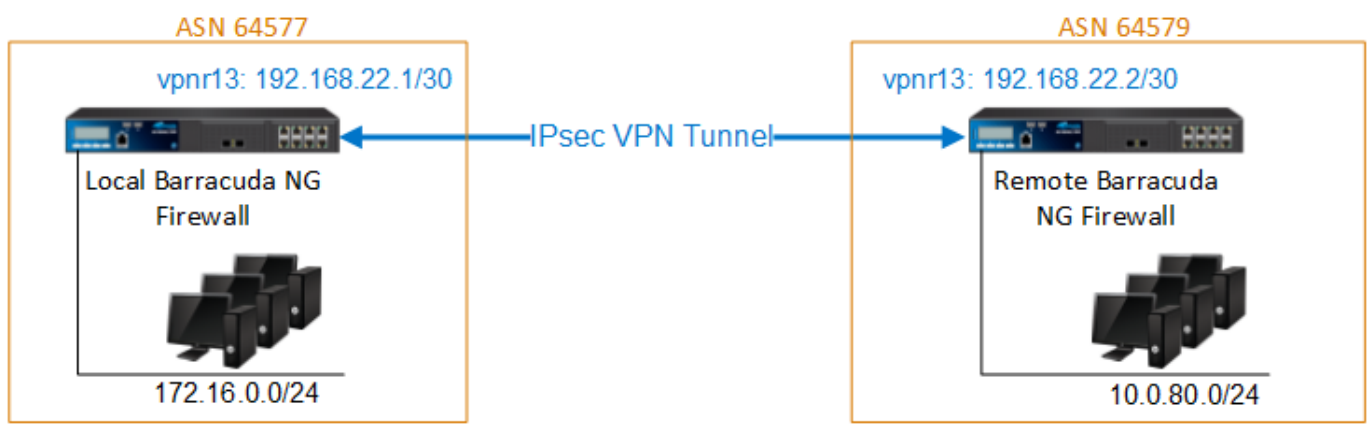


How to Configure BGP Routing over IPsec VPN

<https://campus.barracuda.com/doc/41115817/>

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 NG Firewalls.



	Example Values for the Local Barracuda NG Firewall	Example Values for the Remote Barracuda NG Firewall
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	vpn13	vpn13

In this article:

Before You Begin

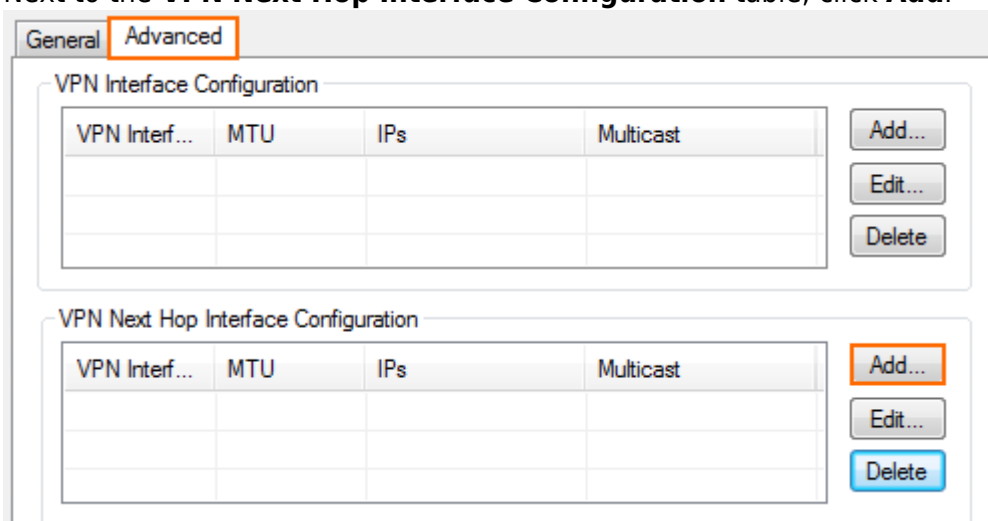
Before you configure BGP over an IPsec VPN, obtain the following:

