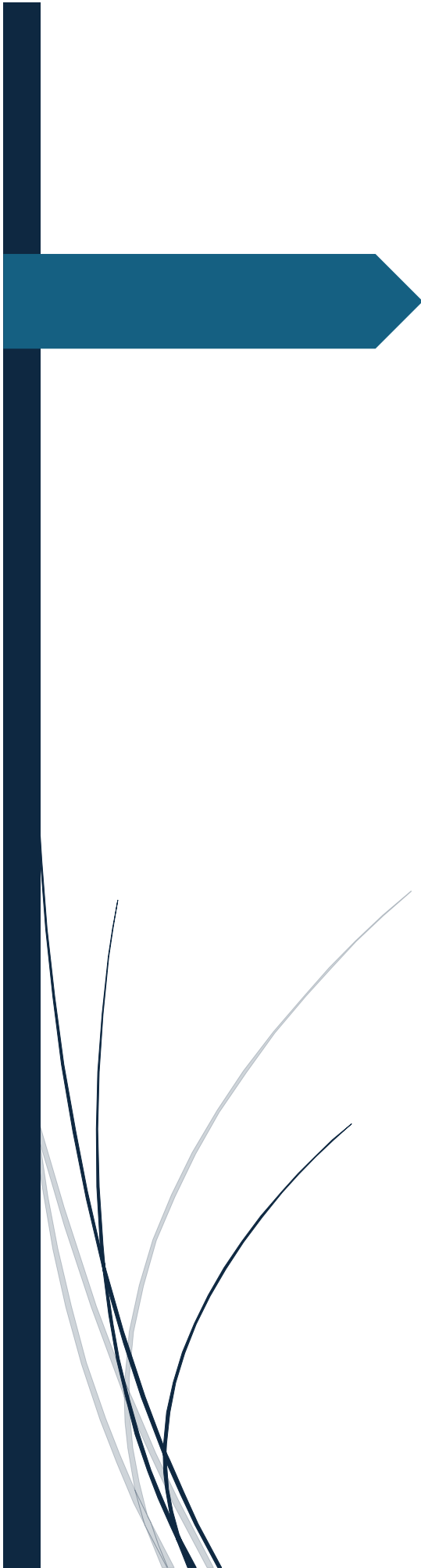


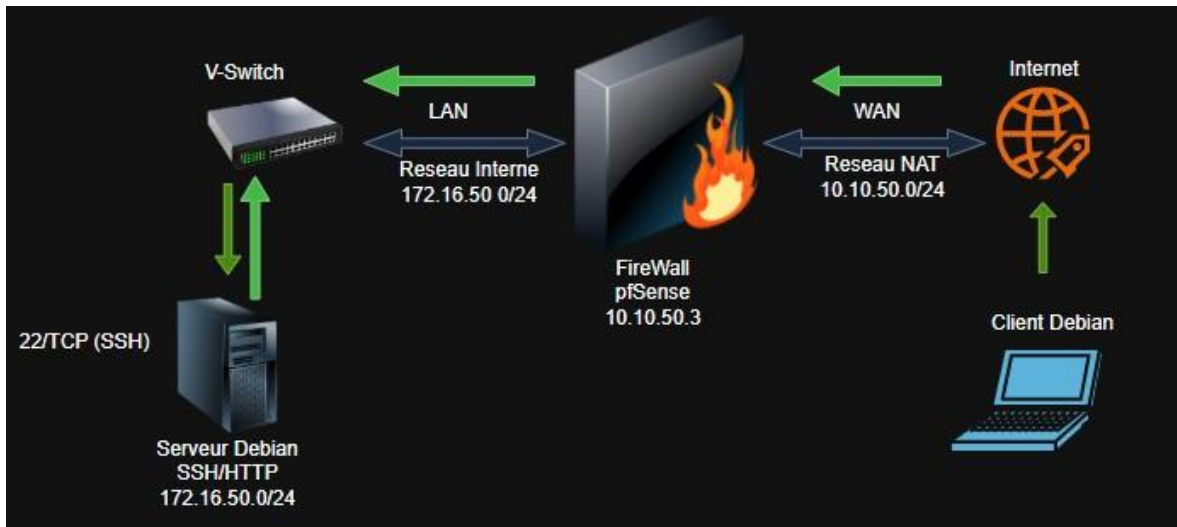


Pare-feu pfSense & Redirection

Paula Andrea Contreras Ovalle

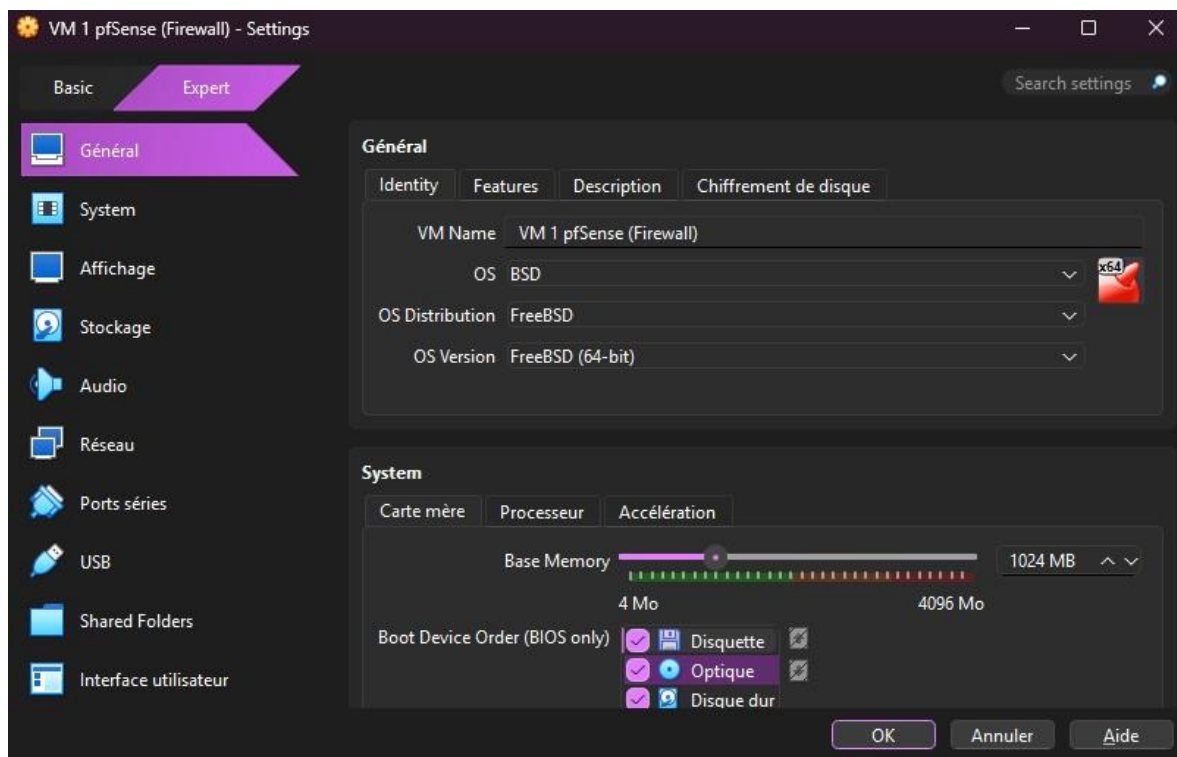
IRIS ECOLE SUPERIEURE D'INFORMATIQUE TOULOUSE

Schéma du LAB sur Draw.io :

