DDoS Protections:

- DDoS Attack: Distributed denial of service.
  - AWS Shield (Standard):
    - protects against DDoS
    - for all instances at no cost
- Aws Shield Advanced:
  - 24/7 protection DDoS response team
- AWS WAF: Web Application Firewall
  - filter specific requests based on rules
- Cloudfront and Route 53:
  - availability protection using global edge network
  - Combined with Aws Shield provides attack mitigation at the edge

Aws Shield:

- Free service
- Attacks such as SYN/UDP floods, Reflection attacks & other layer 3/4 attacks

Aws Shield Advanced:

- Optional DDoS mitigation service (paid service)
- Protect against more sophisticated attack on specific resources
- 24/7 access to Aws DDoS response team (DRT)

Aws WAF:

- Protect web applications from common web exploits (Layer 7) - HTTP
- Deploy on Application Balancer, API Gateway, Cloudfront
- Define Web Acl (Access Control Lists)
  - Rules: Can include IP addresses, HTTP headers, HTTP body, or URI strings
  - Protect from common attacks - SQL injection & Cross site scripting (XSS)
  - Size constraints, geo-match (block, count, allow)

Aws Network Firewall:

- Protect your entire Amazon VPC
- From Layer 3 to Layer 7 protection
- Any direction, you can inspect
  - VPC to VPC
  - Outbound to Internet
  - Inbound from Internet
  - To/from Direct Connect & Site to Site VPN

Aws Firewall Manager:

- Manage security rules in all accounts of an Aws Organization
- Security policy: common set of security rules
- WAF rules (Application Load Balancer, API Gateway, Cloudfront)
- Aws Shield Advanced
- Aws network Firewall
- Rules are applied all resources including to future ones

Penetration Testing:

- Pen & Exercise, you can test AWS any approval
  - Cloudfront, EC2 Instance, NAT Gateways and Elastic Load Balancers
  - Amazon RDS
  - Amazon Aurora
  - Amazon Elasticache
  - AWS Lambda and Lambda Edge functions
  - Amazon Elastic Beanstalk
  - Amazon Gateway Rest API endpoints

Prohibited Activities!

- DNS Zone walking via Route 53
- DNS DOS
- Port flooding, Protocol flooding
- Request flooding

Encryption with KMS & Cloudhsm:

- Data at Rest: Encrypted at rest
- Data on Transit: Encrypted while in motion/replicating
- Pen Test on Storage Encryption Keys

Aws KMS:

- KMS = key management service
- Aws manages software for encryption keys
- Encryption Opt is:
  - EBS volumes
  - S3 Buckets + Kinesis/SQS
  - RDS DB + EFS drives
- Encryption automatically enabled
  - Cloudtrail logs
  - S3 Glacier
  - Storage Gateway

Cloud HSM:

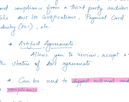
- Aws provisions encryption hardware
- Dedicated Hardware (DDoS + Tamperproof tamper resistant)
- You manage your own encryption keys entirely (not Aws)
- Compliance requirement - FIPS 140-2 level 3 compliance

Types of KMS Keys:

- Customer Managed Key - Customer created
- Aws Managed Key - Aws generated & stored
- Aws Owned Key - Aws owns (cost low)
- Cloudhsm Keys - Cloudhsm hardware

Aws Certificate Manager:

- Lets you easily provision, manage + deploy SSL/TLS certificates
- Used to provide in-flight encryption for website certificates
- Supports both public + private TLS certificates
- Free of charge when public TLS Certificate
- Auto TLS Cert renewal



Secrets Manager:

- Manager rotating secrets
- Capability to generate secrets on demand using a lambda
- Integration with Amazon RDS
- Secrets are encrypted using KMS
- Mostly meant for RDS integration

Artifact: (not really a service)

- Portal that provides customers with on-demand access to compliance documentation and AWS agreements
- Artifact Reports:
  - Allows you to download AWS security and compliance from a third party auditor like Ernst & Yoshiyama, Payment Card Industry (PCI), etc.
- Artifact Agreements
  - Allows you to review, accept & track the status of AWS agreements
- Can be used to support internal audit requirements

Guard Duty:

- Intelligent threat discovery to protect AWS account
- Uses machine learning, anomaly detection, and cyber intel
- Input data includes:
  - Cloudtrail Event Logs
  - VPC Flow Logs
  - DNS Logs
  - Optional feeds
- Can setup cloudwatch rules to be notified in case of findings
- Can protect against compromised instances

Amazon Inspector:

- Automated Security Assessments
- For instances
  - Looking for unintended network accessible ports
  - Agent installed
- Inspector + integration with Aws Security Hub
- Send findings to Amazon EventBridge

Aws Config:

- Helps with auditing + recording compliance
- Records configurations + changes over time
- Flexibility of storing data into documents + configuration data
- It is a per-region service

Aws Macie:

- Fully managed data security and data privacy service.
- Uses machine learning to discover & protect your sensitive data in Aws
- Macie helps identify & alert you to sensitive data, such as personally identifiable information (PII)

Aws Security Hub:

- Central security tool
- Aggregates findings from various AWS services
- Must first enable the Aws Config service

Amazon Detective:

- Analyzes, investigates + identifies root cause of security issues
- Automatically collects & processes events + produces visualizations

Aws Macie:

- Reporting sensitive information (protected) (Kept behavior)

Root User Privileges:

- Root user = Account Owner
- Complete Access to all resources
- Manage root the root user access keys
- Activate multi factor authentication
  - Change account settings
  - Close Aws account
  - Change Cloudtrail log files
  - Regular as a root or Rootkeyfobs

IAM Access Analyzer:

- Find out which resources are shared externally
  - Logging access activity not shared
  - Allows admins zero of trust & policy

Summary: