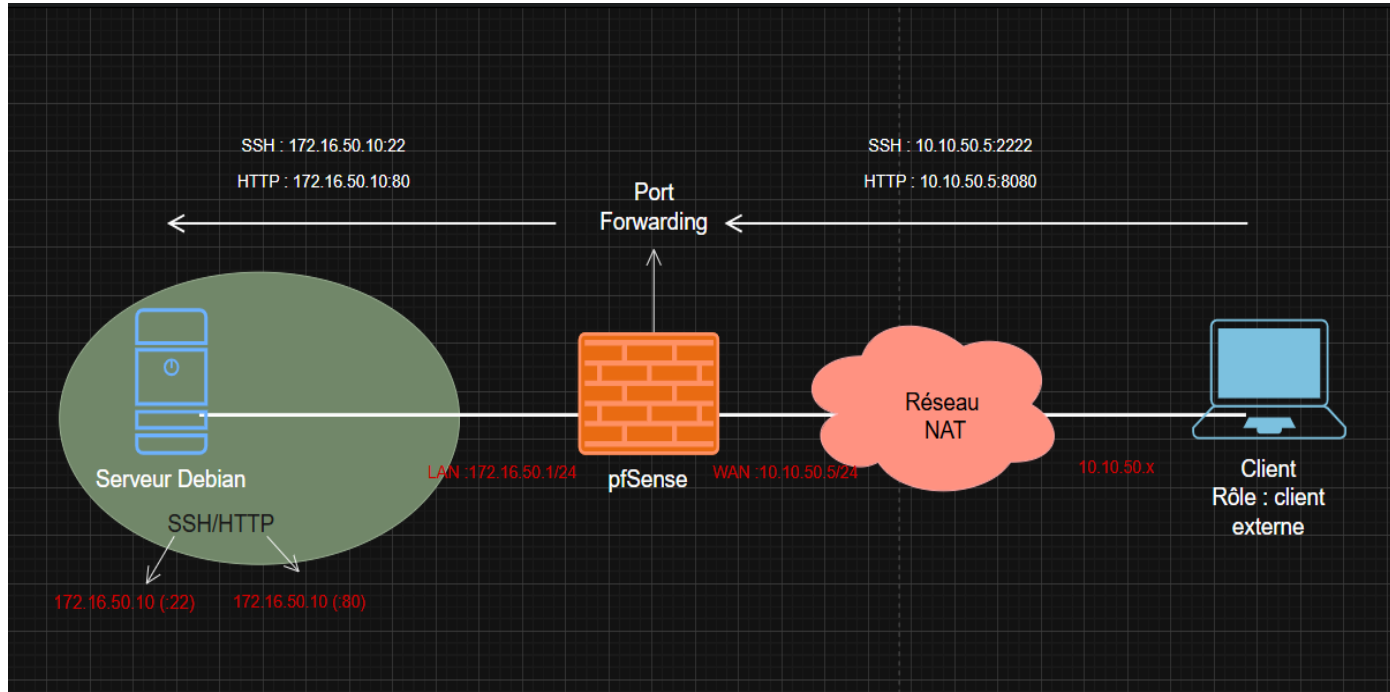


TP pfSense : Redirection de ports

Schéma du lab



Etape 1 et 2 :

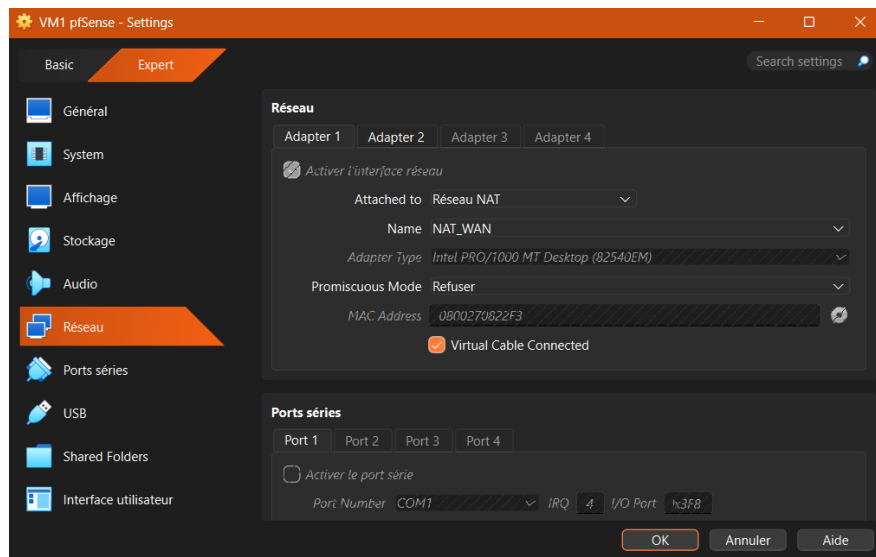
Réseau NAT_WAN :

Host-only Networks NAT Networks Cloud Networks			
Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NAT_WAN	10.10.50.0/24	fd17:625c:f037:a32::/64	Enabled

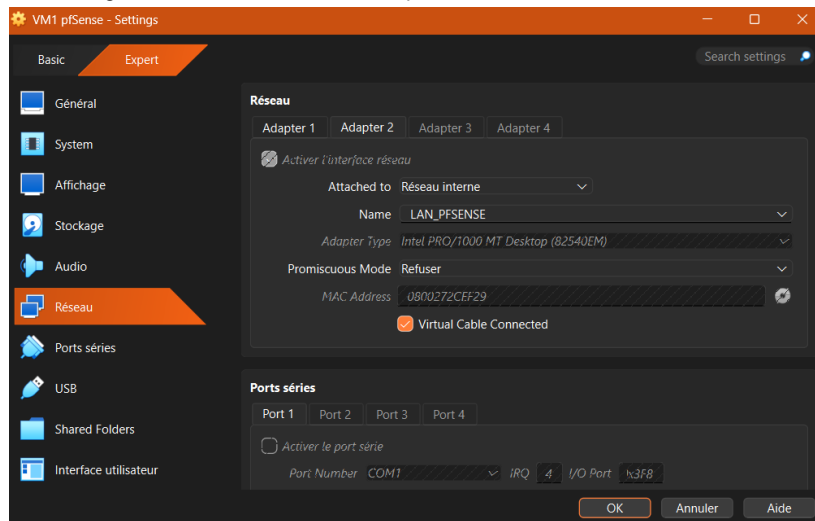
General Options	Redirection de ports
Nom :	NAT_WAN
IPv4 Prefix:	10.10.50.0/24
	☒ Enable DHCP

Configuration du réseau NAT_WAN (WAN) avec DHCP activé

VM1 pfSense (Firewall) :

