1- **Introduction**
2- **Activation du portail captive**
3- **Configuration du DHCP**
4- **Création des règles sur le firewall**
5- **Test de notre portail captive**

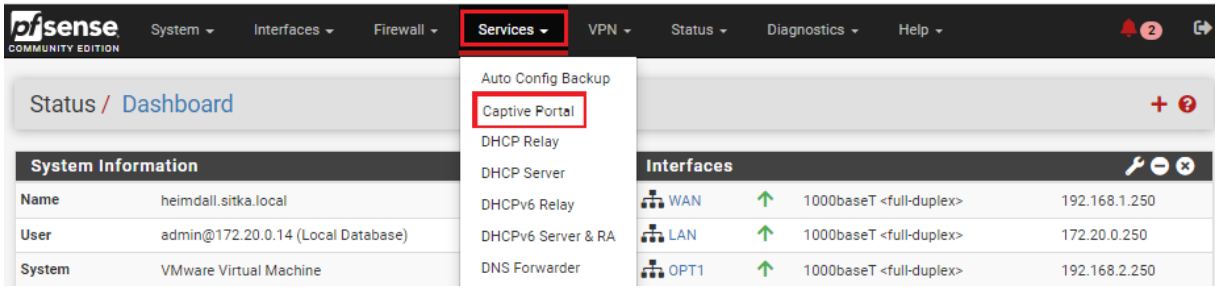
1- Introduction

Le portail captif est un moyen qui force les clients d'un réseau de passer par une page Web d'authentification pour pouvoir se connecter à Internet.

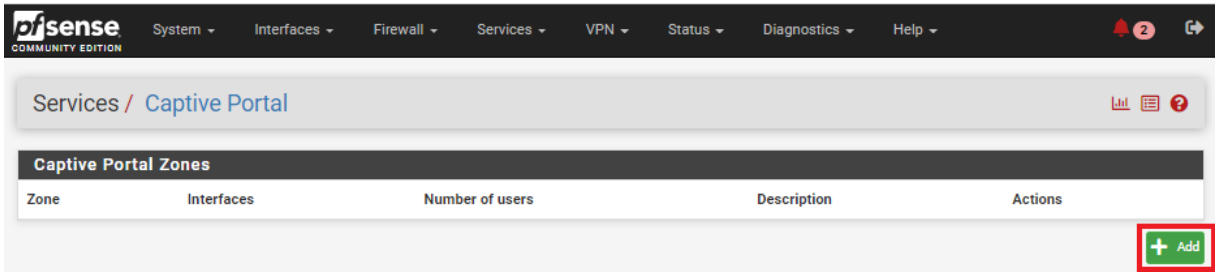
Il est utilisé dans des réseaux assurant un accès public comme certain espace de la SNCF, les hôtels, les établissement scolaires …

2- Activation du portail captive

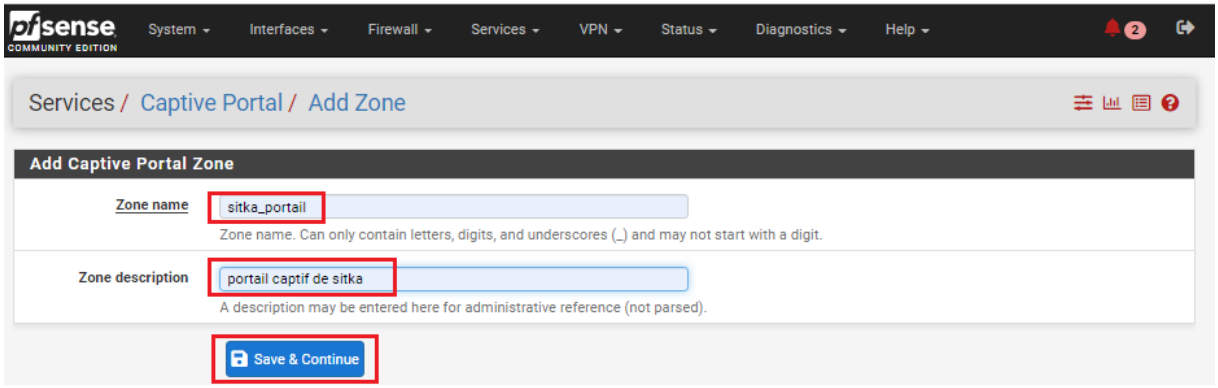
On se connecte sur l'interface de web de pfsense, après on va sur **Services + Captive Portal**



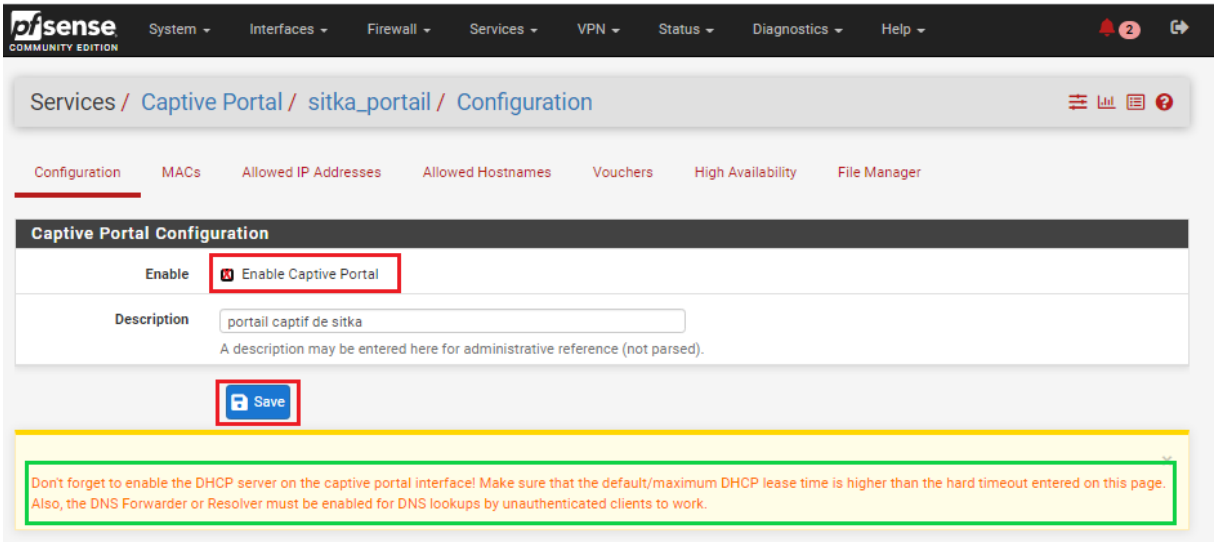
On clique sur **Add**



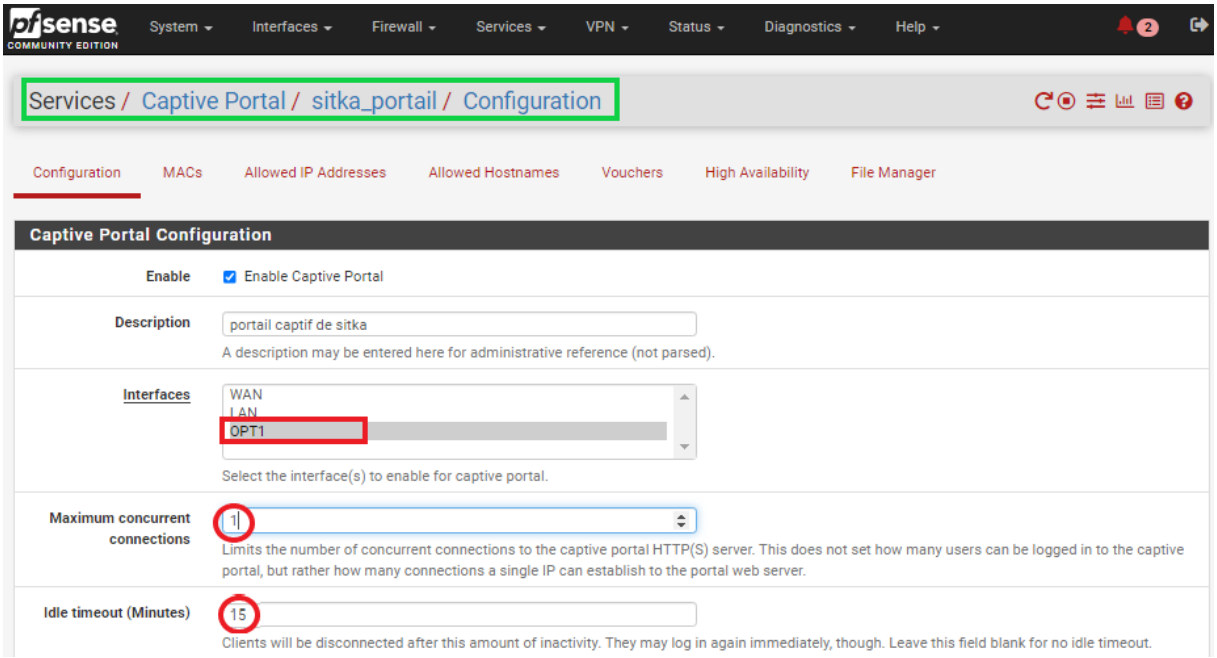
On renseigner le Nom du Portail Captif et sa description :
Sitka_portal pour le nom de la zone
Portail captive sitka pour la description de la zone



On active le portail et on enregistre

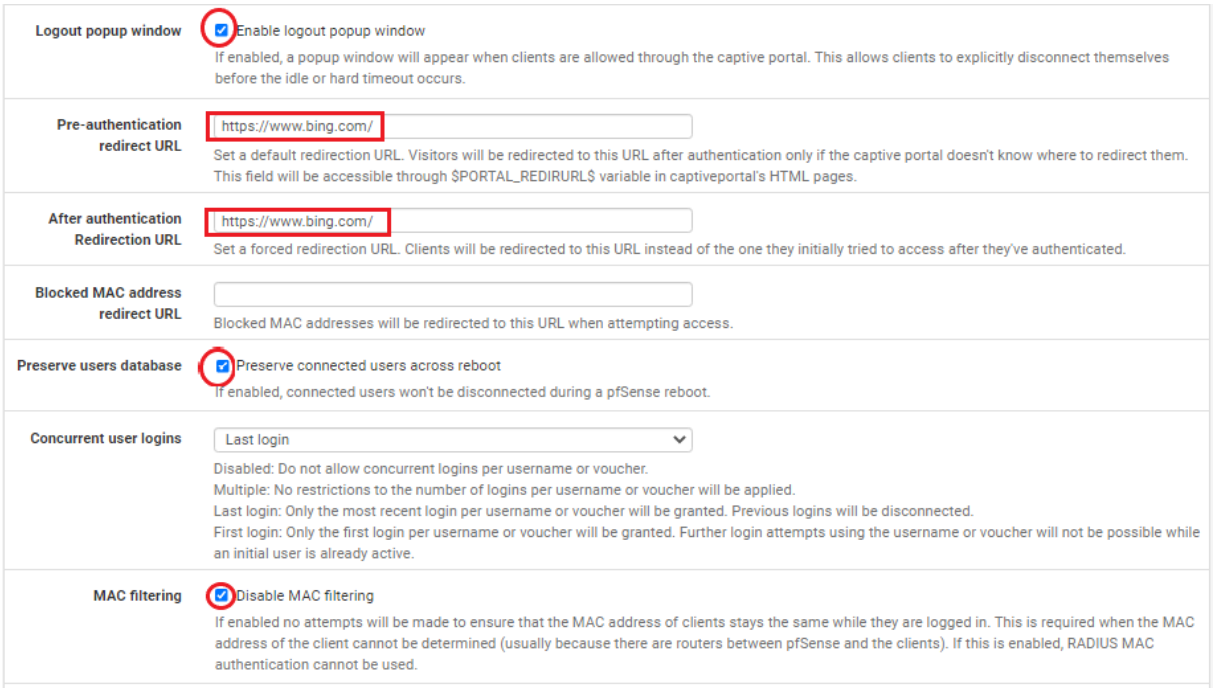


- On active **Enable Captive Portal**
- On sélectionne l'interface **Opt1**
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur)
- Idle timeout (Minutes) on choisit **15**:(Les clients seront déconnectés après cette période d'inactivité)

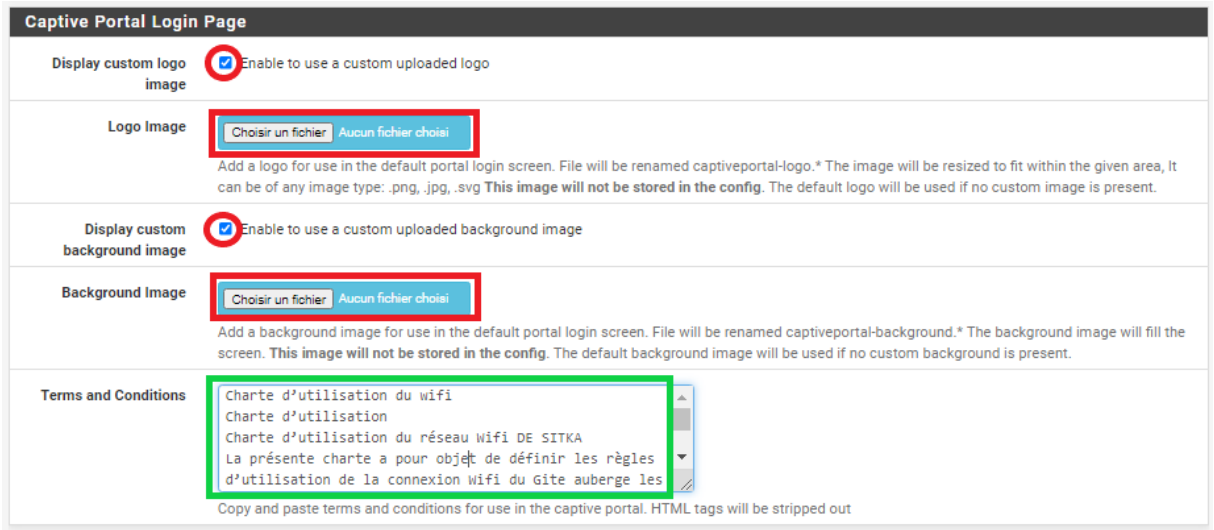


- Définir **After authentication Redirection URL** (**URL HTTP** de redirection Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont tenté d'accéder après s'être authentifiés)

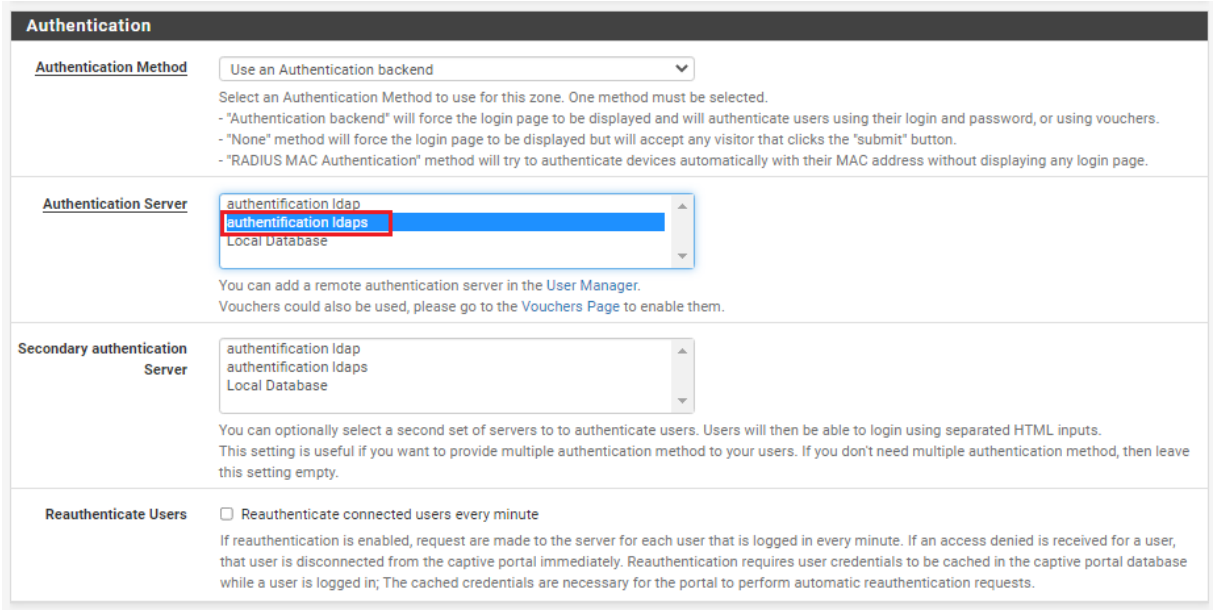
- Activer **Disable Concurrent user logins** (seule la connexion la plus récente par nom d'utilisateur sera active)
- Activer **Disable MAC filtering** (lorsque l'adresse MAC du client ne peut pas être déterminée)



