

# Documentation PFSense

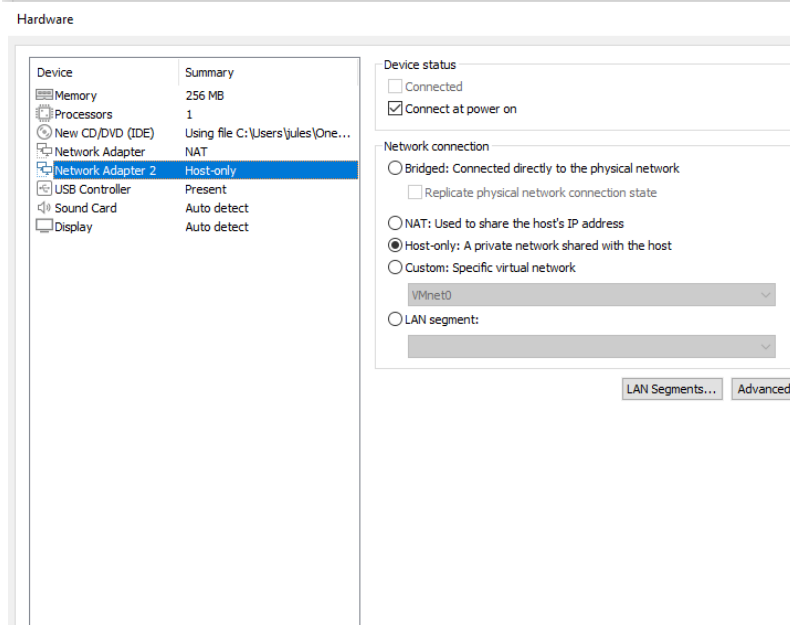
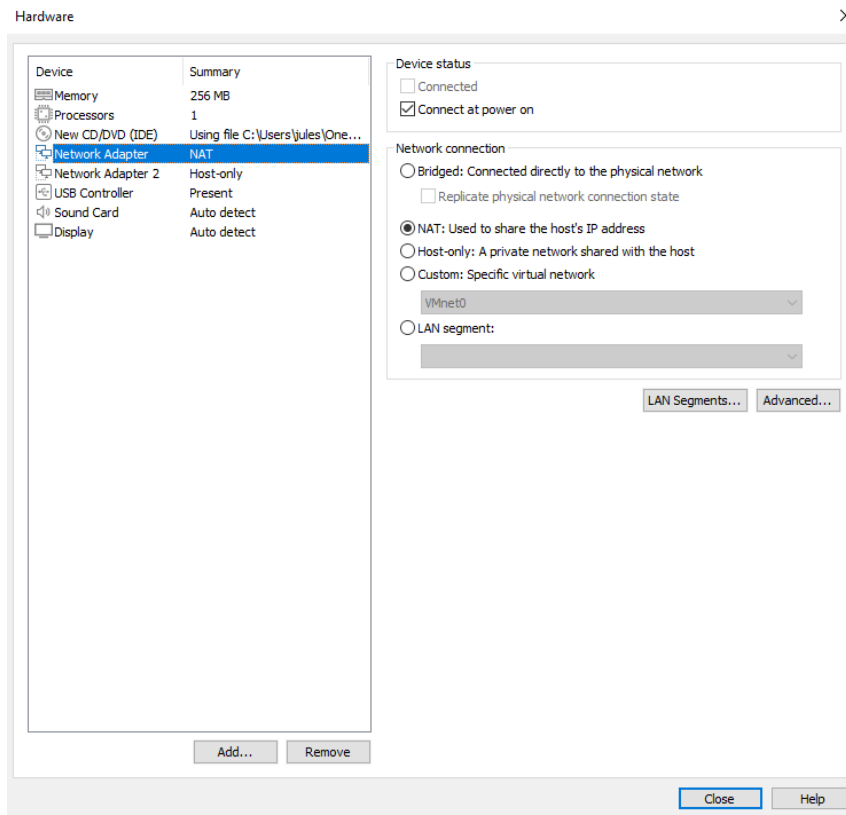


## Table des matières

I.	Installation pfSense :	3
II.	Deny all:	10
III.	Règle internet :	12
IV.	Captive portail :	14

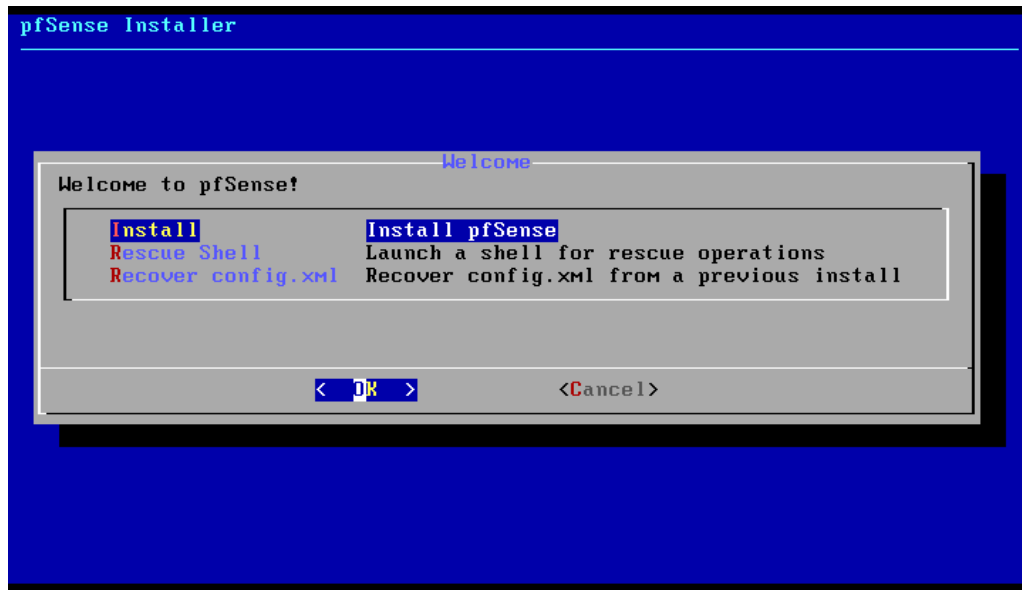
## I. Installation pfSense :

Configuration des cartes réseau de la VM PFsense :

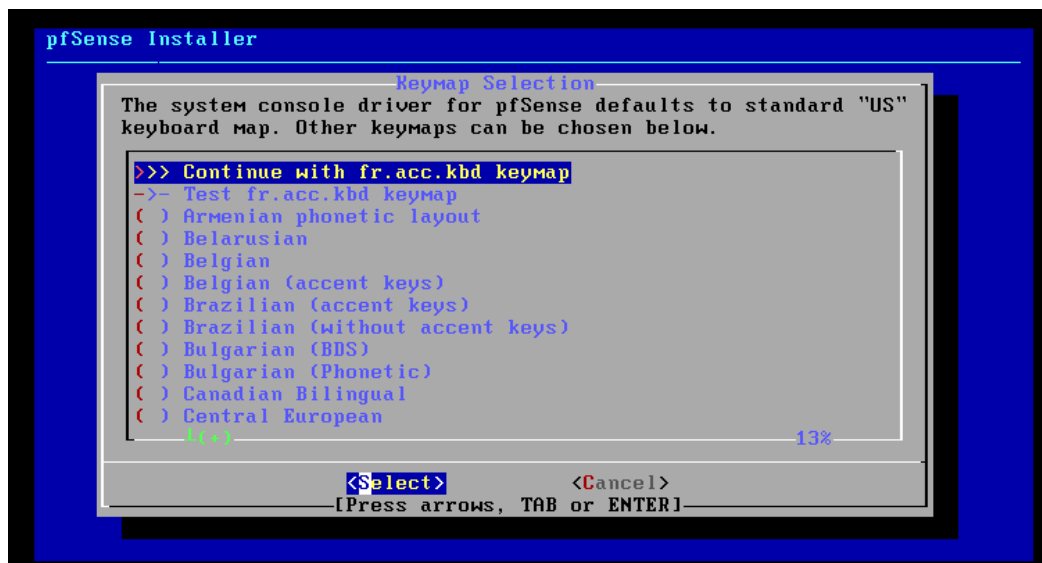


Liste des étapes durant l'installation de pfsense :

