

TP PFSENSE

Sommaire :

1. Configuration virtualBox vm pfsense
2. Installation PfSense
3. Configuration réseau
4. Connexion à pfsense
5. Règles Firewall
6. Portail captif

1) Configuration VirtualBox vm pfsense

La première carte sera en accès par pont :

The screenshot shows the 'Adapter 1' tab in the VirtualBox network configuration window. The 'Adapter 2' tab is selected. The 'Activer l'interface réseau' checkbox is checked. The 'Mode d'accès réseau' dropdown is set to 'Accès par pont'. The 'Nom' dropdown is set to 'Intel(R) Wi-Fi 6 AX200 160MHz'. There is a blue play button icon and the word 'Avancé' below the 'Nom' dropdown.

Et la 2eme en Réseau interne

☒ Activer l'interface réseau

Mode d'accès réseau : Réseau interne ▼

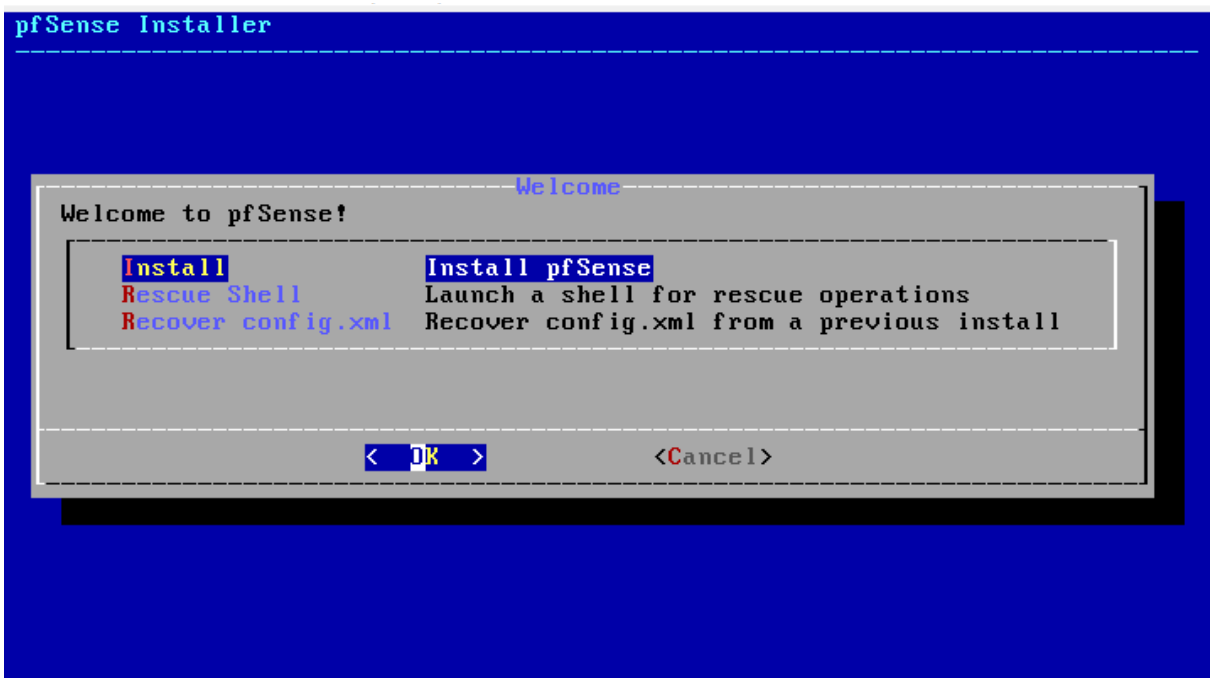
Nom : intrnet ▼

▼ 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

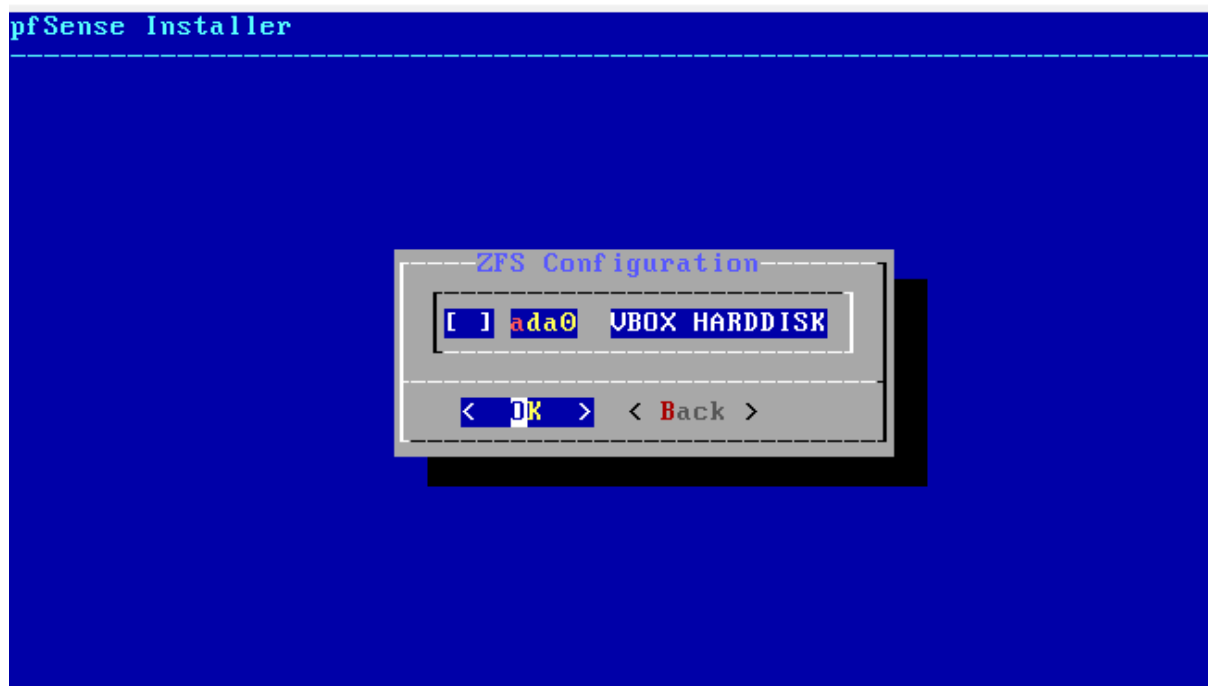
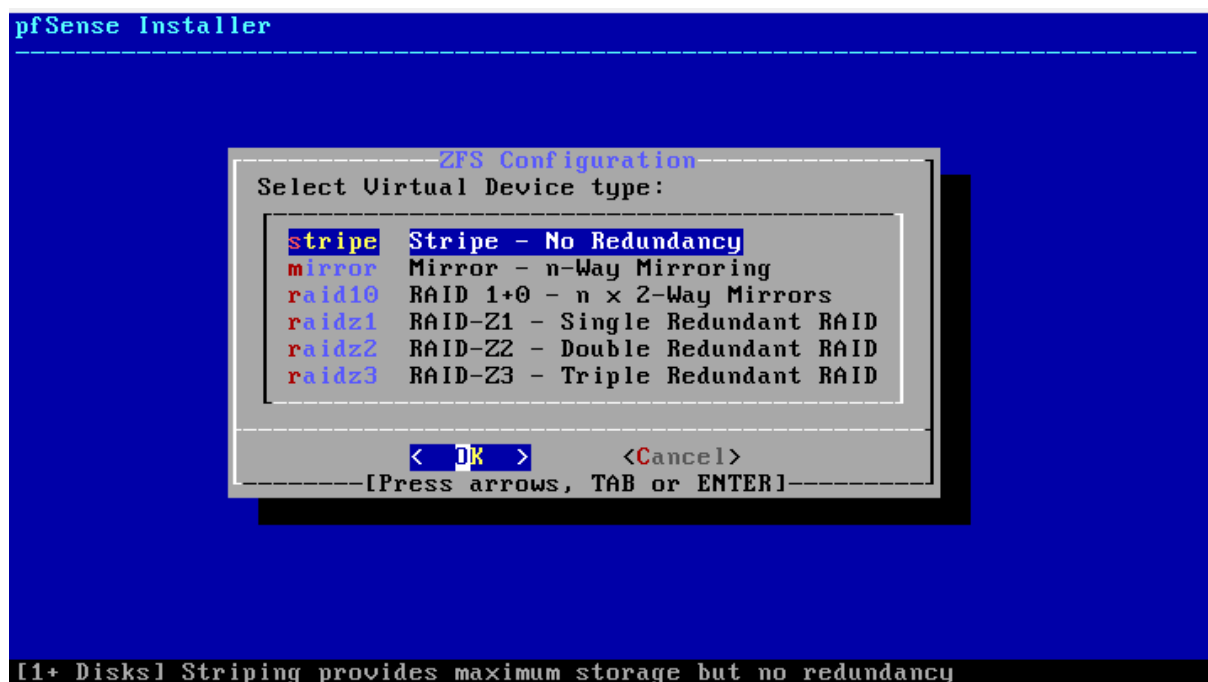
Configure Options:

>>> 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



Tapez espace pour cocher la case.

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%

pfSense Installer

Manual Configuration

The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?

< Yes >

< No >

pfSense Installer

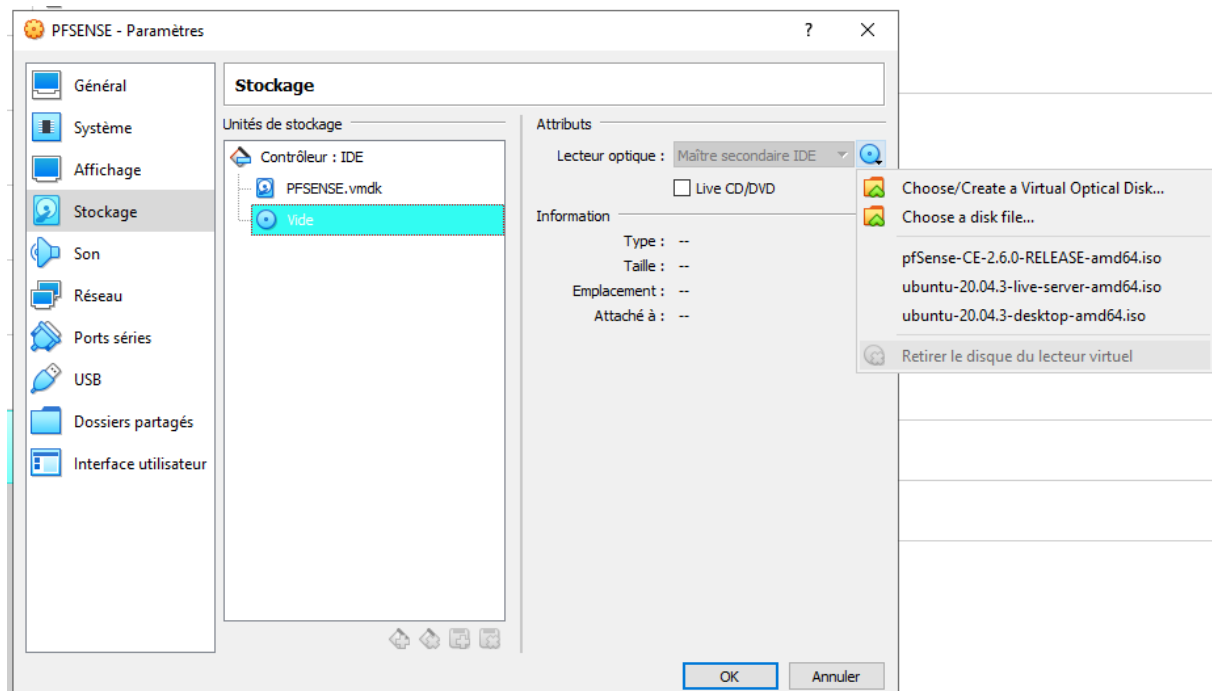
Complete

Installation of pfSense
complete! Would you like
to reboot into the
installed system now?

