LOGO ORGANISME ACADEMIQUE

ADISCA N°	
Date du rapport de stage :	**19/03/2025**

MEMOIRE TECHNIQUE ARIANEGROUP

TITRE DU RAPPORT :	Mise en place d'un serveur RADIUS et du protocole de sécurité 802.1x sur un moyen industriel
APPPRENTI :	Maxime, Laville
Date de l'alternance :	Du 04/12/2023 au 31/07/2025
TUTEUR D'ENTREPRISE :	**R.L**
Service :	Systems & Products CyberSecurity Engineer
ORGANISME D'ACCUEIL :	**ARIANEGROUP**
Adresse :	51/61 route de Verneuil BP71040 78131 LES MUREAUX CEDEX
ORGANISME ACADEMIQUE :	**Aurlom BTS+**
Adresse :	118 Avenue Jean Jaurès 75019, PARIS
TUTEUR PEDAGOGIQUE :	Corentin, DAGUET

Exemplaire Papier n° 1/ Y : Prénom, Nom
Exemplaire Papier n° 2/ Y : Prénom, Nom
Exemplaire Papier n° 3/ Y : Prénom, Nom
Exemplaire Papier n° 4/ Y : Prénom, Nom
Exemplaire Papier n° 5/ Y : Prénom, Nom
Exemplaire Papier n° 6/ Y : Prénom, Nom

MENTION DE PROPRIETE

Ce document et les informations qu'il contient sont propriété d'ArianeGroup. Il ne doit pas être utilisé à d'autres fins que celles pour lesquelles il a été remis. Il ne peut être ni reproduit, ni divulgué à des tiers (en tout ou partie) sans l'accord préalable et écrit d'ArianeGroup. ArianeGroup SAS –Tous droits réservés. // This document and the information it contains are property of ArianeGroup. It shall not be used for any purpose other than those for which it was supplied. It shall not be repro-duced or disclosed (in whole or in part) to any third party without ArianeGroup prior written consent. ArianeGroup SAS – All rights reserved.

CLAUSE DE DEONTOLOGIE

Les activités d'ArianeGroup intéressent la défense et la sécurité nationale et les intérêts fondamentaux de la nation. Ses salariés et sous-traitants sont soumis à un devoir de discrétion professionnelle et ne sont pas autorisés à diffuser ou rendre accessible ces informations à des personnes ou organismes non-autorisés. Les informations auxquelles j'ai eu l'accès pendant mon apprentissage en entreprise sont non-publiques, voire confidentielles.

De fait, ce document à vocation académique ne comporte aucun nom et chiffres réels. Les informations qu'il contient sont propriété d'ArianeGroup. Il ne doit pas être utilisé à d'autres fins que celles pour lesquelles il a été remis. Il ne peut être ni reproduit, ni divulgué à des tiers (en tout ou partie) sans l'accord préalable et écrit d'ArianeGroup SAS.

2024/2025

Mission professionnelle N°6

Maxime Laville

ArianeGroup

19/03/2025

Mise en place d’un serveur RADIUS et du protocole de sécurité 802.1x sur un moyen industriel.

Description :

Cette mission consiste à mettre en place un serveur d’authentification RADIUS avec le protocole de sécurité 802.1x et génération de certificat d’autorité sur un moyen industriel.

Validation de la mission professionnelle :

Nom	Date	Tampon
Maxime Laville	19/03/2025	

S o m m a i r e

Table des illustrations

1. FORMALISATION DU BESOIN

Le projet vise à mettre en place un serveur d'authentification RADIUS, en s'appuyant sur le protocole de sécurité 802.1x. L'objectif principal, est de sécuriser un de nos moyens industriels afin de pouvoir gérer les accès non autorisés et les cyberattaques. Cette solution permet par la suite de :

1. Authentifier les utilisateurs et les équipements qui se connectent au réseau.
2. Garantir une sécurité renforcée en évitant les potentielles connexions frauduleuses.
3. Assurer une traçabilité des accès grâce aux journaux du serveur RADIUS.

2. ARCHITECTURE ET TECHNOLOGIES UTILISEES

2.1 INFRASTRUCTURE MISE EN PLACE

L'architecture du protocole 802.1x repose sur trois éléments de base :

1. **Un client (Demandeur) :** L'appareil qui demande l'accès au réseau (2 clients utilisés : Windows et Debian)
2. **Un équipement réseau (Authentificateur) :** Un switch Cisco qui relaie les requêtes d'authentification.
3. **Le serveur d'authentification :** Vérifie l'identité de l'utilisateur ou de la machine.

2.2 TECHNOLOGIES UTILISEES

Pour mettre en place le serveur RADIUS (Remote Authentication Dial-In User Service), nous avons utilisés l'outil Open Source FreeRADIUS qui est actuellement le serveur RADIUS le plus utilisé au monde.

FreeRADIUS est un serveur RADIUS qui gère l'authentification, l'autorisation ainsi que la comptabilité à l'aide du protocole de sécurité 802.1x qui définit la méthode d'authentification. La méthode d'authentification utilisée dans le protocole 802.1x est le protocole EAP-TLS qui s'occupe de sécuriser la communication entre les clients et le serveur d'authentification RADIUS en la chiffrant à l'aide d'un certificat d'authentification.

EAP-TLS (Extensible Authentication Protocole – Transport Layer Security) est un protocole d'authentification mutuelle du supplicant et du serveur par certificats. Cette méthode nécessite que le serveur et chaque supplicant possèdent un certificat. Elle impose donc l'utilisation d'une infrastructure de gestion de clés dans le système d'information.

2.3 SCHEMA RESEAU

Ce schéma représente l'infrastructure du réseau mis en place lors du déploiement du serveur d'authentification RADIUS.

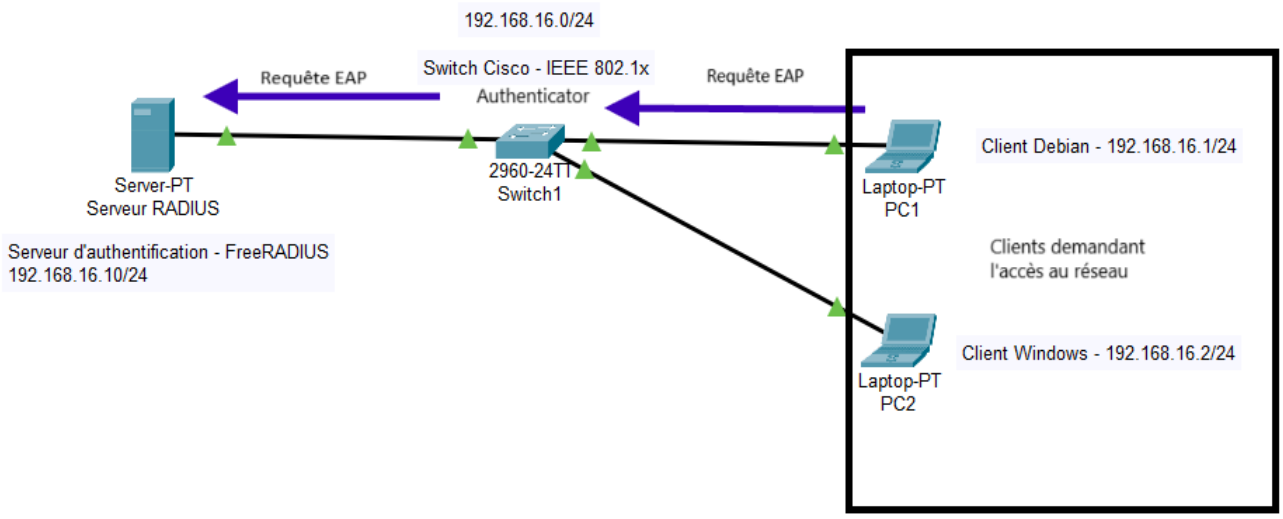

Figure 1 – Infrastructure du réseau

3. MISE EN ŒUVRE ET DEPLOIEMENT

3.1 INSTALLATION ET CONFIGURATION DU SERVEUR RADIUS

Ce paragraphe détaille l'ensemble des commandes qui ont été utilisées pour mettre en œuvre le serveur RADIUS.

Installation de FreeRADIUS sur la machine qui joue le rôle du serveur d'authentification :

```
#sudo apt update
#sudo apt install freeradius
```

Configuration des clients autorisés (sudo nano /etc/freeradius/clients.conf) :

```
#Client Debian
        #ipaddr = 192.168.16.1/24
        #secret = motdepasse
    #Client Windows
        #ipaddr = 192.168.16.2/24
        #secret = motdepasse
```

3.2 CONFIGURATION DES EQUIPEMENTS RESEAU

L'objectif ici est d'activer IEEE 802.1x pour forcer les clients à s'authentifier avant d'accéder au réseau.

Configuration d'un port spécifique (Ex : Gig0/1) :

```
#Interface GigabitEthernet0/1
        #authentication port-control auto
        #dot1x pae authenticator
```

Interface GigabitEthernet0/1 : Configuration du port où est connecté le client (Ex : PC1/Client Linux.
Authentication port-control auto : Le switch va attendre une authentification avant d'autoriser l'accès.
Dot1x pae authenticator : Le switch agit comme authenticator, il va donc relayer les demandes des clients au serveur RADIUS.