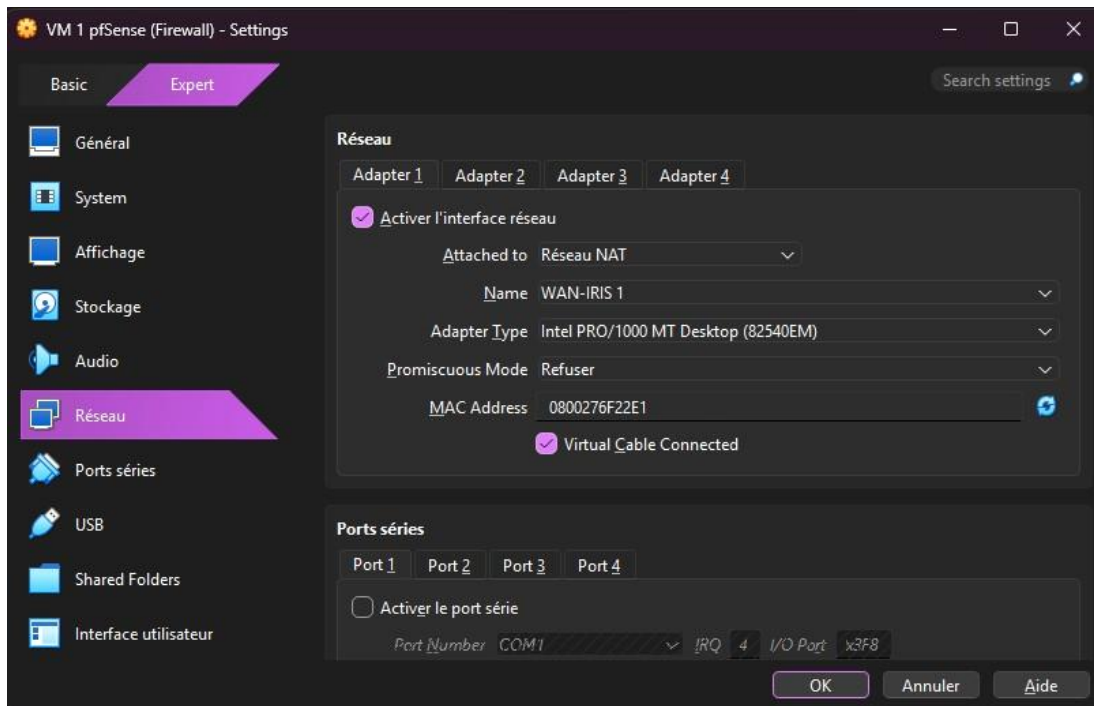


Configuration des réseaux :

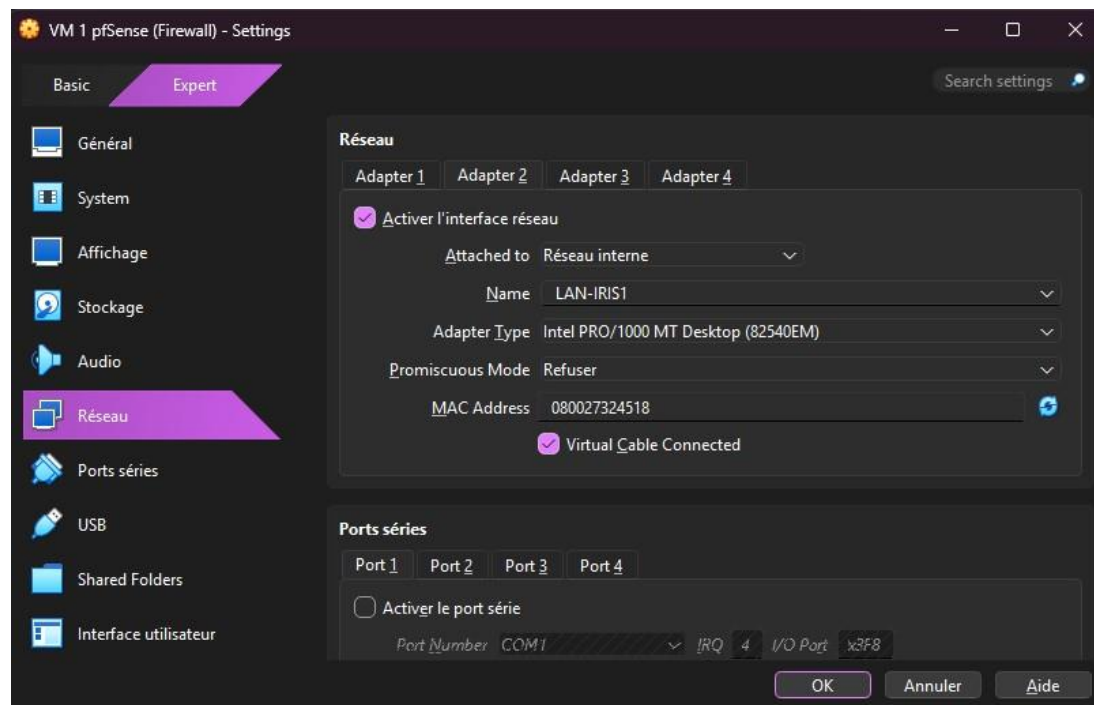
VM 1 – pfSense (Firewall)



