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: Harshana Perianayaki B Department : IT

INTRODUCTION

In modern cloud environments, securing access to virtual machines (VMs) is critical to prevent unauthorized access and potential security breaches. Directly exposing VMs to the internet via public IP addresses increases vulnerability to attacks. A **Bastion Host** provides a secure and controlled method for accessing private instances without exposing them to external threats. This document outlines the process of setting up a **Bastion Host in Azure** to securely access instances within a **private subnet**.

OBJECTIVES

The primary objectives of setting up a Bastion Host in Azure include:

- **Enhancing Security**: Prevent direct exposure of VMs to the internet.
- **Enabling Secure Access**: Allow RDP/SSH connections without requiring a VPN.
- **Reducing Attack Surface**: Eliminate the need for public IP addresses on private VMs.
- **Simplifying Management**: Provide browser-based access via Azure Portal.
- **Improving Compliance**: Adhere to security best practices and regulatory requirements.

OVERVIEW

Azure Bastion is a fully managed service that enables secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Azure Virtual Machines without exposing them to the public internet. It eliminates the need for jump servers or VPNs while providing enhanced security by restricting direct access. The Bastion Host is deployed in a **public subnet** and acts as an intermediary, allowing administrators to securely connect to instances in a **private subnet** using Azure Portal.

IMPORTANCE

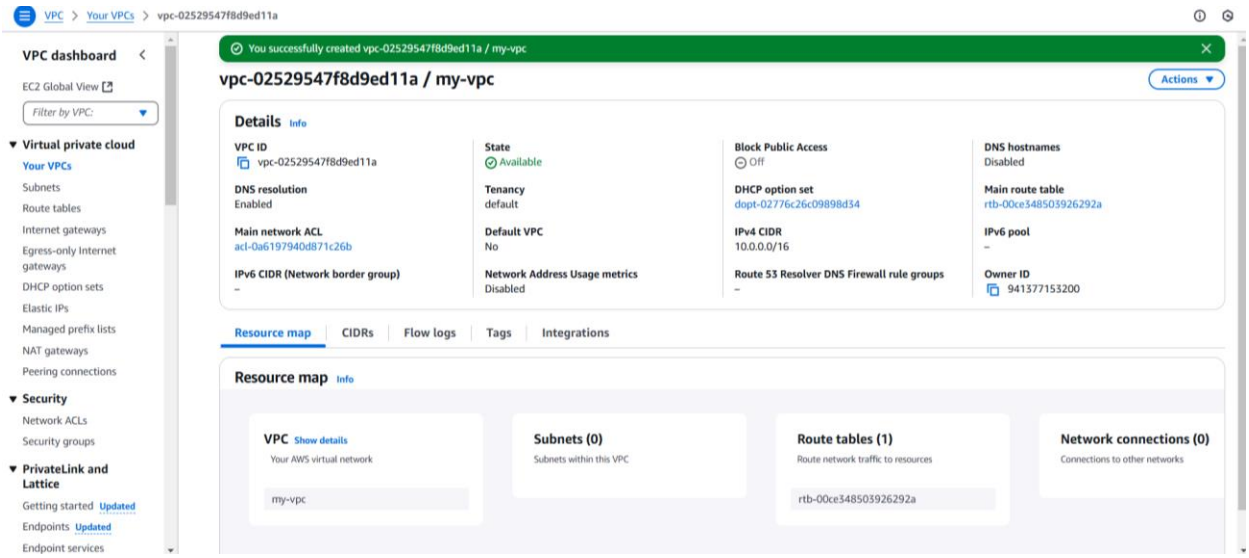
- **Mitigates Security Risks**: By eliminating public IP addresses, Bastion Hosts significantly reduce the risk of brute-force attacks and unauthorized access.
- **Ensures Network Isolation**: Private instances remain inaccessible from external sources, improving security posture.
- **Simplifies Access Management**: Administrators can access VMs directly from the Azure Portal without additional software or VPN configurations.
- **Supports Scalability**: The managed nature of Azure Bastion ensures that organizations can scale access securely without managing additional infrastructure.
- **Enhances Compliance**: Organizations can meet security and regulatory requirements by implementing **Zero Trust Network Access (ZTNA)** principles.

By implementing Azure Bastion, organizations can **strengthen security, enhance access control, and streamline operations** while maintaining a robust cloud infrastructure.

