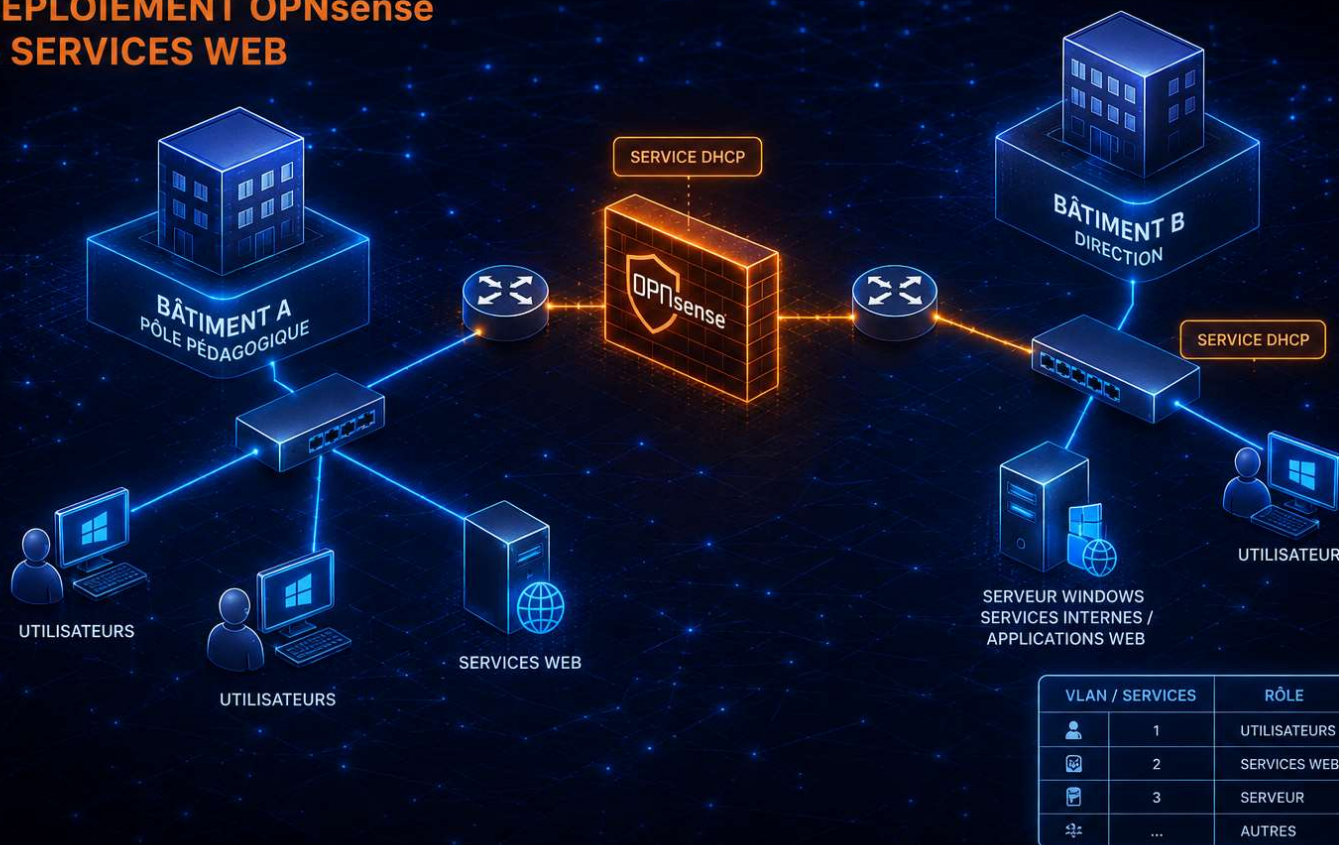


SÉCURISATION D'UNE INFRASTRUCTURE MULTI-SITES : DÉPLOIEMENT OPNsense & SERVICES WEB



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 réseaux différents : 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.
- ☞ **Paramétrage 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.

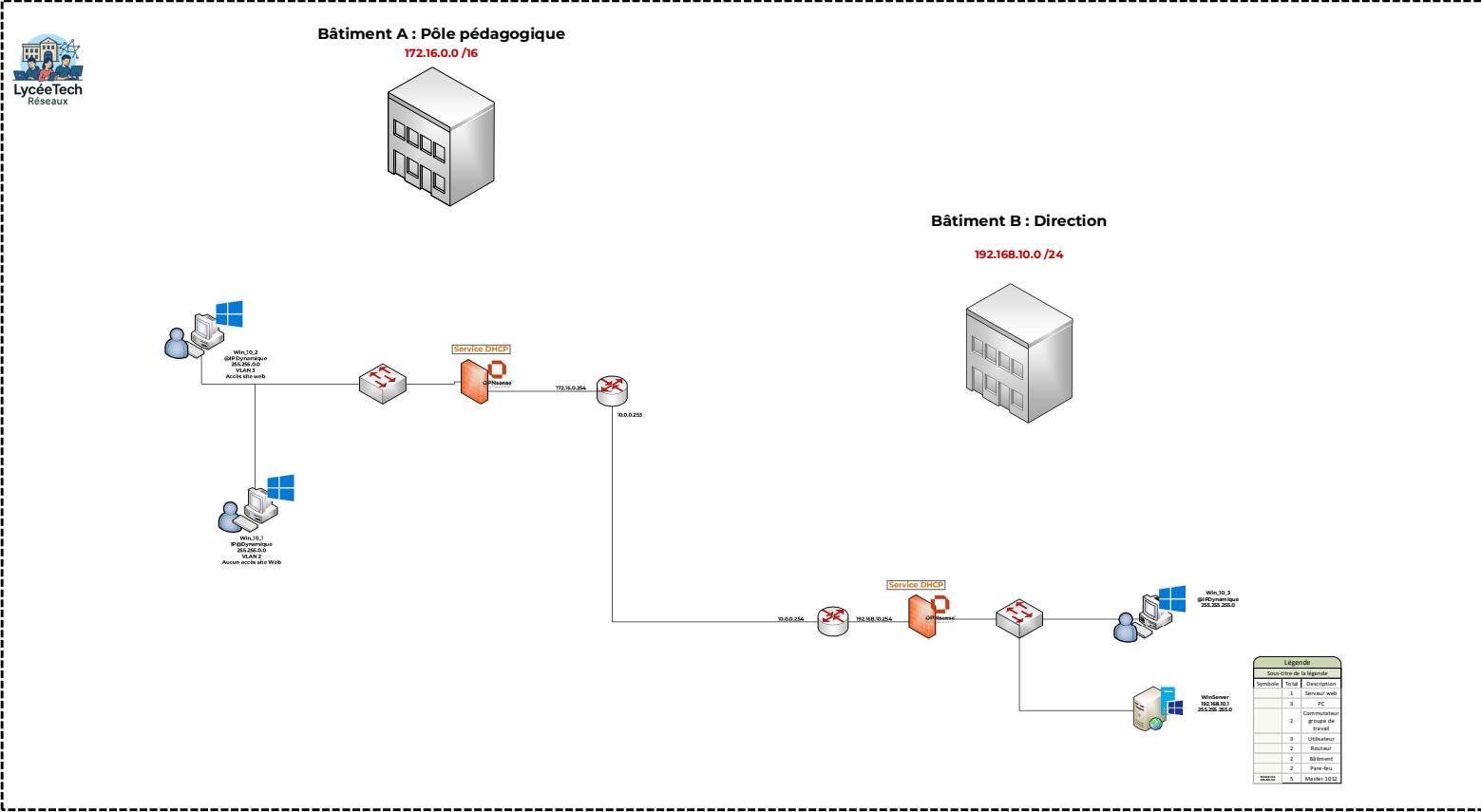
Partie Configuration Opnsense1 :

Sécuriser l'accès Web des pare feu Opnsense

Dans **System → Settings**, configure ces éléments :

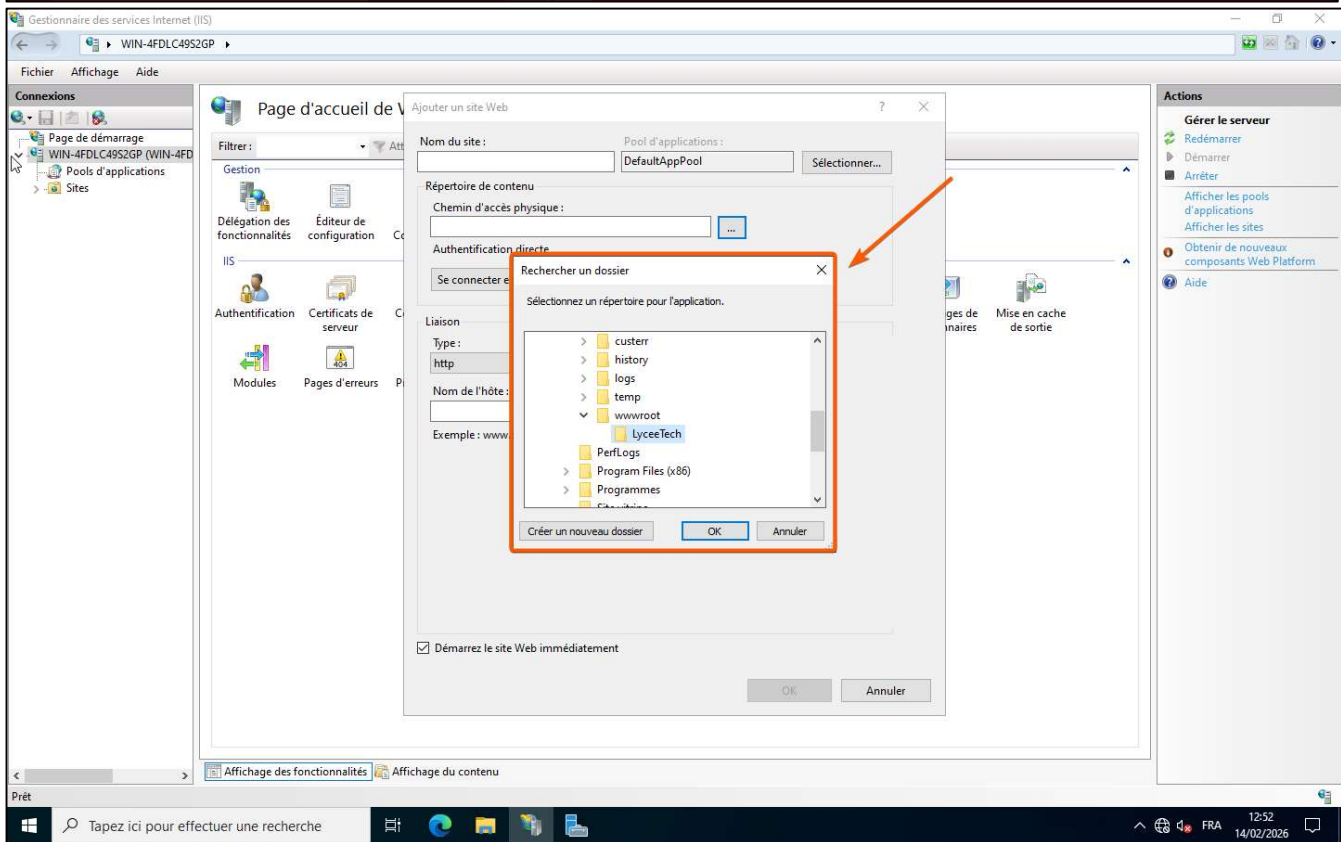
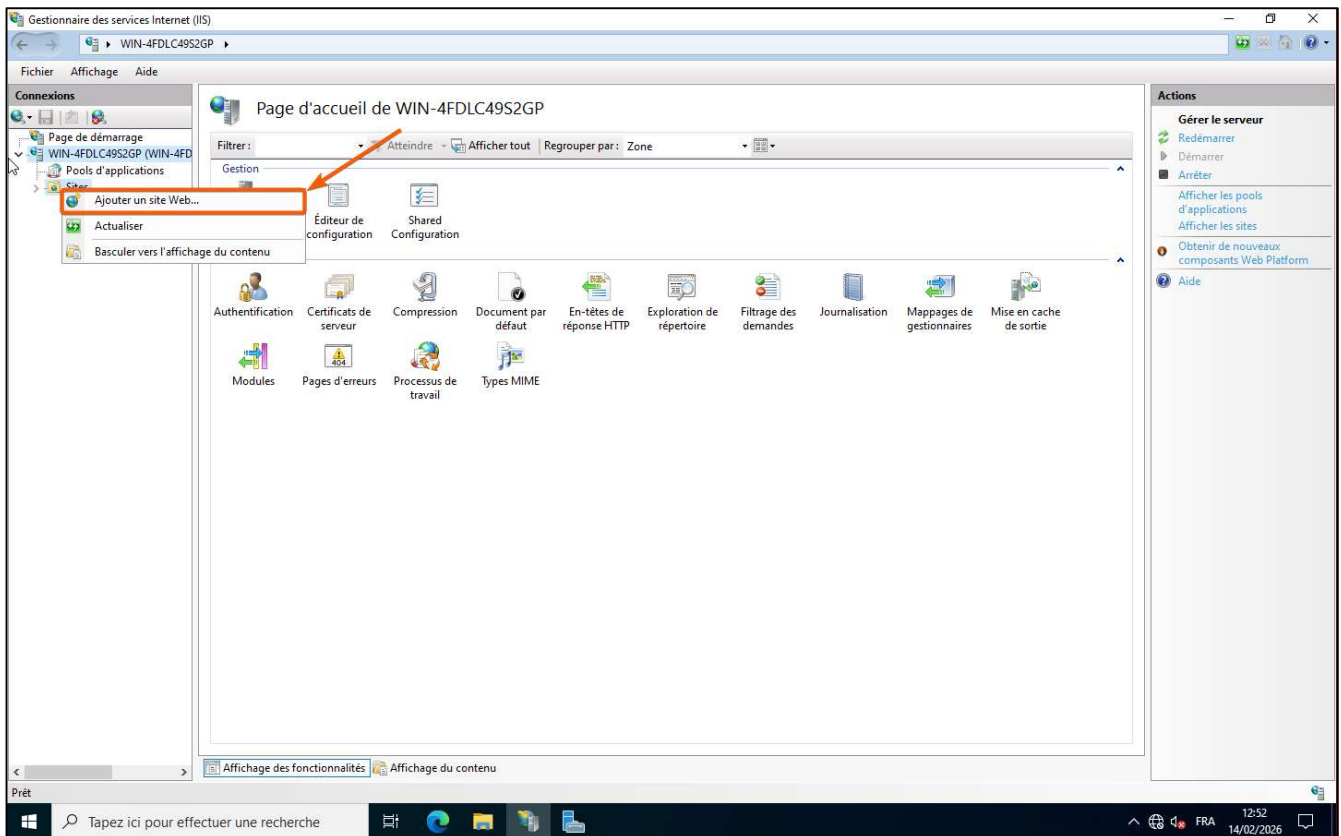
- ☞ **Accès VLAN 2 – non autorisé**
- ☞ **Accès VLAN 3 – Autorisé**
- ☞ **Configuration du service DHCP**
- ☞ **Configuration des règles du pare feu nécessaire pour les accès au site Web du bâtiment B**

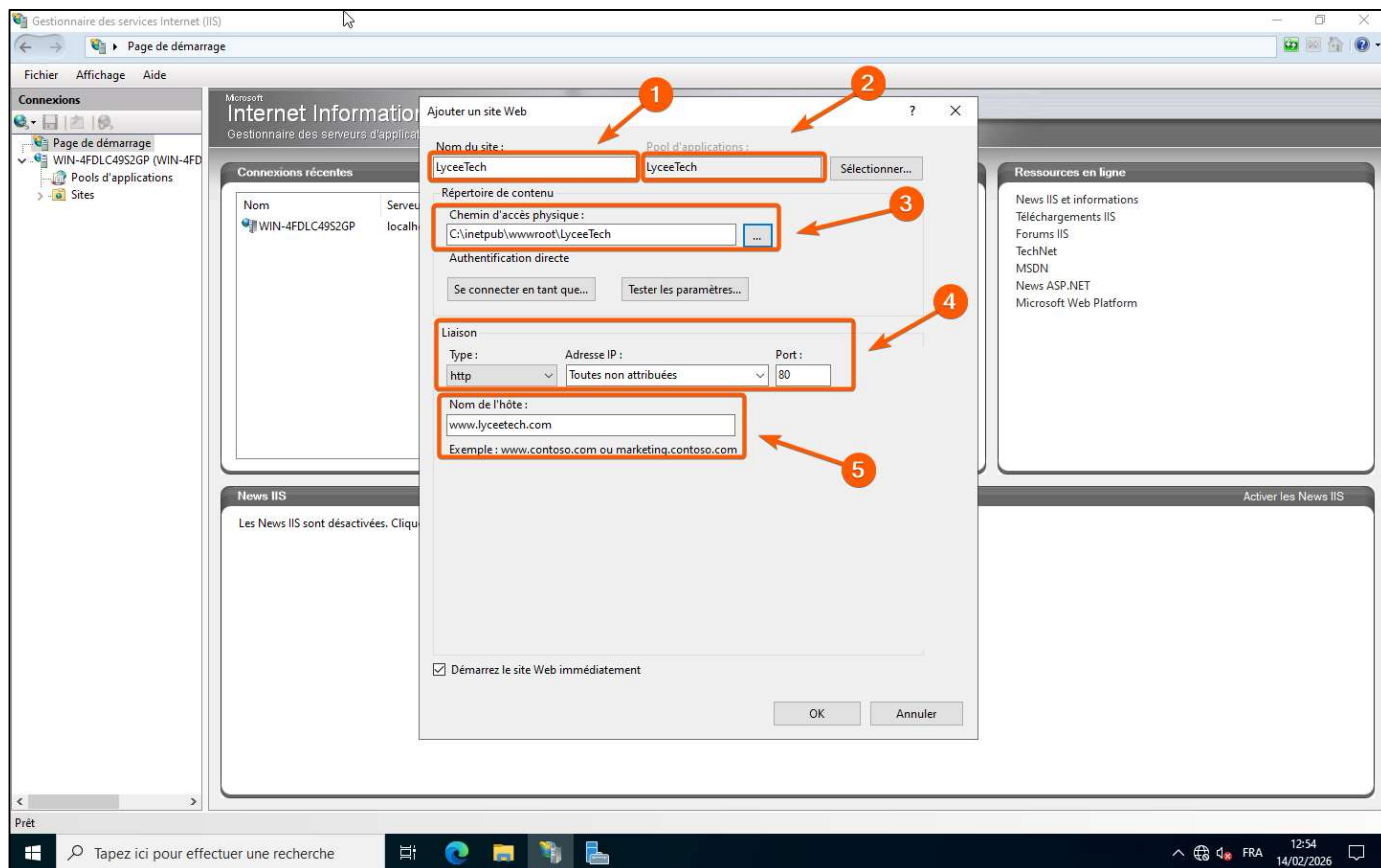
Schéma Réseau - LycéeTech Réseaux :



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

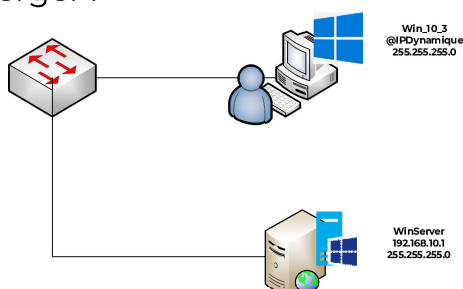
① Ajouter le rôle WebServer (IIS) et hébergé le site:





2 Tester :

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



```

Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Users\bretont>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=5 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=4 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=7 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=6 ms TTL=128

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 4ms, Maximum = 7ms, Moyenne = 5ms

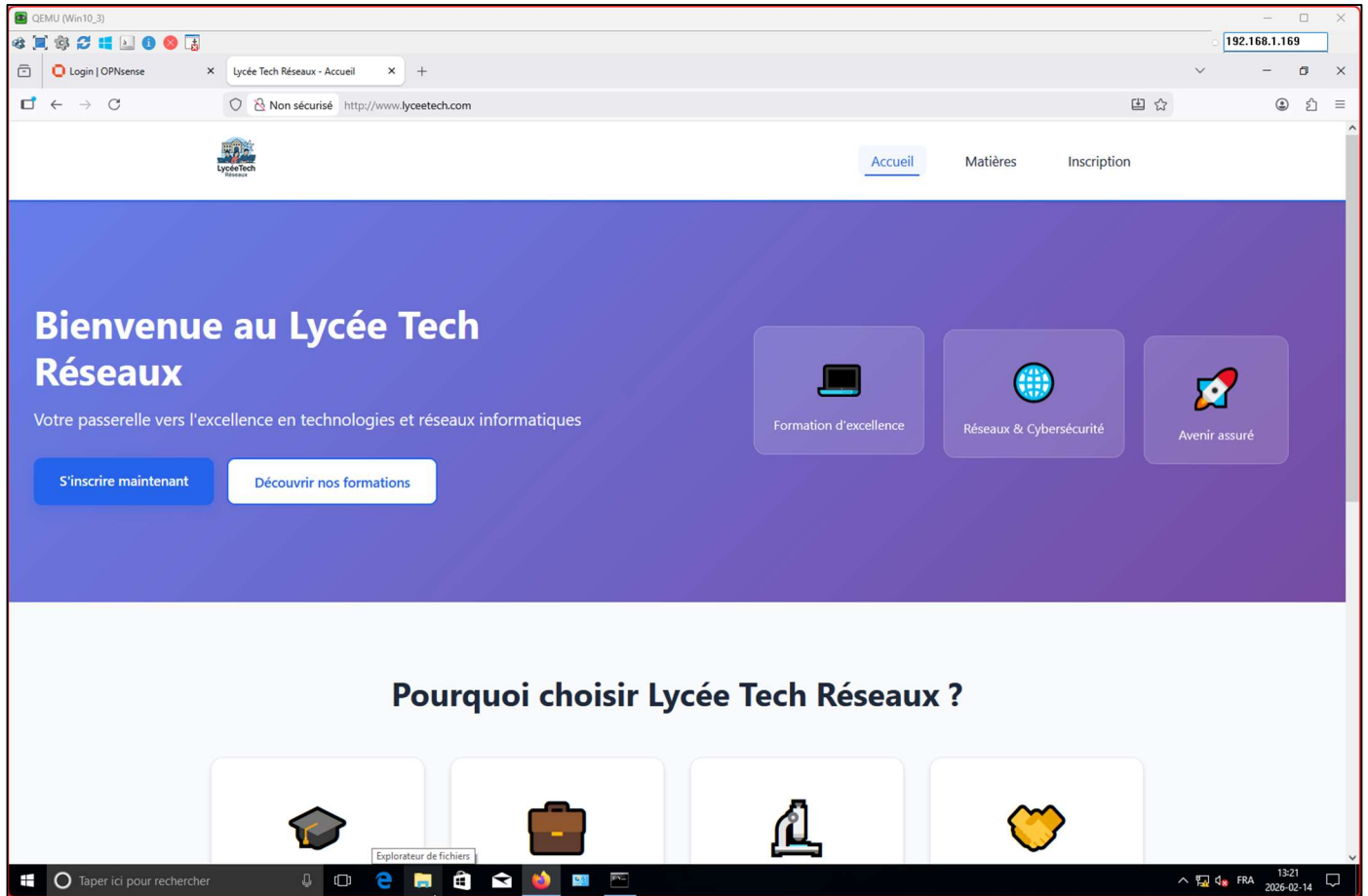
C:\Users\bretont>ping www.lyceetech.com

Envoi d'une requête 'ping' sur www.lyceetech.com [192.168.10.1] avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=7 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=8 ms TTL=128
Réponse de 192.168.10.1 : octets=32 temps=11 ms TTL=128

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 11ms, Moyenne = 6ms

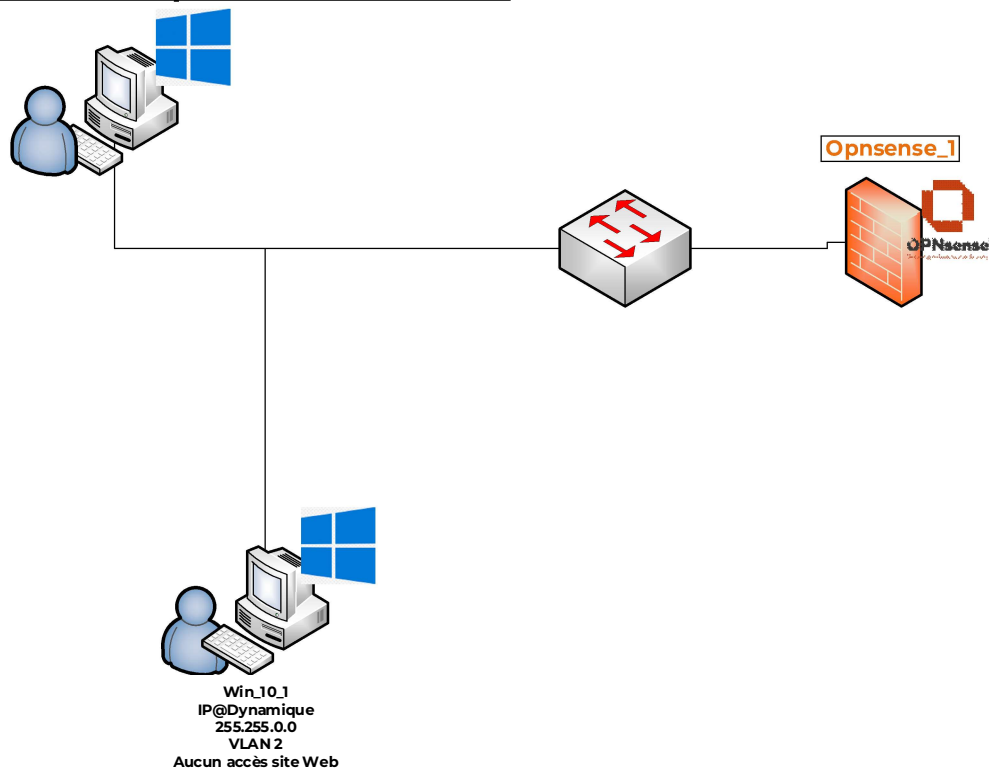
C:\Users\bretont>
  
```


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/opnsense-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:~# cd /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

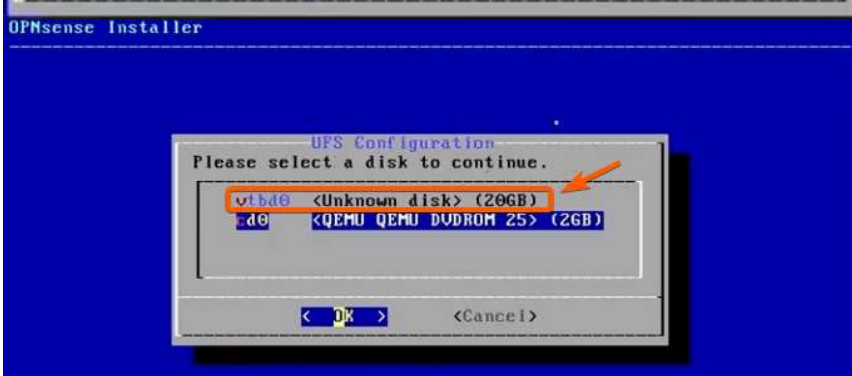
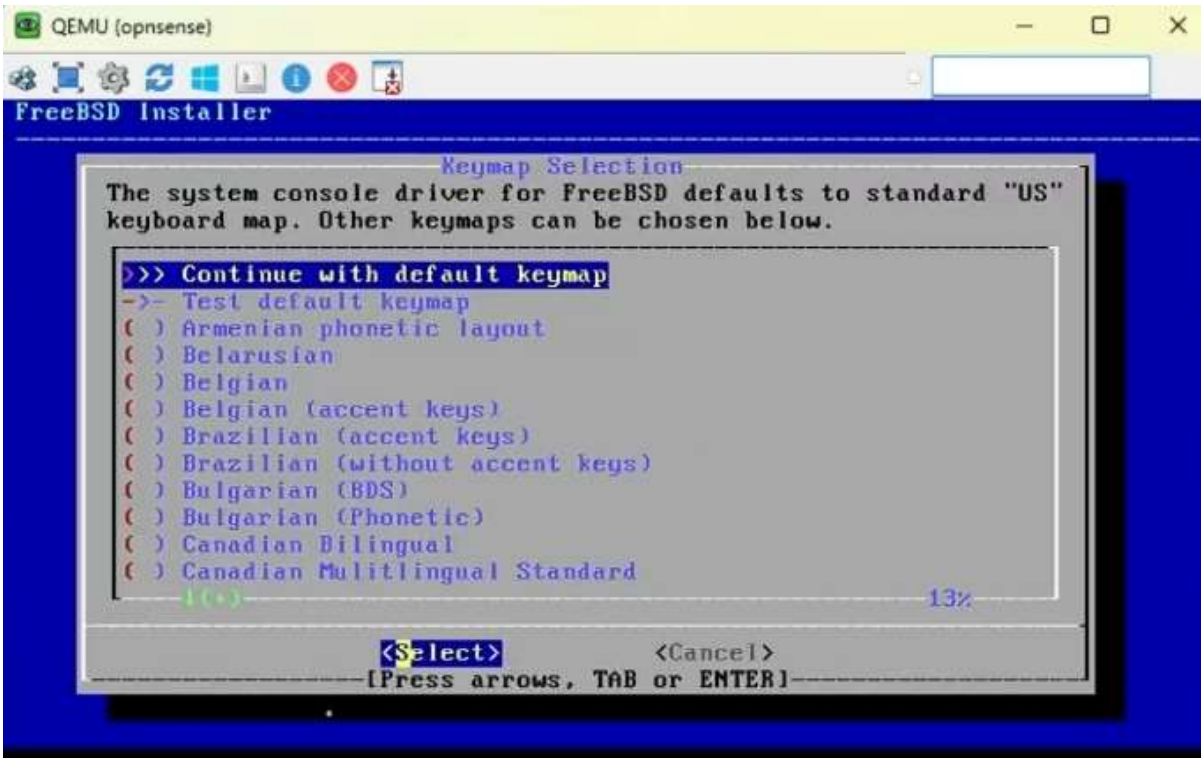
7. Démarrez le nœud et ouvrez la console (vnc)

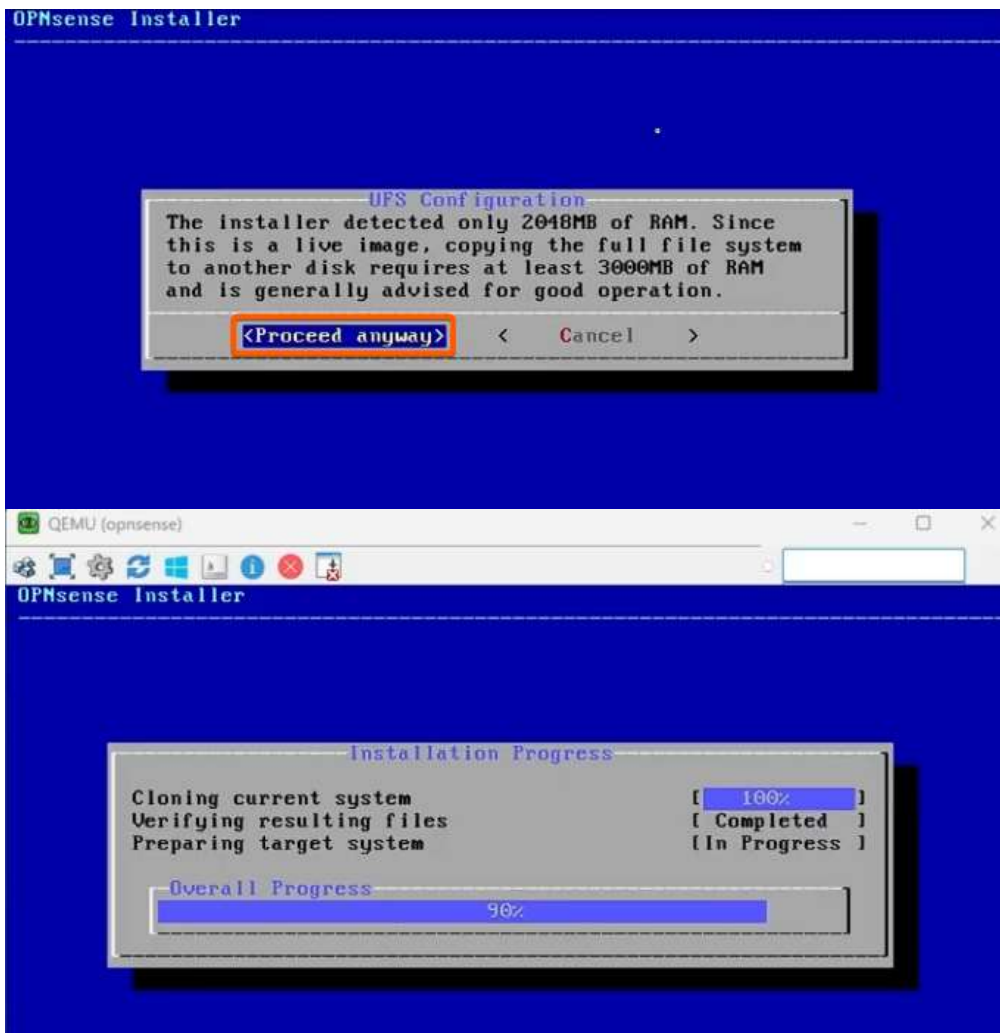
8. Attendez jusqu'à ce que le nœud démarre complètement à partir de l'ISO et utilisez la connexion avec le nom d'utilisateur: mot de passe d'installation: opnsense pour démarrer l'installation OPNsense

9. Utilisez tous les paramètres par défaut et l'installation complète

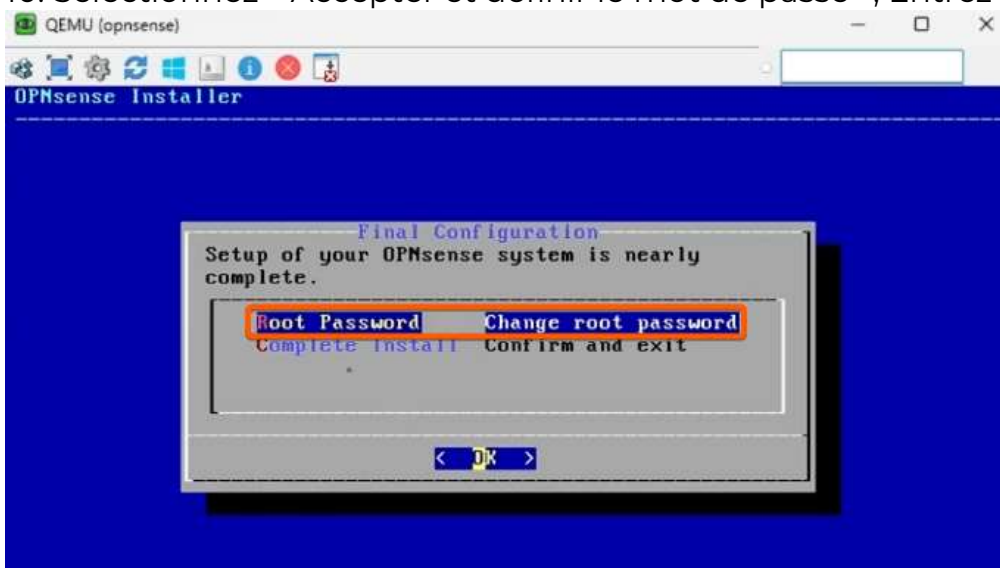
login : installer

mot de passe : opnsense



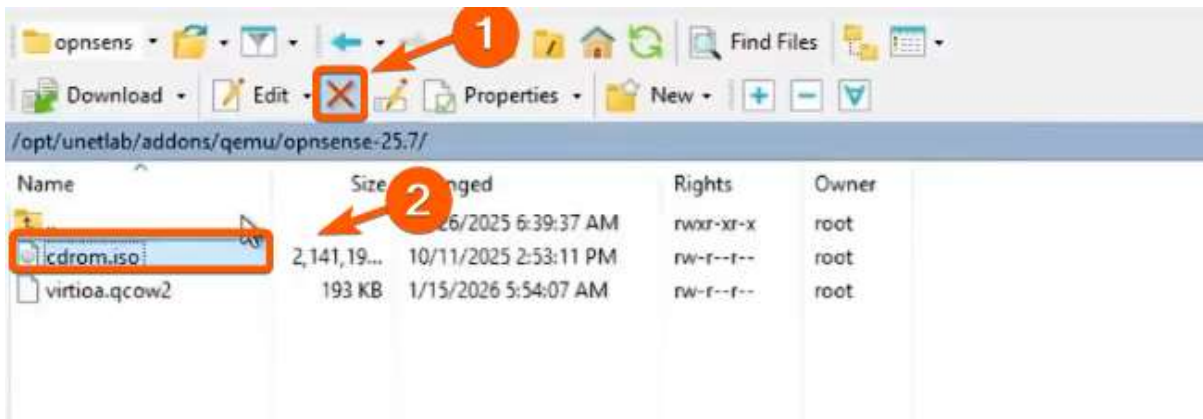


10. Sélectionnez « Accepter et définir le mot de passe », Entrez



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

```

QEMU (opnsense)

Website:  https://opnsense.org/
Handbook: https://docs.opnsense.org/
Forums:   https://forum.opnsense.org/
Code:     https://github.com/opnsense
Reddit:   https://reddit.com/r/opnsense

*** OPNsense.internal: OPNsense 25.7 (amd64) ***

LAN (vtnet0)  -> v4: 192.168.1.1/24
WAN (vtnet1)  ->

HTTPS: sha256 D7 07 8A 03 C3 F6 19 DA FD AB 89 B4 9B 82 1C E1
              3F 3A 41 D5 36 7D 69 6F 03 EA 59 70 7B 3A 39 93

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system

7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option:

```

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

```
QEMU (Opnsense_1)
192.168.1.169
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK

>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: zroot/ROOT/default
Sat Feb 21 15:24:01 UTC 2026

*** OPNsense.internal: OPNsense 26.1 (amd64) ***

LAN (vtnet0)    -> v4: 172.16.0.1/24
ULAN2 (vlan01)  -> v4: 172.16.2.1/24
ULAN3 (vlan02)  -> v4: 172.16.3.1/24
WAN (vtnet1)    -> v4: 172.16.0.253/24

HTTPS: SHA256 EE 6F 79 11 63 F0 A9 7E 4A 0A 9B 16 BA 6F C0 F8
              C9 BC B5 D4 B8 1F C8 F8 E9 21 AF C1 1C BB 27 D7

FreeBSD/amd64 (OPNsense.internal) (ttyv0)
login: 
```

```
QEMU (Opnsense_2)
192.168.1.169
Starting hostwatch.
>>> Invoking start script 'syslog'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK

>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: zroot/ROOT/default
Sat Feb 21 18:03:20 UTC 2026

*** OPNsense.internal: OPNsense 26.1 (amd64) ***

LAN (vtnet0)    -> v4: 192.168.10.3/24
WAN (vtnet1)    -> v4: 192.168.10.253/24

HTTPS: SHA256 37 F6 46 F3 80 07 C5 8F 7B 80 A1 32 CF 5F 06 16
              87 67 89 86 7A E3 91 14 05 63 C9 5C 91 8C 4D A0

FreeBSD/amd64 (OPNsense.internal) (ttyv0)
login: 
```

3^{ème} phase du projet : Configuration du pare-feu OPNsense_1 :

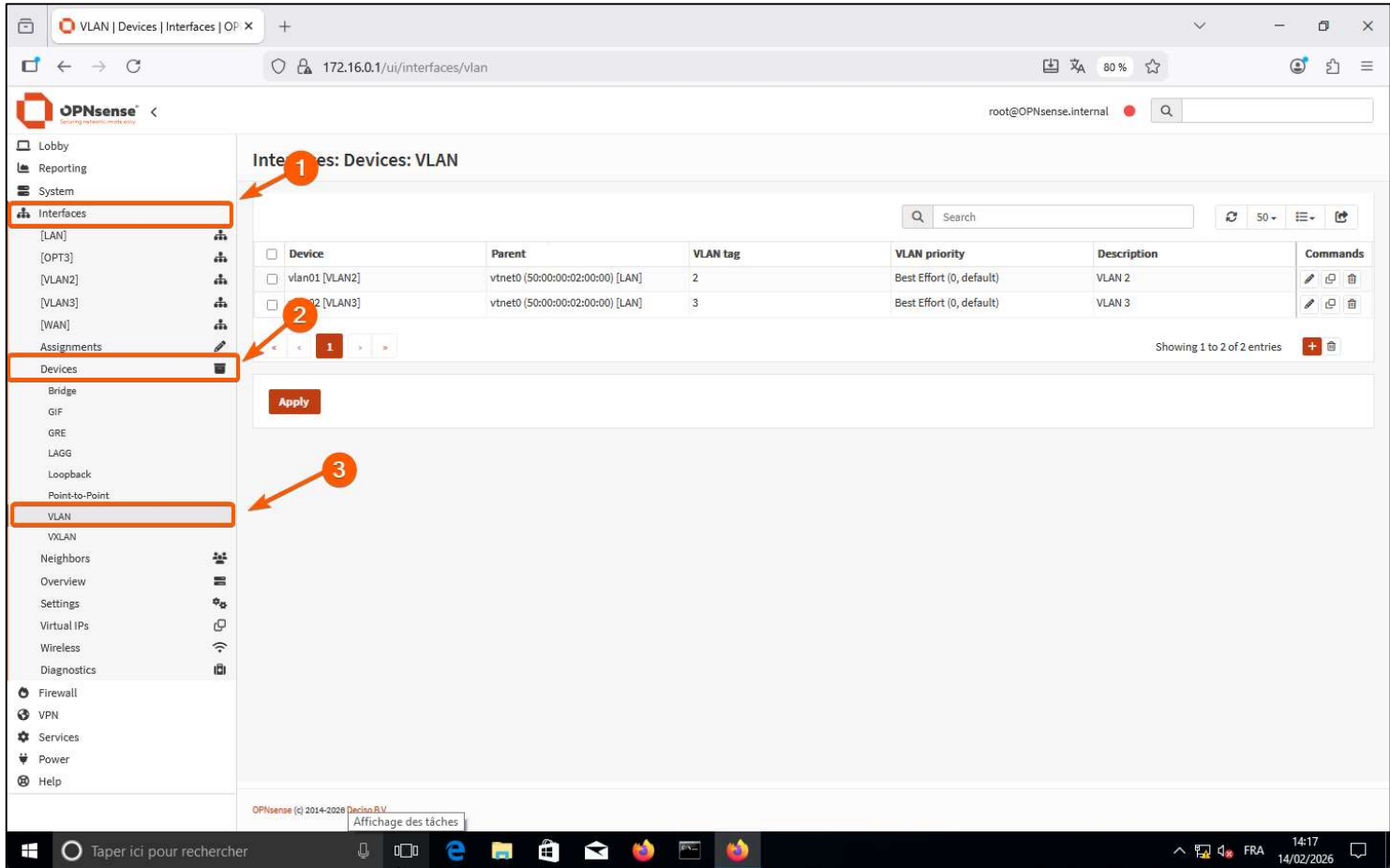
Etape 1 : Configuration des VLAN2 et VLAN3 sur le pare-feu **OPNsense_1** :

1. Création des VLANs dans OPNsense

Aller dans le menu VLAN

Dans le menu de gauche :

Interfaces → VLAN



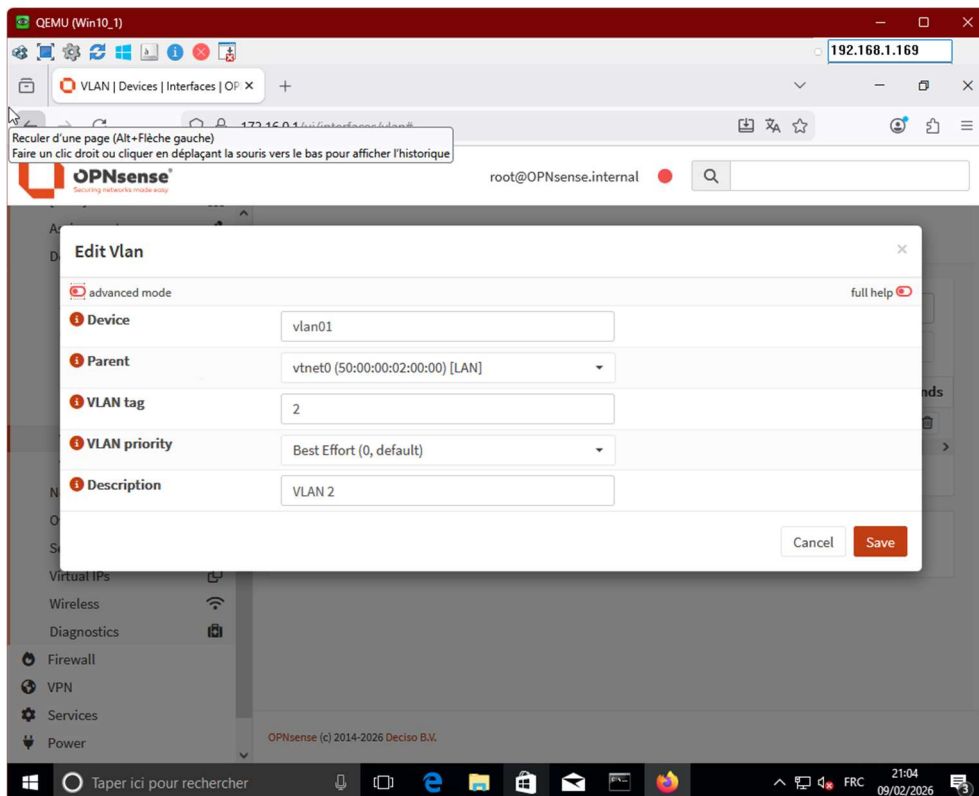
2. Créer un VLAN

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**.

