Controlling Access to VPC Networks

1 hour 30 minutesFree

Rate Lab

**Overview**

In this lab, you create two nginx web servers and control external HTTP access to the web servers using tagged firewall rules. Then you explore IAM roles and service accounts.

Objectives

In this lab, you learn how to perform the following tasks:

* Create an nginx web server
* Create tagged firewall rules
* Create a service account with IAM roles
* Explore permissions for the Network Admin and Security Admin roles

**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 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 the Google Cloud Platform 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 GCP account or project, do not use it for this lab.

**Task 1. Create the web servers**

Create two web servers (**blue** and **green**) in the **default** VPC network. Then install **nginx** on the web servers and modify the welcome page to distinguish the servers.

Create the blue server

Create the **blue** server with a network tag.

1. In the Cloud Console, on the **Navigation menu** (Navigation menu), click **Compute Engine** > **VM instances**.
2. Click **Create**.
3. Specify the following, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | blue |
| Region | *Choose a region* |
| Zone | *Choose a zone* |

1. You can choose the **region** and **zone** provided in the Qwiklabs Connection Details or choose your own. For more information on available regions and zones, refer [here](https://cloud.google.com/compute/docs/regions-zones/#available).
2. Click **Management, security, disks, networking, sole tenancy**.
3. Click **Networking**.
4. For **Network tags**, type **web-server**.

Network tags are used by networks to identify which VM instances are subject to certain firewall rules and network routes. In the next task, you create a firewall rule to allow HTTP access for VM instances with the **web-server** tag. Alternatively, you could select the **Allow HTTP traffic** checkbox, which would tag this instance as **http-server** and create the tagged firewall rule for tcp:80 for you.

1. Click **Create**.

Create the green server

Create the **green** server without a network tag.

1. Click **Create instance**.
2. Specify the following, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | green |
| Region | *Choose a region* |
| Zone | *Choose a zone* |

1. You can choose the **region** and **zone** provided in the Qwiklabs Connection Details or choose your own. For more information on available regions and zones, refer [here](https://cloud.google.com/compute/docs/regions-zones/#available).
2. Click **Create**.

Install nginx and customize the welcome page

Install nginx on both VM instances and modify the welcome page to distinguish the servers.

1. For **blue**, click **SSH** to launch a terminal and connect.
2. Run the following command to install nginx:

sudo apt-get install nginx-light -y

1. Run the following command to open the welcome page in the nano editor:

sudo nano /var/www/html/index.nginx-debian.html

1. Replace the <h1>Welcome to nginx!</h1> line with <h1>Welcome to the blue server!</h1>.
2. Press **CTRL+O**, **ENTER**, **CTRL+X**.
3. Run the following command to verify the change:

cat /var/www/html/index.nginx-debian.html

The output should contain the following (**do not copy; this is example output**):

...

<h1>Welcome to the blue server!</h1>

<p>If you see this page, the nginx web server is successfully installed and

working. Further configuration is required.</p>

...

1. Close the SSH terminal to **blue**:

exit

Repeat the same steps for the **green** server:

1. For **green**, click **SSH** to launch a terminal and connect.
2. Run the following command to install nginx:

sudo apt-get install nginx-light -y

1. Run the following command, to open the welcome page in the nano editor:

sudo nano /var/www/html/index.nginx-debian.html

1. Replace the <h1>Welcome to nginx!</h1> line with <h1>Welcome to the green server!</h1>.
2. Press **CTRL+O**, **ENTER**, **CTRL+X**.
3. Run the following command to verify the change:

cat /var/www/html/index.nginx-debian.html

The output should contain the following (**do not copy; this is example output**):

...

<h1>Welcome to the green server!</h1>

<p>If you see this page, the nginx web server is successfully installed and

working. Further configuration is required.</p>

...

1. Close the SSH terminal to **green**:

exit

Click *Check my progress* to verify the objective.

Create the web servers

Check my progress

**Task 2. Create the firewall rule**

Create the tagged firewall rule and test HTTP connectivity.

Create the tagged firewall rule

Create a firewall rule that applies to VM instances with the **web-server** network tag.

1. In the Cloud Console, on the **Navigation menu**, click **VPC network** > **Firewall rules**.
2. Notice the **default-allow-internal** firewall rule.

The **default-allow-internal** firewall rule allows traffic on all protocols/ports within the **default** network. You want to create a firewall rule to allow traffic from outside this network to only the **blue** server, by using the network tag **web-server**.

1. Click **Create Firewall Rule**.
2. Specify the following, and leave the remaining settings as their defaults:

|  |  |
| --- | --- |
| **Property** | **Value (type value or select option as specified)** |
| Name | allow-http-web-server |
| Network | default |
| Targets | Specified target tags |
| Target tags | web-server |
| Source filter | IP Ranges |
| Source IP ranges | 0.0.0.0/0 |
| Protocols and ports | Specified protocols and ports |

1. For **tcp**, specify port **80**.

Make sure to include the **/0** in the **Source IP ranges** to specify all networks.

