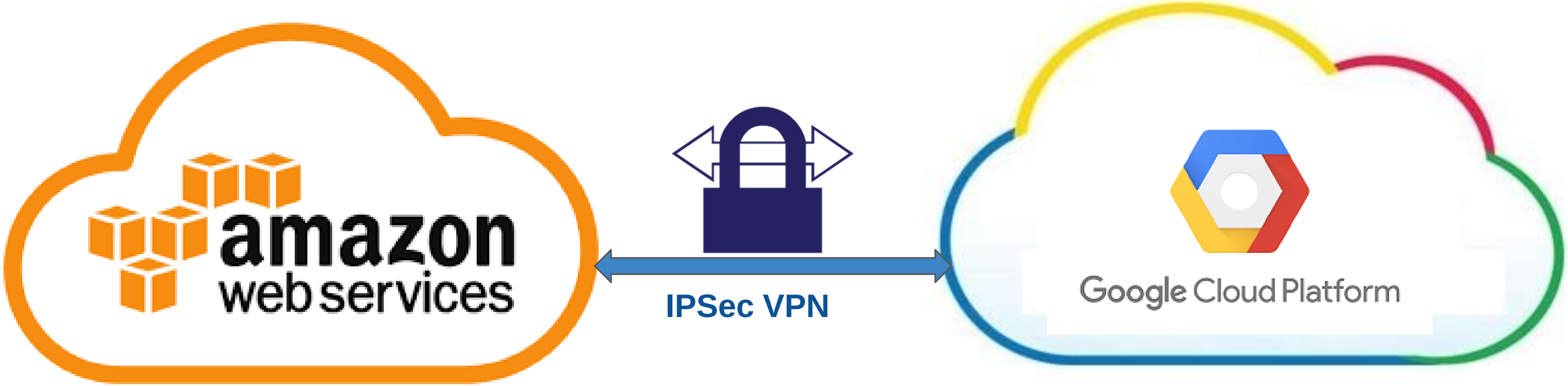
AWS - Google Site to Site VPN using BGP Routing

What do we want to achieve?

Site to Site VPN - IPSec (Dynamic Routing - BGP)

