Access a firewall and create a rule

Scenario

Cymbal Bank has a demo web server that is provisioned on an existing Virtual Private Cloud (VPC) network. Your team lead, Chloe, is concerned about the security configurations of this web server and wants you to analyze the inbound network traffic to the web server and block connections to unnecessary ports using firewall rules. You have been tasked with analyzing the firewall rules for this web server and testing its connection. To complete this task, you will need to create several firewall rules, connect to the web server, and analyze the logs associated with the network connections.

Here's how you'll do this task: **First**, you'll create a firewall rule to allow network traffic to the demo web server. **Then**, you'll generate HTTP network traffic to the server and analyze its network logs. **Next**, you'll create and test a new firewall rule to deny HTTP traffic to the server. **Finally**, you'll analyze the firewall logs to verify that the new firewall rule works as intended.

Task 1. Create a firewall rule

In this task, you'll create a firewall rule that allows HTTP and SSH connectivity. You will also specify a target tag for the newly created firewall rule.

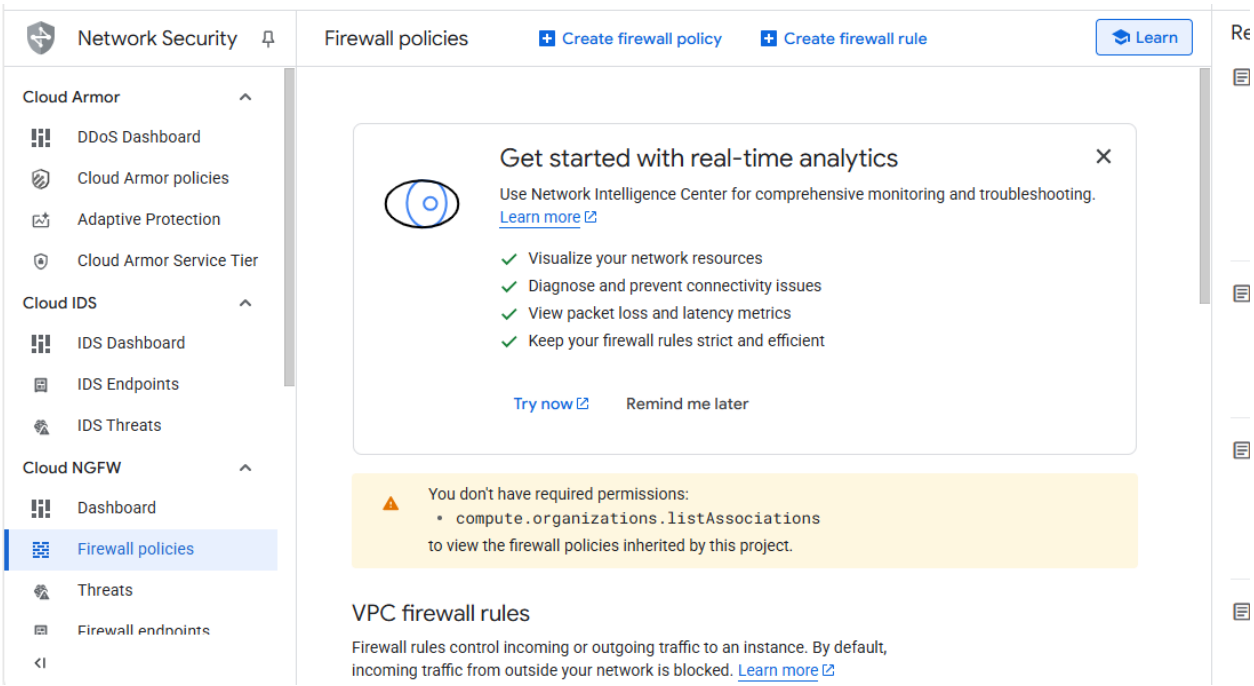
In Google Cloud, firewall rules must specify *targets* to define which VM instances they apply to. *Target tags* can be used to apply a firewall rule to a specific group of VMs, helping simplify the management of firewall rules. You'll use target tags to enable this firewall rule to the web server only.

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**. 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**.



