Lab

From Google Cloud Console

1. Go to the Cloud Console VPC network > Firewall rules.

2. Select the checkbox next to the following rules:

o default-allow-http

o default-allow-https

o default-allow-internal

3. Click Delete.

4. Click Create firewall rule and set the following values:

o Name: allow-iap-traffic

o Targets: All instances in the network

o Source IP ranges (press Enter after you paste each value in the box, copy

each full CIDR IP address):

▪ IAP Proxy Addresses 35.235.240.0/20

▪ Google Health Check 130.211.0.0/22

▪ Google Health Check 35.191.0.0/16

o Protocols and ports:

▪ Specified protocols and ports required for access and management of your app. For example most health check connection protocols would be covered by;

▪ tcp:80 (Default HTTP Health Check port)

▪ tcp:443 (Default HTTPS Health Check port)

Note: if you have custom ports used by your load balancers, you will need to list them here

5. When you're finished updating values, click Create.

Lab 2:

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.

6. Alternatively, if teh user selects the profile Custom, make sure that the following

features are disabled:

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA