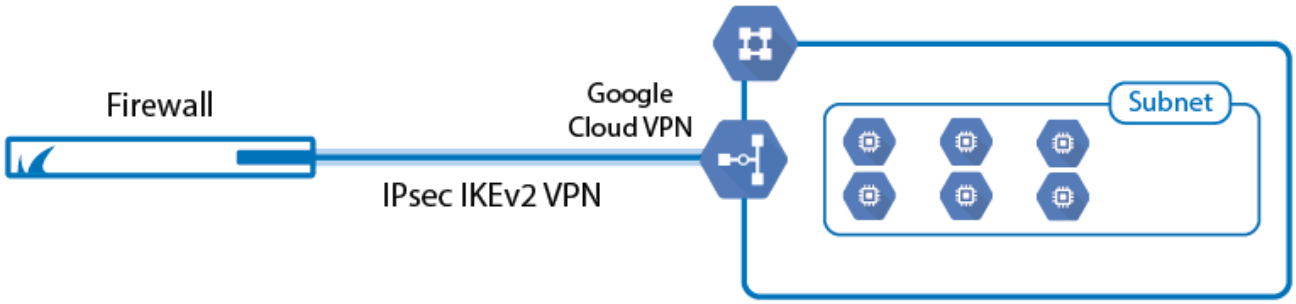
How to Configure BGP over IKEv2 IPsec Site-to-Site VPN to an Google Cloud VPN Gateway

https://campus.barracuda.com/doc/73701650/

To connect to the Google Cloud VPN gateway, create an IPsec IKEv2 site-to-site VPN tunnel on your F-Series Firewall and configure BGP to exchange information with the Google BGP peer.

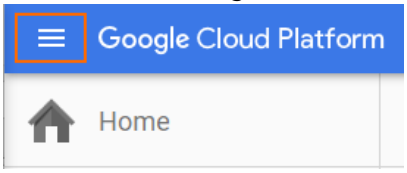


Before You Begin

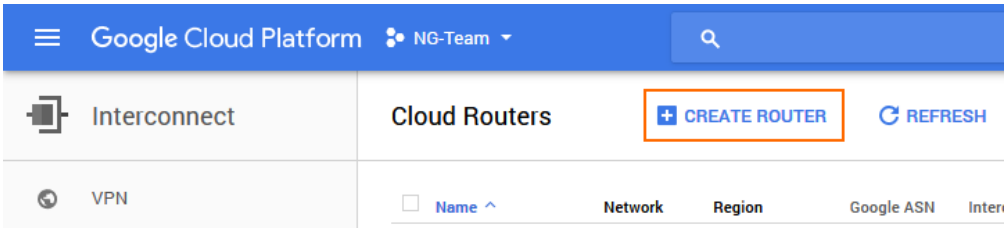
- You will need the following information:
  - Public IP address of your on-premises F-Series Firewall
  - (private) ASN number
- Create a VPC network in Google Cloud.

Step 1. Create a Google Cloud Router

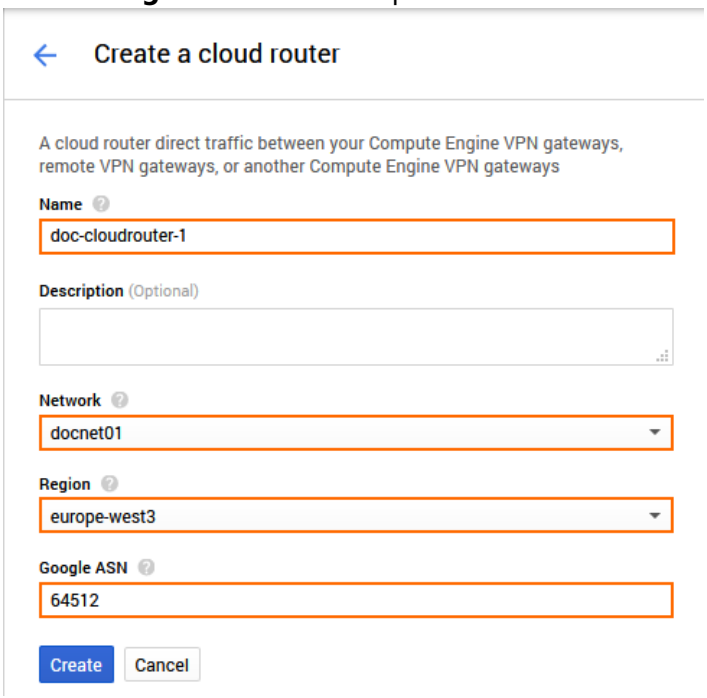
1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper-left corner.