4. SECURITE ET GESTION DES MENACES

4.1 RISQUES ET ATTAQUES POSSIBLES

De nos jours, les cyberattaques sont de plus en plus fréquentes et élaborées, c'est donc pour cela qu'il est important de bien protéger son système et d'avoir une bonne gestion des menaces. Les menaces les plus courantes sont :

1. **Attaque Man-in-the-Middle (MITM) :** Tentative d'interception des échanges d'authentification. L'utilisation de EAP-TLS avec des certificats chiffrés permet d'éviter ce type d'attaque.
2. **Usurpation d'identité :** L'attaquant utilise un faux identifiant, la vérification des logs et l'application d'une politique de sécurité de mots de passe robustes peut permettre de contrer ce type d'attaque. L'utilisation de clé privée peut aussi contrer cette attaque.
3. **Attaque sur le Serveur RADIUS :** Il peut y avoir des tentatives de surcharge ou d'injection SQL. La sécurisation du serveur via le pare-feu, les restrictions d'accès ou encore la surveillance des logs peut prévenir ce genre d'attaque. La limitation du nombre tentatives dans le temps par l'adresse IP peut également éviter les demandes de connexions abusives.

4.2 SUPERVISION ET MONITORING

La surveillance des logs RADIUS permet de surveiller les tentatives de connexion et d'authentification et nous permet de connaître l'adresse IP du demandeur (client).

La commande pour la surveillance des logs est la suivante :

```
#tail -f /var/log/freeradius/radius.log
```

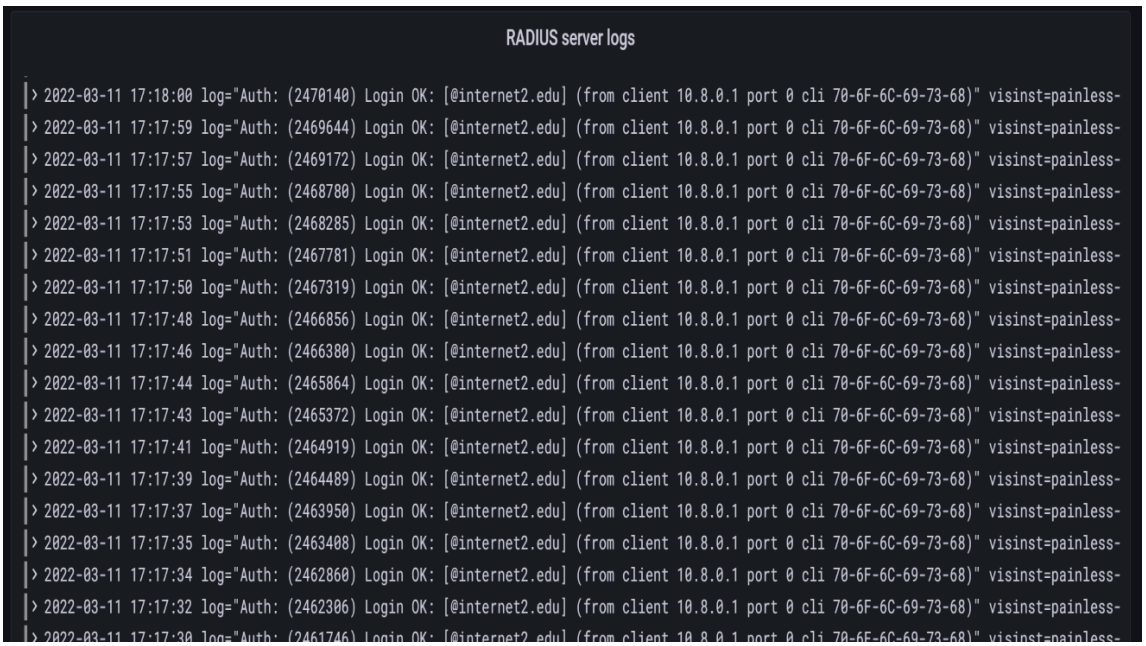

Figure 2 – Logs du serveur RADIUS

5. CONCLUSION

La mise en place de cette infrastructure avec l'utilisation d'un serveur d'authentification RADIUS nous permet ainsi de protéger davantage les communications et les informations qui y transitent.

Cette mission m'a permis de comprendre le fonctionnement du serveur RADIUS ainsi que du protocole de sécurité 802.1x et sa méthode d'authentification EAP-TLS, et de l'appliquer sur une infrastructure réseau afin de sécuriser les communications et d'authentifier les clients.