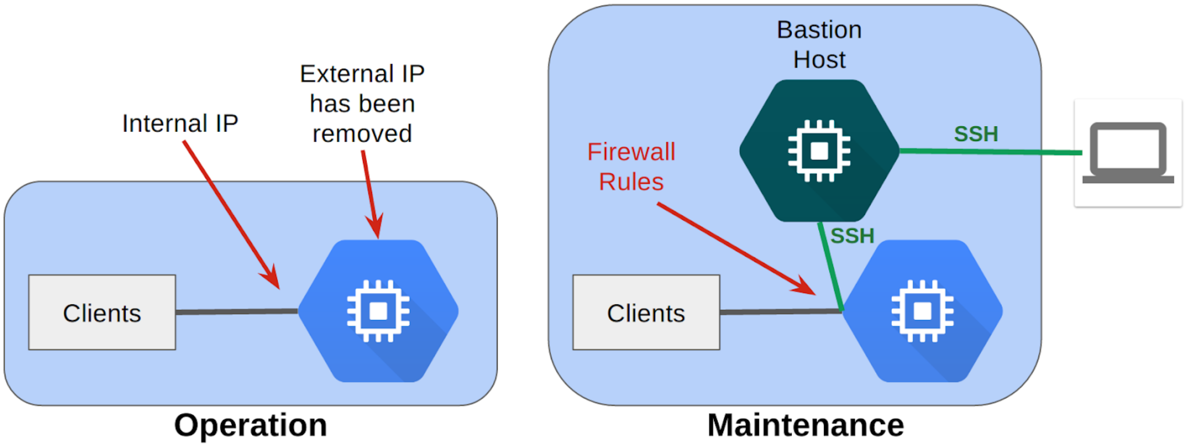
A best practice for infrastructure administration is to limit access to the resources. In this lab, you learn one method of hardening an infrastructure called a Bastion Host.



During operations, you harden the server by removing its external IP address, which prevents connections from the internet. During maintenance, you start up a bastion host that has an external IP address. You then connect via SSH to the bastion host, and from there to the server over the internal IP address. You can further restrict access with firewall rules.

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

- Create an application web server to represent a service provided to an internal corporate audience
- Prevent the web server from access to or from the internet
- Create a maintenance server, called a Bastion Host, to gain access to and verify internal connectivity to the application server

Launch an instance

Create VM instance .

1. Specify the following, and leave the remaining settings as their defaults:

Property	**Value (type value or select option as specified)**
Name	**webserver**

Region	**us-central1**
Zone	**us-central1-c**
Firewall	**Allow HTTP traffic**

4. Click **Create**.

Verify IP access

1. For **webserver**, click **SSH** to launch a terminal and connect.

Task 2: Restrict firewall rule settings for SSH

The default setting for a default or auto-type network is to allow SSH access from any source IP address. Restrict access to just your source IP address to see what happens when you try to connect from the GCP Console.

Find your IP address

Find the IP address of the computer you are using. One easy way to do this is to go to a website that provides this address.

1. Open a browser in a new tab.
2. Go to www.google.com and search for "what's my IP." It will either directly reply with your IP or give you a list of sites that perform this service.
3. Ensure that the IP address only contains numerals (IPv4) and is not represented in hexadecimals (IPv6).
4. Copy your IP address. It will be referred to as YOUR_IP_ADDRESS. You will be using it to modify the default firewall rule.

Edit the default SSH rule

1. **VPC network** > **Firewall rules**.
2. Click the **default-allow-ssh** rule, and then click **Edit**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	**Value (type value or select option as specified)**
Description	**Allow SSH from my IP only**
Source IP ranges	Remove **0.0.0.0/0** Add **[YOUR_IP_ADDRESS]**

4. Click **Save**. Wait until the firewall rule is updated (
5. **Compute Engine** > **VM instances**.
6. For **webserver**, click **SSH** to launch a terminal and connect.

What happened?

When you connect via SSH to an instance from your browser, you need to allow SSH from Cloud Platform resources, so you must allow connections from either any IP address or from Google's IP address range, which you can get from Public SPF records. If you want to restrict SSH access to just your IP address, you need to SSH from a terminal session.

For this lab, leaving SSH open to any connections is sufficient.

Reset the IP address range in the firewall rule

1. **VPC network** > **Firewall rules**.
2. Click the **default-allow-ssh** rule, and then click **Edit**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	**Value (type value or select option as specified)**

Description	**Allow SSH from all IPs**
Source IP ranges	Add **0.0.0.0/0**

4. Click **Save**. Wait until the firewall rule is updated (

Verify the change

1. On the **Navigation menu** (☰), click **Compute Engine** > **VM instances**.
2. For **webserver**, click **SSH** to launch a terminal and connect. Leave the terminal open for the next task.

Task 3: Install a simple web application

Install a simple web application on your instance to represent an internal application. You then secure it by preventing access from the internet.

Install and configure a web server

1. In the webserver SSH terminal, update the package index:

```
sudo apt-get update
content_copy
```

2. Install the apache2 package:

```
sudo apt-get install apache2 -y
content_copy
```

3. To create a new default web page by overwriting the default, run the following:

```
echo '<!doctype html><html><body><h1>Hello World!</h1></body></html>' | sudo
tee /var/www/html/index.html
content_copy
```

Verify that the web server is working

1. **Compute Engine** > **VM instances**.
2. For **webserver**, click the **external IP** to open in a new tab.

Task 4: Restrict firewall rule settings for HTTP

Restrict access to the web interface by changing the source IP address in the **default-allow-http** rule to your IP address.

Restrict HTTP access

1. In the GCP Console, on the **Navigation menu** (☰), click **VPC network** > **Firewall rules**.
2. Click the **default-allow-http** rule, and then click **Edit**.
3. Specify the following, and leave the remaining settings as their defaults:

Property	**Value (type value or select option as specified)**
Description	**Allow HTTP from my IP only**
Source IP ranges	Remove **0.0.0.0/0** Add **[YOUR_IP_ADDRESS]**

4. Click **Save**. Wait until the firewall rule is updated

Verify that you still have access to the web server

1. On the **Navigation menu** (☰), click **Compute Engine** > **VM instances**.
2. For **webserver**, click the **external IP** to open in a new tab. You should still see the "Hello World!" page.

Task 5: Restrict access to the VM from the internet

Edit the VM Properties

1. Return to the **VM instances** page of the GCP Console.
2. Click **webserver** to access the instance details.
3. Click **Edit**.
4. For **Network interfaces**, click the default network and change **External IP** from **Ephemeral** to **None**.
5. Click **Done**.
6. Click **Save**.

Try to access the VM

1. First try HTTP: In the left pane, click **VM instances**. Notice that **webserver** doesn't have a value under **External IP**.
2. Try SSH: for **webserver**, try to use the **SSH** link to launch a terminal and connect.

What happened?

The VM is no longer associated with an External IP. It is no longer reachable from the internet.

Task 6: Create a Bastion Host

Launch another instance

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	**bastion**

Region	**us-central1**
Zone	**us-central1-c**

3. Click **Create**.

Connect to the Bastion Host via SSH and verify access to webserver

1. For **bastion**, click **SSH** to launch a terminal and connect.
2. Verify that the home page on **webserver** is reachable from **bastion** by running the following command:

```
curl webserver
content_copy
```

Even though **webserver** is no longer associated with an external IP address, clients inside your network can still view and use the web service on this VM over the internal IP address.

3. From the **bastion** SSH terminal, connect to **webserver** by running the following command:

```
ssh -a webserver
```

4. When prompted, type **yes** to continue.

When instances do not have external IP addresses, they can only be reached by other instances on the network or via a managed VPN gateway.

In this case, the bastion VM serves as a management and maintenance interface to the webserver VM.

Task 7: Review

You restricted access to the **webserver** VM by removing the external IP address.

You created a bastion host named **bastion** to gain access to the webserver VM over its internal IP. Normally, you would harden the bastion host by restricting the source IPs that can access the bastion host, by editing the firewall rules just as you did earlier in this lab. When you're not using the bastion host, you can shut it down.