Galaxy Swiss Bourdin

Sommaire

I. Introduction 2

1. Contexte 2

2. Besoin 2

II. Solution 3

1. Choix de la technologie 3

2. Analyse comparative 3

III. PfSense 4

1. Qu'est-ce que PfSense ? 4

2. Origines de PfSense 4

3. Les avantages de PfSense 4

IV. Infrastructure 5

1. Schéma réseau actuel 5

2. Tableau d'Adressage IP des VLAN 6

3. Schéma réseau de la réalisation professionnelle 7

4. Matériel à disposition 8

V. Mise en place du portail captif 9

1. Installation 9

2. Configuration 11

3. Test 13

VI. Évolution possible 14

VII. Conclusion 15

I. Introduction

1. Contexte

Le laboratoire Galaxy Swiss Bourdin (GSB), né de la fusion entre Galaxy et Swiss Bourdin, est devenu un acteur majeur du secteur pharmaceutique mondial en 2009. Basé à Paris, GSB a entrepris d'optimiser la gestion de ses activités de visite médicale en France, tandis que son siège social reste implanté à Philadelphie, aux États-Unis.
J'interviens en tant qu'administrateur système et réseau au sein du groupe.

2. 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.

II. 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

Afin de choisir le portail captif le plus adapté, j'ai procédé à une analyse rapide de quelques solutions courantes :

Critère	pfSense	PacketFence	Chillispot	MicroTik Hotspot
Facilité d'utilisation	☆☆☆☆☆	☆☆☆☆	☆☆☆	☆☆☆☆
Communauté / Écosystème	☆☆☆☆☆	☆☆☆☆	☆☆☆	☆☆☆
Fonctionnalités avancées	Pare-feu, VPN, etc.	Gestion NAC complète	Captive portal basique	Hotspot natif, firewall
Performance	Très bonne	Bonne	Moyenne	Bonne
Modèle open source	Oui (BSD-based)	Oui	Oui	Non (firmware)
Coût	Gratuit	Gratuit	Gratuit	Payant / Freemium

Au regard de ces critères, 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 libre (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

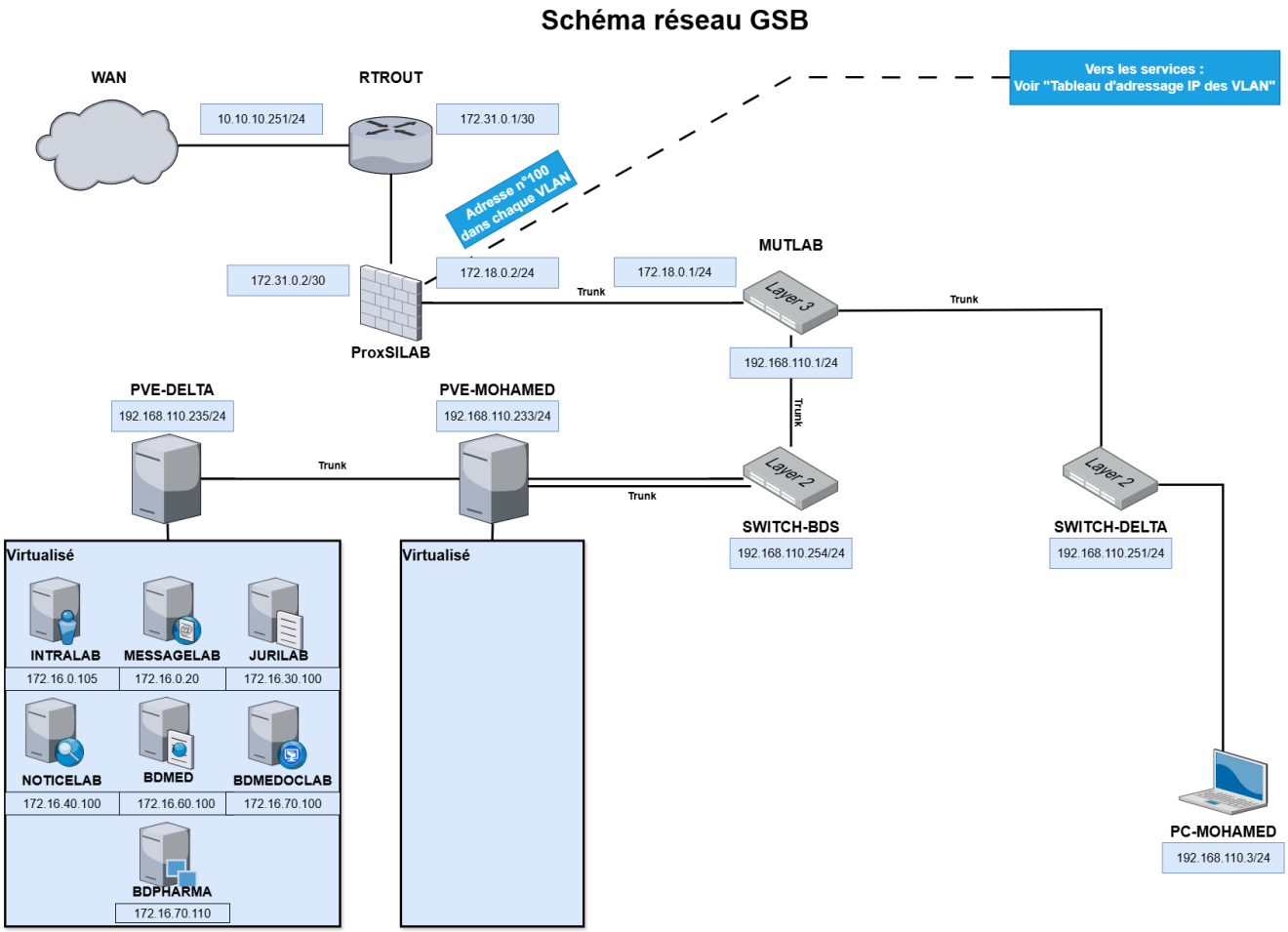
- **Simplicité d'utilisation** : L'accès via une interface web et la structure claire des menus facilitent la prise en main.
- **Modularité** : De nombreux packages peuvent être ajoutés (Squid, Snort, OpenVPN…).
- **Communauté dynamique** : Une documentation riche et réactive, des forums spécialisés, 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

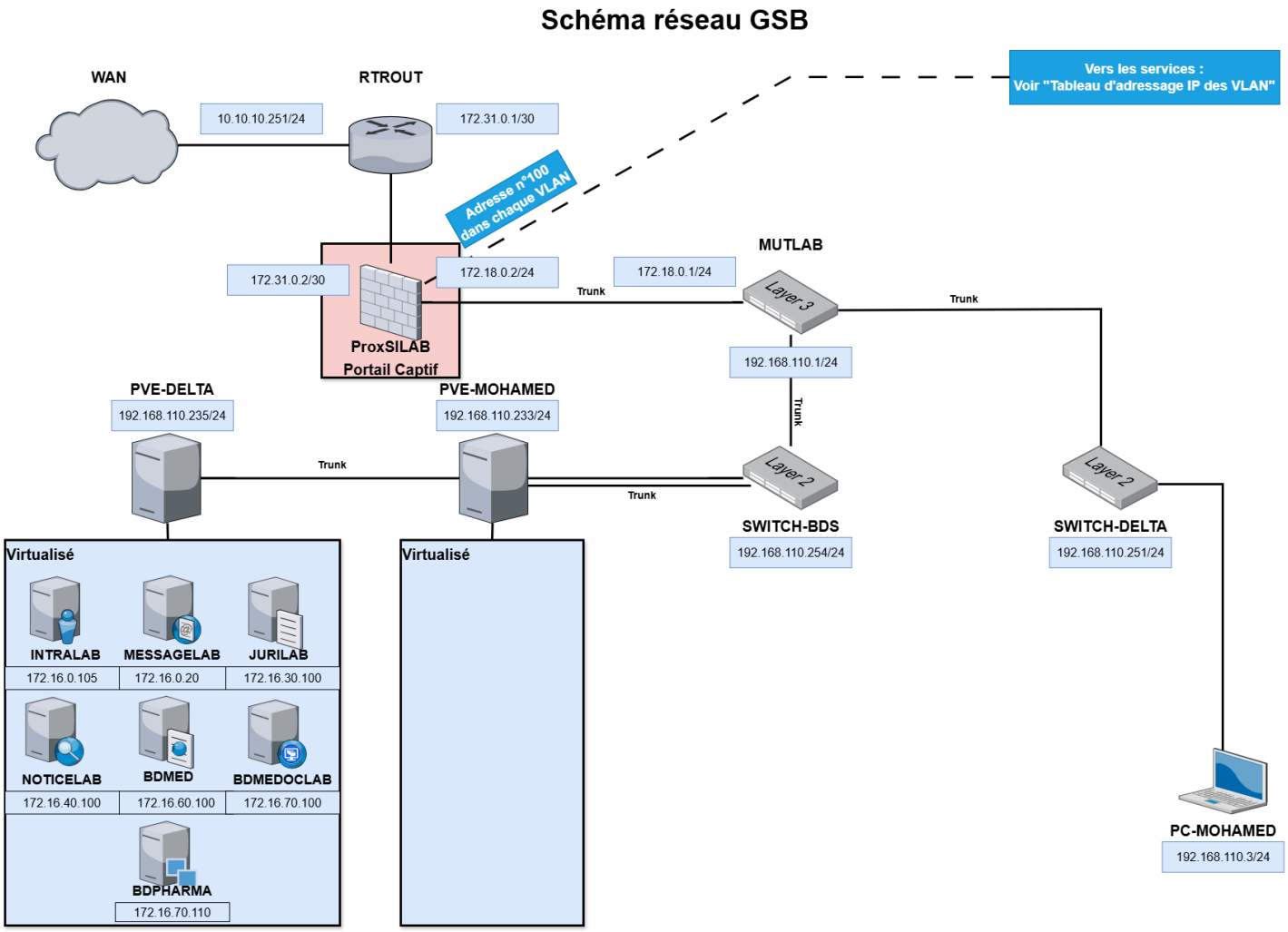
1. Schéma réseau actuel



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	192.168.40.0/24
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 :

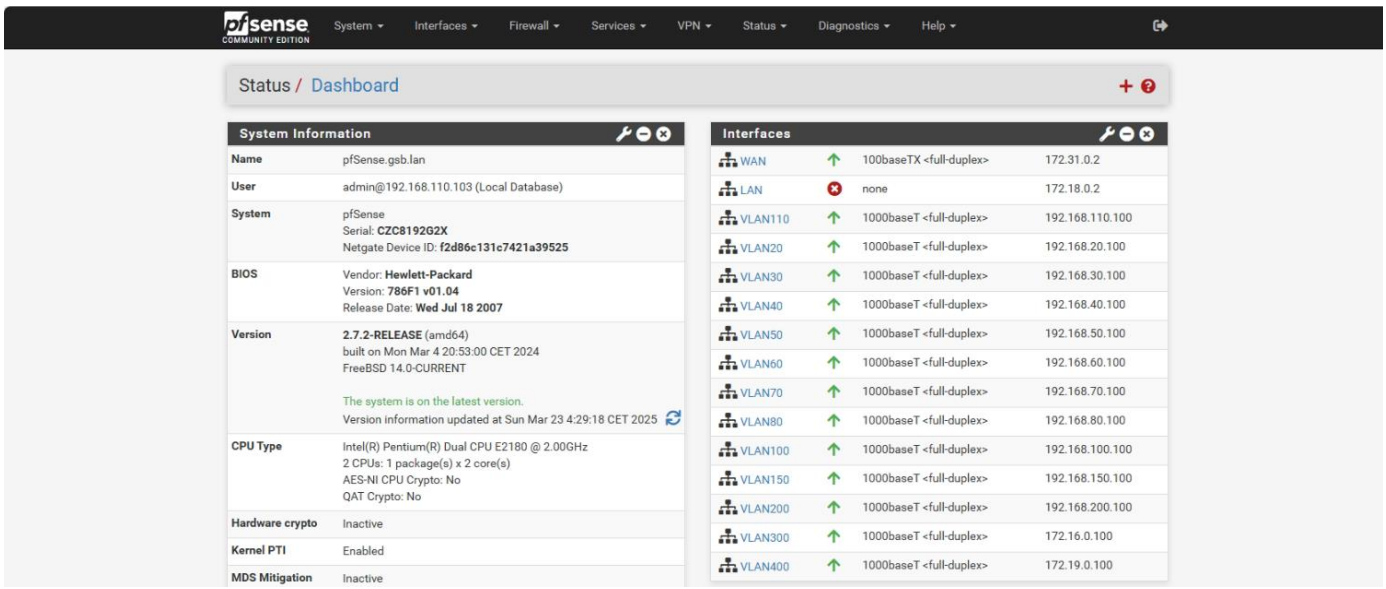
- **Cisco Catalyst 3560G (MUTLAB)**
- **Cisco Catalyst 3750G (SW-RS-DELTA)**
- **Cisco Catalyst 2960-S (SWITCH-BDS)**
- **Un routeur Cisco (RTROUT)**
- **Un routeur/pare-feu pfSense (ProxSilab)**
- **Hyperviseur de type 1 (PVE-DELTA)**
- **Hyperviseur de type 1 (PVE-MOHAMED)**
- **Un point d'accès WiFi**

