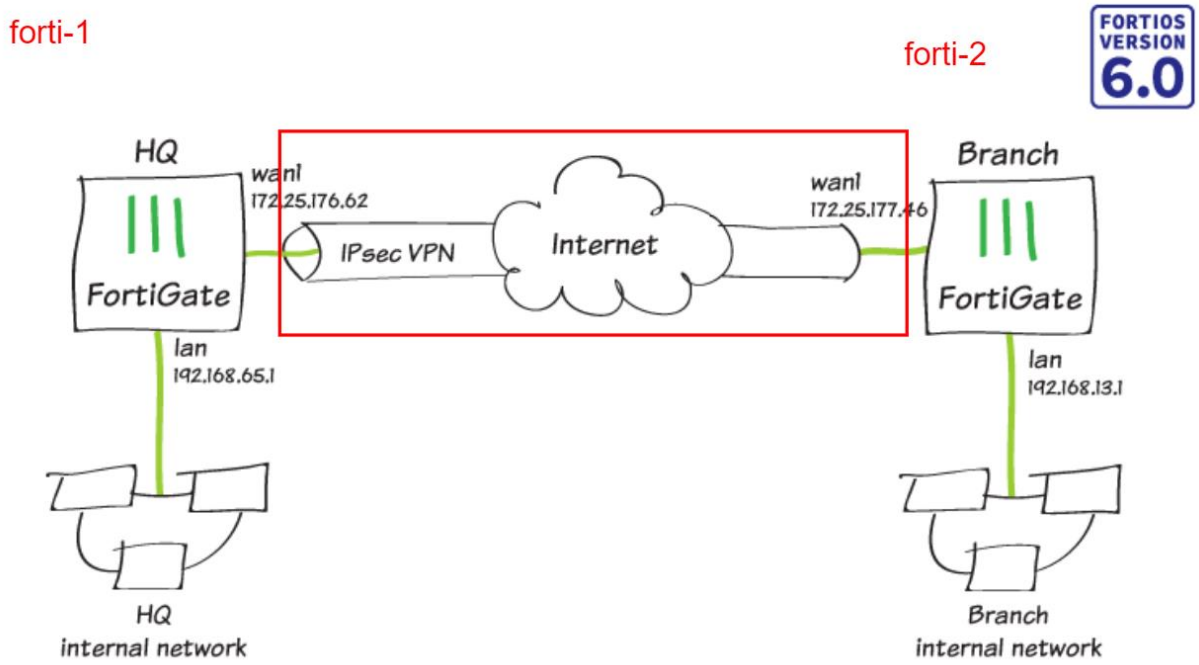
Lab VPN IPSEC site-à-site Fortinet

https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/281288/site-to-site-ipsec-vpn-with-two-fortigate-devices



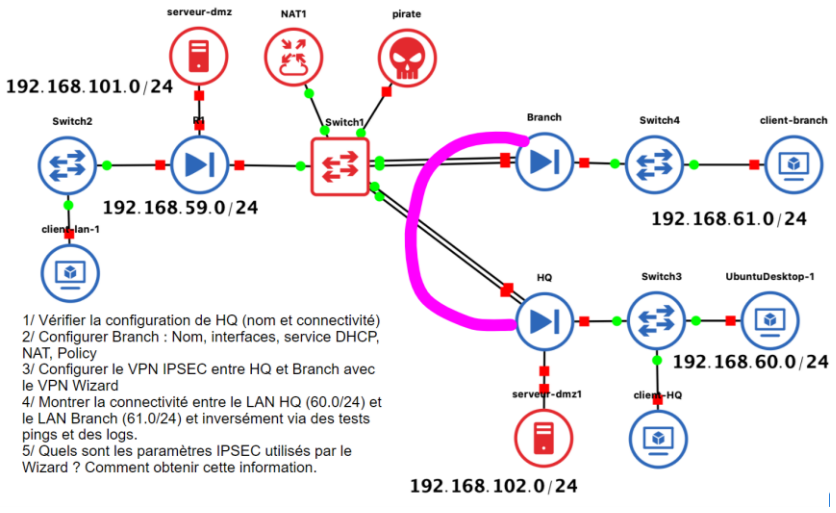
Objectifs :

On va créer tunnel VPN site à site pour faire communiquer deux réseaux.

On doit reprendre une topologie fonctionnelle, ajouter pare-feu fortinate que l'on devra configurer.

L'idée est que le réseau local du réseau local du fortinate 1 arrive à joindre réseau local du fortinate 2 et inversement.

Topologie à faire



Consignes Lab

1/ Vérifier la configuration de HQ (nom et connectivité)

2/ Configurer Branch : Nom, interfaces, service DHCP, NAT, Policy

3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard

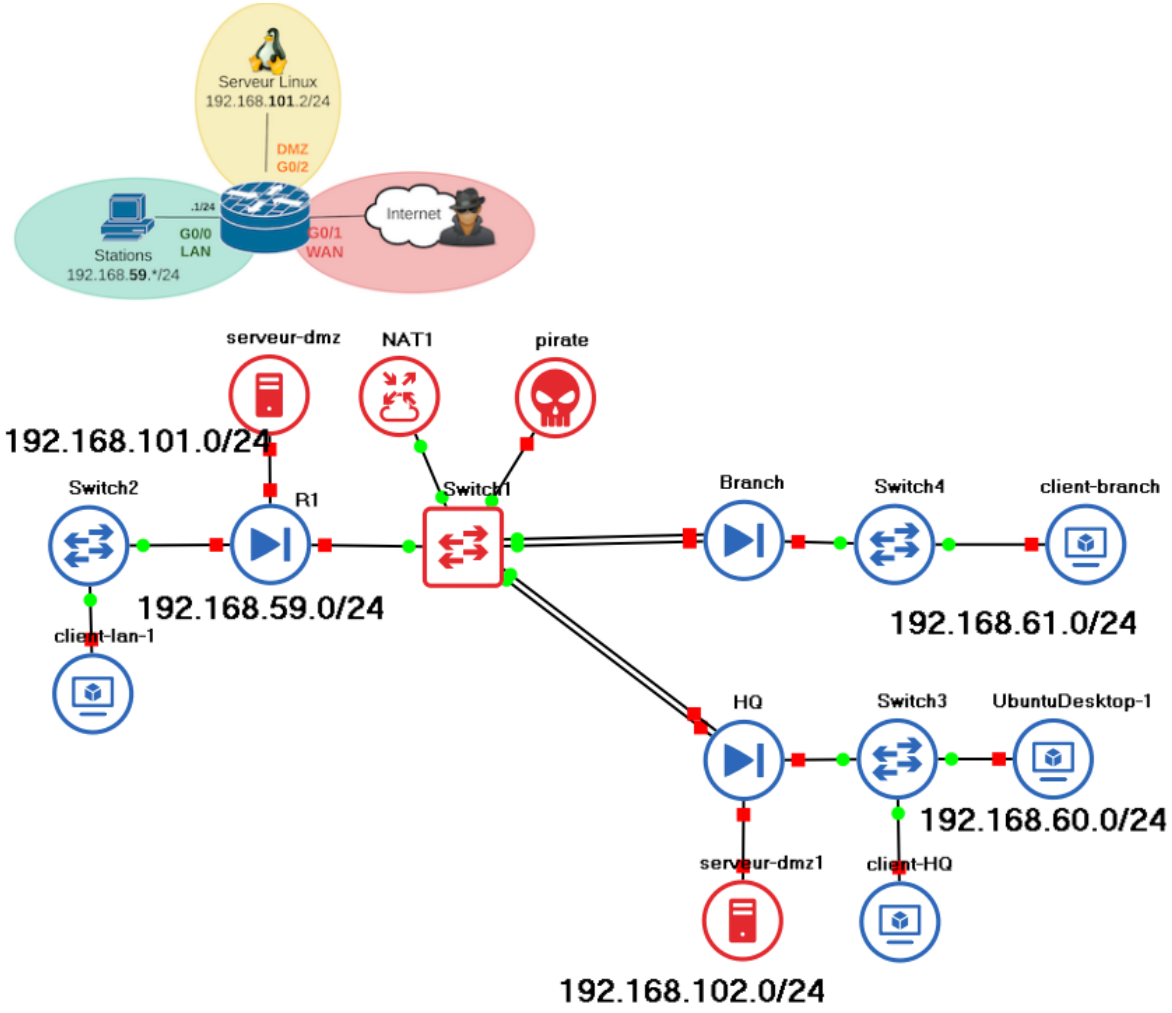
4/ Montrer la connectivité entre le LAN HQ (60.0/24) et le LAN Branch (61.0/24) et inversement via des tests pings et des logs.

5/ Quels sont les paramètres IPSEC utilisés par le Wizard ? Comment obtenir cette information.

6/ Exporter sa config et la livrer sur un repo github

Ouvrir GNS3, le projet « 2020-05-04-lab-ipsec-fortinet-2 »

Topologie à l'ouverture GNS3



1/ Vérifier la configuration de HQ (nom et connectivité)

HQ : HeadQuaters : Quartier Général

Ouvrir la console de HQ. Admin : login Password : testtest

Pour vérifier les interfaces :

#get system interface physical

```
HQ-18 # get system interface physical
== [onboard]
        ==[port1]
                mode: dhcp
                ip: 192.168.122.233 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port2]
                mode: dhcp
                ip: 192.168.122.234 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port3]
                mode: static
                ip: 192.168.60.1 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port4]
                mode: static
                ip: 192.168.102.1 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
```

IP à entrer dans l'interface Web Fortigate : **192.168.122.233**

Login : admin Password : testtest

Rappel :

