I. Introduction

1. Contexte:

L’entreprise GSB est une industrie pharmaceutique.

L’entreprise GSB est la fusion entre deux grosses entreprises déjà bien implantées dans le secteur pharmaceutique. La première entreprise est Galaxy qui est le géant américain (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et pour la deuxième entreprise nous retrouvons le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels) lui-même déjà union de trois petits laboratoires.

J’interviens en tant qu’administrateur système et réseau au sein du groupe.

II. Besoin

Dans le cadre de l'amélioration de son environnement réseau, le laboratoire GSB souhaite mettre en place un portail captif.
Cet outil doit répondre à plusieurs exigences :

- **Authentification des utilisateurs :**

S'assurer que chaque utilisateur (collaborateurs, visiteurs, partenaires) se connecte via un mécanisme d'authentification fiable (identifiants, certificats, etc.).

- **Contrôle d'accès :**

Limiter et encadrer la navigation en imposant des règles spécifiques (bande passante, URL autorisées ou interdites, temps de connexion maximal).

- **Renforcement de la sécurité :**

Centraliser la gestion des accès, prévenir les connexions non autorisées et protéger les données circulant sur le réseau.

Ce dispositif permettra à GSB de mieux superviser et sécuriser l'accès au Wi-Fi ou aux segments de réseau dédiés aux visiteurs, tout en restant conforme aux réglementations internes et aux standards de sécurité.

III. Solution

1. Choix de la technologie

Pour doter GSB d'un portail captif efficace et évolutif, j'ai étudié plusieurs solutions open source et propriétaires.

L'objectif est de sélectionner un outil offrant :

• Une interface de gestion claire et intuitive.

• Des possibilités de configuration avancées (quotas de bande passante, systèmes d'authentification multiples, etc.).

• Une intégration fluide avec l'infrastructure réseau existante (VLAN, routeurs, switches).

2. Analyse comparative

Critère	pfSense	PacketFence	ChilliSpot	MikroTik Hotspot
Type de solution	Pare-feu avec portail captif	NAC (contrôle d'accès)	Portail captif dédié	Hotspot intégré
Portail captif intégré	Oui	Non (via NAC)	Oui	Oui
Gestion des utilisateurs	Basique	Avancée	Basique	Avancée
Authentification	Locale / RADIUS	RADIUS / LDAP / AD	RADIUS	Locale / RADIUS
Facilité de mise en place	Simple	Complexe	Simple	Moyenne
Personnalisation du portail	Avancée	Avancée	Limitée	Avancée
Scalabilité	Moyenne	Élevée	Faible	Élevée

PfSense s'est démarqué par sa richesse fonctionnelle, sa simplicité de configuration et son importante communauté d'utilisateurs. De plus, GSB dispose déjà d'un pare-feu pfSense en production, ce qui facilite grandement la mise en place et la maintenance du portail captif.

III. PfSense

1. Qu’est-ce que PfSense ?

PfSense est une solution open source basée sur le système FreeBSD. Initialement conçu comme un routeur/pare-feu de haute fiabilité, PfSense propose une interface d’administration web ergonomique et prend en charge une multitude de fonctionnalités réseau (VPN, VLAN, haute disponibilité, etc.). Parmi ses modules, on retrouve un portail captif entièrement personnalisable, permettant de contrôler l’accès Internet sur un ou plusieurs VLAN.

2. Origines de PfSense

Créé en 2004, PfSense est issu du projet m0n0wall, une distribution minimaliste de pare-feu. L’équipe à l’origine de PfSense souhaitait proposer une solution plus complète et modulable, tout en conservant la robustesse de FreeBSD. Au fil des années, PfSense a connu de nombreuses améliorations (interface, sécurité, nouvelles fonctionnalités) et est aujourd’hui considéré comme l’une des références en matière de firewall et de gestion réseau.

3. Les avantages de PfSense

• Simplicité d’utilisation : L’accès via une interface web et la structure claire des menus facilitent la prise en main.

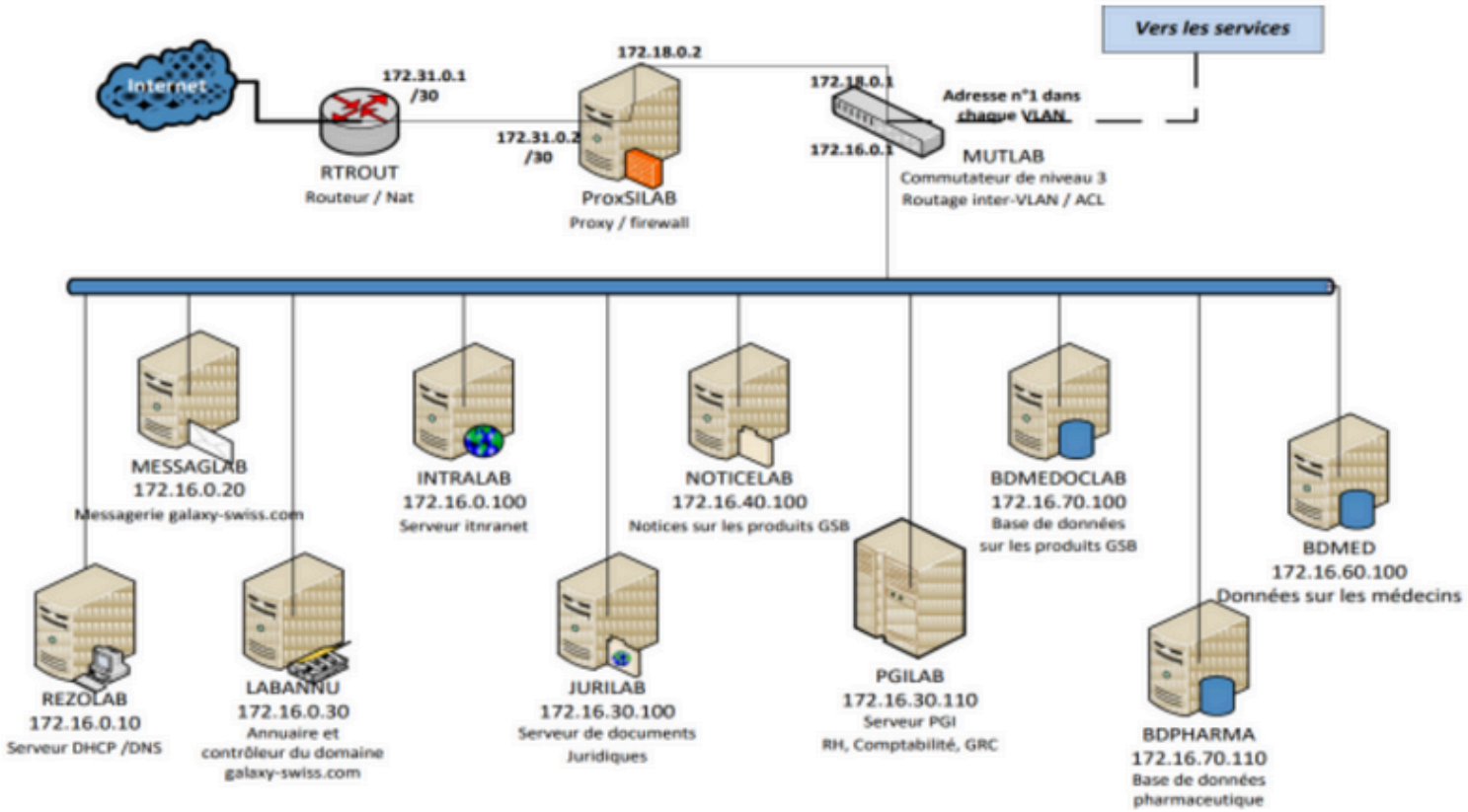
• Modularité : De nombreux packages peuvent être ajoutés (Squid, Snort, OpenVPN…).

