

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 supportés	+	-	+	+	+	+
Crédit temps	+	-	-	+	+	-
Interface d'administration/Statistique	+	-	+	+	-	+

Legend:

	Non disponible
	Plus au moins disponible

Figure 1 Tableau des différentes solutions de portail captif

2.2 Pourquoi PFSENSE ?

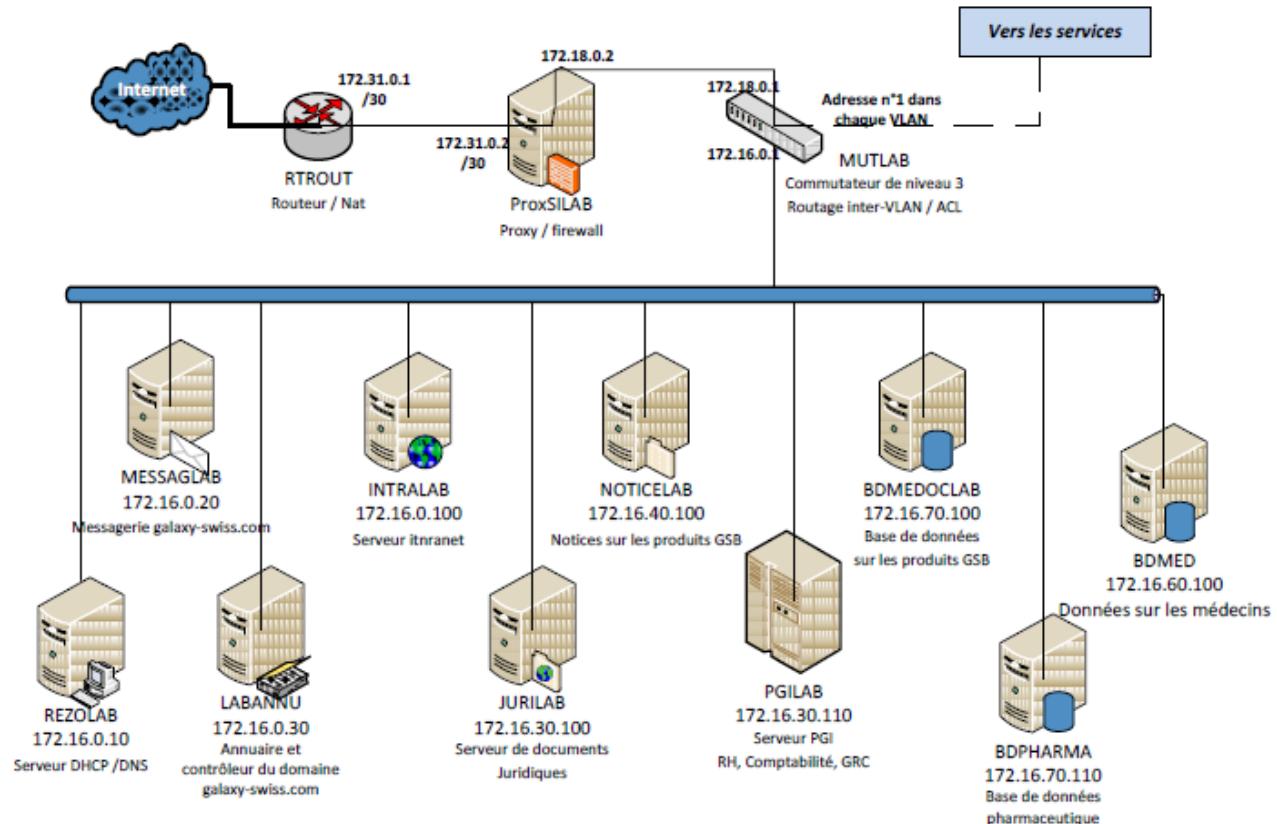
PfSense est une distribution routeur/pare-feu OpenSource basée sur FreeBSD, pouvant être installée sur un simple ordinateur personnel comme sur un serveur, il est réputé pour sa fiabilité.

