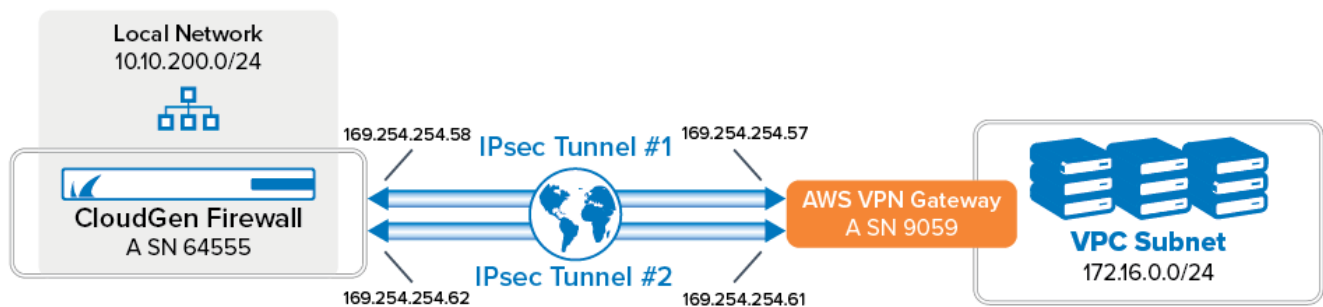


How to Configure an IKEv1 IPsec VPN to an AWS VPN Gateway with BGP

<https://campus.barracuda.com/doc/96026149/>

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**.

[Customer Gateways](#) > Create Customer Gateway

Create Customer Gateway

Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

Name ⓘ

Routing
☒ **Dynamic**
☐ Static

BGP ASN* ⓘ

IP Address ⓘ

Certificate ARN ⓘ

* Required

[Cancel](#) [Create Customer Gateway](#)

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.

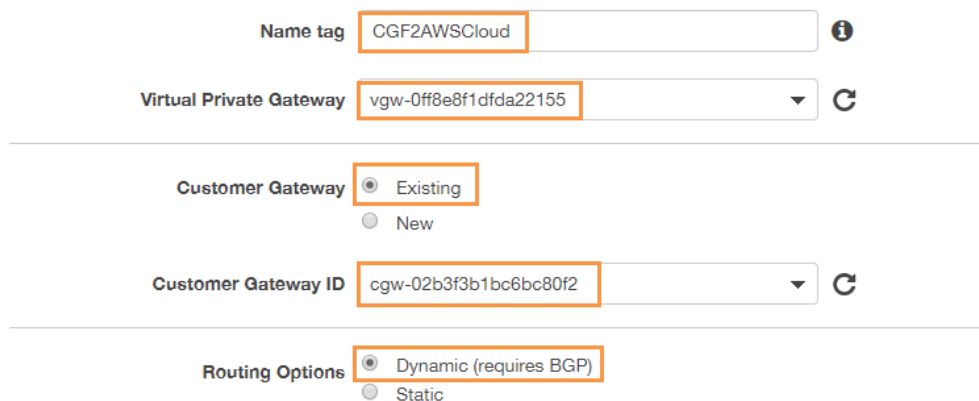
The Amazon VPN configuration file is different for every VPN connection.

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)**.

[VPN Connections](#) > Create VPN Connection

Create VPN Connection

Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.



Name tag CGF2AWSCloud ⓘ

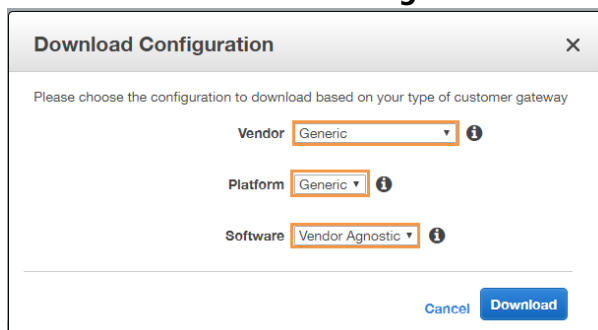
Virtual Private Gateway vgw-0ff8e8f1dfda22155 ↕ ↻

Customer Gateway ☒ Existing ☐ New

Customer Gateway ID cgw-02b3f3b1bc6bc80f2 ↕ ↻

Routing Options ☒ Dynamic (requires BGP) ☐ Static

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**.