• Communauté dynamique : Une documentation riche et réactive, des forums spécialisés, et un écosystème de plugins permettant de répondre à la plupart des besoins d’entreprise.

• Coût : PfSense est gratuit et open source, ce qui réduit les frais de licence tout en bénéficiant d’un produit professionnel.

IV. Infrastructure

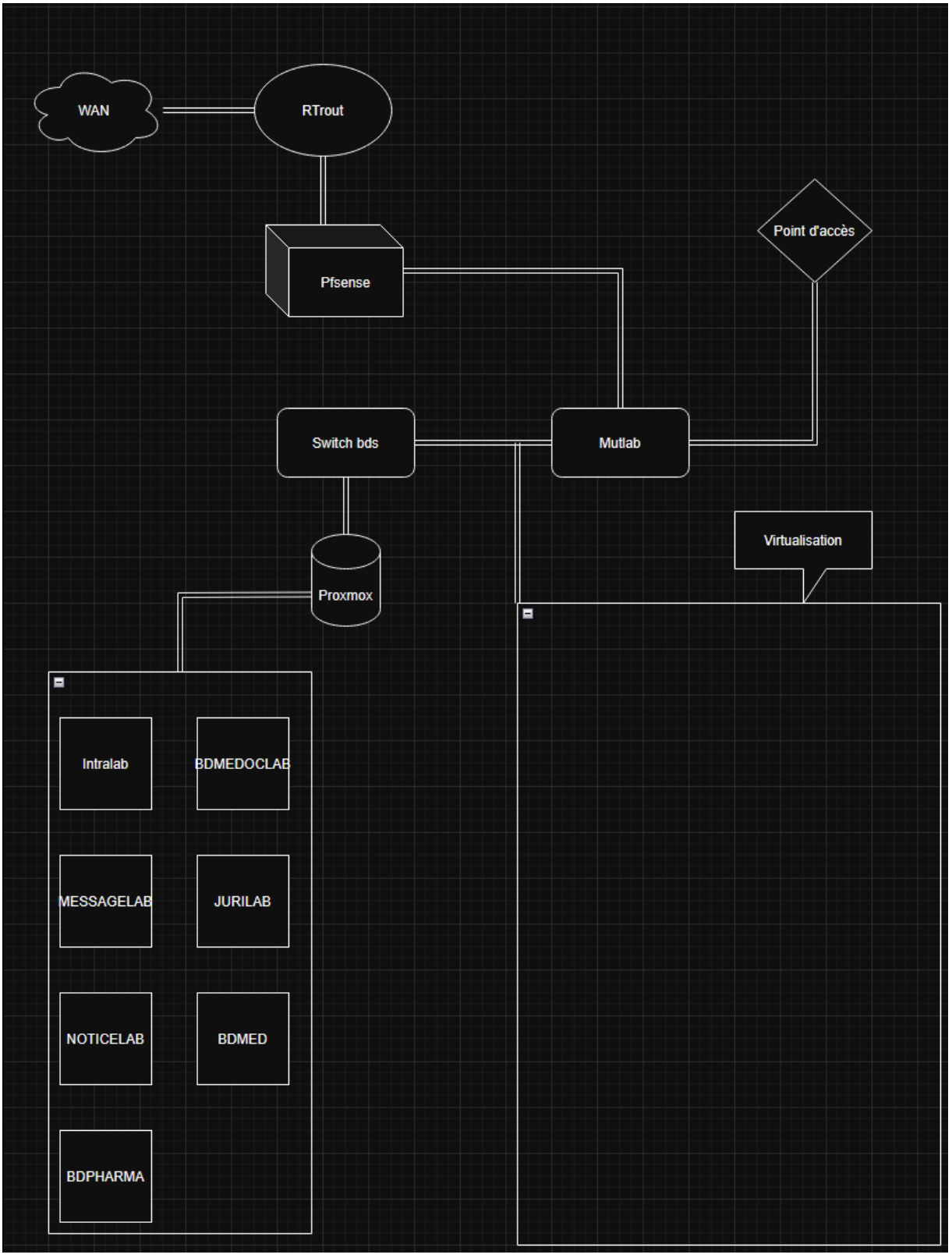
1.Infrastructure gsb existante



2. Tableau d'Adressage IP des VLAN

VLAN	Service(s)	Passerelle IP
110	Réseau & Système	192.168.110.0/24
20	Direction / DSI	192.168.20.0/24
30	RH / Compta / Juridique / Secrétariat	192.168.30.0/24
40	Communication / Rédaction	192.168.50.0/24
50	Développement	192.168.50.0/24
60	Commercial	192.168.60.0/24
70	Labo-Recherche	192.168.70.0/24
100	Accueil	192.168.100.0/24
150	Visiteurs	192.168.150.0/24
200	Démonstration	192.168.200.0/24
300	Serveurs	172.16.0.0/17
400	Sortie	172.18.0.0/30

3. Schéma réseau de la réalisation professionnelle



4. Matériel à disposition

Dans la mise en place de ma réalisation professionnelle, voici le matériel mis à ma disposition
par le groupe GSB :

