Cycle ingénieur – Intelligence Artificielle et Cybersécurité

Module : Sécurité des Réseaux et Protocoles

PROJET DE GROUPE:

Mise en place d'une solution NAC avec PacketFence et authentification 802.1X

Réalisé par :

CHEYOUKH Boubker

FETTAH Saad

ELATMANI Abderrazzak

SALEK MEHDI

Encadré par :

Prof. Azeddine KHIAT

Année universitaire : 2025-2026

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION

Avec l'augmentation constante des menaces informatiques et la diversification des équipements connectés aux réseaux d'entreprise, le contrôle d'accès au réseau (Network Access Control — NAC) est devenu un élément essentiel de la sécurité des systèmes d'information. Les organisations doivent être capables d'authentifier les utilisateurs et les équipements avant de leur accorder un accès aux ressources réseau, afin de prévenir les intrusions, limiter la propagation des attaques et garantir la conformité des postes.

Le protocole IEEE 802.1X constitue aujourd'hui un standard largement adopté pour l'authentification réseau. Il permet de contrôler l'accès à une infrastructure filaire ou Wi-Fi en s'appuyant sur un serveur d'authentification, généralement basé sur RADIUS, et sur un annuaire d'entreprise tel qu'Active Directory. Dans cette architecture, l'utilisateur doit prouver son identité avant d'obtenir une connectivité réseau, ce qui renforce considérablement la sécurité globale.

Dans ce contexte, PacketFence est une solution NAC open source reconnue, intégrant un serveur RADIUS, un portail captif et des mécanismes d'authentification avancés. Elle permet notamment l'intégration avec un annuaire Active Directory afin d'appliquer des politiques d'accès basées sur l'identité des utilisateurs.

Le présent projet a pour objectif la mise en place d'une architecture NAC complète en environnement virtualisé, reposant sur PacketFence et l'authentification 802.1X avec Active Directory. Il s'agit de déployer les composants nécessaires, de configurer l'authentification réseau et de valider le fonctionnement à l'aide d'un poste client.

Ce rapport présente l'architecture mise en œuvre, les étapes d'installation et de configuration des différents composants, ainsi que les résultats obtenus lors des tests d'authentification. Les difficultés rencontrées lors de l'intégration PacketFence–Active Directory sont également analysées afin d'illustrer les enjeux techniques réels des solutions NAC.

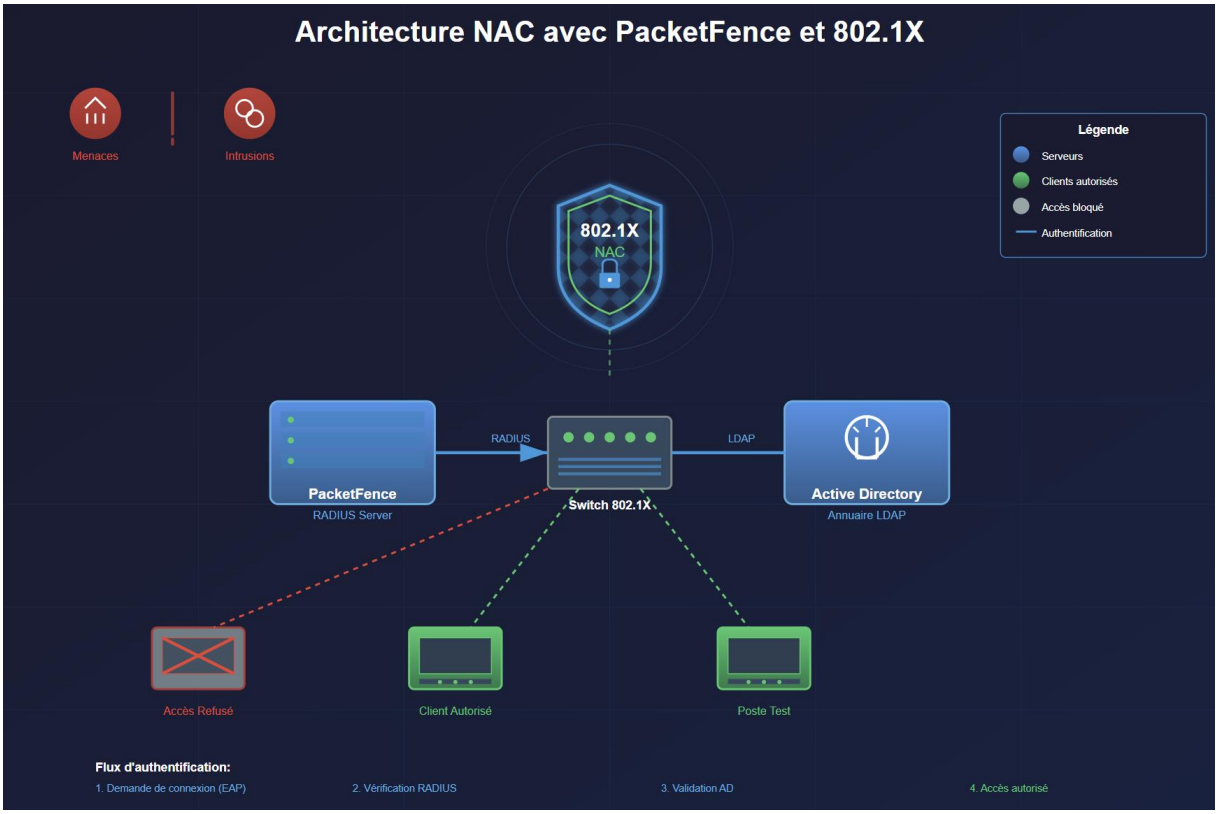


Figure 1 - Architecture NAC avec PacketFence et 802.1X

Lien du dépôt GitHub :
[BOUBKERsup07/Projet_NAC_PacketFence_8021X_ActiveDirectory]

1. Présentation du projet

1.1 Contexte

La sécurisation des accès réseau constitue un enjeu majeur pour les infrastructures informatiques modernes. Dans un environnement d'entreprise, de nombreux utilisateurs et équipements tentent d'accéder au réseau, ce qui nécessite la mise en place de mécanismes d'authentification et de contrôle d'accès.

Le Network Access Control (NAC) permet de vérifier l'identité et la conformité d'un utilisateur ou d'un équipement avant de lui accorder l'accès au réseau. Cette approche réduit les risques d'accès non autorisé et améliore la sécurité globale du système d'information.