- 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

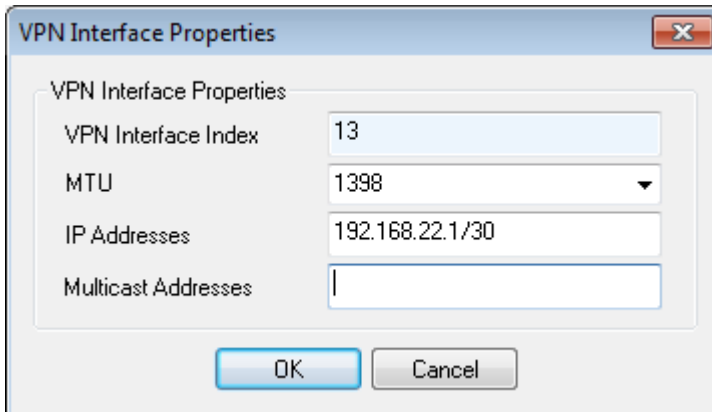
Add a VPN next hop interface using a /30 subnet.

1. 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.
4. In the **Server Settings** window, click the **Advanced** tab.
5. Next to the **VPN Next Hop Interface Configuration** table, click **Add**.



The screenshot shows the 'Advanced' tab of the VPN settings. It contains two tables: 'VPN Interface Configuration' and 'VPN Next Hop Interface Configuration'. Both tables have columns for 'VPN Interf...', 'MTU', 'IPs', and 'Multicast'. The 'Add...' button for the 'VPN Next Hop Interface Configuration' table is highlighted with an orange border.

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 an the VPN interface IP address. E.g., 192.168.22.1/30 for the local NG Firewall or 192.168.22.2/30 for the remote NG Firewall



VPN Interface Properties

VPN Interface Index: 13

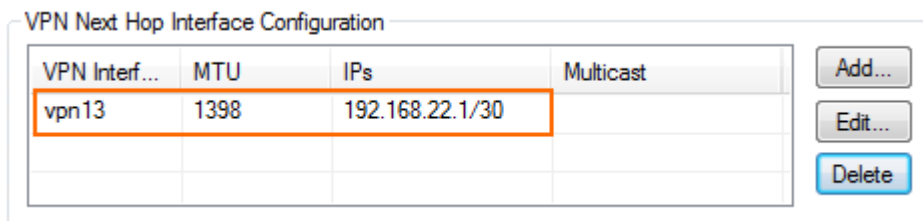
MTU: 1398

IP Addresses: 192.168.22.1/30

Multicast Addresses:

OK Cancel

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



VPN Interf...	MTU	IPs	Multicast
vpn13	1398	192.168.22.1/30	

Add... Edit... Delete

- Click **OK**.
- 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.

