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 inversément 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

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

On execute la commande

HQ-18 # get system interface physical

Ip de HQ : 192.168.122.57

```
maxime — HQ — telnet 172.16.253.1 5526 — 80×41
voip                    VoIP configuration.
vpn                     VPN configuration.
waf                     Web Application Firewall configuration.
wanopt                  WAN optimization configuration.
web-proxy               Web proxy configuration.
webfilter               Web filter configuration.
wireless-controller     Wireless access point configuration.

HQ-18 # get system interface physical
== [onboard]
        ==[port1]
                mode: dhcp
                ip: 192.168.122.57 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
        ==[port2]
                mode: dhcp
                ip: 192.168.122.58 255.255.255.0
                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)
        ==[port5]
```

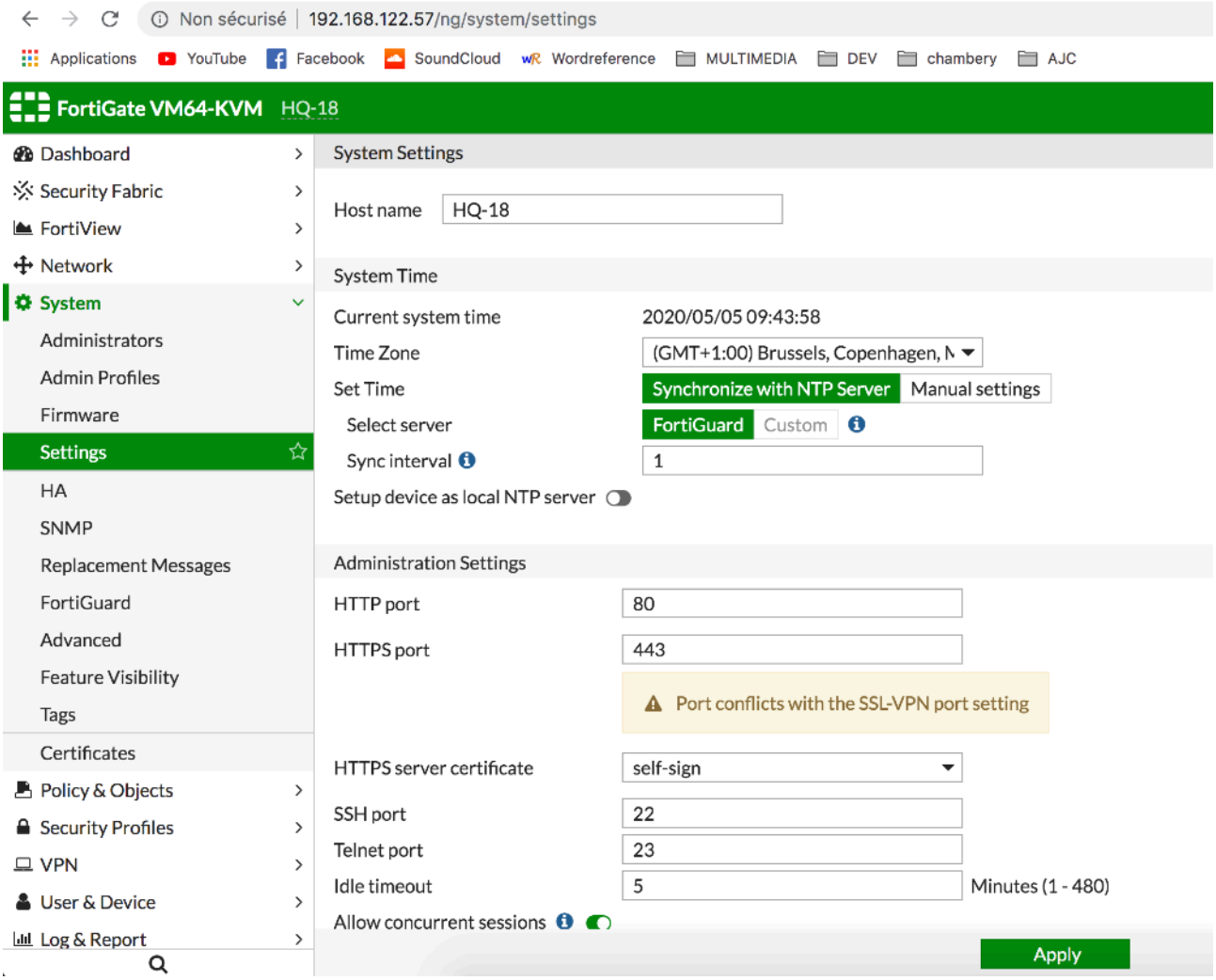
Connection sur le portail fortigate :

http://192.168.122.57

Changement du nom de l’hôte :

