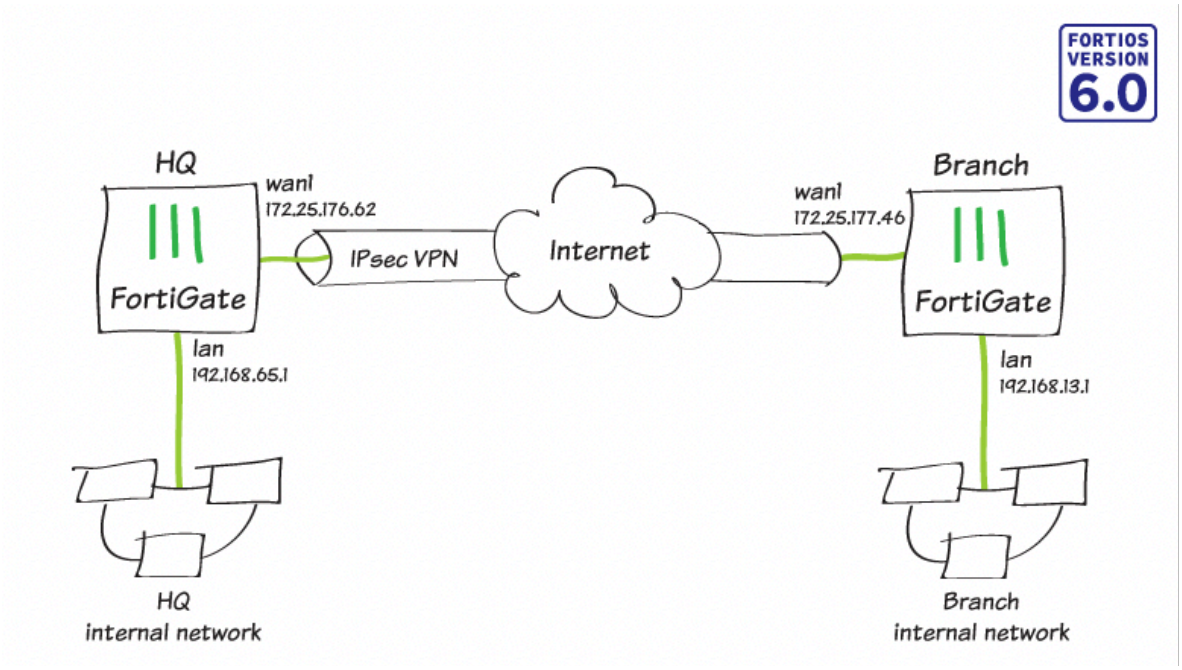
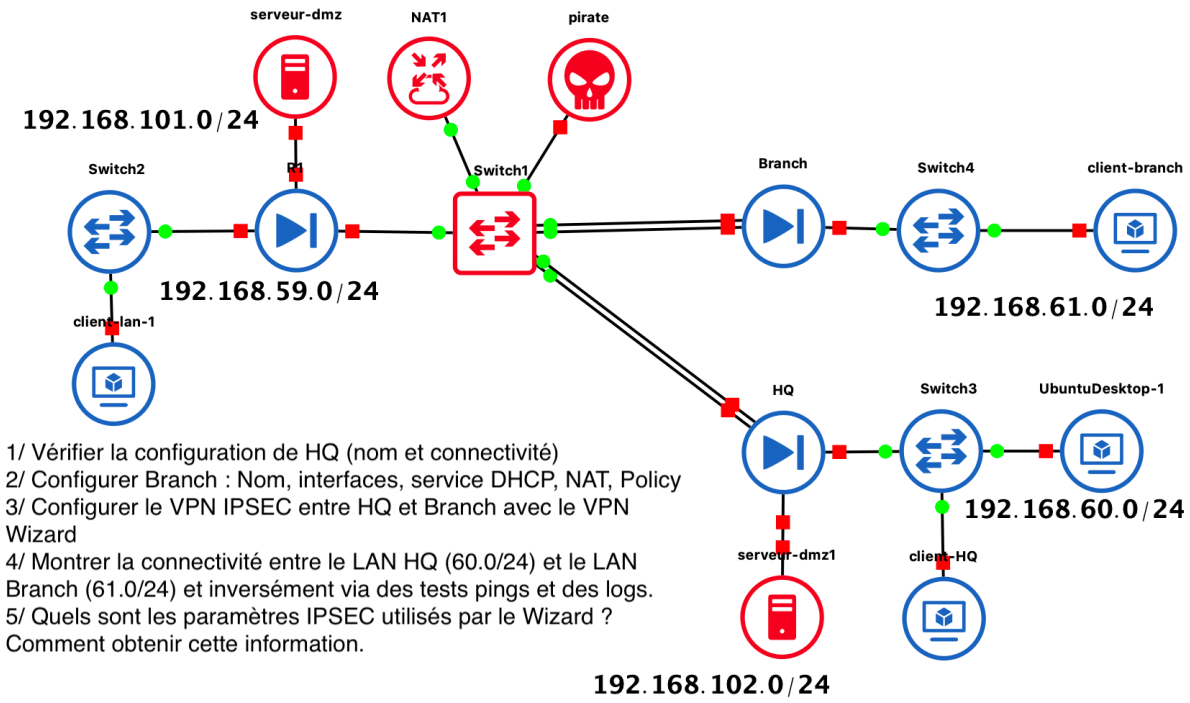
Lab VPN IPSEC site-à-site Fortinet



