

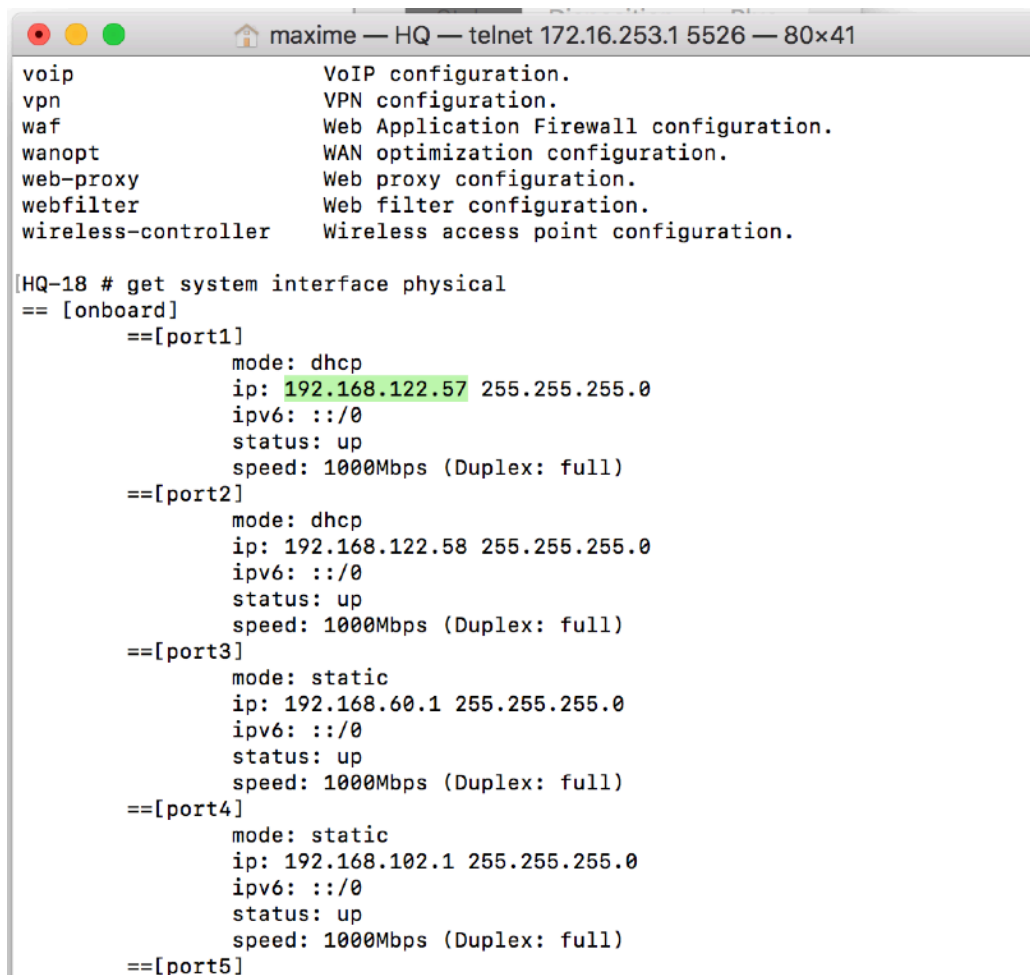
- 1/ Vérifier la configuration de HQ (nom et connectivité)
- 2/ Configurer Branch : Nom, interfaces, service DHCP, NAT, Policy
- 3/ Configurer le VPN IPSEC entre HQ et Branch avec le VPN Wizard
- 4/ Montrer la connectivité entre le LAN HQ (60.0/24) et le LAN Branch (61.0/24) et inversement via des tests 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