HQ-18 (global) # set hostname HQ-9

Vérification des informations sur l’interface fortigate :



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

Récupération de l'IP :

FortiGate-VM64-KVM # get system interface physical

maxime — Branch — telnet 172.16.253.1 5537 — 80×24

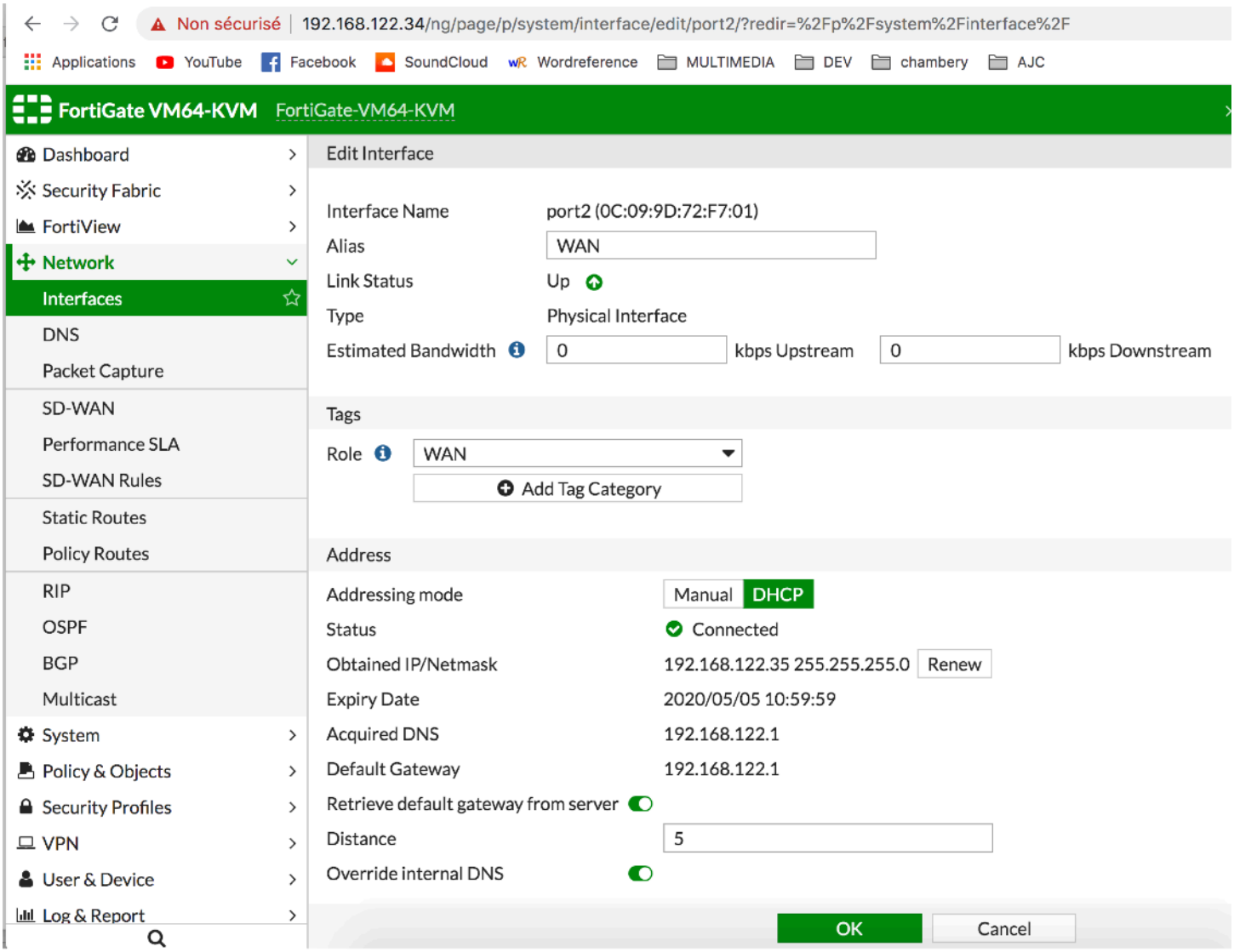
```
ing.
Please run 'execute disk scan 17'
Note: The device will reboot and scan during startup. This may take up to an hou
r
FortiGate-VM64-KVM # get system interface physical
== [onboard]
        ==[port1]
                mode: dhcp
                ip: 192.168.122.34 255.255.255.0
                ipv6: ::/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)
```

Pour le port 2 :

Alias : WAN

Rôle : WAN

DCHP activé.



