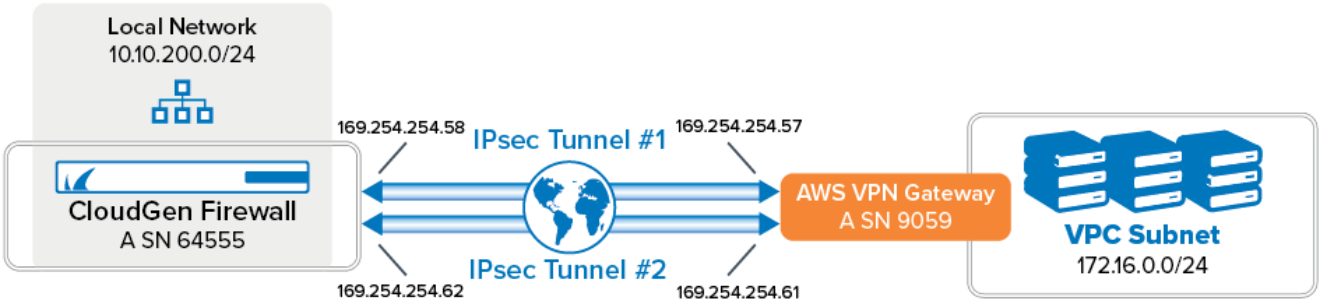
# How to Configure an IKEv1 IPsec VPN to an AWS VPN Gateway with BGP

https://campus.barracuda.com/doc/79462886/

If you are using the Amazon Virtual Private Cloud, you can transparently extend your local network to the cloud by connecting the private networks through a site-to-site IKEv1 IPsec VPN tunnel. The Amazon virtual private gateway uses two parallel IKEv1 IPsec tunnels to ensure constant connectivity. The subnets behind the VPN gateway are propagated via BGP.

Additional Amazon AWS charges apply. For more information, see Amazon's monthly pricing calculator at http://calculator.s3.amazonaws.com/calc5.html.




## Before You Begin

- Create an Amazon Virtual Private Cloud (VPC).
  The local and remote (VPC) subnets must not overlap. E.g, if your local network is 10.0.1.0/24, do not use 10.0.0.0/16 for your VPC.
- Create at least one subnet in the VPC.
- Create and configure the Amazon Routing Table.
- The security group of the VPC must allow the desired connections. For more information, see https://docs.aws.amazon.com/en_pv/vpn/latest/s2svpn/SetUpVPNConnections.html#vpn-configure-security-groups.
- On your CloudGen Firewall, create the VPN service if it does not already exist.
- Configure the VPN Service Listeners.
- Create the OPSF/RIP/BGP service if it does not already exist.

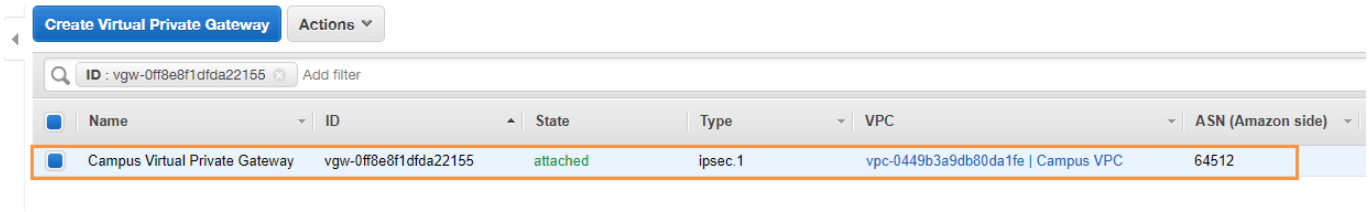
## Step 1 - Create the Amazon VPN Gateway

#### Step 1.1 - Create a Virtual Private Gateway

The Amazon virtual private gateway is the VPN concentrator on the remote side of the IPsec VPN connection.

1. Go to the Amazon VPC Management Console.
2. In the left menu, click **Virtual Private Gateways**.
3. Click **Create Virtual Private Gateway**.
4. Enter the **Name tag** for the VPN gateway (e.g., `Campus Virtual Private Gateway`).
5. Click **Create Virtual Private Gateway**.
6. Select the newly created virtual private gateway, click **Actions** and select **Attach to VPC**.
7. Select your VPC from the **VPC** list, and click **Yes, Attach**.

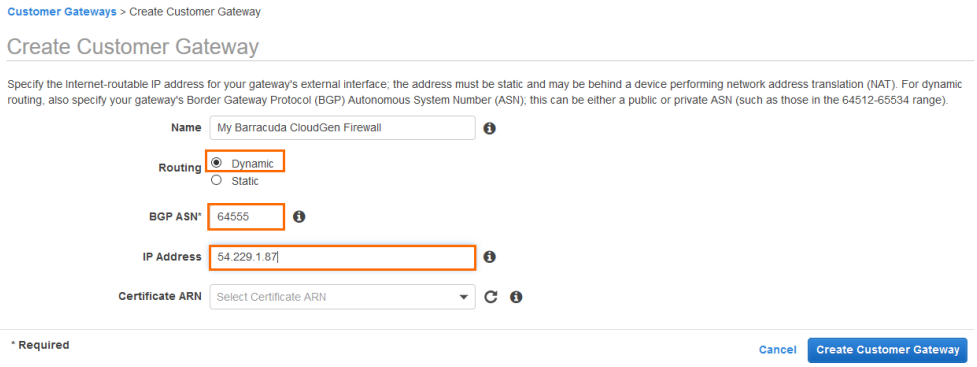
The virtual private gateway is now available.




#### Step 1.2 - Add Your Customer Gateway Configuration

The Amazon customer gateway is your Barracuda CloudGen Firewall on your end of the VPN connection. Specify your external IP address and routing type in the customer gateway configuration:

1. Go to the Amazon VPC Management Console.
2. In the left menu, click **Customer Gateways**.
3. Click **Create Customer Gateway**.
4. Enter the connection information for your firewall:
   - **Name** – Enter a name for your device (e.g., `My Barracuda CloudGen Firewall`).
   - **Routing** – Select **Dynamic**.
   - **BGP ASN** – Enter your BGP ASN number.
   - **IP Address** – Enter your external **IP Address**. To look up your external IP address, go to **CONTROL > Network**.




5. Click **Create Customer Gateway**.

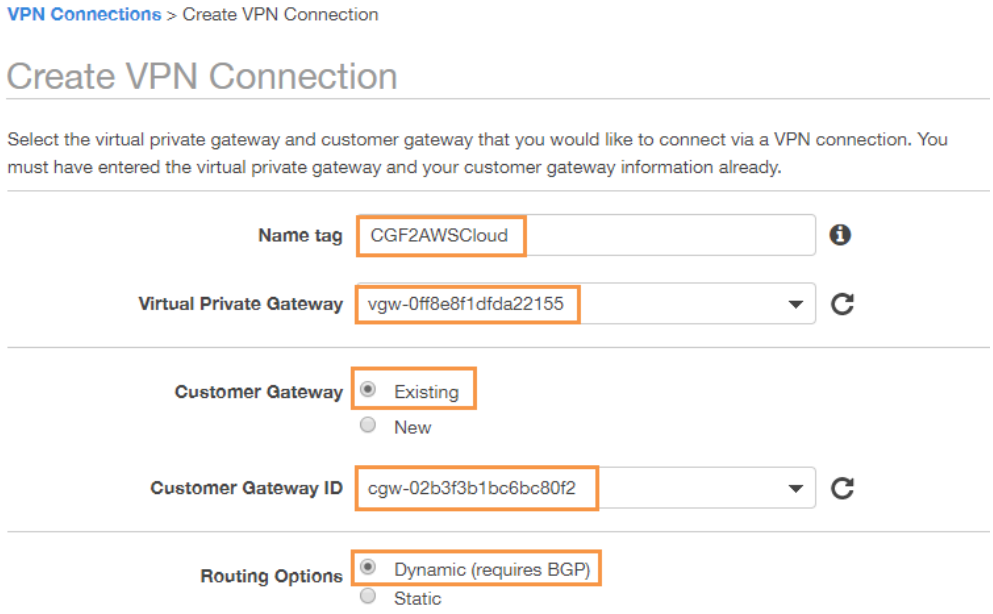
Your firewall is now registered in the AWS cloud and you can configure VPN connections.

#### Step 1.3 - Create a VPN Connection

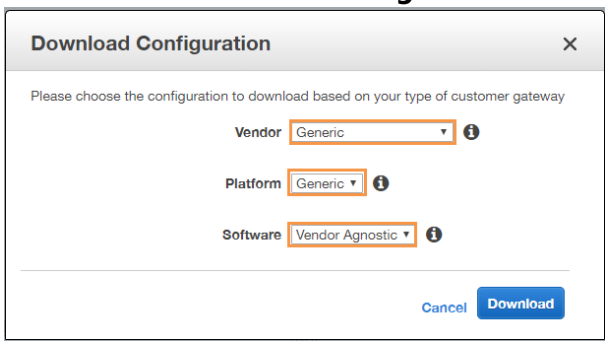
Create a VPN connection with the Customer Gateway (Your CloudGen Firewall) and the Amazon Virtual Private Gateway that you just created. Then download the VPN configuration file that contains all necessary information for configuring the VPN connection on the firewall.

> The Amazon VPN configuration file is different for every VPN connection.

1. Go to the Amazon VPC Management Console.
2. In the left menu, click **Site-to-Site VPN Connections**.
3. Click **Create VPN Connection**.
4. In the **Create VPN Connection** window, enter the configuration information for your VPN connection:
   - **Name tag** – Enter a name for your VPN connection (e.g., `CGF2AWSCloud`).
   - **Virtual Private Gateway** – Select the virtual private gateway created in Step 1.
   - **Customer Gateway** – Select the customer gateway created in Step 1.
   - **Routing Options** – Select **Dynamic (requires BGP)**.



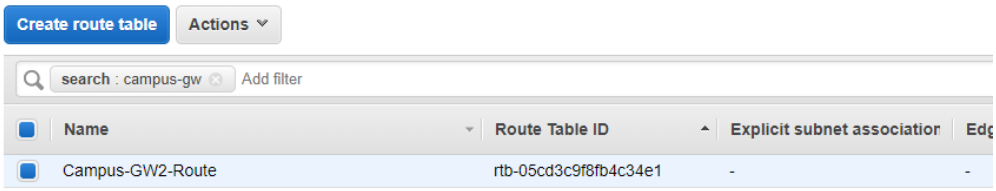

5. Click **Create VPN Connection**.
6. Once the connection is available in AWS, click **Download Configuration**.
7. Select generic vendor and platform settings for the configuration file:
   - **Vendor** – Select **Generic**.
   - **Platform** – Select **Generic**.
   - **Software** – Select **Vendor Agnostic**.

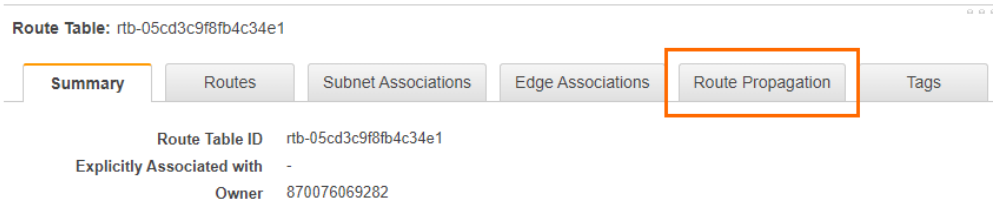



8. Click **Download**, and save the `vpn-<YOUR-VPC-ID>.txt` file. The configuration file contains all required information to configure each VPN tunnel and the respective BGP routing options on your CloudGen Firewall.

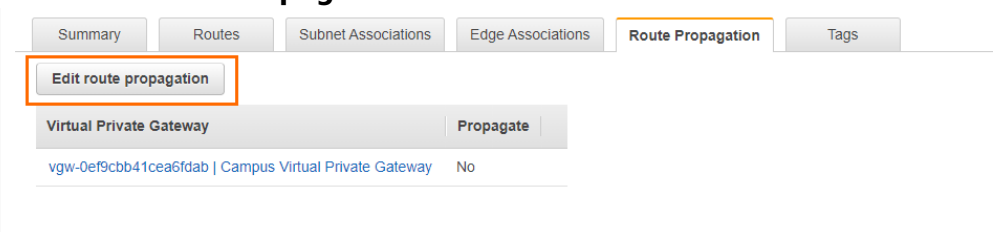
#### Step 1.4 - Enable Route Propagation

1. Go to the Amazon VPC Management Console.
2. In the left menu, click **Route Tables**.
3. Select the route table attached to your VPC used in Step 1.1.
4. Click **Route Propagation**.

