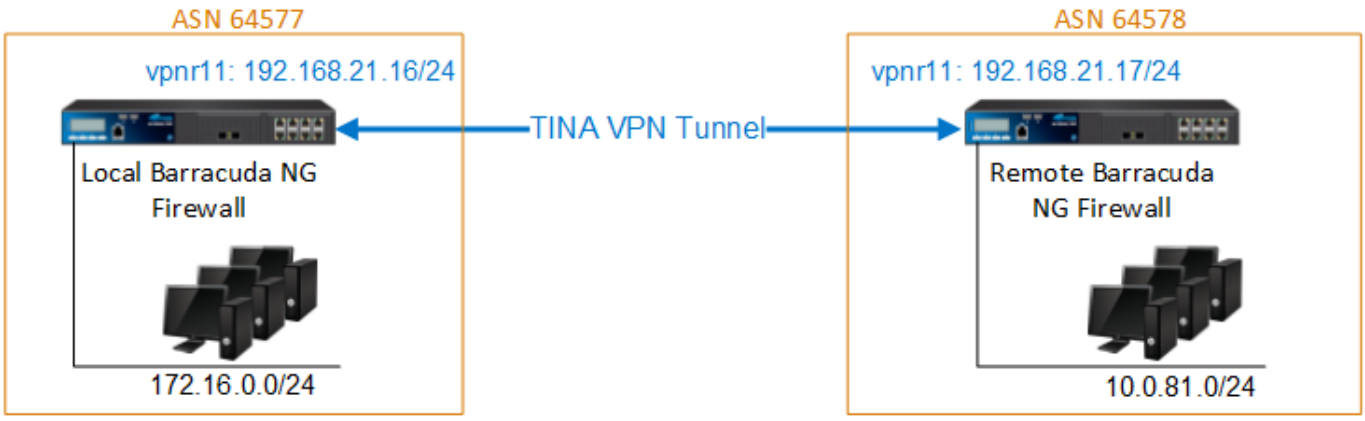
How to Configure BGP Routing over TINA VPN

https://campus.barracuda.com/doc/41115827/

To dynamically learn BGP propagated routes from a remote location connected via TINA VPN tunnel, VPN next hop interfaces are used to create an intermediary network. The BGP service is configured to use the remote IP address in the intermediary network as a BGP neighbor.



You must complete this configuration on both the local and the remote Barracuda NG Firewall using the respective values below:

	Example Values for the Local Barracuda NG Firewall	Example Values for the Remote Barracuda NG Firewall
VPN Next Hop Interface Index	11	11
VPN Next Hop Interface IP Address	192.168.21.16/24	192.168.21.17/24
Virtual Server Additional IP	192.168.21.16	192.168.21.17
VPN Local Networks	192.168.21.16	192.168.21.17
VPN Remote Networks	192.168.21.17	192.168.21.16
VPN Interface Index	11	11
ASN	64577	64578
Router ID	192.168.21.16	192.168.21.17
Neighbor IPv4	192.168.21.17	192.168.21.16
Neighbor AS Number	64578	64577
Neighbor Update Source Interface	vpnr11	vpnr11

In this article:

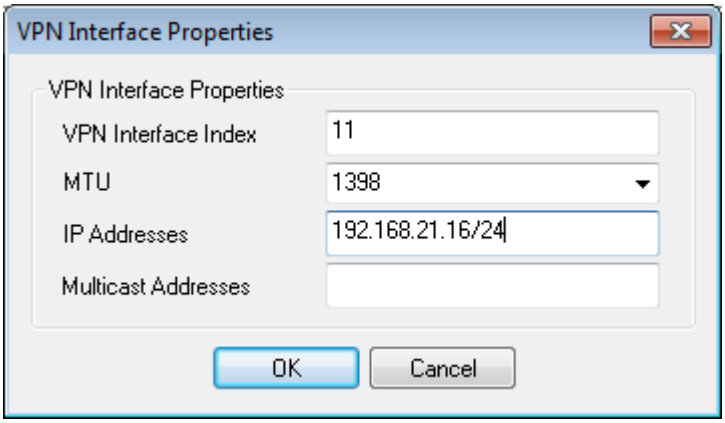
Before You Begin

- A free /24 subnet (e.g., `192.168.21.0/24`) for the intermediary network is needed.
- You must have or assign private Autonomous system numbers (ASNs) for the remote and local networks. The ASNs can be private if you are not propagating these networks to other public networks.

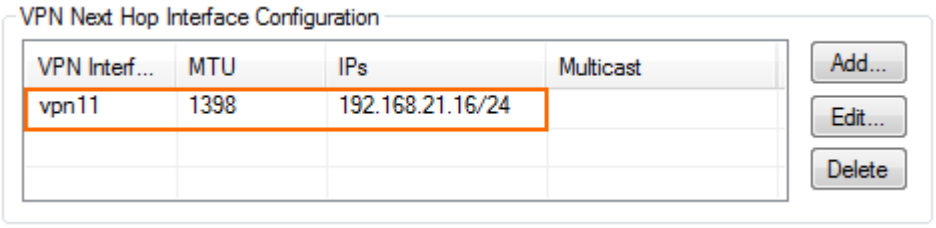
Step 1. Add a VPN Next Hop Interface

Add a VPN next hop interface using a /24 subnet (e.g., `192.168.21.0/24`).

1. Open the **VPN Settings** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service**).
2. Click **Lock**.
3. In the **Settings** tab, click the **Click here for Server Settings** link. The **Server Settings** window opens.
4. In the **Server Settings** window, click the **Advanced** tab.
5. Next to the **VPN Next Hop Interface Configuration** table, click **Add**.
6. In the **VPN Interface Properties** window, configure the following settings and then click **OK**.
   - In the **VPN Interface Index** field, enter a number between `0` and 999. E.g., 11
   - In the **IP Addresses** field, enter the VPN interface IP address including the subnet. E.g., `192.168.21.16/24` for the local or `192.168.21.17/24` for the remote NG Firewall.



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



7. In the **Server Settings** window, click **OK**.
8. Click **Send Changes** and **Activate**.

Step 2. Add the VPN Next Hop Interface IP Address to the Virtual Server Listening IP Addresses

Introduce the IP address of the VPN next hop interface as a virtual server IP address.

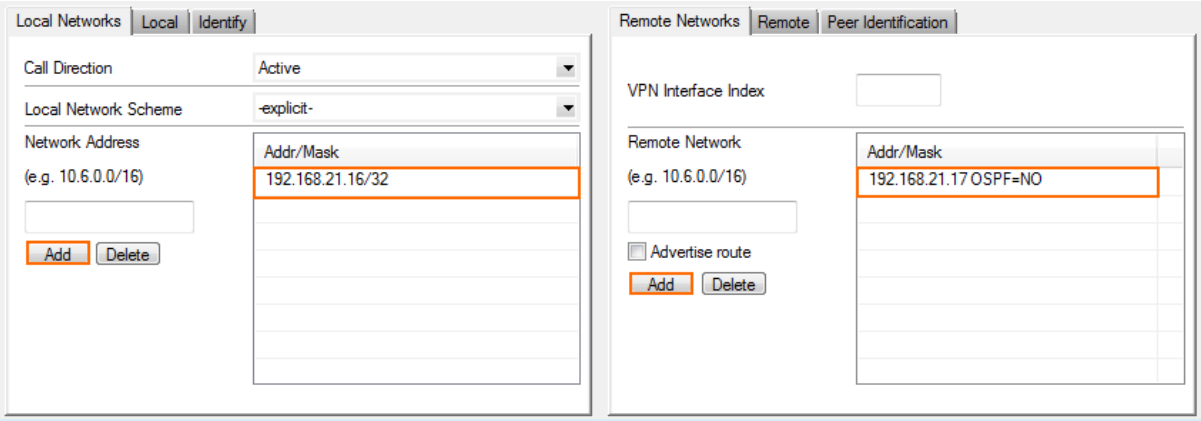
1. Open the **Server Properties** page (**Config > Full Config > Box > Virtual Servers > *your virtual server***).
2. Click **Lock** .
3. In the **Additional IP** table, add the IP address of the VPN interface.
4. Click **Send Changes** and **Activate** .