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

On exécute la commande

HQ-18 # get system interface physical

Ip de HQ : 192.168.122.57

A screenshot of a telnet window titled "maxime — HQ — telnet 172.16.253.1 5526 — 80x41". The window displays a list of configuration categories: voip (VoIP configuration), vpn (VPN configuration), waf (Web Application Firewall configuration), wanopt (WAN optimization configuration), web-proxy (Web proxy configuration), webfilter (Web filter configuration), and wireless-controller (Wireless access point configuration). Below this, the command "[HQ-18 # get system interface physical]" is entered, followed by the output "=="[onboard]". The output then lists five ports: port1, port2, port3, port4, and port5. Each port has a mode (dhcp or static), an IP address, an IPv6 address (all set to ::/0), a status (up), and a speed (1000Mbps Duplex: full). The IP address for port1, 192.168.122.57, is highlighted in green.

```
voip                VoIP configuration.
vpn                 VPN configuration.
waf                 Web Application Firewall configuration.
wanopt              WAN optimization configuration.
web-proxy           Web proxy configuration.
webfilter           Web filter configuration.
wireless-controller Wireless access point configuration.

[HQ-18 # get system interface physical]
== [onboard]
    ==[port1]
        mode: dhcp
        ip: 192.168.122.57 255.255.255.0
        ipv6: ::/0
        status: up
        speed: 1000Mbps (Duplex: full)
    ==[port2]
        mode: dhcp
        ip: 192.168.122.58 255.255.255.0
        ipv6: ::/0
        status: up
        speed: 1000Mbps (Duplex: full)
    ==[port3]
        mode: static
        ip: 192.168.60.1 255.255.255.0
        ipv6: ::/0
        status: up
        speed: 1000Mbps (Duplex: full)
    ==[port4]
        mode: static
        ip: 192.168.102.1 255.255.255.0
        ipv6: ::/0
        status: up
        speed: 1000Mbps (Duplex: full)
    ==[port5]
```

Connection sur le portail fortigate :

<http://192.168.122.57>

Changement du nom de l'hôte :

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

Vérification des informations sur l'interface fortigate :

← → ↻ Non sécurisé | 192.168.122.57/ng/system/settings

Applications YouTube Facebook SoundCloud Wordreference MULTIMEDIA DEV chambery AJC

FortiGate VM64-KVM HQ-18

- Dashboard >
- 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 >

System Settings

Host name

System Time

Current system time 2020/05/05 09:43:58

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 ⓘ ☐

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

Récupération de l'IP :

FortiGate-VM64-KVM # get system interface physical

```
ing.  
Please run 'execute disk scan 17'  
Note: The device will reboot and scan during startup. This may take up to an hour  
FortiGate-VM64-KVM # get system interface physical  
== [onboard]  
  ==[port1]  
    mode: dhcp  
    ip: 192.168.122.34 255.255.255.0  
    ipv6: ::/0  
    status: up  
    speed: 1000Mbps (Duplex: full)  
  ==[port2]  
    mode: static  
    ip: 0.0.0.0 0.0.0.0  
    ipv6: ::/0  
    status: up  
    speed: 1000Mbps (Duplex: full)  
  ==[port3]  
    mode: static  
    ip: 0.0.0.0 0.0.0.0  
    ipv6: ::/0  
    status: up  
    speed: 1000Mbps (Duplex: full)
```

Pour le port 2 :

Alias : WAN

Rôle : WAN

DCHP activé.

← → ↻ Non sécurisé | 192.168.122.34/ng/page/p/system/interface/edit/port2/?redir=%2Fp%2Fsystem%2Finterface%2F

Applications YouTube Facebook SoundCloud Wordreference MULTIMEDIA DEV chambery AJC

FortiGate VM64-KVM FortiGate-VM64-KVM

- 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 >

Edit Interface

Interface Name port2 (0C:09:9D:72:F7:01)

Alias

Link Status Up ↑

Type Physical Interface

Estimated Bandwidth ⓘ kbps Upstream kbps Downstream

Tags

Role ⓘ

[+ Add Tag Category](#)

Address

Addressing mode **DHCP**

Status ☒ Connected

Obtained IP/Netmask 192.168.122.35 255.255.255.0 [Renew](#)

Expiry Date 2020/05/05 10:59:59

Acquired DNS 192.168.122.1

Default Gateway 192.168.122.1

Retrieve default gateway from server ☒

Distance

Override internal DNS ☒

[OK](#) [Cancel](#)

Pour le port 3 :

Alias : LAN

Rôle : LAN

Administrative access : HTTPS PING SSH RADIUS accounting

DCHP Server activé.

Spécify DNS : 1.1.1.1

Device detection activé.

← → ↻ Non sécurisé | 192.168.122.34/ng/page/p/system/interface/edit/port3?redir=%2Fp%2Fsystem%2Finterface%2F

Applications YouTube Facebook SoundCloud Wordreference MULTIMEDIA DEV chambery AJC

FortiGate VM64-KVM FortiGate-VM64-KVM

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

Edit Interface

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...

OK Cancel

Ipv4 policy > create new

← → ↻ Non sécurisé | 192.168.122.34/ng/firewall/policy/policy/standard

Applications YouTube Facebook SoundCloud Wordreference MULTIMEDIA DEV chambery AJC

FortiGate VM64-KVM FortiGate-VM64-KVM

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

+ Create New Edit Delete Policy Lookup Search

Interface Pair View By Sequence

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Internet	all	all	always	ALL	ACCEPT	Enabled	+	UTM	
+ Implicit										

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

VPN > ipsec wizard

Non sécurisé | 192.168.122.34/ng/vpn/ipsec/wizard

Applications YouTube Facebook SoundCloud Wordreference MULTIMEDIA DEV chambery AJC

FortiGate VM64-KVM FortiGate-VM64-KVM

Dashboard > VPN Creation Wizard

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 >

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

This FortiGate Internet Remote FortiGate

< Back Next > Cancel

Adresse IP du port 2 : 192.168.122.35 255.255.255.0

Non sécurisé | 192.168.122.34/ng/vpn/ipsec/wizard

Applications YouTube Facebook SoundCloud Wordreference MULTIMEDIA DEV chambery AJC

FortiGate VM64-KVM FortiGate-VM64-KVM

Dashboard > VPN Creation Wizard

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 >

VPN Setup 2 Authentication 3 Policy & Routing

Remote Device IP Address Dynamic DNS

IP Address 192.168.122.35

Outgoing Interface WAN (port2) Detected via routing lookup

Authentication Method Pre-shared Key Signature

Pre-shared Key

Branch-to-HQ: Site to Site - FortiGate

This FortiGate Internet Remote FortiGate

< Back Next > Cancel

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

Création du VPN ok :

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

impossible d'afficher les tunnels VPN : chargement infini...

Dans Policy & objects > ipv4 :

The screenshot shows the FortiGate VM64-KVM web interface. The left sidebar has 'Policy & Objects' selected, with 'IPv4 Policy' highlighted. The main content area shows a table of IPv4 policies. The table has columns: ID, Name, Source, Destination, Schedule, Service, Action, and NAT. There are three policies listed: 1. 'Branch-to-HQ' (ID 1) with Source 'LAN (port3)' and Destination 'Branch-to-HQ_remote'. 2. 'vpn_Branch-to-HQ_remote' (ID 2) with Source 'Branch-to-HQ_remote' and Destination 'Branch-to-HQ_local'. 3. 'vpn_Branch-to-HQ_local' (ID 3) with Source 'Branch-to-HQ_local' and Destination 'Branch-to-HQ_remote'. All policies have a schedule of 'always' and a service of 'ALL'. The action is 'ACCEPT' and NAT is 'Disable'. There is also an 'Implicit' policy at the bottom.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Branch-to-HQ	LAN (port3)	Branch-to-HQ_remote	always	ALL	ACCEPT	Disable
2	vpn_Branch-to-HQ_remote	Branch-to-HQ_remote	Branch-to-HQ_local	always	ALL	ACCEPT	Disable
3	vpn_Branch-to-HQ_local	Branch-to-HQ_local	Branch-to-HQ_remote	always	ALL	ACCEPT	Disable
1	Internet	all	all	always	ALL	ACCEPT	Enable
	Implicit						

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

The screenshot shows the FortiGate VM64-KVM web interface. The left sidebar has 'System' selected, with 'Interface' highlighted. The main content area shows a table of interfaces. The table has columns: Status, Name, Members, IP/Netmask, Type, Access, and Ref. There are four interfaces listed: 1. 'port1' (Physical Interface) with IP/Netmask '192.168.122.34 255.255.255.0'. 2. 'port2 (WAN)' (Physical Interface) with IP/Netmask '192.168.122.35 255.255.255.0'. 3. 'Branch-to-HQ' (Tunnel Interface) with IP/Netmask '0.0.0.0 0.0.0.0'. 4. 'port3 (LAN)' (Physical Interface) with IP/Netmask '192.168.61.1 255.255.255.0'. All interfaces have a status of 'Up'.