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

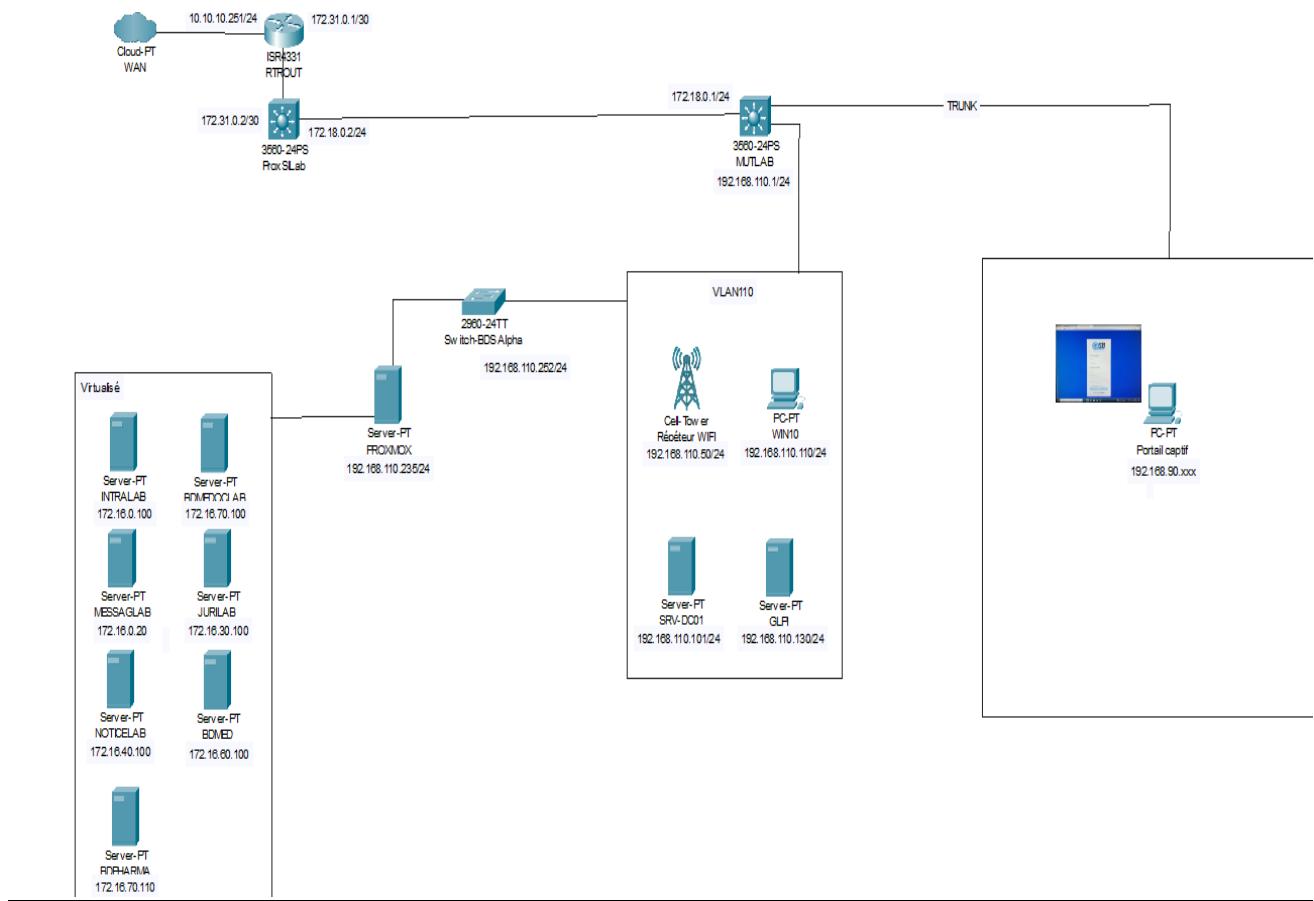
De plus j'utilise cette solution car je m'appuie sur l'infrastructure GSB déjà existante et contenant également un proxSylab (192.168.110.100) mis en place et fonctionnel.

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

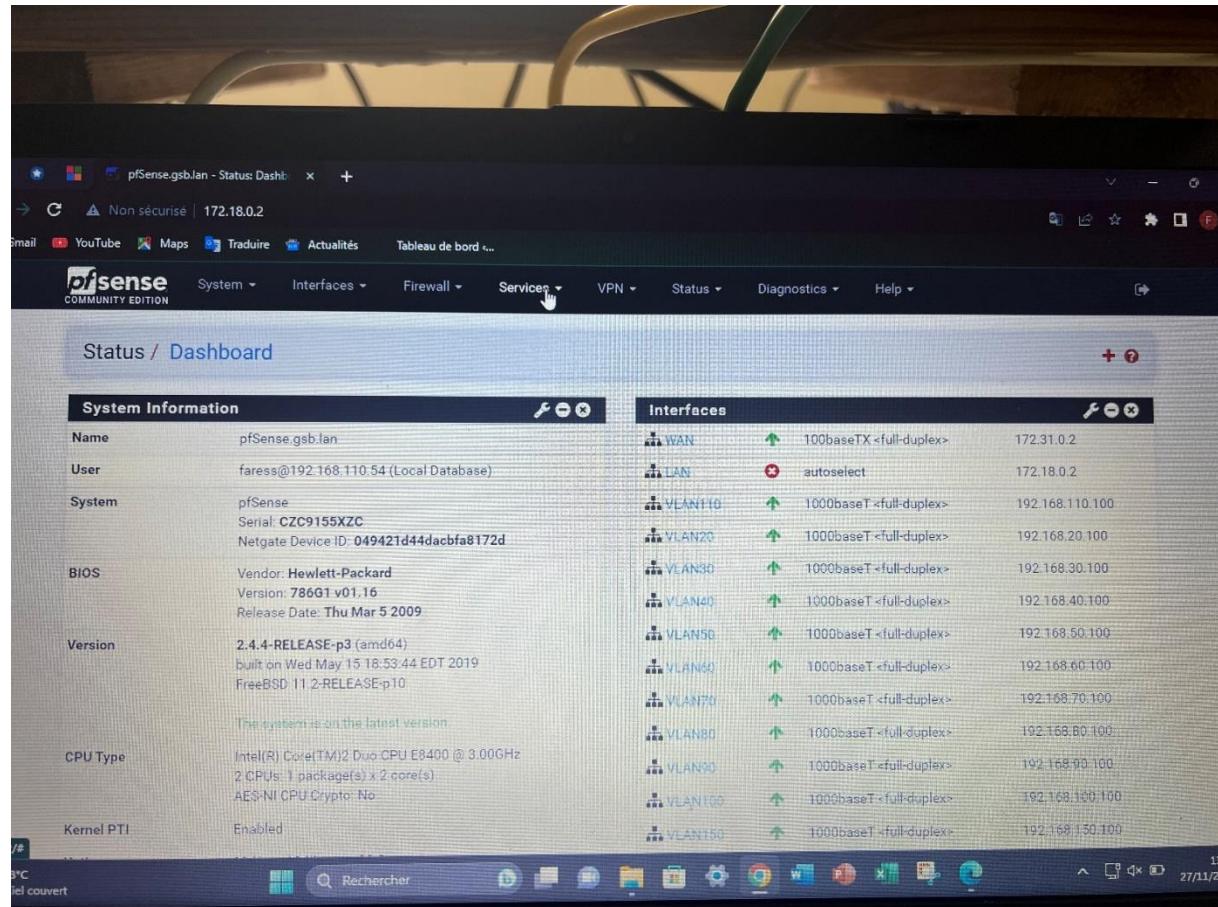
ID VLAN	Services	Passerelle VLAN
110	Réseau & Système	192.168.110.100/24
20	Direction / DSI	192.168.20.100/24
30	RH/Compta / Juridique/Secretariat	192.168.30.100/24
40	Communication / Rédaction	192.168.40.100/24
50	Développement	192.168.50.100/24
60	Commercial	192.168.60.100/24
70	Labo-Recherche	192.168.70.100/24
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 :



