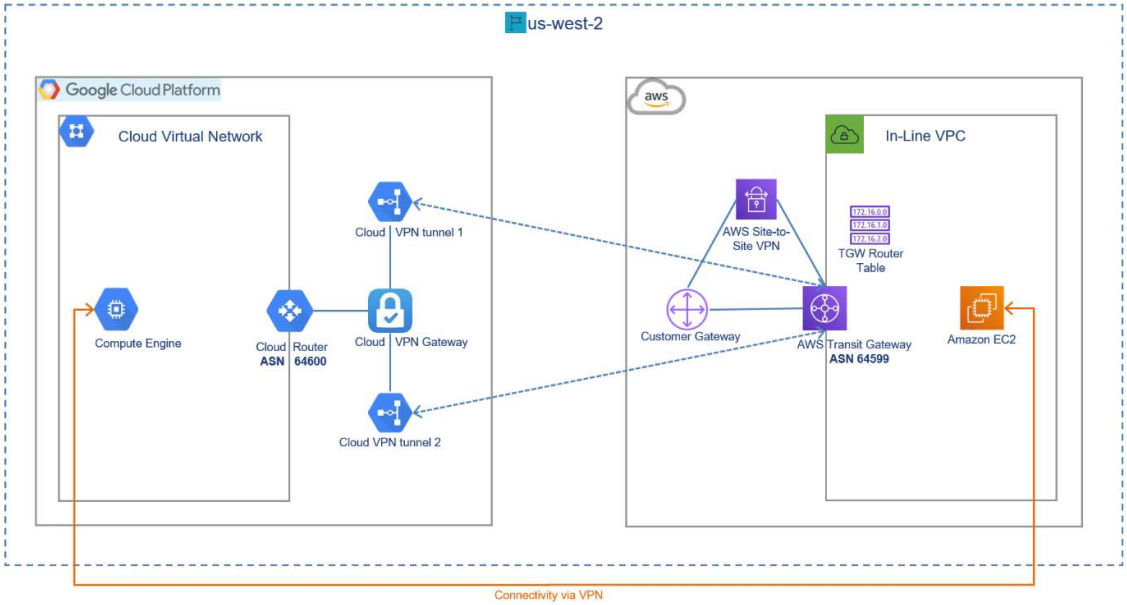
# Site-to-site VPN between GCP and AWS Transit Gateway with dynamic BGP routing.

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

Schema:




**Site-to-Site VPN between GCP and AWS Transit Gateway with dynamic BGP routing**

Created by César Sánchez Pacheco (cese)

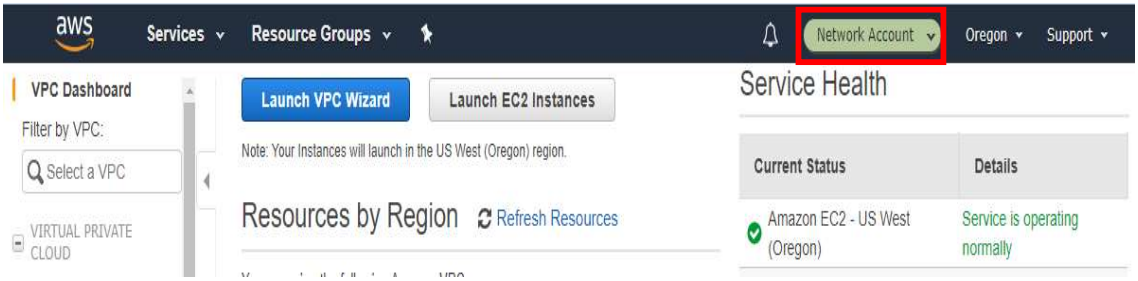
Revision: 1.0.0

Project: GFT Tranquility Base - AWS Landing Zone

Date: 4/23/2020

## 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 an 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.

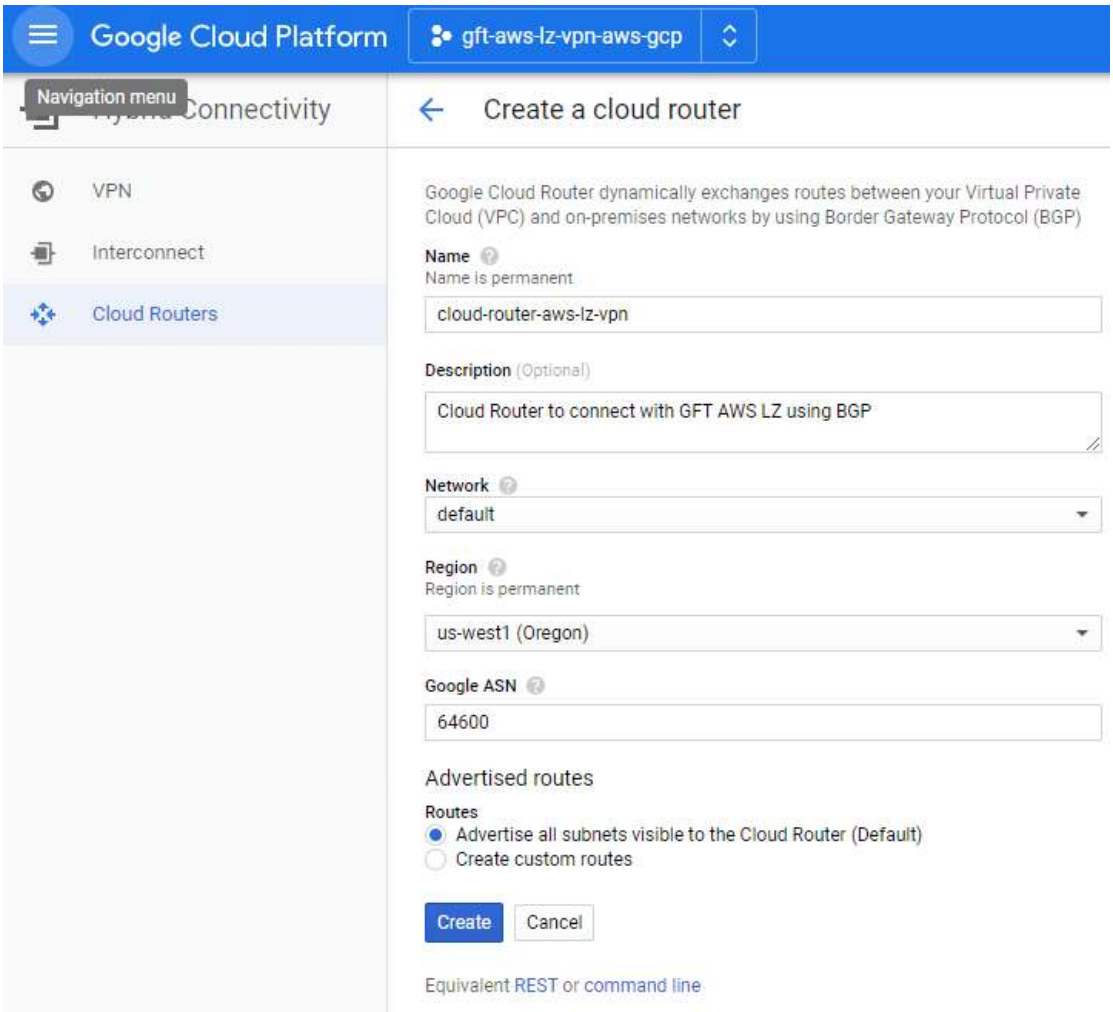



The steps to complete the connection are:

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 Cloud VPN tunnels.
7. Check in AWS, connectivity, TGW router table.
8. AWS Network Manager monitoring tool.