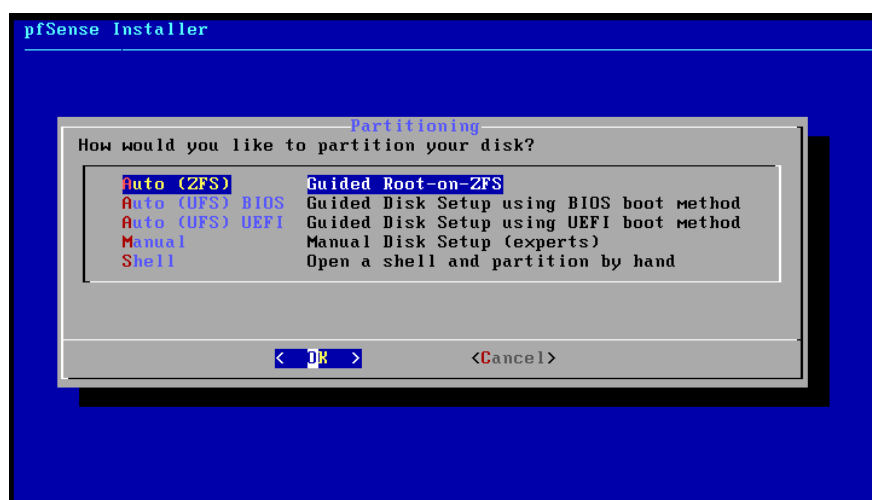
sélectionner install pfSense pour procéder à l'installation



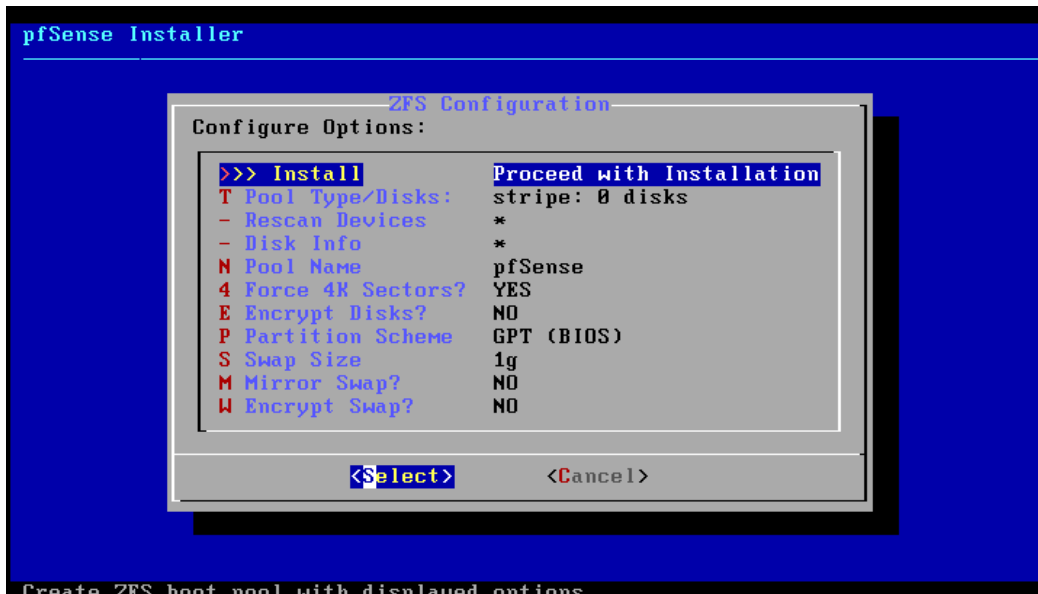
sélectionner votre langue pour le clavier : ici français



