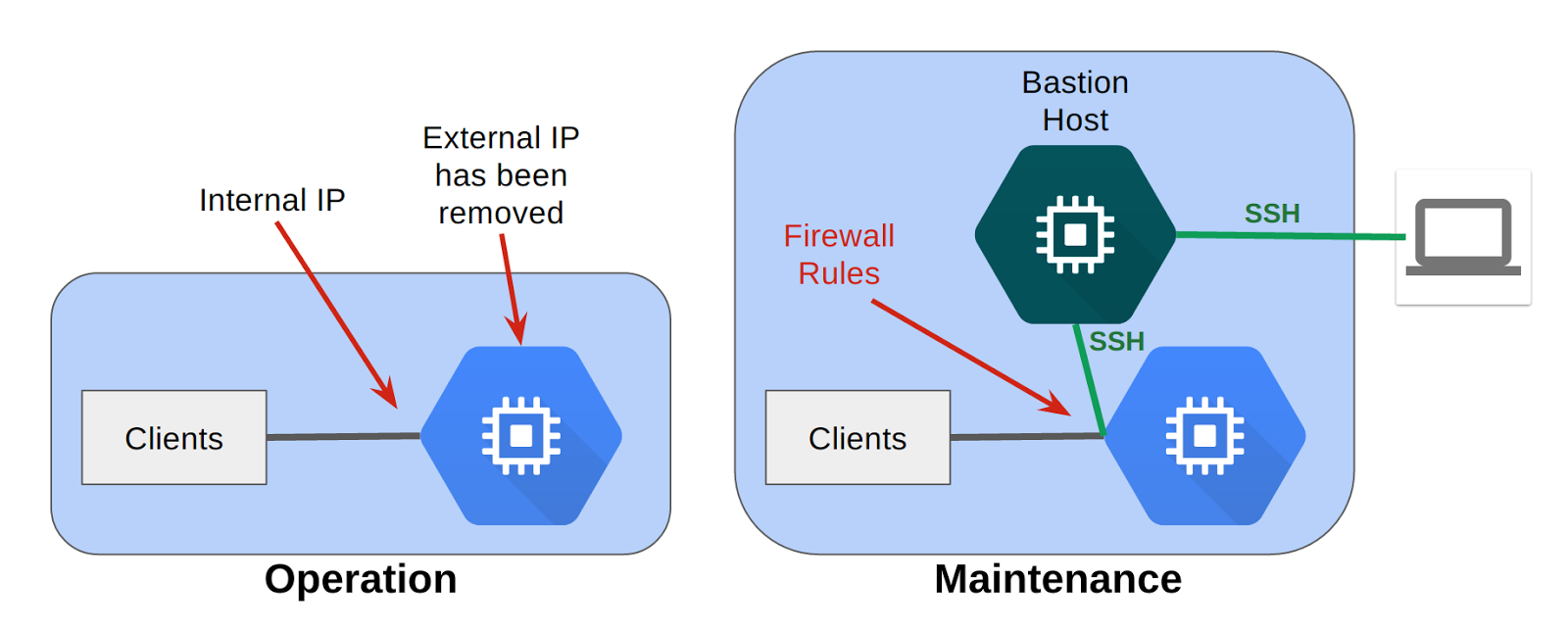
* [Bastion Host](https://googlecloud.qwiklabs.com/focuses/3291" \l "bastion-host)
* [Overview](https://googlecloud.qwiklabs.com/focuses/3291#overview)
  + [**What you do**](https://googlecloud.qwiklabs.com/focuses/3291#what-you-do)
  + [**What you learn**](https://googlecloud.qwiklabs.com/focuses/3291#what-you-learn)
* [Launch an Instance](https://googlecloud.qwiklabs.com/focuses/3291#launch-an-instance)
  + [**Step 1: Launch an Instance**](https://googlecloud.qwiklabs.com/focuses/3291#step-1-launch-an-instance)
  + [**Step 2 Verify IP access**](https://googlecloud.qwiklabs.com/focuses/3291#step-2-verify-ip-access)
* [Restrict firewall rule settings for SSH](https://googlecloud.qwiklabs.com/focuses/3291#restrict-firewall-rule-settings-for-ssh)
  + [**Step 1: Find your IP**](https://googlecloud.qwiklabs.com/focuses/3291#step-1-find-your-ip)
  + [Step 2: Edit the default SSH rule](https://googlecloud.qwiklabs.com/focuses/3291#step-2-edit-the-default-ssh-rule)
  + [**Step 3: Test connectivity**](https://googlecloud.qwiklabs.com/focuses/3291#step-3-test-connectivity)
  + [**Step 4: Reset the IP address range**](https://googlecloud.qwiklabs.com/focuses/3291#step-4-reset-the-ip-address-range)
  + [**Step 5: Verify the change**](https://googlecloud.qwiklabs.com/focuses/3291#step-5-verify-the-change)
* [Install a Simple Web Application](https://googlecloud.qwiklabs.com/focuses/3291#install-a-simple-web-application)
  + [**Step 1: SSH to webserver**](https://googlecloud.qwiklabs.com/focuses/3291#step-1-ssh-to-webserver)
  + [**Step 2: Install and configure a web server**](https://googlecloud.qwiklabs.com/focuses/3291#step-2-install-and-configure-a-web-server)
  + [**Step 3: Verify that the web server is working**](https://googlecloud.qwiklabs.com/focuses/3291#step-3-verify-that-the-web-server-is-working)
* [Restrict firewall rule settings for HTTP](https://googlecloud.qwiklabs.com/focuses/3291#restrict-firewall-rule-settings-for-http)
  + [**Step 1: Restrict HTTP access**](https://googlecloud.qwiklabs.com/focuses/3291#step-1-restrict-http-access)
  + [**Step 2: Verify that you still have access to the web server**](https://googlecloud.qwiklabs.com/focuses/3291#step-2-verify-that-you-still-have-access-to-the-web-server)
* [Restrict access to the VM from the Internet](https://googlecloud.qwiklabs.com/focuses/3291#restrict-access-to-the-vm-from-the-internet)
  + [**Step 1: Edit the VM properties**](https://googlecloud.qwiklabs.com/focuses/3291#step-1-edit-the-vm-properties)
  + [**Step 2: Remove the External IP**](https://googlecloud.qwiklabs.com/focuses/3291#step-2-remove-the-external-ip)
  + [**Step 3: Try to access the VM**](https://googlecloud.qwiklabs.com/focuses/3291#step-3-try-to-access-the-vm)
* [Create a Bastion Host](https://googlecloud.qwiklabs.com/focuses/3291#create-a-bastion-host)
  + [**Step 1: Launch another Instance**](https://googlecloud.qwiklabs.com/focuses/3291#step-1-launch-another-instance)
  + [**Step 2: SSH into bastion**](https://googlecloud.qwiklabs.com/focuses/3291#step-2-ssh-into-bastion)
  + [**Step 3: verify HTTP access to webserver**](https://googlecloud.qwiklabs.com/focuses/3291#step-3-verify-http-access-to-webserver)
  + [\_Step 4: verify SSH access to webserver \_](https://googlecloud.qwiklabs.com/focuses/3291#_step-4-verify-ssh-access-to-webserver-_)
* [Review](https://googlecloud.qwiklabs.com/focuses/3291#review)

# BASTION HOST

# Overview

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



During operations, you harden the server by removing its External IP, preventing connections from the Internet. During maintenance, you would start-up a Bastion Host which has an External IP. You can then SSH to the Bastion Host, and from there SSH to the server over Internal IP. You can further restrict access with Firewall Rules.

## ****What you do****

* 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

## ****What you learn****

* How to secure an internal service
* How to maintain systems with a Bastion Host

# Launch an Instance

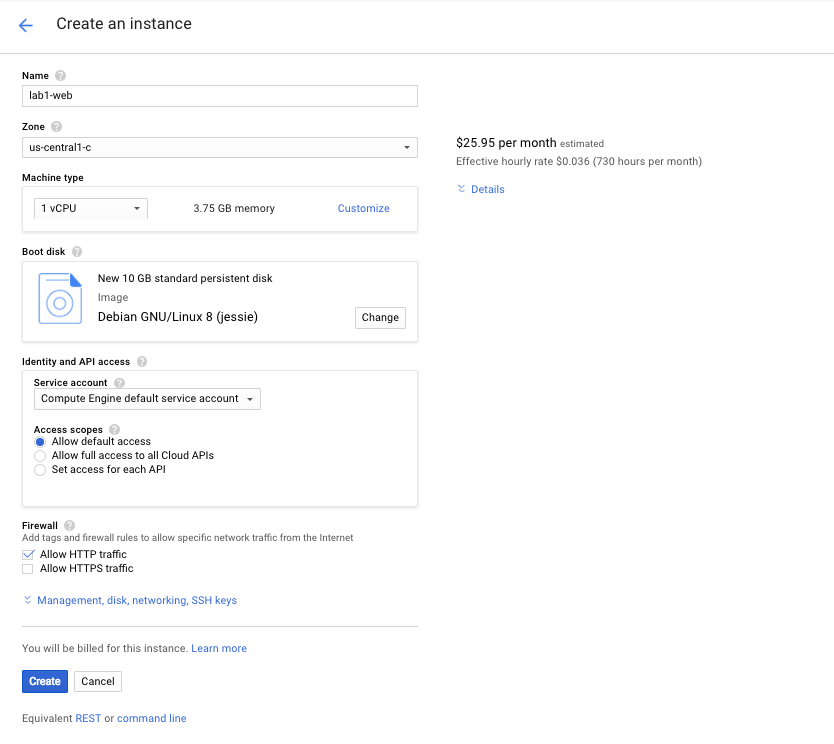
## ****Step 1: Launch an Instance****

Console: **Products and Services > Compute Engine > VM instances**

Click **[Create Instance]**

|  |  |
| --- | --- |
| **Property** | **Value** |
| **Name**: | webserver |
| **Zone:** | us-central1-c |
| **Machine type:** | 1vCPU (n1-standard-1) |
| You shouldn't need to change the following settings, just verify them. | |
| **Boot disk:** | New 10GB, Debian Linux |
| Under Identity and API access:  **Service account:** | don't change  Compute Engine default service account |
| **Firewall:** | **[x]** Allow HTTP traffic |

Example:



## ****Step 2 Verify IP access****

Console: **Products and Services > Compute Engine > VM instances**

Use the SSH link in the line with your VM to launch a terminal and connect.

**Tip:**Setting the Source IP at creation time is best practice.

Enter a few commands to test connectivity. Then exit to close the terminal.

 Copy Code Block

$ ls

$ pwd

$ exit

# Restrict firewall rule settings for SSH

The default setting for an 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 and connect from the console.

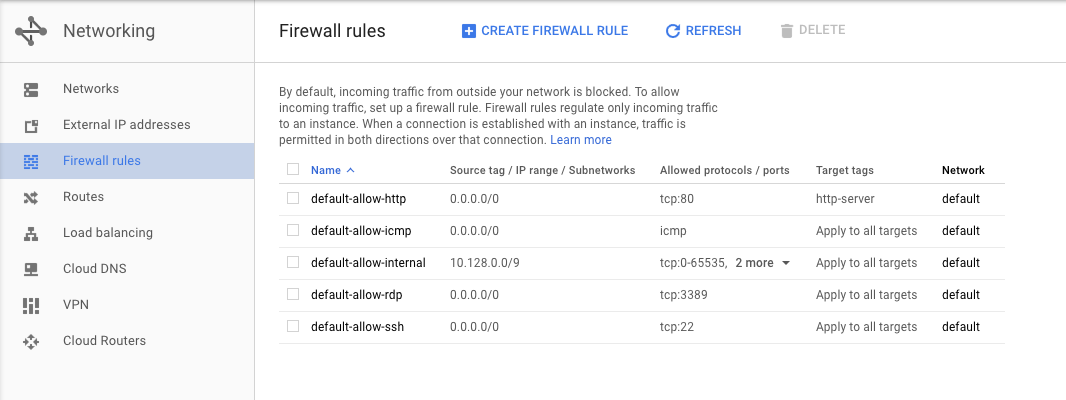
## ****Step 1: Find your IP****

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. Open a browser in a new tab. Go to[www.google.com](http://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 will perform this service.

Copy your IP address. You will be using it to modify the default firewall rule.

Console: **Products and Services > Networking > Firewall rules**

Select **[Firewall rules]**



## Step 2: Edit the default SSH rule

Select the **default-allow-ssh rule** by clicking on it, then click edit. In the drop-down Source filter, change this to **IP ranges**.

Change the existing Source filter from 0.0.0.0/0 rule and to your IP address.

|  |  |
| --- | --- |
| **Property** | **Value** |
| **Description:** | Allow SSH from my IP only |
| **Source Filter**: | IP ranges |
| **Range:** | your IP address |

Click [Save]

## ****Step 3: Test connectivity****

Console: **Products and Services > Compute Engine > VM instances**

Use the SSH link in the line with your VM to launch a terminal and connect.

What happened?

When you 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](https://support.google.com/a/answer/60764). If you want to restrict SSH access to just your IP address, then you need to SSH from a terminal session.

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

## ****Step 4: Reset the IP address range****

|  |  |
| --- | --- |
| **Property** | **Value** |
| **Description:** | Allow SSH from anywhere |
| **Source Filter**: | Allow from any IP (0.0.0.0/0) |

Click **[Save]**

## ****Step 5: Verify the change****

Console: **Products and Services > Compute Engine > VM instances**

Use the SSH link in the line with your VM to launch a terminal and connect.

# Install a Simple Web Application

To install a simple web application on your instance to represent an internal application.

You will then secure it by preventing access from the internet.

## ****Step 1: SSH to webserver****

Console: **Products and Services > Compute Engine > VM instances**

Use the SSH link in the line with your VM to launch a terminal and connect.

## ****Step 2: Install and configure a web server****

Update the package index.

 Copy Code Block

$ sudo apt-get update

Install the apache2 package.

 Copy Code Block

$ sudo apt-get install apache2 -y

Create a new default web page by overwriting the default by typing:

 Copy Code Block

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

## ****Step 3: Verify that the web server is working****

Test that your instance is serving traffic on its external IP.

Console: **Products and Services > Compute Engine > VM instances**

Click the external IP for\_\_ webserver\_\_ under the EXTERNAL IP column.

You should see the "Hello World!" page.

# Restrict firewall rule settings for HTTP

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

## ****Step 1: Restrict HTTP access****

Console: **Products and Services > Networking > Firewall rules**

Select **[Firewall rules]**

Select the **default-allow-http rule** by clicking on it, then click edit. In the drop-down Source filter, change this to **IP ranges**.

Change the existing Source filter from 0.0.0.0/0 rule and to your IP address.

|  |  |
| --- | --- |
| **Property** | **Value** |
| **Description:** | Allow HTTP from my IP only |
| **Source Filter**: | IP ranges |
| **Range:** | your IP address |

Navigate to the firewall rules console and modify the source IP address to your IP. Validate that you can still access the web server.

## ****Step 2: Verify that you still have access to the web server****

Console: **Products and Services > Compute Engine > VM instances**

Click the external IP for webserver under the EXTERNAL IP column.

You should still be able to reach the "Hello World!" page.

# Restrict access to the VM from the Internet

## ****Step 1: Edit the VM properties****

Console: **Products and Services > Compute Engine > VM instances**

Click on [**webserver**]

## ****Step 2: Remove the External IP****

Scroll down to the External IP property and use the pull down menu to change it from **Ephemeral** to **none**.

Click **[Save]**

## ****Step 3: Try to access the VM****

First try HTTP:

Console: **Products and Services > Compute Engine > VM instances**

Click the external IP for\_\_ webserver\_\_ under the EXTERNAL IP column.

Next try SSH:

Console: **Products and Services > Compute Engine > VM instances**

Use the SSH link for \_\_webserver \_\_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.

# Create a Bastion Host

## ****Step 1: Launch another Instance****

Console: **Products and Services > Compute Engine > VM instances**

Click**[Create Instance]>/b>**

|  |  |
| --- | --- |
| **Property** | **Value** |
| **Name**: | bastion |
| **Zone:** | us-central1-c |
| **Machine type:** | 1vCPU (n1-standard-1) |
| You shouldn't need to change the following settings, just verify them. | |
| **Boot disk:** | New 10GB, Debian Linux |
| Under Identity and API access:  **Service account:** | don't change  Compute Engine default service account |
| **Firewall:** | don't change |

Click **[Create]**.

## ****Step 2: SSH into bastion****

Console: **Products and Services > Compute Engine > VM instances**

Use the SSH link for \_\_bastion \_\_to launch a terminal and connect.

## ****Step 3: verify HTTP access to webserver****

Verify that the home page on **webserver** is reachable.

**Copy Code Block**

$ curl webserver

Even though the **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.

## \_Step 4: verify SSH access to webserver \_

SSH into **webserver** from **bastion** by typing the following.

**Copy Code Block**

$ ssh -a webserver

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.

# REVIEW

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

You created a bastion host named **bastion** to gain access to the webserver VM over it's 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.

©Google, Inc. or its affiliates. All rights reserved. Do not distribute.

|  |
| --- |
| **Levels:**[**introductory**](https://googlecloud.qwiklabs.com/tags/introductory/level)  **Lab Description:**In this lab you create a bastion host and learn to restrict access to a server and harden access through firewall rules.  **Lab Creator:** Enis Konuk  **Date Created:** April 10, 2017 19:11 |