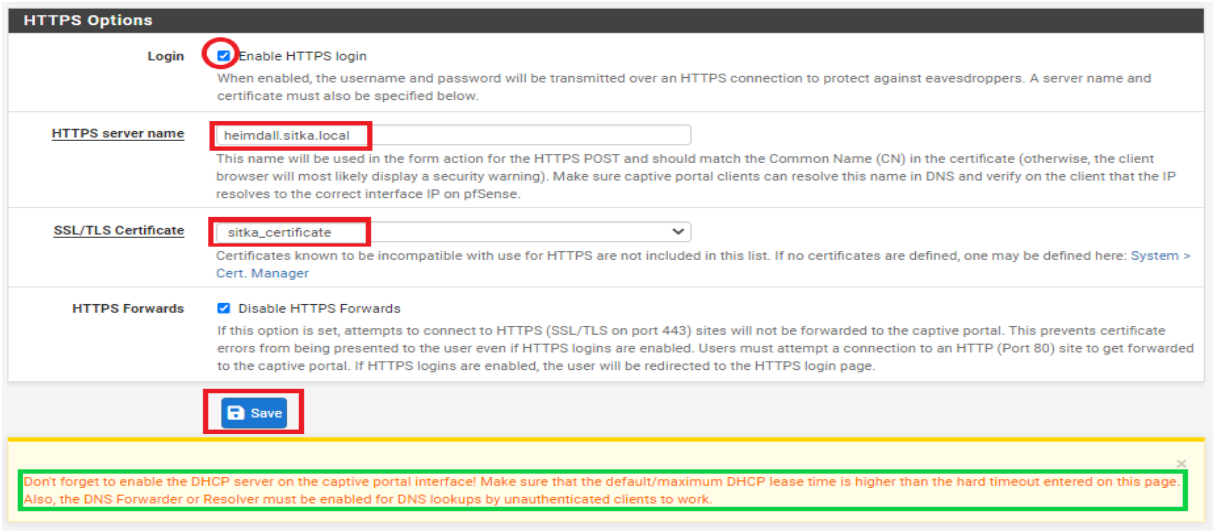
On peut choisir un logo et une image d'arrière-plan ainsi qu'un charte de connexion



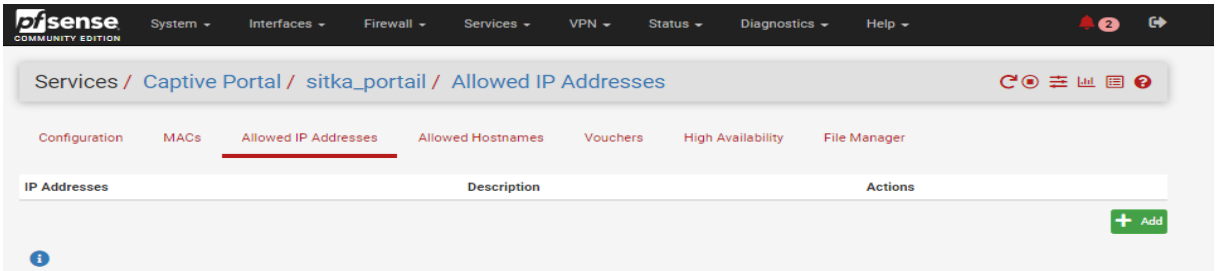
- On sélectionne **Use an Authentication backend**
- On sélectionne **Authentification LDAPS** comme méthode d'authentication