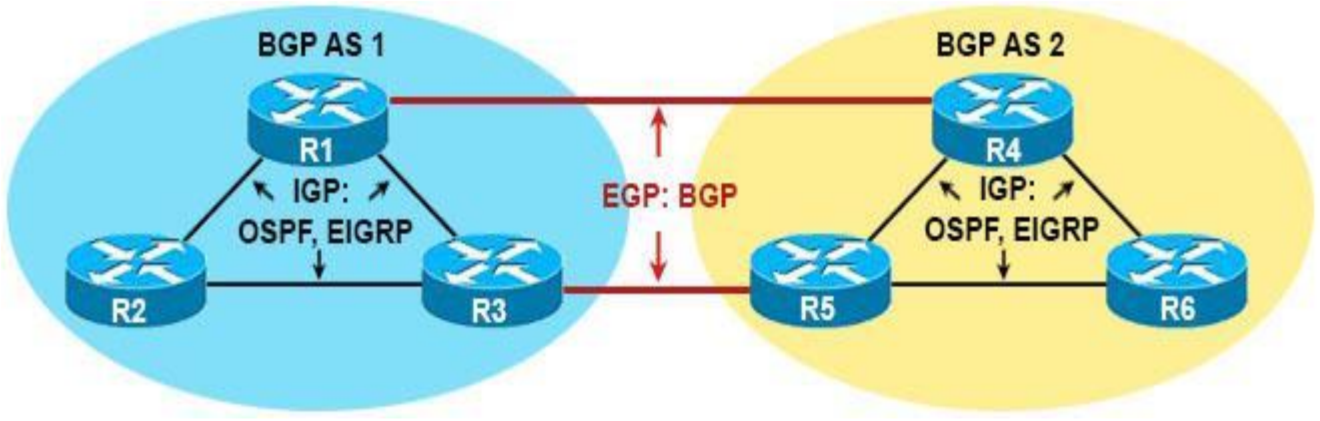


BGP related terminologies

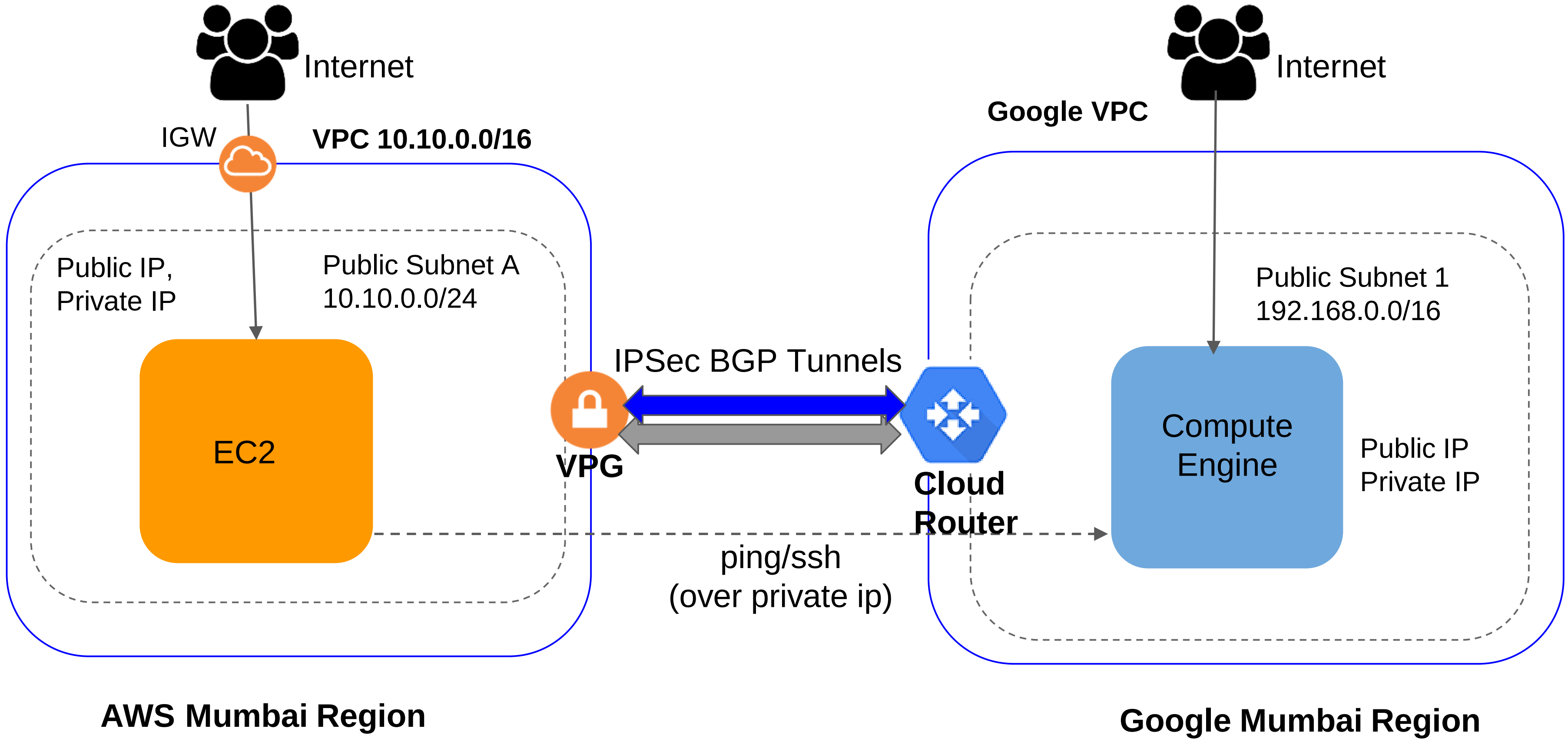
- BGP - Border Gateway Protocol
- AS - Autonomous Systems
- ASN - Autonomous System Number
- IPSec - Internet Protocol Security
- IKE - Internet Key Exchange
- PSK - Pre Shared Key

Understanding BGP - Border Gateway Protocol

- *Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet*
- iBGP vs eBGP



Network Topology



What we need?

