Access a firewall and create a rule

CREATE A FIREWALL RULE:

1. In the Google Cloud console, click the **Navigation menu** (☰).
2. Select **VPC Network > Firewall**. The **Firewall policies** page displays.

Note: *If a message is displayed stating that you don't have the required permissions to view the firewall policies inherited by this project, you can disregard it and continue with the next steps.*

3. On the toolbar, click **+ Create Firewall Rule**. The **Create a firewall rule** dialog displays.

4. Specify the following, and leave the remaining settings as their defaults:

Field	**Value**
Name	allow-http-ssh
Logs	On
Network	vpc-net
Targets	Specified target tags
Target tags	http-server
Source filter	IPv4 ranges
Source IPv4 ranges	0.0.0.0/0
In the **Protocols and ports** section	Select **Specified protocols and ports** Select the **TCP** checkbox In the **Ports** field enter **80, 22**

5. Click **Create**.

GENERATE HTTP NETWORK TRAFFIC

1. In the Google Cloud console, click the **Navigation menu** (≡).

2. Select **Compute Engine** > **VM instances**. The **VM instances** page opens.

3. For **web-server**, click on the **External IP** link to access the server.

(Alternatively, you can add the **External IP** value to **http://EXTERNAL_IP/** in a new browser window or tab.) A default web page should display.

Next, you need to find the IP address of the computer you're using.

4. Access your IP address using the following link whatismyip.com. It will directly reply with your IP.

Note: *Ensure that the IP address only contains numerals (IPv4) and is not represented in hexadecimal (IPv6).*

5. Copy the **IP address** and save it in a notepad. You'll need to use this in the next task.

ANALYZE THE WEB SERVER FLOW LOGS

1. In the Google Cloud console, click the **Navigation menu** (≡).

2. Select **Logging** > **Logs Explorer**. The **Logs Explorer** page opens. (You may need to expand the **More Products** drop-down menu within the **Navigation** menu and locate Logging under **Operations**.)

3. On the left side of the **Logs Explorer** page, the **Log fields** pane is presented. The **Resource type** and **Severity** sections are available. Under the **Resource type** section, select **Subnetwork**.

Entries from the subnetwork logs will display on the **Query results** pane to the right of the **Log fields** pane.

4. On the **Log fields** pane, in the **Log name** section, select **compute.googleapis.com/vpc_flows** to access the VPC Flow logs for the

network. If this option doesn’t display, wait a few minutes for this log type to show up.

Once selected, entries from the VPC Flow Logs display on the **Query results** pane.

5. In the **Query** builder at the top of the page, at the end of line 2, press **ENTER** to create a new line.

6. On line 3, enter the following:

```
jsonPayload.connection.src_ip=YOUR_IP
```

Copied!

content_copy

Your query should resemble the following:

```
resource.type="gce_subnetwork"
log_name="projects/qwiklabs-gcp-04-bce3c5fc51b3/logs/compute.googleapis.com%2Fvpc_flows"
jsonPayload.connection.src_ip=YOUR_IP
```

7. Replace `YOUR_IP` with the IP address you saved from Task 2. This query will search for network traffic logs originating from your IP address that you had generated in the previous task.

8. Click **Run query**. The query results should display on the **Query results** pane

9. In the **Query results** pane, expand one of the log entries.

10. Within the entry, expand **jsonPayload** by clicking the expand arrow >. Then, expand the **connection** field.

CREATE A FIREWALL RULE TO DENY HTTP TRAFFIC

1. In the Google Cloud console, click the **Navigation menu** (☰).

2. Select **VPC network** > **Firewall**. The Firewall policies page displays.

3. On the toolbar, click **+ Create Firewall Rule**.

4. In the **Create a firewall rule** dialog, specify the following, and leave the remaining settings as their defaults:

Field	**Value**

Name	deny-http
Logs	On
Network	vpc-net
Action on match	Deny
Targets	Specified target tags
Target tags	http-server
Source filter	IPv4 ranges
Source IPv4 ranges	0.0.0.0/0
In the **Protocols and ports** section	Select **Specified protocols and ports** Select the **TCP** checkbox In the **Ports** field enter **80**

5. Click **Create**.

ANALYZE THE FIREWALL LOG

1. Click the **Navigation menu** (☰).
2. Select **Compute Engine > VM instances**. The **VM instances** page opens.
3. For **web-server**, click on the **External IP** link to access the server.
4. In the Google Cloud console, click the **Navigation menu** (☰).

5. Select **Logging** > **Logs Explorer**. The **Logs Explorer** page opens. (You may need to expand the **More Products** drop-down menu within the **Navigation** menu and locate Logging under **Operations**.)

6. Under the **Resource type** section, select **Subnetwork**.

7. On the **Log fields** pane, in the **Log name** section, select **compute.googleapis.com/firewall** to access the firewall logs for the network.

8. In the **Query** builder at the top of the page, at the end of line 2, press **ENTER** to create a new line.

9. On line 3, enter the following:

```
jsonPayload.connection.src_ip=YOUR_IP DENIED
```

Copied!

content_copy

Replace `YOUR_IP` with the IP address you saved from Task 2. This query will search for firewall logs that denied your IP address connection to the web server. Your query should resemble the following:

```
resource.type="gce_subnetwork"
log_name="projects/qwiklabs-gcp-04-
bce3c5fc51b3/logs/compute.googleapis.com%2Ffirewall"
jsonPayload.connection.src_ip=YOUR_IP DENIED
```

10. Click **Run query**. The query results should display on the Query results pane.

11. In the **Query results** pane, expand one of the log entries.

12. Within the log entry, expand the **jsonPayload** field by clicking the expand arrow >. Then, expand the **connection** field. You can examine the details about the network connection to the web server to verify if the firewall rule was successfully triggered: