aws Cloud Clubs

Domain 1: Design Secure Architectures

Task 1:
Design secure access to AWS resources

Design secure access to AWS resources

- Access Controls
  - AWS federated access
    - Allows external entities to temporarily connect to resources
  - AWS Identity and Access Management [IAM]
  - AWS IAM Identity Center

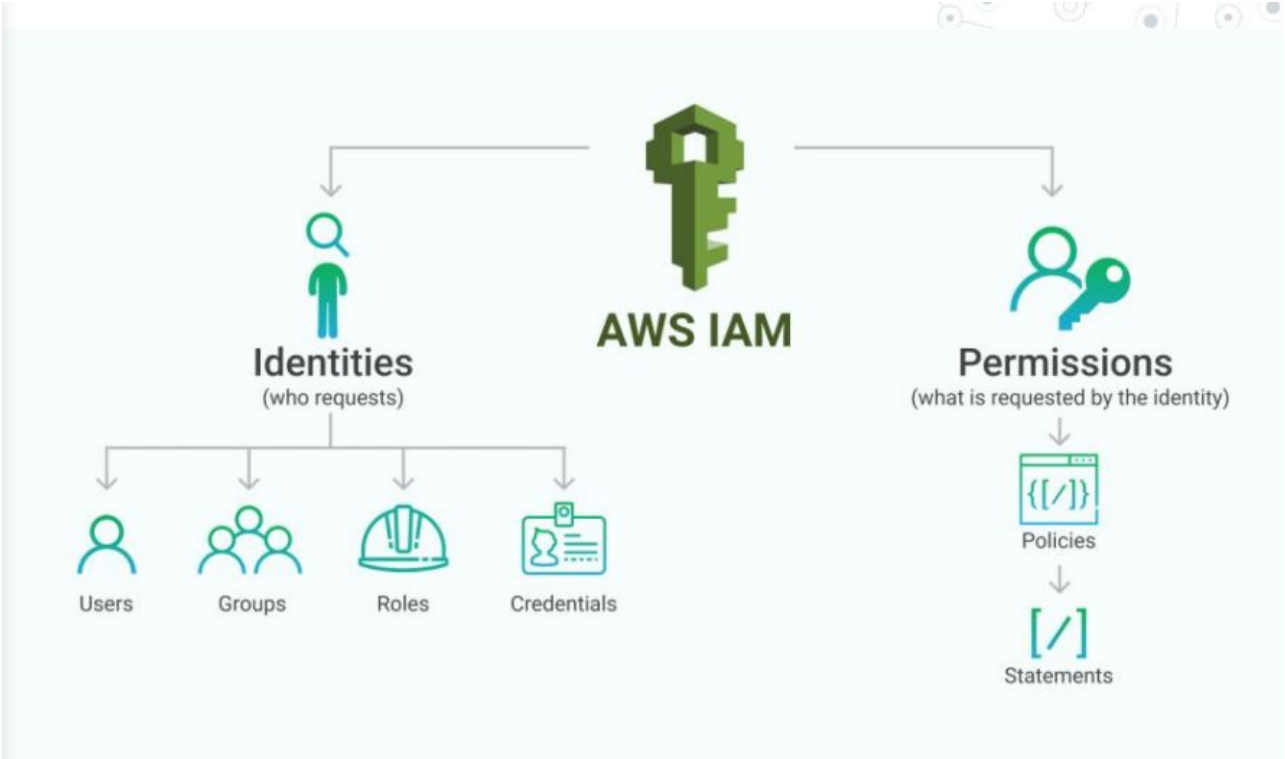
Design secure access to AWS resources

- AWS Users
  - Root User
    - User when you create AWS account
    - Complete access to all AWS account services and resources
  - IAM user
    - AWS Identity and Access Management (IAM) allows you to configure security settings
    - You create IAM users
    - You assign IAM users permissions to what they can access
    - New user has no permissions

Design secure access to AWS resources

- IAM Policy, Groups, and Roles
  - Policy
    - Allows a specific action
      - Ex: Attach policy to let user view S3 bucket
  - IAM Groups
    - A collection of IAM users
    - You can assign policies to IAM Groups
      - Ex: Group “students” given certain policies
  - IAM Roles
    - “An IAM role is an identity that you can assume to gain temporary acces to permissions

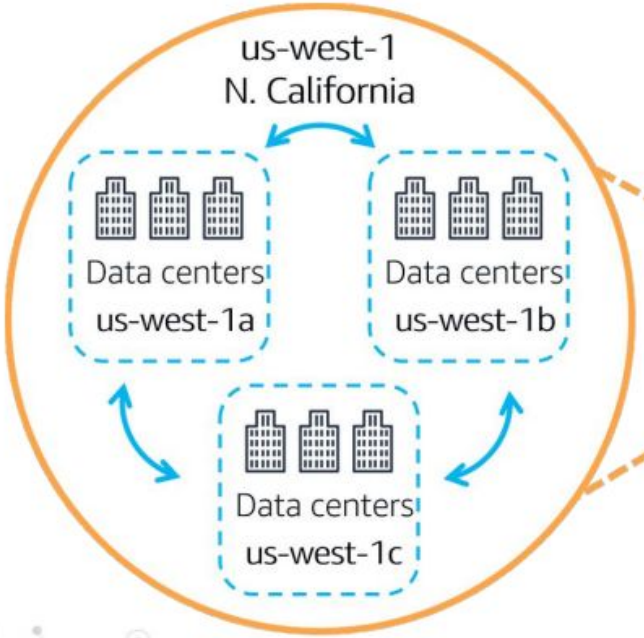
Design secure access to AWS resources



Design secure access to AWS resources

- AWS Global Infrastructure
  - Availability Zones
    - A single (or group of) data center(s)
    - Redundant power, networking, connectivity
  - AWS Regions
    - Consists of multiple isolated Availability zones

Design secure access to AWS resources

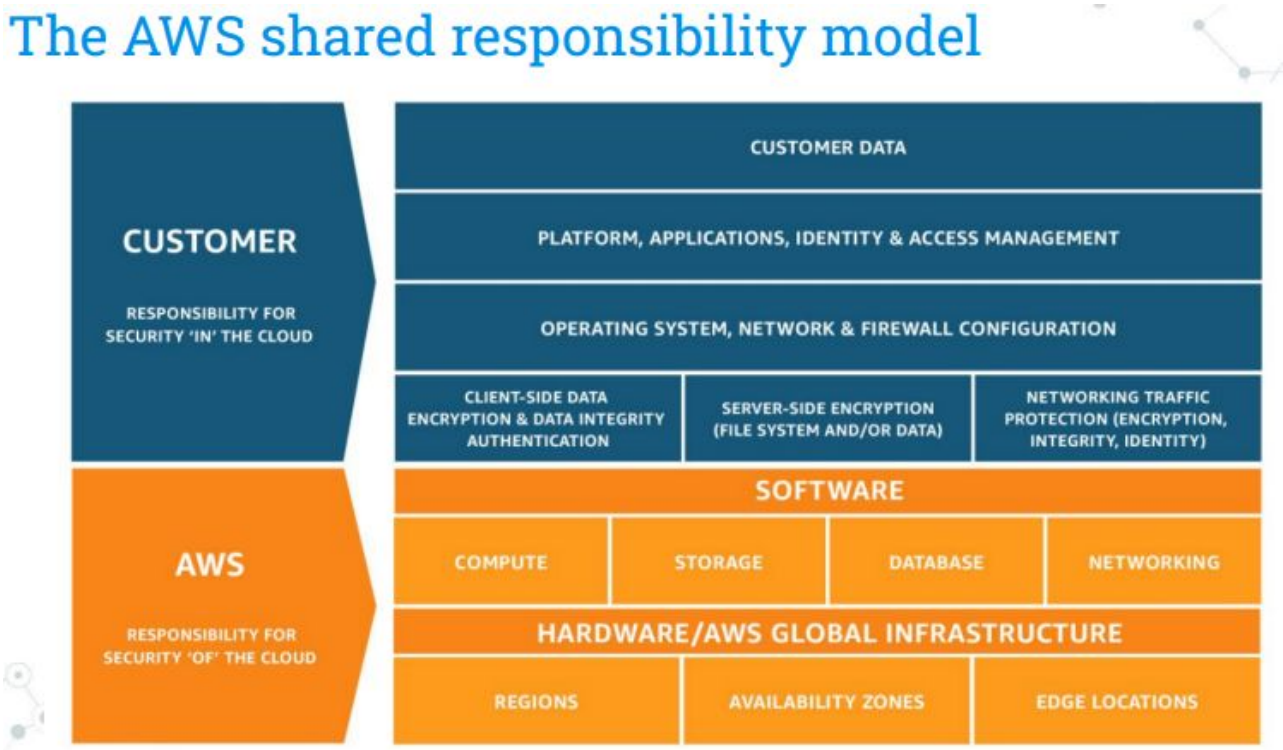


Regions

Availability Zones

Design secure access to AWS resources

- AWS Security best practices
  - Principle of least privilege
- AWS Shared responsibility model