Le port 1 port de contrôle/ de gestion

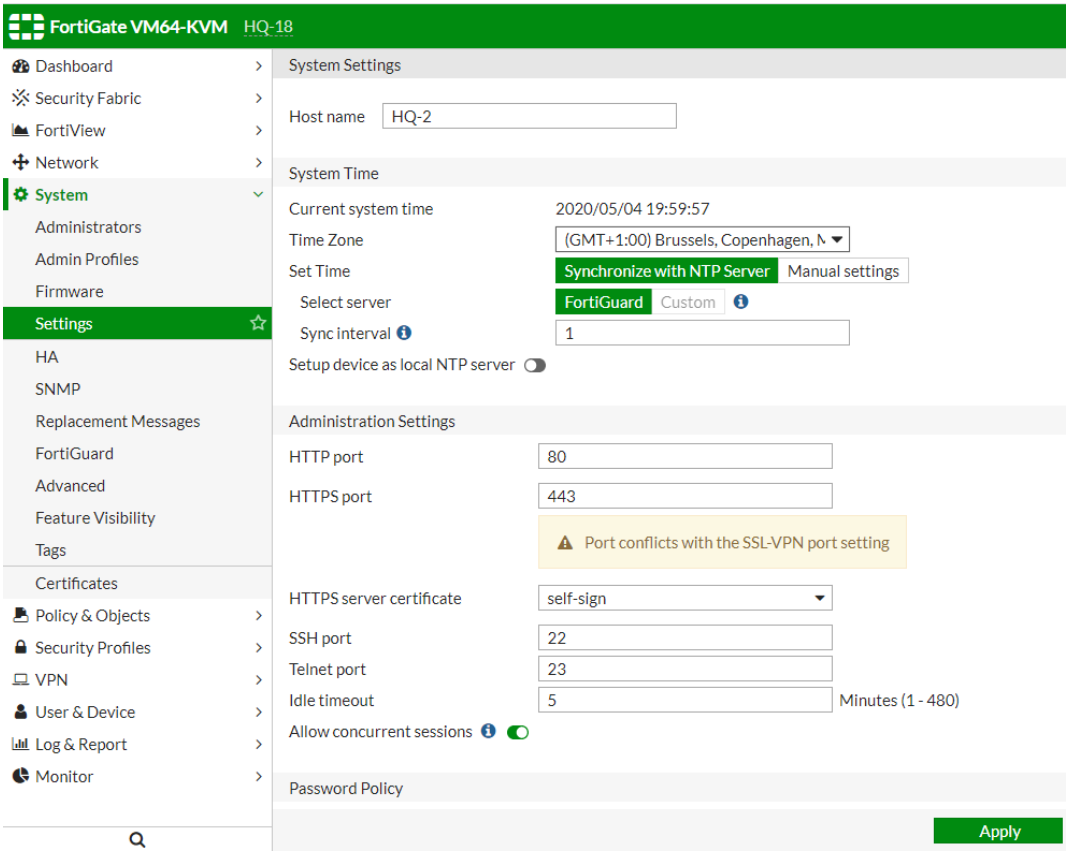
Port 2 port internet

Port 3 LAN

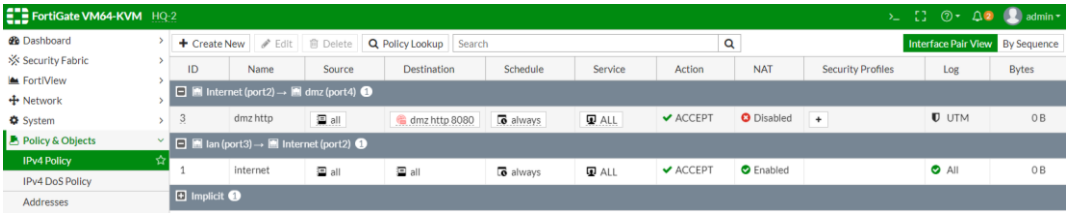
A partir de l'interface Web : **System -> Settings ->**

Nom : **Hostname** : HQ-2

Zone horaire : **Time Zone** : (GMT+1:00) : Paris



Policy & Objects -> IPv4 Policy




```
HQ-2 # execute ping 192.168.122.233
PING 192.168.122.233 (192.168.122.233): 56 data bytes
64 bytes from 192.168.122.233: icmp_seq=0 ttl=255 time=0.1 ms
64 bytes from 192.168.122.233: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 192.168.122.233: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.122.233: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 192.168.122.233: icmp_seq=4 ttl=255 time=0.0 ms

--- 192.168.122.233 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms

HQ-2 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=56 time=2.4 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=2.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=2.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=2.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=2.1 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.1/2.4/2.6 ms
```

2/ Configurer Branch : Nom, interfaces, service DHCP, NAT, Policy

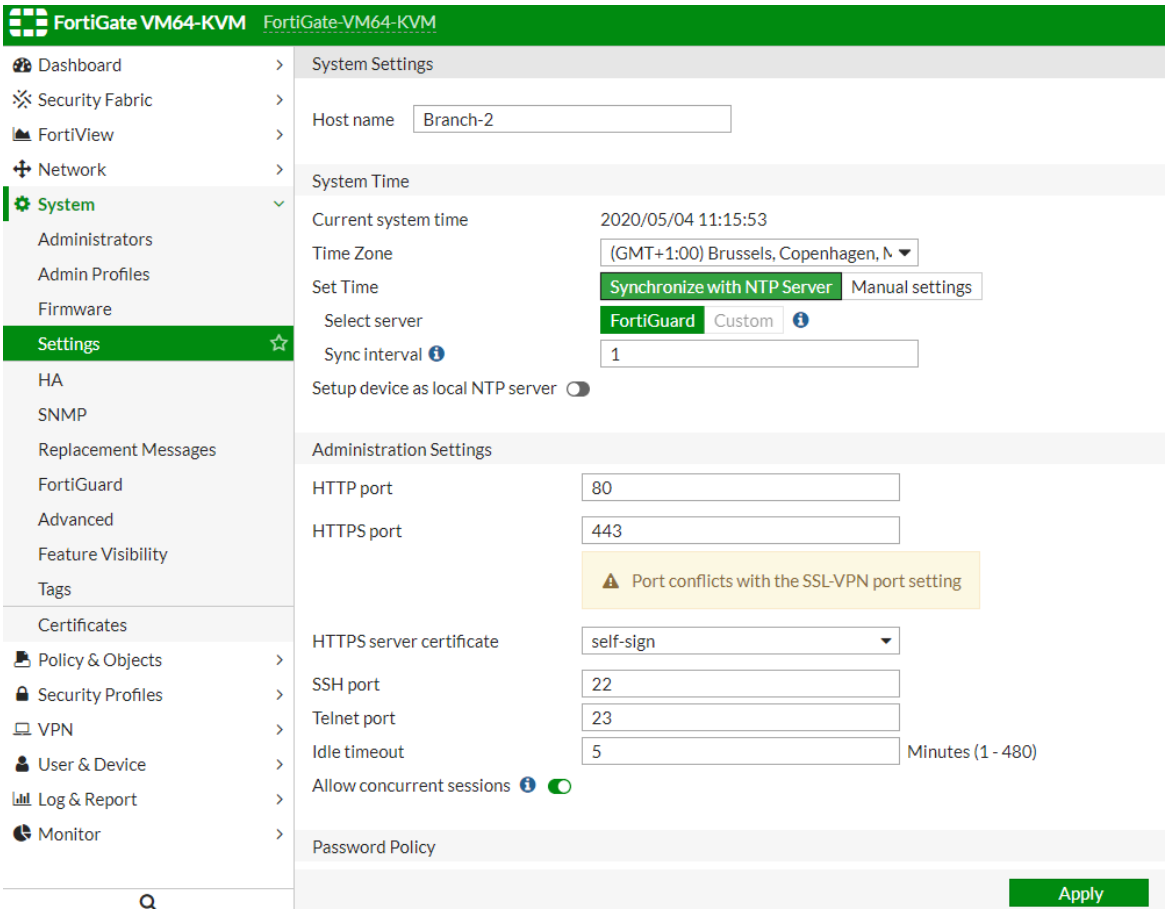
Ouvrir la console Branch. Login : admin Password : aucun !

```
FortiGate-VM64-KVM # get system interface physical
== [onboard]
        ==[port1]
                mode: dhcp
                ip: 192.168.122.62 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port3]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port4]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
```

A partir de l'interface Web : **System -> Settings ->**

Nom : **Hostname** : Branch-2

Zone horaire : **Time Zone** : (GMT+1:00) : Paris



Network -> Interfaces ->

Port 1 : port de gestion.

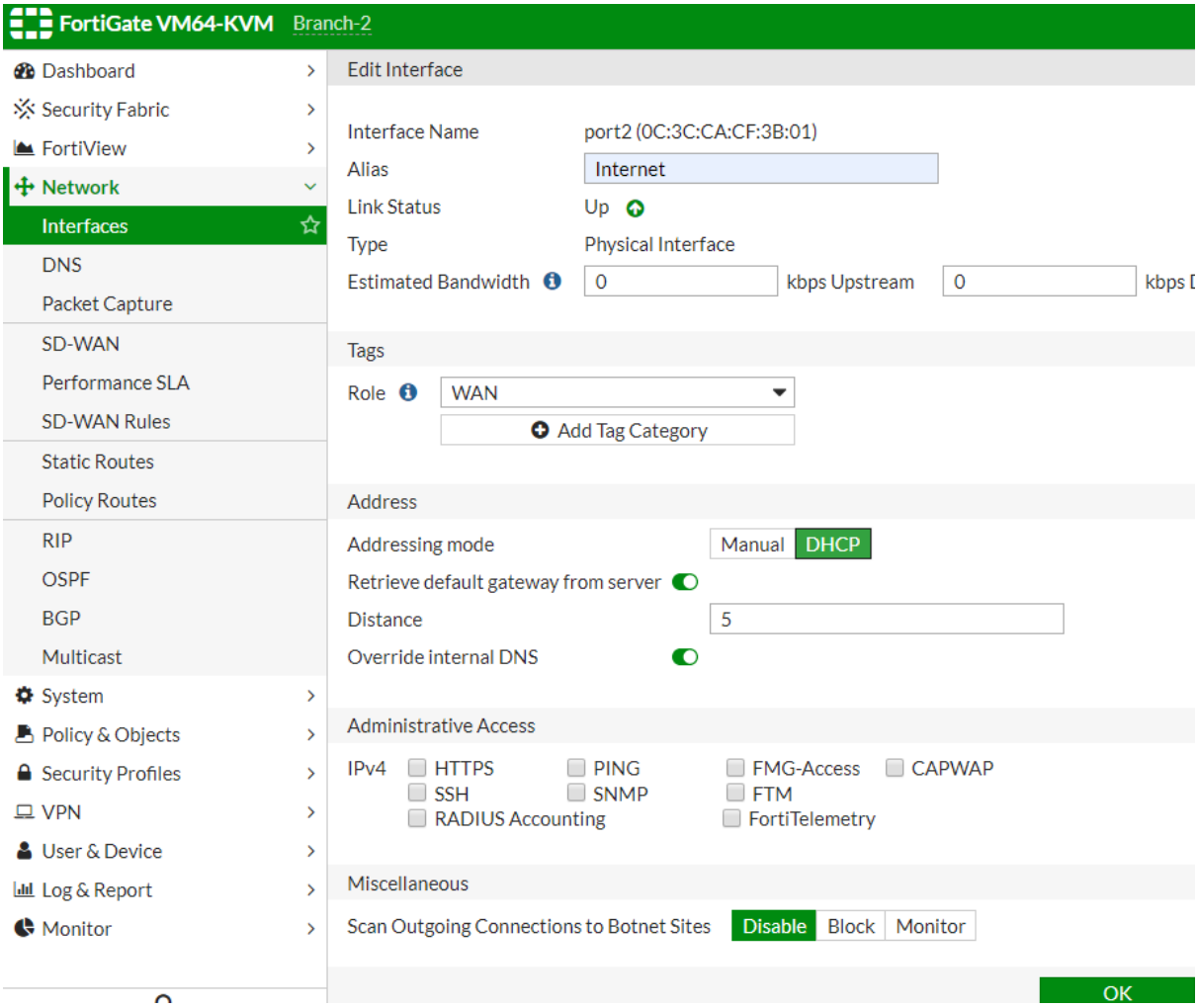
Déjà configuré, vérification IP et Adminsitrative Access. Il est configuré en DHCP.