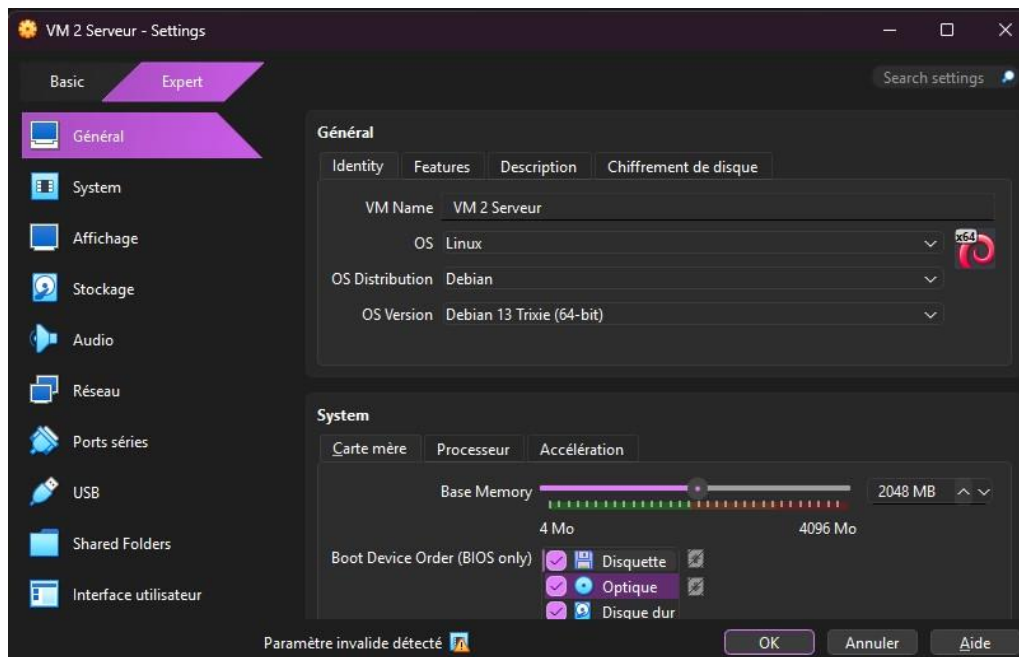
Reseau Adapter 1 :



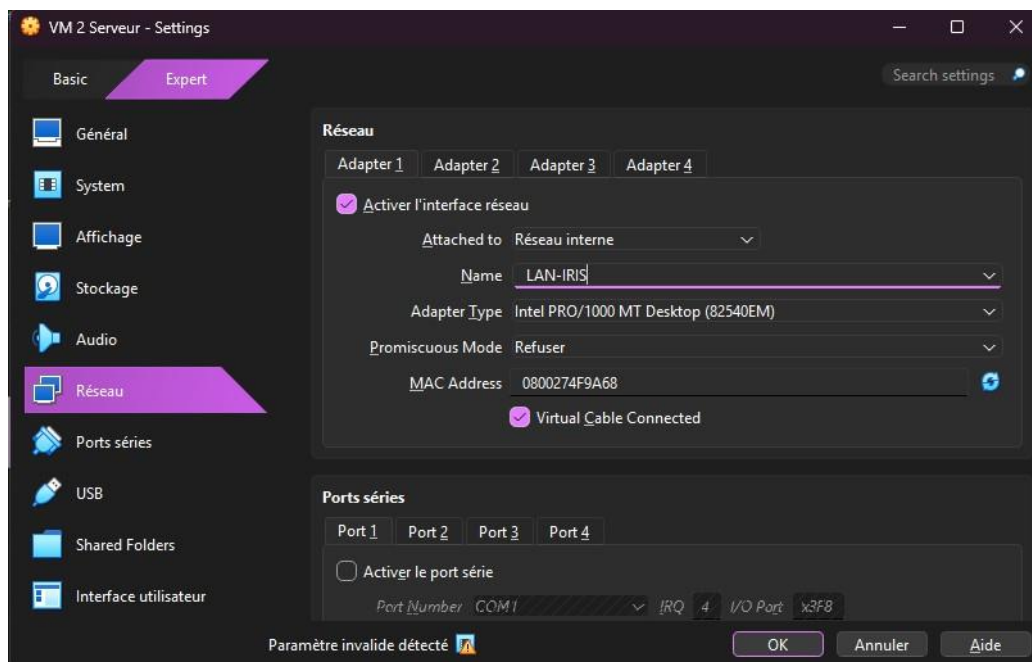
Reseau Adapter 2 :



