynamique qui isole efficacement les équipements non conformes, réduisant ainsi les risques de sécurité.

La phase de réalisation a mis en lumière l'importance de l'interopérabilité entre les trois piliers du NAC. L'intégration réussie de l'authentification 802.1X via RADIUS assure désormais l'identification des utilisateurs avant l'accès au réseau, tandis que l'intégration de Nessus Essentials comme scanner de vulnérabilités garantit la conformité de sécurité des équipements connectés. Parallèlement, la configuration des profils de connexion et des événements de sécurité a transformé une infrastructure réseau classique en un véritable système de défense en profondeur capable de détecter, isoler et remédier automatiquement aux menaces.

Enfin, la validation de cette architecture par la configuration complète de la base de données MariaDB, l'installation et l'intégration du scanner Nessus, ainsi que la création des policies de scan personnalisées ont démontré la viabilité et l'efficacité du système. La solution déployée répond aux exigences de disponibilité, d'intégrité et de confidentialité nécessaires dans un environnement académique où la sécurité doit s'adapter aux comportements variés des utilisateurs tout en maintenant la fluidité d'accès aux ressources pédagogiques.

CONCLUSION GÉNÉRALE

Au terme de ce projet consacré au Network Access Control (NAC), nous avons pu approfondir l'un des mécanismes les plus importants de la sécurité réseau moderne. Le NAC s'impose aujourd'hui comme une solution incontournable pour protéger les infrastructures informatiques face à l'augmentation des menaces, à la multiplication des équipements connectés et à la complexité croissante des environnements numériques.

À travers l'étude et la mise en œuvre d'une architecture NAC, nous avons pu comprendre comment un réseau peut analyser, filtrer et contrôler l'accès des utilisateurs et des machines en se basant sur des politiques strictes. Ce travail nous a notamment permis de :

- appréhender les principes fondamentaux du modèle 802.1X,
- manipuler le rôle central du serveur RADIUS dans le processus d'authentification,
- observer l'interaction entre les commutateurs, les utilisateurs et les serveurs,
- analyser le concept de posture de sécurité et la vérification de conformité des terminaux,
- comprendre comment des politiques adaptées permettent d'autoriser, restreindre ou bloquer l'accès.

La mise en œuvre pratique réalisée dans ce projet nous a également permis d'identifier les avantages concrets d'une solution NAC : amélioration du niveau de sécurité, meilleure visibilité sur les équipements connectés, capacité de réaction face aux comportements suspects, et renforcement global de la gouvernance du réseau. Le NAC devient ainsi une véritable couche de défense, proactive et intelligente, qui contribue à réduire les risques d'intrusion, de propagation de malware ou d'accès non autorisé.

Ce projet nous a également sensibilisés aux défis liés au déploiement d'un NAC dans un environnement réel, notamment la complexité de la configuration, la nécessité de bien maîtriser chaque composant (switch, serveur, certificats, politiques), ainsi que l'importance de tester les scénarios d'accès pour garantir une expérience utilisateur fluide. Ces difficultés constituent autant d'opportunités d'apprentissage qui nous ont permis d'améliorer nos compétences techniques et notre compréhension globale de la sécurité réseau.

En conclusion, cette expérience a été particulièrement enrichissante sur les plans théorique et pratique. Elle nous a permis non seulement de renforcer notre maîtrise des concepts de sécurité mais aussi de développer une approche structurée pour concevoir, implémenter et évaluer une solution NAC. Dans un contexte où les cybermenaces évoluent constamment, ce type de projet représente un atout essentiel pour mieux comprendre les bonnes pratiques de cybersécurité et préparer une intégration professionnelle solide dans le domaine.

Perspectives et Évolutions Futures

Bien que la solution NAC mise en œuvre dans ce projet permette déjà de renforcer efficacement le contrôle d'accès au réseau, plusieurs axes d'amélioration et de développement peuvent être envisagés afin d'étendre ses fonctionnalités et d'optimiser sa performance.

