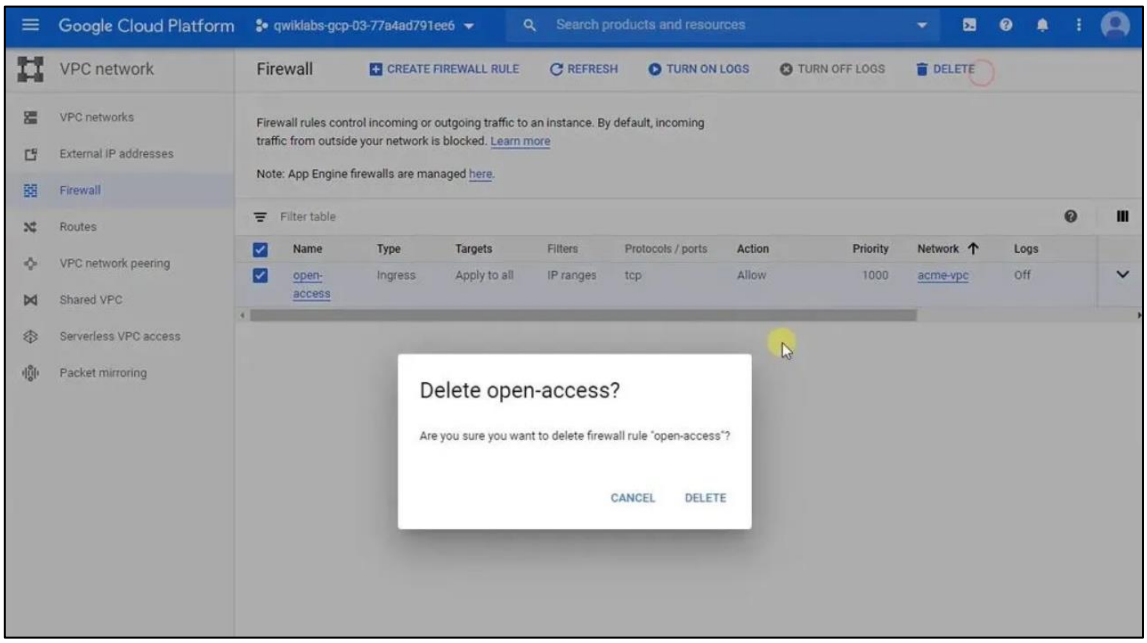
Build and Secure Networks in Google Cloud: Challenge Lab

Author: Vedant Kakde | **GitHub Profile:** github.com/vedant-kakde | **LinkedIn Profile:** linkedin.com/in/vedant-kakde/

1. Remove the overly permissive rules

This task is very simple. You only need to the open-access firewall rules.

1. In the Cloud Console, navigate to **Menu** > **VPC Network** > **Firewall**
2. Check the box next to the rule named `open-access`.
3. Click on **DELETE** to remove it.



2. Start the bastion host instance

1. In the Cloud Console, navigate to **Menu** > **Compute Engine** > **VM instances**
2. Check the box next to the instance named `bastion`.
3. Click on **Start** to run the instance.

