

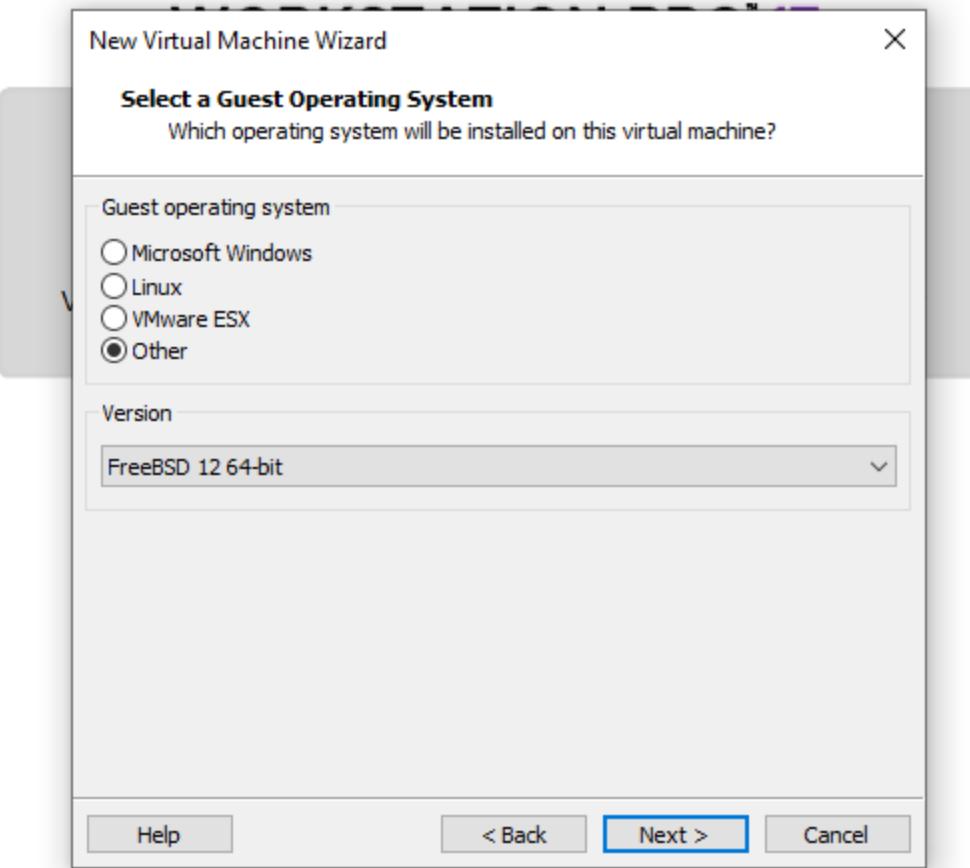


FIREWALL & PFSENSE

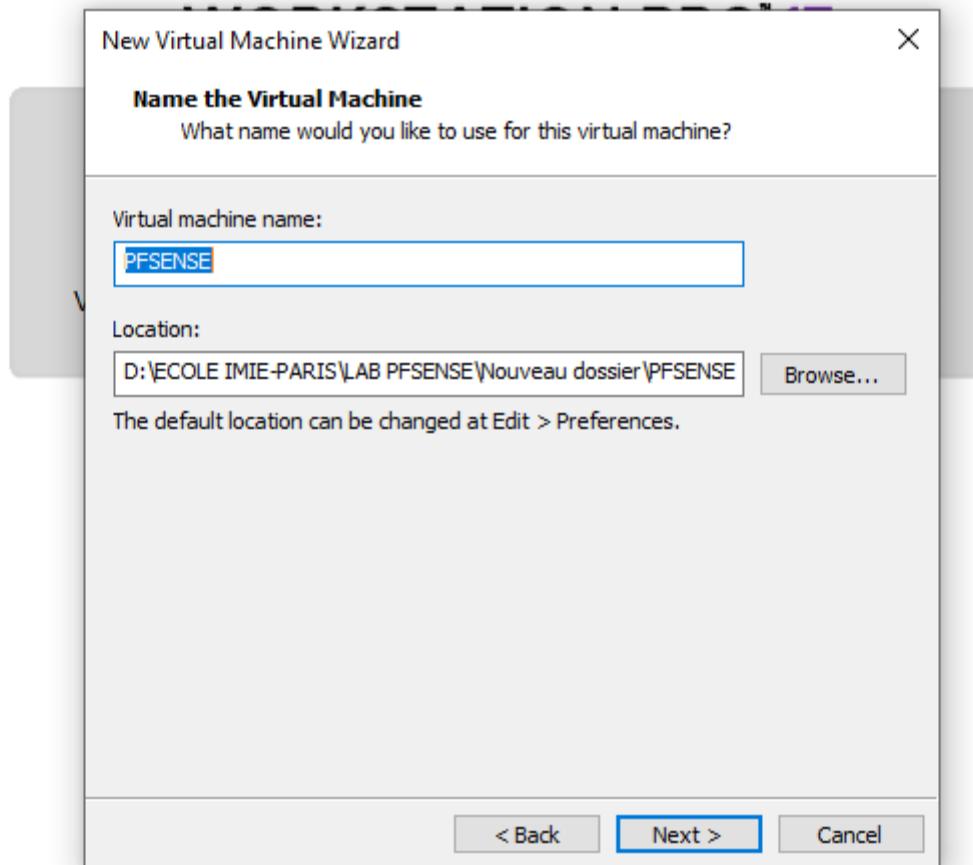
**MACHINE PFSENSE / CLIENT WINDOWS 10
/ UBUNTU SERVER**

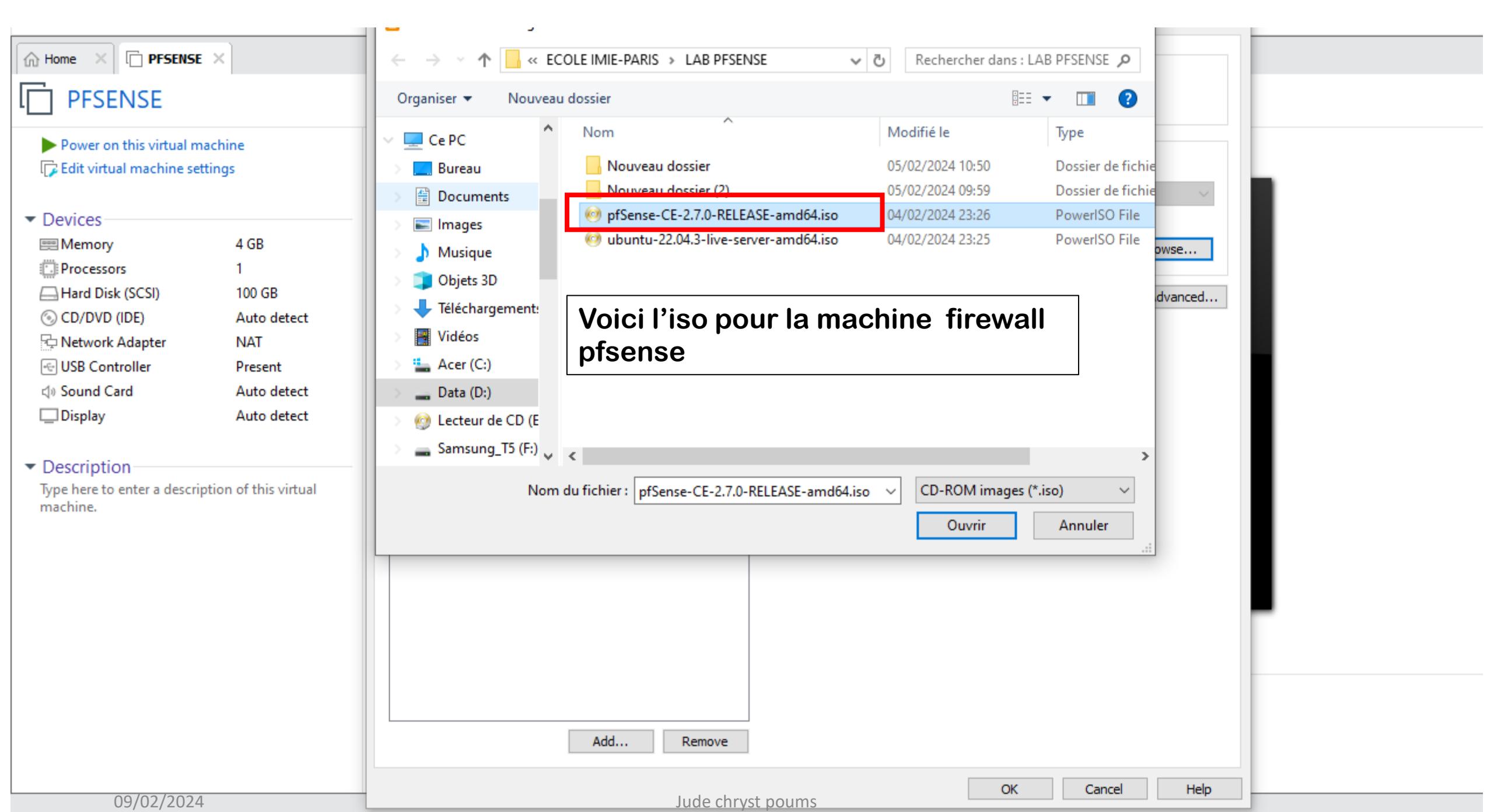
Etape 1: Création de la machine virtuelle Firewall pfSense

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





Virtual machine settings

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

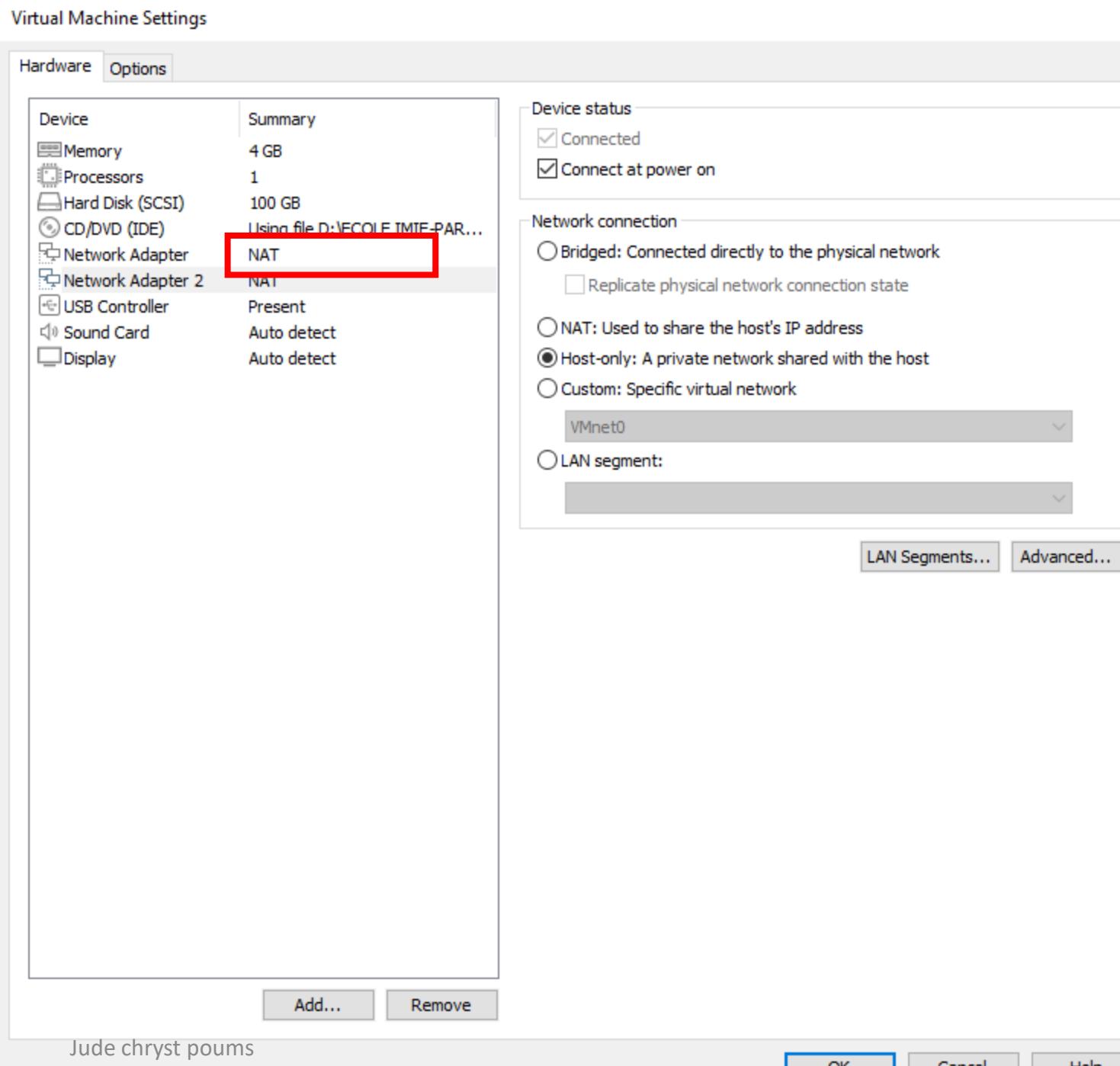
1^{er} carte : mettre la première carte en NAT

2^{eme} carte : mettre la deuxième carte en LAN

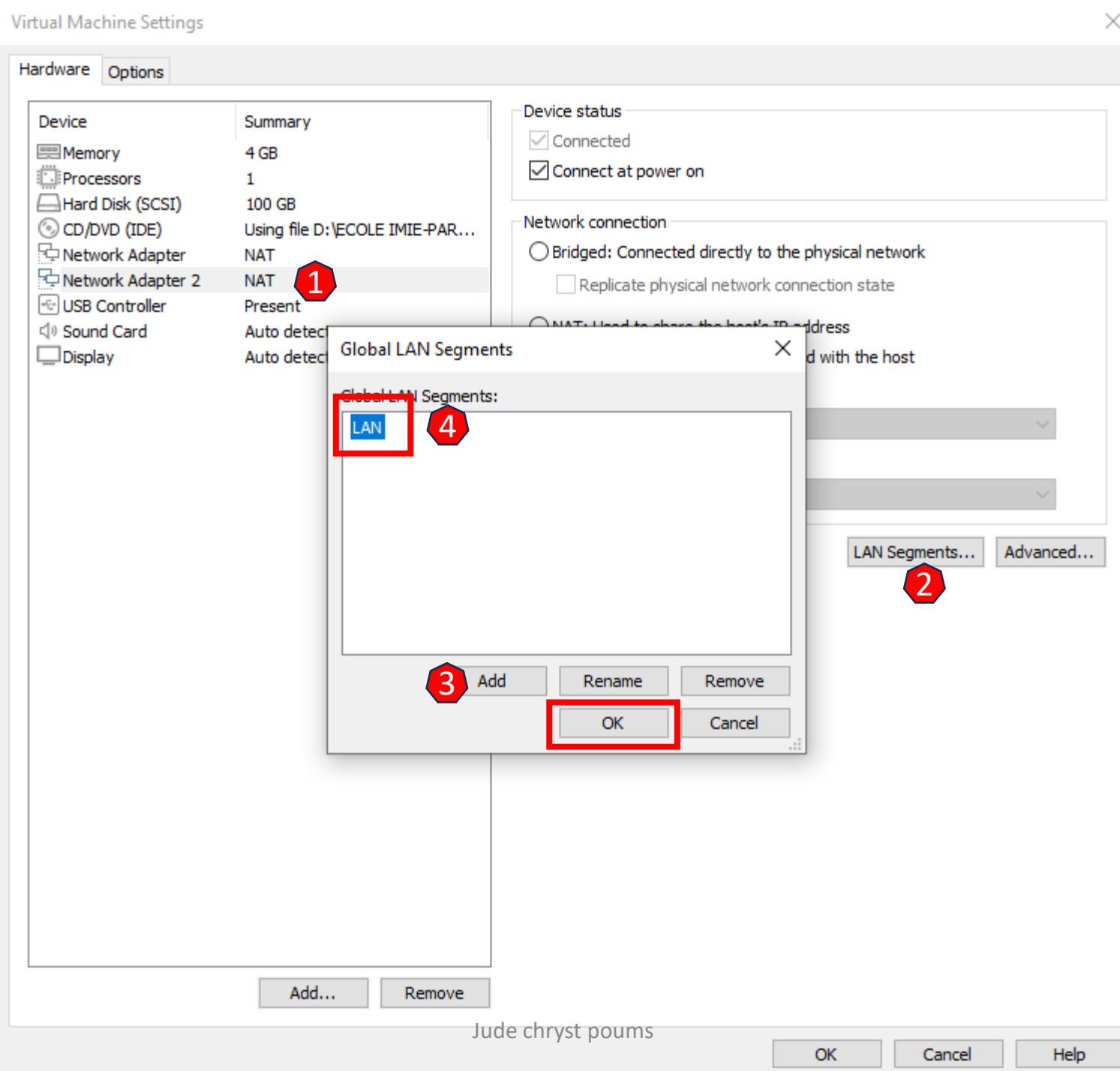
Pour ce faire, il faudrait sélectionner LAN segment, cliquer sur LAN segments... puis add pour créer un réseau local qui sera non lue par l'ordinateur physique.

3^e carte : mettre la deuxième carte en DMZ

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



1





Virtual Machine Settings

X

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

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...Add...Remove

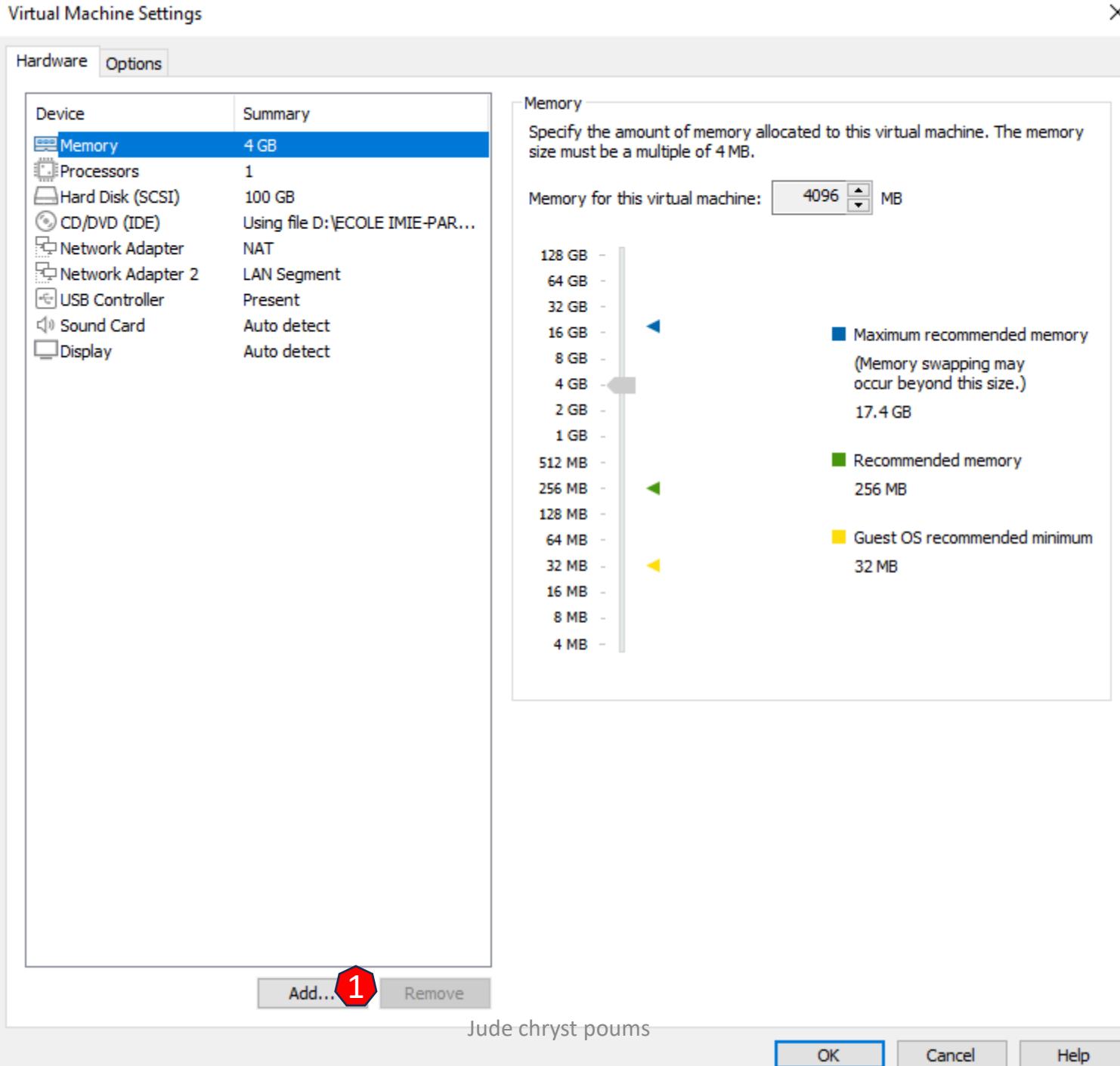
Jude chryst poums

OK

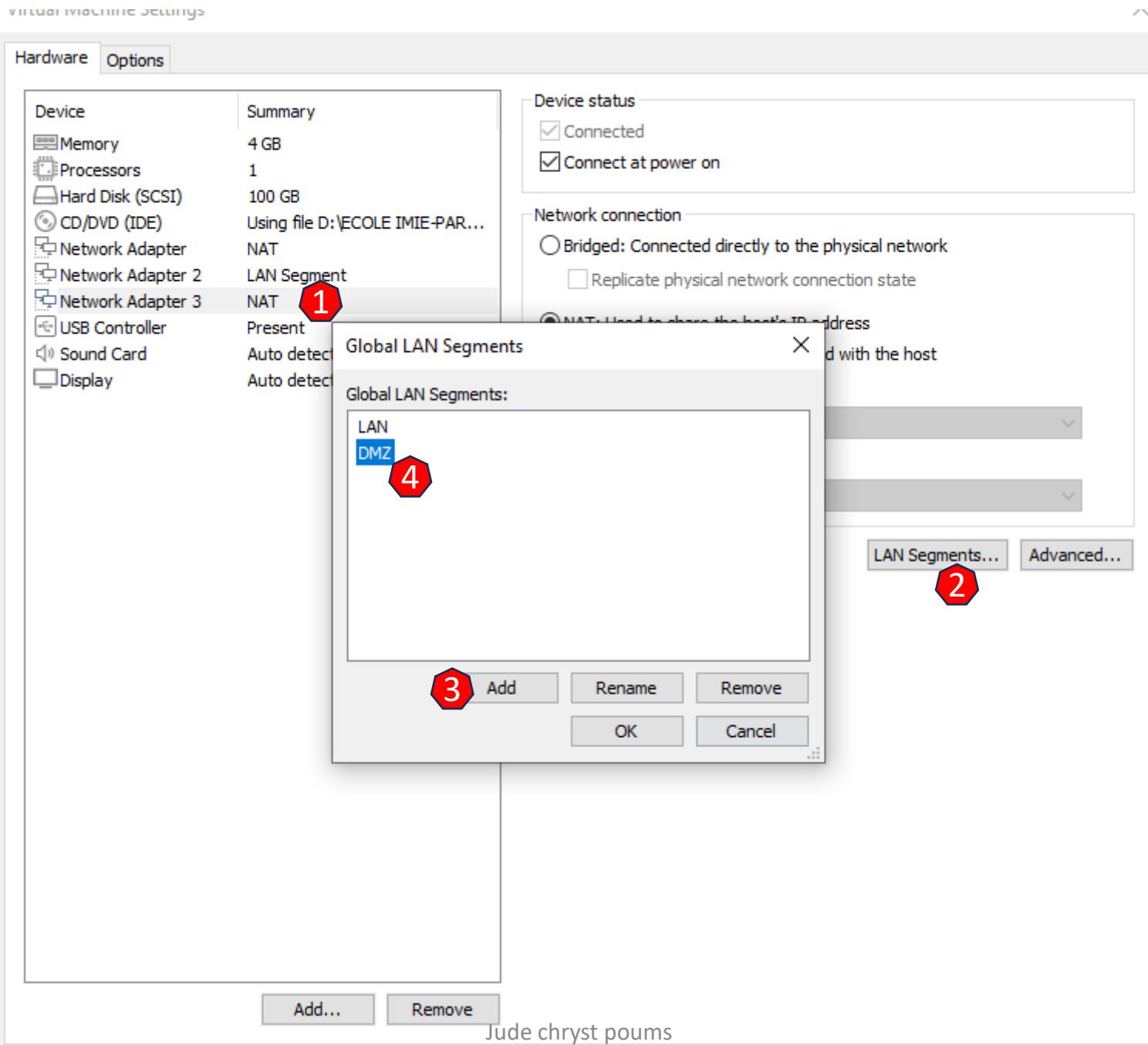
Cancel

Help

2



2





Virtual Machine Settings

X

Hardware Options

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

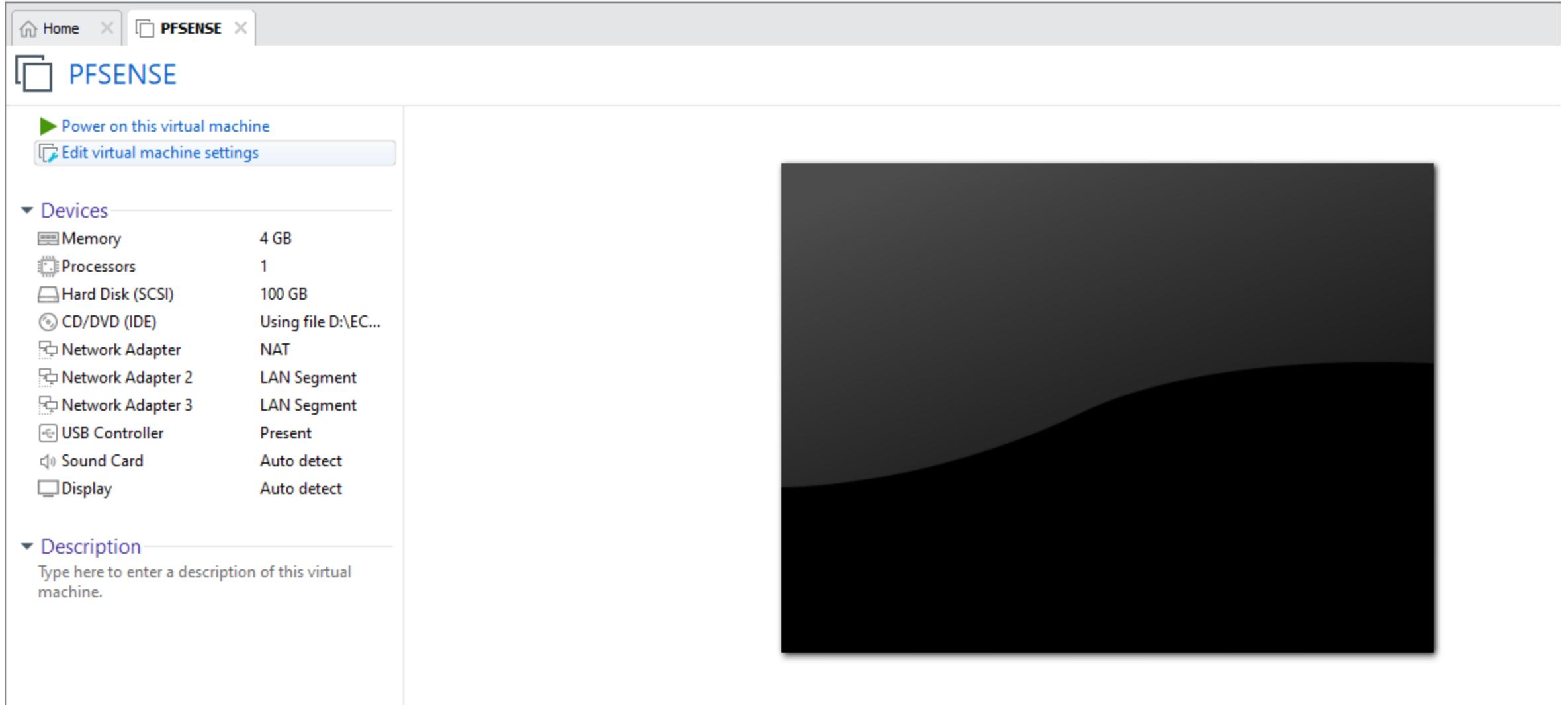
VMnet0

- LAN segment:

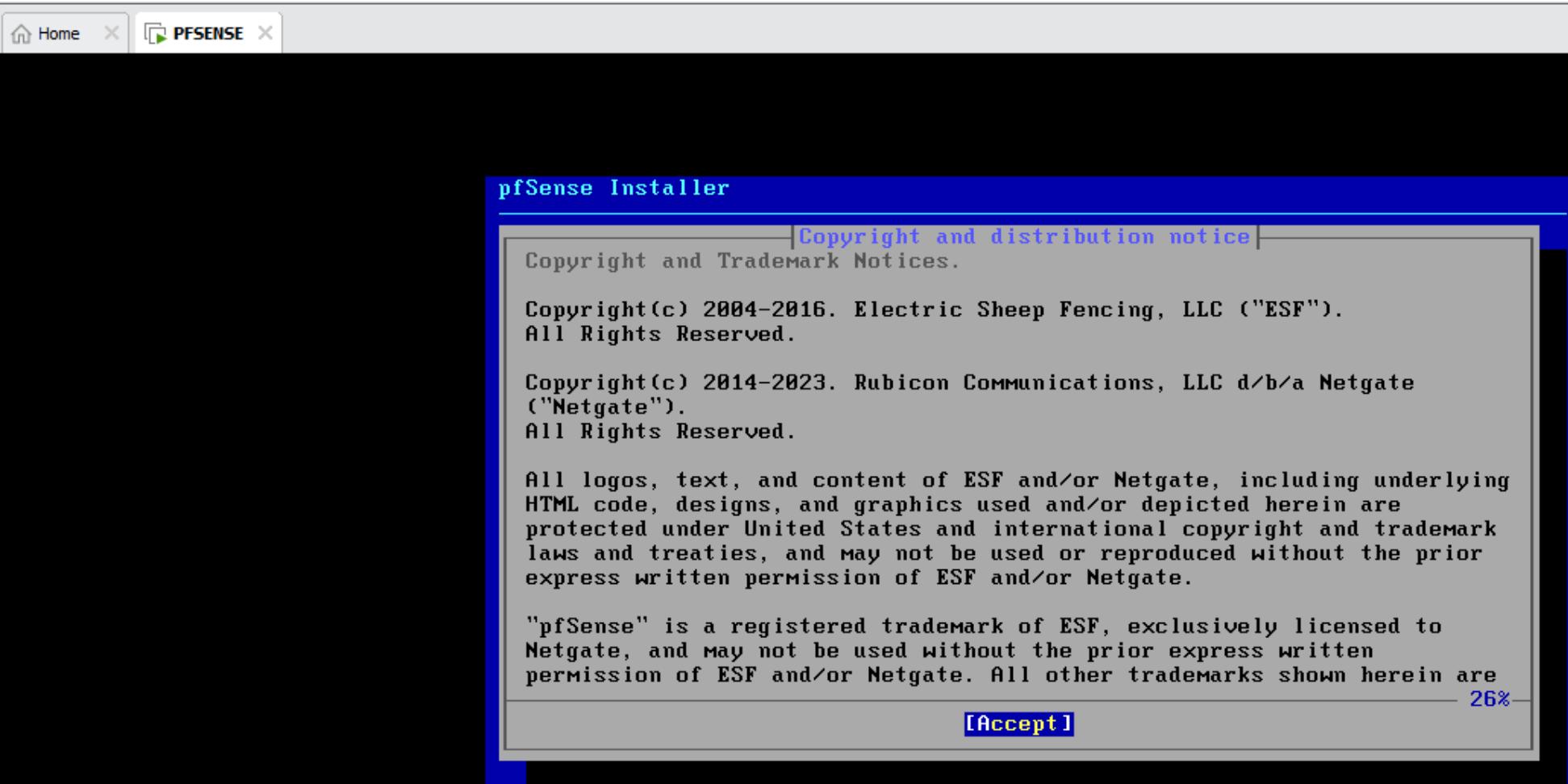
DMZ

LAN Segments... Advanced...Add...Remove

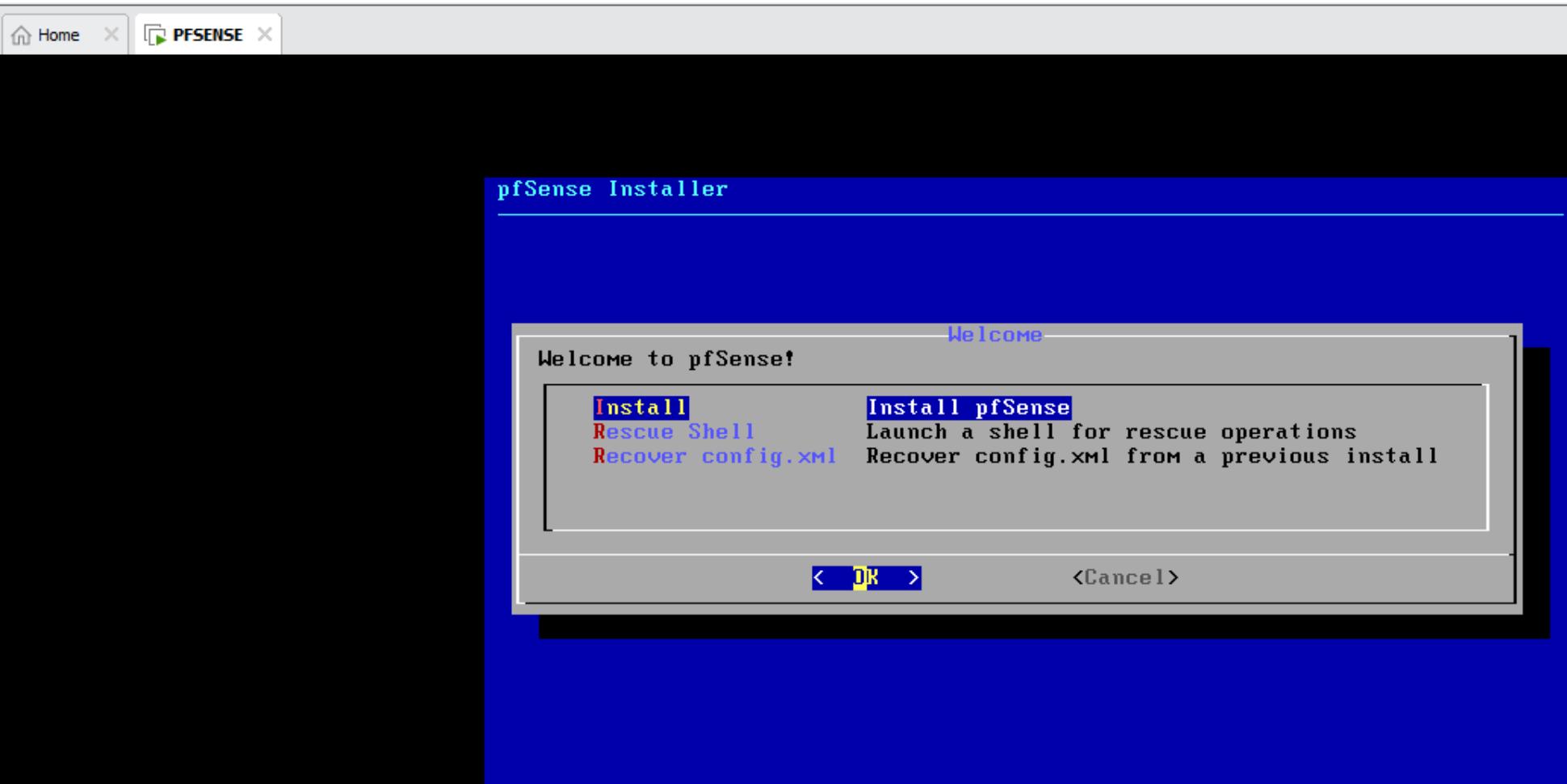
LANCER LA MACHINE PFSENSE



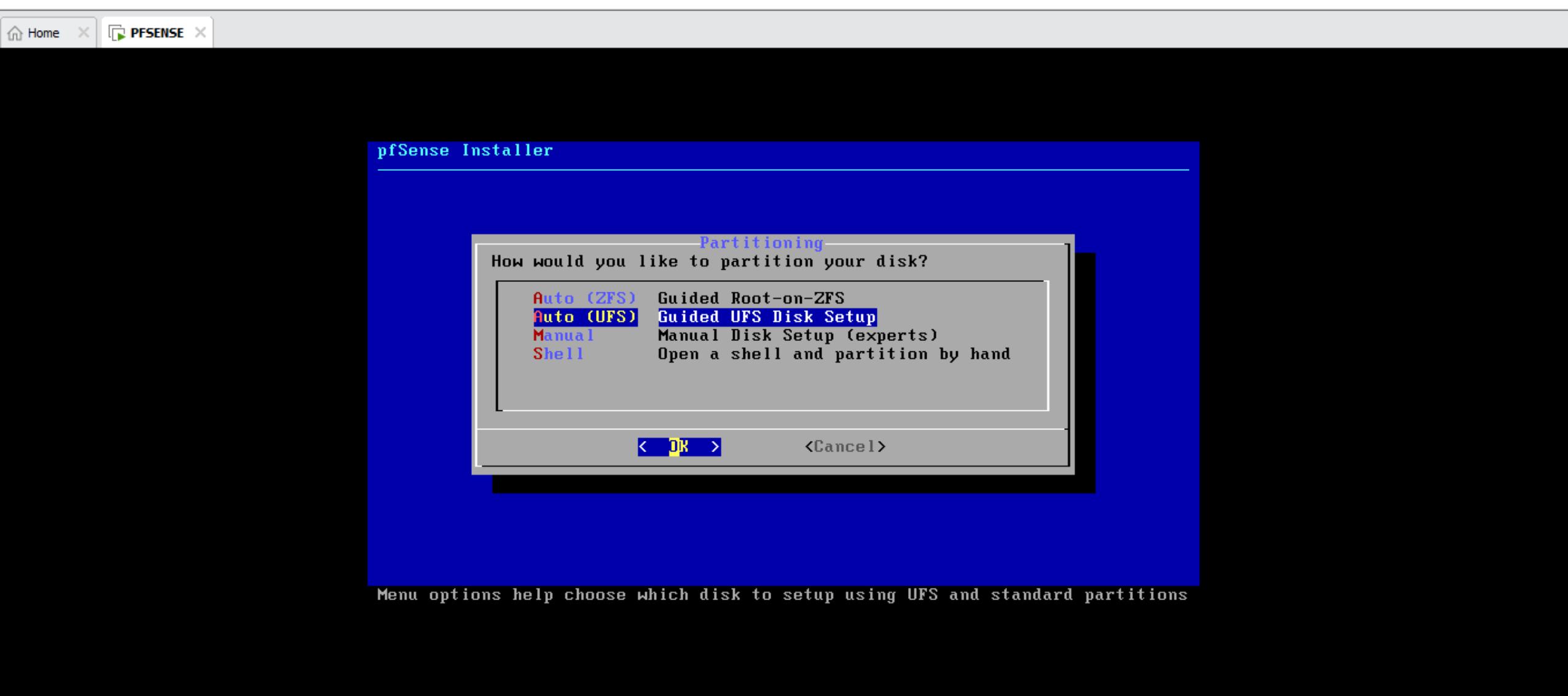
✓ Accepter l'installation pfSense



✓ Choisir install pfSense



✓ Choisir Auto (UFS) Guided UFS Disk Setup

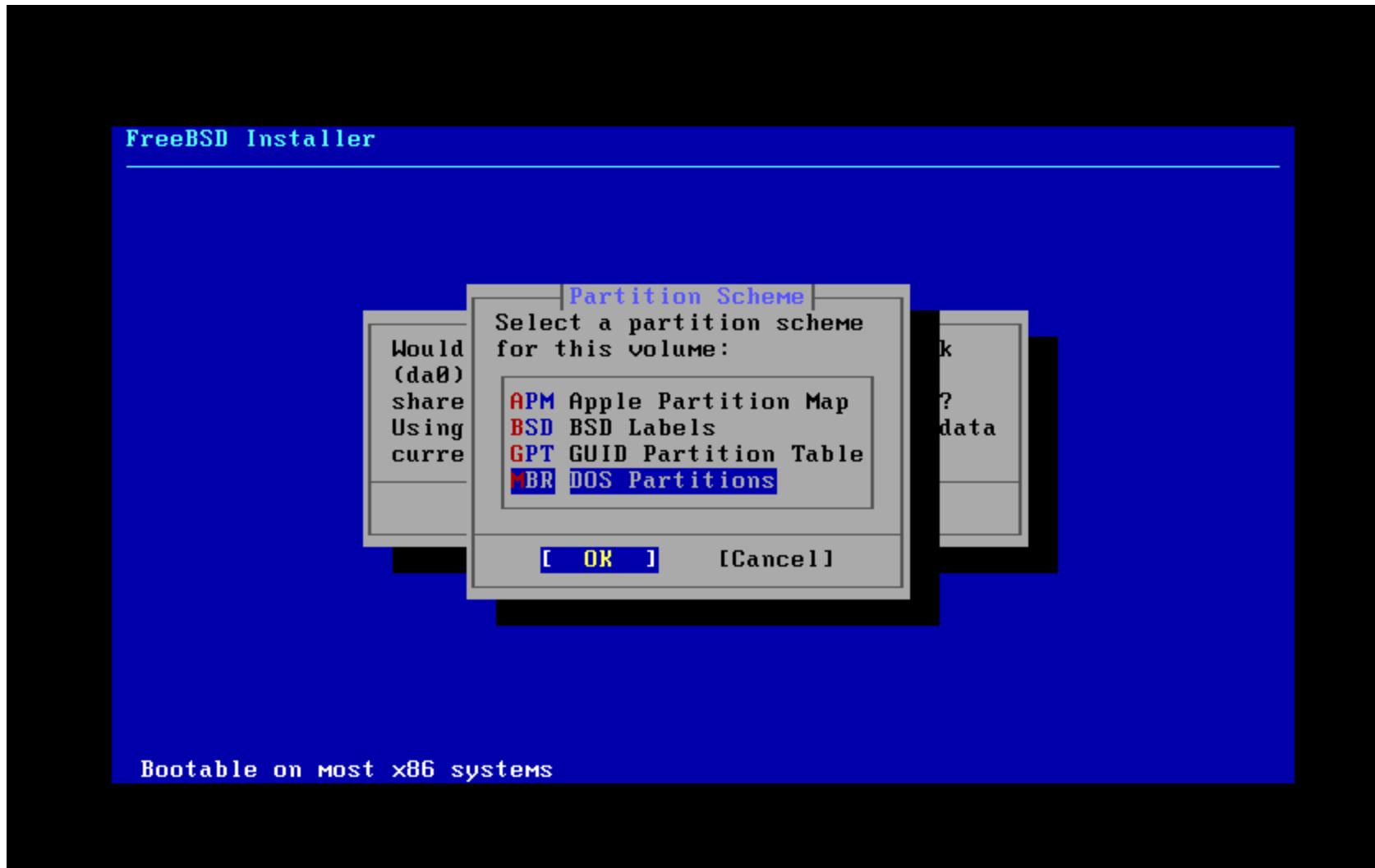


✓ Choisir Entire Disk

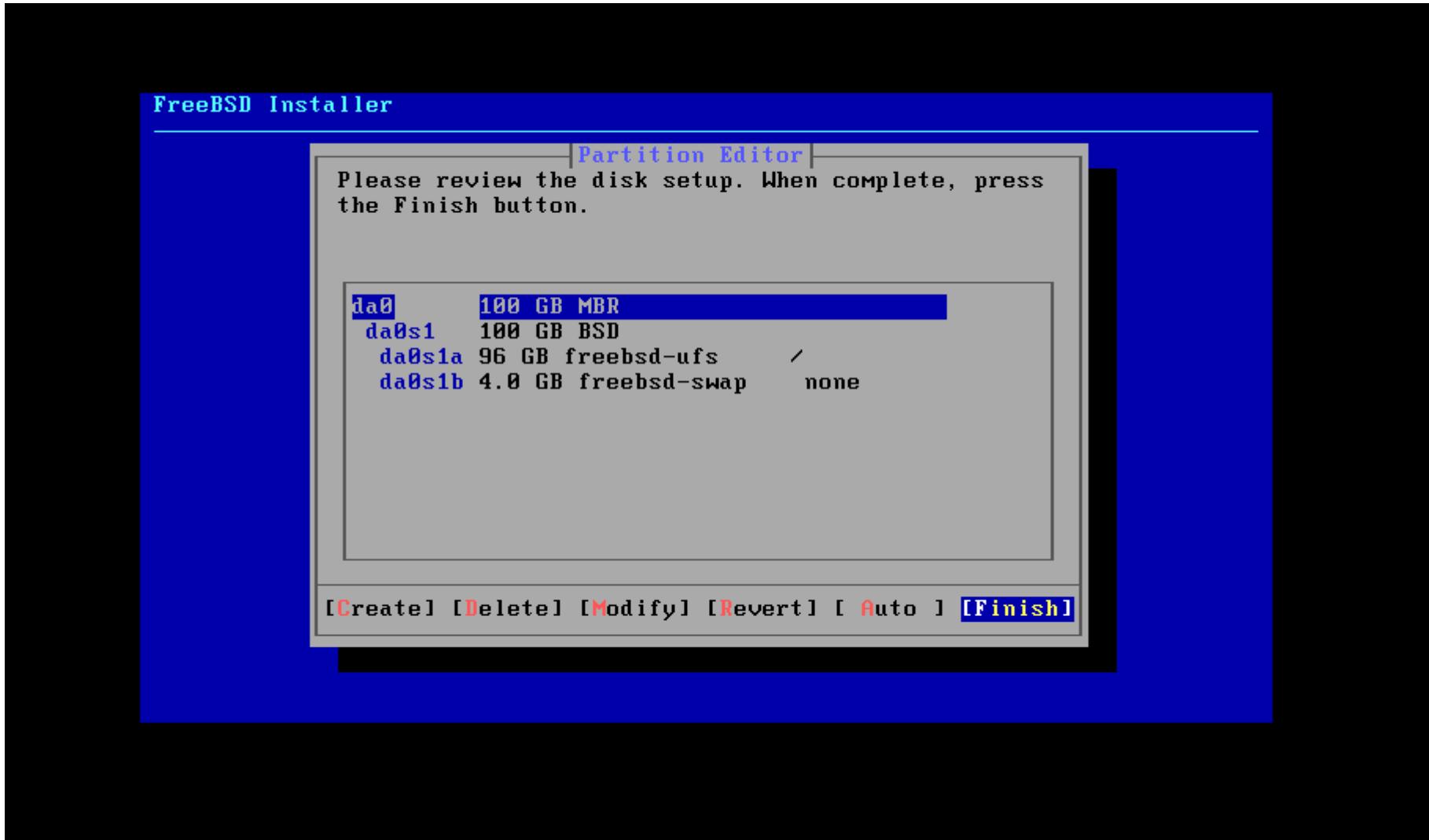


✓ Choisir BR DOS Partitions

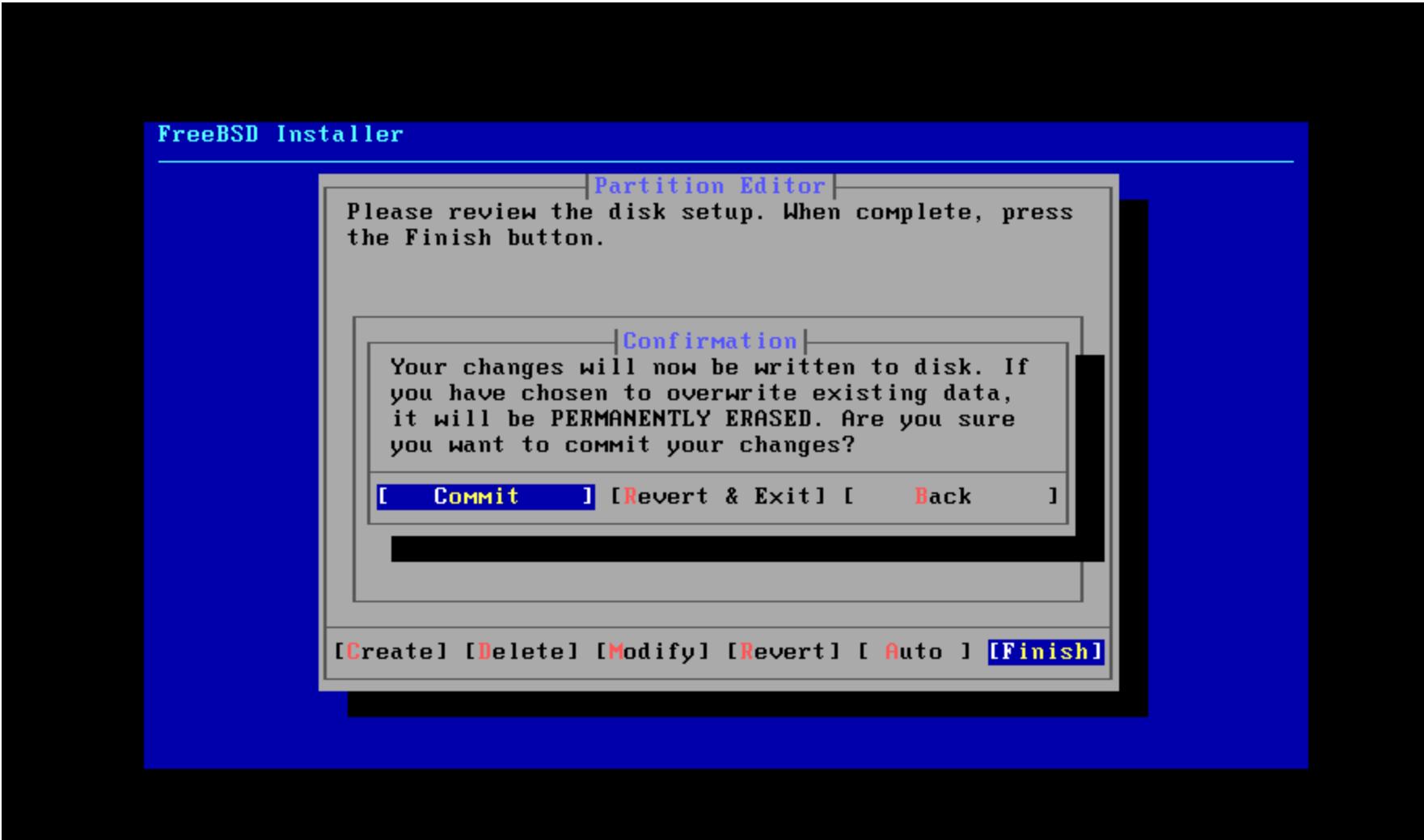
OK



✓ Choisir (Finish)

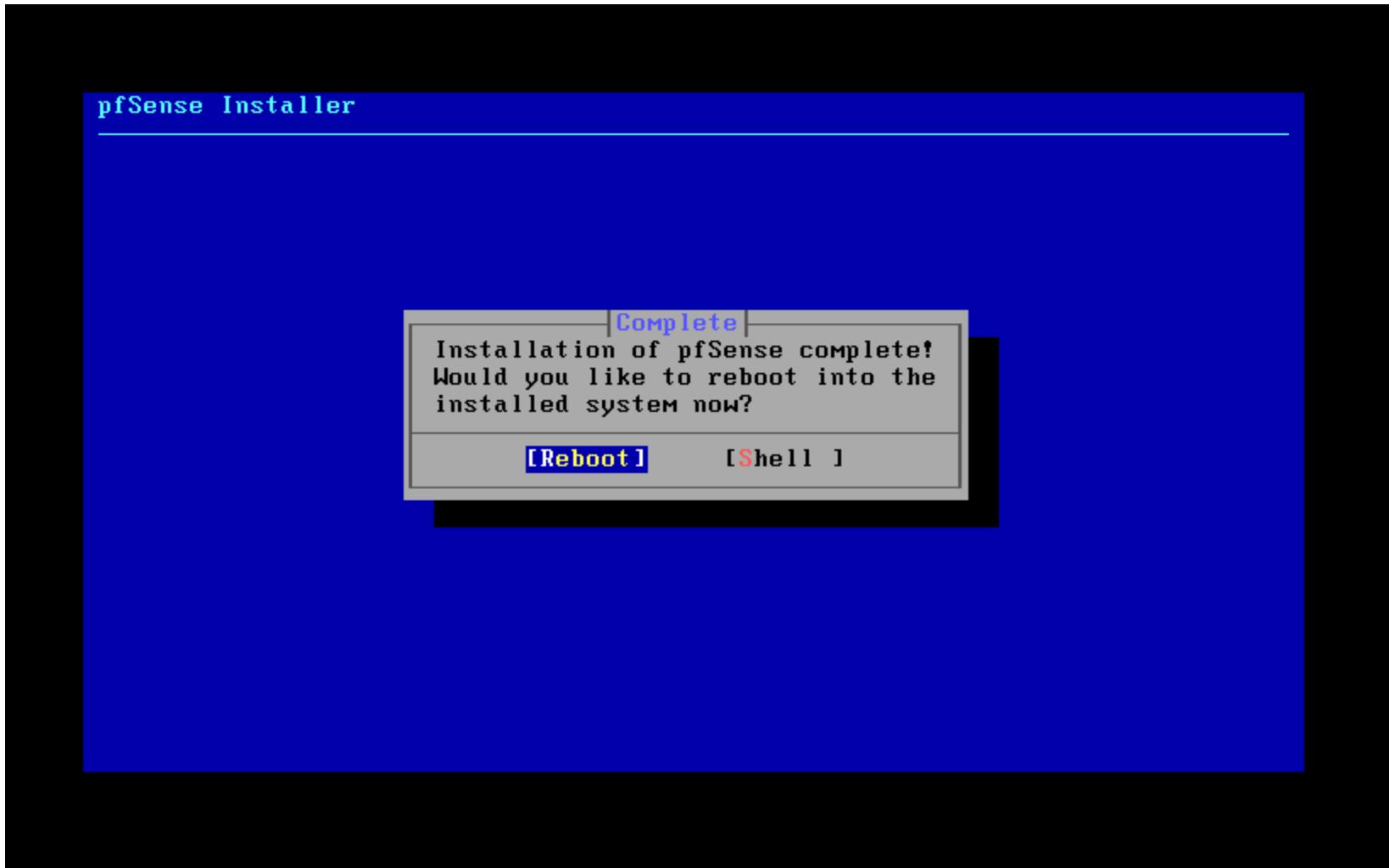


✓ Confirmation [Commit]



✓ 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

```
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: █
```

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)

```
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

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2■
```

- ✓ 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

```
6) Halt system          15) Restore recent configuration
7) Ping host            16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

- ✓ IPv6 DHCP6 (y/n) n
- ✓ A cet étape il faudrait accepter l'attribution DHCP LAN (y/n) y
Parce que à notre niveau nous voulons que notre réseau LAN puisse attribuer automatiquement l'adresse ip aux machines qui seront dans le même réseau

```
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.254
Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) y█
```

- ✓ 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

```
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.10.50
Enter the end address of the IPv4 client address range: 192.168.10.150
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
    Reloading filter...
    Reloading routing configuration...
    DHCPD...

