

# TP Pfsense

Koehler Erwann

15/06/2022

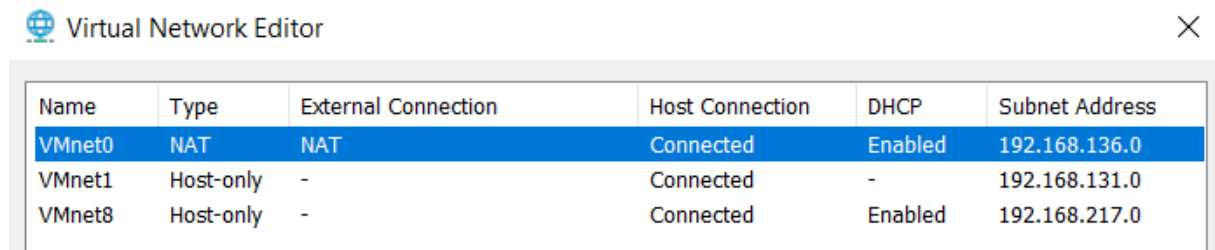
## Table des matières

|   |    |
|---|----|
| Installation de Pfsense .....             | 2  |
| Configuration de Pfsense .....            | 6  |
| Configuration des interfaces réseaux..... | 6  |
| Configuration de base .....               | 8  |
| Configuration du DHCP.....                | 10 |
| Paramétrage du Firewall .....             | 11 |
| Bloquer tous les trafics.....             | 11 |
| Filtrage internet.....                    | 12 |
| Création de l'alias .....                 | 12 |
| Création de la règle .....                | 13 |
| Paramétrage du portail captif .....       | 14 |
| Création de l'utilisateur.....            | 15 |
| Création du groupe .....                  | 15 |
| Tests .....                               | 17 |
| Test des règles du Firewall .....         | 17 |
| Test du portail captif .....              | 19 |

## Installation de Pfsense

Télécharger l'ISO depuis le site officiel : <https://www.pfsense.org/download/>

Voici les paramètres réseaux de VmWare :



| Name   | Type      | External Connection | Host Connection | DHCP    | Subnet Address |
|--------|-----------|---------------------|-----------------|---------|----------------|
| VMnet0 | NAT       | NAT                 | Connected       | Enabled | 192.168.136.0  |
| VMnet1 | Host-only | -                   | Connected       | -       | 192.168.131.0  |
| VMnet8 | Host-only | -                   | Connected       | Enabled | 192.168.217.0  |

Il faut créer une machine virtuelle avec l'ISO que l'on vient de télécharger.

Sélectionner FreeBSD (x64) pour le type de système d'exploitation.

Attribuer au minimum 512 mo de RAM, 1 processeur et 10 Go de stockage.

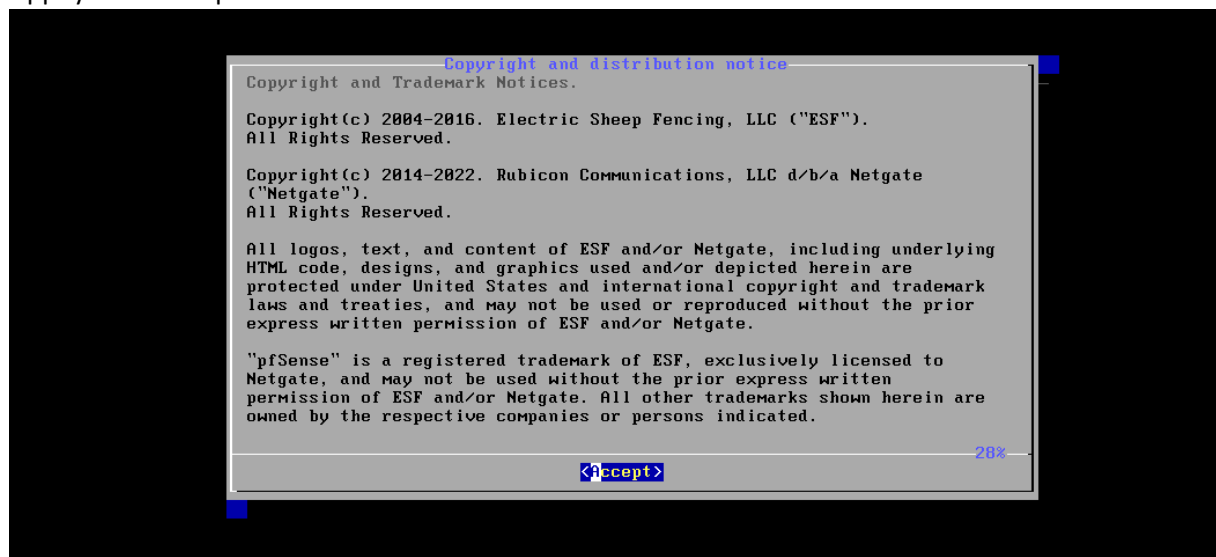
Nous allons configurer 2 cartes réseaux sur la machine virtuelle.

