Ajili Faress
Aristee Formation
2022-2024

Réalisation Professionnelle : PORTAIL CAPTIF

Tables des matières

1. Introduction 3
1.1 Contexte 3
1.2 Besoin : Mise en place d'un portail captif 3
2. Choix de la technologie 4
2.1 Différents portails captifs : 4
2.2 Pourquoi PFSENSE? 5
3. Schémas Réseau : 5
3.1 Schéma réseau GSB 5
3.2 Schéma réseau RP 6
4. Matériel à Disposition 7
5. Tableau d'Adressage IP 8
6. Mise en Place et configuration du portail captif 9
7. Evolution possible 17
8. Conclusion 17

1. Introduction

1.1 Contexte

Le laboratoire Galaxy Swiss Bourdin (GSB), issu de la fusion entre Galaxy et Swiss Bourdin, est devenu un leader mondial en 2009. Basé à Paris, GSB a choisi la France pour améliorer le suivi de ses activités de visite médicale, tout en ayant son siège social à Philadelphie, aux États-Unis. J'interviens en tant qu'administrateur système et réseau au sein de ce groupe.

1.2 Besoin : Mise en place d'un portail captif

Le laboratoire Galaxy Swiss Bourdin (GSB) a besoin de mettre en place un portail captif, pour plusieurs raisons cruciales liées à la gestion et à la sécurité de son infrastructure informatique.

Voici quelques motifs :

•**Authentification des utilisateurs :** le portail captif permet aux administrateurs réseau de mettre en place des mécanismes d'authentification tels que les noms d'utilisateur et les mots de passe, ou des méthodes plus avancées

•**Contrôle d'accès :** ils permettent aux administrateurs de définir des règles d'accès, telles que la limitation du temps de connexion, la bande passante disponible ou l'accès restreint à certains services ou sites web.

•**Sécurité renforcée :** les portails captifs peuvent contribuer à renforcer la sécurité en garantissant que tous les utilisateurs sont authentifiés et en empêchant l'accès non autorisé au réseau. Cela peut aider à protéger les réseaux contre les attaques telles que le vol d'identité ou l'interception de données.

2. Choix de la technologie

Un portail captif est donc un outil efficace pour gérer l'accès au réseau, authentifier les utilisateurs et mettre en place des politiques de sécurité et d'utilisation, ce qui en fait un choix indispensable dans les environnements publics et privés où un contrôle d'accès est nécessaire.

2.1 Différents portails captifs :

Il existe plusieurs solutions pour mettre en place un portail captif, Propriétaire ou open-source.

Voici un tableau comparatif :

	NoCat	Talweg	Wifidog	Chillispot	Public IP	PfSense
Simplicité d'installation	🟢	🟡	🟡	🔴	🟡	🟡
Infrastructure nécessaire	🟢	🔴	🟡	🟡	🟢	🟢
Performances	🟢	🟢	🟢	🟡	🟢	🟢
Gestions utilisateurs	❌	🟢	🟡	🟢	🟡	🟢
Sécurité d'authentification	❌	🟢	🟢	🟢	🟢	🟢
Sécurité communications	❌	🟢	❌	❌	❌	🟡
Protocoles supportes	🟢	🔴	🟢	🟢	🟢	🟢
Crédit temps	❌	❌	❌	🟢	🟢	❌
Interface d'administration/Statistique	❌	🔴	🟢	🟢	🔴	🟢

❌	Non disponible
🟢 🟡 🔴	Plus au mois disponible

Figure 1 Tableau des différentes solutions de portail captif

2.2 Pourquoi PFSENSE ?

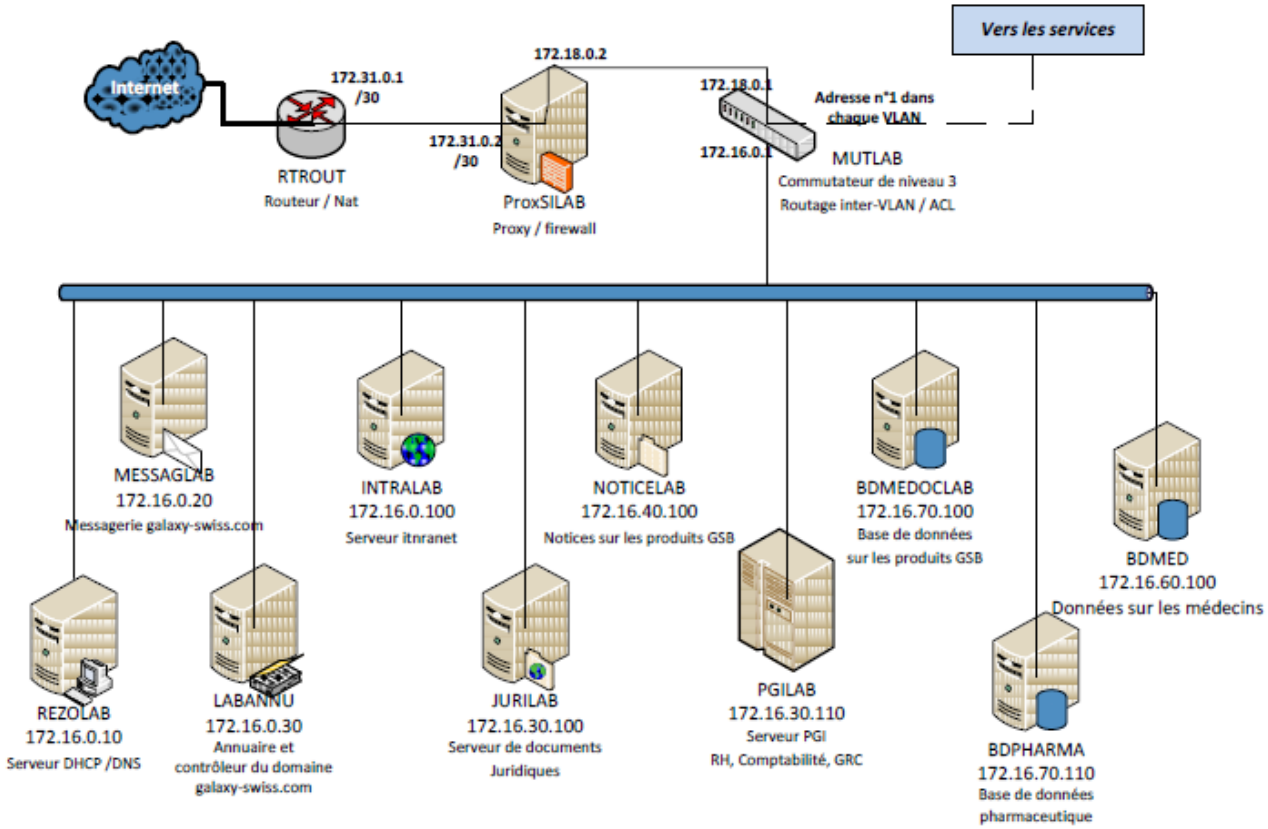
PfSense est une distribution routeur/pare-feu OpenSource basée sur FreeBSD, pouvant être installée sur un simple ordinateur personnel comme sur un serveur, il est réputé pour sa fiabilité.