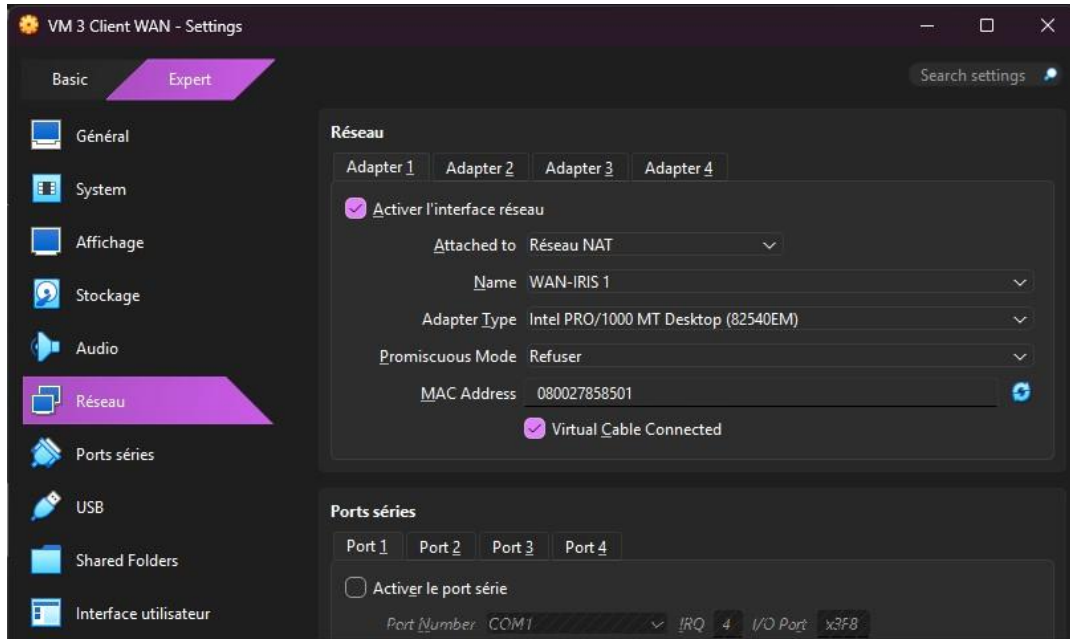
VM2 Serveur :



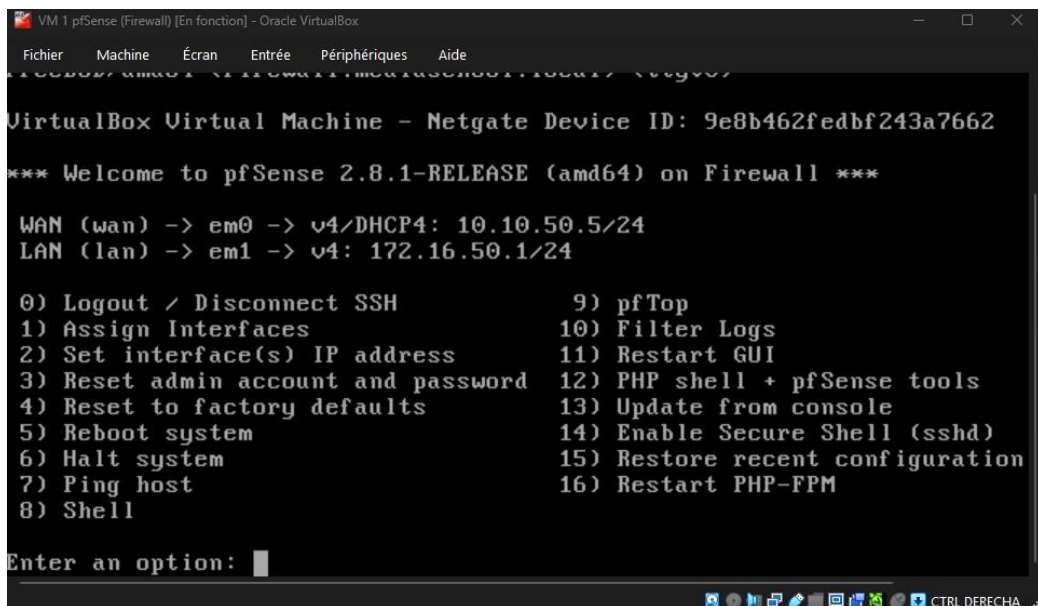
Réseau Adapter 1 :



VM3 Client WAN :



Étape 2 – Installation et configuration de pfSense :

