



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

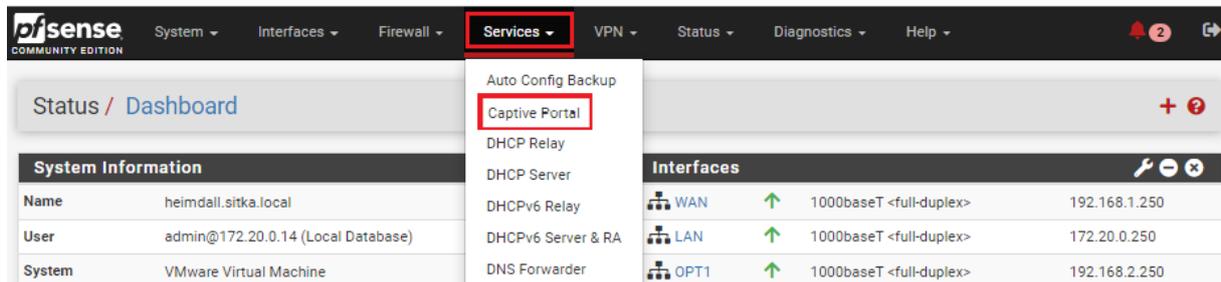
1- Introduction

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.

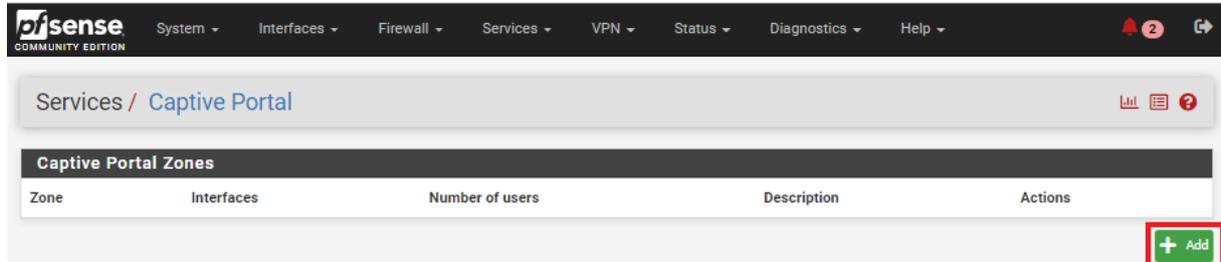
Il est utilisé dans des réseaux assurant un accès public comme certain espace de la SNCF, les hôtels, les établissements scolaires ...

