AWS VPC Automation — Scenario Document

Project Overview

This project focused on automating the deployment of AWS networking infrastructure through Terraform (Infrastructure as Code). The aim was to create a scalable, secure, and reusable Virtual Private Cloud (VPC) with essential networking components, aligning with cloud best practices and compliance requirements.

Scenario

Organizations often face delays and inconsistencies in setting up secure AWS environments. Manual provisioning of networking resources (VPC, subnets, route tables, gateways) increases the risk of misconfigurations, weak security boundaries, and scalability issues. To address these challenges, this project automated the entire VPC setup process, enabling reliable and repeatable deployments across environments.

Solution Proposed

- Designed and implemented Terraform configurations to provision AWS VPC resources automatically.
- Created parameterized variables for CIDR blocks, subnets, and routing to support different use cases.
- Implemented Internet Gateways, Route Tables, and Subnets for both public and private access.
- Configured outputs to expose key resource identifiers (VPC ID, subnet IDs, route tables) for integration with other modules.
- Proposed extensions for network segmentation, firewalls/security groups, and logging/monitoring integration.

Services & Tools Used

- AWS VPC — Core networking backbone.
- AWS Subnets (Public/Private) — Segmentation for workloads.
- AWS Internet Gateway (IGW) — Public connectivity.
- AWS Route Tables — Routing control for traffic flow.
- Terraform — Infrastructure as Code for automation.
- AWS CLI — Deployment & credentials management.
- Security Add-ons (planned): AWS KMS (encryption), Security Groups, NACLs, CloudWatch for monitoring.

Frameworks Applied

- Infrastructure as Code (IaC) principles — for scalability, reproducibility, and compliance.
- AWS Well-Architected Framework — networking and security best practices.
- Network Segmentation Model — isolation of public/private workloads.

Skills Demonstrated

- Cloud Infrastructure Design (AWS VPC, subnets, routing).
- Infrastructure as Code (Terraform).
- Networking (CIDR, DNS, Routing, IGW, VPN, Segmentation).
- Security Controls (NACLs, Security Groups, TLS/SSL, KMS).
- DevOps Practices (automation, reusability, modular code).
- Documentation & Reporting for technical and non-technical stakeholders.