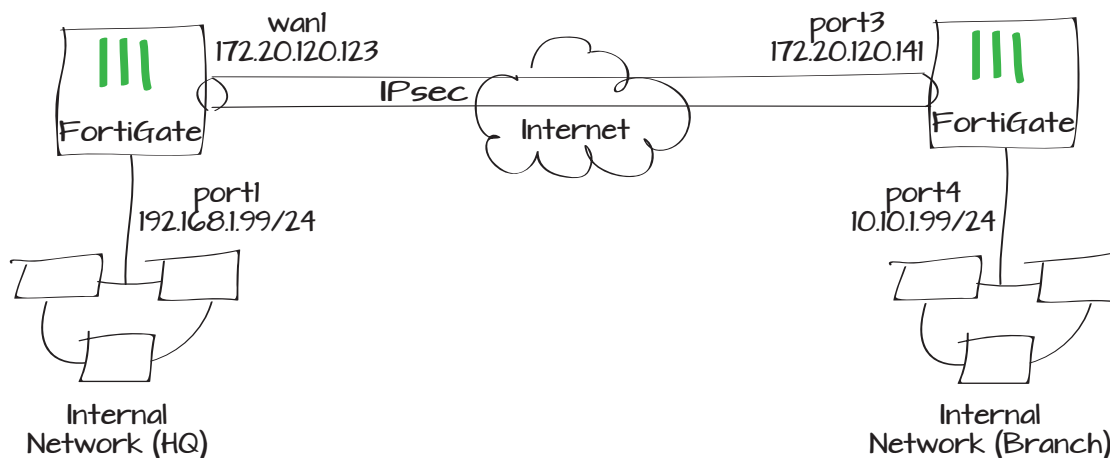


Using policy-based IPsec VPN for communication between offices

This example uses policy-based IPsec VPN, and assumes that both offices have connections to the Internet with static IP addresses. In this example, one FortiGate unit will be called HQ and the other will be called Branch.

1. Enabling policy-based VPN on the HQ FortiGate unit
2. Configuring the HQ IPsec VPN Phase 1 and Phase 2 settings
3. Adding the HQ firewall addresses for the local and remote LAN
4. Creating an HQ IPsec security policy
5. Configuring the Branch IPsec VPN Phase 1 and Phase 2 settings
6. Adding Branch firewall addresses for the local and remote LAN
7. Creating a branch IPsec security policy
8. Results



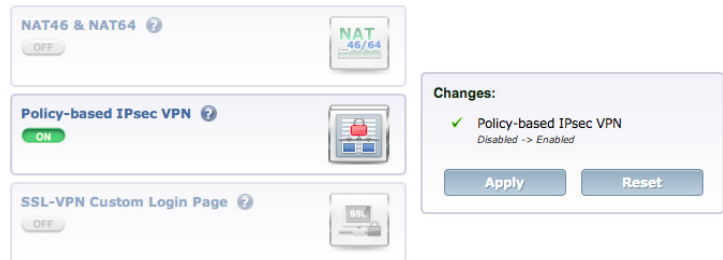
Enabling policy-based VPN on the HQ FortiGate unit

Go to **System > Config > Features**. Select **Show More** and turn on **Policy-based IPsec VPN**.

Configuring the HQ IPsec VPN Phase 1 and Phase 2 settings

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the Branch FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.



Name: HQ_to_Branch_P1

Comments: Write a comment... 0/255

Remote Gateway: Static IP Address

IP Address: 172.20.120.141

Local Interface: wan1

Mode: Aggressive Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key:

Peer Options

Accept any peer ID

IKE Version: 1 2

Mode Config:

Local Gateway IP: Main Interface IP Specify

P1 Proposal

1 - Encryption: 3DES Authentication: SHA1

2 - Encryption: AES128 Authentication: SHA1

DH Group: 1 2 5 14

Now select **Create Phase 2**, set it to use the new Phase 1, and expand the **Advanced** options.

Specify **Source address** as the HQ subnet and **Destination address** as the Branch subnet.

Adding HQ addresses for the local and remote LAN on the HQ FortiGate unit

Go to **Firewall Objects > Address > Address**.

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to an internal port.

Name

Comments 0/255

Phase 1

Advanced...

P2 Proposal

1- Encryption: Authentication:

2- Encryption: Authentication:

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group 1 2 5 14

Keylife: (Seconds) (KBy)

Autokey Keep Alive Enable

Quick Mode Selector

Source address Specify

Select

Source port

Destination address Specify

Select

Destination port

Protocol

Category Address IPv6 Address Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to the Internet-facing interface.

Creating an HQ IPsec security policy

Go to **Policy > Policy > Policy**.

Create a new policy. Set **Type** to **VPN** and **Subtype** to **IPsec**. Configure the policy to allow traffic from the local interface to pass through the outgoing VPN interface (in the example, wan1) using the VPN tunnel created in Phase 1.

When the policy is created, ensure that it is placed at the top of the policy list by clicking on the policy sequence number and dragging the row to the top of the policy table.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	Remote LAN
Color	[Change]
Type	Subnet
Subnet / IP Range	10.10.1.0/255.255.255.0
Interface	wan1
Show in Address List	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

Policy Type	<input type="radio"/> Firewall <input checked="" type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> IPsec <input type="radio"/> SSL-VPN
Local Interface	port1
Local Protected Subnet	Local LAN
Outgoing VPN Interface	wan1
Remote Protected Subnet	Remote LAN
Schedule	always
Service	ALL
Logging Options	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
VPN Tunnel	
<input type="radio"/> Create New <input checked="" type="radio"/> Use Existing	
VPN Tunnel	HQ_to_Branch_P1
<input checked="" type="checkbox"/> Allow traffic to be initiated from the remote	

Configuring the Branch IPsec VPN Phase 1 and Phase 2 settings

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the HQ FortiGate, **Local Interface** to the Internet-facing interface, and enter the same **Pre-shared Key** used in the HQ Phase 1.