Download Configuration ✕

Please choose the configuration to download based on your type of customer gateway

Vendor Generic ⓘ

Platform Generic ⓘ

Software Vendor Agnostic ⓘ

Cancel Download

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**.

Create route table Actions ▾

search : campus-gw Add filter

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge
<input type="checkbox"/>	Campus-GW2-Route	rtb-05cd3c9f8fb4c34e1	-	-

Route Table: rtb-05cd3c9f8fb4c34e1

Summary Routes Subnet Associations Edge Associations **Route Propagation** Tags

Route Table ID rtb-05cd3c9f8fb4c34e1
Explicitly Associated with -
Owner 870076069282

5. Click **Edit Route Propagation**.

Summary Routes Subnet Associations Edge Associations **Route Propagation** Tags

Edit route propagation

Virtual Private Gateway	Propagate
vgw-0ef9cbb41cea6fdab Campus Virtual Private Gateway	No

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

[Route Tables](#) > Edit route propagation

Edit route propagation

Route table rtb-05cd3c9f8fb4c34e1

Route propagation	Virtual Private Gateway	Propagate
	vgw-0ef9cbb41cea6fdab Campus Virtual Private Gateway	<input checked="" type="checkbox"/>

* Required

Cancel **Save**

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**.

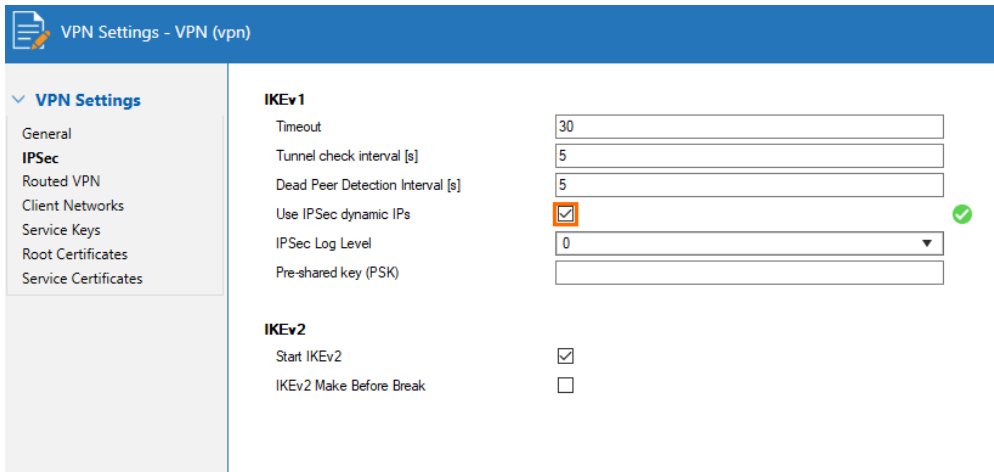
Interface Configuration

VPN I...	MTU	IPs	Multicast	
				<input type="button" value="Add"/>
				<input type="button" value="Edit"/>
				<input type="button" value="Delete"/>

Next Hop Interface Configuration

VPN I...	MTU	IPs	Multicast	
				<input type="button" value="Add"/>
				<input type="button" value="Edit"/>
				<input type="button" value="Delete"/>

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.



VPN Settings - VPN (vpn)

VPN Settings

- General
- IPSec**
- Routed VPN
- Client Networks
- Service Keys
- Root Certificates
- Service Certificates