The screenshot shows the pfSense Status Dashboard. The top navigation bar includes links for Email, YouTube, Maps, Traduire, Actualités, and Tableau de bord. The main menu bar has links for System, Interfaces, Firewall, Services (which is currently selected), VPN, Status, Diagnostics, and Help. The left sidebar shows the pfSense logo and the text "COMMUNITY EDITION". The main content area is titled "Status / Dashboard". It contains two tables: "System Information" and "Interfaces".

System Information		
Name	pfSense.gsb.lan	
User	fares@192.168.110.54 (Local Database)	
System	pfSense Serial: CZC9155XZC Netgate Device ID: 049421d44dacbfa8172d	
BIOS	Vendor: Hewlett-Packard Version: 786G1 v01.16 Release Date: Thu Mar 5 2009	
Version	2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10	
CPU Type:	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: No	
Kernel PTI	Enabled	

Interfaces		
WAN	100baseTX <full-duplex>	172.31.0.2
LAN	autoselect	172.18.0.2
VLAN10	1000baseT <full-duplex>	192.168.110.100
VLAN20	1000baseT <full-duplex>	192.168.20.100
VLAN30	1000baseT <full-duplex>	192.168.30.100
VLAN40	1000baseT <full-duplex>	192.168.40.100
VLAN50	1000baseT <full-duplex>	192.168.50.100
VLAN60	1000baseT <full-duplex>	192.168.60.100
VLAN70	1000baseT <full-duplex>	192.168.70.100
VLAN80	1000baseT <full-duplex>	192.168.80.100
VLAN90	1000baseT <full-duplex>	192.168.90.100
VLAN100	1000baseT <full-duplex>	192.168.100.100
VLAN150	1000baseT <full-duplex>	192.168.150.100



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

The screenshot shows the pfSense 2.4.4-RELEASE-p3 dashboard. The left sidebar has 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The main area has a 'Status / Dashboard' header. The 'System Information' section contains details like Name (pfSense.gsb.lan), User (faress@192.168.110.54), System (pfSense), BIOS (Vendor: Hewlett-Packard, Version: 786G1 v01.16, Release Date: Thu Mar 5 2009), Version (2.4.4-RELEASE-p3), CPU Type (Intel(R) Core(TM)2 Duo CPU E8400 @ 3.2 GHz, AES-NI CPU Crypto: No), and Kernel PTI (Enabled). The 'Interfaces' section lists the following ports and their configurations:

Interface	Description	IP Address
WAN	100baseTX <full-duplex>	172.31.0.2
LAN	autoselect	172.18.0.2
VLAN10	1000baseT <full-duplex>	192.168.110.100
VLAN20	1000baseT <full-duplex>	192.168.20.100
VLAN30	1000baseT <full-duplex>	192.168.30.100
VLAN40	1000baseT <full-duplex>	192.168.40.100
VLAN50	1000baseT <full-duplex>	192.168.50.100
VLAN60	1000baseT <full-duplex>	192.168.60.100
VLAN70	1000baseT <full-duplex>	192.168.70.100
VLAN80	1000baseT <full-duplex>	192.168.80.100
VLAN90	1000baseT <full-duplex>	192.168.90.100
VLAN100	1000baseT <full-duplex>	192.168.100.100
VLAN150	1000baseT <full-duplex>	192.168.150.100

The screenshot shows the Services / Captive Portal page. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', 'Gold', and 'Help'. The main area has a 'Services / Captive Portal' header. The 'Captive Portal Zones' table has the following columns: Zone, Interfaces, Number of users, Description, and Actions. A green 'Add' button is located at the bottom right of the table.

Zone	Interfaces	Number of users	Description	Actions
				+ Add



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

Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name	visiteurs
Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.	
Zone description	visiteurs
A description may be entered here for administrative reference (not parsed).	

Save & Continue

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

Services / Captive Portal / LANPORTAIL / Configuration

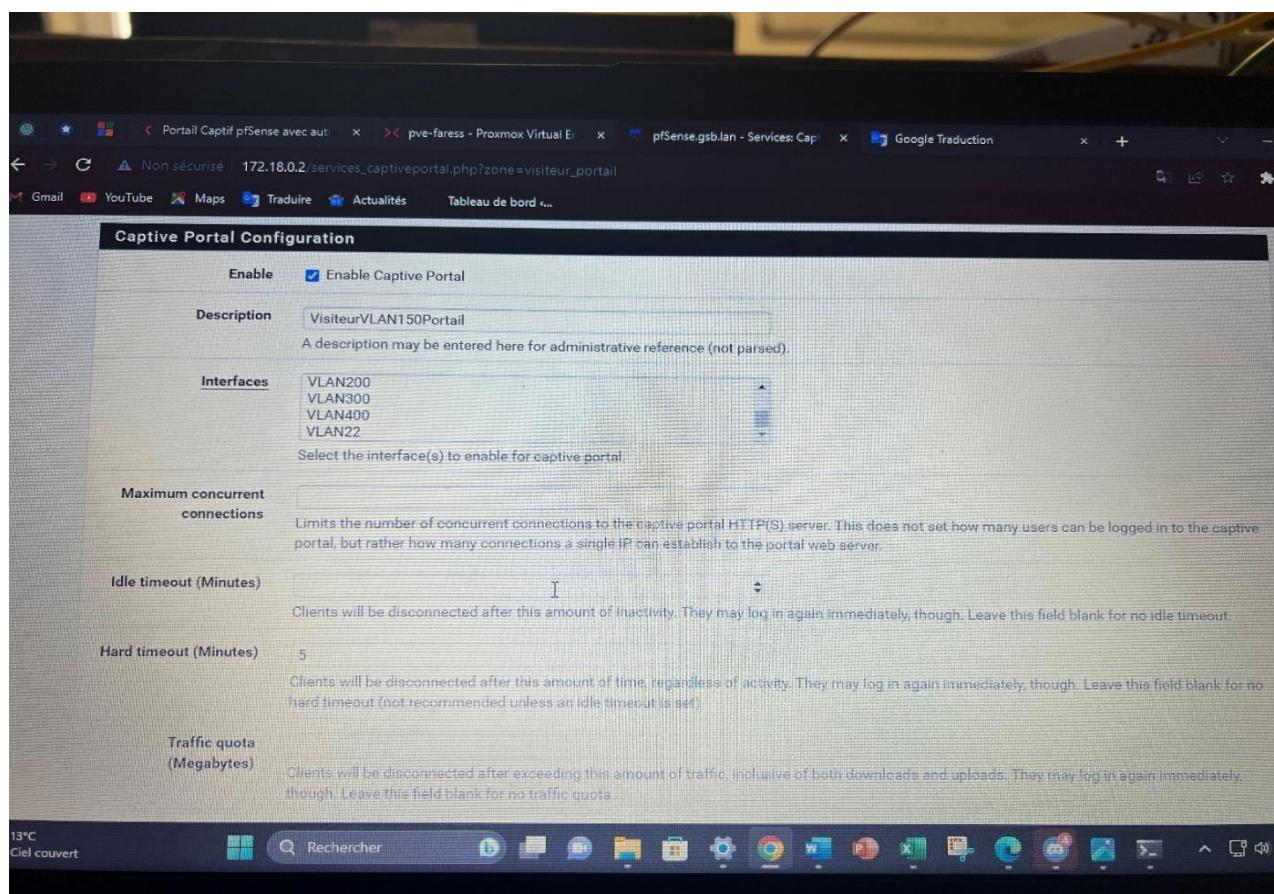
Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers File Manager

Captive Portal Configuration

Enable	<input checked="" type="checkbox"/> 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.



The screenshot shows the 'Captive Portal Configuration' page on a pfSense web interface. The configuration includes:

- Enable:** Checked.
- Description:** VisiteurVLAN150Portail.
- Interfaces:** VLAN200, VLAN300, VLAN400, VLAN22.
- Maximum concurrent connections:** 100.
- Idle timeout (Minutes):** 5.
- Hard timeout (Minutes):** 5.
- Traffic quota (Megabytes):** 0.

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 authentication Redirection URL (page où les utilisateurs qui se connectent seront redirigé, ici <https://google.fr>)

Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	<input type="text"/> Use this field to set \$PORTAL_REDIRURL\$ variable which can be accessed using the custom captive portal index.php page or error pages.
After authentication Redirection URL	<input type="text"/> https://www.google.fr Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

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).

Per-user bandwidth restriction	<input checked="" type="checkbox"/> Enable per-user bandwidth restriction
Default download (Kbit/s)	<input type="text"/> 10000
Default upload (Kbit/s)	<input type="text"/> 2000 If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty for no limit.

Ensuite dans la partie Authentification un peu plus bas

-Méthode d'authentification : Use an Authentication backend

-Serveur d'authentification : localdatabase

Authentication

Authentication Method	<input type="button" value="Use an Authentication backend"/> 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	<input type="button" value="PortalCaptive"/> <input type="button" value="radius"/> <input type="button" value="Local Database"/> You can add a remote authentication server in the User Manager . Vouchers could also be used, please go to the Vouchers Page to enable them.
Secondary authentication Server	<input type="button" value="PortalCaptive"/> <input type="button" value="radius"/> <input type="button" value="Local Database"/> You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

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

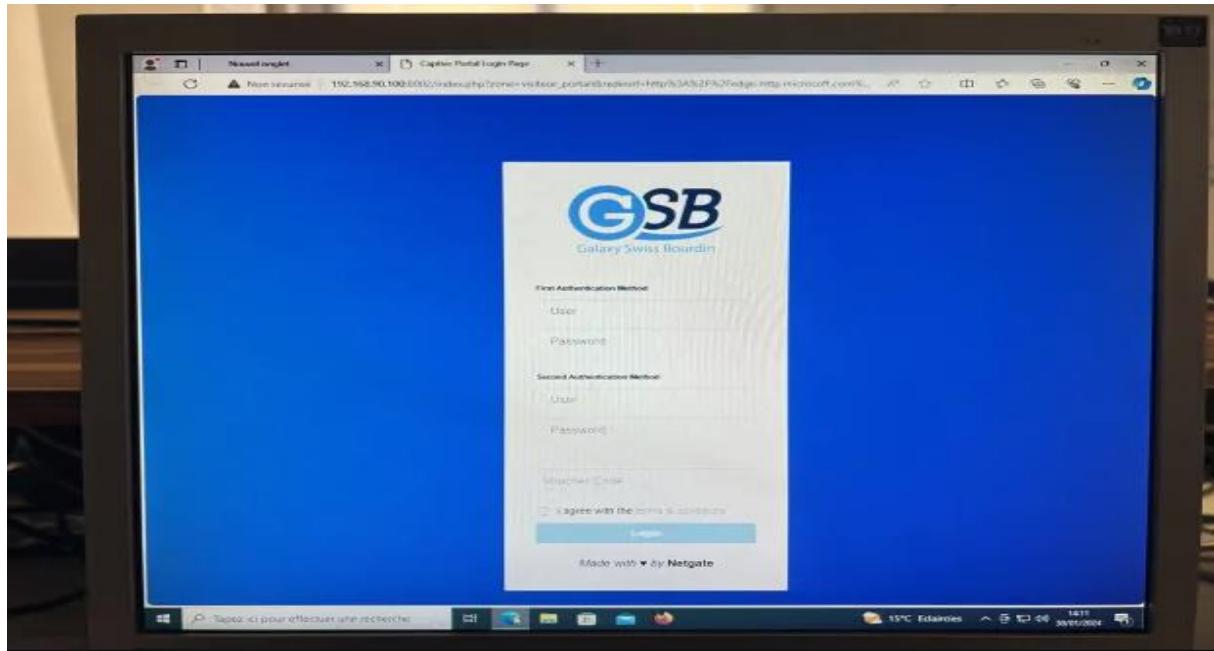
Use custom captive portal page Enable to use a custom captive portal login page
If set a portal.html page must be created and uploaded. If unchecked the default template will be used

