AWS VPC - Day 3: Security, High Availability & Best Practices

🔔 **Follow me SHAIK HARI SADIA ANJUM for more AWS content!** 🚀

1. Introduction

On **Day 1**, we covered **VPC fundamentals**, and on **Day 2**, we explored **advanced networking concepts** like **VPC Peering, Transit Gateway, PrivateLink, and hybrid cloud connectivity**. Today, we will focus on **VPC security, high availability (HA), compliance, and best practices**, along with **real-world case studies** to demonstrate how organizations implement VPC designs.

🔹 **Key Objectives:**
✅ Secure AWS VPC using **IAM, NACLs, Security Groups & WAF**.
✅ Design **highly available & fault-tolerant VPC architectures**.
✅ Implement **monitoring & compliance best practices**.
✅ Understand **real-world implementations** of AWS VPC security and HA.

2. VPC Security Best Practices

2.1 Security Groups (SGs) – Instance-Level Protection

🔹 **Stateful firewall** that controls inbound and outbound traffic at the **instance level**.
🔹 Default setting: **All inbound traffic is denied, outbound traffic is allowed**.

Best Practices:
✔ Follow **least privilege access** → Allow only required ports.
✔ Use **different SGs per application tier** (Web, App, DB).
✔ Enable **restricted SSH/RDP access** → Only allow specific IPs.

Real-World Case Study 1: Preventing Data Breaches with Security Groups

📌 **Problem:**
A **financial services company** had an **open security group rule (0.0.0.0/0 for SSH)**, allowing attackers to brute-force their EC2 instances.

✅ **Solution:**

- Implemented **Security Groups** allowing **only specific IPs** for SSH access.

- Enabled **AWS Systems Manager Session Manager** to remove the need for SSH altogether.
- Monitored **failed SSH attempts** using **AWS CloudTrail** and set up alerts.

🛠️ **Outcome:**
🔹 Eliminated unauthorized SSH access.
🔹 Reduced **attack surface** and improved **security posture**.

2.2 Network ACLs (NACLs) – Subnet-Level Protection

🔹 **Stateless firewall** that controls inbound and outbound traffic at the **subnet level**.
🔹 Rules are **evaluated in order** (lowest number first).

Best Practices:
✔️ Deny **all unnecessary ports** (e.g., 3389 for RDP).
✔️ Allow only **trusted IP ranges** for SSH/HTTP access.
✔️ Use **custom NACLs** instead of the default ACL.

Real-World Case Study 2: Protecting Sensitive Data in a Healthcare Application

📌 **Problem:**
A **healthcare company** needed to secure **patient data** stored in AWS, ensuring compliance with **HIPAA** regulations.

✅ **Solution:**

- Created a **separate private subnet** for databases with **strict NACL rules**.
- Implemented **VPC Flow Logs** to monitor unusual traffic patterns.
- Blocked **all inbound traffic** except from **application servers**.

🛠️ **Outcome:**
🔹 **Ensured compliance with HIPAA**.
🔹 **Prevented unauthorized database access**.

2.3 AWS Web Application Firewall (WAF) & AWS Shield

🔹 Protects **web applications from Layer 7 attacks** (SQL Injection, XSS, DDoS).
🔹 Works with **ALB, API Gateway, and CloudFront**.

Best Practices:
✔️ Use **AWS Managed Rule Sets** to block common threats.
✔️ Implement **rate limiting** to prevent DDoS attacks.
✔️ Enable **Geo-Blocking** to restrict access from specific countries.

Real-World Case Study 3: Defending an E-commerce Website from DDoS Attacks

📌 **Problem:**
A **leading e-commerce company** experienced **DDoS attacks** during Black Friday sales, impacting website performance.

✅ **Solution:**

- Implemented **AWS WAF** to block malicious requests.
- Upgraded to **AWS Shield Advanced** for enhanced **DDoS protection**.
- Used **CloudFront** to cache static content, reducing backend load.

🛠️ **Outcome:**
🔹 Website remained **operational during peak traffic**.
🔹 Blocked **90% of attack traffic** before reaching application servers.

3. Designing High Availability (HA) in AWS VPC

3.1 Multi-AZ Architecture

🔹 Deploy resources across **multiple Availability Zones (AZs)** to ensure redundancy.

✔️ **Multi-AZ RDS** for database failover.
✔️ **Multi-AZ ALB & Auto Scaling Groups** for application servers.
✔️ Use **AWS Route 53 health checks** for DNS failover.

Real-World Case Study 4: High Availability for a SaaS Application

📌 **Problem:**
A **SaaS company** needed to ensure **zero downtime** for its global customers.

✅ **Solution:**

- Used **Multi-AZ RDS deployment** for automatic failover.
- Deployed **Auto Scaling Groups** across **three AZs**.
- Configured **Route 53 failover routing** with health checks.

🛠️ **Outcome:**
🔹 **99.99% uptime achieved**.
🔹 **Zero downtime during AZ failures**.

3.2 NAT Gateway High Availability

🔹 **Single-AZ NAT Gateway = Single Point of Failure (SPOF)**.
✔️ Deploy **multiple NAT Gateways across AZs**.
✔️ Use **multiple route tables** to distribute traffic.

Real-World Case Study 5: Preventing Network Outages with NAT Gateway HA

📌 **Problem:**
A **media streaming company** faced **downtime** when their **NAT Gateway** failed in a **single AZ**.

✅ **Solution:**

- Deployed **multiple NAT Gateways across different AZs**.
- Configured **route tables** to direct traffic through the **nearest healthy NAT Gateway**.

🛠️ **Outcome:**
🔹 **Continuous network availability**.

🔹 **Zero impact on user experience**.

4. Compliance & Auditing in AWS VPC

AWS Security Hub – Centralized Security Monitoring

🔹 Aggregates security alerts from **GuardDuty, IAM Access Analyzer, and AWS Config**.
✔️ Enables **automated compliance checks** for **PCI DSS, ISO 27001, HIPAA**.

Real-World Case Study 6: Automating Compliance for a Banking Institution

📌 **Problem:**
A **banking institution** needed to **automate security audits** to comply with **PCI DSS**.

✅ **Solution:**

- Enabled **AWS Security Hub** to aggregate security insights.
- Set up **AWS Config rules** to track changes in **VPC settings**.
- Used **AWS Lambda** to auto-remediate security violations.

🛠️ **Outcome:**
🔹 **Automated compliance reporting**.
🔹 **Reduced manual security audits by 80%**.

5. AWS VPC Best Practices Summary

✅ **Use Multi-AZ deployments** for high availability.
✅ **Restrict access with IAM roles, SGs, and NACLs**.
✅ **Monitor traffic using VPC Flow Logs and AWS Config**.
✅ **Use AWS Shield & WAF to prevent DDoS and web attacks**.
✅ **Implement NAT Gateway HA** to prevent network failures.
✅ **Use Transit Gateway instead of multiple VPC Peerings**.

Conclusion

On **Day 3**, we covered:
🚀 **VPC security best practices** (IAM, NACLs, WAF, Flow Logs).
🚀 **Designing high-availability VPC architectures**.
🚀 **Compliance & monitoring tools (AWS Config, Security Hub)**.
🚀 **Real-world case studies** demonstrating best practices.