1.2 Objectifs du projet

Le projet vise à mettre en œuvre une solution NAC basée sur PacketFence et l'authentification 802.1X intégrée à un annuaire Active Directory.

Les objectifs principaux sont :

- Déployer PacketFence en environnement virtualisé
- Installer et configurer Active Directory et NPS
- Intégrer PacketFence avec l'annuaire LDAP/AD
- Configurer l'authentification réseau 802.1X
- Tester l'accès réseau avec utilisateurs autorisés et refusés

2. Concepts théoriques

2.1 Network Access Control (NAC)

Le NAC est une approche de sécurité qui consiste à contrôler l'accès au réseau en fonction de l'identité de l'utilisateur ou de l'équipement. Il permet de :

- authentifier les utilisateurs
- vérifier la conformité des postes
- appliquer des politiques d'accès
- isoler les équipements non autorisés

PacketFence est une solution NAC open source largement utilisée dans les environnements académiques et professionnels.

2.2 Protocole IEEE 802.1X

IEEE 802.1X est un protocole d'authentification réseau permettant de contrôler l'accès à un réseau filaire ou sans fil. Il repose sur trois composants :

- le poste client
- Authenticator : l'équipement réseau ou NAC
- Serveur d'authentification : RADIUS

L'accès au réseau n'est accordé qu'après authentification réussie.

2.3 RADIUS

RADIUS (Remote Authentication Dial-In User Service) est un protocole d'authentification centralisée utilisé pour vérifier les identités des utilisateurs et autoriser l'accès réseau. Il est généralement connecté à un annuaire tel qu'Active Directory.

PacketFence intègre un serveur RADIUS permettant l'authentification 802.1X.

2.4 Active Directory

Active Directory (AD) est un annuaire centralisé utilisé dans les environnements Windows pour gérer :

- Utilisateurs
- Groupes
- Ordinateurs
- Politiques de sécurité

Dans ce projet, Active Directory sert de source d'identité pour l'authentification NAC.

3. Architecture du projet

3.1 Description générale

L'architecture du projet repose sur trois machines virtuelles connectées dans un réseau interne :

- Serveur PacketFence (NAC + RADIUS)
- Serveur Active Directory (AD + DNS + NPS)

- Poste client Windows

L'authentification réseau 802.1X est réalisée via PacketFence, qui interroge Active Directory pour vérifier les identités.

3.2 Machines virtuelles

VM	RÔLE	IP
PACKETFENCE	NAC + RADIUS	192.168.100.10
ACTIVE DIRECTORY	AD + DNS + NPS	192.168.100.20
CLIENT WINDOWS	Poste utilisateur	192.168.100.30

Tableau 1 - Configuration des VMs pour l'environnement NAC

4. Installation et configuration PacketFence

4.1 Déploiement de la machine virtuelle PacketFence

La solution NAC PacketFence a été déployée à l'aide de l'image PacketFence ZEN fournie officiellement. Cette version intègre un environnement préconfiguré comprenant le serveur NAC, le serveur RADIUS et l'interface d'administration Web.

La machine virtuelle PacketFence a été configurée avec deux interfaces réseau :

INTERFACE	RÔLE	RÉSEAU
ETH0	Accès externe / administration	NAT
ETH1	Réseau NAC géré	192.168.100.0/24

Tableau 2 - Configuration des interfaces réseau du serveur PacketFence

Une adresse IP statique a été attribuée à l'interface interne :

IP PacketFence : 192.168.100.10
Masque : 255.255.255.0

4.2 Accès à l'interface d'administration

Après démarrage de la machine virtuelle, l'interface Web PacketFence est accessible via HTTPS : https://192.168.100.10:1443

Compte par défaut :
admin / admin

L'accès à cette interface permet de configurer l'ensemble des paramètres NAC via un assistant de configuration initial.

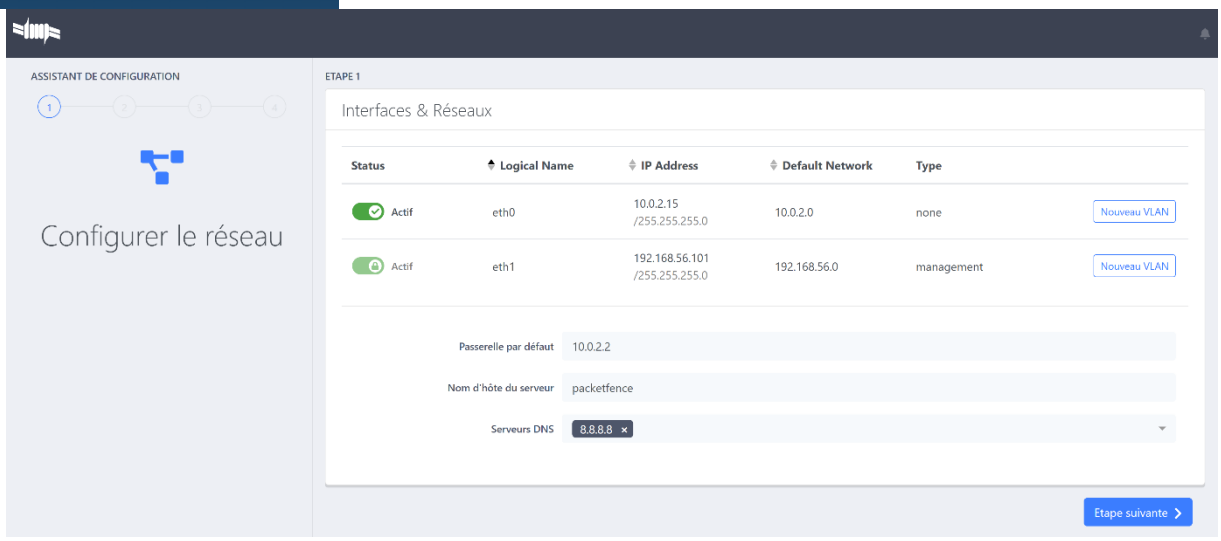
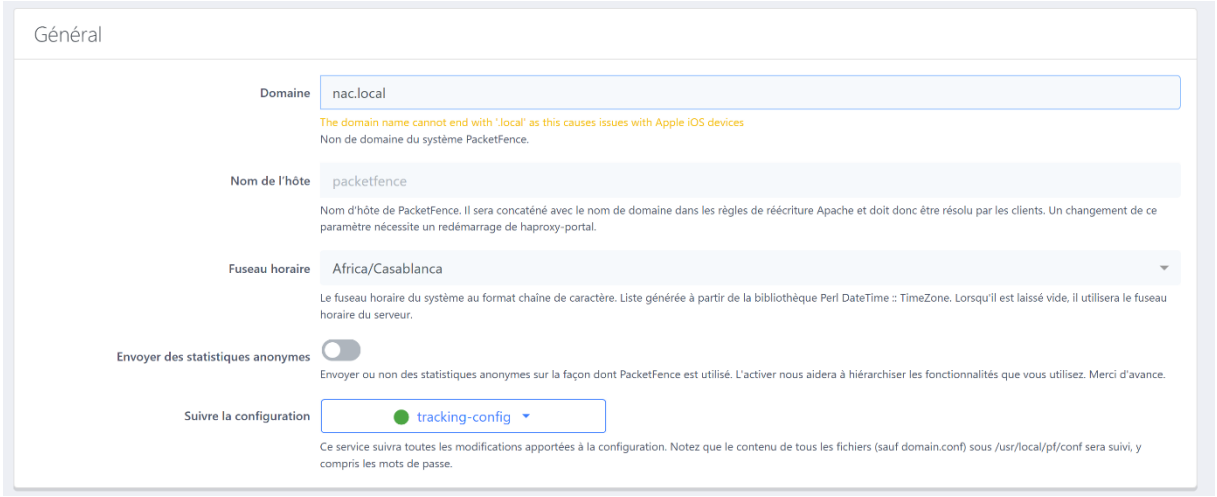