IKEv1

Timeout: 30

Tunnel check interval [s]: 5

Dead Peer Detection Interval [s]: 5

Use IPsec dynamic IPs: ☒

IPsec Log Level: 0

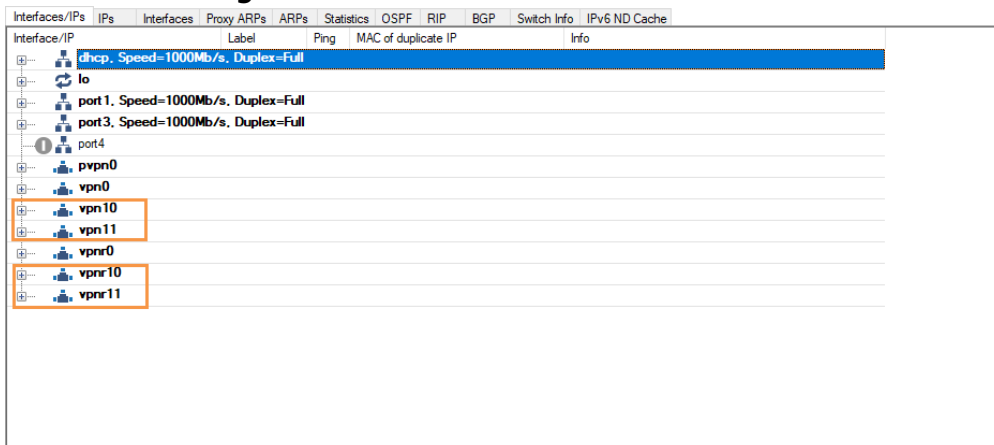
Pre-shared key (PSK):

IKEv2

Start IKEv2: ☒

IKEv2 Make Before Break: ☐

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



Interfaces/IPs | IPs | Interfaces | Proxy ARPs | ARP's | Statistics | OSPF | RIP | BGP | Switch Info | IPv6 ND Cache

Interface/IP	Label	Ping	MAC of duplicate IP	Info
dhcp, Speed=1000Mb/s, Duplex=Full				
lo				
port 1, Speed=1000Mb/s, Duplex=Full				
port 3, Speed=1000Mb/s, Duplex=Full				
port 4				
pvpn0				
vpn0				
vpn10				
vpn11				
vpnr0				
vpnr10				
vpnr11				

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

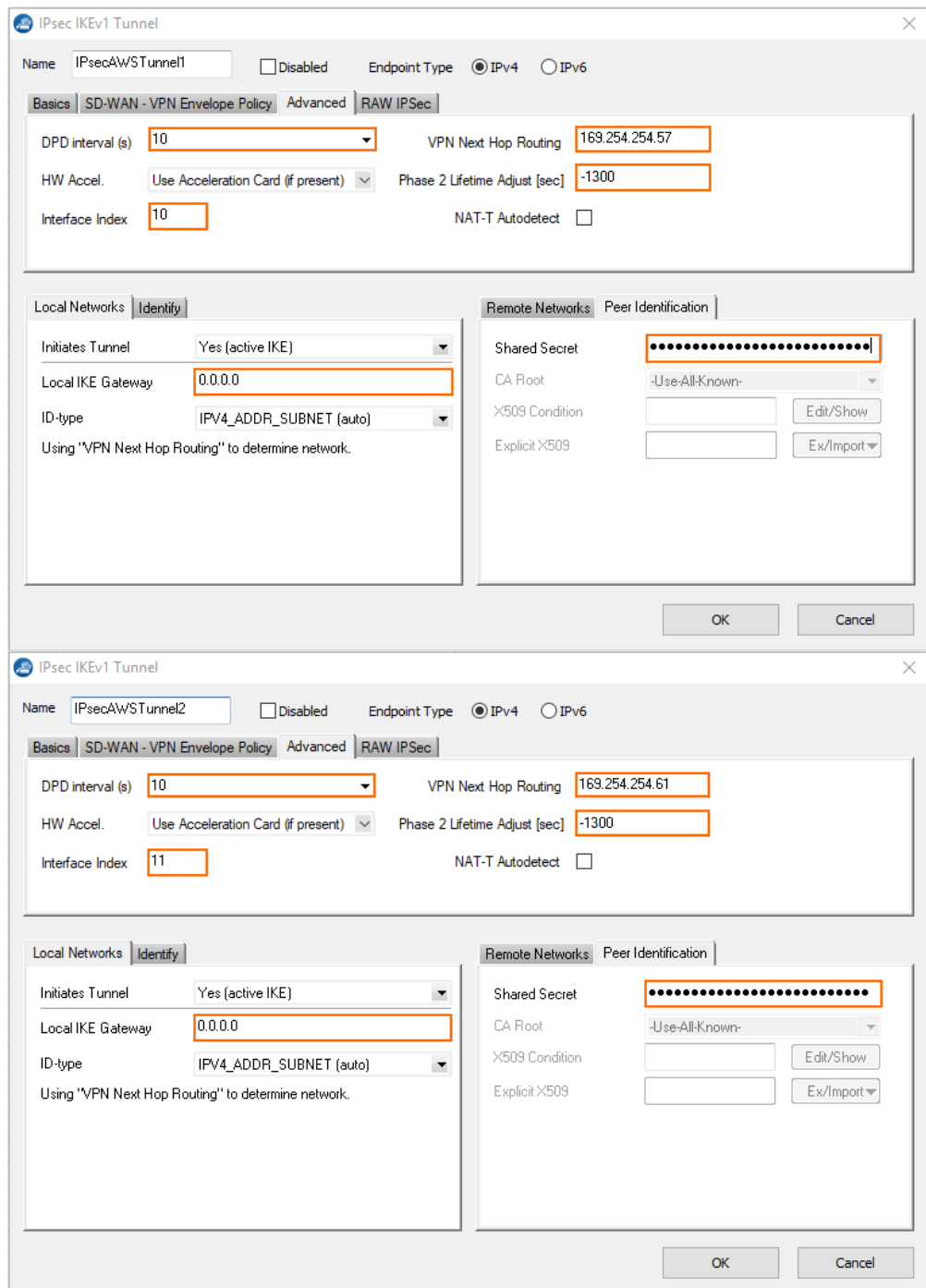
Configure two site-to-site IPsec tunnels using the VPN next-hop interfaces. Make sure to use the correct IP addresses and corresponding next-hop interfaces listed in the Amazon generic VPN configuration file for each tunnel.

- Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site**.
- Click on the **IPSEC IKEv1 Tunnels** tab.
- Click **Lock**.
- For each IPsec tunnel, right-click and click **New IPsec IKEv1 tunnel**.
 - Enter the IPsec tunnel configurations:
 - Enter a **Name**. E.g, IPsec Tunnel 1: IPsecAWSTunnel1 and for IPsec Tunnel 2: IPsecAWSTunnel2
 - 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 AES 256	AES AES 256

Hash Meth.	SHA SHA256	SHA SHA256
DH-Group	Group 2 Group 14 Group 15 Group 16 Group 17 Group 18	Group 2 Group 5 Group 14 Group 15 Group 16 Group 17 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**.



IPsec IKEv1 Tunnel

Name: IPsecAwSTunnel1 ☐ Disabled Endpoint Type: ☒ IPv4 ☐ IPv6

Basics | SD-WAN - VPN Envelope Policy | Advanced | RAW IPsec

DPD interval (s): 10 VPN Next Hop Routing: 169.254.254.57

HW Accel.: Use Acceleration Card (if present) Phase 2 Lifetime Adjust [sec]: -1300

Interface Index: 10 NAT-T Autodetect: ☐

Local Networks | Identify

Initiates Tunnel: Yes (active IKE)

Local IKE Gateway: 0.0.0.0

ID-type: IPv4_ADDR_SUBNET (auto)

Using "VPN Next Hop Routing" to determine network.

Remote Networks | Peer Identification

Shared Secret: [Masked]

CA Root: -Use-All-Known-

X509 Condition: [Empty] Edit/Show

Explicit X509: [Empty] Ex/Import

OK Cancel

IPsec IKEv1 Tunnel

Name: IPsecAwSTunnel2 ☐ Disabled Endpoint Type: ☒ IPv4 ☐ IPv6

Basics | SD-WAN - VPN Envelope Policy | Advanced | RAW IPsec

DPD interval (s): 10 VPN Next Hop Routing: 169.254.254.61

HW Accel.: Use Acceleration Card (if present) Phase 2 Lifetime Adjust [sec]: -1300

Interface Index: 11 NAT-T Autodetect: ☐

Local Networks | Identify

Initiates Tunnel: Yes (active IKE)

Local IKE Gateway: 0.0.0.0

ID-type: IPv4_ADDR_SUBNET (auto)

Using "VPN Next Hop Routing" to determine network.