STEP-BY-STEP OVERVIEW

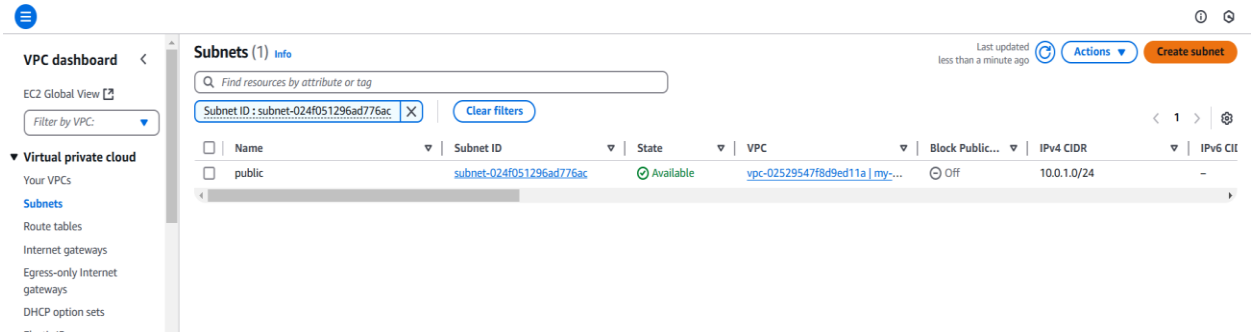
Step 1: CREATE VPC

- 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.



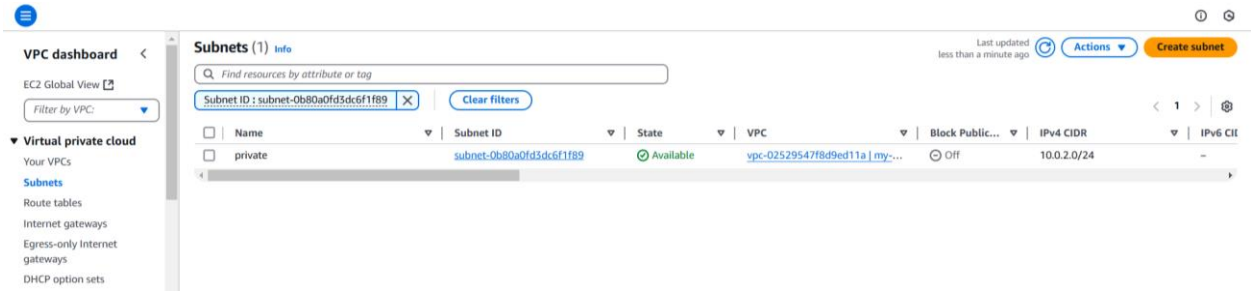
Step 2: CREATE A PUBLIC SUBNETS

- 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.