Après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN.

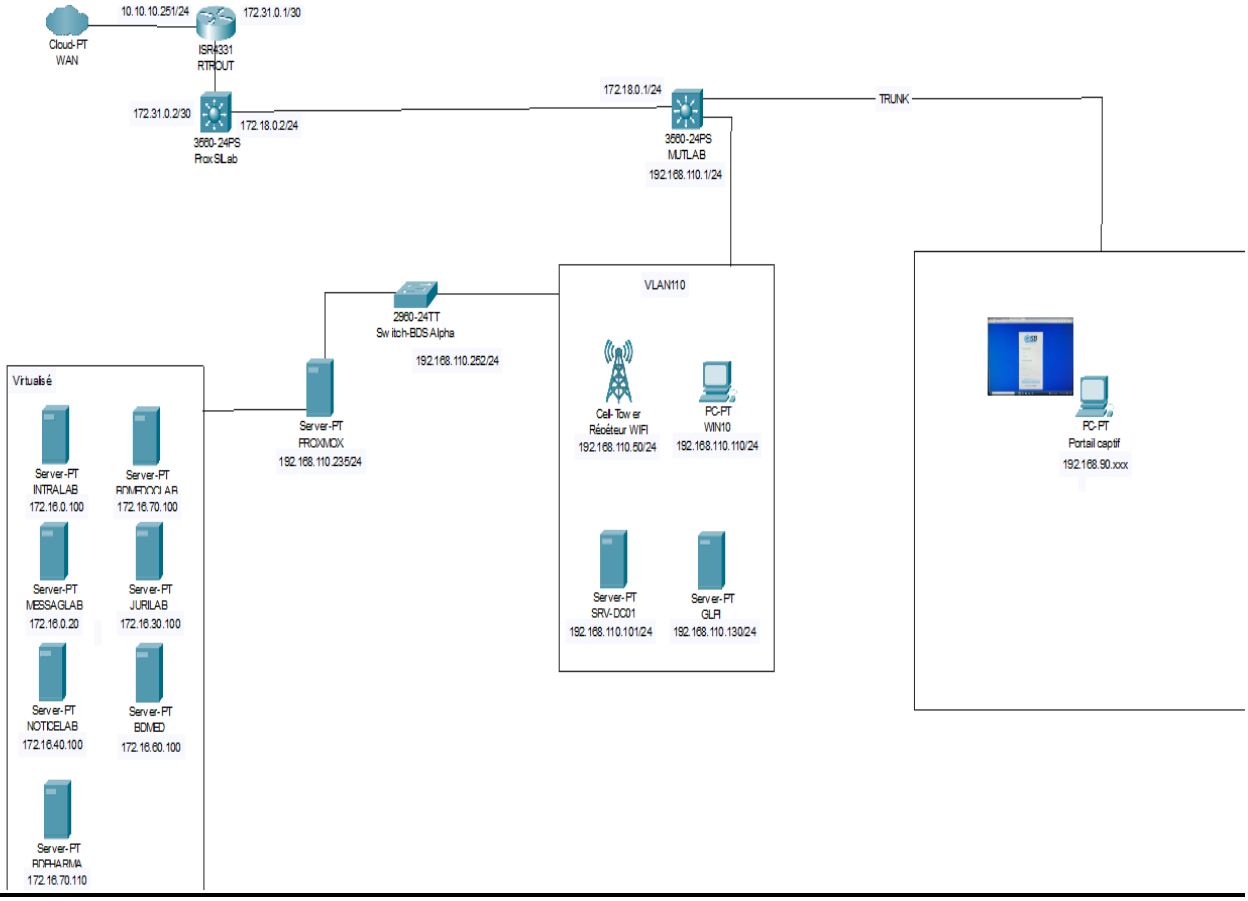
De plus j'utilise cette solution car je m'appuis sur l'infrastructure GSB déjà existante et contenant également un proxSylab (192.168.110.100) mis en place et fonctionnel.