< Reboot >

< Shell >

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



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

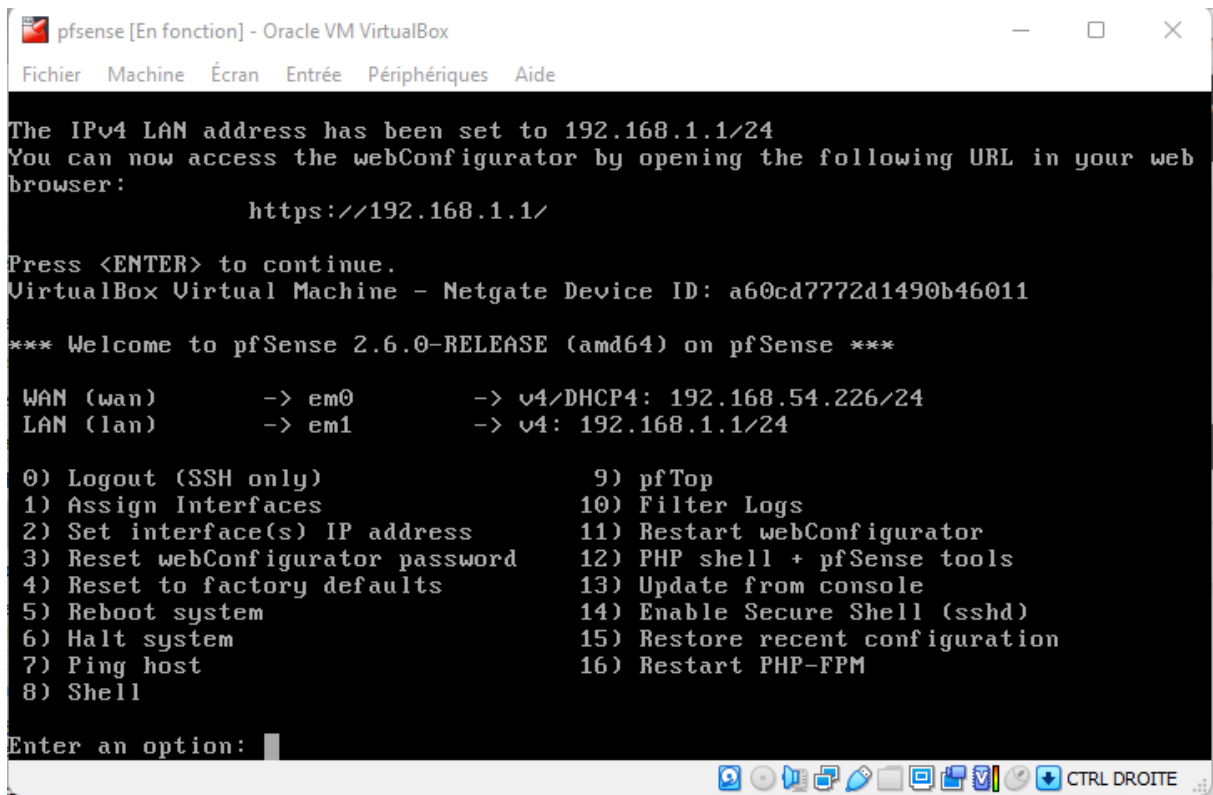
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable 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



```
pfsense [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

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

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: a60cd7772d1490b46011

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.54.226/24
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: 
```

