Course 3_Lab 2: 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.

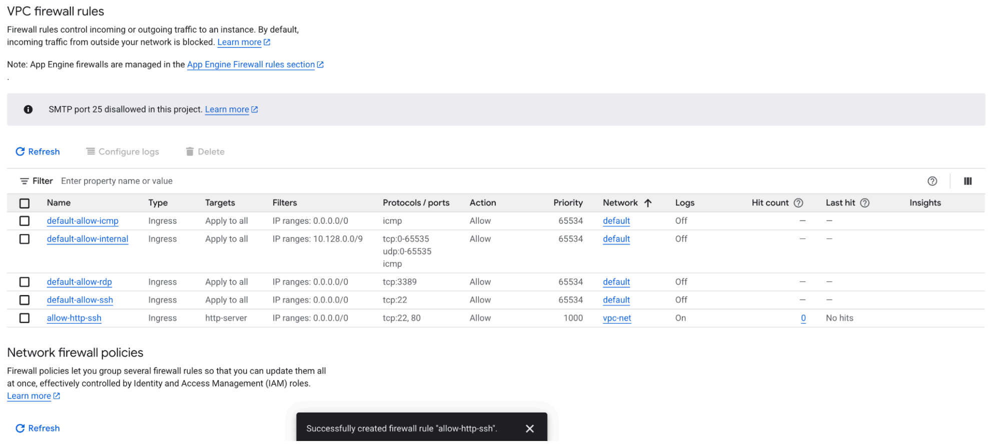
Here's how you'll do this task: **First**, you'll create a firewall rule to allow network traffic to the demo web server. **Then**, you'll generate HTTP network traffic to the server and analyze its network logs. **Next**, you'll create and test a new firewall rule to deny HTTP traffic to the server.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

***Note:** In this lab, you are provided with a custom-mode network VPC, **vpc-net**, and subnet, **vpc-subnet**, configured with VPC Flow Logs in Default region region. You are also provided with a VM instance, **web-server**, installed with an Apache web server within **vpc-subnet** with attached network tag **http-server** in Default zone zone.*

MY WORK:

Task 1: Create a firewall rule

In this task, I created a Firewall Rule based on default information provided by Google.



VPC firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine Firewall rules section

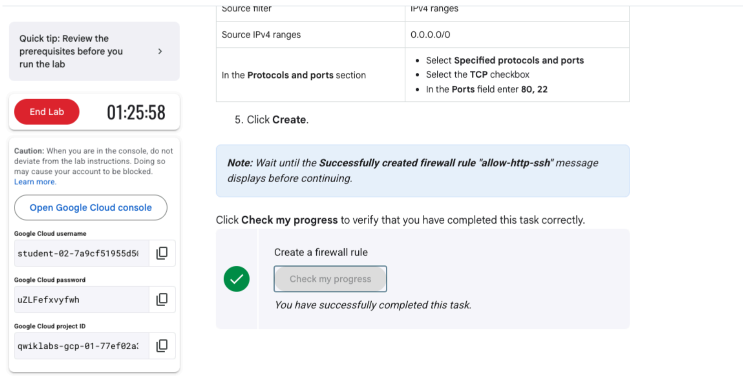
SMTP port 25 disallowed in this project. Learn more

☐	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count	Last hit	Insights
☐	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default	Off	–	–	
☐	default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	–	–	
☐	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default	Off	–	–	
☐	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default	Off	–	–	
☐	allow-http-ssh	Ingress	http-server	IP ranges: 0.0.0.0/0	tcp:22, 80	Allow	1000	vpc-net	On	0	No hits	

Network firewall policies

Firewall policies let you group several firewall rules so that you can update them all at once, effectively controlled by Identity and Access Management (IAM) roles. Learn more

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



Quick tip: Review the prerequisites before you run the lab
End Lab
01:25:58

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username: student-02-7a9cf51955d5

Google Cloud password: uZLFefxvyfwh

Google Cloud project ID: qwiklabs-gcp-01-77ef02a

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**.

