AWS Assignment 4
VPC: BASTION HOST

Overview

The DevOps Team created an Amazon Linux 2023(Linux/Unix) EC2 instance with resources as requested by the Front-End Team for their builds and workflows, but we want to set it up in a private, secure, and isolated area in the cloud where they can run their applications and store their data e.g A THREE TIER ARCHITECTURE(Front End, Backend and Database) servers. This is where a VPC comes into play.

A VPC is a virtual network that you create in the cloud. It allows you to have your own private section of the internet, just like having your own network within a larger network. Within this VPC, you can create and manage various resources, such as servers, databases, and storage.

Also, to add a stronger security because of hackers, we need an extra layer of security by using a special server with set rules to achieve that. That's where a BASTION HOST comes into play.

A bastion host forms a bridge between your device and the network you want to connect to. Only authorized users can access the other computers on this private network using this bridge. This prevents unauthorized access to your business network, blocking hackers from accessing your resources and sensitive data.

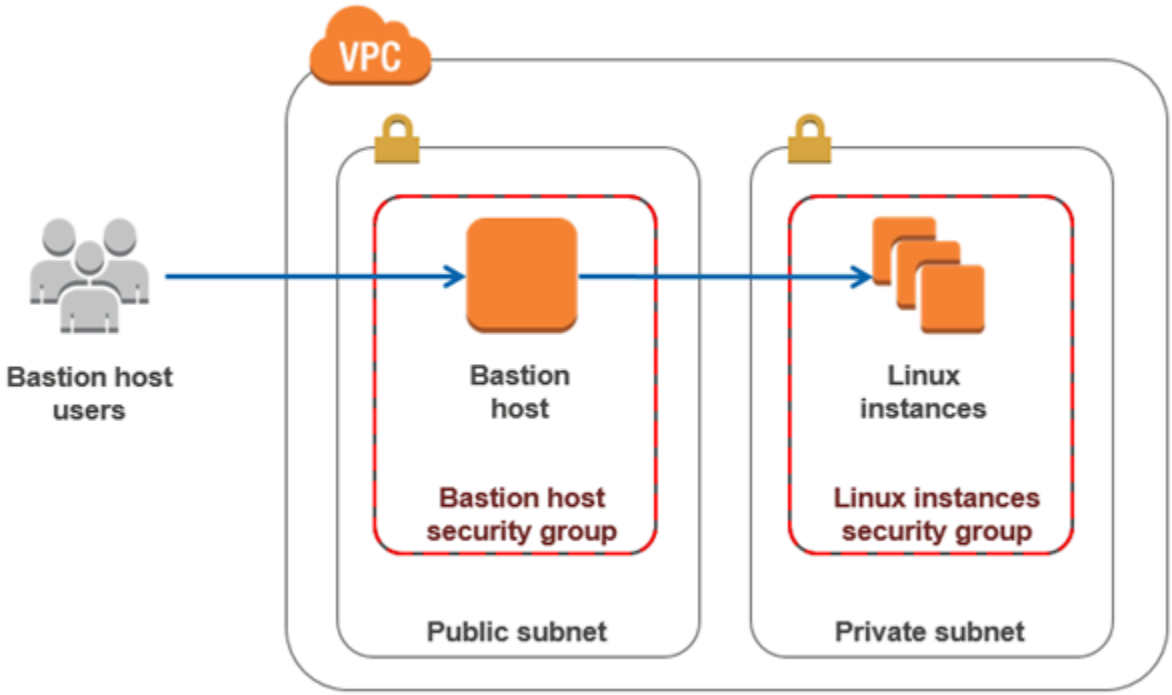
The private servers where our applications are, should not be reached by any means at all. They should only be reached from the Bastion host through SSH. This security measure makes sure that if a hacker or an unauthorized user gains access to the architecture by any means, he has to compromise the Bastion Host first before getting to the Prod Servers.

Resources:

- VPC - Set up a VPC (VPC only) in us-east-1 region
- The CIDR of the VPC should be /16 IP address range but decide on the IP address of the VPC
- Subnets - Set up 1 private subnet (us-east-1c) and 1 public subnet (us-east-1d) manually. You can decide the IP addresses of the Subnets
- Availability Zones: us-east-1c and us-east-1d
- Route tables: Associate the RT created to the right subnets
- Security Group(Firewall) for Prod and Bastion
- Internet Gateway(IGW) and attach it to your VPC
- AMI - Ubuntu(Linux/Unix) - For Bastion
- AMI - Amazon Linux 2023(Linux/Unix) - For Prod Server
- Instance Type: t3.micro for both
- Key pair: RSA .pem
- EBS - 2 Volumes of 8GiB gp3 - volume type: gp3…The second volume should be encrypted for both PROD and BASTION
- CIDR Block Calculator: https://mxtoolbox.com/subnetcalculator.aspx

The Front End Engineers who have access to AWS to spin up EC2 instances for their jobs, just use default VPC and Security Groups but we have fixed that problem already, we the DevOps Team are to ADD A LAYER OF EXTRA SECURITY to this setup by creating a BASTION HOST, thereby making the PROD SERVER only accessible through the Bastion.

Proposed Infrastructure Design for POC(Proof of Concept)



Proposed Solution for POC(Proof of Concept)

1. To solve this problem, we have to Create a VPC
2. Check for VPC preview to guide you on how it is been routed(RESOURCE MAP)
3. Number of AZ - 2
4. Public Subnets - 1
5. Private Subnets - 1
6. VPC endpoint - s3 Gateway
7. Launch the instance and configure it with the VPC
8. SSH into the Private Server if it works, and if it doesn't, try to SSH into the Bastion Host server first before SSHing into the Private Server
9. Allow only SSH in the security group of the Prod Server so that it only allows the Security Group of the Bastion Host to be able to access it.
10. **NOTE:** Try to UPDATE THE PROD SERVER and see if it works. **IF IT DOESN'T, FIX IT!!!**