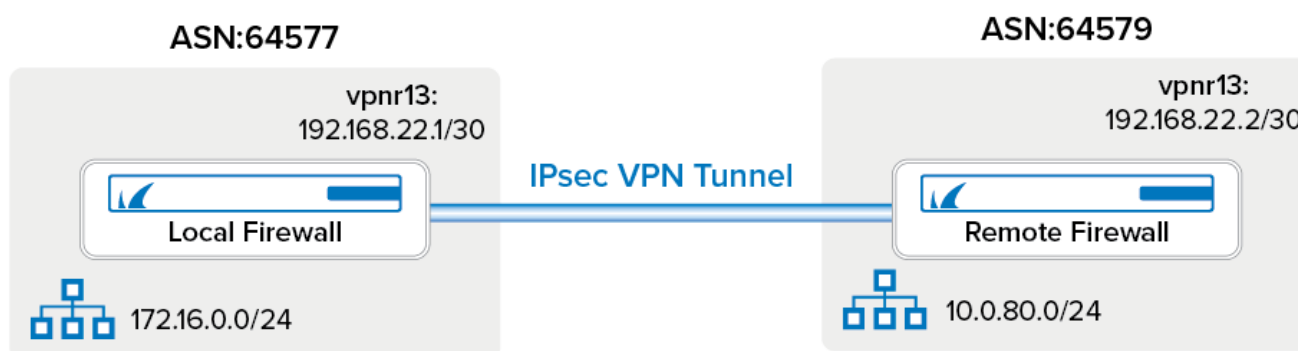


## How to Configure BGP Routing over an IKEv1 IPsec VPN Tunnel

<https://campus.barracuda.com/doc/96026044/>

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 CloudGen Firewalls.



	Example Values for the Local Barracuda CloudGen Firewall	Example Values for the Remote Barracuda CloudGen Firewall
VPN Next Hop Interface Index	13	13
VPN Next Hop Interface IP Address	192.168.22.1/30	192.168.22.2/30
Shared Network IP Address	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

### Before You Begin

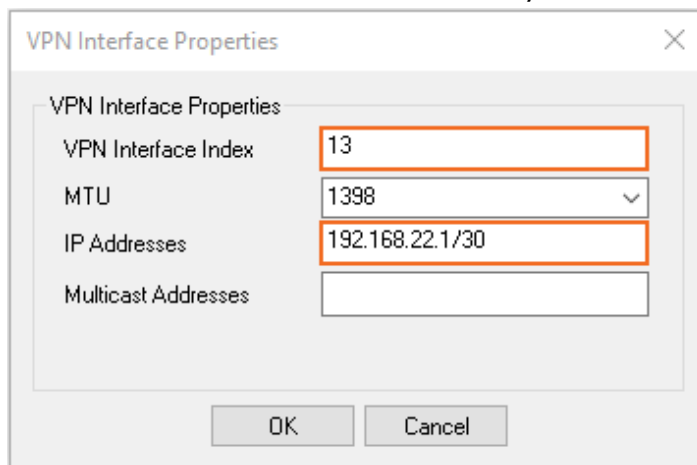
Before you configure BGP over an IPsec VPN, obtain the following:

- 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 > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, select **Routed VPN**.
4. Next to the **Next Hop Interface Configuration** table, click **Add**.
5. 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 firewall or 192.168.22.2/30 for the remote firewall.



The dialog box titled "VPN Interface Properties" contains the following fields:

Field	Value
VPN Interface Index	13
MTU	1398
IP Addresses	192.168.22.1/30
Multicast Addresses	

Buttons: OK, Cancel

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

### Next Hop Interface Configuration

VPN I...	MTU	IPs	Multicast	
vpn13	1398	192.168.22.1...		

Add  
Edit  
Delete

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

---

## Step 2. Add the VPN Interface IP to the Shared IP Addresses

---

Introduce the IP address of the VPN next hop interface on the firewall.

CloudGen Firewalls installed using version 8.0.2 (or higher) do not require the interface IP address to be added to the Shared Networks table as this is handled by the host firewall ruleset.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, select **IP Configuration**.
3. Click **Lock**.
4. In the **Shared Networks and IPs** section, click **+**. The **Shared Network and IPs** window opens.
  1. Select the virtual **Interface**.
  2. In the **Network Address** field, enter the network the virtual interface resides in.
  3. In the **Shared IPs in this Network** table, click **+** and add the intermediary VPN IP address of the VPN interface. E.g., 192.168.22.1 for the local firewall or 192.168.22.2 for the remote firewall.
  4. Click **OK**.
5. Click **Send Changes** and **Activate**.