V. Mise en place du portail captif

1. Installation

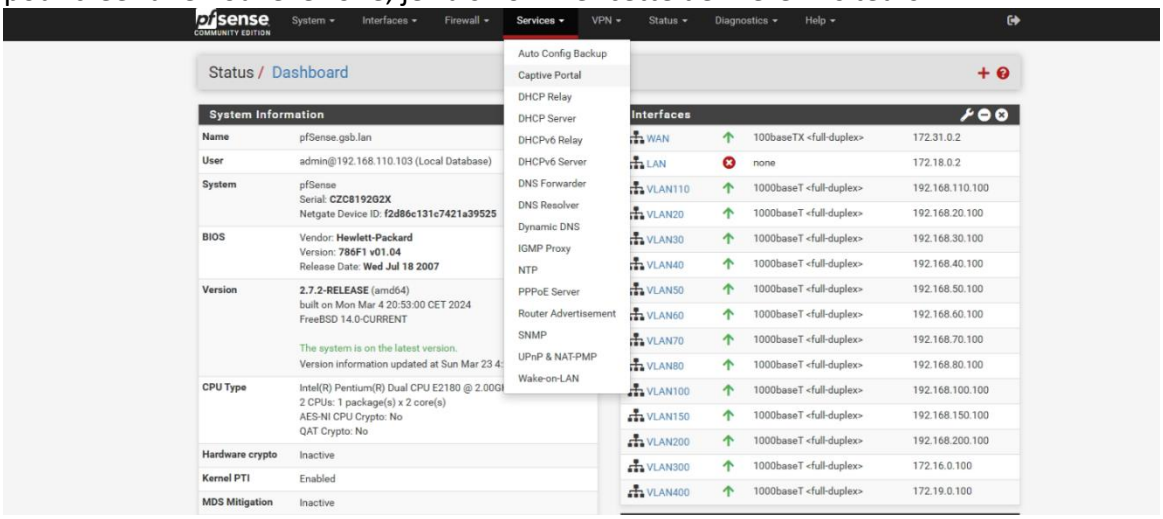
1. **Accès à l'interface PfSense**

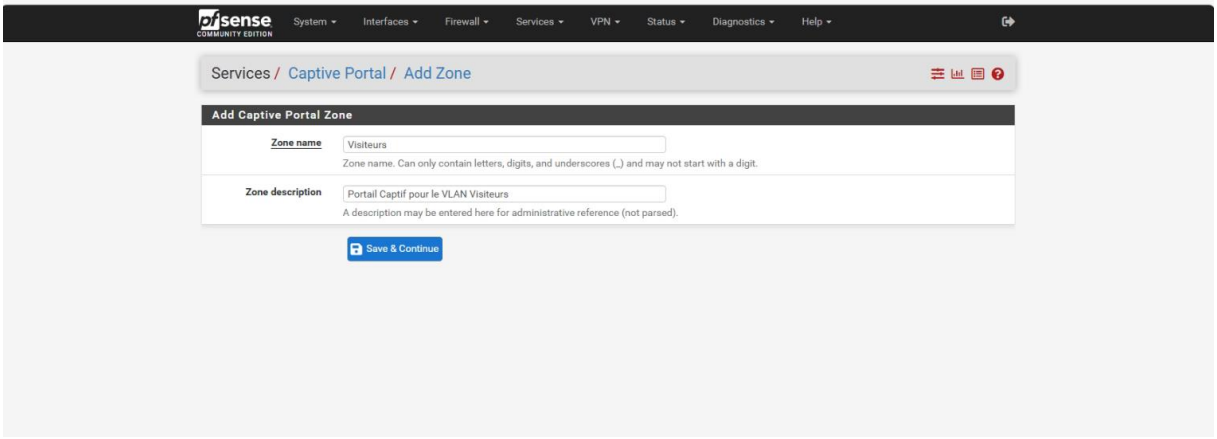
GSB dispose déjà d'un serveur pfSense opérationnel. Je me connecte via un navigateur en utilisant son adresse IP : ' 192.168.110.100 '



