**Royaume du Maroc**
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique et de l'Innovation
Université Cadi Ayyad
École Nationale des Sciences Appliquées
Marrakech

**المملكة المغربية**
وزارة التعليم العالي والبحث العلمي والإبتكار
جامعة القاضي عياض
المدرسة الوطنية للعلوم التطبيقية
مراكش

# Projet Architecture d'entreprise H.A (Cisco : Routage, Politiques de sécurité ...)

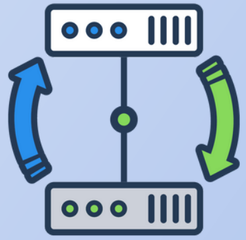
Sous le module de protocoles de sécurité & sécurité des réseaux et des communications

**Réaliser par:**

BELADEL Hasna
CHAARAOUI Mouad
ED-DARRAJY Hajar
KNIOUI Brahim
NASSIRI Noussaiba

**Encadré par :**

Pr AZOUGAGHE Ali



Année universitaire: 2023/2024

# PLAN

# Haute disponibilité

# H.A

**La haute disponibilité (HA)** dans un réseau informatique se réfère à la capacité du réseau à rester opérationnel et à fournir des services de manière continue et fiable, même en présence de défaillances matérielles ou logicielles. Techniquement, cela implique la mise en œuvre de diverses stratégies, protocoles et technologies pour minimiser les temps d'arrêt et assurer une disponibilité maximale des services réseau.

- **Fiabilité accrue :** Elle offre une résilience élevée en répartissant la charge de travail sur plusieurs serveurs ou nœuds. Ainsi, si l'un d'entre eux échoue, les autres prennent le relais, évitant ainsi une interruption de service.
- **Redondance :** Les systèmes en architecture HA ont souvent des composants redondants. Si un composant tombe en panne, un autre prend le relais automatiquement pour garantir la continuité du service.
- **Temps d'arrêt réduit :** En cas de panne ou de maintenance planifiée, les architectures haute disponibilité permettent de minimiser voire d'éliminer le temps d'arrêt en redirigeant automatiquement le trafic vers des ressources disponibles.

- **Évolutivité :** Elles peuvent être conçues pour évoluer facilement en ajoutant de nouveaux serveurs ou en mettant à niveau les composants existants sans interrompre les opérations en cours.
- **Performance améliorée :** En distribuant la charge de travail, l'architecture HA peut offrir des performances plus constantes même en cas de fluctuations de la demande.
- **Plan de reprise après sinistre (PRAS) :** Elle facilite la mise en place de plans de continuité des activités en assurant la disponibilité des services même en cas de sinistre majeur.
- **Amélioration de la tolérance aux erreurs :** Les systèmes HA sont conçus pour détecter et isoler les erreurs afin d'éviter qu'elles ne se propagent à l'ensemble du système.

**Active-Standby (Actif-passif) :**

Un système actif qui est utilisé pour traiter le trafic ou fournir les services en temps normal. En cas de défaillance, un système de secours, en mode veille, prend automatiquement le relais pour assurer la continuité des opérations. Cela est souvent utilisé dans des environnements où la bascule entre les systèmes doit être rapide et où la continuité des services est prioritaire.

**Actif-actif :**

Tous les systèmes sont actifs et traitent le trafic ou les services en même temps. La charge de travail est répartie entre eux pour garantir une utilisation équilibrée des ressources. En cas de défaillance d'un système, la charge de travail est redistribuée automatiquement vers les systèmes restants. Cela est utilisé pour optimiser les performances et la capacité en maintenant plusieurs systèmes actifs simultanément.

# Problématique,
# Solutions,
# Objectives

# PROBLÉMATIQUE

**Redondance et Tolérance aux Pannes**

Comment concevoir une architecture qui minimise les interruptions de service en cas de défaillance ?

**Évolutivité et Scalabilité**

Comment concevoir une architecture qui puisse s'adapter à la croissance de l'entreprise tout en maintenant une haute disponibilité ?

**Gestion de la Charge**

Comment répartir la charge de manière équilibrée entre les différents composants du systèmes ?

**Coût et Ressources**

Comment maximiser la disponibilité tout en optimisant les coûts opérationnels ?

# SOLUTIONS

## Redondance et Réplication

La redondance des composants critiques, tels que les serveurs et bases de données,les pare-feux...

La réplication en temps réel des données sur des serveurs de secours

## Basculement Automatique

Les mécanismes de basculement automatique permettent de commuter rapidement vers des ressources de secours sans perturbation majeure des services

## Scalabilité Horizontale

Concevoir une architecture qui peut facilement évoluer en ajoutant des ressources supplémentaires sans interruption de service

## Surveillance Proactive

L'utilisation d'outils de surveillance avancés facilitant une intervention proactive pour prévenir les incidents et maintenir la disponibilité du système

# OBJECTIVES

## Concevoir l'architecture du réseau HA

Cela implique la création d'une infrastructure réseau capable de fournir une disponibilité élevée

## Configuration des appareils

Une fois l'architecture conçue, la configuration des appareils implique la mise en œuvre concrète des composants réseau, routeurs, commutateurs, etc.

## Tester le fonctionnement

Après la configuration, il est essentiel de tester le fonctionnement de l'ensemble du réseau HA. Cela peut inclure des simulations de défaillance pour évaluer la résilience du système, des tests de basculement pour s'assurer que la redondance fonctionne correctement,

# Outils


## GNS3

GNS3 est une plateforme de virtualisation de réseau utilisée pour créer, simuler et tester des réseaux informatiques. C'est un logiciel open-source qui permet aux utilisateurs de concevoir des topologies réseau complexes en utilisant des dispositifs virtuels.

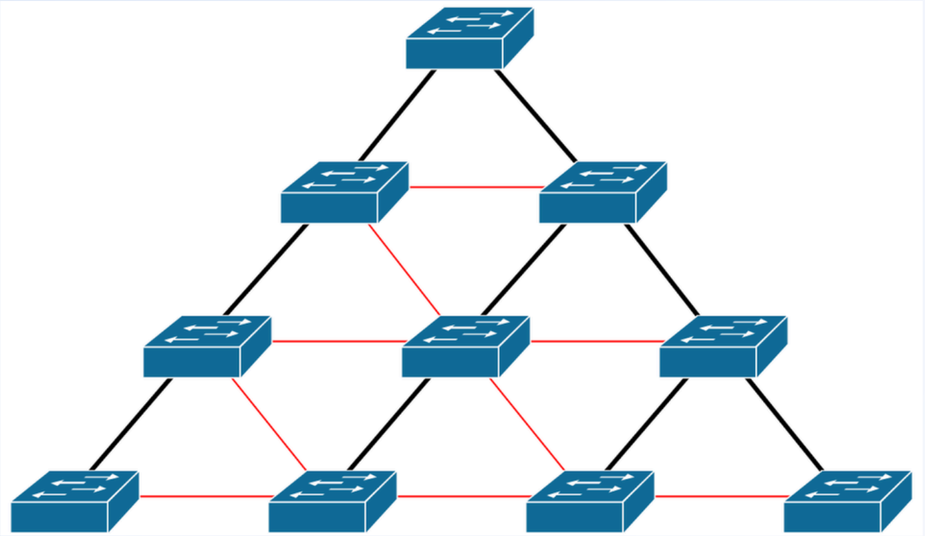

## VMware

VMware est une application de virtualisation populaire permettant de créer et de gérer des machines virtuelles sur un ordinateur hôte.

# Protocole

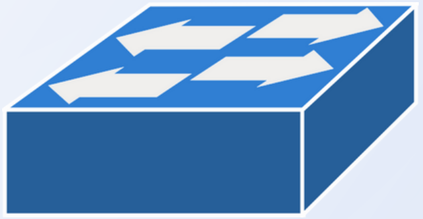
# SPANNING TREE

**Spanning Tree Protocol (STP)** est un protocole de couche 2 utilisé dans les réseaux Ethernet pour prévenir la formation de boucles et assurer la redondance des chemins sans créer de boucles de trafic.
Voici quelques points clés sur le fonctionnement du Spanning Tree Protocol (STP) :

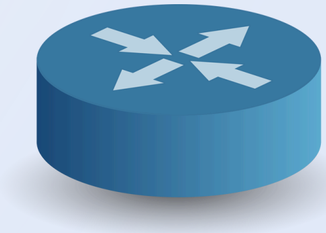


**1. Prévention des boucles**
**2. Élection du bridge root**
**3. Calcul des chemins**
**4. Rétablissement de la redondance**
**5. Variantes de STP**

# Technologies



Switch (cisco IOU 15.2d)



Routeur(Cisco 3745 124-25.T14)

Firewall ( Fortigate 7.0.0)

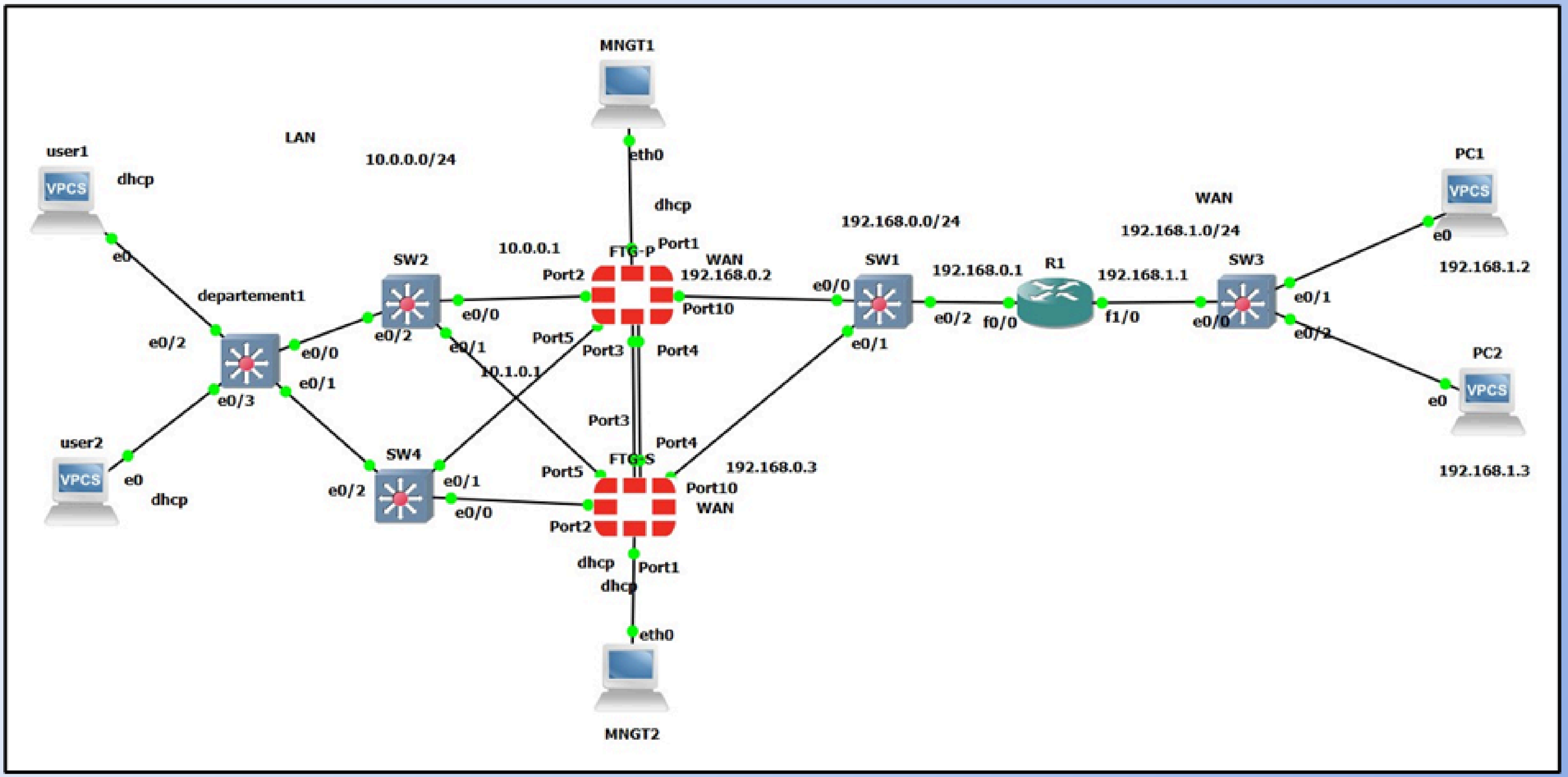
PC

# CONFIGURATION

- Configuration initiale
- Configuration H.A

# CONFIGURATION INITIALE

# ARCHITECTURE



# CONFIGURATION DE FTG-P

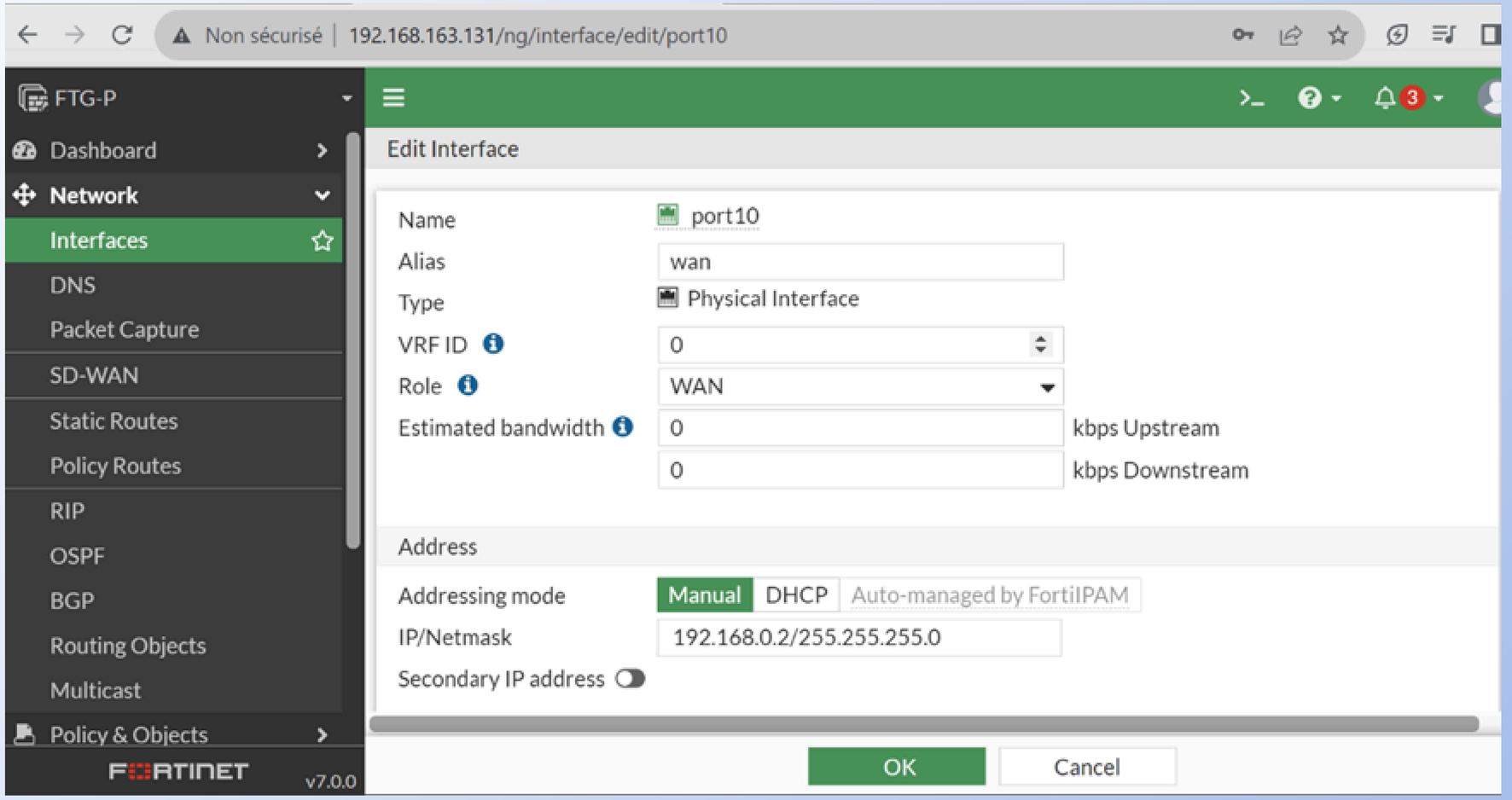
Configuration des interfaces :