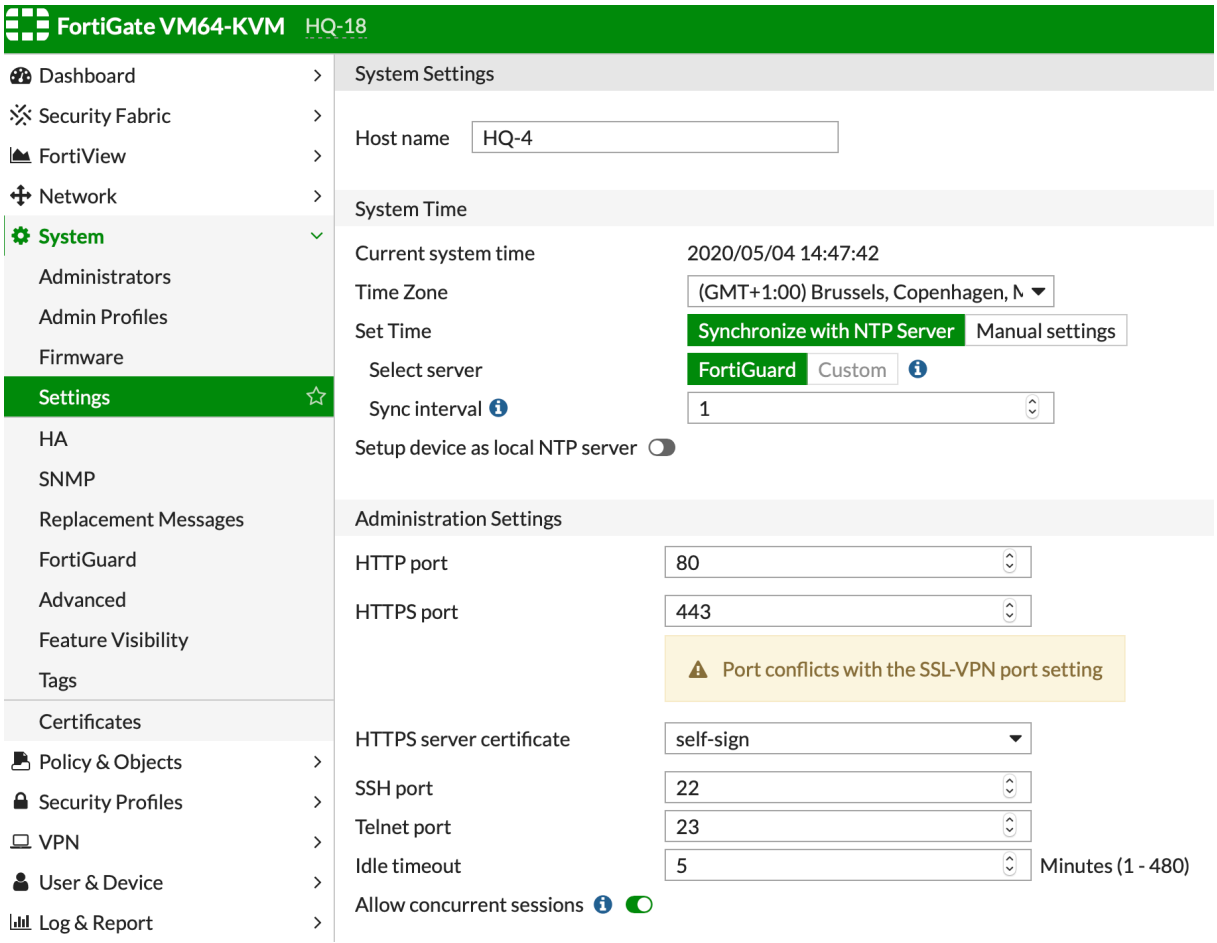
https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/281288/site-to-site-ipsec-vpn-with-two-fortigate-devices

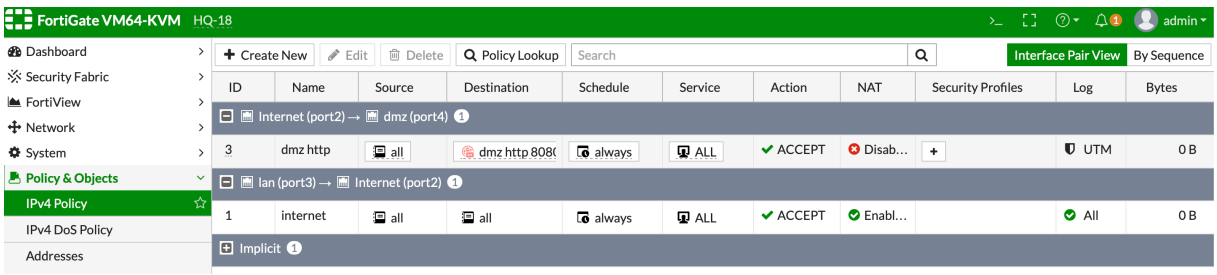


1/ Vérifier la configuration de HQ (nom et connectivité)
2/ Configurer Branch : Nom, interfaces, service DHCP, NAT, Policy
3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard
4/ Montrer la connectivité entre le LAN HQ (60.0/24) et le LAN Branch (61.0/24) et inversément via des tests pings et des logs.
5/ Quels sont les paramètres IPSEC utilisés par le Wizard ? Comment obtenir cette information.

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

```
HQ-18 # get system interface physical
== [onboard]
      ==[port1]
            mode: dhcp
            ip: 192.168.122.131 255.255.255.0
            ipv6: ::/0
            status: up
            speed: 1000Mbps (Duplex: full)
      ==[port2]
            mode: dhcp
            ip: 192.168.122.132 255.255.255.0
            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]
            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
```





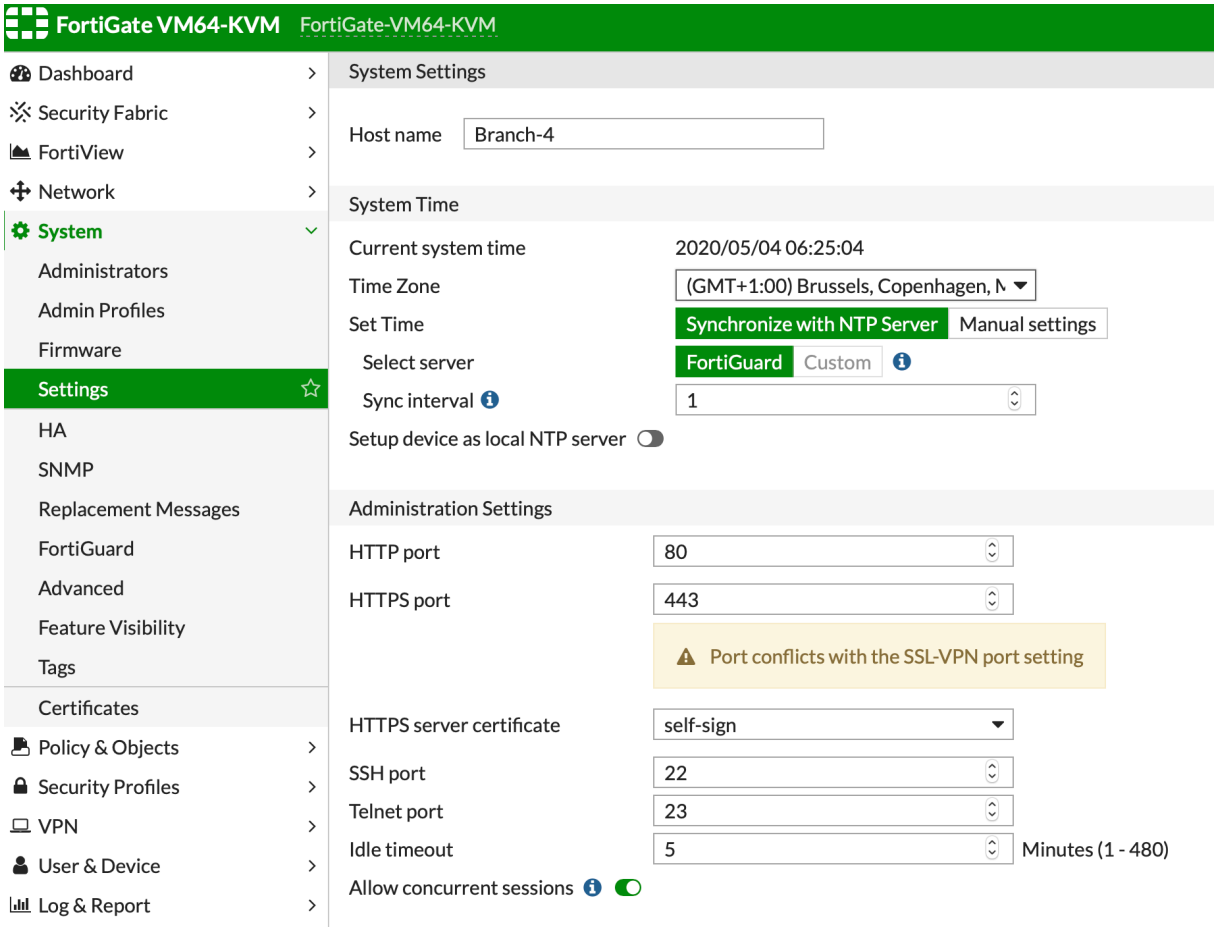

```
[root@client-hq ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=55 time=3.25 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=55 time=3.13 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=55 time=3.31 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=55 time=3.48 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=55 time=3.49 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=55 time=2.71 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=55 time=3.06 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=55 time=3.22 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=55 time=3.25 ms
```

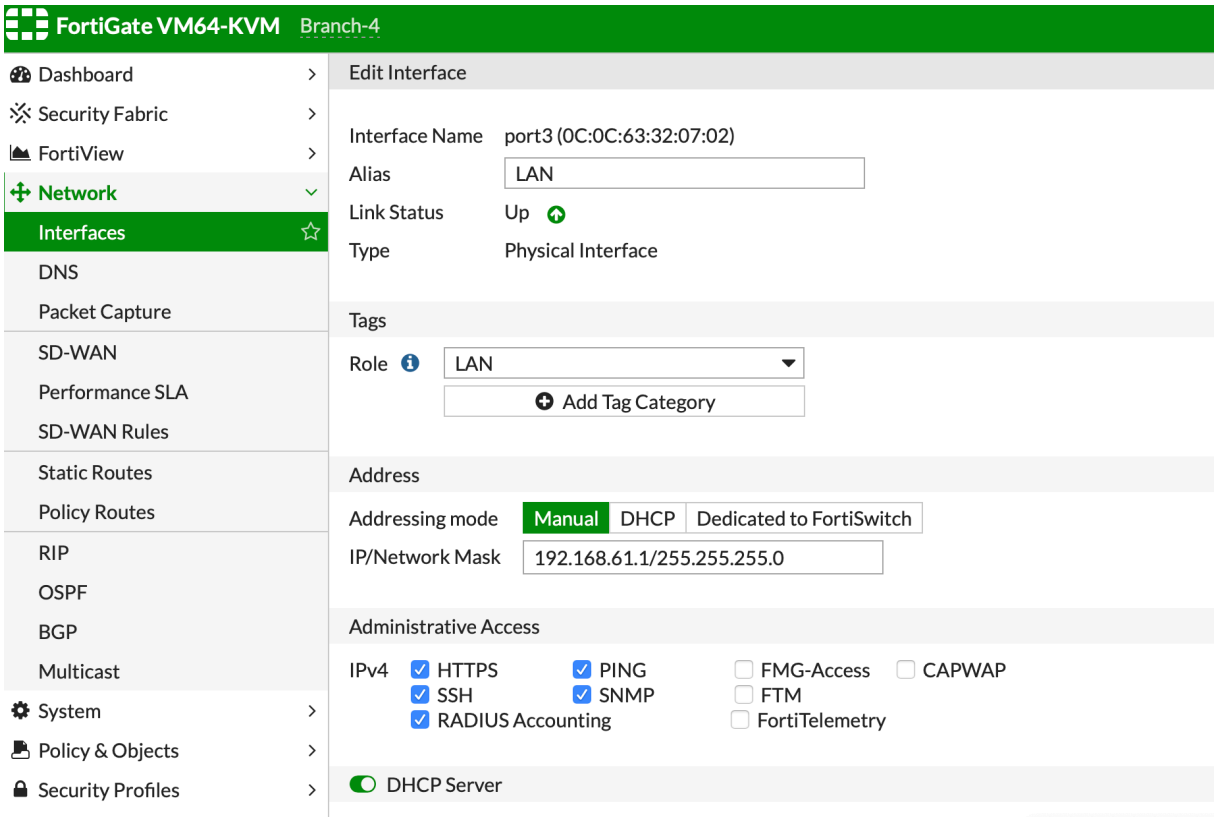
```
HQ-4 # execute ping 192.168.122.131
PING 192.168.122.131 (192.168.122.131): 56 data bytes
64 bytes from 192.168.122.131: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 192.168.122.131: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 192.168.122.131: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.122.131: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 192.168.122.131: icmp_seq=4 ttl=255 time=0.0 ms

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

HQ-4 # 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=6.0 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=2.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=2.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=2.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=2.4 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.3/3.1/6.0 ms
```