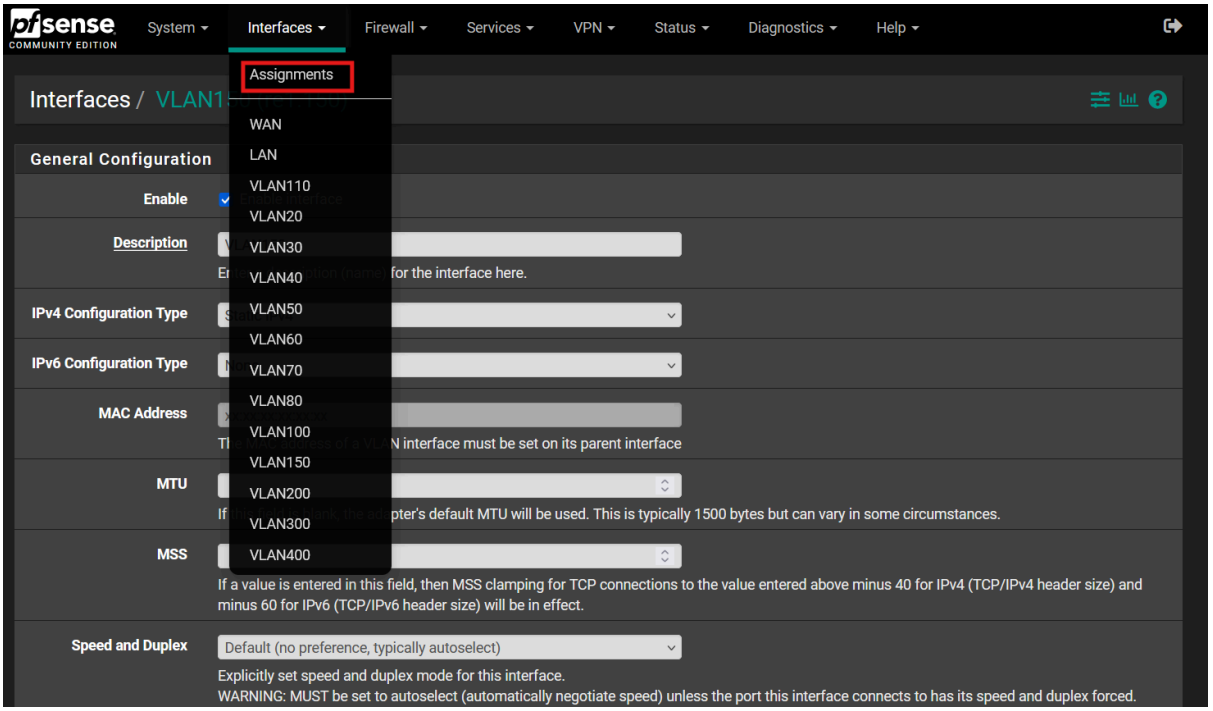
- **Cisco Catalyst 3560G (MUTLAB)**
- **Cisco Catalyst 3750G (SW-RS-DELTA)**
- **Cisco Catalyst 2960-S (SWITCH-BDS)**
- **Un routeur Cisco (RTROUT)**
- **Un routeur/pare-feu pfSense (ProxSilab)**
- **Hyperviseur de type 1 (PVE-DELTA)**
- **Hyperviseur de type 1 (PVE-ETHAN)**
- **Un point d’accès WiFi**

V. Mise en place du portail captif

1.Installation

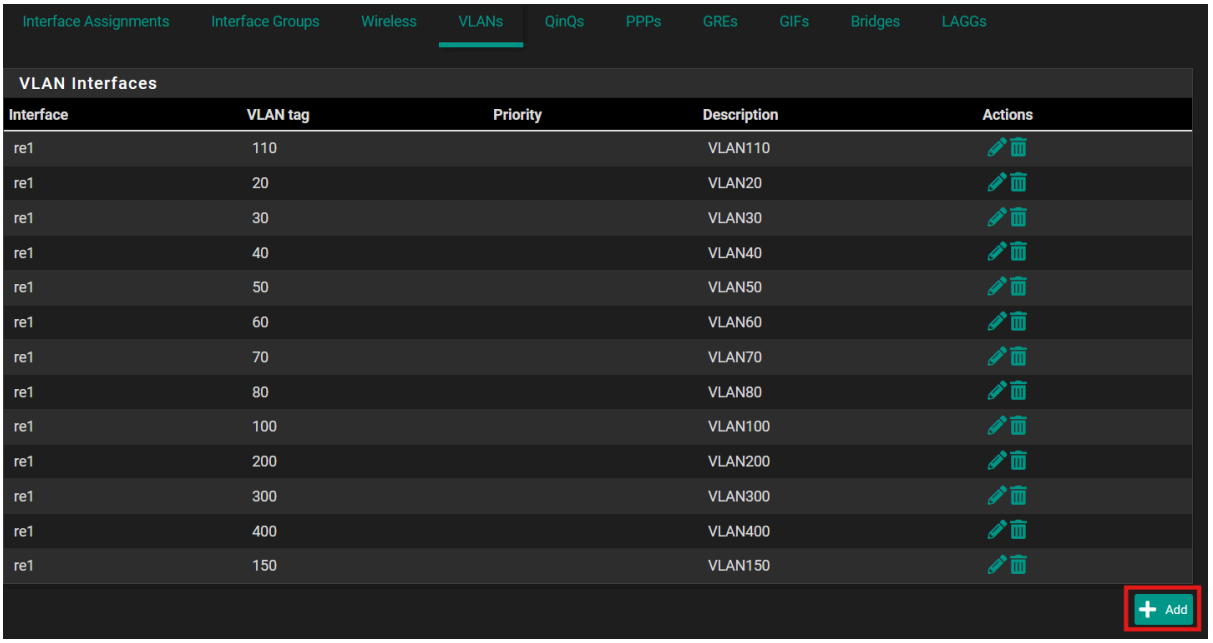
GSB dispose déjà d'un serveur pfSense opérationnel. Je me connecte via un navigateur, l'adresse du pfSense est 192.168.110.100.

Une fois connecté, je me rend dans "interface > Assignments."

