

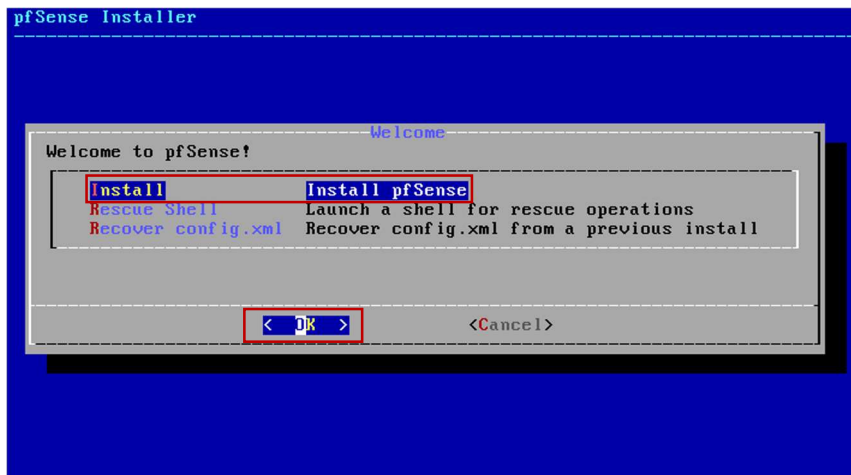
# *Installation* *pfSense :*

# Sommaire

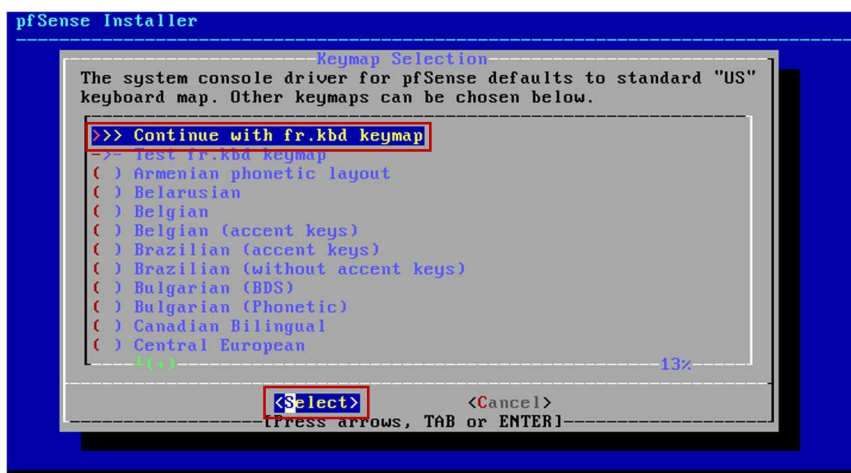
<b>Installation serveur pfSense.....</b>	<b>3</b>
<b>Configuration WAN / LAN .....</b>	<b>8</b>
<b>Configuration pfSense web .....</b>	<b>12</b>
<b>Captive Portail .....</b>	<b>15</b>

# Installation serveur pfSense

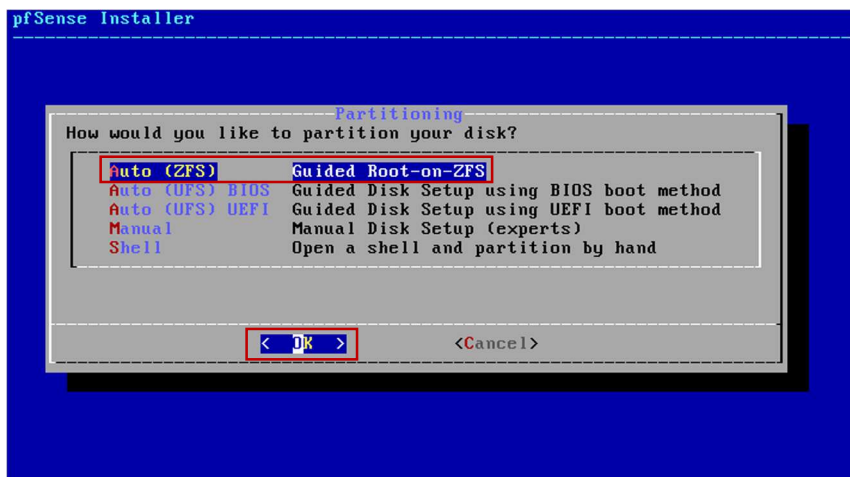
Sélectionner « Install pfSense » puis appuyer sur Enter.



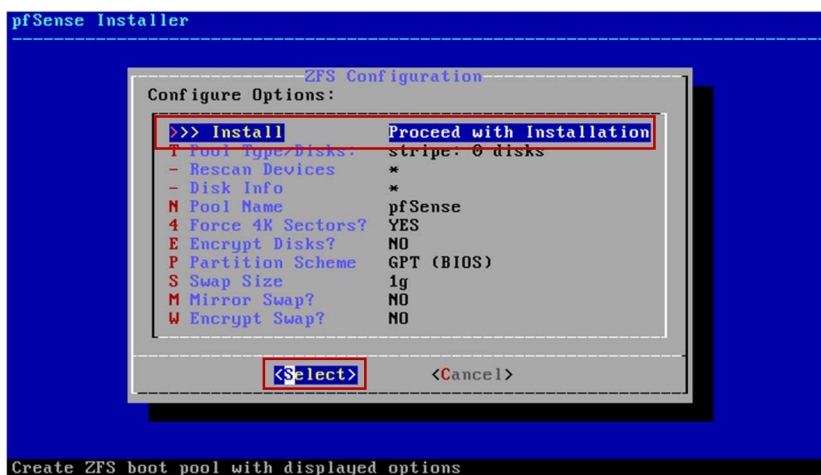
Sélectionner la langue de clavier voulu (Cela dépend du clavier).



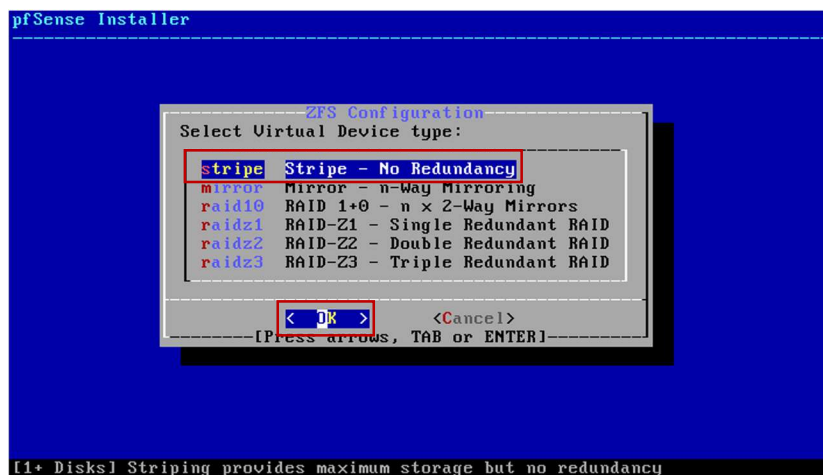
Laisse sur « Auto (ZFS) » puis appuyer sur Enter.



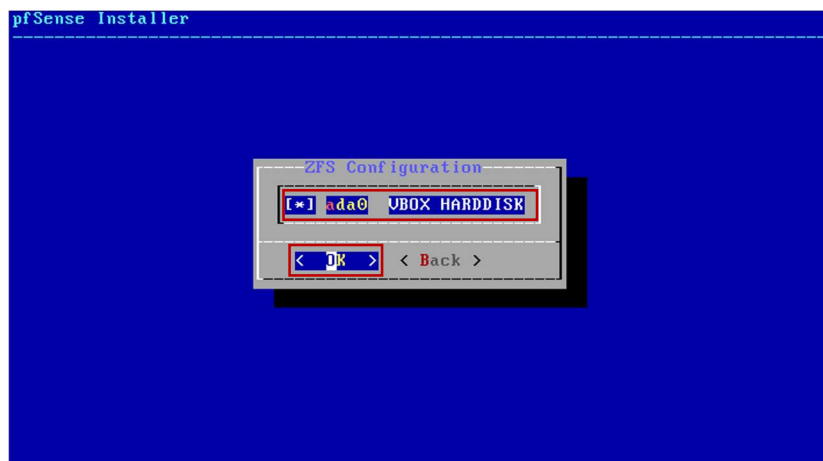
Sélectionner « Proceed with Installation » puis appuyer sur Enter.



