Azure and AWS Secure Multi-Cloud VPN Architecture

# 1. Problem Statement

A fintech company with a global customer base needs to ensure high availability and security by leveraging a multi-cloud environment. To meet business continuity and data confidentiality needs, the company seeks to deploy app components across both AWS and Azure without exposing traffic to the public internet. A secure, encrypted site-to-site VPN tunnel is required to allow seamless private communication between the two cloud environments.

# 2. Objectives

To establish a secure connection between AWS and Azure to support the migration of a fintech application. The solution ensures multi-cloud availability, encrypted communication, and no exposure to the public internet.

# 3. Requirement Gathering Questions and Assumptions

- Are both clouds under our control? Yes

- Do both VMs need bidirectional access? Yes

- Should the connection be fully private (no public IP access)? Yes

- Which regions are being used? AWS (N. Virginia), Azure (East US)

- Do we need to manage routing manually or dynamically? Static routing preferred

- Are we using static PSKs (pre-shared keys)? Yes, manually configured to match

# 4. Key Deliverables

• Virtual Network and Subnet in Azure

• Virtual Private Cloud (VPC) in AWS

• Gateways (VPN) in both Azure and AWS

• Secure VPN tunnel interconnection

• Connectivity testing across clouds

# 5. Current Architecture Diagram

Azure:

- Virtual Network: azure-vnet

- Subnet: azure-subnet (10.0.1.0/24)

- VM IP: 10.0.1.4 (Private), 52.188.184.10 (Public)

- Gateway: Virtual Network Gateway (VPN type)

AWS:

- VPC: aws-vpc (10.1.0.0/16)

- Subnet: aws-subnet (10.1.1.0/24)

- EC2 VM IP: 10.1.1.117 (Private), 54.157.200.221 (Public)

- Gateway: Virtual Private Gateway with Site-to-Site VPN connection

# 6. Proposed Solution Diagram

[Diagram Placeholder: Will include arrows for tunnel, show both clouds, VM endpoints, and route tables]

- AWS and Azure networks connected through VPN gateways

- Static routing enabled for 10.0.0.0/16 and 10.1.0.0/16

- VPN Tunnel 1 & 2 show status: UP

- VMs created and used for connectivity testing

# 7. Project Tasks

1. Created Azure VNet and subnet

2. Created Azure VPN Gateway

3. Created AWS VPC and subnet

4. Deployed AWS VPN Gateway and Customer Gateway

5. Created VPN connection with matched PSK and BGP disabled

6. Verified bi-directional connectivity with private IP ping test

# 8. Mapping Problem Statement to Solution

| Requirement | Implemented? | Notes |

|-------------|--------------|-------|

| Private communication between clouds | Yes | VPN tunnel established |

| Avoid public internet exposure | Yes | No inbound rules to public IPs used |

| Redundant tunnels | Yes | Tunnel 1 and 2 established in AWS VPN |

| Successful communication between VMs | Yes (one-way) | EC2 successfully pinged Azure VM |

# 9. Cost Analysis

Estimated Costs (Based on hourly rates for short-term testing purposes):

• Azure VPN Gateway (~$0.42/hr): ~$10.08/day or ~$302.40/month

• AWS VPN Connection (~$0.05/hr per tunnel): ~$2.40/day or ~$72/month

• Azure VM (B1s): ~$0.011/hr = ~$0.26/day

• AWS EC2 (t2.micro): ~$0.0116/hr = ~$0.28/day

Estimated Daily Cost: ~$13

Estimated Monthly Cost: ~$390 (if left running 24/7)

# 10. Compliance and Security

- IPsec/IKE encryption

- Subnet isolation

- No public IP exposure for workload communication

- NSGs and Security Groups tightly controlled

Compliance Standards:

- Encryption in Transit: IPSec VPN uses AES-256 and SHA-256

- Isolation: VPCs and VNets are isolated logically and securely

- Access Control: Only authenticated users (via SSH with private keys) can access VMs

- Supported: AWS and Azure both support ISO 27001, SOC 2, HIPAA, FedRAMP

# 11. Screenshots and Documentation

Captured:

- Azure VNet and Subnet Creation

- Azure VPN Gateway Setup

- AWS VPC and Subnet Creation

- AWS VPN Gateway and Customer Gateway Configuration

- Tunnel Setup and PSK Matching

- Routing Table Configuration

- Private IP Ping Tests

- SSH Attempts

- Azure VM IP and Subnet Confirmation

- Cost Snapshots

(Note: Screenshots compiled in separate file/PPT)

# Prepared By

Prepared by: James King

Project: Multi-Cloud VPN Architecture

Date: May 2025