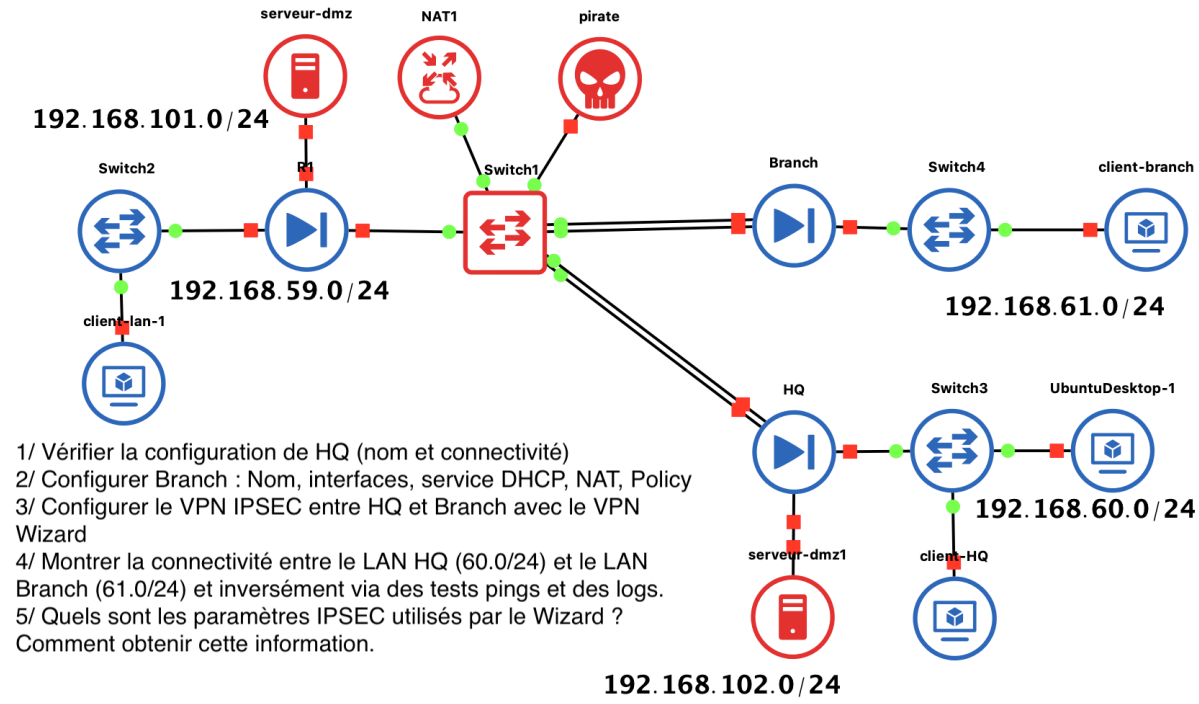
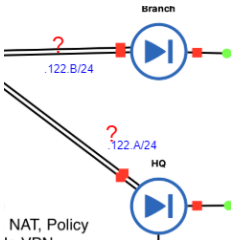
Lab VPN IPSEC site-à-site Fortinet

Objectif : le réseau local du fortinate BRANCH arrive à joindre réseau local du fortinate HQ et inversement.

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



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.



Port	Nom	Adresse IP HQ (HeadQuaters : Quartier Général)-14	Adresse IP Brunch - 14
Port 1	gestion	192.168.122.89	192.168.122.50
Port 2	Internet	192.168.122.90	192.168.122.51
Port 3	Lan	192.168.60.1	192.168.61.1

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

Changer nom, redémarrer le périphérique, vérifier la sécurité=politique de pare-feu

Sur la console :

HQ-18 # get system interface physical

== [onboard]

==[port1] (gestion)

mode: dhcp

ip: 192.168.122.89 255.255.255.0

ipv6: ::/0

status: up

speed: 1000Mbps (Duplex: full)

==[port2] (internet)

mode: dhcp

ip: 192.168.122.90 255.255.255.0

ipv6: ::/0

status: up

speed: 1000Mbps (Duplex: full)

==[port3] LAN

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]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port6]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port7]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port8]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port9]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port10]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

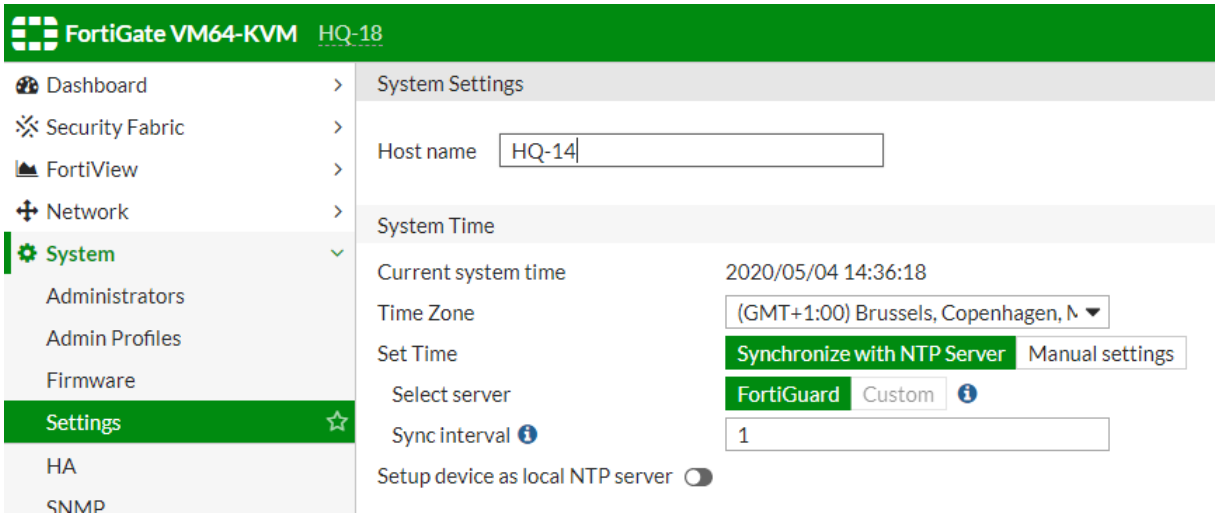
speed: n/a

avec ip: 192.168.122.89, j'ouvre fortinet sur le navigateur firefox

Login : admin / MP : testtest

je change le nom et time zone = (GMT+1:00) : Paris

! N'oublier pas de valider



Ping sur pirate

```
[root@pirate ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:e5:e0:8d:d4:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.40/24 brd 192.168.122.255 scope global noprefixroute dynamic eth0
       valid_lft 2790sec preferred_lft 2790sec
    inet6 fd85:48ad:ad71::8d0/128 scope global tentative noprefixroute dadfailed
       valid_lft forever preferred_lft forever
    inet6 2001:470:c814:ffff::8d0/128 scope global tentative noprefixroute dadfailed

[root@pirate ~]# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=59 time=3.09 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=59 time=3.15 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=59 time=3.13 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=59 time=3.07 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=59 time=3.01 ms

[1]+  Stopped                 ping 1.1.1.1
```

Ping client-HQ

```
[root@client-hq ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
```

link/ether 0c:e5:e0:33:0b:00 brd ff:ff:ff:ff:ff:ff

inet 192.168.60.6/24 brd 192.168.60.255 scope global noprefixroute dynamic eth0

valid_lft 603963sec preferred_lft 603963sec

inet6 fe80::ee5:e0ff:fe33:b00/64 scope link noprefixroute

valid_lft forever preferred_lft forever

[root@client-hq ~]# ping 1.1.1.1

PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.

--- 1.1.1.1 ping statistics ---

12 packets transmitted, 0 received, 100% packet loss, time 10999ms

[root@client-hq ~]# 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=255 time=1.76 ms

64 bytes from 192.168.60.1: icmp_seq=2 ttl=255 time=0.878 ms

64 bytes from 192.168.60.1: icmp_seq=3 ttl=255 time=0.868 ms

64 bytes from 192.168.60.1: icmp_seq=4 ttl=255 time=0.889 ms

64 bytes from 192.168.60.1: icmp_seq=5 ttl=255 time=0.956 ms

64 bytes from 192.168.60.1: icmp_seq=6 ttl=255 time=1.17 ms

64 bytes from 192.168.60.1: icmp_seq=7 ttl=255 time=0.822 ms

--- 192.168.60.1 ping statistics ---

7 packets transmitted, 7 received, 0% packet loss, time 6010ms

rtt min/avg/max/mdev = 0.822/1.050/1.760/0.309 ms

pas de ping pour la DMZ et internet

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

Sur la console Branch :

Login : admin / MP : aucun

FortiGate-VM64-KVM # get system interface physical

== [onboard]

==[port1]

mode: dhcp

ip: 192.168.122.51 255.255.255.0

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

speed: n/a

==[port5]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port6]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port7]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port8]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port9]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

==[port10]

mode: static

ip: 0.0.0.0 0.0.0.0

ipv6: ::/0

status: down

speed: n/a

avec ip: 192.168.122.51, j'ouvre fortinet sur le navigateur firefox

Login : admin / MP : aucun

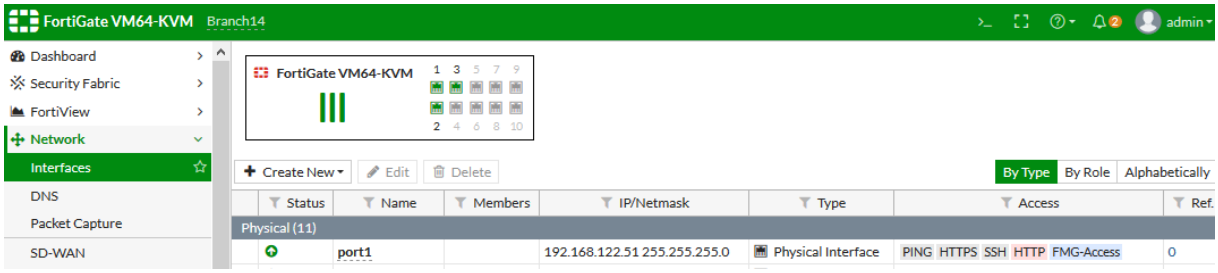
je change le nom et time zone = (GMT+1:00) : Paris

!!! N'oublier pas de valider

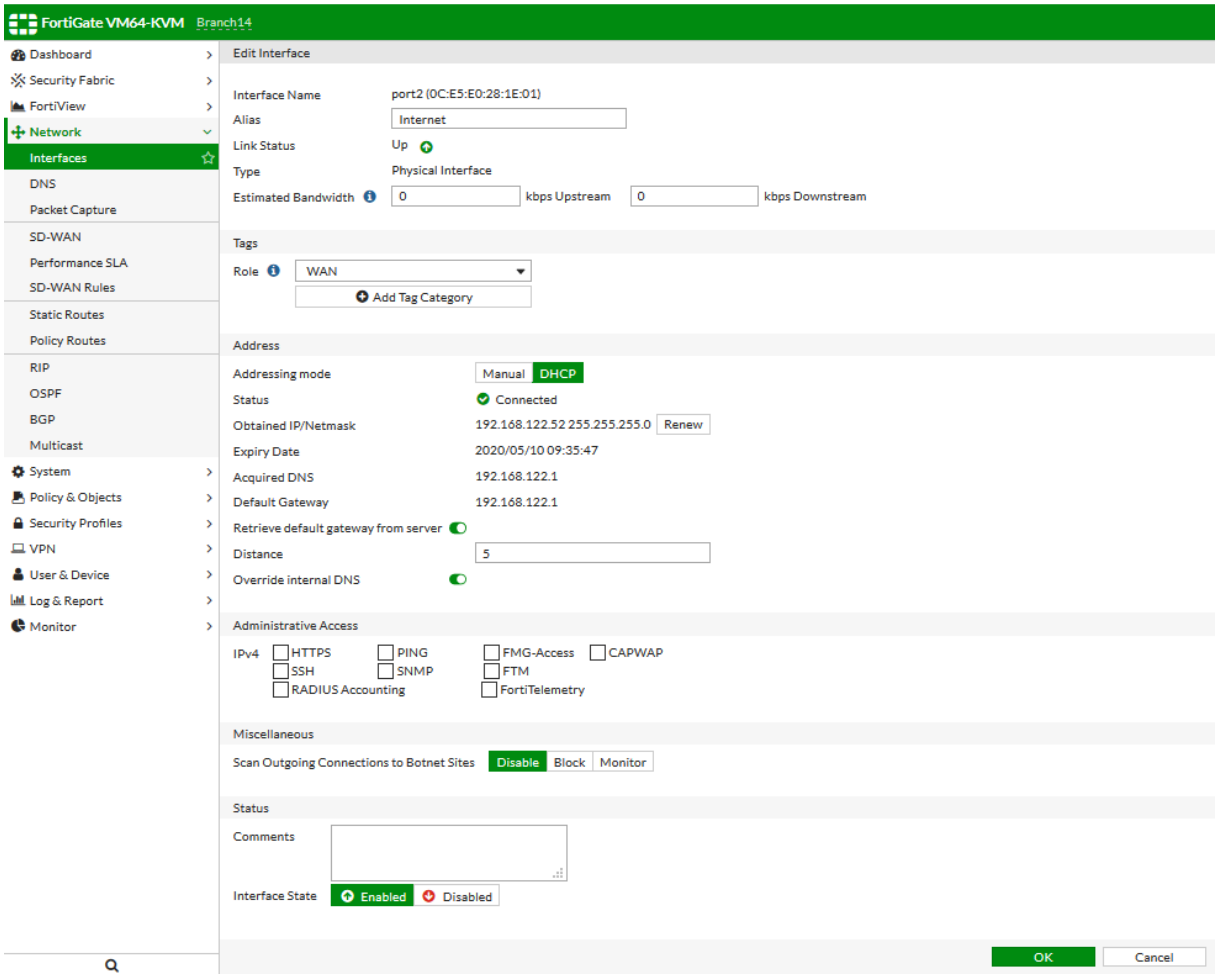
Configurer les interfaces

Port 1 : port de gestion. Déjà configuré.

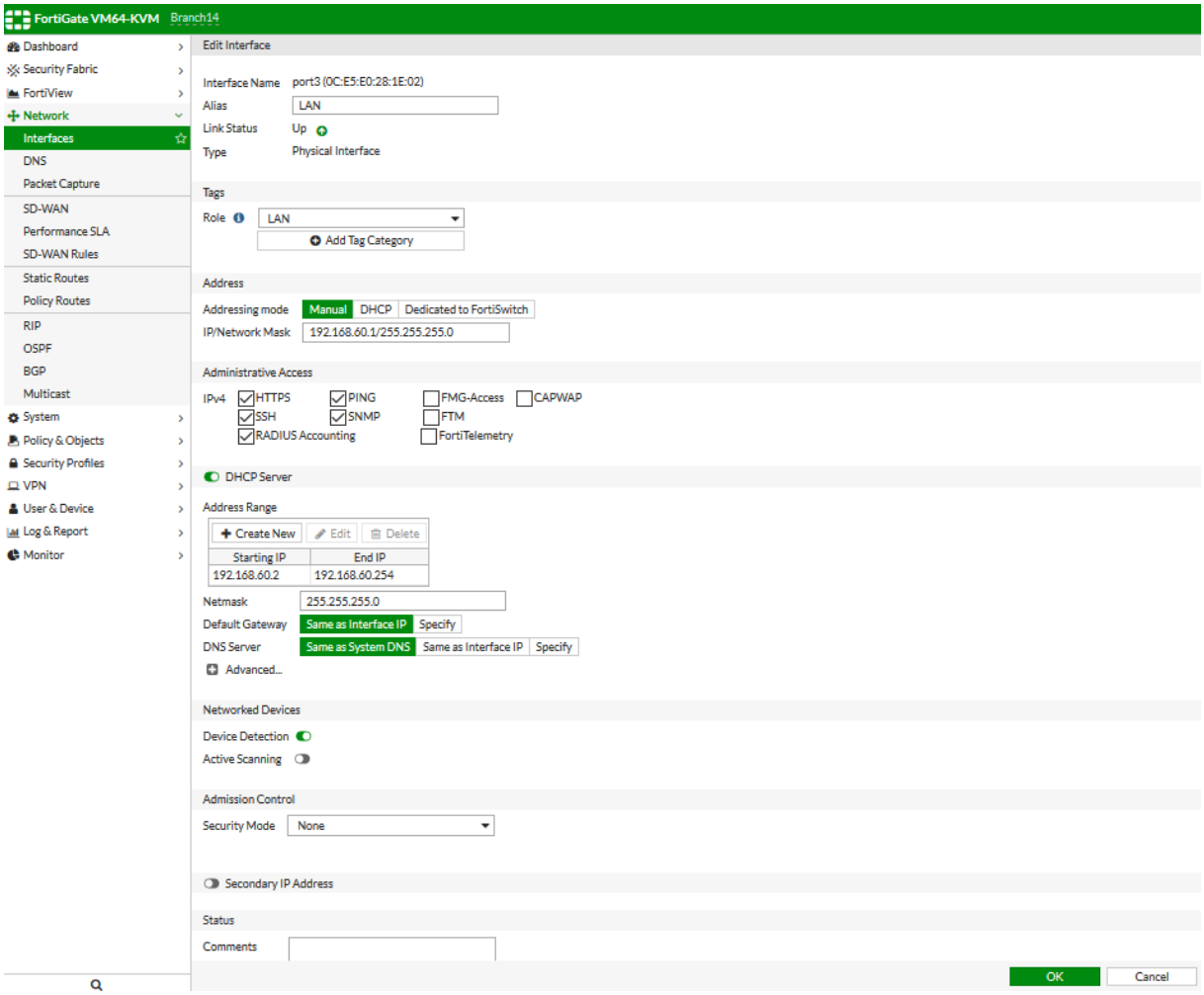
Vérification IP et Access.


FortiGate VM64-KVM
Branch14
admin
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
FortiGate VM64-KVM
1 3 5 7 9
2 4 6 8 10
Create New
Edit
Delete
By Type
By Role
Alphabetically
Status
Name
Members
IP/Netmask
Type
Access
Ref.
Physical (11)
port1
192.168.122.51 255.255.255.0
Physical Interface
PING HTTPS SSH HTTP FMG-Access
0

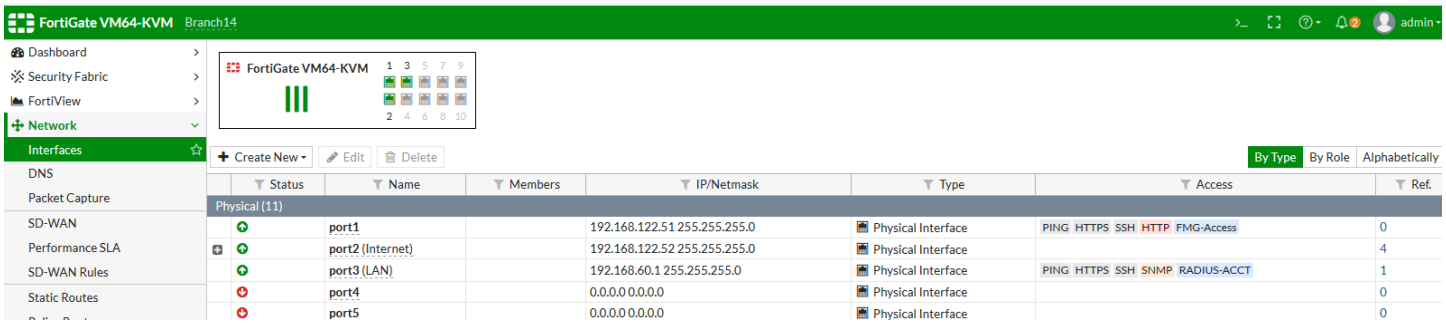
Port 2


FortiGate VM64-KVM
Branch14
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
Performance SLA
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
Edit Interface
Interface Name
port2 (0C:E5:E0:28:1E:01)
Alias
Internet
Link Status
Up
Type
Physical Interface
Estimated Bandwidth
0
kbps Upstream
0
kbps Downstream
Tags
Role
WAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
Status
Connected
Obtained IP/Netmask
192.168.122.52 255.255.255.0
Renew
Expiry Date
2020/05/10 09:35:47
Acquired DNS
192.168.122.1
Default Gateway
192.168.122.1
Retrieve default gateway from server
Distance
5
Override internal DNS
Administrative Access
IPv4
HTTPS
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
Miscellaneous
Scan Outgoing Connections to Botnet Sites
Disable
Block
Monitor
Status
Comments
Interface State
Enabled
Disabled
OK
Cancel

Port 3



Les ports sont configurés

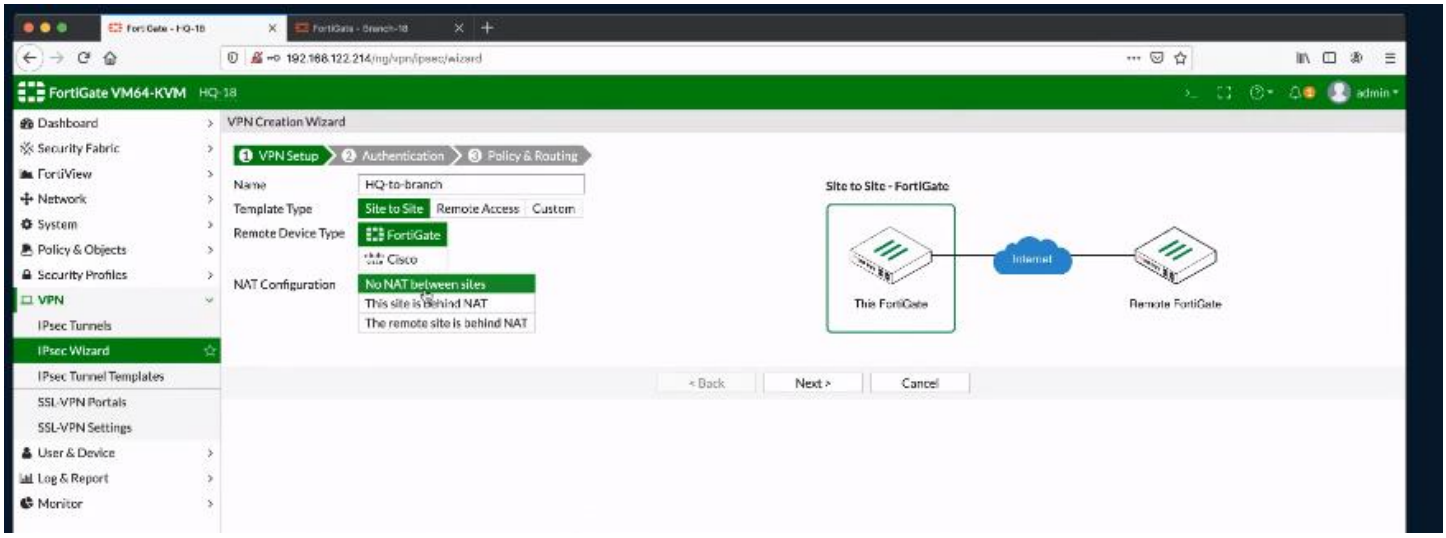


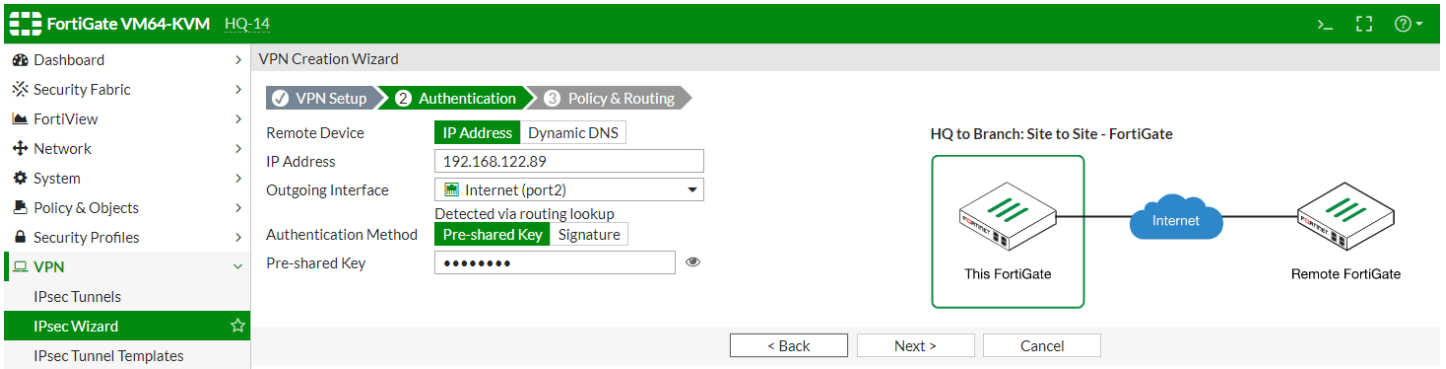
3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard

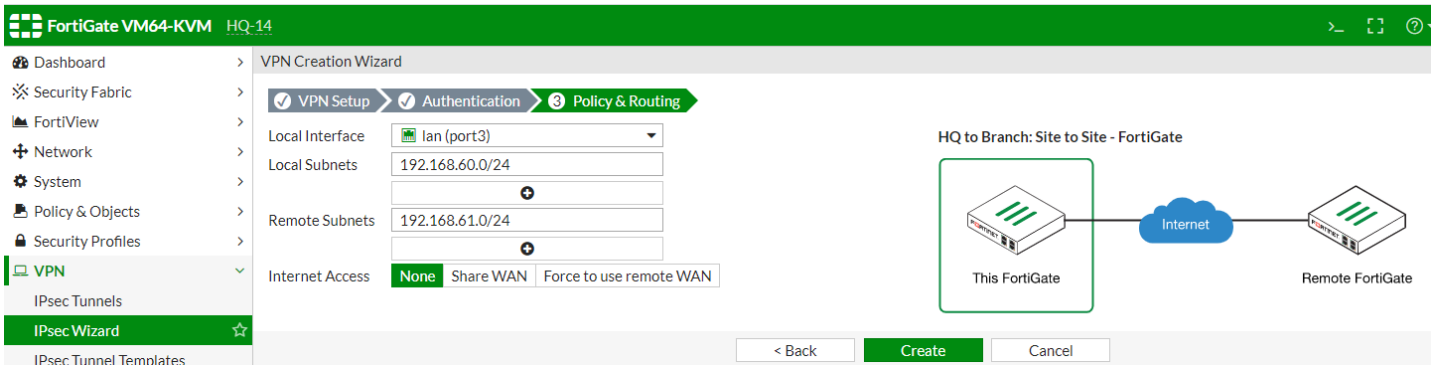
Configurer manuellement

Test de connectivite ping de hq et branch

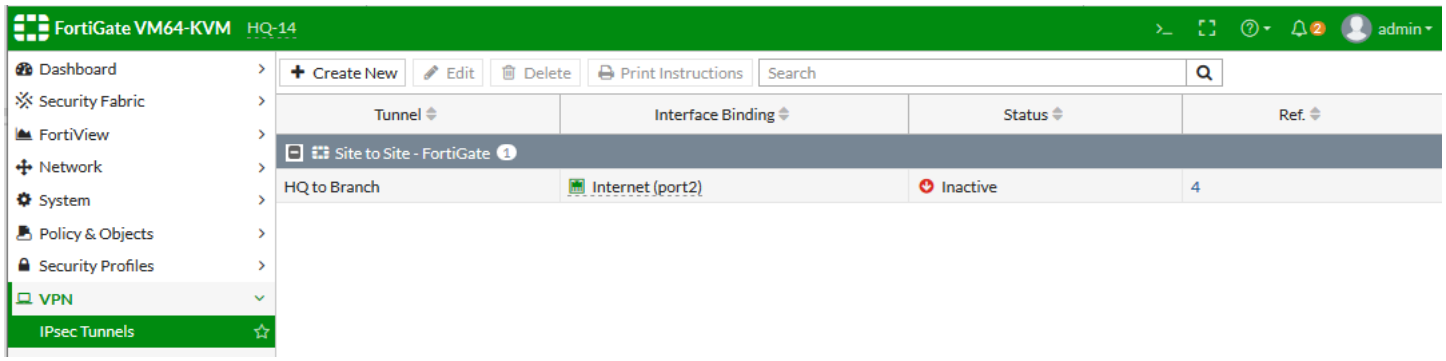
HQ to BRANCH



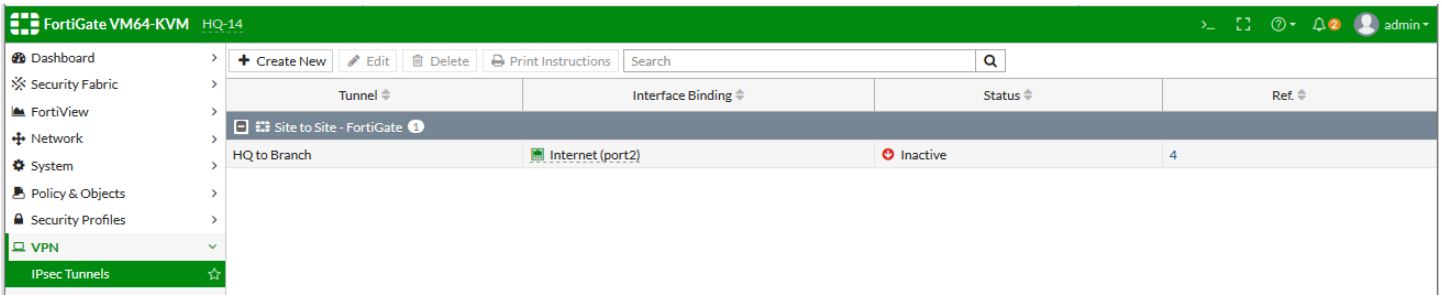




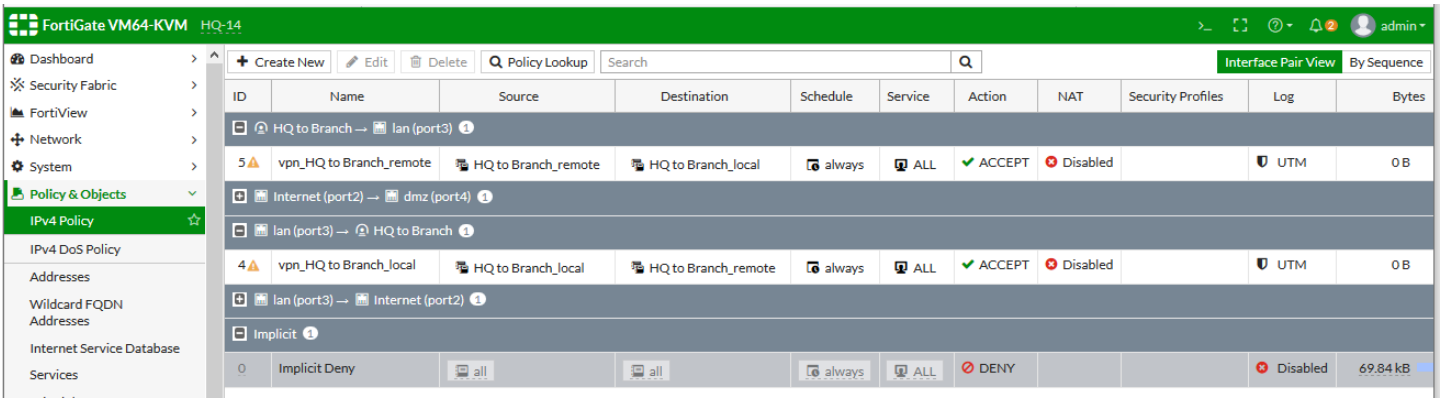
Cliquer sur VPN > IPsec tunnels pour vérifier si le tunnel est monté