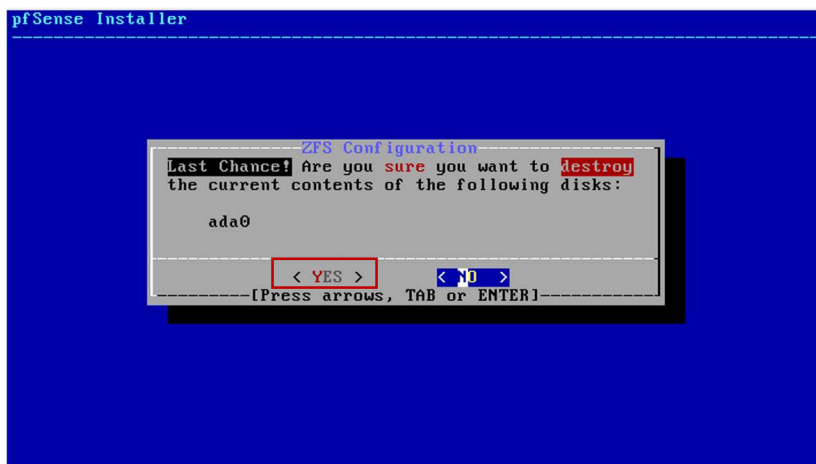
Sélectionner « Stripe – No Redundancy » puis appuyer sur Enter.



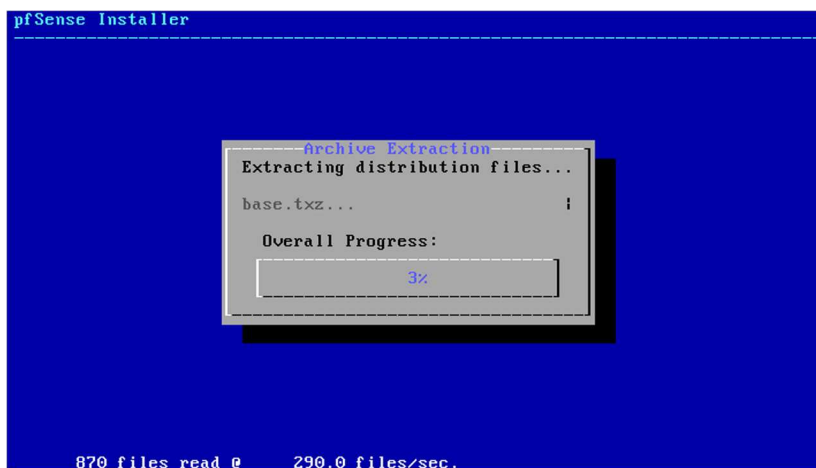
Cocher la configuration affichée et appuyer sur Enter.



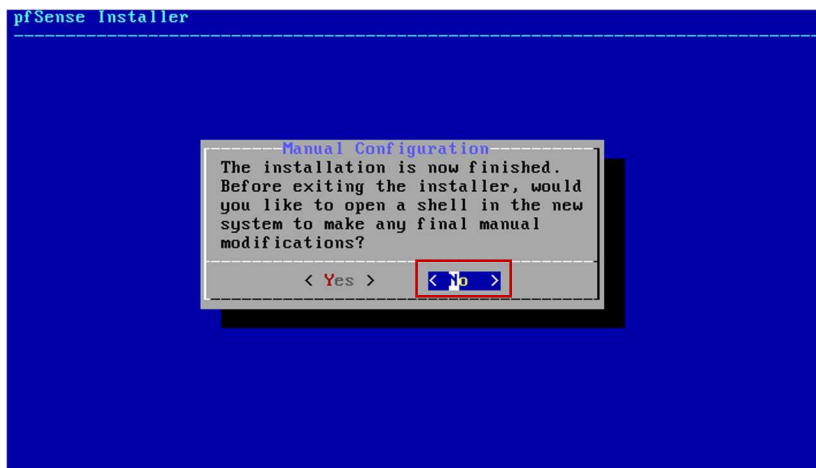
Sélectionner « YES » puis appuyer sur Enter.