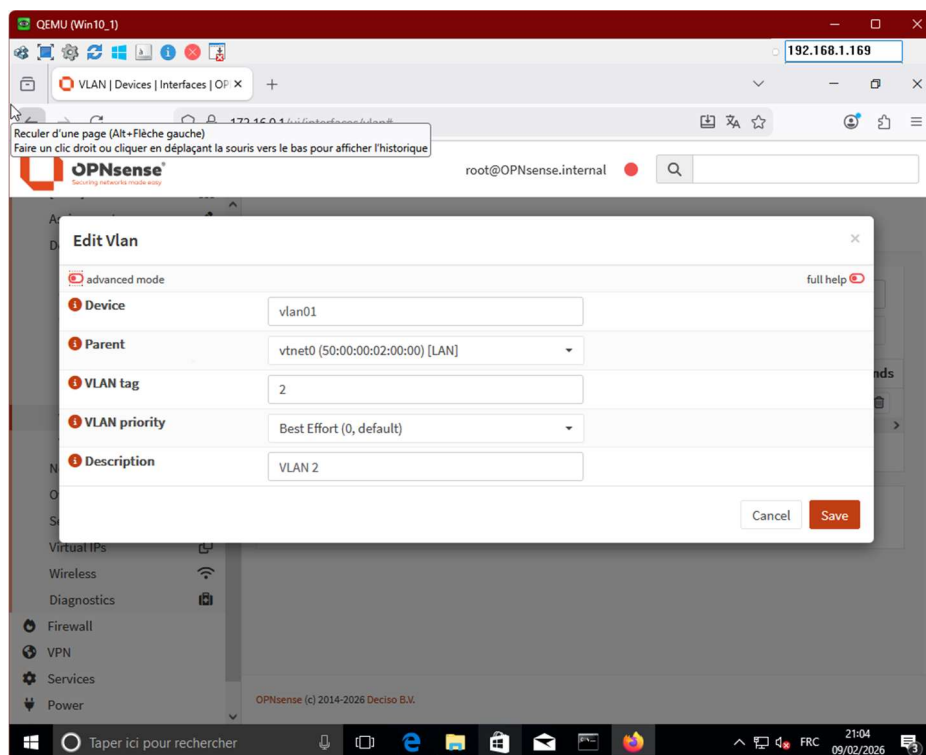


3. Créer le deuxième VLAN

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**.

The screenshot shows the OPNsense web interface in a browser window. The page title is 'Interfaces: Assignments'. It features a table with the following columns: Interface, Identifier, and Device. The table contains four rows of data:

Interface	Identifier	Device
[LAN]	lan	vtnet0 (50:00:00:02:00:00)
[VLAN2]	opt1	vlan01 VLAN2 (Parent: vtnet0, Tag: 2)
[VLAN3]	opt2	vlan02 VLAN3 (Parent: vtnet0, Tag: 3)
[WAN]	wan	vtnet1 (50:00:00:02:00:01)

Below the table is a section titled '+ Assign a new interface' with a 'Device' dropdown menu and a 'Description' text input field. At the bottom of this section is an 'Add' button. A 'Save' button is located at the bottom of the table. Five orange arrows with numbers 1 through 5 point to the following elements: 1 points to the 'Interface' column header, 2 points to the 'Identifier' column header, 3 points to the 'Device' column header, 4 points to the 'Save' button, and 5 points to the 'Add' button in the 'Assign a new interface' section.

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** !

The screenshot shows the OPNsense web interface for configuring the [VLAN2] interface. The interface is being configured with the following settings:

- Basic configuration:**
 - Enable: ☒ Enable interface
 - Lock: ☐ Prevent interface removal
 - Identifier: opt1
 - Device: vlan01
 - Description: VLAN2
- Generic configuration:**
 - Block private networks: ☐
 - Block bogon networks: ☐
 - IPv4 Configuration Type: Static IPv4
 - IPv6 Configuration Type: None
 - MAC address:
 - Promiscuous mode: ☐
 - MTU:
 - MSS:
 - Dynamic gateway policy: ☐ This interface does not require an intermediate system to act as a gateway
- Static IPv4 configuration:**
 - IPv4 address: 172.16.2.1 /24
 - IPv4 gateway rules: Disabled

The Save button is highlighted with a red box and a number 5.

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** !

The screenshot shows the OPNsense web interface for configuring the 'VLAN3' interface. The interface is named 'opt2' and is associated with 'vlan02'. The configuration is set to 'Static IPv4' with the address '172.16.3.1' and a subnet mask of '24'. The 'Enable interface' checkbox is checked. Red arrows and numbers 1 through 5 highlight the key configuration steps: 1. Enable interface, 2. Identifier and Device, 3. IPv4 Configuration Type, 4. IPv4 address and gateway rules, 5. Save button.

6. Configurer la passerelle pour l'interface WAN

Aller dans :

System → Gateways → Configuration

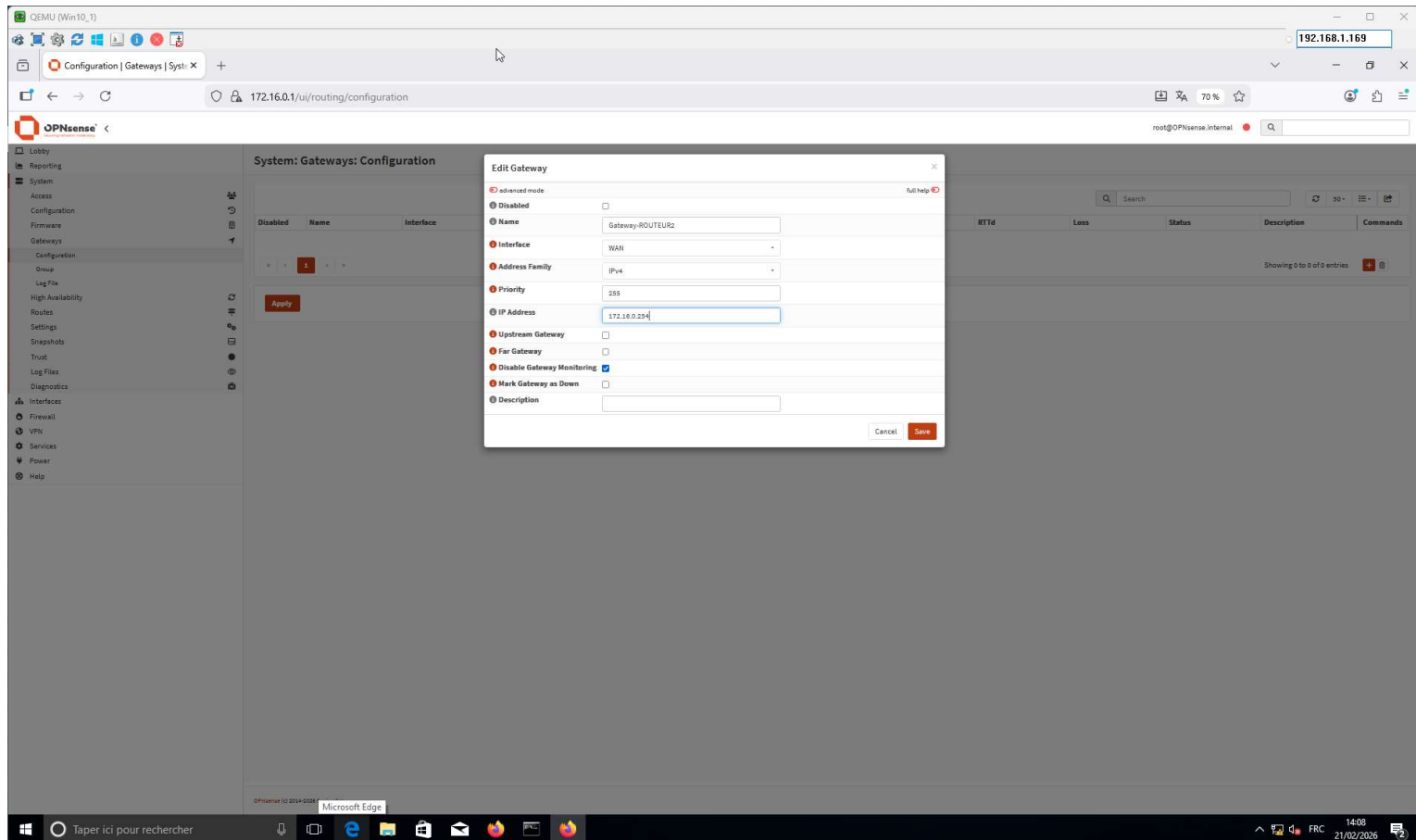
Décocher **Disabled**

Description : Gateway-ROUTEUR2

IPv4 Configuration Type : Static IPv4

IPv4 Address : 172.16.0.254

Save, puis **Apply Changes** !



QEMU (Win10_T)

192.168.1.169

Configuration | Gateways | Syst: X

172.16.0.1/ui/routing/configuration

70 %

root@OPNsense.internal

OPNsense

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

50

Disabled	Name	Interface	Address Family	Priority	IP Address	Monitor IP	RTT	RTTid	Loss	Status	Description	Commands
	Gateway-ROUTEUR2 (active)	WAN	IPv4	255	172.16.0.224		~	~	~			

Showing 1 to 1 of 1 entries

Apply

OPNsense

Affichage des tâches

Taper ici pour rechercher

14:06

FRC

21/02/2026



7. Configuration de l'interface WAN

Interfaces → WAN

Cocher **Enable Interfaces**

Décocher les cases suivantes :

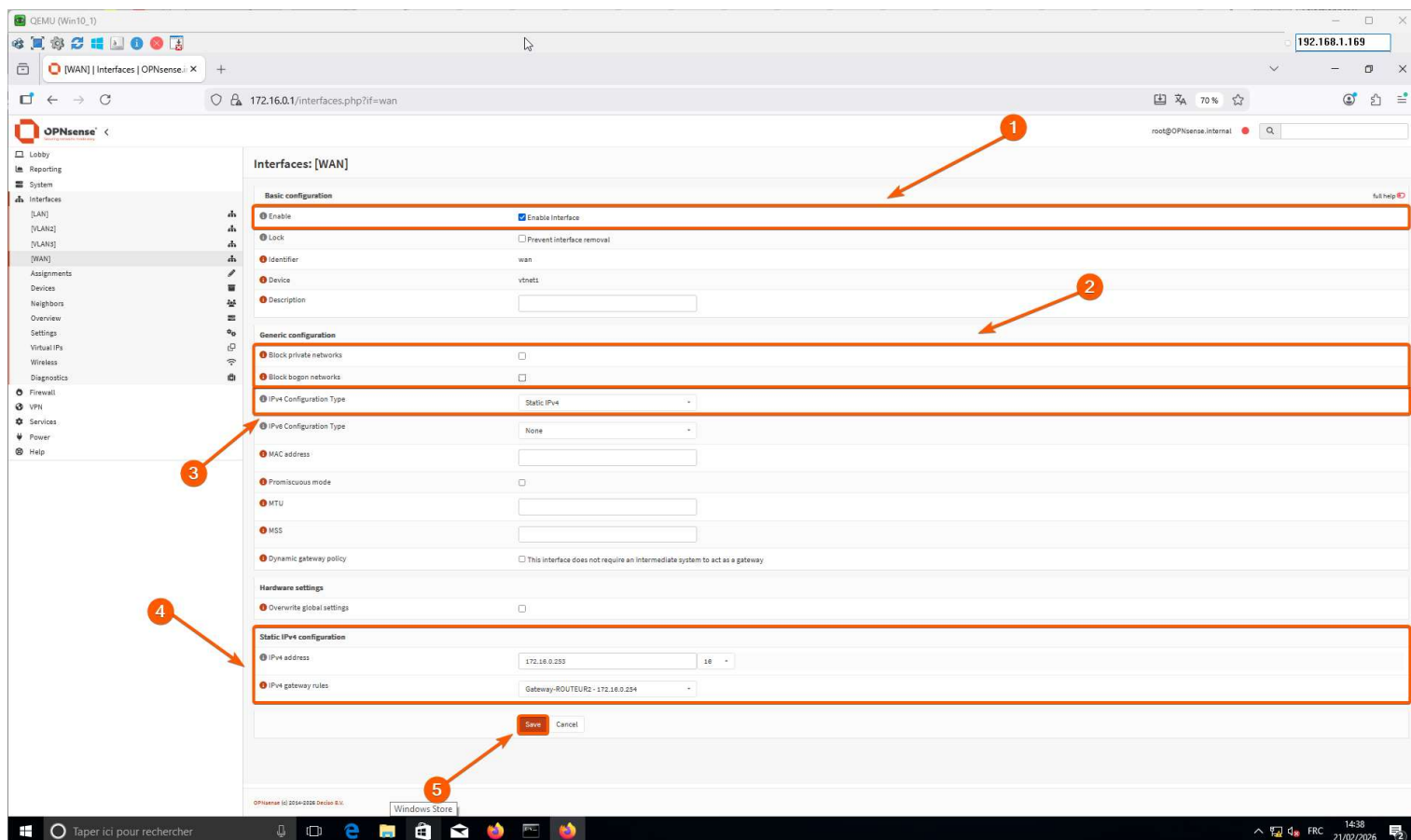
- ☐ **Block private networks** → Interdit les IPs type 192.168.x.x, 172.16.x.x ou 10.x.x.x sur le WAN.
- ☐ **Block bogon networks** → Interdit les IPs qui n'existent pas officiellement sur le web (IPs non assignées).