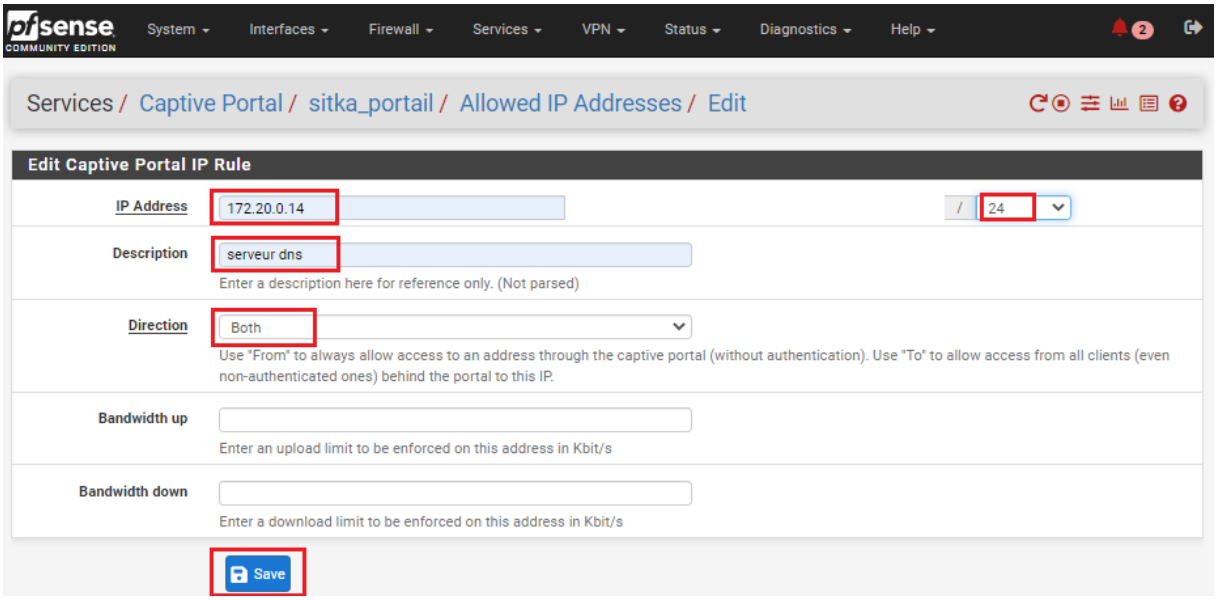


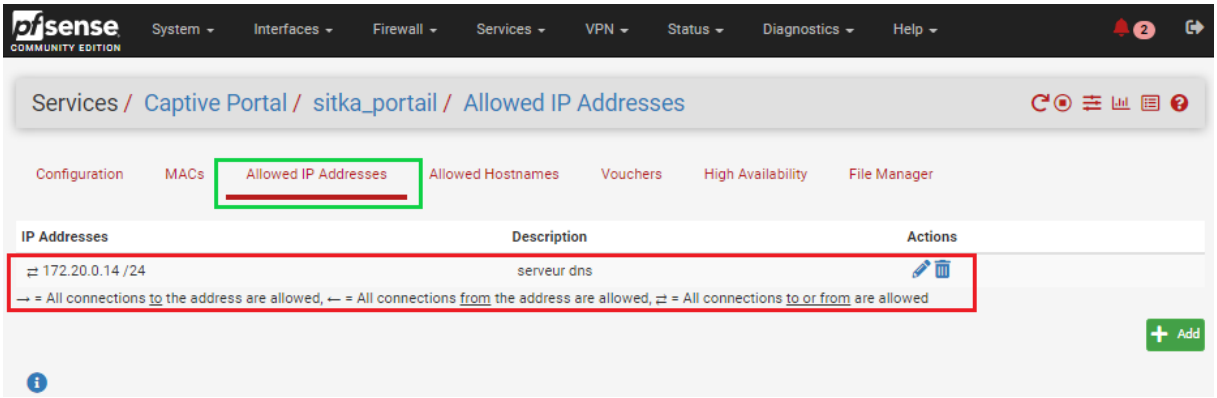
On active ssl pour notre portail active



Les clients ont besoin d'une résolution DNS donc on va autoriser cette résolution en autorisant l'adresse IP du DNS 172.20.0.14

