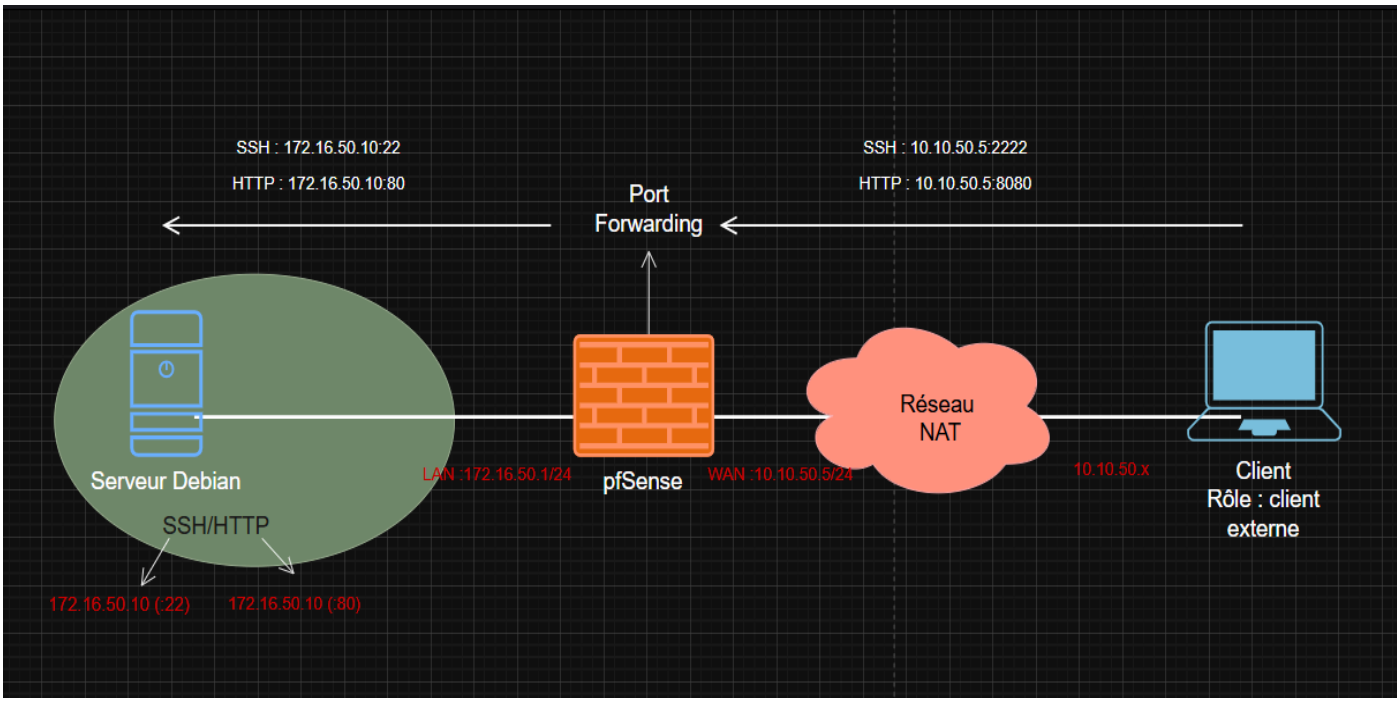
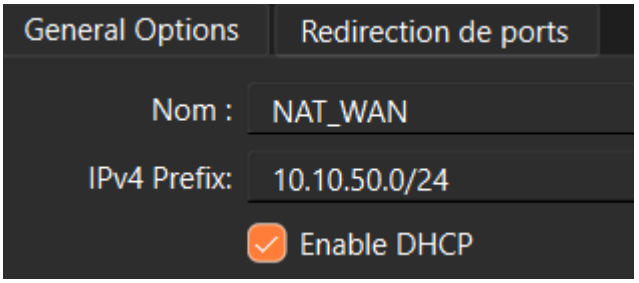
TP pfSense : Redirection de ports

Schéma du lab



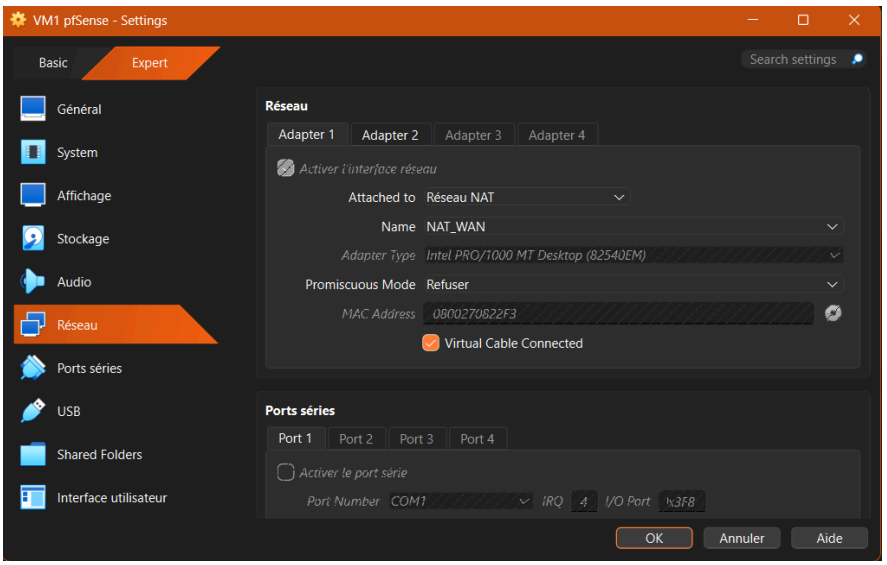
Etape 1 et 2 :

Réseau NAT_WAN :

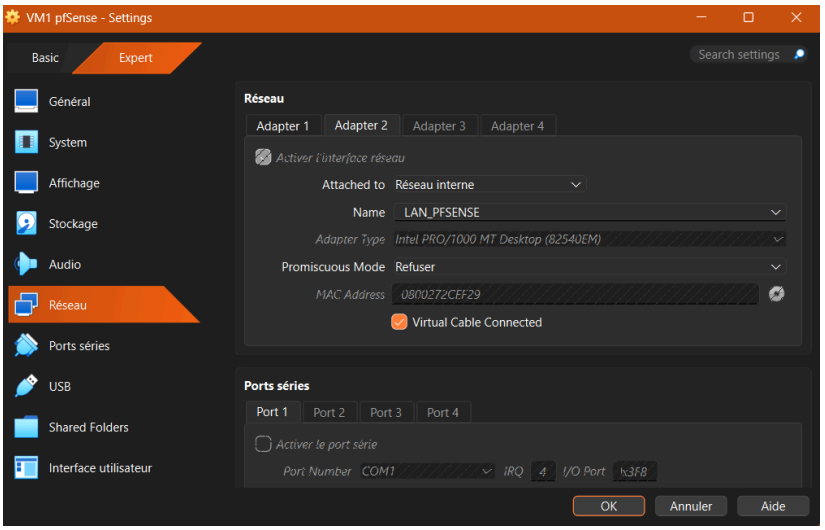


Configuration du réseau NAT_WAN (WAN) avec DHCP activé

VM1 pfSense (Firewall) :

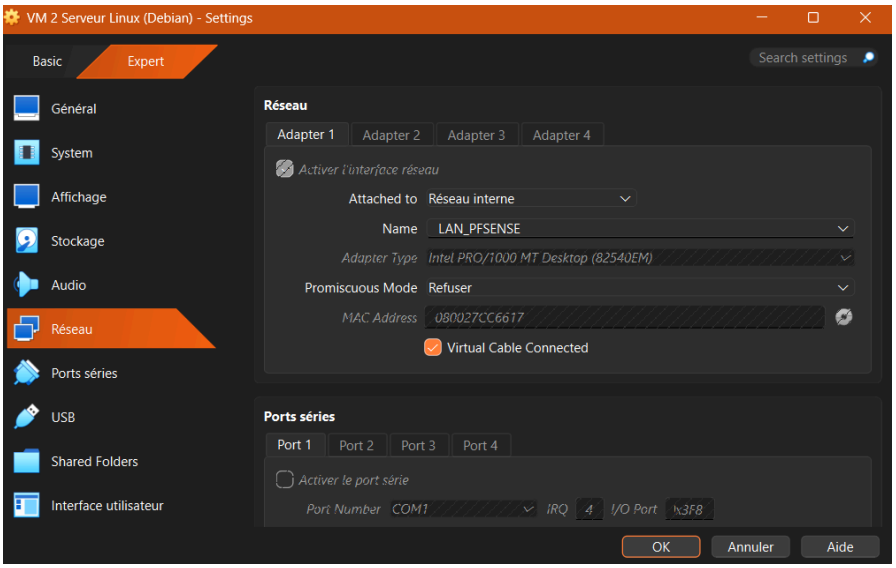


Paramétrage de l'interface WAN de la VM pfSense



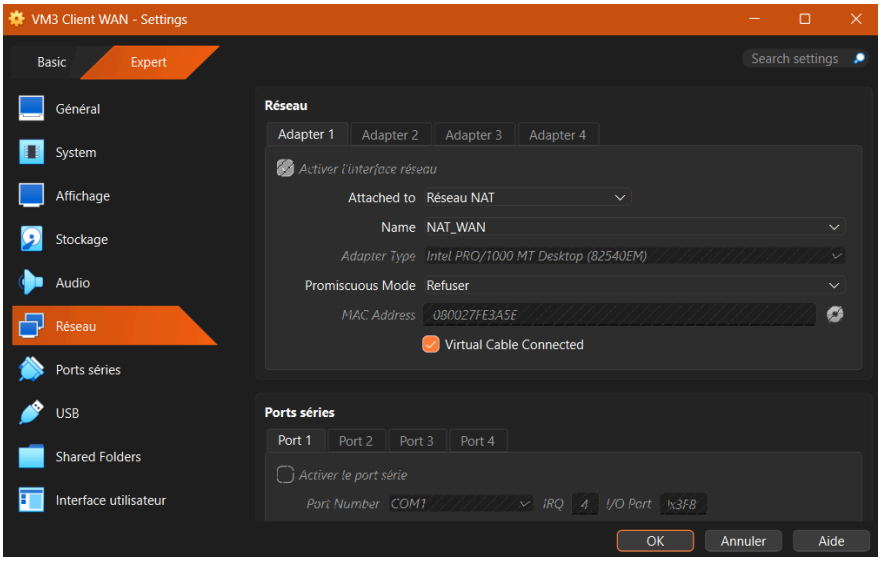
Paramétrage de l'interface LAN de la VM pfSense

