



 **PNsense**[®]
Securing networks made easy

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

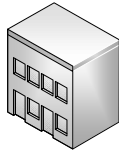
Dans **System → Settings**, configure ces éléments :

- ☞ **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**

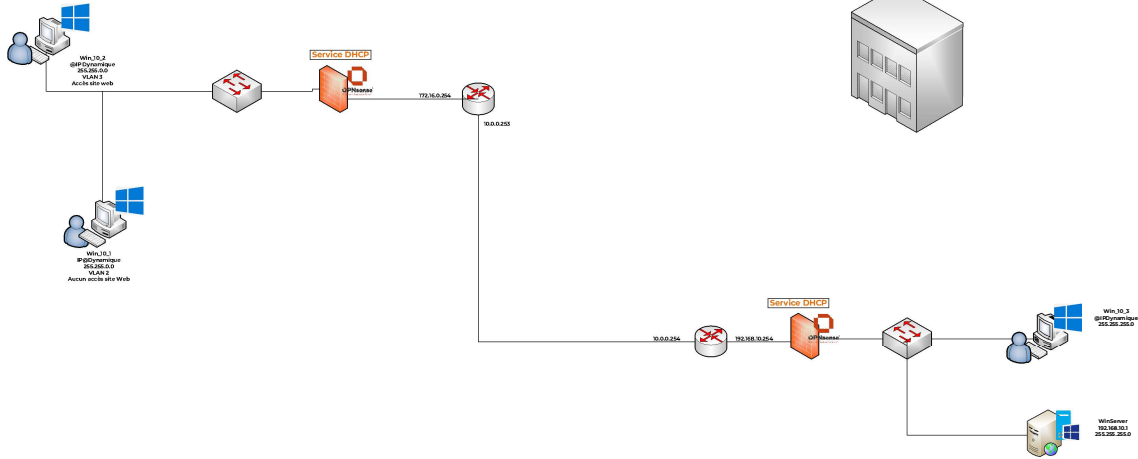
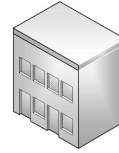
Schéma Réseau - LycéeTech Réseaux :



Bâtiment A : Pôle pédagogique
172.16.0.0 /16



Bâtiment B : Direction
192.168.10.0 /24

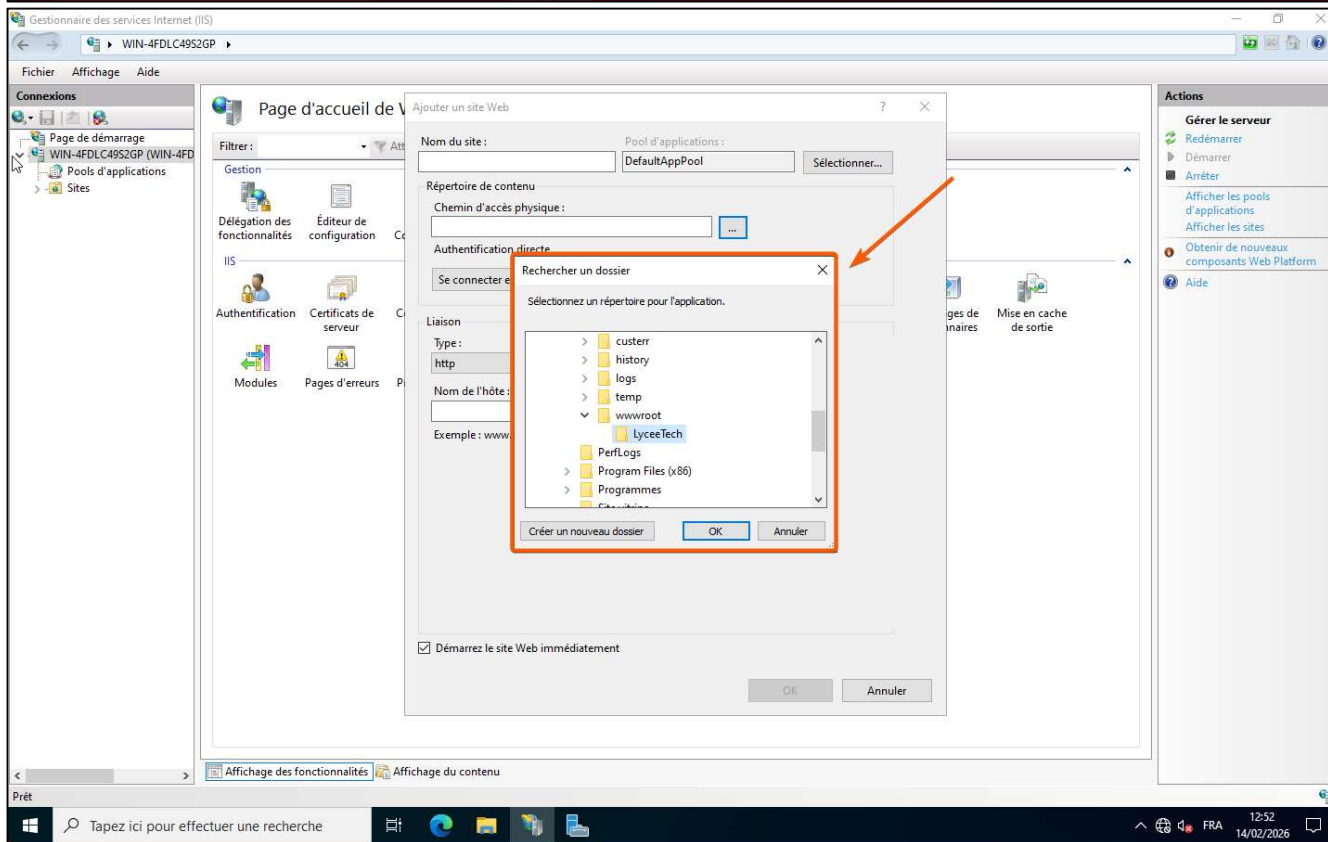
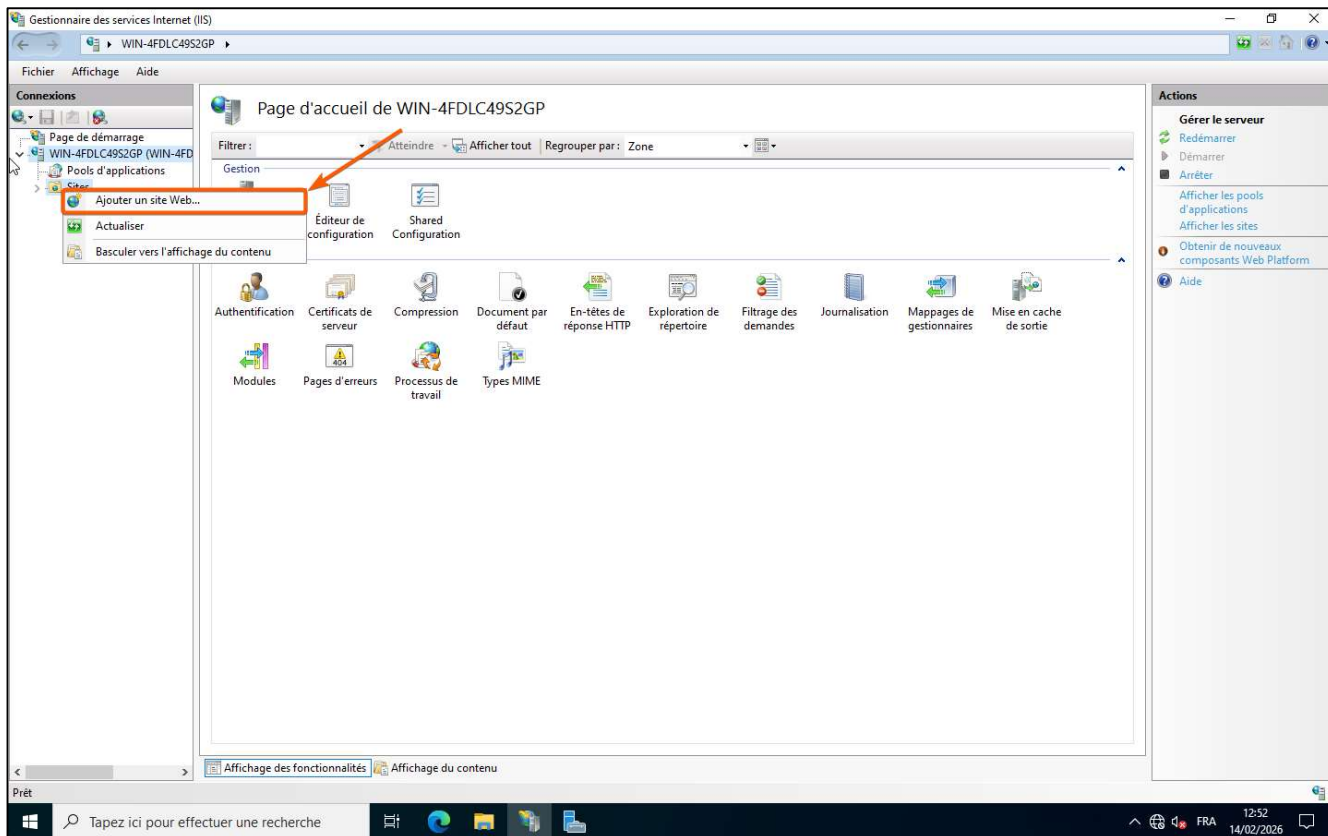


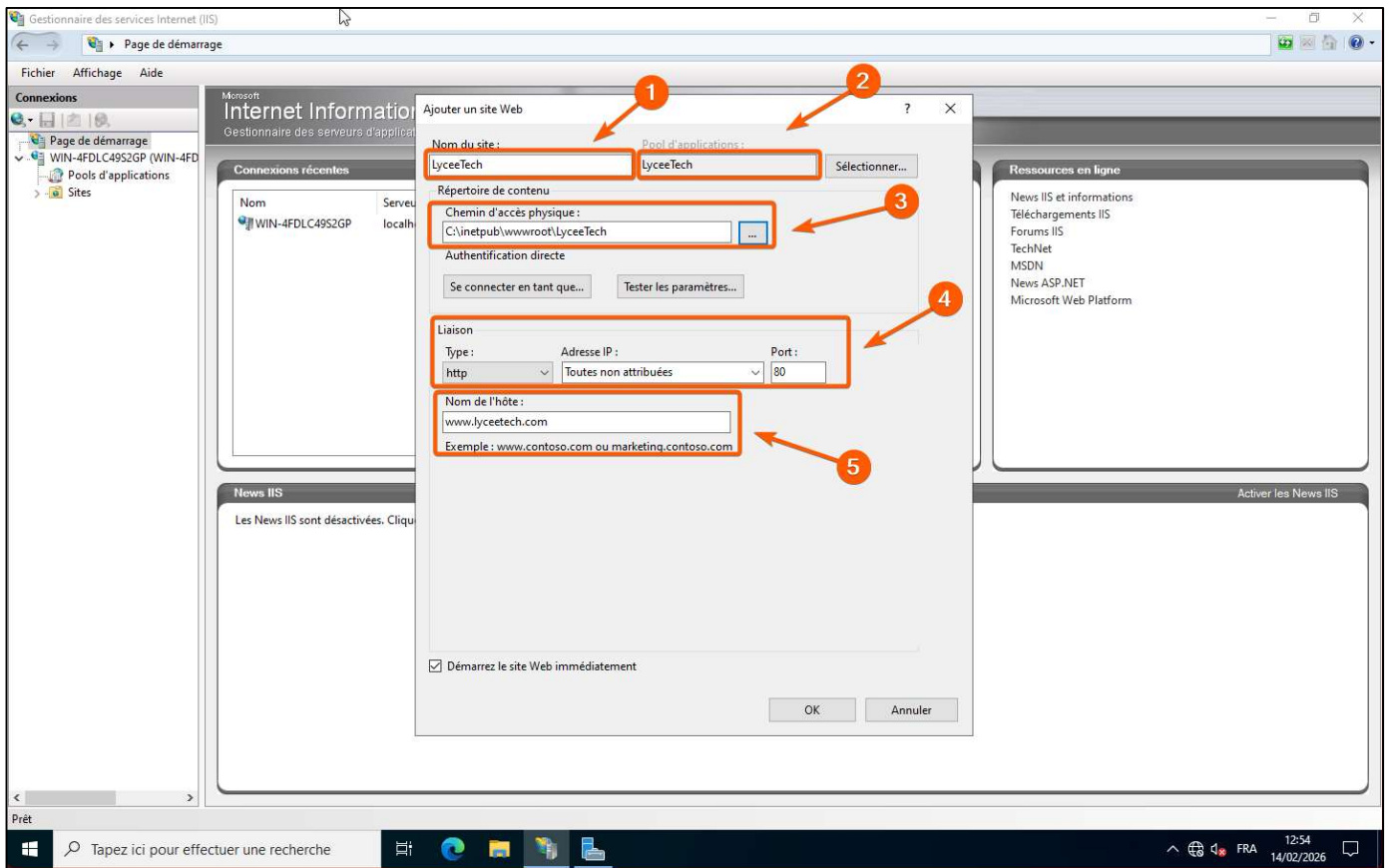
Légende		
Sous-cadre de la légende		
Symbole	Titre	Description
[Server Icon]	1	Serveur web
[PC Icon]	3	PC
[Computer Icon]	2	Ordinateur groupe de travail
[User Icon]	3	Utilisateur
[Router Icon]	2	Routeur
[Building Icon]	2	Bâtiment
[Firewall Icon]	2	Pare-feu
[Switch Icon]	5	Switch 24x24