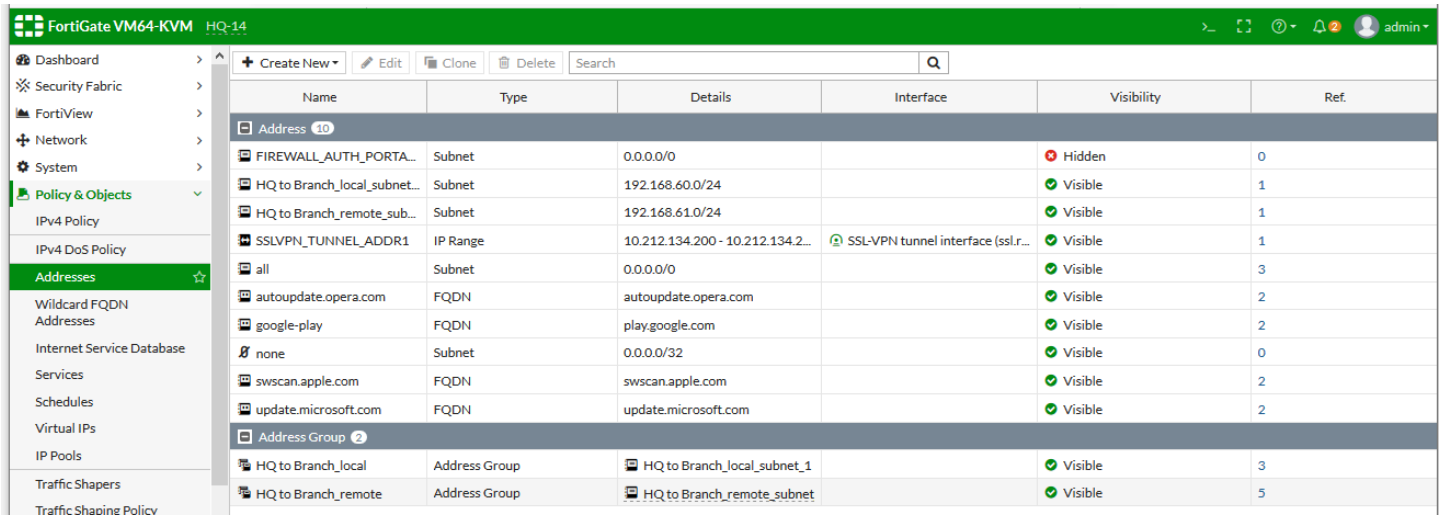


Vérifier la configuration

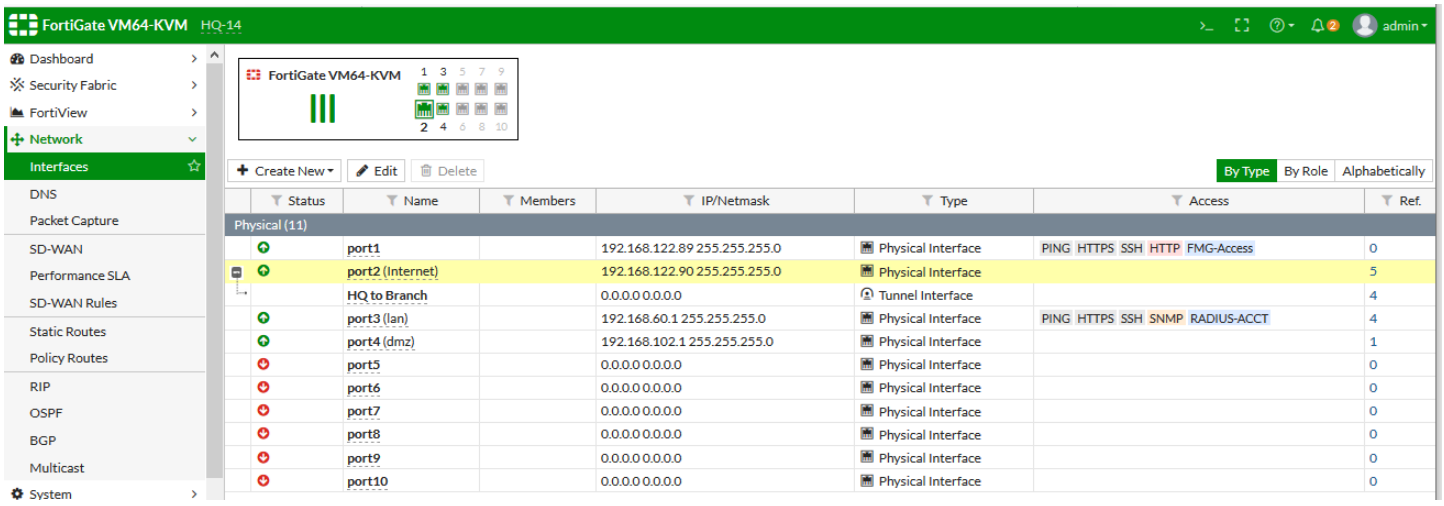


Vérifier la configuration

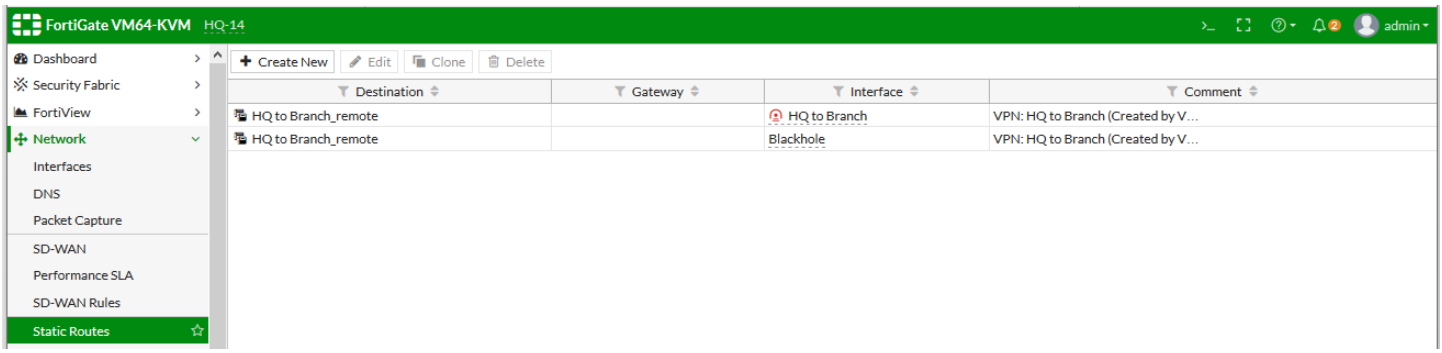




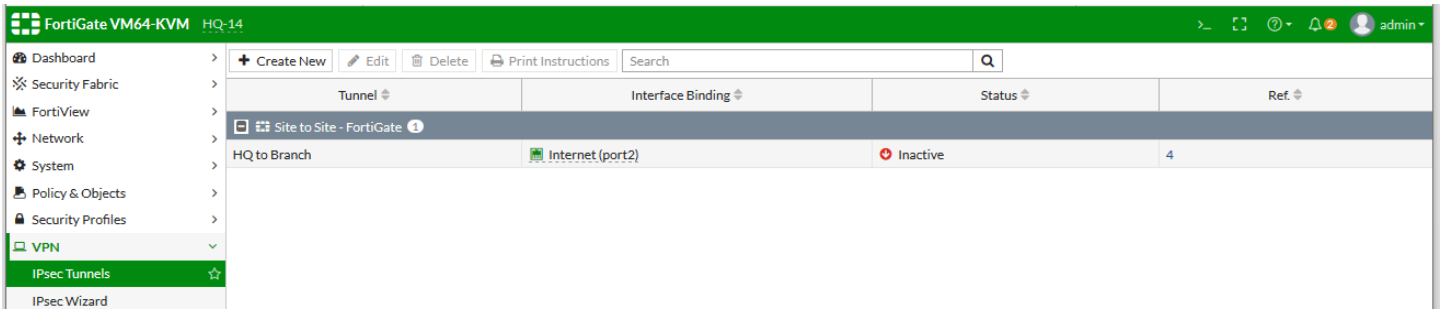
Vérification de la sous interface sur le port WAN