Remote Networks | Peer Identification

Shared Secret: [Masked]

CA Root: -Use-All-Known-













X509 Condition: [Empty] Edit/Show







Explicit X509: [Empty] Ex/Import

OK Cancel

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.

Interfaces/IPs				IPs	Interfaces	Proxy ARPs	ARPs	Statistics	OSPF	RIP	BGP	Switch Info	IPv6 ND Cache
Interface/IP	Label	Ping	MAC of duplicate IP	Info									
 dhcp	Speed=1000Mb/s, Duplex=Full												
 lo													
 port1	Speed=1000Mb/s, Duplex=Full												
 port3	Speed=1000Mb/s, Duplex=Full												
 port4													
 pvpn0													
 vpn0													
 vpn10													
 vpn11													
 vpnr0													
 vpnr10													
 vpnr11													

Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start		
 TINA							958.8 K	13.01.2019 20:37:32		
 IPsecAWS01	 IPSec-IKEv1						0	14.01.2019 14:32:22		
IPsecAWS01-169.254.41.12...	 IPSec-IKEv1	213.	.87:4500	18.	.195:4500	ESPoUDP	AES128	0%	0	14.01.2019 14:32:22
 IPsecAWS02	 IPSec-IKEv1						1024	14.01.2019 14:32:22		
IPsecAWS02-169.254.40.20...	 IPSec-IKEv1	213.	.87:4500	52.	.229:4500	ESPoUDP	AES128	0%	1024	14.01.2019 14:32:22

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.

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 your **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 border="1"> <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>	Name	Network Prefix	LocalNetwork	10.10.200.0/24
Name	Network Prefix				
LocalNetwork	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**.

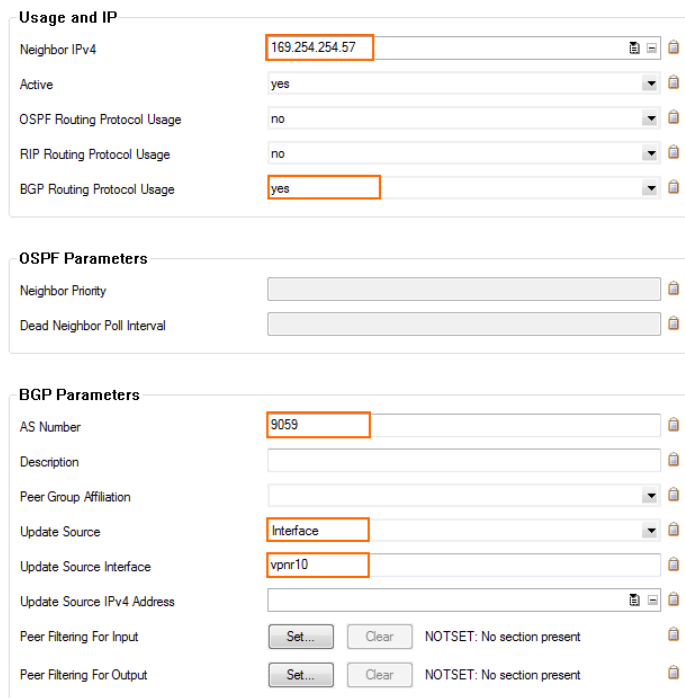
Step 3.3 - Add a BGP Neighbor for Each IPsec Tunnel

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.



The screenshot displays the configuration interface for a neighbor in the Barracuda CloudGen Firewall. It is divided into three main sections: 'Usage and IP', 'OSPF Parameters', and 'BGP Parameters'.

Usage and IP

Neighbor IPv4	169.254.254.57	[Icon]
Active	yes	[Icon]
OSPF Routing Protocol Usage	no	[Icon]
RIP Routing Protocol Usage	no	[Icon]
BGP Routing Protocol Usage	yes	[Icon]

OSPF Parameters

Neighbor Priority	[Text Field]	[Icon]
Dead Neighbor Poll Interval	[Text Field]	[Icon]

BGP Parameters

AS Number	9059	[Icon]
Description	[Text Field]	[Icon]
Peer Group Affiliation	[Dropdown]	[Icon]
Update Source	Interface	[Icon]
Update Source Interface	vpnr10	[Icon]
Update Source IPv4 Address	[Text Field]	[Icon]
Peer Filtering For Input	[Set...] [Clear] NOTSET: No section present	[Icon]
Peer Filtering For Output	[Set...] [Clear] NOTSET: No section present	[Icon]

Usage and IP	
Neighbor IPv4	169.254.254.61
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	9059
Description	
Peer Group Affiliation	
Update Source	Interface
Update Source Interface	vpn11
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 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** window 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**.

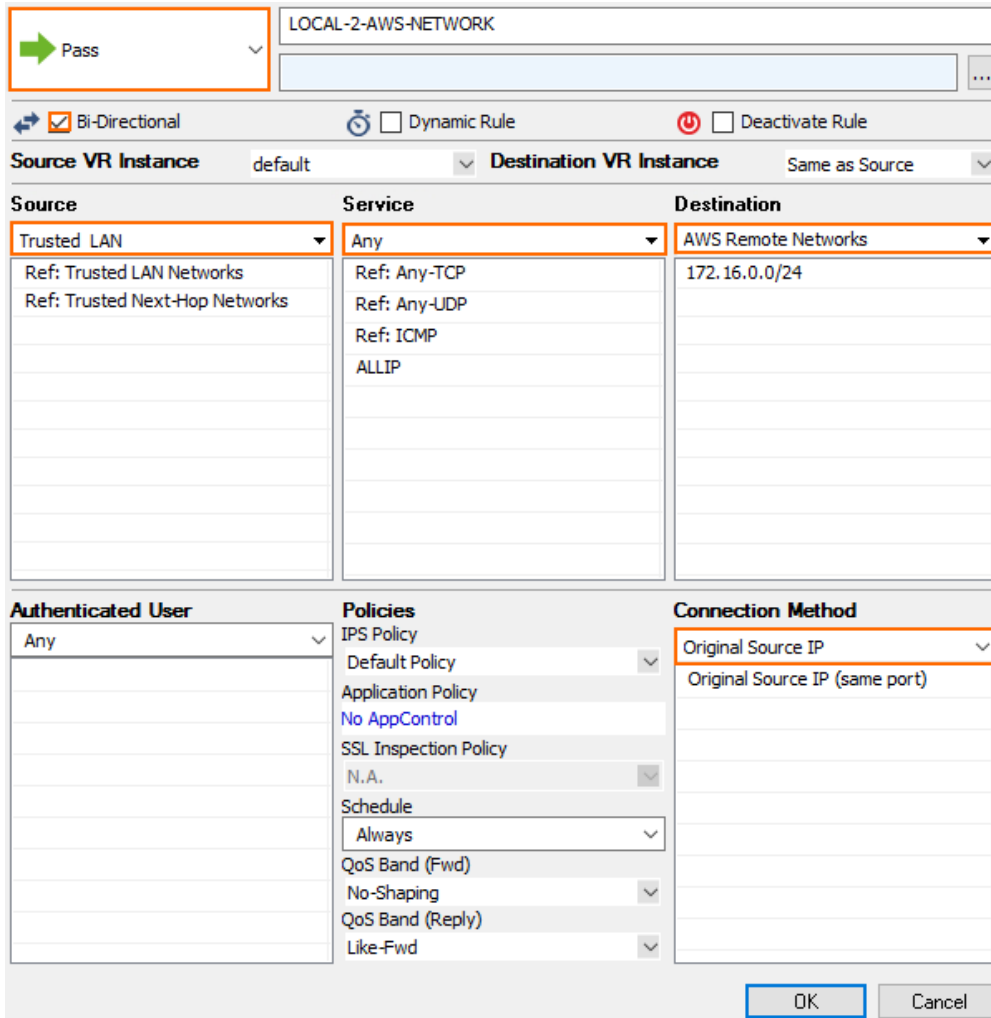
Step 3.6 - Bind the Filters to the Neighbors

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**.