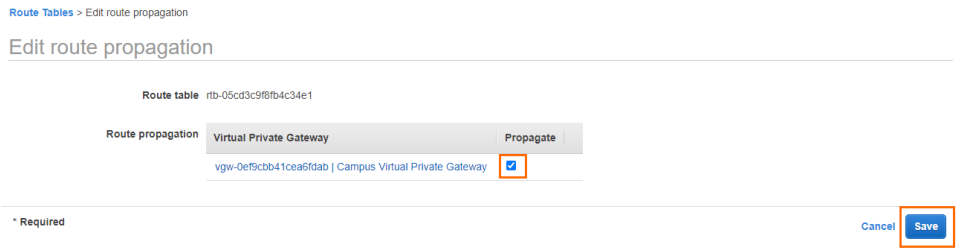



5. Click **Edit Route Propagation**.




6. Enable the route propagation for your virtual private gateway created in Step 1.1 by selecting the check box next to it.




7. Click **Save**.

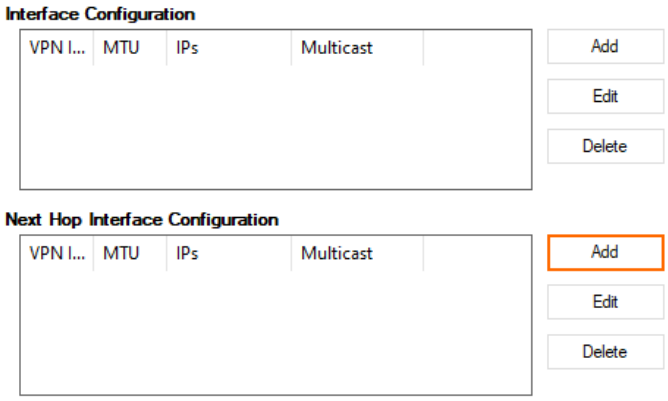
## Step 2 - Configure IPsec Tunnels on the Barracuda CloudGen Firewall

For each IPsec tunnel, create a next-hop interface and then configure two IPsec site-to-site VPN tunnel. Use the IP addresses provided in the Amazon generic VPN configuration file you downloaded at the end of Step 1.

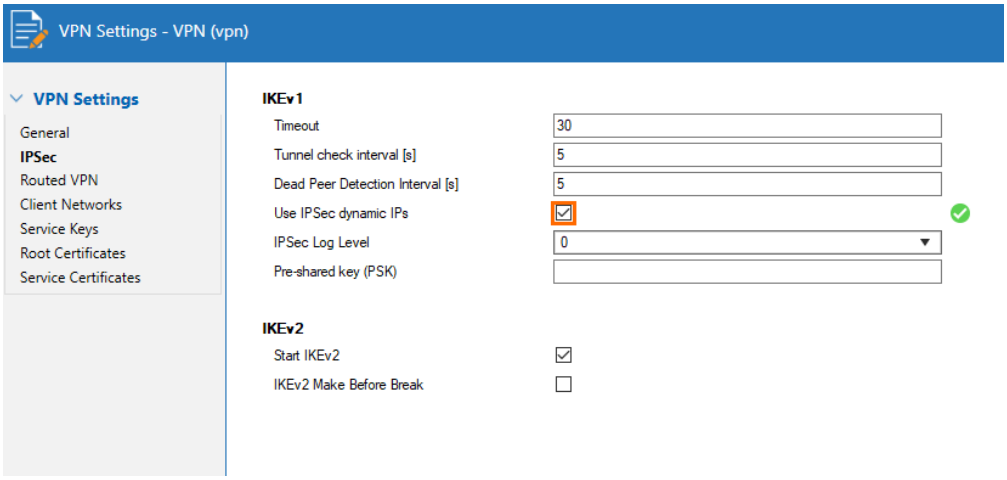
#### Step 2.1 - Create VPN Next-Hop Interfaces

For each IPsec tunnel, a VPN next-hop interface must be created. Use the IP addresses provided in the Amazon generic VPN configuration file you downloaded at the end of Step 1.

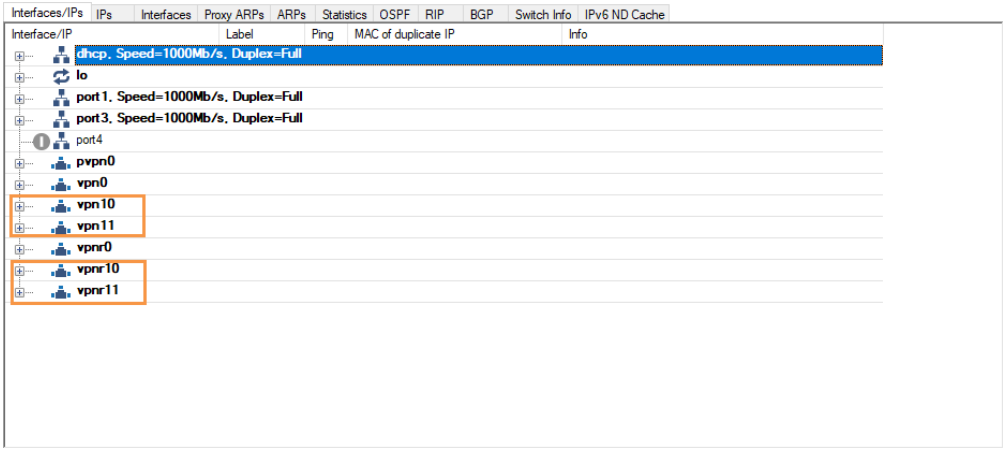
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left navigation bar, click **Routed VPN**.




4. Create a VPN next-hop interface for each IPsec tunnel by clicking **Add** in the **VPN Next Hop Interface Configuration** section.
    1. In the **VPN Interface Properties** window enter:
        - **VPN Interface Index** – Enter a number between 0 and 99. Each interface index number must be unique. E.g., IPsec tunnel1: `10` and IPsec tunnel: `11`
        - **MTU** – Enter 1436.
        - **IP Addresses** – Enter the **Inside IP Address** of the **Customer Gateway** provided by Amazon. E.g., IPsec tunnel1: `169.254.254.58/30`, IPsec tunnel 2: `169.254.254.62/30`
    2. Click **OK**.
5. (optional) In the left navigation bar, click **IPSec**. Enable **Use IPSec dynamic IPs** if you are using a dynamic WAN IP address. This will create an IPsec VPN listener on 0.0.0.0/0.




