

How to Configure BGP Routing over TINA VPN

<https://campus.barracuda.com/doc/46208965/>

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 NextGen Firewall F-Series using the respective values below:

	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	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	vpn11	vpn11

In this article:

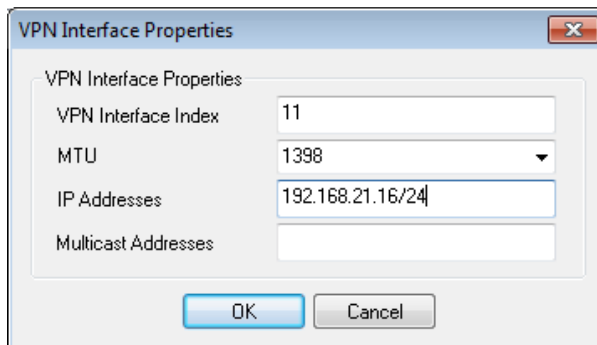
Before You Begin

- 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. 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. 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 NextGen Firewall F-Series.



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

VPN Next Hop Interface Configuration

VPN Interf...	MTU	IPs	Multicast
vpn11	1398	192.168.21.16/24	

Add...
Edit...
Delete

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

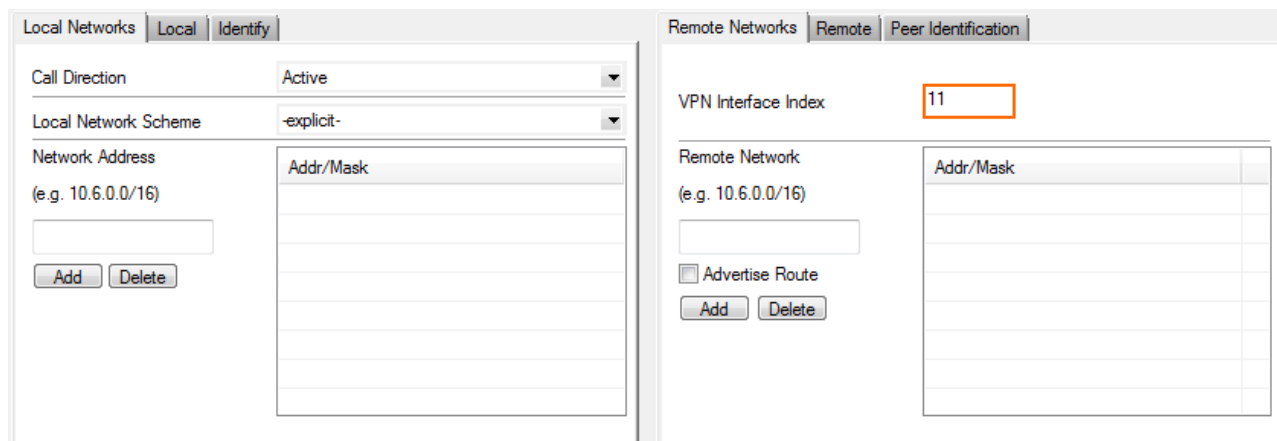
Introduce the IP address of the VPN next hop interface as a virtual server IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Server Properties**.
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. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Site to Site**.
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 F-Series Firewalls](#).
6. Leave the **Local** and **Remote Network** empty.
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**.