Create a firewall rule

Name *
allow-http-ssh

Lowercase letters, numbers, hyphens allowed

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Logging. Learn more

- (●) On
- ( ) Off

Show logs details

Network *
vpc-net

Priority *
1000 Compare

Priority can be 0 - 65535

Direction of traffic

- (●) Ingress

Create a firewall rule

Action on match

- (•) Allow
- ( ) Deny

Targets
Specified target tags

Target tags *
http-server ×

Source filter
IPv4 ranges

Source IPv4 ranges *
0.0.0.0/0 × for example, 0.0.0.0/0, 192.168.2.0/24

Second source filter
None

Destination filter
None

Protocols and ports

Create a firewall rule

Destination filter
None

Protocols and ports

- ○ Allow all
- ◉ Specified protocols and ports

☑ TCP

Ports
80,22

E.g. 20, 50-60

☐ UDP

Ports

E.g. all

☐ SCTP

Ports

E.g. 20, 50-60

☐ Other

Protocols

Firewall policies Create firewall policy Create firewall rule

SMTP port 25 disallowed in this project. Learn more

Refresh Configure logs Delete

Filter Enter property name or value

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	default
default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default
default-allow-rdp	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	default
default-allow-ssh	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	default
allow-http-ssh	Ingress	http-server	IP ranges:	tcp:22, 80	Allow	1000	vpc-net

Network firewall po

Successfully created firewall rule "allow-http-ssh".

Firewall policies let you group several firewall rules so that you can update them all

Task 2. Generate HTTP network traffic

In this task, you'll generate HTTP network traffic to the web server by visiting its external IP address. The network traffic you generate will then be recorded as logs that you can analyze in the Logs Explorer.

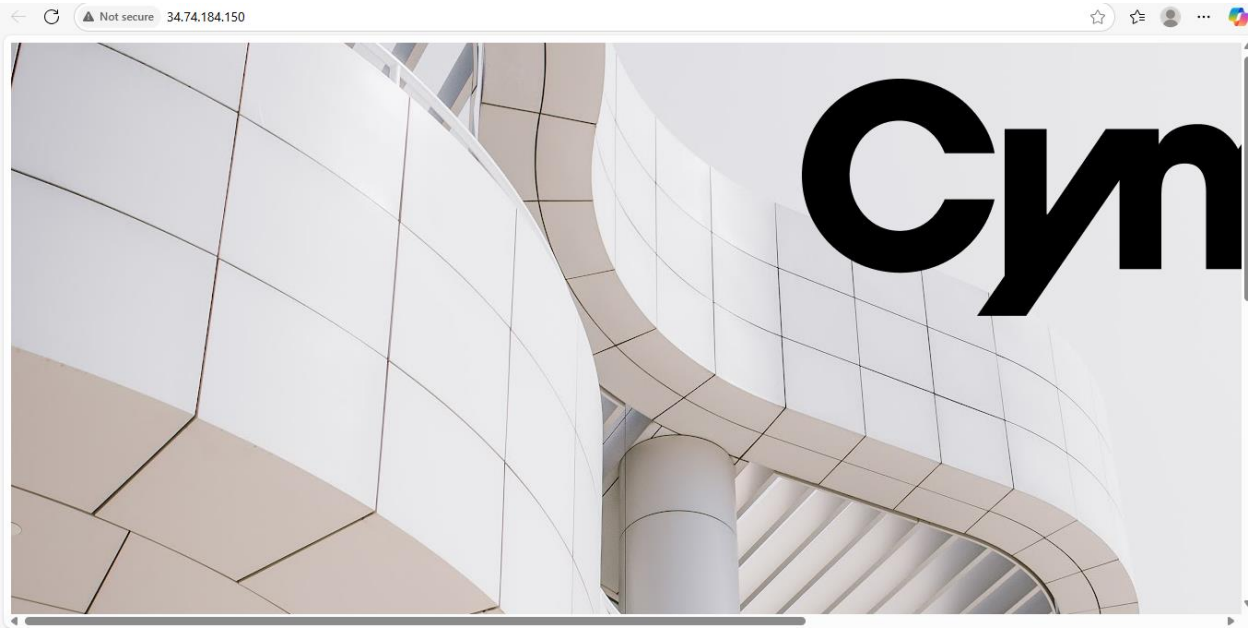
First, you need to generate network traffic.

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.

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

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



Task 3. Analyze the web server Flow Logs

In this task, you'll access and analyze the VPC Flow Logs for the web server using the Logs Explorer.

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

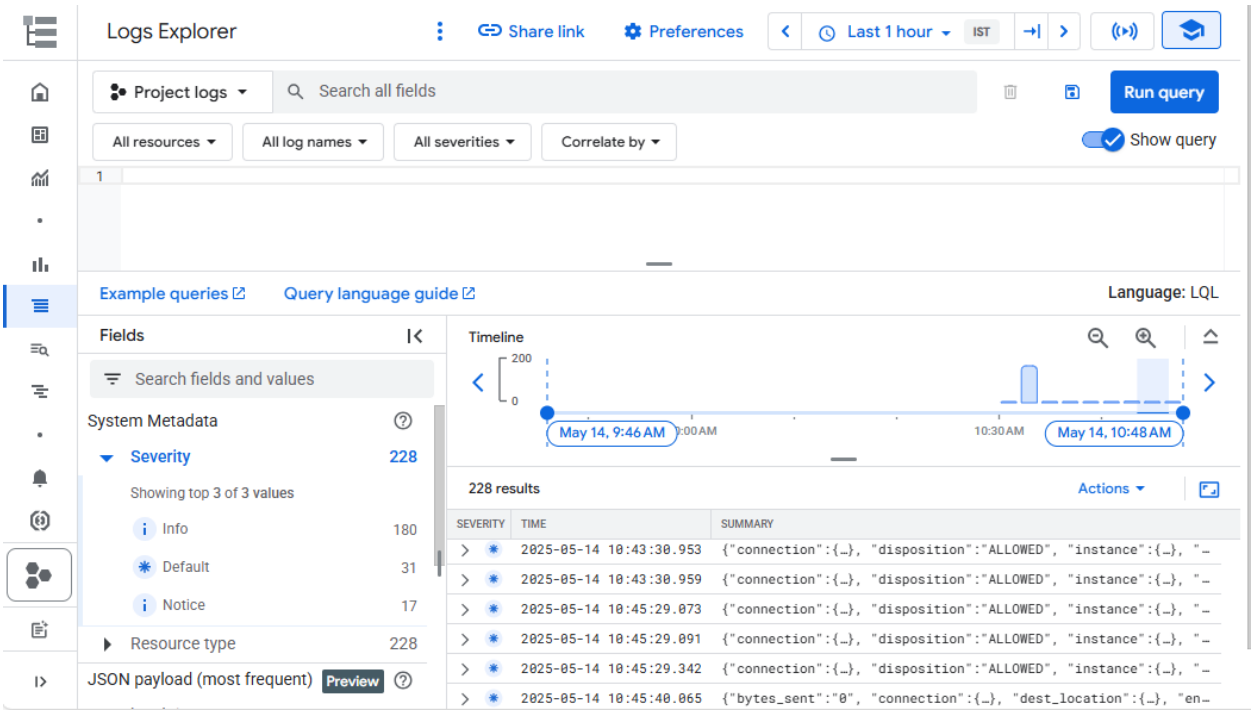
7. Replace YOUR_IP with the IP address you saved from Task 2. This query will search for network traffic logs originating from your IP address that you had generated in the previous task.
8. Click **Run query**. The query results should display on the **Query results** pane
9. In the **Query results** pane, expand one of the log entries.
10. Within the entry, expand **jsonPayload** by clicking the expand arrow **>**. Then, expand the **connection** field.

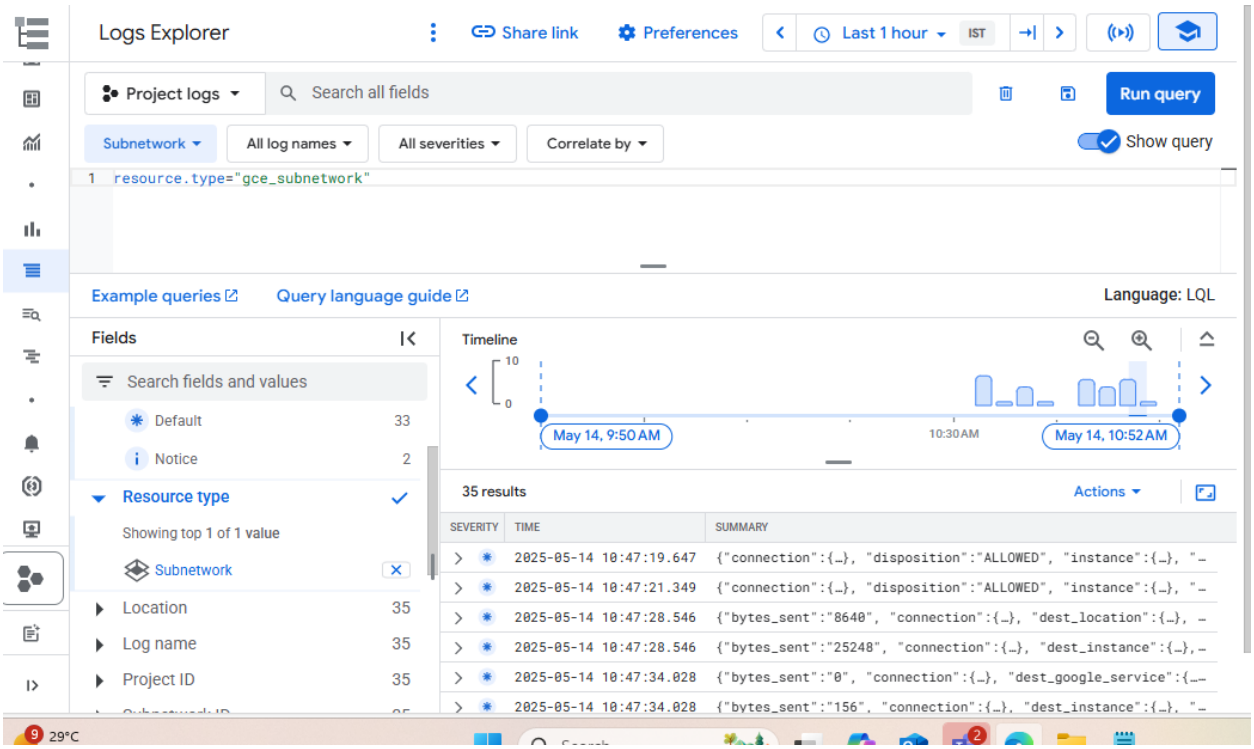
Here you can examine the details about the network connection to the web server:

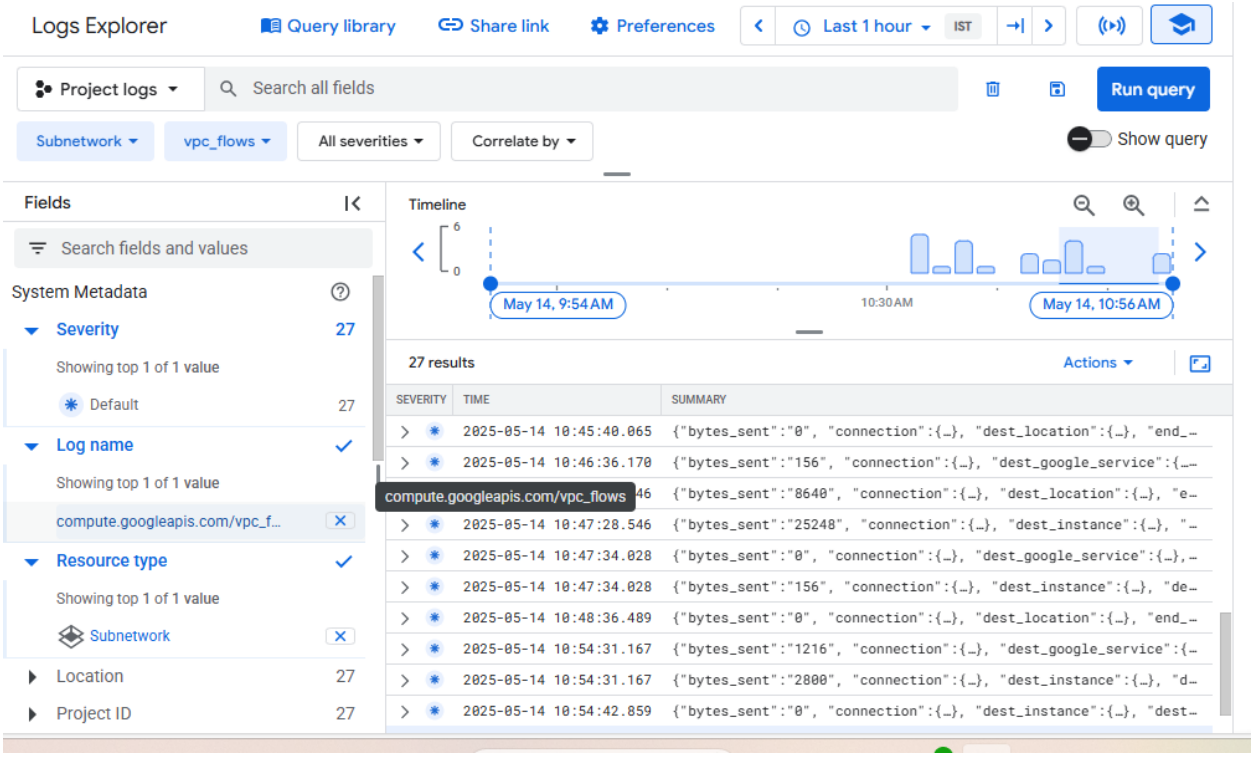
- **dest_ip** - This is the destination IP address of the web server.
- **dest_port** - This is the destination port number of the web server which is HTTP port 80.
- **protocol** - The protocol is 6 which is the IANA protocol for TCP traffic.

- **src_ip** - This is the source IP address of your computer.
- **src_port** - This is the source port number that's assigned to your computer. According to Internet Assigned Numbers Authority (IANA) standards, this is typically a random port number between 49152-65535.

After analyzing the details of this log entry, you should notice that the network traffic you generated (on HTTP port 80) was allowed due to the firewall rule **allow-http-ssh** you created previously. This rule allowed incoming traffic on ports 80 and 22



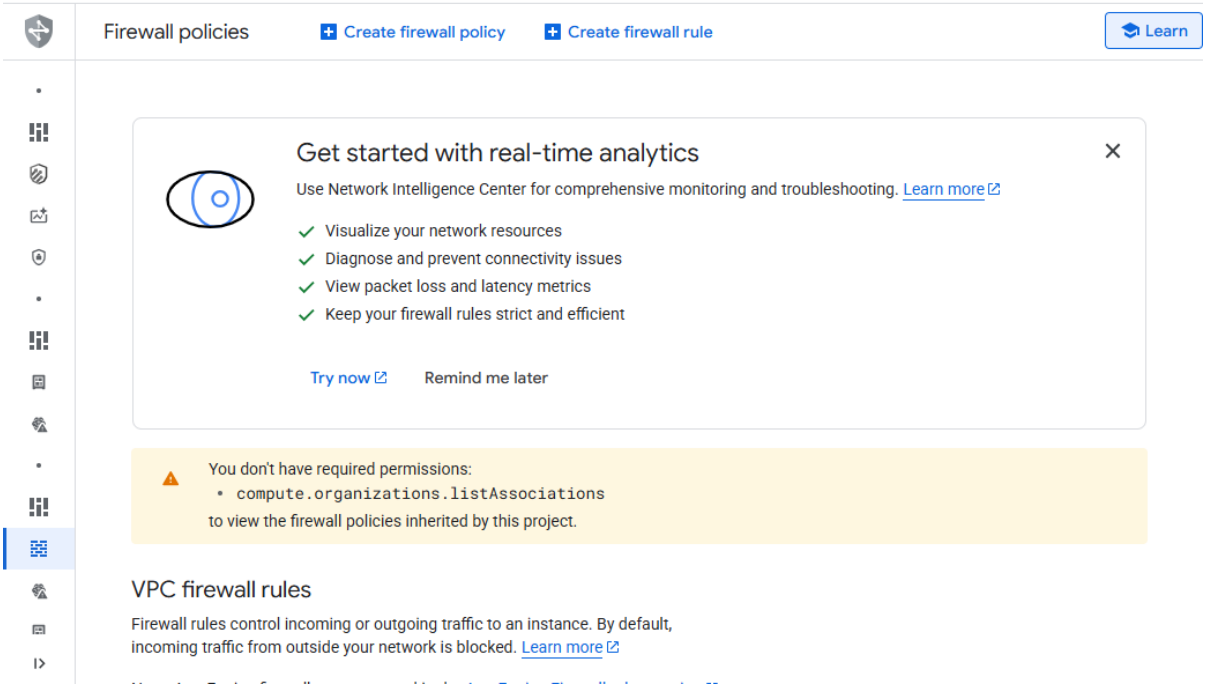




Task 4. Create a firewall rule to deny HTTP traffic

In this task, you'll create a new firewall rule that denies traffic from port 80.

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



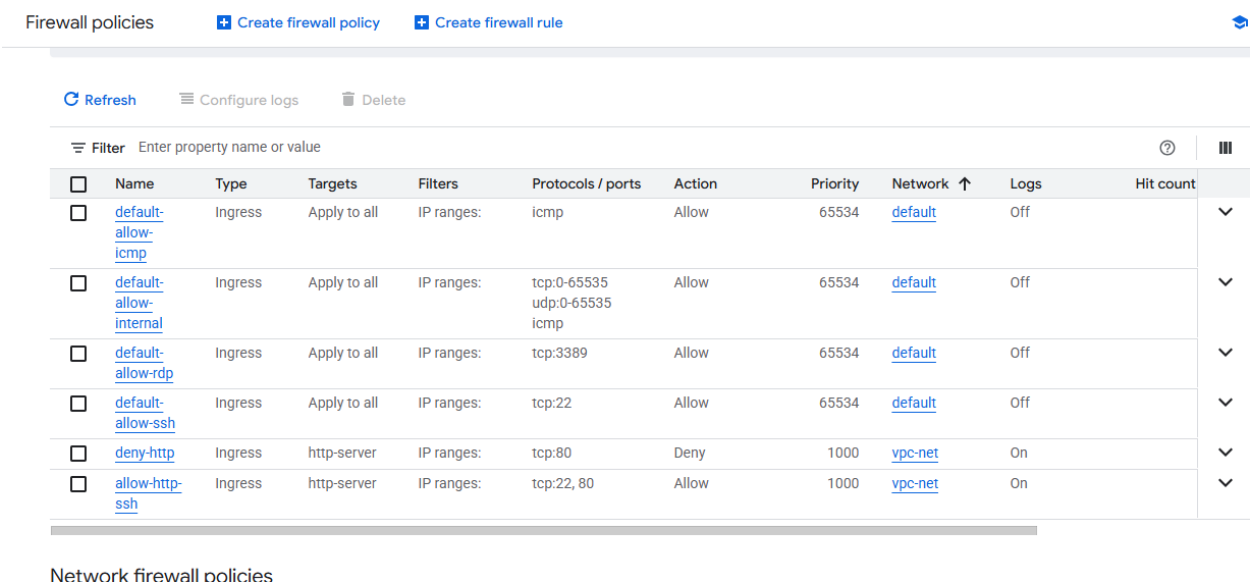
).

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**.



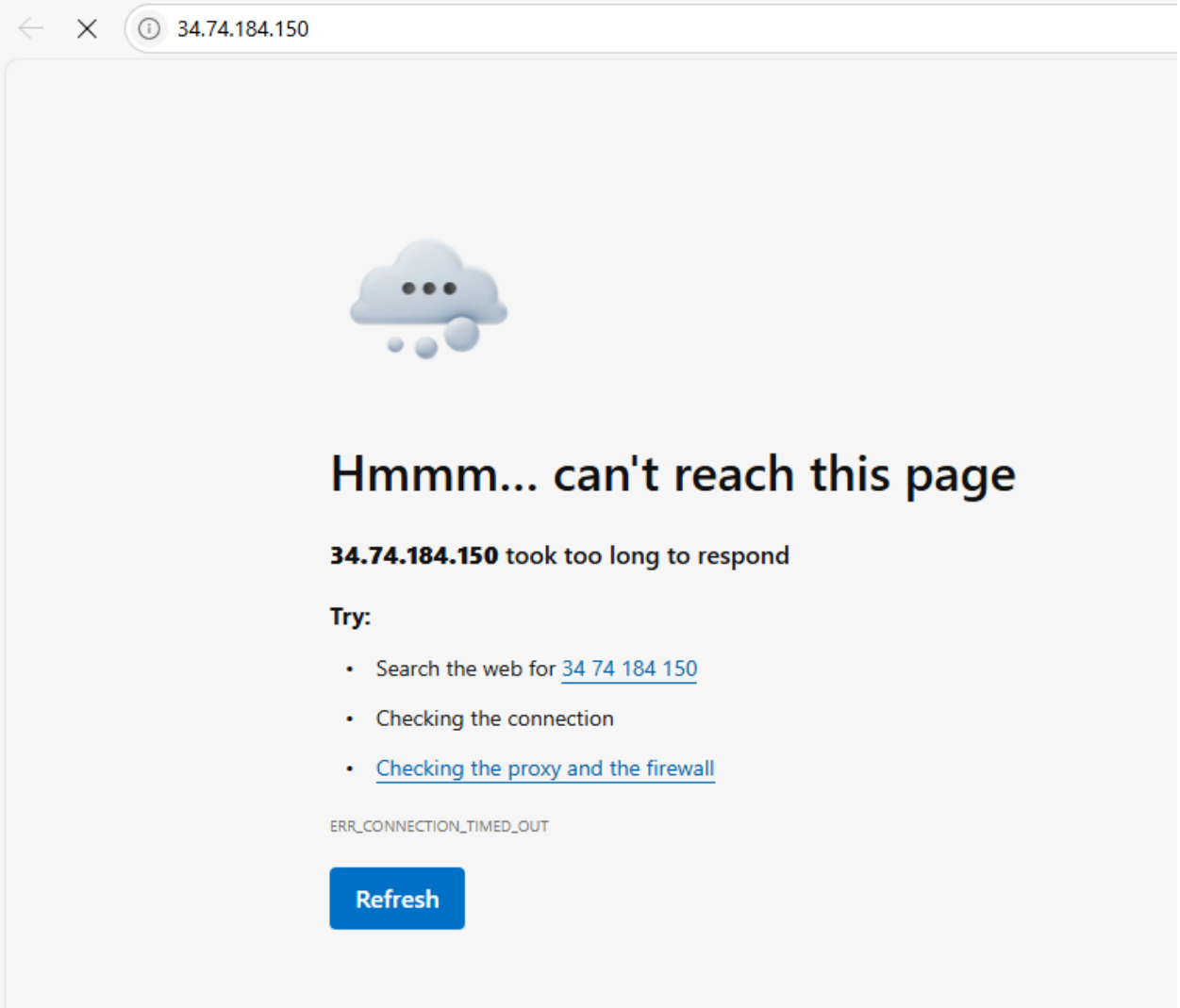
Task 5. Analyze the firewall logs

In this task, you'll test the **deny-http** firewall rule that you created in the previous task.

First, attempt to connect to the web server.

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.

The following error message should display on



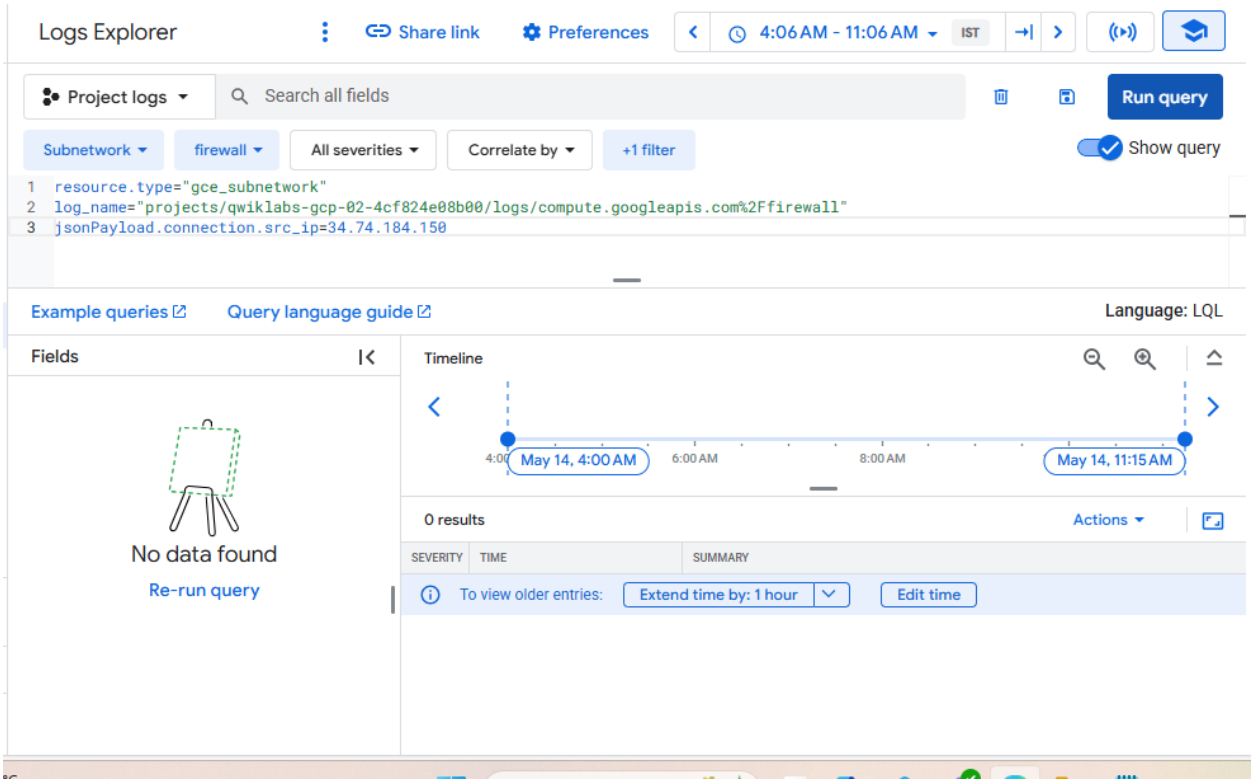
This error occurred because of the **deny-http** firewall rule you created in the previous task. To verify this, access the Logs Explorer to analyze the firewall logs for the web server.

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



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:

- **dest_ip** - This is the destination IP address of the web server which is **10.1.3.2**.
- **dest_port** - This is the destination port number of the web server which is HTTP port **80**.
- **protocol** - The protocol is **6** which is the IANA protocol for TCP traffic.
- **src_ip** - This is the source IP address of your computer.
- **src_port** - This is the source port number that's assigned to your computer.

- **disposition** - This field indicates whether the connection was allowed or denied. Here, it's **denied** which indicates that the connection to the server was denied.

13. Within the log entry, expand the **rule_details** field by clicking the expand arrow **>**. You can examine the details about the firewall rule. Additionally, you can extract more information from the following fields in the log entry by expanding them:

- **action** - The action taken by the rule, **DENY** in this case.
- **direction** - The rule's traffic direction can be either ingress or egress, here it is **INGRESS** which means the action will apply to incoming traffic.
- **ip_port_info** - The protocol and ports this rule controls. The **ip_protocol** and **port_range** lists **TCP port 80**.
- **source_range** - The traffic sources that the firewall rule is applied to. Here it is **0.0.0.0/0**.
- **target_tag** - This lists all the target tags that the firewall rule applies to. Here, it is **http-server**, the target tag you added to the firewall rule in the previous task.

  By examining the details of this firewall log entry, you should notice that the firewall rule **deny-http** you set up to deny HTTP traffic was successfully triggered. This rule denied incoming network traffic on port 80.