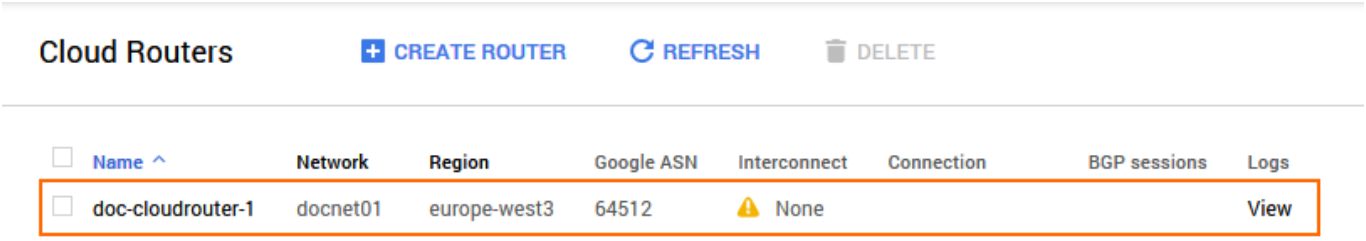
3. In the **Networking** section, click **Interconnect**.
4. In the left menu, click **Cloud Routers**.
5. In the main area, click **Create Router**.



6. Configure the settings for the Google Cloud router:
   - **Name** – Enter a name for the cloud router.
   - **Network** – Select the network from the list.
   - **Region** – Select the region from the list.
   - **Google ASN** – Enter a private ASN. This ASN number must be unique in your network.

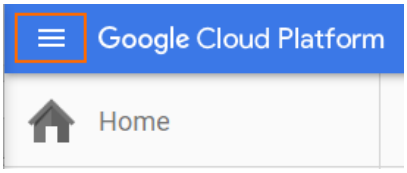


7. Click **Create**.

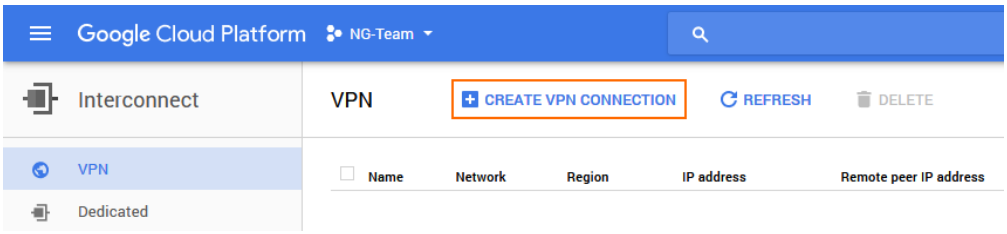


Step 2. Create a Google VPN

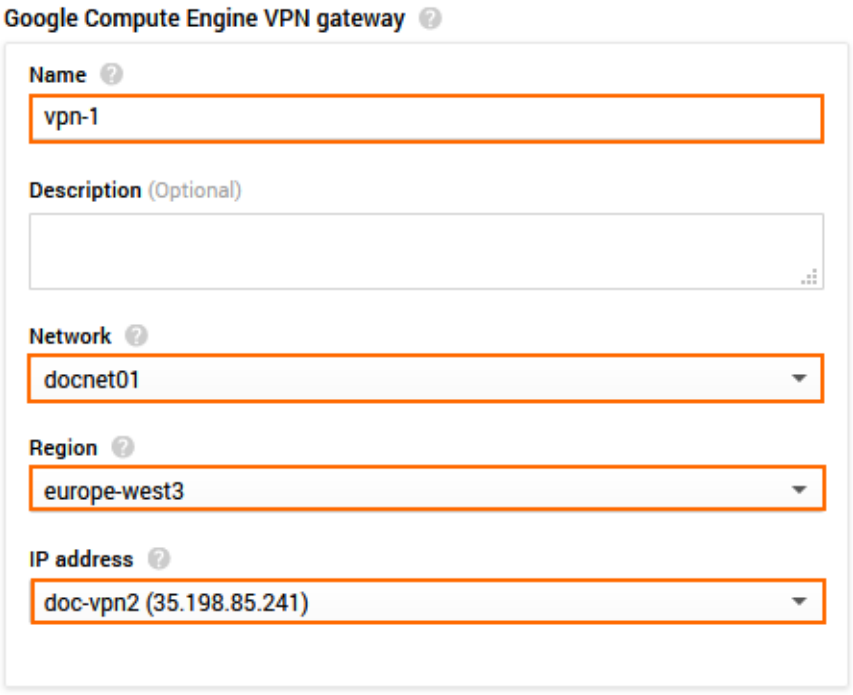
1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper-left corner.