***Note:** Wait until the **Successfully created firewall rule "allow-http-ssh"** message displays before continuing.*

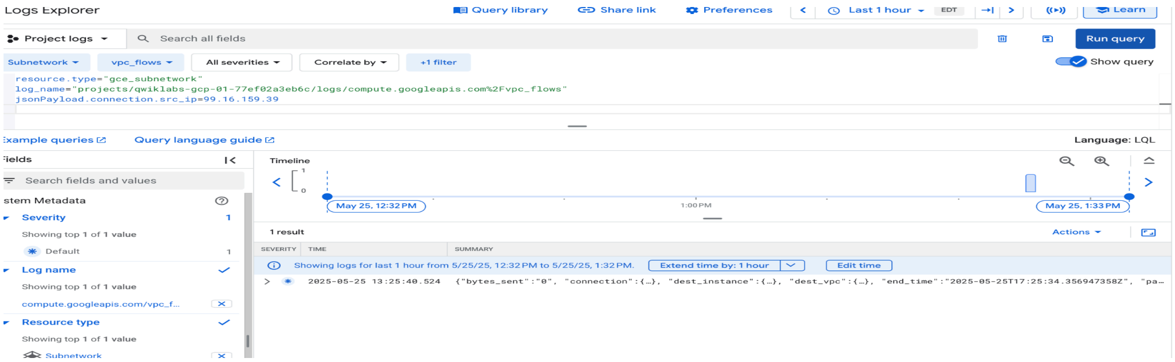
Click **Check my progress** to verify that you have completed this task correctly.

Create a firewall rule

You have successfully completed this task.

Task 2: Generate HTTP network traffic

In this task, I was able to generate HTTP web traffic to the server in order to view log information in Logs Explorer.

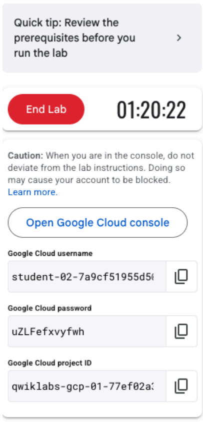


```
resource.type="gce_subnetwork"
log_name="projects/qwiklabs-gcp-01-77ef02a3eb6c/logs/compute.googleapis.com%2Fvpc_flows"
jsonPayload.connection.src_ip=99.16.159.39
```

ystem Metadata
Severity 1
Showing top 1 of 1 value
Default 1
Log name
Showing top 1 of 1 value
compute.googleapis.com/vpc_f...
Resource type
Showing top 1 of 1 value
Subnetwork

1 result

```
SEVERITY  TIME                      SUMMARY
Showing logs for last 1 hour from 5/25/25, 12:32 PM to 5/25/25, 1:32 PM.   Extend time by: 1 hour   Edit time
>  ✱  2025-05-25 13:25:40.524  {"bytes_sent":"0", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T17:25:34.356947358Z", "pa…
```


Quick tip: Review the prerequisites before you run the lab

End Lab 01:20:22

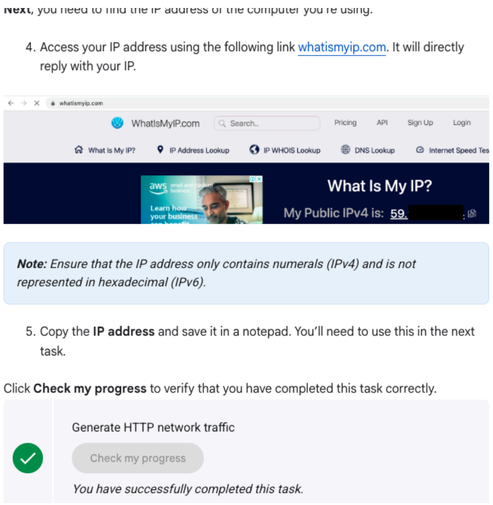
Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username: student-02-7a9cf51955d5(

Google Cloud password: uZLFefxvyfwh

Google Cloud project ID: qwiklabs-gcp-01-77ef02a:


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.

