

Controlling Access for VPC Networks

Introduction:

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. You will 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

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

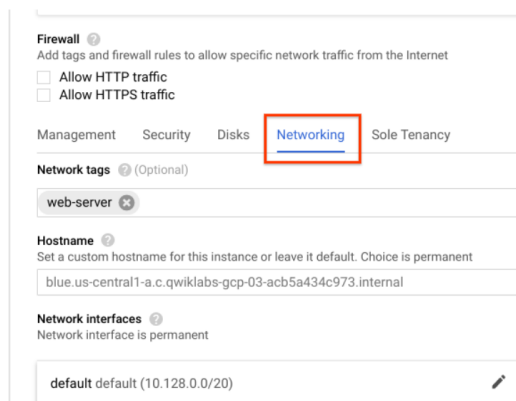
Create the **blue** server with a network tag.

1. In the Console, navigate to **Navigation menu > Compute Engine > VM instances**.
2. Click **Create Instance**.
3. Set the following values, leave all other values at their defaults:

Property	Value (type value or select option as specified)
Name	blue
Region	us-central1 (Iowa)
Zone	us-central1-a

For more information on available regions and zones, refer [here](#).

4. Click **Management, disks, networking, sole tenancy**.
5. Click **Networking**.



The screenshot shows the 'Networking' tab in the Google Cloud Platform console for a VM instance configuration. The 'Firewall' section is at the top, with options to 'Allow HTTP traffic' and 'Allow HTTPS traffic'. Below this, the 'Networking' tab is selected, showing 'Network tags' with a tag named 'web-server'. The 'Hostname' section shows a custom hostname: 'blue.us-central1-a.c.qwiklabs-gcp-03-acb5a434c973.internal'. The 'Network interfaces' section shows a default interface with IP '10.128.0.0/20'.

6. For **Network tags**, type **web-server**.
7. Click Create.

Create the green server

Create the green server without a network tag.

1. Still in the Console, in the VM instances dialog, click Create instance.
2. Set the following values, leave all other values at their defaults:
3. Click Create.

Property	Value (type value or select option as specified)
Name	green
Region	us-central1 (Iowa)
Zone	us-central1-a

Install nginx and customize the welcome page

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

1. Still in the VM instances dialog, for blue, click SSH to launch a terminal and connect.
2. In the SSH terminal to blue, run the following command to install nginx:
sudo apt-get install nginx-light -y
3. Open the welcome page in the nano editor:
sudo nano /var/www/html/index.nginx-debian.html
4. Replace the `<h1>Welcome to nginx!</h1>` line with `<h1>Welcome to the blue server!</h1>`.
5. Press CTRL+o, ENTER, CTRL+x.
6. 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>
...
```

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

exit

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

8. For green, click SSH to launch a terminal and connect.

9. Install nginx:

sudo apt-get install nginx-light -y

10. Open the welcome page in the nano editor:

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

11. Replace the `<h1>Welcome to nginx!</h1>` line with `<h1>Welcome to the green server!</h1>`.

12. Press CTRL+o, ENTER, CTRL+x.

13. 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>
...
```

14. Close the SSH terminal to green:

exit

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 Console, navigate to Navigation menu > VPC network > Firewall.

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.

3. Click Create Firewall Rule.

4. Set the following values, leave all other values at their defaults and click

Create:

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, and then <i>check tcp, type: 80;</i> and <i>check Other protocols, type: icmp.</i>

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

Create a test-vm

Create a test-vm instance using the Cloud Shell command line.

Create a test-vm instance, in the us-central1-a zone:

```
> gcloud compute instances create test-vm --machine-type=f1-micro --subnet=default
--zone=us-central1-a
```

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  f1-micro      10.142.0.4
35.237.134.68  RUNNING
```

Test HTTP connectivity

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

1. In the Console, navigate to Navigation menu > Compute Engine > VM instances.
2. Note the internal and external IP addresses of blue and green.
3. For test-vm, click SSH to launch a terminal and connect.
4. 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.
5. To test HTTP connectivity to green's internal IP, run the following command, replacing green's internal IP: **curl -c 3 <Enter green's internal IP here>**

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

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

6. 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>`**
7. To test HTTP connectivity to green's external IP, run the following command, replacing green's external IP: **`curl -c 3 <Enter green's external IP here>`**
This should not work! The request hangs.
8. Press `CTRL+c` to stop the HTTP request.

As expected, you are only able to HTTP access the external IP address of the blue server as the `allow-http-web-server` only applies to VM instances with the `web-server` tag.

You can verify the same behavior from your browser by opening a new tab and navigating to `http://[External IP of server]`.

Explore the Network and Security Admin roles

Cloud IAM lets you authorize who can take action on specific resources, giving 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. Rather than creating a new user, you will authorize **test-vm** to use the service account to demonstrate the permissions of the **Network Admin** and **Security Admin** roles.

Verify current permissions

Currently, **test-vm** uses the [Compute Engine default service account](#), which is enabled on all instances created by Cloud Shell command-line 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. 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!

3. Try to delete the allow-http-web-server firewall rule:
`> gcloud compute firewall-rules delete allow-http-web-server`
4. 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 Console, navigate to **Navigation menu > IAM & admin > Service Accounts**.
2. Notice the **Compute Engine default service account**.
3. Click **Create service account**.
4. Set the **Service account** name to **Network-admin** and click **CREATE AND CONTINUE**.
5. For **Select a role**, select **Compute Engine > Compute Network Admin** and click **CONTINUE** then click **DONE**.

6. After creating a service account 'Network-admin', click on three dots at the right corner and click **Manage Key** in the dropdown, then click on **Add Key** and select **Create new key** from the dropdown. Click **Create** to download your JSON output.

7. Click **Close**.

A JSON key file download to your local computer. Find this key file, you will upload it into the VM in a later step.

8. Rename the JSON key file on your local machine to **credentials.json**.

Authorize test-vm and verify permissions

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

1. Return to the **SSH** terminal of the **test-vm** instance.
2. To upload **credentials.json** through the SSH VM terminal, click on the gear icon in the upper-right corner, and then click **Upload file**.
3. Select **credentials.json** and upload it.
4. Click **Close** in the File Transfer window.
5. Authorize the VM with the credentials you just uploaded:

```
gcloud auth activate-service-account --key-file credentials.json
```

The image you are using has the Cloud SDK pre-installed; therefore, you don't need to initialize the Cloud SDK. If you are attempting this lab in a different environment, make sure you have followed the procedures regarding installing the Cloud SDK.

6. 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!

7. Try to delete the **allow-http-web-server** firewall rule:

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

8. 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 the Security Admin role.

1. In the Console, navigate to Navigation menu > 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. 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!

8. Try to delete the **allow-http-web-server** firewall rule:

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

9. Enter **Y**, if asked to continue.

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 -c 3 <Enter blue's external IP here>
```

This should not work!

3. 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!