1. Intégration avec des solutions de sécurité avancées
2. L'une des évolutions les plus prometteuses consiste à intégrer le NAC avec d'autres outils de cybersécurité tels que les SIEM, les IDS/IPS ou encore les solutions EDR/XDR. Ces interconnexions permettraient d'automatiser davantage les réponses aux incidents, de corréler les événements en temps réel et d'améliorer la détection des comportements anormaux.
3. Automatisation et orchestration des politiques
4. Le déploiement de politiques dynamiques basées sur le contexte (lieu, heure, type d'appareil, état de conformité) pourrait permettre un contrôle plus précis et plus flexible. L'utilisation de scripts d'orchestration ou de solutions comme Ansible faciliterait la gestion massive des configurations, réduirait les erreurs humaines et améliorerait la réactivité du système.
5. Support des environnements Zero Trust
6. Les architectures Zero Trust reposent sur le principe « Never trust, always verify ». Intégrer le NAC dans une approche Zero Trust constituerait une évolution naturelle, où chaque accès serait continuellement vérifié et réévalué. Cela permettrait d'obtenir une sécurité renforcée dans les environnements hybrides ou multi-cloud de plus en plus courants.
7. Extension du contrôle aux environnements IoT
8. Avec l'augmentation rapide des objets connectés (IoT), souvent peu sécurisés, il devient indispensable de prévoir un module NAC dédié à l'identification, la segmentation et la surveillance des appareils IoT. Une évolution future pourrait inclure la classification automatique de ces appareils et la mise en quarantaine des équipements à risque.
9. Amélioration de l'expérience utilisateur
10. Une autre perspective importante concerne la simplification du processus d'authentification pour les utilisateurs, notamment grâce à l'utilisation de solutions Single Sign-On, de certificats plus faciles à déployer ou encore d'outils self-service. Cela réduirait les frictions tout en conservant un même niveau de sécurité.
11. Renforcement de la conformité et des audits
12. Le NAC pourrait intégrer davantage de fonctionnalités de reporting, de journaux détaillés et d'audits automatisés afin d'aider les organisations à répondre aux exigences réglementaires (ISO 27001, RGPD, PCI-DSS). Une telle évolution faciliterait la surveillance continue et la traçabilité des accès réseau.
13. Utilisation de l'intelligence artificielle

Références

1. IEEE 802.1X – Port-Based Network Access Control
https://standards.ieee.org/standard/802_1X-2020.html
2. Documentation RADIUS (RFC 2865)
https://datatracker.ietf.org/doc/html/rfc2865
3. Cisco – Network Access Control (NAC) Overview
https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
4. Aruba ClearPass – NAC Documentation
https://www.arubanetworks.com/products/security/network-access-control/
5. Fortinet – FortiNAC Technical Overview
https://www.fortinet.com/products/identity-access-management/fortinac
6. Microsoft – NAP & NAC Concepts
https://learn.microsoft.com/en-us/windows/security/threat-protection/network-access-protection
7. Juniper Networks – NAC Architecture
https://www.juniper.net/documentation/en_US/junos/topics/concept/user-access-control-overview.html
8. 802.1X Explained – PowerCert Animated Videos
https://www.youtube.com/watch?v=2Ab1lT8_L7U
(Très clair, simple, parfait pour les étudiants)
9. Network Access Control (NAC) Tutorial – CBT Nuggets
https://www.youtube.com/watch?v=jYq7aj3oF38
10. RADIUS Server Explained – PowerCert
https://www.youtube.com/watch?v=Le-cK_cWE9w
11. Cisco ISE (NAC) Full Explanation – Network Direction
https://www.youtube.com/watch?v=UUf8KeqMbQw
12. Zero Trust Architecture (pour les perspectives futures)
https://www.youtube.com/watch?v=Vc0nJjokM7A