

Sriskandarajah Lavisian
Traore Koba
Singh Manjot
Damba Aly
Sossoe Asiwome
GRP9

SAE 501 : Concevoir, Réaliser et Présenter une Solution Technique



Table des matières

1) Introduction à la Conception Technique.....	3
A) Définitions de la conception technique.....	3
Composants principaux :.....	3
B) Les différentes phases du processus de conception.....	3
C) Importance de la conception dans les réseaux et télécommunications.....	4
2) Nomenclature :.....	5
3) Élaboration du Cahier des Charges.....	6
4) Conception Conceptuelle.....	8
A) Création de solutions conceptuelles.....	8
B) Évaluation des différentes alternatives.....	9
C) Sélection d'une solution optimale.....	9
5) Conception Détaillée.....	10
Introduction aux termes essentiels:.....	10
6) Mise en oeuvre pratique.....	12
6.1 Configuration du réseau.....	12
6.2 Configuration du Point d'Accès TP-Link TL-MR100 et de pfsense.....	12
6.2.1 Mode de Fonctionnement.....	12
6.3 Configuration de pfSense pour gérer l'interface OPT1.....	14
6.3.1 Ajout d'une troisième interface réseau.....	14
6.3.2 Configurer le serveur DHCP pour OPT1.....	14
6.4 Choix du Type de Réseau Virtuel pour l'Infrastructure.....	16
6.4.1 Réseau Privé Hôte (Host-Only Network).....	16
6.4.2 Réseau Interne (Internal Network).....	16
6.5 Configuration du Pare-feu sur pfSense : Application de Règles pour le WAN et le LAN.....	18
6.5.1 Interface WAN (Internet).....	18
6.5.2 Interface LAN (Réseau local).....	19
6.6 Installation des composants.....	20
6.6.1 Installation et Configuration de MySQL et FreeRADIUS.....	20
6.6.1.1 Installation de MySQL.....	20
6.6.1.2 Installation de FreeRADIUS.....	20
6.6.2 Configuration de MySQL pour FreeRADIUS.....	21
6.6.3 Configuration de FreeRADIUS pour utiliser MySQL.....	21
6.6.4 Redémarrage de FreeRADIUS.....	21
6.6.5 Vérification du bon fonctionnement.....	21
6.6.6 Configuration et Vérification de FreeRADIUS avec MySQL.....	22
6.7 Configuration du Portail Captif sur pfSense avec FreeRADIUS.....	25
6.8 Poste de la secrétaire.....	29
7) Gestion de projet.....	32
8) Sécurité et Fiabilité.....	33
Sécurité.....	33
Fiabilité.....	40
9) Tests et Validation.....	40
10) Documentation Technique.....	42
Rédaction de manuel technique:.....	42

1) Introduction à la Conception Technique

A) Définitions de la conception technique

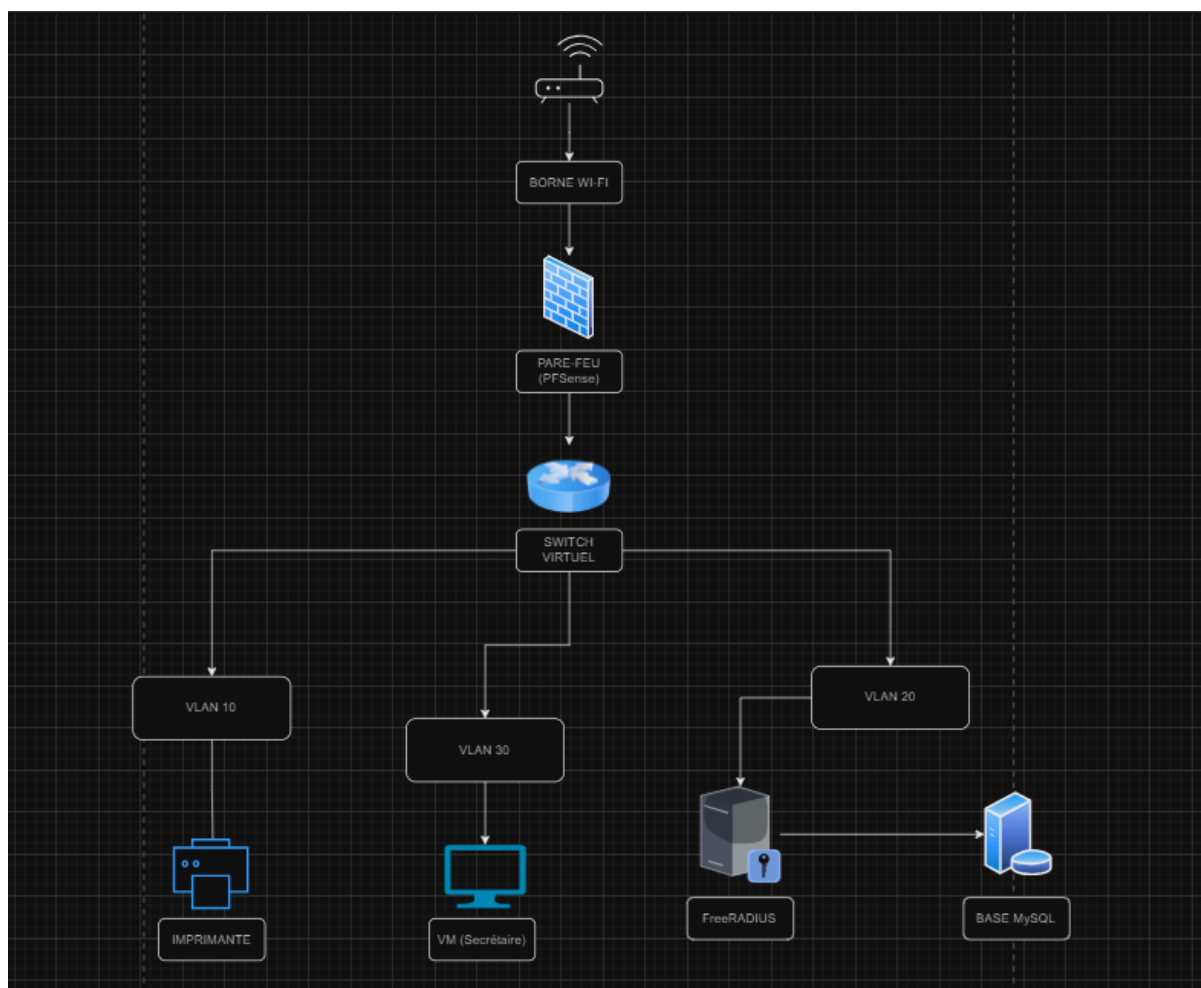
Dans le cadre de ce projet, la conception technique consiste à planifier et structurer de manière détaillée l'architecture du réseau Wi-Fi d'entreprise. Cette architecture repose sur plusieurs composants clés interconnectés pour garantir une connectivité sans fil sécurisée et performante.

Composants principaux :

- **Borne Wi-Fi (TP-Link)** : Fournit un accès sans fil au réseau et supporte les protocoles récents pour assurer une connexion sécurisée.
- **Pare-feu (PFSense)** : Filtre le trafic réseau entrant et sortant, gère les VLANs et inclut des fonctions avancées comme la détection d'intrusions.
- **Serveur RADIUS (FreeRADIUS)** : Authentifie les utilisateurs de manière centralisée en utilisant une base de données MySQL.
- **Base de données (MySQL)** : Stocke les informations d'authentification (identifiants, mots de passe) avec des politiques de sécurité robustes et gère efficacement les requêtes de FreeRADIUS.
- **VM (interface utilisateur)** : Fournit un outil pour créer et gérer les identifiants des utilisateurs.
- **Imprimante** : Intégrée au réseau, son accès est restreint aux utilisateurs

B) Les différentes phases du processus de conception.

Pour structurer et implémenter efficacement le réseau Wi-Fi , le processus de conception s'est articulé autour de plusieurs phases. Lors de la définition des besoins, nous avons identifié les composants nécessaires. Ensuite, pendant la conception préliminaire, plusieurs architectures réseau ont été étudiées, notamment en intégrant des VLANs via un switch virtuel pour isoler les services critiques.



C) Importance de la conception dans les réseaux et télécommunications.

Optimisation des performances :

- Une conception rigoureuse permet une gestion efficace de la bande passante et une réduction de la latence.
- Elle garantit une qualité de service adaptée aux besoins des utilisateurs.

Sécurité renforcée :

- Intégration de mécanismes robustes, comme l'authentification via RADIUS
- Protection des données et limitation des accès non autorisés.

Évolutivité :

- Prévoit l'ajout de nouveaux points d'accès ou périphériques sans modification majeure de l'infrastructure.
- Anticipe les besoins futurs grâce à une architecture flexible.

Fiabilité :

- Réduction des interruptions grâce à des mécanismes de redondance et de récupération rapide.
- Garantit un fonctionnement continu même en cas de panne.

Conformité réglementaire :

- Assure le respect des normes, notamment le RGPD pour la protection des données personnelles.
- Permet la conservation des logs pendant 6 mois conformément aux exigences légales.

Innovation et pérennité :

- Prépare l'infrastructure aux nouvelles technologies (WPA3, IoT).
- Encourage l'innovation en facilitant l'intégration de solutions avancées.

2) Nomenclature :

Élément	Description	Quantité	Fournisseur	Rôle/Fonction	Type
Ordinateur Hôte	Ordinateur Hôte exécutant les VMs	1	Dell/HP	Hébergement des VLANs et VMs	Physique
Pare-feu	Pare-feu (Virtual Appliance)	1	PfSense	Sécurisation et filtrage des flux	Virtuel
Windows	Système d'exploitation Windows 10	1	Microsoft	Expérience utilisateur	Virtuel
Serveur d'Authentification	Serveur RADIUS FreeRADIUS sur Linux	1	Open Source	Authentification des utilisateurs	Virtuel
Serveur de base de données	Serveur de base de données MySQL	1	Oracle/MySQL Community	Gestion des bases de données	Virtuel
Imprimante	Imprimante réseau (Wifi et filaire)	2	HP	Impression de documents	Physique
Point d'accès	Point d'accès Wi-Fi	1	TP-Link	Fournir une couverture Wi-Fi	Physique

	TP-Link MR100				
--	------------------	--	--	--	--

3) Élaboration du Cahier des Charges

1. Introduction

- **Contexte** : L'entreprise souhaite mettre en place une infrastructure Wi-Fi sécurisée pour ses employés et utilisateurs. Cette infrastructure doit inclure un point d'accès Wi-Fi, un serveur d'authentification RADIUS, et une base de données MySQL pour gérer les identifiants.
- **Objectif principal** : Fournir une connexion Wi-Fi sécurisée et gérer les utilisateurs via une interface centralisée tout en respectant les normes de sécurité et les réglementations (RGPD).

