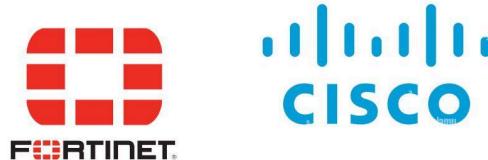


 **Mise en place d'un lab FortiGate  
sur GNS3 : VLAN, switch Cisco L2 et  
segmentation réseau – Partie 1**



# Introduction

Dans le monde de la cybersécurité et de l'administration réseau, comprendre le fonctionnement d'un **pare-feu comme FortiGate** et savoir configurer un réseau segmenté est essentiel.

Ce lab vous permettra de :

- Mettre en place un environnement virtuel complet dans **GNS3**
- Créer un réseau simulant une **infrastructure d'entreprise**
- Tester la **connectivité et la segmentation VLAN** avant de passer à la configuration avancée du FortiGate

Ce lab est idéal pour les étudiants, passionnés d'infrastructure ou professionnels souhaitant se familiariser avec **la sécurité réseau et le contrôle des flux**.

**Objectifs :**

L'objectif de ce lab est de **simuler un réseau d'entreprise** afin de préparer les configurations avancées de FortiGate (sécurité, firewall, routage).

À la fin de cette Partie 1, vous serez capable de :

- Ajouter et tester les images Cisco et FortiGate dans GNS3
- Créer un réseau de test complet avec un FortiGate et des switchs
- Configurer des VLANs pour segmenter le réseau
- Répartir les adresses IP par VLAN et tester la connectivité

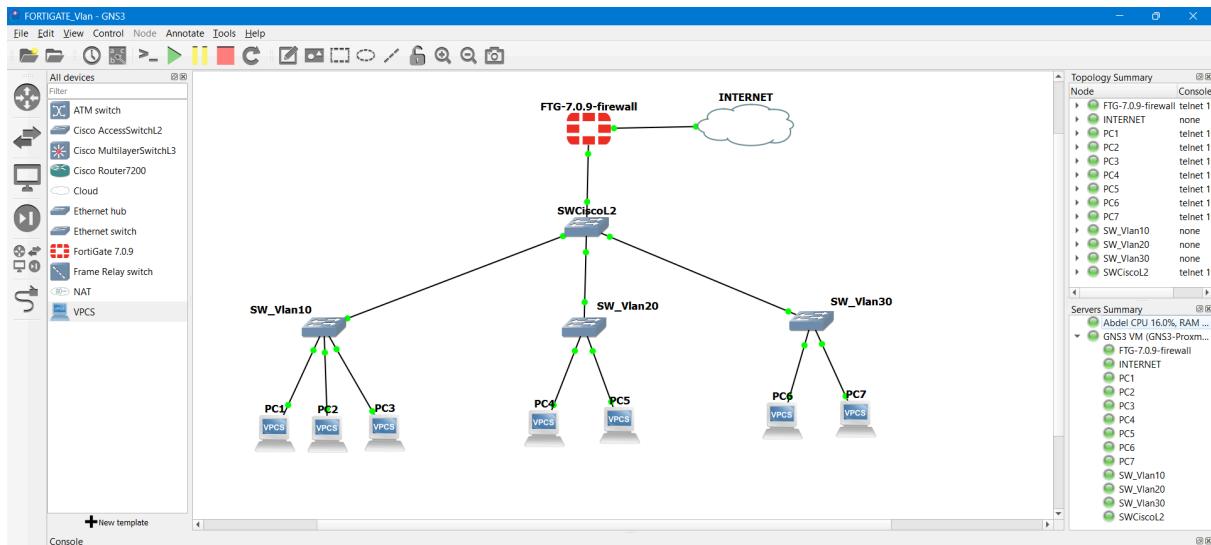
**Prérequis :**

- **GNS3** installé sur votre poste
- Image **FortiGate** fonctionnelle dans GNS3
- Image **Switch Cisco L2**
- Quelques PCs virtuels pour tester la connectivité
- Connexion internet pour télécharger les images si nécessaire

# 1. Architecture et Topologie du lab

Notre architecture inclura les éléments suivants :

- Un FortiGate (pare-feu central)
- Un switch Cisco L2 pour la configuration des VLAN
- Trois switches GNS3 reliés au switch Cisco
- Des PCs connectés pour tester la connectivité



## FortiGate FTG-7.0.9 – Connexions

Interface FortiGate	Type	Connecté à	Rôle
port1	WAN	INTERNET (Cloud)	Accès Internet
port2	LAN/TRUNK	SWCiscoL2 (Et0/0)	Transport des VLAN 10/20/30

## Switch central – SWCiscoL2

Port SWCiscoL2	Mode	VLAN autorisés	Connecté à
Et0/0	Trunk	10,20,30	FortiGate port2
Et0/1	Trunk	10	SW_Vlan10
Et0/2	Trunk	20	SW_Vlan20
Et0/3	Trunk	30	SW_Vlan30

Abdourahamane AbdelWahab

### **Switch d'accès VLAN 10 – SW\_Vlan10**

Port SW_Vlan10	Mode	VLAN	Connecté à
Et0	Trunk	10	SWCiscoL2 Et0/1
Et1	Access	10	PC1
Et2	Access	10	PC2
Et3	Access	10	PC3

### **Switch d'accès VLAN 20 – SW\_Vlan20**

Port SW_Vlan10	Mode	VLAN	Connecté à
Et0	Trunk	20	SWCiscoL2 Et0/2
Et1	Access	20	PC4
Et2	Access	20	PC5

### **Switch d'accès VLAN 30 – SW\_Vlan30**

Port SW_Vlan10	Mode	VLAN	Connecté à
Et0	Trunk	30	SWCiscoL2 Et0/3
Et1	Access	30	PC6
Et2	Access	30	PC7

## 2. Ajout des images dans GNS3

Une **image GNS3**, c'est simplement le fichier système d'un équipement (routeur, switch, firewall, VM...) que GNS3 va utiliser pour l'émuler ou le simuler. De façon générale, c'est le « système d'exploitation » ou la VM (Qemu, VirtualBox, VMware, etc.) que GNS3 va lancer pour représenter un équipement réseau dans ta topologie.

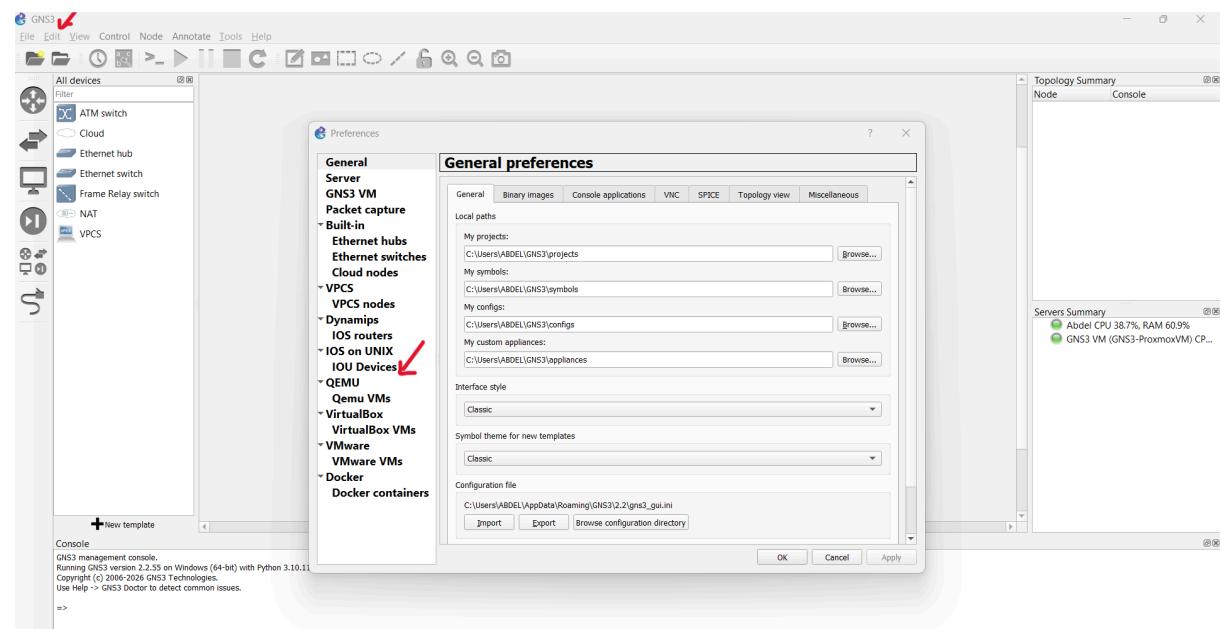
### 2.1 Ajout d'une image cisco switch L2

Dans le cas de Cisco, une image GNS3 est souvent une image IOS au format ".bin" ou ".image" qu'on importe dans GNS3 pour créer un routeur ou un switch virtuel.

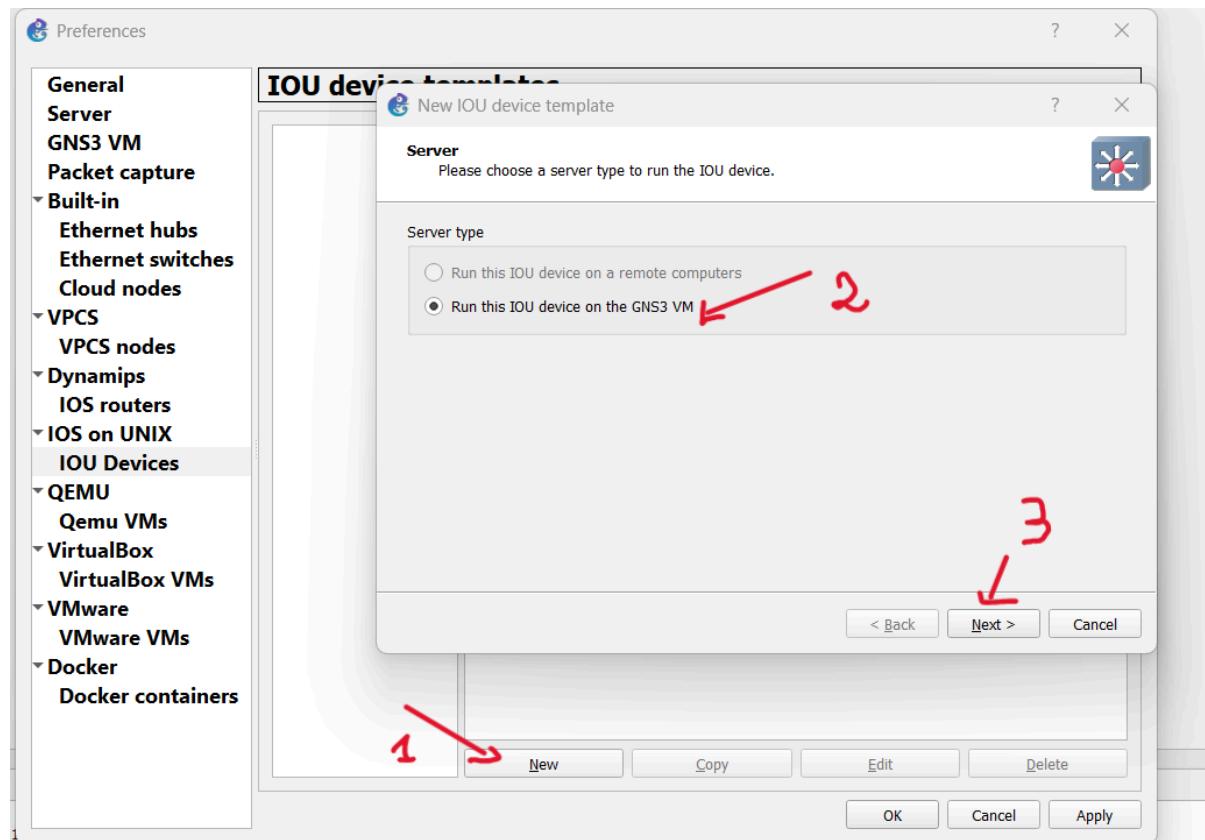
Tout d'abord télécharger les images via github

<https://github.com/hegdepavankumar/Cisco-Images-for-GNS3-and-EVE-NG>

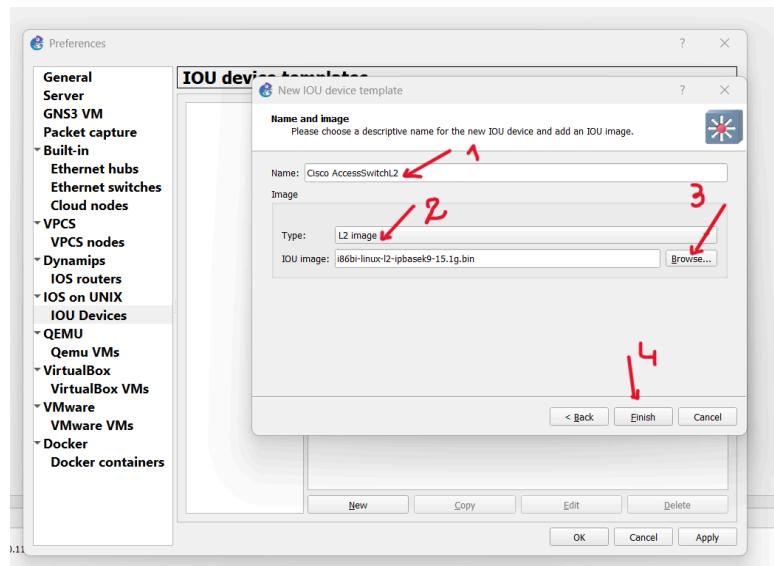
ensuite ajouter l'image de notre switch sur GN3 ouvrir GNS3 et aller dans l'onglet **Edit → Preferences →IOS on UNIX** puis cliquer sur **IOU Devices**



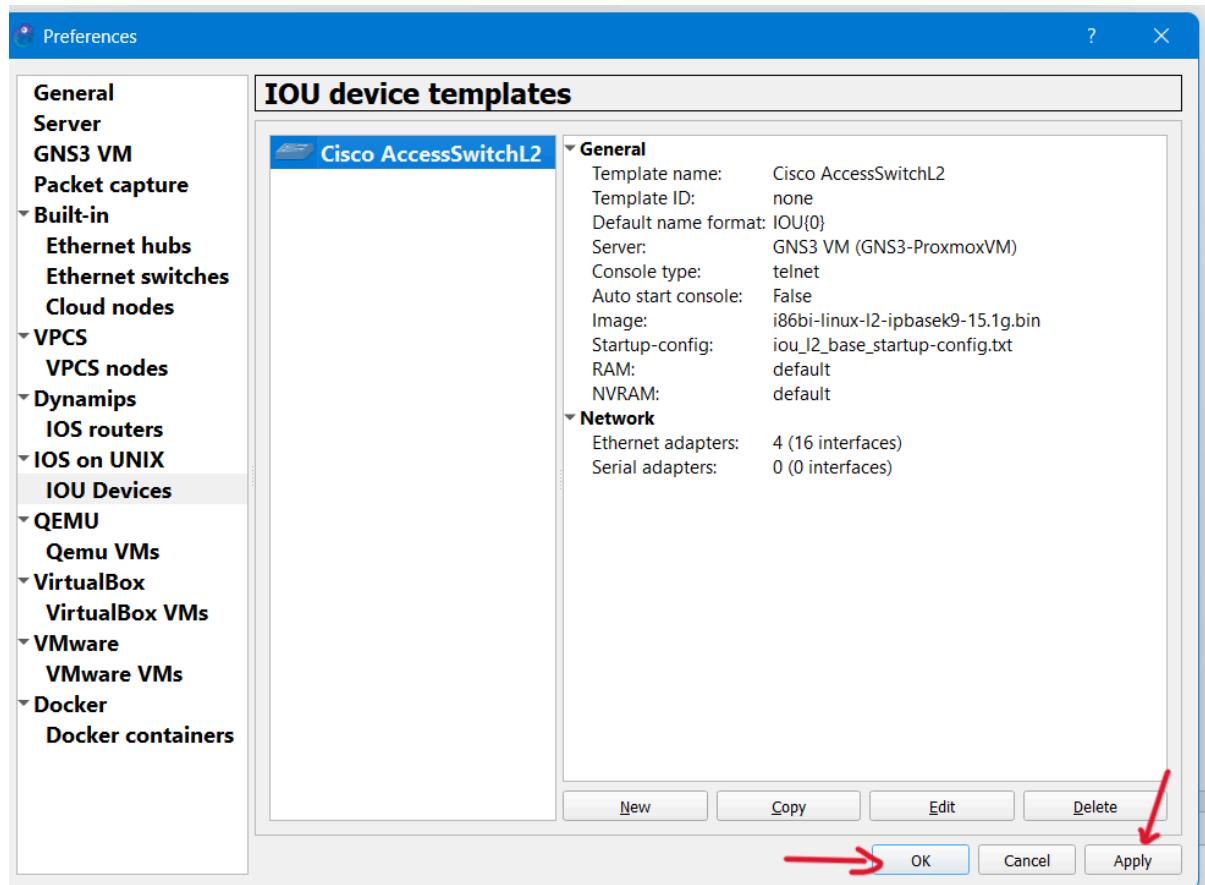
cliquer ensuite sur **NEW** sélectionner “RUN this IOU device on the GNS3 VM” après cliquer **next**



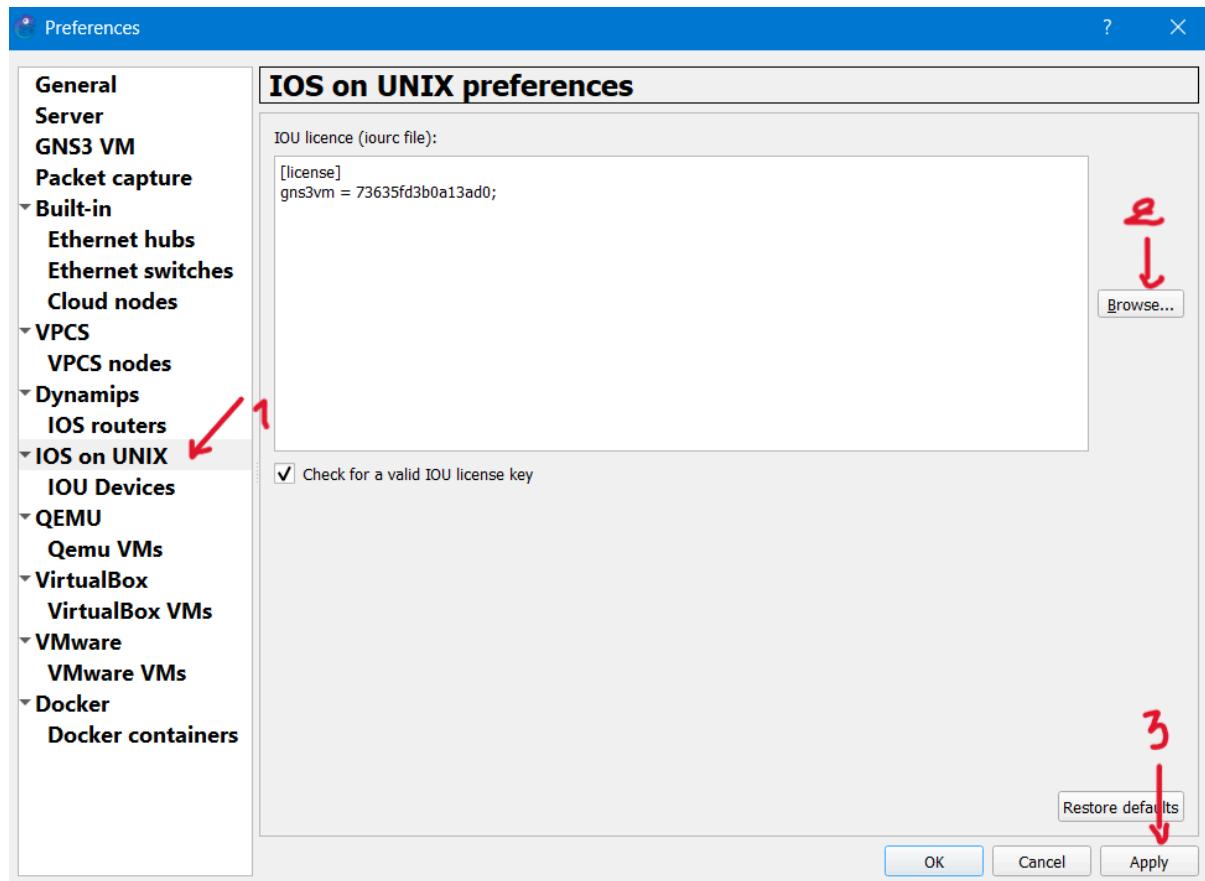
Après on nomme notre image puis sélectionner type “L2 Image” et on importe l’image de notre switch cisco qu’on a téléchargé puis on clique sur finish.



Voilà notre image est déjà ajouter sur gns3 on clique sur **apply** puis **OK**



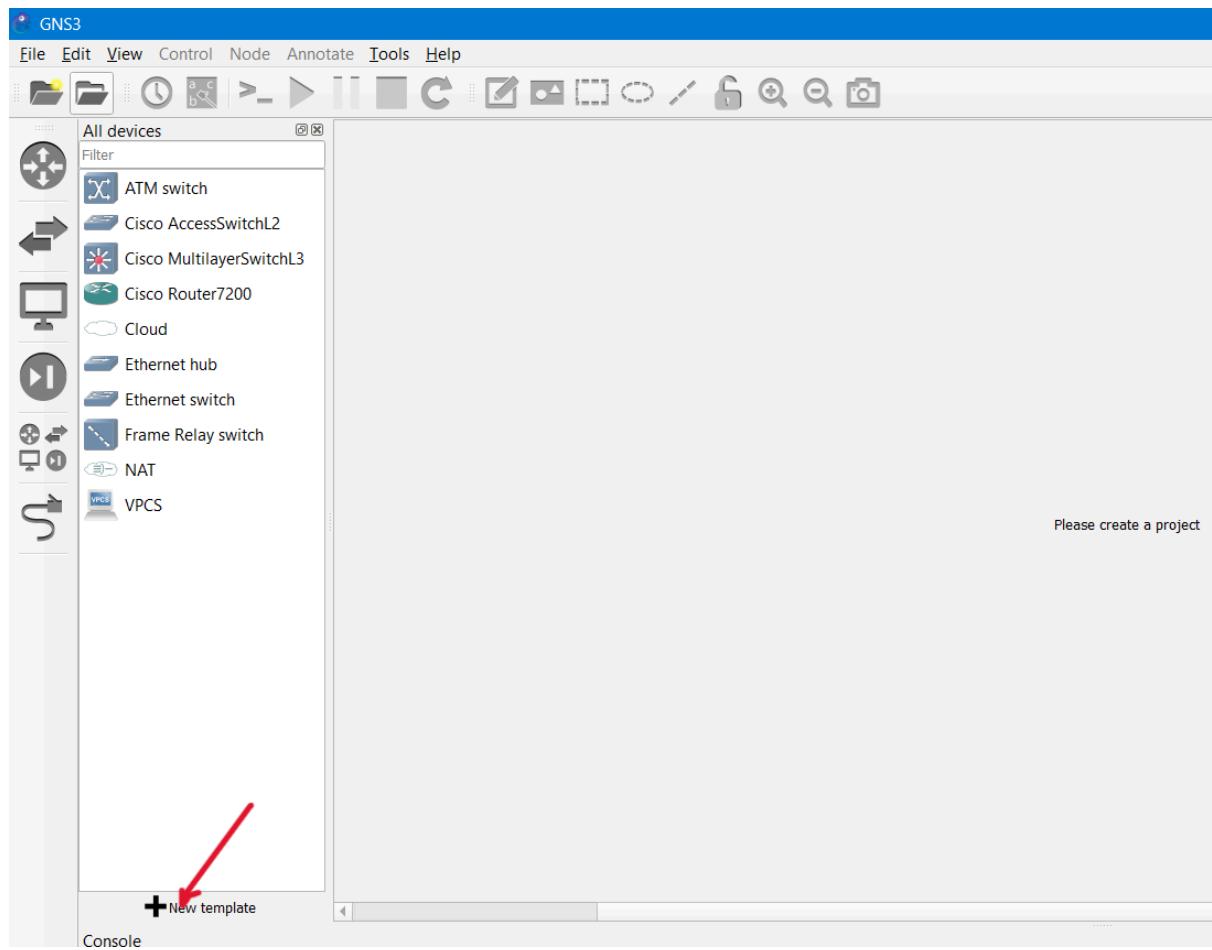
ajouter maintenant la licence fourni sinon on ne va pas pouvoir utiliser cette image,pour faire cela on clique dans **IOS on UNIX** puis on importe le fichier texte de la licence et on coche “check for...” puis **apply** et **OK**

