



I. Introduction.....	2
1. Contexte:.....	2
II. Besoin.....	3
III. Solution.....	4
1. Choix de la technologie.....	4
III. PfSense.....	6
1. Qu'est-ce que PfSense ?.....	6
2. Origines de PfSense.....	6
3. Les avantages de PfSense.....	6
1. Infrastructure gsb.....	7
2. Tableau d'Adressage IP des VLAN.....	8
3. Schéma réseau de la réalisation professionnelle.....	9
4. Matériel à disposition.....	10
V. Mise en place du portail captif.....	11
VI. Évolution possible.....	22
1. Intégration avec un serveur RADIUS.....	22



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.

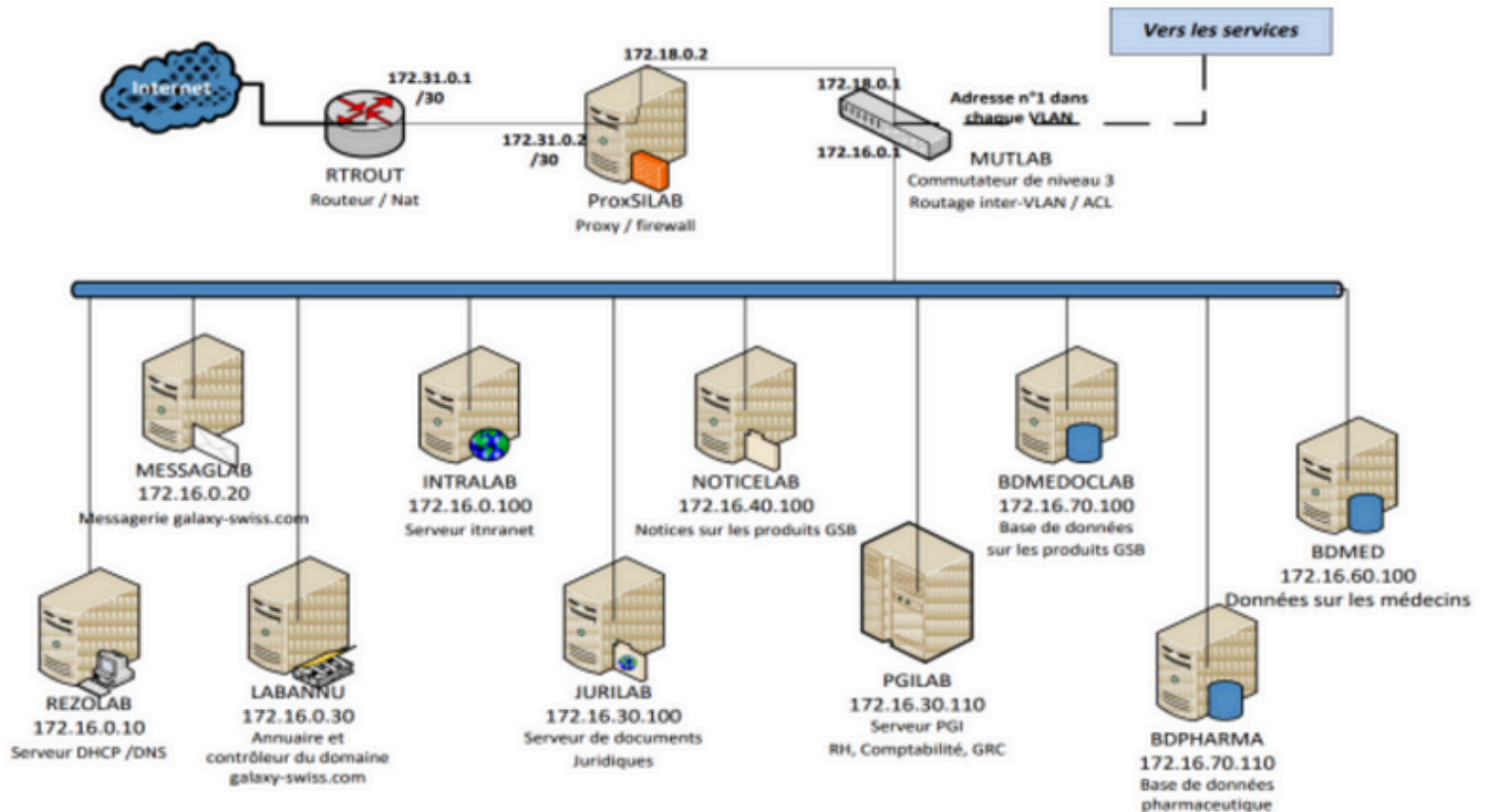
3. Les avantages de PfSense

- 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



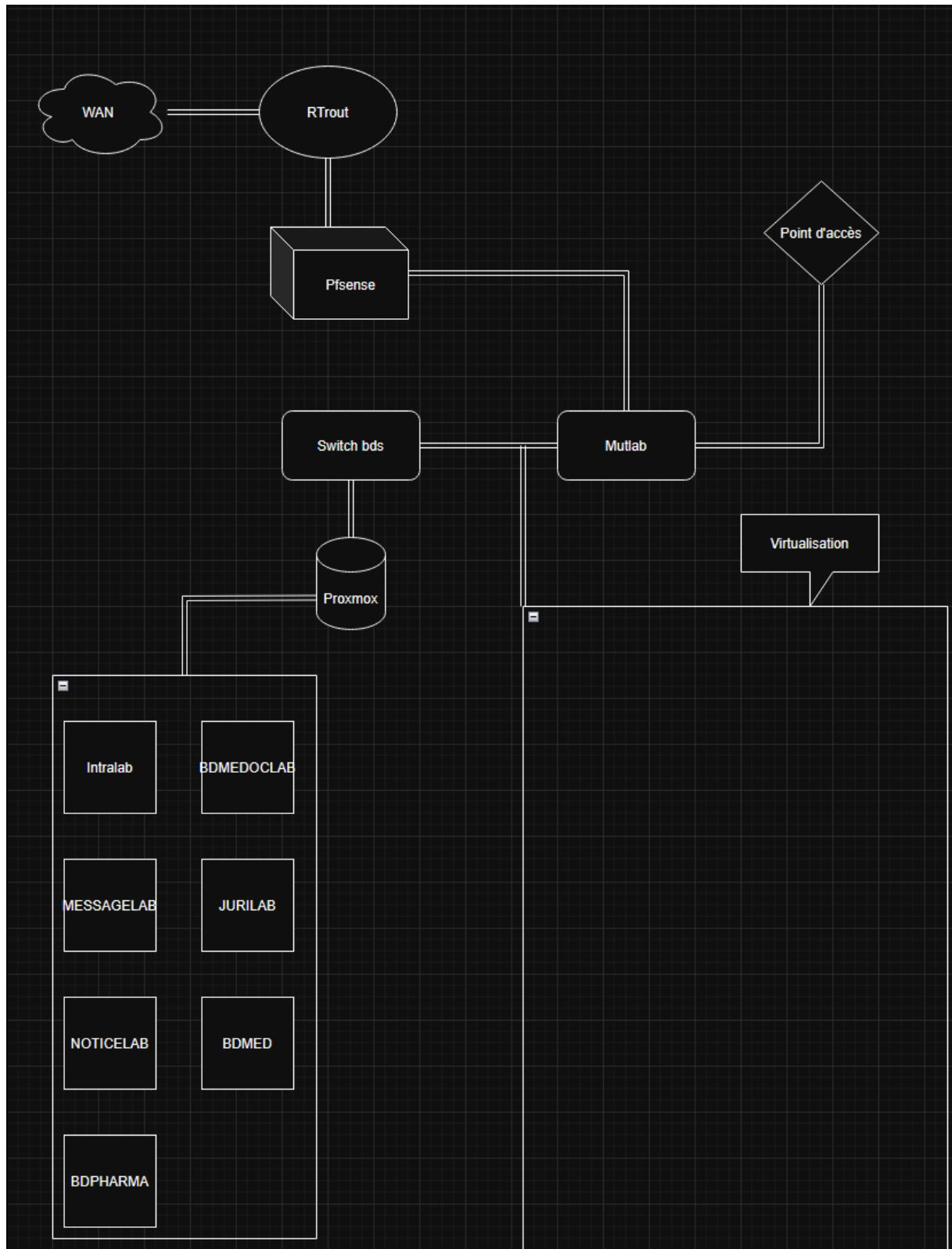


2. Tableau d'Adressage IP des VLAN

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**

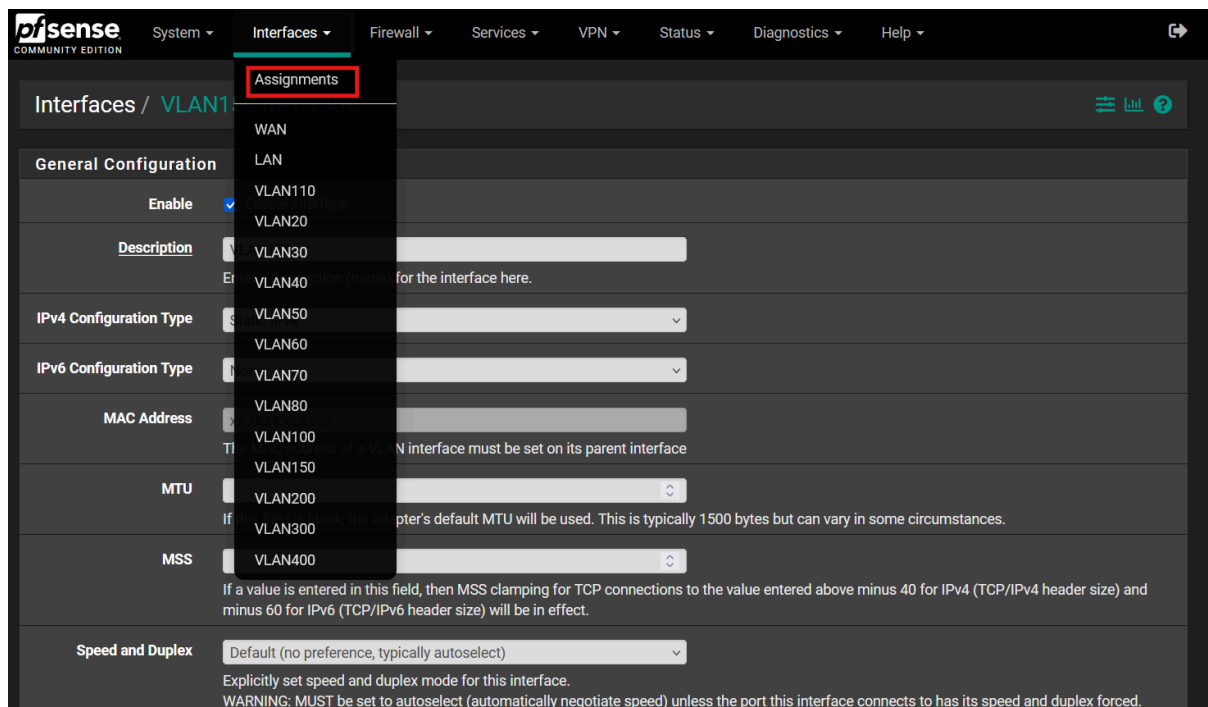


V. Mise en place du portail captif

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.

Interface Assignments				
Interface Groups				
Wireless				
VLANs				
QinQs				
PPPs				
GREs				
GIFs				
Bridges				
LAGGs				
VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
re1	110		VLAN110	 
re1	20		VLAN20	 
re1	30		VLAN30	 
re1	40		VLAN40	 
re1	50		VLAN50	 
re1	60		VLAN60	 
re1	70		VLAN70	 
re1	80		VLAN80	 
re1	100		VLAN100	 
re1	200		VLAN200	 
re1	300		VLAN300	 
re1	400		VLAN400	 
re1	150		VLAN150	 
				 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.

pfisense

COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Interfaces / VLANs / Edit

VLAN Configuration

Parent Interface

re1

Only VLAN capable interfaces will be shown.