VM2 Serveur Linux :



Configuration réseau du serveur Debian dans le LAN

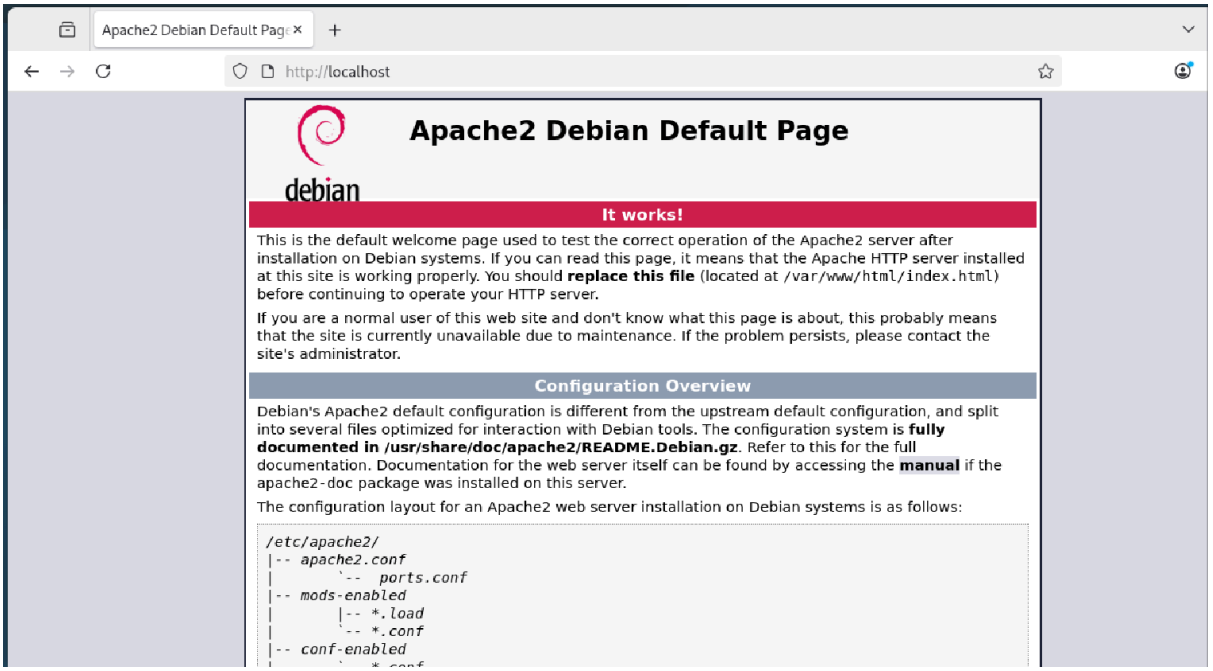
VM3 Client WAN :

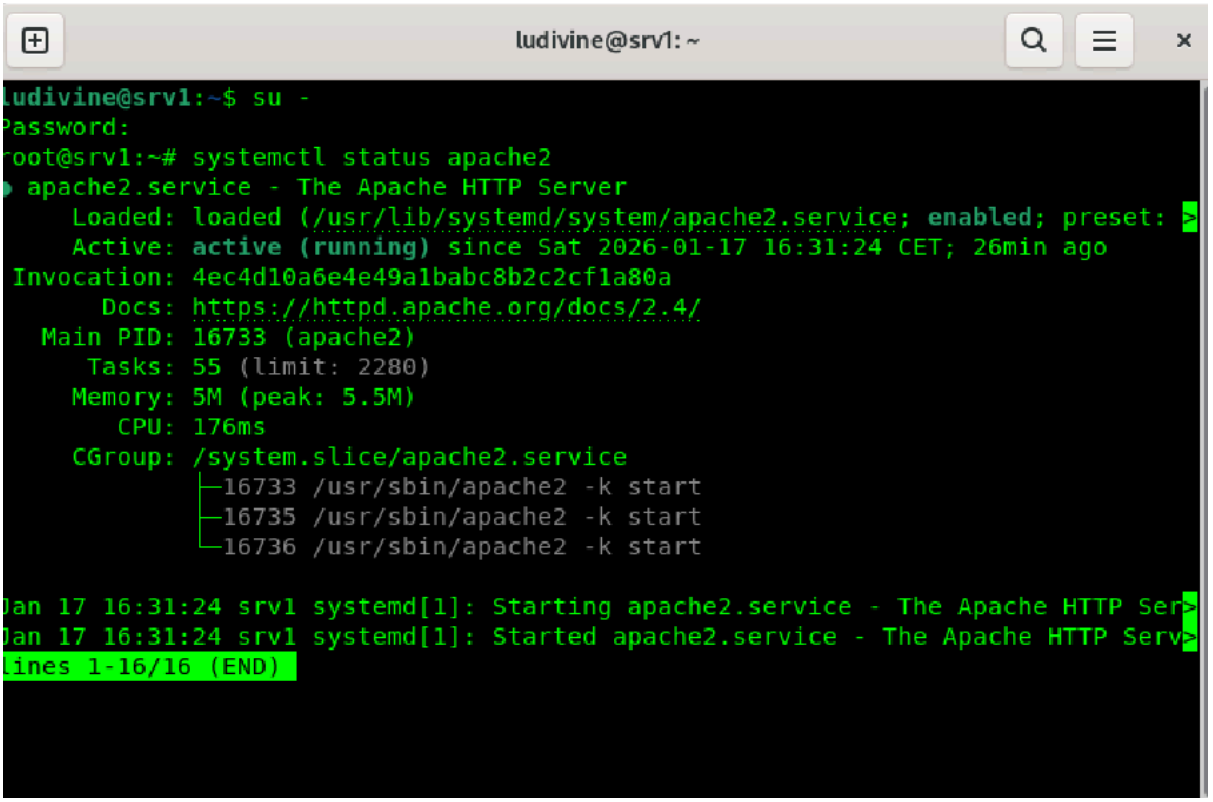


Configuration réseau du client WAN

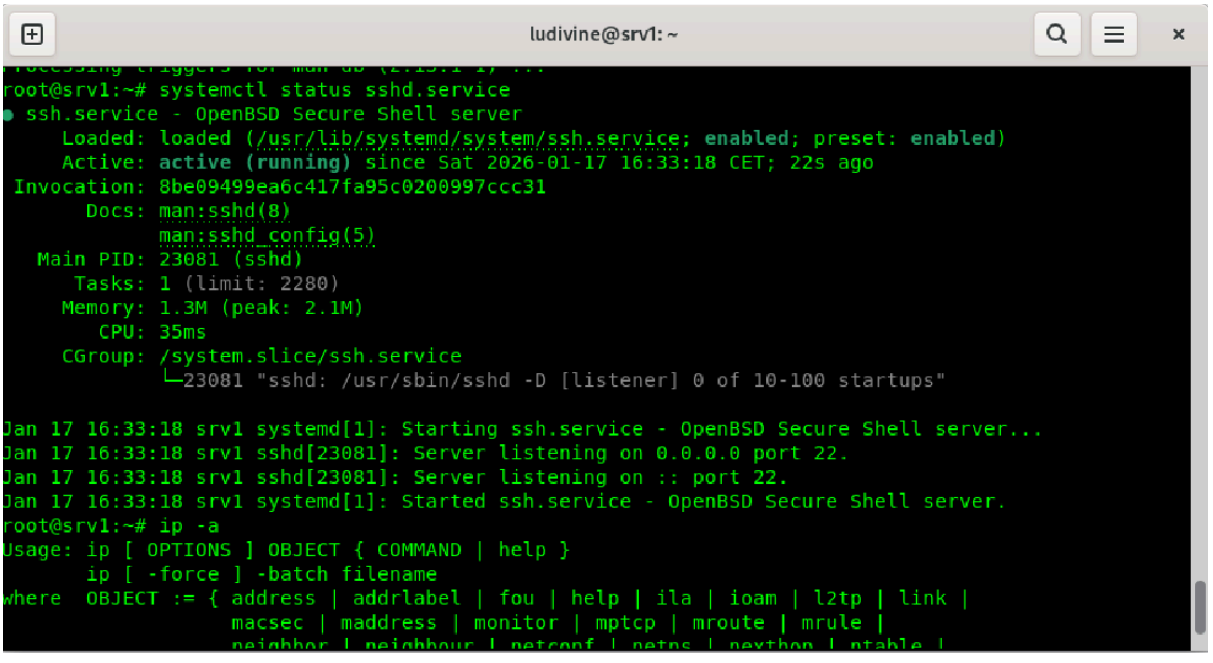
Etape 3 :

Configuration Apache :