Vérification des routes



Vérification si le tunnel est monté



BRANCH to HQ

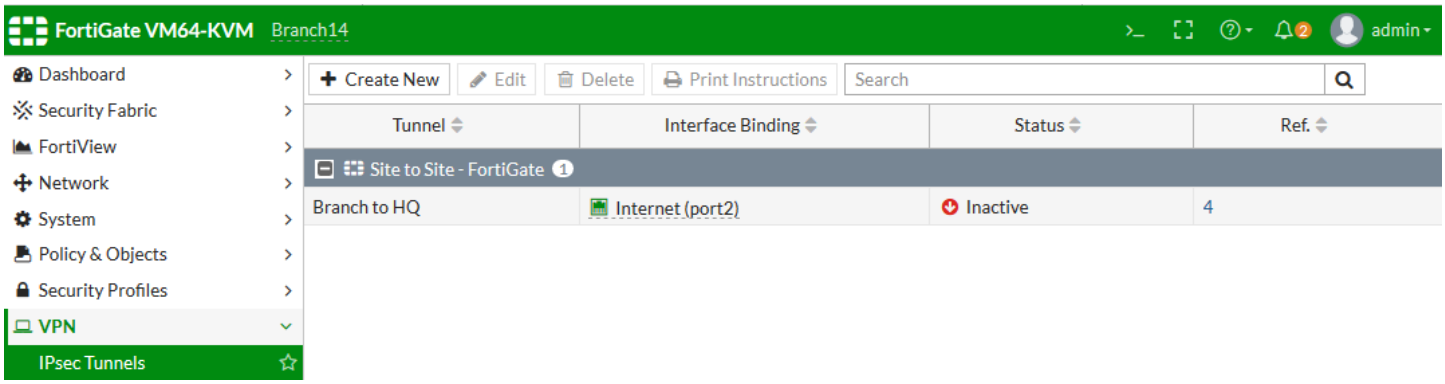
IP address 192.168.122.52

Outgoing interface: internet port 2

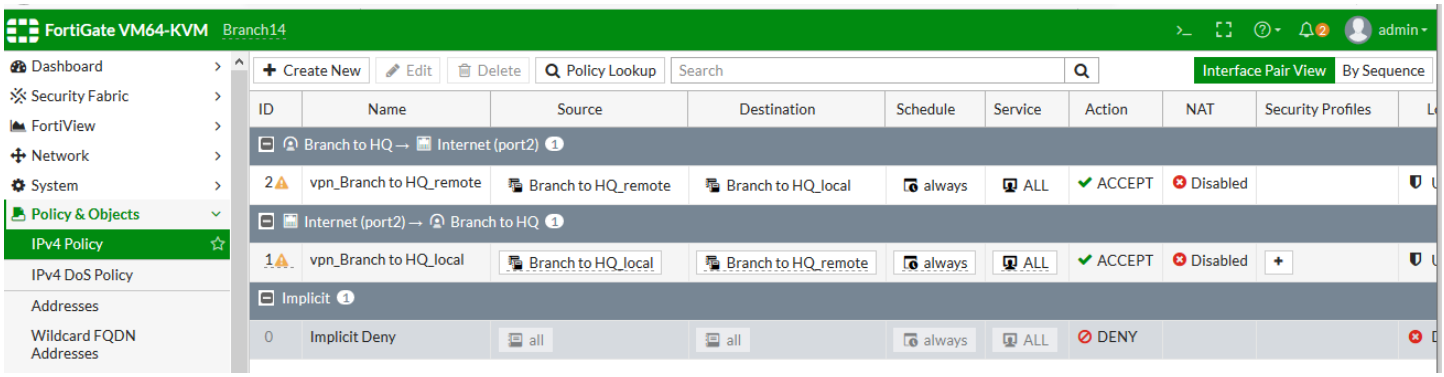
Key: testtest

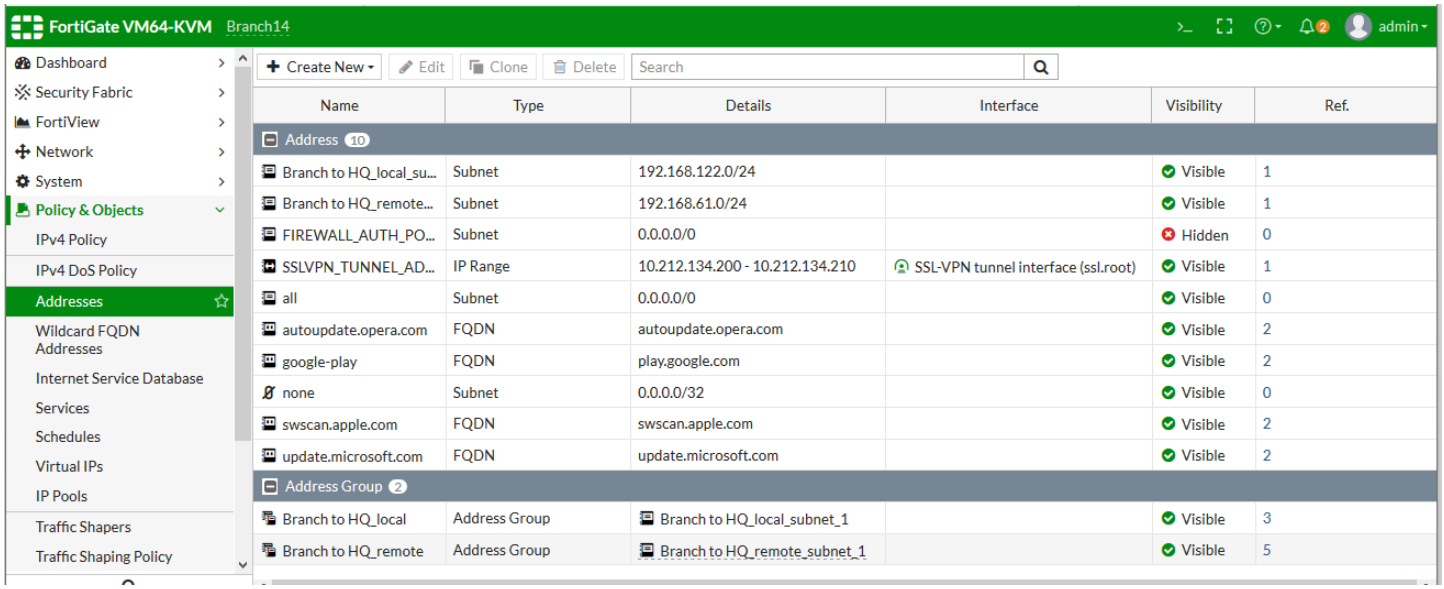
Local interface: port3

Subnets: 60.0 et 60.1

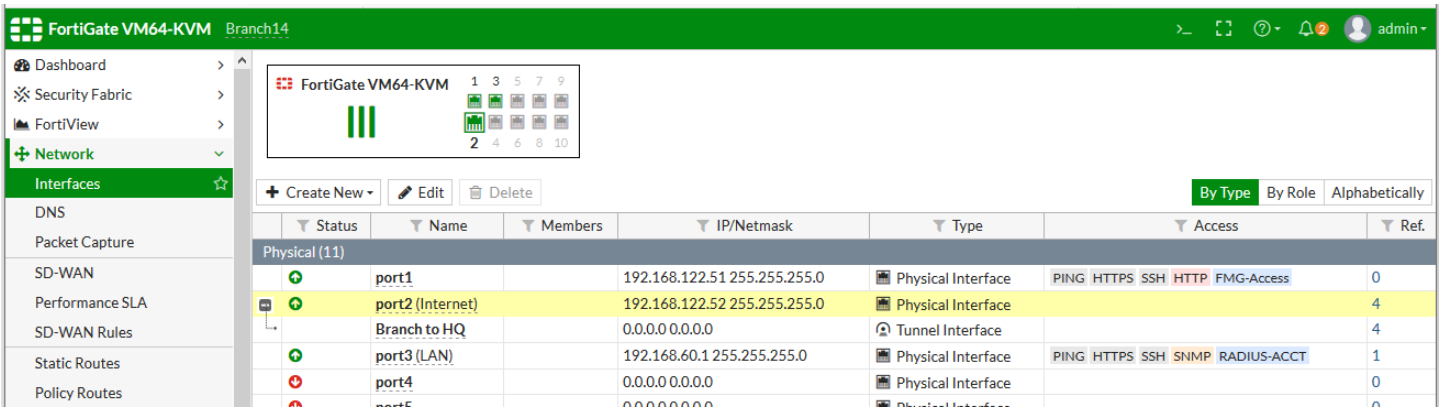


Vérifier la configuration

