

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

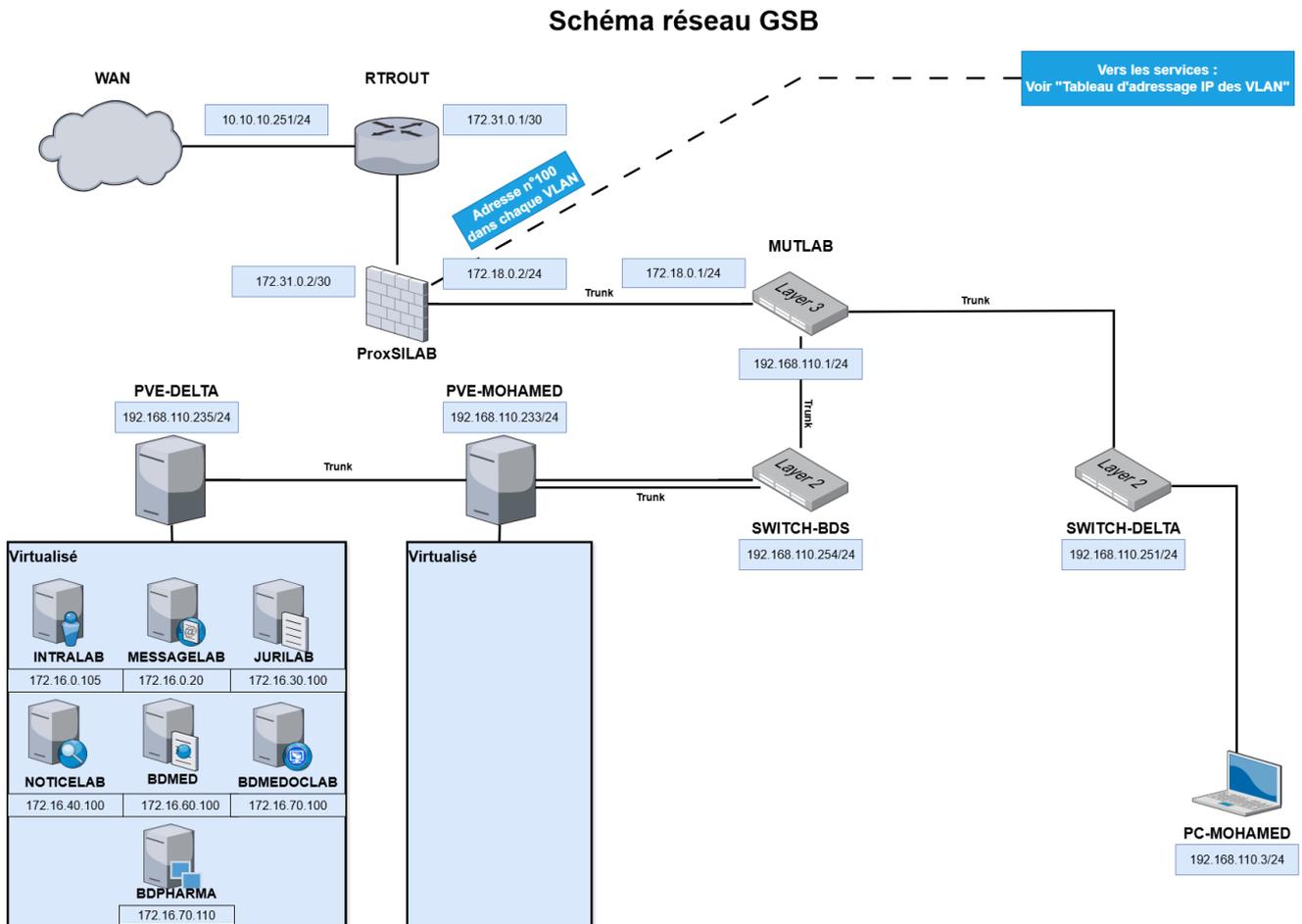
- **Simplicité d'utilisation** : L'accès via une interface web et la structure claire des menus facilitent la prise en main.
- **Modularité** : De nombreux packages peuvent être ajoutés (Squid, Snort, OpenVPN...).
- **Communauté dynamique** : Une documentation riche et réactive, des forums spécialisés,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