PORT 1 : interface de management

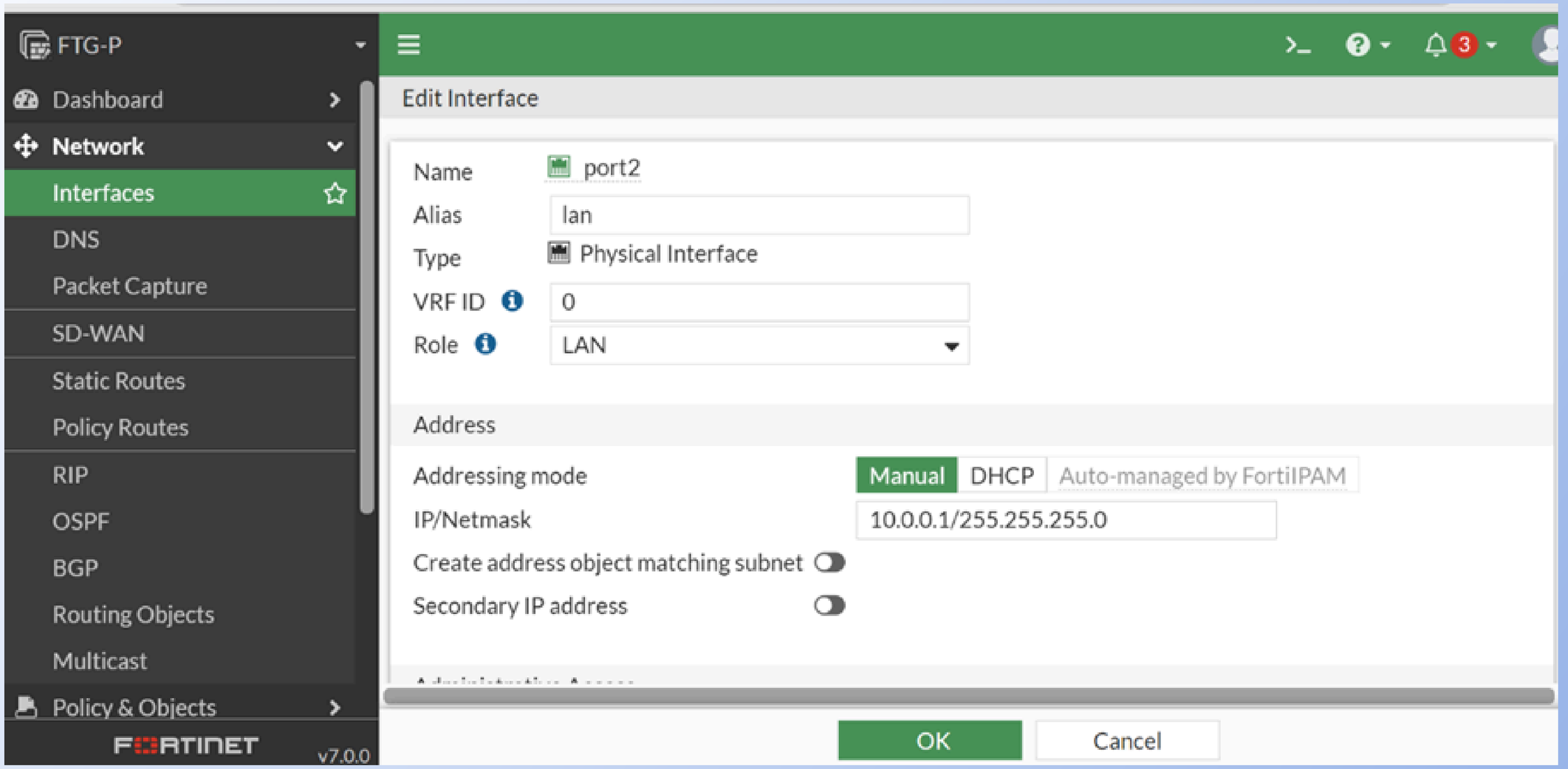
```
FortiGate-VM64-KVM #
FortiGate-VM64-KVM # config sys inter

FortiGate-VM64-KVM (interface) # edit  port1

FortiGate-VM64-KVM (port1) # set mode dhcp

FortiGate-VM64-KVM (port1) # set allowaccess http ping ssh

FortiGate-VM64-KVM (port1) # end
```

```
FortiGate-VM64-KVM # config sys inter

FortiGate-VM64-KVM (interface) # get port1
name                : port1
vdom                : root
vrf                 : 0
cli-conn-status     : 2
fortilink           : disable
mode                : dhcp
client-options:
distance            : 5
priority            : 0
dhcp-relay-service  : disable
ip                  : 192.168.163.131 255.255.255.0
allowaccess         : ping ssh http
fail-detect         : disable
arpforward          : enable
broadcast-forward   : disable
bfd                 : global
l2forward           : disable
icmp-send-redirect  : enable
```