---

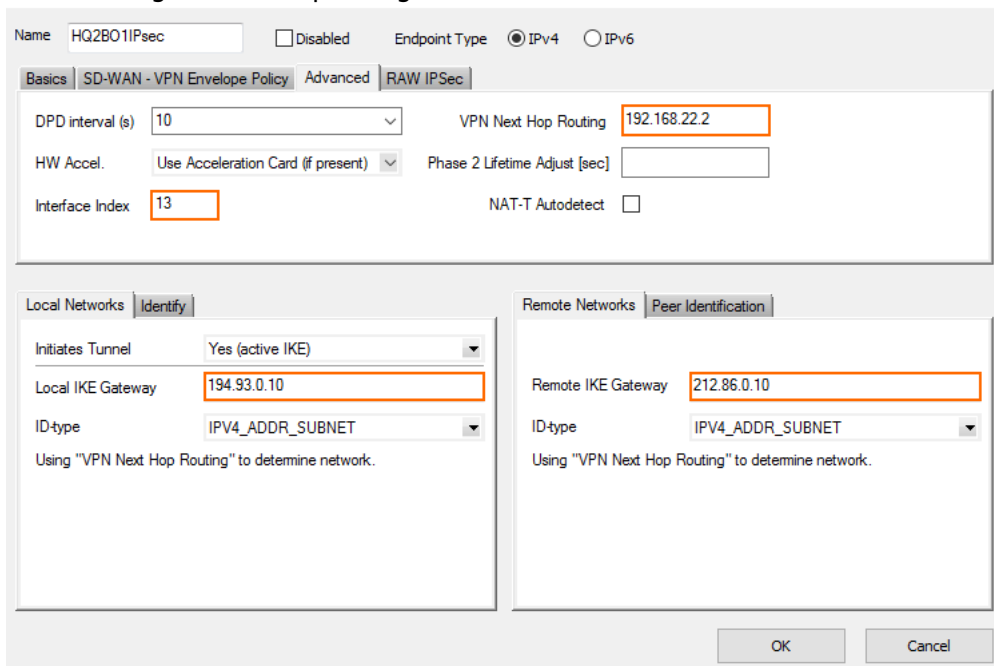
## Step 3. Configure the Site-to-Site VPN Settings

---

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

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 (opposite) VPN next hop interface. E.g., 192.168.22.2 for the local firewall or 192.168.22.1 for the remote firewall.
  - **Interface Index** - Enter the interface number of the VPN next hop interface configured in Step 1. 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.

**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 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="checkbox"/> Other
Gateway	10.0.10.1	
Route Metric		
Source Address		
Trust Level	Unclassified	
Default Gateway		
Advertise Route	yes	
Route Origin	User created	
Active	yes	

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

#### Step 4.2 Configure the BGP Router

1. Go to **CONFIGURATION > Configuration Tree > Box > 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 firewall 192.168.22.1 for the remote firewall.

**Operational Setup**

Run OSPF Router	no	
Run RIP Router	no	
Run BGP Router	yes	
Hostname		
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 firewall or 64579 for the remote 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.

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

**BGP Router Configuration**

AS Number	64577	
Terminal Password	Current	
	New	•••••
	Confirm	•••••
	Strength	<div></div>

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

**Route Redistribution Configuration**

Kernel Routes	yes	
Static Routes	yes	
Connected Routes	yes	
RIP Routes	no	
OSPF Routes	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