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 :

QEMU (Win10_T)

192.168.1.169

Assignments | Interfaces | OPN: X

172.168.0.1/interfaces_assign.php

OPNsense

root@OPNsense.internal

Lobby

Reporting

System

Interfaces

[LAN]

[VLAN2]

[VLAN3]

[WAN]

Assignments

Devices

Neighbors

Overview

Settings

Virtual IPs

Wireless

Diagnostics

Firewall

VPN

Services

Power

Help

Interfaces: Assignments

Interface	Identifier	Device	
[LAN]	lan	vtnet0 (50:00:00:02:00:00)	
[VLAN2]	opt1	vlan01 VLAN2 (Parent: vtnet0, Tag: 2)	
[VLAN3]	opt2	vlan02 VLAN3 (Parent: vtnet0, Tag: 3)	
[WAN]	wan	vtnet1 (50:00:00:02:00:01)	

Save

+ Assign a new interface

Device

vtnet2 (50:00:00:02:00:02)

Description

Add

OPNsense

Affichage des tâches

Windows Taskbar

14:32 21/02/2026

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

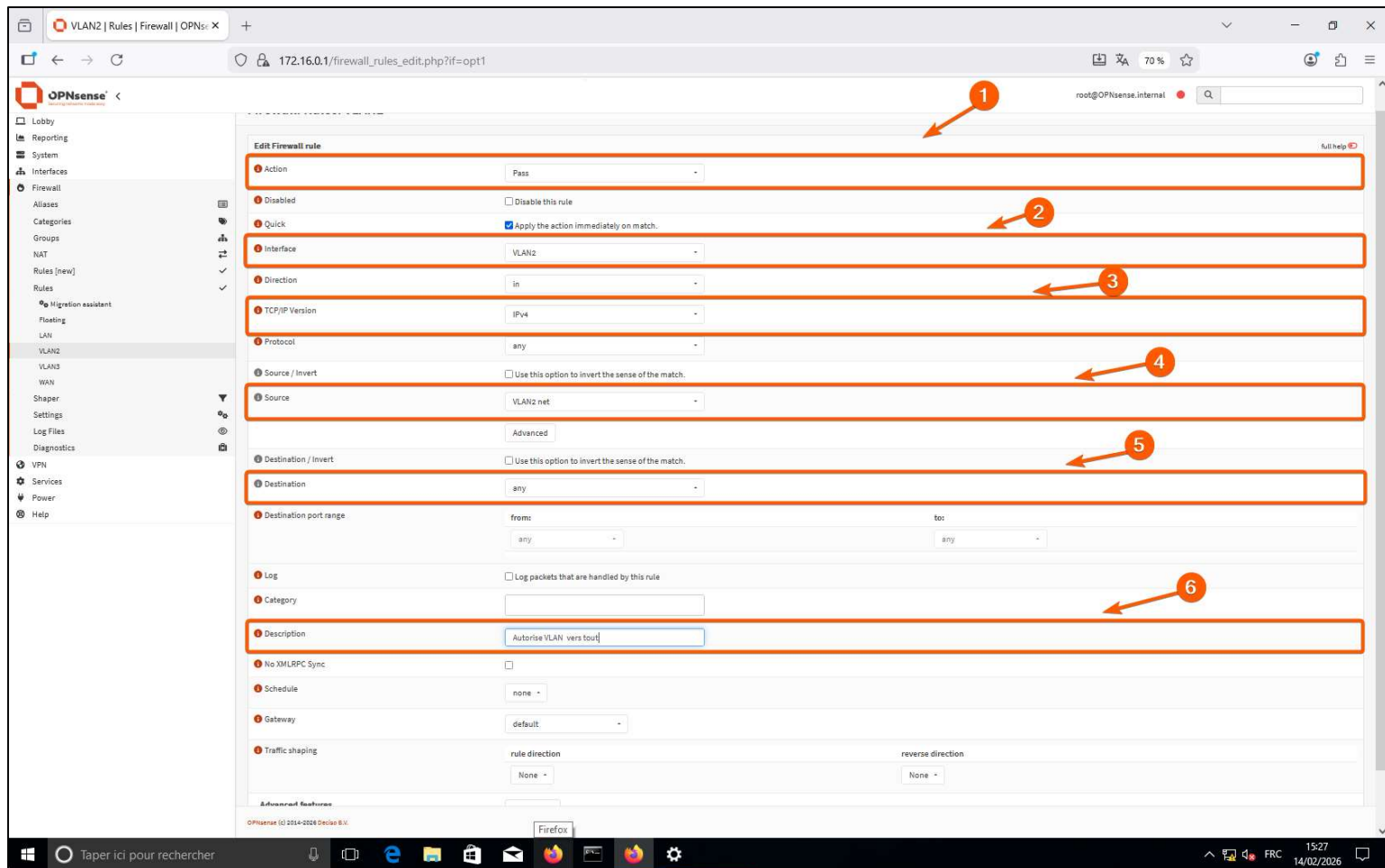
En haut → cliquer sur **+ Add**

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 :

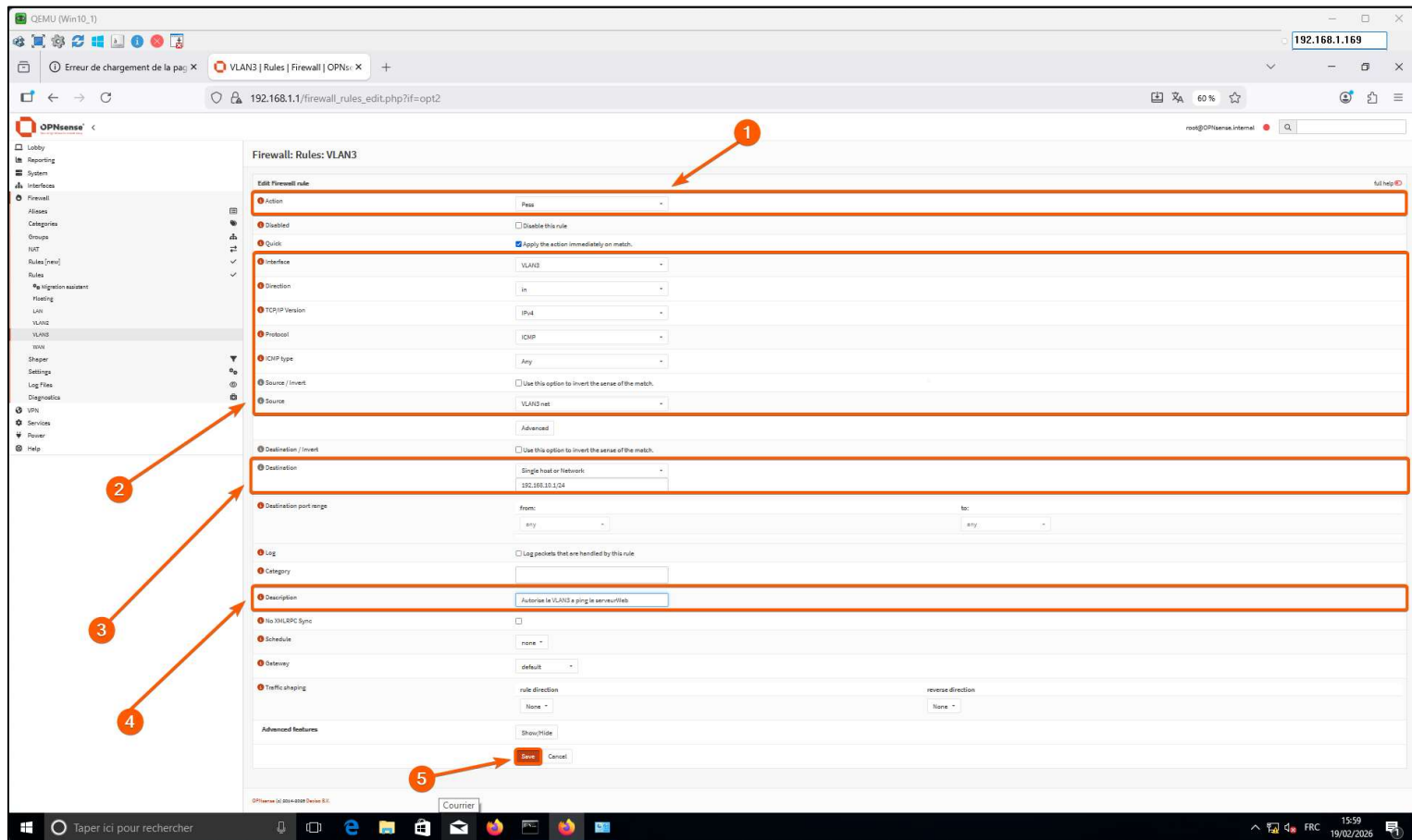
- **Action** : Pass
- **Interface** : VLAN3
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : ICMP

→ 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 accéder 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)

VLAN3 | Rules | Firewall | OPNsense

172.16.0.1/firewall_rules_edit.php?if=opt2

192.168.1.169

OPNsense

1

2

3

4

5

6

7

8

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

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 LycéeTech

No SNLRPC Sync: ☐

Schedule: none

Gateway: default

Traffic shaping: rule direction: None reverse direction: None

Advanced features: Show/Hide

Save Cancel

OPNsense (c) 2014-2026 Deciso B.V.

Taper ici pour rechercher

15:30 14/02/2026

VLAN3 | Rules | Firewall | OPNsense

172.16.0.1/firewall_rules.php?if=opt2

192.168.1.169

OPNsense

Firewall: Rules: VLAN3

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 LycéeTech
☒	pass							
☒	pass (disabled)							
☒	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.

OPNsense (c) 2014-2026 Deciso B.V.

Invite de commandes

Taper ici pour rechercher

15:33 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 :

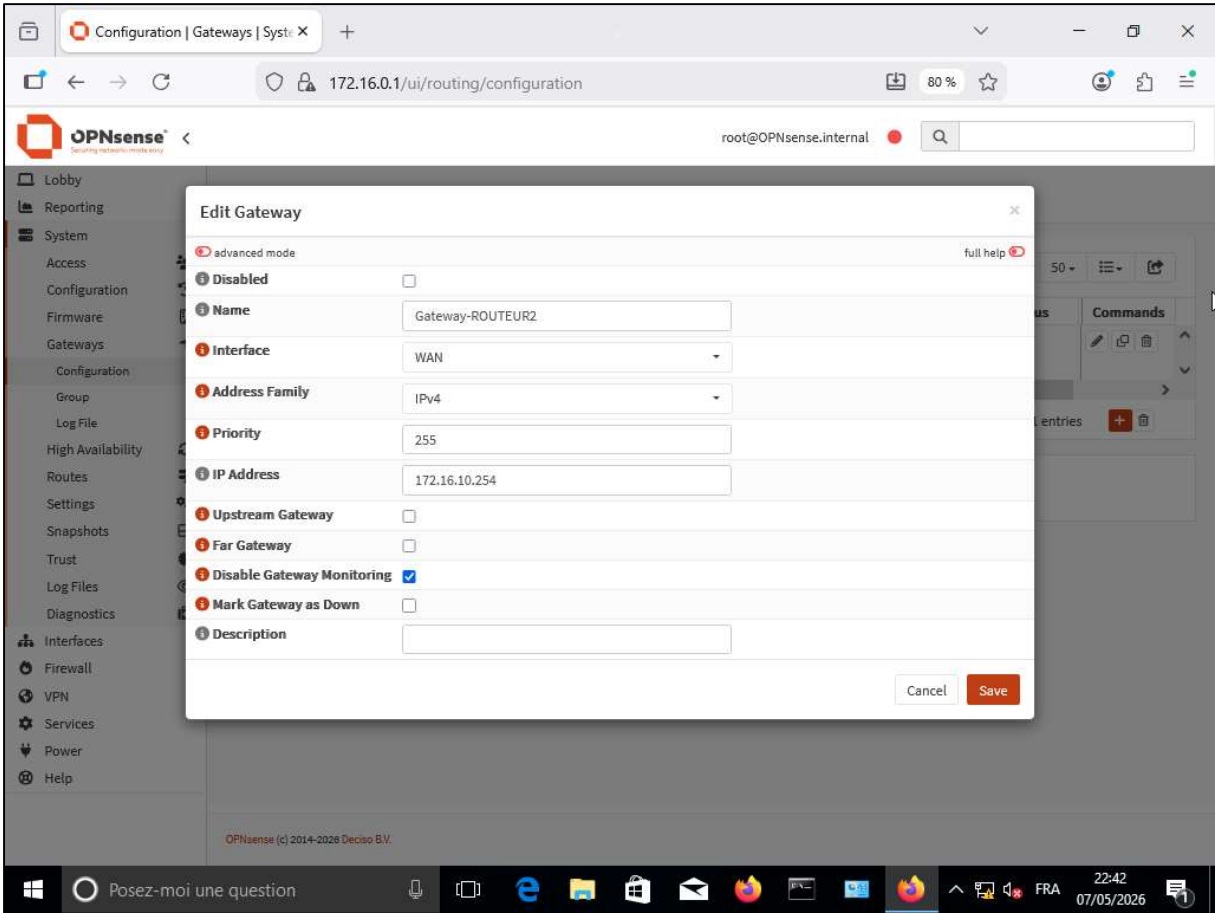
- **Action** : Pass
- **Interface** : VLAN3
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : any
- **Source** : VLAN3 net
- **Destination** : any
- **Description** : TEST FULL OPEN VLAN 3

Puis :

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

The screenshot shows the OPNsense web interface for configuring a firewall rule. The left sidebar contains navigation links like Lobby, Reporting, System, Interfaces, Firewall, and various rule categories. The main area is titled 'Firewall: Rules: VLAN3' and contains the 'Edit Firewall rule' form. The form has several sections: 'Action' (Pass), 'Quick' (Apply the action immediately on match), 'Interface' (VLAN3), 'Direction' (In), 'TCP/IP Version' (IPv4), 'Protocol' (any), 'Source / Invert' (Source: VLAN3 net), 'Destination / Invert' (Destination: any), 'Destination port range' (from: any, to: any), 'Log' (Log packets that are handled by this rule), 'Category' (empty), 'Description' (TEST FULL OPEN VLAN3), 'No XMLRPC Sync' (checkbox), and 'Schedule' (none). Four orange boxes with numbered arrows (1, 2, 3, 4) highlight specific configuration steps: 1. Action: Pass; 2. Quick: Apply the action immediately on match; 3. Source: VLAN3 net; 4. Description: TEST FULL OPEN VLAN3. The bottom of the page shows the OPNsense footer and a Windows taskbar.

Paramétrage de la Gateway du Routeur 2.



