

Guide d'administration et personnalisation

Sommaire :

[I. Configuration Portail Captif](#)

[II. Configuration d'un groupe et des utilisateurs pour la délégation du Portail Captif](#)

[A. Groupes](#)

[B. Utilisateurs](#)

[C. Vérification](#)

[III. Personnalisation du portail captif](#)

[A. Personnalisation du Logo](#)

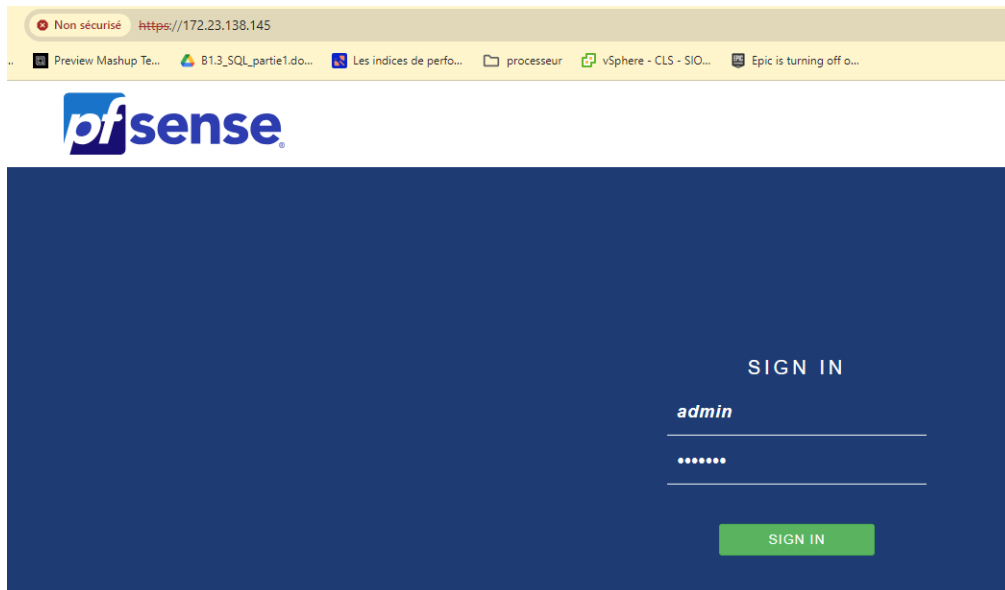
[B. Personnalisation des fenêtres d'affichage](#)

[IV. Enregistrement des logs](#)

[A. Squid : Qu'est-ce que c'est ?](#)

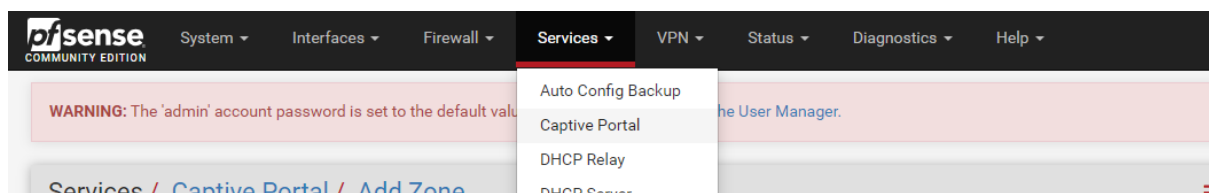
[B. LightSquid : Qu'est-ce que c'est ?](#)

[V. Gestion Vlans](#)



Login : admin/pfsense

I. Configuration Portail Captif



Appuyez sur add

Add Captive Portal Zone

Zone name


PORTAIL

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

Zone description

portail captif

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

 Save & Continue

Pour activer le portail captif sur pfSense et configurer les paramètres spécifiés, suivez ces étapes :

- Connectez-vous à l'interface web de pfSense.
- Accédez à l'onglet "**Services**" dans le menu principal.
- Cliquez sur "**Captive Portal**" dans le menu déroulant.
- Cochez la case "**Enable Captive Portal**" pour activer le portail captif.
- Sélectionnez "**LAN**" dans le menu déroulant de l'interface pour spécifier que le portail captif sera appliqué à l'interface LAN.
- Définissez le nombre maximum de connexions concurrentes pour un même utilisateur en entrant "**1**" dans le champ "**Maximum concurrent connections**". Cela limitera le nombre de connexions simultanées autorisées pour un même utilisateur.
- Choisissez la durée d'inactivité après laquelle les clients seront déconnectés en sélectionnant une valeur entre 1 et 5 dans le champ "**Idle timeout (Minutes)**". Cette valeur représente le nombre de minutes d'inactivité avant que le système déconnecte automatiquement un utilisateur.
- Cliquez sur "**Save**" pour enregistrer les modifications.