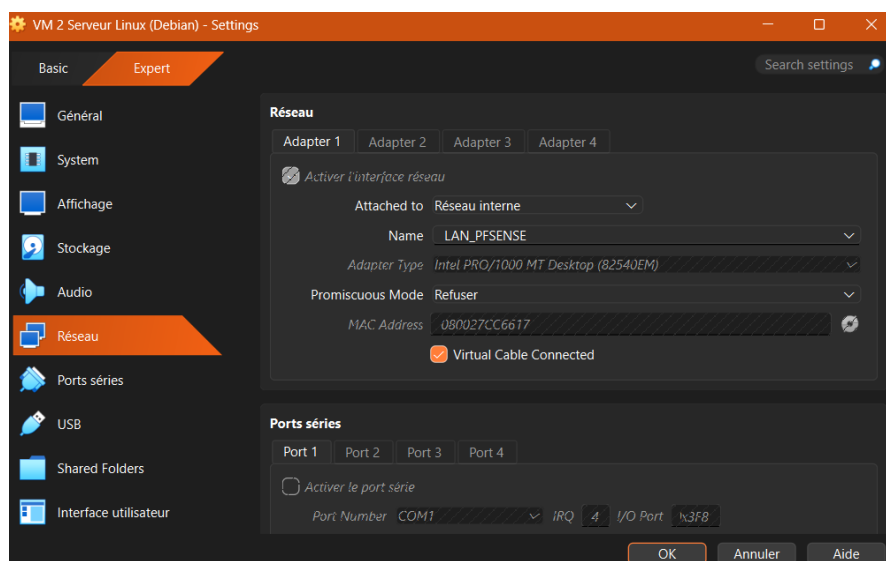


Paramétrage de l'interface WAN de la VM pfSense



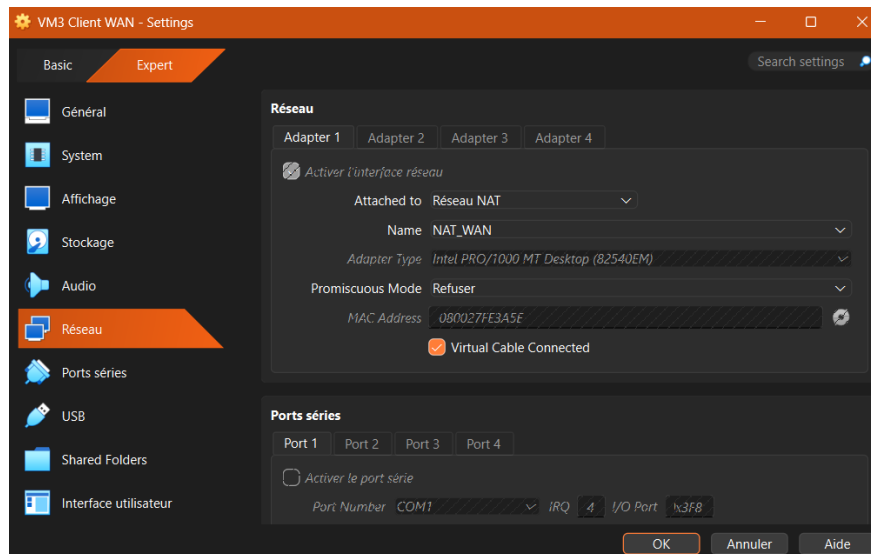
Paramétrage de l'interface LAN de la VM pfSense