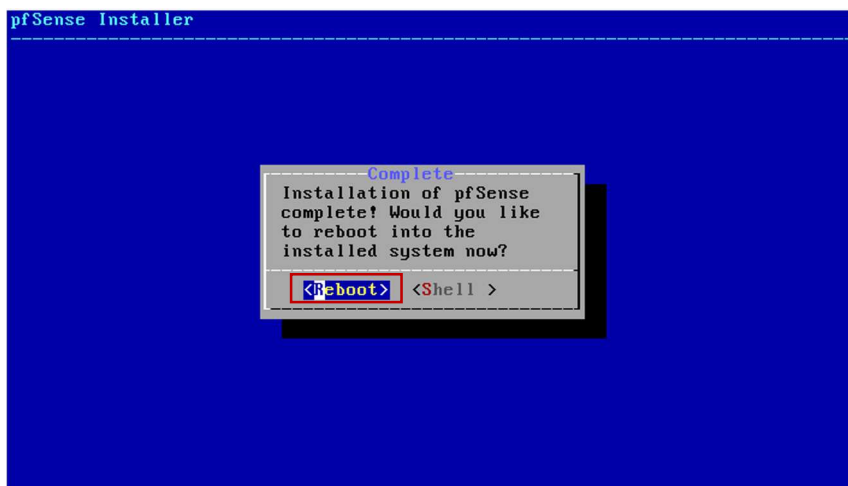
Attendre la fin de l'extraction des archives.



Sélectionner « No » puis appuyer sur Enter.



Sélectionner « Reboot » puis appuyer sur Enter.



# Configuration WAN / LAN

Ecrire « 2 » pour “Set interface(s) IP address”.

```
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to dhcp

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 9a00f38b0ae2ea9ec024

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.110/24
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
```

Ecrire « 2 » pour configurer l'adresse du « LAN ».

```
VirtualBox Virtual Machine - Netgate Device ID: 9a00f38b0ae2ea9ec024

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.110/24
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)
2 - LAN (em1 - static)

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



Renseigner l'adresse IP voulue (192.168.10.254) puis appuyer sur Enter.

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.110/24
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)
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
```

Renseigner le CIDR (24) puis appuyer sur Enter.

```
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)
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
```

Ne rien renseigner puis appuyer sur Enter.

```
8) Shell
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp)
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
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Ecrire « n » puis appuyer sur Enter.

```
1 - WAN (em0 - dhcp)
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
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
```

Configuration serveur pfSense terminé.

```
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.
VirtualBox Virtual Machine - Netgate Device ID: 9a00f38b0ae2ea9ec024

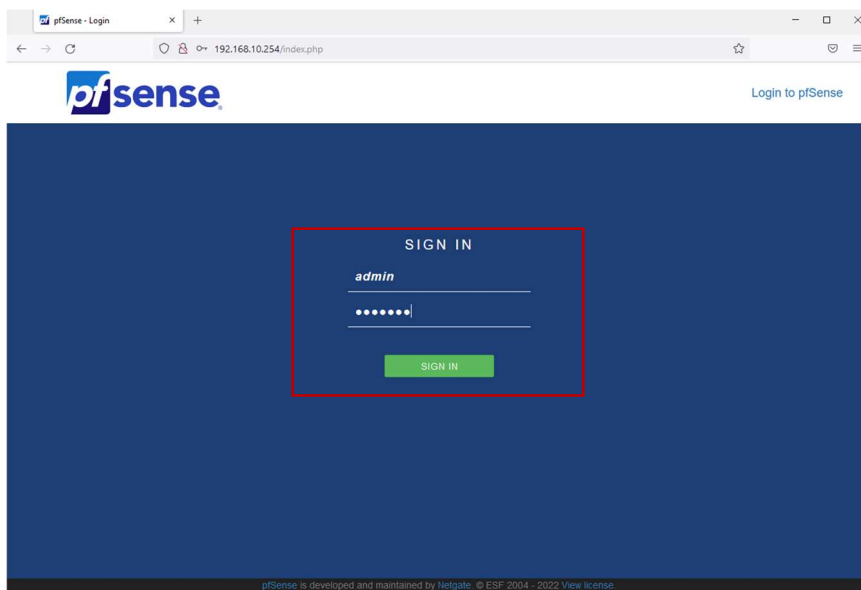
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.110/24
LAN (lan)      -> em1      -> v4: 192.168.10.254/24