3. Schémas Réseau du contexte :

3.1 Schéma réseau GSB



3.2 Schéma réseau de la réalisation professionnelle



4. Matériel à Disposition

Afin de mettre en place ma réalisation professionnelle, j'ai à ma disposition au sein de l'entreprise GSB le matériel suivant :

- Un hyperviseur de type 1, Proxmox, hébergeant les machines virtuelles du contexte
- Un routeur (RTROUT)
- Un pare-feu ProxSilab (Pfsense)
- Plusieurs switches de niveau 3 (Cisco 3750 G et 3560 G)
- Un Switch BDS niveau 2 (Cisco 2960)
- Un hyperviseur de type 1, proxmox hébergeant entre autres les machines de mes réalisations professionnelles
- Un point d'accès (Gsb alpha)
- Plusieurs ordinateurs pour effectuer les simulations et les tests

5. Tableau d'Adressage IP des VLAN

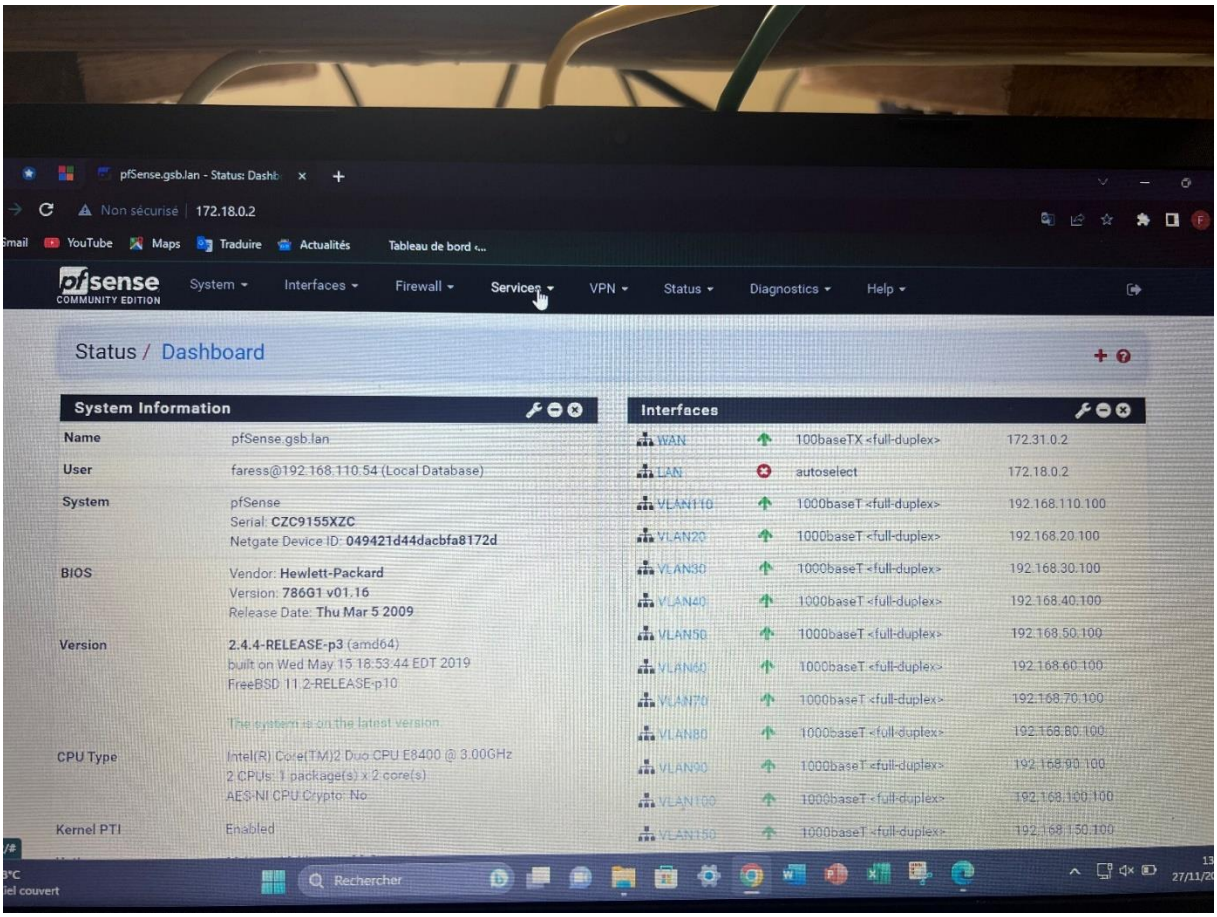
ID VLAN	Services	Passerelle VLAN
110	Réseau & Système	192.168.110.100/24
20	Direction / DSI	192.168.20.100/24
30	RH/Compta / Juridique/Secretariat	192.168.30.100/24
40	Communication / Rédaction	192.168.40.100/24
50	Développement	192.168.50.100/24
60	Commercial	192.168.60.100/24
70	Labo-Recherche	192.168.70.100/24
80	Deploiment	192.168.80.100/24
90	Salle de formation	192.168.90.100/24
100	Accueil	192.168.150.100/24
150	Visiteurs	192.168.150.100/24
200	Démonstration	192.168.200.100/24
300	Serveurs	172.16.0.100/17
400	Sorties	172.19.0.1/24