La 1ere carte sera sur le VMnet0 (donc en NAT) pour permettre l'accès à internet (interface WAN)

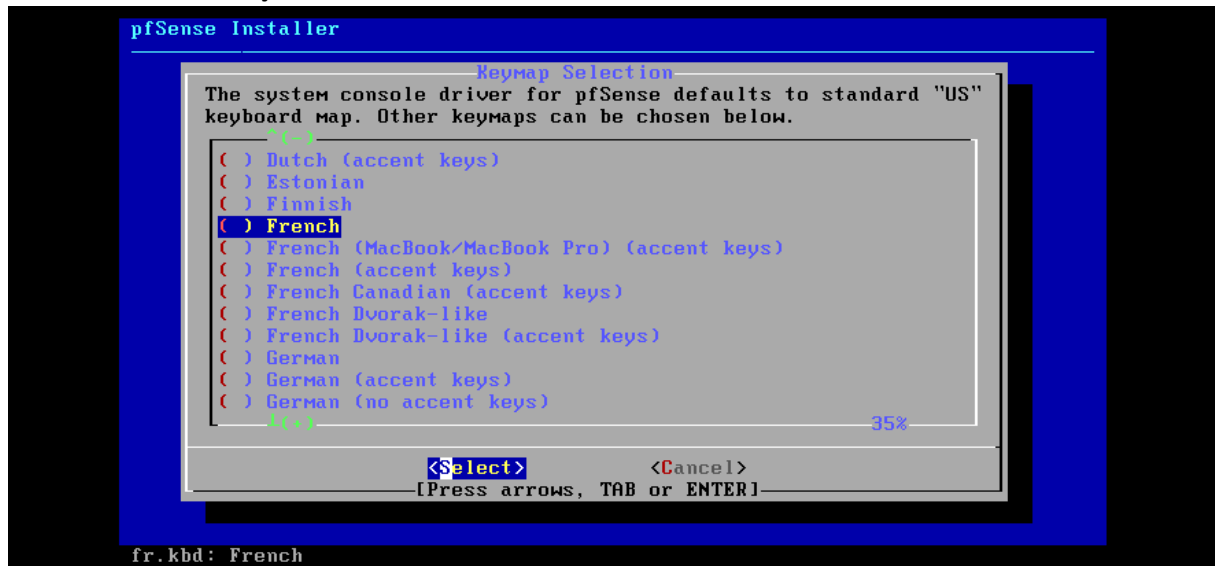
La 2e carte sera sur le VMnet1 (donc en réseau privé) pour communiquer avec le réseau local (interface LAN).

Démarrer la machine virtuelle.

Appuyer sur accept :



Choisir le clavier français :



Laisser la partition du disque par défaut :



Laisser les options par défaut :



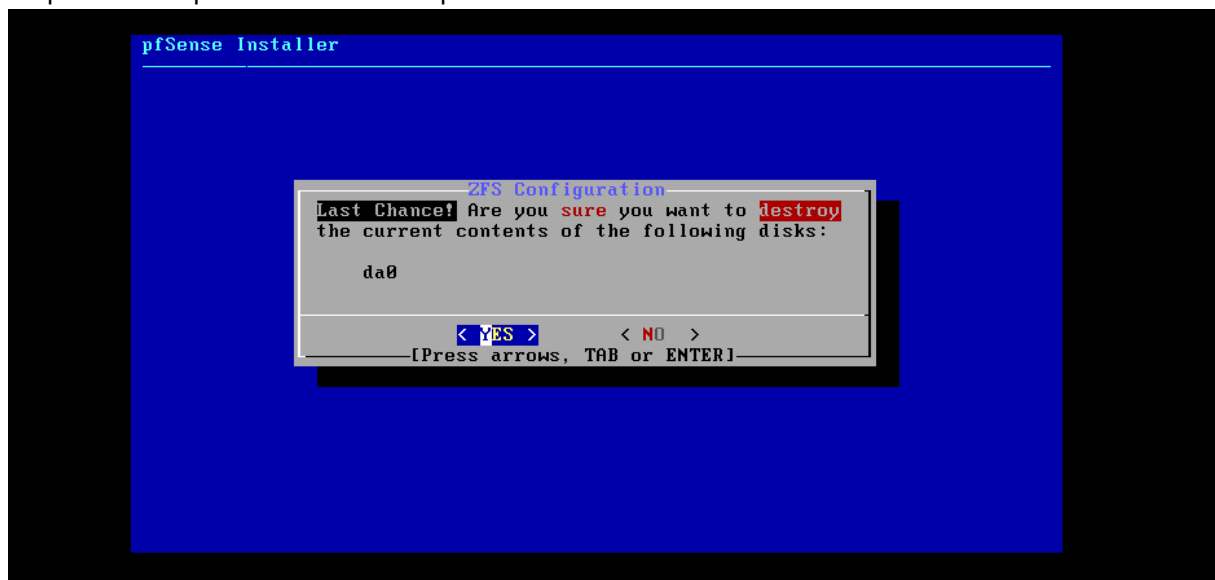
Ne pas mettre de raid en place :



Sélectionner le bon disque dur :