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.■
```



```
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 ***
```

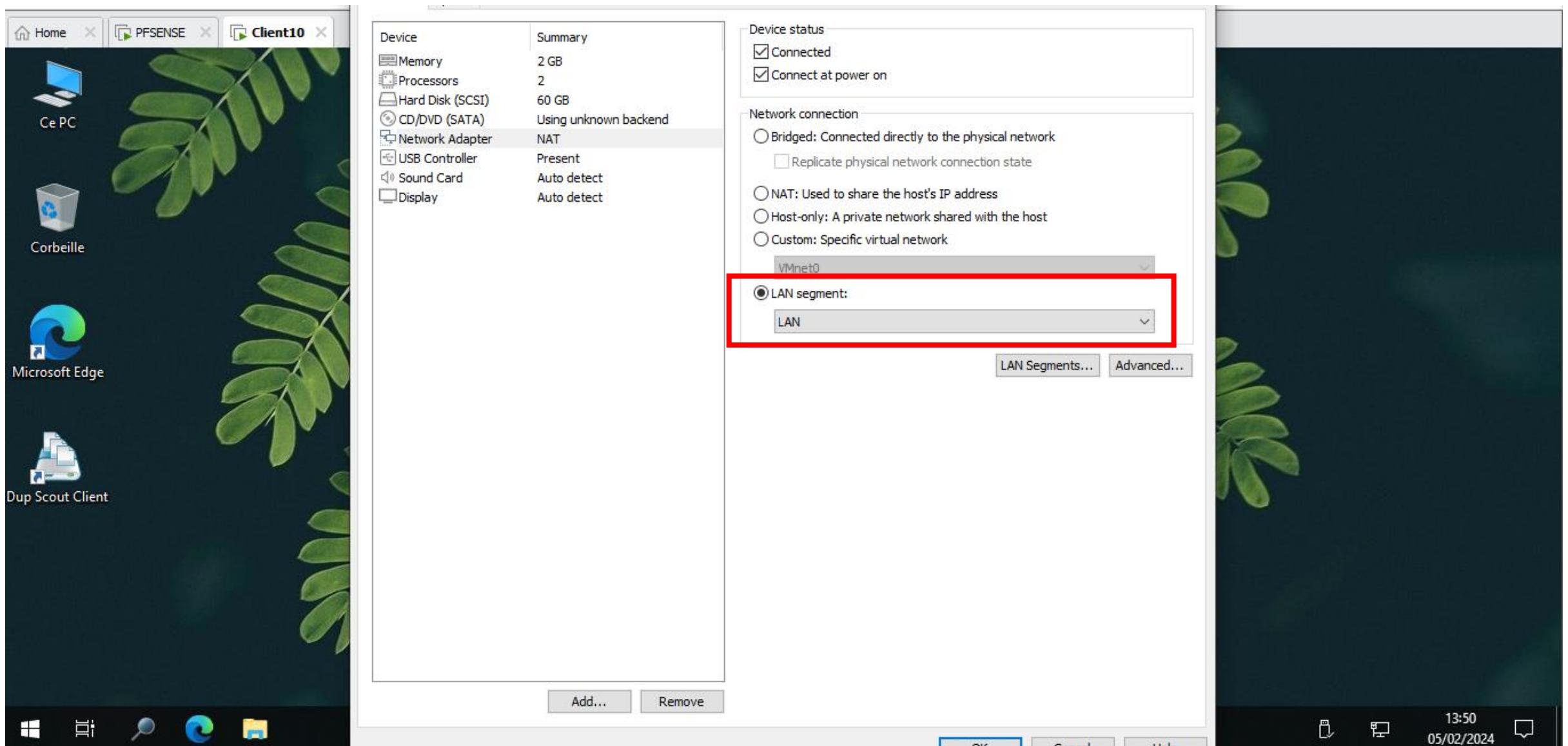
```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.8.128/24  
LAN (lan)      -> em1      -> v4: 192.168.10.254/24
```

- 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

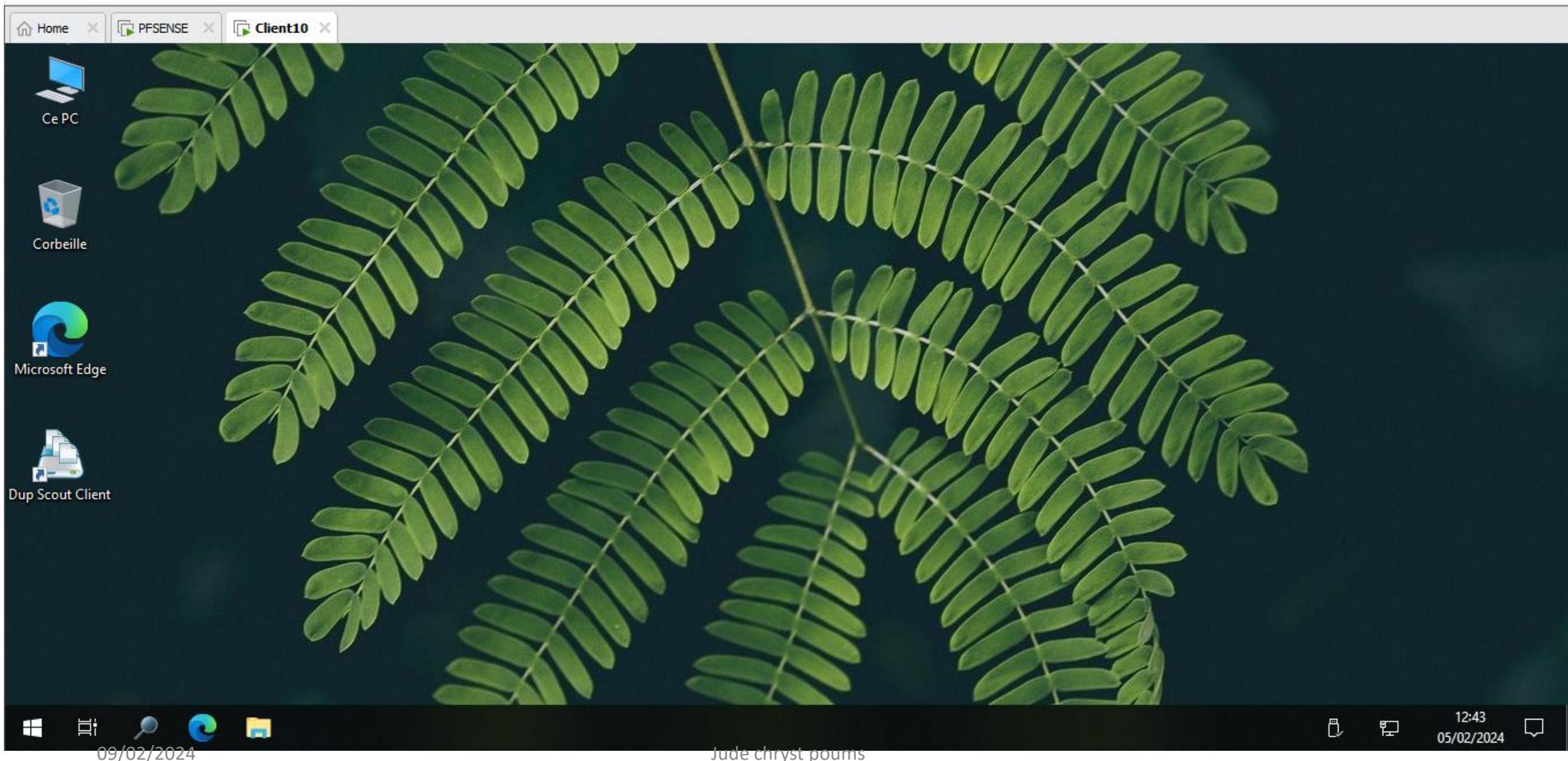
```
Enter an option: █
```

MACHINE CLIENTE WINDOWS 10 PFSENSE INTERFACE WEB

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

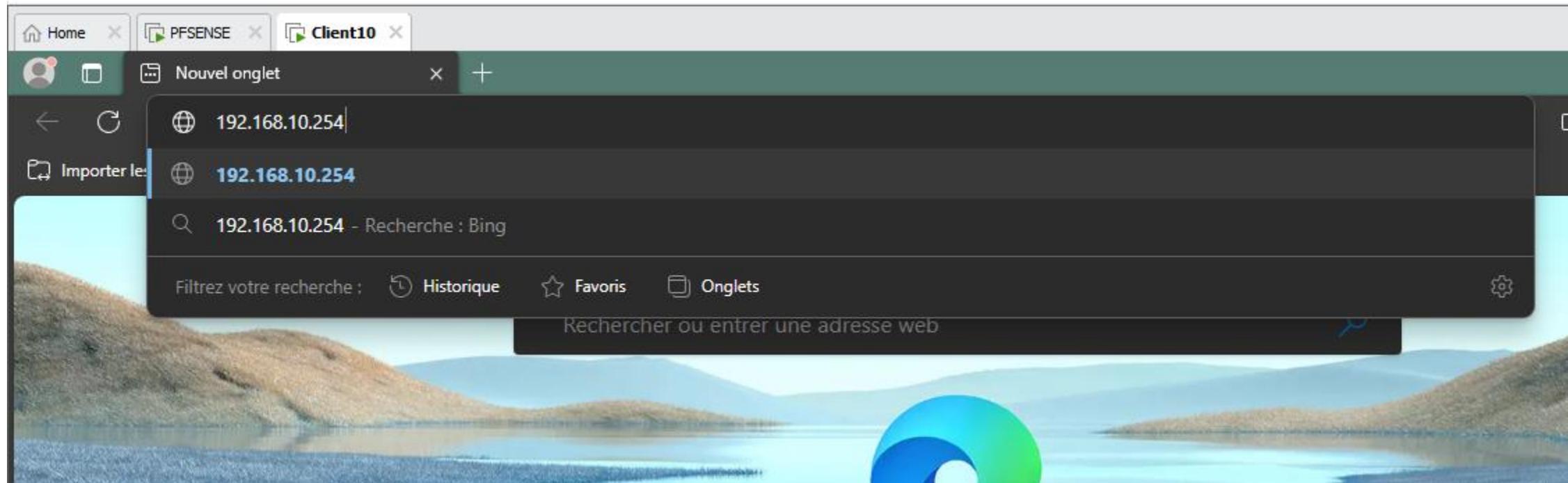


- ✓ Démarrer une machine windows 10
- ✓ Vérifier on adresse ip

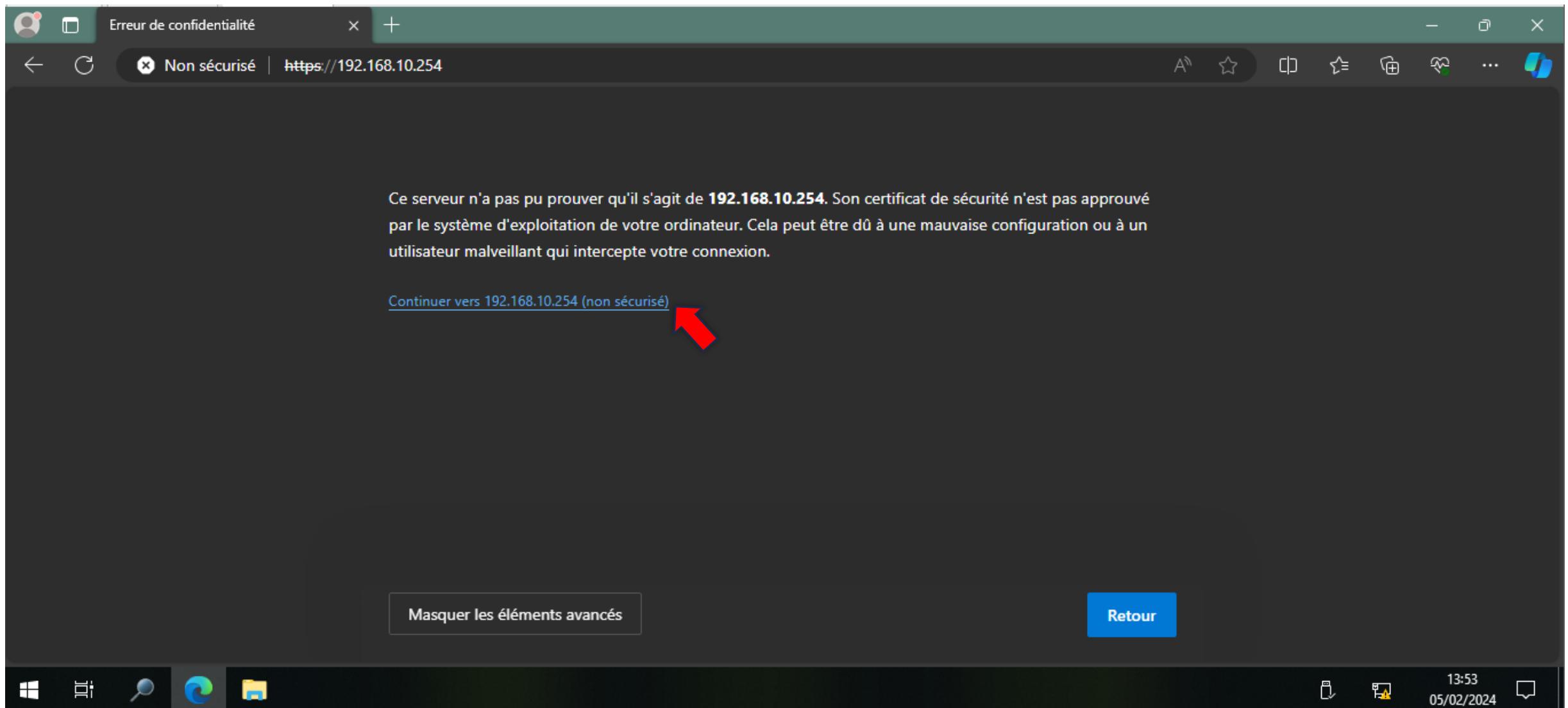


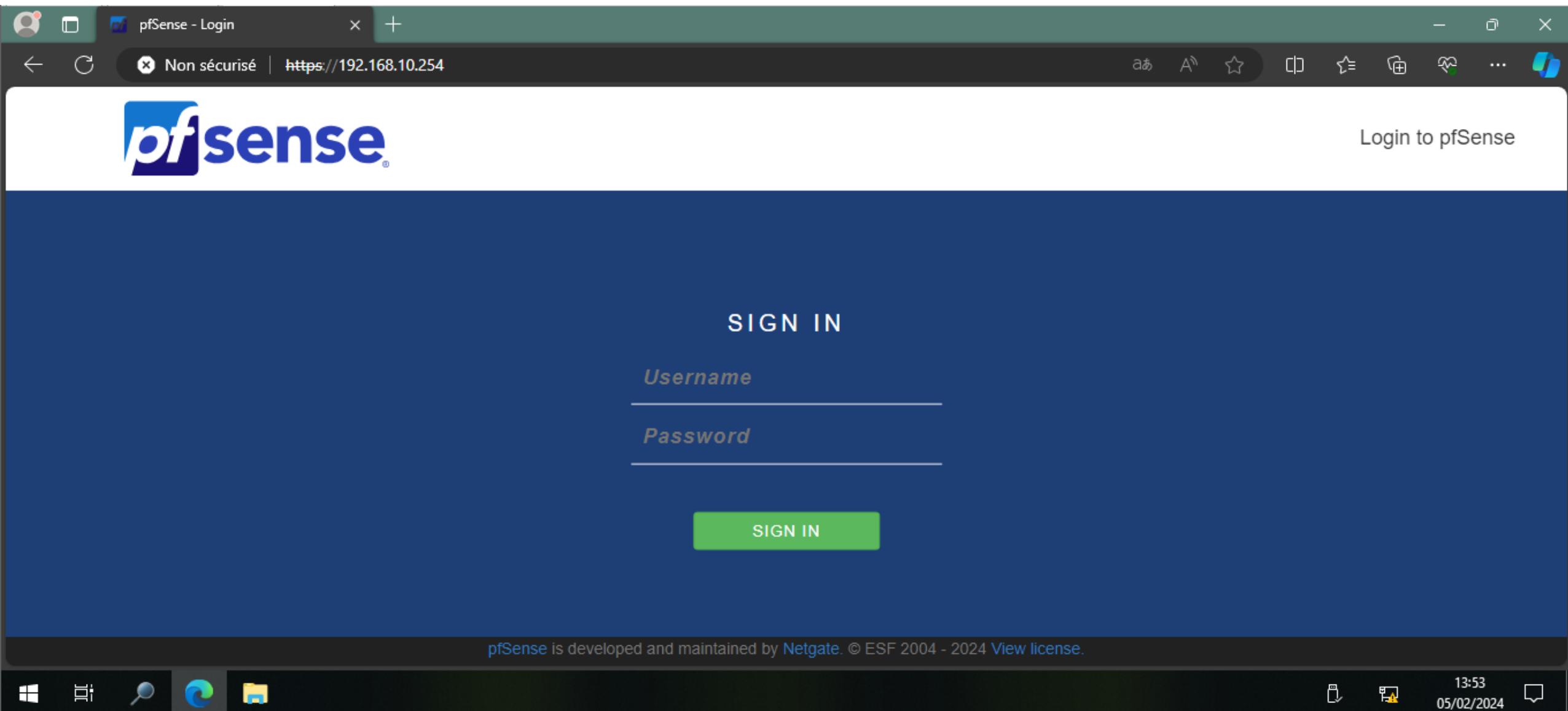
✓ Etape 2 : Connexion au firewall pfSense pour sa configuration

Dans la barre de recherche tapez : 192.168.10.254



✓ Cliquer sur continuer vers 192.168.10.254 (non sécurisé)







Login to pfSe

SIGN IN

admin

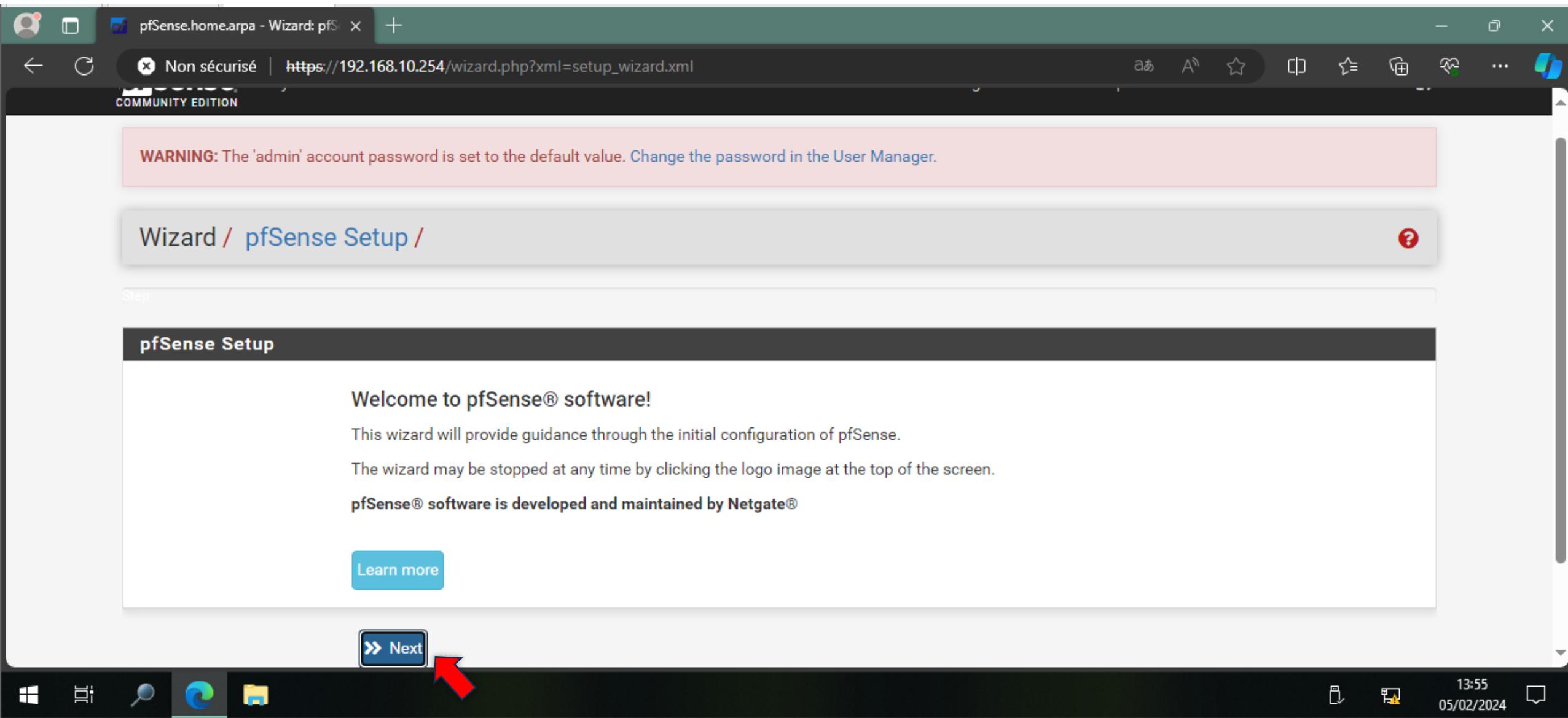
pfsense

✓ Sur pfSense la connexion de la session d'ouverture par défaut est
Username : **admin**
Mot de passe : **pfsense**

SIGN IN



pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).



pfSense.home.arpa - Wizard: pfSense

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

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

Domain: home.arpa
Domain name for the firewall.

**Nom du firewall :
pfsense**

**Ici mettre un domaine
par exemple tssr.lan**

09/02/2024 Jude chryst poums 13:57 05/02/2024

pfSense.home.arpa - Wizard: pfSense

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



pfSense.home.arpa - Wizard: pfS X +

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

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

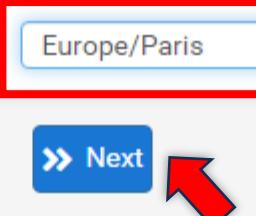
Time Server Information

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



Windows Taskbar icons: File Explorer, File History, Search, Start, Task View, Taskbar settings, Taskbar search, Taskbar settings, Taskbar search.

pfSense.home.arpa - Wizard: pfS X +

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

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

Windows File Explorer Search File

pfSense.home.arpa - Wizard: pfsense

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 timeout is used to detect 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, 192.168/16) and loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space.

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 private IP addresses that 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: pfSense

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

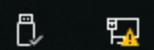
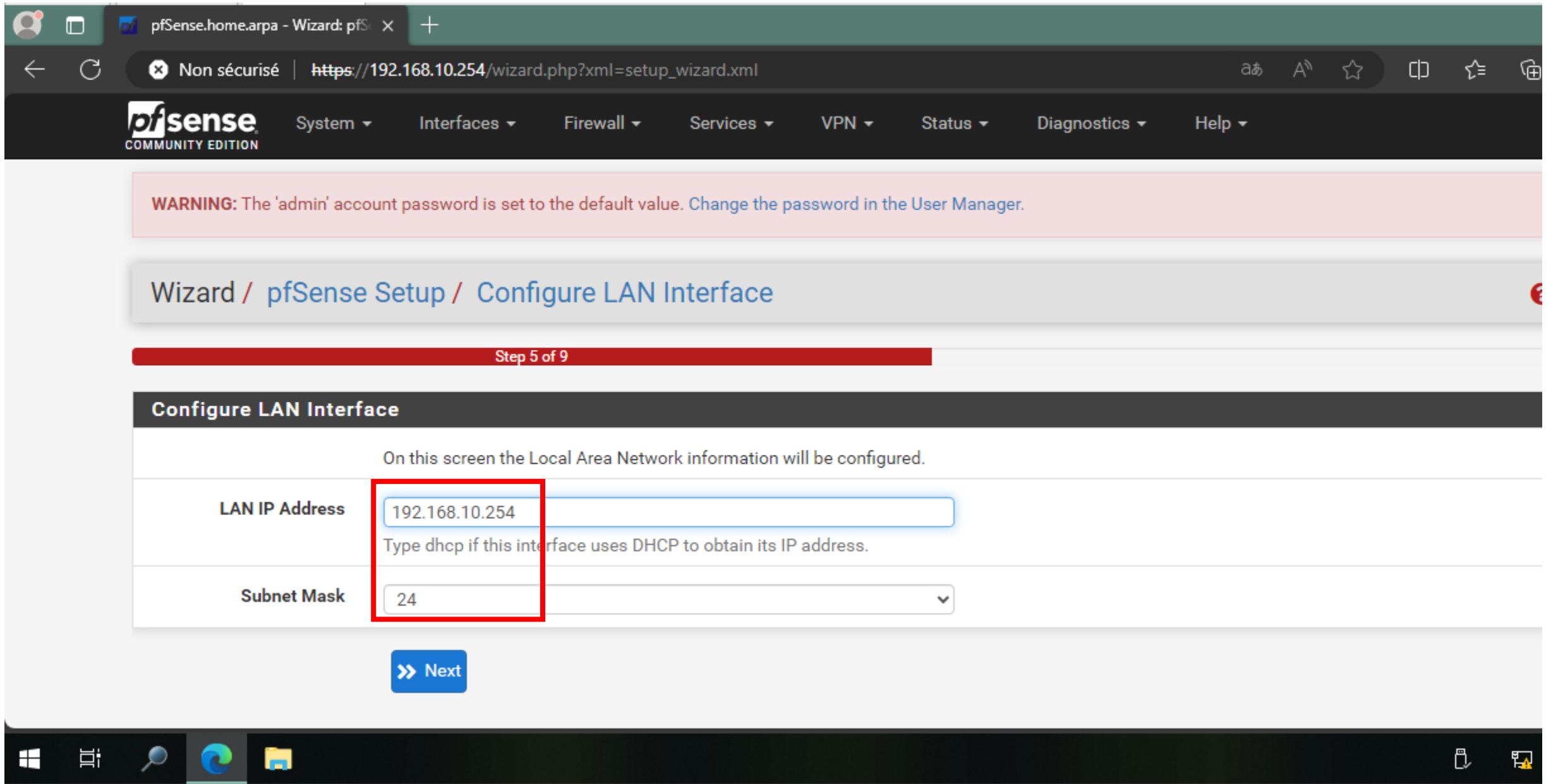
On this screen the Local Area Network information will be configured.

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: pfSense Setup

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

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 X +

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

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

pfSense COMMUNITY EDITION

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](#).

pfSense.home.arpa - Wizard: pfs X +

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](#)

A red arrow points to the "Finish" button at the bottom left of the window.

pfSense.home.arpa - Status: Dash X +

Non sécurisé | https://192.168.10.254

Restricted Rights Legend...

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.

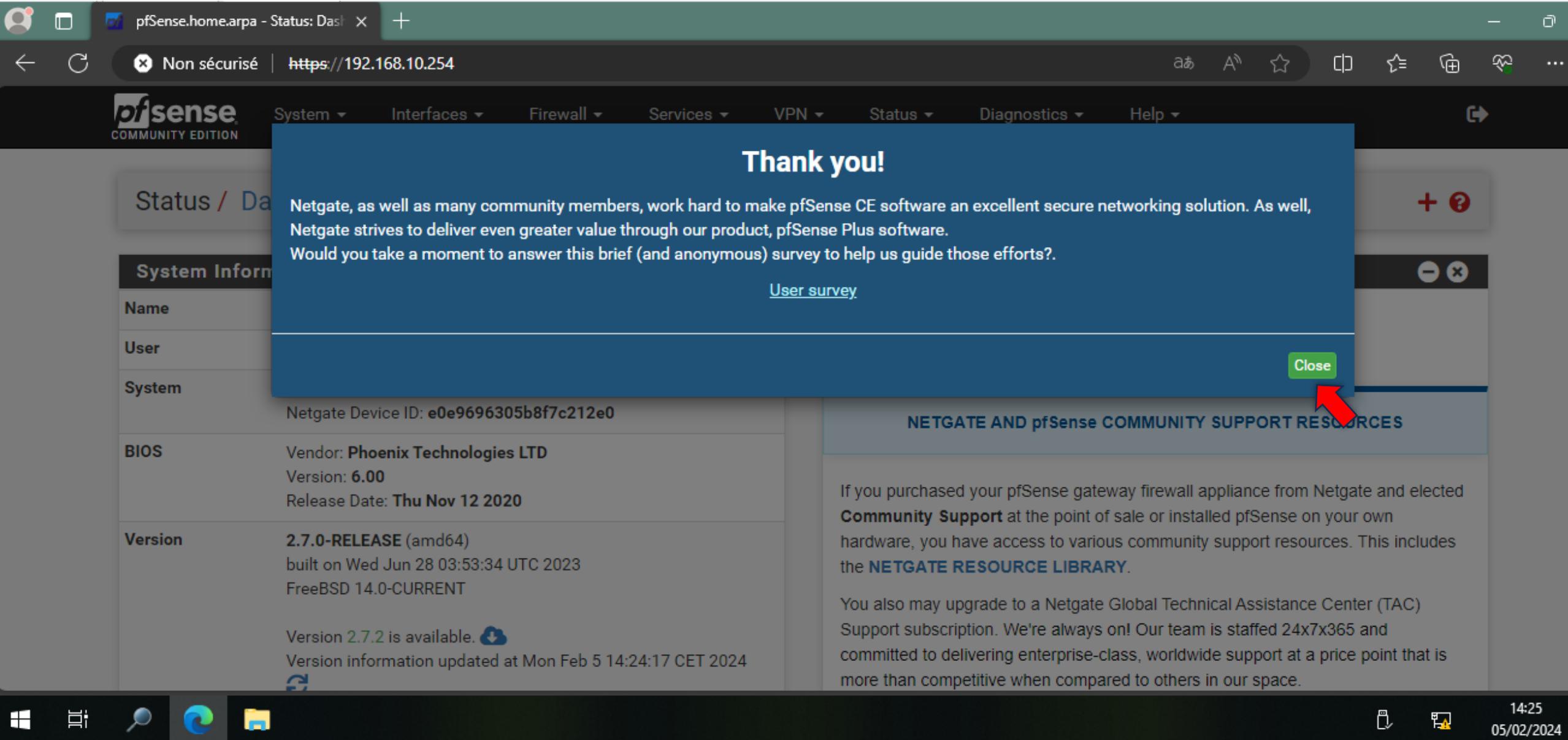
The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export 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

Version information updated at Mon Feb 5 14:24:17 CET 2024

committed to delivering enterprise-class, worldwide support at a 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.

The screenshot shows the pfSense Status Dashboard at <https://192.168.10.254>. The left sidebar contains system statistics:

- Version 2.7.2 is available.
- Version information updated at Mon Feb 5 14:24:17 CET 2024
- CPU Type: Intel(R) Core(TM) i3-7020U CPU @ 2.30GHz
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No
- Hardware crypto: Inactive
- Kernel PTI: Enabled
- MDS Mitigation: Inactive
- Uptime: 02 Hours 23 Minutes 16 Seconds
- Current date/time: Mon Feb 5 14:26:30 CET 2024
- DNS server(s): 127.0.0.1, 8.8.8.8, 1.1.1.1
- Last config change: Mon Feb 5 14:23:27 CET 2024
- State table size: 0% (118/403000) Show states
- MBUF Usage: 0% (2556/1000000)

The right side features a support subscription message from Netgate:

Support Subscription: We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports [here](#).

The bottom section displays the Interfaces configuration:

Interfaces			
	WAN	↑ 1000baseT <full-duplex>	192.168.8.128
	LAN	↑ 1000baseT <full-duplex>	192.168.10.254

The WAN interface row is highlighted with a red border.

Dans setting ensuite virtual network Editor

Changer l'adresse ip et mettre celui d'un réseau public pour la simulation

Subnet IP: 209.165.200.0

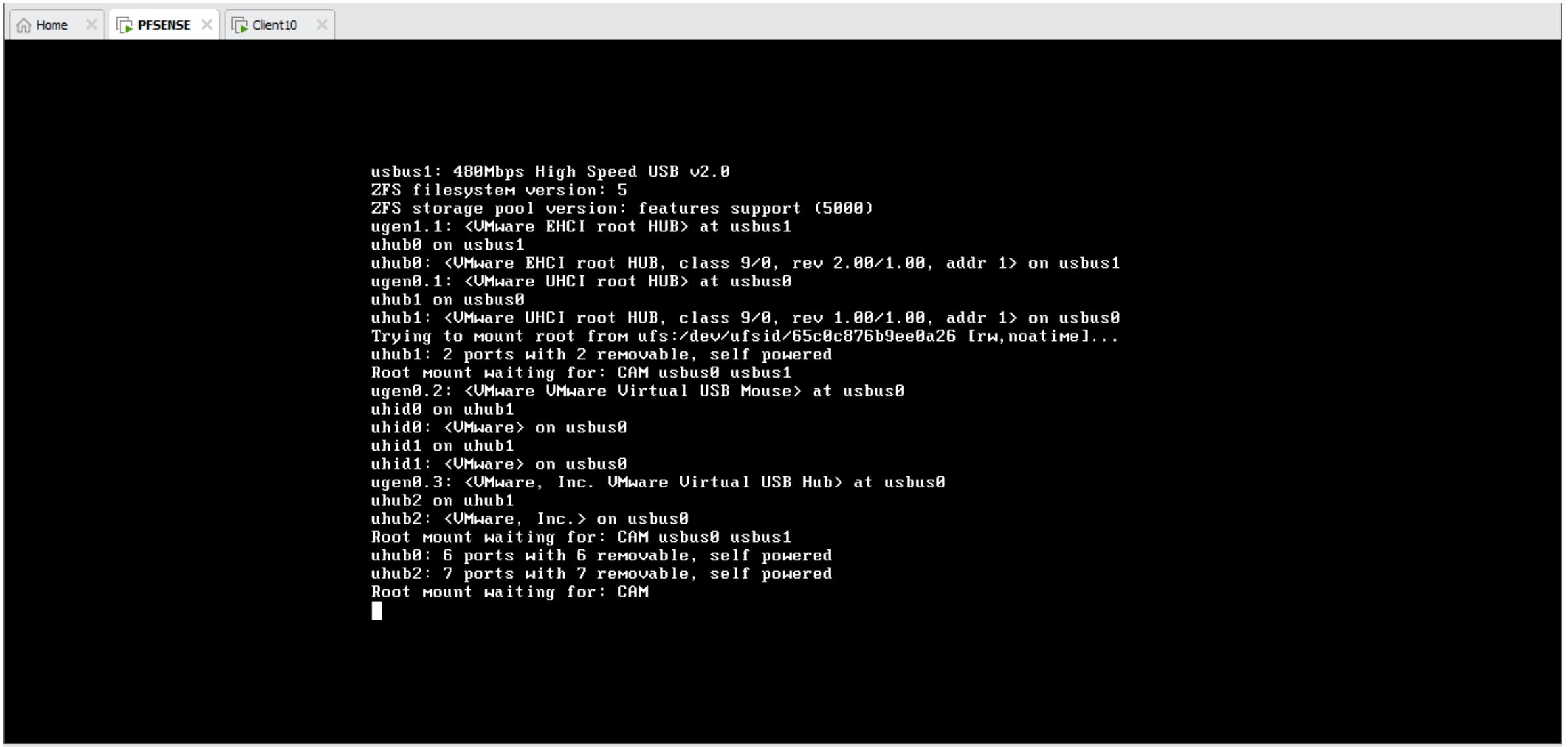
The screenshot shows a Windows desktop environment with several windows open:

- Virtual Network Editor:** A window titled "Virtual Network Editor" displays a table of network interfaces. The row for "VMnet8" is highlighted with a red box. The table columns are: Name, Type, External Connection, Host Connection, DHCP, and Subnet Address. The "VMnet8" row shows: Type "NAT", External Connection "NAT", Host Connection "Connected", DHCP "Enabled", and Subnet Address "209.165.200.0".
- pfSense.home.apra - Status: Dashboard:** A browser window showing pfSense system status. It includes sections for CPU Type (Intel(R) Core(TM) i3-7100U), Hardware crypto (Inactive), Kernel PTI (Enabled), MDS Mitigation (Inactive), Uptime (02 Hours 24 Minutes 21 Seconds), Current date/time (Mon Feb 5 14:27:35 CEST 2024), DNS server(s) (127.0.0.1, 8.8.8.8, 1.1.1.1), Last config change (Mon Feb 5 14:23:27 CEST 2024), State table size (0% (102/403000)), and MBUF Usage (0% (2556/1000000)).
- Client10:** A browser window showing a news article from Netgate.com about pfSense support.

The taskbar at the bottom shows the date (05/02/2024), time (14:27), and system icons.

MACHINE **PFSENSE**

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



The screenshot shows a terminal window with three tabs at the top: "Home", "PFSENSE", and "Client10". The "PFSENSE" tab is active, displaying a log of USB device enumeration. The log output is as follows:

```
usbus1: 480Mbps High Speed USB v2.0
ZFS filesystem version: 5
ZFS storage pool version: features support (5000)
ugen1.1: <VMware EHCI root HUB> at usbus1
uhub0 on usbus1
uhub0: <VMware EHCI root HUB, class 9/0, rev 2.00/1.00, addr 1> on usbus1
ugen0.1: <VMware UHCI root HUB> at usbus0
uhub1 on usbus0
uhub1: <VMware UHCI root HUB, class 9/0, rev 1.00/1.00, addr 1> on usbus0
Trying to mount root from ufs:/dev/ufs/65c0c876b9ee0a26 [rw,noatime]...
uhub1: 2 ports with 2 removable, self powered
Root mount waiting for: CAM usbus0 usbus1
ugen0.2: <VMware VMware Virtual USB Mouse> at usbus0
uhid0 on uhub1
uhid0: <VMware> on usbus0
uhid1 on uhub1
uhid1: <VMware> on usbus0
ugen0.3: <VMware, Inc. VMware Virtual USB Hub> at usbus0
uhub2 on uhub1
uhub2: <VMware, Inc.> on usbus0
Root mount waiting for: CAM usbus0 usbus1
uhub0: 6 ports with 6 removable, self powered
uhub2: 7 ports with 7 removable, self powered
Root mount waiting for: CAM
```



```
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)          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: █
```

MACHINE CLIENTE WINDOWS 10 PFSENSE INTERFACE WEB

pfSense® COMMUNITY EDITION

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

Interfaces / Interface Assignments List 

Interface Assignments In          

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.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

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)

OPT1 em2 (00:0c:29:c5:74:bf)

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: OPT1

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 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

09/02/2024

Jude chryst poums

pfSense.tssr.lan - Interfaces: OPT X +

Non sécurisé | https://192.168.10.254/interfaces.php?if=opt1

Explicitly set speed and duplex mode for this interface.
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 /

IPv4 Upstream gateway [+ 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.
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.

09/02/2024 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](#).

09/02/2024 Jude chryst poums 16:05/02

Home X PFSENSE X Client10 X

pfSense.tssr.lan - Interfaces: DMZ X +

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

Status / Dashboard

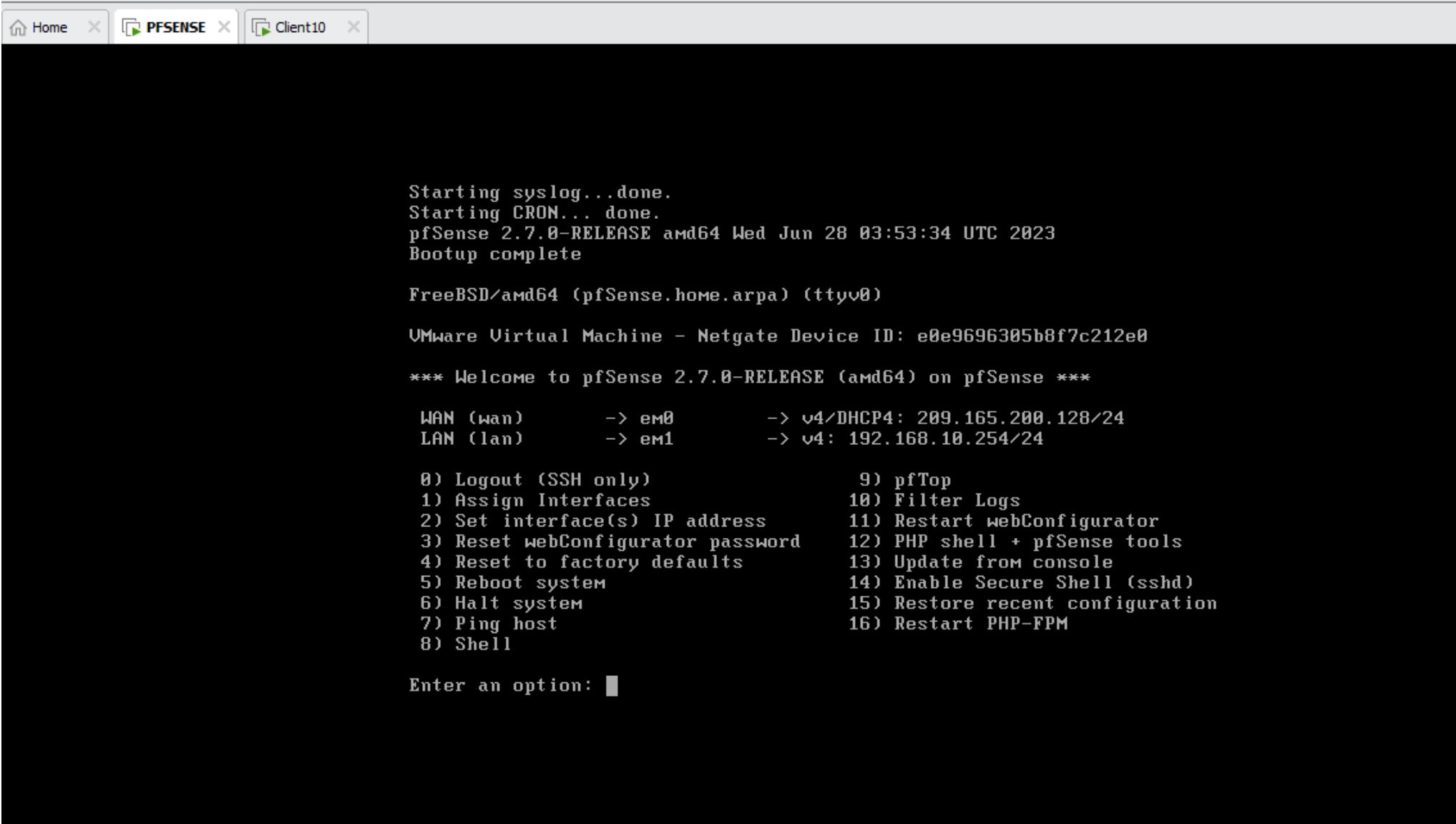
+ ?

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

MACHINE PFSENSE

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



The screenshot shows a terminal window with three tabs at the top: "Home", "PFSENSE" (which is active), and "Client10". The main area displays the pfSense boot logs and a command-line menu:

```
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)          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: █
```

Home X PFSENSE X Client10 X

```
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 ***

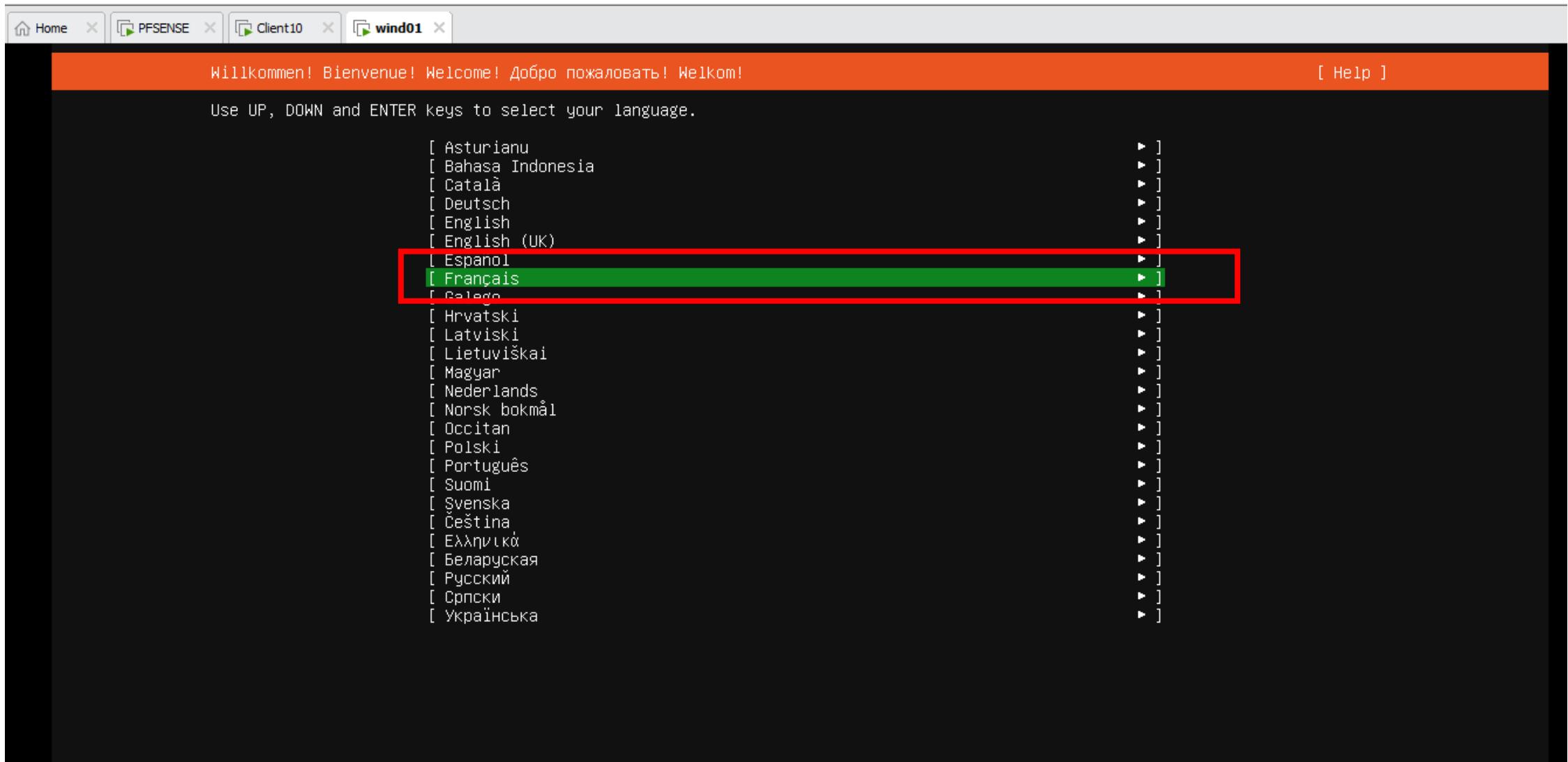
WAN (wan)      -> em0      -> v4/DHCP4: 209.165.200.128/24
LAN (lan)      -> em1      -> v1: 192.168.10.251/24
DMZ (opt1)     -> em2      -> v4: 192.168.20.254/32

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

Enter an option: █
```

MACHINE UBUNTU-SERVER

WEB



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.comcanonical/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

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.

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

() Ubuntu Server (minimized)

This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.

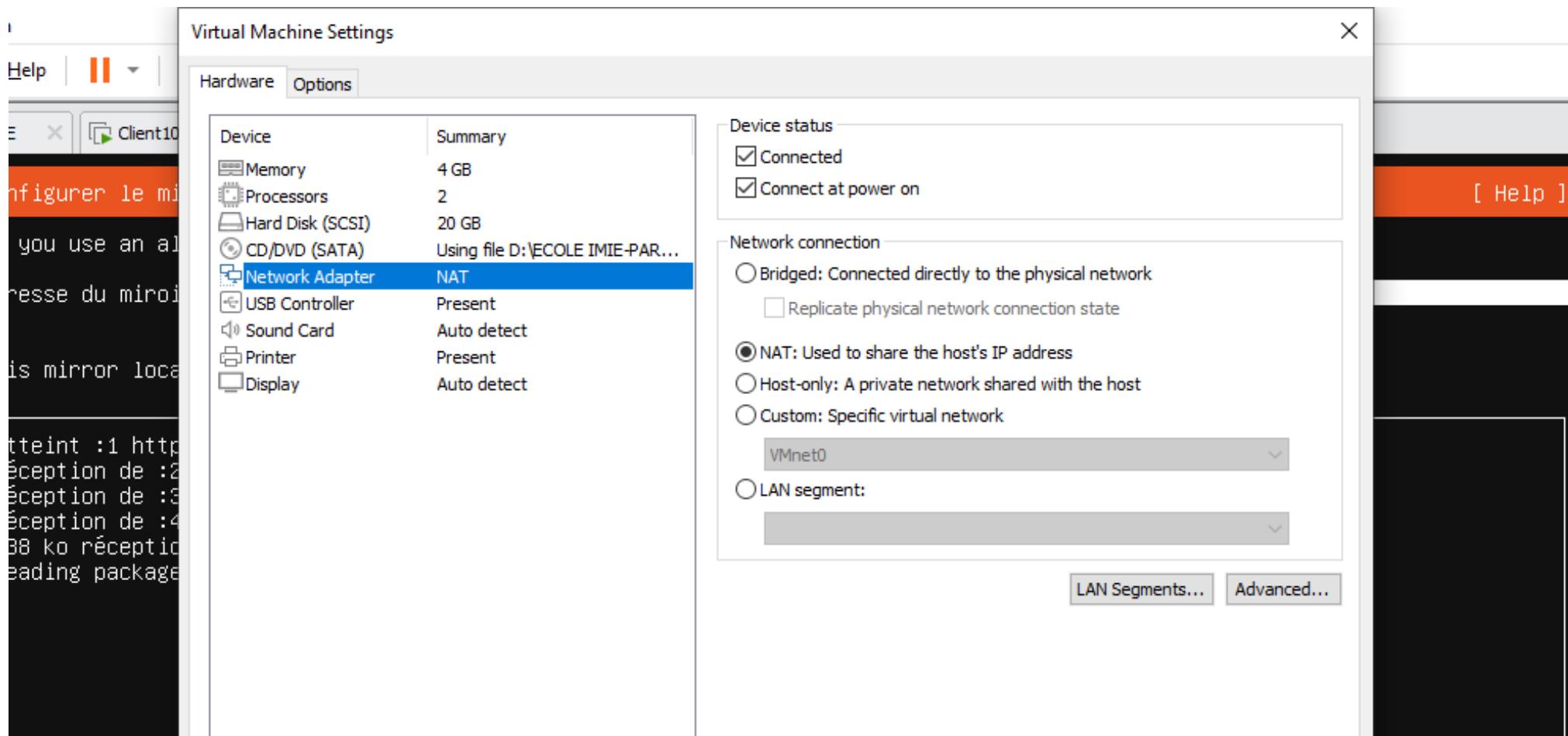
Additional options

[] 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

[Terminé]
[Retour]



Configurez au moins une interface pour que ce serveur puisse communiquer avec les autres machines sur le réseau, préféablement 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

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

- Set up this disk as an LVM group
- Encrypt the LVM group with LUKS
 - Phrase de passe : ****
 - Confirmez la phrase de passe : ****
- Custom storage layout

Tout en bas cliquer sur Done

[Terminé]

DISQUES DISPONIBLES

PÉRIPHÉRIQUE

[ubuntu-vg (nouveau, chiffrée)	TYPE	LVM volume group	TAILLE
espace libre		97.980G	►]
		48.992G	►

[Create software RAID (md) ►]
[Create volume group (LVM) ►]

PÉRIPHÉRIQUES UTILISÉS

PÉRIPHÉRIQUE

[ubuntu-vg (nouveau, chiffrée)	TYPE	LVM volume group	TAILLE
ubuntu-lv nouveau, to be formatted as ext4, mounted at /		97.980G	►]
		48.988G	►

[/dev/sda

partition 1 nouveau, BIOS grub spacer	disque local	100.000G	►]
partition 2 nouveau, to be formatted as ext4, mounted at /boot		1.000M	►
partition 3 nouveau, PV of LVM volume group ubuntu-vg		2.000G	►
		97.997G	►

Tout en bas cliquer sur terminer

[Terminé]
[Rétablir]

DISQUES DISPONIBLES

PÉRIPHÉRIQUE

[ubuntu-vg (nouveau, chiffrée)
espace libre

TYPE

LVM volume group
97.980G ►
48.992G ►

TAILLE

[Create software RAID (md) ►]
[Create volume group (

PÉRIPHÉRIQUES UTILISÉS

PÉRIPHÉRIQUE

[ubuntu-vg (nouveau, c
ubuntu-lv nouveau

[/dev/sda
partition 1 nouveau
partition 2 nouveau
partition 3 nouveau

Confirmer l'action

Selecting Continue below will begin the installation process and result in the loss of data on the disks selected to be formatted.

You will not be able to return to this or a previous screen once the installation has started.

Are you sure you want to continue?

[Non]
[Continuer]

Cliquer sur continuer

[Terminé]
[Rétablir]

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.

Installer le serveur OpenSSH

Importer une identité SSH: [Non ▾]

You can import your SSH keys from GitHub or Launchpad.

Importer le nom d'utilisateur :

Autoriser l'authentification par mot de passe via SSH

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

```
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_volvgroup: lvm_volvgroup-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
```

```
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
            writing etc/fstab
            configuring multipath
            updating packages on target system
            configuring pollinate user-agent on target
            updating initramfs configuration
            configuring target system bootloader
            installing grub to target devices
final system configuration
  configuring cloud-init
  calculating extra packages to install
  installing openssh-server
    retrieving openssh-server
    curtin command system-install
    unpacking openssh-server
    curtin command system-install
  downloading and installing security updates
    curtin command in-target
  restoring apt configuration
    curtin command in-target
subiquity/Late/run
```

Tout en bas cliquer sur Redémarrer
maintenant

[View full log]
[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 Processes: 218  
Usage of /: 14.0% of 47.92GB Users logged in: 0  
Memory usage: 9% IPv4 address for ens33: 209.165.200.129  
Swap usage: 0%
```

```
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.
```

Jude chryst poums

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

```
jude@web01:~$ sudo su
[sudo] password for jude:
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
    altnet enp2s1
    inet 209.165.200.129/24 metric 100 brd 209.165.200.255 scope global dynamic ens33
        valid_lft 1574sec preferred_lft 1574sec
    inet6 fe80::20c:29ff:fe22:c4b8/64 scope link
        valid_lft forever preferred_lft forever
root@web01:/home/jude# 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
```

GNU nano 6.2 /etc/netplan/00-installer-config.yaml *

```
# This is the network config written by 'subiquity'  
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
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^Y Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

```
# 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

The screenshot shows the 'Virtual Machine Settings' dialog box for a virtual machine named 'wind01'. The 'Hardware' tab is selected, displaying configuration details for various components:

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	100 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

In the 'Network connection' section, the 'LAN segment:' dropdown is set to 'DMZ' and is highlighted with a red rectangle. Other options include Bridged, NAT, Host-only, and Custom.

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...

MACHINE CLIENTE WINDOWS 10 PFSENSE INTERFACE WEB

The screenshot shows the pfSense Status Dashboard. The top navigation bar includes links for System, Interfaces, Firewall (selected), Services, VPN, Status, Diagnostics, Help, and a pfSense logo. A sub-menu for Firewall is open, showing options: Aliases, NAT, Rules, Schedules, Traffic Shaper, and Virtual IPs. The main dashboard area has two main sections: 'System Information' and 'Interfaces'. The 'System Information' section displays details like Name (pfSense.tssr.lan), User (admin@192.168.10.50), System (VMware Virtual Machine, Netgate Device ID: e0e9696305b8f7c212e0), BIOS (Vendor: Phoenix Technologies LTD, Version: 6.00, Release Date: Thu Nov 12 2020), and Version (2.7.0-RELEASE (amd64), built on Wed Jun 28 03:53:34 UTC 2023, FreeBSD 14.0-CURRENT). It also states 'The system is on the latest version.' and 'Version information updated at Mon Feb 5 16:56:50 CET 2024'. The 'Interfaces' section lists three interfaces: WAN (1000baseT <full-duplex>, IP: 209.165.200.128), LAN (1000baseT <full-duplex>, IP: 192.168.10.254), and DMZ (1000baseT <full-duplex>, IP: 192.168.20.254). A status bar at the bottom shows icons for network, battery, and system status, along with the time (15:29) and date (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

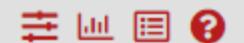
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0/3 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

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

09/02/2024 Jude chryst poums 15 06/02

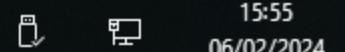
Firewall / Rules / LAN



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 80	443	*	*	Anti-Lockout Rule	
<input type="checkbox"/>		3/1.22 MiB	IPv4 *	LAN net	*	*	*	*	none	
<input type="checkbox"/>		0/0 B	IPv6 *	LAN net	*	*	*	*	none	



<input checked="" type="checkbox"/>		3/1.22 MiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule					
<input checked="" type="checkbox"/>		0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule					

[Floating](#) [WAN](#) **LAN** [DMZ](#)**Rules (Drag to Change Order)**

<input type="checkbox"/>	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.

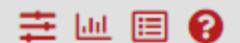


MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

Créer une règle de ping LAN vers tous

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

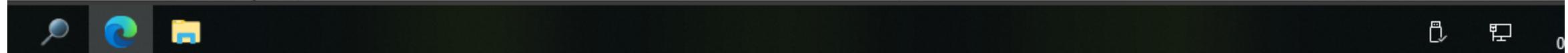
LAN

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 which

Address Family

IPv4

Select the Internet Protocol ver

Protocol

TCP

Choose which IP protocol this r

Source

Source

Invert match

any

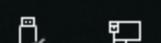
Source Address

/

v

 **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 Specify the destination port or range

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

Custom
only filtering a single port.

Extra Options

Log Log packets that are handled Hint: the firewall has limited log storage. Check the Status: System Logs: Settings link for more information.

09/02/2024 Jude chryst poums

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](#).



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](#) **LAN** [DMZ](#)**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/10.56 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP	LAN net	*	*	*	*	none		ping LAN vers tous	

▲ Add **▼ Add** **Delete** **Toggle** **Copy** **Save** **Separator**

A screenshot of a Windows Command Prompt window titled "pfSense.tssr.lan - Firewall: Rules". The window shows the following output:

```
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>
```

The right side of the window displays a sidebar titled "Actions" with icons for "Module", "Edit", "Copy", and "Save".

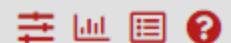
MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

**Créer une règle de ping entre LAN
IN WAN**

Source	
<u>Source</u>	<input type="checkbox"/> Invert match
LAN net	
Source Address	
/	
▼	
Destination	
<u>Destination</u>	<input type="checkbox"/> Invert match
Single host or alias	
1.1.1.1	
/	
▼	
Extra Options	
Log	<input type="checkbox"/> 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

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](#) **LAN** [DMZ](#)

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	5/10.66 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/480 B	IPv4 ICMP	LAN net	*	1.1.1.1	*	*	none		ping WAN in WAN	

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

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>

Action

Rule

NAN

Add

Del

Toggle

Copy

Print

MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

Créer une règle de résolution DNS

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.

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).

