

PROJET INFRA
B1 INFO 2020 - 2021
GROUPE n°19
PROJET 2 : ROUTEUR



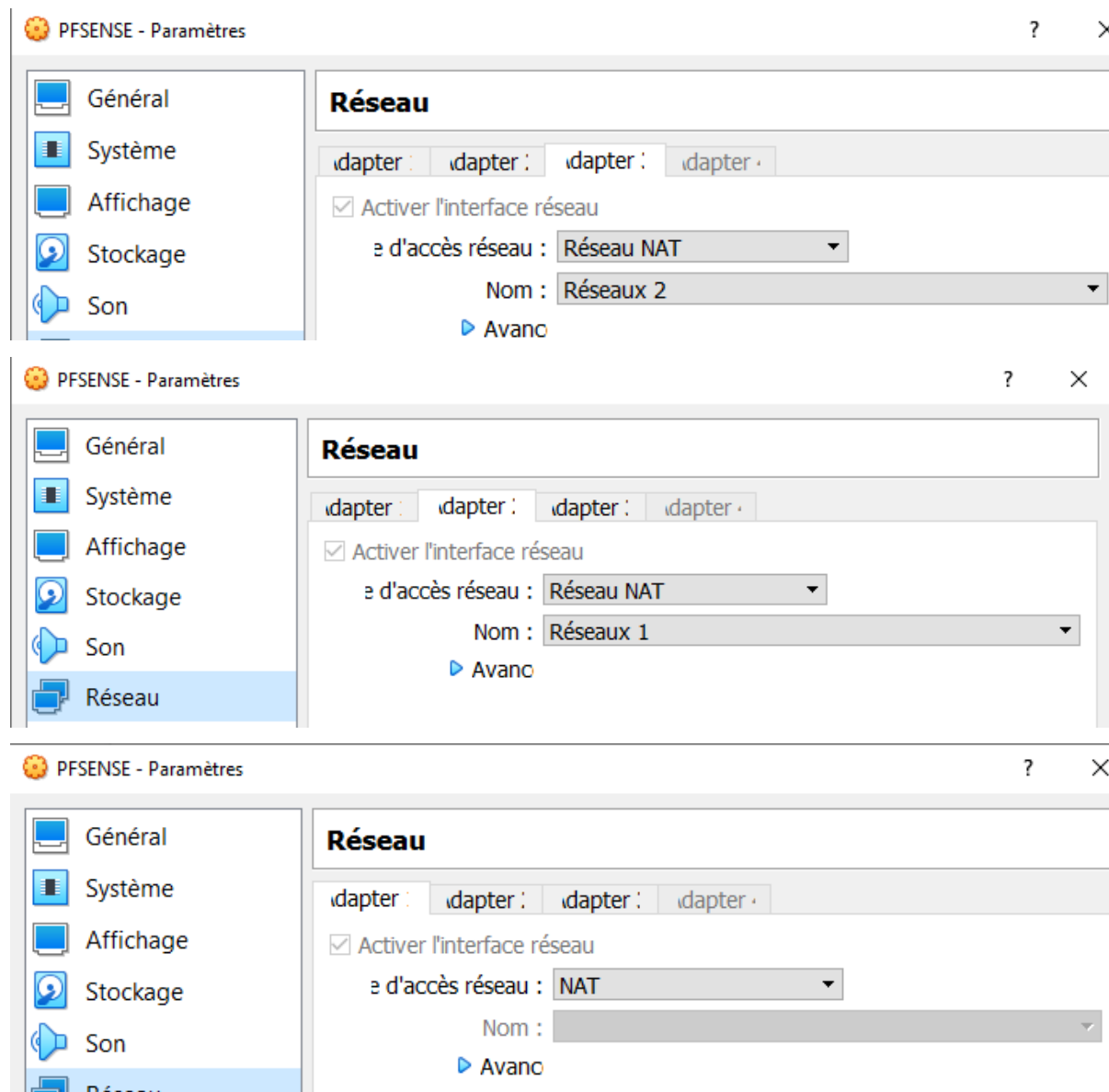
GNAOUI Brahim B1 B
BAUDRIN Corentin B1 B

Choix de l'OS permettant le routeur.

Après avoir étudié les documentations des 2 principaux OS, OPNSense et PFSense. Nous avons décidé de choisir l'OS de routeur de PFSense.

I - Configuration de PFSense

Dans un premier temps avant l'installation de la machine nous lui avons créé plusieurs réseaux. Ces réseaux étant un NAT permettant d'accéder à internet pour le routeur. Et deux réseaux NAT différents afin que les machines qui veulent se connecter à internet doivent passer par le routeur.



Dans un second temps après avoir accepté la licence de PFSense il fallait configurer la LAN afin de pouvoir accéder à l'interface graphique de cette dernière.