VLAN Tag

150

802.1Q VLAN tag (between 1 and 4094).

VLAN Priority

0

802.1Q VLAN Priority (between 0 and 7).

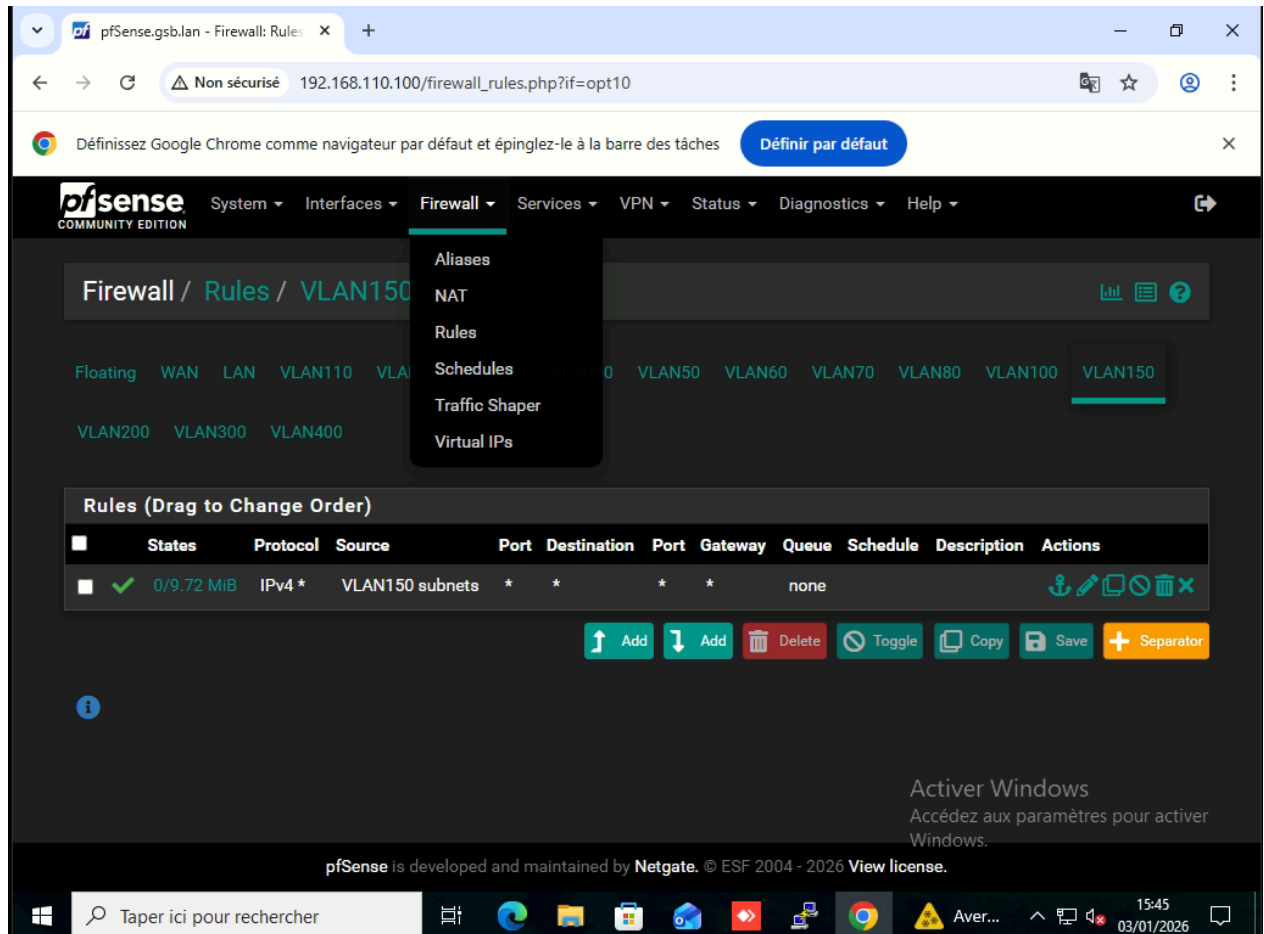
Description

VLAN150

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

Save

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

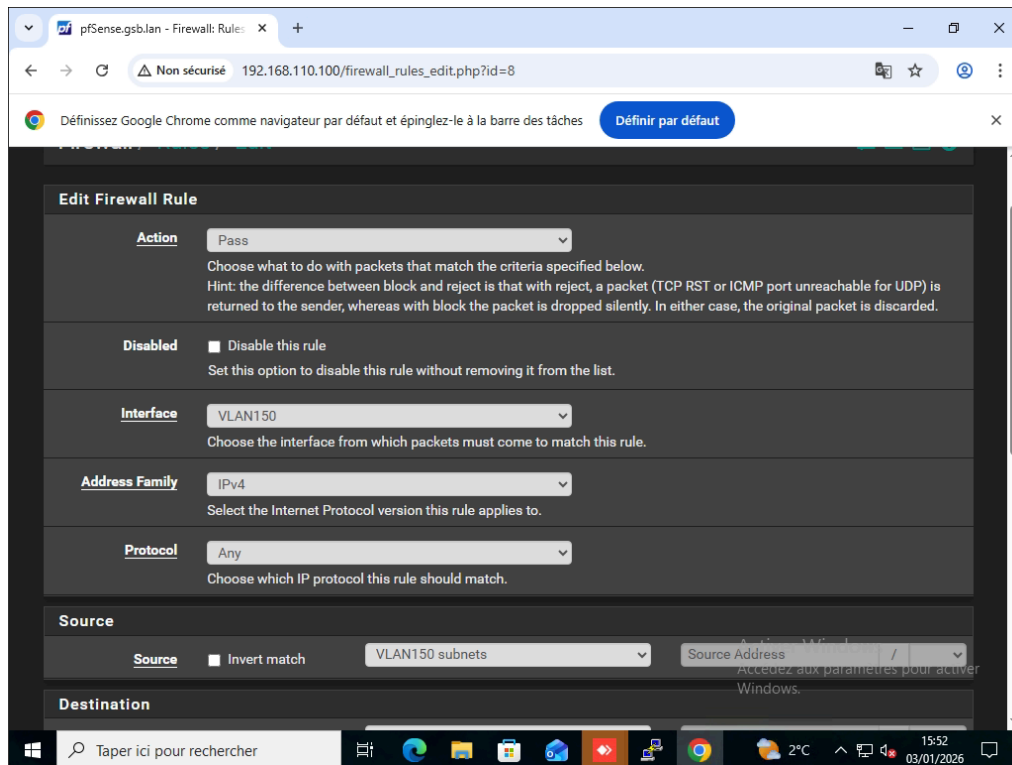
Enable	☒ Enable interface
Description	VLAN150 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx The MAC address of a VLAN interface must be set on its parent interface
MTU	 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	192.168.150.100 / 24
IPv4 Upstream gateway	None + Add a new gateway

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

Ethan GRISON



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.

TP-Link Wireless N Access Point WA801N
Model No. TL-WA801N

Wireless Basic Settings

Wireless: ☒ Enable ☐ Disable

☒ SSID1: GSB-Visiteurs VLAN ID: 150

☒ SSID2: GSB-Delta VLAN ID: 110

☐ SSID3: TP-Link_AP_856C_03 VLAN ID: 1

☐ SSID4: TP-Link_AP_856C_04 VLAN ID: 1

Mode: 11bgn mixed

Channel Width: Auto

Channel: Auto

☒ Enable SSID Broadcast

☒ Enable VLAN

Save

Wireless Settings Help

Note: The operating distance or range of your wireless connection varies significantly based on the physical placement of the AP. For best results, place your AP:

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position. Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to connect.

