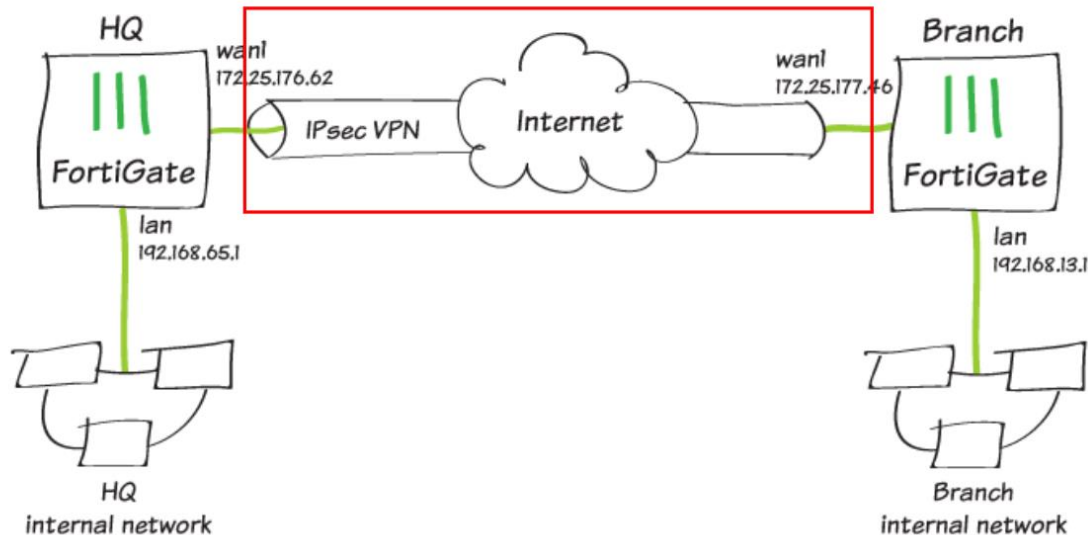


Lab VPN IPSEC site-à-site Fortinet

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

forti-1

forti-2



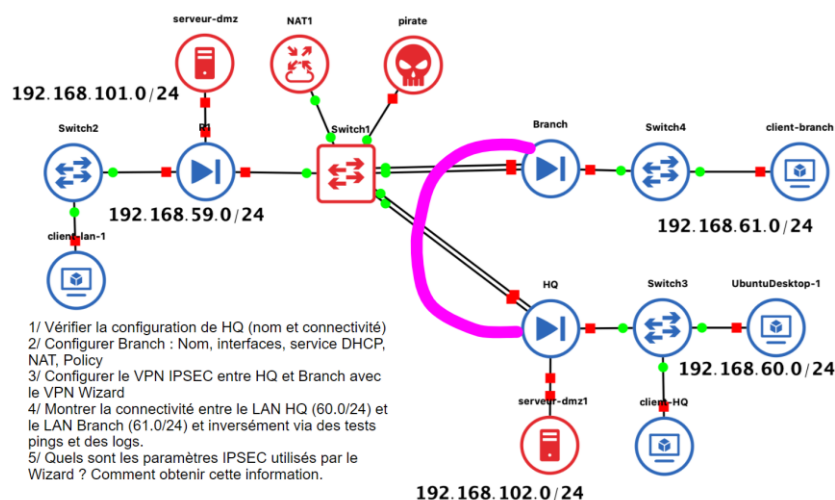
Objectifs :

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

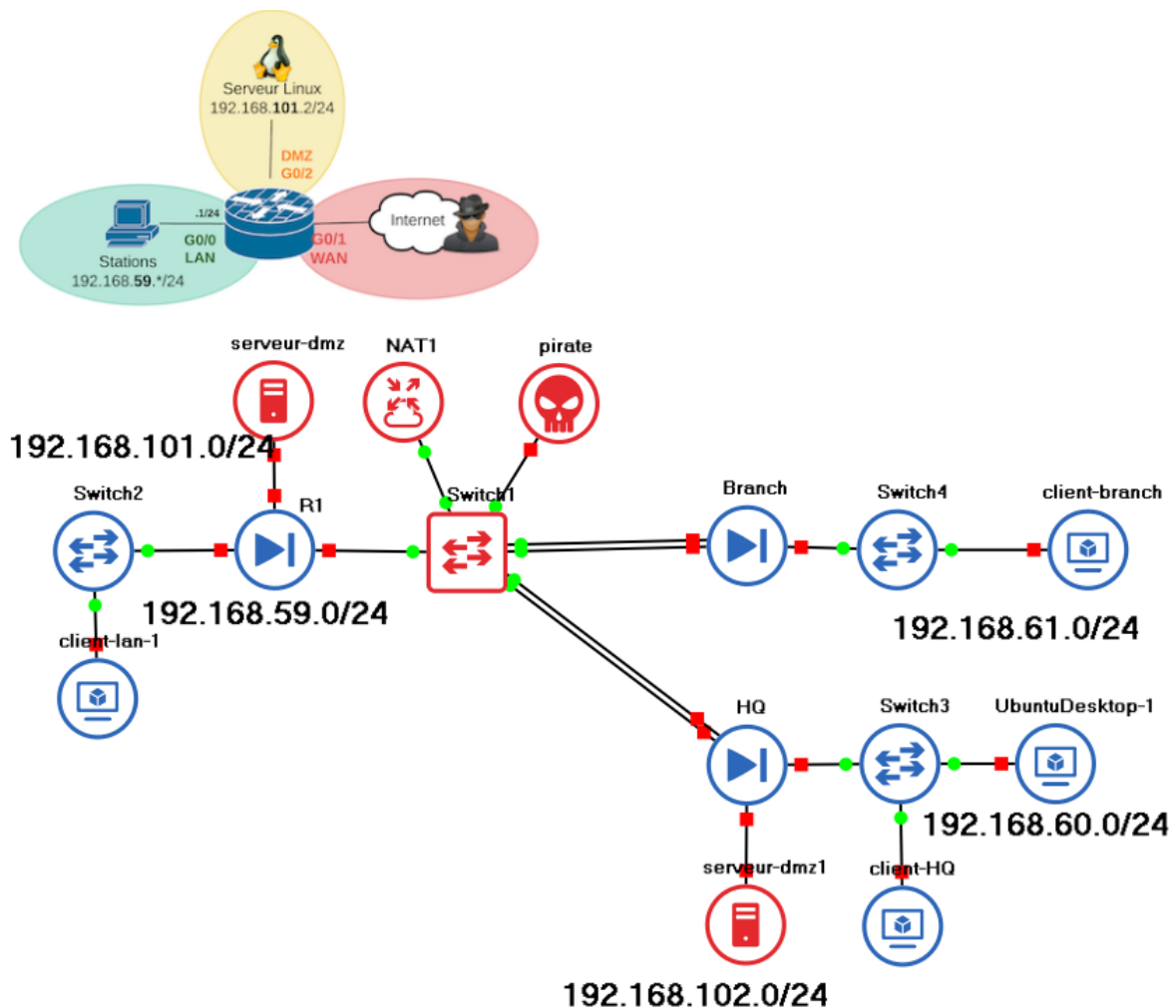


Consignes Lab

- 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

FortiGate VM64-KVM HQ-18

Dashboard > System Settings

Security Fabric >

FortiView >

Network >

System >

Administrators

Admin Profiles

Firmware

Settings ☆

HA

SNMP

Replacement Messages

FortiGuard

Advanced

Feature Visibility

Tags

Certificates

Policy & Objects >

Security Profiles >

VPN >

User & Device >

Log & Report >

Monitor >

System Settings

Host name

System Time

Current system time 2020/05/04 19:59:57

Time Zone

Set Time

Select server ⓘ

Sync interval ⓘ

Setup device as local NTP server ☐

Administration Settings

HTTP port

HTTPS port

⚠ Port conflicts with the SSL-VPN port setting

HTTPS server certificate

SSH port

Telnet port

Idle timeout Minutes (1 - 480)