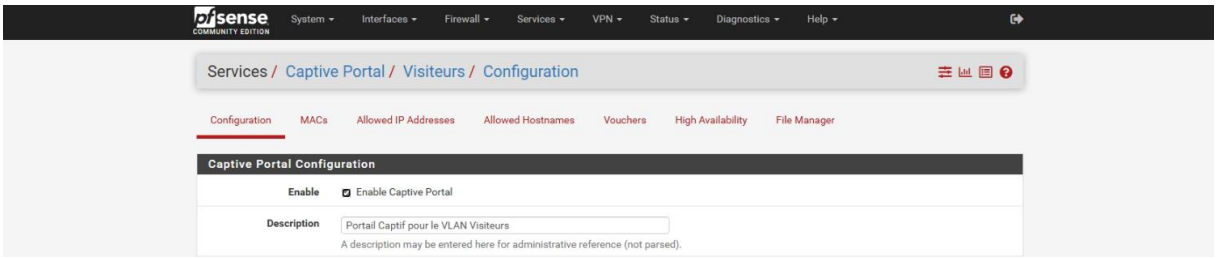
2. **Création d'une zone de portail captif**

Dans le menu principal, je me rends dans **Services > Captive Portal**, puis je clique sur **Add** pour créer une nouvelle zone, je vais nommer cette dernière 'Visiteurs'



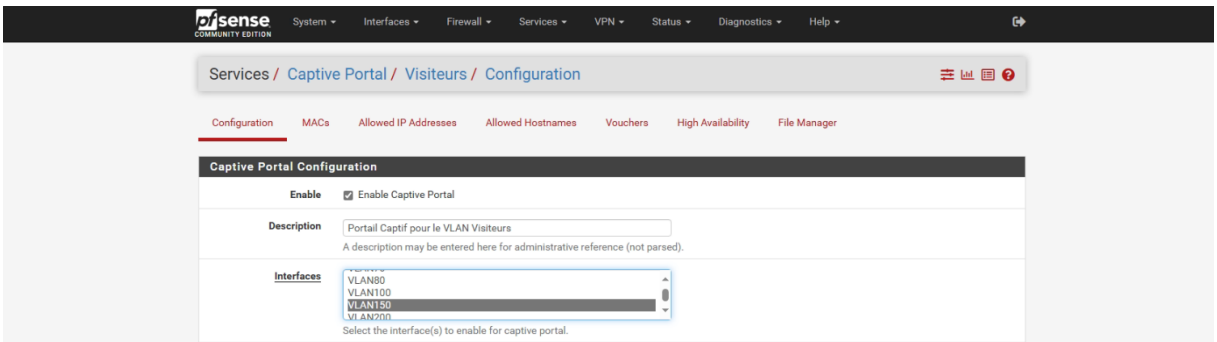


J'active ensuite la zone en cochant Enable Captive Portal.

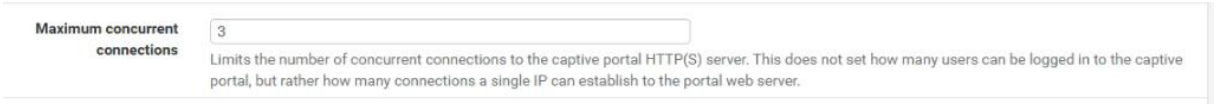


3. **Paramétrages clés**

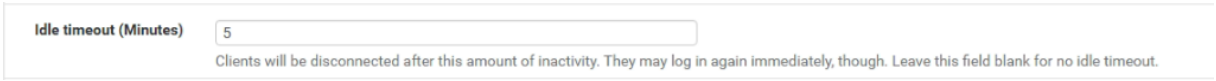
Je sélectionne l'interface sur laquelle je souhaite appliquer le portail captif, le VLAN150.



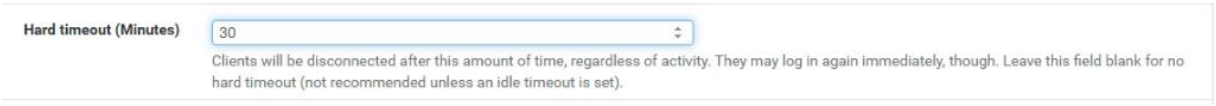
Je mets en place une limitation du le nombre de sessions sur le portail captif depuis la même adresse IP simultanément.



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



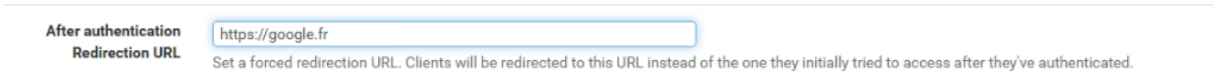
Je définis une durée maximale avant une déconnexion forcée, quelle que soit l'activité de l'utilisateur.



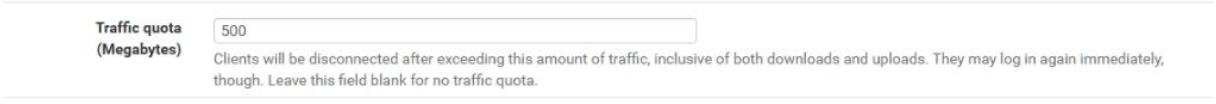
2. Configuration

1. **Redirection et bande passante**

Je choisis la page d'accueil de Google pour le renvoi de l'utilisateur une fois authentifié



Je choisis un quota d'utilisation de bande passante avant la déconnexion de l'utilisateur de 500 Megabytes en téléchargement et/ou en téléversement.

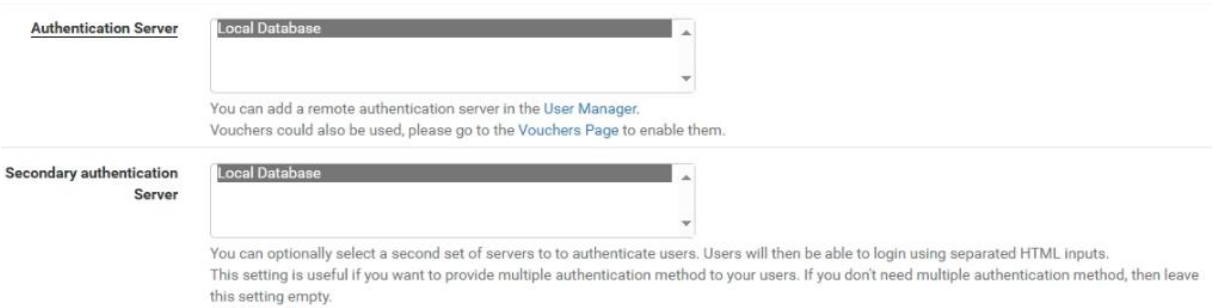


Je mets en place une limitation de débit par utilisateur connecté.

2. **Authentification**

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

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

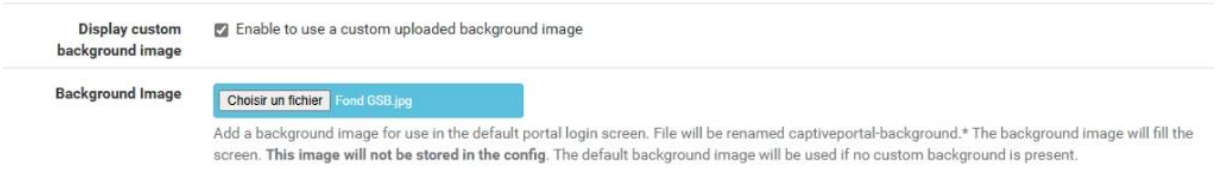


3. **Personnalisation de la page de connexion**

Je coche « Enable to use a custom uploaded log » afin de pouvoir téléverser le logo de GSB.

Je téléverse le logo.

J'active le fond customisé et téléverse un fond pour la page de login.

