**Monitoring and Securing AWS VPC Traffic Using Flow Logs and CloudWatch**

**Project Overview**

This mini project demonstrates how to:

- Create a custom AWS VPC with public and private subnets.

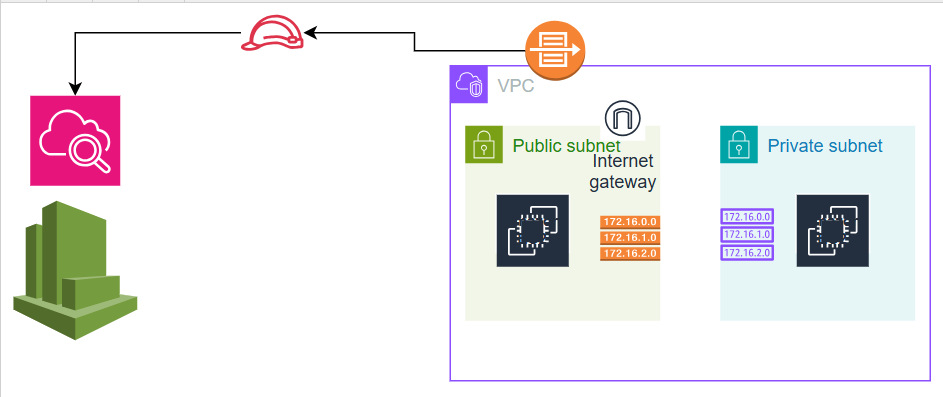
- Deploy an EC2 instance in the public subnet with internet access.

- Enable VPC Flow Logs and direct the logs to Amazon CloudWatch Logs.

- Use IAM roles to securely deliver flow logs.

- Monitor traffic in real time and validate secure logging.

Architecture Diagram



**AWS Services Used:**

- Amazon VPC (Public & Private Subnets, Route Tables)

- Amazon EC2

- Internet Gateway

- VPC Flow Logs

- IAM (Role + Policy for Flow Log delivery)

- Amazon CloudWatch (Log Groups & Logs)

**Steps Performed**

1. VPC Setup

- Created a custom VPC with one public and one private subnet.

- Attached an Internet Gateway to the VPC.

- Configured routing for internet access in the public subnet.

2. EC2 Instance Launch

- Deployed an EC2 instance in the public subnet.

- Associated a public IP to enable internet access.

3. CloudWatch Setup

- Created a Log Group in Amazon CloudWatch.

- Ensured CloudWatch Logs permissions via IAM role.

4. VPC Flow Logs

- Enabled VPC Flow Logs for all traffic.

- Mapped flow logs to the CloudWatch Log Group.

- Verified log data is delivered securely and in near real-time.

5. IAM Role

- Created an IAM Role with the following policy:

JSON TEMPLATE:

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"logs:CreateLogGroup",

"logs:CreateLogStream",

"logs:PutLogEvents",

"logs:DescribeLogGroup",

"logs:DescribeLogStreams"

],

"Resource": "\*"

}

]

}

**Outcome**

This project simulates a real-world cloud monitoring scenario where VPC traffic visibility is crucial. By enabling VPC Flow Logs with CloudWatch, secure data transfer and operational insights were achieved, aligning with AWS best practices for network observability and security.