Allow concurrent sessions ⓘ ☒

Password Policy

Policy & Objects -> IPv4 Policy

FortiGate VM64-KVM HQ-2

Dashboard > + Create New Edit Delete Policy Lookup Search

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

IPv4 Policy ☆

IPv4 DoS Policy

Addresses

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	Internet (port2) -> dmz (port4)	dmz http	all	always	http 8080	ACCEPT	Disabled	UTM		0B
1	Internet (port2) -> Internet (port2)	all	all	always	ALL	ACCEPT	Enabled	All		0B
2	Internet (port2) -> Internet (port2)	all	all	always	ALL	ACCEPT	Enabled	All		0B
3	Implicit	all	all	always	ALL	ACCEPT	Enabled	All		0B

```
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

FortiGate VM64-KVM FortiGate-VM64-KVM

Dashboard > System Settings

Security Fabric >

FortiView >

Network >

System >

Administrators

Admin Profiles

Firmware

Settings ☆

HA

SNMP

Replacement Messages

FortiGuard

Advanced

Feature Visibility

Tags

Certificates

Policy & Objects >

Security Profiles >

VPN >

User & Device >

Log & Report >

Monitor >

Host name Branch-2

System Time

Current system time 2020/05/04 11:15:53

Time Zone (GMT+1:00) Brussels, Copenhagen, N

Set Time Synchronize with NTP Server Manual settings

Select server FortiGuard Custom

Sync interval 1

Setup device as local NTP server

Administration Settings

HTTP port 80

HTTPS port 443

Port conflicts with the SSL-VPN port setting

HTTPS server certificate self-sign

SSH port 22

Telnet port 23

Idle timeout 5 Minutes (1 - 480)

Allow concurrent sessions

Password Policy

Apply

Network -> Interfaces ->

Port 1 : port de gestion.

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

Port 2 : Internet

IP 192.168.59.1/255.255.255.0

Alias : Internet

Type -> Role : WAN

FortiGate VM64-KVM Branch-2

Network > **Interfaces** > **Edit Interface**

Interface Name: port2 (0C:3C:CA:CF:3B:01)
Alias: Internet
Link Status: Up
Type: Physical Interface
Estimated Bandwidth: 0 kbps Upstream: 0 kbps

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

Miscellaneous
Scan Outgoing Connections to Botnet Sites: **Disable** Block Monitor

OK

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.

DNS Server – Specify **1.1.1.1**

FortiGate VM64-KVM Branch-2

Dashboard > **Edit Interface**

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 >

Interface Name port3 (0C:3C:CA:CF:3B: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

Address Range

+ Create New Edit Delete

Starting IP	End IP
192.168.61.2	192.168.61.254

Netmask 255.255.255.0

Default Gateway Same as Interface IP Specify

DNS Server Same as System DNS Same as Interface IP Specify 1.1.1.1

+ Advanced...

Networked Devices

Device Detection ☒

Active Scanning ☐

Admission Control

Security Mode None

☐ Secondary IP Address

Status

Comments

OK

FortiGate VM64-KVM Branch-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									

Policy & Objects -> Ipv4 Policy -> Create New

FortiGate VM64-KVM Branch-2

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

Edit 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

☐

SSL Inspection

☐

OK

FortiGate VM64-KVM Branch-2									
Dashboard									
Security Fabric									
FortiView									
Network									
System									
Policy & Objects									
