

## **Tp PfSense**

### **Sommaire :**

- 1/ Configuration virtualBox vm pfsense
- 2/ Installation PfSense
- 3/ Configuration réseau
- 4/ Connexion à pfsense
- 5/ Deny all
- 6/ ouvrir l'accès à internet
- 7/ Portail captif
- 8/ création groupe et utilisateur

## 1) Configuration VirtualBox vm pfsense

La première carte sera en accès par pont :

Adapter 1   Adapter 2   Adapter 3   Adapter 4

☒ Activer l'interface réseau

Mode d'accès réseau : Accès par pont

Nom : Intel(R) Wi-Fi 6 AX200 160MHz

▶ Avancé

Et la 2eme en Réseau interne

☒ Activer l'interface réseau

Mode d'accès réseau : Réseau interne

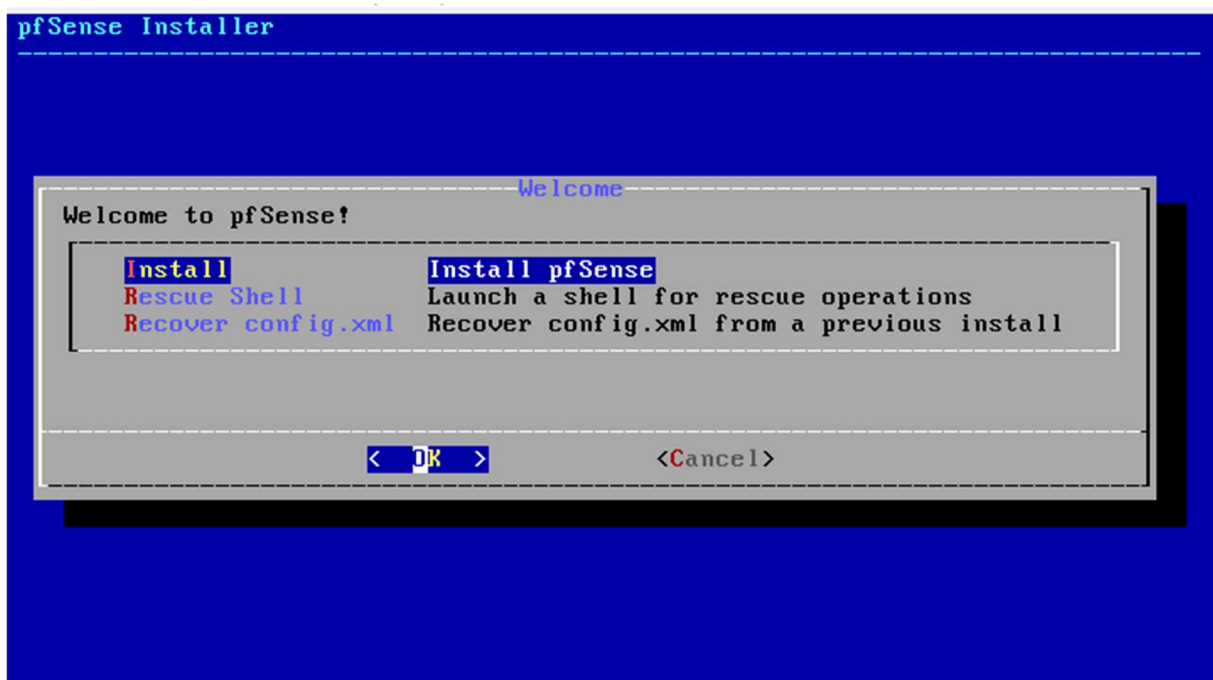
Nom : intnet

▼ Avancé

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Allow All

## 2) Installation PfSense



pfSense Installer

Partitioning

How would you like to partition your disk?