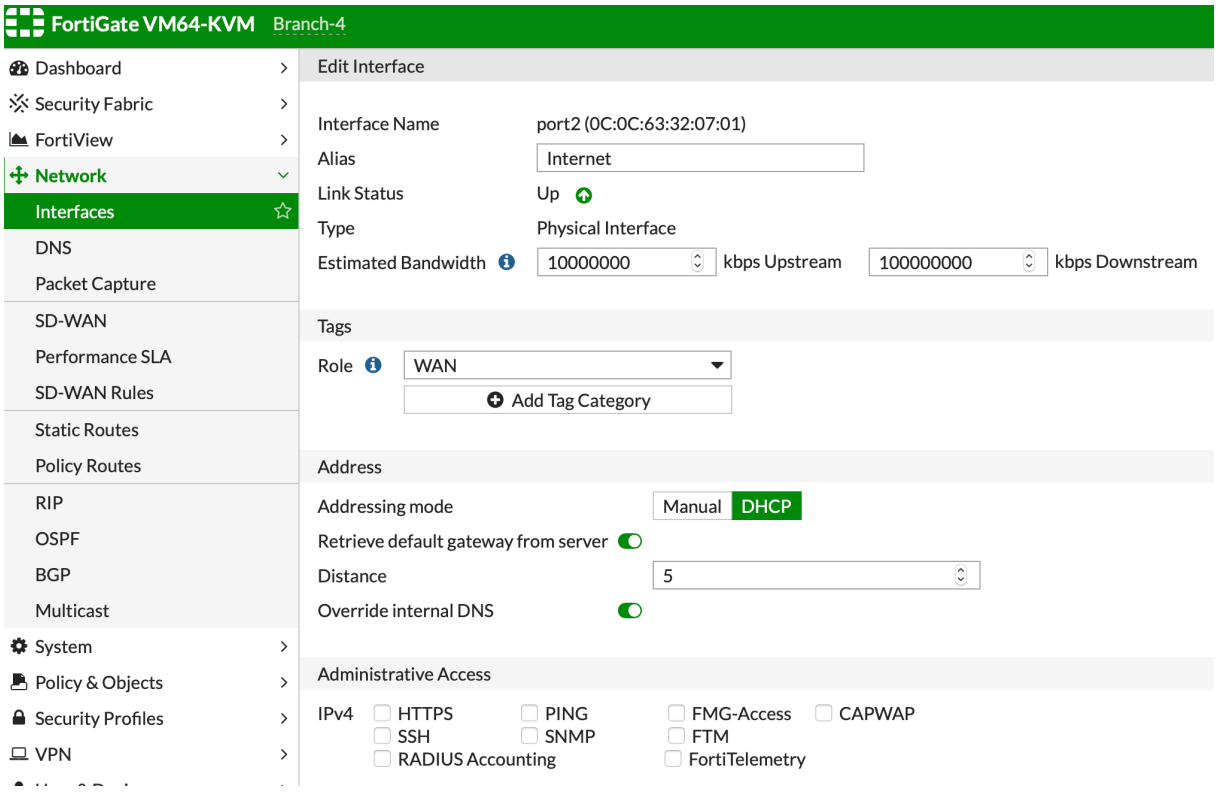
2/ Configurer Branch : Nom, interfaces, service DHCP, NAT, Policy

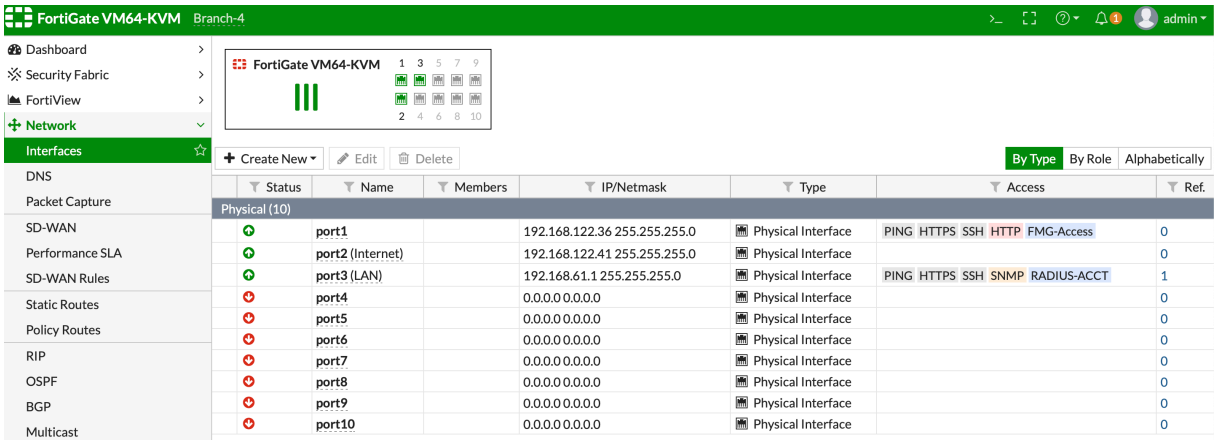
```
FortiGate-VM64-KVM # get system interface physical
== [onboard]
     ==[port1]
          mode: dhcp
          ip: 192.168.122.36 255.255.255.0
          ipv6: ::/0
          status: up
          speed: 1000Mbps (Duplex: full)
     ==[port2]
          mode: static
          ip: 0.0.0.0 0.0.0.0
          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
```

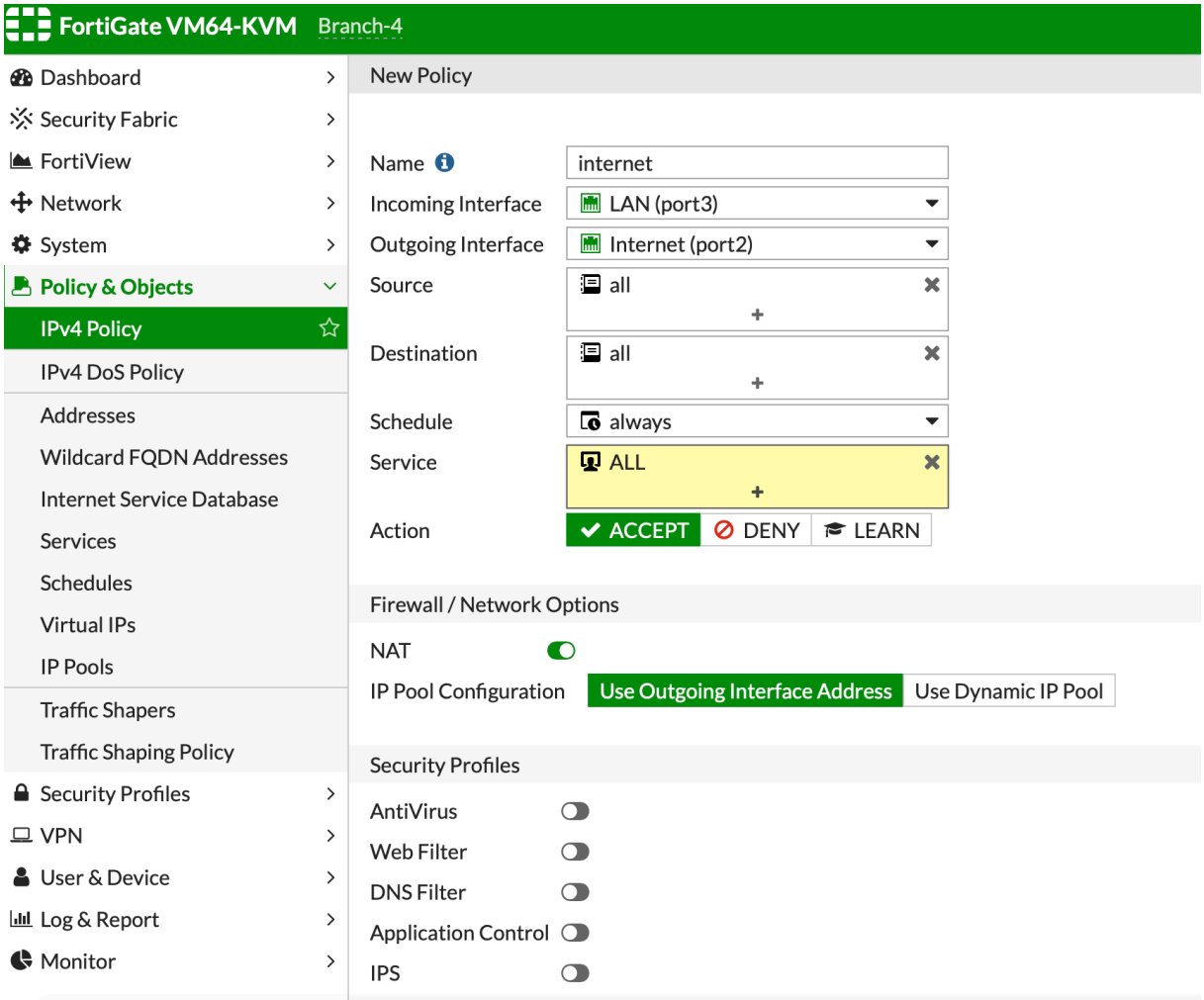
```
      ip: 0.0.0.0 0.0.0.0
      ipv6: ::/0
      status: down
      speed: n/a
==[port8]
      mode: static
      ip: 0.0.0.0 0.0.0.0
      ipv6: ::/0
      status: down
           speed: n/a
==[port9]
      mode: static
      ip: 0.0.0.0 0.0.0.0
      ipv6: ::/0
      status: down
      speed: n/a
==[port10]
      mode: static
      ip: 0.0.0.0 0.0.0.0
      ipv6: ::/0
      status: down
         speed: n/a
```