Figure 2 Tableau d'adressage IP des VLAN

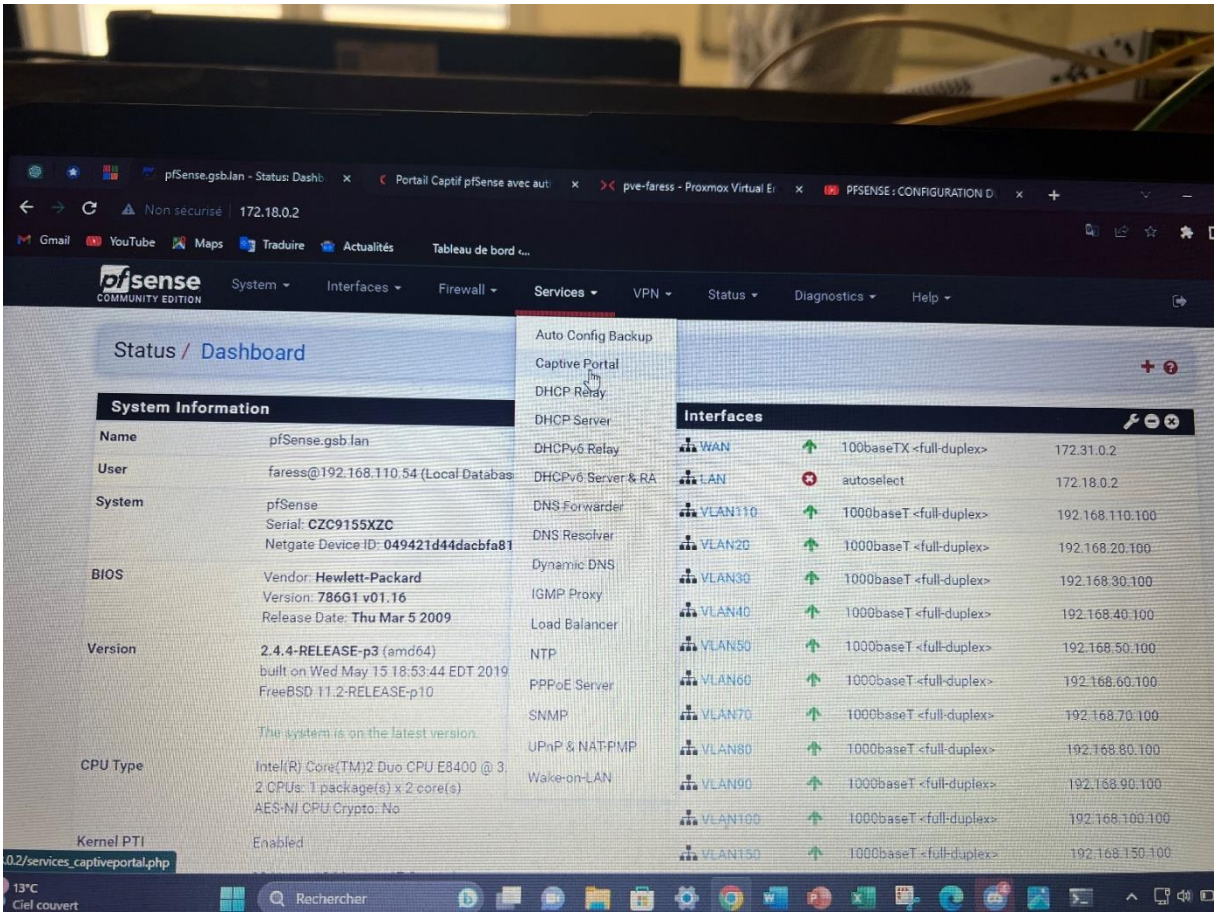
6. Mise en Place et configuration du portail captif

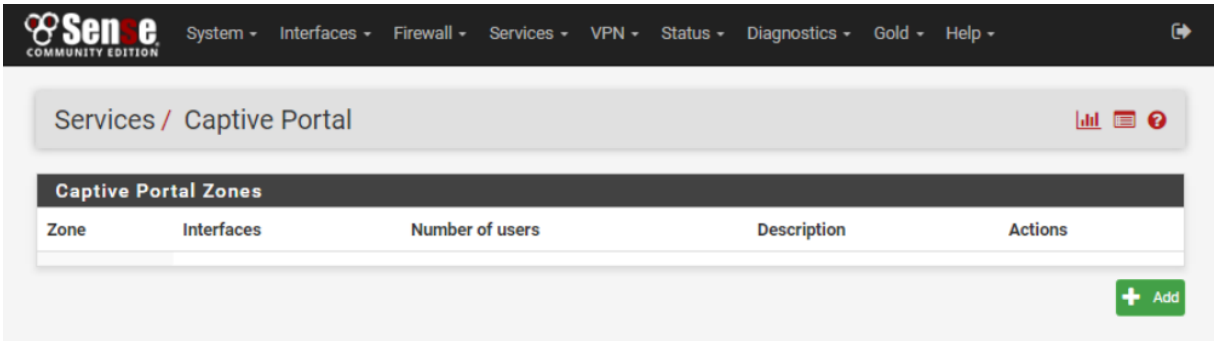
Premièrement je me connecte au Pfsense existant en rentrant dans la barre de recherche l'adresse suivante : 172.18.0.2

Une fois connecté à notre Pfsense on a notre tableau de bord :

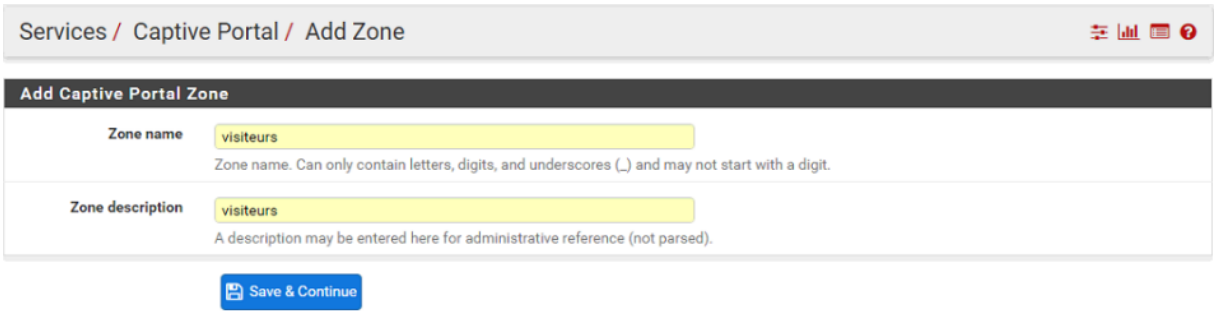


Ensuite il faut aller dans Services, puis Captive Portal et cliquer sur Add pour créer une nouvelle zone