4^{ème} 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

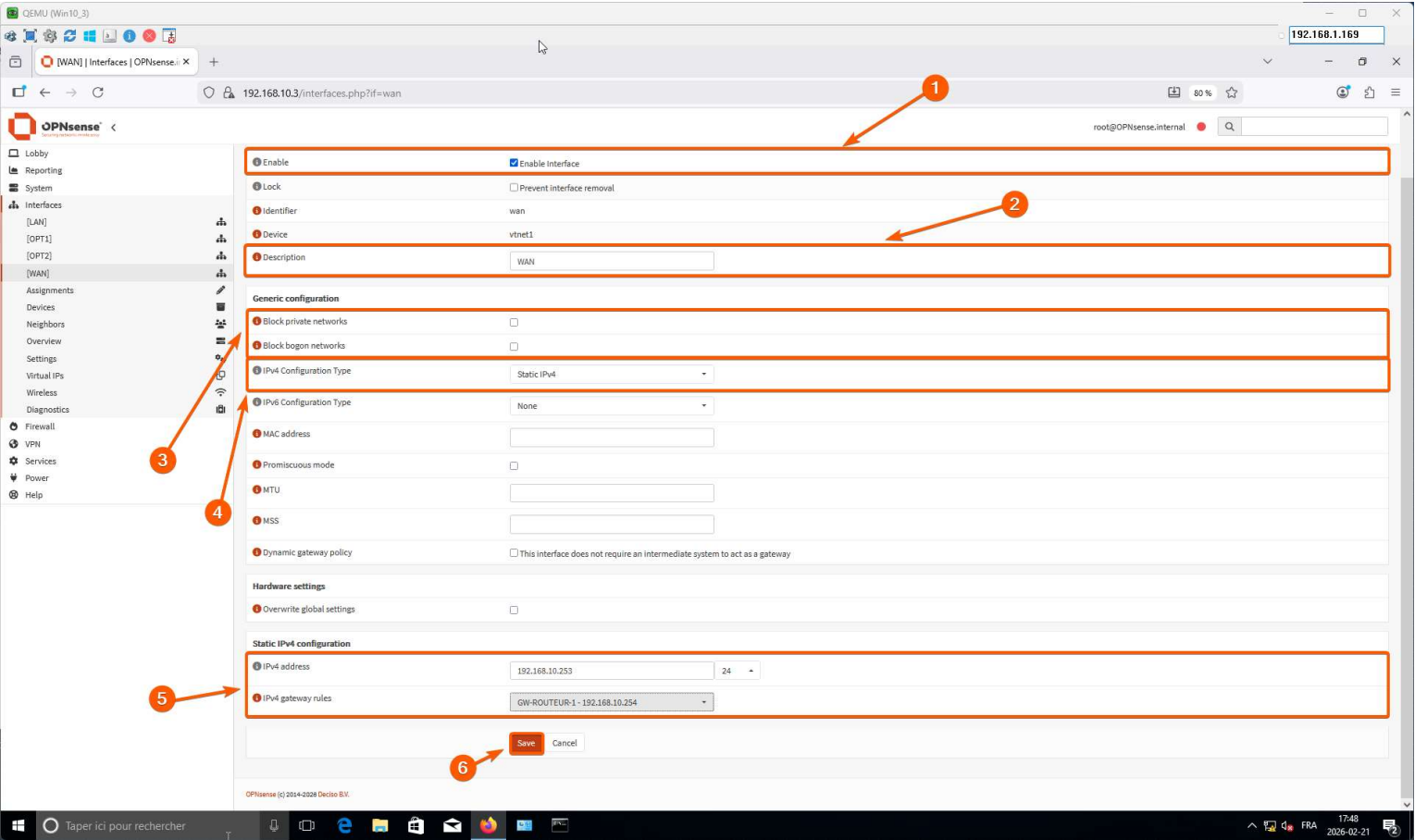
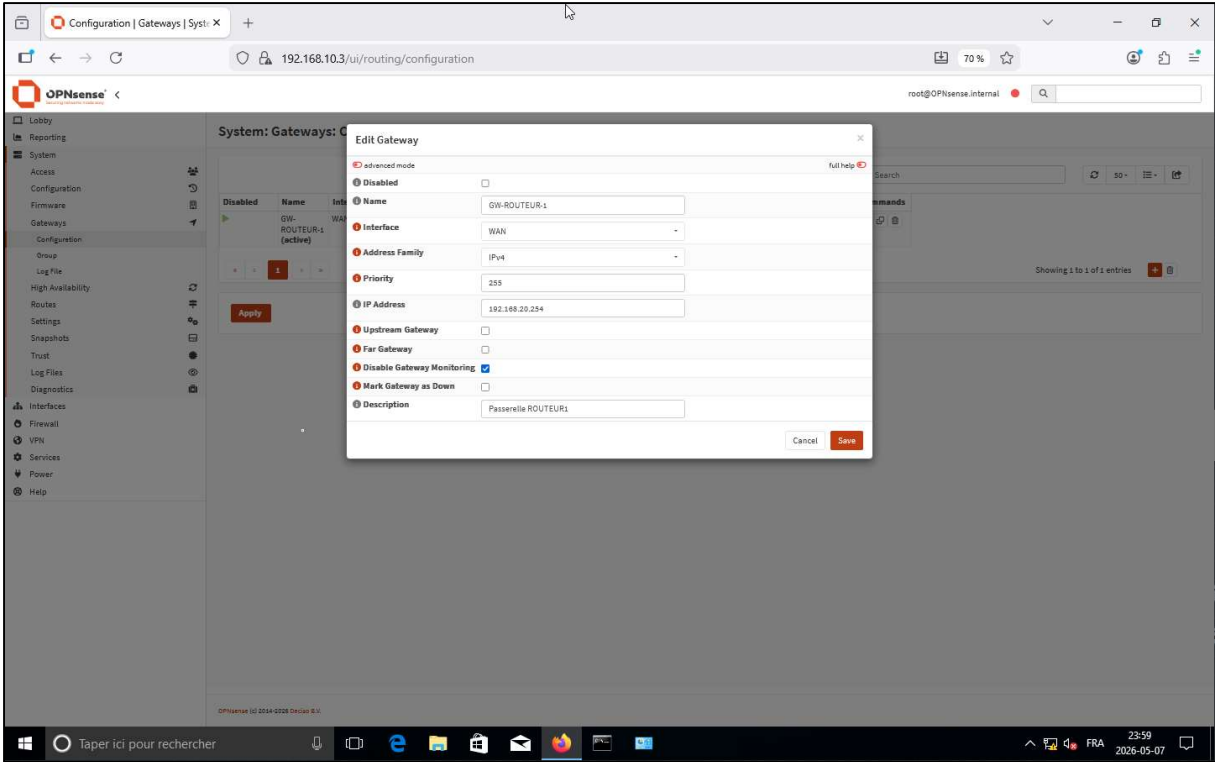
IPv4 Configuration Type : Static IPv4

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** !

The screenshot shows the OPNsense Firewall Rules configuration page for the LAN interface. The page is titled "Firewall: Rules: LAN" and "Edit Firewall rule". The configuration is as follows:

- Action:** Pass
- Disabled:** ☐ Disable this rule
- Quick:** ☒ Apply the action immediately on match.
- Interface:** LAN
- Direction:** In
- TCP/IP Version:** IPv4
- Protocol:** TCP
- Source / Invert:** ☐ Use this option to invert the sense of the match.
- Source:** any
- 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: 80, To: 443
- Log:** ☐ Log packets that are handled by this rule
- Category:**
- Description:** Autoriser l'accès au serveur
- No XSLRPC Sync:** ☐
- Schedule:** none
- Gateway:** default
- Traffic shaping:** rule direction: None, reverse direction: None
- Advanced features:** Show/Hide
- Rule Information:** Created: 2/11/24 20:53:22 (root@192.168.10.2), Updated: 2/11/24 20:53:56 (root@192.168.10.2)
- Buttons:** Save, Cancel

Red arrows and numbers 1 through 5 highlight specific elements: 1 points to the "Edit Firewall rule" title, 2 points to the "Action" field, 3 points to the "Destination" field, 4 points to the "Destination port range" field, and 5 points to the "Save" button.

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** !

The screenshot shows the OPNsense Firewall Rules configuration page for the LAN interface. The rule is named 'LAN' and is configured with the following settings:

- Action:** Pass
- Disabled:** unchecked
- Quick:** checked (Apply the action immediately on match)
- Interface:** LAN
- Direction:** In
- TCP/IP Version:** IPv4
- Protocol:** any
- Source:** LAN net
- Destination:** LAN net
- Destination port range:** from: any, to: any
- Log:** unchecked (Log packets that are handled by this rule)
- Category:** (empty)
- Description:** Autoriser le trafic interne LAN
- No XSNRPC Sync:** unchecked
- Schedule:** none
- Gateway:** default
- Traffic shaping:** rule direction, reverse direction: None

The 'Save' button is highlighted with a red circle and arrow, indicating the next step in the configuration process.

Troisième règle qui va bloquer par défaut le LAN

Aller dans
Firewall → Rules → LAN

Ajouter une règle BLOCK

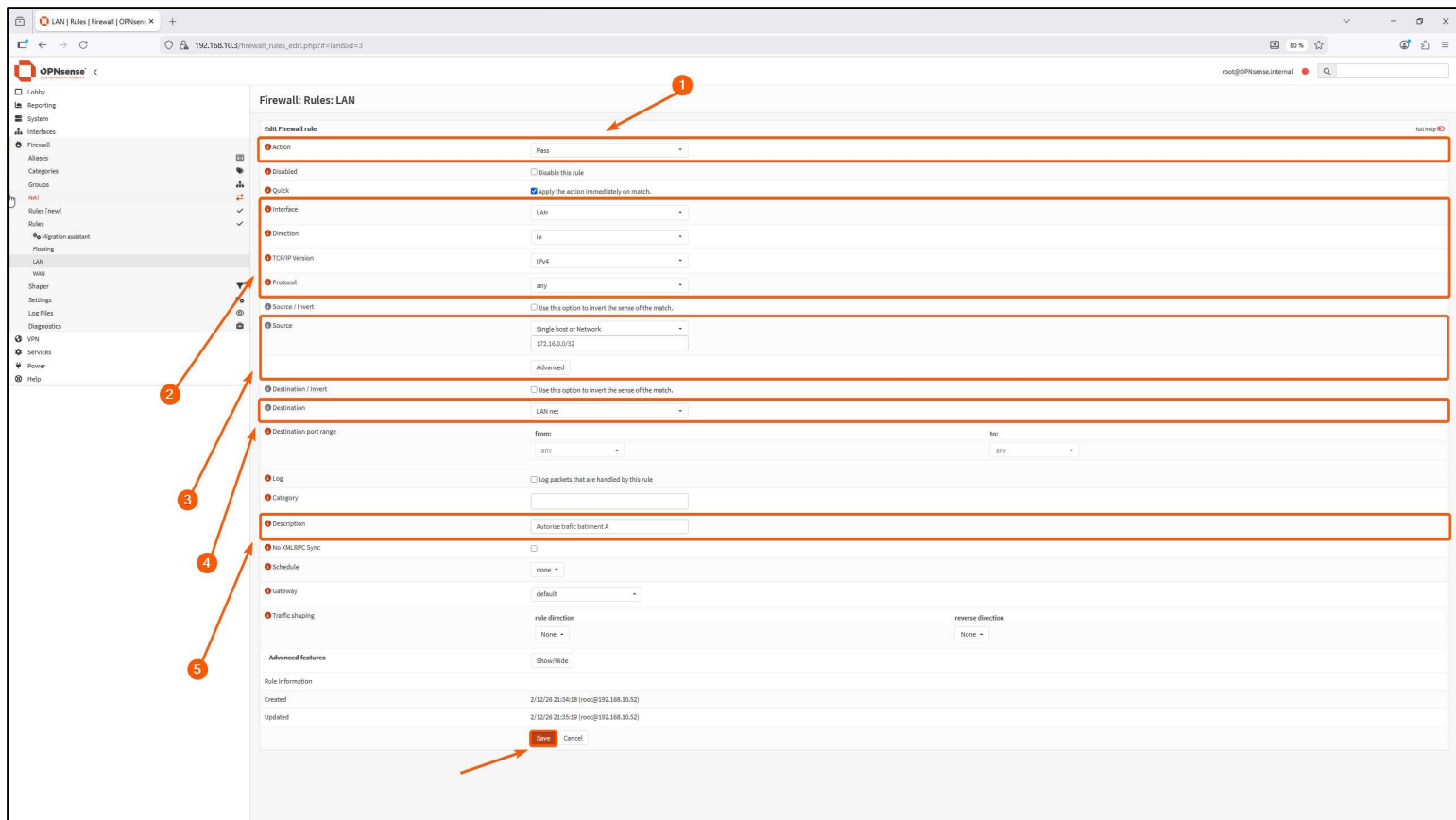
En haut → cliquer sur + Add

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 | OPNsense

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'accès au serveur
☐	IPv4 *	LAN net	*	LAN net	*	*	*	Autorise le trafic interne LAN
☐	IPv4 *	LAN net	*	*	*	*	*	Blocage par défaut LAN
☒	pass	pass (disabled)	X	block	reject	log	in	first match
☒	pass (disabled)	X	block (disabled)	reject (disabled)	log (disabled)	out	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.

OPNsense (c) 2014-2024 Deciso B.V.

LAN | Rules | Firewall | OPNsense

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'accès au serveur
☐	IPv4 *	LAN net	*	LAN net	*	*	*	Autorise le trafic interne LAN
☐	IPv4 *	LAN net	*	*	*	*	*	Blocage par défaut LAN
☒	pass	pass (disabled)	X	block	reject	log	in	first match
☒	pass (disabled)	X	block (disabled)	reject (disabled)	log (disabled)	out	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.

OPNsense (c) 2014-2024 Deciso B.V.



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** !

QEMU (Win10_3)

LAN | Rules | Firewall | OPNsense: X

192.168.10.3/firewall_rules_edit.php?if=lan

Importez les marqueurs...

OPNsense

root@OPNsense.internal

Firewall: Rules: LAN

Edit Firewall rule

1 Action: Pass

2 Disabled: ☐ Disable this rule

3 Quick: ☒ Apply the action immediately on match.

4 Interface: LAN

5 Direction: In

TCP/IP Version: IPv4

Protocol: ICMP

ICMP type: Any

Source / Invert: ☐ Use this option to invert the sense of the match.

6 Source: Single host or Network
172.16.5.1

Advanced

Destination / Invert: ☐ Use this option to invert the sense of the match.

7 Destination: Single host or Network
192.168.10.1

Destination port range: from: any to: any

Log: ☐ Log packets that are handled by this rule

Category:

8 Description: Autoriser les ping venant du VLAN 3 vers le serveur

No XMLRPC Sync: ☐

Schedule: none

OPNsense (c) 2014-2018 Deciso E.V.

Courrier

Windows taskbar: Taper ici pour rechercher, 14:45, 2026-02-17



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

Aller dans :
Firewall → Rules → WAN

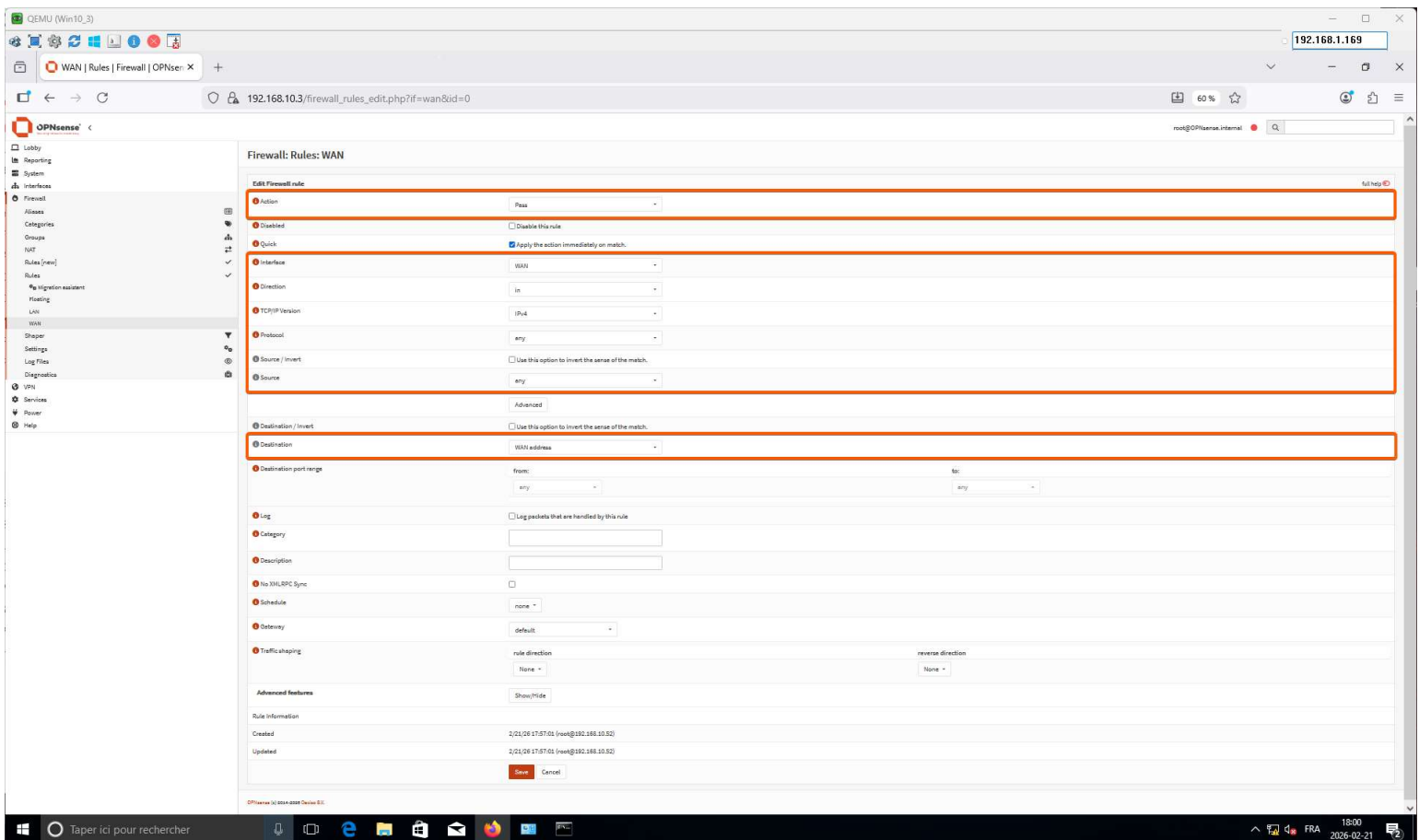
Ajouter une règle PASS

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** !



5^{ème} 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**. 

Services: Dnsmasq DNS & DHCP

General Domains Hosts DHCP ranges DHCP options DHCP boot DHCP tags

advanced mode

full help

Default

Enable ☒

Interface LAN, VLAN2, VLAN3

DNS

Listen port 53053

DNSSEC ☐

No hosts lookup ☐

DNS Query Forwarding

Query DNS servers sequentially ☐

Require domain ☐

Do not forward to system defined DNS servers ☐

Do not forward private reverse lookups ☐

DHCP

DHCP FQDN ☒

DHCP default domain internal

DHCP local domain ☒

DHCP authoritative ☒

DHCP reply delay

DHCP register firewall rules ☒

Router advertisements ☒

Disable HA sync ☐

ISC / KEA DHCP (legacy)

Register ISC DHCPv4 leases ☐

DHCP domain override

Register DHCP static mappings ☐

Prefer DHCP ☐

Apply

Activer Windows
Accédez aux paramètres pour activer Windows.

Etape 2 : Définir la plage DHCP pour VLAN2

Aller dans :

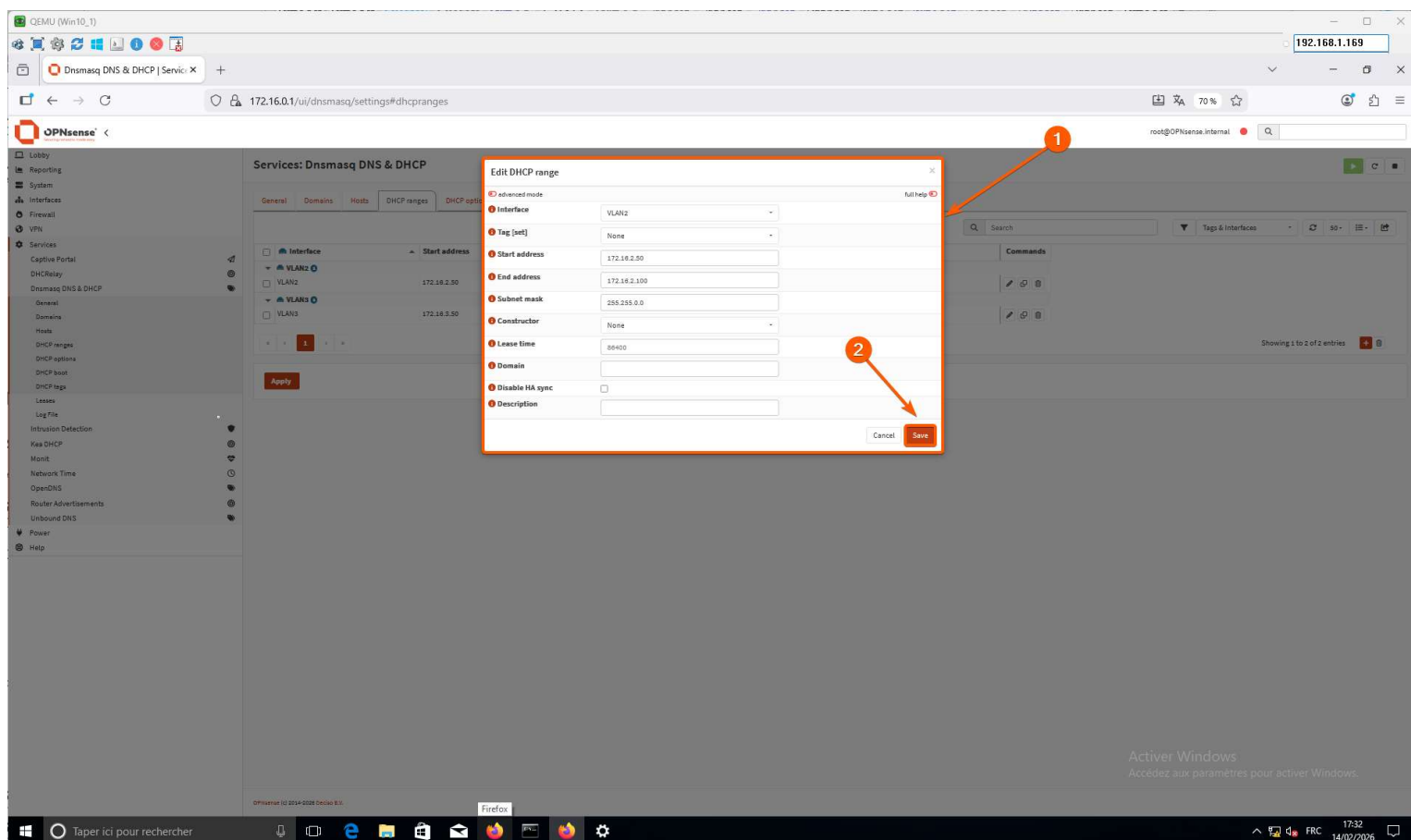
Services → Dnsmasq DNS & DHCP → DHCP ranges

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 :

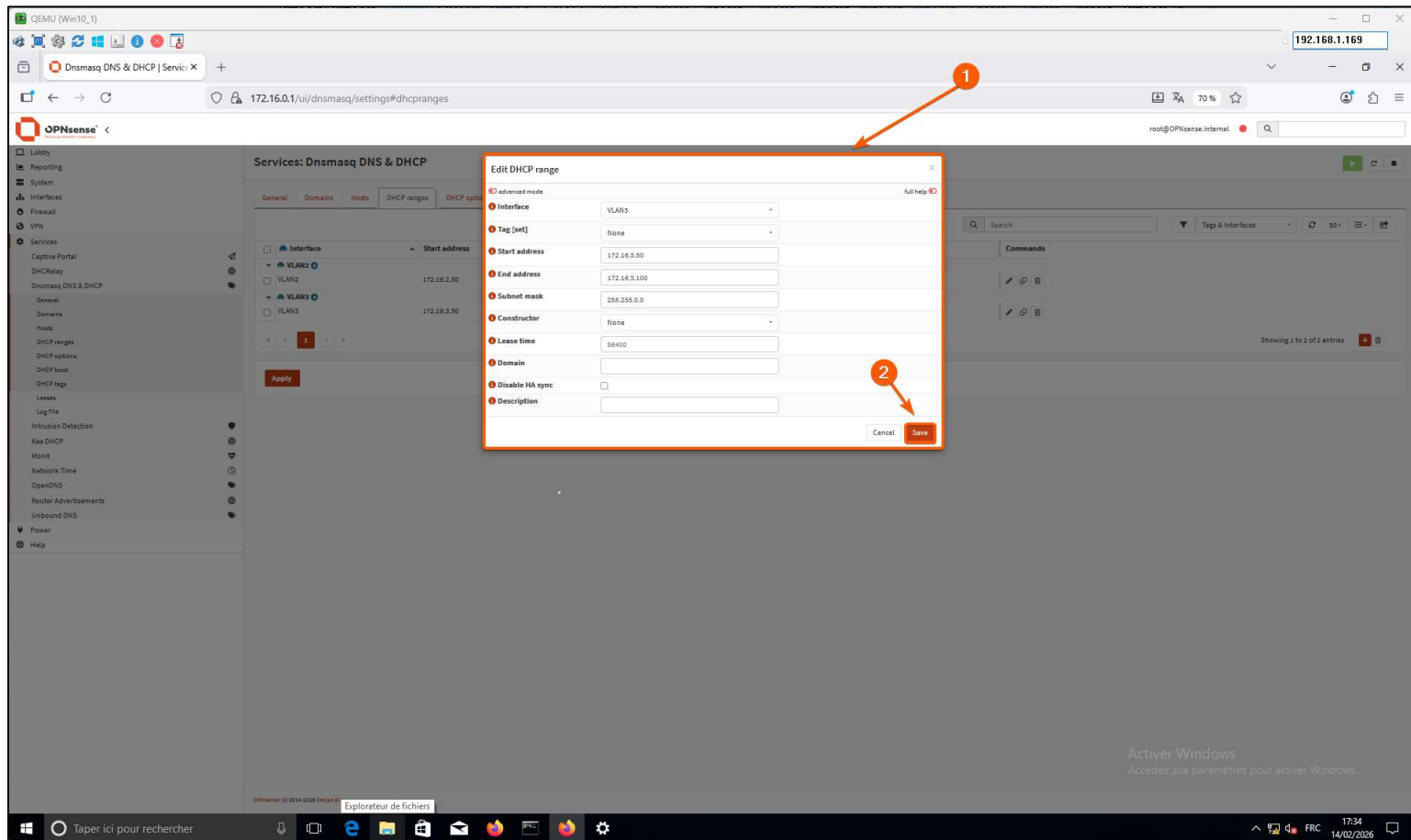
Services → Dnsmasq DNS & DHCP → DHCP ranges

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.

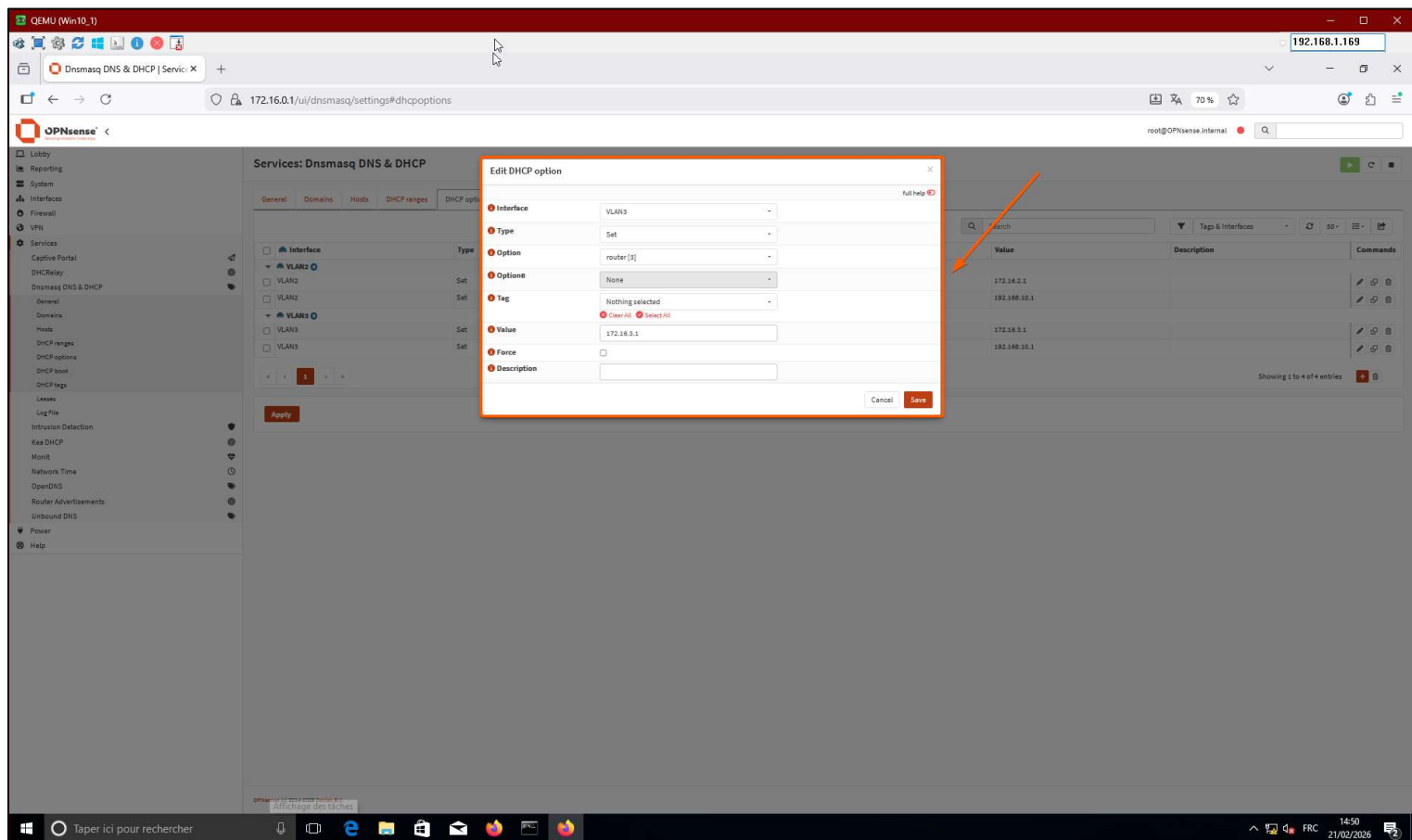
Pour VLAN2 :

