SEAS-8414

Analytical Tools for Cyber Analytics

Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Dr. M

Welcome to SEAS Online at George Washington University

SEAS-8414 class will begin shortly

- **Audio:** To eliminate background noise, please be sure your audio is muted. To speak, please click the hand icon at the bottom of your screen (**Raise Hand**). When instructor calls on you, click microphone icon to unmute. When you've finished speaking, ***be sure to mute yourself again***.
- **Chat:** Please type your questions in Chat.
- **Recordings:** As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. Releasing these recordings is strictly prohibited.

Agenda

Week-4: Secure Cloud Computing tools

So far, we have built data and endpoint-centric security for gwuscc.com. In this class, we will learn about how to build secure cloud computing using the following tools:

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- Cloud Access Security Broker (CASB)

For hands-on activities, we will limit exercises to native AWS cloud offerings.

Class-4

Structure

Agenda

- Data Centers
- Networking
- Identity and Access Management (IAM)
- Elastic Compute Cloud (EC2)
- Simple Storage Service (S3)
- Midterm

Basics of IT

AWS Data Breaches

Case Study

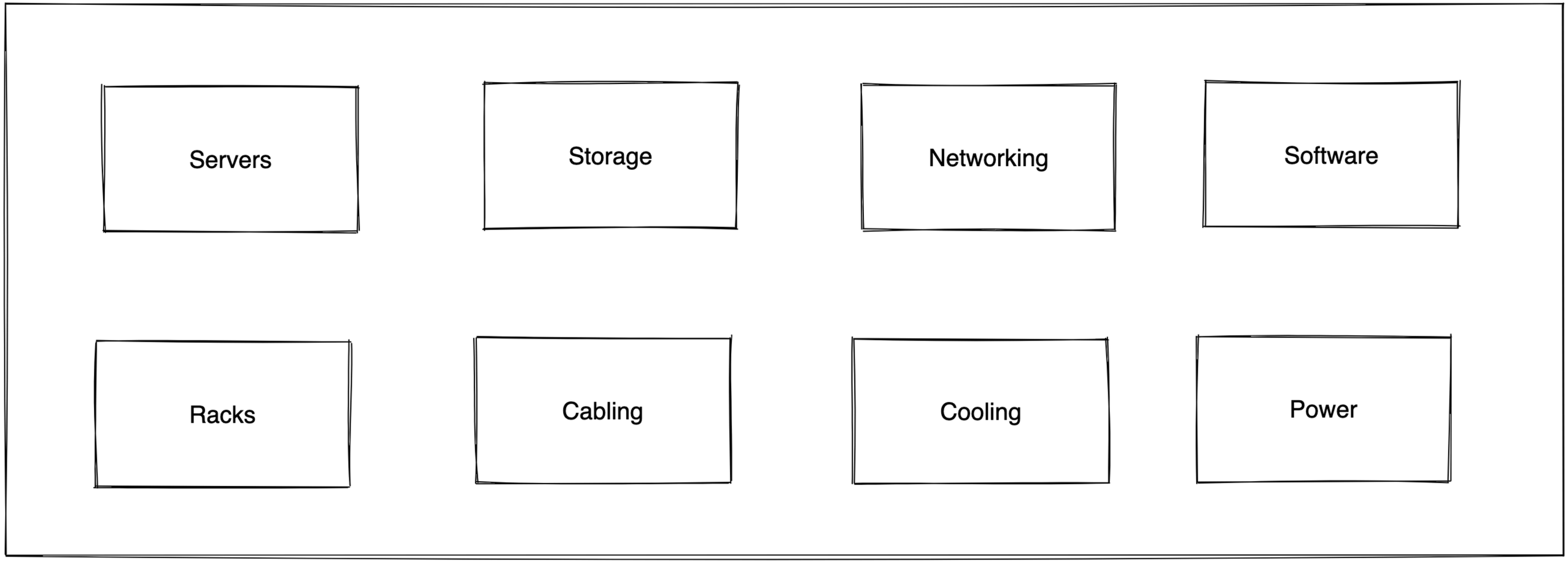
https://firewalltimes.com/amazon-web-services-data-breach-timeline/

Data Centers

Cloud Data Centers

Data Center

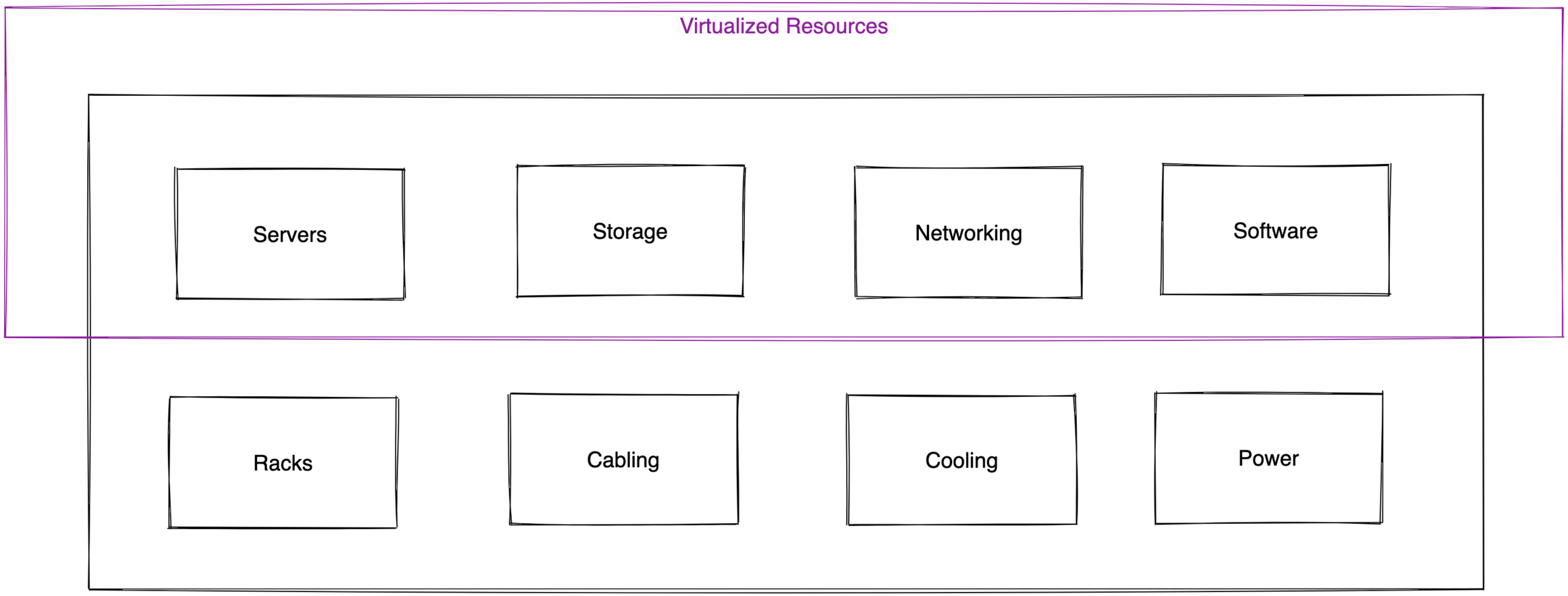
Basics



Cloud Data Center

What is AWS Local Zone?

