**Experiment - 6**

**Aim:** To design the secure network architecture for a cloud-based application.

**Learning Objective:**

* Learners will be able to identify and implement key components of a secure cloud network architecture.
* Learners will be able to apply best practices in network segmentation, access control, and encryption to enhance the security of cloud-based applications.
* Learners will understand how to use cloud-native security services to protect applications and data. **Tools:**

AWS Virtual Private Cloud (VPC) or Azure Virtual Network, along with associated security services (e.g., AWS Security Groups, Network ACLs, Azure Network Security Groups)

**Theory:**

Secure network architecture in cloud computing involves designing and implementing a network infrastructure that protects applications, data, and resources from unauthorized access and cyber threats. It combines various security measures and best practices to create a robust and resilient environment for cloudbased applications.

**Key Components of Secure Cloud Network Architecture:**

1. **Virtual Private Cloud (VPC) / Virtual Network**: An isolated section of the cloud where you can launch resources in a virtual network that you define.
2. **Subnets**: Segments of the VPC IP address range where you can place groups of isolated resources.
3. **Network Access Control Lists (NACLs)**: Act as a firewall for controlling traffic in and out of subnets.
4. **Security Groups**: Act as a virtual firewall for instances to control inbound and outbound traffic.
5. **Bastion Hosts**: Secure, hardened instances that serve as a gateway for access to your VPC from external networks.
6. **VPN Gateways**: Allow secure communication between your VPC and on-premises network.
7. **Web Application Firewalls (WAF)**: Help protect your web applications from common web exploits.
8. **Load Balancers**: Distribute incoming application traffic across multiple targets and virtual appliances in one or more Availability Zones.

**Best Practices for Secure Network Architecture:**

1. **Network Segmentation**: Divide the network into segments or subnets based on security requirements and function.
2. **Principle of Least Privilege**: Grant only the minimum necessary permissions to users, processes, and applications.
3. **Defense in Depth**: Implement multiple layers of security controls throughout your network architecture.
4. **Encryption**: Use encryption for data in transit and at rest.
5. **Monitoring and Logging**: Implement comprehensive logging and monitoring to detect and respond to security events.
6. **Regular Updates and Patching**: Keep all systems and software up to date with the latest security patches.
7. **Disaster Recovery and Business Continuity**: Design for resilience and have plans in place for potential failures or attacks.

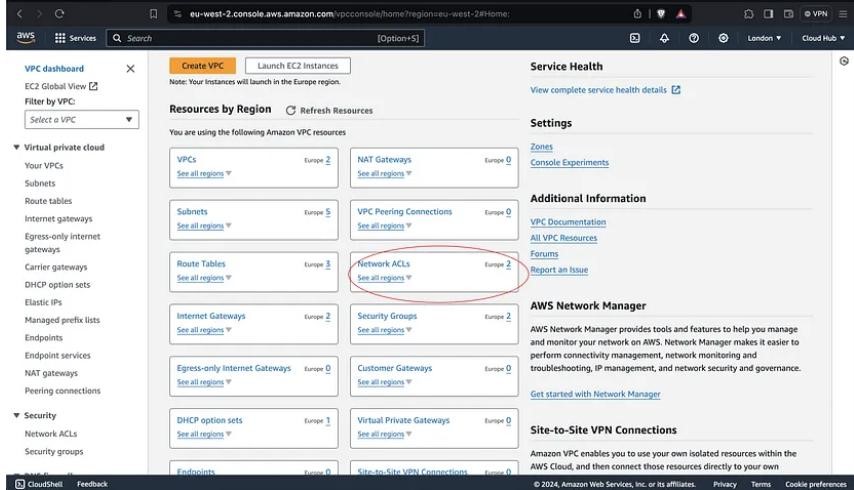
**Implementation:**

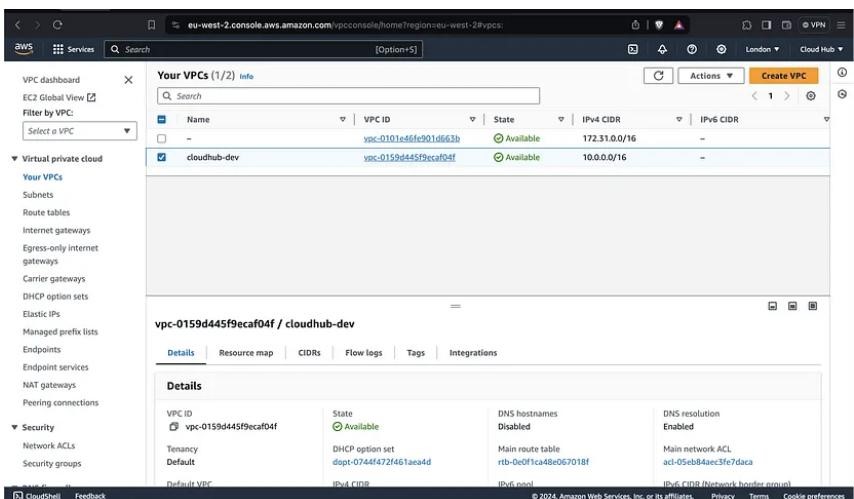
1. **VPC Design**:
   * Create a VPC with public and private subnets across multiple availability zones. o Configure route tables to control traffic flow between subnets.
2. **Security Groups and NACLs**:
   * Set up security groups for each tier of your application (e.g., web, application, database). o Configure NACLs as an additional layer of security at the subnet level.
3. **Bastion Host**:
   * Set up a bastion host in a public subnet for secure SSH access to instances in private subnets.
4. **VPN or Direct Connect**:
   * If required, set up a VPN or Direct Connect for secure communication with on-premises networks.
5. **Web Application Firewall**:
   * Implement a WAF to protect your web applications from common exploits.
6. **Load Balancer**: o Set up a load balancer to distribute traffic and potentially terminate SSL/TLS.
7. **Encryption**:
   * Implement encryption for data in transit using TLS. o Use encryption for data at rest in databases and storage services.
8. **Monitoring and Logging**:
   * Set up cloud-native monitoring and logging services (e.g., AWS CloudWatch, Azure Monitor).
   * Configure alerts for suspicious activities or policy violations.

**Lab Outcome:**

* Successfully design and implement a secure network architecture for a cloud-based application using cloud provider services.
* Demonstrate the ability to apply network segmentation, access controls, and encryption to enhance security.
* Configure and use cloud-native security services to protect the application and its data.
* Create documentation explaining the security measures implemented and their purposes.

This experiment provides a comprehensive approach to learning about and implementing secure network architecture for cloud-based applications. It covers key concepts, best practices, and expected learning outcomes, similar to the serverless computing experiment in the original document.





]