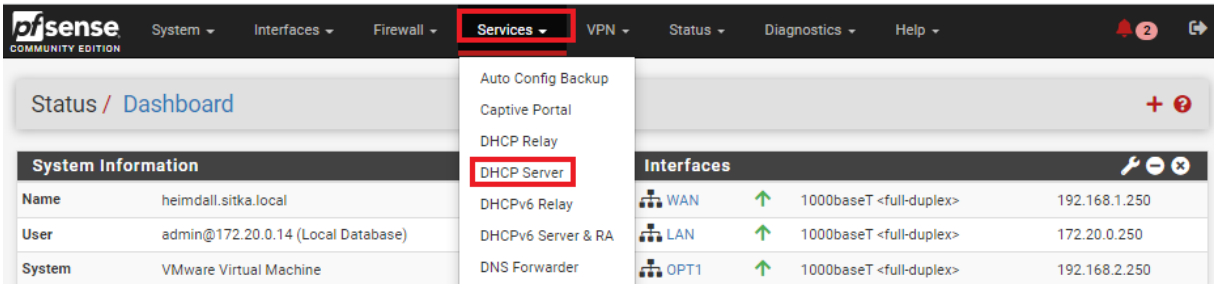




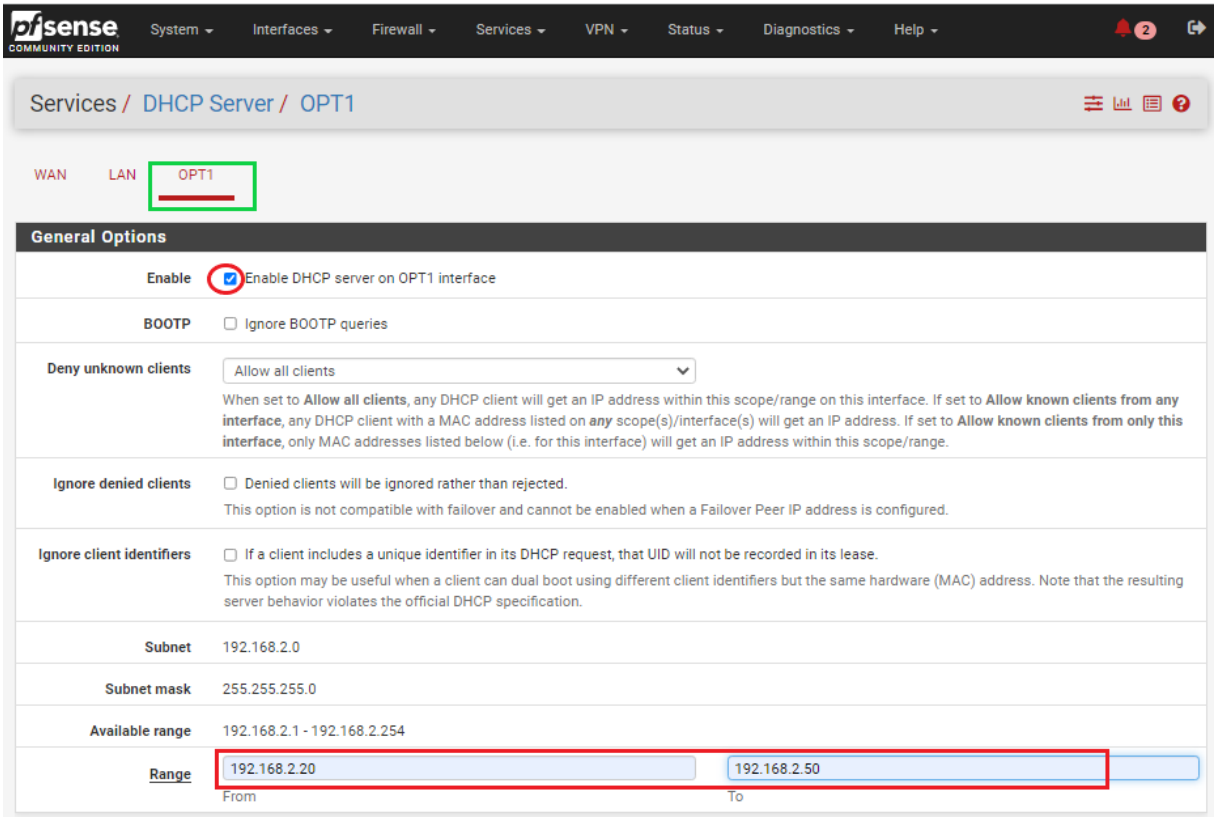


3- Configuration du DHCP

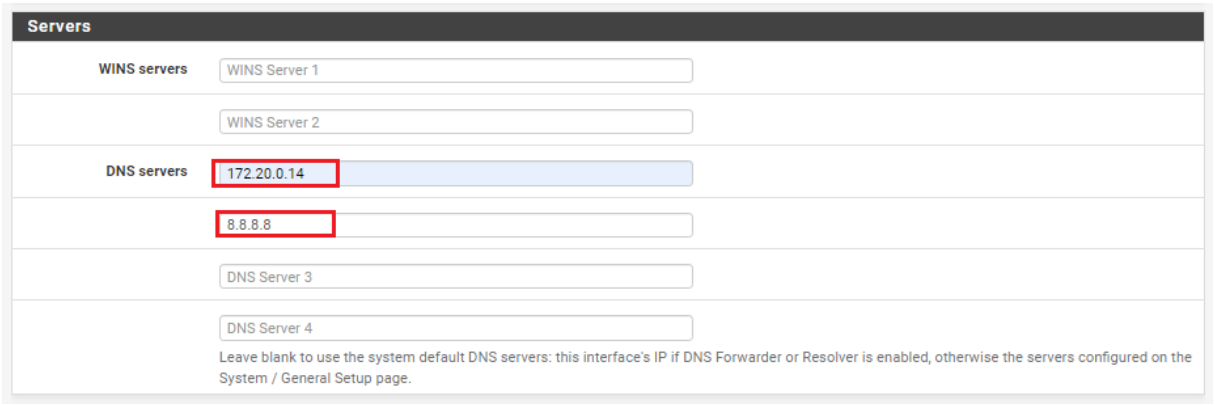
Maintenant On va activer le DHCP sur l'interface opt1



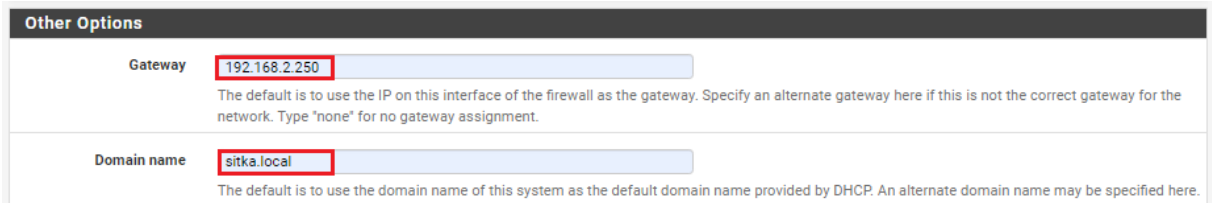
On déclare notre étendue



On rentre l'adresse de notre DNS

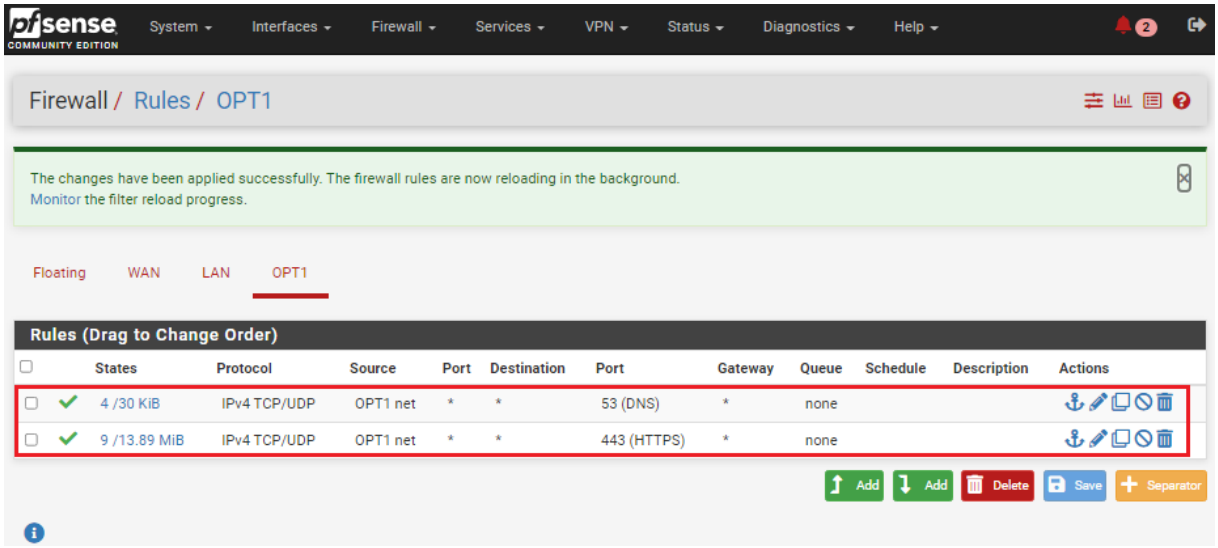


On rentre l'adresse de la passerelle et du nom de domaine



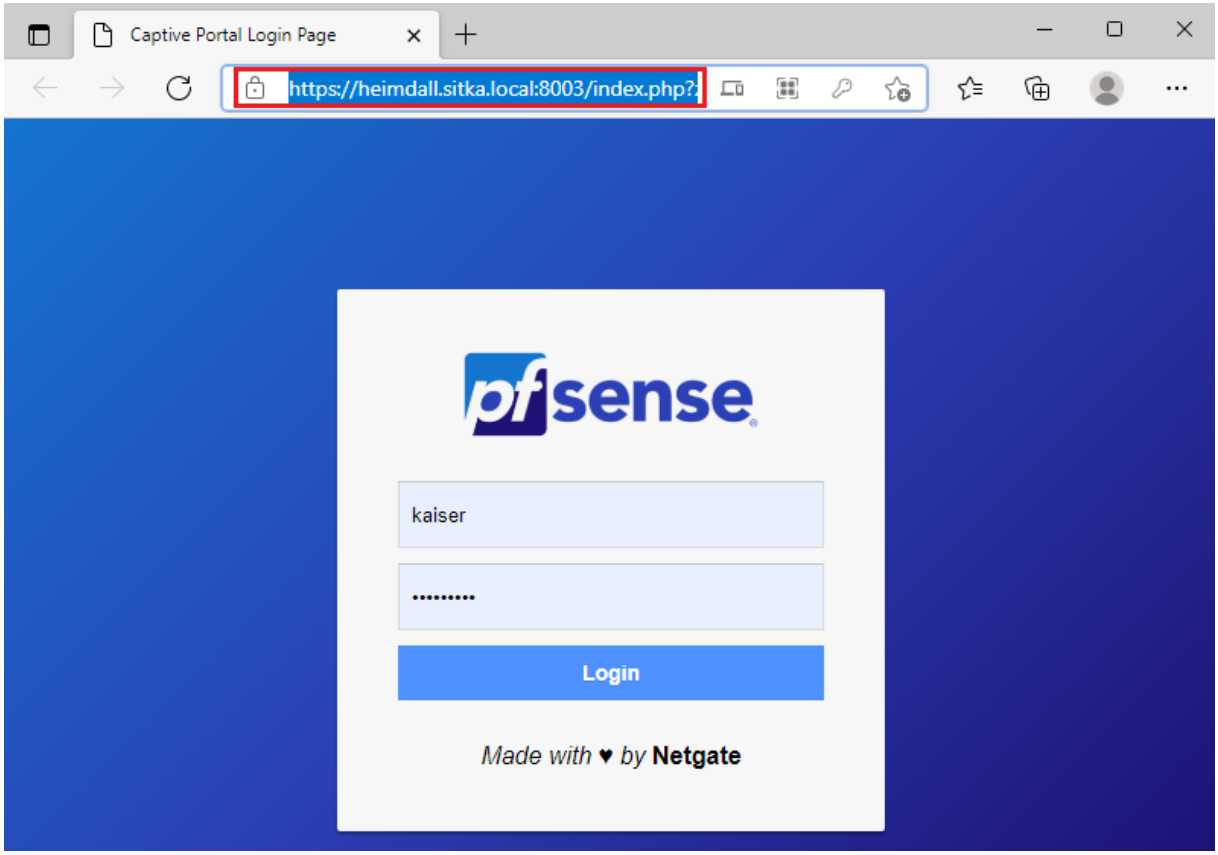
4- **Création des règles sur le firewall**