VM2 Serveur Linux :



Configuration réseau du serveur Debian dans le LAN

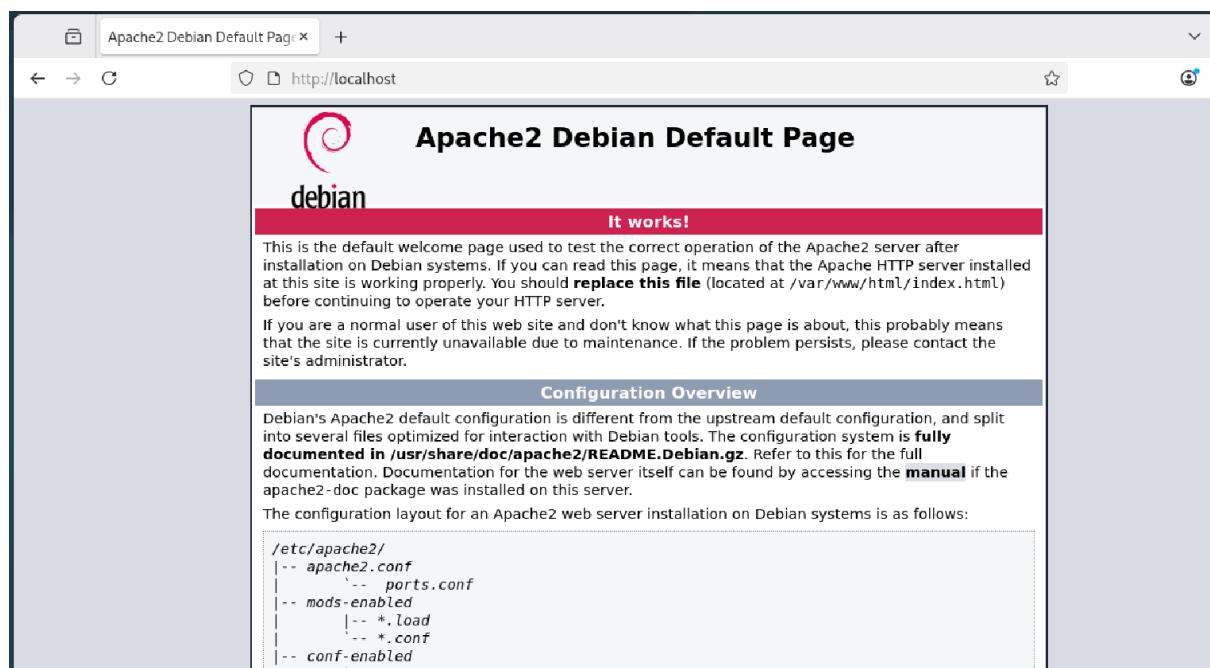
VM3 Client WAN :



