

<b>BTS SERVICES INFORMATIQUES AUX</b>		<b>SESSION 2025</b>
<b>ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)</b>		
<b>DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE</b>		<b>N° réalisation : 1</b>
Nom, prénom : CHEVREL Mathis		N° candidat :
Épreuve ponctuelle <input checked="" type="checkbox"/> Contrôle en cours de formation		Date : 15 / 12 /2025
Organisation support de la réalisation professionnelle ISFAC		
Intitulé de la réalisation professionnelle Mise en place d'un Wi-Fi d'entreprise avec authentification RADIUS		
Période de réalisation : 15/12/2025 Lieu : Isfac		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées @ Concevoir une solution d'infrastructure réseau X Installer, tester et déployer une solution d'infrastructure réseau @ Exploiter, dépanner et superviser une solution d'infrastructure réseau		
<b>Conditions de réalisation<sup>1</sup> (ressources fournies, résultats attendus)</b>		
La réalisation est menée dans le cadre d'un projet d'école. L'objectif consiste à mettre en place un réseau Wi-Fi d'entreprise sécurisé nécessitant l'authentification individuelle des utilisateurs toute authentification d'un utilisateur non référencé est refusée. L'objectif attendu est la mise en place d'un Wi-Fi professionnel sécurisé permettant l'identification de chaque utilisateur et garantissant un contrôle strict des accès réseau.		
<b>Description des ressources documentaires, matérielles et logicielles utilisées</b>		
<ul style="list-style-type: none"> <li>• Routeur / Pare-feu OPNsense (Virtuel)</li> <li>• Switch administrable</li> <li>• Borne Wi-Fi Ubiquiti</li> <li>• Hyperviseur Proxmox</li> </ul> <p>Logiciels / Éléments virtuels :</p> <ul style="list-style-type: none"> <li>• Machine virtuelle FreeRADIUS</li> <li>• Contrôleur UniFi Network</li> <li>• OPNsense (routage, VLAN, firewall)</li> <li>• Documentation FreeRADIUS, UniFi et OPNsense</li> <li>• Schéma réseau fourni dans le cadre du projet scolaire</li> </ul>		
<b>Modalités d'accès aux productions* et à leur documentation<sup>^</sup></b>		

<sup>1</sup> En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

\* Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont ses/ls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

<sup>^</sup> Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

## **Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**

### **I – Présentation du système d'information**

Dans le cadre de ce projet réalisé en environnement professionnel, j'ai participé à la mise en place et à l'exploitation d'une infrastructure informatique basée sur un serveur Proxmox, utilisé pour héberger plusieurs machines virtuelles.

Le réseau a été segmenté en différents VLAN afin de séparer les flux (utilisateurs, administrateurs, Wi-Fi) et de renforcer la sécurité globale de l'infrastructure. Le routage, la gestion des VLAN ainsi que les règles de pare-feu ont été confiés à un routeur OPNsense.

La solution Wi-Fi repose sur une borne Ubiquiti, configurée et administrée via le contrôleur UniFi Network. L'objectif principal était de déployer un Wi-Fi d'entreprise sécurisé, nécessitant une authentification individuelle des utilisateurs.

Cette authentification est assurée par un serveur FreeRADIUS, installé sur une machine virtuelle hébergée sur Proxmox, permettant la vérification des identifiants avant l'accès au réseau.

### **II – Présentation de la réalisation professionnelle**

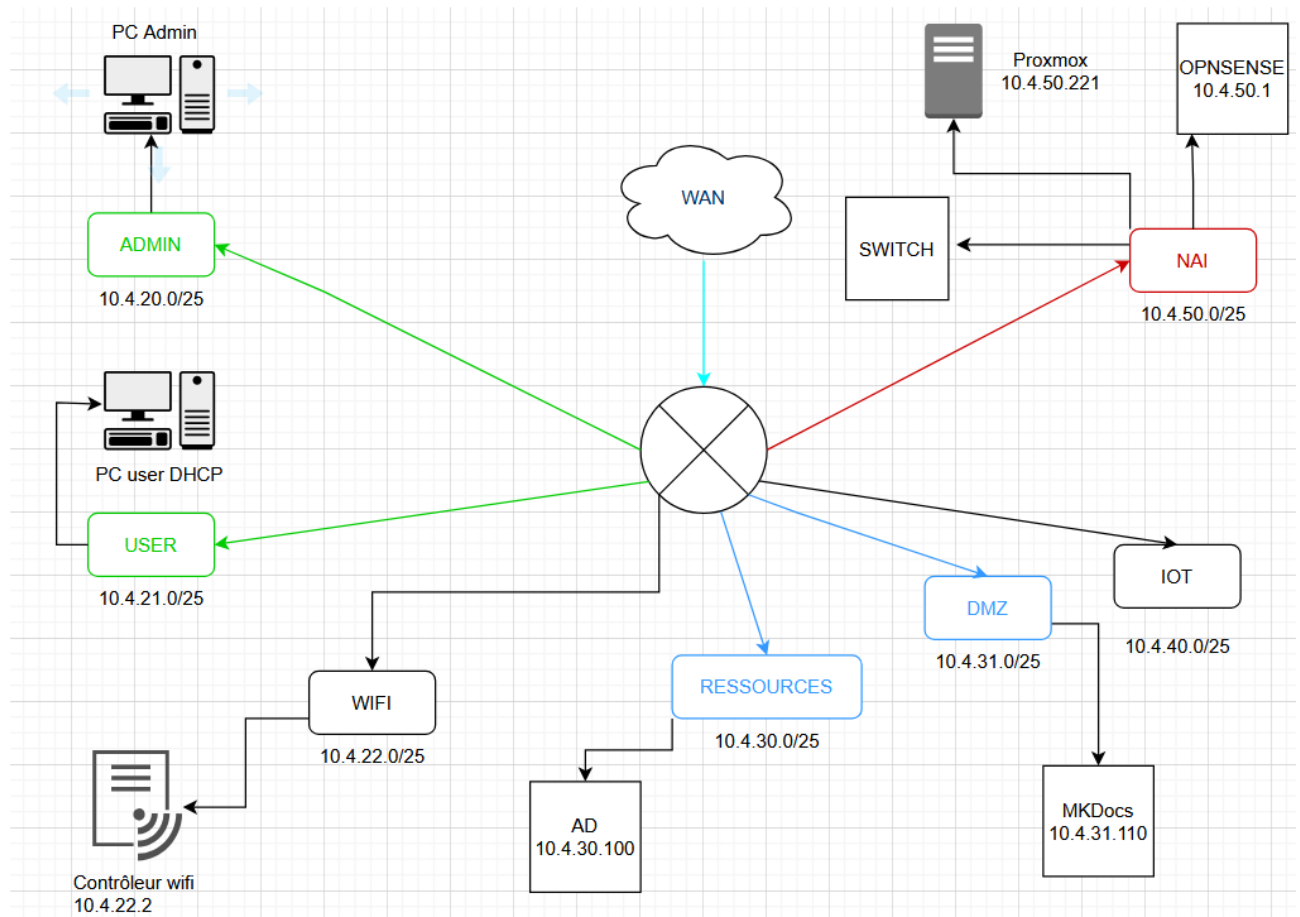
L'objectif de la réalisation était de mettre en place une authentification Wi-Fi à l'aide d'un serveur FreeRADIUS. Ce système permet de sécuriser l'accès au réseau : seuls les utilisateurs enregistrés sont autorisés à se connecter, et toute tentative d'un utilisateur non reconnu est automatiquement refusée.

Pour que tous les éléments communiquent correctement, la borne Wi-Fi doit pouvoir joindre le serveur FreeRADIUS, et OPNsense doit laisser passer les flux nécessaires (ports 1812 et 1813).

