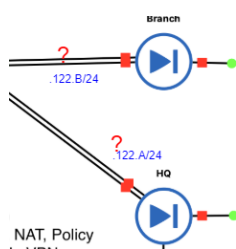
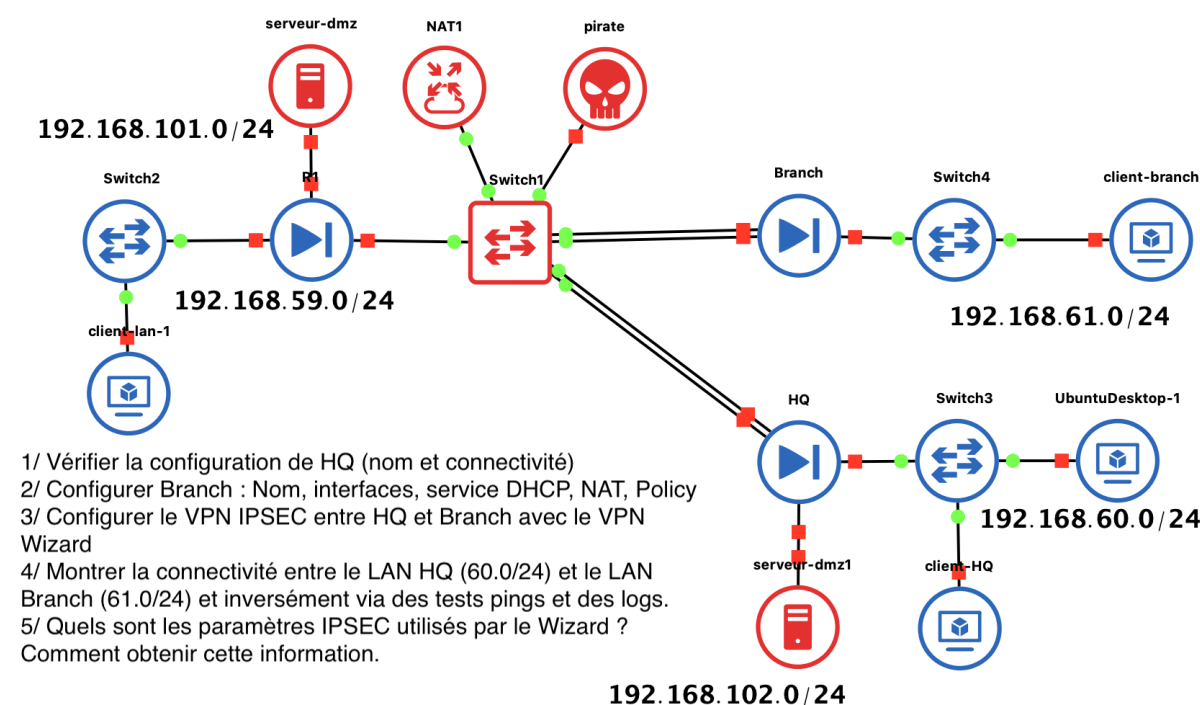


## Lab VPN IPSEC site-à-site Fortinet

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>



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

The screenshot shows the FortiGate VM64-KVM web interface. The top bar is green with the FortiGate logo and the text "FortiGate VM64-KVM HQ-18". The left sidebar contains a menu with the following items: Dashboard, Security Fabric, FortiView, Network, System (highlighted in green), Administrators, Admin Profiles, Firmware, Settings (highlighted in green), HA, and SNMP. The main content area is titled "System Settings" and contains the following fields: Host name (HQ-14), System Time (2020/05/04 14:36:18), Time Zone ((GMT+1:00) Brussels, Copenhagen, N), Set Time (Synchronize with NTP Server, Manual settings), Select server (FortiGuard, Custom), Sync interval (1), and Setup device as local NTP server (toggle off).

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

2

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

admin

2

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

SSH

RADIUS Accounting

PING

SNMP

FTM

FortiTelemetry

FMG-Access

CAPWAP

Miscellaneous

Scan Outgoing Connections to Botnet Sites

Disable

Block

Monitor

Status

Comments

Interface State

Enabled

Disabled

OK

Cancel

## Port 3



FortiGate VM64-KVM Branch14

Dashboard > Security Fabric > FortiView > Network > Interfaces

### Edit Interface

Interface Name: port3 (OC:E5:E0:28:1E: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: 192.168.60.1/255.255.255.0

Administrative Access  
 IPv4: ☒ HTTPS ☒ PING ☐ FMG-Access ☐ CAPWAP  
☒ SSH ☒ SNMP ☐ FTM  
☒ RADIUS Accounting ☐ FortiTelemetry

DHCP Server  
 Address Range  
 Create New Edit Delete  
 Starting IP End IP  
 192.168.60.2 192.168.60.254  
 Netmask: 255.255.255.0  
 Default Gateway: Same as Interface IP Specify  
 DNS Server: Same as System DNS Same as Interface IP Specify  
 Advanced...

Networked Devices  
 Device Detection: ☒  
 Active Scanning: ☐

Admission Control  
 Security Mode: None

Secondary IP Address

Status  
 Comments

OK Cancel

Les ports sont configurés

FortiGate VM64-KVM Branch14

Dashboard > Security Fabric > FortiView > Network > Interfaces

FortiGate VM64-KVM

1 3 5 7 9  
2 4 6 8 10

By Type By Role Alphabetically

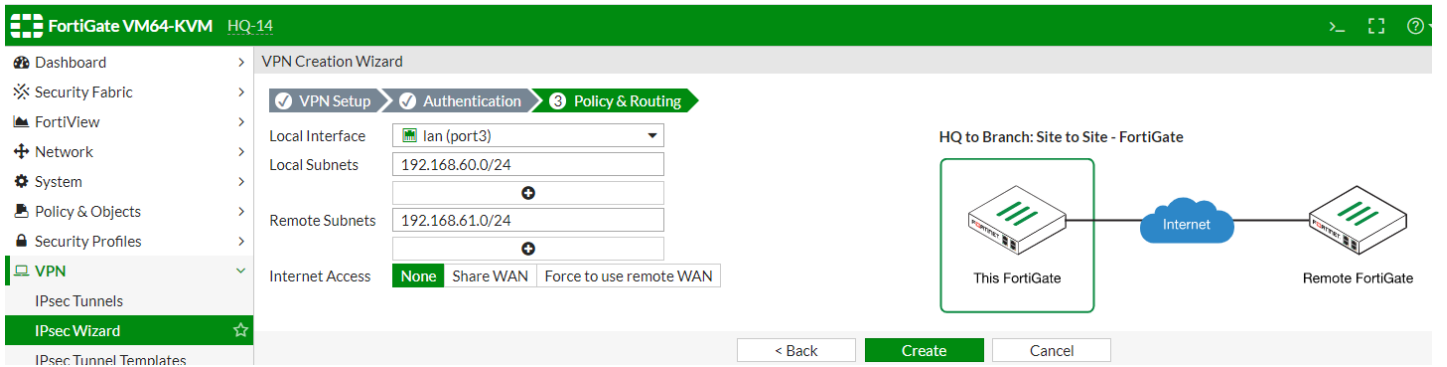
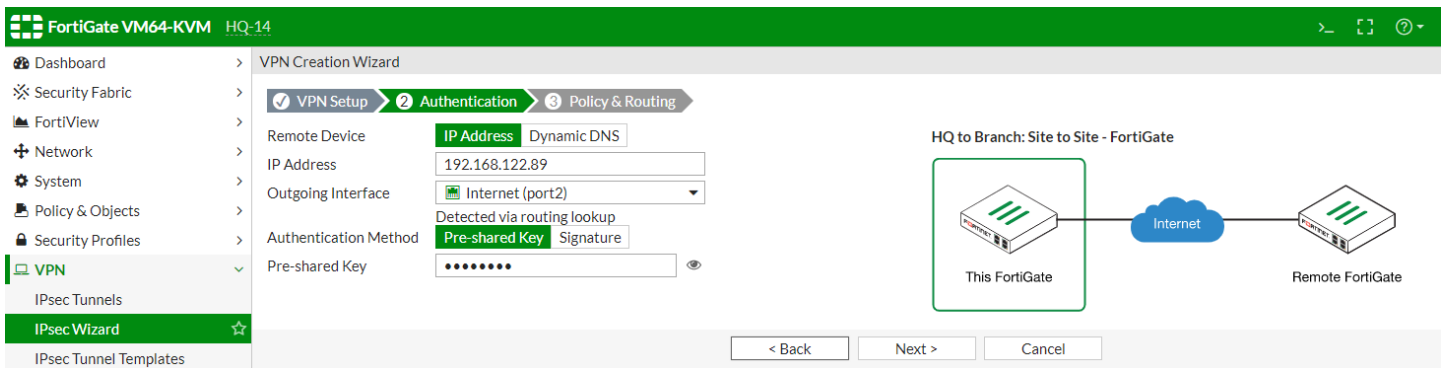
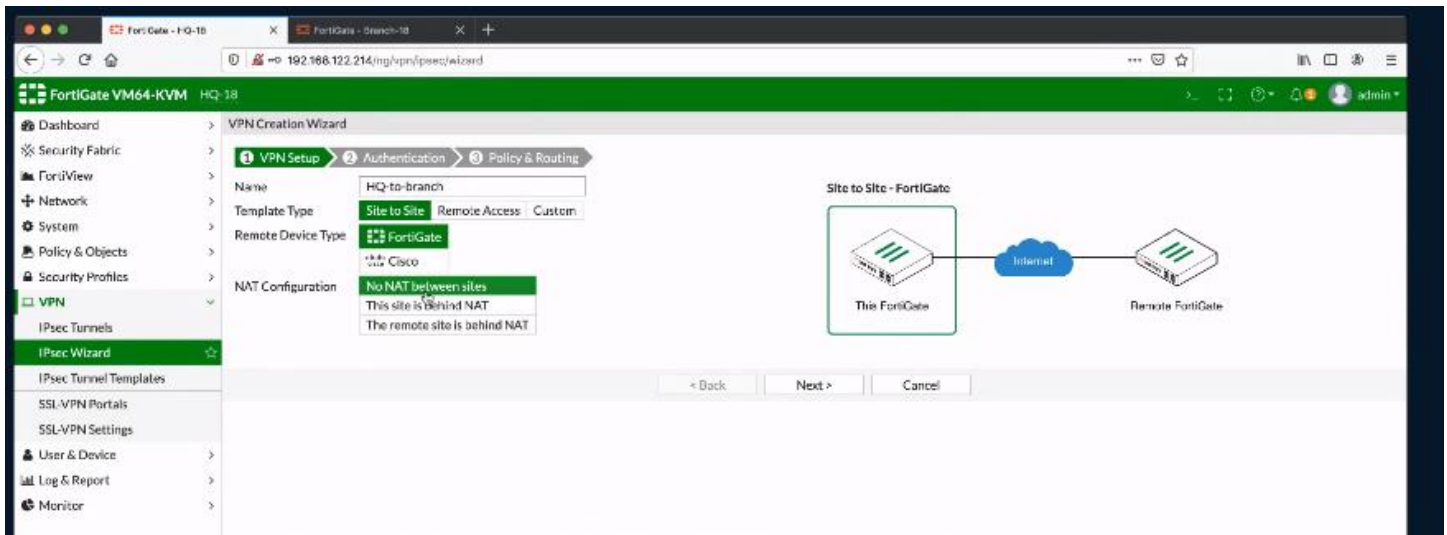
Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (11)						
<input checked="" type="checkbox"/>	port1		192.168.122.51 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
<input checked="" type="checkbox"/>	port2 (Internet)		192.168.122.52 255.255.255.0	Physical Interface		4
<input checked="" type="checkbox"/>	port3 (LAN)		192.168.60.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP RADIUS-ACCT	1
<input checked="" type="checkbox"/>	port4		0.0.0.0 0.0.0.0	Physical Interface		0
<input checked="" type="checkbox"/>	port5		0.0.0.0 0.0.0.0	Physical Interface		0

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

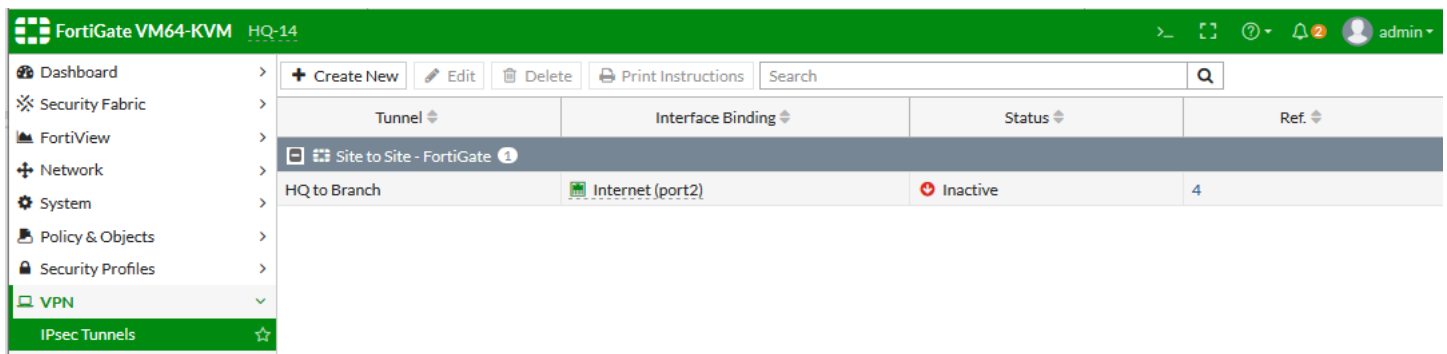
Configurer manuellement

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

FortiGate VM64-KVM

HQ-14

admin

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

IPsec Tunnels

Create New

Edit

Delete

Print Instructions

Search

Tunnel

Interface Binding

Status

Ref

Site to Site - FortiGate

HQ to Branch

Internet (port2)

Inactive

4

Vérifier la configuration

FortiGate VM64-KVM

HQ-14

admin

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPsec Tunnels

Create New

Edit

Delete

Policy Lookup

Search

Interface Pair View

By Sequence

ID

Name

Source

Destination

Schedule

Service

Action

NAT

Security Profiles

Log

Bytes

HQ to Branch → lan (port3)

5

vpn\_HQ to Branch\_remote

HQ to Branch\_remote

HQ to Branch\_local

always

ALL

ACCEPT

Disabled

UTM

0 B

Internet (port2) → dmz (port4)

4

vpn\_HQ to Branch\_local

HQ to Branch\_local

HQ to Branch\_remote

always

ALL

ACCEPT

Disabled

UTM

0 B

lan (port3) → Internet (port2)

0

Implicit Deny

all

all

always

ALL

DENY

Disabled

69.84 kB

FortiGate VM64-KVM

HQ-14

admin

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPsec Tunnels

Create New

Edit

Clone

Delete

Search

Name

Type

Details

Interface

Visibility

Ref.

Address

FIREWALL\_AUTH\_PORTA...

Subnet

0.0.0.0/0

Hidden

0

HQ to Branch\_local\_subnet...

Subnet

192.168.60.0/24

Visible

1

HQ to Branch\_remote\_sub...

Subnet

192.168.61.0/24

Visible

1

SSLVPN\_TUNNEL\_ADDR1

IP Range

10.212.134.200 - 10.212.134.2...

SSL-VPN tunnel interface (ssl.r...

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

HQ to Branch\_local

Address Group

HQ to Branch\_local\_subnet\_1

Visible

3

HQ to Branch\_remote

Address Group

HQ to Branch\_remote\_subnet

Visible

5

Vérification de la sous interface sur le port WAN

FortiGate VM64-KVM

HQ-14

admin

Dashboard

Security Fabric

FortiView

Network

System

Create New

Edit

Delete

By Type

By Role

Alphabetically

Status

Name

Members

IP/Netmask

Type

Access

Ref.