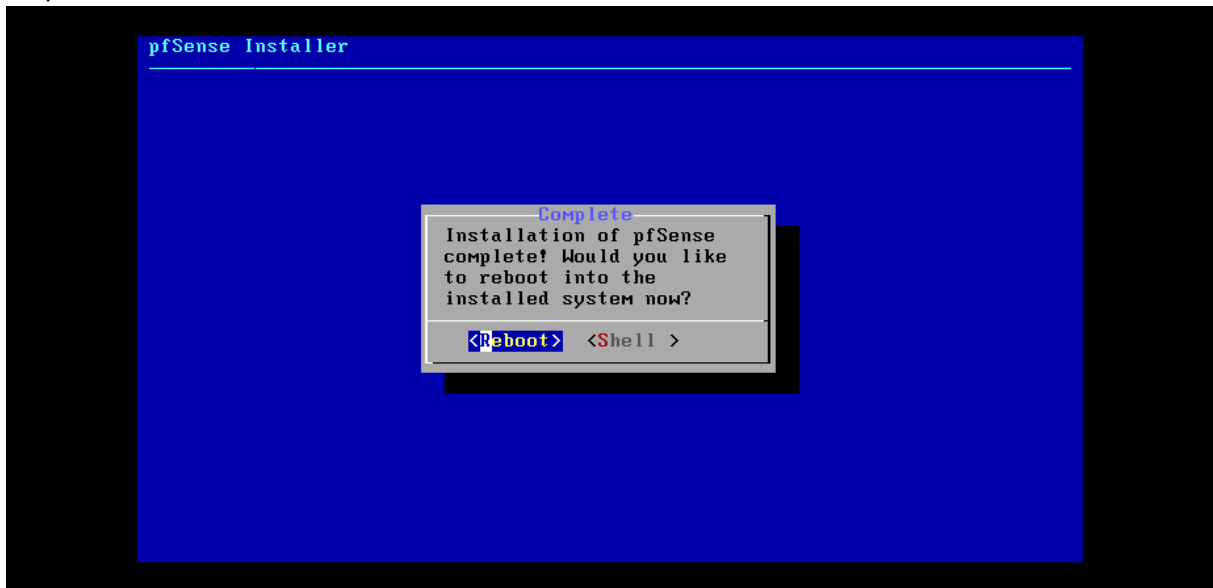
Cliquer sur YES pour formater le disque dur :



Cliquer sur No, car nous n'allons pas faire de modifications finales :



Cliquer sur Reboot :



## Configuration de Pfsense

### Configuration des interfaces réseaux

Nous allons maintenant configurer les cartes réseaux. Pour cela dans le shell :

- Taper '2' (pour entrer dans l'option 2)
- Taper '2' (pour entrer dans l'interface LAN)
- Taper '192.168.10.254' (l'adresse ip de cette interface réseau)
- Taper '24' (la taille du masque de sous réseau en CIDR)

```

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: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.254

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 32):
> 24

```

- On ne donne pas de passerelle par défaut.
- On ne donne pas d'adresse ipv6.
- On n'active pas le serveur dhcp.
- On dit oui pour utiliser le protocole http
- Appuyer sur Entrer pour finir

```

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

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

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

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

The IPv4 LAN address has been set to 192.168.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://192.168.10.254/

Press <ENTER> to continue.

```

On peut voir que l'adresse ip a bien été modifié :

```

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.136.128/24
LAN (lan)      -> em1      -> v4: 192.168.10.254/24

```

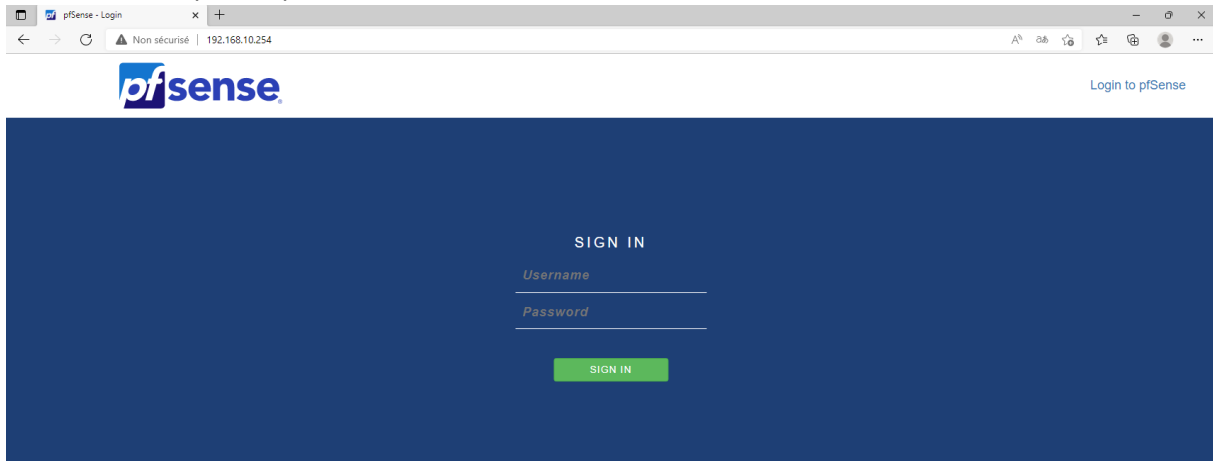
## Configuration de base

Depuis un client windows10 qui est aussi dans le réseau Vmnet1, ouvrir un navigateur et aller à l'adresse suivante : <http://192.168.10.254>

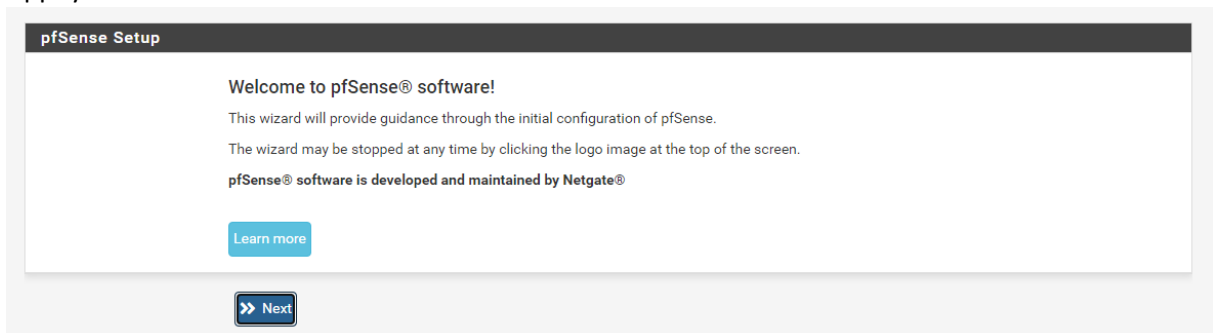
Utiliser les identifiants suivants pour se loguer :