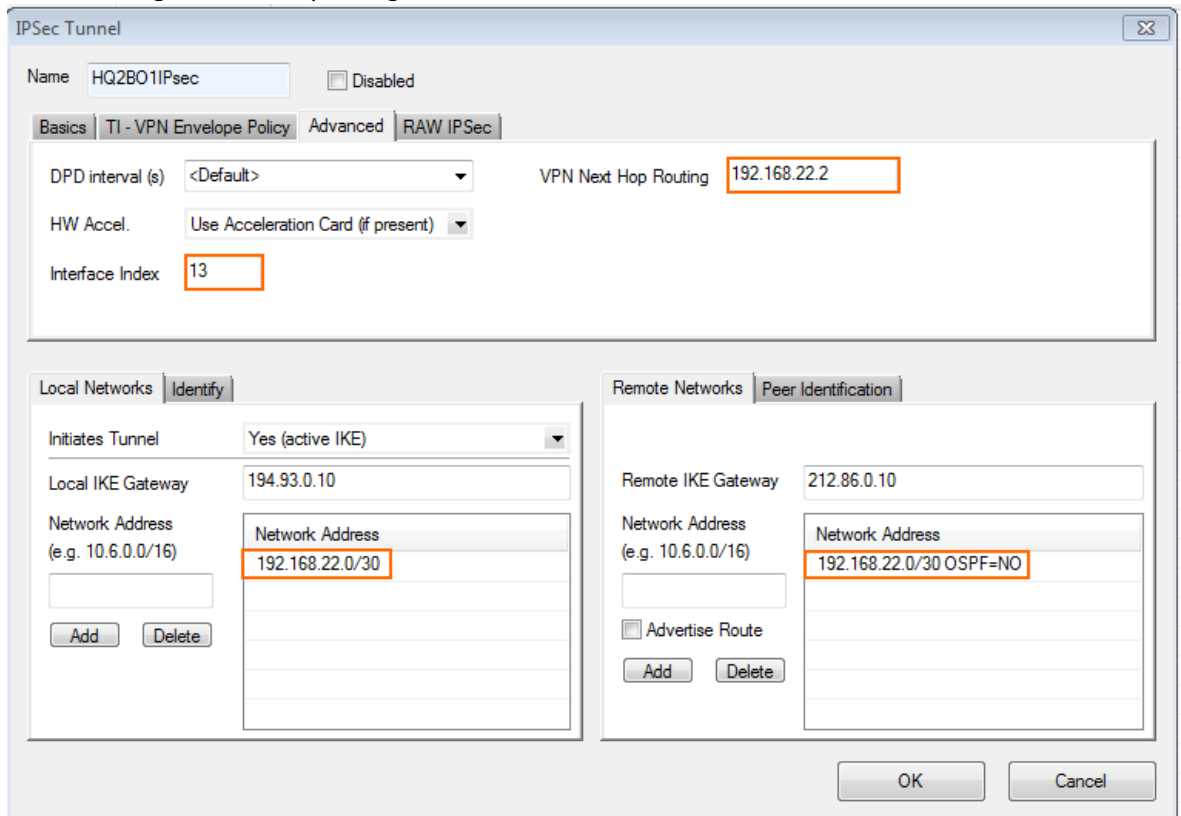
- Open the **Server Properties** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Server Properties**).
- Click **Lock**.
- In the **Additional IP** table, add the intermediary VPN IP address of the local VPN interface.
E.g., 192.168.22.1 for the local NG Firewall or 192.168.22.2 for the remote NG Firewall
- 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.

- Open the **Site to Site** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Site to Site**).
- Click **Lock**.
- Click the **IPSEC Tunnels** tab.

4. Right-click the table under the **IPSEC Tunnels** tab and then select **New IPsec tunnel**.
5. In the **IPsec 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**
 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 NG Firewall or 192.168.22.1 for the remote NG Firewall
 - **Interface Index:** Enter the interface number of the VPN next hop interface configured in step1. E.g. 13



The screenshot shows the 'IPsec Tunnel' configuration window. The 'Advanced' tab is active, displaying the following settings:

- VPN Next Hop Routing:** 192.168.22.2
- Interface Index:** 13

The 'Local Networks' section (Identify) shows:

- Initiates Tunnel:** Yes (active IKE)
- Local IKE Gateway:** 194.93.0.10
- Network Address (e.g. 10.6.0.0/16):** 192.168.22.0/30

The 'Remote Networks' section (Peer Identification) shows:

- Remote IKE Gateway:** 212.86.0.10
- Network Address (e.g. 10.6.0.0/16):** 192.168.22.0/30 OSPF=NO
- Advertise Route:** (unchecked)

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. 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.

Management IP and Network

Interface Name	eth0	<input type="checkbox"/> Other	
Management IP (MIP)	10.0.10.88		
Associated Netmask	25-Bit		
Responds to Ping	yes		
Use for NTPd	yes		
Advertise Route	yes		

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**.

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

1. Open the **OSPF/RIP/BGP Settings** page (**Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services > OSPF-RIP-BGP-Service**).
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 NG Firewall 192.168.22.1 for the remote NG Firewall.

Operational Setup	
Run OSPF Router	no
Run RIP Router	no
Run BGP Router	yes
Hostname	<input type="text"/>
Operation Mode	advertise-learn
Router ID	192.168.22.1

5. In the left menu, click **BGP Router Setup**.
6. Enter the **AS Number**. E.g., 64577 for the local NG Firewall or 64579 for the remote NG Firewall
7. 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	<input type="text" value="64577"/>
Terminal Password	Current <input type="text"/>
	New <input type="password" value="*****"/>
	Confirm <input type="password" value="*****"/>
Strength	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

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

Route Redistribution Configuration

Kernel Routes	<input type="text" value="yes"/>
Static Routes	<input type="text" value="yes"/>
Connected Routes	<input type="text" value="yes"/>
RIP Routes	<input type="text" value="no"/>
OSPF Routes	<input type="text" value="no"/>

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

Networks

Name	Network Prefix
DMZ	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.

- 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., 192.168.22.2 for the local NG Firewall 192.168.22.1 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., 64579 for the local NG Firewall 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., vpnr13

Usage and IP

Neighbor IPv4	<input type="text" value="192.168.22.2"/>
Active	<input type="text" value="yes"/>
OSPF Routing Protocol Usage	<input type="text" value="no"/>
RIP Routing Protocol Usage	<input type="text" value="no"/>
BGP Routing Protocol Usage	<input type="text" value="yes"/>

OSPF Parameters

Neighbor Priority	<input type="text"/>
Dead Neighbor Poll Interval	<input type="text"/>

BGP Parameters

AS Number	<input type="text" value="64579"/>
Description	<input type="text"/>
Peer Group Affiliation	<input type="text"/>
Update Source	<input type="text" value="Interface"/>
Update Source Interface	<input type="text" value="vpnr13"/>
Update Source IPv4 Address	<input type="text"/>
Peer Filtering For Input	<input type="button" value="Set..."/> <input type="button" value="Clear"/> NOTSET: No section present
Peer Filtering For Output	<input type="button" value="Set..."/> <input type="button" value="Clear"/> NOTSET: No section present

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:

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						
Neighbor: 192.168.22.2						
PrefixesReceived: 1						
Up/Down-Time: 00:28:45						
Sent Messages: 62						
Received Messages: 51						
> 10.0.80.0/24	192.168.22.2	0		0	64579	IGP
AS 64578						

Remote Firewall **Network > BGP** page:

Network	Next Hop	Metric	Local Pref	Weight	Path	Origin
Local						
> 10.0.80.0/24	0.0.0.0	0		32768	Local	IGP
AS 64577						
Neighbor: 192.168.22.1						
PrefixesReceived: 8						
Up/Down-Time: 00:27:03						
Sent Messages: 369						
Received Messages: 398						
> 10.0.10.0/25	192.168.22.1	0		0	64577	Incomplete
> 10.0.81.0/24	192.168.22.1			0	64577 64578	IGP
> 10.10.10.0/24	192.168.22.1			0	64577 64580	IGP
> 10.10.200.0/24	192.168.22.1			0	64577 64580	IGP
> 10.17.0.0/16	192.168.22.1	0		0	64577	Incomplete
> 10.27.0.0/16	192.168.22.1	0		0	64577	Incomplete
> 172.16.0.0/24	192.168.22.1	0		0	64577	IGP
> 192.168.200.0	192.168.22.1			0	64577 64580	IGP

Figures

1. BGPOverIPsecVPN.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

© Barracuda Networks Inc., 2020 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.