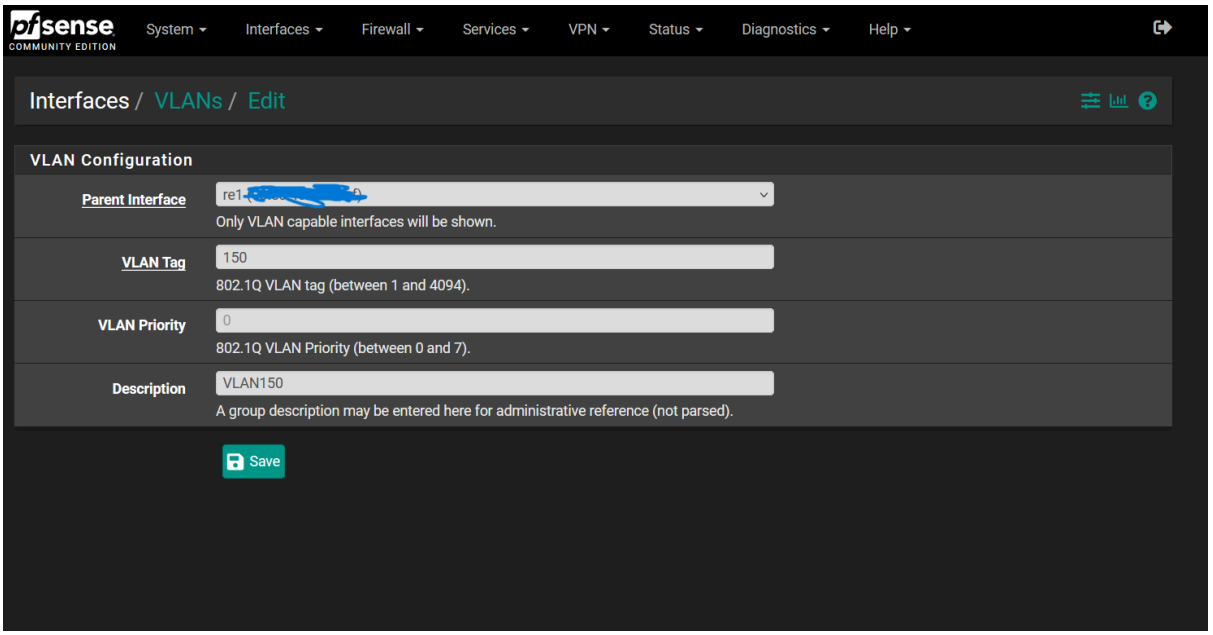


Il faut ensuite créer le vlan 150 que nous utiliserons pour le portail captif

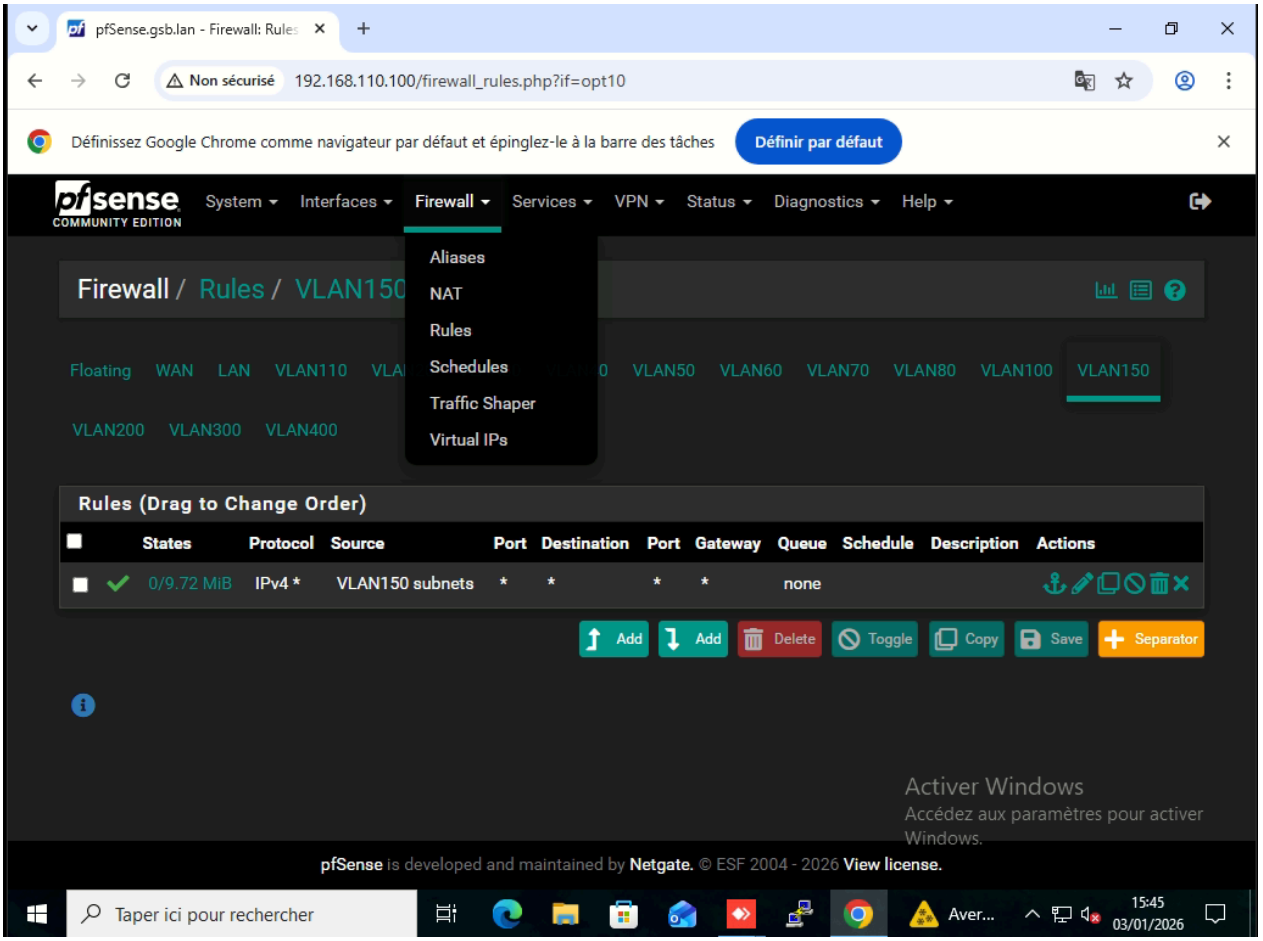
Pour ce faire, je me rend dans l'onglet VLANs puis je clique sur +add.



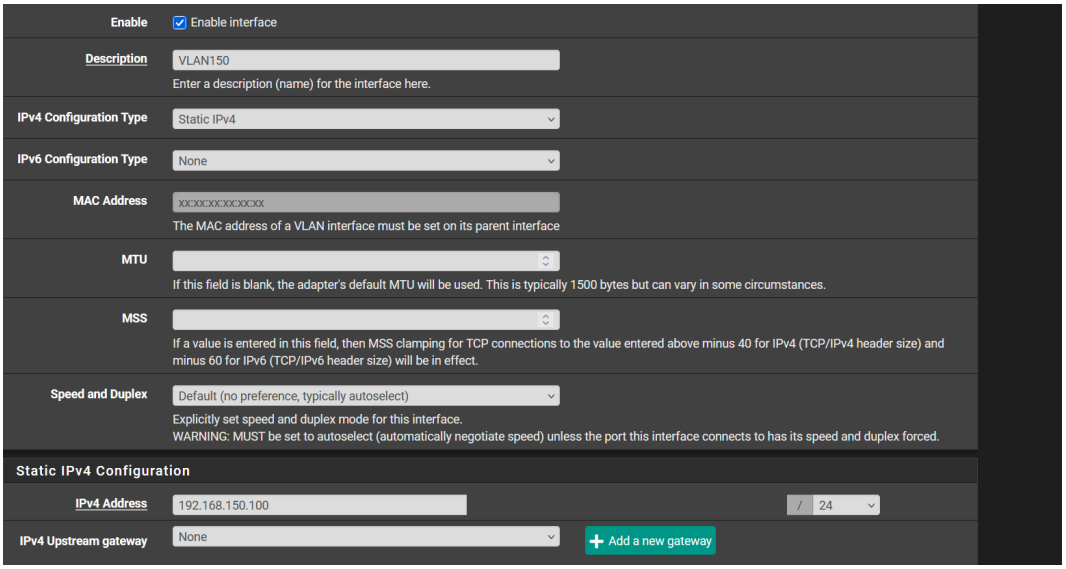
Je mets ensuite l'interface qui est connectée au reste du matériel dont le point d'accès et le reste du matériel pour le vlan 150.



je me rend ensuite dans firewall > rules > Le vlan j'ai créé(150) > add

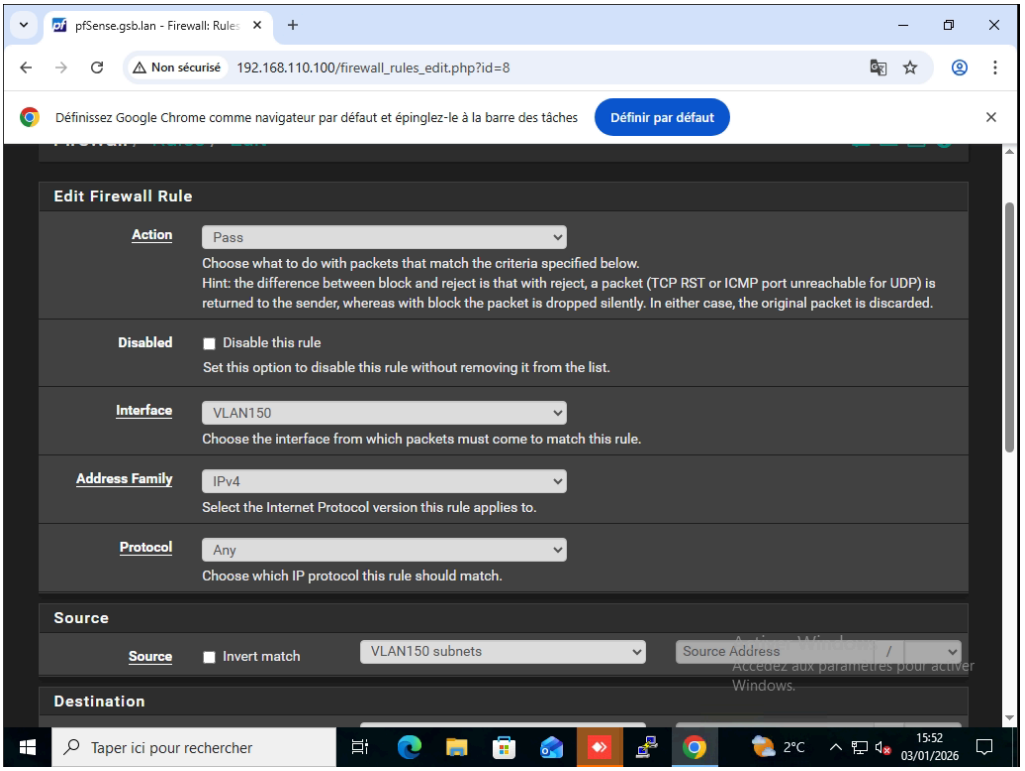


Voici les paramètres pour mon vlan adapté à l'entreprise GSB



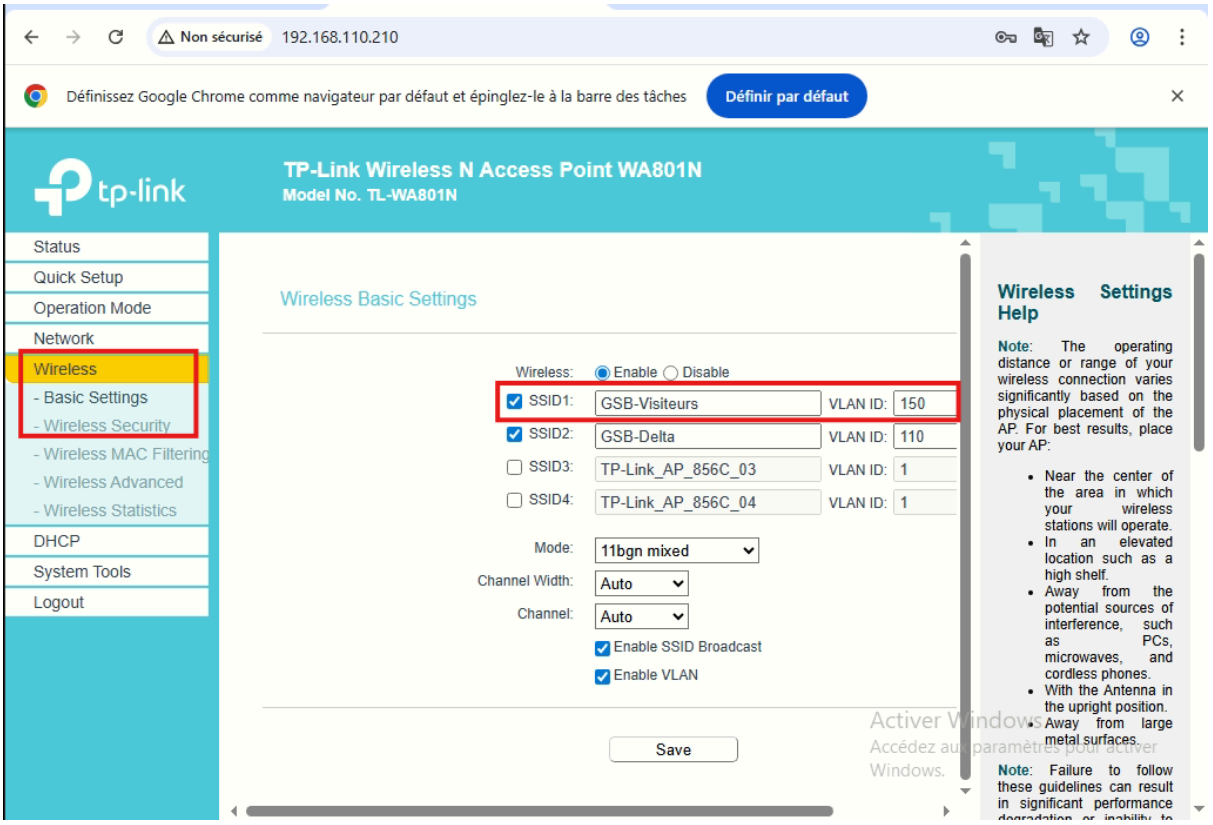
Je réalise ensuite les réglages adapter au réseau GSB, j'ai personnellement fais en sorte qu'il n'y est aucun blocage vers les autres

vlan, comme vous pouvez le voir actuellement, cela à été fait pour réaliser des tests, des changements de paramètres ont été réalisés ensuite.



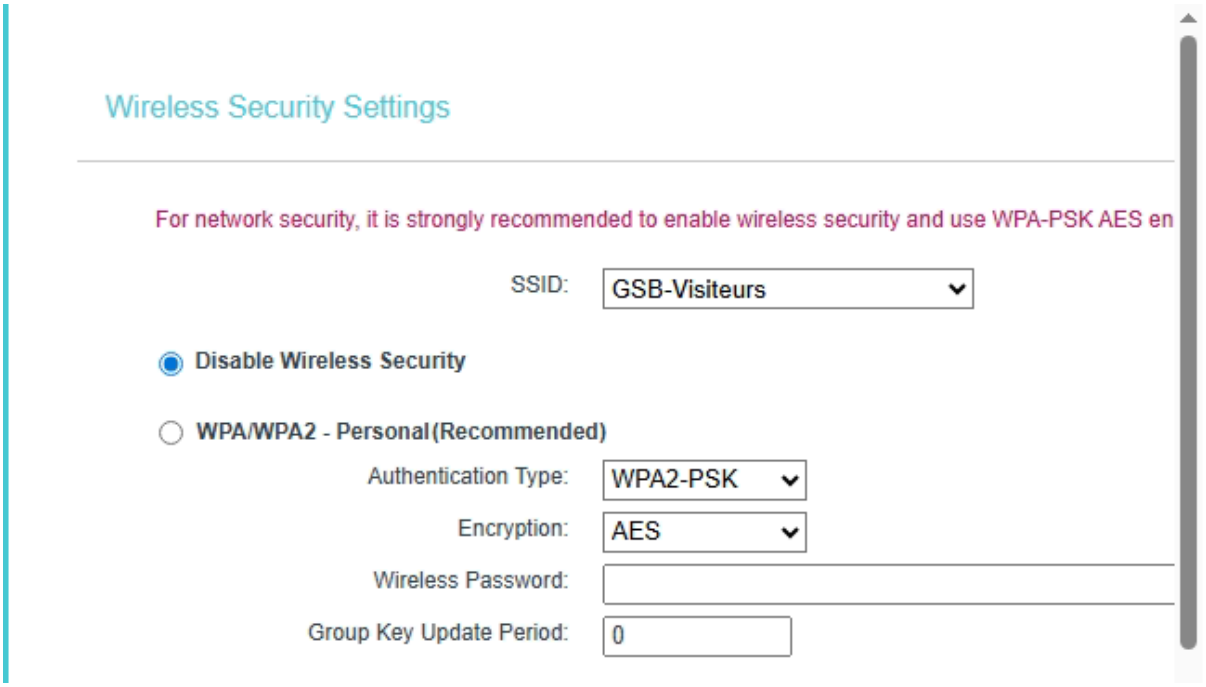
Une fois tous les réglages du VLAN réalisés, je me rend sur le point d'accès et réalise les réglages nécessaires. Je me connecte via un

navigateur, l’adresse du point d’accès est 192.168.110.210.



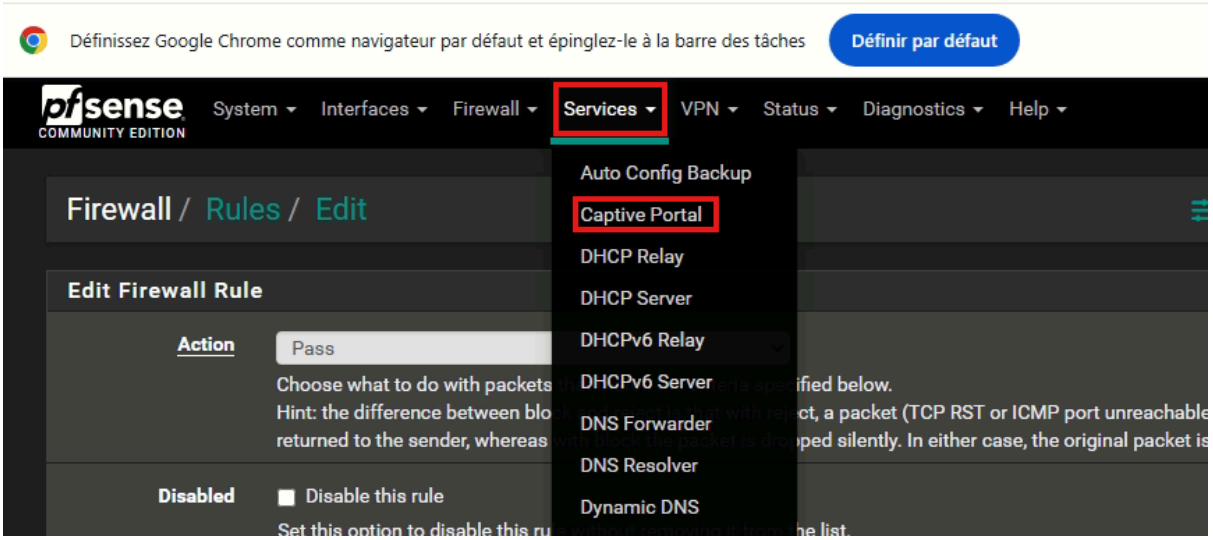
Pour le wifi j’ai mis le nom de la société + visiteurs pour bien indiquer que ce wifi est un wifi invité. J’ai ensuite mis le vlan dédié. Une fois cela réalisé, je me suis rendu sur wireless security qui est juste en dessous de basic settings à gauche de l’écran.

je désactive le mot de passe pour le wifi GSB-Visiteurs, le portail captif dans le Pfsense va gérer la sécurité du réseau.

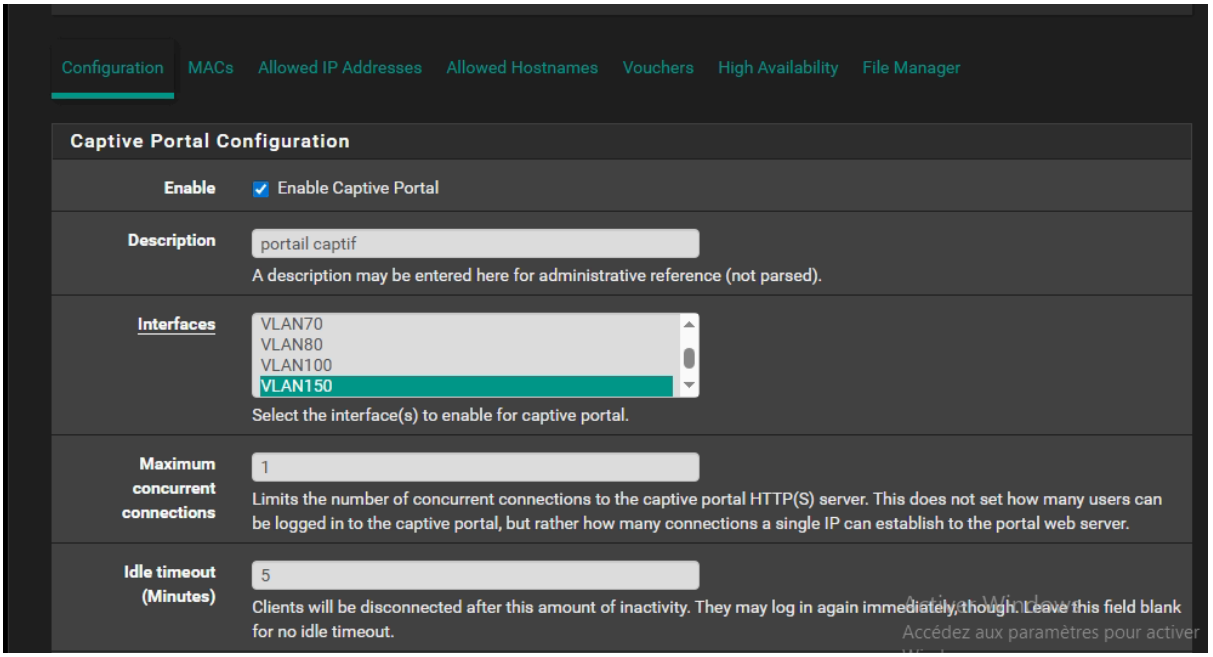


Comme vu ci-dessus je désactive le mot de passe du wifi, ce qui permet au visiteur de se connecter au wifi dans le VLAN 150, les visiteurs seront automatiquement redirigé vers le portail captif dans le pfsense, là où ils pourront oui ou non accéder à internet.

Maintenant, je commence la configuration du portail captif.
je me rend à nouveau sur Pfsense, je me dirige ensuite dans “services > Captive portal”.



Une fois sur la page je clique sur add et cette page apparaît :



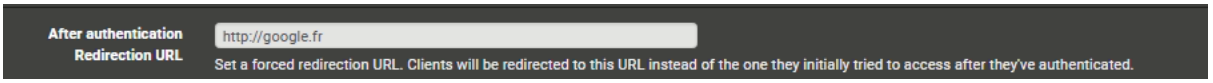
J'active ensuite la zone en cochant Enable Captive Portal.

- Je sélectionne l'interface sur laquelle je souhaite appliquer le portail captif, le VLAN150.

- Je mets en place une limitation du nombre de sessions sur le portail captif depuis la même adresse ip.

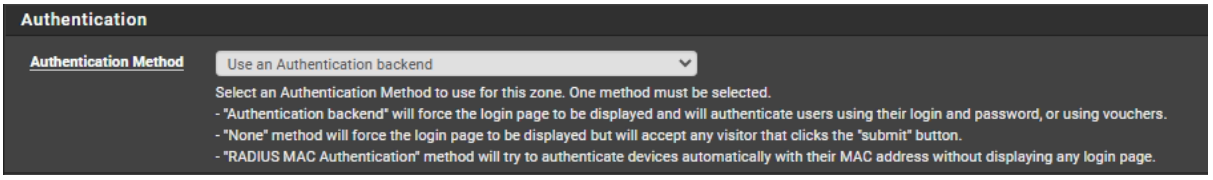
- Je définis également le temps d'inactivité au-delà duquel la session sera automatiquement coupée.

Je mets également en place une redirection après l'authentification.

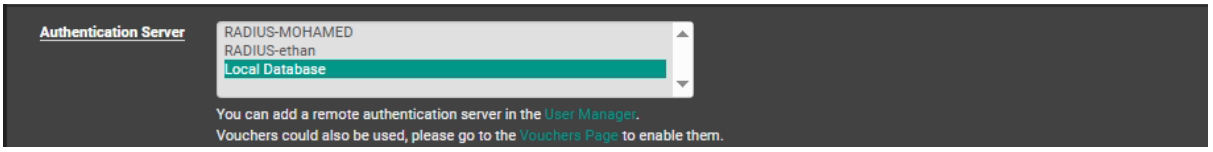


Je met la page de google pour que le visiteur puisse tomber sur une page de recherche fiable et simple d'utilisation.