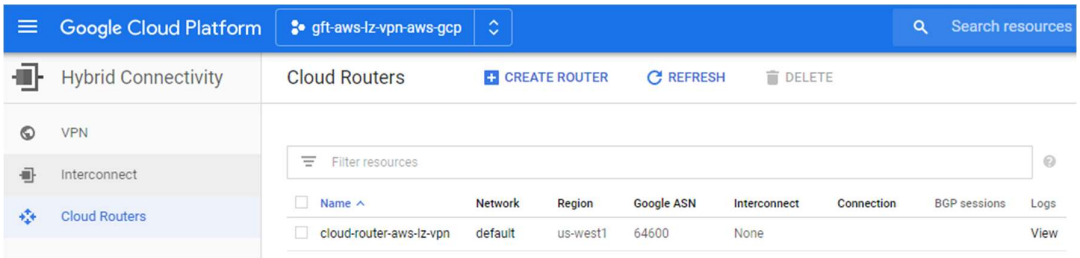
## 1. Create GCP Cloud Router

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



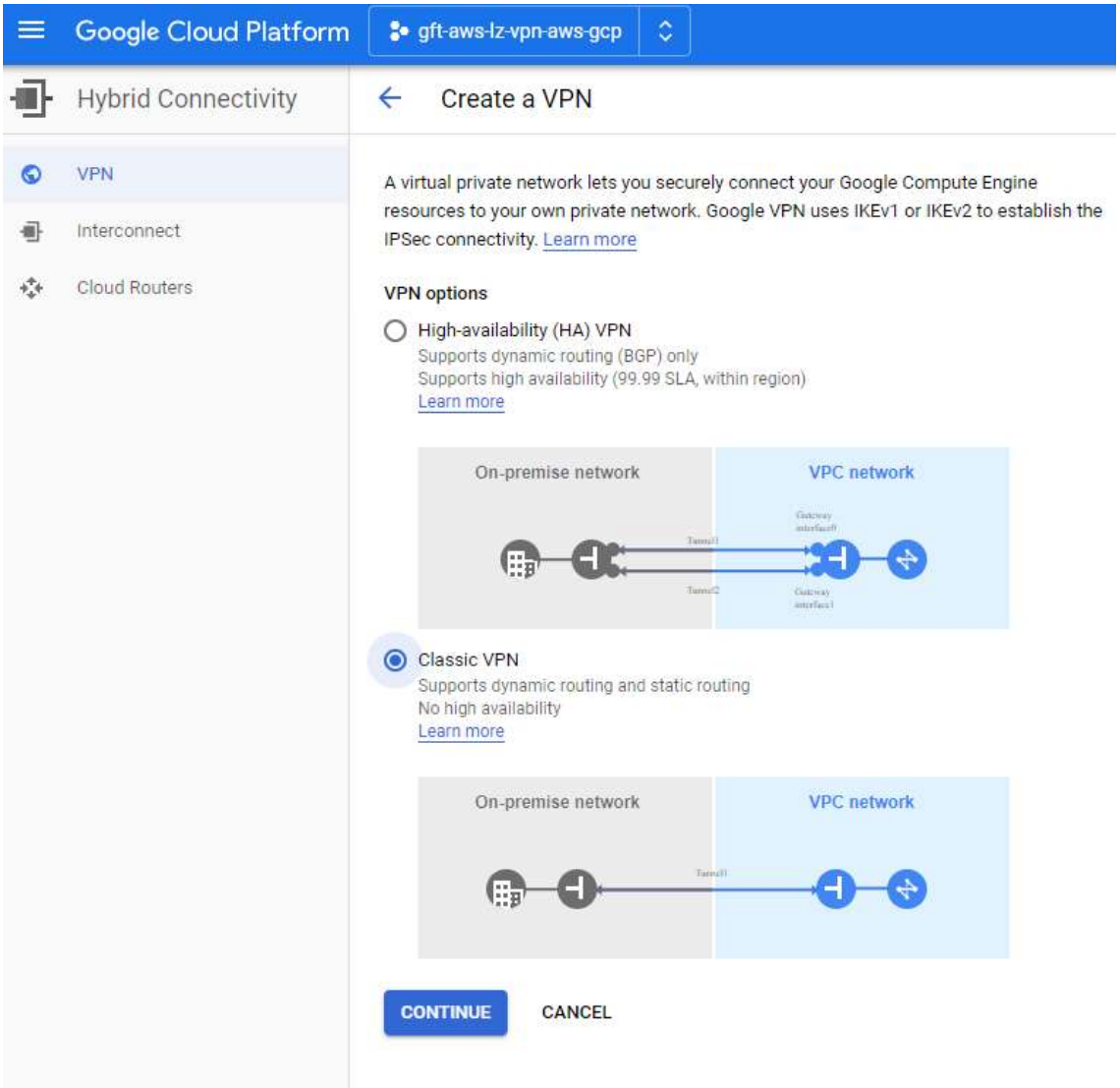

Select “Advertise all subnets visible to the Cloud Router” in order to expose your subnets to BGP routing and to AWS router.

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



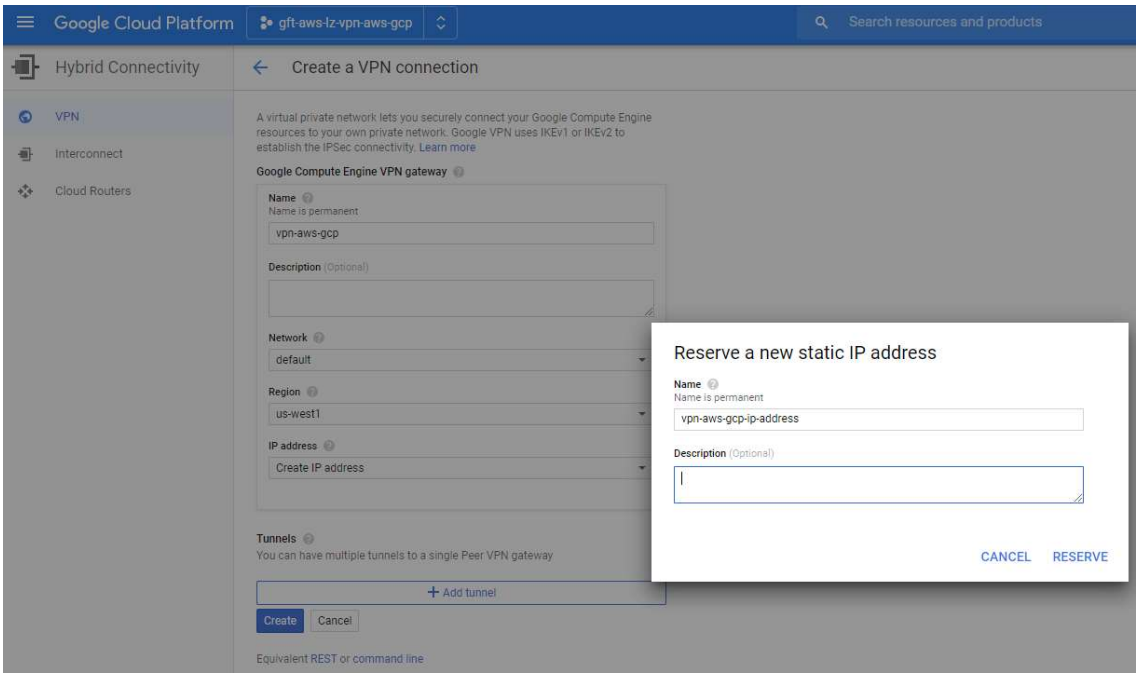
## 2. Create GCP Cloud VPN gateway.