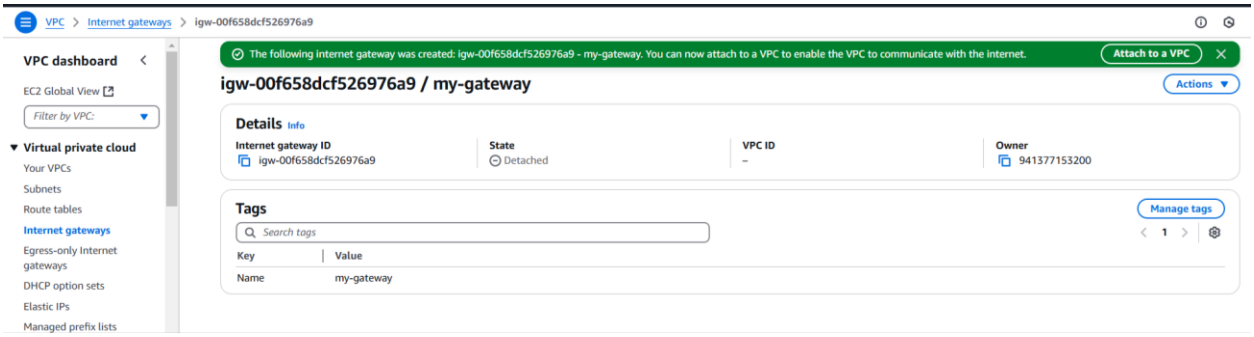
Step 3: CREATE A PRIVATE SUBNET

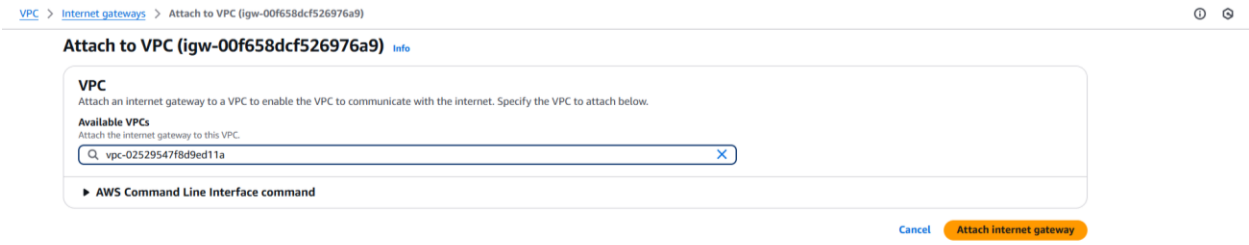
- ☐ Click on create subnets and select the VPC you have just created.
- ☐ Create a private subnet with CIDR block of 10.0.2.0/24.
- ☐ Don't enable the 'auto-assign' public IP.

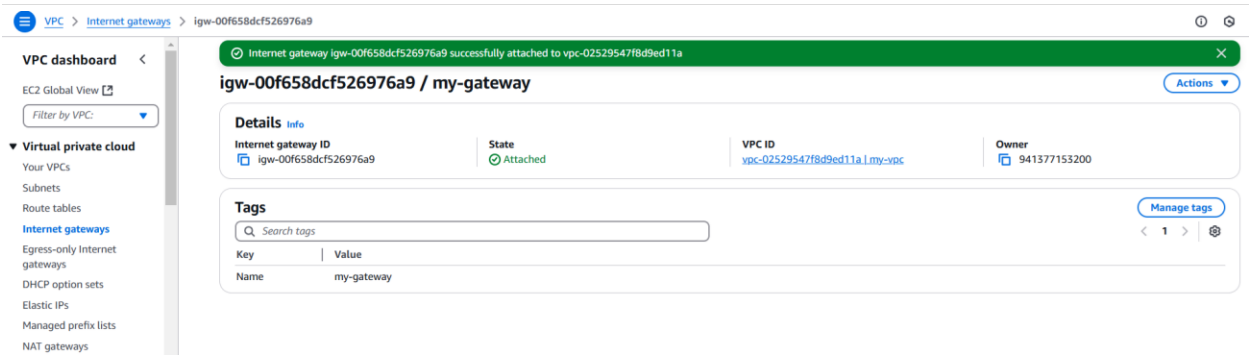


Step 4: CREATE THE INTERNET GATEWAY

- ☐ Go to the Internet Gateways and click on Internet gateway.
- ☐ Name it and attack it to the VPC that we have created.