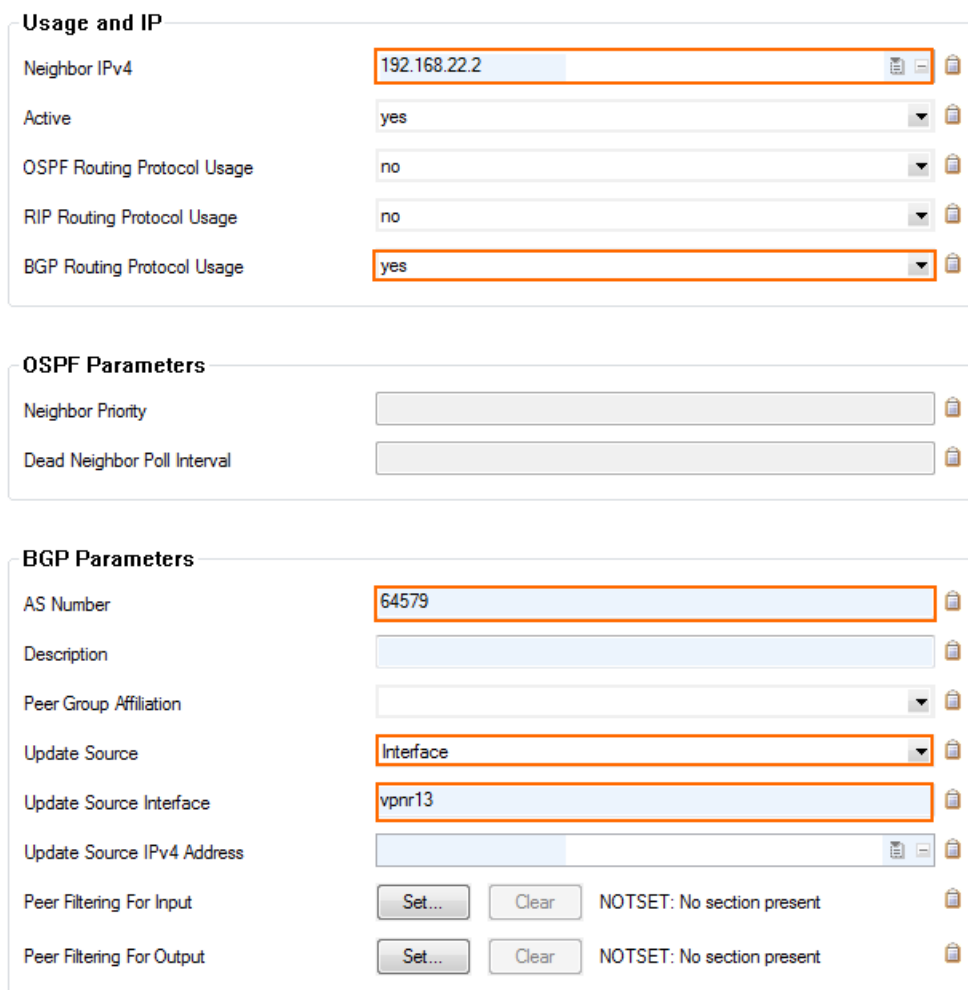
10. Click **Send Changes** and **Activate**.

### 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.

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 firewall 192.168.22.1 for the remote 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 firewall 64577 for the remote firewall.
  - **Update Source** – Select **Interface**.
  - **Update Source Interface** – Enter the VPN next hop interface in the format: vpnr<interface number>. E.g., vpnr13



The screenshot displays the configuration interface for a new neighbor in the 'Neighbor Setup IPv4' section. It is divided into three main panels: 'Usage and IP', 'OSPF Parameters', and 'BGP Parameters'. In the 'Usage and IP' panel, 'Neighbor IPv4' is set to 192.168.22.2, 'Active' is checked, 'OSPF Routing Protocol Usage' is 'no', 'RIP Routing Protocol Usage' is 'no', and 'BGP Routing Protocol Usage' is 'yes'. The 'OSPF Parameters' panel shows empty fields for 'Neighbor Priority' and 'Dead Neighbor Poll Interval'. The 'BGP Parameters' panel shows 'AS Number' as 64579, 'Update Source' as 'Interface', and 'Update Source Interface' as 'vpnr13'. Other fields like 'Description', 'Peer Group Affiliation', and 'Update Source IPv4 Address' are empty. At the bottom, there are 'Set...' and 'Clear' buttons for 'Peer Filtering For Input' and 'Peer Filtering For Output', both currently set to 'NOTSET: No section present'.

Usage and IP	
Neighbor IPv4	192.168.22.2
Active	yes
OSPF Routing Protocol Usage	no
RIP Routing Protocol Usage	no
BGP Routing Protocol Usage	yes

OSPF Parameters	
Neighbor Priority	
Dead Neighbor Poll Interval	

BGP Parameters	
AS Number	64579
Description	
Peer Group Affiliation	
Update Source	Interface
Update Source Interface	vpnr13
Update Source IPv4 Address	
Peer Filtering For Input	Set... Clear NOTSET: No section present
Peer Filtering For Output	Set... 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:

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										
> 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:

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										
> 10.0.80.0/24	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. bgp\_over\_ipsec\_vpn01.png
2. ipsec\_bgp1.png
3. ipsec\_bgp2.png
4. ipsec\_bgp03.png
5. tina\_bgp06d.png
6. tina\_bgp06c.png
7. ipsec-bgp04.png
8. tina\_bgp06a.png
9. tina\_bgp06e.png
10. tina\_bgp06b.png
11. ipsec\_bgp06.png
12. ipsec-bgp07.png
13. ipsec-bgp08.png

© Barracuda Networks Inc., 2024 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.