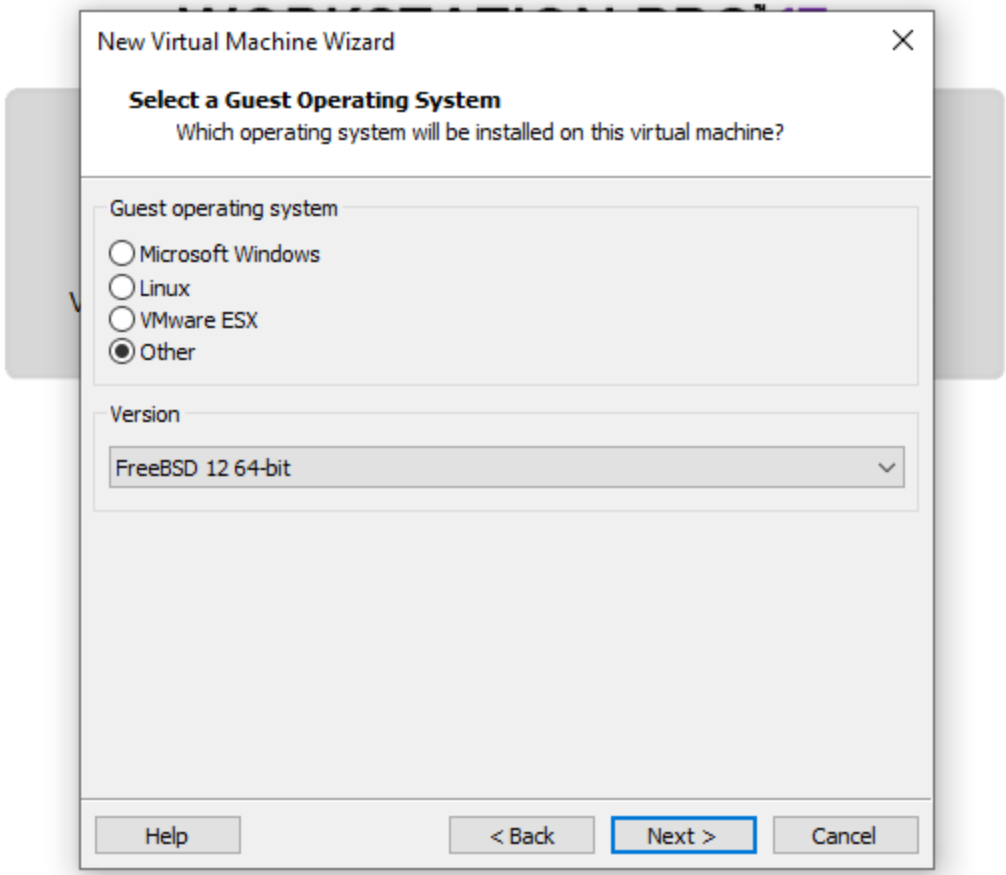
FIREWALL & PFSENSE

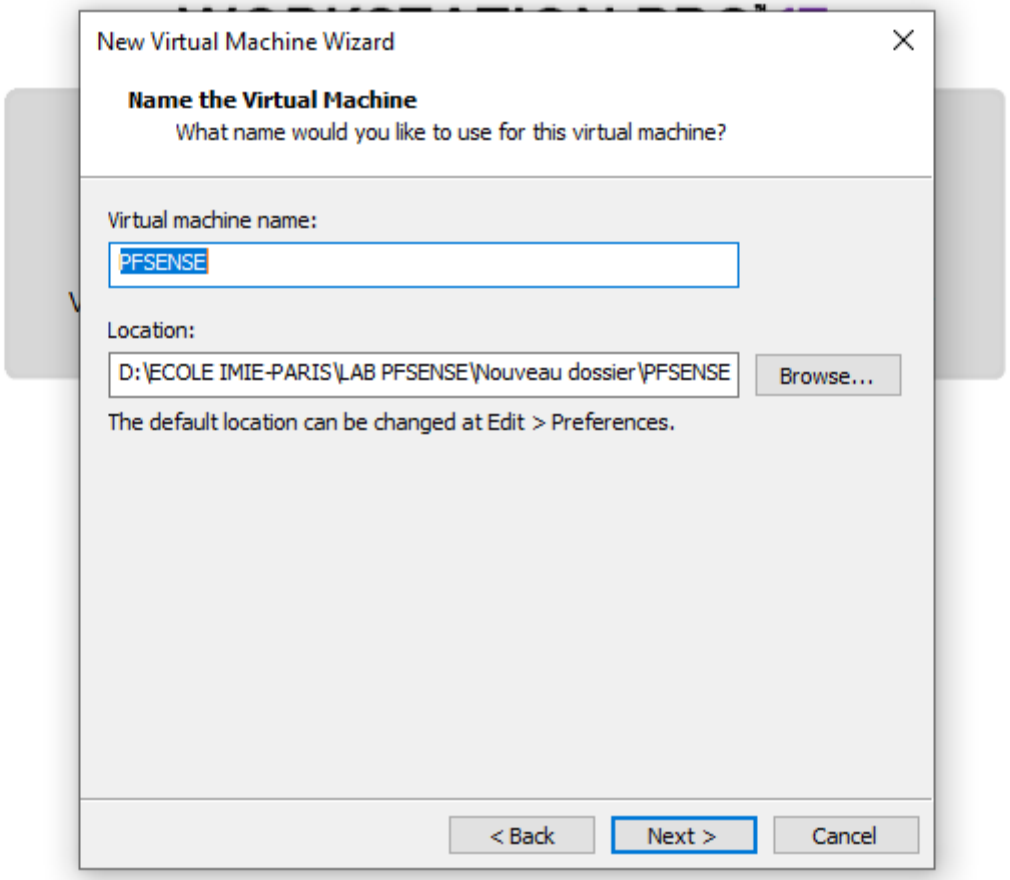
MACHINE PFSENSE / CLIENT WINDOWS 10 / UBUNTU SEVER

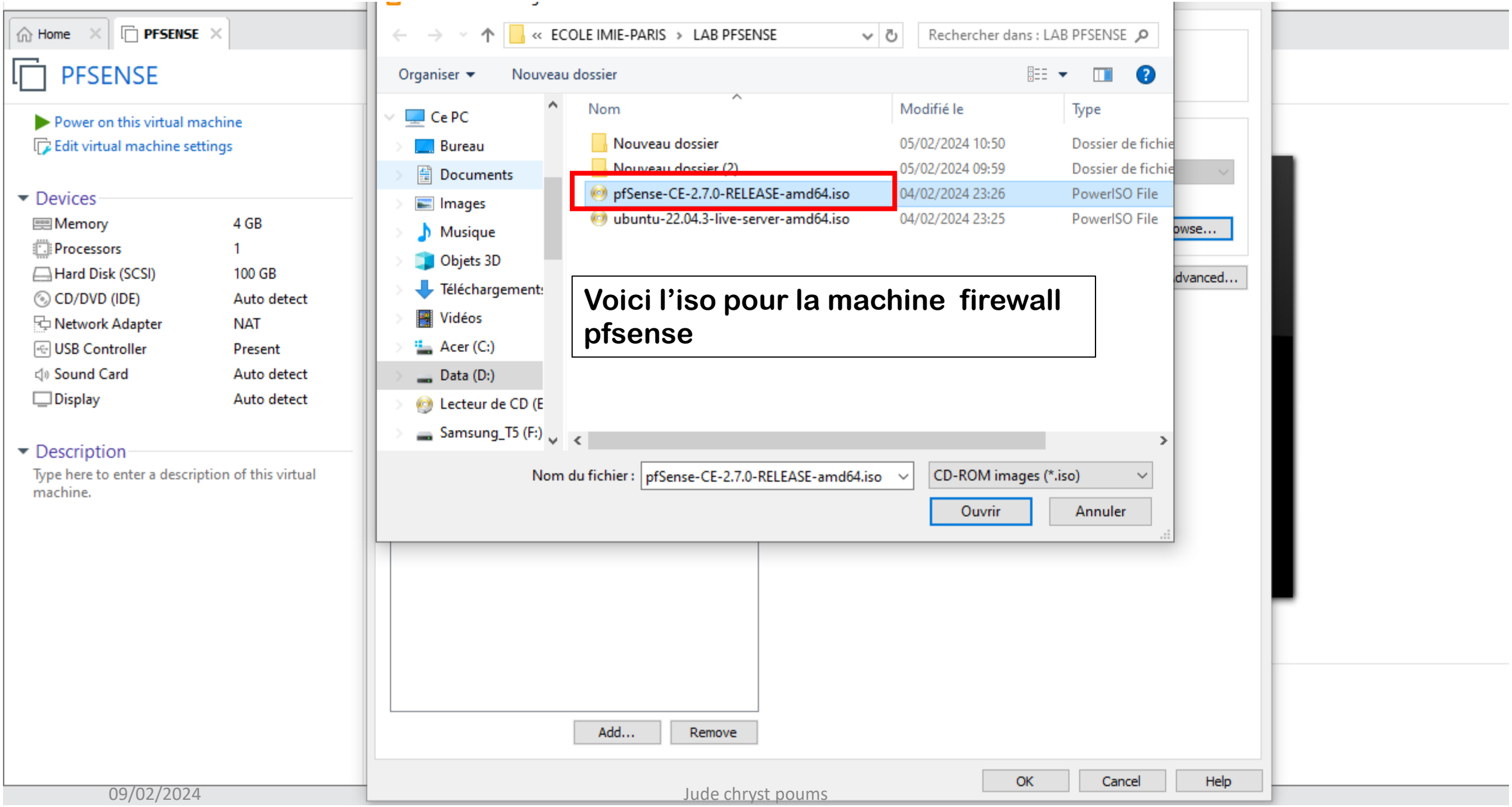
Etape 1: Création de la machine virtuelle Firewall pfsense

Système: FreeBSD 12 64-bit



A ce niveau donner un nom à la machine virtuelle : PFSENSE et choisir le chemin de stockage pour celui ci




Home
PFSENSE
PFSENSE
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 4 GB
Processors 1
Hard Disk (SCSI) 100 GB
CD/DVD (IDE) Auto detect
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Description
Type here to enter a description of this virtual machine.
« ECOLE IMIE-PARIS › LAB PFSENSE
Rechercher dans : LAB PFSENSE
Organiser
Nouveau dossier
Ce PC
Bureau
Documents
Images
Musique
Objets 3D
Téléchargements
Vidéos
Acer (C:)
Data (D:)
Lecteur de CD (E
Samsung_T5 (F:)
Nom
Modifié le
Type
Nouveau dossier 05/02/2024 10:50 Dossier de fichie
Nouveau dossier (2) 05/02/2024 09:59 Dossier de fichie
pfSense-CE-2.7.0-RELEASE-amd64.iso 04/02/2024 23:26 PowerISO File
ubuntu-22.04.3-live-server-amd64.iso 04/02/2024 23:25 PowerISO File
Voici l'iso pour la machine firewall pfsense
Nom du fichier : pfSense-CE-2.7.0-RELEASE-amd64.iso
CD-ROM images (*.iso)
Ouvrir
Annuler
owse...
dvanced...
Add...
Remove
OK
Cancel
Help

Virtual machine settings

Ajouter 2 cartes réseaux pour avoir en totalement 3 cartes réseaux.

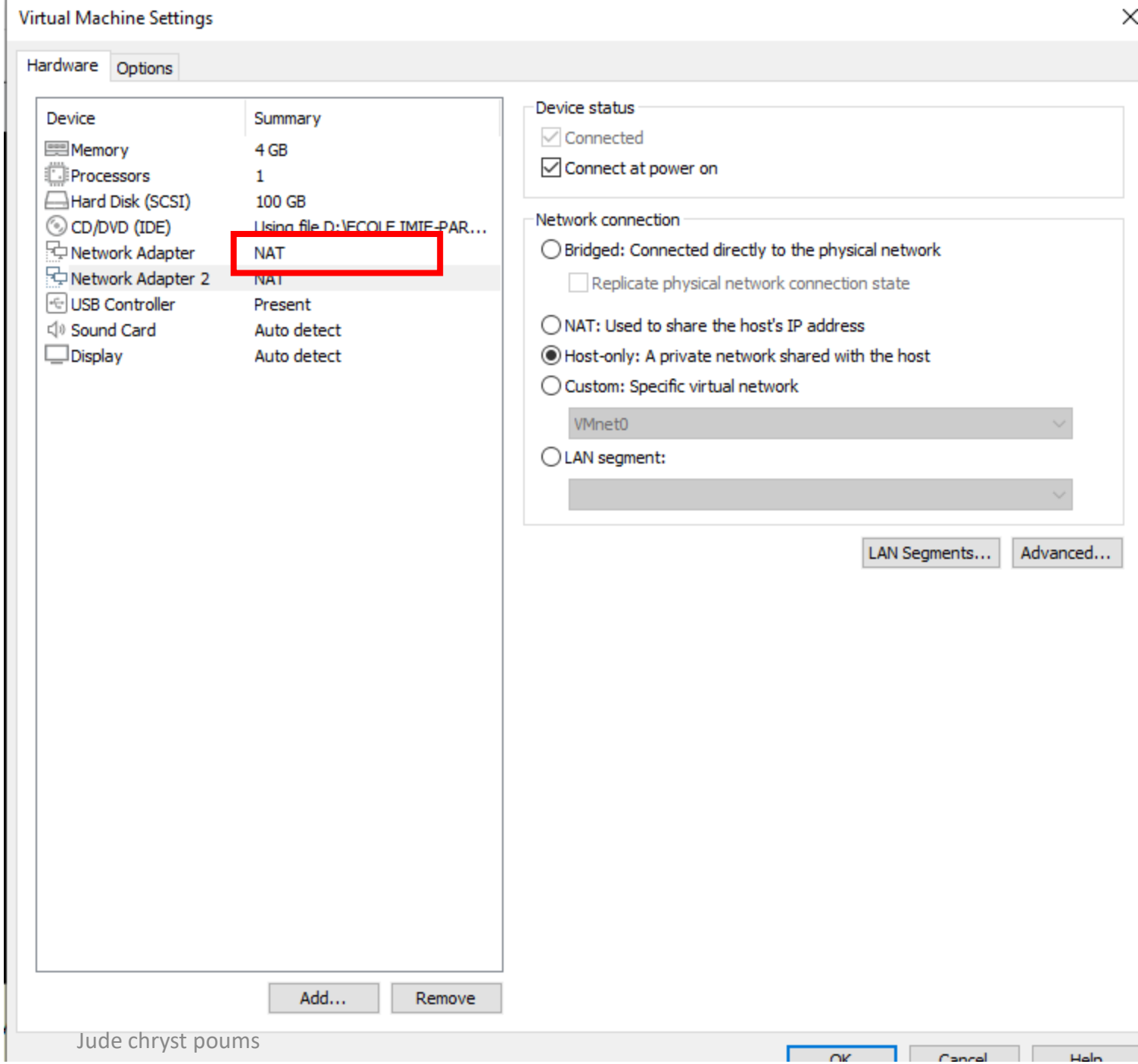
1er carte : mettre la première carte en NAT

2eme carte : mettre la deuxième carte en LAN

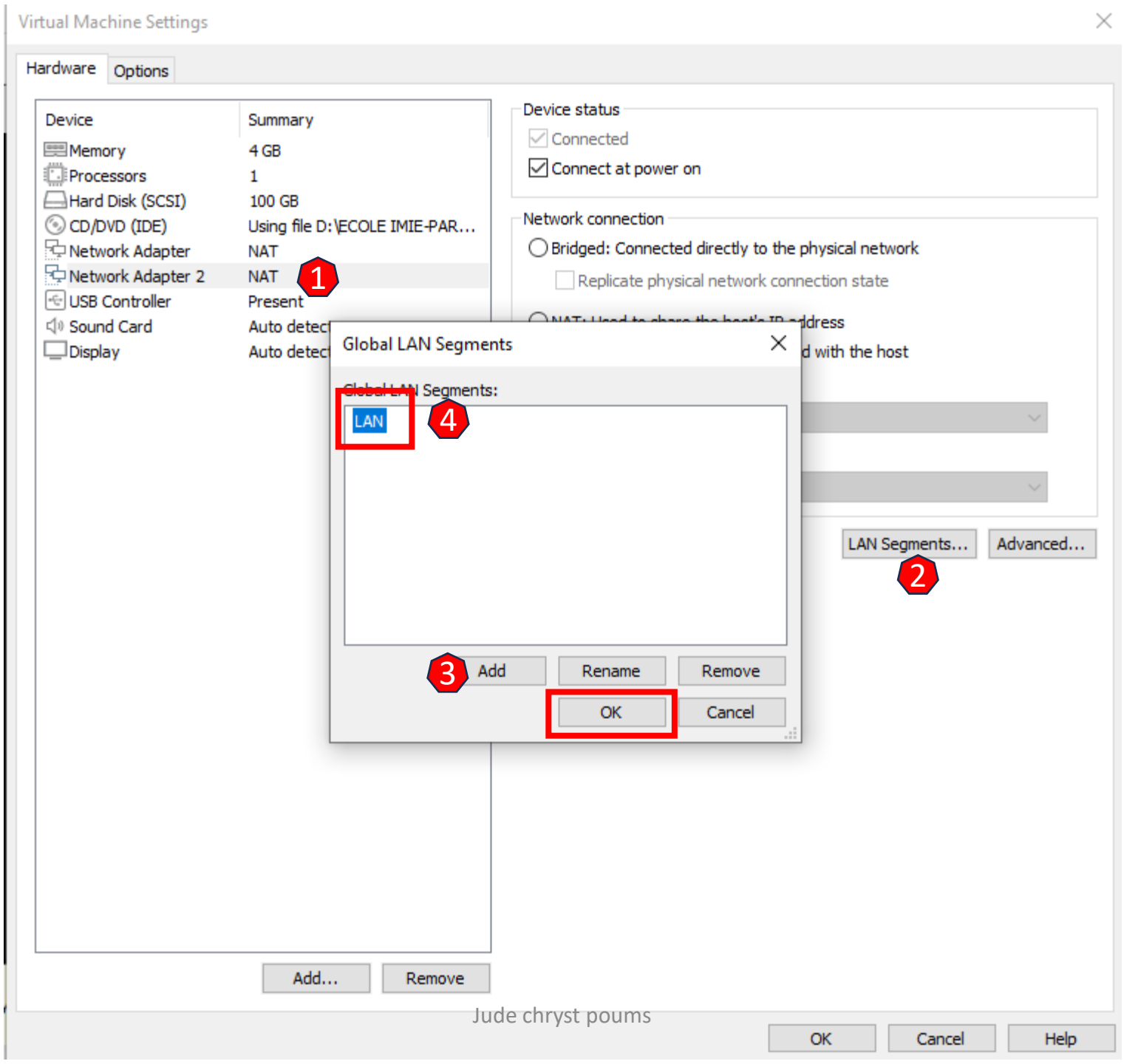
Pour ce faire, il faudrait sélectionner LAN segment, cliquer sur LAN segments... puis add pour créer un réseau local qui sera non lue par l'ordinateur physique.

3e carte : mettre la deuxième carte en DMZ

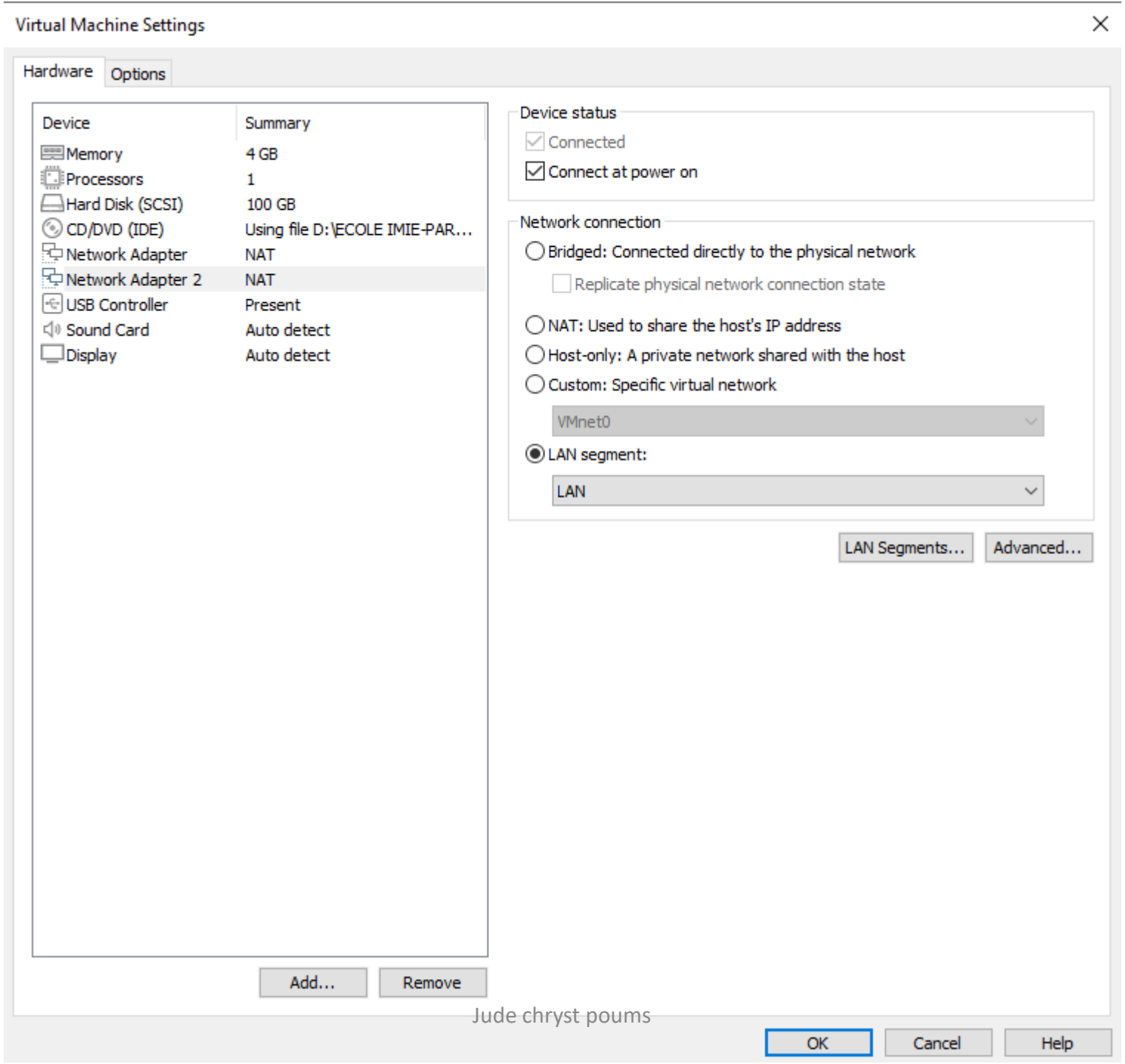
Suivre la méthode de la 2eme carte, puis add et créer le réseau DMZ qui sera non lue par l'ordinateur physique.



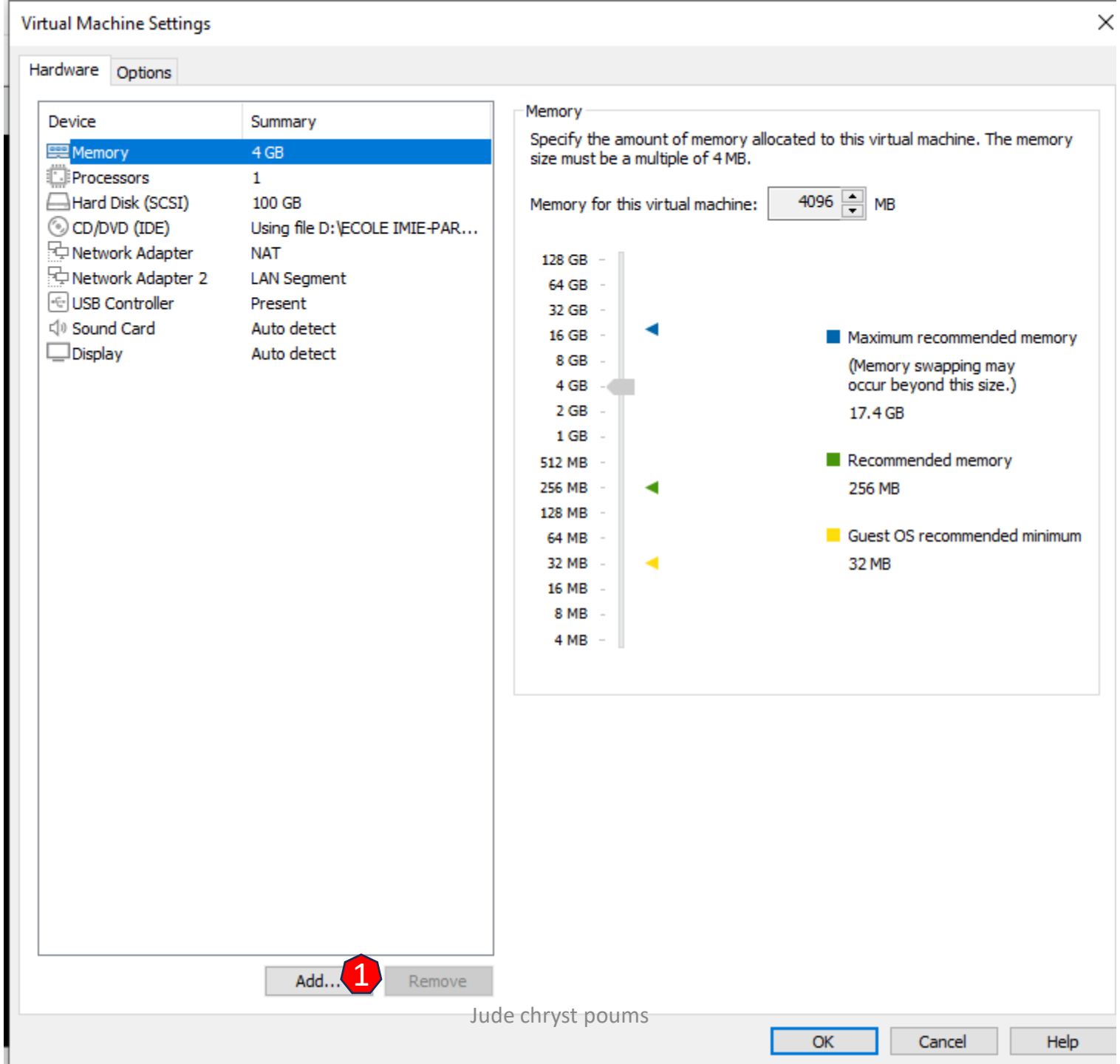
1


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
4 GB
Processors
1
Hard Disk (SCSI)
100 GB
CD/DVD (IDE)
Using file D:\ECOLE IMIE-PAR...
Network Adapter
NAT
Network Adapter 2
NAT
USB Controller
Present
Sound Card
Display
1
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
with the host
LAN Segments...
Advanced...
2
Add...
Remove
OK
Cancel
Help
Global LAN Segments
Global LAN Segments:
LAN
4
3
Add
Rename
Remove
OK
Cancel

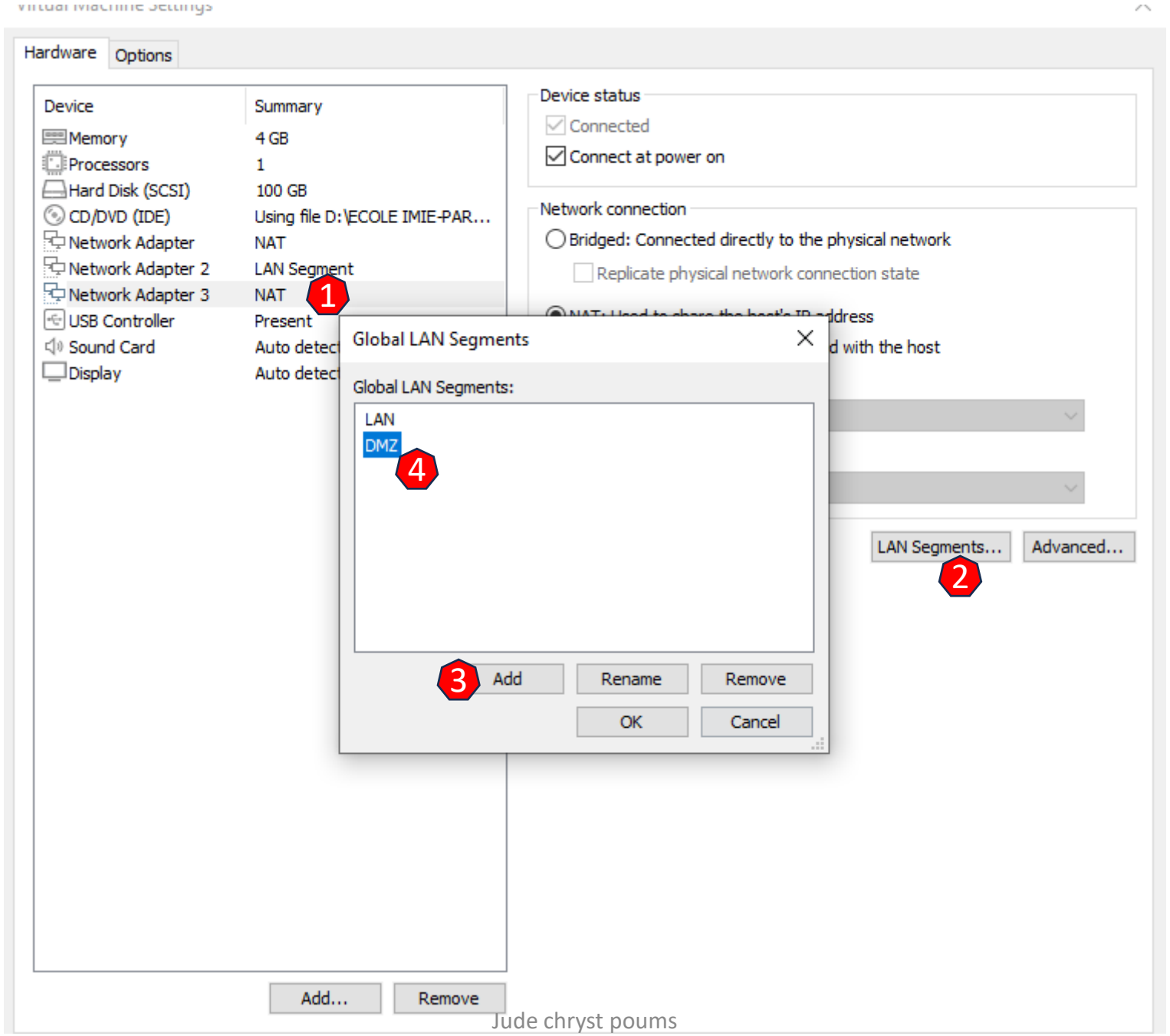
1


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
4 GB
Processors
1
Hard Disk (SCSI)
100 GB
CD/DVD (IDE)
Using file D:\ECOLE IMIE-PAR...
Network Adapter
NAT
Network Adapter 2
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN
LAN Segments...
Advanced...
OK
Cancel
Help

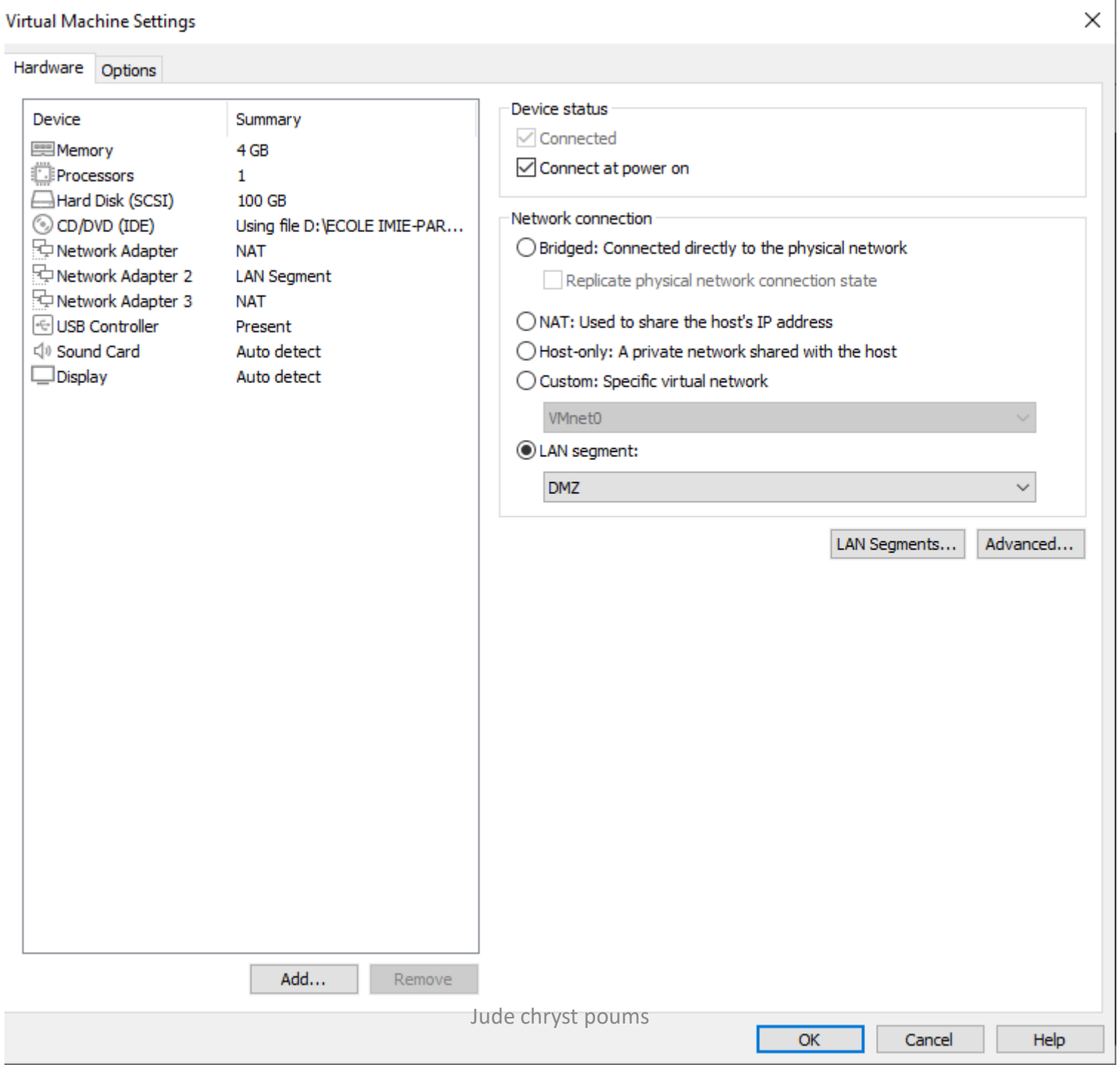
2


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
4 GB
Processors
1
Hard Disk (SCSI)
100 GB
CD/DVD (IDE)
Using file D:\ECOLE IMIE-PAR...
Network Adapter
NAT
Network Adapter 2
LAN Segment
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
1
Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine:
4096
MB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
17.4 GB
Recommended memory
256 MB
Guest OS recommended minimum
32 MB
OK
Cancel
Help

2


Hardware
Options
Device
Summary
Memory
4 GB
Processors
1
Hard Disk (SCSI)
100 GB
CD/DVD (IDE)
Using file D:\ECOLE IMIE-PAR...
Network Adapter
NAT
Network Adapter 2
LAN Segment
Network Adapter 3
NAT
USB Controller
Present
Sound Card
Display
1
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
with the host
LAN Segments...
Advanced...
2
Global LAN Segments
Global LAN Segments:
LAN
DMZ
4
3
Add
Rename
Remove
OK
Cancel

2


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
4 GB
Processors
1
Hard Disk (SCSI)
100 GB
CD/DVD (IDE)
Using file D:\ECOLE IMIE-PAR...
Network Adapter
NAT
Network Adapter 2
LAN Segment
Network Adapter 3
NAT
USB Controller
Present
Sound Card
Auto detect
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
DMZ
LAN Segments...
Advanced...
OK
Cancel
Help

LANCER LA MACHINE PFSENSE

Home | PFSENSE

PFSENSE

Power on this virtual machine

Edit virtual machine settings

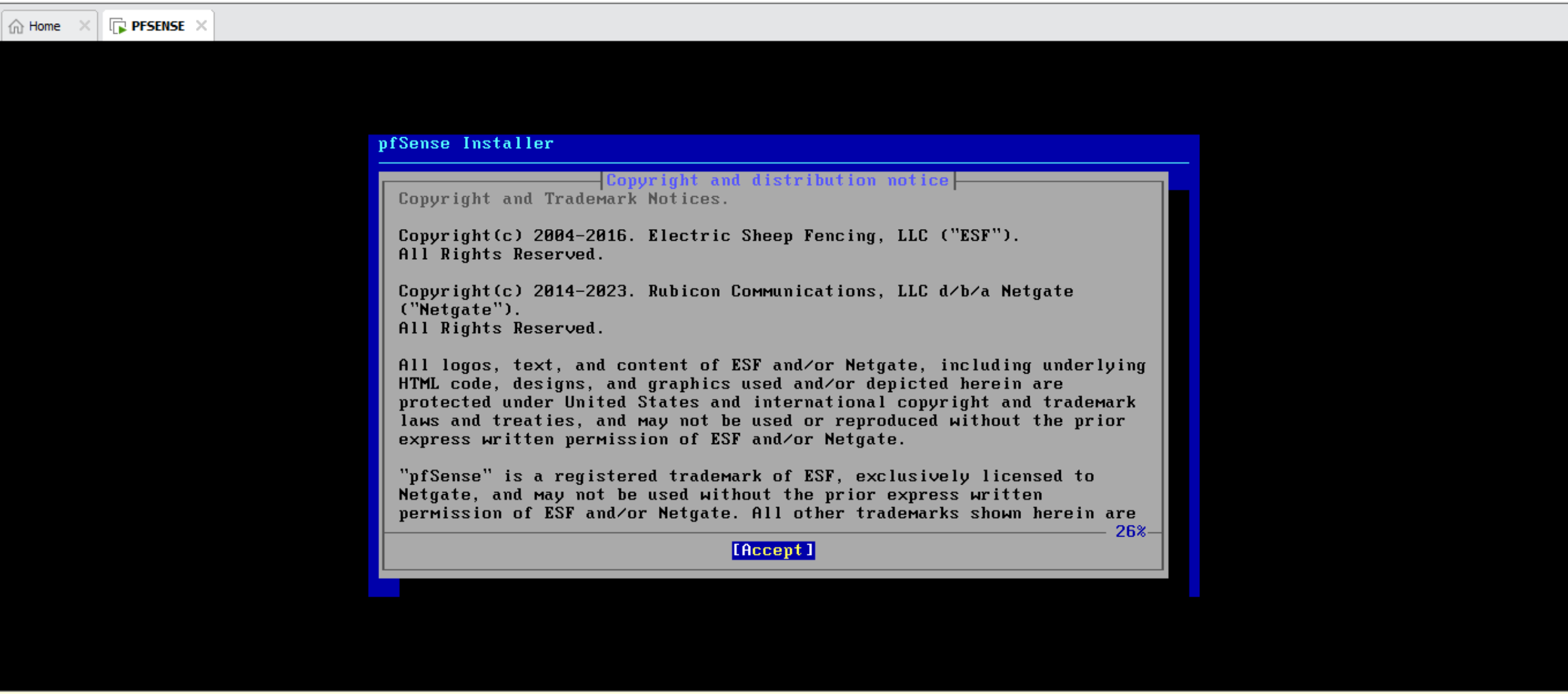
Devices

Memory	4 GB
Processors	1
Hard Disk (SCSI)	100 GB
CD/DVD (IDE)	Using file D:\EC...
Network Adapter	NAT
Network Adapter 2	LAN Segment
Network Adapter 3	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

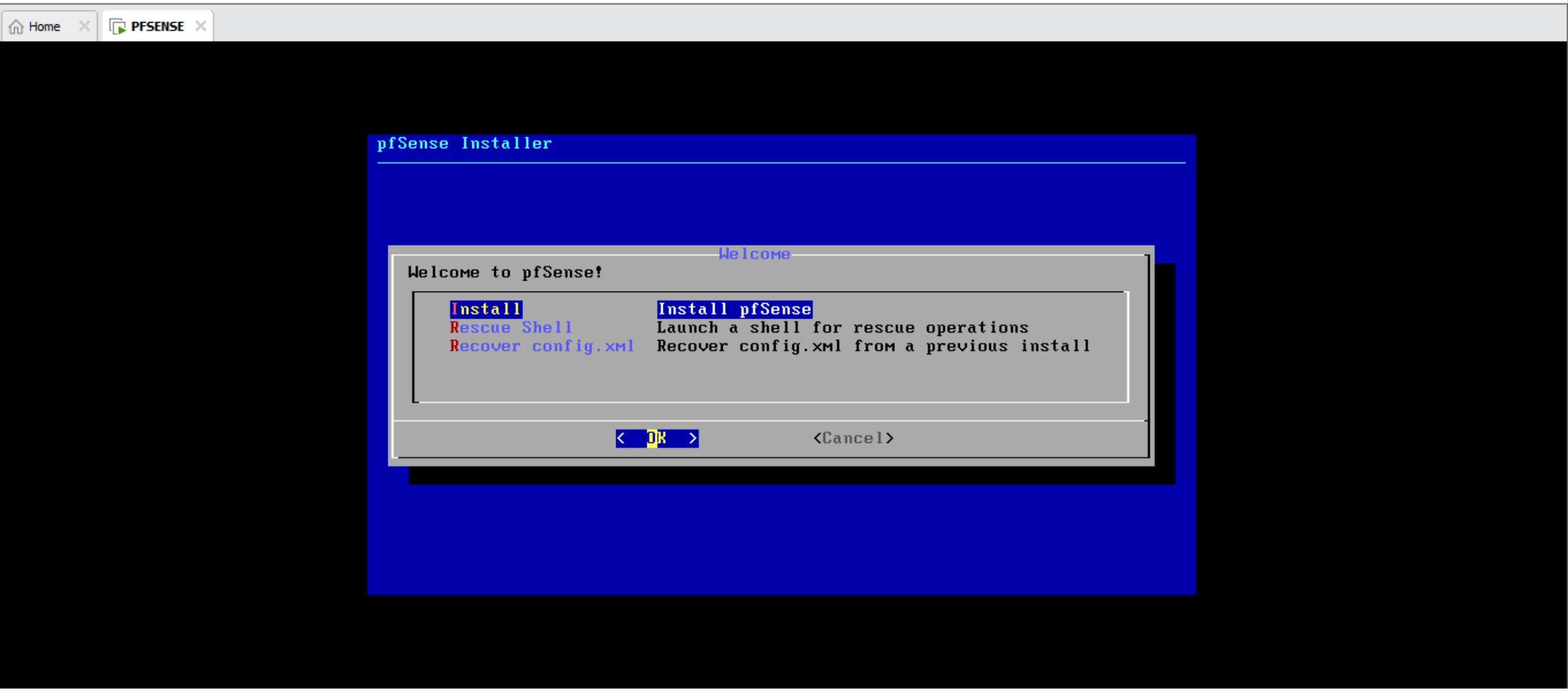
Description

Type here to enter a description of this virtual machine.

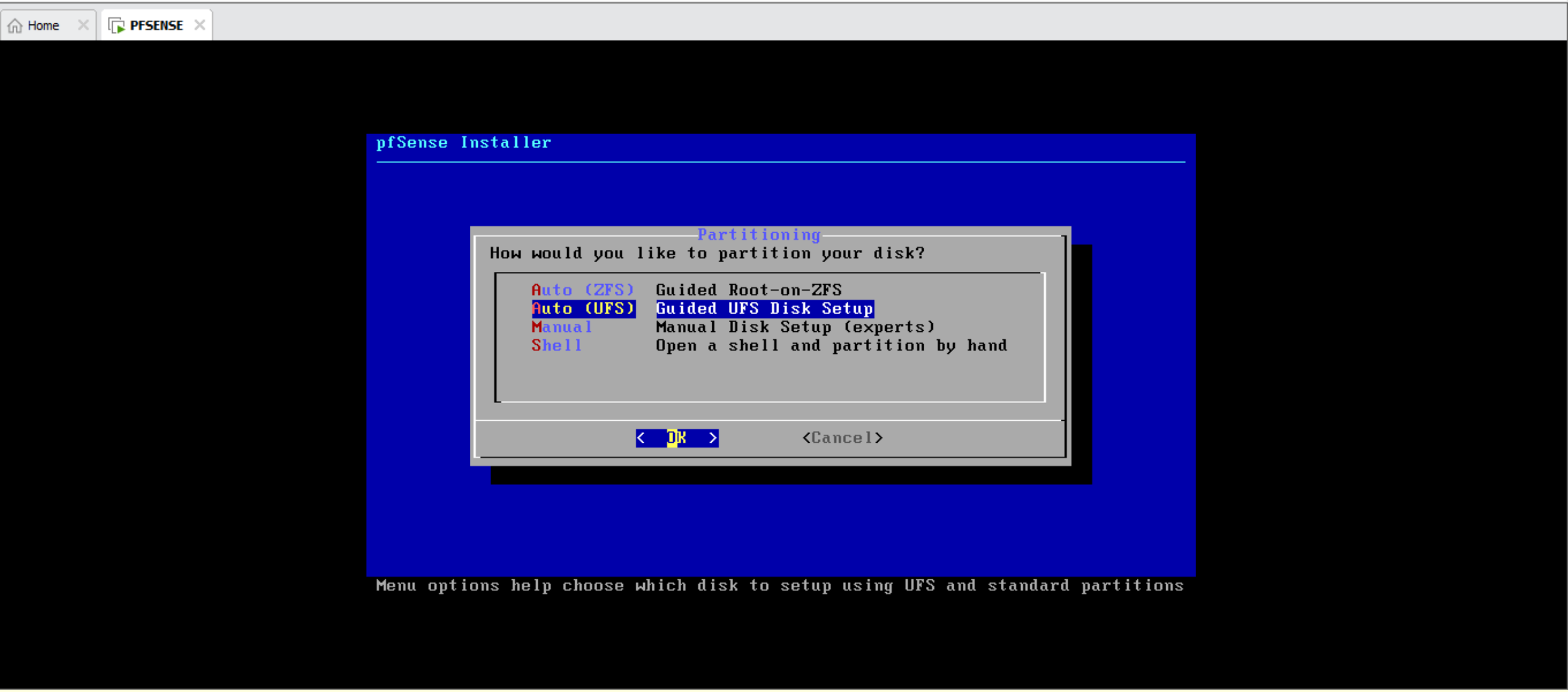
✓ Accepter l'installation pfsense



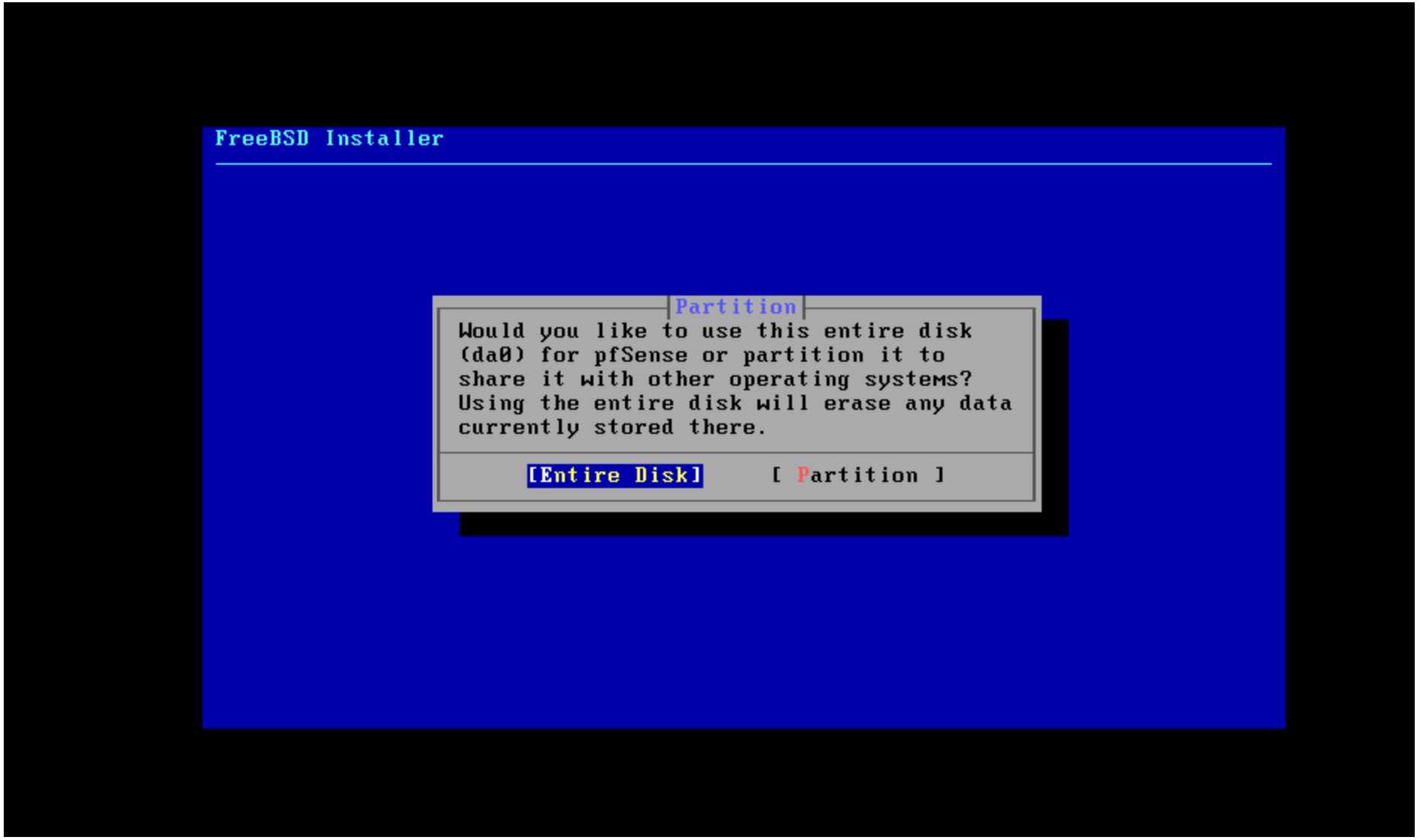
✓ Choisir install pfsense



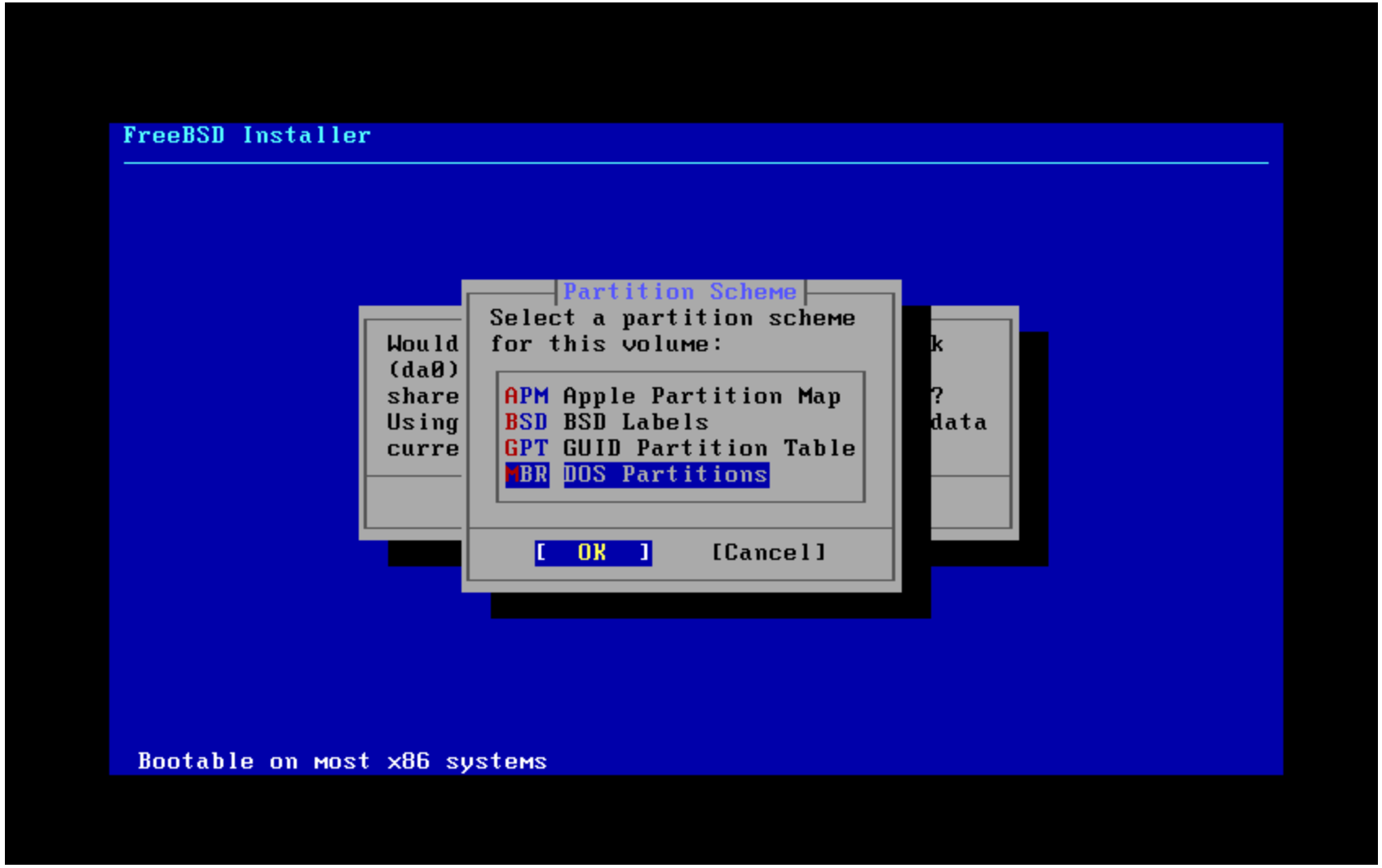
✓ Choisir Auto (UFS) Guided UFS Disk Setup



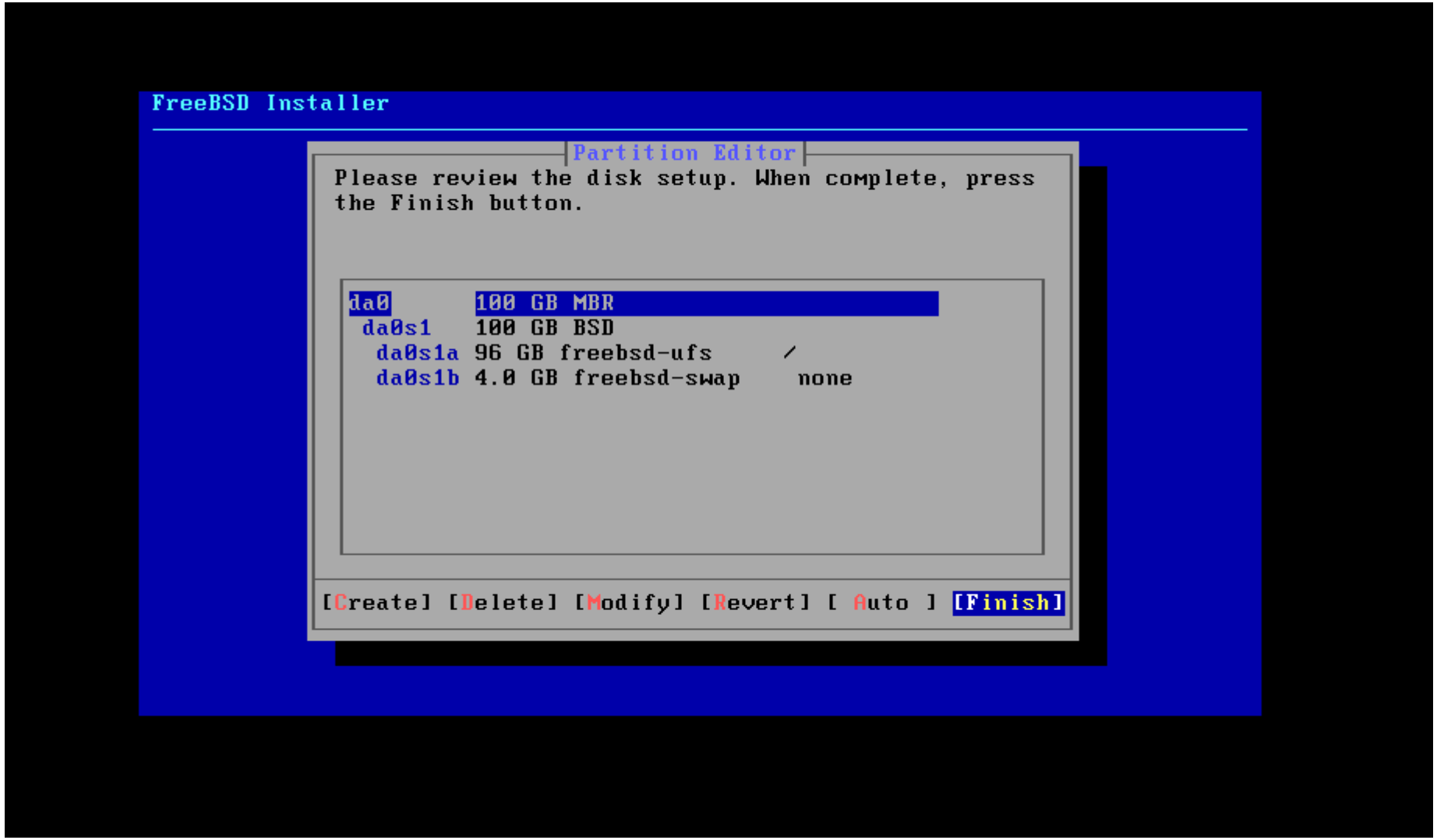
✓ Choisir Entire Disk



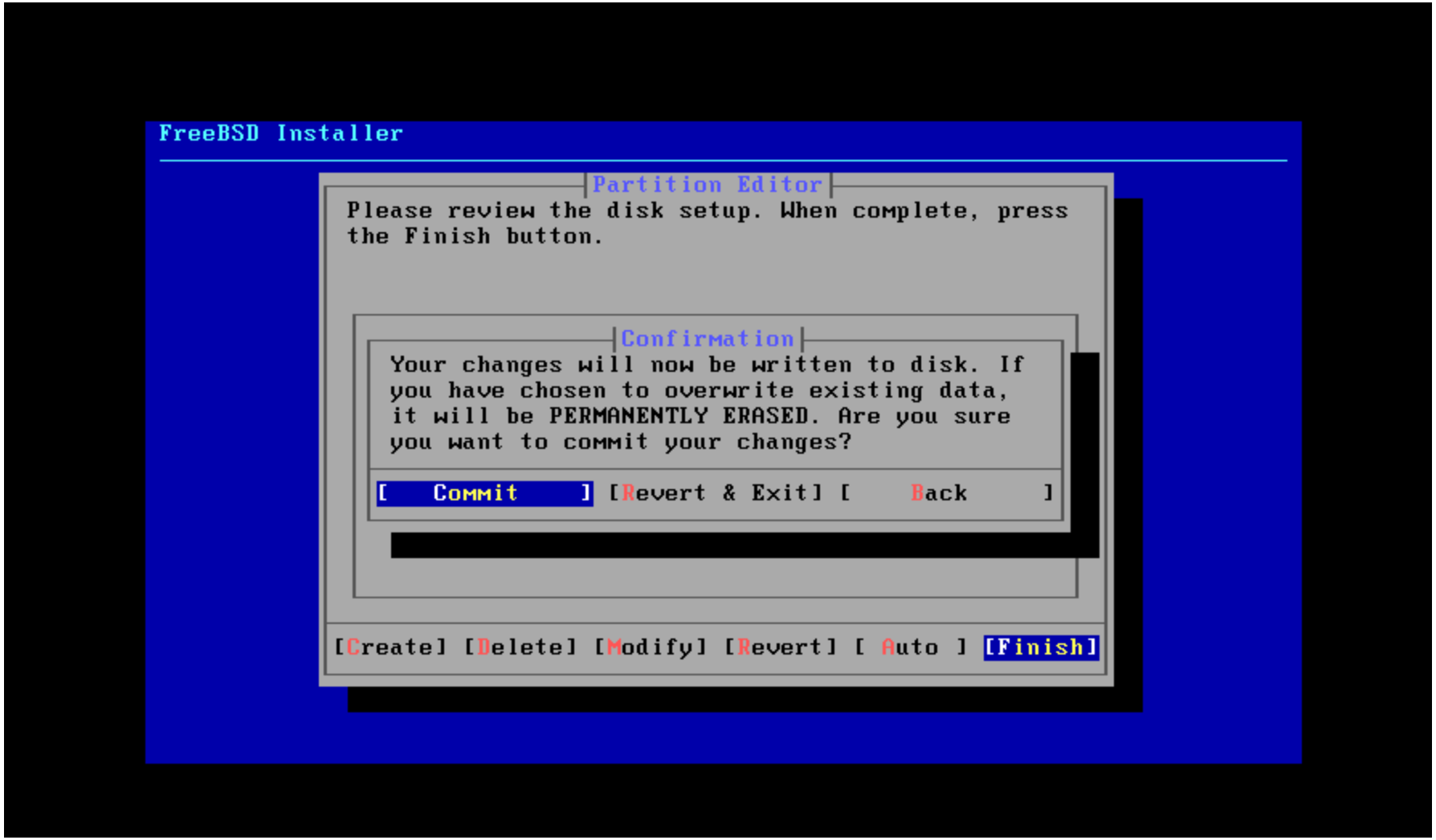
✓ Choisir BR DOS Partitions OK



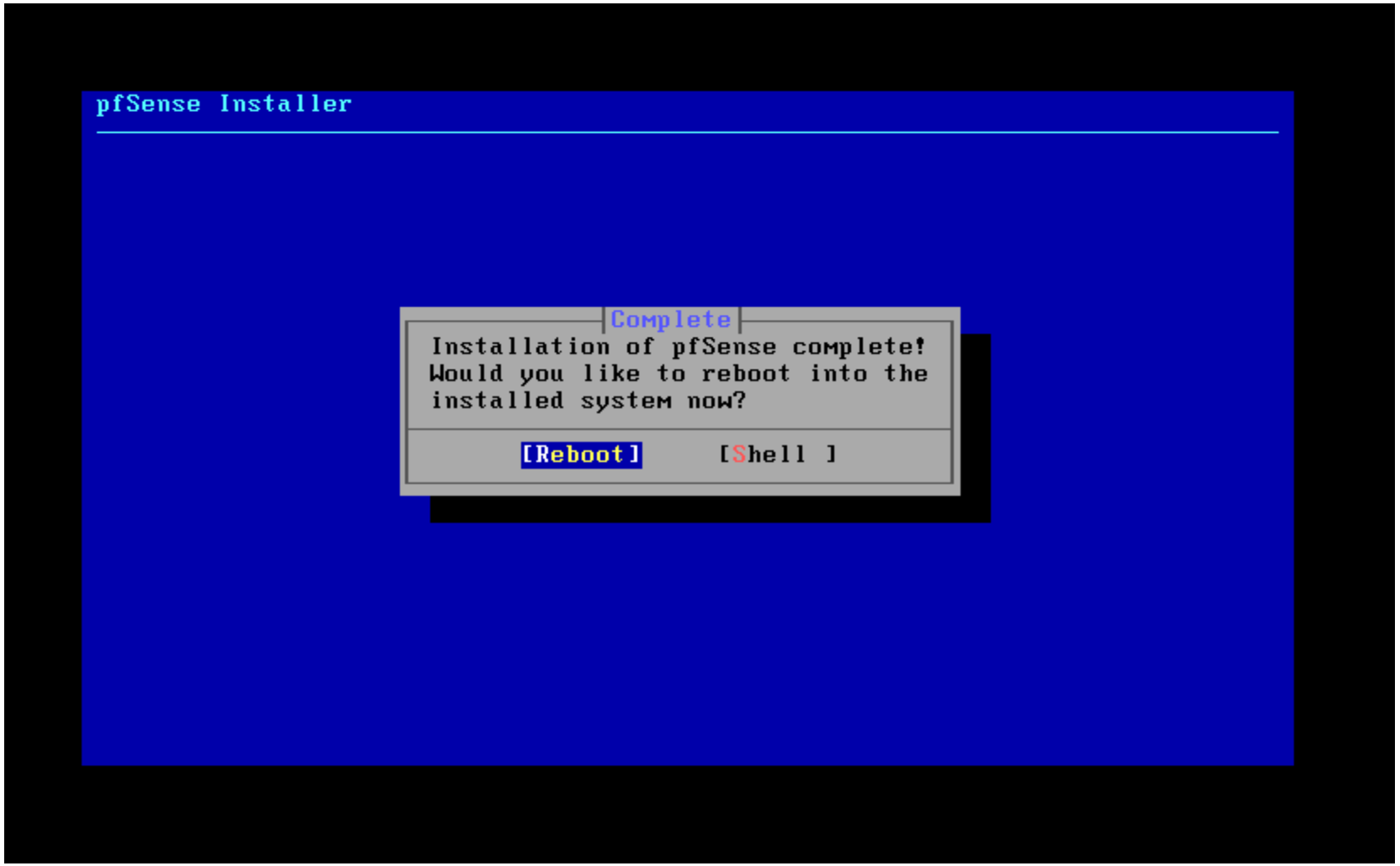
✓ Choisir (Finish)



✓ Confirmation [Commit]



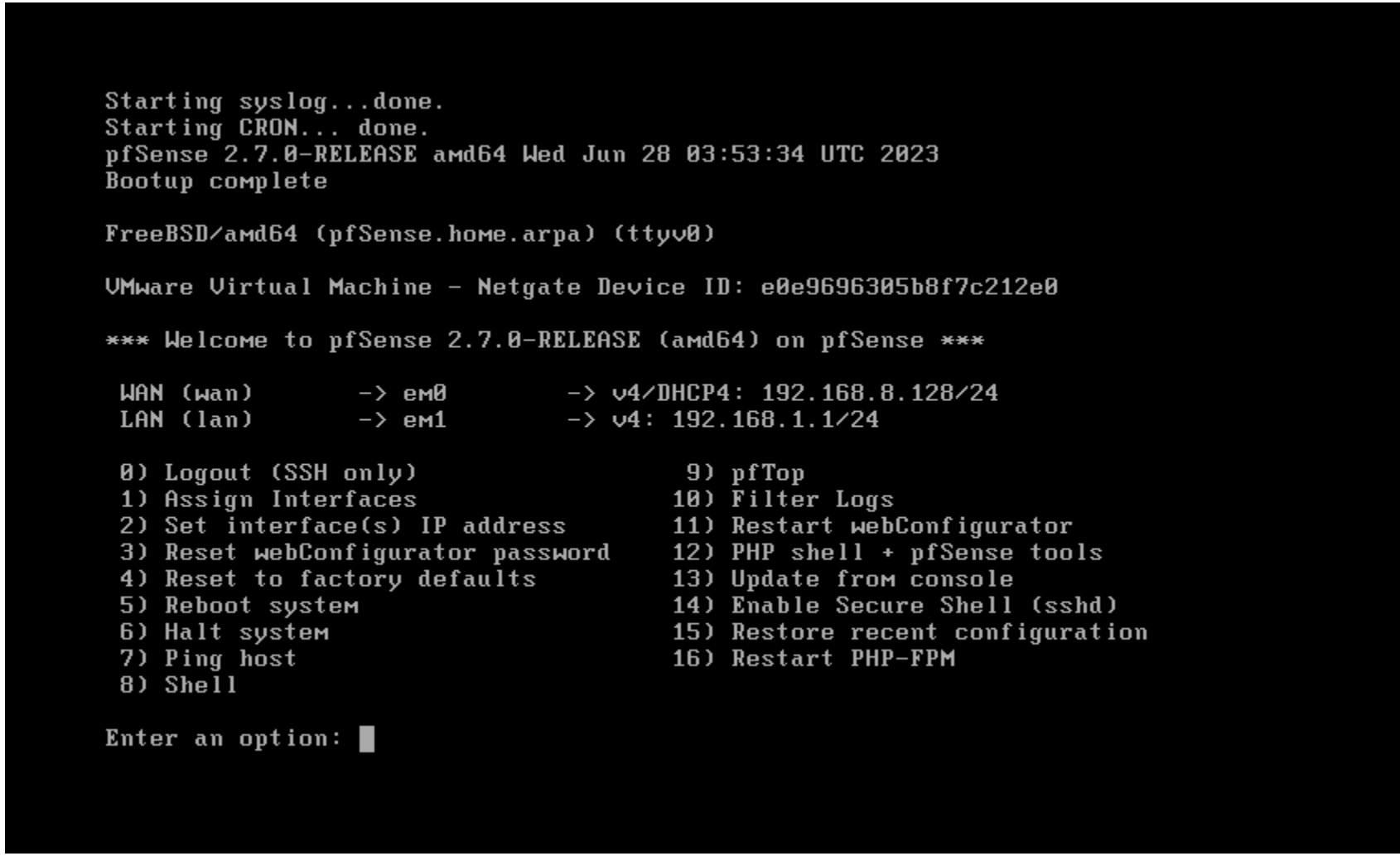
✓ Choisir Reboot



Affichage du Menu pfsense

Le WAN nous attribue une adresse ip automatique. Cette adresse est transmit par workstation, grâce à ça il nous permettra de naviguer sur internet

Le LAN attribue une adresse ip par défaut, dans cette situation il va savoir modifier l'adresse ip pour le LAN



