Implement Private Google Access and Cloud NAT

### **Objectives**

In this lab, you learn how to perform the following tasks:

* Configure a VM instance that doesn't have an external IP address
* Connect to a VM instance using an Identity-Aware Proxy (IAP) tunnel
* Enable Private Google Access on a subnet
* Configure a Cloud NAT gateway
* Verify access to public IP addresses of Google APIs and services and other connections to the internet

## Task 1. Create the VM instance

Create a VPC network with some firewall rules and a VM instance that has no external IP address, and connect to the instance using an IAP tunnel.

### **Create a VPC network and firewall rules**

First, create a VPC network for the VM instance and a firewall rule to allow SSH access.

1. In the Cloud Console, click **Activate Cloud Shell** (Cloud Shell).
2. If prompted, click **Continue**.
3. Copy the following command in the cloud shell to create privatenet nerwork:  
     
   gcloud compute networks create privatenet--subnet-mode=custom --bgp-routing-mode=regional
4. To create subnet privatenet-us on privatenet network run the following command  
     
   gcloud compute networks subnets create privatenet-us --project=qwiklabs-gcp-03-702c7a7c1f83 --range=10.130.0.0/20 --network=privatenet --region=us-central1
5. Copy the following command in the cloud shell to create firewall rules that allow ssh traffic on privatenet network:  
     
   gcloud compute firewall-rules create privatenet-allow-ssh --direction=INGRESS --priority=1000 --network=privatenet --action=ALLOW --rules=tcp:22 --source-ranges=35.235.240.0/20

### **Create the VM instance with no public IP address**

1. To create vm-internal vm that has no external pi address, run the following command:  
     
   gcloud beta compute instances create vm-internal --zone=us-central1-c --machine-type=n1-standard-1 --subnet=privatenet-us --no-address --maintenance-policy=MIGRATE --scopes=https://www.googleapis.com/auth/devstorage.read\_only,https://www.googleapis.com/auth/logging.write,https://www.googleapis.com/auth/monitoring.write,https://www.googleapis.com/auth/servicecontrol,https://www.googleapis.com/auth/service.management.readonly,https://www.googleapis.com/auth/trace.append --image=debian-10-buster-v20200902 --image-project=debian-cloud --boot-disk-size=10GB --boot-disk-type=pd-standard --boot-disk-device-name=vm-internal --no-shielded-secure-boot --no-shielded-vtpm --no-shielded-integrity-monitoring --reservation-affinity=any

### **SSH to vm-internal to test the IAP tunnel**

1. To connect to vm-internal, run the following command:

gcloud compute ssh vm-internal --zone us-central1-c --tunnel-through-iap

1. If prompted about continuing, type Y.
2. When prompted for a passphrase, press ENTER.
3. When prompted for the same passphrase, press ENTER.
4. To test the external connectivity of vm-internal, run the following command:

ping -c 2 www.google.com

This should not work because vm-internal has no external IP address!

1. Wait for the ping command to complete.
2. To return to your Cloud Shell instance, run the following command:

Exit

## Task 2. Enable Private Google Access

### **Create a Cloud Storage bucket**

1. To create bucket run the following command:  
     
   gsutil mb gs://<bucket\_name>  
     
   replace <bucket\_name> with unique bucket name you can use your project id as a bucket name
2. Note the name of your storage bucket for the next subtask. It will be referred to as [my\_bucket]

### **Copy an image file into your bucket**

1. In Cloud Shell, run the following command, replacing [my\_bucket] with your bucket's name:

gsutil cp gs://cloud-training/gcpnet/private/access.svg gs://[my\_bucket]

### **Access the image from your VM instance**

1. In Cloud Shell, to try to copy the image from your bucket, run the following command, replacing [my\_bucket] with your bucket's name:

gsutil cp gs://[my\_bucket]/\*.svg .

1. o connect to vm-internal, run the following command:

gcloud compute ssh vm-internal --zone us-central1-c --tunnel-through-iap

1. To try to copy the image to vm-internal, run the following command, replacing [my\_bucket] with your bucket's name:

gsutil cp gs://[my\_bucket]/\*.svg .  
  
This should not work: **vm-internal** can only send traffic within the VPC network because Private Google Access is disabled (by default)

1. Press **Ctrl+C** to stop the request.

To enable private google access for privatenet-us subnet, run the following command:  
  
gcloud compute networks subnets update privatenet-us --region=us-central1 --enable-private-ip-google-access

1. to try to copy the image to vm-internal, run the following command, replacing [my\_bucket] with your bucket's name:

gsutil cp gs://[my\_bucket]/\*.svg .

1. To return to your Cloud Shell instance, run the following command:

Exit

## Task 3. Configure a Cloud NAT gateway

### **Try to update the VM instances**

1. In Cloud Shell, to try to re-synchronize the package index, run the following:

sudo apt-get update

The output should finish like this (do not copy; this is example output):

...

Reading package lists... Done

1. To connect to vm-internal, run the following command:

gcloud compute ssh vm-internal --zone us-central1-c --tunnel-through-iap

1. If prompted, type Y to continue.
2. To try to re-synchronize the package index of vm-internal, run the following command:

sudo apt-get update

This should only work for Google Cloud packages because vm-internal only has access to Google APIs and services!

1. Press Ctrl+C to stop the request.

### **Configure a Cloud NAT gateway**

1. We first need to create cloud router by the following command   
     
   gcloud compute routers create nat-router --region=us-central1 --network=privatenet --asn=65470
2. To create nat gateway run the following command:  
     
   gcloud compute routers nats create nat-config --router=nat-router --auto-allocate-nat-external-ips --nat-all-subnet-ip-ranges --enable-logging  
     
   note: this command also enables logging

### **Verify the Cloud NAT gateway**

1. to try to re-synchronize the package index of vm-internal, run the following command:

sudo apt-get update

The output should finish like this (do not copy; this is example output):

Reading package lists... Done

This should work because vm-internal is using the NAT gateway!

1. To return to your Cloud Shell instance, run the following command:

Exit

## Task 4. view logs with Cloud NAT Logging

### **Viewing Logs**

1. To view nat gateway logging run the following command:  
     
   gcloud logging read 'resource.type=nat\_gateway' --format=json  
     
   note this command will view update logs of vm-internal as logs is enabled on creating the NAT gateway