Je sélectionne la méthode d'authentification « Use an Authentication Backend » qui oblige à se connecter ou à utiliser un voucher.

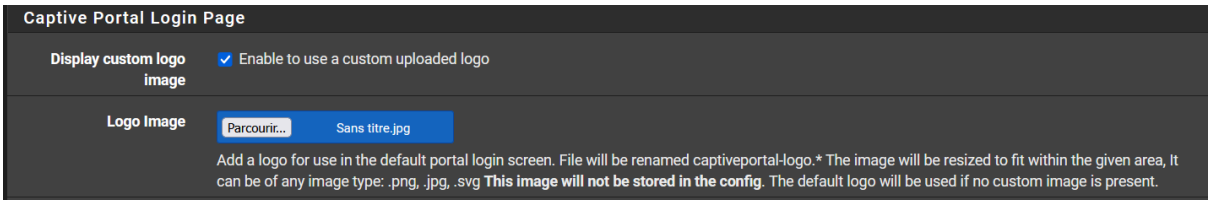


J'utilise le serveur d'authentification de pfSense « Local database ».



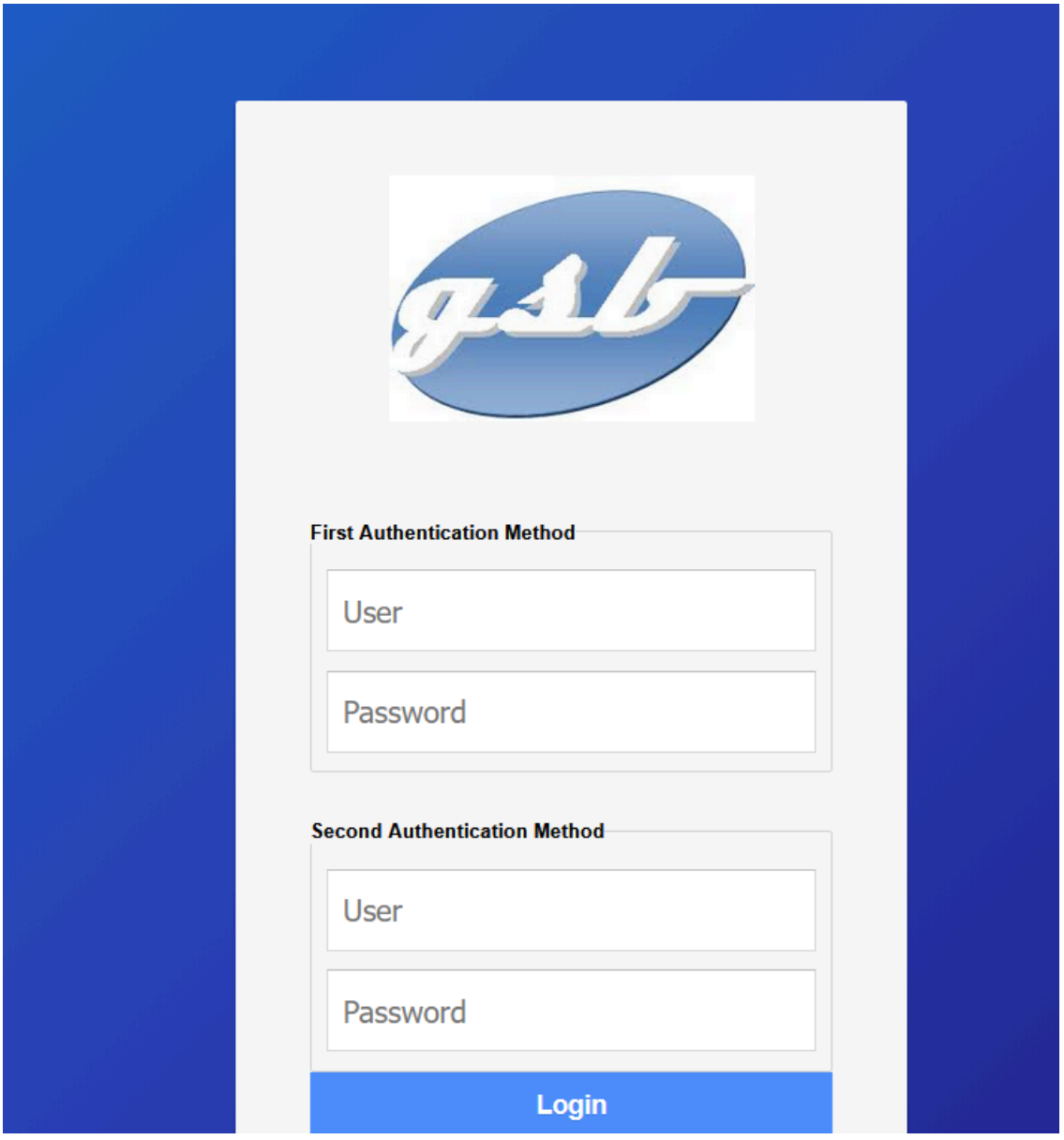
Tous les paramètres sont fonctionnels, je vais maintenant modifier la page du portail captif.

J'active l'option pour custom l'arrière page du portail captif puis je mets l'image de l'entreprise GSB.



La configuration du portail captif est maintenant terminée, je passe à la phase de test.

Je connecte une machine de test sur le VLAN 150 et je tente d’accéder à Internet, je suis automatiquement redirigé vers la page de connexion du portail captif.



Après avoir saisie des identifiants, un message de validation apparaît et l’utilisateur est redirigé vers la page que j’ai créée et configurée plus haut.

VI. Évolution possible

1.Intégration avec un serveur RADIUS

En intégrant un rôle dédié à l'installation et à la configuration d'un serveur RADIUS, GSB peut automatiser la gestion centralisée et sécurisée des identifiants, ainsi que la traçabilité des connexions. Cette approche englobe l'installation des dépendances requises (FreeRADIUS ou autre solution RADIUS), la configuration des politiques d'authentification, et la définition des règles de connexion pour les différents utilisateurs et services.

Intérêts pour GSB :

• Renforcer la sécurité et la traçabilité en centralisant la gestion des identifiants.

• Simplifier l'authentification sur les différents équipements et applications.

• Faciliter la maintenance et l'évolution des politiques d'accès grâce à une architecture standardisée.