Modification de l’adresse ip LAN
Nous avons un Menu de 16 Options

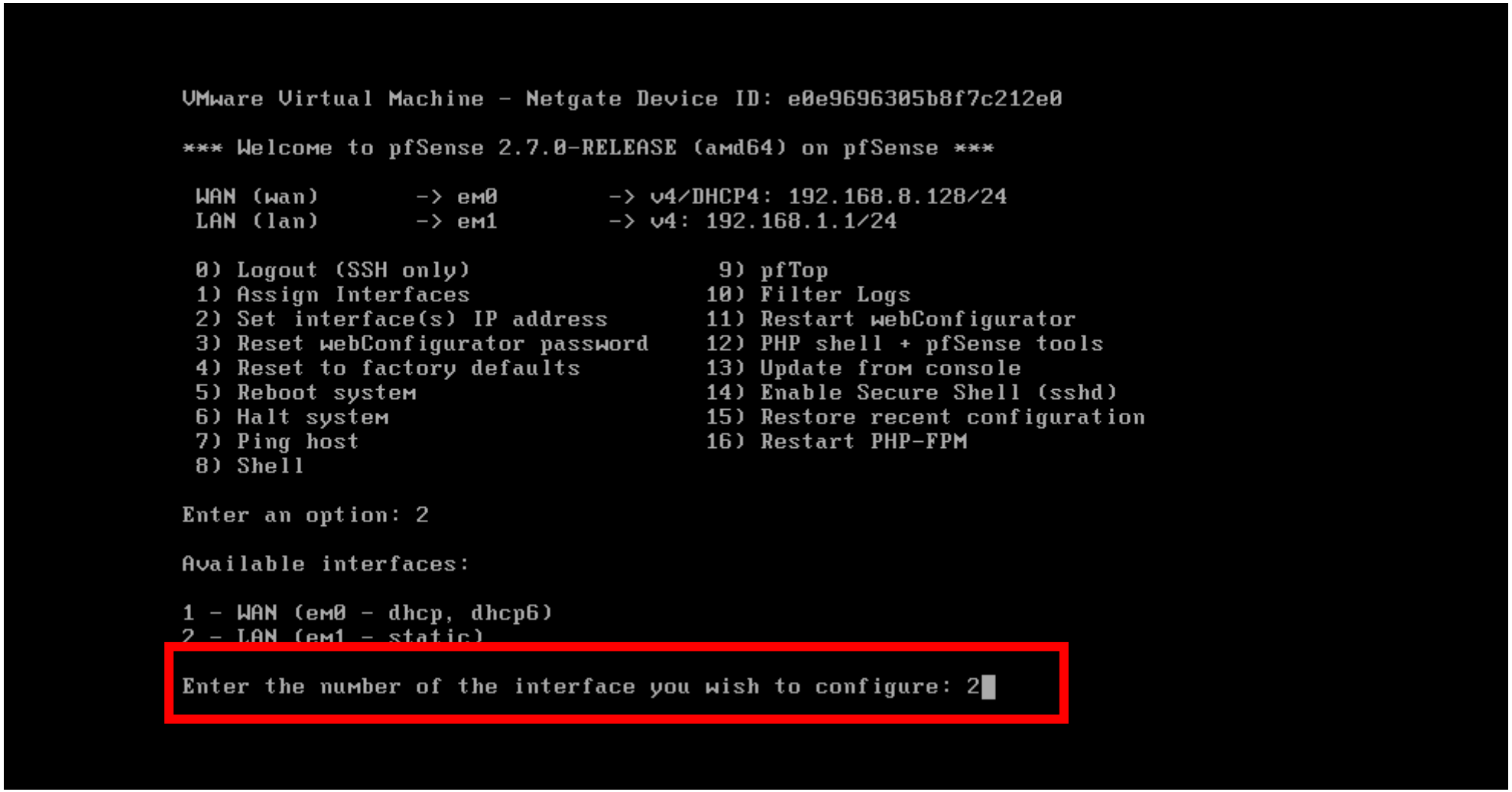
✓ Entrer l’option **2**

2) Set interface IP address

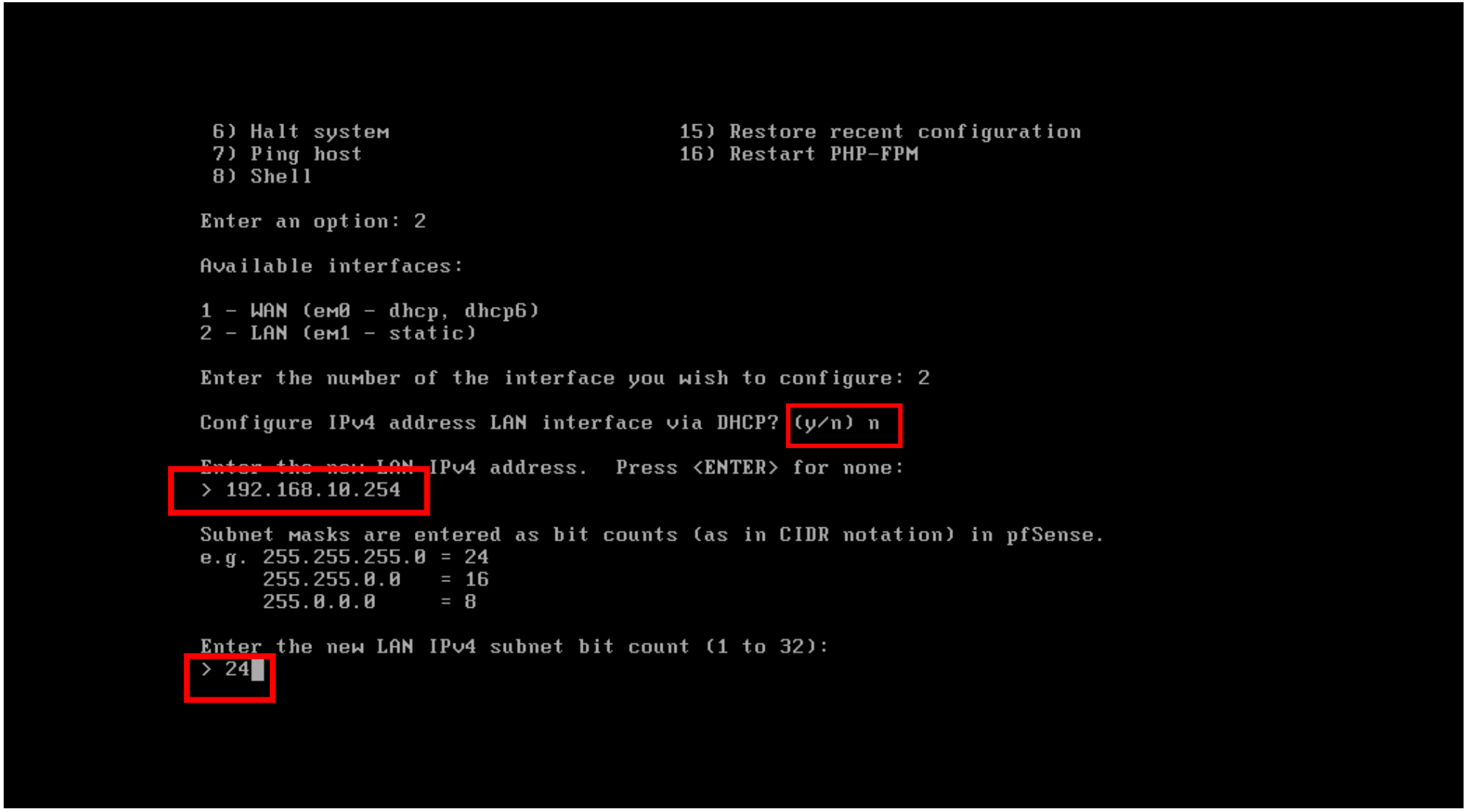
```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: e0e9696305b8f7c212e0

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.8.128/24
 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: 2
```

✓ **Choisir l'interface 2**

2 – LAN (em1 – static)

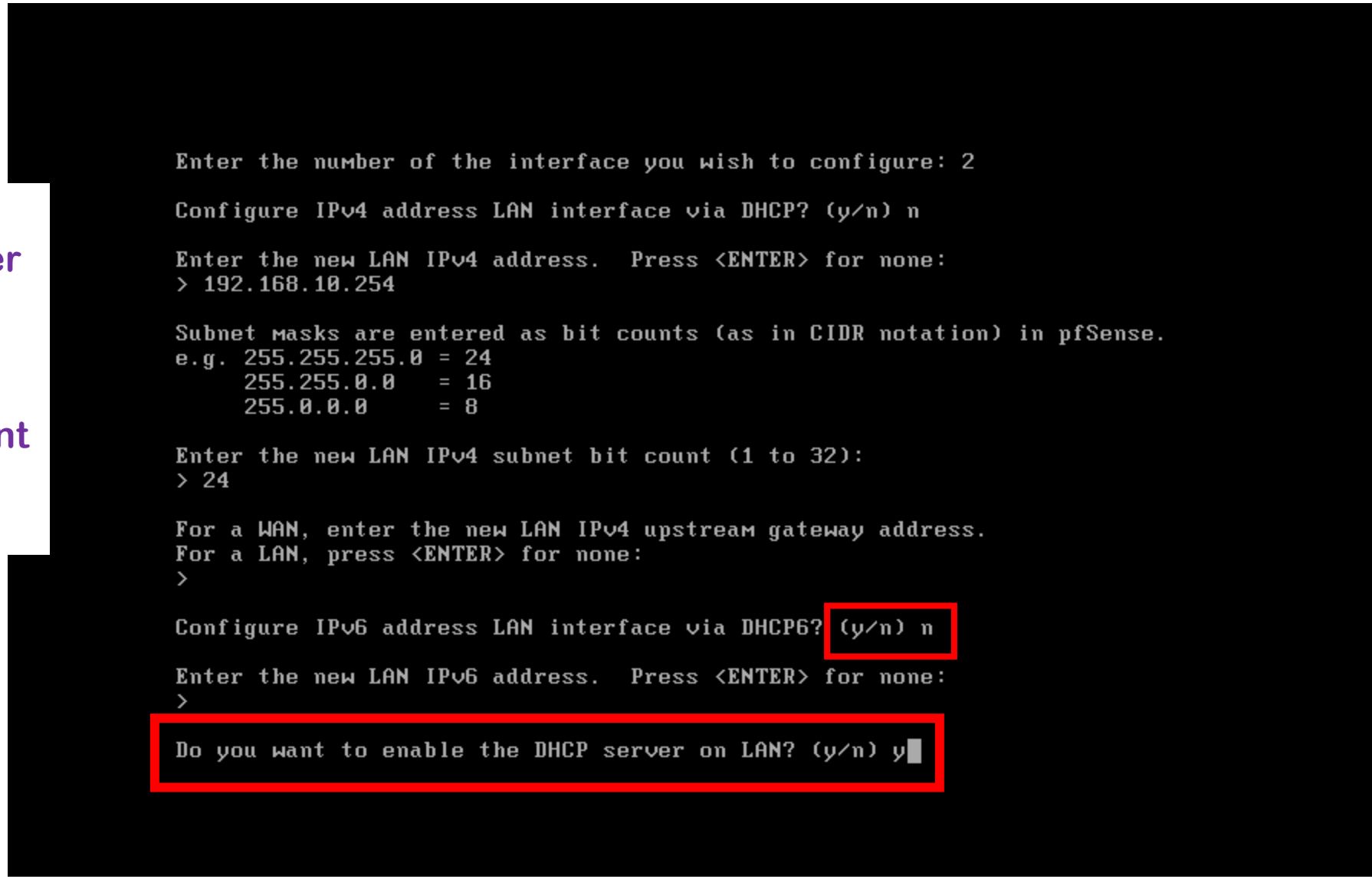


- ✓ Pour IPv4 DHCP choisir(y/n) n (non)
- ✓ Entrer une nouvelle adresse ip pour le LAN : 192.168.10.254
- ✓ Entrer le masque pour l'adresse ip : 24

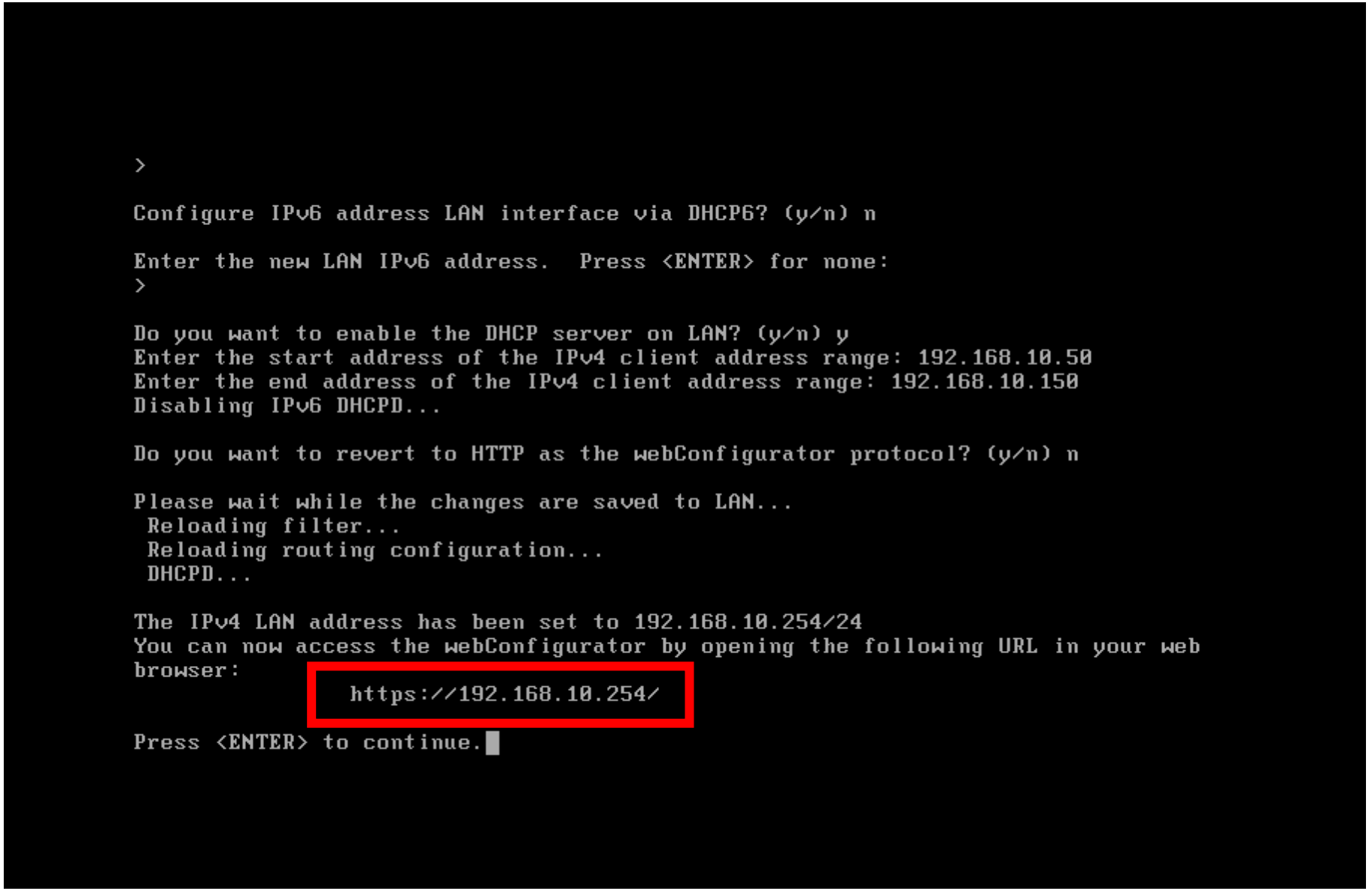


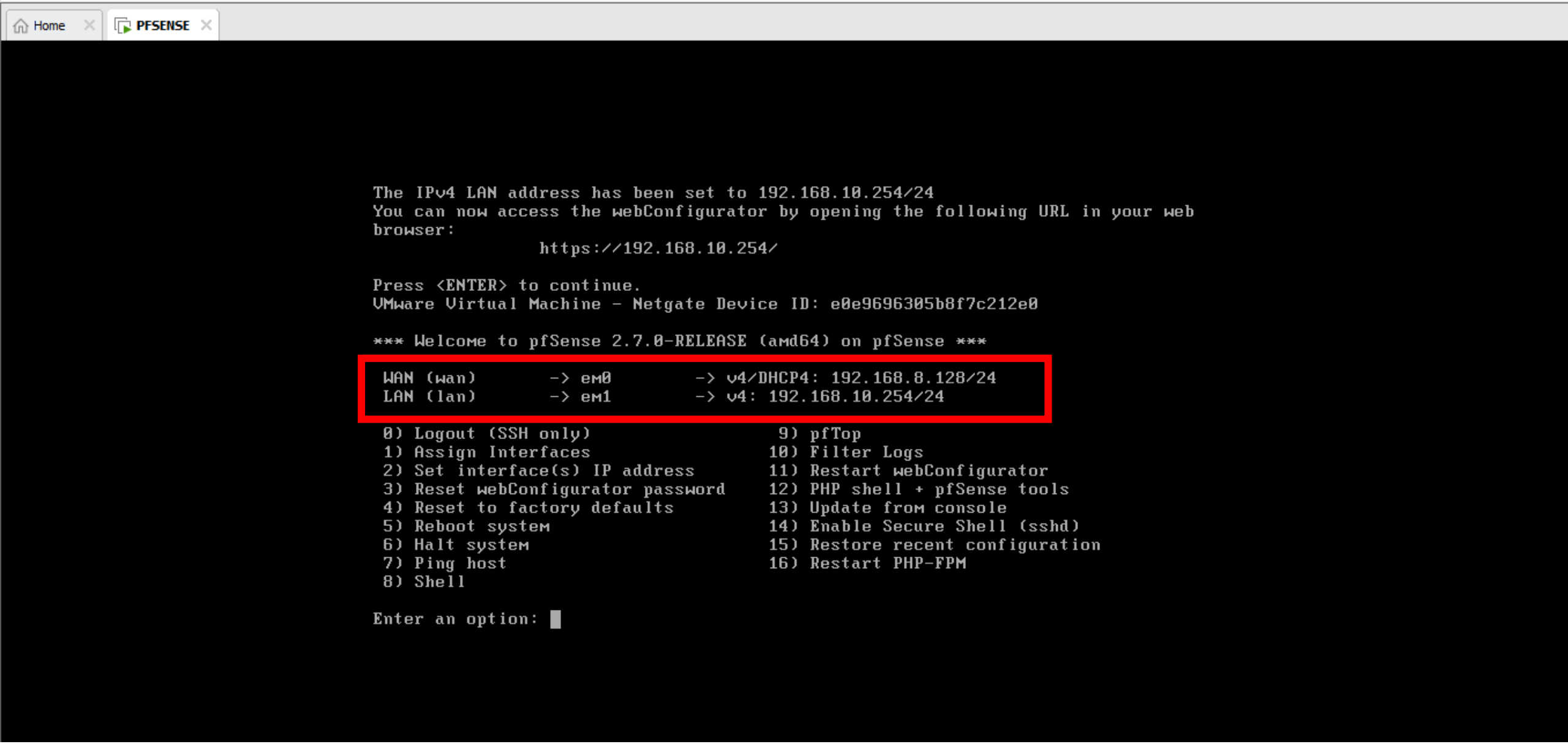
- ✓ IPv6 DHCP6 (y/n) n
- ✓ A cet étape il faudrait accepter l'attribution DHCP LAN (y/n) y

Parce que a notre niveau nous voulons que notre réseau LAN puisse attribuer automatiquement l'adresse ip aux machines qui seront dans le même résea



- ✓ A la fin une adresse ip s'affiche qui est https://192.168.10.254/
- ✓ Cette adresse ip nous permettra d'accéder à l'interface web de pfsense

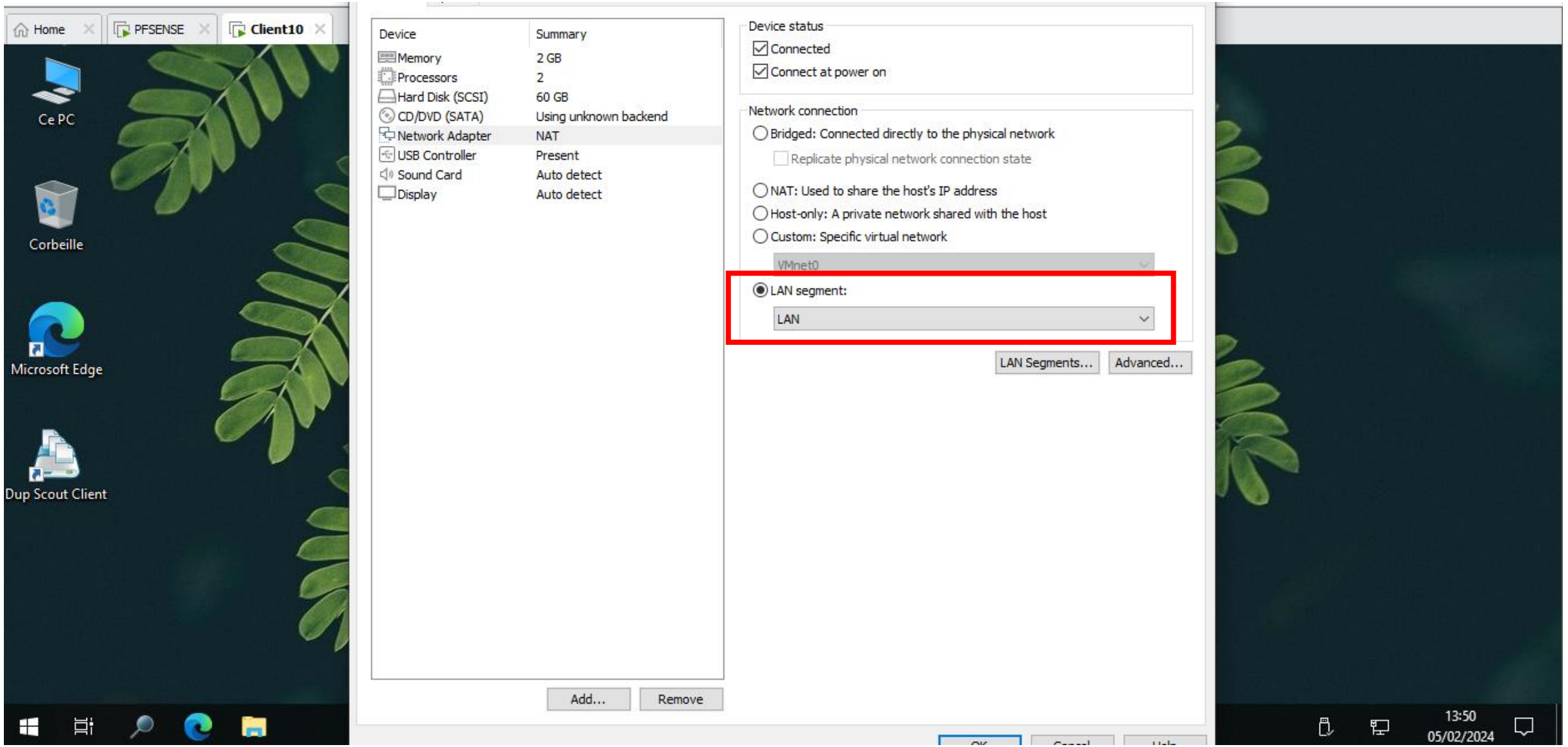



Home
PFSENSE
The IPv4 LAN address has been set to 192.168.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://192.168.10.254/
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: e0e9696305b8f7c212e0
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.8.128/24
LAN (lan) -> em1 -> v4: 192.168.10.254/24
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
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

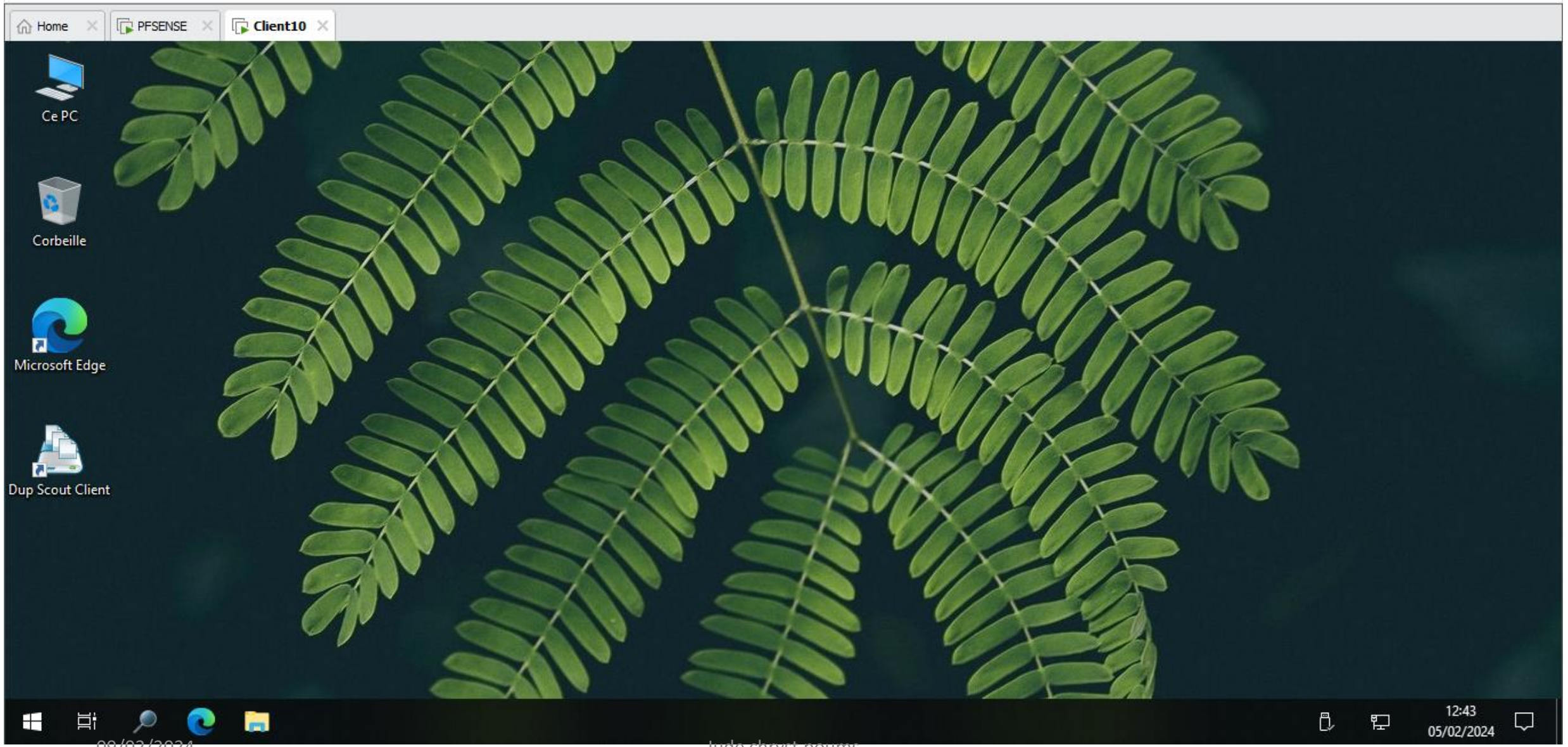
MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

✓ Vérifier que nous machine windows 10 sa carte réseau est bien dans le réseau LAN

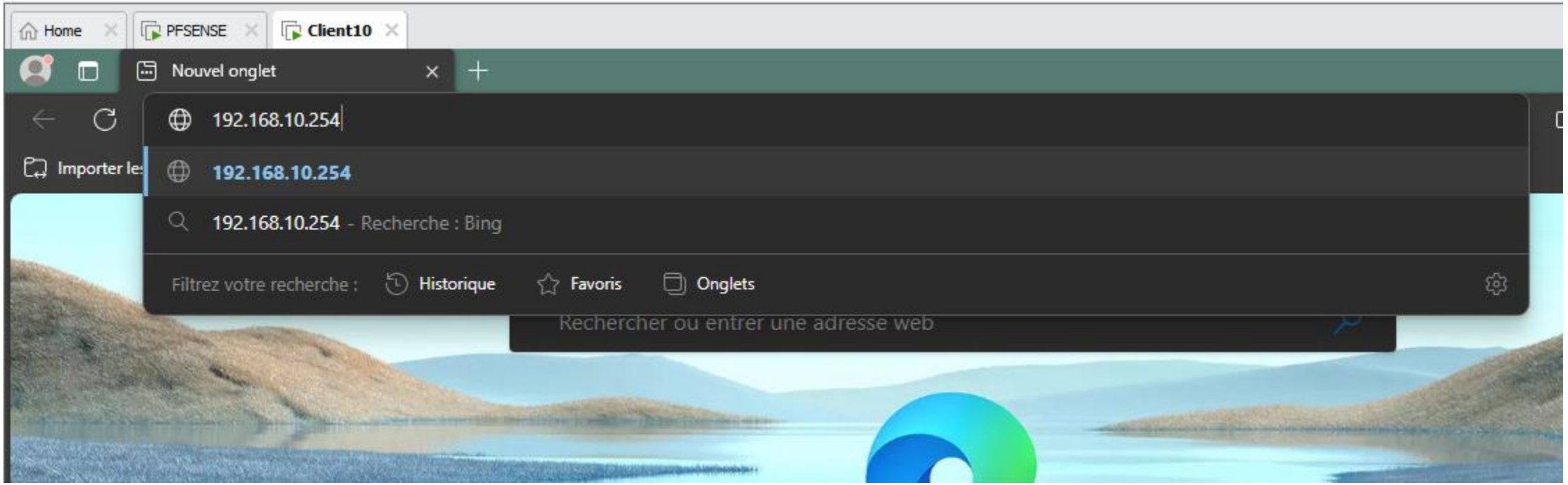


- ✓ Démarrer une machine windows 10
- ✓ Vérifier on adresse ip

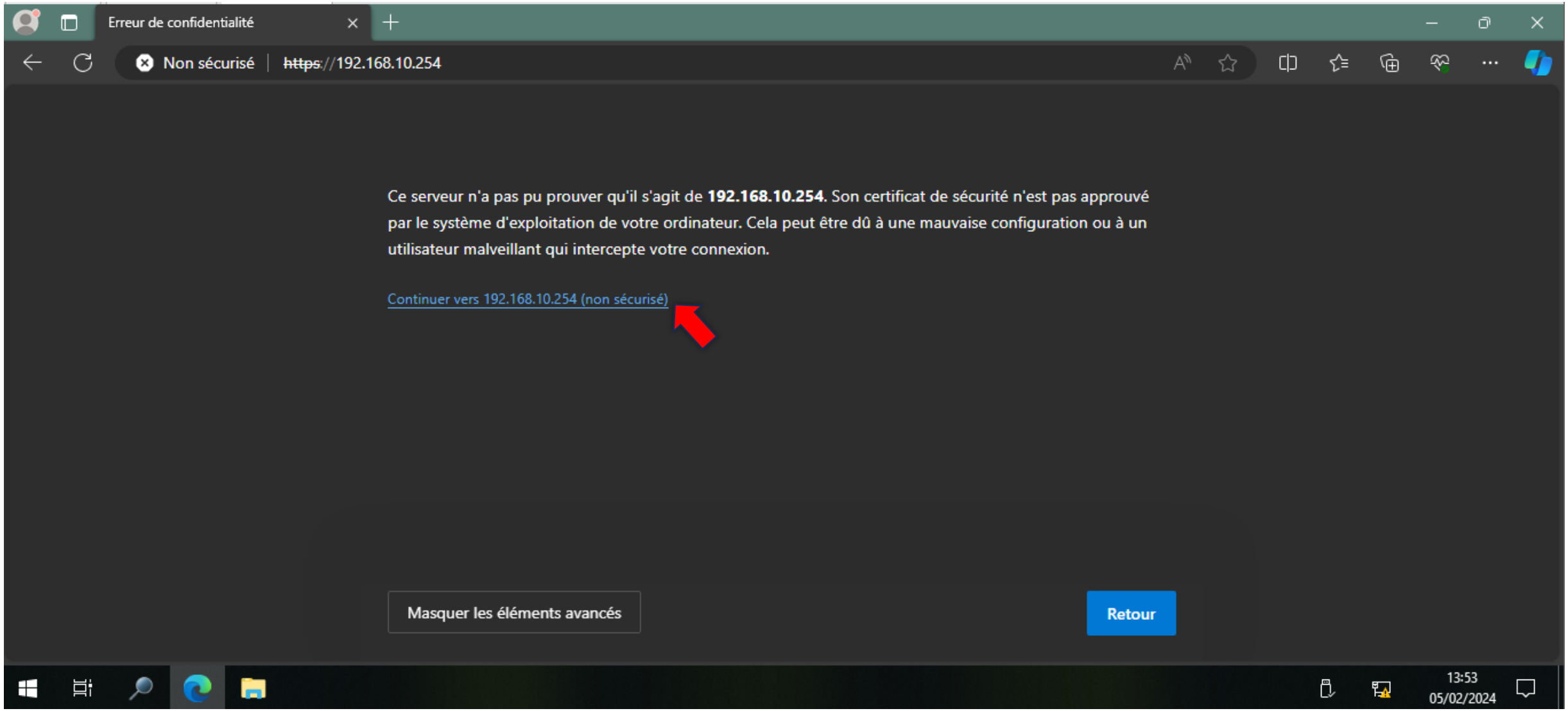


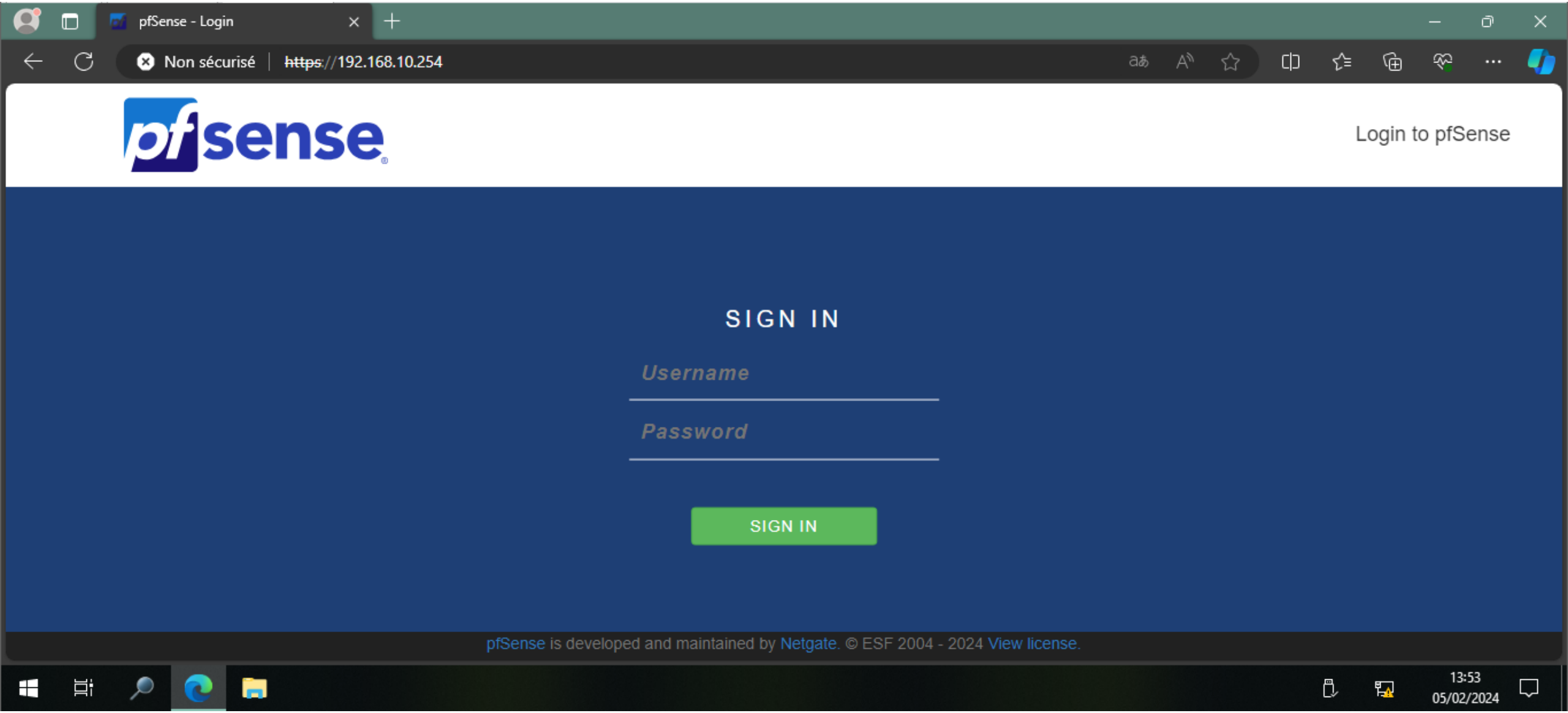
✓ **Etape 2 : Connexion au firewall pfsense pour ca configuration**

Dans la barre de recherche tapez : 192.168.10.254



✓ Cliquer sur continuer vers 192.168.10.254 (non sécurisé)



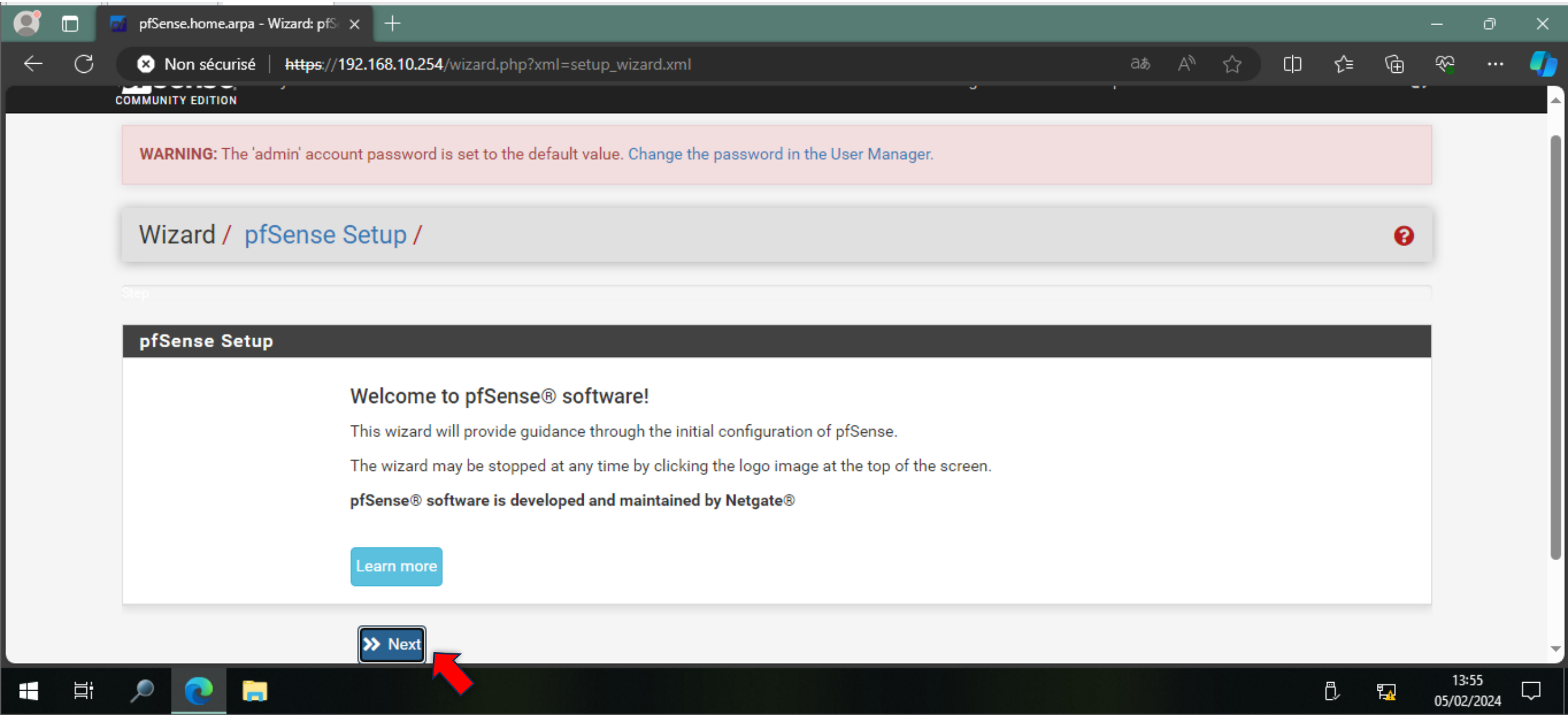

pfSense - Login
Non sécurisé
https://192.168.10.254
pfsense
Login to pfSense
SIGN IN
Username
Password
SIGN IN
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
13:53
05/02/2024

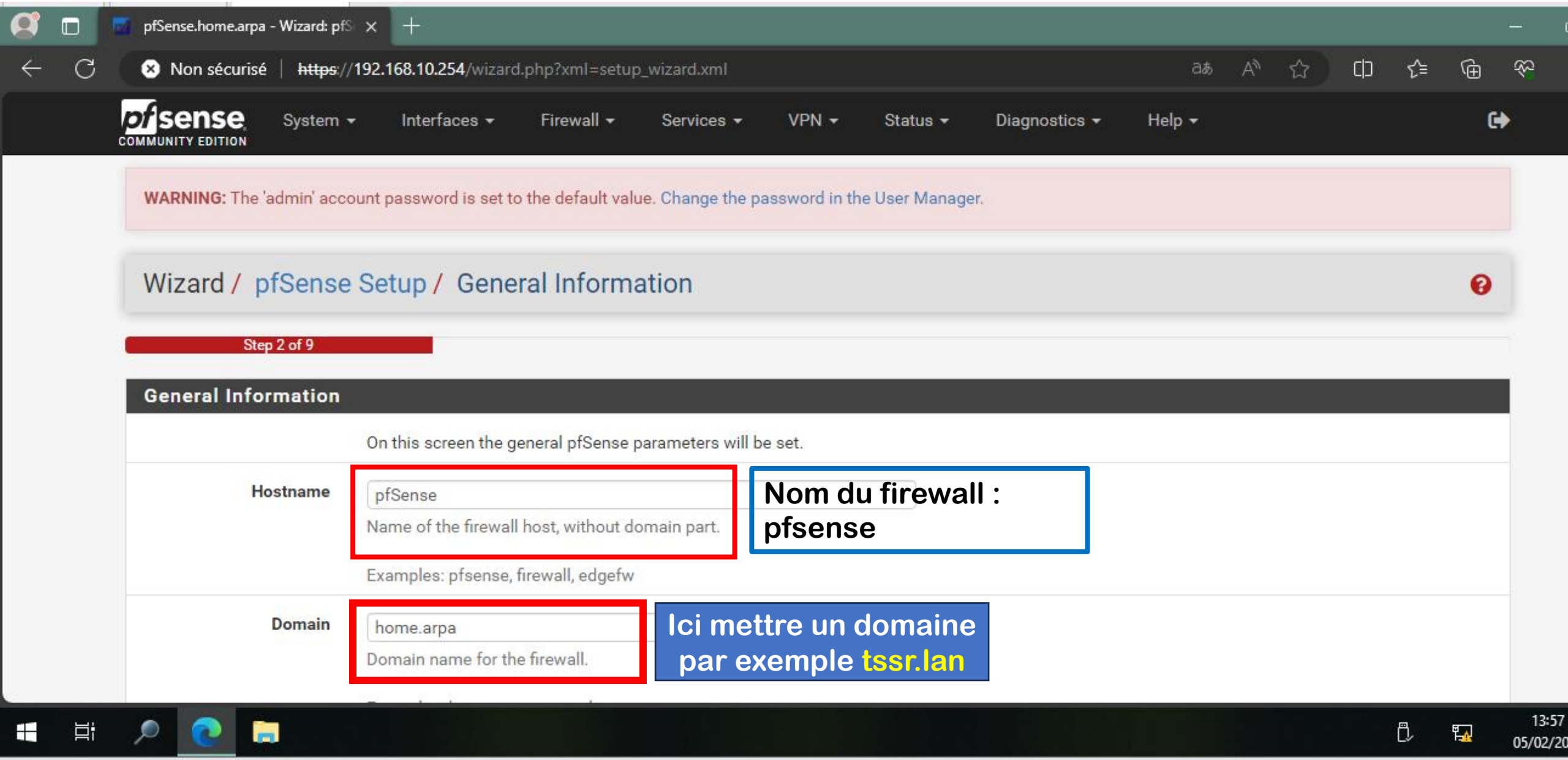
Login to pfSe

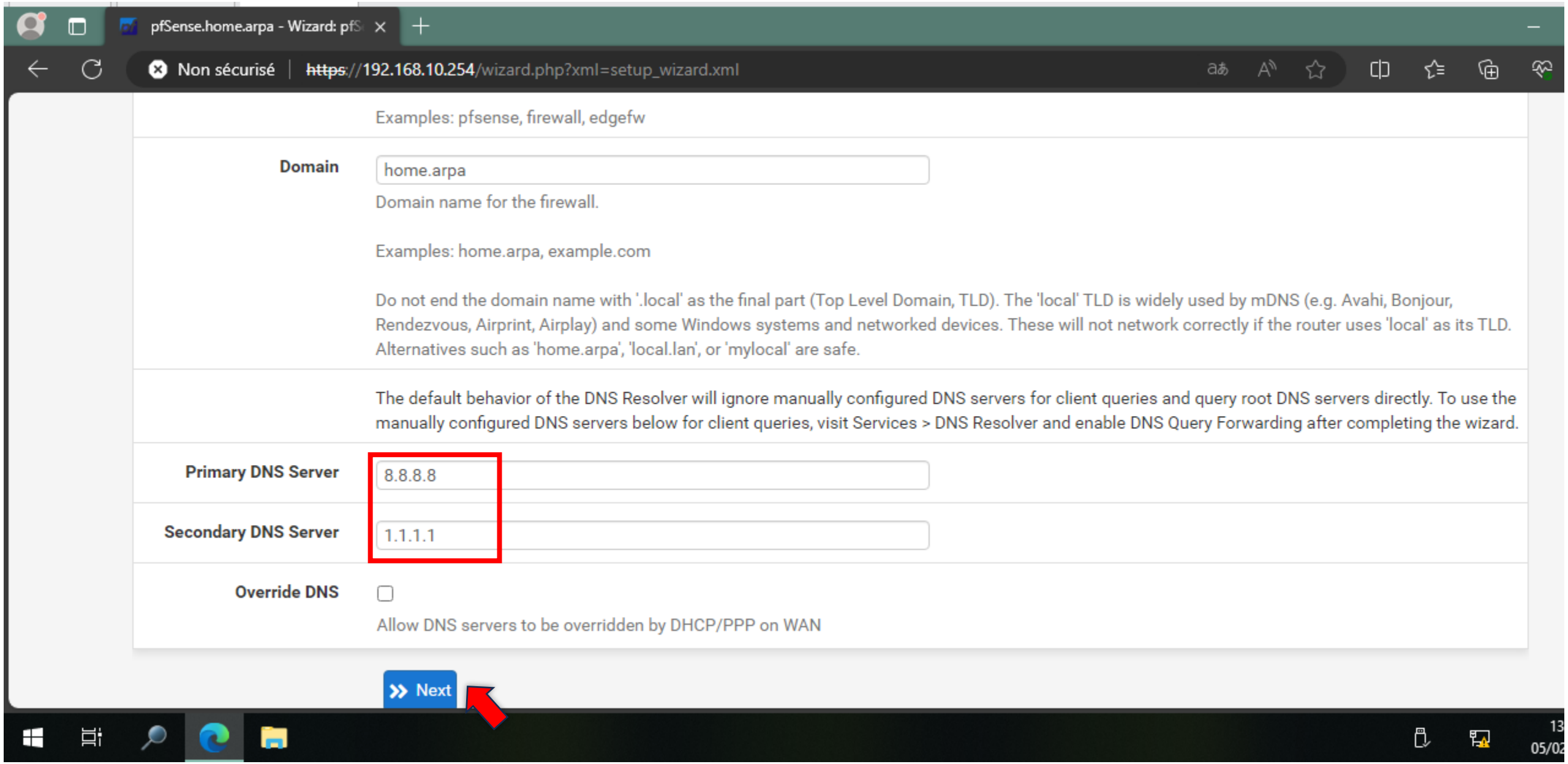
✓ **Sur pfsense la connexion de la session d'ouverture par défaut est**

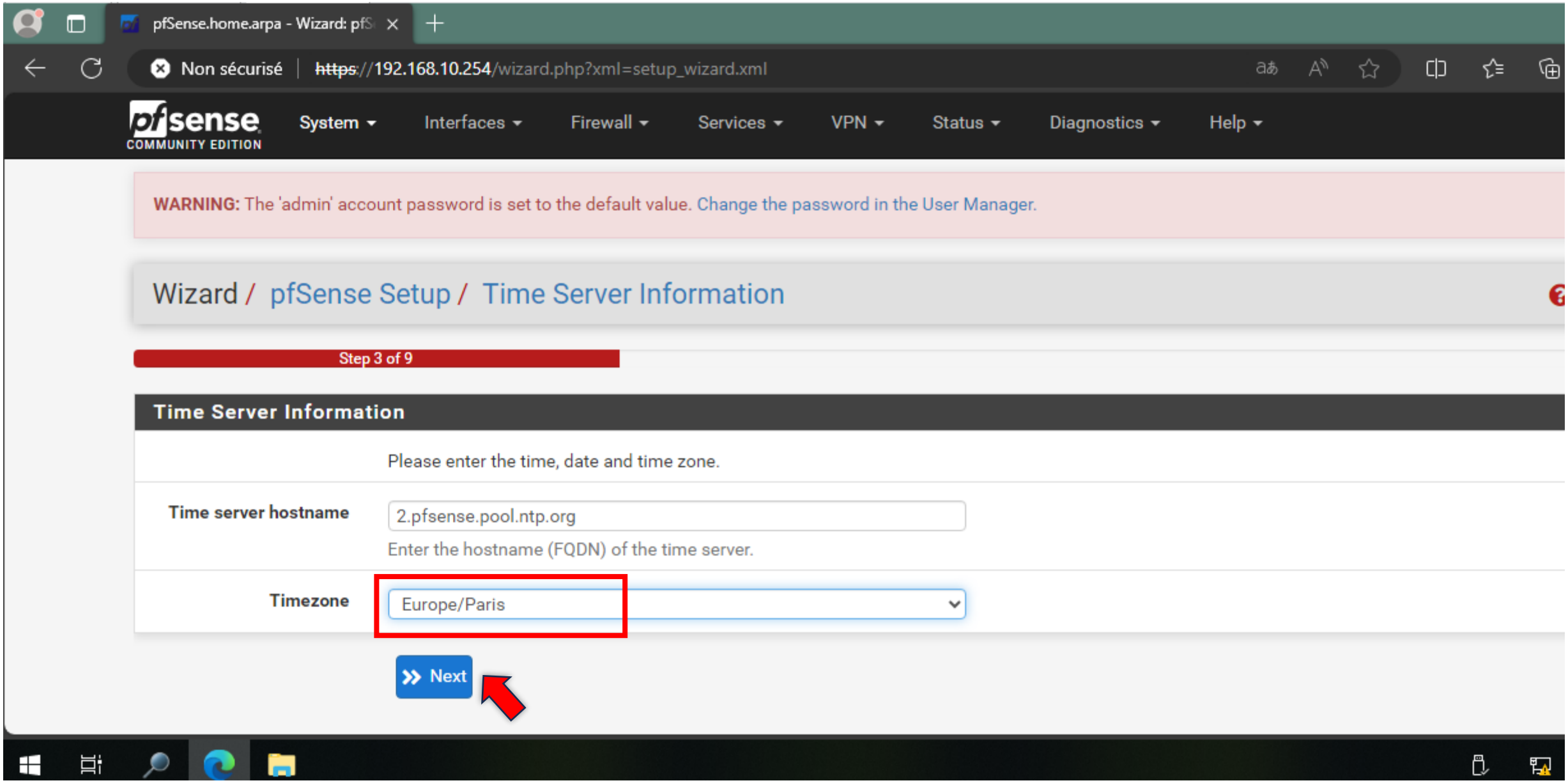
Username : **admin**

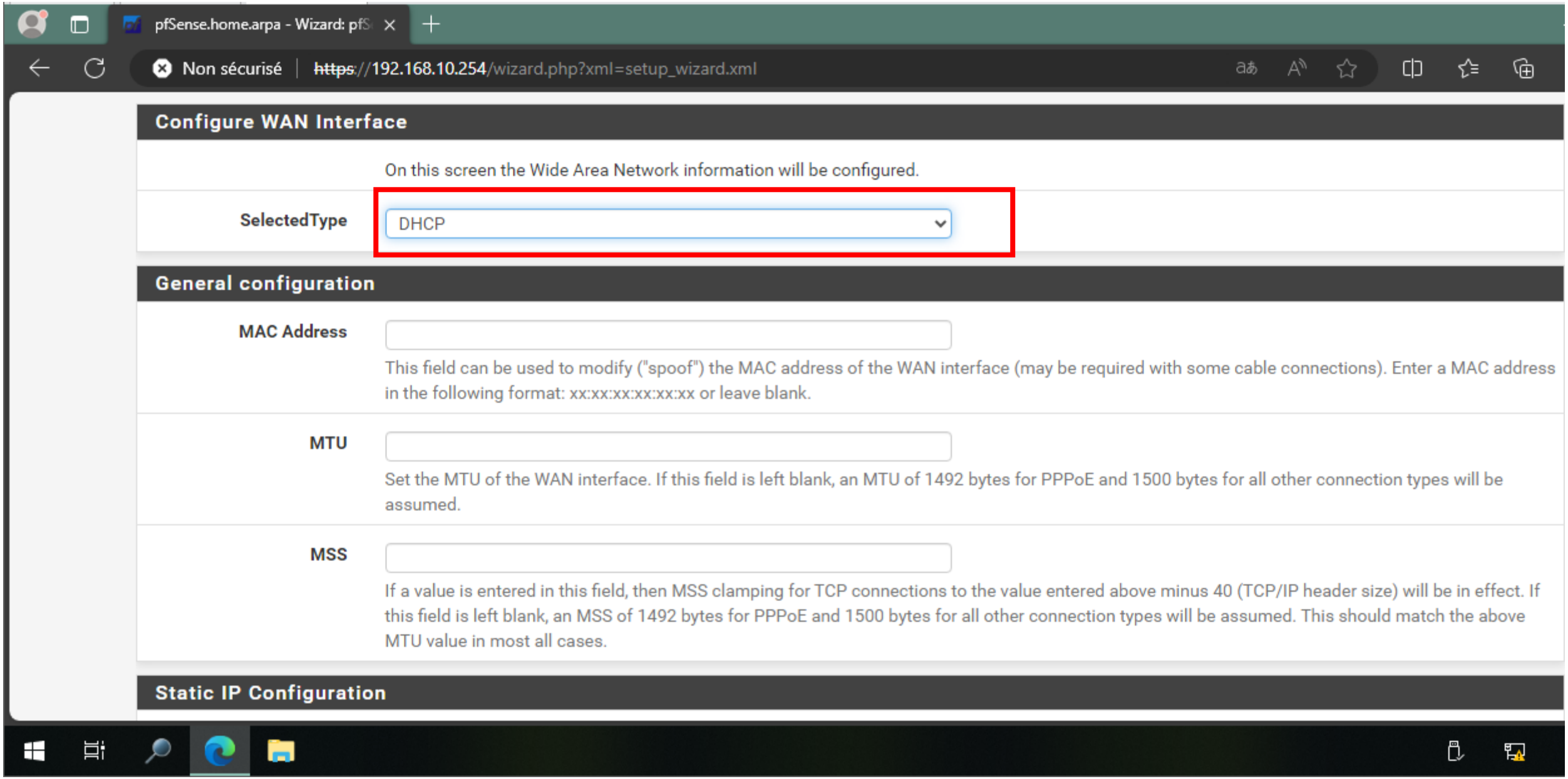
Mot de passe : **pfsense**

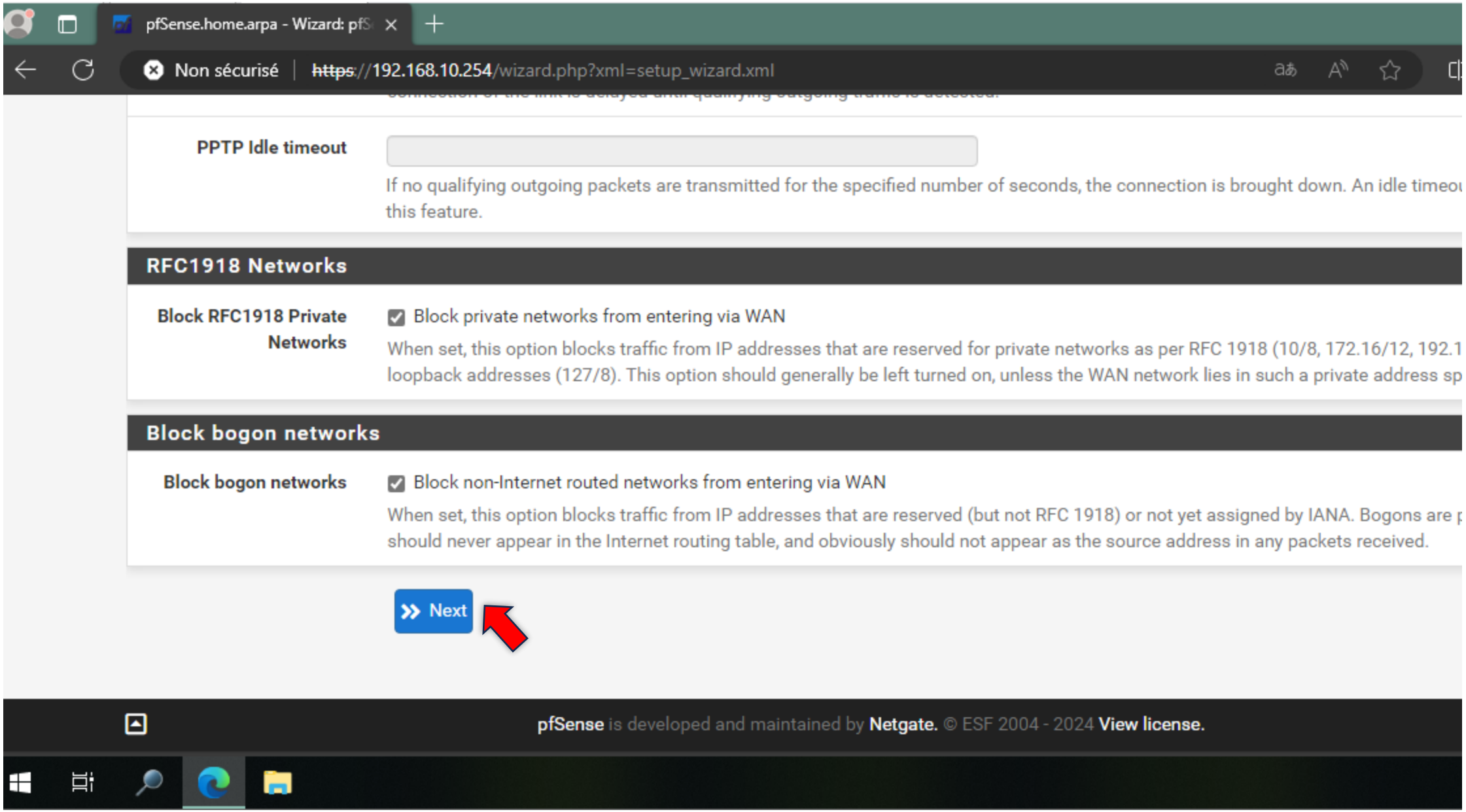

pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
COMMUNITY EDITION
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup /
pfSense Setup
Welcome to pfSense® software!
This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
pfSense® software is developed and maintained by Netgate®
Learn more
Next
13:55
05/02/2024

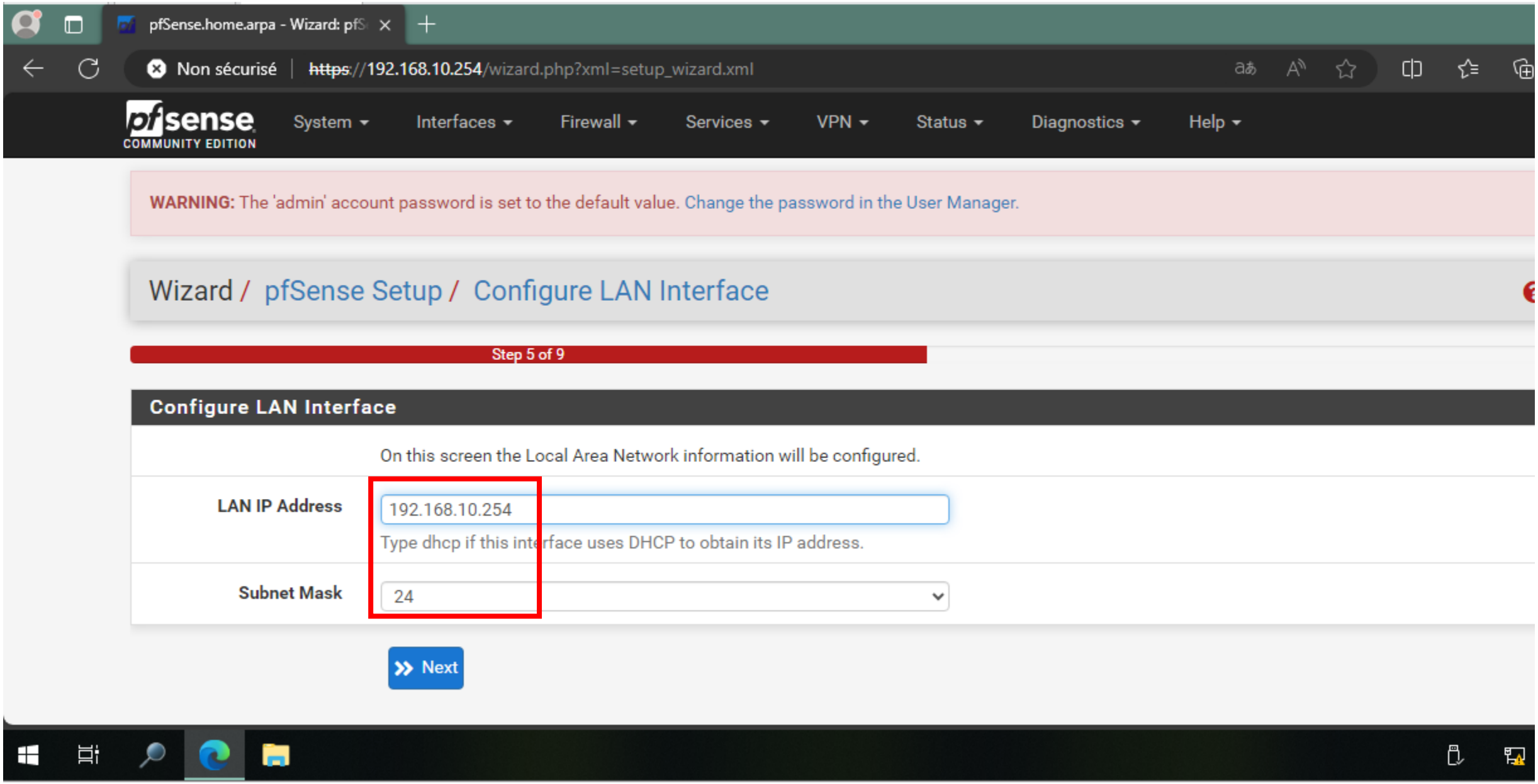

pfSense.home.arpa - Wizard: pfS
Non sécurisé | https://192.168.10.254/wizard.php?xml=setup_wizard.xml
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / General Information
Step 2 of 9
General Information
On this screen the general pfSense parameters will be set.
Hostname
pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw
Nom du firewall : pfsense
Domain
home.arpa
Domain name for the firewall.
Ici mettre un domaine par exemple tssr.lan
13:57
05/02/20

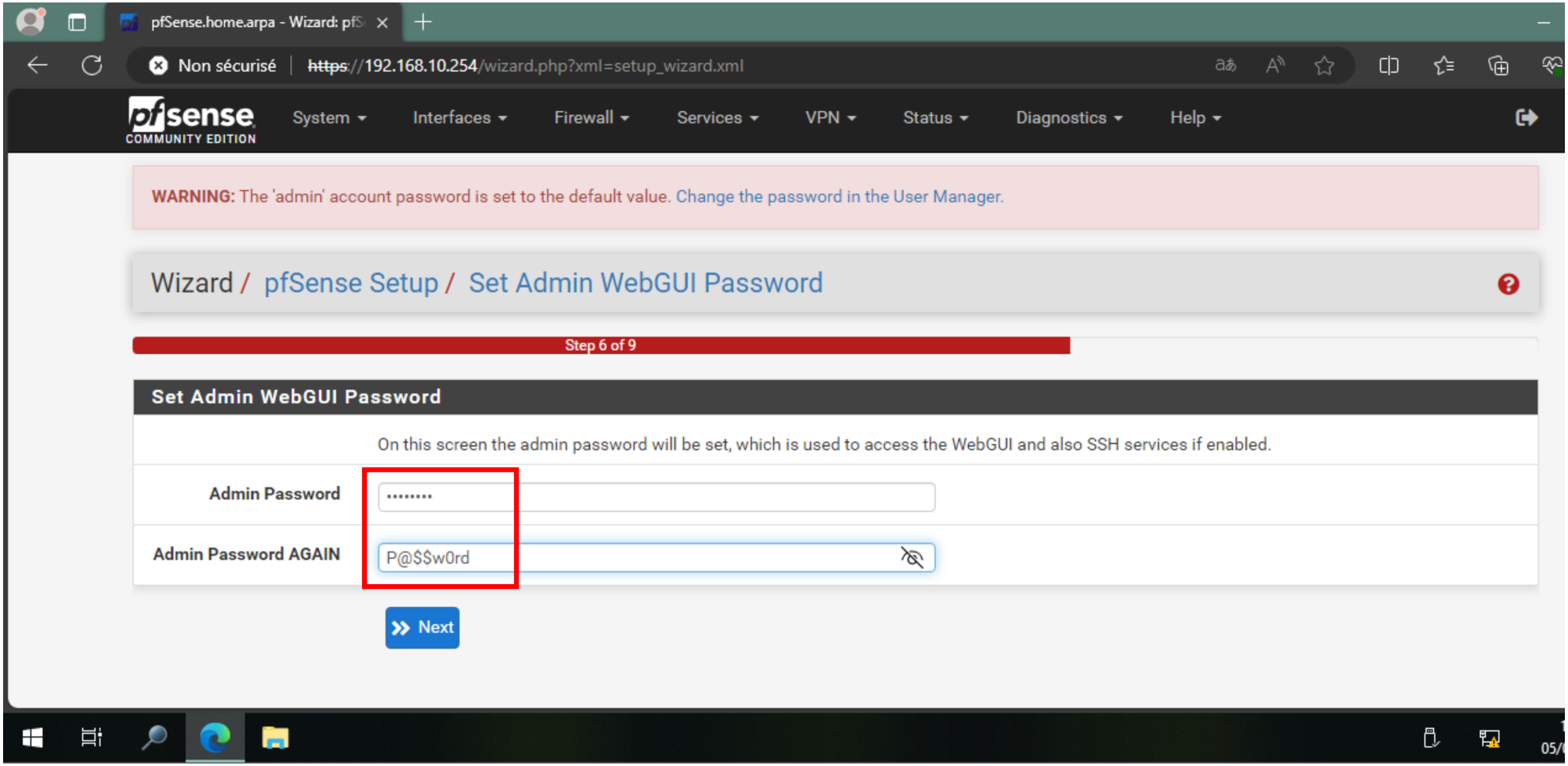

pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
Examples: pfsense, firewall, edgefw
Domain
home.arpa
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server
8.8.8.8
Secondary DNS Server
1.1.1.1
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN
Next

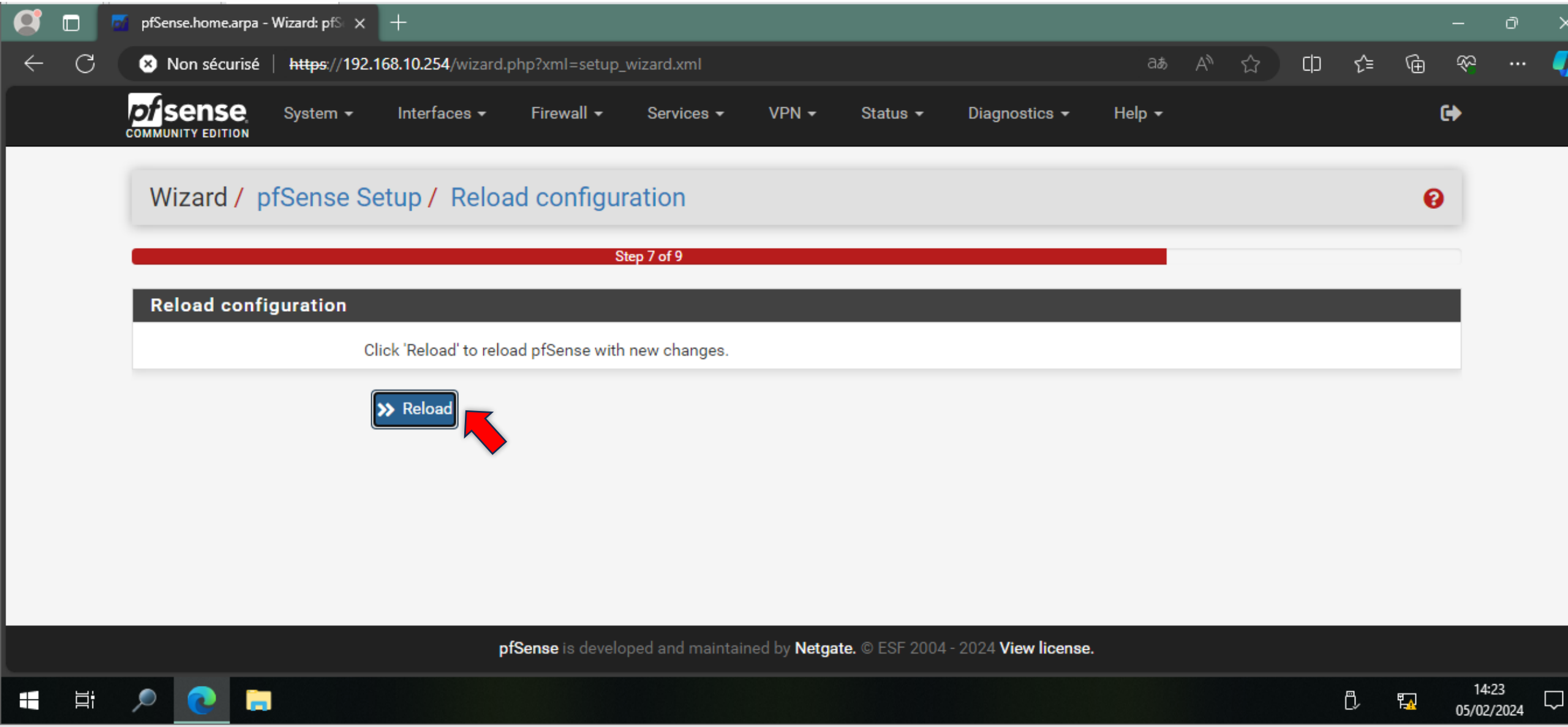

pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / Time Server Information
Step 3 of 9
Time Server Information
Please enter the time, date and time zone.
Time server hostname
2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.
Timezone
Europe/Paris
Next


pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
Configure WAN Interface
On this screen the Wide Area Network information will be configured.
SelectedType
DHCP
General configuration
MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.
Static IP Configuration


pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
PPTP Idle timeout
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeou
this feature.
RFC1918 Networks
Block RFC1918 Private Networks
Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.1
loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address sp
Block bogon networks
Block bogon networks
Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are p
should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.
Next
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / Configure LAN Interface
Step 5 of 9
Configure LAN Interface
On this screen the Local Area Network information will be configured.
LAN IP Address
192.168.10.254
Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask
24
Next


pfSense.home.arpa - Wizard: pfS
Non sécurisé | https://192.168.10.254/wizard.php?xml=setup_wizard.xml
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup / Set Admin WebGUI Password
Step 6 of 9
Set Admin WebGUI Password
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.
Admin Password
Admin Password AGAIN
P@$$w0rd
Next


pfSense.home.arpa - Wizard: pfS
Non sécurisé
https://192.168.10.254/wizard.php?xml=setup_wizard.xml
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Reload configuration
Step 7 of 9
Reload configuration
Click 'Reload' to reload pfSense with new changes.
Reload
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.
14:23
05/02/2024

pfSense.home.arpa - Wizard: pfS

Non sécurisé | https://192.168.10.254/wizard.php?xml=setup_wizard.xml&stepid=9

Check for updates

Remember, we're here to help.