Login : admin

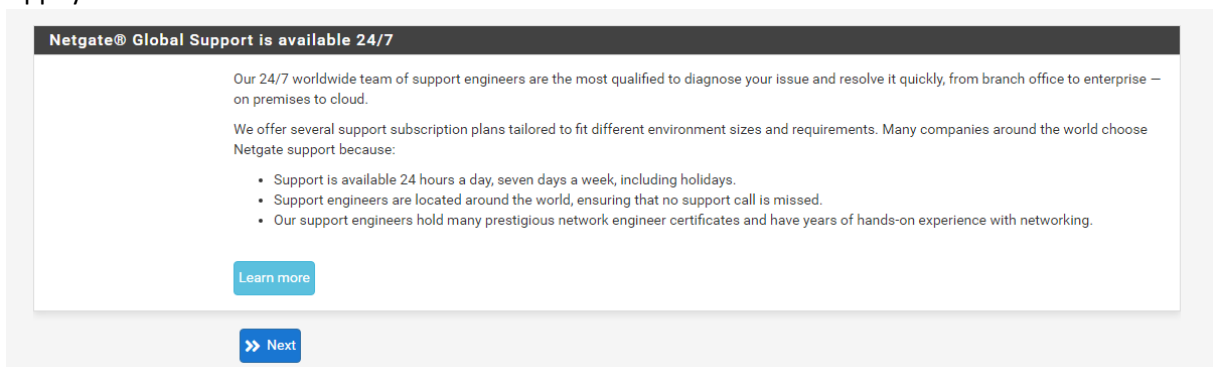
mot de passe : pfsense



Appuyer sur next :



Appuyer sur next :





Mettre un serveur dns et appuyer sur next :

The screenshot shows the 'General Information' configuration page in pfSense. It includes fields for Hostname (pfSense), Domain (home.arpa), Primary DNS Server (1.1.1.1), and Secondary DNS Server. There is a checkbox for 'Override DNS' which is checked. A 'Next' button is at the bottom.

| General Information  |   |
|--|---|
| On this screen the general pfSense parameters will be set.   |   |
| Hostname   | pfSense<br>EXAMPLE: myserver  |
| Domain   | home.arpa<br>EXAMPLE: mydomain.com  |
| The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard. |   |
| Primary DNS Server   | 1.1.1.1   |
| Secondary DNS Server   |   |
| Override DNS   | <input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN |
| <a href="#">Next</a>   |   |

Ne rien changer dans l'interface de configuration WAN.

On fait attention que ces 2 cases soient décochées :

The screenshot shows the WAN configuration page with two sections: 'RFC1918 Networks' and 'Block bogon networks'. Both sections have a checkbox that is checked. A 'Next' button is at the bottom.

| RFC1918 Networks               |  |
|--------------------------------|--|
| Block RFC1918 Private Networks | <input checked="" type="checkbox"/> Block private networks from entering via WAN<br>When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too. |

| Block bogon networks |   |
|----------------------|---|
| Block bogon networks | <input checked="" type="checkbox"/> Block non-Internet routed networks from entering via WAN<br>When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received. |

[Next](#)

Ne rien changer sur l'interface LAN :

The screenshot shows the 'Configure LAN Interface' page. It includes fields for LAN IP Address (192.168.10.254) and Subnet Mask (24). A 'Next' button is at the bottom.

| Configure LAN Interface   |   |
|---|---|
| On this screen the Local Area Network information will be configured. |   |
| LAN IP Address  | 192.168.10.254<br>Type dhcp if this interface uses DHCP to obtain its IP address. |
| Subnet Mask   | 24  |
| <a href="#">Next</a>  |   |

Définir un nouveau mot de passe pour le compte admin :

The screenshot shows the 'Set Admin WebGUI Password' page. It includes two password input fields: 'Admin Password' and 'Admin Password AGAIN'. A 'Next' button is at the bottom.

| Set Admin WebGUI Password   |       |
|---|-------|
| On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled. |       |
| Admin Password  | ***** |
| Admin Password AGAIN  | ***** |
| <a href="#">Next</a>  |       |

Appuyer ensuite sur Reload puis sur finish. Le setup wizard est terminé.

## Configuration du DHCP

Aller dans Services > Dhcp Server, et changer les paramètres suivants :

| General Options           |  |
|---------------------------|--|
| Enable                    | <input checked="" type="checkbox"/> Enable DHCP server on LAN interface  |
| BOOTP                     | <input type="checkbox"/> Ignore BOOTP queries  |
| Deny unknown clients      | <div>Allow known clients from only this interface</div> <div>When set to <b>Allow all clients</b>, any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b>, any DHCP client with a MAC address listed on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b>, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</div> |
| Ignore denied clients     | <div><input type="checkbox"/> Denied clients will be ignored rather than rejected.</div> <div>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</div>   |
| Ignore client identifiers | <div><input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.</div> <div>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</div>   |
| Subnet                    | 192.168.10.0   |
| Subnet mask               | 255.255.255.0  |
| Available range           | 192.168.10.1 - 192.168.10.254  |
| Range                     | <div>192.168.10.100192.168.10.199</div> <div>FromTo</div>  |

| Servers      |  |
|--------------|--|
| WINS servers | <div>WINS Server 1</div> <div>WINS Server 2</div>  |
| DNS servers  | <div>1.1.1.1</div> <div>DNS Server 2</div> <div>DNS Server 3</div> <div>DNS Server 4</div> <div>Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.</div> |

| Other Options |  |
|---------------|--|
| Gateway       | <div>192.168.10.254</div> <div>The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.</div> |

Ne pas oublier de renseigner un serveur DNS et une passerelle.

Appuyer sur Save.

## Paramétrage du Firewall

### Bloquer tous les trafics

Aller dans Firewall > Rules > LAN, puis cliquer sur Add pour créer une nouvelle règle.

Sélectionner les paramètres comme sur l'image suivante, puis appuyer sur Save :

**Edit Firewall Rule**

**Action**    
 Choose what to do with packets that match the criteria specified below.   
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule   
 Set this option to disable this rule without removing it from the list.

**Interface**    
 Choose the interface from which packets must come to match this rule.

**Address Family**    
 Select the Internet Protocol version this rule applies to.

**Protocol**    
 Choose which IP protocol this rule should match.

**Source**   
 ☐ Invert match   /

**Destination**   
 ☐ Invert match   /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule   
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**    
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Nous allons maintenant supprimer les 2 règles qui sont créés par défaut lors de l'installation de PfSense. Pour cela il faut les sélectionner et cliquer sur Delete :

| Rules (Drag to Change Order)        |                |          |         |      |             |      |         |       |          |                                    |         |
|-------------------------------------|----------------|----------|---------|------|-------------|------|---------|-------|----------|------------------------------------|---------|
| <input type="checkbox"/>            | States         | Protocol | Source  | Port | Destination | Port | Gateway | Queue | Schedule | Description                        | Actions |
| <input checked="" type="checkbox"/> | ✓ 1 / 2.04 MiB | *        | *       | *    | LAN Address | 80   | *       | *     |          | Anti-Lockout Rule                  |         |
| <input type="checkbox"/>            | 👉 0 / 234 B    | IPv4+6 * | *       | *    | *           | *    | *       | none  |          | Deny all                           |         |
| <input checked="" type="checkbox"/> | ✓ 0 / 0 B      | IPv4 *   | LAN net | *    | *           | *    | *       | none  |          | Default allow LAN to any rule      |         |
| <input checked="" type="checkbox"/> | ✓ 0 / 0 B      | IPv6 *   | LAN net | *    | *           | *    | *       | none  |          | Default allow LAN IPv6 to any rule |         |

Add Add Delete Save Separator

Ne pas oublier d'appuyer sur Apply Changes pour appliquer les changements.

## Filtrage internet

Pour avoir accès à internet, il faut avoir accès aux ports HTTP, HTTPS et DNS. Nous allons créer un alias qui regroupera les 3 ports citées ci-dessus. Puis nous créerons une règle qui autorise le trafic TCP et UDP entre le réseau LAN et n'importe quelle autre machine sur les ports compris dans l'alias.

### Création de l'alias

Aller dans Firewall > Aliases > Ports, et cliquer sur Add

| Properties  |   |  |  |
|-------------|---|--|--|
| Name        | Accès internet<br><small>The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".</small>              |  |  |
| Description | Inclut les ports 80, 443 et 53<br><small>A description may be entered here for administrative reference (not parsed).</small> |  |  |
| Type        | Port(s) ▼   |  |  |

| Port(s) |  |             |        |
|---------|--|-------------|--------|
| 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    | 53   | Description | Delete |
|         | 443  | Description | Delete |
|         | 80   | Description | Delete |

Appuyer sur Save

## Création de la règle

Aller dans Firewall > Rules > Add

Donner les paramètres suivants :

### Edit Firewall Rule

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** LAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP/UDP  
Choose which IP protocol this rule should match.

**Source**  

**Source** ☐ Invert match LAN net Source Address /

Display Advanced  
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**  

**Destination** ☐ Invert match any Destination Address /

**Destination Port Range** (other) Acces\_internet (other) Acces\_internet  
From Custom To Custom  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Appuyer sur Save.

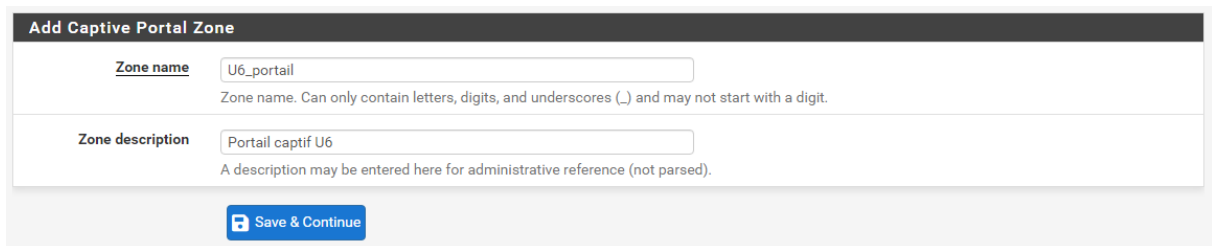
Faire attention que cette règle soit au-dessus de la règle « deny all », sinon elle ne sera pas prise en compte. On obtient donc cela :