IPv4 Policy									
IPv4 DoS Policy									
Addresses									

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Internet	all	all	always	ALL	ACCEPT	Enabled	UTM		0 B
0	Implicit Deny	all	all	always	ALL	DENY		Disabled		1.07 kB

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

FortiGate VM64-KVM Branch-2

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

NAT Configuration: No NAT between sites
This site is behind NAT
The remote site is behind NAT

Site to Site - FortiGate

This FortiGate Remote FortiGate

< Back Next > Cancel

1 VPN Setup 2 Authentication 3 Policy & Routing

Name: Branch-to-HQ

Template Type: Site to Site Remote Access Custom

Remote Device Type: FortiGate

NAT Configuration: No NAT between sites
This site is behind NAT
The remote site is behind NAT

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

FortiGate VM64-KVM Branch-2

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing

Remote Device: IP Address Dynamic DNS

IP Address: 192.168.122.234

Outgoing Interface: Internet (port2)

Authentication Method: Pre-shared Key Signature

Pre-shared Key:

Branch-to-HQ: Site to Site - FortiGate

This FortiGate Remote FortiGate

< Back Next > Cancel

1 VPN Setup 2 Authentication 3 Policy & Routing

Remote Device: IP Address Dynamic DNS

IP Address: 192.168.122.234

Outgoing Interface: Internet (port2)

Authentication Method: Pre-shared Key Signature

Pre-shared Key:

Local Interface : Port 3

Local Subnets: 60.0

Remote Subnets : 61.0

FortiGate VM64-KVM Branch-2

VPN Creation Wizard

VPN Setup Authentication 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

This FortiGate Remote FortiGate

< Back Create Cancel

VPN Creation Wizard

VPN Setup Authentication 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

FortiGate VM64-KVM Branch-2

VPN Creation Wizard

VPN Setup Authentication Policy & Routing

The VPN has been set up

Summary of Created Objects

Phase 1 Interface	Branch-to-HQ
Local Address Group	Branch-to-HQ_local
Remote Address Group	Branch-to-HQ_remote
Phase 2 Interface	Branch-to-HQ
Static Route	1
Blackhole Route	2
Local to Remote Policy	2
Remote to Local Policy	3

Add Another Show Tunnel List

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

FortiGate VM64-KVM Branch-2			
Dashboard	+ Create New	Edit	Delete
Security Fabric	Search		
FortiView	Q		
Network			
System			
Policy & Objects			
Security Profiles			
VPN			
IPsec Tunnels			

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

Double-cliquer sur Branch-to-HQ :

FortiGate VM64-KVM Branch-2

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
SSL-VPN Settings
User & Device
Log & Report
Monitor

Edit VPN Tunnel

Tunnel Template

Site to Site - FortiGate

Convert To Custom Tunnel

Name

Branch-to-HQ

Comments

VPN: Branch-to-HQ (Created by VPN wizard)

41/255

Network

Remote Gateway : Static IP Address (192.168.122.234) , Outgoing Interface : port2

Edit

Authentication

Authentication Method : Pre-shared Key

Edit

Phase 2 Selectors

	Local Address	Remote Address
Branch-to-HQ	Branch-to-HQ_local	Branch-to-HQ_remote

OK

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

➤ **Policy & Objects -> IPv4 Policy** (2 politiques créées);

FortiGate VM64-KVM

Branch-2

</