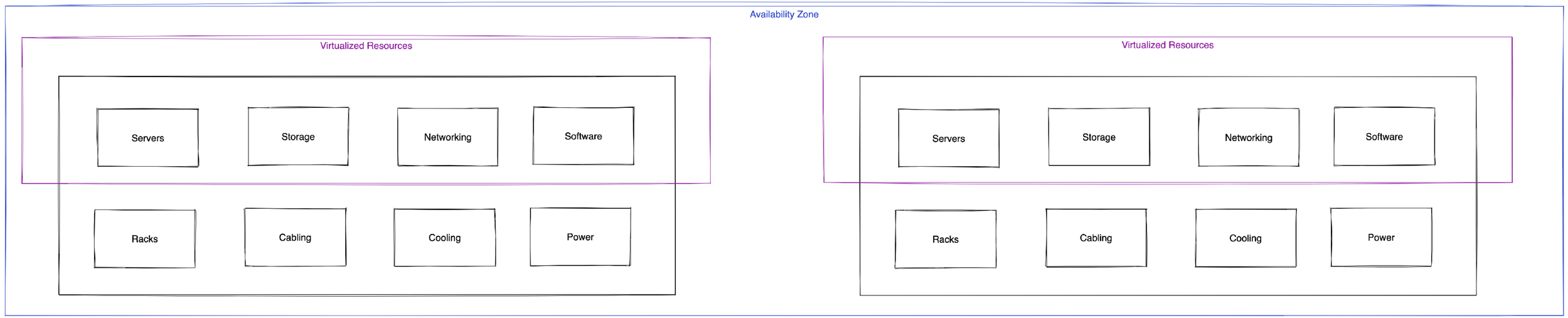
AWS Local Zones are a type of AWS infrastructure deployment that places compute, storage, database, and other select services closer to large population, industry, and IT centers, enabling you to deliver applications that require single-digit millisecond latency to end-users.



Cloud Data Center

What is AWS Availability Zone?

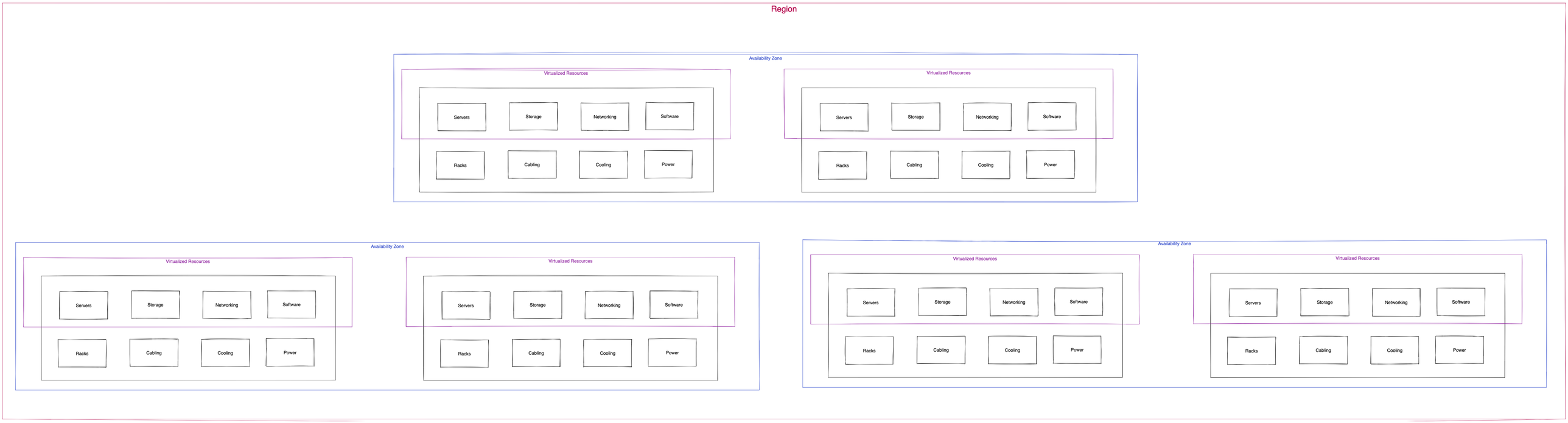
An Availability Zone (AZ) is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region.



Cloud Data Center

What is AWS Region?

AWS Region is a physical location around the world with a cluster of availability zones.
AWS Region can also be defined as a cluster of data centers.

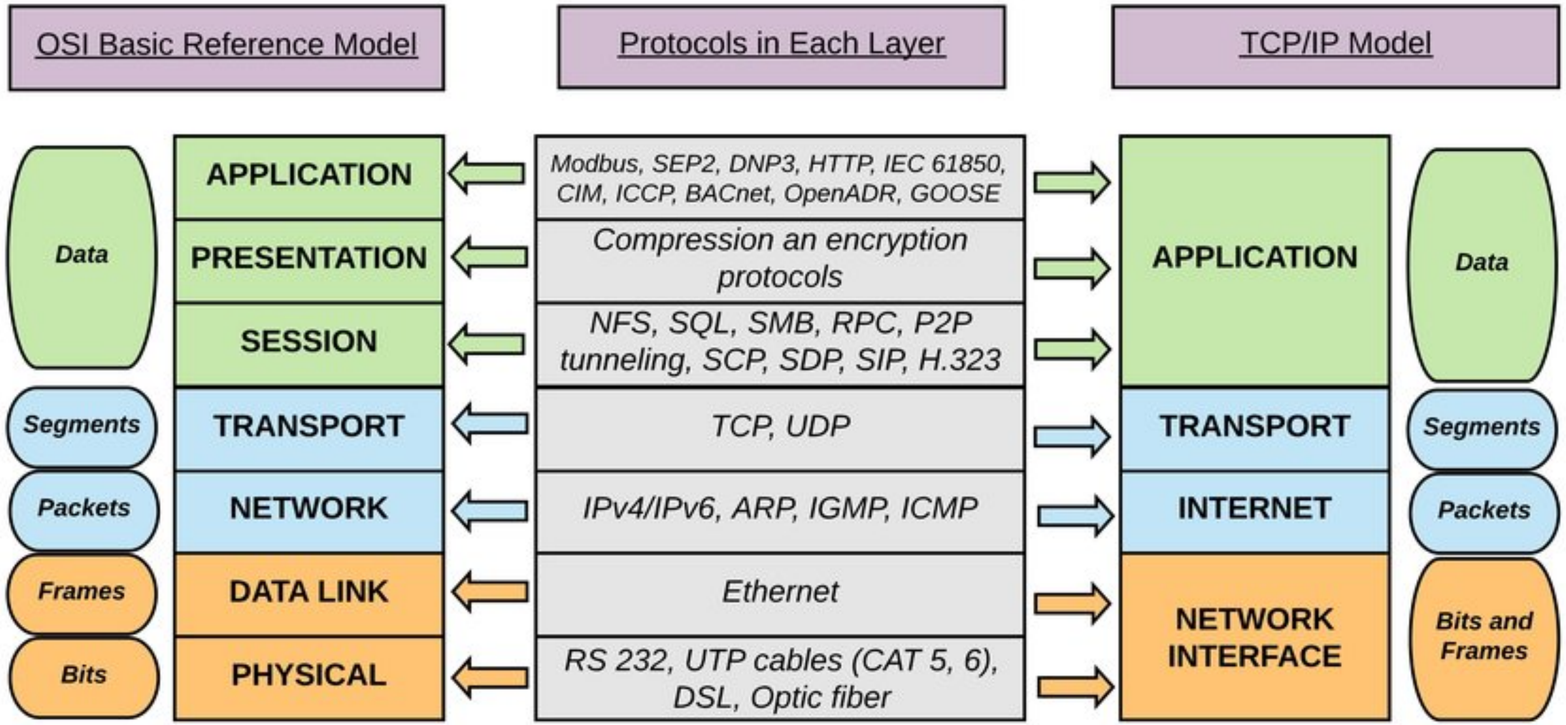


Networking

Basics for Cloud Networking

Introduction to Networking

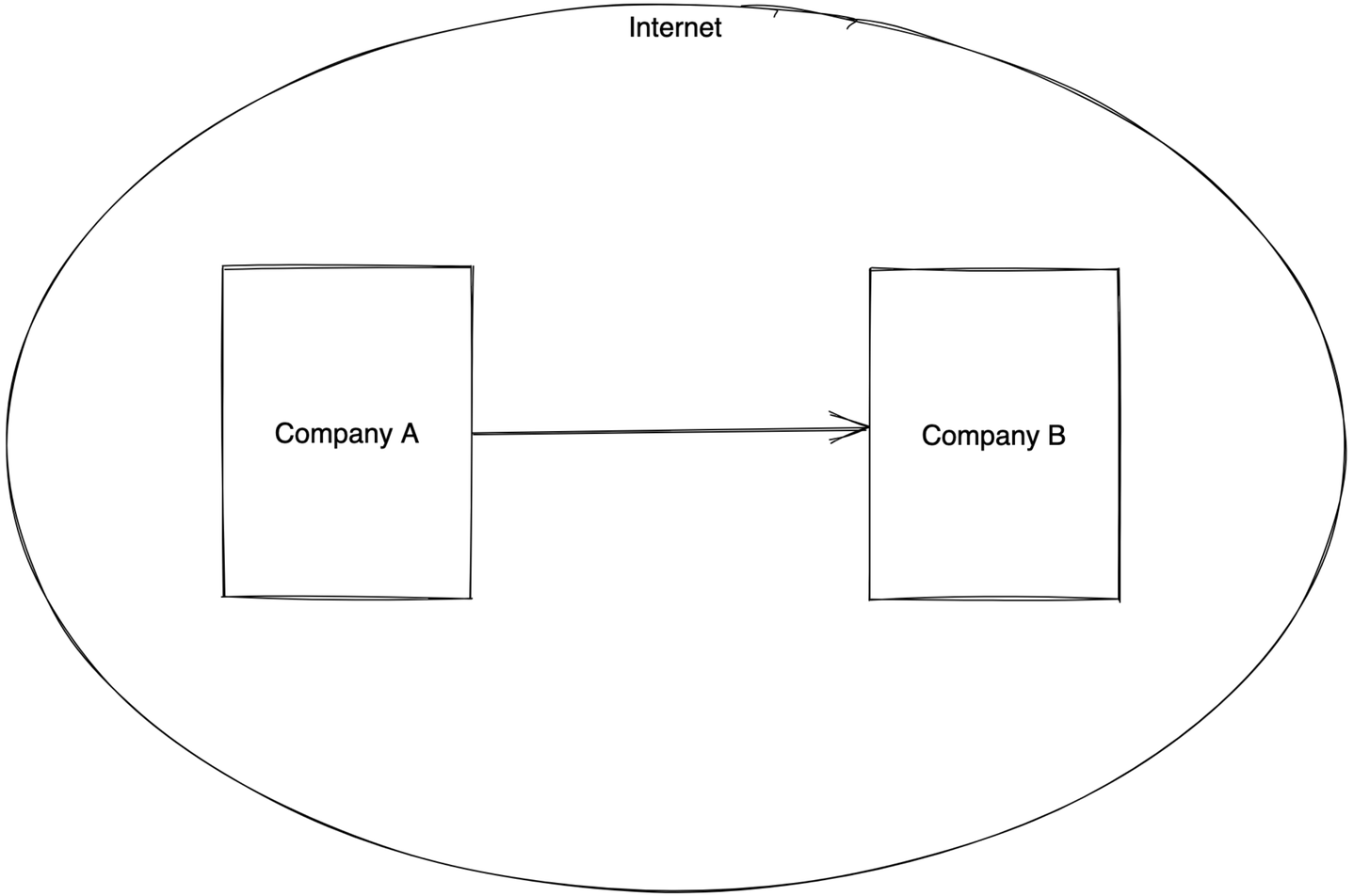
OSI vs TCP/IP



Source: https://www.researchgate.net/figure/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack_fig2_327483011

Networking

Internetworking



Private vs. Public IP address

What do they do?

Public IP:

- With a public IP address, a machine can identify, connect, and communicate over the Internet.
- The IP must be unique across the whole web
- Two machines can **NOT have the same** public IP.
- Can be geographically located easily

- Private IP:

- A private IP address can only identify a machine on a private network only
- The IP must be unique across the private network
- Two different companies can have the **same** private IP range.
- Machines connect to WWW using a Network Address Translation (NAT) + internet gateway (a proxy)
- Only a specified range of IPs can be used as private IPs (https://en.wikipedia.org/wiki/Reserved_IP_addresses)

Elastic IP address

What do they do?

- A public IP need not stay the same across an EC2 instance restart.
- If you need a fixed public IP address, then you need an elastic IP address.
- An elastic IP address can be attached to any instance in the account.
- No two instances can have the same elastic address at a time.
- Elastic IP addresses are used to mask the failure of an instance by rapidly remapping the IP to another instance.

