# PROJET PERSONNEL – MISE EN ŒUVRE DE PARE-FEU DANS UNE INFRA

**BRETON Théo**

**Projet N°2 : LYCEETECH Réseaux**

## Contexte :

Le **LycéeTech Réseaux** est établissement spécialisé dans la conception, la sécurisation et l'exploitation d'infrastructures informatiques destinées aux entreprises du domaine de l'informatique. Elle dispose de deux réseau différent un réseau en classe C. Afin d'assurer la performance, la sécurité et l'isolation des différents services, **le site web hébergé sur le serveur ne doit pas pouvoir être accessible par le poste VLAN 2 mais accessible par le poste qui est sur le VLAN 3.**


Le réseau repose sur une infrastructure virtuelle simulée dans **EVE-NG**, où chaque équipement est représenté par une machine virtuelle

- **Windows Server** pour le service Web
- **Windows 10** pour les postes clients
- **Opnsense** pour le pare-feu et la sécurité périmétrique.

**Objectifs du projet**
Ce projet vise à mettre en œuvre les compétences suivantes

- **Configuration des pare-feu Opnsense** pour filtrer les flux inter-bâtiments et sécuriser les accès
- **Déploiement d'un serveur web** hébergé sur Windows Server, accessible depuis tous les postes clients du lycée
- **Configuration du DHCP sur les pare feu** pour attribuer une adresse aux ordinateurs mais aussi au pare-feu

- **Etablissement des règles de sécurité** pour les accès au site Web.

- **Paramètrage des interfaces** nécessaires dans les pare feu.

## Topologie simulée :

Le réseau est réparti sur 2 bâtiments :

- **Bâtiment A : Pôle pédagogique**
  Le poste du pôle pédagogique doit accéder au site web hébergé sur le serveur. Il doit aussi pouvoir communiquer avec le poste de la direction.

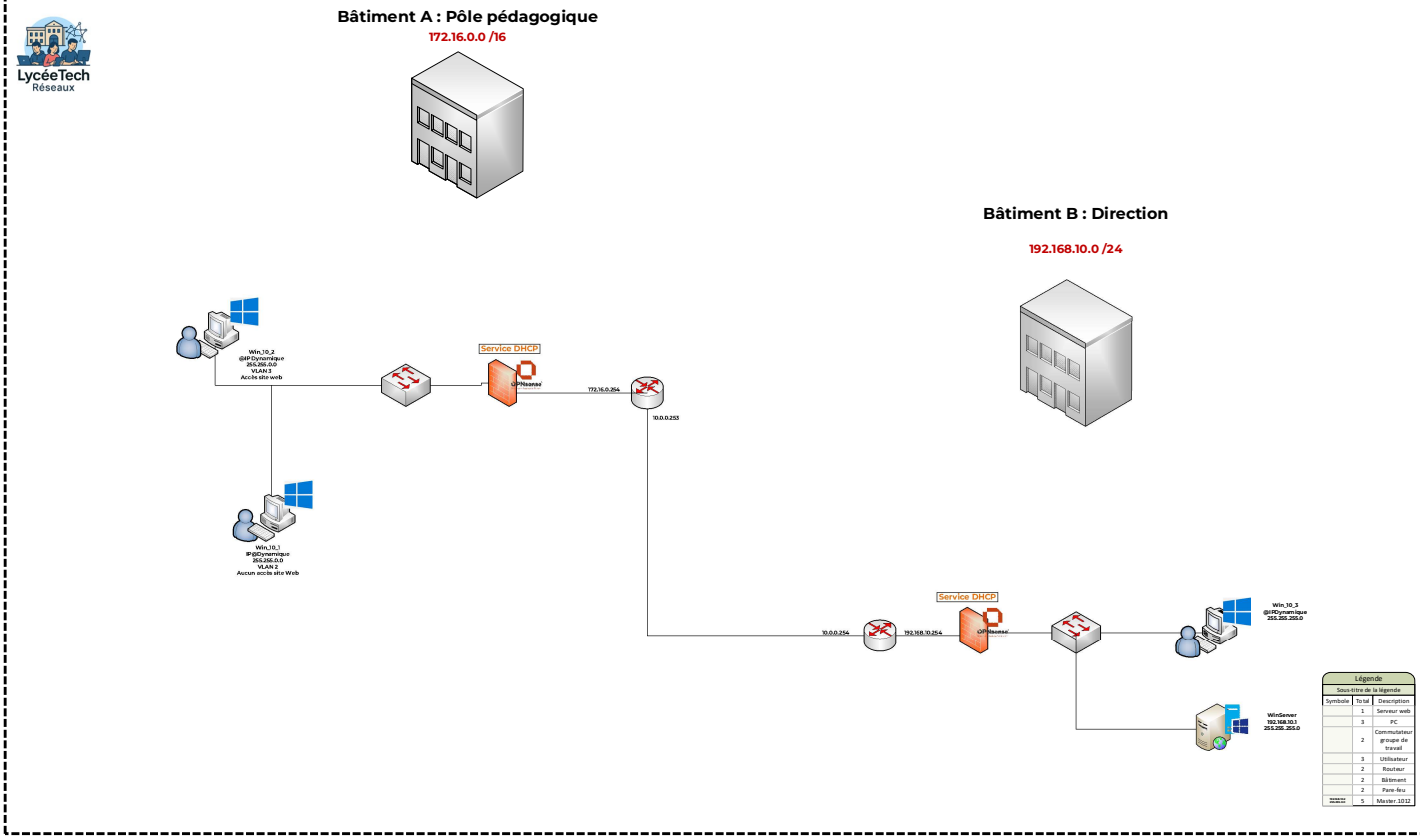
- **Bâtiment B : Direction**
  Le poste de la direction doit accéder au site web hébergé sur le serveur.
  Il doit aussi pouvoir communiquer avec le poste du pôle pédagogique.

## Partie Configuration Opnsense1 :

**Sécuriser l'accès Web des pare feu Opnsense**
Dans **System → Settings**, configure ces éléments :

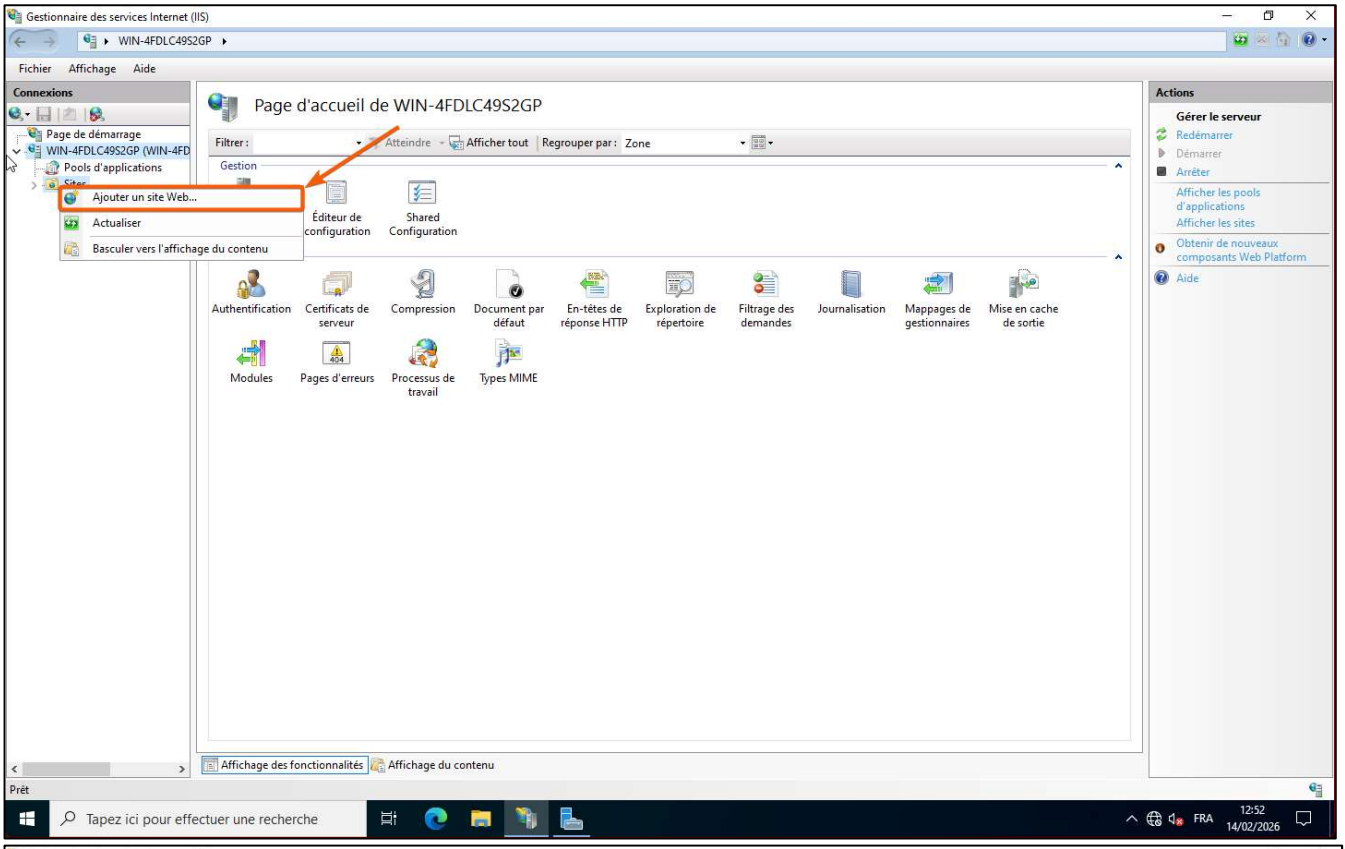
- **Accès VLAN 2 – non autorisé**
- **Accès VLAN 3 – Autorisé**
- **Configuration du service DHCP**
- **Configuration des règles du pare feu nécessaire pour les accès au site Web du bâtiment B**

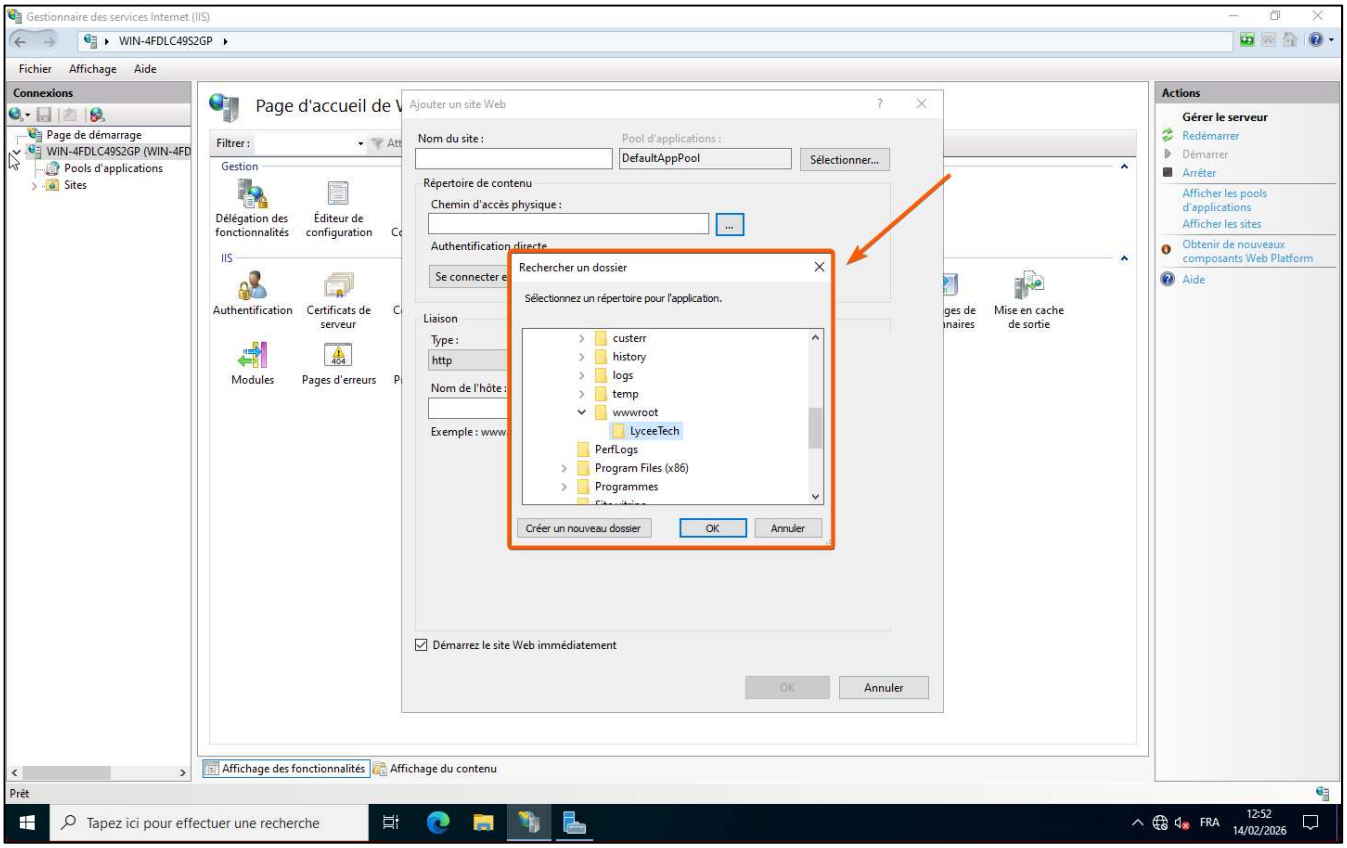
# Schéma Réseau - LycéeTech Réseaux :

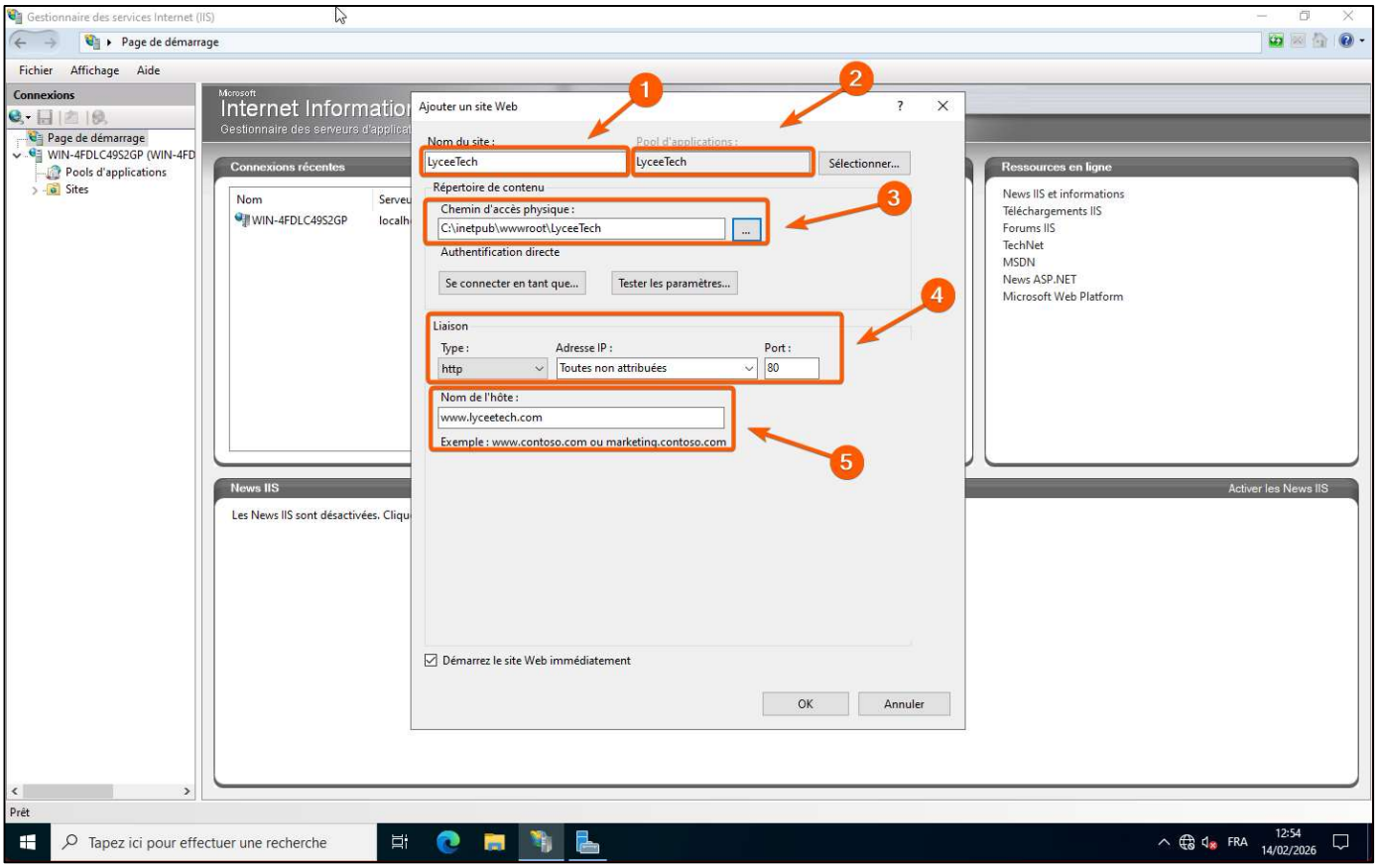


# 1ère phase du projet : Hébergement du site web sur le Serveur du Bâtiment B – Direction :

## ❶ Ajouter le rôle WebServer (IIS) et hébergé le site:

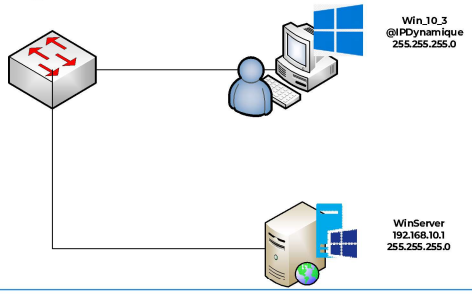


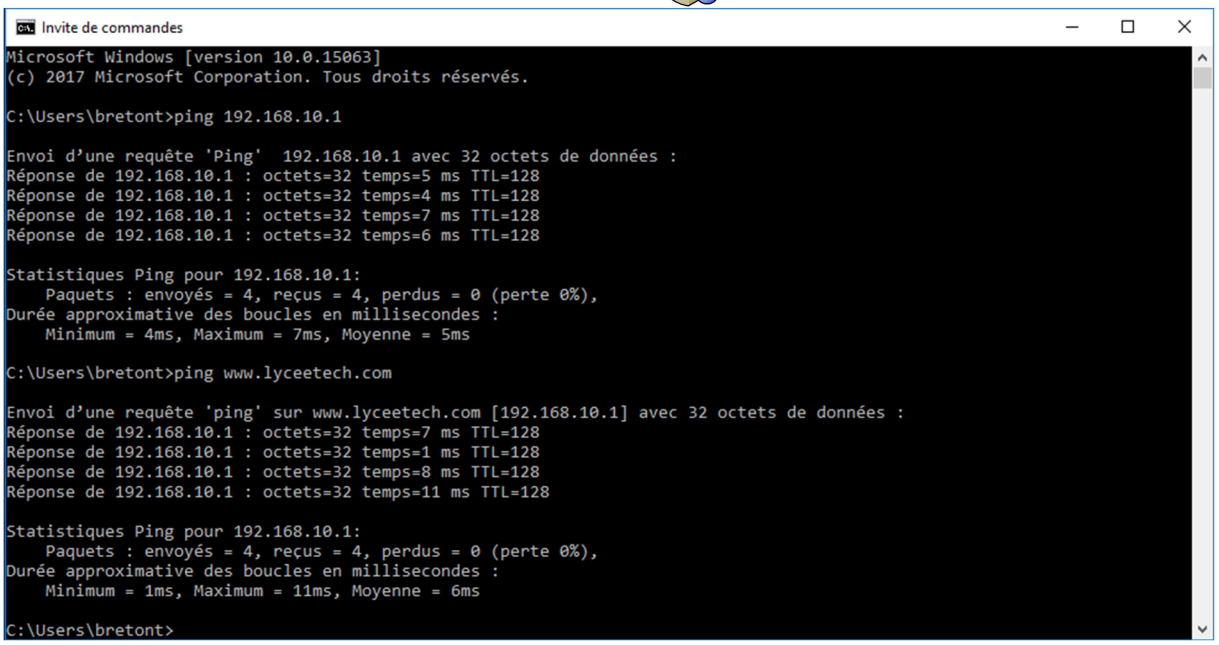





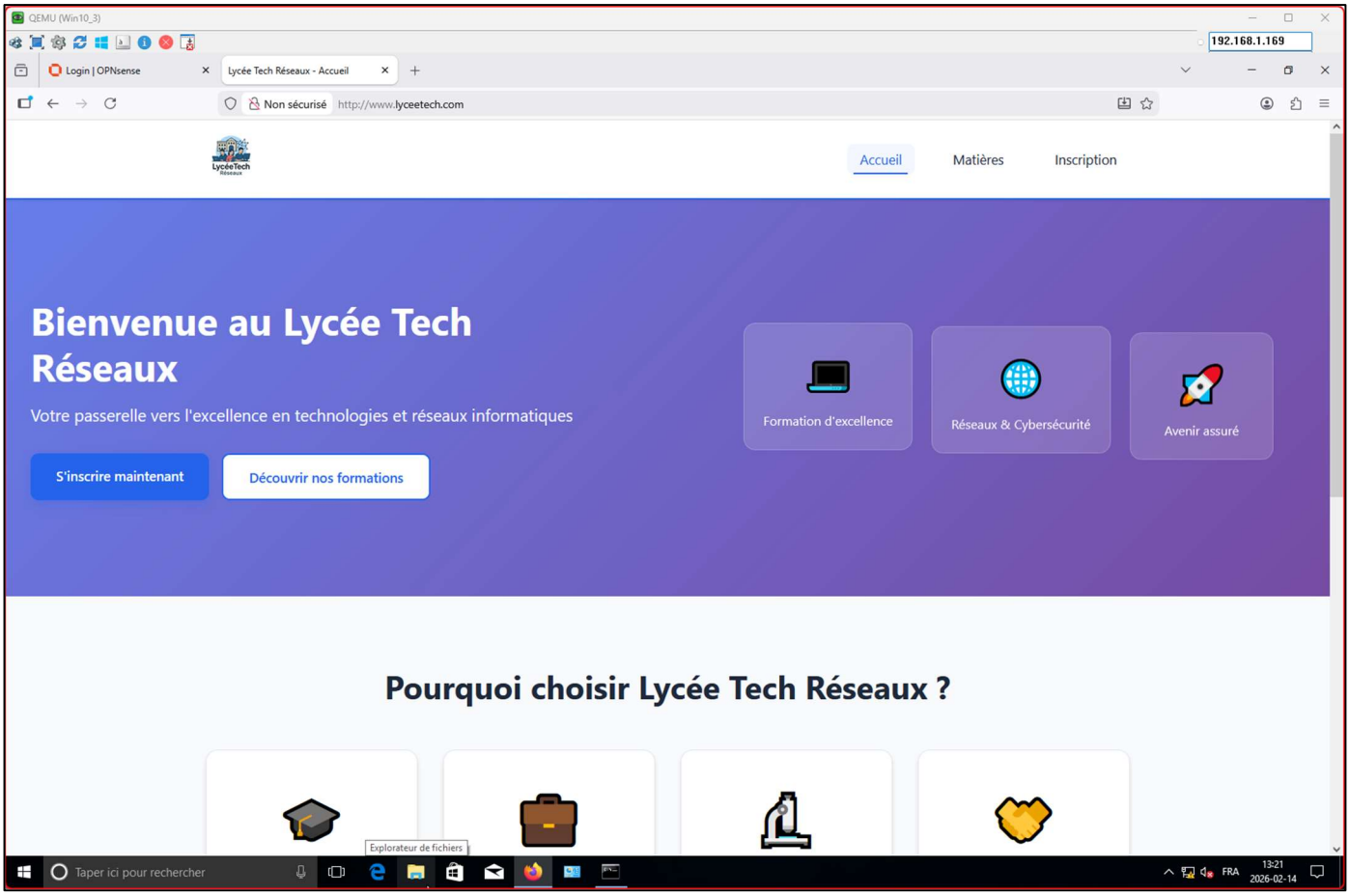

## ❷ Tester :

**Test :** Le PC Win_10_3 arrive à communiquer avec le serveur Web et à resoudre le l'URL du site Web héberger :



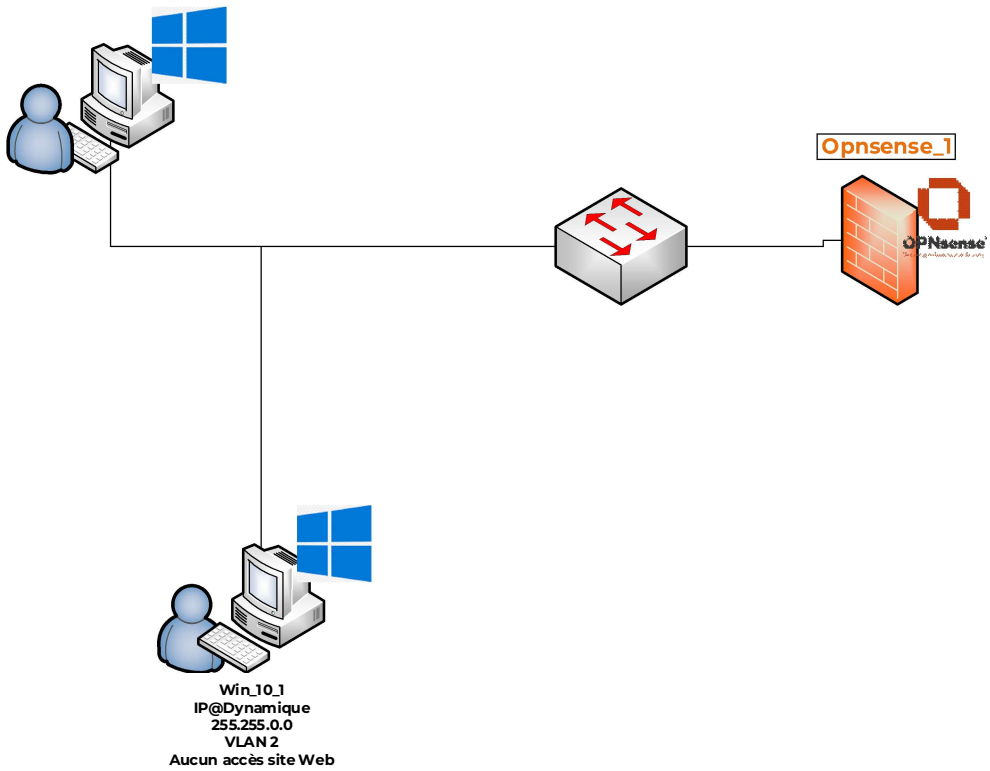



**Résultat :**




## 2ème phase du projet : Configuration des deux pare feu :

### ❶ Configuration des VM pare feu OPNsense :



**Etape 1 :** Installation de la machine virtuelle
Télécharger DVD/ISO installer le support à partir d'OPNsense:
https://opnsense.org/download/
1. Créez le dossier image OPNsense dans l'EVE-NG. Utilisez cli :

```
root@eve-ng:~# mkdir /opt/unetlab/addons/qemu/opnsense-21.1
```

