

**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

# SECURE ACCESS WITH A BASTION HOST (Set up a bastion host in a public subnet to securely access instances in a private subnet)

Name: MADHUMETHRA A P Department: IT



**Introduction**

A ‘bastion host’ is a special-purpose server used to securely access resources in a private network from an external network, like the internet. It acts as a jump server or gateway for managing instances that do not have direct internet access.

**Overview**

Secure access: Prevents exposing all private servers to the internet.

Controlled entry point: Only the bastion host is accessible from the internet.

Better security: Reduces the attack surface by limiting SSH access to one server.

Logging & Monitoring: You can track who accesses internal instances via the bastion.

**Objective**

Deploy a Web Application: Successfully deploy a Python Flask application on a cloud VM.

Configure Firewall Rules: Configure the firewall to allow HTTP traffic on port 80.

Ensure Accessibility: Ensure that the web application is accessible to users.

**Importance**

Reduced Attack Surface - Instead of exposing multiple instances to the internet, only the bastion host is accessible.

Reduces the chances of brute-force attacks, malware infections, or unauthorized access.

Enhances Network Segmentation - Separates public-facing components (bastion) from private infrastructure.

**Step-by-Step Overview**

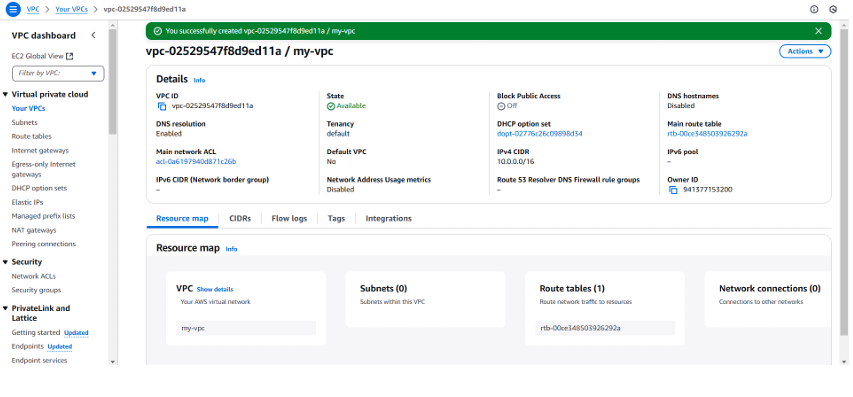
Step1:

CREATE VPC

Login into your AWS console and navigate to VPC dashboard and create your own VPC.

Specify the name tag, IPv4 CIDR block (10.0.0.0/16), IPv6 CIDR (optional)

Then click create.



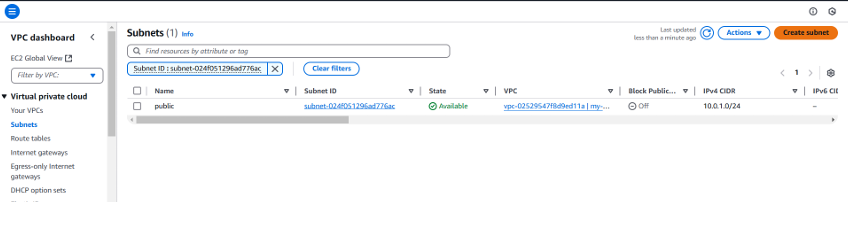
Step 2:

CREATE A PUBLIC SUBNETS

Click on create subnets and select the VPC you have just created.

Create a public subnet with CIDR block of 10.0.1.0/24.

Enable the ‘auto-assign’ public IP.



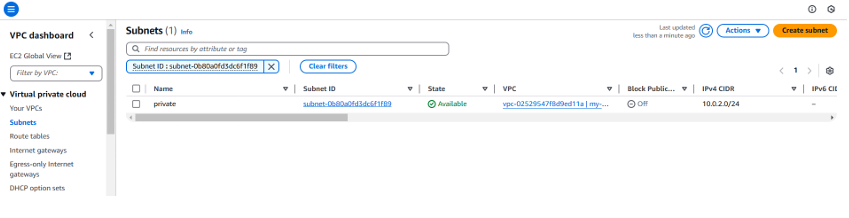
Step 3:

CREATE A PRIVATE SUBNET

Click on create subnets and select the VPC you have just created.

Create a private subnet with CIDR block of 10.0.2.0/24.

Don’t enable the ‘auto-assign’ public IP.

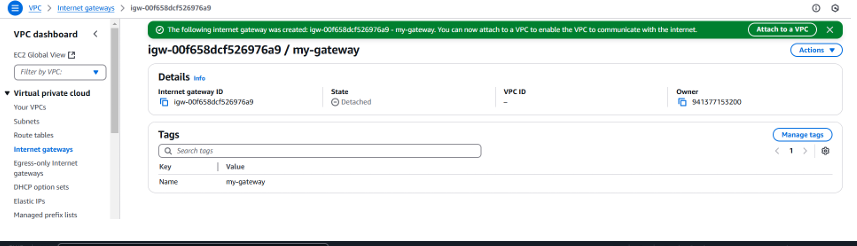


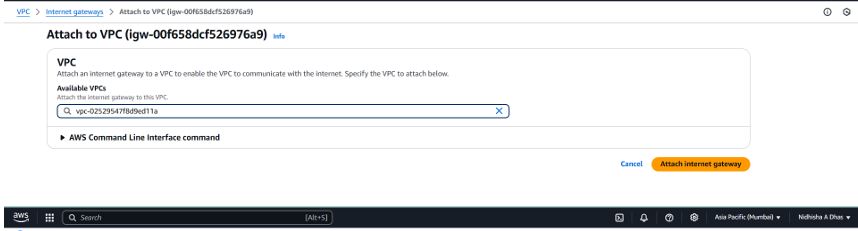
Step 4:

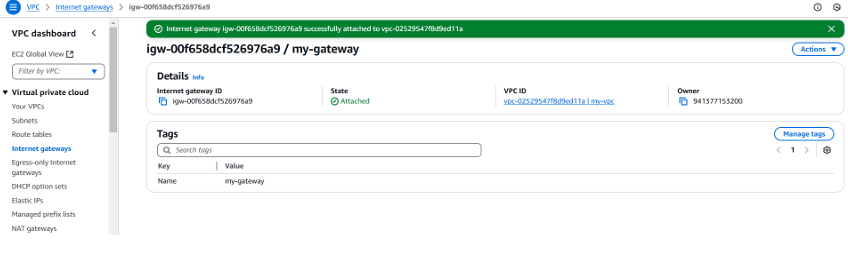
CREATE THE INTERNET GATEWAY

Go to the Internet Gateways and click on Internet gateway.

Name it and attack it to the VPC that we have created.



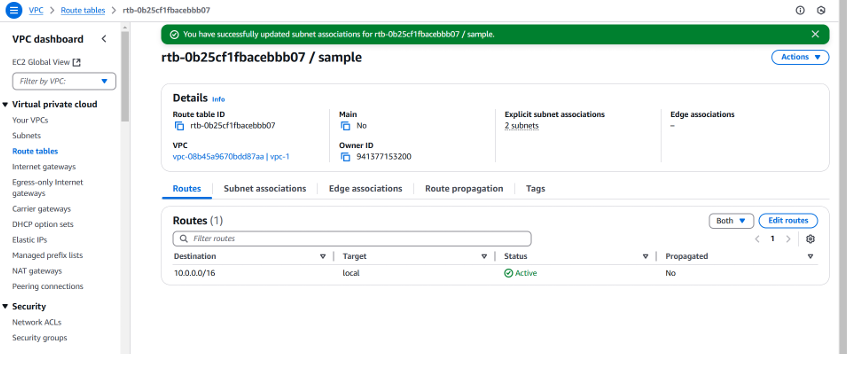




Step 5:

CREATE PUBLIC ROUTE TABLE

Go to route table- click on ‘create route table’. Specify the name and associate it with the public subnet. Add destination and target to the route table. Click create.



Step 6:

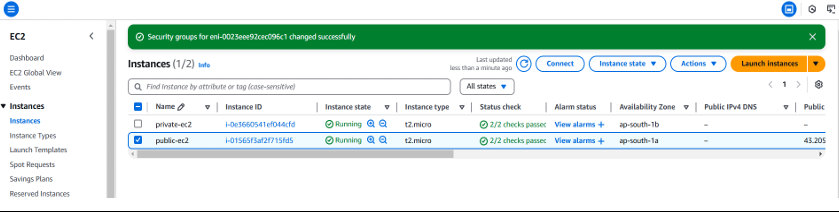
LAUNCH BASTION HOST

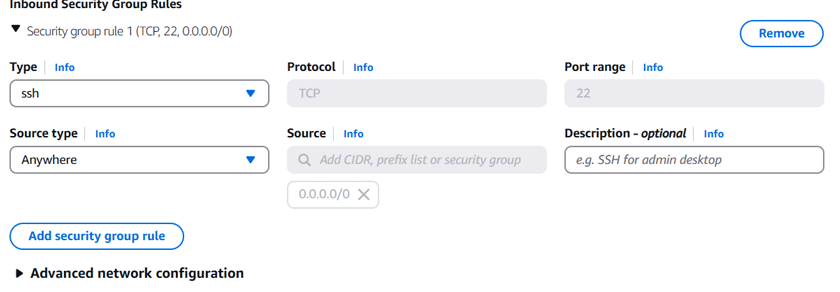
Go to the EC2 dashboard and launch two EC2 instances by specifying the instance name, AMI and Instance Type.

Under the ‘network settings’, select your VPC and select the public subnet and the private subnet respectively for both the instances.

Enable the auto assign Public IP for the public EC2 and disable it for the private EC2 instance. Also, create the Security groups for the instances.

Now, click on launch instance.



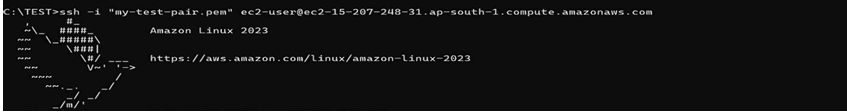


Step 7:

CONNECT THE PRIVATE INSTANCE TO THE BASTION HOST

Open the PowerShell and give the following command to change the directory.

To connect the private instance copy the ssh command from the private instance and paste it in the PowerShell.



**Output**

By completing this PoC, you will be able to: • Create a Bastion host that enhances the security to access resources in a private network from an external network, like the internet.