Step 3. Configure the TINA Site-to-Site VPN Tunnel

Configure a TINA VPN tunnel using the local next hop interface IP address and the VPN next hop interface.

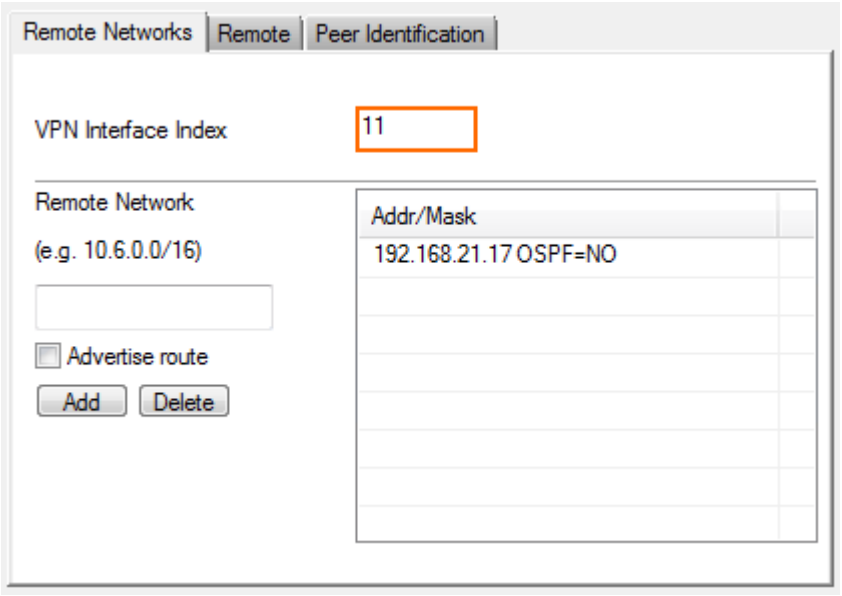
1. Open the **Site to Site** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service**) .
2. Click **Lock**.
3. Right-click In the **TINA Tunnels** tab and select **New TINA tunnel**. The **TINA tunnel** window opens.
4. Enter a **Name**.
5. Configure the **Transport**, **Encryption** and **Authentication** settings as well as the **Local** and **Remote** public IP addresses. . For more information, see How to Create a TINA VPN Tunnel between Barracuda NG Firewalls.
6. Use a free IP address or network as **Local** and **Remote Network**. To avoid multiple tunnels using the same local an remote network it is recommended to use the next hop interface IP addresses. E.g., `192.168.21.16` and `192.168.21.17`
   - In the **Local Networks** tab, enter the local next hop interface IP address, as **Network Address** and click **Add**. E.g., `192.168.21.16` for the local and `192.168.21.17` for the remote NG Firewall
   - In the **Remote Networks** tab, enter the remote next hop interface IP address, as

Network Address and click **Add**. E.g., 192.168.21.17 for the local and 192.168.21.16 for the remote NG Firewall



If used for multiple NG Firewalls connecting to a VPN hub, it is recommended to use the IP address of the local and remote VPN next hop interface to avoid using the same **Remote** and **Local networks** for multiple VPN tunnels.

