**Day 10**





**“CLOUD SECURITY”**

**Elastic Load Balancer Security:**

1. **Traffic Management & Defense:**

* ELB handles encryption/decryption centrally, offloading EC2 instances.
* Acts as a first line of defense against network attacks.
* Integrates with VPC security groups for fine-grained control.

1. **Encryption & Cipher Control:**

* Supports HTTPS/TLS traffic encryption with customizable cipher suites.
* Perfect Forward Secrecy (PFS) ensures session security even if long-term keys are compromised.
* Customers can enforce protocol/cipher compliance (e.g., PCI, SOX) and prioritize secure cipher negotiation.

1. **Logging & Client IP Retention:**

* Preserves original client IPs despite request proxying.
* Access logs contain detailed metadata: request/response size, client/backend IPs, ports, HTTP methods—useful for auditing and analytics.

**Amazon VPC Security**:

1. **Amazon VPC Overview:**

* VPC creates an isolated AWS cloud environment with customizable IP address ranges, subnets, and routing.
* Users can group instances by subnet and control inbound/outbound traffic using security groups and network ACLs.

1. **VPC Architecture Types:**

* Single Public Subnet: Instances directly access the internet; secured using ACLs and security groups.
* Public + Private Subnets: Private subnet instances use NAT via public subnet for outbound internet access.
* Public + Private Subnets with VPN: Adds IPsec VPN for secure connection to on-premises data centers.
* Private Subnet with VPN Only: Fully isolated from internet; accessible only via VPN from on-premises.

1. **Key Benefit:**

* Offers granular control over network architecture, enhanced security isolation, and hybrid cloud connectivity.

**Amazon Route 53 Security:**

1. **What is Route 53?**

* A highly available, scalable DNS service that maps domain names to IP addresses for AWS or external infrastructure.
* Supports domain registration, latency-based routing, Geo DNS, and DNS failover to ensure low-latency and fault-tolerant access.

1. **Security Features:**

* Authenticated API access with HMAC-SHA256/SHA1 and SSL encryption for secure communication.
* IAM integration allows fine-grained access control for managing DNS functions.
* Privacy protection during domain registration prevents data exposure via public Whois.

1. **Availability & Resilience:**

* Distributed architecture using AnyCast routing ensures low-latency and automatic failover.
* Health checks and DNS failover help reroute traffic during endpoint failure or overload.

--The End--