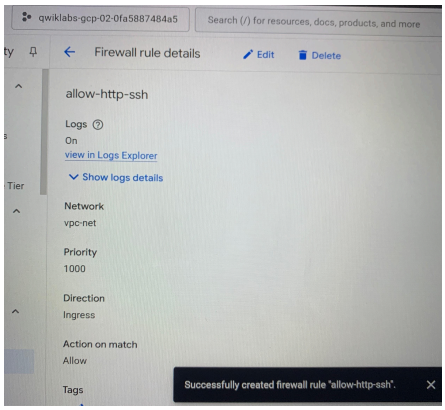
ACCESS A FIREWALL AND CREATE A RULE

In regards to the security configurations of a web server I analyzed the inbound network traffic to the web server and blocked connections to unnecessary ports using firewall rules. I created several firewall rules, connected to the web server and analyzed the logs associated with the network connections.

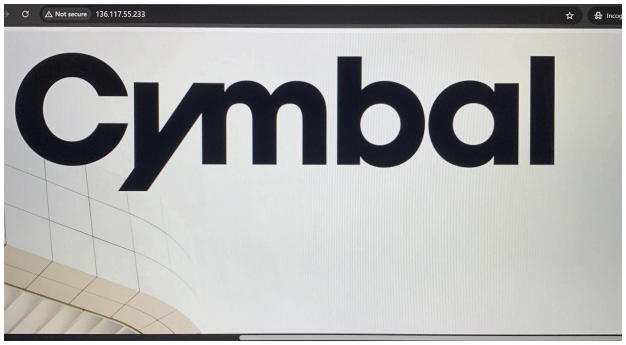
First step: create a firewall rule

In google cloud, firewall rules must specify targets to define which VM instances they apply to. Targets can be used to apply firewall rule to a specific group of VMs, helping simplify the management of firewall rules. I used targets to enable this rule to the web server only.



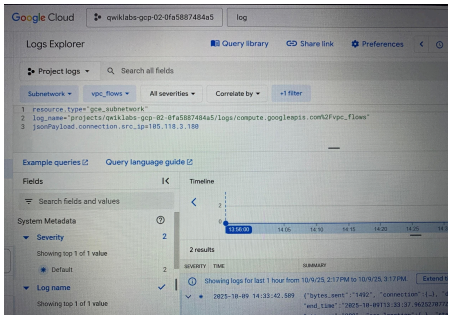
Second step: Generate HTTP network traffic

I generated HTTP network traffic to the web server by visiting its external IP address. The network traffic I generated will then be recorded as logs that I can analyze in the logs explorer.

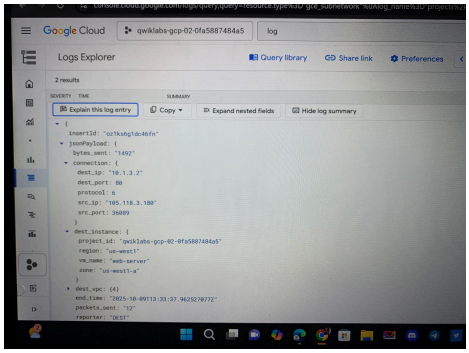


Third step: analyze the web server Flow logs

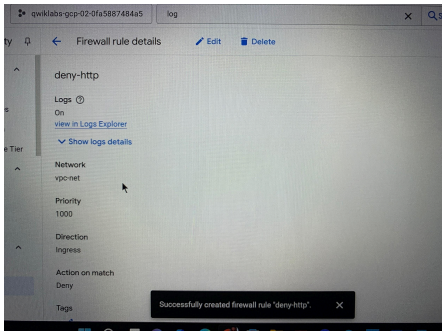
I accessed and analyzed the VPC Flow logs for the web server using the logs explorer.



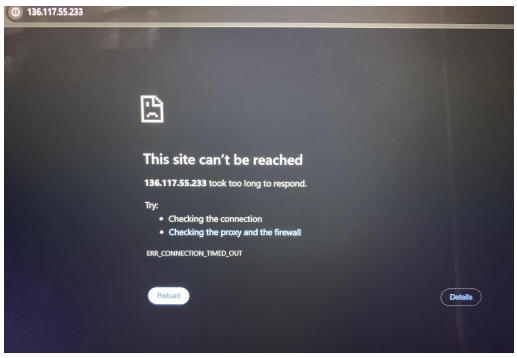
Within the entry, an expansion of **“jsonpayload”** was made by clicking the expanding arrow “>”
Here, I can examine the details about the network connection to the web server ;
dest_ip —> This is destination IP address of the web server which is **“10.1.3.2”**
dest_port —> This is the destination port number of the web server which is HTTP port **“80”**
src_ip —> This is the source port number that’s assigned to my computer **“105.118.3.180”**
src_port —> This is the source port number that’s assigned to my computer, which is **“36089”**



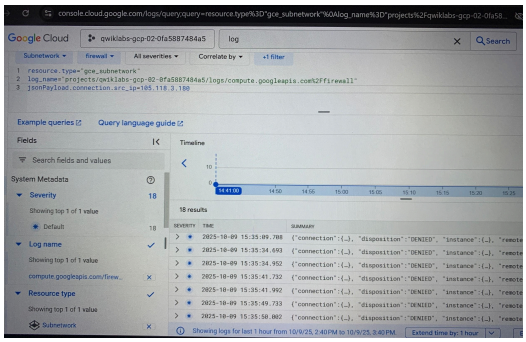
Fourth step: Create a firewall rule to deny HTTP traffic
I created a new firewall rule that denies traffic from port 80



Final step: Analyze The Firewall logs
Here, I’ll test the **“deny-http”** firewall rule that was created previously by trying to access the server once more through the External IP.



This error occurred because of the “ deny-http” firewall rule I created previously. Then, I’ll verify this action by accessing the logs explorer to analyze the firewall logs for the web server.

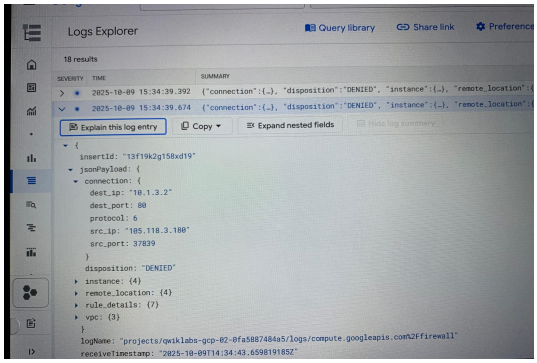


I'll need to examine the details about the network connection to the web server to verify if the firewall rule was successfully triggered

dest_ip —> destination IP address of the web server

Disposition —> this field indicates whether the connection was allowed or denied which in this case is **denied.**

Protocol —> The protocol is " 6" which is the IANA protocol for TCP traffic



Following these steps, I now have practical experience in creating and testing firewall rules for a web server in a cloud environment. By creating firewall rules and analyzing log entries, I have a familiarity with the intricacies of perimeter protection. This is useful for monitoring and analyzing potential security incidents or threats which is an essential part of a security analyst's role.