AWS Assignment 3
VPC: Security Groups and Network Access Control Lists

Overview

The DevOps Team created an Ubuntu 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.

Just like a physical network, a VPC has its own set of rules and configurations. You can define the IP address range for your VPC and create smaller subnetworks within it called subnets. These subnets help you organize your resources and control how they communicate with each other.

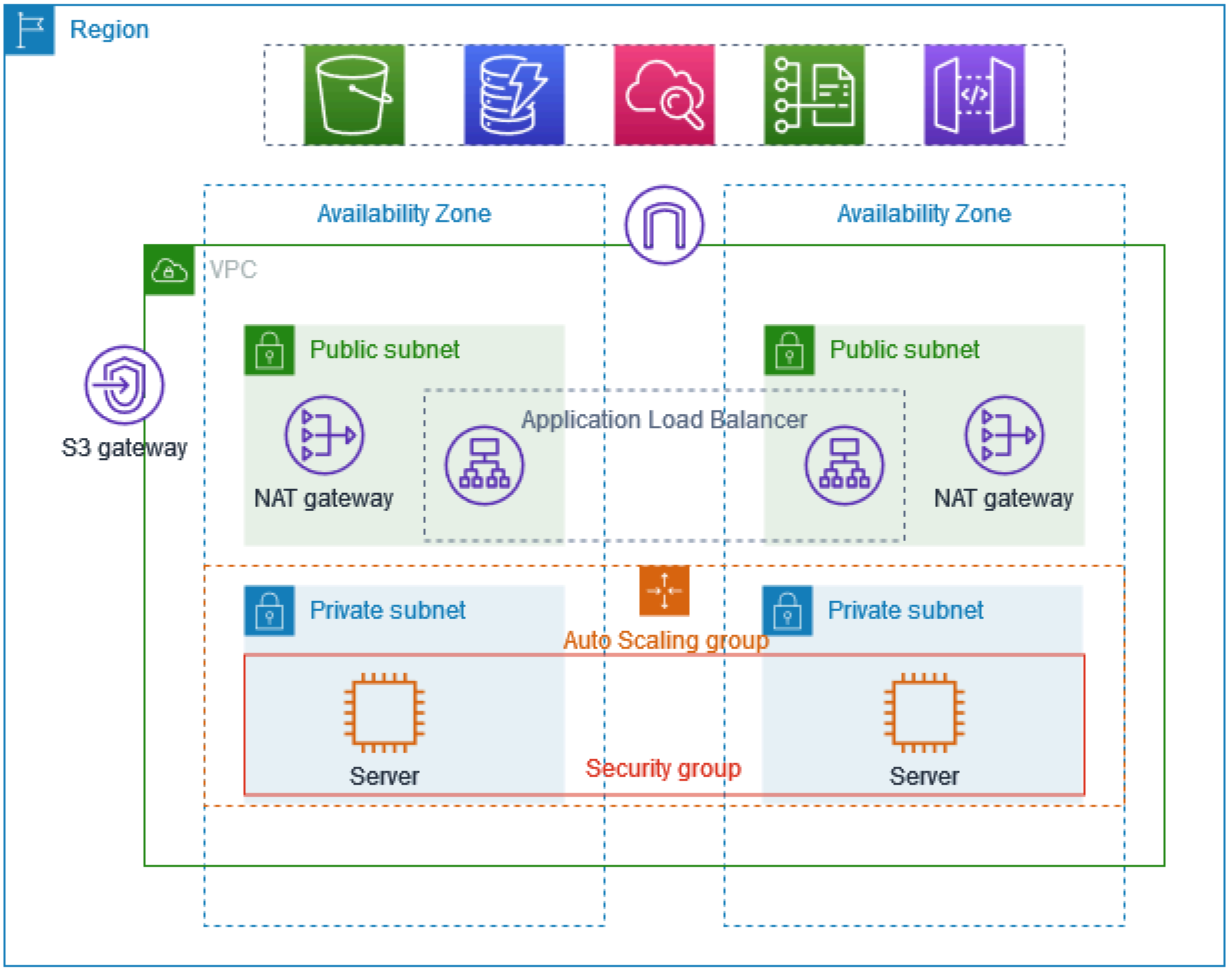
To connect your VPC to the internet or other networks, you can set up gateways or routers. These act as entry and exit points for traffic going in and out of your VPC. You can control the flow of traffic and set up security measures to protect your resources from unauthorized access.

With a VPC, you have control over your network environment. You can define access rules, set up firewalls, and configure security groups to regulate who can access your resources and how they can communicate.

