Build and Secure Networks in Google Cloud: Challenge Lab

GSP322

Overview

For this Challenge Lab you must complete a series of tasks within a limited time period. Instead of following step-by-step instructions, you'll be given a scenario and task - you figure out how to complete it on your own! An automated scoring system (shown on this page) will provide feedback on whether you have completed your tasks correctly.

To score 100% you must complete all tasks within the time period!

When you take a Challenge Lab, you will not be taught Google Cloud concepts. You'll need to use your advanced Compute Engine and general Google Cloud skills to assess how to build the solution to the challenge presented. This lab is only recommended for students who have advanced Google Cloud and Compute Engine skills. Are you up for the challenge?

Topics tested

- Secure remote ssh access via IAP-enabled bastion
- Firewall configuration and review

Prerequisites

- Familiarity with VPC Networks
- Firewall rules and network tags
- IAP

Setup

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This Qwiklabs hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

What you need

To complete this lab, you need:

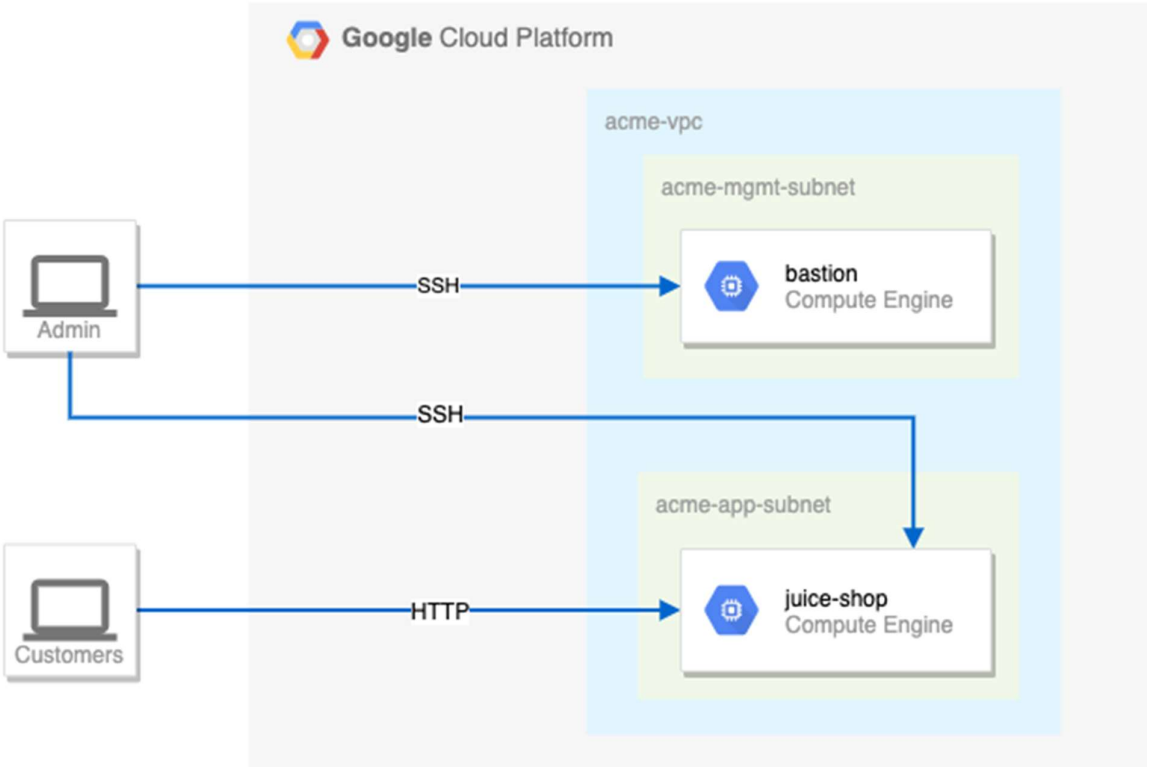
- Access to a standard internet browser (Chrome browser recommended).
- Time to complete the lab.
  Note: If you already have your own personal Google Cloud account or project, do not use it for this lab.

Note: If you are using a Pixelbook, open an Incognito window to run this lab.

Challenge scenario

You are a security consultant brought in by Jeff, who owns a small local company, to help him with his very successful website (juiceshop). Jeff is new to Google Cloud and had his neighbour's son set up the initial site. The neighbour's son has since had to leave for college, but before leaving, he made sure the site was running.