3. In the **Networking** section, click **Interconnect**.
4. In the left menu, click **VPN**.
5. In the main area, click **Create Network**.
6. Click **Create VPN connection**.



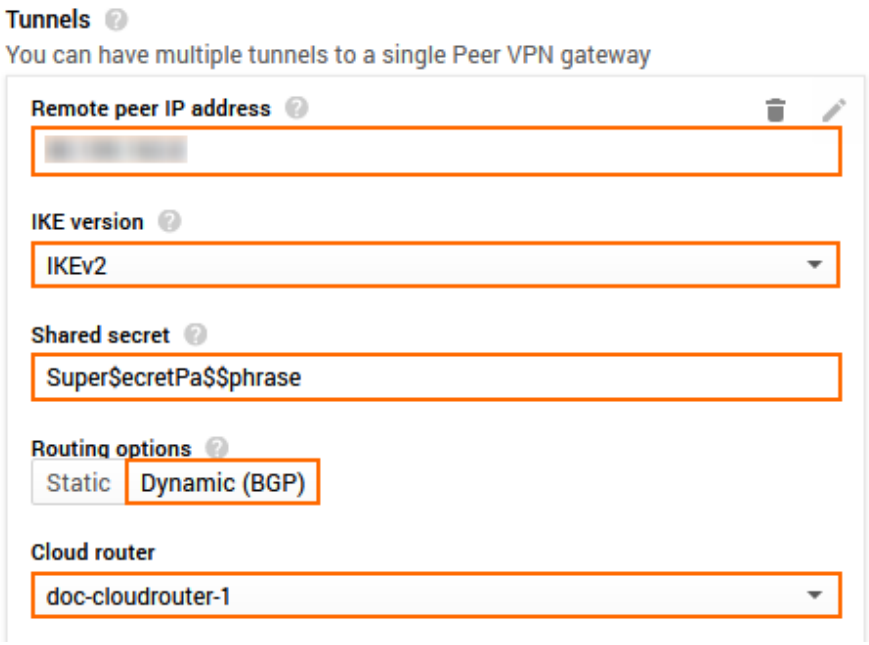
7. Configure the **Google Compute Engine VPN gateway** settings:
   - **Name** – Enter a name.
   - **Network** – Select your Google Cloud network from the list.
   - **Region** – Select the region for the Google VPN gateway. Select a location close to your on-premises firewall.
   - **IP address** – Reserve a new static IP address or select a free, existing static IP address from the list.



8. Configure a VPN tunnel in the **Tunnels** settings:
   - **Remote peer IP address** – Enter the public IP address of the on-premises firewall.
   - **IKE version** – Select **IKEv2**.
   - **Shared secret** – Enter a passphrase as the shared secret.

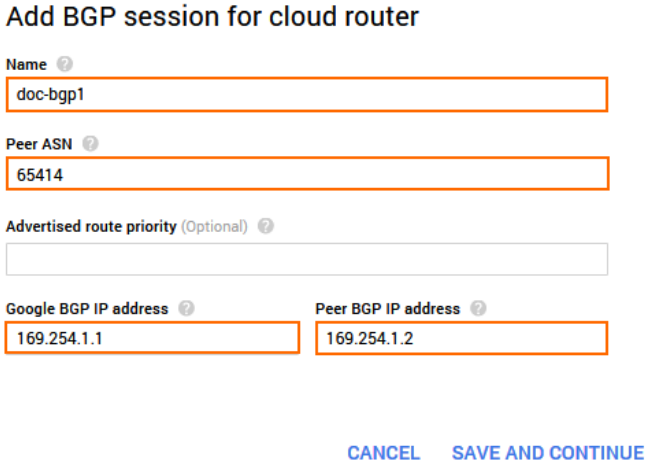
     The shared secret can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).

- **Routing options** – Click **Dynamic (BGP)**.
- **Cloud router** – Select the cloud router created in Step 1.



9. Click the edit icon to configure the **BGP session**.

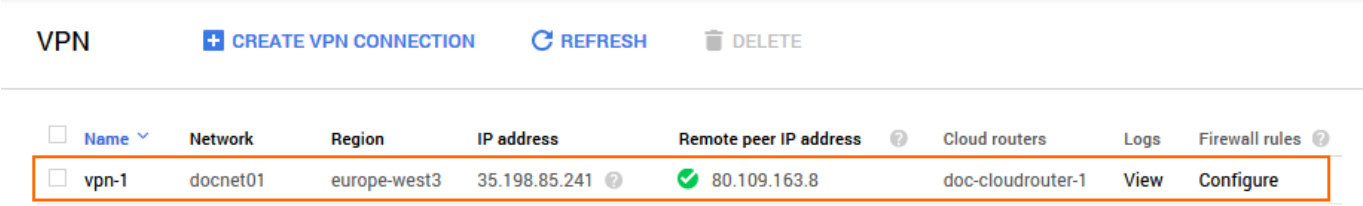
10. Configure the BGP session for the cloud router:
    - **Name** – Enter a name for the BGP configuration.
    - **Peer ASN** – Enter the ASN assigned to the on-premises firewall.
    - **(optional) Advertised route priority** – Enter a priority value. Routes with higher priorities are preferred.
    - **Google BGP IP address** – Enter the first IP address in a private /30 subnet. The IP address must be in the same /30 network as the **Peer BGP IP address**: E.g., `169.254.1.1`
    - **Peer BGP IP address** – Enter the second IP address in the private /30 subnet used for the **Google BGP IP address**. E.g., `169.254.1.2`



11. Click **Save and Continue**.

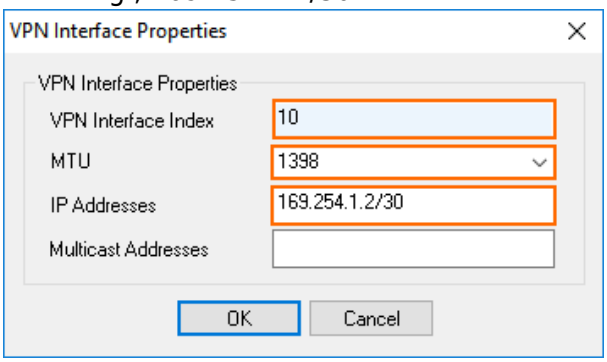
12. Click **Create**.

Wait for the VPN to be created.



Step 3. Create VPN Next Hop Interfaces

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN > VPN Settings** .
2. Click **Lock**.
3. Click **Click here for Server Settings**.
4. Click the **Advanced** tab.
5. Click **Add** in the **VPN Next Hop Interface Configuration** section.
   - **VPN Interface Index** – Enter a number between 0 and 99. Each interface index number must be unique.
   - **MTU** – Enter 1398.
   - **IP Addresses** – Enter the **Peer BGP IP address** from Step 2 with a /30 subnet mask. E.g., 169.254.1.2/30

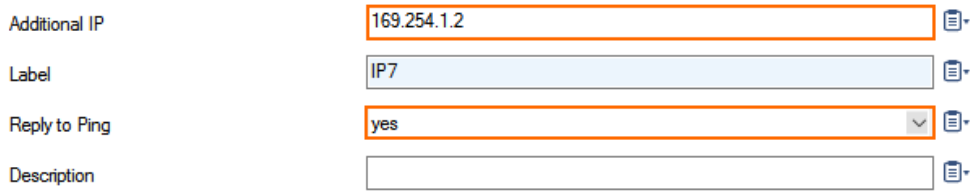


6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 4. Add the VPN Next Hop Interface IP Address to the Virtual Server IPs

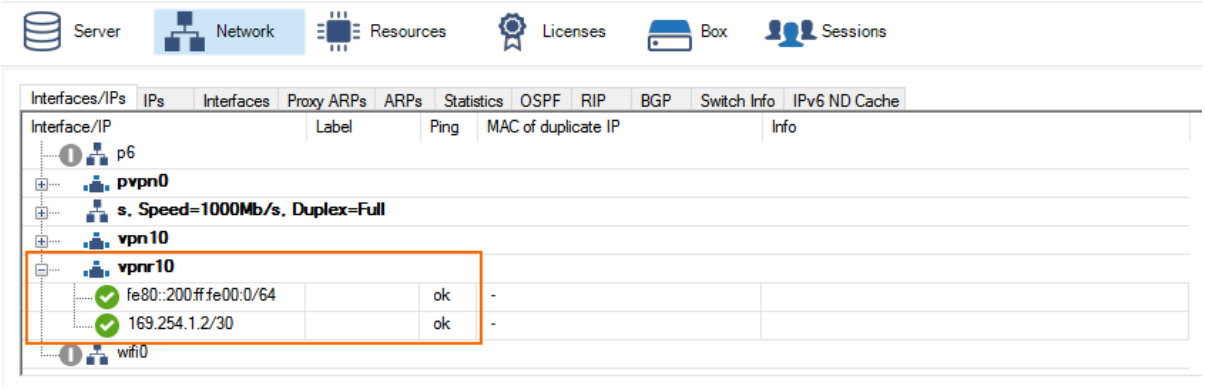
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > Server Properties**.
2. Click **Lock**.
3. Click **+** to add an entry to the **Additional IP** table. The **Additional IP** window opens.