Services / Captive Portal / PORTAIL / Configuration

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

Captive Portal Configuration

Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input type="text" value="portail captif"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Interfaces	<div><div>WAN</div><div>LAN</div></div> <small>Select the interface(s) to enable for captive portal.</small>
Maximum concurrent connections	<input type="text" value="1"/> <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>
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>
Hard timeout (Minutes)	<input type="text"/> <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>

Pour configurer les options supplémentaires du portail captif sur pfSense, suivez ces étapes :

- Cochez la case "**Enable logout popup window**" pour activer une fenêtre popup permettant aux clients de se déconnecter.
- Définissez l'URL de redirection pré-authentification en saisissant l'URL souhaitée dans le champ "**Pre-authentication Redirect URL**". Cette URL sera utilisée pour rediriger les visiteurs qui ne sont pas encore authentifiés vers une page spécifiée.
- Définissez l'URL de redirection après l'authentification en saisissant l'URL souhaitée dans le champ "**After authentication redirection URL**". Cette URL sera utilisée pour rediriger les clients après leur authentification vers une page spécifiée.
- Cochez la case "**Disable Concurrent user logins**" pour activer la désactivation des connexions simultanées des utilisateurs. Cela signifie que seule la connexion la plus récente sera active pour un même nom d'utilisateur.
- Cochez la case "**Disable MAC filtering**" pour activer la désactivation du filtrage MAC. Cela est nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée ou n'est pas utilisée pour restreindre l'accès.
- Cliquez sur "**Save**" pour enregistrer les modifications.

Logout popup window	<input 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.google.fr/"/> 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_REDIRECTURL\$ variable in captiveportal's HTML pages.
After authentication Redirection URL	<input type="text" value="https://www.google.fr/"/> 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 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="Multiple"/> 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.
Pass-through MAC Auto Entry	<input checked="" type="checkbox"/> Enable Pass-through MAC automatic additions When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another system. If this is enabled, the logout window will not be shown.

- Cochez la case **"Use an Authentication backend"** pour activer l'utilisation d'un backend d'authentification.
- Sélectionnez **"Local Database"** dans le menu déroulant pour **"Authentication Server"**. Cela permettra d'utiliser la base de données locale de pfSense pour l'authentification des utilisateurs.
- Assurez-vous de ne pas sélectionner **"Local Database"** pour **"Secondary Authentication Server"**. Laissez cette option non sélectionnée pour ne pas configurer de serveur d'authentification secondaire.
- Cochez la case **"Local Authentication Privileges"** pour autoriser uniquement les utilisateurs avec les droits de **"Connexion au portail captif"**.
- Cliquez sur **"Save"** pour enregistrer les modifications.

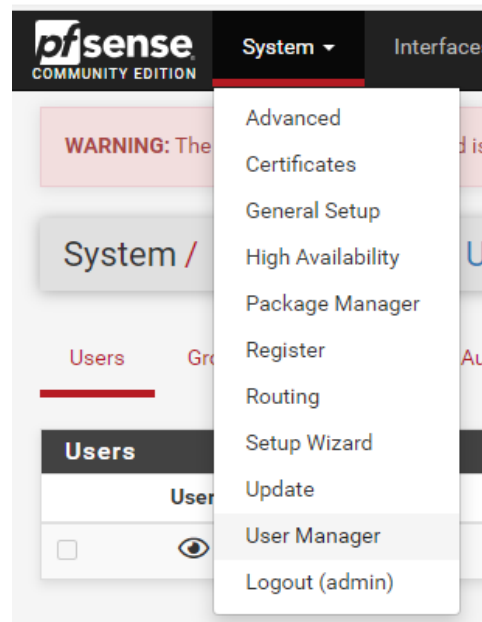
Authentication	
<u>Authentication Method</u>	<div>Use an Authentication backend</div> <div>Select an Authentication Method to use for this zone. One method must be selected.</div> <div>- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.</div> <div>- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.</div> <div>- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.</div>
<u>Authentication Server</u>	<div>Local Database</div> <div>You can add a remote authentication server in the User Manager.</div> <div>Vouchers could also be used, please go to the Vouchers Page to enable them.</div>
<u>Secondary authentication Server</u>	<div>Local Database</div> <div>You can optionally select a second set of servers to to authenticate users. Users will then be able to login using separated HTML inputs.</div> <div>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.</div>
<u>Reauthenticate Users</u>	<div><input type="checkbox"/> Reauthenticate connected users every minute</div> <div>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.</div>
<u>Local Authentication Privileges</u>	<div><input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set</div>

II. Configuration d'un groupe et des utilisateurs pour la délégation du Portail Captif

Pour créer un **groupe** et un **utilisateur** avec des privileges restreints permettant uniquement la création et la gestion des utilisateurs autorisés à se connecter au portail captif sur pfSense, accédez à l'interface web de pfSense et utilisez l'outil "**User Manager**" pour créer un nouveau groupe. Assurez-vous de sélectionner uniquement les permissions liées à la création et à la gestion des utilisateurs du portail captif pour ce groupe.

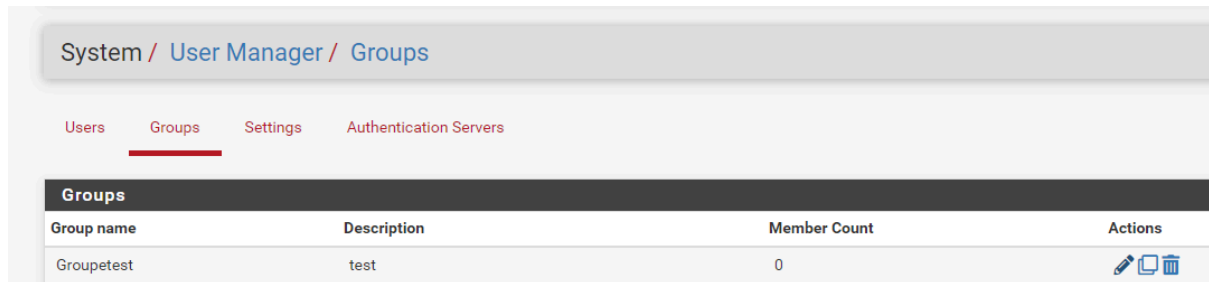
Ensuite, créez un nouvel utilisateur et ajoutez-le à ce groupe, en veillant à ce qu'il n'ait que les permissions nécessaires pour créer et gérer les utilisateurs du portail captif. Enregistrer les modifications pour finaliser la configuration.

Sélectionnez **System > User Manager**






A. Groupes

Puis “Groups”, cliquez sur “add”



System / User Manager / Groups

Users Groups Settings Authentication Servers




Groups			
Group name	Description	Member Count	Actions
Groupetest	test	0	  

Renseigner le nom du groupe puis une description. Cliquez sur “Save”

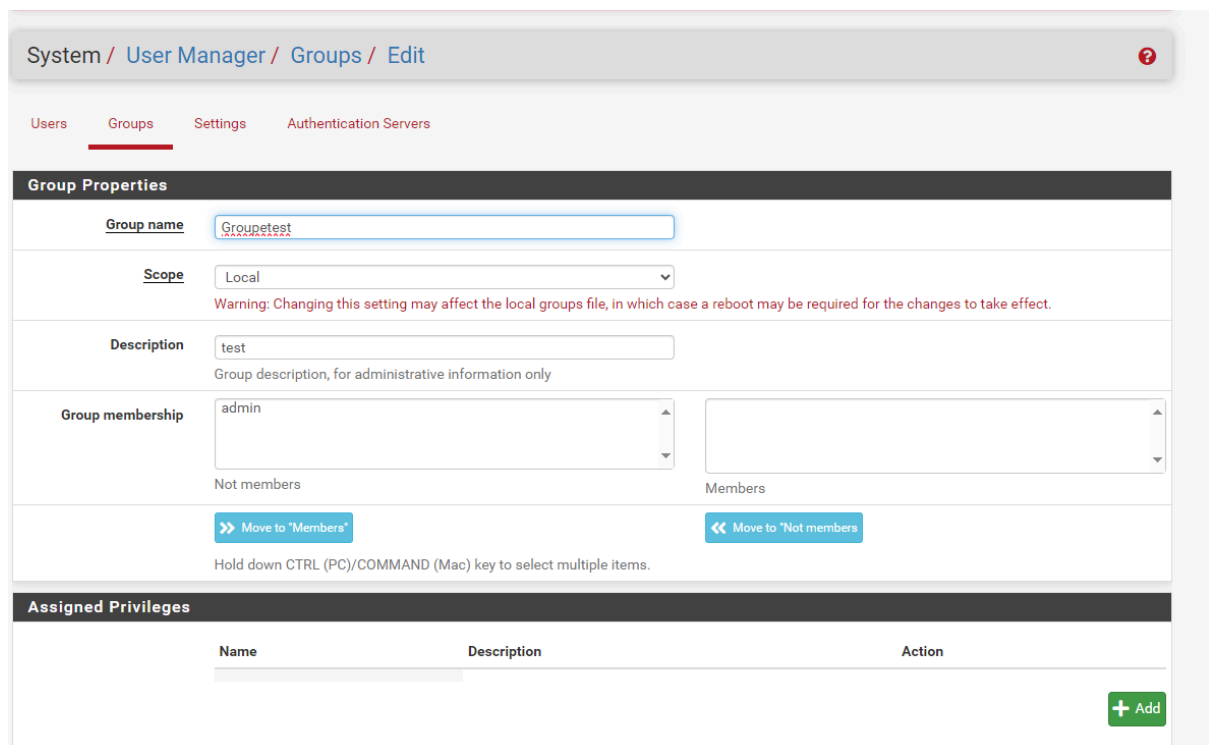


System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups			
Group name	Description	Member Count	Actions
Groupetest	test	0	  

Dans le menu “Actions”, modifier le groupe créé en cliquant sur le stylo.