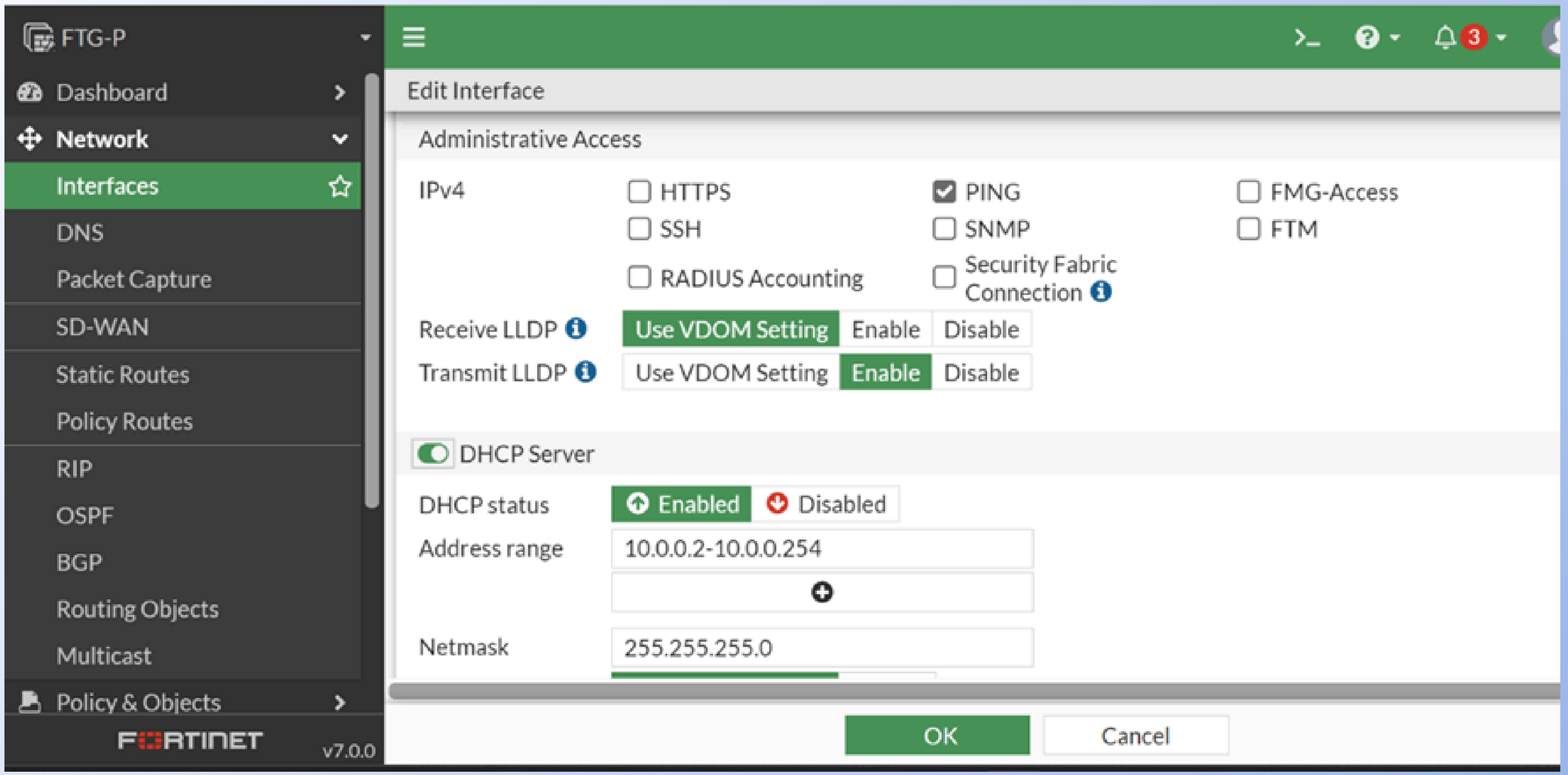
# PORT 10 : port WAN



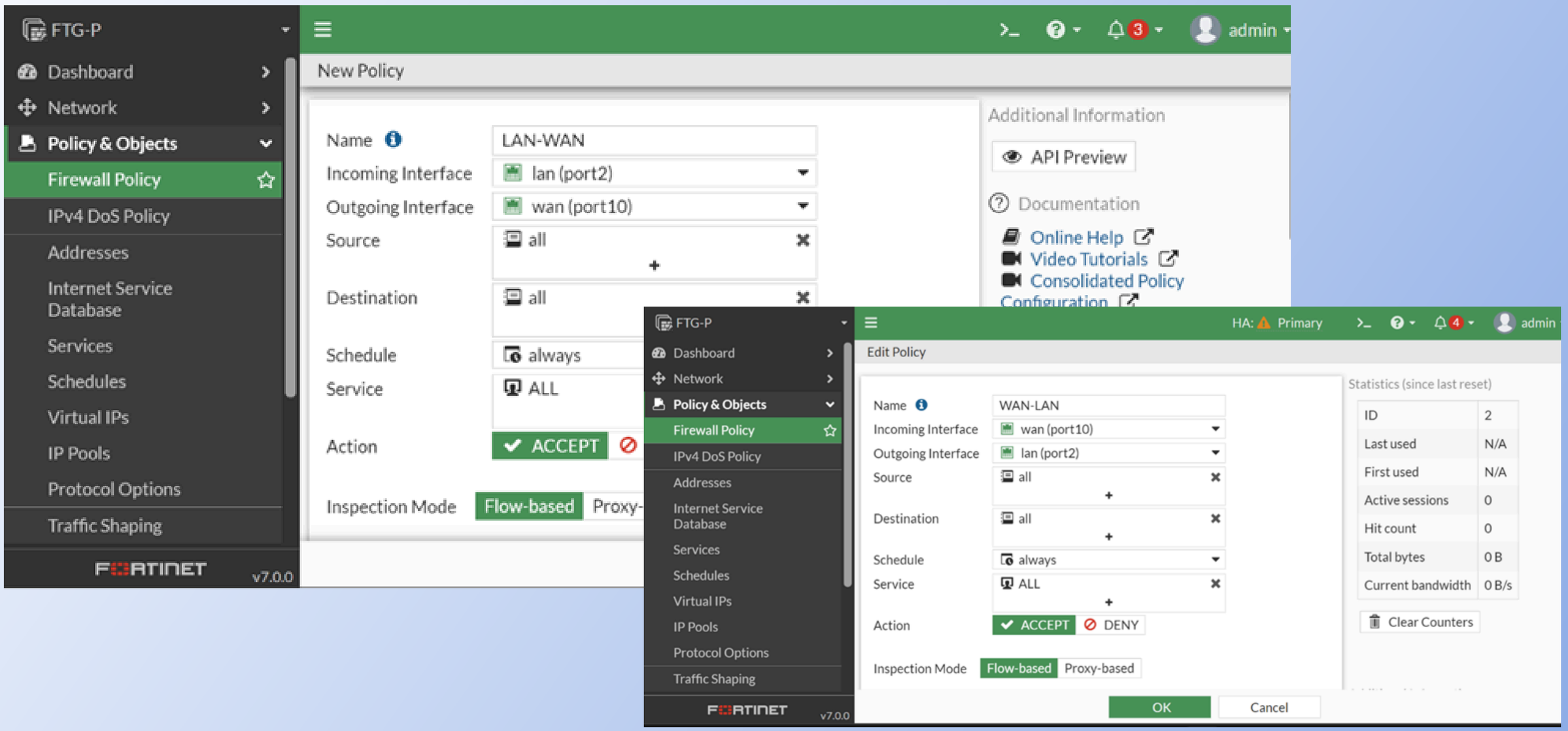
# PORT 2 : 1 ère  port lan



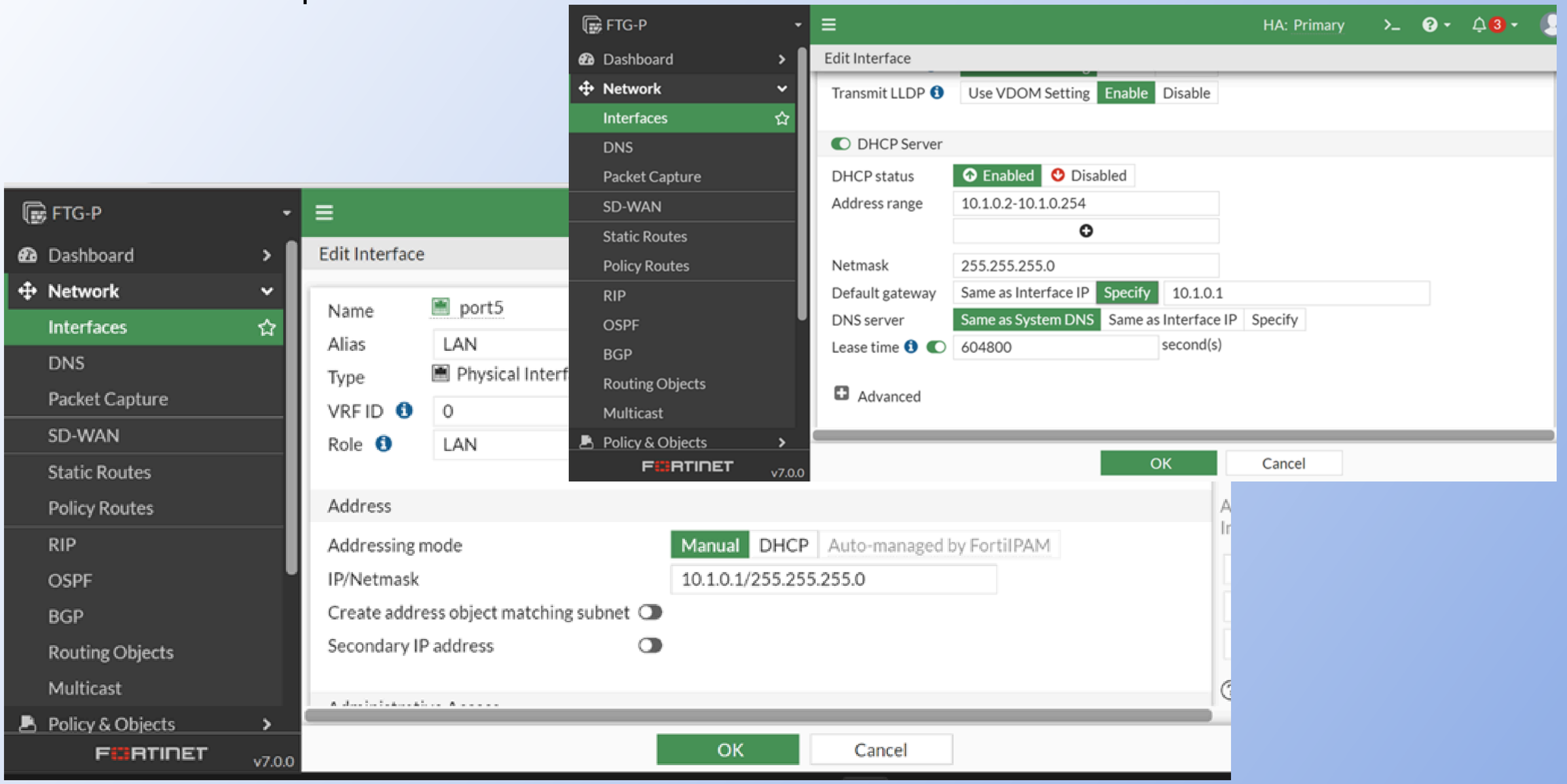
# Configuration de cet interface (port2) comme serveur dhcp pour le lan



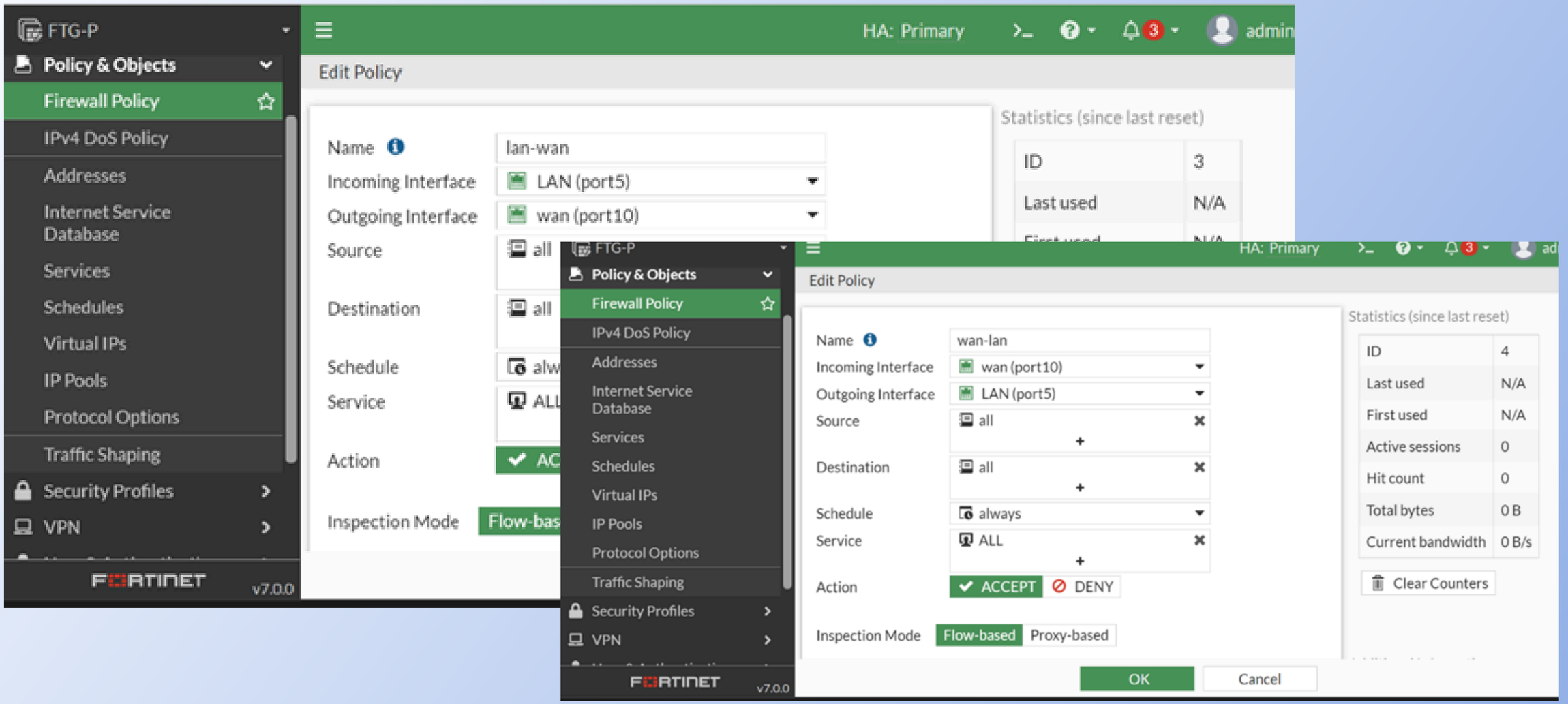
# La politique de sécurité  LAN-WAN et l'inverse