- |                 |  |
|-----------------|--|
| Auto (UFS) BIOS | Guided Disk Setup using BIOS boot method |
| Auto (UFS) UEFI | Guided Disk Setup using UEFI boot method |
| Manual          | Manual Disk Setup (experts)              |
| Shell           | Open a shell and partition by hand       |
| Auto (ZFS)      | Guided Root-on-ZFS                       |

< OK >

<Cancel>

pfSense Installer

ZFS Configuration

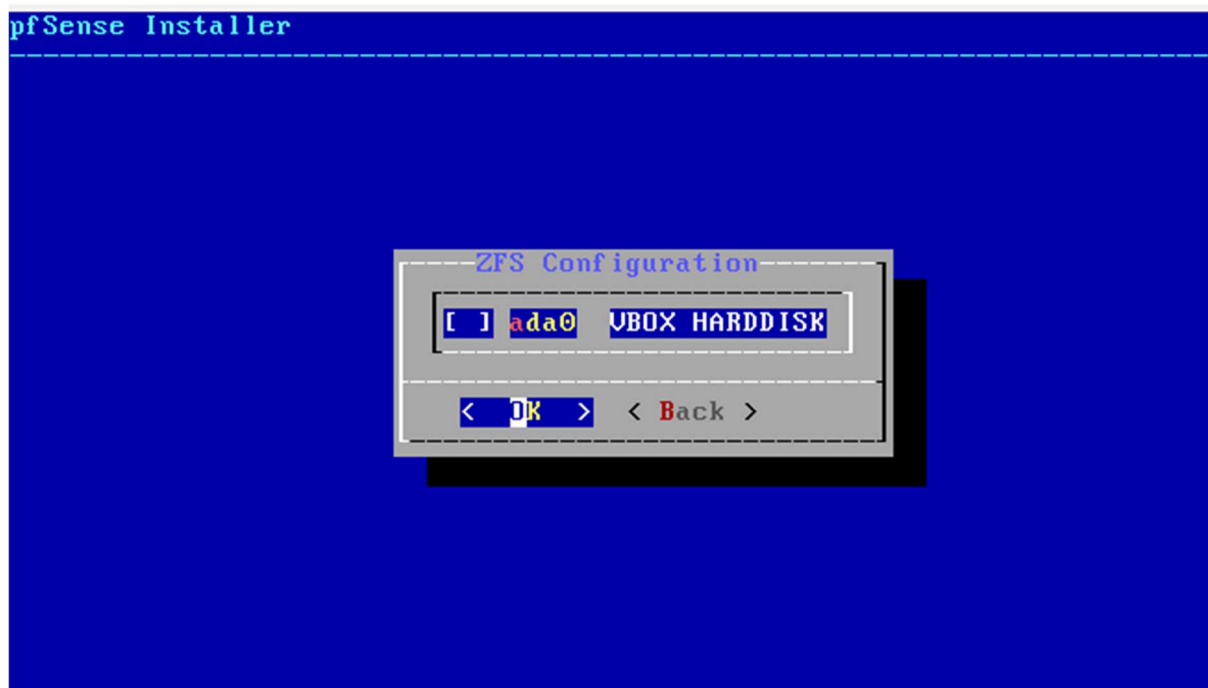
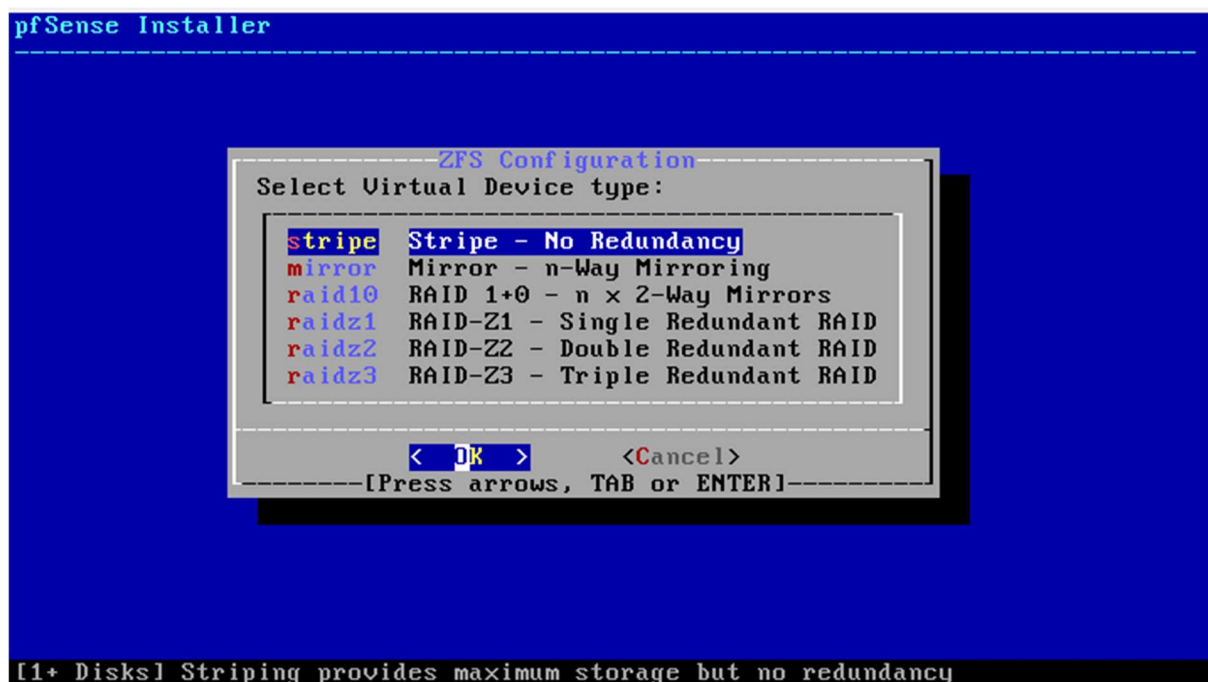
Configure Options:

- |                     |                           |
|---------------------|---------------------------|
| >>> Install         | Proceed with Installation |
| T Pool Type/Disks:  | stripe: 0 disks           |
| - Rescan Devices    | *                         |
| - Disk Info         | *                         |
| N Pool Name         | zroot                     |
| 4 Force 4K Sectors? | YES                       |
| E Encrypt Disks?    | NO                        |
| P Partition Scheme  | GPT (BIOS)                |
| S Swap Size         | 2g                        |
| M Mirror Swap?      | NO                        |
| W Encrypt Swap?     | NO                        |

<Select>

<Cancel>

Create ZFS boot pool with displayed options



Il faut cocher la case avec la barre espace

pfSense Installer

ZFS Configuration

Last Chance! Are you **sure** you want to **destroy**  
the current contents of the following disks:

ada0

< YES >

< NO >

[Press arrows, TAB or ENTER]

pfSense Installer

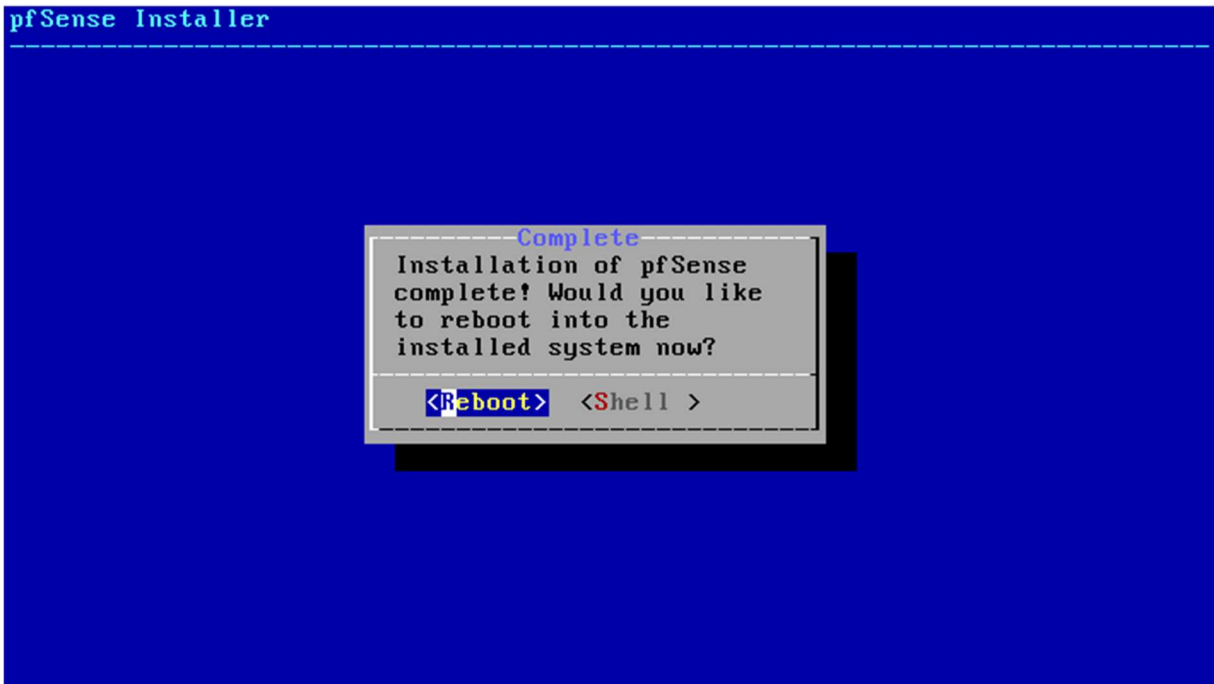
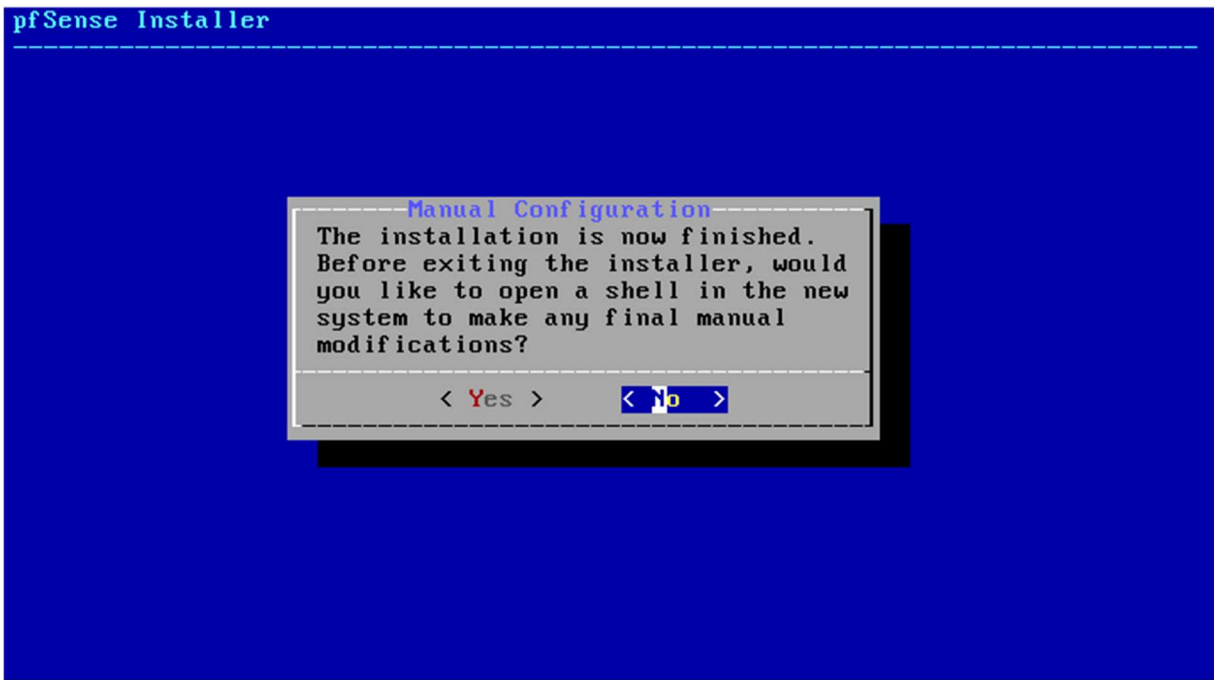
Fetching Distribution

MANIFEST	[ Done ]
base.txz	[ 48% ]