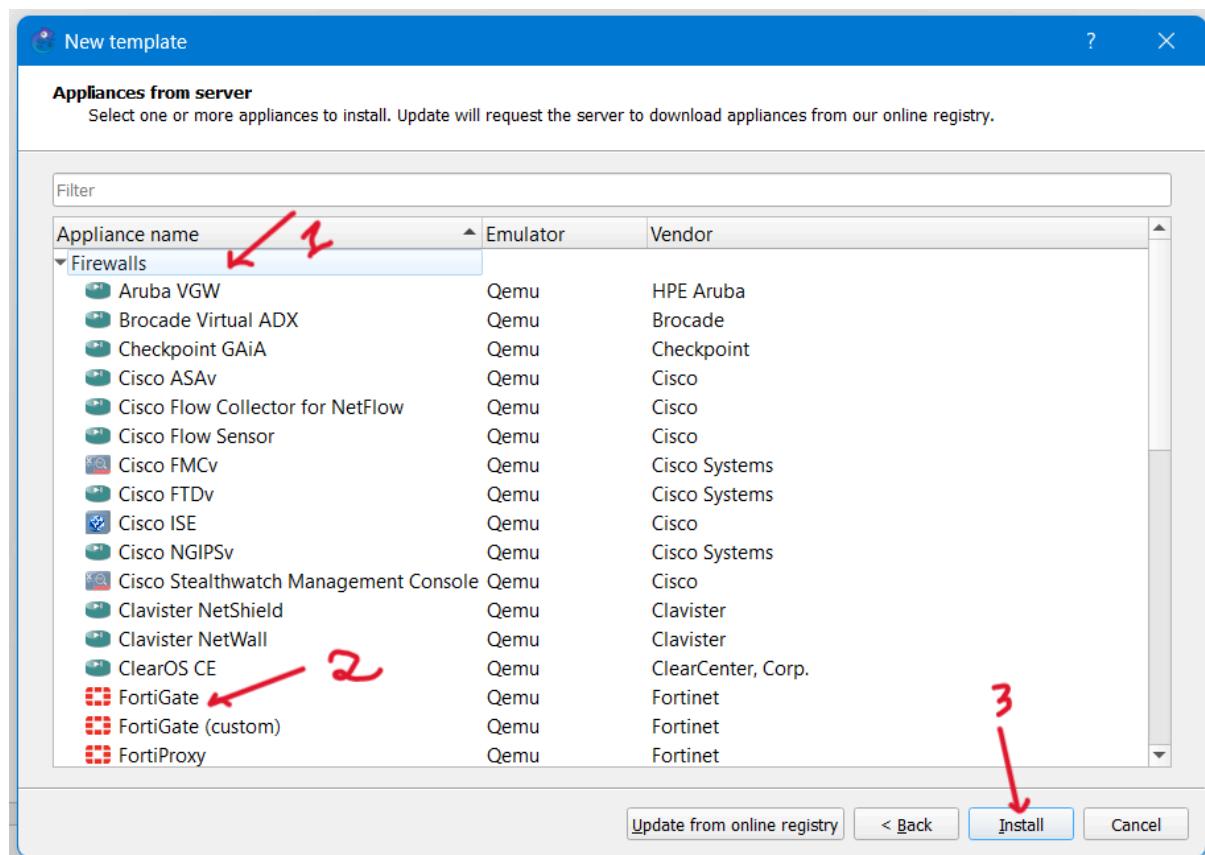
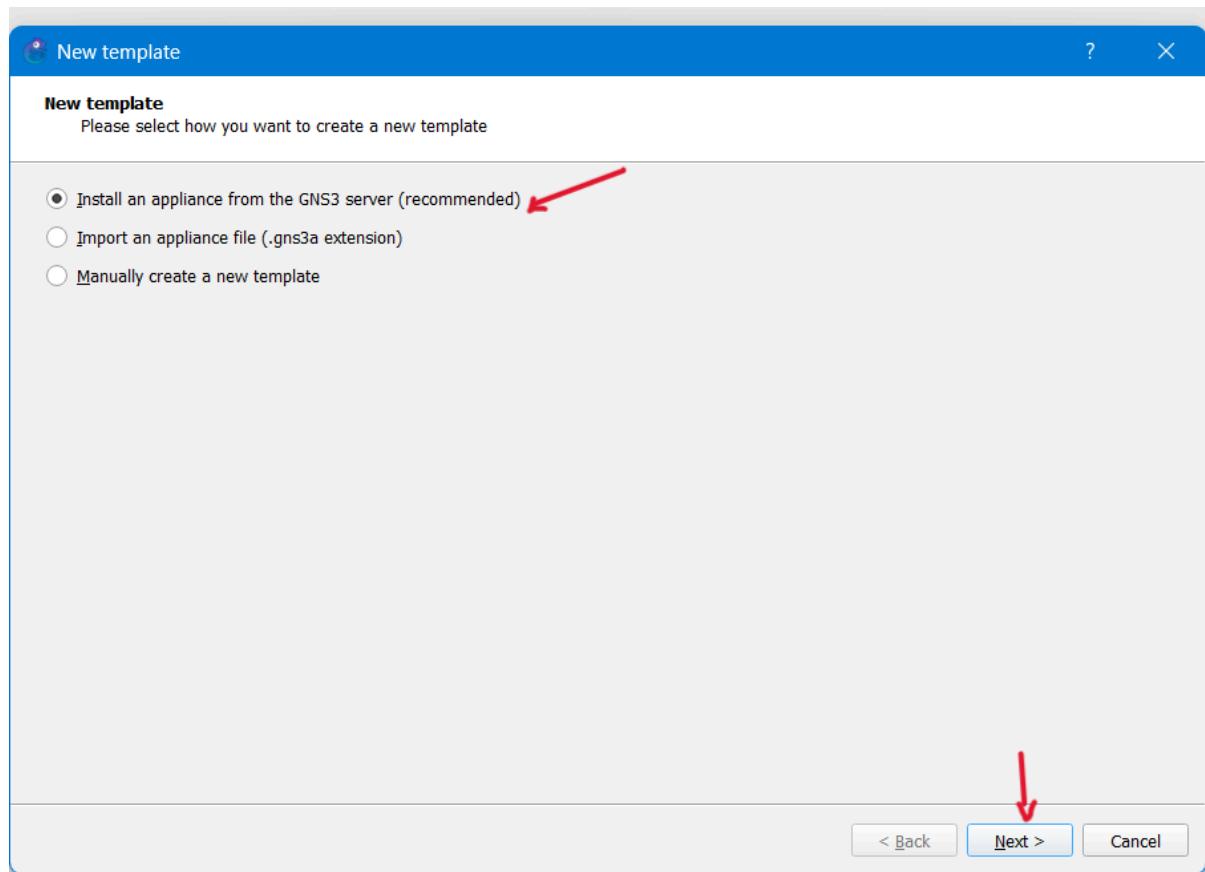


la maintenant notre switch cisco est fonctionnel prêt à être utilisé.

## 2.2 Ajout de l'image de Fortigate

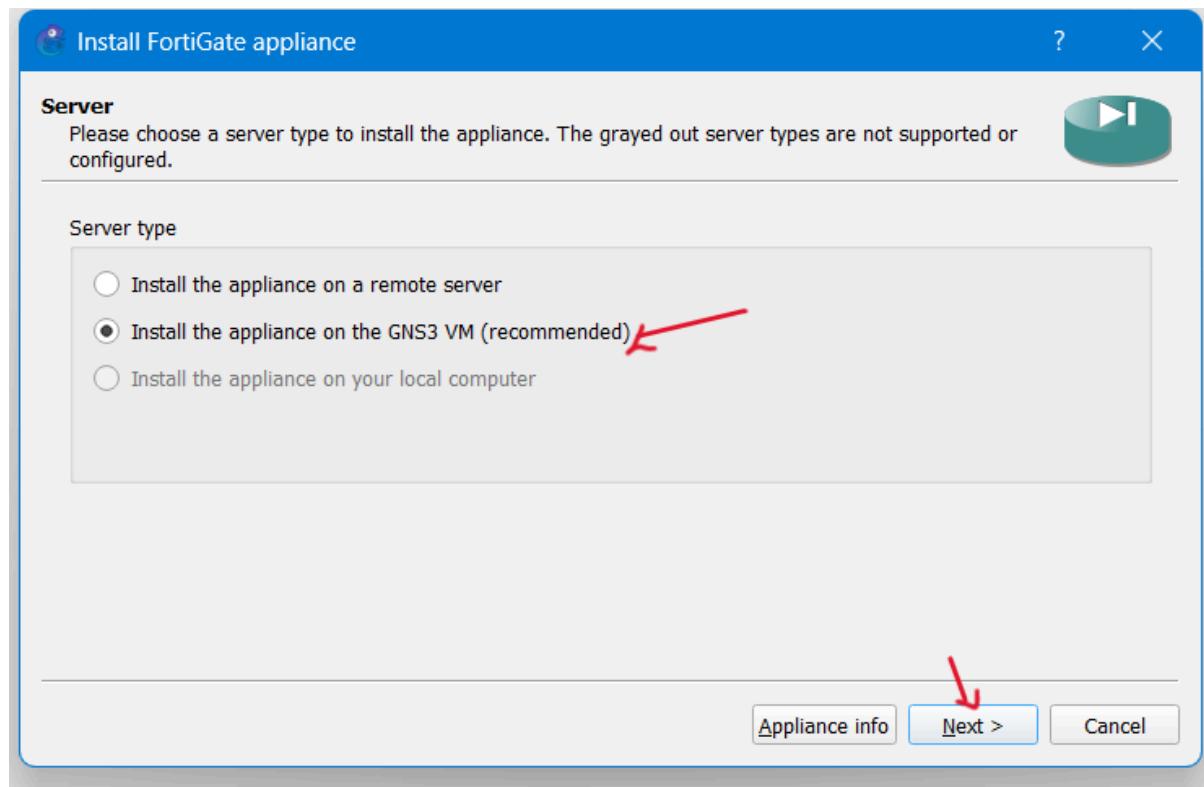
Pour ajouter FortiGate dans GNS3, sélectionner l'option "New Template" cette option dans la barre d'outils pour lancer l'assistant d'installation d'applications depuis le serveur GNS3. Choisissez "Install an appliance from the GNS3 server", puis naviguez vers **Firewalls > FortiGate** et cliquez sur Install pour télécharger le template officiel



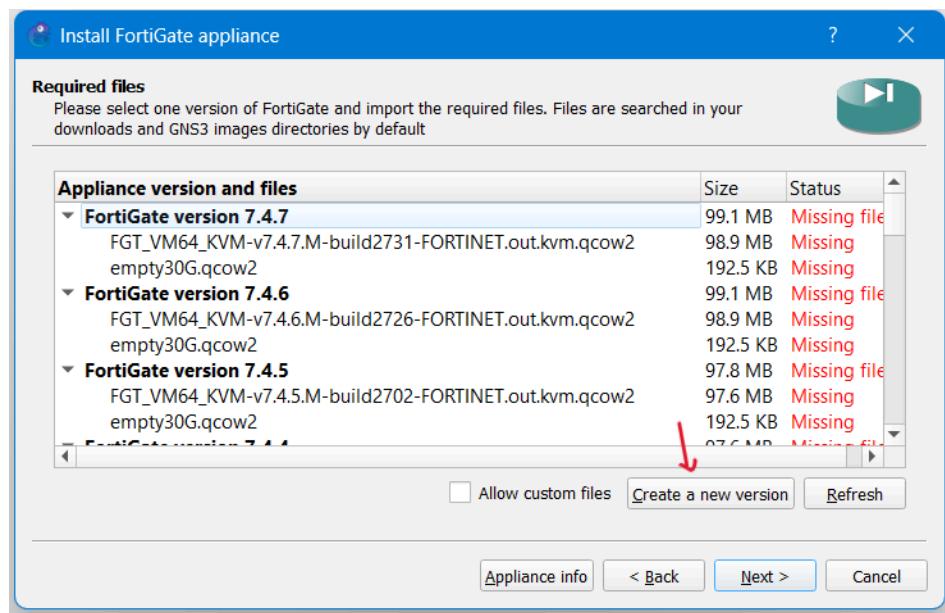


Abdourahamane AbdelWahab

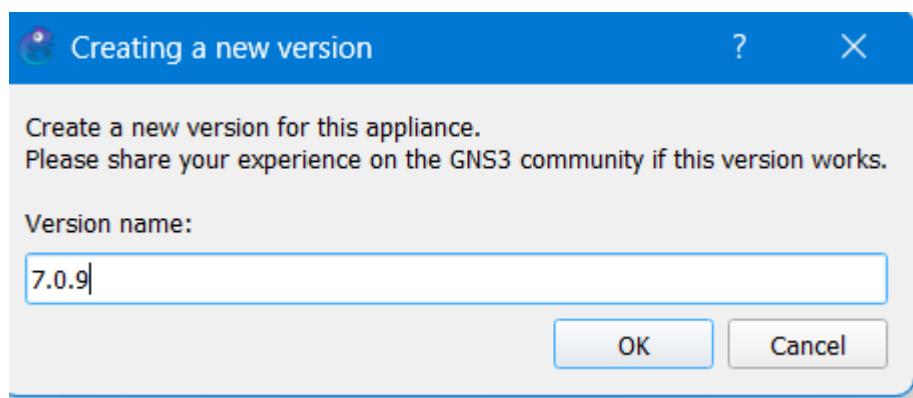
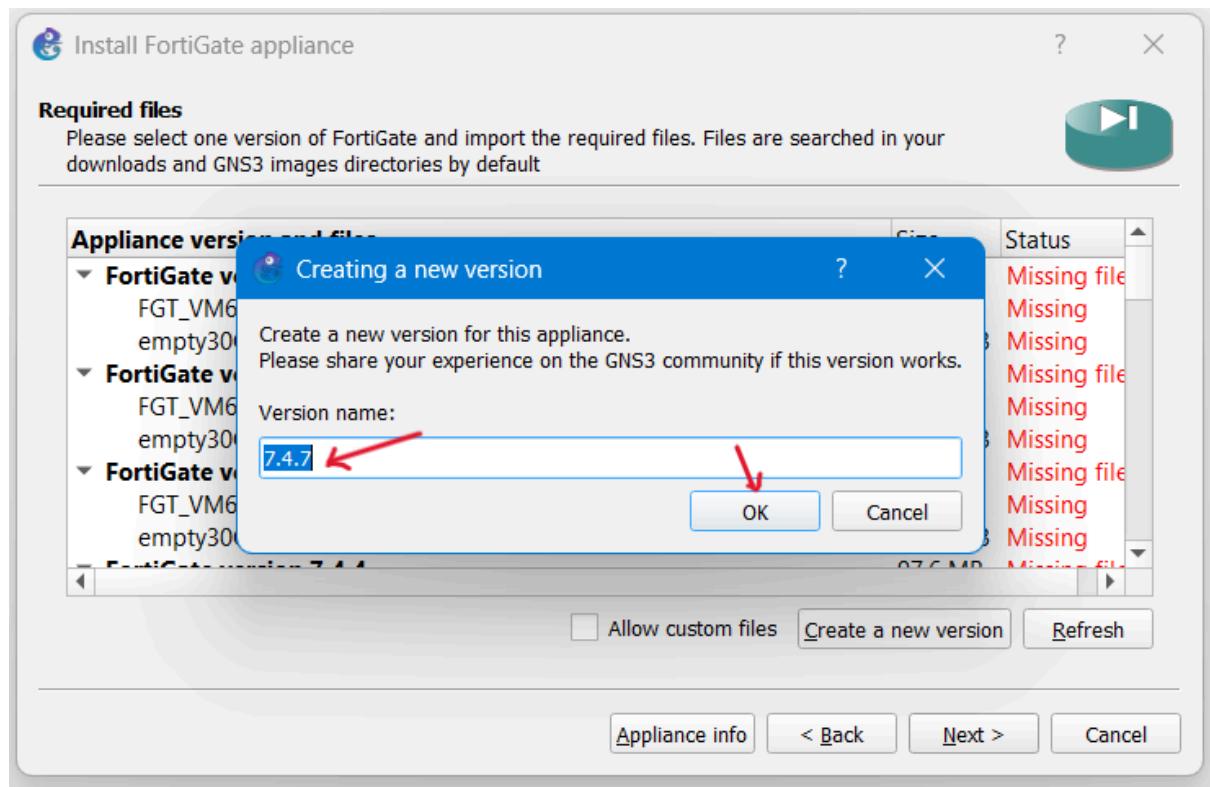
Sélectionnez ensuite "Install the appliance on the GNS3 VM(recommended)" et cliquez Next



