



PROJET INFRA & SI :

2^e PROJET / ARCHITECTURE RESEAU ET SECURITE

Kassab John – Jacques Hugo

Année 2020 / 2021

Ce dossier technique a pour but de montrer comment mettre en place un routeur pour administrer son réseau en y ajoutant diverses fonctionnalités tel qu'un serveur DHCP, un portail captif etc...

Nous avons choisi **pfSense** car c'est un routeur/pare-feu open source avec une documentation très complète. Il a pour but d'assurer la sécurité périmétrique. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels.

INSTALLATION ET CONFIGURATION DE PFSENSE

Avant de commencer à configurer pfSense, nous allons voir comment l'installer. Pour se faire on se rend sur <https://www.pfsense.org/download/> et on télécharge la version souhaitée.

Une fois l'image téléchargé on se rend dans VMWare et on définit les paramètres suivant lors de la création de la machine virtuelle :

- « **Create a New Virtual Machine** »
 - « **Custom (Advanced)** »
 - Hardware Compatibility: « **Workstation 11.x ou Workstation 12.x** »
 - Install From: « **I will install the operating system later** »
 - Select a Guest Operating System: « **Other à FreeBSD 64-bit** »
 - Virtual Machine Name : « **pfSense** »
 - Processors :
 - Numbers of Processors : « **1** »
 - Number of Cores per Processor: « **1** »
 - Memory for this Virtual Machine: « **512 MB** »
 - Network Connection: « **Use Bridged Networking** »
 - SCSI Controller : « **LSI Logic (Recommended)** »
 - Virtual Disk Type : « **IDE ou SCSI** »
 - **Create a New Virtual Disk**
 - Max Disk Size: « **5 GB** » « **Store Virtual Disk as a single file** »

Votre VM s'affiche sur l'interface VMware, cliquez sur « **Edit virtual machine setting** », sélectionnez la ligne « **Sound Card** » et cliquez sur le bouton « **Remove** » en bas. Sélectionnez la ligne « **USB Controller** » et décochez toutes les cases. Sélectionnez la ligne « **CD/DVD** » puis cochez la case « **Use ISO image File** », cliquez sur

« **Browse...** » et sélectionnez l'ISO de pfSense que vous avez sans doute téléchargé. On peut maintenant installer pfSense. Au redémarrage, on y applique les paramètres suivants :

« **Boot Multi User** » accepter les conditions

- Choisir le clavier « **French ISO-8859-1** »
- Montez d'un cran pour continuer avec le clavier «**iso.kbd keymap** »
- Partitioning: « **Auto (UFS) Guided Disk Setup** »
- Manual Configuration « **No** »

Au démarrage, on a une suite de questions, voici les paramètres à appliquer :

```
Should VLANs be set up now [y/n]? n
Enter the WAN interface name or 'a' for auto-detection (em0 or a): em0
Enter the LAN interface name or 'a' for auto-detection NOTE: This enables full Firewalling/NAT mode. ( a or nothing if finished): <ENTÉE>
The interfaces will be assigned as follows
WAN -> em0
Do you want to proceed [y/n]? y
```

Etant donné que nous possédons qu'une seule carte réseau, nous allons en ajouter une autre. Pour se faire, on édite les paramètres de la machine virtuelle pfSense. En bas, cliquez sur le bouton « **Add** » sélectionnez « **Network Adapter** » et valider.

Relancer pfSense pour prendre en compte les nouvelles cartes réseaux qu'on vient de rajouter. Nous allons maintenant les configurer sous pfSense.

- Tapez « **1** » pour *Assign Interfaces* et y appliquer les paramètres suivants
 - o Should VLANs be set up now → **n**
 - o Enter the WAN interface name or 'a' for auto-detection: **em0**
 - o (em1 or nothing if finished): **em1**

Sur votre PC (*machine hôte*), lancez une invite de commande (CMD) et tapez « **ipconfig /all** ». Il faut donc identifier l'**adresse IP de votre PC** et la **passerelle**.

Vous ne pouvez pas utiliser l'adresse de votre PC pour l'interface **WAN de pfSense** car justement votre PC l'utilise déjà. Il faut donc choisir une autre adresse.

J'ai donc choisi **192.168.1.26** ; le masque et la passerelle ne change pas.

Nous allons désormais définir les adresses du WAN et du LAN :

- Tapez « **2** » pour « **Set interface(s) IP address** »
 - Enter the new WAN IPv4 address: **192.168.1.26**
 - Enter the new WAN IPv4 subnet: **24**
 - Configure IPv6 address WAN interface via DHCP6 : **n**
 - Do you want to revert to HTTP as the webConfigurator protocol: **y**

L'interface **WAN** est prête, vous pouvez même faire un test avec la commande PING.

- Tapez « **7** » pour « **Ping host** »
- Tapez : **google.fr**
- Où : **8.8.8.8**

Pour l'interface LAN, c'est la même procédure :

- Tapez « **2** » pour « **Set interface(s) IP address** »
 - Enter the new LAN IPv4 address: **192.168.1.1**
 - Enter the new LAN IPv4 subnet: **24**
 - Do you want to enable DHCP server on LAN: **n**
 - Do you want to revert to HTTP as the webConfigurator protocol: **y**

C'est bon pour le réseau **LAN (LAN-Serveurs)**. L'interface web de pfSense est accessible à l'adresse **http://192.16.1.1/** avec les identifiants par défaut suivant de pfSense : **admin - pfsense**

On obtient un résultat similaire à ça :

```
pfSense 2.5.0-RELEASE amd64 Tue Feb 16 08:56:29 EST 2021
Bootup complete

FreeBSD/amd64 (pfsense.johnhugo.com) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 2bd5c982d3afcc77a870

*** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfsense ***

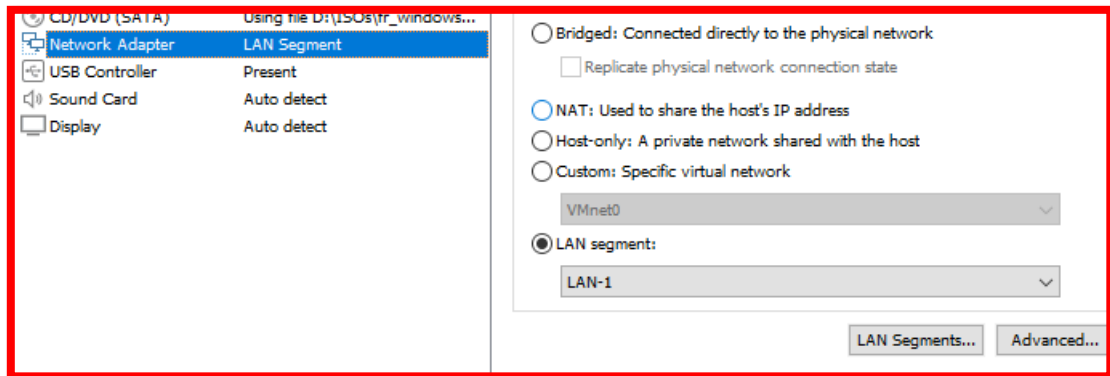
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.26/24
                                v6/DHCP6: 2a01:cb0c:dbd:4700:20c:29ff:fe20:d8b
7/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

C'est terminé pour l'installation et la configuration à partir de la VM, désormais tout se fera à partir de l'interface Web de pfSense. Je vais en profiter pour installer **Windows Education N** et le configurer sur le réseau **LAN**, je pourrais ensuite me connecter à l'interface web de pfSense.

Pour se faire, on accède au paramètre de notre VM Client :



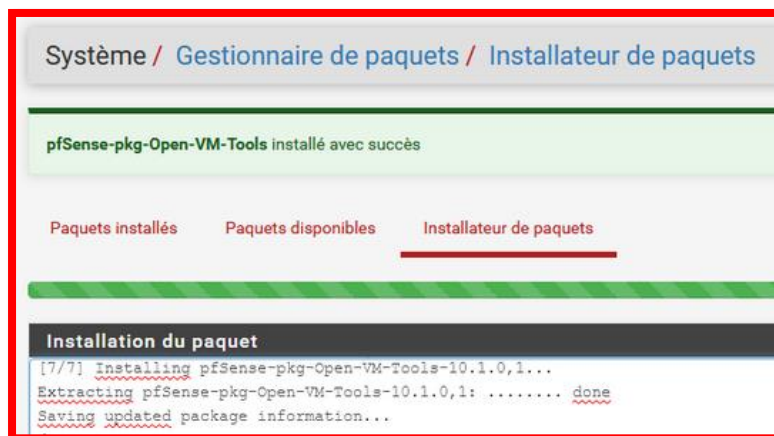
Notre VM Client fait désormais partie du même réseau que notre routeur.

On se connecte à l'interface pfSense à l'adresse suivante (dans mon cas) : <http://192.168.1.1>

Par défaut : user : **admin** ; password : **pfsense**

Une fois connecté, cliquez sur <Next> pour procéder à une configuration initiale. C'est facultatif, vous pouvez aussi cliquer sur le logo pfSense pour atteindre le tableau de bord.

- À l'étape 3/9, « **Time Server Information** », sélectionnez Europe/Paris dans « **Timezone** » laissez le reste par défaut.
- À l'étape 6/9, mettez un mot de passe pour le **compte admin**.
- Vous pouvez mettre pfSense en Français depuis le menu **System / General Setup** .



MISE EN PLACE DU SERVICE DHCP

Dans votre interface pfSense, cliquez sur le menu **Services**, puis sur **DHCP Server**. Vous aurez deux possibilités :

- Mise en place d'un DHCP sur la partie WAN
- Mise en place d'un DHCP sur la partie LAN
- Le plus intéressant, c'est de mettre en place un **DHCP dans la partie LAN** ; cliquez donc sur « LAN », juste en dessous du bandeau gris.
 - On se rend dans « **Services → DHCP Server → LAN** »
 - Pour commencer, nous cochons évidemment la case "Enable DHCP server on LAN interface".
 - On définit la tranche d'IP attribuable sur notre réseau. Dans notre cas, nous autorisons des connexions de 192.168.1.10 à 50