Pour le port 3 :

Alias : LAN

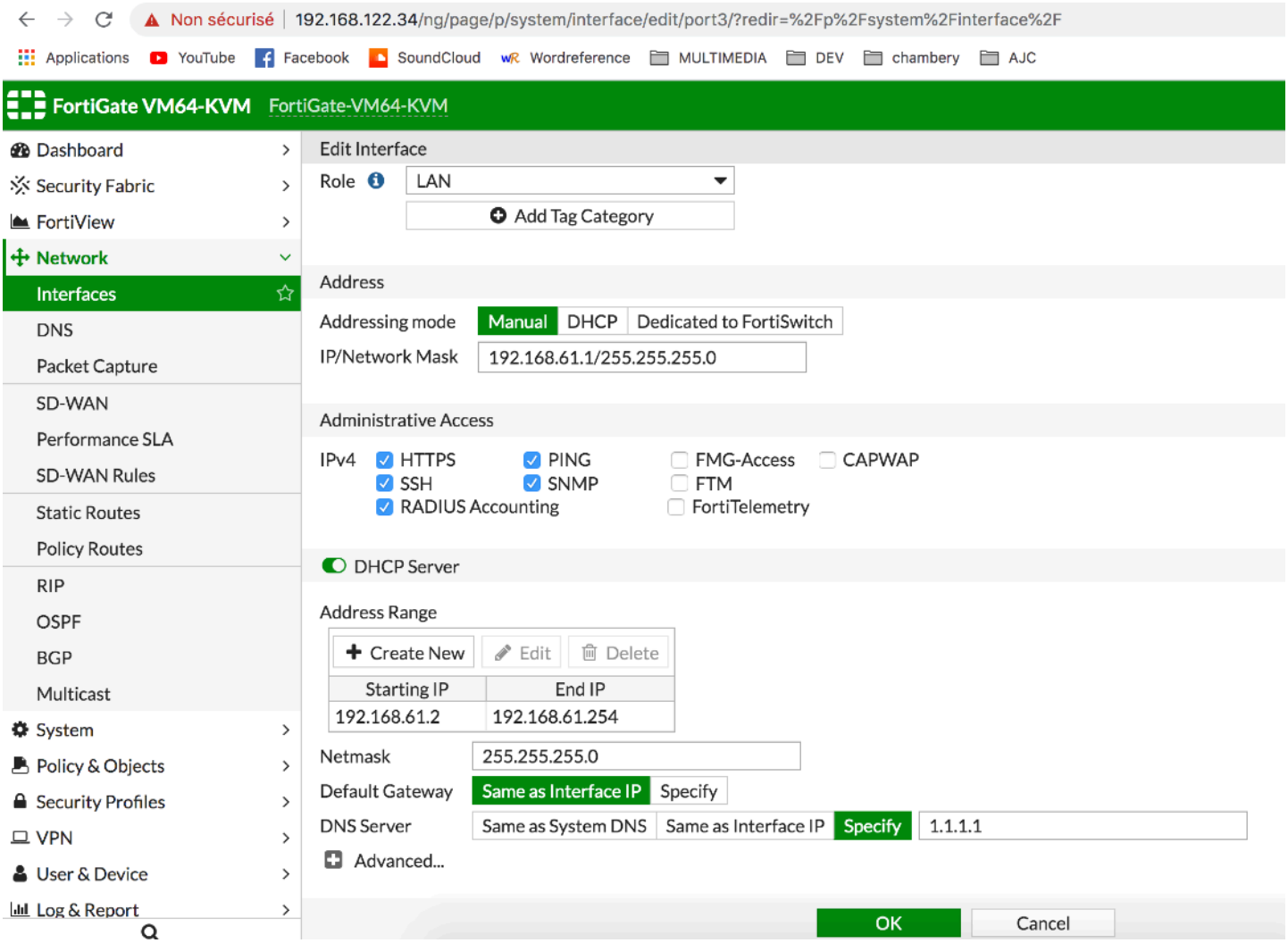
Rôle : LAN

Administrative access : HTTPS PING SSH RADIUS accounting

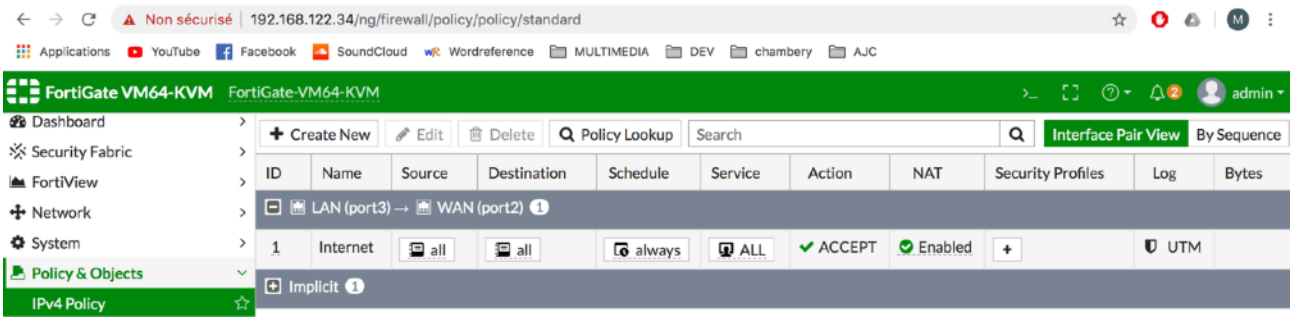
DCHP Server activé.

Spécify DNS : 1.1.1.1

Device detection activé.

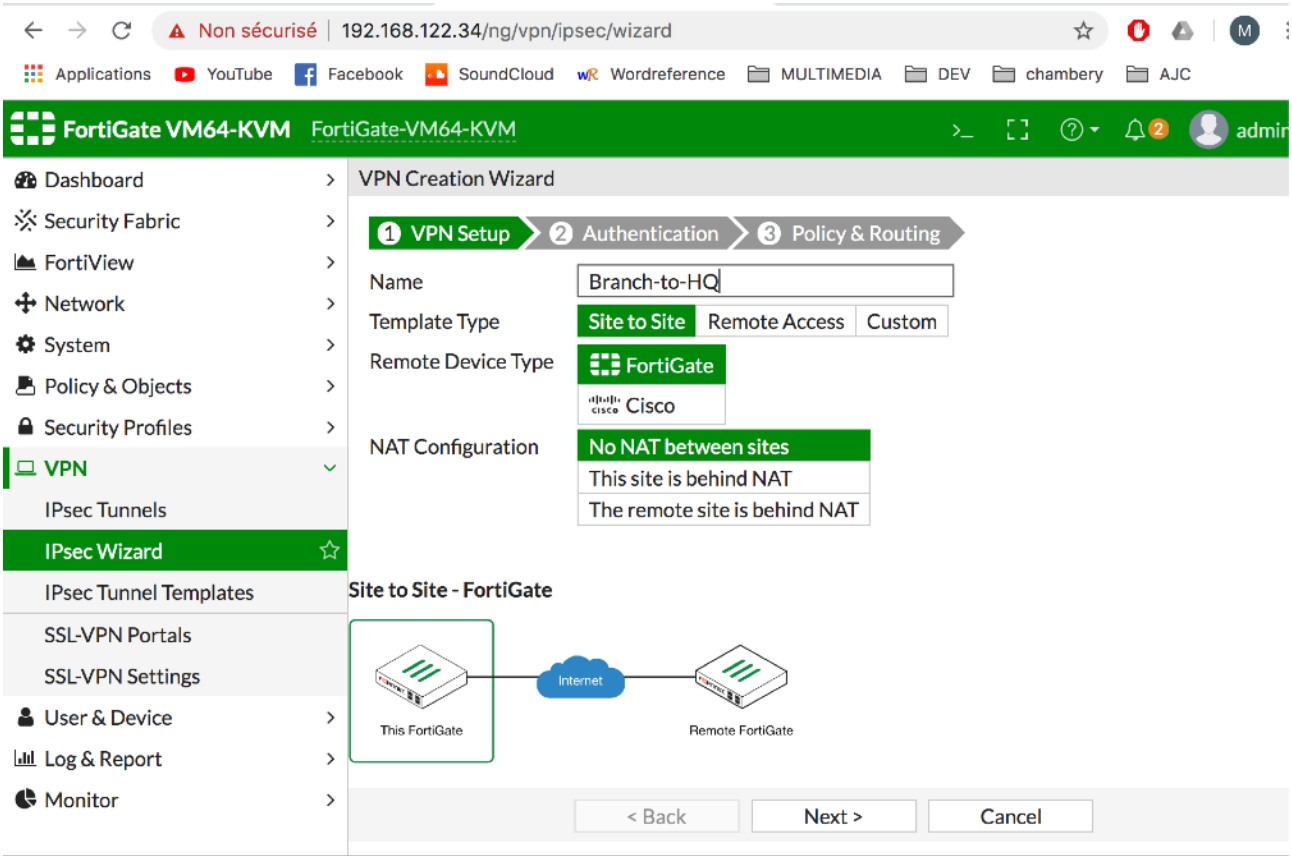


Ipv4 policy > create new