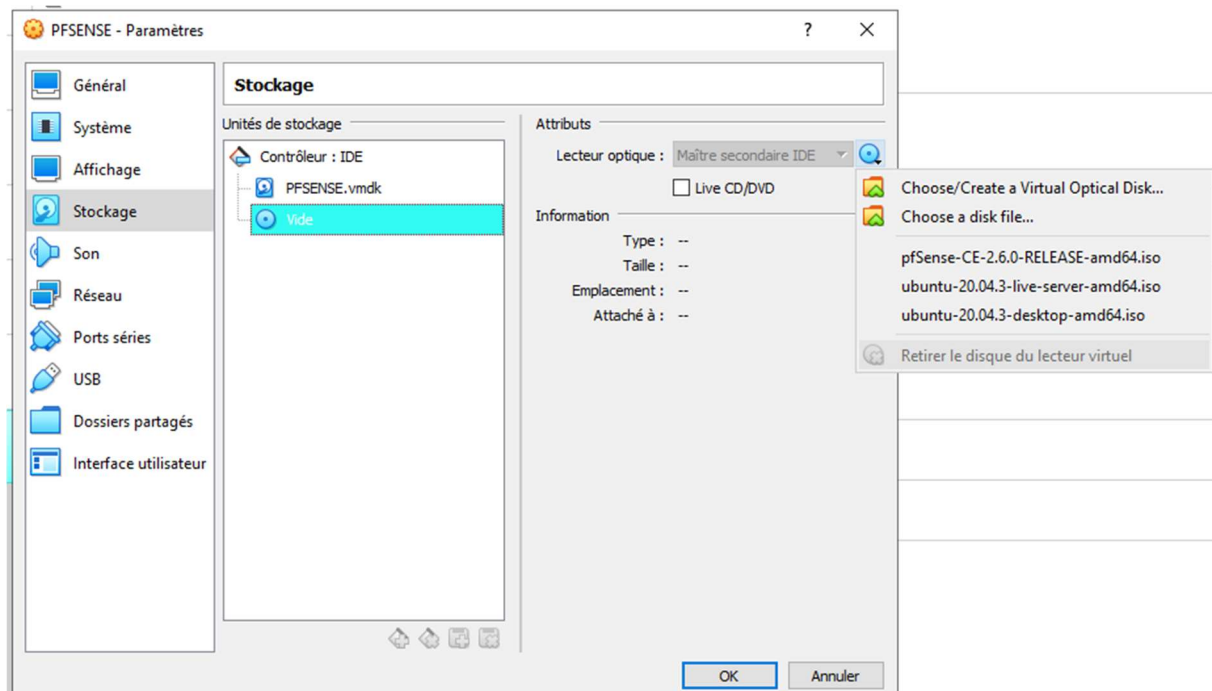
Fetching distribution files...

Overall Progress

48%



Après le reboot, on arrive sur le message de copyright, on éteint la vm et on enlève l'iso du disque sur virtualBox :



On arrive sur cette page :

```

PFSENSE [En fonction] - Oracle VM VirtualBox
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a1f6e38a8df5d1ebe39b

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

WAN (wan)      -> em0      -> v4/DHCP4: 172.20.10.2/28
LAN (lan)      -> em1      -> v4: 192.168.1.45/24

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:

```

### 3) Configuration réseau

Dans le menu principal, entrez l'option 2

```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option: 2
```

