DOMAIN 1 DESIGN SECURE ARCHITECTURES

DOMAIN 1: DESIGN SECURE ARCHITECTURES

📊 Weight: 30% 📘 Core Competency: Designing secure access controls, data protection mechanisms, application-level security, and hybrid/cloud boundary protections using AWS services and security best practices.

SECTION OVERVIEW

Subdomain	Focus Areas
1.1	Secure access to AWS resources
1.2	Secure workloads and applications
1.3	Data protection with encryption
1.4	Secure network architectures

🔹 1.1 Secure Access to AWS Resources

✅ Identity and Access Management (IAM)

Concept	Description
Users/Groups/Roles	IAM identities with fine-grained permissions
IAM Policies	JSON-based access control rules (Allow/Deny)
Service Control Policies (SCP)	Organizational-wide restrictions (used in AWS Organizations)
IAM Roles	Used by EC2, Lambda, etc., to assume access
Temporary Credentials	IAM roles with STS or Identity Federation

IAM Best Practices

- Use least privilege
- Apply MFA for privileged accounts
- Rotate access keys regularly
- Prefer roles over access keys for applications

AWS Single Sign-On (SSO)

- Federated access to AWS accounts and services
- Integrates with Active Directory, SAML, OIDC

🔹 1.2 Secure Workloads and Applications

AWS Secrets Manager & Parameter Store

Tool	Use
Secrets Manager	Manage database passwords, API keys
SSM Parameter Store	Store config strings, supports KMS encryption

- Avoid hardcoding credentials
- Enable automatic secret rotation

Application Security Best Practices

- Use WAF to filter HTTP requests
- Enable Shield / Shield Advanced for DDoS protection
- Use CloudFront for edge security
- Use API Gateway + Lambda Authorizers for APIs

AWS Inspector & GuardDuty

Service	Use
Inspector	Analyze EC2 and ECR images for vulnerabilities
GuardDuty	Detect anomalous activity, malware, threats
Security Hub	Consolidated security posture dashboard

🔹 1.3 Implement Secure Data Storage and Encryption

Encryption Options

Resource	Encryption Type
S3	SSE-S3, SSE-KMS, CSE
EBS	Default encryption with KMS
RDS	Enable at rest & in-transit encryption
SQS, SNS	KMS-supported
Lambda environment	Can encrypt with KMS

✅ KMS Concepts

- Customer Managed Keys (CMK)
- Automatic key rotation
- Audit with CloudTrail

Key Management Tips

- Encrypt sensitive logs and data at rest (e.g., with KMS)
- Use default encryption policies where available
- Use S3 Bucket Policies to enforce encryption requirements

🔹 1.4 Design Secure Network Architectures

VPC Security Layers

Component	Purpose
Security Groups	Stateful firewall for EC2, Lambda, RDS
Network ACLs (NACLs)	Stateless rules applied at subnet level
VPC Endpoints	Private connection to S3/DynamoDB (without NAT/Internet)
VPC Peering / Transit Gateway	Connect VPCs across regions or accounts
PrivateLink	Share internal services across accounts via ENIs

Secure Connectivity Options

Type	Tool
On-prem → AWS	Site-to-Site VPN, AWS Direct Connect
Cross-account access	Resource-based policies, IAM roles
Remote user access	Client VPN, IAM Identity Center (SSO)

Network Security Best Practices

- Use NAT Gateway for private subnet outbound access
- Never place sensitive resources in public subnets
- Deploy bastion hosts with limited IPs for SSH/RDP access
- Use ALBs with HTTPS termination + WAF

🎯 Common Exam Scenarios (Domain 1)

- How do you provide temporary, secure access to S3 for a mobile app?➤ Use pre-signed URLs or Cognito Identity Pools
- You must encrypt all files uploaded to S3, enforce compliance.➤ Use S3 bucket policy + SSE-KMS
- How do you securely share access to an internal API between two AWS accounts?➤ Use PrivateLink with interface VPC endpoint
- What's the best way to allow developers SSH access to EC2 while restricting from the internet?➤ Use bastion host in public subnet + private EC2 in private subnet

✅ Summary Cheat Sheet

Task	AWS Services
Manage user access	IAM, IAM roles, IAM policies
Store secrets	Secrets Manager, SSM Parameter Store
Encrypt data	SSE-S3, SSE-KMS, EBS encryption, KMS
Secure network	VPC, SG, NACL, VPN, Direct Connect
Application-level security	WAF, Shield, Inspector, API Gateway
Audit access	CloudTrail, AWS Config, GuardDuty

📚 Key AWS Resources

- Security best practices in IAM
- Ensure internetwork traffic privacy in Amazon VPC
- Examples of Amazon S3 bucket policies
- AWS Key Management Service
- AWS WAF, AWS Shield Advanced, AWS Shield network security director and AWS Firewall Manager