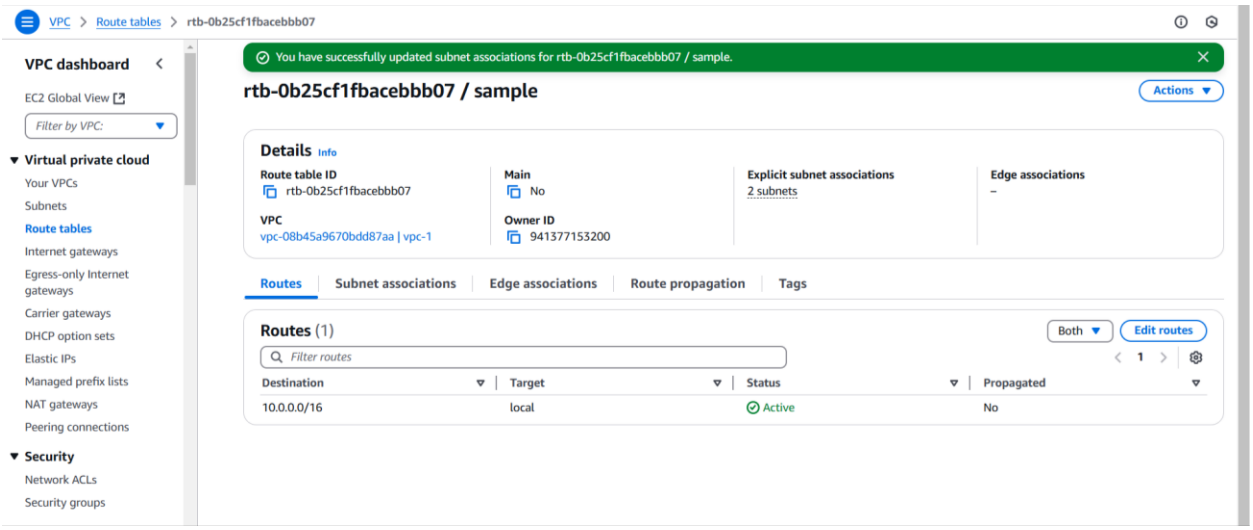






Step 5: CREATE PUBLIC ROUTE TABLE

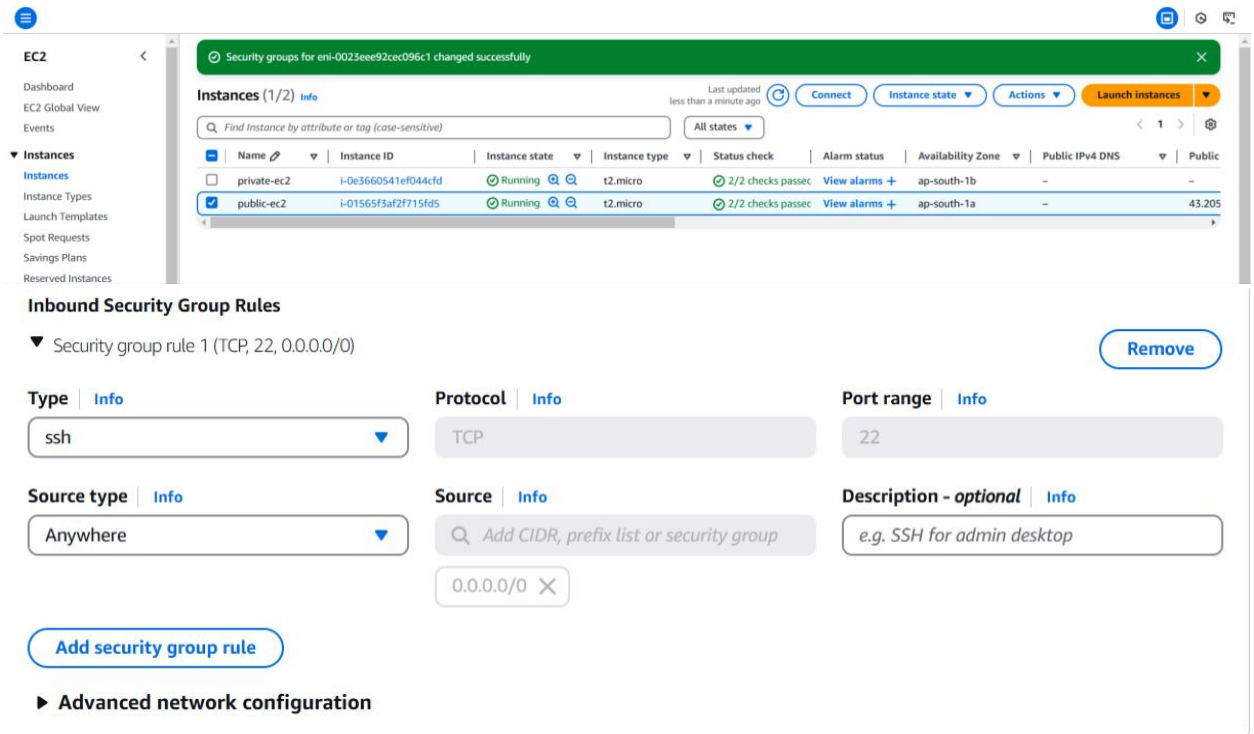
- ☐ Go to route table- click on 'create route table'.
- ☐ Specify the name and associate it with the public subnet.
- ☐ Add destination and target to the route table.
- ☐ Click create.



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.

OUTCOME

After successfully deploying an Azure Bastion Host, users will:

- Have a **secure** and **seamless** way to access private VMs.
- Reduce **security risks** associated with public IP addresses.
- Improve network architecture by isolating workloads from the internet.
- Minimize the administrative overhead of managing jump servers or VPNs.
- Strengthen compliance with security standards and industry best practices