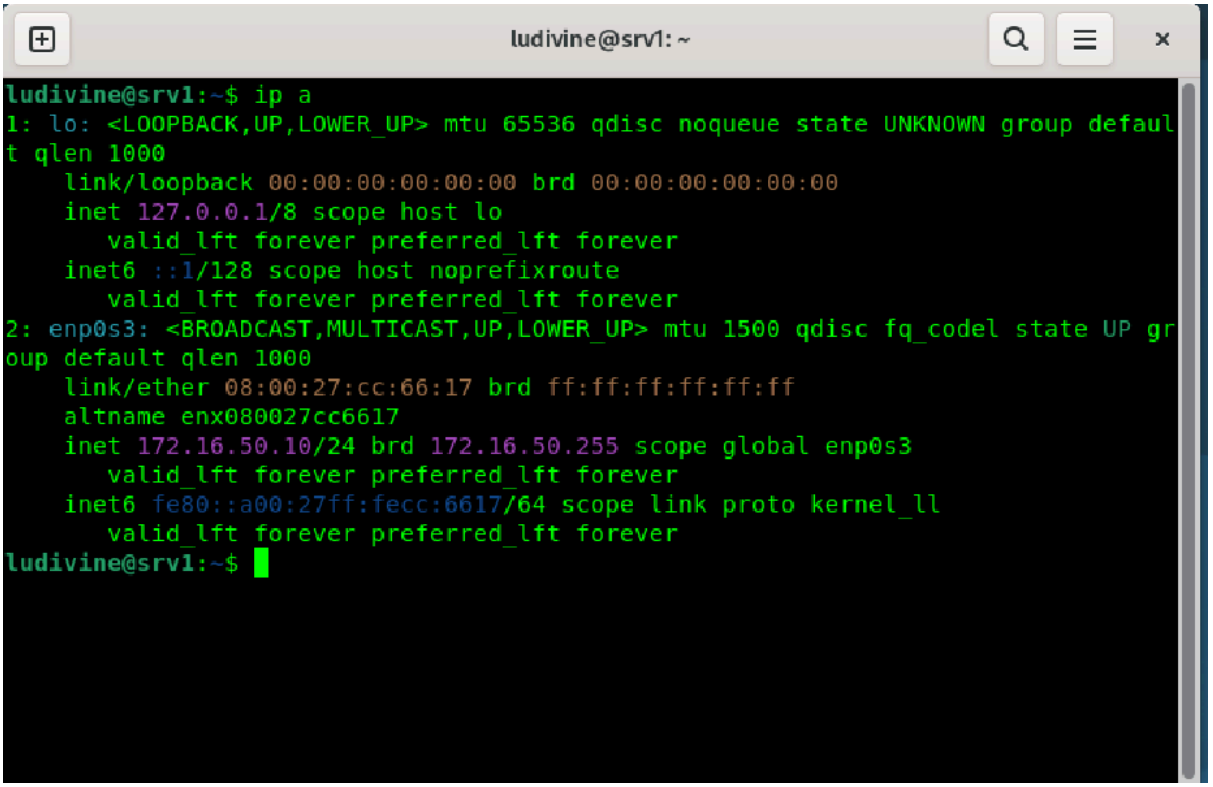


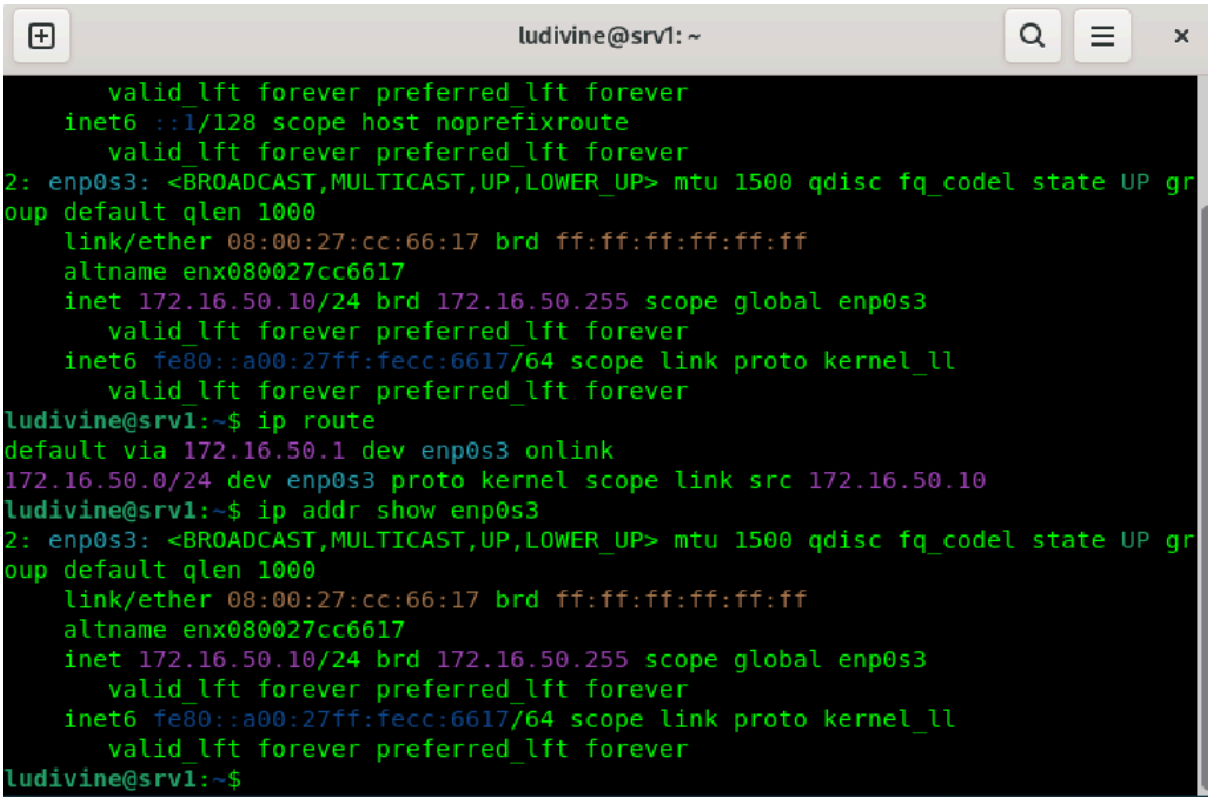


Configuration SSH :



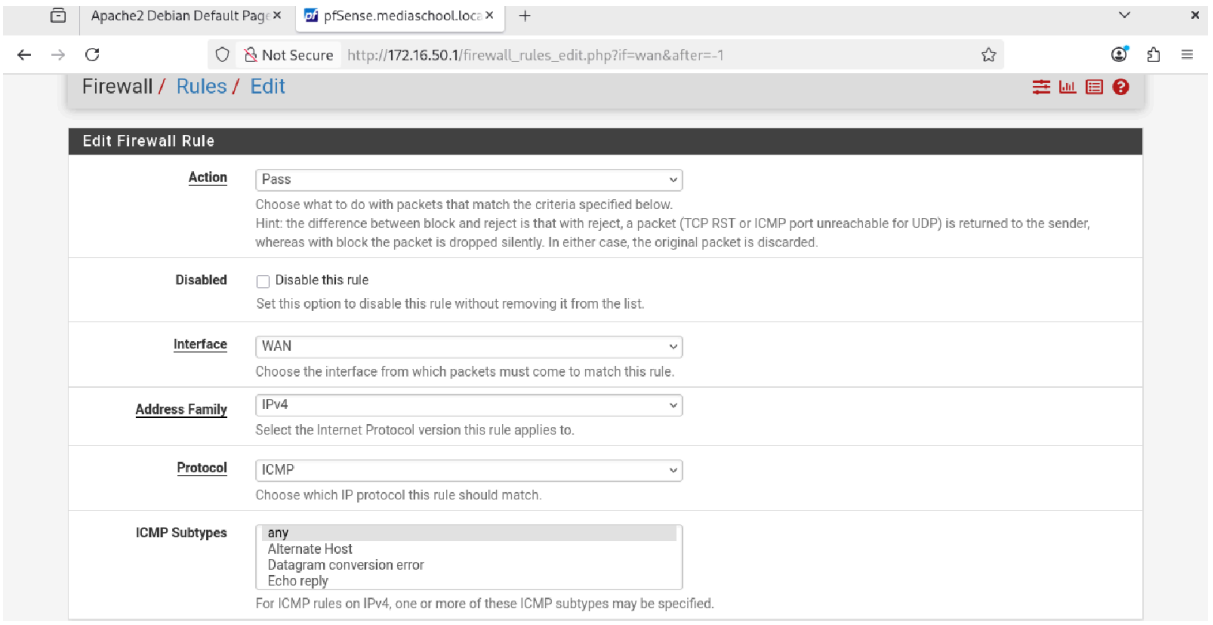
Configuration finale du serveur :

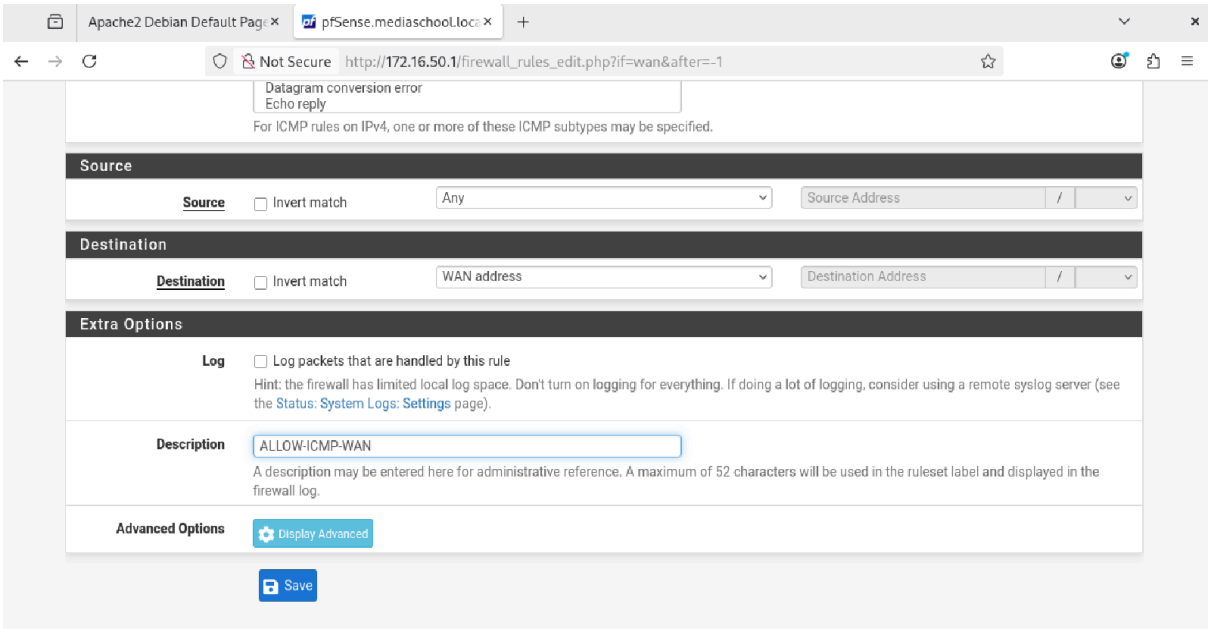

ludivine@srv1: ~
ludivine@srv1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP 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:~$