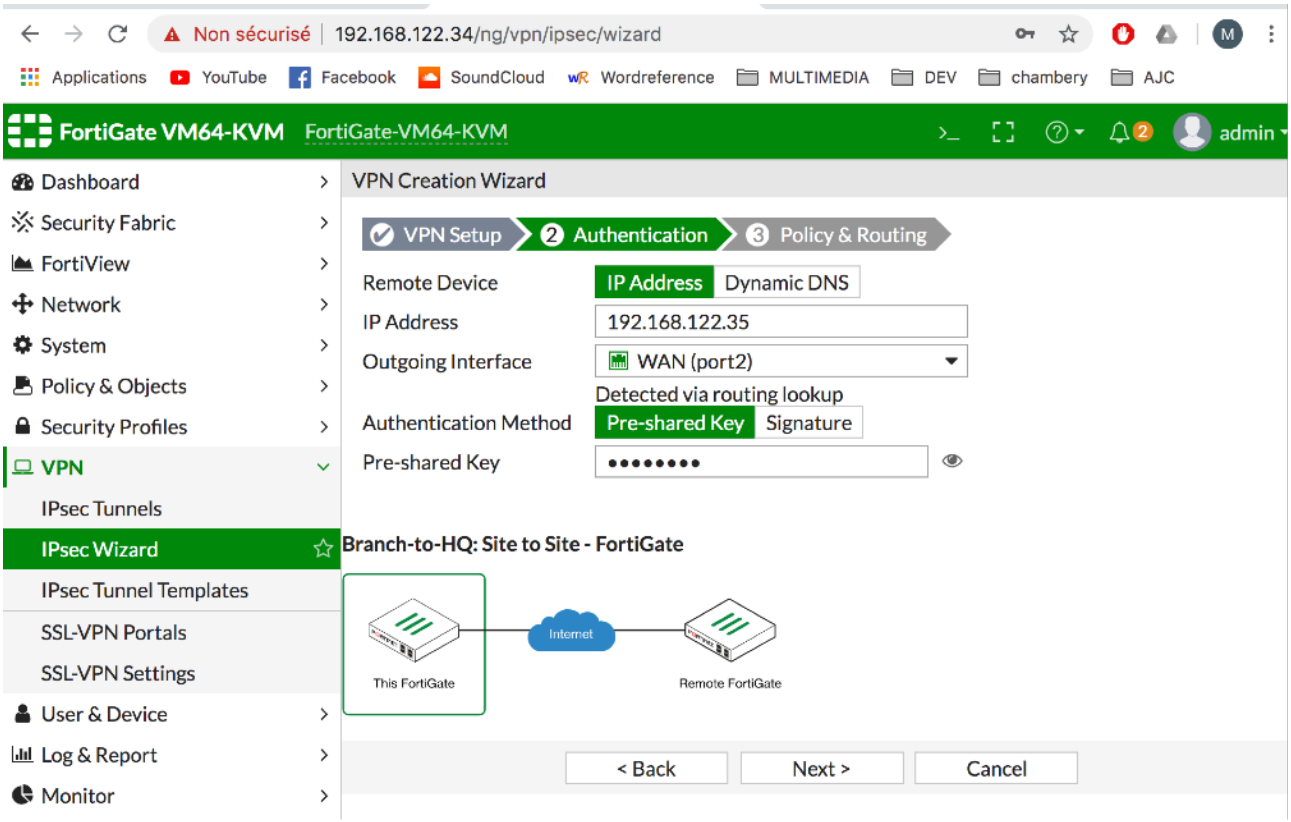


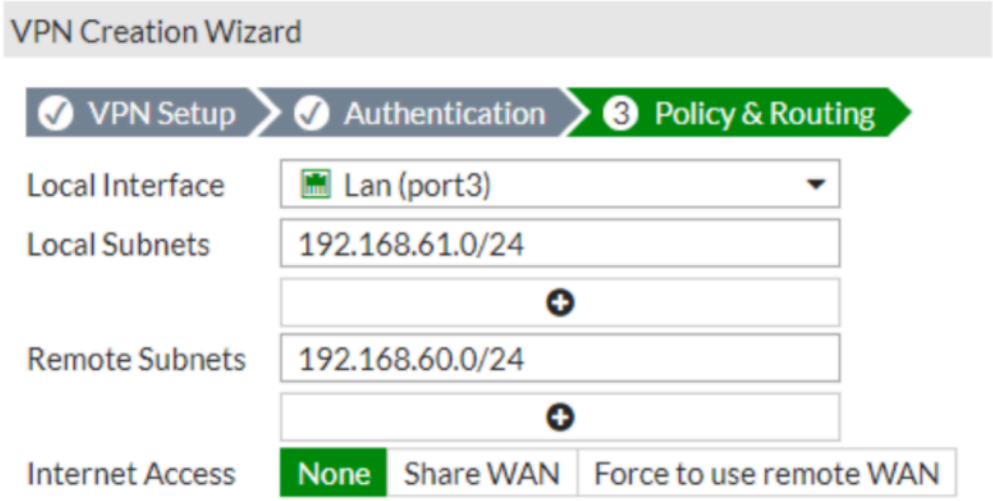
3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard

VPN > ipsec wizard

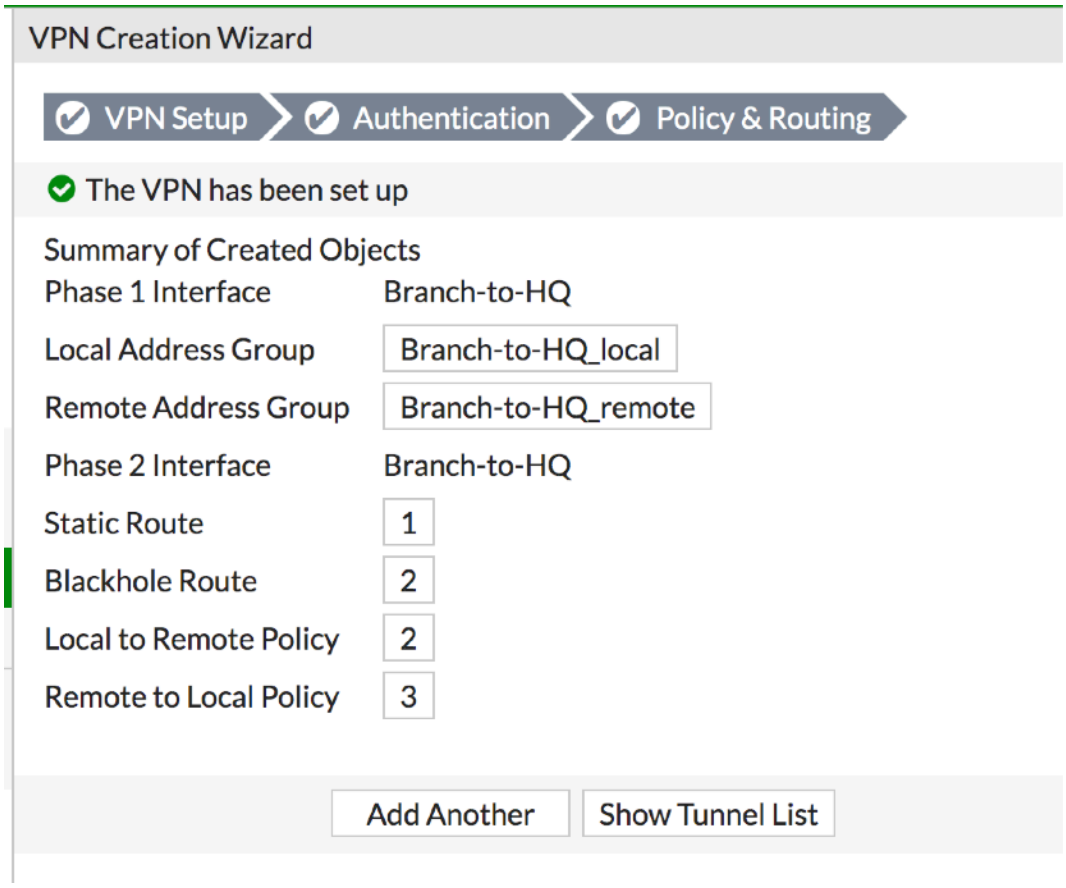


Adresse IP du port 2 : 192.168.122.35 255.255.255.0



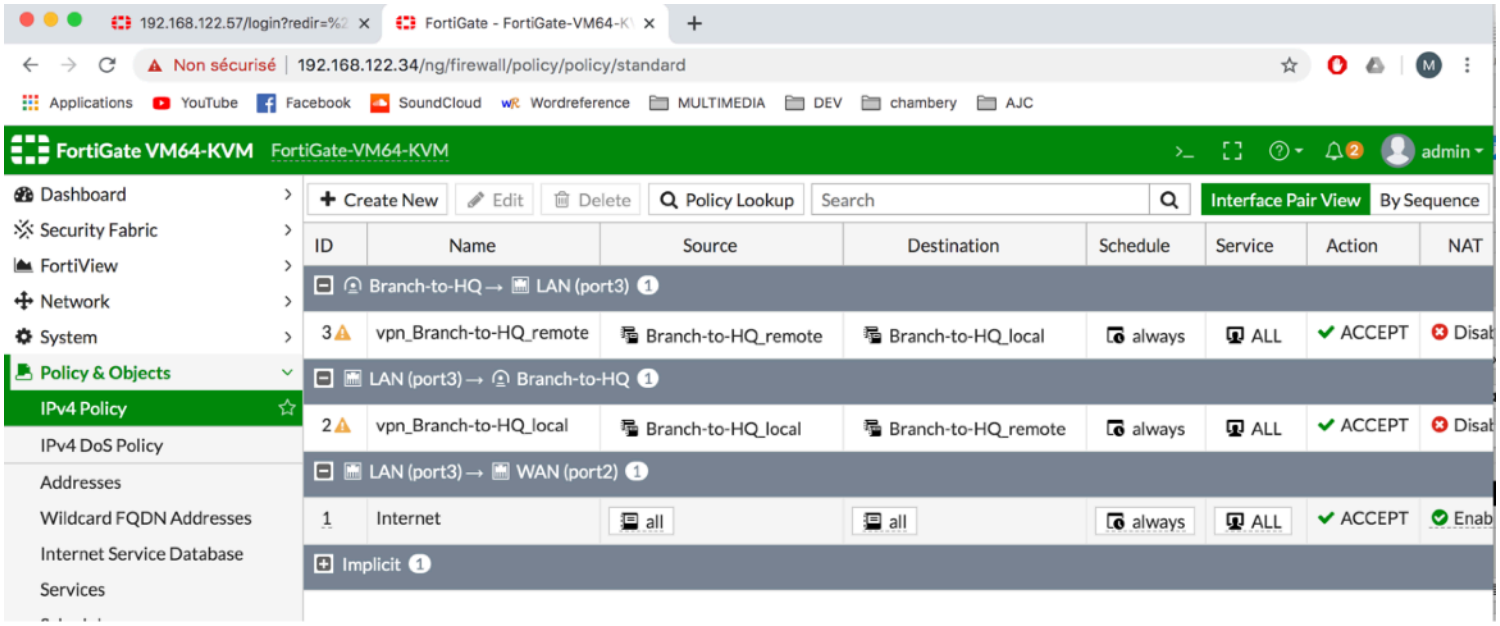


Création du VPN ok :

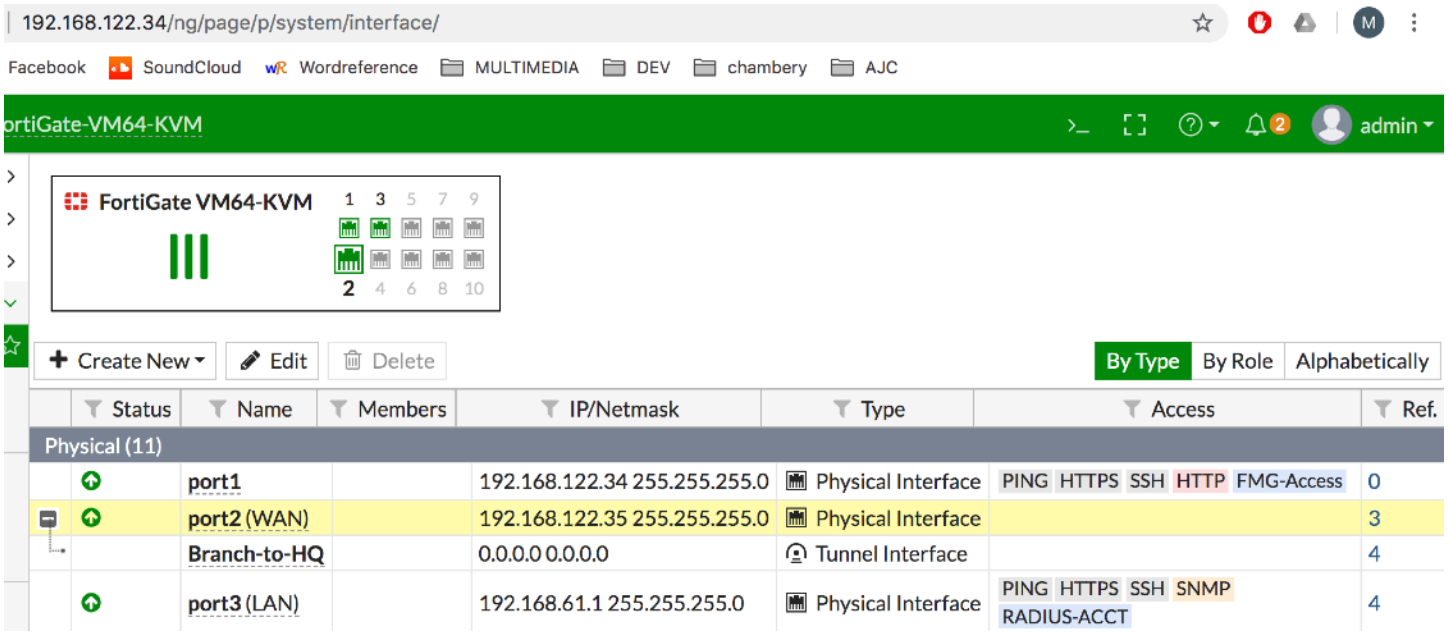


impossible d’afficher les tunnels VPN : chargement infini…

Dans Policy & objects > ipv4 :



L'interface Branch-to-HQ est bien présente sous le port 2



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

IP du poste terminal depuis Branch : 192.168.61.2

IP du poste terminal depuis HQ : 192.168.60.6

PING d'un poste à un autre pour vérifier l'établissement de la connection. De mon côté, impossible de ping.