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



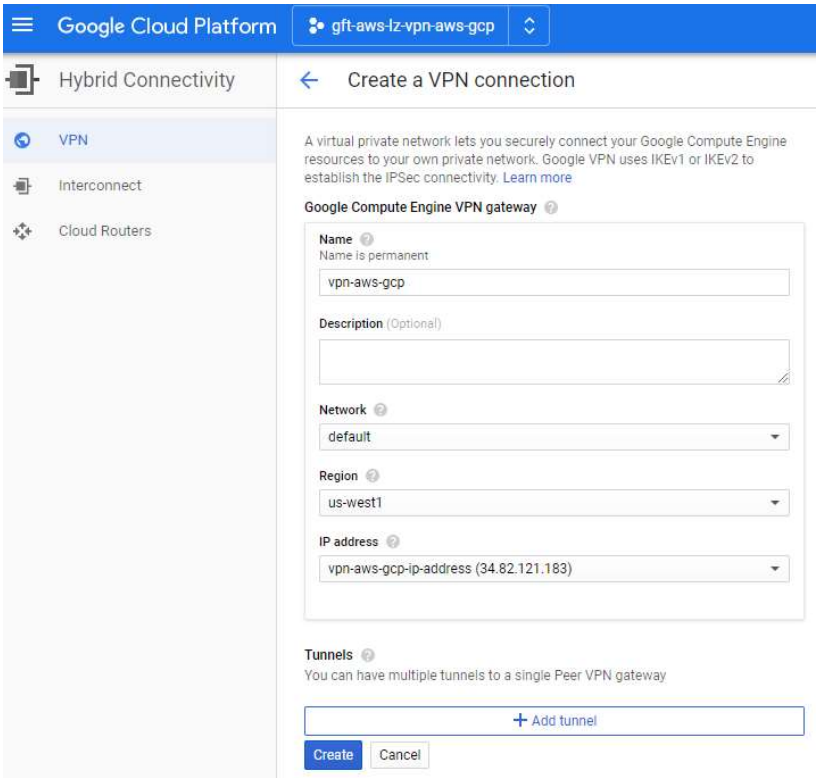

Don't worry about "No high availability", AWS VPN gateway will have 2 public interfaces so there will be 2 VPN tunnels in fact.

Click on "Continue" and set the values as bellow:

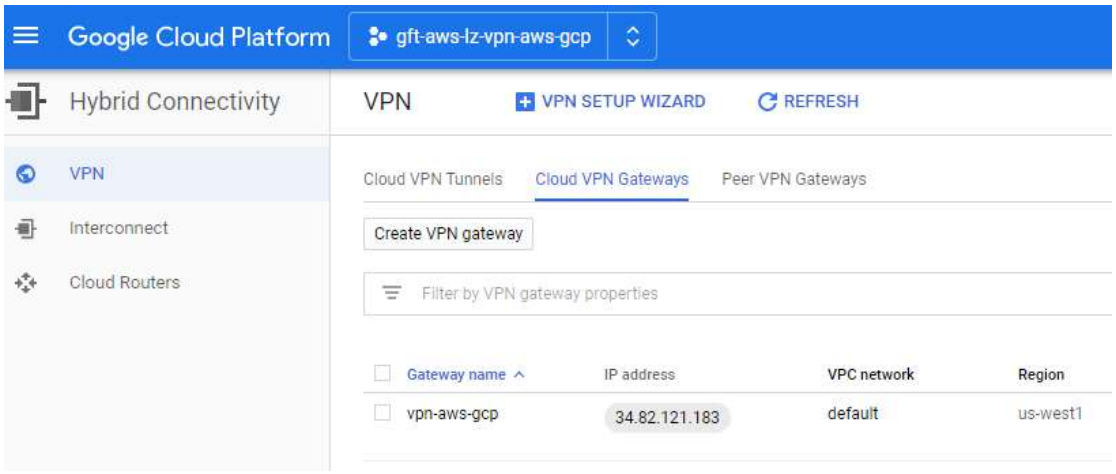



Click on “Reserve”

As we don’t have anything on AWS side remove the tunnel and click on “Create”:



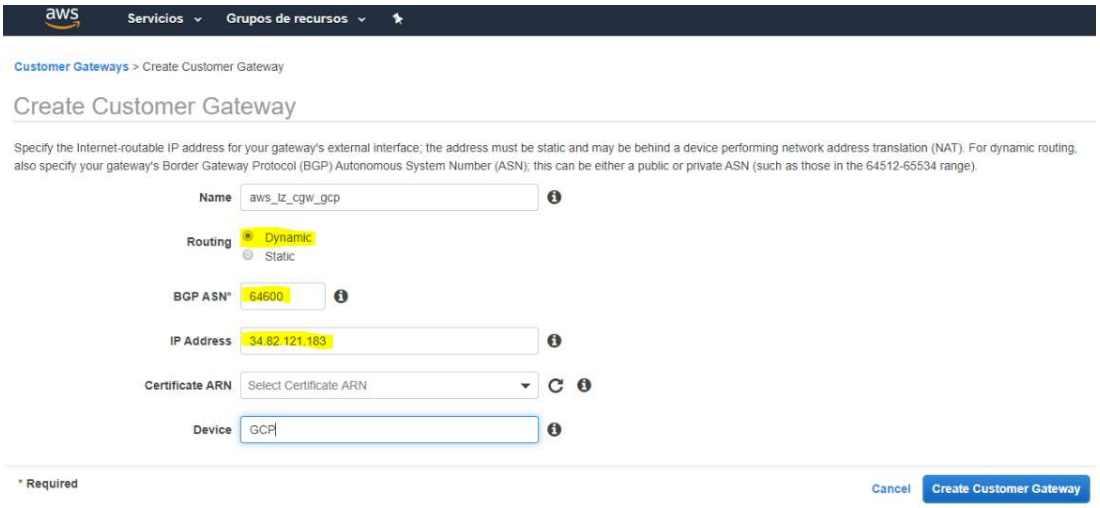
Now this is how it should look like:




We can see public IP address attached to the gateway. This IP should be specified in AWS Customer gateway, so let's got to AWS console and create one.

## 3. Create AWS Customer Gateway.

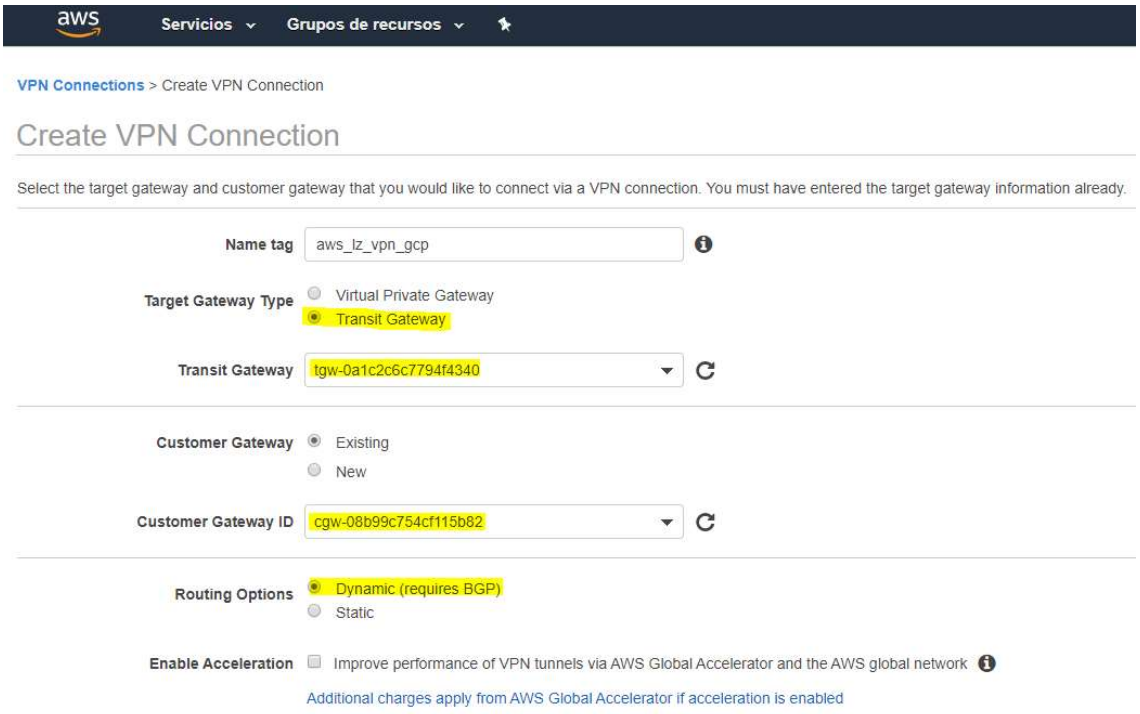
Open AWS console and go to VPC -> Virtual Private Network (VPN) -> Customer Gateways -> Create Customer Gateway:



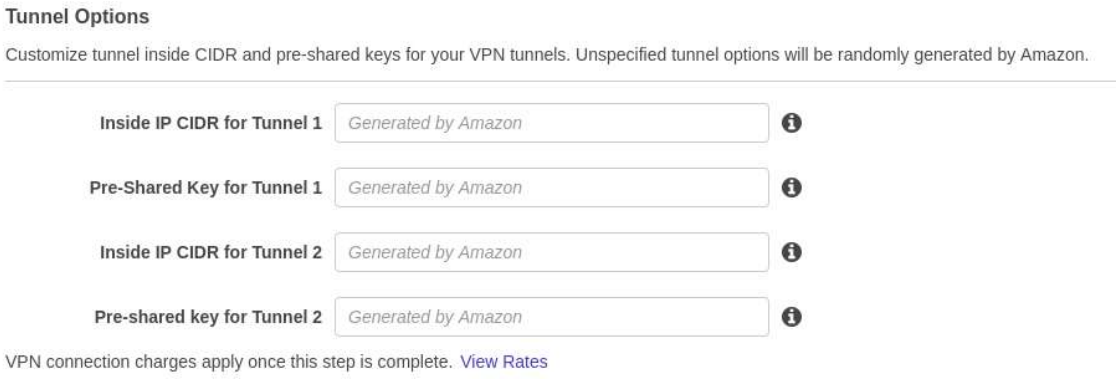

Set Dynamic Routing and specify ASN 64600 of GCP Cloud Router and IP of GCP Cloud VPN gateway you just created and click on "Create Customer Gateway".

## 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:




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:



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

| 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

Details | Tunnel Details | Tags

| | | | |
|---|---|---|---|
| VPN ID | vpn-0e477bd2c83b57a61 | State | pending |
| Virtual Private Gateway | - | Customer Gateway | cgw-08b99c754cf115b82 \| aws_lz_cgw_cp |
| Transit Gateway | tgw-0a1c2c6c7794f4340 | Customer Gateway Address | 34.82.121.183 |
| Type | ipsec.1 | Category | VPN |
| VPC | - | Routing | Dynamic |
| Acceleration Enabled | false | Authentication Type | Pre Shared Key |

Filter by tags and attributes or search by keyword

| 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

Details | Tunnel Details | Tags

**Tunnel State**

| Tunnel Number | Outside IP Address | Inside IP CIDR | Status | Status Last Changed | Details | Certificate ARN |
|---|---|---|---|---|---|---|
| Tunnel 1 | 34.216.185.60 | 169.254.187.100/30 | DOWN | April 22, 2020 at 4:25:09 PM UTC-6 | IPSEC IS DOWN | |
| Tunnel 2 | 54.200.23.92 | 169.254.213.24/30 | DOWN | April 22, 2020 at 4:25:09 PM UTC-6 | IPSEC IS DOWN | |

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

## 5. Getting Tunnels configuration.

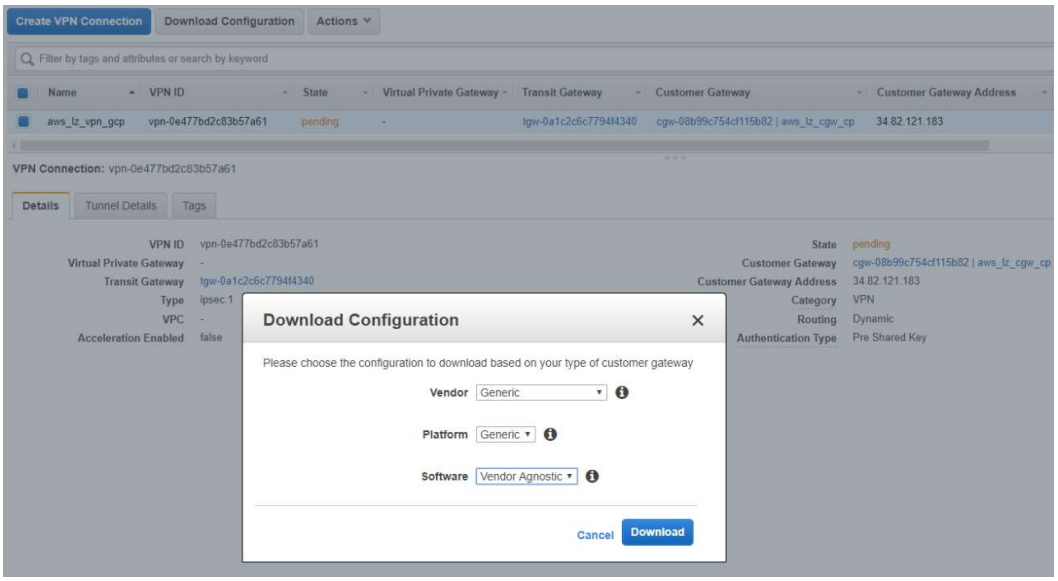
See highlighted IPs from the screenshot above.

Tunnel1: AWS Public IP 34.216.185.60; Inside tunnel subnet 169.254.187.100/30 that means IP 169.254.187.101 (for AWS link) and 169.254.187.102 (for GCP link). To see how the subnet works use ipcalc.