Captive Portal Login Page

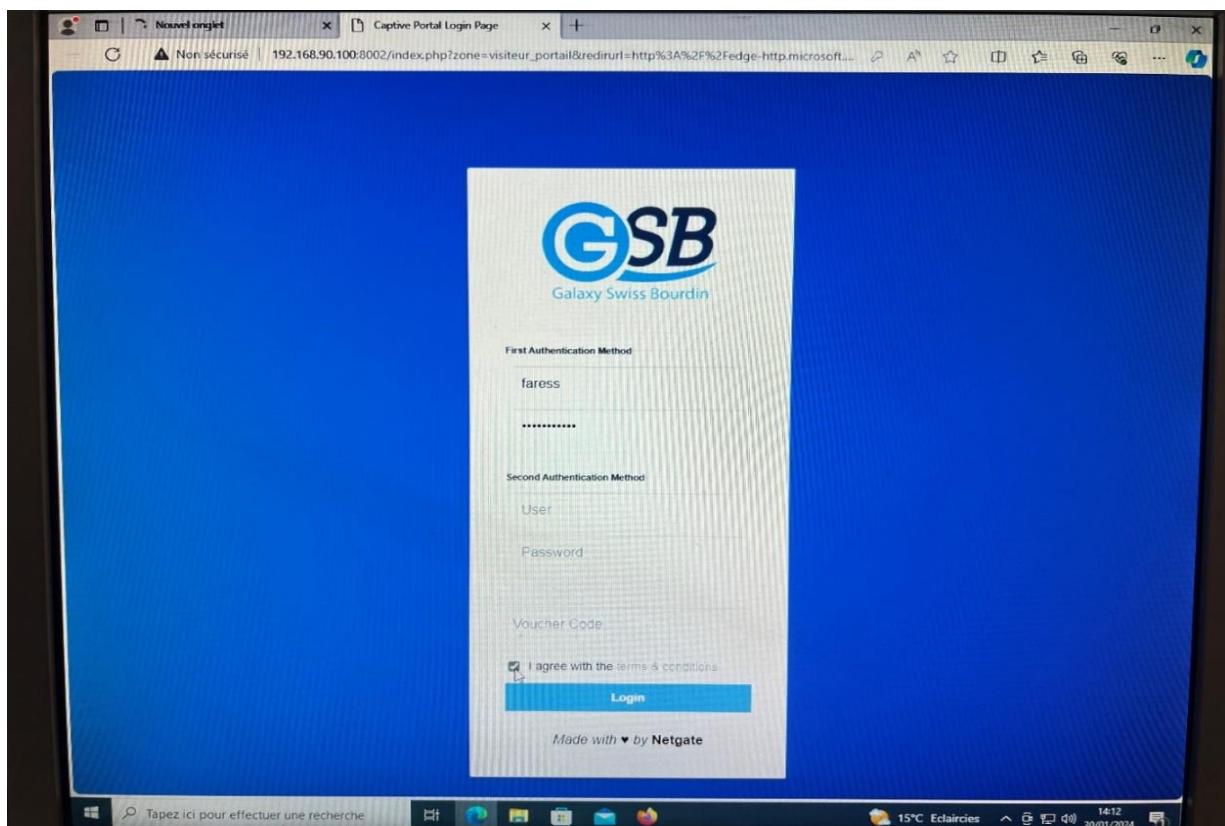
Display custom logo image	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
Logo Image	<input type="button" value="Choisir un fichier"/> Aucun fichier choisi Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, it can be of any image type: .png, .jpg, .svg This image will not be stored in the config. The default logo will be used if no custom image is present.
Display custom background image	<input type="checkbox"/> Enable to use a custom uploaded background image
Background Image	<input type="button" value="Choisir un fichier"/> Aucun fichier choisi Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. This image will not be stored in the config. The default background image will be used if no custom background is present.
Terms and Conditions	Nos conditions d'utilisation : ... Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