What Is My IP?

My Public IPv4 is: 59.[redacted]

***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.

Click **Check my progress** to verify that you have completed this task correctly.

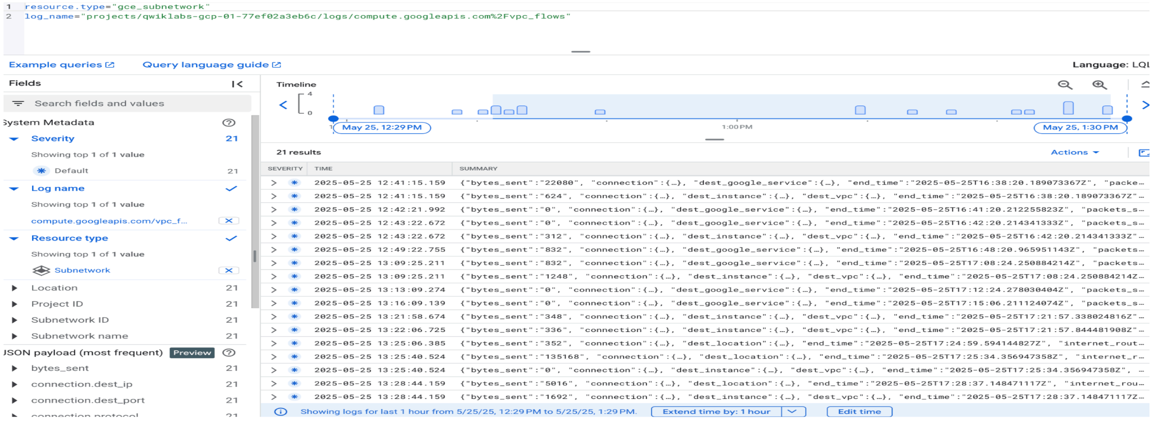
Generate HTTP network traffic

Check my progress

You have successfully completed this task.

Task 3: Analyze the web server Flow Logs

In this task, I honed in on observing and reviewing the web server logs in Logs Explorer. I was able to see how longs are categorized, what's in the summary, while also reviewing the resource type and severity. Overall, I was able to see how I allowed web traffic generated on a specific port.

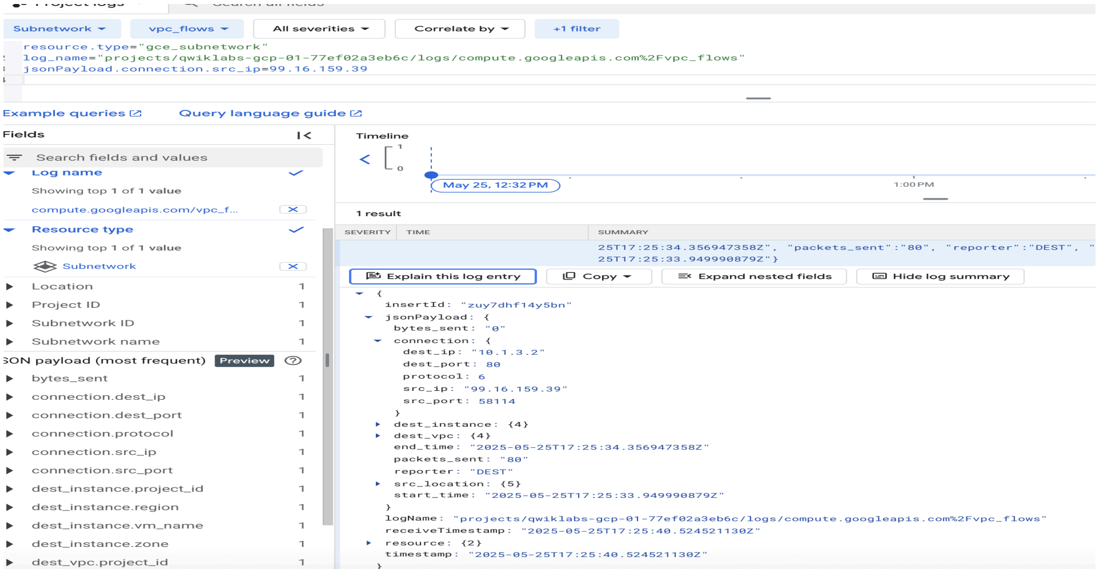


```
resource.type="gce_subnetwork"
log_name="projects/qwiklabs-gcp-01-77ef02a3eb6c/logs/compute.googleapis.com%2Fvpc_flows"
```