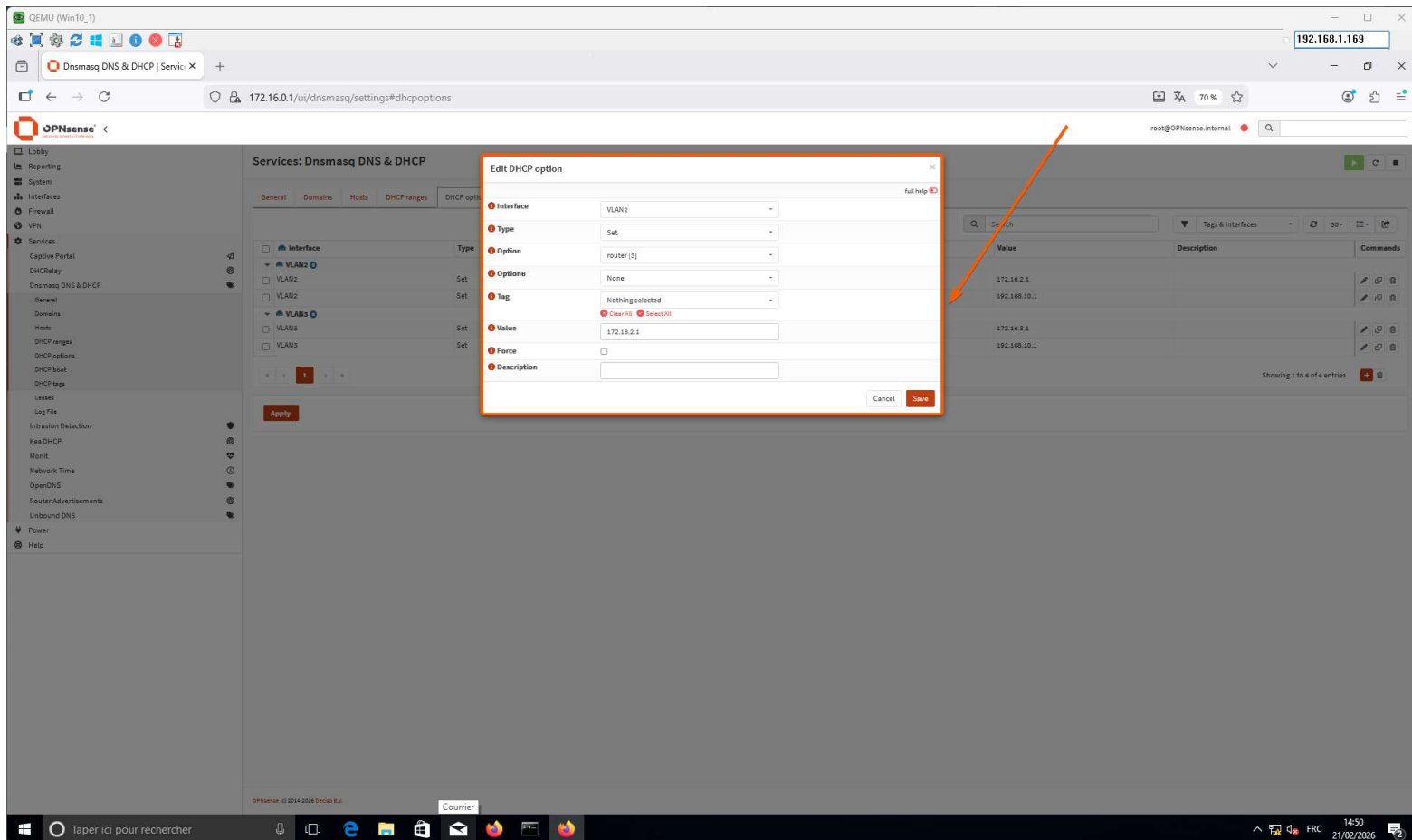
- **Interface** : VLAN2
- **Type** : Set
- **Option** : router [3]
- **Value** : 172.16.2.1

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



Pour le VLAN2 :

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

Pour le VLAN3 :

Aller dans :

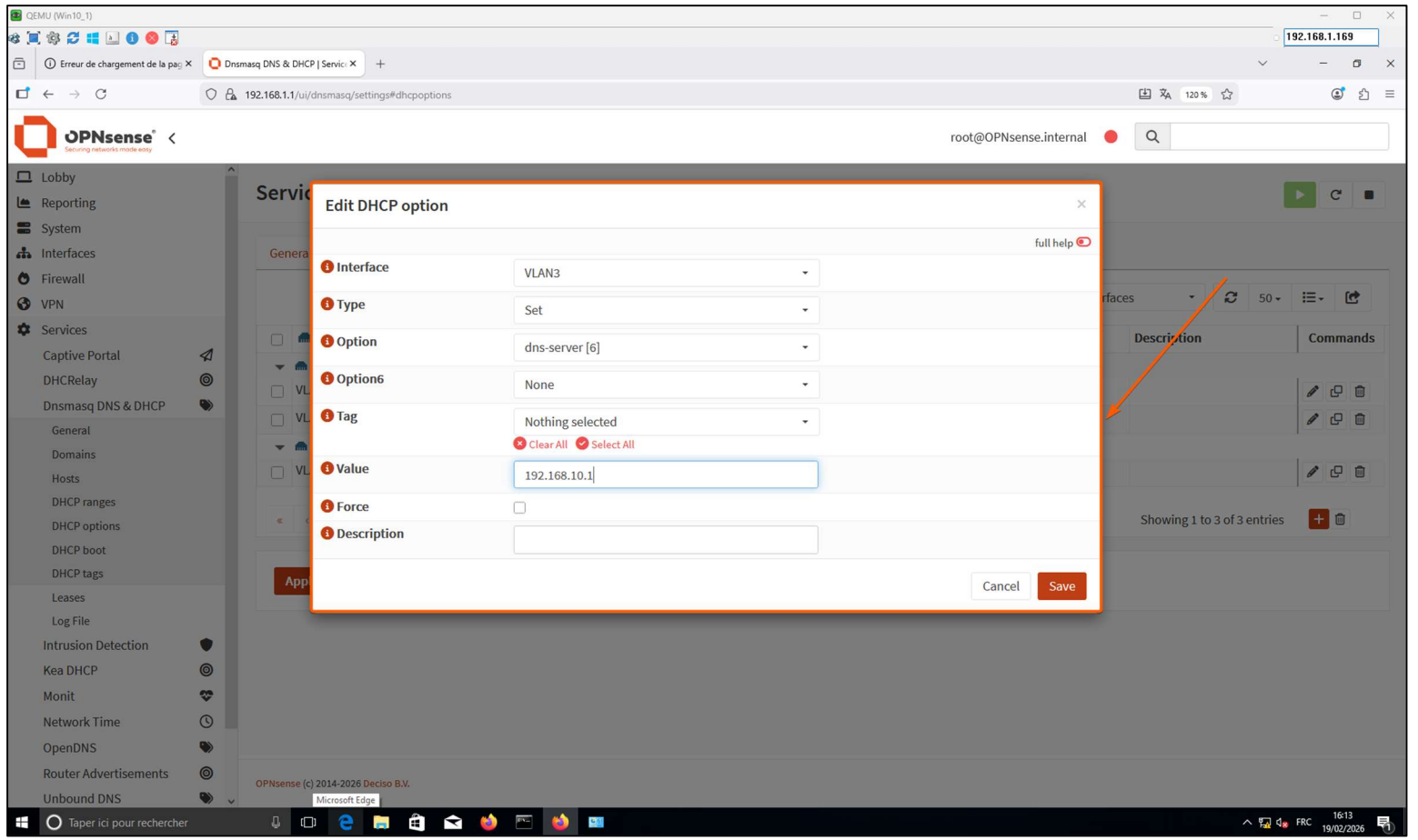
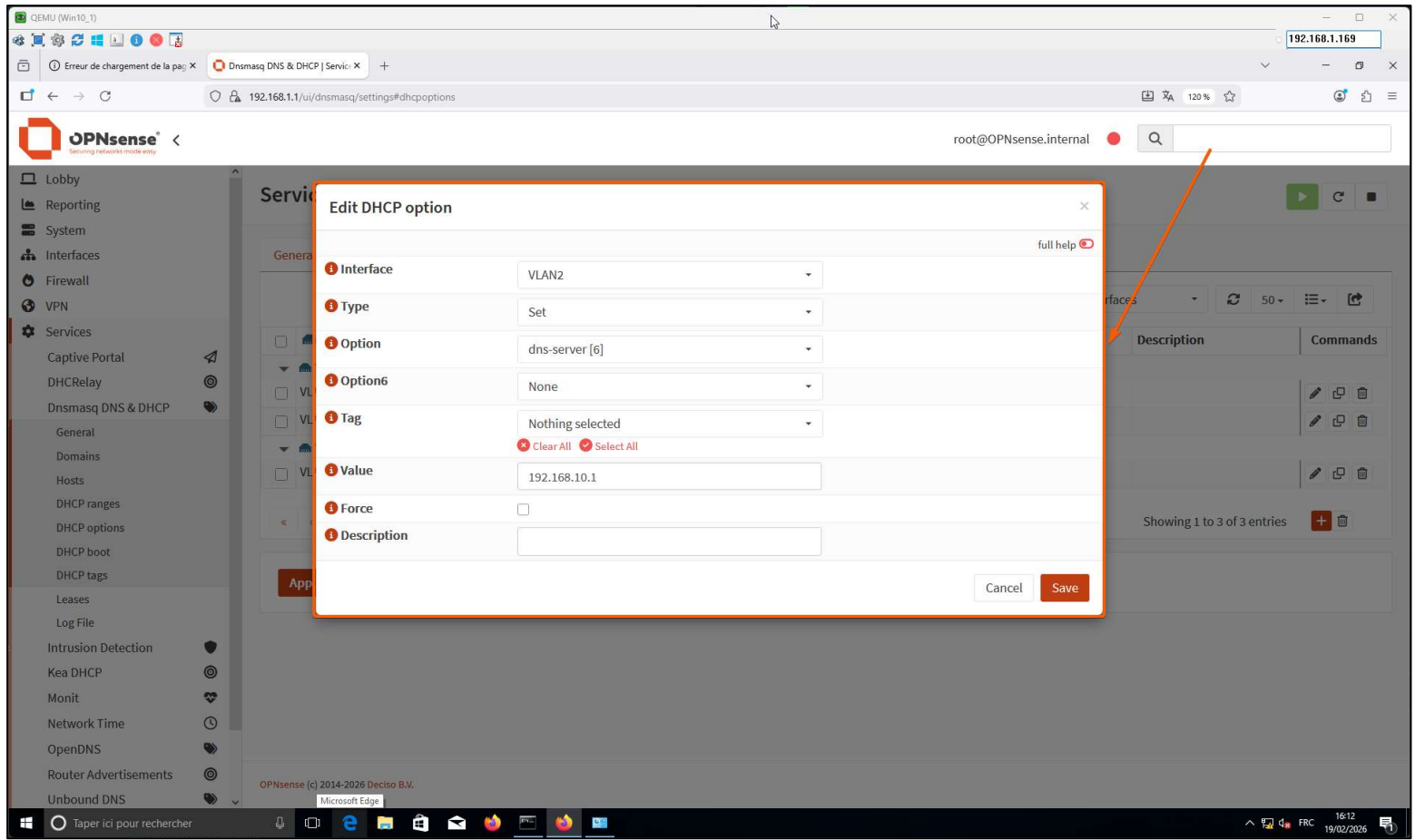
Services → Dnsmasq DNS & DHCP → DHCP options

Cliquer sur **+ Add**.

Configurer :

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

Description : DNS Server pour le vlan 3



Services: Dnsmasq DNS & DHCP

General Domains Hosts **DHCP ranges** DHCP options DHCP boot DHCP tags

Search Tags & Interfaces 50

Interface	Type	Option	Option6	Value	Description	Commands
VLAN2						
VLAN2	Set	router [3]		172.16.0.254		
VLAN2	Set	dns-server [6]		192.168.10.1		
VLAN3						
VLAN3	Set	router [3]		172.16.0.254		
VLAN3	Set	dns-server [6]		192.168.10.1		

Showing 1 to 4 of 4 entries

Apply

OPNsense (c) 2014-2026 Deciso B.V.



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

```
Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.

C:\Users\bretont>ipconfig /release

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

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

Configuration IP de Windows

Nom de l'hôte . . . . . : DESKTOP-004LQUQ
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 . . . . . : 50-00-00-00-00-00
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . : fe80::a096:ca1f:9f58:4116%11(préfééré)
    Adresse IPv4. . . . . : 172.16.3.58(préfééré)
    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-80-08-50-00-00-00-00-00-00
    Serveurs DNS. . . . . : 192.168.10.1
    NetBIOS sur Tcpip. . . . . : Activé

C:\Users\bretont>
```




BILAN DE CONFIGURATION DES CARTE RESEAU

Carte réseau : Win_10_1 :

Détails de connexion réseau

Détails de connexion réseau :

Propriété	Valeur
Suffixe DNS propre à la ...	internal
Description	Intel(R) PRO/1000 MT Network Connecti
Adresse physique	50-00-00-01-00-00
DHCP activé	Oui
Adresse IPv4	172.16.2.85
Masque de sous-réseau ...	255.255.255.0
Bail obtenu	samedi 21 février 2026 18:07:31
Bail expirant	dimanche 22 février 2026 18:07:31
Passerelle par défaut IPv4	172.16.2.1
Serveur DHCP IPv4	172.16.2.1
Serveur DNS IPv4	192.168.10.1
Serveur WINS IPv4	
NetBIOS sur TCP/IP act...	Oui
Adresse IPv6 locale de li...	fe80::6477:b172:dcf4:61c9%5
Passerelle par défaut IPv6	
Serveur DNS IPv6	

Fermer

Carte réseau : Win_10_2 :

Détails de connexion réseau

Détails de connexion réseau :

Propriété	Valeur
Suffixe DNS propre à la ...	internal
Description	Intel(R) PRO/1000 MT Network Connecti
Adresse physique	50-00-00-06-00-00
DHCP activé	Oui
Adresse IPv4	172.16.3.58
Masque de sous-réseau ...	255.255.255.0
Bail obtenu	samedi 21 février 2026 15:40:01
Bail expirant	dimanche 22 février 2026 15:40:02
Passerelle par défaut IPv4	172.16.3.1
Serveur DHCP IPv4	172.16.3.1
Serveur DNS IPv4	192.168.10.1
Serveur WINS IPv4	
NetBIOS sur TCP/IP act...	Oui
Adresse IPv6 locale de li...	fe80::a096:ca1f:9f58:4116%11
Passerelle par défaut IPv6	
Serveur DNS IPv6	

Fermer

Carte réseau : Win_10_3 :

Détails de connexion réseau

Détails de connexion réseau :

Propriété	Valeur
Suffixe DNS propre à la ...	internal
Description	Intel(R) PRO/1000 MT Network Connecti
Adresse physique	50-00-00-09-00-00
DHCP activé	Oui
Adresse IPv4	192.168.10.52
Masque de sous-réseau ...	255.255.255.0
Bail obtenu	21 février 2026 17:00:39
Bail expirant	22 février 2026 17:00:39
Passerelle par défaut IPv4	192.168.10.254
Serveur DHCP IPv4	192.168.10.3
Serveur DNS IPv4	192.168.10.1
Serveur WINS IPv4	
NetBIOS sur TCP/IP act...	Oui
Adresse IPv6 locale de li...	fe80::c79:8f58:7c3d:6bb9%11
Passerelle par défaut IPv6	
Serveur DNS IPv6	

Fermer

Carte réseau : WinServer :

Détails de connexion réseau

Détails de connexion réseau :

Propriété	Valeur
Suffixe DNS propre à la ...	
Description	Intel(R) PRO/1000 MT Network Connecti
Adresse physique	50-00-00-0B-00-00
DHCP activé	Non
Adresse IPv4	192.168.10.1
Masque de sous-réseau ...	255.255.255.0
Passerelle par défaut IPv4	192.168.10.254
Serveur DNS IPv4	192.168.10.1
Serveur WINS IPv4	
NetBIOS sur TCP/IP act...	Oui
Adresse IPv6 locale de li...	fe80::891b:7e75:ef51:105f%5
Passerelle par défaut IPv6	
Serveur DNS IPv6	

Fermer

7^{ème} phase du projet : Administration réseau des équipements :

Etape 1 : Configuration des équipements d'interconnexion :

<u>Configuration des ports de Switch 1 :</u>	<u>Configuration des ports de Switch 2 :</u>
<pre>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</pre>	→ Création d'un vlan pour le service de la Direction <pre>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 !</pre>

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 :