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




**Step 2.2. Configure Two Site-to-Site IPsec Tunnels**

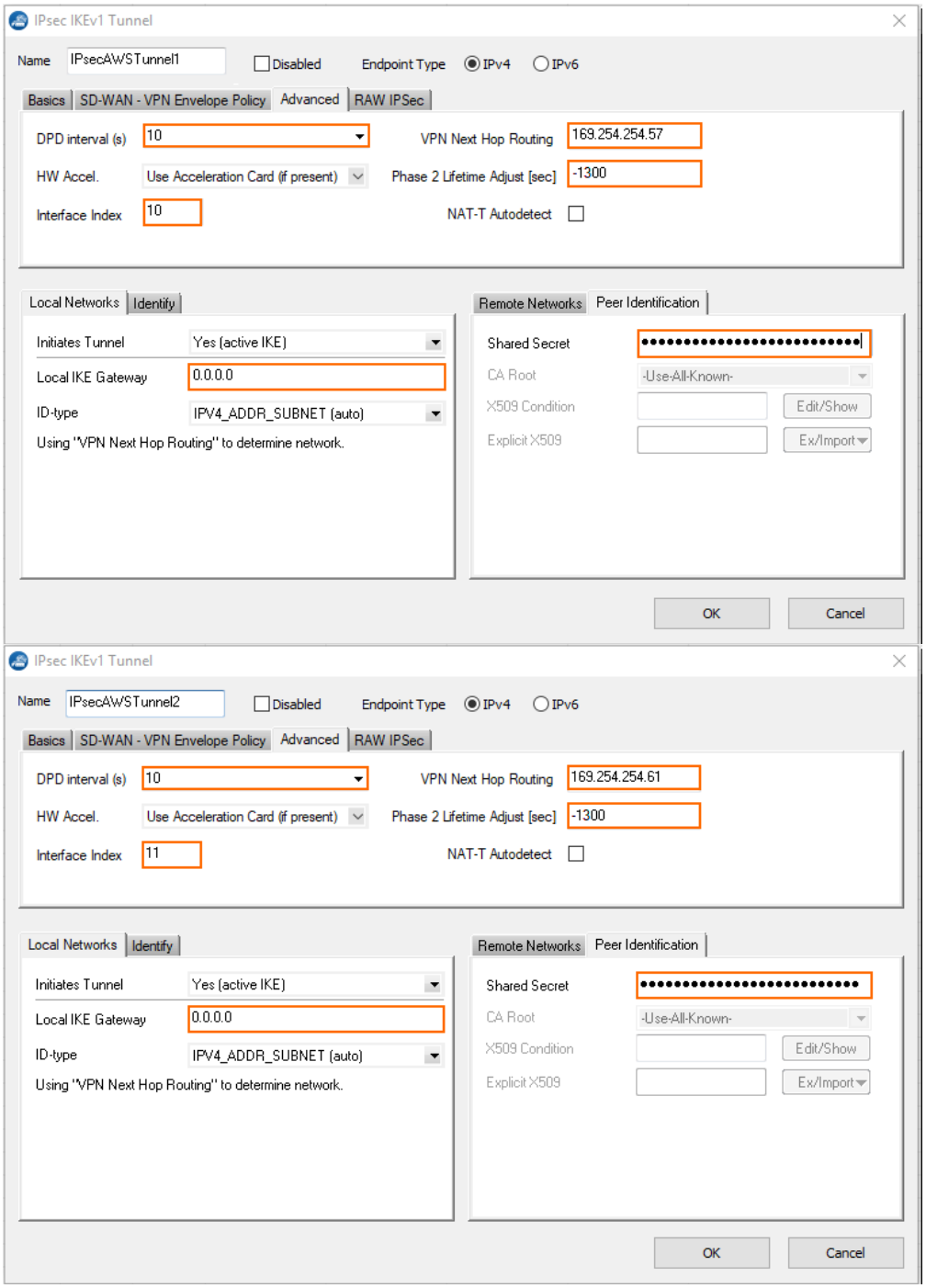
Configure two site-to-site IPsec tunnels using the VPN next-hop interfaces. Make sure to use the correct IP addresses and corresponding next-hop interfaces listed in the Amazon generic VPN configuration file for each tunnel.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site**.
2. Click on the **IPSEC IKEv1 Tunnels** tab.
3. Click **Lock**.
4. For each IPsec tunnel, right-click and click **New IPsec IKEv1 tunnel**.
    1. Enter the IPsec tunnel configurations:
        1. Enter a **Name**. E.g, IPsec Tunnel 1: `IPsecAWSTunnel1` and for IPsec Tunnel 2: `IPsecAWSTunnel2`
        2. Enter the **Phase 1** and **Phase 2** settings. The following values are supported for a tunnel to the AWS VPN gateway:

| | **Phase 1** | **Phase 2** |
|---|---|---|
| **Encryption** | AES<br>AES 256 | AES<br>AES 256 |

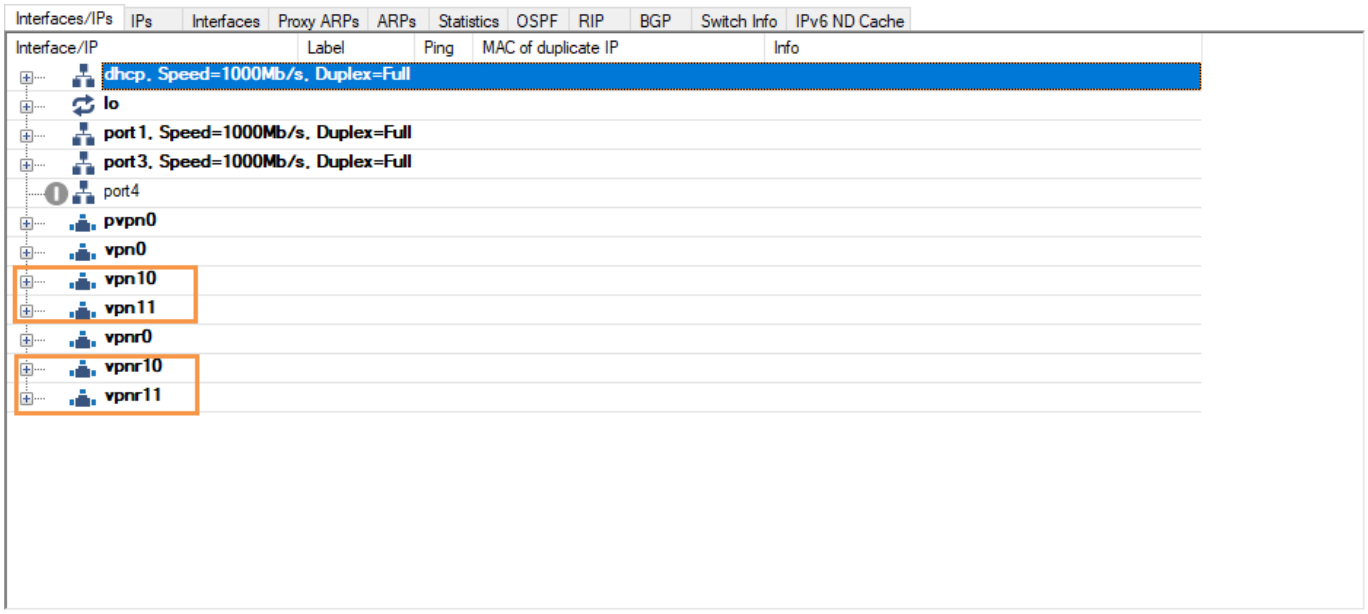
| | | |
|---|---|---|
| **Hash Meth.** | SHA<br>SHA256 | SHA<br>SHA256 |
| **DH-Group** | Group 2<br>Group 14<br>Group 15<br>Group 16<br>Group 17<br>Group 18 | Group 2<br>Group 5<br>Group 14<br>Group 15<br>Group 16<br>Group 17<br>Group 18 |
| **Lifetime(sec)** | 28800 | 3600 |
| **Perfect Forward Secrecy** | - | Enable |