Elastic IP address

Best Practice

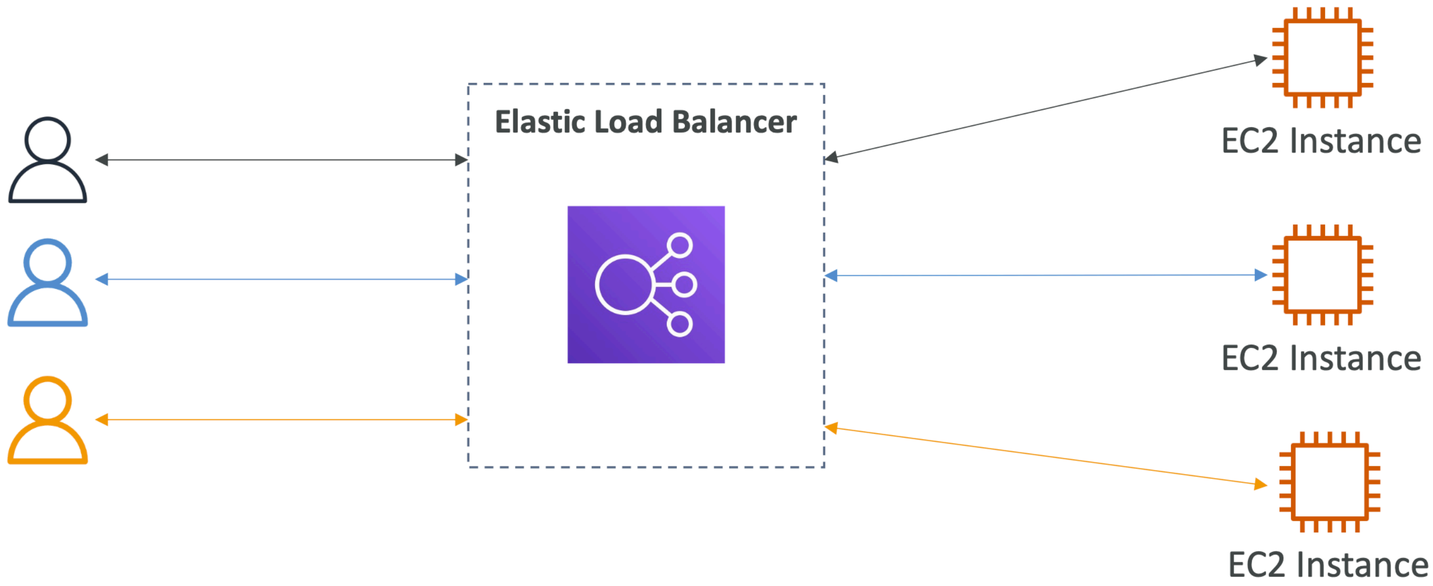
- Elastic IP addresses reflect a poor architectural decision
- Leverage DNS name instead of an elastic IP address
- Leverage Load balancers for exposing services

Load Balancer

Basics

Load Balances are servers that forward traffic to multiple servers (e.g., EC2 instances) downstream

.



Load Balancer

Basics

- Spread load across multiple downstream instances
- Expose a single point of access (DNS) to your application
- Seamlessly handle failures of downstream instances
- Do regular health checks to your instances
- Provide SSL termination (HTTPS) for your websites
- Enforce stickiness with cookies
- High availability across zones
- Separate public traffic from private traffic

====
LLB = Local Load Balancer is a load balancer of servers
GLB = Global Load Balancer is a load balancer of LLBs

===
ELB = AWS implementation of GLB + LLB

Load Balancer

Why use ELB?

- An Elastic Load Balancer is a managed load balancer
- AWS guarantees that it will be working
- AWS takes care of upgrades, maintenance, high availability
- AWS provides only a few configuration knobs

Types of ELBs:

- Classic LB = LB any network port (22, 80, 443, 5555)
- Application LB = (cloud) 80 (http) /443 (https) = Web LB = 80/443
- Network LB = is a new type of Classic LB
- Gateway LB = meant for virtual appliances

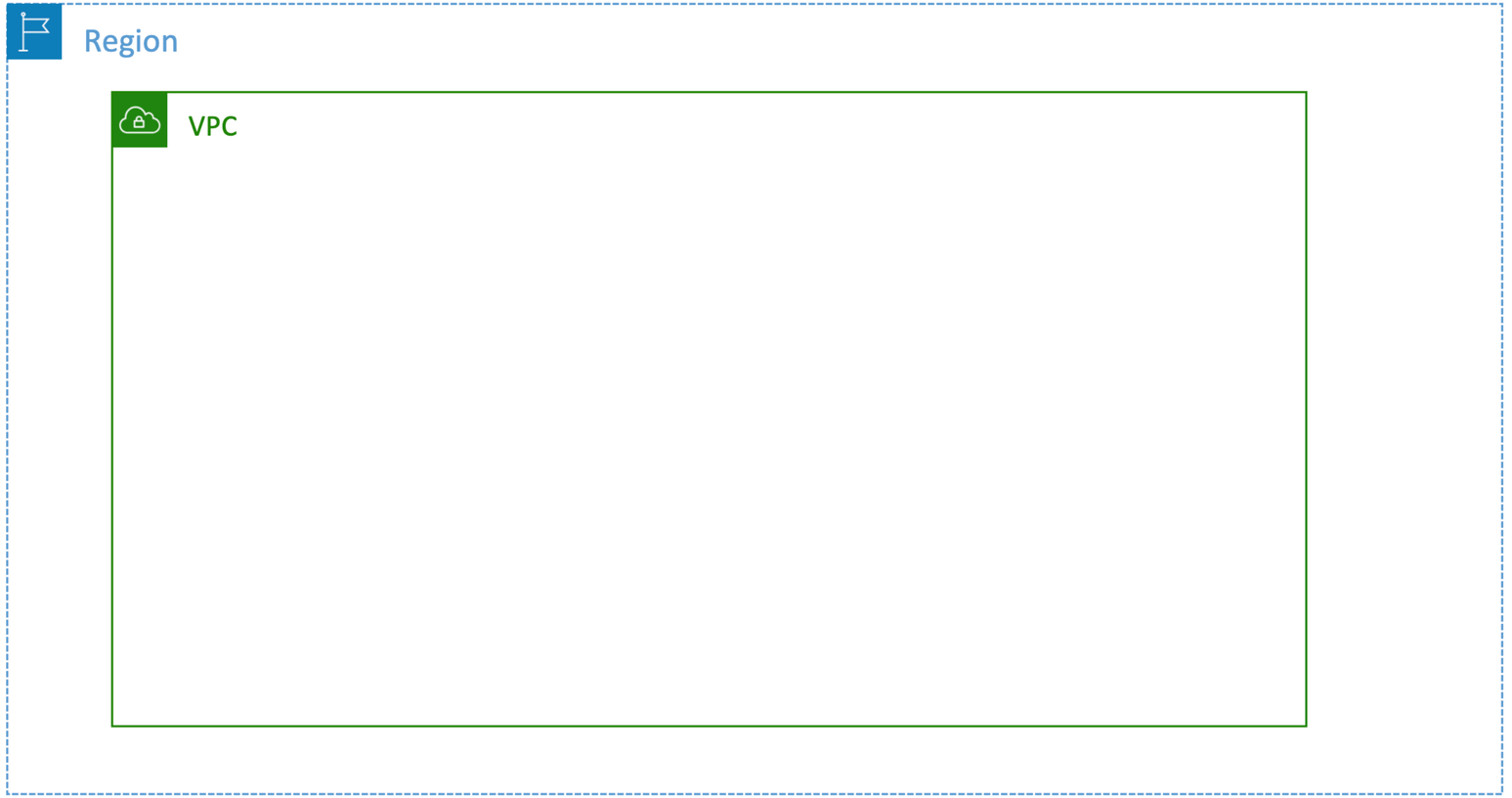
Virtual Private Cloud

Cloud Data Center

- All new AWS accounts have a default VPC
- New EC2 instances are launched into the default VPC if no subnet is specified
- Default VPC has Internet connectivity and all EC2 instances inside it have public IPv4 addresses
- We also get a public and a private IPv4 DNS names

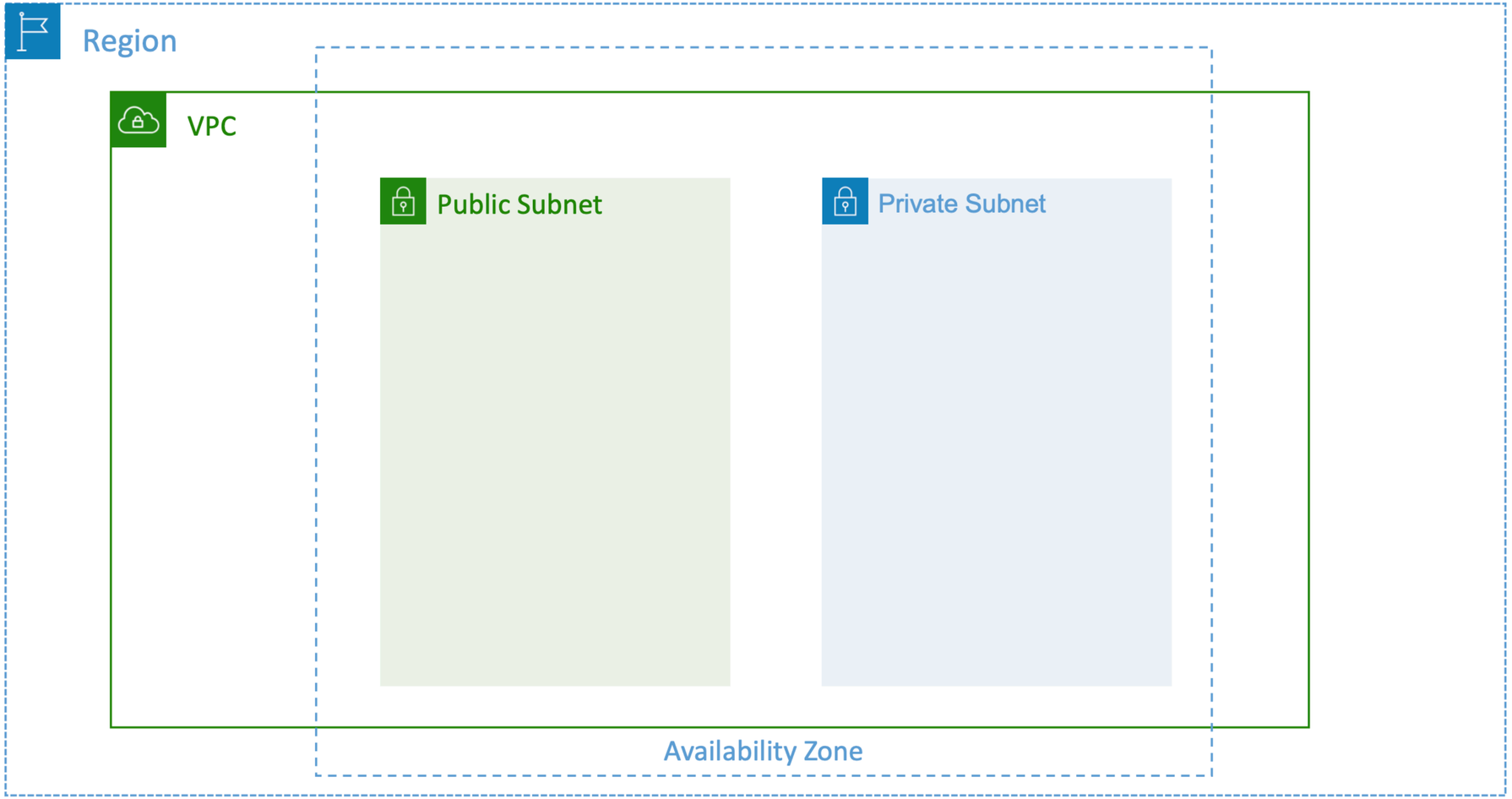
Virtual Private Cloud

Hands-on



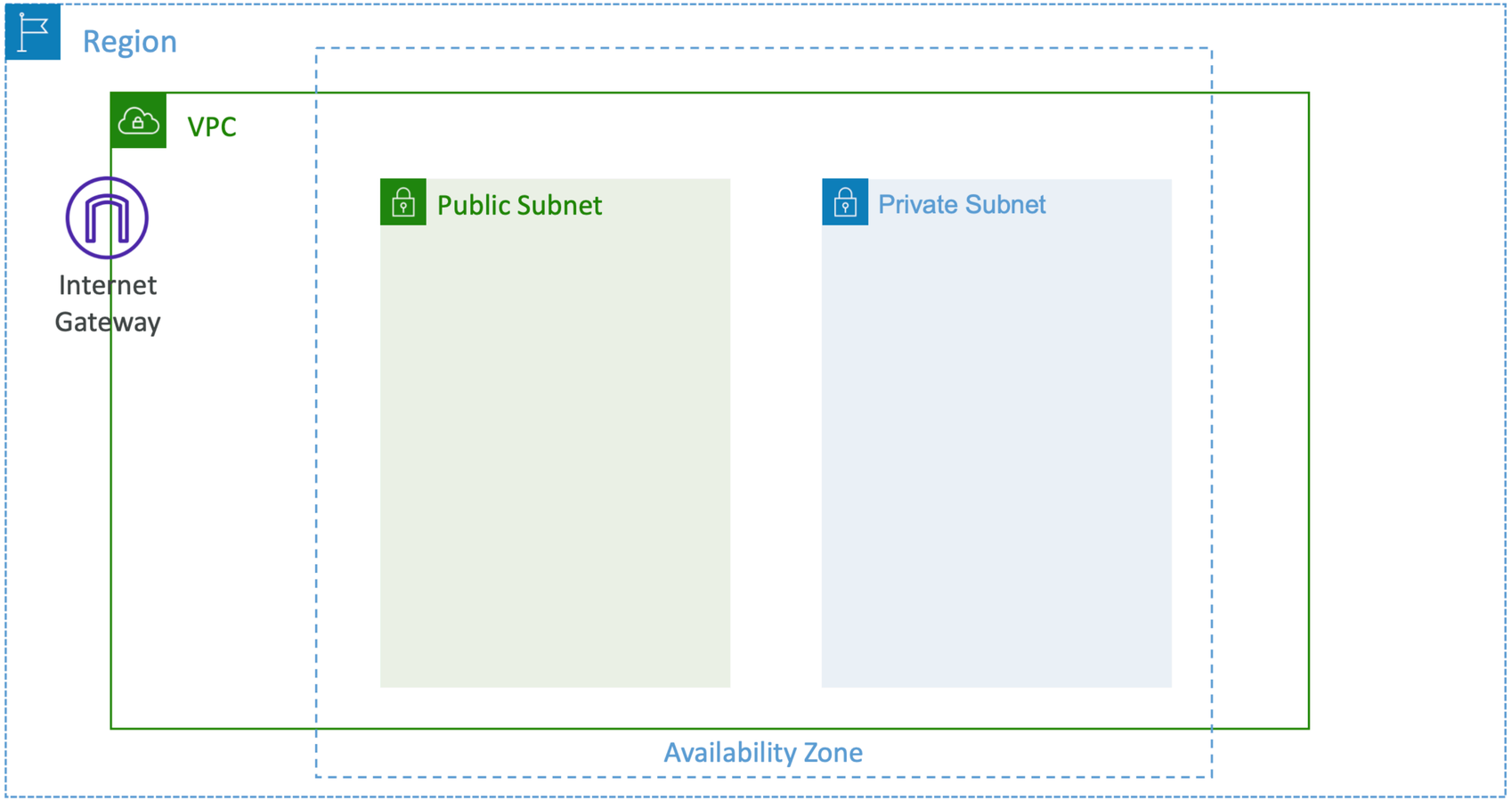
Virtual Private Cloud

Add Subnets



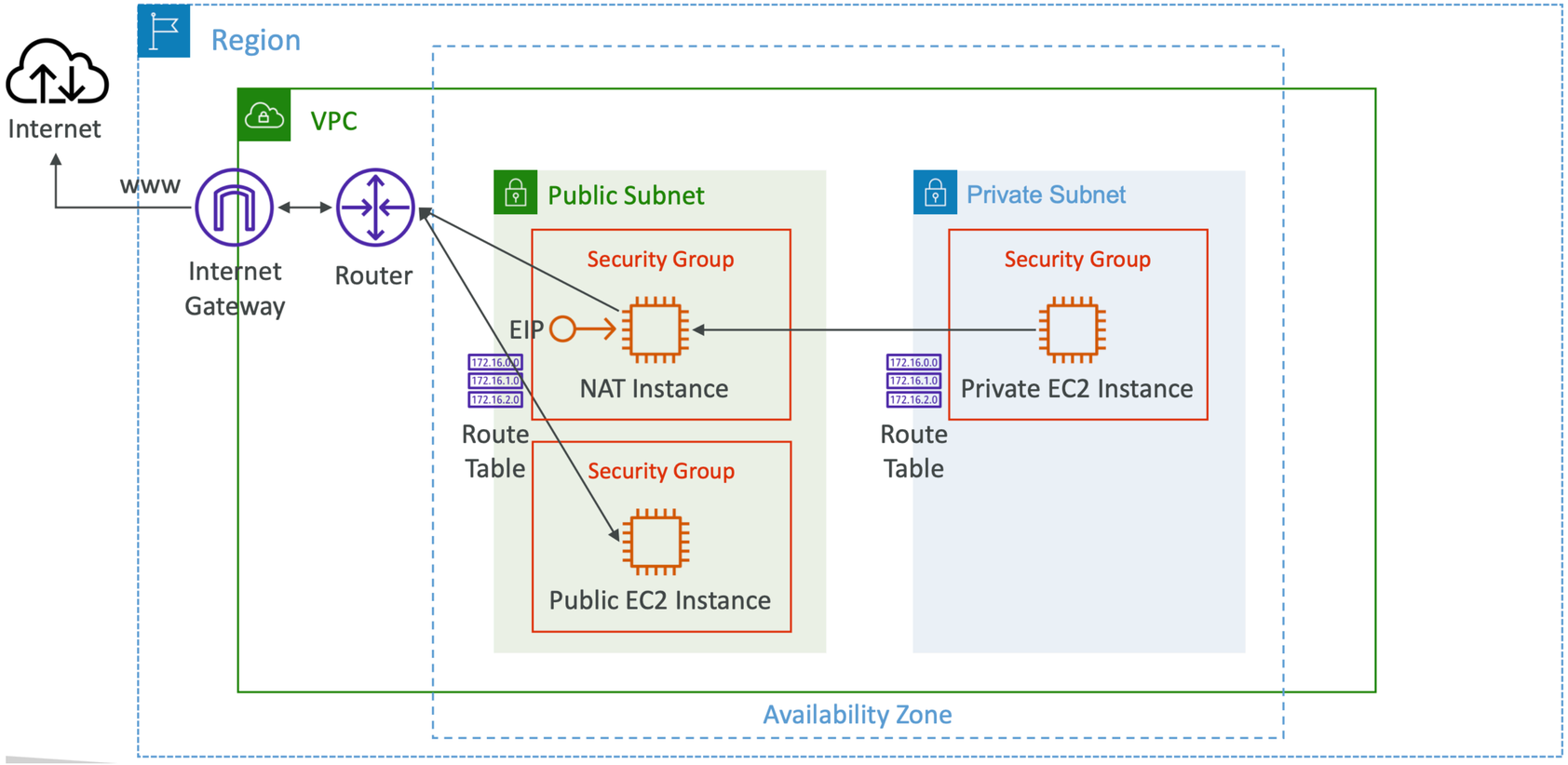
Virtual Private Cloud

Add Internet Gateway (IGW)



Virtual Private Cloud

Add Hosts & Subnets



IAM

Identity and Access Management

IAM

Basics

- IAM = Identity and Access Management
- IAM is generally a Global service.
- Root account created by default
- You should not use the root account for normal operations.
- Users are people within your organization
- Groups only contain users, not other groups
- Users can belong to multiple groups

MFA

Multi-Factor Authentication

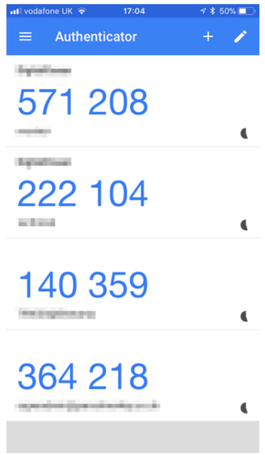
- Protect your Root Accounts and IAM users
- MFA = password *you know* + **security device** *you own*

Primary Benefit: if a password is stolen or hacked, the account is not compromised

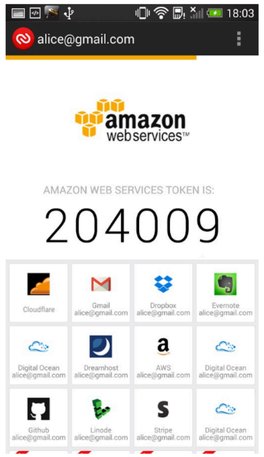
MFA

Multi-Factor Authentication

Virtual MFA device



Google Authenticator
(phone only)



Authy
(multi-device)

Support for multiple tokens on a single device.