4. Add the local BGP peering IP address as a virtual server IP address:
   - **Additional IP** – Enter the **Peer BGP IP address** from Step 2.
   - **Reply to Ping** – Select **yes**.



5. Click **OK**.
6. Click **Send Changes** and **Activate**.

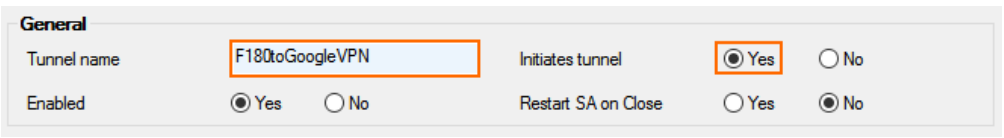
The VPN next hop interface is now listed on the **CONTROL > Network** page.



Step 5. Configure a IPsec IKEv2 Site-to-Site VPN on the Firewall

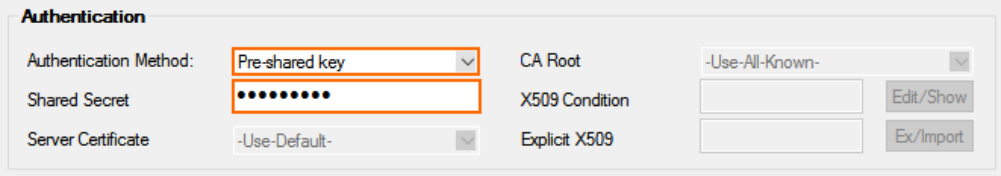
Configure a site-to-site IKEv2 VPN tunnel on the firewall. The firewall is configured as the active VPN endpoint.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site** .
2. Click the **IPsec IKEv2 Tunnels** tab.
3. Click **Lock**.
4. Right-click the table and select **New IKEv2 tunnel**. The **IKEv2 Tunnel** window opens.
5. In the **IKEv2 Tunnel Name** field, enter your tunnel name**.**
6. Set **Initiates Tunnel** to **Yes**.

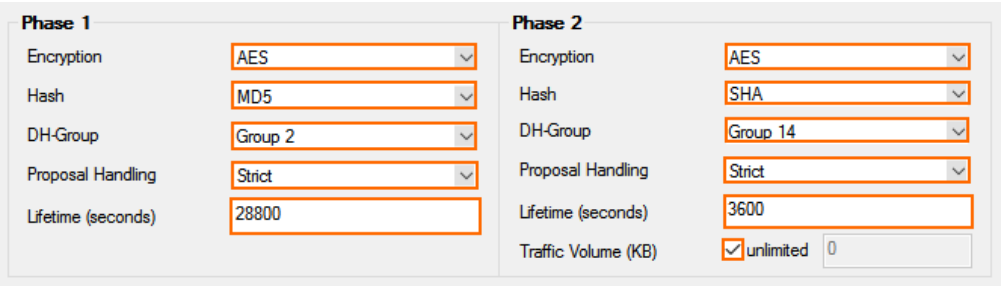


7. Configure the **Authentication** settings:
   - **Authentication Method** – Select **Pre-shared key**.

- **Shared Secret** – Enter the passphrase you used to create the Google VPN.

