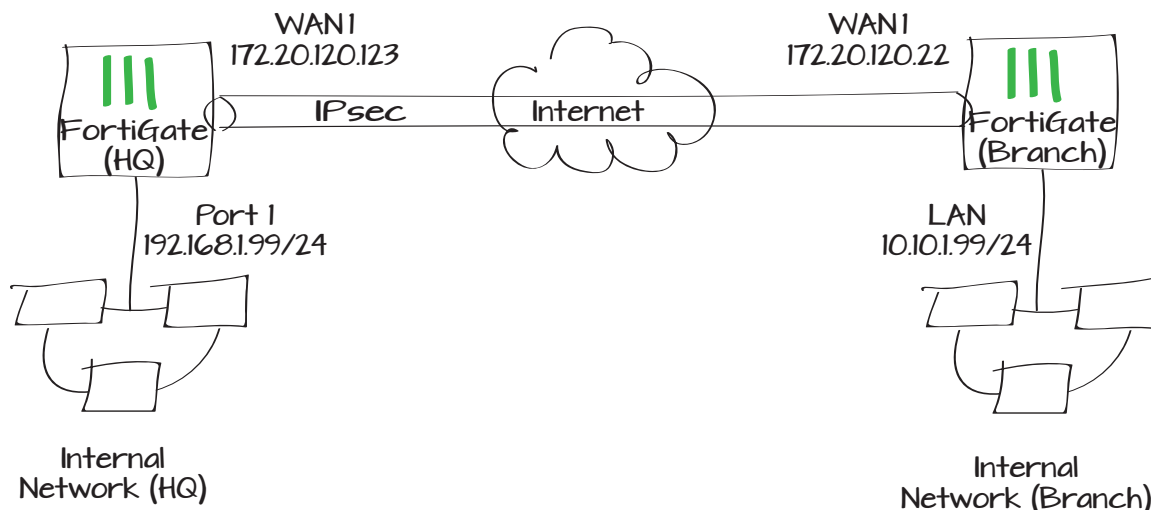


Using IPsec VPN to provide communication between offices

This example provides secure, transparent communication between two FortiGates located at different offices using route-based IPsec VPN. In this example, one office will be referred to as HQ and the other will be referred to as Branch.

1. Configuring the HQ IPsec VPN
2. Adding firewall addresses for the local and remote LAN on HQ
3. Creating an HQ security policy and static route
4. Configure the Branch IPsec VPN Phase 1 and Phase 2 settings
5. Add Branch firewall addresses for the local and remote LAN
6. Create a branch IPsec security policy and static route
7. Results



Configuring the HQ's IPsec VPN

On the HQ FortiGate, 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	<input type="text" value="To_Branch_Net"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Remote Gateway	<input type="text" value="Static IP Address"/>
IP Address	<input type="text" value="172.20.120.22"/>
Local Interface	<input type="text" value="wan1"/>
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	<input type="text" value="Preshared Key"/>
Pre-shared Key	<input type="text" value="....."/>
Peer Options	
	<input checked="" type="radio"/> Accept any peer ID
IKE Version	<input checked="" type="radio"/> 1 <input type="radio"/> 2
Mode Config	<input type="checkbox"/>
Local Gateway IP	<input checked="" type="radio"/> Main Interface IP <input type="radio"/> Specify <input type="text" value="0.0.0.0"/>
P1 Proposal	
1 - Encryption	<input type="text" value="3DES"/> Authentication <input type="text" value="SHA1"/>
2 - Encryption	<input type="text" value="AES128"/> Authentication <input type="text" value="SHA1"/>
DH Group	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 14
Keylife	<input type="text" value="28800"/> (120-172800 seconds)
Local ID	<input type="text"/> (optional)
XAUTH	<input checked="" type="radio"/> Disable <input type="radio"/> Enable as Client <input type="radio"/> Enable as Server
NAT Traversal	<input checked="" type="checkbox"/> Enable
Keepalive Frequency	<input type="text" value="10"/> (10-900 seconds)
Dead Peer Detection	<input checked="" type="checkbox"/> Enable

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.

Name

Comments 0/255

Phase 1

Advanced...

P2 Proposal

1- Encryption: 3DES Authentication: SHA1

2- Encryption: AES128 Authentication: SHA1

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group 1 2 5 14

Keylife: Seconds 1800 (Seconds) 5120 (KBytes)

Autokey Keep Alive Enable

Auto-negotiate Enable

Quick Mode Selector

Source address Specify 192.168.1.0/24 Select -----Address-----

Source port

Destination address Specify 10.10.1.0/24 Select -----Address-----

Destination port

Protocol

Adding firewall addresses for the local and remote LAN on HQ

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

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

Category Address IPv6 Address Multicast Address

Name

Color [Change]

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 VPN Phase 1.