sélectionné auto (ZFS) pour l'installation standard

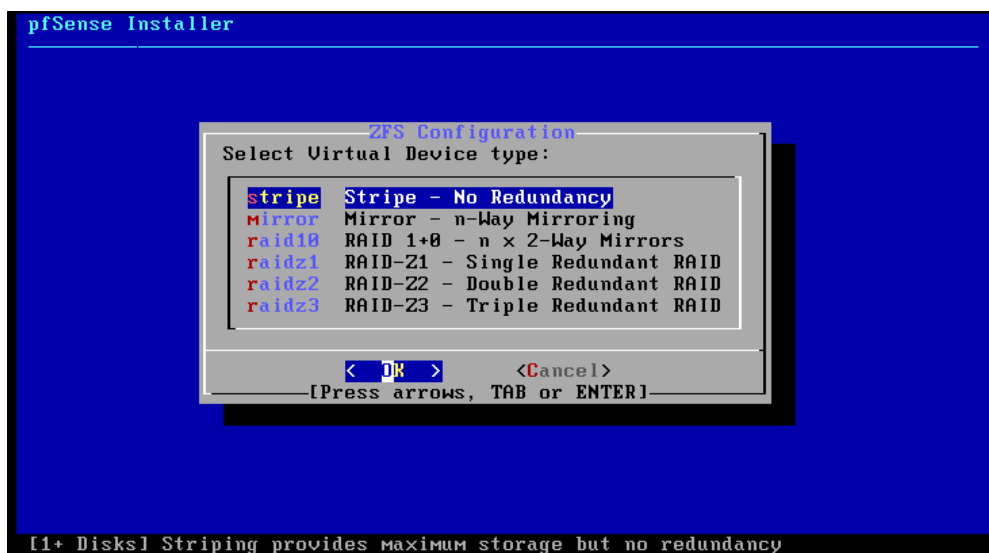


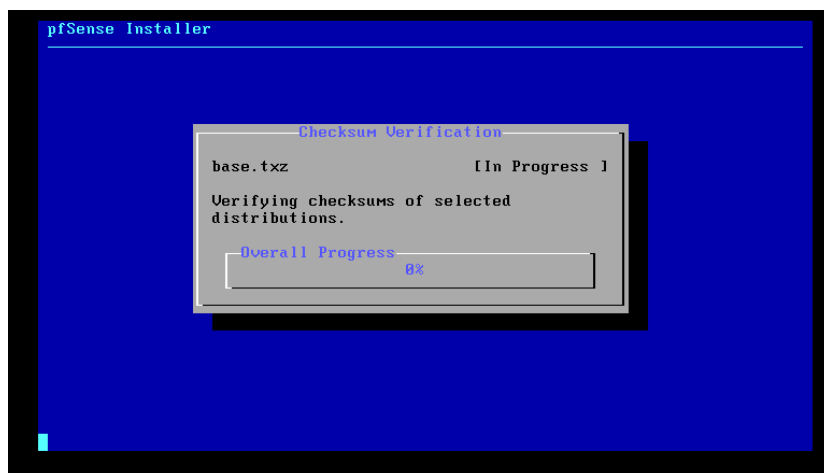
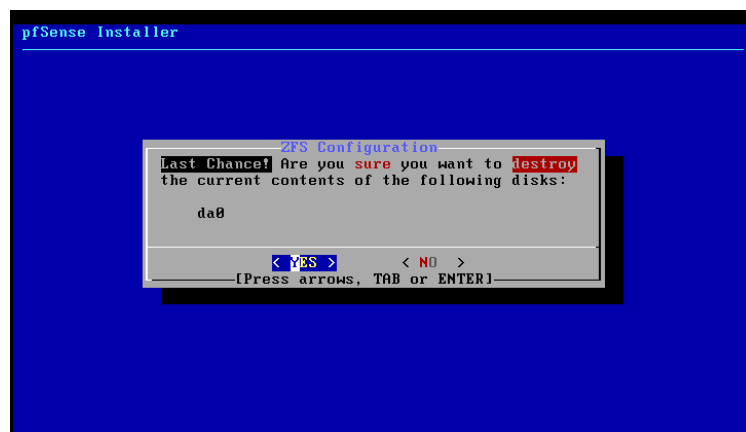
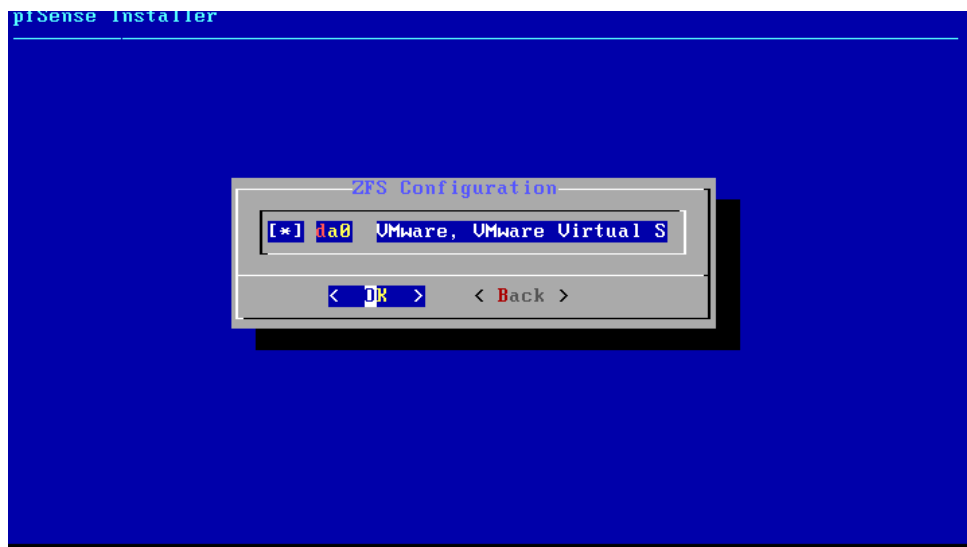
Pour continuer valider install : proceed with installation car notre configuration est bonne



Ensuite choisir le type de stockage pour l'installation que vous souhaitez

Puis valider et attendez que l'installation ce termine.





Une fois installé il faut faire un reboot de la machine. Une fois celui-ci effectue vous arriverez sur l'affichage ci-dessous.

```
VMware Virtual Machine - Netgate Device ID: 74b69c927fac3ed023fb
```

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.245.143/24
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
```

Entrer 2 pour accéder au adresse IP :

Nous pouvons bien voir que notre première carte réseau est configuré en DHCP et que la deuxième est en ip static, donc la première en 192.168.245.143 et la suivante qui est en IP fixe est : 192.168.1.1.

```
VMware Virtual Machine - Netgate Device ID: 74b69c927fac3ed023fb
```

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.245.143/24
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
```

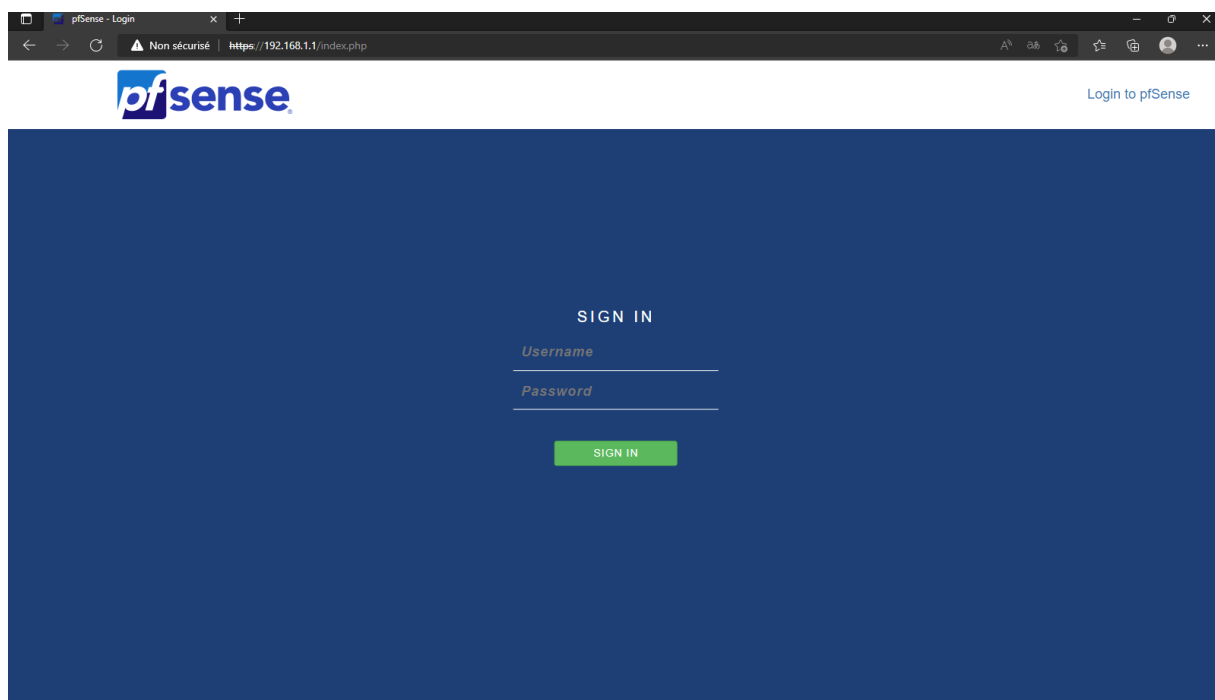
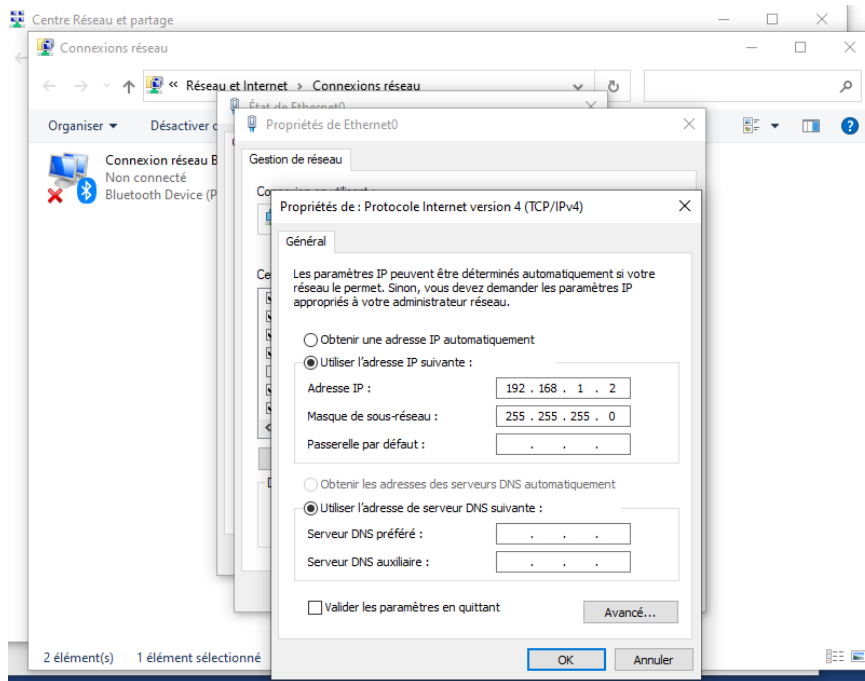
```
Enter an option: 2
```

```
Available interfaces:
```

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

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

Ensuite pour accéder au firewall, nous prenons une vm sous windows 10 que l'on va configurer sur le même réseau que notre vm pfSense :



Une fois les vm configuré sur le même réseau, taper l'IP du firewall dans le navigateur, ici 192.168.1.1  
username : admin

password par défaut : pfsense

il faudra simplement changer au moins le mot de passe pour pouvoir commencer à configurer.