2- Activation du portail captif

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



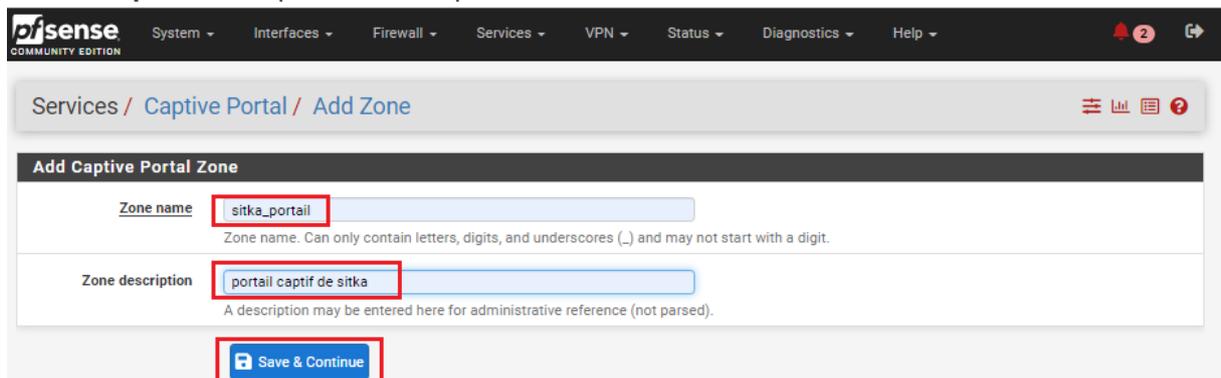
On clique sur **Add**



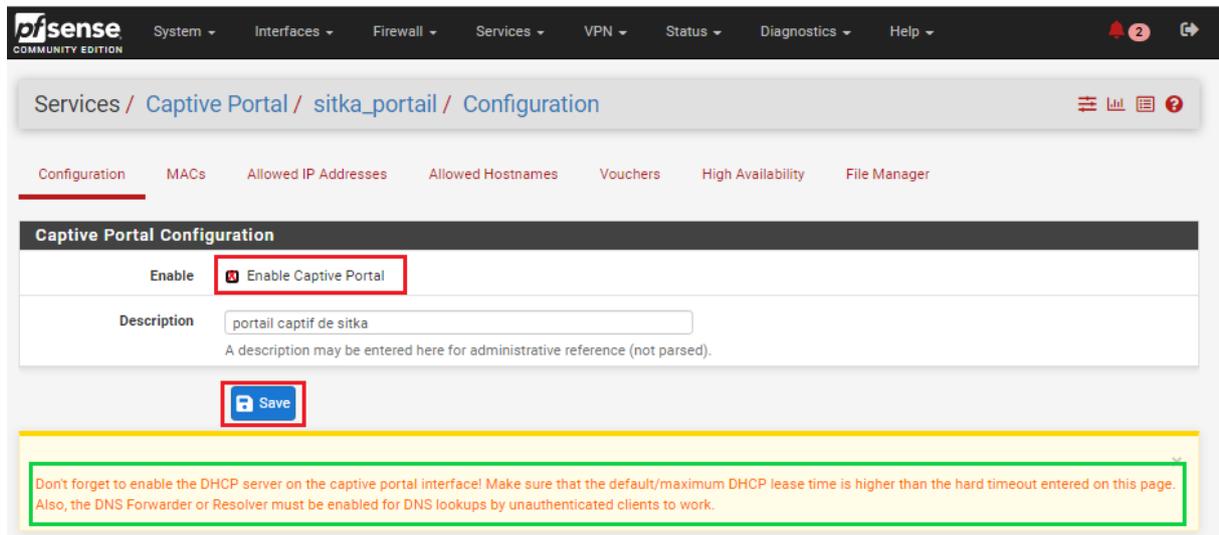
On renseigner le Nom du Portail Captif et sa description :

Sitka_portal pour le nom de la zone

Portail captif sitka pour la description de la zone

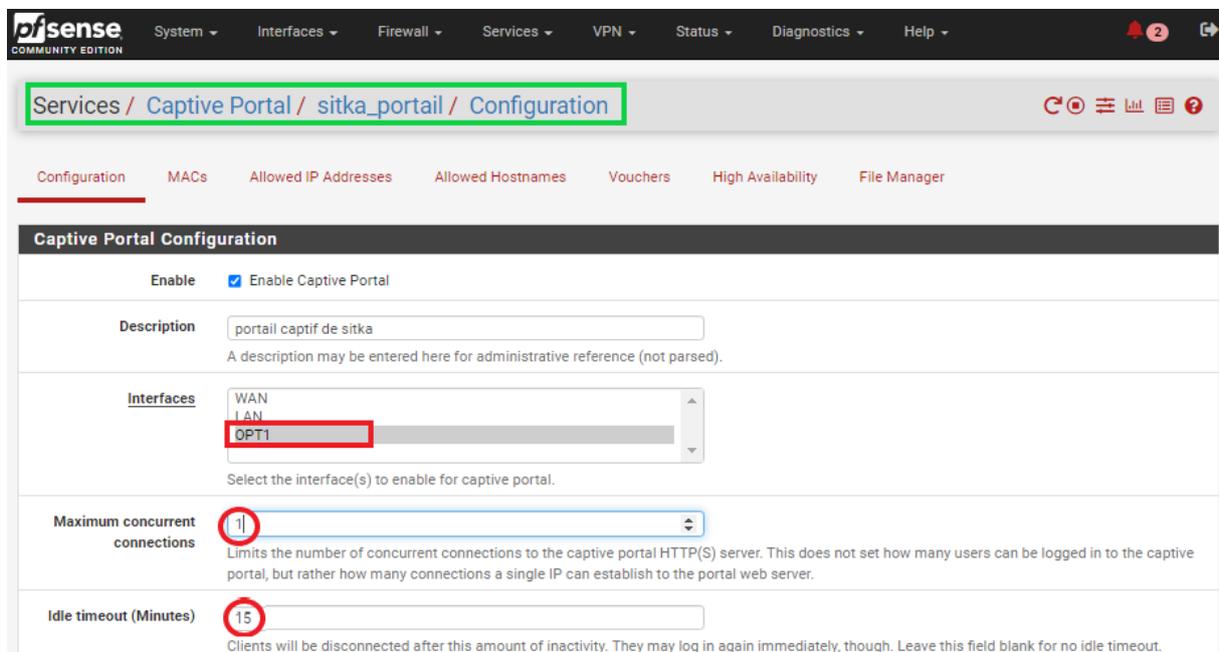


On active le portail et on enregistre



The screenshot shows the pfSense web interface for the Captive Portal configuration of the 'sitka_portail' interface. The 'Enable' checkbox is checked, and the 'Save' button is highlighted with a red box. A yellow warning box at the bottom states: 'Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.'

- 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)



The screenshot shows the pfSense web interface for the Captive Portal configuration of the 'sitka_portail' interface. The 'Interfaces' dropdown is set to 'OPT1', 'Maximum concurrent connections' is set to 1, and 'Idle timeout (Minutes)' is set to 15. The 'Save' button is also visible.

- 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)

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" value="https://www.bing.com"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURLS variable in captiveportal's HTML pages.
After authentication Redirection URL	<input type="text" value="https://www.bing.com"/> 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.
Blocked MAC address redirect URL	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
Preserve users database	<input checked="" type="checkbox"/> Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
Concurrent user logins	<input type="text" value="Last login"/> Disabled: Do not allow concurrent logins per username or voucher. Multiple: No restrictions to the number of logins per username or voucher will be applied. Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected. First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

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

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"/> <input type="button" value="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 checked="" type="checkbox"/> Enable to use a custom uploaded background image
Background Image	<input type="button" value="Choisir un fichier"/> <input type="button" value="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	<input type="text" value="Charte d'utilisation du wifi
Charte d'utilisation
Charte d'utilisation du réseau wifi DE SITKA
La présente charte a pour objet de définir les règles d'utilisation de la connexion wifi du Gîte auberge les"/> Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out

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

Authentication

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.

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.

Reauthenticate Users Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

On active ssl pour notre portail active

HTTPS Options

Login Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name

This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL/TLS Certificate

Certificates known to be incompatible with use for HTTPS are not included in this list. If no certificates are defined, one may be defined here: [System > Cert. Manager](#)

HTTPS Forwards Disable HTTPS Forwards

If this option is set, attempts to connect to HTTPS (SSL/TLS on port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.

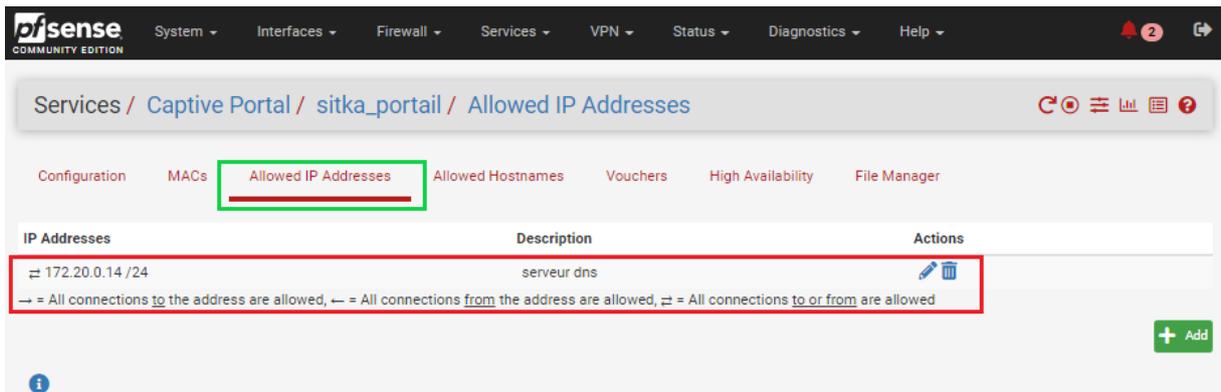
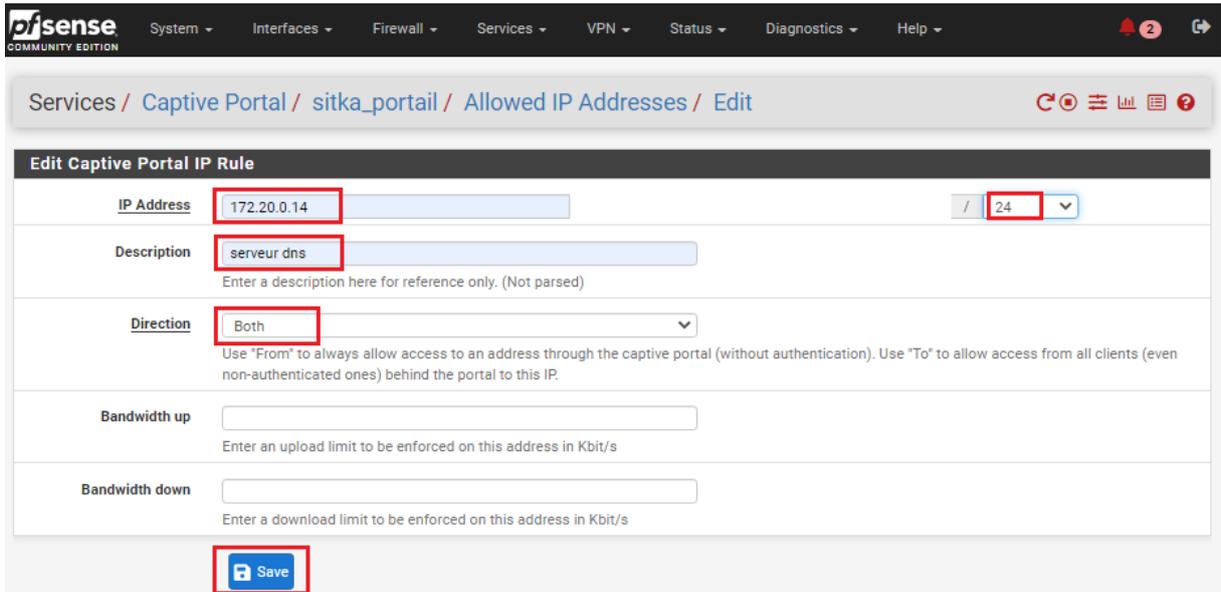
Les clients ont besoin d'une résolution DNS donc on va autoriser cette résolution en autorisant l'adresse IP du DNS 172.20.0.14

pfSense COMMUNITY EDITION System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Services / Captive Portal / sitka_portail / Allowed IP Addresses

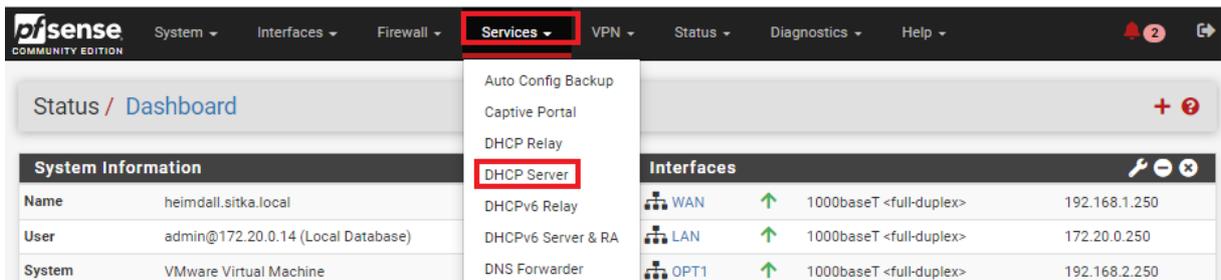
Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

IP Addresses	Description	Actions
<input type="button" value="+ Add"/>		



3- Configuration du DHCP

Maintenant On va activer le DHCP sur l'interface opt1



On déclare notre étendue

The screenshot shows the pfSense web interface for configuring the DHCP server on the OPT1 interface. The 'Enable' checkbox is checked, and the 'Range' is set to 192.168.2.20 to 192.168.2.50. Other options like BOOTP, Deny unknown clients, and Ignore denied clients are also visible.

Services / DHCP Server / OPT1

WAN LAN **OPT1**

General Options

Enable Enable DHCP server on OPT1 interface

BOOTP Ignore BOOTP queries

Deny unknown clients
When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 192.168.2.0

Subnet mask 255.255.255.0

Available range 192.168.2.1 - 192.168.2.254

Range From To

On rentre l'adresse de notre DNS

The screenshot shows the 'Servers' configuration page in pfSense. The 'DNS servers' field is filled with 172.20.0.14 and 8.8.8.8. There are also fields for WINS servers and DNS Server 3 and 4.

Servers

WINS servers

DNS servers

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

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

The screenshot shows the 'Other Options' configuration page in pfSense. The 'Gateway' field is filled with 192.168.2.250 and the 'Domain name' field is filled with sitka.local.

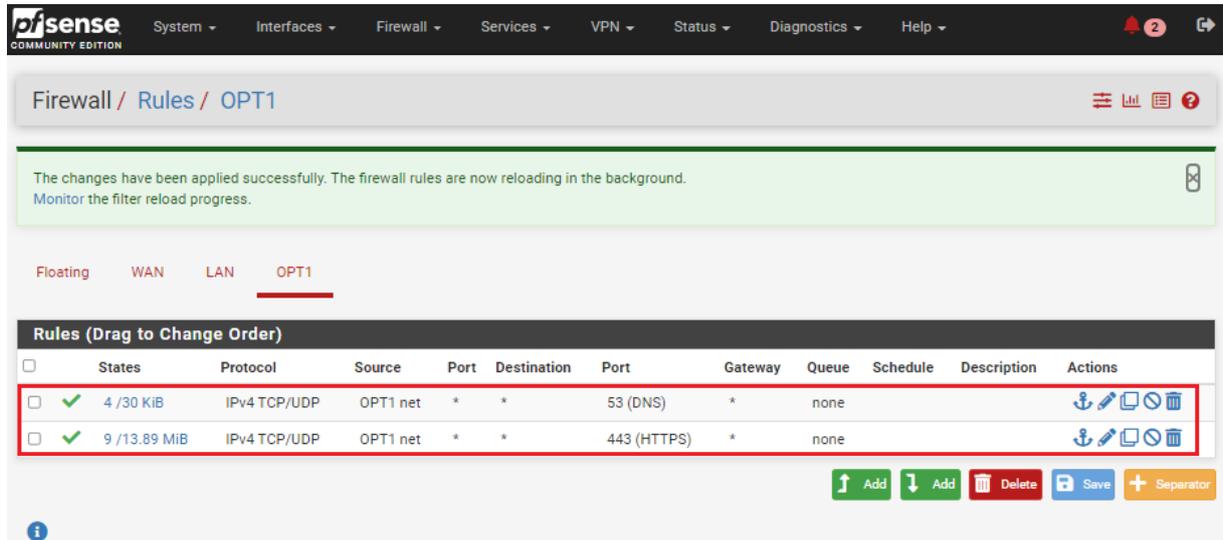
Other Options

Gateway
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Domain name
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

4- Création des règles sur le firewall

On Cree deux règles autorisant le DNS et le https



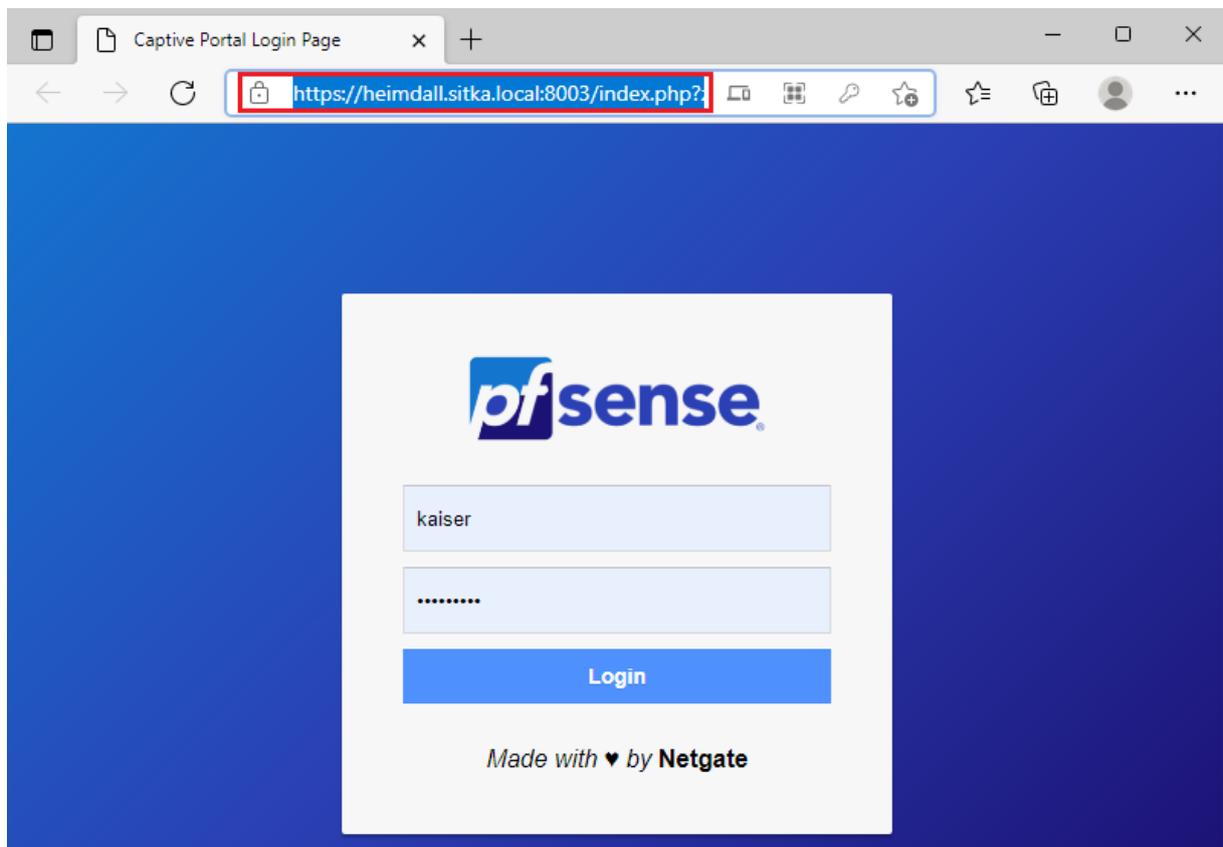
The screenshot shows the pfSense Firewall Rules configuration page for the OPT1 interface. The page displays two rules that have been successfully applied and are now reloading in the background. The rules are:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
4 / 30 KiB	IPv4 TCP/UDP	OPT1 net	*	*	53 (DNS)	*	none			
9 / 13.89 MiB	IPv4 TCP/UDP	OPT1 net	*	*	443 (HTTPS)	*	none			

Buttons at the bottom: Add, Add, Delete, Save, Separator.