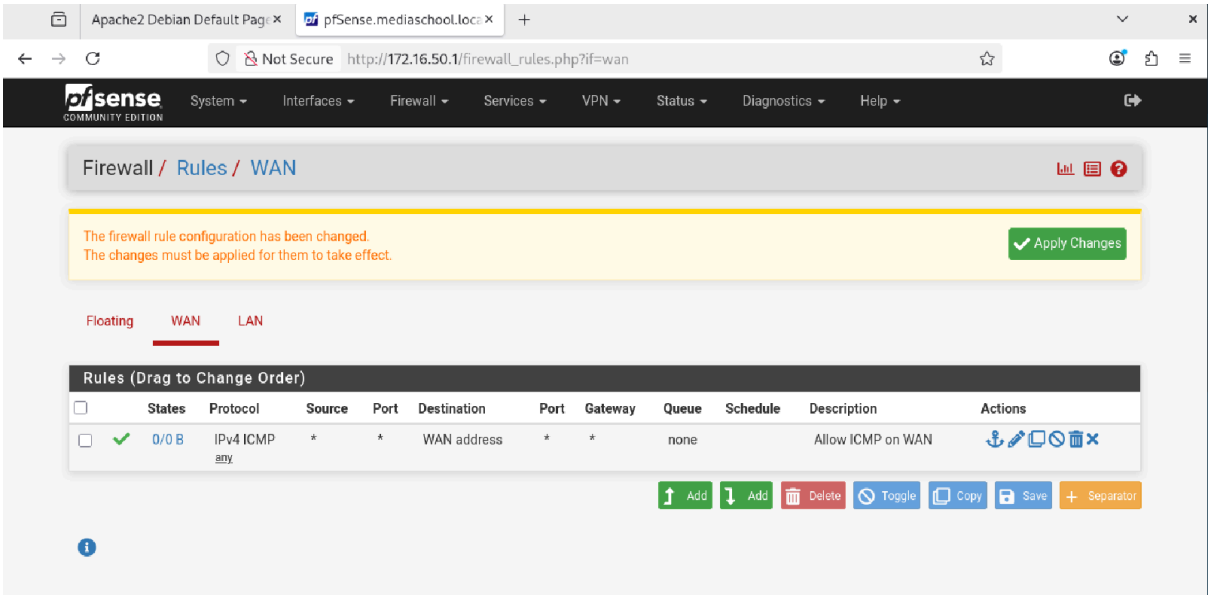

ludivine@srv1: ~
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
link/ether 08:00:27:cc:66:17 brd ff:ff:ff:ff:ff:ff
altname enx080027cc6617
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:~$

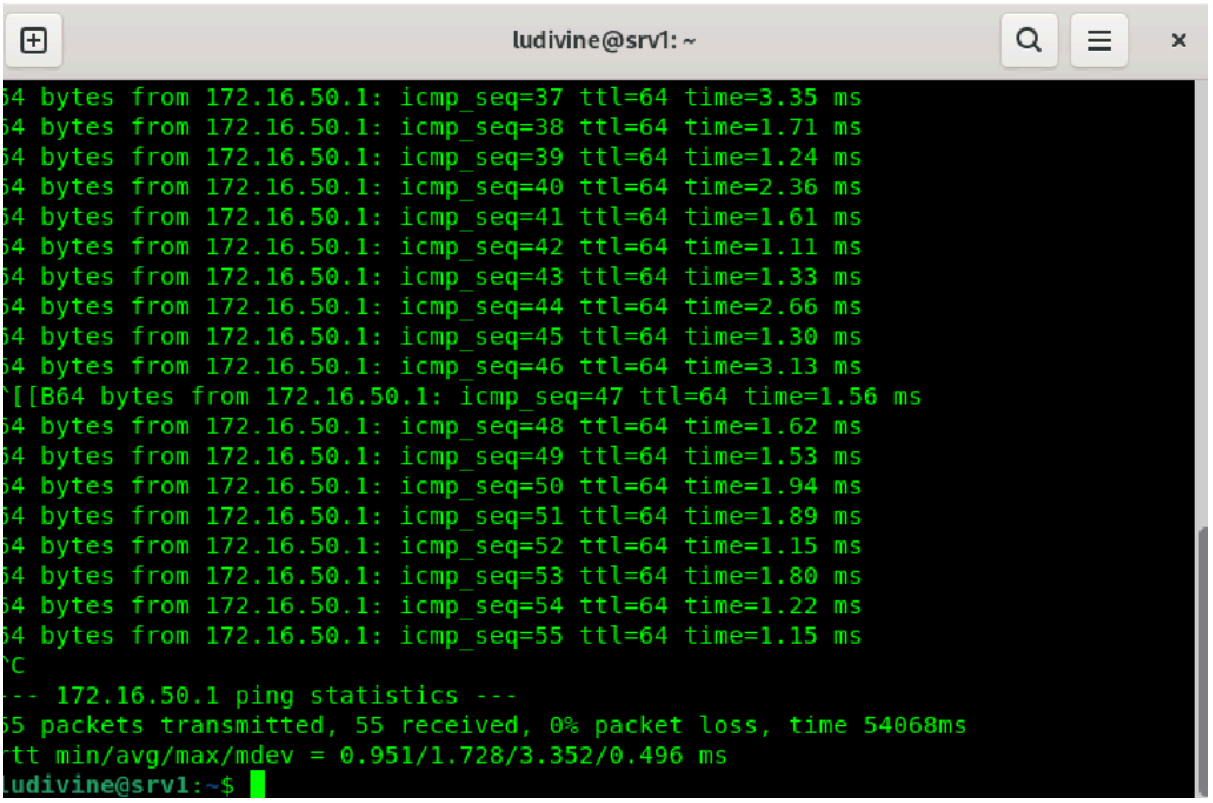
Etape 4 :

Etape 5 :


Apache2 Debian Default Page
pfSense.mediaschool.local
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.

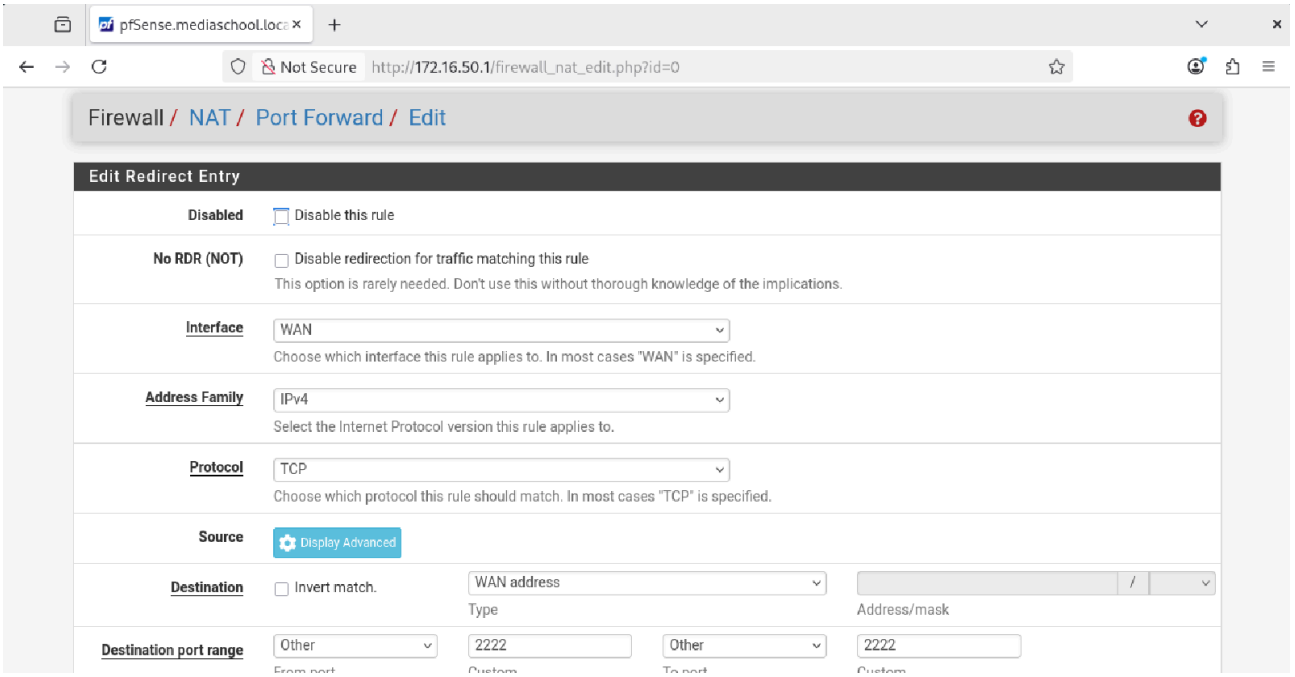

Apache2 Debian Default Page
pfSense.mediaschool.local
Not Secure
http://172.16.50.1/firewall_rules_edit.php?if=wan&after=-1
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.
Source
Source
Invert match
Any
Source Address
Destination
Destination
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
Save

