Cloud Network Security on AWS

Course Duration- 4 Days

Prerequisites

- Basic AWS knowledge
- Understanding of TCP/IP networking
- Familiarity with IAM concepts
- Basic Linux or Windows administration

Learning Outcomes

By the end of this course, participants will be able to:

- Design secure AWS network architectures.
- Implement layered network security using Security Groups, NACLs, AWS Network Firewall, WAF, and Shield.
- Secure hybrid and multi-account connectivity with Transit Gateway, VPN, Direct Connect, and PrivateLink.
- Monitor and investigate network activity using VPC Flow Logs, CloudTrail, GuardDuty, and Security Hub.
- Apply AWS networking security best practices, Zero Trust principles, and defense-in-depth strategies for production environments.

Day 1: AWS Networking Fundamentals and Security Foundations

Module 1: AWS Global Infrastructure

- AWS Regions and Availability Zones
- Edge Locations, AWS Local Zone, AWS Wavelength, AWS Outpost
- Shared Responsibility Model
- Security Pillar of AWS Well-Architected Framework

Module 2: Amazon VPC

- Amazon VPC and VPC Components
- IP Fundamentals and CIDR Planning
- Public and Private Subnets

- Route Tables
- Internet Gateway
- Egress-only Internet Gateway
- NAT Gateway
- NAT Instance
- Elastic IP Addresses
- ENI

Lab 1- Create a VPC with Public and Private subnet

Module 3: Traffic Control

- Security Groups
- Network ACLs
- Stateless vs Stateful Firewalls
- VPC Reachability Analyzer

Lab 2- Configure traffic control using NACL and SG

Module 4: DNS and Name Resolution

- Amazon Route 53
- Route 53 Resolver
- Hosted Zones
- DNS Firewall

Lab 3- Configure private hosted zone

Day 2: Advanced Network Security

Module 5: VPC Connectivity

- VPC Endpoint
- VPC Peering
- Transit Gateway
- AWS PrivateLink

Lab 4- Create VPC Peering and test the connectivity

Module 6: Hybrid Connectivity

- Site-to-Site VPN
- Client VPN
- AWS Direct Connect

Module 7: Load Balancer Security

- Application Load Balancer
- Network Load Balancer
- Gateway Load Balancer
- TLS Offloading
- SSL Certificates
- AWS Certificate Manager

Lab 5- Securing applications using Application load balancer

Day 3: Network Protection Services

Module 8: AWS Network Firewall

- Architecture
- Stateless Rule Groups
- Stateful Rule Groups
- Domain Filtering
- Threat Signatures
- TLS Inspection
- Firewall Manager Integration

Lab6- Set up Network Firewall

Module 9: AWS WAF

- Web ACLs
- Managed Rules
- Rate Limiting
- Custom Rules
- Bot Control

- CAPTCHA
- Integration with CloudFront and ALB

Lab 7- Secure web application using AWS WAF WebACL

Module 10: AWS Shield

- DDoS Protection
- Shield Standard
- Shield Advanced
- Global Threat Dashboard
- Cost Protection

Module 11: Firewall Manager

- Organization-wide Security Policies
- Centralized Firewall Management
- Compliance Enforcement

Day 4: Monitoring, Detection, and Best Practices

Module 12: Logging and Monitoring

- VPC Flow Logs
- CloudWatch Logs
- CloudTrail
- Route 53 Resolver Query Logs
- ELB Access Logs
- Network Firewall Logs

Module 13: Threat Detection

- Amazon GuardDuty
- Amazon Inspector
- AWS Security Hub
- Amazon Detective
- IAM Access Analyzer
- AWS Trusted Advisor Security Checks

Module 14: Incident Response

- Investigating Network Threats
- Traffic Analysis
- Isolation Techniques
- Security Automation
- AWS Config Rules
- EventBridge Automation

Capstone Project- Build and secure Enterprise Network Design