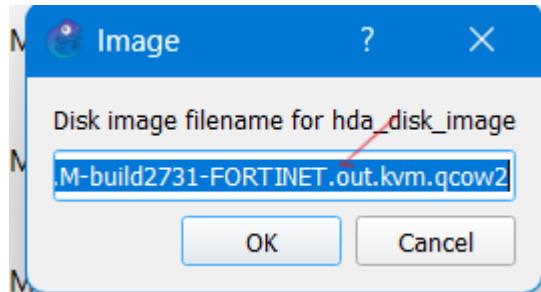
Ensuite, utilisez l'option "Create new version" lorsque la version exacte de votre image n'est pas listée dans le serveur GNS3. Cela permet d'adapter le template à votre fichier .qcow2



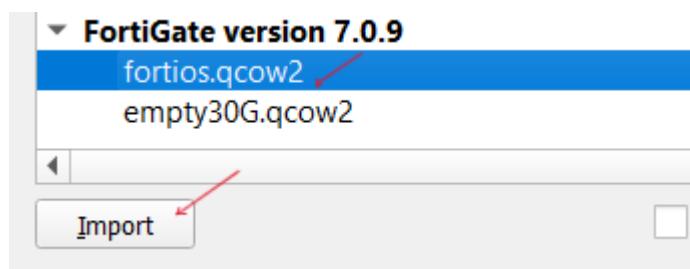
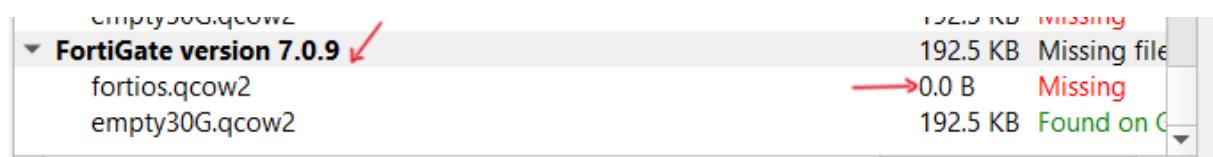
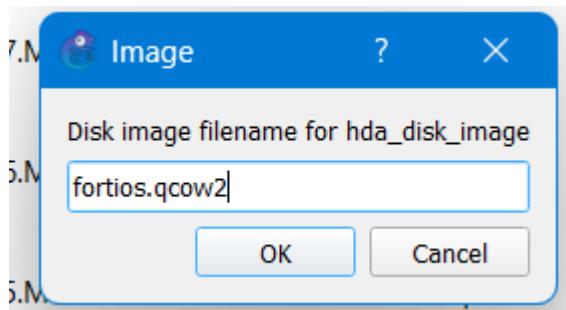
Nommez-la en indiquant la version de votre image (ex. "FortiGate-7.6.3"), confirmez OK

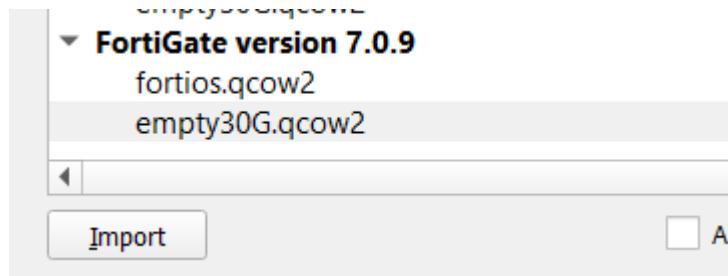


Le template affiche les fichiers requis : importez d'abord le fichier FortiGate.qcow2 (FGT\_VM64v7.6.3.qcow2 ou similaire) via "Import", puis le fichier empty30G.qcow2 sur l'autre entrée.

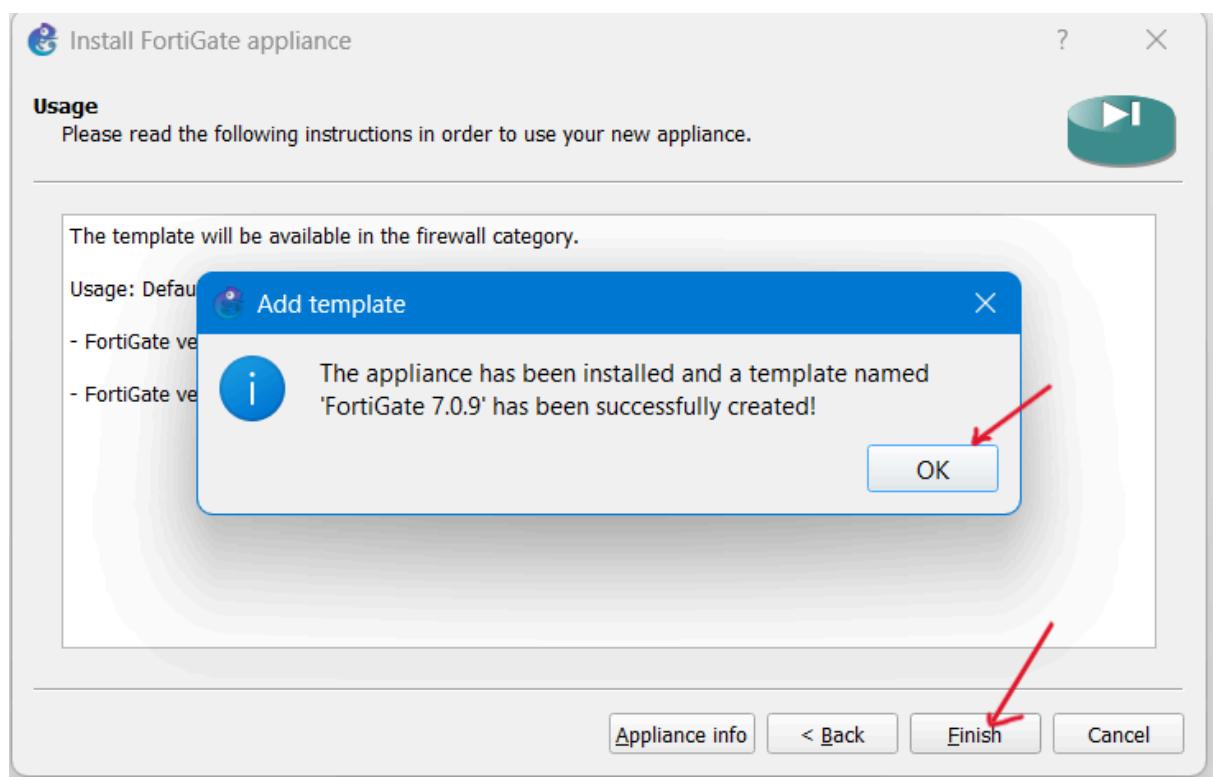
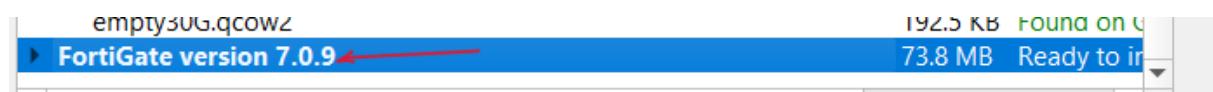


empty30G.qcow2	Fichier QCOW2	193 Ko
fortios.qcow2	Fichier QCOW2	75 328 Ko

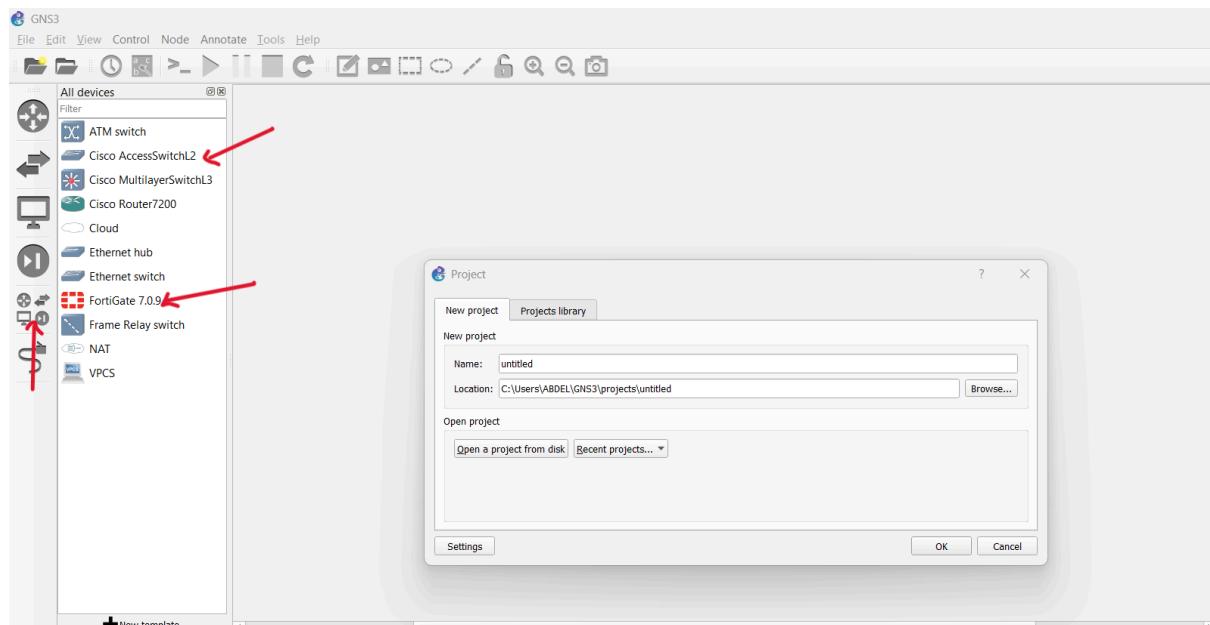




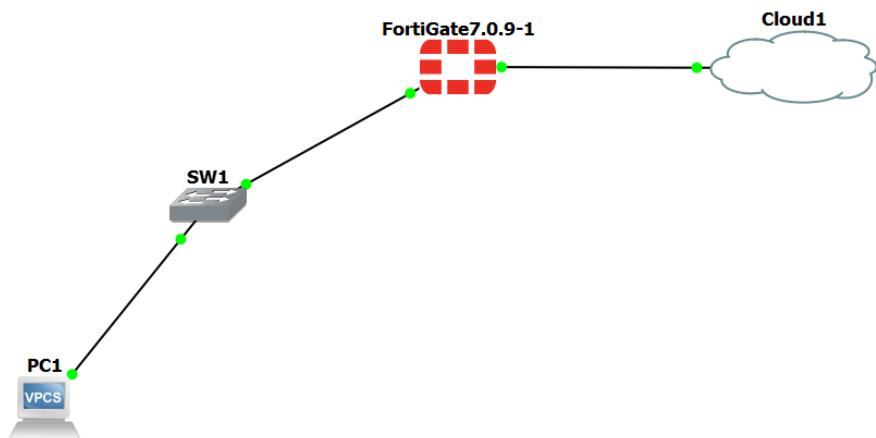
on sélectionne notre version de fortigate, on clique sur next, finish et sur OK



On a maintenant nos images importées sur GN3, on crée un nouveau projet dans l'onglet file pour tester nos images



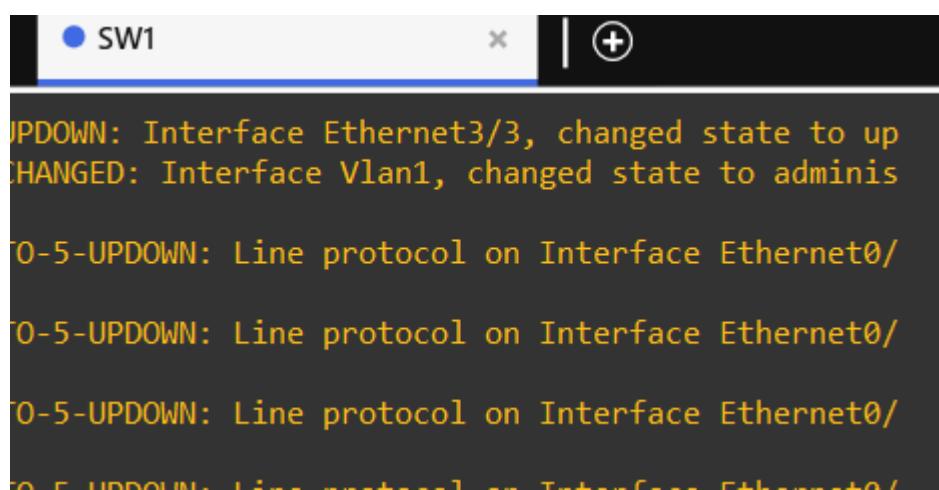
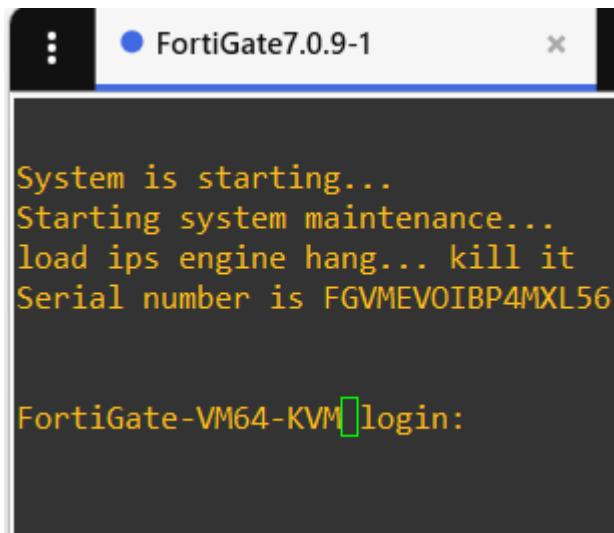
ensuite on fait un glisser déposer de nos images dans notre espace de travail GNS3



une fois les images et qu'on les relie on clique sur le bouton start



ca devrait tous être en vert, on fait clique droit sur un des images par exemple le fortigate puis on clique sur console



Voilà nos images de fonctionnement. On peut maintenant fermer ça et stopper.