Tunnel2: AWS Public IP 54.200.3.92; Inside tunnel subnet 169.254.213.24/30 that means IP 169.254.213.25 (for AWS link) and 169.254.213.26 (for GCP link). To see how the subnet works use ipcalc.

GCP Public IP is generic for both tunnels: 34.82.121.183

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



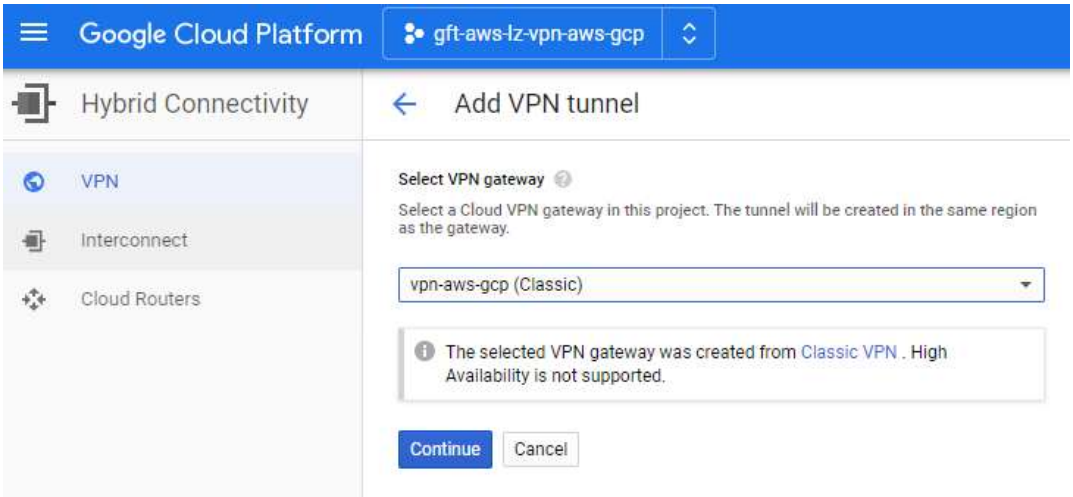

Select Generic Vendor and click “Download”. Open .txt file and find section tunnel-group 34.216.185.60 (tunnel 1, see the IP bellow) and get ikev1 pre-shared-key F1Bolwh1VNOhuwKCCf3lo8NwRpCLClqF (the key will be different)

The same for tunnel 2: Find section tunnel-group 54.200.23.92 and get ikev1 pre-shared-key ac.tSbqpjHyiVobNurSajJqB75ML1xpS (the key will be different)

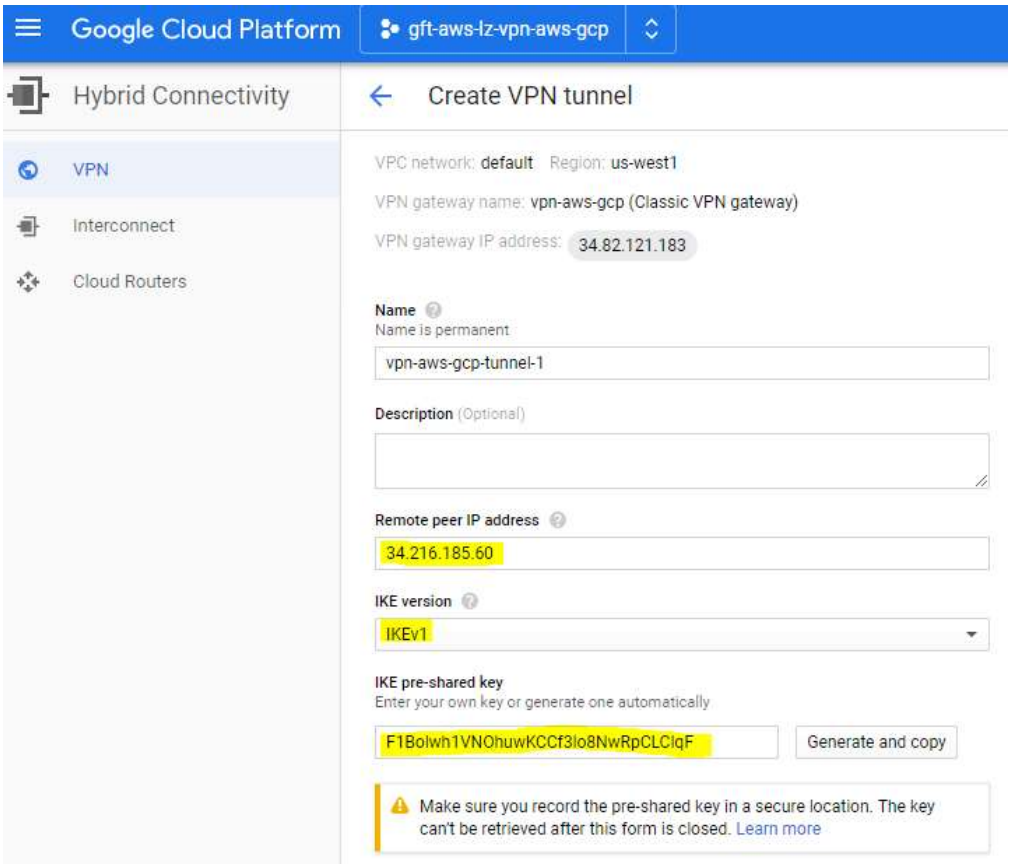
Save the file and the keys in a safe place, so let’s go ahead to GCP Console and configure VPN tunnels.

## 6. Create GCP Cloud VPN tunnels.

Open GCP console and go to NETWORKING -> Hybrid connectivity -> VPN -> Cloud VPN Tunnels -> Create VPN Tunnel:

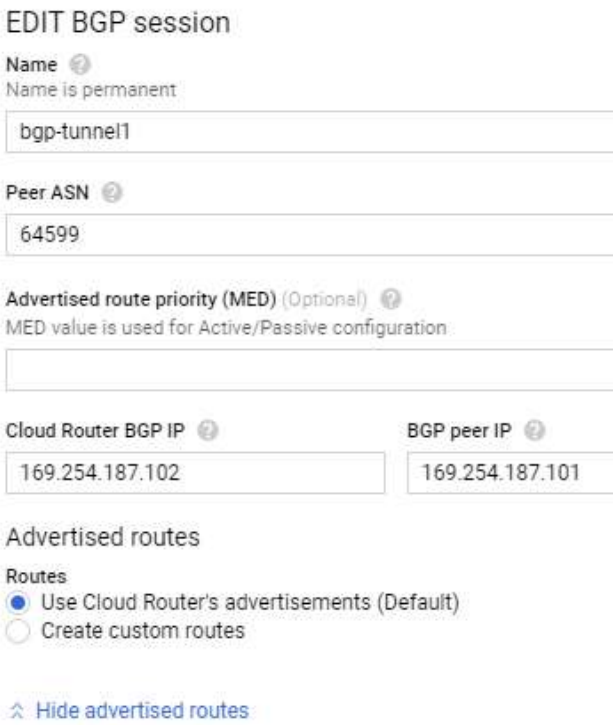



Select VPN gateway “vpn-aws-gcp” we created above and click on “Continue”:




Set remote peer IP address of tunnel 1 (see “Getting Tunnels configuration” above). Set BGP options as bellow and change BGP session:

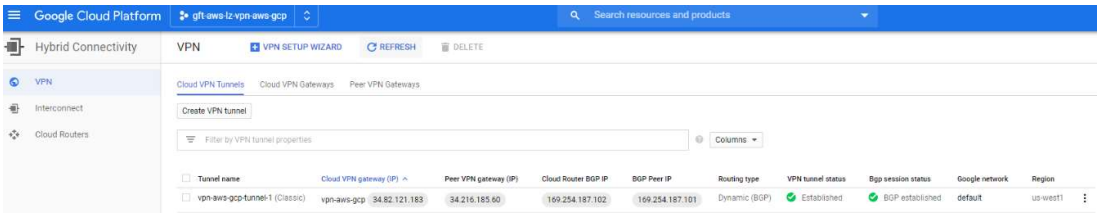

Set Peer ASN 64599 (of AWS Transit Gateway already created by the Landing Zone), Cloud Router BGP IP and BGP peer IP (see Tunnel 1 of “Getting Tunnels configuration” above), Select “Use Cloud Router’s advertisements” to expose all your subnets of the VPC Network (Default Network in this case) and click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



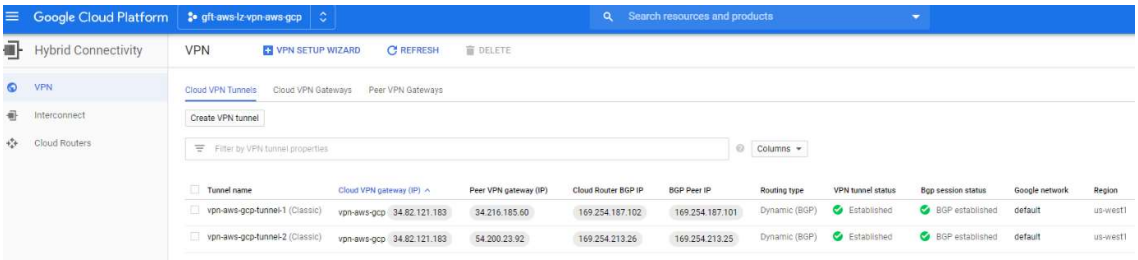

Now this is how Routing options should look like:


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:

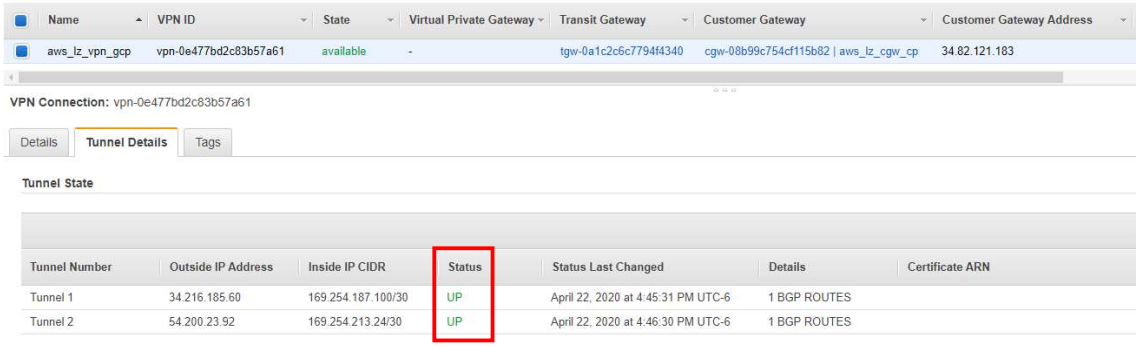



Create tunnel 2 repeating the same operations but using options of tunnel 2 (see “Getting Tunnels configuration” above). This is how it should look like eventually:

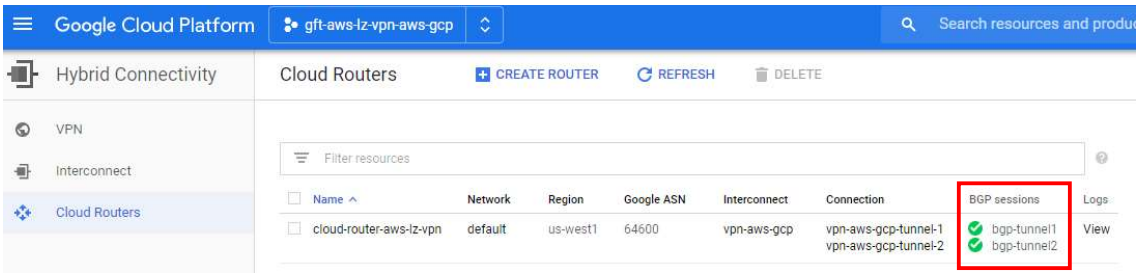



## 7. Check in AWS, connectivity, TGW router table.

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




GCP Cloud Router BGP Sessions Status




**All is UP!**

All the connectivity, attachment, association, propagation, and record into the TGW route table is automatically generated by the BGP dynamic routing.

Transit Gateway Attachment

Filter by tags and attributes or search by keyword

| Name | Transit Gateway attachment ID | Transit Gateway ID | Resource type | Resource ID | State | Associated route table ID | Association state |
|---|---|---|---|---|---|---|---|
| | tgw-attach-01ce88fd192e2d95f | tgw-0a1c2c6c7794f4340 | VPC | vpc-01acddd91006d6c8a | available | - | |
| | tgw-attach-05fc48bfe786b5d35 | tgw-0a1c2c6c7794f4340 | VPC | vpc-04e9799837f21f32a | available | tgw-rtb-0142e93fec2f6ed81 | associated |
| | tgw-attach-0d6a5004a8671b20f | tgw-0a1c2c6c7794f4340 | VPC | vpc-01db1a19a30f3f1f9 | available | tgw-rtb-0142e93fec2f6ed81 | associated |
| | tgw-attach-046d546dc0d0f0b92 | tgw-0a1c2c6c7794f4340 | VPN | vpn-0e477bd2c83b57a61 | available | tgw-rtb-0142e93fec2f6ed81 | associated |
| aws_lz_egress_vpc_attach_615513573213 | tgw-attach-09ef2dd5d47d00ca8 | tgw-0a1c2c6c7794f4340 | VPC | vpc-0203258e0cc80e57e | available | tgw-rtb-0142e93fec2f6ed81 | associated |
| aws_lz_ingress_vpc_attach_615513573213 | tgw-attach-05ee73e1974623033 | tgw-0a1c2c6c7794f4340 | VPC | vpc-0b0e9de9501d97b7b | available | tgw-rtb-0142e93fec2f6ed81 | associated |
| aws_lz_inline_vpc_attach_615513573213 | tgw-attach-0ea1344837e5bf74c | tgw-0a1c2c6c7794f4340 | VPC | vpc-09aff651a5cacbb87 | available | tgw-rtb-0142e93fec2f6ed81 | associated |

Transit Gateway Associations

| Name | Transit Gateway route table ID | Transit Gateway ID | State | Default as |
|---|---|---|---|---|
| | tgw-rtb-0142e93fec2f6ed81 | tgw-0a1c2c6c7794f4340 | available | Yes |

**Transit Gateway Route Table:** tgw-rtb-0142e93fec2f6ed81

Details | **Associations** | Propagations | Routes | Tags

**Create association** | Delete association

Filter by attributes or search by keyword

| Attachment ID | Resource type | Resource ID | State |
|---|---|---|---|
| tgw-attach-046d546dc0d0f0b92 | VPN | vpn-0e477bd2c83b57a61 | associated |
| tgw-attach-09ef2dd5d47d00ca8 | VPC | vpc-0203258e0cc80e57e | associated |
| tgw-attach-05ee73e1974623033 | VPC | vpc-0b0e9de9501d97b7b | associated |
| tgw-attach-05fc48bfe786b5d35 | VPC | vpc-04e9799837f21f32a | associated |
| tgw-attach-0d6a5004a8671b20f | VPC | vpc-01db1a19a30f3f1f9 | associated |
| tgw-attach-0ea1344837e5bf74c | VPC | vpc-09aff651a5cacbb87 | associated |

Transit Gateway Propagations

| Name | Transit Gateway route table ID | Transit Gateway ID | State | Default |
|---|---|---|---|---|
| | tgw-rtb-0142e93fec2f6ed81 | tgw-0a1c2c6c7794f4340 | available | Yes |

**Transit Gateway Route Table:** tgw-rtb-0142e93fec2f6ed81

Details | Associations | **Propagations** | Routes | Tags

**Create propagation** | Delete propagation

Filter by attributes or search by keyword

| Attachment ID | Resource type | Resource ID | State |
|---|---|---|---|
| tgw-attach-046d546dc0d0f0b92 | VPN | vpn-0e477bd2c83b57a61 | enabled |
| tgw-attach-05ee73e1974623033 | VPC | vpc-0b0e9de9501d97b7b | enabled |
| tgw-attach-05fc48bfe786b5d35 | VPC | vpc-04e9799837f21f32a | enabled |
| tgw-attach-09ef2dd5d47d00ca8 | VPC | vpc-0203258e0cc80e57e | enabled |
| tgw-attach-0d6a5004a8671b20f | VPC | vpc-01db1a19a30f3f1f9 | enabled |
| tgw-attach-0ea1344837e5bf74c | VPC | vpc-09aff651a5cacbb87 | enabled |

Transit Gateway Route Table

| Name | Transit Gateway route table ID | Transit Gateway ID | State | Default association route t |
|---|---|---|---|---|
| | tgw-rtb-0142e93fec2f6ed81 | tgw-0a1c2c6c7794f4340 | available | Yes |

**Transit Gateway Route Table:** tgw-rtb-0142e93fec2f6ed81

Details | Associations | Propagations | **Routes** | Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route | Replace route | Delete route

Filter by attributes or search by keyword

| CIDR | Attachment | Resource type | Route type | Route state |
|---|---|---|---|---|
| 0.0.0.0/0 | tgw-attach-09ef2dd5d47d00ca8 \| vpc-0203258e0cc80e57e | VPC | static | active |
| 10.100.0.0/22 | tgw-attach-05fc48bfe786b5d35 \| vpc-04e9799837f21f32a | VPC | propagated | active |
| 10.101.0.0/22 | tgw-attach-0d6a5004a8671b20f \| vpc-01db1a19a30f3f1f9 | VPC | propagated | active |
| 10.138.0.0/20 | 2 Attachments | VPN | propagated | active |
| 10.99.0.0/22 | tgw-attach-09ef2dd5d47d00ca8 \| vpc-0203258e0cc80e57e | VPC | propagated | active |
| 10.99.4.0/22 | tgw-attach-05ee73e1974623033 \| vpc-0b0e9de9501d97b7b | VPC | propagated | active |
| 10.99.8.0/22 | tgw-attach-0ea1344837e5bf74c \| vpc-09aff651a5cacbb87 | VPC | propagated | active |

## 8. AWS Network Manager monitoring tool.

AWS Network Manager Dashboard

aws | Services | Resource Groups

Network manager

Global networks

aws_lz_global_network

Dashboard

Transit gateways

On-premises

Devices

Sites

Network manager > Global networks > aws_lz_global_network

Overview | Details | Geographic | Topology | Events | Monitoring

**aws_lz_global_network Inventory**

Network resources that are part of your global network

1 Transit gateways | 0 Sites | 0 Devices

**Transit gateways VPN status** (1)

Search transit gateways vpn status

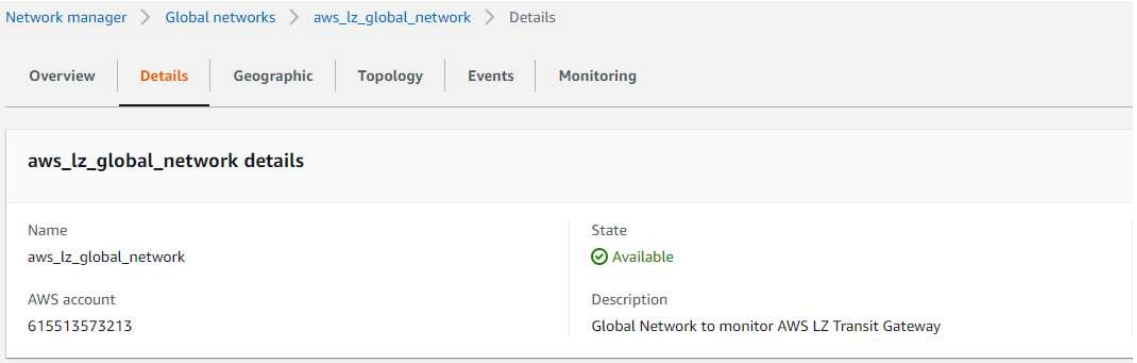
| ID | Name | Region | Down VPN | Impaired VPN | Up VPN |
|---|---|---|---|---|---|
| tgw-0a1c2c6c7794f4340 | aws_lz_tgw_6... | us-west-2 | 0% | 0% | 100% |