2. Présentation du Projet

- **Résumé** : Le projet consiste à concevoir une solution technique complète pour un accès sécurisé au Wi-Fi, en intégrant des technologies open source (PFSense, FreeRADIUS, MySQL) et des équipements compatibles
- **Description** :
 - Configuration d'un réseau Wi-Fi sécurisé.
 - Mise en place d'un système d'authentification centralisé.
 - Gestion simplifiée des utilisateurs grâce à une interface dédiée.

3. Besoins et Objectifs

- Objectifs techniques** :
 - Authentification des utilisateurs via FreeRADIUS.
 - Chiffrement sécurisé des communications via TLS.
 - Gestion des identifiants avec une interface utilisateur connectée à MySQL.
- Objectifs fonctionnels** :
 - Supporter jusqu'à 50 utilisateurs simultanés sans interruption.
 - Assurer une disponibilité réseau de 99 %.
 - Fournir des guides techniques pour la maintenance et la gestion des utilisateurs.
- Conformité** :
 - Se conformer au RGPD pour la gestion des données personnelles.

4. Périmètre

1. **Infrastructure à déployer :**
 - Pare-feu PFSense pour sécuriser le trafic réseau.
 - Serveur RADIUS (FreeRADIUS) pour gérer l'authentification.
 - Base de données MySQL pour stocker les identifiants.
2. **Wi-Fi sécurisé :**
 - Gestion centralisée des utilisateurs et des autorisations.
3. **Documentation :**
 - Fournir des guides pour l'installation, la configuration et le dépannage.
 - Former l'équipe IT à l'utilisation et la maintenance de la solution.

5. Contraintes

1. **Techniques :**
 - Utilisation de machines virtuelles hébergées sur des PC existants.
 - Compatibilité des équipements réseau avec FreeRADIUS.
2. **Organisationnelles :**
 - Installation sans interruption des services réseau existants.
 - Prévoir une phase de tests avant la mise en production.
3. **Réglementaires :**
 - Conformité au RGPD pour la gestion des données personnelles.
 - Conservation des logs d'accès pendant six mois.

6. Spécifications Fonctionnelles et Techniques

1. **Fonctionnalités principales :**
 - Interface pour créer et gérer les identifiants des utilisateurs.
 - Authentification sécurisée via RADIUS.
 - Journal des connexions pour un suivi.
2. **Spécifications techniques :**
 - **Pare-feu** : Filtrage du trafic et gestion des VLANs avec PFSense.
 - **Base de données** : MySQL pour gérer jusqu'à 50 utilisateurs simultanés.
 - **Sécurité** : Chiffrement TLS et stockage sécurisé des identifiants.

7. Livrables

1. **Techniques :**
 - Configurations des VMs (PFSense, FreeRADIUS, MySQL).
 - Scripts SQL pour la gestion des utilisateurs.
 - Plan d'adressage réseau.
2. **Documentations :**
 - Guide d'installation et de configuration.
 - Procédures de dépannage pour les problèmes courants.
 - Documentation des politiques de sécurité.

8. Gestion des Risques

- **Risques techniques :**
 - Incompatibilité des équipements avec WPA2-Enterprise.
 - Pannes matérielles ou interruptions réseau imprévues.
- **Mesures d'atténuation :**
 - Effectuer des tests approfondis avant la mise en production.
 - Prévoir des sauvegardes régulières et une documentation complète.

4) Conception Conceptuelle

A) Création de solutions conceptuelles

Le projet repose sur une architecture intégrant des composants en machines virtuelles (VM) et des équipements physiques. Les solutions conceptuelles explorées prennent en compte la configuration suivante :

- **Serveur RADIUS** : Déployé sur une machine virtuelle pour centraliser l'authentification des utilisateurs.
- **Pare-feu (PFSense)** : Hébergé sur une VM pour sécuriser le réseau et gérer le trafic entrant et sortant.
- **Base de données (MySQL)** : Installée sur une VM pour stocker les identifiants et les informations d'authentification.
- **Ordinateur physique** : Héberge les VMs et assure la gestion globale du système.
- **Point d'accès Wi-Fi** : Équipement physique fournissant une connexion Wi-Fi sécurisée aux utilisateurs.

Trois solutions conceptuelles ont été envisagées pour structurer cette architecture :

1. **Solution 1 : Infrastructure entièrement virtualisée**
 - Tous les composants (RADIUS, PFSense, MySQL) sont déployés sur des VMs.
 - L'ordinateur physique joue un rôle de serveur hôte pour les VMs.
 - Le point d'accès est connecté directement au réseau local.
2. **Solution 2 : Infrastructure semi-isolée**
 - Le serveur RADIUS et la base de données restent sur des VMs.
 - PFSense est isolé sur une VM dédiée pour une meilleure gestion des règles de pare-feu.
 - Le point d'accès est segmenté en VLANs via le pare-feu pour sécuriser les communications.
3. **Solution 3 : Infrastructure modulaire**
 - Les VMs (RADIUS, PFSense, MySQL) partagent les ressources de l'ordinateur physique, mais chaque composant est configuré pour fonctionner indépendamment.

B) Évaluation des différentes alternatives

Voici une évaluation des solutions proposées selon des critères clés : **coût**, **sécurité**, **performance**, **évolutivité**, et **simplicité de maintenance**.

Critères	Solution 1 : Virtualisée	Solution 2 : Semi-isolée	Solution 3 : Modulaire
Coût	Faible (uniquement VMs)	Modéré (segmentation VLANs)	Modéré
Sécurité	Bonne	Très bonne (isolation PFSense)	Bonne
Performance	Moyenne (ressources partagées)	Bonne	Bonne
Évolutivité	Très bonne (ajout facile de VMs)	Bonne	Bonne
Maintenance	Facile	Moyennement complexe	Moyenne

C) Sélection d'une solution optimale

La **solution 2 : Infrastructure semi-isolée** est retenue comme solution optimale pour les raisons suivantes :

1. **Sécurité renforcée** : L'isolation de PFSense sur une VM dédiée permet un contrôle précis du trafic réseau et une meilleure gestion des VLANs.
2. **Performance équilibrée** : Chaque composant (RADIUS, PFSense, MySQL) est hébergé sur une VM distincte, réduisant les conflits de ressources.
3. **Évolutivité et modularité** : La solution permet d'ajouter de nouveaux points d'accès ou utilisateurs sans impact sur les performances globales.
4. **Coût maîtrisé** : L'utilisation de machines virtuelles limite les dépenses liées à l'achat de matériel supplémentaire.

5) Conception Détaillée

Après une analyse rigoureuse des solutions disponibles pour réaliser notre projet, nous avons sélectionné plusieurs outils. Le serveur RADIUS sera mis en place à l'aide de FreeRadius, la base de données sera gérée par MySQL, et le pare-feu sera assuré par Pfsense. De plus, nous utiliserons un point d'accès TP Link pour garantir la connectivité réseau. Le Tp Link représente un élément central dans chaque configuration, car il est systématiquement inclus dans notre architecture.

Introduction aux termes essentiels:

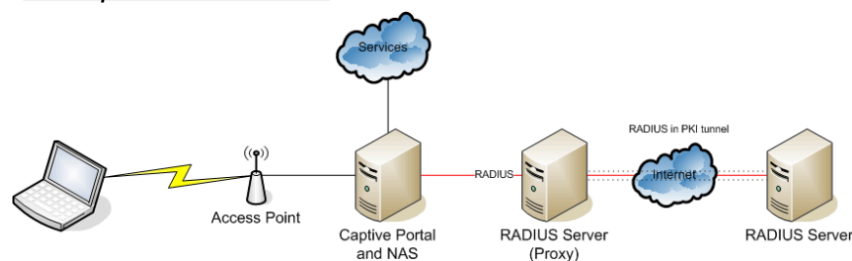
- **Serveur RADIUS**

Le Remote Authentication Dial-in User Service (RADIUS) est un protocole servant à gérer les accès distants sur un réseau. Il permet notamment d'authentifier les utilisateurs, de les autoriser, et de contrôler leurs comptes lorsqu'ils accèdent à un réseau distant, qu'il s'agisse de connexions filaires ou sans fil. Le serveur RADIUS, comme FreeRADIUS, joue un rôle clé dans l'administration des identifiants et des droits d'accès.

- **FreeRADIUS**

c'est une version libre et gratuite du protocole RADIUS. Cet outil est très prisé dans les environnements réseau pour son efficacité dans l'authentification et la gestion des utilisateurs. Son adaptabilité et sa modularité en font un choix pertinent pour diverses structures réseau.

exemple d'illustration:



- **Pare-feu**

Un pare-feu est un outil, qu'il soit matériel ou logiciel, qui sert à surveiller, filtrer et réguler les échanges de données entre un réseau interne et des réseaux externes (comme internet). Son but principal est d'assurer la sécurité en empêchant les accès non autorisés ou en limitant certains types de trafic réseau.

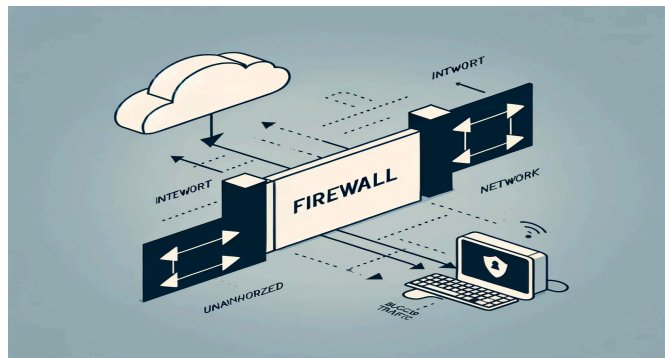
- **PfSense**

Il constitue une solution open source de pare-feu bâtie sur FreeBSD. Cet outil peut être utilisé comme un routeur et pare-feu au sein d'un réseau informatique. PfSense offre de nombreuses fonctionnalités telles que:

- Filtrage avancé du trafic
- Réseau privé Virtuel (VPN)
- Proxy et redirection de ports

il est couramment utilisé pour protéger les infrastructures réseau contre les menaces potentielles en filtrant les flux de données entrants et sortants.

exemple d'illustration:



- **Base de données MySQL**

Un système de base de données relationnel comme MySQL permet d'organiser et de stocker des informations sous forme de tables. MySQL est une solution open source souvent employée pour des applications web ou des besoins de gestion des données, grâce à sa robustesse et sa fiabilité.

- **Point d'accès sans fil**

Un point d'accès est un dispositif permettant aux appareils sans fil (ordinateurs, smartphones, etc..) de se connecter à un réseau filaire. Il agit comme un relais pour étendre la couverture du réseau et permettre la connectivité Wi-Fi. Les points d'accès peuvent être intégrés à d'autres équipements, comme des routeurs, ou fonctionner de manière indépendante.

exemple d'illustration:



6) Mise en oeuvre pratique

Pour réaliser ce projet de manière économique et compacte, nous avons choisi une approche basée sur la virtualisation. Seul le point d'accès TP-Link est un dispositif physique, connecté via un câble RJ45 à notre infrastructure. Les principaux composants sont hébergés sur VirtualBox.

6.1 Configuration du réseau

Pour mettre en place l'infrastructure, plusieurs éléments ont été configurés :

Interfaces réseau sur pfSense :

- **WAN** : Cette interface est connectée au routeur principal pour fournir l'accès à Internet.
 - **Mode** : Configuré en DHCP pour recevoir automatiquement une adresse IP dynamique.
 - **Utilité** : Permet de relier le réseau interne au monde extérieur tout en le sécurisant via pfSense.

- **LAN** : Interface dédiée au réseau interne des serveurs et des machines.
 - **Adresse IP** : 192.168.2.1/24 (statique).
 - **DHCP activé** : Plage d'adresses de 192.168.2.100 à 192.168.2.200.
 - **Utilité** : Fournit des adresses IP automatiques aux appareils connectés au LAN.

- **OPT1** : Connectée au point d'accès Wi-Fi TP-Link.
 - **Adresse IP** : 192.168.3.1/24 (statique).
 - **DHCP activé** : Plage d'adresses de 192.168.3.100 à 192.168.3.200.
 - **Utilité** : Permet la gestion des appareils connectés au réseau Wi-Fi.

6.2 Configuration du Point d'Accès TP-Link TL-MR100 et de pfsense

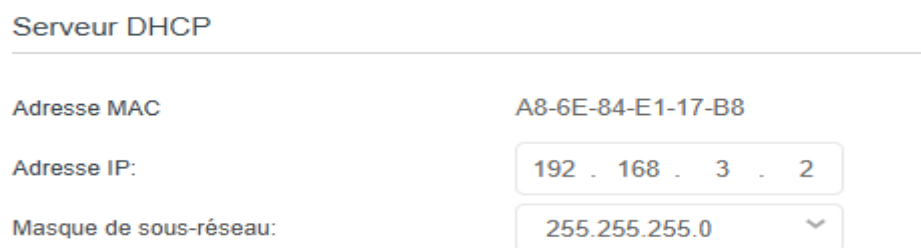
6.2.1 Mode de Fonctionnement

Nous avons configuré le point d'accès pour permettre aux utilisateurs de se connecter au réseau. Ce point d'accès ne fournit pas directement l'accès à Internet, car tout le trafic passe par pfSense pour être routé vers le WAN.

Voici les étapes principales de configuration :

- **Changer l'adresse IP :**

Par défaut, le TP-Link utilise l'adresse IP 192.168.1.1, ce qui peut provoquer des conflits avec d'autres équipements. En attribuant l'adresse 192.168.3.2, nous intégrons le point d'accès au sous-réseau dédié au Wi-Fi (192.168.3.0/24). Cette modification garantit une communication fluide entre le point d'accès et le pfSense:



Serveur DHCP

Adresse MAC: A8-6E-84-E1-17-B8

Adresse IP: 192 . 168 . 3 . 2

Masque de sous-réseau: 255.255.255.0

Une fois la modification effectuée, le point d'accès a été redémarré pour appliquer les changements.

- **Désactivation du serveur DHCP du TP-Link :**

Le serveur DHCP intégré au TP-Link a été désactivé pour éviter une gestion concurrente des adresses IP. pfSense devient l'unique gestionnaire des adresses IP, ce qui simplifie l'administration du réseau et renforce la sécurité.

DHCP: ☐ Activer

- **Désactiver le chiffrement WPA :**

Le chiffrement WPA a été désactivé temporairement pour faciliter les tests initiaux de connectivité et de configuration. Cela permet de s'assurer que les paramètres réseau de base fonctionnent correctement:



Nom du réseau (SSID): TP-Link_17B8 ☐ Masquer

Sécurité: WPA / WPA2 Personnel (rec...)

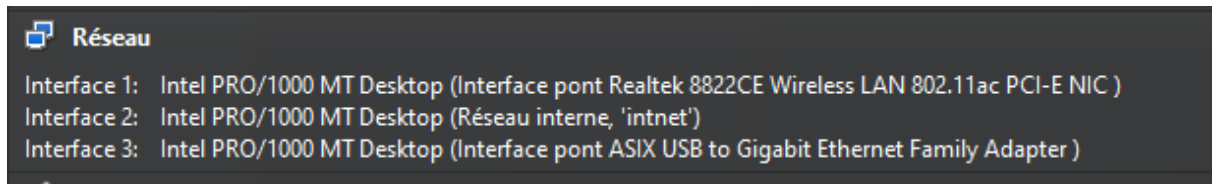
Version: Pas de sécurité

chiffrement: WPA / WPA2 Personnel

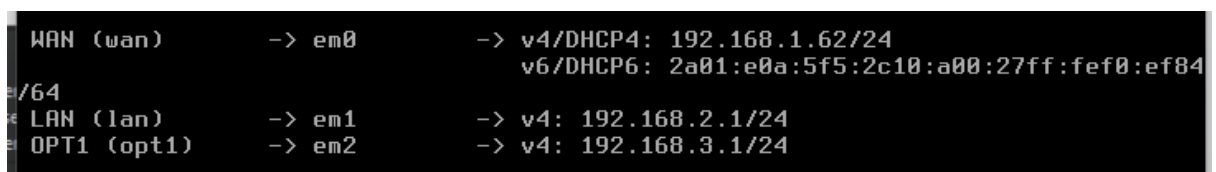
6.3 Configuration de pfSense pour gérer l'interface OPT1

6.3.1 Ajout d'une troisième interface réseau

Sur VirtualBox, une troisième interface réseau a été ajoutée pour la machine pfSense avec un accès en mode pont:

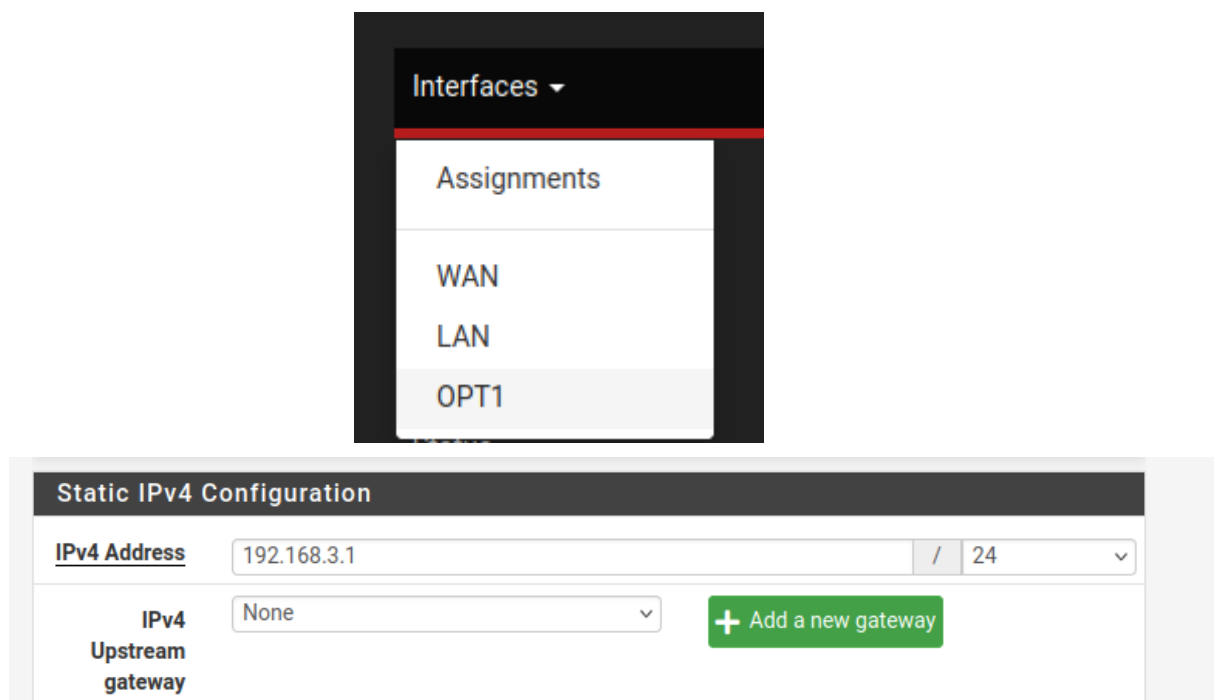


Cette interface, nommée OPT1, a été activée et configurée avec l'adresse IP 192.168.3.1, voir dans la capture ci-dessous:

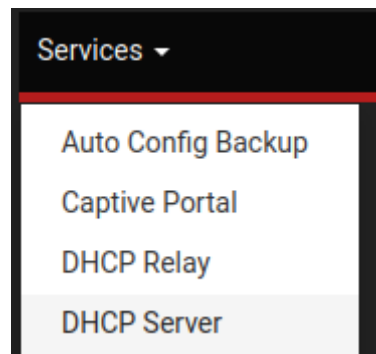


6.3.2 Configurer le serveur DHCP pour OPT1

Dans l'interface graphique de pfSense, nous avons vérifié que l'adresse IP de l'interface **OPT1** était correctement définie:



Nous avons activé le serveur DHCP pour le réseau 192.168.3.0/24 avec les paramètres suivants :



- **Plage d'adresses** : 192.168.3.100 à 192.168.3.200.

Available range	192.168.3.1 - 192.168.3.254	
Range	<input type="text" value="192.168.3.100"/>	<input type="text" value="192.168.3.200"/>
	From	To

Serveurs DNS :

- 192.168.3.1 (adresse locale de pfSense pour assurer la résolution DNS interne).
- 8.8.8.8 (serveur DNS public de Google pour la résolution externe).

DNS servers	<input type="text" value="192.168.3.1"/>
	<input type="text" value="8.8.8.8"/>

- **Passerelle** : 192.168.3.1 (pfSense).

Gateway	<input type="text" value="192.168.3.1"/>
----------------	--

6.4 Choix du Type de Réseau Virtuel pour l'Infrastructure

Lors de la mise en place de notre infrastructure réseau sur VirtualBox, nous avons analysé deux options principales pour connecter nos machines virtuelles : le réseau privé hôte et le réseau interne. Voici une présentation des deux options, leurs avantages et leurs inconvénients, ainsi que notre recommandation adaptée à nos besoins.

6.4.1 Réseau Privé Hôte (Host-Only Network)

Le réseau privé hôte permet une communication directe entre toutes les machines virtuelles (pfSense, serveur RADIUS/MySQL, machine d'impression, contrôleur d'imprimante) et la machine physique qui exécute VirtualBox (l'hôte). Ce type de réseau est idéal pour gérer les connexions internes entre les services, tout en maintenant un accès local pour la gestion et le dépannage.

