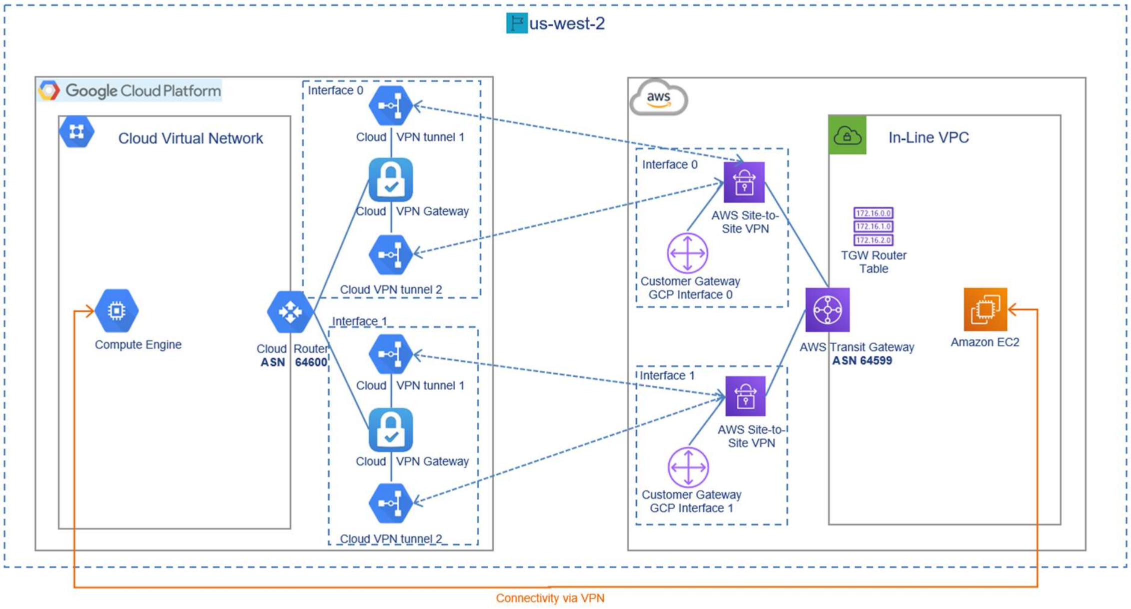
HA VPN between GCP and AWS Transit Gateway with dynamic BGP routing.

A walk-through for configuring secure redundant connectivity between AWS Transit Gateway and GCP Cloud VPC default network with dynamic BGP routing.

Schema:



HA VPN between GCP and AWS Transit Gateway with dynamic BGP routing

Created by César Sánchez Pacheco (cese)

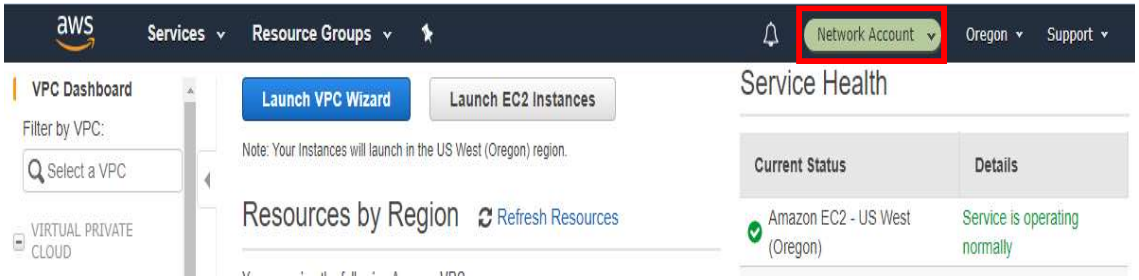
Revision: 1.0.0

Project: GFT Tranquility Base - AWS Landing Zone

Date: 06/09/2020

Overview

The VPN was created in an AWS Landing Zone implemented by GFT for the project Tranquility base, below you can see some steps to connect GFT AWS LZ and GCP default VPC Network, but the configuration for AWS side will be the same for another cloud or On-Premise peer. The context here is one Organization with multi-account interconnecting or sharing resources, so first of all, you have to work in the same account where the AWS Transit Gateway was created, for our case we have a Network Account where was created all the resources related to the GFT AWS Landing Zone.



Note: Your Instances will launch in the US West (Oregon) region.

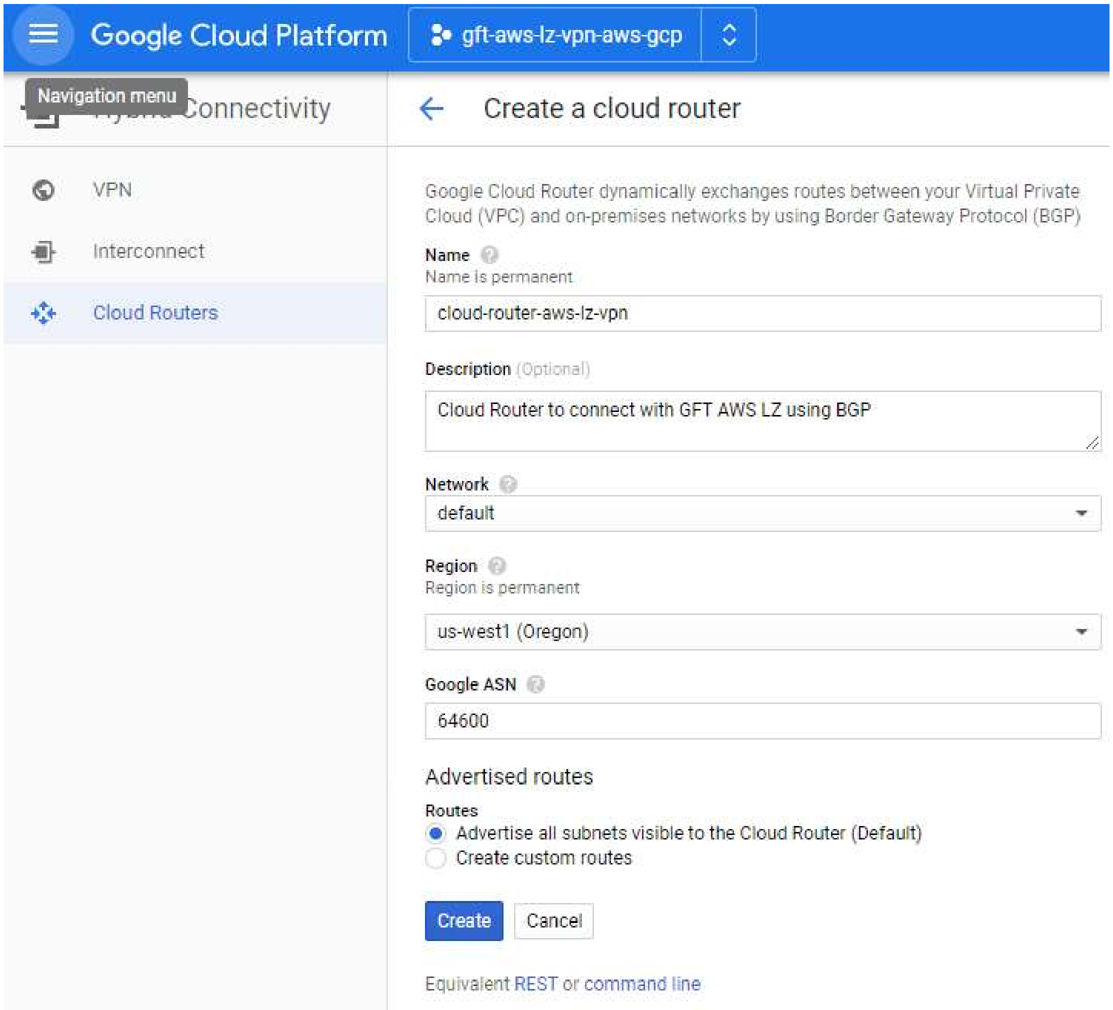
Current Status	Details
Amazon EC2 - US West (Oregon)	Service is operating normally

The steps to complete the connection are:

1. Create GCP Cloud Router.
2. Create GCP Cloud VPN Gateway.
3. Create AWS Customer Gateway.
4. Create AWS Site-to-site VPN Connection.
5. Getting Tunnels configuration.
6. Create GCP Peer VPN.
7. Configure GCP Cloud VPN tunnels.
8. Configure BGP Sessions.
9. Check in AWS, connectivity.

1. Create GCP Cloud Router

Open GCP console and go to NETWORKING -> Hybrid connectivity -> Cloud routers -> Create router:



Create a cloud router

Google Cloud Router dynamically exchanges routes between your Virtual Private Cloud (VPC) and on-premises networks by using Border Gateway Protocol (BGP)

Name
Name is permanent
cloud-router-aws-lz-vpn

Description (Optional)
Cloud Router to connect with GFT AWS LZ using BGP

Network
default

Region
Region is permanent
us-west1 (Oregon)

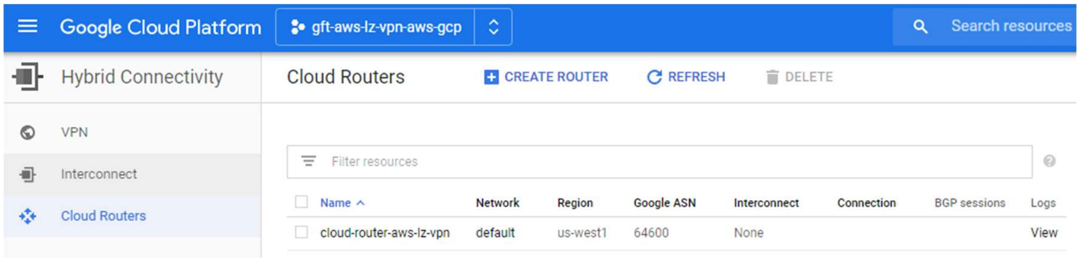
Google ASN
64600

Advertised routes

Routes
● Advertise all subnets visible to the Cloud Router (Default)
○ Create custom routes

Select “Advertise all subnets visible to the Cloud Router” in order to expose your subnets to BGP routing and to AWS router.

Click “Create” and this is how it should look like:

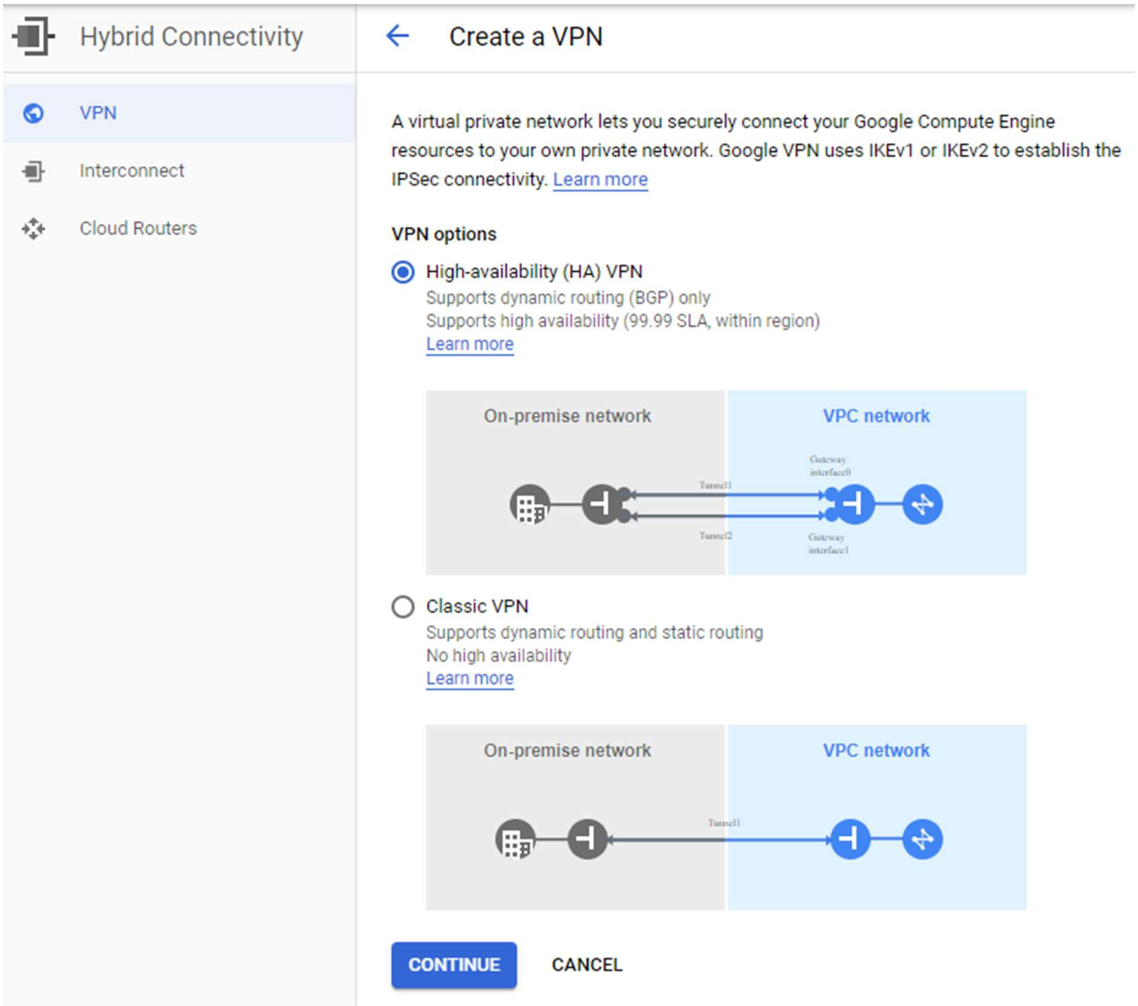


Cloud Routers

Name	Network	Region	Google ASN	Interconnect	Connection	BGP sessions	Logs
cloud-router-aws-lz-vpn	default	us-west1	64600	None			View

2. Create GCP Cloud HA VPN gateway.

Go to NETWORKING -> Hybrid connectivity -> VPN -> Create a VPN:



Create a VPN

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPSec connectivity. Learn more

VPN options

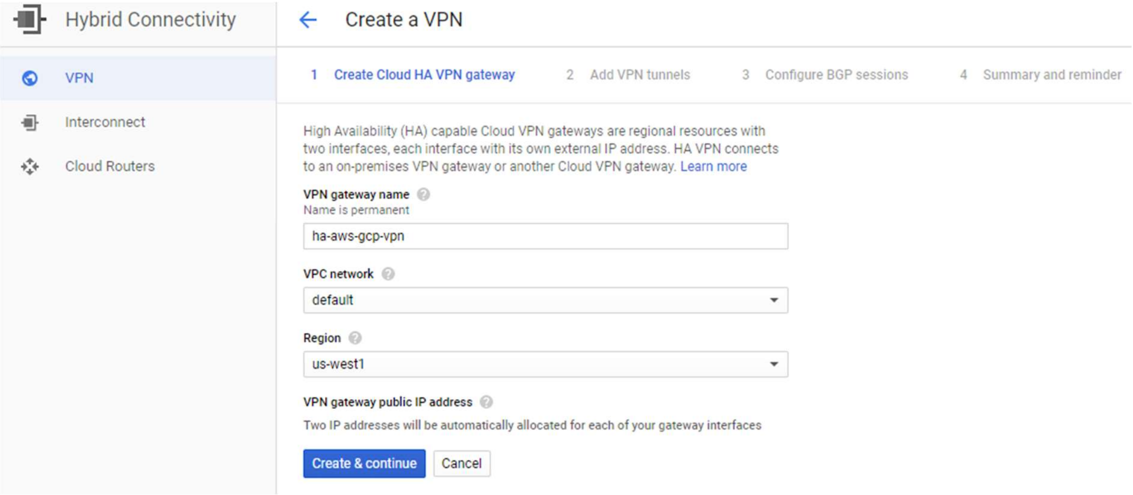
● High-availability (HA) VPN
Supports dynamic routing (BGP) only
Supports high availability (99.99 SLA, within region)
Learn more

○ Classic VPN
Supports dynamic routing and static routing
No high availability
Learn more

CONTINUE CANCEL

High availability handle 2 interfaces with a public address for each interface, AWS VPN gateway will have 2 public interfaces so there will be 2 VPN tunnels in fact, so for AWS side we have to create 2 Customer Gateway and 2 Site-Site VPN connection.