1. Click **Create**.

Create a test-vm

Create a **test-vm** instance using the gcloud command line.

1. In the Cloud Console, click **Activate Cloud Shell** (Cloud Shell).
2. If prompted, click **Continue**.
3. Run the following command to display the available zones:

gcloud compute zones list

1. Choose a zone from this list or use the one provided in the Qwiklabs Connection Details. It will be referred to as [YOUR\_ZONE].
2. Run the following command to create a **test-vm** instance, replacing [YOUR\_ZONE]:

gcloud compute instances create test-vm --machine-type=n1-standard-1 --subnet=default --zone=[YOUR\_ZONE]

The output should look like this (**do not copy; this is example output**):

NAME ZONE MACHINE\_TYPE PREEMPTIBLE INTERNAL\_IP EXTERNAL\_IP STATUS

test-vm us-central1-a n1-standard-1 10.142.0.4 35.237.134.68 RUNNING

You can easily create VM instances from the Cloud Console or the gcloud command line.

Click *Check my progress* to verify the objective.

Create the firewall rule and instance

Check my progress

Test HTTP connectivity

From **test-vm** curl the internal and external IP addresses of **blue** and **green**.

1. In the Cloud Console, on the **Navigation menu**, click **Compute Engine** > **VM instances**. Note the internal and external IP addresses of **blue** and **green**.
2. For **test-vm**, click **SSH** to launch a terminal and connect.
3. To test HTTP connectivity to **blue**'s internal IP, run the following command, replacing **blue**'s internal IP:

curl <Enter blue's internal IP here>

You should see the Welcome to the blue server! header.

1. To test HTTP connectivity to **green**'s internal IP, run the following command, replacing **green**'s internal IP:

curl <Enter green's internal IP here>

You should see the Welcome to the green server! header.

You can HTTP access both servers using their internal IP addresses. The connection on tcp:80 is allowed by the **default-allow-internal** firewall rule, because **test-vm** is on the same VPC network as the web servers (**default** network).

1. To test HTTP connectivity to **blue**'s external IP, run the following command, replacing **blue**'s external IP:

curl <Enter blue's external IP here>

You should see the Welcome to the blue server! header.

1. To test HTTP connectivity to **green**'s external IP, run the following command, replacing **green**'s external IP:

curl <Enter green's external IP here>

This should not work!

1. Press **CTRL+C** to stop the HTTP request.

As expected, you can only HTTP access the external IP address of the **blue** server, because the **allow-http-web-server** only applies to VM instances with the **web-server** tag.

To verify the same behavior from your browser, open a new tab and navigate to http://[External IP of server].

**Task 3. Explore the Network and Security Admin roles**

Cloud IAM lets you authorize who can take action on specific resources, which give you full control and visibility to manage cloud resources centrally. The following roles are used in conjunction with single-project networking to independently control administrative access to each VPC network:

* **Network Admin:** Permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates.
* **Security Admin:** Permissions to create, modify, and delete firewall rules and SSL certificates.

Explore these roles by applying them to a service account, which is a special Google account that belongs to your VM instance instead of to an individual end user. You will authorize **test-vm** to use the service account to demonstrate the permissions of the **Network Admin** and **Security Admin** roles, instead of creating a new user.

Verify current permissions

Currently, **test-vm** uses the [Compute Engine default service account](https://cloud.google.com/compute/docs/access/service-accounts#compute_engine_default_service_account), which is enabled on all instances created by the gcloud command-line tool and the Cloud Console.

Try to list or delete the available firewall rules from **test-vm**.

1. Return to the **SSH** terminal of the **test-vm** instance.
2. Run the following command to try to list the available firewall rules:

gcloud compute firewall-rules list

The output should look like this (**do not copy; this is example output**):

ERROR: (gcloud.compute.firewall-rules.list) Some requests did not succeed:

- Insufficient Permission

This should not work!

1. Run the following command to try to delete the **allow-http-web-server** firewall rule:

gcloud compute firewall-rules delete allow-http-web-server

1. Enter **Y**, if asked to continue.

The output should look like this (**do not copy; this is example output**):

ERROR: (gcloud.compute.firewall-rules.delete) Could not fetch resource:

- Insufficient Permission

This should not work!

The **Compute Engine default service account** does not have the right permissions to allow you to list or delete firewall rules. The same applies to other users who do not have the right roles.

Create a service account

Create a service account and apply the **Network Admin** role.

1. In the Cloud Console, on the **Navigation menu** (Navigation menu), click **IAM & admin** > **Service accounts**. Notice the **Compute Engine default service account**.
2. Click **Create service account**.
3. Set the **Service account name** to **Network-admin**.
4. Click **Create**.
5. For **Select a role**, select **Compute Engine > Compute Network Admin**.
6. Click **Continue**.
7. Click **Done**.