2. Téléchargez l'image OPNsense-21.1-OpenSSL-dvd-amd64.iso sur l'option /opt/unetlab/addons/qemu/ opensense-21.1 en utilisant par exemple FileZilla ou WinSCP. Connectez-vous ensuite à EVE en tant que root en utilisant le protocole SSH
3. Allez dans le dossier créé et renommez l'image OPNsense-21.1-OpenSSL-dvd-amd64.iso téléchargée sur cdrom.iso:

```
root@eve-ng:~#
```

```
root@eve-ng:~# c d /opt/unetlab/addons/qemu/opnsense-21.1/
```

```
root@eve-ng:/opt/unetlab/addons/qemu/opnsense-21.1# mv OPNsense-21.1-
OpenSSL-dvd-amd64.iso cdrom.iso
```

4. Créer un disque dur pour l'installation d'image OPNsense FW. *Remarque: Taille du disque dur que vous pouvez définir selon vos besoins, dans ce cadre comment être créé 10Gb HDD*

```
root@eve-ng:~#
```

```
root@eve-ng:~# cd /opt/unetlab/addons/qemu/opnsense-21.1/
```

```
root@eve-ng:/opt/unetlab/addons/qemu/opnsense-21.1# /opt/qemu/bin/qemu-img
create -f qcow2 virtioa.qcow2 10G
```

```
Formatage 'virtioa.qcow2', fmt=qcow2 taille=10737418240 chiffrement=off
cluster_size=65536 lazy_refcounts=off refcount_bits=16
```

```
root@eve-ng:/opt/unetlab/addons/qemu/opnsense-21.1#
```

5. Correction des autorisations:

```
root@eve-ng:~# cd
```

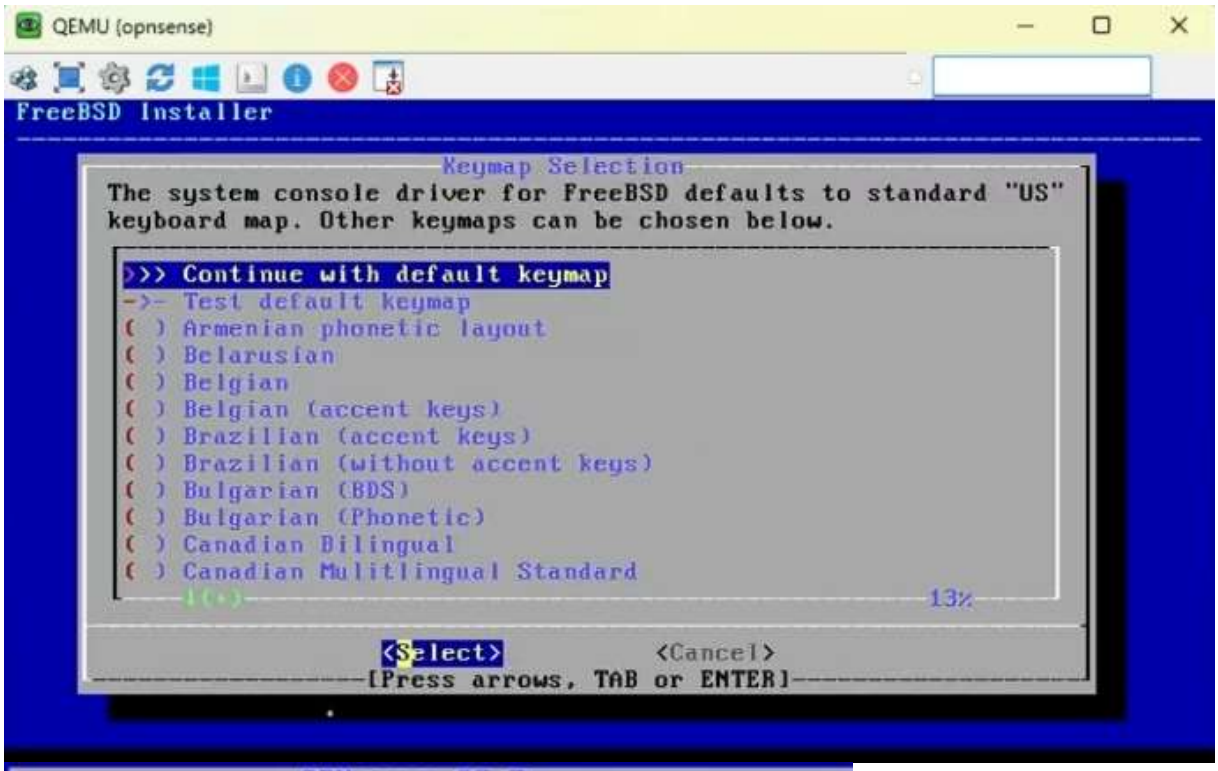
```
root@eve-ng:~# /opt/unetlab/wrappers/unl_wrapper -a fixpermissions
```

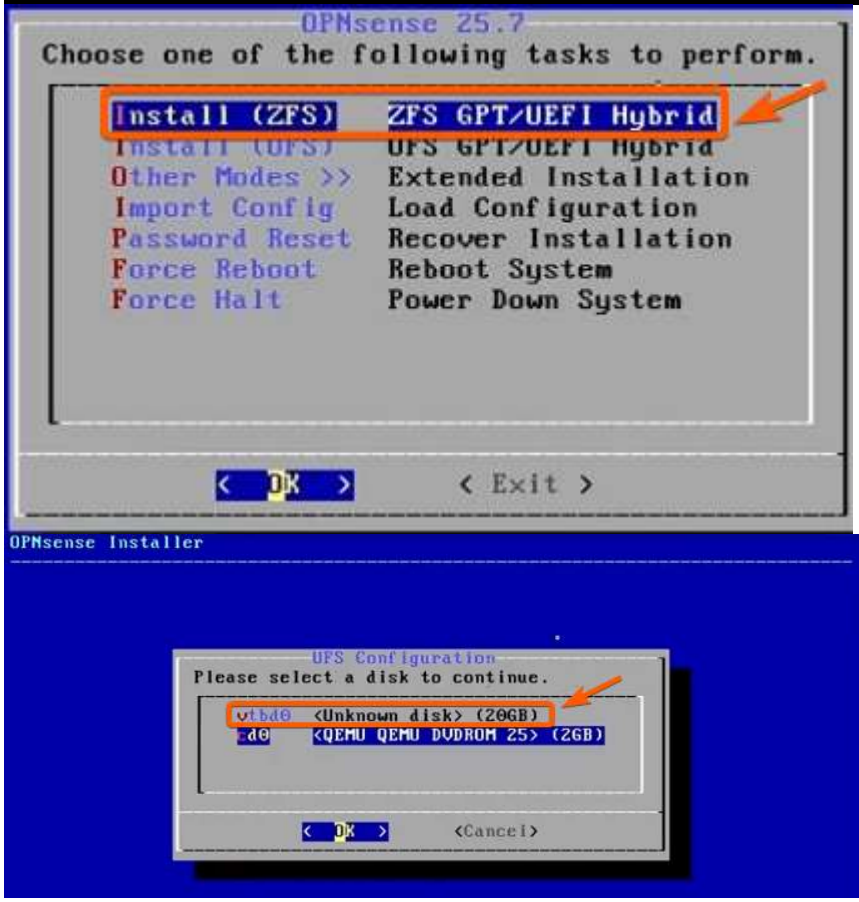
6. Créez un nouveau laboratoire EVE et ajoutez un nouveau nœud OPNsense sur la Topologie

7. Démarrez le nœud et ouvrez la console (vnc)

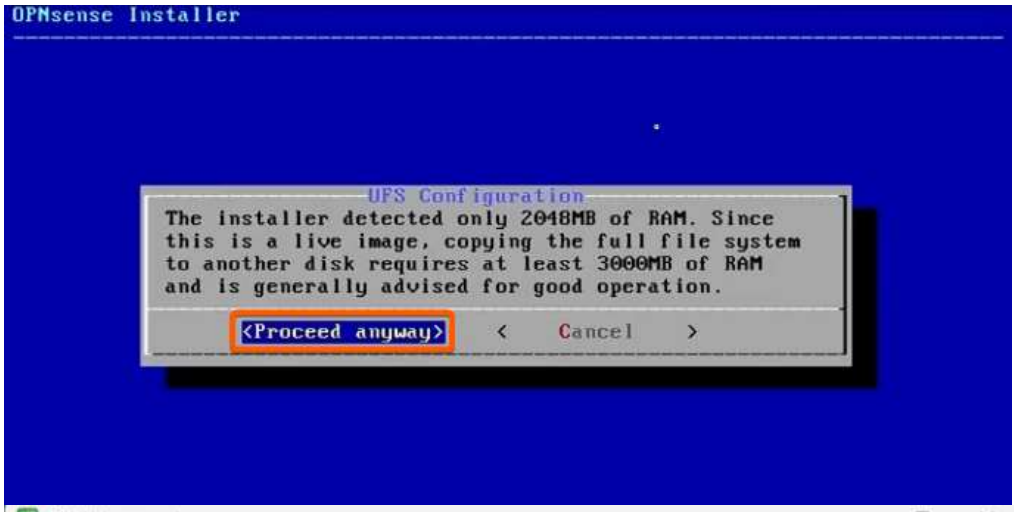
8. Attendez jusqu'à ce que le nœud démarre complètement à partir de l'ISO et utilisez la connexion avec le nom d'utilisateur: mot de passe d'installation: opensense pour démarrer l'installation OPNsense

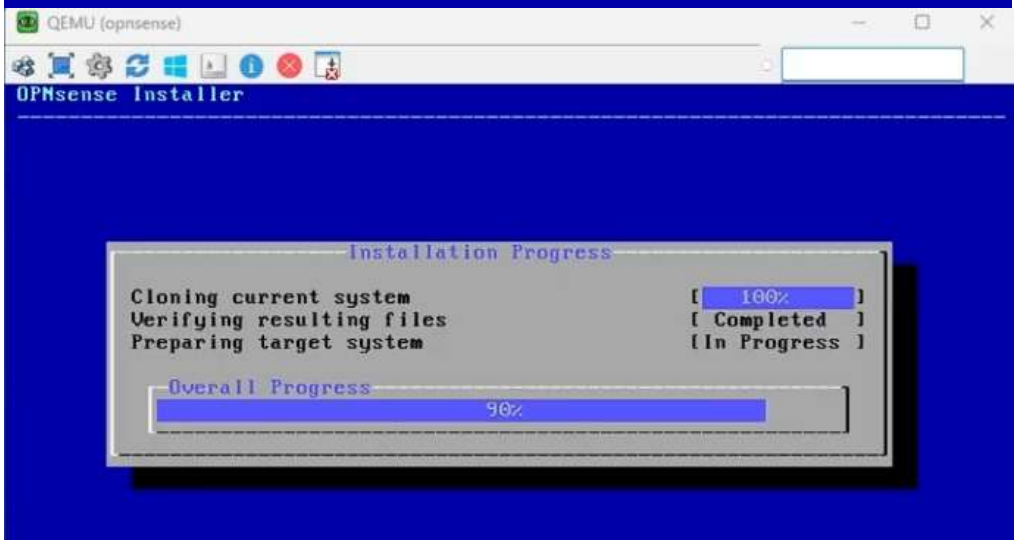
9. Utilisez tous les paramètres par défaut et l'installation complète
**login** : installer
**mot de passe** : opnsense


QEMU (opnsense)
FreeBSD Installer
Keymap Selection
The system console driver for FreeBSD defaults to standard "US" keyboard map. Other keymaps can be chosen below.
>>> Continue with default keymap
-->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Canadian Mulitlingual Standard
13%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

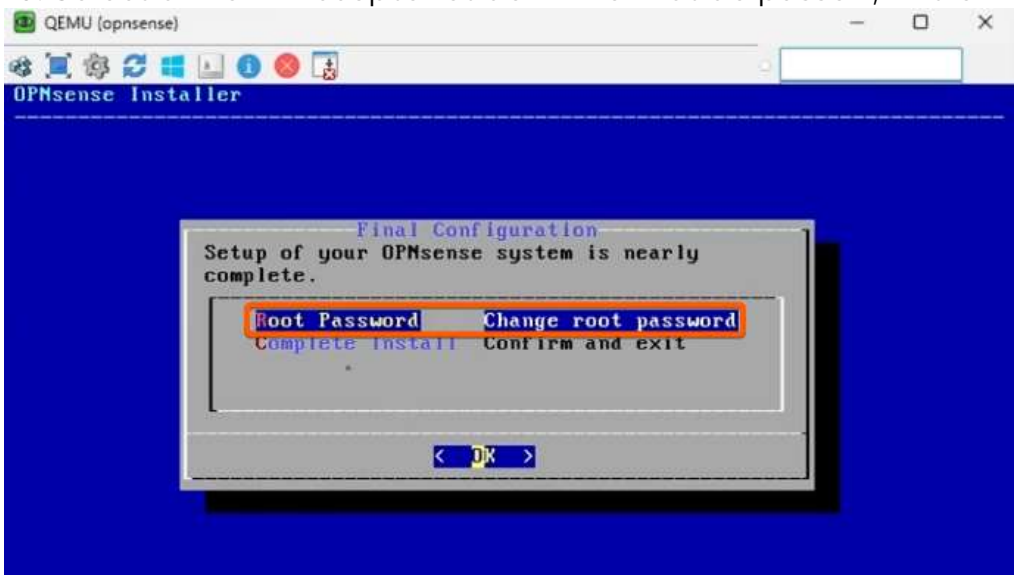

OPNsense 25.7
Choose one of the following tasks to perform.
Install (ZFS) ZFS GPT/UEFI Hybrid
Install (UFS) UFS GPT/UEFI Hybrid
Other Modes >> Extended Installation
Import Config Load Configuration
Password Reset Recover Installation
Force Reboot Reboot System
Force Halt Power Down System
< OK >
< Exit >


OPNsense Installer
UFS Configuration
Please select a disk to continue.
vtbd0 <Unknown disk> (20GB)
cd0 <QEMU QEMU DVDROM 25> (2GB)
< OK >
<Cancel>



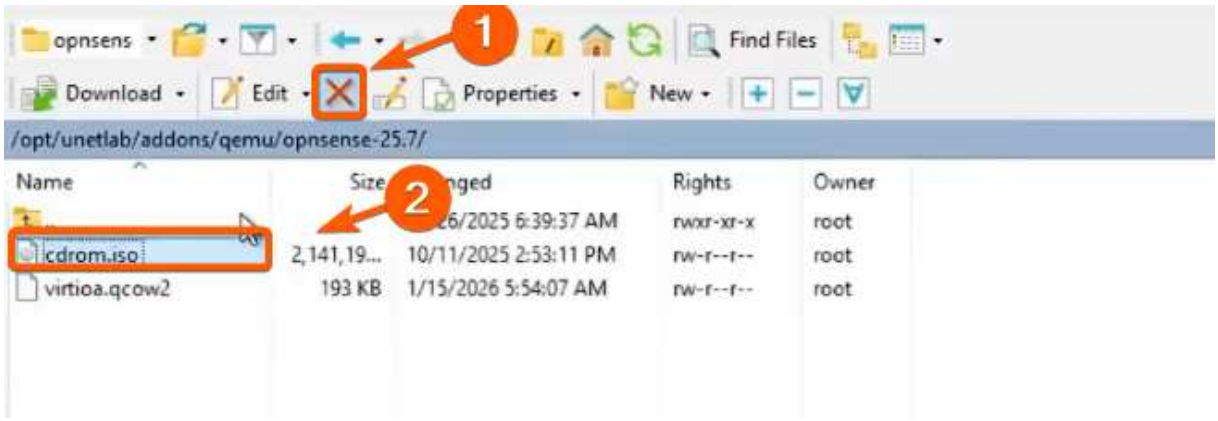




10. Sélectionnez « Accepter et définir le mot de passe », Entrez

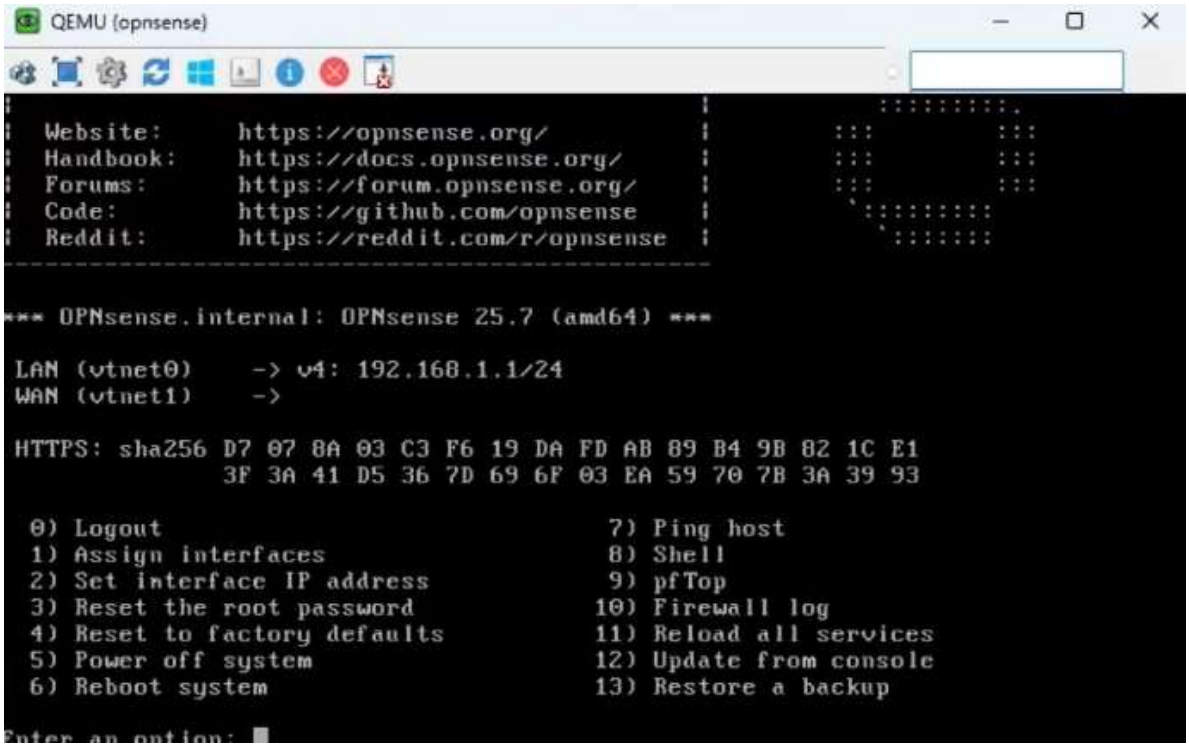



Une fois le mot de passe changer → Complete Install et le système va redémarrer.

11. Supprimer le cdrom une fois l'installation terminé :




12. Corriger les options QEMU (IMPORTANT)
Dans **Edit → Custom QEMU options**, mettre EXACTEMENT :
-machine type=pc,accel=kvm -nographic -usbdevice tablet -serial mon:stdio
**Aucune option de boot**
Pas de -boot order=dc
Pas de -cdrom
Pas de -hdb



**Etape 2 :** Configuration des interfaces WAN et LAN sur le pare-feu OPNsense :

**1) Accéder au menu de configuration**
Au démarrage d'OPNsense, le menu console apparaît.
Sélectionner :
Cliquez sur la touche « 1 » Assign interfaces

**2) Configuration des LAGG**
OPNsense demande :
Do you want to configure LAGGs now? [y/N]:
Répondre :
**N**
*(Aucun agrégat de liens n'est utilisé.)*

**3) Configuration des VLAN**
OPNsense demande :
Do you want to configure VLANs now? [y/N]:
Répondre :
**N**
*(Les VLAN ne sont pas gérés sur ce pare-feu.)*

**4) Choisir l'interface WAN**
OPNsense affiche la liste des interfaces disponibles (vtnet0, vtnet1, vtnet2, vtnet3).
Quand il demande :
Enter the WAN interface name:
Saisir :
**vtnet1**
*(Interface WAN, même si elle n'est pas utilisée.)*

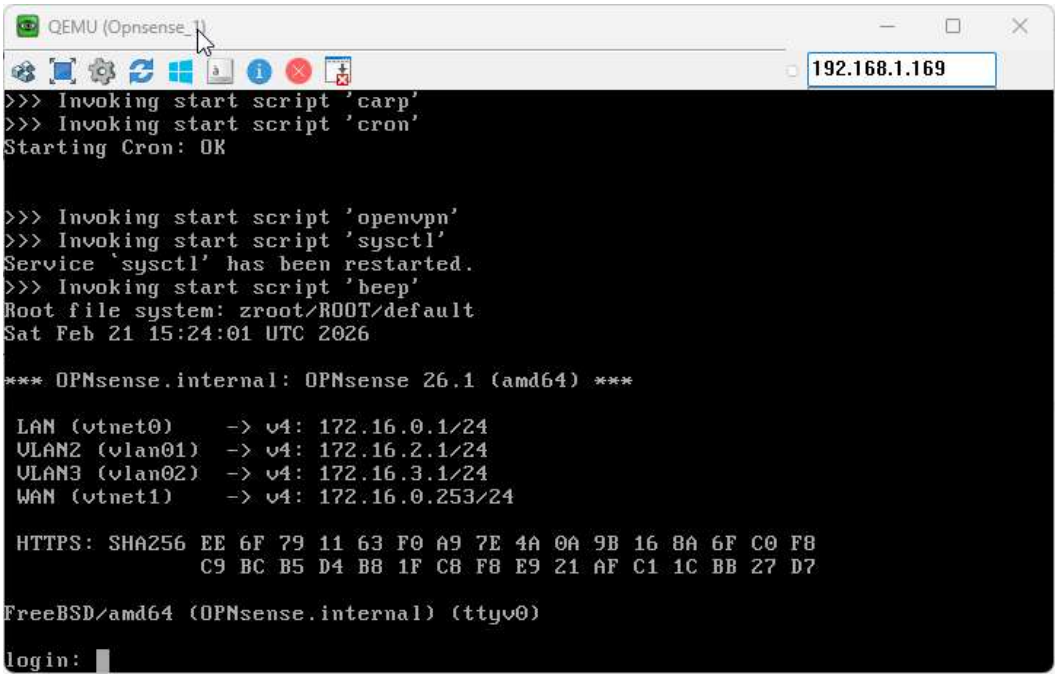
**5) Choisir l'interface LAN**
OPNsense demande :
Enter the LAN interface name:
Saisir :
vtnet0
*(Interface connectée au réseau 192.168.10.0/24.)*

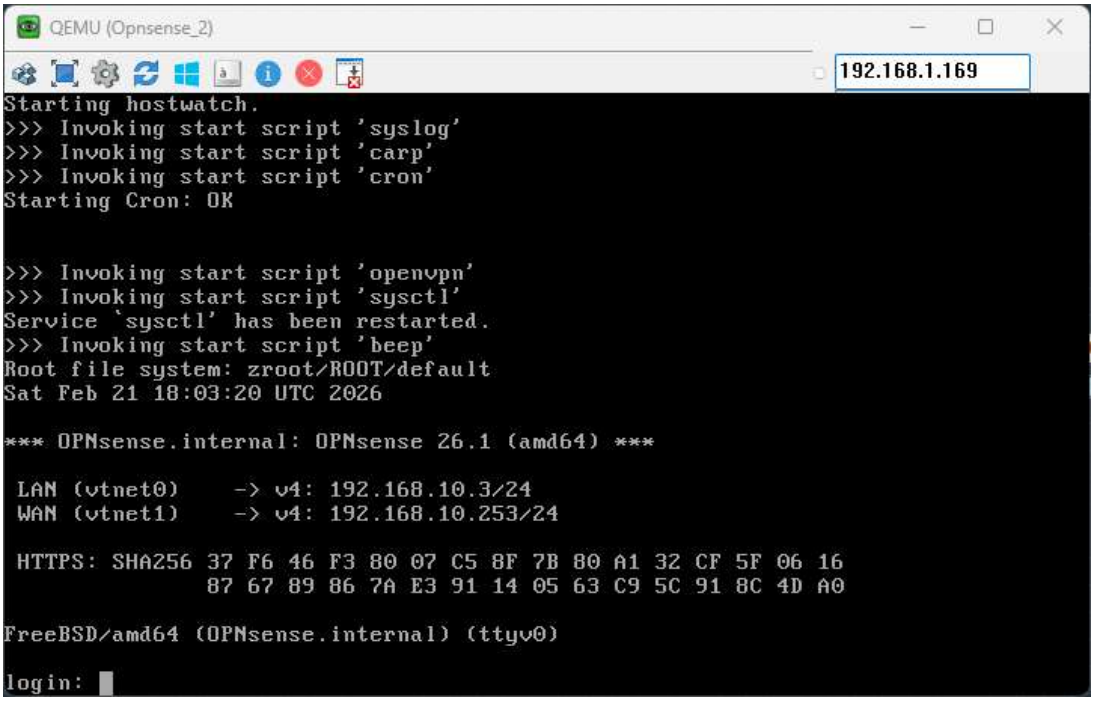
**6) Interfaces optionnelles**
OPNsense demande :
Enter the Optional interface 1 name (or nothing if finished):
Ne rien saisir → simplement appuyer sur :
Entrée

**7) Confirmation**
OPNsense affiche un résumé :
WAN -> vtnet1
LAN -> vtnet0
Puis demande :
Do you want to proceed? [y/N]:
Répondre : **Y**

**8) Configurer l'adresse IP du LAN**
Revenir au menu principal, puis choisir :
2) Set interface IP address
Sélectionner **LAN**.
Configurer :
**IP Address : 192.168.10.254**
**Subnet mask : 24**
**Gateway :** *laisser vide*
**DHCP server : N**
**IPv6 : ignorer / désactiver**
Valider

Maintenant que mes pares-feux sont opérationnels je peux accéder à l'interface Web depuis un VM Windows 10 Client pour les configurer.