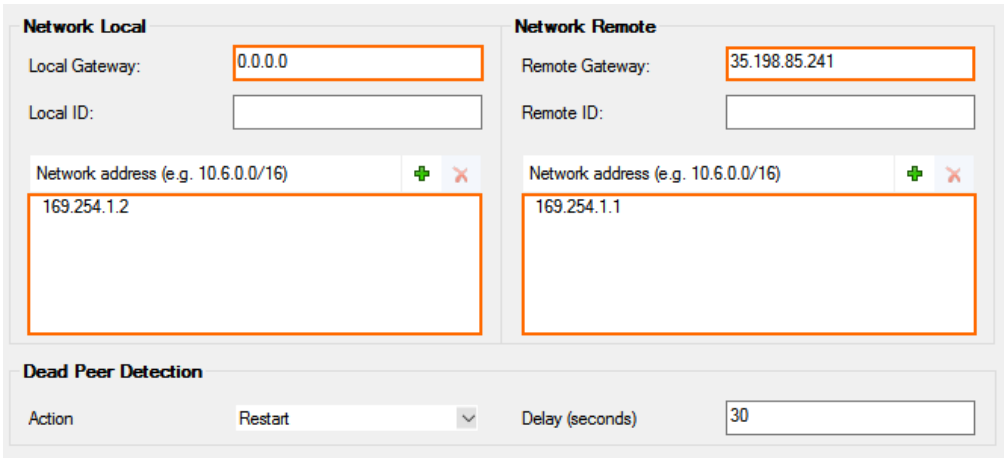


8. Configure the **Phase 1** encryption settings:
   - **Encryption** – Select **AES**.
   - **Hash Meth.** – Select **MD5**.
   - **DH Group** – Select **Group 2**.
   - **Proposal Handling** – Select **Strict**.
   - **Lifetime** – Enter 28800.
9. Configure the **Phase 2** encryption settings:
   - **Encryption** – Select **AES**.
   - **Hash Meth.** – Select **SHA**.
   - **DH Group** – Select **Group 14**.
   - **Proposal Handling** – Select **Strict**.
   - **Lifetime (seconds)** – Enter 3600
   - **LIfetime (KB)** – Select **unlimited**.



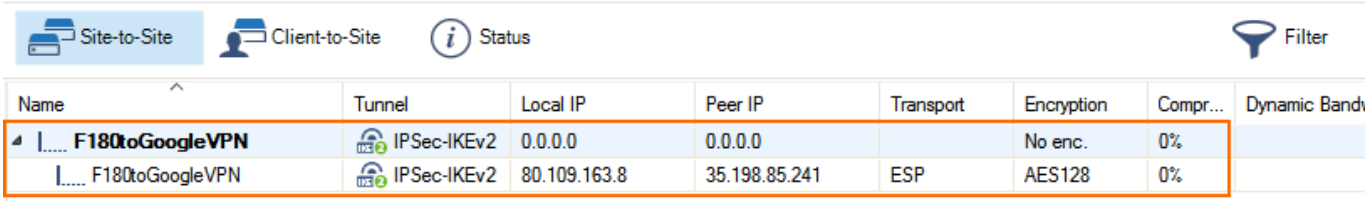
10. In the **Network Settings** section, click the **Advanced** tab:
    - **One VPN Tunnel per Subnet Pair** – Clear the check box.
    - **Universal Traffic Selectors** – Select the check box.
    - **Force UDP Encapsulation** – Clear the check box.
    - **IKE Reauthentication** – Select the check box.
    - **Next Hop Routing** – Enter the **Peer BGP IP address** address from Step 2.
    - **Interface Index** – Enter the index of the VPN next hop interface created in Step 3.

11. Configure the **Local Network** settings:
    - **Local Gateway** – Enter the public IP address of the firewall, or use 0.0.0.0 if you are using a dynamic IP address.
    - **Network Address** – Click **+** and enter the **Peer BGP IP address** from Step 2.
12. Configure the **Remote Network** settings:
    - **Remote Gateway** – Enter the gateway IP address of the Google Cloud VPN.
    - **Network Address** – Click **+** and enter the **Google VPN IP address**.



13. Click **OK**.
14. Click **Send Changes** and **Activate**.

The VPN tunnel to the Google VPN gateway is now established.



Step 6. Configure the BGP Service

Configure BGP routing to learn the subnets from the remote BGP peer behind the Google VPN on the other side of the VPN tunnels.

Step 6.1. Configure Routes to be Advertised via BGP

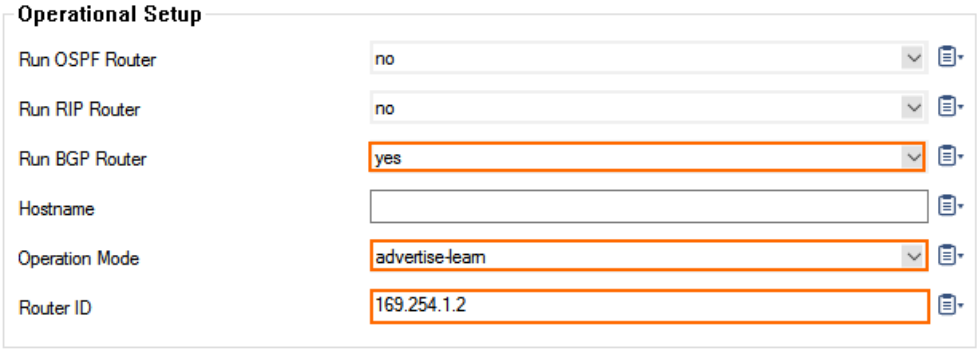
Only routes with the parameter **Advertise** set to **yes** will be propagated via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network** .
2. Click **Lock**.
3. (optional) To propagate the management network, switch to **Advanced** view and set **Advertise Route** to **yes**.
4. In the left menu, click **Routing**.
5. Edit the **Routes** you want to propagate, and set **Advertise Route** to **yes**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

