Project 2: Configure VPC Flow Logs and Store Logs in S3 Using IAM Role

Intern: Shyam Champakbhai Chotaliya **Company:** Fortune Cloud Technologies **Date:** [14-07-2025]

Project Overview

This project involved setting up a durable and secure logging system for network traffic within an AWS Virtual Private Cloud (VPC). The primary objective was to capture all IP traffic (accepted and rejected) using VPC Flow Logs and deliver these logs to a centralized, private Amazon S3 bucket for long-term storage, analysis, and security auditing. Access control was implemented using a dedicated IAM Role to ensure the process followed security best practices.

Step-by-Step Setup Instructions

The following high-level steps were performed to complete the project:

1. **S3 Bucket Creation:** A new, private S3 bucket (`fortunetech-vpc-flow-logs-...`) was created in the same region as the VPC to serve as the log destination. All public access was blocked at the bucket level.
2. **IAM Policy and Role Creation:**
    - A custom **IAM Permissions Policy** was created to grant `s3:PutObject` and `s3:GetBucketAcl` permissions, scoped specifically to the log bucket's ARN.
    - A new **IAM Role** was created with a **Trust Relationship** allowing the `vpc-flow-logs.amazonaws.com` service to assume it. The permissions policy was attached to this role.
3. **VPC Flow Log Activation:** VPC Flow Logs were enabled on the target VPC (`internship-vpc`). It was configured to send logs to the S3 bucket using the newly created IAM role.
4. **Testing and Verification:** An EC2 instance within the VPC was used to generate network traffic (`ping`, `curl`). After waiting for the aggregation interval, the S3 bucket was checked to confirm that gzipped log files were successfully delivered and contained the expected traffic data.

Importance of Each Configuration

- **IAM Role (vs. Access Keys):** Using an IAM Role is significantly more secure than using IAM user access keys. The role provides temporary, automatically-rotated credentials to the AWS service, eliminating the risk of long-lived keys being exposed.
- **S3 as a Destination:** S3 is an ideal destination for logs because it is highly durable, scalable, and cost-effective. It integrates seamlessly with other analysis tools like Amazon Athena, allowing for powerful querying of log data directly from S3.
- **Structured Log Path:** The default S3 path (`/AWSLogs/[account-id]/...`) automatically organizes logs by date, which is crucial for efficient log management and simplifies querying based on time ranges.

Traffic Type Selected and Reasoning

I chose to capture **All** traffic (both `ACCEPT` and `REJECT`).

Reasoning: Capturing only `ACCEPT` traffic shows you what's working, but capturing `REJECT` traffic is critical for security. It allows you to see malicious scanning attempts, misconfigured security groups, or network ACLs that are blocking legitimate traffic. For a comprehensive security and operational view, logging "All" traffic is the best practice.

Included Deliverables

- **README.md:** This project report.
- **/iam-policies/:** Folder containing the `permissions-policy.json` and `trust-relationship.json` files.
- **sample-log-explanation.txt:** A sample VPC Flow Log line with a detailed field-by-field explanation.
- **/screenshots/:** A folder containing supporting screenshots of the AWS Console configuration.

> ***Note:*** *This document covers only Project 2 out of the 6 assigned internship projects. The remaining projects are in progress and will be submitted separately.*