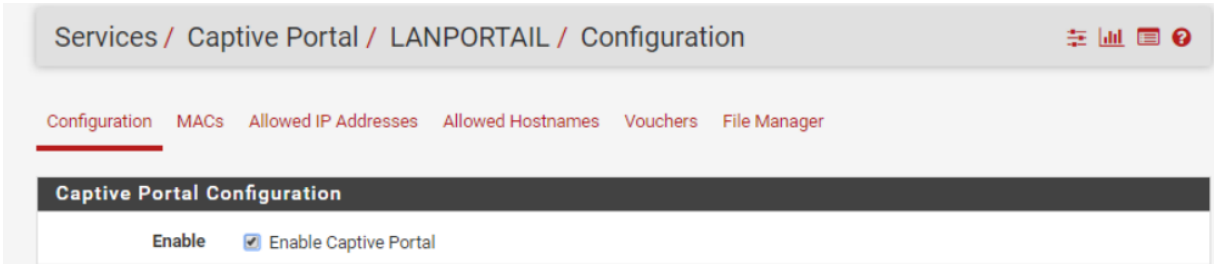




Je donne un nom à la zone créée, la description n'ai pas obligatoire dans notre cas je le nommerai « visiteurs » :



Une fois le portail créer, il faut l'activer en cochant « enable Captive Portal » :



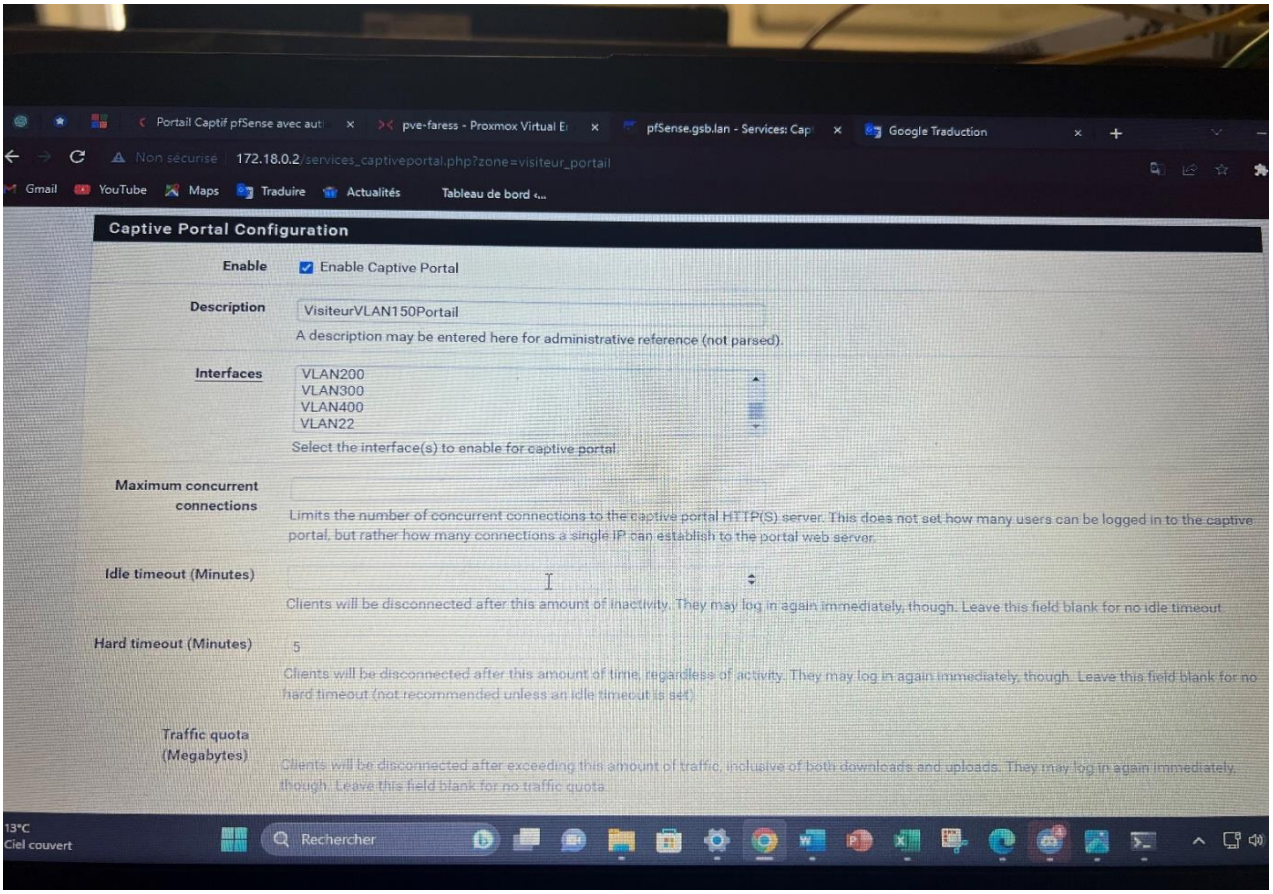
Une fois activé tous les paramètres de configuration du portail apparaissent, les différentes configurations :

• Interfaces : Cette option permet de définir sur quelle interface le portail captif sera exploité. Pour cela, il faut cliquer sur l'interface correspondant dans notre cas : « VLAN 90 ».

• Maximum concurrent connections : Cette option permet de limiter le nombre de connexions en même temps sur le portail captif. Si cette limite est dépassée, les autres clients ne pourront pas accéder au portail captif, jusqu'à ce qu'une place se libère.

• Idle timeout : Cette option démontre le délai (en minutes) à laquelle les clients seront déconnectés s'ils n'ont pas effectué leur activité.