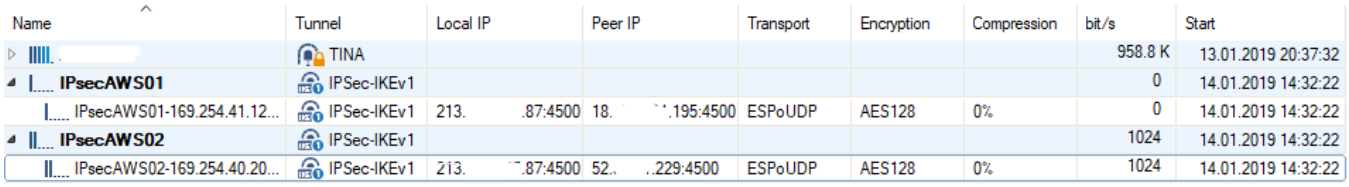
3. In the **Local Networks** tab:
   - **Local IKE Gateway** – Enter your external IP address. If you are using a dynamic WAN interface, or if the appliance is hosted in Azure, AWS or GCP, enter `0.0.0.0`
   - **Network Address** – Enter the **Inside IP Address** of the **Customer Gateway** (without the /30) and click **Add**. E.g., IPsec tunnel 1 `169.254.254.58` and for IPsec tunnel 2 `169.254.254.62`.
4. In the **Remote Networks** tab:
   - **Remote IKE Gateway** – Enter the **Outside IP Address** of the **Virtual Private Gateway**.
5. In the **Peer Identification** tab:
   - **Shared Secret** – Enter the Amazon **Pre-Shared Key**.
6. In the **Advanced** tab:
   - **DPD intervals (s)** – Enter `10`.
   - **Interface Index** – Enter the **VPN Next Hop Interface index** number you entered in step 1.1. E.g., IPsec tunnel 1 `10` and for IPsec tunnel 2 `11`.
   - **VPN Next Hop Routing** – Enter the **Inside IP address** of the **Virtual Private Gateway.** E.g., IPsec tunnel 1 `169.254.254.57` and for IPsec tunnel 2 `169.254.254.61`
   - (Optional) **Phase 2 Lifetime Adjust (sec)** – Enter `-1300`. This setting ensures that the firewall initiates rekeying.
     On CloudGen Firewall devices with firmware 8.0.1 or higher, you can leave this field blank.
7. Click **OK**.




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

You now have two VPN next-hop interfaces listed in the **Interfaces/IPs** section on the **CONTROL > Network** page and the VPN tunnels on the **VPN > STATUS** page.




## Step 3. Configure the BGP Service

Configure BGP routing to learn the subnets on the other side of the VPN tunnels. The BGP route propagated by the second (backup) IPsec tunnel is artificially elongated so traffic is routed per default over the first IP tunnel, as suggested by Amazon.

#### Step 3.1. Configure Routes to be Advertised via BGP

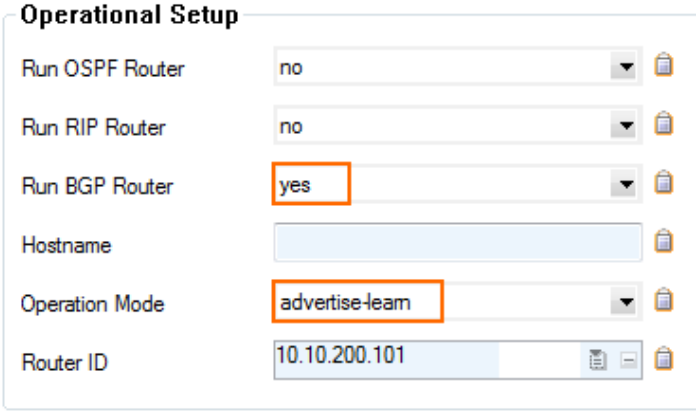
Only routes with the parameter **Advertise** set to **yes** will be propagated via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. (optional) To propagate the management network, set **Advertise Route** to **yes**.
4. In the left menu, click **Advanced Routing**.
5. Double-click on the **Routes** you want to propagate, and set **Advertise Route** to **yes**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

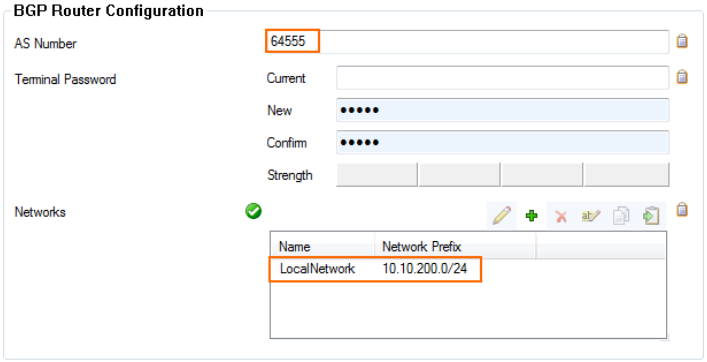
#### Step 3.2 - Configure the BGP Routes

Configure the BGP setting for the BGP service on the firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
2. Select **yes** from the **Run BGP Router** list.
3. Select **advertise-learn** from the **Operations Mode** list.