ystem Metadata
Severity 21
Showing top 1 of 1 value
Default 21
Log name
Showing top 1 of 1 value
compute.googleapis.com/vpc_f...
Resource type
Showing top 1 of 1 value
Subnetwork
Location 21
Project ID 21
Subnetwork ID 21
Subnetwork name 21
JSON payload (most frequent)
bytes_sent 21
connection.dest_ip 21
connection.dest_port 21
connection.protocol 21

21 results

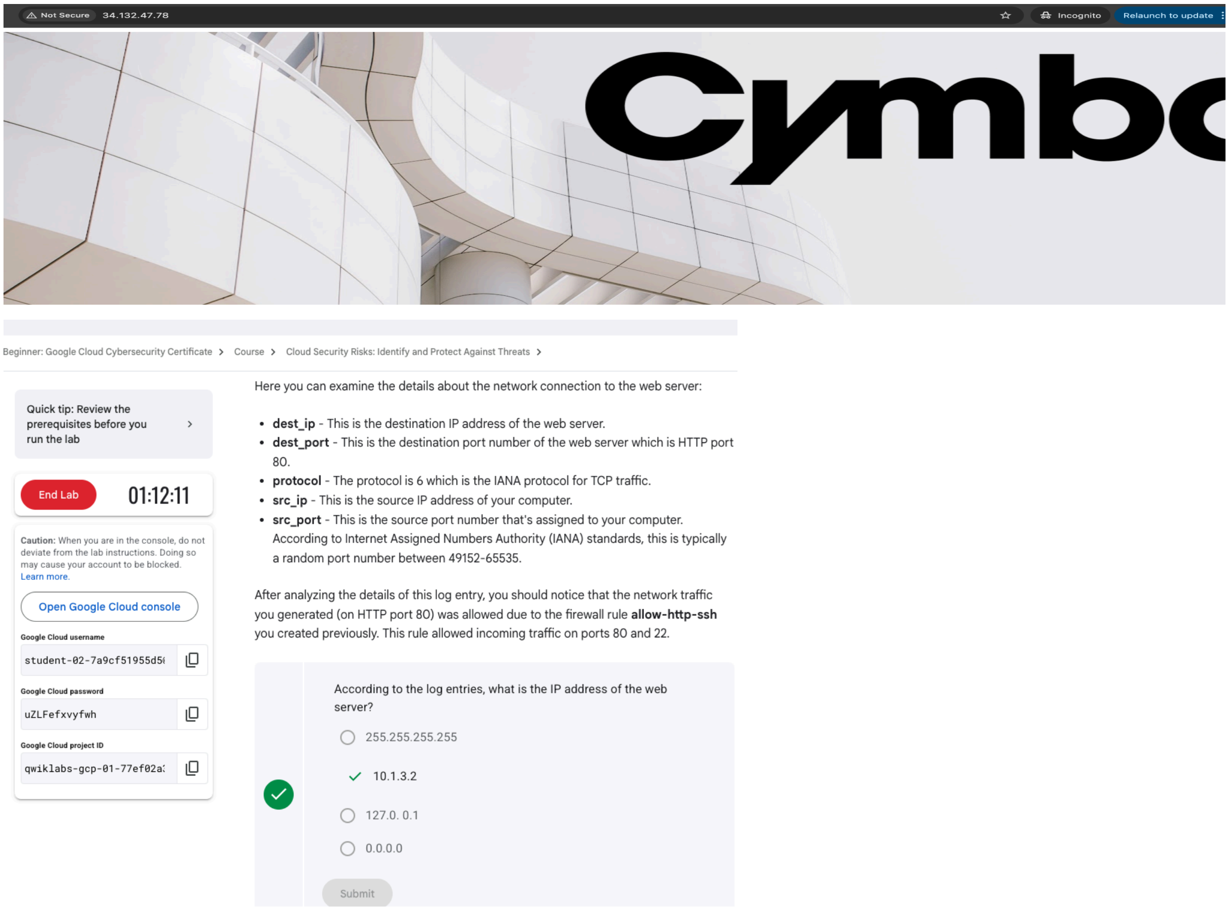
```
SEVERITY  TIME                      SUMMARY
>  ✱  2025-05-25 12:41:15.159  {"bytes_sent":"22080", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T16:38:20.189073367Z", "packe…
>  ✱  2025-05-25 12:41:15.159  {"bytes_sent":"624", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T16:38:20.189073367Z"…
>  ✱  2025-05-25 12:42:21.992  {"bytes_sent":"0", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T16:41:20.212255823Z", "packets_s…
>  ✱  2025-05-25 12:43:22.672  {"bytes_sent":"0", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T16:42:20.214341333Z", "packets_s…
>  ✱  2025-05-25 12:43:22.672  {"bytes_sent":"312", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T16:42:20.214341333Z"…
>  ✱  2025-05-25 12:49:22.755  {"bytes_sent":"832", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T16:48:20.965951143Z", "packets…
>  ✱  2025-05-25 13:09:25.211  {"bytes_sent":"832", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T17:08:24.250884214Z", "packets…
>  ✱  2025-05-25 13:09:25.211  {"bytes_sent":"1248", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T17:08:24.250884214Z…
>  ✱  2025-05-25 13:13:09.274  {"bytes_sent":"0", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T17:12:24.278030404Z", "packets_s…
>  ✱  2025-05-25 13:16:09.139  {"bytes_sent":"0", "connection":{…}, "dest_google_service":{…}, "end_time":"2025-05-25T17:15:06.211124074Z", "packets_s…
>  ✱  2025-05-25 13:21:58.674  {"bytes_sent":"348", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T17:21:57.338024816Z"…
>  ✱  2025-05-25 13:22:06.725  {"bytes_sent":"336", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T17:21:57.844481908Z"…
>  ✱  2025-05-25 13:25:06.385  {"bytes_sent":"352", "connection":{…}, "dest_location":{…}, "end_time":"2025-05-25T17:24:59.594144827Z", "internet_rout…
>  ✱  2025-05-25 13:25:40.524  {"bytes_sent":"135168", "connection":{…}, "dest_location":{…}, "end_time":"2025-05-25T17:25:34.356947358Z", "internet_r…
>  ✱  2025-05-25 13:25:40.524  {"bytes_sent":"0", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T17:25:34.356947358Z", …
>  ✱  2025-05-25 13:28:44.159  {"bytes_sent":"5016", "connection":{…}, "dest_location":{…}, "end_time":"2025-05-25T17:28:37.148471117Z", "internet_rou…
>  ✱  2025-05-25 13:28:44.159  {"bytes_sent":"1692", "connection":{…}, "dest_instance":{…}, "dest_vpc":{…}, "end_time":"2025-05-25T17:28:37.148471117Z…
Showing logs for last 1 hour from 5/25/25, 12:29 PM to 5/25/25, 1:29 PM.   Extend time by: 1 hour   Edit time
```



```
resource.type="gce_subnetwork"
log_name="projects/qwiklabs-gcp-01-77ef02a3eb6c/logs/compute.googleapis.com%2Fvpc_flows"
jsonPayload.connection.src_ip=99.16.159.39
```

```
25T17:25:34.356947358Z", "packets_sent":"80", "reporter":"DEST", "
25T17:25:33.949990879Z"}
```

```
{
 insertId: "zuy7dhf14y5bn"
 jsonPayload: {
  bytes_sent: "0"
  connection: {
   dest_ip: "10.1.3.2"
   dest_port: 80
   protocol: 6
   src_ip: "99.16.159.39"
   src_port: 58114
  }
  dest_instance: {4}
  dest_vpc: {4}
  end_time: "2025-05-25T17:25:34.356947358Z"
  packets_sent: "80"
  reporter: "DEST"
  src_location: {5}
  start_time: "2025-05-25T17:25:33.949990879Z"
 }
 logName: "projects/qwiklabs-gcp-01-77ef02a3eb6c/logs/compute.googleapis.com%2Fvpc_flows"
 receiveTimestamp: "2025-05-25T17:25:40.524521130Z"
 resource: {2}
 timestamp: "2025-05-25T17:25:40.524521130Z"
}
```