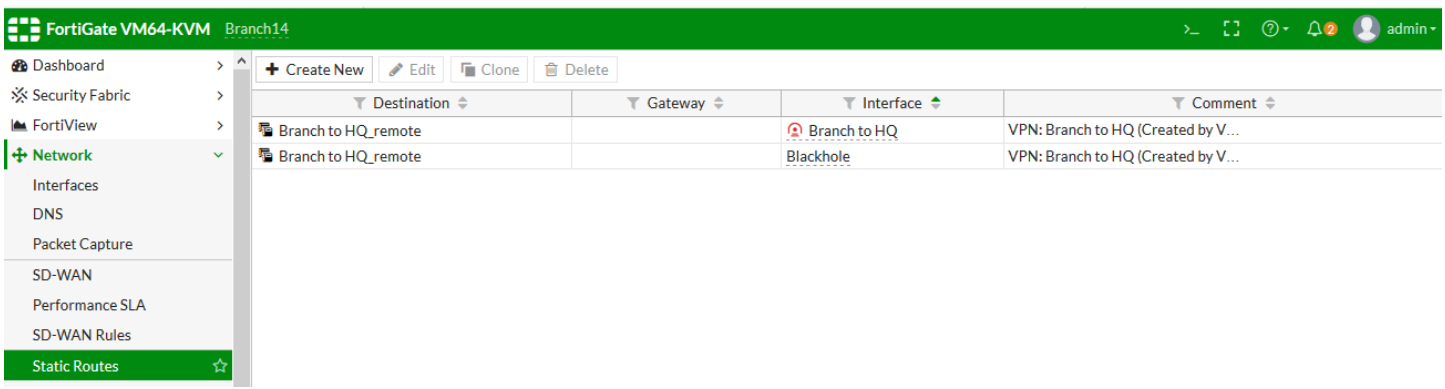




Vérification de la sous interface sur le port WAN



Verification des routes statiques



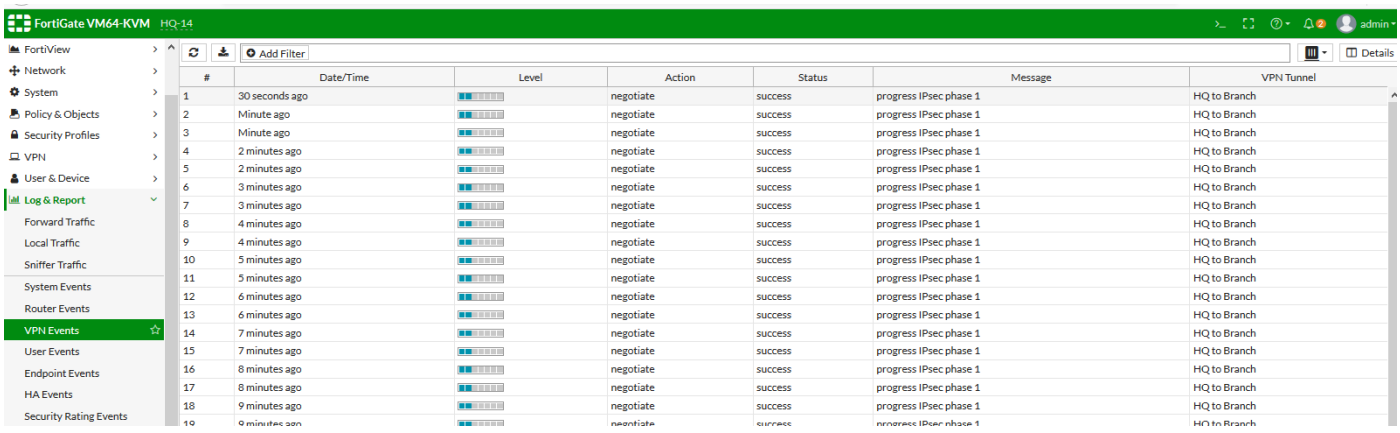
4/ Montrer la connectivité entre le LAN HQ (60.0/24) et le LAN Branch (61.0/24) et inversément via des tests pings et des logs.

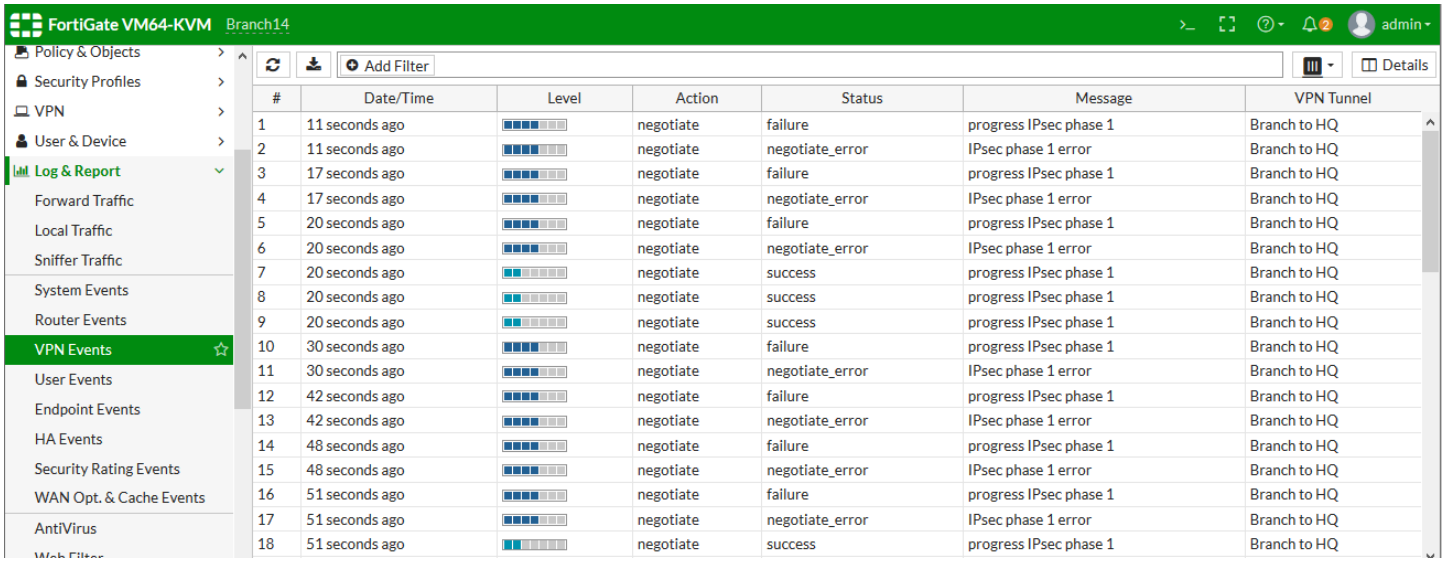
Acceder aux PC Branch et HQ et faire un ping, ainsi on monte la connectivité

Login : root
Password : testtest

```
[root@client-hq ~]# ping 192.168.61.1
PING 192.168.61.1 (192.168.61.1) 56(84) bytes of data.
From 192.168.60.1 icmp_seq=1 Destination Net Unreachable
From 192.168.60.1 icmp_seq=2 Destination Net Unreachable
From 192.168.60.1 icmp_seq=3 Destination Net Unreachable
From 192.168.60.1 icmp_seq=4 Destination Net Unreachable
From 192.168.60.1 icmp_seq=5 Destination Net Unreachable
From 192.168.60.1 icmp_seq=6 Destination Net Unreachable
From 192.168.60.1 icmp_seq=7 Destination Net Unreachable
From 192.168.60.1 icmp_seq=8 Destination Net Unreachable

--- 192.168.61.1 ping statistics ---
8 packets transmitted, 0 received, +8 errors, 100% packet loss, time 7011ms

[root@client-hq ~]#
```

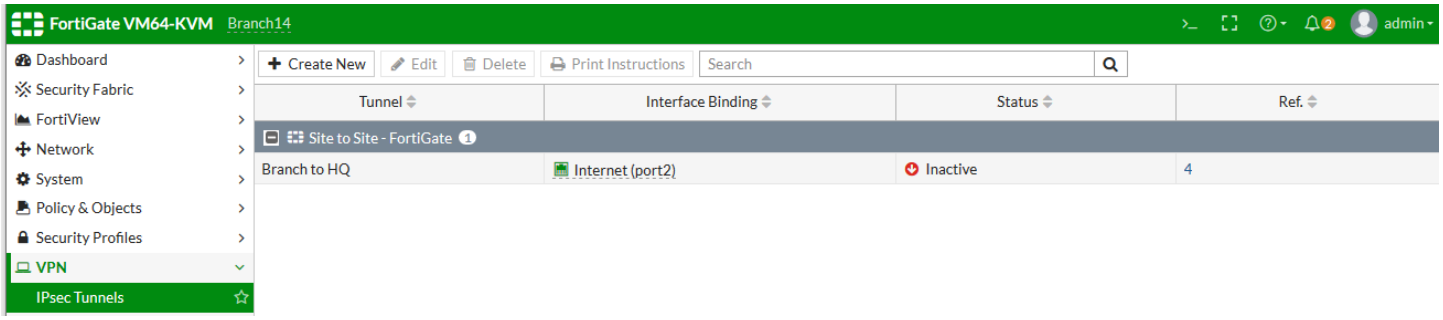
```
[root@client-branch ~]# ping 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.
64 bytes from 192.168.60.1: icmp_seq=1 ttl=255 time=2.08 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=255 time=1.00 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=255 time=0.959 ms
64 bytes from 192.168.60.1: icmp_seq=4 ttl=255 time=0.964 ms
64 bytes from 192.168.60.1: icmp_seq=5 ttl=255 time=0.947 ms
64 bytes from 192.168.60.1: icmp_seq=6 ttl=255 time=1.00 ms
64 bytes from 192.168.60.1: icmp_seq=7 ttl=255 time=0.703 ms
64 bytes from 192.168.60.1: icmp_seq=8 ttl=255 time=0.927 ms

--- 192.168.60.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7011ms
rtt min/avg/max/mdev = 0.703/1.074/2.087/0.394 ms
[root@client-branch ~]#
```



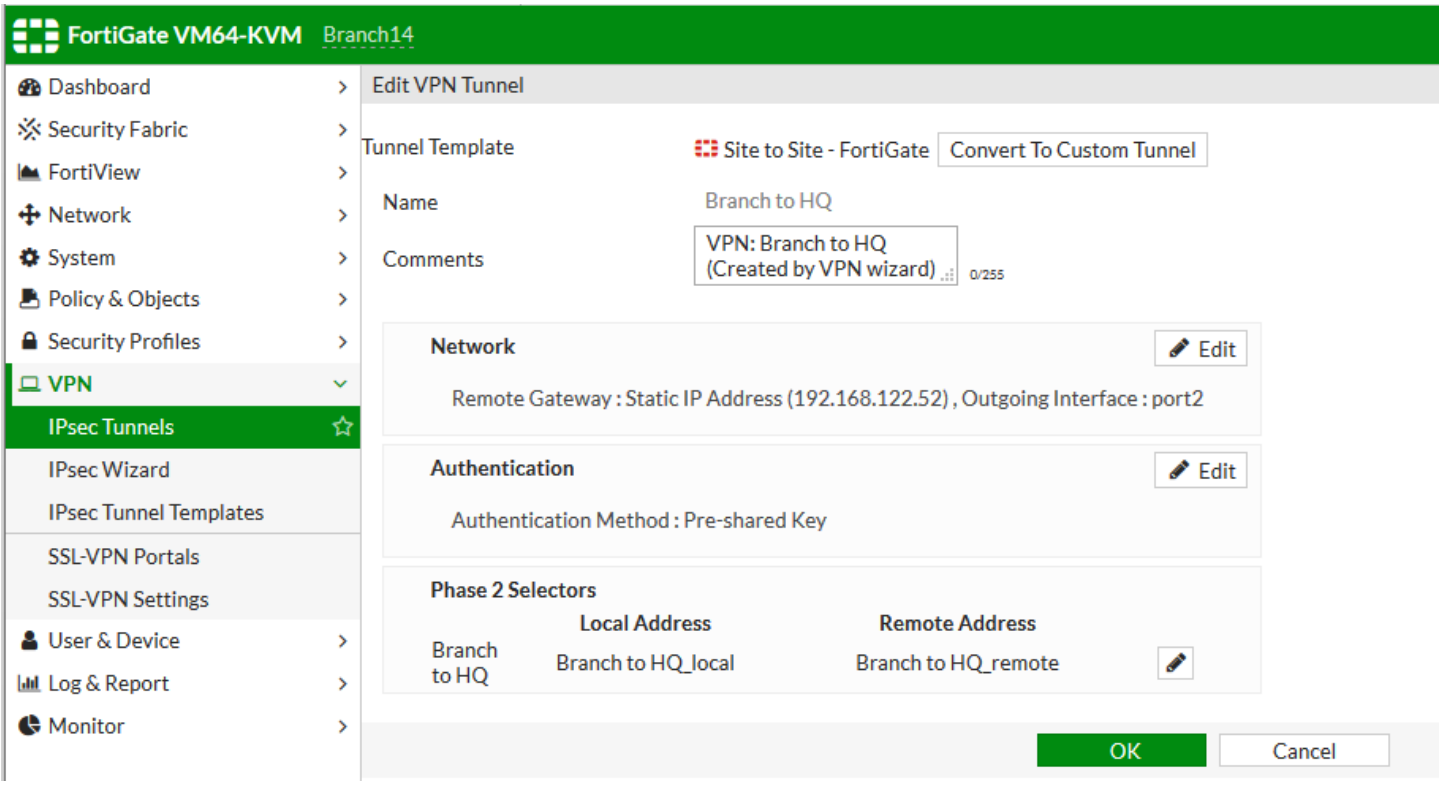


5/ Quels sont les paramètres IPSEC utilisés par le Wizard ? Comment obtenir cette information.

Dans VPN -> Ipsec tunnel

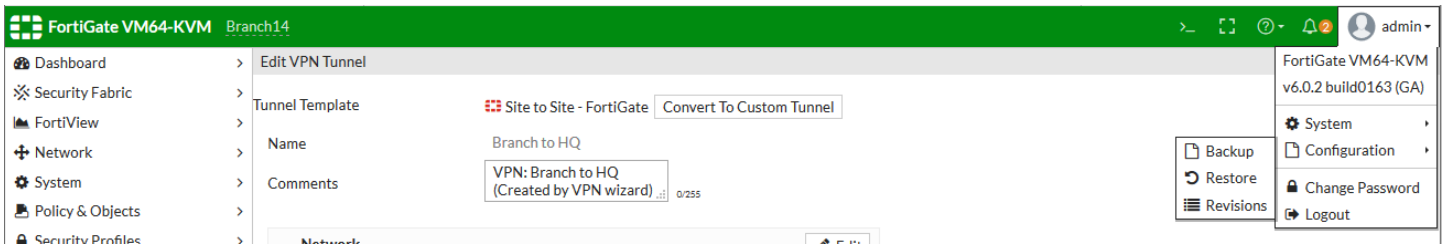


on double-clique :



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

Aller dans Admin >> Configuration >> Backup



Pour ouvrir la console sans passer par gns 3