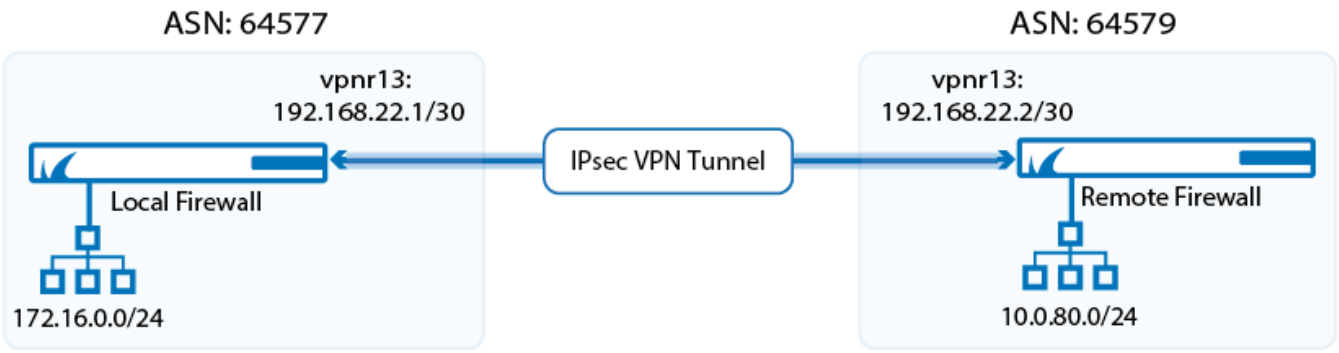
How to Configure BGP Routing over a IKEv1 IPsec VPN Tunnel

https://campus.barracuda.com/doc/53248601/

Follow the instructions in this article to configure the BGP service with an intermediary /30 network between a local and remote VPN gateway. The BGP service uses the IPsec tunnel to dynamically learn the routes of the remote network. You must configure both the local and remote Barracuda NextGen F-Series Firewalls.



	Example Values for the Local Barracuda NextGen Firewall F-Series	Example Values for the Remote Barracuda NextGen Firewall F-Series
VPN Next Hop Interface Index	13	13
VPN Next Hop Interface IP Address	192.168.22.1/24	192.168.22.2/24
Virtual Server Additional IP	192.168.22.1	192.168.22.2
VPN Local Networks	192.168.22.0/30	192.168.22.0/30
VPN Remote Networks	192.168.22.0/30	192.168.22.0/30
VPN Interface Index	13	13
VPN Next Hop Routing	192.168.22.2	192.168.22.1
ASN	64577	64579
Router ID	192.168.22.1	192.168.22.2
Neighbor IPv4	192.168.22.2	192.168.22.1
Neighbor AS Number	64579	64577
Neighbor Update Source Interface	vpnr13	vpnr13

Before You Begin

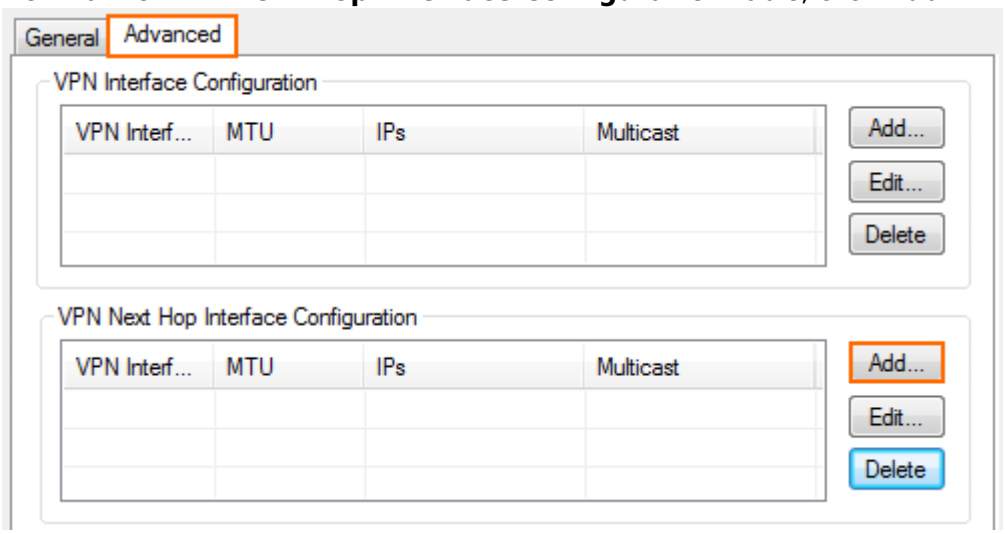
Before you configure BGP over an IPsec VPN, obtain the following:

- A free /30 subnet. E.g., `192.168.22.0/30`
- Autonomous system numbers (ASNs) for the remote and local networks. The ASNs can be private or public because the VPN is not directly connected to the Internet.

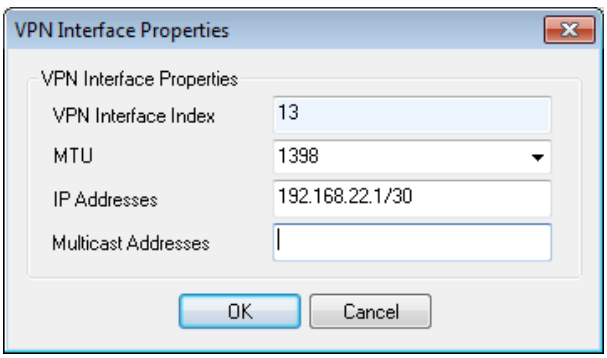
Step 1. Add a VPN Next Hop Interface

Add a VPN next hop interface using a /30 subnet.

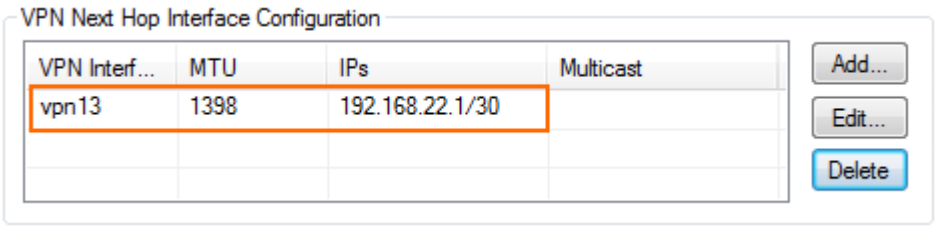
1. Go to **CONFIGURATION** > **Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the **Settings** tab, click the **Click here for Server Settings** link.
4. In the **Server Settings** window, click the **Advanced** tab.
5. Next to the **VPN Next Hop Interface Configuration** table, click **Add**.



6. Configure the VPN next hop interface settings:
   - In the **VPN Interface Index** field, enter a number between `0` and 999. E.g., 13
   - In the **IP Addresses** field, enter the VPN interface IP address. E.g., `192.168.22.1/30` for the local NextGen Firewall F-Series or `192.168.22.2`/30 for the remote NextGen Firewall F-Series.



- Click **OK**. The VPN next hop interface is listed in the **VPN Next Hop Interface Configuration** table.



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

Step 2. Add the VPN Interface IP to the Virtual Server Addresses

Add the IP address of the virtual interface to the list of IP addresses that the virtual server listens on.

1. Go to **CONFIGURATION** > **Configuration Tree > Box > Virtual Servers > *your virtual server* > Server Properties**.
2. Click **Lock**.
3. In the **Additional IP** table, add the intermediary VPN IP address of the local VPN interface. E.g., `192.168.22.1` for the local NextGen Firewall F-Series or `192.168.22.2` for the remote NextGen Firewall F-Series.
4. Click **Send Changes** and **Activate**.