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

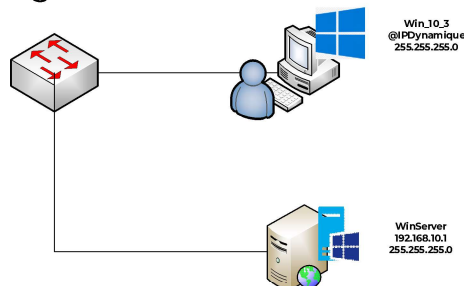
1 Ajouter le rôle WebServer (IIS) et hébergé le site:





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

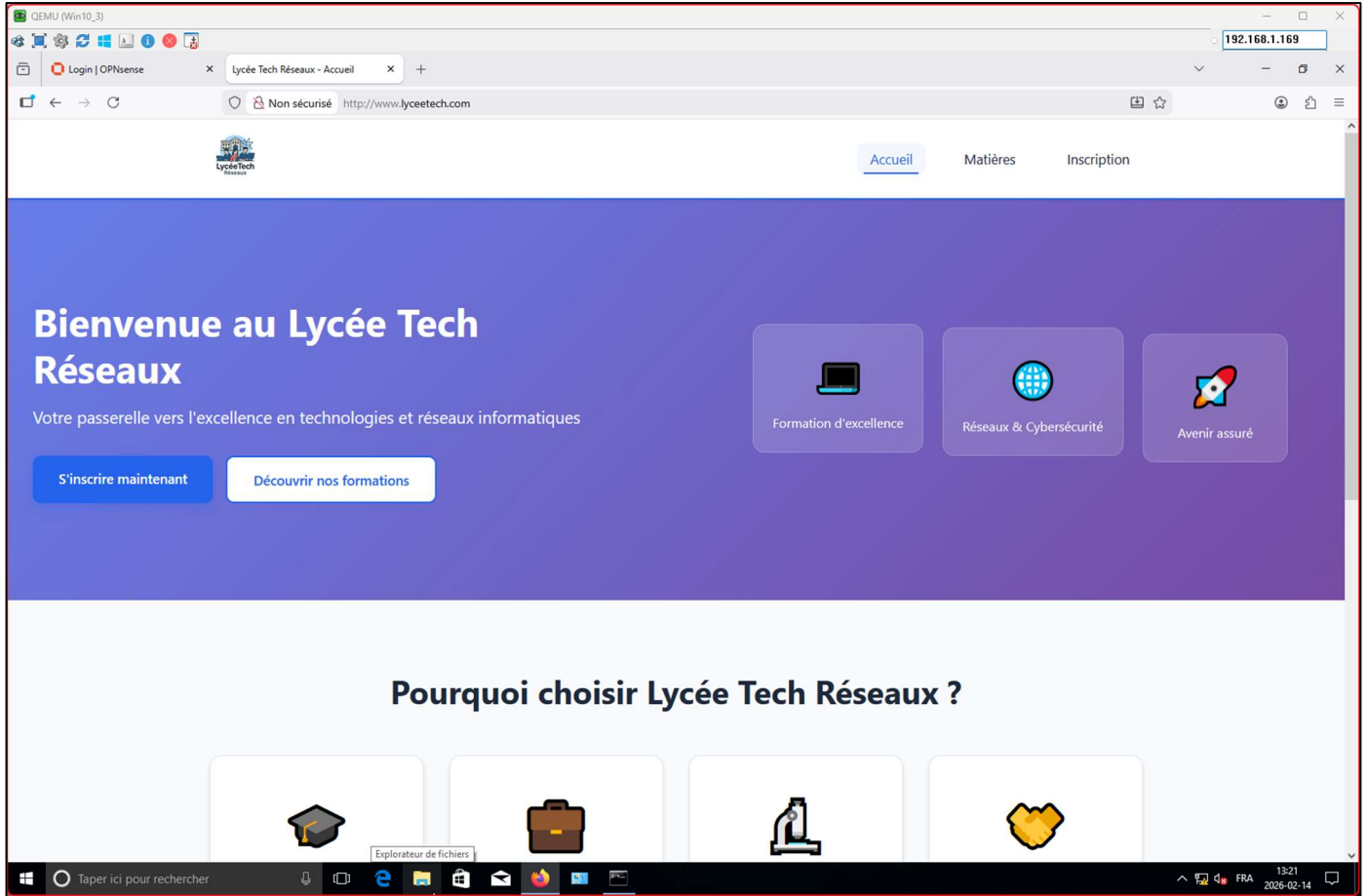
C:\Users\bretont>ping www.lyceetech.com

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

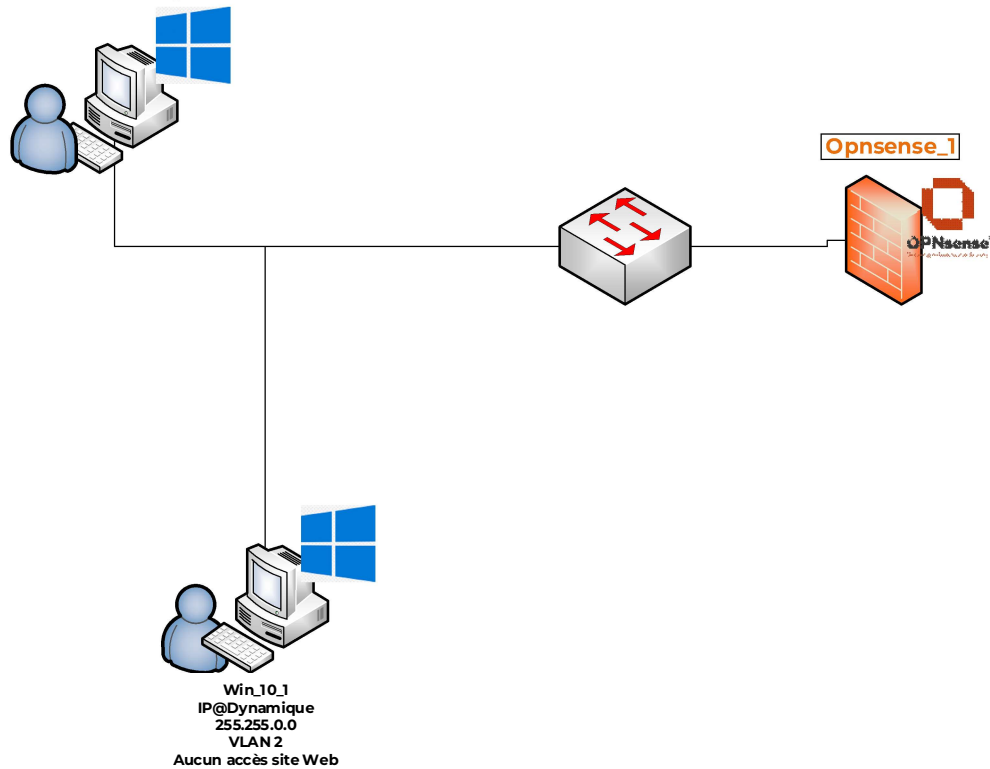
C:\Users\bretont>
  
```

Résultat :



2^{ème} phase du projet : Configuration des deux pare feu :

1 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

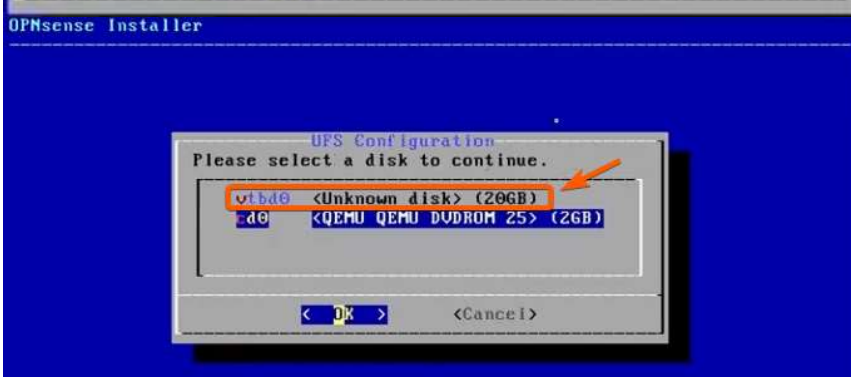
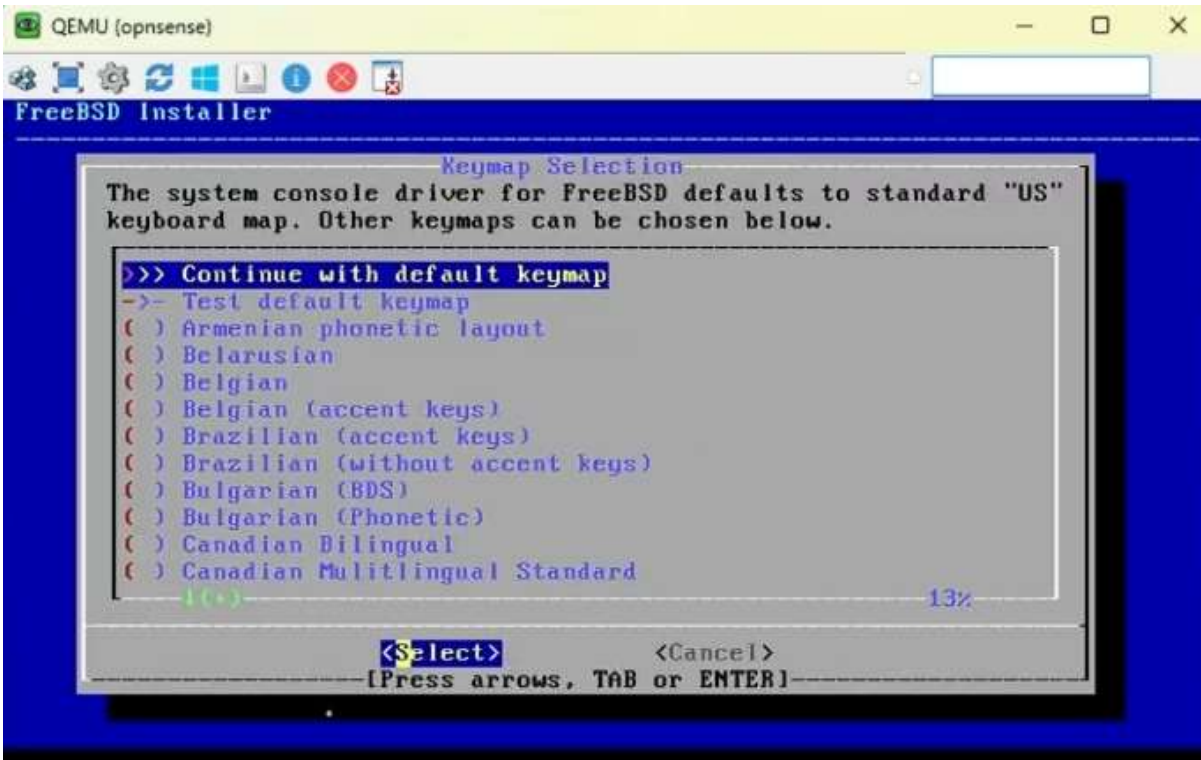
7. Démarrez le nœud et ouvrez la console (vnc)

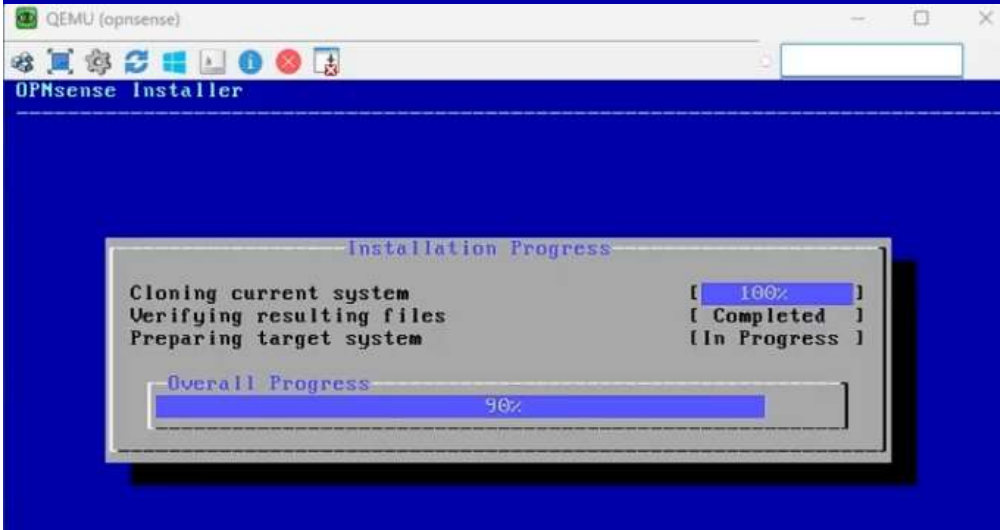
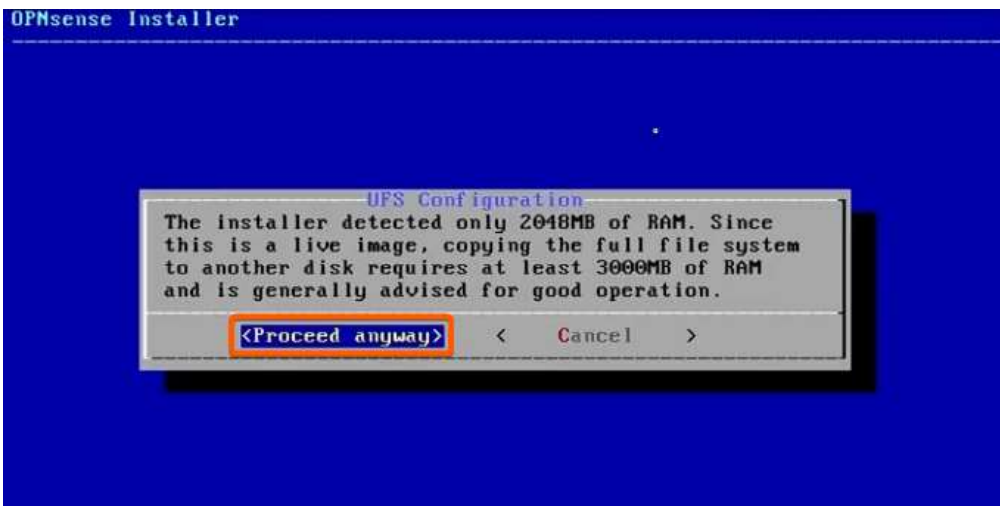
8. Attendez jusqu'à ce que le nœud démarre complètement à partir de l'ISO et utilisez la connexion avec le nom d'utilisateur: mot de passe d'installation: opnsense pour démarrer l'installation OPNsense

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

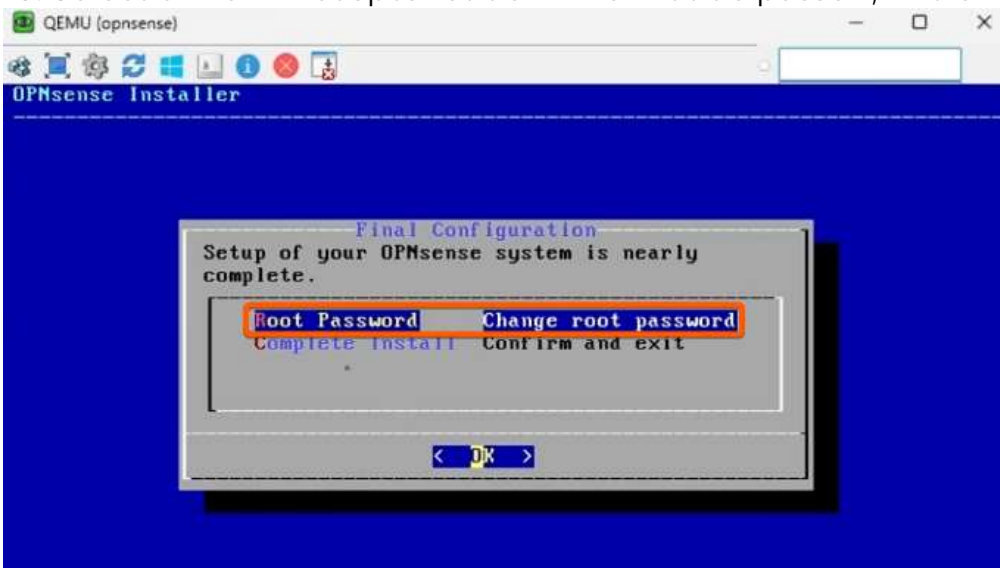
login : installer

mot de passe : opnsense



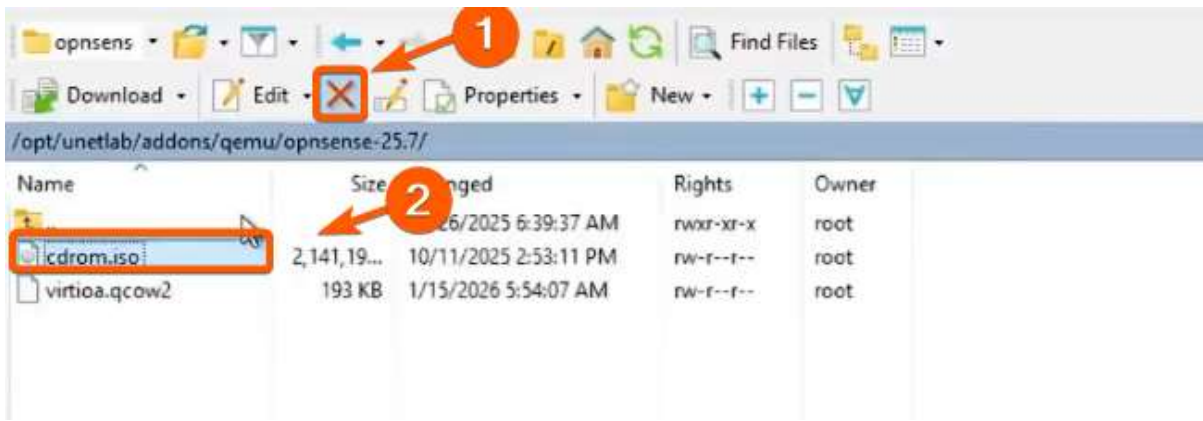


10. Sélectionnez « Accepter et définir le mot de passe », Entrez



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 :

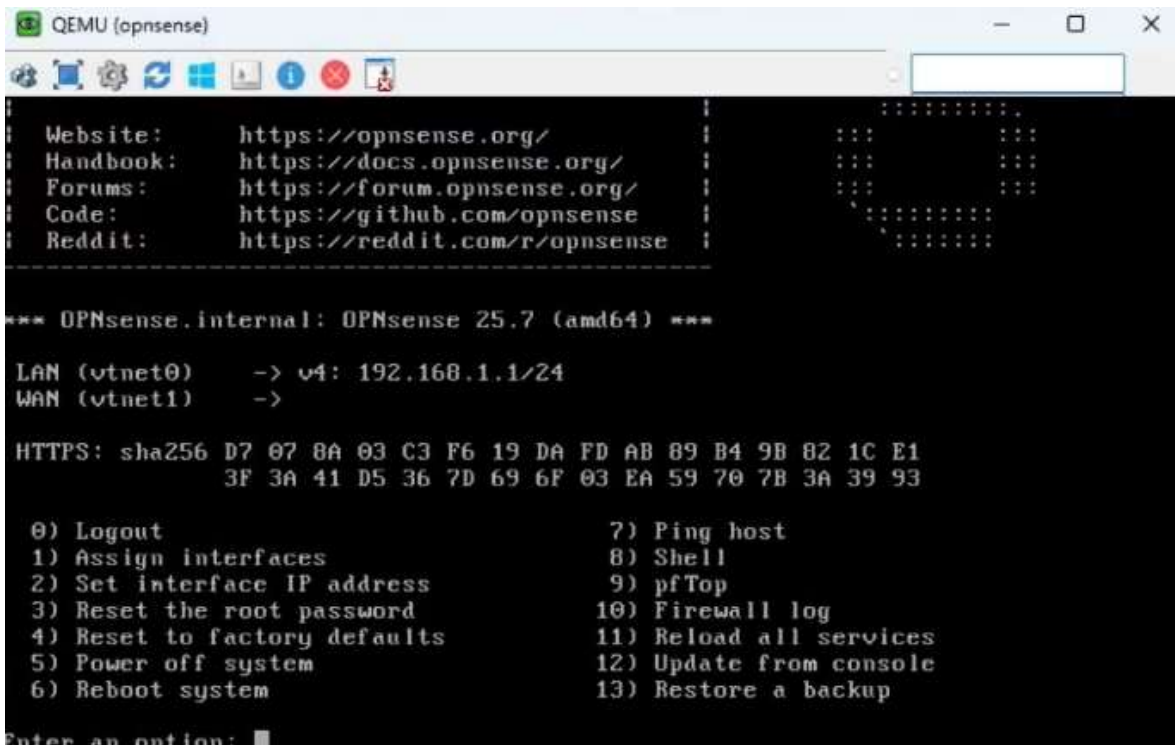
-machine type=pc,accel=kvm -nographic -usbdevice tablet -serial mon:stdio

Aucune option de boot

Pas de -boot order=dc

Pas de -cdrom

Pas de -hdb



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

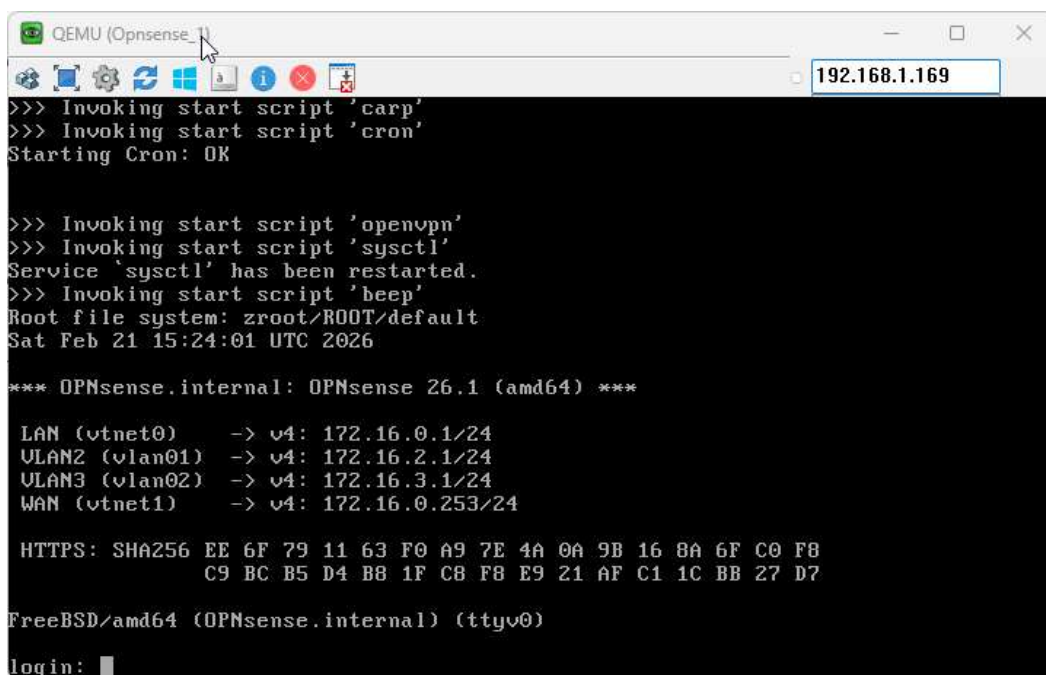
Gateway : laisser vide

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

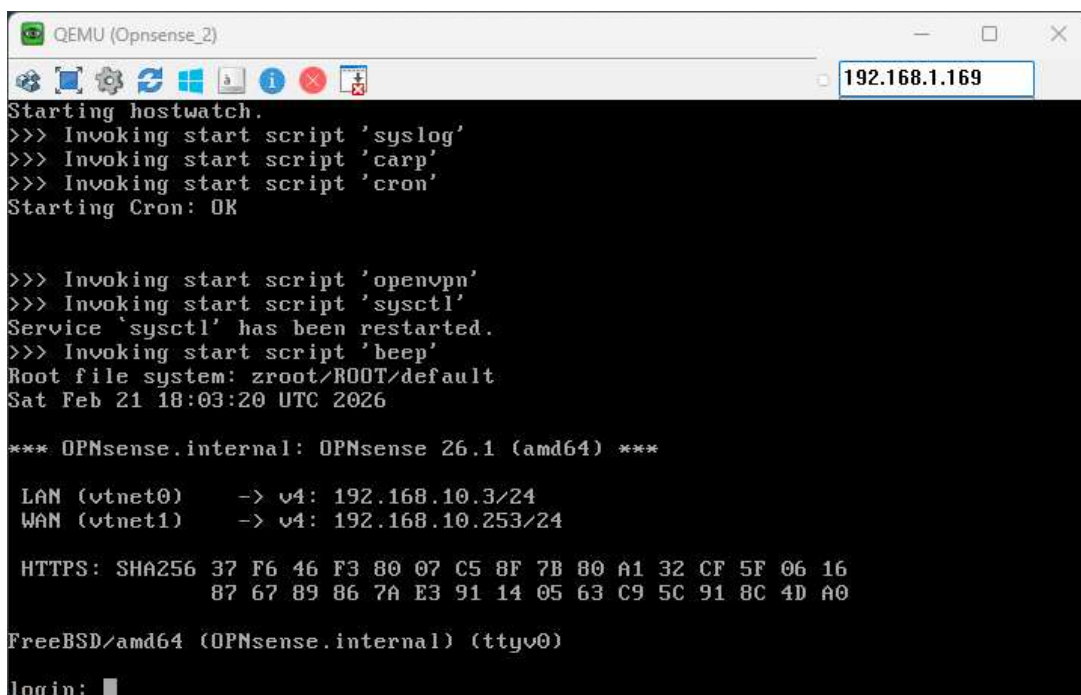
>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: zroot/ROOT/default
Sat Feb 21 15:24:01 UTC 2026

*** 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 BB 1F CB 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

The screenshot shows the OPNsense web interface for configuring VLANs. The left sidebar has 'Interfaces' (1) and 'VLAN' (3) highlighted. The main content area shows a table with two entries:

Device	Parent	VLAN tag	VLAN priority	Description	Commands
<input type="checkbox"/> vlan01 [VLAN2]	vtnet0 (50:00:00:02:00:00) [LAN]	2	Best Effort (0, default)	VLAN 2	
<input type="checkbox"/> vlan02 [VLAN3]	vtnet0 (50:00:00:02:00:00) [LAN]	3	Best Effort (0, default)	VLAN 3	

Below the table is an 'Apply' button. The interface also shows a search bar and pagination controls.

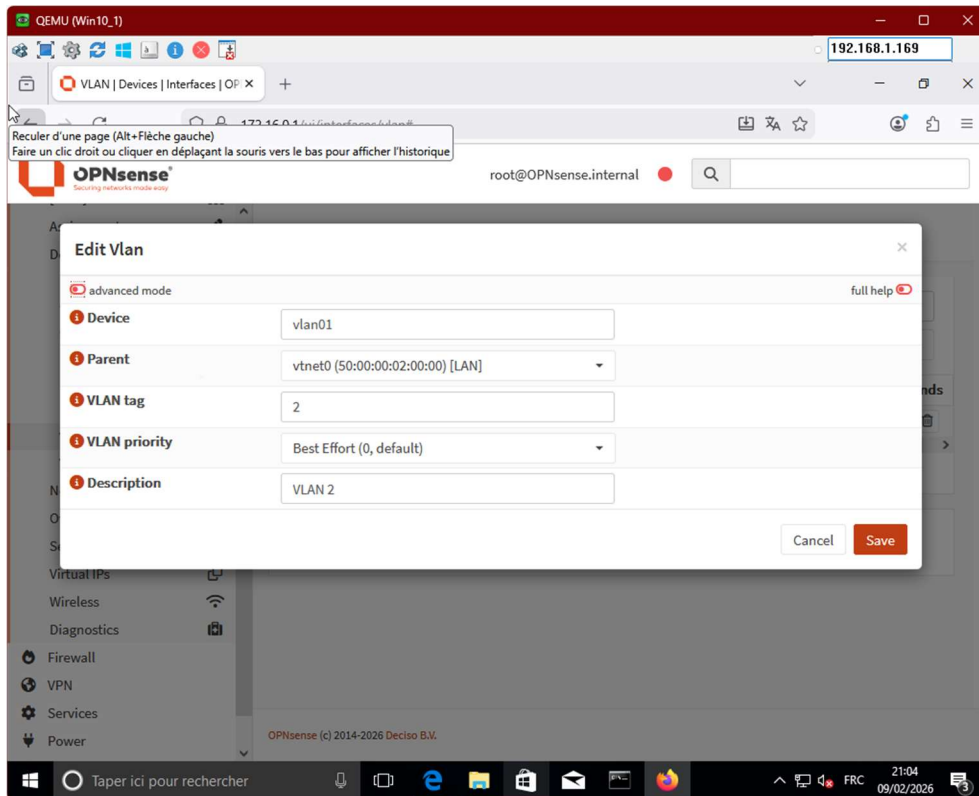
2. Créer un VLAN

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**.

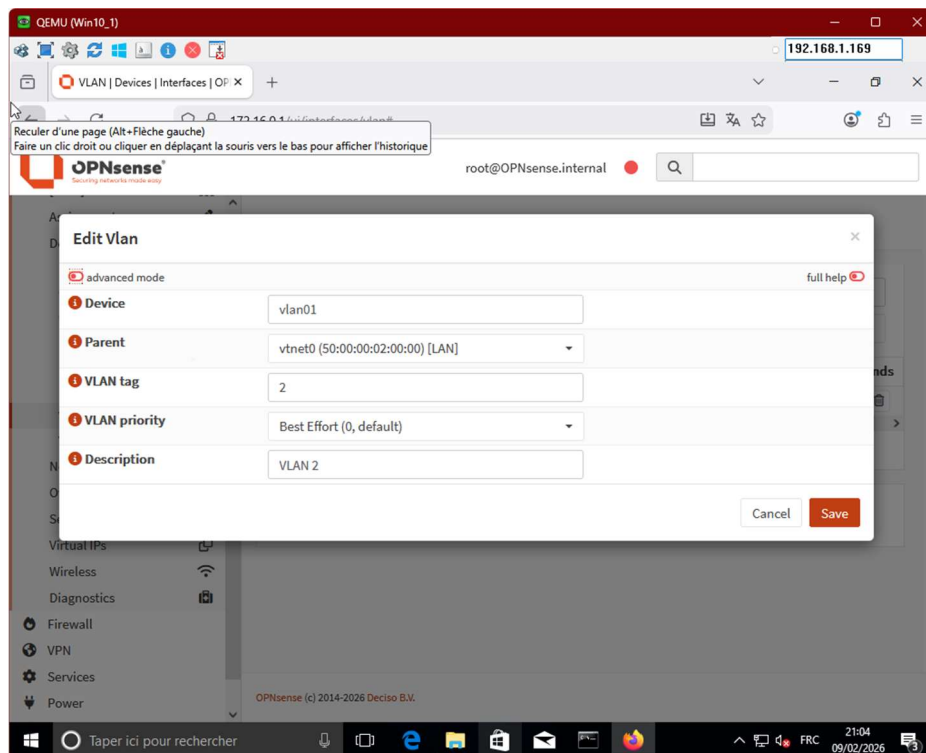


3. Créer le deuxième VLAN

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**.

Interfaces: Assignments

Interface	Identifier	Device	
[LAN]	lan	vtnet0 (50:00:00:02:00:00)	1
[VLAN2]	opt1	vlan01 VLAN2 (Parent: vtnet0, Tag: 2)	2
[VLAN3]	opt2	vlan02 VLAN3 (Parent: vtnet0, Tag: 3)	3
[WAN]	wan	vtnet1 (50:00:00:02:00:01)	4

Save 5

+ Assign a new interface

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

Description:

Add

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 highlighted with orange boxes and numbered 1 through 5. 1: Basic configuration section, 'Enable interface' checkbox is checked. 2: Identifier is 'opt1' and Device is 'vlan01'. 3: IPv4 Configuration Type is 'Static IPv4'. 4: IPv4 address is '172.16.2.1' with a subnet mask of '24'. 5: The 'Save' button is highlighted.