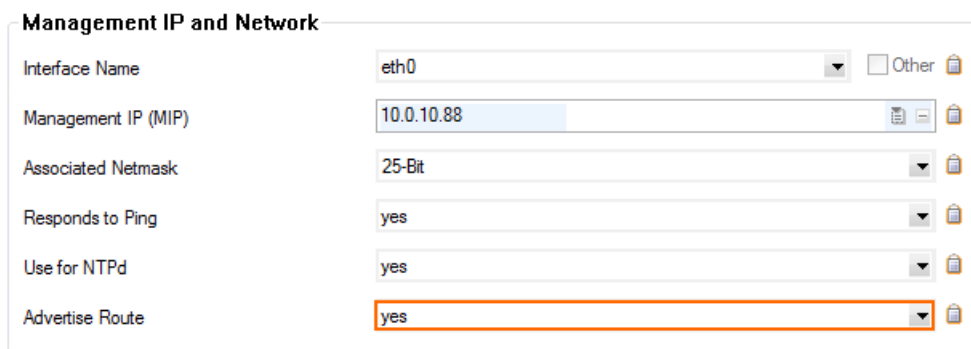
Step 4. Configure the BGP Service

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. 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**.

Route Configuration

Target Network Address	10.17.0.0/16
Route Type	gateway
Interface Name	<input type="text"/> <input type="checkbox"/> Other
Gateway	10.0.10.1
Route Metric	<input type="text"/>
Source Address	<input type="text"/>
Trust Level	Unclassified
Default Gateway	<input type="text"/>
Advertise Route	yes
Route Origin	User created
Active	yes

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. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
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 NextGen Firewall F-Series.

Operational Setup

Run OSPF Router	no
Run RIP Router	no
Run BGP Router	yes
Hostname	<input type="text"/>
Operation Mode	advertise-learn
Router ID	192.168.21.16

6. In the left menu, click **BGP Router Setup**.
7. Enter the **AS Number**. E.g., 64577 for the local NextGen Firewall F-Series or 64578 for the remote NextGen Firewall F-Series.
8. Enter the **Terminal Password**. Use this password if you must directly connect to the dynamic

routing daemon via command line for debugging purposes.

BGP Router Configuration

AS Number

Terminal Password

Current

New

Confirm

Strength

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

Route Redistribution Configuration

Kernel Routes

Static Routes

Connected Routes

RIP Routes

OSPF Routes

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

Networks

Name	Network Prefix
DMZ	172.16.0.0/24

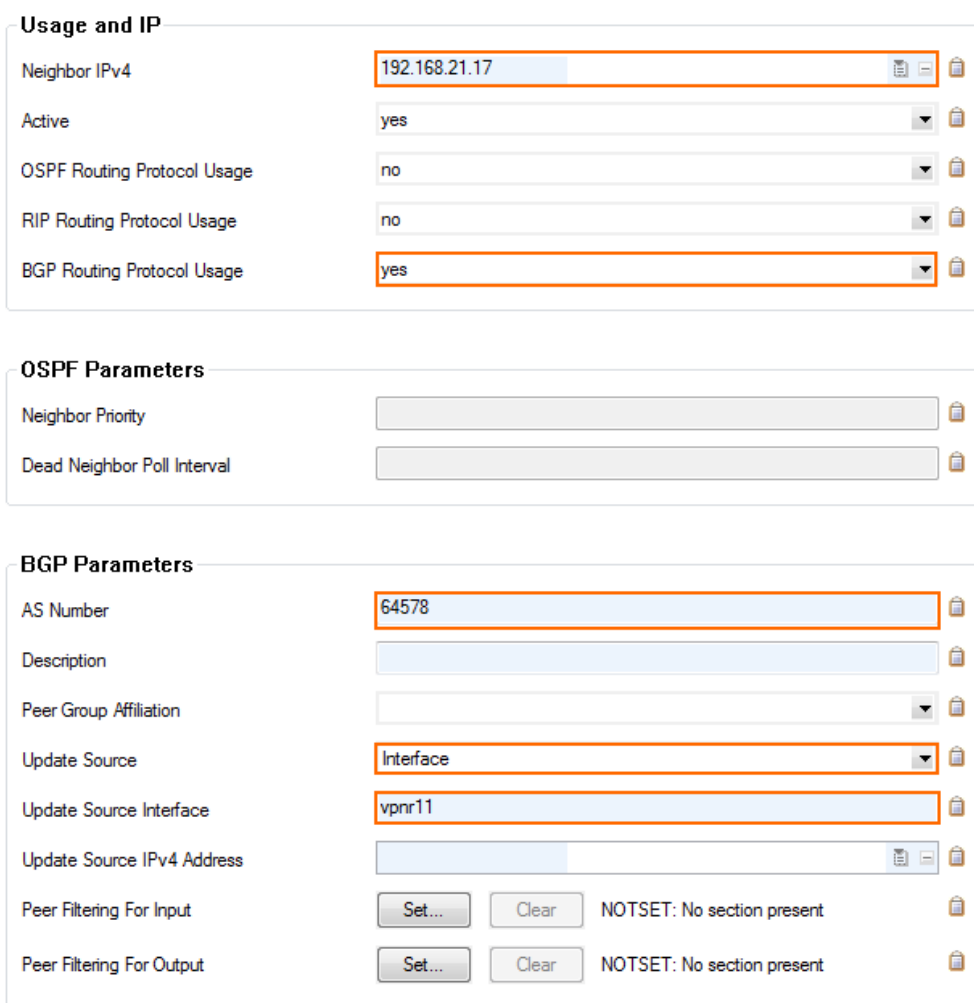
11. Click **Send Changes** and **Activate**.

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.

- In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
- Click **Lock**.
- Next to the **Neighbors** table, click the plus sign (+) to add a new neighbor.
- Enter a **Name** for the neighbor and click **OK**. The **Neighbors** window opens.
- 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 NextGen Firewall F-Series or 192.168.21.16 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**.

- In the **BGP Parameters** section, configure the following settings:
 - AS Number** - Enter the ASN for the remote network. E.g., 64578 for the local NextGen Firewall F-Series or 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., vpnr11



The screenshot displays three configuration sections for BGP:

- Usage and IP:** Neighbor IPv4 (192.168.21.17), Active (yes), OSPF Routing Protocol Usage (no), RIP Routing Protocol Usage (no), BGP Routing Protocol Usage (yes).
- OSPF Parameters:** Neighbor Priority (empty), Dead Neighbor Poll Interval (empty).
- BGP Parameters:** AS Number (64578), Description (empty), Peer Group Affiliation (empty), Update Source (Interface), Update Source Interface (vpn11), Update Source IPv4 Address (empty), Peer Filtering For Input (Set... Clear NOTSET: No section present), Peer Filtering For Output (Set... Clear NOTSET: No section present).

- Click **OK**.
- 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.

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
- Click **Lock**.
- In the left menu, click on **BGP Router Setup**.
- 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 **CONTROL > Network > BGP** page:

Network	Next Hop	Metric	Local Pref	Weight	Path	Origin
Local						
> 172.16.0.0/24	0.0.0.0	0		32768	Local	IGP
AS Incomplete						
> 10.0.10.0/25	0.0.0.0	0		32768		Incomplete
> 10.17.0.0/16	10.0.10.1	0		32768		Incomplete
> 10.27.0.0/16	10.0.10.1	0		32768		Incomplete
AS 64580						
AS 64579						
AS 64578						
Neighbor: 192.168.21.17						
PrefixesReceived: 1						
Up/Down-Time: 00:06:08						
Sent Messages: 14						
Received Messages: 8						
> 10.0.81.0/24	192.168.21.17	0		0	64578	IGP

Remote Firewall **CONTROL > Network > BGP** page:

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						
Prefixes Received: 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 F-Series Firewalls to allow traffic from the learned networks through the VPN tunnel.

Figures

1. bgp_over_tina_vpn.png
2. tina_bgp01.png
3. tina_bgp02.png
4. ipsec_bgp03.png
5. tina_bgp06d.png
6. tina_bgp06c.png
7. tina_bgp05.png
8. tina_bgp06a.png
9. tina_bgp06e.png
10. tina_bgp06b.png
11. tina_bgp07.png
12. tina_bgp08.png
13. tina_bgp09.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.