**Creating Firewall Rules on a Google Cloud VPC Network**

**Introduction**

In this hands-on lab, we will be presented with a custom VPC that has four instances spread across three subnets with zero firewall rules created. We will configure two different firewall rules: one to allow SSH access to all instances on the network, and another one using specific network tags to only allow ICMP (ping) access to one instance, and only from a specific subnet. This will demonstrate using both wide-scope and narrow-scope firewall rules.

**How to Log in to Google Lab Accounts**

On the lab page, right-click **Open GCP Console** and select the option to open it in a new private browser window (this option will read differently depending on your browser — e.g., in Chrome, it says "Open Link in Incognito Window"). Then, sign in to Google Cloud Platform using the credentials provided on the lab page.

On the *Welcome to your new account* screen, review the text, and click **Accept**. In the "Welcome L.A.!" pop-up once you're signed in, check to agree to the terms of service, choose your country of residence, and click **Agree and Continue**.

**Steps Before Starting the Lab**

1. In the top-left menu, click **VPC network**.
2. Click the **default** network.
3. Click **DELETE VPC NETWORK**.
4. Click **DELETE** in the *Delete a network* dialog. You can continue on to the next steps while it's deleting. You may have to refresh the page after the operation is complete.
5. Click **Firewall rules** in the left-hand menu. Notice we do not have any created for the custom-vpc network.
6. From the top-left menu, click **Compute Engine**.
7. Click on the **SSH** button to the right of any of the four instances listed. The SSH session will eventually time out because we do not have port 22 access (SSH) to any instances on our network, which we need to fix.

**Allow SSH Access to All Instances**

1. In the Google console, from the top-left menu, scroll down to *VPC network*, and then click on **Firewall rules** from the sub-menu.
2. Click **Create firewall rule**.
3. Set the following values:
   * *Name*: **ssh-allow**
   * *Network*: **custom-vpc**
   * *Targets*: **All instances in the network**
   * *Source filter*: **IP ranges**
   * *Source IP ranges*: **0.0.0.0/0**
   * *Protocols and ports*: **Specified protocols and ports**
     + *tcp*: Check, and type in **22**
4. Click **Create**. It will take about 10 seconds for the rule to finish creating.
5. From the top-left menu, click **Compute Engine**.
6. Click any of the **SSH** buttons next to our instances. It should successfully connect. Close out of the session.

**Apply Network Tag to instance-2**

1. Still on the *VM instances* page, click **instance-2**.
2. Click **EDIT**.
3. Under *Network tags*, enter "icmp-allow".
4. Hit **Enter** to confirm the tag.
5. Click **Save** at the bottom.
6. From the top-left menu, select **VPC network**.
7. Copy the IP address listed for *subnet-a* into a text file, as we will need it a little later.

**Create a Narrow-Scope Firewall Rule for instance-2**

1. Click **Firewall rules** in the left-hand menu.
2. Click **CREATE FIREWALL RULE**.
3. Set the following values:
   * *Name*: **allow-icmp**
   * *Network*: **custom-vpc**
   * *Targets*: **Specified target tags**
   * *Target tags*: Enter "icmp-allow", and hit **Enter**
   * *Source filter*: **IP ranges**
   * *Source IP ranges*: Enter the *subnet-a* IP address you noted a minute ago
   * *Protocols and ports*: **Specified protocols and ports**
     + *Other protocols*: Check, and type in **icmp**
4. Click **Create**.

**Test ICMP Firewall Rule for Success**

1. From the top-left menu, click **Compute Engine**.
2. Copy the internal IP next to *instance-2* (it should be 10.0.2.2).
3. Click **SSH** next to *instance-1a*.
4. Once the connection is established, attempt to ping *instance-2*:

ping <INSTANCE-2\_INTERNAL\_IP>

It should be successful.

1. Hit **Ctrl+C** to quit ping.
2. Copy the internal IP next to *instance-3* (it should be 10.0.3.2).
3. Back in the *instance-1a* terminal, attempt to ping *instance-3*:

ping <INSTANCE-3\_INTERNAL\_IP>

It will fail because *instance-3* doesn't have the *icmp-allow* applied to it.

1. Hit **Ctrl+C** to quit ping.
2. Close out of the *instance-1a* session.
3. Click **SSH** next to *instance-3*.
4. Once the connection is established, attempt to ping *instance-2* again:

ping <INSTANCE-2\_INTERNAL\_IP>

It should *not* be successful because the firewall rule allowing ICMP access doesn't apply to the IP range for *subnet-c*.

**Conclusion**

Congratulations on successfully completing this hands-on lab!