Nous pouvons ici activé ou désactivé le DHCP, configuré notre range d'IP, nos masques, nos DNS etc..

D'ailleurs ici nous allons configuré les DNS de la manière suivante :

---

**DNS servers**

8.8.8.8

---

4.4.4.4

---

Une fois notre serveur DHCP configuré avec l'adresse de la passerelle entré donc ici notre vm pfSense (192.168.1.1) nous pouvons repassé la vm windows 10 en DHCP, et celle-ci devais avoir accès a Mais il ne faut pas oublier de décocher ce paramètre de vmware :

The screenshot shows the 'Virtual Network Editor' window. At the top, there is a table listing virtual networks:

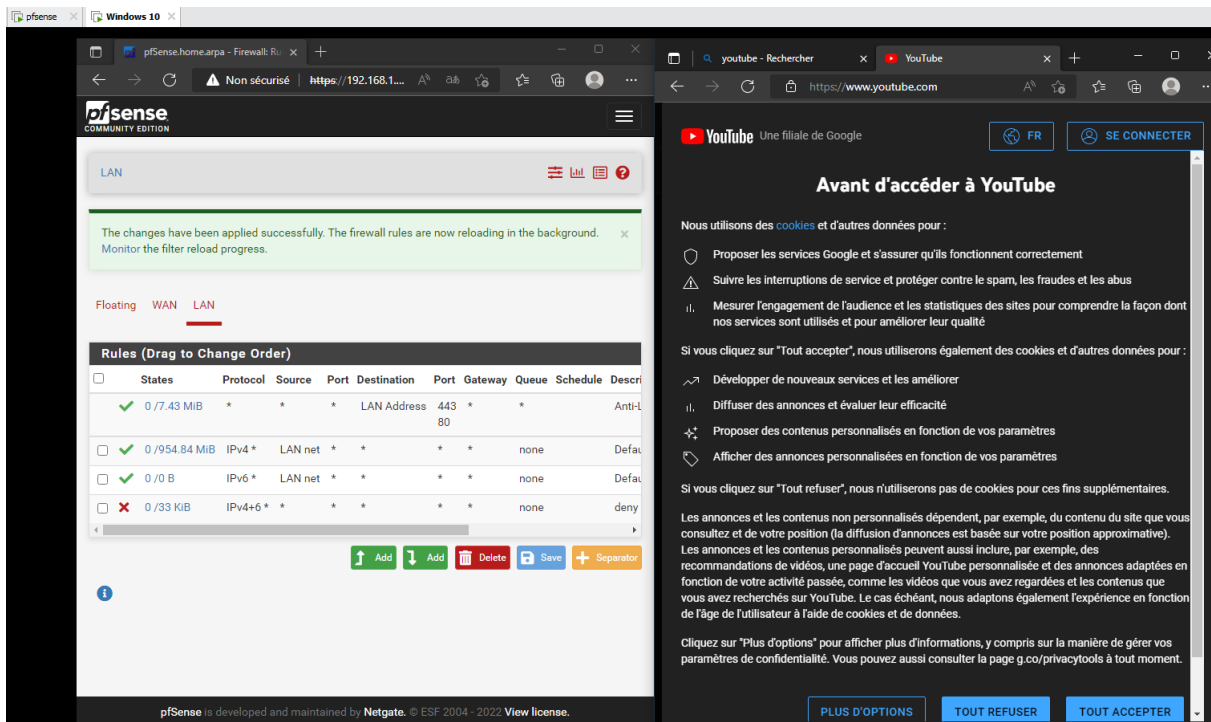
Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	-	192.168.95.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.245.0

Below the table are buttons: 'Add Network...', 'Remove Network', and 'Rename Network...'. The 'VMnet Information' section for VMnet1 is expanded, showing the following options:

- ☐ Bridged (connect VMs directly to the external network)  
Bridged to: [dropdown menu] [Automatic Settings...]
- ☐ NAT (shared host's IP address with VMs) [NAT Settings...]
- ☒ Host-only (connect VMs internally in a private network)
- ☒ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet1
- ☐ Use local DHCP service to distribute IP address to VMs [DHCP Settings...]

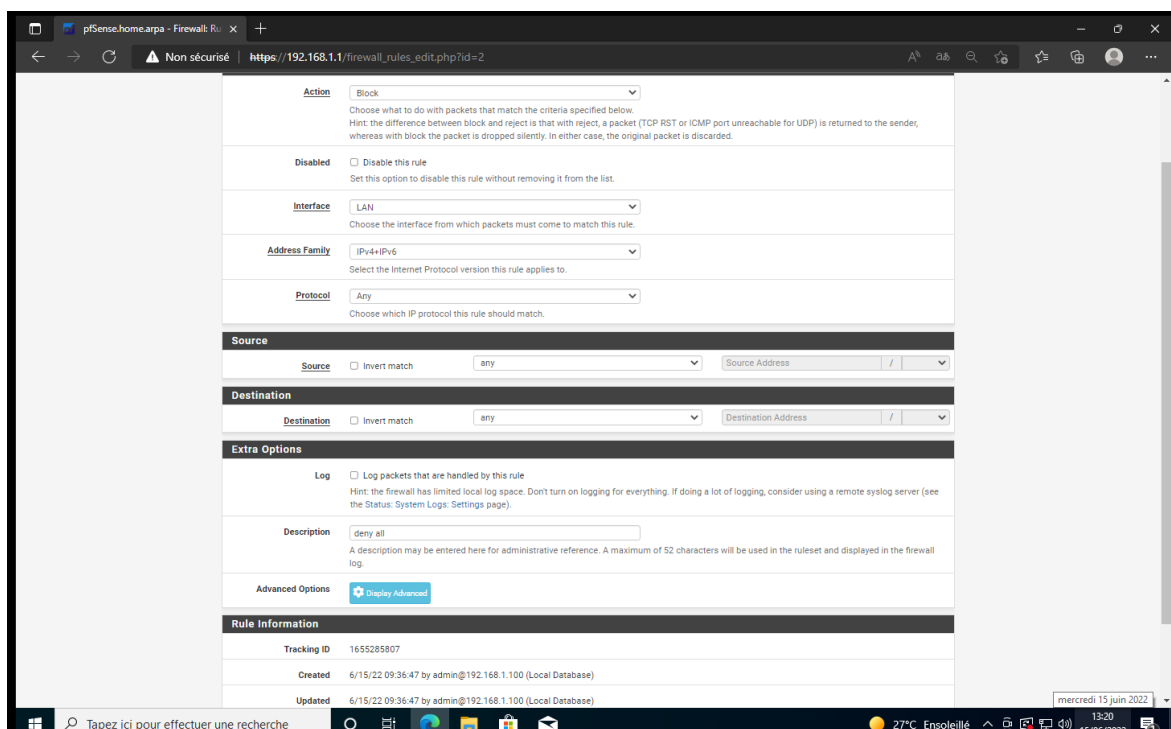
At the bottom, the 'Subnet IP' is set to 192.168.95.0 and the 'Subnet mask' is set to 255.255.255.0. A warning message at the bottom states: 'Administrator privileges are required to modify the network configuration.' with a 'Change Settings' button. At the very bottom are buttons: 'Restore Defaults', 'Import...', 'Export...', 'OK', 'Cancel', 'Apply', and 'Help'.

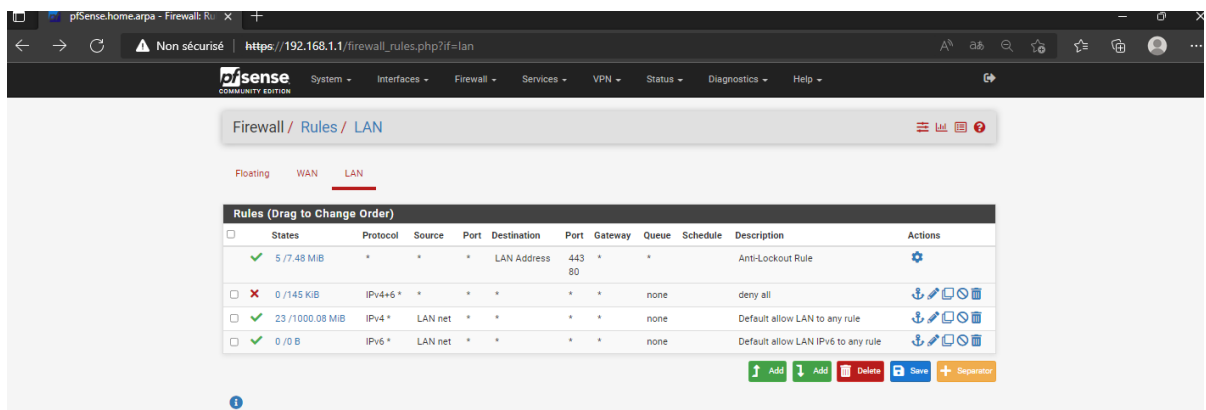
Nous avons maintenant accès à internet et à notre firewall comme le montre l'image ci-dessous :



## II. Deny all:

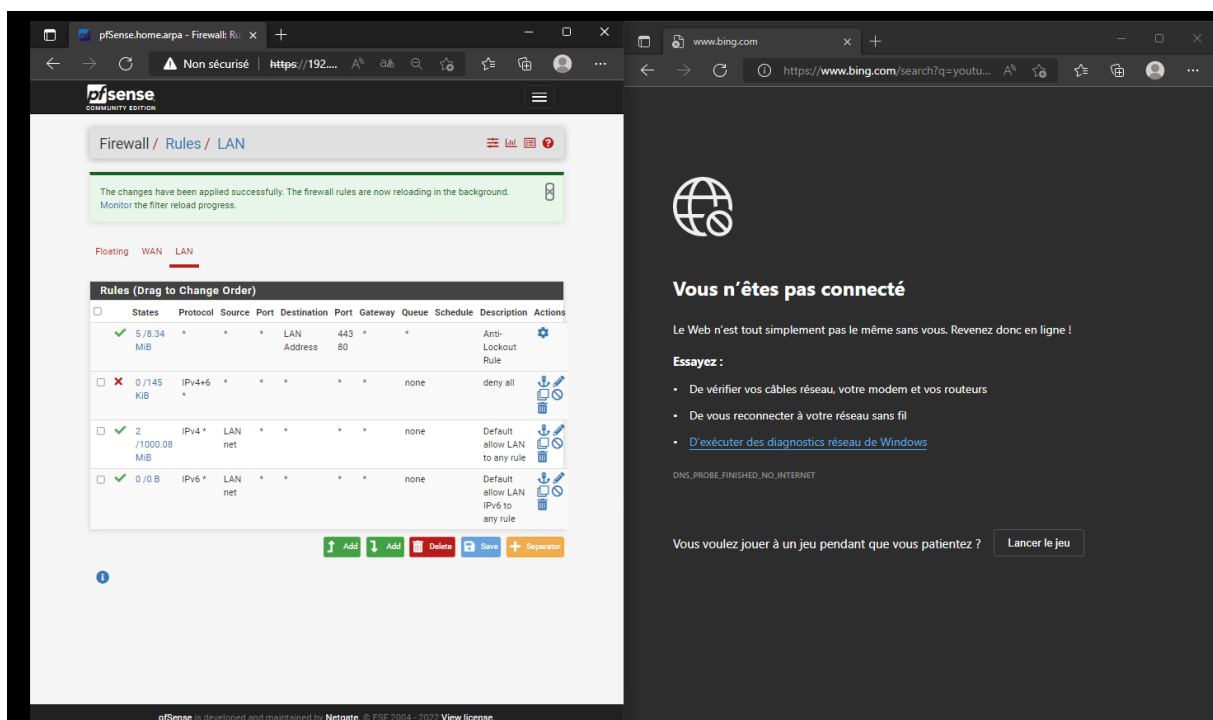
Pour cette règle-là, nous allons configurer les paramètres de manière à ce que rien ne passe, aucune connexion. Ce qui devrait par la même occasion couper l'accès à internet de la vm windows vu précédemment :





Nous pouvons donc voir maintenant si nous mettons notre nouvelle règles de blocage en vigueur et en avant par rapport au autres que cela bloque correctement.

Comme montrer ci-dessous, après application des modifications des règles nous n'avons en effet plus accès à internet.



### III. Règle internet :

Pour compléter la règle précédente qui bloque tout les connexions, nous allons autoriser l'accès à internet uniquement avec une autre règles.

Pour commencer il faut crée un Aliases qui va comprendre les ports que l'on autorise :

The screenshot shows the MikroTik WinBox interface for configuring Firewall Aliases. The breadcrumb navigation is "Firewall / Aliases / Edit".

**Properties section:**

- Name:** Internet (The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".)
- Description:** accès internet (A description may be entered here for administrative reference (not parsed).)
- Type:** Port(s)

**Port(s) section:**

Hint: Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	Entry added	Action
443	Wed, 15 Jun 2022 12:03:54 +0000	Delete
80	Wed, 15 Jun 2022 12:03:54 +0000	Delete
53	Wed, 15 Jun 2022 12:03:54 +0000	Delete

Buttons at the bottom: Save, Export to file, Add Port.

---

The second screenshot shows the "Firewall / Aliases / Ports" view. The breadcrumb navigation is "Firewall / Aliases / Ports".

Tabbed interface: IP, Ports (selected), URLs, All.

**Firewall Aliases Ports table:**

Name	Values	Description	Actions
Internet	443, 80, 53	accès internet	[Edit] [Copy] [Delete]

Buttons at the bottom right: Add, Import.

---

The third screenshot shows the MikroTik WinBox interface for configuring Firewall Rules. The breadcrumb navigation is "Firewall / Rules / LAN".