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Up	port1		192.168.122.34 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	0
Up	port2 (WAN)		192.168.122.35 255.255.255.0	Physical Interface		3
Up	Branch-to-HQ		0.0.0.0 0.0.0.0	Tunnel Interface		4
Up	port3 (LAN)		192.168.61.1 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP RADIUS-ACCT	4

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.

IP du poste terminal depuis Branch : 192.168.61.2

IP du poste terminal depuis HQ : 192.168.60.6

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

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

```
[client-branch login: root
```

```
[Password:
```

```
Last login: Tue May  5 11:13:36 on ttyS0
```

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

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

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

```
[[root@client-branch ~]# ping 192.168.60.6
```

```
PING 192.168.60.6 (192.168.60.6) 56(84) bytes of data.
```

```
From 192.168.61.1 icmp_seq=1 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=2 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=3 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=4 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=5 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=6 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=7 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=8 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=9 Destination Net Unreachable
```

```
From 192.168.61.1 icmp_seq=10 Destination Net Unreachable
```

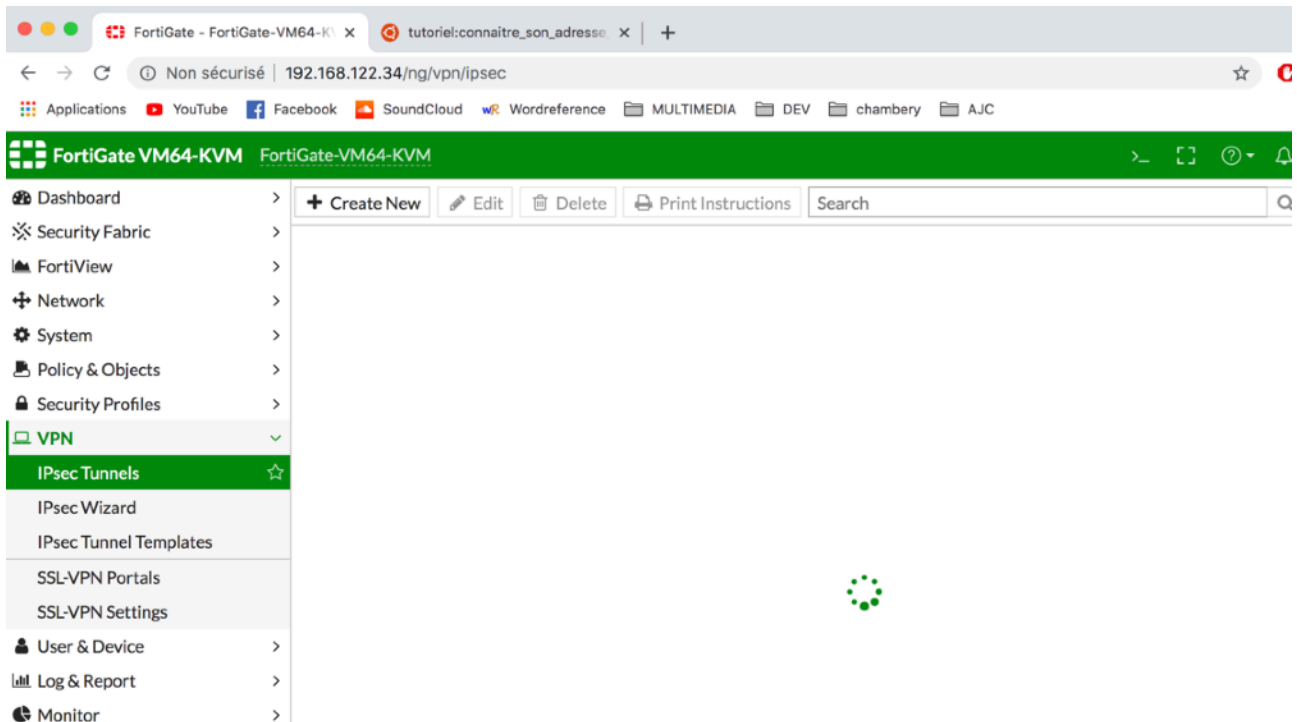
```
From 192.168.61.1 icmp_seq=11 Destination Net Unreachable
```

```
--- 192.168.60.6 ping statistics ---
```

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

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

Affichage impossible des tunnels VPN: chargement infini.



Exportation de la configuration : admin > configuration > backup OK