Resources:

- VPC - Set up a VPC (VPC and others)
- The CIDR of the VPC should be /16 IP address range but decide on the IP address of the VPC
- Subnets - 2 private subnets and 2 public subnets, though for this task we'll be using a public subnet to test
- You can decide the IP addresses of the Subnets
- Availability Zones: us-east-1a and us-east-1b
- Route tables
- Security Group(Firewall)
- NACL
- Internet Gateway(IGW)
- AMI - Ubuntu(Linux/Unix)
- Instance Type: t2.micro
- Key pair: RSA .pem
- EBS - 2 Volumes of 10GiB gp3 - volume type: gp3
- 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, Security Groups and NACL and thereby ALLOWING ALL INBOUND TRAFFIC into the machines, so we the DevOps Team are to correct this by setting up Security Group inbound and outbound rules at the instance level, also create NACL inbound and outbound rules which is the most important of all, so that once they use the VPC that we have specified for them, no matter the configuration at the instance level, our NACL is going to handle the security of the instances.

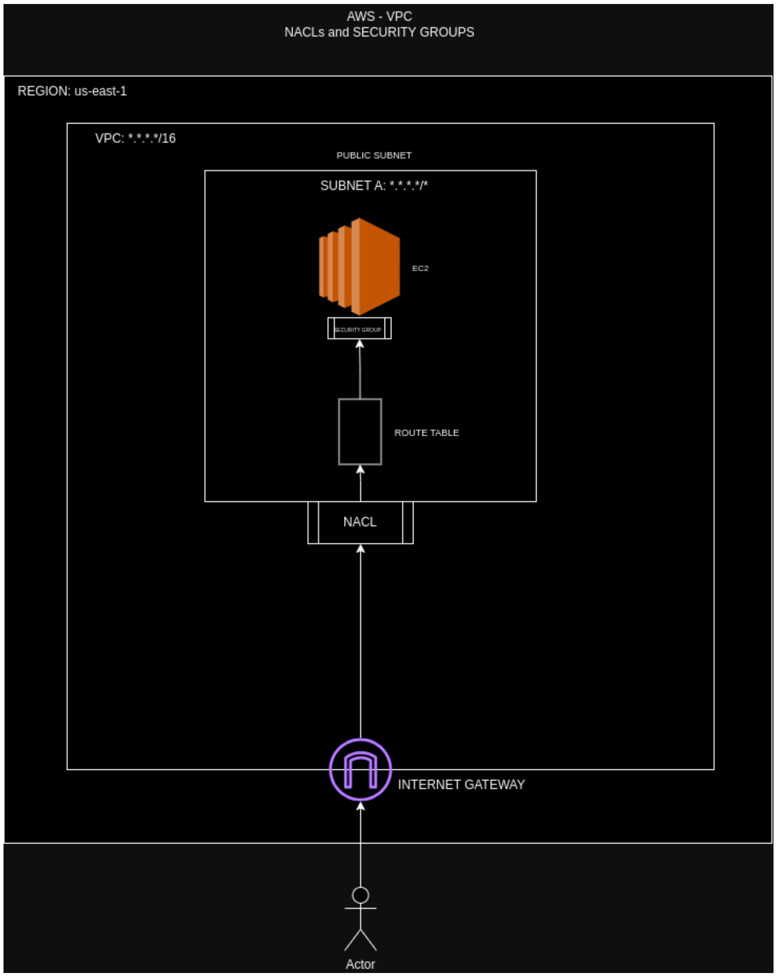


Proposed Solution for POC(Proof of Concept)

1. To solve this problem, we have to Create a VPC and define the inbound and outbound rules in the NACL so that when they create their instances they will use the VPC and it will automatically pick up the NACL attached to the VPC no matter their SECURITY GROUP rules
2. Check for VPC preview to guide you on how it is been routed
3. Number of AZ - 2
4. Public Subnets - 1

5. NAT Gateways - None
6. VPC endpoint - s3 Gateway
7. Launch the instance and configure it with the VPC
8. SSH and install an application e.g python application
9. Run a simple http server or any other application: **$ python3 -m http.server 9674**
10. Allow only **port 7475** and block any traffic coming from **port 9674** in the NACL inbound rule
11. Allow traffic from **port 9674** in Security Group and see if you can reach it
12. Tweak the rules in NACL and SG by denying in NACL and allowing in SG, allowing in NACL and denying in SG and try to reach the application on your browser to see results
13. Therefore you are using NACL for automating rules instead of doing it in the Security Groups at instance level. This saves a lot of stress going into all the machines individually to define rules
14. **NOTE:** NACL Rule Number - the lowest number takes effect before the higher number is accessed. So if you set a DENY RULE with Rule Number 20 and you set an ALLOW RULE with Rule Number 10, NACL obeys the lesser number, so it will allow traffic to be routed to that port or IP. You can also BLOCK AN IP, not just ports.

Proposed Design


AWS - VPC
NACLs and SECURITY GROUPS
REGION: us-east-1
VPC: *.*.*.*/16
PUBLIC SUBNET
SUBNET A: *.*.*.*/*
EC2
SECURITY GROUP
ROUTE TABLE
NACL
INTERNET GATEWAY
Actor