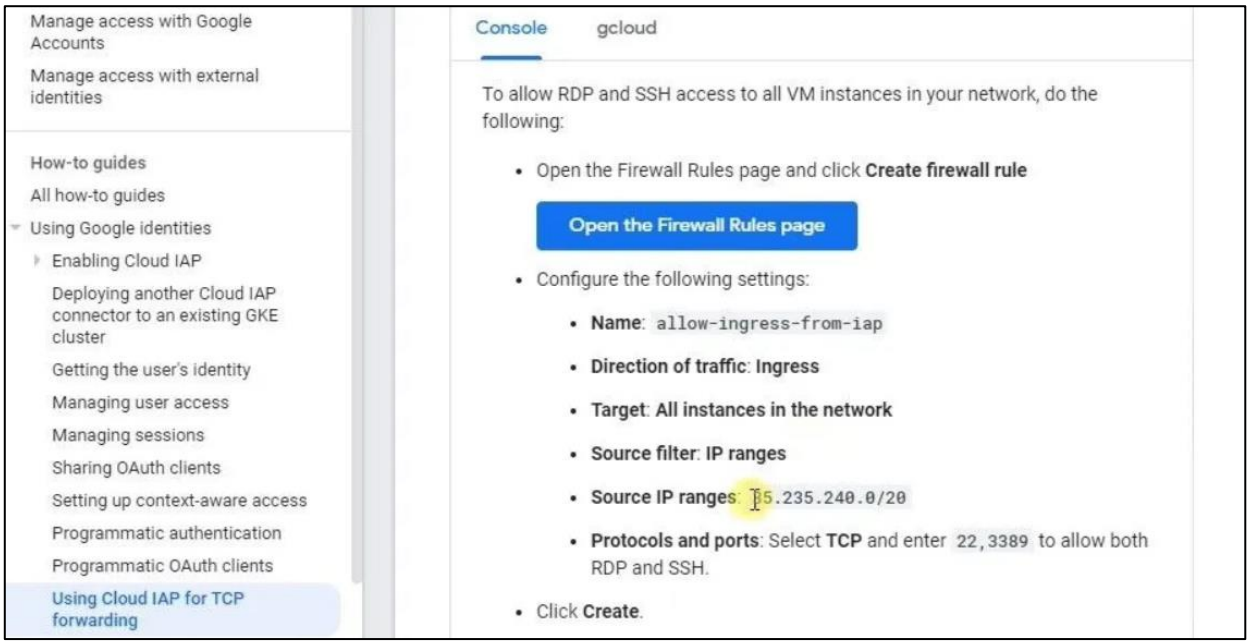
3. Create a firewall rule that allows SSH (tcp/22) from the IAP service and add network tag on bastion

Add network tag on bastion

1. On the VM instances page, click on the name of the **bastion** instance.
2. Click **EDIT** on the details page.
3. Add `bastion` to the **Network tags** field.
4. Scroll to the button of the page and click **Save**.

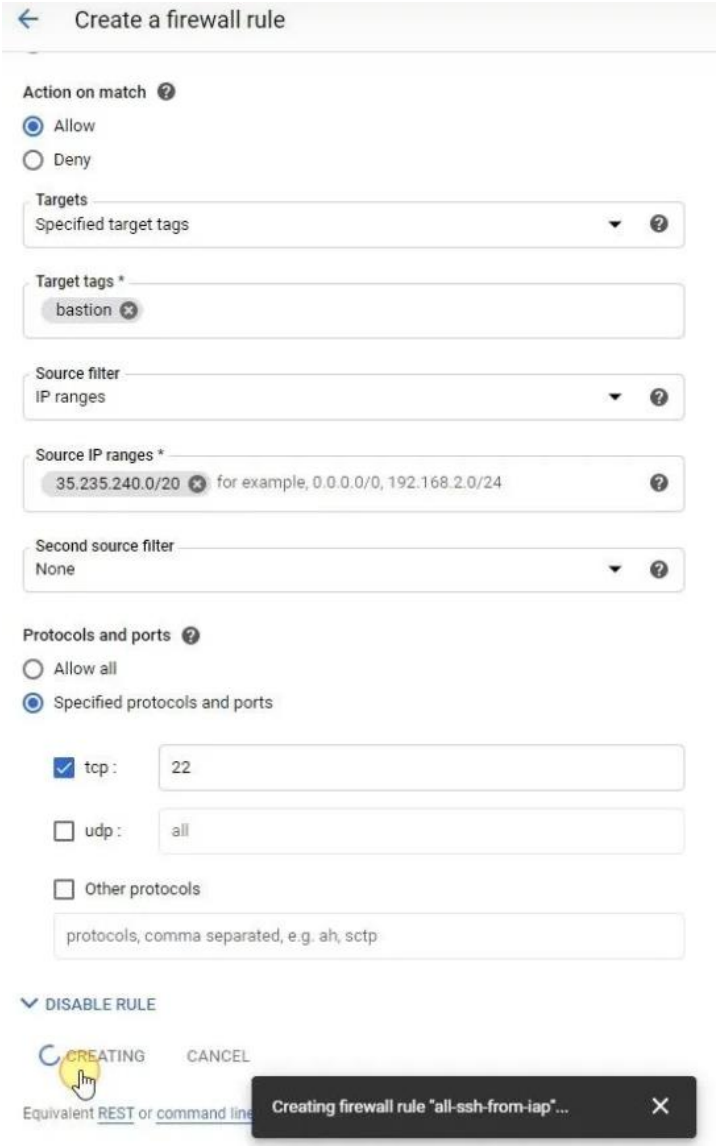
Create firewall rule to allow SSH from the IAP service

Read **Using IAP for TCP forwarding** in the Google Cloud Documentation before you create the firewall rule.