Avantages :

- Permet la communication entre toutes les machines virtuelles et l'hôte.
- Simplifie la gestion et le dépannage grâce à l'accès direct depuis l'hôte.
- Configuration relativement simple pour des interactions entre les services.

Inconvénients :

- Aucune connexion directe à Internet. Cependant, une passerelle peut être configurée via pfSense pour permettre un accès contrôlé.

6.4.2 Réseau Interne (Internal Network)

Le réseau interne est une option plus isolée, permettant uniquement la communication entre les machines virtuelles sans accès à l'hôte ni à Internet. Cette configuration renforce la sécurité en limitant les connexions externes, mais complique la gestion et l'accès distant.

Avantages :

- Isolation complète des machines virtuelles, idéale pour des environnements de test sécurisés.
- Aucun risque d'exposition des services à l'hôte ou à Internet.

Inconvénients :

- Impossible d'accéder aux services depuis l'hôte, ce qui rend la gestion plus complexe.
- Nécessite une configuration supplémentaire via pfSense pour obtenir un accès Internet, ce qui peut alourdir l'installation.

Recommandation pour Notre Projet

Pour répondre aux besoins spécifiques de notre projet, nous avons choisi d'utiliser un réseau privé hôte. Cette configuration offre un bon équilibre entre accessibilité et isolation partielle :

- Communication facilitée : Toutes les machines virtuelles peuvent communiquer entre elles et avec l'hôte.
- Gestion simplifiée : L'accès depuis l'hôte permet de tester, configurer et gérer facilement les services (RADIUS, MySQL, etc.).
- Flexibilité : Bien que l'accès direct à Internet ne soit pas disponible par défaut, nous pouvons le configurer via pfSense pour contrôler les connexions externes.

6.5 Configuration du Pare-feu sur pfSense : Application de Règles pour le WAN et le LAN

Nous avons configuré le pare-feu de **pfSense** sur deux interfaces principales : **WAN** (Internet) et **LAN** (réseau interne). Ces règles nous permettent de **contrôler précisément le trafic autorisé ou bloqué** pour garantir la sécurité et le bon fonctionnement de notre infrastructure.

6.5.1 Interface WAN (Internet)

Sur l'interface WAN, nous avons appliqué des règles qui définissent ce qui peut entrer dans le réseau depuis Internet.

Voici ce que nous avons fait :






























1. Autoriser uniquement ce qui est nécessaire :

Par exemple, nous avons permis les connexions pour :

- **RADIUS** (ports 1812-1813) : pour les utilisateurs ou services qui doivent s'authentifier via notre serveur RADIUS.
- **HTTP/HTTPS** (ports 80 et 443) : pour permettre l'accès au portail captif ou à des services web spécifiques.

2. Tout bloquer par défaut :

La dernière règle bloque tout le trafic non explicitement autorisé par les règles précédentes. Ça garantit qu'aucune connexion non prévue ne peut pénétrer notre réseau:

Firewall / Rules / WAN											  
Floating WAN LAN OpenVPN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	*	*	WAN address	1812 - 1813	*	none		Radius	    
<input type="checkbox"/>	✓ 0/19 KiB	IPv4 TCP/UDP	*	*	WAN address	80 - 443	*	none		Portail captif	    
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Acces VPN GR9	    
<input type="checkbox"/>	✗ 0/28 KiB	IPv4+6 *	*	*	*	*	*	none		TOUT BLOQUE!!!!!!!	   
 Add  Add  Delete  Toggle  Copy  Save  Separator											

6.5.2 Interface LAN (Réseau local)

Sur l'interface LAN, nous avons défini des règles pour gérer le trafic à l'intérieur du réseau local et entre le LAN et l'extérieur (WAN).

Voici comment ça fonctionne :

1. Sécurisation de l'accès local à pfSense :

Une règle spéciale appelée Anti-Lockout Rule permet de toujours accéder à l'interface web de pfSense via HTTPS (port 443). Cela nous évite de nous bloquer nous-mêmes si une règle est mal configurée.

2. Gestion des services internes :

Nous avons permis l'accès à certains services critiques sur le réseau local, comme :

- MySQL (port 3306) : Pour les machines qui ont besoin d'accéder à la base de données.
- RADIUS (ports 1812-1813) : Pour les équipements locaux qui s'authentifient via le serveur RADIUS.

3. Blocage du trafic non autorisé vers l'extérieur :

Nous avons bloqué tout le trafic du LAN vers le WAN qui n'est pas explicitement autorisé.

Par exemple, nous empêchons certains appareils ou utilisateurs d'accéder à Internet s'ils n'en ont pas besoin.

4. Tout bloquer par défaut :

Comme pour l'interface WAN, une règle par défaut bloque tout trafic qui n'a pas été spécifiquement autorisé. Cela nous permet de garder un contrôle total sur le réseau:

Firewall / Rules / LAN

Floating

WAN

LAN

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/3.59 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	LAN address	1194 (OpenVPN)	*	none		VPN LAN	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN address	*	LAN address	3306	*	none		Mysql	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN address	*	LAN address	1812 - 1813	*	none		Radius	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN address	*	WAN address	*	*	none		Bloque LAN vers WAN	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	LAN address	*	LAN address	*	*	none		bloque trafic client à client	
<input type="checkbox"/>	0/916 B	IPv4 *	*	*	*	*	*	none		block default	

Add

Add

Delete

Toggle

Copy

Save

Separator

6.6 Installation des composants

6.6.1 Installation et Configuration de MySQL et FreeRADIUS

Avant de commencer l'installation de MySQL et de FreeRADIUS, nous avons effectué une mise à jour complète des paquets du système. Cette étape permet de garantir que toutes les dépendances nécessaires aux logiciels à installer soient à jour, réduisant ainsi les risques de conflits entre différentes versions de logiciels ou de bibliothèques.

6.6.1.1 Installation de MySQL

Nous avons installé MySQL Server car il est essentiel pour stocker les informations d'authentification des utilisateurs dans le cadre de l'utilisation de FreeRADIUS. MySQL est une base de données relationnelle largement utilisée qui permet de gérer de manière sécurisée et structurée les données relatives aux utilisateurs, comme les identifiants de connexion. Cela permet à FreeRADIUS de vérifier les informations des utilisateurs lors de leur tentative de connexion.

En installant MySQL, nous avons configuré son démarrage automatique pour nous assurer que le service soit toujours disponible lors de chaque démarrage du système. Nous avons également sécurisé l'installation de MySQL pour éviter toute exploitation malveillante, notamment en configurant un mot de passe fort pour l'utilisateur root et en supprimant les configurations par défaut qui ne sont pas sécurisées.

6.6.1.2 Installation de FreeRADIUS

FreeRADIUS a été installé car c'est un serveur d'authentification utilisé pour contrôler l'accès aux réseaux. FreeRADIUS est un outil clé dans un environnement où il est nécessaire de vérifier l'identité des utilisateurs avant de leur permettre d'accéder à des ressources sensibles, comme un réseau sans fil ou un accès à Internet via un portail captif.

FreeRADIUS peut fonctionner avec plusieurs types de bases de données pour stocker les informations des utilisateurs, mais dans notre cas, il est configuré pour utiliser MySQL. Cela nous permet de centraliser la gestion des utilisateurs dans une base de données relationnelle, facilitant ainsi leur gestion et l'intégration avec d'autres systèmes.

6.6.2 Configuration de MySQL pour FreeRADIUS

L'intégration de MySQL avec FreeRADIUS permet de stocker de manière sécurisée les informations des utilisateurs, telles que leurs noms d'utilisateur et mots de passe, dans une base de données centralisée. Cela permet de gérer facilement les utilisateurs et leurs droits d'accès, tout en permettant à FreeRADIUS de valider les informations d'authentification lors des tentatives de connexion. Nous avons donc configuré MySQL pour qu'il soit prêt à recevoir et stocker ces informations.

Cette configuration garantit que FreeRADIUS puisse accéder à la base de données, effectuer les requêtes nécessaires pour vérifier les informations d'identification et accorder ou refuser l'accès aux utilisateurs en fonction de leurs informations stockées.

6.6.3 Configuration de FreeRADIUS pour utiliser MySQL

La configuration de FreeRADIUS pour utiliser MySQL est importante, car elle permet à FreeRADIUS d'interagir avec la base de données afin de vérifier les informations d'identification des utilisateurs lors de l'authentification. En activant et en configurant le module SQL de FreeRADIUS, nous avons assuré que les données nécessaires à l'authentification des utilisateurs soient correctement extraites de la base de données MySQL chaque fois qu'un utilisateur tente de se connecter.

Cette étape est importante pour intégrer FreeRADIUS dans un environnement de gestion d'accès où les informations des utilisateurs sont déjà centralisées dans MySQL, ce qui facilite la gestion et l'évolutivité du système.

6.6.4 Redémarrage de FreeRADIUS

Le redémarrage de FreeRADIUS après avoir effectué les modifications dans sa configuration permet d'appliquer toutes les modifications effectuées et de s'assurer que le serveur fonctionne avec les paramètres les plus récents. Cela garantit que toutes les configurations liées à MySQL sont correctement prises en compte, et que FreeRADIUS est opérationnel avec ses nouvelles fonctionnalités.

6.6.5 Vérification du bon fonctionnement

Enfin, une fois la configuration terminée, il est essentiel de vérifier que FreeRADIUS fonctionne correctement avec MySQL. Pour ce faire, nous avons utilisé des outils de débogage pour examiner les logs détaillés de FreeRADIUS et nous assurer qu'il se connecte correctement à la base de données et que l'authentification fonctionne comme prévu.

6.6.6 Configuration et Vérification de FreeRADIUS avec MySQL

1. Fichier de configuration SQL :

Le fichier sql situé dans /etc/freeradius/3.0/mods-available/sql configure FreeRADIUS pour communiquer avec une base de données MySQL.

Voici, ci-dessous les paramètres importants :

```
root@koba-VirtualBox: /home/koba
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 2.9.3 /etc/freeradius/3.0/mods-available/sql

sql {
    # The sub-module to use to execute queries. This should match
    # the database you're attempting to connect to.
    #
    # * rlm_sql_mysql
    # * rlm_sql_mssql
    # * rlm_sql_oracle
    # * rlm_sql_postgresql
    # * rlm_sql_sqlite
    # * rlm_sql_null (log queries to disk)
    #
    driver = "rlm_sql_mysql"
    dialect = "mysql"
    server = "localhost"
    login = "radius"
    password = "Lost2004*"
    radius_db = "radius"

    #
    # Several drivers accept specific options, to set them, a
    # config section with the the name as the driver should be added
    # to the sql instance.
    #
    # Driver specific options are:
    #
    # sqlite {
    #     # Path to the sqlite database
    #     filename = "/tmp/freeradius.db"
    #
    #     # How long to wait for write locks on the database to be
    #     # released (in ms) before giving up.
    #     busy_timeout = 200
    # }
}

[ 269 lignes écrites ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier  ^C Pos. cur.
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller    ^T Orthograp. ^_ Aller liq.
```

Mot de passe : Lost2004*

Ce mot de passe respecte les exigences de sécurité MySQL (longueur minimale de 8 caractères avec majuscules, minuscules, chiffres et symboles).