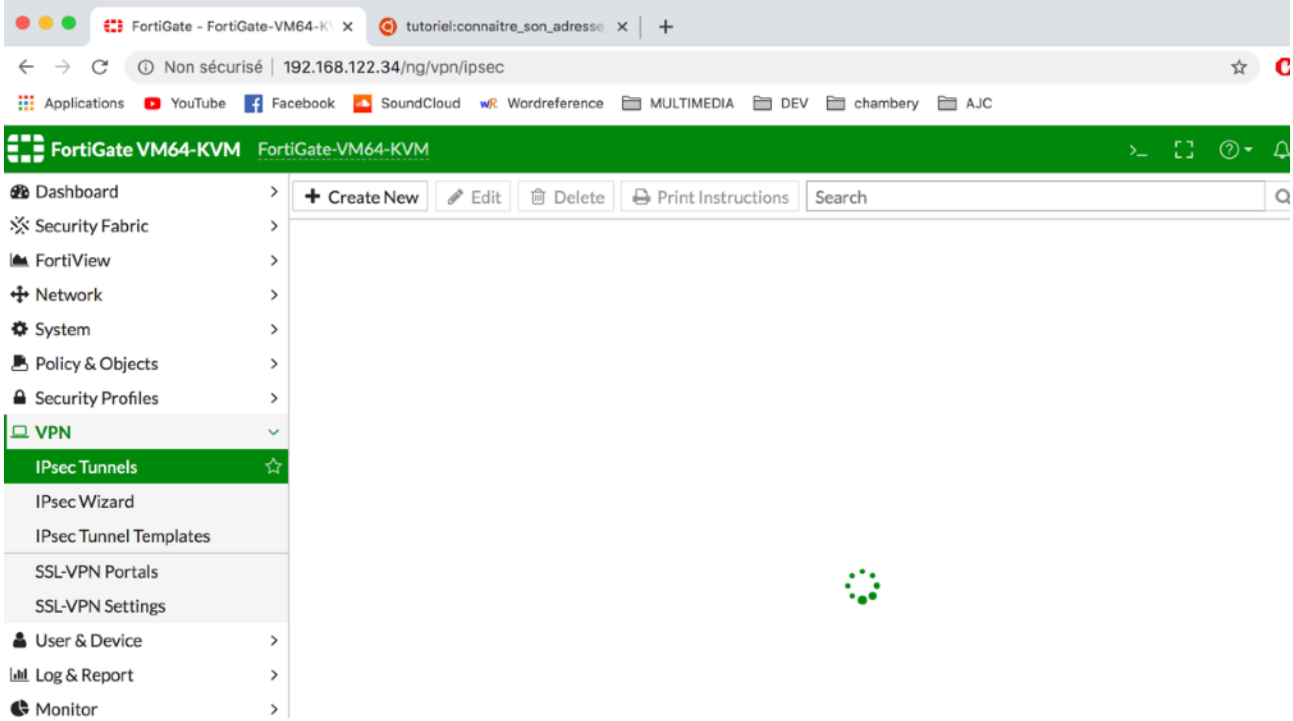
```
Kernel 3.10.0-957.12.2.el7.x86_64 on an x86_64

client-branch login: root
Password:
Last login: Tue May  5 11:13:36 on ttyS0
[root@client-branch ~]#
[root@client-branch ~]#
[root@client-branch ~]#
[root@client-branch ~]# ping 192.168.60.6
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
From 192.168.61.1 icmp_seq=1 Destination Net Unreachable
From 192.168.61.1 icmp_seq=2 Destination Net Unreachable
From 192.168.61.1 icmp_seq=3 Destination Net Unreachable
From 192.168.61.1 icmp_seq=4 Destination Net Unreachable
From 192.168.61.1 icmp_seq=5 Destination Net Unreachable
From 192.168.61.1 icmp_seq=6 Destination Net Unreachable
From 192.168.61.1 icmp_seq=7 Destination Net Unreachable
From 192.168.61.1 icmp_seq=8 Destination Net Unreachable
From 192.168.61.1 icmp_seq=9 Destination Net Unreachable
From 192.168.61.1 icmp_seq=10 Destination Net Unreachable
From 192.168.61.1 icmp_seq=11 Destination Net Unreachable

--- 192.168.60.6 ping statistics ---
11 packets transmitted, 0 received, +11 errors, 100% packet loss, time 10018ms
```

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

Affichage impossible des tunnels VPN: chargement infini.



Exportation de la configuration : admin > configuration > backup OK