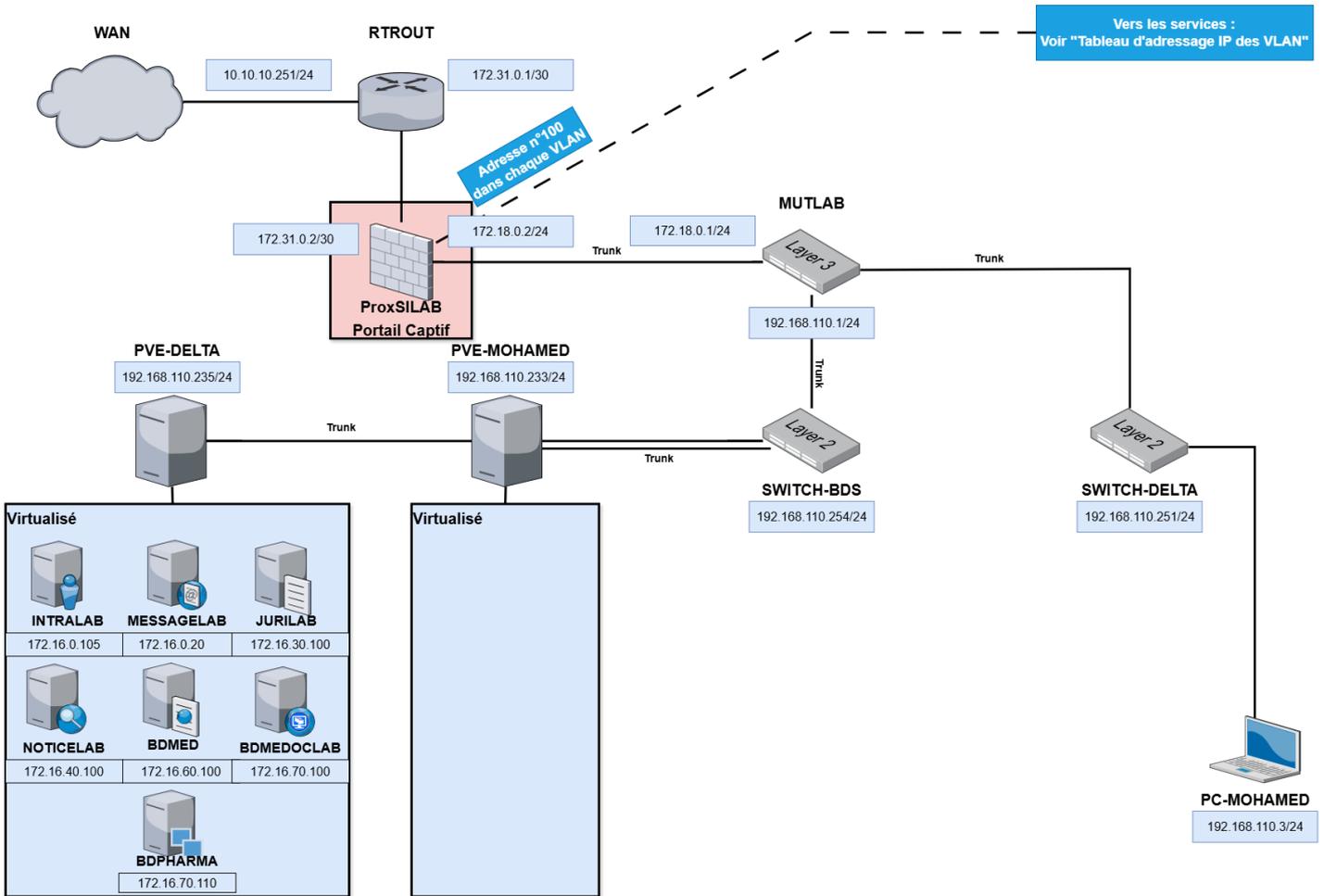


2. Tableau d'Adressage IP des VLAN

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

Schéma réseau GSB



4. Matériel à disposition

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

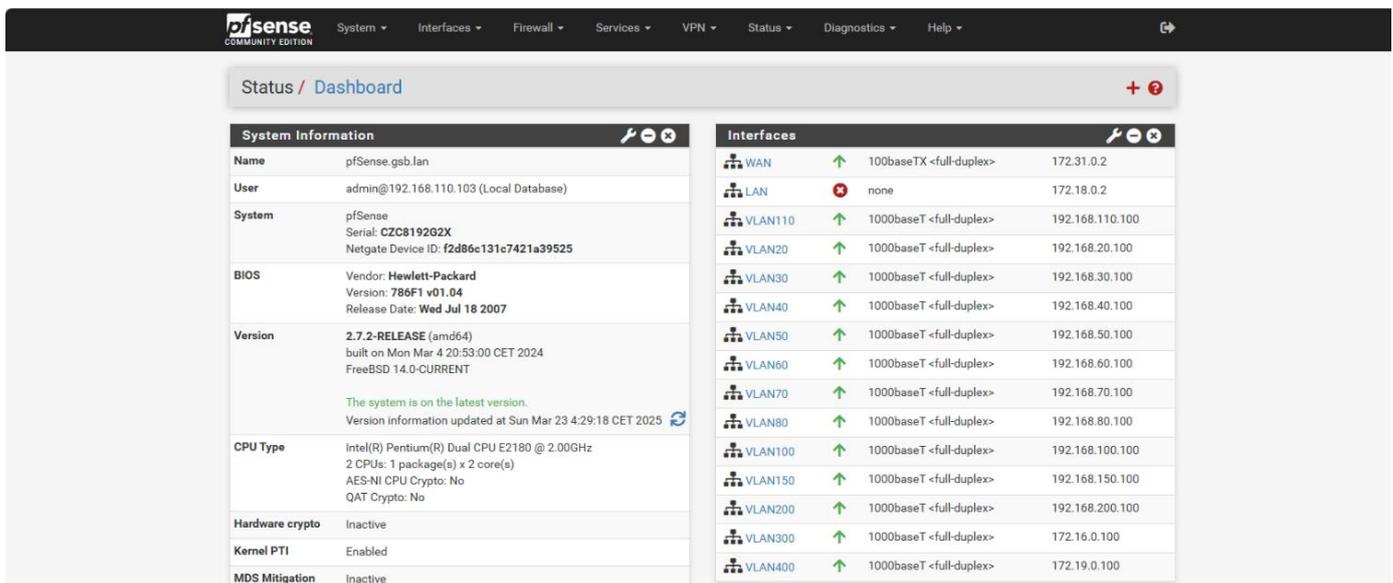
- **Cisco Catalyst 3560G (MUTLAB)**
- **Cisco Catalyst 3750G (SW-RS-DELTA)**
- **Cisco Catalyst 2960-S (SWITCH-BDS)**
- **Un routeur Cisco (RTROUT)**
- **Un routeur/pare-feu pfSense (ProxSilab)**
- **Hyperviseur de type 1 (PVE-DELTA)**
- **Hyperviseur de type 1 (PVE-MOHAMED)**
- **Un point d'accès WiFi**

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 '

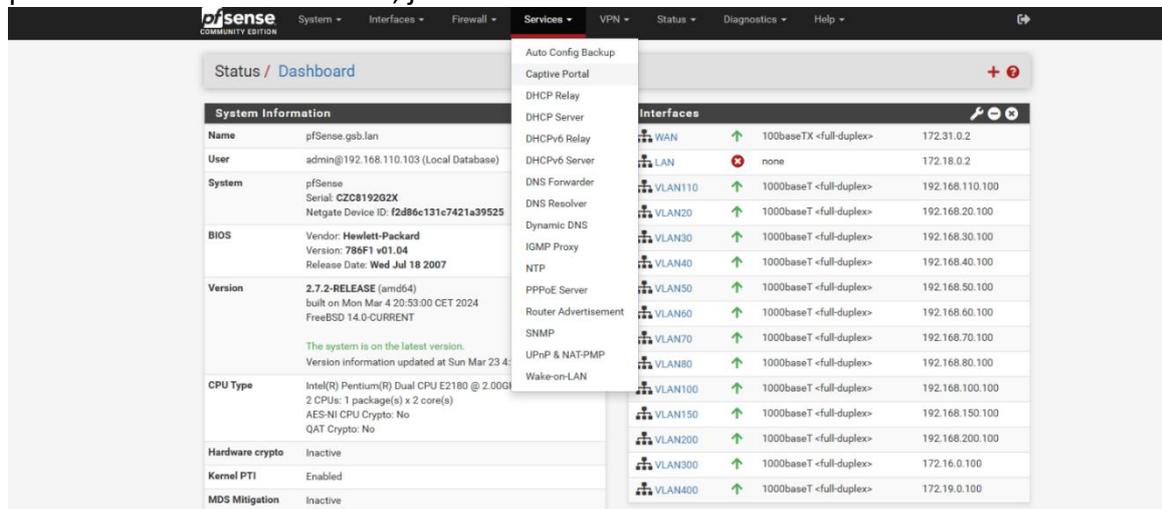


The screenshot shows the pfSense dashboard with the following data:

System Information		Interfaces	
Name	pfSense.gsb.lan	WAN	100baseTX <full-duplex> 172.31.0.2
User	admin@192.168.110.103 (Local Database)	LAN	none 172.18.0.2
System	pfSense Serial: CZC819202X Netgate Device ID: f2d86c131c7421a39525	VLAN110	1000baseT <full-duplex> 192.168.110.100
BIOS	Vendor: Hewlett-Packard Version: 786F1 v01.04 Release Date: Wed Jul 18 2007	VLAN20	1000baseT <full-duplex> 192.168.20.100
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT	VLAN30	1000baseT <full-duplex> 192.168.30.100
CPU Type	Intel(R) Pentium(R) Dual CPU E2180 @ 2.00GHz 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: No QAT Crypto: No	VLAN40	1000baseT <full-duplex> 192.168.40.100
Hardware crypto	Inactive	VLAN50	1000baseT <full-duplex> 192.168.50.100
Kernel PTI	Enabled	VLAN60	1000baseT <full-duplex> 192.168.60.100
MDS Mitigation	Inactive	VLAN70	1000baseT <full-duplex> 192.168.70.100
		VLAN80	1000baseT <full-duplex> 192.168.80.100
		VLAN100	1000baseT <full-duplex> 192.168.100.100
		VLAN150	1000baseT <full-duplex> 192.168.150.100
		VLAN200	1000baseT <full-duplex> 192.168.200.100
		VLAN300	1000baseT <full-duplex> 172.16.0.100
		VLAN400	1000baseT <full-duplex> 172.19.0.100

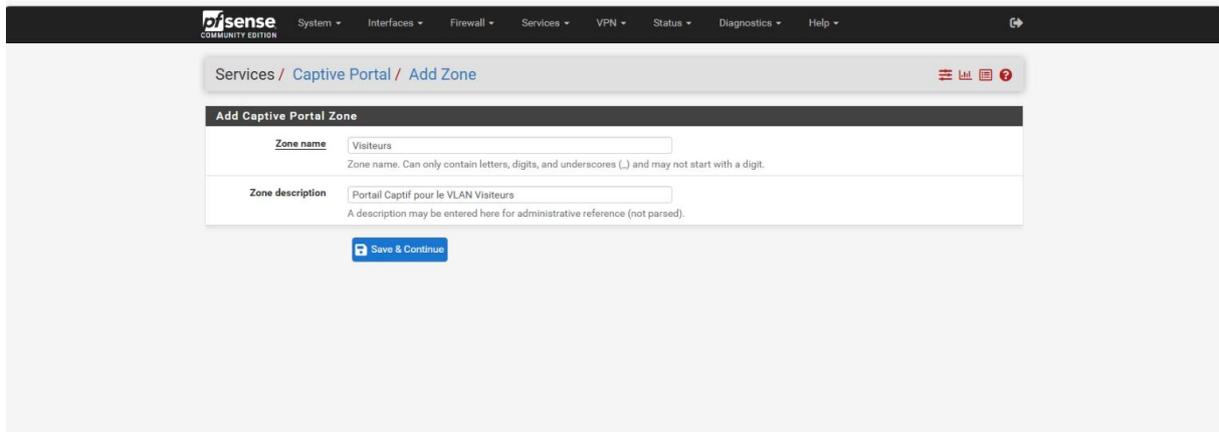
2. Création d'une zone de portail captif

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'



The screenshot shows the pfSense Services menu with 'Captive Portal' highlighted. The menu items are:

- Auto Config Backup
- Captive Portal**
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- NTP
- PPPoE Server
- Router Advertisement
- SNMP
- UPnP & NAT-PMP
- Wake-on-LAN



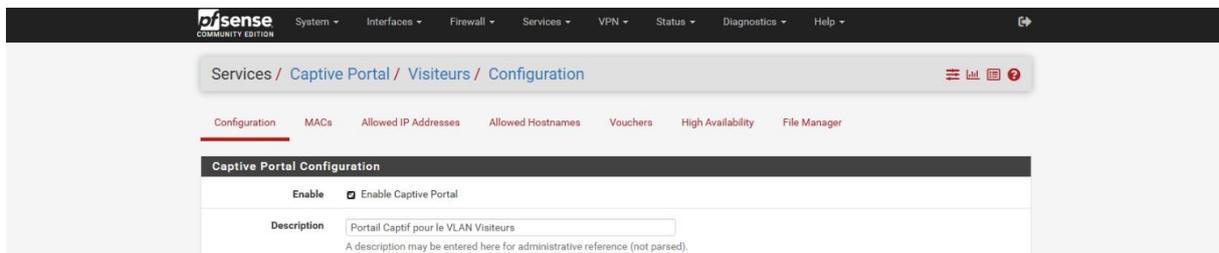
Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name
Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description
A description may be entered here for administrative reference (not parsed).

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



Services / Captive Portal / Visiteurs / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

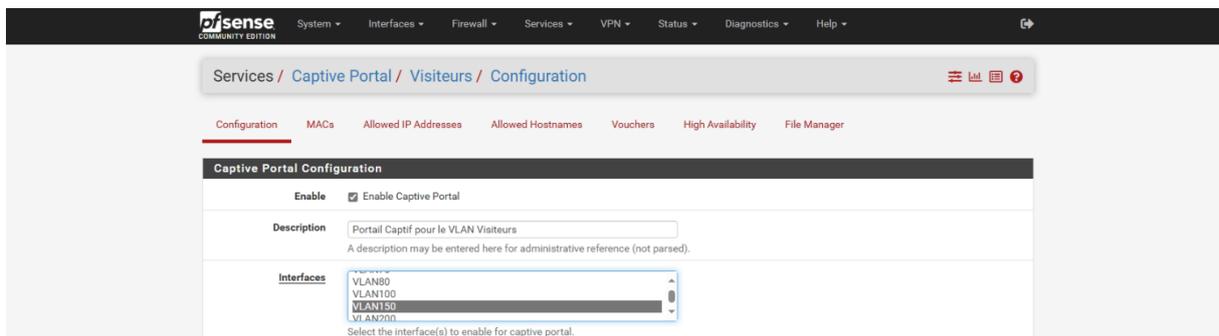
Captive Portal Configuration

Enable Enable Captive Portal

Description
A description may be entered here for administrative reference (not parsed).

3. Paramétrages clés

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



Services / Captive Portal / Visiteurs / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable Enable Captive Portal

Description
A description may be entered here for administrative reference (not parsed).

Interfaces
Select the interface(s) to enable for captive portal.

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

Maximum concurrent connections	<input type="text" value="3"/>
<small>Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.</small>	

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

Idle timeout (Minutes)	<input type="text" value="5"/>
<small>Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.</small>	

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

Hard timeout (Minutes)	<input type="text" value="30"/>
<small>Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).</small>	

2. Configuration

1. Redirection et bande passante

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

After authentication Redirection URL	<input type="text" value="https://google.fr"/>
<small>Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.</small>	

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

Traffic quota (Megabytes)	<input type="text" value="500"/>
<small>Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.</small>	

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

Per-user bandwidth restriction	<input checked="" type="checkbox"/> Enable per-user bandwidth restriction
Default download (Kbit/s)	<input type="text" value="50000"/>
Default upload (Kbit/s)	<input type="text" value="20000"/>

If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS servers can override the default settings. Leave empty for no limit.

2. Authentification

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

Authentication Method

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.

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

Authentication Server

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

You can optionally select a second set of servers to 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.