2. Base de données MySQL pour FreeRADIUS

La table radcheck est une table clé dans la base de données MySQL utilisée par FreeRADIUS pour stocker les informations d'authentification des utilisateurs.

2.1 radcheck

Rôle principal : La table radcheck contient les informations d'authentification des utilisateurs. Elle permet à FreeRADIUS de vérifier les identifiants des utilisateurs lorsqu'ils tentent de se connecter à un service protégé par RADIUS (par exemple, un réseau Wi-Fi ou un VPN).

- Colonnes principales :
 - username : Nom d'utilisateur.
 - attribute : L'attribut utilisé pour l'authentification, généralement Cleartext-Password pour un mot de passe en texte clair.
 - op : L'opérateur d'authentification, habituellement :=, indiquant une affectation.
 - value : La valeur de l'attribut (par exemple, le mot de passe de l'utilisateur).

Test de l'authentification:

Nous allons vérifier la base de données grâce à notre configuration au fichier précédent

On utilise la commande SELECT * FROM radcheck:

```
mysql> USE radius;
Database changed
mysql> SELECT * FROM radcheck;
Empty set (0,00 sec)

mysql> show database;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'database' at line 1
mysql> INSERT INTO radcheck (username, attribute, op, value)
  -> VALUES ('radius', 'Cleartext-Password', ':=', 'Lost2004*');
Query OK, 1 row affected (0,01 sec)

mysql> show database;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'database' at line 1
mysql> USE radius;
Database changed
mysql> SELECT * FROM radcheck;
+----+-----+-----+-----+-----+
| id | username | attribute          | op | value      |
+----+-----+-----+-----+-----+
| 1  | radius   | Cleartext-Password | := | Lost2004*  |
+----+-----+-----+-----+-----+
1 row in set (0,00 sec)

mysql>
```


Test utilisateur avec radtest:

Si l'utilisateur est dans la base de données radcheck :

```
root@koba-VirtualBox:/home/koba# radtest radius Lost2004* 127.0.0.1 0 testing123
Sent Access-Request Id 141 from 0.0.0.0:59532 to 127.0.0.1:1812 length 76
  User-Name = "radius"
  User-Password = "Lost2004*"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "Lost2004*"
Received Access-Accept Id 141 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
root@koba-VirtualBox:/home/koba#
```

Réponse : Access-Accept.

Sinon, si l'utilisateur n'est pas trouvé :

```
root@koba-VirtualBox:/home/koba# radtest radiu Lost2004* 127.0.0.1 0 testing123
Sent Access-Request Id 177 from 0.0.0.0:41196 to 127.0.0.1:1812 length 75
  User-Name = "radiu"
  User-Password = "Lost2004*"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "Lost2004*"
Received Access-Reject Id 177 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
(0) -: Expected Access-Accept got Access-Reject
root@koba-VirtualBox:/home/koba#
```

Réponse : Access-Reject.

6.7 Configuration du Portail Captif sur pfSense avec FreeRADIUS

Le portail captif est une interface qui oblige les utilisateurs à s'authentifier avant d'accéder au réseau. Dans cette configuration, pfSense utilise FreeRADIUS comme backend d'authentification pour valider les identifiants des utilisateurs.

1. Configuration de FreeRADIUS :

FreeRADIUS est configuré pour vérifier les identifiants des utilisateurs via une base de données MySQL. Les informations d'authentification, comme le nom d'utilisateur et le mot de passe, sont stockées dans la table radcheck.

Par exemple, pour l'utilisateur radius avec le mot de passe Lost2004*, une entrée est ajoutée dans la table radcheck.

FreeRADIUS est également configuré pour accepter pfSense comme client en définissant son adresse IP (par exemple, 192.168.56.102) et un secret partagé (ici Mbozu13*) dans le fichier `/etc/freeradius/3.0/clients.conf`. Ce secret partagé garantit que pfSense est autorisé à interagir avec FreeRADIUS.

2. Liaison avec pfSense :

Dans pfSense, le portail captif est activé sur une interface réseau (par exemple, LAN ou Wi-Fi). Dans les paramètres du portail captif, FreeRADIUS est configuré comme méthode d'authentification. Cela permet à pfSense de transmettre les identifiants saisis par les utilisateurs au serveur FreeRADIUS pour vérification.

Le secret partagé (Mbozu13*) est utilisé pour sécuriser la communication entre pfSense et FreeRADIUS. Une fois configuré, pfSense redirige automatiquement les utilisateurs vers une page de connexion où ils saisissent leurs identifiants. Si ceux-ci sont valides, l'accès réseau est accordé.

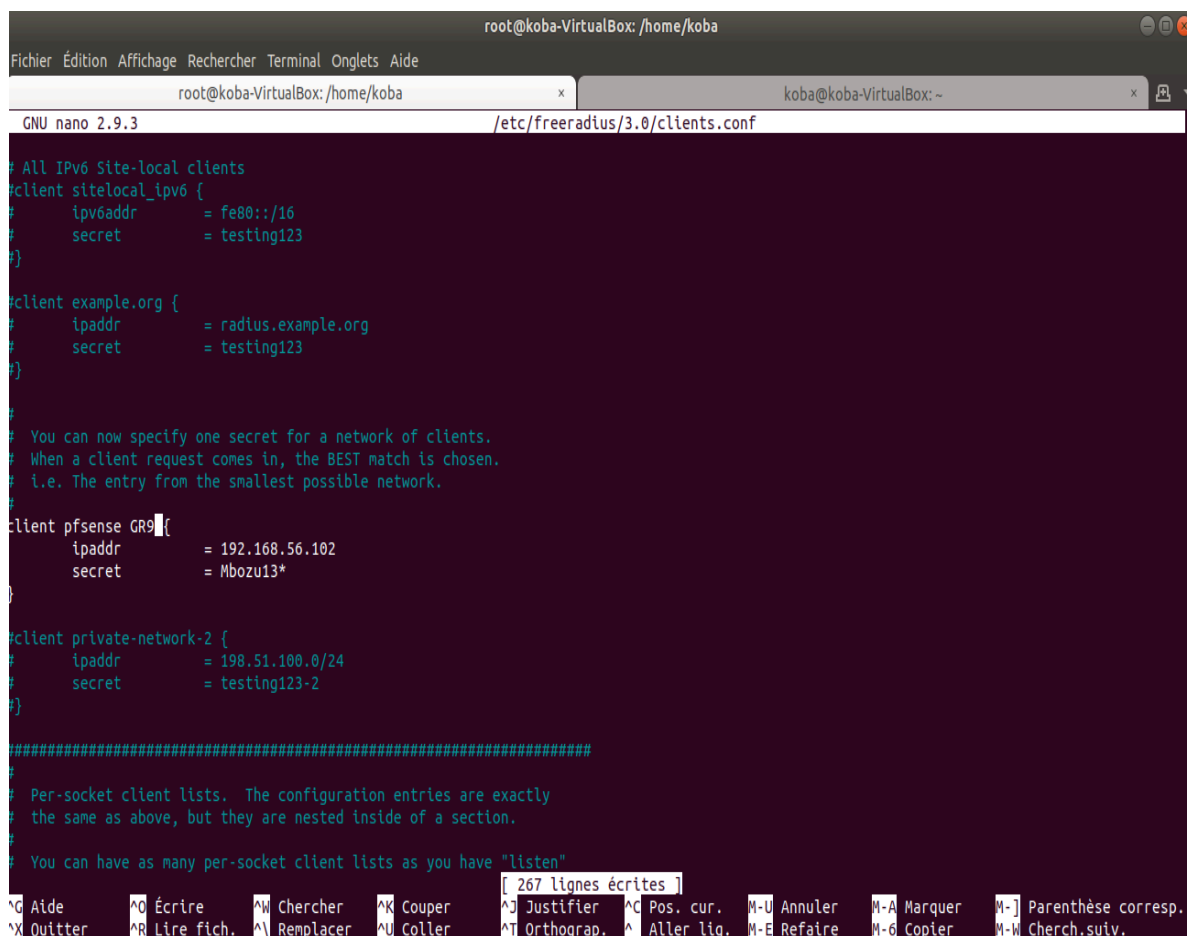
3. Validation et logs :

Les tentatives de connexion réussies ou échouées peuvent être suivies dans les journaux de pfSense et FreeRADIUS. Les erreurs, comme une configuration incorrecte ou des identifiants invalides, apparaissent dans ces logs, facilitant le dépannage.

Voici la configuration de FreeRadius:

On se rend dans le fichier `/etc/freeradius/3.0/clients.conf`:

- Ce fichier est utilisé pour définir les clients (comme pfSense) autorisés à se connecter au serveur FreeRADIUS.
- Chaque client est défini par un **nom** (client pfsense GR9), une **adresse IP** (ici 192.168.56.102), et un **secret partagé** (Mbozu13*).
- Le client pfsense GR9 est spécifiquement configuré pour qu'il puisse interagir avec le serveur FreeRADIUS.
- Le secret partagé (Mbozu13*) permet d'établir une connexion sécurisée entre pfSense et FreeRADIUS.



```
root@koba-VirtualBox: /home/koba
Fichier Édition Affichage Rechercher Terminal Onglets Aide
root@koba-VirtualBox: /home/koba x koba@koba-VirtualBox: ~ x
GNU nano 2.9.3 /etc/freeradius/3.0/clients.conf

# All IPv6 Site-local clients
client sitelocal_ipv6 {
#   ipv6addr    = fe80::/16
#   secret      = testing123
}

client example.org {
#   ipaddr      = radius.example.org
#   secret      = testing123
}

#
# You can now specify one secret for a network of clients.
# When a client request comes in, the BEST match is chosen.
# i.e. The entry from the smallest possible network.
#
client pfsense GR9 {
#   ipaddr      = 192.168.56.102
#   secret      = Mbozu13*
}

client private-network-2 {
#   ipaddr      = 198.51.100.0/24
#   secret      = testing123-2
}

#####
#
# Per-socket client lists. The configuration entries are exactly
# the same as above, but they are nested inside of a section.
#
# You can have as many per-socket client lists as you have "listen"

[ 267 lignes écrites ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier ^C Pos. cur. ^U Annuler   ^-A Marquer  ^-] Parenthèse corresp.
^X Quitter   ^R Lire fich.^_ Remplacer ^U Coller    ^T Orthograp.^_ Aller lig. ^-E Refaire  ^-6 Copier   ^-M Cherch.suiv.
```

Configuration de pfSense pour utiliser FreeRADIUS comme serveur d'authentification:

1. **Paramètres du serveur d'authentification dans pfSense :**
 - **Descriptive name** : Un nom descriptif, ici "Radius GR9", pour identifier le serveur.
 - **Hostname or IP address** : L'adresse IP du serveur FreeRADIUS (192.168.56.104 dans cet exemple).
 - **Shared Secret** : Le même secret partagé que celui configuré dans le fichier `clients.conf` de FreeRADIUS (Mbozu13*).
2. **Protocole** :
 - Le protocole d'authentification est défini comme **MS-CHAPv2**, souvent utilisé pour les connexions sécurisées.
3. **Ports utilisés** :
 - **1812** pour l'authentification.
 - **1813** pour l'accounting (journalisation des connexions).
4. **Services** : pfSense est configuré pour utiliser le serveur FreeRADIUS à la fois pour l'authentification et la gestion des sessions des utilisateurs.