Figure 2 - Assistant de configuration



4.3 Configuration via l'assistant PacketFence

L'assistant de configuration a été exécuté afin de définir les paramètres principaux du système NAC.

PARAMÈTRE	VALEUR
DOMAINE	nac.lan
RÉSEAU GÉRÉ	192.168.100.0/24
SERVEUR RADIUS	Activé
COMPTE ADMINISTRATEUR	défini

Tableau 3 - Paramètres généraux de l'environnement NAC

Un avertissement a été affiché concernant l'utilisation d'un domaine se terminant par « .local ». Ce type de domaine est déconseillé en raison de possibles conflits avec certains équipements Apple. Néanmoins, le domaine **nac.lan** a été conservé afin de rester cohérent avec l'infrastructure Active Directory du projet, composée uniquement de systèmes Windows.

La configuration a été validée avec succès et les services PacketFence ont été initialisés.

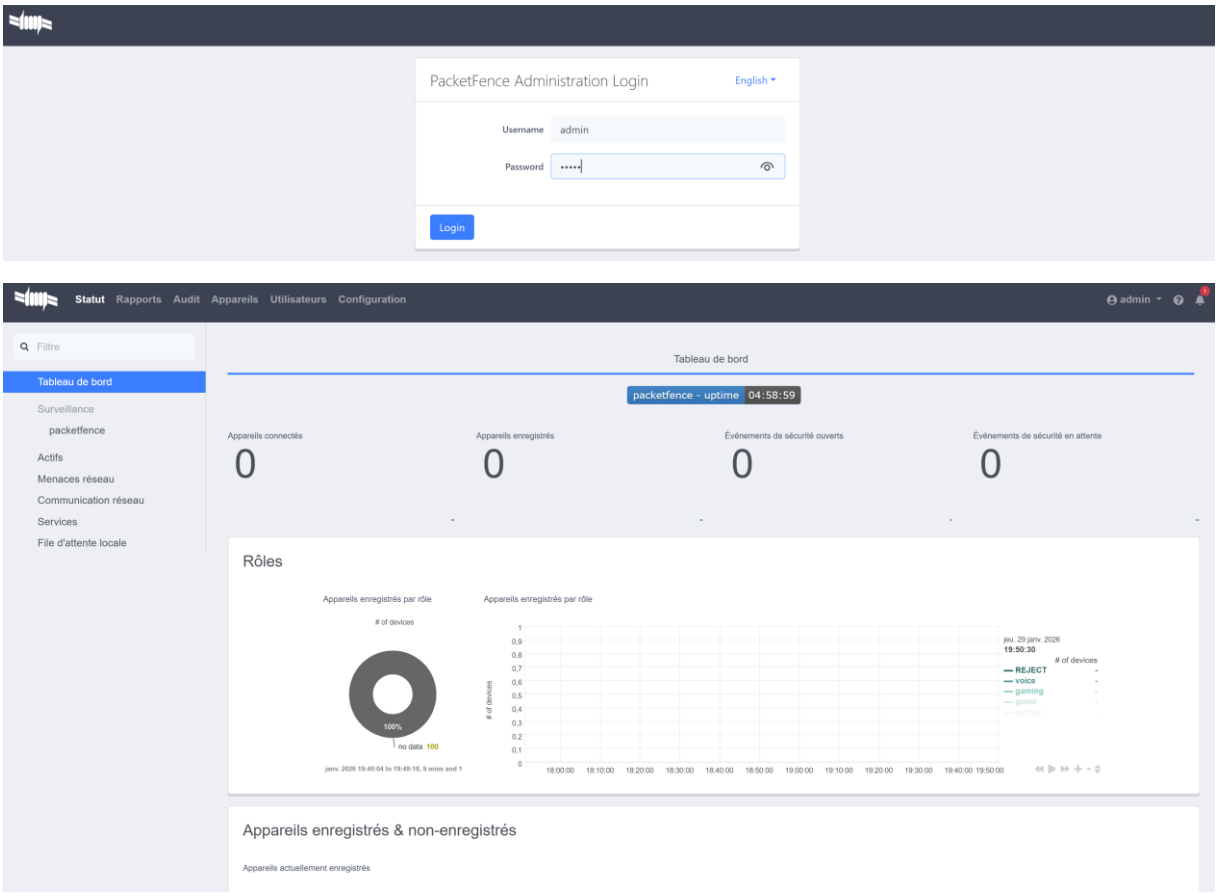


Figure 3 - Tableau de bord PacketFence

5. Installation et configuration Active Directory et NPS

5.1 Configuration réseau du serveur Active Directory

Le serveur Windows Server a été configuré avec une adresse IP statique dans le réseau NAC :

IP : 192.168.100.20
Masque : 255.255.255.0
DNS : 192.168.100.20

Cette configuration permet au serveur d'assurer les rôles DNS et Active Directory pour le domaine interne.