Click on “Continue” and set the values as bellow:



High Availability (HA) capable Cloud VPN gateways are regional resources with two interfaces, each interface with its own external IP address. HA VPN connects to an on-premises VPN gateway or another Cloud VPN gateway. Learn more

VPN gateway name
Name is permanent
ha-aws-gcp-vpn

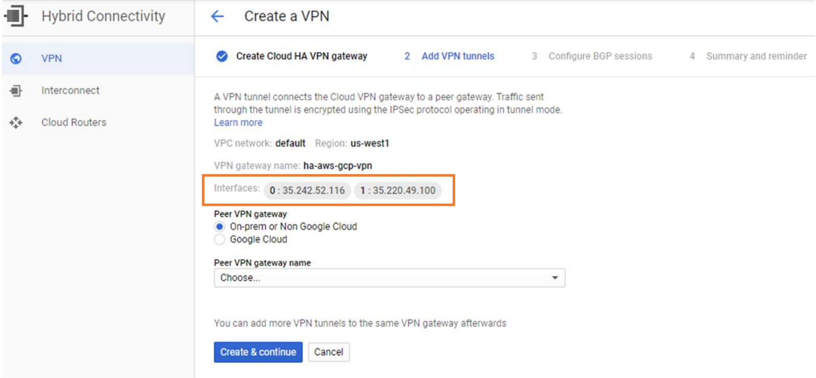
VPC network
default

Region
us-west1

VPN gateway public IP address
Two IP addresses will be automatically allocated for each of your gateway interfaces

Fill the information regarding Name, VPC Network, and Region, then click on “Create & continue”.

Below, we can see public IP addresses attached to the GCP Cloud HA VPN gateway. These IP should be specified in each AWS Customer gateway, so let’s got to AWS console and create them.



A VPN tunnel connects the Cloud VPN gateway to a peer gateway. Traffic sent through the tunnel is encrypted using the IPSec protocol operating in tunnel mode.
Learn more

VPC network: default Region: us-west1

VPN gateway name: ha-aws-gcp-vpn

Interfaces: 0 : 35.242.52.116 1 : 35.220.49.100

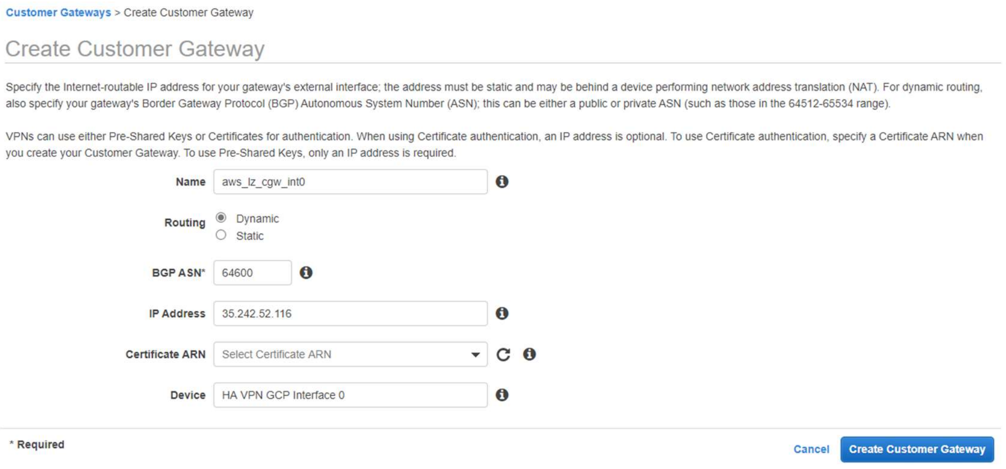
Peer VPN gateway
● On-prem or Non Google Cloud
○ Google Cloud

Peer VPN gateway name
Choose...

You can add more VPN tunnels to the same VPN gateway afterwards

3. Create AWS Customer Gateway.

Open AWS console and go to VPC -> Virtual Private Network (VPN) -> Customer Gateways -> Create Customer Gateway:



Create Customer Gateway

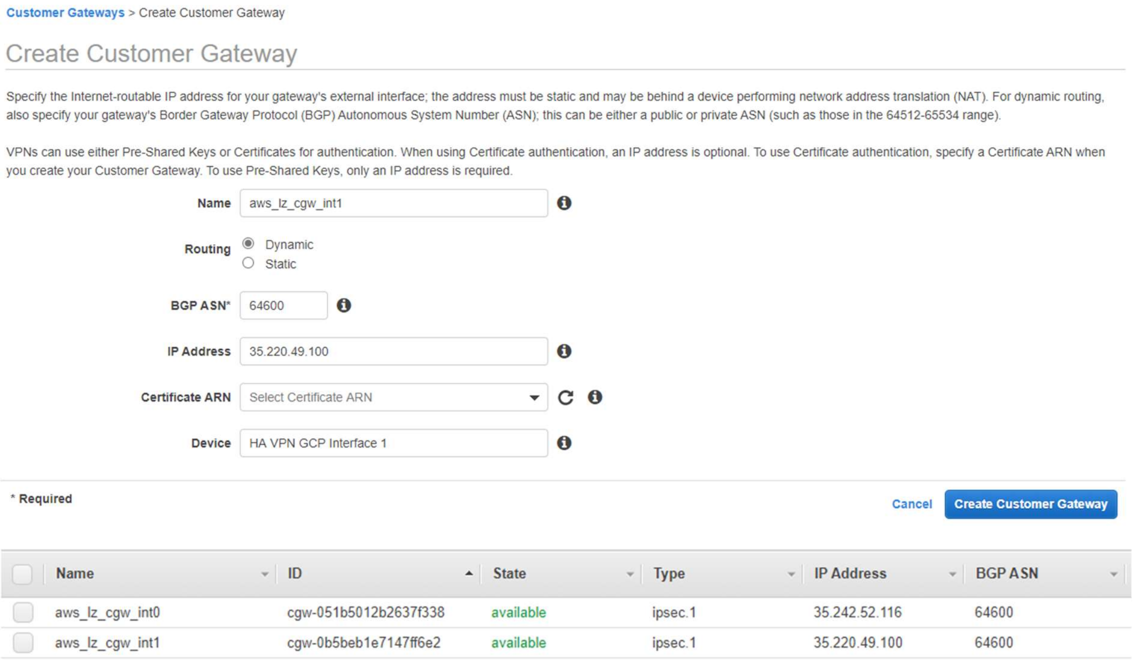
Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be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

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name: aws_lz_cgw_int0
Routing: ● Dynamic ○ Static
BGP ASN*: 64600
IP Address: 35.242.52.116
Certificate ARN: Select Certificate ARN
Device: HA VPN GCP Interface 0

* Required

Set Dynamic Routing and specify **ASN 64600** of GCP Cloud Router and IP of GCP Cloud HA VPN gateway interface you just created and click on “Create Customer Gateway”. **Repeat** these steps with the IP for interface 1 set to ***35.220.49.100*** (this is not a fixed value for the ip).



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).