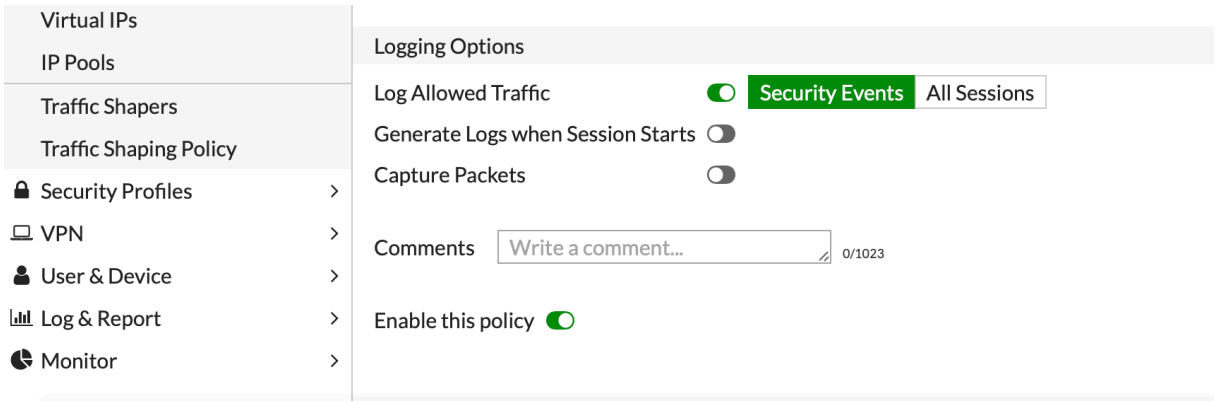


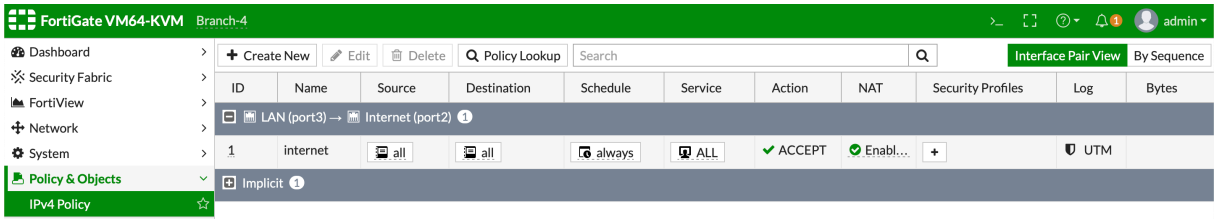

FortiGate VM64-KVM
Branch-4
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
Performance SLA
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
Edit Interface
Interface Name
port3 (0C:0C:63:32:07:02)
Alias
LAN
Link Status
Up
Type
Physical Interface
Tags
Role
LAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
Dedicated to FortiSwitch
IP/Network Mask
192.168.61.1/255.255.255.0
Administrative Access
IPv4
HTTPS
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry
DHCP Server


FortiGate VM64-KVM
Branch-4
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
Edit Interface
Interface Name
port2 (0C:0C:63:32:07:01)
Alias
Internet
Link Status
Up
Type
Physical Interface
Estimated Bandwidth
10000000
kbps Upstream
100000000
kbps Downstream
Tags
Role
WAN
Add Tag Category
Address
Addressing mode
Manual
DHCP
Retrieve default gateway from server
Distance
5
Override internal DNS
Administrative Access
IPv4
HTTPS
PING
FMG-Access
CAPWAP
SSH
SNMP
FTM
RADIUS Accounting
FortiTelemetry


FortiGate VM64-KVM
Branch-4
admin
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
Performance SLA
SD-WAN Rules
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
FortiGate VM64-KVM
Create New
Edit
Delete
By Type
By Role
Alphabetically
Status
Name
Members
IP/Netmask
Type
Access
Ref.
Physical (10)
port1 192.168.122.36 255.255.255.0 Physical Interface PING HTTPS SSH HTTP FMG-Access 0
port2 (Internet) 192.168.122.41 255.255.255.0 Physical Interface 0
port3 (LAN) 192.168.61.1 255.255.255.0 Physical Interface PING HTTPS SSH SNMP RADIUS-ACCT 1
port4 0.0.0.0 0.0.0.0 Physical Interface 0
port5 0.0.0.0 0.0.0.0 Physical Interface 0
port6 0.0.0.0 0.0.0.0 Physical Interface 0
port7 0.0.0.0 0.0.0.0 Physical Interface 0
port8 0.0.0.0 0.0.0.0 Physical Interface 0
port9 0.0.0.0 0.0.0.0 Physical Interface 0
port10 0.0.0.0 0.0.0.0 Physical Interface 0