| Rules (Drag to Change Order)                  |              |              |         |      |             |                |         |       |          |                          |         |
|---|--------------|--------------|---------|------|-------------|----------------|---------|-------|----------|--------------------------|---------|
| <input type="checkbox"/>                      | States       | Protocol     | Source  | Port | Destination | Port           | Gateway | Queue | Schedule | Description              | Actions |
| <input checked="" type="checkbox"/>           | 3 / 3.96 MiB | *            | *       | *    | LAN Address | 80             | *       | *     |          | Anti-Lockout Rule        |         |
| <input type="checkbox"/>                      | 0 / 0 B      | IPv4 TCP/UDP | LAN net | *    | *           | Acces_internet | *       | none  |          | Allow access to internet |         |
| <input type="checkbox"/>                      | 0 / 50 KiB   | IPv4+6 *     | *       | *    | *           | *              | *       | none  |          | Deny all                 |         |
| <div> Add  Add  Delete  Save  Separator</div> |              |              |         |      |             |                |         |       |          |                          |         |

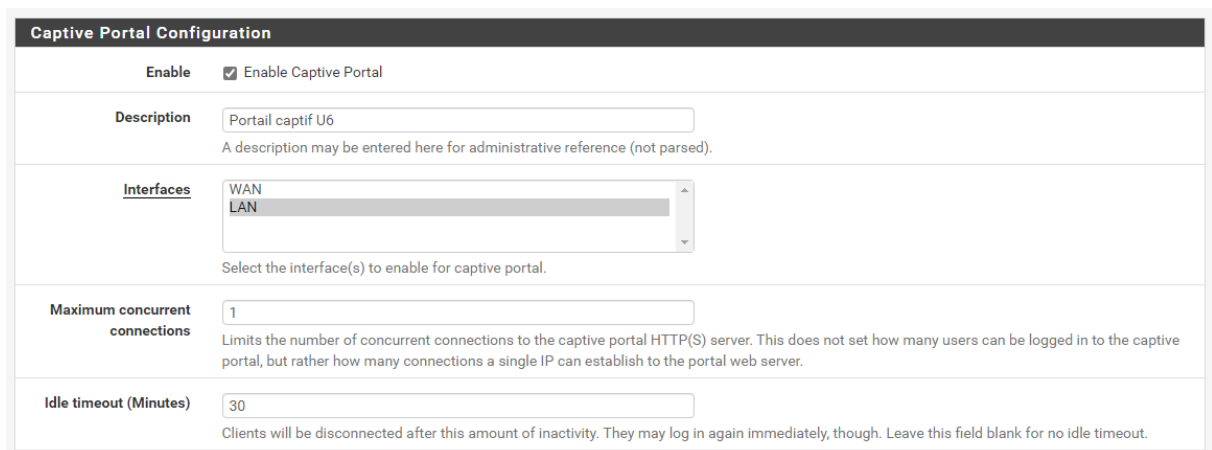
## Paramétrage du portail captif

Aller dans Services > Captive Portal, puis Add pour ajouter un nouveau portail.

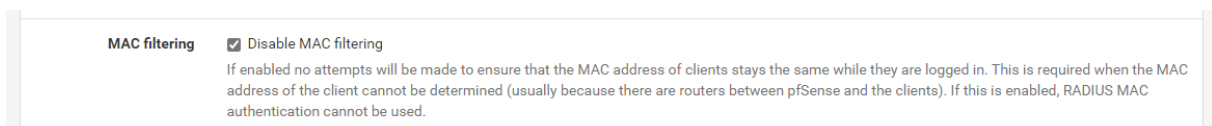
- On lui donne un nom



- On coche Enable pour l'activer
- On choisit l'interface LAN
- On écrit 1 dans *Maximum concurrent connections*. Cela signifie que une machine (une seule adresse ip) ne pourra pas établir plusieurs connexions avec le portail
- On écrit 30 dans *Idle timeout*. Cela signifie qu'après 30 min d'inactivité, l'utilisateur sera déconnecté.



- Il n'est pas nécessaire de filtrer les adresses MAC. On coche donc la case *Disable MAC filtering*



- Dans *Authentication Server*, sélectionner Local Database :

**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.

Ne pas modifier les autres paramètres. Appuyer sur Save

## Création de l'utilisateur

Nous allons créer un utilisateur qui pourra se connecter au portail captif. Cette utilisateur s'appellera test.

Aller dans System > User Manager > Users > Add

On donne les informations à propos du nouvel utilisateurs, puis on appuie sur Save :

**User Properties**

Defined by USER

Disabled ☐ This user cannot login

Username test

Password \*\*\*\*\*

## Création du groupe

Nous allons créer un groupe qui réunira tous les membres devant accéder au portail captif. Nous allons mettre l'utilisateur test dedans.

