VPC

How many VPCs in an Account?

Default VPC Settings

Problems with using Default VPC

# AWS Security

## AWS Shared Responsibility Model

Identity and Access Management

Detective Controls

Network Infrastructure Security

Data Security/Protection

Logging & Monitoring

Incident Response

## VPC (Network Security)

VPC provides a Virtual Private Cloud on the Internet – Private Datacenter on the Cloud. Users can configure the access to the Data-center in any manner they want.

Subnets – Public and Private Subnets. Subnet-level Firewall using NACLs.

Only Public Subnets are allowed external Access

Instances in Private Subnets given access using Bastions and NAT Gateways

## IAM (User Security)

Users, Groups, Policies to use Infrastructure

## Encryption

### Encryption of Data at Rest

Storage (S3, EBS, EFS), Database (RDS, DynamoDB etc.), Cache (Elasti-cache)

### Encryption of Data in Motion

–

### Encryption Key Management

KMS

## Specialized Security Features

DDoS Protection

Penetration Testing

# Security Design Principles

## Implement a Strong Identity Foundation

* Implement principle of least privilege
* Enforce separation of duties
* Authorization for each interaction with AWS Resources
* Centralize privilege management
* Eliminate reliance on long-term credentials

Principals – Users, Groups, Services, Roles

OWASP Top 10 – Web Applications

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient Logging & Monitoring

Misc

1. CSRF – Cross-Site Request Forgery
2. AppDos – Resource Exhaustion (Uncontrolled Resource Consumption)
3. Unrestricted Upload of File with Dangerous Type
4. Clickjacking etc. – UI Misrepresentation of Critical Information
5. Unvalidated Forwards and Redirects
6. Anti-automation – Improper control of Interaction Frequency
7. SSRF – Server Side Request Forgery
8. 3rd Party Content – Functionality from Untrusted Control Sphere