RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mira Abderrahmane de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

Pour L'obtention du Diplôme de Fin de Cycle en Informatique

Spécialité : *Administration et Sécurité des Réseaux*

Thème

Analyse, conception et mise en place d'une solution open source pour la gestion de l'accés au réseau au sein du district GPL de Naftal

---

Réalisé par :

- M^{elle} KHODJA Kenza
- M^{elle} SACI Sabrina

Défendu le 30/06/2025, devant le jury composé de :

Présidente du jury	M^{me} BATTAT Nadia	UAMB - Bejaia.
Examinateur	M^{r} MOKTEFI Mohand	UAMB - Bejaia
Examinateur	M^{r} CHEKRID Mohamed	UAMB - Bejaia
Examinatrice	M^{me} HOUHA Amel	UAMB - Bejaia.
Encadré par	M^{me} BACHIRI Lina	UAMB - Bejaia.

Année Universitaire 2024 – 2025

Remerciements

Avant de présenter notre travail,

Nous tenons à remercier le bon Dieu de nous avoir aidé et donné le courage et la volonté pour réaliser ce travail et aboutir à son accomplissement.
Nous exprimons nos remerciements à notre encadrante Madame BACHIRI Lina pour son valeureux conseils et orientations qui nous ont permis de mener à bien notre projet.
Nos vifs remerciements aux membres de jury pour l'honneur qu'ils nous font en acceptant d'examiner et d'évaluer ce travail.
Nous tenons enfin à remercier nos chers parents et toute personne pour l'encouragement et le soutien qui nous ont apportés durant ce travail et tous ceux qui ont contribué de près ou de loin à sa réussite.

Dédicace

Je dédie ce modeste travail

Je Dédie Ce Travail, Tout D'abord A Ma Chère Famille, Sans Qui, Ma Vie N'aurait Pas Etée Aussi Belle, Riche Et Réussie. Une Pensée Spéciale A Mon Père, Paix A Son Ame, Qui Reste A jamais Présent Dans Mon Cœur.

Je Les Remercie Pour Leur Encouragement Et Leur Présence A Mes Côtés Tout Au Long De Mon Parcours : Ma Chère Mère, Mes Frères et Soeurs (Hani,Amine,Lehna Et Lina), Mon Chère Ami Slimane Et Mes Proches.

A Mon Binôme ,Avec qui on Partagé Ce Parcours Difficile Mais Accompli SACI Sabrina.

Un Grand Merci à Tous Mes Amis Que Je Ne Peux Malheureusement Pas Citer Tellement La Liste Est Longue, Mais Merci D'avoir Fait Partie De Ma Vie Et D'avoir Embellie Ma Vie Avec Une Amitié Si Sincère Qui fait Mon Bonheur.

KHODJA Kenza

Dédicace

J*e dédie ce modeste travail*

Je Dédie Ce Travail, avant tout, à ma précieuse famille, pilier de ma vie. Je leur suis infiniment reconnaissante pour leur soutien indéfectible et leur présence constante à mes côtés.

À ma mère Saida, pour son amour inconditionnel, sa force et sa bienveillance.

À Mes Frères (Hamza,Anis Et Akkache) ainsi qu'à mes proches.

En hommage à mon père, dont la mémoire m'a portée tout au long de ce parcours. Une pensée particulière pour lui, que Dieu ait son âme.

À mon binôme, KHODJA Kenza, avec qui j'ai traversé ce parcours exigeant, mais couronné de succès. Merci pour cette belle aventure partagée.

Je souhaite également exprimer ma profonde gratitude à tous mes amis, trop nombreux pour être cités individuellement. Sachez que vous occupez tous une place spéciale dans ma vie. Merci d'avoir contribué à mon bonheur par votre amitié sincère et précieuse.

SACI Sabrina

Table des matières

Table des figures

Liste des tableaux

Liste des Abréviations

AAA	Authentication,Authorization,Accounting
ACL	Access ControlList
AD	Active Directory
AD DS	Active Directory Domain Services
API	Application Programming Interface
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CHAP	Challenge-Handshake Authentication Protocol
CN	Common Name
DB	Data Base
DC	Domain Component
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DN	Distinguished Name
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IoT	Internet of Things
ISE	Identity Services Engine

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

MAB MAC Authentication Bypass

MAC Media Access Control

MAN Metropolitan Area Network

MDM Mobile Device Management

MitM Man-in-the-Middle

MSCHAPv2 Microsoft Challenge-Handshake Authentication Protocol version 2

NAC Network Access Control

NAD Network Access Device

NAS Network Access Server

NAP Network Access Protection

NGFW Next-Generation Firewall

NPS Network Policy Server

OSI Open Systems Interconnection

OU Unité d'Organisation

PAE Port Access Entity

PAN Personal Area Network

PAP Password Authentication Protocol

PEAP Protected Extensible Authentication Protocol

QoS Quality of Service

RADIUS Remote Authentication Dial-In User Service

RBAC Role-Based Access Control

SHA Secure Hash Algorithm

SHV System Health Validator

SMS Short Message Service

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SQL Structured Query Language

SSH Secure Socket Shell

TCP Transmission Control Protocol

Telnet Telecommunication Network

URL Uniform Resource Locator

VLAN Virtual Local Area Network

VPN Virtual Private Network

WAN Wide Area Network

Introduction générale

À l'heure actuelle, la sécurité des réseaux est devenue un axe de recherche et un fondement fondamental de toute organisation connectée. Avec la multiplication des postes de travail, des objets connectés et des accès à distance, savoir précisément qui se connecte au réseau, quand, dans quelles conditions et à quel privilège devient un enjeu incontournable. C'est donc à juste titre que les solutions de contrôle d'accès réseau pouvant être désignées par leurs sigles NAC (Network Access Control) se forgent un sens très particulier.

Exposé dans ce sujet, ce mémoire, présente la mise en œuvre de PacketFence, une solution NAC open-source au sein du réseau de Naftal, afin d'assurer un accès sécurisé des clients au réseau. L'objectif est, à travers d'une approche pratique, de démontrer comment une entreprise peut s'appuyer sur une solution libre, fiable et évolutive face aux exigences de sécurité d'aujourd'hui.

Les différentes étapes qui ont été suivies à la réalisation de ce projet furent de réaliser une analyse approfondie des besoins, se lancer dans la recherche des différentes technologies de contrôle d'accès réseau disponibles sur le marché puis enfin de procéder à l'implémentation opérationnelle au sein de l'organisation. Suite à une analyse critique des différentes offres, PacketFence s'est ainsi avéré être le meilleur choix afin de créer une solution NAC open-source performante et évolutive compatible avec la majeure partie des équipements de réseau existants ainsi que la plupart des systèmes d'exploitation.

L'étude a utilisé le réseau physique du district GPL de la société Naftal et avait pour objectif de configurer une architecture sécurisée apte à contrôler les connexions filaires et sans fil, à administrer l'authentification via 802.1X, MAB, ou le portail captif, et à suivre efficacement les activités du réseau. Ce travail a également permis de configurer un switch Cisco, d'intégrer un serveur Active Directory et de tester différentes politiques d'accès selon les profils utilisateurs.

Pour mieux structurer cette étude, le mémoire est organisé selon la logique suivante :

Chapitre 1 : Généralités et étude de l'existant Présentation des bases des réseaux informatiques, des protocoles, des types de réseaux, et des notions essentielles liées à la sécurité (principes fondamentaux, types de cyberattaques, solutions de sécurisation).

Chapitre 2 : État de l'art sur la gestion des accès au réseau, Ce chapitre présente les bases conceptuelles du contrôle d'accès réseau (NAC). Il en décrit le fonctionnement, les composants, les protocoles associés, puis propose une comparaison détaillée des solutions disponibles sur le marché, en mettant en avant les alternatives open source.

Chapitre 3 : Présentation de la solution de contrôle d'accès, Ce chapitre débute par une présentation de Naftal et du district GPL de Béjaïa. Il expose ensuite la problématique de sécurité identifiée et analyse les besoins précis du réseau. Sur cette base, PacketFence est retenue comme solution adaptée. Le chapitre décrit ses fonctionnalités, son architecture, ainsi que les interactions prévues à travers un diagramme de cas d'utilisation.

Chapitre 4 : Mise en place de la solution, Ce chapitre décrit la mise en œuvre concrète de PacketFence dans l'environnement réseau cible. Il commence par une présentation de l'architecture du réseau, puis détaille l'ensemble des étapes techniques : configuration du switch Cisco, installation de PacketFence, intégration avec Active Directory, et définition des politiques d'authentification (802.1X, MAB, portail captif). La dernière partie est consacrée aux tests de validation pour vérifier le bon fonctionnement du système mis en place.

Enfin, nous clôturons ce mémoire par une conclusion synthétisant l'ensemble du projet, les connaissances acquises tout au long de sa réalisation.

1

Généralités et Etude de l'Existant

1.1 Introduction

Les réseaux informatiques contribuent de manière efficace à la communication et au partage d'informations à l'échelle mondiale. Toutefois, leur croissance rapide pose de nombreux défis, en particulier en termes de sécurité. Ce chapitre présente les fondamentaux des réseaux informatiques, en présentant leurs concepts de base, leurs différentes typologies ainsi que les protocoles qui les régissent. Par la suite, il souligne les défis liés à la sécurité des réseaux, en détaillant les principes fondamentaux, les cyberattaques courantes et les solutions de protection existantes. Cette étude de l'existant constitue une base solide pour comprendre les défis et les solutions liés à la sécurisation des infrastructures réseau.

1.2 Généralité sur les réseaux informatique

Les réseaux informatiques permettent la communication et le partage de données entre plusieurs appareils. Ils ont devenus indispensables dans notre quotidien, aussi bien les environnements personnel que professionnels.

1.2.1 Réseau informatique

Un réseau informatique est un ensemble de matériels et de logiciels interconnectés permettant l'échange d'informations et le partage de ressources, avec ou sans fil. Le réseau le plus simple relie deux ordinateurs en pair à pair, où chaque machine est au même niveau et peut partager des données et des périphériques. Les réseaux modernes, plus complexes, adoptent souvent une architecture client/serveur, où un ordinateur central (serveur) fournit des services et des ressources aux autres ordinateurs (clients) [1].

1.2.2 Types des réseaux

Selon leurs zones de couvertures, différents types de réseau existent :

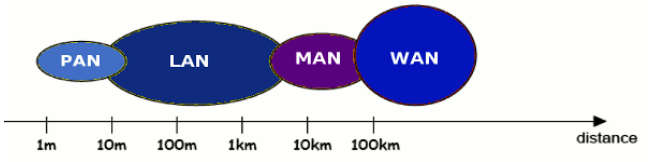


Figure 1.1 – Types des réseaux informatique
[2]

Réseau personnel PAN (Personal Area Network) : Pour permettre l'échange de données entre appareils modernes comme les smartphones, tablettes et ordinateurs. Ils peuvent être filaires (USB, FireWire) ou sans fil (WPAN) avec des technologies comme Bluetooth, ZigBee, ou Z-Wave. Un réseau Bluetooth est appelé « Piconet ». Ces réseaux ont une portée limitée à quelques mètres et ne conviennent pas pour des connexions entre pièces ou bâtiments différents [3].

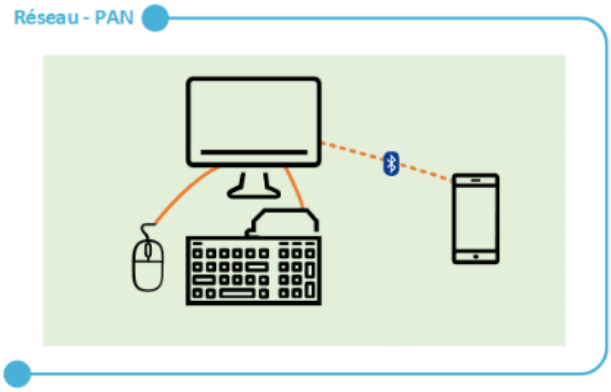


Figure 1.2 – Réseau PAN
[4]

Réseau local LAN (Local Area Network) : Est un réseau local dépendant de plusieurs ordinateurs, que ce soit dans une maison, une entreprise ou une institution publique. Il utilise principalement le protocole Ethernet via des câbles en cuivre ou en fibre optique. Des équipements comme hubs, commutateurs et ponts sont nécessaires pour connecter plusieurs appareils. Les LAN permettent un transfert rapide de données et facilitent le partage de fichiers, d'imprimantes et d'applications [5].

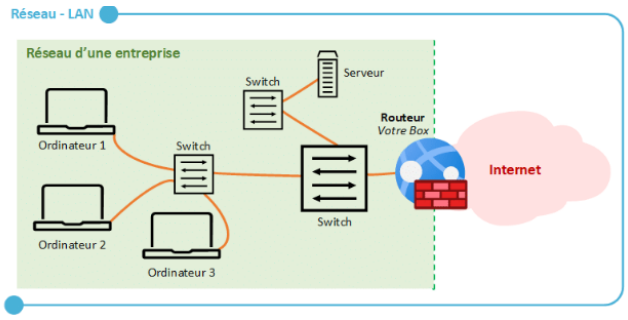


Figure 1.3 – Réseau LAN
[6]

Réseau métropolitain MAN (Metropolitan Area Network) : Est un réseau dont l'étendue est de plusieurs dizaines de kilomètres, donc on peut considérer que c'est un réseau à l'échelle d'une ville entière. L'objectif d'un réseau MAN est d'interconnecter plusieurs réseaux LAN par l'intermédiaire de liaison à très haut débit grâce à la fibre optique et ce que l'on appelle une dorsale haute capacité (backbone). En fait, ces différents réseaux locaux (LAN) dispersés dans une ville sont physiquement reliés entre eux pour constituer le réseau MAN [7].

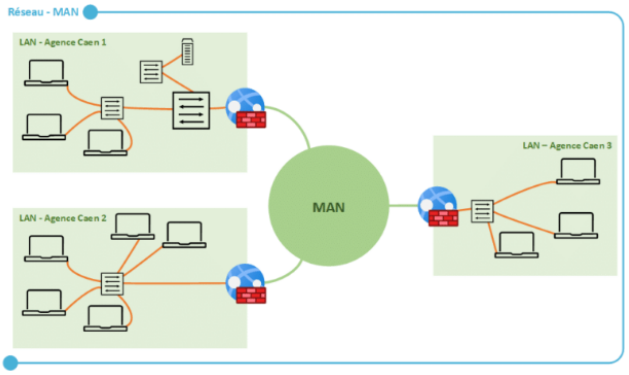


Figure 1.4 – Réseau MAN
[8]

Réseau étendu WAN (Wide Area Network) : Un WAN est un réseau étendu qui couvre de vastes zones géographiques, allant d'un pays à plusieurs continents. Il s'étend bien au-delà des réseaux locaux (LAN) et métropolitains (MAN). Internet est un exemple typique de WAN public, dépendant de milliards d'appareils à travers le monde. Les infrastructures du WAN reposent principalement sur la fibre optique, les liaisons satellites et les câbles sous-marins pour assurer la connectivité internationale [9].

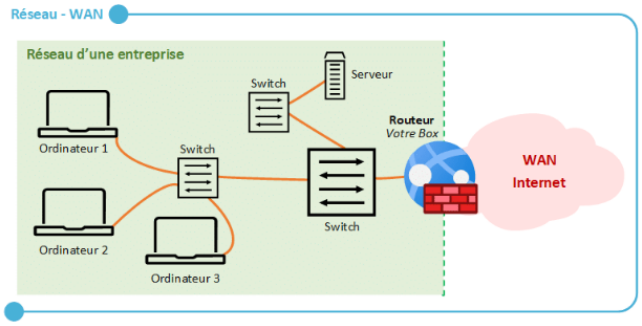


Figure 1.5 – Réseau WAN
[10]

1.2.3 Protcoles réseaux

Les protocoles réseau sont un ensemble de règles, de conventions et de structures de données qui dictent la manière dont les appareils échangent des données sur les réseaux.

— Pour comprendre les nuances des protocoles réseau, il est impératif de connaître d'abord le modèle d'interconnexion des systèmes ouverts (OSI). Considéré comme le principal modèle architectural des communications de travail sur Internet, il est structuré en sept couches, jouant chacune un rôle spécifique dans le traitement et la transmission des données. La majorité des protocoles réseau utilisés aujourd'hui sont basés sur cette architecture, permettant une meilleure standardisation et interopérabilité des systèmes [11].Les couches sont :

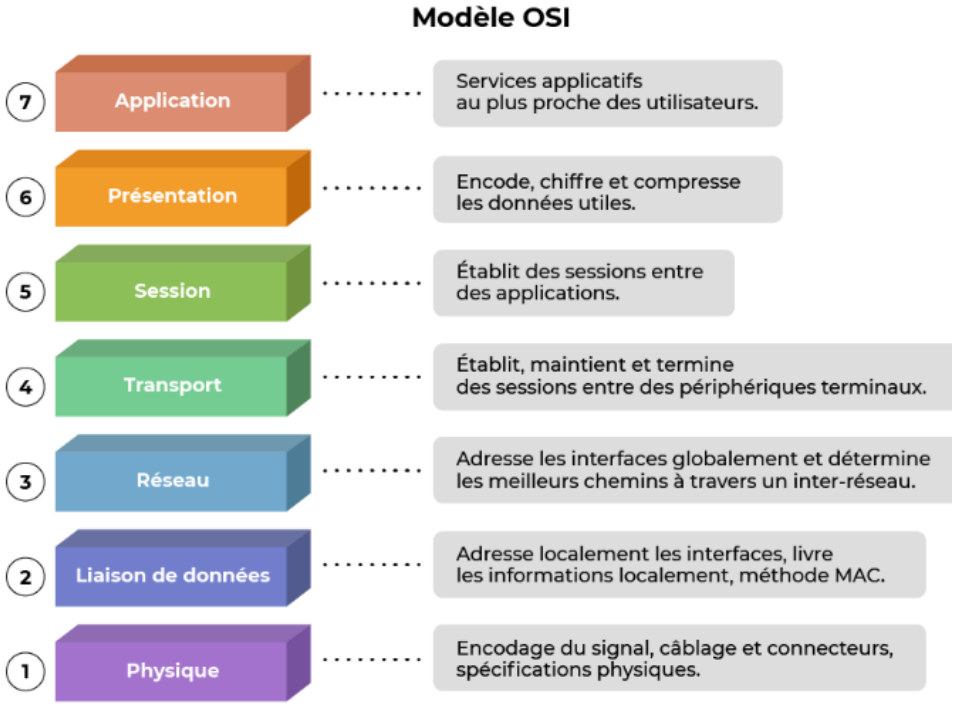


Figure 1.6 – Modèle OSI
[12]

- Couche physique (1) : Transmission des données sur le support physique.

• Couche de liaison de données (2) : Détection et correction des erreurs, organisation des données en trames.
• Couche réseau (3) : Routage des données à travers le réseau en utilisant des adresses logiques.
•Couche transport (4) : Gestion des flux de données, contrôle de la transmission.
• Couche session (5) : Établissement et gestion des sessions de communication.
• Couche présentation (6) : Formatage et compression des données.
• Couche application (7) : Services applicatifs tels que FTP, HTTP, SMTP, etc.

— **Catégories de Protocoles Réseau :**

1. Protocoles de Liaison de Données (Couche 2) :
   Ces protocoles permettent la communication entre appareils sur le même réseau local (LAN).

   •Ethernet (IEEE 802.3) : Protocole filaire utilisé dans la plupart des réseaux locaux.
   •Wi-Fi (IEEE 802.11) : Protocole sans fil pour les connexions réseau.
   •PPP (Point-to-Point Protocol) : Utilisé pour les connexions directes comme les modems.

2. Protocoles Réseau (Couche 3) :
   Ces protocoles assurent l'adressage et le routage des paquets entre différents réseaux.

   •IP (Protocole Internet) :IPv4 : Adresse 32 bits (ex. 192.168.1.1) et IPv6 : Adresse 128 bits (ex. 2001 :db8 : :1).
   •ICMP (Internet Control Message Protocol) : Utilisé pour le diagnostic réseau (ex. ping).
   •ARP (Address Resolution Protocol) : Associe une adresse IP à une adresse MAC.

3. Protocoles de Transport (Couche 4) :
   Ils gèrent la transmission des données entre applications sur différents hôtes.

   •TCP (Transmission Control Protocol) : Communication fiable, orientée connexion.
   •UDP (User Datagram Protocol) : Communication rapide, non fiable.

4. Protocoles Applicatifs (Couche 7) :
   Ils permettent la communication entre les applications utilisateur.

   •HTTP/HTTPS (HyperText Transfer Protocol Secure) : Navigation web.
   •FTP (File Transfer Protocol) : Transfert de fichiers.
   •DNS (Domain Name System) : Traduction des noms de domaine en adresses IP.
   •SMTP/POP3/IMAP : Protocoles de messagerie électronique.

1.3 Généralités sur la sécurité des réseaux informatiques

La sécurité des réseaux informatiques est essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des informations. Face aux nombreuses menaces, elle joue un rôle crucial dans la protection des systèmes et des communications.

1.3.1 Sécurité informatique

La sécurité informatique, aussi appelée sécurité des technologies de l'information(IT), consiste à protéger les actifs informatiques d'une organisation, y compris les systèmes informatiques, les réseaux, les appareils numériques et les données, contre les accès non autorisés, les violations de données, les cyberattaques et autres activités malveillantes [13].

1.3.2 Principes fondamentaux de la sécurité des réseaux

La cybersécurité se base sur cinq notions : la **Disponibilité**, l'**Intégrité**, la **Confidentialité**, l'**Authentification** et la **Non-répudiation**. Ces cinq principes forment l'acronyme **DICAN** [14][15].

Disponibilité :
La disponibilité permet le bon fonctionnement du système d'information. Le but est de garantir que les services et les données soient disponibles au moment requis sans interruption non désirée.

— La panne de Facebook, Messenger, WhatsApp et Instagram du 4 octobre 2021 qui a duré 6h30.

— Une panne de plusieurs heures ayant affecté les clients Microsoft 365, Outlook et Teams en octobre 2020.

— Les pannes des fournisseurs d'accès à Internet (Orange, SFR et Bouygues) qui rendent indisponible toutes les données et services qui sont dans le cloud.

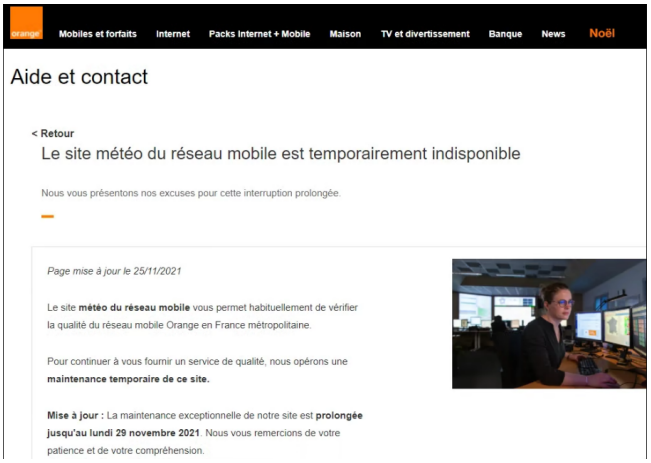


Figure 1.7 – Du 25 au 29 novembre 2021, le site de surveillance des incidents mobiles chez Orange était en panne

[13]

Intégrité :
C'est-à-dire garantir que les données sont bien celles que l'on croit être, consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

Confidentialité :
Consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées, consiste aussi à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

Authentification :
L'authentification consistant à assurer que seules les personnes autorisées aient accès aux ressources. L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

Non-répudiation :
La non-répudiation assure qu'une action ou une transaction ne peut pas être niée par l'une des parties impliquées. Elle garantit la preuve de l'origine et de l'authenticité d'un accord, qu'il s'agisse d'une communication entre machines ou d'un échange entre utilisateurs, grâce à des mécanismes comme les signatures numériques.

1.3.3 Cyberattaques

Une cyberattaque est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques [16].

1.3.4 Différents types de cyberattaques

Les réseaux informatiques sont exposés à différentes attaques, dont l'objectif est soit de mettre fin à leur activité, soit de dérober ou de modifier les informations [16].

Les attaques par ingénierie sociale (la faille humaine)

1. **Le Hameçonnage (Phishing)** :L'attaque par hameçonnage correspond à l'envoi d'un e-mail contenant une pièce jointe ou un lien cliquable frauduleux. L'astuce consiste à donner à cet e-mail toutes les apparences d'un message fiable et authentique. La pièce jointe ou le lien ont pour but principal de collecter des données sensibles, d'inciter la personne réceptrice du message à télécharger un logiciel malveillant sur son ordinateur ou de la conduire à effectuer une autre action qui sera bénéfique aux cybercriminels.
   - **Exemples :**
     - E-mails frauduleux imitant des services bancaires, demandant à la victime de "vérifier son compte".
     - Pièces jointes ou liens infectés qui, une fois ouverts, téléchargent un logiciel malveillant.
2. **Le Spear Phishing** : Le hameçonnage peut souvent rimer avec un envoi groupé et grossier. Lorsque les cyberattaquants mènent un travail de préparation plus poussé, dont

le but est d'obtenir un e-mail plus difficile à identifier comme frauduleux, l'attaque prend le nom de spearphishing. Le message est davantage personnalisé et dissémine des références personnelles afin de tromper le destinataire : les chances de réussite de l'attaque sont plus grandes.

   — **Exemple :** Un e-mail qui semble provenir du responsable IT de l'entreprise, incluant des références spécifiques à des projets internes, et demandant de changer son mot de passe ou de cliquer sur un lien pour "mettre à jour un document important".

3. **L'Usurpation de Compte** : Un attaquant a pu accéder au compte d'un utilisateur cible après avoir préalablement obtenu ses identifiants. La récupération de ses identifiants a pu se faire en amont par du phishing, du bruteforce de compte, du social engineering (en se faisant par exemple passer pour l'un de ses proches) ou encore, ils ont pu être achetés directement sur des forums spécialisés sur le darkweb (dataleaks contenant des credentials obtenus par des dumps de bases de données ou des "infostealers").

   — **Exemples :**

      — Utilisation de techniques de brute force pour deviner le mot de passe d'un compte de messagerie.

      — Achat de bases de données compromises contenant des informations d'identification volées.

4. **Le Piratage de Compte** : Le **piratage de compte**, bien qu'il puisse être lié à l'usurpation d'identité, Les hackers se contentent ici de cracker le mot de passe d'un compte de messagerie, d'un accès à un compte bancaire ou du compte administrateur du site d'une entreprise. Les répercussions sont potentiellement lourdes.

   — **Exemples :**

      — Cracking de mots de passe pour accéder à des comptes financiers ou à des plateformes d'entreprise sensibles.

5. **La Fraude au Président (FOVI)** : La **fraude au président** (ou FOVI) est une attaque par ingénierie sociale particulièrement dangereuse, qui cible les entreprises.La fraude au président consiste à se faire passer pour le président d'une société, dans le but d'obtenir un virement bancaire auprès de cette dernière ou d'autres informations. Le lien peut aussi bien être établi par e-mail que par téléphone, en insistant sur la nécessité de procéder au virement sous les plus brefs délais et en maintenant l'opération confidentielle. Le Faux Ordre de Virement est toujours lié à un virement international.

   — **Exemples :**

      — Faux e-mails ou appels où l'attaquant se fait passer pour le directeur général, en incitant les employés à transférer des fonds rapidement pour une "opération urgente".

      — Attaque de social engineering par excellence, elle a été démocratisée par Gilbert Chikli en 200.

Les attaques par logiciel malveillant

Les réseaux informatiques et les utilisateurs individuels font face à une menace sérieuse due aux attaques de logiciels malveillants (malwares). Ces malwares peuvent être dissimulés dans des pièces jointes d'emails, des liens à cliquer ou encore sur des sites internet piratés. Souvent, ces attaques sont associés à des méthodes d'ingénierie sociale comme le phishing, qui cherchent à tirer parti de la vulnérabilité humaine pour réussir l'infection. Voici quelques illustrations de ces attaques malicieuses et leur mécanisme.

1. **Le rançongiciel (Ransomware)** : Le principe du rançongiciel est simple. Les hackers s'introduisent dans un équipement informatique par le biais d'un simple e-mail contenant, le plus souvent, une pièce jointe infectée : on retrouve le piège du phishing. Après téléchargement de la pièce jointe, l'ordinateur ayant servi de point d'entrée ne répond plus. Un message de demande de rançon tourne en boucle sur tous les ordinateurs : pour reprendre la main sur ses appareils et récupérer ses données, la victime est invitée à payer une rançon. En échange, les hackers promettent de livrer la clé de déchiffrement ou le mot de passe qui permettront de débloquer les machines infectées. Dans les faits, de nombreuses rançons sont payées. Le paiement de la rançon a, de fait, tendance à encourager les hackers et à faire de la technique du ransomware une cyberattaque fructueuse, donc dangereuse.

   — **Exemples :**

      — Les Les signalements par des entreprises françaises ont été multipliés par 4 sur la seule année 2020.

      — en 2021, 35 nouveaux groupes de cybcerciminels spécialisés dans le rançongiciel ont été répertoriés.

2. **La désactivation des outils de sécurité via un Cheval de Troie** : Le Cheval de Troie est un programme malveillant caché dans un programme d'apparence inoffensive, qui fait partie de l'outillage informatique choisi par l'utilisateur lui-même. Ce sont précisément les outils de sécurité qui sont, la plupart du temps, choisis pour dissimuler un Cheval de Troie. En 2019, des hackers ont mené une attaque de ce genre contre les fonctionnalités de protection en temps réel de Windows Defender. Le Cheval de Troie, baptisé Novter, procédait de manière classique en téléchargeant de logiciels malveillants supplémentaires sur le système déjà infecté.

   Dans certains cas, les attaquants se contentent d'empêcher l'exécution de programmes spécifiques en ajoutant des certificats, dont le rôle est d'inscrire les programmes de sécurité sur une blacklist pour empêcher le bon fonctionnement de ces outils de protection. Parfois, un port à numéro élevé peut être visé, afin de pouvoir écouter des conversations. De manière générale, le Cheval de Troie sert – comme son nom l'indique parfaitement – à ouvrir des portes d'accès qui permettront aux criminels de nuire.

Les attaques réseau

Les attaques réseau sont principalement basées sur des compétences techniques avancées, visant à perturber ou à compromettre le fonctionnement des infrastructures informatiques.

1. **Le Déni de Service (DoS) et le Déni de Service Distribué (DDoS)** : Le déni de service, également connu sous le terme de DdoS Attack (Distributed Denial of Service Attack) rejoint le palmarès des cyberattaques les plus couramment utilisées contre les entreprises et les services publics. Il s'agit de gêner le bon fonctionnement d'un réseau informatique en bloquant le serveur web, le serveur de fichiers ou les services de messagerie. Toute l'opération consiste à saturer le système ciblé. Pour cela, les hackers s'appuient sur un grand nombre de bots et de robots de relais.
2. **L'Attaque par Drive-by Download** : Le Drive-by Download se produit lorsque des malwares ou des logiciels malveillants sont téléchargés et installés automatiquement sur le système d'un utilisateur sans son consentement, simplement par la visite d'un site web malveillant.
3. **L'Attaque de l'Homme du Milieu (MitM)** : L'attaque dite de l'homme du milieu, plus connue sous l'appellation Man-in-the-middle Attack ou sous l'abréviation MitM, consiste à se placer en position d'interception sur le réseau, par exemple un attaquant qui usurperait l'adresse MAC du routeur afin de récupérer les communications. Concrètement, un hacker ou un serveur est positionné entre deux points communicants : un client et un serveur, par exemple.

   Différentes méthodes existent pour réussir à se greffer de la sorte sur un chemin de communication. Un attaquant peut ainsi se mettre en écoute sur un service de Wifi public pour collecter des données. Il est également possible de créer un faux réseau Wifi (rogue AP), destiné à tromper les utilisateurs et à faire en sorte qu'ils s'y connectent. Si le Rogue AP se fait passer pour un point d'accès légitime en utilisant un nom et une configuration similaire, on parle alors de "Evil Twin" et dans ce cas précis, les individus pensent se connecter à leur réseau habituel, alors qu'ils se connectent en réalité au réseau de l'attaquant et mettent en danger leurs données." Enfin, l'attaquant peut usurper le protocole de résolution d'une adresse (ARP spoofing) sur un réseau local pour récupérer les trames réseaux qui transitent alors par lui.

   Dans une configuration plus artisanale, exploitant la faille humaine, le cybercriminel peut choisir de récupérer et d'utiliser de vieux e-mails dans le but d'entrer en contact avec un utilisateur et de le tromper sur son identité réelle. L'objectif est de le conduire à transmettre ses accès. C'est la tactique dite du rejeu ou de la relecture.

1.3.5 Solutions et Technologies de Sécurisation

La sécurité des réseaux combine de nombreuses couches de défenses en périphérie et dans le réseau. Chaque couche de sécurité du réseau met en œuvre des politiques et des contrôles. Les utilisateurs autorisés obtiennent un accès aux ressources de réseau, tandis que les intervenants malveillants sont bloqués et ne peuvent pas accomplir leurs exploitations et menaces [18][19].

1. **Protection du réseau**
   - **Pare-feu :** contrôle et filtre le trafic réseau selon des règles prédéfinies pour autoriser ou bloquer le trafic.Un pare-feu peut être matériel, logiciel ou une combinaison des deux.
   - **Systèmes de Détection et de Prévention d'Intrusion (IDS/IPS) :** Ils surveillent constamment le réseau pour détecter et bloquer les activités malveillantes.
   - **Réseaux Privés Virtuels (VPN) :** Ils chiffrent les communications pour assurer une connexion sécurisée pour les employés à distance.
   - **NAC (Network Access Control) :** Limite l'accès au réseau aux seuls dispositifs autorisés.
   - **CDN (Content Delivery Network) :** Protège contre les attaques DDoS et accélère la distribution du contenu.
2. **Contrôle d'accès et authentification :**
   - **MFA (Multi-Factor Authentication) :** Pour une sécurité renforcée, combinant un mot de passe avec un code unique.
   - **Chiffrement :** L'utilisation d'algorithmes de cryptage (AES, RSA, TLS/SSL) pour garantir la confidentialité des échanges et assurer que seules les personnes autorisées peuvent lire les données.
   - **Gestion des clés de chiffrement :** Stocke et gère en toute sécurité les clés.
   - **Signature numérique :** Permet de vérifier l'authenticité d'un message ou d'un document.
   - **Gestion des Droits d'Accès (RBAC, ACLs) :** Met en œuvre le principe du moindre privilège, contrôle d'accès qui définit les rôles et les autorisations de chaque utilisateur.
3. **Supervision et Réaction aux Incidents**
   - **SIEM (Security Information and Event Management) :** Centralise la surveillance en collectant et analysant les journaux et événements de sécurité.
   - **Centre d'Opérations de Sécurité (SOC) :** Une équipe dédiée pour surveiller et répondre aux menaces.
   - **XDR (Extended Detection and Response) :** Offre une vue consolidée des menaces.

4. **Protection des points de terminaison (endpoints) :**
   - **EDR (Endpoint Detection and Response) :** Surveille les comportements suspects sur les postes de travail et les serveurs.
   - **Antivirus et Antimalware :** Détecte et supprime les logiciels malveillants avant qu'ils ne causent des dommages.
   - **DLP (Data Loss Prevention) :** Empêche la fuite de données sensibles.

1.4 Conclusion

À travers ce chapitre, nous avons approfondi les bases des réseaux informatiques et les principaux enjeux liés à leur sécurité. Nous avons mis en lumière les différentes typologies de réseaux, les essentiels à leur fonctionnement, ainsi que les menaces qui les ciblent, telles que les cyberattaques par ingénierie sociale, logiciels malveillants ou attaques réseau. Face à ces risques, des solutions et technologies de sécurisation sont continuellement développées afin de garantir l'intégrité, la confidentialité et la disponibilité des systèmes d'information. Cette étude préliminaire constitue une base essentielle pour comprendre l'importance de la sécurisation des réseaux, un enjeu majeur dans le contexte numérique actuel.

2

État de l'Art sur la Gestion des Accés au Réseau

2.1 Introduction

La protection des réseaux d'entreprises est devenue un problème essentiel. S'il s'agit de protéger son réseau des menaces extérieures, les dégradations internes peuvent se révéler nettement plus dommageables. De ce fait il est nécessaire de développer, au sein des entreprises, des architectures permettant d'accroître la sécurité informatique.
Dans ce chapitre nous allons présenter le contrôle d'accès au réseau avec ses protocole, ainsi que les différentes solutions qui assurent le contrôle de conformité.

2.2 Les fondamentaux du contrôle d'accès au réseau (NAC)

Le contrôle d'accès au réseau joue un rôle principale dans la sécurisation des connexions. Il permet de vérifier chaque tentative d'accès afin de protéger les ressources contre les intrusions.

2.2.1 Défintion du NAC

est un mécanisme de sécurité visant à restreindre l'accès à un réseau privé ou d'entreprise aux seuls utilisateurs et appareils autorisés. Il permet d'assurer que seuls les équipements conformes aux politiques de sécurité et les utilisateurs dûment authentifiés peuvent se connecter, renforçant ainsi la protection contre les accès non autorisés et les menaces potentielles [20].

2.2.2 Principe du fonctionnement du NAC

Le fonctionnement du NAC repose sur plusieurs étapes clés [21] :

1. **Identification et authentification des utilisateurs et des appareils :** avant d'autoriser un appareil à se connecter au réseau, le NAC effectue une vérification de son identité. Cette étape comprend :
   - **Identification de l'appareil :** reconnaissance via son adresse MAC, son type (PC, smartphone, imprimante, etc.).
   - **Authentification de l'utilisateur :** basée sur :
     •Un nom d'utilisateur et un mot de passe (via LDAP, Active Directory).
     •Un certificat numérique (PKI).
     •Une authentification biométrique ou multi-facteur.
   - **Utilisation de protocoles de sécurité :**
     •802.1X (norme pour l'authentification réseau).
     •RADIUS (Service d'authentification à distance des utilisateurs).
     •LDAP (Lightweight Directory Access Protocol) pour les annuaires d'entreprise.
2. **Évaluation de la conformité :** Une fois l'utilisateur et ses appareils identifiés, le NAC vérifie que l'équipement respecte les politiques de sécurité définies . Cette évaluation comprend :
   - La présence d'un antivirus actif et à jour .
   - La mise à jour des correctifs de sécurité du système d'exploitation.
   - La configuration adéquate du pare-feu .
   - L'absence de logiciels malveillants ou de failles de sécurité connues .

   Si l'appareil est conforme aux exigences de sécurité, il est autorisé à se connecter au réseau sans restriction. En revanche, si des non-conformités sont détectées, le NAC applique des mesures adaptées pour limiter les risques :
   - Mise en quarantaine dans un réseau isolé pour éviter tout risque de propagation d'une menace.
   - Restriction d'accès à certaines ressources sensibles pour limiter les risques.
   - Redirection vers un portail de remédiation , où l'utilisateur doit corriger les problèmes détectés (ex. : installer un antivirus, mettre à jour le système) avant d'obtenir un accès complet au réseau.
3. **Application des politiques d'accès :** En fonction des résultats des étapes précédentes, le NAC applique des règles d'accès spécifiques :
   - **Accès total :** si l'appareil est conforme et que l'utilisateur est autorisé.
   - **Accès restreint :** si les critères de conformité ne sont pas remplis.
   - **Refus d'accès :** si l'appareil est considéré comme une menace.

4. **Surveillance et remédiation :** Une fois l'appareil connecté, le NAC continue de surveiller en temps réel son comportement pour détecter toute anomalie ,si un changement dans la conformité est détecté (exemple : l'antivirus est désactivé après la connexion), le NAC peut :
   — Restreindre l'accès ou isoler l'appareil .
   — Une mise à jour ou une correction avant de rétablir l'accès.
   — Débranchez temporairement l'appareil en cas de menace critique.

2.2.3 Composants du NAC

Les solutions de contrôle d'accès au réseau (NAC) se composent de plusieurs composants essentiels qui interagissent pour appliquer les politiques d'accès et sécuriser les ressources réseau. Parmi ceux-ci [22][23] :

— Agents de posture : Des logiciels installés sur les appareils clients qui évaluent leur conformité aux politiques de sécurité avant de leur permettre l'accès au réseau.
— Serveurs d'authentification : Des serveurs, tels que RADIUS, qui valident les identifiants des utilisateurs ou des appareils et déterminent leur niveau d'accès autorisé.
— Dispositifs d'accès réseau (NAD) : Des équipements comme des commutateurs ou des points d'accès sans fil qui contrôlent l'accès au réseau en fonction des décisions prises par le serveur d'authentification.
— Serveurs de politiques : Des serveurs qui définissent et appliquent les politiques d'accès en fonction des informations fournies par les agents de posture et les serveurs d'authentification.
— Serveurs d'audit : Des serveurs qui enregistrent et analysent les événements liés à l'accès réseau pour faciliter la surveillance et la génération de rapports.

2.2.4 Les protocoles du contrôle d'accès réseau

Le contrôle d'accès utilise différents protocoles pour sécuriser les connexions et gérer l'authentification des utilisateurs. Parmi ces protocoles, on trouve :

— **Protcole IEEE 802.1X :**

Le protcole IEEE 802.1X est une norme IEEE qui permet de contrôler l'accès réseau basé sur les ports . Elle fait partie du groupe de protocoles réseau IEEE 802.1. Cette norme permet de sécuriser l'accès aux réseaux locaux (LAN) ou aux réseaux locaux sans fil (WLAN) en exigeant une authentification des appareils souhaitant se connecter. Elle fournit ainsi un mécanisme d'authentification afin de garantir que seuls les dispositifs autorisés puissent accéder aux ressources réseau [24].

Dans le cadre de l'authentification réseau selon la norme IEEE 802.1X, trois acteurs principaux interagissent [25] :

1. Les demandeurs (supplicants) : Ce sont les appareils qui sollicitent l'accès au réseau, tels que les ordinateurs, imprimantes ou scanners.
2. L'authentificateur (authenticator) : Il agit comme un intermédiaire qui contrôle l'accès au réseau en vérifiant les informations fournies par le demandeur. Il peut s'agir d'un commutateur, d'un routeur ou d'un point d'accès Wi-Fi conforme à la norme IEEE 802.1X.
3. Le serveur d'authentification : Ce serveur valide les informations d'identification transmises par l'authentificateur. Il est généralement représenté par un serveur RADIUS ou une passerelle LDAP, installé dans un réseau protégé.

Fonctionnement du protocole 802.1X : Le processus d'authentification commence lorsque le supplicant tente de se connecter au réseau. L'authenticator détecte cette tentative et initie une demande d'identification. Le supplicant répond en fournissant ses informations d'identification, qui sont transmises par l'authenticator au serveur d'authentification. Si les informations sont validées avec succès, l'authenticator autorise l'accès au réseau pour le supplicant.

— **Protcole EAP :**

Le protcole EAP (Extensible Authentication Protocol) est un cadre flexible et robuste permettant de prendre en charge différentes méthodes d'authentification. Il est largement utilisé pour sécuriser les communications entre un client et un serveur, notamment dans les réseaux sans fil, les VPN et les connexions point à point [26].

Principales méthodes d'authentification EAP [27] :

— EAP-TLS : Utilise des certificats pour l'authentification des clients et des serveurs, offrant une sécurité élevée, mais avec une mise en œuvre complexe.

— EAP-TTLS : Crée un tunnel sécurisé pour chiffrer les identifiants, avec un certificat uniquement côté serveur, plus facile à configurer que EAP-TLS.

— PEAP : Semblable à EAP-TTLS, utilise aussi un tunnel sécurisé pour protéger les informations d'identification sans nécessiter de certificat client, ce qui le rend plus simple à déployer.

— EAP-MD5 : Méthode simple basée sur mot de passe. Peu sécurisé (pas de chiffrement).

— EAP-FAST : Utilise un mot de passe pour l'authentification, mais offre une sécurité moindre comparé aux autres méthodes d'authentification EAP.

— **Protcole Radius :**

La protcole Radius (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Il repose sur le principe des 3A :

— Authentication (Authentification) : le protocole permet d'effectuer une authentification distante, centraliser les données d'authentification et gérer les connexions des utilisateurs vers des services distants.
— Authorization (Autorisation) : c'est la capacité à accéder, une fois l'authentification validée, à un service ou des ressources du système d 'information.
— Accounting (Comptabilité) : le protocole est en mesure de journaliser l'activité d'un utilisateur sur le réseau (les accès, les temps de session, les ressources consommées, etc...) pour effectuer entre autres une future facturation.

Radius repose sur deux éléments principaux :

— Un serveur RADIUS : c'est un serveur qui vérifie si un utilisateur a le droit d'accéder à un réseau. Il contrôle l'accès en demandant un nom d'utilisateur et un mot de passe, puis il accepte ou refuse la connexion.
— Un client RADIUS : c'est un appareil comme un routeur, un point d'accès Wi-Fi ou un switch, qui envoie les informations de connexion des utilisateurs au serveur RADIUS pour vérifier s'ils peuvent se connecter.

Le protocole RADIUS utilise UDP, principalement sur les ports 1812 (authentification/ autorisation) et 1813 (comptabilité). Il est rapide, mais moins fiable que TCP car il ne gère pas la retransmission. Seuls les mots de passe sont chiffrés, ce qui impose l'utilisation d'un environnement sécurisé.
RADIUS fonctionne selon un modèle client/serveur où un NAS (Network Access Server) agit comme intermédiaire entre l'utilisateur et le serveur RADIUS. Ce dernier est relié à une base d'identification (base de données, Active Directory, LDAP, etc.) pour vérifier les accès des utilisateurs distants. Les échanges entre le client et le serveur sont chiffrés et authentifiés via un secret partagé.
Le sénario du principe de fonctionnement est le suivant :

— Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
— Le NAS achemine la demande au serveur RADIUS.
— Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé par l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

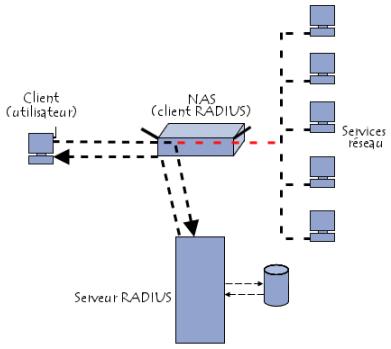


Figure 2.1 – Fonctionnement du protocole RADIUS
[27]

Le serveur RADIUS retourne ainsi une des quatres réponses suivantes [28] :

- ACCEPT : l'identification a réussi ;
- REJECT : l'identification a échoué ;
- CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un défi (en anglais « challenge ») ;
- CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

2.3 Comparatif des solutions NAC

Pleusieurs solutions existent pour sécuriser l'accèes au réseau, chacune avec ses propres caractéristiques et avantages.

2.3.1 Les solutions existantes

Les deux catégories principales dans lesquelles les solutions NAC peuvent être classées sont : les solutions libres et les solutions commerciales.

Un logiciel est considéré comme libre s'il peut être librement copier, utiliser, analyser, modifier et partager.
A l'inverse, les solutions commerciales sont remarquables par leur opacité, et sont développés par une entreprise dans le cadre de son activité.

1. **Solutions commerciales**

   NAC Cisco (Network Admission Control)

   est une solution de contrôle d'accès réseau qui identifie, authentifie et autorise les utilisateurs et les périphériques tentant de se connecter. Elle applique des politiques de sécurité pour protéger contre les menaces et les accès non autorisés. Son architecture inclut le

Cisco Identity Services Engine (ISE) pour la gestion AAA, des agents sur les terminaux pour évaluer la conformité, des commutateurs et points d'accès pour le contrôle basé sur le port 802.1X, et des serveurs de politiques pour définir les règles d'accès. Le processus typique comprend l'authentification via ISE et l'évaluation de la conformité, avec des accès accordés ou refusés selon les politiques définies [29].

Microsoft Network Access Protection (NAP)

La protection d'accès réseau (NAP) est un ensemble de composants de système d'exploitation fournissant une plateforme d'accès protégé aux réseaux privés. Cette plateforme NAP offre un moyen intégré d'évaluer l'état de santé d'un client réseau qui tente de se connecter ou de communiquer sur un réseau, et de restreindre son accès jusqu'à ce que les exigences de la politique de sécurité soient respectées.
Network Access Protection de Microsoft repose sur plusieurs composants :

- **NPS** (Network Policy Server) : un serveur RADIUS qui applique les politiques de contrôle d'accès.
- **SHV** (System Health Validator) : évalue la conformité des systèmes clients.
- **SHA** (System Health Agent) : fournit un bilan de santé des machines clientes.
- **PDP** (Policy Decision Point) : définit la politique de sécurité pour chaque machine.

L'API NAP est conçue pour les développeurs C/C++. Pour appliquer les méthodes NAP, les programmeurs doivent maîtriser les protocoles et technologies réseau tels que RADIUS (Remote Authentication Dial-in User Service), DHCP (Dynamic Host Configuration Protocol), les réseaux privés virtuels (VPN), la norme IEEE 802.1X pour l'accès filaire et sans fil, et IPsec (Internet Protocol Security).
La plateforme NAP nécessite des serveurs d'infrastructure NAP exécutant Windows Server 2008 ou version ultérieure, et des clients NAP exécutant Windows XP avec Service Pack 3 (SP3), Windows Vista ou version ultérieure. Pour plus d'informations sur les systèmes d'exploitation prenant en charge un élément de programmation particulier.

Le système peut être complété par des plugins SHA vérifiant différents aspects des terminaux (antivirus, pare-feu, registre) [30].

Juniper

Juniper Mist Access Assurance est un service avancé de contrôle d'accès réseau (NAC) basé sur le cloud qui sécurise les réseaux sans fil et filaire en fournissant un accès réseau basé sur l'identité aux appareils et aux utilisateurs. Grâce à ce service, Il permet de contrôler qui et quoi peut accéder aux réseaux. Il permet de définir des règles simples pour autoriser ou refuser l'accès à différents types d'appareils, tels que les invités, les appareils d'entreprise et les appareils générant du trafic IoT et BYOD. Le service vérifie l'identité des utilisateurs et des appareils avant de les autoriser à se connecter au réseau.

Le service utilise l'authentification 802.1X pour les appareils compatibles 802.1 et la vérification MAC Authentication Bypass (MAB) pour les appareils non 802.1X [31].

2. **Solutions libres**

Open NAC

OpenNAC est un système de contrôle d'accès réseau open source pour les environnements LAN/WAN d'entreprise. Il permet l'authentification, l'autorisation et l'audit de tous les accès au réseau, basés sur des politiques. Il est compatible avec différents fournisseurs de réseaux tels que Cisco, Alcatel, 3Com ou Extreme Networks, et différents clients tels que les PC Windows ou Linux, les Mac, les smartphones et les tablettes.

Basé sur des composants open source et auto-développés, il s'appuie sur des normes industrielles telles que FreeRadius, 802.1x, AD, LDAP, etc. Très extensible, il permet l'intégration de nouvelles fonctionnalités grâce à son architecture en plugins. Facilement intégrable aux systèmes existants , il offre également des services à valeur ajoutée tels que la gestion de la configuration, le réseau, les configurations de sauvegarde, la découverte et la surveillance du réseau [32].

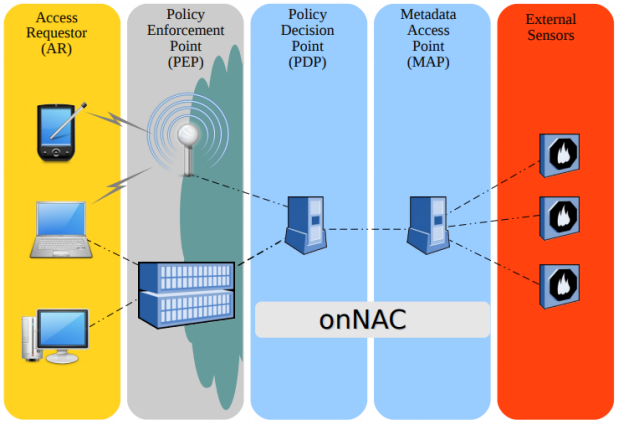


Figure 2.2 – Architecture d'une solution OpenNac [33]

PacketFence

PacketFence est une solution de contrôle d'accès réseau (NAC) entièrement prise en charge, fiable, gratuite et open source. Dotée d'un ensemble impressionnant de fonctionnalités, notamment un portail captif pour l'enregistrement et la correction, une gestion centralisée des connexions filaires et sans fil, la prise en charge de la norme 802.1X, l'isolation de couche 2 des périphériques problématiques, l'intégration avec Snort IDS et le scanner de vulnérabilités Nessus, PacketFence permet de sécuriser efficacement les réseaux, des plus petits aux plus grands réseaux hétérogènes [34].

Free NAC

FreeNAC est une solution Open Source pour gérer l'accès au réseau local et la gestion de VLAN. FreeNAC fournit une assignation de réseau local virtuel conviviale, un contrôle d'accès au réseau local (pour tous types de périphériques réseau tels que serveurs, stations de travail, imprimantes, téléphones IP, webcams, etc.), un inventaire des périphériques finaux du réseau en direct, la gestion de VLAN et permet documentation sur le câblage de correction [35].

Comparaison entre les solutions libres

Le choix de la solution NAC open source la plus appropriée dépend des besoins spécifiques de l'environnement à sécuriser. Ainsi, pour des exigences avancées et une gestion fine des accès, des solutions comme PacketFence ou OpenNAC sont particulièrement adaptées. En revanche, pour des structures plus modestes, telles qu'une petite entreprise ou un réseau domestique, une solution plus légère comme FreeNAC peut s'avérer suffisante [36].
Voici un tableau comparant les trois solutions NAC open source mentionnées ci-dessus :

Table 2.1 – Comparaison entre les solutions libres

[36][37]

Fonctionnalité	**PacketFence**	**OpenNAC**	**FreeNAC**
Prise en charge 802.1X	Oui	Oui	Oui
Portail captif	Oui	Non	Oui
Contrôle basé sur les rôles	Oui	Non	Oui
Support BYOD (Bring Your Own Device)	Oui	Oui	Non
Détection des anomalies réseau	Oui	Non	Non
Enregistrement des appareils	Oui	Non	Oui
Support de PKI / EAP-TLS	Oui	Non	Oui
Intégration LDAP / AD	Oui	Oui	Oui
Configuration de masse des appareils	Oui	Oui	Non
Basé sur des normes	Oui	Oui	Oui
Vérification de la conformité des terminaux	Oui	Oui	Oui
Gestion du réseau invité	Oui	Oui	Non
Compatibilité matérielle	Large gamme d'appareils	Large gamme d'appareils	Appareils limités

2.4 Conclusion

Les solutions NAC sont nécessaires pour protéger les réseaux en contrôlant l'accès des utilisateurs et la conformité des équipements. Elles permettent grâce aux standards 802.1X, RADIUS ou EAP de gérer dynamiquement et de façon sécurisée le traitement des connexions. Les solutions commerciales existent mais sont souvent coûteux, alors que les solutions libres, comme PacketFence ou OpenNAC, sont bien plus flexibles avec un mode de fonctionnement Open Source.

3

Conception de la Solution de Contrôle d'Accés

3.1 Introduction

Au sein de ce chapitre, nous présentons l'entreprise Naftal et relevé les besoins de l'entreprise en matière de sécurité et de contrôle d'accès, nous dressons une analyse fonctionnelle et technique afin d'adopter la solution la mieux adaptée. Cette étape comprend également le travail de comparaison entre les différentes solutions disponibles, avec un soin particulier sur les solutions open source.

Le choix de PacketFence s'est présenté comme une réponse adéquate aux contraintes de sécurité et de flexibilité.

3.2 Présentation de l'entreprise Naftal

Naftal est une société par actions (SPA) au capital social de 40 000 000 000 DA. Fondée en 1982 et filiale à 100% du Groupe Sonatrach, elle est rattachée à l'activité commercialisation.

Elle a pour mission principale, la distribution et la commercialisation des produits pétroliers et dérivés sur le marché national. Elle intervient également dans le domaine de :

• L'enfûtage des GPL.

• La formulation des bitumes.

• La distribution, le stockage et la commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux.

• Le transport des produits pétroliers.

Pour assurer la disponibilité des produits sur tout le territoire, Naftal met à contribution plusieurs modes de transport :

• Le cabotage et les pipes, pour l'approvisionnement des entrepôts à partir des raffineries.
• Le rail pour le ravitaillement des dépôts à partir des entrepôts.
• La route pour livraison des clients et le ravitaillement des dépôts non desservis par le rail.
A l'ère de la mondialisation, Naftal a jugé indispensable la mise en place d'une nouvelle organisation par ligne de produit (bitumes, lubrifiants, réseau, logistique, GPL, pneumatique, Aviation, Marine).
Naftal fournit près de 13,3 millions de tonnes de produits pétroliers par an, un chiffre appelé à augmenter avec une demande en constante croissance.
Elle a également mis en place une nouvelle vision stratégique à moyen terme orientée client avec un plan de mise en œuvre [38].

3.2.1 Présentation du District GPL de Bejaia

La branche GPL de NAFTAL est organisée en plusieurs districts, parmi lesquels figure le district de Béjaïa, situé à l'arrière-port, BP123. Cette localisation stratégique, en bordure du port, offre un avantage considérable en facilitant l'approvisionnement direct de la raffinerie vers le port par capotage. Le district est placé sous la direction d'un responsable, lui-même rattaché à la société NAFTAL, afin d'assurer efficacement la gestion des activités dans la wilaya.

3.2.2 Organigramme du district GPL Bejaia

L'organigramme présenté ci-dessous illustre la hiérarchie organisationnelle du district GPL de Béjaïa. Il présente les différents départements ainsi que les services qui leur sont rattachés, illustrant ainsi la répartition des responsabilités au sein de l'organisation district.

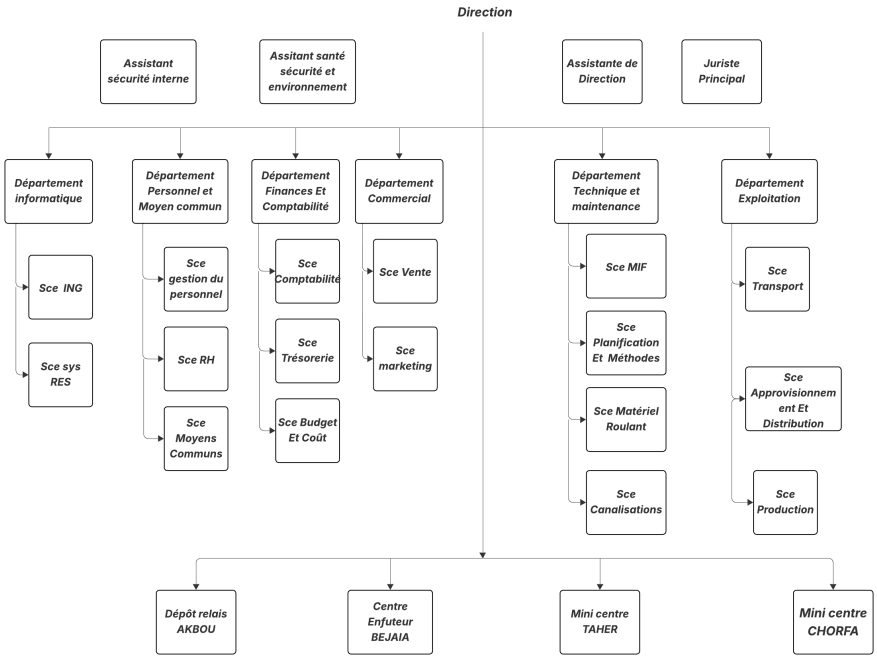


Figure 3.1 – Organigramme du district GPL (Bejaia)

3.2.3 Structure du district GPL

L'organisation interne du district GPL repose sur une structure composée de six départements. Dans le cadre de notre projet, nous nous concentrerons exclusivement sur le département informatique.

Département informatique

Le département informatique du district GPL est composé de deux services principaux :

- **Service réseau** : Ce service est chargé de :
  - La maintenance du matériel informatique.
  - La gestion des logiciels, qu'il s'agisse de systèmes d'exploitation ou d'applications.
  - L'administration et la supervision des réseaux informatiques.
- **Service Informatique de Gestion (ING)** : Ce service assure les missions suivantes :
  - Le suivi de la messagerie, (envoi et réception).
  - La consolidation et le suivi des rapports de production.
  - La gestion du P.R.C (Plan de Relation en Commun), incluant son suivi et son établissement.

3.3 Problématique

Face à la croissance du nombre de périphériques connectés et à la diversité des utilisateurs, les entreprises doivent adapter la gestion des accès à leurs réseaux. Cette complexité augmente les risques de sécurité, rendant indispensable la mise en place de solutions adaptées.

Dans ce contexte, le département réseau de l'entreprise Naftal a exprimé le besoin de mettre en place une solution de gestion des accès réseau permettant de contrôler efficacement les hôtes connectés, d'assurer leur authentification, d'identifier les utilisateurs et de segmenter dynamiquement le réseau. L'objectif est de renforcer la posture de sécurité globale du système d'information tout en maintenant un haut niveau de disponibilité et de flexibilité pour les utilisateurs. Pour cela, une solution open-source comme PacketFence, étudiée dans le chapitre précédent, s'impose comme une alternative pertinente et économique pour répondre à ces nouveaux défis.

3.4 Analyse des besoins

Pour choisir une solution NAC adaptée à Naftal, il est nécessaire d'analyser les besoins fonctionnels et non fonctionnels de l'entreprise afin de garantir que la solution réponde aux exigences techniques, organisationnelles et stratégiques du réseau.

3.4.1 Besoins fonctionnels

— **Authentification des utilisateurs et des équipements :** Garantir que chaque utilisateur ou appareil accédant au réseau est identifié et authentifié via LDAP, Active Directory ou 802.1X.

— **Contrôle d'accès réseau :** Appliquer des règles spécifiques selon le rôle (employé, invité, prestataire), le service, ou le type de terminal (ordinateur, smartphone, etc.).

— **Portail captif :** Fournir une interface d'enregistrement pour les utilisateurs invités ou les appareils BYOD, avec acceptation d'une charte d'utilisation.

— **Détection et réaction aux anomalies :** Surveiller le comportement réseau des terminaux et isoler automatiquement les postes suspects (comportement anormal, tentative d'intrusion, terminal non conforme).

— **Quarantaine des appareils non conformes :** Empêcher les terminaux non à jour (antivirus, OS, correctifs de sécurité) d'accéder au réseau avant leur mise en conformité.

3.4.2 Besoins non fonctionnels

— **Disponibilité** : Le système doit être opérationnel en continu, avec une tolérance aux pannes et une haute disponibilité, en particulier dans les sites stratégiques.

— **Scalabilité** : La solution doit pouvoir s'adapter à une montée en charge (augmentation du nombre d'utilisateurs ou d'équipements) sans perte de performance.

— **Sécurité** : La confidentialité, l'intégrité et la traçabilité des données doivent être garanties (accès aux logs, protection des échanges, etc.).

— **Efficacité de la surveillance** : Capacité à surveiller le réseau en temps réel sans impact significatif sur la performance réseau globale.

— **Coût maîtrisé** : Privilégier une solution open-source ou hybride pour réduire les coûts de licence, tout en conservant un bon niveau de support.

3.5 Choix de la solution

Le choix de la solution open-source de contrôle d'accès réseau (NAC), nous nous sommes appuyés sur le tableau comparatif présenté dans le chapitre précédent. Chaque critère a été étudié afin de déterminer la solution la plus adaptée à notre problématique.

Il existe cependant des différences significatives au niveau de la compatibilité matérielle, de la richesse fonctionnelle, des actions possibles sur le réseau, de la documentation, de la taille de la communauté et de l'ergonomie de l'interface Web. La comparaison a été recentrée sur les fonctionnalités critiques, à savoir "Contrôle d'accès basé sur les rôles", "L'enregistrement de l'appareil", "Le portail captif" et "La détection des activités anormales dans le réseau".

Parmi les solutions open source et gratuites de NAC, PacketFence, offrent une alternative économique sans compromis sur les fonctionnalités, notamment : Contrôle des accès basé sur des

politiques (policies). Gestion des invités (portail captif). Visibilité des appareils connectés au réseau. Sécurité renforcée contre les menaces internes. PacketFence se distingue particulièrement par sa capacité à répondre à ces besoins tout en restant gratuit, évolutif et simple à utiliser. PacketFence propose également la possibilité de gestion centralisée des accès filaires et sans fil, une prise de contrôle du terminal BYOD, l'isolement automatique des dispositifs non conformes et une intégration avec Active Directory.

3.6 PacketFence

PacketFence est une solution largement adoptée dans le domaine de contôle d'accès au réseau. Elle se démarque par son approche open source et sa capcité à s'adapter a divers environnements informatiques.

3.6.1 Définition

PacketFence est un logiciel libre de contrôle d'accès au réseau, développé par Inverse inc, une entreprise canadienne spécialisée dans les solutions de sécurité réseau. Il a été créé en 2003 par Dominik Gehl et Régis Balzard. Depuis sa création, PacketFence a connu plusieurs versions, la dernière en date étant la version 14.1. PacketFence est une solution non-intrusive qui fonctionne avec une multitude d'équipements réseaux (filaire ou sans fil), ce qui en fait un outil polyvalent pour le contrôle d'accès au réseau [39] [40].

3.6.2 Fonctionnalités principales

Authentification 802.1X : PacketFence prend en charge le protocole 802.1X, garantissant ainsi que seuls les utilisateurs ou dispositifs dûment authentifiés peuvent obtenir un accès au réseau.
Contrôle d'accès basé sur les rôles : Grâce à PacketFence, il est possible de mettre en place des règles d'accès précises, adaptées aux profils des utilisateurs ou aux caractéristiques des équipements connectés.
Détection et prévention des intrusions : En s'intégrant avec des systèmes IDS/IPS, PacketFence permet de détecter les comportements malveillants sur le réseau et de réagir automatiquement pour les bloquer.
Rapports et analyses : Le système offre des tableaux de bord et des rapports détaillés qui facilitent l'évaluation de la sécurité réseau et l'identification des axes d'amélioration [39] [40].

3.6.3 Composants de PacketFence

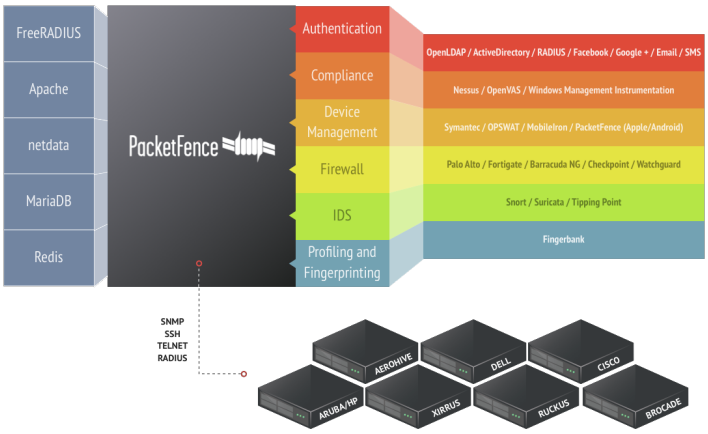


Figure 3.2 – Composants de PacketFence
[40]

3.6.4 Architecture de PacketFence

L'architecture de PacketFence est structurée en plusieurs couches fonctionnelles, chacune jouant un rôle spécifique dans le contrôle et la sécurisation des accès réseau [40].

Couche d'infrastructure : Elle regroupe les composants matériels essentiels comme les routeurs, commutateurs et pare-feux. Ces équipements assurent la connectivité physique entre les différents hôtes et segments réseau, ainsi que le routage du trafic et la première ligne de défense réseau.
Couche de services : Cette couche fournit les services applicatifs indispensables au fonctionnement du système de contrôle d'accès. Elle comprend :

- FreeRADIUS : serveur d'authentification RADIUS centralisé.
- Sources d'identités : comme OpenLDAP, Active Directory, Google, Facebook, Email ou SMS, permettant diverses méthodes d'authentification.
- Apache : utilisé comme serveur web pour l'administration et le portail captif.
- MariaDB : base de données relationnelle contenant les informations des utilisateurs, des équipements et des politiques d'accès.
- Netdata : outil de surveillance en temps réel de l'état des services et des ressources.
- Redis : base en mémoire utilisée pour accélérer les traitements et la gestion des événements.

Couche de sécurité : Elle est au cœur de la protection du réseau et comprend des outils de détection et d'analyse des menaces :

— Scanners de vulnérabilités : tels que Nessus, OpenVAS ou encore WMI pour identifier les failles de sécurité.

— IDS/IPS (détection/prévention d'intrusion) : Snort, Suricata, TippingPoint, qui inspectent le trafic à la recherche d'anomalies ou d'attaques.

— Pare-feux de nouvelle génération (NGFW) : comme ceux de Fortinet, Palo Alto, Checkpoint, Watchguard, offrant une protection avancée et contextuelle.

Couche de gestion des terminaux : Cette couche concerne la gestion des appareils qui se connectent au réseau, avec des solutions MDM (Mobile Device Management) telles que PacketFence (pour Android/iOS), Symantec, MobileIron ou OPSWAT.

Parmi les composants supplémentaires qui enrichissent la solution, on retrouve Fingerbank, une base de données d'empreintes digitales utilisée pour la reconnaissance et la classification des appareils. La solution supporte également plusieurs protocoles essentiels à la gestion et à l'administration réseau, notamment SNMP, SSH, TELNET et RADIUS. En outre, elle est compatible avec une large gamme de fabricants de points d'accès réseau, tels que AEROHIVE, ARUBA/HP, DELL, XIRRUS, CISCO, RUCKUS et BROCADE, offrant ainsi une flexibilité optimale dans l'intégration des équipements.

Parmi les différentes couches abordées précédemment, la couche de sécurité occupe une place centrale. La surveillance du réseau est composante essentielle de la cybersécurité : elle permet de détecter, analyser et répondre aux menaces en temps réel. En assurant une visibilité constante sur les activités réseau, elle contribue à identifier tout comportement suspect ou malveillant. Une surveillance efficace permet donc aux administrateurs de réagir rapidement, de réduire les interruptions de service et de garantir la continuité des opérations.

Pour cela, de nombreuses solutions de détection d'intrusion (IDS/IPS) et outils de surveillance sont disponibles, offrant un large éventail de fonctionnalités pour sécuriser les environnements réseau. Parmi les plus connues :

• Snort : Solution open source très répandue, Snort repose sur des règles prédéfinies pour détecter et bloquer les attaques réseau.
• Suricata : Un moteur de détection open source capable d'analyser le trafic en temps réel. Il propose aussi des fonctions avancées de détection d'anomalies et de prévention d'intrusion.
• Cisco Firepower : Solution commerciale intégrant l'intelligence artificielle et l'apprentissage automatique pour une protection avancée, notamment contre les attaques de type zero-day.

L'intégration de Snort et Nessus dans PacketFence

La solution PacketFence s'appuie sur Snort pour mettre en œuvre la détection d'intrusion. Grâce à ce moteur, le trafic réseau est analysé en temps réel à la recherche de signatures d'at-

taque ou de comportements suspects. En cas de détection, PacketFence peut générer des alertes ou bloquer automatiquement certains équipements ou services, renforçant ainsi la sécurité du réseau.
En complément, PacketFence intègre également Nessus, un outil spécialisé dans l'analyse des vulnérabilités. Nessus permet d'évaluer régulièrement les systèmes connectés, d'identifier les failles potentielles et de proposer des mesures correctives [41].

L'association de Snort et Nessus dans PacketFence fournit une défense en profondeur, elle combine surveillance active, détection d'anomalies et évaluation des vulnérabilités, offrant ainsi une protection complète et proactive du réseau.

Fonctionnement

1. **Tentative d'accès au réseau :** Un utilisateur ou un appareil tente de se connecter au réseau via un point d'accès ou un commutateur compatible 802.1X.
2. **Initiation de l'authentification 802.1X :** Le point d'accès ou le commutateur (authenticator) détecte la tentative de connexion et initie une session d'authentification 802.1X en utilisant le protocole EAP.
3. **Transmission des informations au serveur RADIUS :** L'authenticator transmet les informations d'identification du supplicant au serveur RADIUS intégré dans PacketFence (basé sur FreeRADIUS).
4. **Vérification auprès de la source d'identité :** L'authentification est transmise au serveur RADIUS qui s'authentifie auprès d'une source d'identité (LDAP, Active Directory, etc.).
5. **Réponse du serveur RADIUS :** Si l'authentification est réussie, le serveur RADIUS renvoie une réponse Access-Accept à l'authenticator, autorisant l'accès au réseau. Sinon, une réponse Access-Reject est envoyée.
6. **Application des politiques d'accès :** En fonction du rôle attribué à l'utilisateur ou à l'appareil (par exemple, employé, invité), PacketFence applique des politiques d'accès spécifiques, telles que l'assignation à un VLAN particulier ou la restriction de l'accès à certaines ressources.
7. **Surveillance et détection des incidents :** PacketFence surveille en continu l'activité réseau et détecte les incidents de sécurité.

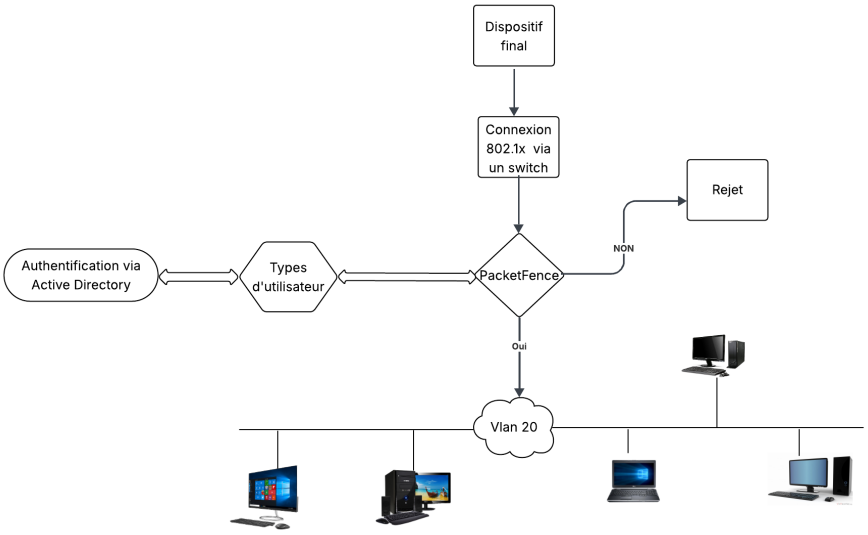


FIGURE 3.3 – Schéma illustratif du fonctionnement de PacketFence

3.6.5 Diagramme de cas d'utilisation

Identification des cas d'utilisation

Pour illustrer les interactions entre l'administrateur et le système, un diagramme des cas d'utilisation a été réalisé à l'aide de l'outil en ligne Creately.
L'acteur identifié est l'administrateur, qui interagit directement avec le système. Deux cas d'utilisation principaux ont été définis :
-La configuration du switch.
-La configuration de PacketFence.

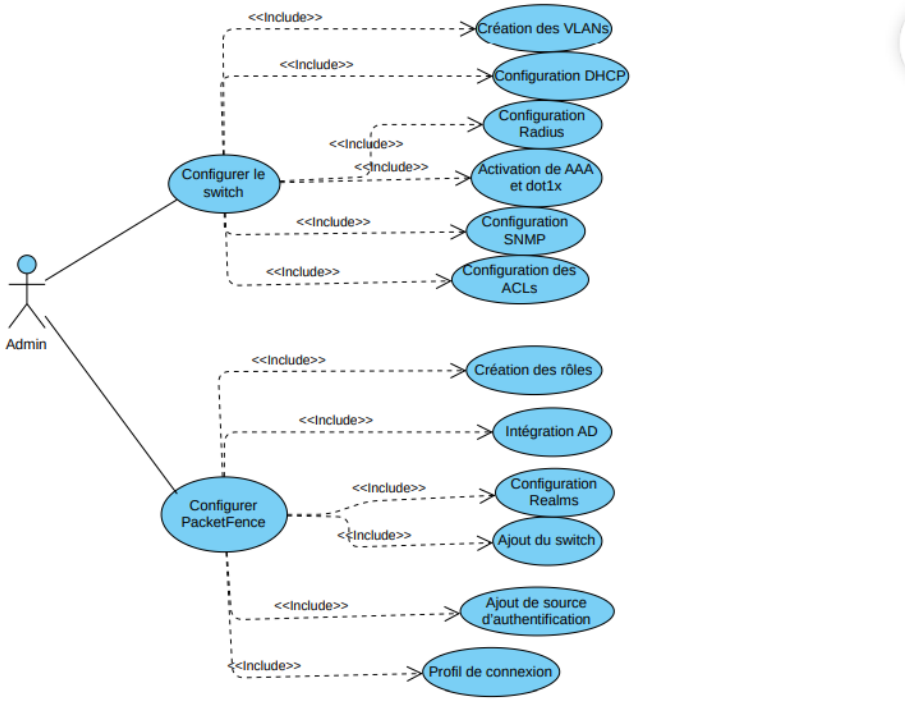


FIGURE 3.4 – Diagramme de cas d'utilisation

3.7 Conclusion

La conception de la solution a conduit à une architecture adéquate par rapport aux objectifs et contraintes de l' entreprise Naftal. En mesurant les besoins fonctionnels et non fonctionnels, nous avons pu faire le choix de PacketFence comme solution NAC (Network Access Control) libre. Cette étape constitue une base technique solide pour la phase suivante, l'implémentation, garantissant que tous les éléments nécessaires à un déploiement efficace sont planifiés et structurés.

4

Mise en Place de la Solution

4.1 Introduction

À travers ce chapitre, nous présentons La mise en œuvre d'une Solution NAC. L'objectif est de sécuriser l'accès au réseau en authentifiant les utilisateurs à travers différents mécanismes tels que 802.1X, MAB et portail captif. Nous détaillons les étapes de configuration du switch Cisco Catalyst, l'intégration avec PacketFence, ainsi que les tests d'authentification des postes clients. Cette partie illustre concrètement l'application des concepts de sécurité réseau étudiés, dans un environnement de type entreprise.

4.2 Architecture du réseau

Notre solution consiste à déployer PacketFence dans un environnement réseau restreint et isolé, afin de valider le bon fonctionnement de la stratégie de sécurité mise en place et d'observer clairement les effets de la configuration.

Ce réseau est composé d'un serveur relié à un commutateur Cisco Catalyst 3560, qui contrôle chaque nouvelle tentative de connexion via une interface Ethernet. La machine de gestion est connectée à la fois à la machine virtuelle hébergeant PacketFence, à un serveur Active Directory intégrant un service DNS, ainsi qu'à plusieurs autres équipements (imprimantes, postes de travail, téléphones IP, etc.) via le commutateur. Cette architecture permet d'appliquer la politique NAC (Network Access Control) à l'ensemble des équipements connectés.

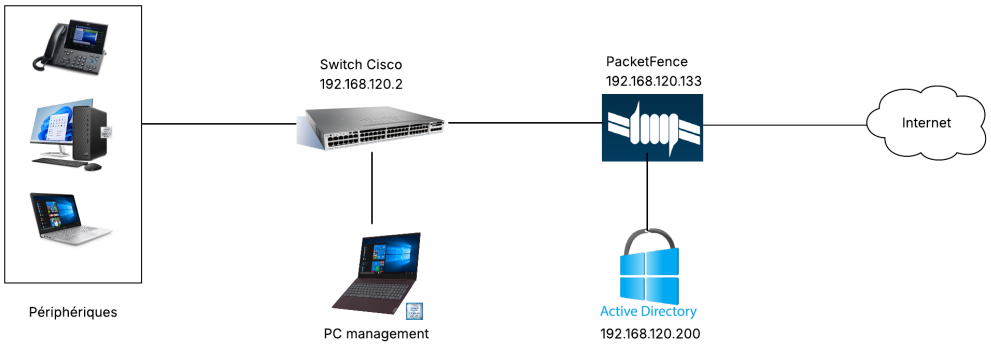


Figure 4.1 – Architecture réseau déployée

4.2.1 Informations sur notre réseau

Table 4.1 – Informations sur notre réseau

PacketFence Server	192.168.120.133
Adresse IP du switch	192.168.120.2
DNS Server	192.168.120.200
Active Directory Server	192.168.120.200
RADIUS Server	192.168.120.133

4.3 Implémentation de la solution

La première étape de l'implémentation consiste à configurer le switch Cisco, qui jouera un rôle central dans la gestion des accès au réseau.

4.3.1 Configuration du switch

Paramètres initiaux du commutateur

Dans un premier temps, il est nécessaire de configurer le switch. Pour cela, nous avons commencé par établir une connexion via le port console, en utilisant le logiciel d'émulation de terminal PuTTY. Nous avons ensuite attribuer un nouveau nom au switch à l'aide des commandes suivantes :

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

Figure 4.2 – Modification du nom du switch

Création des VLANs et configuration des interfaces

Une fois la configuration de base terminée, l'étape suivante consiste à créer les VLANs.

-VLAN 120 : dédié à la gestion, il est attribué au port trunk.

-VLAN 20 : réservé aux données, il sera utilisé pour les postes clients.

La création des VLANs, suivie de l'attribution d'une adresse IP à l'interface VLAN 20 et VLAN 120.

-Les ports reliés aux postes clients sont définis en mode access et associés au VLAN 20.

-Le port relié au serveur PacketFence est configuré en mode trunk, avec encapsulation Dot1Q, afin de transporter plusieurs VLANs.

```
NAC(config)#vlan 120
NAC(config-vlan)#name admin
NAC(config-vlan)#exit
NAC(config)#vlan 20
NAC(config-vlan)#name data
NAC(config-vlan)#
```

Figure 4.3 – Création des VLANs

```
NAC(config)#interface vlan 120
NAC(config-if)#ip a
*Mar  1 00:29:11.029: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state t
NAC(config-if)#ip add
NAC(config-if)#ip address 192.168.120.2 255.255.255.0
NAC(config-if)#no shu
NAC(config-if)#
```

Figure 4.4 – Attribution d'adresse au vlan 120

```
NAC(config)#interface vlan 20
NAC(config-if)#ip address 192.168.20.2 255.255.255.0
NAC(config-if)#no sh
NAC(config-if)#
```

Figure 4.5 – Attribution d'adresse au vlan 20

```
NAC(config)#interface range fa0/2 - 40
NAC(config-if-range)#switchport mode access
NAC(config-if-range)#switchport access vlan 20
NAC(config-if-range)#
*Mar  1 00:18:22.254: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
NAC(config-if-range)#no sh
```

Figure 4.6 – Configuration d'un port en mode access

```
NAC(config)#int fa0/1
NAC(config-if)#switchport trunk encapsulation dot1q
NAC(config-if)#switchport mode trunk
NAC(config-if)#switchport trunk allowed vlan 120,20
NAC(config-if)#no sh
```

Figure 4.7 – Configuration d'un port en mode trunk

Configuration DHCP

Il est donc nécessaire de configurer le protocole DHCP afin qu'il puisse attribuer dynamiquement des adresses IP pour le vlan 20. Nous configurons les pools DHCP pour le VLAN 20 en définissant sa plage d'adresses IP ainsi que le masque du réseau. La commande lease 100 jours permet de régler la durée pendant laquelle l'adresse IP est attribuée à l'utilisateur.

```
NAC(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.5
NAC(config)#ip dhcp pool DATA
NAC(dhcp-config)#network 192.168.20.0 255.255.255.0
NAC(dhcp-config)#defaukt-router 192.168.20.2
                        ^
% Invalid input detected at '^' marker.

NAC(dhcp-config)#default-router 192.168.20.2
NAC(dhcp-config)#lease 100
NAC(dhcp-config)#exit
NAC(config)#
```

Figure 4.8 – Application du protocole DHCP au VLAN 20

Configuration du serveur RADIUS

Création d'un modèle de serveur RADIUS pointant vers PacketFence avec une clé partagée définie "N@ftAl97".
Ensuite, spécifier l'adresse IP et les numéros de port du serveur RADIUS pour l'authentification (par défaut : 1812) et la comptabilité(par défaut : 1813).

```
NAC(config)#aaa new-model
NAC(config)#$2.168.120.133 auth-port 1812 acct-port 1813 key N@ftAl97
NAC(config)#aaa authentication dot1x default group radius
NAC(config)#aaa authorization network default group radius
NAC(config)#aaa accounting dot1x default start-stop group radius
NAC(config)#
```

Figure 4.9 – Configuration de serveur RADIUS

Cette section active l'autorisation dynamique (Change of Authorization) permettant à PacketFence d'envoyer des changements d'état en temps réel (CoA) vers le switch.

```
NAC(config)#aaa server radius dynamic-author
NAC(config-locsvr-da-radius)#client 192.168.120.133 server-key N@ftAl97
NAC(config-locsvr-da-radius)#exit
NAC(config)#
```

Figure 4.10 – Configuration de RADIUS pour l'autorisation dynamique

Activation de la fonction dot1x

L'activation de la fonction dot1x (IEEE 802.1X) sur le switch est habituellement indispensable pour déployer des mécanismes de sécurité avancés, permettant l'authentification des utilisateurs et des périphériques qui accèdent au réseau.

```
NAC(config)#dot1x system-auth-control
NAC(config)#
```

Figure 4.11 – Activer dot1x globalement

Configuration SNMP

Le SNMP (Simple Network Management Protocol) est un protocole couramment utilisé pour la gestion et la surveillance des réseaux. Nous avons configuré les chaînes de communauté pour permettre l'accès en lecture et en écriture. Ensuite, nous avons défini l'ID du moteur local (local engine ID).

```
NAC(config)#snmp-server community N@ftAl97 RO
NAC(config)#snmp-server community N@ftAl97 RW
NAC(config)#end
```

Figure 4.12 – Configuration de lecture et écriture

```
NAC#show snmp engineID
Local SNMP engineID: 800000090300002583B7C003
Remote Engine ID          IP-addr    Port
```

Figure 4.13 – Définition de l'ID du moteur

Configuration ACL

Un paramètre clé pour le NAC (Network Access Control) consiste à créer une liste de contrôle d'accès (ACL) qui filtre le trafic réseau pour limiter l'accès à certaines ressources.

Dans notre cas, l'objectif de l'ACL est de bloquer tout trafic IP provenant du VLAN de données (VLAN 20) vers le VLAN de gestion (VLAN 120). De plus, tout appareil en dehors du réseau connu ne pourra pas envoyer de trafic IP vers l'un quelconque des VLANs.

La plage IP de destination 192.168.120.0/24 n'est pas autorisée à recevoir du trafic IP en provenance de la plage IP source 192.168.20.0/24.

```
NAC(config)#ip access-list extended BLOCK_MGMT
NAC(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.120.0 0.0.0.255
NAC(config-ext-nacl)#permit ip any any
```

Figure 4.14 – Configuration ACL pour blocage Réseau

Configuration des ports du switch pour 802.1X, MAB

La configuration d'un port du switch (fa0/2) pour le contrôle d'accès réseau basé sur 802.1X. Le port est placé en mode accès et configuré pour exiger une authentification avant de permettre la communication.
Si le terminal ne prend pas en charge ce protocole, l'authentification se fait via MAB (MAC Authentication Bypass), en utilisant l'adresse MAC de l'appareil. Cela garantit un contrôle d'accès réseau même pour les équipements non compatibles 802.1X.

Figure 4.15 – Configuration du port pour 802.1X et MAB

Portail Captif

Cette configuration active les services HTTP (ip http server) et HTTPS (ip http secure-server) sur le switch. Elle est nécessaire pour permettre l'affichage du portail captif, utilisé pour l'authentification web des utilisateurs connectés au réseau.

Figure 4.16 – Activation du serveur HTTP/HTTPS

Création d'une ACL nommée PortailCaptif. Cette liste interdit l'accès à l'hôte 192.168.120.133, puis autorise les connexions TCP sur les ports 80 (HTTP) et 443 (HTTPS).

Enfin, une règle générale permet tout autre trafic. Cette ACL est utilisée pour rediriger les utilisateurs vers le portail captif tout en bloquant l'accès direct à certains services non autorisés.

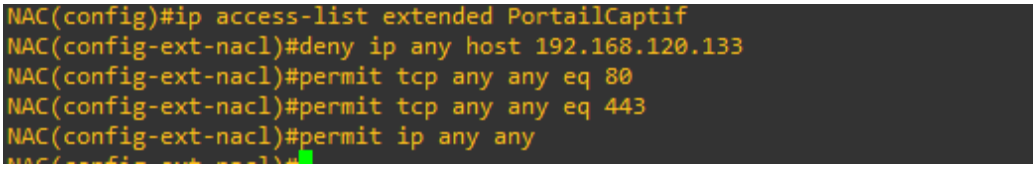


Figure 4.17 – ACL pour Portail Captif

4.3.2 Installation et intégration de PacketFence et Active Directory

Ce qui rend notre projet particulièrement intéressant, c'est qu'il repose sur une solution open source. L'avantage majeur d'un tel logiciel est sa compatibilité étendue avec divers types de matériels et de systèmes d'exploitation. PacketFence, par exemple, peut être déployé aussi bien sur Windows que sur plusieurs distributions Linux.

Dans notre cas, nous avons opté pour l'utilisation de l'image OVF de PacketFence, construite sur Debian, que nous avons directement installée sur notre serveur. Ce choix nous a permis d'éviter l'installation préalable d'un système d'exploitation, ce qui contribue à améliorer les performances de la solution. L'installation a été menée selon les recommandations détaillées dans la documentation officielle fournie par les développeurs de PacketFence.

Configuration initiale de PacketFence

Une fois PacketFence installé et le serveur correctement relié au réseau, nous accédons à son interface Web à l'aide d'un navigateur, en saisissant son adresse IP. La configuration initiale se déroule de manière guidée à travers plusieurs étapes, permettant de préparer le système à son intégration dans l'environnement réseau.

Etape 1 : Configuration de l'interface management.

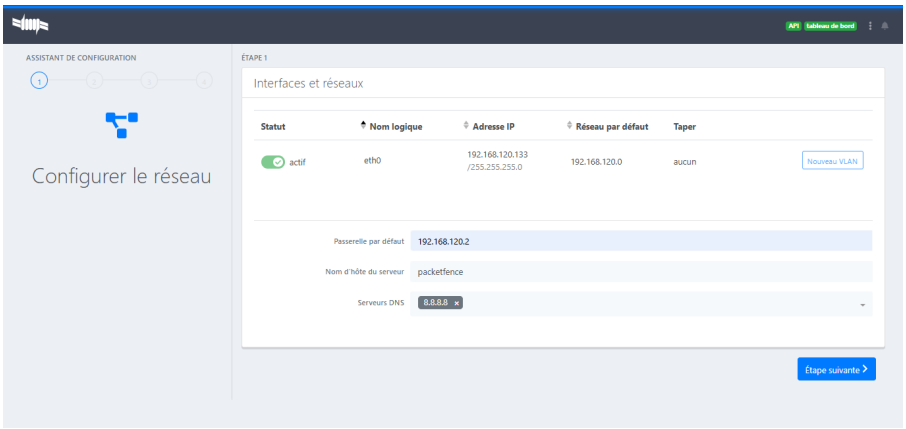


FIGURE 4.18 – Configuration de l'interface management

Etape 2 : Configuration de la base de données

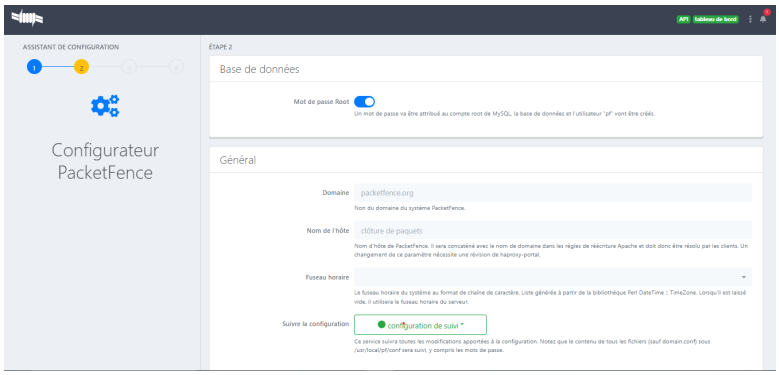


FIGURE 4.19 – Configuration de la base de données

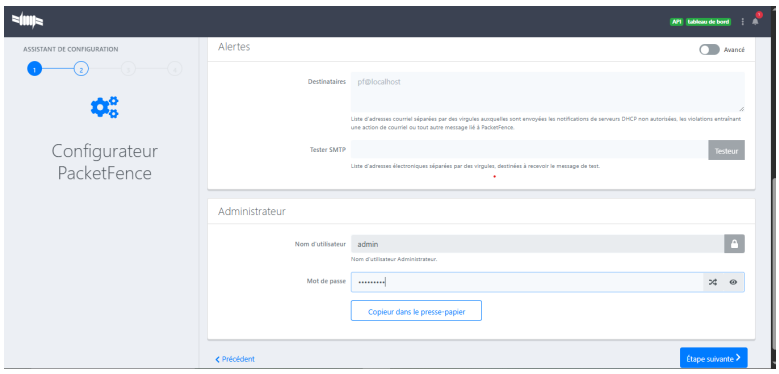


Figure 4.20 – Création du compte Admin

Etape 3 : Démmarer PacketFence

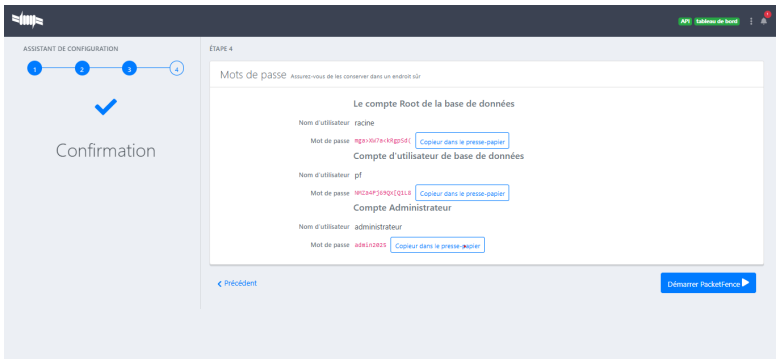


Figure 4.21 – Démmarer PacketFence

Installation du contrôleur de domaine (Active Directory)

L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Il sert à regrouper et organiser divers objets, tels que les utilisateurs, les postes de travail ou encore les imprimantes. Son rôle principal est de fournir une infrastructure centralisée pour gérer l'identification des ressources et l'authentification des utilisateurs au sein d'un système d'information [42].

Principales fonctionnalités d'Active Directory [43]

1. Gestion centralisée des identités : AD permet de créer, modifier et supprimer des comptes utilisateurs et ordinateurs, assurant une administration cohérente des identités au sein de l'organisation.
2. Authentification et autorisation : AD vérifie les identifiants des utilisateurs et détermine leurs droits d'accès aux ressources réseau.
3. Application de politiques de sécurité : Les administrateurs peuvent définir des stratégies de groupe pour appliquer des configurations spécifiques aux utilisateurs et ordinateurs, renforçant ainsi la sécurité et la conformité.
4. Organisation hiérarchique des ressources : AD structure les objets en unités organisationnelles (OU), domaines et forêts, facilitant la délégation des tâches administratives et la gestion des permissions.

5. Répartition et réplication des données : Les informations stockées dans AD sont réparties sur plusieurs contrôleurs de domaine, assurant la disponibilité et la résilience du service.

Pour centraliser l'authentification des utilisateurs dans notre infrastructure PacketFence, nous avons installé un contrôleur de domaine sous Windows Server 2012 dans une machine virtuelle. Le rôle Active Directory Domain Services (AD DS) a été ajouté pour mettre en place l'annuaire LDAP.

Configuration du serveur AD :
• Nom du serveur : DC
• Adresse IP : 192.168.120.200
• Masque réseau : 255.255.255.0
• Nom de domaine : Ad.test

Une unité d'organisation (OU) nommée "Utilisateurs" a été créée pour structurer les comptes. À l'intérieur, trois groupes ont été définis pour classifier les profils :
•Employes : personnel interne.
•Stagiaires : utilisateurs en formation.
•Invites : invités ou utilisateurs temporaires.

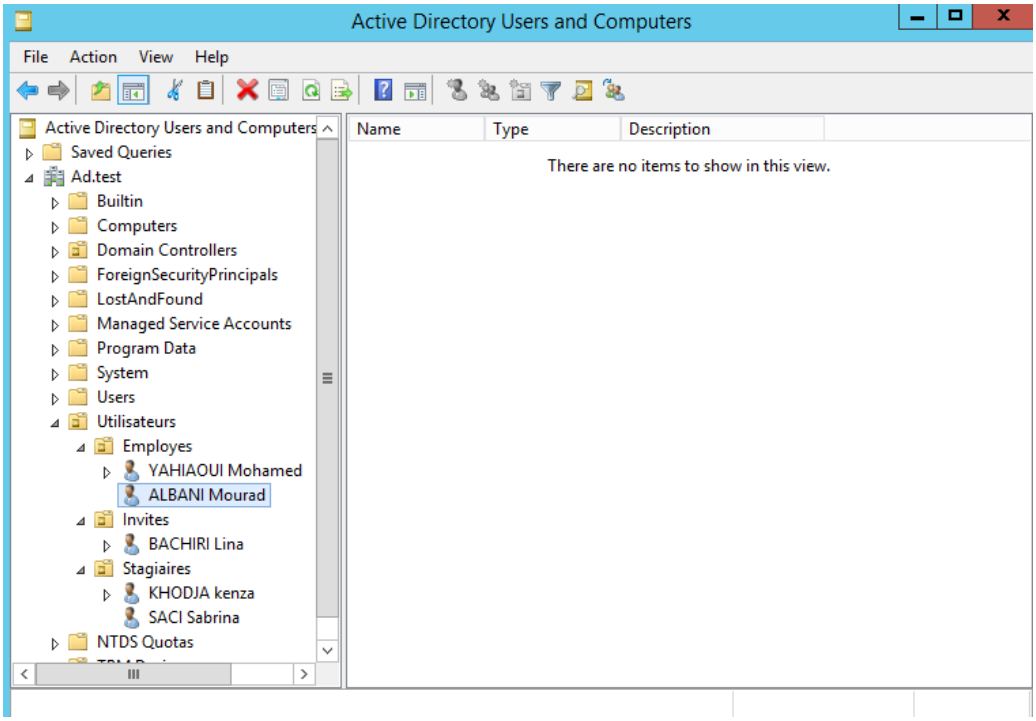


Figure 4.22 – Création des utilisateurs

Intégration de PacketFence et AD

Avant d'intégrer Active Directory comme source d'authentification dans PacketFence, il est essentiel d'accomplir une étape préalable cruciale, à savoir l'intégration de PacketFence au domaine Active Directory. Cette opération permet à PacketFence de communiquer avec le contrôleur de domaine, d'interroger l'annuaire LDAP, et de valider les identifiants des utilisateurs. Sans cette jonction, il serait impossible pour PacketFence de s'appuyer sur l'annuaire AD pour authentifier les connexions réseau.

Pour cela, il est nécessaire de configurer PacketFence en y renseignant le nom du domaine Active Directory ainsi que le nom d'hôte du serveur AD, comme indiqué ci-dessous :

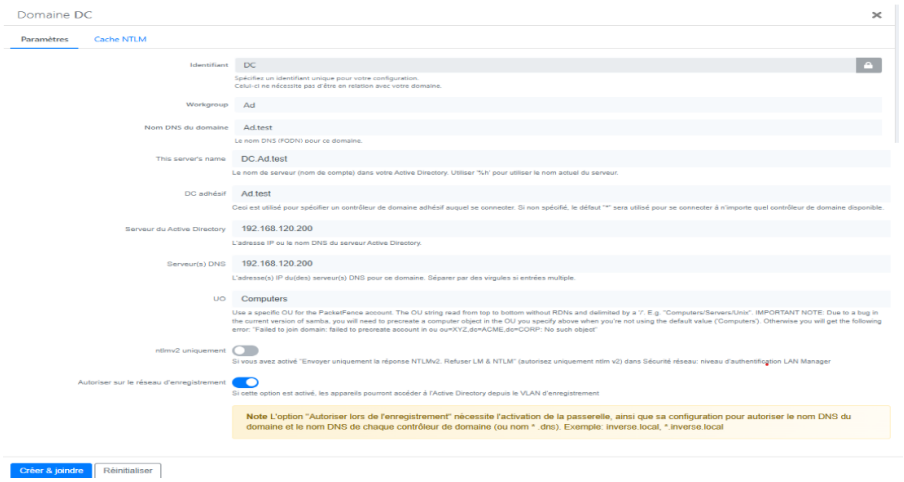


Figure 4.23 – Interface Création du domaine

Renseigner les identifiants du compte administrateur Active Directory (nom d'utilisateur et mot de passe) dans l'interface de gestion de PacketFence, afin d'autoriser ce dernier à joindre le domaine.

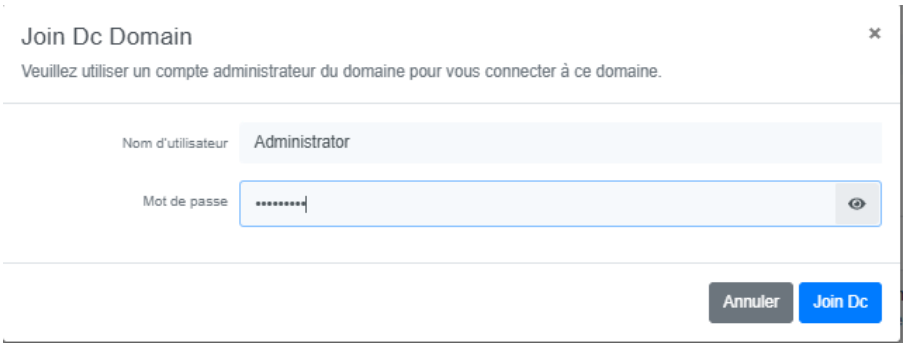


Figure 4.24 – Joindre un domaine

Lorsque PacketFence rejoint correctement le domaine Active Directory, l'interface affiche le résultat suivant :

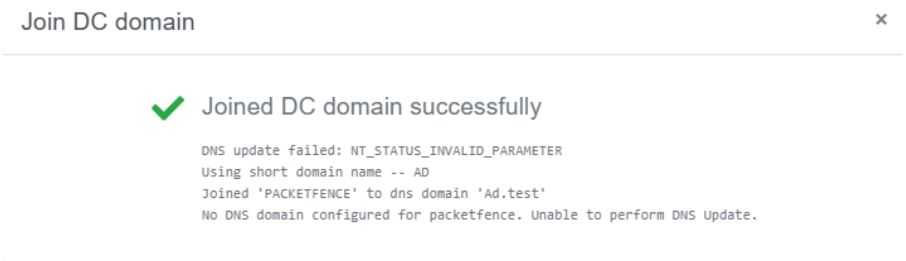


FIGURE 4.25 – Domaine joint avec succès

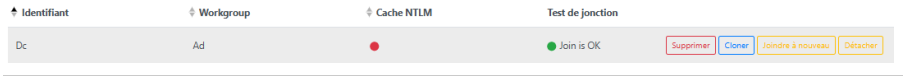


FIGURE 4.26 – Domaine joint avec succès

Pour finaliser l'intégration, le domaine est ajouté aux "REALMS". Cela permet à PacketFence de savoir comment traiter les authentifications en se basant sur le nom d'utilisateur.

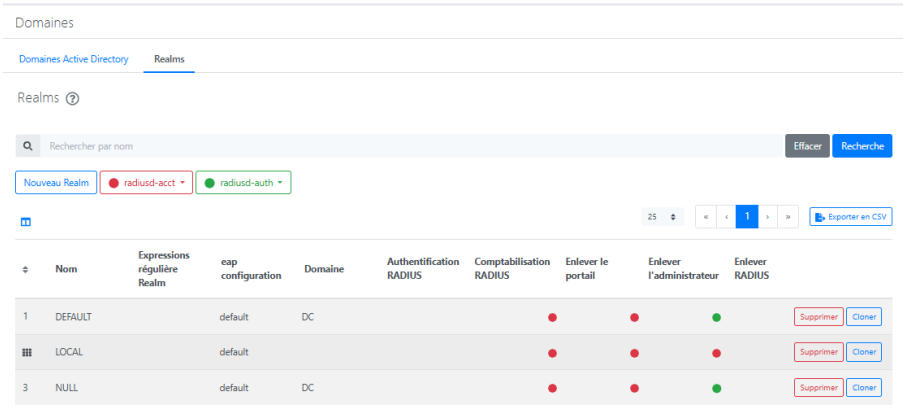


FIGURE 4.27 – Interface de l'onglet Realms

La création des rôles

PacketFence repose sur un système de rôles pour la gestion des autorisations des utilisateurs. Chaque rôle peut être associé à des droits d'accès spécifiques, permettant de contrôler l'utilisation des différentes fonctionnalités de la plateforme.

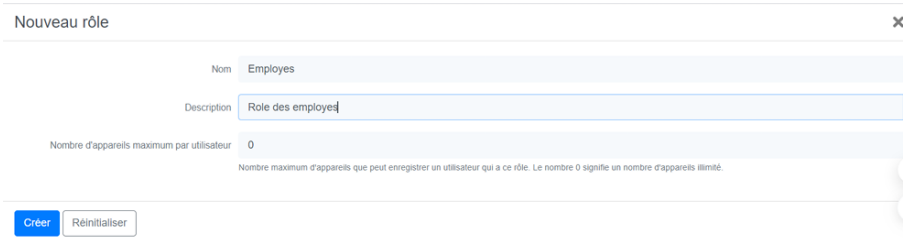


FIGURE 4.28 – Interface Création des rôles

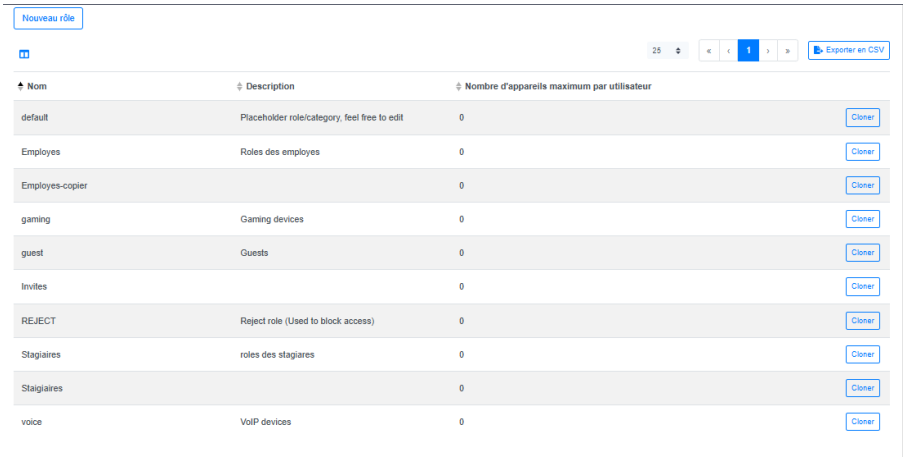


FIGURE 4.29 – Rôles crées

Configuration des périphériques réseau

Le commutateur réseau sera intégré à l'infrastructure PacketFence afin d'assurer la gestion des accès.
Un switch de type Cisco Catalyst 3560 sera ajouté avec l'adresse IP 192.168.120.2, en mode Production, pour permettre son interaction avec le serveur PacketFence dans un environnement opérationnel.

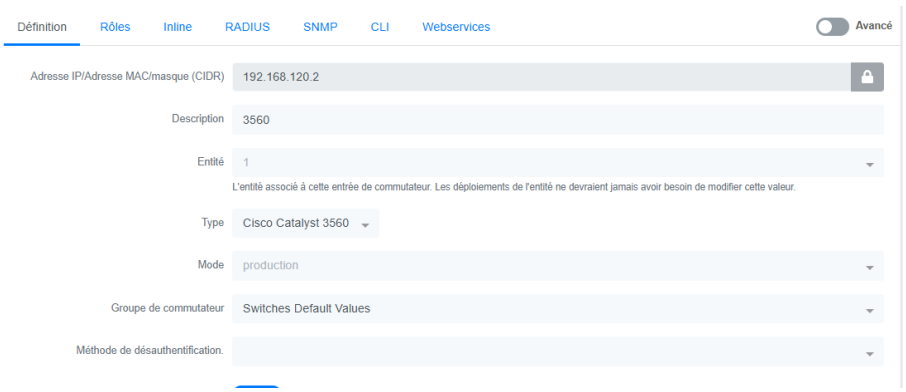


FIGURE 4.30 – Interface Ajout du switch

Dans l'onglet Rôles, les différents profils d'accès ont été définis, chacun étant associé à un VLAN spécifique. Par exemple, un périphérique non enregistré est automatiquement placé dans le VLAN par défaut (VLAN 2), ne bénéficiant d'aucun accès particulier. En revanche, une fois l'utilisateur authentifié avec des identifiants valides, son équipement est transféré vers le VLAN de DATA (VLAN 20). Ce VLAN est commun à tous les utilisateurs légitimes, qu'il s'agisse d'employés, de stagiaires ou d'invités.

Dans l'onglet RADIUS, la clé secrète utilisée a été renseignée de manière identique à celle configurée sur le commutateur Cisco Catalyst 3560 lors de la mise en place du protocole 802.1X. Cette clé partagée assure une communication sécurisée entre le switch et le serveur RADIUS intégré à PacketFence.

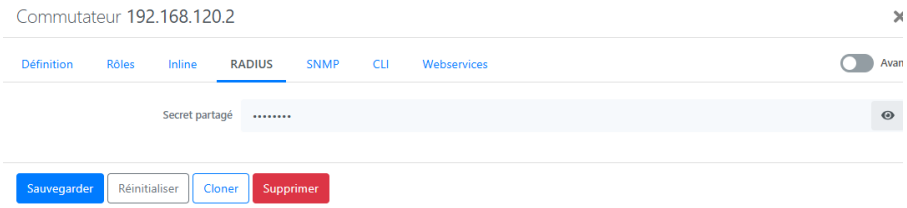


Figure 4.31 – Interface de l'onglet Radius

Enfin, dans l'onglet SNMP, les chaînes de communauté en lecture et en écriture ont été renseignées conformément à celles préalablement configurées sur le commutateur, afin de permettre la supervision et le contrôle à distance via le protocole SNMP.

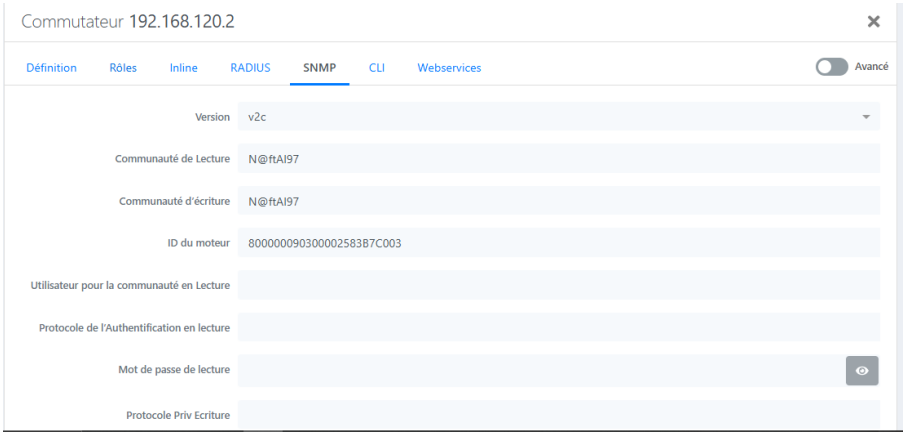


Figure 4.32 – Interface de l'onglet SNMP

4.3.3 Définition et politiques de la source d'authentification

Dans cette section, nous procédons à l'intégration de Microsoft Active Directory à PacketFence en tant que source d'authentification. Cette opération consiste à déclarer une nouvelle source interne de type AD (Active Directory), en y renseignant les champs requis et en définissant les règles d'accès au réseau qui correspondent à la politique de sécurité souhaitée.

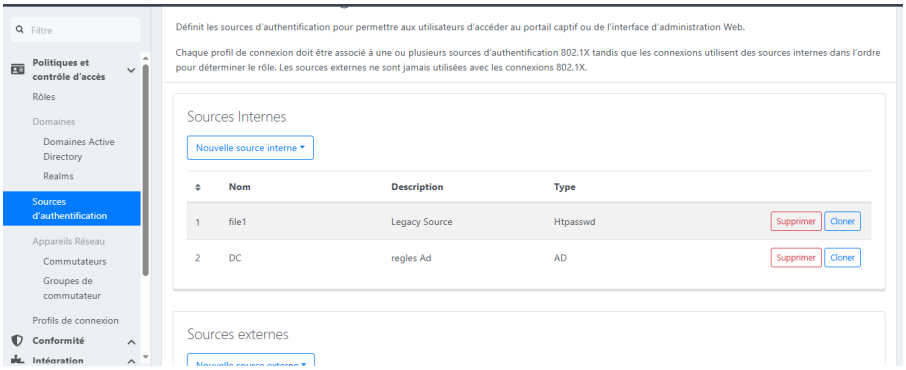
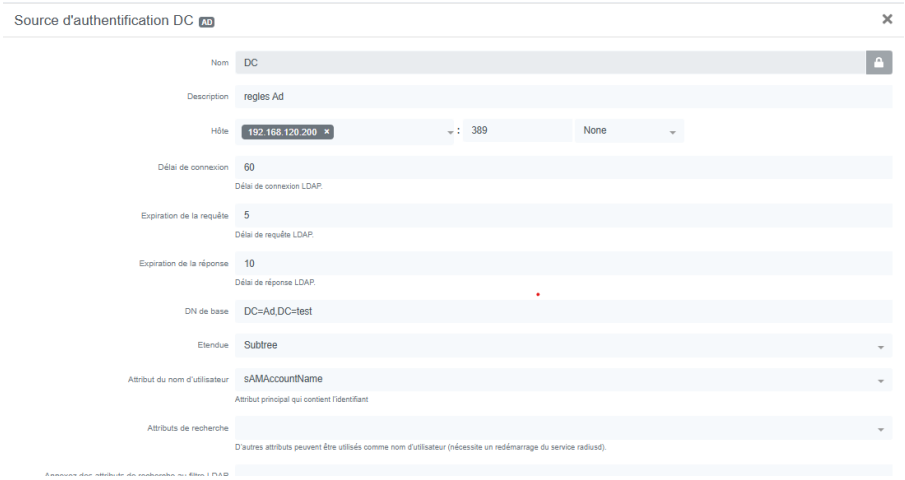


FIGURE 4.33 – Interface de l'onglet Sources d'authentification

•Nom : DC (ce nom correspond à celui attribué à notre serveur Active Directory).
•Description : regles Ad.
•Hôte : 192.168.120.200 (l'adresse IP du contrôleur de domaine Active Directory). La communication s'effectue par défaut via le port 389, utilisé par LDAP.
•Base DN : DC=Ad,DC=pf, il s'agit du chemin de base (Distinguished Name) pointant vers le haut de la hiérarchie LDAP, à partir duquel les recherches d'utilisateurs seront effectuées.
•Attribut de nom d'utilisateur : sAMAccountName (PacketFence utilisera cet attribut pour identifier les utilisateurs lors de l'authentification).
•Bind DN : CN=Administrator,CN=Users,DC=Ad,DC=test (chemin complet vers le compte d'administration Active Directory utilisé pour interroger l'annuaire).
•Mot de passe : @Dmin2025 (mot de passe du compte spécifié dans le Bind DN, nécessaire pour établir la connexion et effectuer les requêtes LDAP).



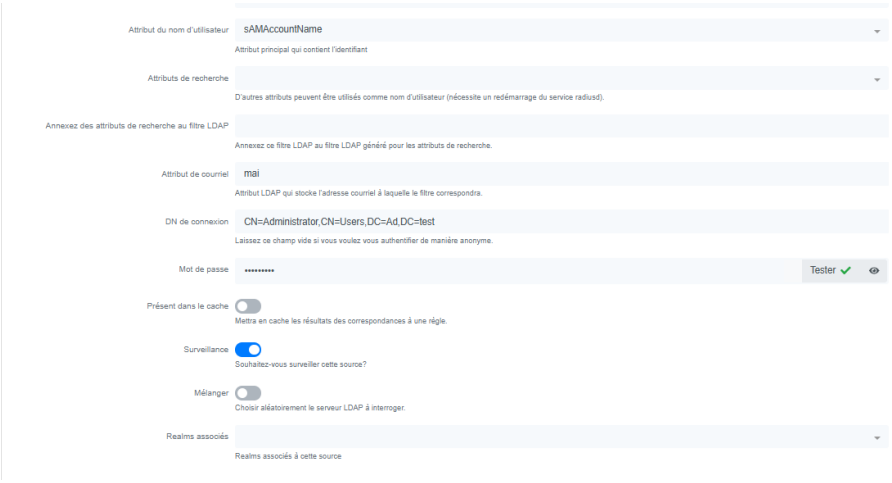


Figure 4.34 – Interface de la création d'une source d'authentification

À cette étape, il est nécessaire de définir des règles d'autorisation permettant d'assigner des rôles précis aux utilisateurs selon leur profil. Chaque catégorie d'utilisateur se verra attribuer un rôle spécifique ainsi qu'une durée d'accès adaptée. Pour cela, nous avons mis en place trois règles distinctes correspondant aux profils suivants : employé, stagiaire et invité.

Concernant la règle dédiée aux employés, nous avons défini comme critère d'appartenance que l'utilisateur doit se trouver dans le groupe LDAP suivant : OU=Employés,OU=Utilisateurs,DC=Ad,DC=test. Si cette condition est remplie, le système attribuera automatiquement le rôle Employe à l'utilisateur, avec une durée d'accès au réseau de 5 jours.

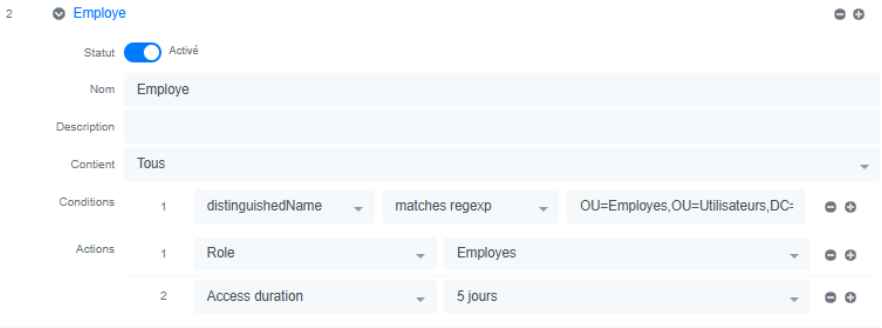


Figure 4.35 – Interface Création de la règle d'authentification Employe

Pour la règle correspondant aux stagiaires, la condition d'appartenance est définie comme suit : l'utilisateur doit être membre du groupe OU=Stagiaires,OU=Utilisateurs,DC=Ad,DC=test. Lorsque cette condition est remplie, le rôle Stagiaire lui est attribué, avec un accès réseau limité à 2 jours.

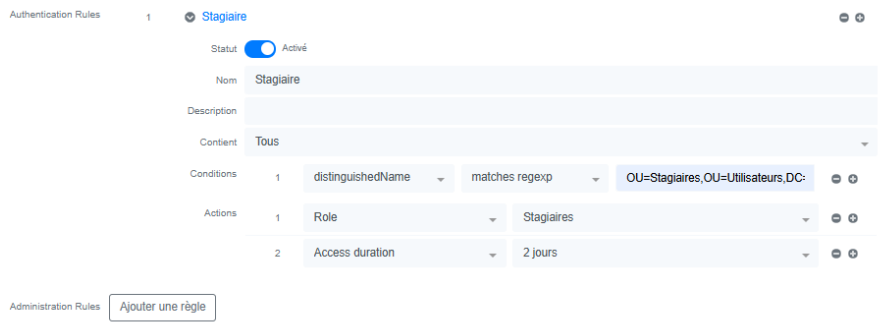


Figure 4.36 – Interface Création de la règle d'authentification Stagiaire

La règle appliquée aux invités repose sur la condition que l'utilisateur soit membre du groupe OU=Invites,OU=Utilisateurs,DC=Ad,DC=test. Si cette condition est respectée, le système lui attribue le rôle Guest, avec un accès au réseau limité à 12 heures.

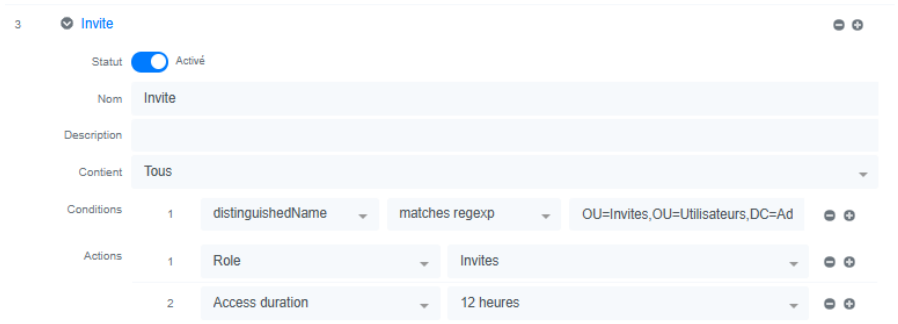


Figure 4.37 – Interface Création de la règle d'authentification Invité

Afin de valider le bon fonctionnement des règles d'authentification configurées, nous utilisons le script ./pftest authentication fourni par PacketFence. Ce test nous permet de simuler différents scénarios en modifiant les attributs des utilisateurs pour vérifier l'attribution correcte des rôles.

Dans le cas d'un employé :

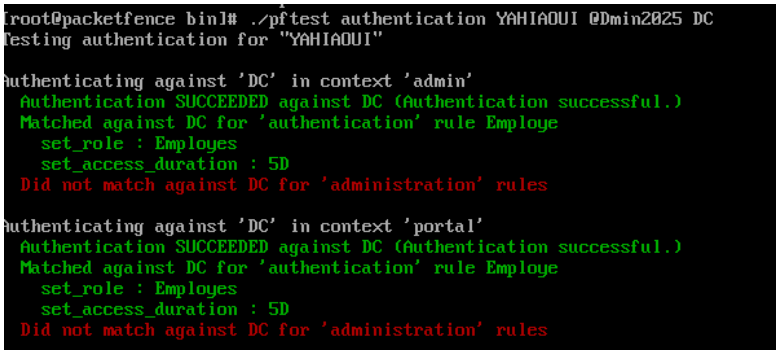


Figure 4.38 – Evaluation de la règle Employe

Dans le cas d'un stagiaire :

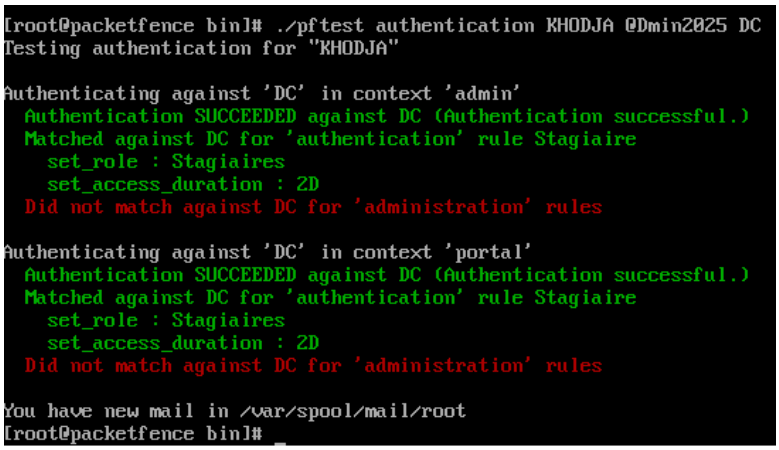


Figure 4.39 – Evaluation de la règle Stagiaire

Dans le cas d'un invité :

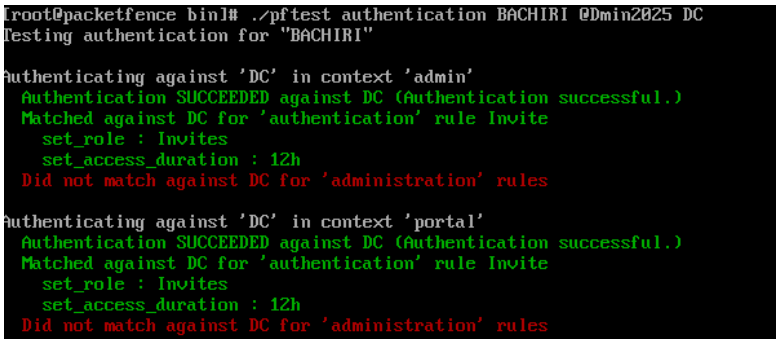


Figure 4.40 – Evaluation de la règle Invite

4.3.4 Définition du profil de connexion pour l'authentification 802.1X et MAC

Dans PacketFence, les profils de connexion permettent de gérer l'authentification de différents types de sessions en s'appuyant sur des protocoles standards tels que PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), PEAP (Protected Extensible Authentication Protocol) et EAP (Extensible Authentication Protocol).
Chaque profil définit les protocoles d'authentification autorisés en fonction des périphériques réseau à partir desquels l'utilisateur tente de se connecter. Il précise également les sources d'identité (comme un annuaire LDAP ou une base de données) qui seront utilisées pour valider les identifiants de l'utilisateur.
Ces profils s'appuient sur un système de règles basées sur des attributs (adresse IP, VLAN, rôle, etc.) afin de sélectionner dynamiquement le protocole et la source d'identité appropriés pour chaque demande d'authentification.

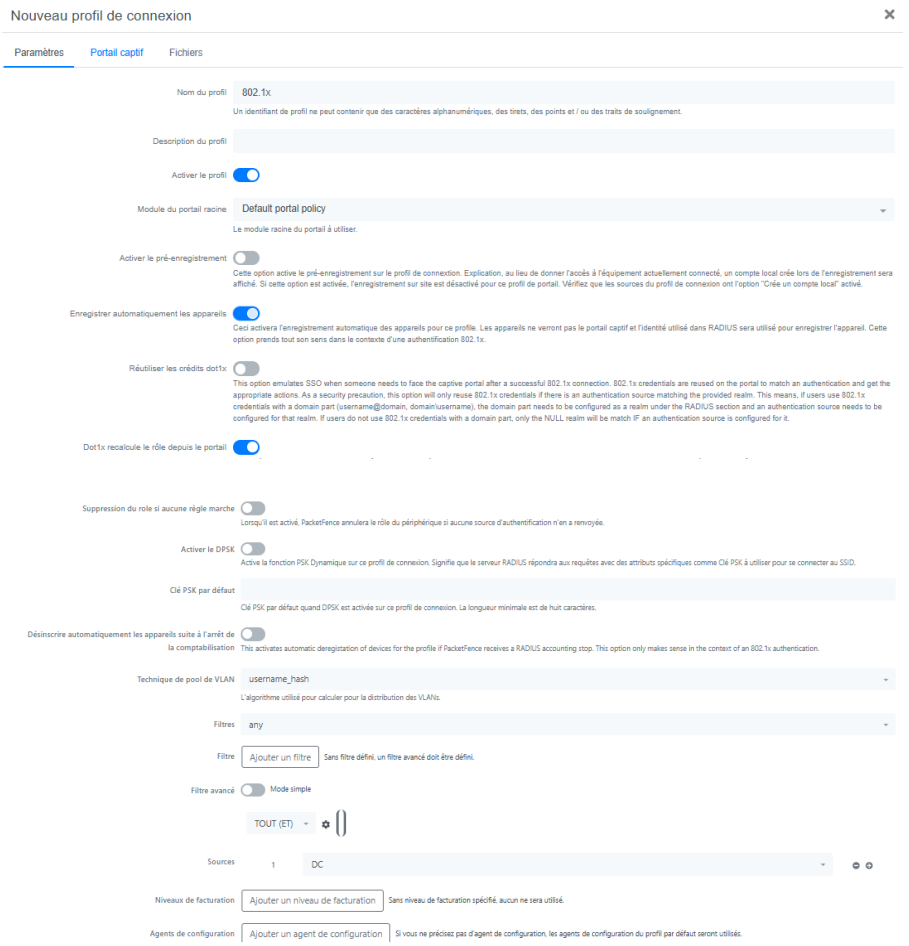


FIGURE 4.41 – Création d'un profil de connexion

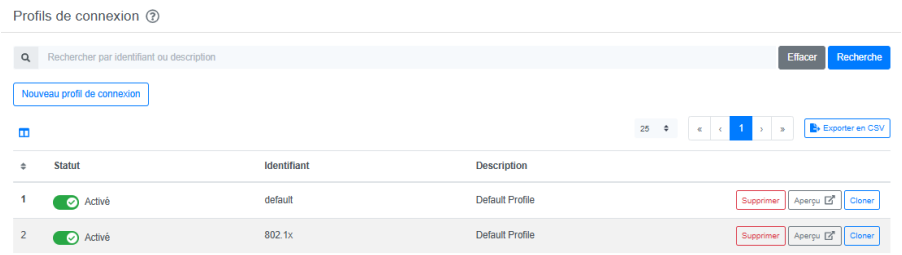


FIGURE 4.42 – Interface des profils crées

4.3.5 Définition du profil de connexion pour l'authentification avec un portail captif

Un portail captif est une méthode de contrôle d'accès au réseau qui oblige les utilisateurs à passer par une page web spéciale (le "portail captif") avant de pouvoir accéder à Internet ou à d'autres ressources réseau. Cette page web peut être utilisée pour authentifier les utilisateurs, collecter des informations, présenter des conditions d'utilisation ou fournir des instructions. Les utilisateurs sont redirigés vers cette page lors de leur tentative d'accès à Internet, et ils doivent suivre les étapes nécessaires (telles que la saisie de leurs identifiants ou l'acceptation des termes et conditions) pour être autorisés à naviguer sur le réseau. Dans PacketFence, il existe deux manières principales d'afficher ce portail captif pour les appareils inconnus ou non enregistrés :

— Authentification Web (Hotspot) : Cette méthode est prise en charge par de nombreux fournisseurs d'équipements et redirige les utilisateurs vers la page de connexion du portail captif lorsqu'ils tentent d'accéder à Internet.

— VLAN d'enregistrement : PacketFence utilise des services DHCP et de black-holing DNS pour isoler les appareils dans un VLAN spécifique jusqu'à ce qu'ils soient authentifiés. Cette méthode est compatible avec tous les équipementiers prenant en charge l'attribution dynamique de VLAN via RADIUS.

Pour notre exemple, nous utiliserons l'authentification Web.

Depuis l'onglet « Rôles », nous vérifions que dans la section « Role by VLAN ID », les VLANs d'enregistrement et des invités sont bien configurés avec l'ID VLAN 2. Cela permet de s'assurer que tous les clients non enregistrés sont automatiquement placés dans le VLAN 2 dès leur connexion, et qu'aucun changement de VLAN ne se produit une fois qu'ils s'authentifient correctement via le portail captif.

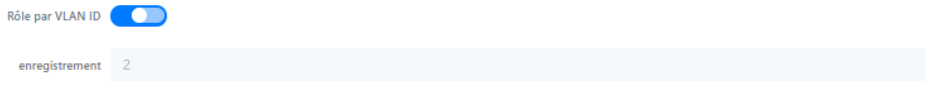


Figure 4.43 – Role by Vlan ID

Nous nous assurons que l'option « Role by Switch Role » est activée, puis nous définissons le rôle d'enregistrement sur « enregistrement ». Cette configuration garantit que la liste d'accès définie pour l'enregistrement est appliquée aux utilisateurs non enregistrés, limitant ainsi leur accès exclusivement au portail captif de PacketFence.

Figure 4.44 – Role by Switch Role

Nous nous assurons que l'option « Role by Web Auth URL » est activée, puis nous définissons l'URL d'enregistrement sur http ://192.168.120.133/catalyst : :3560. Cette configuration permet d'associer automatiquement un rôle en fonction de l'URL d'authentification web utilisée par le switch.

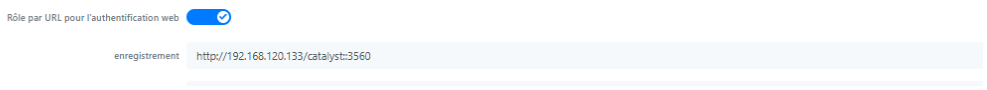


Figure 4.45 – Role by Web Auth URL

Pour l'authentification Web, un nouveau profil de connexion sera créé dans PacketFence. Ainsi, le profil de connexion par défaut continuera à être utilisé pour l'authentification 802.1X, tandis que le nouveau profil sera dédié à l'authentification Web. Ce dernier permettra d'afficher un portail captif basé sur notre source d'authentification nommée « DC ».

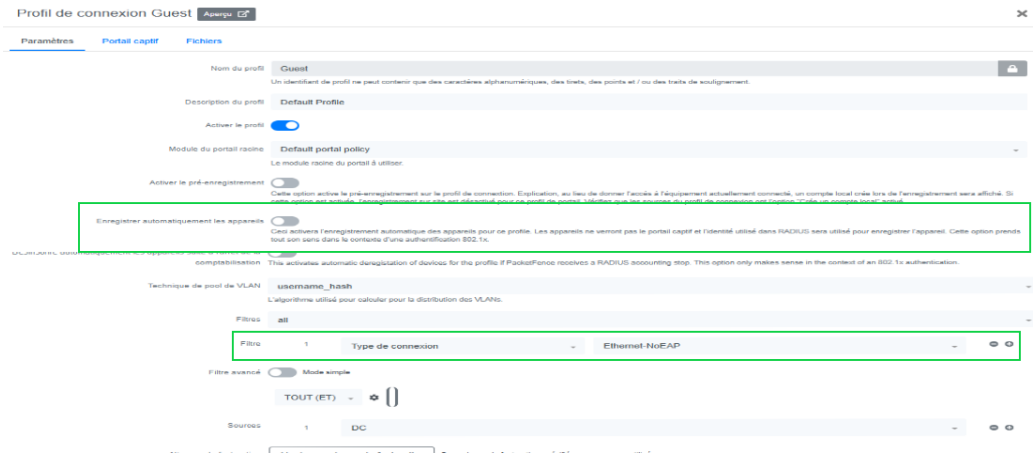


Figure 4.46 – Profil de connexion Guest

4.4 Tests et validation

4.4.1 Test de l'authentification

Le service dot3svc, dit aussi «Wired AutoConfig», qui fait partie du système Windows permet dans les interfaces réseau Ethernet d'activer l'authentification 802.1X. Le bon fonctionnement de ce service permet à l'ordinateur client de négocier automatiquement une connexion sécurisée avec l'infrastructure réseau, ce qui est particulièrement utile dans les environnements NAC (Network Access Control) comme PacketFence. L'utilisation de ce service est indispensable pour les scénarios où l'authentification réseau repose sur :

- 802.1X, pour un accès réseau sécurisé.
- EAP -MSCHAPv2 ou PEAP, comme méthode d'authentification· Un serveur RADIUS.

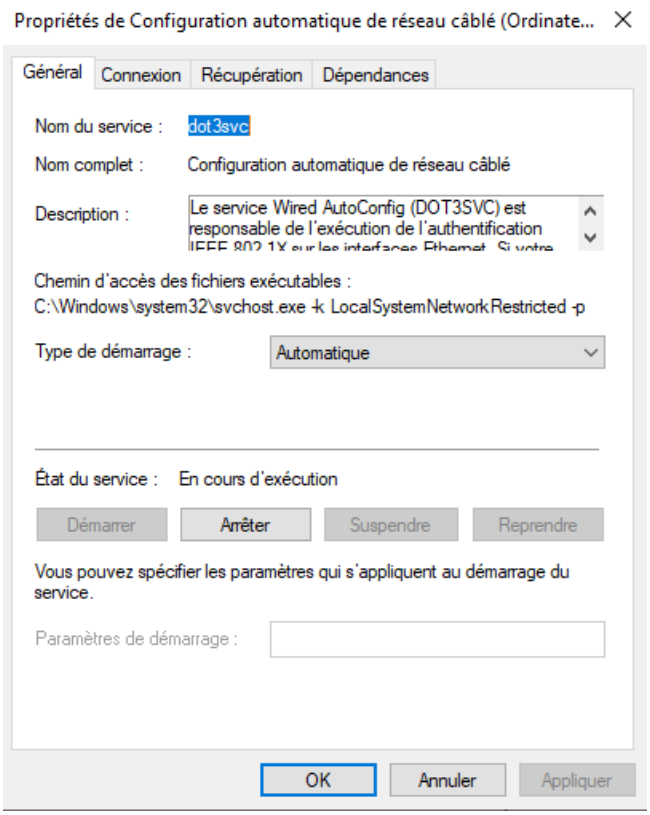


Figure 4.47 – Interface Configuration automatique de réseau câblé

Dans les Propriétés de la carte réseau Ethernet, sur l'onglet Réseau, nous activons le protocole d'authentification 802.1X. Puis nous vérifions que « Mot de passe sécurisé (EAP MSCHAPv2) » est sélectionné dans les paramètres du protocole EAP et que « Valider le certificat du serveur » est désélectionné. Puis, nous cliquons sur Configurer et vérifions que la case à côté de « Utiliser automatiquement mon nom de connexion et mon mot de passe Windows (et le domaine approprié) » est désélectionnée. Puis validons ces opérations.

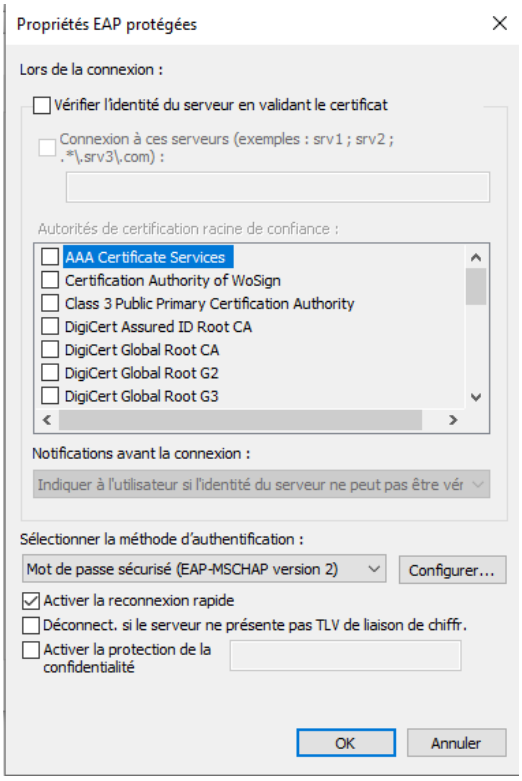


Figure 4.48 – Interface propriétés ethernet

Dès que le câble de réseau est connecté sur l'interface Ethernet de la machine, le système affiche directement une fenêtre d'authentification d'identification de l'utilisateur (nom d'utilisateur et mot de passe).

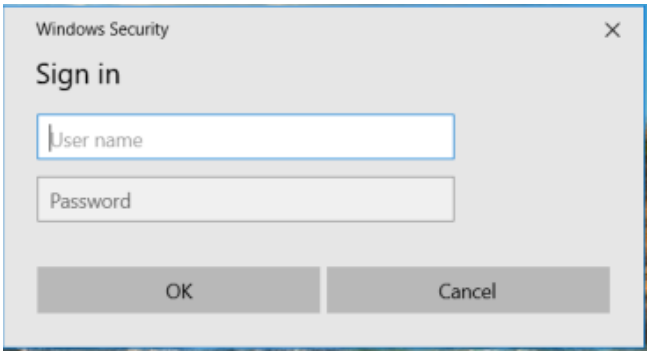


Figure 4.49 – Interface de connexion

Après avoir saisi les identifiants corrects de l'utilisateur, le statut du réseau passe à "Connecté", et l'on constate dans les propriétés que l'adresse IP du VLAN 20 est attribuée automatiquement à la machine.

Figure 4.50 – Interface Propriétés du réseau

4.4.2 Contrôle et surveillance de l'infrastructure réseau

Dans une configuration de solution de contrôle d'accès au réseau qui lui est propre, l'audit correspond au processus d'examen et d'enregistrement systématiques, c'est-à-dire préétablis et programmés, des événements survenant dans le cadre des accès au réseau ou de l'authentification. L'audit est au cœur du processus de suivi, d'analyse et de restauration (ou de mémorisation) des comportements et activités des utilisateurs (et de leurs appareils respectifs, ainsi que des applications utilisées) au sein d'un environnement réseau.

Dans notre cas, on voit dans le journal d'audit de PacketFence que le profil de connexion « 802.1X » est appliqué à l'utilisateur avec lequel on vient de se connecter (Stgrkenza). On remarque que le statut d'authentification est "Accepté", le statut de l'appareil est "Enregistré", le nom d'utilisateur est affiché avec la date et l'heure de la jonction au réseau.

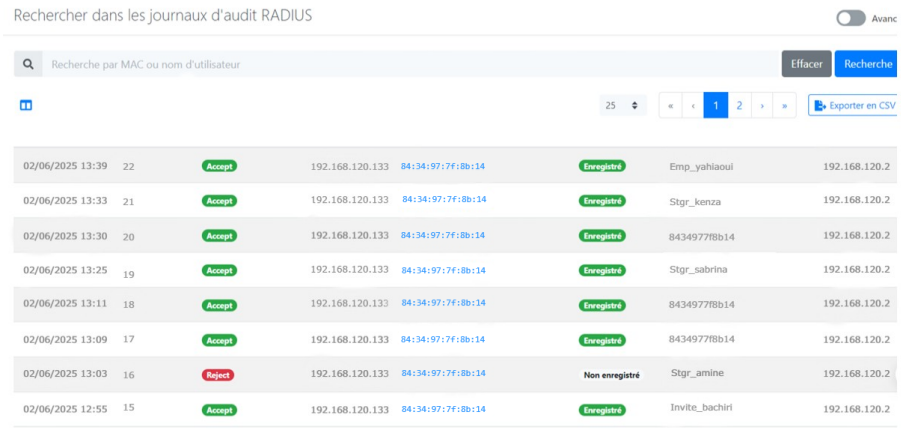


Figure 4.51 – Journal d'audit

Après le processus d'authentification, le nouveau nœud obtient l'accès au réseau local (VLAN 20), dont le réseau par défaut est 192.168.20.0/24. Il est ensuite automatiquement ajouté à la base de données des nœuds locaux de PacketFence avec le statut "enregistré". Un rôle d'utilisateur lui est attribué en fonction des informations d'identification fournies ; dans

notre exemple, le rôle attribué est "Stagiaires".

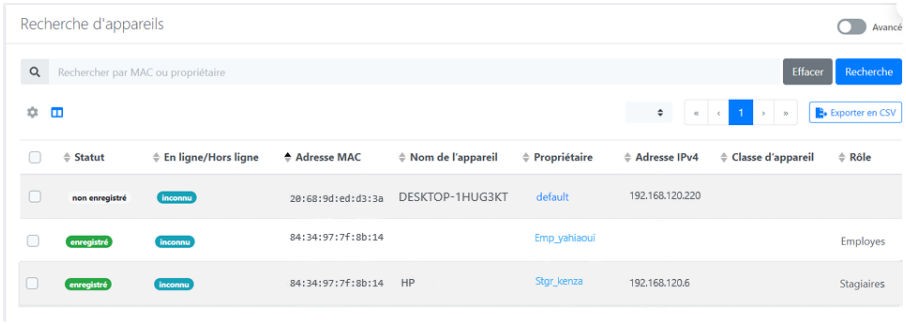


Figure 4.52 – Rôle attribué

Cette fenêtre permet de vérifier à tout moment les appareils connectés au réseau ainsi que les détails relatifs à chaque connexion.

En cliquant sur l'adresse MAC d'un appareil, une nouvelle fenêtre s'ouvre affichant des informations détaillées le concernant.

Figure 4.53 – Interface de modification des informations

Il est possible de visualiser l'ensemble de l'infrastructure réseau dans l'onglet « Réseau », qui fournit des informations détaillées sur tous les périphériques, qu'ils soient enregistrés ou non.

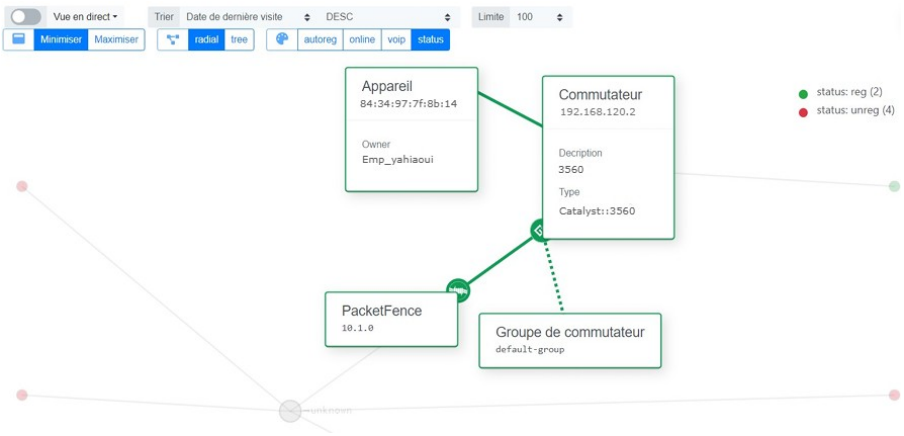


Figure 4.54 – Visualisation du réseau

4.4.3 Rapports

Dans PacketFence, un onglet dédié permet de visualiser diverses statistiques, telles que le nombre d'appareils enregistrés par rôle, facilitant ainsi le suivi et l'analyse de l'utilisation du réseau.

Figure 4.55 – Rapport sur le nombre d'appareils enregistrés par rôle

Les requêtes radius :

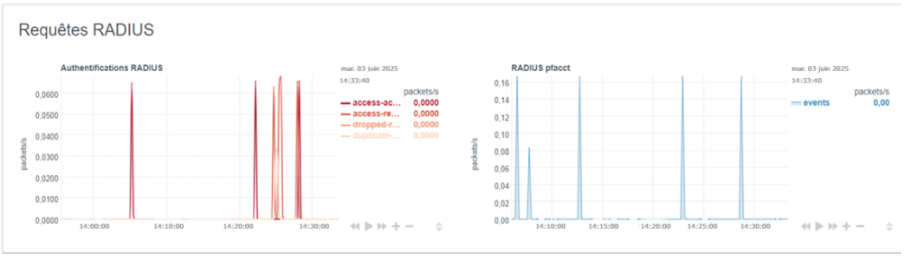


Figure 4.56 – Rapport des requêtes radius

Authentifications radius réussies et celles échouées :

Figure 4.57 – Rapport des authentifications radius réussies et celles échouées

Appareils enregistrés par tranche de temps :

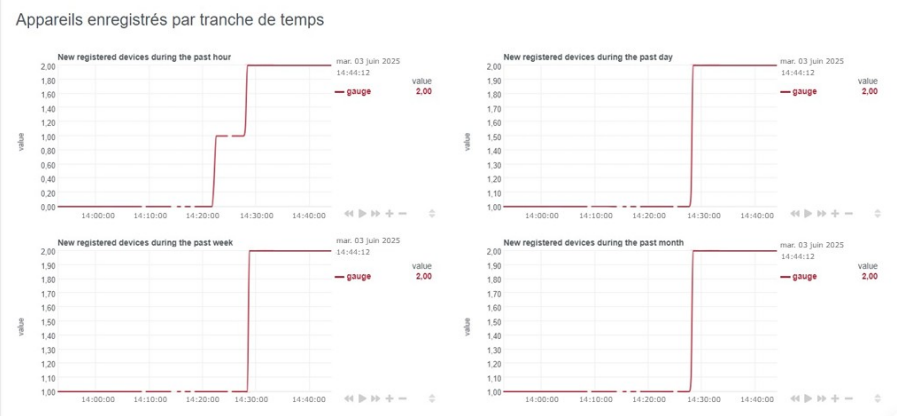


Figure 4.58 – Rapport des appareils enregistrés par tranche de temps

4.5 Conclusion

La mise en place de PacketFence avec un switch Cisco Catalyst 3560 nous a permis de comprendre et de maîtriser le fonctionnement d'un système NAC. L'authentification des utilisateurs via 802.1X et MAB, la configuration du switch, la gestion des VLANs et l'interfaçage avec un serveur RADIUS ont constitué les principaux axes techniques de cette expérimentation. Malgré certaines contraintes rencontrées (notamment liées à la connectivité ou à la configuration de la VM), le déploiement s'est avéré concluant, renforçant ainsi notre expérience dans la sécurisation d'accès réseau.

Conclusion générale

Ce mémoire est consacrée au travail accompli dans le cadre du projet de fin d'études, visant l'étude puis l'implémentation d'une solution de contrôle d'accès réseau (NAC) au sein de l'infrastructure de Naftal. Avec pour objectif de sécuriser le réseau via une solution libre, fiable et adaptable : PacketFence. Ce projet a été formatif tant dans le cadre technique que méthodologique.

À travers une démarche méthodologique stricte, nous avons pu concevoir et mettre en œuvre ladite solution dans un environnement d'application réel en adéquation avec les besoins de l'entreprise Naftal. Les différents tests effectués ont montré que PacketFence offre la possibilité d'un contrôle d'accès centrale, une traçabilité des connexions, et une adaptabilité à l'ensemble des politiques de sécurité.

La solution a fait l'objet d'évaluations dans un cadre isolé, qui nous ont permis d'évaluer sa réelle efficacité dans l'accès et la protection du système d'information, sur lequel nous avons suivi une démarche au cours de l'ensemble du projet, structurée dans notre présentation en quatre chapitres.

Les résultats obtenus ont mis en évidence la capacité de PacketFence à contrôler efficacement les accès via plusieurs méthodes d'authentification (802.1X, MAB, portail captif), tout en s'intégrant avec des composants existants comme l'annuaire Active Directory.

Pour conclure, cette aventure a solidifié nos aptitudes compétences en protection des réseaux, mais a aussi mis en lumière combien une démarche rigoureuse est essentielle pour bâtir des systèmes informatiques mieux protégés. Des pistes d'amélioration, comme rendre automatique la gestion des alertes ou élargir le champ d'action du dispositif, pourraient davantage enrichir ce projet dans un contexte professionnel.

Bibliographie

[1] WEODEO, Réseau informatique : comment ça marche ? [En ligne]. Disponible sur : https://www.weodeo.com/digitalisation/reseau-informatique-comment-ca-marche (consulté le [14/02/2025]).

[2] CAMÉRÉCOLE, Configuration d'un réseau informatique . [En ligne]. Disponible sur : https://www.camerecole.org/classes/1441-configuration-d-un-reseau-informatique.html (consulté le [14/02/2025]).

[3] IONOS, Personal Area Network (PAN). [En ligne]. Disponible sur : https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-ae/#c73796 (consulté le [14/02/2025]).

[4] IT-CONNECT : https ://www.it-connect.fr/les-types-de-reseaux-lan-man-wan-et-pan-pour-les-debutants/ (consulté le [14/02/2025]).

[5] IONOS, "Local Area Network (LAN)". [En ligne]. Disponible sur : https://www.ionos.fr/digitalguide/serveur/know-how/les-types-de-reseaux-informatiques-a-connaitre/#c73796 (consulté le [14/02/2025]).

[6] IT-CONNECT : https ://www.it-connect.fr/les-types-de-reseaux- lan-man-wan-et-pan-pour-les-debutants/ (consulté le [14/02/2025]).

[7] IT-CONNECT, " C'est quoi un réseau MAN ? ". [En ligne]. Disponible sur : https://www.it-connect.fr/les-types-de-reseaux-lan-man-wan-et-pan-pour-les-debutants#google_vignette (consulté le [14/02/2025]).

[8] IT-CONNECT, C'est quoi un réseau MAN ? ". [En ligne]. Disponible sur : https://www.it-connect.fr/les-types-de-reseaux-lan-man-wan-et-pan-pour-les-debutants/ (consulté le [14/02/2025]).

[9] IT-CONNECT, "C'est quoi un réseau WAN ?". [En ligne]. Disponible sur : https://www.it-connect.fr/les-types-de-reseaux-lan-man-wan-et-pan-pour-les-debutants#google_vignette (consulté le [14/02/2025]).

[10] IT-CONNECT : https ://www.it-connect.fr/les-types-de-reseaux-lan-man-wan-et-pan-pour-les-debutants/ (consulté le [14/02/2025]).

[11] ManageEengine , "Le modèle OSI : comment fonctionnent les protocoles réseau". [En ligne]. Disponible sur : https://www.manageengine.com/fr/network-monitoring/network-protocols.html (consulté le [14/02/2025]).

[12] OpenClassrooms :Modèle OSI https://openclassrooms.com/fr/courses/6944606-concevez-votre-reseau-tcp-ip/7236472-prenez-du-recul-sur-votre-pratique-grace-au-modele-osi (consulté le [16/02/2025]).

[13] CrowdStrike, "Définition de la sécurité informatique", Disponible sur : https://www.crowdstrike.fr/cybersecurity-101/it-security/ (consulté le [17/02/2025]).

[14] SecuriteInfo, Objectifs de la sécurité informatique. [En ligne]. Disponible sur : https://www.securiteinfo.com/conseils-cybersecurite/les-5-principes-fondamentaux-cybersecurite-dican.shtml (consulté le [17/02/2025]).

[15] SecuriteInfo, Objectifs de la sécurité informatique. [En ligne]. Disponible sur : https://fr.scribd.com/document/730927347/principes-fondamantaux-securite-informatique-et-protection-des-donnees-Copie-2 (consulté le [17/02/2025]).

[16] Netwrix, "Les 10 types de cyberattaques les plus courants", Disponible sur : https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/ (consulté le [17/02/2025]).

[17] Guardia, "Les différents types de cyberattaques", Disponsible sur : https://guardia.school/boite-a-outils/panorama-des-attaques-cyber.html (consulté le [18/02/2025])

[18] Cisco, Types de sécurité des réseaux. [En ligne]. Disponible sur : https://www.cisco.com/c/fr_ca/products/security/what-is-network-security.html (consulté le [18/02/2025]).

[19] LinkedIn, Solutions et Technologies de Sécurisation. Disponible sur : https://www.linkedin.com/pulse/strat%C3%A9gie-de-s%C3%A9curit%C3%A9-informatique-en-entreprise-comment-prot%C3%A9ger (consulté le [20/02/2025]).

[20] Serma-Safety-Security, "Qu'est-ce que le Contrôle d'Accès Réseau (NAC) ?".Disponible sur : https://www.serma-safety-security.com/controle-dacces-reseau-nac-securisez-vos-infrastructures-avec-cisco-ise/ (consulté le [01/03/2025]).

[21] Cyberinstitut.fr, Comment fonctionne le NAC ?. [En ligne]. Disponible sur : https://cyberinstitut.fr/securiser-acces-reseau-nac-network-access-control/ (consulté le [01/03/2025]).

[22] MotaData, Composants du contrôle d'accès au réseau. [En ligne]. Disponible sur : https://www.motadata.com/it-glossary/network-access-control/ (consulté le [01/03/2025]).

[23] IBM, Network Access Control. [En ligne]. Disponible sur : https://www.ibm.com/docs/en/aix/7.2?topic=security-network-access-control (consulté le [05/03/2025]).

[24] Juniper Networks,Qu'est-ce que le contrôle d'accès réseau (NAC) 802.1X ?.Disponible sur :https ://www.juniper.net/fr/fr/research-topics/what-is-802-1x-network-access-control.html(consulté le [05/03/2025]).

[25] IONOS. IEEE 802.1X,"Quels sont les prérequis pour IEEE 802.1X ?".Disponible sur : https://www.ionos.fr/digitalguide/serveur/know-how/ieee-8021x/ (consulté le [05/03/2025]).

[26] phoenixNAP,"Qu'est-ce que le protocole d'authentification extensible (EAP) ?".Disponible sur : https://phoenixnap.fr/glossaire/protocole-d%27authentification-extensible-eap (consulté le [05/03/2025]).

[27] Huawei Enterprise Support Community. Le protocole d'authentification EAP. Disponible sur https://forum.huawei.com/enterprise/intl/fr/thread/Le-protocole-d-authentification-EAP/667502537487564800?blogId=667502537487564800(consulté le [06/03/2025]).

[28] Lafaye, Le protocole RADIUS.Disponible sur https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/radius.htm(consulté le [06/03/2025]).

[29] Cisco, NAC Authentication Failure Operation. [En ligne]. Disponible sur : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_nac/configuration/15-mt/sec-usr-nac-15-mt-book/sec-nat-auth-fail-op.html (consulté le [10/03/2025]).

[30] Microsoft, Network Access Protection (NAP) – Start Page. [En ligne]. Disponible sur : https://learn.microsoft.com/fr-fr/windows/win32/nap/network-access-protection-start-page (consulté le [10/03/2025]).

[31] Juniper, Mist NAC Overview. [En ligne]. Disponible sur : https://www.juniper.net/documentation/fr/fr/software/mist/mist-access/topics/concept/mist-nac-overview.html (consulté le [10/03/2025]).

[32] OpenNAC,https://sourceforge.net/projects/opennac/ (consulté le [10/03/2025]).

[33] CentOS Wiki, Présentation de OpenNAC à l'événement Dojo Madrid 2013. [En ligne]. Disponible sur : https://wiki.centos.org/attachments/Events(2f)Dojo(2f)Madrid2013/overview_opennac_org_eng_v9.pdf (consulté le [11/03/2025]).

[34] PacketFence, Solutions libres. [En ligne]. Disponible sur : https://www.packetfence.org/about.html#/overview (consulté le [11/03/2025]).

[35] FreeNAC, Page du projet sur OpenHub. [En ligne]. Disponible sur : https://openhub.net/p/8572 (consulté le [11/03/2025]).

[36] Sanjay Seth, Which Open Source NAC is Good ?. [En ligne]. Disponible sur : https://sanjayseth.com/which-open-source-nac-is-good/ (consulté le [15/03/2025]).

[37] ResearchGate, A Review of Opensource Network Access Control (NAC) Tools for Enterprise Educational Networks. [En ligne]. Disponible sur : https://www.researchgate.net/publication/277012927_A_Review_of_Opensource_Network_Access_Control_NAC_Tools_for_Enterprise_Educational_Networks (consulté le [15/03/2025]).

[38] Ministère de l'Énergie (Algérie), Document officiel - Naftal. [En ligne]. Disponible sur : https://www.energy.gov.dz/Media/galerie/naftal_5fe30cd256ffd.pdf (consulté le [06/04/2025]).

[39] Emmanuel Bama, PacketFence : la sécurité réseau open source sans prise de tête. [En ligne]. Disponible sur : https://emmanuelbama.net/2024/02/06/packetfence-la-securite-reseau-open-source-sans-prise-de-tete/ (consulté le [06/04/2025]).

[40] PacketFence, Présentation officielle. [En ligne]. Disponible sur https://www.packetfence.org/about.html (consulté le [07/04/2025]).

[41] Cyber University, Qu'est-ce que Snort ?. [En ligne]. Disponible sur : https://www.cyberuniversity.com/post/snort-definition-fonctionnement-avantages (consulté le [07/04/2025]).

[42] IT-Connect, Notions de base de l'Active Directory. [En ligne]. Disponible sur : https://www.it-connect.fr/cours/notions-de-base-de-lactive-directory/ (consulté le [10/05/2025]).

[43] Quest, What is Active Directory ?. [En ligne]. Disponible sur : https://www.quest.com/fr-fr/solutions/active-directory/what-is-active-directory.aspx (consulté le [10/05/2025]).

Résumé

Dans une situation où le domaine de la sécurité des réseaux reste une préoccupation majeure pour toute entreprise, ce mémoire présente les travaux d'analyse, de conception et de réalisation d'une solution open source de contrôle d'accès réseau.

Ce mémoire traite de la mise en place d'une solution open source de contrôle d'accès réseau (NAC) au sein du district GPL de Naftal à Béjaïa, pour sécuriser l'accès aux ressources réseau. Après une analyse des concepts de sécurité et des solutions NAC existantes, PacketFence a été choisie pour ses fonctionnalités, sa compatibilité et son caractère libre.

La partie pratique comprend la configuration d'un switch Cisco, son intégration avec Active Directory et la mise en place de méthodes d'authentification comme 802.1X, MAB et le portail captif, suivies de tests de validation.
Ce projet démontre qu'une solution libre peut améliorer efficacement la sécurité réseau tout en restant flexible et évolutive.

Mots-clés : sécurité des réseaux, NAC, PacketFence, open source, 802.1X, MAB, Cisco, Active Directory, Naftal, accès réseau sécurisé.

Abstract

In a context where network security remains a major concern for all companies, this thesis presents the analysis, design, and implementation of an open-source network access control (NAC) solution.

This work focuses on the deployment of an open-source NAC solution within the GPL district of Naftal in Béjaïa, aiming to secure access to network resources.Following an analysis of security concepts and existing NAC solutions, PacketFence was selected for its features, compatibility, and open-source nature.

The practical part includes the configuration of a Cisco switch, its integration with Active Directory, and the implementation of authentication methods such as 802.1X, MAB, and captive portal, followed by validation tests.
This project demonstrates that a free solution can effectively enhance network security while remaining flexible and scalable.

Keywords : network security, NAC, PacketFence, open source, 802.1X, MAB, Cisco, Active Directory, Naftal, secure network access.