## 3ème phase du projet : Configuration du pare-feu OPNsense_1 :

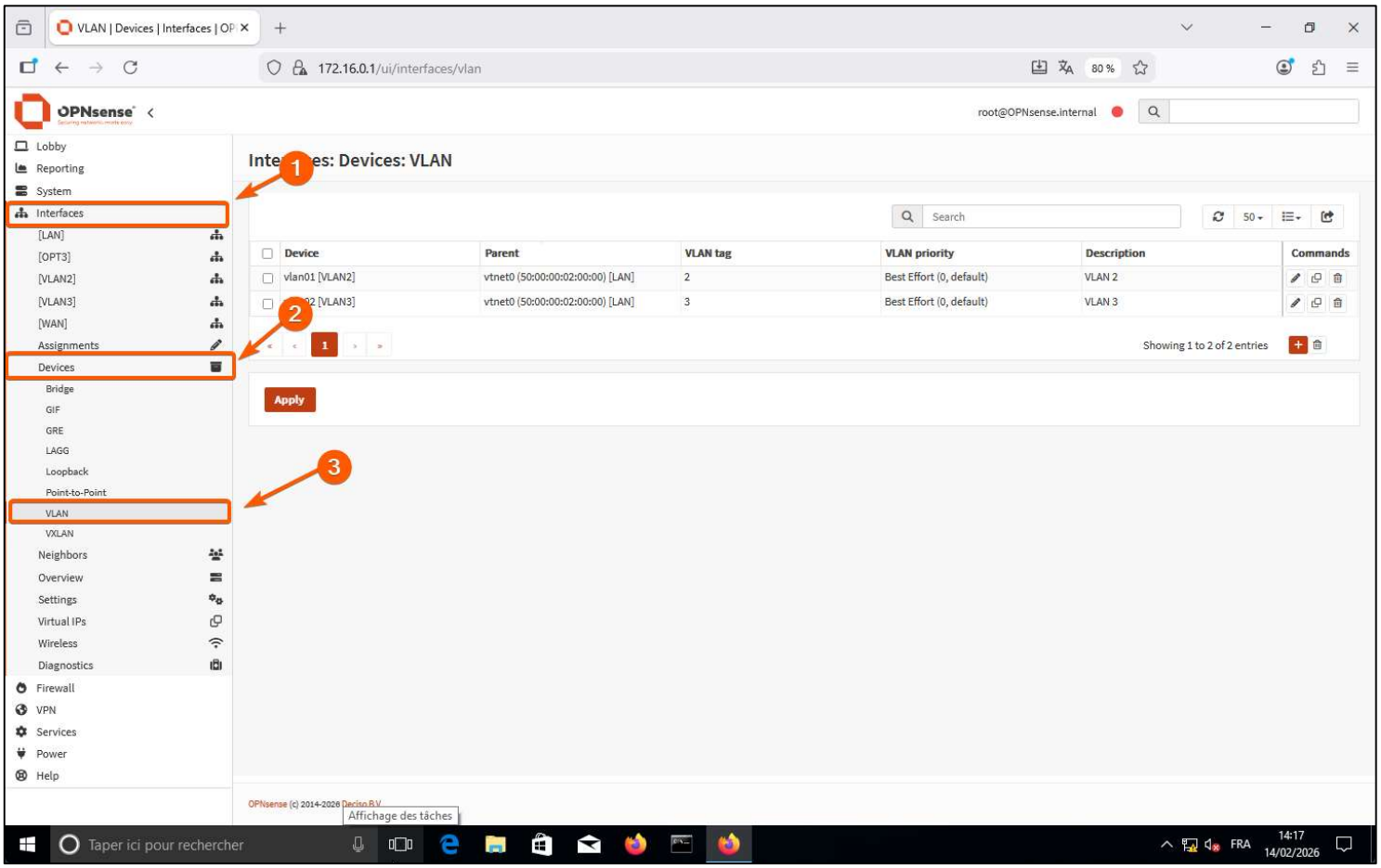
**Etape 1 :** Configuration des VLAN2 et VLAN3 sur le pare-feu **OPNsense_1** :

### 1. Création des VLANs dans OPNsense

Aller dans le menu VLAN

Dans le menu de gauche :

**Interfaces → VLAN**



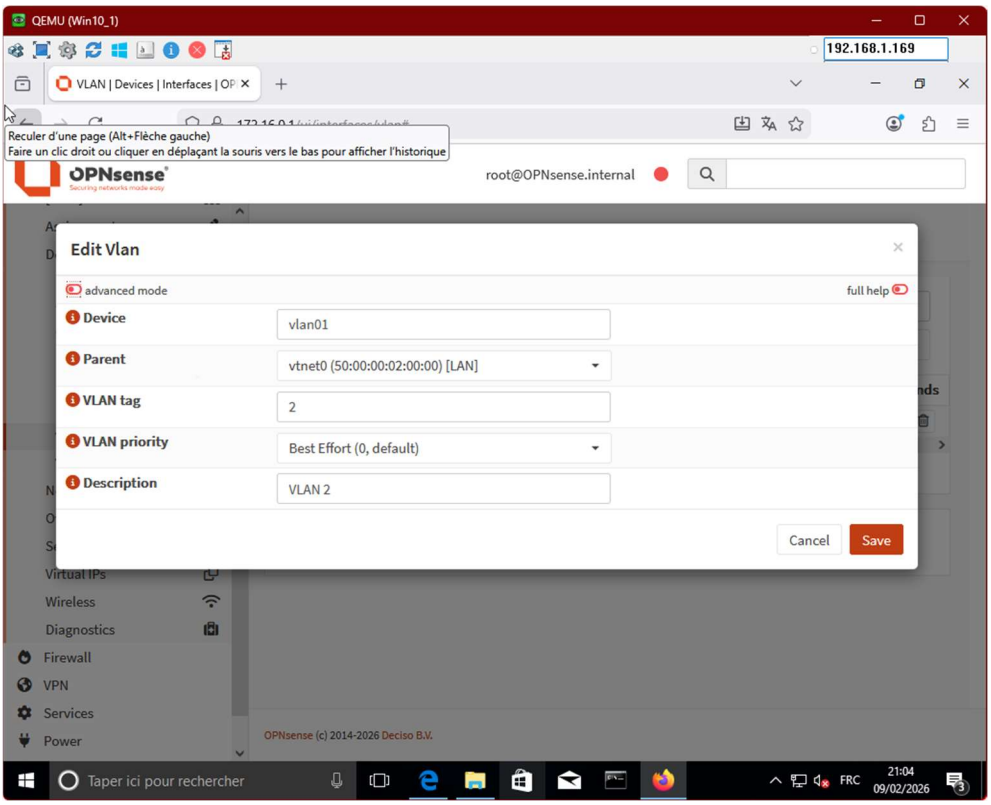

### 2. Créer un VLAN

Cliquer sur **+ Add**.

Remplir les champs :

- **Parent interface** : l'interface reliée au switch (souvent vtnet1)
- **VLAN tag** : numéro du VLAN (ex : 2)
- **Description** : VLAN2

Cliquer **Save**.

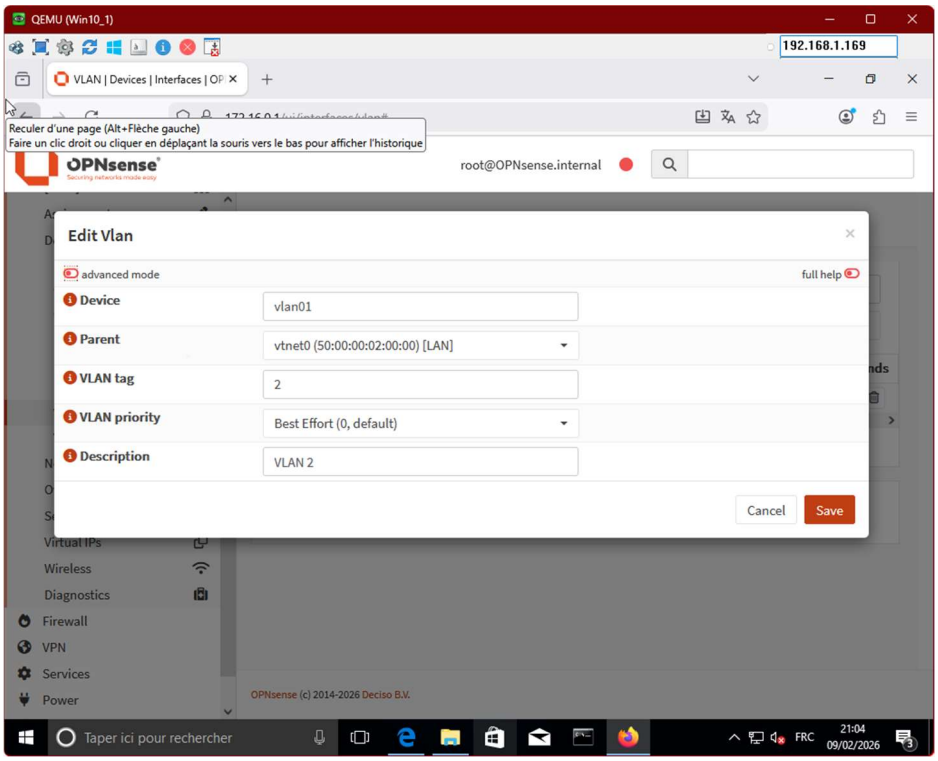



### 3. Créer le deuxième VLAN

Refaire la même manipulation :

- Parent interface : vtnet1
- VLAN tag : 3
- Description : VLAN3

Puis **Save**.



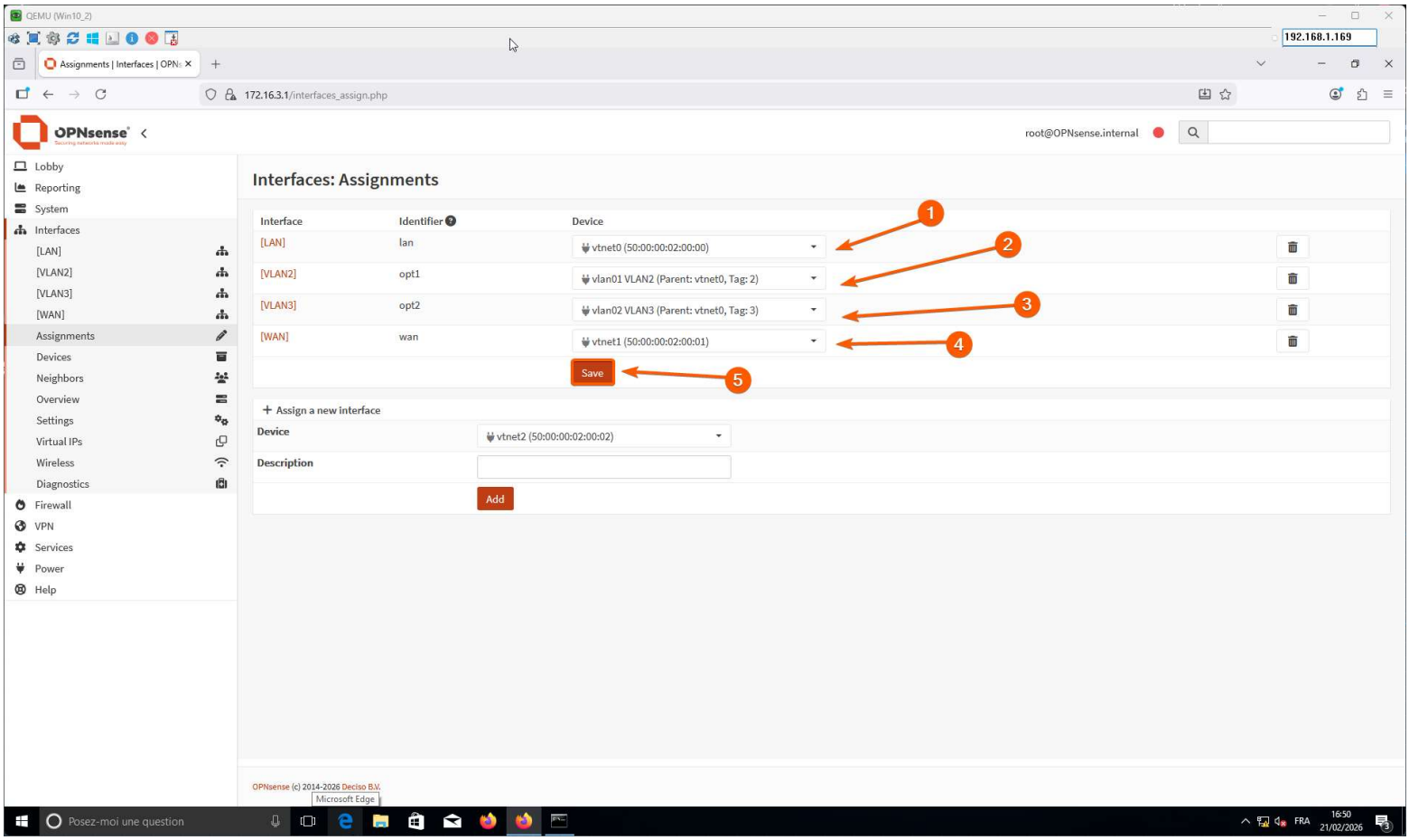
**4. Assigner les VLANs comme interfaces**
Aller dans :
**Interfaces → Assignments**

Dans la liste déroulante en bas, sélectionner :

vlan01 → cliquer **Add**

vlan02 → cliquer **Add**

On obtient deux nouvelles interfaces : **OPT1** et **OPT2**.



## 5. Activer et configurer les VLANs

**Pour OPT1 (VLAN2)**
Aller dans :
**Interfaces → VLAN2** *(ou Interfaces → OPT1 si tu ne l'as pas encore renommée)*

Cocher **Enable interface**

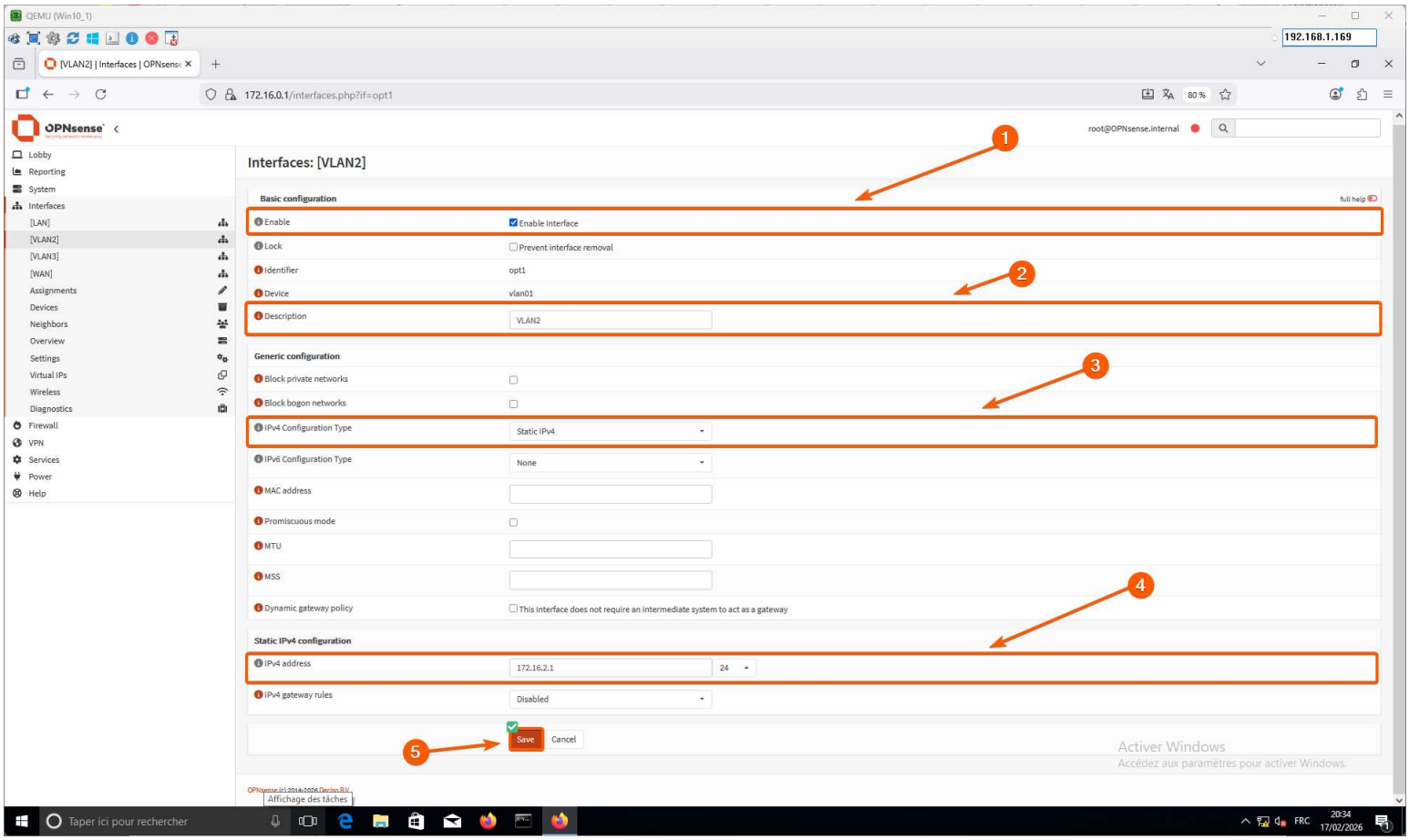
**Description** : VLAN2

**IPv4 Configuration Type** : Static IPv4

**IPv4 Address** : 172.16.2.1 /24

**IPv6 Configuration Type** : None

Cliquer **Save**, puis **Apply Changes** ⚠



**Pour OPT2 (VLAN3)**
Aller dans :
**Interfaces → VLAN3** *(ou Interfaces → OPT2 si pas encore renommée)*

Cocher **Enable interface**

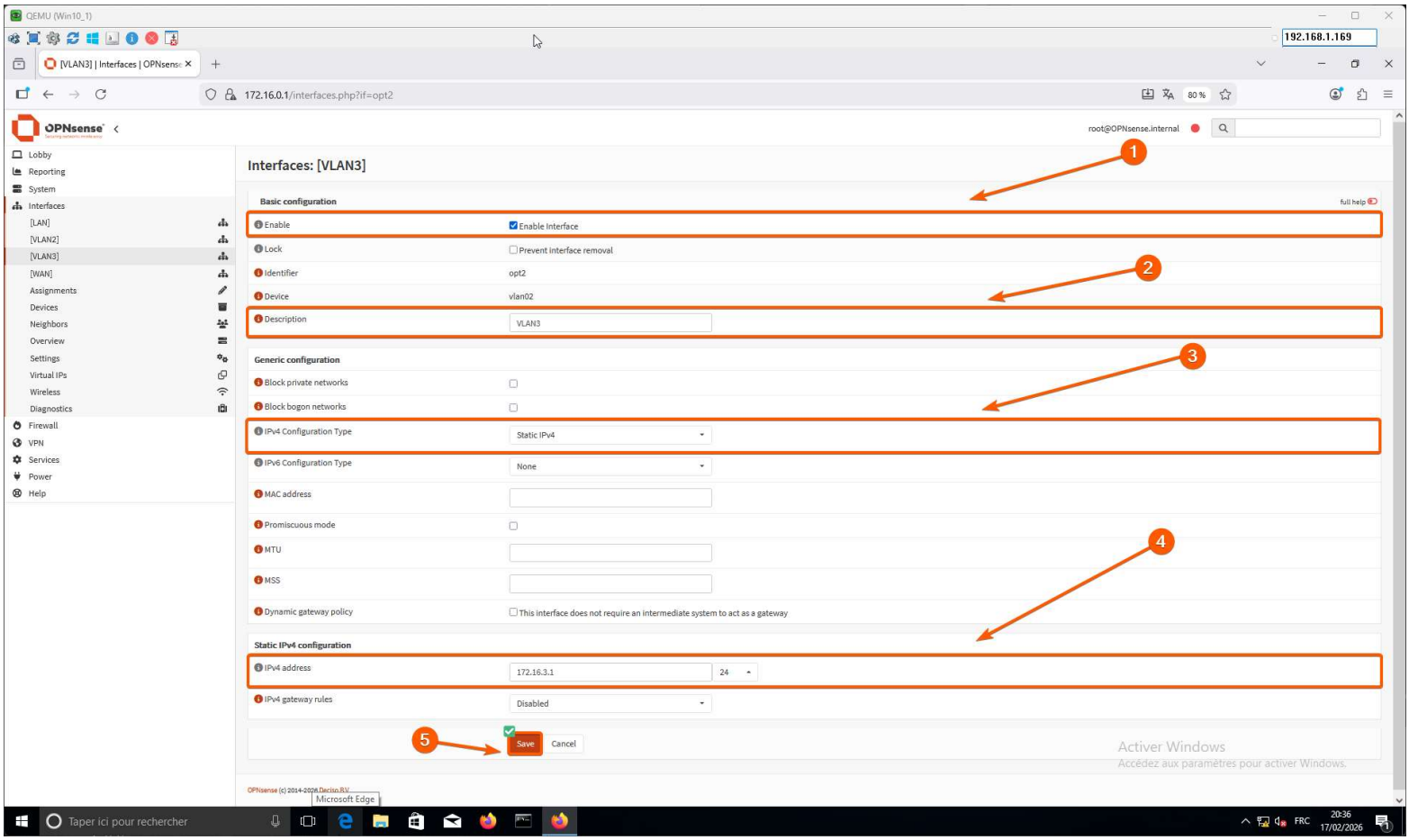
**Description** : VLAN3

**IPv4 Configuration Type** : Static IPv4

**IPv4 Address** : 172.16.3.1 /16

**IPv6 Configuration Type** : None

**Save**, puis **Apply Changes** ⚠



## 6. Configurer la passerelle pour l'interface WAN

Aller dans :
**System → Gateways → Configuration**

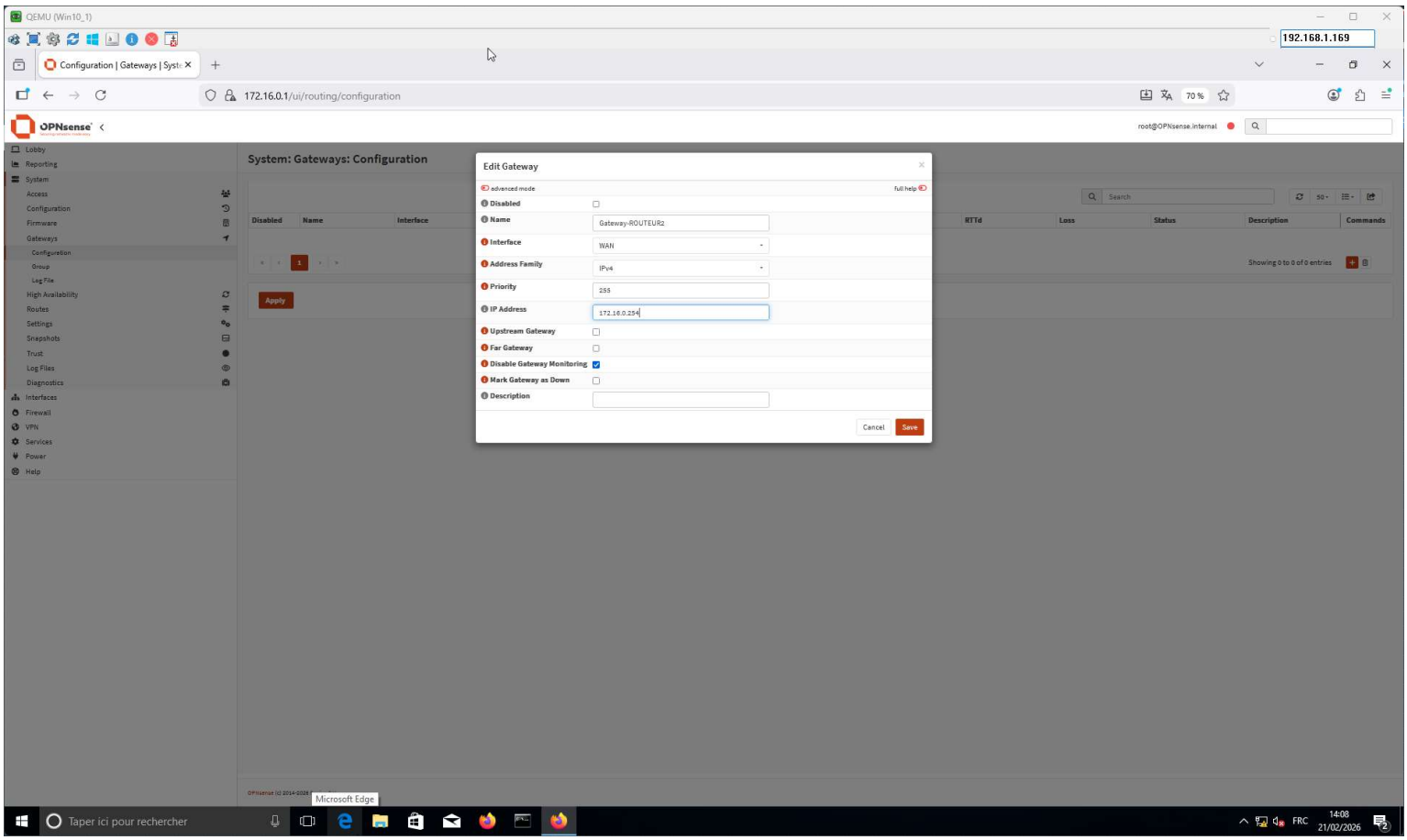
Décocher **Disabled**

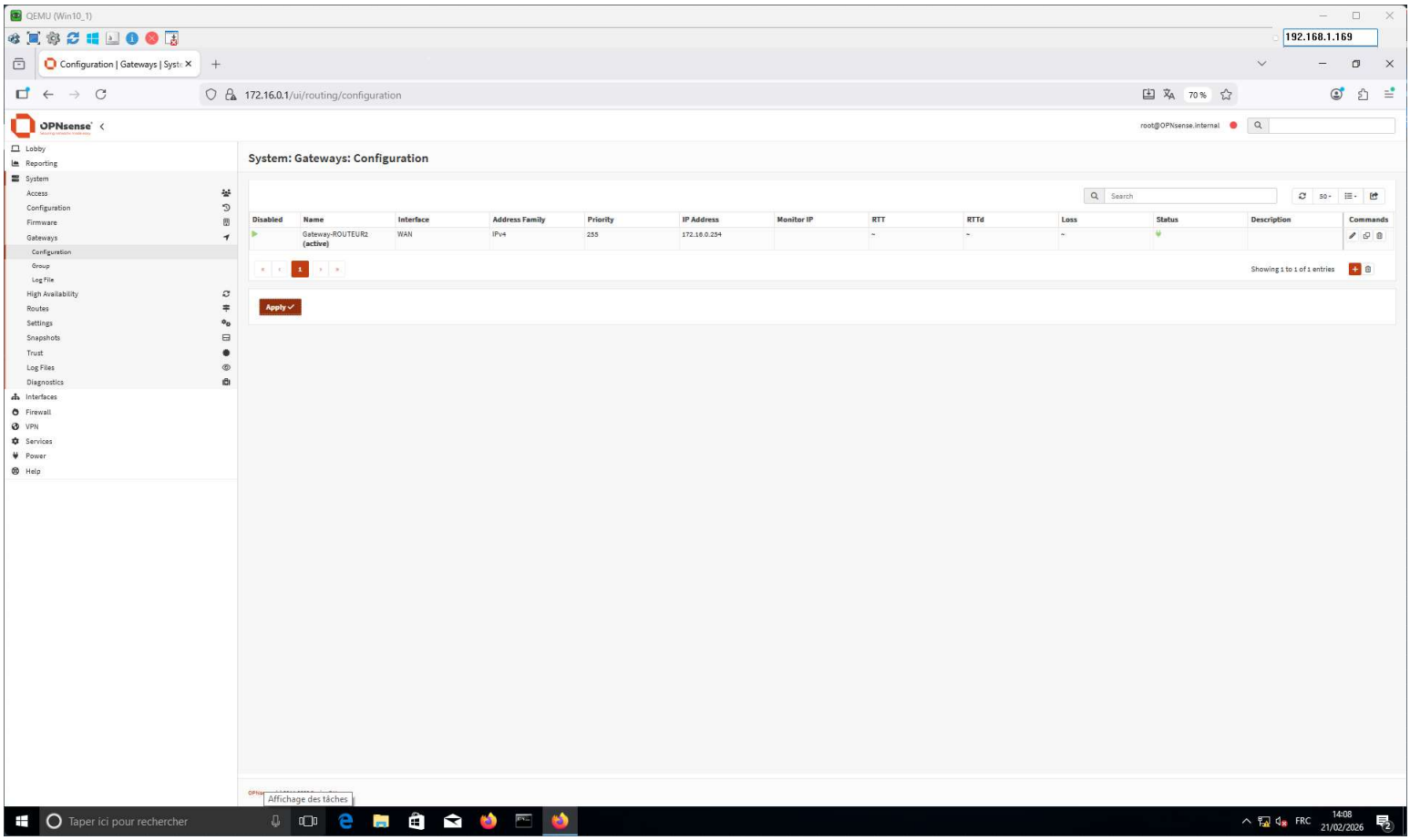
**Description** : Gateway-ROUTEUR2

**IPv4 Configuration Type** : Static IPv4

**IPv4 Address** : 172.16.0.254

**Save**, puis **Apply Changes** ⚠




QEMU (Win10_1)
192.168.1.169
Configuration | Gateways | Syst
172.16.0.1/ui/routing/configuration
OPNsense
root@OPNsense.internal
Lobby
Reporting
System
Access
Configuration
Firmware
Gateways
Configuration
Group
Log File
High Availability
Routes
Settings
Snapshots
Trust
Log Files
Diagnostics
Interfaces
Firewall
VPN
Services
Power
Help
System: Gateways: Configuration
Search
Disabled
Name
Interface
Address Family
Priority
IP Address
Monitor IP
RTT
RTTd
Loss
Status
Description
Commands
Gateway-ROUTEUR2 (active)
WAN
IPv4
255
172.16.0.254
Showing 1 to 1 of 1 entries
Apply
Affichage des tâches
Taper ici pour rechercher
FRC
14:08
21/02/2026

## 7. Configuration de l'interface WAN

**Interfaces → WAN**

Cocher **Enable Interfaces**

**Décocher les cases suivantes :**

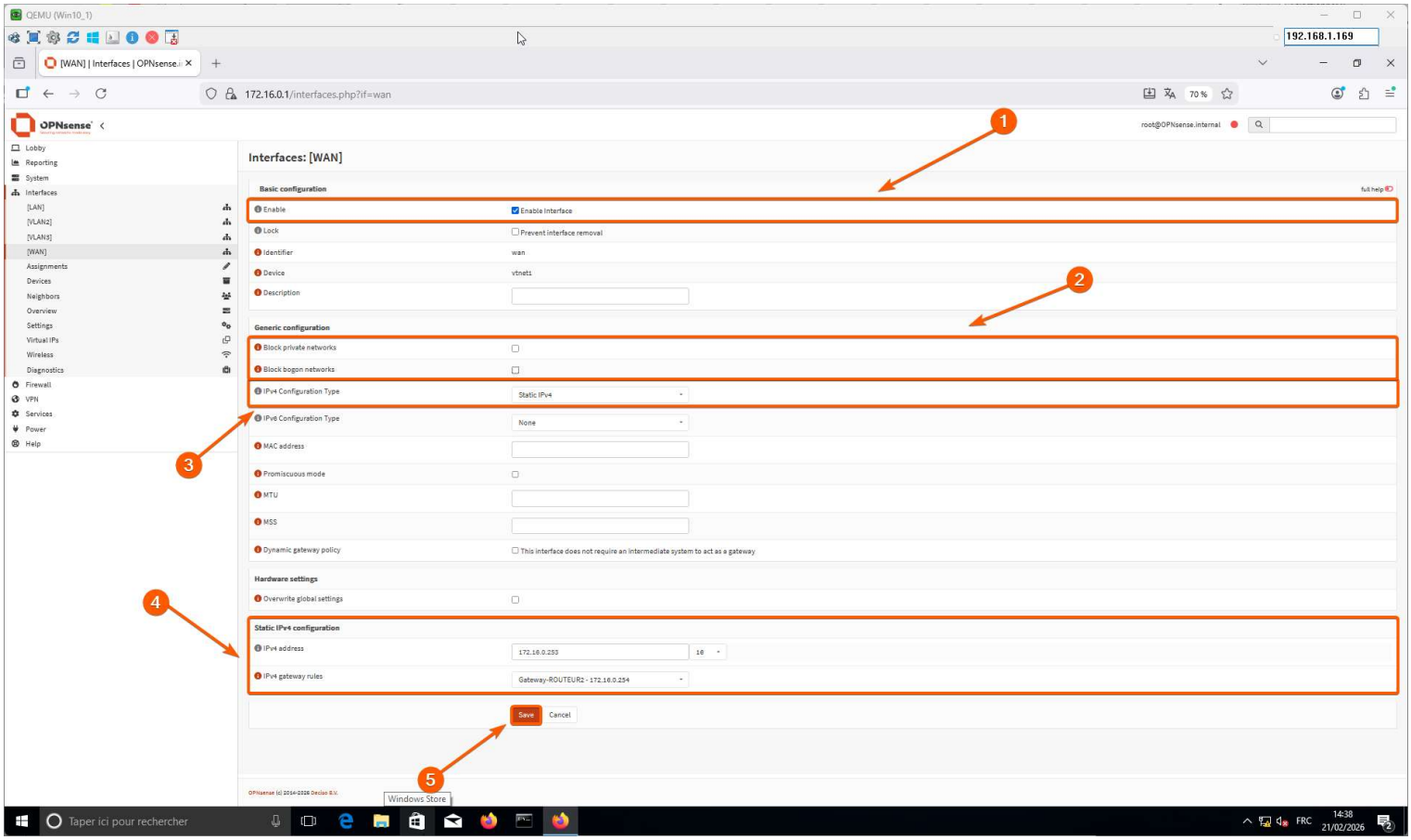
- ❒ **Block private networks** → Interdit les IPs type 192.168.x.x, 172.16.x.x ou 10.x.x.x sur le WAN.
- ❒ **Block bogon networks** → Interdit les IPs qui n'existent pas officiellement sur le web (IPs non assignées).

**IPv4 Configuration Type** : Static IPv4

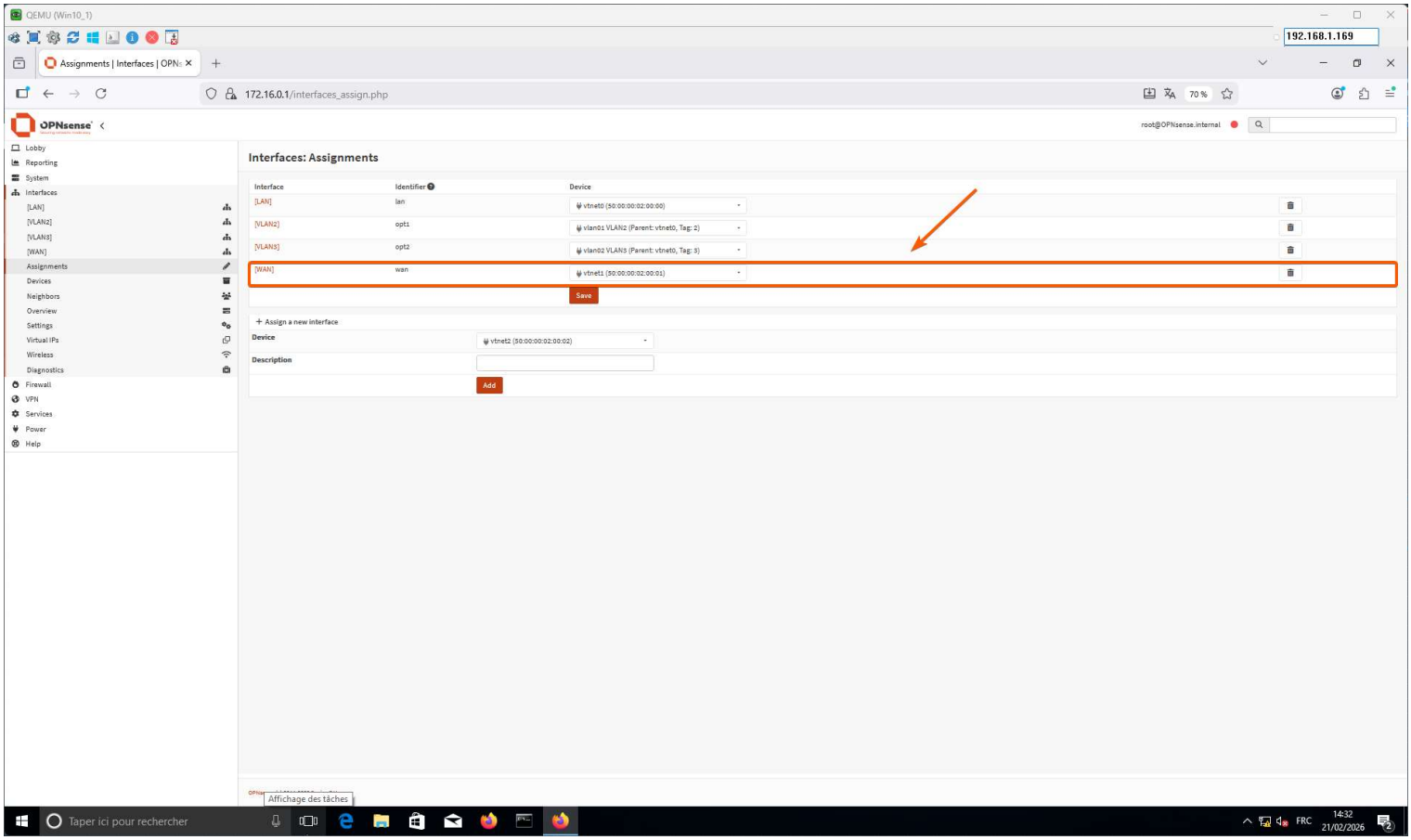
**IPv4 Address** : 172.16.0.253/16

**IPv4 gateway rules** : 172.16.0.254

**Save**, puis **Apply Changes** ❗



## Assigné l’interface vtnet1 au WAN :



**Etape 2 :** Configuration des règles du **OPNsense_1** :

## Rappel du cahier de charges :

- Autoriser les PC du bâtiment A (VLAN2 et VLAN3) à sortir vers l'extérieur
- Autoriser l'accès au bâtiment B (serveur 192.168.10.x)
- Garder une segmentation propre entre VLAN2 et VLAN3
- Laisser le LAN (172.16.0.1) intact pour l'administration

### 1. Aller dans les règles du pare-feu

Menu :
**Firewall → Rules**
Tu vas voir une liste d'interfaces :

- LAN
- VLAN2
- VLAN3

On va configurer **VLAN2** et **VLAN3**

### 2. Règles pour VLAN2

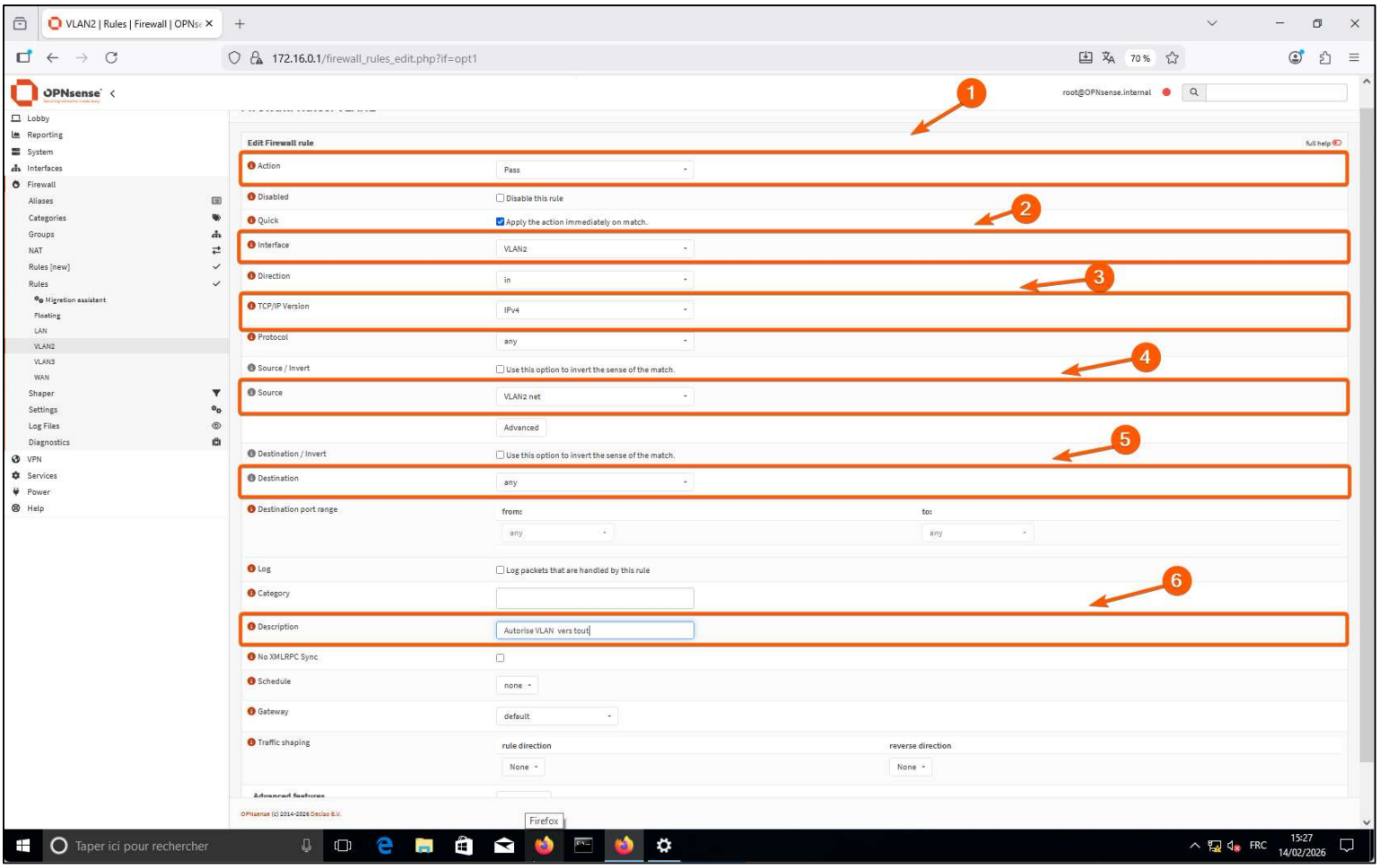
***Aller dans***
***Firewall → Rules → VLAN2***

***Ajouter une règle PASS***
En haut → cliquer sur **+ Add**

Puis configure :

- ***Action*** *: Pass*
- ***Interface*** *: VLAN2*
- ***Direction*** *: In*
- ***TCP/IP Version*** *: IPv4*
- ***Protocol*** *: any*
- ***Source*** *: VLAN2 net*
- ***Destination*** *: any*
- ***Description*** *: Autoriser VLAN2 vers tout*

Puis :
Cliquer **Save**, puis **Apply Changes**




### 3. Règles pour le VLAN3

**Première règle qui va autoriser le ping entre le Win_10_2 et le ServeurWeb :**

**Aller dans**
**Firewall → Rules → VLAN3**

**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

Puis configure :

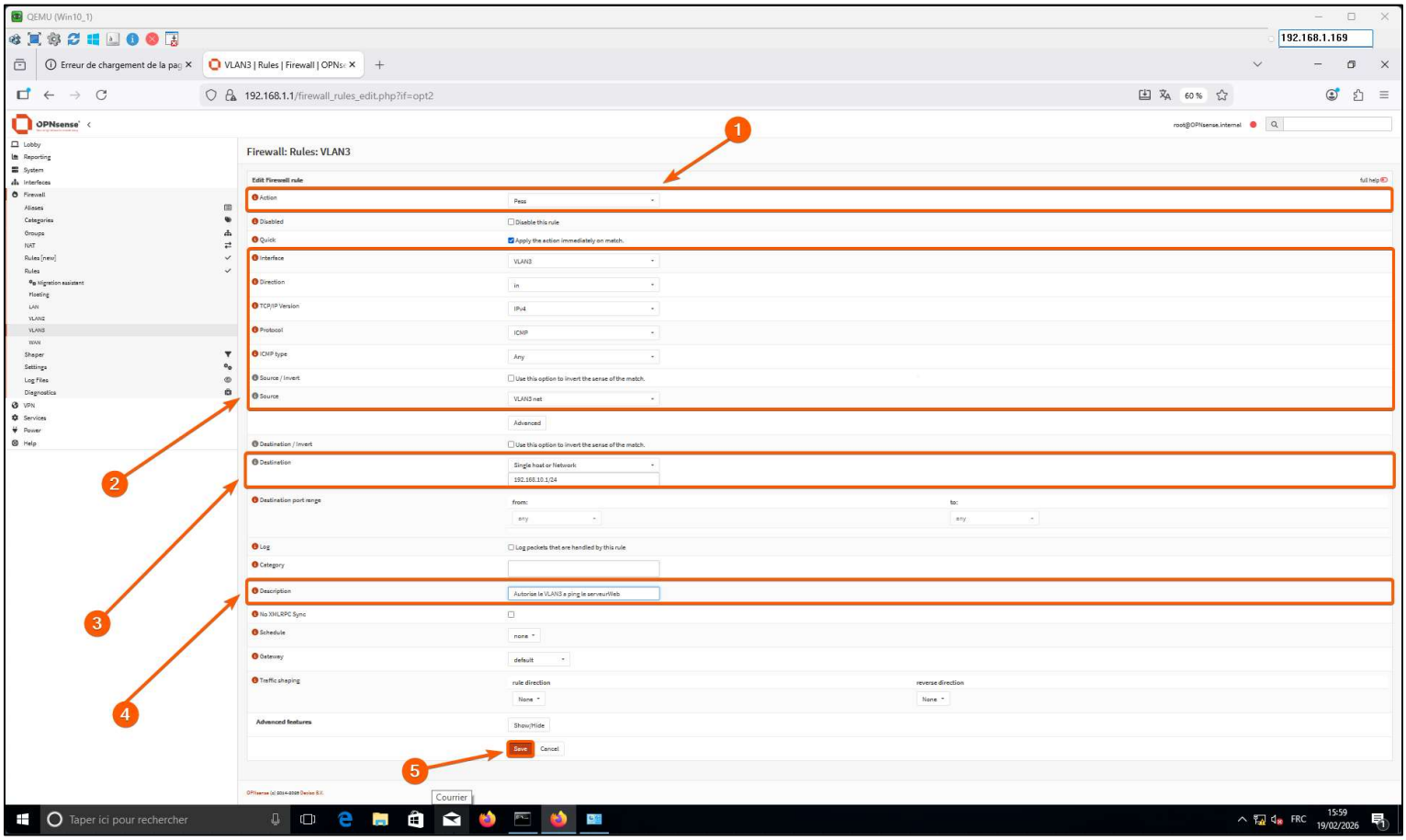
- **Action** : Pass
- **Interface** : VLAN3
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : ICMP

  → Ça veut dire : **VLAN3 peut ping le site, mais pas encore y accéder en HTTP/HTTPS**.

- **Source** : VLAN3 net
- **Destination** : 192.168.10.1/24
- **Description** : Autoriser VLAN3 à ping le serveur Web

Puis :

Cliquer **Save**, puis **Apply Changes** ⚠




**Deuxième règle qui va autoriser VLAN3 à accèder au site web du ServeurWeb :**

**Aller dans**
**Firewall → Rules → VLAN3**

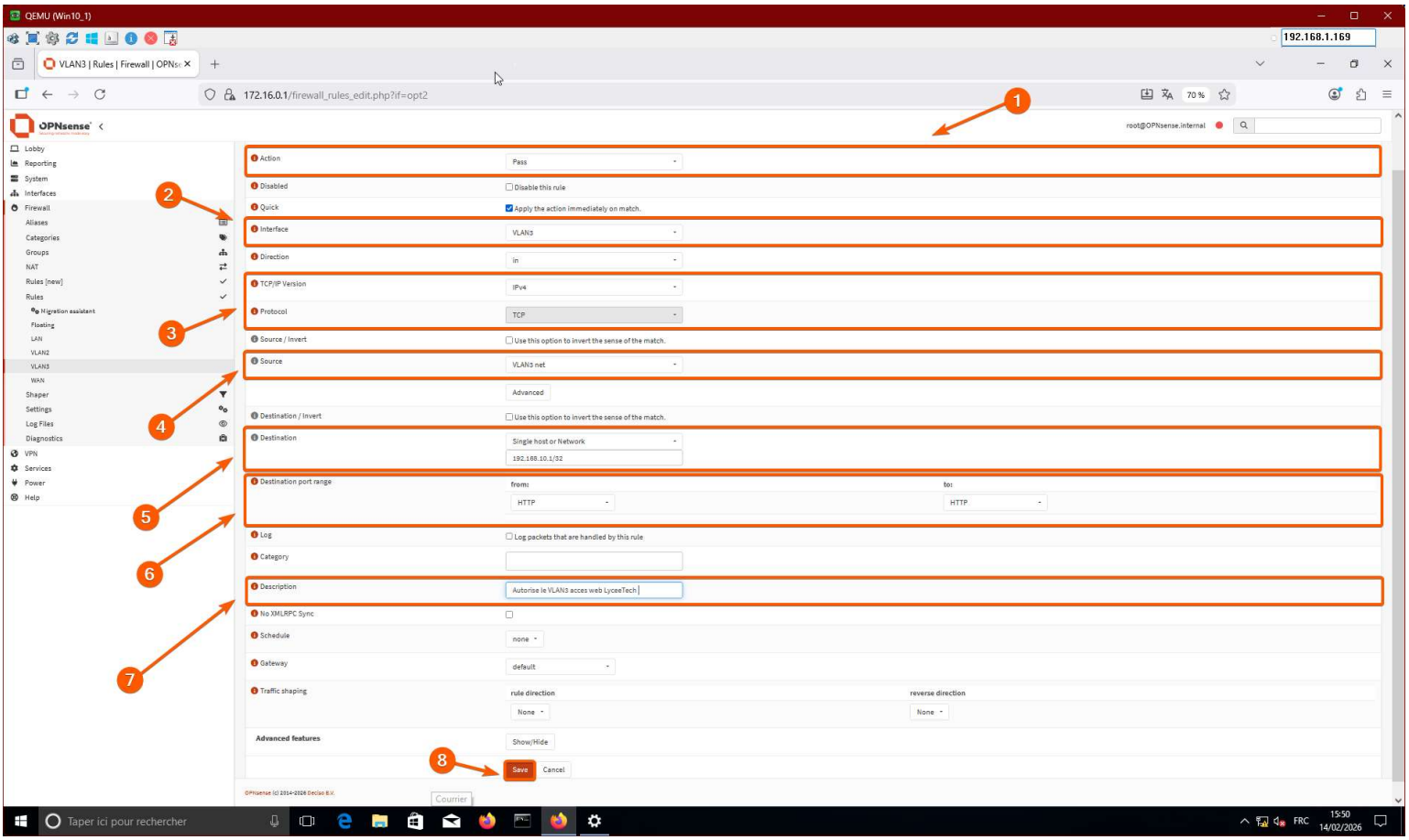
**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

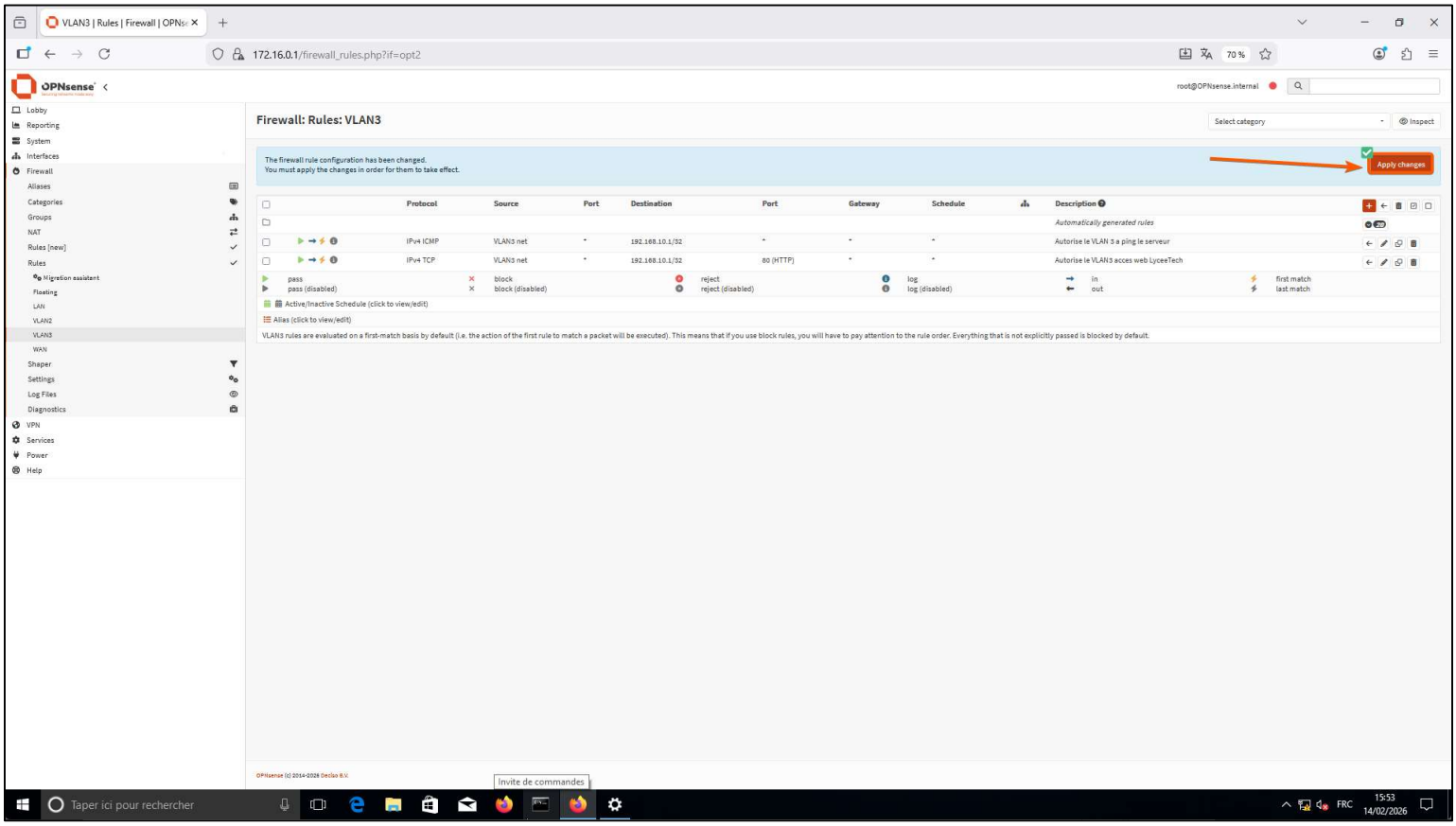
Puis configure :

- **Action** : Pass
- **Interface** : VLAN3
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : TCP
- **Source** : VLAN3 net
- **Destination** : 192.168.10.1/32
- **Destination port range**
  - ☞ From : HTTP (80)
  - ☞ To : HTTP (80)
- **Description** : Autoriser le VLAN3 accès web LyceeTech (HTTP)

Puis :

Cliquer **Save**, puis **Apply Changes** ❗


QEMU (Win10_1)
192.168.1.169
VLAN3 | Rules | Firewall | OPNs
172.16.0.1/firewall_rules_edit.php?if=opt2
OPNsense
root@OPNsense.internal
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules [new]
Rules
Migration assistant
Floating
LAN
VLAN2
VLAN3
WAN
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
Help
Action
Pass
Disabled
Disable this rule
Quick
Apply the action immediately on match.
Interface
VLAN3
Direction
in
TCP/IP Version
IPv4
Protocol
TCP
Source / Invert
Use this option to invert the sense of the match.
Source
VLAN3 net
Advanced
Destination / Invert
Use this option to invert the sense of the match.
Destination
Single host or Network
192.168.10.1/32
Destination port range
from:
HTTP
to:
HTTP
Log
Log packets that are handled by this rule
Category
Description
Autorise le VLAN3 acces web LyceeTech
No XMLRPC Sync
Schedule
none
Gateway
default
Traffic shaping
rule direction
None
reverse direction
None
Advanced features
Show/Hide
Save
Cancel
1
2
3
4
5
6
7
8
Taper ici pour rechercher
FRC
15:50
14/02/2026