The screenshot shows the 'Services / DHCP Server / LAN' configuration page. Under 'General Options', the 'Enable DHCP server on LAN interface' checkbox is checked. The 'Deny unknown clients' dropdown is set to 'Allow all clients'. The 'Subnet' is 192.168.1.0, the 'Subnet mask' is 255.255.255.0, and the 'Available range' is 192.168.1.1 - 192.168.1.254. At the bottom, the 'Range' is defined from 192.168.1.10 to 192.168.1.50.

On peut vérifier le fonctionnement du serveur DHCP en se rendant dans « **Status → DHCP Leases** »

The screenshot shows the 'Status / DHCP Leases' page. It includes a search bar and a table of leases. One lease is shown for IP 192.168.1.10, MAC 00:0c:29:bd:43:29, and Client ID PC-Client01. Below the table, a summary for the LAN interface shows a pool from 192.168.1.10 to 192.168.1.50 with 1 lease in use.

IP address	MAC address	Client Id	Hostname	Description	Start	End	On
192.168.1.10	00:0c:29:bd:43:29	PC-Client01			2021/03/16 09:02:54	2021/03/16 11:02:54	or

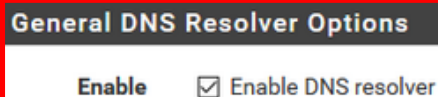
Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.1.10	192.168.1.50	1

On aperçoit bien que ma machine soit connectée en utilisant la première adresse de la range que nous avons attribué, c'est-à-dire **192.168.1.10**

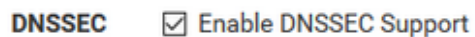
MISE EN PLACE DU SERVEUR DNS

- La configuration du serveur DNS se fait via le menu « **Services / DNS Resolver** »

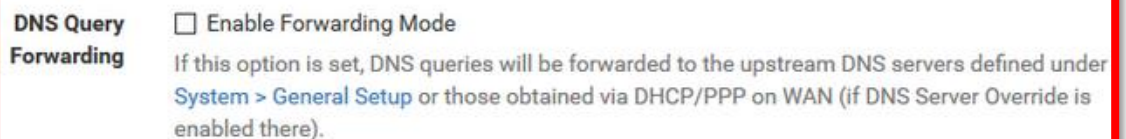
- On commence par activer le service (on coche la case *Enable*).



- On active la vérification des domaines, il suffit de cocher *DNSSE*.



- Ne reste qu'à s'assurer que le serveur effectue ses requêtes plutôt que les transmettre à d'autres serveurs. Pour ça, on décoche *DNS Query Forwarding*.

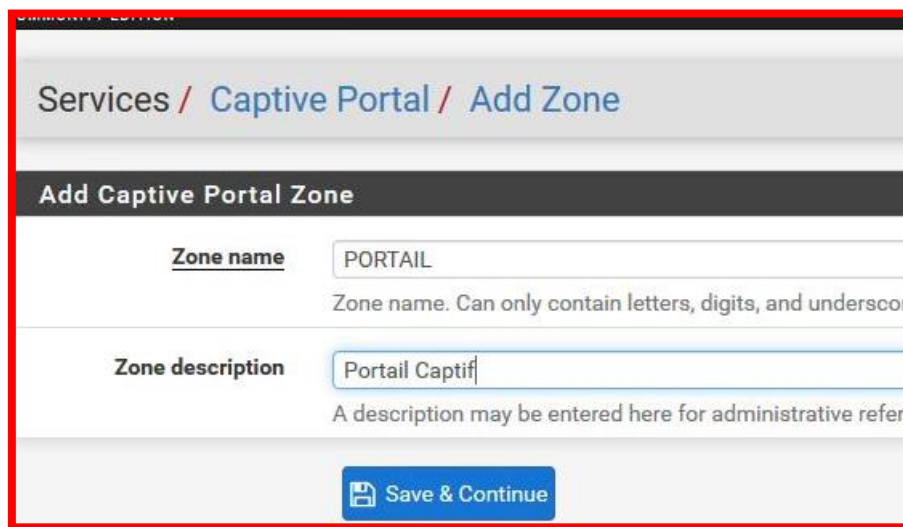


Pour connaître l'état du serveur, vous pouvez passer par le menu « **Status / DNS Resolver** ». Cet écran vous liste les serveurs *racines* qu'il connaît. La liste est longue mais montre que, globalement, tout marche correctement.

Status / DNS Resolver									
DNS Resolver Infrastructure Cache Speed									
Server	Zone	TTL	Ping	Var	RTT	RTO	Timeout A	Timeout AAAA	Timeout Other
216.40.47.26	johnhugo.com.	881	12	95	392	392	0	0	0
13.107.24.205	azure.com.	703	13	97	401	401	0	0	0
2620:1ec:8ec::c9	azuredns-prd.org.	900	4	79	320	320	0	0	0
192.12.94.30	net.	307	2	76	306	306	0	0	0
131.253.21.1	msedge.net.	307	8	20	88	88	0	0	0
2a01:111:4000::cd	msftncsi.com.	738	3	77	311	311	0	0	0
64.4.48.205	azure.com.	289	3	79	319	319	0	0	0
2603:1061::c9	cloudapp.net.	770	2	76	306	306	0	0	0
2603:1061::c9	azuredns-prd.info.	900	9	70	289	289	0	0	0
95.100.168.130	akadns.net.	12	6	50	206	206	0	0	0
2.22.22.167	dscd.akamai.net.	81	2	77	310	310	0	0	0
2620:1ec:bda::c9	azuredns-prd.info.	289	2	76	306	306	0	0	0