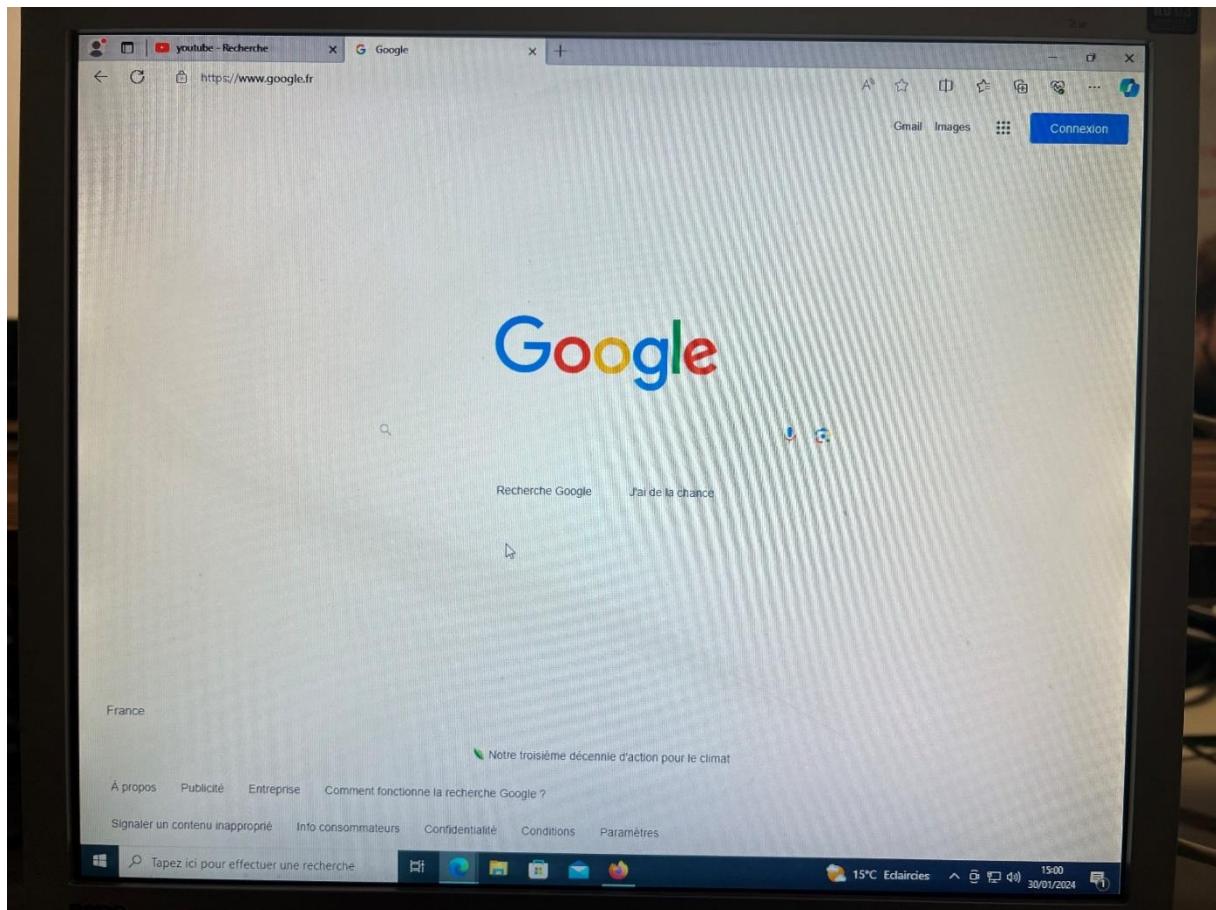
Ensuite je teste mon portail captif :

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.