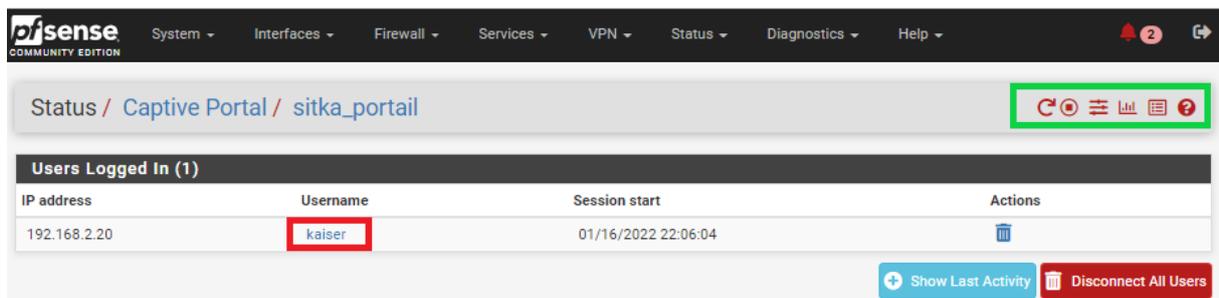
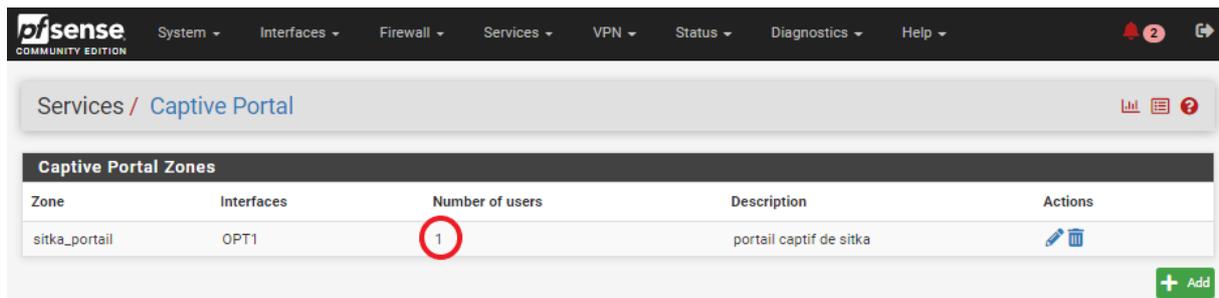
5- Test de notre portail captive

On fait notre test de connexion

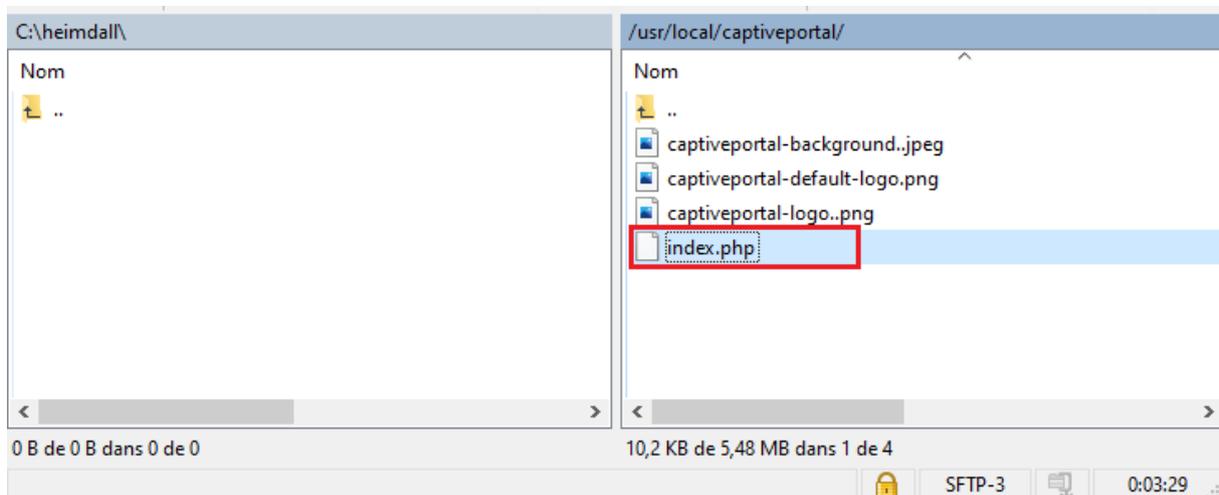


The screenshot shows a web browser window displaying the Captive Portal Login Page. The address bar shows the URL <https://heimdall.sitka.local:8003/index.php?>, which is highlighted with a red box. The page features the pfSense logo, a login form with fields for username (kaiser) and password (masked with dots), and a Login button. The footer text reads "Made with ♥ by Netgate".

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 recherche **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