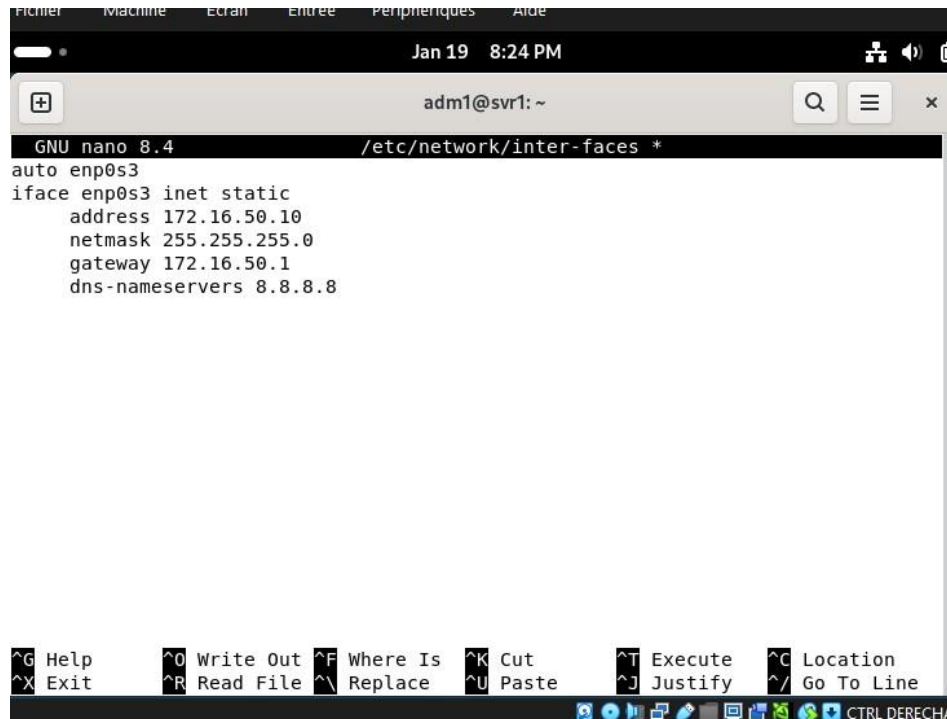


Étape 3 – Configuration du serveur Linux (Debian)

Configuration réseau

Éditer le fichier réseau

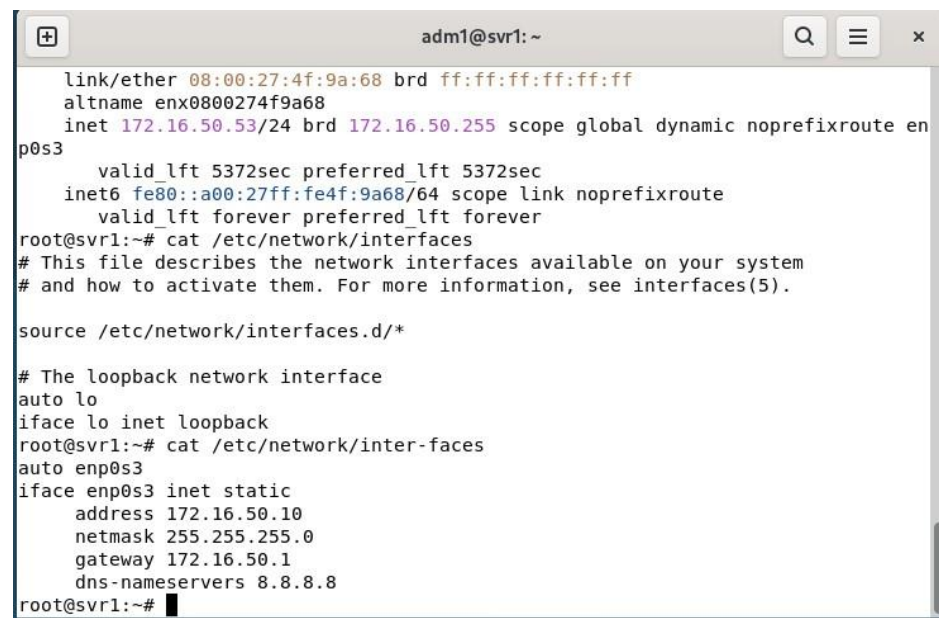
J'ai modifié les informations en utilisant la commande : `sudo nano /etc/network/interfaces`



```
GNU nano 8.4 /etc/network/interfaces *
auto enp0s3
iface enp0s3 inet static
    address 172.16.50.10
    netmask 255.255.255.0
    gateway 172.16.50.1
    dns-nameservers 8.8.8.8
```

The screenshot shows a terminal window with the nano text editor open. The file being edited is `/etc/network/interfaces`. The configuration for the `enp0s3` interface is set to static with IP `172.16.50.10`, netmask `255.255.255.0`, gateway `172.16.50.1`, and DNS servers `8.8.8.8`. The terminal window title is `adm1@svr1: ~` and the system clock shows `Jan 19 8:24 PM`.

