Using redundant OSPF routing over IPsec VPN

This example sets up redundant secure communication between two remote networks using an Open Shortest Path First (OSPF) VPN connection. In this example, the HQ FortiGate unit will be called FortiGate 1 and the Branch FortiGate unit will be called FortiGate 2.

1. Creating redundant IPsec tunnels on FortiGate 1
2. Configuring IP addresses and OSPF on FortiGate 1
3. Configuring firewall addresses on FortiGate 1
4. Configuring security policies on FortiGate 1
5. Creating redundant IPsec tunnels for FortiGate 2
6. Configuring IP addresses and OSPF on FortiGate 2
7. Configuring firewall addresses on FortiGate 2
8. Configuring security policies on FortiGate 2
9. Results
Creating redundant IPsec tunnels on FortiGate 1

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

Select **Create Phase 1** and create the primary tunnel. Set **IP Address** to FortiGate 2’s wan1 IP, **Local Interface** to **wan1** (the primary Internet-facing interface) and enter a **Pre-shared Key**.

Select **Create Phase 2**. Set it to use the new Phase 1.
Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1** and create the secondary tunnel. Set **IP Address** to use FortiGate 2’s wan2 IP, **Local Interface** to **wan2** (the secondary Internet-facing interface) and enter the **Pre-shared Key**.

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

Select **Create Phase 2**. Set it to use the new Phase 1
Configuring IP addresses and OSPF on FortiGate 1

Go to **System > Network > Interfaces**.

Select the arrow for **wan1** to expand the list. Edit the primary tunnel interface and create IP addresses.

Select the arrow for **wan2** to expand the list. Edit the secondary tunnel interface and create IP addresses.

Go to **Router > Dynamic > OSPF**.

Enter the **Router ID** for FortiGate 1.

Select **Create New** in the **Area** section.

Add the backbone area of **0.0.0.0**.

Select **Create New** in the **Networks** section.

Create the networks and select Area **0.0.0.0** for each one.
Select **Create New** in the **Interfaces** section.

Create primary and secondary tunnel interfaces. Set a **Cost** of 10 for the primary interface and 100 for the secondary interface.

**Configuring firewall addresses on FortiGate 1**

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

Edit the subnets behind FortiGate 1 and FortiGate 2.
Edit the primary and secondary interfaces of FortiGate 2.

Configuring security policies on FortiGate 1

Go to Policy > Policy > Policy.

Create the four security policies required for both FortiGate 1’s primary and secondary interfaces to connect to FortiGate 2’s primary and secondary interfaces.
Creating redundant IPsec tunnels on FortiGate 2

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

Select Create Phase 1 and create the primary tunnel. Set IP Address to FortiGate 1’s wan1 IP, Local Interface to wan1 (the primary Internet-facing interface) and enter a Pre-shared Key.

Select Create Phase 2. Set it to use the new Phase 1.
Select **Create Phase 1** and create the secondary tunnel. Set **IP Address** to use FortiGate 2’s IP, **Local Interface** to wan2 (the secondary Internet-facing interface) and enter the **Pre-shared Key**.

Select **Create Phase 2**. Set it to use the new Phase 1.
Configuring IP addresses and OSPF on FortiGate 2

Go to **System > Network > Interfaces**.

Select the arrow for **wan1** to expand the list. Edit the primary tunnel interface and create IP addresses.

Select the arrow for **wan2** to expand the list. Edit the secondary tunnel interface and create IP addresses.

Go to **Router > Dynamic > OSPF**.

Enter the **Router ID** for FortiGate 2.

Select **Create New** in the **Area** section.

Add the backbone area of 0.0.0.0.

Select **Create New** in the **Networks** section.

Create the networks and select Area 0.0.0.0 for each one.
Select Create New in the Interfaces section.

Create primary and secondary tunnel interfaces. Set a Cost of 10 for the primary interface and 100 for the secondary interface.

**Configuring firewall addresses on FortiGate 2**

Go to Firewall Objects > Address > Addresses.

Edit the subnets behind FortiGate 1 and FortiGate 2.
Edit the primary and secondary interfaces of FortiGate 1.

**Configuring security policies on FortiGate 2**

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

Create the four security policies required for both FortiGate 2’s primary and secondary interfaces to connect to FortiGate 1’s primary and secondary interfaces.
Results

Go to **VPN > Monitor > IPsec Monitor** to verify the statuses of both the primary and secondary IPsec VPN tunnels on FortiGate 1 and FortiGate 2.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Remote Gateway</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>To_FGT1_Primary</td>
<td>Static IP or Dynamic DNS</td>
<td>172.20.120.24</td>
<td>0</td>
</tr>
<tr>
<td>To_FGT1_Second</td>
<td>Static IP or Dynamic DNS</td>
<td>172.20.120.23</td>
<td>0</td>
</tr>
</tbody>
</table>

Go to **Router > Monitor > Routing Monitor** to verify the routing table on FortiGate 1 and FortiGate 2. Type OSPF for the **Type** and select **Apply Filter** to verify the OSPF route.

<table>
<thead>
<tr>
<th>IP Version</th>
<th>Type</th>
<th>Subtype</th>
<th>Network</th>
<th>Gateway</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>OSPF</td>
<td></td>
<td>10.21.1.0/24</td>
<td>10.1.1.2</td>
<td>To_FGT2_Pr</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Version</th>
<th>Type</th>
<th>Subtype</th>
<th>Network</th>
<th>Gateway</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>OSPF</td>
<td></td>
<td>10.20.1.0/24</td>
<td>10.1.1.1</td>
<td>To_FGT1_Pr</td>
</tr>
</tbody>
</table>

Verify that traffic flows via the primary tunnel.

From a PC1 set to IP:10.20.1.100 behind FortiGate 1, run a tracert to a PC2 set to IP address 10.21.1.00 behind FortiGate 2 and vise versa.

From PC1, you should see that the traffic goes through 10.1.1.2 which is the primary tunnel interface IP set on FortiGate 2.

From PC2, you should see the traffic goes through 10.1.1.1 which is the primary tunnel interface IP set on FortiGate 1.

The VPN network between the two OSPF networks uses the primary VPN connection. Disconnect the wan1 interface and
confirm that the secondary tunnel will be used automatically to maintain a secure connection.

Verify the IPsec VPN tunnel statuses on FortiGate 1 and FortiGate 2. Both FortiGates should show that primary tunnel is DOWN and secondary tunnel is UP.

Go to VPN > Monitor > IPsec Monitor to verify the status.

Verify the routing table on FortiGate 1 and FortiGate 2.

The secondary OSPF route (with cost = 100) appears on both FortiGate units.

Go to Router > Monitor > Routing Monitor. Type OSPF for the Type and select Apply Filter to verify OSPF route.

Verify that traffic flows via the secondary tunnel.

From a PC1 set to IP:10.20.1.100 behind FortiGate 1, run a tracert to a PC2 set to IP:10.21.1.100 behind FortiGate 2 and vice versa. From PC1, you should see that the traffic goes through 10.2.1.2 which is the secondary tunnel interface IP set on FortiGate 2.

From PC2, you should see the traffic goes through 10.2.1.1 which is the secondary tunnel interface IP set on FortiGate 1.