On Cree deux règles autorisant le DNS et le https

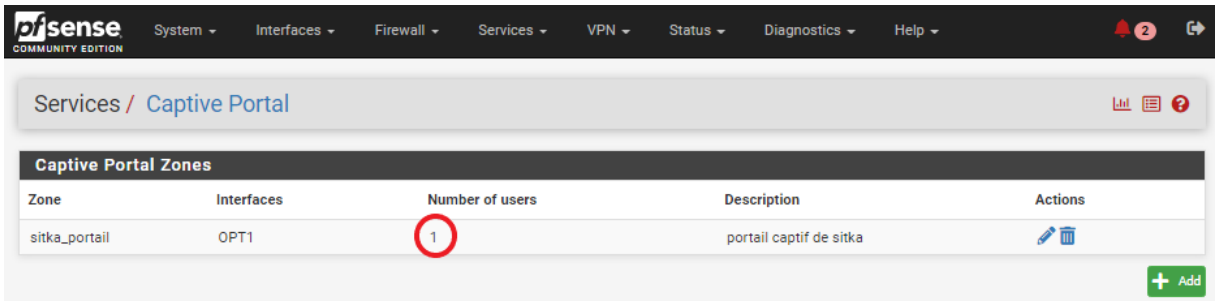


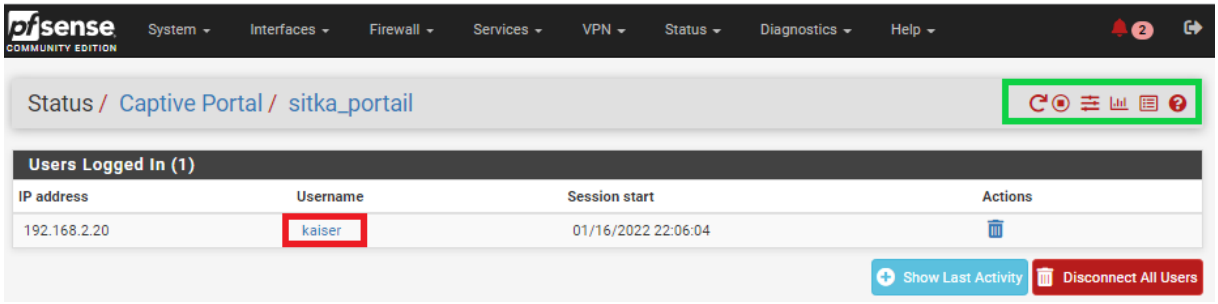
5- **Test de notre portail captive**

On fait notre test de connexion

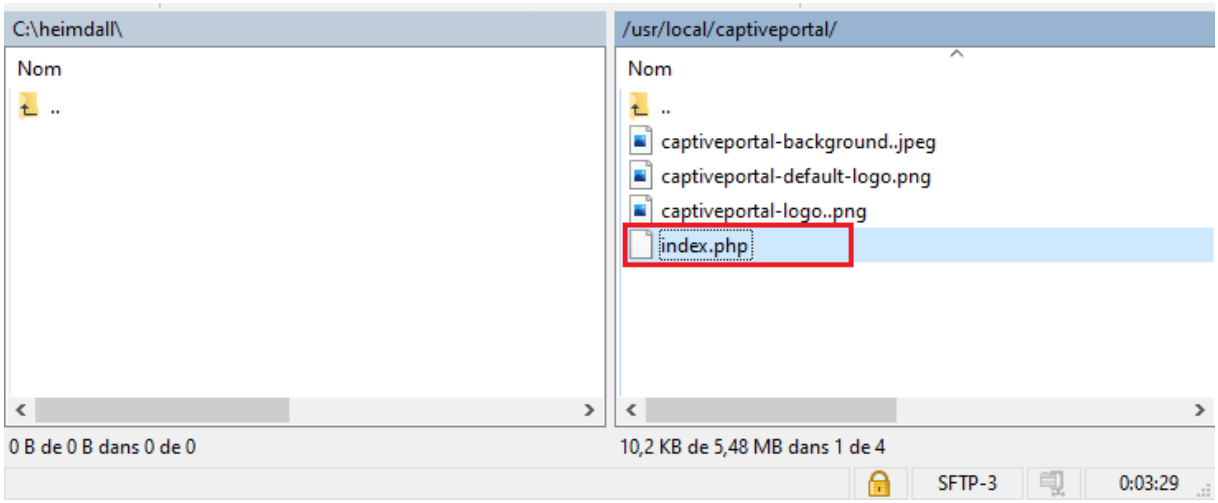


Sur pfsense on peut vérifier les connexions





- On chercher **You are connected** et remplacer par **Vous êtes connecté**
- On chercher **Disconnecting**… et **You have been disconnected** et on remplacer par **Déconnexion…** et **Vous êtes déconnecté**
- On cherche **Invalid credentials specified** et on remplace **par Les informations saisies sont invalides,** il y a 2 lignes à modifier
- Après on enregistre les modifications



Maintenant on va sur /etc/inc puis et on ouvre captiveportal.inc

- On chercher Captive Portal login Page et on remplacer par : Portail Captif de sitka
- On chercher Login et Made with … by … Netgate et on remplacer par Connexion et Connectez-vous avec votre compte LDAPS
- On chercher User et Password et on Remplace par Utilisateur et Mot de Passe
- On rechercher Logout et Click the button below to disconnect on remplace par **Déconnexion et Cliquez sur le bouton ci-dessous pour vous déconnecter**

- On enregistre les modifications