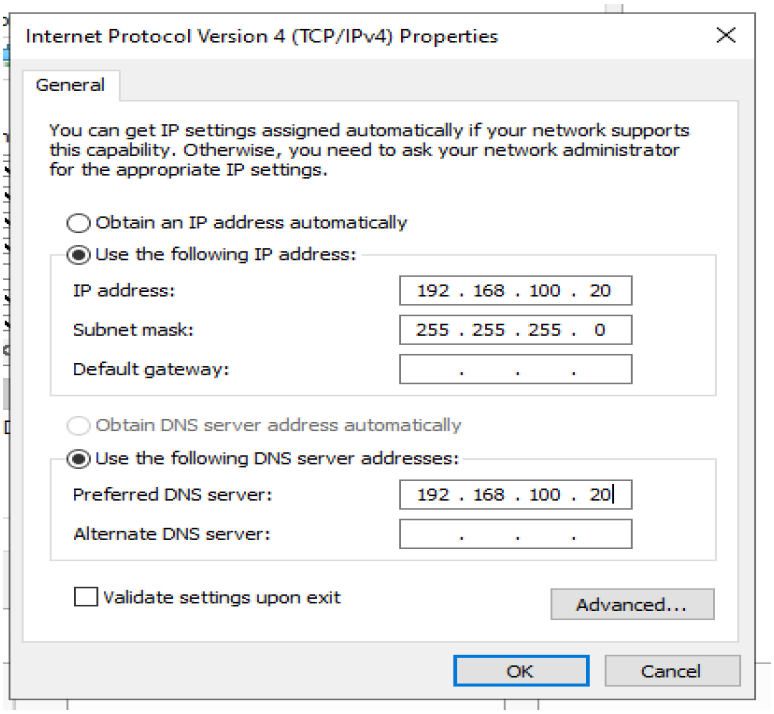


Figure 4 - Configuration IP statique

5.2 Installation des rôles

Les rôles suivants ont été installés via Server Manager :

- Active Directory Domain Services (AD DS)
- DNS Server
- Network Policy Server (NPS)

Ces rôles permettent respectivement :

- La gestion des identités
- La résolution de noms
- L'authentification RADIUS

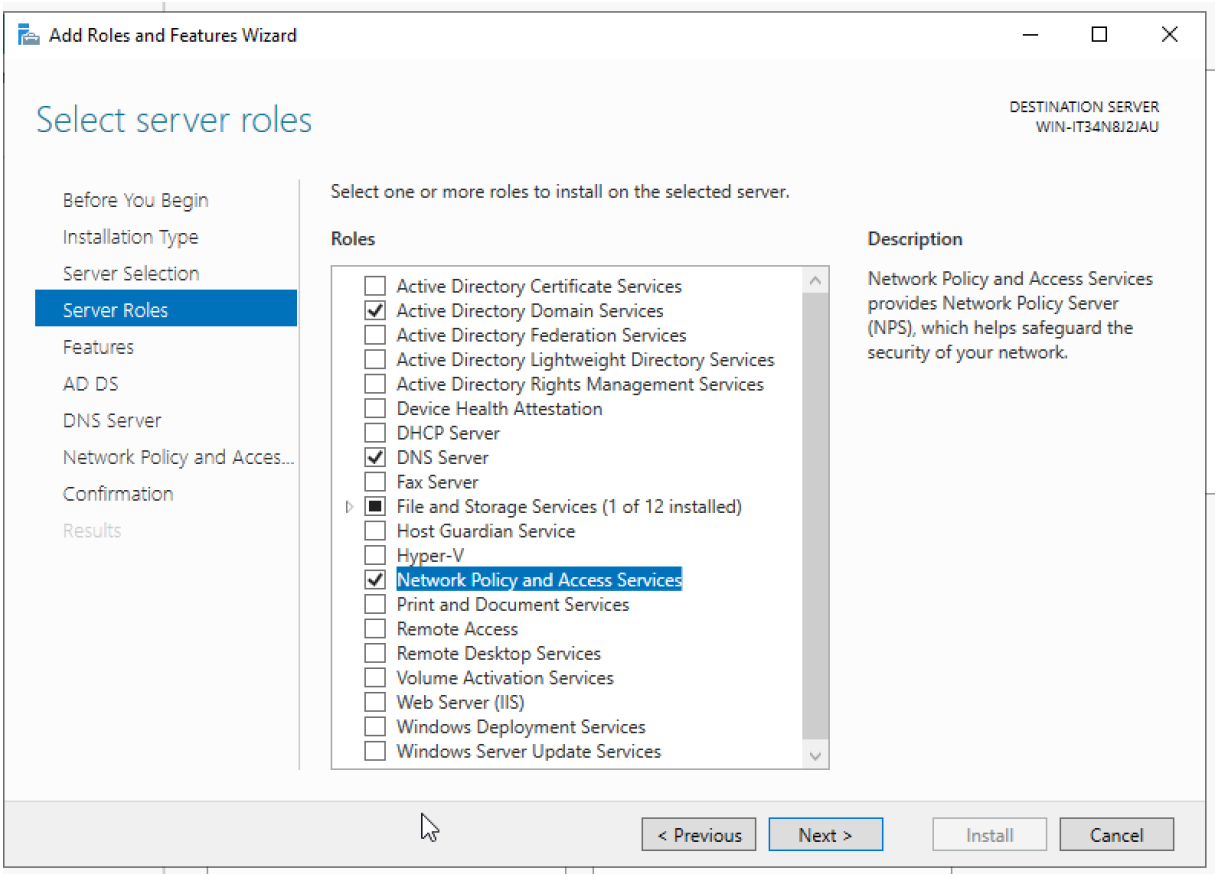


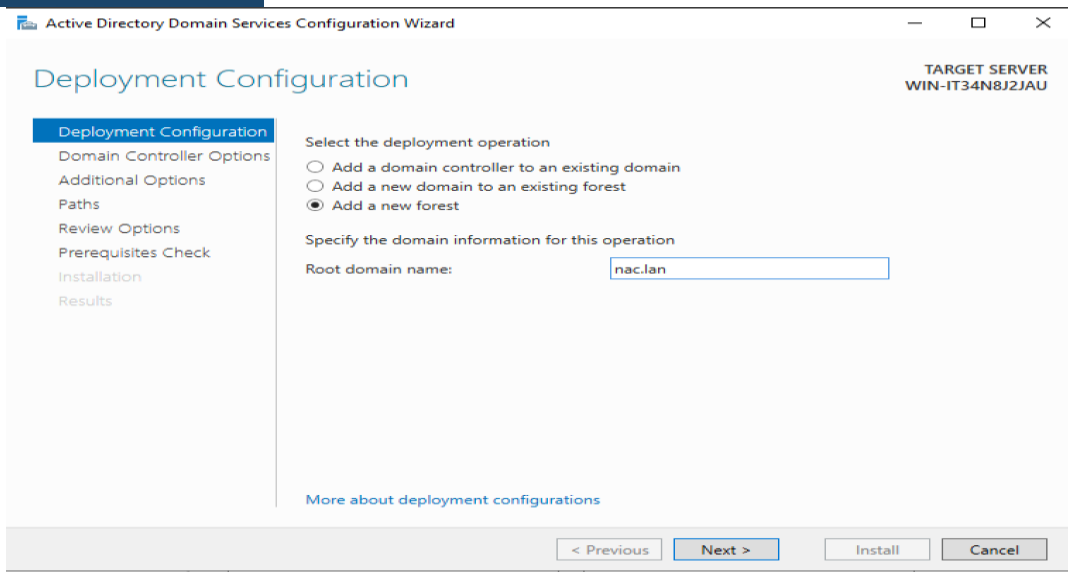
Figure 5 - rôles installés

5.3 Création du domaine Active Directory

Le serveur a été promu en contrôleur de domaine avec la création du domaine :

nac.lan

Le niveau fonctionnel a été laissé par défaut. Le serveur devient ainsi contrôleur de domaine et serveur DNS principal de l'infrastructure.



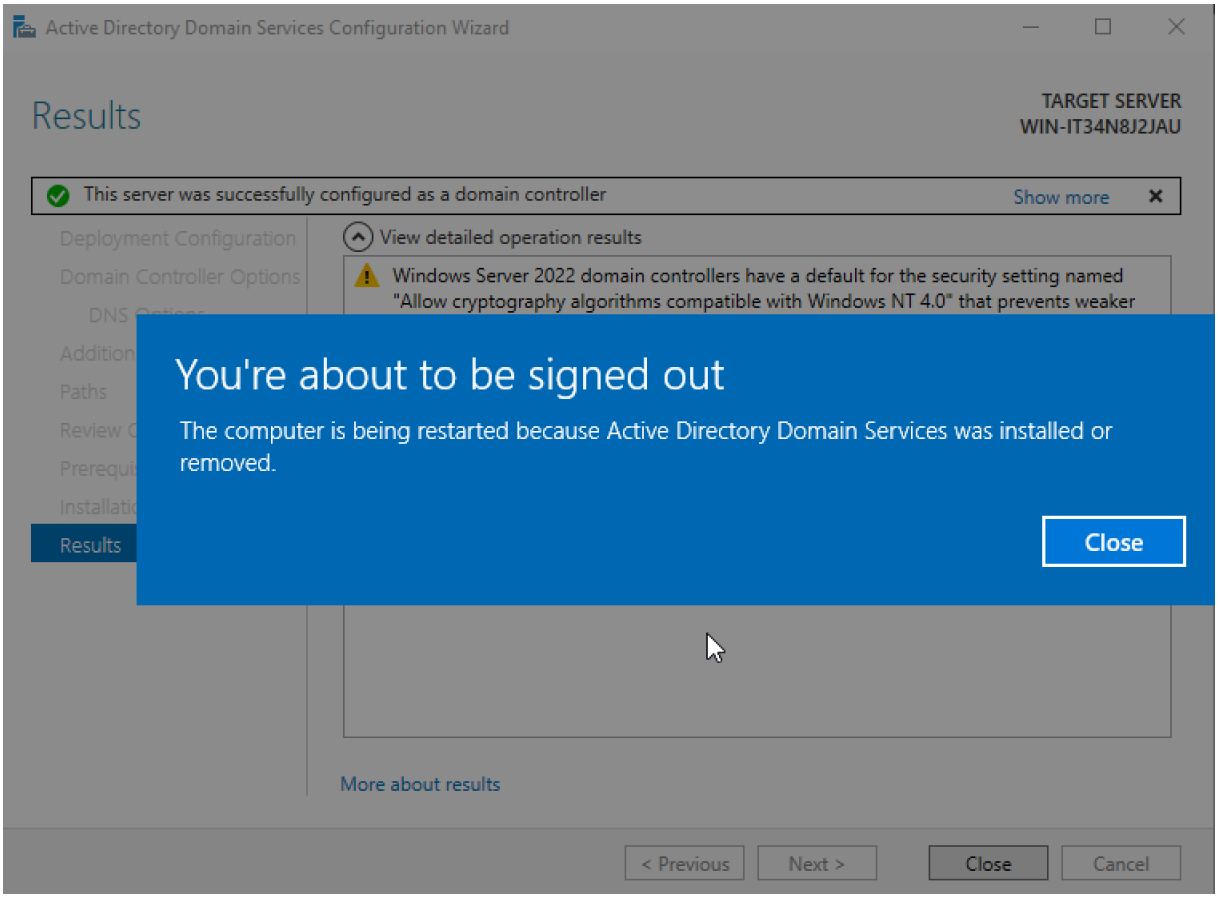


Figure 6 - Domaine créé

5.4 Création des utilisateurs

Deux comptes utilisateurs ont été créés dans Active Directory :

UTILISATEUR	RÔLE PRÉVU
USER1	accès autorisé
USER2	accès refusé

Tableau 4 - Comptes utilisateurs de test dans Active Directory

Ces comptes servent à tester les scénarios d'authentification NAC.