1. Go back to the Firewall Rules page, and click **Create firewall rule**.
2. Configure the following settings:

Field	**Value**
Name	e.g. `allow-ssh-from-iap`
Direction of traffic	Ingress
Targets	Specified target tags
Target tags	`bastion`
Source IP ranges	`35.235.240.0/20`
Protocols and ports	Select **TCP** and enter `22` to allow SSH

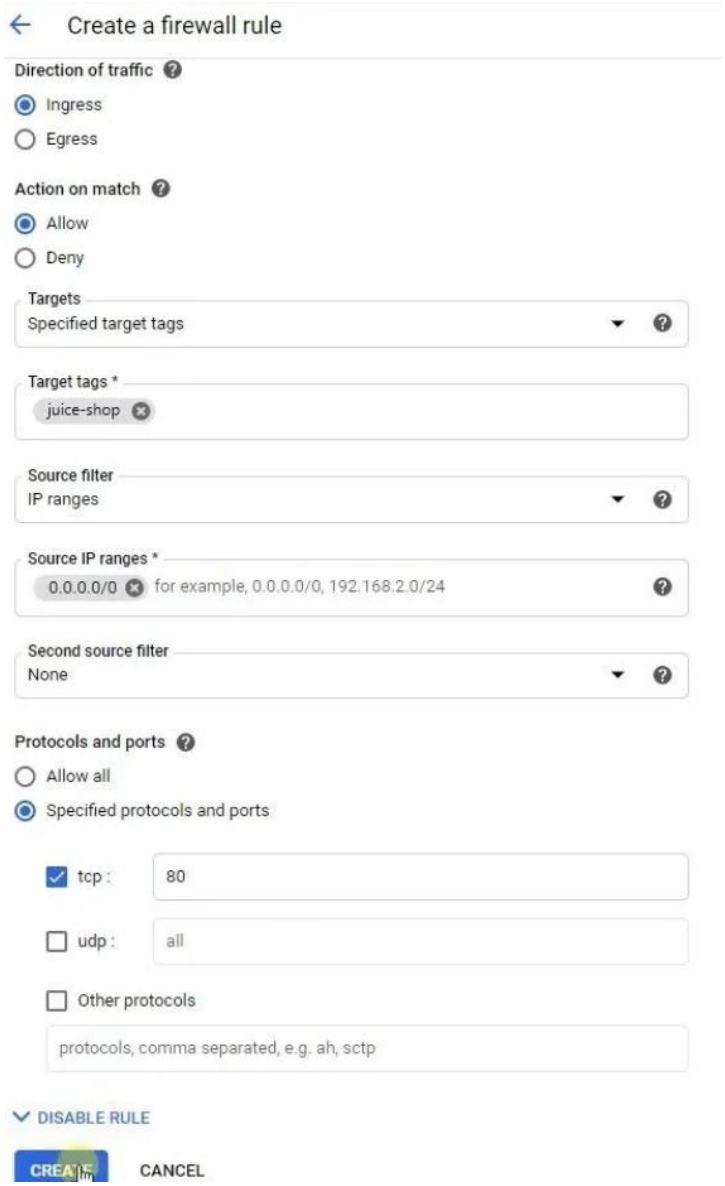


4. Create a firewall rule that allows traffic on HTTP (tcp/80) to any address and add network tag on juice-shop

Create firewall rule to allow HTTP traffic to juice-shop

1. On the Firewall Rules page, and click **Create firewall rule**.
2. Configure the following settings:

Field	**Value**
Name	e.g. `allow-http-ingress`
Direction of traffic	Ingress
Targets	Specified target tags
Target tags	`juice-shop`
Source IP ranges	`0.0.0.0/0`
Protocols and ports	Select **TCP** and enter `80` to allow HTTP