Universal 2nd Factor (U2F) Security Key

YubiKey by Yubico (3rd party)

Support for multiple root and IAM users using a single security key

How to access AWS?

Three ways

- AWS Management Console (protected by password + MFA)
- AWS Command Line Interface (CLI): protected by access & secret key
- AWS Software Developer Kit (SDK) - for code: protected by access & secret key

IAM Tools

Account & User Level

- IAM Credentials Report (account-level)
  - a report that lists users and the status of their various credentials

- IAM Access Advisor (user-level)
  - Access advisor shows the service permissions granted to a user
  - You can use this information to revise your policies.

IAM Best Practices

Dos & Don'ts

- Don't use the root account except for AWS account setup
- Assign users to groups and assign permissions to groups
- Create a strong password policy
- Enforce the use of Multi-Factor Authentication (MFA)
- Use roles for giving permissions to AWS services
- Use Access Keys for Programmatic Access (CLI / SDK)
- Audit permissions of your account with the IAM Credentials Report
- Never share IAM users & Access Keys

AWS EC2

AWS Elastic Compute Cloud

EC2 Key Services

Basics

- EC2 Instance: AMI (OS) + Instance Size (CPU + RAM) + EBS Storage + security groups + EC2 User Data
- Security Groups: Firewall attached to the EC2 instance
- EC2 User Data: Script launched at the first start of an instance
- SSH: start a terminal into our EC2 Instances (port 22)
- EC2 Instance Role: link to IAM roles
- Purchasing Options: On-Demand, Reserved, Dedicated Host, Dedicated Instance, Spot

EC2 Key Services

Basics

- Virtual machines for rent => EC2 = Elastic Cloud Compute
- Virtual storage for rent => EBS = Elastic Block Storage
- Virtual load balancers for rent => ELB = Elastic Load Balancer
- Automated Horizontal Scaling => ASG = Auto Scaling Group
- Virtual host-based firewall => Security Groups

EC2 Forensics

Basics

- Any suspicious should not be stopped. Instead, leverage hibernate.
- Stopping will lose the runtime memory image, and hibernate saves the runtime environment to a file.
- Leverage hibernate for long-running processes when memory usage is <150GB.

EC2 Nitro

For advanced users

- It is a combination of dedicated hardware, a lightweight hypervisor, and enhanced security.
- Dedicated cards and chips for faster IO and advanced security
- Leverage it for low-latency service: https://aws.amazon.com/ec2/nitro/

EBS

Basics

- An EBS (Elastic Block Store) Volume is a network drive
- It allows your instances to persist data, even after their termination
- They can only be mounted to one instance at a time
- They are bound to a specific availability zone

EBS

Basics

- It is a network drive (i.e. not a physical drive)
  - It uses the network to communicate the instance, which means there will be latency
  - It can be detached from an EC2 instance and attached to another one quickly

- It's locked to an Availability Zone (AZ)
  - An EBS Volume in us-east-1a cannot be attached to us-east-1b
  - To move a volume across, you first need to snapshot it

- Have a provisioned capacity (size in GBs, and IOPS)
  - You get billed for all the provisioned capacity
  - You can increase the capacity of the drive over time

EBS

Encrypted EBS

- When you create an **encrypted EBS** volume, you get the following:
  - Data at rest is encrypted inside the volume
  - All snapshots are encrypted
  - All volumes created from the snapshot are encrypted
- Encryption and decryption are handled transparently
- Encryption has a minimal impact on latency
- EBS Encryption leverages keys from KMS (AES-256)
- Copying an unencrypted snapshot allows encryption

AMI

Basics

- AMI = Amazon Machine Image
- AMI is a customization of an EC2 instance
  - You add your own software, configuration, operating system, monitoring...
  - Faster boot/configuration time because all your software is pre-packaged
- AMI is built for a specific region and can be copied across regions

Security Groups

Basics

- Security Groups are the fundamental to network security in AWS
- They control how traffic is allowed into or out of our EC2 Instances.
- Security groups only contain "ALLOW" rules.
- Security groups rules can reference by IP or by other security group ID.

Security Groups

What do they do?

- Access to the Host's network ports
- Authorized IP ranges – IPv4 and IPv6
- Control host's inbound network traffic
- Control host's outbound network traffic