Configuration réseau du client WAN

[Etape 3 :](#)

Configuration Apache :



```
ludivine@srv1: ~  
ludivine@srv1:~$ su -  
Password:  
root@srv1:~# systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: ▶  
   Active: active (running) since Sat 2026-01-17 16:31:24 CET; 26min ago  
  Invocation: 4ec4d10a6e4e49a1babc8b2c2cf1a80a  
     Docs: https://httpd.apache.org/docs/2.4/  
   Main PID: 16733 (apache2)  
     Tasks: 55 (limit: 2280)  
    Memory: 5M (peak: 5.5M)  
       CPU: 176ms  
    CGroup: /system.slice/apache2.service  
            └─16733 /usr/sbin/apache2 -k start  
              └─16735 /usr/sbin/apache2 -k start  
                └─16736 /usr/sbin/apache2 -k start  
  
Jan 17 16:31:24 srv1 systemd[1]: Starting apache2.service - The Apache HTTP Serv  
Jan 17 16:31:24 srv1 systemd[1]: Started apache2.service - The Apache HTTP Serv  
lines 1-16/16 (END)
```

Configuration SSH :

```
ludivine@srv1: ~  
root@srv1:~# systemctl status sshd.service  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)  
   Active: active (running) since Sat 2026-01-17 16:33:18 CET; 22s ago  
  Invocation: 8be09499ea6c417fa95c0200997ccc31  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
   Main PID: 23081 (sshd)  
     Tasks: 1 (limit: 2280)  
    Memory: 1.3M (peak: 2.1M)  
       CPU: 35ms  
    CGroup: /system.slice/ssh.service  
            └─23081 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Jan 17 16:33:18 srv1 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...  
Jan 17 16:33:18 srv1 sshd[23081]: Server listening on 0.0.0.0 port 22.  
Jan 17 16:33:18 srv1 sshd[23081]: Server listening on :: port 22.  
Jan 17 16:33:18 srv1 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.  
root@srv1:~# ip -a  
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }  
       ip [ -force ] -batch filename  
where  OBJECT := { address | addrlabel | fou | help | ila | ioam | l2tp | link |  
                  macsec | maddress | monitor | mptcp | mroute | mrule |  
                  neighbor | neighbour | netconf | netns | nexthop | ntable |
```

Configuration finale du serveur :

```
ludivine@srv1: ~  
ludivine@srv1:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr  
oup default qlen 1000  
    link/ether 08:00:27:cc:66:17 brd ff:ff:ff:ff:ff:ff  
    altname enx080027cc6617  
    inet 172.16.50.10/24 brd 172.16.50.255 scope global enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fecc:6617/64 scope link proto kernel_ll  
        valid_lft forever preferred_lft forever  
ludivine@srv1:~$
```

```
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr  
oup default qlen 1000  
    link/ether 08:00:27:cc:66:17 brd ff:ff:ff:ff:ff:ff  
    altname enx080027cc6617  
    inet 172.16.50.10/24 brd 172.16.50.255 scope global enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fecc:6617/64 scope link proto kernel_ll  
        valid_lft forever preferred_lft forever  
ludivine@srv1:~$ ip route  
default via 172.16.50.1 dev enp0s3 onlink  
172.16.50.0/24 dev enp0s3 proto kernel scope link src 172.16.50.10  
ludivine@srv1:~$ ip addr show enp0s3  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr  
oup default qlen 1000  
    link/ether 08:00:27:cc:66:17 brd ff:ff:ff:ff:ff:ff  
    altname enx080027cc6617  
    inet 172.16.50.10/24 brd 172.16.50.255 scope global enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fecc:6617/64 scope link proto kernel_ll  
        valid_lft forever preferred_lft forever  
ludivine@srv1:~$
```

[Etape 4 :](#)

Etape 5 :

Apache2 Debian Default Page x pfsense.mediaschoolloc: x +

← → ↻ Not Secure http://172.16.50.1/firewall_rules_edit.php?if=wan&after=-1 ☆ ⓘ ⌵

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	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.

Apache2 Debian Default Page x pfsense.mediaschoolloc: x +

← → ↻ Not Secure http://172.16.50.1/firewall_rules_edit.php?if=wan&after=-1 ☆ ⓘ ⌵

Datagram conversion error
Echo reply

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

Source

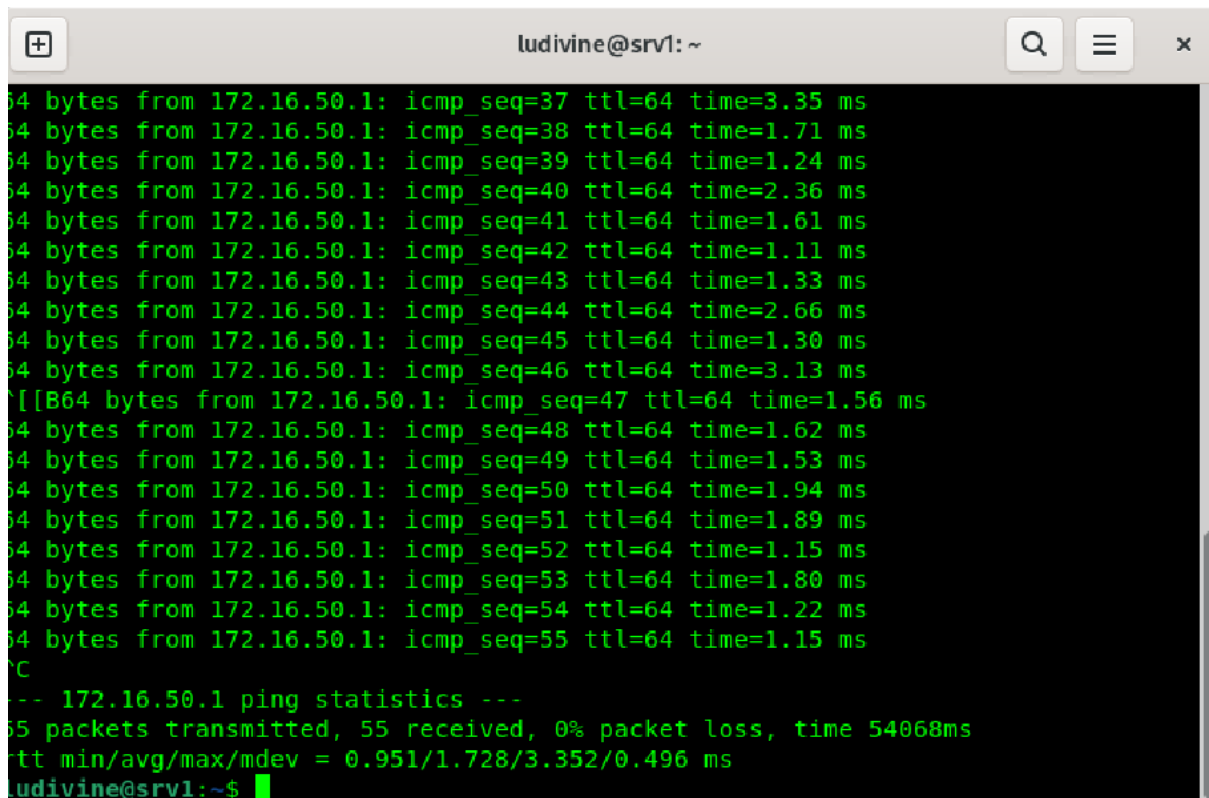
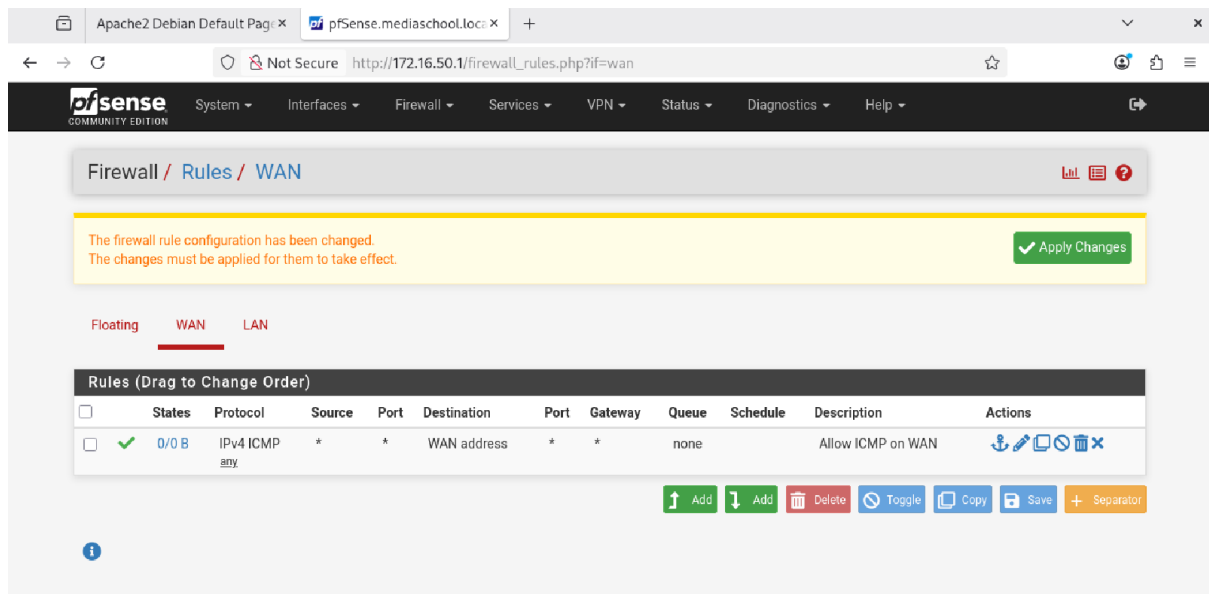
Source	☐ Invert match	Any	Source Address	/	
---------------	---------------------------------------	-----	----------------	---	--