The screenshot shows the pfSense web interface for configuring an authentication server. The browser address bar displays `https://192.168.56.102/system_authservers.php?act=edit&id=0`. The navigation breadcrumb is `System / User Manager / Authentication Servers / Edit`. The main menu includes `Users`, `Groups`, `Settings`, and `Authentication Servers`, with the last one being the active tab. The configuration form is titled **Server Settings** and includes the following fields:

- Descriptive name**: Text input containing "Radius GR9".
- Type**: Dropdown menu set to "RADIUS".

Below this is the **RADIUS Server Settings** section with the following fields:

- Protocol**: Dropdown menu set to "MS-CHAPv2".
- Hostname or IP address**: Text input containing "192.168.56.104".
- Shared Secret**: Password input field with masked characters.
- Services offered**: Dropdown menu set to "Authentication and Accounting".
- Authentication port**: Spin box set to "1812".
- Accounting port**: Spin box set to "1813".
- Authentication Timeout**: Spin box set to "5". Below this field is a note: "This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token."
- RADIUS NAS IP Attribute**: Dropdown menu set to "LAN - 192.168.56.102".

Configuration du Portail Captif dans pfSense

1. Activation du portail captif :

- "Enable Captive Portal" est cochée pour activer cette fonctionnalité sur pfSense.

2. Description :

- Une brève description est ajoutée pour identifier l'objectif du portail captif, ici "Wifi sécurisé par nos soins".

3. Interfaces réseau :

- Les interfaces WAN et LAN sont sélectionnées. Cela signifie que le portail captif contrôlera les connexions des utilisateurs sur ces interfaces.

4. Liaison avec FreeRADIUS :

- Dans cette configuration, le portail captif est configuré pour rediriger les utilisateurs vers une page de connexion, où ils doivent entrer leurs identifiants. Ces identifiants sont ensuite validés via le serveur FreeRADIUS.

The screenshot shows the pfSense web interface. At the top is the navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this is a breadcrumb trail: Services / Captive Portal / Groupe9 / Configuration. To the right of the breadcrumb are icons for refresh, save, undo, redo, and help. Below the breadcrumb is a horizontal tab bar with the following tabs: Configuration (active), MACs, Allowed IP Addresses, Allowed Hostnames, Vouchers, High Availability, and File Manager. The main content area is titled "Captive Portal Configuration". It contains three sections: 1. "Enable" with a checkbox labeled "Enable Captive Portal" which is checked. 2. "Description" with a text input field containing "Wifi sécurisé par nos soins :)" and a note below it stating "A description may be entered here for administrative reference (not parsed)." 3. "Interfaces" with a multi-select dropdown menu showing "WAN" and "LAN" selected. Below the dropdown is the instruction "Select the interface(s) to enable for captive portal."

https://192.168.56.102/services_captiveportal.php?zone=groupe9

Authentication

Authentication Method Use RADIUS MAC Authentication

Select an Authentication Method to use for this zone. One method must be selected.

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server Radius GR9

You can add a remote authentication server in the [User Manager](#).

NAS Identifier

Specify a NAS identifier to override the default value (CaptivePortal-groupe9)

Reauthenticate Users ☒ Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

RADIUS MAC Secret Mbozu13*

RADIUS MAC will automatically try to authenticate devices with their MAC address as username, and the password entered below as password. Devices will still need to make one HTTP request to get connected, through.

Login page Fallback ☒ Display the login page as fallback if RADIUS MAC authentication failed.

When enabled, users will be redirected to the captive portal login page when RADIUS MAC authentication failed.

Session timeout ☐ Use RADIUS Session-Timeout attributes

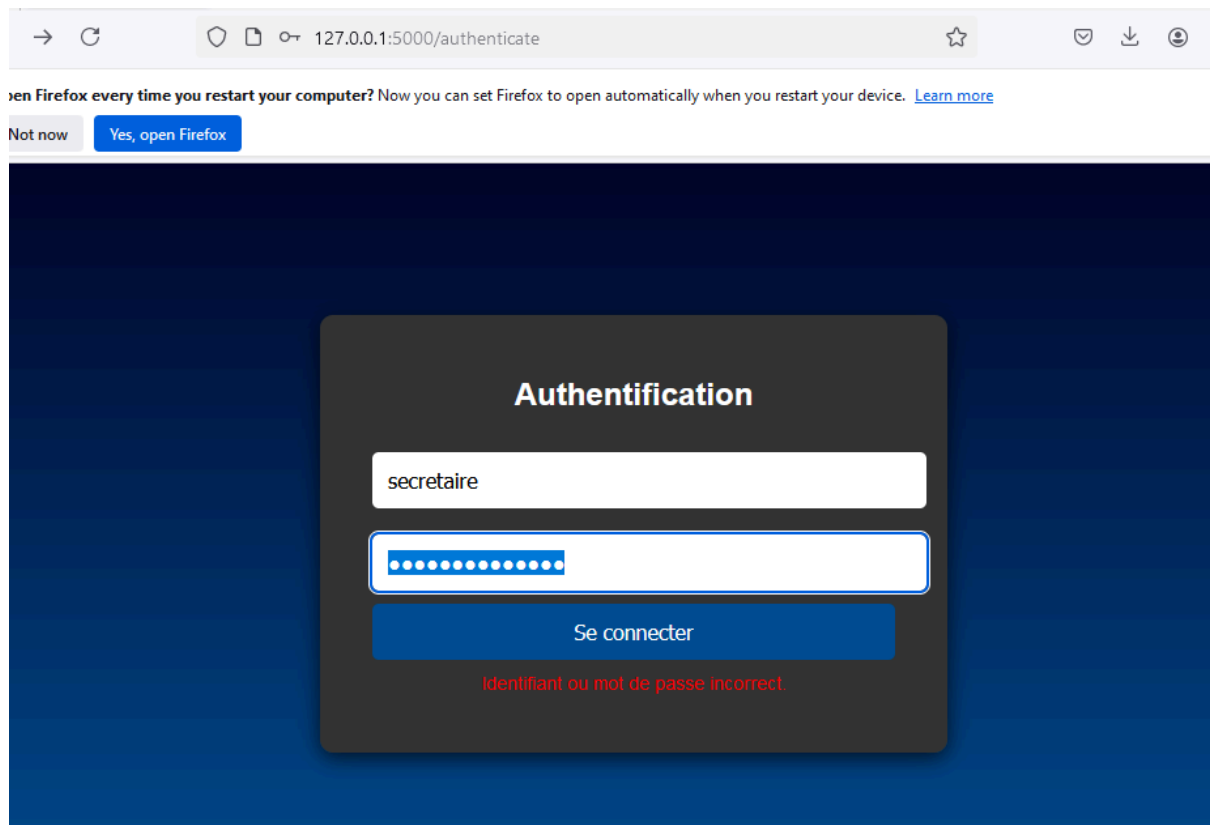
When enabled, clients will be disconnected after the amount of time retrieved from the RADIUS Session-Timeout attribute.

Traffic quota ☐ Use RADIUS pfSense-Max-Total-Octets attribute

When enabled, clients will be disconnected after exceeding the amount of traffic, inclusive of both downloads and uploads, retrieved from the RADIUS

6.8 Poste de la secrétaire

Un utilisateur spécifique a été créé pour la secrétaire dans la base de données **RADIUS**. Cet utilisateur dispose des privilèges nécessaires pour accéder et gérer les données via une application web développée en **Python**.



L'application web, hébergée localement, offre des fonctionnalités telles que l'ajout, la modification et la suppression d'utilisateurs dans la base de données **RADIUS**. Ces actions sont directement répercutées grâce aux privilèges accordés à l'utilisateur secrétaire.

Liste des utilisateurs			
ID	Identifiant	Mot de passe	Actions
2	Koba	koba@GP9*	Modifier Supprimer Imprimer
5	mario	mario@GP9*	Modifier Supprimer Imprimer
10	rio_rar	rar@-7	Modifier Supprimer Imprimer
11	mario_mario	mario@-6	Modifier Supprimer Imprimer

Ajouter un utilisateur

Pour simplifier l'accès, le poste de la secrétaire a été configuré de manière à ne pas passer par le portail captif. Cela a été réalisé en :

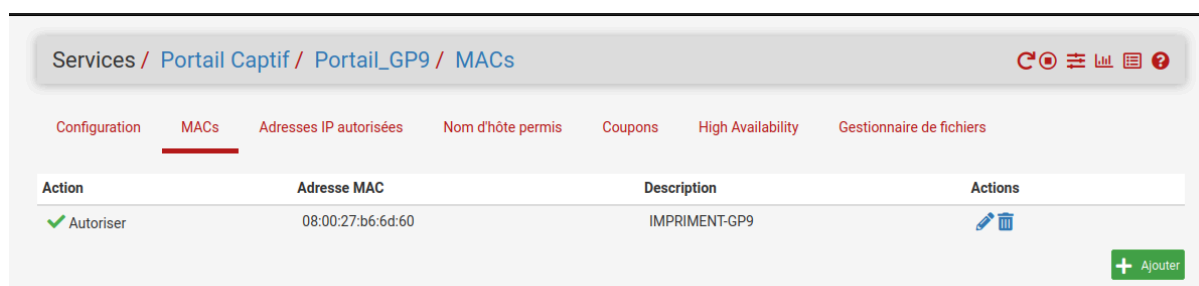
- Fixant l'adresse IP de son poste dans le sous-réseau.
- Ajoutant son adresse IP dans la liste des appareils exemptés du portail captif.




Une imprimante a été configurée pour fonctionner sans authentification sur le portail captif, contrairement aux autres terminaux qui doivent s'authentifier via le portail pour accéder au réseau.

Pour ce faire, deux actions spécifiques ont été réalisées :

1. Ajout dans la liste des équipements autorisés du portail captif :

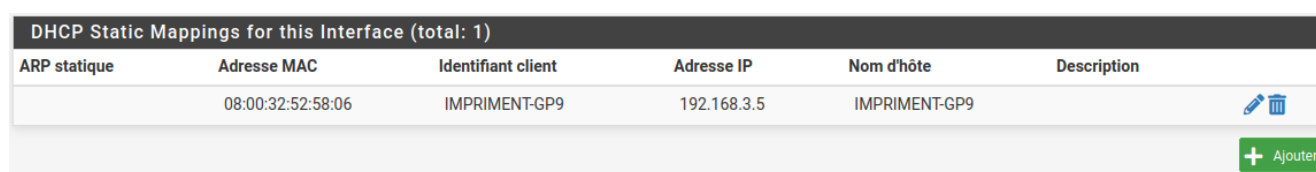
L'adresse MAC de l'imprimante a été ajoutée à la liste des appareils autorisés, permettant ainsi à l'imprimante de contourner les restrictions imposées par le portail captif.






Services / Portail Captif / Portail_GP9 / MACs			
Configuration	MACs	Adresses IP autorisées	Nom d'hôte permis
Coupons	High Availability	Gestionnaire de fichiers	
Action	Adresse MAC	Description	Actions
✓ Autoriser	08:00:27:b6:6d:60	IMPRIMENT-GP9	 
			

2. Mappage de l'adresse IP dans les configurations DHCP :

Une adresse IP fixe a été assignée à l'imprimante via un mappage spécifique dans les configurations DHCP. Cela garantit que l'imprimante conserve toujours la même adresse IP et simplifie son identification dans le réseau.



DHCP Static Mappings for this Interface (total: 1)					
ARP statique	Adresse MAC	Identifiant client	Adresse IP	Nom d'hôte	Description
	08:00:32:52:58:06	IMPRIMENT-GP9	192.168.3.5	IMPRIMENT-GP9	 
					

Ces configurations ont été mises en place à titre exceptionnel pour répondre aux besoins spécifiques de l'imprimante. Contrairement aux autres terminaux, qui doivent passer par le portail captif pour s'authentifier, l'imprimante bénéficie de cette exemption afin de fonctionner de manière autonome et sans interruption.

7) Gestion de projet

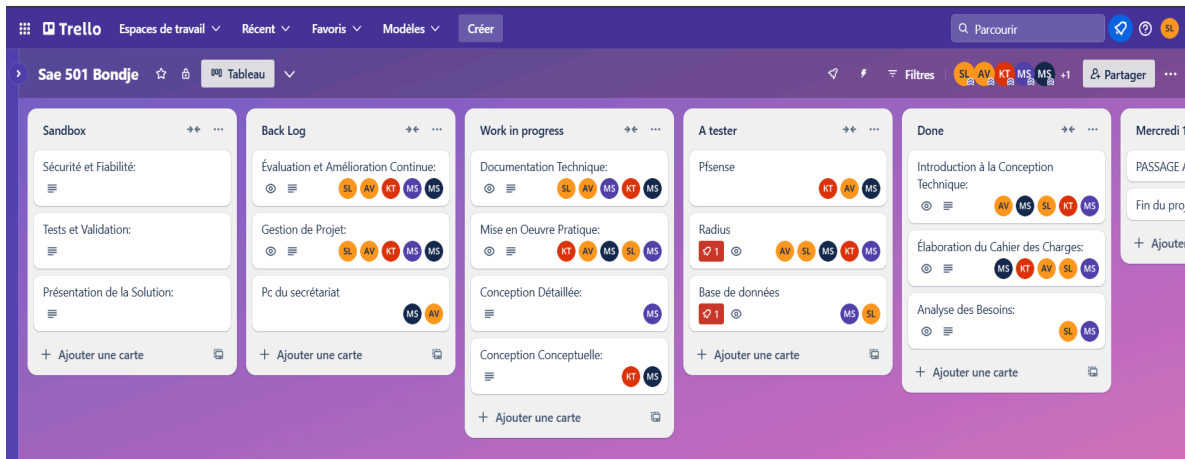
Pour réaliser ce projet, nous avons préféré utiliser Trello au lieu d'un diagramme de Gantt, car bien que le diagramme de Gantt soit un outil puissant pour planifier des projets complexes avec des dépendances entre les tâches, il peut être trop rigide et difficile à mettre à jour pour des projets nécessitant plus de flexibilité. Tandis que Trello lui est une application en ligne conçue pour la gestion des projets et la coordination des équipes. Cet outil permet aux utilisateurs d'accéder à leurs informations depuis n'importe quel appareil connecté à internet. Trello facilite la gestion des tâches en offrant une interface visuelle simple et efficace.

Trello fonctionne principalement à l'aide de trois éléments: des tableaux, des listes et des cartes.

- Les tableaux représentent les grands projets ou objectifs sur lesquels travaille une équipe.
- Les listes permettent de diviser le tableau en sections, souvent pour décrire différentes phases d'un projet (comme "Backlog", "Work in progress", "À tester", "Done").
- Les cartes symbolisent les tâches spécifiques à réaliser. Elles peuvent inclure divers détails comme une description, des pièces jointes, des dates limites ou encore des commentaires pour la communication entre les membres.

Grâce à son système de glisser-déposer, les utilisateurs peuvent facilement déplacer les cartes d'une liste à l'autre afin de représenter visuellement l'avancement des tâches. Cela permet de suivre le flux de travail de manière dynamique et intuitive.

Voici à quoi ressemble notre interface sur trello:

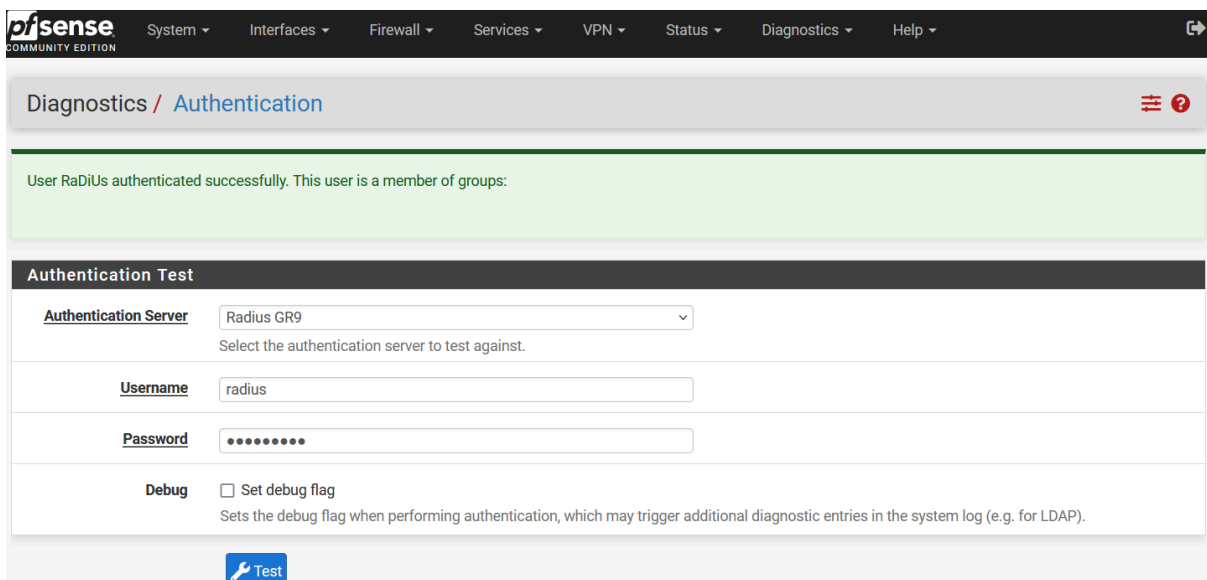


8) Sécurité et Fiabilité

Sécurité

1. Gestion des utilisateurs et authentification :

- **Validation d'authentification via FreeRADIUS** : Des tests ont été réalisés avec des identifiants utilisateur (LOGIN + MDP ainsi que LOGIN FULL MAJ + MDP, LOGIN ALTERNE + MDP) pour s'assurer de la compatibilité avec FreeRADIUS.
- Capture 1 : Test avec LOGIN + MDP.



- Capture 2 : Test avec LOGIN FULL MAJ + MDP.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Diagnostics / Authentication

User RADIUS authenticated successfully. This user is a member of groups:


Authentication Test

Authentication Server Radius GR9
Select the authentication server to test against.

Username RADIUS

Password

Debug ☐ Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

 Test

- Capture 2 : Test avec LOGIN ALTERNE + MDP

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Diagnostics / Authentication

User RaDiUs authenticated successfully. This user is a member of groups:


Authentication Test

Authentication Server Radius GR9
Select the authentication server to test against.

Username RaDiUs

Password

Debug ☐ Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

 Test

Ici on voit que le login est insensible à la casse donc, nous allons rajouter une ligne dans notre mods-available pour que radius fasse la distinction entre les Maj et les min d'un login:

```
sql {
    # The sub-module to use to execute queries. This should match
    # the database you're attempting to connect to.
    #
    # * rlm_sql_mysql
    # * rlm_sql_mssql
    # * rlm_sql_oracle
    # * rlm_sql_postgresql
    # * rlm_sql_sqlite
    # * rlm_sql_null (log queries to disk)
    #
    driver = "rlm_sql_mysql"
    dialect = "mysql"
    server = "localhost"
    login = "radius"
    password = "Lost2004*"
    radius_db = "radius"
    case_sensitive = yes
}
```

avec une commande **ALTER TABLE**, nous allons appliquer sur la table radcheck ou se trouve les login + mdp qu'utilise radius depuis mysql. Cette commande va modifier la colonne username de la table radcheck pour qu'elle utilise le jeu de caractères utf8_bin, qui est sensible à la casse.

```
root@koba-VirtualBox:/home/koba# sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 114
Server version: 5.7.42-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> USE radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> ALTER TABLE radcheck MODIFY username VARCHAR(255) COLLATE utf8_bin;
Query OK, 2 rows affected (0,26 sec)
Records: 2  Duplicates: 0  Warnings: 0

mysql> DESCRIBE radcheck;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id    | int(11) unsigned | NO | PRI | NULL | auto_increment |
| username | varchar(255) | YES | MUL | NULL | |
| attribute | varchar(64) | NO | | | |
| op    | char(2) | NO | | == | |
| value | varchar(253) | NO | | | |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0,01 sec)

mysql>
```

Maintenant les login doivent être rentrés tels qu'ils ont été définis dans mysql sur l'authentification radius :

- Capture 1 : Test avec LOGIN FULL MAJ + MDP.