Click here to learn about Netgate 24/7/365 support services.

User survey

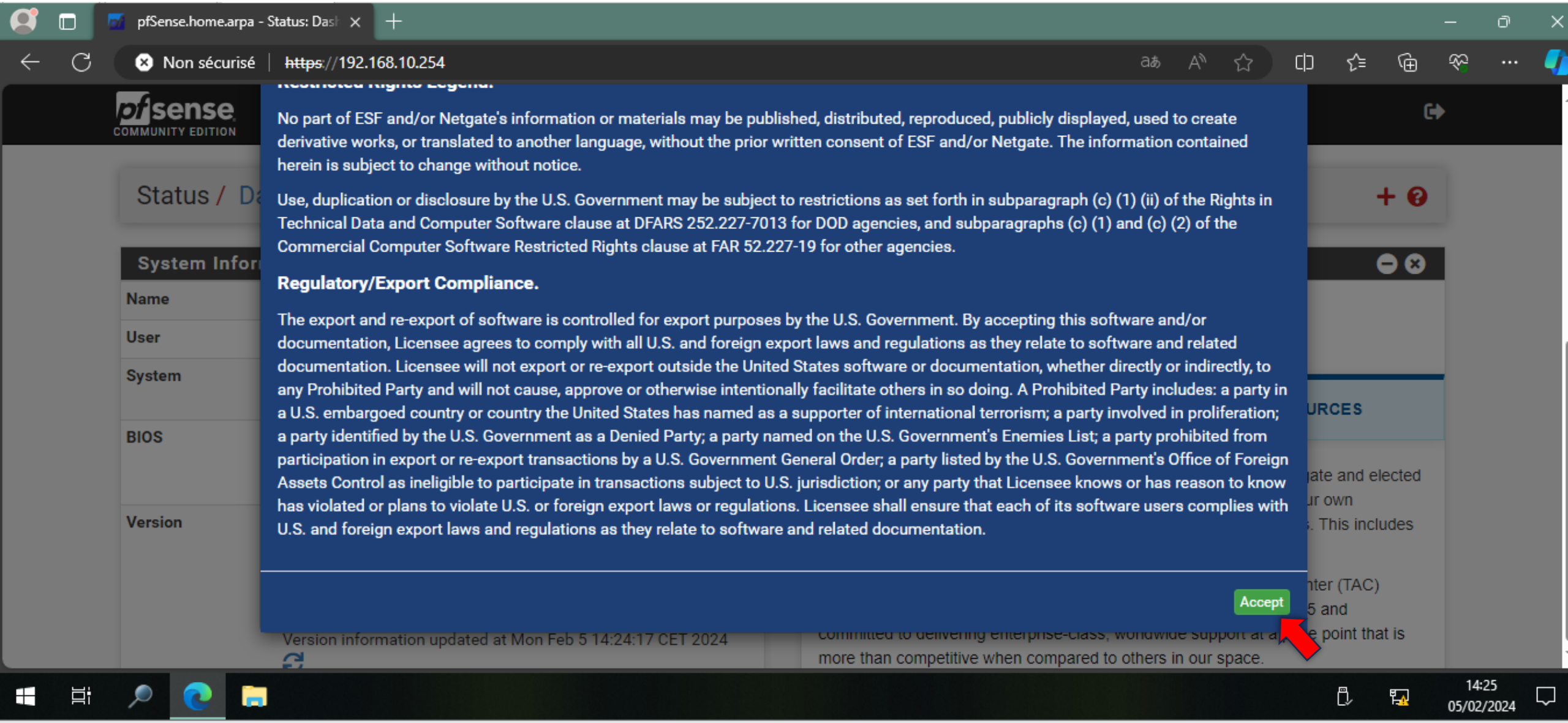
Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

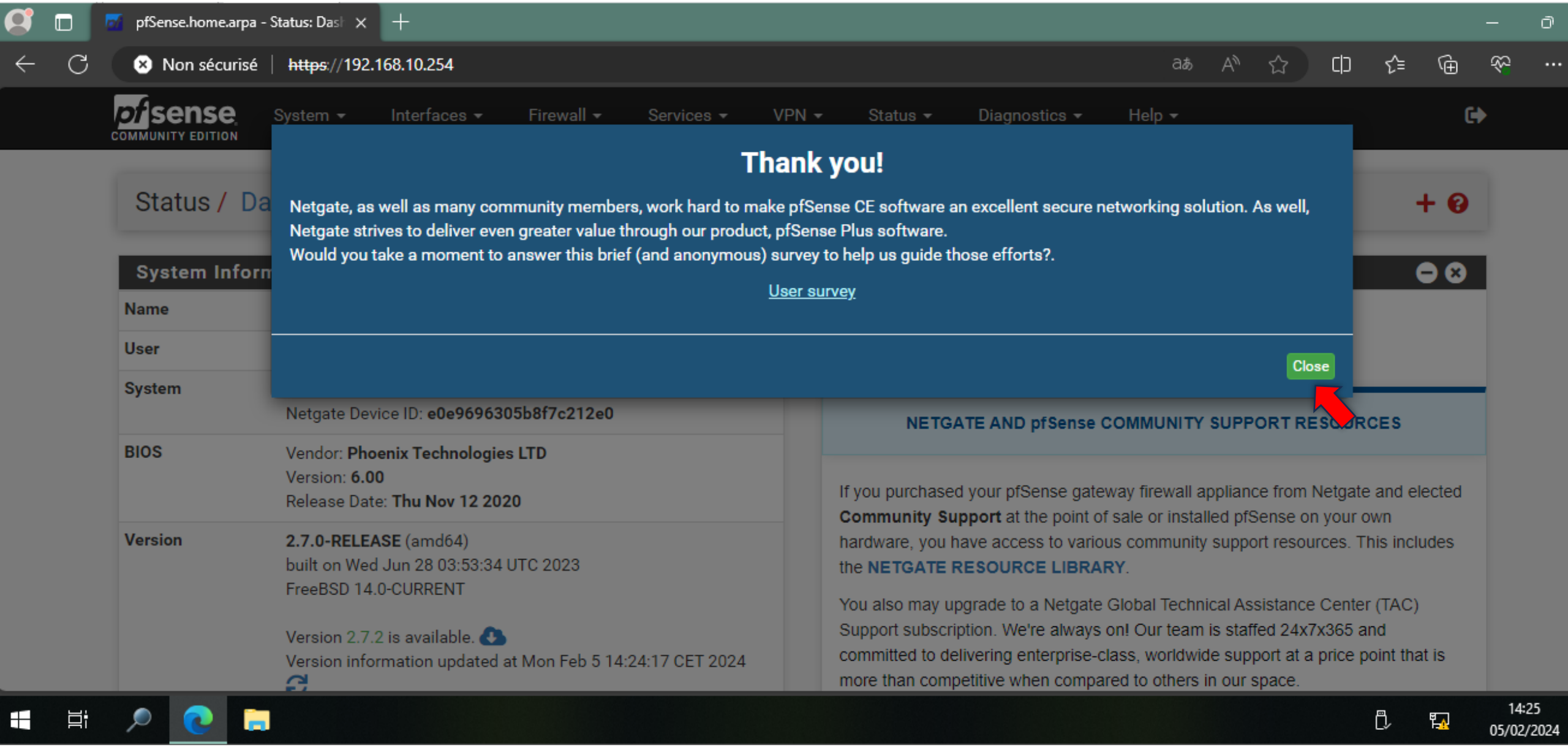
Anonymous User Survey

Useful resources.

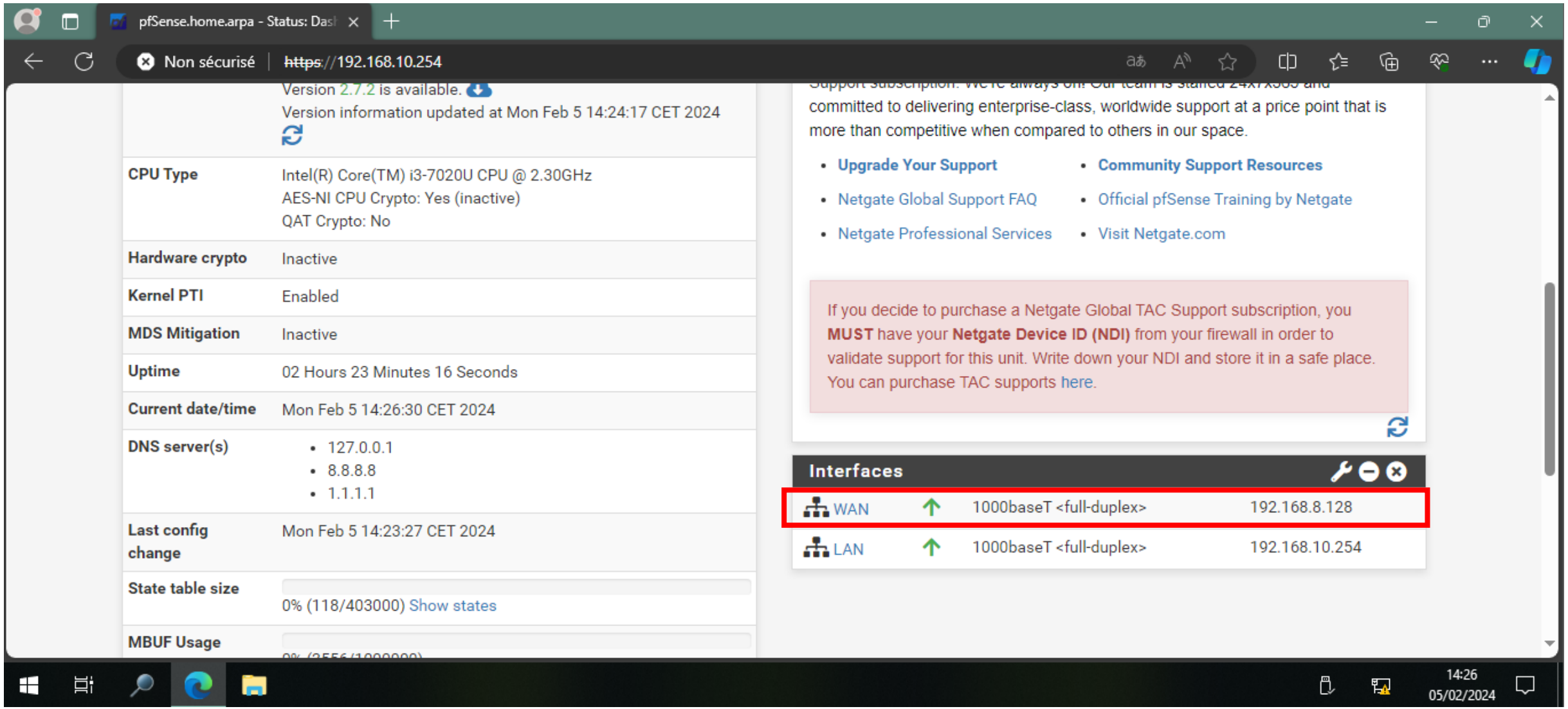
- **Learn more about Netgate's product line, services, and pfSense software from our website**
- **To learn about Netgate appliances and other offers, visit our store**
- **Become part of the pfSense community. Visit our forum**
- **Subscribe to our newsletter for ongoing product information, software announcements and special offers.**

Finish

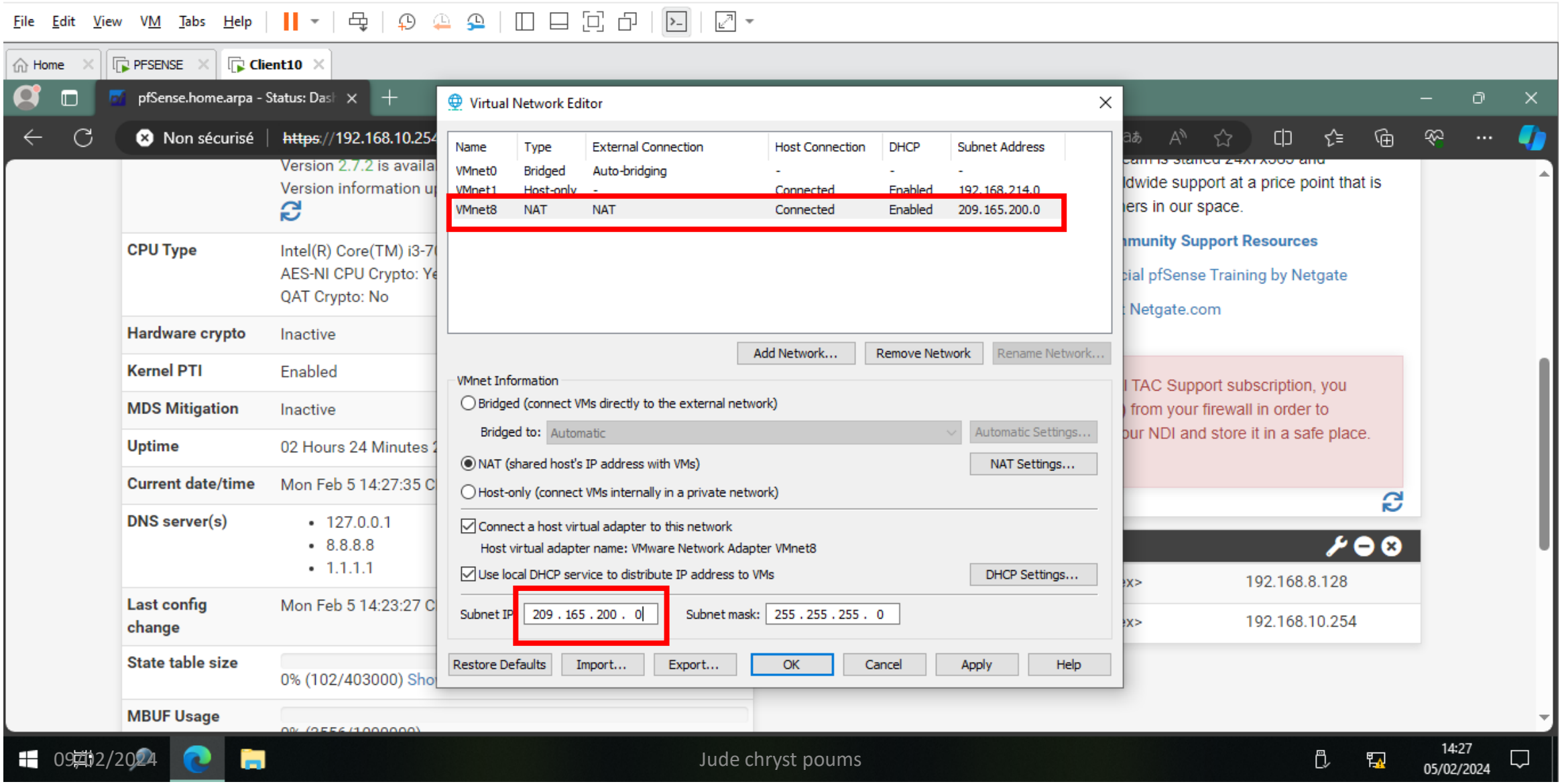

pfSense.home.arpa - Status: Dash
Non sécurisé
https://192.168.10.254
pfsense
COMMUNITY EDITION
No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.
Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.
Regulatory/Export Compliance.
The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.
Accept
Status / Da
System Infor
Name
User
System
BIOS
Version
Version information updated at Mon Feb 5 14:24:17 CET 2024
URCES
ate and elected
ur own
. This includes
nter (TAC)
5 and
e point that is
more than competitive when compared to others in our space.
14:25
05/02/2024


pfSense.home.arpa - Status: Dash
Non sécurisé
https://192.168.10.254
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Thank you!
Netgate, as well as many community members, work hard to make pfSense CE software an excellent secure networking solution. As well, Netgate strives to deliver even greater value through our product, pfSense Plus software.
Would you take a moment to answer this brief (and anonymous) survey to help us guide those efforts?.
User survey
Close
Status / Da
System Inform
Name
User
System
Netgate Device ID: e0e9696305b8f7c212e0
BIOS
Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Version
2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT
Version 2.7.2 is available.
Version information updated at Mon Feb 5 14:24:17 CET 2024
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.
14:25
05/02/2024

Nous allons créer une adresse ip publique afin de simuler un réseau externe. Cela veut dire changer l'adresse du WAN en allant dans virtuel network, changer setting et cliquer sur NAT.

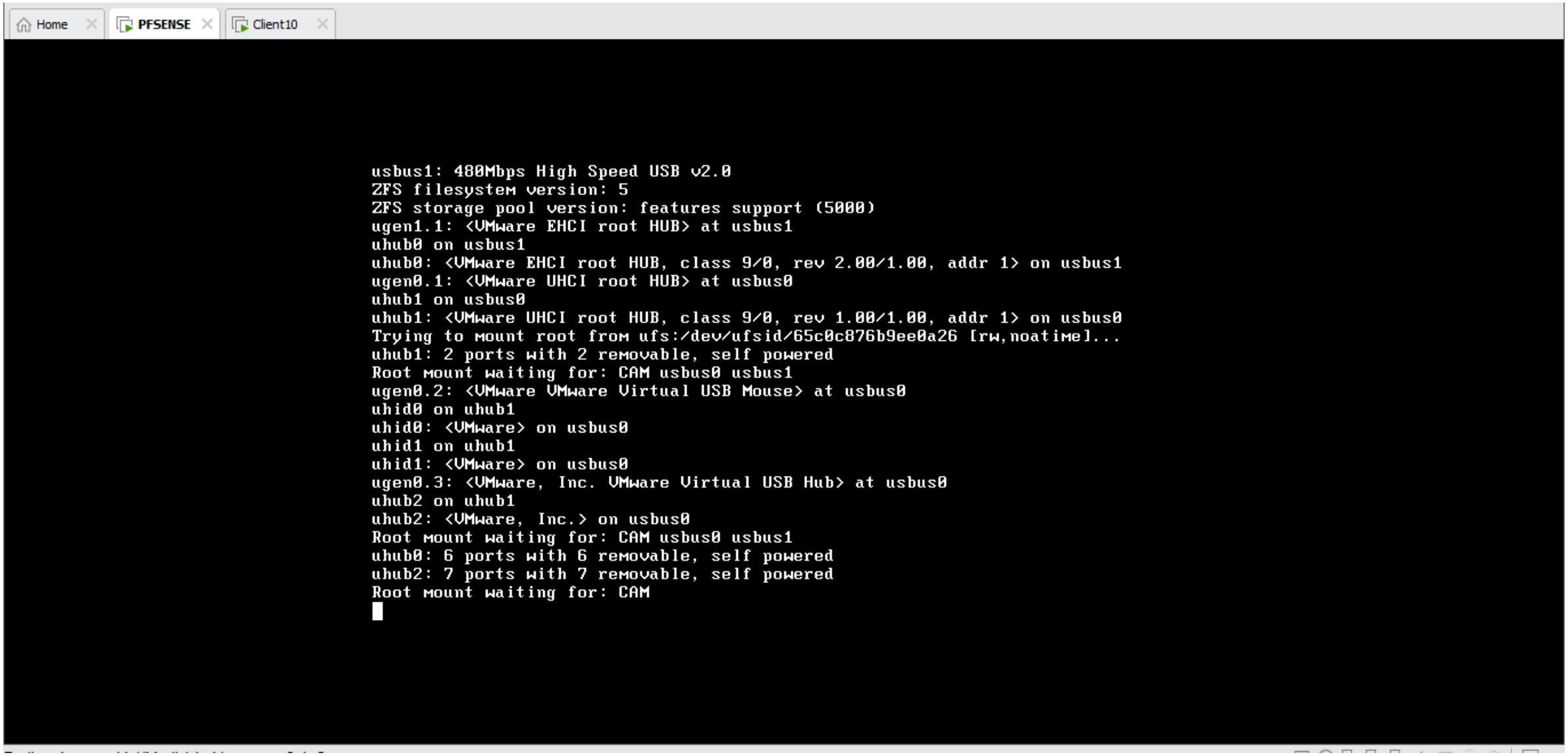


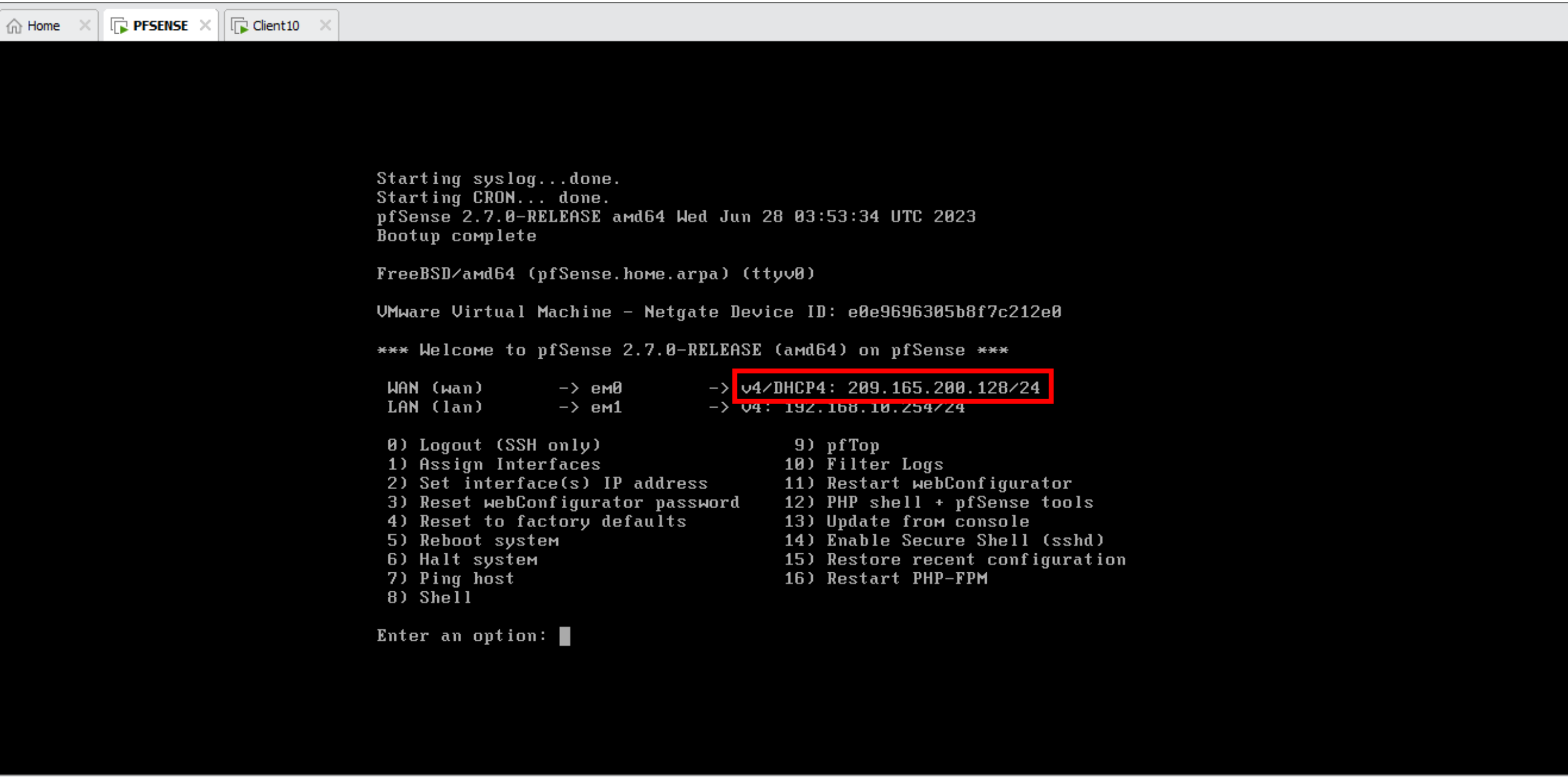
Dans setting ensuite virtual network Editor
Changer l'adresse ip et mettre celui d'un réseau publique pour la simulation
Subnet IP: 209.165.200.0



MACHINE
PFSENSE

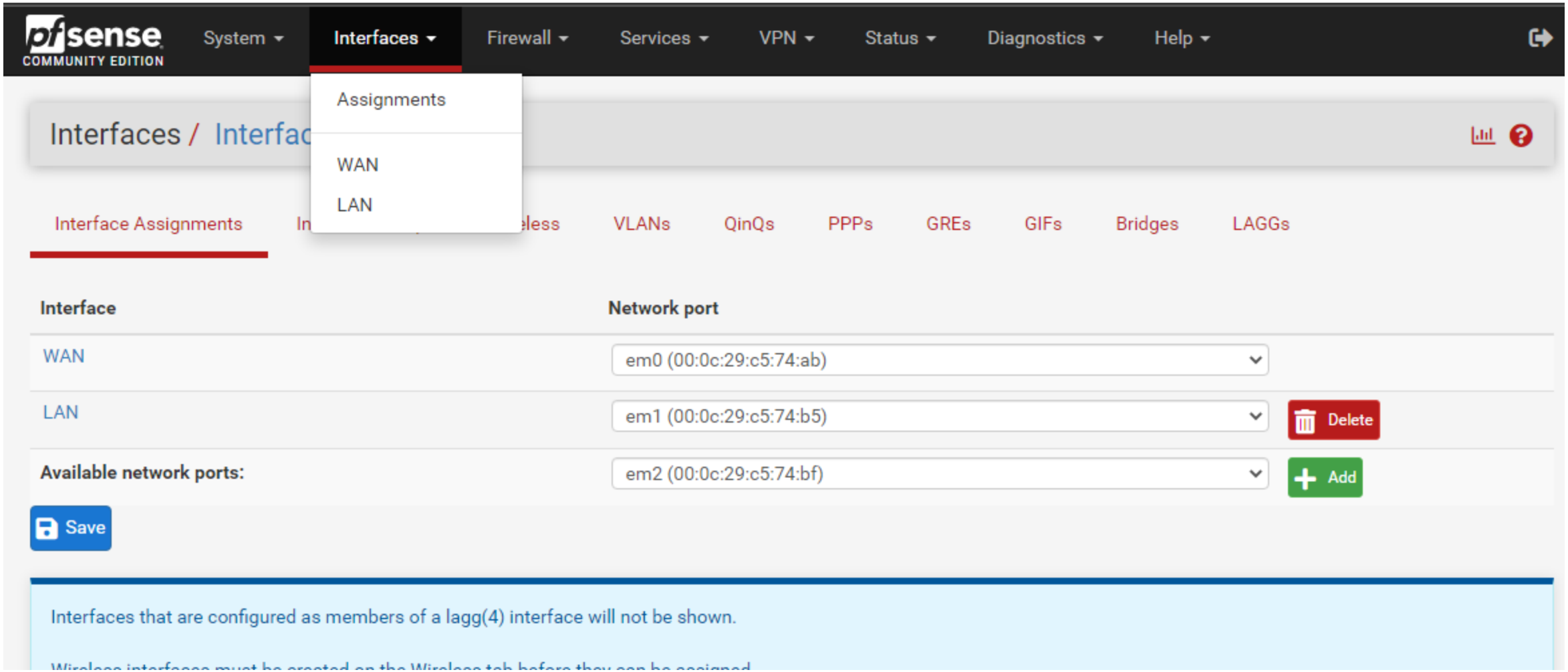
Redémarrer la machine PFSENSE pour que le changement d'adresse puisse être prise en compte

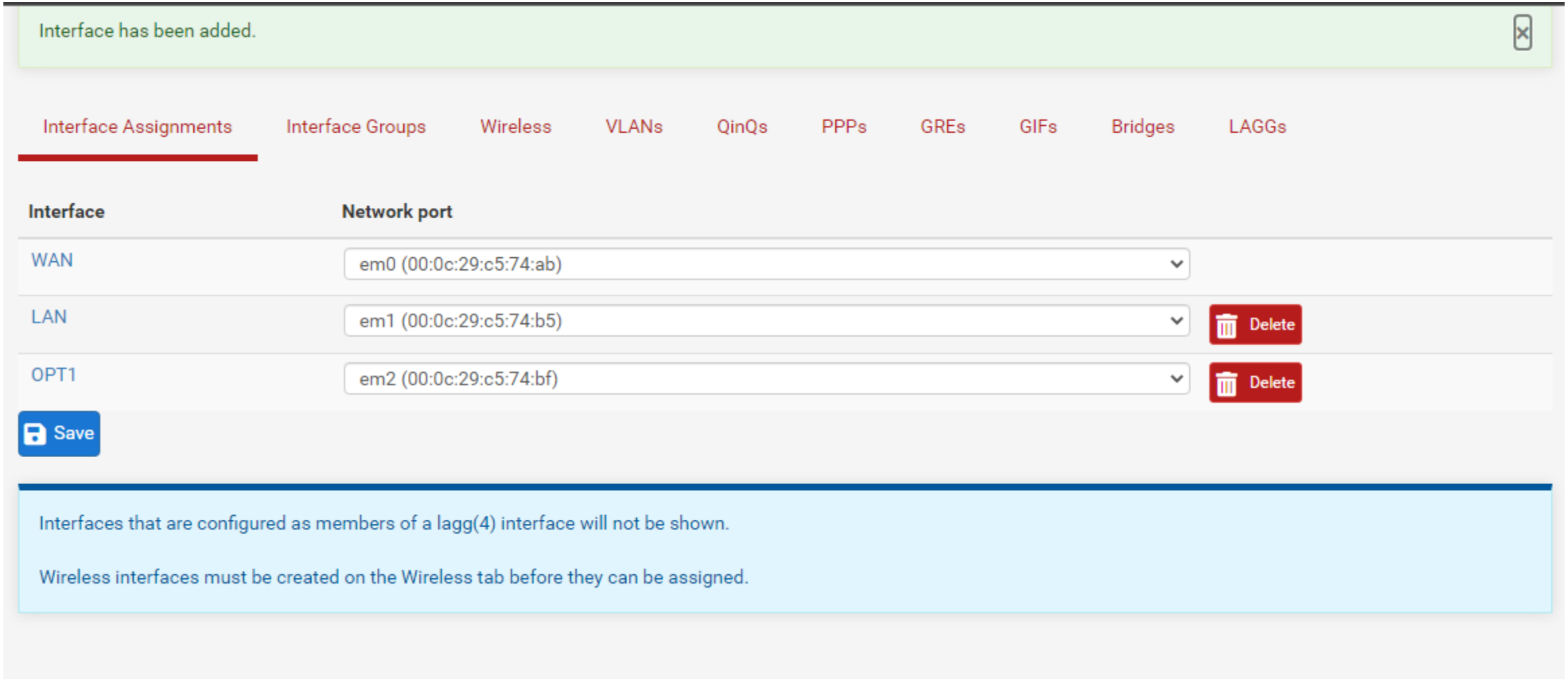


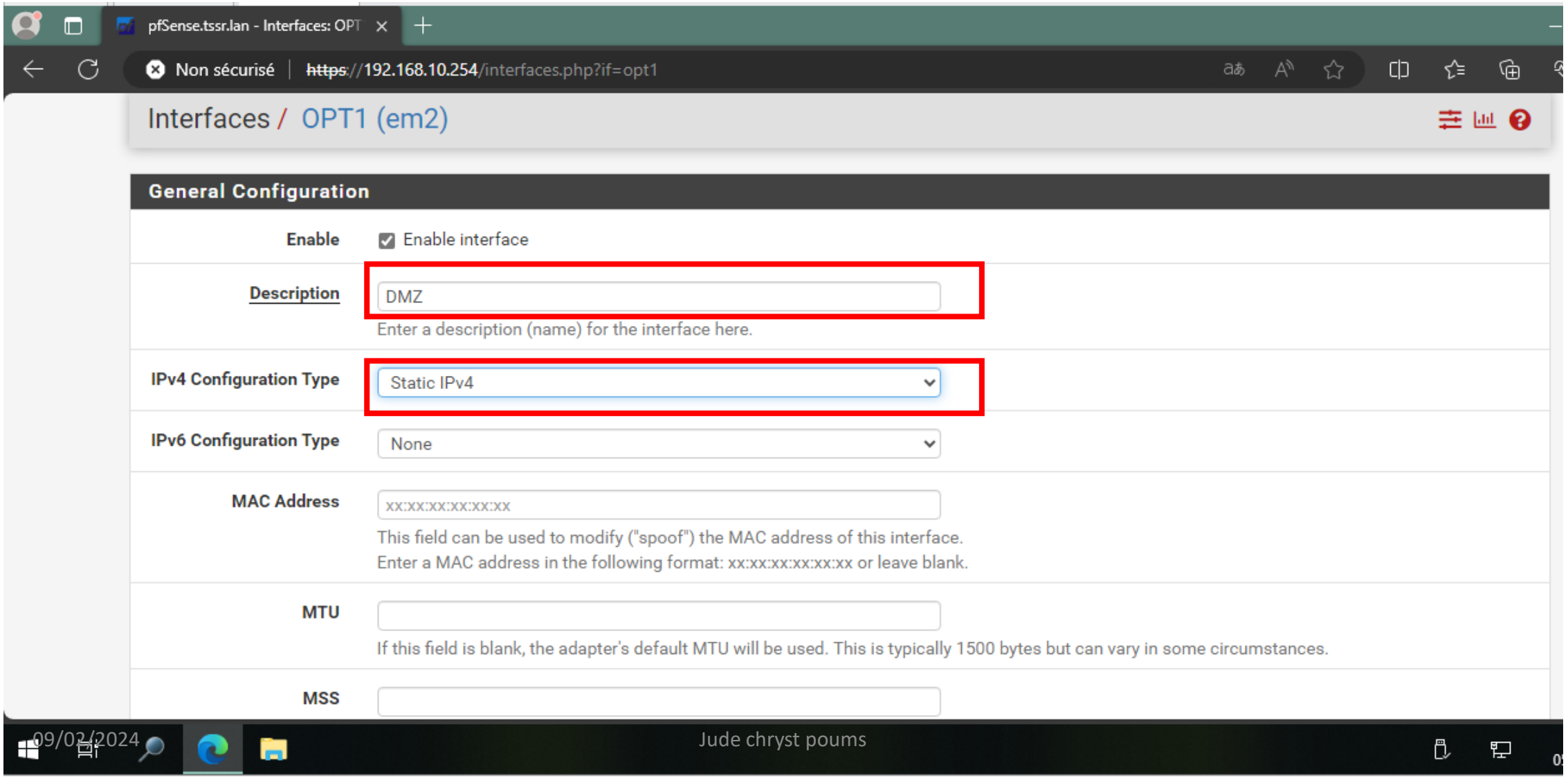

Home
PFSENSE
Client10
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: e0e9696305b8f7c212e0
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 209.165.200.128/24
LAN (lan) -> em1 -> v4: 192.168.10.254/24
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
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

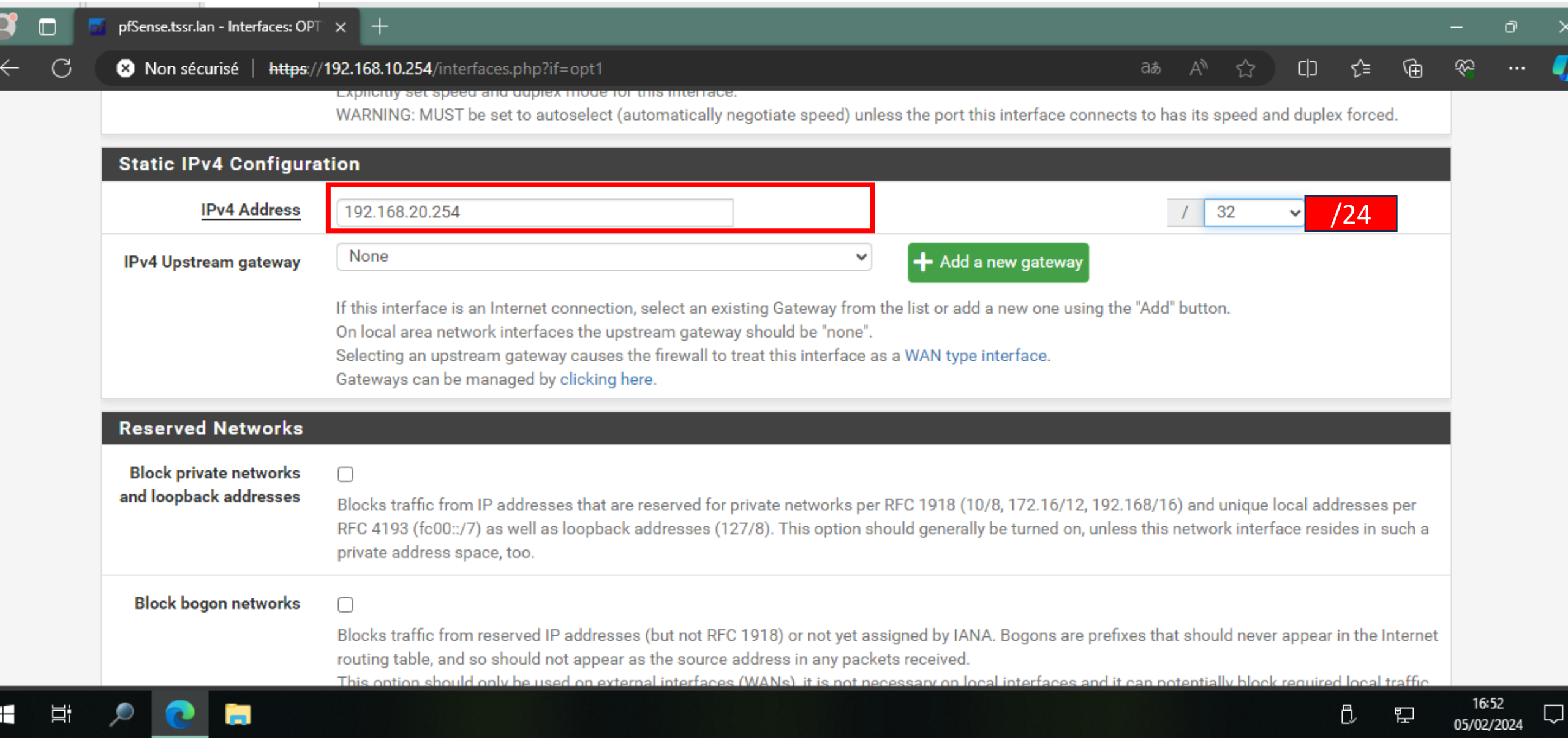
MACHINE CLIENTE WINDOWS 10

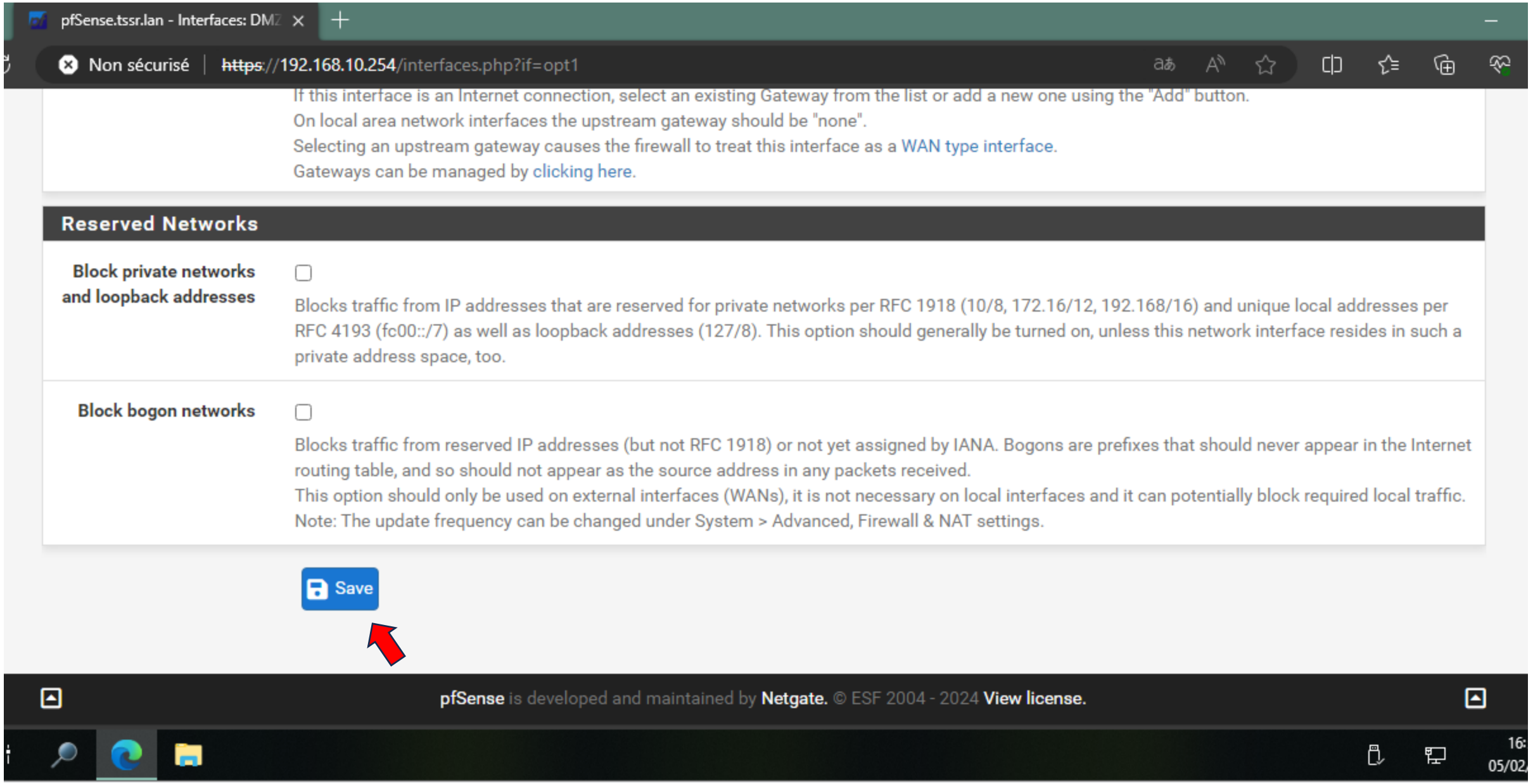
PFSENSE INTERFACE WEB

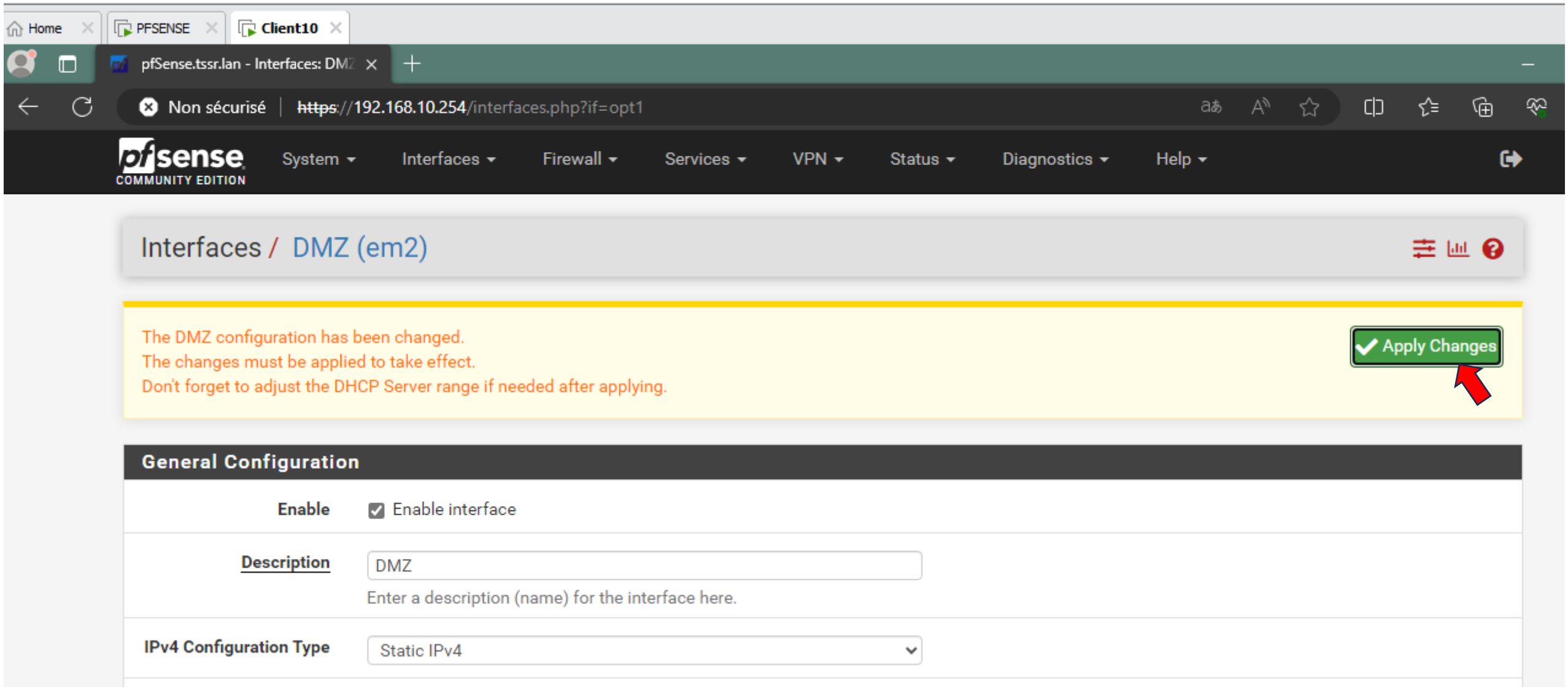

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
WAN
LAN
Interfaces / Interfac
Interface Assignments
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (00:0c:29:c5:74:ab)
LAN
em1 (00:0c:29:c5:74:b5)
Delete
Available network ports:
em2 (00:0c:29:c5:74:bf)
Add
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.

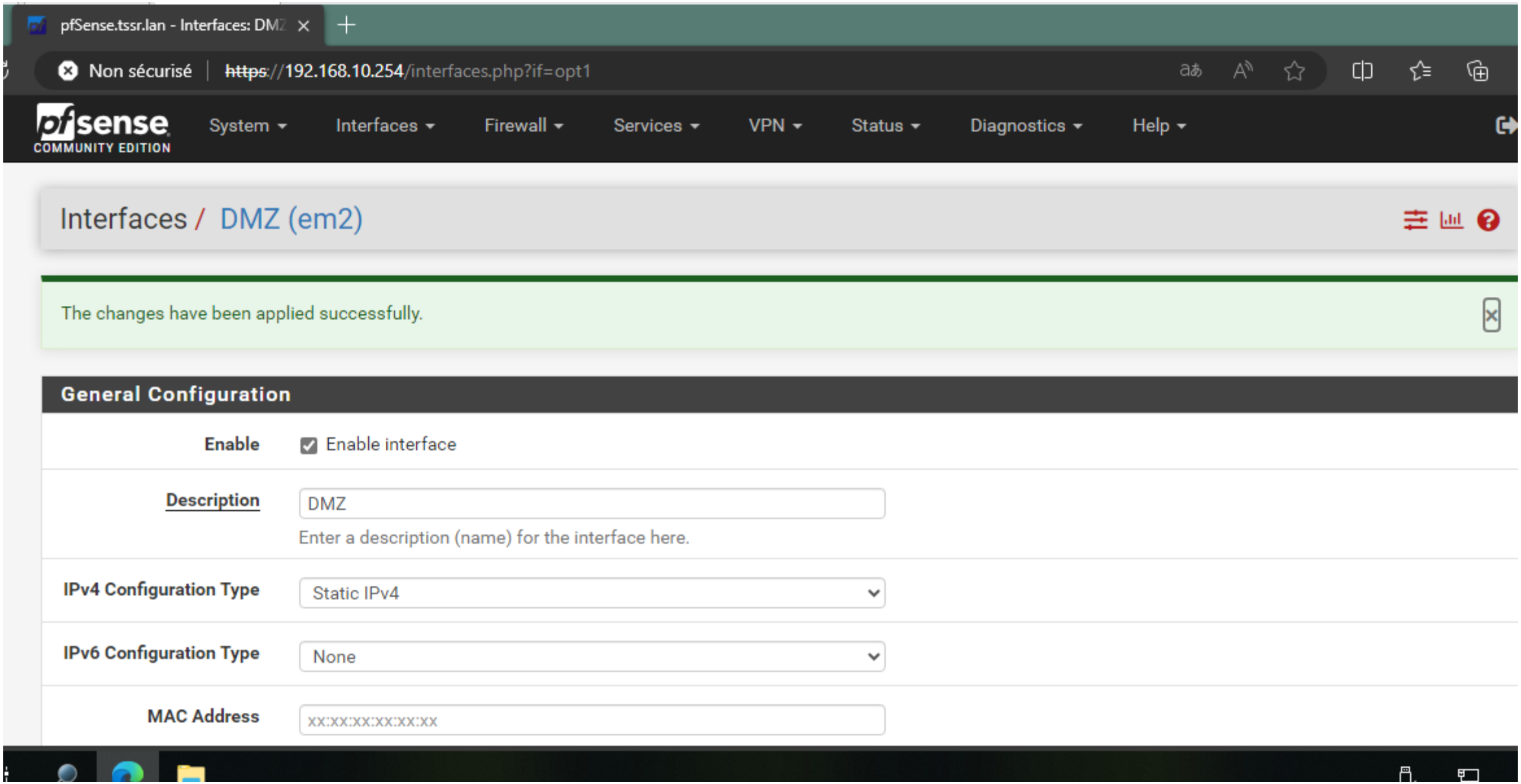

Interface has been added.
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (00:0c:29:c5:74:ab)
LAN
em1 (00:0c:29:c5:74:b5)
Delete
OPT1
em2 (00:0c:29:c5:74:bf)
Delete
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.

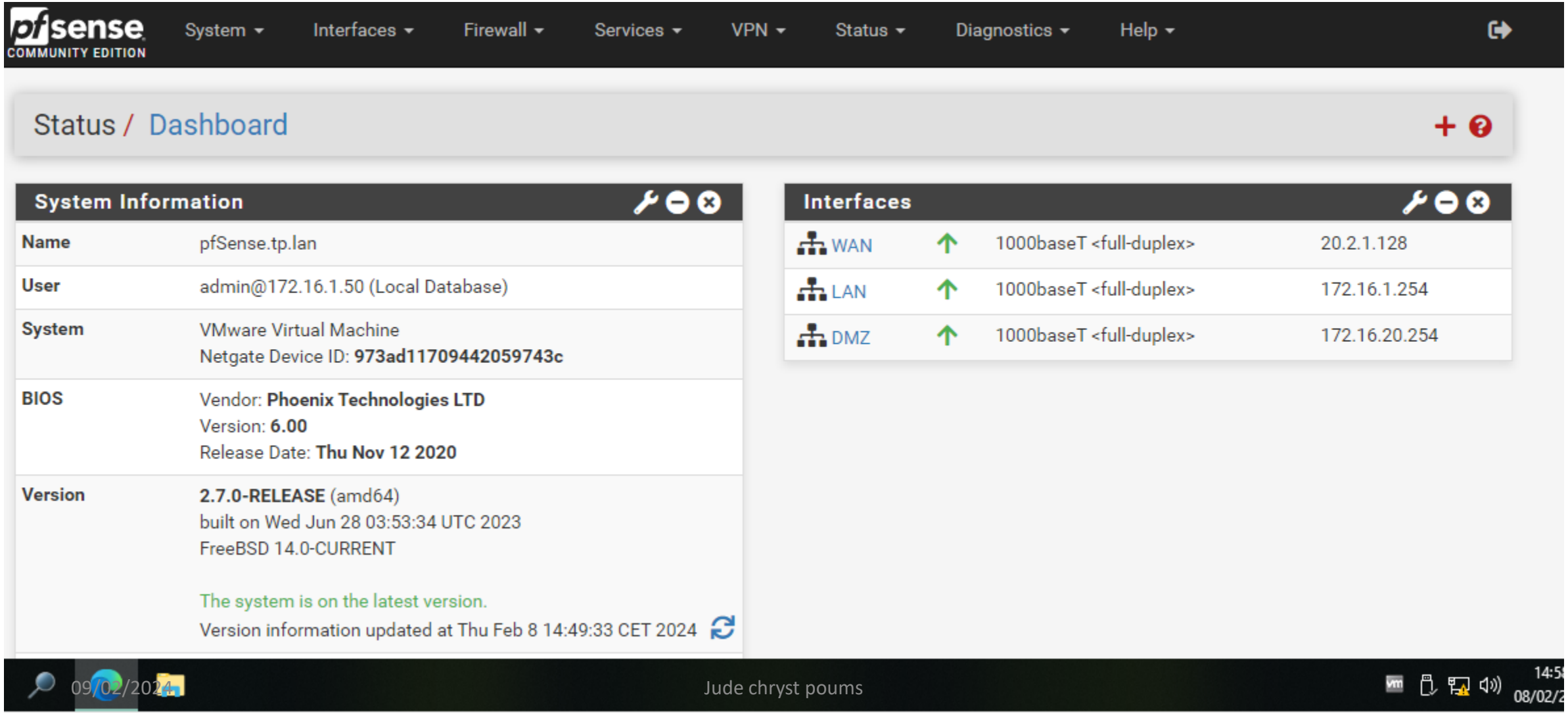

pfSense.tssr.lan - Interfaces: OPT
Non sécurisé
https://192.168.10.254/interfaces.php?if=opt1
Interfaces / OPT1 (em2)
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS


pfSense.tssr.lan - Interfaces: OPT
Non sécurisé | https://192.168.10.254/interfaces.php?if=opt1
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.20.254
/ 32
/24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
16:52
05/02/2024


pfSense.tssr.lan - Interfaces: DMZ
Non sécurisé
https://192.168.10.254/interfaces.php?if=opt1
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Reserved Networks
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

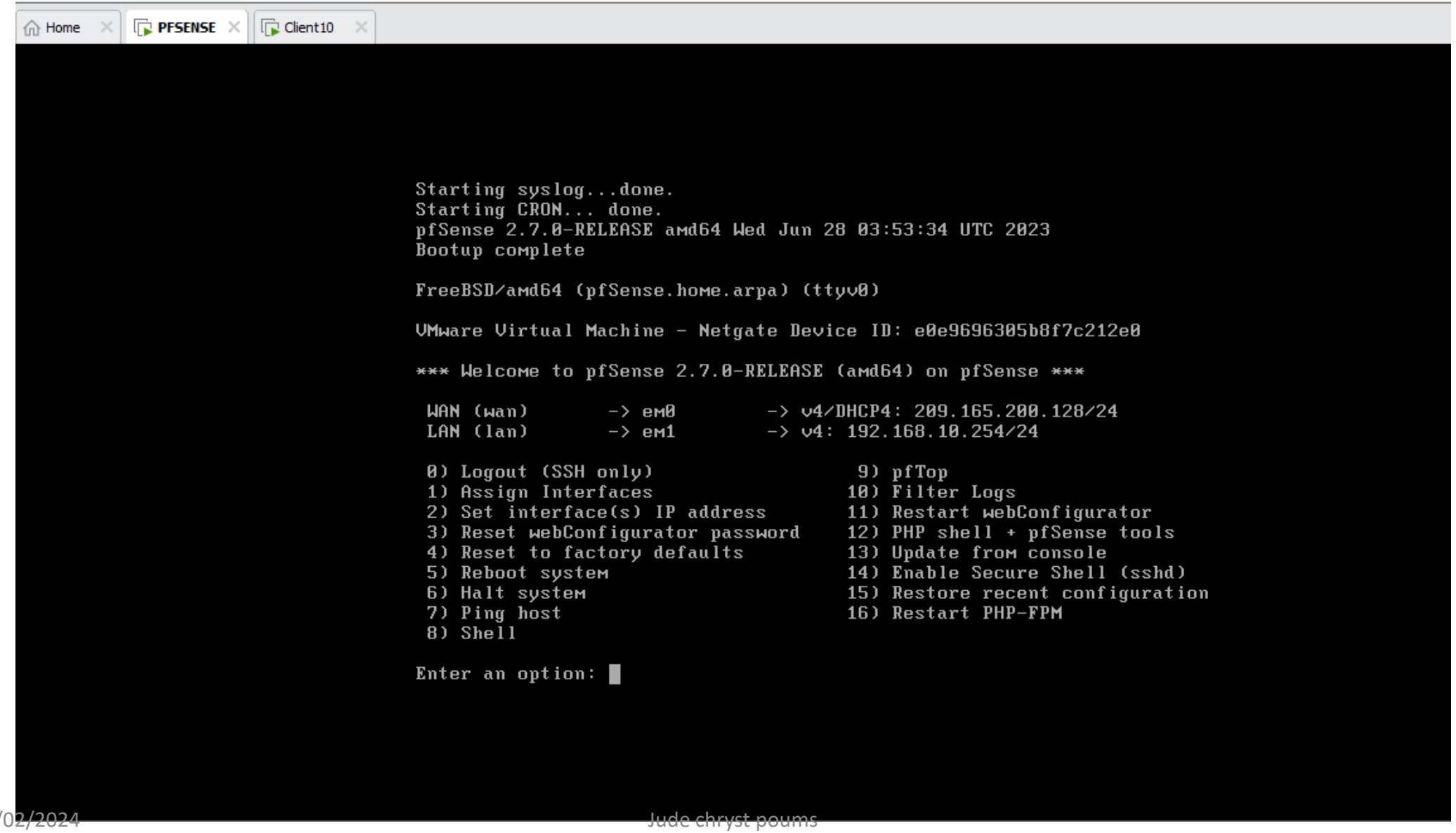

Home
PFSENSE
Client10
pfSense.tssr.lan - Interfaces: DMZ
Non sécurisé
https://192.168.10.254/interfaces.php?if=opt1
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / DMZ (em2)
The DMZ configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.
Apply Changes
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4

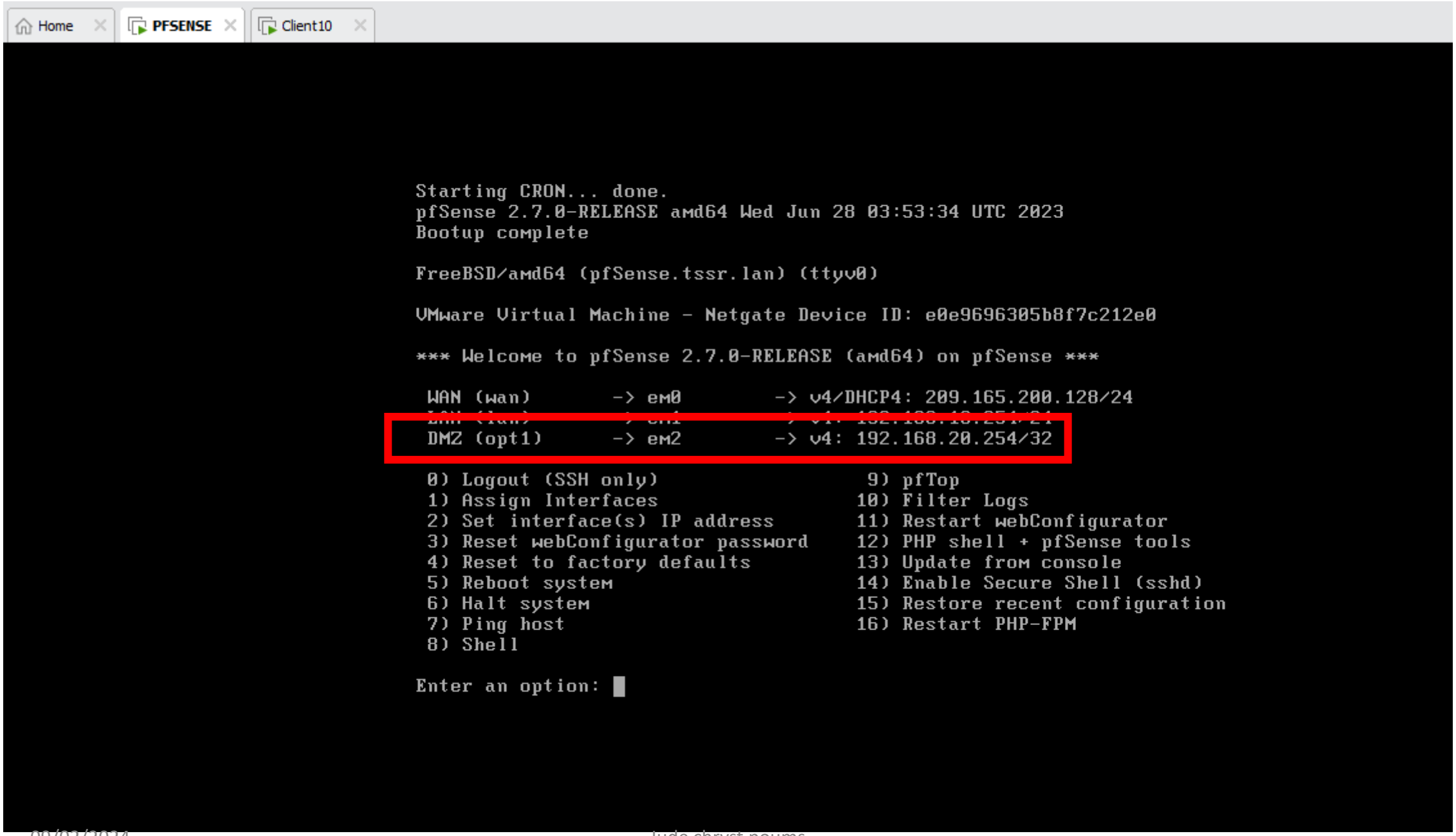

pfSense.tssr.lan - Interfaces: DMZ
Non sécurisé
https://192.168.10.254/interfaces.php?if=opt1
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Interfaces / DMZ (em2)
The changes have been applied successfully.
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / Dashboard
System Information
Name
pfSense.tp.lan
User
admin@172.16.1.50 (Local Database)
System
VMware Virtual Machine
Netgate Device ID: 973ad11709442059743c
BIOS
Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Version
2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT
The system is on the latest version.
Version information updated at Thu Feb 8 14:49:33 CET 2024
Interfaces
WAN
1000baseT <full-duplex>
20.2.1.128
LAN
1000baseT <full-duplex>
172.16.1.254
DMZ
1000baseT <full-duplex>
172.16.20.254
09/02/2024
Jude chryst poums
08/02/2

MACHINE
PFSENSE

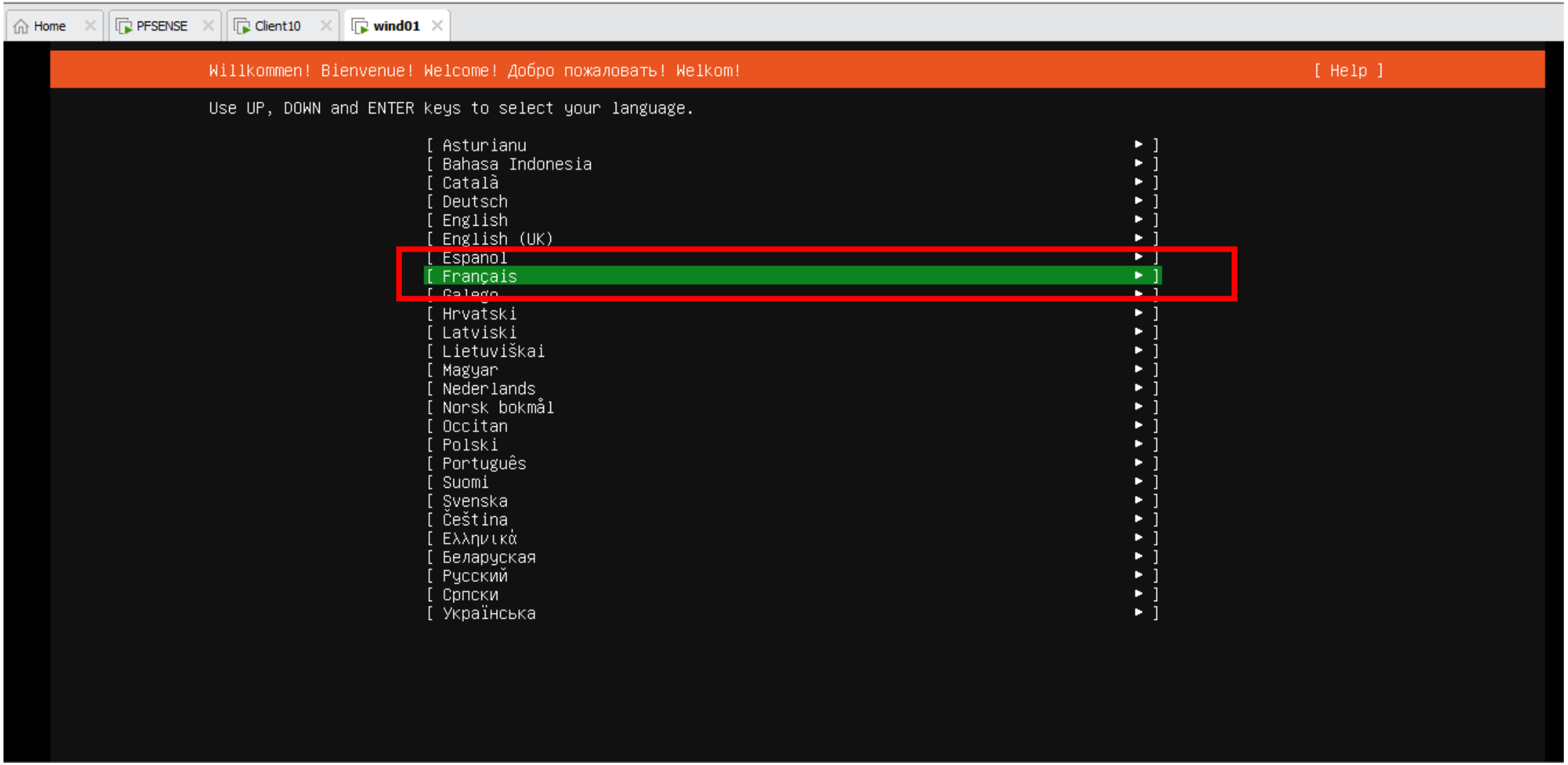
Redémarrer la machine PFSENSE pour que le changement d'adresse puisse être prise en compte

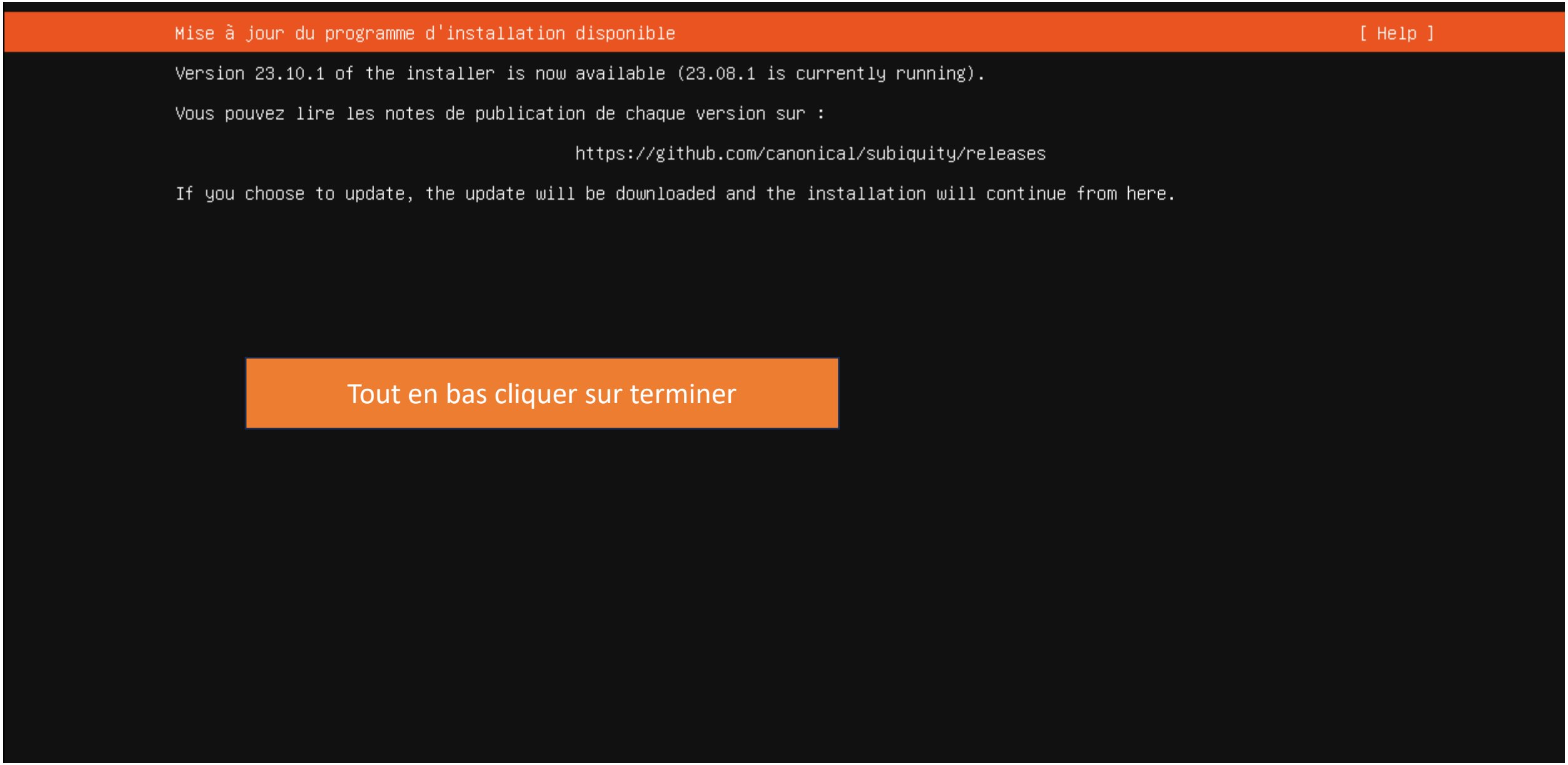



Home
PFSENSE
Client10
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete
FreeBSD/amd64 (pfSense.tssr.lan) (ttyv0)
VMware Virtual Machine - Netgate Device ID: e0e9696305b8f7c212e0
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 209.165.200.128/24
DMZ (opt1) -> em2 -> v4: 192.168.20.254/32
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
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

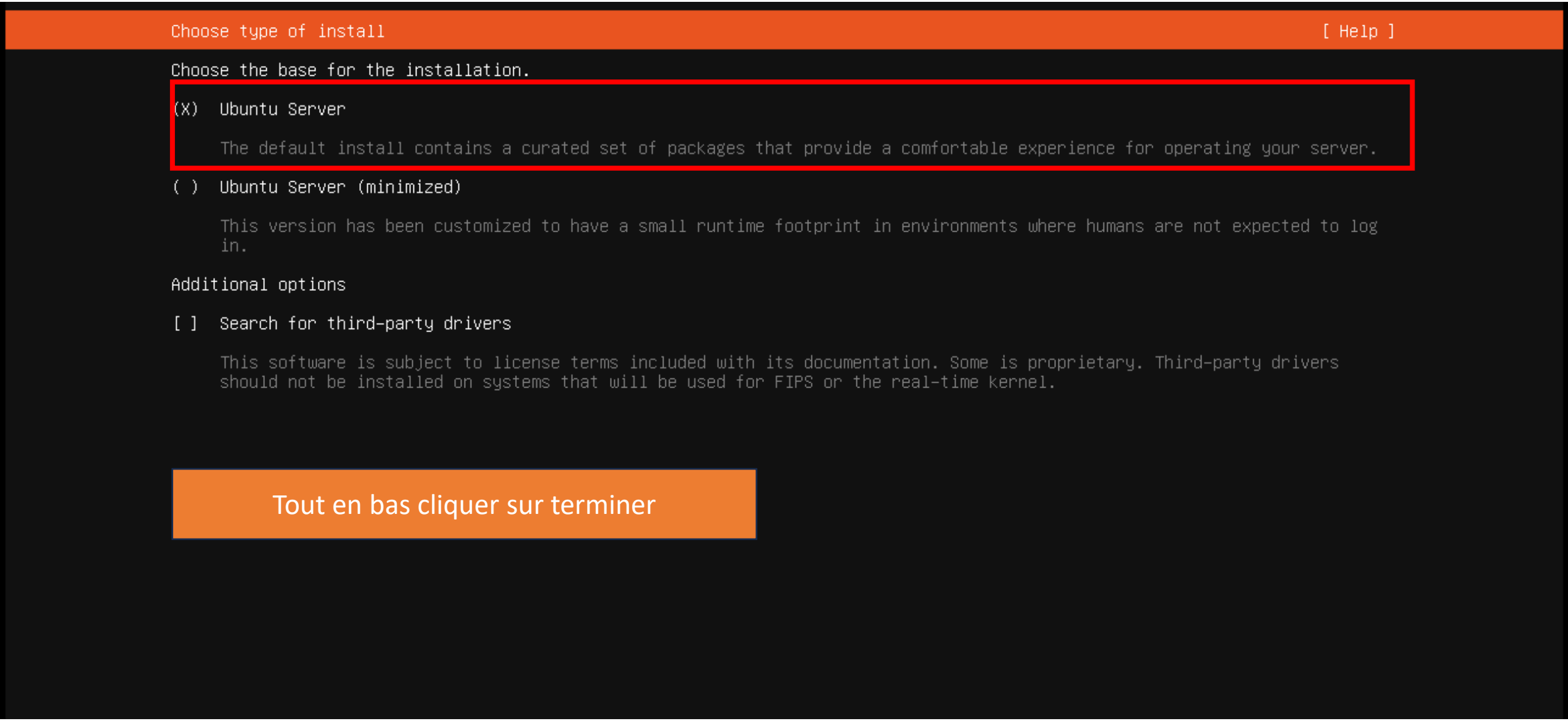
MACHINE UBUNTU-SERVER

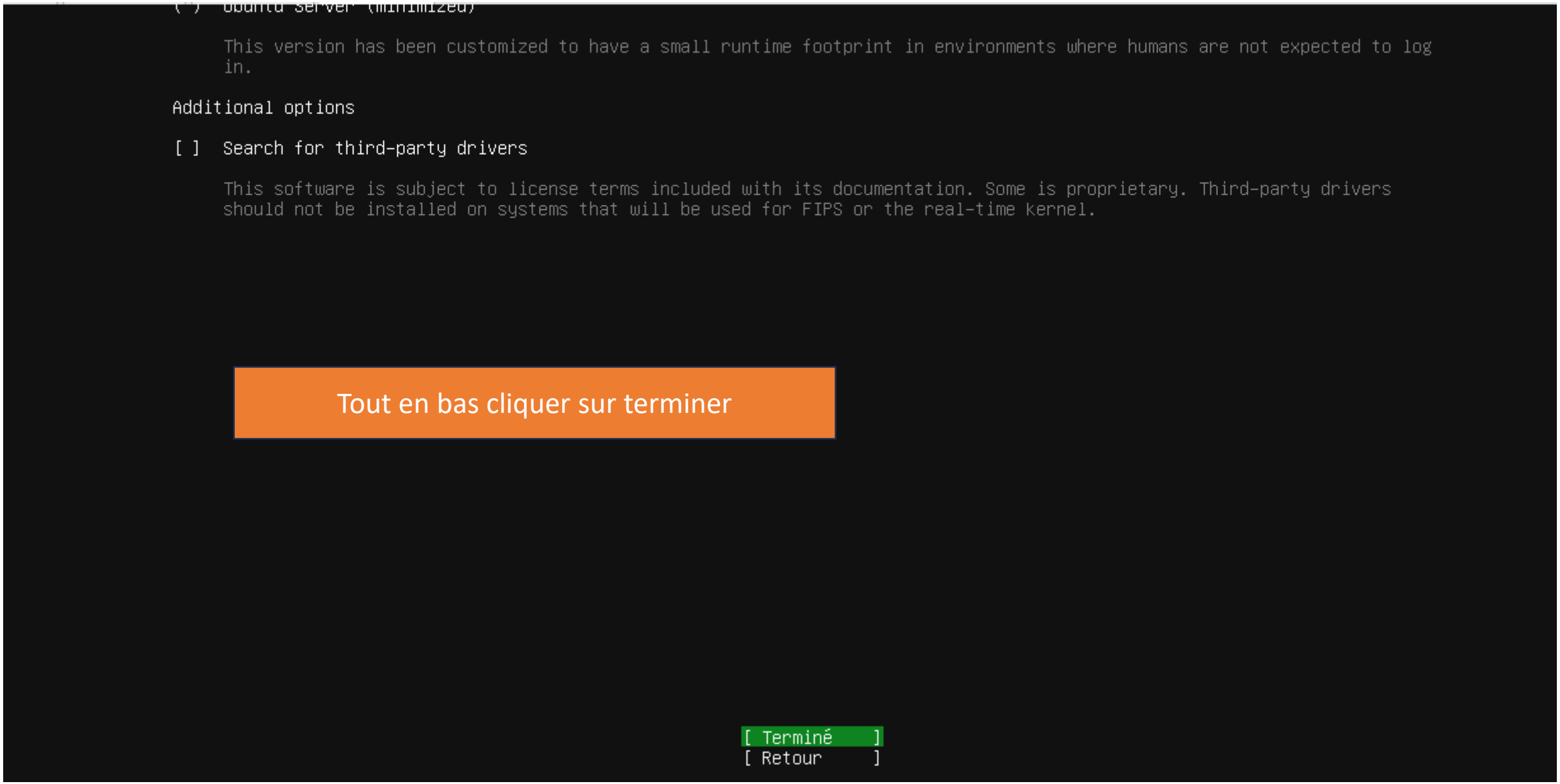
WEB


Home
PFSENSE
Client10
wind01
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!
[Help]
Use UP, DOWN and ENTER keys to select your language.
[Asturianu ▸]
[Bahasa Indonesia ▸]
[Català ▸]
[Deutsch ▸]
[English ▸]
[English (UK) ▸]
[Español ▸]
[Français ▸]
[Galego ▸]
[Hrvatski ▸]
[Latviski ▸]
[Lietuviškai ▸]
[Magyar ▸]
[Nederlands ▸]
[Norsk bokmål ▸]
[Occitan ▸]
[Polski ▸]
[Português ▸]
[Suomi ▸]
[Svenska ▸]
[Čeština ▸]
[Ελληνικά ▸]
[Беларуская ▸]
[Русский ▸]
[Српски ▸]
[Українська ▸]

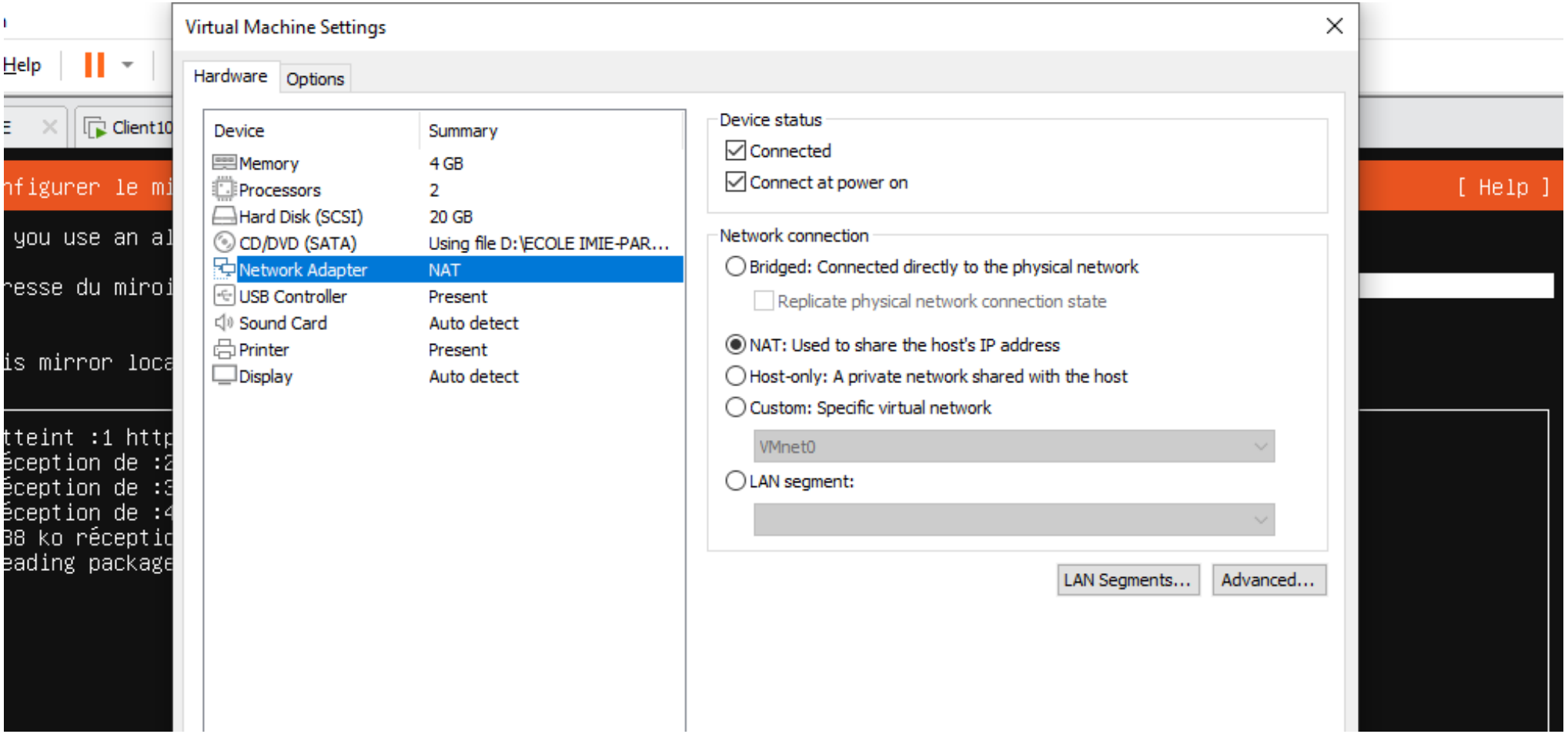

Mise à jour du programme d'installation disponible
[Help]
Version 23.10.1 of the installer is now available (23.08.1 is currently running).
Vous pouvez lire les notes de publication de chaque version sur :
https://github.com/canonical/subiquity/releases
If you choose to update, the update will be downloaded and the installation will continue from here.
Tout en bas cliquer sur terminer

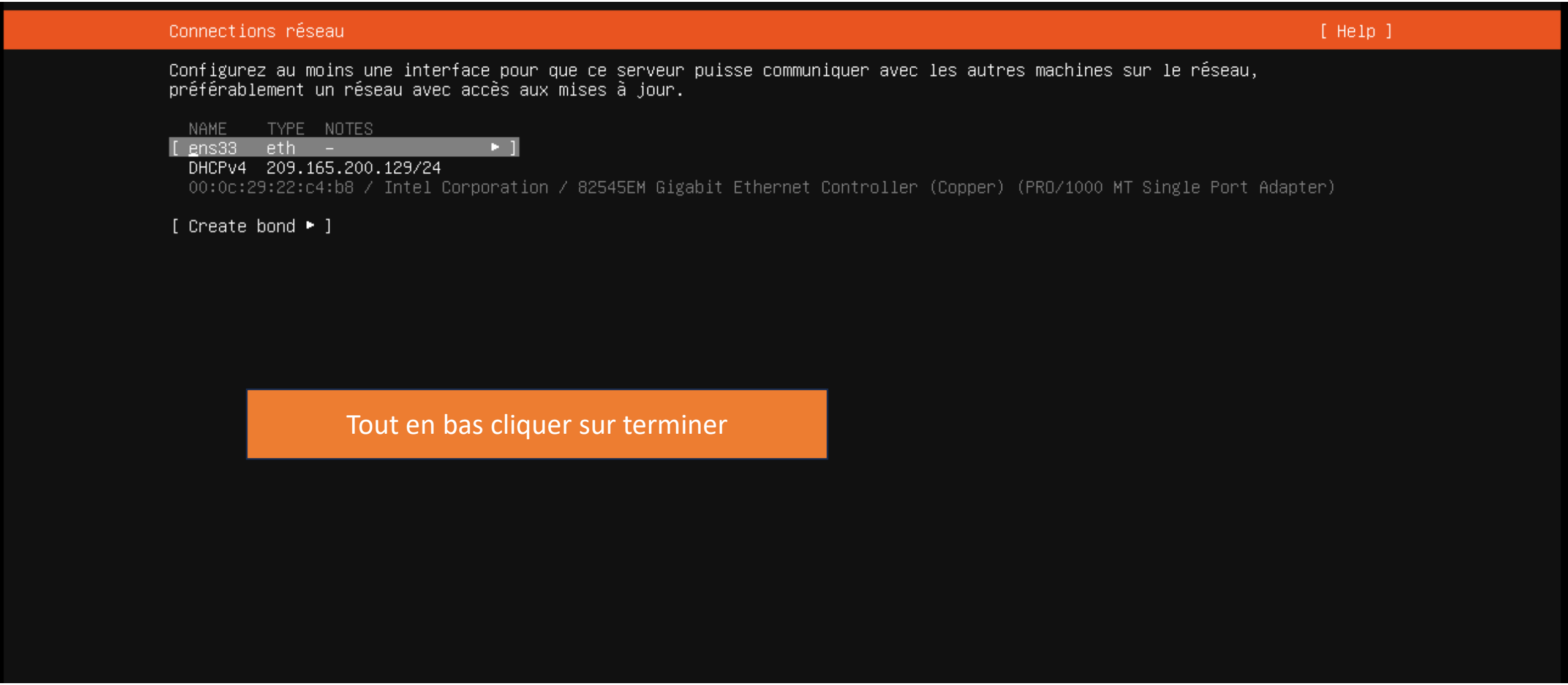

Configuration clavier
[Help]
Veuillez sélectionner votre disposition de clavier ci-dessous, ou sélectionner "Identifier le clavier" afin de détecter votre disposition automatiquement.
Disposition : [French ▾]
Variante : [French - French (legacy, alt.) ▾]
[Identifier le clavier]
Tout en bas cliquer sur terminer

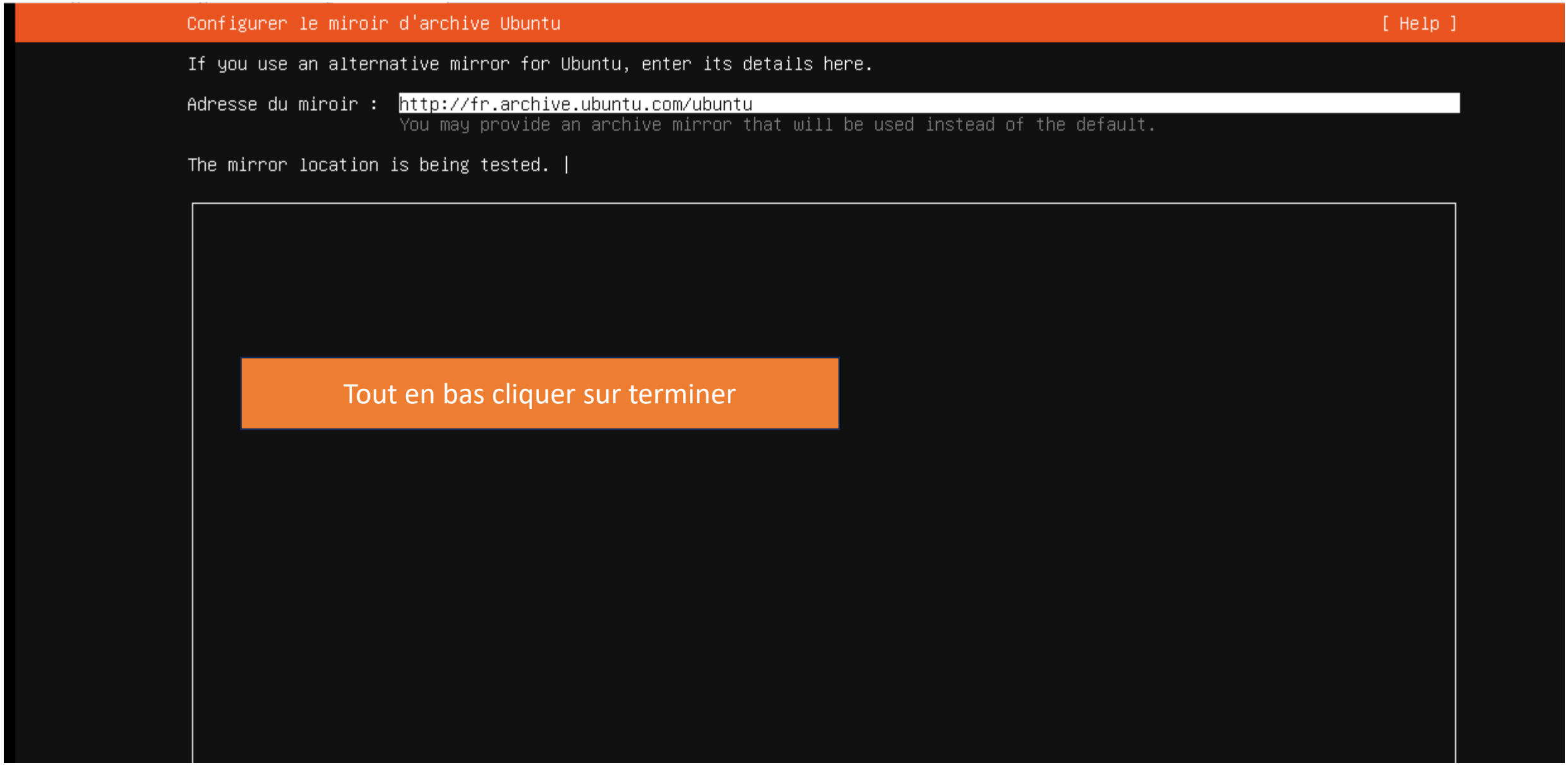

Choose type of install
[Help]
Choose the base for the installation.
(X) Ubuntu Server
The default install contains a curated set of packages that provide a comfortable experience for operating your server.
( ) Ubuntu Server (minimized)
This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.
Additional options
[ ] Search for third-party drivers
This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers should not be installed on systems that will be used for FIPS or the real-time kernel.
Tout en bas cliquer sur terminer

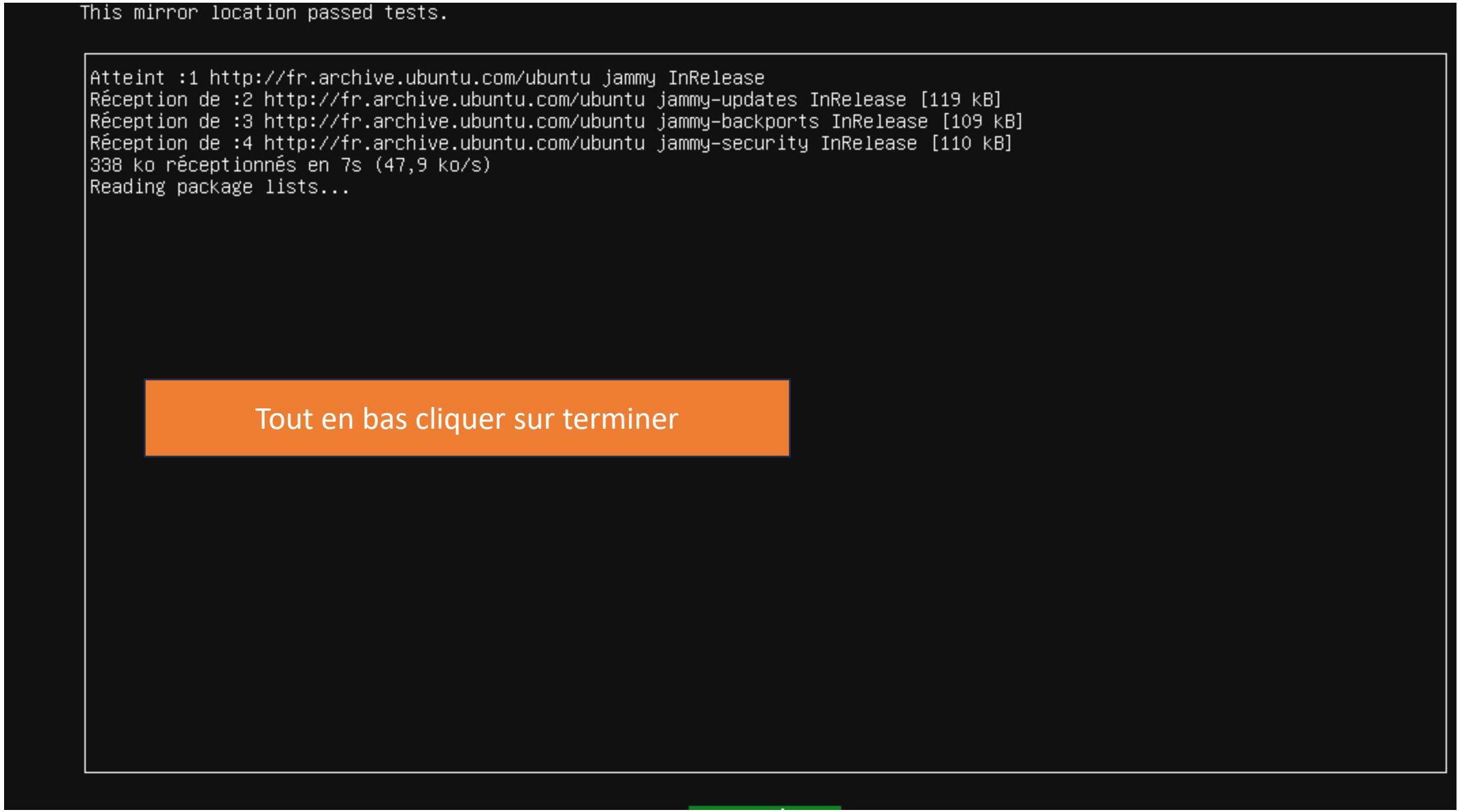


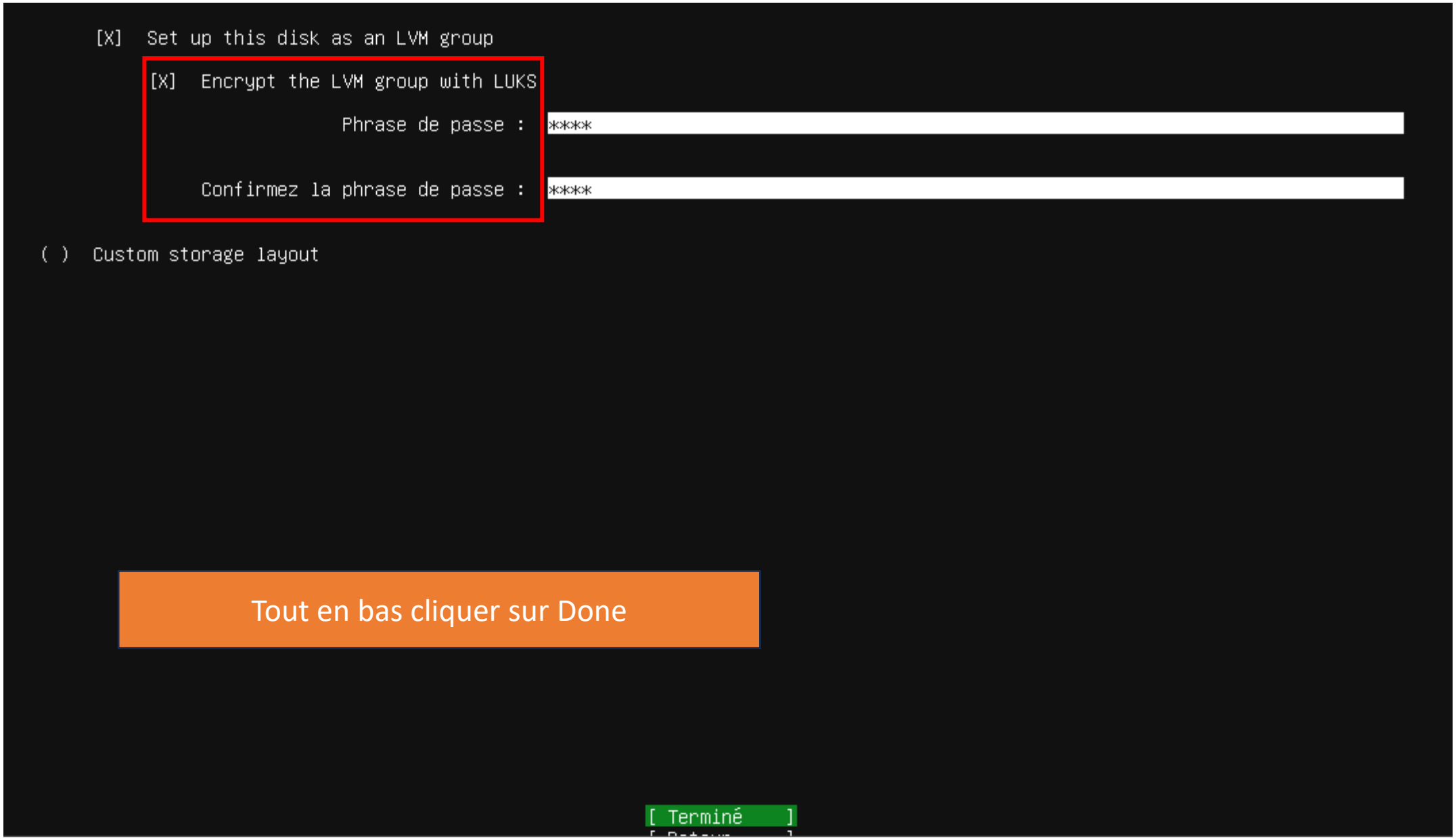
Tout en bas cliquer sur terminer


Help
Client10
nfigurer le mi
you use an al
esse du miroi
is mirror loca
tteint :1 http
éception de :2
éception de :3
éception de :4
88 ko réceptio
eading package
[Help]
Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
4 GB
Processors
2
Hard Disk (SCSI)
20 GB
CD/DVD (SATA)
Using file D:\ECOLE IMIE-PAR...
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Printer
Present
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...


Connections réseau
[Help]
Configurez au moins une interface pour que ce serveur puisse communiquer avec les autres machines sur le réseau,
préférablement un réseau avec accès aux mises à jour.
NAME TYPE NOTES
[ens33 eth - ▸]
DHCPv4 209.165.200.129/24
00:0c:29:22:c4:b8 / Intel Corporation / 82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)
[Create bond ▸]
Tout en bas cliquer sur terminer

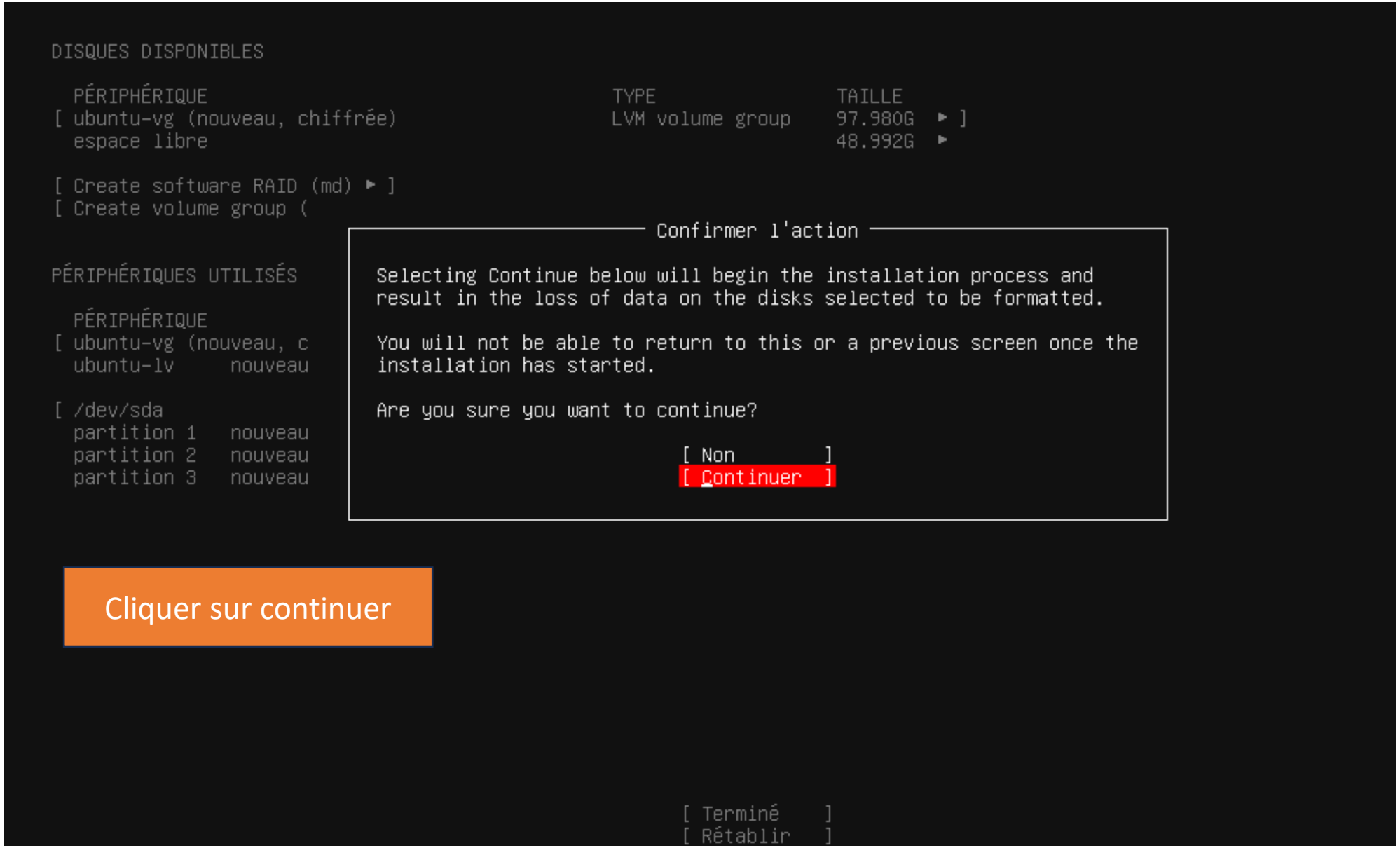

Configurer le miroir d'archive Ubuntu
[Help]
If you use an alternative mirror for Ubuntu, enter its details here.
Adresse du miroir : http://fr.archive.ubuntu.com/ubuntu
You may provide an archive mirror that will be used instead of the default.
The mirror location is being tested.
Tout en bas cliquer sur terminer


This mirror location passed tests.
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Réception de :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Réception de :3 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Réception de :4 http://fr.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
338 ko réceptionnés en 7s (47,9 ko/s)
Reading package lists...
Tout en bas cliquer sur terminer

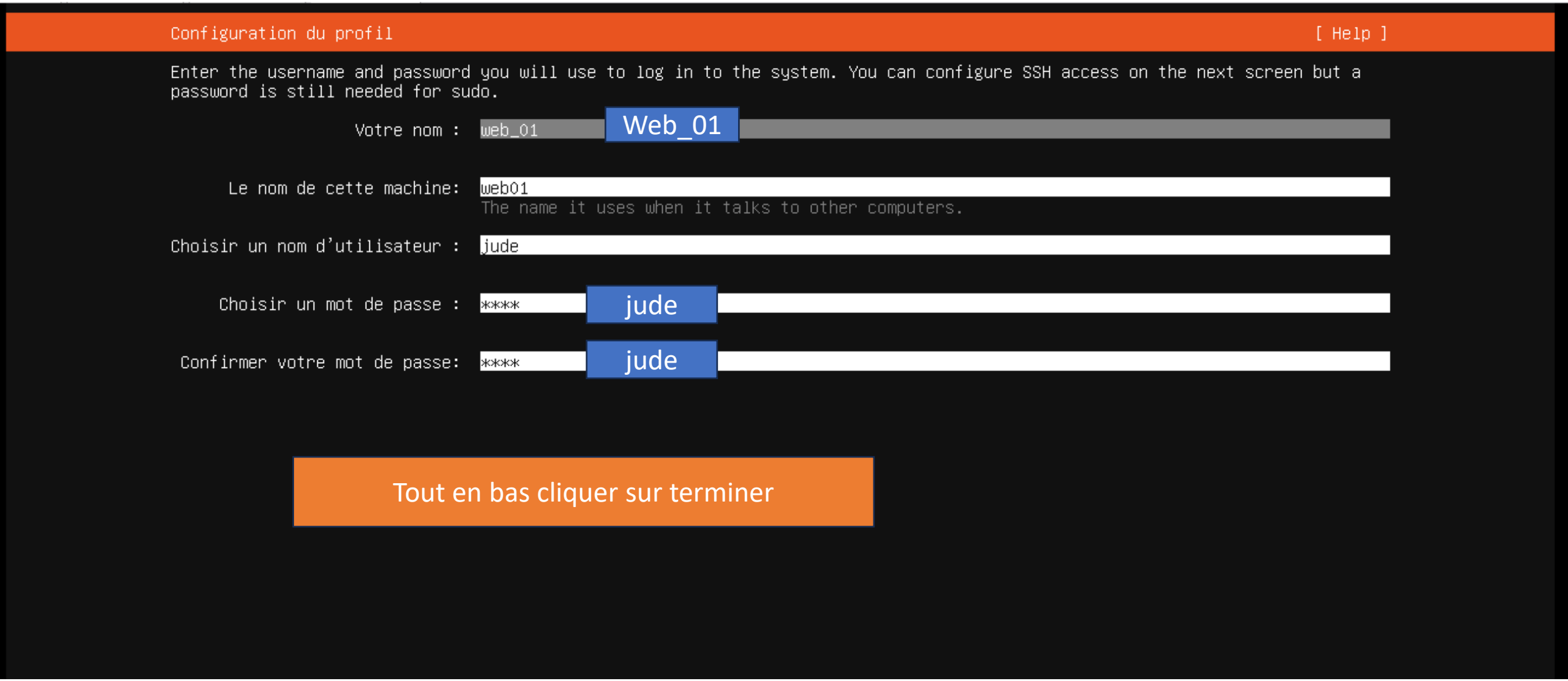


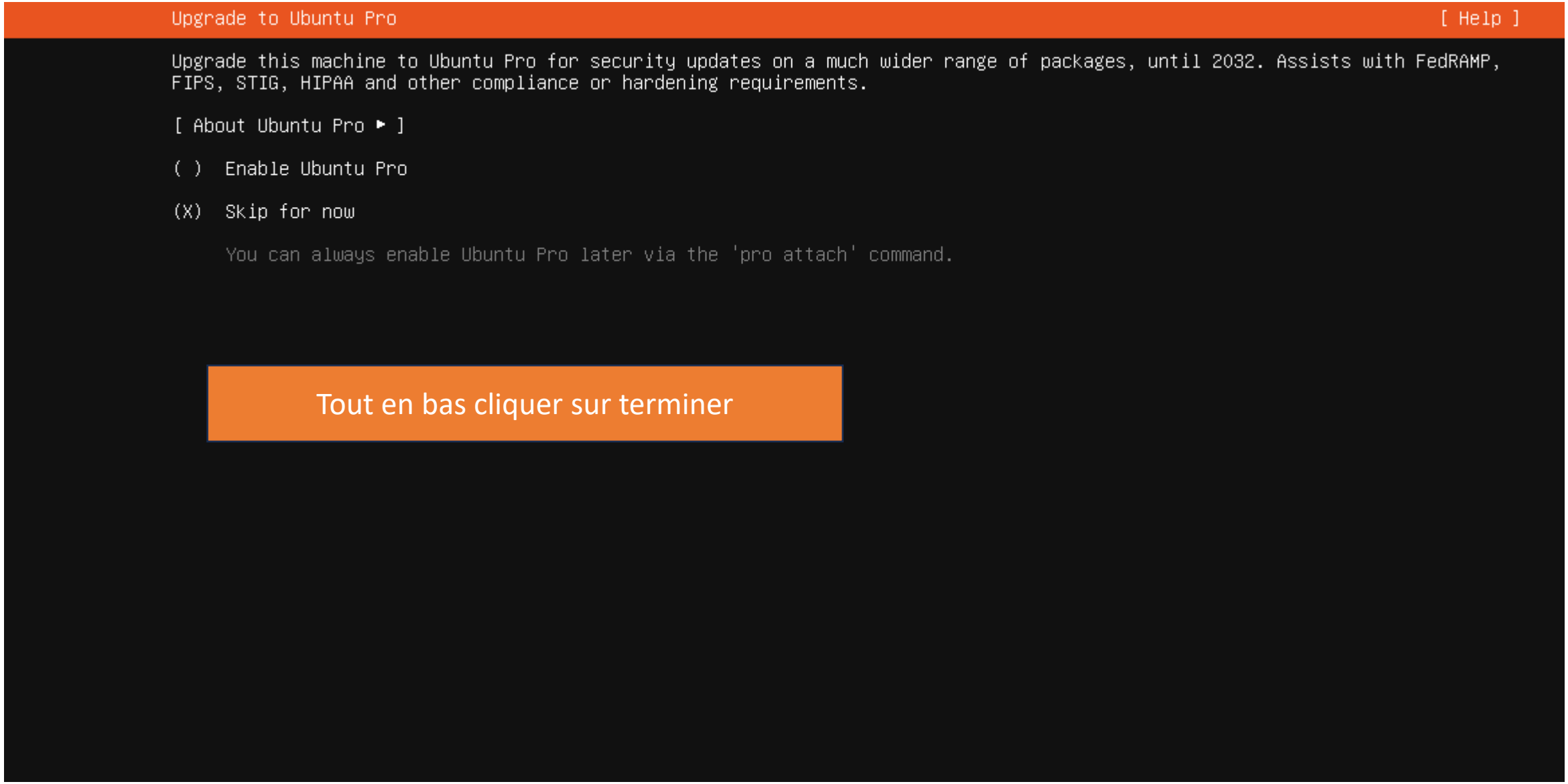
Tout en bas cliquer sur Done

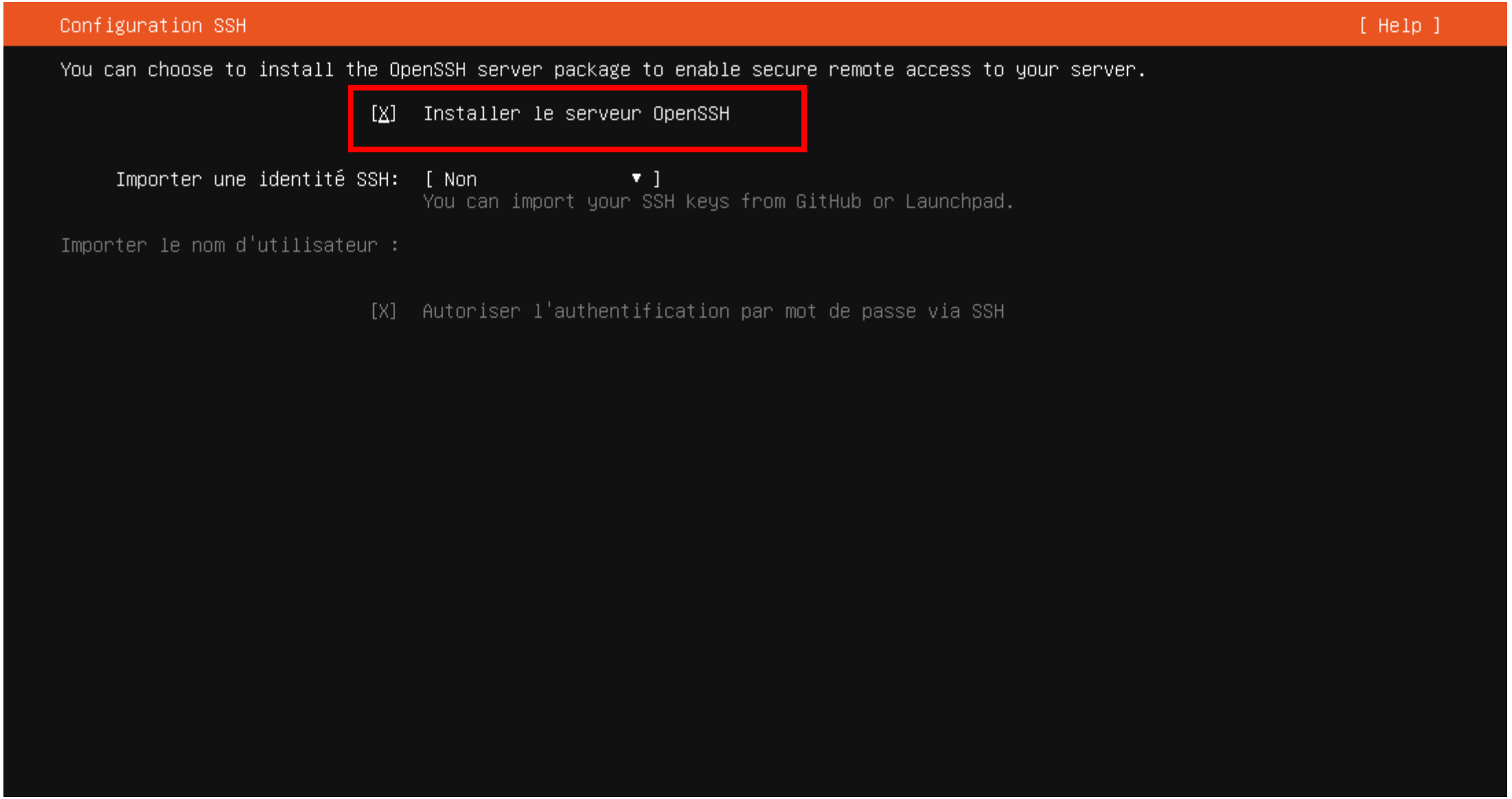
Tout en bas cliquer sur terminer

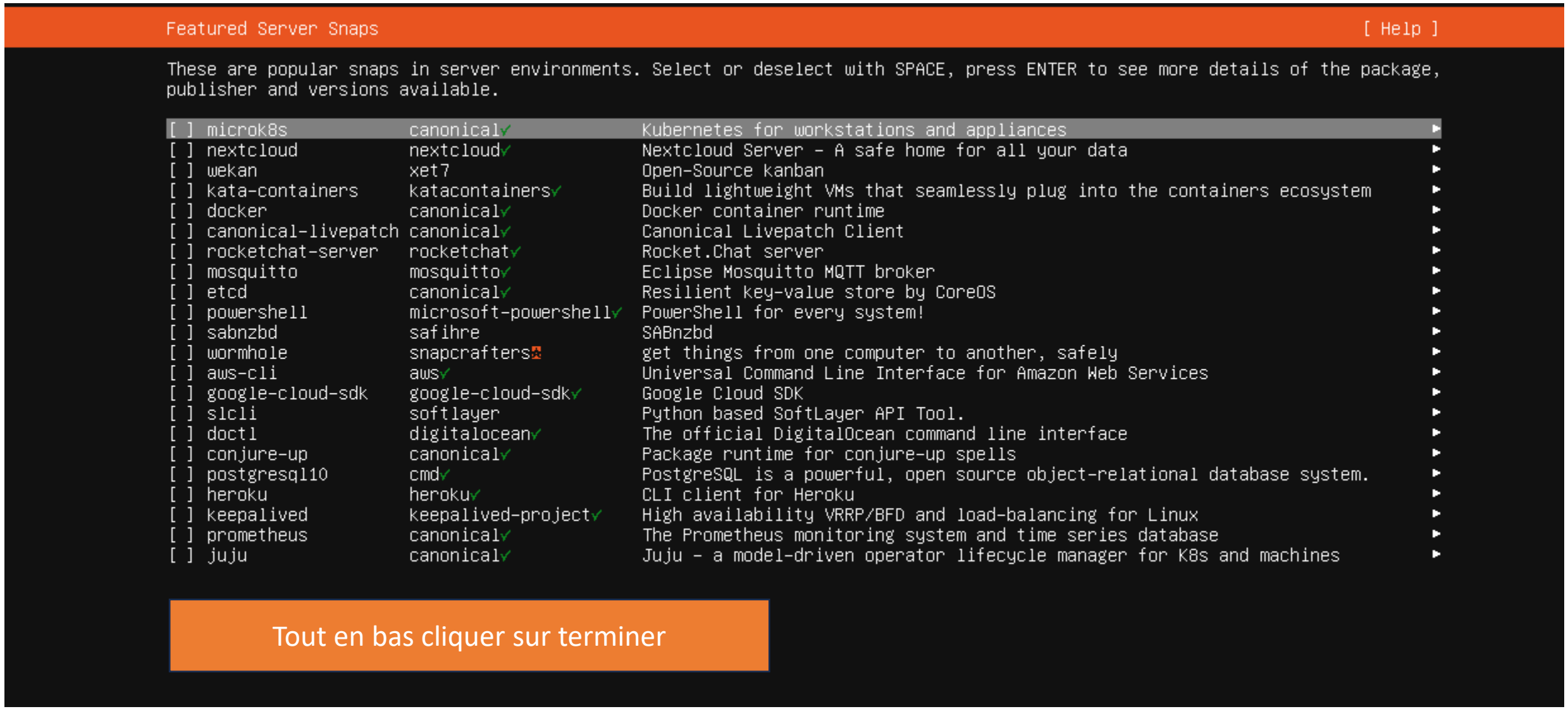


Cliquer sur continuer


Configuration du profil
[Help]
Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.
Votre nom :
web_01
Web_01
Le nom de cette machine:
web01
The name it uses when it talks to other computers.
Choisir un nom d'utilisateur :
jude
Choisir un mot de passe :
****
jude
Confirmer votre mot de passe:
****
jude
Tout en bas cliquer sur terminer

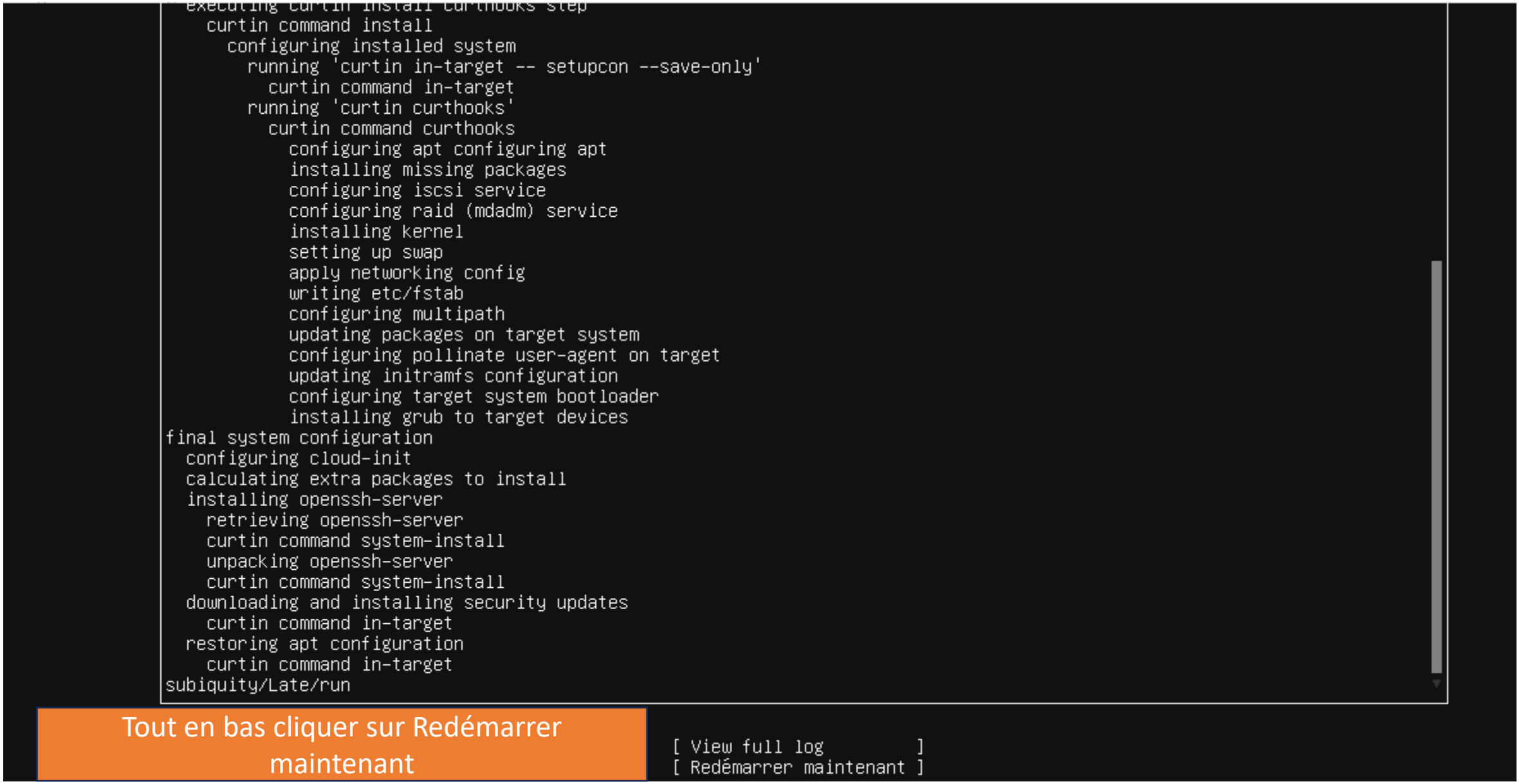

Upgrade to Ubuntu Pro
[Help]
Upgrade this machine to Ubuntu Pro for security updates on a much wider range of packages, until 2032. Assists with FedRAMP, FIPS, STIG, HIPAA and other compliance or hardening requirements.
[About Ubuntu Pro ▸]
( ) Enable Ubuntu Pro
(X) Skip for now
You can always enable Ubuntu Pro later via the 'pro attach' command.
Tout en bas cliquer sur terminer


Configuration SSH
[Help]
You can choose to install the OpenSSH server package to enable secure remote access to your server.
[X] Installer le serveur OpenSSH
Importer une identité SSH: [Non ▾]
You can import your SSH keys from GitHub or Launchpad.
Importer le nom d'utilisateur :
[X] Autoriser l'authentification par mot de passe via SSH

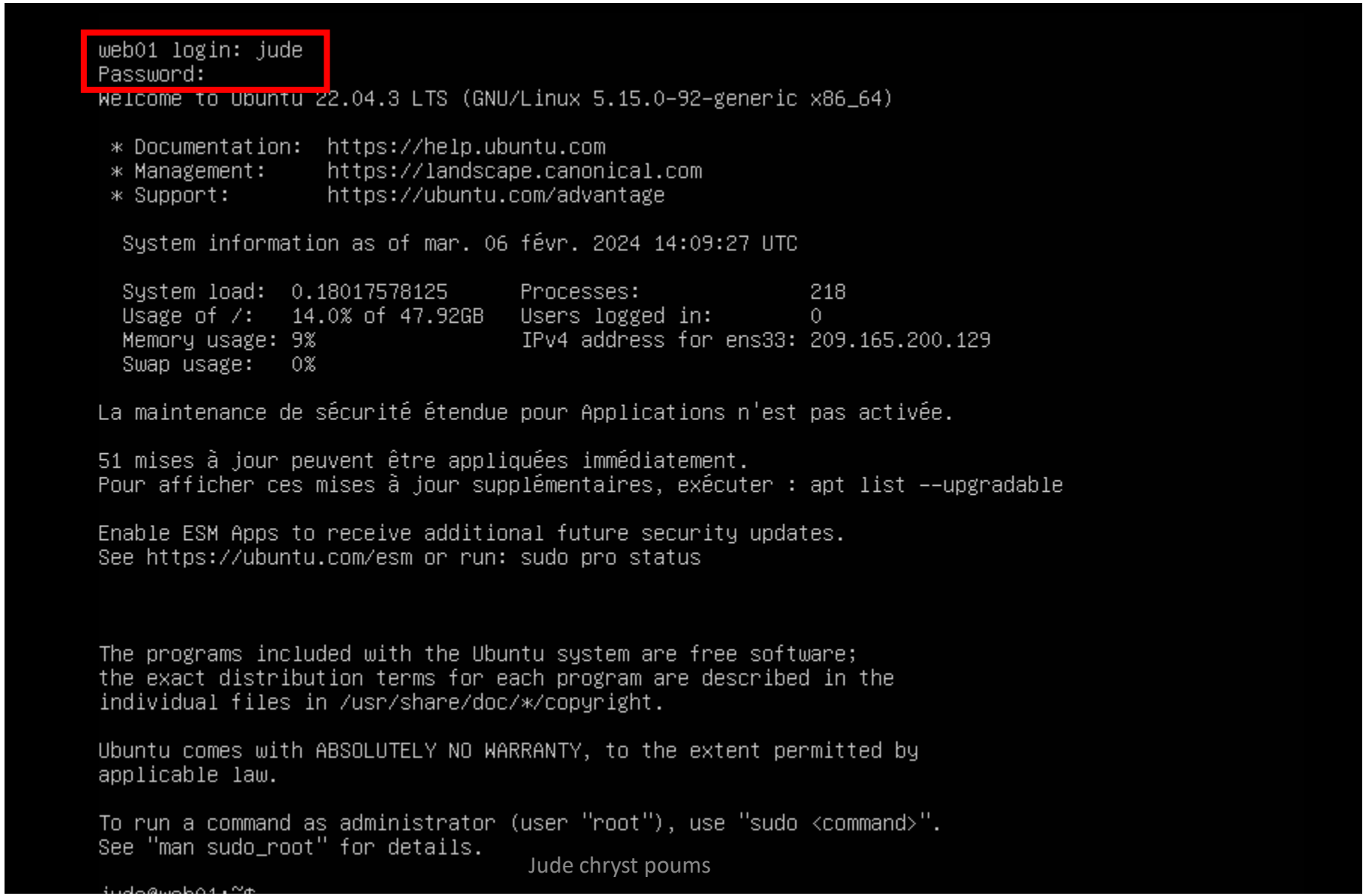

Featured Server Snaps
[Help]
These are popular snaps in server environments. Select or deselect with SPACE, press ENTER to see more details of the package, publisher and versions available.
[ ] microk8s canonical✓ Kubernetes for workstations and appliances
[ ] nextcloud nextcloud✓ Nextcloud Server - A safe home for all your data
[ ] wekan xet7 Open-Source kanban
[ ] kata-containers katacontainers✓ Build lightweight VMs that seamlessly plug into the containers ecosystem
[ ] docker canonical✓ Docker container runtime
[ ] canonical-livepatch canonical✓ Canonical Livepatch Client
[ ] rocketchat-server rocketchat✓ Rocket.Chat server
[ ] mosquitto mosquitto✓ Eclipse Mosquitto MQTT broker
[ ] etcd canonical✓ Resilient key-value store by CoreOS
[ ] powershell microsoft-powershell✓ PowerShell for every system!
[ ] sabnzbd safihre SABnzbd
[ ] wormhole snapcrafters get things from one computer to another, safely
[ ] aws-cli aws✓ Universal Command Line Interface for Amazon Web Services
[ ] google-cloud-sdk google-cloud-sdk✓ Google Cloud SDK
[ ] slcli softlayer Python based SoftLayer API Tool.
[ ] doctl digitalocean✓ The official DigitalOcean command line interface
[ ] conjure-up canonical✓ Package runtime for conjure-up spells
[ ] postgresql10 cmd✓ PostgreSQL is a powerful, open source object-relational database system.
[ ] heroku heroku✓ CLI client for Heroku
[ ] keepalived keepalived-project✓ High availability VRRP/BFD and load-balancing for Linux
[ ] prometheus canonical✓ The Prometheus monitoring system and time series database
[ ] juju canonical✓ Juju - a model-driven operator lifecycle manager for K8s and machines
Tout en bas cliquer sur terminer

Installation du système [Help]

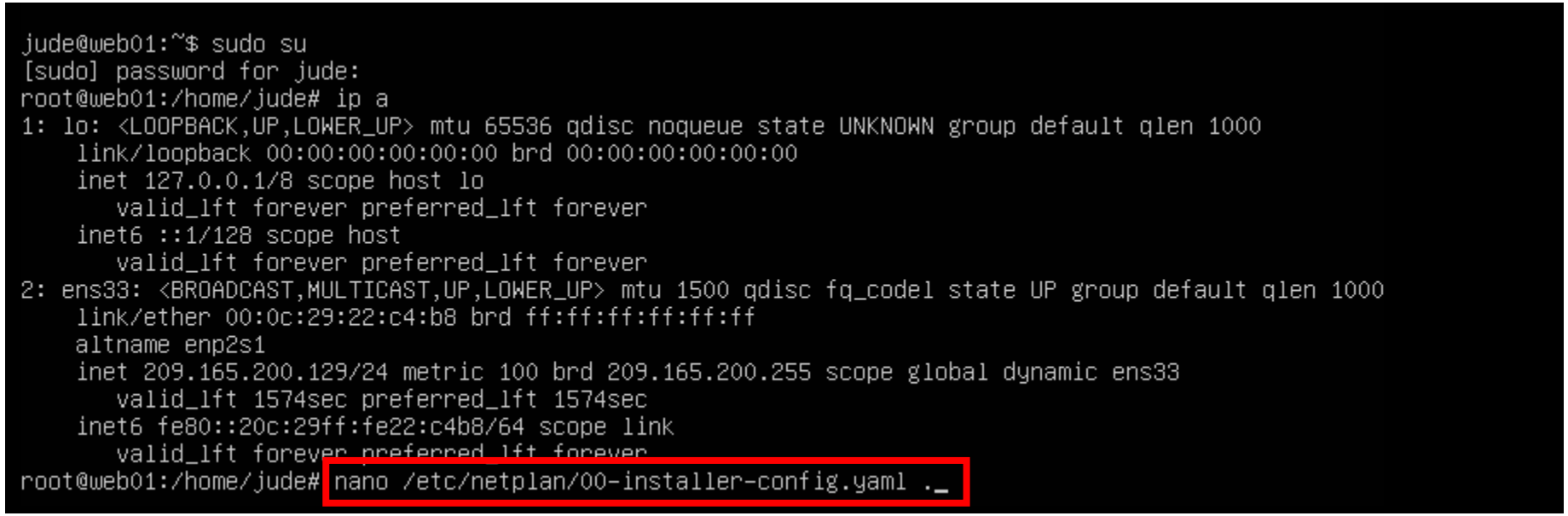
```
    configuring storage
      running 'curtin block-meta simple'
        curtin command block-meta
          removing previous storage devices
          configuring disk: disk-sda
        configuring partition: partition-0
        configuring partition: partition-1
        configuring format: format-0
        configuring partition: partition-2
        configuring dm_crypt: dm_crypt-0
        configuring lvm_volgroup: lvm_volgroup-0
        configuring lvm_partition: lvm_partition-0
        configuring format: format-1
        configuring mount: mount-1
        configuring mount: mount-0
executing curtin install extract step
  curtin command install
    writing install sources to disk
      running 'curtin extract'
        curtin command extract
          acquiring and extracting image from cp:///tmp/tmp13dt9mhx/mount
executing curtin install curthooks step
  curtin command install
    configuring installed system
      running 'curtin in-target -- setupcon --save-only'
        curtin command in-target
      running 'curtin curthooks'
        curtin command curthooks
          configuring apt configuring apt
          installing missing packages
          configuring iscsi service
          configuring raid (mdadm) service
          installing kernel
          setting up swap
          apply networking config
```



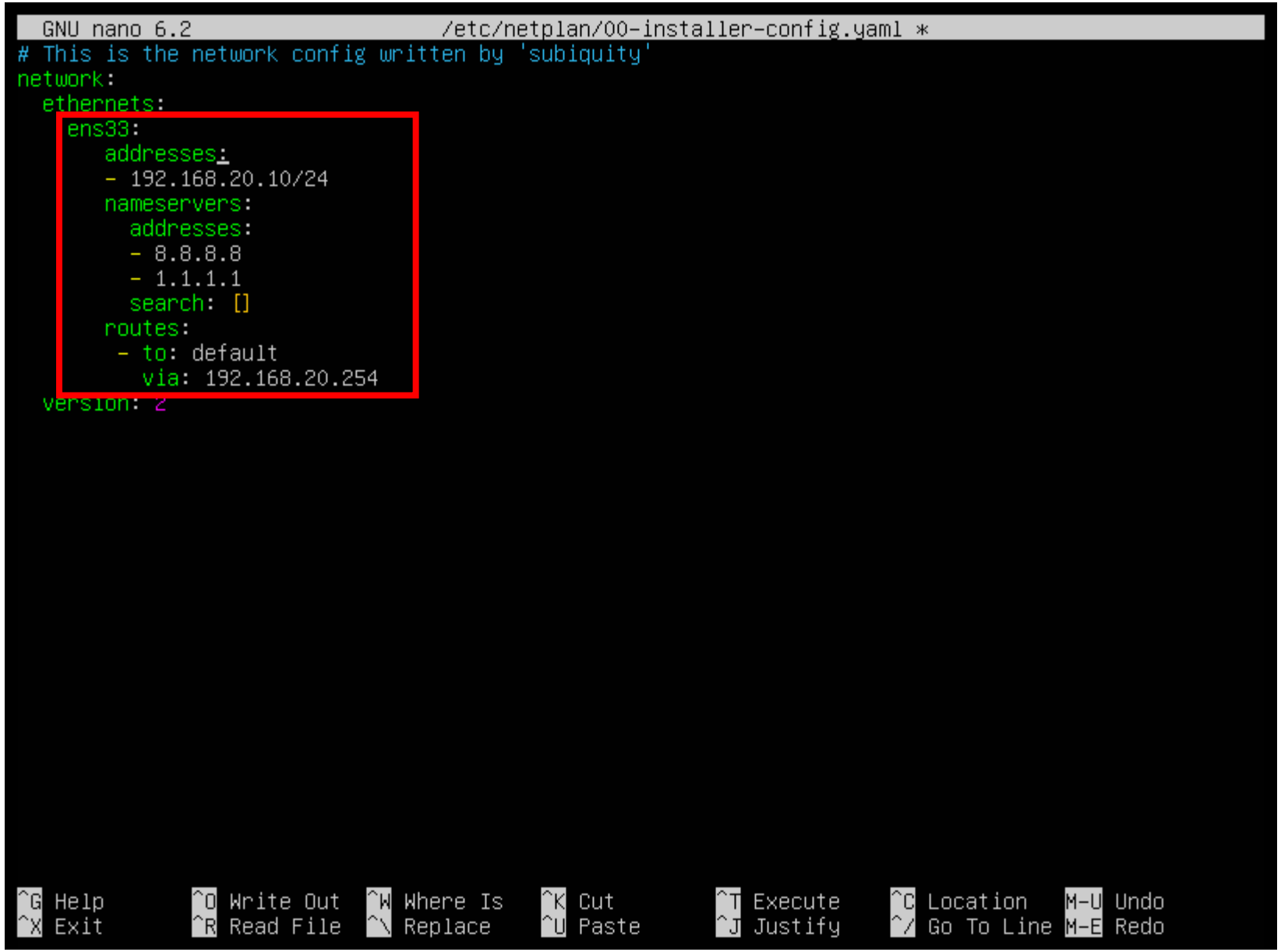
Tout en bas cliquer sur Redémarrer maintenant


web01 login: jude
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-92-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of mar. 06 févr. 2024 14:09:27 UTC
System load: 0.18017578125
Usage of /: 14.0% of 47.92GB
Memory usage: 9%
Swap usage: 0%
Processes: 218
Users logged in: 0
IPv4 address for ens33: 209.165.200.129
La maintenance de sécurité étendue pour Applications n'est pas activée.
51 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

 # nano /etc/netplan/00-installer-config.yaml



```
network:
  ethernets:
    ens33:
      addresses:
      - 192.168.20.10/24
      nameservers:
       addresses:
       - 8.8.8.8
       - 1.1.1.1
       search:  []
      routes:
      - to: default
        via: 192.168.20.254
 version: 2
```



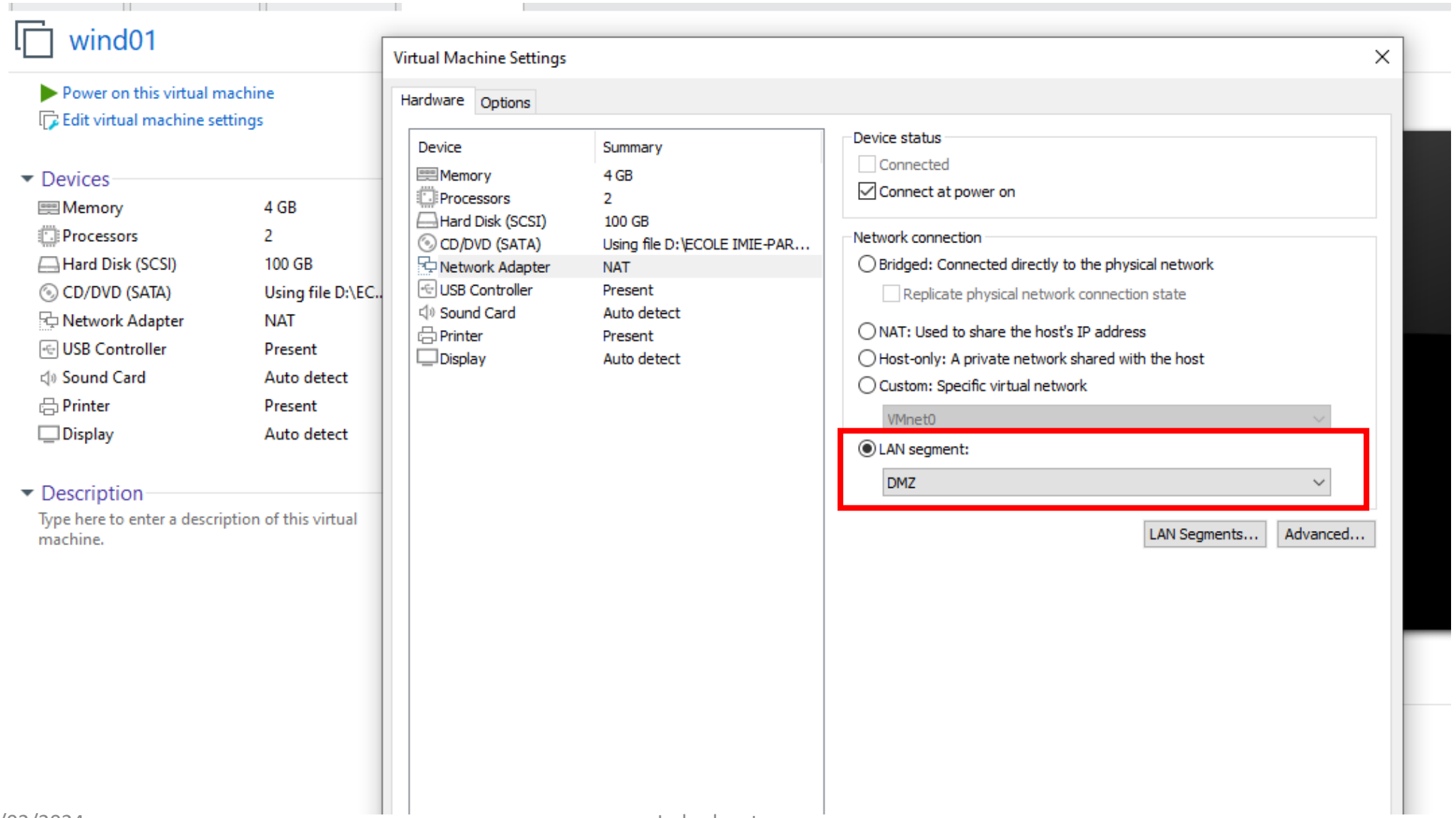
 # netplan apply
 # ping 8.8.8.8
 # ip a

```
        routes:
        -to: default
          via: 192.168.20.254
    version: 2
```

```
root@web01:/home/jude# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=6.01 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=5.23 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=5.40 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=5.15 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=5.18 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 5.146/5.391/6.008/0.320 ms
root@web01:/home/jude# netplan apply_
```

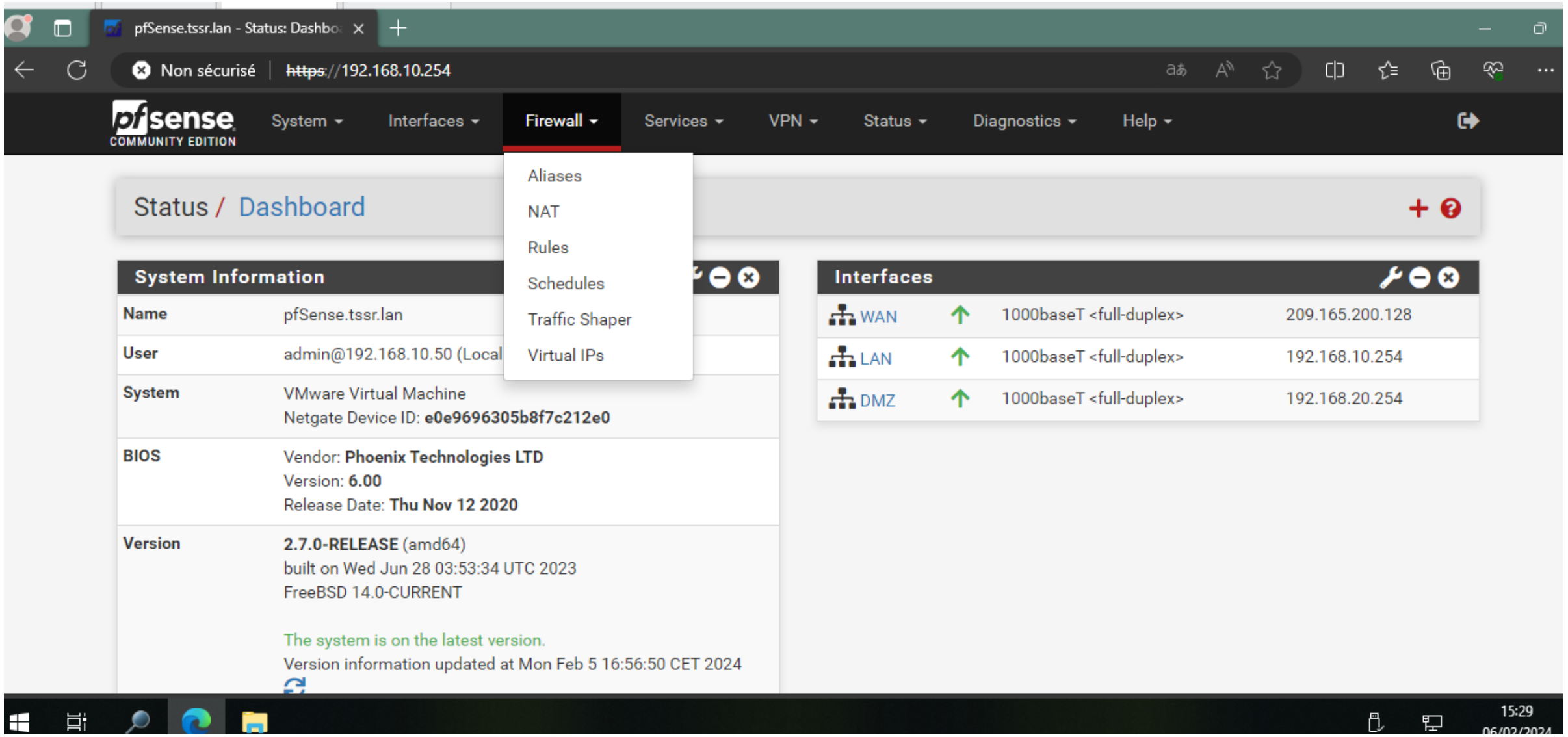
```
root@web01:/home/jude# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=5.59 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=5.09 ms
^X^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 5.094/5.341/5.588/0.247 ms
root@web01:/home/jude# netplan apply
root@web01:/home/jude# 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
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:22:c4:b8 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.10/24 brd 192.168.20.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe22:c4b8/64 scope link
       valid_lft forever preferred_lft forever
root@web01:/home/jude# ^C
root@web01:/home/jude# _
```

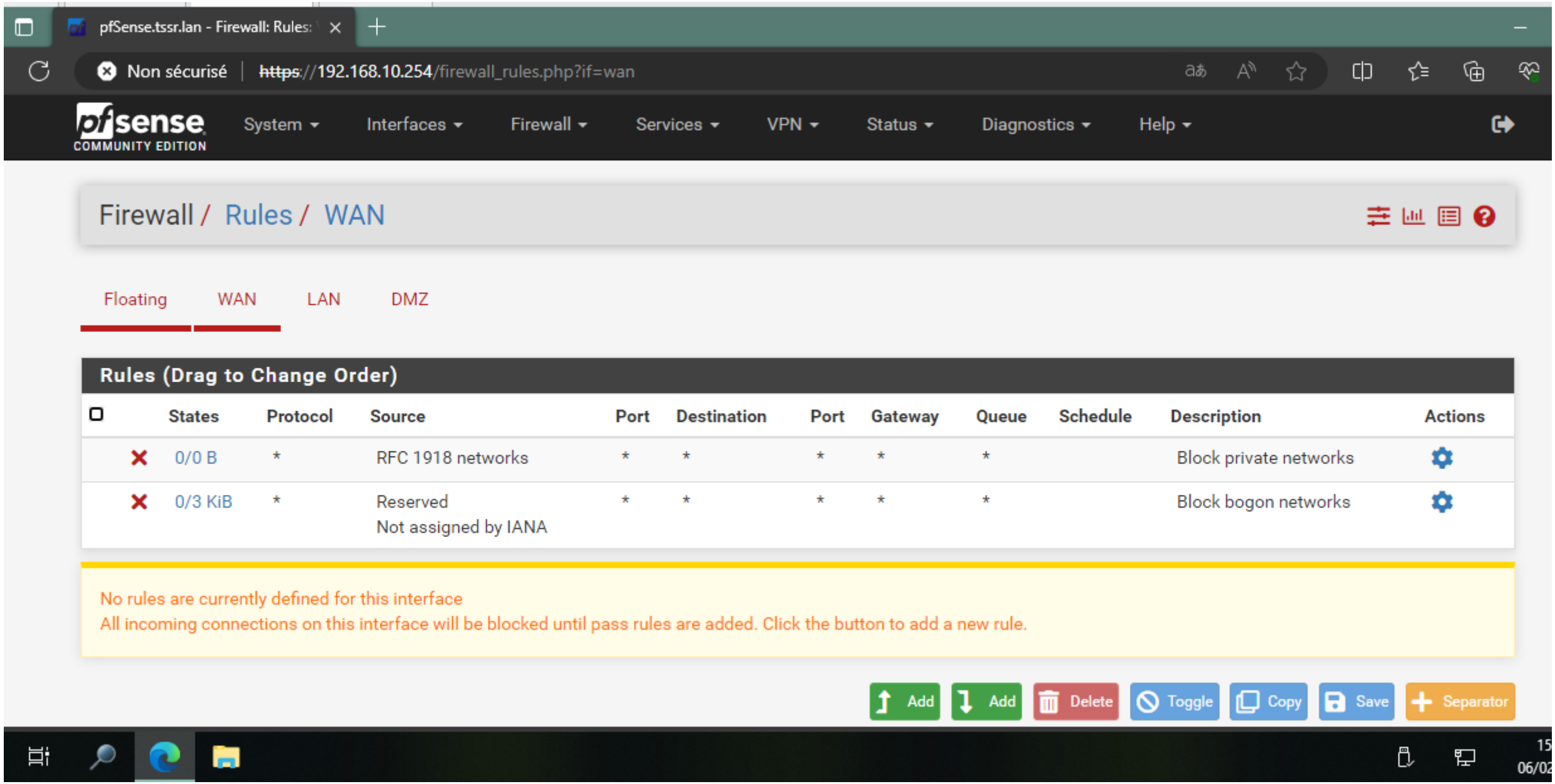
Mettre la machine ubuntu-server en DMZ

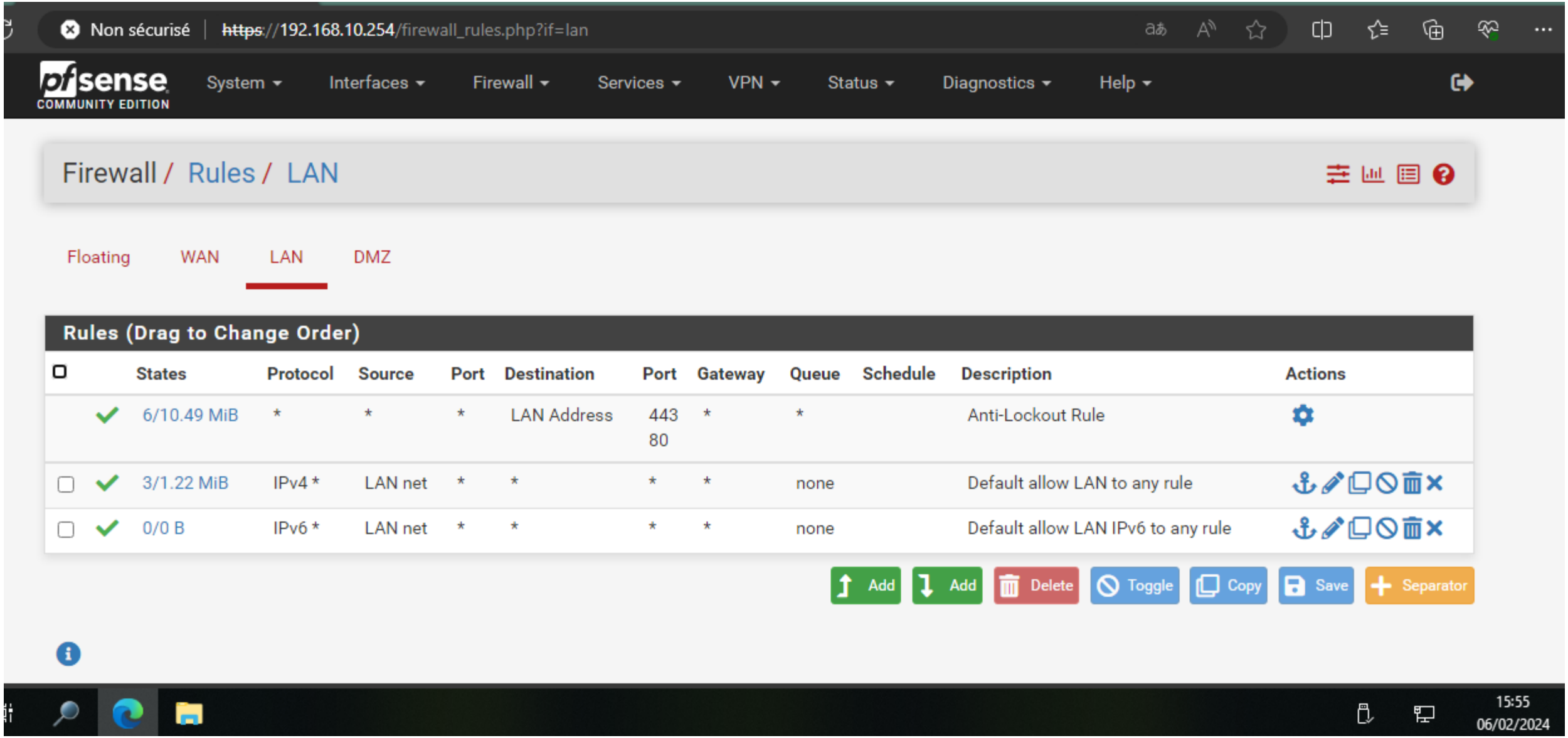


MACHINE CLIENTE WINDOWS 10

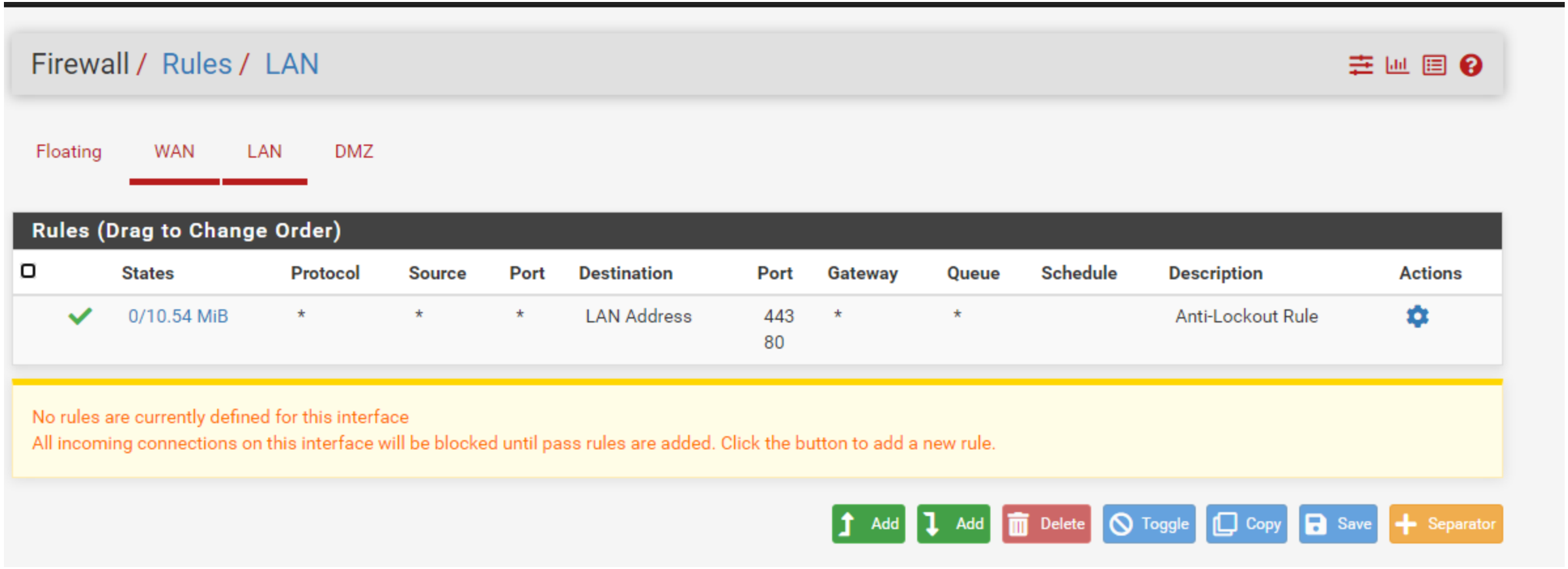
PFSENSE INTERFACE WEB


pfSense.tssr.lan - Status: Dashbo
Non sécurisé | https://192.168.10.254
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs
Status / Dashboard
System Information
Name pfSense.tssr.lan
User admin@192.168.10.50 (Local
System VMware Virtual Machine
Netgate Device ID: e0e9696305b8f7c212e0
BIOS Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020
Version 2.7.0-RELEASE (amd64)
built on Wed Jun 28 03:53:34 UTC 2023
FreeBSD 14.0-CURRENT
The system is on the latest version.
Version information updated at Mon Feb 5 16:56:50 CET 2024
Interfaces
WAN 1000baseT <full-duplex> 209.165.200.128
LAN 1000baseT <full-duplex> 192.168.10.254
DMZ 1000baseT <full-duplex> 192.168.20.254
15:29
06/02/2024


pfSense.tssr.lan - Firewall: Rules:
Non sécurisé
https://192.168.10.254/firewall_rules.php?if=wan
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / WAN
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
*
RFC 1918 networks
Block private networks
0/3 KiB
Reserved
Not assigned by IANA
Block bogon networks
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.
Add
Add
Delete
Toggle
Copy
Save
Separator


Non sécurisé | https://192.168.10.254/firewall_rules.php?if=lan
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
6/10.49 MiB * * * LAN Address 443 80 * * Anti-Lockout Rule
3/1.22 MiB IPv4 * LAN net * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator
15:55
06/02/2024

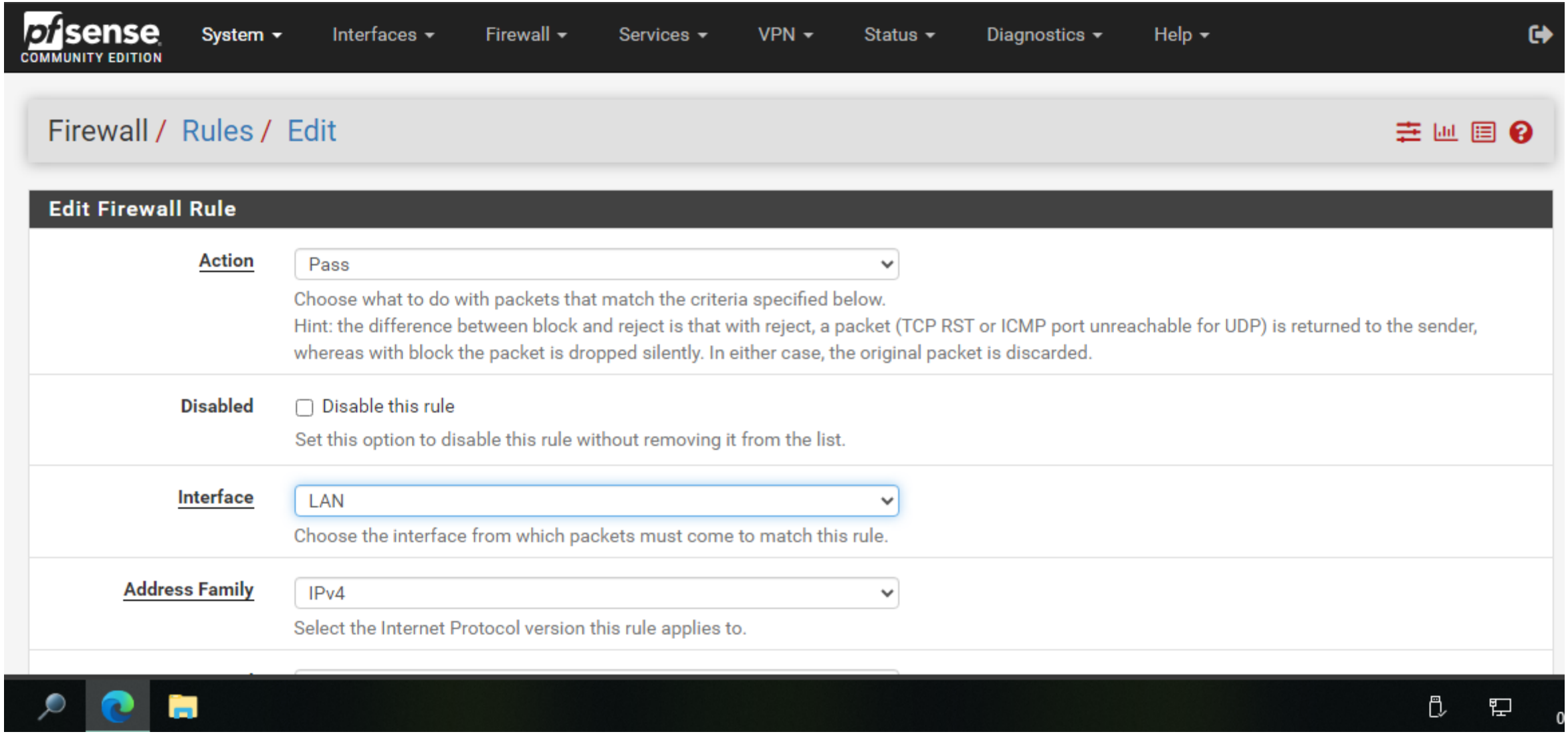

3/1.22 MiB IPv4 * LAN net * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN net * * * * none Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator

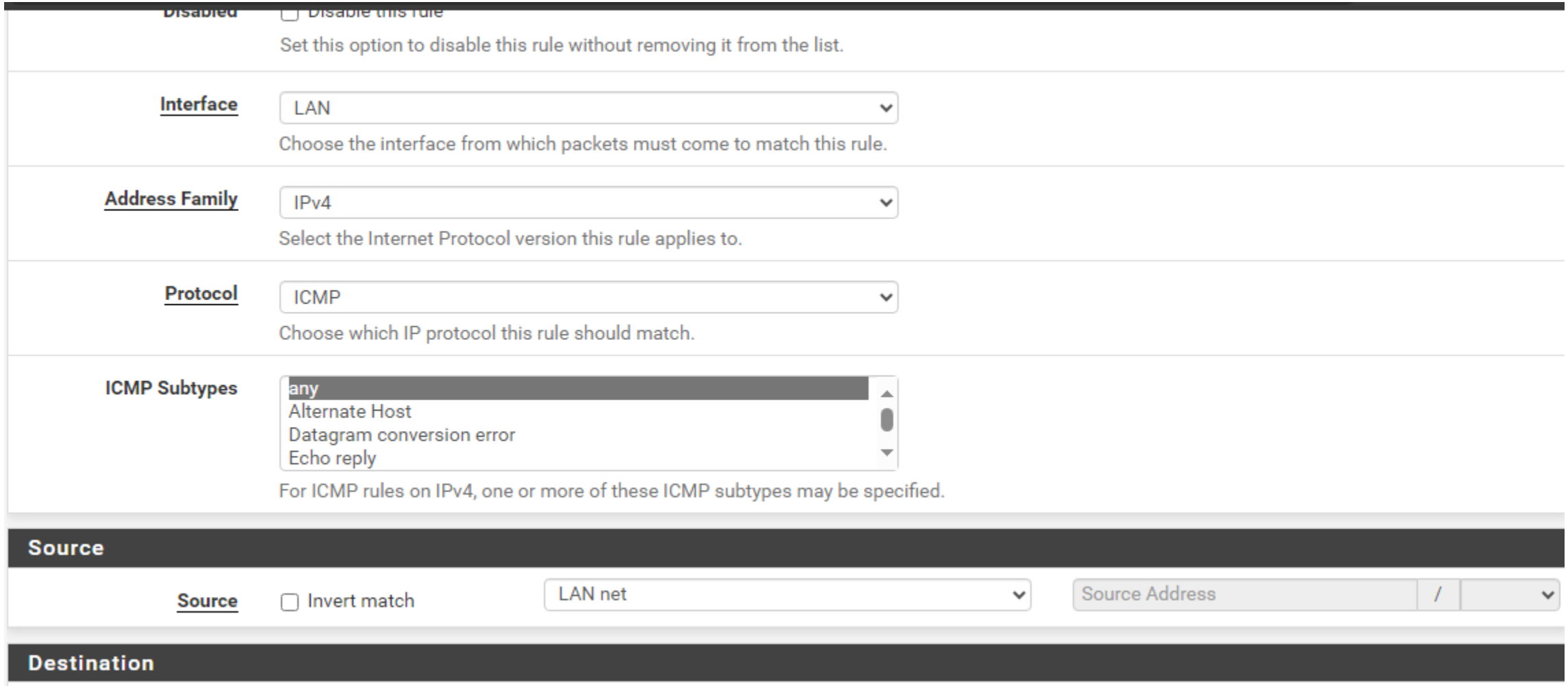

Firewall / Rules / LAN
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/10.54 MiB
*
*
*
LAN Address
443
80
*
*
Anti-Lockout Rule
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.
Add
Add
Delete
Toggle
Copy
Save
Separator

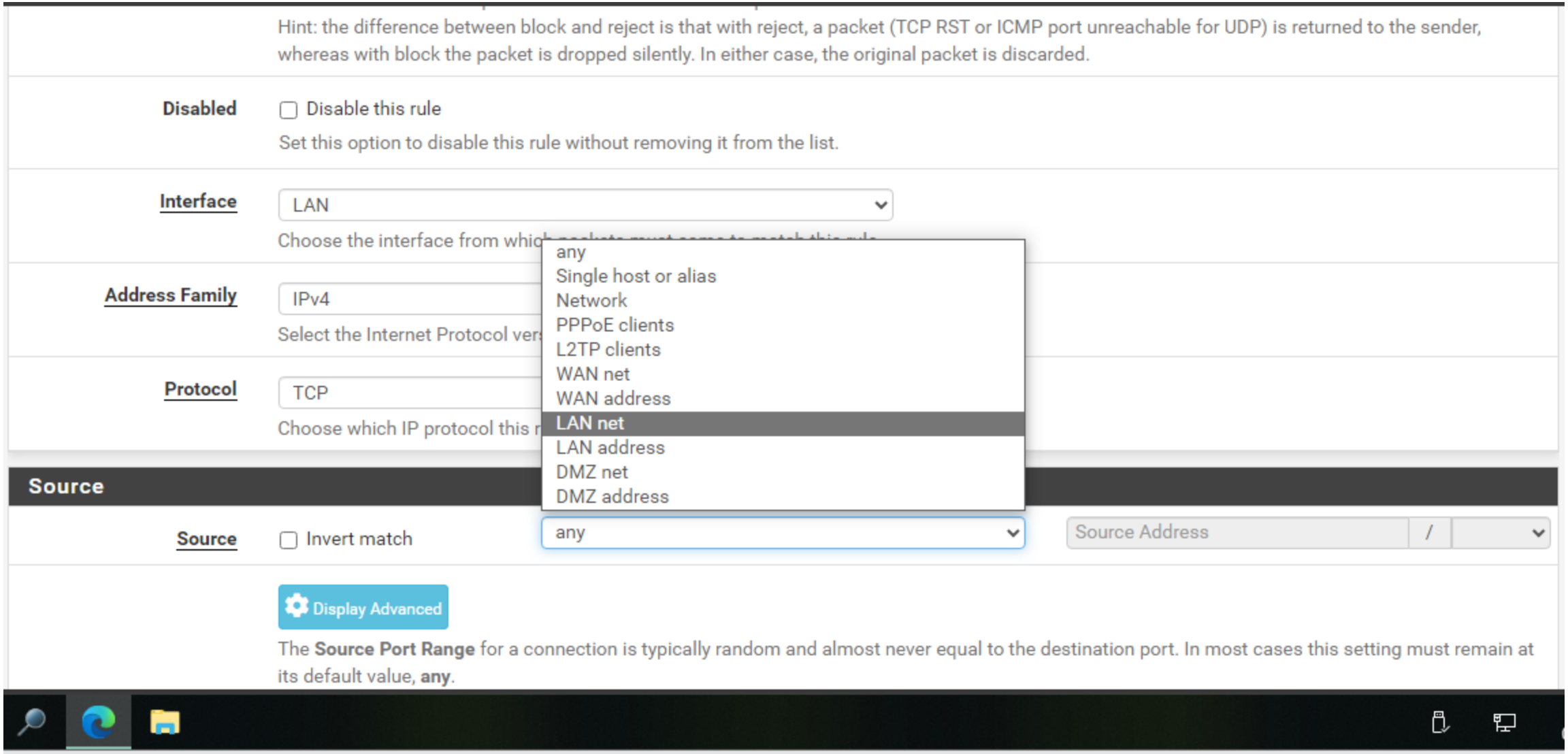
MACHINE CLIENTE WINDOWS 10

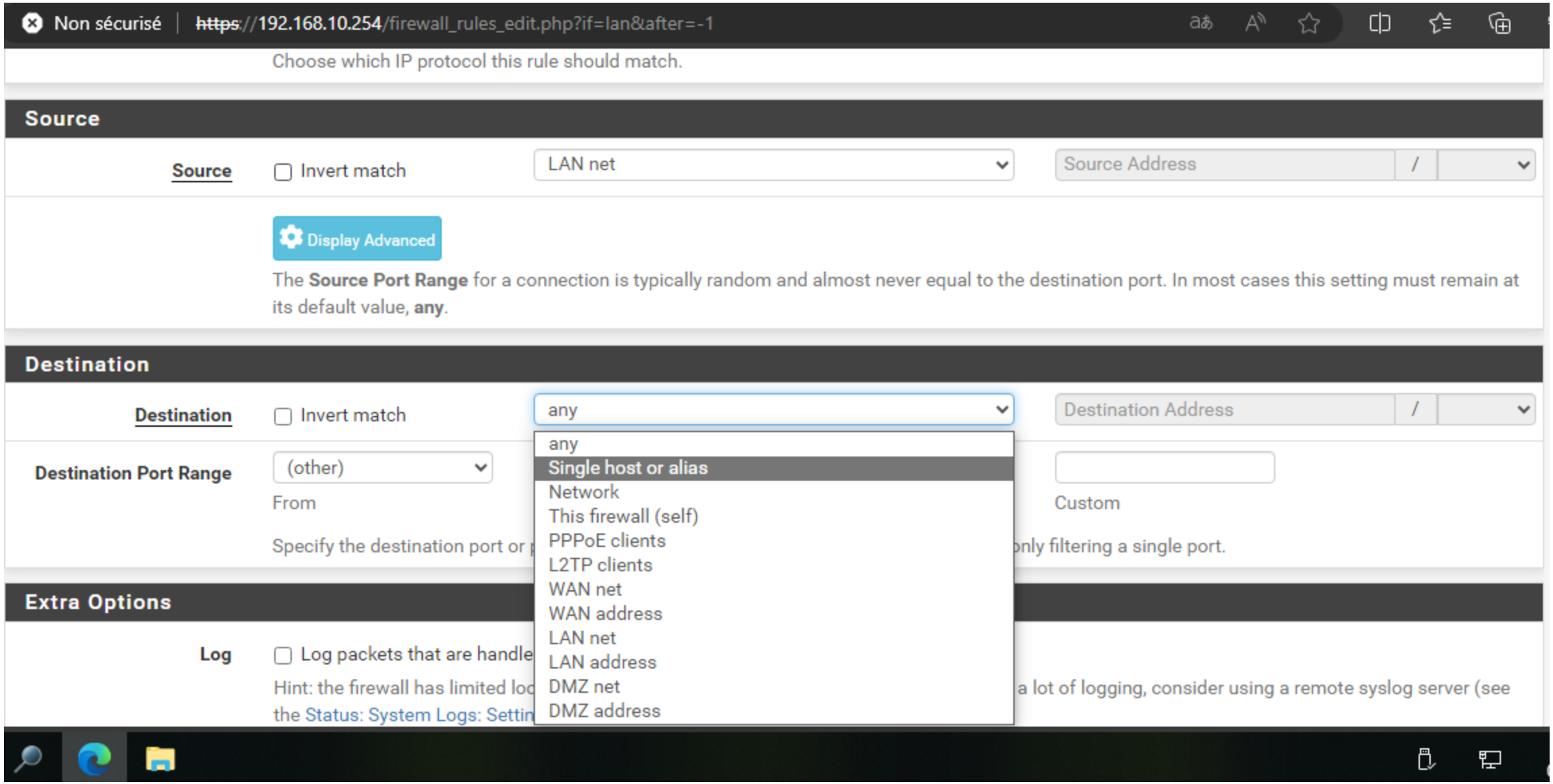
PFSENSE INTERFACE WEB

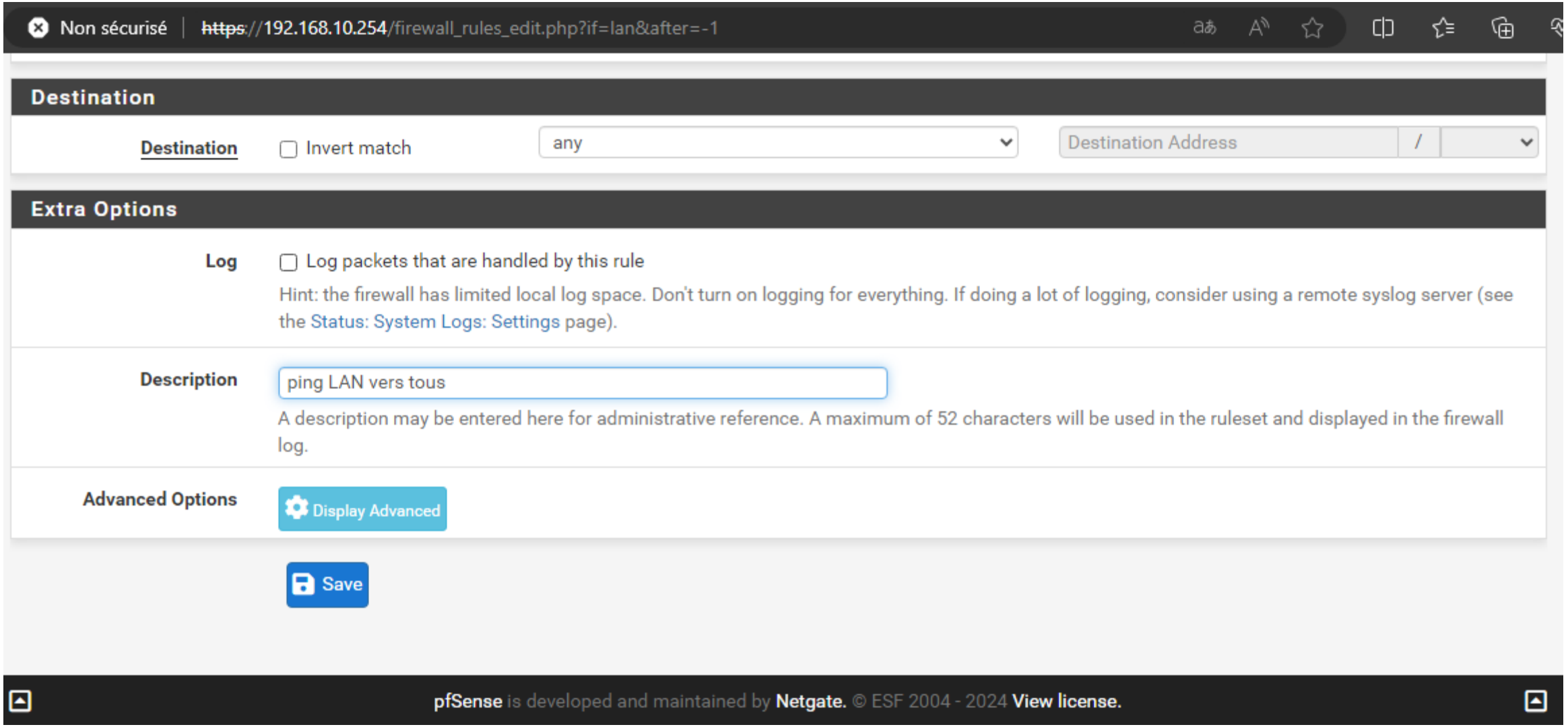
Créer une règle de ping LAN vers tous

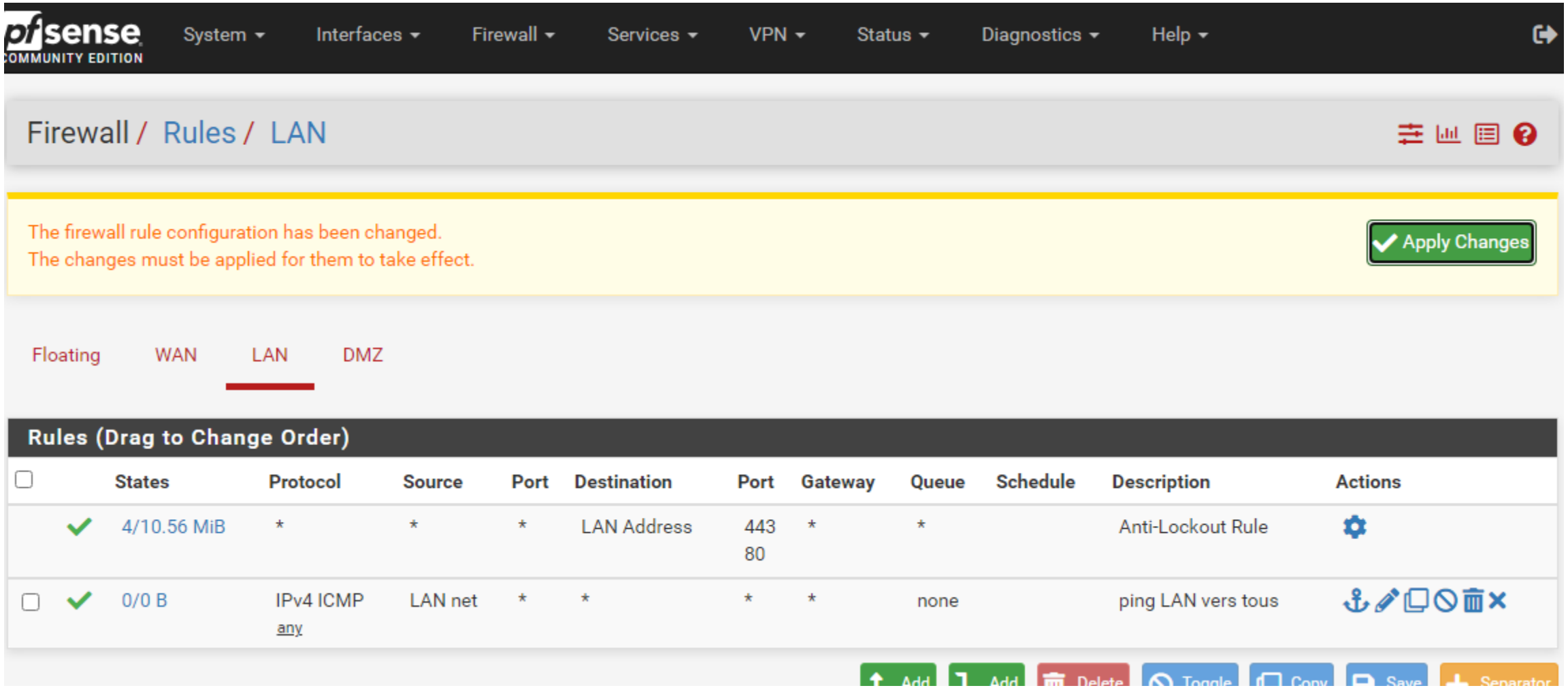

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST 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
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.

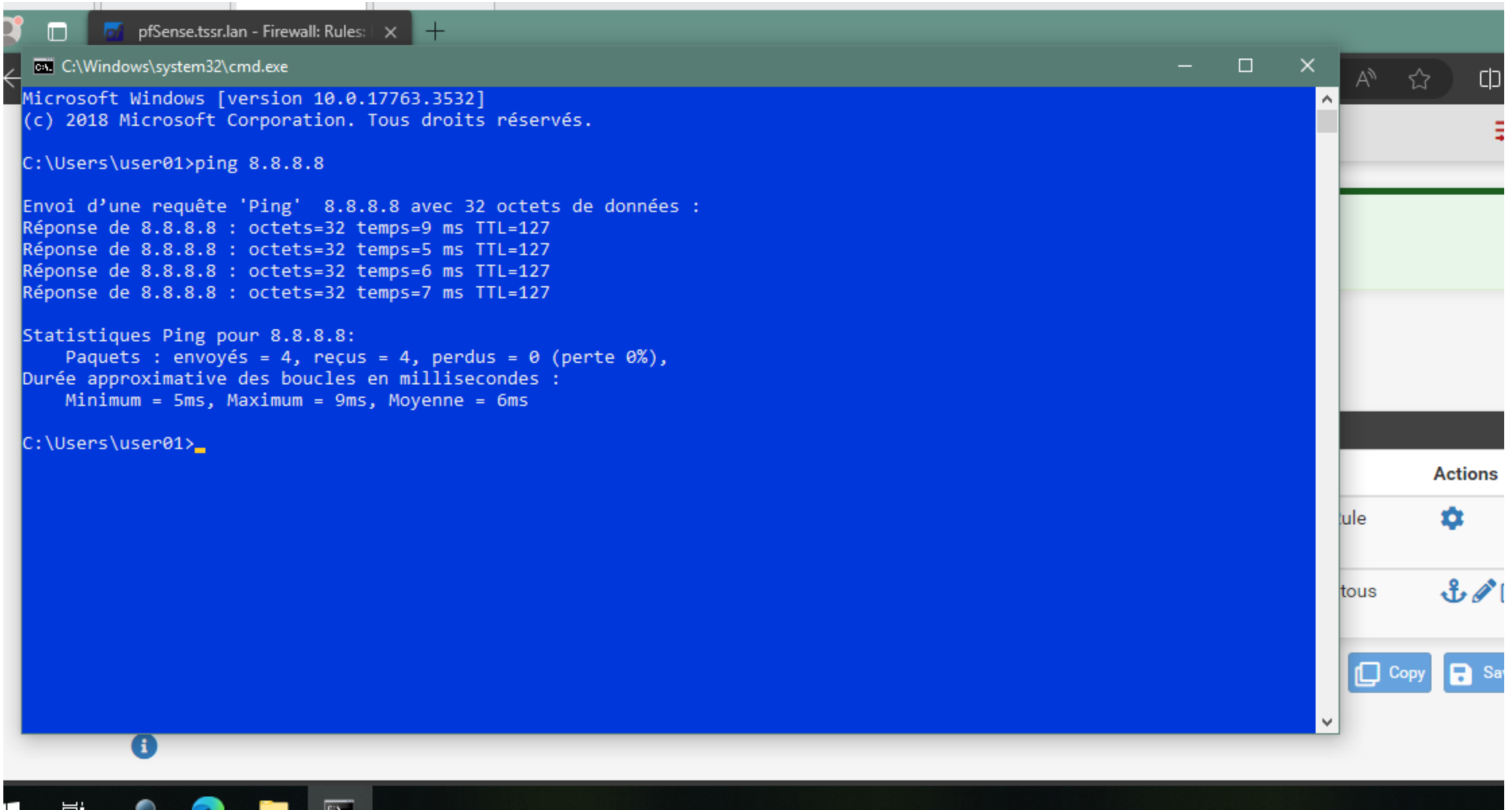

Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
ICMP
Choose which IP protocol 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
LAN net
Source Address
/
Destination


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 whic
Address Family
IPv4
Select the Internet Protocol ver
Protocol
TCP
Choose which IP protocol this r
any
Single host or alias
Network
PPPoE clients
L2TP clients
WAN net
WAN address
LAN net
LAN address
DMZ net
DMZ address
Source
Source
Invert match
any
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.


Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?if=lan&after=-1
Choose which IP protocol this rule should match.
Source
Source
Invert match
LAN net
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
/
Destination Port Range
(other)
From
Custom
Specify the destination port or
nly filtering a single port.
any
Single host or alias
Network
This firewall (self)
PPPoE clients
L2TP clients
WAN net
WAN address
LAN net
LAN address
DMZ net
DMZ address
Extra Options
Log
Log packets that are handle
Hint: the firewall has limited loc
a lot of logging, consider using a remote syslog server (see
the Status: System Logs: Settin


Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?if=lan&after=-1
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
ping LAN vers tous
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
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4/10.56 MiB
*
*
*
LAN Address
443
80
*
*
Anti-Lockout Rule
0/0 B
IPv4 ICMP
any
LAN net
*
*
*
*
none
ping LAN vers tous
Add
Add
Delete
Toggle
Copy
Save
Separator


pfSense.tssr.lan - Firewall: Rules:
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.17763.3532]
(c) 2018 Microsoft Corporation. Tous droits réservés.
C:\Users\user01>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=5 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=6 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=127
Statistiques Ping pour 8.8.8.8:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 5ms, Maximum = 9ms, Moyenne = 6ms
C:\Users\user01>
Actions
Copy

MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

Créer une règle de ping entre LAN IN WAN

Source

Source ☐ Invert match — LAN net — Source Address /

Destination

Destination ☐ Invert match — Single host or alias — 1.1.1.1 /

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).

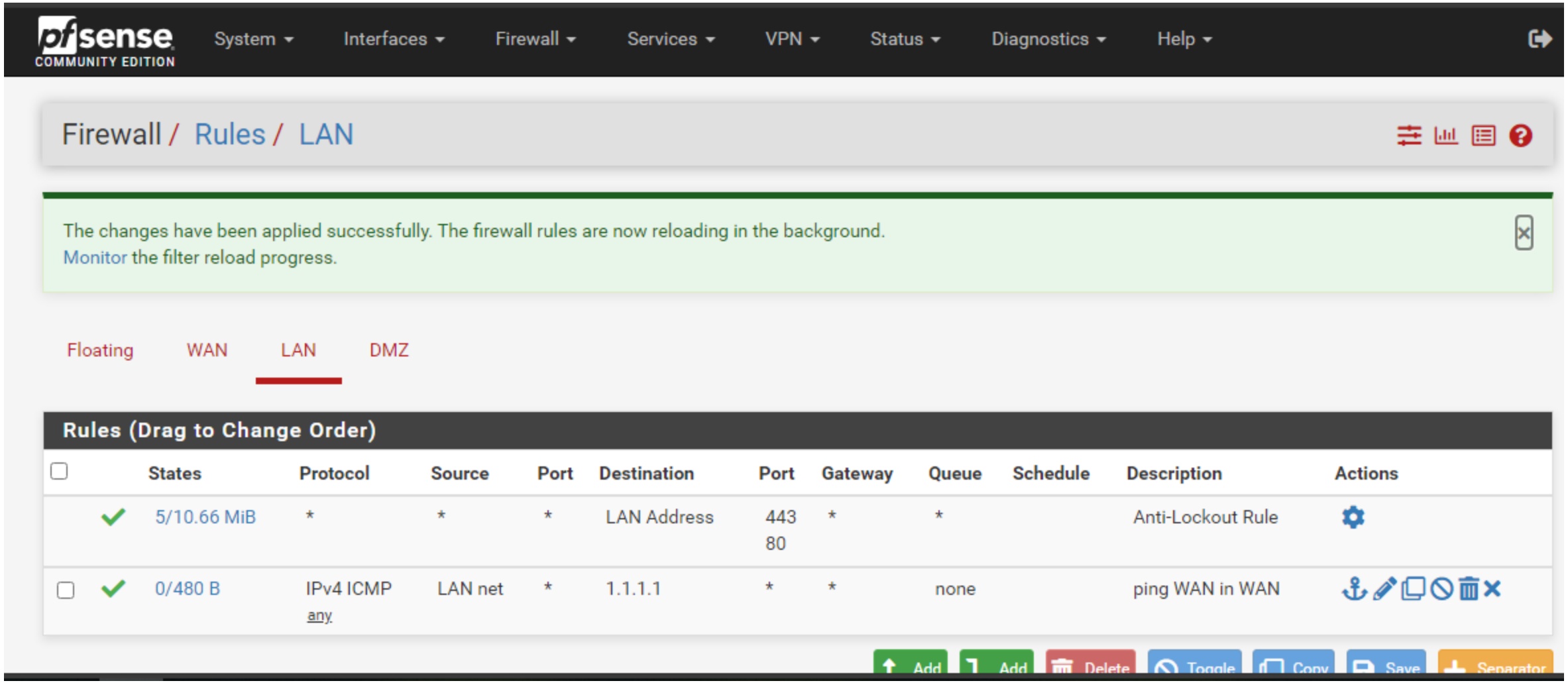
Description ping WAN in WAN

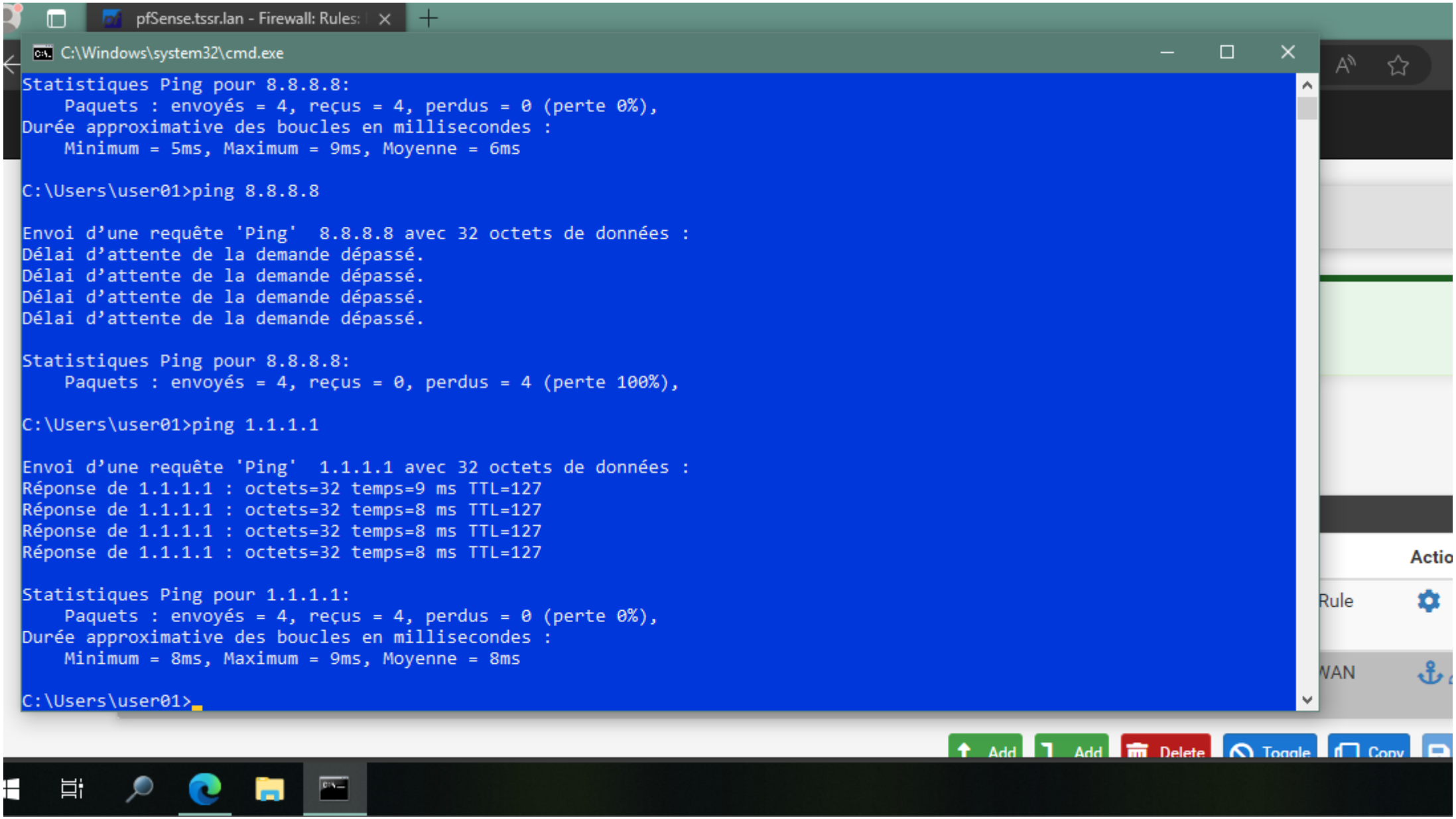
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Rule Information

Tracking ID 1707232465

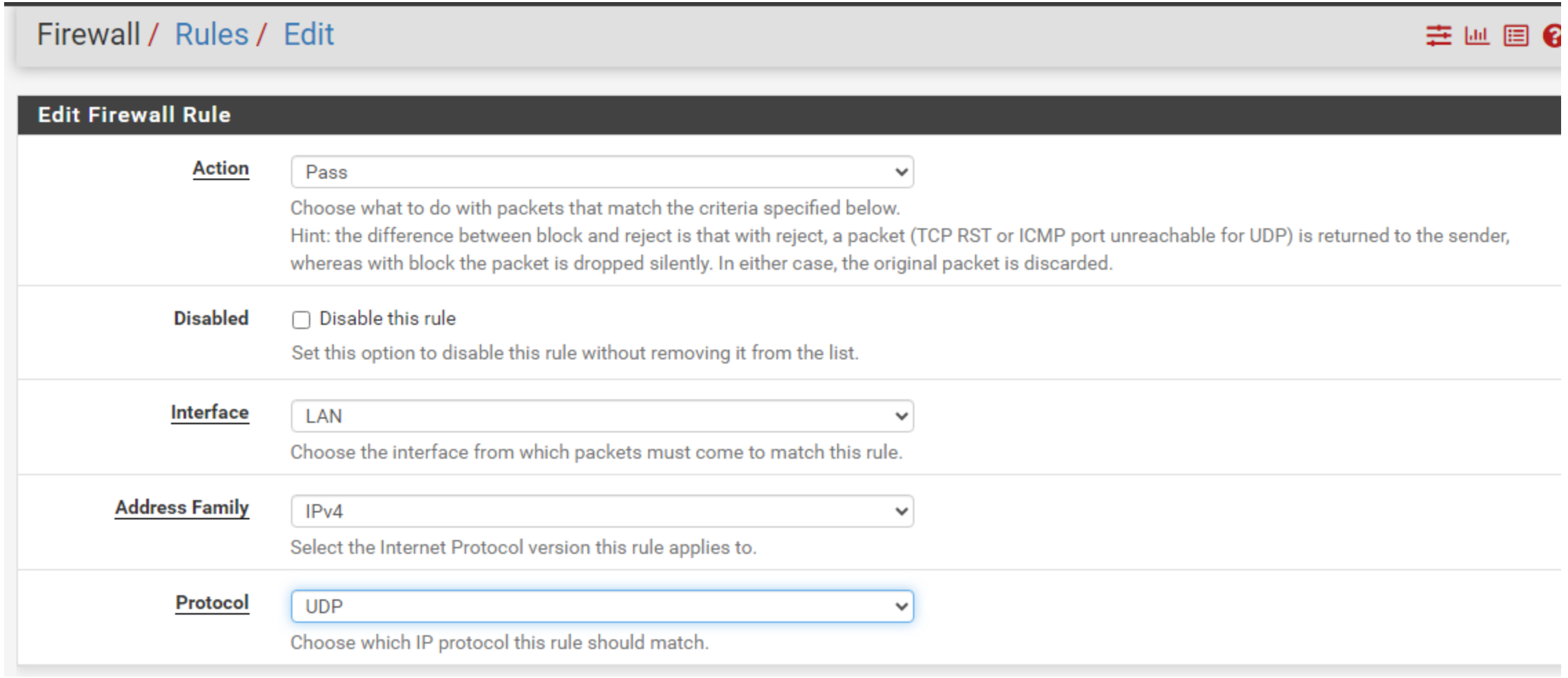

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
5/10.66 MiB
*
*
*
LAN Address
443
80
*
*
Anti-Lockout Rule
0/480 B
IPv4 ICMP
any
LAN net
*
1.1.1.1
*
*
none
ping WAN in WAN
Add
Add
Delete
Toggle
Copy
Save
Separator

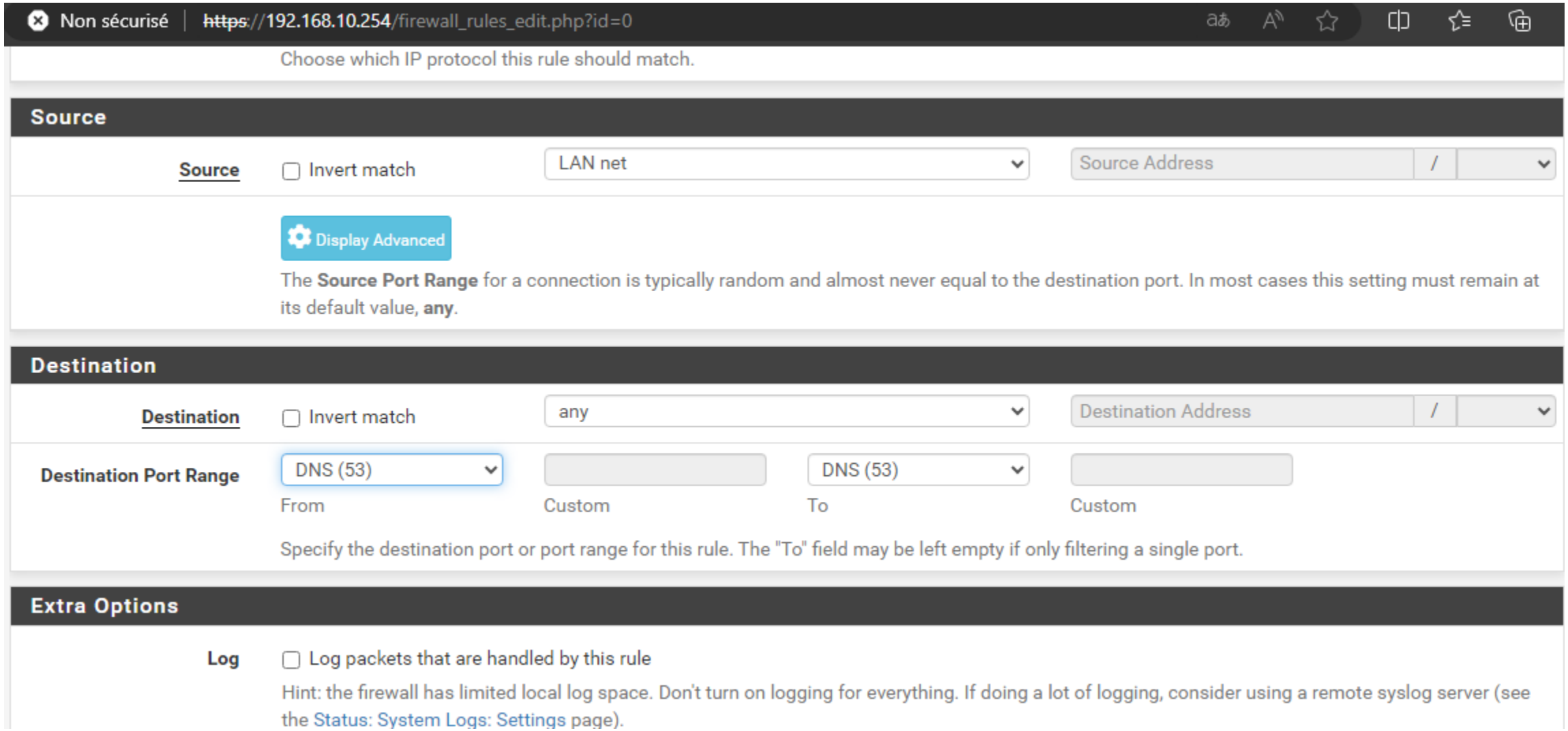

pfSense.tssr.lan - Firewall: Rules:
C:\Windows\system32\cmd.exe
Statistiques Ping pour 8.8.8.8:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 5ms, Maximum = 9ms, Moyenne = 6ms
C:\Users\user01>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Statistiques Ping pour 8.8.8.8:
Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
C:\Users\user01>ping 1.1.1.1
Envoi d'une requête 'Ping' 1.1.1.1 avec 32 octets de données :
Réponse de 1.1.1.1 : octets=32 temps=9 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=8 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=8 ms TTL=127
Réponse de 1.1.1.1 : octets=32 temps=8 ms TTL=127
Statistiques Ping pour 1.1.1.1:
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 8ms, Maximum = 9ms, Moyenne = 8ms
C:\Users\user01>
Actio
Rule
WAN
Add
Add
Delete
Toggle
Copy

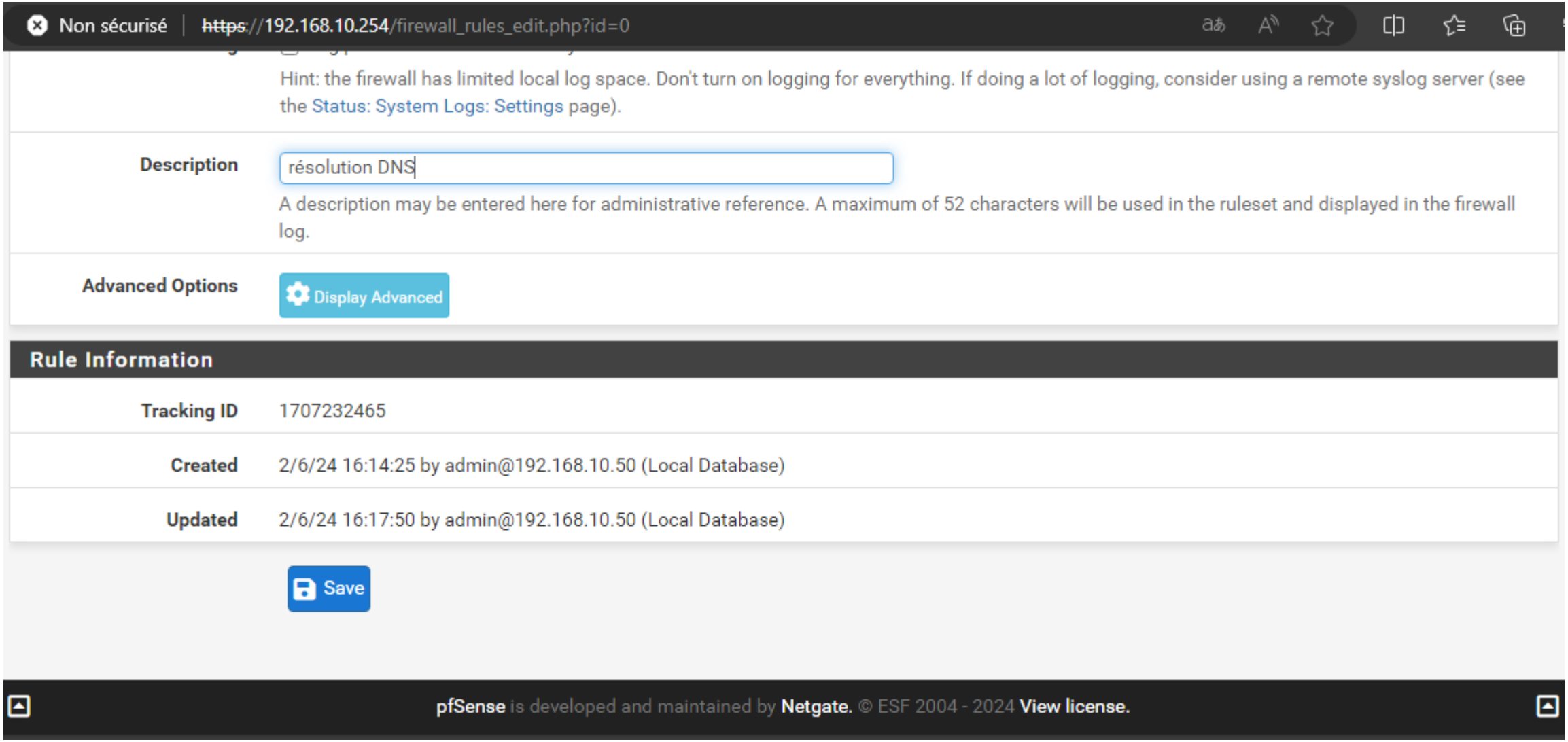
MACHINE CLIENTE WINDOWS 10

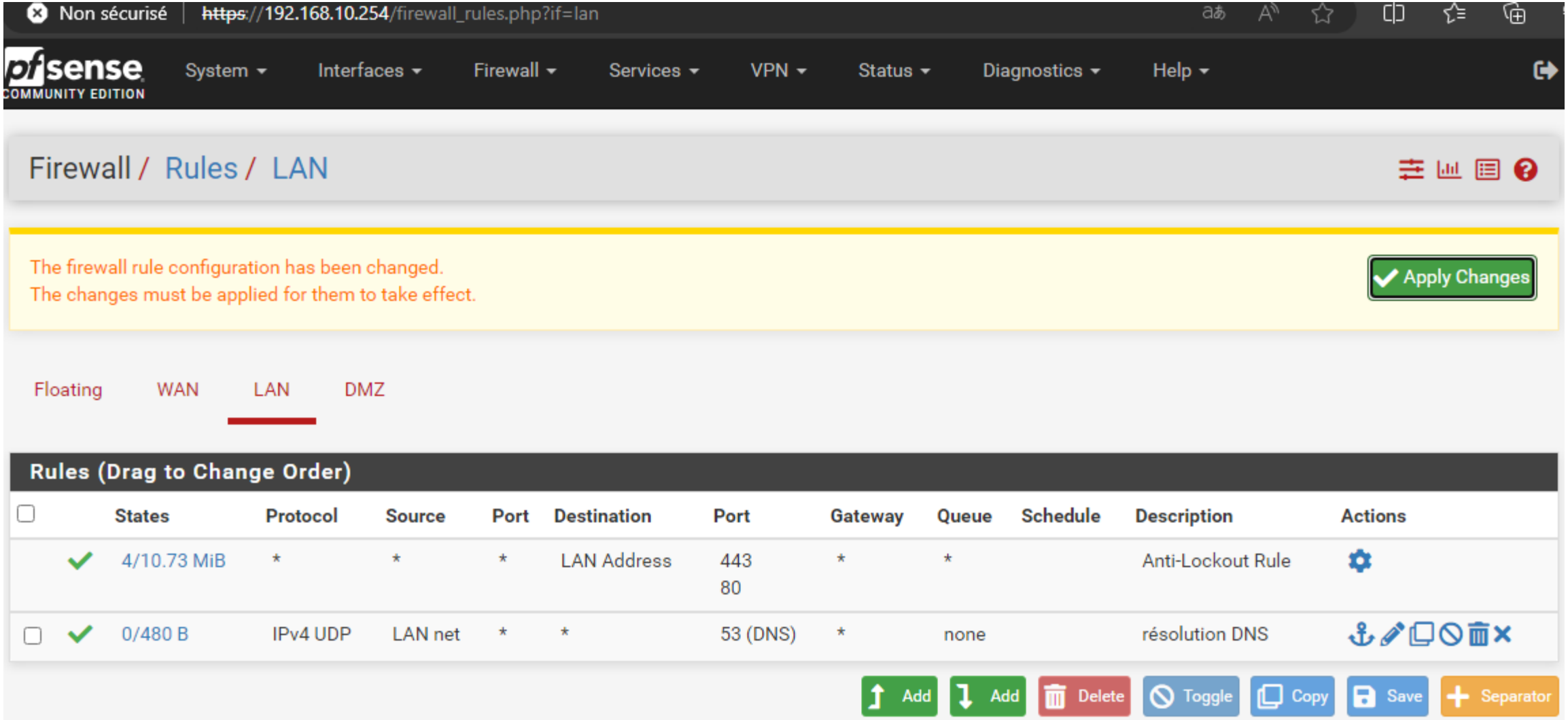
PFSENSE INTERFACE WEB

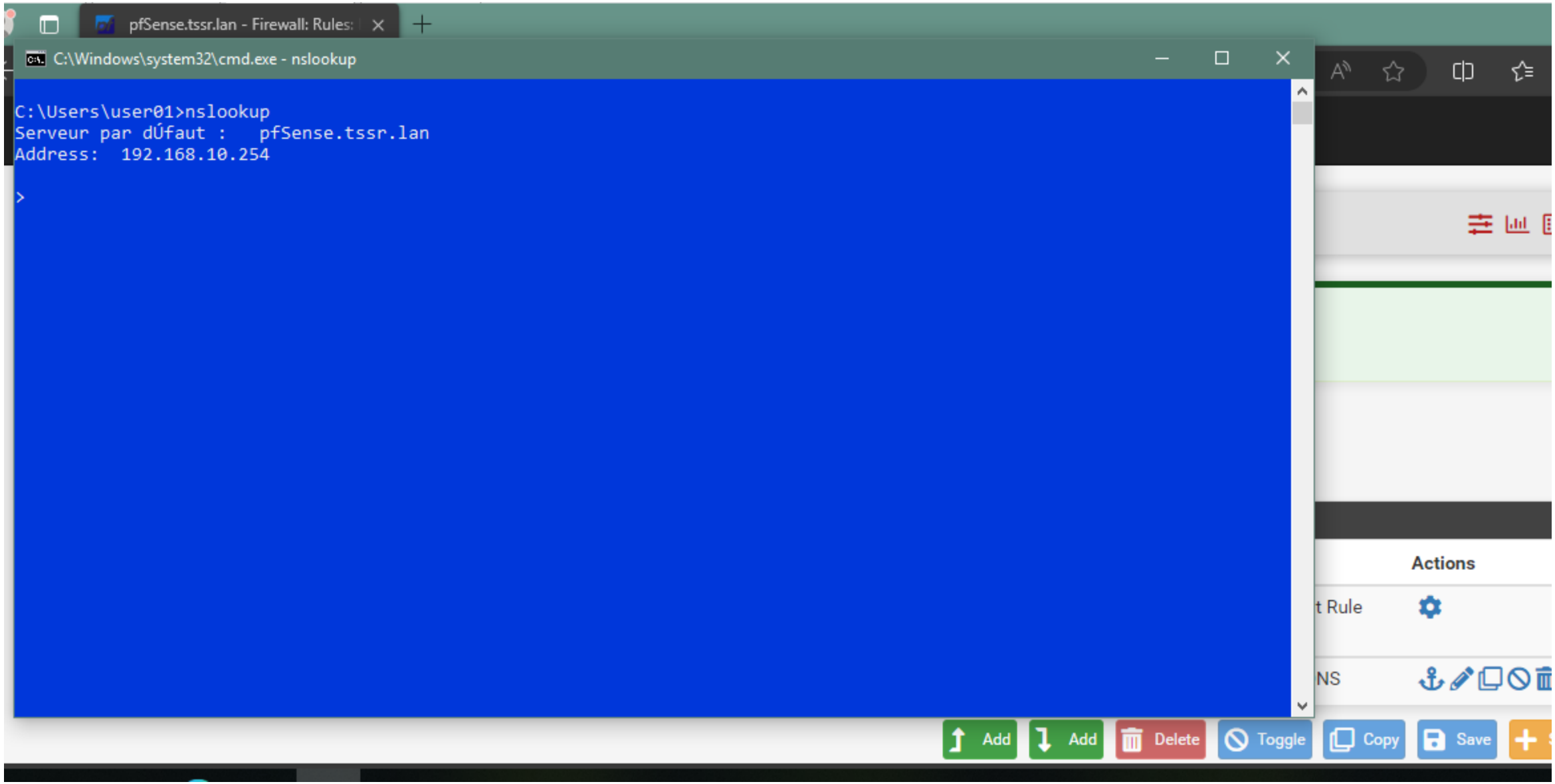
Créer une règle de résolution DNS


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
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
UDP
Choose which IP protocol this rule should match.


Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?id=0
Choose which IP protocol this rule should match.
Source
Source
Invert match
LAN net
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
/
Destination Port Range
DNS (53)
From
Custom
DNS (53)
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.
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).


Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?id=0
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
résolution DNS
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
Rule Information
Tracking ID
1707232465
Created
2/6/24 16:14:25 by admin@192.168.10.50 (Local Database)
Updated
2/6/24 16:17:50 by admin@192.168.10.50 (Local Database)
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


Non sécurisé
https://192.168.10.254/firewall_rules.php?if=lan
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4/10.73 MiB
* * * LAN Address 443 80 * * Anti-Lockout Rule
0/480 B
IPv4 UDP LAN net * * 53 (DNS) * none résolution DNS
Add
Add
Delete
Toggle
Copy
Save
Separator


pfSense.tssr.lan - Firewall: Rules:
C:\Windows\system32\cmd.exe - nslookup
C:\Users\user01>nslookup
Serveur par dÚfaut : pfSense.tssr.lan
Address: 192.168.10.254
>
Actions
t Rule
NS
Add
Add
Delete
Toggle
Copy
Save

MACHINE CLIENTE WINDOWS 10

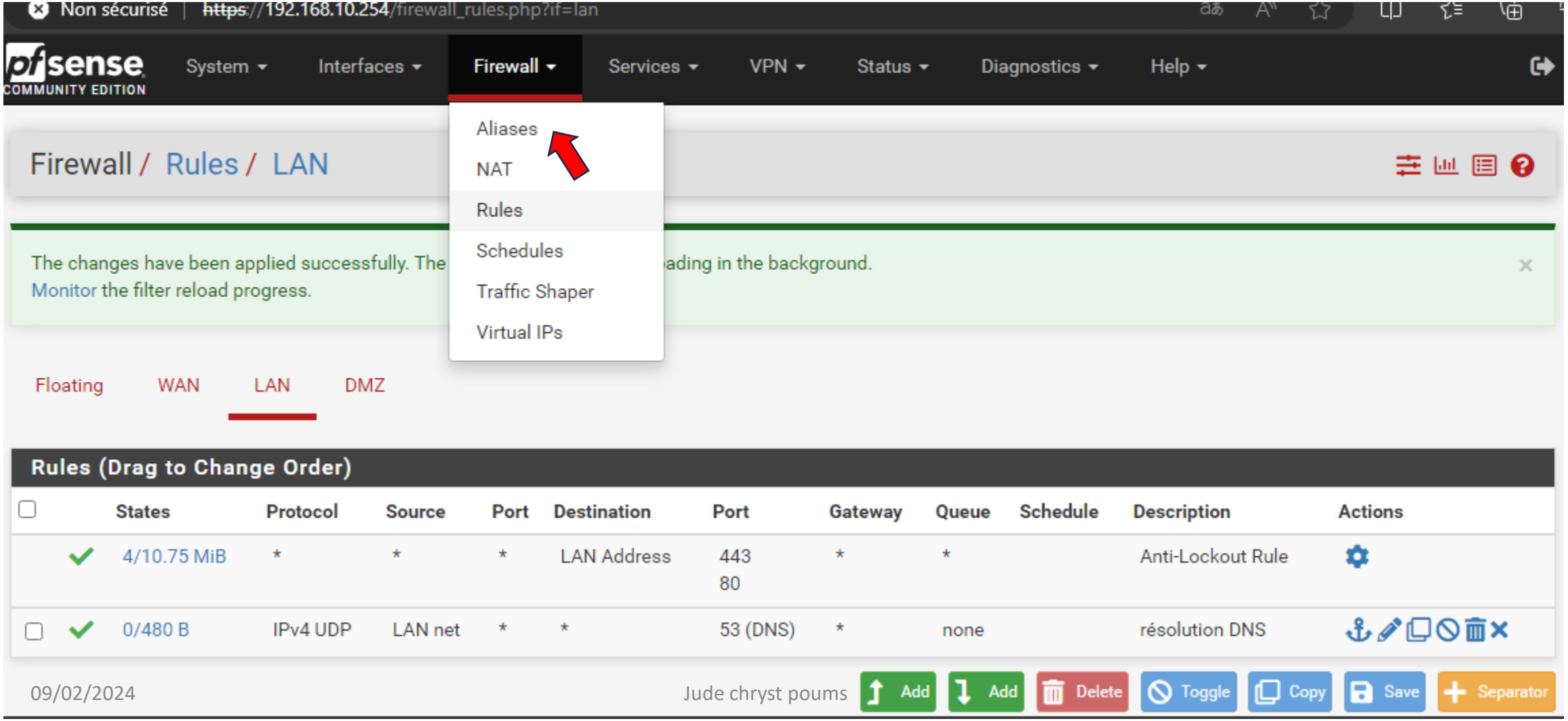
PFSENSE INTERFACE WEB

Créer un alias pour accéder a des pages web http(80)/https(443)

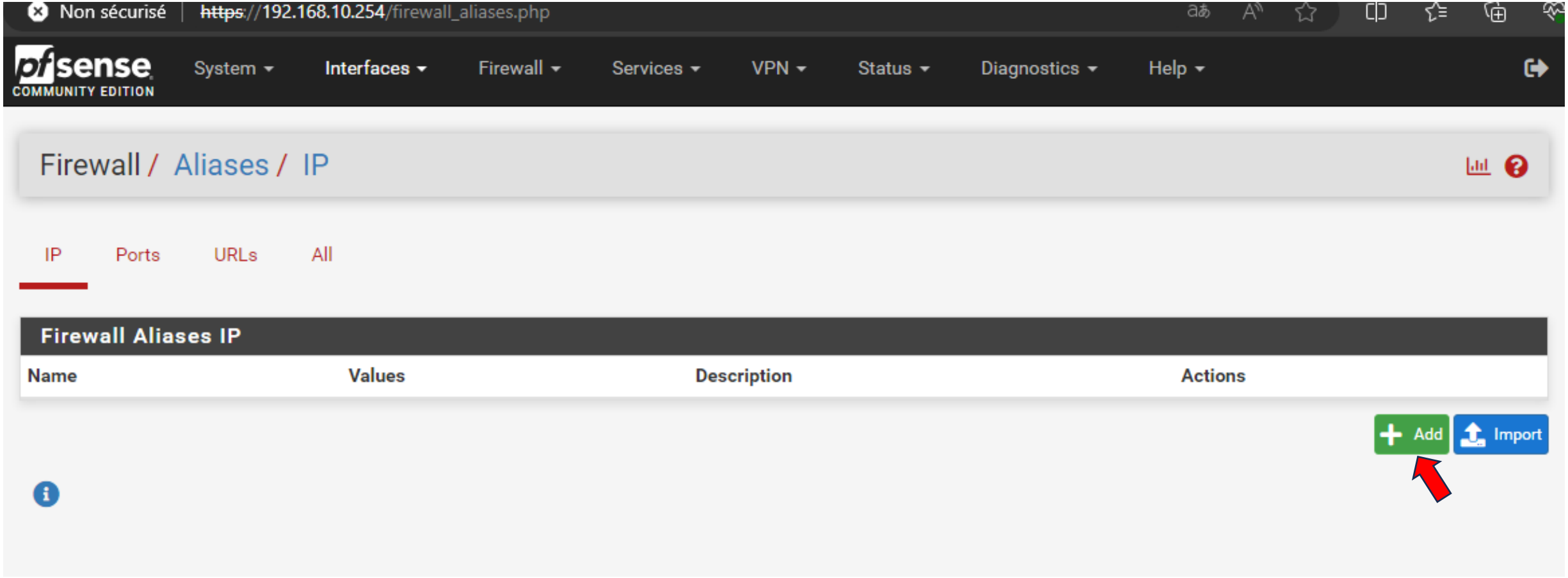
Dans l'onglet Firewall

Avant de créer la règle de navigation web, il est nécessaire de créer un alias pour accéder a des pages web http(80) /https(443).

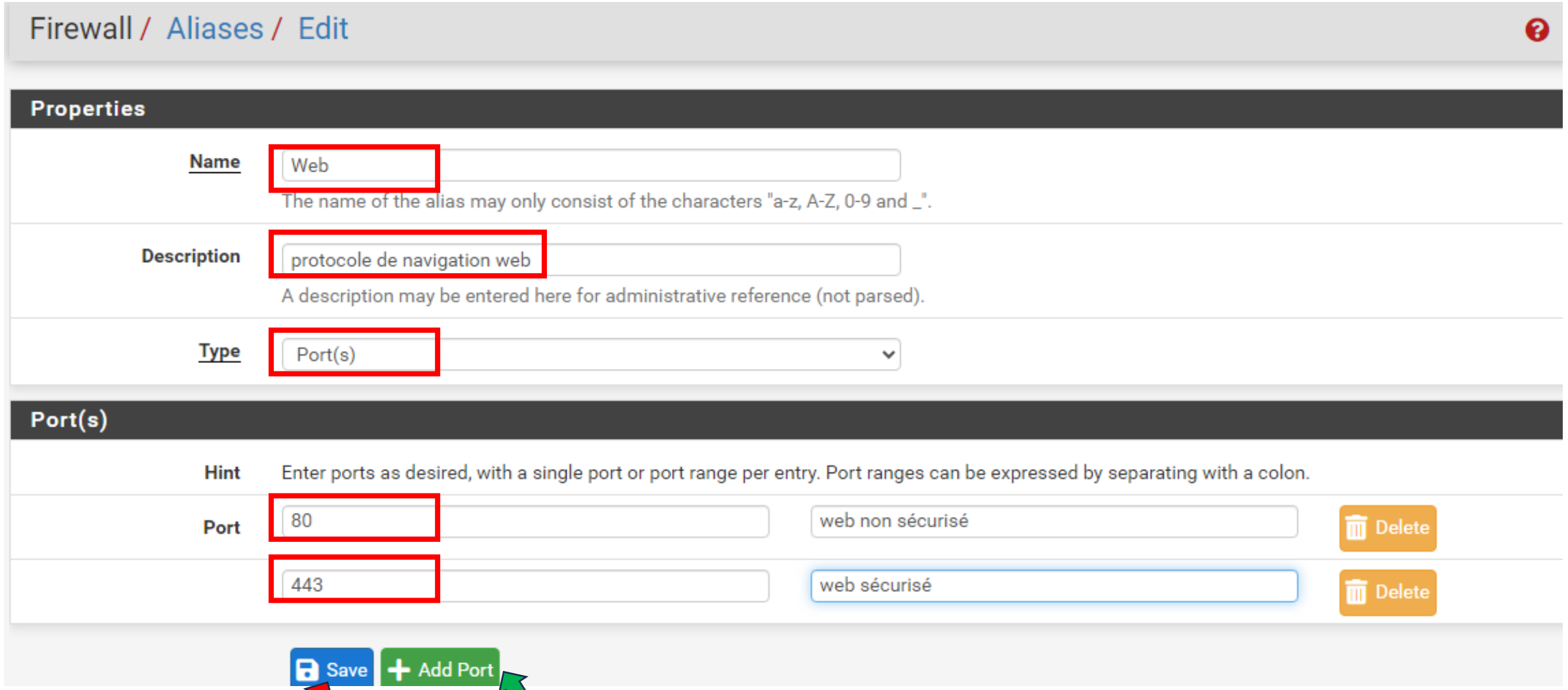
- ✓ **Clic sur Aliases**



✓ **Ensuite faire un clic sur le bouton Add**

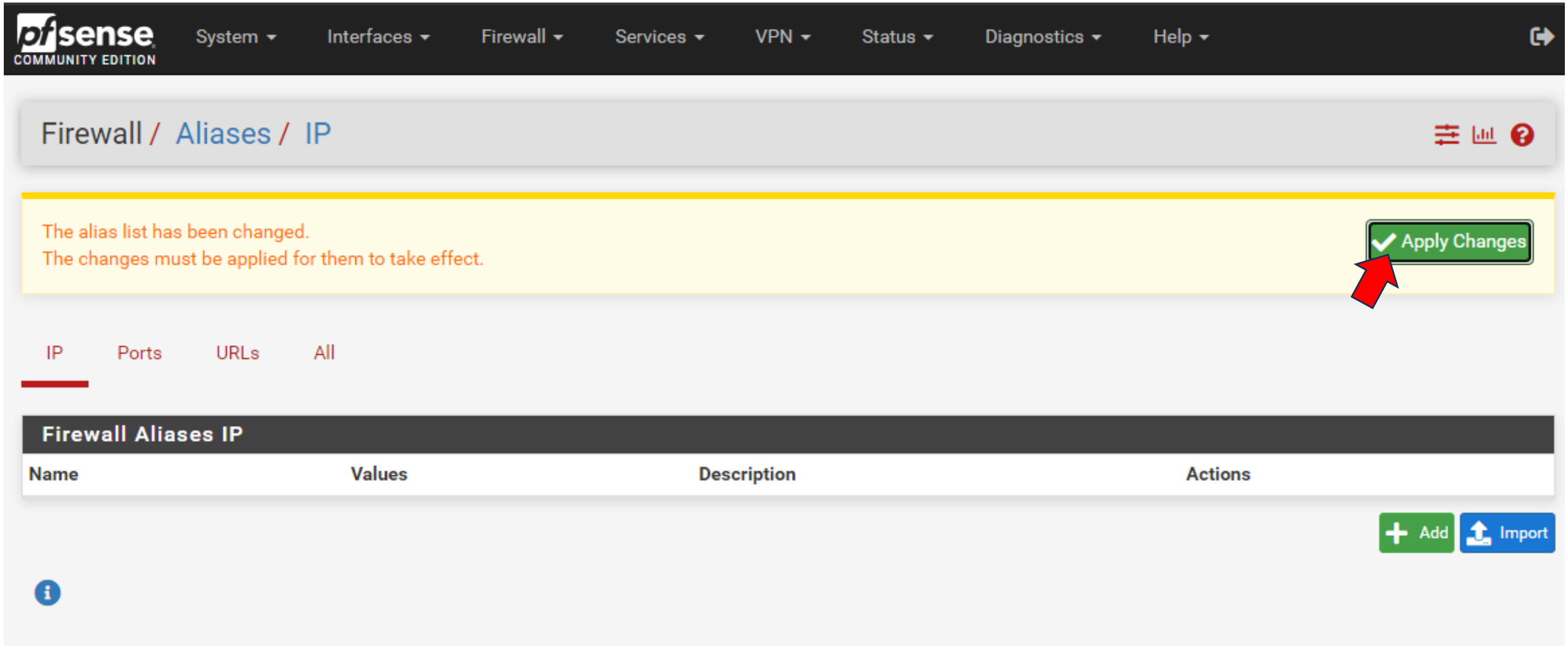


Cet alias aura pour nom web,
description protocole de navigation web,
Type port(s)

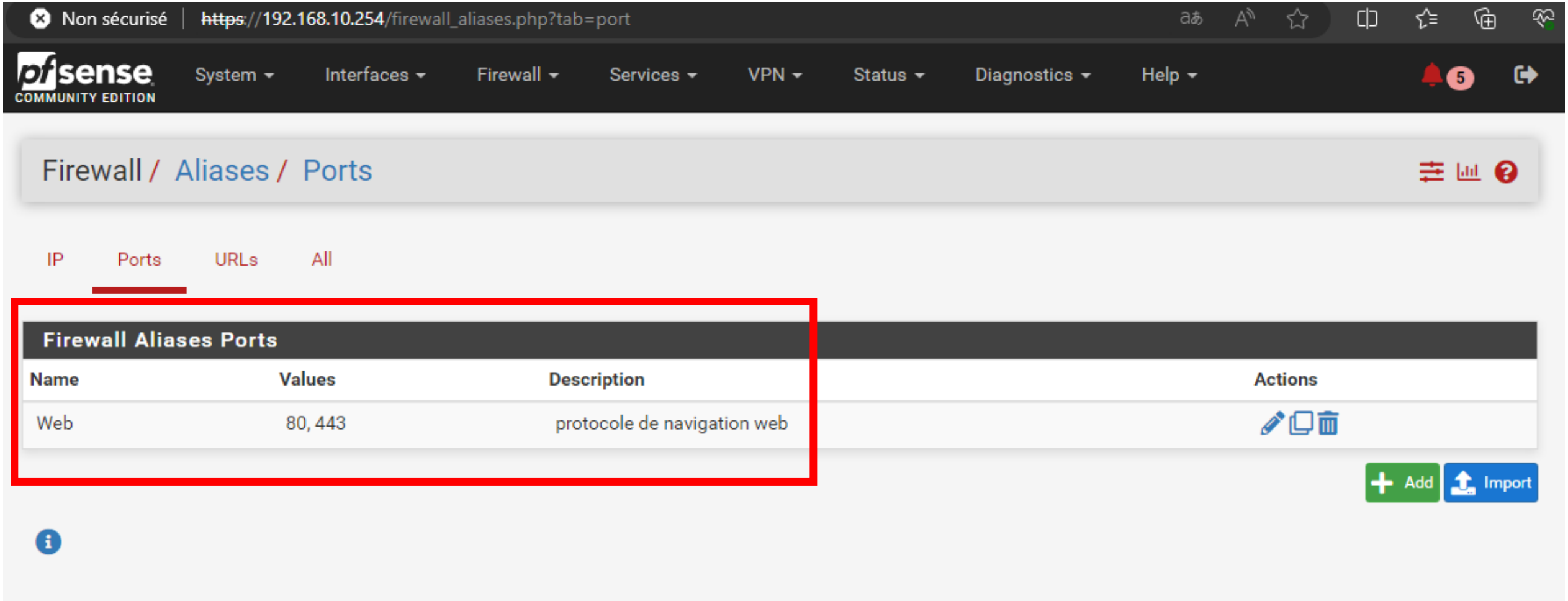


Toujours

- ✓ Cliquer sur Apply Changes apres une modification dans une règle



❑ Cliquer sur Ports pour voir l'alias qui à été parfaitement ajouter

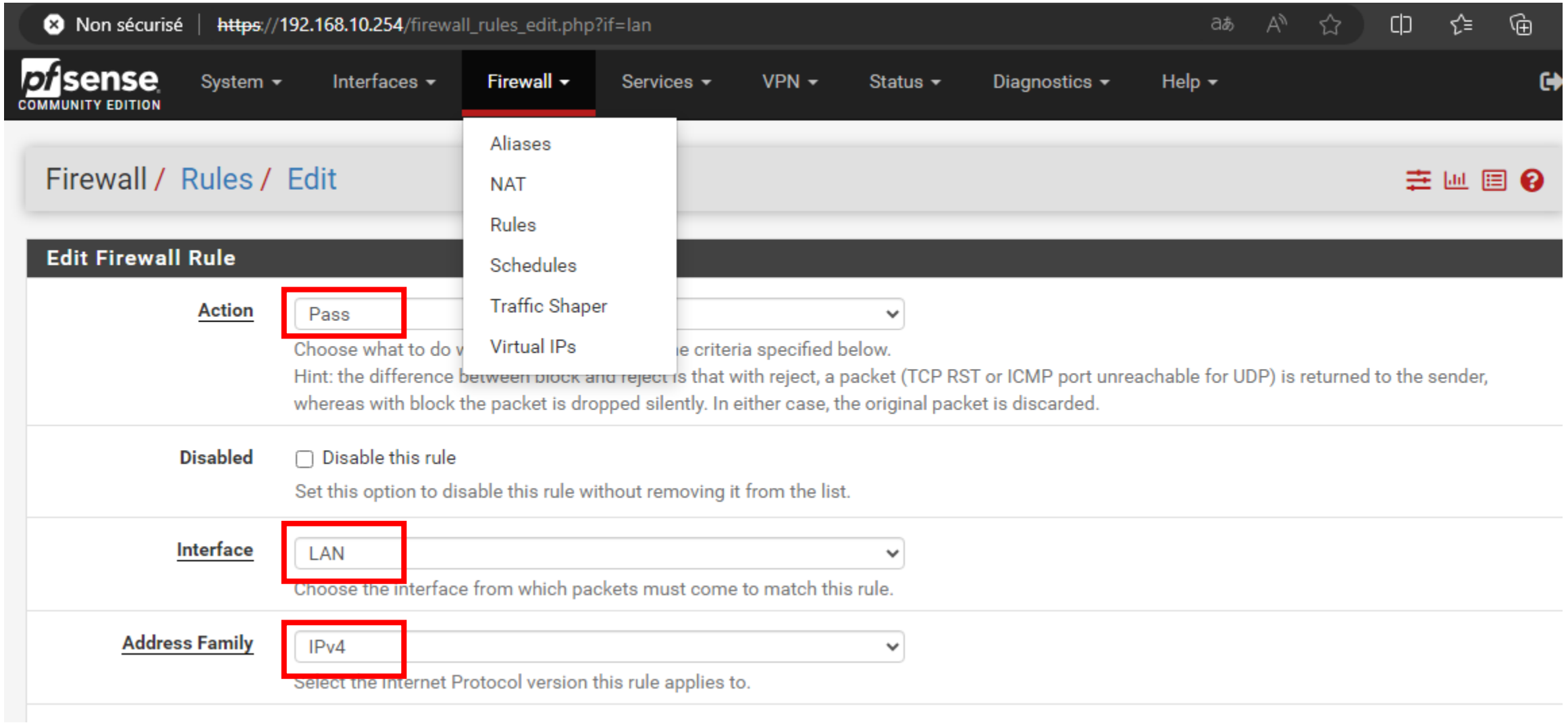


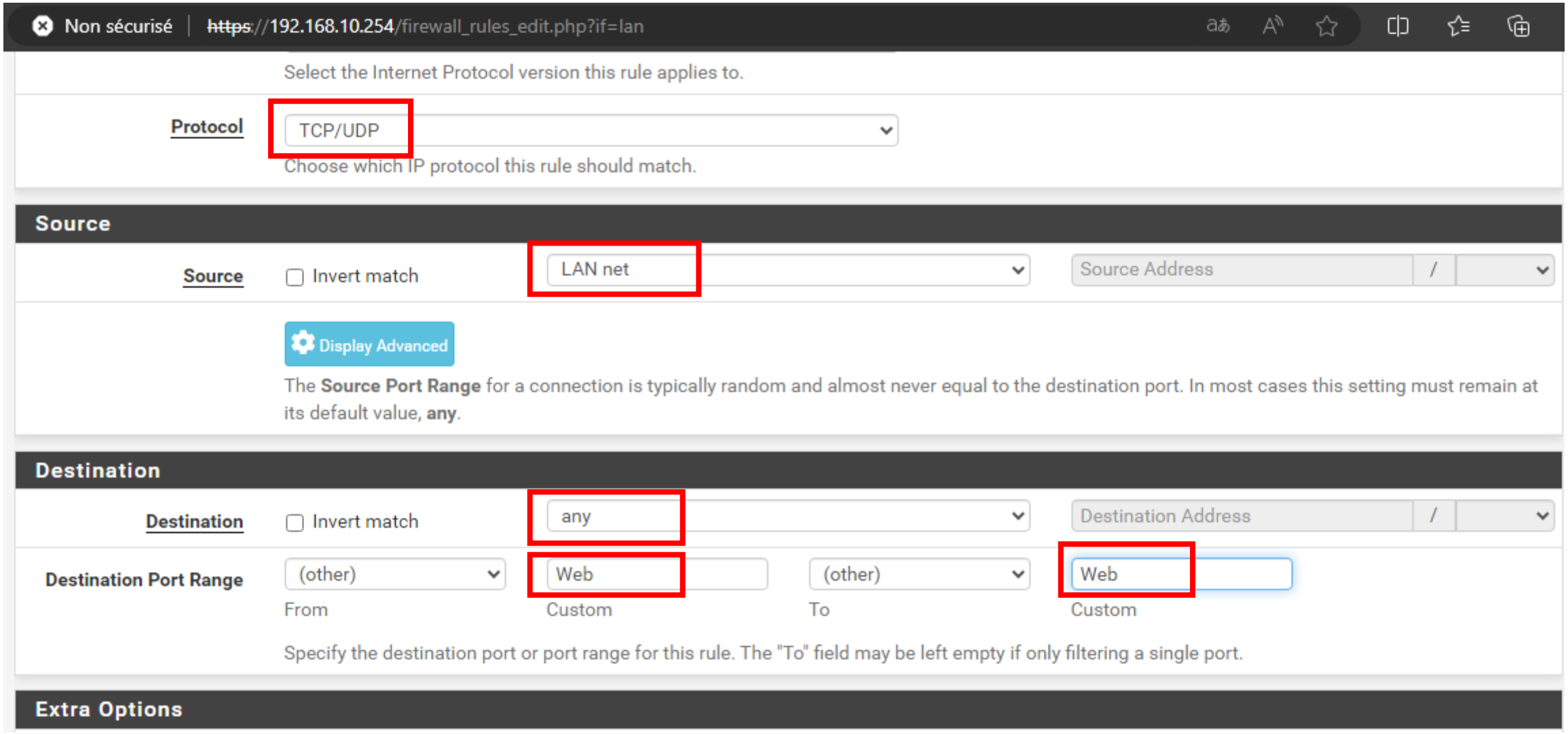
MACHINE CLIENTE WINDOWS 10

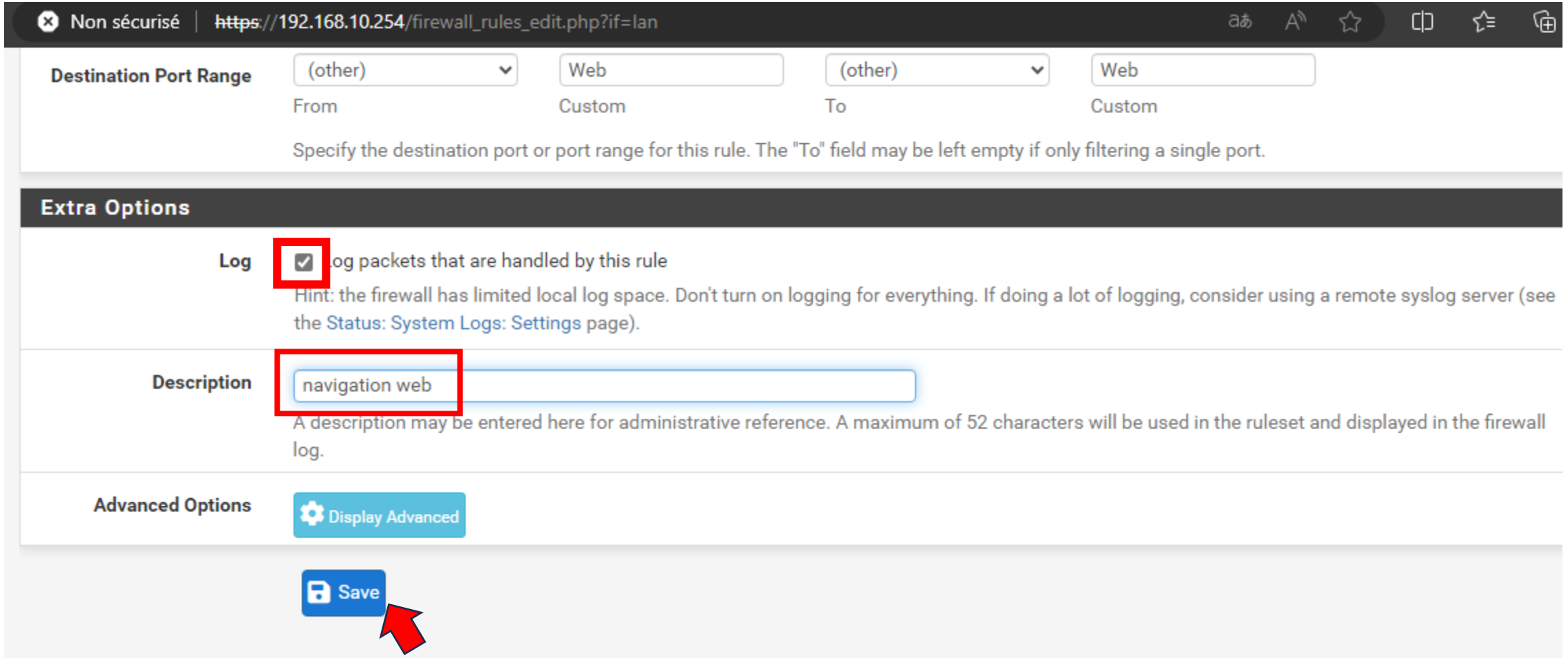
PFSENSE INTERFACE WEB

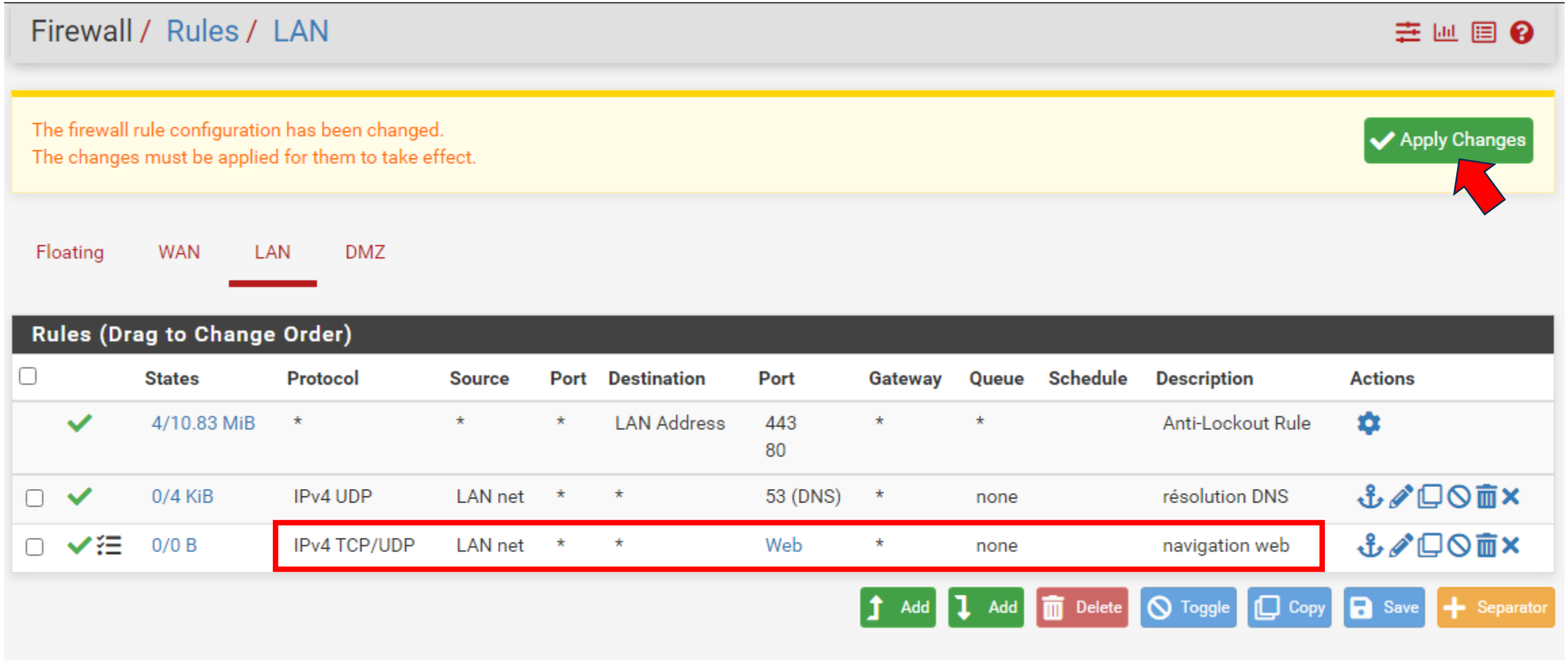
Créer une règle de navigation web

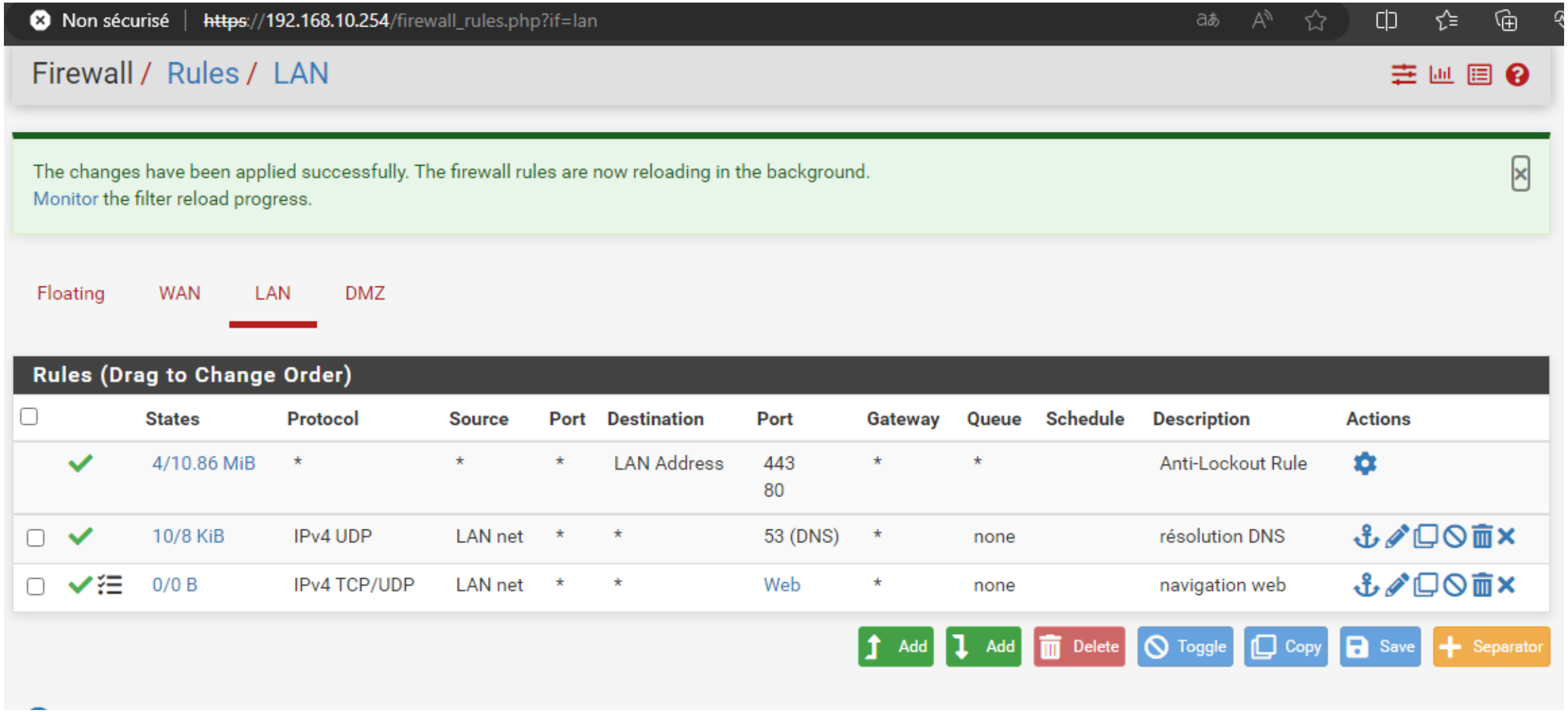
- ✓ **Clic sur Rules,**
- ✓ **Ensuite sur LAN pour créer la règle**




Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?if=lan
Select the Internet Protocol version this rule applies to.
Protocol
TCP/UDP
Choose which IP protocol this rule should match.
Source
Source
Invert match
LAN net
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
/
Destination Port Range
(other)
Web
(other)
Web
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.
Extra Options


Non sécurisé
https://192.168.10.254/firewall_rules_edit.php?if=lan
Destination Port Range
(other)
Web
(other)
Web
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.
Extra Options
Log
og 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
navigation web
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


Firewall / Rules / LAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4/10.83 MiB
*
*
*
LAN Address
443
80
*
*
Anti-Lockout Rule
0/4 KiB
IPv4 UDP
LAN net
*
*
53 (DNS)
*
none
résolution DNS
0/0 B
IPv4 TCP/UDP
LAN net
*
*
Web
*
none
navigation web
Add
Add
Delete
Toggle
Copy
Save
Separator


Non sécurisé | https://192.168.10.254/firewall_rules.php?if=lan
Firewall / Rules / LAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4/10.86 MiB
*
*
*
LAN Address
443
80
*
*
Anti-Lockout Rule
10/8 KiB
IPv4 UDP
LAN net
*
*
53 (DNS)
*
none
résolution DNS
0/0 B
IPv4 TCP/UDP
LAN net
*
*
Web
*
none
navigation web
Add
Add
Delete
Toggle
Copy
Save
Separator

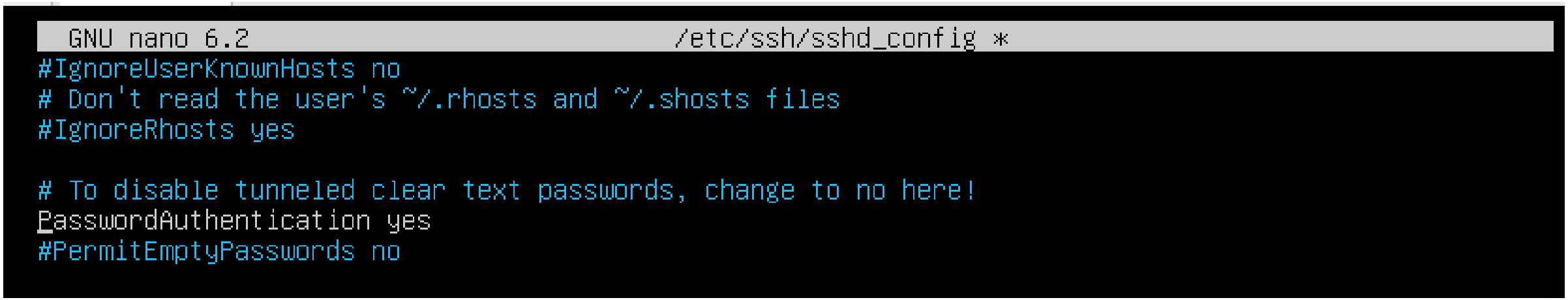
MACHINE UBUNTU-SERVER

WEB

Dans la machine ubuntu-servers qui joue le rôle de server web, afin de prendre de la main à distance en SSH de cette machine.
Il faut décommenter dans le fichier sshd_config PASSWORDAUTHENTIFICATION YES

nano /etc/ssh/sshd_config

```
jude@web01:~$ ping 192.168.10.254
PING 192.168.10.254 (192.168.10.254) 56(84) bytes of data.
^C
--- 192.168.10.254 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6151ms

jude@web01:~$ sudo su
[sudo] password for jude:
root@web01:/home/jude# tree
Command 'tree' not found, but can be installed with:
apt install tree
root@web01:/home/jude# nano /etc/ssh/sshd_config
```


GNU nano 6.2 /etc/ssh/sshd_config *
#IgnoreUserKnownHosts no
Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no

 # systemctl restart ssh
 # systemctl status ssh

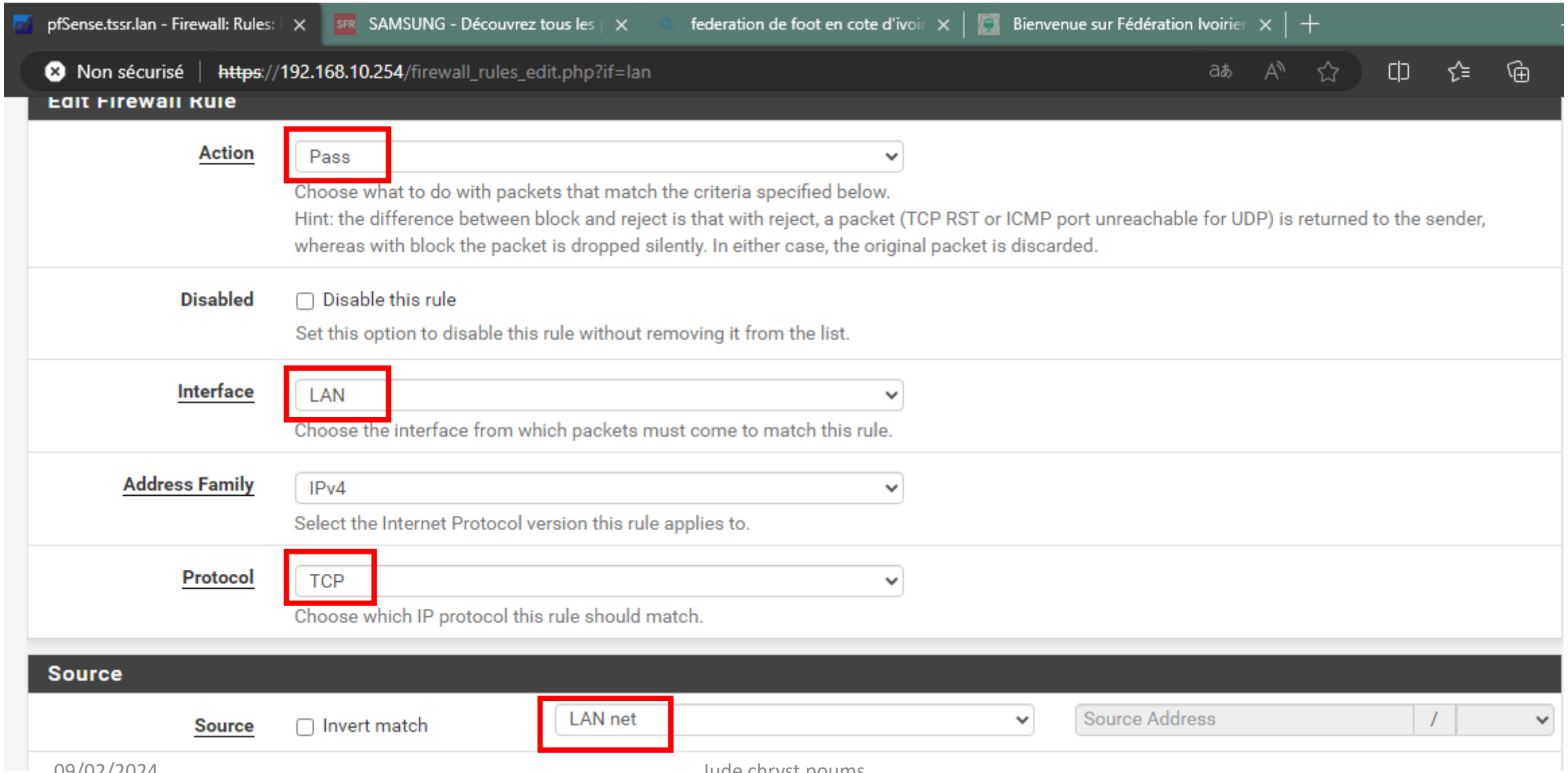
```
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.


root@web01:/home/jude# systemclt restart ssh
Command 'systemclt' not found, did you mean:
  command 'systemctl' from deb systemd (249.11-0ubuntu3.11)
  command 'systemctl' from deb systemctl (1.4.4181-1.1)
Try: apt install <deb name>
root@web01:/home/jude# systemctl restart ssh
root@web01:/home/jude# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-02-06 15:42:44 UTC; 18s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1376 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1377 (sshd)
      Tasks: 1 (limit: 4515)
     Memory: 1.7M
        CPU: 34ms
     CGroup: /system.slice/ssh.service
             └─1377 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

févr. 06 15:42:44 web01 systemd[1]: Starting OpenBSD Secure Shell server...
févr. 06 15:42:44 web01 sshd[1377]: Server listening on 0.0.0.0 port 22.
févr. 06 15:42:44 web01 sshd[1377]: Server listening on :: port 22.
févr. 06 15:42:44 web01 systemd[1]: Started OpenBSD Secure Shell server.
root@web01:/home/jude#
```

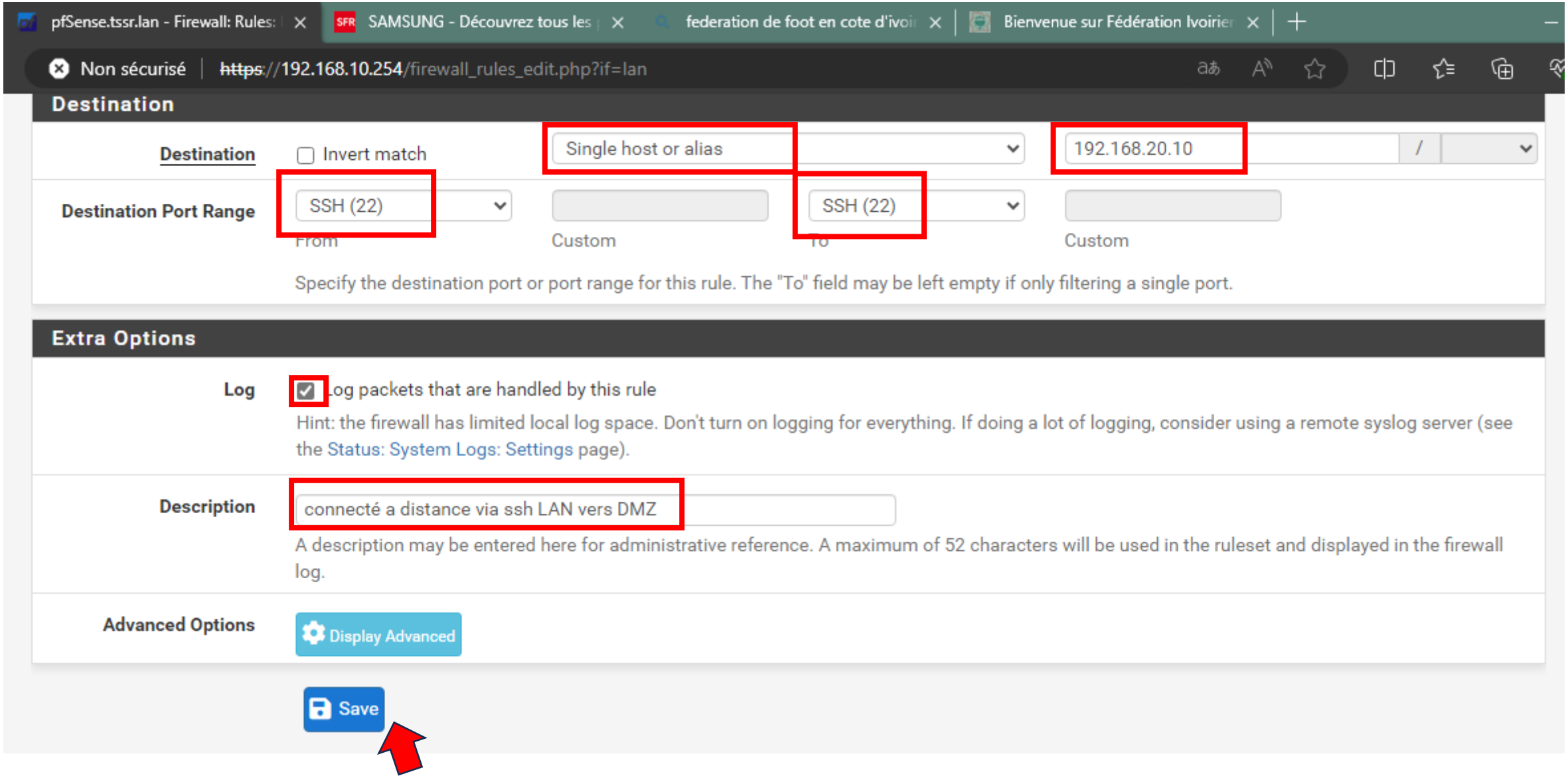
MACHINE CLIENTE WINDOWS 10

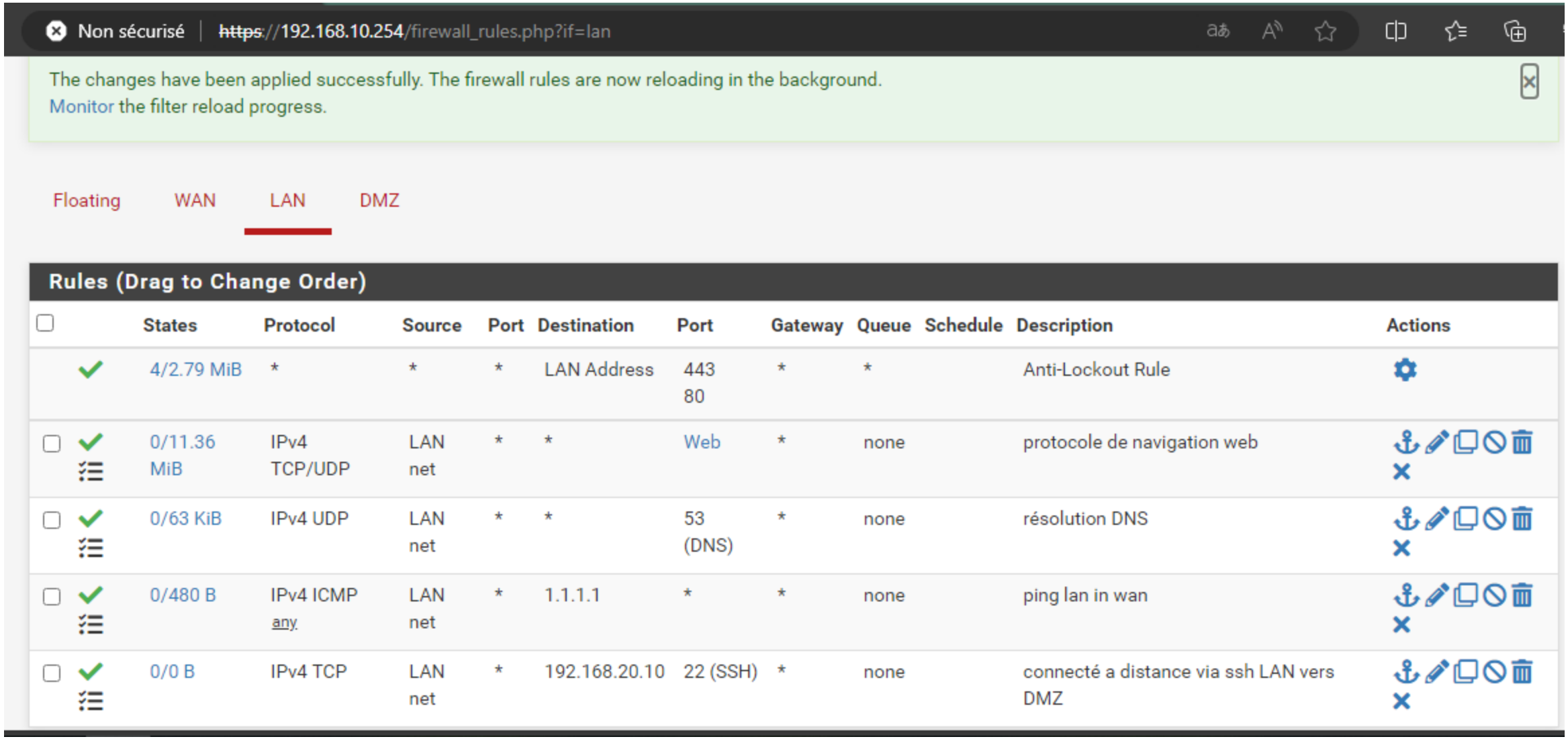
PFSENSE INTERFACE WEB

Créer une règle pour se connecté a distance via ssh LAN vers DMZ

- ✓ Clic sur Rules,
- ✓ Ensuite sur LAN pour créer la règle



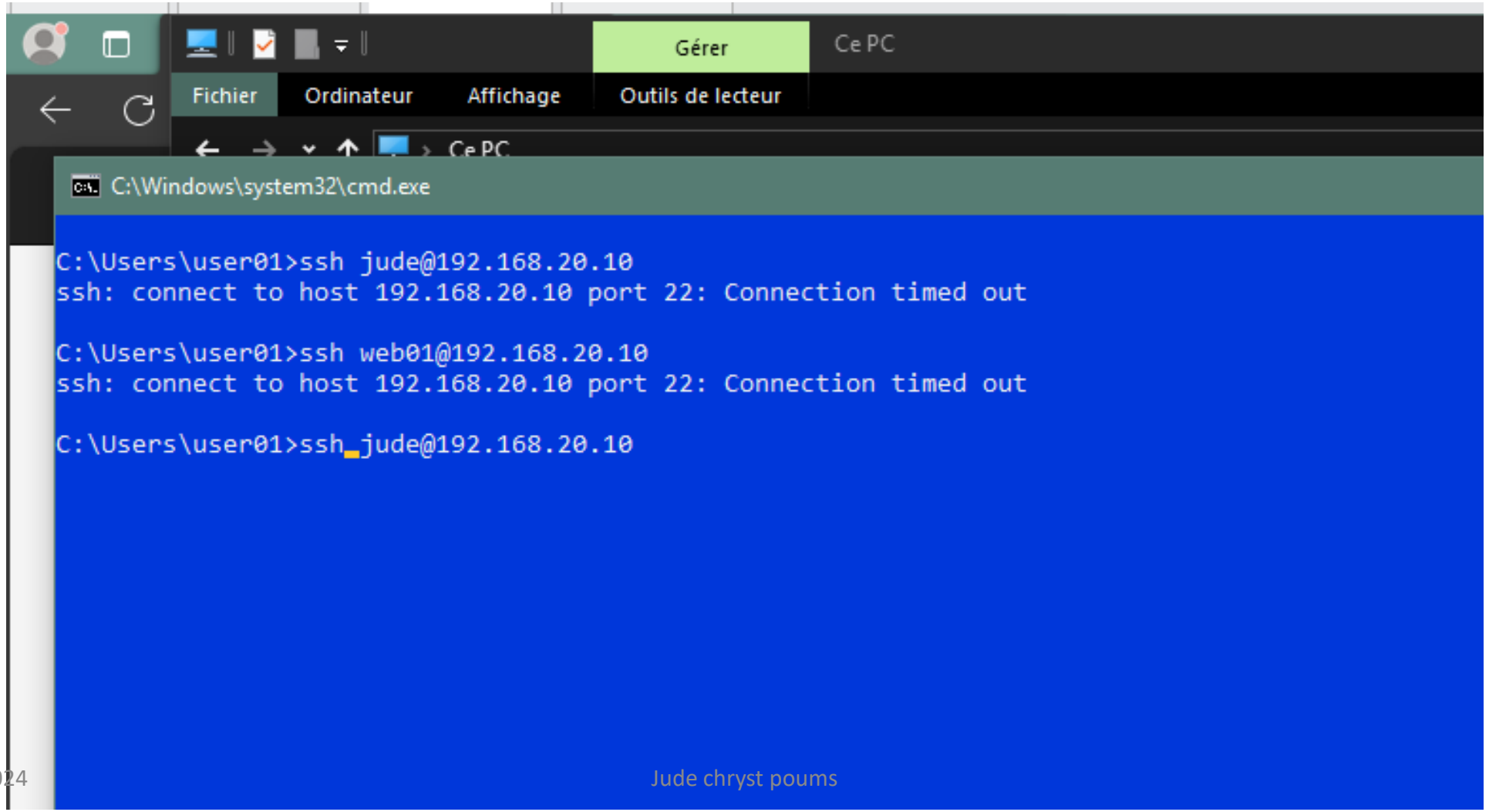

pfSense.tssr.lan - Firewall: Rules:
SAMSUNG - Découvrez tous les
federation de foot en cote d'ivoi
Bienvenue sur Fédération Ivoirie
Non sécurisé
https://192.168.10.254/firewall_rules_edit.php?if=lan
Destination
Destination
Invert match
Single host or alias
192.168.20.10
/
Destination Port Range
SSH (22)
From
Custom
SSH (22)
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.
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
connecté a distance via ssh LAN vers DMZ
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


Non sécurisé | https://192.168.10.254/firewall_rules.php?if=lan
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
4/2.79 MiB * * * LAN Address 443 80 * * Anti-Lockout Rule
0/11.36 MiB IPv4 TCP/UDP LAN net * * Web * none protocole de navigation web
0/63 KiB IPv4 UDP LAN net * * 53 (DNS) * none résolution DNS
0/480 B IPv4 ICMP any LAN net * 1.1.1.1 * * none ping lan in wan
0/0 B IPv4 TCP LAN net * 192.168.20.10 22 (SSH) * none connecté a distance via ssh LAN vers DMZ

Vous pouvez maintenant accéder à distance via ssh

Depuis le CMD c'est-à-dire la touche Windows + R

Voici la commande pour prendre la main avec le ssh **> ssh jude@192.168.20.10**

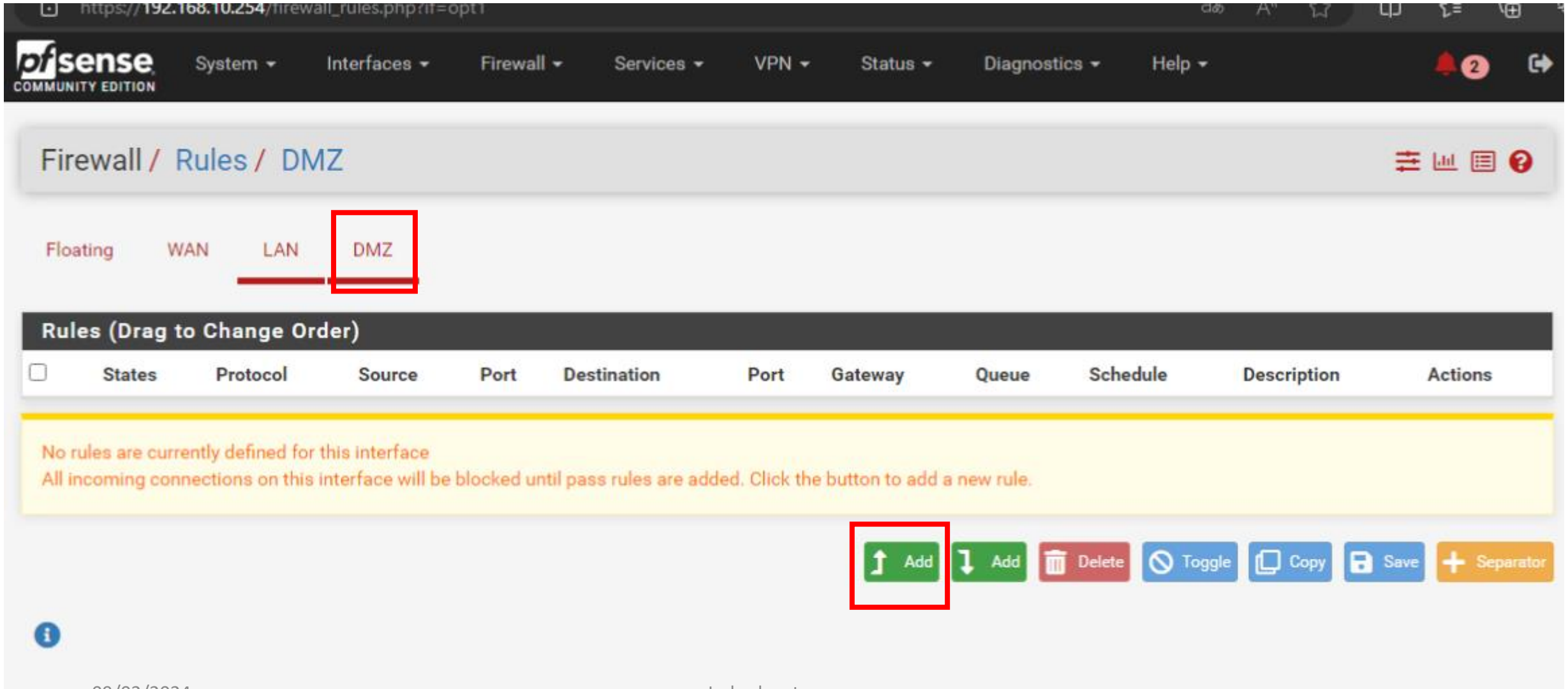


MACHINE CLIENTE WINDOWS 10

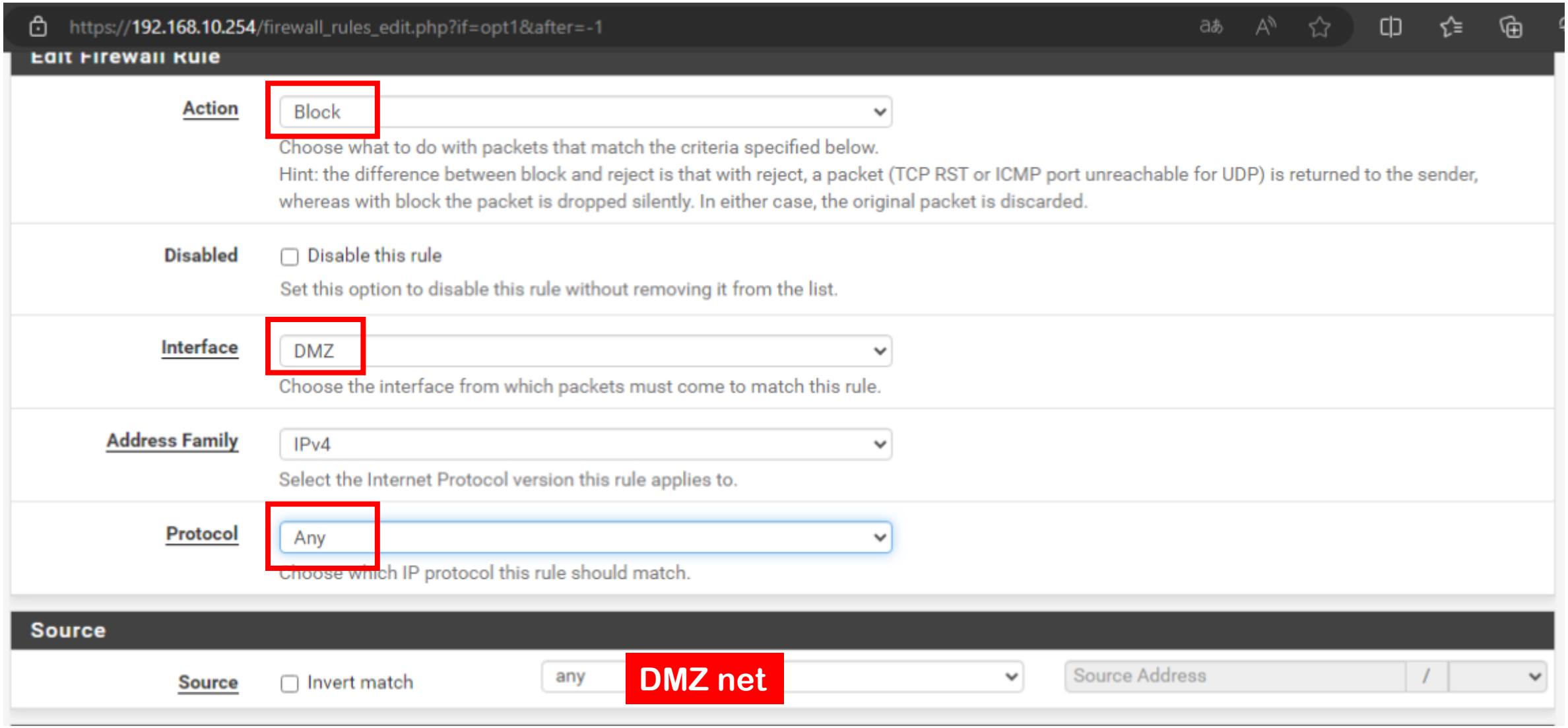
PFSENSE INTERFACE WEB

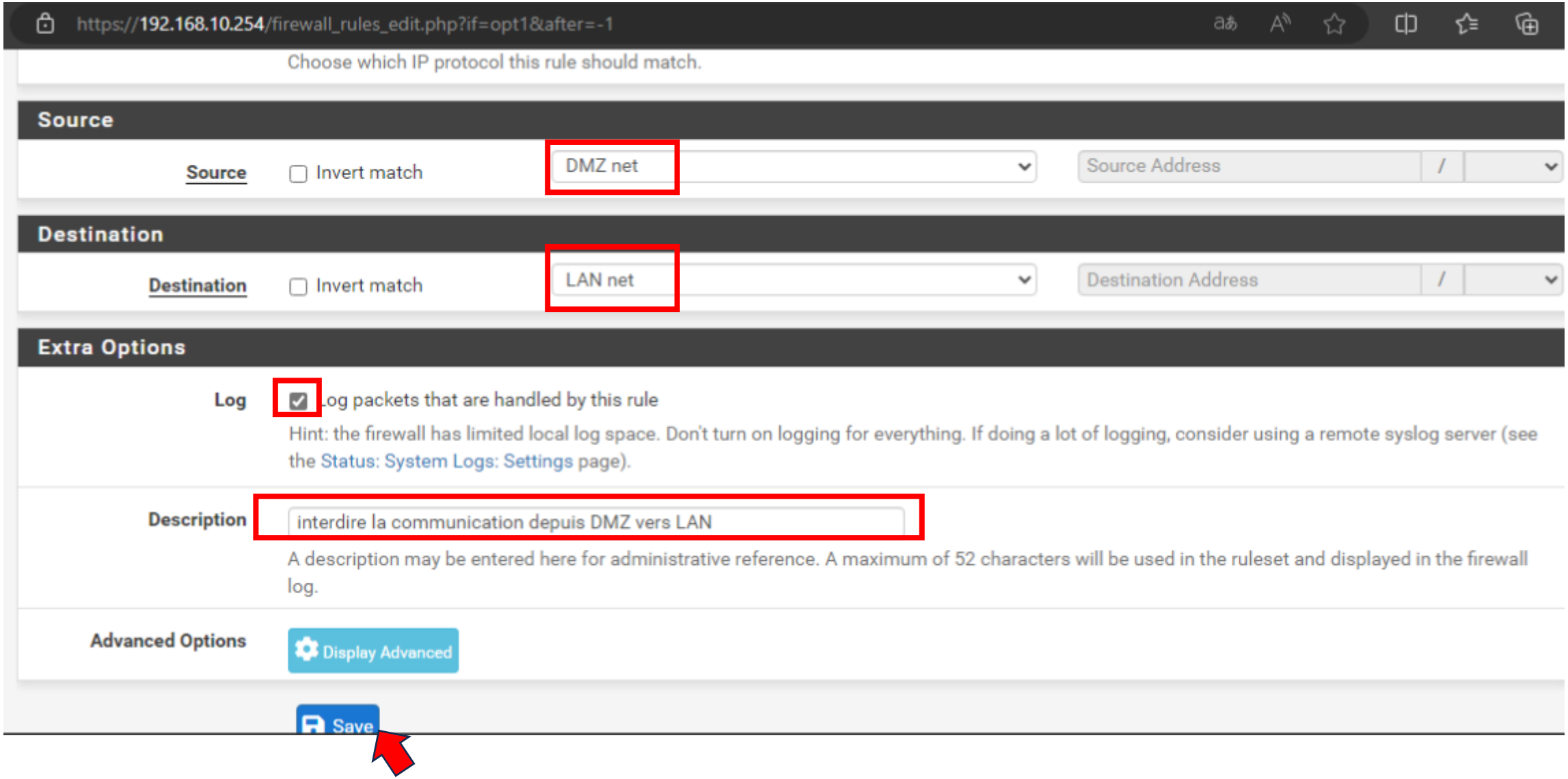
Créer une règle pour interdire la communication depuis DMZ vers LAN