On choisit la carte à configurer, ici la carte du réseau LAN

```
Available interfaces:

1 - WAN (em0)
2 - LAN (em1 - static)

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

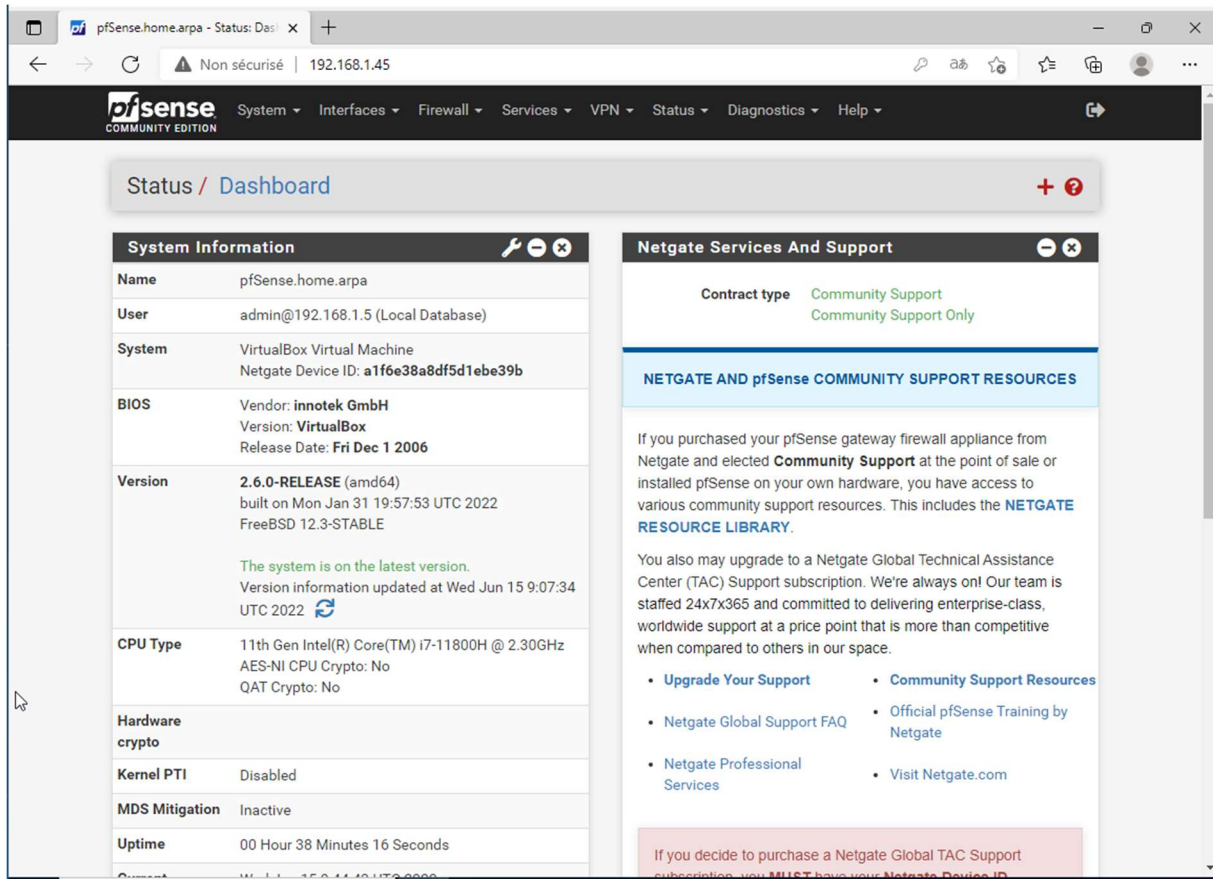
On entre ensuite l'ip et la passerelle de la carte

```
WAN (wan)      -> em0      -> v4/DHCP4: 172.20.10.2/28
LAN (lan)      -> em1      -> v4: 192.168.1.45/24
```



#### 4) Connexion à pfsense

Pour ensuite accéder à pfsense, il suffit de rentrer l'adresse ip LAN de votre server dans votre navigateur sur votre client windows :



The screenshot displays the pfSense Community Edition web interface. The browser address bar shows the URL `192.168.1.45`. The dashboard is titled "Status / Dashboard" and features two main panels:

- System Information:** A table providing details about the system, including the name, user, system type, BIOS version, and CPU type.
- Netgate Services And Support:** A section detailing the contract type and providing links to various support resources.

System Information	
Name	pfSense.home.arpa
User	admin@192.168.1.5 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: a1f6e38a8df5d1ebe39b
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE  The system is on the latest version. Version information updated at Wed Jun 15 9:07:34 UTC 2022
CPU Type	11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz AES-NI CPU Crypto: No QAT Crypto: No
Hardware crypto	
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 38 Minutes 16 Seconds

Netgate Services And Support	
Contract type	Community Support Community Support Only
<b>NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES</b>	
<p>If you purchased your pfSense gateway firewall appliance from Netgate and elected <b>Community Support</b> at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the <a href="#">NETGATE RESOURCE LIBRARY</a>.</p> <p>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.</p>	
<ul style="list-style-type: none"><li>Upgrade Your Support</li><li>Netgate Global Support FAQ</li><li>Netgate Professional Services</li></ul>	<ul style="list-style-type: none"><li>Community Support Resources</li><li>Official pfSense Training by Netgate</li><li>Visit Netgate.com</li></ul>

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID.

## 5) Deny all

On va maintenant créer une règle qui va bloquer tous les accès sur le réseau WAN et LAN :

Pour ce faire, on va se rendre dans Firewall → Rules → WAN puis on va cliquer sur Add :

The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules. The breadcrumb navigation at the top reads "Firewall / Rules / WAN". Below this, there are tabs for "Floating", "WAN", and "LAN", with "WAN" being the active tab. A table titled "Rules (Drag to Change Order)" lists existing rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 5 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0 / 1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

Below the table, a yellow warning box states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom right, there are buttons for "Add" (up arrow), "Add" (down arrow), "Delete", "Save", and "Separator".

Ensuite on va configurer la ligne action en « block » et la ligne Protocol en « any » pour bloquer tous les ports.

The screenshot shows the "Edit Firewall Rule" configuration page. The breadcrumb navigation at the top reads "Firewall / Rules / Edit". The configuration fields are as follows:

- Action:** A dropdown menu set to "Block". Below it, a hint explains the difference between block and reject.
- Disabled:** A checkbox labeled "Disable this rule" is unchecked.
- Interface:** A dropdown menu set to "WAN".
- Address Family:** A dropdown menu set to "IPv4".
- Protocol:** A dropdown menu set to "Any".

Below these fields are sections for "Source" and "Destination":

- Source:** Includes a checkbox for "Invert match" (unchecked), a dropdown set to "any", and a "Source Address" field.
- Destination:** Includes a checkbox for "Invert match" (unchecked), a dropdown set to "any", and a "Destination Address" field.

**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.

**Advanced Options**

Display Advanced

Save

Puis cliquez sur Save.

Ensuite on va faire la même chose sur le réseau LAN

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

Select the Internet Protocol version this rule applies to.

**Protocol**

Any

