How to build HA VPN connection between Google Cloud & AWS

Create a VPC network

Name: vpc-aws-gcp-vpn

Description:

**New Subnet:**

Name: subnet-us-east1

Description:

Region: us-east1

IP address range: 10.0.0.0/24

Done.

Dynamic routing mode

Global: YES

**CREATE**

Firewall =🡺 Create a firewall rule: icmp & SSH

Name: allow-icmp

Description:

Network: vpc-aws-gcp-vpn

Targets: All instances

Source IP ranges: 0.0.0.0/0

Other protocols 🡺 icmp

**CREATE**

Name: allow-ssh-from-console

Description:

Network: vpc-aws-gcp-vpn

Targets: All instances in the network

Source IP ranges: 35.235.240.0/20

Tcp protocols 🡺 22

**CREATE**

**AWS**

Virtual Private Cloud

Your VPC 🡺 **Create VPC**

Name tag: vpc-aws-gcp-vpn

IPv4 CIDR block: 10.1.0.0/16

Create VPC

Subnets 🡺 Create subnet

Select VPC 🡺 vpc-aws-gcp-vpn

Subnet name: subnet-us-east-2

Availability Zone: us-east-2a

IPv4 subnet CIDR block: 10.1.0.0/16

Create subnet

Route Tables

Name Route: rt-aws-gcp-vpc

Select VPC: vpc-aws-gcp-vpn

Create route table

Subnet associations

EDIT (WITHOUT)

Select: subnet-us-east-2

Save associations

Internet Gateways 🡺 Create Internet gateway

Name: igw-aws-gcp-vpn

 Create Internet gateway

**Attach to a VPC 🡺 top of page!!**

Select: vpc-aws-gcp-vpn

Attach internet gateway

Route Tables: 🡺 Routes

Edit routes 🡺 rt-aws-gcp-vpc

Target: Internet gateway 🡺 your gateway

Add route: 0.0.0.0/0

Save Changes

Your VPC 🡺 ACTION 🡺 Edit VPC

Edit DNS hostnames: Enable

Save changes:

**GCP**

Hybrid Connectivity 🡺Cloud Routers

**Create a cloud router**

Name: cloud-router-aws-gcp-vpn

Description:

Network: vpc-aws-gcp-vpn

Region: us-east1

Google ASN: 65420

**CREATE**

VPN 🡺 Create VPN Connection

HA VPN

CONTINUE

Create a VPN

Name: vpn-gateway-aws-gcp

Network: vpc-aws-gcp-vpn

Region: us-east1

**Create & continue**

**Now You have two Interfaces with addresses**

**Copy your IP addresses here !!!**

**0:34.152.79.193 1:34.177.47.96**

**AWS**

**VIRTUAL PRIVATE NETWORK**

**Customer Gateways 🡪 Create 2 Customer Gateway**

**Name:** cg-aws-gcp-vpn-1

**BGP ASN**: 65420

**IP Address:** 34.152.79.193

**Create Customer Gateway**

**Customer Gateways 🡪 Create 2 Customer Gateway**

**Name:** cg-aws-gcp-vpn-2

**BGP ASN**: 65420

**IP Address:** 34.177.47.96

**Create Customer Gateway**

Virtual Private Gateways 🡺 Create Virtual Private Gateway

**Name tag:** vpg-aws-gcp

**ASN:** Custom ASN 🡺 **DIFFERENT CUST. GATEWAY**

64512

**Create Virtual Private Gateway**

**ACTION:**

**Attach to VPC:** vpc-aws-gcp-vpn

**Attach to VPC**

Route Tables:

**Select Route:**

Route propagation 🡺 Edit route propagation

**Select:** Enable

**Save**

**Site-to-Site VPN Connections**

**Create VPN Connection**

**Name tag: vpn-aws-gcp-1**

**Virtual Private Gateway: vpg-aws-gcp**

**Customer Gateway ID: cgw- cg-aws-gcp-vpn-1**

**Advanced Options for Tunnel 1**

**Edit Tunnel 1 Options**

**Xxx256 & 14 only**

**Ikev2**

**Advanced Options for Tunnel 2**

**Edit Tunnel 2 Options**

**Xxx256 & 14 only**

**Ikev2**

**Create VPN Connection**

**Site-to-Site VPN Connections**

Create VPN Connection

Name tag: vpn-aws-gcp-2

Virtual Private Gateway: vpg-aws-gcp

Customer Gateway ID: cg-aws-gcp-vpn-2

Advanced Options for Tunnel 1

Edit Tunnel 1 Options

Xxx256 & 14 only

Ikev2

Advanced Options for Tunnel 2

Edit Tunnel 2 Options

Xxx256 & 14 only

Ikev2

**Create VPN Connection**

**Site-to-Site VPN Connections 🡺**

**Download Configuration**

SELECT 🡺Vpn-aws-gcp-1

Vender = Generic

Platform = Generic

Software = Vender Agnostic

IKE version = ikev2

**Download** file name = 1-vpn.txt

SELECT 🡺Vpn-aws-gcp-2

Vender = Generic

Platform = Generic

Software = Vender Agnostic

IKE version = ikev2

**Download** file name = 2-vpn.txt

GCP

Back to Create a VPC

Peer VPN gateway name

Create new peer VPN gateway

Add a peer VPN gateway

Name = pvg-aws-gcp-vpn

Interfaces = four interfaces

**USING THE 2 FILES DOWNLOAD**

**Outside IP addresses**

1-vpn.txt Interface 0 IP address = Virtual Private Gateway

1-vpn.txt Interface 1 IP address = Virtual Private Gateway

2-vpn.txt Interface 2 IP address = Virtual Private Gateway

2-vpn.txt Interface 3 IP address = Virtual Private Gateway

**Create**

Cloud Router = cloud-router-aws-gcp-vpn

Name = vpm-tunnel-1-1

Description

IKE version = IKEv2

IKE pre-shared key = [ 1-vpn.txt Pre-Shared Key ]

Name = vpm-tunnel-1-2

Description

IKE version = IKEv2

IKE pre-shared key = [ 1-vpn.txt Pre-Shared Key ]

Name = vpm-tunnel-2-1

Description

IKE version = IKEv2

IKE pre-shared key = [ 2-vpn.txt Pre-Shared Key ]

Name = vpm-tunnel-2-2

Description

IKE version = IKEv2

IKE pre-shared key = [ 2-vpn.txt Pre-Shared Key ]

**Create & continue**

**Create a VPN 🡺 8 Inside IP Address**

**Configure**

**Create GBP session 🡺 4 BGP sessions**

**Name = bgp-tunnel-1-1**

**Peer ASN = 64512 [same as AWS]**

**Allocate BGP IPv4 address = Manually**

**Cloud Router BGP IP = [Inside IP-Customer Gateway]**

BGP peer IP = [Inside IP-Virtual Private Gateway]

**Save and continue**

**Configure**

**Create GBP session**

**Name = bgp-tunnel-1-2**

**Peer ASN = 64512 [same as AWS]**

**Allocate BGP IPv4 address = Manually**

**Cloud Router BGP IP = [Inside IP-Customer Gateway]**

BGP peer IP = [Inside IP-Virtual Private Gateway]

**Save and continue**

**Configure**

**Create GBP session**

**Name = bgp-tunnel-2-1**

**Peer ASN = 64512 [same as AWS]**

**Allocate BGP IPv4 address = Manually**

**Cloud Router BGP IP = [Inside IP-Customer Gateway]**

**BGP peer IP = [Inside IP-Virtual Private Gateway]**

**Save and continue**

**Configure**

**Create GBP session**

**Name = bgp-tunnel-2-2**

**Peer ASN = 64512 [same as AWS]**

**Allocate BGP IPv4 address = Manually**

**Cloud Router BGP IP = [Inside IP-Customer Gateway]**

**BGP peer IP = [Inside IP-Virtual Private Gateway]**

**Save and continue**