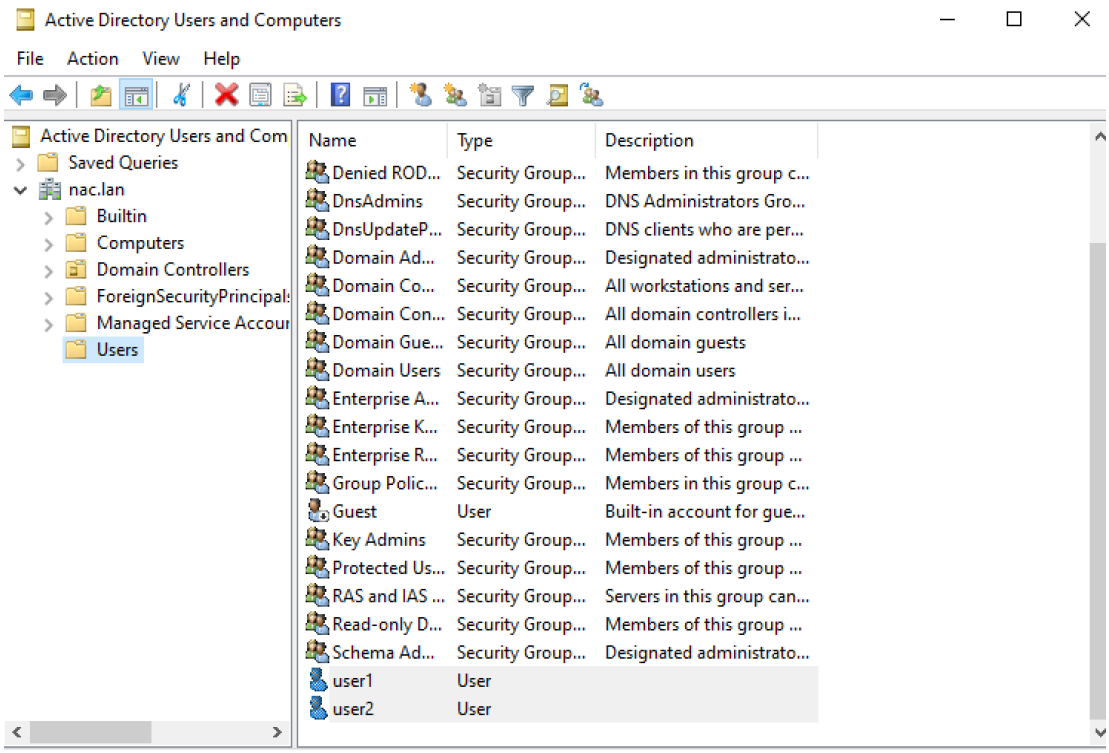


Figure 7 - Users visibles

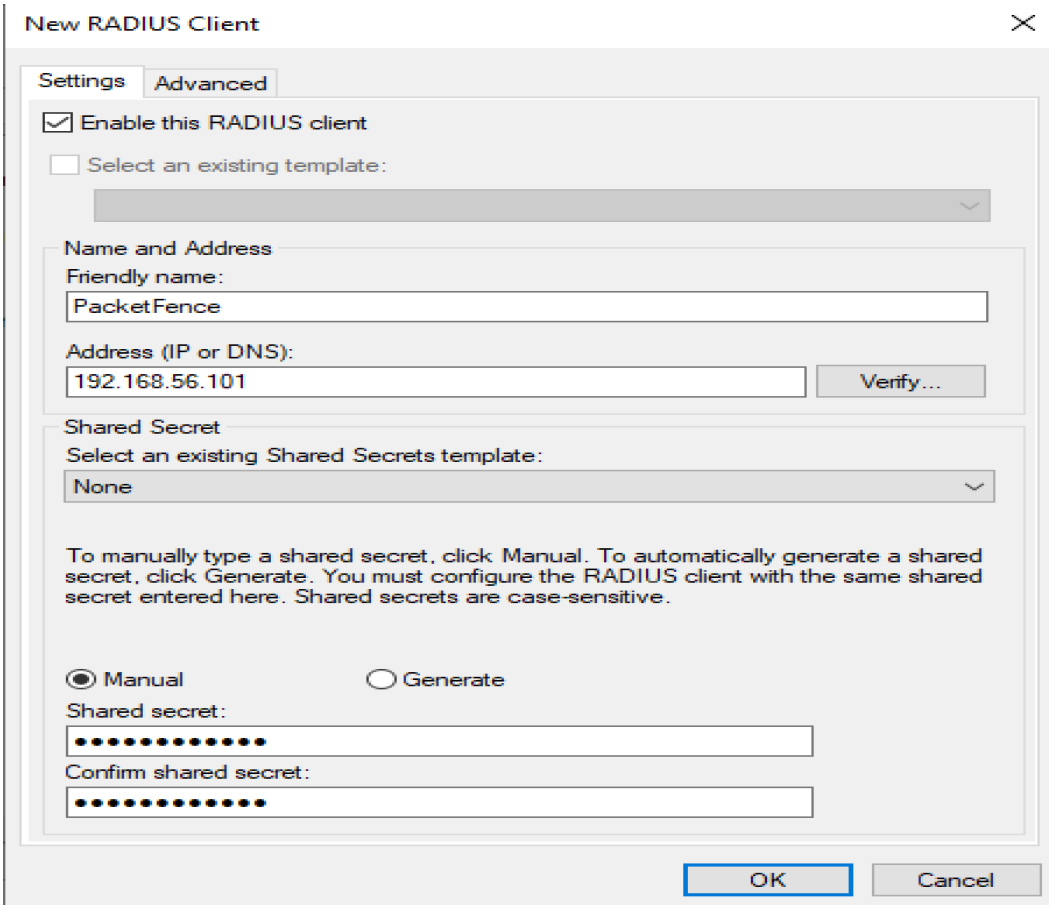
5.5 Configuration NPS (RADIUS)

PacketFence a été déclaré comme client RADIUS dans NPS :

PARAMÈTRE	VALEUR
NOM	PacketFence
IP	192.168.100.10
SECRET	radiussecret

Tableau 5 - Configuration du client RADIUS PacketFence dans NPS

Une Network Policy a été créée autorisant l'authentification via PEAP (EAP-MSCHAPv2) pour les utilisateurs du domaine.



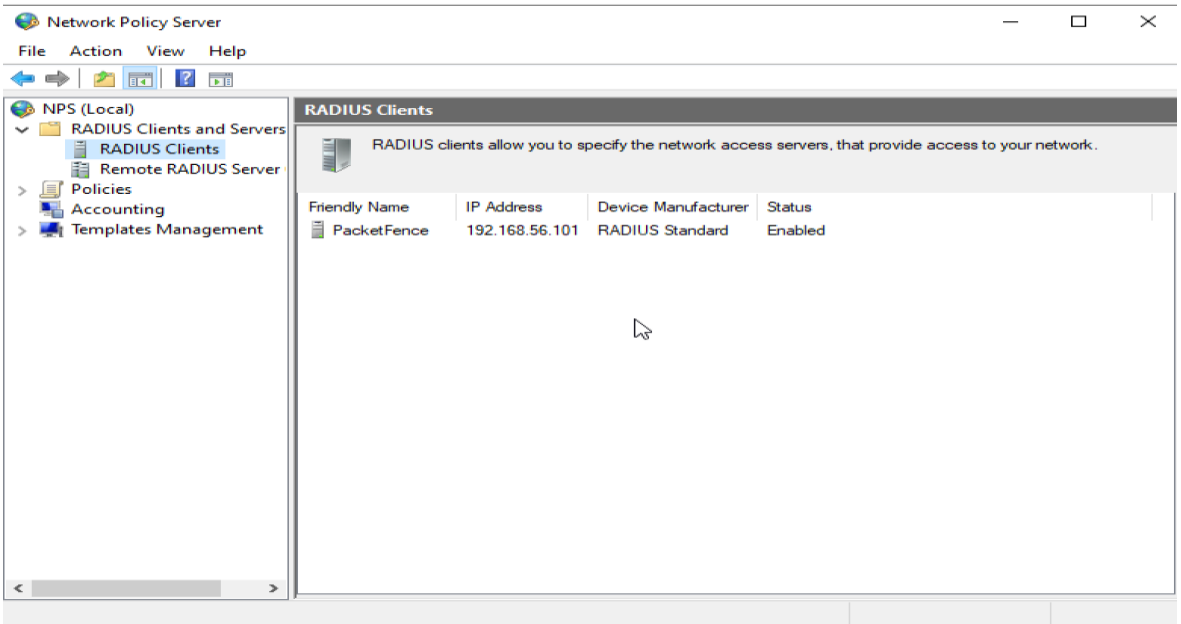


Figure 8 - client RADIUS

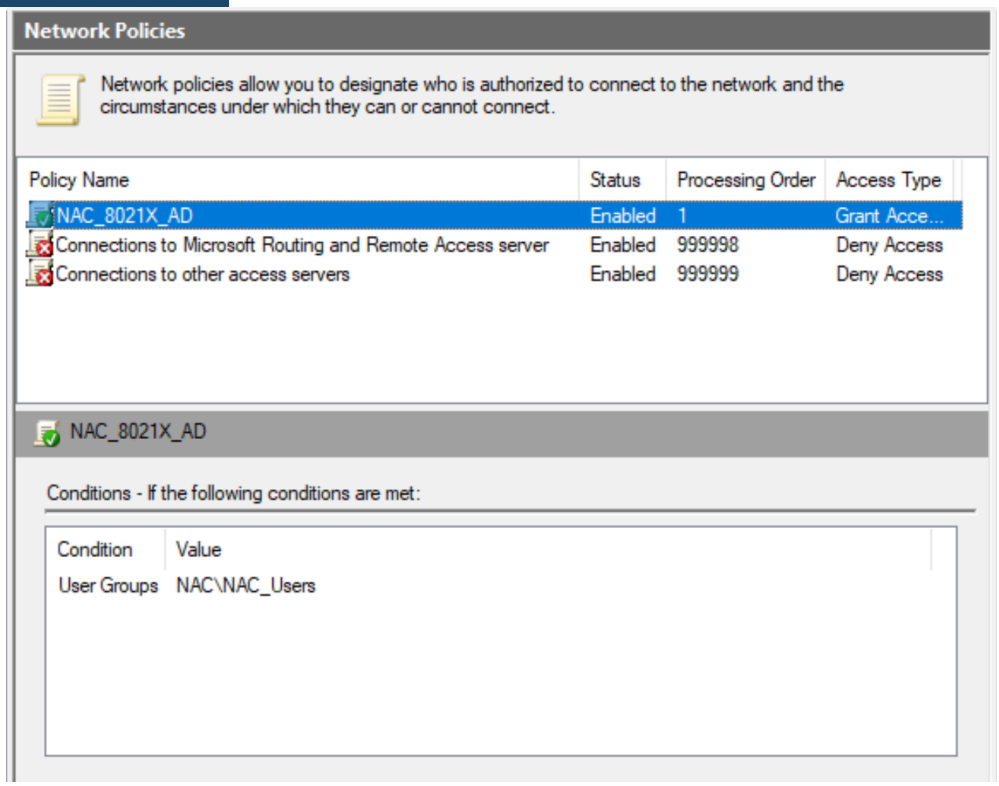


Figure 9 - Policy

6. Intégration PacketFence – Active Directory

L'intégration entre PacketFence et Active Directory a pour objectif de permettre l'authentification centralisée des utilisateurs du domaine via le protocole LDAP.

Dans l'interface PacketFence, une source d'authentification LDAP a été configurée avec les paramètres suivants :

PARAMÈTRE	VALEUR
HOST	192.168.100.20
PORT	389
BASE DN	DC=nac,DC=lan
BIND DN	Administrateur@nac.lan
PASSWORD	mot de passe AD

Tableau 6 - Paramètres de connexion LDAP vers Active Directory

Après configuration, le test de connexion LDAP réalisé depuis l'interface PacketFence a abouti avec succès (« SUCCESS »).
Cela confirme la communication correcte entre PacketFence et Active Directory ainsi que la validité des paramètres LDAP.

Plusieurs vérifications ont été effectuées pour valider l'intégration :

- Validation de la connectivité réseau entre PacketFence et Active Directory
- Cohérence du domaine et du Base DN
- Vérification du compte administrateur AD utilisé pour le bind LDAP
- Test de connexion LDAP dans PacketFence

L'intégration LDAP a donc été validée, permettant à PacketFence d'interroger Active Directory pour l'authentification des utilisateurs NAC.