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 displays the OPNsense web interface for configuring the 'opt2' interface. The configuration is organized into sections: Basic configuration, Generic configuration, and Static IPv4 configuration. The 'Enable Interface' checkbox is checked. The 'Description' field is set to 'VLAN3'. The 'IPv4 Configuration Type' is set to 'Static IPv4'. The 'IPv4 address' is set to '172.16.3.1' with a subnet mask of '24'. The 'Save' button is highlighted with a green checkmark and a red circle with the number 5. The left sidebar shows the navigation menu with 'Interfaces' selected. The top navigation bar shows 'Interfaces | OPNsense' and the current page is '172.16.0.1/interfaces.php?if=opt2'.

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** !

The screenshot shows the OPNsense web interface in a QEMU (Win10_1) environment. The browser address bar shows the URL `172.16.0.1/ui/routing/configuration`. The main content area displays the 'System: Gateways: Configuration' page. A modal window titled 'Edit Gateway' is open, showing the configuration for a gateway named 'Gateway-ROUteur2'. The configuration includes the following settings:

- Disabled**:
- Name**: Gateway-ROUteur2
- Interface**: WAN
- Address Family**: IPv4
- Priority**: 255
- IP Address**: 172.16.0.254
- Upstream Gateway**:
- Far Gateway**:
- Disable Gateway Monitoring**:
- Mark Gateway as Down**:
- Description**: (empty text field)

The 'Apply' button is located at the bottom left of the modal window. The background shows the OPNsense configuration page with a table of gateways and a sidebar menu.

QEMU (Win10_1) 192.168.1.169

Configuration | Gateways | Syst: X

172.16.0.1/ui/routing/configuration

OPNsense

System: Gateways: Configuration

Disabled	Name	Interface	Address Family	Priority	IP Address	Monitor IP	RTT	RTTid	Loss	Status	Description	Commands
<input type="checkbox"/>	Gateway-ROUTEUR2 (active)	WAN	IPv4	255	172.19.0.224		-	-	-	✔		

Showing 1 to 1 of 1 entries

Apply

Affichage des tâches

Taper ici pour rechercher

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** !

The screenshot shows the OPNsense web interface for configuring the WAN interface. The page is titled "Interfaces: [WAN]" and contains several sections:

- Basic configuration:** Includes the "Enable Interface" checkbox (checked), "Lock" checkbox (unchecked), "Prevent interface removal" checkbox (unchecked), "Identifier" (wan), "Device" (vtnet1), and "Description" (empty).
- Generic configuration:** Includes "Block private networks" (unchecked), "Block bogon networks" (unchecked), "IPv4 Configuration Type" (Static IPv4), "IPV4 Configuration Type" (None), "MAC address" (empty), "Promiscuous mode" (unchecked), "MTU" (empty), "MSS" (empty), and "Dynamic gateway policy" (unchecked).
- Hardware settings:** Includes "Override global settings" (unchecked).
- Static IPv4 configuration:** Includes "IPV4 address" (172.16.0.253/16) and "IPV4 gateway rules" (Gateway-ROU/TEU/R2 - 172.16.0.254).

Five red arrows point to specific elements: 1. The "Enable Interface" checkbox. 2. The "Block private networks" and "Block bogon networks" checkboxes. 3. The "IPv4 Configuration Type" dropdown menu. 4. The "IPV4 address" and "IPV4 gateway rules" fields. 5. The "Save" button.

Assigné l'interface vtnet1 au WAN :

The screenshot shows the OPNsense web interface for interface assignments. The browser address bar shows '172.16.0.1/interfaces_assign.php'. The left sidebar contains navigation options like 'Interfaces', 'Assignments', 'Devices', etc. The main content area is titled 'Interfaces: Assignments' and contains a table with the following 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, there is a section for '+ Assign a new interface' with a 'Device' dropdown set to 'vtnet2 (50:00:00:02:00:02)' and a 'Description' field. A red box highlights the 'wan' row in the table, and an orange arrow points to the 'Device' column of that row.

