AWS PORTFOLIO

This portfolio demonstrates my ability to design secure, scalable, and well-architected AWS environments following AWS best practices, security principles, and the AWS Well-Architected Framework.

Candidate: Shedrach Elutilo

Secure AWS VPC Architecture – Technical Design Document

1. Document Purpose

This document provides the technical explanation of a secure AWS VPC architecture designed using AWS best practices. It is intended to accompany an architecture diagram as part of my portfolio, demonstrating real-world design thinking across security, networking, scalability, availability, and operations.

---

2. Architecture Overview

The architecture is built around a multi-AZ Virtual Private Cloud (VPC) that hosts a scalable application tier behind a secure ingress layer. The design enforces:

- No direct internet access to compute or databases
- Strong perimeter security using AWS-managed services
- Private connectivity to AWS services using VPC Endpoints
- Centralized logging, monitoring, and threat detection
- Automated scaling and high availability

Key design goals:

- Security first (zero trust principles)
- High availability across multiple Availability Zones
- Operational excellence with observability and alerting
- Cost awareness without sacrificing security

---

3. Edge and Ingress Security Layer

3.1 Internet (Untrusted Network)

The public internet is treated as an untrusted zone. No AWS resources are directly exposed except through managed ingress services.

3.2 AWS Web Application Firewall (WAF)

AWS WAF is attached to the Application Load Balancer to provide Layer 7 application-level protection.

Characteristics and Benfits:

- AWS Managed Rules (OWASP Top 10)
- Rate limiting to mitigate HTTP floods
- IP reputation and geo-blocking
- Bot and scanner mitigation
- Prevents malicious requests before they reach the application
- Reduces risk of injection, XSS, and abuse attacks

---

4. Load Balancing and Traffic Management

4.1 Application Load Balancer (ALB)

The Application Load Balancer serves as the single public entry point into the VPC.

Characteristics and Benefits:

- Terminates TLS using ACM-managed certificates
- Forwards traffic only to approved targets in private subnets
- HTTPS-only listeners
- Security Groups restricting inbound traffic to WAF-approved sources
- Health checks and intelligent routing
- Seamless integration with Auto Scaling Groups

---

5. Network Segmentation and Isolation

5.1 Virtual Private Cloud (VPC)

The VPC provides logical network isolation for all application resources.

Characteristics and Benefits:

- Spans multiple Availability Zones
- No default internet exposure for workloads
- Strong isolation from other AWS tenants
- Full control over routing and traffic flow

5.2 Subnet Design

Public Subnets

- Host only internet-facing resources (NAT Gateway)

- No application workloads
- Limits public exposure strictly to required components.

Private Application Subnets

- Host EC2 instances in Auto Scaling Groups
- No public IP addresses
- Prevents direct internet access to compute layer.

Aurora Cluster Subnet

- Fully isolated subnet for Aurora RDS
- No route to internet gateway or NAT
- Strongest isolation for sensitive data.

---

6. Compute Layer Security

6.1 EC2 Auto Scaling Group

The application tier runs on EC2 instances managed by an Auto Scaling Group.

Characteristics and Benefits:

- IAM Instance Roles (no static credentials)
- Security Groups allowing traffic only from ALB
- No SSH access
- Automatic scaling based on demand
- Self-healing through instance replacement

6.2 AWS Systems Manager – Session Manager

Session Manager replaces traditional bastion hosts and SSH access.

Security Benefits:

- No inbound ports required
- IAM-based access control
- Fully encrypted and logged sessions
- Simplified access management
- Reduced attack surface

---

7. Database Layer Security

7.1 Amazon Aurora

Amazon Aurora is used as the managed relational database service, deployed in private database subnets across multiple Availability Zones. Aurora provides high availability, scalability, and enhanced security compared to traditional RDS engines.

Characteristics and Benefits:

- Aurora instances are not publicly accessible and reside only in isolated DB subnets
- Encryption at Rest: All data is encrypted using AWS KMS-managed keys
- Encryption in Transit: TLS is enforced for all client connections
- Security Groups restrict inbound access exclusively to the application tier
- Fast, managed failover without application-level intervention
- Automated backups with point-in-time recovery
- No manual patching of underlying database infrastructure
- Read replicas for horizontal read scaling

---

8. Egress and Private Service Access

8.1 NAT Gateway

The NAT Gateway allows controlled outbound internet access for private subnets.

Characteristics and Benefits:

- No inbound connections allowed
- Centralized egress point
- Enables updates and external API calls without exposing workloads

---

8.2 VPC Endpoints

Interface and Gateway Endpoints provide private access to AWS services.

Endpoints Used:

- S3
- Systems Manager
- CloudWatch

Security Benefits:

- Traffic stays within AWS network

- No internet traversal

---

9. Logging, Monitoring, and Threat Detection

9.1 AWS CloudWatch

CloudWatch provides centralized metrics, logs, and alarms.

Characteristics:

- Application and infrastructure monitoring
- Alarm-based alerting
- Operational dashboards

9.2 AWS CloudTrail

CloudTrail records all API and IAM activity.

Characteristics:

- Immutable audit trail
- Detection of unauthorized or anomalous actions

9.3 VPC Flow Logs

Flow Logs capture accepted and rejected network traffic.

Characteristics:

- Network forensics
- Detection of scanning or misconfigurations

9.4 Amazon GuardDuty

GuardDuty acts as the intrusion detection system for the environment.

Characteristics:

- Credential compromise
- Port scanning
- Malware and C2 communication

- Continuous threat detection without agents

9.5 Amazon SNS

SNS is used for security and operational alerts.

Characteristics:

- Notify security teams of incidents
- Integrate with email, Slack, or ticketing systems

---

10. Identity and Access Management (IAM)

IAM provides centralized identity and permission management across the architecture.

Characteristics and Benefits:

- Least privilege
- Role-based access
- MFA for human users
- Prevents credential sprawl
- Enables secure automation

---

11. Conclusion

This secure AWS VPC architecture is designed to be deployable in production, not just theoretical. It leverages AWS-managed services to reduce operational burden while maintaining a strong security posture.