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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/10.73 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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 défaut : pfSense.tssr.lan
Address: 192.168.10.254

>
```

Actions

Rule

NS

Add Add Delete Toggle Copy Save +

This screenshot shows a pfSense firewall configuration interface. On the left, there is a terminal window titled 'C:\Windows\system32\cmd.exe - nslookup' displaying the command 'nslookup' being run by user 'user01'. The output shows the default server is 'pfSense.tssr.lan' at address '192.168.10.254'. Below the terminal is a sidebar with sections for 'Actions' (containing 'Rule' and 'NS' buttons), and a row of buttons for 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and a plus sign. The main area of the interface is currently empty.

MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

**Créer un alias pour accéder a des pages web
[http\(80\)](http://)/[https\(443\)](https://)**

Dans l'onglet Firewall

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

- ✓ Clic sur Aliases

The screenshot shows the pfSense Firewall Rules LAN page. At the top, there is a message: "The changes have been applied successfully. The Monitor the filter reload progress." Below this, there are tabs for Floating, WAN, LAN (which is selected), and DMZ. A red arrow points to the "Aliases" option in the "Firewall" dropdown menu, which is currently open. The main table displays two rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 4/10.75 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓ 0/480 B	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		résolution DNS	

At the bottom, there are navigation buttons: Add, Delete, Toggle, Copy, Save, and Separator.

✓ Ensuite faire un clic sur le bouton Add

The screenshot shows the pfSense Firewall Aliases IP configuration page. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the title is "Firewall / Aliases / IP". There are tabs for IP, Ports, URLs, and All, with IP selected. A table titled "Firewall Aliases IP" lists columns for Name, Values, Description, and Actions. In the Actions column, there are two buttons: a green "+ Add" button and a blue "Import" button. A red arrow points to the "+ Add" button. The bottom right corner of the page has a small "i" icon.

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

Firewall / Aliases / Edit ?

Properties

Name	<input type="text" value="Web"/>	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	<input type="text" value="protocole de navigation web"/>	A description may be entered here for administrative reference (not parsed).
Type	<input type="text" value="Port(s)"/>	

Port(s)

Hint	Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.		
Port	<input type="text" value="80"/>	web non sécurisé	Delete
	<input type="text" value="443"/>	web sécurisé	Delete

Save + Add Port

09/02/2024 Jude chryst poums

Toujours

✓ Cliquer sur Apply Changes apres une modification dans une règle

pfSense® COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Aliases / IP

The alias list has been changed.
The changes must be applied for them to take effect.

Apply Changes

IP Ports URLs All

Firewall Aliases IP

Name	Values	Description	Actions
			Add Import

09/02/2024 Jude chryst poums

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

The screenshot shows the pfSense web interface for managing firewall aliases. The URL in the address bar is https://192.168.10.254/firewall_aliases.php?tab=port. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help, and a notification bell with 5 alerts.

The main title is "Firewall / Aliases / Ports". Below it, there are tabs for IP, Ports (which is selected), URLs, and All. The "Ports" section displays a table titled "Firewall Aliases Ports".

Name	Values	Description	Actions
Web	80, 443	protocole de navigation web	

At the bottom right of the table are "Add" and "Import" buttons. A small information icon is located at the bottom left of the page.

MACHINE CLIENTE WINDOWS 10

PFSENSE INTERFACE WEB

**Créer une règle de navigation
web**

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

The screenshot shows the pfSense Firewall Rules Edit interface. The top navigation bar includes links for Non sécurisé, https://192.168.10.254/firewall_rules_edit.php?if=lan, System, Interfaces, Firewall (selected), Services, VPN, Status, Diagnostics, Help, and a search icon. The main title is Firewall / Rules / Edit. On the left, there's a sidebar with links for Aliases, NAT, Rules (highlighted in red), Schedules, Traffic Shaper, and Virtual IPs. The main content area has tabs for Action, Traffic Shaper, and Virtual IPs. The Action tab is selected and shows "Pass" highlighted with a red box. Below it, there's a note about choosing what to do with packets and a hint about the difference between block and reject. The Disabled section contains a checkbox for disabling the rule. The Interface section shows "LAN" selected from a dropdown menu, with a note about choosing the interface. The Address Family section shows "IPv4" selected from a dropdown menu, with a note about selecting the Internet Protocol version.

Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?if=lan

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

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with this packet based on 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.

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 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 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

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

Apply Changes

[Floating](#) [WAN](#) [LAN](#) **LAN** [DMZ](#)**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	4/10.83 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>		0/4 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none	résolution DNS	
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	LAN net	*	*	Web	*	none	navigation web	

Add Add Delete Toggle Copy Save Separator

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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/10.86 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 10/8 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		résolution DNS	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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`

PASSWORDAUTHENTICATION 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# systemctl 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: | X SFR SAMSUNG - Découvrez tous les | X federation de foot en cote d'ivoir | Bienvenue sur Fédération Ivoirien | +

Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?if=lan

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 TCP

Choose which IP protocol this rule should match.

Source

Source	Invert match	LAN net	Source Address	/	▼
Source	<input type="checkbox"/> Invert match	LAN net	Source Address	/	▼

09/02/2024 Jude chryst poums

pfSense.tssr.lan - Firewall: Rules | X SFR SAMSUNG - Découvrez tous les | X federation de foot en cote d'ivoir | Bienvenue sur Fédération Ivoirien | +

Non sécurisé | https://192.168.10.254/firewall_rules_edit.php?if=lan

Destination

Destination	<input type="checkbox"/> Invert match	Single host or alias	192.168.20.10	
Destination Port Range	SSH (22)	Custom	SSH (22)	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

09/02/2024 Jude chryst poums

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

Floating WAN LAN DMZ

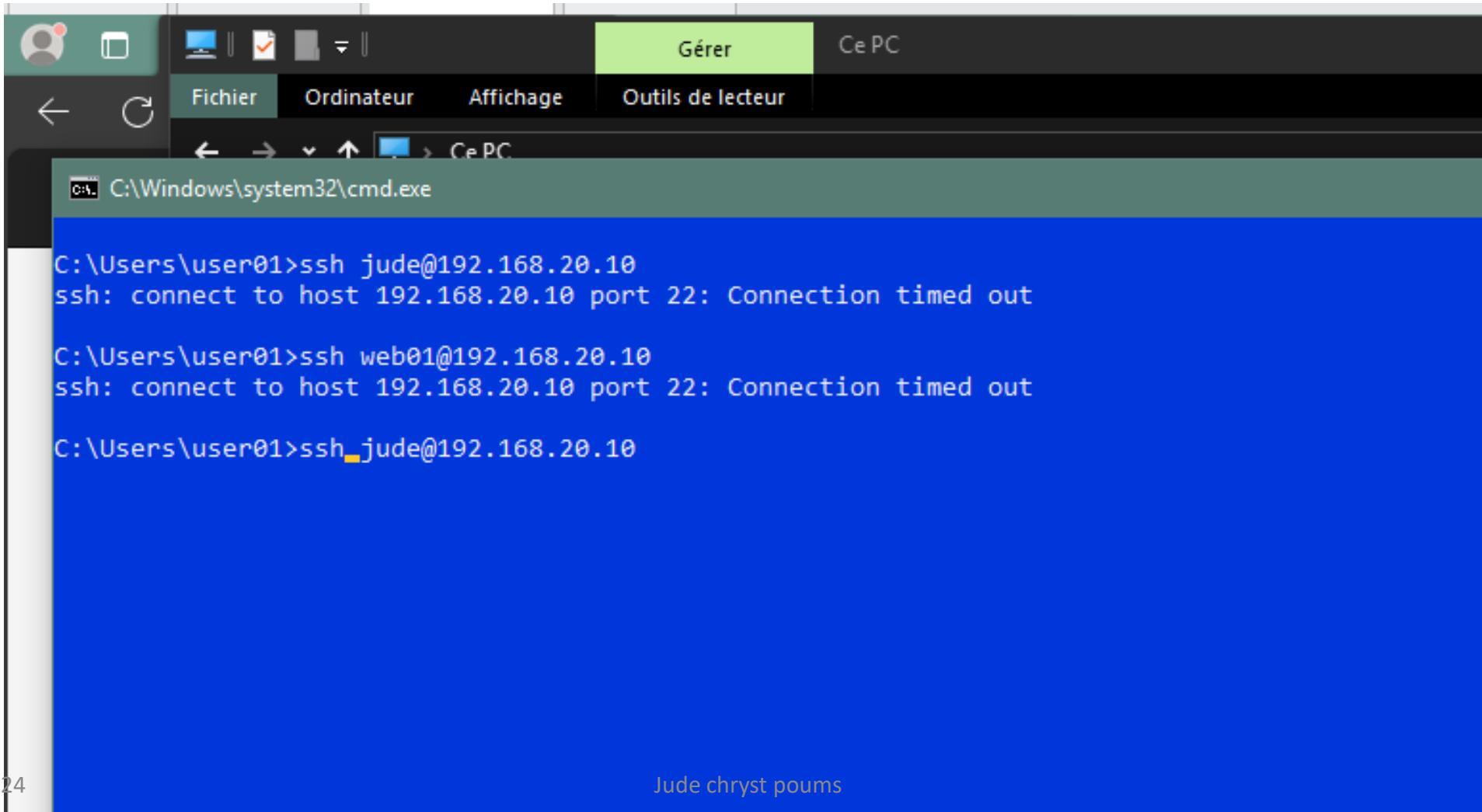
Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/2.79 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/11.36 MiB	IPv4 TCP/UDP	LAN net	*	*	Web	*	none		protocole de navigation web	
<input type="checkbox"/>	0/63 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		résolution DNS	
<input type="checkbox"/>	0/480 B	IPv4 ICMP any	LAN net	*	1.1.1.1	*	*	none		ping lan in wan	
<input type="checkbox"/>	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



The screenshot shows a Windows Command Prompt window titled 'cmd' with the path 'C:\Windows\system32\cmd.exe'. The window contains the following text:

```
C:\Users\user01>ssh jude@192.168.20.10
ssh: connect to host 192.168.20.10 port 22: Connection timed out

C:\Users\user01>ssh web01@192.168.20.10
ssh: connect to host 192.168.20.10 port 22: Connection timed out

C:\Users\user01>ssh jude@192.168.20.10
```

The window has a dark theme with a light blue header bar. The menu bar includes 'Fichier', 'Ordinateur', 'Affichage', 'Outils de lecteur', 'Gérer', and 'Ce PC'. The title bar says 'cmd C:\Windows\system32\cmd.exe'. The status bar at the bottom left shows the date '09/02/2024'.

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

The screenshot shows the pfSense Firewall Rules configuration page. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red bell icon indicates 2 notifications. Below the navigation bar, the URL https://192.168.10.254/firewall_rules.php?if=opt1 is displayed.

The main title is "Firewall / Rules / DMZ". On the left, there are tabs for Floating, WAN, LAN, and DMZ, with the DMZ tab currently selected and highlighted by a red box.

The main area is titled "Rules (Drag to Change Order)". It includes a header row with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The "Actions" column contains several icons: up arrow, Add, down arrow, Delete, Toggle, Copy, Save, and Separator.

A message at the bottom states: "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." The "Add" button in the Actions column is also highlighted with a red box.

At the bottom left, there is an information icon (i). The bottom right corner shows the date 09/02/2024 and the name Jude chryst poums.

✓ Interdiction absolue d'accéder au LAN

https://192.168.10.254/firewall_rules_edit.php?if=opt1&after=-1

EDIT Firewall Rule

Action **Block** Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface **DMZ** 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 **Any** Any

Choose which IP protocol this rule should match.

Source

Source Invert match any **DMZ net** DMZ net Source Address /

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	
<input type="checkbox"/>		0/0 B	IPv4 *	*	DMZ net	*	LAN net	*	*	none	interdire la communication depuis DMZ vers LAN	

Add Add Delete Toggle Copy Save Separator

i

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

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: UDP

Choose which IP protocol this rule should match.

Source

Source: DMZ net

Invert match:

Source Address: /

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

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

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

Destination Invert match any Destination Address:

Destination Port Range DNS (53) From Custom To 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 ▾

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
<input type="checkbox"/>	X	0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none	interdire la communication depuis DMZ vers LAN	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	DMZ net	*	*	53 (DNS)	*	none	RESOLUTION DNS	X

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

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: TCP

Choose which IP protocol this rule should match.

Source

Source: DMZ net Invert match

Source Address: /

09/02/2024 Jude chryst poums

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 WFR

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

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 TCP

Choose which IP protocol this rule should match.

Source Invert match LAN net /

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 Port Range NTP (123) NTP (123)

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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	4/5.79 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	 	0/0 B	IPv4 TCP	LAN net	*	*	123 (NTP)	*	none	synchronisation horloge	   
<input type="checkbox"/>	 	0/3 KiB	IPv4 ICMP	LAN net	*	*	*	*	none	ping vers tous les reseaux	   
<input type="checkbox"/>	 	0/28 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none	DNS vers tous	   
<input type="checkbox"/>	 	2/3.93 MiB	IPv4 TCP	LAN net	*	*	web	*	none	web vers tous	   
<input type="checkbox"/>	 	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)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/5.81 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN net	*	*	123 (NTP)	*	none		synchronisation horloge	
<input type="checkbox"/>	0/3 KiB	IPv4 ICMP	LAN net	*	*	*	*	none		ping vers tous les reseaux	
<input type="checkbox"/>	0/28 KiB	IPv4 UDP	LAN net	*	*	53 (DNS)	*	none		DNS vers tous	
<input type="checkbox"/>	1/3.93 MiB	IPv4 TCP	LAN net	*	*	web	*	none		web vers tous	
<input type="checkbox"/>	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

The screenshot shows the pfSense Firewall Rules Edit interface. The URL in the browser is https://192.168.10.254/firewall_rules_edit.php?if=opt1. The page title is "Firewall / Rules / Edit". The main section is titled "Edit Firewall Rule".

Action: Pass (dropdown menu)

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 (dropdown menu)
Choose the interface from which packets must come to match this rule.

Address Family: IPv4 (dropdown menu)
Select the Internet Protocol version this rule applies to.

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

NTP (123)

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

SYNCHRONISATION HORLOGE

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

Destination Port Range NTP (123) From Custom To 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

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
<input type="checkbox"/>	✗ ☰	0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none	interdire la communication depuis DMZ vers LAN	🔗 ✎ 📄 🚫 🗑️
<input type="checkbox"/>	✓ ☰	0/1 KiB	IPv4 UDP	DMZ net	*	*	53 (DNS)	*	none	RESOLUTION DNS	🔗 ✎ 📄 🚫 🗑️
<input type="checkbox"/>	✓ ☰	0/0 B	IPv4 TCP	DMZ net	*	*	web	*	none	NAVIGATIONS WEB	🔗 ✎ 📄 🚫 🗑️
<input type="checkbox"/>	✓ ☰	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

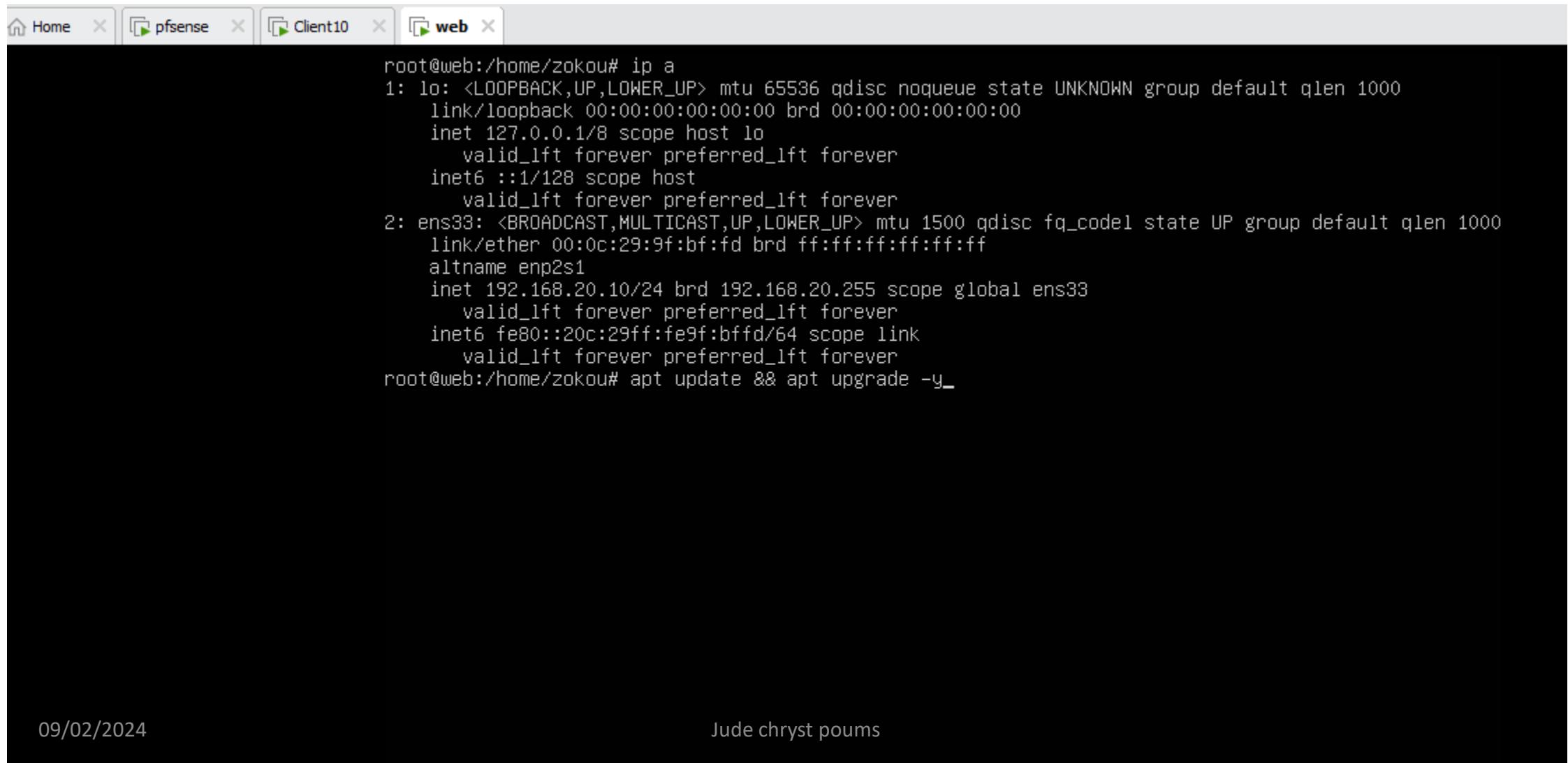
synchronisation horloge permet à notre machine web c'est-à-dire ubuntu d'accéder sur internet

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



The screenshot shows a terminal window titled 'web' with several tabs above it: 'Home', 'pfsense', 'Client10', and 'web'. The terminal displays the following command and its output:

```
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
```

```
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 kB]
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**

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

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

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](#)

âches

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		interdire la communication depuis DMZ vers LAN	
<input type="checkbox"/>	✓ 0/5 KiB ✗	IPv4 UDP	DMZ net	*	*	53 (DNS)	*	none		RESOLUTION DNS	
<input type="checkbox"/>	✓ 1/120.36 MiB ✗	IPv4 TCP	DMZ net	*	*	web	*	none		NAVIGATIONS WEB	
<input type="checkbox"/>	✓ 0/608 B	IPv4 TCP/UDP	DMZ net	*	*	123 (NTP)	*	none		SYNCHRONISATION HORLOGE	
<input type="checkbox"/>	✓ 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

```
jude@web01:~$ 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=127 time=6.49 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=6.68 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=5.89 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=6.01 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=8.07 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=5.01 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=15.6 ms
^C64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=7.35 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=127 time=5.72 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=127 time=6.43 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=127 time=16.7 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=127 time=6.06 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=127 time=11.6 ms
CV64 bytes from 8.8.8.8: icmp_seq=16 ttl=127 time=111 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=127 time=8.31 ms
^C
--- 8.8.8.8 ping statistics ---
17 packets transmitted, 16 received, 5.88235% packet loss, time 16188ms
rtt min/avg/max/mdev = 5.012/14.903/111.453/25.160 ms
jude@web01:~$ ^C
jude@web01:~$
```

Installer le paquet apache2

apt install apache2

```
root@web01:/home/jude
Swap usage: 0%
La maintenance de sécurité étendue pour Applications n'est pas activée.
0 mise à jour peut être appliquée immédiatement.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
R
 Last login: Thu Feb  8 20:56:13 2024 from 172.16.1.50
jude@web01:~$ sudo su
[sudo] password for jude:
root@web01:/home/jude# apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
liblua5.3-0 mailcap mime-support ssl-cert
 Paquets suggérés :
 apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
 Les NOUVEAUX paquets suivants seront installés :
 apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
liblua5.3-0 mailcap mime-support ssl-cert
0 mis à jour, 13 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 2 139 ko dans les archives.
Après cette opération, 8 518 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] 
```

```
# nano /etc/apache2/apache2.conf
```