## 2.3 Cas Particulier

Pour ceux comme moi qui ont installé GN3 VM sur proxmox, au moment du démarrage il y a cette erreur

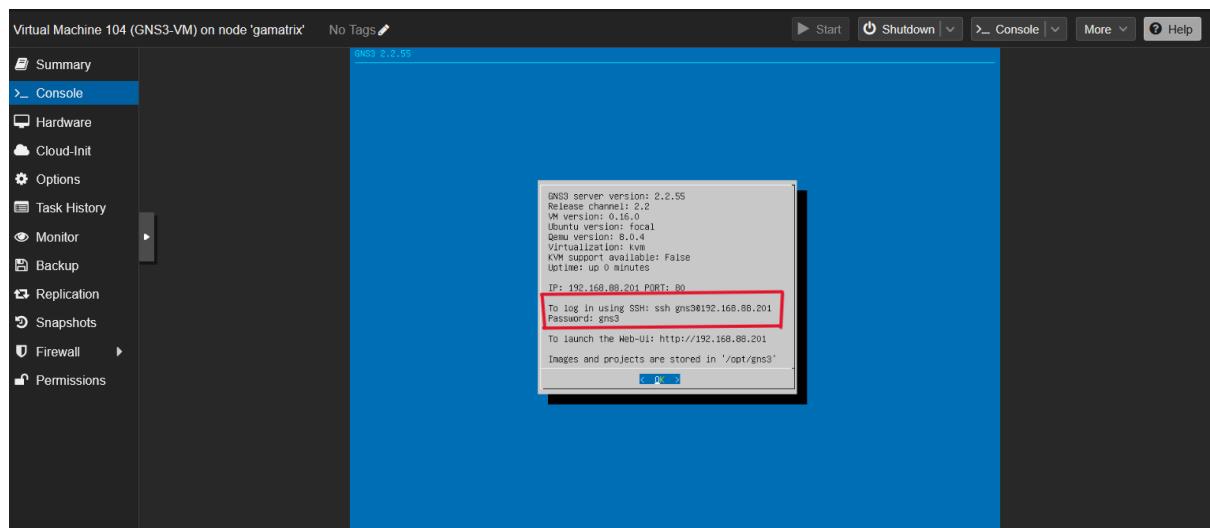
“KVM acceleration cannot be used (/dev/kvm doesn't exist). It is possible to turn off KVM support in the gns3\_server.conf by adding enable\_kvm = false to the [Qemu] section.”

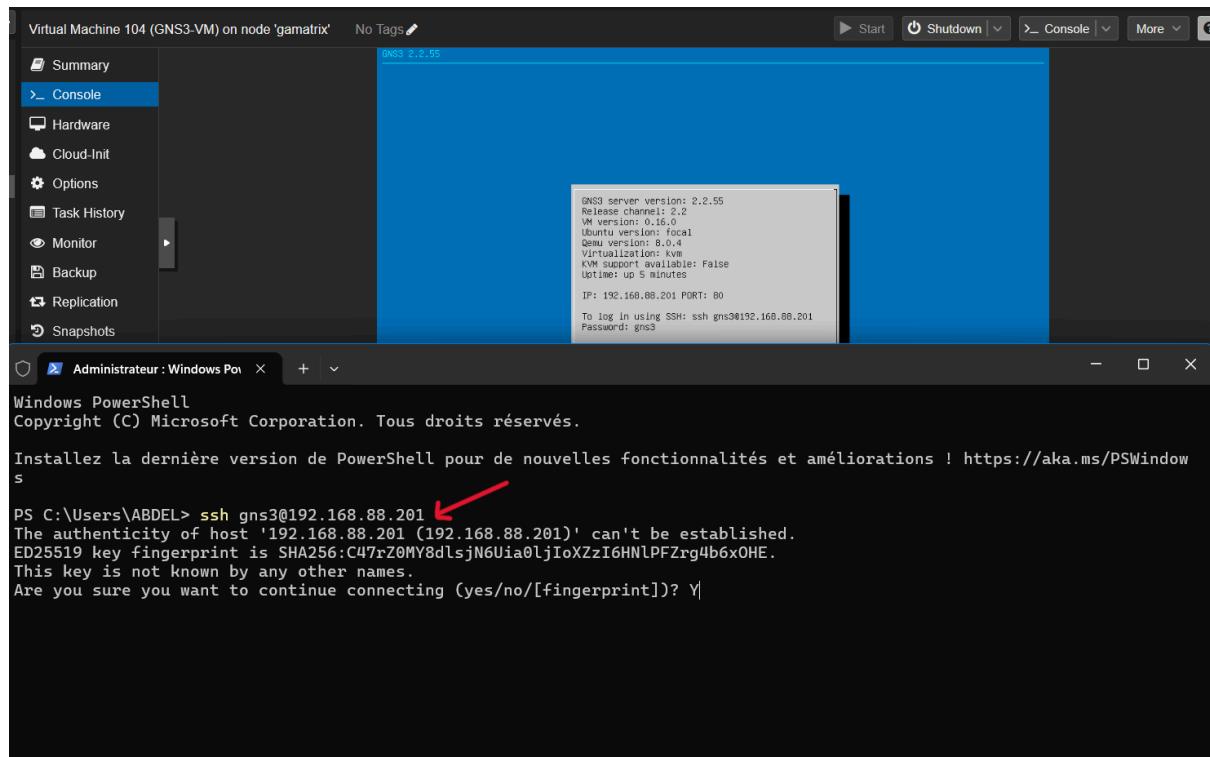
KVM acceleration cannot be used (/dev/kvm doesn't exist). It is possible to turn off KVM support in the gns3\_server.conf by adding enable\_kvm = false to the [Qemu] section.  
KVM acceleration cannot be used (/dev/kvm doesn't exist). It is possible to turn off KVM support in the gns3\_server.conf by adding enable\_kvm = false to the [Qemu] section. ↗

L'erreur indique que QEMU dans GNS3 (sur notre VM Proxmox) ne trouve pas /dev/kvm pour l'accélération KVM lors du démarrage du FortiGate.

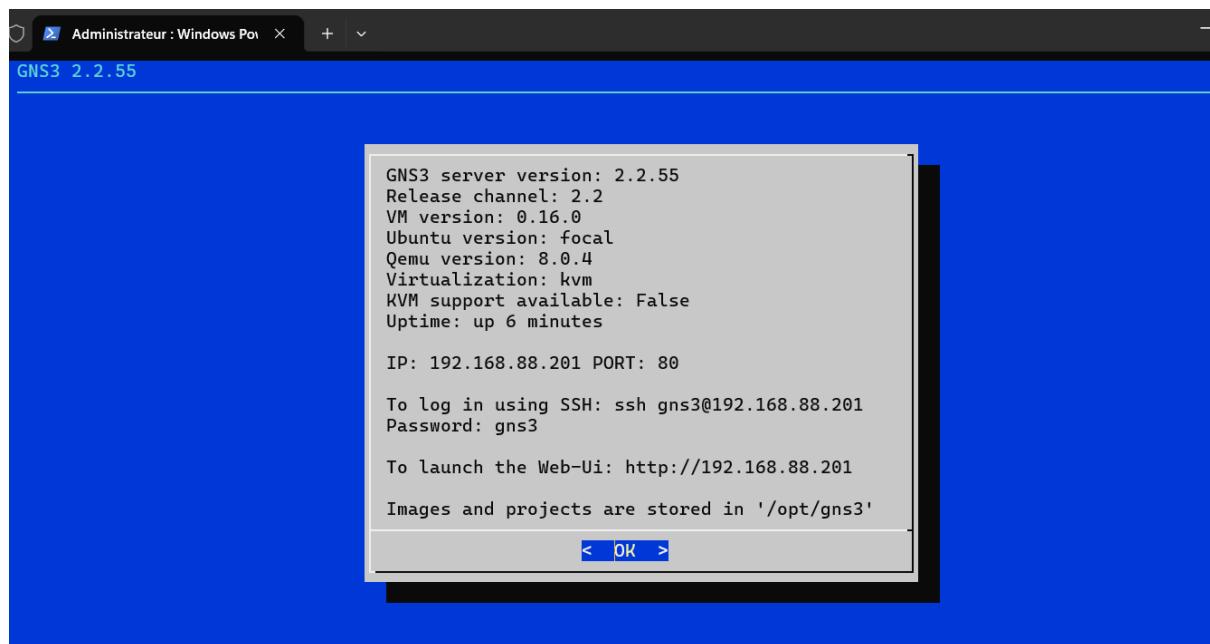
Dans ce cas de figure la solution rapide et recommandée est de désactiver KVM dans la config GNS3, car le nested KVM est complexe sur Proxmox sans ajustements CPU/host. Cela permet au FortiGate de démarrer en mode software (plus lent mais fonctionnel pour labs).

Pour réaliser cela Connectez-vous en console SSH à la VM GNS3 sur Proxmox



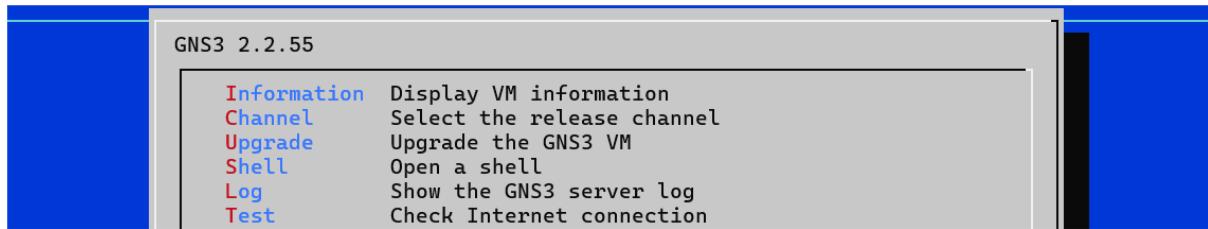


une fois connecté on clique sur OK



**Abdourahamane AbdelWahab**

Puis dans l'option Shell



pour cherchez le fichier “gns3\_server.conf” en faisant la commande  
“sudo find / -name gns3\_server.conf 2>/dev/null” ,une fois le fichier  
trouvé on fait la commande

“sudo nano /chemin/gns3\_server.conf” puis on ajouter sous la  
section :

“[Qemu]

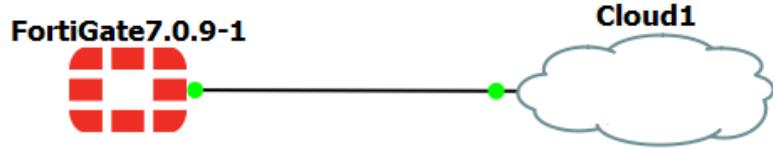
enable\_kvm = false”

A screenshot of a terminal window titled "Administrateur : Windows Pow...". The command "GNU nano 4.8" is at the top. Below it is the path "/home/gns3/.config/GNS3/2.2/gns3\_server.conf". The content of the file is displayed: [Server] host = 0.0.0.0 port = 80 images\_path = /opt/gns3/images projects\_path = /opt/gns3/projects report\_errors = True [Qemu] enable\_kvm = false. A red arrow points to the line "enable\_kvm = false".

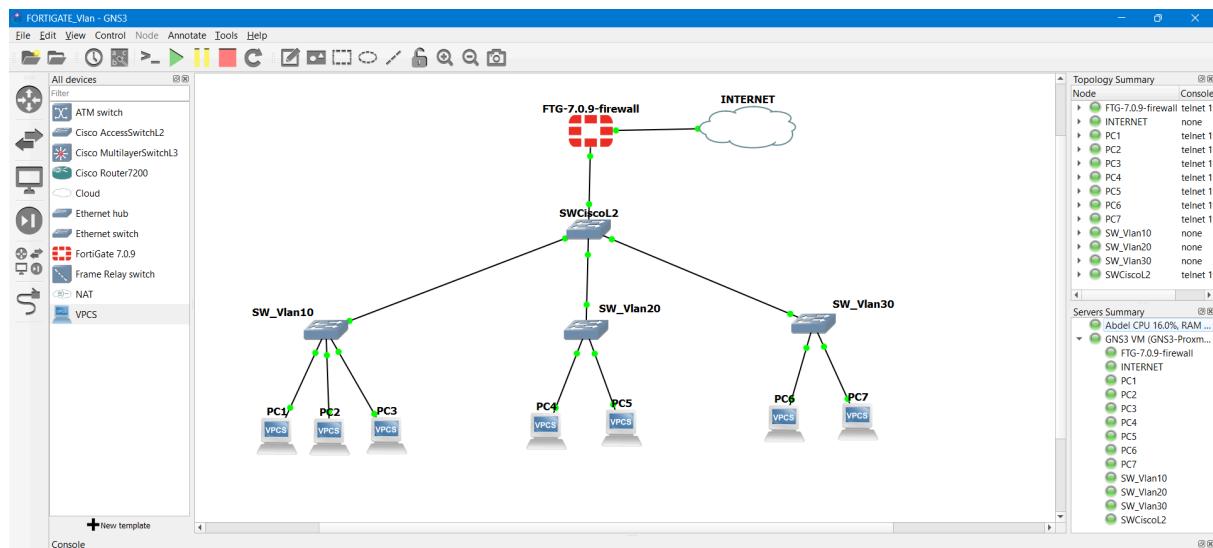
Après on enregistre et redémarrez le service

A screenshot of a terminal window titled "gns3@gns3vm: ~". The command "gns3@gns3vm:~\$ sudo systemctl restart gns3-server" is shown. A red arrow points to the end of the command line.

Une fois démarrer on refait un start de notre fortigate sur GN3 ca va démarrer sans erreur



Maintenant que tout fonctionne on peut enfin faire notre architecture présentée au début du projet pour après passer au configuration des vlans...



### **3. Configuration des VLANs**

On va tout d'abord créer nos vlans au niveau de notre fortigate ensuite les configurer au niveau de notre switch cisco

#### **3.1 Création des VLANs sur Fortigate**

Tout d'abord on va accéder à notre fortigate avec la console GNS3 une fois sur la console pour se connecter :

**user : admin**

**Password :**

dans password on met rien juste on tape sur entrer après on va nous demander de configurer un nouveau password, apres ca on se connecte avec nos nouveau identifiant :

**user: admin**

**password: votre nouveau mot de passe**

Une fois connecté on fait cette commande

“config system interface” après on fait “edit ?” ça va afficher les interfaces, on pourra ensuite récupérer l’ip de notre fortigate pour se connecter via navigateur.

```

Starting system maintenance...
Load ips engine hang... kill it
Serial number is FGWMEVNF8Q08KMF4

Disk usage changed, please wait for reboot...

Formatting the disk...
unmounting /data2 : ok
Partitioning and formatting /dev/vdb label LOGUSEDX90EC920F ... done

The system is going down NOW !!
Please stand by while rebooting the system.
Restarting system.

System is starting...
load ips engine hang... kill it
Serial number is FGWMEVNF8Q08KMF4

FortiGate-VN64-KVM login: admin
Password: [REDACTED]
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

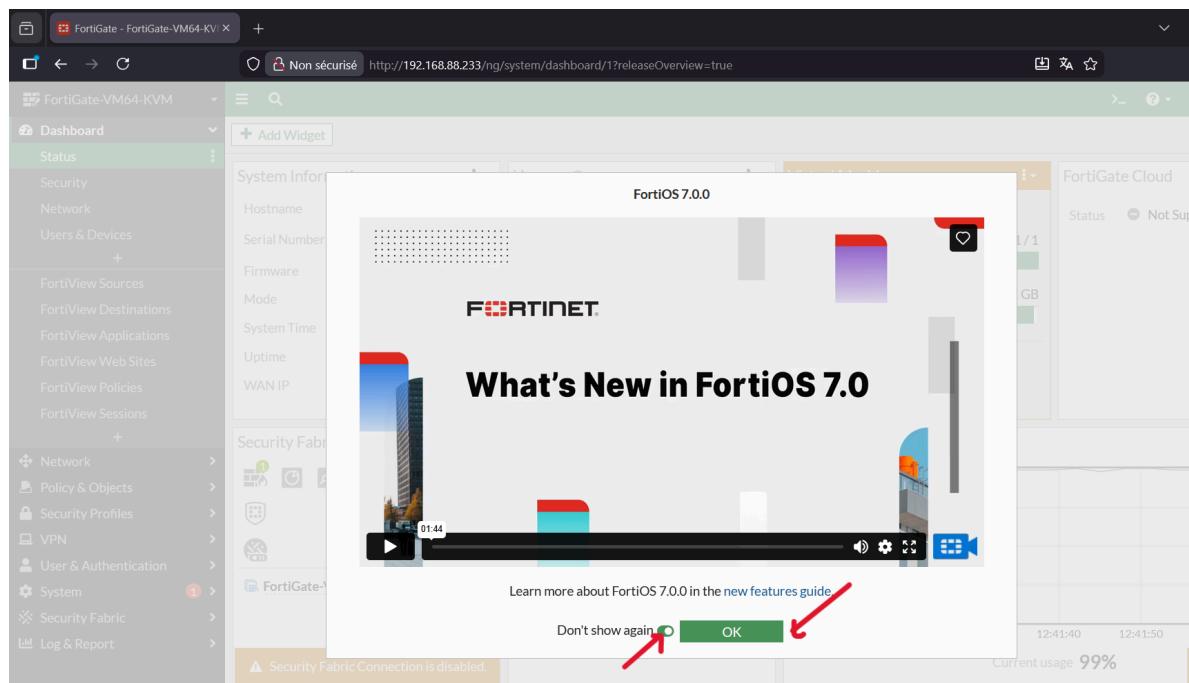
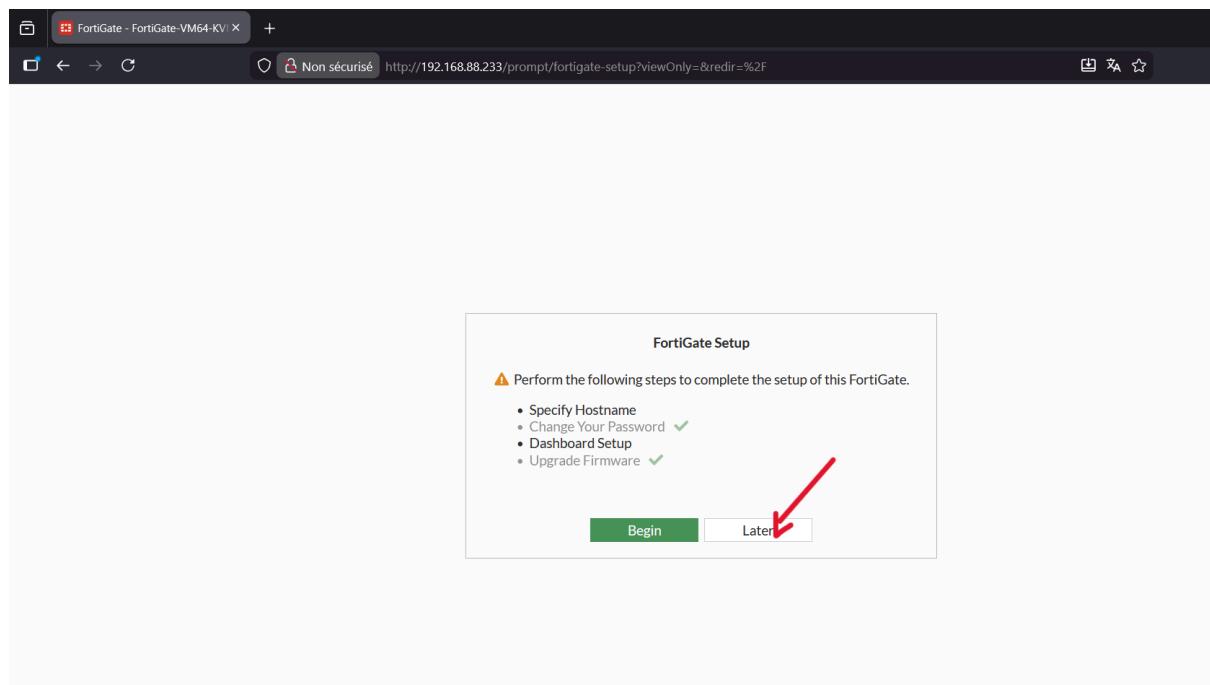
FortiGate-VN64-KVM # config system interface
FortiGate-VN64-KVM (interface) # edit
name Name.
fortilink static 0.0.0.0 0.0.0.0 10.255.1.1 255.255.255.0 up disable aggregate
l2t.root static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable tunnel
naf.root static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable tunnel
port1 dhcp 0.0.0.0 0.0.0.0 192.168.89.2 255.255.255.0 up disable physical
port2 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port3 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port4 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port5 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port6 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port7 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port8 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port9 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
port10 static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical
ssl.root static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable tunnel

```

on tape ensuite l'ip sur notre navigateur, on sera dans la page de connexion de notre fortigate, on met nos identifiant ca va nous rediriger sur la page d'accueil du fortigate.



admin
*****



**Abdourahamane AbdelWahab**

The screenshot shows the FortiGate management interface. The left sidebar is open, showing various navigation options under 'FortiGate-VM64-KVM'. A red arrow points to the 'Network' option. The main dashboard area contains several cards: 'System Information' (Hostname: FortiGate-VM64-KVM, Serial Number: FGVMEVNF8Q08KMF4, Firmware: v7.0.9 build0444 (Mature), Mode: NAT, System Time: 2026/01/05 12:42:47, Uptime: 00:00:06:25, WAN IP: Unknown), 'Licenses' (FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering), 'Virtual Machine' (FGVMEV License, Allocated vCPUs: 1/1, Allocated RAM: 2 GB / 2 GB, Auto Scaling: 100%), 'FortiGate Cloud' (Status: Not Supported), 'Security Fabric' (Icon showing 1 connection, FortiGate-VM64-KVM listed), 'Administrators' (Console: 1, HTTP: 2, FortiExplorer: 0, admin: super\_admin), and performance graphs for 'CPU' (1 minute average at 100%, current usage 100%, high CPU usage) and 'Memory' (100% usage). A message at the bottom left says 'Unable to connect to FortiGuard servers.'

Une fois dans la page d'accueil on va dans **Network > Interfaces > Create New > Interface**

The screenshot shows the 'Interfaces' list in the FortiGate management interface. A red arrow points to the 'Interfaces' option in the left sidebar. Another red arrow points to the 'Create New' button in the top toolbar. The list displays two main categories: '802.3ad Aggregate' and 'Physical Interface'. Under '802.3ad Aggregate', there is one entry for 'fortilink'. Under 'Physical Interface', there are nine entries labeled 'port1' through 'port9'. Each entry includes columns for Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, DHCP Ranges, and Ref. The 'Administrative Access' column for port1 shows 'PING', 'HTTPS', 'SSH', 'HTTP', and 'FMG Access'.

pour configurer nos vlans avec les paramètres suivant :

Name : administration.

Aliase: VLAN\_ADMIN

Type : VLAN.

Interface : port2 (connecter au switch).

VLAN ID : 10.

Role : LAN.

IP/Netmask : 192.168.10.1/24

The screenshot shows the FortiGate interface configuration page. The left sidebar is collapsed. The main area displays the 'New Interface' configuration form. The fields are as follows:

- Name: Administratif (highlighted by a red arrow)
- Alias: VLAN\_ADMIN (highlighted by a red arrow)
- Type: VLAN (highlighted by a red arrow)
- VLAN protocol: 802.1Q (highlighted by a red arrow)
- Interface: port2 (highlighted by a red arrow)
- VLAN ID: 10 (highlighted by a red arrow)
- VRF ID: 0
- Role: LAN

Below the form, under the 'Address' section, the 'Addressing mode' dropdown is set to 'Man.' (highlighted by a red arrow). The 'IP/Netmask' field contains '192.168.10.1/24' (highlighted by a red arrow). A note below says 'Create address object matching subnet'. Under 'Administrative Access', several checkboxes are checked: PING, SNMP, and Security Fabric Connection. Other options like HTTPS, SSH, RADIUS Accounting, and various FTM and Speed Test checkboxes are available but unchecked.