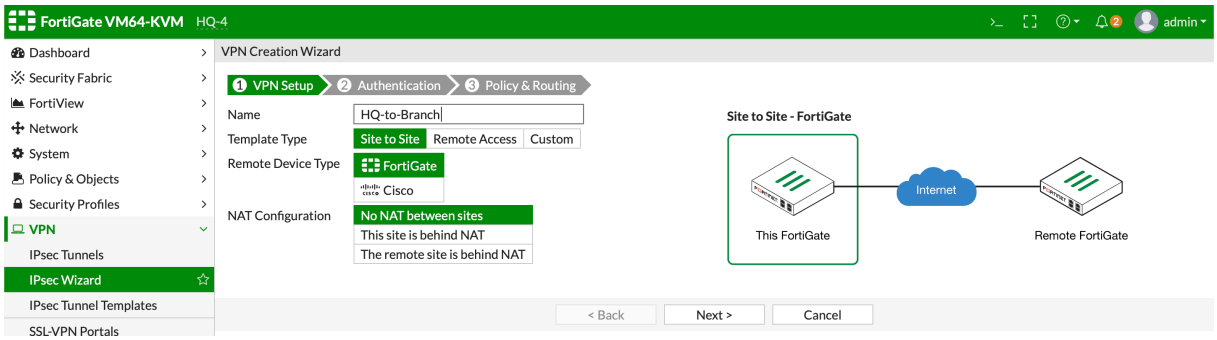

FortiGate VM64-KVM
Branch-4
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
IPv4 DoS Policy
Addresses
Wildcard FQDN Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Traffic Shapers
Traffic Shaping Policy
Security Profiles
VPN
User & Device
Log & Report
Monitor
New Policy
Name
internet
Incoming Interface
LAN (port3)
Outgoing Interface
Internet (port2)
Source
all
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
IPS

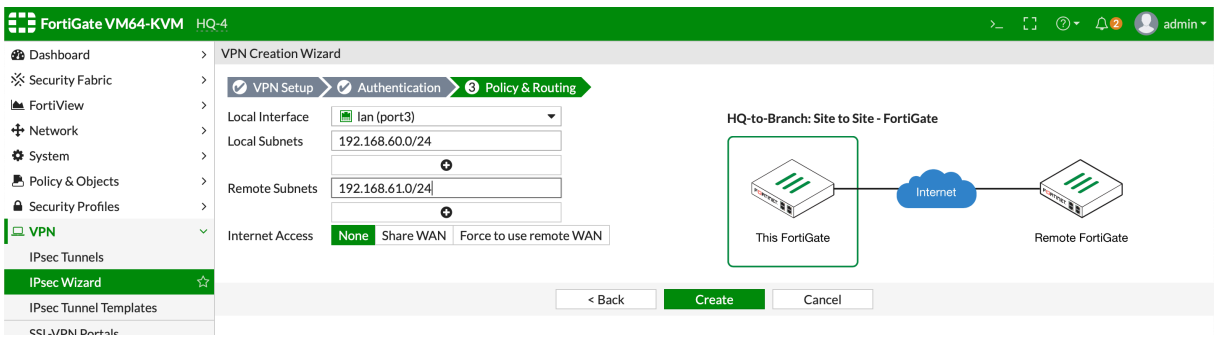


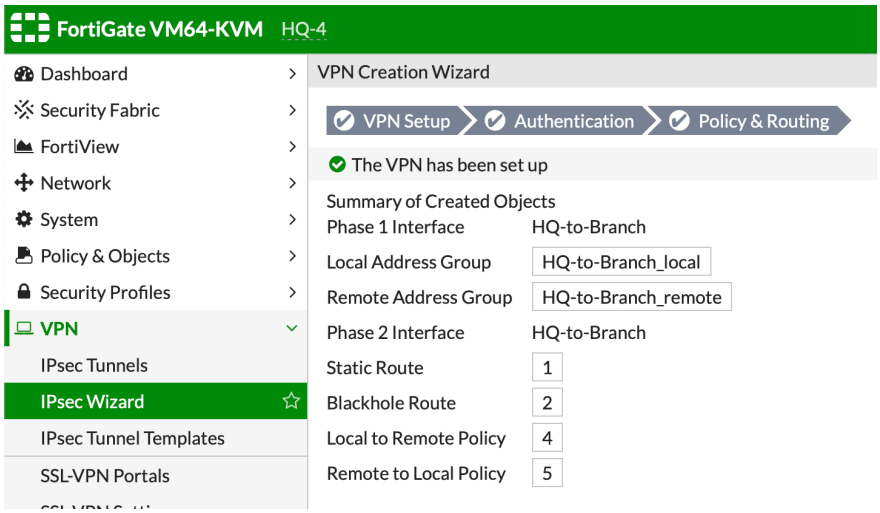


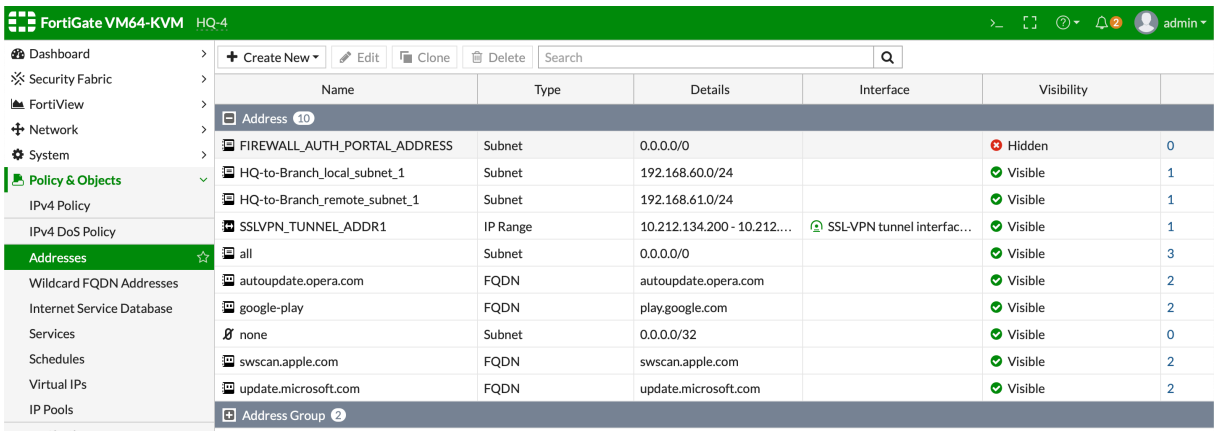
3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard

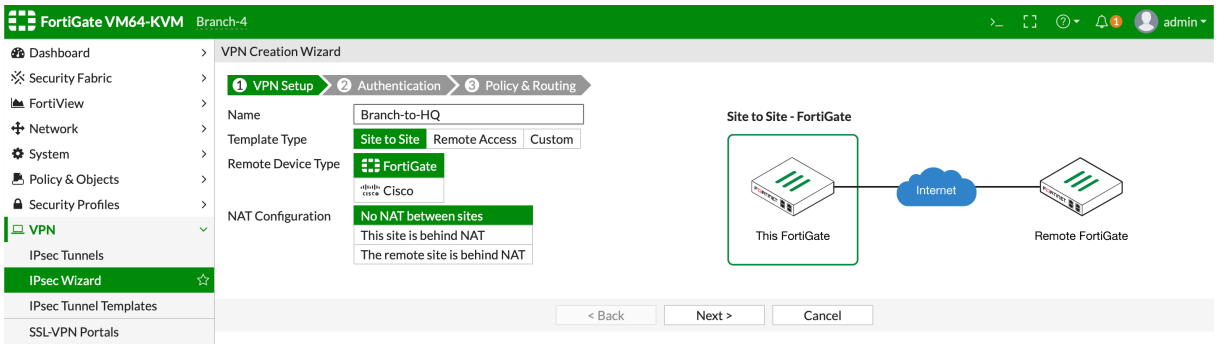
On suit l'énoncé du lien suivant en adaptant par rapport à notre topologie : https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/783623/configuring-ipsec-vpn-on-hq

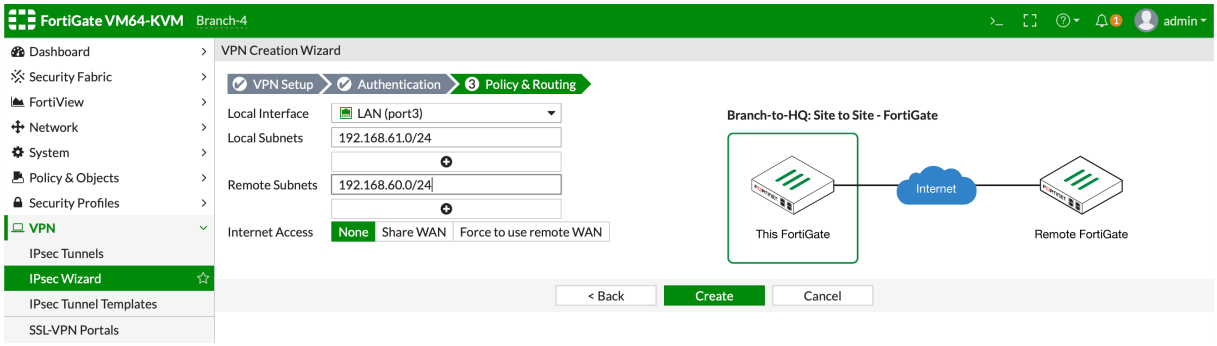


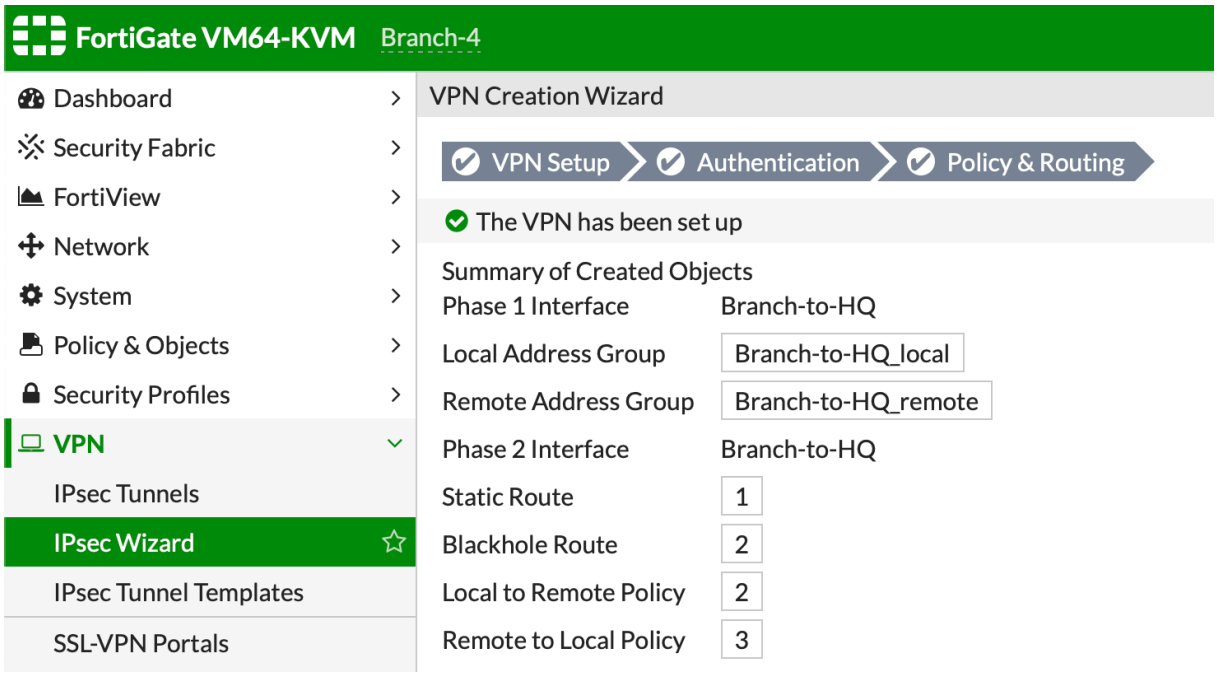



FortiGate VM64-KVM HQ-4
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
VPN Creation Wizard
VPN Setup
Authentication
Policy & Routing
The VPN has been set up
Summary of Created Objects
Phase 1 Interface HQ-to-Branch
Local Address Group HQ-to-Branch_local
Remote Address Group HQ-to-Branch_remote
Phase 2 Interface HQ-to-Branch
Static Route 1
Blackhole Route 2
Local to Remote Policy 4
Remote to Local Policy 5