VLAN3 | Rules | Firewall | OPNs
172.16.0.1/firewall_rules.php?if=opt2
OPNsense
root@OPNsense.internal
Firewall: Rules: VLAN3
Select category
Inspect
The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.
Apply changes
Protocol
Source
Port
Destination
Port
Gateway
Schedule
Description
Automatically generated rules
IPv4 ICMP
VLAN3 net
192.168.10.1/32
Autorise le VLAN 3 a ping le serveur
IPv4 TCP
VLAN3 net
192.168.10.1/32
80 (HTTP)
Autorise le VLAN3 acces web LyceeTech
pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)
in
out
first match
last match
Active/Inactive Schedule (click to view/edit)
Alias (click to view/edit)
VLAN3 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.
Invite de commandes
Taper ici pour rechercher
FRC
15:53
14/02/2026

## Troisième règle qui va autoriser tous les protocoles sur le l'interface du VLAN3

**Aller dans**
**Firewall → Rules → VLAN3**

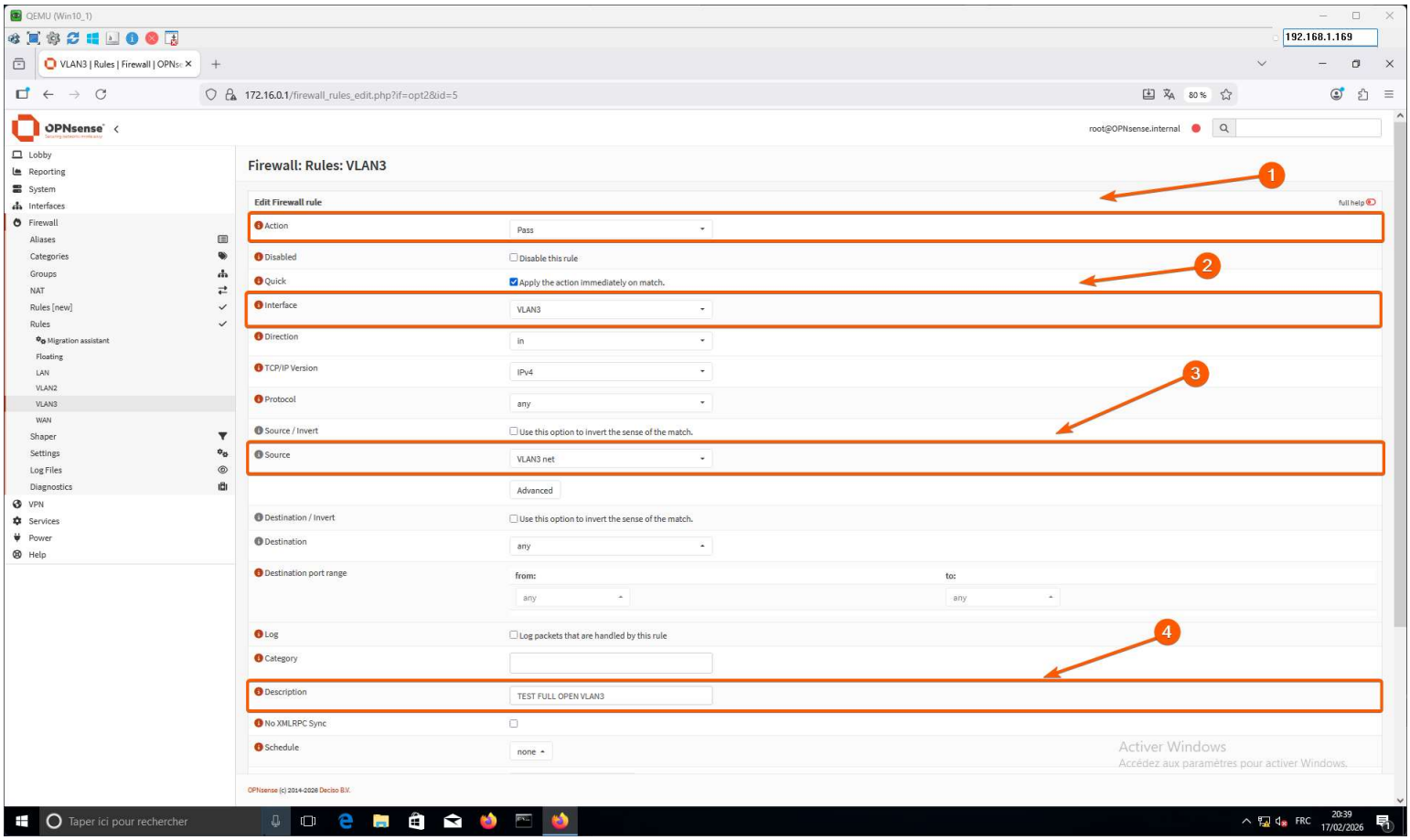
**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

Puis configure :

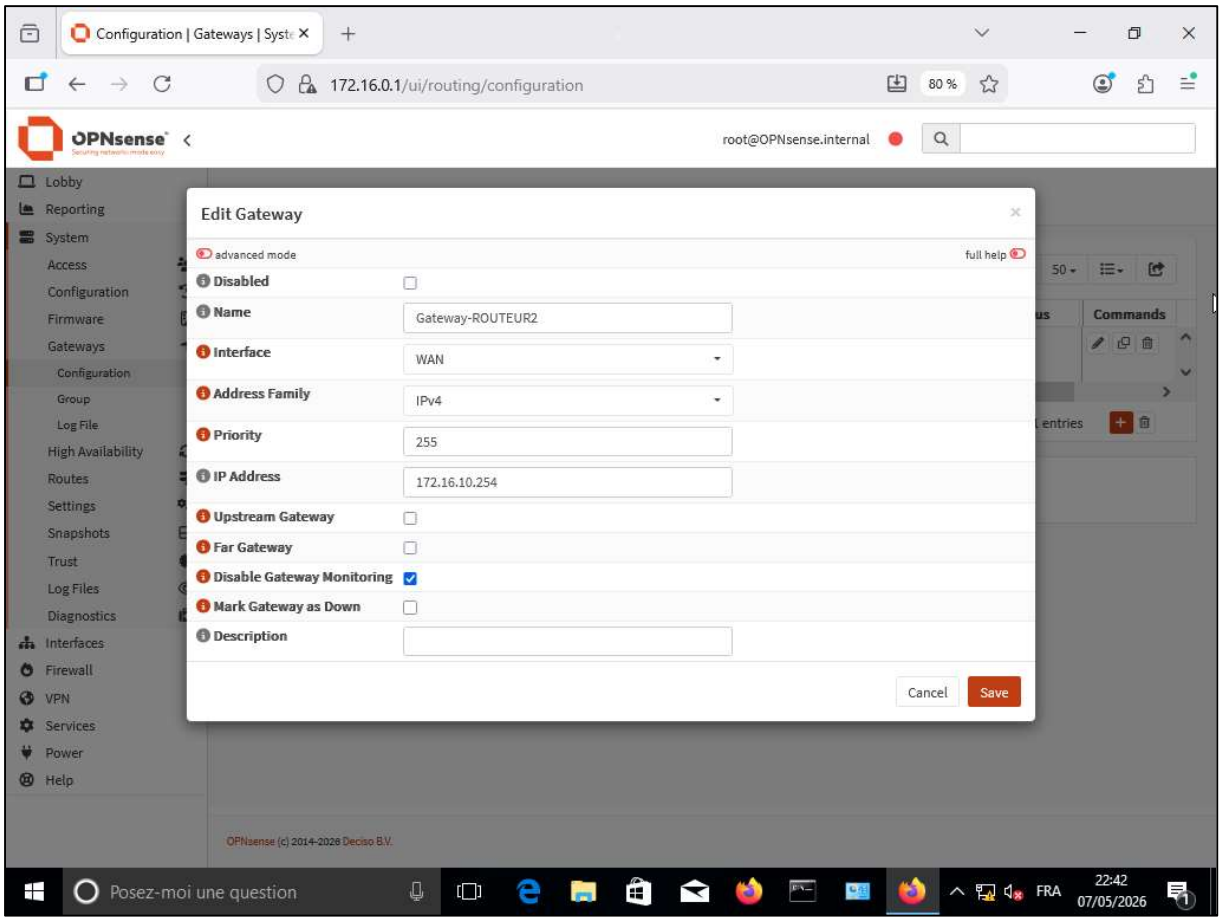
- **Action** : Pass
- **Interface** : VLAN3
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : any
- **Source** : VLAN3 net
- **Destination** : any
- **Description** : TEST FULL OPEN VLAN 3

Puis :

Cliquer **Save**, puis **Apply Changes**



## Paramétrage de la Gateway du Routeur 2.



## 4ème phase du projet : Configuration du pare-feu OPNsense_2 :

Configuration des règles du **OPNsense_2** :

### Rappel du cahier de charges :

- **Autoriser VLAN3** (172.16.3.0/24) à accéder au serveur web
- **Bloquer VLAN2** (172.16.2.0/24) si tu veux
- Protéger le réseau 192.168.10.0/24
- Gérer les règles entrantes vers le serveur

### Rappel des rôles de chaque configuration :

Le premier pare-feu laisse sortir.
Le deuxième pare-feu décide qui a le droit d'entrer.

**Configuration de l'interface WAN :**

Aller dans :
**Interfaces → WAN**

**Décocher les cases :**

- ❒ **Block private networks** → Interdit les IPs type 192.168.x.x, 172.16.x.x ou 10.x.x.x sur le WAN.
- ❒ **Block bogon networks** → Interdit les IPs qui n'existent pas officiellement sur le web (IPs non assignées).

**Description** : Gateway-ROUTEUR1

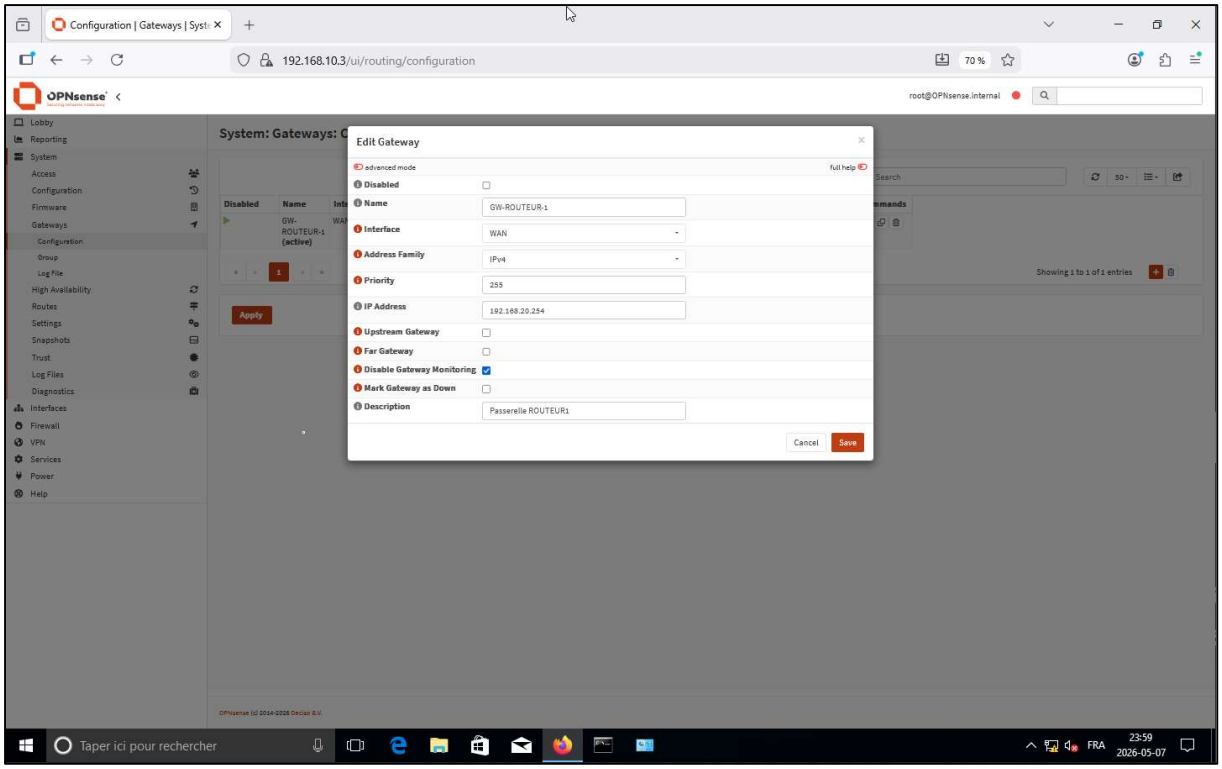
**IPv4 Configuration Type** : Static IPv4

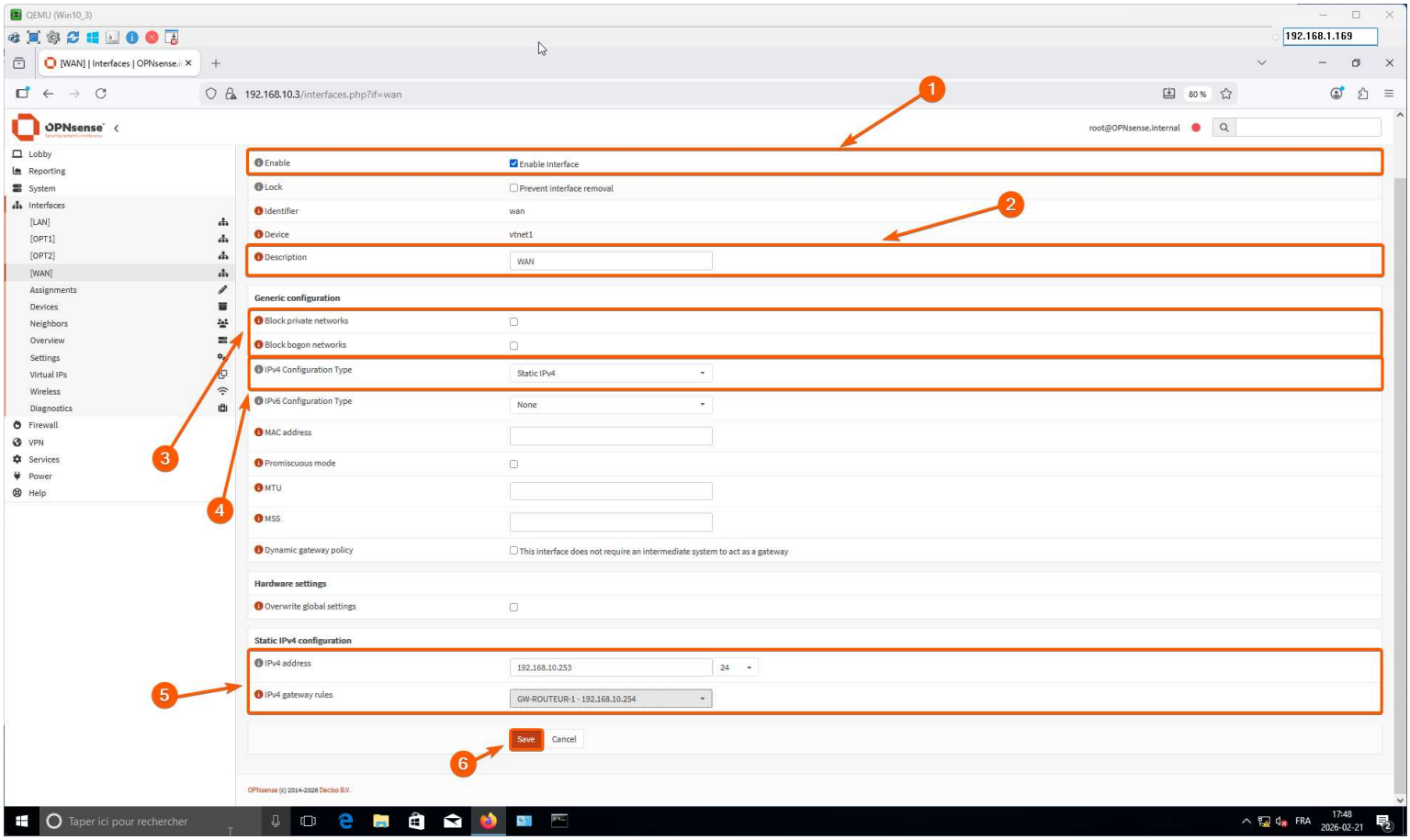
**IPv4 Address** : 192.168.10.253

**IPv4 gateway rules** : 192.168.10.254

**Save**, puis **Apply Changes**

# Configurer la gateway du Routeur 1



**Première règle qui va autoriser l'accès au serveur (HTTP):**

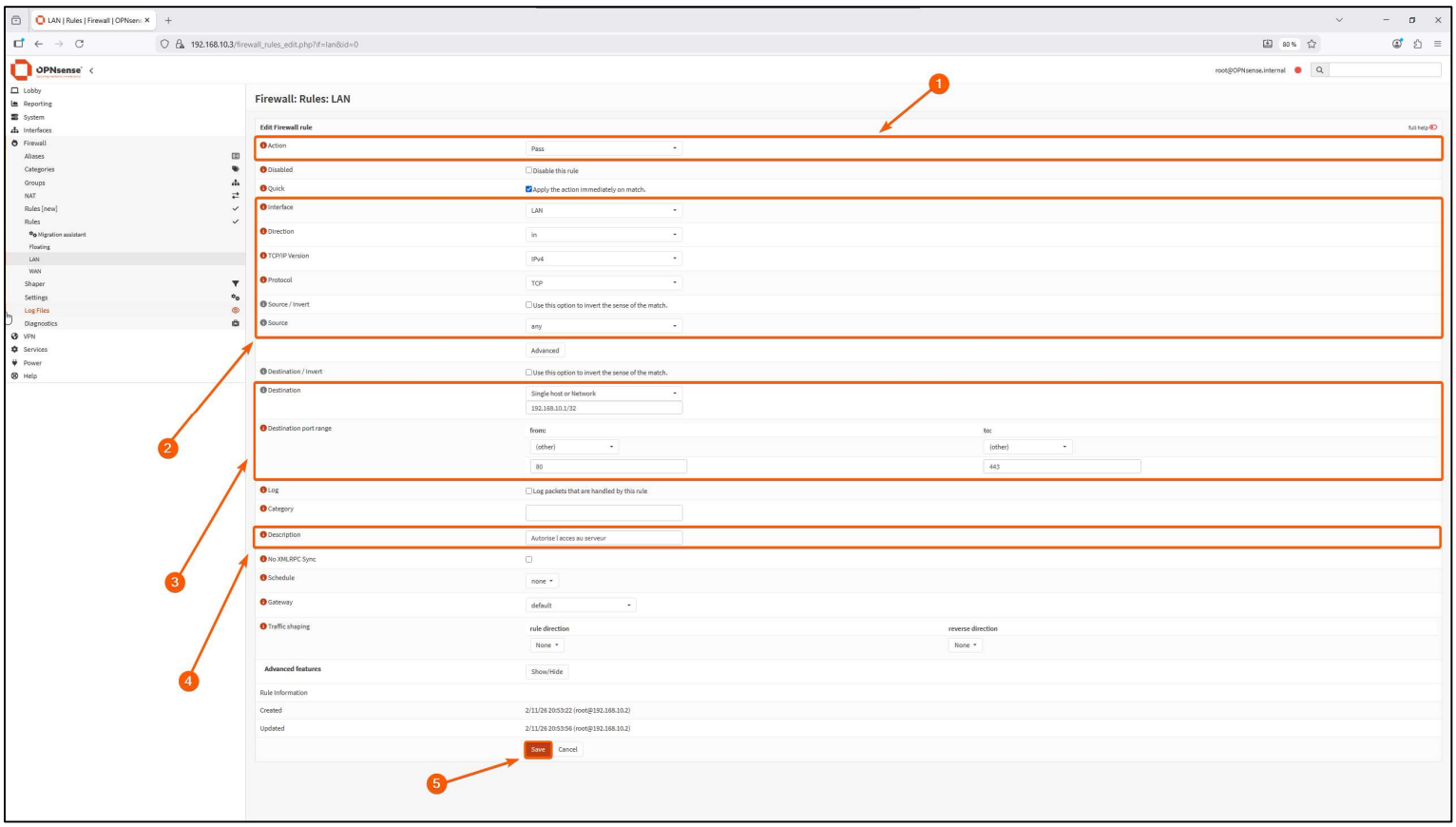
**Aller dans**
**Firewall → Rules → LAN**

**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

Puis configure :

- **Action** : Pass
- **Interface** : LAN
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : TCP
- **Source** : any
- **Destination** : 192.168.10.1/32
- **Destination port range**
  - ☞ From : HTTP (80)
  - ☞ To : HTTPS (443)
- **Description** : Autoriser l'accès au serveur web (HTTP)

Puis :
Cliquer **Save**, puis **Apply Changes** ⚠



**Deuxième règle qui va autoriser le trafic interne LAN**

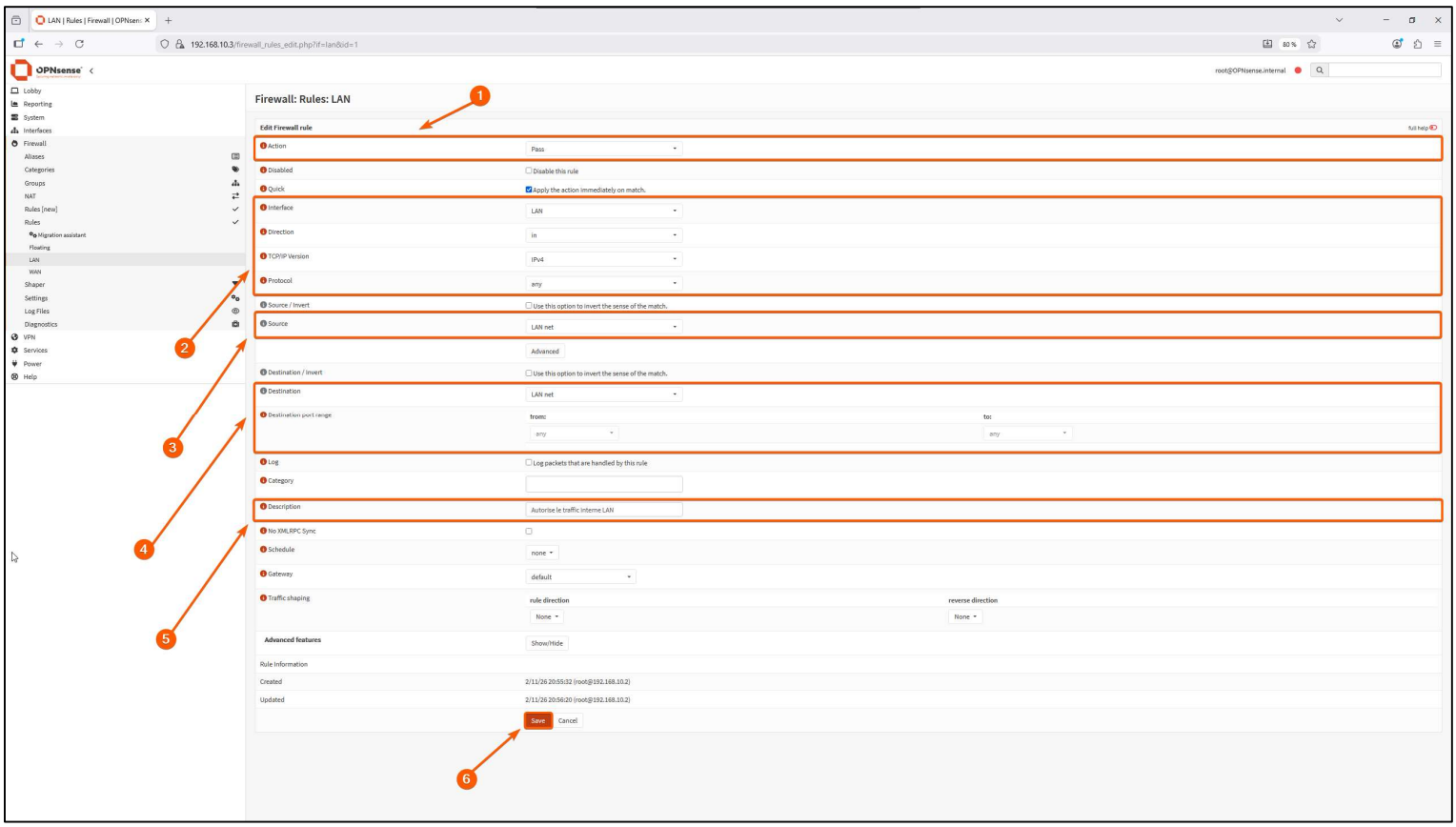
**Aller dans**
**Firewall → Rules → LAN**

**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

Puis configure :

- **Action** : Pass
- **Interface** : LAN
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : any
- **Source** : LAN net
- **Destination** : LAN net
- **Destination port range**
  - ☞ From : any
  - ☞ To : any
- **Description** : Autoriser l'accès au serveur web (HTTP)

Puis :
Cliquer **Save**, puis **Apply Changes** ❗



**Troisième règle qui va bloquer par défaut le LAN**

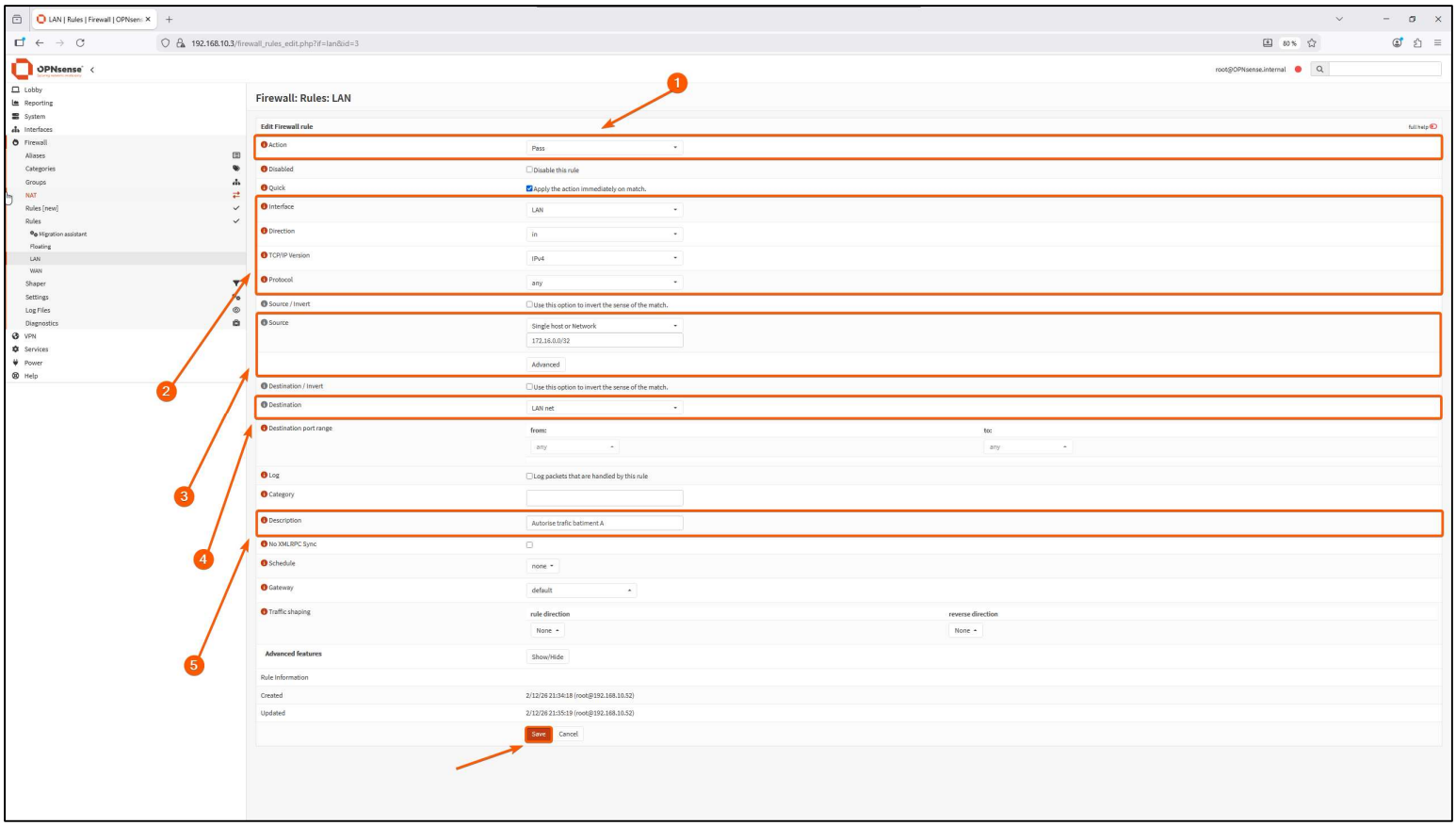
**Aller dans**
**Firewall → Rules → LAN**