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

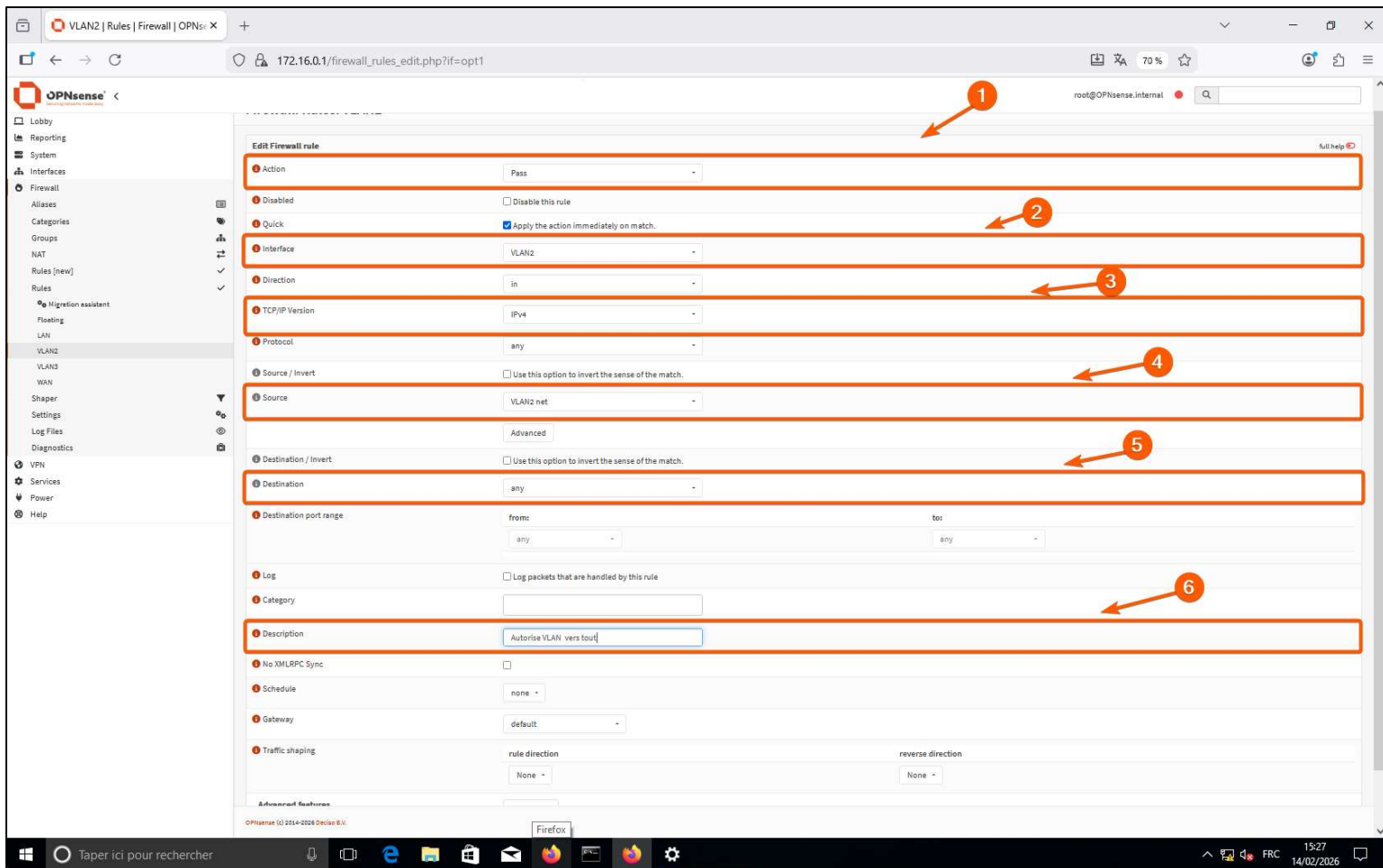
En haut → cliquer sur **+ Add**

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 :

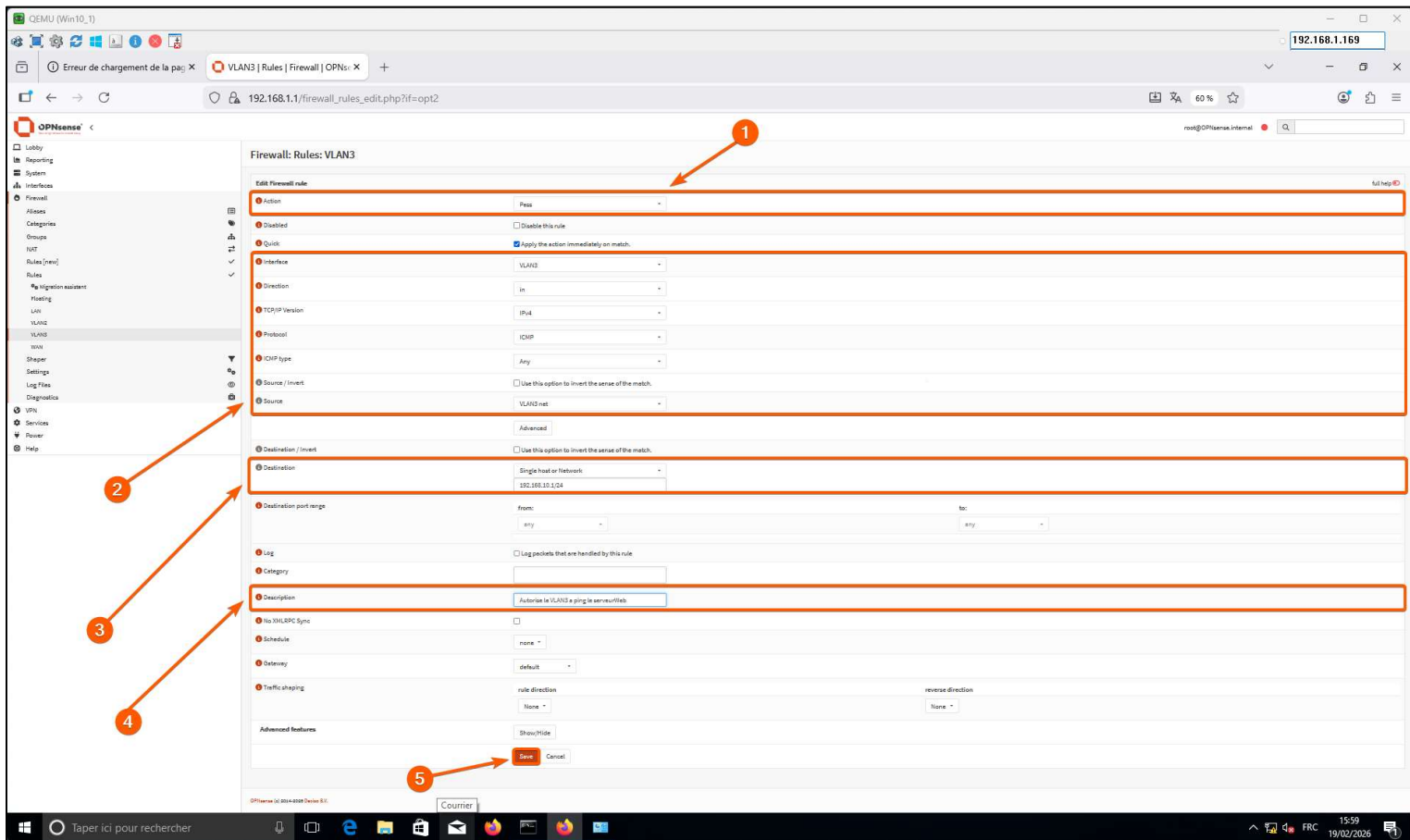
- **Action** : Pass
- **Interface** : VLAN3
- **Direction** : In
- **TCP/IP Version** : IPv4
- **Protocol** : ICMP

→ 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** !



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 editing a firewall rule. The page title is "Firewall: Rules: VLAN3". The "Edit Firewall rule" form is displayed with the following settings:

- Action:** Pass (highlighted with box 1)
- Disabled:** Disable this rule
- Quick:** Apply the action immediately on match. (highlighted with box 2)
- Interface:** VLAN3
- Direction:** In
- TCP/IP Version:** IPv4
- Protocol:** any
- Source / Invert:** Use this option to invert the sense of the match.
- Source:** VLAN3 net (highlighted with box 3)
- Destination / Invert:** Use this option to invert the sense of the match.
- 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 (highlighted with box 4)
- No XMLRPC Sync:**
- Schedule:** none

At the bottom right, there is a "full help" link and a Windows activation watermark: "Activer Windows. Accédez aux paramètres pour activer Windows."

Paramétrage de la Gateway du Routeur 2.

The screenshot displays the OPNsense web interface for configuring a gateway. The browser address bar shows the URL `172.16.0.1/ui/routing/configuration`. The main navigation menu on the left includes options like 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, and Help. The 'Edit Gateway' modal window is open, showing the following configuration details:

- advanced mode** (toggle)
- Disabled** (checkbox)
- Name**: Gateway-ROUteur2
- Interface**: WAN
- Address Family**: IPv4
- Priority**: 255
- IP Address**: 172.16.10.254
- Upstream Gateway** (checkbox)
- Far Gateway** (checkbox)
- Disable Gateway Monitoring** (checkbox checked)
- Mark Gateway as Down** (checkbox)
- Description** (text field)

Buttons for 'Cancel' and 'Save' are located at the bottom right of the modal. The footer of the interface shows 'OPNsense (c) 2014-2026 Deciso B.V.' and the system tray includes the text 'Posez-moi une question', the date '07/05/2026', and the time '22:42'.



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

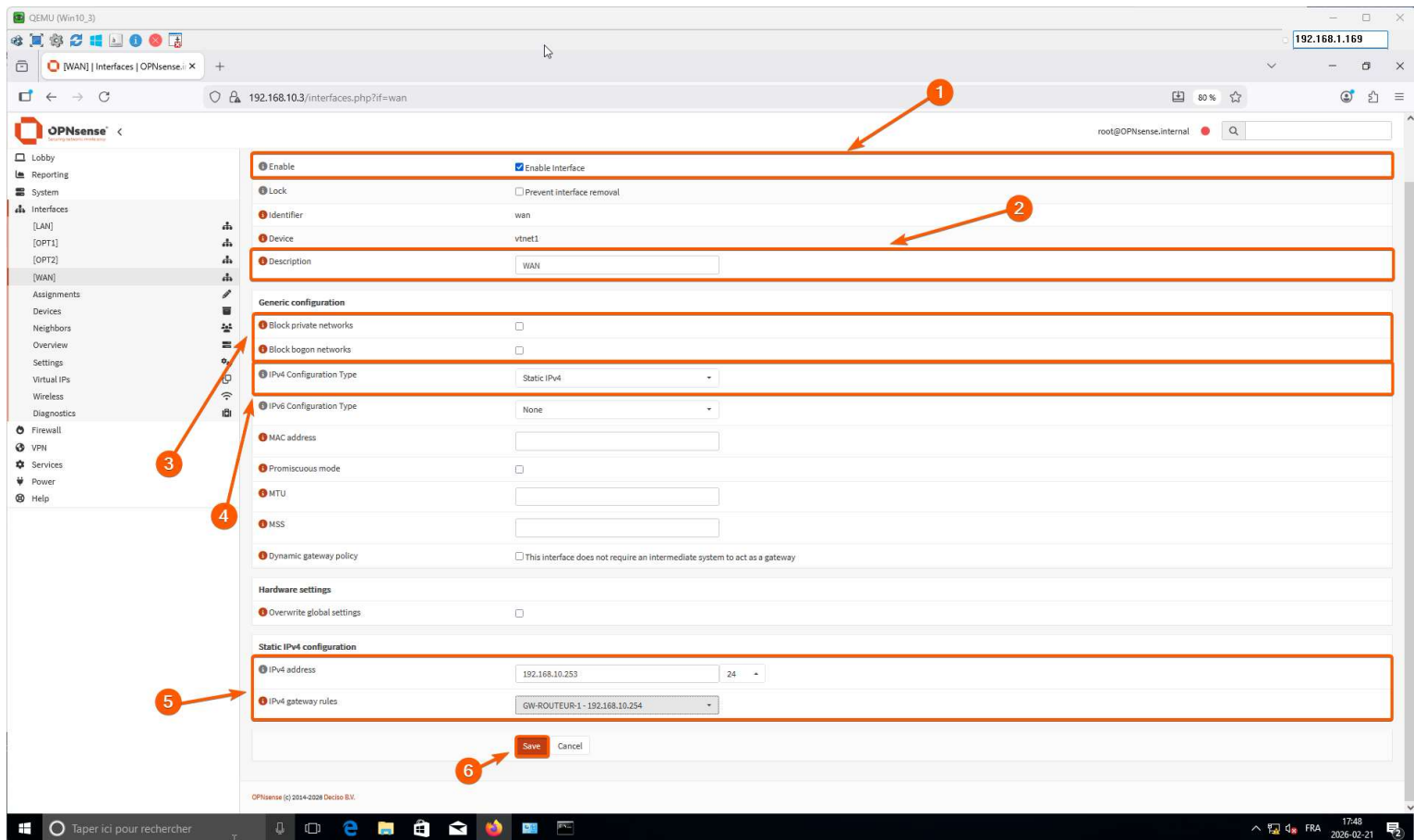
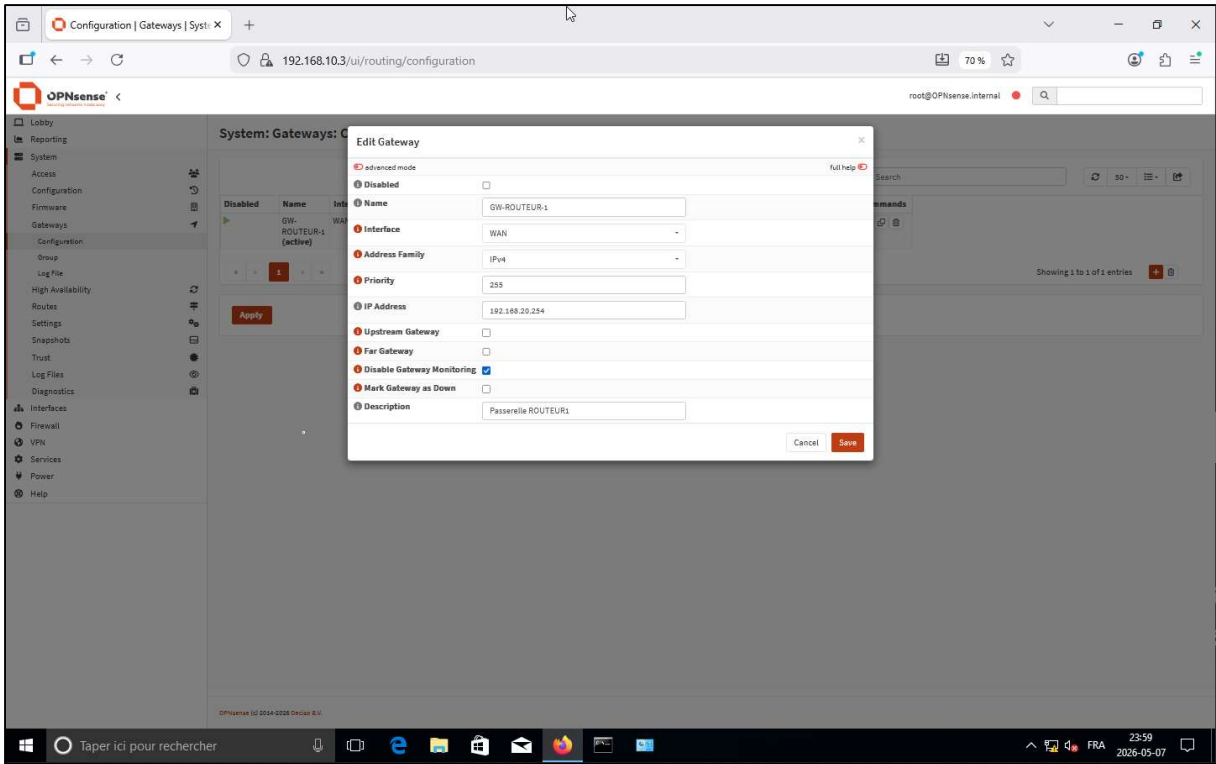
IPv4 Configuration Type : Static IPv4

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 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 XMLRPC Sync**:
- Schedule**: none
- Gateway**: default
- Traffic shaping**: rule direction (None), reverse direction (None)
- Advanced features**: Show/Hide
- Rule Information**: Created: 2/11/20 20:53:22 (root@192.168.10.2), Updated: 2/11/20 20:53:56 (root@192.168.10.2)

At the bottom, the 'Save' button is highlighted with a red circle and arrow labeled '5'. Other red circles and arrows point to the 'Add' button (1), the 'Action' field (2), the 'Destination' field (3), and the 'Description' field (4).

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 currently disabled. The configuration is as follows:

- 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 le trafic interne LAN

The 'Save' button is highlighted with a red circle and arrow labeled '6'. Other numbered arrows point to the 'Add' button (1), the 'Action' field (2), the 'Interface' field (3), the 'Description' field (4), and the 'Advanced features' section (5).

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
 - ☞ From : any