The screenshot shows a terminal window titled "Client10" with the command "root@web: /home/zokou". The file being edited is "/etc/apache2/apache2.conf". The content of the file is as follows:

```
GNU nano 6.2
/etc/apache2/apache2.conf

# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.

#
#
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.

# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#      /etc/apache2/
#          |-- apache2.conf
#              '-- ports.conf
#          '-- mods-enabled
#              '-- *.load
#                  '-- *.conf
#          '-- conf-enabled
#              '-- *.conf
#          '-- sites-enabled
#              '-- *.conf
#

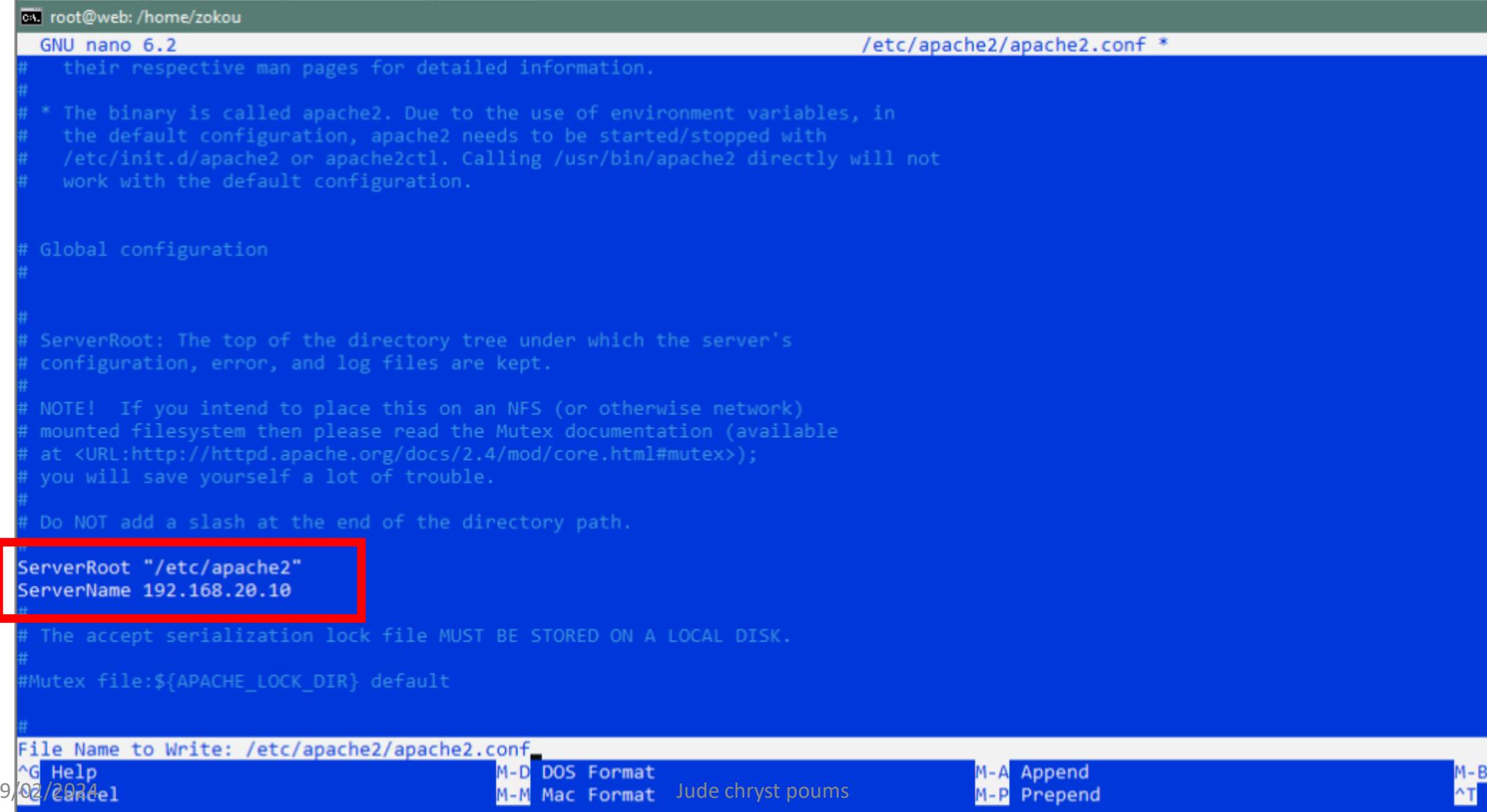

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute      ^C Location      M-U Undo       M-A Set Mar
09/02/2024 Exit  ^R Read File     ^X Replace       ^U Paste        ^J Justify      ^/ Go To Line   M-E Redo       M-6 Copy
```

```
# 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



```
root@web:/home/zokou
GNU nano 6.2
/etc/apache2/apache2.conf *

# their respective man pages for detailed information.
#
# * The binary is called apache2. Due to the use of environment variables, in
#   the default configuration, apache2 needs to be started/stopped with
#   /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not
#   work with the default configuration.

# Global configuration
#
#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE! If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.

ServerRoot "/etc/apache2"
ServerName 192.168.20.10
#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
#Mutex file:${APACHE_LOCK_DIR} default
#
File Name to Write: /etc/apache2/apache2.conf
^G Help          M-D DOS Format     M-A Append
09/02/2024      M-M Mac Format     M-P Prepend
Cancel          Jude chryst poums  ^T
```

```
# systemctl restart apache2  
# systemctl status apache2
```

```
root@web: /home/zokou  
  
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@web:/home/zokou# apt install apache2  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
apache2 est déjà la version la plus récente (2.4.52-1ubuntu4.7).  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.  
root@web:/home/zokou# nano /etc/ap  
apache2/ apparmor/ apparmor.d/ apport/ apt/  
root@web:/home/zokou# nano /etc/apache2/apache2.conf  
root@web:/home/zokou# systemctl restart apache2  
root@web:/home/zokou# systemctl status apache2  
● apache2.service - The Apache HTTP Server  
    Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)  
    Active: active (running) since Wed 2024-02-07 14:55:09 UTC; 8s ago  
      Docs: https://httpd.apache.org/docs/2.4/  
    Process: 14605 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
   Main PID: 14610 (apache2)  
     Tasks: 55 (limit: 9346)  
    Memory: 5.0M  
      CPU: 56ms  
     CGroup: /system.slice/apache2.service  
             └─14610 /usr/sbin/apache2 -k start  
                 ├─14612 /usr/sbin/apache2 -k start  
                 ├─14613 /usr/sbin/apache2 -k start  
                 └─14614 /usr/sbin/apache2 -k start  
  
févr. 07 14:55:09 web systemd[1]: Starting The Apache HTTP Server...  
févr. 07 14:55:09 web systemd[1]: Started The Apache HTTP Server.  
root@web:/home/zokou#
```



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

The screenshot shows a Microsoft Edge browser window with the address bar displaying "pfSense.tssr.lan - Firewall: Rules" and "Page par défaut d'Apache2 Ubuntu". The main content is the Apache2 default page, which features the Ubuntu logo and the text "Page par défaut d'Apache2". A red button labeled "Ça marche!" is visible. Below the logo, there is a paragraph of text explaining the purpose of the page and instructions to replace the file if it's not the intended content. At the bottom, a section titled "Vue d'ensemble de la configuration" provides details about the Apache2 configuration on Ubuntu. The taskbar at the bottom shows various icons and the date "07/02/2024" along with a timestamp "16:06".

Non sécurisé | 192.168.20.10

Page par défaut d'Apache2 Ubuntu

Ça marche!

Il s'agit de la page d'accueil par défaut utilisée pour tester le bon fonctionnement du serveur Apache2 après l'installation sur les systèmes Ubuntu. Il est basé sur la page équivalente sur Debian, à partir de laquelle l'Ubuntu Apache l'emballage est dérivé. Si vous pouvez lire cette page, cela signifie que le serveur HTTP Apache installé à Ce site fonctionne correctement. Vous devez remplacer ce fichier (situé à l'emplacement /var/www/html/index.html) avant de continuer à utiliser votre serveur HTTP.

Si vous êtes un utilisateur normal de ce site Web et que vous ne savez pas ce qu'est cette page , cela signifie probablement que le site est actuellement indisponible en raison de entretien. Si le problème persiste, veuillez contacter l'administrateur du site.

Vue d'ensemble de la configuration

La configuration par défaut d'Apache2 d'Ubuntu est différente de celle de la configuration par défaut en amont, et divisé en plusieurs fichiers optimisés pour interaction avec les outils Ubuntu. Le système de configuration est entièrement documenté dans /usr/share/doc/apache2/README.Debian.gz. Référez-vous à ceci pour l'intégralité documentation. La documentation du serveur web lui-même peut être trouvé en accédant au manuel si le paquet apache2-doc a été installé sur ce serveur.

La configuration d'une installation de serveur Web Apache2 sur les systèmes Ubuntu est la suivante :

```
# 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, 13.249.9.121
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%[=====]  6,00 MB/s

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# 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#
```

ÉTUDIANTS PARENTS PROFESSIONNELS ENTREPRISES

CONCEPT 6 FORMATIONS 81 MÉTIERS EMPLOYABILITÉ 3 CAMPUS PLUS → PORTES OUVERTES → CANDIDATER →

GUARDIA

1ÈRE ÉCOLE D'INFORMATIQUE DÉDIÉE À LA CYBERSÉCURITÉ

- › Bachelor & MSc spécialisés en cybersécurité
- › Formations en initiale et en alternance
- › +100 entreprises partenaires

Jude chryst poums

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

The screenshot shows the pfSense web interface for managing network rules. The URL in the browser is `https://192.168.10.254/firewall_nat.php`. The top navigation bar includes links for System, Interfaces, Firewall (which is currently active), Services, VPN, Status, Diagnostics, Help, and a notifications icon showing 2 alerts. Below the navigation is a breadcrumb trail: Firewall / NAT / Port Forward. A red box highlights the 'NAT' option in the Firewall dropdown menu. The main content area displays a table for 'Port Forward' rules with columns: Interface, Protocol, Source Address, Source Ports, Dest. Address, Dest. Ports, NAT IP, NAT Ports, Description, and Actions. The 'Actions' column contains buttons for Add, Delete, Toggle, Save, and Separator. The 'Add' button is specifically highlighted with a red box.

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

The screenshot shows a configuration interface for a firewall rule. The URL in the address bar is https://192.168.10.254/firewall_nat_edit.php. The page displays several configuration fields:

- Source:** A dropdown menu labeled "Display Advanced".
- Destination:** An "Invert match" checkbox.
- Destination port range:** A dropdown menu set to "HTTP" (highlighted with a red box). Below it are "from port" (Custom), "To port" (HTTP), and "Address/mask" fields.
- Redirect target IP:** A dropdown menu set to "Single host" (highlighted with a green box). To its right is an "Address" field containing "192.168.20.10".
- Redirect target port:** A dropdown menu set to "Other" (highlighted with a red box). To its right is a "Port" field containing "80" (highlighted with a red box).

Below the "Redirect target port" section, there is descriptive text: "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."

https://192.168.10.254/firewall_nat.php

pfSense COMMUNITY EDITION

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

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

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.20.10	80 (HTTP)	REDIRECTION DE PORT	

Legend

Add Add Delete Toggle Save Separator

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

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	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

The screenshot shows the pfSense Firewall Rules configuration page. The URL in the browser is https://192.168.10.254/firewall_rules.php. The navigation bar includes links for System, Interfaces, Firewall (selected), Services, VPN, Status, Diagnostics, Help, and a notification bell with 2 alerts.

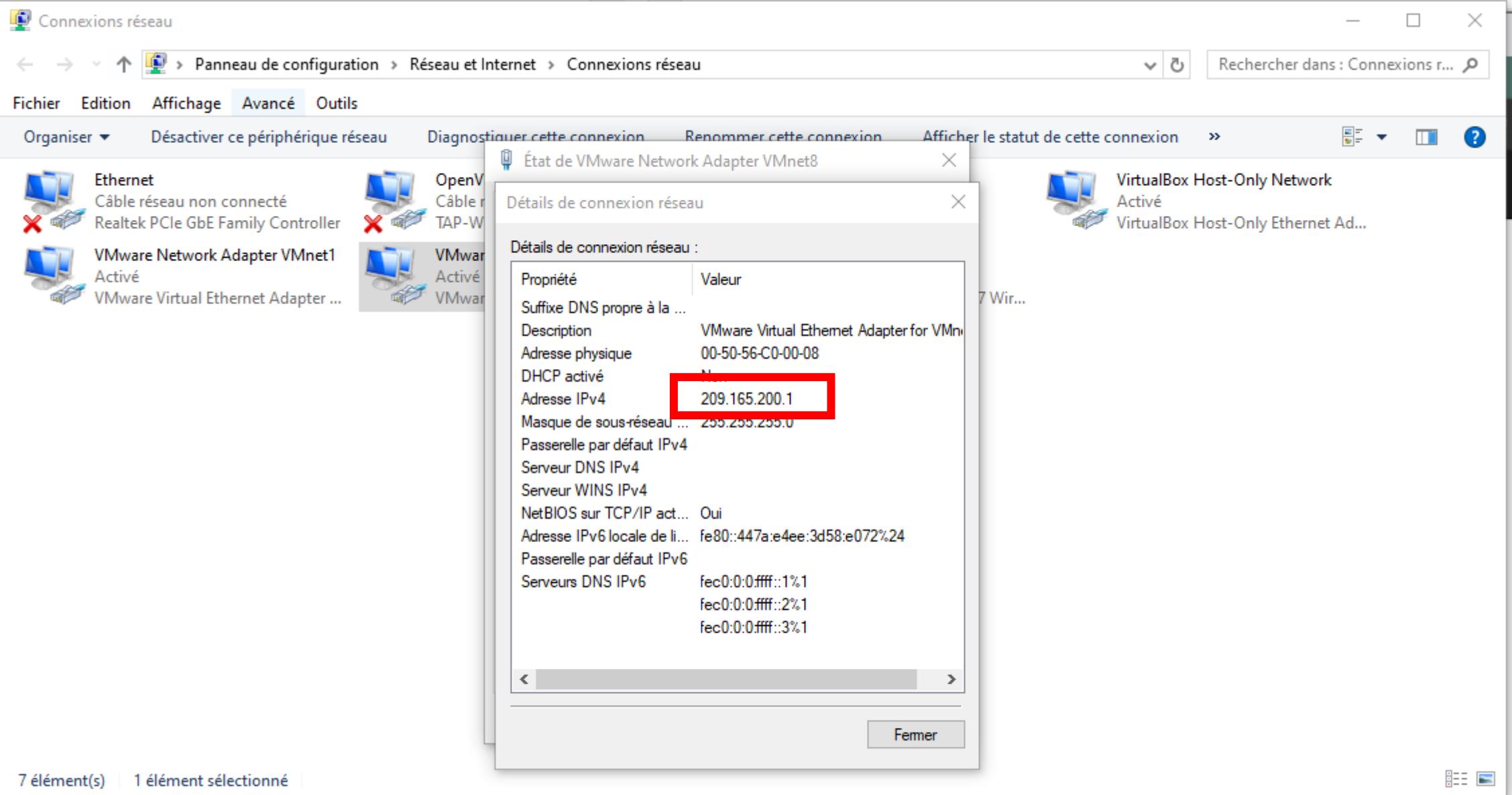
The main content area displays the "Firewall / Rules / WAN" section. Below it, tabs for Floating, WAN (selected), LAN, and DMZ are visible. A dropdown menu under the Firewall tab shows options: Aliases, NAT, Rules (which is highlighted with a red box), Schedules, Traffic Shaper, and Virtual IPs.

The "Rules (Drag to Change Order)" table lists three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
0/48 KiB	IPv4 TCP	*	*	192.168.20.10	80 (HTTP)	*	none		NAT REDIRECTION DE PORT	

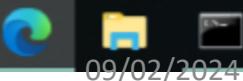
A red dashed box highlights the last rule, which is a NAT redirection rule for port 80 (HTTP) to 192.168.20.10. Below the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

The bottom left corner shows the date 09/02/2024, and the bottom right corner shows the name Jude chryst poums.



7 élément(s) | 1 élément sélectionné

Pass



09/02/2024

Jude chryst poums

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**

The screenshot shows the homepage of the Guardia website. The header features a navigation bar with links for ÉTUDIANTS, PARENTS, PROFESSIONNELS, and ENTREPRISES. Below the header is a large banner with the text "1ÈRE ÉCOLE D'INFORMATIQUE DÉDIÉE À LA CYBERSÉCURITÉ". On the left, there's a "GUARDIA" logo and a "CONCEPT" section. The main content area includes sections for "6 FORMATIONS", "81 MÉTIERS", "EMPLOYABILITÉ", "3 CAMPUS", and "PLUS". A "PORTES OUVERTES" button is highlighted in blue. To the right, there's a "CANDIDATER" button. A large image of two students working on a computer is overlaid on the background. In the bottom right corner of the image, there's a small inset showing a window titled "file_" containing text about "Titre RNCP NIVEAU 6" and "Titre RNCP NIVEAU 7", along with the "PRIX DE L'INNOVATION EDUNIVERSAL 2022".

Activer la synchronisation du système clock: Yes

```
Tasks: 2 (limit: 4515)
Memory: 1.3M
CPU: 32ms
CGroup: /system.slice/ntp.servi
└─1349 /usr/sbin/ntpd - 

févr. 09 10:55:59 web01 ntpd[1349]: 
févr. 09 10:55:59 web01 systemd[1]: 
févr. 09 10:56:00 web01 ntpd[1349]: 
févr. 09 10:56:01 web01 ntpd[1349]: 
févr. 09 10:56:02 web01 ntpd[1349]: 
févr. 09 10:56:03 web01 ntpd[1349]: 
févr. 09 10:56:04 web01 ntpd[1349]: 
root@web01:/home/jude# systemctl res
Failed to restart systemd-timesyncd.
root@web01:/home/jude# timedatectl
          Local time: ven. 2024
          Universal time: ven. 2024
             RTC time: ven. 2024
           Time zone: Etc/UTC (System clock synchronized: no
                  NTP service: n/a
                 RTC in local TZ: no
root@web01:/home/jude# systemctl res
Failed to restart systemd-timesyncd.
root@web01:/home/jude# timedatectl
          Local time: ven. 2024
          Universal time: ven. 2024
             RTC time: ven. 2024
           Time zone: Etc/UTC (System clock synchronized: yes
                  NTP service: n/a
                 RTC in local TZ: no
root@web01:/home/jude#
```

Virtual Machine Settings

Hardware Options

Settings	Summary
General	WEB_01
Power	
Shared Folders	Disabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	
Access Control	Not encrypted
VMware Tools	Time sync on
VNC Connections	Disabled
Unity	
Appliance View	
Autologin	Not supported
Advanced	Default/Default

VMware Tools features

Synchronize guest time with host

VMware Tools updates

If a new version of VMware Tools is available:

Update manually (do nothing)

Update automatically

Use application default (currently update manually)

To change the default setting, go to Edit > Preferences > Updates

```
# 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 T2: 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 T2: no  
root@web01:/home/jude#
```