3. Personnalisation de la page de connexion

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

Display custom logo image	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
----------------------------------	--

Je téléverse le logo.

Logo Image Logo GSB.png

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.

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

Display custom background image Enable to use a custom uploaded background image

Background Image Fond GSB.jpg

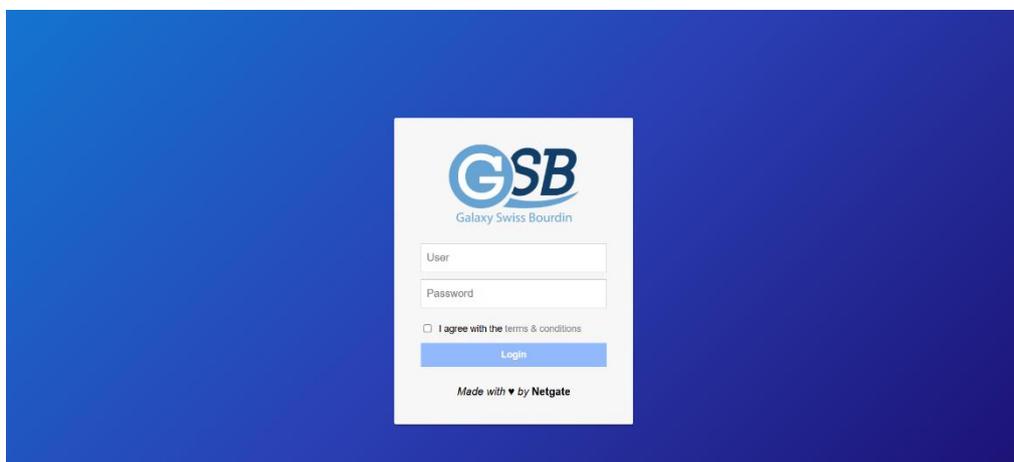
Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. **This image will not be stored in the config.** The default background image will be used if no custom background is present.

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

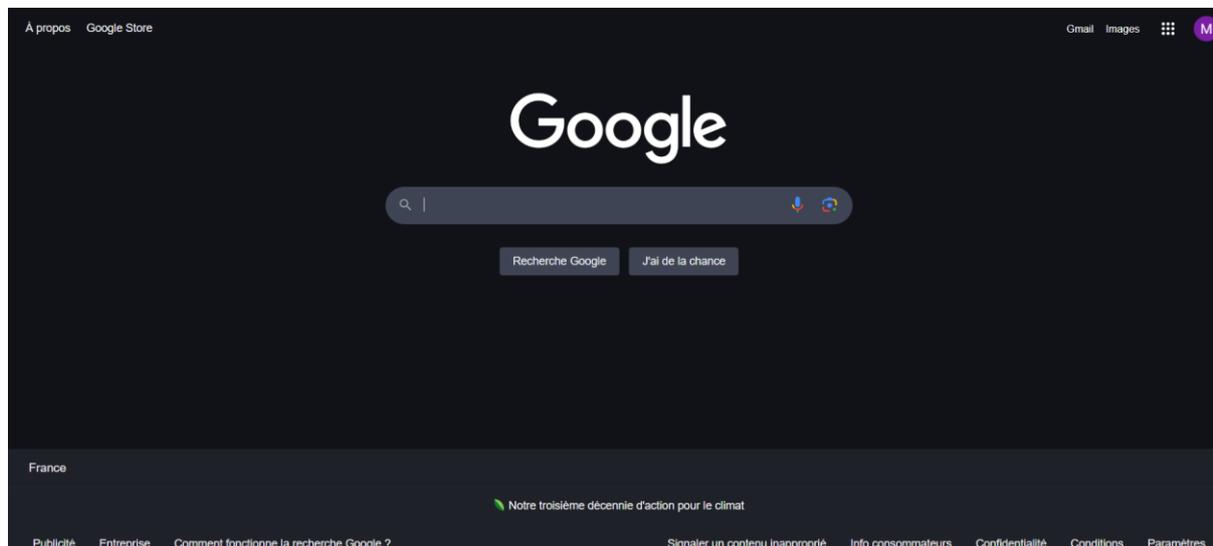
3. Test

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 saisi 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.