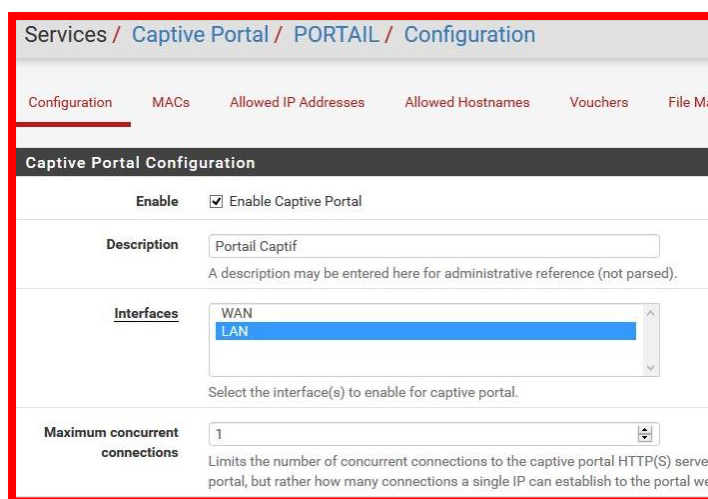
MISE EN PLACE D'UN PORTAIL CAPTIF

- On commence par la configuration du portail captif :
 - On se rend dans « **Services** → **Captive Portal** »
 - On ajoute un portail captif en appuyant sur le « + »



The screenshot shows the 'Add Captive Portal Zone' configuration page. The breadcrumb trail is 'Services / Captive Portal / Add Zone'. The page title is 'Add Captive Portal Zone'. There are two input fields: 'Zone name' with the value 'PORTAIL' and 'Zone description' with the value 'Portail Captif'. Below the 'Zone name' field, there is a note: 'Zone name. Can only contain letters, digits, and underscores'. Below the 'Zone description' field, there is a note: 'A description may be entered here for administrative reference'. At the bottom of the form, there is a blue button labeled 'Save & Continue'.

- Activer « **Enable Captive Portal** » et sélectionner l'interface « **LAN** »
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur)



The screenshot shows the 'Captive Portal Configuration' page. The breadcrumb trail is 'Services / Captive Portal / PORTAIL / Configuration'. The page title is 'Captive Portal Configuration'. There are several tabs: 'Configuration', 'MACs', 'Allowed IP Addresses', 'Allowed Hostnames', 'Vouchers', and 'File Manager'. The 'Configuration' tab is selected. The page has several sections: 'Enable' with a checked checkbox 'Enable Captive Portal'; 'Description' with the value 'Portail Captif' and a note 'A description may be entered here for administrative reference (not parsed)'; 'Interfaces' with a dropdown menu showing 'WAN' and 'LAN' (selected); and 'Maximum concurrent connections' with a value of '1'. Below the 'Maximum concurrent connections' field, there is a note: 'Limits the number of concurrent connections to the captive portal HTTP(S) server, but rather how many connections a single IP can establish to the portal web page'.

- Activer « **Enable logout popup window** » (une fenêtre popup permet aux clients de se déconnecter)

- Définir « **Pre-authentication Redirect URL** » (URL de redirection par défaut. Les visiteurs ne seront redirigés vers cette URL après authentification que si le portail captif ne sait pas où les rediriger)
- **Note** : Avec « **http://....** » devant le domaine : Exemple : <http://www.google.fr>
- Définir « **After authentication Redirection URL** » (URL de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement tenté d'accéder après s'être authentifiés)
- **Note** : Avec « **http://....** » devant le domaine : Exemple : <http://www.google.fr>
- Activer « **Disable Concurrent user logins** » (seule la connexion la plus récente par nom d'utilisateur sera active)
- Activer « **Disable MAC filtering** » (nécessaire 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 to disconnect before the idle or hard timeout occurs.