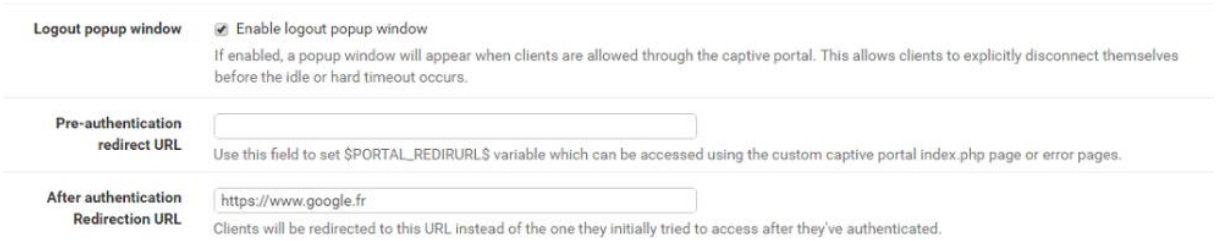
• Hard timeout : Cette option démontre le délai (en minutes) pour forcer la déconnexion des utilisateurs, peu importe leur activité.



Juste en dessous on peut configurer les paramètres suivants comme nous pouvons le voir sur l'image suivante :

- Logout popup window : page de session où les visiteurs devront entrer leurs identifiants

- After authentification Redirection URL (page où les utilisateurs qui se connectent seront redirigé, ici https://google.fr)

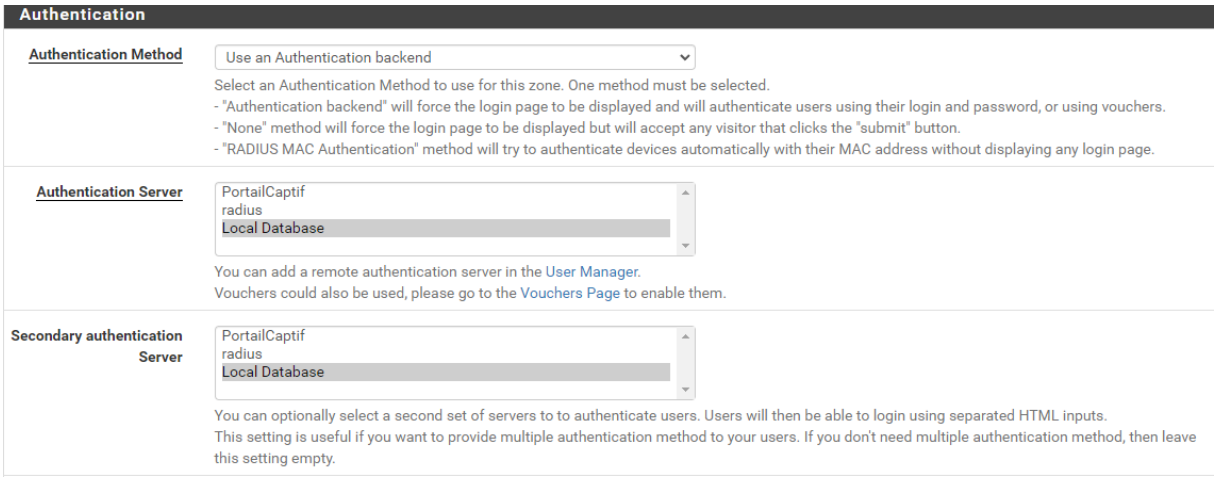


Puis, la mise en place de quota de débits (entrants/sortants) est importante, ce qui permet d'assurer une qualité de service fiable. Pour cela, il faut cocher la case "Enable per-user bandwidth restriction" (dans Peruser bandwidth restriction).

Ensuite dans la partie Authentification un peu plus bas

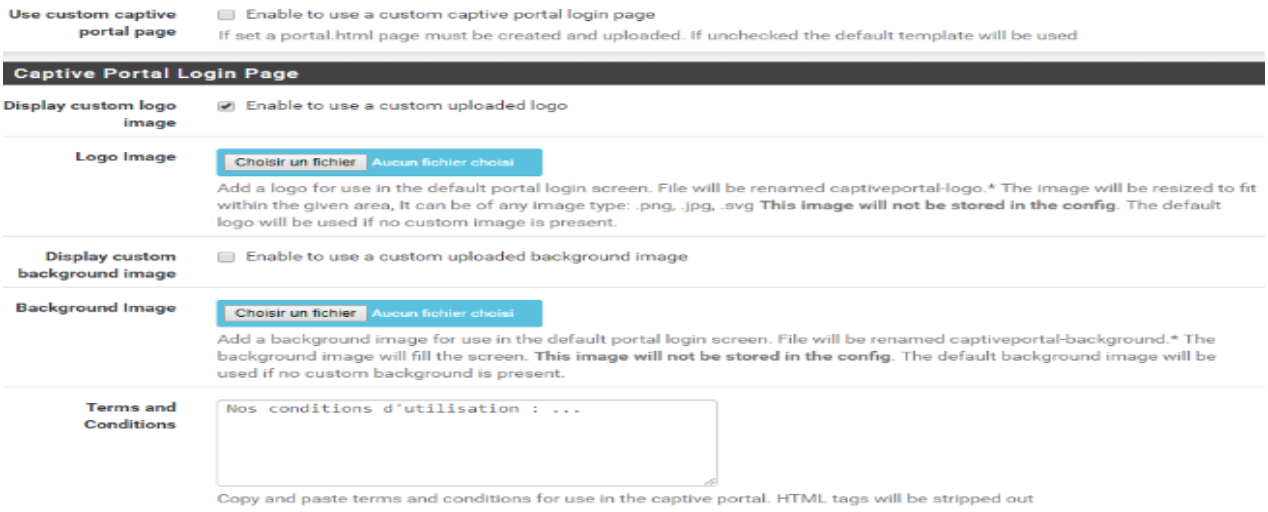
-Méthode d'authentification : Use an Authentication backend

-Serveur d'authentification : localdatabase



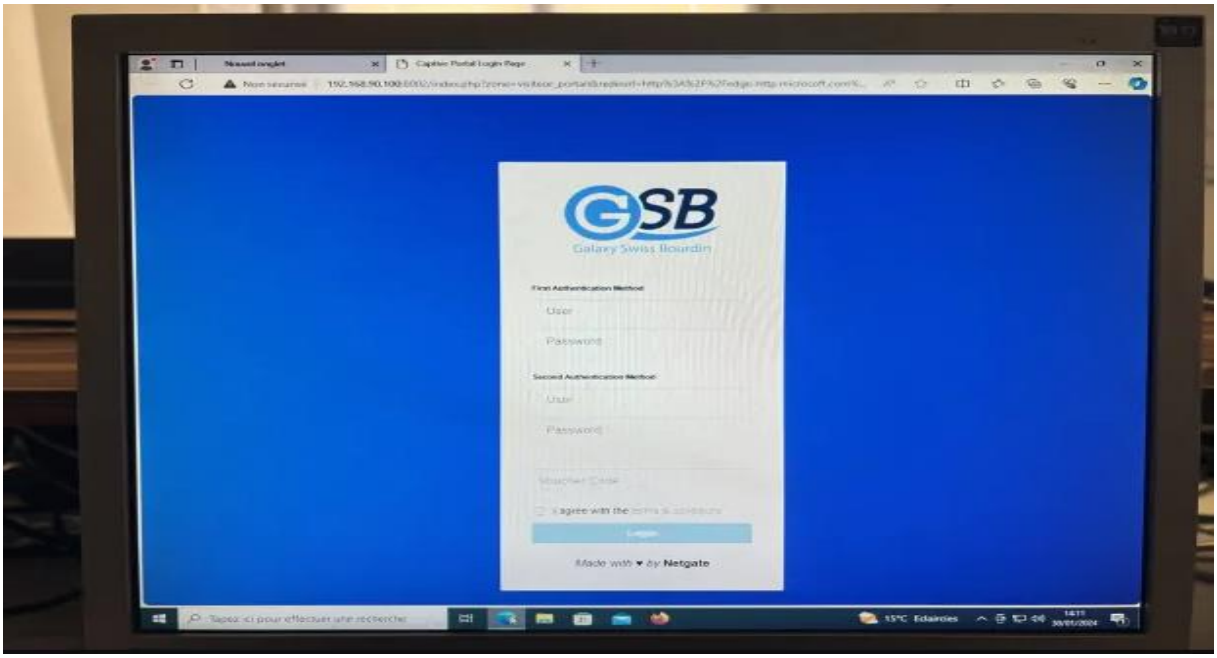
La page de connexion de votre portail captif est totalement personnalisable. Depuis l'interface pfSense, dans les paramètres du portail captif (Services > Portail Captif), vous pouvez :

- Changer le design de la page HTML
- Ajouter un fond (background)
- Changer de logo
- Ajouter les conditions d'utilisation

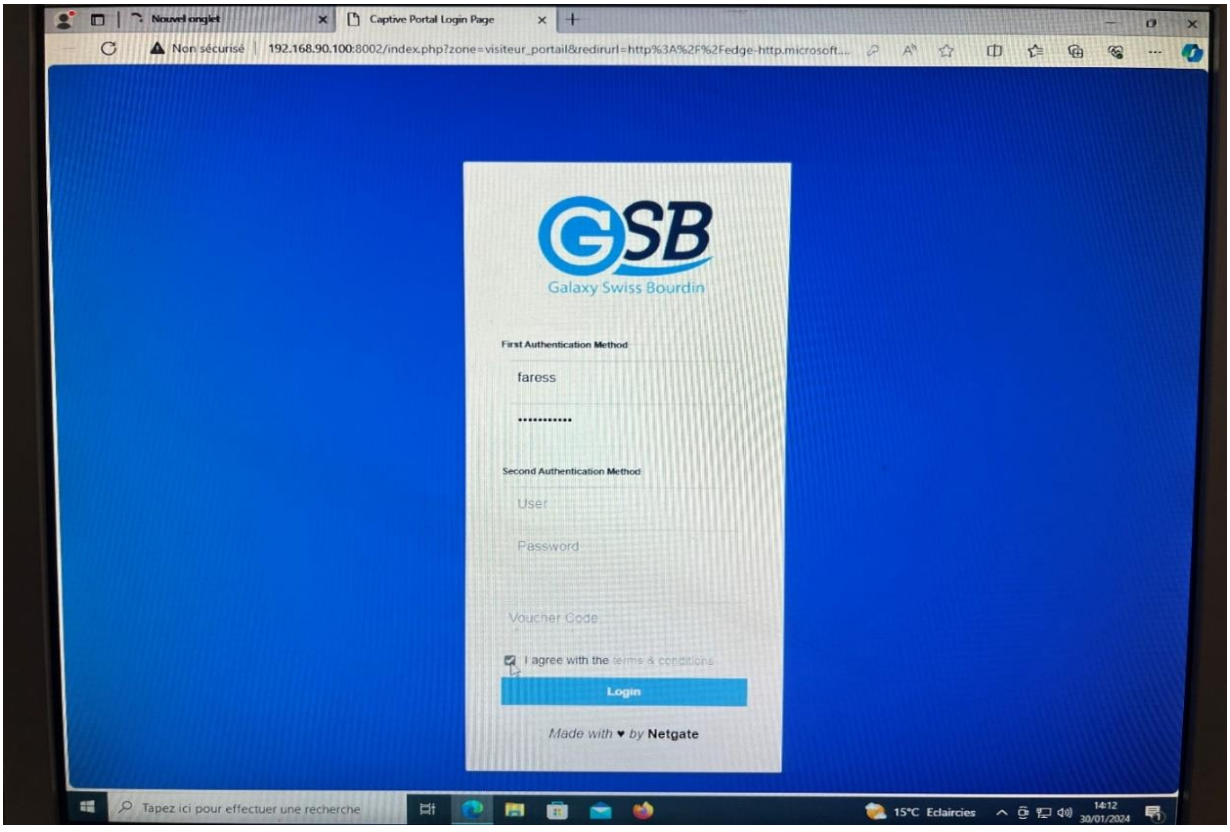


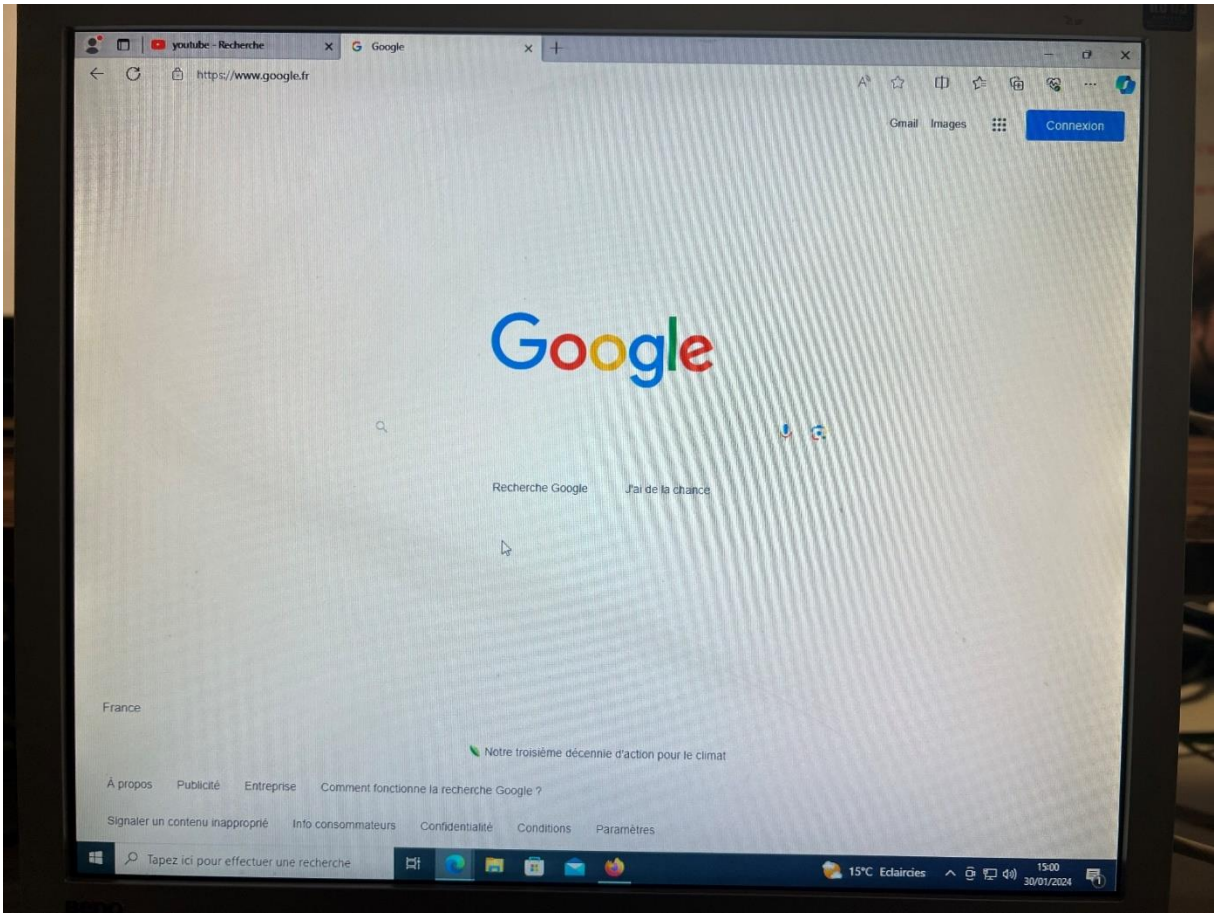
Ensuite je teste mon portail captif :

Pour cela je me connecte via un pc à disposition dans la salle informatique je me branche en réseau sur le bon VLAN donc 90 et en essayant de naviguer sur internet la page du portail captif apparait comme nous pouvons le voir dans l'image suivante :



Je test avec mes identifiants





Voilà la page de redirection que l'on a configurer après l'authentification des utilisateurs en amont.

7. Evolution possible

Une évolution possible avec ma réalisation professionnelle, serait l'installation du portail captif avec authentification radius.

Radius est un protocole de gestion d'authentification et d'autorisation de connexion à un réseau, Il permet une gestion centralisée des connexions d'utilisateurs et des politiques de sécurité, en offrant une traçabilité des activités pour les utilisateurs.

Cette implémentation est prise en charge par un serveur windows.

8. Conclusion

Le portail captif est une application chargée de contrôler et de gérer de manière automatisée l'accès des utilisateurs aux réseaux wifi ; qu'ils soient publics ou privés. Ainsi, les portails captifs sont couramment utilisés dans les réseaux à accès ouvert. Ces mêmes réseaux wifi disponibles dans les magasins, les centres commerciaux, les hôpitaux, les aéroports, etc.

Le portail captif permet donc aux administrateurs du réseau wifi de fournir un accès à l'internet. Au préalable, l'utilisateur doit y renseigner les informations permettant de l'identifier.