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name: aws_lz_cgw_int1

Routing: ● Dynamic ○ Static

BGP ASN*: 64600

IP Address: 35.220.49.100

Certificate ARN: Select Certificate ARN

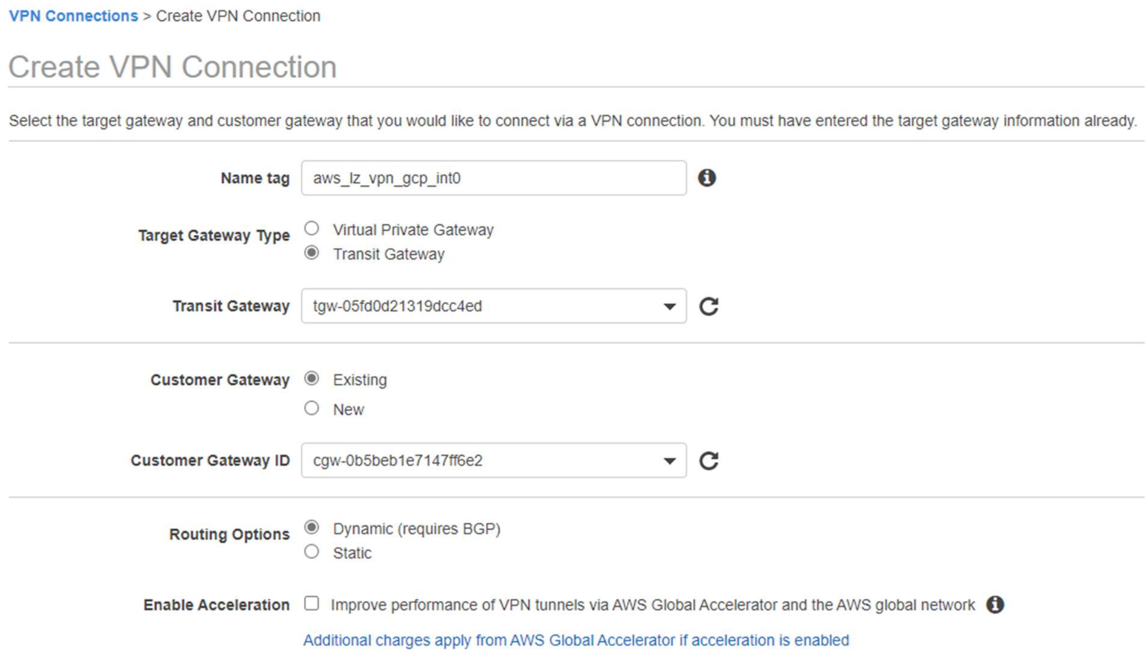
Device: HA VPN GCP Interface 1

* Required

□	Name	ID	State	Type	IP Address	BGP ASN
□	aws_lz_cgw_int0	cgw-051b5012b2637f338	available	ipsec.1	35.242.52.116	64600
□	aws_lz_cgw_int1	cgw-0b5beb1e7147ff6e2	available	ipsec.1	35.220.49.100	64600

4. Create AWS Site-to-site VPN Connection.

Go to VPC -> Virtual Private Network (VPN) -> Site-to-site VPN Connections -> Create VPN Connection and select Transit Gateway and Customer Gateway you just created. Also select Dynamic Routing:



VPN Connections > Create VPN Connection

Create VPN Connection

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

Name tag: aws_lz_vpn_gcp_int0

Target Gateway Type: ○ Virtual Private Gateway ● Transit Gateway

Transit Gateway: tgw-05fd0d21319dcc4ed

Customer Gateway: ● Existing ○ New

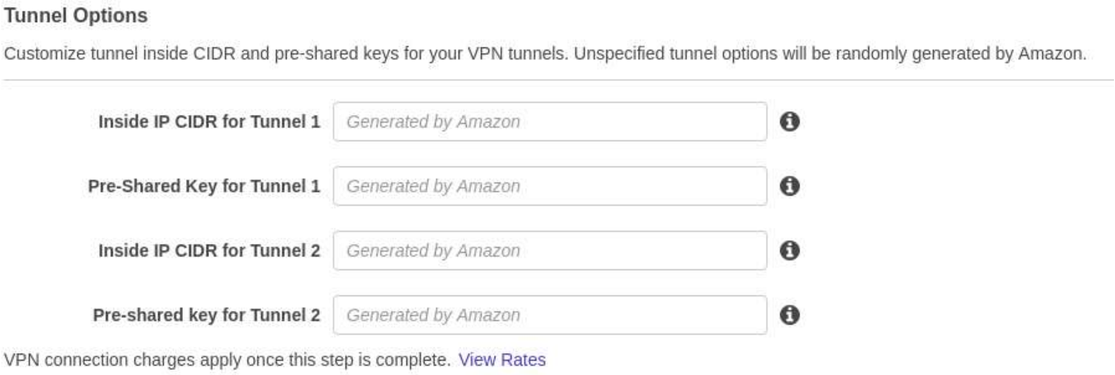
Customer Gateway ID: cgw-0b5beb1e7147ff6e2

Routing Options: ● Dynamic (requires BGP) ○ Static

Enable Acceleration: □ Improve performance of VPN tunnels via AWS Global Accelerator and the AWS global network

Additional charges apply from AWS Global Accelerator if acceleration is enabled

Leave Tunnel Options unchanged. AWS will generate Pre-Shared IPSec keys and Link-local addresses (e.g. 169.254.46.225/30) for the tunnels automatically:



Tunnel Options

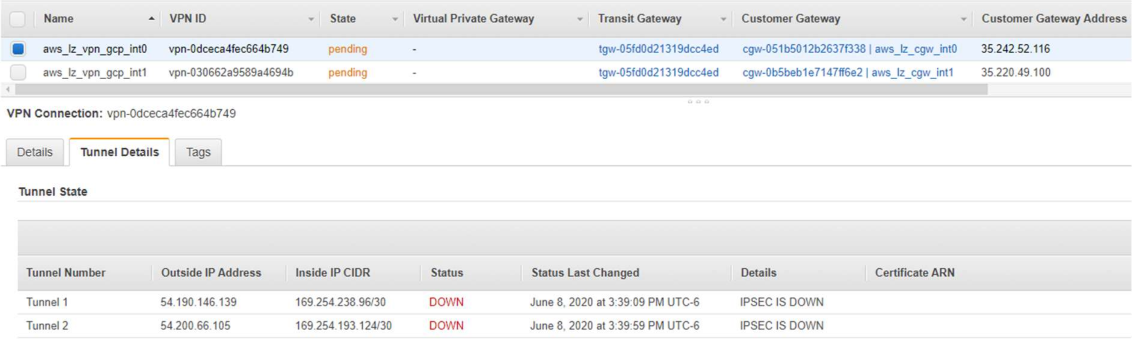
Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1	Generated by Amazon
Pre-Shared Key for Tunnel 1	Generated by Amazon
Inside IP CIDR for Tunnel 2	Generated by Amazon
Pre-shared key for Tunnel 2	Generated by Amazon

VPN connection charges apply once this step is complete. View Rates

Click on “Create VPN Connection”.

Repeat previous steps with information regarding to customer gateway for interface 1.



☐	Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address
☑	aws_lz_vpn_gcp_int0	vpn-0dceca4fec664b749	pending	-	tgw-05fd0d21319dcc4ed	cgw-051b5012b2637f338 | aws_lz_cgw_int0	35.242.52.116
☐	aws_lz_vpn_gcp_int1	vpn-030662a9589a4694b	pending	-	tgw-05fd0d21319dcc4ed	cgw-0b5beb1e7147ff6e2 | aws_lz_cgw_int1	35.220.49.100

VPN Connection: vpn-0dceca4fec664b749

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	54.190.146.139	169.254.238.96/30	DOWN	June 8, 2020 at 3:39:09 PM UTC-6	IPSEC IS DOWN	
Tunnel 2	54.200.66.105	169.254.193.124/30	DOWN	June 8, 2020 at 3:39:59 PM UTC-6	IPSEC IS DOWN	

The links are down because there are no tunnels configured on GCP side, but first let's figure out what configuration we will need.

5. Getting Tunnels configuration.

See highlighted IPs from the screenshot above.

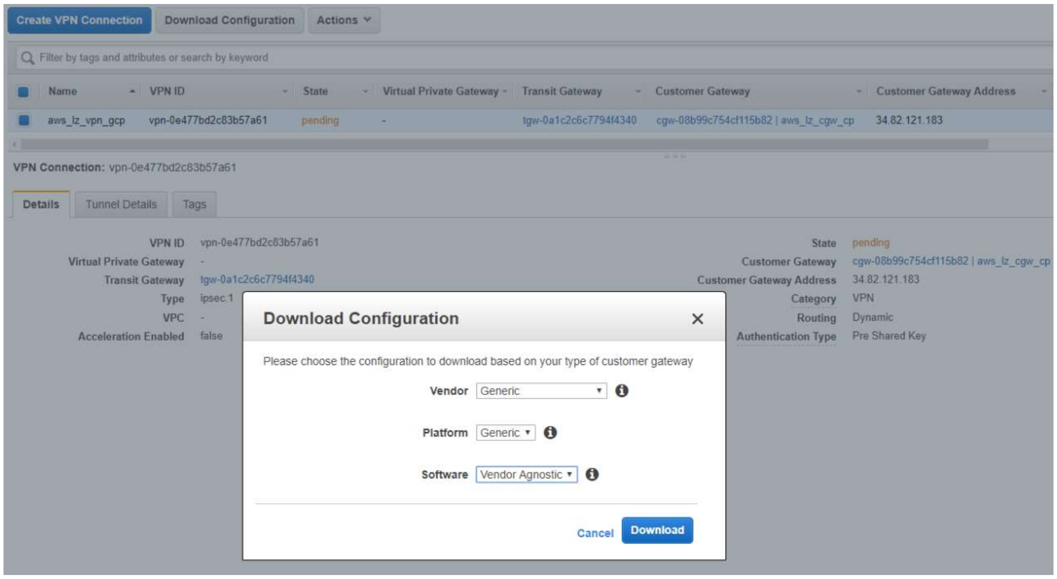
Interface 0: 35.242.52.116
Tunnel1: AWS Public IP 54.190.146.139; Inside tunnel subnet 169.254.238.96/30 that means IP 169.254.238.**97** (for BGP peer IP) and 169.254.238.**98** (for Cloud router BGP IP). To see how the subnet works use ipcalc.

Tunnel2: AWS Public IP 54.200.66.105; Inside tunnel subnet 169.254.193.124/30 that means IP 169.254.193.**125** (for BGP peer IP) and 169.254.193.**126** (for Cloud router BGP IP). To see how the subnet works use ipcalc.

Interface 1: 35.220.49.100
Tunnel1: AWS Public IP 52.10.65.167; Inside tunnel subnet 169.254.66.84/30 that means IP 169.254.66.**85** (for BGP peer IP) and 169.254.66.**86** (for Cloud router BGP IP). To see how the subnet works use ipcalc.

Tunnel2: AWS Public IP 52.11.71.190; Inside tunnel subnet 169.254.193.124/30 that means IP 169.254.193.**125** (for BGP peer IP) and 169.254.193.**126** (for Cloud router BGP IP). To see how the subnet works use ipcalc.

We also need to get ikev1 pre-shared keys so click on “Download Configuration”:



Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address
aws_lz_vpn_gcp	vpn-0e477bd2c83b57a61	pending	-	tgw-0a1c2c6c7794f4340	cgw-08b99c754cf115b82 | aws_lz_cgw_cp	34.82.121.183

VPN Connection: vpn-0e477bd2c83b57a61

VPN ID vpn-0e477bd2c83b57a61
Virtual Private Gateway -
Transit Gateway tgw-0a1c2c6c7794f4340
Type ipsec.1
VPC -
Acceleration Enabled false

State pending
Customer Gateway cgw-08b99c754cf115b82 | aws_lz_cgw_cp
Customer Gateway Address 34.82.121.183
Category VPN
Routing Dynamic
Authentication Type Pre Shared Key

Download Configuration

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

Vendor Generic
Platform Generic
Software Vendor Agnostic

Select Generic Vendor and click “Download”. Open vpn-xxxx.txt file and find the section

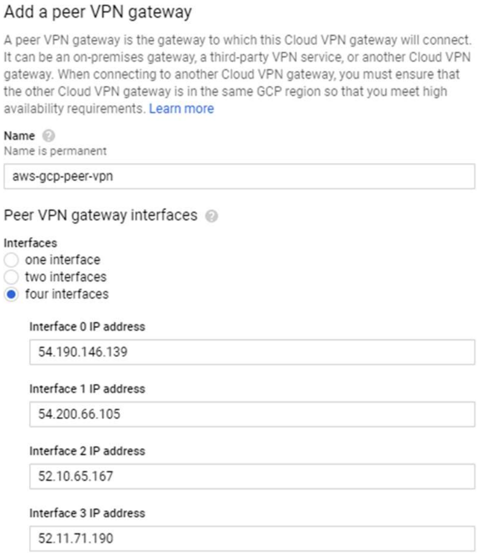
IPSec Tunnel #1 → #1: Internet Key Exchange Configuration
- Pre-Shared Key : M6xwVXx1Rg_JjLJq.z.XI0WB0bbKFxKt (the key will be different)

The same for tunnel 2: Internet Key Exchange Configuration
- Pre-Shared Key : qJFIXPv0D6itSOrbBXy16mQnlxogUbK6 (the key will be different)

Save the files and the keys in a safe place, you have to download 2 files one for each Site-to-Site VPN connection, so let’s go ahead to GCP Console and configure VPN tunnels.

6. Create GCP Peer VPN

Choose four interfaces to be filled with the information showed in step **5**, put the public ip for both AWS VPN connection, Interface 0 – Tunnel 1 – Tunnel 2, and Interface 1 – Tunnel 1 – Tunnel 2.



Add a peer VPN gateway

A peer VPN gateway is the gateway to which this Cloud VPN gateway will connect. It can be an on-premises gateway, a third-party VPN service, or another Cloud VPN gateway. When connecting to another Cloud VPN gateway, you must ensure that the other Cloud VPN gateway is in the same GCP region so that you meet high availability requirements. Learn more

Name
Name is permanent
aws-gcp-peer-vpn

Peer VPN gateway interfaces

Interfaces
○ one interface
○ two interfaces
● four interfaces

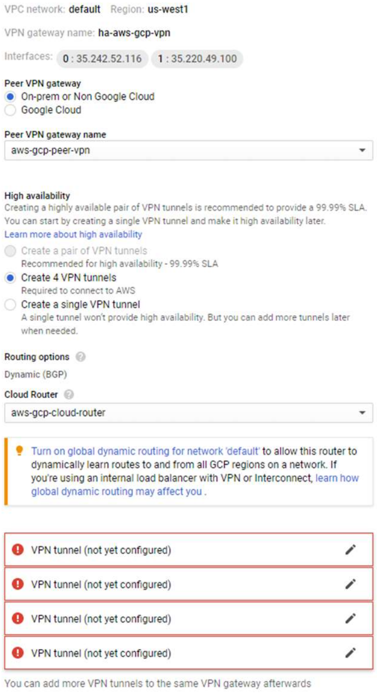
Interface 0 IP address
54.190.146.139

Interface 1 IP address
54.200.66.105

Interface 2 IP address
52.10.65.167

Interface 3 IP address
52.11.71.190

7. Configure GCP Cloud VPN tunnels.



VPC network: default Region: us-west1

VPN gateway name: ha-aws-gcp-vpn

Interfaces: 0 : 35.242.52.116 1 : 35.220.49.100

Peer VPN gateway

● On-prem or Non Google Cloud

○ Google Cloud

Peer VPN gateway name

aws-gcp-peer-vpn

High availability

Creating a highly available pair of VPN tunnels is recommended to provide a 99.99% SLA. You can start by creating a single VPN tunnel and make it high availability later.