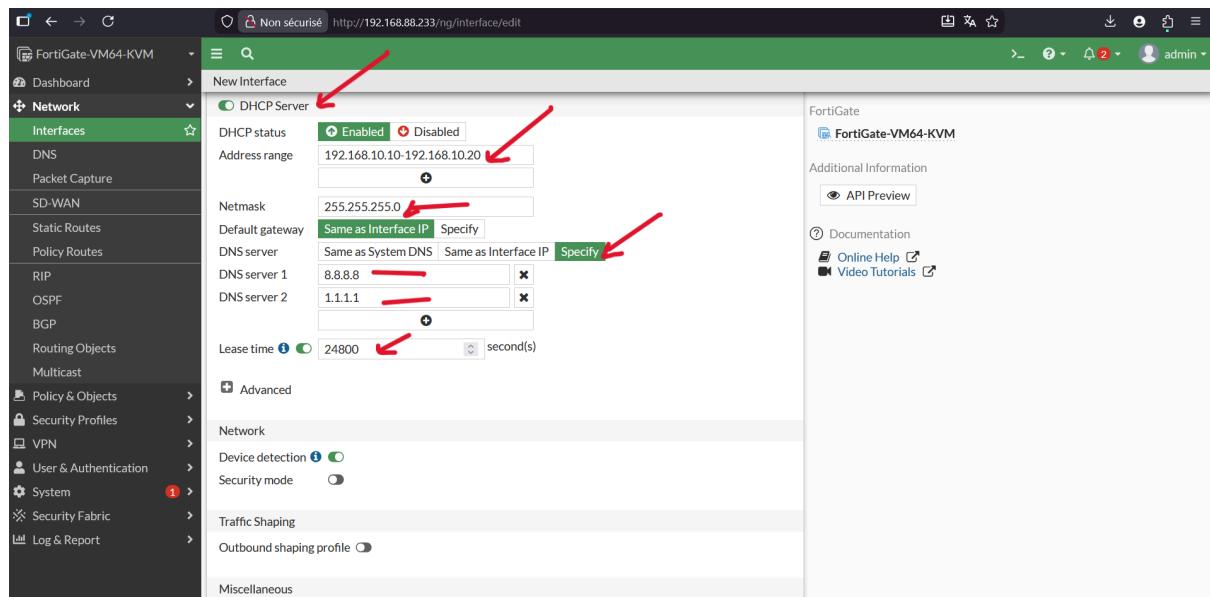
## Active DHCP Server (Enable)

Address Range : 192.168.10.10 - 192.168.10.20(ajuste selon vos besoins)

Default Gateway : (on laisse par défaut)

DNS Server : 8.8.8.8

puis on clique sur OK



Et on fait le même procédure avec les autres VLANs

Physical Interface 13					
	port1	Physical Interface		192.168.88.233/255.255.255.0	PING HTTPS SSH <b>HTTP</b> FMG-Access
	port2	Physical Interface		0.0.0.0/0.0.0	
•	VLAN_ADMIN (Administratif)	VLAN		192.168.10.1/255.255.255.0	PING SNMP
•	VLAN_GUEST (Invités)	VLAN		192.168.30.1/255.255.255.0	PING SNMP
•	VLAN_TECH (Technique)	VLAN		192.168.20.1/255.255.255.0	PING SNMP
	port3	Physical Interface		0.0.0.0/0.0.0	
	port4	Physical Interface		0.0.0.0/0.0.0	

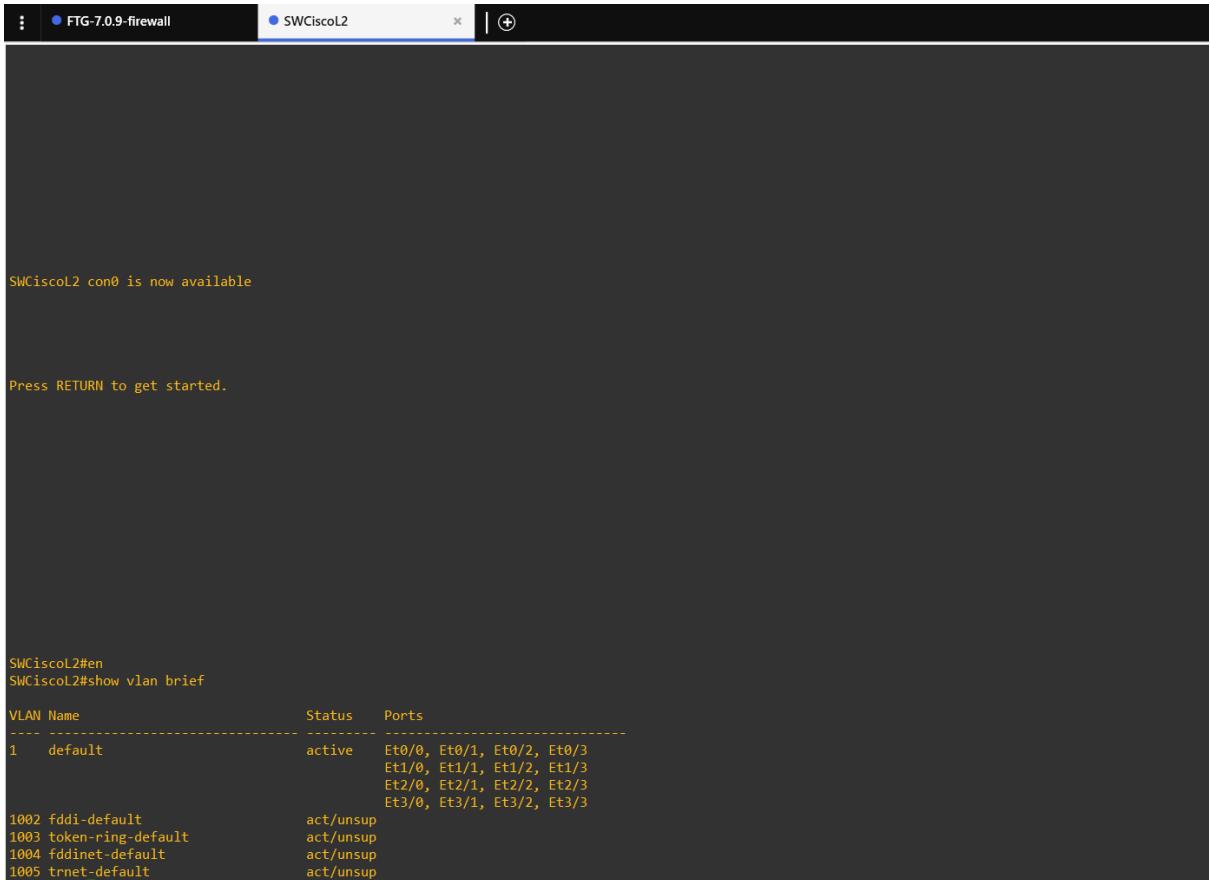
Maintenant on peut passer à la création et la configuration des VLANs au niveau de notre switch cisco

## 3.2 Crédation et Configuration des VLAN sur le Switch Cisco L2

On se connecte au switch via le console de GN3 comme on la fait avec le fortigate puis une fois sur l'interface on fait les configuration en suivant ses étapes :

- Créer les VLANs

d'abord on fait la commande "show vlan brief" ca va nous montrer les vlan présent sur notre switch pour l'instant ca sera juste les vlan par défaut



The screenshot shows a terminal window titled 'SWCiscoL2'. The window displays the output of the 'show vlan brief' command. The output includes a header and five entries for VLANs 1, 1002, 1003, 1004, and 1005, detailing their names, status, and associated ports.

VLAN Name	Status	Ports
1 default	active	Et0/0, Et0/1, Et0/2, Et0/3 Et1/0, Et1/1, Et1/2, Et1/3 Et2/0, Et2/1, Et2/2, Et2/3 Et3/0, Et3/1, Et3/2, Et3/3
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

ensuite on entre en mode configuration avec la commande "configure terminal" ou "conf t" pour créer nos nouvelles vlan

```
enable
configure terminal
vlan 10
name VLAN_ADMIN
exit
vlan 20
name VLAN_TECH
exit
vlan 30
name VLAN_GUEST
exit
```

```

SWCiscoL2 con0 is now available

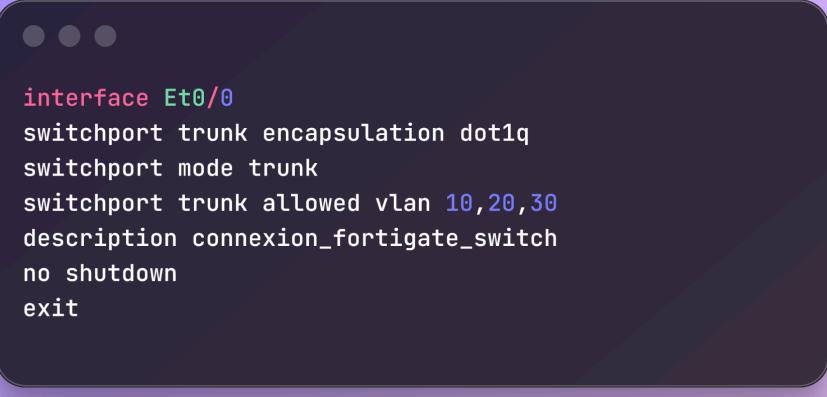
Press RETURN to get started.

SWCiscoL2#en
SWCiscoL2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWCiscoL2(config)#vlan 10
SWCiscoL2(config-vlan)#name ADMIN
SWCiscoL2(config-vlan)#vlan 20
SWCiscoL2(config-vlan)#name TECH
SWCiscoL2(config-vlan)#vlan 30
SWCiscoL2(config-vlan)#name GUEST
SWCiscoL2(config-vlan)#exit
SWCiscoL2(config)#exit
SWCiscoL2#
*Jan  5 20:56:40.499: %SYS-5-CONFIG_I: Configured from console by console
SWCiscoL2#show vlan brief
VLAN Name          Status    Ports
---- -----
1   default        active    Et0/0, Et0/1, Et0/2, Et0/3
                           Et1/0, Et1/1, Et1/2, Et1/3
                           Et2/0, Et2/1, Et2/2, Et2/3
                           Et3/0, Et3/1, Et3/2, Et3/3
10  ADMIN          active
20  TECH           active
30  GUEST          active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
SWCiscoL2#]

```

On va ensuite Configurer l'interface de notre switch relier vers FortiGate(Et0/0) en mode trunk pour faire passer les vlans

- Configurer l'interface(Et0/0) en mode trunk vers FortiGate



```

interface Et0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
description connexion_fortigate_switch
no shutdown
exit

```

```

SWCiscoL2#show interfaces status
Port      Name          Status     Vlan      Duplex   Speed Type
Et0/0      connected    1          auto      auto unknown
Et0/1      connected    1          auto      auto unknown
Et0/2      connected    1          auto      auto unknown
Et0/3      connected    1          auto      auto unknown
Et1/0      connected    1          auto      auto unknown
Et1/1      connected    1          auto      auto unknown
Et1/2      connected    1          auto      auto unknown
Et1/3      connected    1          auto      auto unknown
Et2/0      connected    1          auto      auto unknown
Et2/1      connected    1          auto      auto unknown
Et2/2      connected    1          auto      auto unknown
Et2/3      connected    1          auto      auto unknown
Et3/0      connected    1          auto      auto unknown
Et3/1      connected    1          auto      auto unknown
Et3/2      connected    1          auto      auto unknown
Et3/3      connected    1          auto      auto unknown
SWCiscoL2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWCiscoL2(config)#interface Et0/0
SWCiscoL2(config-if)#switchport trunk encapsulation dot1q
SWCiscoL2(config-if)#switchport trunk encapsulation dot1q
*Jan 5 21:06:11.934: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
SWCiscoL2(config-if)#switchport trunk encapsul
*Jan 5 21:06:14.938: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
SWCiscoL2(config-if)#switchport mode trunk
SWCiscoL2(config-if)#switchport mode trunk
*Jan 5 21:06:36.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
SWCiscoL2(config-if)#switchport mode trunk
*Jan 5 21:06:39.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
SWCiscoL2(config-if)#switchport trunk allowed vlan 10,20,30
SWCiscoL2(config-if)#description connexion_fortigate_switch
SWCiscoL2(config-if)#exit
SWCiscoL2(config)#exit
SWCiscoL2#
*Jan 5 21:08:24.493: %SYS-5-CONFIG_I: Configured from console by console
SWCiscoL2#

```

```

SWCiscoL2#show interface trunk
Port      Mode          Encapsulation  Status       Native vlan
Et0/0      on           802.1q        trunking    1

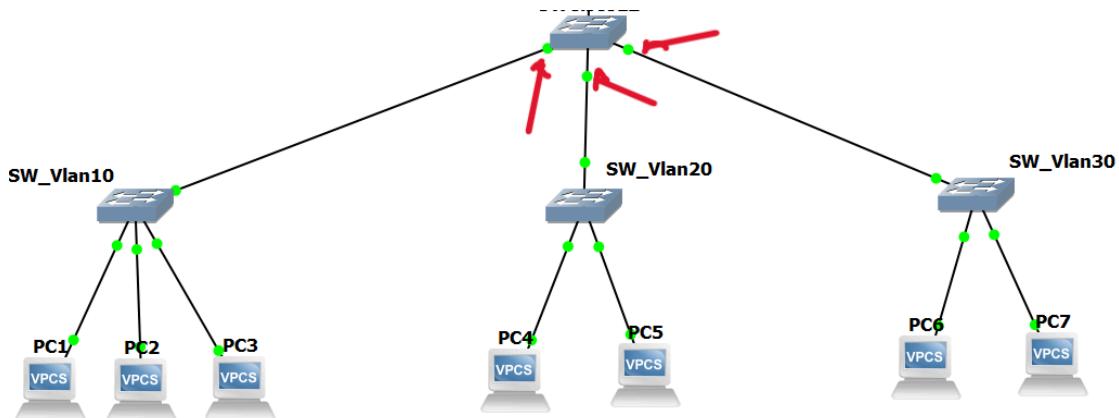
Port      Vlans allowed on trunk
Et0/0      10,20,30

Port      Vlans allowed and active in management domain
Et0/0      10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0      10,20,30

```

- Configurer les interfaces du cisco qui ramène aux switch GNS3 en mode access



```

interface Et0/1
switchport mode access
switchport access vlan 10
spanning-tree portfast
no shutdown
exit
interface Et0/2
switchport mode access
switchport access vlan 20
spanning-tree portfast
no shutdown
exit
interface Et0/3
switchport mode access
switchport access vlan 30
spanning-tree portfast
no shutdown
exit

