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

If you are using the Amazon Virtual Private Cloud, you can transparently extend your local network to the cloud by connecting both networks with a site-to-site IPsec VPN tunnel. The Amazon virtual private gateway uses two parallel 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.

In this article:

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.
How to Configure an IPsec VPN to an AWS VPN Gateway with BGP

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., Techlib Virtual Private Gateway).
5. Click Yes, Create.
6. Select the newly created virtual private gateway, and click 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 NG 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 Gateway.
3. Click Create Customer Gateway.
4. Enter the connection information for your Barracuda Firewall:
   - Name Tag – Enter a name for your device (e.g., My Barracuda NG Firewall).
   - Routing – Select Dynamic.
   - IP Address – Enter your external IP Address. To look up your external IP address, go to CONTROL > Network.

5. Click Yes, Create.

How to Configure an IPsec VPN to an AWS VPN Gateway with BGP
2 / 17
Your Barracuda NG Firewall is now configured in the AWS cloud and can be used to configure VPN connections.

**Step 1.3. Create a VPN Connection**

Create a VPN connection with the customer gateway and the virtual private gateway that you just created. Then download the VPN configuration file, because it contains all the necessary information for configuring the VPN connection on the Barracuda NG Firewall.

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

1. Go to the [Amazon VPC Management Console](https://aws.amazon.com/vpc/).
2. In the left menu, click **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., NG2AWSCloud).
   - **Virtual Private Gateway** – Select the virtual private gateway created in Step 1.
   - **Routing Options** – Select Dynamic (requires BGP).

5. Click **Yes, Create**.
6. 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 Yes, Download, and save the vpn-.txt file.

Click here to see an example Amazon VPN configuration file
Amazon Web Services Virtual Private Cloud VPN Connection Configuration

AWS utilizes unique identifiers to manipulate the configuration of a VPN Connection. Each VPN Connection is assigned a VPN Connection Identifier and is associated with two other identifiers, namely the Customer Gateway Identifier and the Virtual Private Gateway Identifier. Your VPN Connection ID: vpn-YOUR-VPN-CONNECTION-ID Your Virtual Private Gateway ID: vgw-YOUR-VIRTUAL-PRIVATE-GATEWAY-ID Your Customer Gateway ID: cgw-YOUR-CUSTOMER-GATEWAY-ID A VPN Connection consists of a pair of IPSec tunnel security associations (SAs). It is important that both tunnel security associations be configured. IPSec Tunnel #1

#1: Internet Key Exchange Configuration Configure the IKE SA as follows:
  Authentication Method: Pre-Shared Key - Pre-Shared Key: YOUR-PRESHARED-KEY -
  Authentication Algorithm: sha1 - Encryption Algorithm: aes-128-cbc - Lifetime: 28800 seconds - Phase 1 Negotiation Mode: main - Perfect Forward Secrecy: Diffie-Hellman Group 2 #2: IPSec Configuration Configure the IPSec SA as follows:
  - Protocol: esp - Authentication Algorithm: hmac-sha1-96 -
  - Encryption Algorithm: aes-128-cbc - Lifetime: 3600 seconds - Mode: tunnel -
  - Perfect Forward Secrecy: Diffie-Hellman Group 2 IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your endpoint as follows:
    - DPD Interval: 10 - DPD Retries: 3 IPSec ESP (Encapsulating Security Payload) inserts additional headers to transmit packets. These headers require additional space, which reduces the amount of space available to transmit application data. To limit the impact of this behavior, we recommend the following configuration on your Customer Gateway:
      - TCP MSS Adjustment: 1387 bytes - Clear Don't Fragment Bit: enabled -
      - Fragmentation: Before encryption #3: Tunnel Interface Configuration Your Customer Gateway must be configured with a tunnel interface that is associated with the IPSec tunnel. All traffic transmitted to the tunnel interface is encrypted and transmitted to the Virtual Private Gateway. The Customer Gateway and Virtual Private Gateway each have two addresses that relate to this IPSec tunnel. Each contains an outside address, upon which encrypted traffic is exchanged. Each also contain an inside address associated with the tunnel interface. The Customer Gateway outside IP address was provided when the Customer Gateway was created. Changing the IP address requires the creation of
Barracuda NextGen Firewall F

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

5 / 17

Step 2. Configure IPsec Tunnels on the Barracuda NG 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.

Click here to see the relevant part of an example Amazon VPN configuration file

[...]
IPSec Tunnel #1
================================================================================
[...]
#3: Tunnel Interface Configuration
[...]
Inside IP Addresses
- Customer Gateway : 169.254.254.58/30
- Virtual Private Gateway : 169.254.254.57/30
Configure your tunnel to fragment at the optimal size:
- Tunnel interface MTU : 1436 bytes
[...]
IPSec Tunnel #2
================================================================================
[...]
#3: Tunnel Interface Configuration
[...]
Inside IP Addresses
- Customer Gateway : 169.254.254.62/30
- Virtual Private Gateway : 169.254.254.61/30
Configure your tunnel to fragment at the optimal size:
- Tunnel interface MTU : 1436 bytes
[...]

1. Go to CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings.
2. Click Lock.
3. Click on Click here for Server Settings.
4. Click on the Advanced tab.
5. Create a VPN next hop interface for each IPsec tunnel by clicking Add in the VPN Next Hop Interface Configuration n 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 for 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.

6. Click OK.

7. 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.

Click here to see the relevant part of an example Amazon VPN configuration file

Amazon Web Services
Virtual Private Cloud
[...]

IPSec Tunnel #1
==================================================================================================
#1: Internet Key Exchange Configuration

How to Configure an IPsec VPN to an AWS VPN Gateway with BGP
6 / 17
Configure the IKE SA as follows:
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: YOUR-PRESHARED-KEY
- Authentication Algorithm: sha1
- Encryption Algorithm: aes-128-cbc
- Lifetime: 28800 seconds
- Phase 1 Negotiation Mode: main
- Perfect Forward Secrecy: Diffie-Hellman Group 2

#2: IPSec Configuration
Configure the IPSec SA as follows:
- Protocol: esp
- Authentication Algorithm: hmac-sha1-96
- Encryption Algorithm: aes-128-cbc
- Lifetime: 3600 seconds
- Mode: tunnel
- Perfect Forward Secrecy: Diffie-Hellman Group 2

IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your endpoint as follows:
- DPD Interval: 10

#3: Tunnel Interface Configuration
Outside IP Addresses:
- Customer Gateway: YOUR-EXTERNAL-IP-ADDRESS
- Virtual Private Gateway: AMAZON-VPN-GATEWAY-IP-ADDRESS-TUNNEL-2

Configure your tunnel to fragment at the optimal size:
- Tunnel interface MTU: 1436 bytes

IPSec Tunnel #2

#1: Internet Key Exchange Configuration
Configure the IKE SA as follows:
- Authentication Method: Pre-Shared Key
- Pre-Shared Key: YOUR-PRESHARED-KEY
- Authentication Algorithm: sha1
- Encryption Algorithm: aes-128-cbc
- Lifetime: 28800 seconds
- Phase 1 Negotiation Mode: main
- Perfect Forward Secrecy: Diffie-Hellman Group 2

#2: IPSec Configuration
Configure the IPSec SA as follows:
- Protocol: esp
- Authentication Algorithm: hmac-sha1-96
- Encryption Algorithm: aes-128-cbc
- Lifetime: 3600 seconds
- Mode: tunnel
- Perfect Forward Secrecy: Diffie-Hellman Group 2
IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We recommend configuring DPD on your endpoint as follows:
- DPD Interval : 10

#3: Tunnel Interface Configuration

Outside IP Addresses:
- Customer Gateway : YOUR-EXTERNAL-IP-ADDRESS
- Virtual Private Gateway : AMAZON-VPN-GATEWAY-IP-ADDRESS-TUNNEL-2

Configure your tunnel to fragment at the optimal size:
- Tunnel interface MTU : 1436 bytes

1. Go to CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Site to Site.
2. Click on the IPSEC Tunnels tab.
3. Click Lock.
4. For each IPsec tunnel right click and click New IPSec 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:
         - Encryption: AES
         - Hash Meth.: SHA
         - DH-Group: Group2
         - Lifetime(sec): 28800
         - 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 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.
      - Network Address – Enter the Inside IP Address of the Virtual Private Gateway (without the /30) and click Add. E.g., IPsec tunnel 1 169.254.254.57 and for IPsec tunnel 2 169.254.254.61.
   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
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 **CONTROL > VPN > STATUS**.
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.