Select **Create Phase 2**, set it to use the new Phase 1, and expand the **Advanced** options.

Specify **Source address** as the Branch subnet and **Destination address** as the HQ subnet.

The screenshot shows the configuration for Phase 1 of an IPsec VPN. The Name is 'Branch_to_HQ_P1'. The Remote Gateway is set to 'Static IP Address' with an IP of '172.20.120.123'. The Local Interface is 'lan'. The Mode is 'Main (ID protection)'. The Authentication Method is 'port3 (External Interface)'. The Pre-shared Key field is empty. Under Peer Options, 'Accept any peer ID' is selected. The IKE Version is '1'. The Local Gateway IP is set to 'Main Interface IP'. The P1 Proposal section shows two proposals: Proposal 1 with 3DES encryption and SHA1 authentication, and Proposal 2 with AES128 encryption and SHA1 authentication. The DH Group is set to '5'.


The screenshot shows the configuration for Phase 2 of an IPsec VPN. The Name is 'Branch_to_HQ_P2'. The Phase 1 is set to 'Branch_to_HQ_P1'. The Advanced options are expanded. The P2 Proposal section shows two proposals: Proposal 1 with 3DES encryption and SHA1 authentication, and Proposal 2 with AES128 encryption and SHA1 authentication. Both proposals have 'Enable replay detection' and 'Enable perfect forward secrecy (PFS)' checked. The DH Group is set to '14'. The Keylife is set to 'Seconds' with a value of '1800' and a maximum of '5120' (KBytes). The Autokey Keep Alive option is 'Enable'. The Quick Mode Selector section shows the Source address set to 'Specify' with the value '10.10.1.0/24', the Source port set to '0', the Destination address set to 'Specify' with the value '192.168.1.0/24', the Destination port set to '0', and the Protocol set to '0'.


Adding Branch addresses for the local and remote LAN on the HQ FortiGate unit

Go to **Firewall Objects > Address > Address**.

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to an internal port.

Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to the Internet-facing interface.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="Local LAN"/>
Color	 [Change]
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="10.10.1.0/255.255.255.0"/>
Interface	<input type="text" value="port4 (Internal Interface)"/>
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="Remote LAN"/>
Color	 [Change]
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="192.168.1.0/255.255.255.0"/>
Interface	<input type="text" value="port3 (External Interface)"/>
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Creating a Branch IPsec security policy

Go to **Policy > Policy > Policy**.

Create a new policy. Set **Type** to **VPN** and **Subtype** to **IPsec**. Configure the policy to allow traffic from the local interface to pass through the outgoing VPN interface (in the example, wan1) using the VPN tunnel created in Phase 1.

When the policy is created, ensure that it is placed at the top of the policy list by clicking on the policy sequence number and dragging the row to the top of the policy table.

Results

Go to **VPN > Monitor > IPSec Monitor** to verify the status of the VPN tunnel. It should be up.

A user on either of the office networks should be able to connect to any address on the other office network transparently.

From the HQ FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic**.

From the Branch FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic**.

The screenshot shows the configuration for a VPN policy. The Policy Type is set to VPN, and the Policy Subtype is IPsec. The Local Interface is port4 (Internal Interface), and the Local Protected Subnet is Local LAN. The Outgoing VPN Interface is port3 (External Interface), and the Remote Protected Subnet is Remote LAN. The Schedule is set to 'always' and the Service is 'ALL'. Under Logging Options, 'Log all Sessions' is selected. For the VPN Tunnel, 'Use Existing' is selected, and the tunnel name is 'Branch_to_HQ_P1'. The checkbox 'Allow traffic to be initiated from the remote site' is checked.

Name	Remote Gateway	Proxy ID Source	Proxy ID Destination	Status	Incoming
to_Branch_P1	172.20.120.141	192.168.1.0/24	10.10.1.0/24	Bring Down	23664 E

Src	Dst	Sent / Received	Policy ID	Service	VPN	VPN
192.168.1.117	208.91.112.50	304 B / 304 B	3	ALL_UDP_CUSTOM		
192.168.1.114	10.10.1.100	1.08 KB / 1.24 KB	11	PING	HQ_to_Branch_P1	ipsec-sta
192.168.1.117	208.91.113.70	1.19 KB / 1.19 KB	3	ALL_UDP_CUSTOM		
172.20.120.141	172.20.120.125	1.79 KB / 1.90 KB	5	RDP		
10.10.1.100	192.168.1.114	468 B / 1.29 KB	11	ALL_UDP_CUSTOM	HQ_to_Branch_P1	ipsec-sta
10.10.1.100	192.168.1.114	516 B / 876 B	11	PING	HQ_to_Branch_P1	ipsec-sta
192.168.1.117	208.91.112.53	3.26 KB / 10.00 KB	3	ALL_UDP_CUSTOM		
10.10.1.100	192.168.1.150	441 B / 525 B	11	12101/udp	HQ_to_Branch_P1	ipsec-sta

Date/Time	Src	Dst	Sent / Received	Policy ID	Service	VPN
09:57:05	10.10.1.100	172.20.181.32	0 B / 0 B	1	57622/udp	
09:56:57	10.10.1.100	111.221.77.146	0 B / 0 B	1	40039/udp	
09:56:57	10.10.1.100	157.55.235.154	0 B / 0 B	1	40042/udp	
09:56:55	10.10.1.100	192.168.1.114	552 B / 276 B	4	PING	Branch_to_HQ_P1
09:56:35	10.10.1.100	111.221.74.23	0 B / 0 B	1	40045/udp	