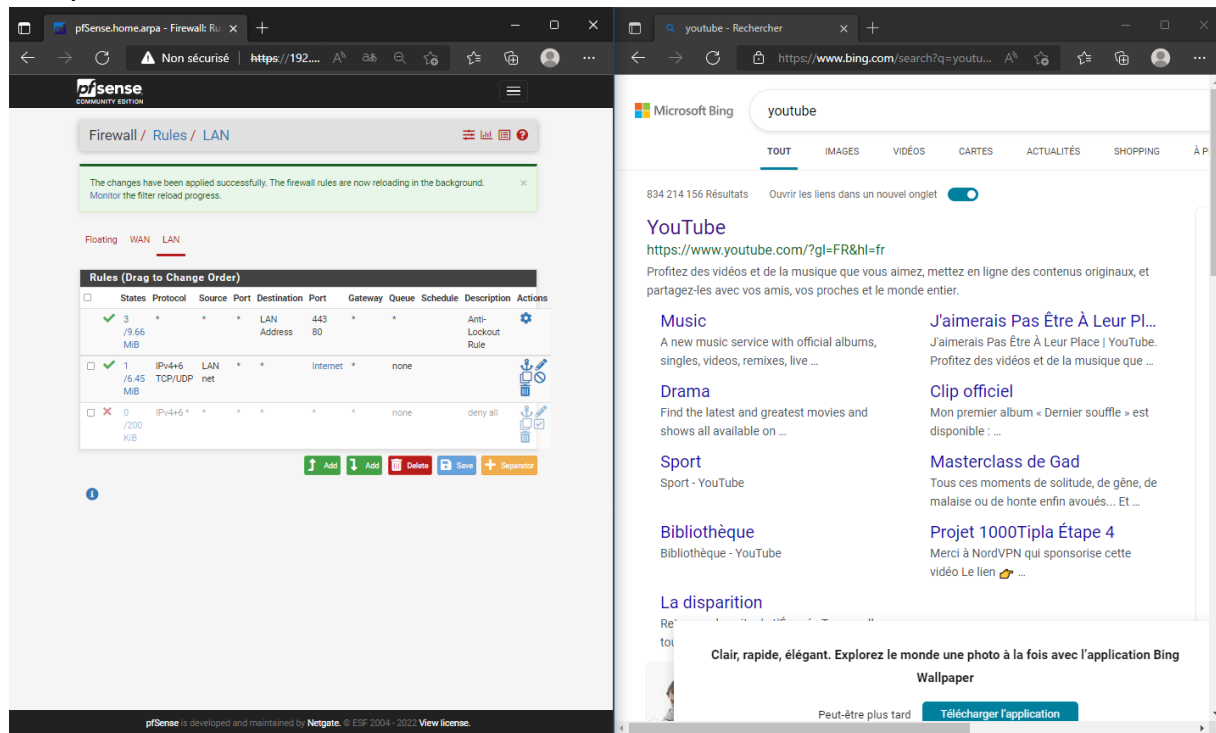
Tabbed interface: Floating, WAN, LAN (selected).

**Rules (Drag to Change Order) table:**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4 / 9.42 MiB	*	*	LAN Address	443, 80	*	*		Anti-Lockout Rule	[Settings]
<input checked="" type="checkbox"/>	28 / 6.35 MiB	IPv4+6 TCP/UDP	LAN net	*	Internet	*	none			[Add] [Edit] [Copy] [Delete]
<input checked="" type="checkbox"/>	0 / 195 KiB	IPv4+6 *	*	*	*	*	none		deny all	[Add] [Edit] [Copy] [Delete]

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

Nous avons donc maintenant de nouveau accès à internet tout en ayant bloquer les connexions indésirables



## IV. Captive portail :

Dans un premier temps nous devons activer le portail captif en remplissant les paramètres sur les image ci-contre :

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>
Traffic quota (Megabytes)	<input type="text"/> <small>Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.</small>
Pass-through credits per MAC address	<input type="text"/> <small>Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.</small>
Waiting period to restore pass-through credits (Hours)	<input type="text"/> <small>Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.</small>
Reset waiting period	<input type="checkbox"/> Enable waiting period reset on attempted access <small>If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.</small>
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window <small>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.</small>
Pre-authentication	<input type="text"/>

pass-through credits (Hours)	<small>Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.</small>
Reset waiting period	<input type="checkbox"/> Enable waiting period reset on attempted access <small>If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.</small>
Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window <small>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.</small>
Pre-authentication redirect URL	<input type="text" value="http://google.fr"/> <small>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_REDIRECT_URL\$ variable in captiveportal's HTML pages.</small>
After authentication Redirection URL	<input type="text" value="http://google.fr"/> <small>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.</small>
Blocked MAC address redirect URL	<input type="text"/> <small>Blocked MAC addresses will be redirected to this URL when attempting access.</small>
Preserve users database	<input checked="" type="checkbox"/> Preserve connected users across reboot <small>If enabled, connected users won't be disconnected during a pfSense reboot.</small>
Concurrent user logins	<div>Multiple</div> <small>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.</small>
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering <small>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.</small>
Pass-through MAC Auto Entry	<input type="checkbox"/> Enable Pass-through MAC automatic additions <small>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 <a href="#">MAC tab</a> or send a POST from another system. If this is enabled, the logout window will not be shown.</small>
Per-user bandwidth restriction	<input type="checkbox"/> Enable per-user bandwidth restriction
Use custom captive portal page	<input type="checkbox"/> Enable to use a custom captive portal login page <small>If set a portal.html page must be created and uploaded. If unchecked the default template will be used</small>

Captive Portal Login Page

Also a background image for use in the captive portal login screen. It will be retained as the portal background. The background image will be on 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**

Copy and paste terms and conditions for use in the captive portal. HTML tags will be stripped out.

**Authentication**

**Authentication Method** 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 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** 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** Local Database

You can optionally select a second set of servers 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.

**Local Authentication Privileges** ☒ Allow only users/groups with "Captive portal login" privilege set

**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.

**Save**

Une fois celui-ci sauvegarder avec le bouton save, vous le retrouverez dans votre liste de captive portail

Services / Captive Portal

Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
Portail	LAN	0	portail captif	

**+ Add**

Nous allons maintenant crée notre premier groupe nommé agent

System / User Manager / Groups / Edit

**Users** **Groups** Settings Authentication Servers

**Group Properties**

**Group name** Agent

**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** Delegation création utilisateurs portail

Group description, for administrative information only

**Group membership**

admin

Not members

Members

**>> Move to "Members"** **<< Move to "Not members"**

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

**Save**

pfSense.home.arpa - System: User Manager: Groups: Edit  
- Profil 1 - Microsoft Edge

nous lui attribuons les privilèges WebCfg-System : User Manager et WebCfg- statues : captive portal comme montré en dessous

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

**Group Privileges**

Group

Agent

Assigned privileges

WebCfg - System: Gateways

WebCfg - System: Gateways: Edit Gateway

WebCfg - System: Gateways: Edit Gateway Groups

WebCfg - System: General Setup

WebCfg - System: Group Manager

WebCfg - System: Group Manager: Add Privileges

WebCfg - System: High Availability Sync

WebCfg - System: Login / Logout / Dashboard

WebCfg - System: Package Manager

WebCfg - System: Package Manager: Install Package

WebCfg - System: Package Manager: Installed

WebCfg - System: Static Routes

WebCfg - System: Static Routes: Edit route

WebCfg - System: Update: Settings

**WebCfg - System: User Manager**

WebCfg - System: User Manager: Add Privileges

WebCfg - System: User Manager: Settings

WebCfg - System: User Password Manager

WebCfg - System: User Settings

WebCfg - VPN: IPsec

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

Filter

Show only the choices containing this term

**Privilege information**

The following privileges effectively give administrator-level access to users in the group because the user gains access to execute general commands, edit system files, modify users, change passwords or similar:

User - System: Copy files (scp)

User - System: Shell account access

System - HA node sync

WebCfg - All pages

WebCfg - Diagnostics: Backup & Restore

System / [User Manager](#) / [Groups](#) / [Edit](#) / [Add Privileges](#)

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

**Group Privileges**

Group

Agent

Assigned privileges

WebCfg - Services: RFC 2136 Client: Edit

WebCfg - Services: RFC 2136 Clients

WebCfg - Services: Router Advertisements

WebCfg - Services: SNMP

WebCfg - Services: UPnP

WebCfg - Services: Wake-on-LAN

WebCfg - Services: Wake-on-LAN: Edit

**WebCfg - Status: Captive Portal**

WebCfg - Status: Captive Portal Voucher Rolls

WebCfg - Status: Captive Portal Vouchers

WebCfg - Status: Captive Portal: Expire Vouchers

WebCfg - Status: Captive Portal: Test Vouchers

WebCfg - Status: CARP

WebCfg - Status: CPU load

WebCfg - Status: DHCP leases

WebCfg - Status: DHCPv6 leases

WebCfg - Status: DNS Resolver

WebCfg - Status: Filter Reload Status

WebCfg - Status: Gateway Groups

WebCfg - Status: Gateways

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

Filter

Show only the choices containing this term

**Privilege information**

The following privileges effectively give administrator-level access to users in the group because the user gains access to execute general commands, edit system files, modify users, change passwords or similar:



les rôles ont bien été ajoutés à notre groupe

The screenshot shows the pfSense web interface for managing groups. The browser address bar indicates the URL is `https://192.168.1.1/system_groupmanager.php?act=edi...`. The navigation menu at the top includes 'Users', 'Groups' (which is selected), 'Settings', and 'Authentication Servers'.

The main content area is titled 'Group Properties' and contains the following fields:

- Group name:** A text input field containing the value 'Agent'.
- Scope:** A dropdown menu set to 'Local'. Below it, a warning message states: '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:** A text input field containing 'Délégation création utilisateurs portail'. Below it, a note says: 'Group description, for administrative information only'.
- Group membership:** Two list boxes. The 'Not members' box contains 'admin'. The 'Members' box is empty.
- Below the membership boxes are two buttons: 'Move to Members' and 'Move to Not members'.
- A note below the buttons says: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.'

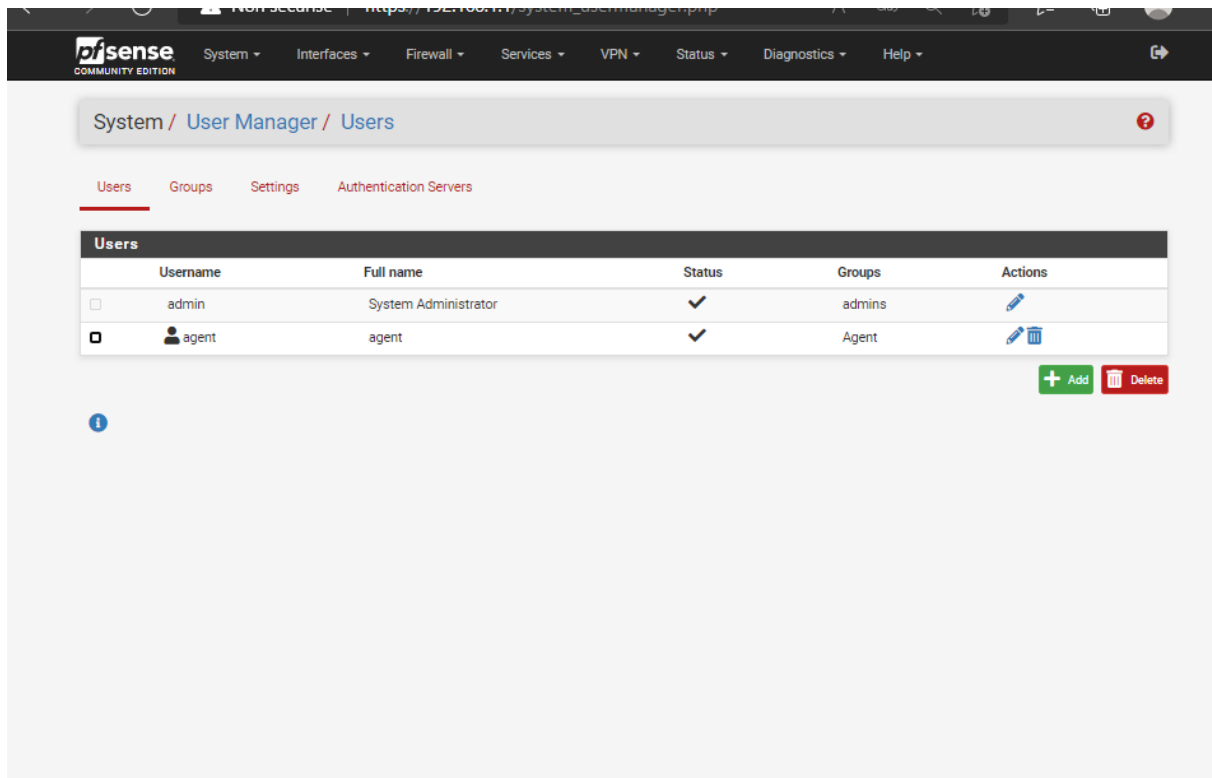
The second section is titled 'Assigned Privileges' and contains a table with the following data:

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.	

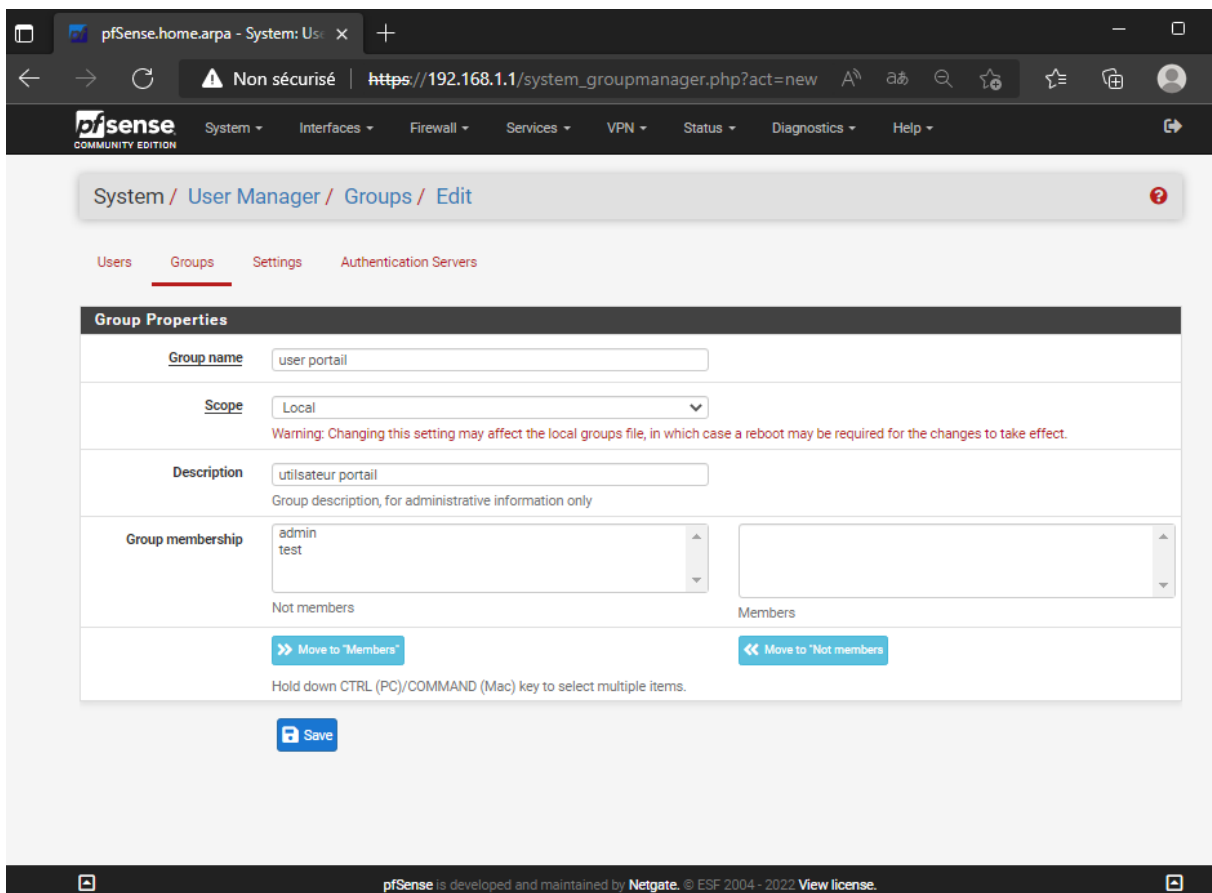
Below the table, there is a security notice: 'Security notice: Users in this group effectively have administrator-level access'. At the bottom right of this section is a green '+ Add' button.