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - CEKEJEVE (em2 - static)

Enter the number of the interface you wish to configure: 2
```

On choisit donc la nouvelle adresse IPV4 de la machine dans notre cas nous avons choisis 192.168.1.1

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1
```

On choisit ensuite le masque : 24 dans notre cas

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

On ne veut pas de passerelle donc on n'entre rien

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Pas d'IPV6

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

On active le DHCP sur notre LAN

```
Do you want to enable the DHCP server on LAN? (y/n) y
```

On rentre ensuite notre plage d'adresse

```
Enter the start address of the IPv4 client address range: 192.168.1.2
Enter the end address of the IPv4 client address range: 192.168.1.254
```

Et voilà l'accès à l'interface graphique est défini et configuré

```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

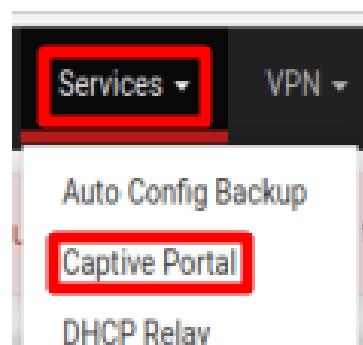
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.1.1/

Press <ENTER> to continue.
```

II - Configuration du portail captif :

1 - Mise en place du portail captif

Depuis l'interface web du routeur en tant qu'administrateur, dans les services proposés il y a la possibilité de mettre en place un portail captif.



Lorsqu'on clique sur "Captive portal" on nous donne la possibilité de configurer son portail captif avec nos propres paramètres.

Nous avons choisi de le configurer en interface LAN et d'y autoriser 6 connexions au maximum.

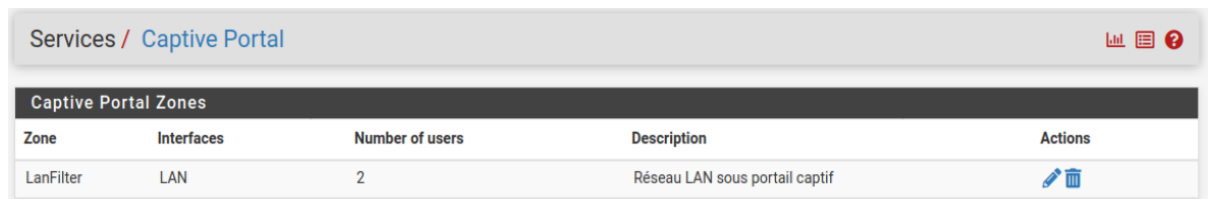
Le client sera également déconnecté au bout de 30 minutes d'inactivité et sera déconnecté au bout de 900 minutes de force quoi que le client fasse.



Configuration	MACs	Allowed IP Addresses	Allowed Hostnames	Vouchers	High Availability
Captive Portal Configuration					
Enable	<input checked="" type="checkbox"/> Enable Captive Portal				
Description	<input type="text" value="Réseau LAN sous portail captif"/> A description may be entered here for administrative reference (not parsed).				
Interfaces	<div> <input type="checkbox"/> WAN <input checked="" type="checkbox"/> LAN </div> Select the interface(s) to enable for captive portal.				
Maximum concurrent connections	<input type="text" value="6"/> Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not limit the number of connections to the portal web server, but rather how many connections a single IP can establish to the portal web server.				
Idle timeout (Minutes)	<input type="text" value="30"/> Clients will be disconnected after this amount of inactivity. They may log in again immediately.				
Hard timeout (Minutes)	<input type="text" value="900"/> Clients will be disconnected after this amount of time, regardless of activity. They may log in again after the hard timeout (not recommended unless an idle timeout is set).				

Comme méthode d'authentification nous utilisons "Use an authentication backend" afin que le client soit obligé de s'identifier pour accéder au réseau.

Authentication	
Authentication Method	<input type="text" value="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 the backend. - "None" method will force the login page to be displayed but will accept any visitor that clicks the login button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address.
Authentication Server	<input type="text" value="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.
Secondary authentication Server	<input type="text" value="Local Database"/> You can optionally select a second set of servers to authenticate users. Users will then be able to authenticate with either server. This setting is useful if you want to provide multiple authentication methods to your users. If you do not want a secondary server, leave this setting empty.
Reauthenticate Users	<input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, requests are made to the server for each user that is logged in every minute. If a user is disconnected from the captive portal immediately, reauthentication requires user credentials. While a user is logged in, the cached credentials are necessary for the portal to perform automatic reauthentication.
Local Authentication Privileges	<input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set

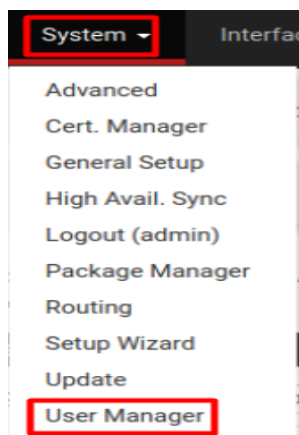
Dans l’affichage des portails captifs on doit y voir apparaître le ce dernier configuré, comme on le voit ci-dessous.



Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
LanFilter	LAN	2	Réseau LAN sous portail captif	 

2 - Configuration d’un groupe d’utilisateurs

Ensuite, toujours dans l’interface web du routeur, on est aller dans l’onglet “System” puis dans “User manager”



Il faut choisir la rubrique “Groups”. On choisit le nom de groupe de notre portail captif afin d’y intégrer tous nos utilisateurs autorisés.

Et dans le scope il faut absolument mettre en local.

Les cases dans “Group membership” est ce qui devrait apparaître lorsqu’on y créer des utilisateurs. L’admin doit toujours être dans la case “Not members”, dans le cas contraire tous les utilisateurs seront reconnus en tant qu’administrateurs.

Users **Groups** Settings Authentication Servers

Group Properties

Group name Captive-Portal

Scope Local
 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 Utilisateurs du portail captif
 Group description, for administrative information only

Group membership

Not members: admin

Members: user2, user3

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

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

Dans les options de “Assigned Privileges” parmi la liste des services proposés il faut choisir “User - Services: Captive Portal Login”, c’est cette option qui va permettre au client du groupe de se connecter au portail captif.

Assigned Privileges		
Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	
Add		

3 - Création d’un utilisateur

Pour créer un utilisateur, il faut quitter l’onglet “Groups” et aller dans “Users”. Nous y avons toutes les options comme la création d’un nom d'utilisateur et un mot de passe.

Dans “Group membership” il faut que le groupe crée précédemment soit dans le case “member of” ce qui va permettre d'intégrer l'utilisateur au groupe.

Users Groups Settings Authentication Servers

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username

Password

Full name
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

Not member of

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

Normalement si toutes les étapes ont été respectées, nous devons voir apparaître dans “Users” la liste des utilisateurs créés en plus de l’admin.

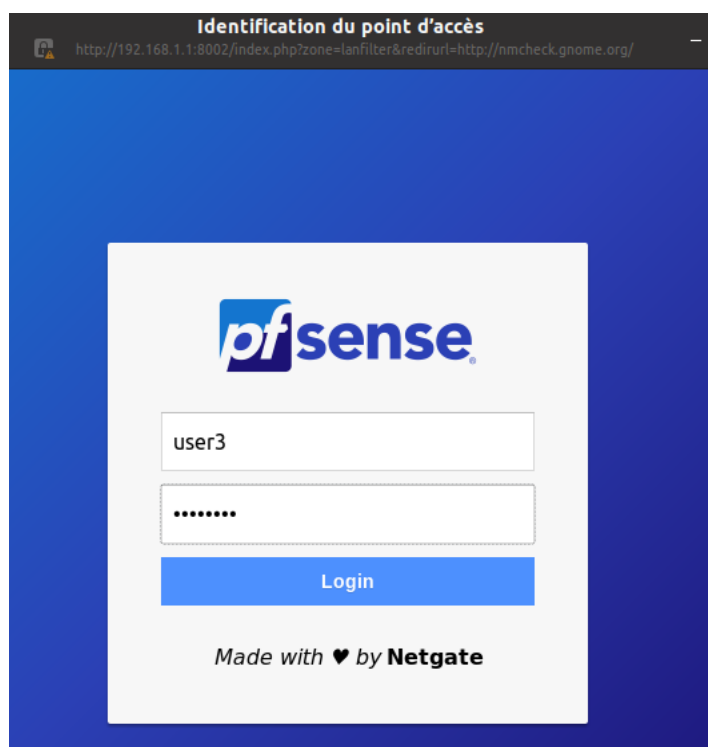
System / User Manager / Users

Users Groups Settings Authentication Servers









	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	user2	user2	✓	Captive-Portal	
<input type="checkbox"/>	user3	user3	✓	Captive-Portal	

4 - Connexion au réseau avec une VM

Lorsque l’on ouvre une VM qui est dans le même LAN notre notre routeur Pfsense, lorsque l’on essaie d’accéder à n’importe quelle page web, il doit y apparaître une page d’identification, il faut donc y rentrer les identifiants d’un utilisateur que nous avons créé dans notre groupe dédié au portail captif.



Si l'identifiant que l'on a entré est correct, on peut donc accéder au réseau, et on peut également voir dans l'interface web de l'admin que des utilisateurs sont connectés au réseau via le portail captif.

Status / Captive Portal / LanFilter				   
Users Logged In (2)				
IP address	MAC address	Username	Session start	Actions
192.168.1.101	08:00:27:4e:b4:06	user2	04/01/2021 20:23:26	
192.168.1.104	08:00:27:be:26:ba	user3	04/01/2021 20:37:33	
				 Show Last Activity  Disconnect All Users