```

```

SWCiscoL2#en
SWCiscoL2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWCiscoL2(config)#interface Et0/1
SWCiscoL2(config-if)#switchport mode access
SWCiscoL2(config-if)#switchport access vlan 10
SWCiscoL2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/1 but will only
have effect when the interface is in a non-trunking mode.
SWCiscoL2(config-if)#exit
SWCiscoL2(config)#interface Et0/2
SWCiscoL2(config-if)#switchport mode access
SWCiscoL2(config-if)#switchport access vlan 20
SWCiscoL2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/2 but will only
have effect when the interface is in a non-trunking mode.
SWCiscoL2(config-if)#exit
SWCiscoL2(config)#interface Et0/3
SWCiscoL2(config-if)#switchport mode access
SWCiscoL2(config-if)#switchport access vlan 30
SWCiscoL2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on Ethernet0/3 but will only
have effect when the interface is in a non-trunking mode.
SWCiscoL2(config-if)#exit
SWCiscoL2(config)#exit
SWCiscoL2#
*Jan 5 21:15:17.610: %SYS-5-CONFIG_I: Configured from console by console
SWCiscoL2#
```

```

SWCiscoL2#show vlan brief

VLAN Name                               Status    Ports
----- -----
1      default                            active    Et1/0, Et1/1, Et1/2, Et1/3
                                         Et2/0, Et2/1, Et2/2, Et2/3
                                         Et3/0, Et3/1, Et3/2, Et3/3
10     ADMIN                             active    Et0/1
20     TECH                             active    Et0/2
30     GUEST                            active    Et0/3
1002   fddi-default                     act/unsup
1003   token-ring-default               act/unsup
1004   fddinet-default                 act/unsup
1005   trnet-default                   act/unsup
SWCiscoL2#show interfaces status

Port      Name          Status      Vlan      Duplex  Speed Type
Et0/0    connexion_fortigat  connected  trunk    auto    auto unknown
Et0/1                connected  10       auto    auto unknown
Et0/2                connected  20       auto    auto unknown
Et0/3                connected  30       auto    auto unknown
Et1/0    connected      connected  1        auto    auto unknown
Et1/1    connected      connected  1        auto    auto unknown
Et1/2    connected      connected  1        auto    auto unknown
Et1/3    connected      connected  1        auto    auto unknown
Et2/0    connected      connected  1        auto    auto unknown
Et2/1    connected      connected  1        auto    auto unknown
Et2/2    connected      connected  1        auto    auto unknown
Et2/3    connected      connected  1        auto    auto unknown
Et3/0    connected      connected  1        auto    auto unknown
Et3/1    connected      connected  1        auto    auto unknown
Et3/2    connected      connected  1        auto    auto unknown
Et3/3    connected      connected  1        auto    auto unknown
SWCiscoL2#

```

voilà nos vlans sont créé on passe à la phase de teste pour voir si nos pc on reçu des adresse ip via dhcp sur leur vlan respectifs.

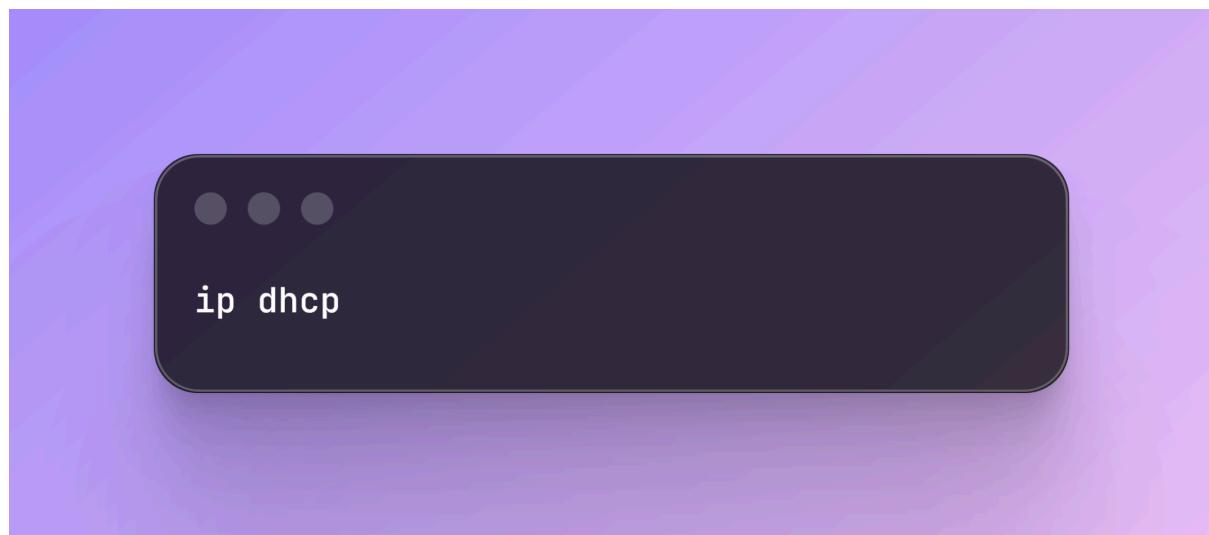
## 4. Tests finaux

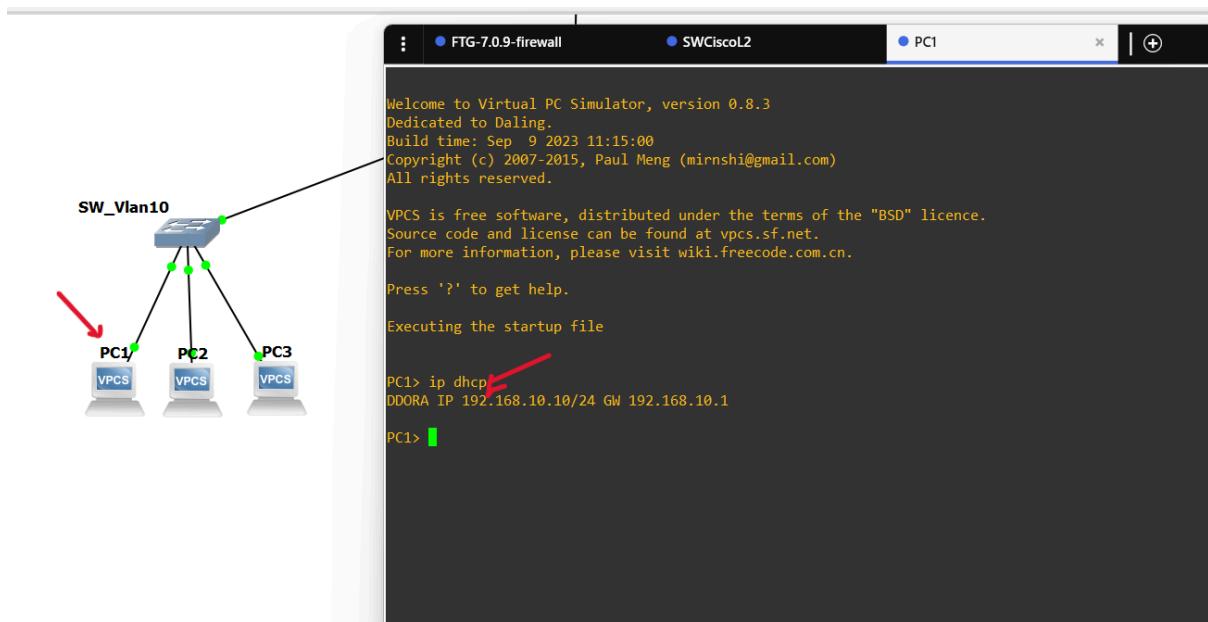
On revient sur notre fortigate **Dashboard > Network > DHCP**

The screenshot shows the FortiGate management interface. The left sidebar is open, showing various network-related sections like FortiView Sources, FortiView Destinations, and FortiView Applications. The main panel is titled 'DHCP' and has two tabs: 'Status' and 'Interface'. Both tabs show 'No results'. Below the tabs are filter options: Device, IP, Interface, Status, MAC, Reserved, Host Information, and Expires. A red arrow points from the text 'On devrait voir tous nos pc dans cet onglet mais c'est vide,c'est tout à fait normal parce qu'on doit d'abord aller activer le dhcp au niveau de nos pc pour qu'ils puissent recevoir des IP.' to the 'Interface' tab.

On devrait voir tous nos pc dans cet onglet mais c'est vide,c'est tout à fait normal parce qu'on doit d'abord aller activer le dhcp au niveau de nos pc pour qu'ils puissent recevoir des IP.

On revient dans GNS3 sur un des PC on fait clique droit puis sur console après on tape la commande :





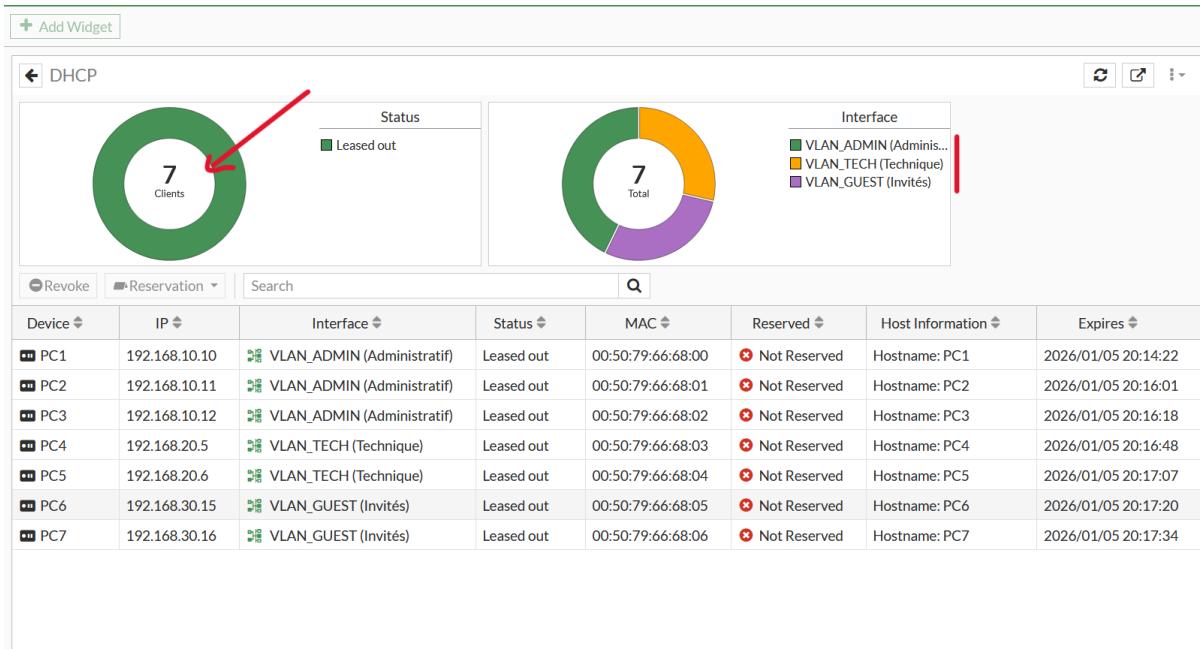
on revient sur notre fortigate

The screenshot shows the Fortigate's DHCP management interface. At the top, there are two circular statistics: one for "Clients" (1) and one for "Total" (1). Below these are buttons for "Revoke" and "Reservation". A search bar and a refresh icon are also present.

Device	IP	Interface	Status	MAC	Reserved	Host Information	Expires
PC1	192.168.10.10	VLAN_ADMIN (Administratif)	Leased out	00:50:79:66:68:00	Not Reserved	Hostname: PC1	2026/01/05 20:14:22

A red arrow points from the text "voilà notre PC vient d'être détecté par notre fortigate sur le vlan 10" in the accompanying text to the row for "PC1" in the table.

voilà notre PC vient d'être détecté par notre fortigate sur le vlan 10 sur lequel il se trouve. on va par la suite faire de même pour tous les autres PC puis au final on aura tous les pc répertoriés par notre fortigate.



Pour l'instant nos pc ne peuvent ni communiquer entre vlan ni aller sur internet c'est normal on a pas encore configuré.

```

PC1> ping 8.8.8.8

8.8.8.8 icmp_seq=1 timeout
8.8.8.8 icmp_seq=2 timeout
8.8.8.8 icmp_seq=3 timeout
8.8.8.8 icmp_seq=4 timeout
8.8.8.8 icmp_seq=5 timeout

PC1> ping 192.168.10.11

84 bytes from 192.168.10.11 icmp_seq=1 ttl=64 time=0.287 ms
84 bytes from 192.168.10.11 icmp_seq=2 ttl=64 time=0.496 ms
84 bytes from 192.168.10.11 icmp_seq=3 ttl=64 time=0.385 ms
84 bytes from 192.168.10.11 icmp_seq=4 ttl=64 time=0.574 ms
84 bytes from 192.168.10.11 icmp_seq=5 ttl=64 time=0.668 ms

PC1> ping 192.168.20.5

192.168.20.5 icmp_seq=1 timeout
192.168.20.5 icmp_seq=2 timeout
192.168.20.5 icmp_seq=3 timeout
192.168.20.5 icmp_seq=4 timeout
192.168.20.5 icmp_seq=5 timeout

PC1> 
```

# Conclusion

Dans cette **Partie 1**, nous avons :

- Préparer un lab complet avec FortiGate et switchs
- Configuré 3 VLANs et attribué les IPs correspondantes
- Vérifié que le réseau fonctionne correctement, prêt pour la **Partie 2** : configuration des firewall policies et sécurité

**Next step (Partie 2) :**

- Créer une organisation claire des objets FortiGate (adresses, groupes, services)
- Configurer les firewall policies pour gérer l'accès entre VLANs et vers Internet
- Activer les Security Profiles et VIP pour exposer un serveur interne
- Bloquer certains services (réseaux sociaux, streaming, jeux...)