4. In the left menu, click **BGP Router Setup**.
5. Enter your **AS Number** (e.g., 64555).
6. In the **Networks** table, add the local network(s)(e.g., `10.10.200.0/24` ).




7. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
8. Click the **Set** button for the **Advanced Settings**. The **Advanced Settings** window opens.
9. Set the **Hold timer** to `30` seconds.
10. Set the **Keep Alive Timer** to `10` seconds.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

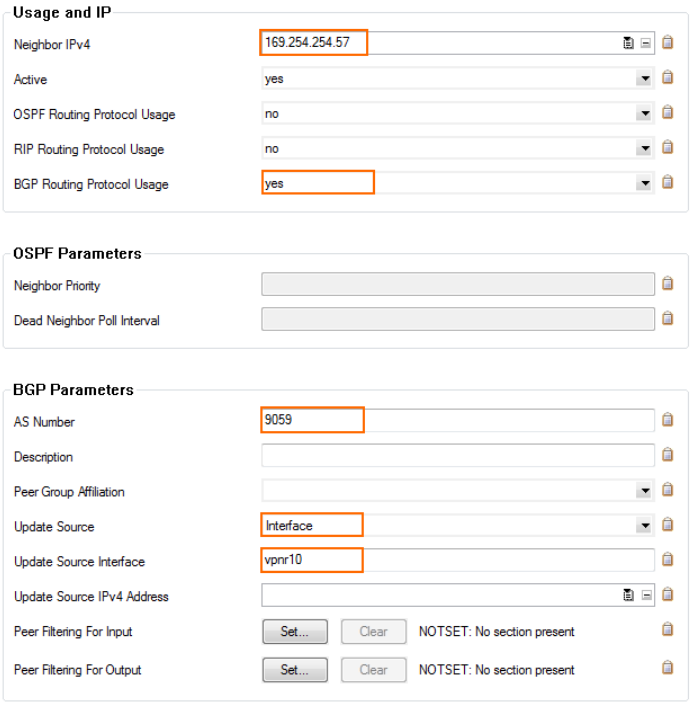
#### Step 3.3 - Add a BGP Neighbor for Each IPsec Tunnel

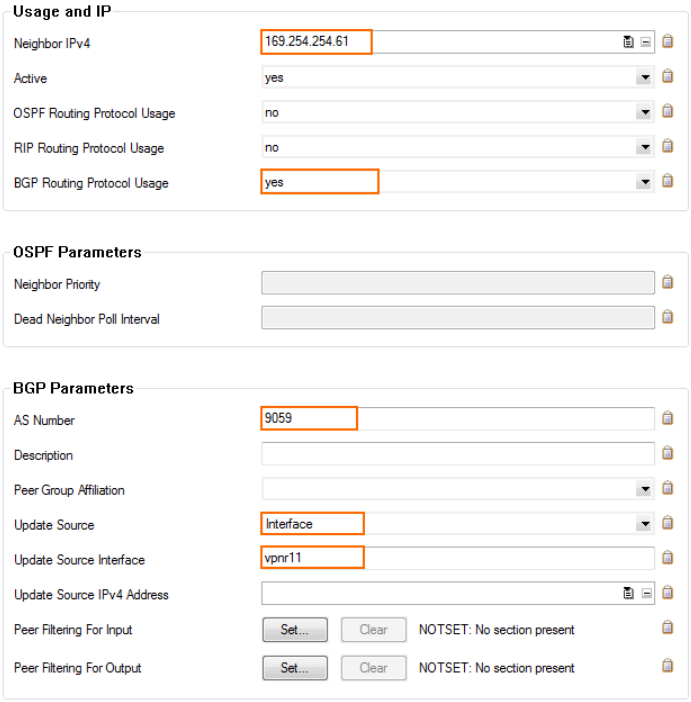
To dynamically learn the routing of the neighboring network, set up a BGP neighbor for each VPN next-hop interface.

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
2. Click **Lock**.
3. For each IPsec tunnel, click the plus sign (**+**) next to the **Neighbors** table to add a new

neighbor.

4. Enter a **Name** for the neighbor. E.g., AWS1 and AWS2
5. In the **Neighbors** window, configure the following settings in the **Usage and IP** section:
   - **Neighbor IPv4** – Enter the inside IP Address of the Virtual Private Gateway (remote address for the VPN next hop interface on the CloudGen Firewall)  E.g., IPsec Tunnel 1: 169.254.254.57 and for IPsec Tunnel 2 169.254.254.61.
   - **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: 9059
   - **Update Source**: Select **Interface**
   - **Update Source Interface**: Enter the vpnr interface for the IPsec tunnels. E.g., IPsec Tunnel 1: vpnr10 and for IPsec Tunnel 2 vpnr11.






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

#### Step 3.4 - Add an Access List for the Second IPsec Tunnel

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Filter Setup IPv4**.
2. In the **Access List IPv4 Filters** section, click **+**.
3. Enter a **Name** for the Access List. E.g., `2ndGWIP` The **Access List IPv4** windows opens.
4. Click **+** to add an access list **Type**. The **Type** window opens.
5. Select **permit** from the **Type** drop-down menu.
6. Enter the **Inside IP** for the **Virtual Private Gateway** for IPsec Tunnel #2. E.g., `169.254.254.62` to the **Network Prefix** field.
7. Click **OK**.
8. Click **OK**.

#### Step 3.5 - Add a Filter Setup for the Second IPsec Tunnel

To make the route over the first IPsec tunnel the preferred route, we will lengthen the AS-Path of the second tunnel.

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Filter Setup IPv4**.
2. Click **Lock**.
3. In the **Route Map IPv4 Filters** section, click **+**. The **Route Maps IPv4** window opens.
4. In the **BGP Specific Conditions** section, click **+**. The **Route Map Entry** window opens.
5. In the **Route Map Entry** window, specify the following settings:
   - **Sequence Number** – Enter a unique sequence number (e.g., 1). This sequence number must be unique across all route maps. For additional entries, iterate the sequence

numbers.
- **Type** – Select **permit**.
- **Match Condition** – Select **Gateway_IP**.
- **Gateway IP (Access List)** – Select the access list entry created in Step 3.4.
- **Set Action** – Select **AS_Path**.
- **Set addition to AS-Path** – Enter Amazons ASN number 9059.

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

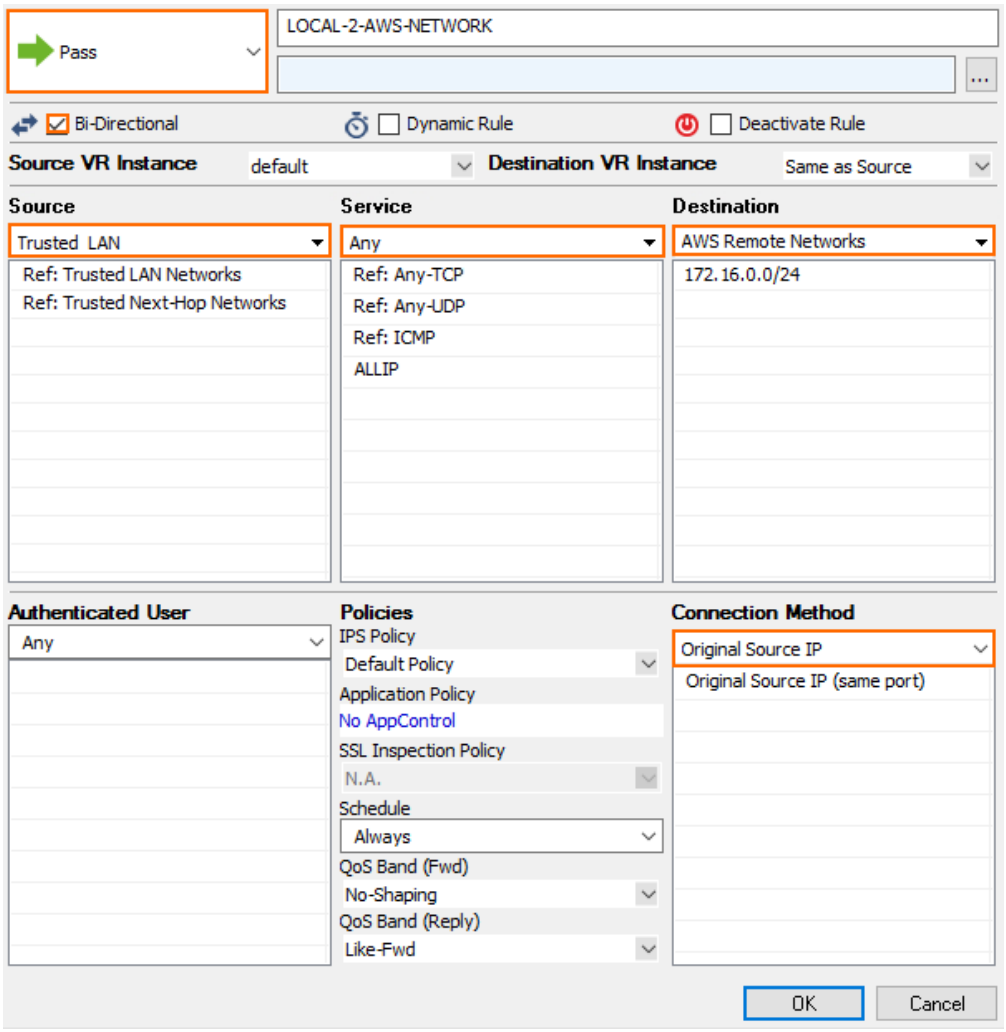
#### Step 3.6 - Bind the Filters to the Neighbors

1. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
2. Click **Lock**.
3. Edit the entries in the **Neighbors** table.
4. In the **Neighbors** window, click **Set/Edit** next to **Peer Filtering for Input**.
5. Select the **ACL Filter** and the **Route Map Filter** you previously created.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

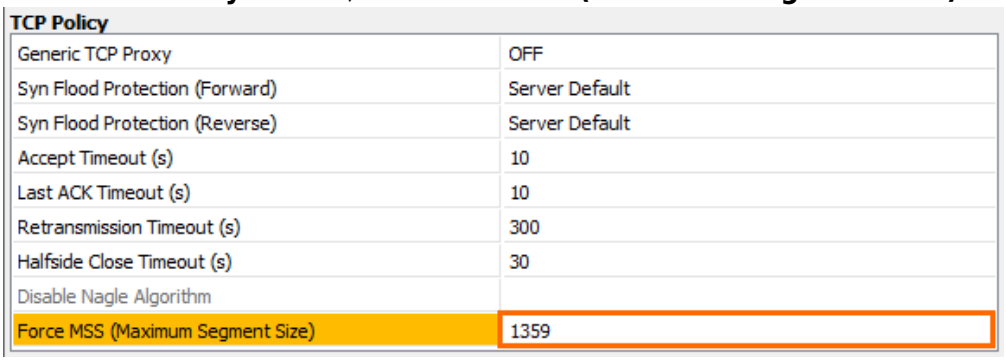
## Step 4. Create an Access Rule for VPN Traffic

To allow traffic to and from the VPN networks, a pass access rule is needed. You also need to set the **Clear DF bit** and **Force Maximum Segment Size** settings according to the Amazon configuration file in the advanced firewall rule settings. You also need to set **Reverse Interface (Bi-directional)** to **Any** to allow return traffic using a different VPN tunnel than was used to initiate the connection.

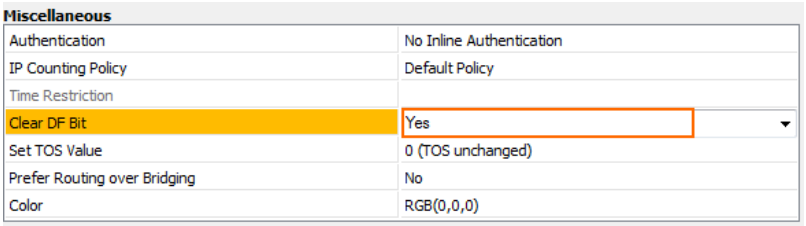
1. Create a Pass access rule:
   - **Bi-Directional** – Enable.
   - **Source** – Select the local network(s) you are propagating via BGP.
   - **Service** – Select the service you want to have access to the remote network or **ALL** for complete access.
   - **Destination** – Select the remote VPC subnet(s).
   - **Connection Method** – Select **Original Source IP**.




2. In the left navigation, click **Advanced.**
3. In the **TCP Policy** section, set **Force MSS (Maximum Segment Size)** to 1359.

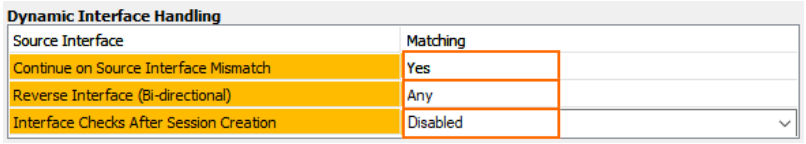



4. In the **Miscellaneous** section, set **Clear DF Bit** to **Yes**.




5. In the **Dynamic Interface Handling** section:
    1. Set **Continue on Source Interface Mismatch** to **Yes**.

2. Set **Reverse Interface (Bi-directional)** to **Any**.
3. Set **Interface Checks after Session Creation** to **Disabled**.




6. Click **OK**.
7. Move the access rule up in the rule list, so that it is the first rule to match the firewall traffic.
8. Click **Send Changes** and **Activate**.

You now have two IPsec VPN tunnels connecting your CloudGen Firewalls to the Amazon AWS cloud. Per default, the first IPsec tunnel is chosen. It may take some time for BGP to learn the new routes, in case of a failure.

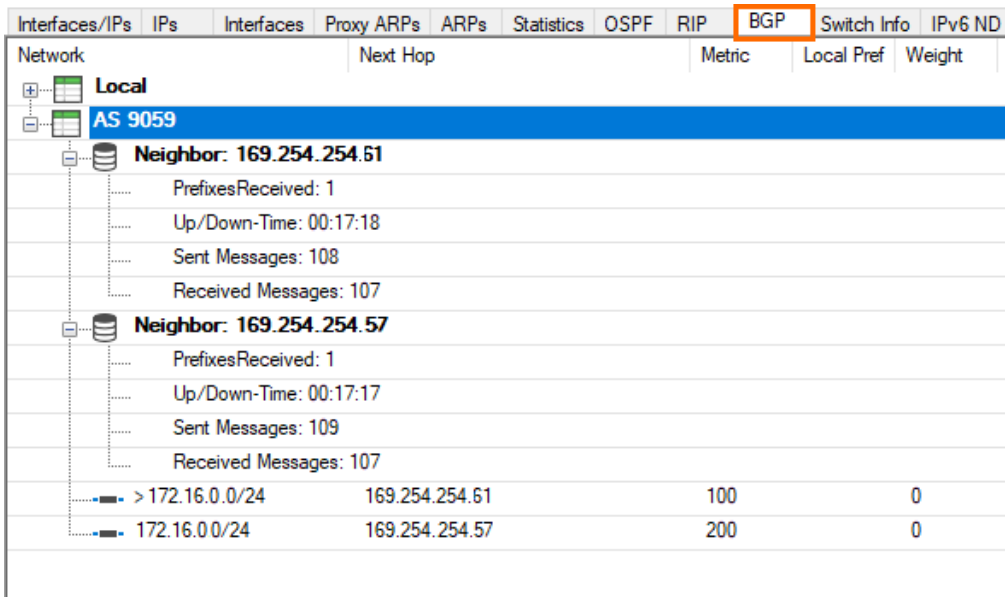
If the TCP 179 connection is established via loopback IP, check which interface is used by the VPN IP.

### IPsec Tunnels are Connected (VPN > Status)



| Tunnel | Name | Type | Group | Info | State | Succ. | Fail | Last Access | Last Peer | Last Info |
|---|---|---|---|---|---|---|---|---|---|---|
| IPSEC | IPsecAWSTunnel1-169.254.254.57-169.25... | | | | ACTIVE | 1 | 1 | 4m 31s | 87.238.85.42 | Access Granted |
| IPSEC | IPsecAWSTunnel2-169.254.254.61-169.25... | | | | ACTIVE | 1 | 1 | 4m 31s | 87.238.85.46 | Access Granted |

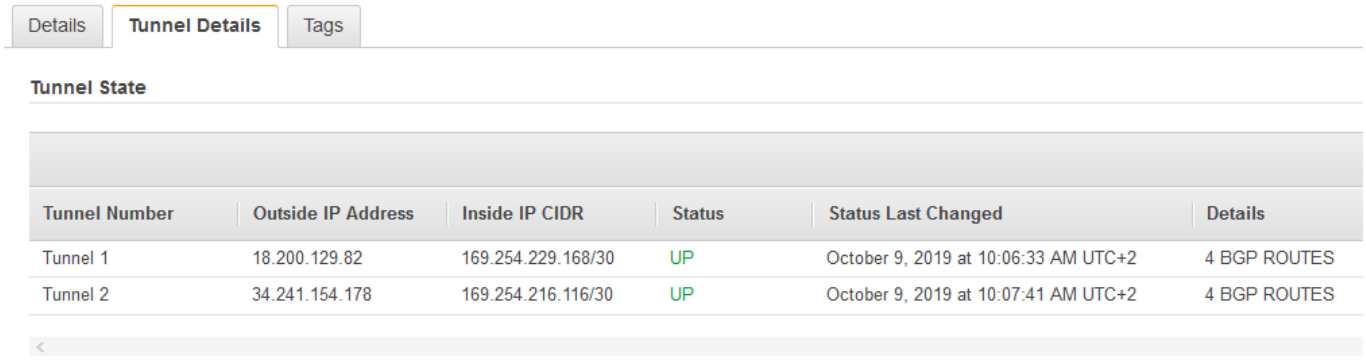
### BGP Configuration (CONTROL > NETWORK > BGP)




### AWS VPN Status in the Amazon AWS Management Interface

It may take some time until the tunnel is displayed as up in AWS.

1. Go to the Amazon VPC Management Console.
2. In the left menu, click **Site-to-Site VPN Connections**.
3. Search for your connection created in Step 1.
4. Click **Tunnel Details**.



## Figures

1. amazon_vpn_gw.png
2. IPsecAWS01.png
3. aws_create_customer_gw.png
4. IPsecAWS04.png
5. IPsecAWS05.png
6. route_propagation.png
7. edit_rp.png
8. save.png
9. vpn_settings_set_next_hop_interface.png
10. enable_UseIPSecdynamicIPs.png
11. next_hopVPN01.png
12. IPsecTunnel1_sdwan.png
13. IPsecTunnel2_sdwan.png
14. next_hopVPN01.png
15. IPsecTunnel03.png
16. BGP00.png
17. BGP01.png
18. BGP02.png
19. BGP03.png
20. FW01.png
21. forcemss.png
22. FW02.png
23. FW04.png
24. finished01.png
25. bgp_status.png
26. aws_tunnel_details.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.