Pre-authentication redirect URL	<input type="text" value="http://www.google.fr"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication. This field will be accessible through \$PORTAL_REDURL\$ variable.
After authentication Redirection URL	<input type="text" value="http://www.google.fr"/> Set a forced redirection URL. Clients will be redirected to this URL after authentication.
Blocked MAC address redirect URL	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting to connect.
Concurrent user logins	<input checked="" type="checkbox"/> Disable Concurrent user logins If enabled only the most recent login per username will be active. All other logins will be disconnected.
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of the client cannot be determined (usually because there is no DHCP server on the network).

- Sélectionner «**Use an Authentication backend** »
- Sélectionner «**Local Database**» pour «**Authentication Server**»

- **Attention** : Ne pas sélectionner «**Local Database** » pour «**Secondary Authentication Server**»
- Activer « **Local Authentication Privileges** » (Autoriser uniquement les utilisateurs avec les droits de « Connexion au portail captif ») puis **Save**

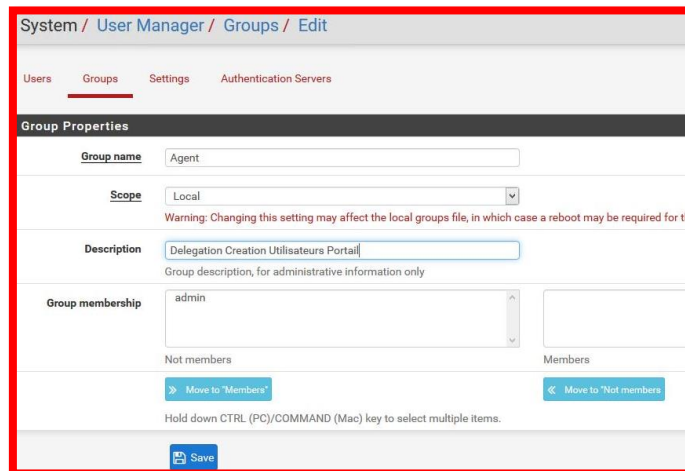
On obtient ce résultat :



Zone	Interfaces	Number of users	Description	Action
PORTAIL	LAN	0	Portail Captif	 





→ Création d'un groupe et utilisateur qui aura pour fonction de créer des Utilisateurs autorisés a se connecter au Portail Captif. Ce groupe et utilisateurs associés auront seulement le droit de créer des Utilisateurs du Portail Captif.

- Dans « **Groups** », cliquez sur « **Add** »
- Renseignez le **Nom du Groupe** "Agent" et sa **description** "Delegation Creation Utilisateurs Portail". Cliquez "**Save**"



- Dans le menu « **Actions** », **modifier le groupe** créé en cliquant sur le stylo



Group name	Description	Member Count	Actions
Agent	Delegation Creation Utilisateurs Portail	0	 
admins	System Administrators	1	
all	All Users	1	

- Cliquez sur « **Add** » puis « **Assign Privileges** »
 - Sélectionnez dans la liste « **WebCfg – System: User Manager** » (Accès à la page de gestion des utilisateurs "User Manager")
 - Sélectionnez dans la liste « **WebCfg – Status: Captive Portal** » (Voir le Status des utilisateurs connectés")
 - **Vérifier les droits**, puis cliquez sur « **Save** »
- Dans « **Users** », cliquez sur « **Add** »
 - Entrer un **Nom d'Utilisateur** "agent", son **mot de passe** et sa **description** (Agent autorisé à créer des utilisateurs du Portail Captif).
 - Sélectionner dans « **Group membership** » le groupe « Agent » précédemment créé. Cliquez sur « **Move to Member of list** » puis « **Save** »

La délégation pour l'utilisateur "Agent" est autorisé a créer des utilisateurs pour connexion au Portail Captif

The screenshot shows the 'User Properties' configuration page. The 'Group membership' section is highlighted, showing a list of groups with 'Agent' selected. The 'Move to Member of list' button is visible at the bottom right of the group membership section.

Configuration du Groupe et Utilisateurs autorisés à se connecter au Portail Captif

Ce groupe et utilisateurs associés auront seulement le droit d'utiliser le Portail Captif.

Onglet « **Groups** », cliquez sur « **+ Add** »

Groups Properties

Group name Portail

Scope Local

Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the c

Description Utilisateurs du Portail

Group description, for administrative information only

Group membership admin agent

Not members Members

» Move to "Members" « Move to "Not members"

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

Renseigner le **Nom du Groupe** « Portail » et sa **description** « Utilisateurs du Portail ». Cliquez « **Save** »

Dans le menu « Actions », **modifier** le groupe créé en cliquant sur le stylo

Cliquez sur « **+ Add** » rubrique « **Assigned Privileges** ».

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

Onglet « **Users** », cliquez sur « **+ Add** »

Entrer un **Nom d'Utilisateur** « testportail », son **mot de passe** et sa **description** : « Un Utilisateur du Portail ».

Sélectionner dans « **Group membership** » le groupe « Portail » précédemment créé. Cliquez sur « **Move to Member of list** » puis « **Save** »

Defined by USER

Disabled ☐ This user cannot login

Username test

Password ****

Full name Un Utilisateur du Portail

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

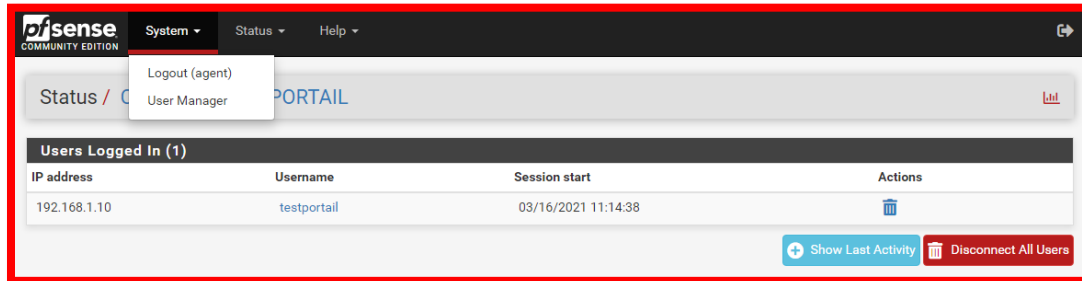
Group membership Agent admins

Not member of Member of

L'utilisateur testportail est désormais autorisé à se connecter au portail captif

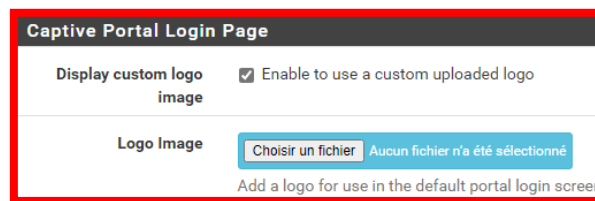
→ Connexion avec le Compte "agent"

Cet utilisateur a seulement le droit de créer des Utilisateurs du Portail Captif par délégation et de voir le Statut des utilisateurs connectés.

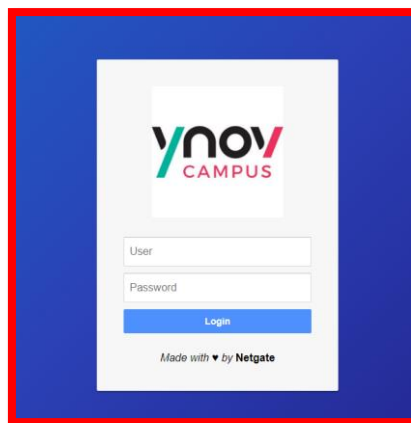


Pour personnaliser le portail captif, on se rend dans « **Services** », « **Captive Portal** » puis on modifie la configuration du portail.

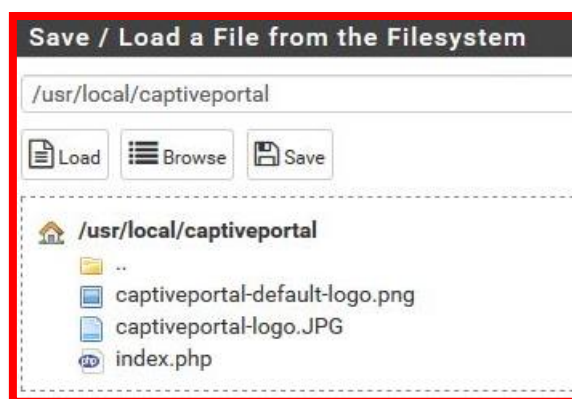
Rubrique « **Captive Portal Login Page** » : Activer « **Enable Custom Logo Image** » puis parcourir pour sélectionner votre image



Lors de la prochaine connexion, les utilisateurs auront le droit à cette interface de connexion :



- Pour que le portail s'affiche en français :
 - Sélectionner « **Diagnostics** » puis « **Edit File** »
 - Tapez : /usr/local/captiveportal puis « Browse » puis cliquez sur « index.php »



Rechercher (Ctrl + F) « You are connected » → Remplacer par : « Vous êtes connecté »