Optionally you could create and download a file that contains the private key. However, we can just stop **test-vm** and authorize it to use the service account.

Authorize test-vm

Authorize **test-vm** to use the **Network-admin** service account.

The Network Admin role, provides permissions to:



List the available firewall rules



Create a firewall rules



Modify the available firewall rules



Delete the available firewall rules



Neither list, create, modify, or delete the available firewall rules

Submit

1. On the **Navigation menu**, click **Compute Engine** > **VM instances**.
2. Click on the name of the **test-vm** instance to open the **VM instance details** page.
3. Click **Stop** and confirm to **Stop** the instance. Wait for the instance to stop before proceeding to the next step.

An instance must be stopped to edit its service account.

1. Once the instance stopped, click **Edit**.

Click on the name of the **test-vm** instance to open the **VM instance details** page.

1. Click **Edit**.
2. Select **Network-admin** for **Service account**.
3. Click **Save** and wait for the instance to update.
4. Click **Start** and confirm to **Start** the instance.
5. Return to the **Vm instances** page and wait for **test-vm** to change to a running state.
6. Click **SSH** for the **test-vm** instance.

verify permissions

1. Run the following command to try to list the available firewall rules:

gcloud compute firewall-rules list

The output should look like this (**do not copy; this is example output**):

NAME NETWORK DIRECTION PRIORITY ALLOW DENY

allow-http-web-server default INGRESS 1000 tcp:80

default-allow-icmp default INGRESS 65534 icmp

default-allow-internal default INGRESS 65534 all

default-allow-rdp default INGRESS 65534 tcp:3389

default-allow-ssh default INGRESS 65534 tcp:22

This should work!

1. Run the following command to try to delete the **allow-http-web-server** firewall rule:

gcloud compute firewall-rules delete allow-http-web-server

1. Enter **Y**, if asked to continue.

The output should look like this (**do not copy; this is example output**):

ERROR: (gcloud.compute.firewall-rules.delete) Could not fetch resource:

- Required 'compute.firewalls.delete' permission for 'projects/[PROJECT\_ID]/global/firewalls/allow-http-web-server'

This should not work!

As expected, the **Network Admin** role has permissions to list but not modify/delete firewall rules.

Update service account and verify permissions

Update the **Network-admin** service account by providing it with the **Security Admin** role.

The Security Admin role, provides permissions to:



List the available firewall rules



Create a firewall rules



Modify the available firewall rules



Delete the available firewall rules



Neither list, create, modify, or delete the available firewall rules

Submit

1. In the Cloud Console, on the **Navigation menu** (Navigation menu), click **IAM & admin** > **IAM**.
2. Find the **Network-admin** account. Focus on the **Name** column to identify this account.
3. Click on the pencil icon for the **Network-admin** account.
4. Change **Role** to **Compute Engine > Compute Security Admin**.
5. Click **Save**.
6. Return to the **SSH** terminal of the **test-vm** instance.
7. Run the following command to try to list the available firewall rules:

gcloud compute firewall-rules list

The output should look like this (**do not copy; this is example output**):

NAME NETWORK DIRECTION PRIORITY ALLOW DENY

allow-http-web-server default INGRESS 1000 tcp:80

default-allow-icmp default INGRESS 65534 icmp

default-allow-internal default INGRESS 65534 all

default-allow-rdp default INGRESS 65534 tcp:3389

default-allow-ssh default INGRESS 65534 tcp:22

This should work!

1. Run the following command to try to delete the **allow-http-web-server** firewall rule:

gcloud compute firewall-rules delete allow-http-web-server

1. Enter **Y**, if asked to continue.

The output should look like this (**do not copy; this is example output**):

Deleted [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-00e186e4b1cec086/global/firewalls/allow-http-web-server].

This should work!

As expected, the **Security Admin** role has permissions to list and delete firewall rules.

Verify the deletion of the firewall rule

Verify that you can no longer HTTP access the external IP of the **blue** server because you deleted the **allow-http-web-server** firewall rule.

1. Return to the **SSH** terminal of the **test-vm** instance.
2. To test HTTP connectivity to **blue**'s external IP, run the following command, replacing **blue**'s external IP:

curl <Enter blue's external IP here>

This should not work!

1. Press **CTRL+C** to stop the HTTP request.

Provide the **Security Admin** role to the right user or service account to avoid any unwanted changes to your firewall rules!

Click *Check my progress* to verify the objective.

Explore the Network and Security Admin roles

Check my progress

**Task 4. Review**

In this lab, you created two nginx web servers and controlled external HTTP access using a tagged firewall rule. Then you created a service account with first the **Network Admin** role and then the **Security Admin** role to explore the different permissions of these roles.

If your company has a security team that manages firewalls and SSL certificates and a networking team that manages the rest of the networking resources, grant the security team the **Security Admin** role and the networking team the **Network Admin** role.