On utilise la commande : `cat /etc/network/interfaces` pour vérifier si les informations ont changé.



```
link/ether 08:00:27:4f:9a:68 brd ff:ff:ff:ff:ff:ff
altname enx0800274f9a68
inet 172.16.50.53/24 brd 172.16.50.255 scope global dynamic noprefixroute en
p0s3
    valid_lft 5372sec preferred_lft 5372sec
    inet6 fe80::a00:27ff:fe4f:9a68/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
root@svr1:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
root@svr1:~# cat /etc/network/inter-faces
auto enp0s3
iface enp0s3 inet static
    address 172.16.50.10
    netmask 255.255.255.0
    gateway 172.16.50.1
    dns-nameservers 8.8.8.8
root@svr1:~#
```

The screenshot shows the output of the `cat /etc/network/interfaces` command. It displays the configuration for the `enp0s3` interface, including its MAC address, IPv4 address, and IPv6 address. The terminal window title is `adm1@svr1: ~`.

Installation d'Apache2

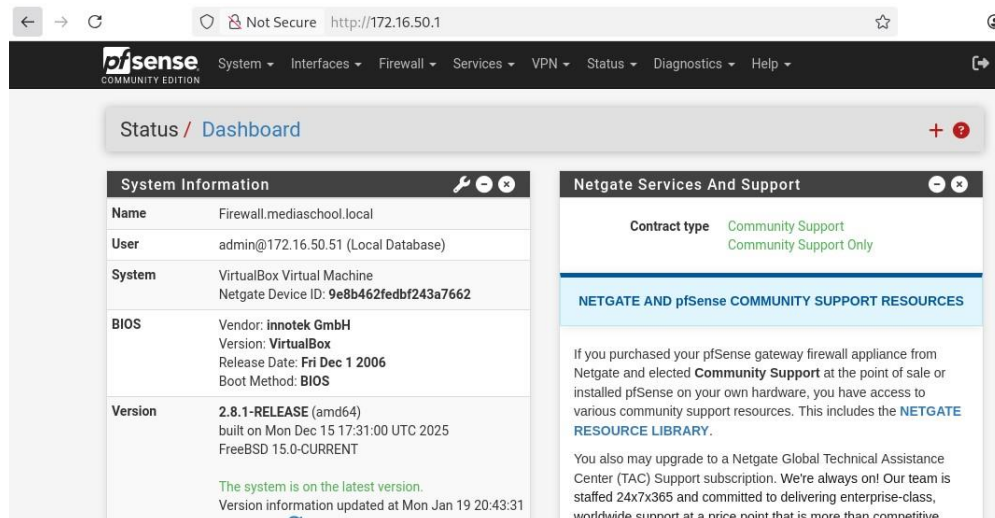
Pour réaliser l'installation, j'ai utilisé les commandes suivantes :

- ❶ **sudo apt update**
- ❷ **sudo apt install apache2 -y**
- ❸ **sudo systemctl status apache2.service**

```
adm1@svr1: ~  
111 packages can be upgraded. Run 'apt list --upgradable' to see them.  
root@svr1:~# sudo apt install apache2 -y  
apache2 is already the newest version (2.4.66-1-deb13u1).  
Summary:  
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 111  
root@svr1:~# sudo systemctl status apache2.service  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset:  
   Active: active (running) since Mon 2026-01-19 19:59:18 CET; 8min ago  
   Invocation: 95fd227342c2485d85971e858cea0d37  
     Docs: https://httpd.apache.org/docs/2.4/  
   Process: 987 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC  
   Main PID: 1373 (apache2)  
     Tasks: 55 (limit: 2282)  
    Memory: 7.4M (peak: 7.6M)  
       CPU: 299ms  
    CGroup: /system.slice/apache2.service  
            └─1373 /usr/sbin/apache2 -k start  
              └─1374 /usr/sbin/apache2 -k start  
                └─1375 /usr/sbin/apache2 -k start  
  
Jan 19 19:59:16 svr1 systemd[1]: Starting apache2.service - The Apache HTTP Ser  
Jan 19 19:59:18 svr1 systemd[1]: Started apache2.service - The Apache HTTP Ser  
lines 1-17/17 (END)
```

Étape 4 – Accès à l'interface Web pfSense

Depuis le serveur Linux : - Navigateur Web → <https://172.16.50.1>



Étape 5 – Autorisation du ping (ICMP) sur le WAN

pfSense
COMMUNITY EDITION

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

Firewall / Rules / 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

ICMP

Choose which IP protocol this rule should match.