 - ☞ To : any
- **Description** : Blocage par défaut LAN

Puis :

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

The screenshot shows the OPNsense web interface for configuring a firewall rule. The rule is named 'LAN' and is configured with the following settings:

- Action:** Pass
- Disabled:**
- Quick:** Apply the action immediately on match.
- Interface:** LAN
- Direction:** in
- TCP/IP Version:** IPv4
- Protocol:** any
- Source / Invert:** Use this option to invert the sense of the match.
- Source:** Single host or Network (172.16.0.0/32)
- Destination / Invert:** Use this option to invert the sense of the match.
- Destination:** LAN net
- Destination port range:** From: any, To: any
- Log:** Log packets that are handled by this rule
- Category:** none
- Description:** Autorise trafic batiement A
- No XMLRPC Sync:**
- Schedule:** none
- Gateway:** default
- Traffic shaping:** rule direction: None, reverse direction: None
- Advanced Features:** Show/Hide

The 'Save' button is highlighted with an orange arrow. The page title is 'Firewall: Rules: LAN' and the user is 'root@OPNsense.internal'.

LAN | Rules | Firewall | OPNsense

192.168.10.3/firewall_rules.php?f=lan

root@OPNsense.internal

Firewall: Rules: LAN

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)	block (disabled)	reject (disabled)	log (disabled)	in	out	first match last match

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.

LAN | Rules | Firewall | OPNsense

192.168.10.3/firewall_rules.php?f=lan

root@OPNsense.internal

Firewall: Rules: LAN

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)	block (disabled)	reject (disabled)	log (disabled)	in	out	first match last match

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.



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** !

The screenshot displays the OPNsense web interface for configuring a firewall rule. The browser address bar shows the URL `192.168.10.3/firewall_rules_edit.php?if=lan`. The page title is "Firewall: Rules: LAN". The configuration form includes the following fields:

- Action:** Pass
- Disabled:** Disable this rule
- Quick:** Apply the action immediately on match.
- Interface:** LAN
- Direction:** In
- TCP/IP Version:** IPv4
- Protocol:** ICMP
- ICMP type:** Any
- Source / Invert:** Use this option to invert the sense of the match.
- Source:** Single host or Network: 172.16.5.1
- Destination / Invert:** Use this option to invert the sense of the match.
- 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:** (empty)
- Description:** Autoriser les ping venant du VLAN 5 vers le serveur
- No XMLRPC Sync:**
- Schedule:** none

Five red arrows with numbers 1 through 5 point to specific elements in the interface: 1 points to the rule title, 2 points to the left sidebar menu, 3 points to the 'Destination / Invert' section, 4 points to the 'Destination' field, and 5 points to the 'Description' field.



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** !

The screenshot displays the OPNsense web interface for configuring a Firewall Rule. The browser address bar shows the URL `192.168.10.3/firewall_rules_edit.php?if=wanduid=0`. The page title is "Firewall: Rules: WAN". The configuration form includes the following fields:

- Action:** Pass
- Disabled:** Disable this rule
- Quick:** Apply the action immediately on match.
- Interface:** WAN
- Direction:** In
- TCP/IP Version:** IPv4
- Protocol:** any
- 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:** WAN address
- Destination port range:** Name: any, Min: any, Max: any
- Log:** Log packets that are handled by this rule
- Category:** (empty)
- Description:** (empty)
- No SNL/SPC Sync:**
- Schedule:** none
- Priority:** default
- Traffic shaping:** rule direction: None, reverse direction: None
- Advanced features:** Show/Hide
- Rule Information:**
 - Created: 2/21/24 17:57:02 (user@192.168.10.3)
 - Updated: 2/21/24 17:57:02 (user@192.168.10.3)

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**.

The screenshot shows the OPNsense web interface for configuring Dnsmasq DNS & DHCP. The 'General' tab is selected. The 'Default' section has 'Enable' checked and 'Interface' set to 'LAN, VLAN2, VLAN3'. The 'DNS' section has 'Listen port' at 53053, 'DNSSEC' unchecked, and 'No hosts lookup' unchecked. The 'DNS Query Forwarding' section has 'Query DNS servers sequentially' unchecked, 'Require domain' unchecked, 'Do not forward to system defined DNS servers' unchecked, and 'Do not forward private reverse lookups' unchecked. The 'DHCP' section has 'DHCP FQDN' checked, 'DHCP default domain' set to 'internal', 'DHCP local domain' checked, 'DHCP authoritative' checked, 'DHCP reply delay' empty, 'DHCP register firewall rules' checked, and 'Router advertisements' checked. The 'ISC / KEA DHCP (legacy)' section has 'Register ISC DHCP4 leases' unchecked, 'DHCP domain override' empty, 'Register DHCP static mappings' unchecked, and 'Prefer DHCP' unchecked. The 'Apply' button is at the bottom.

Etape 2 : Définir la plage DHCP pour VLAN2

Aller dans :

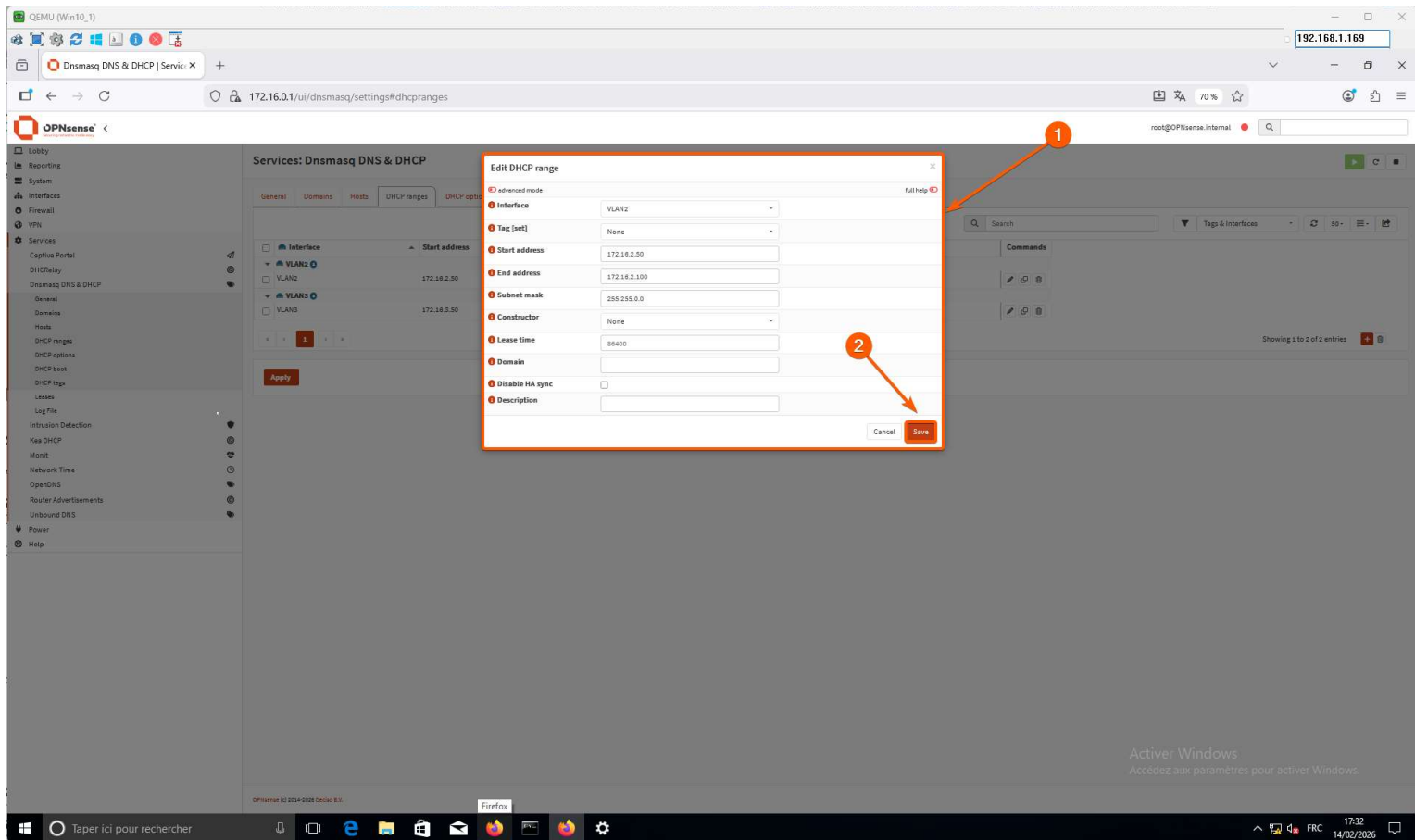
Services → Dnsmasq DNS & DHCP → DHCP ranges

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**. 



The screenshot shows the OPNsense web interface. The main content area is titled 'Services: Dnsmasq DNS & DHCP' and has tabs for 'General', 'Domains', 'Hosts', 'DHCP ranges', and 'DHCP options'. The 'DHCP ranges' tab is active, showing a table with columns for 'Interface' and 'Start address'. There are three entries: 'VLAN2' with '172.16.2.50', 'VLAN3' with '172.16.3.50', and a '+' button to add more. An 'Apply' button is visible below the table. A modal window titled 'Edit DHCP range' is open, showing the configuration for a new range. The fields are: Interface (VLAN2), Tag [opt] (None), Start address (172.16.2.50), End address (172.16.2.100), Subnet mask (255.255.255.0), Constructor (None), Lease time (86400), Domain, Disable HA sync (checkbox), and Description. A red box highlights the 'Save' button in the modal, and a red arrow points to the 'Apply' button in the background. The browser address bar shows '172.16.0.1/ui/dnsmasq/settings#dhcpranges'.

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**.

The screenshot shows the OPNsense web interface. The main content area displays the 'Services: Dnsmasq DNS & DHCP' configuration page, specifically the 'DHCP ranges' tab. A table lists existing DHCP ranges for VLAN2 and VLAN3. A modal window titled 'Edit DHCP range' is open, allowing configuration for a new range. The configuration fields are as follows:

Field	Value
Interface	VLAN3
Tag [set]	None
Start address	172.16.3.50
End address	172.16.3.100
Subnet mask	255.255.0.0
Constructor	None
Lease time	86400
Domain	
Disable HA sync	<input type="checkbox"/>
Description	

The 'Save' button at the bottom right of the modal is highlighted with a red circle and the number 2. The background interface shows the 'DHCP ranges' table with columns for 'Interface' and 'Start address'.

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

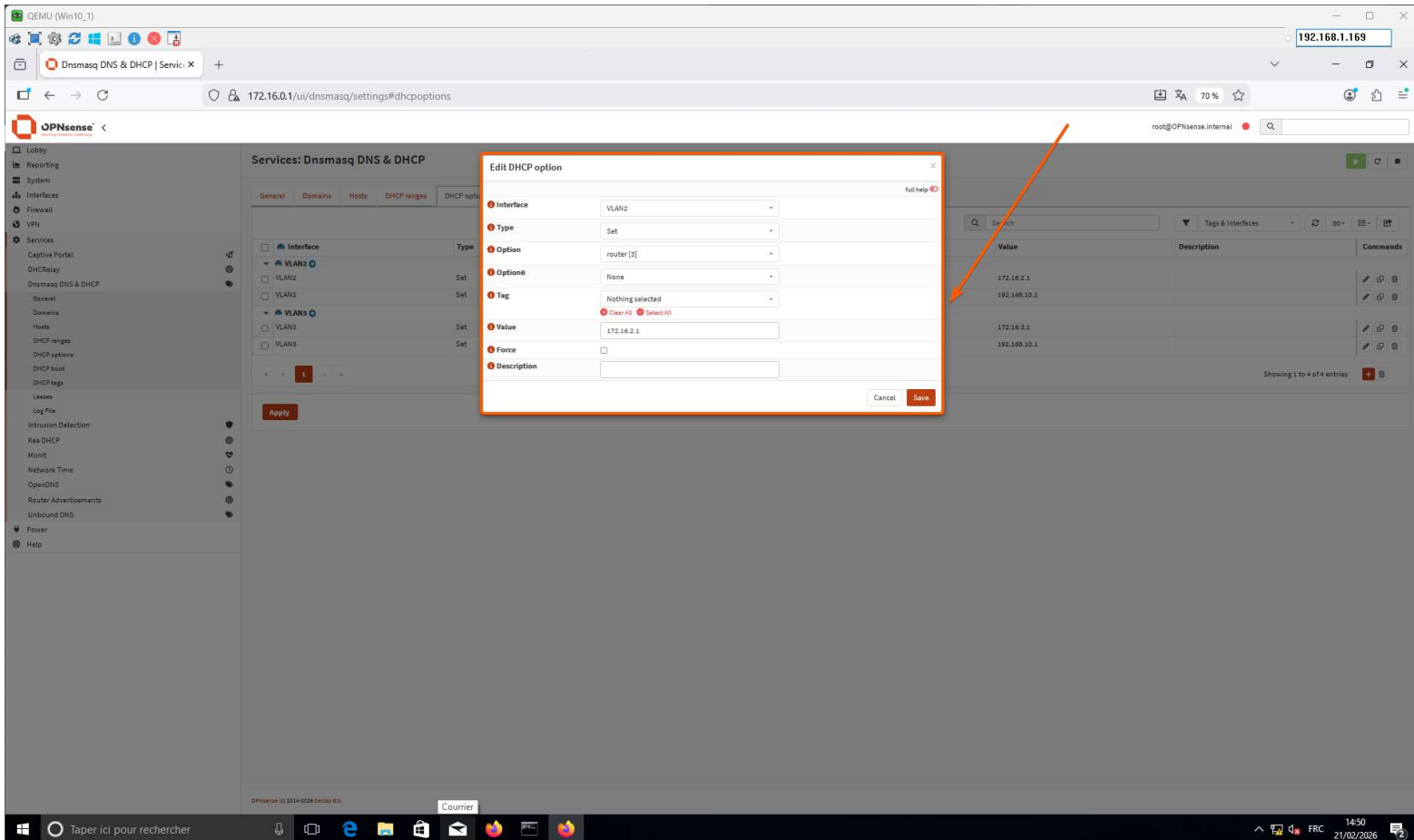
Puis cliquer **Save**, puis **Apply**.