Port 2 : Internet

IP 192.168.59.1/255.255.255.0

Alias : Internet

Type -> Role : WAN



Port 3 : le LAN.

IP 192.168.61.1/255.255.255.0

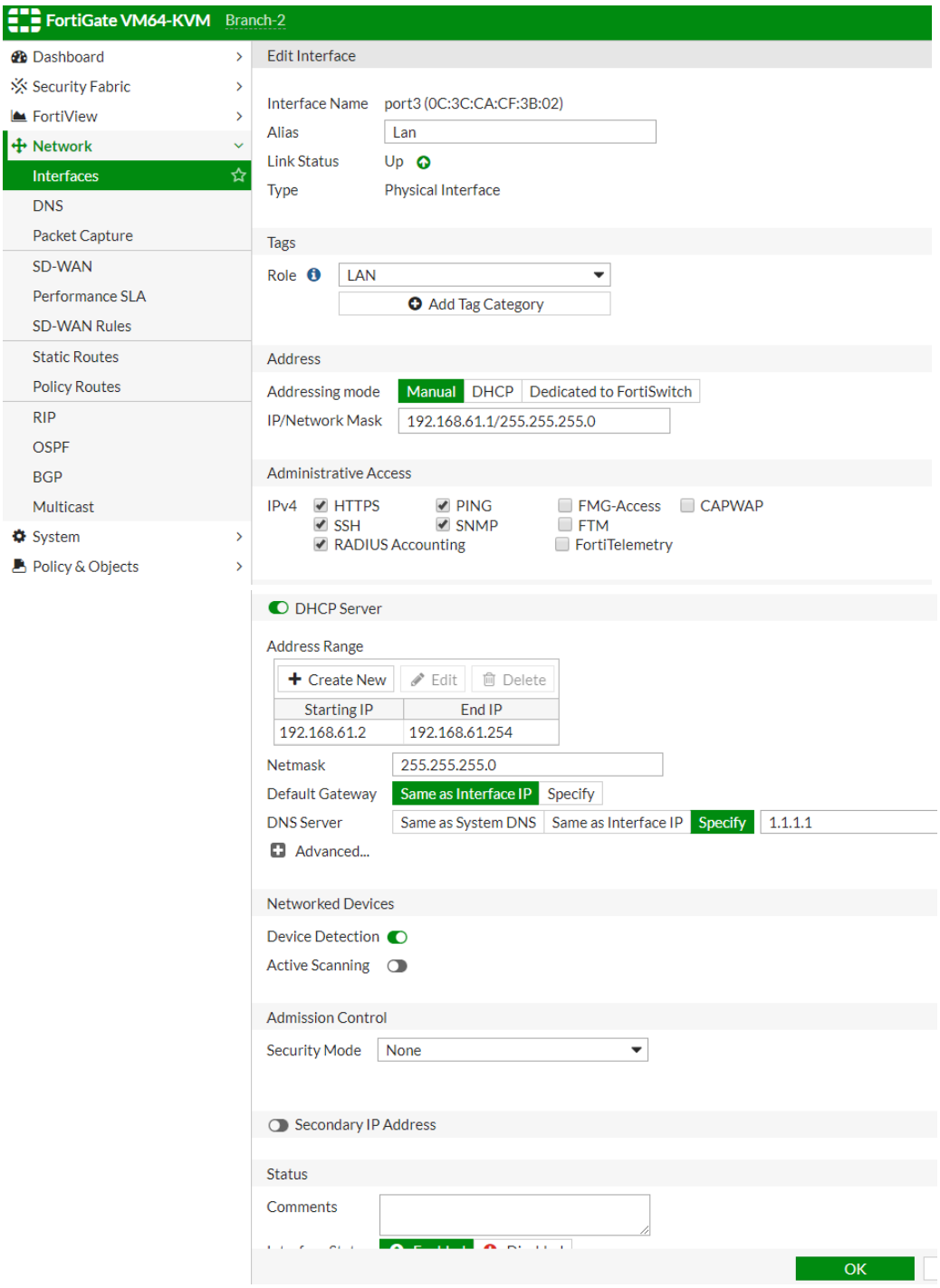
Alias : LAN

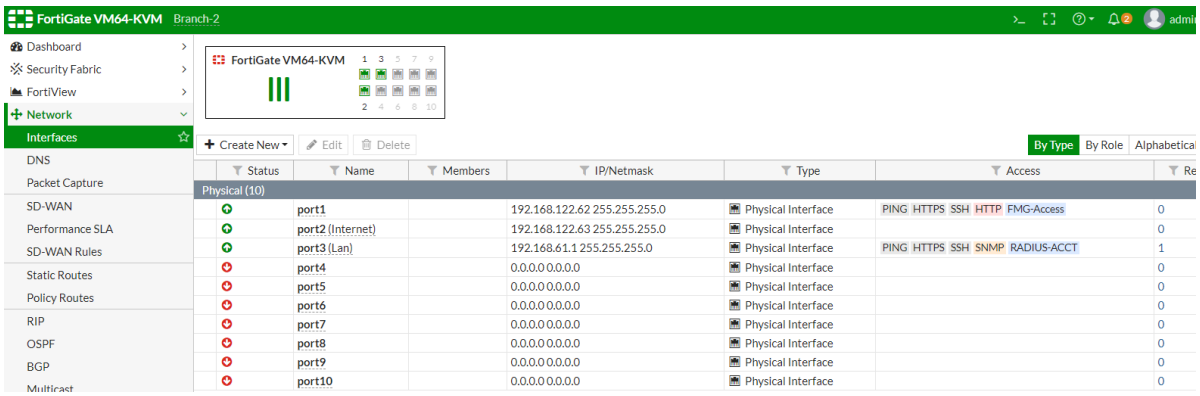
Type -> Role : LAN

Administrative Access : HTTPS, PING, SSH, SNMP, RADIUS Accounting

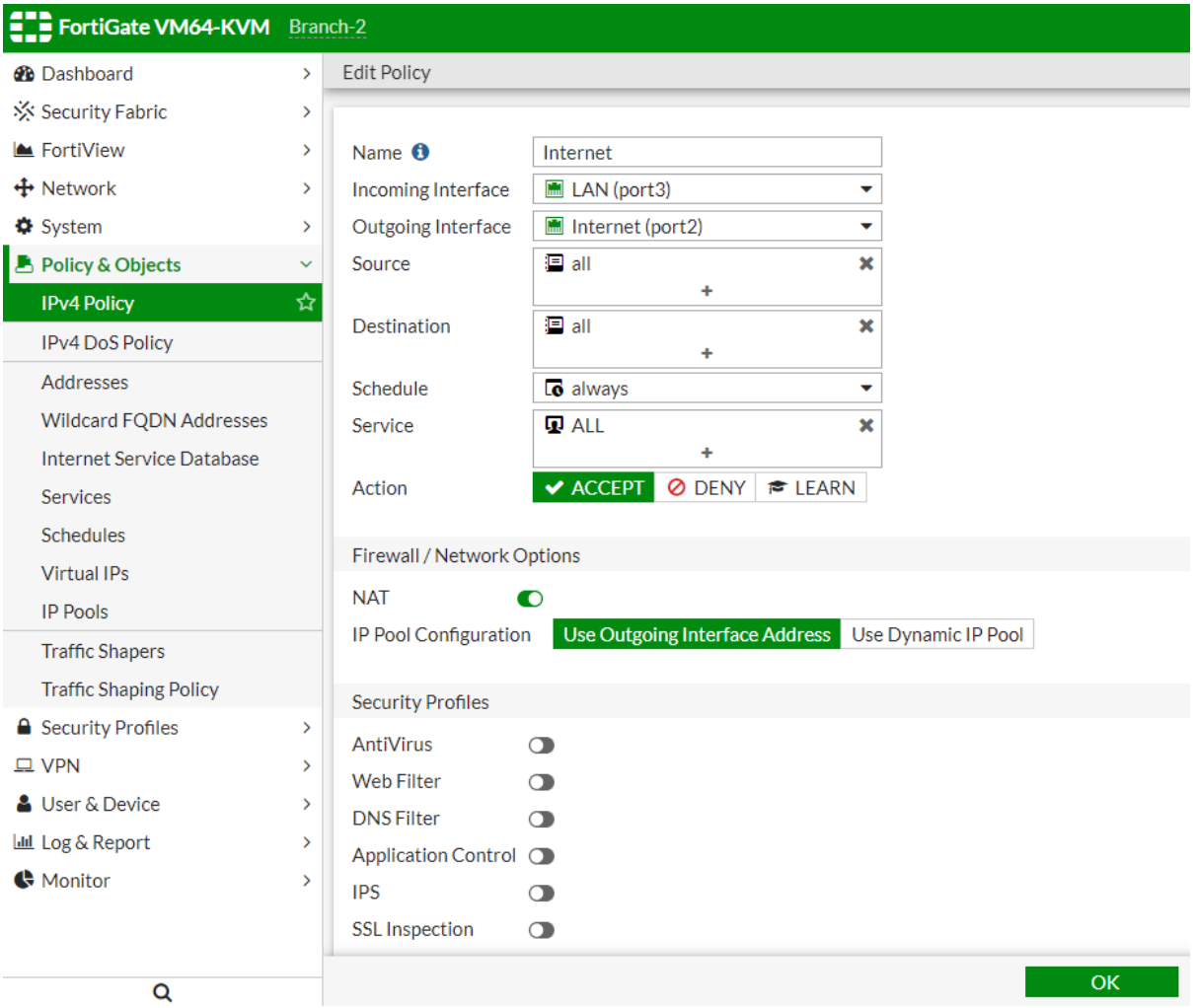
Cocher DHCP Server.

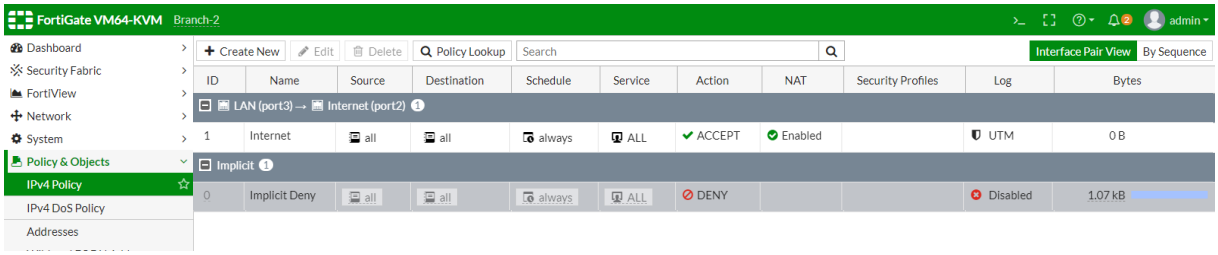
DSN Server – Specify **1.1.1.1**





Policy & Objects -> Ipv4 Policy -> Create New



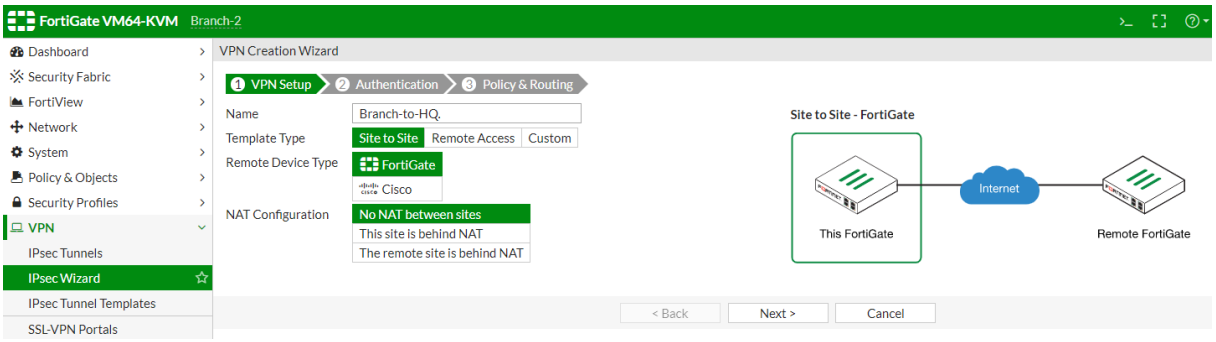


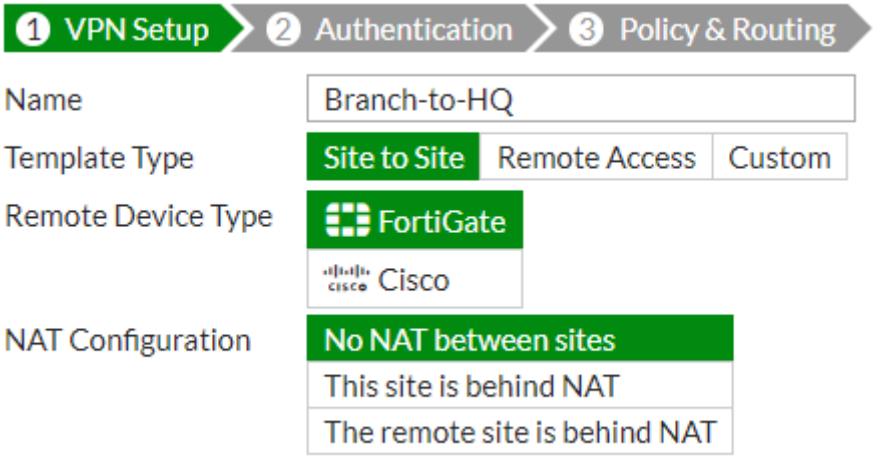
3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard

https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/783623/configuring-ipsec-vpn-on-hq

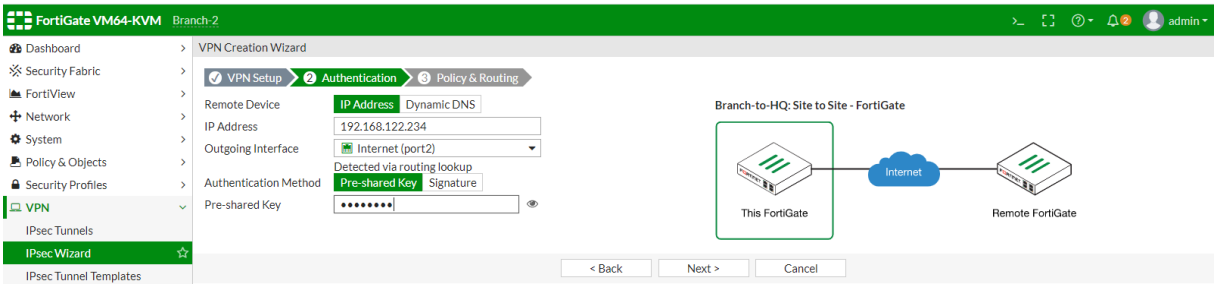
VPN -> IPsec Wizard

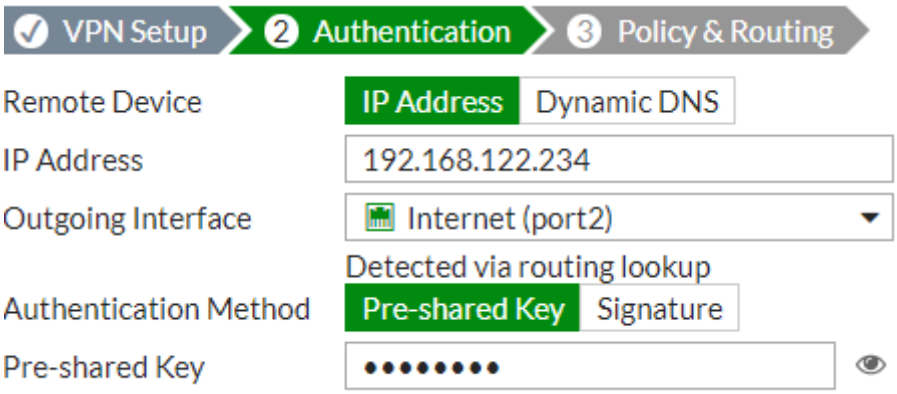
- Branch-to-HQ



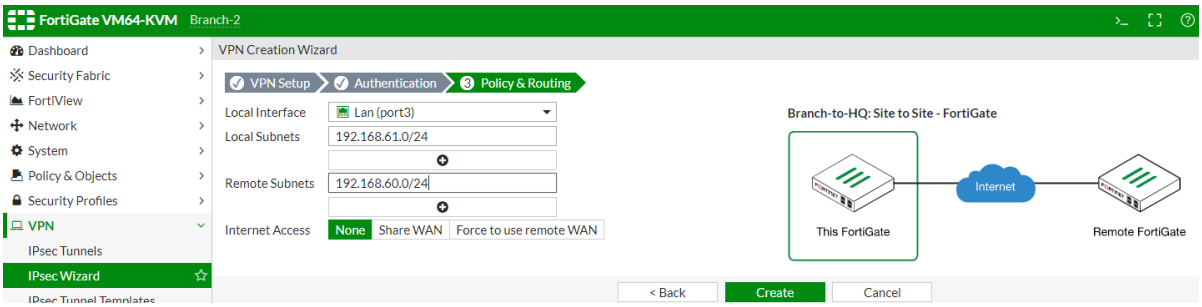


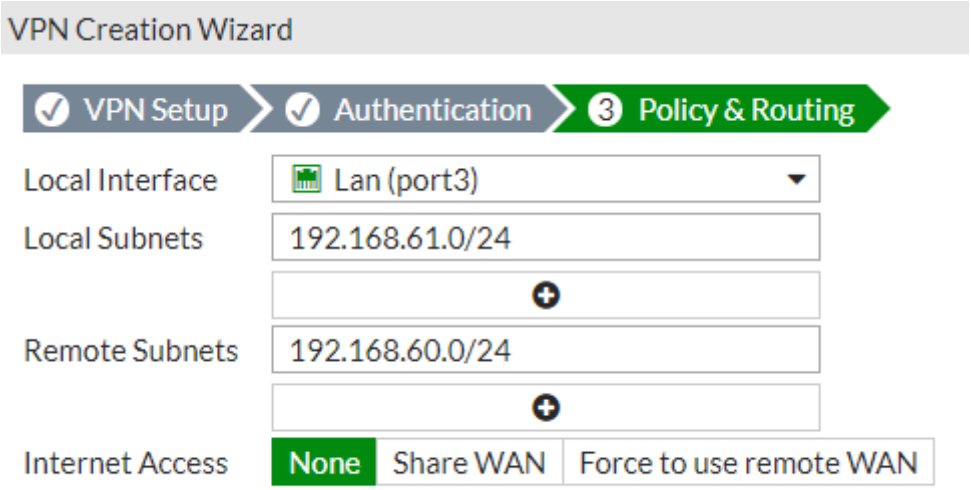
Pour IP Address, vérifier dans Network Interface de HQ Port 2 : **192.168.122.234**

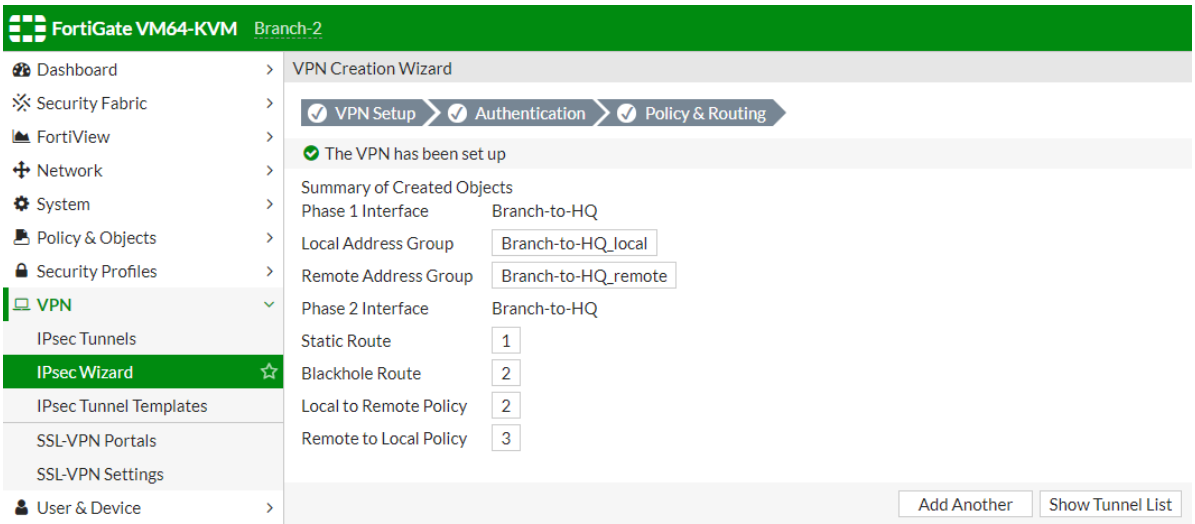




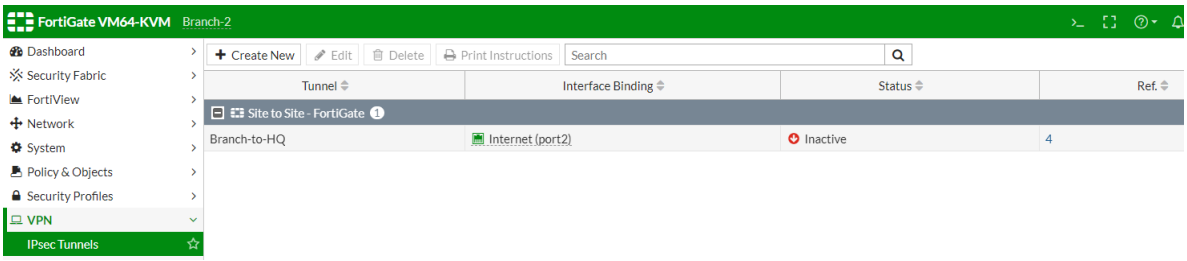
Local Interface : Port 3 **Local Subnets: 60.0** **Remote Subnets : 61.0**



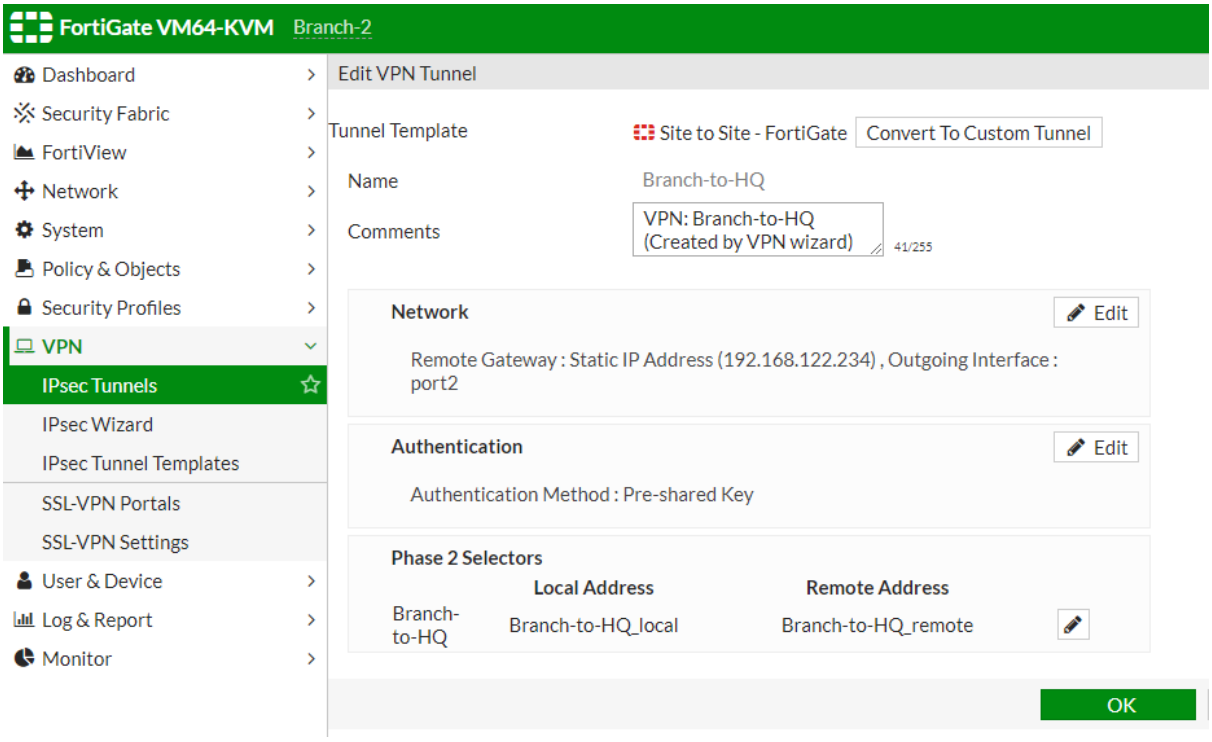




Cliquer sur **Show Tunnel List** : (ou **VPN -> IPsec Tunnels**)

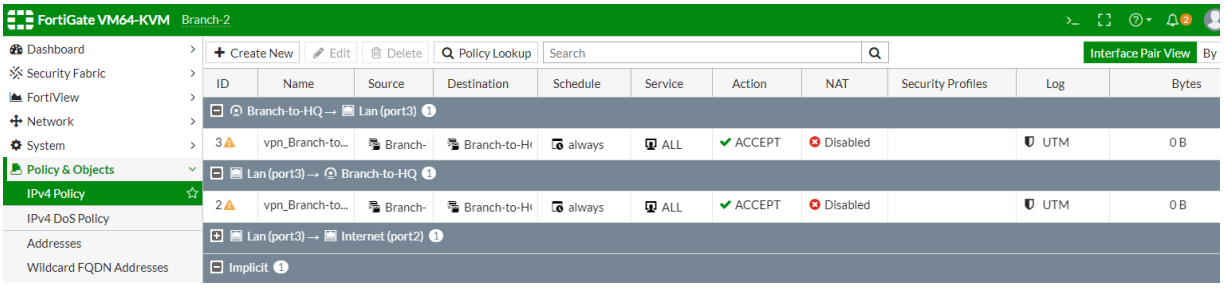


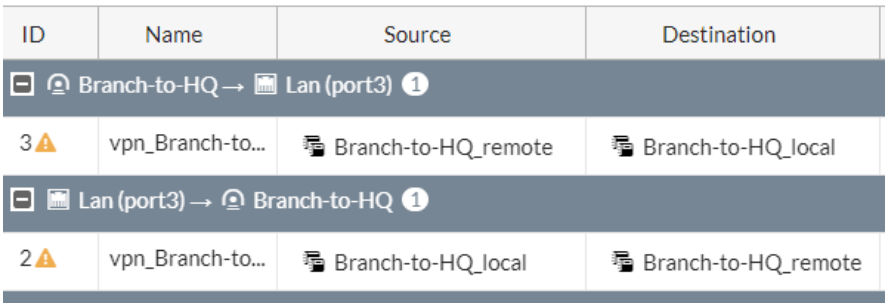
Double-cliquer sur Branch-to-HQ :



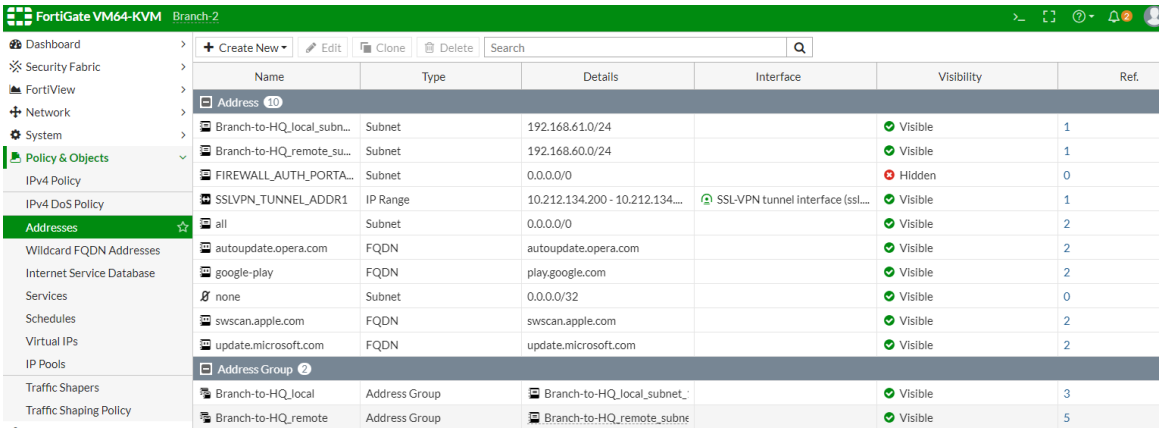
Pour vérifier si la config est bien présente, deux solutions :

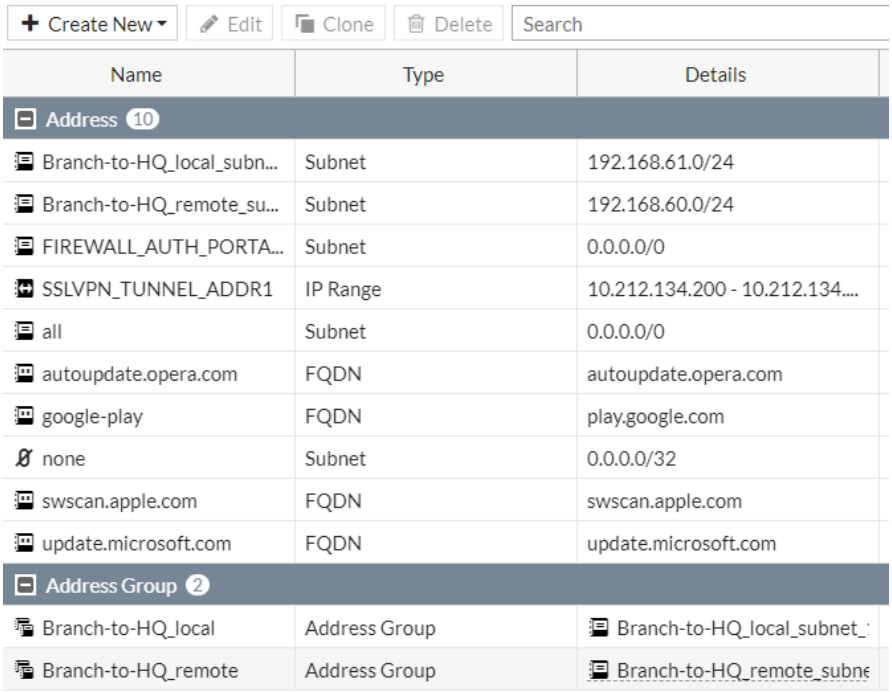
- **Policy & Objects -> IPv4 Policy** (2 policies crées);



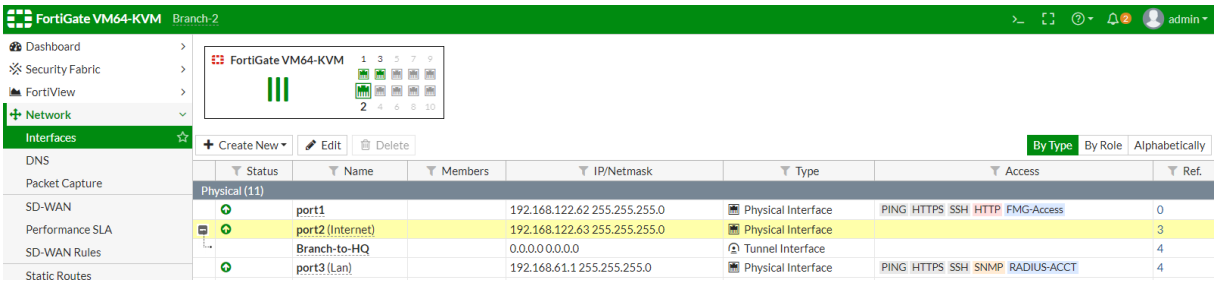


➢ **Policy&Objects -> Addresses** (2 subnets configurés)

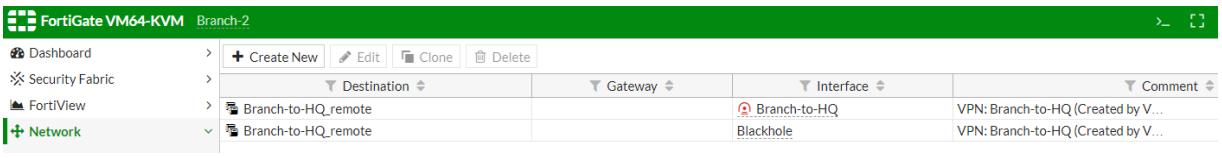




➢ **Network -> Interfaces** sous le port WAN on a bien une sous interface HQ-to-Branch



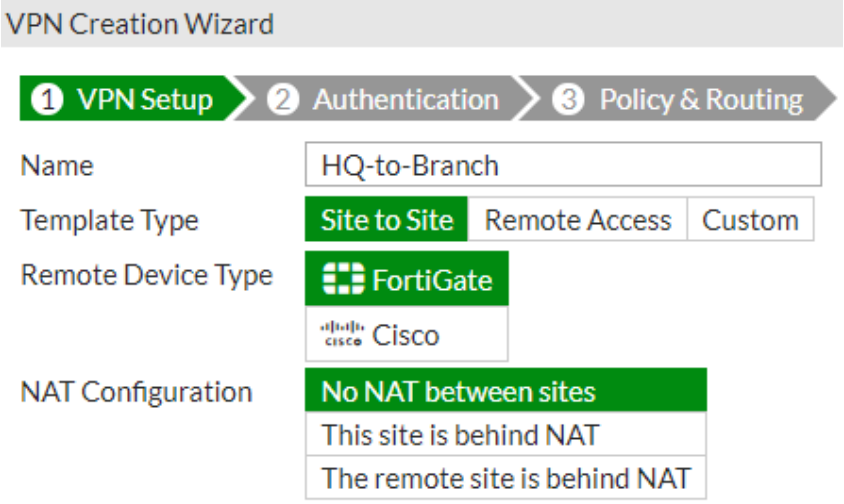
➢ **Network --> Static Routes** (2 routes)

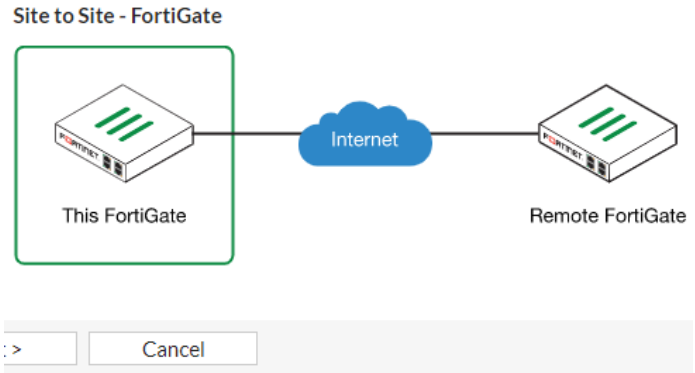


➢ HQ-to-branch

VPN -> IPsec Wizard

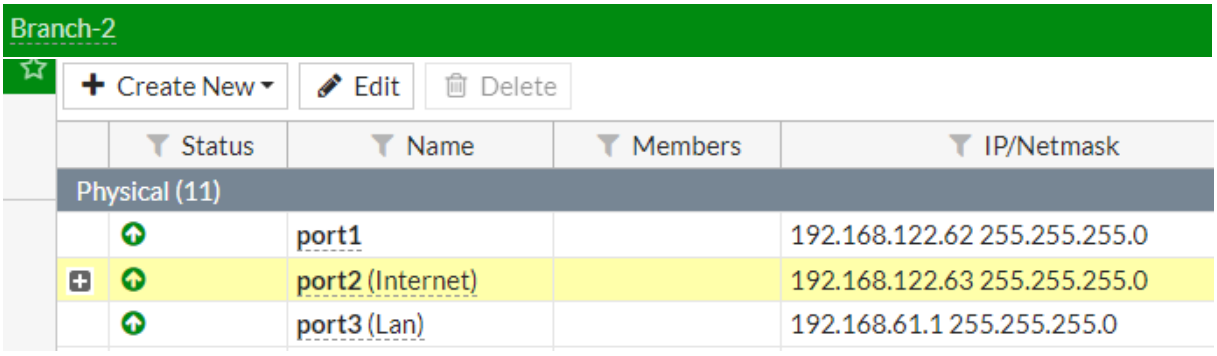
- Etape 1

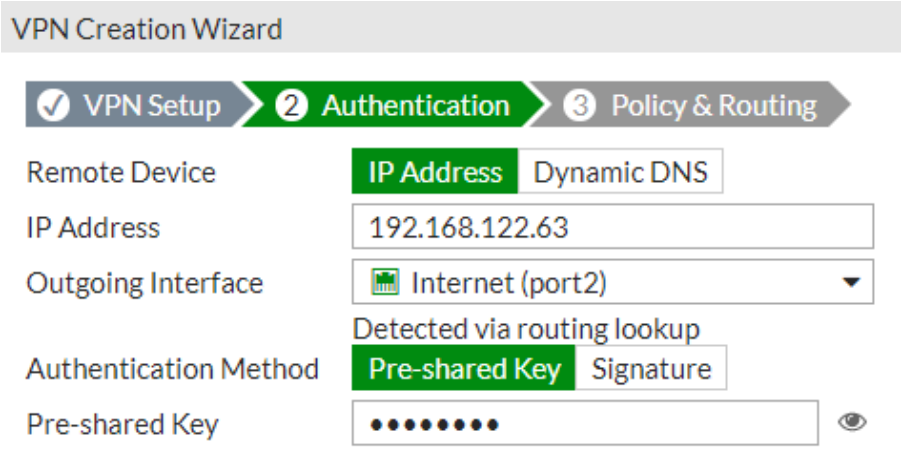




- Etape 2

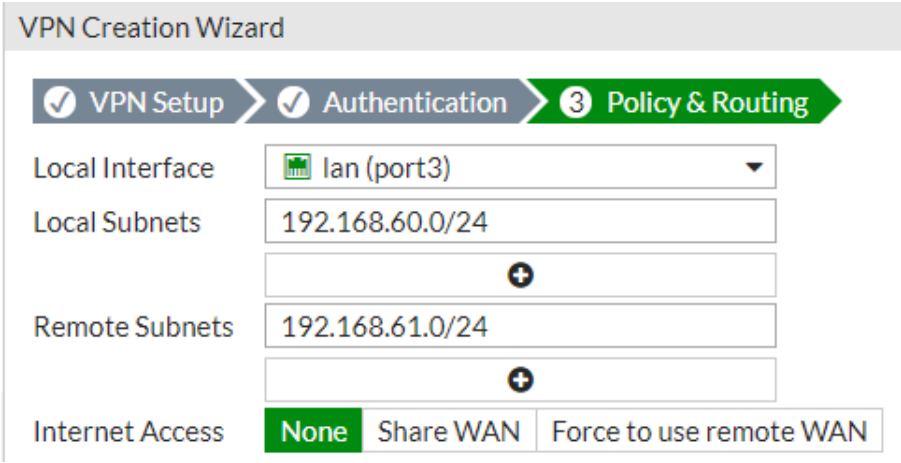
L'IP Address est nécessaire : vérifier dans Network Interface IP de Branch Port 2 : **192.168.122.63**



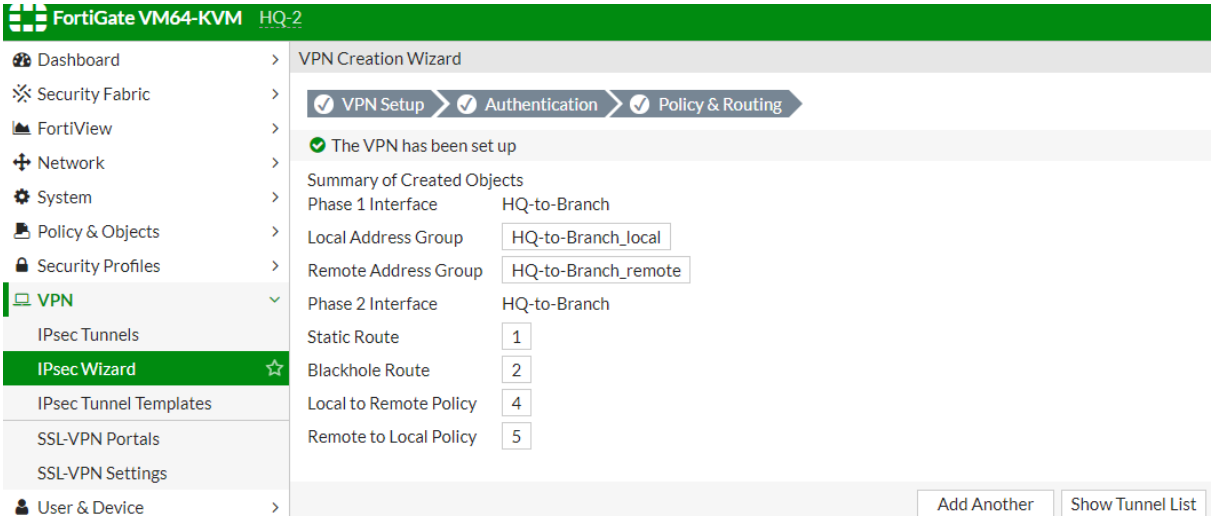


- Etape 3

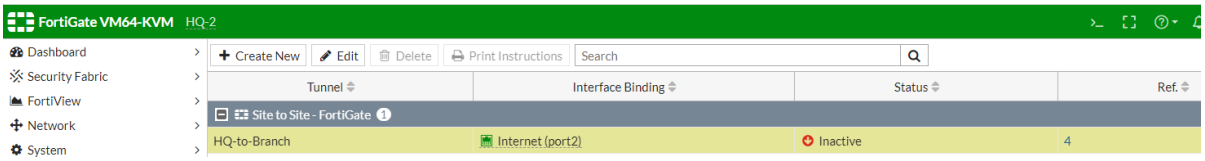
Local Interface : Port 3 **Local Subnets: 60.0** **Remote Subnets : 61.0**



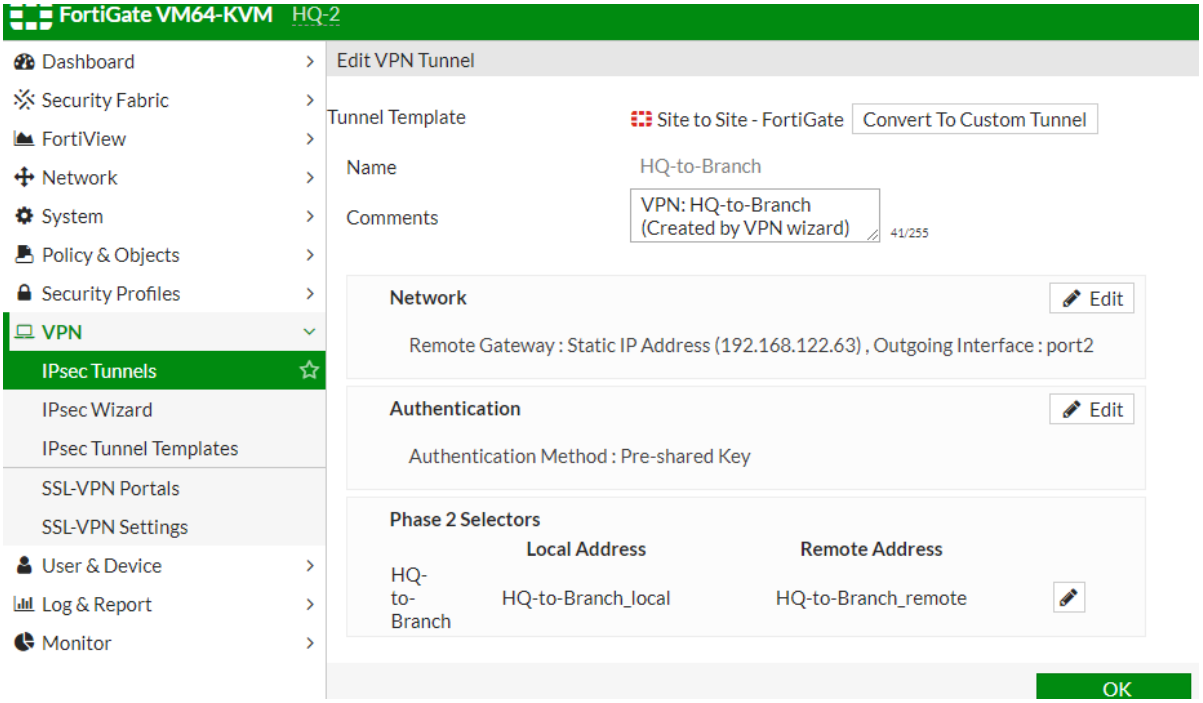
- Etape 4



Cliquer sur **Show Tunnel List** : (ou **VPN -> IPsec Tunnels**)

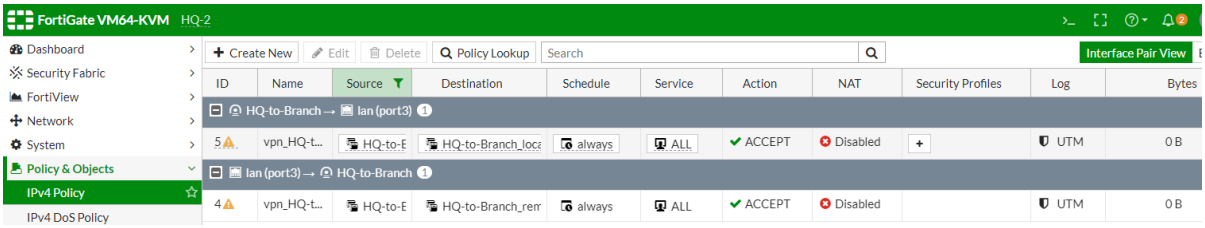


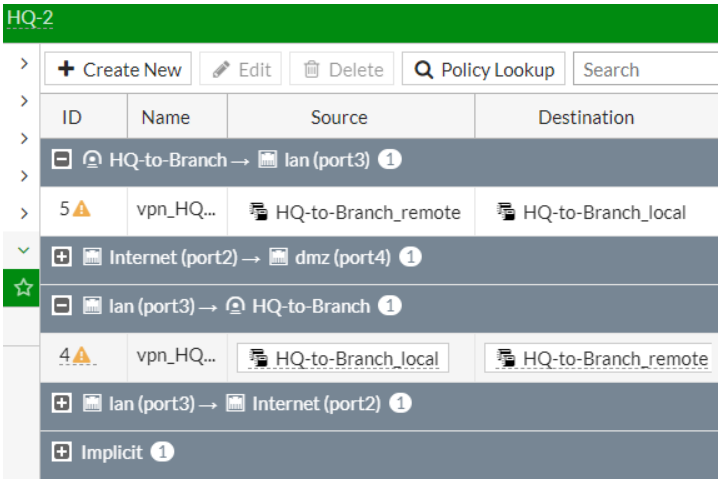
Double-cliquer sur Branch-to-HQ :



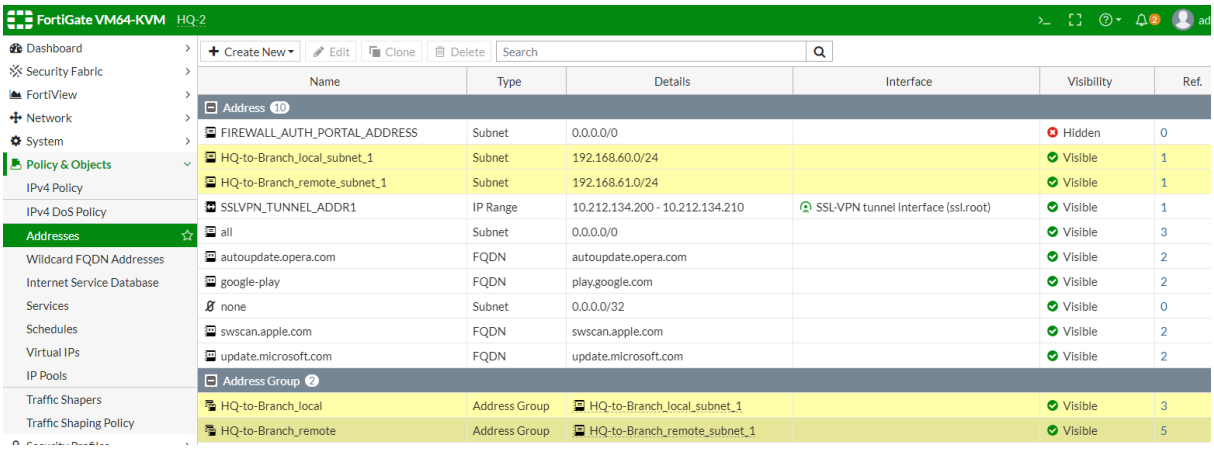
Pour vérifier si la config est bien présente, deux solutions :

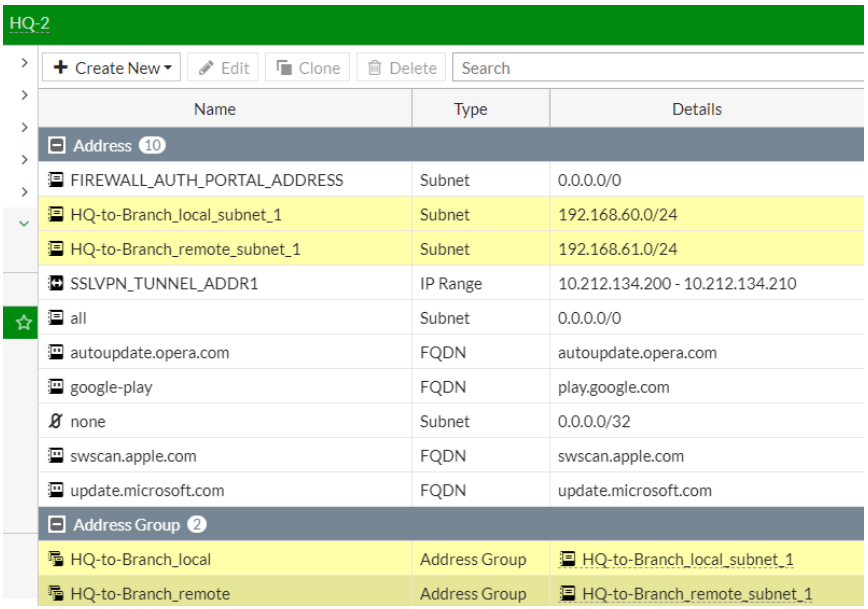
- **Policy&Objects -> IPv4 Policy** (2 policies crées);



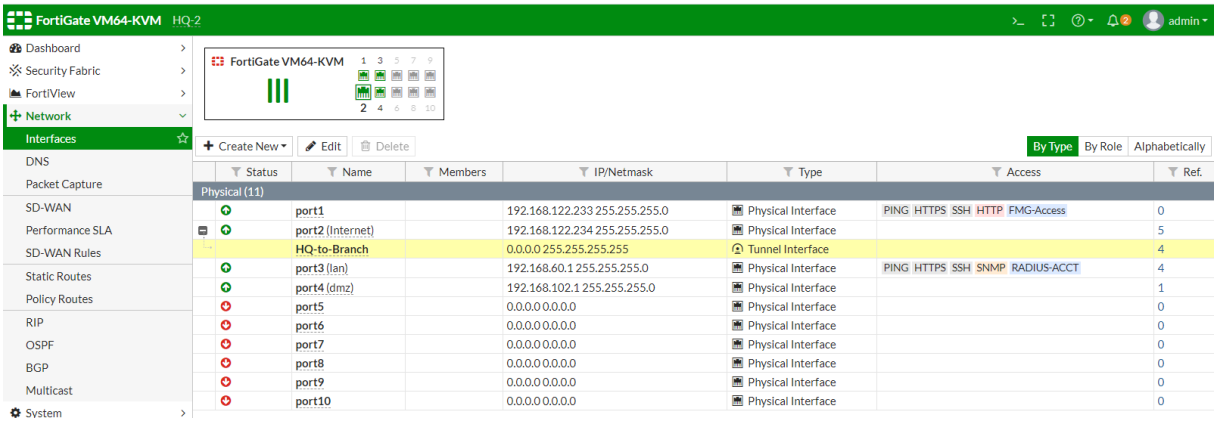


➢ **Policy&Objects -> Addresses** (2 subnets configurés)

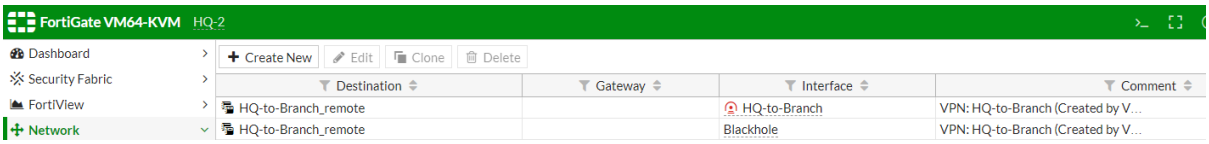




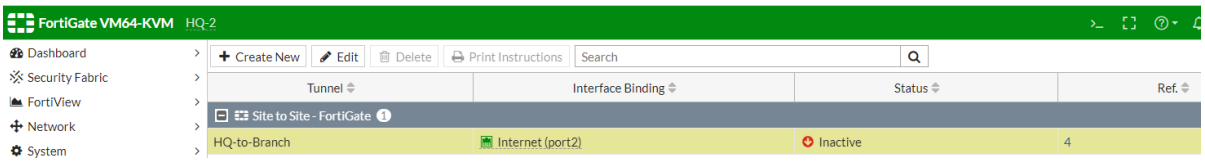
➢ **Network -> Interfaces** sous le port WAN on a bien une sous interface HQ-to-Branch



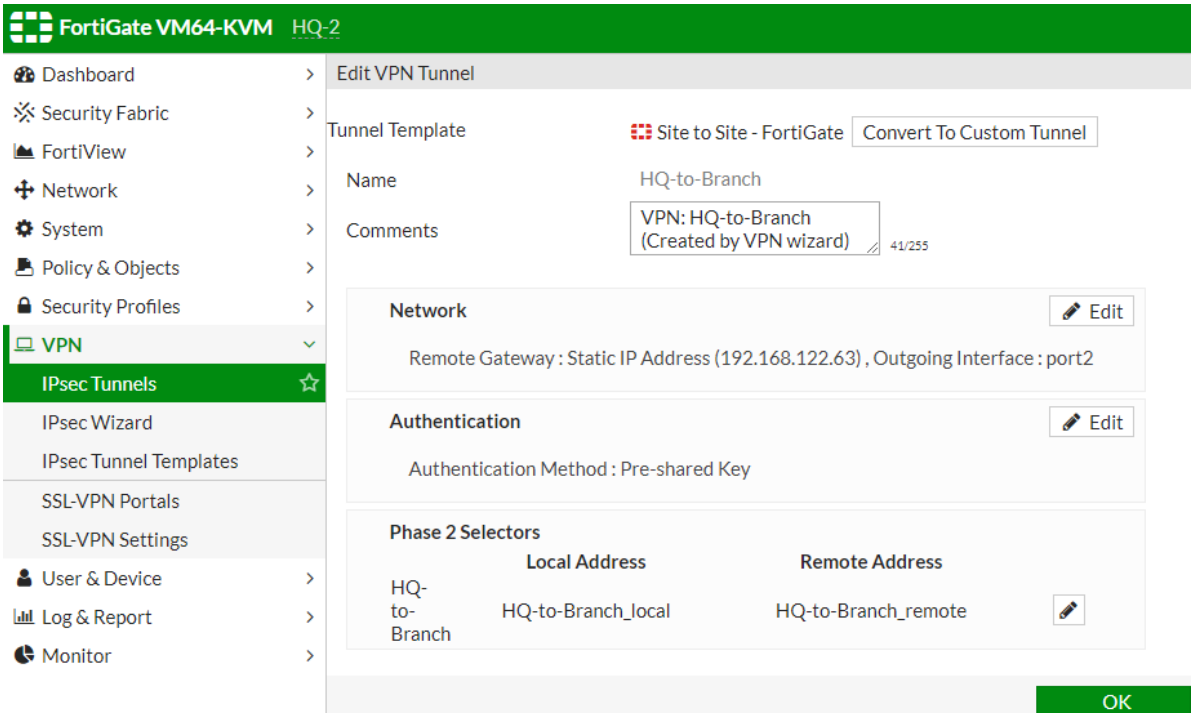
➢ **Network --> Static Routes** (2 routes)



➢ **VPN -> Ipsec Tunnels**



On double-clique :



4/ Montrer la connectivité entre le LAN HQ (60.0/24) et le LAN Branch (61.0/24) et inversement via des tests pings et des logs.

Pour accéder aux consoles Client-branch et Client-HQ,

Login : root

Password : testtest

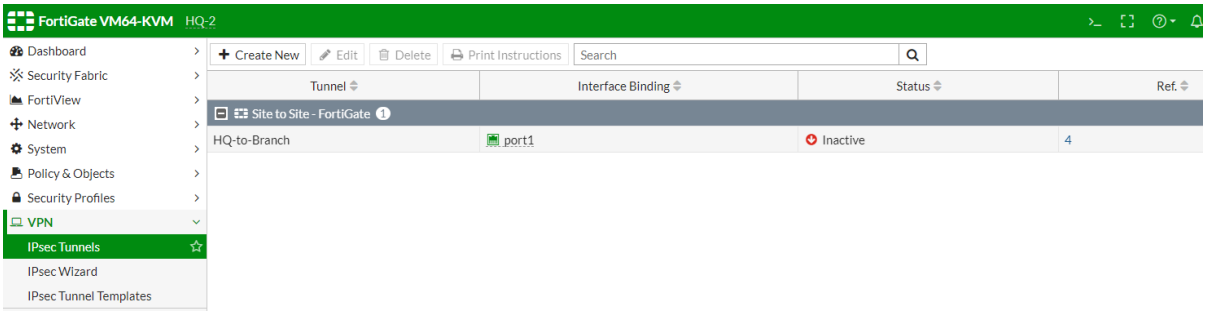
Pour monter la connectivité on crée du trafic depuis un poste du LAN de HQ on ping un poste du LAN de Branch et inversement.

```
[root@client-branch ~]# ping 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.
64 bytes from 192.168.60.1: icmp_seq=1 ttl=254 time=2.60 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=254 time=2.11 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=254 time=1.98 ms
64 bytes from 192.168.60.1: icmp_seq=4 ttl=254 time=1.92 ms
64 bytes from 192.168.60.1: icmp_seq=5 ttl=254 time=2.12 ms
64 bytes from 192.168.60.1: icmp_seq=6 ttl=254 time=2.03 ms
64 bytes from 192.168.60.1: icmp_seq=7 ttl=254 time=2.26 ms

--- 192.168.60.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 1.921/2.148/2.601/0.216 ms
```

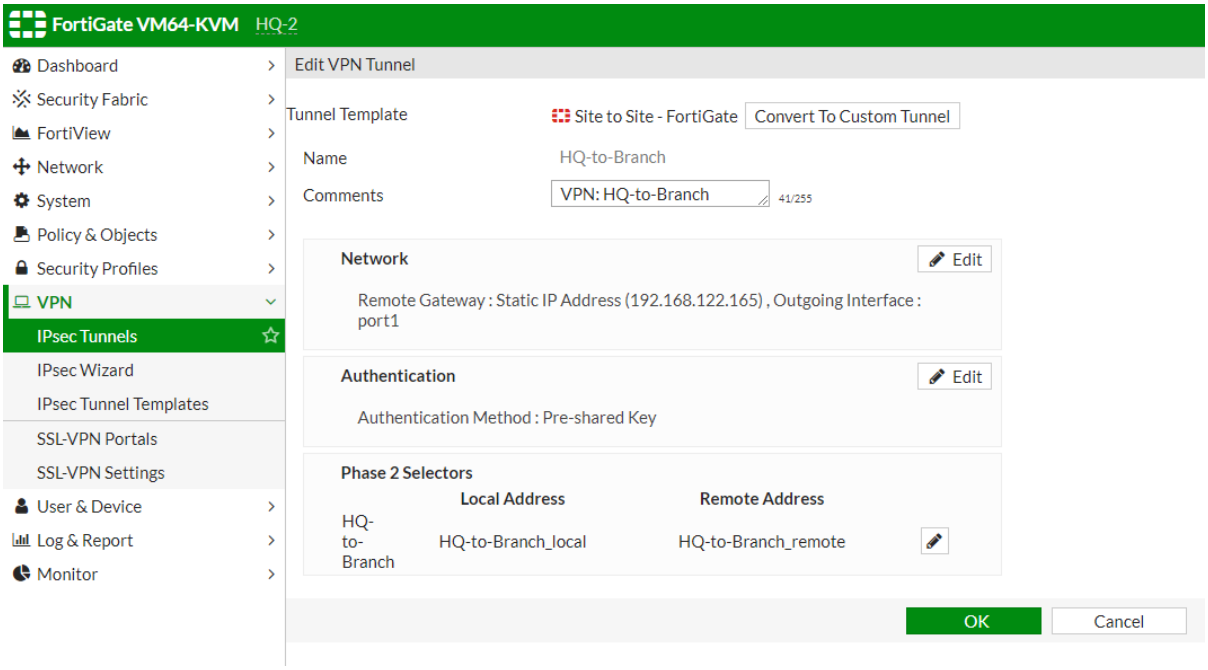
```
[root@client-hq ~]# ping 192.168.61.1
PING 192.168.61.1 (192.168.61.1) 56(84) bytes of data.
64 bytes from 192.168.61.1: icmp_seq=1 ttl=254 time=3.43 ms
64 bytes from 192.168.61.1: icmp_seq=2 ttl=254 time=2.33 ms
64 bytes from 192.168.61.1: icmp_seq=3 ttl=254 time=2.16 ms
64 bytes from 192.168.61.1: icmp_seq=4 ttl=254 time=2.13 ms
64 bytes from 192.168.61.1: icmp_seq=5 ttl=254 time=2.21 ms
64 bytes from 192.168.61.1: icmp_seq=6 ttl=254 time=2.05 ms
64 bytes from 192.168.61.1: icmp_seq=7 ttl=254 time=2.02 ms
64 bytes from 192.168.61.1: icmp_seq=8 ttl=254 time=2.12 ms

--- 192.168.61.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.025/2.309/3.434/0.438 ms
```

5/ Quels sont les paramètres IPSEC utilisés par le Wizard ? Comment obtenir cette information.

Dans VPN -> Ipsec tunnel,

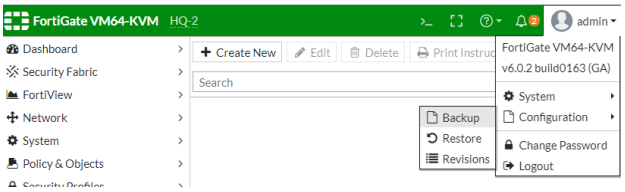


On double-clique :



Pour télécharger la configuration, aller an haut à droite de l'écran,

Admin -> Configuration -> Back up



Fichier à télécharger :

Branch-2-

HQ-2