System / User Manager / Groups / Edit

Users Groups Settings Authentication Servers

Group Properties

Group name

Scope
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description
Group description, for administrative information only

Group membership

Not members

Members


» Move to "Members"

« Move to "Not members"

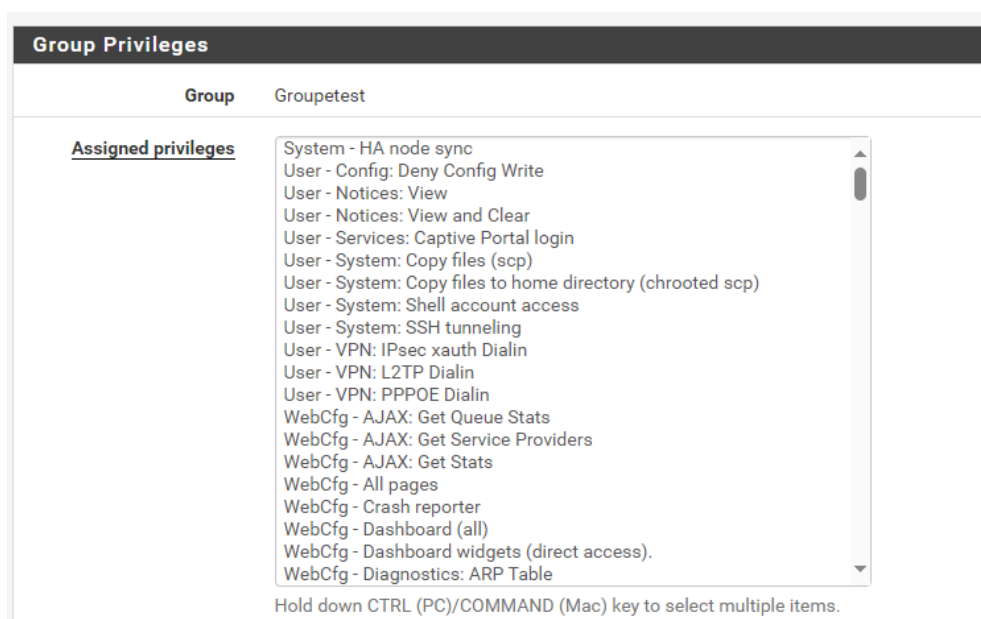
Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

Name	Description	Action
------	-------------	--------

 Add

Ensuite dans la rubrique “**Assigned Privileges**”, cliquez sur “**Add**”






Sélectionnez **WebCfg - System: User Manager**

Dans la rubrique "Assigned Privileges", cliquez sur "+ Add" pour ajouter de nouveaux privilèges.

Choisissez "**WebCfg - Status: Captive Portal**" dans la liste déroulante pour permettre à l'utilisateur de voir le statut des utilisateurs connectés au portail captif.

Enregistrez les modifications pour appliquer les nouveaux privilèges à l'utilisateur.

Assigned Privileges		
Name	Description	Action
WebCfg - System: User Manager	Allow access to the 'System: User Manager' page. (admin privilege)	
WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.	
Security notice: Users in this group effectively have administrator-level access		
		

Vérifier les droits, puis cliquez sur **“Save”**

Créez aussi un autre groupe pour les utilisateurs.

Onglet « Groups », cliquez sur « + Add »

Group Properties	
Group name	<input type="text" value="Portail"/>
Scope	<input type="text" value="Local"/> <small>Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.</small>
Description	<input type="text" value="Utilisateurs du portail"/> <small>Group description, for administrative information only</small>
Group membership	<div> <div> <input type="text" value="MrTest"/> <input type="text" value="admin"/> </div> <div> <small>Not members</small> </div> </div> <div> <input type="text"/> <div> <small>Members</small> </div> </div>
<div> <input type="button" value="» Move to 'Members'"/> <input type="button" value="« Move to 'Not members'"/> </div> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>	

Cliquez sur **“ + Add”** rubrique **“Assigned Privileges”**.

Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login**
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted scp)
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPOE Dialin
- WebCfg - AJAX: Get Queue Stats
- WebCfg - AJAX: Get Service Providers
- WebCfg - AJAX: Get Stats
- WebCfg - All pages
- WebCfg - Crash reporter
- WebCfg - Dashboard (all)
- WebCfg - Dashboard widgets (direct access).
- WebCfg - Diagnostics: ARP Table

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Sélectionnez dans la liste « **User – Services: Captive Portal login** » (Autorisé seulement à se connecter au Portail Captif)

Puis cliquez sur “**Save**”

B. Utilisateurs

On va commencer par créer un utilisateur ayant les droits de délégué pour la gestion du portail captif.

Users				
	Username	Full name	Status	Groups
<input type="checkbox"/>	admin	System Administrator	✓	admins

+ Add
Delete

Cliquez sur “**add**”

Entrez un nom d'utilisateur, son mot de passe.

Pensez aussi à sélectionner le groupe créé précédemment. c'est la rubrique “**Group Membership**”. cliquez sur “**Move to Member of list**” puis “**Save**”

The screenshot shows the 'User Properties' form for a user named 'MrTest'. The form includes fields for 'Username' (MrTest), 'Password' (masked with dots), 'Full name' (Utilisateur autorisé à créer des utilisateurs du Portail Captif), 'Expiration date' (empty), 'Custom Settings' (unchecked), 'Group membership' (admins), and 'Certificate' (No private CAs found). The 'Group membership' section shows a list of groups with 'Groupetest' selected. Below the list are buttons to 'Move to Member of list' and 'Move to Not member of list'.

L'utilisateur est autorisé à créer des utilisateurs pour la connexion et l'utilisation du portail captif.

Puis par la suite, on va créer un autre utilisateur pour le **portail captif**.

The screenshot shows the 'User Properties' form for a user named 'test'. The form includes fields for 'Username' (test), 'Password' (Password), 'Confirm Password' (empty), 'Full name' (Un utilisateur du portail), 'Expiration date' (empty), 'Custom Settings' (unchecked), 'Group membership' (Groupetest, admins), and 'Effective Privileges' (empty). The 'Group membership' section shows a list of groups with 'Groupetest' and 'admins' selected. Below the list are buttons to 'Move to Member of list' and 'Move to Not member of list'.

L'utilisateur « test » est autorisé à se connecter au Portail Captif.

C. Vérification

Connexion avec le compte “MrTest”

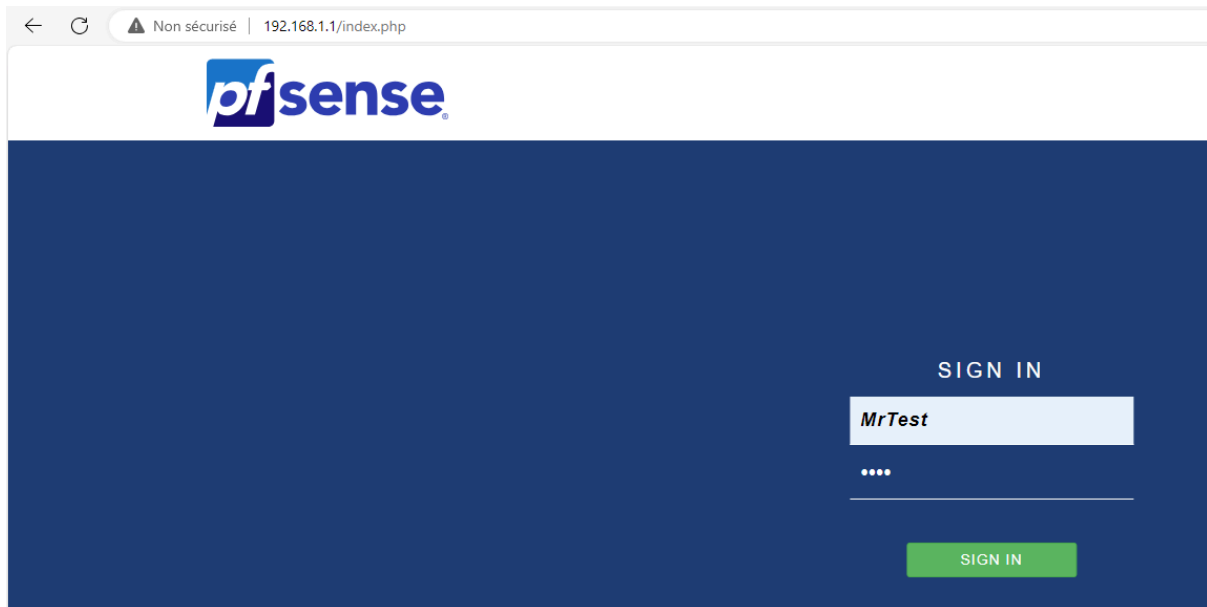
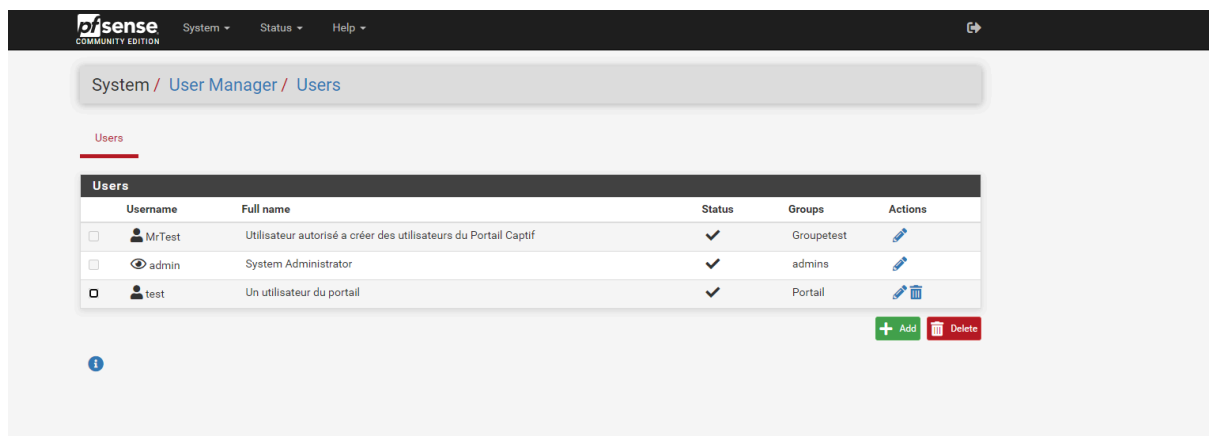





Tableau de bord restreint. Seulement les fonctions de création d'utilisateur et de Statut du Portail Captif sont disponibles.



III. Personnalisation du portail captif

A. Personnalisation du Logo

Services / Captive Portal				
Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
Portail_captif	LAN	0	portail captif	 
				 Add

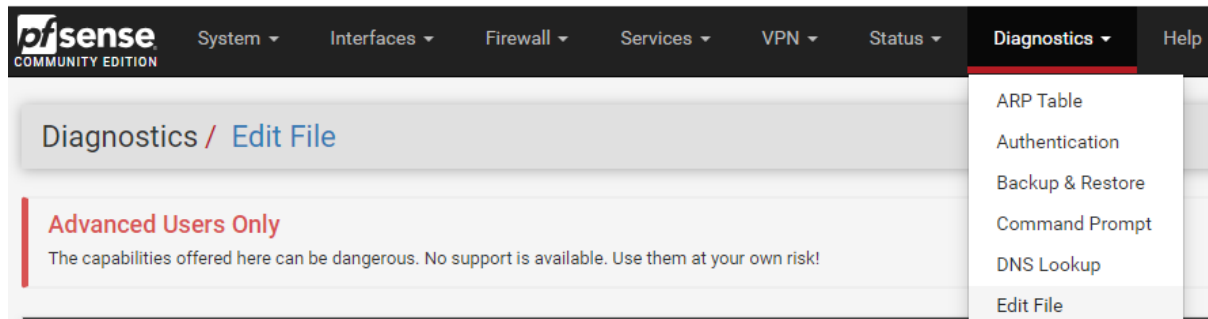
vous pourrez activer et configurer un logo personnalisé pour la page de connexion du portail captif sur pfSense. Cela permettra d'améliorer l'apparence et la convivialité de la page de connexion pour les utilisateurs.

- Cliquez sur l'onglet "**Services**" dans le menu principal de pfSense.
- Dans le menu déroulant, sélectionnez "**Captive Portal**" pour accéder aux paramètres du portail captif.
- Pour modifier la configuration du portail captif, cliquez sur l'icône en forme de stylo à côté de la rubrique "**Captive Portal Login Page**".
- Dans la section "**Captive Portal Login Page**", activez l'option **Enable Custom Logo Image** pour permettre l'utilisation d'un logo personnalisé.
- Cliquez sur le bouton "**Parcourir**" pour sélectionner l'image (logo) que vous souhaitez utiliser.
- Une fois que vous avez sélectionné votre image, enregistrez les modifications pour appliquer le logo personnalisé à la page de connexion du portail captif.

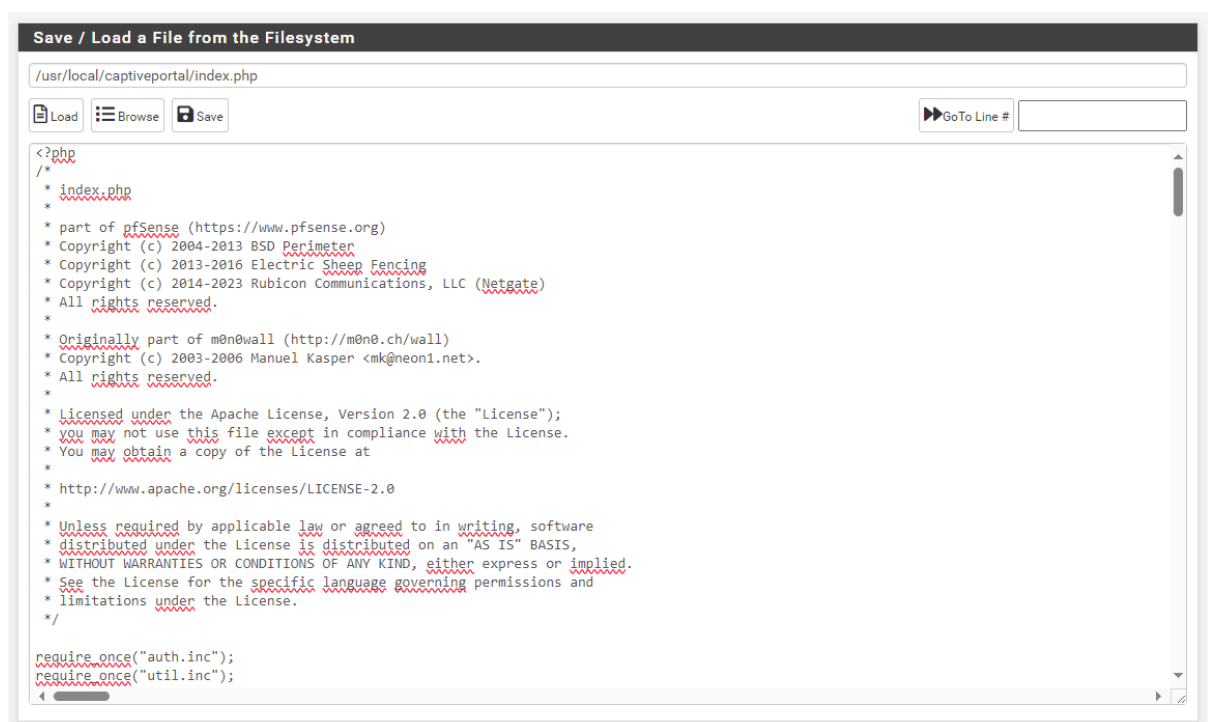
Captive Portal Login Page	
Display custom logo image	<input checked="" type="checkbox"/> Enable to use a custom uploaded logo
Logo Image	<div> <div>Choisir un fichier</div> <div>Aucun fichier n'a été sélectionné</div> </div> <p>Add a logo for use in the default portal login screen. File will be renamed 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.</p>
Display custom background image	<input type="checkbox"/> Enable to use a custom uploaded background image
Background Image	<div> <div>Choisir un fichier</div> <div>Aucun fichier n'a été sélectionné</div> </div> <p>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.</p>
Terms and Conditions	<div> <div></div> <div></div> </div> <p>Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out</p>

B. Personnalisation des fenêtres d'affichage

Sélectionnez “**Diagnostics > Edit Files**”



Tapez : `/usr/local/captiveportal` puis « **Browse** » puis cliquez sur « **index.php** »



Puis vous modifiez les phrases que vous souhaitez à l'aide de la recherche (**Ctrl+F**).

Par exemple “**You are connected**” ...

Une fois toutes les modifications effectuées, pensez à faire “**save**” pour enregistrer.

Il vous faudra ensuite redémarrer pfSense dans “**Diagnostics > Reboot**”

Résultat :

Pour voir le résultat, accéder à l'interface du portail captif.

IV. Enregistrement des logs

A. Squid : Qu'est-ce que c'est ?

Squid Proxy Server est un outil puissant qui peut améliorer les performances, la sécurité et le contrôle de l'accès à Internet sur votre réseau. Le service Squid Proxy Server permet de créer un serveur proxy sur votre réseau, ce qui offre plusieurs avantages :

- **Cache de contenu web** : Squid agit comme un cache de contenu web, ce qui signifie qu'il stocke localement les pages web fréquemment demandées. Cela permet d'accélérer l'accès aux sites web en réduisant le temps nécessaire pour récupérer le contenu à partir d'Internet.
- **Contrôle d'accès** : Squid permet de mettre en place des règles de contrôle d'accès, appelées ACL (Access Control Lists), qui vous permettent de contrôler quelles requêtes web sont autorisées à passer à travers le proxy et quelles requêtes sont bloquées. Cela vous permet de restreindre l'accès à certains sites web ou types de contenu.
- **Surveillance du trafic** : En configurant Squid pour enregistrer les logs de connexion, vous pouvez surveiller et analyser le trafic web qui passe à travers le proxy. Cela vous permet de surveiller l'activité des utilisateurs, de détecter les problèmes de sécurité potentiels et de générer des rapports sur l'utilisation d'Internet.
- **Anonymat et filtrage de contenu** : Squid peut être utilisé pour masquer l'adresse IP des clients lorsqu'ils accèdent à des sites web, ce qui peut améliorer la confidentialité et la sécurité en ligne. De plus, Squid peut être configuré pour filtrer le contenu web en fonction de critères tels que les mots-clés, les types de fichiers, etc.

Pour installer le package "**Squid**"

Vous pour le faire dans **Package Manager > Available Packages**

pfSense COMMUNITY EDITION

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

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: squid Both [Search] [Clear]

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
Lightsquid	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.72 lightsquid-1.8_5	+ Install
squid	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-7.2 squid_radius_auth-1.10 squid-6.3 c-icap-modules-0.5.5_1	+ Install
squidGuard	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15 pfSense-pkg-squid-0.4.46	+ Install

Le téléchargement du package peut prendre un peu de temps. Veuillez patienter.

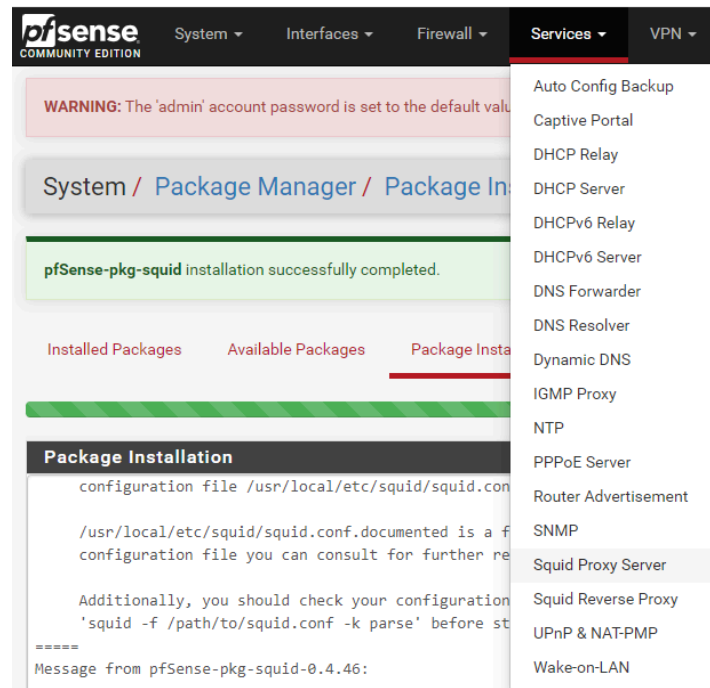
Installed Packages Available Packages Package Installer

Package Installation

```
>>> Installing pfSense-pkg-squid...
Updating pfSense-core repository catalogue...
Fetching meta.conf:
Fetching packagesite.pkg:
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
Fetching meta.conf:
```

Une fois terminée, vous verrez les services suivantes apparaître :

- **Squid Proxy Server**
- **Squid Reverse proxy**



Sélectionnez “**Services > Squid Proxy Server**”

Onglet “**Authentication**” – Sélectionner la méthode d'authentification “**Captive Portal**”

B. **LightSquid** : Qu'est-ce que c'est ?

LightSquid est un outil précieux pour les administrateurs réseau et les responsables informatiques, car il fournit des informations détaillées sur l'utilisation d'Internet, ce qui permet une gestion plus efficace du réseau et une meilleure sécurité.

- **Rapports d'utilisation d'Internet** : LightSquid génère des rapports détaillés sur l'utilisation d'Internet, notamment les sites web visités, la quantité de bande passante utilisée, les utilisateurs les plus actifs, les heures de pointe, etc.
- **Visualisations graphiques** : Les données de trafic web sont présentées sous forme de graphiques et de tableaux faciles à comprendre, ce qui permet de visualiser rapidement les tendances et les schémas d'utilisation.
- **Suivi de la productivité** : LightSquid peut être utilisé pour surveiller l'activité Internet des employés, ce qui peut aider les entreprises à garantir que les ressources informatiques sont utilisées de manière appropriée et productive.
- **Détection des problèmes de sécurité** : En analysant les logs de Squid, LightSquid peut aider à détecter les activités suspectes ou non autorisées sur le réseau, telles

que l'accès à des sites web malveillants ou le téléchargement de fichiers potentiellement dangereux.

- **Planification des capacités réseau** : En fournissant des données sur la quantité de bande passante utilisée et les tendances de trafic, LightSquid peut aider à planifier les capacités réseau et à identifier les éventuels goulets d'étranglement.
- **Conformité aux politiques** : LightSquid peut aider les entreprises à surveiller et à garantir la conformité aux politiques en matière d'utilisation d'Internet, telles que les politiques de sécurité informatique et les politiques d'utilisation acceptable.

Pour l'installer, procéder comme précédemment.

V. Gestion Vlan

Accédez à l'onglet VLAN et cliquez sur le bouton Ajouter.

Sur l'écran VLAN, effectuez les configurations suivantes :

- Interfaces parent - Sélectionnez l'interface physique
- Étiquette VLAN - Entrez le numéro d'identification VLAN
- Description - Entrez une description en option

VLAN Configuration

Parent Interface

hn1 (00:15:5d:c9:0b:15) - lan

Only VLAN capable interfaces will be shown.

VLAN Tag

1

802.1Q VLAN tag (between 1 and 4094).

VLAN Priority

0

802.1Q VLAN Priority (between 0 and 7).

Description

Description

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

Cliquez sur le bouton **save** pour créer le pfsense Vlan.

Une fois le VLAN créé, il sera visible dans les interfaces.

Vous pourrez donc le modifier et le configurer comme bon vous semble.