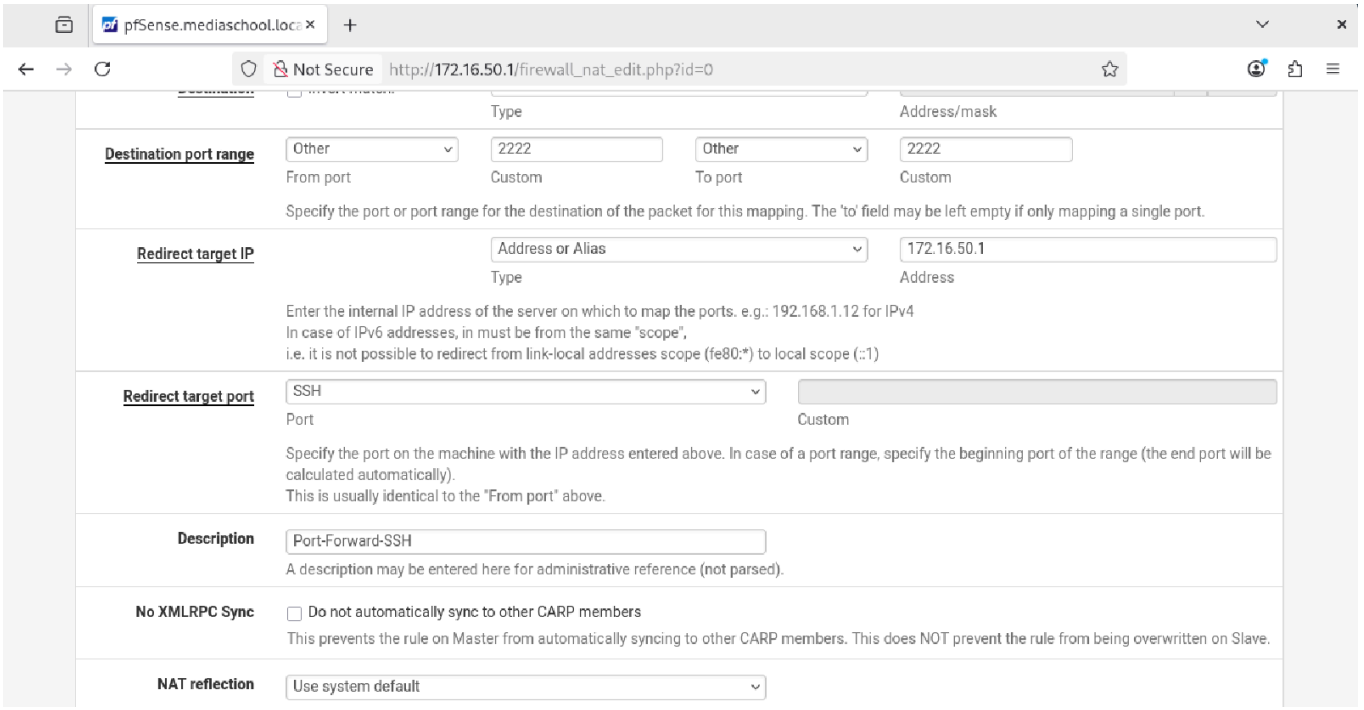


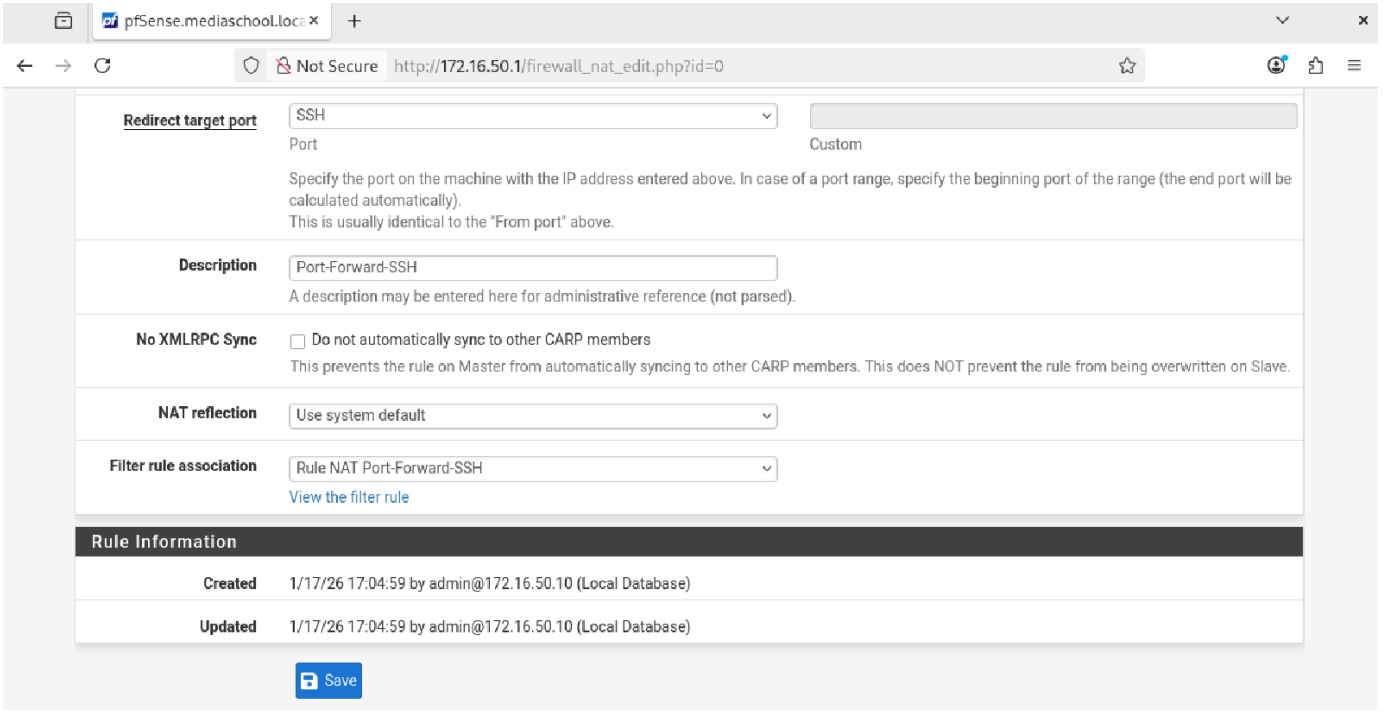


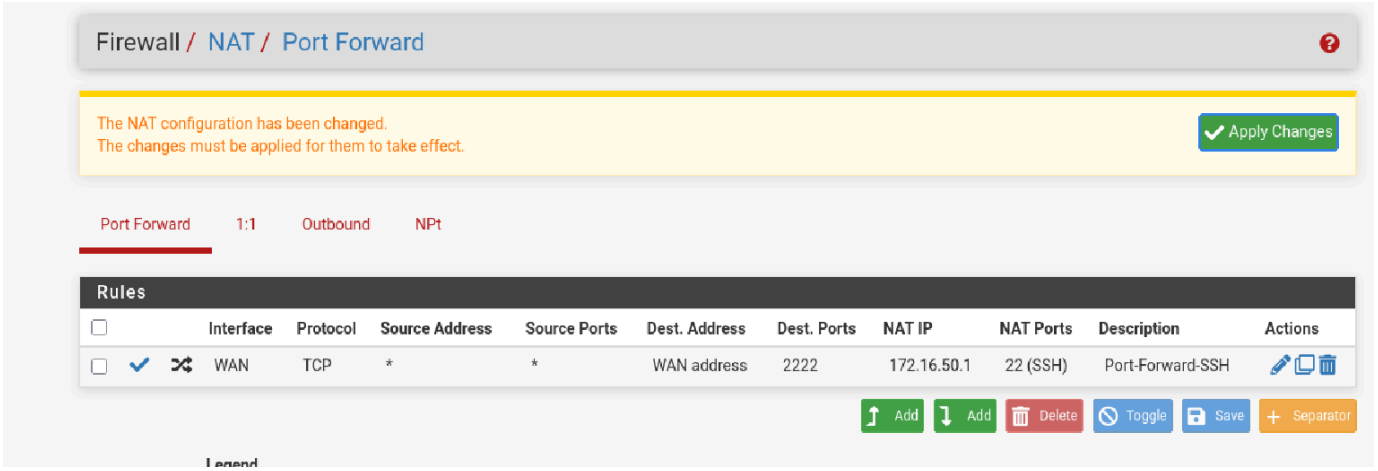
Etape 6 :

Redirection SSH :

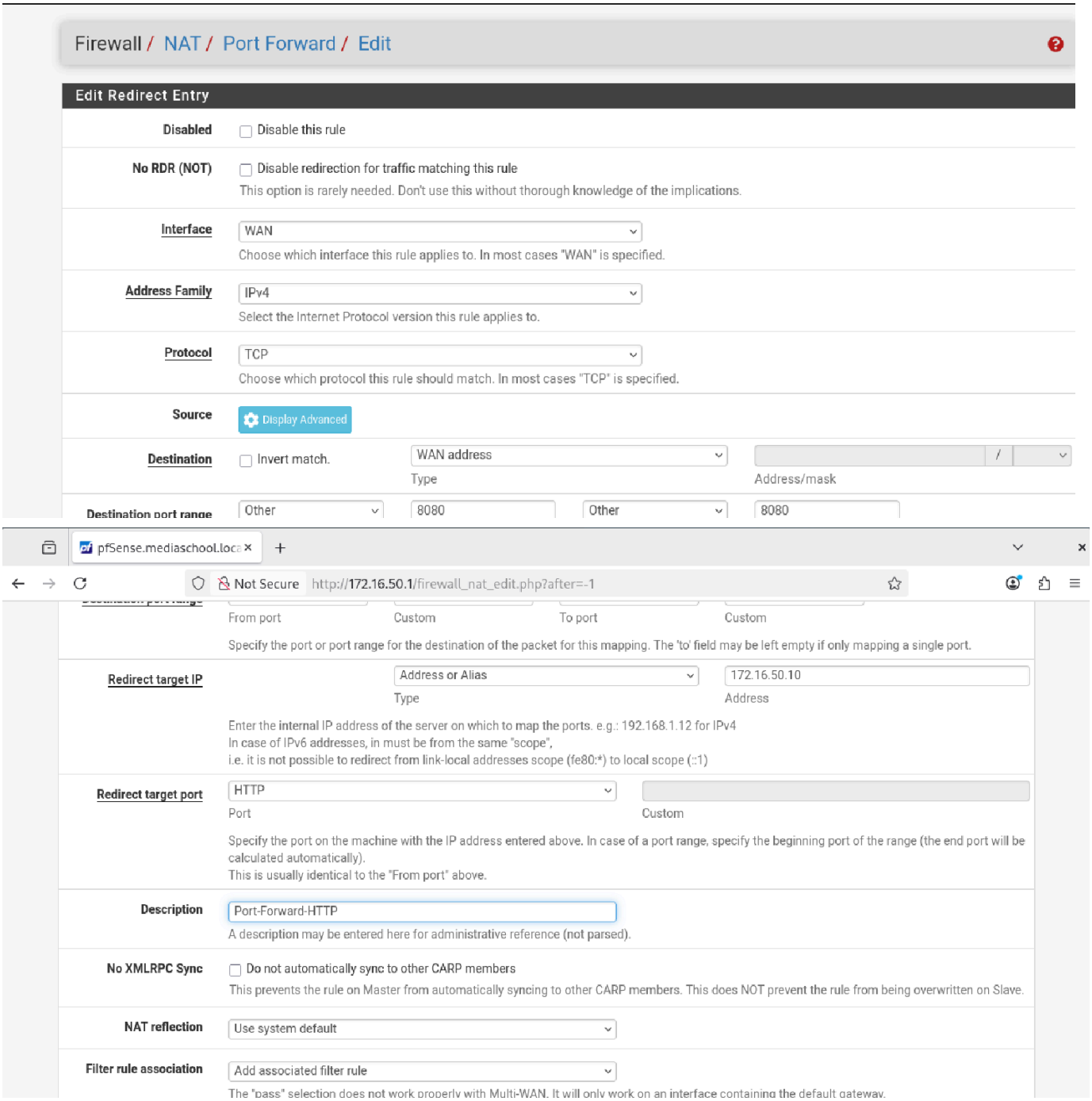

pfSense.mediaschool.loca
Not Secure
http://172.16.50.1/firewall_nat_edit.php?id=0
Firewall / NAT / Port Forward / Edit
Edit Redirect Entry
Disabled
Disable this rule
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge 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
2222
Other
2222

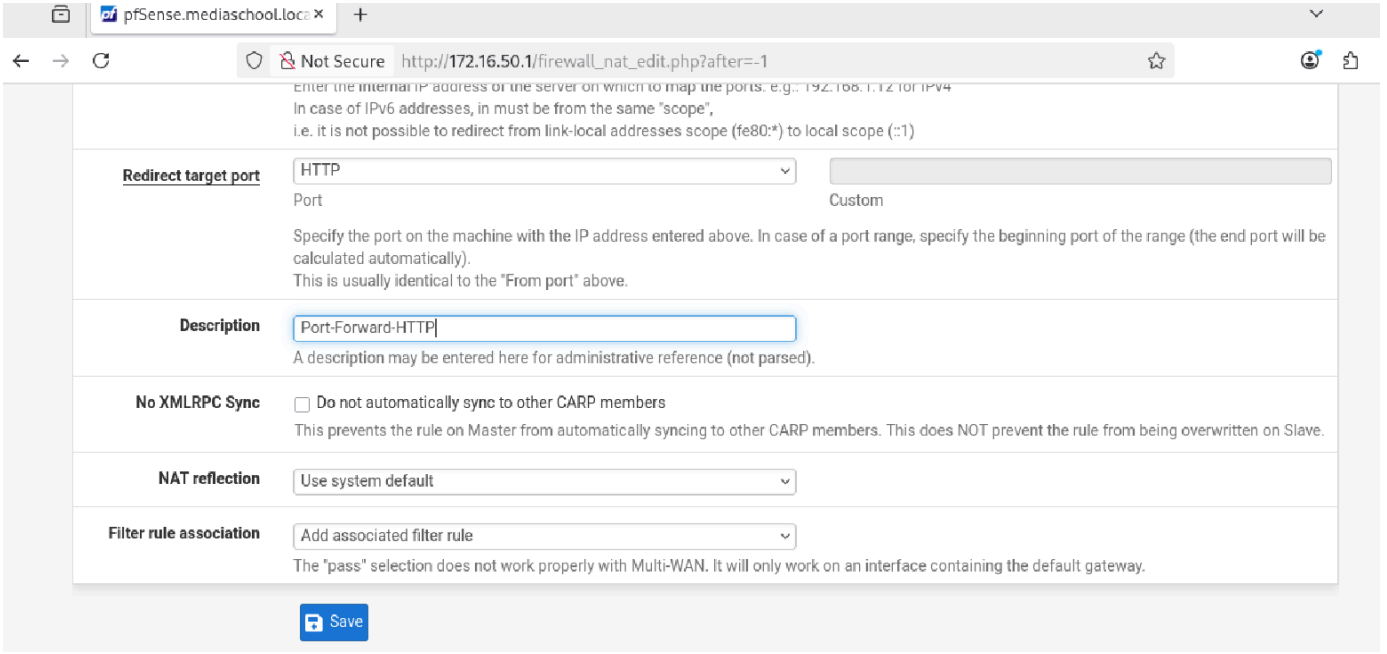

pfSense.mediaschool.loca
Not Secure
http://172.16.50.1/firewall_nat_edit.php?id=0
Type
Address/mask
Destination port range
Other
2222
Other
2222
From port
Custom
To port
Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP
Address or Alias
172.16.50.1
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, in 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

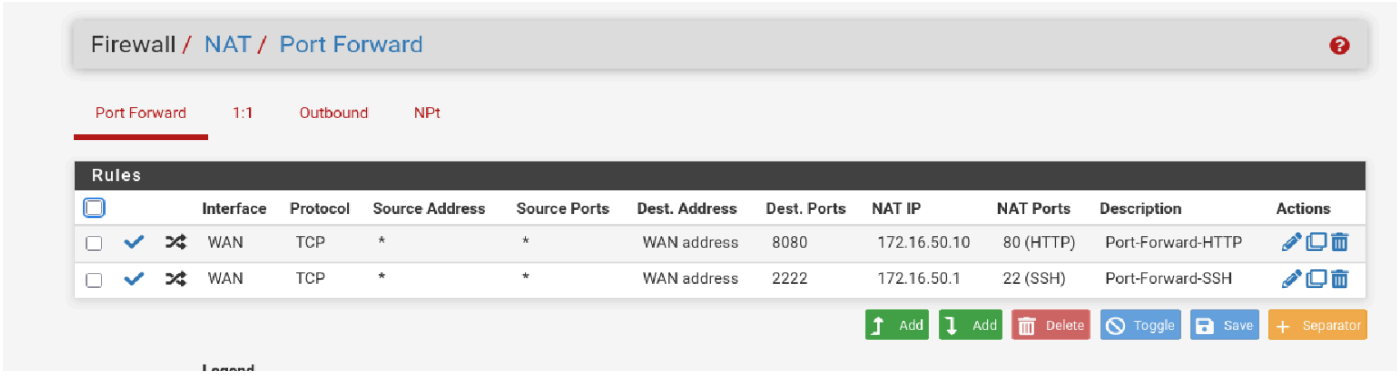




Redirection HTTP :


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
pfSense.mediaschool.loca
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
Address or Alias
Type
172.16.50.10
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, in 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.

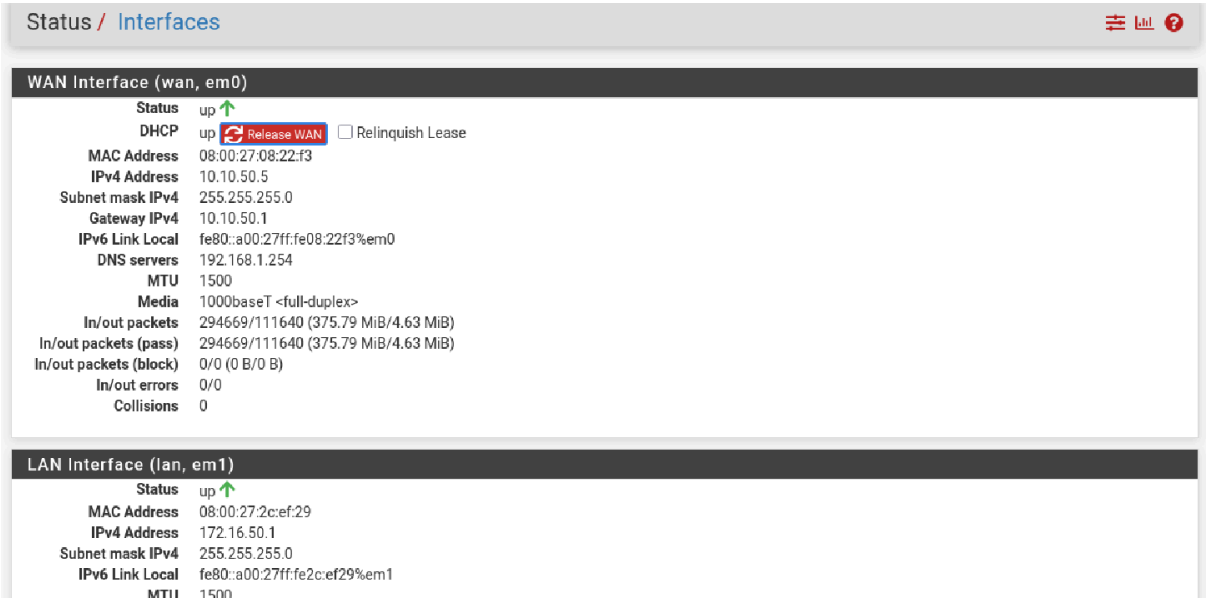




Etape 7 :