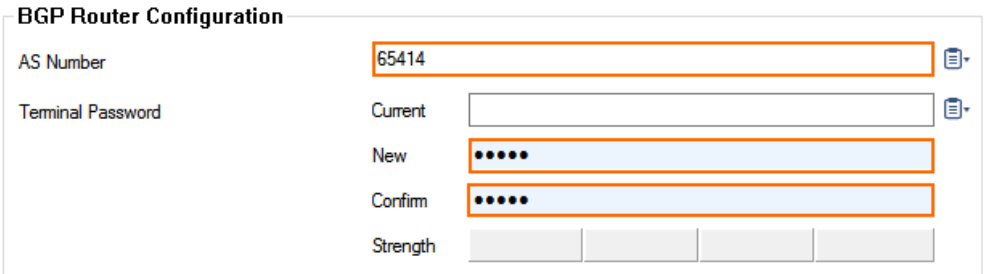
Step 6.2. Enable BGP

Configure the BGP setting for the BGP service on the firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings** .
2. From the **Run BGP Router** list, Select **yes**.
3. From the **Operations Mode** list, select **advertise-learn**.
4. Enter the local BGP peering IP address as the **Router ID**.



5. In the left menu, click **BGP Router Setup**.
6. Enter the **AS Number** for the local BGP peer as per Step 2. E.g., 65414
7. Enter the **Terminal Password**.



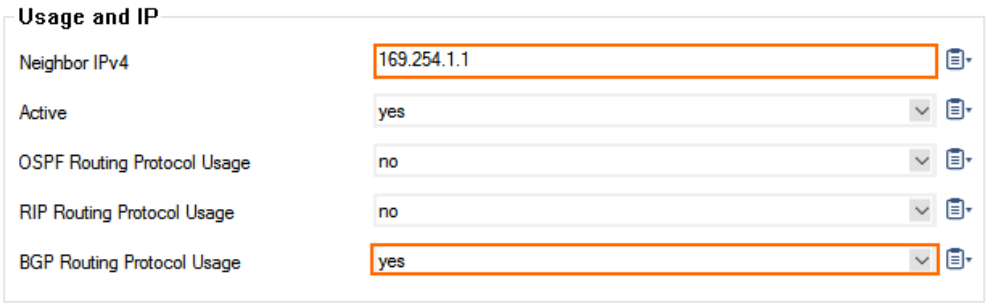
8. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
9. Click the **Set** button for the **Advanced Settings.** The **Advanced Settings** window opens.
10. Set the **Hold timer** to `30` seconds.
11. Set the **Keep Alive Timer** to `10` seconds.
12. Click **OK**.
13. Click **Send Changes** and **Activate**.

Step 6.3. Add a BGP Neighbor for the Google VPN

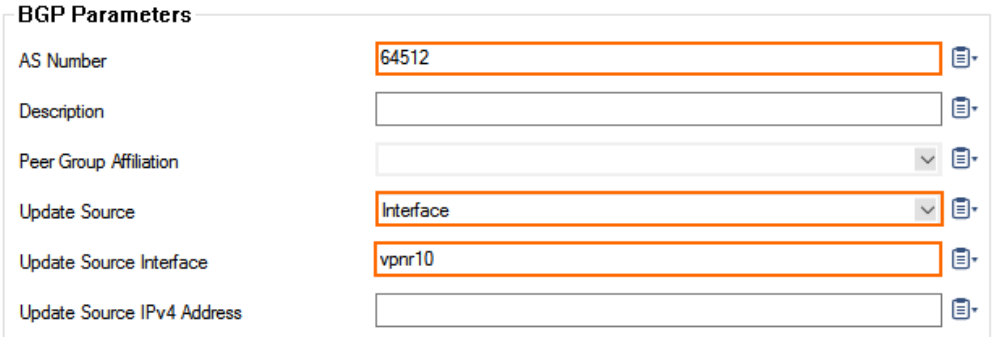
To dynamically learn the routing of the neighboring network, set up a BGP neighbor for the Google VPN.

