**Virtual Private Networks (VPN)**

**Overview**

In this lab, you establish VPN tunnels between two networks in separate regions such that a VM in one network can ping a VM in the other network over its internal IP address.

**Objectives**

* In this lab, you learn how to perform the following tasks:
* Create VPN gateways in each network
* Create VPN tunnels between the gateways

**Task 1: Explore the networks and instances**

Two custom networks with VM instances have been configured for you. For the purposes of the lab, both networks are VPC networks within a Google Cloud project. However, in a real-world application, one of these networks might be in a different Google Cloud project, on-premises, or in a different cloud. Check console to view the network and firewall rules.

Go your instance and ssh into it your vm-1 instance and ping the the internal IP and External IP on vm-2 instance

***ping -c 3 <Enter server-2's external IP address here>***

***ping -c 3 <Enter server-2's Internal IP address here>***

You notice you cannot connect to vm-2 using the internal IP.

Do the same for vm-1, ssh into vm-2 and ping the internal and External IP addresses

***ping -c 3 <Enter server-1's external IP address here>***

***ping -c 3 <Enter server-1's Internal IP address here>***

This applies here too. you can connect to vm-1 using it extrernal ip address but you cannot connect to it using it internal ip addresss

**Task 2: Create the VPN gateways and tunnels**

Establish private communication between the two VM instances by creating VPN gateways and tunnels between the two networks.

**Reserve two static IP addresses**

Reserve one static IP address for each VPN gateway.

Using the Cloud SDK enter the command to reserve two IP address.

This command reserves an IP at us-central1

***gcloud compute addresses create vpn1-static-ip --project=qwiklabs-gcp-00-4ea209d27602 --region=us-central1***

The second reserves the IP at europe-west1

***gcloud compute addresses create vpn2-static-ip --project=qwiklabs-gcp-00-4ea209d27602 --region=europe-west1***

**Create the vpn-1 gateway and tunnel1to2**

To create a gateway and a vpn tunnel to vm-2 enter the command

This command creates the vpn gateway and gives it a name(vpn-1)

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" target-vpn-gateways create "vpn-1" --region "us-central1" --network "vpn-network-1"***

This allows firewall rules and also attaches the reserve IP address to your vm

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" forwarding-rules create "vpn-1-rule-esp" --region "us-central1" --address "35.223.66.183" --ip-protocol "ESP" --target-vpn-gateway "vpn-1"***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" forwarding-rules create "vpn-1-rule-udp500" --region "us-central1" --address "35.223.66.183" --ip-protocol "UDP" --ports "500" --target-vpn-gateway "vpn-1"***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" forwarding-rules create "vpn-1-rule-udp4500" --region "us-central1" --address "35.223.66.183" --ip-protocol "UDP" --ports "4500" --target-vpn-gateway "vpn-1"***

This command creates the vpn tunnel from your vm-1 to vm-2

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" vpn-tunnels create "tunnel1to2" --region "us-central1" --peer-address "35.241.133.167" --shared-secret "gcprocks" --ike-version "2" --local-traffic-selector "0.0.0.0/0" --target-vpn-gateway "vpn-1"***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" routes create "tunnel1to2-route-1" --network "vpn-network-1" --next-hop-vpn-tunnel "tunnel1to2" --next-hop-vpn-tunnel-region "us-central1" --destination-range "10.1.3.0/24"***

**Create the vpn-2 gateway and tunnel2to1**

This command creates a vpn gateway and gives it a name(vpn-2)

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" target-vpn-gateways create "vpn-2" --region "europe-west1" --network "vpn-network-2"***

***This allows firewall rules and also attaches the reserve IP address to your vm***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" forwarding-rules create "vpn-2-rule-esp" --region "europe-west1" --address "35.241.133.167" --ip-protocol "ESP" --target-vpn-gateway "vpn-2"***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" forwarding-rules create "vpn-2-rule-udp500" --region "europe-west1" --address "35.241.133.167" --ip-protocol "UDP" --ports "500" --target-vpn-gateway "vpn-2"***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" forwarding-rules create "vpn-2-rule-udp4500" --region "europe-west1" --address "35.241.133.167" --ip-protocol "UDP" --ports "4500" --target-vpn-gateway "vpn-2"***

This command creates the vpn tunnel from your vm-2 to vm-1

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" vpn-tunnels create "vpn-2-tunnel-1" --region "europe-west1" --peer-address "35.223.66.183" --shared-secret "gcprocks" --ike-version "2" --local-traffic-selector "0.0.0.0/0" --target-vpn-gateway "vpn-2"***

***gcloud compute --project "qwiklabs-gcp-00-4ea209d27602" routes create "vpn-2-tunnel-1-route-1" --network "vpn-network-2" --next-hop-vpn-tunnel "vpn-2-tunnel-1" --next-hop-vpn-tunnel-region "europe-west1" --destination-range "10.5.4.0/24"***

**Task 3: Verify VPN connectivity**

Wait for the VPN tunnels status to change to Established for both tunnels before continuing.

Go your instance and ssh into it your vm-1 instance and ping the the internal IP and External IP on vm-2 instance

***ping -c 3 <Enter server-2's external IP address here>***

***ping -c 3 <Enter server-2's Internal IP address here>***

You are now able to connect to your vm-2 using both the internal and external IP address.

Also ssh into vm-2 and ping the internal and External IP addressess of your vm-1

***ping -c 3 <Enter server-1's external IP address here>***

***ping -c 3 <Enter server-1's Internal IP address here>***

This time you are able to connect to vm-1 using the internal and external IP address