Learn more about high availability

○ Create a pair of VPN tunnels
Recommended for high availability - 99.99% SLA

● Create 4 VPN tunnels
Required to connect to AWS

○ Create a single VPN tunnel
A single tunnel won't provide high availability. But you can add more tunnels later when needed.

Routing options

Dynamic (BGP)

Cloud Router

aws-gcp-cloud-router

Turn on global dynamic routing for network 'default' to allow this router to dynamically learn routes to and from all GCP regions on a network. If you're using an internal load balancer with VPN or Interconnect, learn how global dynamic routing may affect you .

VPN tunnel (not yet configured)

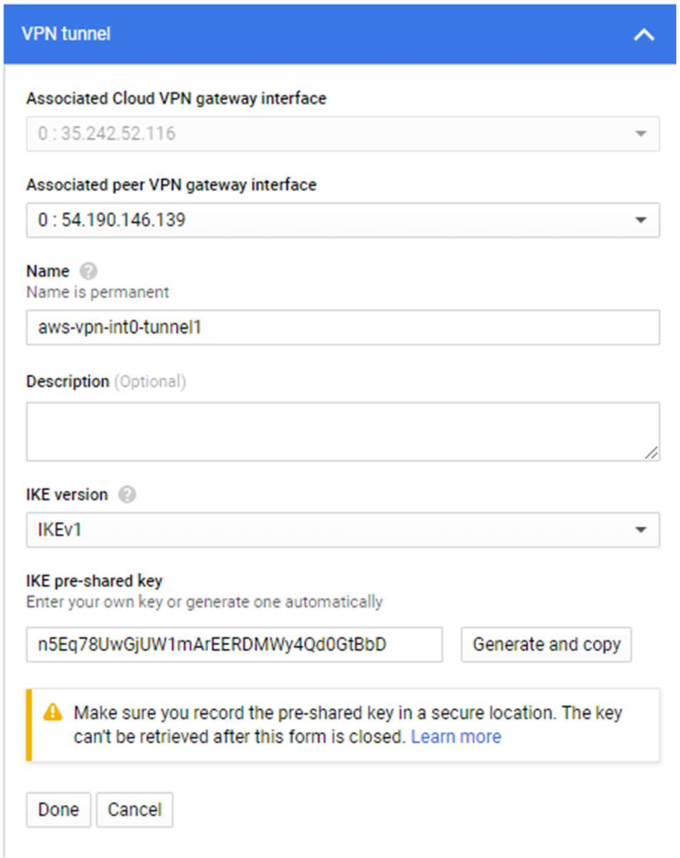
VPN tunnel (not yet configured)

VPN tunnel (not yet configured)

VPN tunnel (not yet configured)

You can add more VPN tunnels to the same VPN gateway afterwards

Click in each VPN tunnel icon to configure it:



VPN tunnel

Associated Cloud VPN gateway interface

0 : 35.242.52.116

Associated peer VPN gateway interface

0 : 54.190.146.139

Name

Name is permanent

aws-vpn-int0-tunnel1

Description (Optional)

IKE version

IKEv1

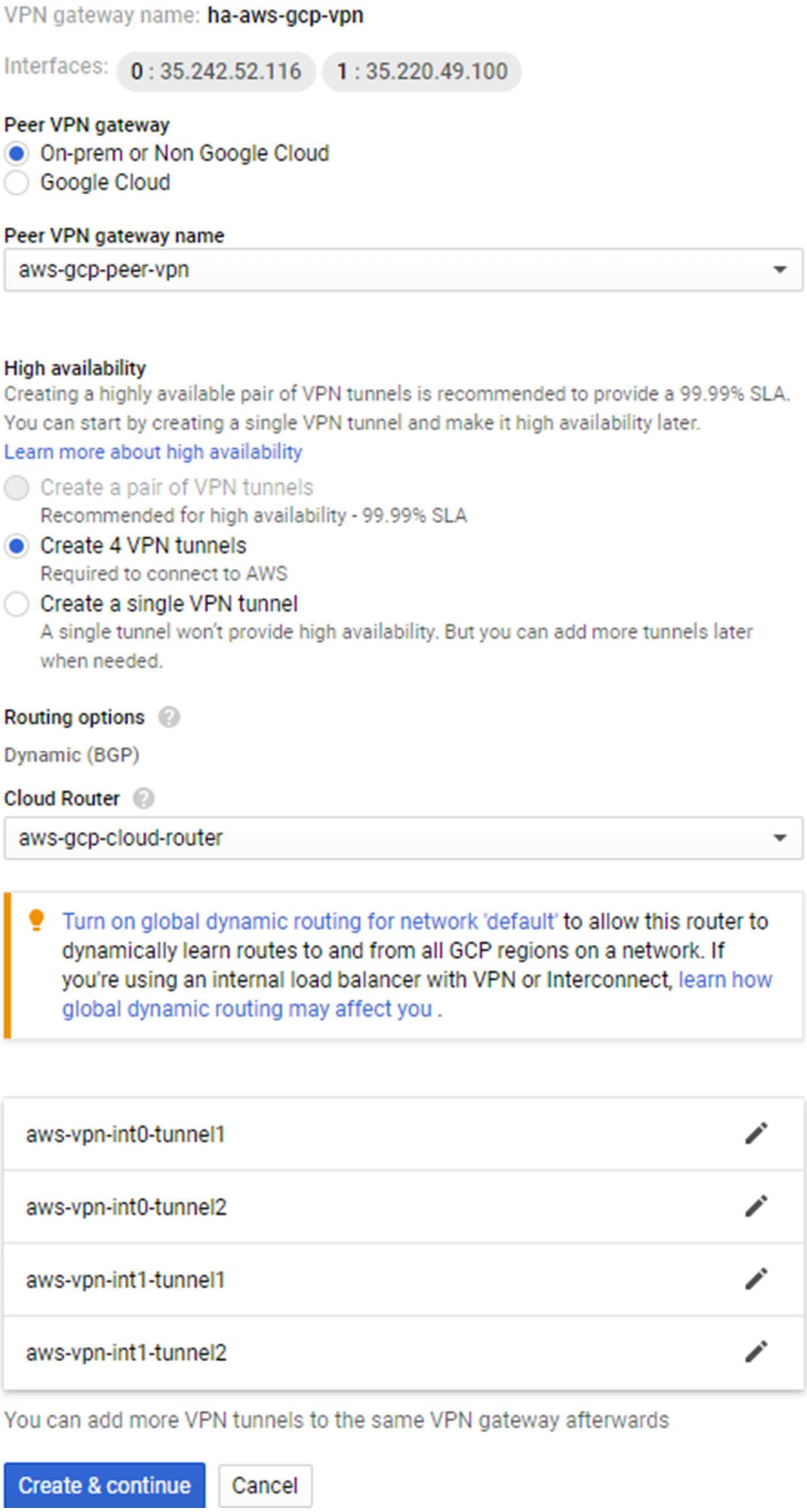
IKE pre-shared key

Enter your own key or generate one automatically

n5Eq78UwGjUW1mArEERDMWy4Qd0GtBbD

Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. Learn more

Repeat previous step for interface 1 – tunnel 1, tunnel 2, the final configuration is showing it in below picture.



VPN gateway name: ha-aws-gcp-vpn

Interfaces: 0 : 35.242.52.116 1 : 35.220.49.100

Peer VPN gateway

● On-prem or Non Google Cloud
○ Google Cloud

Peer VPN gateway name

aws-gcp-peer-vpn

High availability

Creating a highly available pair of VPN tunnels is recommended to provide a 99.99% SLA. You can start by creating a single VPN tunnel and make it high availability later.

Learn more about high availability

○ Create a pair of VPN tunnels
Recommended for high availability - 99.99% SLA
● Create 4 VPN tunnels
Required to connect to AWS
○ Create a single VPN tunnel
A single tunnel won't provide high availability. But you can add more tunnels later when needed.