7. In the **Remote Networks** tab, enter the **VPN Interface Index** number that you created in the **VPN Interface Configuration** in step 1. E.g. 11



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

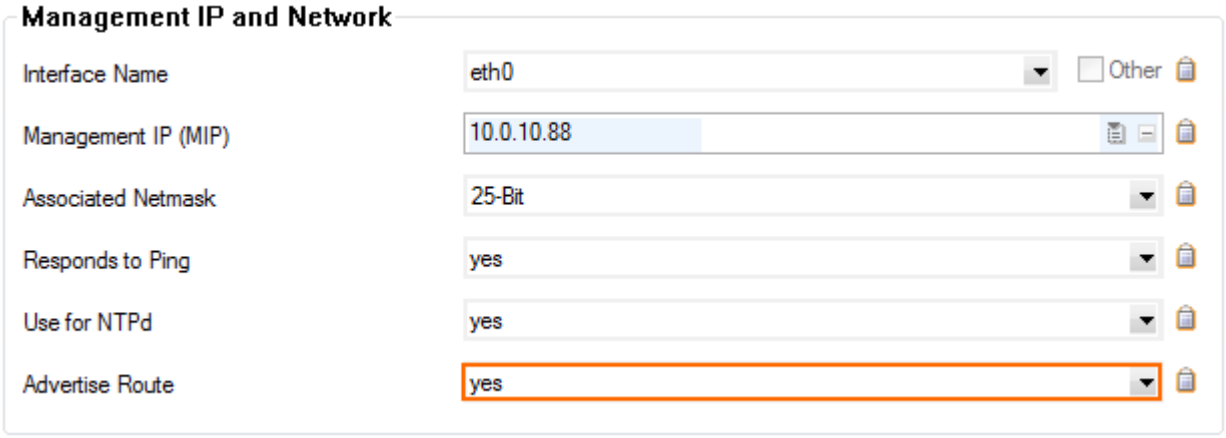
Step 4. Configure the BGP Service

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.

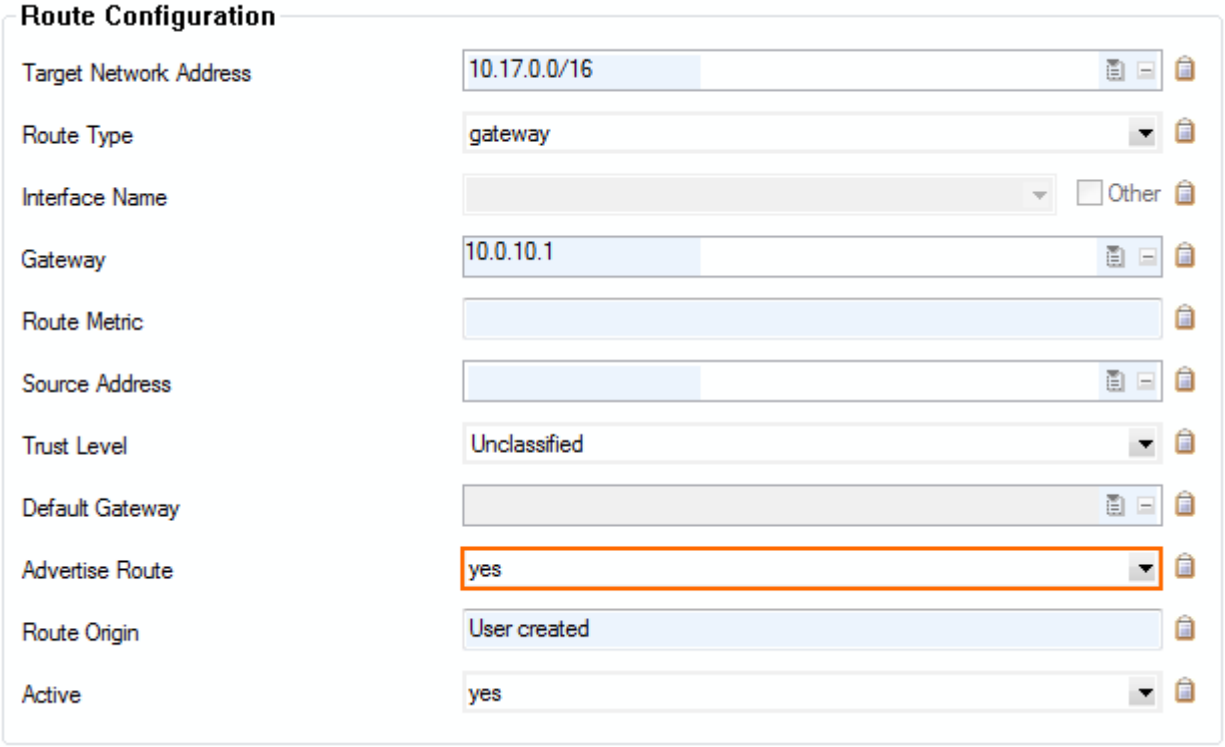
Step 4.1 Configure which Routes to Propagate into BGP

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. Open the **Network** page (**Config > Full Config > Box**).
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 direct attached and gateway routes you want to propagate. The **Routes** window opens.
6. Set **Advertise Route** to **yes** and click **OK.**



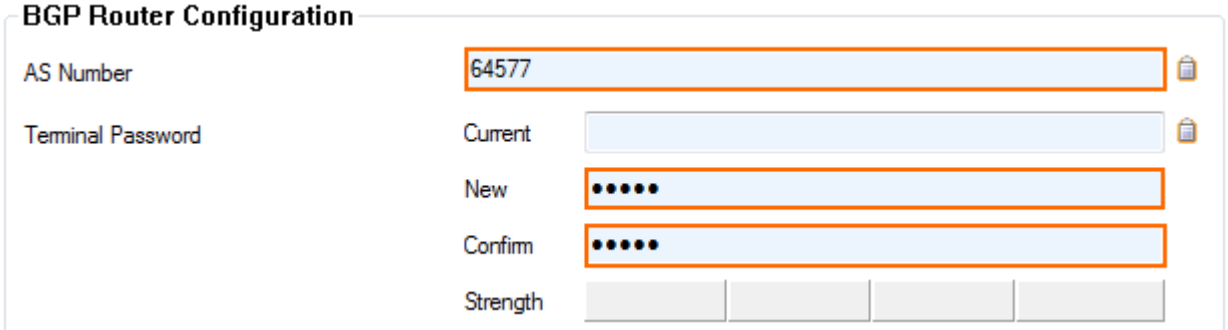
7. Click **Send Changes** and **Activate**.

Step 4.2 Configure the BGP Router

Enable BGP and use the VPN next hop interface IP address as the Router ID.

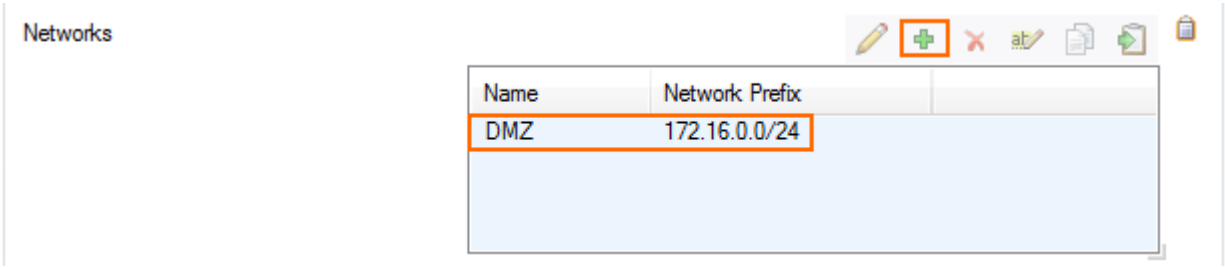
1. Open the **OSPF/RIP/BGP Settings** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > OSPF-RIP-BGP-Service**).
2. Click **Lock**.
3. Set **Run BGP Router** to **Yes**.
4. (optional)To learn routes from the remote ASN set **Operation Mode** to **advertise-learn**.
5. Enter the **Router ID**. Typically the VPN next hop interface IP address is used. E.g., `192.168.21.16` for the local or `192.168.21.17` for the remote NG Firewall.

6. In the left menu, click **BGP Router Setup**.
7. Enter the **AS Number**. E.g., 64577 for the local NG Firewall or 64578 for the remote NG Firewall
8. Enter the **Terminal Password**. Use this password if you must directly connect to the dynamic routing daemon via command line for debugging purposes.



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

10. (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`

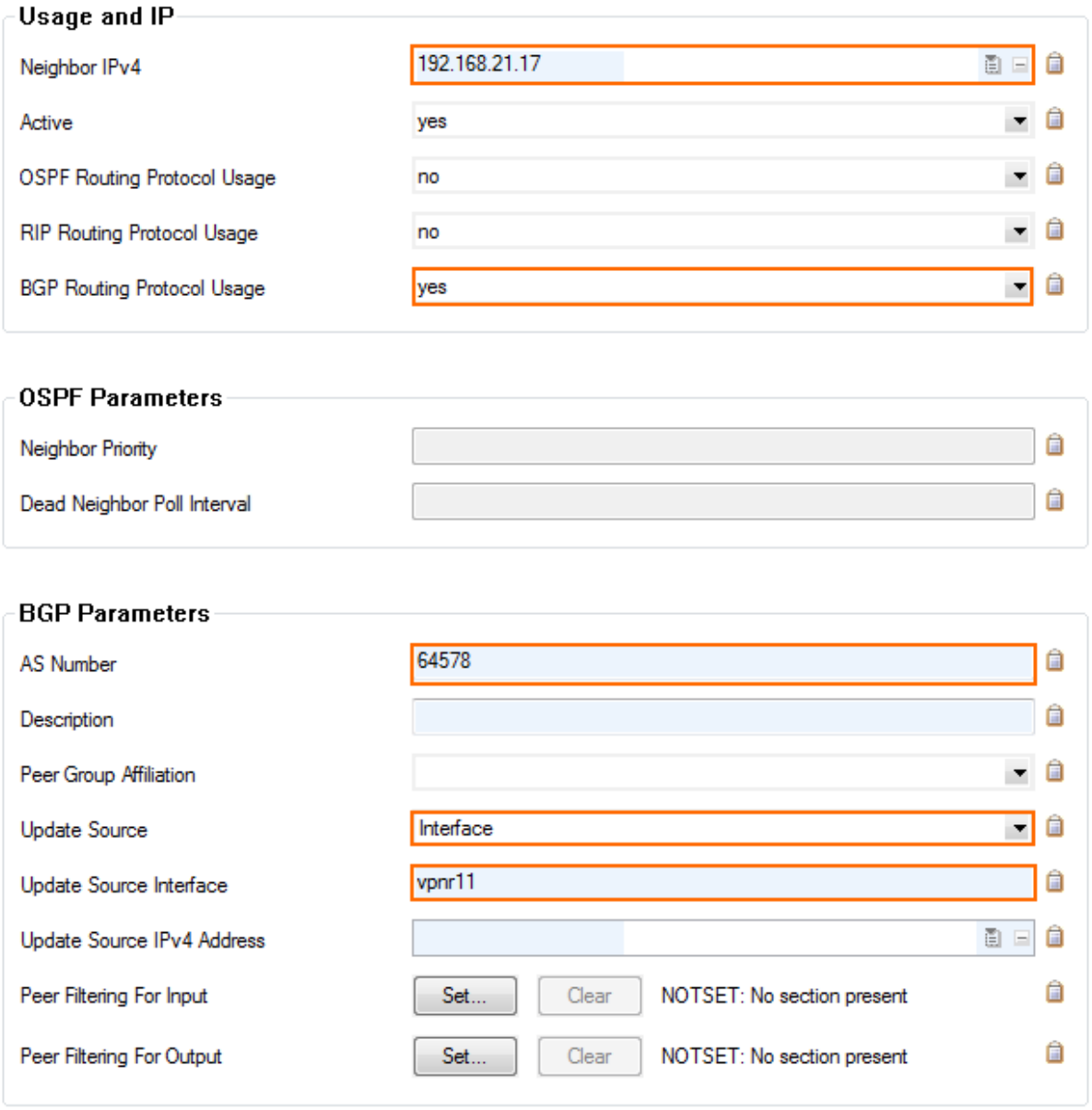


11. Click **Send Changes** and **Activate**.

Step 4.3. Add a BGP Neighbor

To dynamically learn the routing of the neighboring network, set up a BGP neighbor for the 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.,`192.168.21.17` for the local NG Firewall or `192.168.21.16` for the remote NG Firewall.
   - **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., 64578 for the local NG Firewall or 64577 for the remote NG Firewall.