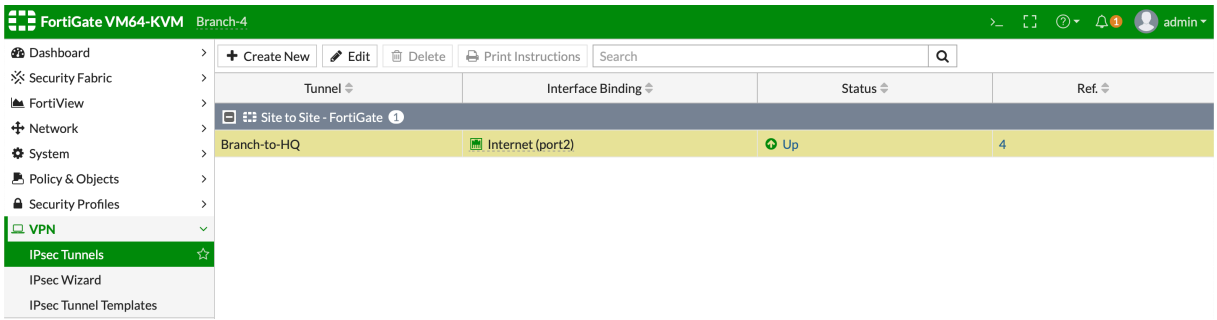

FortiGate VM64-KVM HQ-4
admin
Create New
Edit
Clone
Delete
Search
Name
Type
Details
Interface
Visibility
Address 10
FIREWALL_AUTH_PORTAL_ADDRESS Subnet 0.0.0.0/0 Hidden 0
HQ-to-Branch_local_subnet_1 Subnet 192.168.60.0/24 Visible 1
HQ-to-Branch_remote_subnet_1 Subnet 192.168.61.0/24 Visible 1
SSLVPN_TUNNEL_ADDR1 IP Range 10.212.134.200 - 10.212.... SSL-VPN tunnel interfac... Visible 1
all Subnet 0.0.0.0/0 Visible 3
autoupdate.opera.com FQDN autoupdate.opera.com Visible 2
google-play FQDN play.google.com Visible 2
none Subnet 0.0.0.0/32 Visible 0
swscan.apple.com FQDN swscan.apple.com Visible 2
update.microsoft.com FQDN update.microsoft.com Visible 2
Address Group 2
Policy & Objects
IPv4 Policy
IPv4 DoS Policy
Addresses
Wildcard FQDN Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools


FortiGate VM64-KVM Branch-4
admin
VPN Creation Wizard
1 VPN Setup
2 Authentication
3 Policy & Routing
Name Branch-to-HQ
Template Type Site to Site Remote Access Custom
Remote Device Type FortiGate Cisco
NAT Configuration No NAT between sites
This site is behind NAT
The remote site is behind NAT
Site to Site - FortiGate
Internet
This FortiGate
Remote FortiGate
< Back
Next >
Cancel


FortiGate VM64-KVM Branch-4
admin
VPN Creation Wizard
VPN Setup
Authentication
3 Policy & Routing
Local Interface LAN (port3)
Local Subnets 192.168.61.0/24
Remote Subnets 192.168.60.0/24
Internet Access None Share WAN Force to use remote WAN
Branch-to-HQ: Site to Site - FortiGate
Internet
This FortiGate
Remote FortiGate
< Back
Create
Cancel



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.




```
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=3.44 ms
64 bytes from 192.168.61.1: icmp_seq=2 ttl=254 time=2.03 ms
64 bytes from 192.168.61.1: icmp_seq=3 ttl=254 time=2.35 ms
64 bytes from 192.168.61.1: icmp_seq=4 ttl=254 time=2.02 ms
64 bytes from 192.168.61.1: icmp_seq=5 ttl=254 time=2.24 ms
64 bytes from 192.168.61.1: icmp_seq=6 ttl=254 time=5.83 ms
64 bytes from 192.168.61.1: icmp_seq=7 ttl=254 time=2.34 ms
64 bytes from 192.168.61.1: icmp_seq=8 ttl=254 time=2.21 ms
64 bytes from 192.168.61.1: icmp_seq=9 ttl=254 time=2.03 ms

[root@client-hq ~]# ping 192.168.61.2
PING 192.168.61.2 (192.168.61.2) 56(84) bytes of data.
64 bytes from 192.168.61.2: icmp_seq=1 ttl=62 time=2.95 ms
64 bytes from 192.168.61.2: icmp_seq=2 ttl=62 time=3.04 ms
64 bytes from 192.168.61.2: icmp_seq=3 ttl=62 time=3.14 ms
64 bytes from 192.168.61.2: icmp_seq=4 ttl=62 time=3.16 ms
64 bytes from 192.168.61.2: icmp_seq=5 ttl=62 time=2.90 ms
64 bytes from 192.168.61.2: icmp_seq=6 ttl=62 time=2.85 ms
64 bytes from 192.168.61.2: icmp_seq=7 ttl=62 time=3.06 ms
```

```
64 bytes from 192.168.61.2: icmp_seq=8 ttl=62 time=3.01 ms
```

```
[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=2.54 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=254 time=2.31 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=254 time=2.15 ms
64 bytes from 192.168.60.1: icmp_seq=4 ttl=254 time=1.89 ms
64 bytes from 192.168.60.1: icmp_seq=5 ttl=254 time=2.15 ms
64 bytes from 192.168.60.1: icmp_seq=6 ttl=254 time=1.74 ms
64 bytes from 192.168.60.1: icmp_seq=7 ttl=254 time=1.91 ms
64 bytes from 192.168.60.1: icmp_seq=8 ttl=254 time=2.27 ms
64 bytes from 192.168.60.1: icmp_seq=9 ttl=254 time=2.13 ms
```

```
[root@client-branch ~]# ping 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
From 192.168.122.131 icmp_seq=3 Destination Host Unreachable
From 192.168.122.131 icmp_seq=6 Destination Host Unreachable
From 192.168.122.131 icmp_seq=9 Destination Host Unreachable
From 192.168.122.131 icmp_seq=12 Destination Host Unreachable
From 192.168.122.131 icmp_seq=15 Destination Host Unreachable
From 192.168.122.131 icmp_seq=18 Destination Host Unreachable
From 192.168.122.131 icmp_seq=21 Destination Host Unreachable
From 192.168.122.131 icmp_seq=24 Destination Host Unreachable
From 192.168.122.131 icmp_seq=27 Destination Host Unreachable
From 192.168.122.131 icmp_seq=30 Destination Host Unreachable
From 192.168.122.131 icmp_seq=33 Destination Host Unreachable
From 192.168.122.131 icmp_seq=36 Destination Host Unreachable
From 192.168.122.131 icmp_seq=39 Destination Host Unreachable
From 192.168.122.131 icmp_seq=42 Destination Host Unreachable
```

La connectivité ne semble fonctionner que dans un seul sens : de HQ vers Branch

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

Fichiers de configuration :
HQ-4_20200504_1635.conf
Branch-4_20200504_1635.conf