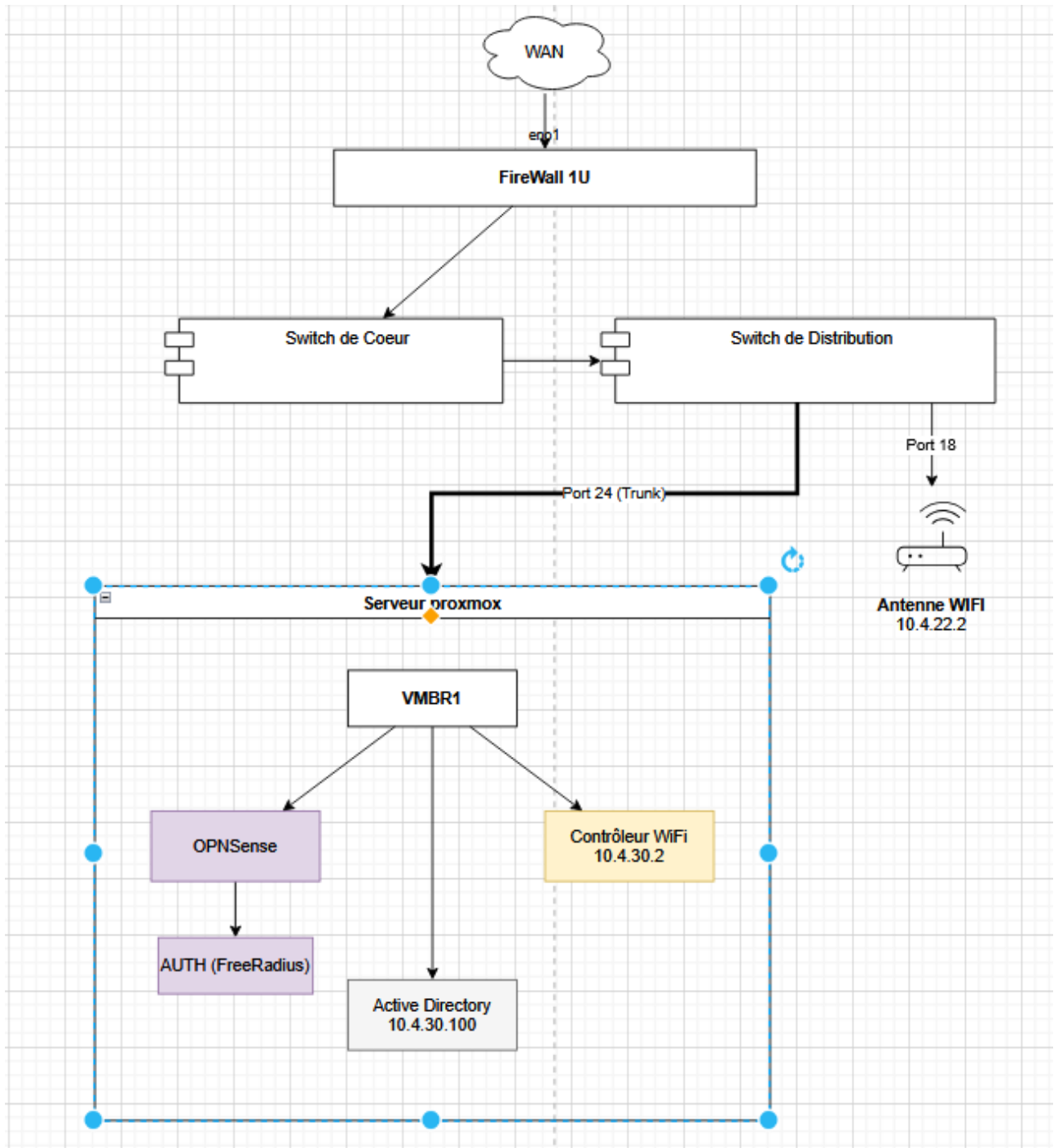
La solution mise en œuvre s'appuie donc sur :

- une borne Ubiquiti pour la diffusion du Wi-Fi,
- le contrôleur UniFi pour la gestion du SSID,
- un serveur FreeRADIUS pour l'authentification des utilisateurs,
- OPNsense pour la gestion des VLAN et du firewall,
- une machine virtuelle sous Proxmox pour héberger les services.