You need to help out Jeff and perform appropriate configuration for security. Below is the current situation:



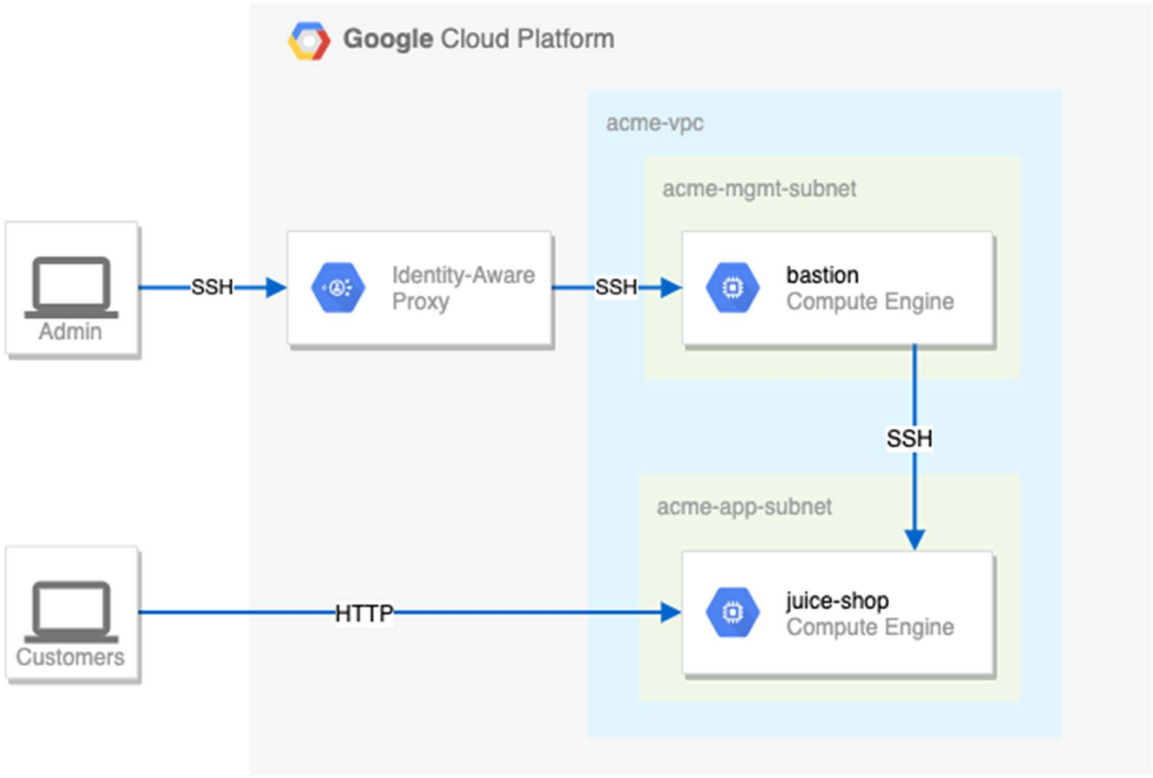
Your challenge

You need to configure this simple environment securely. Your first challenge is to set up appropriate firewall rules and virtual machine tags. You also need to ensure that SSH is only available to the bastion via IAP.

For the firewall rules, make sure:

- The bastion host does not have a public IP address.
- You can only SSH to the bastion and only via IAP.
- You can only SSH to juice-shop via the bastion.
- Only HTTP is open to the world for `juice-shop`.
  Tips and tricks:

- Pay close attention to the network tags and the associated VPC firewall rules.
- Be specific and limit the size of the VPC firewall rule source ranges.
- Overly permissive permissions will not be marked correct.



Suggested order of actions:

1. Check the firewall rules. Remove the overly permissive rules.
2. Navigate to Compute Engine in the Cloud Console and identify the bastion host. The instance should be stopped. Start the instance.
3. The bastion host is the one machine authorized to receive external SSH traffic. Create a firewall rule that allows SSH (tcp/22) from the IAP service. The firewall rule should be enabled on bastion via a network tag.

4. The `juice-shop` server serves HTTP traffic. Create a firewall rule that allows traffic on HTTP (tcp/80) to any address. The firewall rule should be enabled on juice-shop via a network tag.
5. You need to connect to `juice-shop` from the bastion using SSH. Create a firewall rule that allows traffic on SSH (tcp/22) from `acme-mgmt-subnet` network address. The firewall rule should be enabled on `juice-shop` via a network tag.
6. In the Compute Engine instances page, click the SSH button for the bastion host. Once connected, SSH to `juice-shop`.

Congratulations!

You've completed the challenge lab and helped Jeff tighten security.

Take your next lab

This lab is also part of a series of labs called Challenge Labs. These labs are designed test your Google Cloud knowledge and skill. Search for "Challenge Lab" in the lab catalog and challenge yourself!

Google Cloud Training & Certification

...helps you make the most of Google Cloud technologies. Our classes include technical skills and best practices to help you get up to speed quickly and continue your learning journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. Certifications help you validate and prove your skill and expertise in Google Cloud technologies.
Manual Last Updated January 14, 2021
Manual Last Tested October 26, 2020

Solution:

Step 1
gcloud compute firewall-rules delete open-access

step 2
gcloud compute instances start bastion

then n

step 3
gcloud compute firewall-rules create ssh-ingress --allow=tcp:22 --source-ranges 35.235.240.0/20 --target-tags ssh-ingress --network acme-vpc

gcloud compute instances add-tags bastion --tags=ssh-ingress --zone=us-central1-b

step 4
gcloud compute firewall-rules create http-ingress --allow=tcp:80 --source-ranges 0.0.0.0/0 --target-tags http-ingress --network acme-vpc

step 5
gcloud compute instances add-tags juice-shop --tags=http-ingress --zone=us-central1-b

step 6

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>
```