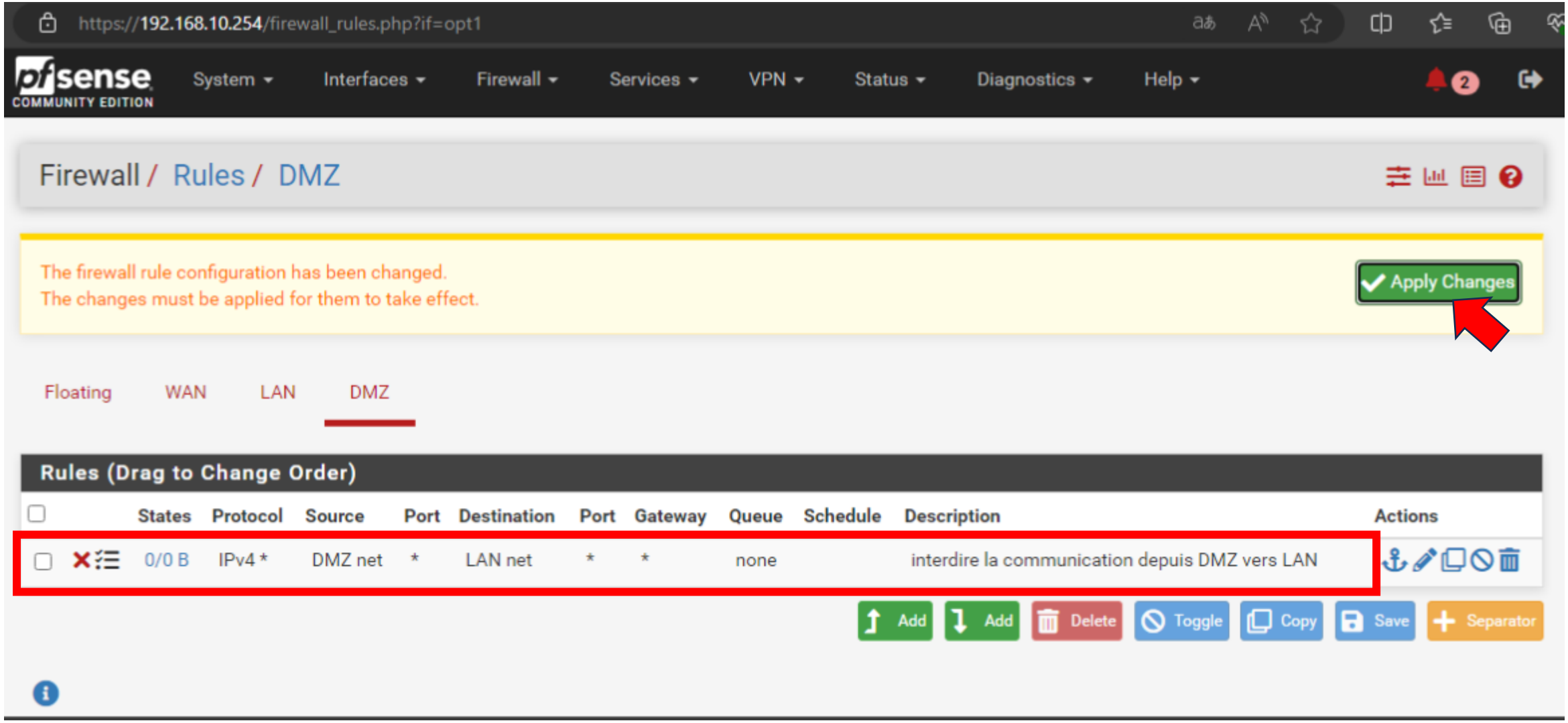
- ✓ Clic sur Rules,
- ✓ Ensuite sur DMZ pour créer la règle
- ✓ Cliquer sur le bouton vert add pour ajouter une nouvelle règle



✓ Interdiction absolue d'accéder au LAN




https://192.168.10.254/firewall_rules_edit.php?if=opt1&after=-1
Choose which IP protocol this rule should match.
Source
Source
Invert match
DMZ net
Source Address
/
Destination
Destination
Invert match
LAN net
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
interdire la communication depuis DMZ vers LAN
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

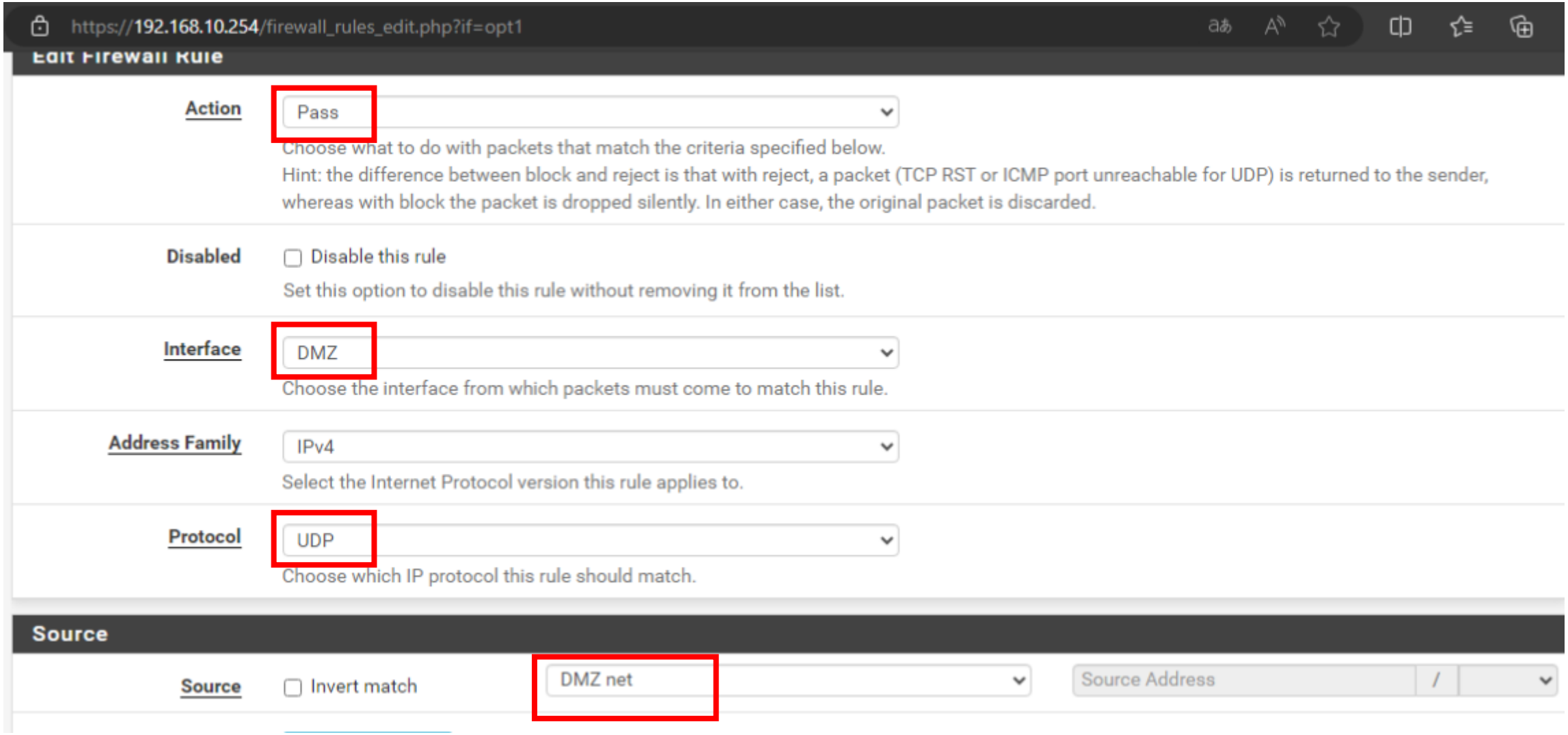

https://192.168.10.254/firewall_rules.php?if=opt1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / DMZ
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
IPv4 *
DMZ net
*
LAN net
*
*
none
interdire la communication depuis DMZ vers LAN
Add
Add
Delete
Toggle
Copy
Save
Separator

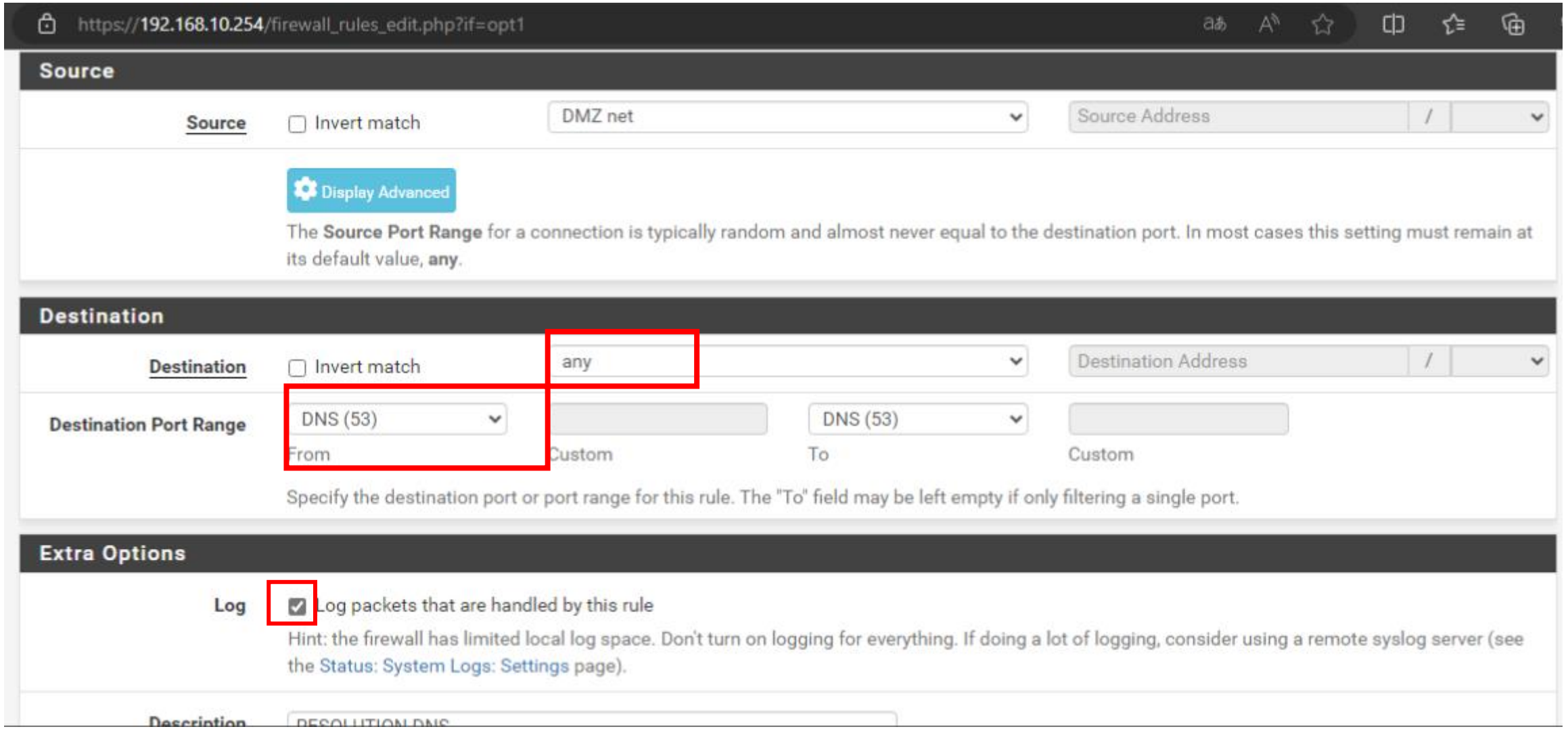
MACHINE CLIENTE WINDOWS 10

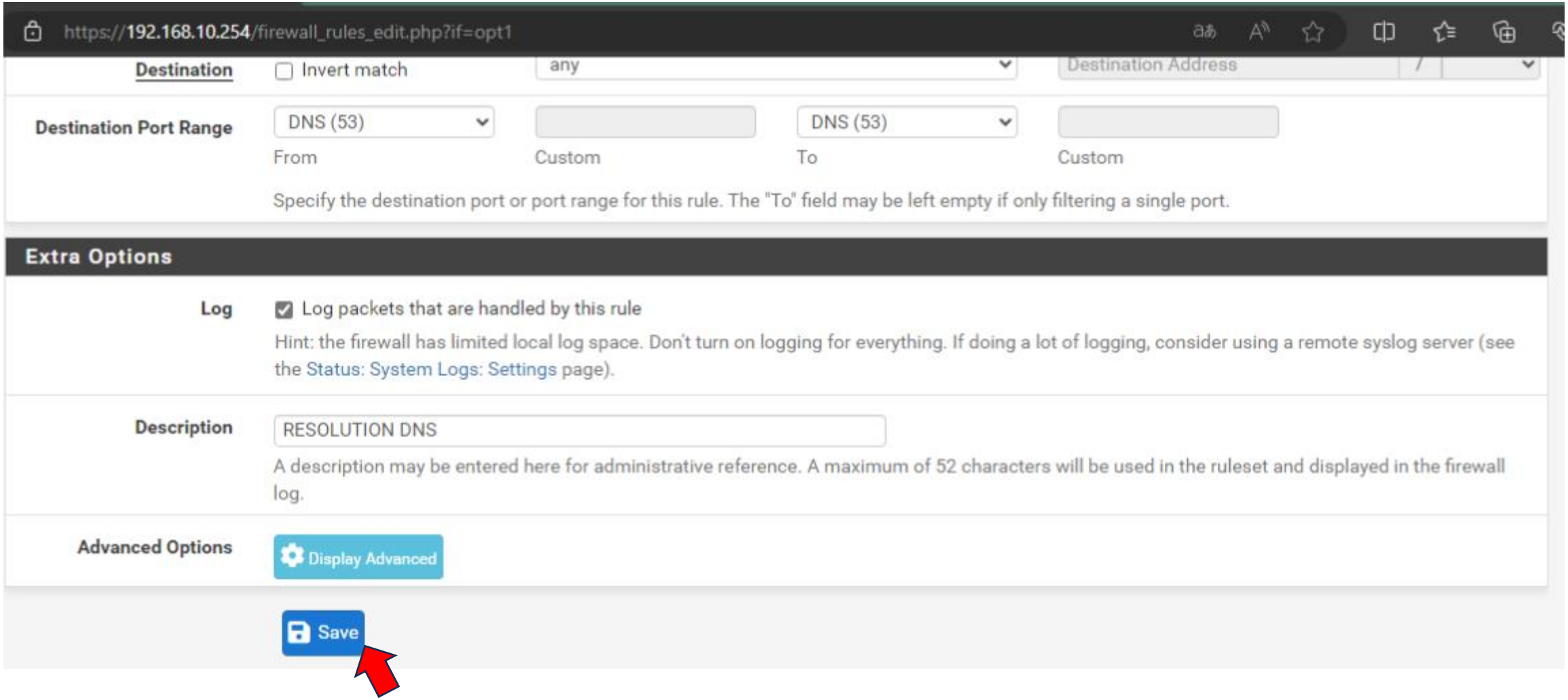
PFSENSE INTERFACE WEB

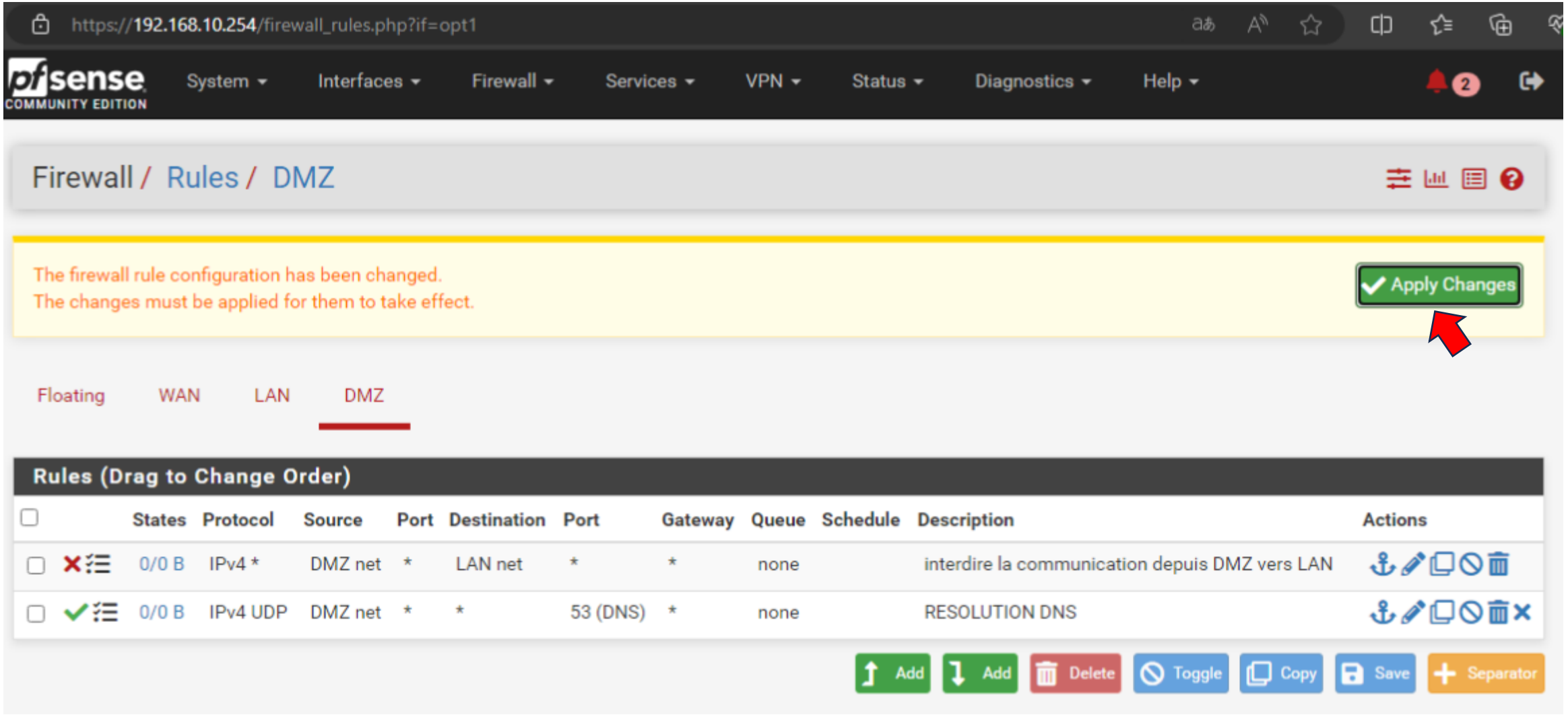
Créer une règle de résolution DNS depuis DMZ vers LAN

- ✓ Clic sur Rules,
- ✓ Ensuite sur DMZ pour créer la règle
- ✓ Cliquer sur le bouton vert add pour ajouter une nouvelle règle




https://192.168.10.254/firewall_rules_edit.php?if=opt1
Source
Source
Invert match
DMZ net
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
/
Destination Port Range
DNS (53)
From
Custom
DNS (53)
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.
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


https://192.168.10.254/firewall_rules_edit.php?if=opt1
Destination
Invert match
any
Destination Address
Destination Port Range
DNS (53)
From
Custom
DNS (53)
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.
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
RESOLUTION DNS
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

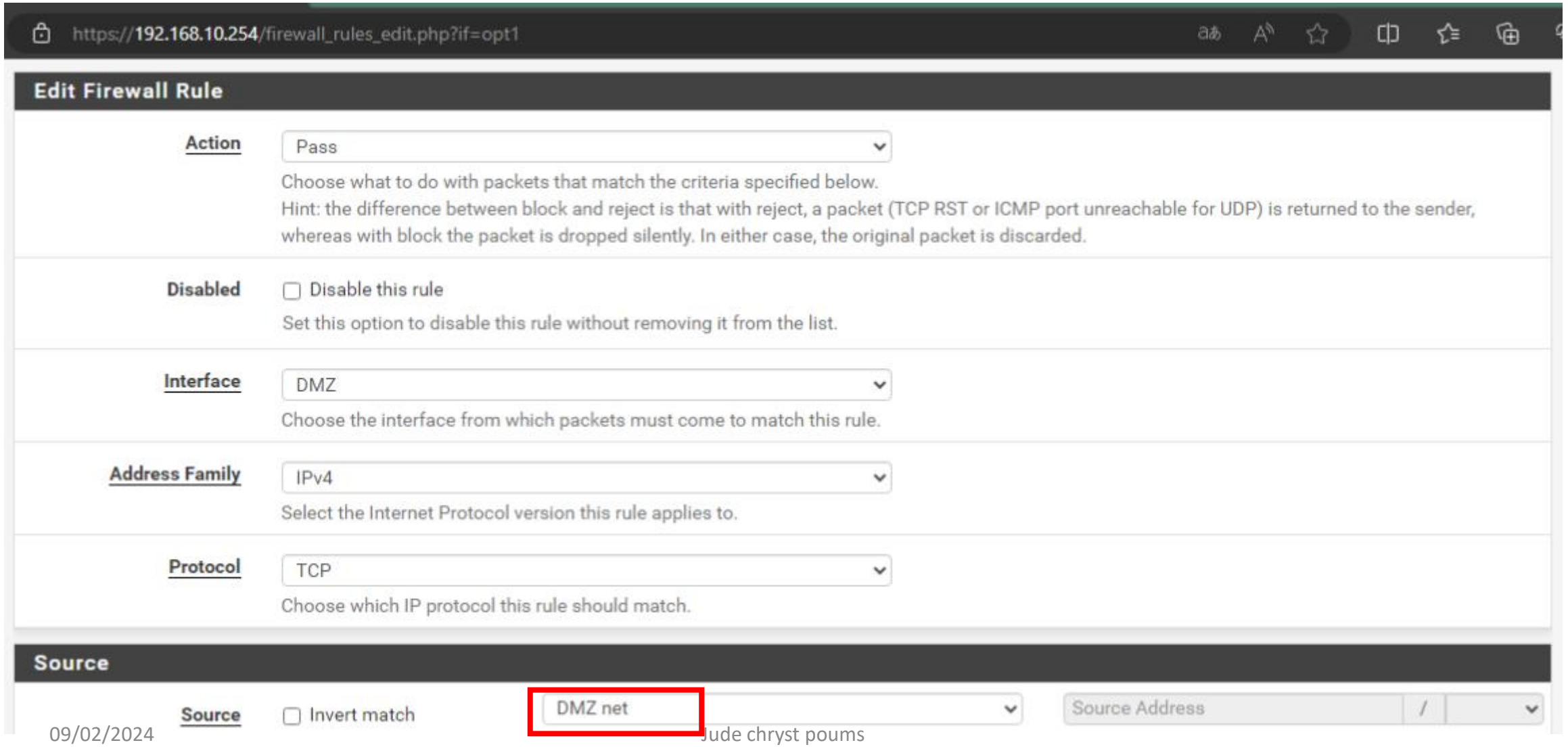

https://192.168.10.254/firewall_rules.php?if=opt1
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
2
Firewall / Rules / DMZ
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
IPv4 *
DMZ net
*
LAN net
*
*
none
interdire la communication depuis DMZ vers LAN
0/0 B
IPv4 UDP
DMZ net
*
*
53 (DNS)
*
none
RESOLUTION DNS
Add
Add
Delete
Toggle
Copy
Save
Separator

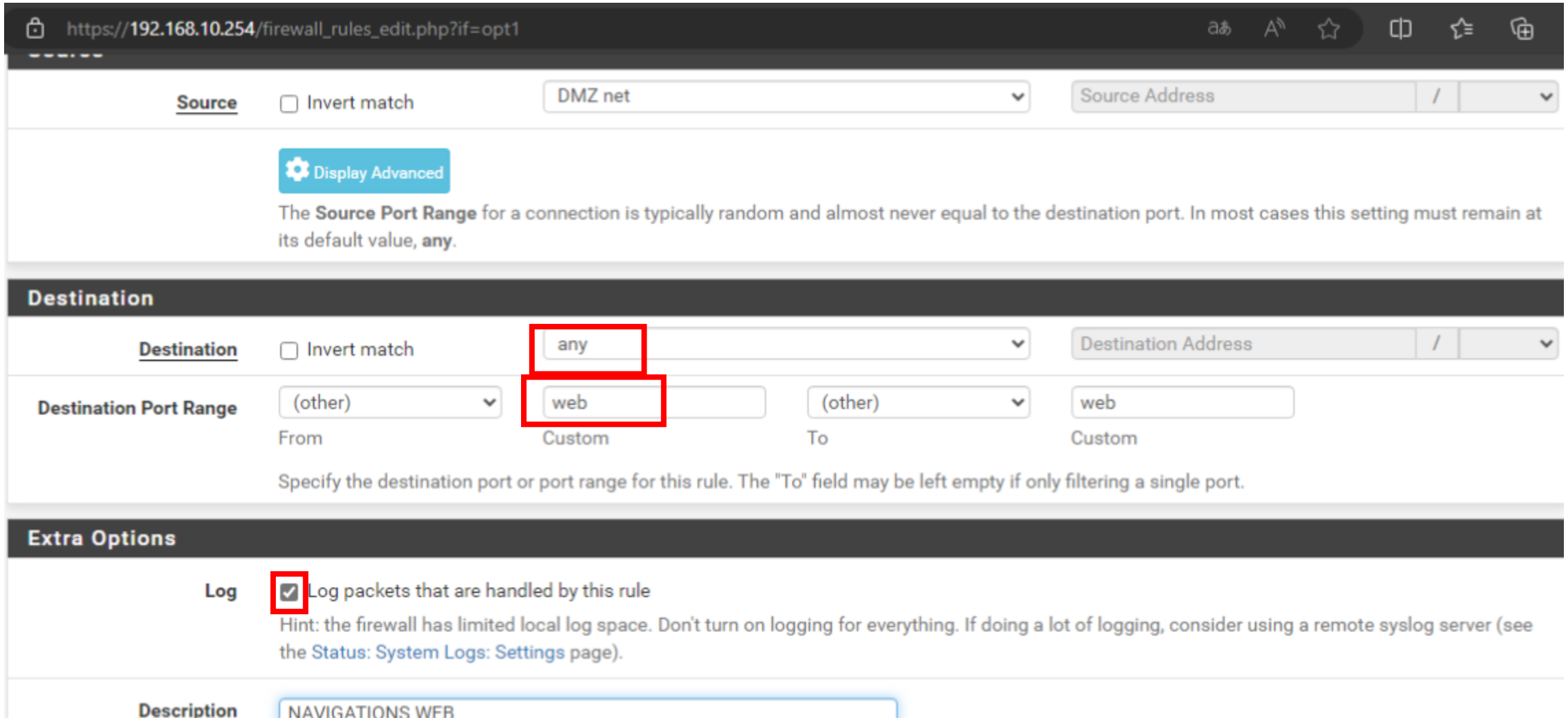
MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

Créer une règle de navigation web depuis DMZ vers LAN

- ✓ Clic sur Rules,
- ✓ Ensuite sur DMZ pour créer la règle
- ✓ Cliquer sur le bouton vert add pour ajouter une nouvelle règle



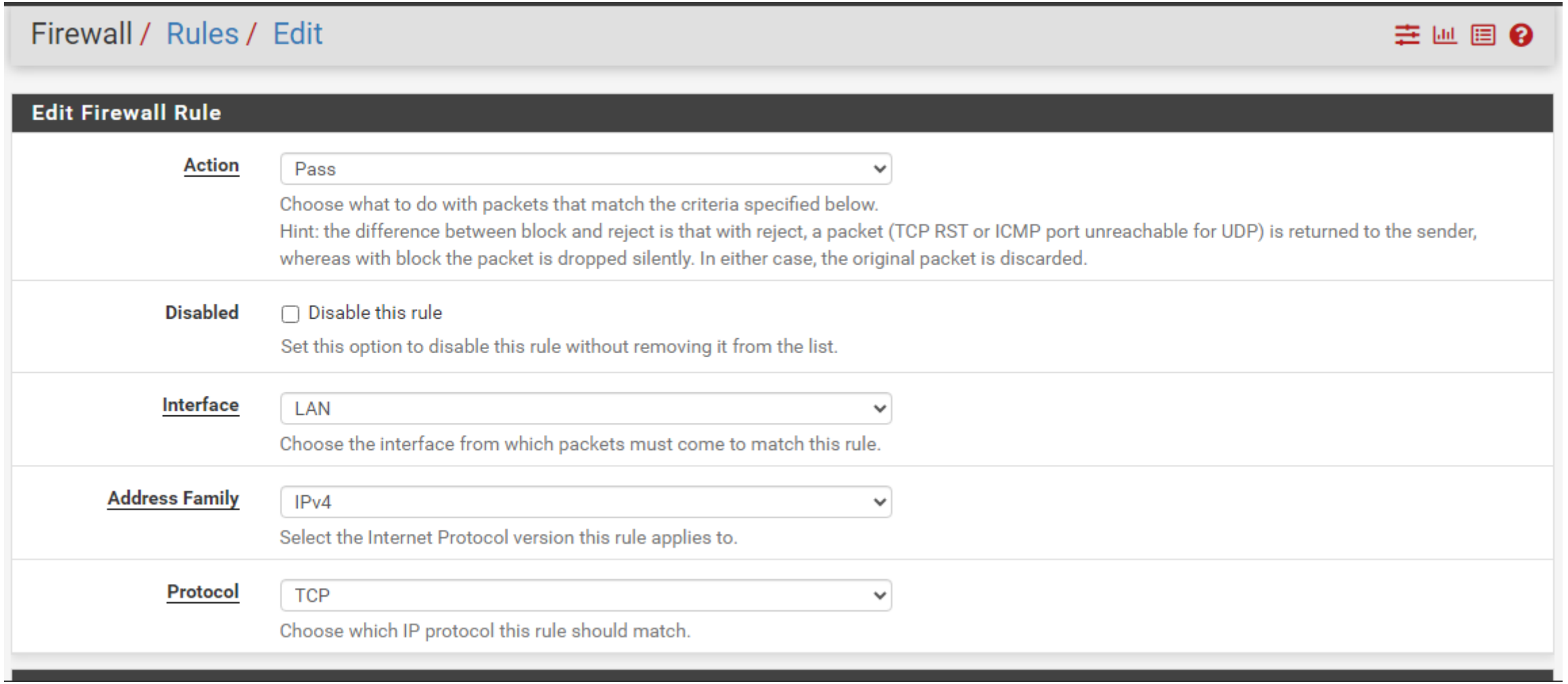

https://192.168.10.254/firewall_rules_edit.php?if=opt1
Source
Invert match
DMZ net
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
/
Destination Port Range
(other)
web
(other)
web
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.
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
NAVIGATIONS WEB

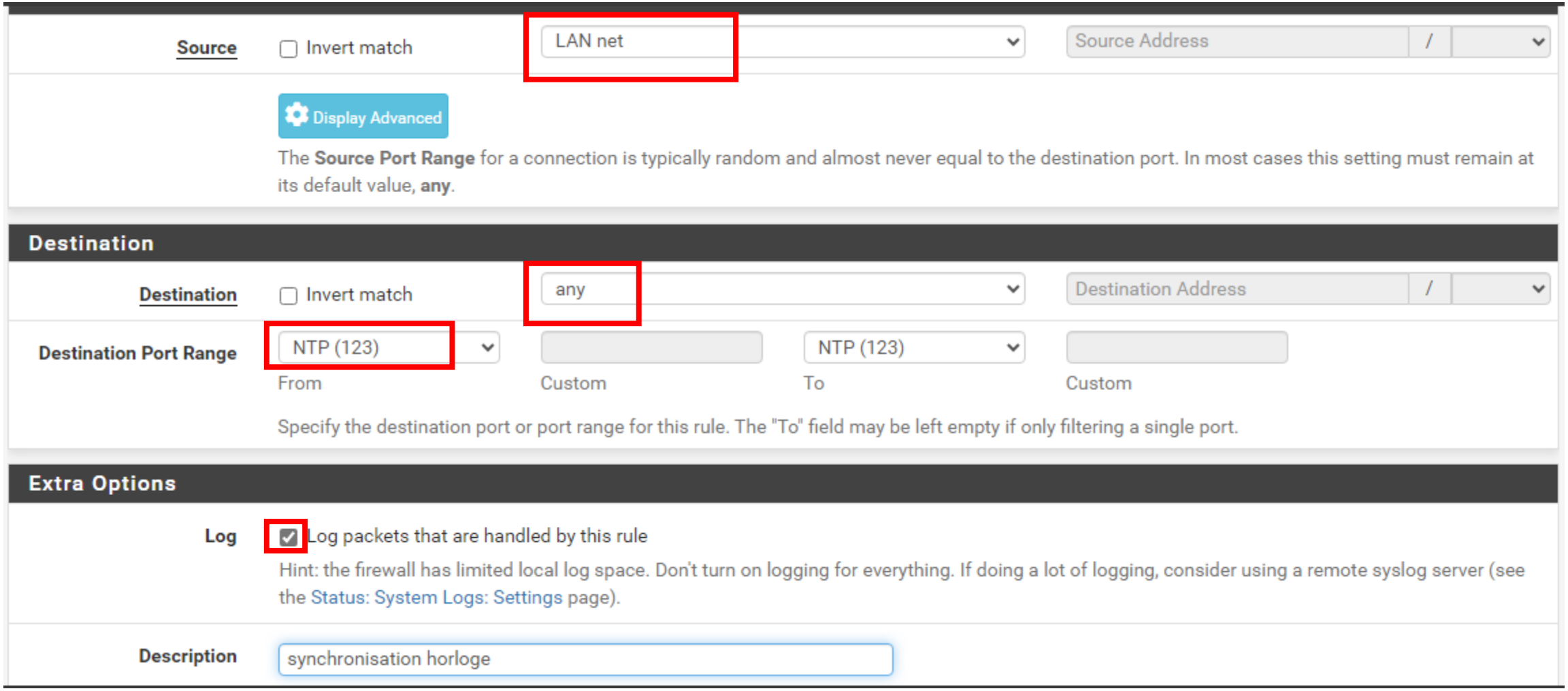
MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

Créer une règle de synchronisation (NTP) horloge depuis LAN vers DMZ

- ✓ Clic sur Rules,
- ✓ Ensuite sur LAN pour créer la règle
- ✓ Cliquer sur le bouton vert add pour ajouter une nouvelle règle




Source
Invert match
LAN net
Source Address
/
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
/
Destination Port Range
NTP (123)
From
Custom
NTP (123)
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.
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
synchronisation horloge

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating | WAN | LAN | DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	4/5.79 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
	0/0 B	IPv4 TCP	LAN net	*	*	123 (NTP)	*	none		synchronisation horloge	
	0/3 KiB	IPv4 ICMP any	LAN net	*	*	*	*	none		ping vers tous les reseaux	
	0/28 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		DNS vers tous	
	2/3.93 MiB	IPv4 TCP	LAN net	*	*	web	*	none		web vers tous	
	0/73 KiB	IPv4 TCP	LAN net	*	172.16.20.100	22 (SSH)	*	none		connecte via ssh a la DMZ	

Add | Add | Delete | Toggle | Copy | Save | Separator

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	4/5.81 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
☐ ✓	0/0 B	IPv4 TCP	LAN net	*	*	123 (NTP)	*	none		synchronisation horloge	⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	0/3 KiB	IPv4 ICMP any	LAN net	*	*	*	*	none		ping vers tous les reseaux	⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	0/28 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		DNS vers tous	⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	1/3.93 MiB	IPv4 TCP	LAN net	*	*	web	*	none		web vers tous	⚓ ✎ ⧉ ⊘ 🗑 ✕
☐ ✓	0/73 KiB	IPv4 TCP	LAN net	*	172.16.20.100	22 (SSH)	*	none		connecte via ssh a la DMZ	⚓ ✎ ⧉ ⊘ 🗑 ✕

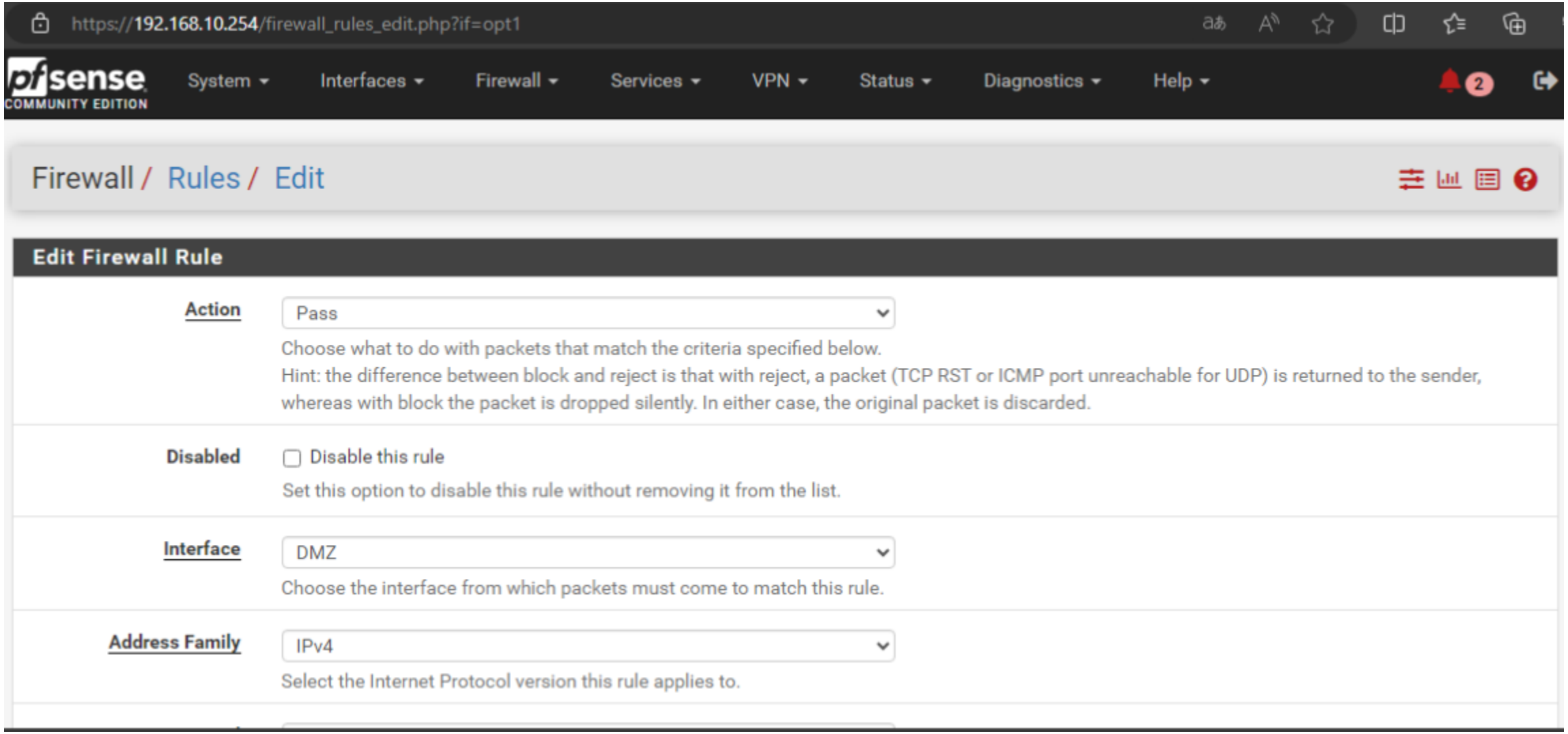
Add Add Delete Toggle Copy Save Separator

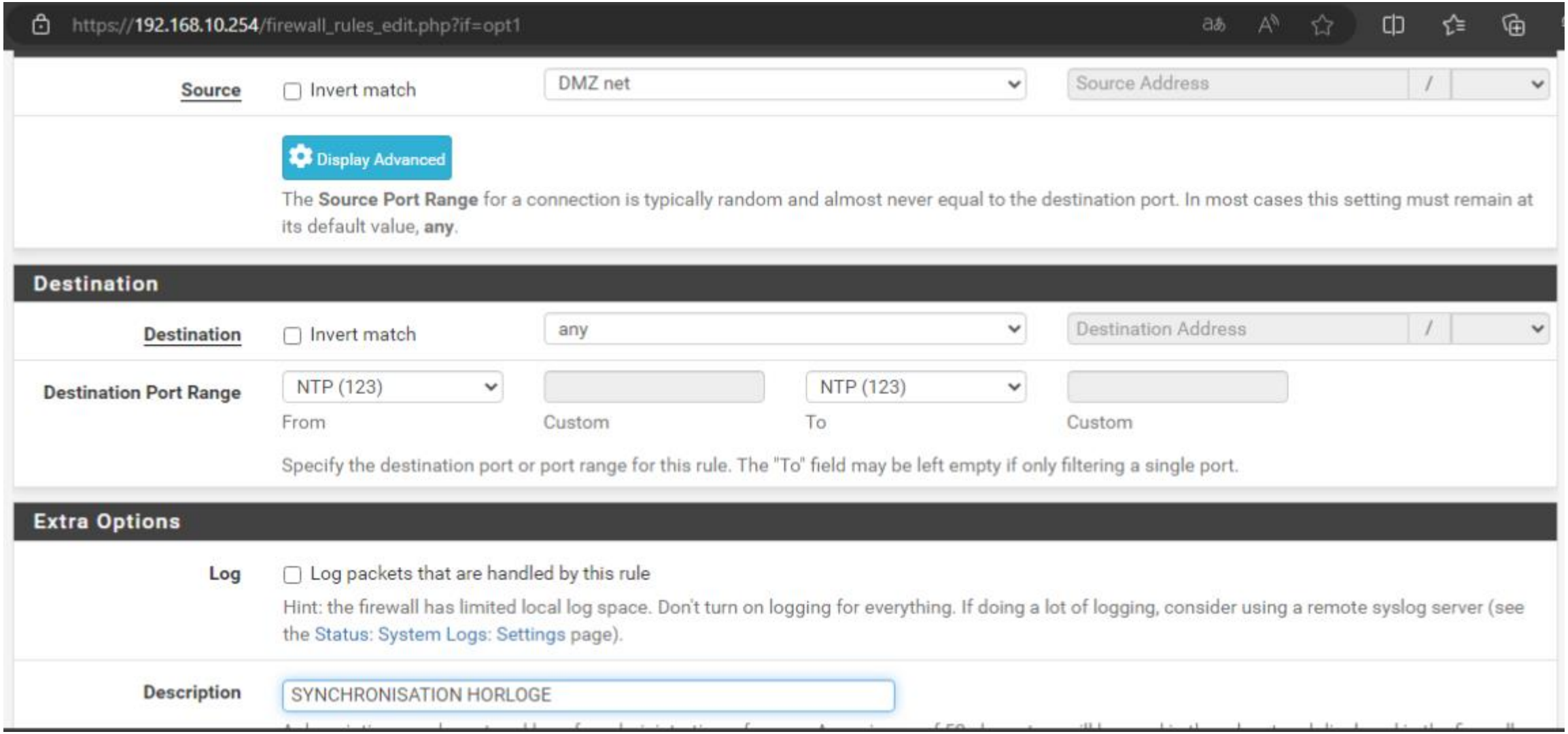
MACHINE CLIENTE WINDOWS 10

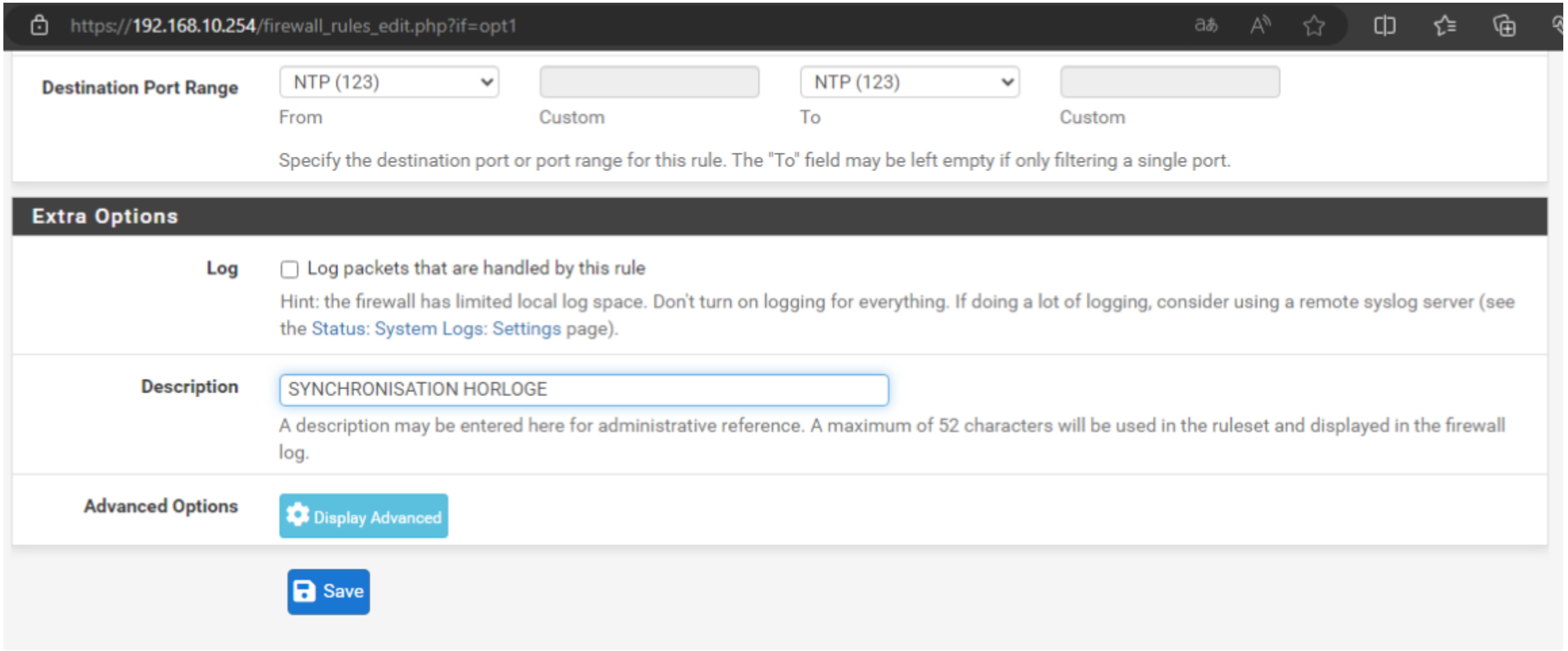
PFSENSE INTERFACE WEB

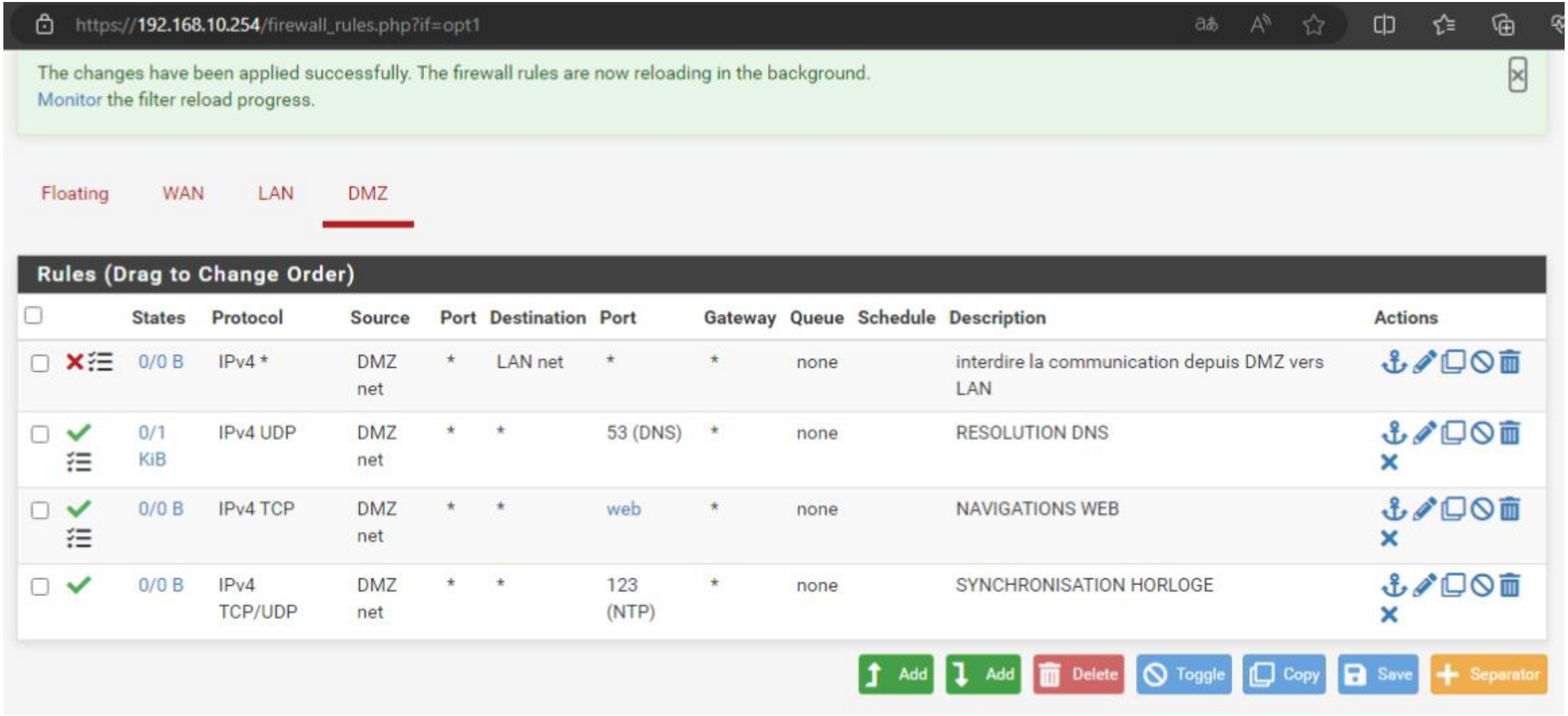
Créer une règle de synchronisation (NTP) horloge depuis DMZ vers LAN

- ✓ Clic sur Rules,
- ✓ Ensuite sur DMZ pour créer la règle
- ✓ Cliquer sur le bouton vert add pour ajouter une nouvelle règle




https://192.168.10.254/firewall_rules_edit.php?if=opt1
Source
Invert match
DMZ net
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
Destination Port Range
NTP (123)
From
Custom
NTP (123)
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.
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
SYNCHRONISATION HORLOGE


https://192.168.10.254/firewall_rules_edit.php?if=opt1
Destination Port Range
NTP (123)
From
Custom
NTP (123)
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.
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
SYNCHRONISATION HORLOGE
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


https://192.168.10.254/firewall_rules.php?if=opt1
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
IPv4 *
DMZ net
*
LAN net
*
*
none
interdire la communication depuis DMZ vers LAN
0/1 KiB
IPv4 UDP
DMZ net
*
*
53 (DNS)
*
none
RESOLUTION DNS
0/0 B
IPv4 TCP
DMZ net
*
*
web
*
none
NAVIGATIONS WEB
0/0 B
IPv4 TCP/UDP
DMZ net
*
*
123 (NTP)
*
none
SYNCHRONISATION HORLOGE
Add
Add
Delete
Toggle
Copy
Save
Separator

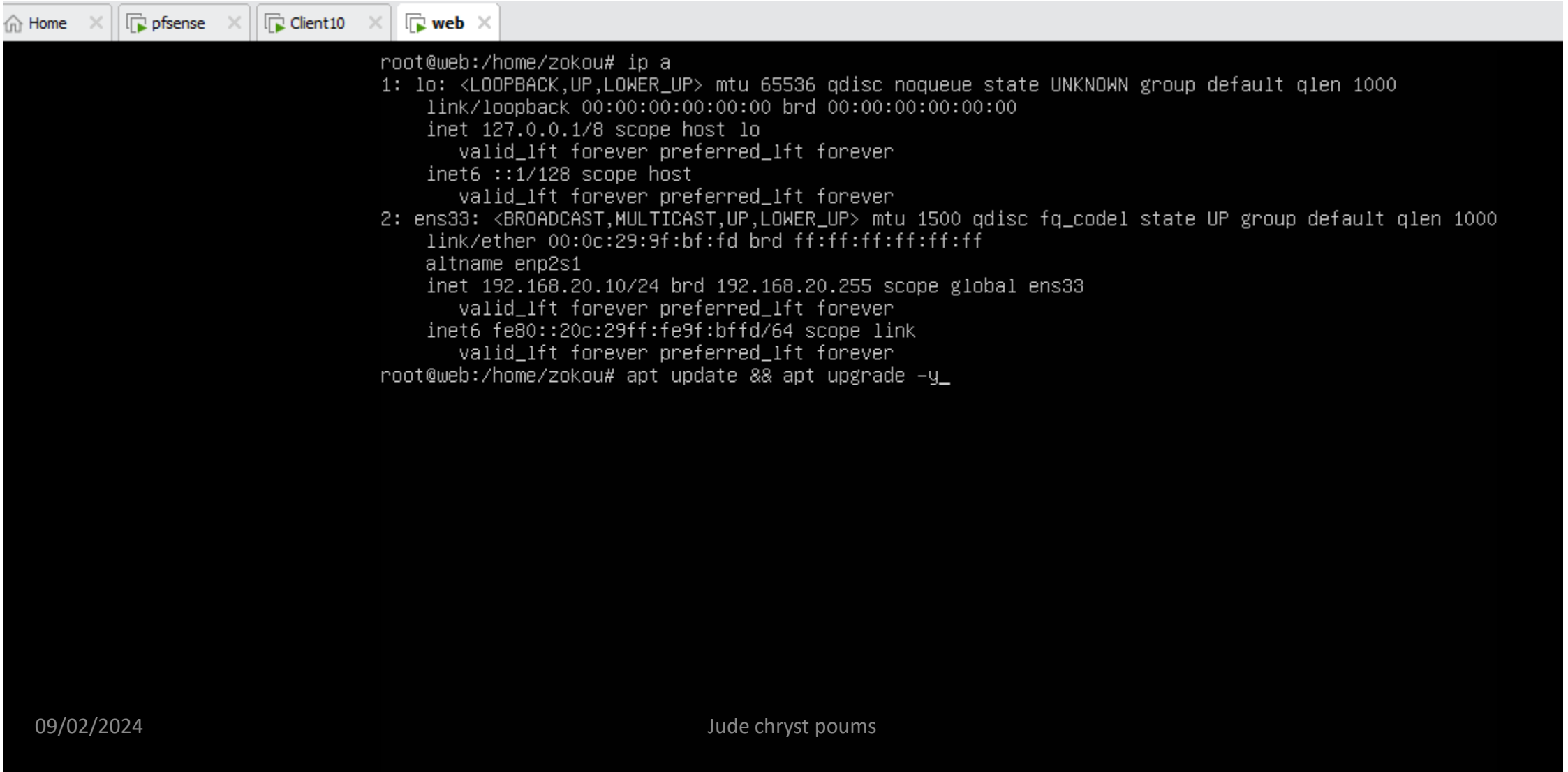
MACHINE UBUNTU-SERVER

WEB_01

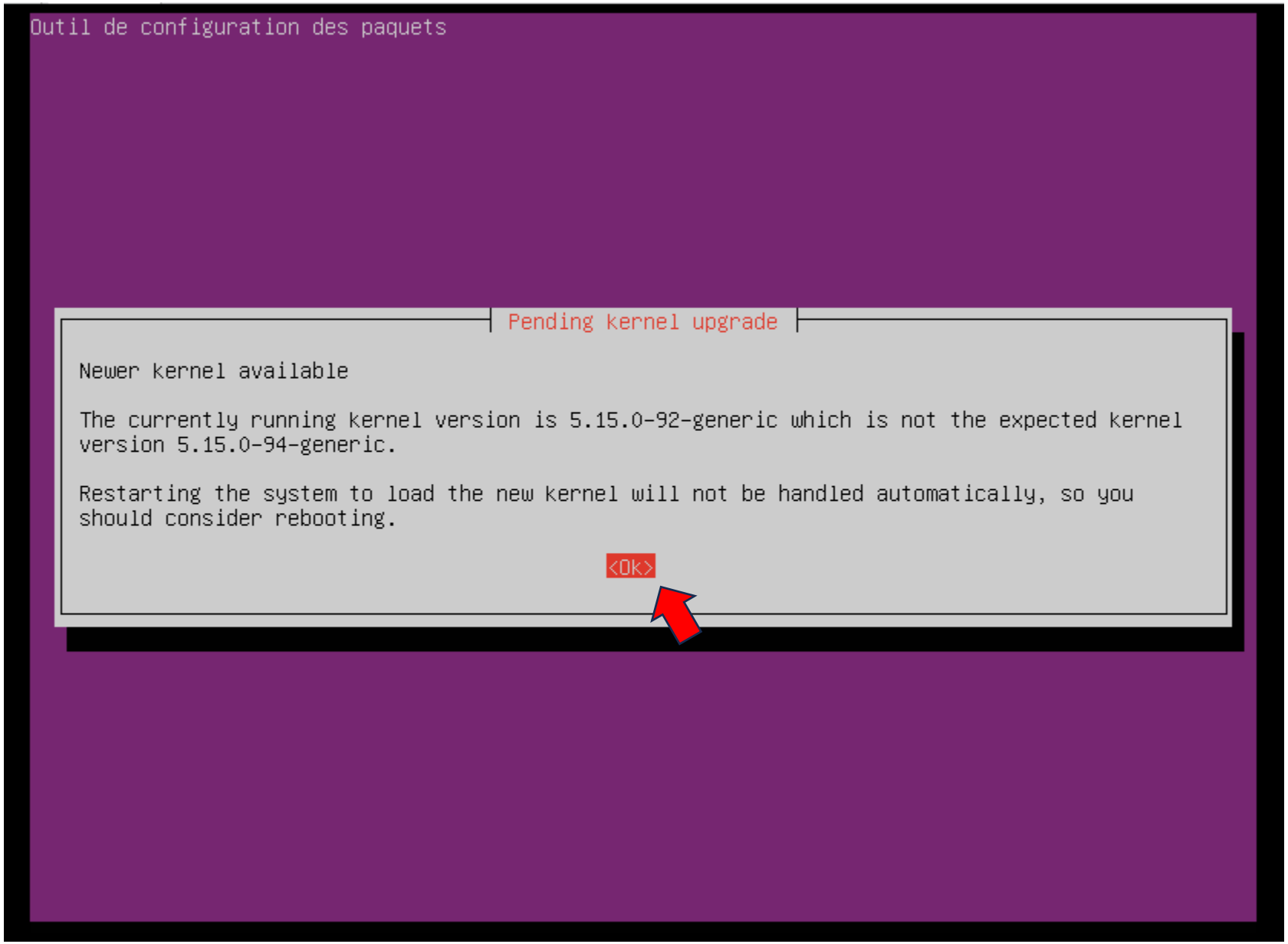
synchronisation horloge permet à notre machine web c’est-à-dire ubuntu d’accéder sur internet

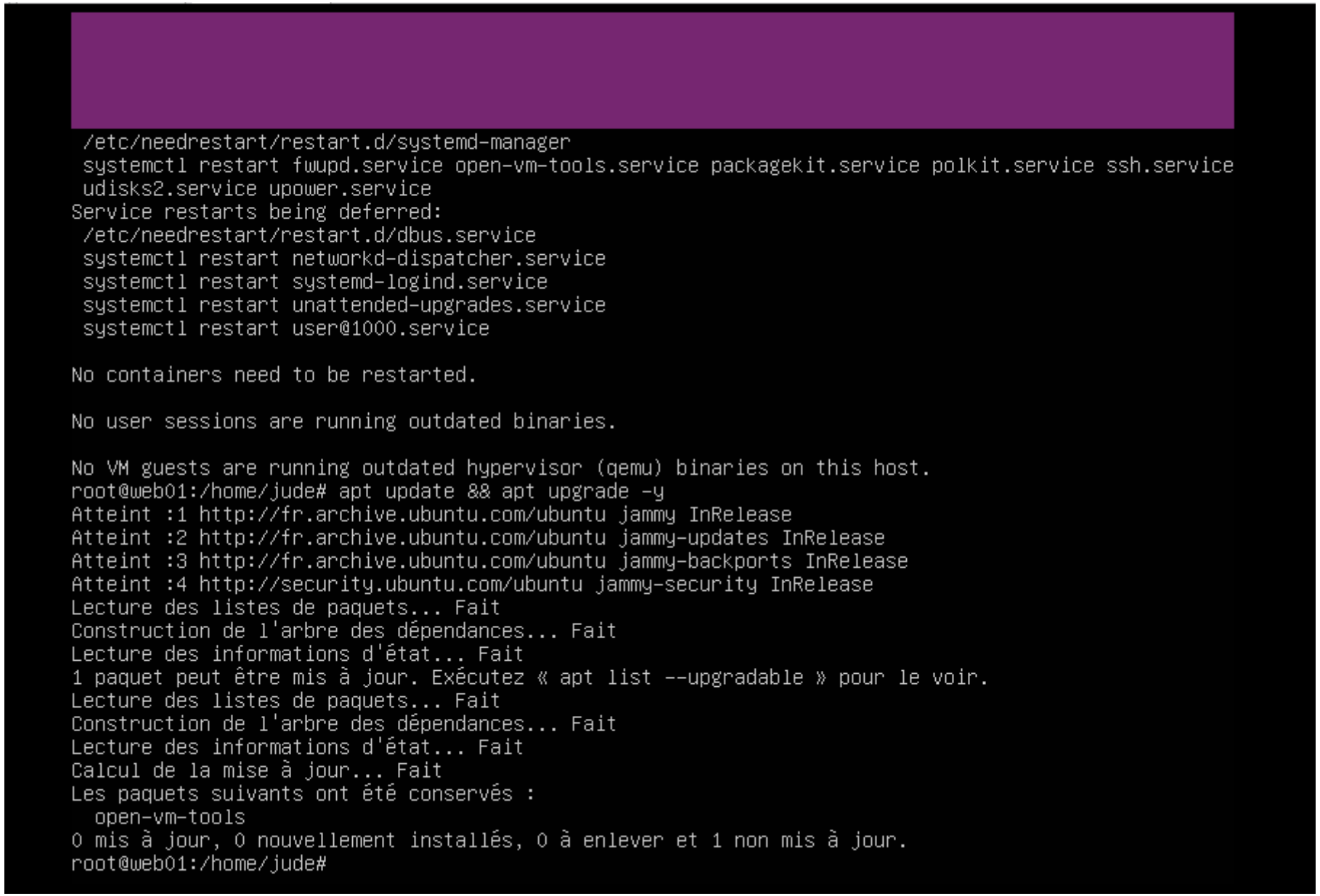
Le NTP est un protocole permettant de synchroniser l'horloge d'un ordinateur avec celle d'un serveur de référence. NTP est un protocole basé sur UDP et utilise le port 123.