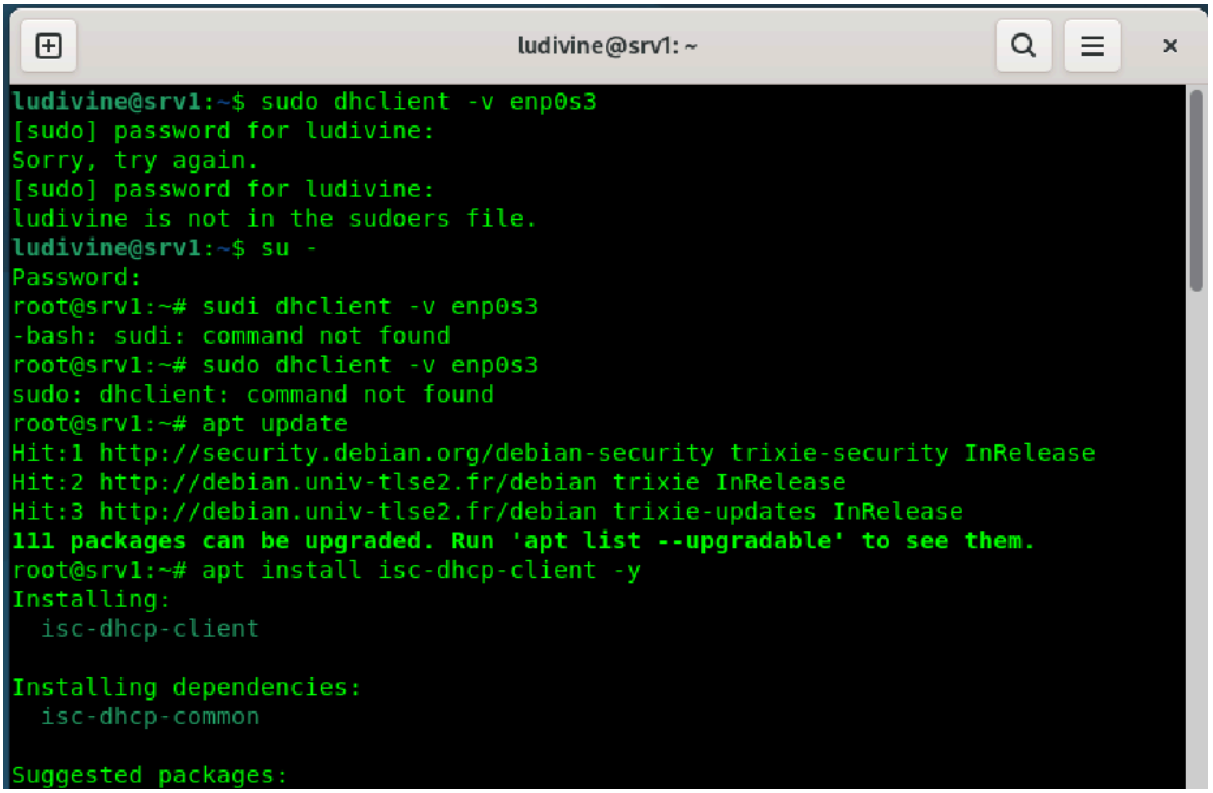
Test connexion SSH :

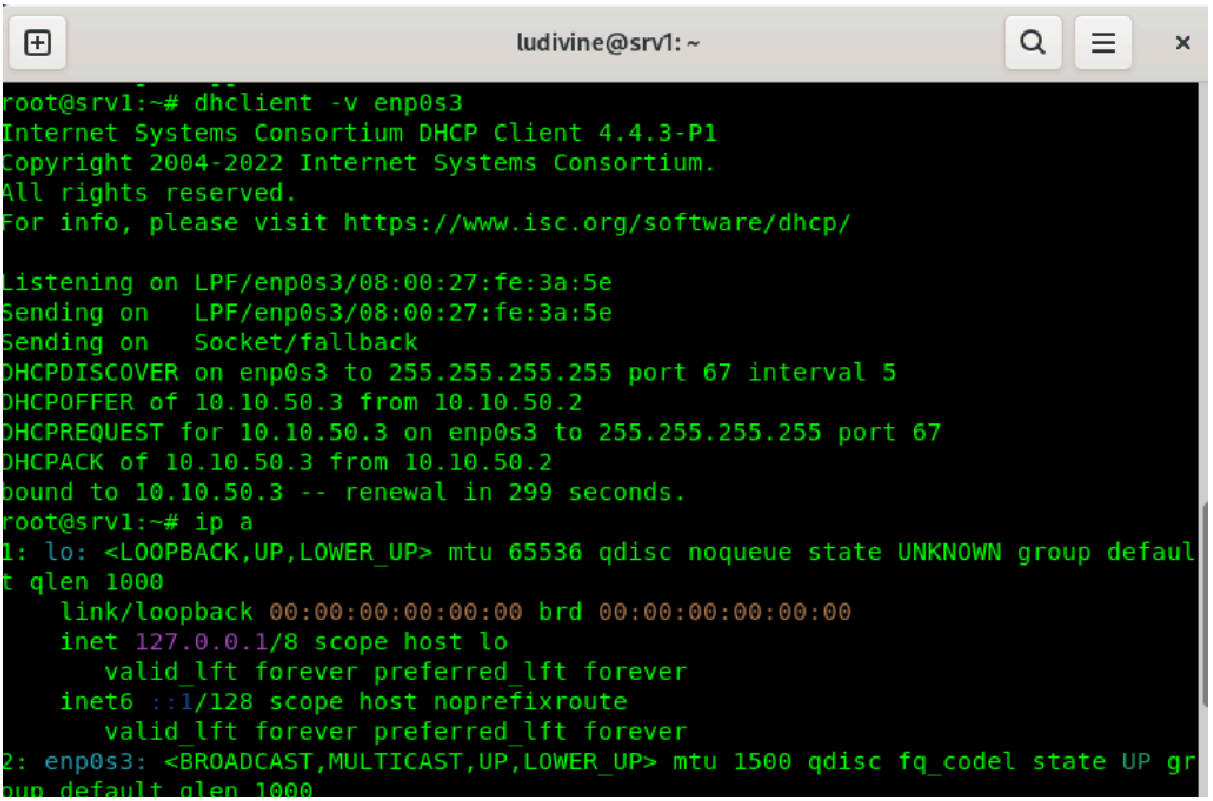
Avant de tester la connexion SSH chez le client je cherche mon adresse IPV4 WAN dans pfsense :

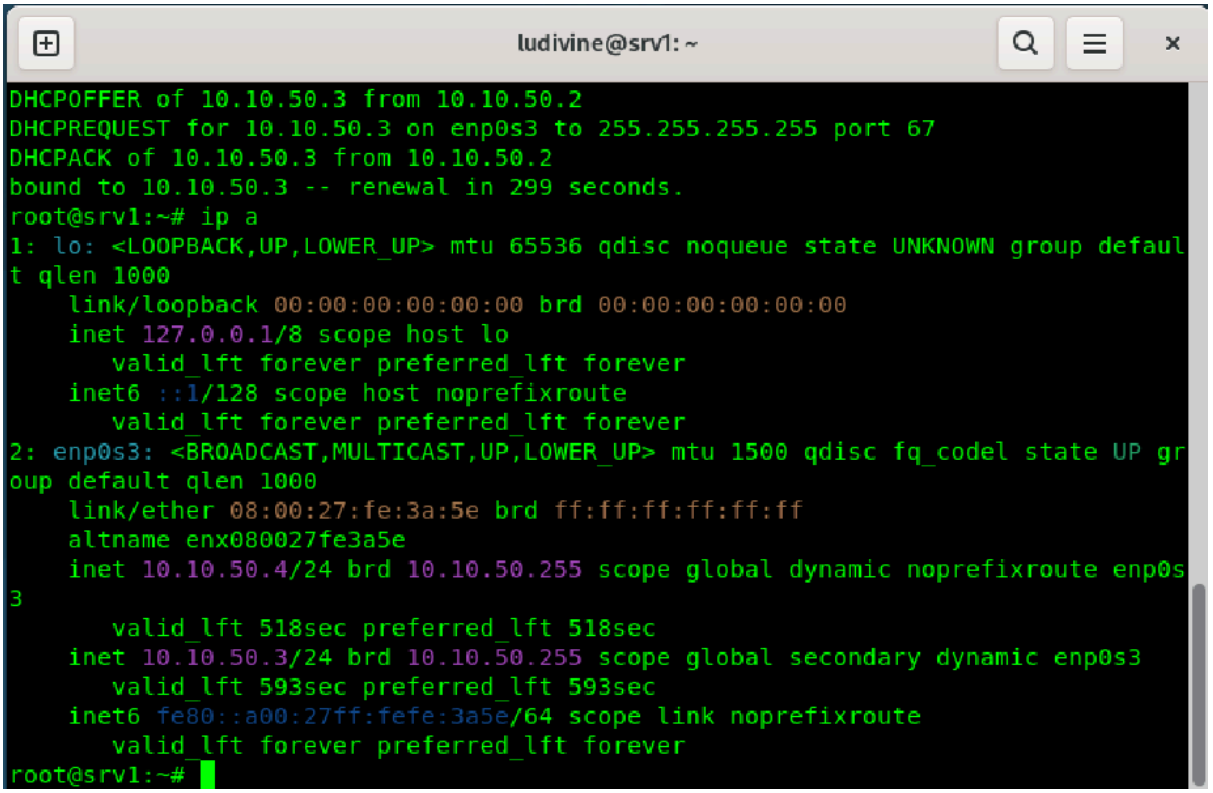


Mon adresse IPv4 est 10.10.50.5

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 :