Routing options

Dynamic (BGP)

Cloud Router

aws-gcp-cloud-router

Turn on global dynamic routing for network 'default' to allow this router to dynamically learn routes to and from all GCP regions on a network. If you're using an internal load balancer with VPN or Interconnect, learn how global dynamic routing may affect you .

aws-vpn-int0-tunnel1

aws-vpn-int0-tunnel2

aws-vpn-int1-tunnel1

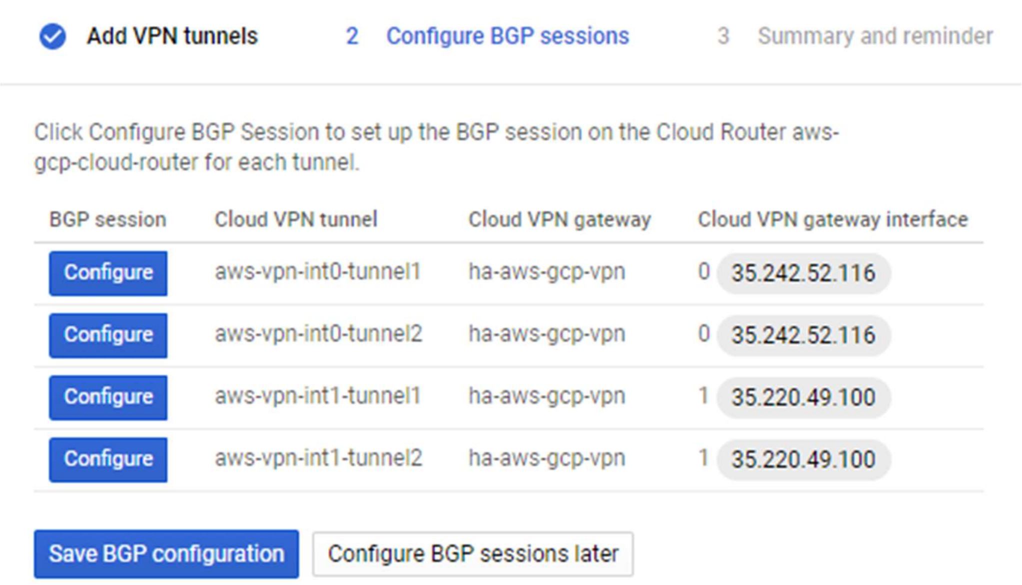
aws-vpn-int1-tunnel2

You can add more VPN tunnels to the same VPN gateway afterwards

Click in “Create & continue”

8. Configure BGP sessions.

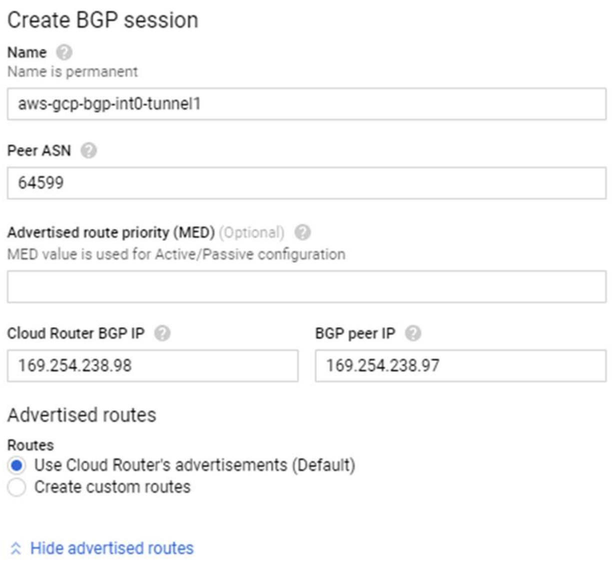
Click in configure button for each interface/tunnel record.



Click Configure BGP Session to set up the BGP session on the Cloud Router aws-gcp-cloud-router for each tunnel.

BGP session	Cloud VPN tunnel	Cloud VPN gateway	Cloud VPN gateway interface
Configure	aws-vpn-int0-tunnel1	ha-aws-gcp-vpn	0 35.242.52.116
Configure	aws-vpn-int0-tunnel2	ha-aws-gcp-vpn	0 35.242.52.116
Configure	aws-vpn-int1-tunnel1	ha-aws-gcp-vpn	1 35.220.49.100
Configure	aws-vpn-int1-tunnel2	ha-aws-gcp-vpn	1 35.220.49.100

Set Peer ASN **64599** (of AWS Transit Gateway already created by the Landing Zone), Cloud Router BGP IP and BGP peer IP (see Interface 0 - tunnel 1 of step 5 “Getting Tunnels configuration”), Select “Use Cloud Router’s advertisements” to expose all your subnets of the VPC Network (Default Network in this case) and click on “Save and continue”:



Create BGP session

Name
Name is permanent
aws-gcp-bgp-int0-tunnel1

Peer ASN
64599

Advertised route priority (MED) (Optional)
MED value is used for Active/Passive configuration

Cloud Router BGP IP
169.254.238.98

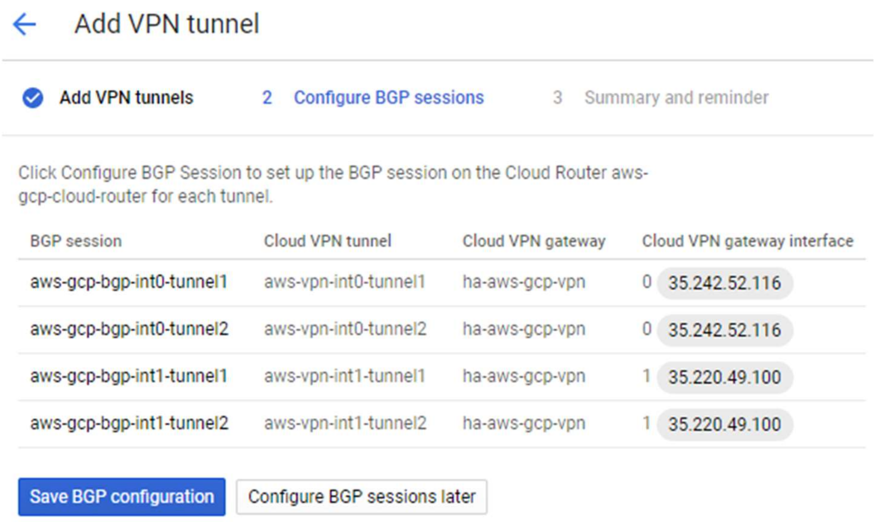
BGP peer IP
169.254.238.97

Advertised routes

Routes
● Use Cloud Router's advertisements (Default)
○ Create custom routes

Repeat previous step until complete all the values for 2 Interfaces and 4 tunnels.

Below you can see the list for all BGP sessions already configured.

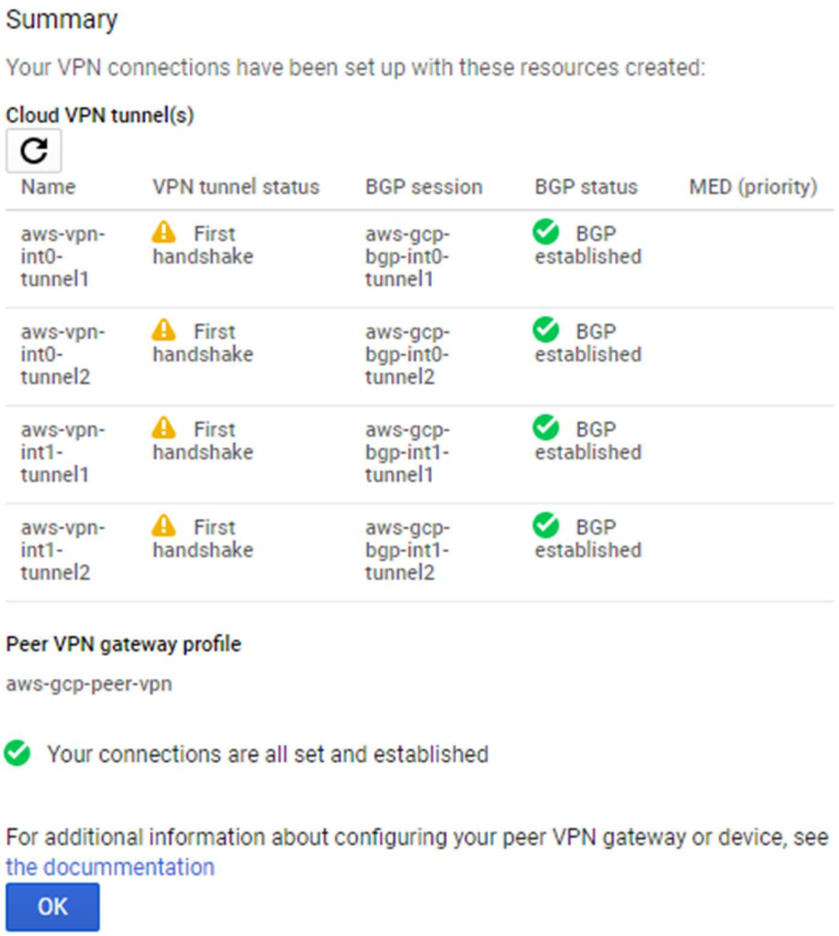


← Add VPN tunnel

✓ Add VPN tunnels   2 Configure BGP sessions   3 Summary and reminder

Click Configure BGP Session to set up the BGP session on the Cloud Router aws-gcp-cloud-router for each tunnel.

BGP session	Cloud VPN tunnel	Cloud VPN gateway	Cloud VPN gateway interface
aws-gcp-bgp-int0-tunnel1	aws-vpn-int0-tunnel1	ha-aws-gcp-vpn	0 35.242.52.116
aws-gcp-bgp-int0-tunnel2	aws-vpn-int0-tunnel2	ha-aws-gcp-vpn	0 35.242.52.116
aws-gcp-bgp-int1-tunnel1	aws-vpn-int1-tunnel1	ha-aws-gcp-vpn	1 35.220.49.100
aws-gcp-bgp-int1-tunnel2	aws-vpn-int1-tunnel2	ha-aws-gcp-vpn	1 35.220.49.100



Summary

Your VPN connections have been set up with these resources created:

Cloud VPN tunnel(s)

Name	VPN tunnel status	BGP session	BGP status	MED (priority)
aws-vpn-int0-tunnel1	⚠ First handshake	aws-gcp-bgp-int0-tunnel1	✓ BGP established	
aws-vpn-int0-tunnel2	⚠ First handshake	aws-gcp-bgp-int0-tunnel2	✓ BGP established	
aws-vpn-int1-tunnel1	⚠ First handshake	aws-gcp-bgp-int1-tunnel1	✓ BGP established	
aws-vpn-int1-tunnel2	⚠ First handshake	aws-gcp-bgp-int1-tunnel2	✓ BGP established	

Peer VPN gateway profile

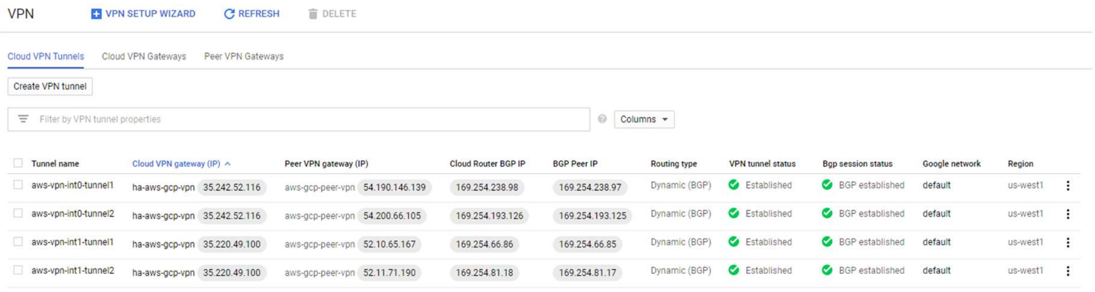
aws-gcp-peer-vpn

✓ Your connections are all set and established

For additional information about configuring your peer VPN gateway or device, see the documentation

Click “Create” and go to NETWORKING -> Hybrid connectivity -> VPN -> Cloud VPN Tunnels.

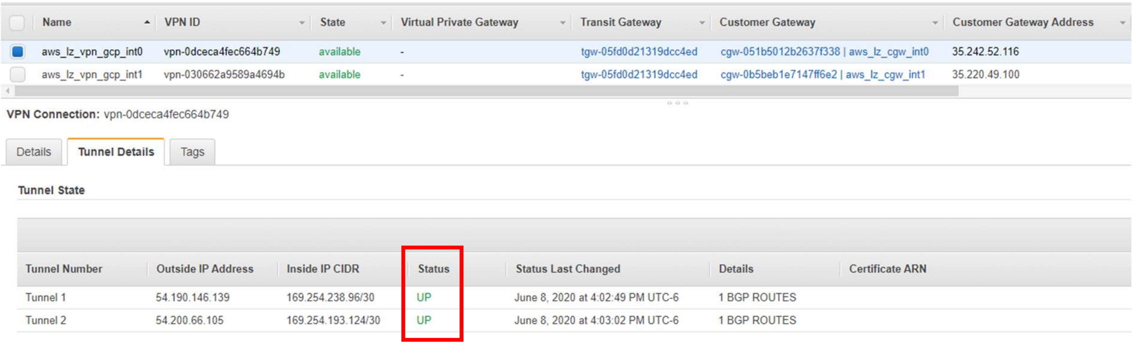
Starting the tunnel takes some time but this is how it looks like eventually:



□	Tunnel name	Cloud VPN gateway (IP)	Peer VPN gateway (IP)	Cloud Router BGP IP	BGP Peer IP	Routing type	VPN tunnel status	Bgp session status	Google network	Region
□	aws-vpn-int0-tunnel1	ha-aws-gcp-vpn 35.242.52.116	aws-gcp-peer-vpn 54.190.146.139	169.254.238.98	169.254.238.97	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-west1
□	aws-vpn-int0-tunnel2	ha-aws-gcp-vpn 35.242.52.116	aws-gcp-peer-vpn 54.200.66.105	169.254.193.126	169.254.193.125	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-west1
□	aws-vpn-int1-tunnel1	ha-aws-gcp-vpn 35.220.49.100	aws-gcp-peer-vpn 52.10.65.167	169.254.66.86	169.254.66.85	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-west1
□	aws-vpn-int1-tunnel2	ha-aws-gcp-vpn 35.220.49.100	aws-gcp-peer-vpn 52.11.71.190	169.254.81.18	169.254.81.17	Dynamic (BGP)	✓ Established	✓ BGP established	default	us-west1

9. Check in AWS, connectivity.

Let’s Go to AWS console and check the status of the tunnel as well:



□	Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address
■	aws_lz_vpn_gcp_int0	vpn-0dceca4fec664b749	available	-	tgw-05fd0d21319dcc4ed	cgw-051b5012b2637f338 | aws_lz_cgw_int0	35.242.52.116
□	aws_lz_vpn_gcp_int1	vpn-030662a9589a4694b	available	-	tgw-05fd0d21319dcc4ed	cgw-0b5beb1e7147ff6e2 | aws_lz_cgw_int1	35.220.49.100

VPN Connection: vpn-0dceca4fec664b749

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	Details	Certificate ARN
Tunnel 1	54.190.146.139	169.254.238.96/30	UP	June 8, 2020 at 4:02:49 PM UTC-6	1 BGP ROUTES	
Tunnel 2	54.200.66.105	169.254.193.124/30	UP	June 8, 2020 at 4:03:02 PM UTC-6	1 BGP ROUTES	

All is UP!