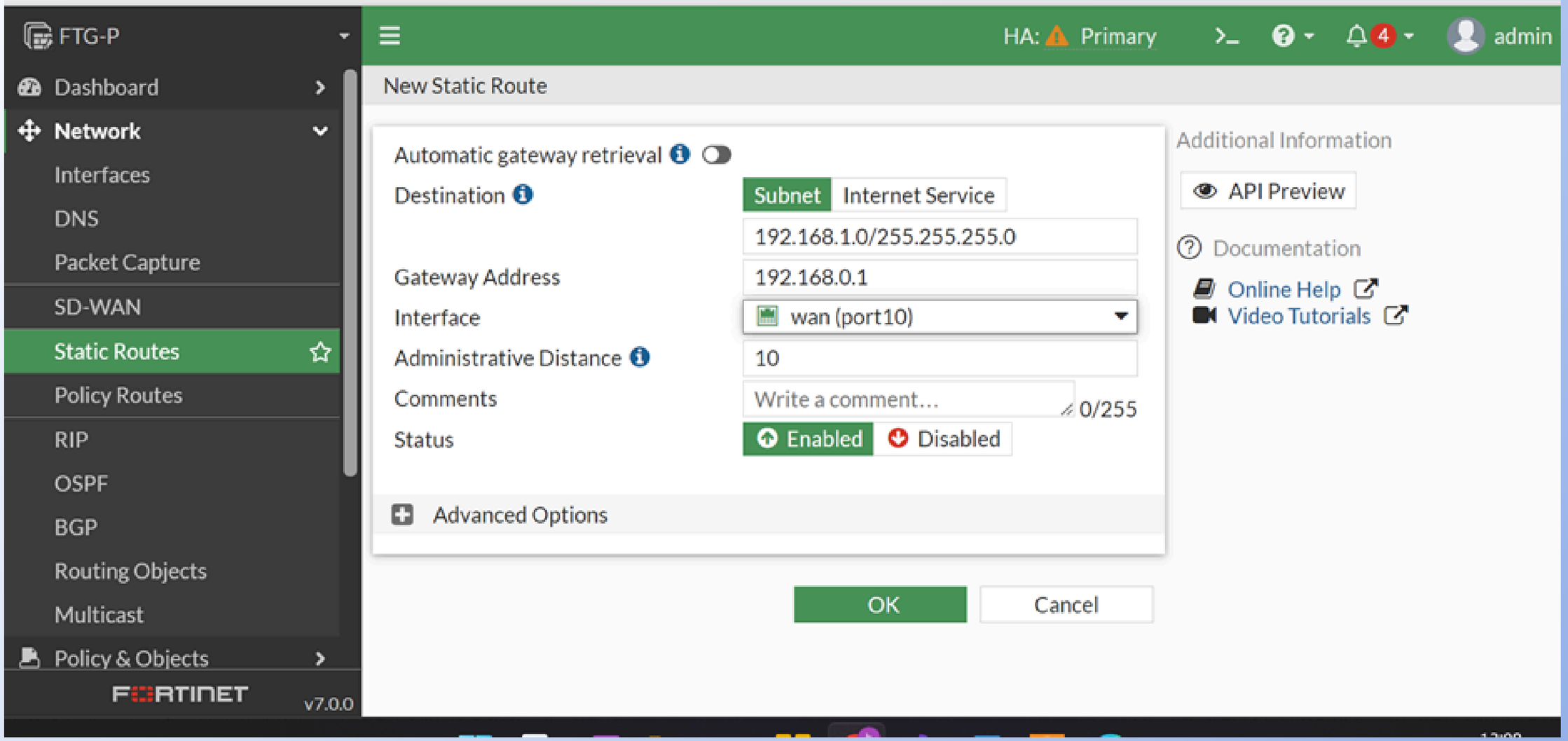
# PORT 5 : 2-ème port lan



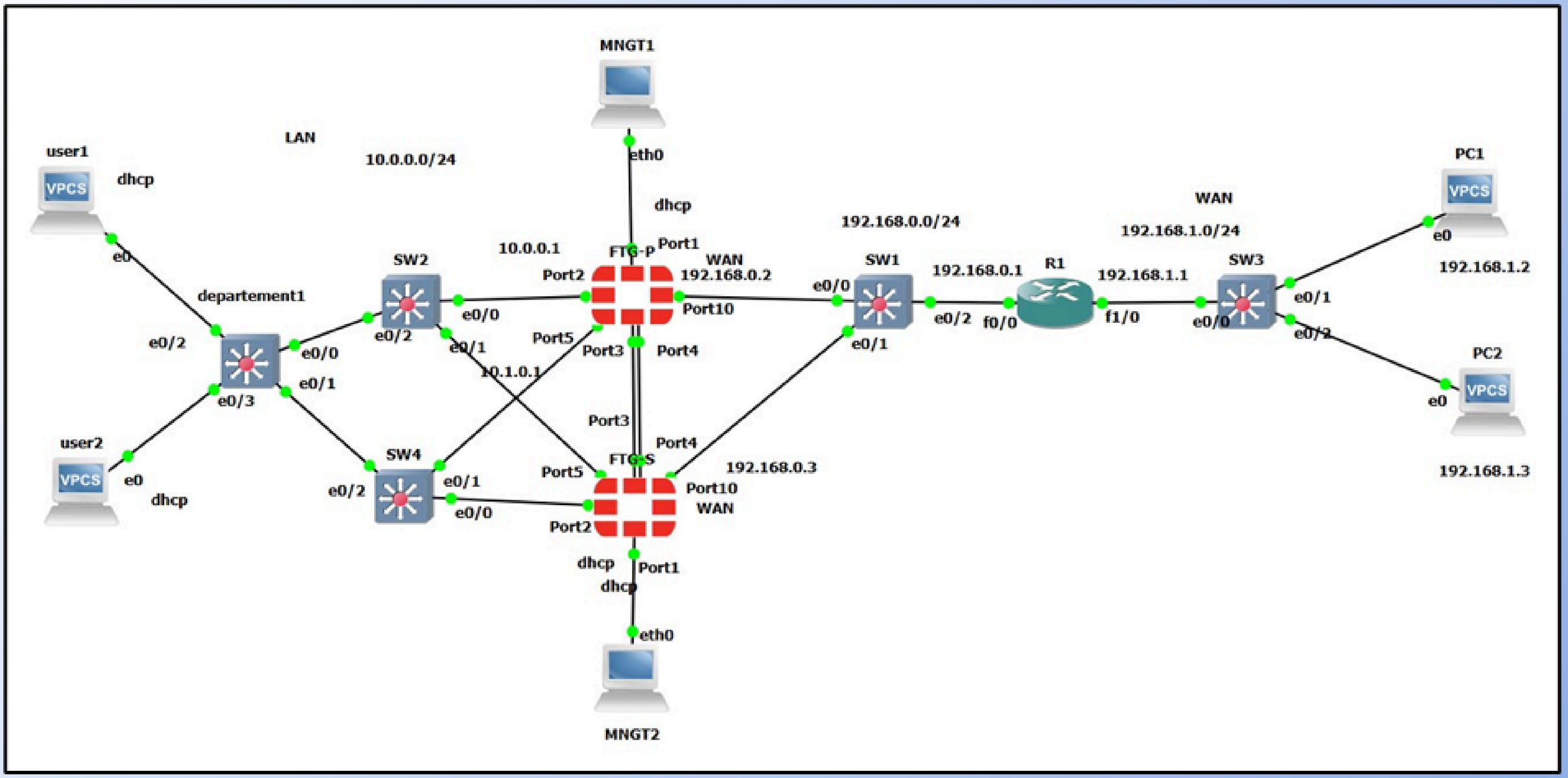
la politique directe et la politique inverse de  lan (port5) au wan



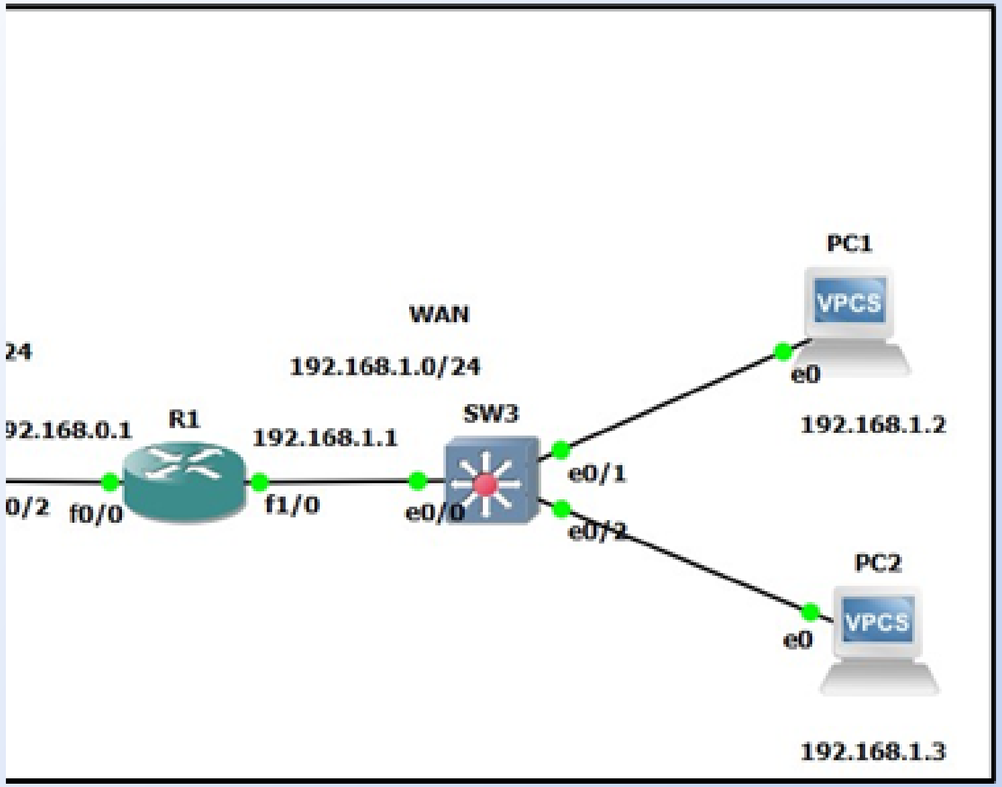
configuration de route statique vers le WAN 192.168.1.0/24