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
2. Click **Lock**.
3. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
4. Click **+** to add an entry to the **Neighbors** table. The **Neighbors** window opens.
5. Enter a **Name** and click **OK**.

6. In the **Neighbors** window, configure the following settings in the **Usage and IP** section:
   - **Neighbor IPv4** – Enter the remote BGP peer IP address.
   - **OSPF Routing Protocol Usage** – Select **no**.
   - **RIP Routing Protocol Usage** – Select **no**.
   - **BGP Routing Protocol Usage** – Select **yes**.

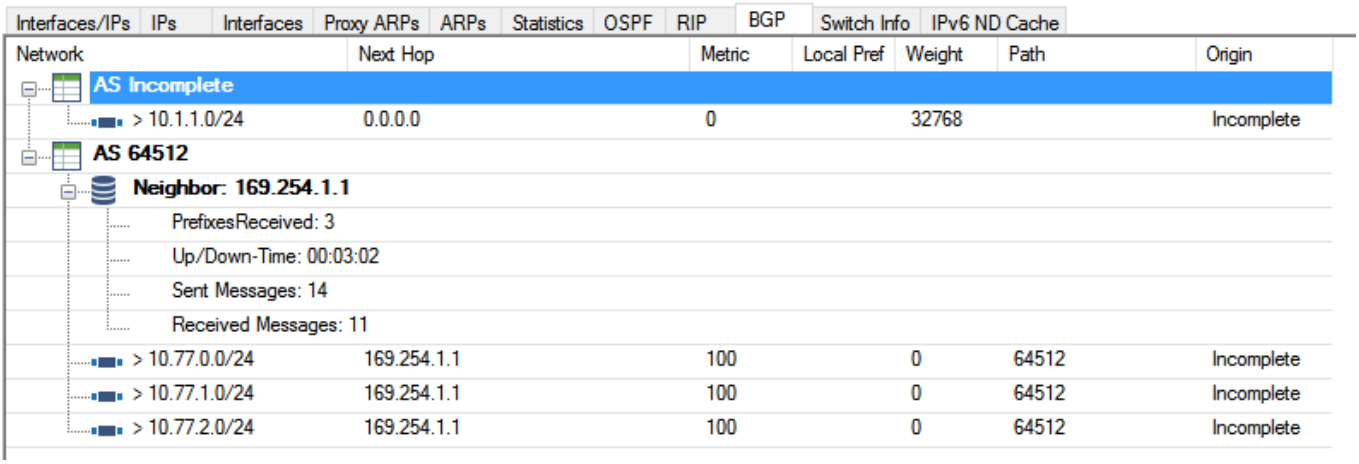


7. In the **BGP Parameters** section, configure the following settings:
   - **AS Number**: Enter the ASN for the remote network as per the information from Step 2. E.g., 65412
   - **Update Source**: Select **Interface**.
   - **Update Source Interface**: Enter the vpnr interface. E.g., `vpnr10`



8. Click **OK**.
9. Click **Send Changes** and **Activate**

Go to **CONTROL > Network > BGP**. The firewall is now learning and advertising networks to the Google VPN BGP peer.



Step 7. Create an Access Rule

Create a pass access rule to allow traffic from the local networks to the networks learned via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Firewall Rules**.
2. Click **Lock**.
3. Create a PASS access rule:
   - **Bi-Directional** – Enable.
   - **Source** – Select the local on-premises network(s) advertised via BGP.
   - **Service** – Select the service you want to have access to the remote network, or select **ALL** for complete access.
   - **Destination** – Select the network object containing the learned networks.
   - **Connection Method** – Select **Original Source IP**.
4. Click **OK**.
5. Move the access rule up in the rule list, so that it is the first rule to match the firewall traffic.
6. Click **Send Changes** and **Activate**.

Figures

1. google_cloud_vpn.png
2. google_VPN_01.png
3. google_VPN_04.png
4. google_VPN_05.png
5. google_VPN_06.png
6. google_VPN_01.png
7. google_VPN_02.png
8. google_VPN_03.png
9. google_VPN_07.png
10. google_VPN_08.png
11. google_VPN_09.png
12. google_VPN_10.png
13. google_VPN_11.png
14. google_VPN_12.png
15. google_VPN_13.png
16. GW_02.png
17. google_VPN_14.png
18. google_VPN_15.png
19. google_VPN_16.png
20. google_VPN_17.png
21. google_VPN_18.png
22. google_VPN_19.png
23. google_VPN_20.png
24. google_VPN_21.png
25. google_VPN_22.png