ID	Name	Source	Destination
Branch-to-HQ → Lan (port3) 1			
3	vpn_Branch-to...	Branch-to-HQ_remote	Branch-to-HQ_local
Lan (port3) → Branch-to-HQ 1			
2	vpn_Branch-to...	Branch-to-HQ_local	Branch-to-HQ_remote

➤ Policy&Objects -> Addresses (2 subnets configurés)

FortiGate VM64-KVM Branch-2						
Dashboard	>	+ Create New ▾ Edit Clone Delete Search				
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	>					

Name	Type	Details	Interface	Visibility	Ref.
Address 10					
Branch-to-HQ_local_subn...	Subnet	192.168.61.0/24		Visible	1
Branch-to-HQ_remote_su...	Subnet	192.168.60.0/24		Visible	1
FIREWALL_AUTH_PORTA...	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134....	SSL-VPN tunnel interface (ssl...	Visible	1
all	Subnet	0.0.0.0/0		Visible	2
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_...		Visible	3
Branch-to-HQ_remote	Address Group	Branch-to-HQ_remote_subne		Visible	5

+ Create New ▾	Edit	Clone	Delete	Search
----------------	------	-------	--------	--------

Name	Type	Details
Address 10		
Branch-to-HQ_local_subn...	Subnet	192.168.61.0/24
Branch-to-HQ_remote_su...	Subnet	192.168.60.0/24
FIREWALL_AUTH_PORTA...	Subnet	0.0.0.0/0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134....
all	Subnet	0.0.0.0/0
autoupdate.opera.com	FQDN	autoupdate.opera.com
google-play	FQDN	play.google.com
none	Subnet	0.0.0.0/32
swscan.apple.com	FQDN	swscan.apple.com
update.microsoft.com	FQDN	update.microsoft.com
Address Group 2		
Branch-to-HQ_local	Address Group	Branch-to-HQ_local_subnet_...
Branch-to-HQ_remote	Address Group	Branch-to-HQ_remote_subne

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

FortiGate VM64-KVM Branch-2						
Dashboard	>	FortiGate VM64-KVM 1 3 5 7 9 2 4 6 8 10				
Security Fabric	>					
FortiView	>					
Network	>					
Interfaces	☆	+ Create New ▾ Edit Delete				
DNS	>					
Packet Capture	>					
SD-WAN	>					
Performance SLA	>					
SD-WAN Rules	>					
Static Routes	>					

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (11)						
port1			192.168.122.62 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
port2 (Internet)			192.168.122.63 255.255.255.0	Physical Interface		3
Branch-to-HQ			0.0.0.0 0.0.0.0	Tunnel Interface		4
port3 (Lan)			192.168.61.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP RADIUS-ACCT	4

➤ Network --> Static Routes (2 routes)

FortiGate VM64-KVM Branch-2				
Dashboard	>	+ Create New ▾ Edit Clone Delete		
Security Fabric	>			
FortiView	>			
Network	>			

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...

➤ HQ-to-branch

VPN -> IPsec Wizard

- Etape 1

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Name:

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

> Cancel

- Etape 2

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


Branch-2				
	+ Create New	Edit	Delete	
	Status	Name	Members	IP/Netmask
Physical (11)				
		port1		192.168.122.62 255.255.255.0
		port2 (Internet)		192.168.122.63 255.255.255.0
		port3 (Lan)		192.168.61.1 255.255.255.0

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing

Remote Device **IP Address** Dynamic DNS

IP Address 192.168.122.63

Outgoing Interface  Internet (port2) ▼

Detected via routing lookup

Authentication Method **Pre-shared Key** Signature

Pre-shared Key •••••••• •