Task 2: Design secure workloads and applications

Design secure workloads and applications

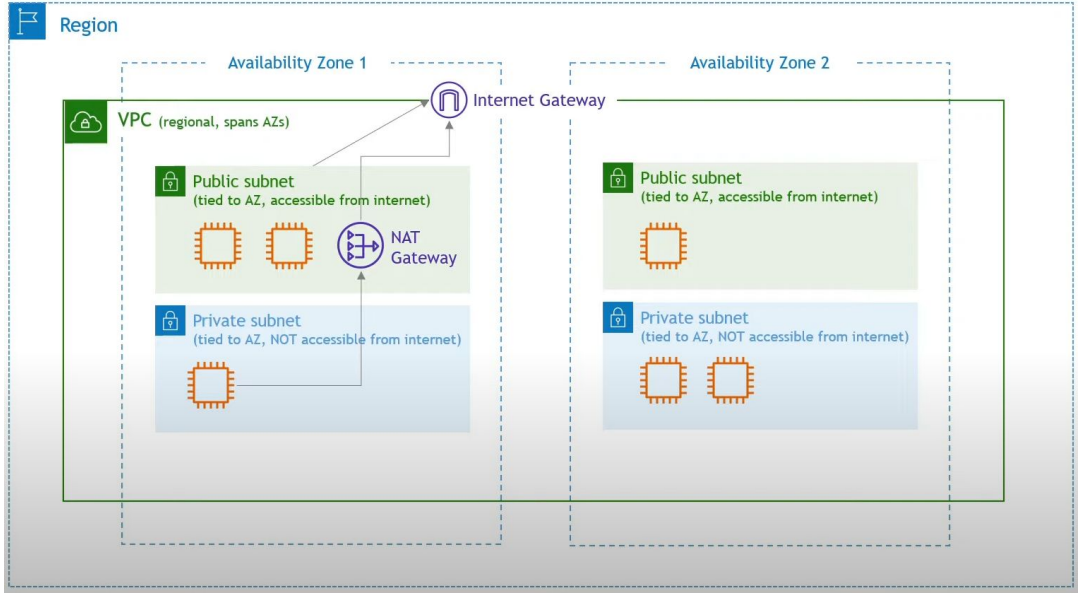
- Application configuration and credentials security
  - AWS Secrets Manager - helps manage, retrieve, and rotate database credentials, API keys, and other secrets
  - AWS Systems Manager Parameter Store - provides hierarchical storage for secrets
- Secure application access
  - Amazon Cognito - enables user authentication
  - AWS IAM - helps manage identities and access to AWS services / resources

Design secure workloads and applications

- Other Security Services
  - Amazon GuardDuty - threat detection service that monitors AWS accounts and workloads for malicious activity
  - Amazon Macie - data security service that discovers sensitive data using ML and pattern matching
- Some Threat Vectors
  - DDoS
  - SQL injection

Design secure workloads and applications

- Virtual Private Cloud (VPC) - enable you to provision an isolated section of the AWS Cloud



Classless Inter-Domain Routing (CIDR) - Notation for describing blocks of IP addresses

https://cidr.xyz/

Design secure workloads and applications

NETWORK ACLs

Firewall that controls traffic in/out of a ***subnet***

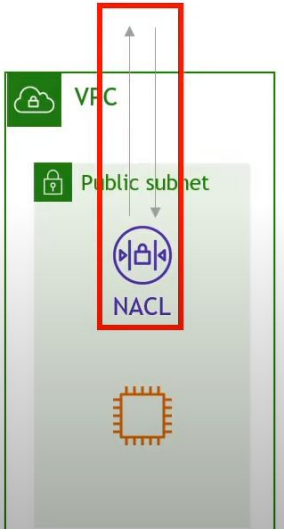
Rules for ***Allow*** and ***Deny***

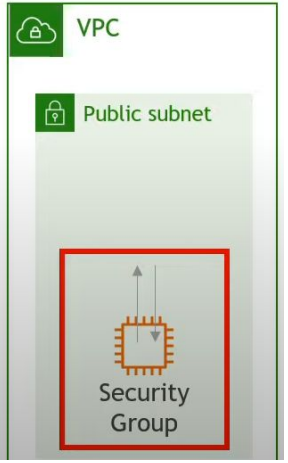
Rules include IP addresses (only)

SECURITY GROUPS

Firewall that controls traffic in/out of an ***EC2 instance***

Rules for ***Allow*** (only)





Task 3: Determine appropriate data security controls

Determine appropriate data security controls

- Data access and governance
  - AWS IAM - managing identities and access to **data** on AWS resources
- Data recovery
  - AWS Backup - centralizes and automates data protection across AWS services
  - Versioning in Amazon S3 - helps to keep multiple variants of an object in the same bucket

Determine appropriate data security controls

- Encryption and appropriate key management
  - Data at rest
    - AWS Key Management Service - lets you create, manage, and control cryptographic keys across AWS applications and services
  - Data in transit
    - AWS Certificate Manager - helps provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services
    - SSL/TLS certificate - digital object that allows systems to verify systems identities & establish an encrypted network connections

Determine appropriate data security controls

- Meeting compliance requirements with AWS
  - AWS Artifact - self-service audit portal that provides access to AWS' compliance documentation and AWS agreements
  - AWS Config Rules - can set rules to monitor compliance information
- Data retention and classification
  - Amazon S3 Object Tagging - key-value pairs applied to S3 objects
  - AWS Config - provides a detailed view of the configuration of AWS resources in your AWS account

Hands-on Demo