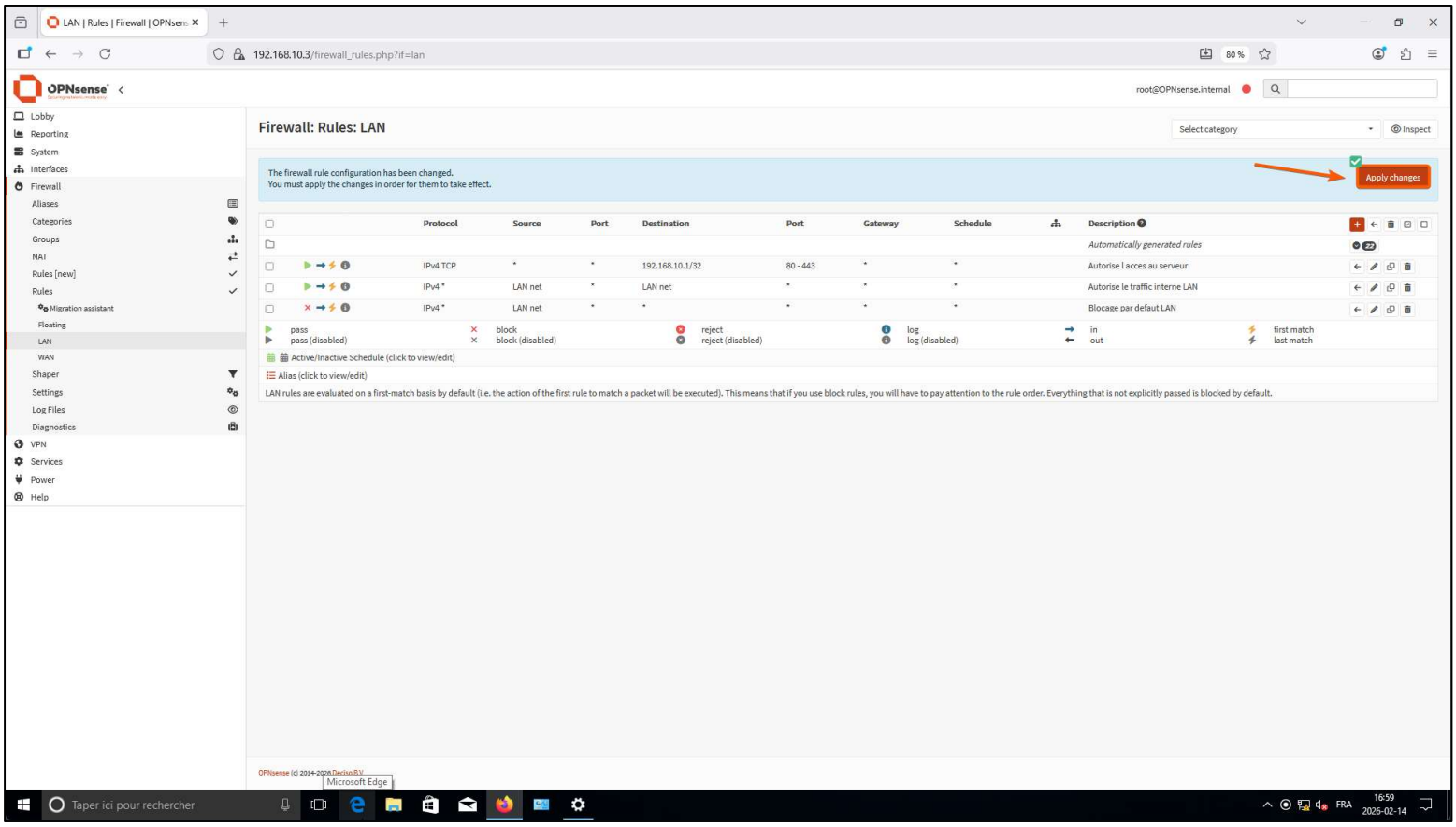
**Ajouter une règle BLOCK**
En haut → cliquer sur **+ Add**

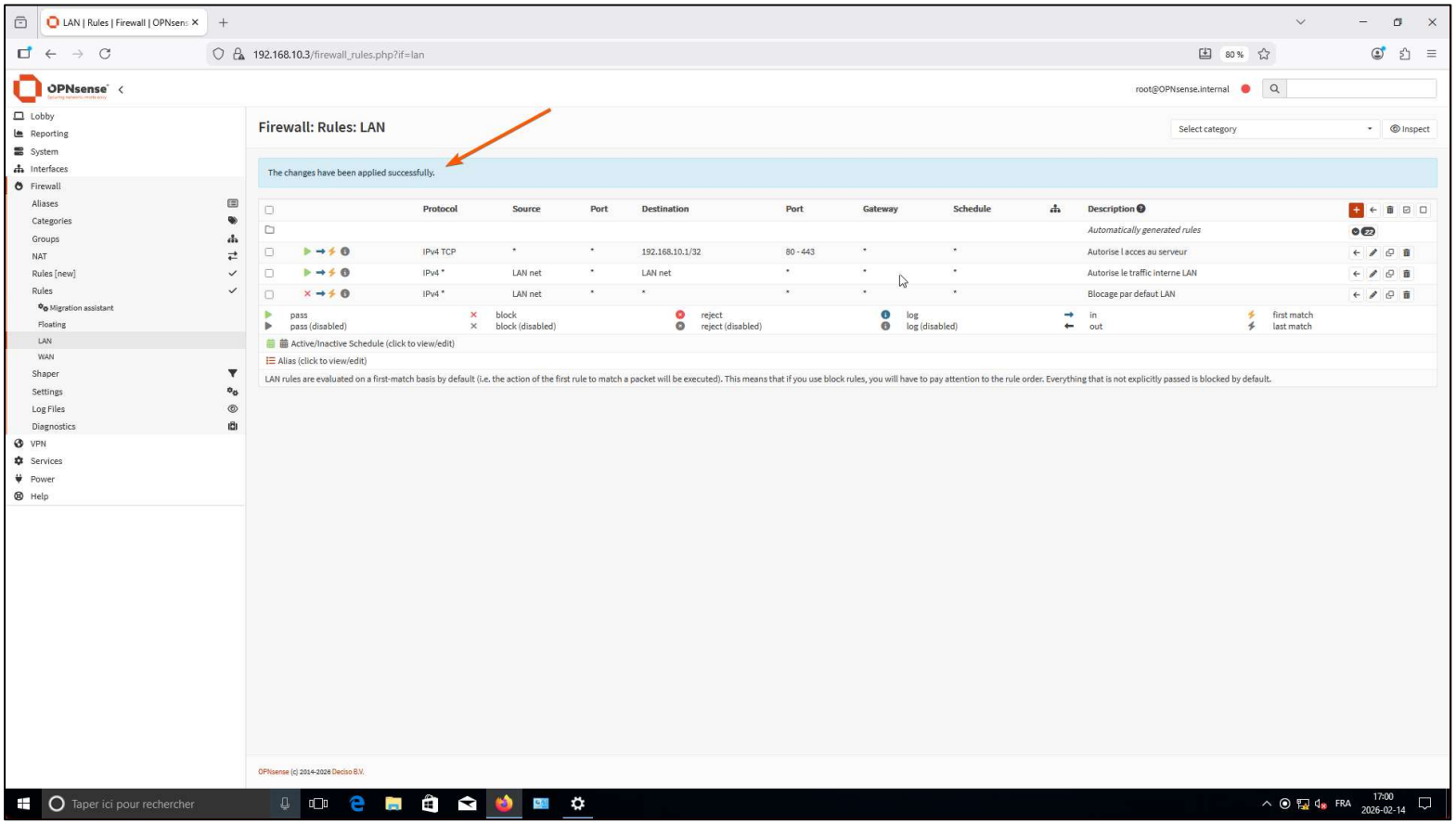
Puis configure :

- **Action** : Block
- **Interface** : LAN
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : any
- **Source** : LAN net
- **Destination** : any
- **Destination port range**
  - ☞ From : any
  - ☞ To : any
- **Description** : Blocage par défaut LAN

Puis :
Cliquer **Save**, puis **Apply Changes** ❗




LAN | Rules | Firewall | OPNsens
192.168.10.3/firewall_rules.php?if=lan
root@OPNsense.internal
Firewall: Rules: LAN
Select category
Inspect
The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.
Apply changes
Protocol
Source
Port
Destination
Port
Gateway
Schedule
Description
Automatically generated rules
IPv4 TCP
*
*
192.168.10.1/32
80 - 443
*
*
Autorise l acces au serveur
IPv4 *
LAN net
*
LAN net
*
*
*
Autorise le traffic interne LAN
IPv4 *
LAN net
*
*
*
*
*
Blocage par defaut LAN
pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)
in
out
first match
last match
Active/Inactive Schedule (click to view/edit)
Alias (click to view/edit)
LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules [new]
Rules
Migration assistant
Floating
LAN
WAN
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
Help
Microsoft Edge
Taper ici pour rechercher
FRA
16:59
2026-02-14


LAN | Rules | Firewall | OPNsens
192.168.10.3/firewall_rules.php?if=lan
root@OPNsense.internal
Firewall: Rules: LAN
Select category
Inspect
The changes have been applied successfully.
Protocol
Source
Port
Destination
Port
Gateway
Schedule
Description
Automatically generated rules
IPv4 TCP
*
*
192.168.10.1/32
80 - 443
*
*
Autorise l acces au serveur
IPv4 *
LAN net
*
LAN net
*
*
*
Autorise le traffic interne LAN
IPv4 *
LAN net
*
*
*
*
*
Blocage par defaut LAN
pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)
in
out
first match
last match
Active/Inactive Schedule (click to view/edit)
Alias (click to view/edit)
LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules [new]
Rules
Migration assistant
Floating
LAN
WAN
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
Help
Taper ici pour rechercher
FRA
17:00
2026-02-14

**Quatrième Règle : Définir la passerelle (gateway) pour VLAN2 et VLAN3**

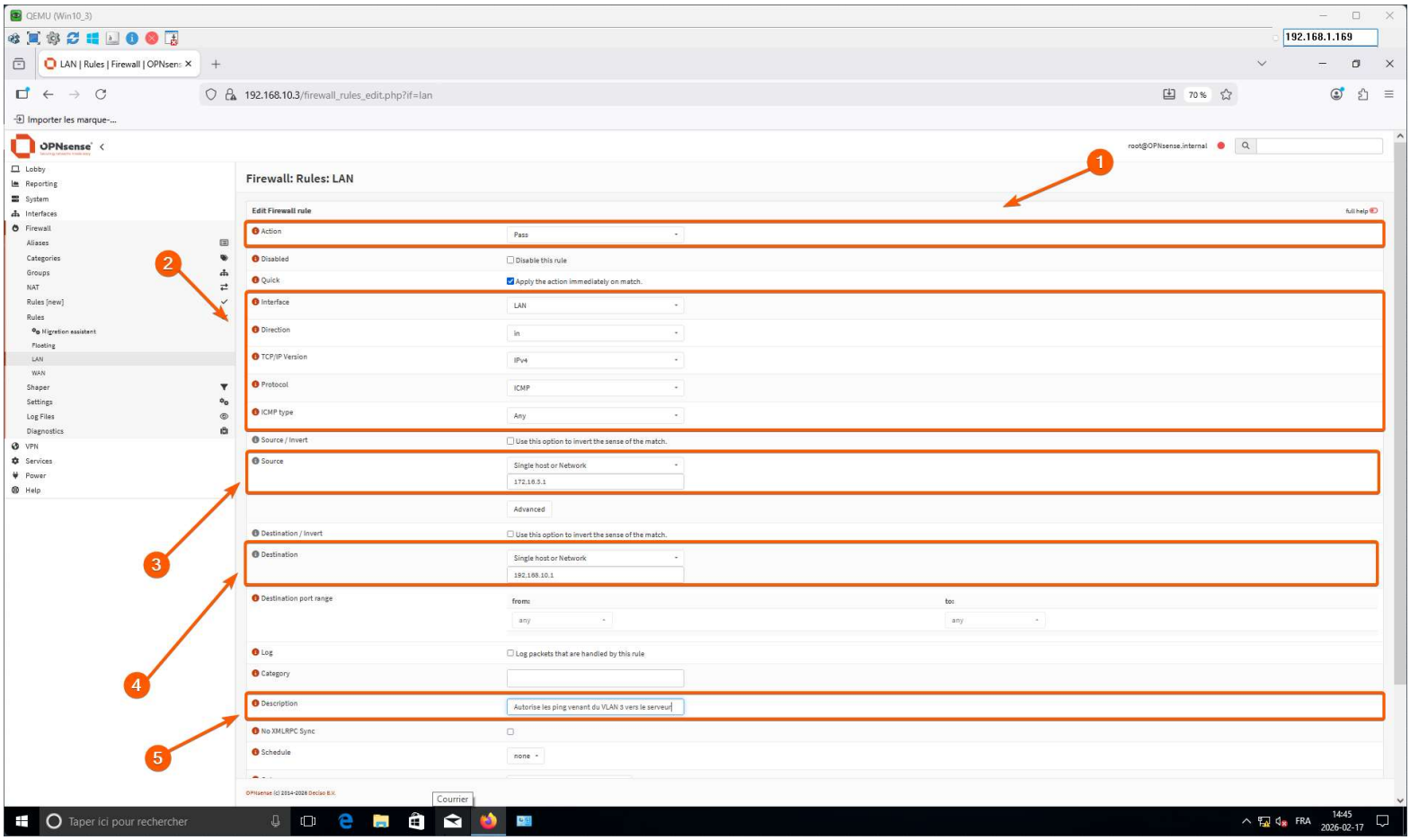
Aller dans :
**Firewall → Rules → LAN**

**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

Puis configure :

- **Action** : Pass
- **Interface** : LAN
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : ICMP
- **Source** : 172.16.3.1
- **Destination** : 192.168.10.1
- **Destination port range**
  - ☞ From : any
  - ☞ To : any
- **Description** : Autorise les ping venant du VLAN 3 vers Serveur

Puis :
Cliquer **Save**, puis **Apply Changes**




## Cinquième Règle : Autoriser la communication de tous les protocoles sur le WAN

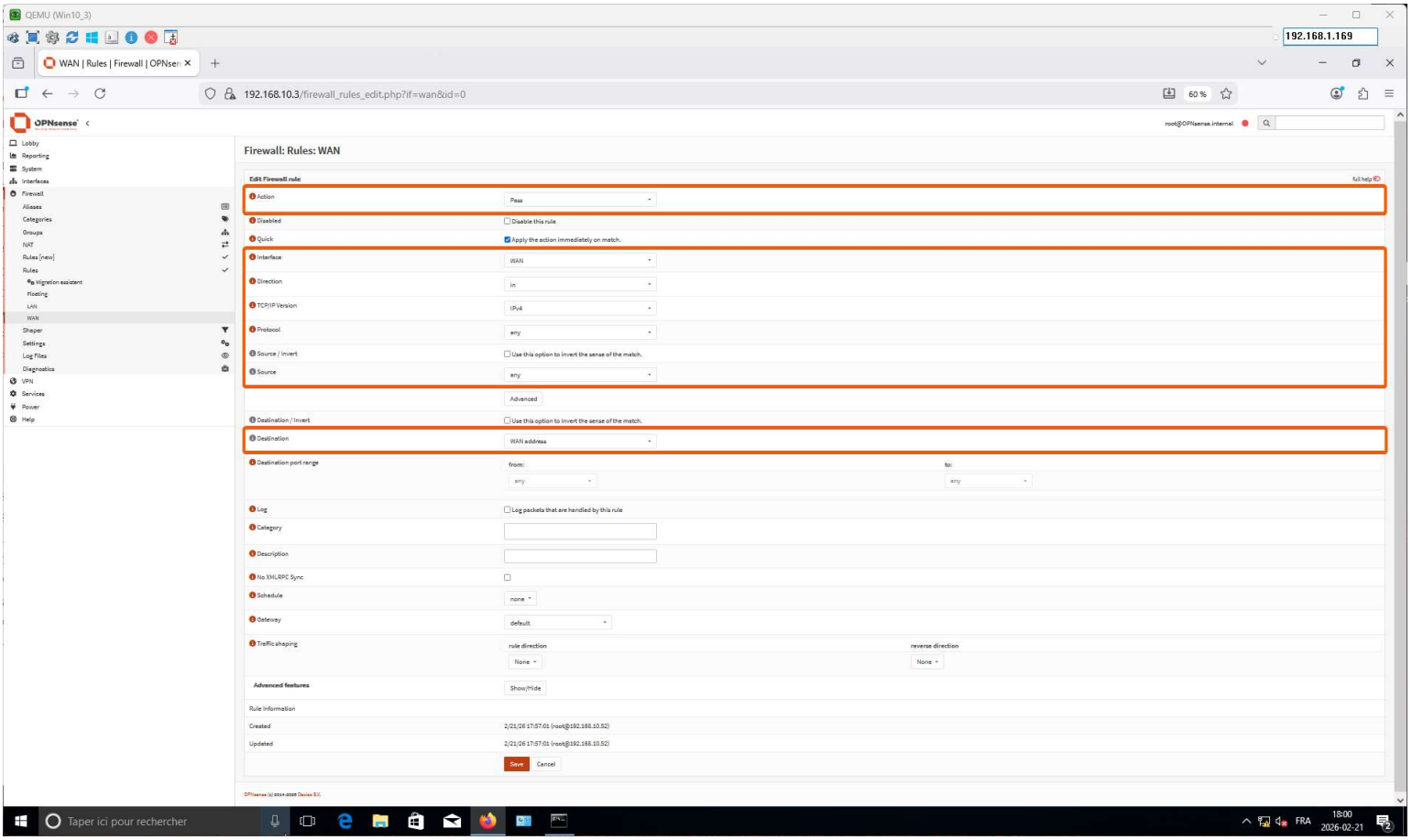
Aller dans :
**Firewall → Rules → WAN**

**Ajouter une règle PASS**
En haut → cliquer sur **+ Add**

Puis configure :

- **Action** : Pass
- **Interface** : WAN
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : any
- **Source** : any
- **Destination** : WAN address
- **Description** : Autorise le ping sur l'interface WAN

Cliquer **Save**, puis **Apply Changes** ⚠




## 5ème phase du projet : Configuration du service DHCP du pare-feu OPNsense_1 :

## Etape 1 : Activer le service DHCP sur les interfaces VLAN

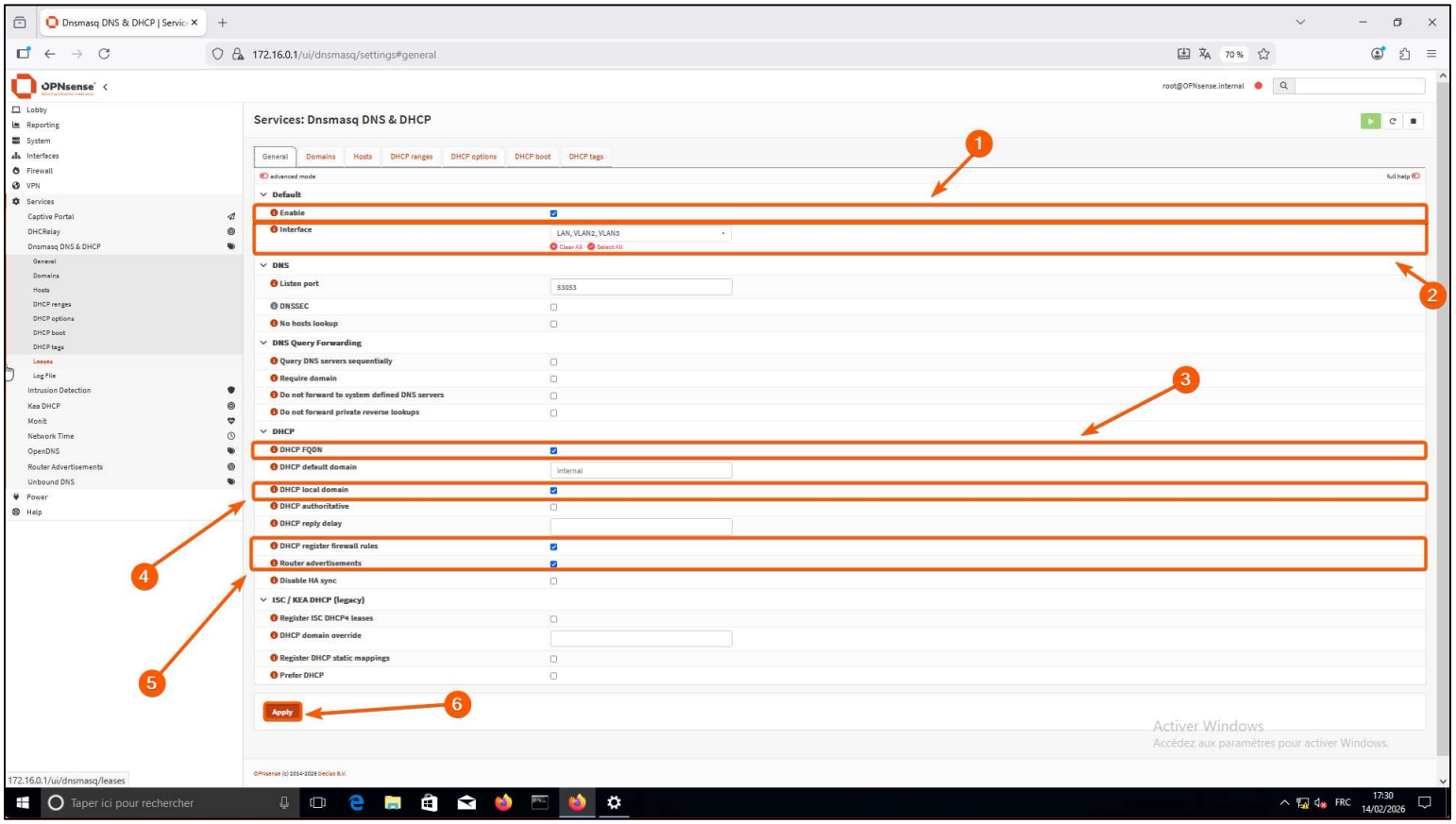
Aller dans :

**Services → Dnsmasq DNS & DHCP → General**

Configurer :

- **Enable :** coché
- **Interfaces :**
  - LAN
  - VLAN2
  - VLAN3
- **DHCP FQDN :** coché
- **DHCP local domain :** coché
- **DHCP default domain :** internal
- **DHCP authoritative :** coché
- **DHCP register firewall rules :** coché

Puis cliquer sur **Apply**.




## Etape 2 : Définir la plage DHCP pour VLAN2

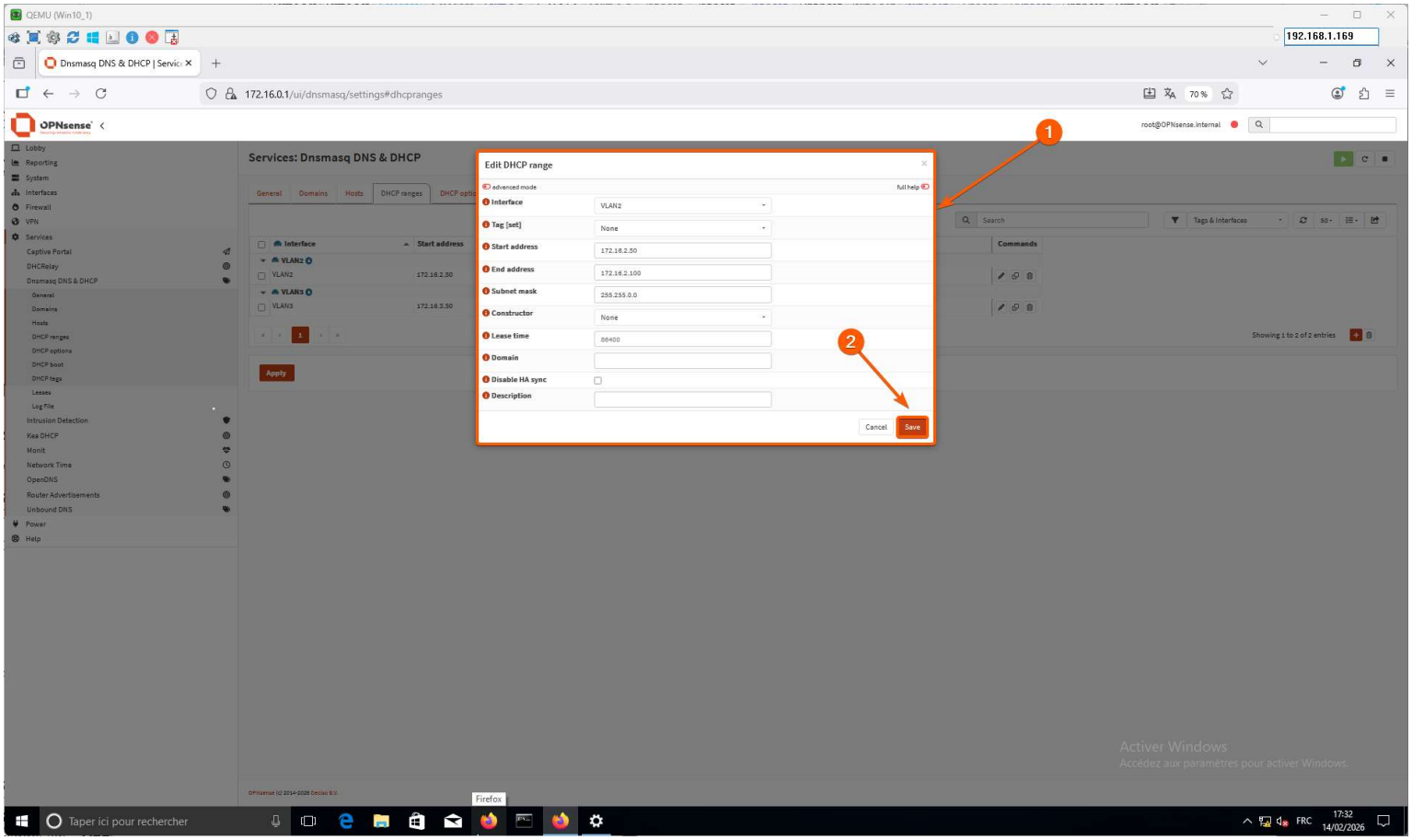
Aller dans :

**Services → Dnsmasq DNS & DHCP → DHCP ranges**
Cliquer sur **+ Add**.

Configurer :

- **Interface :** VLAN2
- **Start address :** 172.16.2.50
- **End address :** 172.16.2.100
- **Subnet mask :** 255.255.255.0
- **Lease time :** 86400
- **Description :** Plage DHCP VLAN2

Puis cliquer **Save**, puis **Apply**.

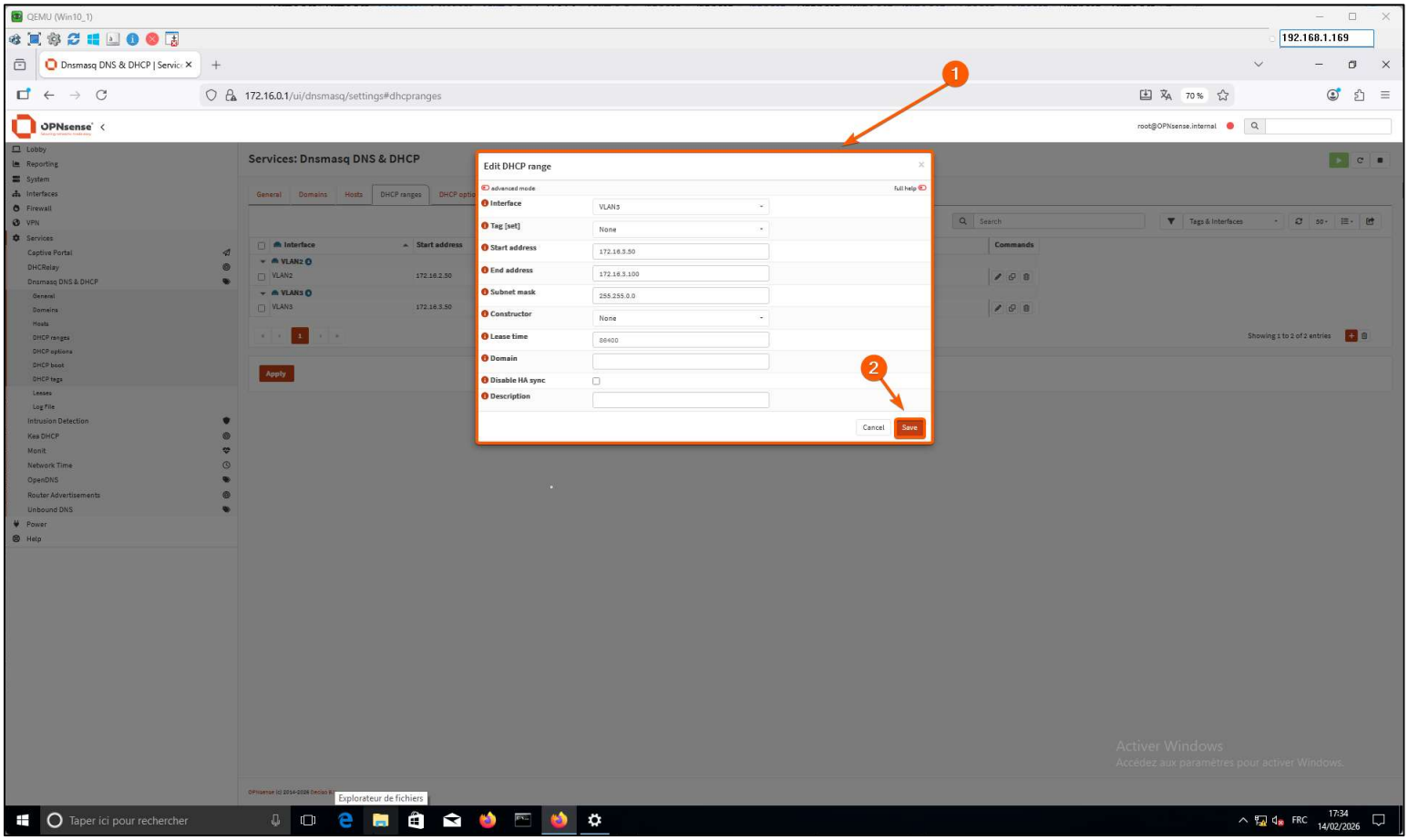



**Etape 3 : Définir la plage DHCP pour VLAN3**

Toujours dans :
**Services → Dnsmasq DNS & DHCP → DHCP ranges**
Cliquer sur **+ Add**.
Configurer :

- **Interface :** VLAN3
- **Start address :** 172.16.3.50
- **End address :** 172.16.3.100
- **Subnet mask :** 255.255.255.0
- **Lease time :** 86400
- **Description :** Plage DHCP VLAN3

Puis cliquer **Save**, puis **Apply**.




## Etape 4 : Définir la passerelle (gateway) pour VLAN2 et VLAN3

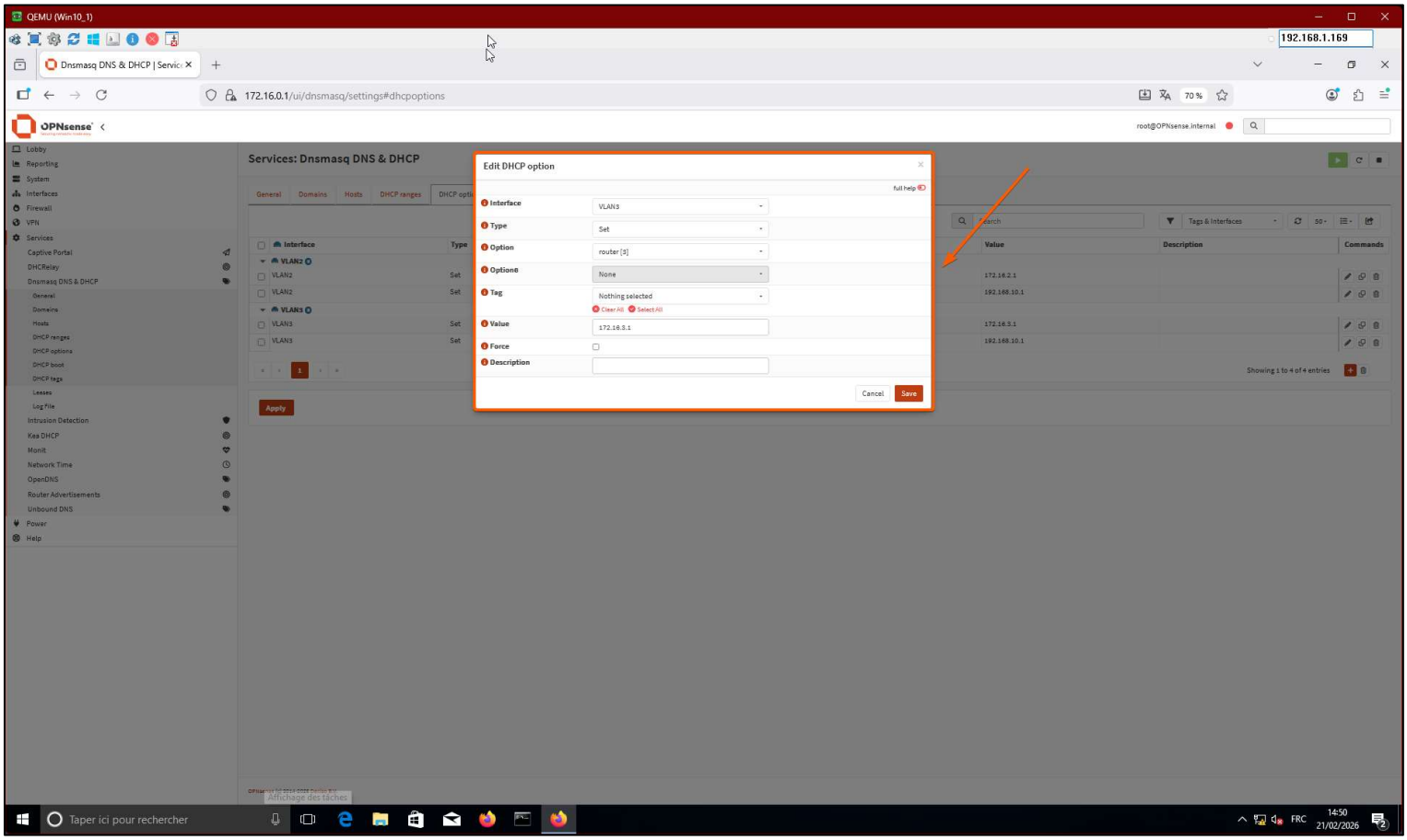
Aller dans :
**Services → Dnsmasq DNS & DHCP → DHCP options**
Cliquer sur **+ Add** pour chaque VLAN.
**Pour VLAN2 :**

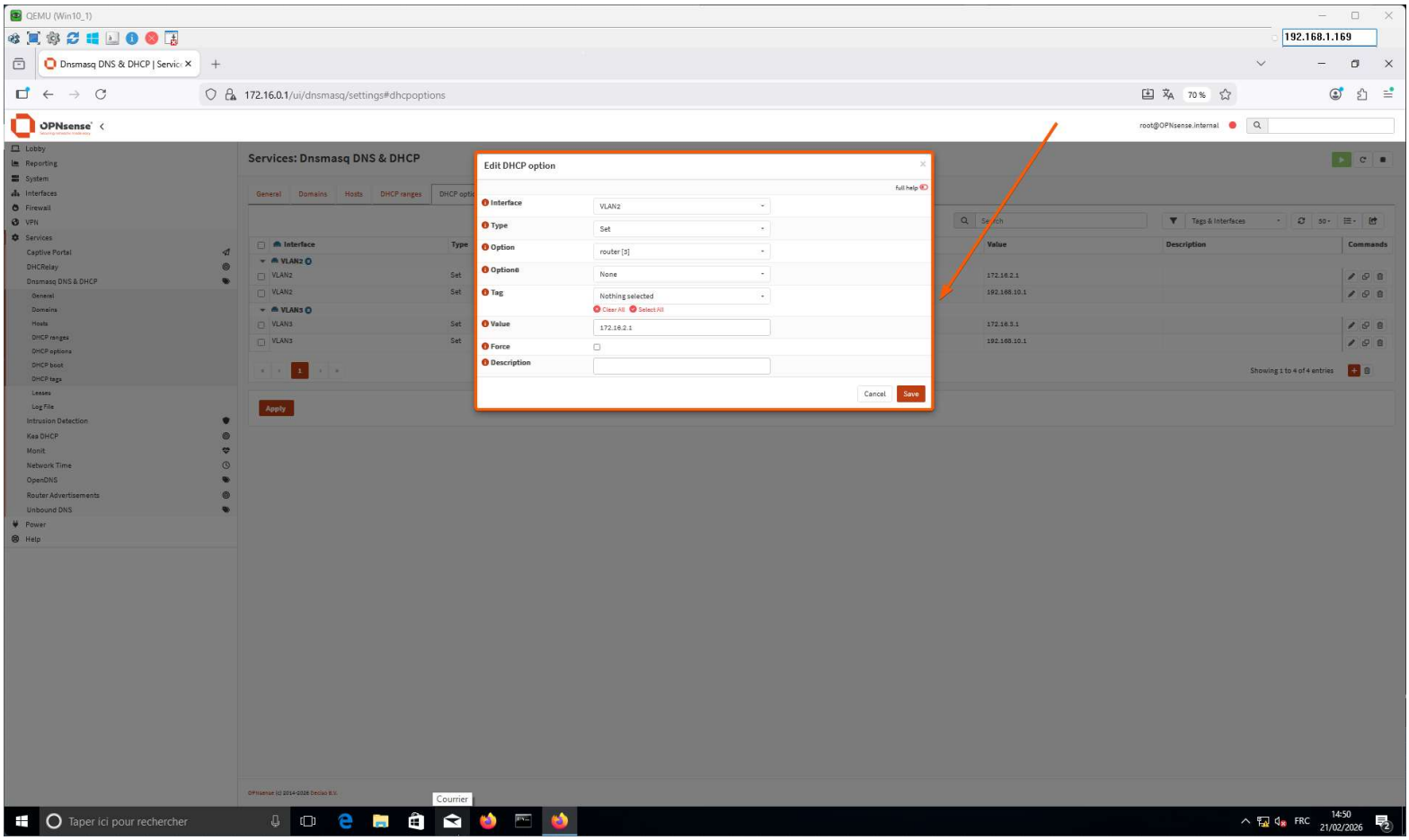
- **Interface :** VLAN2
- **Type :** Set
- **Option :** router [3]
- **Value :** 172.16.2.1

**Pour VLAN3 :**

- **Interface :** VLAN3
- **Type :** Set
- **Option :** router [3]
- **Value :** 172.16.3.1

Puis cliquer **Save**, puis **Apply**.






## 4) Définir l'adresse du serveur (DNS) pour les clients DHCP

**<u>Pour le VLAN2 :</u>**

Aller dans :
**Services → Dnsmasq DNS & DHCP → DHCP options**
Cliquer sur **+ Add**.
Configurer :

- **Interface :** VLAN2
- **Type :** Set
- **Option :** dns-server[6]
- **Value :** 192.168.10.1

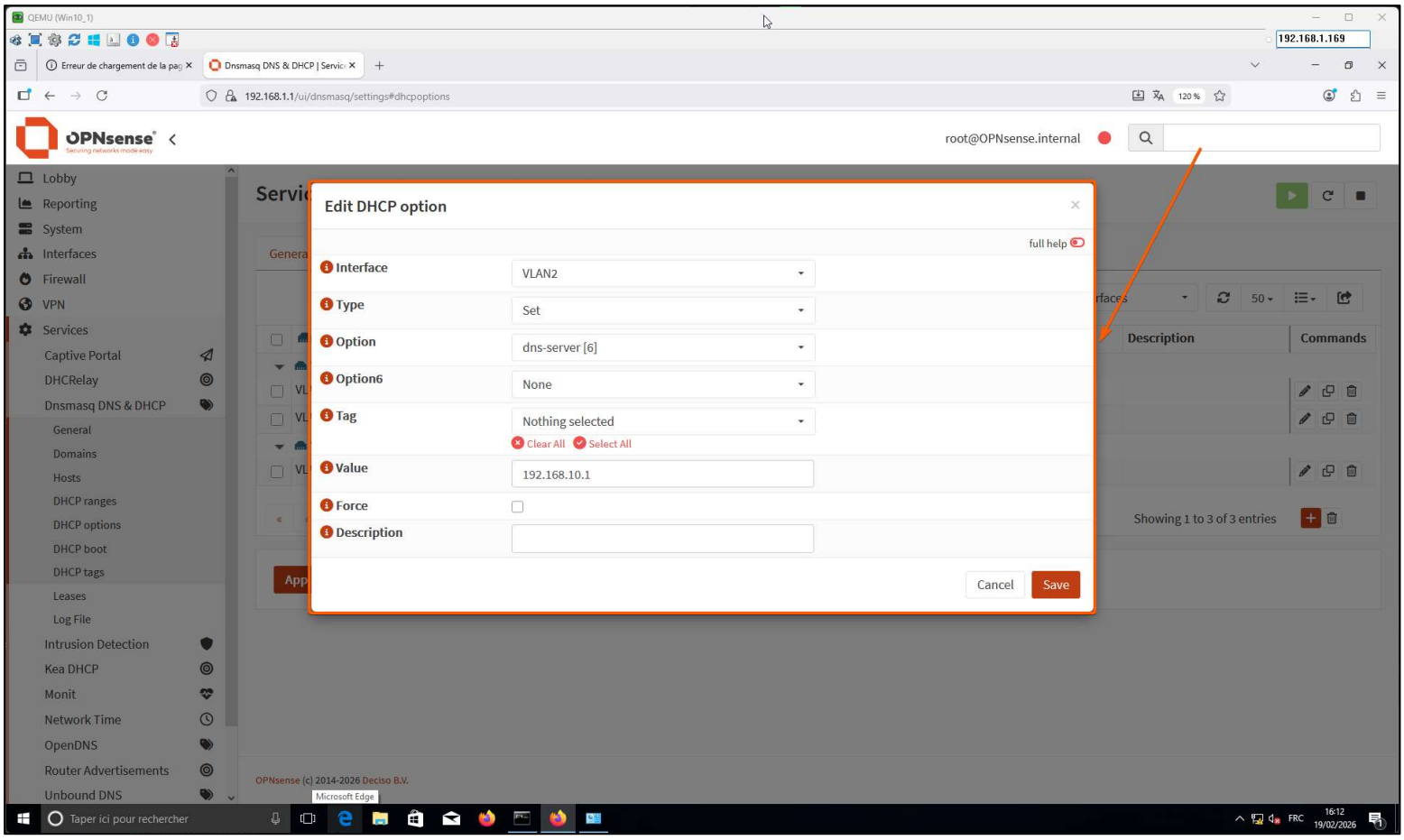
**Description :** DNS Server pour le vlan 2

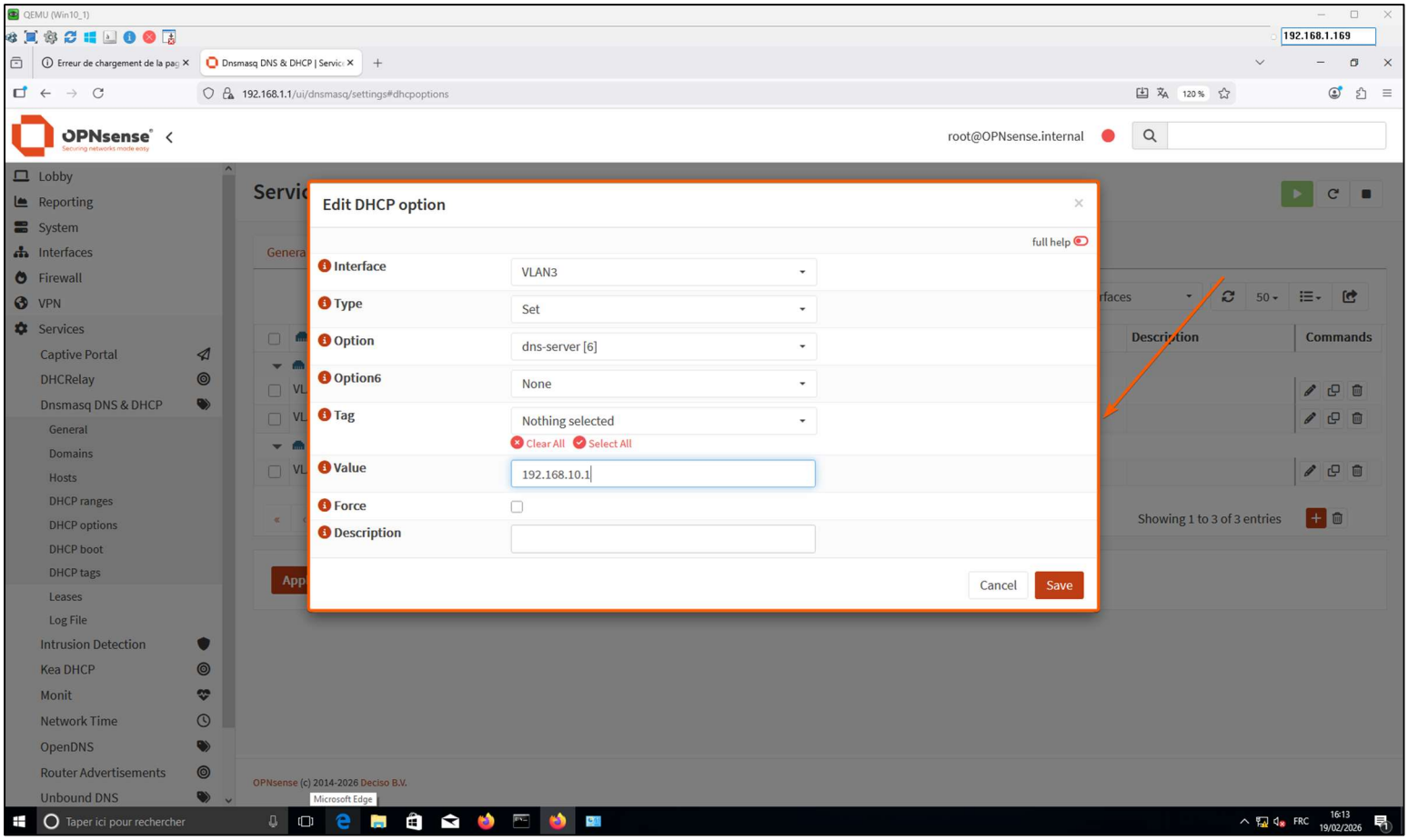
**<u>Pour le VLAN3 :</u>**

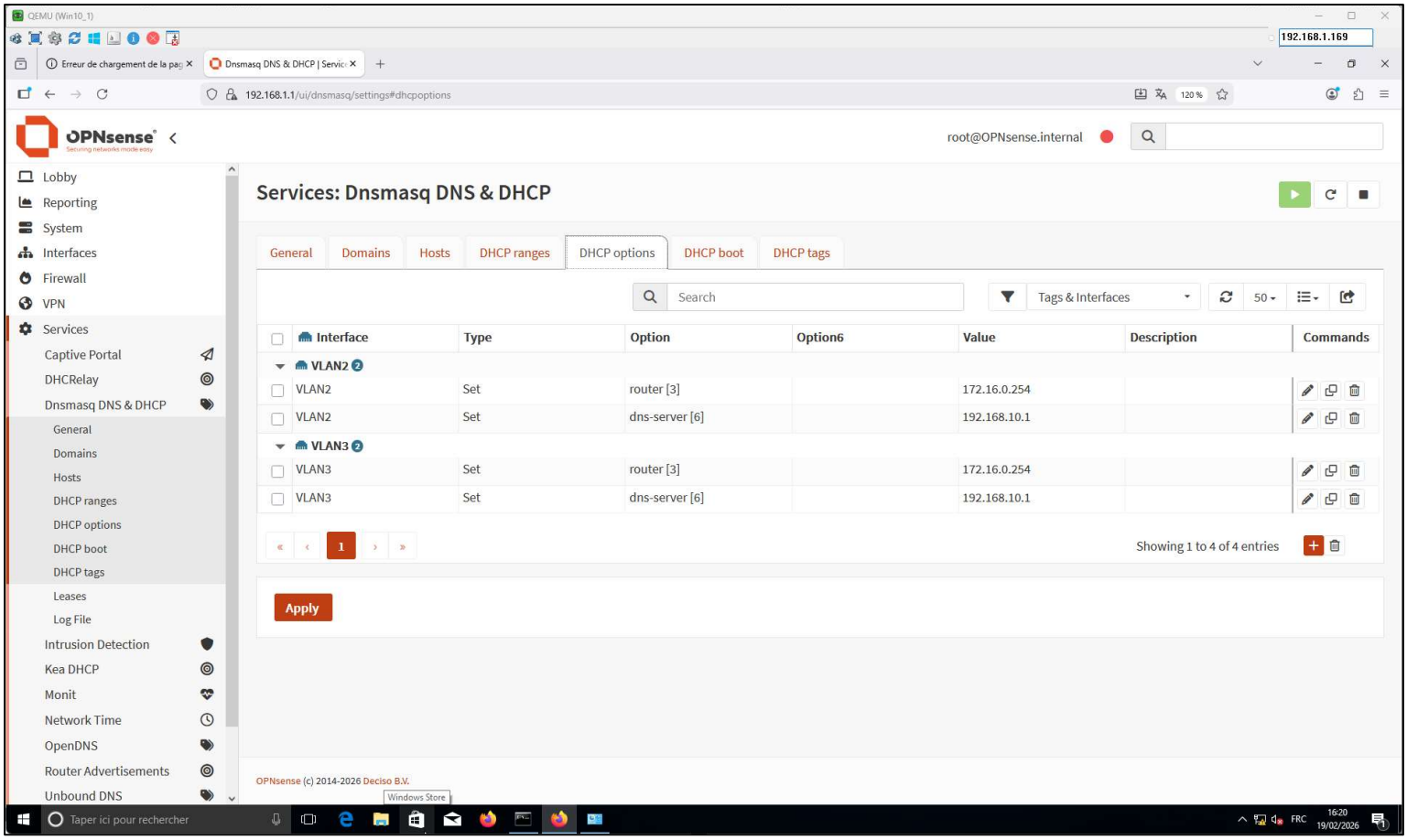
Aller dans :
**Services → Dnsmasq DNS & DHCP → DHCP options**
Cliquer sur **+ Add**.
Configurer :

- **Interface :** VLAN3
- **Type :** Set
- **Option :** dns-server[6]
- **Value :** 192.168.10.1