Pass

LOCAL-2-AWS-NETWORK

Bi-Directional Dynamic Rule Deactivate Rule

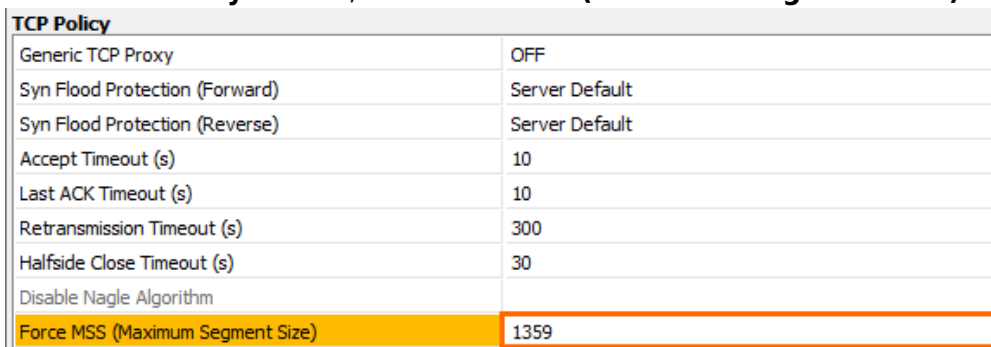
Source VR Instance default Destination VR Instance Same as Source

Source	Service	Destination
Trusted LAN	Any	AWS Remote Networks
Ref: Trusted LAN Networks	Ref: Any-TCP	172.16.0.0/24
Ref: Trusted Next-Hop Networks	Ref: Any-UDP	
	Ref: ICMP	
	ALLIP	

Authenticated User	Policies	Connection Method
Any	IPS Policy	Original Source IP
	Default Policy	Original Source IP (same port)
	Application Policy	
	No AppControl	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	No-Shaping	
	QoS Band (Reply)	
	Like-Fwd	

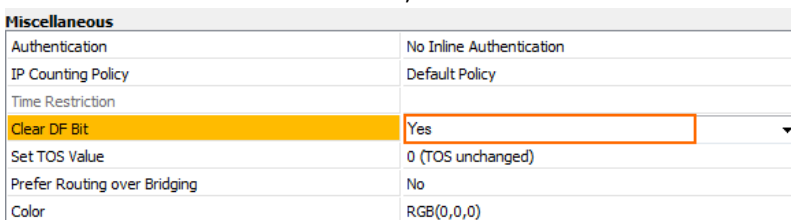
OK Cancel

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



TCP Policy	
Generic TCP Proxy	OFF
Syn Flood Protection (Forward)	Server Default
Syn Flood Protection (Reverse)	Server Default
Accept Timeout (s)	10
Last ACK Timeout (s)	10
Retransmission Timeout (s)	300
Halfside Close Timeout (s)	30
Disable Nagle Algorithm	
Force MSS (Maximum Segment Size)	1359

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



Miscellaneous	
Authentication	No Inline Authentication
IP Counting Policy	Default Policy
Time Restriction	
Clear DF Bit	Yes
Set TOS Value	0 (TOS unchanged)
Prefer Routing over Bridging	No
Color	RGB(0,0,0)

- In the **Dynamic Interface Handling** section:
 - 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**.



Dynamic Interface Handling	
Source Interface	Matching
Continue on Source Interface Mismatch	Yes
Reverse Interface (Bi-directional)	Any
Interface Checks After Session Creation	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)

Interfaces/IPs	IPs	Interfaces	Proxy ARPs	ARPs	Statistics	OSPF	RIP	BGP	Switch Info	IPv6 ND
Network										
Local										
AS 9059										
Neighbor: 169.254.254.61										
PrefixesReceived: 1										
Up/Down-Time: 00:17:18										
Sent Messages: 108										
Received Messages: 107										
Neighbor: 169.254.254.57										
PrefixesReceived: 1										
Up/Down-Time: 00:17:17										
Sent Messages: 109										
Received Messages: 107										
> 172.16.0.0/24										
169.254.254.61										
100										
0										
172.16.0.0/24										
169.254.254.57										
200										
0										

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**.

Details

Tunnel Details

Tags

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details
Tunnel 1	18.200.129.82	169.254.229.168/30	UP	October 9, 2019 at 10:06:33 AM UTC+2	4 BGP ROUTES
Tunnel 2	34.241.154.178	169.254.216.116/30	UP	October 9, 2019 at 10:07:41 AM UTC+2	4 BGP ROUTES

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.