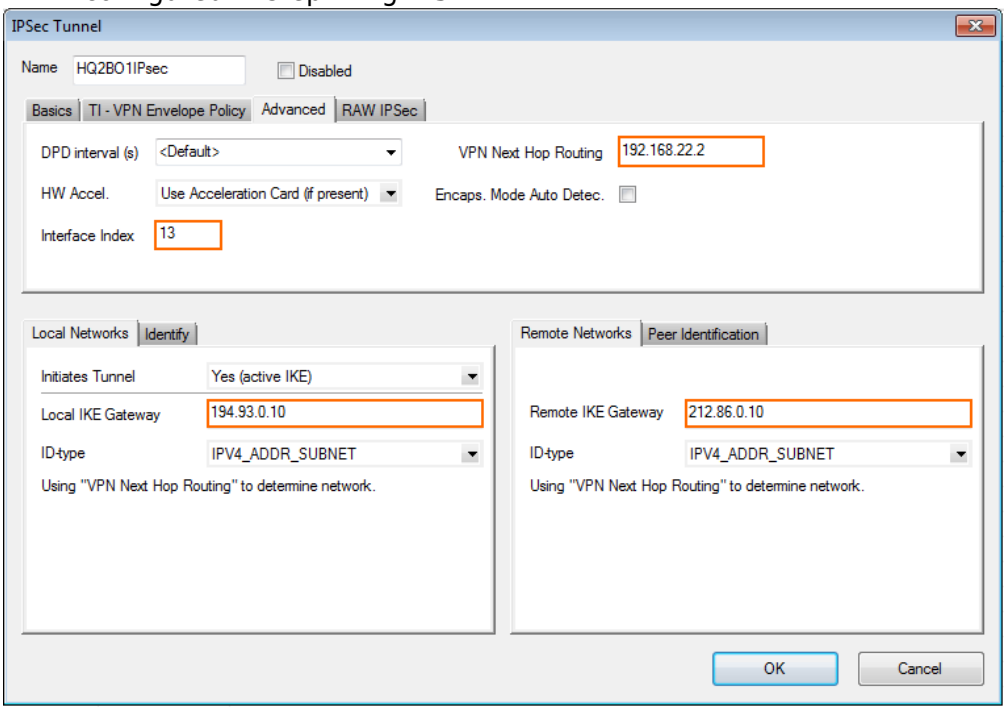
Step 3. Configure the Site-to-Site VPN Settings

Configure a site-to-site VPN IPsec tunnel including the VPN next hop interface.

1. Go to **CONFIGURATION** > **Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click **Lock**.
3. Click the **IPsec IKEv1 Tunnels** tab.
4. Right-click the table under the **IPsec IKEv1 Tunnels** tab and then select **New IPsec IKEv1 tunnel**.
5. In the **IPsec IKEv1 Tunnel** window:
    1. In the **Local Networks** tab, enter:
        - **Local IKE Gateway** – Enter the local public IP address the VPN service is listening on.
        - **Network Address** – Add the intermediary VPN subnet. E.g., `192.168.22.0/30`
    2. In the **Remote Networks** tab, enter:
        - **Remote IKE Gateway** – Enter the remote public IP address the remote VPN service is listening on.

- **Network Address** – Add the intermediary VPN subnet. E.g., `192.168.22.0/30`

3. Click the **Peer Identification** tab and then enter a passphrase the **Shared Secret**.
   The password can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).
4. Click the **Advanced** tab and enter:
   - **VPN Next Hop Routing** – Enter the IP address of the remote VPN next hop interface. E.g., `192.168.22.2` for the local NextGen Firewall F-Series or `192.168.22.1` for the remote NextGen Firewall F-Series
   - **Interface Index** – Enter the interface number of the VPN next hop interface configured in step1. E.g. 13



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

Step 4. Configure the BGP Service

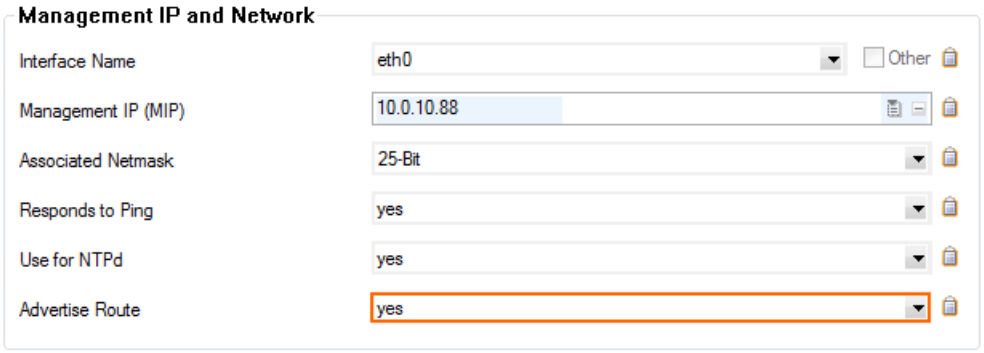
Enable and configure the BGP service. Configure the remote VPN interface IP address as a BGP neighbor to dynamically learn the routes of the neighboring network.

Step 4.1 Configure which Routes to Propagate into BGP

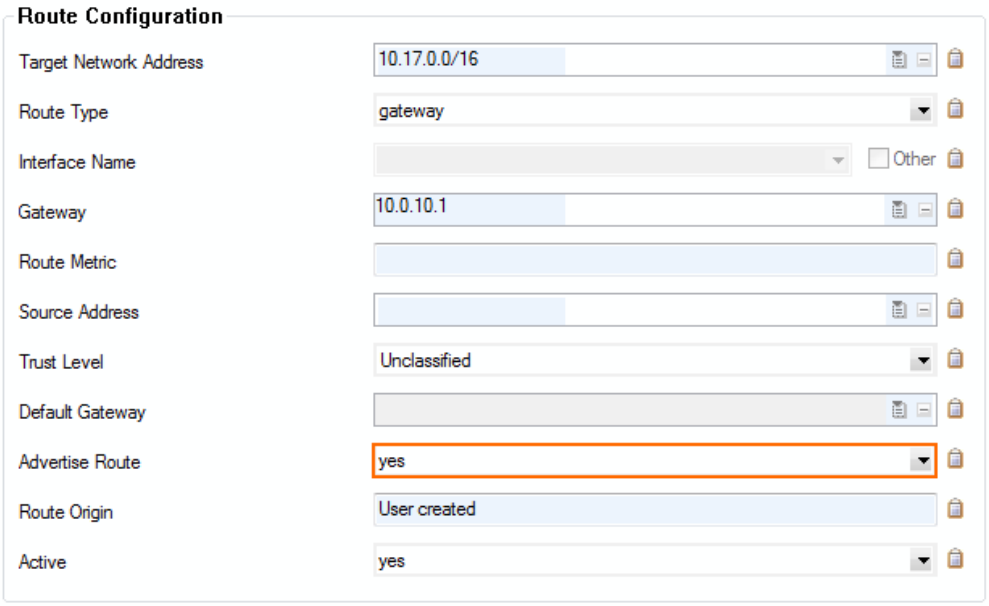
You can either enter the networks you want to propagate manually, or set the **Advertise Route** parameter to **yes** for routes you want propagated.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.

3. To propagate the management network, set **Advertise Route** to **yes** in the **Management IP and Network** section.



4. In the left menu, click on **Routing**.
5. Double-click on the directly attached routes and gateway routes you want to propagate. The **Routes** window opens.
6. Set **Advertise Route** to **yes** and click **OK**.



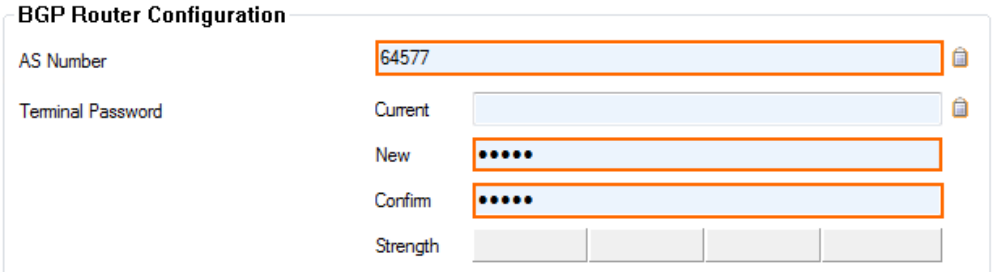
7. Click **Send Changes** and **Activate**.