Physical (11)

port1

192.168.122.89 255.255.255.0

Physical Interface

PING HTTPS SSH HTTP FMG-Access

0

port2 (Internet)

192.168.122.90 255.255.255.0

Physical Interface

5

HQ to Branch

0.0.0.0 0.0.0.0

Tunnel Interface

4

port3 (lan)

192.168.60.1 255.255.255.0

Physical Interface

PING HTTPS SSH SNMP RADIUS-ACCT

4

port4 (dmz)

192.168.102.1 255.255.255.0

Physical Interface

1

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

Vérification des routes

FortiGate VM64-KVM HQ-14

Dashboard

Security Fabric

FortiView

Network

Interfaces

DNS

Packet Capture

SD-WAN

Performance SLA

SD-WAN Rules

Static Routes

Create New

Edit

Clone

Delete

Destination	Gateway	Interface	Comment
HQ to Branch_remote		HQ to Branch	VPN: HQ to Branch (Created by V...
HQ to Branch_remote		Blackhole	VPN: HQ to Branch (Created by V...

Vérification si le tunnel est monté

FortiGate VM64-KVM HQ-14

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

IPsec Tunnels

IPsec Wizard

Create New

Edit

Delete

Print Instructions

Search

Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate 1			
HQ to Branch	Internet (port2)	Inactive	4

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

FortiGate VM64-KVM Branch14

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

IPsec Tunnels

Create New

Edit

Delete

Print Instructions

Search

Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate 1			
Branch to HQ	Internet (port2)	Inactive	4

Vérifier la configuration

FortiGate VM64-KVM Branch14

Dashboard Security Fabric FortiView Network System Policy & Objects IPv4 Policy IPv4 DoS Policy Addresses Wildcard FQDN Addresses

Create New Edit Delete Policy Lookup Search Interface Pair View By Sequence

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Branch to HQ → Internet (port2) 1									
2	vpn_Branch to HQ_remote	Branch to HQ_remote	Branch to HQ_local	always	ALL	ACCEPT	Disabled		
Internet (port2) → Branch to HQ 1									
1	vpn_Branch to HQ_local	Branch to HQ_local	Branch to HQ_remote	always	ALL	ACCEPT	Disabled		
Implicit 1									
0	Implicit Deny	all	all	always	ALL	DENY			

FortiGate VM64-KVM Branch14

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

Create New Edit Clone Delete Search

Name	Type	Details	Interface	Visibility	Ref.
Address 10					
Branch to HQ_local_su...	Subnet	192.168.122.0/24		Visible	1
Branch to HQ_remote...	Subnet	192.168.61.0/24		Visible	1
FIREWALL_AUTH_PO...	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_AD...	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
all	Subnet	0.0.0.0/0		Visible	0
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					
Branch to HQ_local	Address Group	Branch to HQ_local_subnet_1		Visible	3
Branch to HQ_remote	Address Group	Branch to HQ_remote_subnet_1		Visible	5

Vérification de la sous interface sur le port WAN

FortiGate VM64-KVM Branch14

Dashboard Security Fabric FortiView Network Interfaces DNS Packet Capture SD-WAN Performance SLA SD-WAN Rules Static Routes Policy Routes

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
+	port2 (Internet)		192.168.122.52 255.255.255.0	Physical Interface		4
	Branch to HQ		0.0.0.0 0.0.0.0	Tunnel Interface		4
+	port3 (LAN)		192.168.60.1 255.255.255.0	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

Verification des routes statiques

FortiGate VM64-KVM Branch14

Dashboard Security Fabric FortiView Network Interfaces DNS Packet Capture SD-WAN Performance SLA SD-WAN Rules Static Routes

Create New Edit Clone Delete

Destination	Gateway	Interface	Comment
Branch to HQ_remote		Branch to HQ	VPN: Branch to HQ (Created by V...
Branch to HQ_remote		Blackhole	VPN: Branch to HQ (Created by V...