   - **Update Source** – Select **Interface**.
   - **Update Source Interface** – Enter the VPN next hop interface in the format: `vpnr`. E.g., `vpnr11`



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

Step 4.4. (optional) Adjust Keep Alive and Hold Timer

Speed up BGP updates by adjusting the keep alive and hold timer.

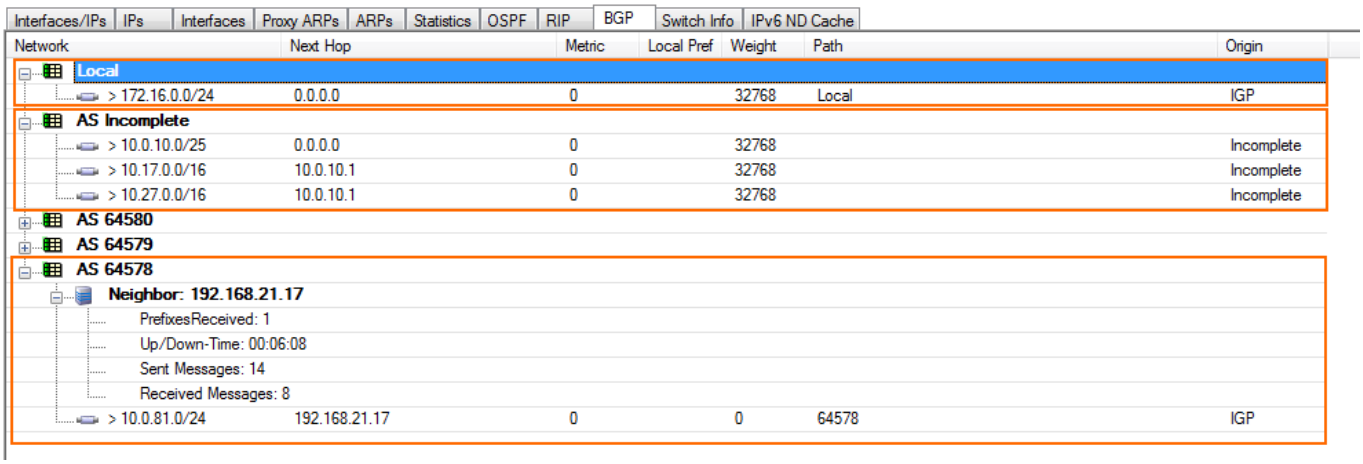
1. Open the **OSPF/RIP/BGP Routing Settings** page (**Config > Full Config > Box > Virtual Servers > *your virtual server* > Assigned Services > OSPF-RIP-BGP-Service**).
2. Click **Lock**.
3. In the left menu, click on **BGP Router Setup.**
4. In the left menu, expand the **Configuration Mode** section and click on **Switch to Advanced View**.
5. Click the **Edit** button for the **Advanced Settings**. The **Advanced Settings** window opens.

6. Adjust the following parameters to influence how fast BGP reacts to connections which are down:
   - **Keep Alive Timer** – Default: 60 Recommended: 10
   - **Hold Timer** – Set to three times the **Keep Alive Timer**. Default: 180 Recommended: 30
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

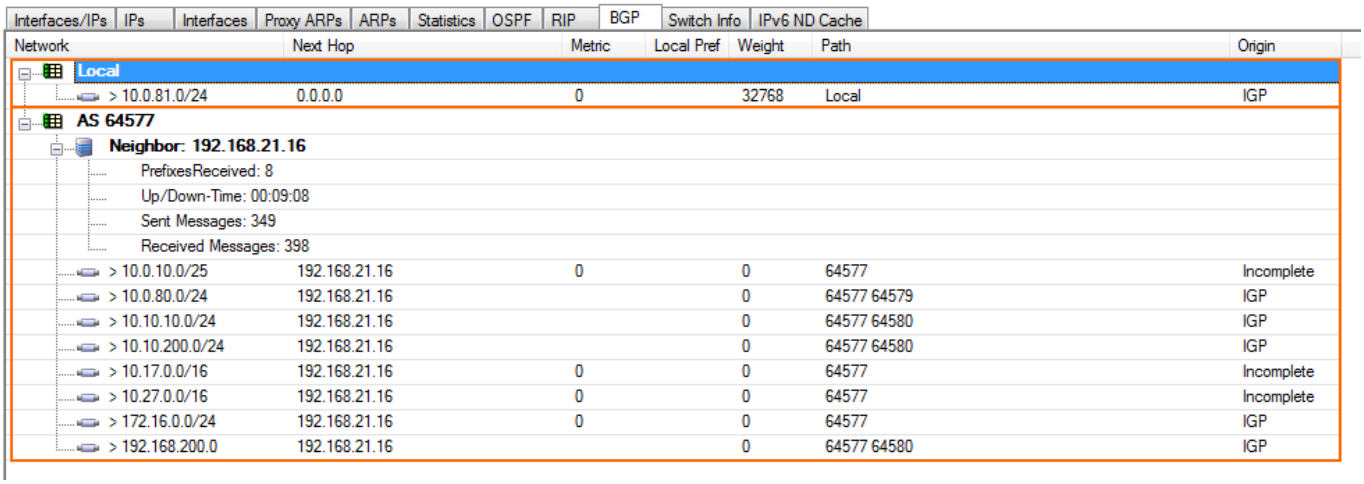
Step 5. Verify the BGP Service Configuration

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.The **Origin** column lists **incomplete** for direct attached or gateway routes or **IGP** routes learned via BGP including manually entered networks.

Local Firewall **Network > BGP** page



Remote Firewall **Network > BGP** page



Interfaces/IPs | IPs | Interfaces | Proxy ARPs | ARPs | Statistics | OSPF | RIP | BGP | Switch Info | IPv6 ND Cache

Network	Next Hop	Metric	Local Pref	Weight	Path	Origin
Local						
> 10.0.81.0/24	0.0.0.0	0		32768	Local	IGP
AS 64577						
Neighbor: 192.168.21.16						
PrefixesReceived: 8						
Up/Down-Time: 00:09:08						
Sent Messages: 349						
Received Messages: 398						
> 10.0.10.0/25	192.168.21.16	0		0	64577	Incomplete
> 10.0.80.0/24	192.168.21.16			0	64577 64579	IGP
> 10.10.10.0/24	192.168.21.16			0	64577 64580	IGP
> 10.10.200.0/24	192.168.21.16			0	64577 64580	IGP
> 10.17.0.0/16	192.168.21.16	0		0	64577	Incomplete
> 10.27.0.0/16	192.168.21.16	0		0	64577	Incomplete
> 172.16.0.0/24	192.168.21.16	0		0	64577	IGP
> 192.168.200.0	192.168.21.16			0	64577 64580	IGP

Step 6. Create Access Rules for VPN Traffic

Create access rules on both local and remote NG Firewalls to allow traffic from the learned networks through the VPN tunnel.

Figures

1. BGPOverTINAVPN.png
2. tina_bgp01.png
3. tina_bgp02.png
4. tina_bgp03.png
5. tina_bgp04.png
6. tina_bgp06d.png
7. tina_bgp06c.png
8. tina_bgp05.png
9. tina_bgp06a.png
10. tina_bgp06e.png
11. tina_bgp06b.png
12. tina_bgp07.png
13. tina_bgp08.png
14. tina_bgp09.png