Click here to see the relevant part of an example Amazon VPN configuration file

```plaintext
[...] IPSec Tunnel #1
IPHockey Tunnel Management Server Authentication Configuration:
#4: Border Gateway Protocol (BGP) Configuration: [...] BGP Configuration Options: - Customer Gateway ASN : YOUR-ASN-NUMBER (e.g., 64555) - Virtual Private Gateway ASN : 9059 - Neighbor IP Address : 169.254.254.57 - Neighbor Hold Time : 30
[...] IPSec Tunnel #2

```

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 on **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 Barracuda NG Firewall.
1. Go to CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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.

Operational Setup

| Run OSPF Router | no |
| Run RIP Router  | no |
| Run BGP Router  | yes |
| Hostname        |    |
| Operation Mode  | advertise-learn |
| Router ID       | 10.10.200.101 |

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

BGP Router Configuration

| AS Number | 64555 |
| Terminal Password | Current |
|              | New |
|                | Confirm |
|                | Strength |

Networks

<table>
<thead>
<tr>
<th>Name</th>
<th>Network Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalNetwork</td>
<td>10.10.200.0/24</td>
</tr>
</tbody>
</table>

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

1. In the **Usage and IP** section, configure the following settings:
   - **Neighbor IPv4**: Enter the IP address for the remote endpoint: 169.254.254.57
   - **Active**: Select **yes**
   - **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 Autonomous System Number for the remote network: 9059
   - **Update Source**: Select **Interface.vpnr**
   - **Update Source Interface**: Enter the vpnr interface for the IPsec tunnels. E.g., IPsec Tunnel 1: vpnr10 and for IPsec Tunnel 2 vpnr11.

   - **OSPF Parameters**
     - **Neighbor Priority**: Enter the priority for the neighbor
     - **Dead Neighbor Poll Interval**: Enter the interval for dead neighbor detection

   - **BGP Parameters**
     - **AS Number**: Enter the Autonomous System Number: 9059
     - **Description**: Enter a description for the BGP peer
     - **Peer Group Affiliation**: Enter the peer group affiliation
     - **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.
     - **Peer Filtering For Input**: Select **Set**
     - **Peer Filtering For Output**: Select **Set**

The VPN next hop interface on the NG Firewall: E.g., IPsec Tunnel 1: 169.254.254.57 and for IPsec Tunnel 2 169.254.254.61.
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** dropdown.
6. Enter the **Inside IP** for the **Virtual Private Gateway** for IPsec Tunnel #2. E.g., 169.254.254.62
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 on +. 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 for the listed created in Step 3.4.
   - Set Action – Select AS_Path.
   - Set addition to AS-Path – Enter Amazon’s ASN number 9059.
6. Click OK.
7. Click OK.
8. Click Send Changes and Activate.

**Step 4. Create a 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 then was used to initiate the connection.

Click here to see the relevant part of an example Amazon VPN configuration file

[...] IPSec ESP (Encapsulating Security Payload) inserts additional headers to transmit packets. These headers require additional space, which reduces the amount of space available to transmit application data. To limit the impact of this behavior, we recommend the following configuration on your Customer Gateway:

- TCP MSS Adjustment : 1387 bytes - Clear Don't Fragment Bit : enabled [...] 

1. Create a Pass firewall 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 No Src NAT.
2. In the left navigation, click on **Advanced**.

3. In the **TCP Policy** section set **Force MSS (Maximum Segment Size)** to 1387.

4. In the **Miscellaneous** section set **Clear DF Bit to Yes**.
5. In the **Dynamic Interface Handling** section set **Reverse Interface (Bi-directional)** to **Any**.

![Dynamic Interface Handling](image)

6. Click **OK**.
7. Move the firewall 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 Barracuda NG 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.

**IPsec Tunnels are connected**

![IPsec Tunnels](image)

**BGP Configuration (CONTROL > NETWORK > BGP)**

![BGP Configuration](image)

**AWS VPN status in the Amazon AWS management interface**

![AWS VPN Status](image)