At the very bottom of the interface is a blue 'Save' button.

nous créons maintenant un rôle agent et nous l'attribuons au groupe du même nom



Passons au utilisateur standard, nous créons le groupe userportail



pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

System / User Manager / Groups

?













Users

Groups

Settings

Authentication Servers

Groups

Group name	Description	Member Count	Actions
Agent	Delegation création utilisateurs portail	1	  
admins	System Administrators	1	  
all	All Users	2	  
userportail	utilisateur portail	0	  

+

Add

passons au privilège du groupe userportail, nous lui attribuons celle-ci contre :

System / User Manager / Groups / Edit / Add Privileges

?

Users

Groups

Settings

Authentication Servers

Group Privileges

Group	userportail
<div><div>Assigned privileges</div><div><div>System - HA node sync</div><div>User - Config: Deny Config Write</div><div>User - Notices: View</div><div>User - Notices: View and Clear</div><div>User - Services: Captive Portal login</div><div>User - System: Copy files (scp)</div><div>User - System: Copy files to home directory (chrooted scp)</div><div>User - System: Shell account access</div><div>User - System: SSH tunneling</div><div>User - VPN: IPsec xauth Dialin</div><div>User - VPN: L2TP Dialin</div><div>User - VPN: PPPoE Dialin</div><div>WebCfg - AJAX: Get Queue Stats</div><div>WebCfg - AJAX: Get Service Providers</div><div>WebCfg - AJAX: Get Stats</div><div>WebCfg - All pages</div><div>WebCfg - Crash reporter</div><div>WebCfg - Dashboard (all)</div><div>WebCfg - Dashboard widgets (direct access).</div><div>WebCfg - Diagnostics: ARP Table</div></div></div>	<div><div>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</div><div><div>Filter</div><div></div><div>Show only the choices containing this term</div></div><div><div>Privilege information</div><div>The following privileges effectively give administrator-level access to users in the group because the user gains access to execute general commands, edit system files, modify users, change passwords or similar:</div></div></div>

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: admin, test

Members:

[Move to 'Members'](#) [Move to 'Not members'](#)

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

### Assigned Privileges

Name	Description	Action
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.	<a href="#">Delete</a>

[+ Add](#)

[Save](#)

pour faire le test nous allons justement crée un utilisateur test qui va nous servir d'utilisateur lambda

← → ↻ ⚠ Non sécurisé | [https://192.168.1.1/system\\_usermanager.php?act=new](https://192.168.1.1/system_usermanager.php?act=new) 🔍 ⚙️ ⭐️ ⚙️ ⚙️ ⚙️ ⚙️

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: Agent, admins

Member of: userportal

**System / User Manager / Users** ?

Users **Groups** Settings Authentication Servers

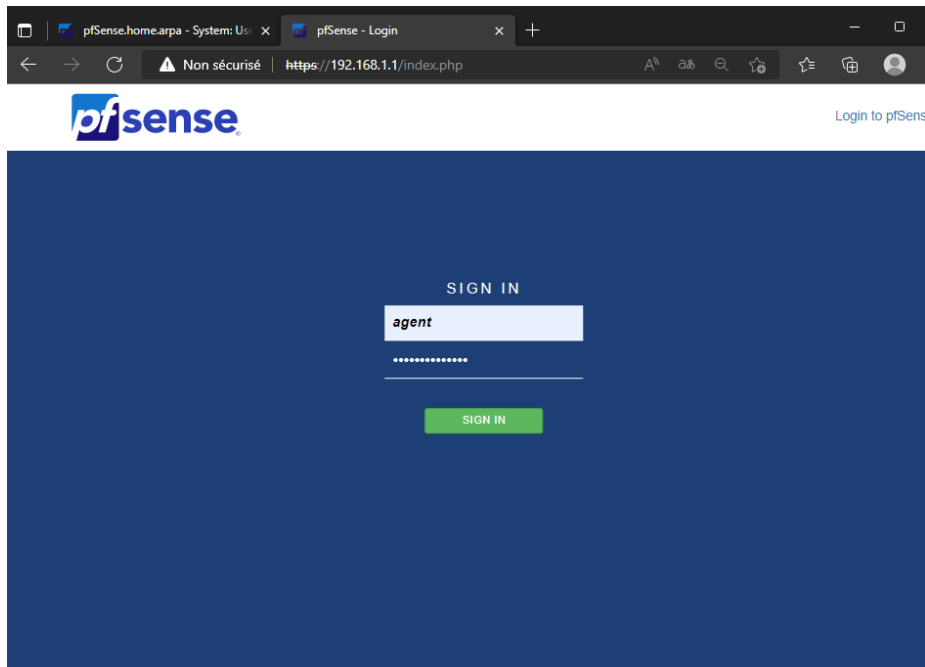
### Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	<a href="#">Edit</a>
<input checked="" type="checkbox"/>	agent	agent	✓	Agent	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	test	user portail	✓	userportal	<a href="#">Edit</a> <a href="#">Delete</a>

[+ Add](#) [Delete](#)

[i](#)

(si besoin nous pouvons maintenant nous connecter avec le compte agent pour faire la gestion des utilisateur inférieur comme l'utilisateur test



Nous allons encore créer un deuxième utilisateur (pour finir la doc)

**Users**

---

**User Properties**

Defined by	USER	
Disabled	<input type="checkbox"/> This user cannot login	
Username	bubu	
Password	****	****
Full name	second utilisateur <small>User's full name, for administrative information only</small>	
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>	
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.	
Group membership	Agent admins	userportail
	Not member of	Member of
	<a href="#">Move to "Member of" list</a>	<a href="#">Move to "Not member of" list</a>
	<small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>	
Certificate	No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.	

**Keys**

Authorized SSH Keys	<input type="text"/>
---------------------	----------------------

System / [User Manager](#) / [Users](#)

Users

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	agent	agent	✓	Agent	
<input type="checkbox"/>	bubu	second utilisateur	✓	userportail	
<input type="checkbox"/>	test	user portail	✓	userportail	

Add Delete