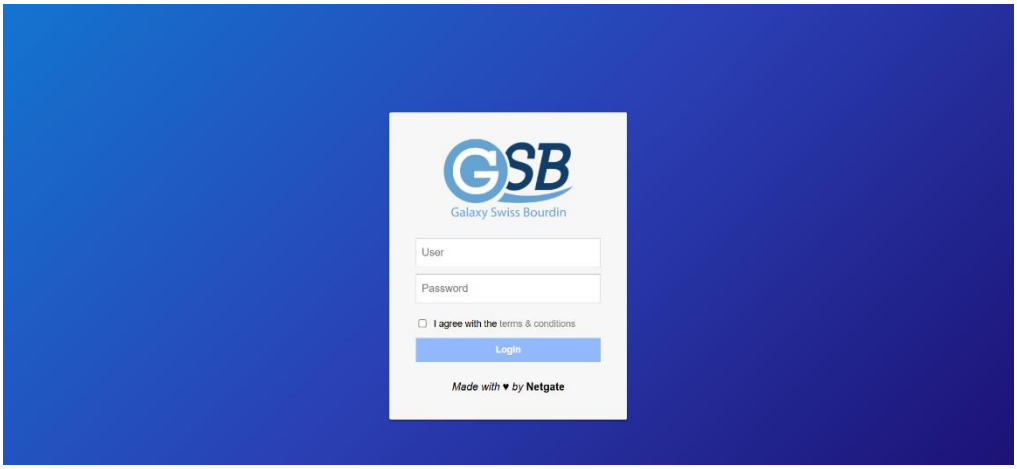


La configuration du portail captif est maintenant terminée, je passe à la phase de test.

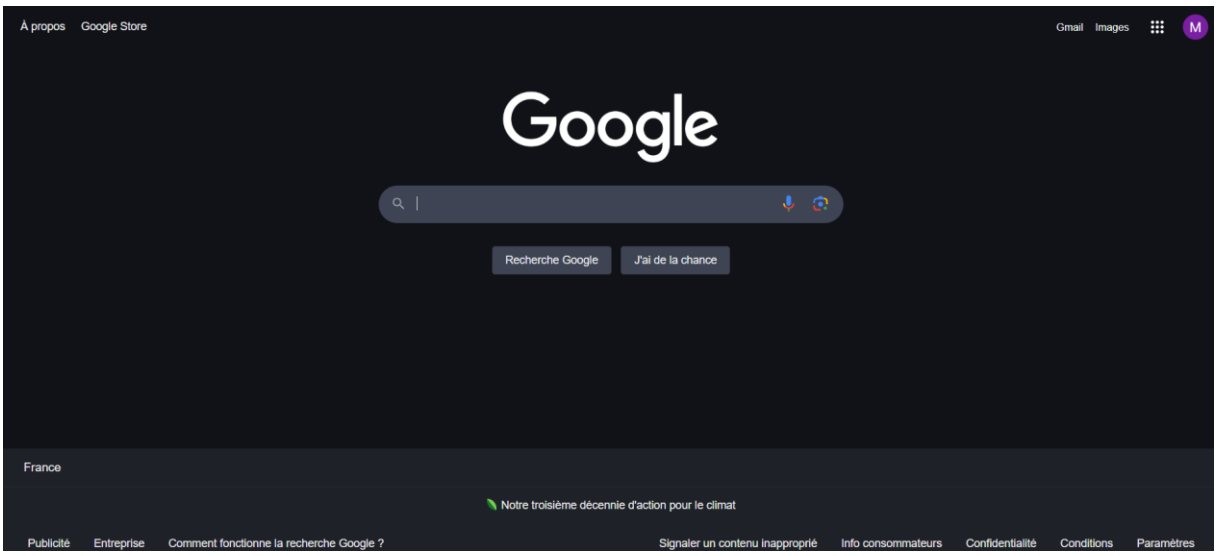
3. Test

1. Connexion depuis un VLAN dédié

Je connecte une machine de test sur le VLAN 150 et en 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 définie.



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.

VII. Conclusion

La mise en place d'un portail captif avec PfSense constitue une réponse adaptée aux besoins du laboratoire Galaxy Swiss Bourdin, qui souhaite sécuriser et contrôler l'accès à son réseau, notamment pour les invités ou les collaborateurs en mobilité.
Grâce à PfSense, GSB dispose d'un outil robuste, flexible et communautaire, minimisant les risques d'accès non autorisé tout en assurant une traçabilité des connexions. De futures évolutions, telles que l'intégration d'un serveur RADIUS ou la personnalisation complète des pages web, permettront d'optimiser davantage l'expérience utilisateur et la gestion du réseau, en ligne avec les exigences de sécurité et de conformité du groupe.

En définitive, le portail captif pfSense renforce la politique de sécurité globale de GSB et offre une base solide pour d'éventuelles extensions ou améliorations à moyen et long terme.