Step 4.2 Configure the BGP Router

1. Go to **CONFIGURATION** > **Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
2. Set **Run BGP Router** to **Yes**.
3. (optional)To learn routes from the remote ASN, set **Operation Mode** to **advertise-learn**.
4. Enter the **Router ID**. Typically the local VPN next hop interface IP address is used. E.g., `192.168.22.2` for the local NextGen Firewall F-Series `192.168.22.1` for the remote NextGen Firewall F-Series.

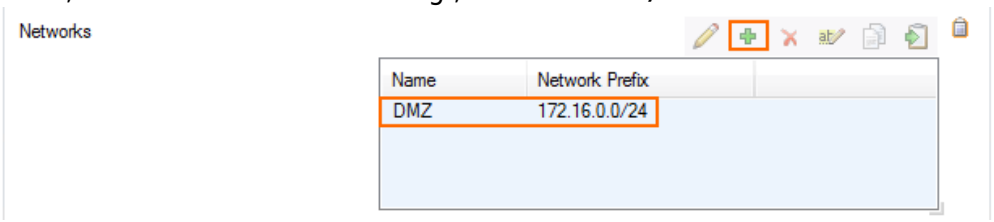
5. In the left menu, click **BGP Router Setup**.
6. Enter the **AS Number**. E.g., 64577 for the local NextGen Firewall F-Series or 64579 for the remote NextGen Firewall F-Series
7. Enter the **Terminal Password**. Use this password if you must directly connect to the dynamic routing daemon via command line for debugging purposes.

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



8. To propagate the directly attached and gateway routes configured in Step 1, set **Connected Routes** to **yes**.

9. (alternative) To manually enter the networks you want to propagate, click **+** in the **Networks** table, and enter the network. E.g., `172.16.0.0/24`



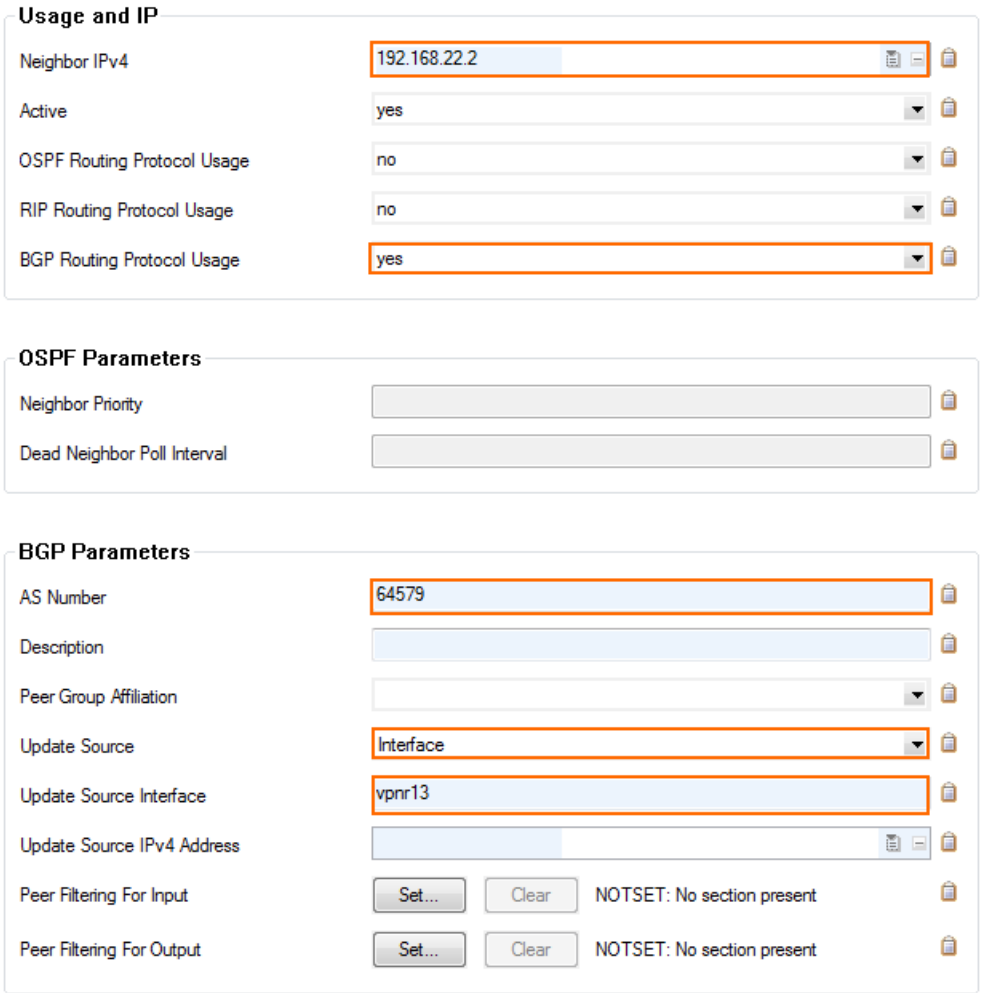
10. Click **Send Changes** and **Activate**.