```
return;
elseif (!empty($session) && (!isset($_POST
/* If client try to access captive portal
but no custom logout page does exist as
echo gettext("You are connected.");
ob_flush();
```

Rechercher (Ctrl + F) « Disconnecting... » et « You have been disconnected » - Remplacer par « Déconnexion... » et « Vous êtes déconnecté »

```
Save / Load a File from the Filesystem
/usr/local/captiveportal/index.php
Load Browse Save
if ($_POST['logout_id']) {
    echo <<EOD
<html>
<head><title>Disconnecting...</title></head>
<body bgcolor="#435370">
<span style="color: #ffffff; font-family: Tahoma, Verdana, sans-serif;">
<b>You have been disconnected.</b>
</span>
```

Rechercher (Ctrl + F) « Invalid credentials specified » - Remplacer par « Les informations saisies sont invalides »

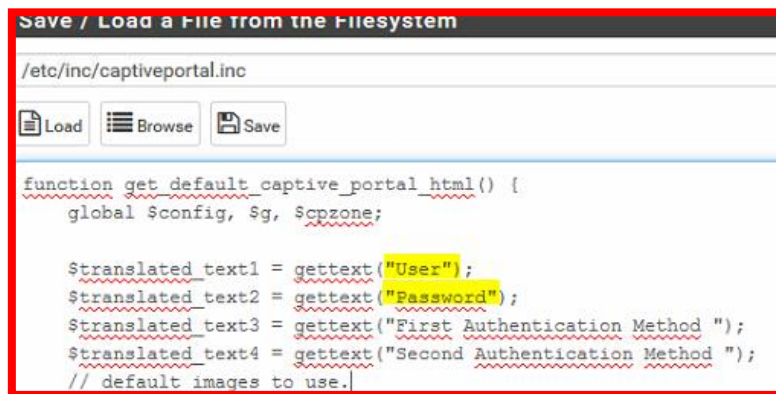
```
if ($auth_result['login_message']) {
    $replymsg = $auth_result['login_message'];
} else {
    $replymsg = gettext("Invalid credentials specified.");
}
```

Tapez : /etc/inc puis « Browse » puis cliquez sur « captiveportal.inc »

Rechercher (Ctrl + F) « Captive Portal login Page » - Remplacer par : « Portail Ynov Project »



Rechercher (Ctrl + F) "User" et "Password" - Remplacer par "Utilisateur" et "Mot de Passe"



On a terminé pour le portail captif. En résumé, nous avons mis un système d'administration et nous avons modifié l'interface de connexion des utilisateurs.

CONFIGURATION DE SQUIDGUARD ET MISE EN PLACE D'UNE BLACKLIST

Sélectionner "Services" et "SquidGuard Proxy Filter"

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ **Services ▾** VPN ▾

Status / Dashboard

System Information	
Name	pfSense.localdomain
User	admin@192.168.2.101 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: 391ed73786ee43989c09
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Wed May 23 2012
Version	2.4.4-RELEASE (amd64) built on Thu Sep 20 09:03:12 EDT 2018 FreeBSD 11.2-RELEASE-p3 The system is on the latest version. Version information updated at Mon Oct 1 15:00:00 UTC 2018
CPU Type	Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	03 Hours 01 Minute 26 Second

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server & RA
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- IGMP Proxy
- Load Balancer
- NTP
- PPPoE Server
- SNMP
- Squid Proxy Server
- Squid Reverse Proxy
- SquidGuard Proxy Filter**
- UPnP & NAT-PMP
- Wake-on-LAN

Activer SquidGuard **"Enable"**

Activer **"Enable Log"** et **"Enable log rotation"**

Logging options	
Enable GUI log	<input type="checkbox"/> Check this option to log the access to the Proxy Filter GUI.
Enable log	<input checked="" type="checkbox"/> Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation	<input checked="" type="checkbox"/> Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Miscellaneous	
Clean Advertising	<input type="checkbox"/> Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

Activer **"Enable Blacklist"** et insérer dans **Blacklist URL** :

`http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz`

Puis cliquez sur **"Save"**

Onglet **"Blacklist"** : Cliquer sur **"Download"** pour télécharger les listes de filtrage

Onglet **"Common ACL"**, Cliquez, dans **"Target Rules List"** sur le **" + "**

Sélectionner les catégories à bloquer (ou à autoriser)

Sélectionnez **"Allow"** pour **"Default access [all]"**

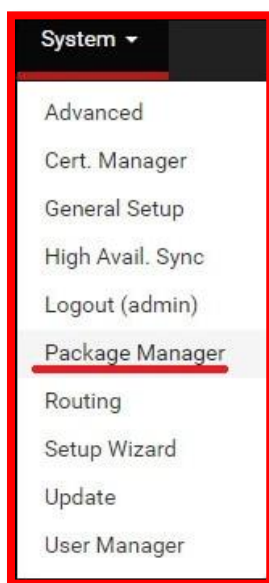
Cochez "Do not allow IP addresses in URL" et "Use Safe Search engine"

Puis cliquer "Save"

MISE EN PLACE DE SNORT

Snort est un système de détection d'intrusion libre publié sous licence GNU GPL

Accédez au menu Pfsense System et sélectionnez l'option De gestionnaire de paquets.