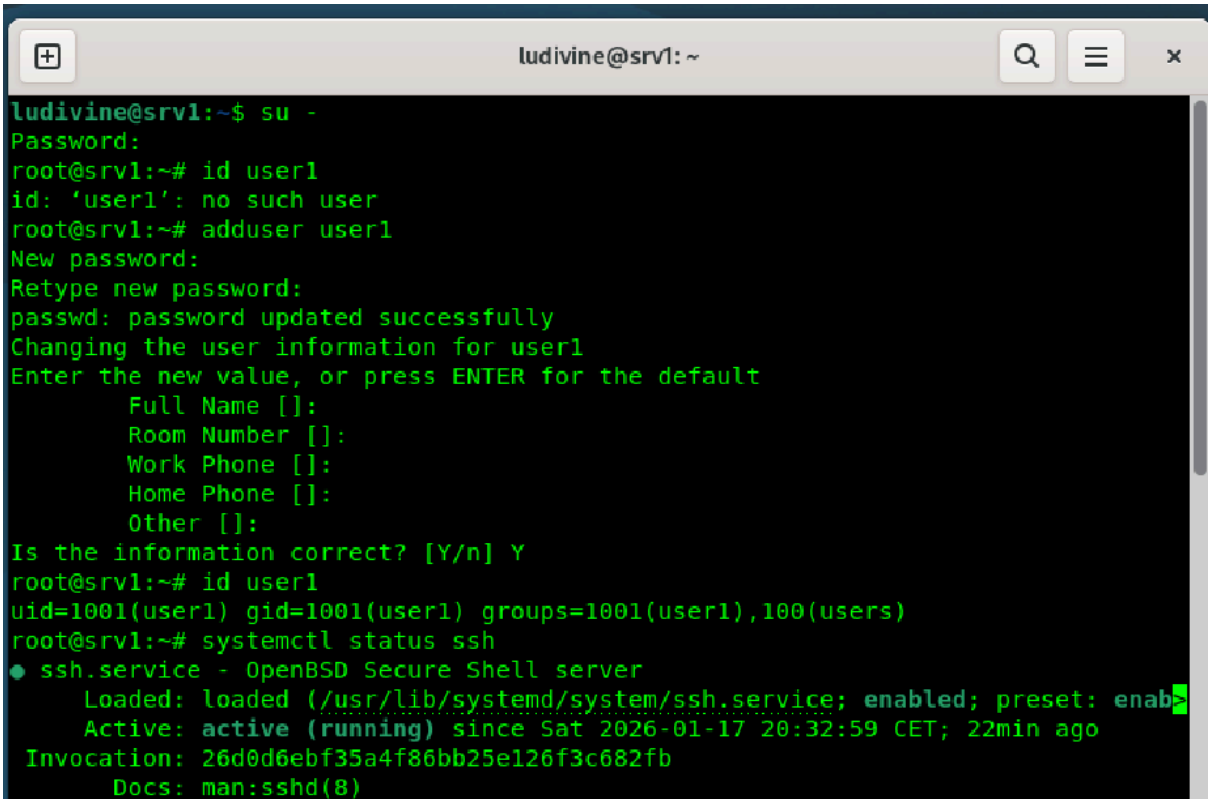


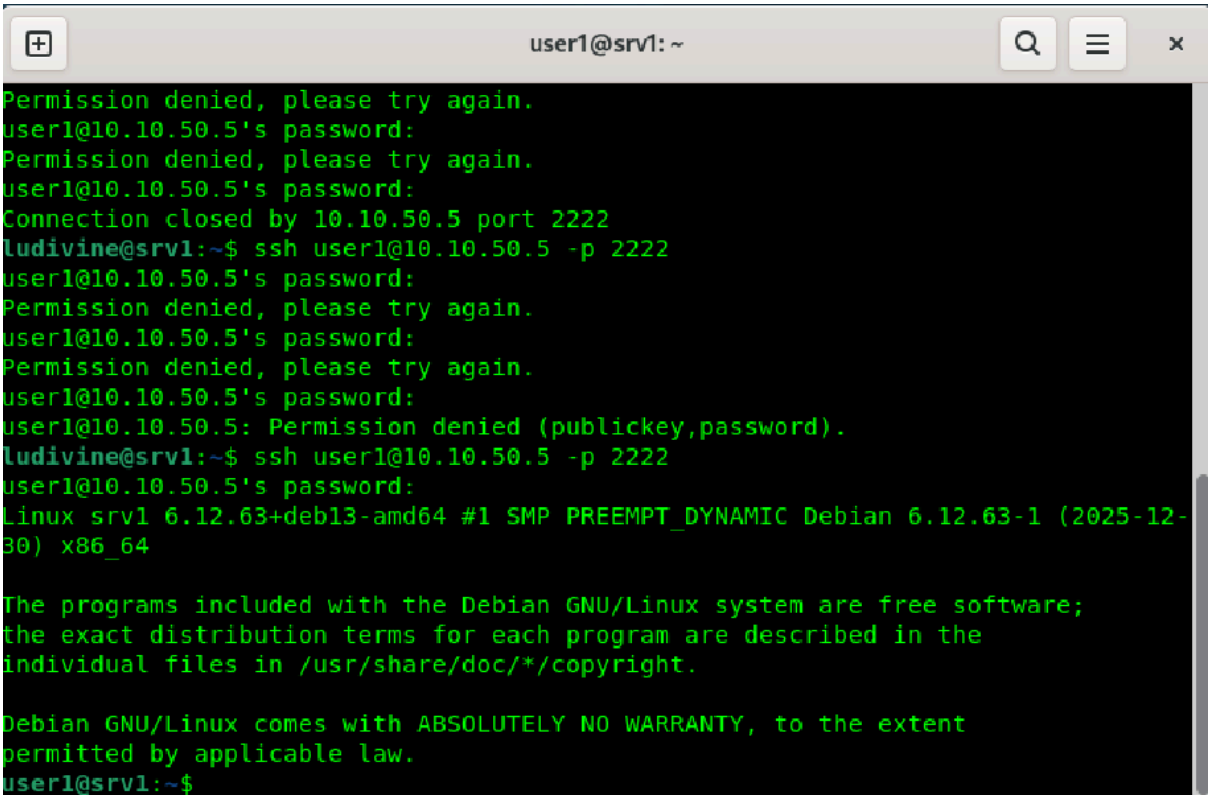




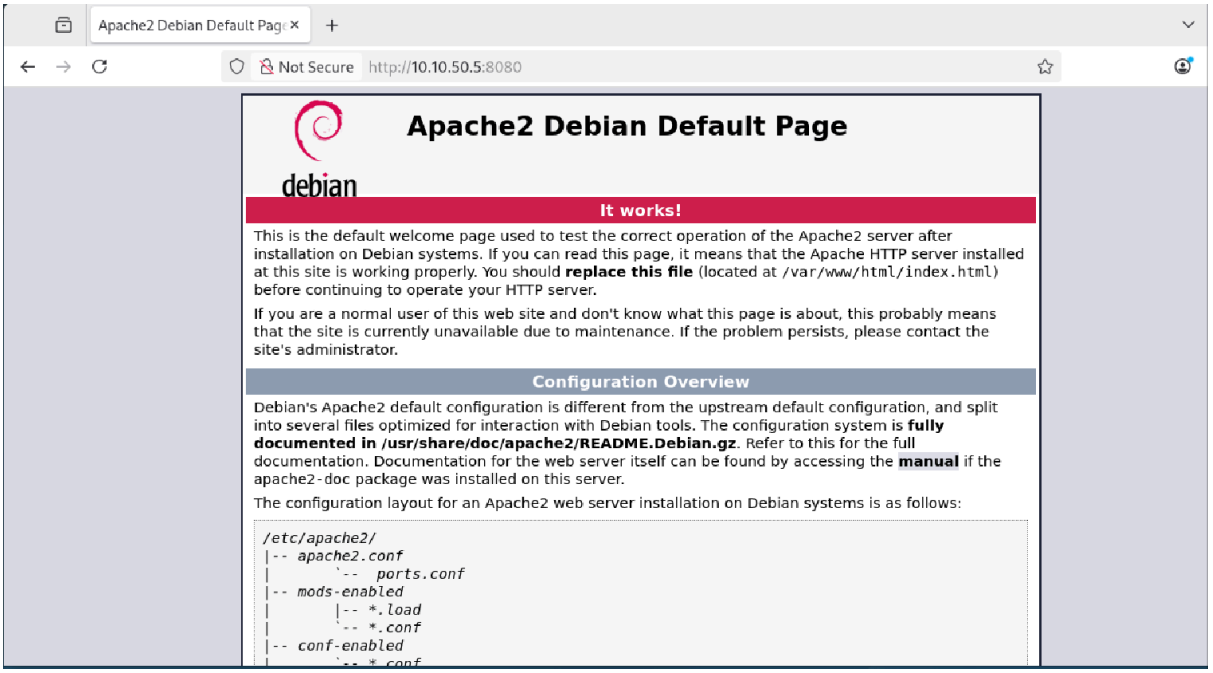
Son adresse IP lui a été donnée (10.10.50.4/24)

Je me suis rendue compte que je n'avais pas crée d'user1. J'en ai crée un sur le serveur avec un mot de passe puis le test peut être fait :





Test connexion HTTP :


Apache2 Debian Default Pag
Not Secure
http://10.10.50.5:8080
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled

Bonus :