The screenshot shows the OPNsense web interface for configuring DHCP options. The main page is titled 'Services: Dnsmasq DNS & DHCP' and has tabs for 'General', 'Domains', 'Hosts', 'DHCP ranges', and 'DHCP options'. The 'DHCP options' tab is active, showing a table with columns for 'Interface', 'Type', 'Option', 'Value', 'Force', and 'Description'. There are four entries in the table, with the first one highlighted in orange. An 'Edit DHCP option' dialog box is open over the first entry, showing the following configuration:

- Interface: VLAN3
- Type: Set
- Option: router [3]
- Options: None
- Tag: Nothing selected
- Value: 172.16.3.1
- Force:
- Description:

The dialog box has 'Cancel' and 'Save' buttons. An orange arrow points from the dialog box to the first entry in the table. The table also shows the other three entries:

Interface	Type	Option	Value	Description
VLAN3	Set	router [3]	172.16.3.1	
VLAN2	Set	router [3]	172.16.2.1	
VLAN2	Set	router [3]	192.168.10.1	
VLAN3	Set	router [3]	192.168.10.1	



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

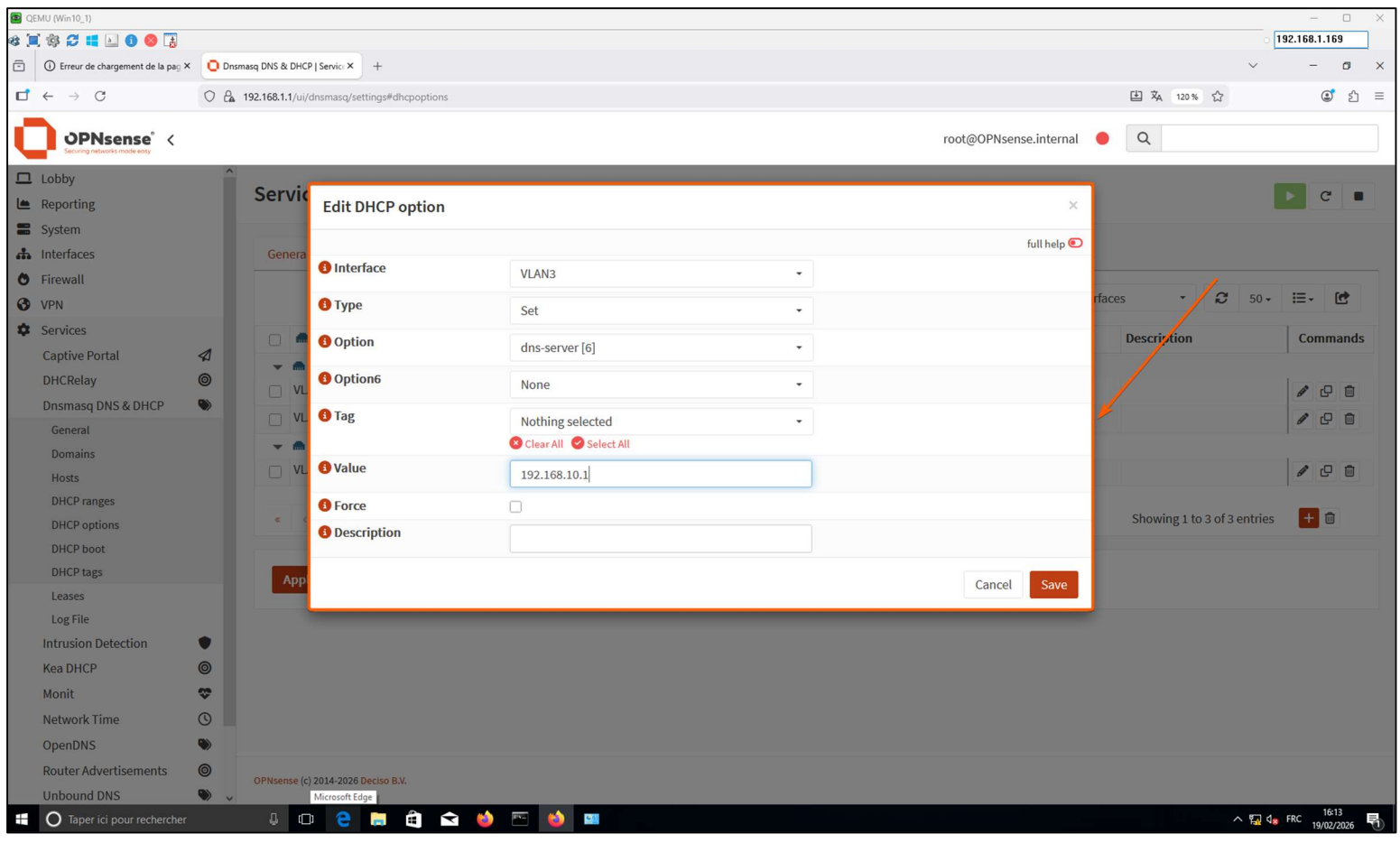
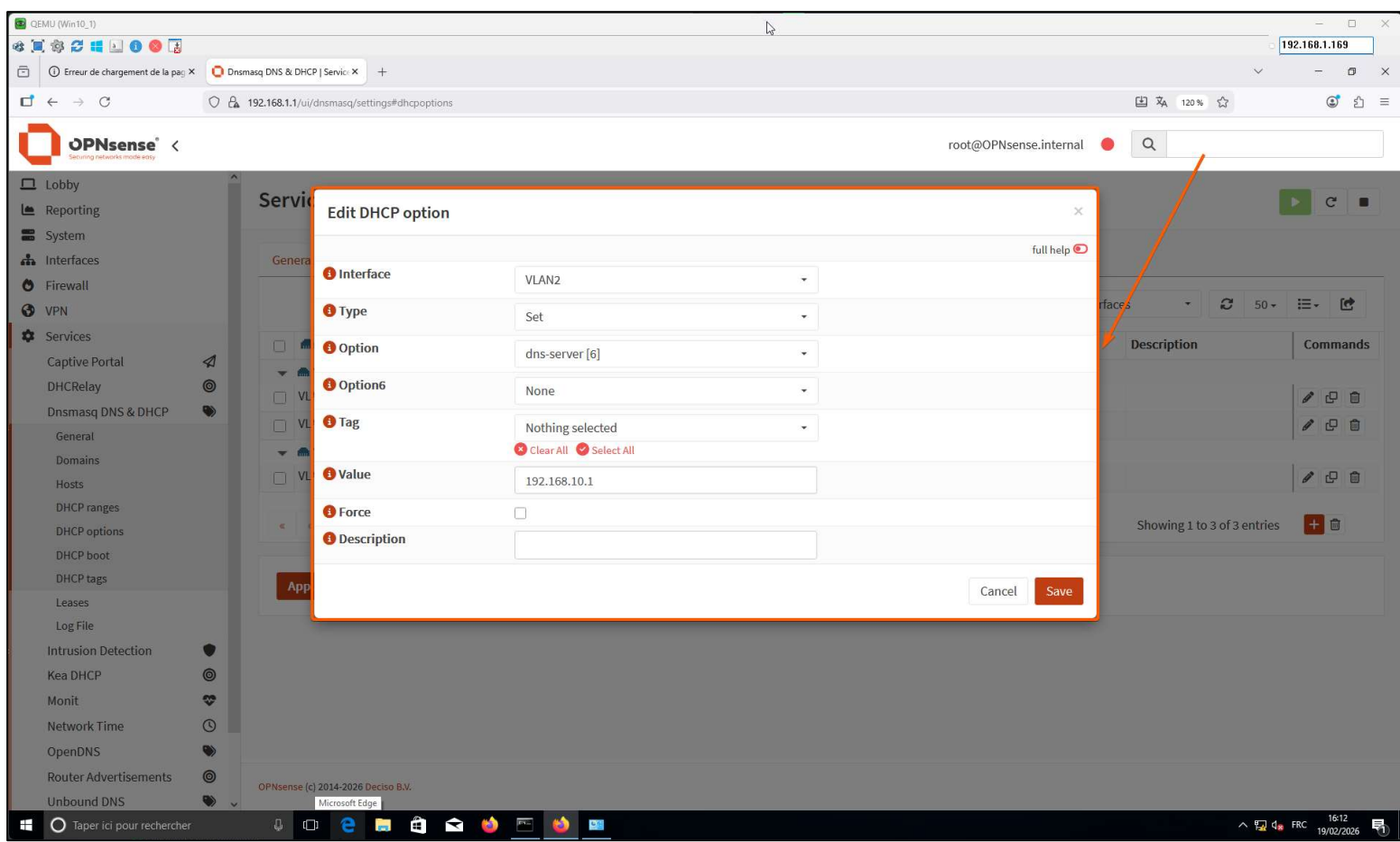
Description : DNS Server pour le vlan 2

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



The screenshot shows the OPNsense web interface for configuring Dnsmasq DNS & DHCP services. The 'DHCP options' tab is selected, showing a table of options for two VLANs: VLAN2 and VLAN3. Each VLAN has two options: 'router' and 'dns-server'. The 'router' option is set to 172.16.0.254 and the 'dns-server' option is set to 192.168.10.1. An 'Apply' button is located at the bottom of the table.

Interface	Type	Option	Option6	Value	Description	Commands
VLAN2						
<input type="checkbox"/> VLAN2	Set	router [3]		172.16.0.254		
<input type="checkbox"/> VLAN2	Set	dns-server [6]		192.168.10.1		
VLAN3						
<input type="checkbox"/> VLAN3	Set	router [3]		172.16.0.254		
<input type="checkbox"/> VLAN3	Set	dns-server [6]		192.168.10.1		

! 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
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-064LQUQ
    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-80-08-50-00-00-06-00-00
    Serveurs DNS. . . . . : 192.168.18.1
    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 ...	intemal
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 ...	intemal
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 ...	intemal
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	

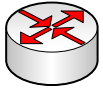
Fermer

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

Etape 1 : Configuration des équipements d'interconnexion :

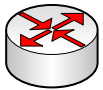
<u>Configuration des ports de Switch 1:</u>	<u>Configuration des ports de Switch 2:</u>
<pre>interface Ethernet0/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 1-3 switchport mode trunk duplex auto ! interface Ethernet0/1 switchport access vlan 2 duplex auto ! interface Ethernet0/2 switchport access vlan 3 duplex auto ! interface Ethernet0/3 switchport mode access duplex auto</pre>	<p>→ Création d'un vlan pour le service de la Direction</p> <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 :

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

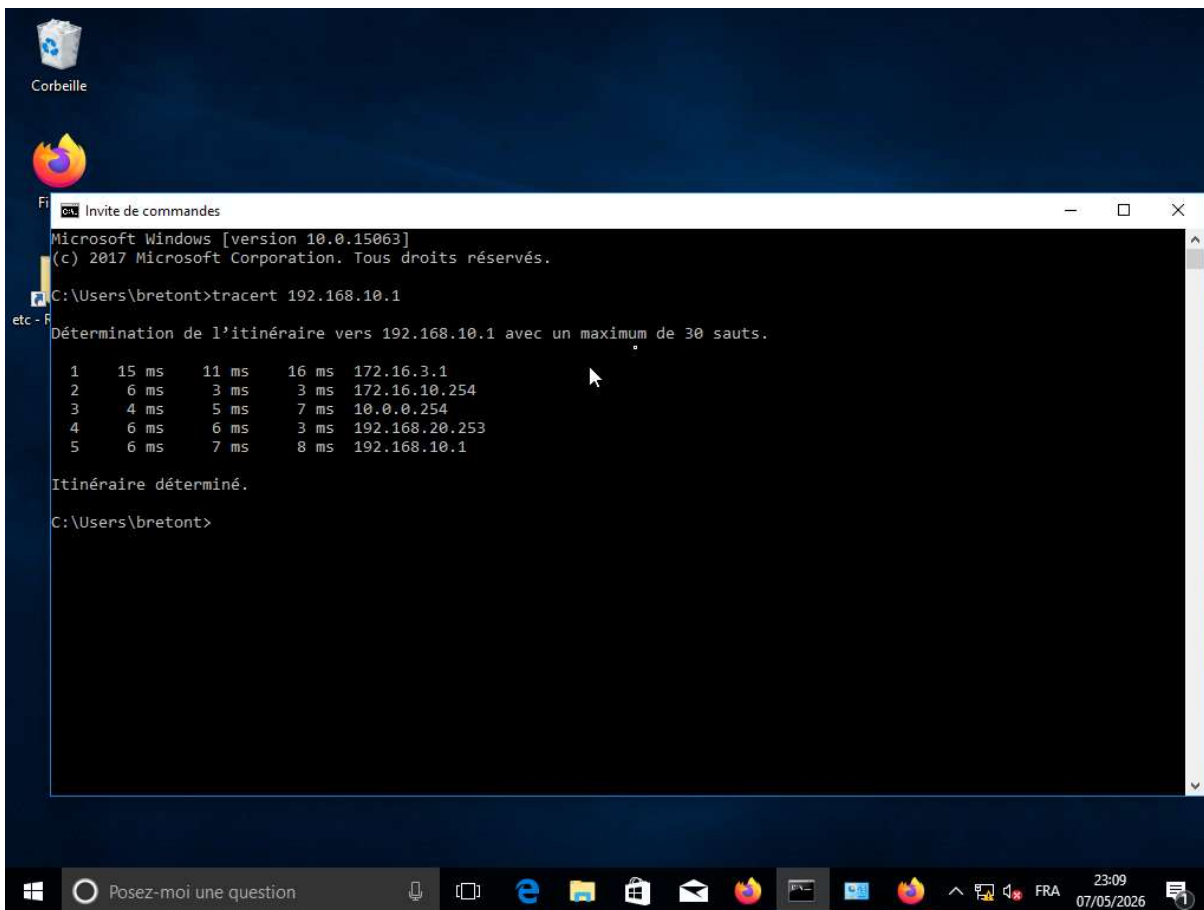
Win_10_1	Windows Server – 192.168.10.1	✓
Win_10_2	Windows Server – 192.168.10.1	✓
Win_10_3	Windows Server – 192.168.10.1	✓

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 :



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

C:\Users\bretont>tracert 192.168.10.1

Détermination de l'itinéraire vers 192.168.10.1 avec un maximum de 30 sauts.

  1  15 ms  11 ms  16 ms  172.16.3.1
  2   6 ms   3 ms   3 ms  172.16.10.254
  3   4 ms   5 ms   7 ms  10.0.0.254
  4   6 ms   6 ms   3 ms  192.168.20.253
  5   6 ms   7 ms   8 ms  192.168.10.1

Itinéraire déterminé.

C:\Users\bretont>
```