# CONFIGURATION DE ROUTEUR


MNGT1
LAN
10.0.0.0/24
eth0
dhcp
user1
VPCS
dhcp
e0
10.0.0.1
FTG-P
Port1
WAN
192.168.0.2
Port2
SW2
departement1
e0/2
e0/0
e0/1
e0/3
e0/2
e0/0
e0/1
10.1.0.1
Port5
Port3
Port4
192.168.0.0/24
SW1
e0/0
e0/1
e0/2
192.168.0.1
R1
f0/0
192.168.1.1
f1/0
WAN
192.168.1.0/24
SW3
e0/0
e0/1
e0/2
PC1
VPCS
e0
192.168.1.2
PC2
VPCS
e0
192.168.1.3
user2
VPCS
e0
dhcp
SW4
e0/2
e0/1
e0/0
Port3
Port4
Port5
FTG-S
192.168.0.3
Port10
WAN
Port2
dhcp
Port1
dhcp
eth0
MNGT2

# Configuration des interfaces  f0/0  et f1/0 :




```
term
nfiguration commands, one per line.  End with CNTL/Z
g)#interface f0/0
g-if)#ip address 192.168.0.1 255.255.255.0
g-if)#no shutdown
```

```
1#
1#conf term
nter configuration commands, one per line.  End with CNTL/Z.
1(config)#inter f1/0
1(config-if)#ip address 192.168.1.1 255.255.255.0
1(config-if)#no shutdown
1(config-if)#
```

configuration de la route statique vers  10.0.0.0/24 et  10.1.0.0/24

```
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip  route 10.0.0.0 255.255.255.0  192.168.0.2
R1(config)#no shutdown
% Incomplete command.

R1(config)#
```

```
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 10.1.0.0 255.255.255.0  192.168.02
```

# CONFIGURATION DES MACHINES

configuration des addresses ip pour les machines user1 ,user2 ,PC1 et PC2

user1 ,user2  ont addresses automatiques  d’apres le  port2 ou port5

```
# This the configuration for user1
#
# Uncomment the following line to enable DHCP
dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.1 255.0.0.0
#

set pcname user1
```

**edit config**

PC1 et PC2 ont des  addresses  statiques

PC2 startup.vpc

```
# This the configuration for PC2
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
ip 192.168.1.3 255.255.255.0 192.168.1.1
#
```

# CONFIGURATION DE FTG-S

# PORT 1 : interface de management

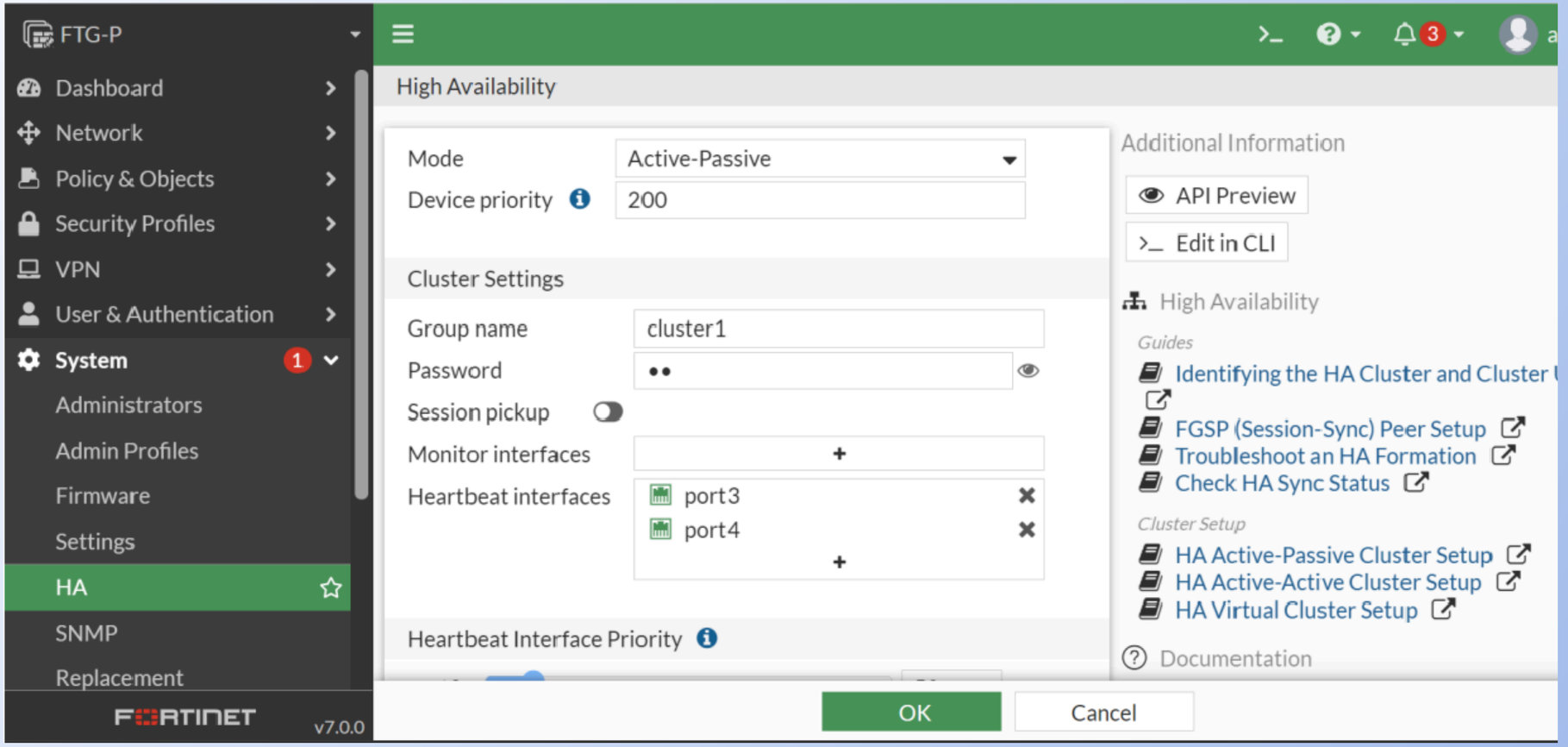
```
FortiGate-VM64-KVM # conf sys inter

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set mode dhcp

FortiGate-VM64-KVM (port1) # set allow\access http ssh ping

FortiGate-VM64-KVM (port1) # set allowaccess http ssh ping

FortiGate-VM64-KVM (port1) # end

FortiGate-VM64-KVM #
```

```
FortiGate-VM64-KVM (interface) # get port1
name                   : port1
vdom                   : root
vrf                    : 0
cli-conn-status        : 2
fortilink              : disable
mode                   : dhcp
client-options:
distance               : 5
priority               : 0
dhcp-relay-service     : disable
ip                     : 192.168.163.130 255.255.255.0
allowaccess            : ping ssh http
fail-detect            : disable
```