• Etape 3


Local Interface : Port 3

Local Subnets: 60.0

Remote Subnets : 61.0

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 Policy & Routing

Local Interface  lan (port3) ▼

Local Subnets 192.168.60.0/24


+

Remote Subnets 192.168.61.0/24

+

Internet Access **None** Share WAN Force to use remote WAN

• Etape 4

 FortiGate VM64-KVM HQ-2

Dashboard >
Security Fabric >
FortiView >
Network >
System >
Policy & Objects >
Security Profiles >
VPN >
IPsec Tunnels >
IPsec Wizard ☆
 IPsec Tunnel Templates
 SSL-VPN Portals
 SSL-VPN Settings
 User & Device >

VPN Creation Wizard

1 VPN Setup 2 Authentication 3 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

Add Another Show Tunnel List

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

FortiGate VM64-KVM HQ-2

Dashboard

Security Fabric

FortiView

Network

System

Create New

Edit

Delete

Print Instructions

Search

Tunnel

Interface Binding

Status

Ref.

Site to Site - FortiGate

HQ-to-Branch

Internet (port2)

Inactive

4

Double-cliquer sur Branch-to-HQ :

FortiGate VM64-KVM HQ-2

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
SSL-VPN Settings
User & Device
Log & Report
Monitor

Edit VPN Tunnel

Tunnel Template

Site to Site - FortiGate

Convert To Custom Tunnel

Name

HQ-to-Branch

Comments

VPN: HQ-to-Branch (Created by VPN wizard)

41/255

Network

Edit

Remote Gateway : Static IP Address (192.168.122.63) , Outgoing Interface : port2

Authentication

Edit

Authentication Method : Pre-shared Key

Phase 2 Selectors

Local Address

Remote Address

HQ-to-Branch

HQ-to-Branch_local

HQ-to-Branch_remote

Edit

OK

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

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

FortiGate VM64-KVM HQ-2

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

IPv4 DoS Policy

+ Create New

Edit

Delete

Q Policy Lookup

Search

Interface Pair View

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
HQ-to-Branch → lan (port3)										
5	vpn_HQ-to-Branch	HQ-to-E	HQ-to-Branch_loca	always	ALL	ACCEPT	Disabled	UTM		0 B
lan (port3) → HQ-to-Branch										
4	vpn_HQ-to-Branch	HQ-to-E	HQ-to-Branch_rerr	always	ALL	ACCEPT	Disabled	UTM		0 B

➤ Policy&Objects -> Addresses (2 subnets configurés)

FortiGate VM64-KVM HQ-2						
<div> <div>Dashboard</div> <div>Security Fabric</div> <div>FortiView</div> <div>Network</div> <div>System</div> <div>Policy & Objects</div> <div>IPv4 Policy</div> <div>IPv4 DoS Policy</div> <div>Addresses</div> <div>Wildcard FQDN Addresses</div> <div>Internet Service Database</div> <div>Services</div> <div>Schedules</div> <div>Virtual IPs</div> <div>IP Pools</div> <div>Traffic Shapers</div> <div>Traffic Shaping Policy</div> </div>						
Name	Type	Details	Interface	Visibility	Ref.	
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 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	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						
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_1		Visible	5	

HQ-2		
<div> <div>+</div> <div>Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> <div>Search</div> </div>		
Name	Type	Details
Address 10		
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0
HQ-to-Branch_local_subnet_1	Subnet	192.168.60.0/24