Aller dans System > User Manager > Groups > Add

Donner les paramètres suivants, puis cliquer sur Save :

**Group Properties**

Group name Portail\_membres

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 Groupe des utilisateurs ayant accès au portail captif

Group description, for administrative information only

Group membership admin

test

Not members

Members

Move to "Members"

Move to "Not members"

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

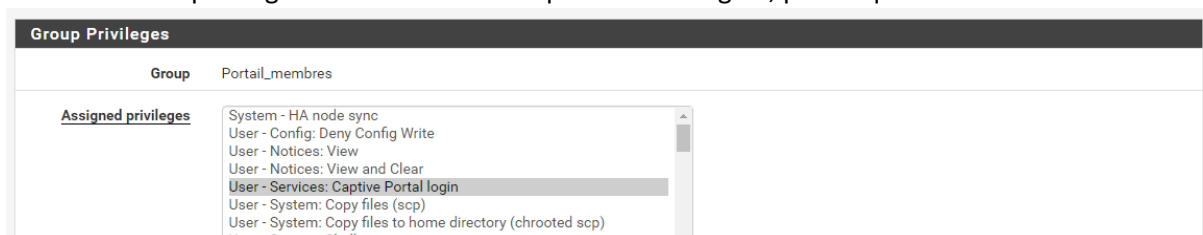
Modifier le groupe que l'on vient de créer.

Dans *Assigned Privileges* cliquer sur Add



The screenshot shows a table titled "Assigned Privileges". The table has three columns: "Name", "Description", and "Action". The table is currently empty. To the right of the table, there is a green button with a white plus sign and the text "Add".

Sélectionner le privilège « User – Services: Captive Portal Login», puis cliquer sur Save :



The screenshot shows the "Group Privileges" interface. At the top, there is a header "Group Privileges". Below it, there is a section for "Group" with the value "Portail\_membres". Underneath, there is a section titled "Assigned privileges" which contains a list of privileges. The list includes: "System - HA node sync", "User - Config: Deny Config Write", "User - Notices: View", "User - Notices: View and Clear", "User - Services: Captive Portal login" (which is highlighted), "User - System: Copy files (scp)", "User - System: Copy files to home directory (chrooted scp)", and "User - System: Shell account access".



# Tests

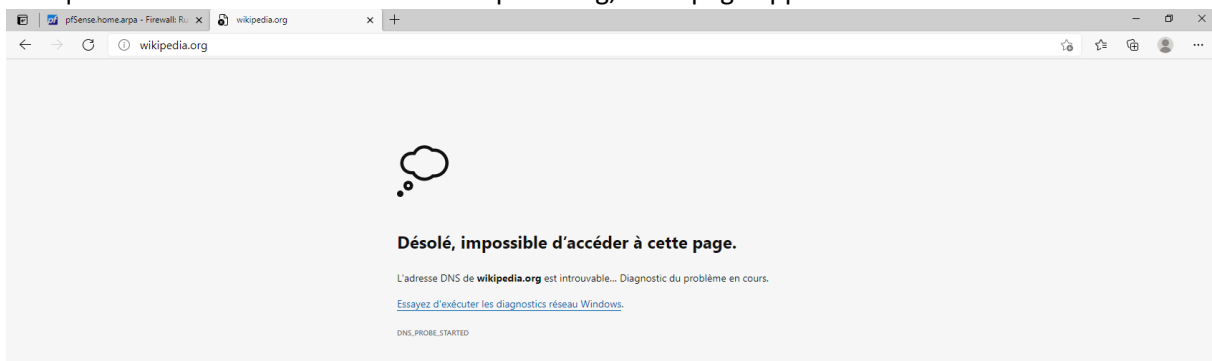
## Test des règles du Firewall

Nous allons vérifier que les règles du Firewall fonctionnent bien.

Nous allons désactiver les 3 règles du firewall autorisant l'accès à internet :

| Rules (Drag to Change Order)                  |               |              |         |      |             |             |         |       |          |                   |         |
|---|---------------|--------------|---------|------|-------------|-------------|---------|-------|----------|-------------------|---------|
| <input type="checkbox"/>                      | States        | Protocol     | Source  | Port | Destination | Port        | Gateway | Queue | Schedule | Description       | Actions |
| <input checked="" type="checkbox"/>           | 3 / 3.75 MiB  | *            | *       | *    | LAN Address | 80          | *       | *     |          | Anti-Lockout Rule |         |
| <input type="checkbox"/>                      | 0 / 15.98 MiB | IPv4 TCP/UDP | LAN net | *    | *           | 443 (HTTPS) | *       | none  |          | Allow https (443) |         |
| <input type="checkbox"/>                      | 26 / 303 KiB  | IPv4 TCP/UDP | LAN net | *    | *           | 53 (DNS)    | *       | none  |          | Allow dns(53)     |         |
| <input type="checkbox"/>                      | 0 / 4 KiB     | IPv4 TCP/UDP | LAN net | *    | *           | 80 (HTTP)   | *       | none  |          | Allow http (80)   |         |
| <input type="checkbox"/>                      | 0 / 62 KiB    | IPv4+6 *     | *       | *    | *           | *           | *       | none  |          | Deny all          |         |
| <div> Add  Add  Delete  Save  Separator</div> |               |              |         |      |             |             |         |       |          |                   |         |

Lorsque l'on essaie d'accéder au site wikipedia.org, cette page apparaît :



Réactivons nos 3 règles :

| Rules (Drag to Change Order)        |              |              |         |      |             |             |         |       |          |                   |         |
|-------------------------------------|--------------|--------------|---------|------|-------------|-------------|---------|-------|----------|-------------------|---------|
| <input type="checkbox"/>            | States       | Protocol     | Source  | Port | Destination | Port        | Gateway | Queue | Schedule | Description       | Actions |
| <input checked="" type="checkbox"/> | 2 / 3.84 MiB | *            | *       | *    | LAN Address | 80          | *       | *     |          | Anti-Lockout Rule |         |
| <input type="checkbox"/>            | 0 / 0 B      | IPv4 TCP/UDP | LAN net | *    | *           | 443 (HTTPS) | *       | none  |          | Allow https (443) |         |
| <input type="checkbox"/>            | 0 / 0 B      | IPv4 TCP/UDP | LAN net | *    | *           | 53 (DNS)    | *       | none  |          | Allow dns(53)     |         |
| <input type="checkbox"/>            | 0 / 0 B      | IPv4 TCP/UDP | LAN net | *    | *           | 80 (HTTP)   | *       | none  |          | Allow http (80)   |         |
| <input type="checkbox"/>            | 0 / 0 B      | IPv4+6 *     | *       | *    | *           | *           | *       | none  |          | Deny all          |         |