Creating an HQ security policy and static route.

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

Create a policy for outbound traffic. Set **Incoming Interface** to an internal port, **Source Address** to the local address, **Outgoing Interface** to the VPN Phase 1, and **Destination Address** to the remote LAN address.

Create a second policy for inbound traffic. Set **Incoming Interface** to the VPN phase 1, **Source Address** to the local address, **Outgoing Interface** to an internal port, and **Destination Address** to the local address.

Category Address IPv6 Address Multicast Address

Name

Color [Change]

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

Policy Type Firewall SSL-VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Policy Type Firewall SSL-VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Go to **Router > Static > Static Routes**.

Create a route for IPsec traffic, setting **Device** to the VPN Phase 1.



If the **Router** menu is not visible, go to **System > Config > Features** to ensure that **Advanced Routing** is turned on.

Configuring the Branch's IPsec VPN

On the Branch FortiGate, 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 previously.

Destination IP/Mask	<input type="text" value="10.10.1.0/255.255.255.0"/>
Device	<input type="text" value="To_Branch_Net"/>
Distance	<input type="text" value="5"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/> 0/255

Name	<input type="text" value="To_HQ_Net"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Remote Gateway	<input type="text" value="Static IP Address"/>
IP Address	<input type="text" value="172.20.120.123"/>
Local Interface	<input type="text" value="wan1"/>
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	<input type="text" value="Preshared Key"/>
Pre-shared Key	<input type="text" value="....."/>

Peer Options

<input checked="" type="radio"/> Accept any peer ID	
IKE Version	<input checked="" type="radio"/> 1 <input type="radio"/> 2
Mode Config	<input type="checkbox"/>
Local Gateway IP	<input checked="" type="radio"/> Main Interface IP <input type="radio"/> Specify <input type="text" value="0.0.0.0"/>

P1 Proposal

1 - Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA1"/>
2 - Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>
DH Group	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 14		
Keylife	<input type="text" value="28800"/> (120-172800 seconds)		
Local ID	<input type="text"/> (optional)		
XAUTH	<input checked="" type="radio"/> Disable <input type="radio"/> Enable as Client <input type="radio"/> Enable as Server		
NAT Traversal	<input checked="" type="checkbox"/> Enable		
Keepalive Frequency	<input type="text" value="10"/> (10-900 seconds)		
Dead Peer Detection	<input checked="" type="checkbox"/> Enable		

Now 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.

Adding firewall addresses for the local and remote LAN on HQ

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

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch 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) (KBytes)

Autokey Keep Alive Enable

Auto-negotiate 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 HQ subnet, and **Interface** to the VPN Phase 1.

Creating an HQ security policy and static route.

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

Create a policy for outbound traffic. Set **Incoming Interface** to an internal port, **Source Address** to the local address, **Outgoing Interface** to the VPN Phase 1, and **Destination Address** to the remote LAN address.

Create a second policy for inbound traffic. Set **Incoming Interface** to the VPN phase 1, **Source Address** to the local address, **Outgoing Interface** to an internal port, and **Destination Address** to the local address.

Category Address IPv6 Address Multicast Address

Name

Color [Change]

Type

Subnet / IP Range

Interface

Show in Address List

Comments 0/255

Policy Type Firewall SSL-VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Policy Type Firewall SSL-VPN

Policy Subtype Address User Identity Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Go to **Router > Static > Static Routes**.

Create a route for IPsec traffic, setting **Device** to the VPN Phase 1.

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** to verify that both inbound and outbound traffic is occurring.

To verify traffic on the Branch FortiGate unit as well, go to **Log & Report > Traffic Log > Forward Traffic**.

Destination IP/Mask	<input type="text" value="192.168.1.0/255.255.255.0"/>
Device	<input type="text" value="To_HQ_Net"/>
Distance	<input type="text" value="5"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/> 0/255

Status	Incoming Data	Outgoing Data	
Bring Down	2232 B	1725 B	1

#	Date/Time	Src Interface	Dst Interface
1	15:17:47	To_Branch_Net	port1
2	15:17:43	port1	To_Branch_Net
3	15:17:32	To_Branch_Net	port1

#	Date/Time	Src	Dst
1	15:12:30	192.168.1.116	10.10.1.200
2	15:10:12	192.168.1.116	10.10.1.200
3	15:07:47	10.10.1.200	192.168.1.114
4	15:05:45	10.10.1.200	192.168.1.114
5	15:04:28	10.10.1.200	192.168.1.114
6	14:40:08	10.10.1.200	192.168.1.114