Depuis la machine ubuntu-server (web), il est maintenant possible de faire la mise à jour depuis qu'il a accès à internet.
La commande pour faire la mise à jour des paquets sur linux est:
 # apt update && apt upgrade -y



```
root@web:/home/zokou# 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
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:9f:bf:fd brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.10/24 brd 192.168.20.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe9f:bffd/64 scope link
       valid_lft forever preferred_lft forever
root@web:/home/zokou# apt update && apt upgrade -y
Atteint :1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Réception de :2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Atteint :3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease
Réception de :4 http://us.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Réception de :5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1 362 kB]
Réception de :6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [271 kB]
Réception de :7 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1 404 k
B]
Réception de :8 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [231 kB]
Réception de :9 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1 043 kB]
Réception de :10 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [235 kB]
Réception de :11 http://us.archive.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1 111 kB]
Réception de :12 http://us.archive.ubuntu.com/ubuntu jammy-security/main Translation-en [208 kB]
Réception de :13 http://us.archive.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [1 317
 kB]
92% [13 Packages 801 kB/1 317 kB 61%]                                    676 kB/s 1s_
```


Outil de configuration des paquets
Pending kernel upgrade
Newer kernel available
The currently running kernel version is 5.15.0-92-generic which is not the expected kernel version 5.15.0-94-generic.
Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.
<Ok>

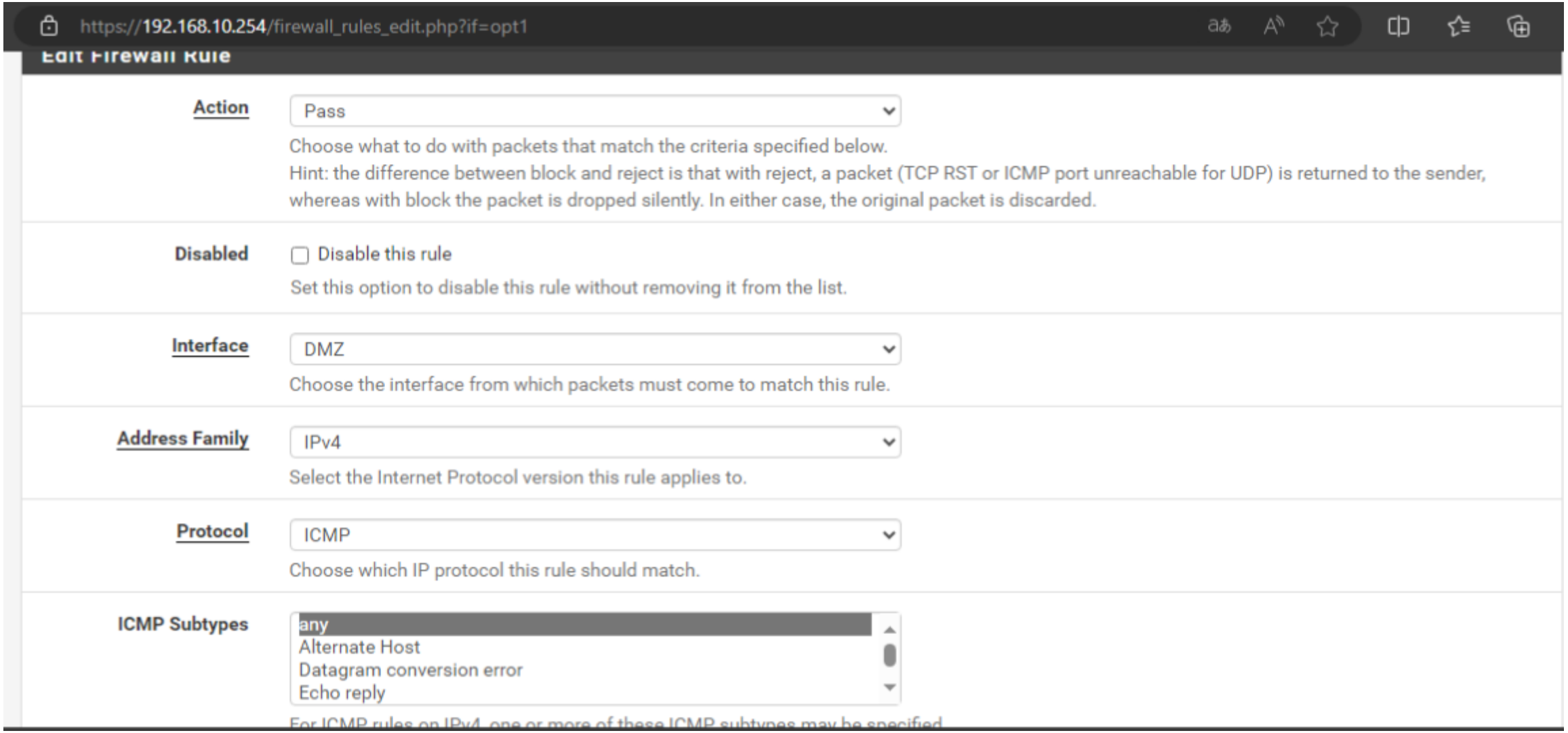

/etc/needrestart/restart.d/systemd-manager
systemctl restart fwupd.service open-vm-tools.service packagekit.service polkit.service ssh.service udisks2.service upower.service
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart networkd-dispatcher.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@web01:/home/jude# apt update && apt upgrade -y
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :3 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Atteint :4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
1 paquet peut être mis à jour. Exécutez « apt list --upgradable » pour le voir.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
Les paquets suivants ont été conservés :
open-vm-tools
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@web01:/home/jude#

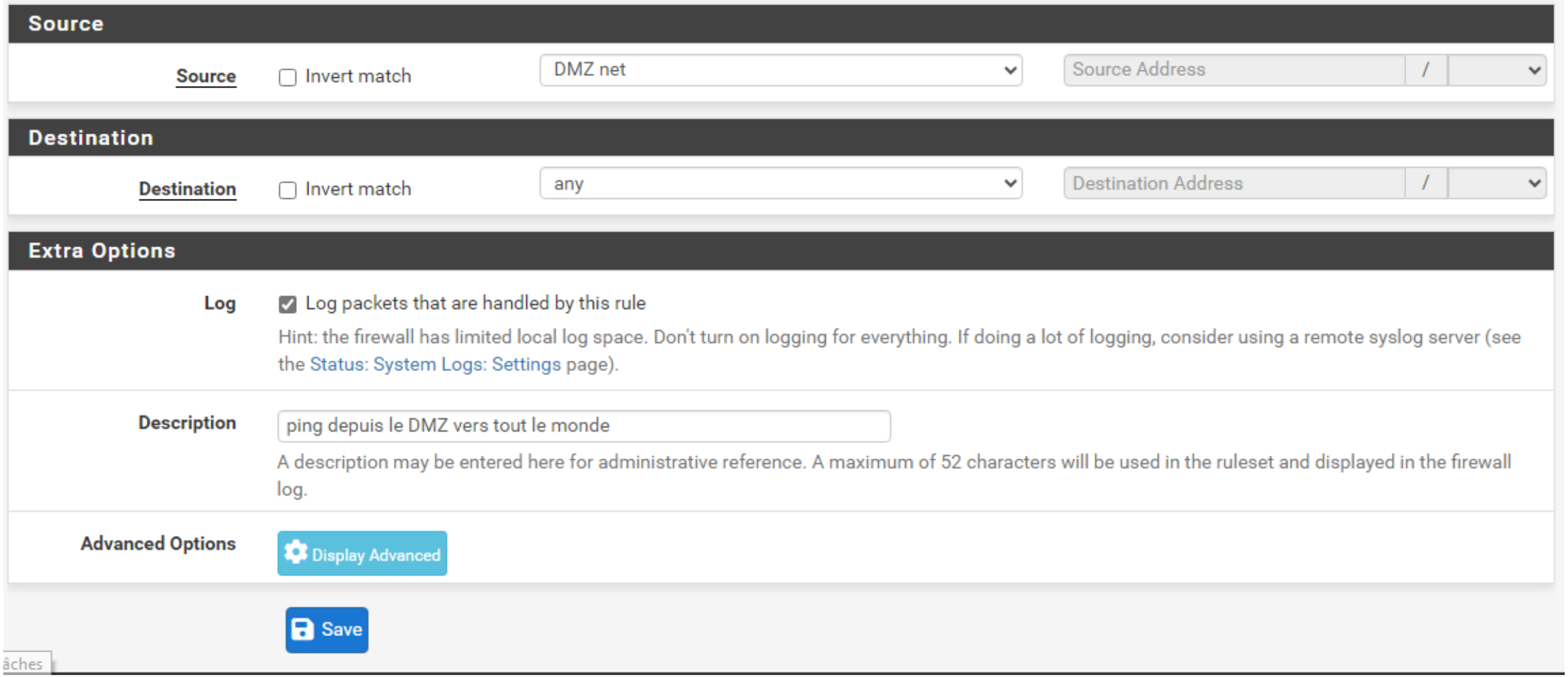
```
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@web01:/home/jude# ping www.google.fr
PING www.google.fr (142.250.74.227) 56(84) bytes of data.
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=1 ttl=127 time=13.3 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=2 ttl=127 time=5.62 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=3 ttl=127 time=5.40 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=4 ttl=127 time=9.89 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=5 ttl=127 time=4.90 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=6 ttl=127 time=6.62 ms
64 bytes from par10s40-in-f3.1e100.net (142.250.74.227): icmp_seq=7 ttl=127 time=7.41 ms
^C
--- www.google.fr ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6055ms
rtt min/avg/max/mdev = 4.896/7.597/13.349/2.812 ms
root@web01:/home/jude#
```

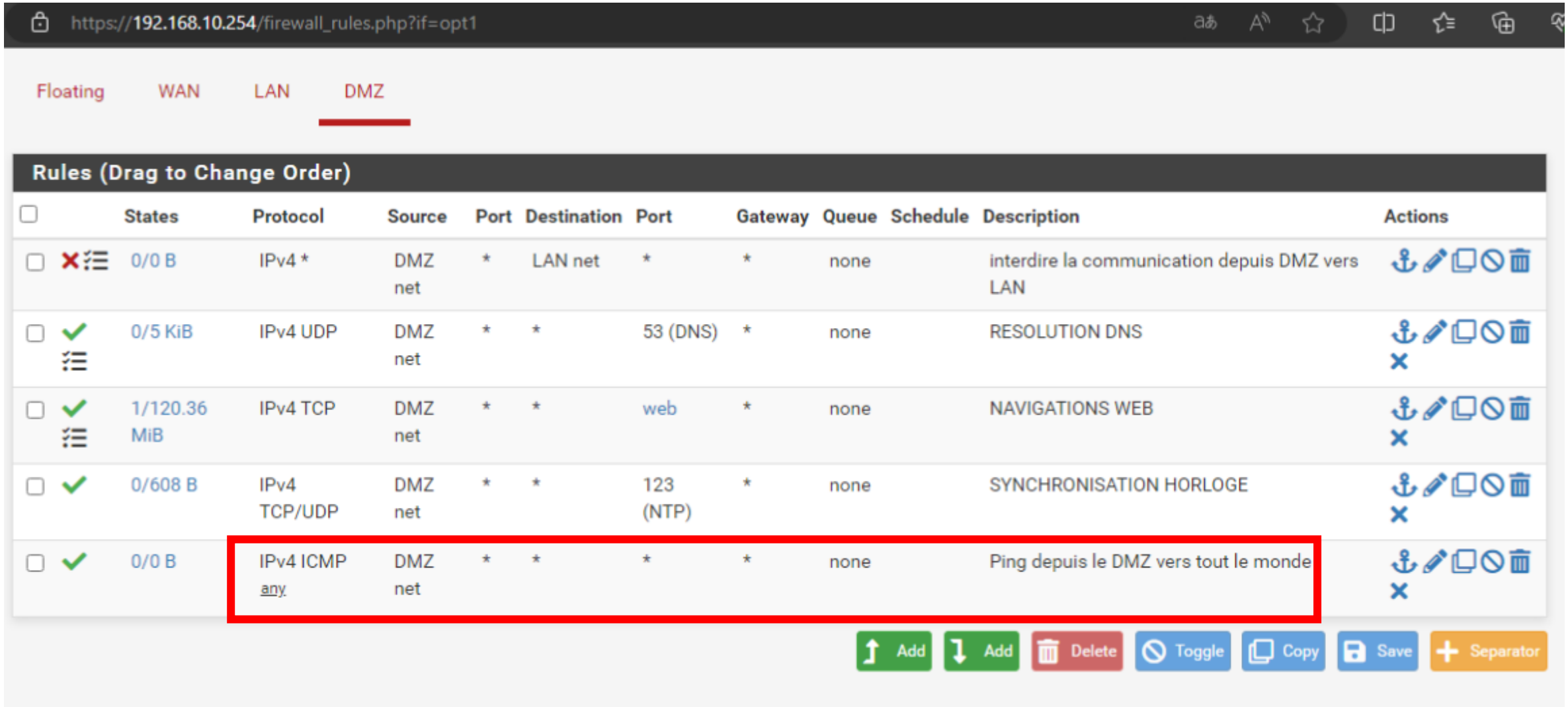
MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

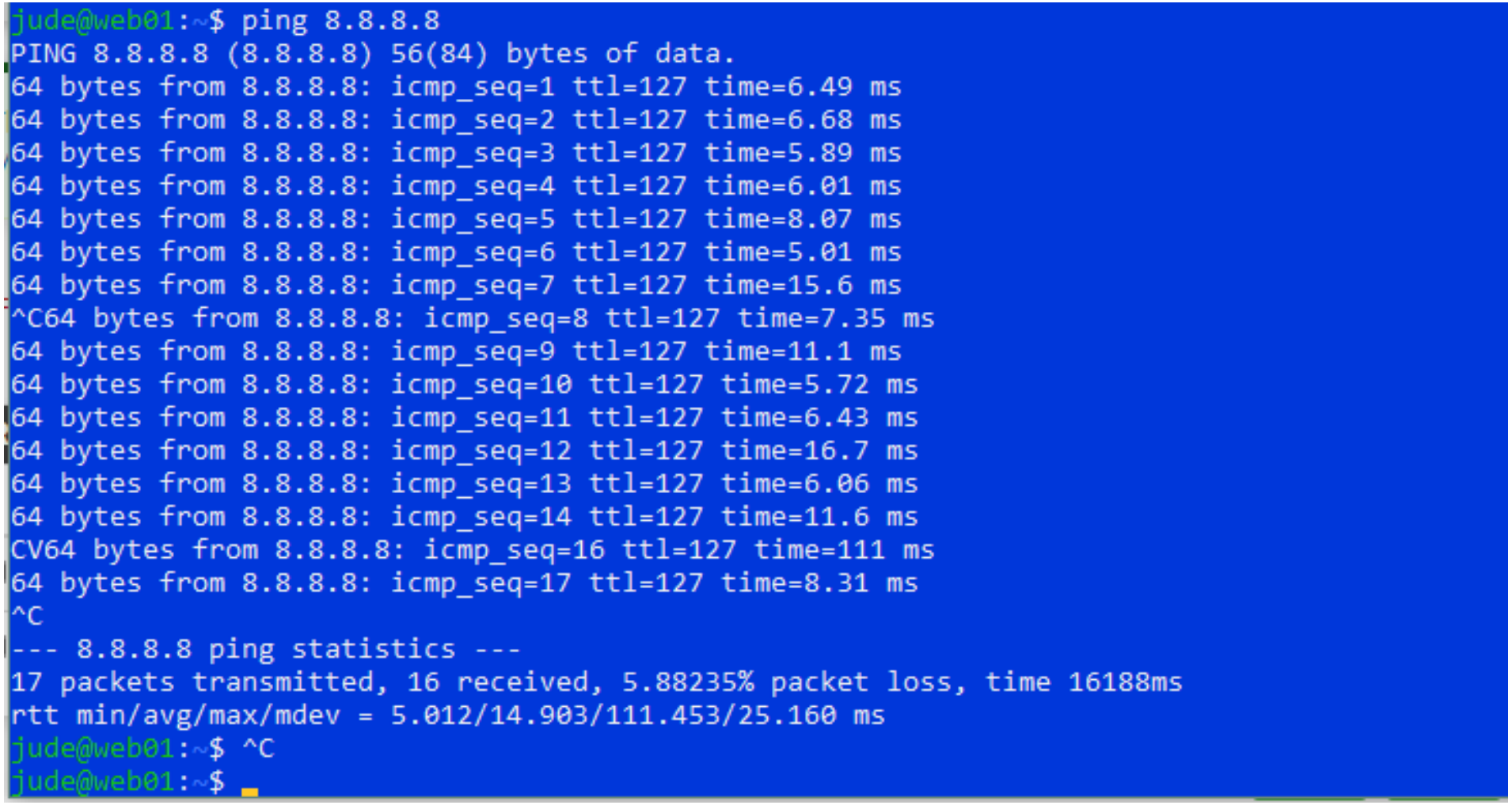
Créer une règle de ping depuis le DMZ vers tout le monde


https://192.168.10.254/firewall_rules_edit.php?if=opt1
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
DMZ
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


Source
Source
Invert match
DMZ net
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
ping depuis le DMZ vers tout le monde
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

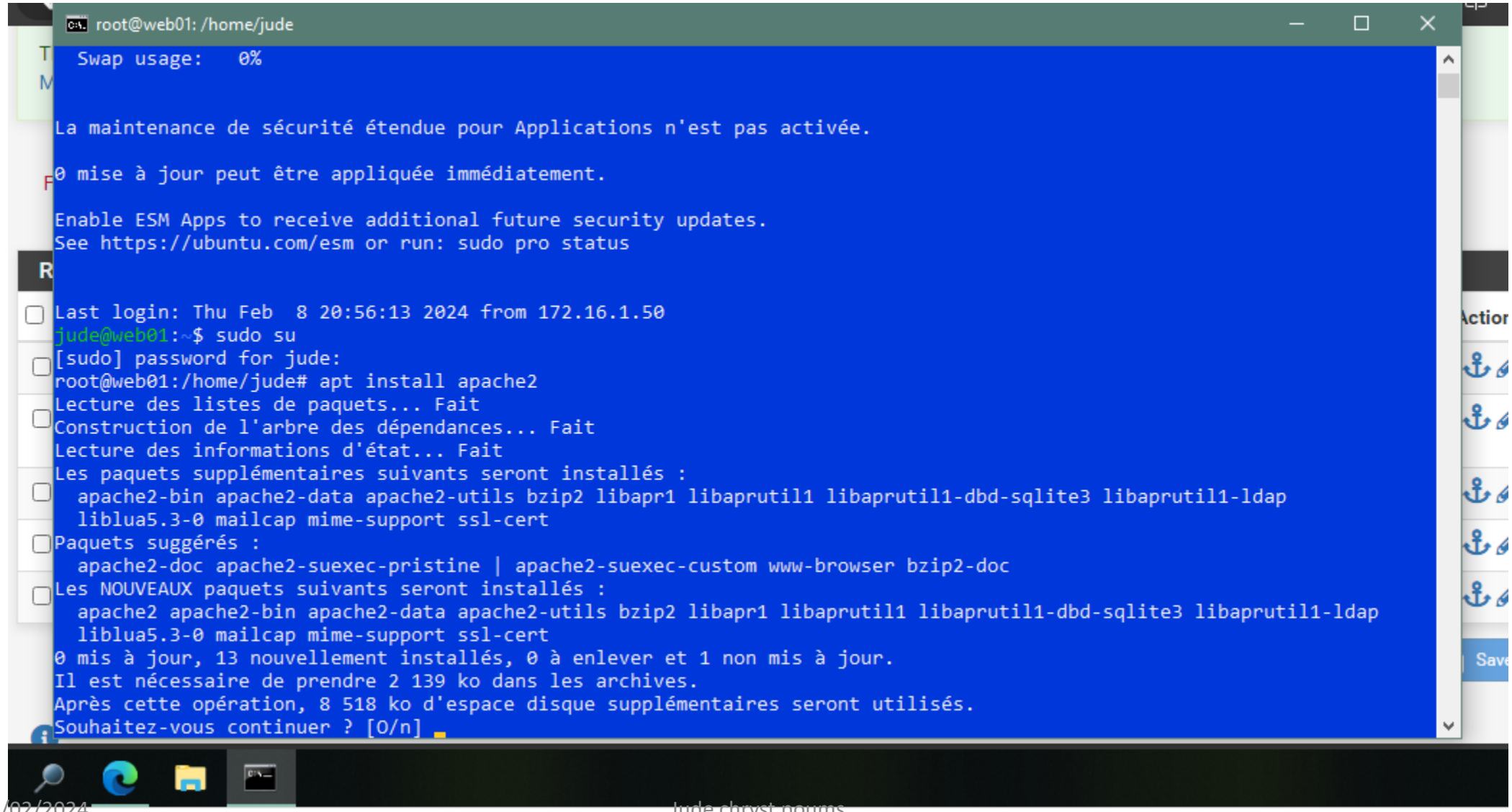

https://192.168.10.254/firewall_rules.php?if=opt1
Floating
WAN
LAN
DMZ
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
IPv4 *
DMZ net
*
LAN net
*
*
none
interdire la communication depuis DMZ vers LAN
0/5 KiB
IPv4 UDP
DMZ net
*
*
53 (DNS)
*
none
RESOLUTION DNS
1/120.36 MiB
IPv4 TCP
DMZ net
*
*
web
*
none
NAVIGATIONS WEB
0/608 B
IPv4 TCP/UDP
DMZ net
*
*
123 (NTP)
*
none
SYNCHRONISATION HORLOGE
0/0 B
IPv4 ICMP any
DMZ net
*
*
*
*
none
Ping depuis le DMZ vers tout le monde
Add
Add
Delete
Toggle
Copy
Save
Separator

Test de connectivité après avoir ajouter la règle de ping depuis le DMZ vers tout le monde.
Depuis la machine Web01, faire un ping vers google
 # ping 8.8.8.8
 # ping www.google.fr

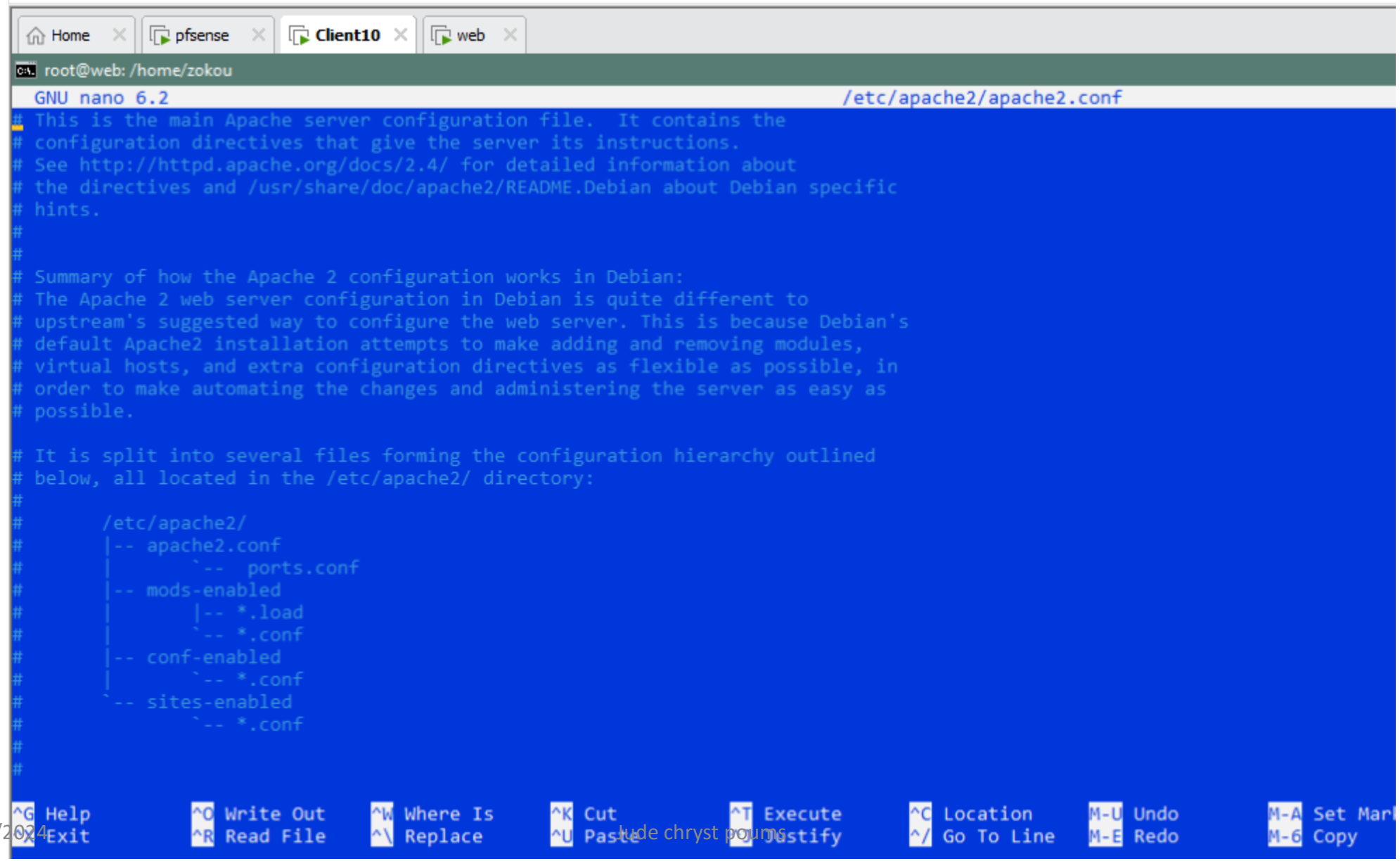


Installer le paquet apache2

apt install apache2



nano /etc/apache2/apache2.conf

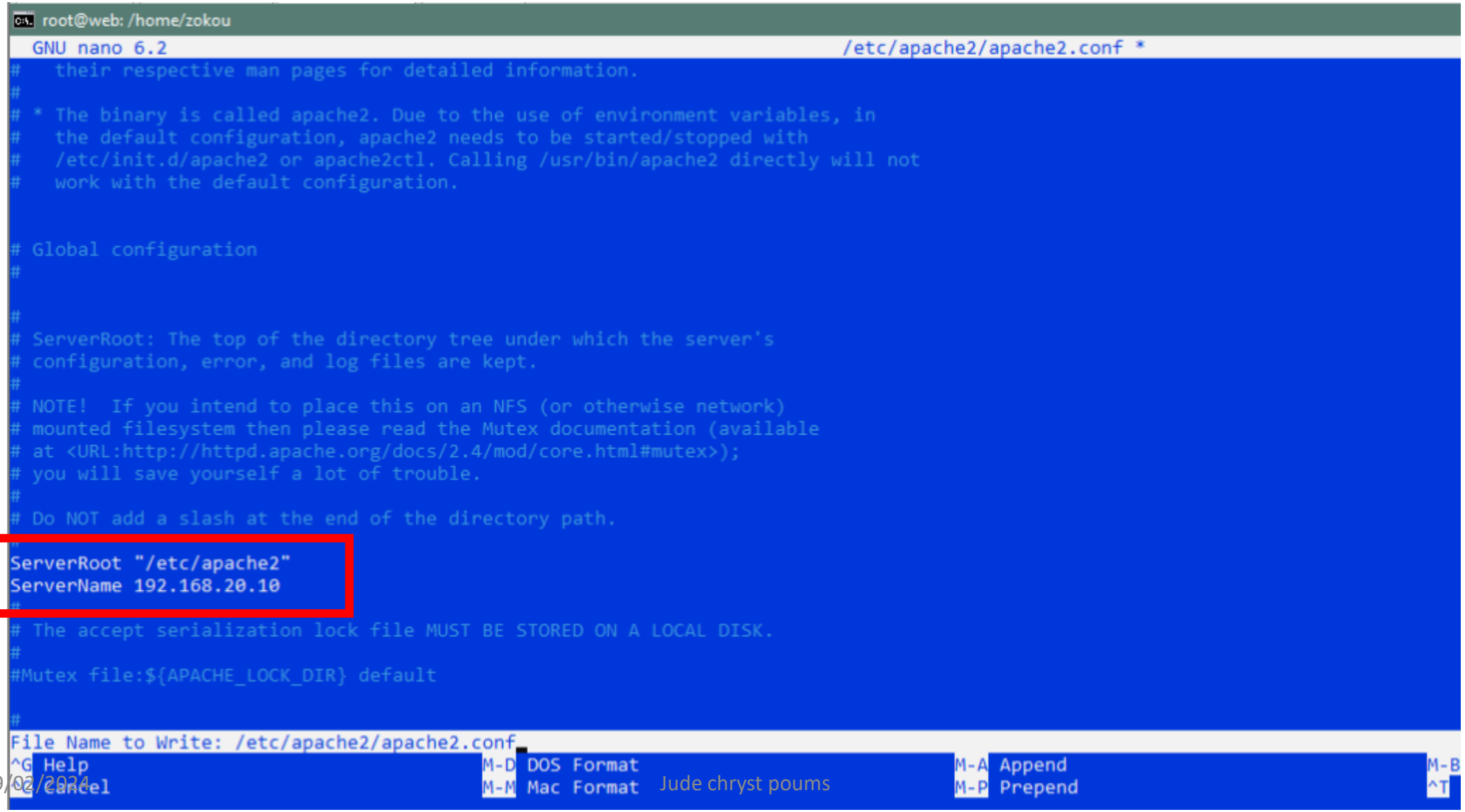


nano /etc/apache2/apache2.conf

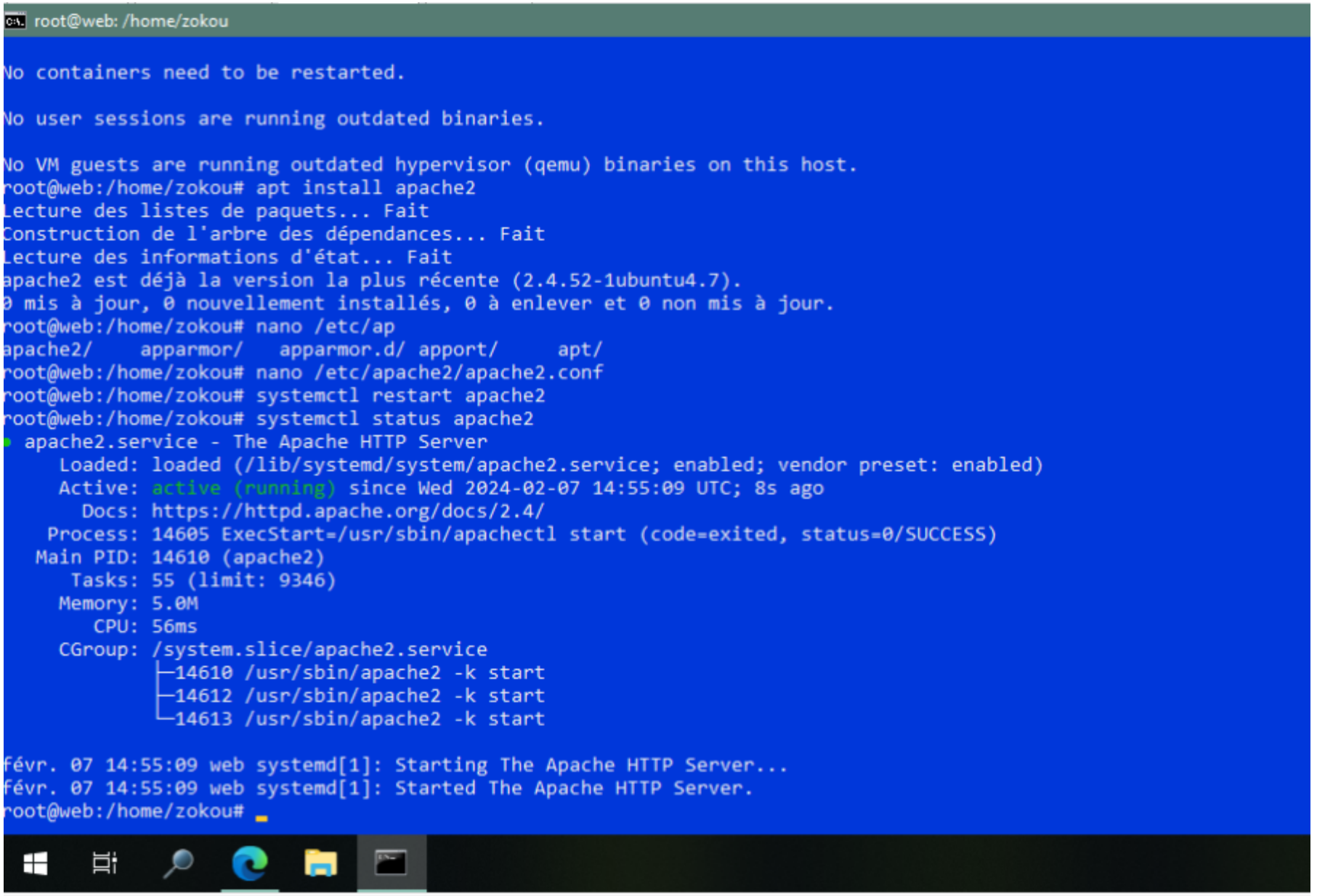
Décommenter ServerRoot "/etc/apache2 "

Ajouter cette ligne ServerName 192.168.20.10

Cette adresse ip est celle du server ubuntu web



systemctl restart apache2
systemctl status apache2



Remplacez le fichier index.html du serveur Web01 par la page web index.html de imie.fr

cd /var/www/html/
ls

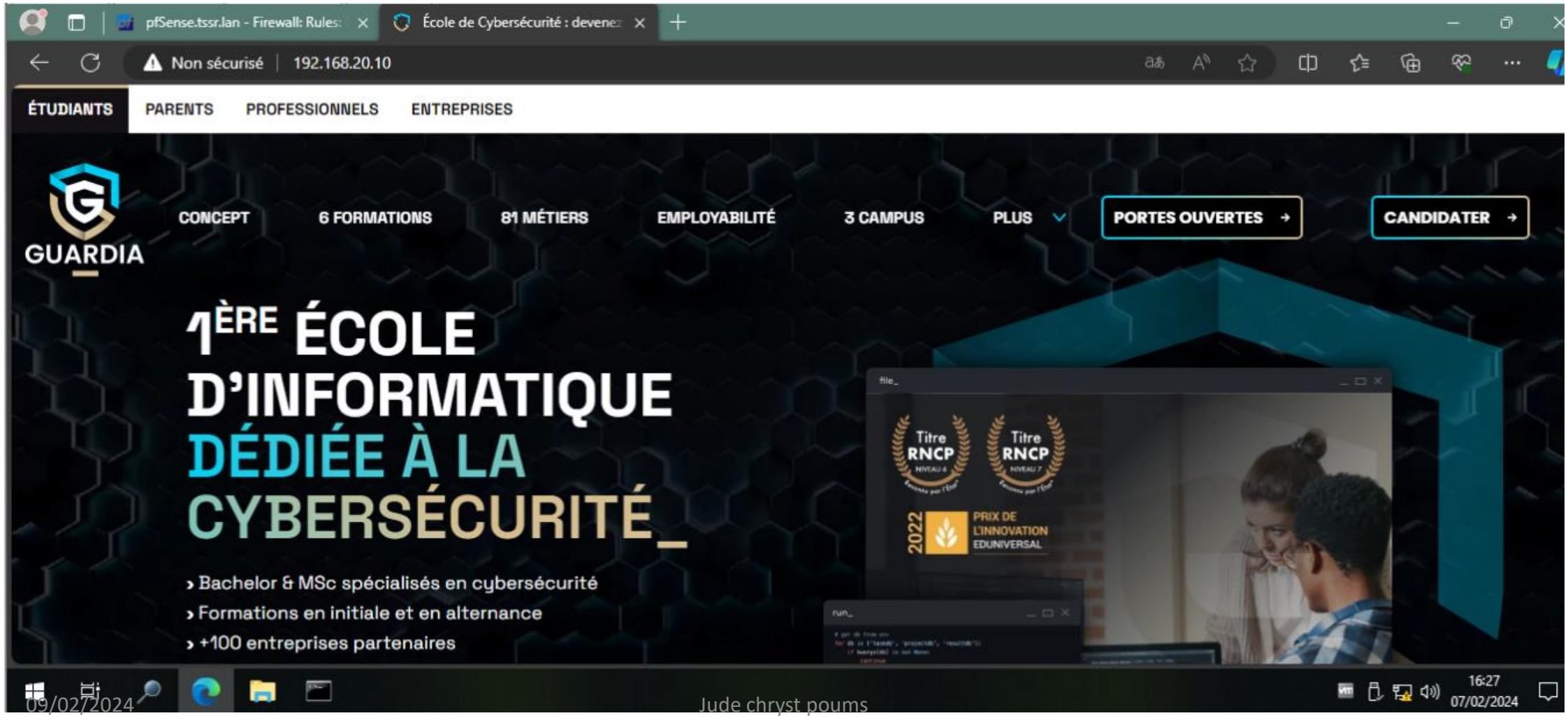
Télécharger la page internet par exemple de imie paris

wget imie.fr -k

```
                RTC time: mer. 2024-02-07 15:11:55
               Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
root@web:/home/zokou# cd /var/www/html/
root@web:/var/www/html# ls
index.html
root@web:/var/www/html# wget imie.fr -k
--2024-02-07 15:24:45--  http://imie.fr/
Resolving imie.fr (imie.fr)... 54.38.21.228
Connecting to imie.fr (imie.fr)|54.38.21.228|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://imie.fr/ [following]
--2024-02-07 15:24:46--  https://imie.fr/
Connecting to imie.fr (imie.fr)|54.38.21.228|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://guardia.school [following]
--2024-02-07 15:24:46--  https://guardia.school/
Resolving guardia.school (guardia.school)... 13.249.9.121, 13.249.9.64, 13.249.9.11, ...
Connecting to guardia.school (guardia.school)|13.249.9.121|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 409715 (400K) [text/html]
Saving to: ‘index.html.1’

index.html.1                                100%[=========================================

2024-02-07 15:24:46 (6,00 MB/s) - ‘index.html.1’ saved [409715/409715]

Converting links in index.html.1... 28.
11-17
Converted links in 1 files in 0,01 seconds.
root@web:/var/www/html# ^C
root@web:/var/www/html#
```

root@web:/var/www/html# ls
mv index.html index.html.old
mv index.html.1 index.html
ls

```
Location: https://guardia.school [following]
--2024-02-07 15:24:46--  https://guardia.school/
Resolving guardia.school (guardia.school)... 13.249.9.121, 13.24
Connecting to guardia.school (guardia.school)|13.249.9.121|:443
HTTP request sent, awaiting response... 200 OK
Length: 409715 (400K) [text/html]
Saving to: ‘index.html.1’

index.html.1                                        100%[==================

2024-02-07 15:24:46 (6,00 MB/s) - ‘index.html.1’ saved [409715/4

Converting links in index.html.1... 28.
11-17
Converted links in 1 files in 0,01 seconds.
root@web:/var/www/html# ^C
root@web:/var/www/html# ls
index.html  index.html.1
root@web:/var/www/html# mv index.html index.html.old
root@web:/var/www/html# mv index.html.1 index.html
root@web:/var/www/html# ls
index.html  index.html.old
root@web:/var/www/html#
```

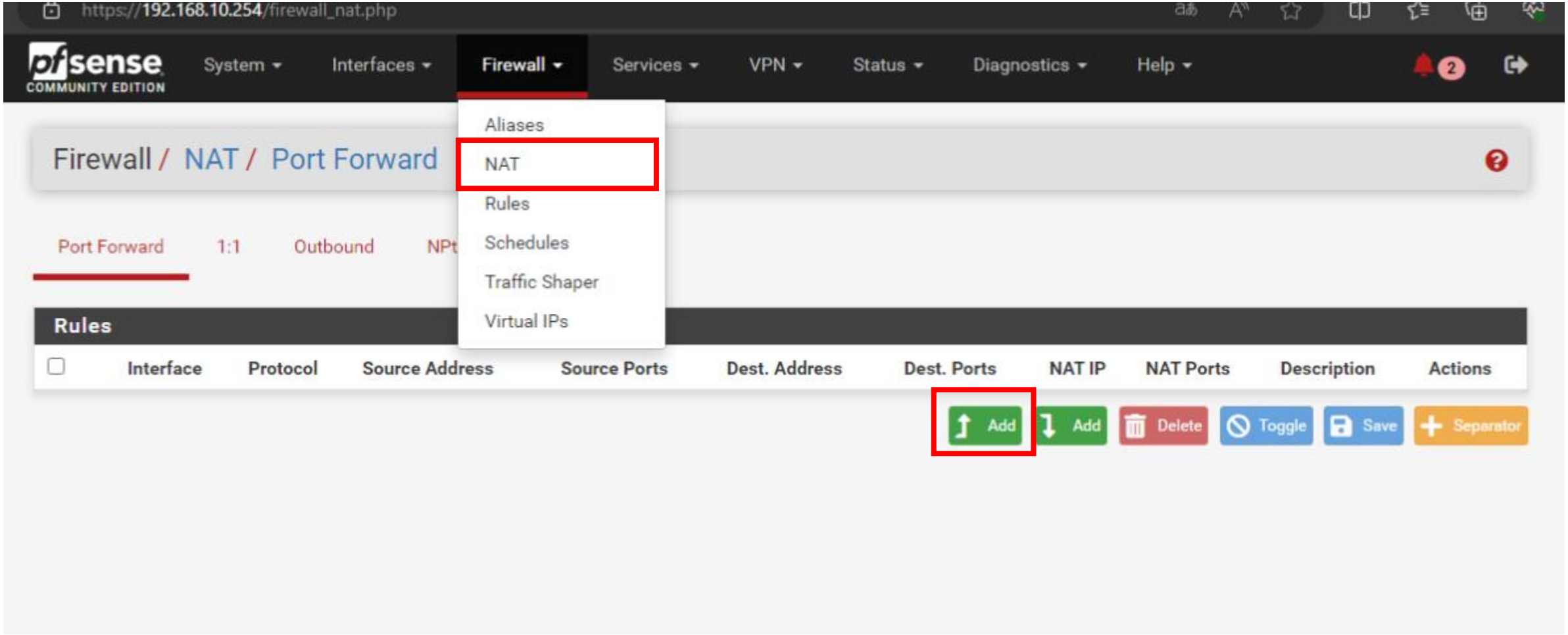

pfSense.tssr.lan - Firewall: Rules:
École de Cybersécurité : devenez
Non sécurisé
192.168.20.10
ÉTUDIANTS
PARENTS
PROFESSIONNELS
ENTREPRISES
GUARDIA
CONCEPT
6 FORMATIONS
81 MÉTIERS
EMPLOYABILITÉ
3 CAMPUS
PLUS
PORTES OUVERTES
CANDIDATER
1ÈRE ÉCOLE D'INFORMATIQUE DÉDIÉE À LA CYBERSÉCURITÉ_
› Bachelor & MSc spécialisés en cybersécurité
› Formations en initiale et en alternance
› +100 entreprises partenaires
Titre RNCP
Titre RNCP
2022
PRIX DE L'INNOVATION EDUNIVERSAL
16:27
07/02/2024

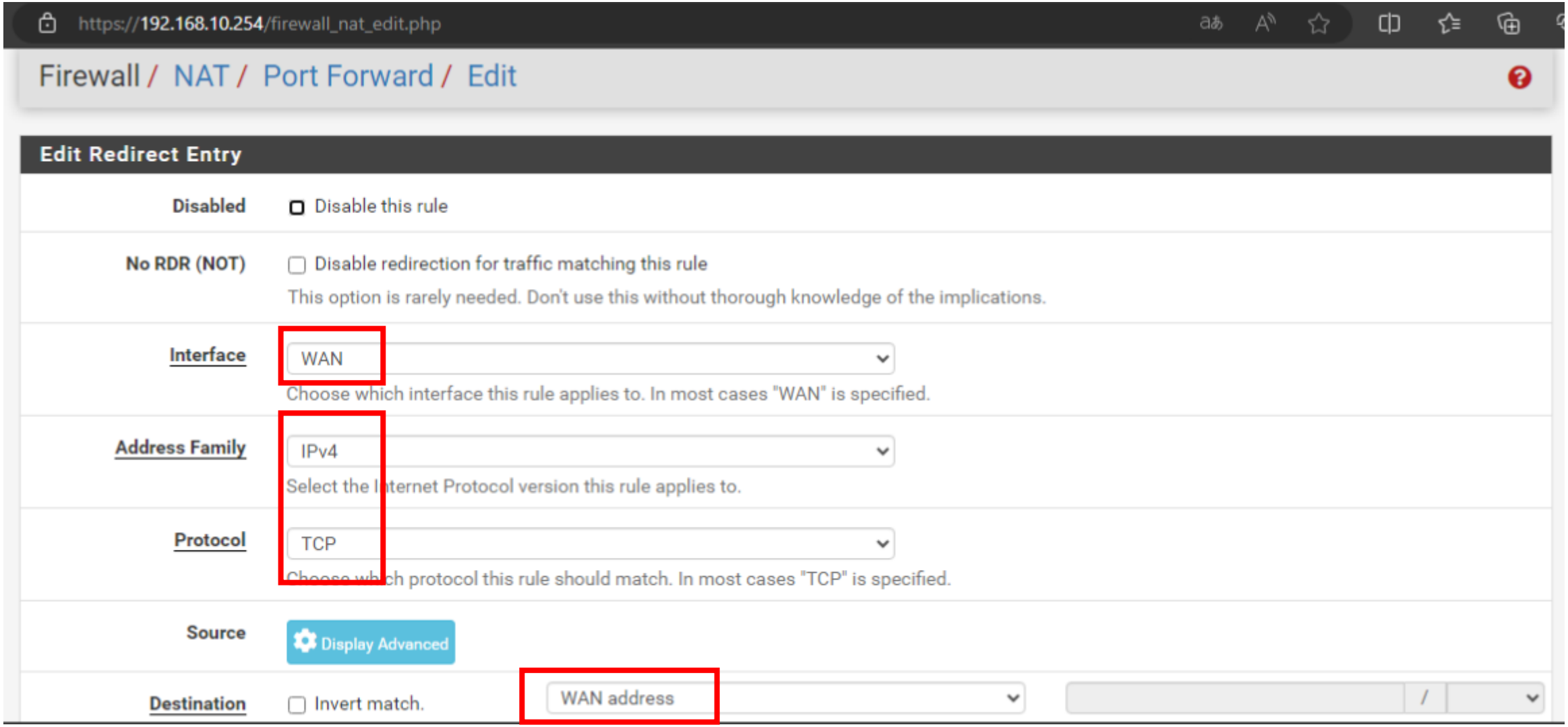
MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

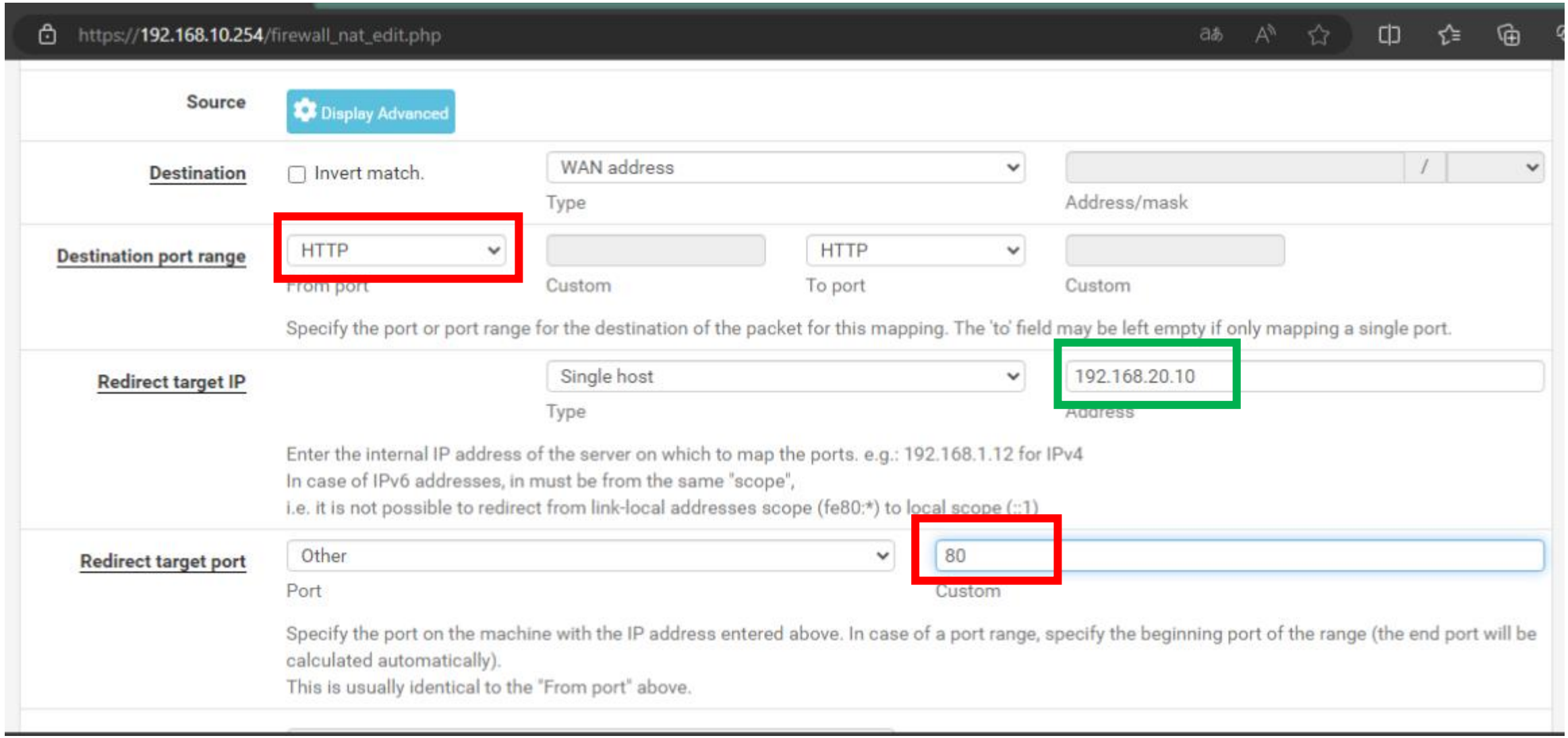
Créer une règle d'accès au serveur web01 de la DMZ depuis le WAN

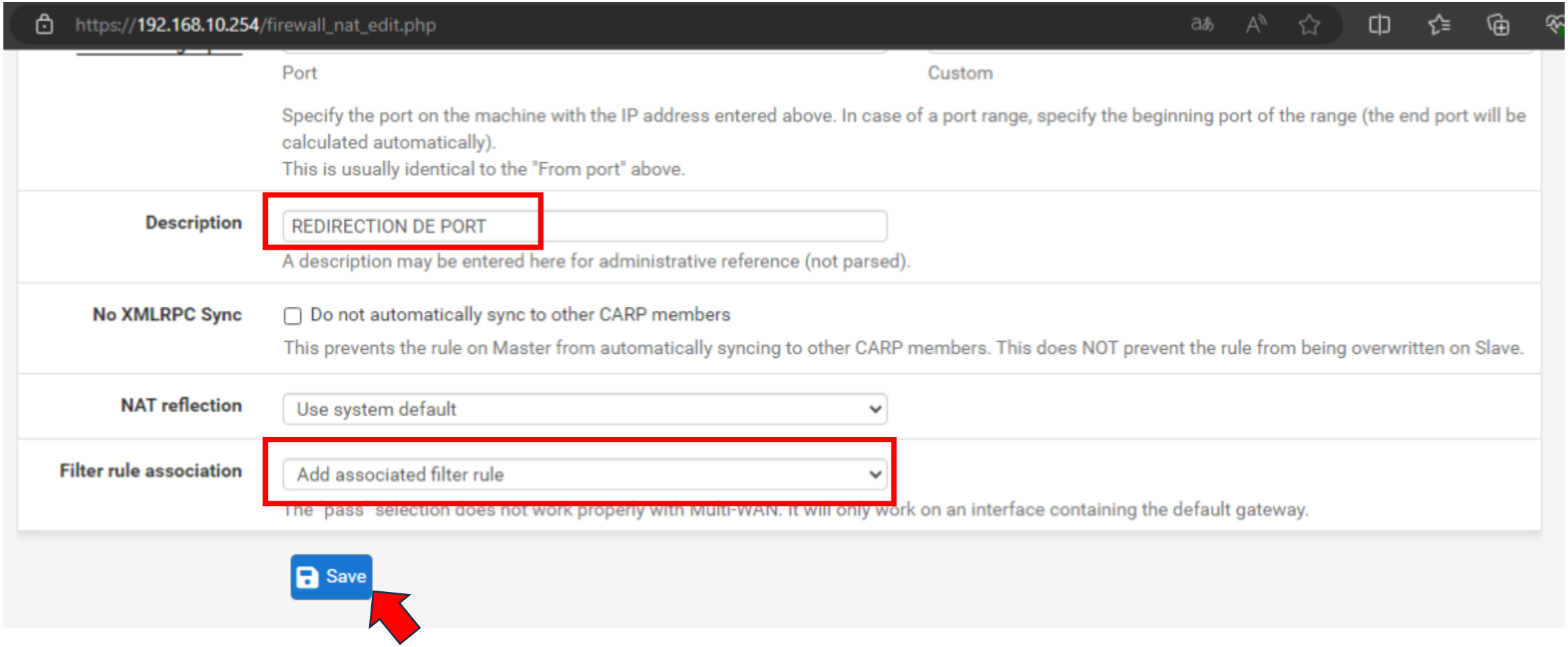
- ✓ Clic sur NAT,
- ✓ Ensuite cliquer sur le bouton add

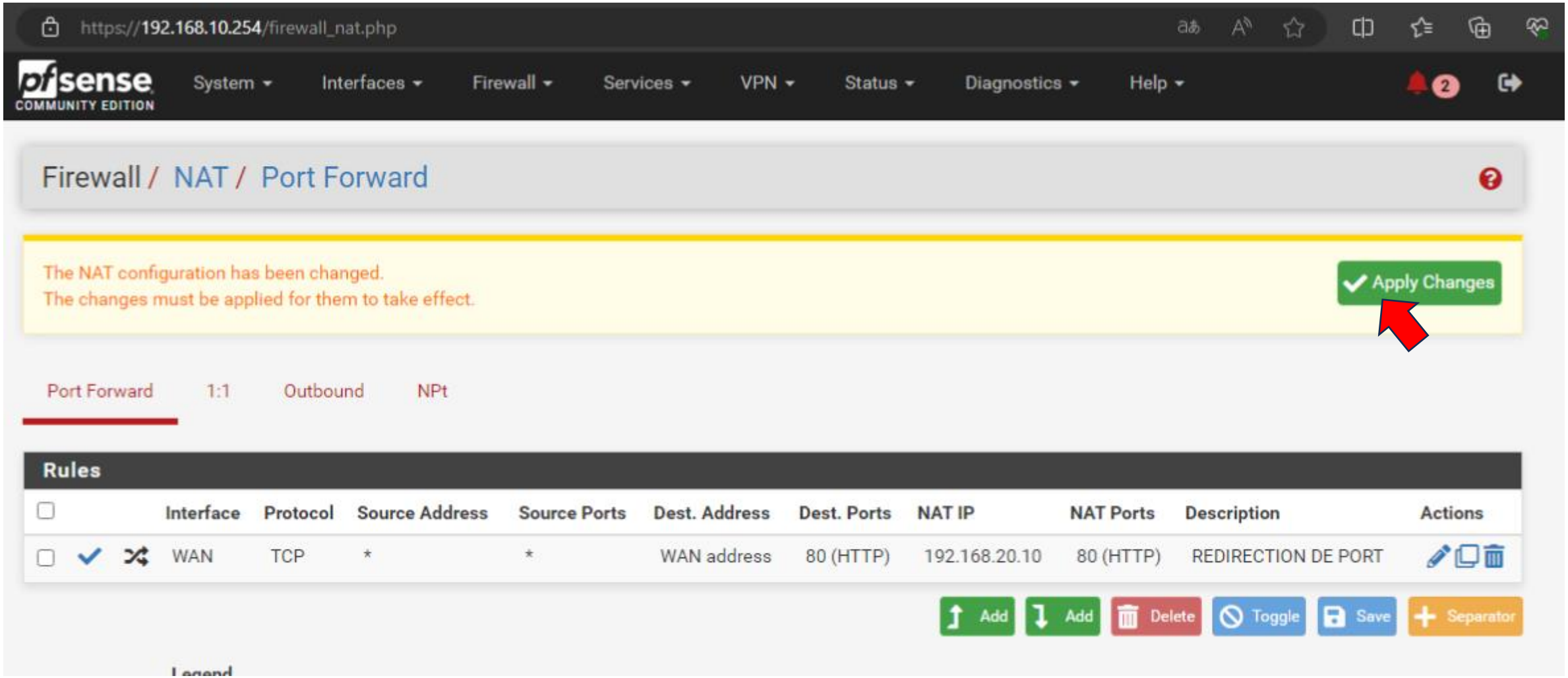


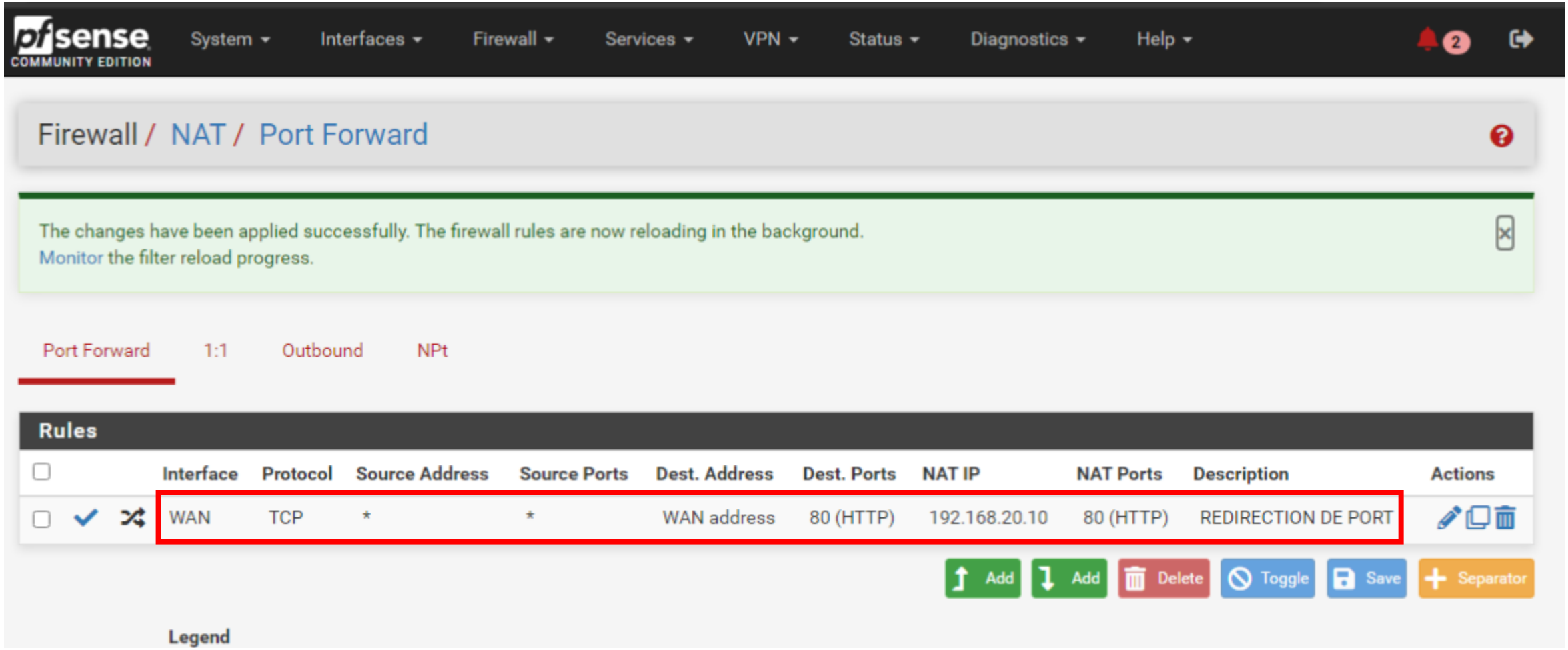

https://192.168.10.254/firewall_nat_edit.php
Firewall / NAT / Port Forward / Edit
Edit Redirect Entry
Disabled
Disable this rule
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface
WAN
Choose 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

L’adresse ip qu’il faut mettre dans la redirect target IP est celle de votre machine ubuntu-server nommé WEB

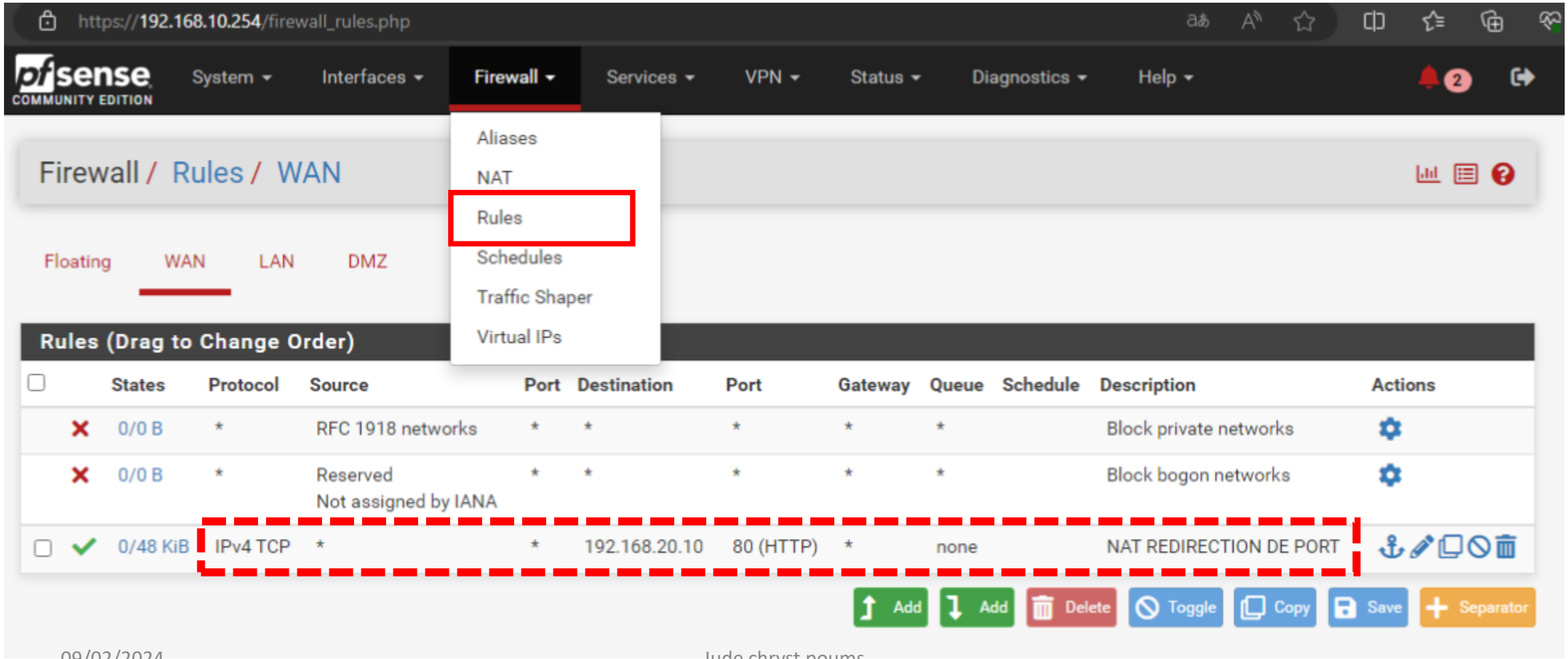


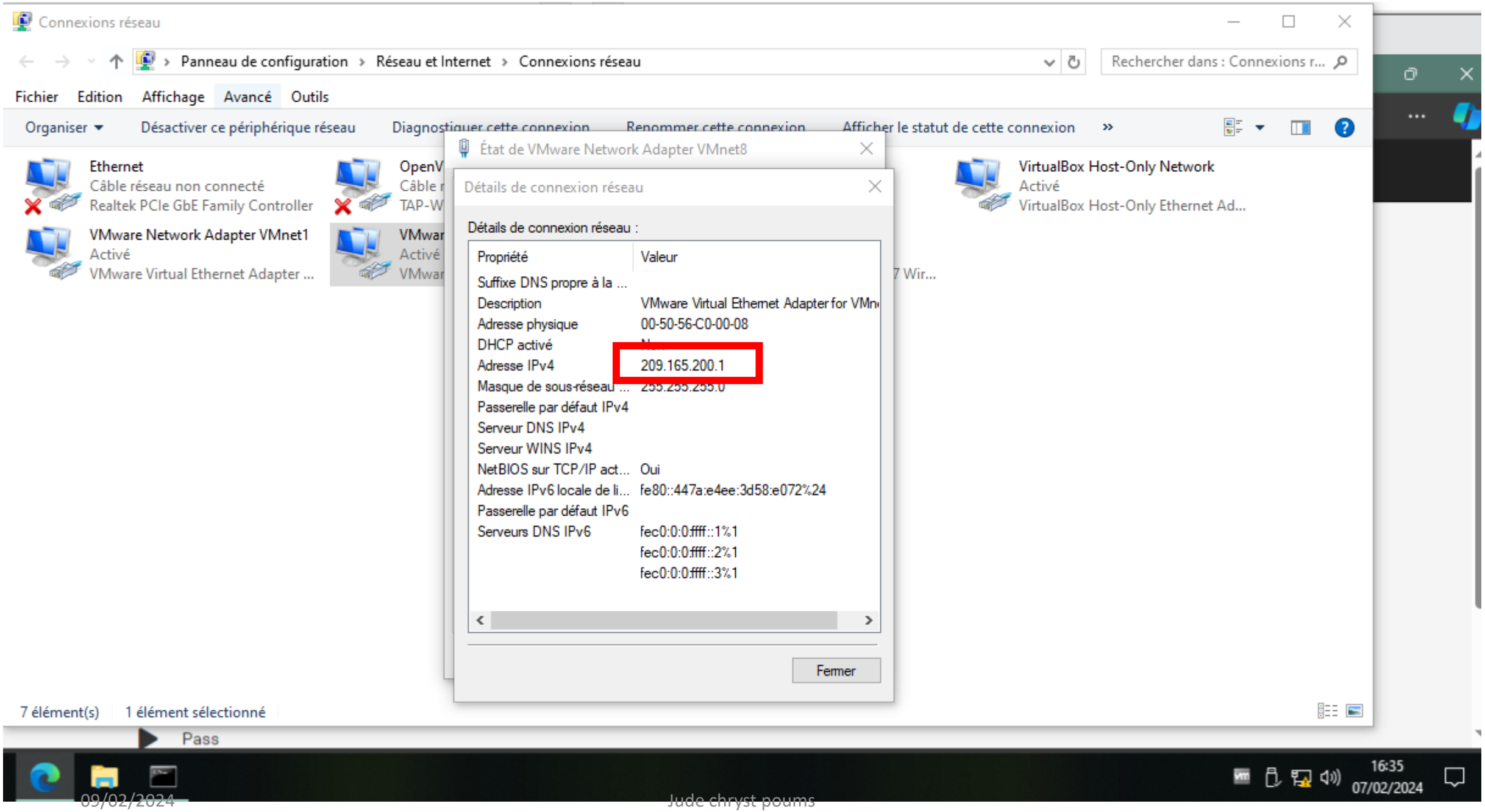

https://192.168.10.254/firewall_nat_edit.php
Port
Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.
Description
REDIRECTION DE PORT
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
Save


https://192.168.10.254/firewall_nat.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
2
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
80 (HTTP)
192.168.20.10
80 (HTTP)
REDIRECTION DE PORT
Add
Add
Delete
Toggle
Save
Separator
Legend


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
2
Firewall / NAT / Port Forward
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
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
80 (HTTP)
192.168.20.10
80 (HTTP)
REDIRECTION DE PORT
Add
Add
Delete
Toggle
Save
Separator
Legend

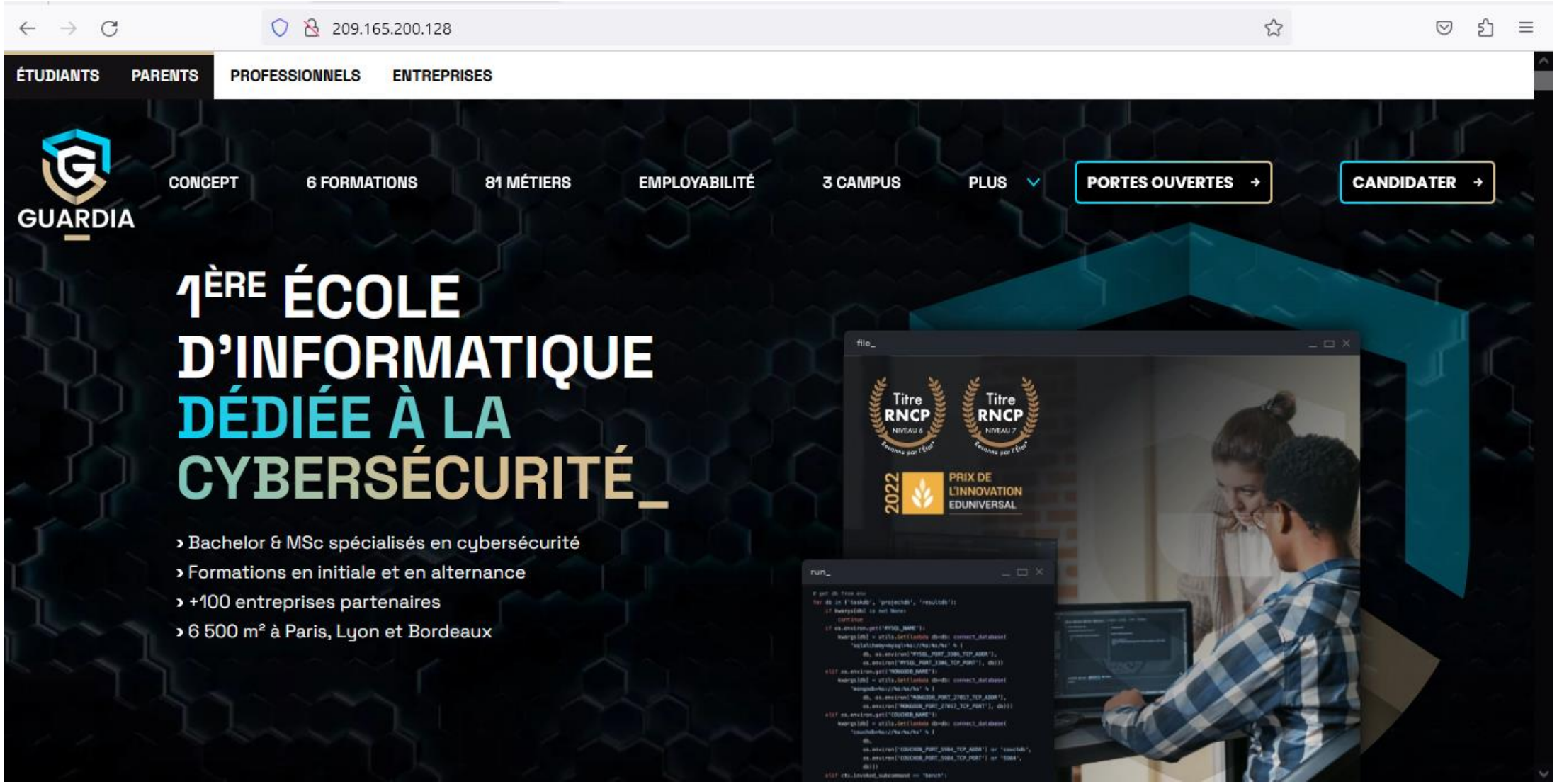
✓ **En allant dans Rules et WAN**
Une règle a été ajouter automatiquement quand nous avons créer une règle d'accès au serveur web01 de la DMZ



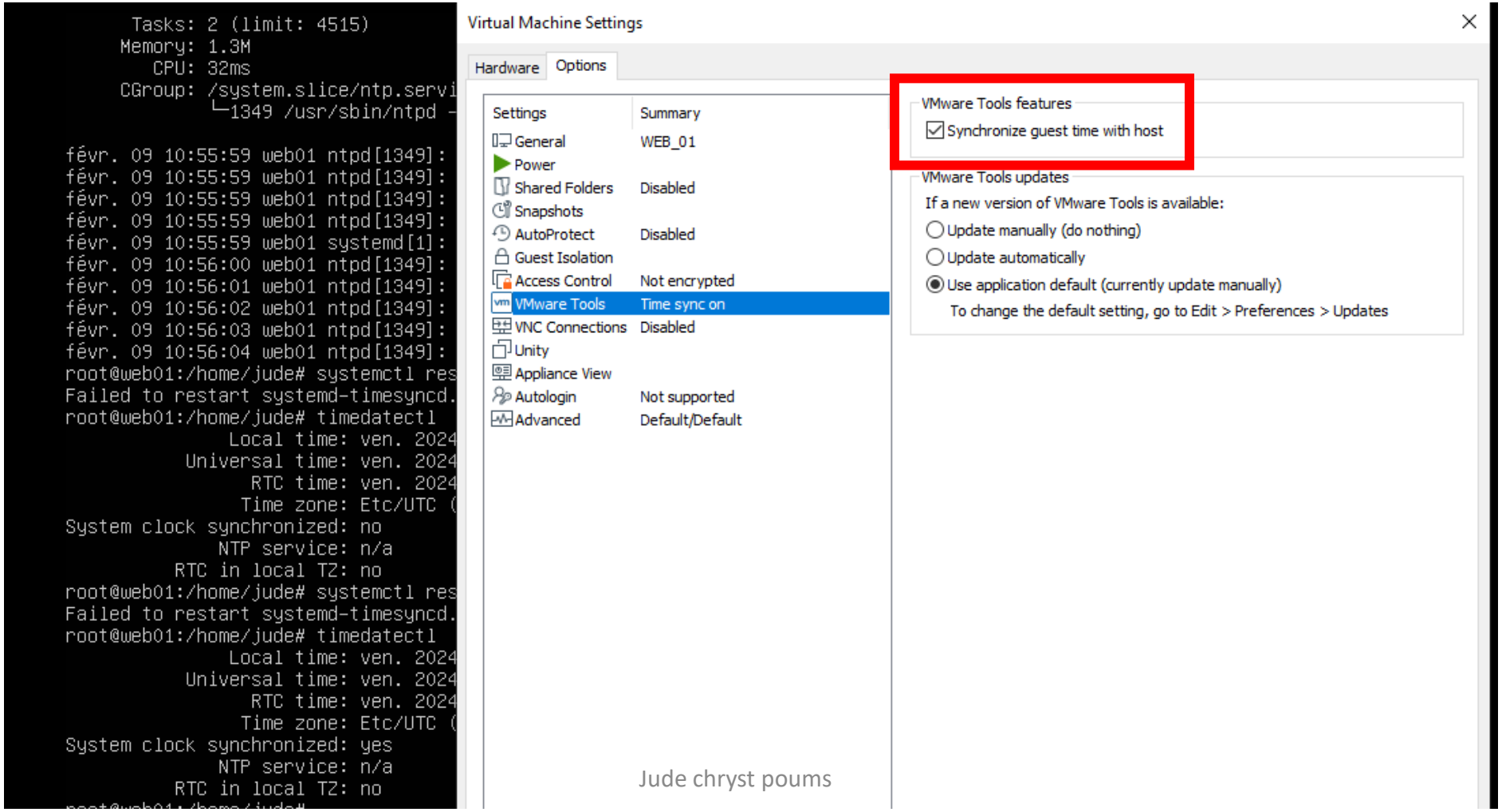

Connexions réseau
Panneau de configuration › Réseau et Internet › Connexions réseau
Rechercher dans : Connexions r...
Fichier Edition Affichage Avancé Outils
Organiser
Désactiver ce périphérique réseau
Diagnostiquer cette connexion
Renommer cette connexion
Afficher le statut de cette connexion
Ethernet
Câble réseau non connecté
Realtek PCIe GbE Family Controller
VMware Network Adapter VMnet1
Activé
VMware Virtual Ethernet Adapter ...
VirtualBox Host-Only Network
Activé
VirtualBox Host-Only Ethernet Ad...
État de VMware Network Adapter VMnet8
Détails de connexion réseau
Détails de connexion réseau :
Propriété
Valeur
Suffixe DNS propre à la ...
Description
VMware Virtual Ethernet Adapter for VMn
Adresse physique
00-50-56-C0-00-08
DHCP activé
Adresse IPv4
209.165.200.1
Masque de sous-réseau ...
255.255.255.0
Passerelle par défaut IPv4
Serveur DNS IPv4
Serveur WINS IPv4
NetBIOS sur TCP/IP act...
Oui
Adresse IPv6 locale de li...
fe80::447a:e4ee:3d58:e072%24
Passerelle par défaut IPv6
Serveurs DNS IPv6
fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
Fermer
7 élément(s)
1 élément sélectionné
Pass
16:35
07/02/2024

Depuis n'importe quel réseau ou ordinateur, il est possible d'avoir accès au site d'imie qu'en a télécharger via la machine web et pour avoir accès de la page internet

Tapez l'adresse ip du WAN sur la barre de recherche : 209.165.200.1



Activer la synchronisation du système clock: Yes



 # systemctl restart systemd-timesyncd
 # timedatectl

```
root@web01:/home/jude# systemctl restart systemd-timesyncd
Failed to restart systemd-timesyncd.service: Unit systemd-timesyncd.service is masked.
root@web01:/home/jude# timedatectl
               Local time: ven. 2024-02-09 10:56:24 UTC
           Universal time: ven. 2024-02-09 10:56:24 UTC
                 RTC time: ven. 2024-02-09 10:56:24
                Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: no
              NTP service: n/a
          RTC in local TZ: no
root@web01:/home/jude# systemctl restart systemd-timesyncd
Failed to restart systemd-timesyncd.service: Unit systemd-timesyncd.service is masked.
root@web01:/home/jude# timedatectl
               Local time: ven. 2024-02-09 11:38:45 UTC
           Universal time: ven. 2024-02-09 11:38:45 UTC
                 RTC time: ven. 2024-02-09 11:38:45
                Time zone: Etc/UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: n/a
          RTC in local TZ: no
```