Beginner: Google Cloud Cybersecurity Certificate › Course › Cloud Security Risks: Identify and Protect Against Threats ›

Quick tip: Review the prerequisites before you run the lab ›

01:12:11

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username: student-02-7a9cf51955d5(

Google Cloud password: uZLFefxvyfwh

Google Cloud project ID: qwiklabs-gcp-01-77ef02a:

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.

✓

According to the log entries, what is the IP address of the web server?

○ 255.255.255.255

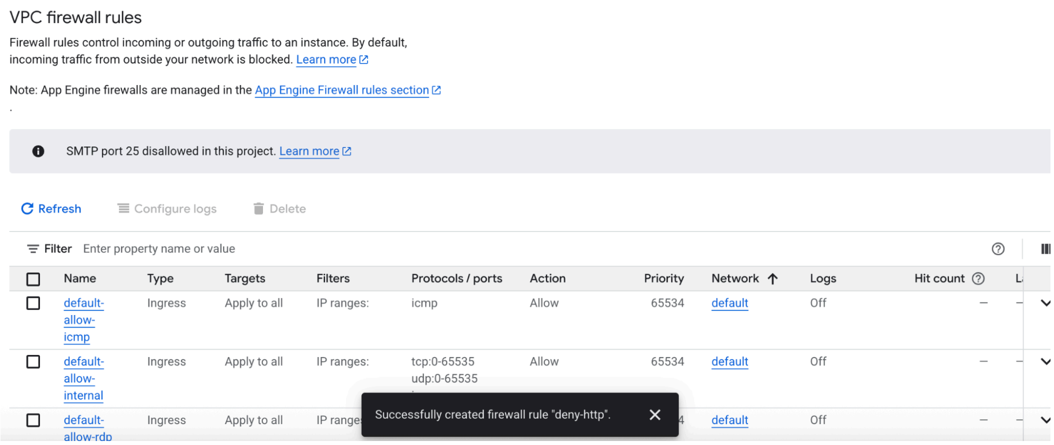
✓ 10.1.3.2

○ 127.0. 0.1

○ 0.0.0.0

Task 4: Create a firewall rule to deny HTTP traffic

After allowing traffic in the previous task, I was able to set up a firewall denying traffic based on a created firewall rule.



VPC firewall rules

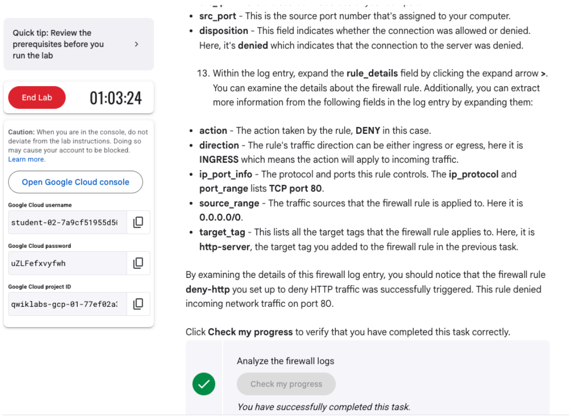
Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine Firewall rules section .

SMTP port 25 disallowed in this project. Learn more

□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network ↑	Logs	Hit count	L
□	default-allow-icmp	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	default	Off	—	—
□	default-allow-internal	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535	Allow	65534	default	Off	—	—
□	default-allow-rdp	Ingress	Apply to all	IP range			4	default	Off	—	—

Successfully created firewall rule "deny-http".



Quick tip: Review the prerequisites before you run the lab
End Lab
01:03:24

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Open Google Cloud console

Google Cloud username: student-02-7a9cf51955d5

Google Cloud password: uZLFefxvyfwh

Google Cloud project ID: qwiklabs-gcp-01-77ef02a

- **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.

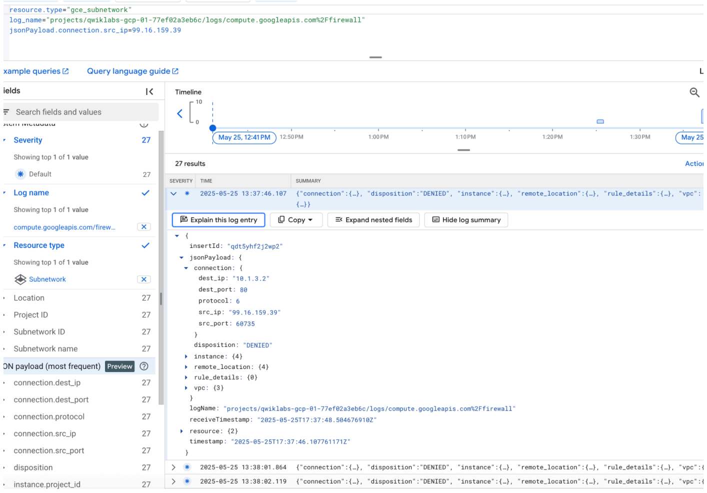
Click **Check my progress** to verify that you have completed this task correctly.

Analyze the firewall logs

You have successfully completed this task.

Task 5: Analyze the firewall logs

In this task, I was able to analyze the “deny” firewall rule after trying to reach the website.



```
resource.type="gce_subnetwork"
log_name="projects/qwiklabs-gcp-01-77ef02a3eb6c/logs/compute.googleapis.com%2Ffirewall"
jsonPayload.connection.src_ip=99.16.159.39
```

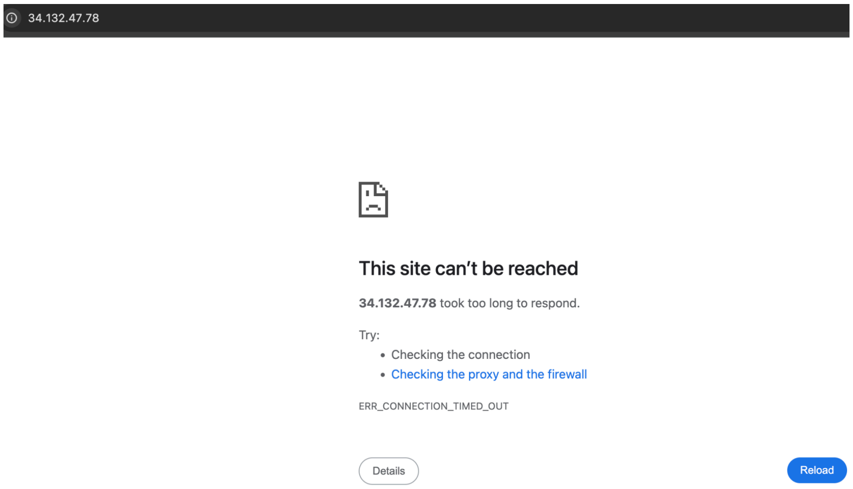
ields	
Severity	27
Showing top 1 of 1 value	
Default	27
Log name	✓
Showing top 1 of 1 value	
compute.googleapis.com/firew...	✕
Resource type	✓
Showing top 1 of 1 value	
Subnetwork	✕
Location	27
Project ID	27
Subnetwork ID	27
Subnetwork name	27
ON payload (most frequent) Preview	
connection.dest_ip	27
connection.dest_port	27
connection.protocol	27
connection.src_ip	27
connection.src_port	27
disposition	27
instance.project_id	27

27 results

SEVERITY	TIME	SUMMARY
✱	2025-05-25 13:37:46.107	{"connection":{…}, "disposition":"DENIED", "instance":{…}, "remote_location":{…}, "rule_details":{…}, "vpc":{…}}

```
{
  insertId: "qdt5yhf2j2wp2"
  jsonPayload: {
    connection: {
      dest_ip: "10.1.3.2"
      dest_port: 80
      protocol: 6
      src_ip: "99.16.159.39"
      src_port: 60735
    }
    disposition: "DENIED"
    instance: {4}
    remote_location: {4}
    rule_details: {0}
    vpc: {3}
  }
  logName: "projects/qwiklabs-gcp-01-77ef02a3eb6c/logs/compute.googleapis.com%2Ffirewall"
  receiveTimestamp: "2025-05-25T17:37:48.504676910Z"
  resource: {2}
  timestamp: "2025-05-25T17:37:46.107761171Z"
}
```

SEVERITY	TIME	SUMMARY
✱	2025-05-25 13:38:01.864	{"connection":{…}, "disposition":"DENIED", "instance":{…}, "remote_location":{…}, "rule_details":{…}, "vpc":{
✱	2025-05-25 13:38:02.119	{"connection":{…}, "disposition":"DENIED", "instance":{…}, "remote_location":{…}, "rule_details":{…}, "vpc":{



34.132.47.78

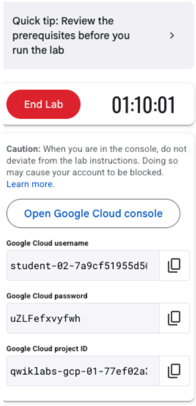
This site can't be reached

34.132.47.78 took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT



Quick tip: Review the prerequisites before you run the lab

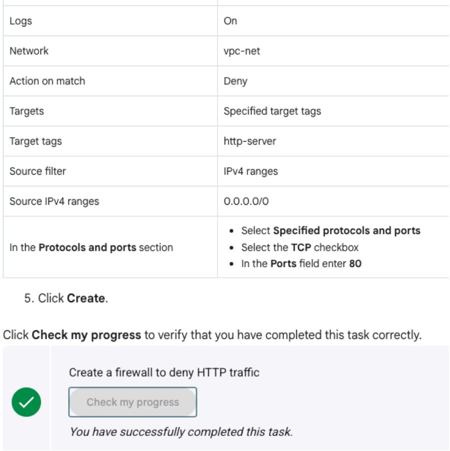
01:10:01

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. Learn more.

Google Cloud username: student-02-7a9cf51955d5

Google Cloud password: uZLFefxvyfwh

Google Cloud project ID: qwiklabs-gcp-01-77ef02a



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**.

Click **Check my progress** to verify that you have completed this task correctly.

✓ Create a firewall to deny HTTP traffic

You have successfully completed this task.

My Assessment:

This lab provided an opportunity to learn how to create an allow and deny firewall rule. A firewall is a security measure used to monitor incoming and outgoing traffic. It acts as a barrier, once configured, between an untrusted and trusted network. It can either allow or block traffic to and from the network.