Sur l'écran du gestionnaire de paquets, accédez à l'onglet Paquets disponibles.

Sur l'onglet Paquets disponibles, recherchez SNORT et installez le paquet Snort.



Dans notre exemple, nous avons installé la version 3.2.9.10 du paquet Snort.

Attendez la fin de l'installation Snort.

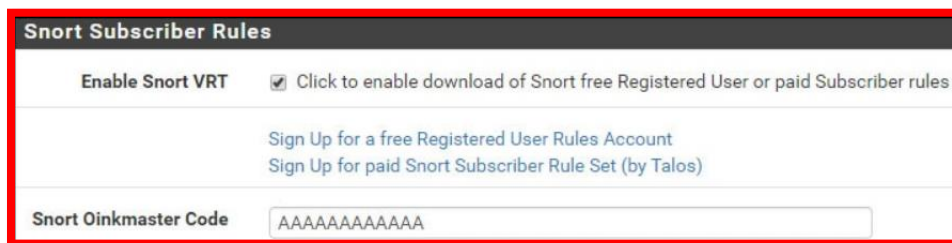
Accédez au menu Pfsense Services et sélectionnez l'option Snort.

Sur l'onglet Paramètres Global, localisez les règles d'abonné Snort et effectuez la configuration suivante :

Activer Snort VRT - Oui

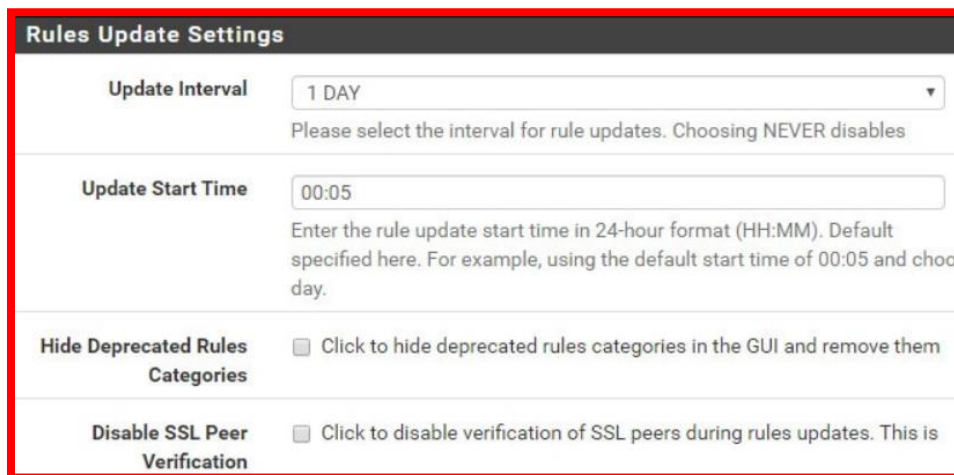
Code Snort Oinkmaster - Entrez-vous OikCode

Si vous n'avez pas d'Oinkcode, accédez au [site Web Snort](#), créez un compte et obtenez un Oinkcode gratuit.



Localiser la zone Paramètres de mise à jour des règles et effectuer la configuration suivante :

- Intervalle de mise à jour - Sélectionnez l'intervalle de mise à jour souhaité
- Heure de démarrage de mise à jour - Définir l'heure désirée pour mettre à jour les règles Snort



Localiser la zone Paramètres généraux et effectuer la configuration suivante :

Supprimer l'intervalle des hôtes bloqués - 1 heure

Supprimer les hôtes bloqués après la désinstallation - Non

- Conserver les paramètres snort après la désinstallation - Oui

- Intervalle de mise à jour de démarrage/shutdown - non

General Settings

Remove Blocked Hosts Interval

1 HOUR

Please select the amount of time you would like hosts to be blocked.

Remove Blocked Hosts After Deinstall

☐ Click to clear all blocked hosts added by Snort when removing the

Keep Snort Settings After Deinstall

☒ Click to retain Snort settings after package removal.

Startup/Shutdown Logging

☐ Click to output detailed messages to the system log when Snort is

Sur l'onglet Interfaces Snort, cliquez sur le bouton Ajouter et effectuez la configuration suivante.

Activer - Oui

Interface - Sélectionnez l'interface désirée pour surveiller

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer.

Sur l'écran des interfaces Snort, modifiez la configuration de l'interface.

Interface Settings Overview						
Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
WAN (em0)		AC-BNFA	ENABLED	DISABLED	WAN	

Accédez à l'onglet Catégories Wan et effectuez la configuration suivante :

Résoudre les débits - Oui

- Utiliser la politique IPS - Oui

Sélection des politiques IPS - Connectivité

Automatic Flowbit Resolution

Resolve Flowbits ☒ If checked, Snort will auto-enable rules required for checked flowbits. Snort will examine the enabled rules in your chosen rule categories for automatically enabled and added to the list of files in the interface rules

Snort Subscriber IPS Policy Selection

Use IPS Policy ☒ If checked, Snort will use rules from one of three pre-defined IPS policies

Selecting this option disables manual selection of Snort Subscriber selected if enabled on the Global Settings tab. These will be added to

IPS Policy Selection Connectivity ▼

On peut observer les dangers repérés par Snort dans Service → Snort → Alert

Services / Snort / Alerts ?

[Snort Interfaces](#)
[Global Settings](#)
[Updates](#)
[Alerts](#)
[Blocked](#)
[Pass Lists](#)
[Suppress](#)
[IP Lists](#)
[SID Mgmt](#)
[Log Mgmt](#)
[Sync](#)

Alert Log View Settings

Interface to Inspect WAN (em0) ▼ ☐ Auto-refresh view 250 Save
Choose interface.. Alert lines to display.

Alert Log Actions Download Clear

Alert Log View Filter +

1 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2021-03-30 10:15:06		3	TCP	Unknown Traffic	64.98.145.30	80	192.168.1.26	34286	120:8	(http_inspect) INVALID CONTENT-LENGTH OR CHUNK SIZE