#### 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 ~]#
```

FortiGate VM64-KVM HQ-14									
Add Filter									
#	Date/Time	Level	Action	Status	Message	VPN Tunnel			
1	30 seconds ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
2	Minute ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
3	Minute ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
4	2 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
5	2 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
6	3 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
7	3 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
8	4 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
9	4 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
10	5 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
11	5 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
12	5 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
13	6 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
14	7 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
15	7 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
16	8 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
17	8 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
18	9 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			
19	9 minutes ago		negotiate	success	progress IPsec phase 1	HQ to Branch			

FortiGate VM64-KVM Branch14						
Add Filter						
#	Date/Time	Level	Action	Status	Message	VPN Tunnel
1	11 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
2	11 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
3	17 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
4	17 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
5	20 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
6	20 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
7	20 seconds ago		negotiate	success	progress IPsec phase 1	Branch to HQ
8	20 seconds ago		negotiate	success	progress IPsec phase 1	Branch to HQ
9	20 seconds ago		negotiate	success	progress IPsec phase 1	Branch to HQ
10	30 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
11	30 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
12	42 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
13	42 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
14	48 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
15	48 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
16	51 seconds ago		negotiate	failure	progress IPsec phase 1	Branch to HQ
17	51 seconds ago		negotiate	negotiate_error	IPsec phase 1 error	Branch to HQ
18	51 seconds ago		negotiate	success	progress IPsec phase 1	Branch to HQ

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

Dans VPN -> Ipsec tunnel

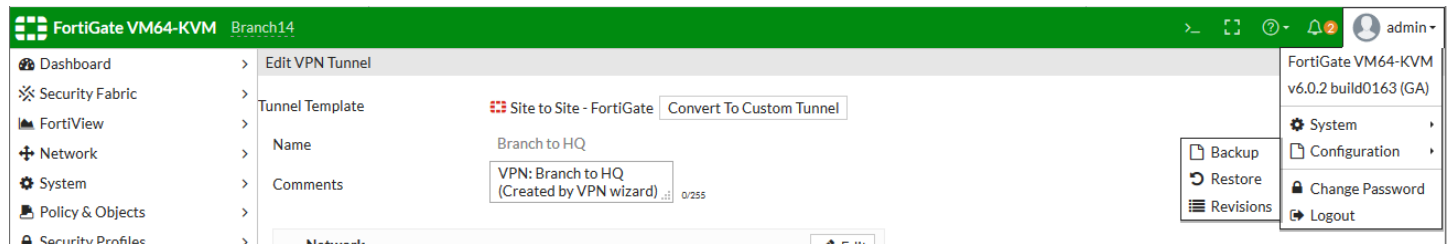
FortiGate VM64-KVM Branch14			
+ Create New Edit Delete Print Instructions Search			
Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate 1			
Branch to HQ	Internet (port2)	Inactive	4

on double-clique :

FortiGate VM64-KVM Branch14							
<div> <div>Dashboard</div> <div>Security Fabric</div> <div>FortiView</div> <div>Network</div> <div>System</div> <div>Policy &amp; Objects</div> <div>Security Profiles</div> <div>VPN</div> <div>IPsec Tunnels</div> <div>IPsec Wizard</div> <div>IPsec Tunnel Templates</div> <div>SSL-VPN Portals</div> <div>SSL-VPN Settings</div> <div>User &amp; Device</div> <div>Log &amp; Report</div> <div>Monitor</div> </div>	<div> <div>Edit VPN Tunnel</div> <div> <div>Tunnel Template</div> <div>Site to Site - FortiGate</div> <div>Convert To Custom Tunnel</div> </div> <div> <div>Name</div> <div>Branch to HQ</div> </div> <div> <div>Comments</div> <div>VPN: Branch to HQ (Created by VPN wizard) 0/255</div> </div> <div> <div>Network</div> <div>Remote Gateway : Static IP Address (192.168.122.52) , Outgoing Interface : port2</div> <div>Edit</div> </div> <div> <div>Authentication</div> <div>Authentication Method : Pre-shared Key</div> <div>Edit</div> </div> <div> <div>Phase 2 Selectors</div> <table> <tr> <th></th><th>Local Address</th><th>Remote Address</th></tr> <tr> <td>Branch to HQ</td><td>Branch to HQ_local</td><td>Branch to HQ_remote</td></tr> </table> </div> <div> <div>OK</div> <div>Cancel</div> </div> </div>		Local Address	Remote Address	Branch to HQ	Branch to HQ_local	Branch to HQ_remote
	Local Address	Remote Address					
Branch to HQ	Branch to HQ_local	Branch to HQ_remote					

## 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