Accès au site Web depuis le poste du VLAN3

Bâtiment A : Pôle pédagogique
172.16.0.0 /24

Bâtiment B : Direction
192.168.10.0 /24

VLAN 3
Accès Site - Autorisé

VLAN 2
Accès Site - Refusé

Accès Oupsense
@ : root
MDP : eve

Firewall Rules: VLAN3

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPV4	VLAN3	net	192.168.10.124	*	*	*	Automatically generated rule!
ICMP	VLAN3	net	*	*	*	*	Autorise le VLAN3 à ping le serveurWeb.
IPV4 TCP	VLAN3	net	*	80 (HTTP)	*	*	Autorise le VLAN3 access web LycéeTech

**Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.
C:\Users\bretont>ping 192.168.1.169**

```

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=15 ms TTL=124
Réponse de 192.168.10.1 : octets=32 temps=17 ms TTL=124
Réponse de 192.168.10.1 : octets=32 temps=20 ms TTL=124
Réponse de 192.168.10.1 : octets=32 temps=19 ms TTL=124

Statistiques Ping pour 192.168.10.1:
    Packets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles de allers-retours :
        Minimum = 15ms, Maximum = 20ms, Moyenne = 18ms
    C:\Users\bretont>
    
```

Hum, nous ne parvenons pas à trouver ce site.

Impossible de se connecter au serveur à l'adresse www.lyceetech.com.

Si l'adresse saisie était correcte, vous pouvez :

- Réessayer plus tard
- Vérifier votre connexion réseau

**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 :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.10.1:
    Packets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
    C:\Users\bretont>
    
```

Accès au site depuis un poste du pôle pédagogique qui se trouve dans le VLAN3 autorisé. Cet accès est possible au moyen des règles administré.

Non Accès au site Web depuis le poste du VLAN2

Bâtiment A : Pôle pédagogique
172.16.0.0 /24

Bâtiment B : Direction
192.168.10.0 /24

VLAN 3
Accès Site - Autorisé

VLAN 2
Accès Site - Refusé

Accès Oupsense
@ : root
MDP : eve

Firewall Rules: VLAN2

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
IPV4	VLAN2	net	*	*	*	*	Block IPv4 2 zone trust
IPV4	VLAN2	net	*	*	*	*	Block IPv4 2 zone trust
IPV4	VLAN2	net	*	*	*	*	Block IPv4 2 zone trust

**Microsoft Windows [version 10.0.15063]
(c) 2017 Microsoft Corporation. Tous droits réservés.
C:\Users\bretont>ping 192.168.1.169**

```

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.10.1:
    Packets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
    C:\Users\bretont>
    
```

Hum, nous ne parvenons pas à trouver ce site.

Impossible de se connecter au serveur à l'adresse www.lyceetech.com.

Si l'adresse saisie était correcte, vous pouvez :

- Réessayer plus tard
- Vérifier votre connexion réseau

**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 :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.10.1:
    Packets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
    C:\Users\bretont>
    
```

Accès non autorisé au site depuis le poste du VLAN2 et impossible de communiquer avec le serveur grâce à une règle qui bloque toute communication.

Accès au site Web depuis le poste de direction :