The screenshot shows the pfSense web interface for the Authentication Test. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main header indicates the current page is Diagnostics / Authentication. A red message box states: "The following input errors were detected: Authentication failed." Below this, the "Authentication Test" section contains the following fields:

- Authentication Server:** A dropdown menu set to "Radius GR9". Below it, the text "Select the authentication server to test against." is displayed.
- Username:** A text input field containing "RADIUS".
- Password:** A password input field with masked characters (dots).
- Debug:** A checkbox labeled "Set debug flag" which is currently unchecked. Below it, a note states: "Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP)." A blue "Test" button is located at the bottom of the form.

- Capture 2 : Test avec LOGIN ALTERNE + MDP

This screenshot is similar to the previous one, showing the pfSense Authentication Test interface. The top navigation bar and header are identical. The red message box again states: "The following input errors were detected: Authentication failed." In the "Authentication Test" section, the fields are:

- Authentication Server:** A dropdown menu set to "Radius GR9". Below it, the text "Select the authentication server to test against." is displayed.
- Username:** A text input field containing "RaDiUs".
- Password:** A password input field with masked characters (dots).
- Debug:** A checkbox labeled "Set debug flag" which is currently unchecked. Below it, a note states: "Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP)." A blue "Test" button is located at the bottom of the form.

- Capture 3 : Test avec LOGIN + MDP.

Diagnostics / Authentication ☰ ?

User radius authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server Radius GR9
Select the authentication server to test against.

Username radius

Password ••••••••

Debug ☐ Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).

⚙️ Test

On peut constater qu'après avoir apporté des modifications aux fichiers de configuration, nous avons pu sécuriser l'authentification seul la capture 3 peut fonctionner.

2. Règles de pare-feu sur pfSense :

- Isolation stricte entre les réseaux :

- **LAN → OPT1** : Blocage total des connexions pour protéger les ressources internes.

Floating WAN LAN OPT1

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/774 KiB	*	*	*	LAN Address	443 80	*	*		Anti- Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	OPT1 net	*	LAN net	*	*	none			⚓ 📄 🚫 🗑️

- **OPT1 → LAN** : Trafic limité pour restreindre l'accès aux ressources sensibles.

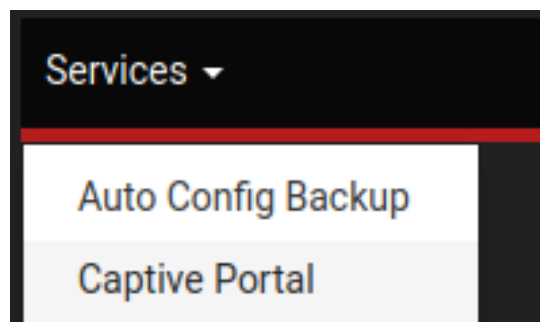
3. Surveillance et gestion des logs :

- Analyse des journaux FreeRADIUS pour identifier les connexions valides et suspectes.
- Détection des tentatives d'accès répétées échouées afin d'ajuster les politiques de sécurité si nécessaire.

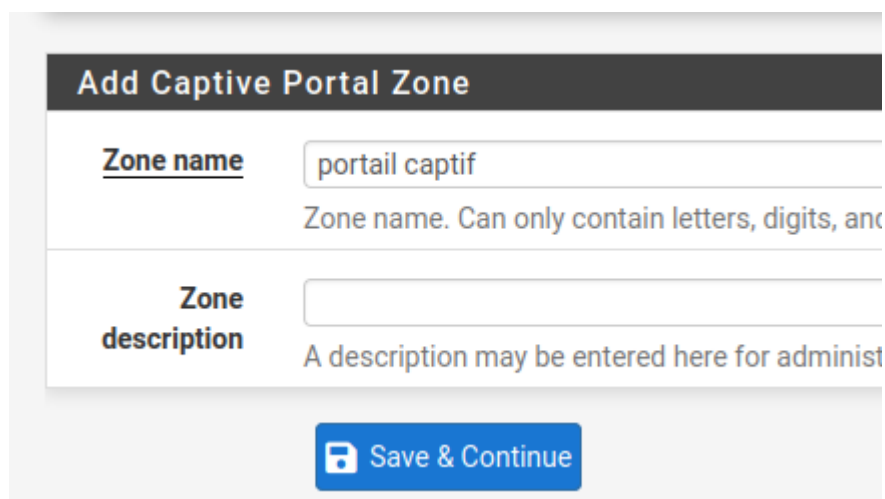
La configuration du Portail Captif sur OPT1 fait aussi partie de la sécurité.

voici les Étapes de Configuration :

1. On accède à l'interface graphique de pfSense.
2. Nous allons dans **Services > Captive Portal**.



3. nous Créons un nouveau portail :
 - On donne un nom au portail et, si besoin, on ajoute une description.

A screenshot of the 'Add Captive Portal Zone' form in the pfSense interface. The form has a dark header with the title 'Add Captive Portal Zone'. Below the header, there are two input fields. The first is labeled 'Zone name' and contains the text 'portail captif'. Below this field is a hint: 'Zone name. Can only contain letters, digits, and'. The second field is labeled 'Zone description' and is currently empty. Below this field is a hint: 'A description may be entered here for administ'. At the bottom of the form is a blue button with a save icon and the text 'Save & Continue'.

- on ajoute le portail (Enable).

Captive Portal Configuration	
Enable	<input type="checkbox"/> Enable Captive Portal
Description	<input type="text" value="captif"/> A description may be entered here

- On sélectionne l'interface **OPT1** où le portail sera actif.

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input type="text" value="captif"/> A description may be entered here for
<u>Interfaces</u>	<div> <div>WAN</div> <div>LAN</div> <div style="background-color: #cccccc;">OPT1</div> </div>

- On configure les paramètres :
 - On choisit la méthode d'authentification. Dans notre cas, nous avons sélectionné **RADIUS**.

<u>Authentication Method</u>
<div>Use RADIUS MAC Authentication</div> <div>Select an Authentication Method to use for this zone. - "Authentication backend" will force the login page using their login and password, or using vouchers</div>

configuré.

- On sélectionne le serveur d'authentification

<u>Authentication Server</u>
grp

- On sauvegarde les modifications.

(Nous allons effectuer les tests de ces configuration dans la partie “**9) Tests et Validation**”)

Fiabilité

1. **Sauvegarde des configurations :**
 - Les configurations de pfSense et de la base MySQL sont sauvegardées régulièrement pour prévenir toute perte de données en cas de panne.
2. **Tests de stabilité :**
 - Vérification des règles de pare-feu et des connexions pour garantir un fonctionnement constant du réseau.
3. **Diagnostic des erreurs :**
 - Les fonctionnalités de diagnostic intégrées à pfSense ont été utilisées pour tester et valider les configurations, comme le montre la section "Diagnostics/Authentication". Cela permet de rapidement identifier et résoudre les éventuels problèmes d'accès ou de paramétrage.

9) Tests et Validation

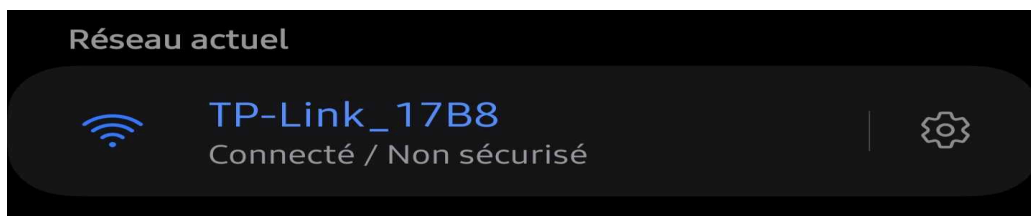
- Les utilisateurs peuvent se connecter au Wi-Fi et reçoivent une adresse IP correcte via DHCP.





- Le portail captif s'affiche correctement lors de la connexion au Wi-Fi.

- L'authentification fonctionne.







via le serveur RADIUS



- Les appareils connectés à OPT1 ont accès à Internet et sur pfsense dans le portail captif on peut voir qu'une personne est connectée via le portail captif

Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
portail	OPT1	1	captif	 

Et dans le DHCP leases nous pouvons voir l'historique du dhcp demander

Status / **DHCP Leases**







Search

All

Enter a search string or *nix regular expression to filter entries.

Leases

	IP address	MAC address	Client Id	Hostname	Description	Start	End
<input checked="" type="checkbox"/>	192.168.3.103	46:59:ab:15:72:f4		S23-Ultra		2024/12/14 21:13:24	2024/12/14 23:13:24

Ici on remarque bien que le téléphone a bien reçu une adresse IP.

10) Documentation Technique

Rédaction de manuel technique:

Fonction de PfSense:

- Adresses IP LAN, WAN et OPT: L'attribution d'adresses IP dédiées pour le réseau local (LAN) et le réseau étendu (WAN) et les interfaces OPT permet une meilleure gestion des connexions et optimise la performance réseau.

- Règle de pare-feu: Une configuration claire des règles de filtrage réseau garantit un niveau élevé de sécurité en contrôlant efficacement le trafic entrant et sortant.
- Administration et gestion: L'accès à l'interface d'administration de PfSense facilite le suivi continu du réseau et permet des ajustements en temps réel, notamment dans la modification des règles de sécurité.

Fonction de MySQL:

- Base de données: Le serveur MySQL permet de centraliser les données en les stockant dans une base unique, facilitant ainsi l'organisation et la gestion des informations.
- Administration des données: L'utilisation d'outils de gestion de base de données simplifie les opérations de sauvegarde et de restauration régulières, assurant la protection et l'intégrité des données.

Fonction du Serveur RADIUS:

- Sécurité et authentification: Le paramétrage des clients autorisés via RADIUS renforce la sécurité d'accès grâce à une authentification centralisée.
- Administration: La gestion des utilisateurs RADIUS (ajout, suppression) offre une flexibilité optimale des autorisations. De plus, la surveillance des journaux d'authentification permet une visibilité accrue sur les tentatives d'accès au réseau.

Fonction du routeur TP-Link:

- Paramétrage du réseau: La définition du SSID et l'intégration d'une clé de sécurité WPA2 assurent une connexion sans fil fiable et protégée. L'attribution d'adresses IP fixes facilite l'organisation et le suivi des équipements connectés.
- Gestion des périphériques: L'interface d'administration du routeur permet de surveiller et de contrôler les appareils autorisés à se connecter au réseau.

Portail Captif:

- Authentification et contrôle d'accès: Le portail captif facilite la gestion des connexions en forçant les utilisateurs à s'authentifier avant d'accéder au réseau. Cette solution

permet de contrôler et restreindre l'accès au réseau en fonction des besoins spécifiques des utilisateurs.

- Surveillance et sécurité: Le portail captif améliore la traçabilité des activités réseau et contribue à renforcer la sécurité en identifiant les utilisateurs connectés.