# CONFIGURATION DE HA

# Configuration FTG-P

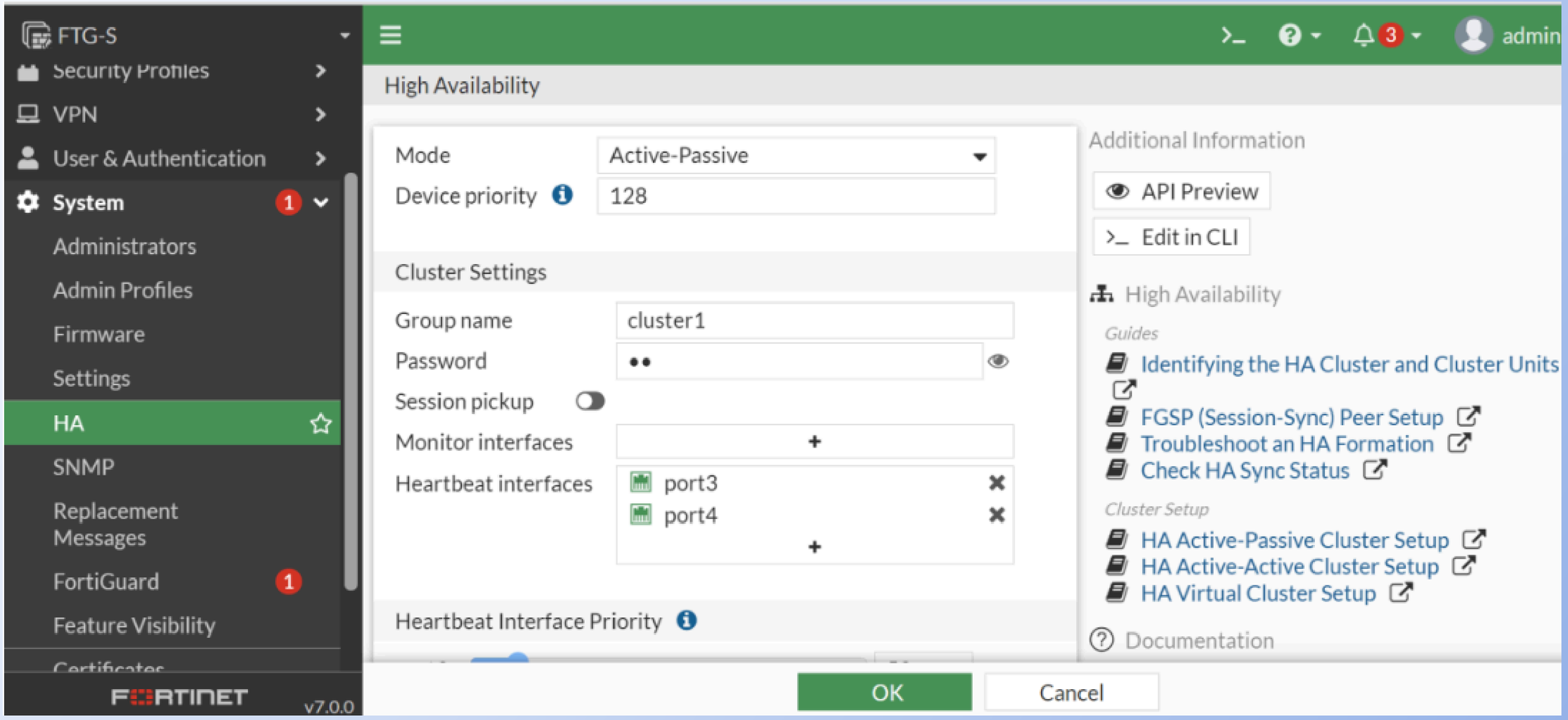
Nous accédons au système du FTG-P et nous modifions les paramètres de la Haute Disponibilité (HA) comme suit



Le port de gestion (port 1) pourrait avoir changé d'adresse IP, Donc On vérifier:

```
FTG-P (interface) # show port1

command parse error before 'port1'
Command fail. Return code -61

FTG-P (interface) # get port1
name                  : port1
vdom                  : root
vrf                   : 0
cli-conn-status       : 2
fortilink             : disable
mode                  : dhcp
client-options:
distance              : 5
priority              : 0
dhcp-relay-service    : disable
management-ip         : 0.0.0.0 0.0.0.0
ip                    : 192.168.163.133 255.255.255.0
allowaccess           : ping ssh http
fail-detect           : disable
arpforward            : enable
broadcast-forward     : disable
bfd                   : global
l2forward             : disable
icmp-send-redirect    : enable
icmp-accept-redirect: enable
vlanforward           : disable
stpforward            : disable
ips-sniffer-mode      : disable
ident-accept          : disable
ipmac                 : disable
```

# Configuration FTG-S

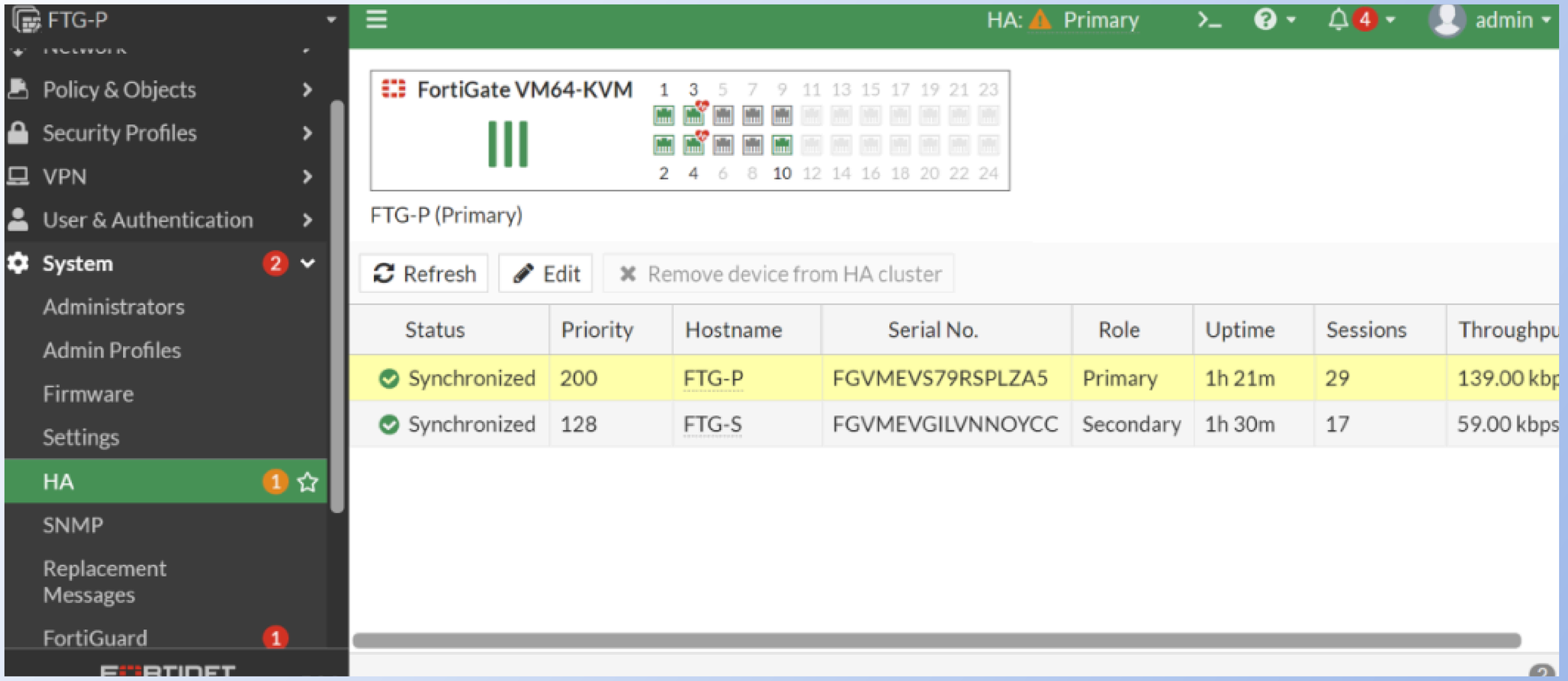


Vérification de synchronisation de FTG-P avec FTG-S:

La synchronisation nécessite quelques secondes à quelques minutes pour se compléter. Pour vérifier l'état de la haute disponibilité (HA), vous pouvez utiliser la commande :

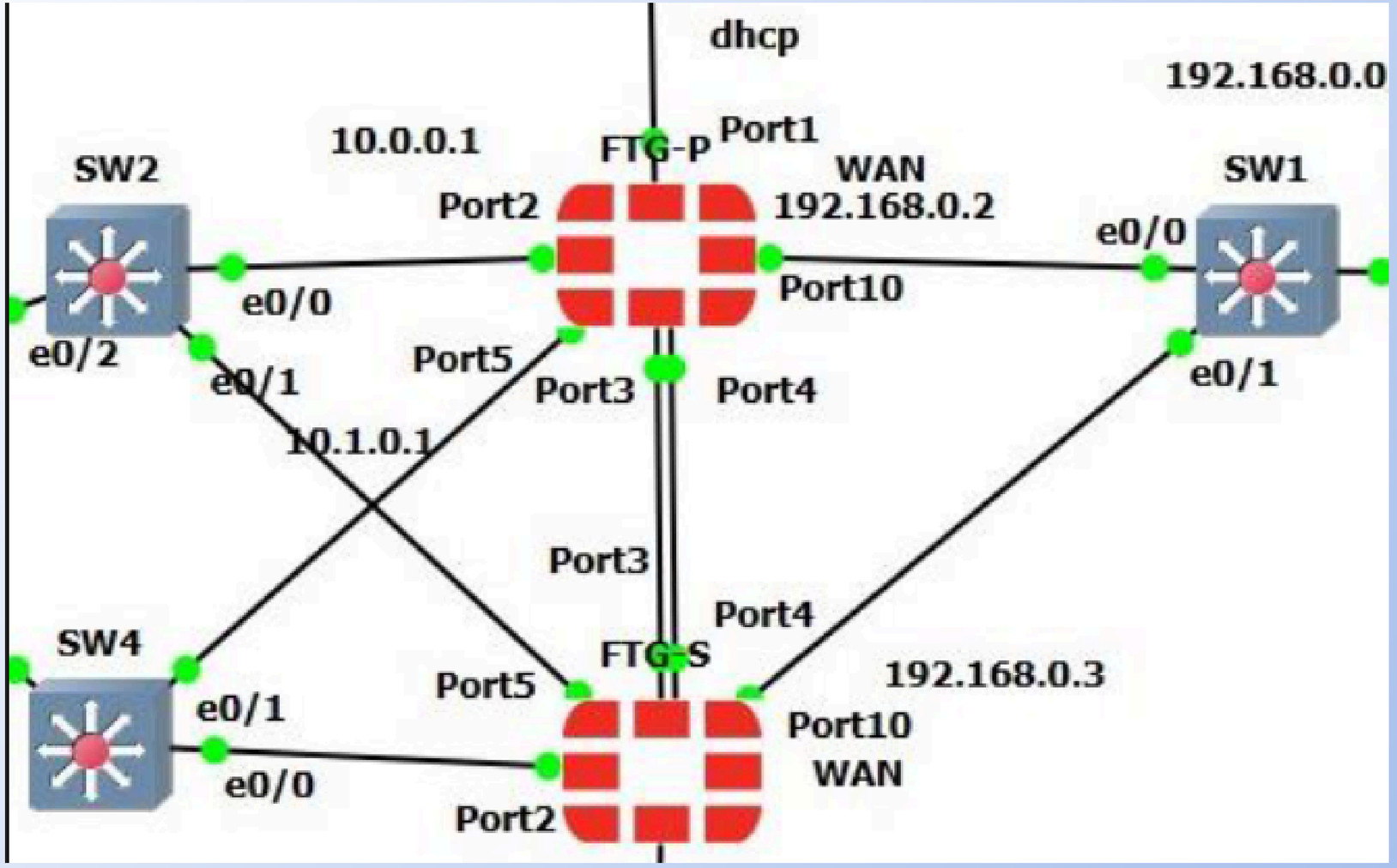
get system ha status

```
FTG-S # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:29:39
Cluster state change time: 2023-12-03 02:52:00
Primary selected using:
    <2023/12/03 02:52:00> FGVMEVS79RSPLZA5 is selected as the primary because its override priority is larger than peer member FGVMEVGILVNN
ses_pickup: disable
override: disable
Configuration Status:
    FGVMEVGILVNNOYCC(updated 2 seconds ago): in-sync
    FGVMEVS79RSPLZA5(updated 4 seconds ago): in-sync
System Usage stats:
    FGVMEVGILVNNOYCC(updated 2 seconds ago):
        sessions=7, average-cpu-user/nice/system/idle=0%/0%/1%/94%, memory=68%
    FGVMEVS79RSPLZA5(updated 4 seconds ago):
```