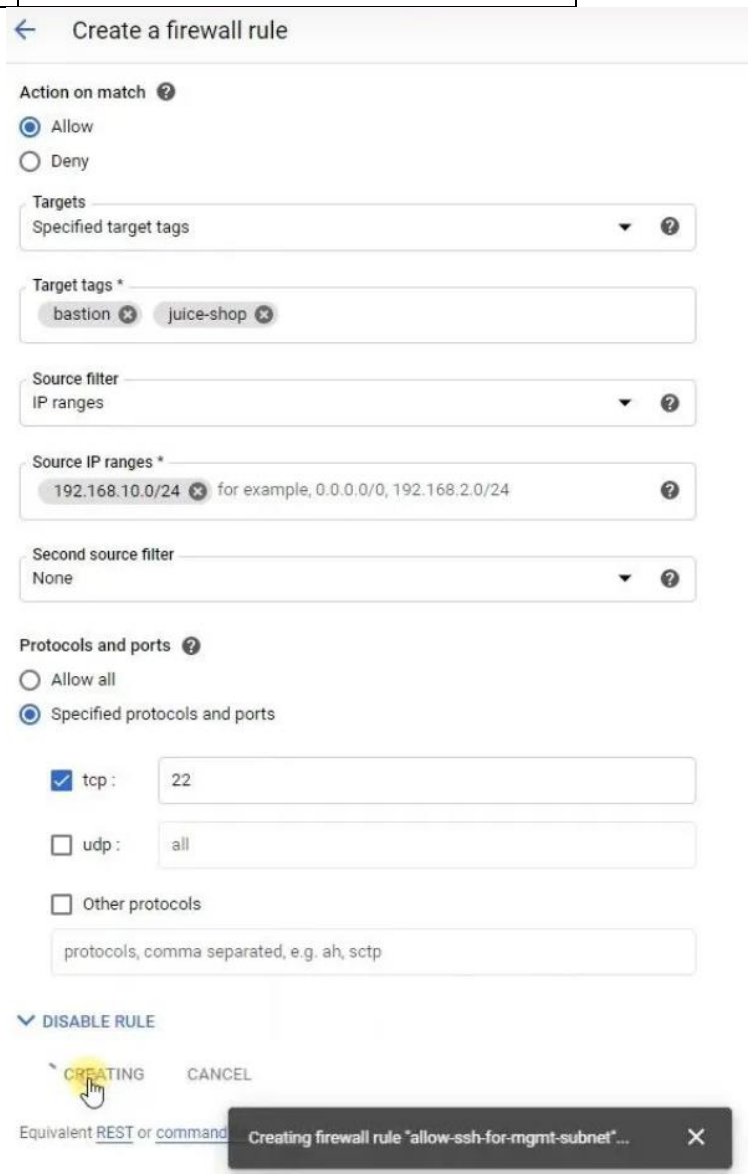
Add network tag on juice-shop

1. On the VM instances page, click on the name of the **juice-shop** instance.
2. Click **EDIT** on the details page.
3. Add `juice-shop` to the **Network tags** field.
4. Scroll to the button of the page and click **Save**.

5. Create a firewall rule that allows traffic on SSH (tcp/22) from acme-mgmt-subnet network address and add network tag on juice-shop

1. Navigate to **VPC network** > **VPC networks**.
2. Copy the IP address range of the `acme-mgmt-subnet`.
3. Go back to the Firewall Rules page, and click **Create firewall rule**.
4. Configure the following settings:

Field	Value
Name	e.g. `allow-ssh-from-mgmt-subnet`
Direction of traffic	Ingress
Targets	Specified target tags
Target tags	`bastion` and `juice-shop`
Source IP ranges	*IP address range of your aceme-mgmt-subnet*
Protocols and ports	Select **TCP** and enter `22` to allow SSH



6. SSH to bastion host via IAP and juice-shop via bastion

After configuring the firewall rules, try to verify the environment via the bastion.

1. Navigate to **Compute Engine** > **VM instances**.
2. Copy the Internal IP of the **juice-shop** instance.
3. Click on the SSH button in the row of the **bastion** instance.
4. In the SSH console, access the juice-shop from the bastion using the following command:

```
ssh <internal-IP-of-juice-shop>
```

(Remember to REPLACE `<internal-IP-of-juice-shop>` with the copied IP address)

Congratulations! You completed this challenge lab.