ICMP Subtypes

any

Alternate Host
Datagram conversion error
Echo reply

For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source

☐ Invert match

Any

Source Address

/

Destination

Destination

☐ Invert match

WAN address

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

ALLOW-ICMP-WAN

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

Advanced Options

Display Advanced

Étape 6 – Redirection de ports (NAT)

Redirection SSH Firewall

Not Secure http://172.16.50.1/firewall_nat_edit.php?id=1 80% ☆

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source Display Advanced

Destination ☐ Invert match.

WAN address
Type

/
Address/mask

Destination port range Other

2222
From port

Other
To port

2222
Custom

Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.

Redirect target IP Address or Alias

172.16.50.10
Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4

Redirect target port SSH

Port Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description Port-SSH-NAT-rule

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

No XMLRPC Sync ☐ Do not automatically sync to other CARP members

This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Port-SSH-NAT-rule

[View the filter rule](#)

Redirection HTTP

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

☐ Disabled [Disable this rule](#)

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. WAN address Type Address/mask

Destination port range Other 8080 Other 8080
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Address or Alias 172.16.50.10
Type: Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4.
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port HTTP Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

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

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Filter rule association Rule NAT Redirection-HTTP
[View the filter rule](#)

Règles

pfSense COMMUNITY EDITION System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

Firewall / Rules / WAN

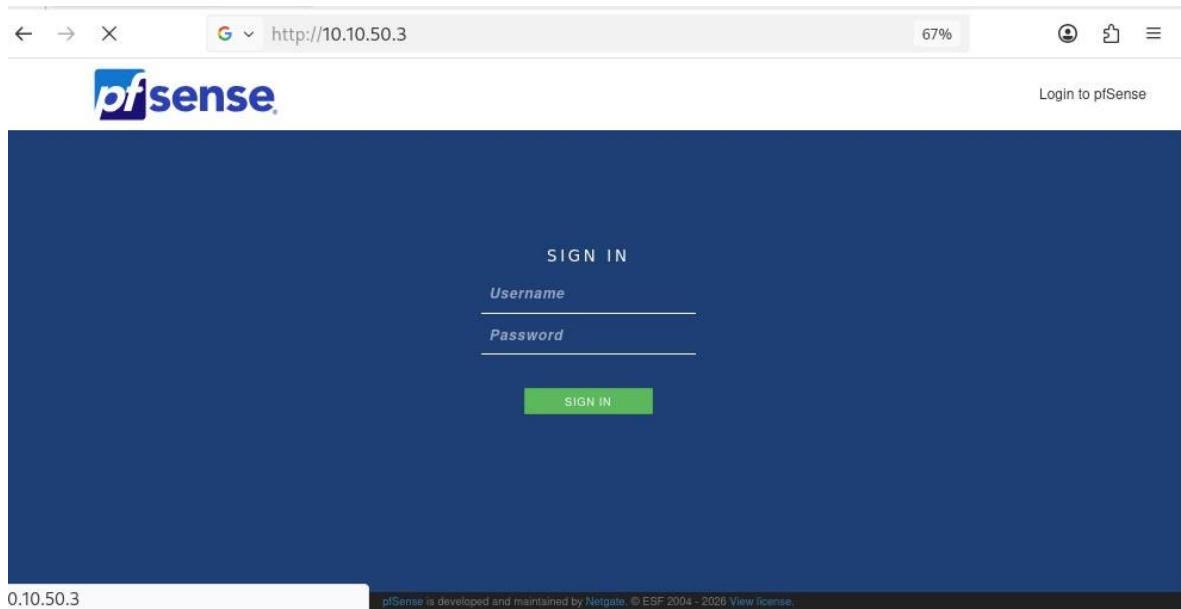
Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 TCP	*	*	172.16.50.10	22 (SSH)	*	none	NAT Port-SSH-NAT-rule	Anchor Edit Copy Delete X
☐	✓	0/0 B	IPv4 TCP	*	*	172.16.50.10	80 (HTTP)	*	none	NAT Redirection-HTTP	Anchor Edit Copy Delete X
☐	✓	0/0 B	IPv4 ICMP	*	*	WAN address	*	*	none	ALLOW-ICMP-WAN	Anchor Edit Copy Delete X

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separation](#)

Étape 7 – Test depuis le client WAN



Fin.