Choose which IP protocol this rule should match.

## 6) Ouvrir l'accès à internet

On va tout d'abord créer un alias qui va regrouper les ports dns, http et https :

Firewall / Aliases / Edit

**Properties**

**Name** Internet  
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description** regroupe DNS HTTP HTTPS  
A description may be entered here for administrative reference (not parsed).

**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.

<b>Port</b>	80	http	Delete
	443	https	Delete
	53	dns	Delete

Save + Add Port

Ensuite on revient dans l'onglet Rules et on crée une règle qui laissera passer nos 3 ports :

Firewall / Rules / Edit

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

**Destination**

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

**Destination Port Range** (other) Internet (other) 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.

## 7) Portail captif

On va maintenant créer un portail captif qui servira à fournir un accès à internet.

Services / Captive Portal / Add Zone

**Add Captive Portal Zone**

**Zone name**   
Zone name. Can only contain letters, digits, and underscores (\_) and may not start with a digit.

**Zone description**   
A description may be entered here for administrative reference (not parsed).

pfSense.home.arpa - Services: Co x +

Non sécurisé | 192.168.1.45/services\_captiveportal.php?zone=portail\_captif

System Interfaces Firewall Services VPN Status Diagnostics Help

Services / Captive Portal / PORTAIL\_CAPTIF / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

**Captive Portal Configuration**

**Enable** ☒ Enable Captive Portal

**Description**   
A description may be entered here for administrative reference (not parsed).

**Interfaces**   
LAN  
Select the interface(s) to enable for captive portal.



**Maximum concurrent connections**   
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.

**Idle timeout (Minutes)**   
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

**Hard timeout (Minutes)**   
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).

Services / Captive Portal

**Captive Portal Zones**

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

## 8) Création groupe et utilisateur

On se rend dans system → user manager

System / User Manager / Users ?

Users Groups Settings Authentication Servers

**Users**

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

Add Delete

On va tout d'abord crée un groupe « users » :

System / User Manager / Groups / Edit ?

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

Members

Move to "Members" Move to "Not members"

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

Save

Ensuite on va créer un user nommer User01 et le rajouter dans ce groupe :

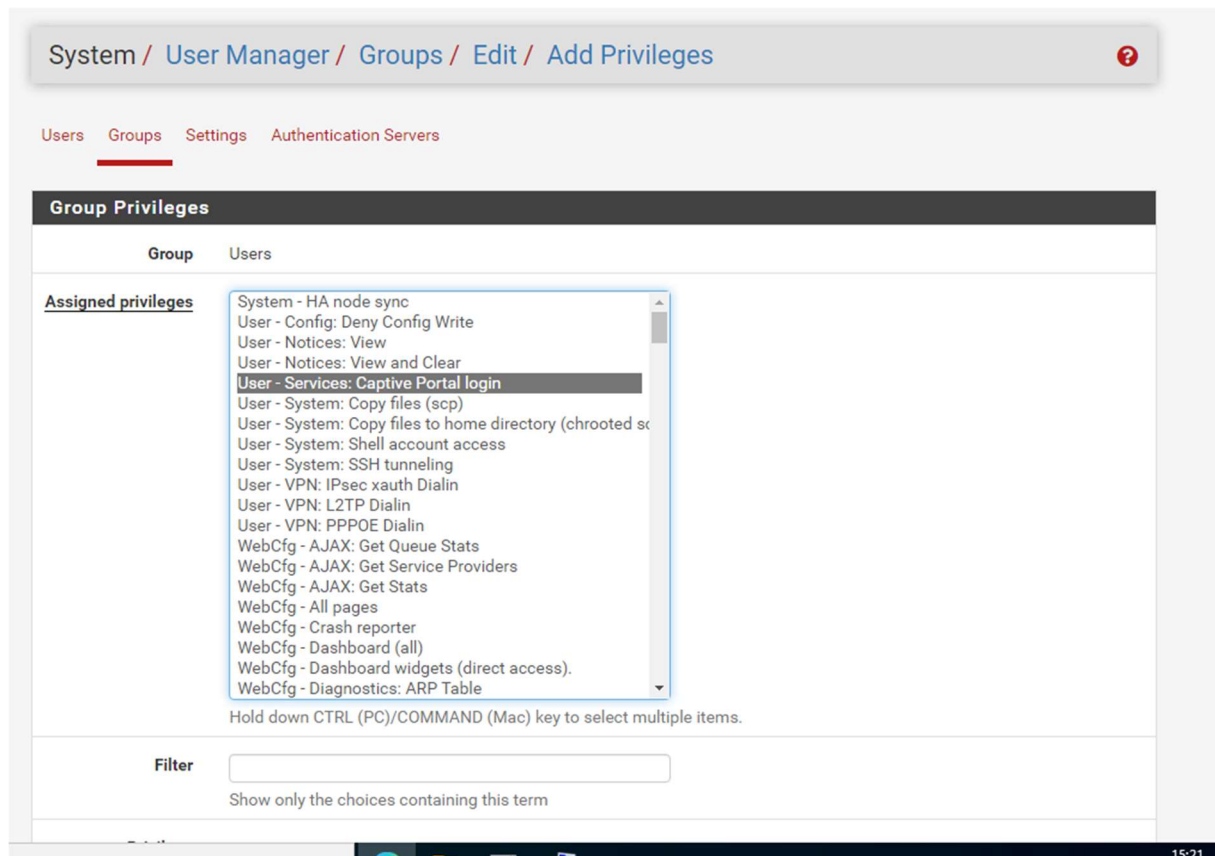
The screenshot shows the pfSense system user manager interface. The browser address bar indicates the URL is 192.168.1.45/system\_usermanager.php?act=new. The interface has a navigation bar with 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'Users' tab is selected. The 'User Properties' section contains the following fields:

- Defined by:** USER
- Disabled:** ☐ This user cannot login
- Username:** user01
- Password:** Two password input fields, both containing six asterisks.
- Full name:** An empty text field with a placeholder text: 'User's full name, for administrative information only'.
- Expiration date:** An empty date field with a placeholder text: '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:** Two dropdown menus. The left one is labeled 'Not member of' and contains 'admins'. The right one is labeled 'Member of' and contains 'Users'. Below these are two buttons: 'Move to "Member of" list' and 'Move to "Not member of" list'.
- 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.

At the bottom, there is a 'Keys' section which is partially visible.

Ensuite, on va donner l'accès à l'interface pfsense au groupe users :

Effective Privileges			
Inherited from	Name	Description	Action
			<a href="#">+ Add</a>



On se connecte ensuite à l'interface utilisateur pfsense avec le compte user01 :