**Network events summary**

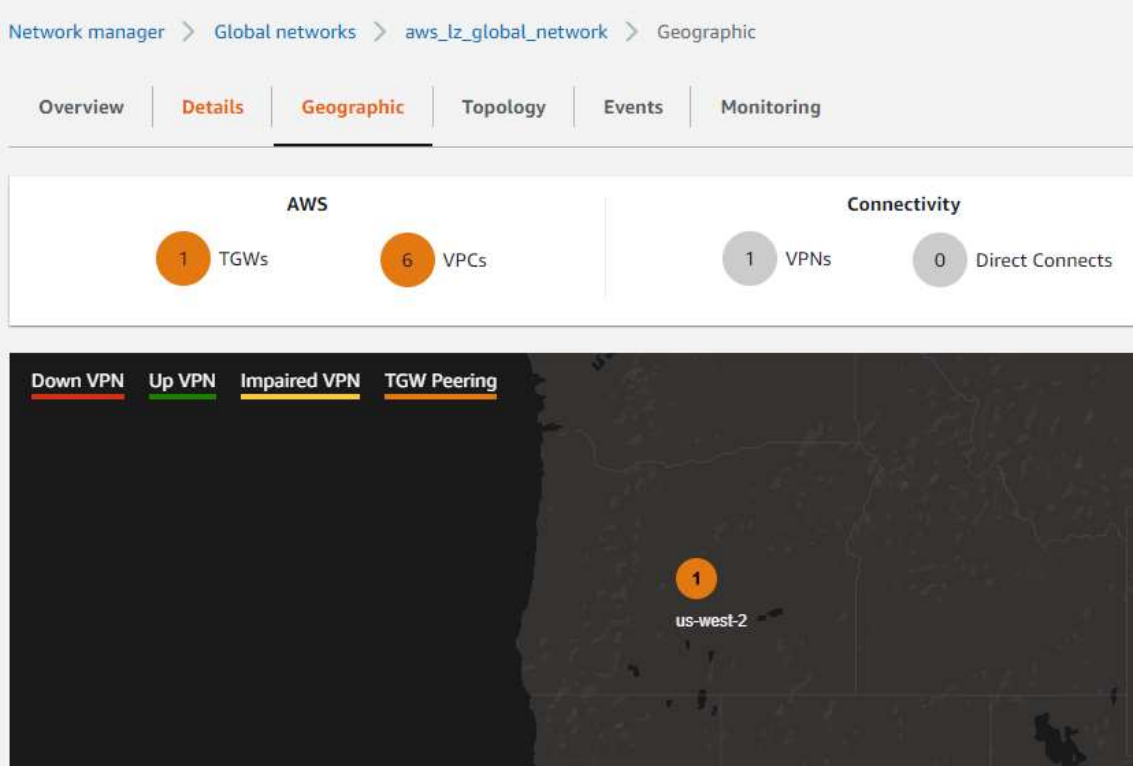
Events

| # | Category | Message | Count |
|---|---|---|---|
| 1 | Network Manager Topology Change | A Site-to-Site VPN connection has been created. | 1 |
| 2 | Network Manager Status Update | IPsec for a VPN connection has gone down. | 2 |
| 3 | Network Manager Status Update | BGP for a VPN connection has gone down. | 2 |
| 4 | Network Manager Routing Update | Routes in one or more Transit Gateway route tables have been installed. | 3 |
| 5 | Network Manager Status Update | IPsec for a VPN connection has come up. | 4 |
| 6 | Network Manager Routing Update | Routes in one or more Transit Gateway route tables have been uninstalled. | 2 |
| 7 | Network Manager Status Update | BGP for a VPN connection has been established. | 4 |

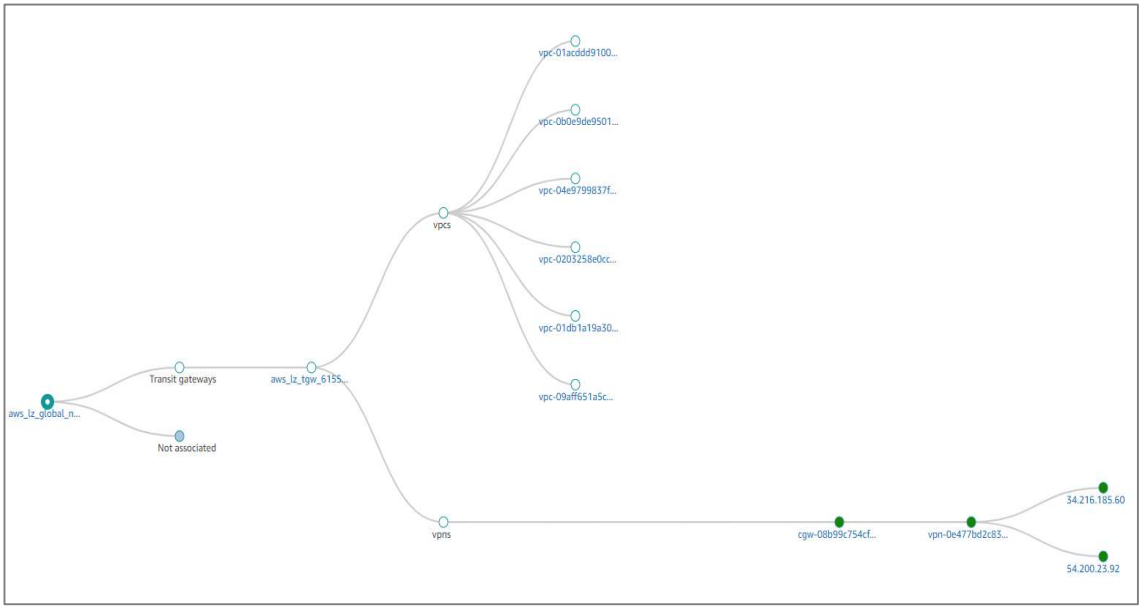
AWS Network Manager details




AWS Network Manager Geographic



## AWS Network Manager Topology




## AWS Network Manager Events

Network manager > Global networks > aws_lz_global_network > Events

Overview | Details | Geographic | Topology | Events | Monitoring

### aws_lz_global_network events

1h 3h 12h 1d 3d 1w custom

Events

| # | Region | Message | Resource | Timestamp |
|---|---|---|---|---|
| 1 | us-west-2 | IPsec for a VPN connection has come up. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:46:21.000Z |
| 2 | us-west-2 | IPsec for a VPN connection has gone down. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:46:17.000Z |
| 3 | us-west-2 | Routes in one or more Transit Gateway route tables have been installed. | arn:aws:ec2:us-west-2:615513573213:transit-gateway/tgw-0a1c2c6c7794f4340 | 2020-04-22T22:45:21.000Z |
| 4 | us-west-2 | BGP for a VPN connection has been established. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:45:20.000Z |
| 5 | us-west-2 | BGP for a VPN connection has gone down. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:45:20.000Z |
| 6 | us-west-2 | IPsec for a VPN connection has come up. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:45:16.000Z |
| 7 | us-west-2 | BGP for a VPN connection has been established. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:45:16.000Z |
| 8 | us-west-2 | Routes in one or more Transit Gateway route tables have been uninstalled. | arn:aws:ec2:us-west-2:615513573213:transit-gateway/tgw-0a1c2c6c7794f4340 | 2020-04-22T22:45:15.000Z |
| 9 | us-west-2 | BGP for a VPN connection has been established. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:45:10.000Z |
| 10 | us-west-2 | BGP for a VPN connection has gone down. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:45:10.000Z |
| 11 | us-west-2 | Routes in one or more Transit Gateway route tables have been installed. | arn:aws:ec2:us-west-2:615513573213:transit-gateway/tgw-0a1c2c6c7794f4340 | 2020-04-22T22:44:45.000Z |
| 12 | us-west-2 | IPsec for a VPN connection has come up. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:44:40.000Z |
| 13 | us-west-2 | Routes in one or more Transit Gateway route tables have been uninstalled. | arn:aws:ec2:us-west-2:615513573213:transit-gateway/tgw-0a1c2c6c7794f4340 | 2020-04-22T22:44:15.000Z |
| 14 | us-west-2 | IPsec for a VPN connection has gone down. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:44:10.000Z |
| 15 | us-west-2 | Routes in one or more Transit Gateway route tables have been installed. | arn:aws:ec2:us-west-2:615513573213:transit-gateway/tgw-0a1c2c6c7794f4340 | 2020-04-22T22:43:34.000Z |
| 16 | us-west-2 | BGP for a VPN connection has been established. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:43:28.000Z |
| 17 | us-west-2 | IPsec for a VPN connection has come up. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:43:10.000Z |
| 18 | us-west-2 | A Site-to-Site VPN connection has been created. | arn:aws:ec2:us-west-2:615513573213:vpn-connection/vpn-0e477bd2c83b57a61 | 2020-04-22T22:31:34.000Z |

AWS Network Manager Monitoring