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: 
```

Test de connexion sur l'interface graphique pfSense depuis un client Windows :



Identifiants et mot de passe par défaut :

ID: admin

MDP: pfsense

# Configuration pfSense web

## Filtrage Deny all:

Ajout règle « Deny » pour tout refuser ;

Choisir l'action « Block » et choisir « Any » pour bloquer tous les filtres.

pfSense COMMUNITY EDITION

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

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Block ▾  
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+IPv6 ▾  
Select the Internet Protocol version this rule applies to.

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

### Source

**Source** ☐ Invert match any ▾ Source Address / ▾

### Destination

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

### 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** Deny all  
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.

**Advanced Options** [Display Advanced](#)

[Save](#)

## Filtrage internet :

Accéder à « Aliases » dans l'onglet « Firewall »

Ajout règle pour Allow l'accès à internet dans la range LAN :

Indiquer le nom et la description.

Indiquer les ports à ouvrir : 53 (DNS), 80 (http), 443 (https)

The screenshot shows the pfSense Firewall Aliases configuration page. The 'Name' field is set to 'Internet' and the 'Description' is 'Autorise la sortie vers internet'. The 'Type' is set to 'Port(s)'. Below, a table lists the ports to be opened: 53 (DNS), 80 (HTTP), and 443 (HTTPS). Each entry has a 'Delete' button.

Appliquer les modifications.

Créer une nouvelle règle dans le « Firewall » :

Choisir « Pass » comme action, « LAN » comme interface, « IPv4 » comme famille d'adresse et TCP/UDP comme protocole.

The screenshot shows the pfSense Firewall Rules configuration page. The 'Action' is set to 'Pass', 'Interface' is 'LAN', 'Address Family' is 'IPv4', and 'Protocol' is 'TCP/UDP'. The 'Disabled' checkbox is unchecked.

