Math and Computer Science

MCS- 7013 – Collaborative Research Project

Cloud Security and Multi-Cloud Environments

Student Name: Sri Vishal Kotari

Date: 01/26/2025

One-Page Proposal: Enhancing Security and Traffic Management in Multi-Cloud Environments

Objective:

This project aims to design a secure, scalable, and optimized multi-cloud architecture leveraging AWS and Azure. The focus is on addressing security challenges, enabling secure cross-cloud connectivity, managing network traffic, and proactively monitoring and mitigating threats to ensure compliance with cloud security best practices.

Approach:

1. **Infrastructure Setup and Traffic Management:**
    - Create isolated environments using **AWS VPC** and **Azure VNet**, connected via secure VPN or Direct Connect.
    - Deploy **Aviatrix** to establish a secure and scalable network connection between AWS and Azure, simplifying cross-cloud communication.
    - Use **AWS Load Balancers** and **Azure Load Balancers** to manage and distribute traffic efficiently.
    - Simulate network traffic using tools like **Apache Benchmark (ab)**, **Iperf**, and **hping3** for HTTP/HTTPS requests and TCP/UDP throughput testing.
2. **Security Implementation:**
    - Implement **IAM (AWS)** and **RBAC (Azure)** for role-based access control.
    - Enable **AWS GuardDuty** and **Azure Security Center** for threat detection and security posture management.
    - Apply encryption for data in transit and at rest using **AWS KMS** and **Azure Key Vault**.
3. **Monitoring and Logging:**
    - Centralize log aggregation using **Splunk** for unified visibility across AWS and Azure.
    - Use **CloudWatch** (AWS) and **Azure Monitor** to track performance and detect anomalies.
    - Enable **VPC Flow Logs** (AWS) and **Network Watcher** (Azure) for network traffic analysis.
4. **Penetration Testing and Vulnerability Assessment:**
    - Perform penetration testing using **PACU** for AWS and general-purpose tools like **Metasploit**.

- Conduct vulnerability scanning with **Nessus** to identify and remediate security gaps.

5. **Automation and Incident Response:**
   - Automate incident response using **AWS Lambda** and **Azure Automation**, such as isolating compromised resources or revoking access.
   - Configure compliance checks and real-time alerts for suspicious activities.

Expected Outcomes:

- **Enhanced Security:** Robust cross-cloud security through IAM, RBAC, and threat detection.
- **Optimized Performance:** Efficient traffic flow and load balancing across AWS and Azure.
- **Proactive Monitoring:** Real-time visibility into security threats and network performance.
- **Compliance Assurance:** Automated compliance checks for industry standards like GDPR and ISO 27001.
- **Scalable Networking:** Secure, scalable multi-cloud connectivity enabled by Aviatrix.

Tools and Technologies:

AWS (VPC, CloudWatch, GuardDuty, Lambda, Security Hub), **Azure (VNet, Monitor, Security Center, Automation)**, **Aviatrix**, **Splunk**, **Apache Benchmark**, **Iperf**, **hping3**, **PACU**, **Nessus**, **Terraform**.

References:

1. Amazon Web Services. (n.d.). AWS Security Best Practices. Retrieved from https://aws.amazon.com/security/
2. Microsoft Azure Documentation. (n.d.). Azure Security Best Practices. Retrieved from https://learn.microsoft.com/en-us/azure/security/
3. Rhino Security Labs. (n.d.). PACU: AWS Exploitation Framework. Retrieved from https://github.com/RhinoSecurityLabs/pacu
4. Aviatrix Documentation. (n.d.). Secure Multi-Cloud Networking. Retrieved from https://aviatrix.com/

5. Nessus Vulnerability Scanner. (n.d.). Retrieved from https://www.tenable.com/products/nessus