Et reéssayons d'accéder au site de wikipedia :

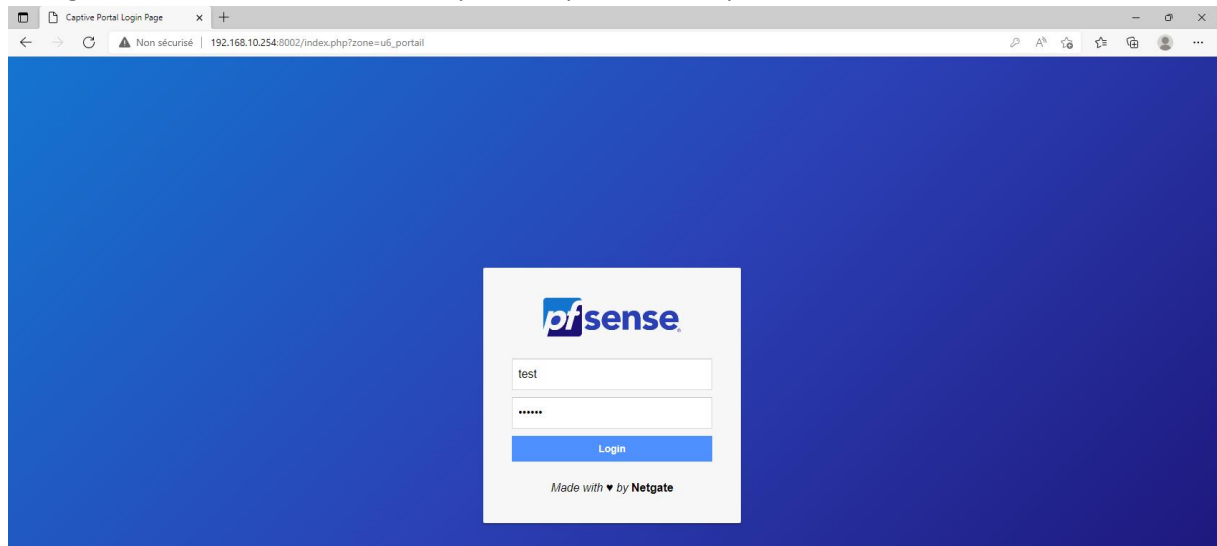


## Test du portail captif

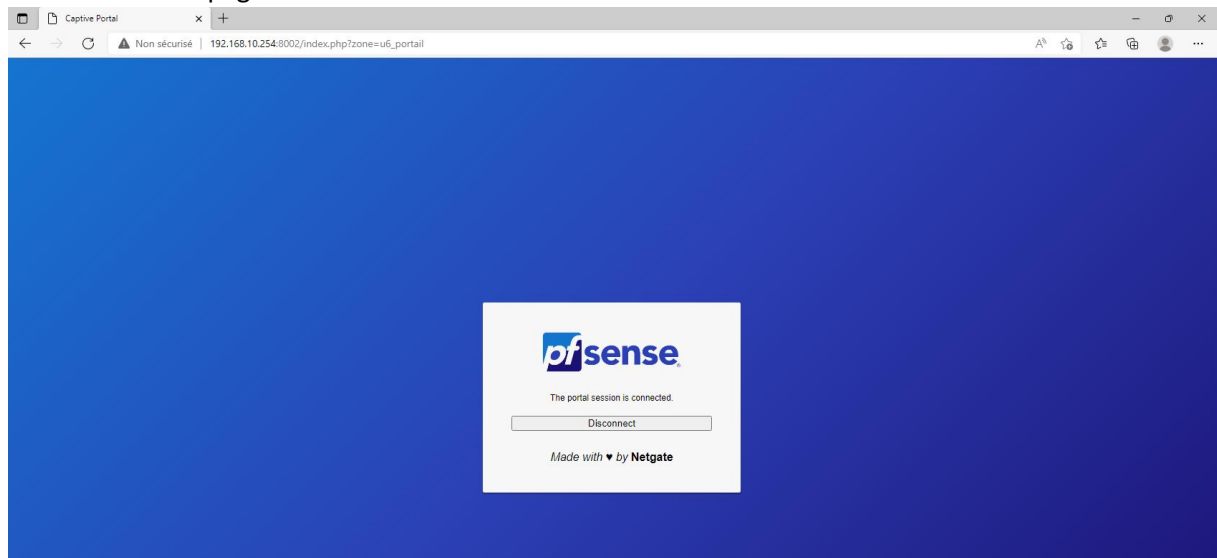
Se rendre à l'adresse suivante pour accéder au portail :

[http://192.168.10.254:8002/index.php?zone=u6\\_portail](http://192.168.10.254:8002/index.php?zone=u6_portail)

Se connecter avec les identifiants du compte test qui a été créé précédemment :



On tombe sur la page suivante :



Le message "The portal session is connected." apparaît. Le portail captif est donc bien opérationnel en local.