Step 4.3. Add a BGP Neighbor

To dynamically learn the routing of the neighboring network, set up a BGP neighbor for the remote

VPN next hop interface.

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
2. Click **Lock**.
3. Next to the **Neighbors** table, click the plus sign (**+**) to add a new neighbor.
4. Enter a **Name** for the neighbor and click **OK**. The **Neighbors** window opens.
5. Configure the following settings in the **Usage and IP** section:
   - **Neighbor IPv4** – Enter the remote address for the VPN next hop interface. E.g., `192.168.22.2` for the local NextGen Firewall F-Series `192.168.22.1` for the remote NextGen Firewall F-Series.
   - **OSPF Routing Protocol Usage** – Select **no**.
   - **RIP Routing Protocol Usage** – Select **no**.
   - **BGP Routing Protocol Usage** – Select **yes**.
6. In the **BGP Parameters** section, configure the following settings:
   - **AS Number** – Enter the ASN for the remote network. E.g., 64579 for the local NextGen Firewall F-Series 64577 for the remote NextGen Firewall F-Series.
   - **Update Source** – Select **Interface**.
   - **Update Source Interface** – Enter the VPN next hop interface in the format: `vpnr<interface number>`. E.g., `vpnr13`

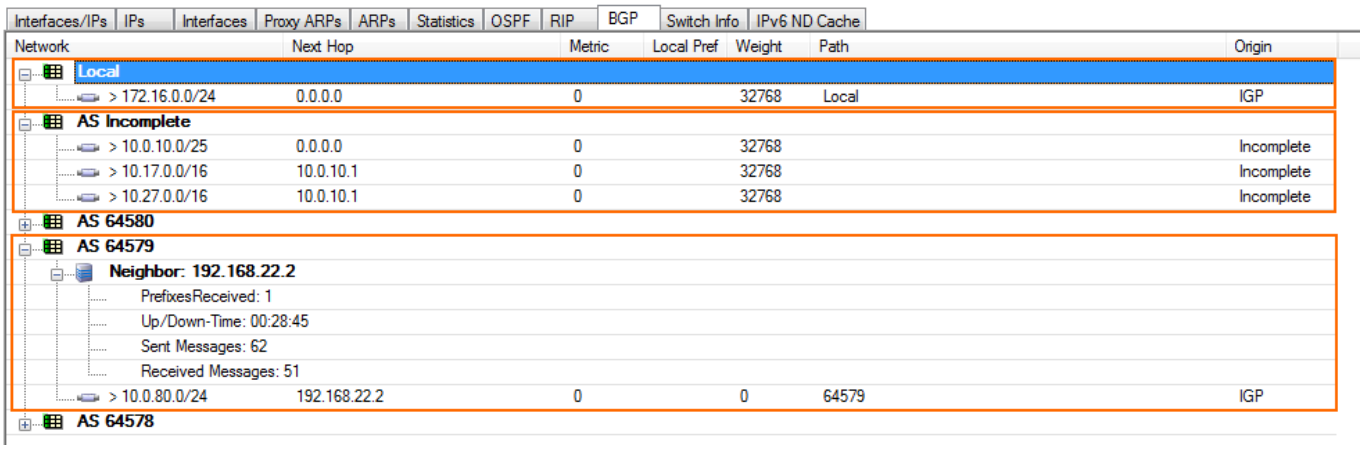


7. Click **OK**.
8. Click **Send Changes** and **Activate**.

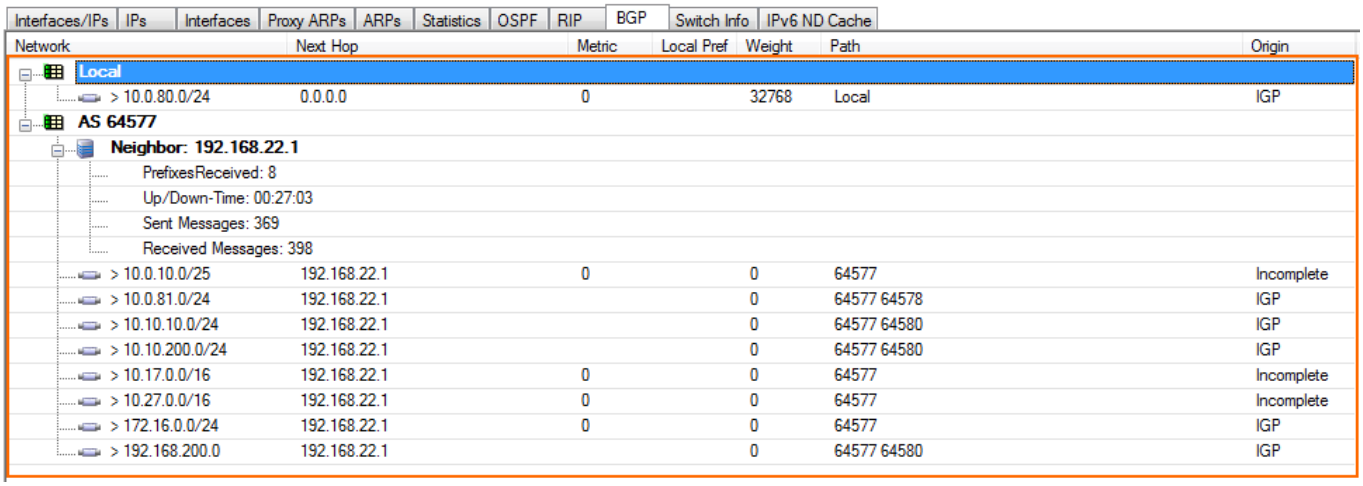
Step 5. Verify the BGP Service Configuration

On the **CONTROL > Network** page, verify that BGP routes are learned. Click the **BGP** tab and expand the relevant AS tree. It can take up to three minutes for new routes to be learned.

Local Firewall **Network > BGP** page:



Remote Firewall **Network > BGP** page:



Figures

1. bgp_over_ipsec_vpn.png
2. ipsec_bgp00.png
3. ipsec_bgp01.png
4. ipsec_bgp02.png
5. ipsec_bgp03.png
6. tina_bgp06d.png
7. tina_bgp06c.png
8. ipsec-bgp04.png
9. tina_bgp06a.png
10. tina_bgp06e.png
11. tina_bgp06b.png
12. ipsec_bgp06.png
13. ipsec-bgp07.png
14. ipsec-bgp08.png