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.



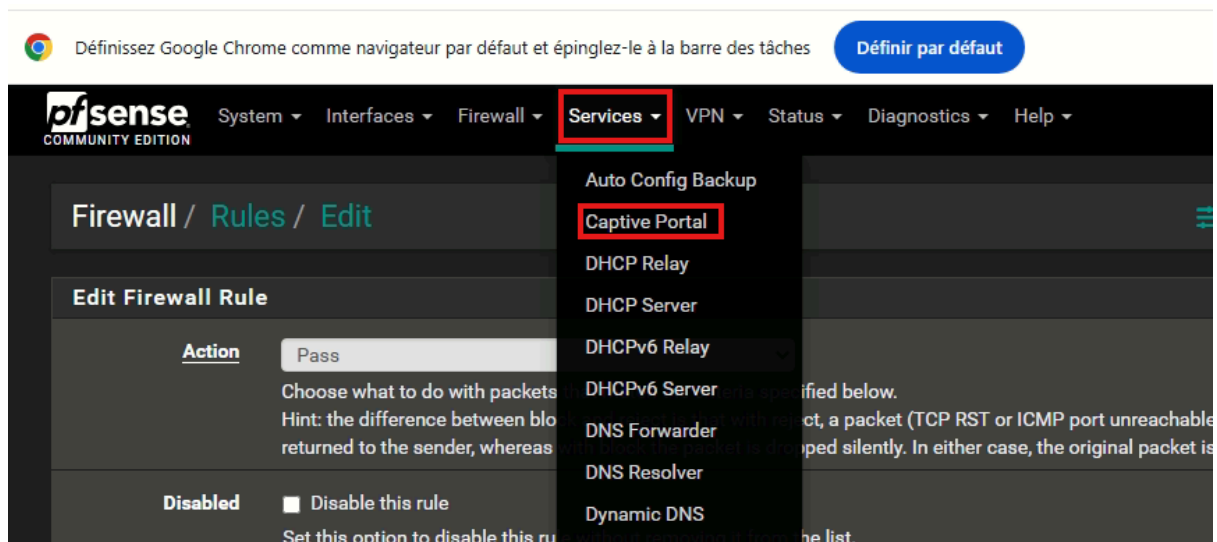
je désactive le mot de passe pour le wifi GSB-Visiteurs, le portail captif dans le Pfsense va gérer la sécurité du réseau.

A screenshot of the 'Wireless Security Settings' page in a web interface. The page has a light blue header with the title 'Wireless Security Settings'. Below the header, there is a red warning message: 'For network security, it is strongly recommended to enable wireless security and use WPA-PSK AES en'. The main content area contains several settings: 'SSID' is set to 'GSB-Visiteurs' in a dropdown menu; 'Disable Wireless Security' is selected with a radio button; 'WPA/WPA2 - Personal(Recommended)' is unselected; 'Authentication Type' is set to 'WPA2-PSK' in a dropdown menu; 'Encryption' is set to 'AES' in a dropdown menu; 'Wireless Password' is an empty text field; and 'Group Key Update Period' is set to '0' in a text field. A vertical scrollbar is visible on the right side of the form.

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.

Authentication

Authentication Method 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.

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

Authentication Server

RADIUS-MOHAMED
RADIUS-ethan
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.

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.

Captive Portal Login Page

Display custom logo image ☒ Enable to use a custom uploaded logo

Logo Image Parcourir... Sans titre.jpg

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.

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.

The image shows a captive portal login page with a blue background. In the center, there is a white rectangular area containing the 'gsb' logo at the top. Below the logo, there are two sections for authentication. The first section, titled 'First Authentication Method', contains two input fields labeled 'User' and 'Password'. The second section, titled 'Second Authentication Method', also contains two input fields labeled 'User' and 'Password'. At the bottom of the white area, there is a blue button labeled 'Login'.

Après avoir saisi 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.