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				



Etape 6 :

Redirection SSH :

pfSense.mediaschool.loc

Not Secure http://172.16.50.1/firewall_nat_edit.php?id=0

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

From port

2222

Custom

To port

Other

2222

Custom

pfSense.mediaschool.loc

Not Secure http://172.16.50.1/firewall_nat_edit.php?id=0

Destination port range

Other

2222

From port

Custom

Other

2222

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

Type

172.16.50.1

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

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-Forward-SSH

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

pfSense.mediaschool.local

Not Secure http://172.16.50.1/firewall_nat_edit.php?id=0

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-Forward-SSH
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-Forward-SSH
[View the filter rule](#)

Rule Information

Created	1/17/26 17:04:59 by admin@172.16.50.10 (Local Database)
Updated	1/17/26 17:04:59 by admin@172.16.50.10 (Local Database)

[Save](#)

Firewall / NAT / Port Forward

The NAT configuration has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

Port Forward 1:1 Outbound NPt

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	WAN	TCP	*	*	WAN address	2222	172.16.50.1	22 (SSH)	Port-Forward-SSH	Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Save](#) [Separator](#)

Redirection HTTP :

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

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

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

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

Source **Destination** ☐ Invert match.

Type

Destination port range

pfSense.mediaschool.local

+

Not Secure http://172.16.50.1/firewall_nat_edit.php?after=-1

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

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

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

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

Filter rule association

The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

pfSense.mediaschool.local

Not Secure http://172.16.50.1/firewall_nat_edit.php?after=-1

Enter the internal IP address or 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 Port-Forward-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 Add associated filter rule
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Save

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules										
	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	WAN	TCP	*	*	WAN address	8080	172.16.50.10	80 (HTTP)	Port-Forward-HTTP	
☐	WAN	TCP	*	*	WAN address	2222	172.16.50.1	22 (SSH)	Port-Forward-SSH	

Add
 Add
 Delete
 Toggle
 Save
 Separator

Etape 7 :

Test connexion SSH :

Avant de tester la connexion SSH chez le client je cherche mon adresse IPV4 WAN dans pfsense :

Status / Interfaces

WAN Interface (wan, em0)

Status	up
DHCP	up Release WAN ☐ Relinquish Lease
MAC Address	08:00:27:08:22:f3
IPv4 Address	10.10.50.5
Subnet mask IPv4	255.255.255.0
Gateway IPv4	10.10.50.1
IPv6 Link Local	fe80::a00:27ff:fe08:22f3%em0
DNS servers	192.168.1.254
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	294669/111640 (375.79 MiB/4.63 MiB)
In/out packets (pass)	294669/111640 (375.79 MiB/4.63 MiB)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0

LAN Interface (lan, em1)

Status	up
MAC Address	08:00:27:2c:ef:29
IPv4 Address	172.16.50.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe2c:ef29%em1
MTU	1500

Mon adresse IPv4 est 10.10.50.5

Le client WAN doit avoir une adresse IP; dans un premier temps je fais les mises à jour puis j'installe le logiciel pour qu'une adresse IP lui soit donnée :

```
ludivine@srv1: ~  
ludivine@srv1:~$ sudo dhclient -v enp0s3  
[sudo] password for ludivine:  
Sorry, try again.  
[sudo] password for ludivine:  
ludivine is not in the sudoers file.  
ludivine@srv1:~$ su -  
Password:  
root@srv1:~# sudi dhclient -v enp0s3  
-bash: sudi: command not found  
root@srv1:~# sudo dhclient -v enp0s3  
sudo: dhclient: command not found  
root@srv1:~# apt update  
Hit:1 http://security.debian.org/debian-security trixie-security InRelease  
Hit:2 http://debian.univ-tlse2.fr/debian trixie InRelease  
Hit:3 http://debian.univ-tlse2.fr/debian trixie-updates InRelease  
111 packages can be upgraded. Run 'apt list --upgradable' to see them.  
root@srv1:~# apt install isc-dhcp-client -y  
Installing:  
  isc-dhcp-client  
  
Installing dependencies:  
  isc-dhcp-common  
  
Suggested packages:
```

```
ludivine@srv1: ~  
root@srv1:~# dhclient -v enp0s3  
Internet Systems Consortium DHCP Client 4.4.3-P1  
Copyright 2004-2022 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
  
Listening on LPF/enp0s3/08:00:27:fe:3a:5e  
Sending on   LPF/enp0s3/08:00:27:fe:3a:5e  
Sending on   Socket/fallback  
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 5  
DHCPOFFER of 10.10.50.3 from 10.10.50.2  
DHCPREQUEST for 10.10.50.3 on enp0s3 to 255.255.255.255 port 67  
DHCPACK of 10.10.50.3 from 10.10.50.2  
bound to 10.10.50.3 -- renewal in 299 seconds.  
root@srv1:~# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
```

```
ludivine@srv1: ~  
DHCPOFFER of 10.10.50.3 from 10.10.50.2  
DHCPREQUEST for 10.10.50.3 on enp0s3 to 255.255.255.255 port 67  
DHCPACK of 10.10.50.3 from 10.10.50.2  
bound to 10.10.50.3 -- renewal in 299 seconds.  
root@srv1:~# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:fe:3a:5e brd ff:ff:ff:ff:ff:ff  
    altname enx080027fe3a5e  
    inet 10.10.50.4/24 brd 10.10.50.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 518sec preferred_lft 518sec  
    inet 10.10.50.3/24 brd 10.10.50.255 scope global secondary dynamic enp0s3  
        valid_lft 593sec preferred_lft 593sec  
    inet6 fe80::a00:27ff:fe3a:5e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
root@srv1:~#
```

Son adresse IP lui a été donnée (10.10.50.4/24)

Je me suis rendue compte que je n'avais pas créé d'utilisateur. J'en ai créé un sur le serveur avec un mot de passe puis le test peut être fait :

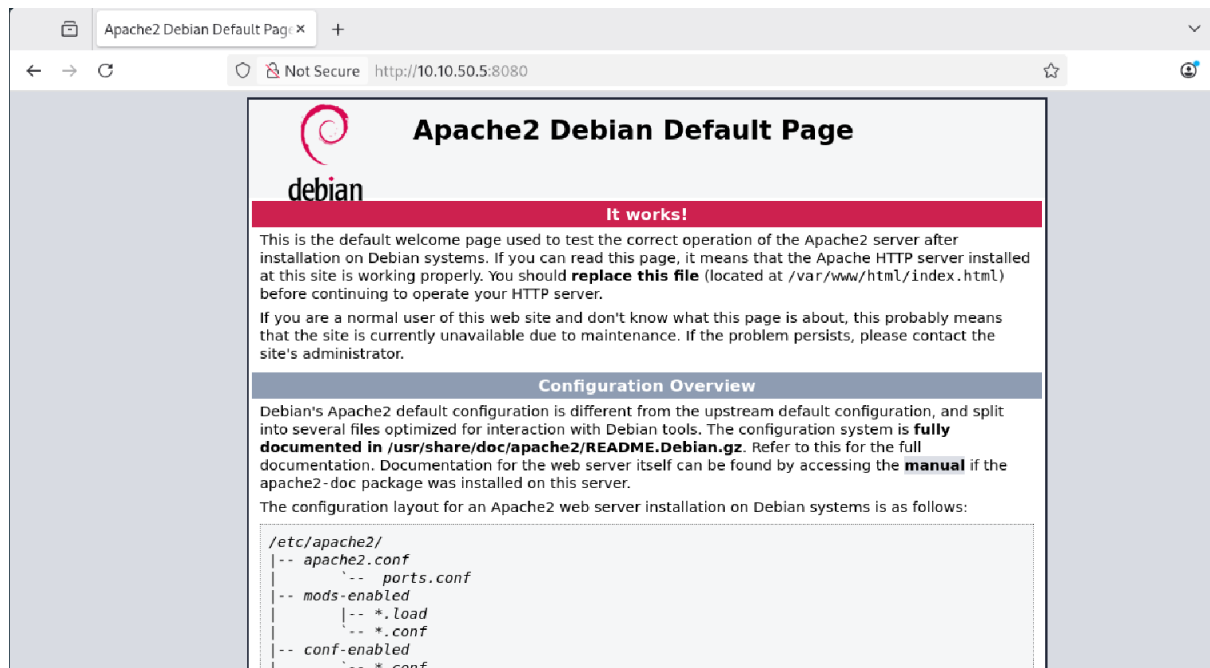
```
ludivine@srv1:~$ su -
Password:
root@srv1:~# id user1
id: 'user1': no such user
root@srv1:~# adduser user1
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user1
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
root@srv1:~# id user1
uid=1001(user1) gid=1001(user1) groups=1001(user1),100(users)
root@srv1:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab
   Active: active (running) since Sat 2026-01-17 20:32:59 CET; 22min ago
   Invocation: 26d0d6ebf35a4f86bb25e126f3c682fb
   Docs: man:sshd(8)
```

```
user1@srv1:~$ ssh user1@10.10.50.5
Permission denied, please try again.
user1@10.10.50.5's password:
Permission denied, please try again.
user1@10.10.50.5's password:
Connection closed by 10.10.50.5 port 2222
ludivine@srv1:~$ ssh user1@10.10.50.5 -p 2222
user1@10.10.50.5's password:
Permission denied, please try again.
user1@10.10.50.5's password:
Permission denied, please try again.
user1@10.10.50.5's password:
user1@10.10.50.5: Permission denied (publickey,password).
ludivine@srv1:~$ ssh user1@10.10.50.5 -p 2222
user1@10.10.50.5's password:
Linux srv1 6.12.63+deb13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.12.63-1 (2025-12-
30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user1@srv1:~$
```

Test connexion HTTP :



[Bonus :](#)