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: 192.168.54.226/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
```


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 shows a Windows 10 virtual machine environment. A web browser is open to the pfSense Community Edition status page at <https://192.168.1.1>. The page features a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels:

- System Information:** A table providing details about the pfSense instance.

System Information	
Name	pfSense.home.arpa
User	admin@192.168.1.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: a60cd772d1490b46011
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 13:48:16 UTC 2022
CPU Type	Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
- Netgate Services And Support:** A panel detailing support options.

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
 - Visit Netgate.com

5) Règles Firewall

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 :

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 2 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	internet	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 *	*	*	*	*	*	none			

Add Add Delete Save Separator

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

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 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 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

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 / LAN

Floating

WAN

LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	13 / 181 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	internet	*	none			
<input type="checkbox"/>	0 / 11 KiB	IPv4 *	*	*	*	*	*	none			
<input type="checkbox"/>	0 / 0 B	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	

Add

Add

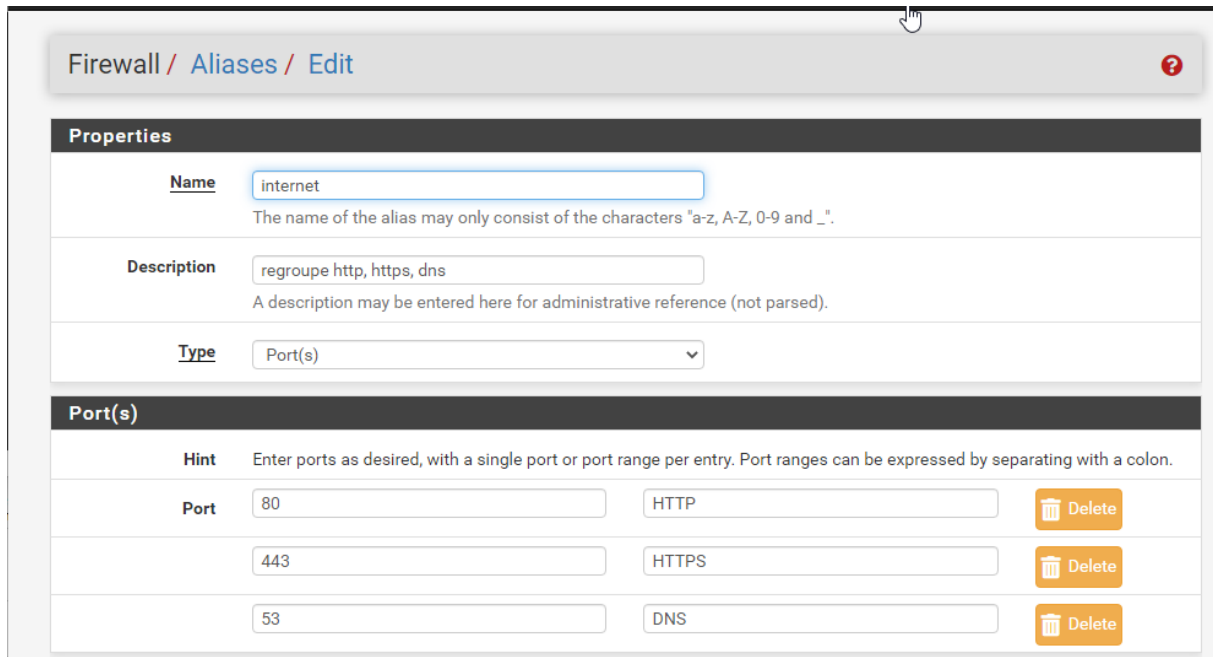
Delete

Save

Separator

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

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

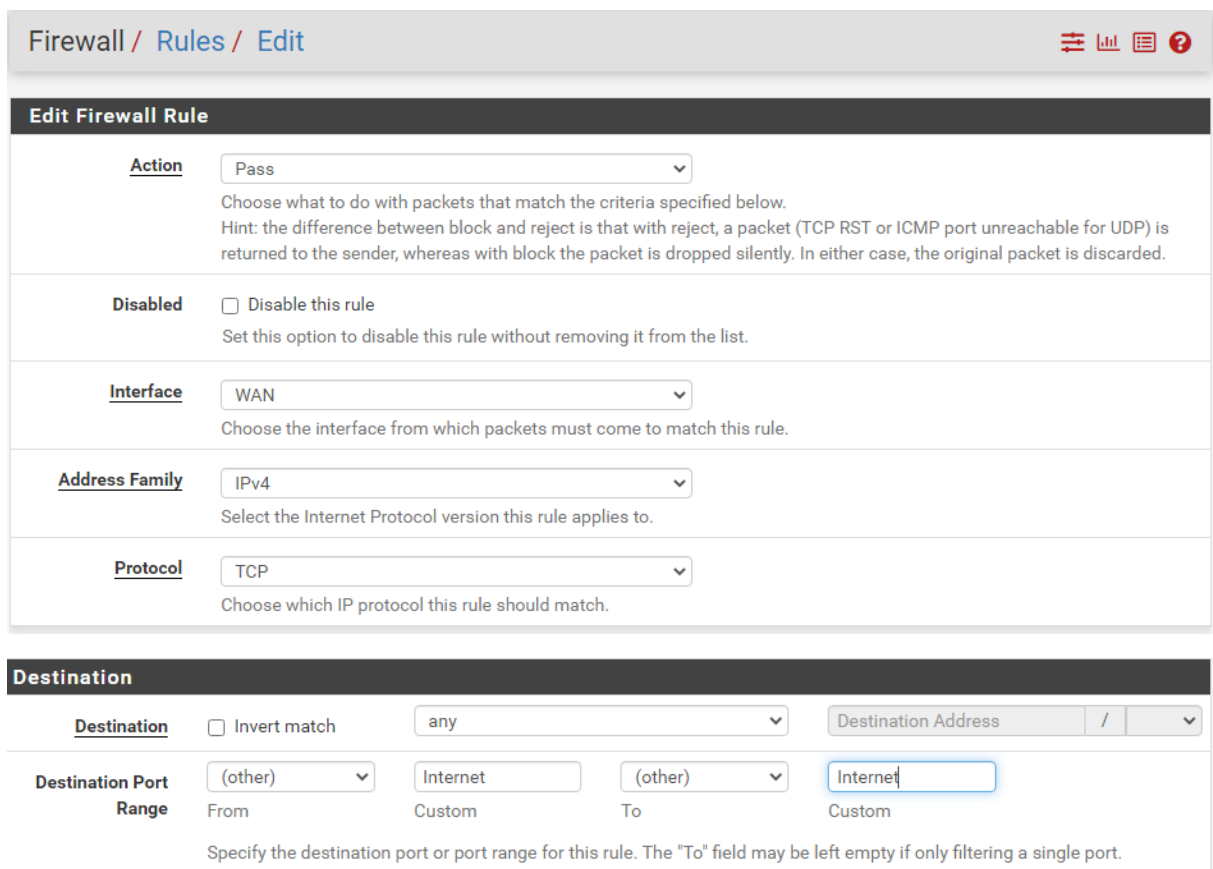
Type

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			
<input type="text" value="80"/>	<input type="text" value="HTTP"/>		Delete
<input type="text" value="443"/>	<input type="text" value="HTTPS"/>		Delete
<input type="text" value="53"/>	<input type="text" value="DNS"/>		Delete

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
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.

Destination



Destination ☐ Invert match /










Destination Port Range 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					  
Captive Portal Zones					
Zone	Interfaces	Number of users	Description	Actions	
PORTAIL	LAN	0	Portail captif	 	

System / User Manager / Groups					
Users Groups Settings Authentication Servers					
Groups					
Group name	Description	Member Count	Actions		
Agent	Delegation Creation Utilisateurs Portail	1	  		
admins	System Administrators	1	 		
all	All Users	2	 		
					 Add

System / User Manager / Users					
Users Groups Settings Authentication Servers					
Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	 robob	Agent autorisé a créer des utilisateurs du Portail Captif	✓	Agent	 
					 Add  Delete

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

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 Test		✓	Portail	 
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	 robrob	Agent autorisé a créer des utilisateurs du Portail Captif	✓	Agent	 

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