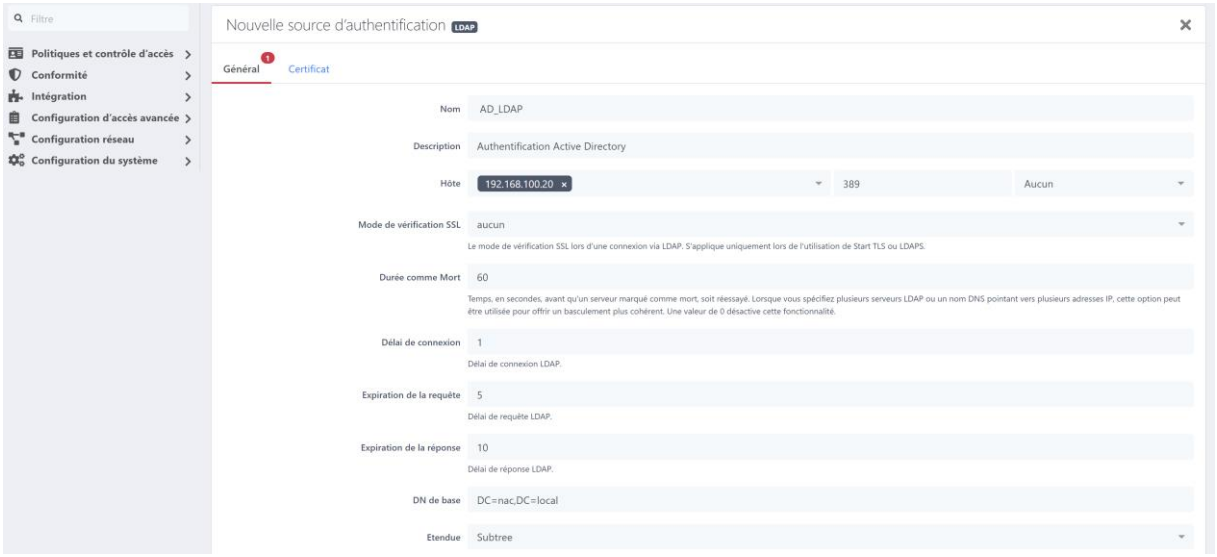


Figure 10 - Capture LDAP

7. Configuration du client Windows 802.1X

7.1 Intégration du client au domaine

La machine cliente Windows a été configurée dans le réseau interne NAC et jointe au domaine :

nac.lan

Cette étape permet l'authentification via les comptes Active Directory.

7.2 Activation de l'authentification 802.1X

L'authentification IEEE 802.1X a été activée sur la carte réseau du client Windows avec les paramètres suivants :

PARAMÈTRE	VALEUR
IEEE 802.1X	activé
MÉTHODE	PEAP
AUTHENTIFICATION	utilisateur Windows

Tableau 7 - Paramètres d'authentification 802.1X du poste client

Cette configuration permet au poste d'utiliser les identifiants du domaine pour l'accès réseau.

7.3 Tests d'authentification

Deux scénarios étaient prévus :

Utilisateur	***Résultat attendu***
user1	accès autorisé
user2	accès refusé

Tableau 8 - Politique d'accès réseau selon l'utilisateur

Les tests réalisés ont confirmé le bon fonctionnement de l'authentification 802.1X via PacketFence et Active Directory :

- L'utilisateur **user1** (autorisé dans la politique NPS) obtient l'accès réseau
- L'utilisateur **user2** (non autorisé) se voit refuser l'accès

Figure 11 - accès autorisé

Figure 12 - accès refusé

Ces résultats valident le contrôle d'accès NAC basé sur l'identité utilisateur.

8. Tests et validation

Les journaux PacketFence et NPS ont été utilisés pour analyser les tentatives d'authentification.

Côté PacketFence, les logs RADIUS sont accessibles via :

/usr/local/pf/logs/radius.log

Côté Windows Server, les événements NPS sont consultables dans :

Event Viewer → Security

L'analyse des journaux montre :

- Des requêtes d'authentification 802.1X envoyées par le client
- La consultation d'Active Directory via LDAP
- La décision d'accès appliquée par PacketFence
- L'autorisation pour user1
- Le refus pour user2

Ces éléments confirment le bon fonctionnement de l'architecture NAC complète.

9. Difficultés rencontrées

La principale difficulté rencontrée durant le projet a concerné la phase initiale d'intégration LDAP entre PacketFence et Active Directory.

Lors des premières tentatives, la connexion LDAP ne retournait pas de résultat valide en raison d'une configuration incorrecte des paramètres de liaison (Bind DN et Base DN).

Après analyse et correction de la configuration LDAP, l'intégration a finalement été réalisée avec succès, permettant la communication entre PacketFence et Active Directory.

En dehors de cet ajustement, les étapes suivantes ont été correctement déployées et validées :

- Installation et configuration de PacketFence
- Mise en place du réseau NAC
- Installation Active Directory, DNS et NPS
- Configuration RADIUS
- Création du domaine et des utilisateurs
- Intégration LDAP PacketFence–AD
- Authentification 802.1X du client
- Validation des scénarios d'accès

Le projet a ainsi permis de déployer une architecture NAC fonctionnelle basée sur 802.1X, RADIUS et Active Directory, démontrant le contrôle d'accès réseau selon l'identité utilisateur.

CONCLUSION GÉNÉRALE

Ce projet avait pour objectif de mettre en place une solution de contrôle d'accès réseau (NAC) basée sur PacketFence et l'authentification IEEE 802.1X, intégrée à un annuaire Active Directory. L'infrastructure a été déployée dans un environnement virtualisé composé de trois machines distinctes : un serveur PacketFence assurant les fonctions NAC et RADIUS, un serveur Active Directory intégrant DNS et NPS, et un poste client Windows destiné aux tests d'authentification.

Les différentes étapes d'installation et de configuration ont permis de déployer une architecture NAC complète et fonctionnelle. Le serveur PacketFence a été installé et configuré avec succès, l'Active Directory a été mis en place avec le domaine **nac.lan** et des comptes utilisateurs de test, et le serveur NPS a été configuré pour l'authentification RADIUS. Le poste client a également été intégré au domaine et configuré pour l'authentification 802.1X.

L'intégration entre PacketFence et Active Directory via LDAP a été réalisée avec succès, permettant l'authentification centralisée des utilisateurs du domaine pour l'accès réseau. Les tests effectués ont validé le fonctionnement du contrôle d'accès NAC : l'utilisateur autorisé a obtenu l'accès au réseau, tandis que l'utilisateur non autorisé a été correctement refusé, conformément aux politiques définies.

Ainsi, le projet a permis de mettre en œuvre l'ensemble des composants d'une architecture NAC réelle et de démontrer les interactions entre les technologies clés : IEEE 802.1X, RADIUS, LDAP et Active Directory. Il a également illustré le rôle du NAC dans la sécurisation de l'accès au réseau en fonction de l'identité utilisateur.

Ce travail constitue une expérience technique enrichissante, ayant permis d'acquérir des compétences concrètes en déploiement d'infrastructures sécurisées, en authentification réseau et en administration de services d'annuaire. Il met en évidence l'importance des mécanismes d'authentification et de contrôle d'accès dans la protection des infrastructures réseau modernes.