**Description :** DNS Server pour le vlan 3



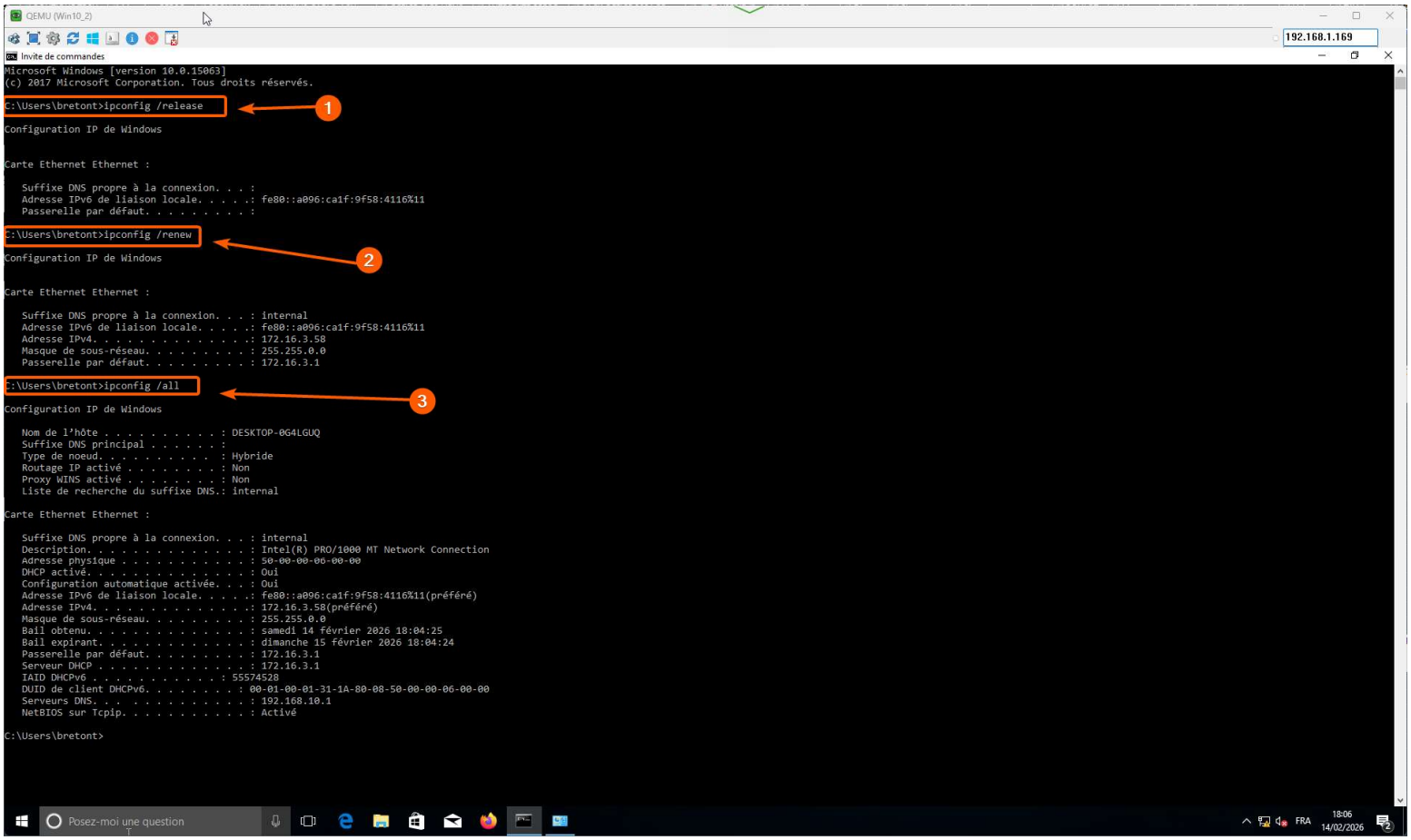






**Sur chaque interface cliquer toujours sur Apply pour appliquer votre paramétrage.**

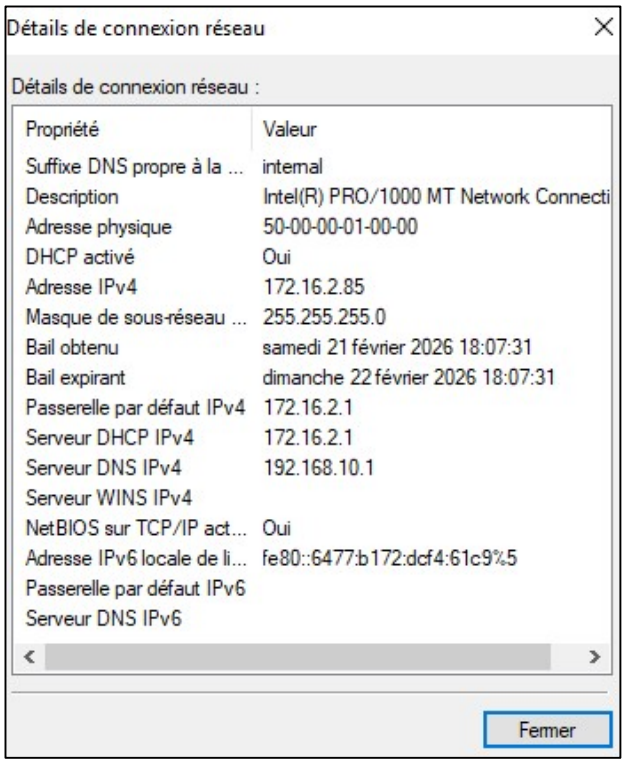
Vérification sur les machine virtuelle cliente sous Windows 10 :

**Est-ce qu'elle obtienne une adresse IP, un Masque de sous réseau, leur passerelle, un serveur DNS ?**

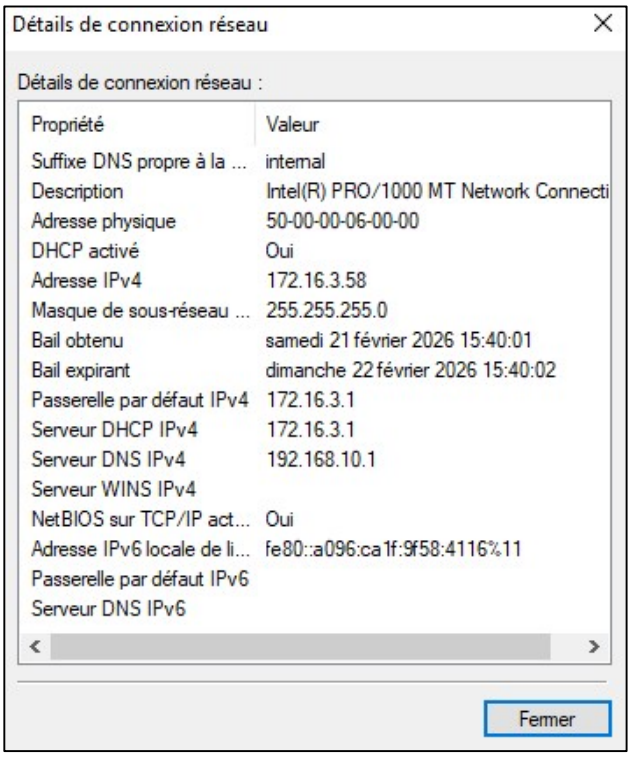

QEMU (Win10_2)
192.168.1.169
Invite de commandes
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.
C:\Users\bretont>ipconfig /release
1
Configuration IP de Windows
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . .: fe80::a096:ca1f:9f58:4116%11
Passerelle par défaut. . . . . :
C:\Users\bretont>ipconfig /renew
2
Configuration IP de Windows
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : internal
Adresse IPv6 de liaison locale. . . . .: fe80::a096:ca1f:9f58:4116%11
Adresse IPv4. . . . . .: 172.16.3.58
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 172.16.3.1
C:\Users\bretont>ipconfig /all
3
Configuration IP de Windows
Nom de l'hôte . . . . . : DESKTOP-0G4LGUQ
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: internal
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . : internal
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : 50-00-00-06-00-00
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . .: fe80::a096:ca1f:9f58:4116%11(préféré)
Adresse IPv4. . . . . .: 172.16.3.58(préféré)
Masque de sous-réseau. . . . . : 255.255.0.0
Bail obtenu. . . . . : samedi 14 février 2026 18:04:25
Bail expirant. . . . . : dimanche 15 février 2026 18:04:24
Passerelle par défaut. . . . . : 172.16.3.1
Serveur DHCP . . . . . : 172.16.3.1
IAID DHCPv6 . . . . . : 55574528
DUID de client DHCPv6. . . . . : 00-01-00-01-31-1A-80-08-50-00-00-06-00-00
Serveurs DNS. . . . . : 192.168.10.1
NetBIOS sur Tcpip. . . . . : Activé
C:\Users\bretont>
Posez-moi une question
FRA
18:06
14/02/2026

# BILAN DE CONFIGURAITON DES CARTE RESEAU

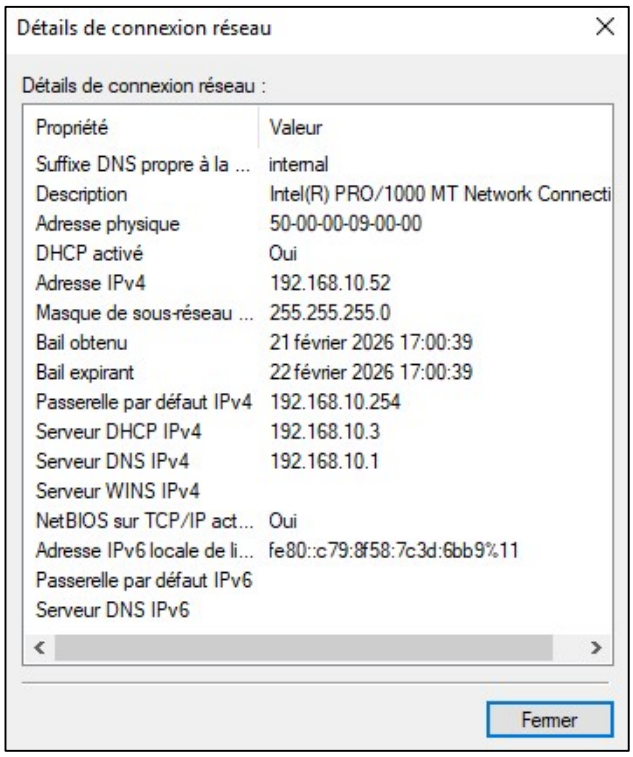
## Carte réseau : Win_10_1 :



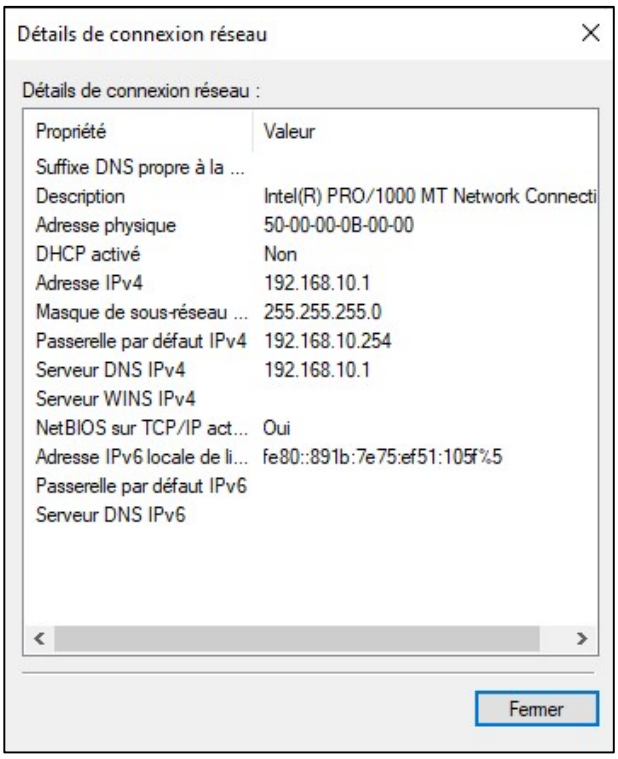

## Carte réseau : Win_10_2 :




## Carte réseau : Win_10_3 :




## Carte réseau : WinServer :



## 7ème phase du projet : Administration réseau des équipements :

**Etape 1 :** Configuration des équipements d'interconnexion :

**Configuration des ports de Switch_1 :**

```
interface Ethernet0/0
 switchport trunk
encapsulation dot1q
 switchport trunk allowed
vlan 1-3
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 switchport access vlan 2
 duplex auto
!
interface Ethernet0/2
 switchport access vlan 3
 duplex auto
!
interface Ethernet0/3
 switchport mode access
 duplex auto
```

**Configuration des ports de Switch_2 :**

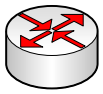
→ Création d'un vlan pour le service de la Direction

```
interface Ethernet0/0
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 switchport mode access
 duplex auto
!
interface Ethernet0/2
 switchport mode access
 duplex auto
!
interface Ethernet0/3
 switchport mode access
 duplex auto
!
```

**Etape 2 :** Configuration du routage :

## Configuration des ports de Routeur_1 :

```
interface Ethernet0/0
 ip address 10.0.0.254 255.0.0.0
!
interface Ethernet0/1
 ip address 192.168.10.254 255.255.255.0
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 172.16.0.0 255.255.0.0 10.0.0.253
ip route 172.16.3.0 255.255.255.0 172.16.0.253
```



## Configuration des ports de Routeur_2 :

```
interface Ethernet0/0
 ip address 172.16.0.254 255.255.0.0
!
interface Ethernet0/1
 ip address 10.0.0.253 255.0.0.0
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 192.168.10.0 255.255.255.0 10.0.0.254
```

## FICHE DE TEST :

### TEST DE COMMUNICATION :

| Paquets envoyés depuis | Destinataire | Résultat |
|---|---|---|
| **TEST DE COMMUNICAITON ENTRE LES ROUTEUR** | | |
| Routeur 2 – ping 192.168.10.254 | Routeur 1 – Ethernet0/1 | ✅ |
| Routeur 1 – ping 172.16.10.254 | Routeur 2 – Ethernet0/0 | ✅ |
| Routeur 1 – ping 172.16.10.253 | OPNsense_1 – Interface WAN | ✅ |
| **TEST DE COMMUNICATION POSTE Win_10_1** | | |
| Win_10_1 – ping 172.16.2.1 | OPNsense_1 – Interface VLAN 2 | ✅ |
| Win_10_2 – ping 172.16.10.253 | OPNsense_1 - Interface WAN | ✅ |
| Win_10-2 – ping 172.16.10.254 | Routeur_2 - Ethernet0/0 | ✅ |
| Win_10-2 – ping 10.0.0.253 | Routeur_2 - Ethernet0/1 – 10.0.0.254 | ✅ |
| Win_10-2 – ping 10.0.0.254 | Routeur_1 - Ethernet0/0 – 10.0.0.254 | ✅ |
| **TEST DE COMMUNICATION POSTE Win_10_2** | | |
| Win_10_2 – ping 172.16.3.1 | OPNsense_1 – VLAN3 | ✅ |
| Win_10_2 – ping 172.16.10.253 | OPNsense_1 - Interface WAN | ✅ |
| Win_10-2 – ping 172.16.10.254 | Routeur_2 - Ethernet0/0 | ✅ |
| Win_10-2 – ping 10.0.0.253 | Routeur_2 - Ethernet0/1 | ✅ |
| Win_10-2 – ping 10.0.0.254 | Routeur_1 - Ethernet0/0 – 10.0.0.254 | ✅ |
| **TEST DE COMMUNICATION POSTE Win_10_3** | | |
| Win_10_3 – ping 192.168.10.1 | Windows Server | ✅ |
| Test URL – ping www.lyceetech.com | Windows Server – Rôle IIS | ✅ |
| Win_10_3 – ping 192.168.20.254 | Routeur 1 – Ethernet0/1 | ✅ |
| **TEST DE COMMUNICATION Windows Serveur** | | |
| WinServer– ping 192.168.10.3 | OPNsense_2 – LAN – 192.168.10.3 | ✅ |
| WinServer – ping 192.168.20.253 | OPNsense_2 – WAN – 192.168.20.253 | ✅ |
| WinServer – ping 192.168.20.254 | Routeur_1 - Ethernet0/1 – 192.168.20.254 | ✅ |
| WinServer – ping 10.0.0.254 | Routeur_1 - Ethernet0/0 – 10.0.0.254 | ✅ |
| WinServer – ping 10.0.0.253 | Routeur_1 - Ethernet0/0 – 10.0.0.253 | ✅ |
| **TEST DE COMMUNICATION OPNsense_1** | | |
| OPNsense1- VLAN3 – ping 172.16.3.58 | Win10_2 – 172.16.3.58 | ✅ |
| OPNsense1- VLAN3 – ping 172.16.2.85 | Win10_1 – 172.16.2.85 | ✅ |
| OPNsense1 – ping 172.16.10.254 | Routeur 1 – Ethernet0/1 | ✅ |
| OPNsense1 – ping 172.16.3.1 | OPNsense1 – VLAN3 - 172.16.3.1 | ✅ |
| **TEST DE COMMUNICATION OPNsense_2** | | |
| OPNsense2 – ping 192.168.10.52 | Win_10_3 – 192.168.10.52 | ✅ |
| OPNsense2 – ping 192.168.20.253 | Routeur_1 - Ethernet0/1 – 192.168.10.254 | ✅ |
| OPNsense2 – ping 192.168.10.1 | Windows Serveur – 192.168.10.1 | ✅ |

### TEST DE SITE :

| Accès Site depuis quel poste ? | Serveur à joindre | Résultat |
|---|---|---|

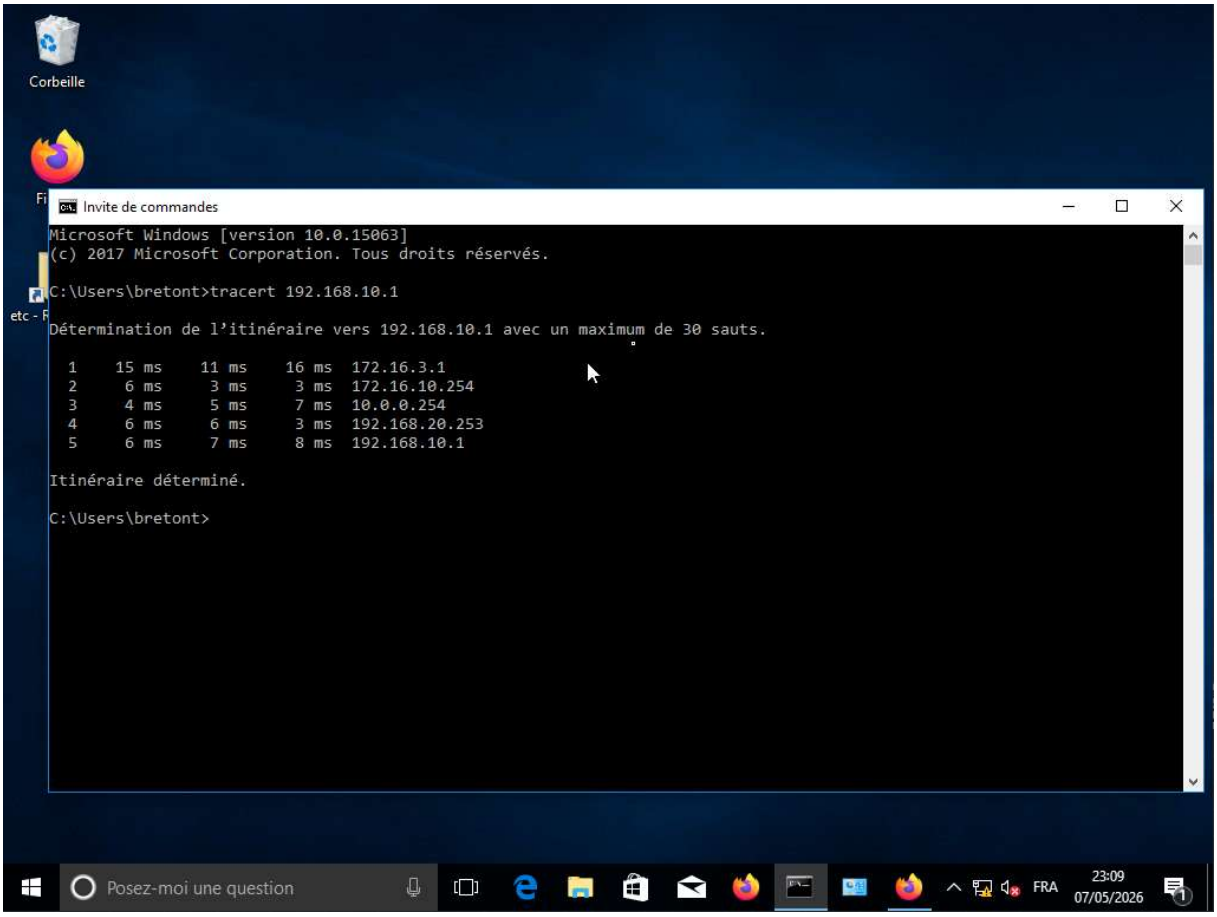
| TEST DE COMMUNICAITON ENTRE LES ROUTEUR | | |
|---|---|---|
| Win_10_1 | Windows Server – 192.168.10.1 | ✅ |
| Win_10_2 | Windows Server – 192.168.10.1 | ✅ |
| Win_10_3 | Windows Server – 192.168.10.1 | ✅ |

**Légende :**

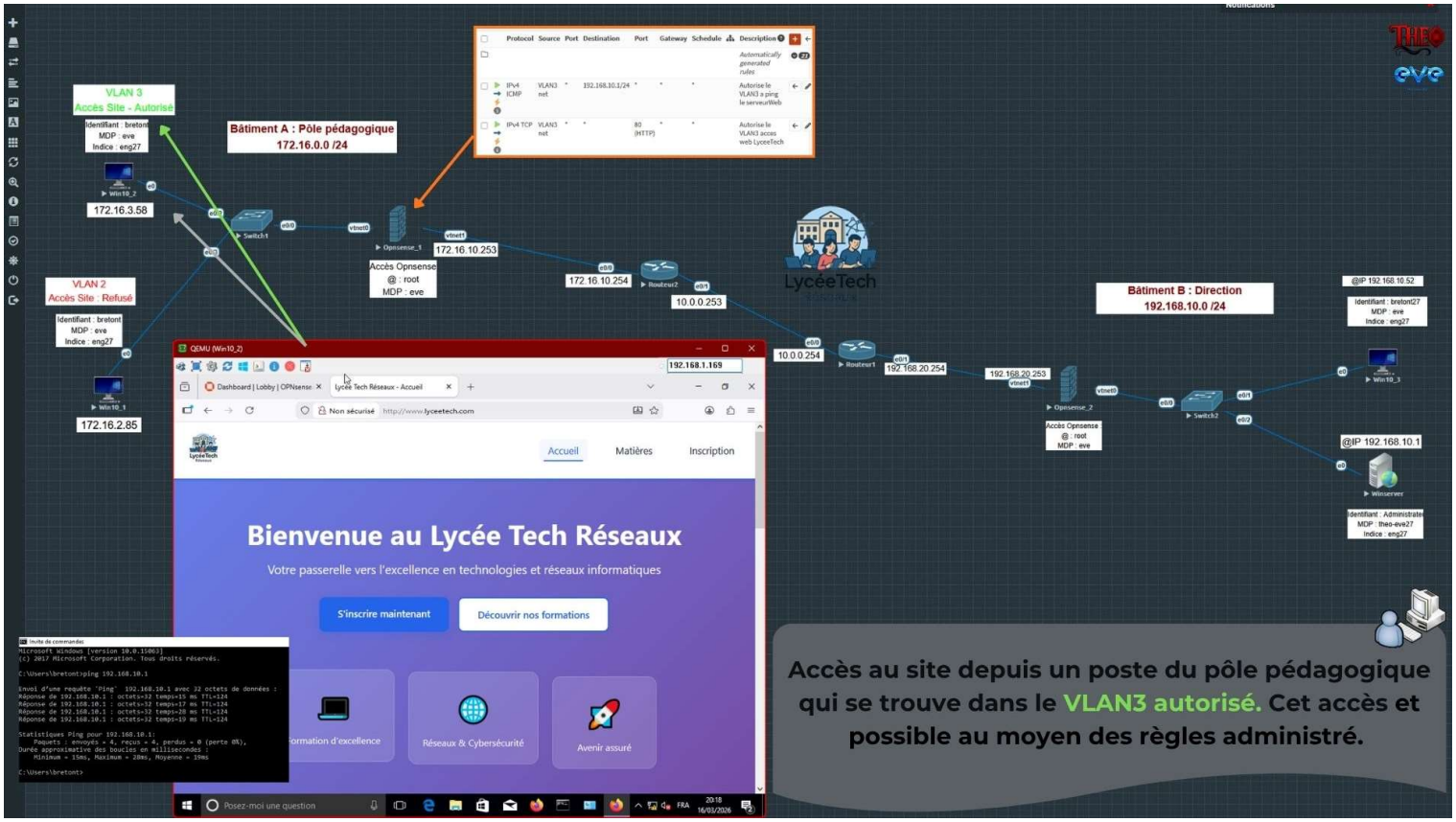
✅ 100% Réussis – 0 paquet perdu
⏱ Délais d'attente dépasser
❌ N'arrive pas à joindre le destinataire
⚠ Impossible de joindre l'hôte de destination

## Test Final

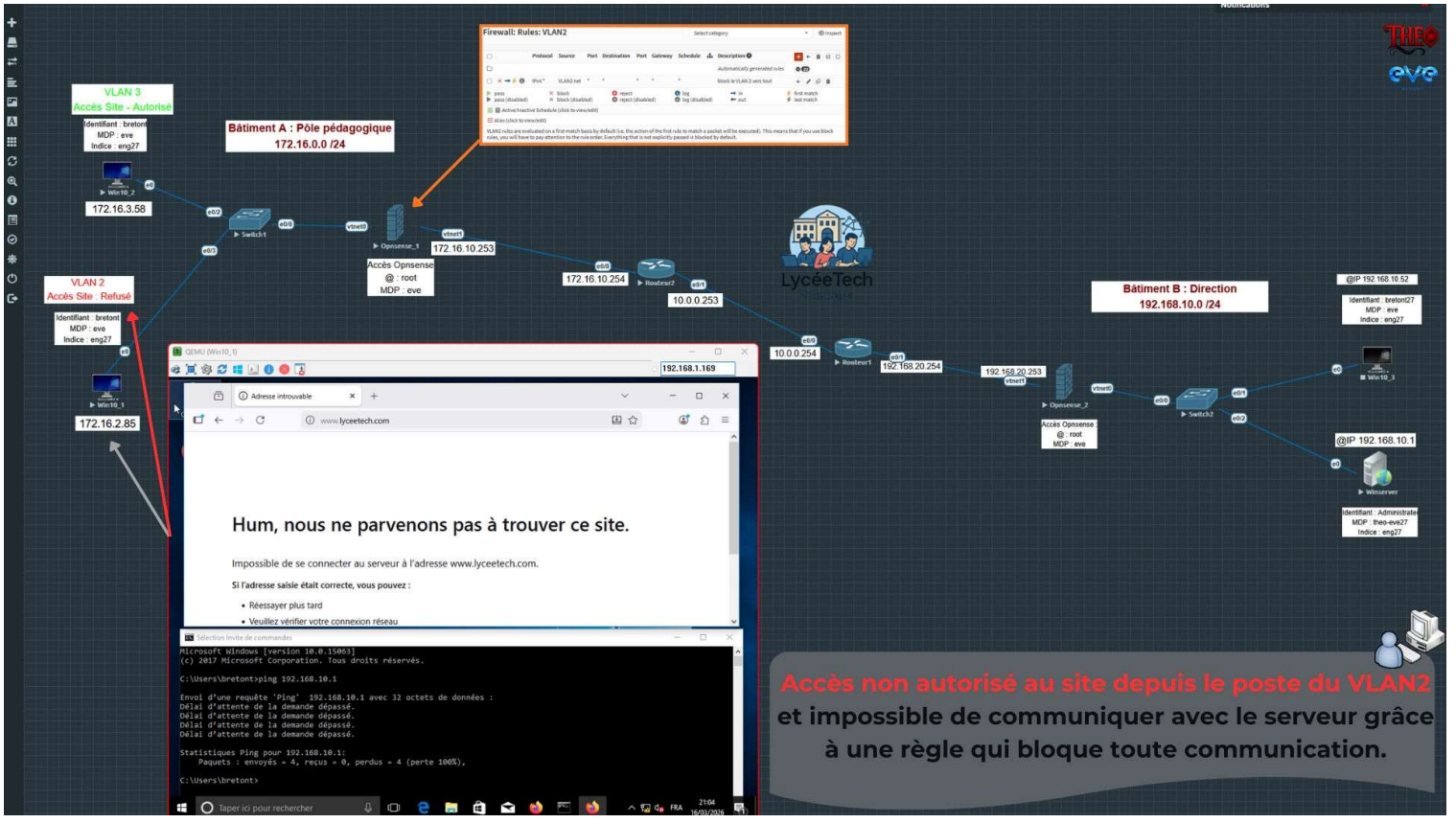
**Tracert depuis le poste du VLAN3 avant d'aller sur le site :**



## Accès au site Web depuis le poste du VLAN3




## Non Accès au site Web depuis le poste du VLAN2



## Accès au site Web depuis le poste de direction :