Dans « Destination », choisir « LAN net » et indiquer dans la destination le chemin de l'alias créer précédemment.

**Source**

Source

☐ Invert match

any

▼

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

LAN net

▼

Destination Address

/

▼

Destination Port Range

(other)

▼

web\_access

(other)

▼

web\_access

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.

**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


Autorise la sortie vers internet

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.




Advanced Options



⚙ Display Advanced

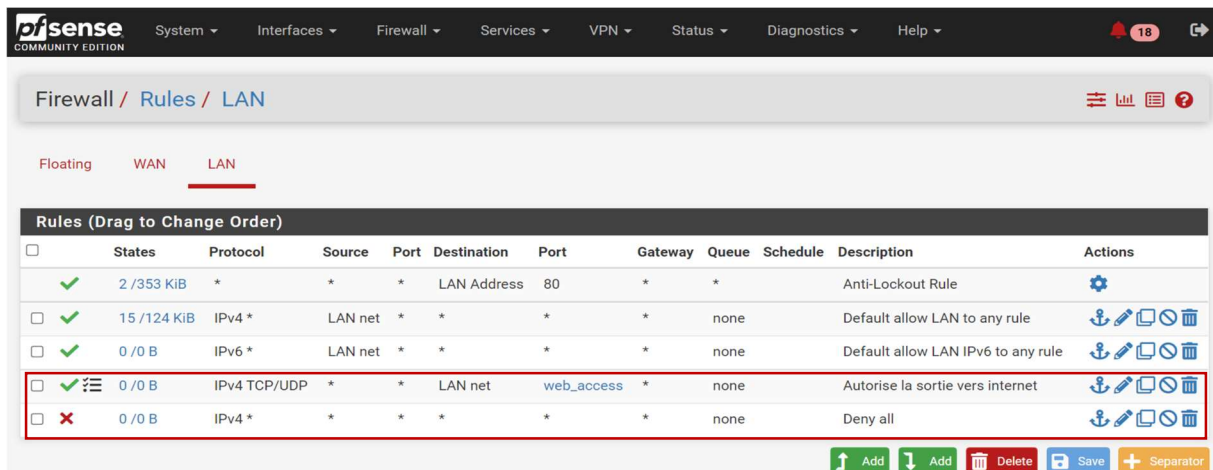
## Récapitulatif des règles appliquées :




















The screenshot shows the PfSense Firewall Aliases Ports configuration page. The breadcrumb trail is "Firewall / Aliases / Ports". The "Ports" tab is selected. The table "Firewall Aliases Ports" has the following data:






Name	Values	Description	Actions
Internet	53, 80, 443	Autorise la sortie vers internet	  

Buttons at the bottom right:  Add,  Import.



The screenshot shows the PfSense Firewall Rules LAN configuration page. The breadcrumb trail is "Firewall / Rules / LAN". The "LAN" tab is selected. The table "Rules (Drag to Change Order)" has the following data:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	2 / 353 KiB	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	15 / 124 KiB	IPv4	*	LAN net	*	*	none		Default allow LAN to any rule	   
<input type="checkbox"/>	✓	0 / 0 B	IPv6	*	LAN net	*	*	none		Default allow LAN IPv6 to any rule	   
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP/UDP	*	LAN net	web_access	*	none		Autorise la sortie vers internet	   
<input type="checkbox"/>	✗	0 / 0 B	IPv4	*	*	*	*	none		Deny all	   

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

# Captive Portal

## Partie Services :

Aller dans service et cliquer sur « Captive Portal »

The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The 'Services' menu is open, and 'Captive Portal' is highlighted. The left sidebar shows 'Status / Dashboard' and 'System Information'. The right sidebar shows 'Netgate Services And Support'.

**System Information**

Name	pfSense.home.arpa
User	admin@192.168.1.10 (Local Database)
System	VMware Virtual Machine Netgate Device ID: caabdc8a6fe77646f
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	11th Gen Intel(R) Core(TM) i7-1165G7 @ AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	

**Netgate Services And Support**

Contract type: Community Support  
Community Support Only

**NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES**

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

Ajouter un portail en cliquant sur « ADD ».

The screenshot shows the pfSense web interface with the 'Services / Captive Portal' page. The 'Captive Portal Zones' table is visible, and the 'Add' button is highlighted.

**Captive Portal Zones**

Zone	Interfaces	Number of users	Description	Actions
<a href="#">+ Add</a>				



Renseigner les informations dans les zones afin de pas s'y perdre si l'on souhaite en rajouter à l'avenir, puis sauvegarder et continuer :

The screenshot shows the 'Add Captive Portal Zone' configuration page in the PfSense web interface. 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 'Main\_zone' and 'Zone description' with the value 'Zone\_principale'. Both fields are highlighted with red rectangles. Below the 'Zone name' field, there is a note: 'Zone name. Can only contain letters, digits, and underscores (\_) and may not start with a digit.' Below the 'Zone description' field, there is a note: 'A description may be entered here for administrative reference (not parsed)'. At the bottom of the form, there is a blue button labeled 'Save & Continue'.

Cliquer sur « Enabled Captivd Portail » puis sélectionner l'interface « LAN » :

The screenshot shows the 'Captive Portal Configuration' page for the 'Main\_zone' in the PfSense web interface. The breadcrumb trail is 'Services / Captive Portal / Main\_zone / Configuration'. The page title is 'Captive Portal Configuration'. There are several tabs: 'Configuration', 'MACs', 'Allowed IP Addresses', 'Allowed Hostnames', 'Vouchers', 'High Availability', and 'File Manager'. The 'Configuration' tab is selected. The 'Enable' section has a checkbox labeled 'Enable Captive Portal' which is checked. The 'Description' field has the value 'Zone\_principale'. The 'Interfaces' section has a dropdown menu with 'WAN' and 'LAN' options, and 'LAN' is selected. The 'Maximum concurrent connections' field is empty. The 'Idle timeout (Minutes)' field is empty. Below the 'Interfaces' section, there is a note: 'Select the interface(s) to enable for captive portal.'

Dans la partie « Authentification », choisir « Local Database » dans l'authentification serveur ainsi que l'authentification secondaire au serveur :

**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.

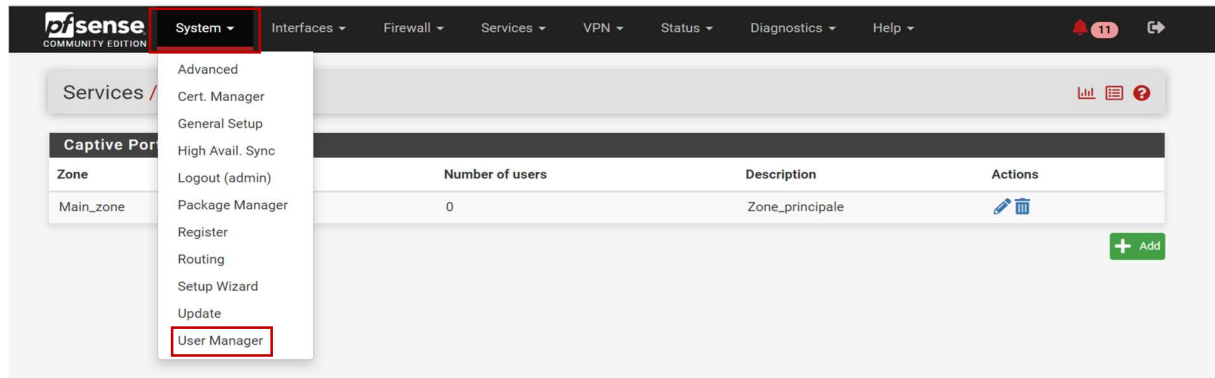
**Reauthenticate Users** ☐ Reauthenticate connected users every minute

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.

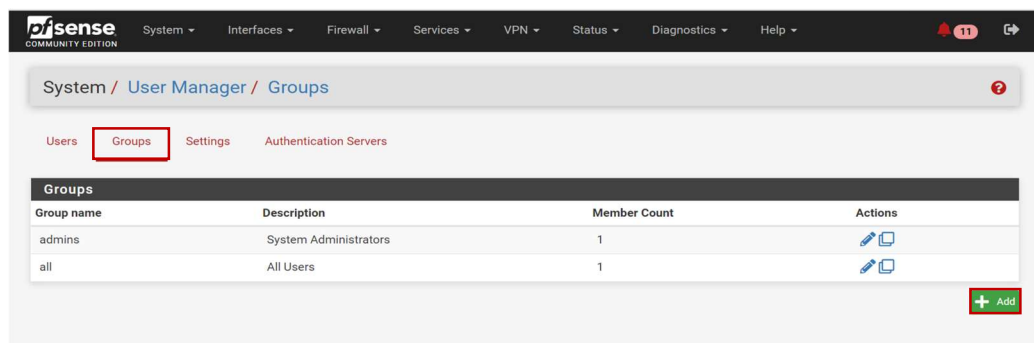
Sauvegarder puis continuer.

## Partie Système :

Aller dans l'onglet « System ».

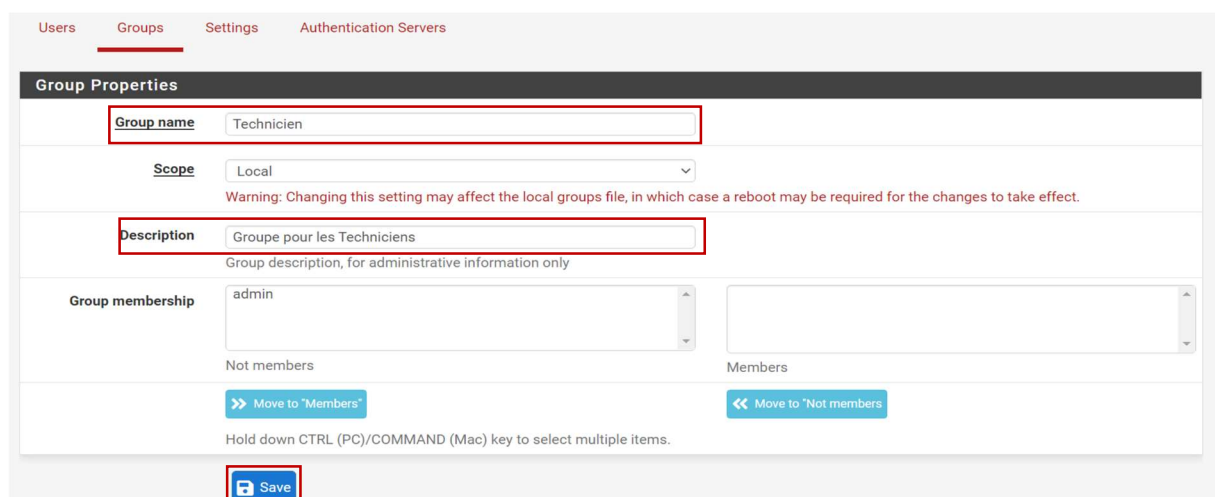


Sélectionner « Groups » puis ajouter un nouveau groupe.

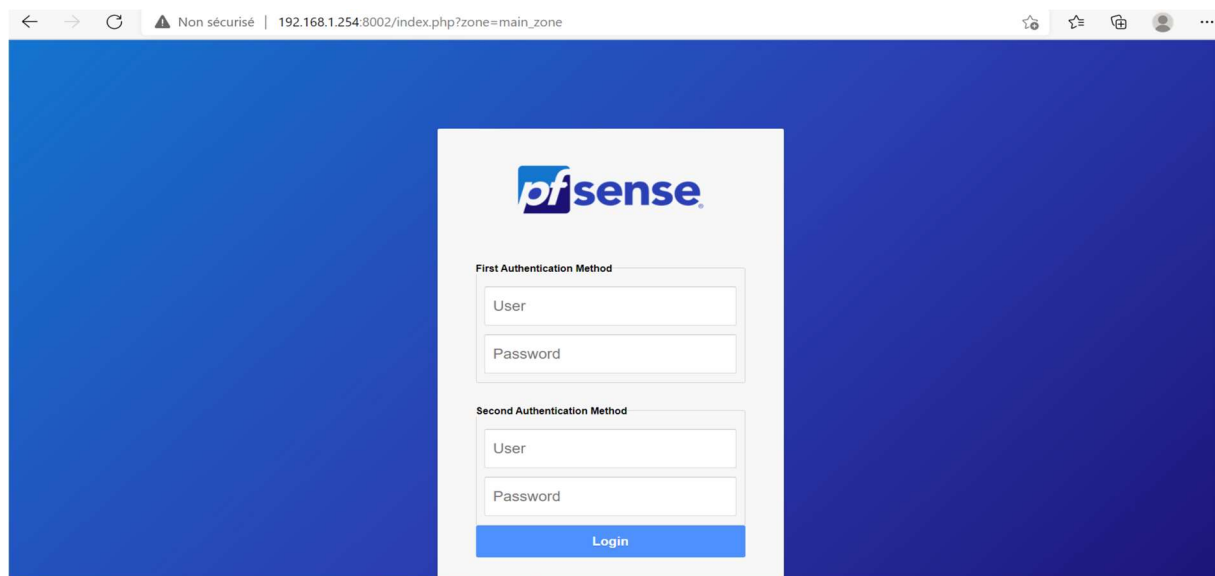


Remplissez les champs de « Group Name » puis de « Description » avec les informations souhaitées.

Sauvegarder et quitter.



## Portail de connexion :



The screenshot shows a web browser window with the address bar displaying "192.168.1.254:8002/index.php?zone=main\_zone". The page has a blue gradient background. In the center, there is a white box containing the pfSense logo at the top. Below the logo, there are two sections for authentication:

- First Authentication Method:** Contains two input fields labeled "User" and "Password".
- Second Authentication Method:** Also contains two input fields labeled "User" and "Password".

At the bottom of the white box is a blue button labeled "Login".