NAME: AMUDA RANTI

ROLE: CLOUD SECURITY ENGINEER

TASK: CLOUD NETWORK SECURITY ENHANCEMENT IN AWS

I led the implementation of a secure cloud networking architecture in AWS. This experience highlights my expertise in designing and enforcing network security controls, enabling secure remote access, and establishing private and encrypted connectivity between cloud environments. By leveraging AWS-native security features, I significantly improved the overall security posture, ensuring compliance with best practices and industry standards.

Project Scope & Key Responsibilities

1. Strengthening Network Security with Security Groups & Network ACLs

Designed and implemented AWS Security Groups to enforce least privilege access control for inbound and outbound traffic.

Configured Network ACLs (NACLs) to provide an additional layer of subnet-level security.

Restricted access to critical resources using IP whitelisting and protocol-based filtering.

2. Implementing Secure Remote Access with a Bastion Host

Deployed a Bastion Host in a public subnet to facilitate secure SSH access to private instances.

Enforced IAM-based authentication and MFA for added security.

Enabled session logging for auditing and compliance tracking.

Restricted SSH access to trusted IPs using Security Groups to minimize exposure.

3. Establishing Secure Connectivity with VPC Peering & VPN Tunneling

Configured VPC Peering to allow private and secure communication between multiple VPCs.

Deployed AWS Site-to-Site VPN to enable encrypted communication between AWS and on-premises networks.

Implemented IPSec encryption to ensure data confidentiality and integrity.

Enforced strict routing policies to control traffic flow and prevent unauthorized access.

Business Impact & Key Outcomes

- Strengthened cloud network security by implementing multi-layered access controls.
- Ensured secure and restricted remote access using a hardened Bastion Host.
- Established encrypted communication between cloud and on-premises infrastructure.
- Reduced the attack surface and mitigated unauthorized access risks.
- Demonstrated proficiency in AWS network security architecture and best practices.

- Documented network security architecture with detailed configuration steps.
- Security Group and Network ACL policies with applied rules.
- Bastion Host setup documentation, including SSH access controls and logging configurations.
- VPC Peering and VPN setup details with security enhancements.

This experience serves as a strong validation of my expertise in designing and implementing secure cloud network infrastructures, reinforcing my ability to protect cloud environments from evolving security threats.