Lab: Firewall Rule

1. Go to VPC network.

2. Go to the Firewall Rules.

3. Ensure that Port is not equal to 22 and Action is not set to Allow.

4. Ensure IP Ranges is not equal to 0.0.0.0/0 under Source filters.

From Google Cloud CLI

gcloud compute firewall-rules list -- format=table'(name,direction,sourceRanges,allowed)'

From Google Cloud Console

1. Go to VPC Network.

2. Go to the Firewall Rules.

3. Click the Firewall Rule you want to modify.

4. Click Edit.

5. Modify Source IP ranges to specific IP.

6. Click Save.

Lab:

From Google Cloud Console

1. Go to VPC network.

2. Go to the Firewall Rules.

3. Ensure Port is not equal to 3389 and Action is not Allow.

4. Ensure IP Ranges is not equal to 0.0.0.0/0 under Source filters.

From Google Cloud CLI

gcloud compute firewall-rules list --format=table'(name,direction,sourceRanges,allowed.ports)'

From Google Cloud Console

1. Go to VPC Network.

2. Go to the Firewall Rules.

3. Click the Firewall Rule to be modified.

4. Click Edit.

5. Modify Source IP ranges to specific IP.

6. Click Save

Flow Log enablement

From Google Cloud Console

1. Go to the VPC network GCP Console visiting

<https://console.cloud.google.com/networking/networks/list>

2. From the list of network subnets, make sure for each subnet:

• Flow Logs is set to On

• Aggregation Interval is set to 5 sec

• Include metadata checkbox is checked

• Sample rate is set to 100%

Gcloud cli

gcloud compute networks subnets list --format json | \ jq -r

To enable vpc flow from cli

To enable VPC Flow Logs for a network subnet, run the following command:

gcloud compute networks subnets update [SUBNET\_NAME] --region [REGION] --enable-flow-logs --logging-aggregation-interval=interval-5-sec --loggingflow-sampling=1 --logging-metadata=include-all

Lab3:

From Google Cloud Console

1. See all load balancers by visiting <https://console.cloud.google.com/netservices/loadbalancing/loadBalancers/list>.

2. For each load balancer for SSL (Proxy) or HTTPS, click on its name to go the Load balancer details

3. Ensure that each target proxy entry in the Frontend table has an SSL Policy configured.

4. Click on each SSL policy to go to its SSL policy details page.

5. Ensure that the SSL policy satisfies one of the following conditions

has a Min TLS set to TLS 1.2 and Profile set to Modern profile, or has Profile set to Restricted. Note that a Restricted profile effectively require clients to use TLS 1.2 regardless of the chosen minimum TLS version,

From Google Cloud CLI

1. List all TargetHttpsProxies and TargetSslProxies.

gcloud compute target-https-proxies list

gcloud compute target-ssl-proxies list

2. For each target proxy, list its properties:

gcloud compute target-https-proxies describe TARGET\_HTTPS\_PROXY\_NAME

gcloud compute target-ssl-proxies describe TARGET\_SSL\_PROXY\_NAME

Lab4:

From Google Cloud Console

If the TargetSSLProxy or TargetHttpsProxy does not have an SSL policy configured,

create a new SSL policy. Otherwise, modify the existing insecure policy.

1. Navigate to the SSL Policies page by visiting:

<https://console.cloud.google.com/net-security/sslpolicies>

2. Click on the name of the insecure policy to go to its SSL policy details page.

3. Click EDIT.

4. Set Minimum TLS version to TLS 1.2.

5. Set Profile to Modern or Restricted.