À ce moment, les deux pare-feux sont en synchronisation.

Configuration de HA dans les switches

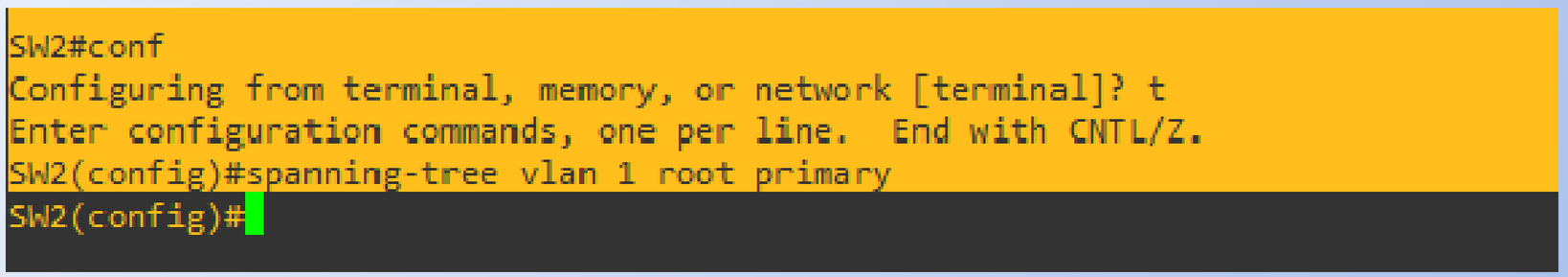


On a utiliser deux switches dans le lan pour eviter d’avoir une architecture a un seul point de défaillance L’utilisation de protocole STP est indispensable pour éviter les boucles réseau

**Configuration de spanning tree protocol (STP)**

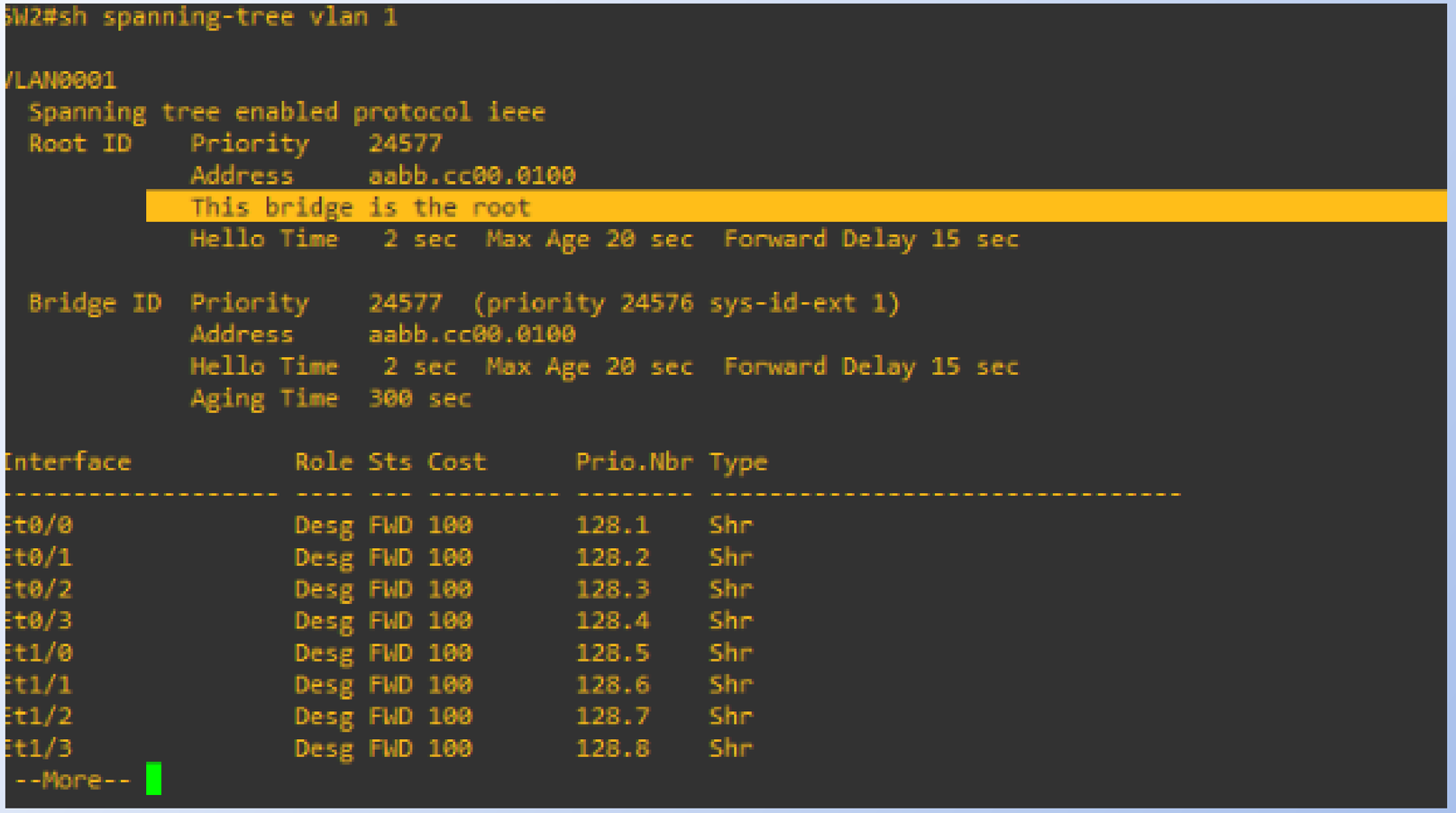
Pour SW2: On forcer SW2 à devenir la racine (root):

Conf ter
Spanning-tree vlan 1 root primary



Pour vérifier que SW2 est la racine (root):

Sh spanning-tree vlan 1



# Pour SW4:

```
SW4#sh spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     aabb.cc00.0100
              Cost        200
              Port        3 (Ethernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     aabb.cc00.0400
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Root FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
Et2/0               Desg FWD 100       128.9    Shr
Et2/1               Desg FWD 100       128.10   Shr
Et2/2               Desg FWD 100       128.11   Shr
Et2/3               Desg FWD 100       128.12   Shr
Et3/0               Desg FWD 100       128.13   Shr
```

# Réalisation

# Video

# Merci pour votre attention

**Royaume du Maroc**
Ministère de l'Enseignement Supérieur,
de la Recherche Scientifique et de l'Innovation
Université Cadi Ayyad
École Nationale des Sciences Appliquées
Marrakech

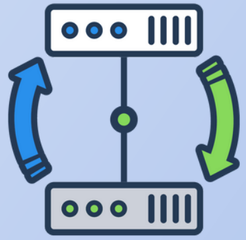
**المملكة المغربية**
وزارة التعليم العالي والبحث العلمي والإبتكار
جامعة القاضي عياض
المدرسة الوطنية للعلوم التطبيقية
مراكش

# projet architecture d'entreprise H.A (Cisco : Routage, Politiques de sécurité ...)

Sous le module de protocoles de sécurité & sécurité des réseaux et des communications

**Realiser par:**

BELADEL Hasna
CHAARAOUI Mouad
ED-DARRAJY Hajar
KNIOUI Brahim
NASSIRI Noussaiba



**Encadré par :**

Pr AZOUGAGHE Ali

Année universitaire: 2023/2024