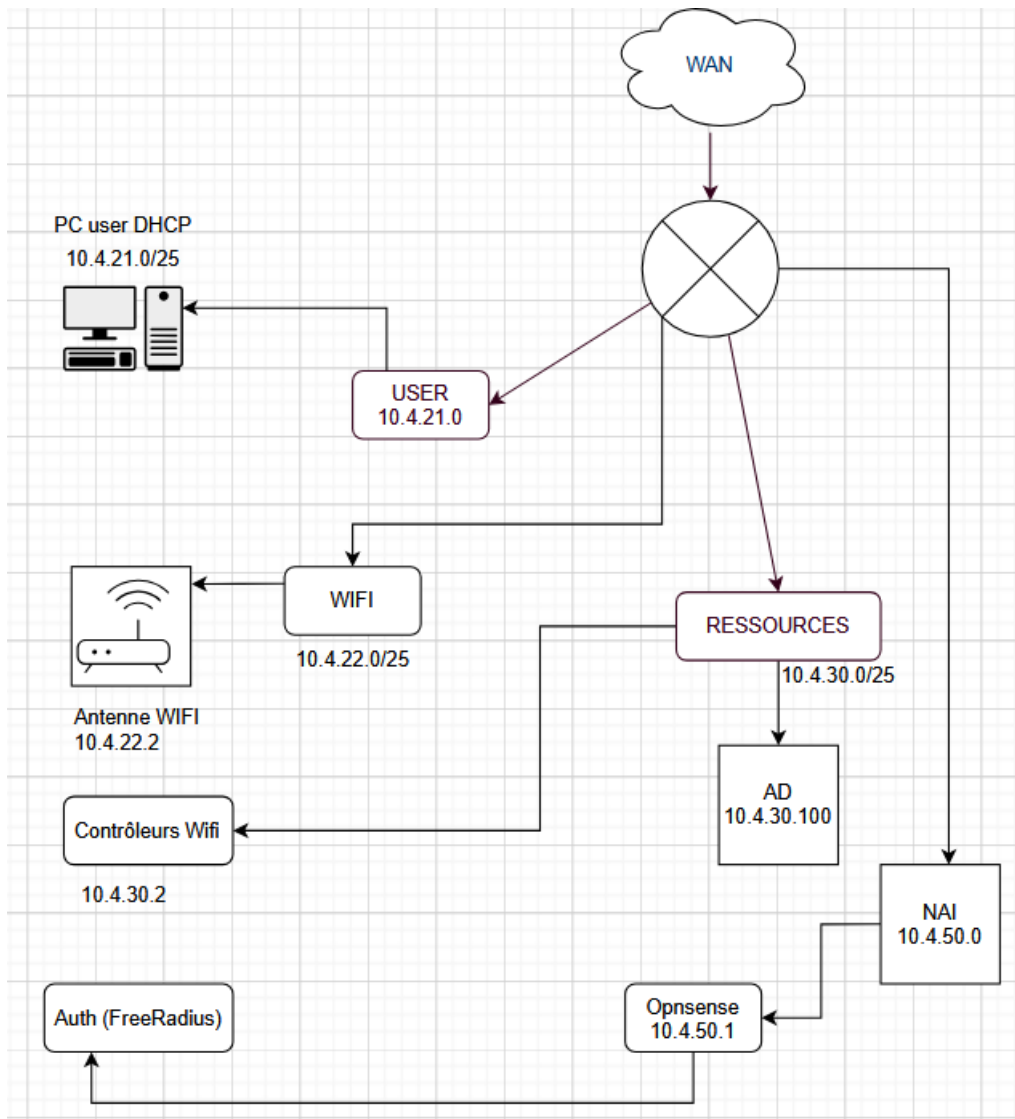
### III – Schéma logique global de l'infrastructure



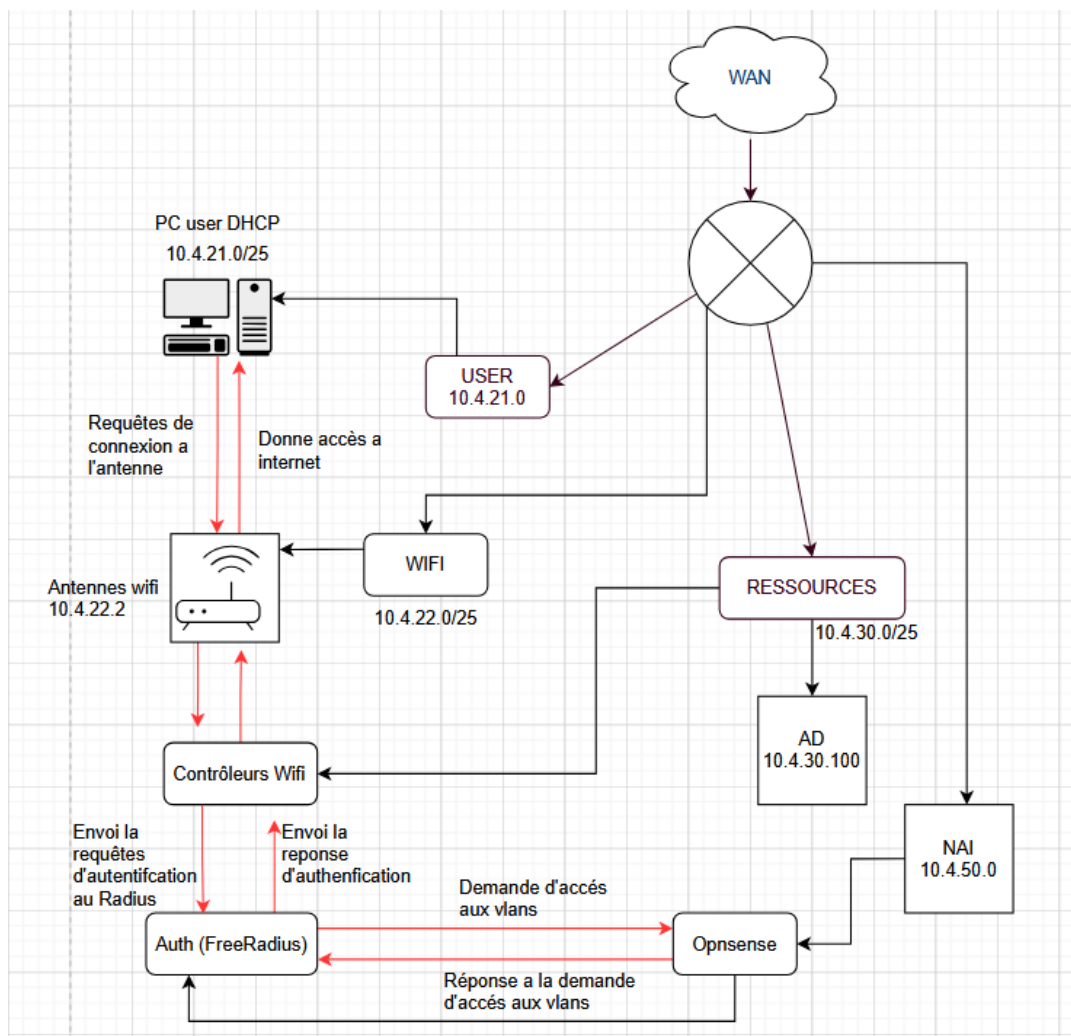
#### IV – Schéma physique de l'infrastructure



## V – Parties prenantes du projet



## VI – Schéma de flux simplifié et explication



1. Un utilisateur tente de se connecter au SSID Wi-Fi.
2. La borne Ubiquiti transmet la requête d'authentification au serveur FreeRADIUS.
3. FreeRADIUS vérifie si l'utilisateur existe et si le mot de passe est correct.
4. Si l'authentification est validée, l'accès au réseau Wi-Fi est autorisé dans le vlan User.
5. Sinon, l'accès est refusé et la connexion ne s'établit pas.

Flux réseau utilisés :

- Wi-Fi → Borne : 802.1X
- Borne → FreeRADIUS : UDP 1812/1813
- FreeRADIUS → OPNsense : routage inter-VLAN

## VII – Étapes du projet

### 1. Installation de FreeRADIUS sur Proxmox

Une machine virtuelle a été créée sur Proxmox pour installer le serveur FreeRADIUS. Ce serveur sert à vérifier les identifiants des utilisateurs Wi-Fi.

### 2. Création des utilisateurs RADIUS

Les utilisateurs autorisés ont été ajoutés dans FreeRADIUS avec un identifiant et un mot de passe. Les utilisateurs non enregistrés ne peuvent pas se connecter.

### 3. Configuration du switch et du VLAN Wi-Fi

Le switch a été configuré avec un VLAN dédié au Wi-Fi afin de séparer le réseau sans fil du reste du réseau.

#### 4. Installation et adoption de la borne Wi-Fi Ubiquiti

La borne Wi-Fi a été installée puis adoptée dans l'interface UniFi pour permettre sa gestion centralisée.

#### 5. Création du Wi-Fi entreprise avec authentification

Un SSID entreprise a été créé dans UniFi en WPA2/WPA3-Enterprise avec FreeRADIUS.

#### 6. Tests d'authentification avec différents comptes (valides / invalides)

### **VIII – Productions réalisées**

- Un Wi-Fi d'entreprise sécurisé avec authentification RADIUS
- Un serveur FreeRADIUS opérationnel
- Un SSID configuré en Enterprise dans UniFi
- Un VLAN Wi-Fi fonctionnel
- Des règles firewall structurées dans OPNsense