1. AWS VPC and Subnet
2. Google VPC and Subnet
3. AWS Virtual Private Gateway and Customer Gateway
4. Google Cloud Router
5. AWS VPN Connection and Google VPN Connection
6. BGP Neighbours IP Addresses (169.254.0.0/16 range)
7. For Testing:
   a. EC2 instance in AWS Subnet
   b. Compute Engine in Google Subnet

Steps

1. AWS: Create “aws-vpc” in AWS Mumbai Region (ap-south-1) and create a public subnet
    a. VPC CIDR - 10.10.0.0/16
    b. Create Internet Gateway and attach to VPC
    c. Create a subnet with CIDR - 10.10.0.0/24
    d. Create a Route Table and add route for 0.0.0.0/0 through target as Internet Gateway
    e. Attach Route table to Subnet to make this subnet Public
2. GCP: Reserve external IP in asia-south1 region
3. AWS: Create Virtual Private Gateway and attach to “aws-vpc”
    1. ASN - Amazon Default ASN
3. AWS: Create Customer Gateway
    1. Routing - Dynamic
    2. ASN - 65000
    3. IP Address - Google side external IP that was reserved in Step 2 above.
4. AWS: Enable Route table Route Propagation and add Virtual Private Gateway route

Steps

6. AWS: Create VPN Connection (Dynamic)
    1. Routing Options - Dynamic (requires BGP)
    2. Inside CIDRS for 2 Tunnels - 169.254.0.4/30, 169.254.0.8/30
    3. Specify pre-shared keys for both the tunnels
7. AWS: Wait for VPN connection to be active
    1. Download VPN Configuration (generic). We will call this file “**AWS Config file**” here onwards.
8. GCP: Create “gcp-vpc” in Mumbai region (asia-south1) and a subnet
    1. GCP: Create a subnet in “gcp-vpc”
        1. Region - asia-south1
        2. CIDR - 192.168.0.0/16
    2. GCP: Create Google Cloud Router
        1. Network - gcp-vpc
        2. Region - asia-south1
        3. Google ASN - 65000 (same as provided in step 4.2)

Steps

9. GCP: Create VPN Connection
    1. **Network** - gcp-vpc
    2. **Region** - asia-south1
    3. **IP address** - Google VPC external IP Address that we had reserved in Step 2
    4. **Tunnel 1**
        1. **Remote peer IP address** - From AWS Config file: IPSec Tunnel #1 Outside IP Address - Virtual Private Gateway
        2. **IKE version** - IKEv1
        3. **Pre-shared Key** - From AWS Config file: IPSec Tunnel #1 Pre-Shared Key
        4. **Routing Options** - Dynamic (BGP)
        5. **Cloud Router** - Created in Step 9 above
        6. **Edit BGP session**
            1. **Peer ASN** - From AWS config file: Tunnel #1 BGP Configuration options Virtual Private Gateway ASN
            2. **Cloud Router BGP IP** - From AWS Config file: Inside IP Addresses - Customer Gateway
            3. **BGP Peer IP** - From AWS Config file: Inside IP Addresses - Virtual Private Gateway
    5. **Tunnel 2 -** Repeat 10.4 steps using IPSec Tunnel #2 details from AWS Config file
10. Wait for 5 minutes and check the status of Tunnel at both the ends. It should be UP.

Testing the BGP Routing - Connectivity Test

1. Launch EC2 instance in AWS Public Subnet
   a. Security group must allow SSH from your IP address
2. Launch Compute Engine instance in Google Subnet
   a. Firewall must allow SSH/Ping from AWS VPC CIDR i.e 10.10.0.0/16
3. Connect to EC2 over SSH
   a. Run ping <compute engine private ip e.g 192.168.0.2>
4. Ping command should be successful
5. Optionally we can also test the connectivity in another direction by logging into Google Compute engine instance and ping to EC2 instance over private IP
   a. Make sure EC2 security group Ingress allows ICMP from Google VPC CIDR
   b. Google compute engine Firewall Egress allows ICMP to AWS VPC CIDR

Testing the BGP Routing - Dynamic Route test

1. Add a new subnet to Google VPC Network with CIDR 172.31.0.0/16
2. Wait for some time and verify in AWS VPC Route Table that new route (172.31.0.0/16) has been automatically added as a new propagated Route table entry
3. Optionally, extend AWS VPC CIDR and add new CIDR to AWS VPC e.g 10.20.0.0/16
4. Verify at Google VPC Connection that there is new route (10.20.0.0/16) detected and added on google side