HQ-to-Branch_remote_subnet_1	Subnet	192.168.61.0/24
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210
all	Subnet	0.0.0.0/0
autoupdate.opera.com	FQDN	autoupdate.opera.com
google-play	FQDN	play.google.com
none	Subnet	0.0.0.0/32
swscan.apple.com	FQDN	swscan.apple.com
update.microsoft.com	FQDN	update.microsoft.com
Address Group 2		
HQ-to-Branch_local	Address Group	HQ-to-Branch_local_subnet_1
HQ-to-Branch_remote	Address Group	HQ-to-Branch_remote_subnet_1

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

FortiGate VM64-KVM HQ-2						
<div> <div>Dashboard</div> <div>Security Fabric</div> <div>FortiView</div> <div>Network</div> <div>System</div> </div>						
Interfaces	Status	Name	Members	IP/Netmask	Type	Access
Physical (11)						
port1	🟢	port1		192.168.122.233 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access
port2 (Internet)	🟢	port2 (Internet)		192.168.122.234 255.255.255.0	Physical Interface	
HQ-to-Branch	🟢	HQ-to-Branch		0.0.0.0 255.255.255.255	Tunnel Interface	
port3 (lan)	🟢	port3 (lan)		192.168.60.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP RADIUS-ACCT
port4 (dmz)	🟢	port4 (dmz)		192.168.102.1 255.255.255.0	Physical Interface	
port5	🔴	port5		0.0.0.0 0.0.0.0	Physical Interface	
port6	🔴	port6		0.0.0.0 0.0.0.0	Physical Interface	
port7	🔴	port7		0.0.0.0 0.0.0.0	Physical Interface	
port8	🔴	port8		0.0.0.0 0.0.0.0	Physical Interface	
port9	🔴	port9		0.0.0.0 0.0.0.0	Physical Interface	
port10	🔴	port10		0.0.0.0 0.0.0.0	Physical Interface	

➤ Network --> Static Routes (2 routes)

FortiGate VM64-KVM HQ-2				
<div> <div>+</div> <div>Create New</div> <div>Edit</div> <div>Clone</div> <div>Delete</div> </div>				
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...	

➤ VPN -> Ipsec Tunnels

FortiGate VM64-KVM HQ-2			
Dashboard	+	Create New	Edit
Security Fabric		Delete	Print Instructions
FortiView		Search	Q
Network		Tunnel	Interface Binding
System		Status	Ref.
Site to Site - FortiGate 1			
HQ-to-Branch		Internet (port2)	Inactive
			4

On double-clique :

FortiGate VM64-KVM HQ-2

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
SSL-VPN Settings
User & Device
Log & Report
Monitor

Edit VPN Tunnel

Tunnel Template

Site to Site - FortiGate

Convert To Custom Tunnel

Name

HQ-to-Branch

Comments

VPN: HQ-to-Branch (Created by VPN wizard)

41/255

Network

Edit

Remote Gateway : Static IP Address (192.168.122.63) , Outgoing Interface : port2

Authentication

Edit

Authentication Method : Pre-shared Key

Phase 2 Selectors

	Local Address	Remote Address	
HQ-to-Branch	HQ-to-Branch_local	HQ-to-Branch_remote	Edit

OK

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

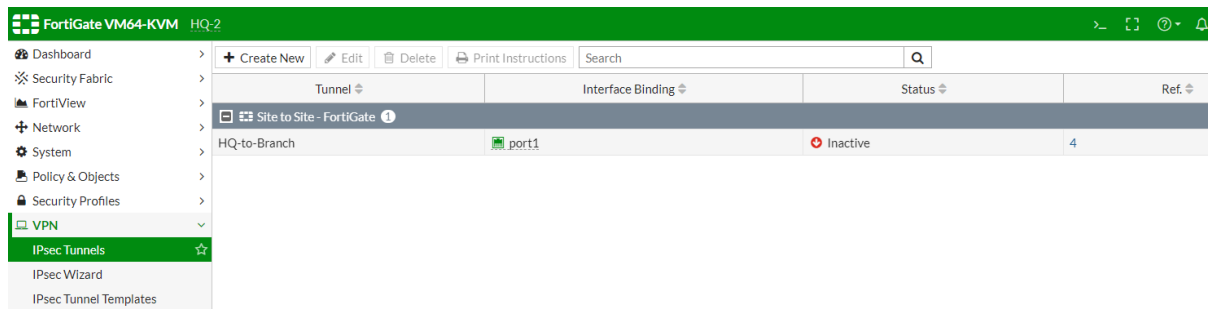
--- 192.168.60.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 1.921/2.148/2.601/0.216 ms
```

```
[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

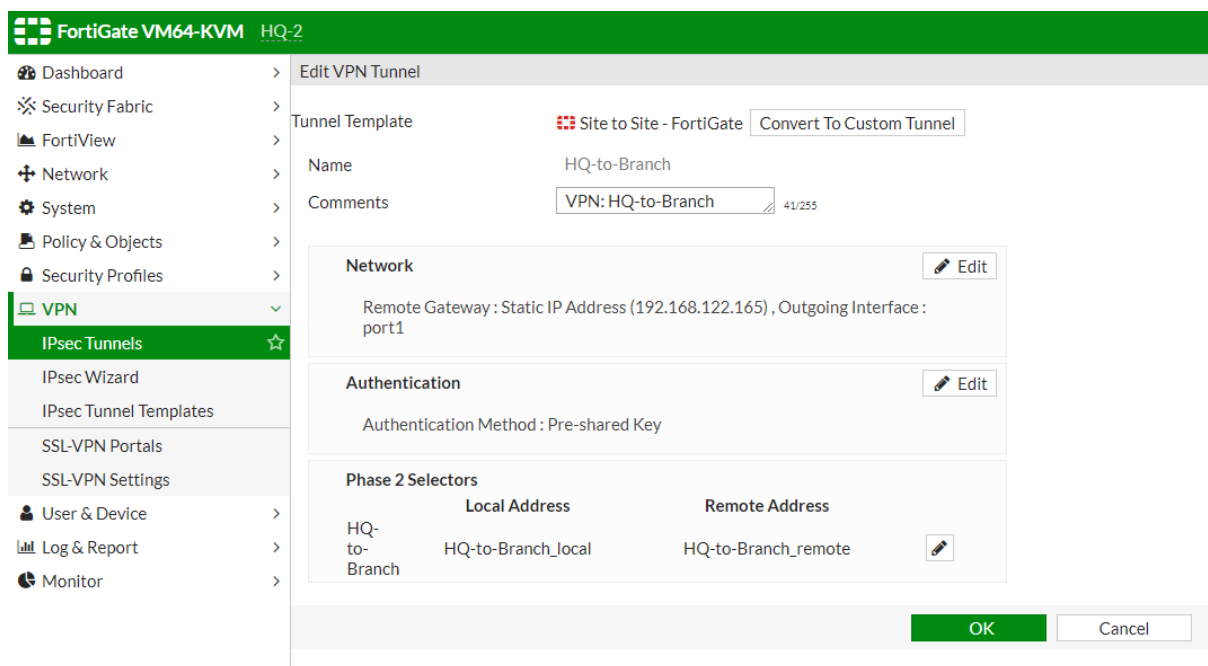
--- 192.168.61.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 2.025/2.309/3.434/0.438 ms
```

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

Dans VPN -> Ipsec tunnel,

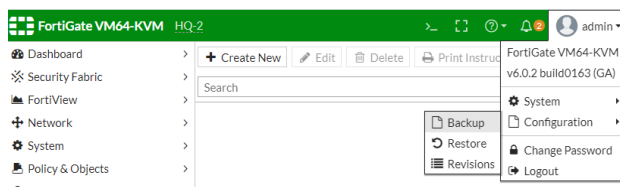


On double-clique :



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

Admin -> Configuration -> Back up



Fichier à télécharger :

Branch-2-

HQ-2