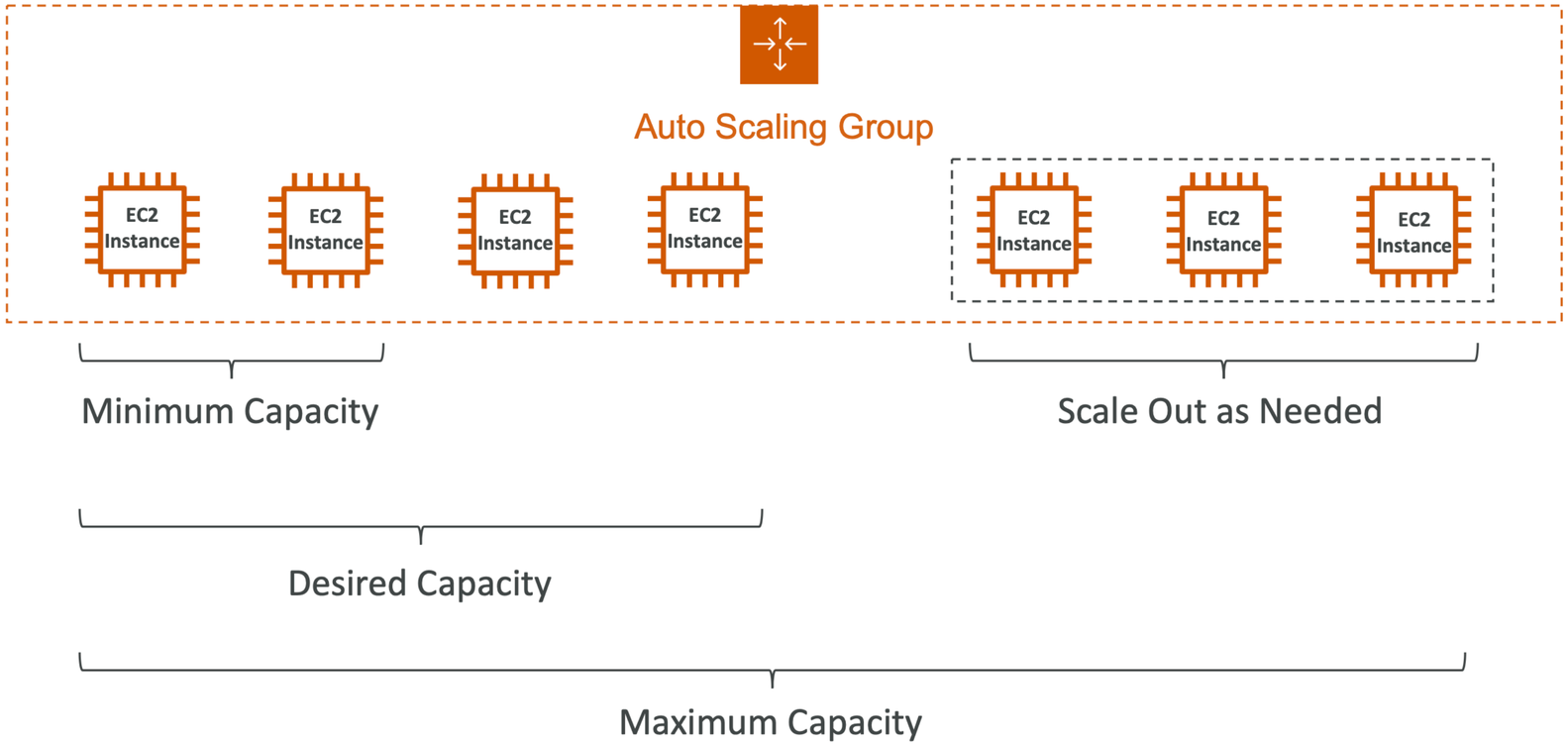
Security Groups

What do they do?

- Security Groups (SG) can be attached to multiple instances
- SG is locked down to a region / VPC combination
- Does live "outside" the EC2 – if traffic is blocked, the EC2 instance won't see it
- It's good to maintain one separate security group for SSH and RDP access
- If your application is not accessible (time out), it is a security group issue.
- If your application gives, a "connection refused" error, it's an application error.
- All inbound traffic is blocked by default
- All outbound traffic is authorized by default

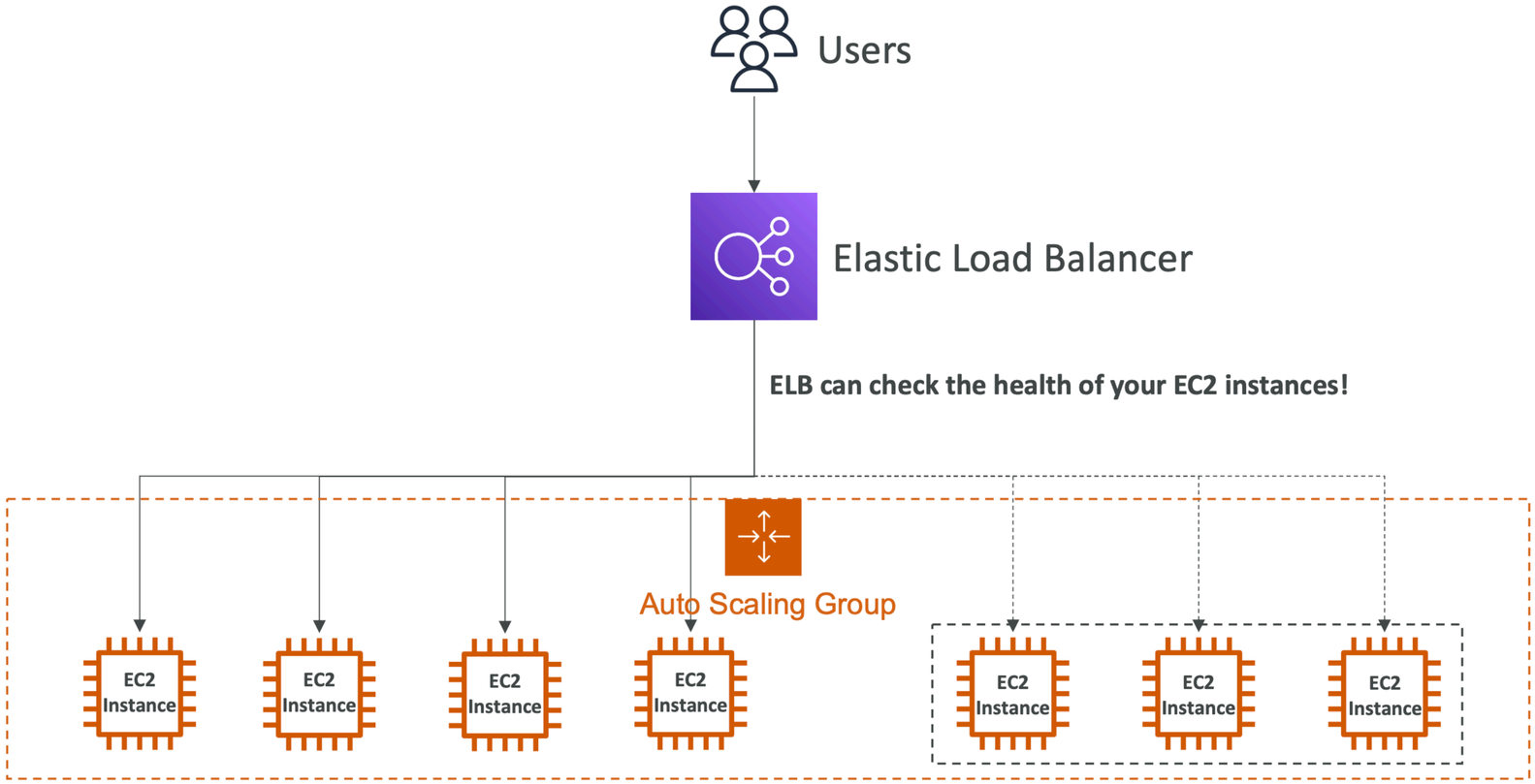
Auto Scaling Group (ASG)

What do they do?



ASG /w ELB

What do they do?



AWS S3

AWS Simple Storage Service

AWS S3 Overview

Basic

- Amazon S3 allows people to store objects (files) in “buckets” (directories)
- Buckets must have a globally unique name
- Buckets are defined at the region level
- Objects (files) have a Key
- The key is the FULL path:
  - `s3://my-bucket/my_file.txt`
  - `s3://my-bucket/my_folder1/another_folder/my_file.txt`
- The key is composed of prefix + object name
  - `s3://my-bucket/my_folder1/another_folder/my_file.txt`
- There’s no concept of “directories” within buckets

AWS S3 Overview

Versioning

- S3 supports versioning at the bucket level.
- The same key overwrite will increment the "version": 1, 2, 3…
- It is best practice to version your buckets
  - Protect against unintended deletes (ability to restore a version)
  - Easy roll back to the previous version

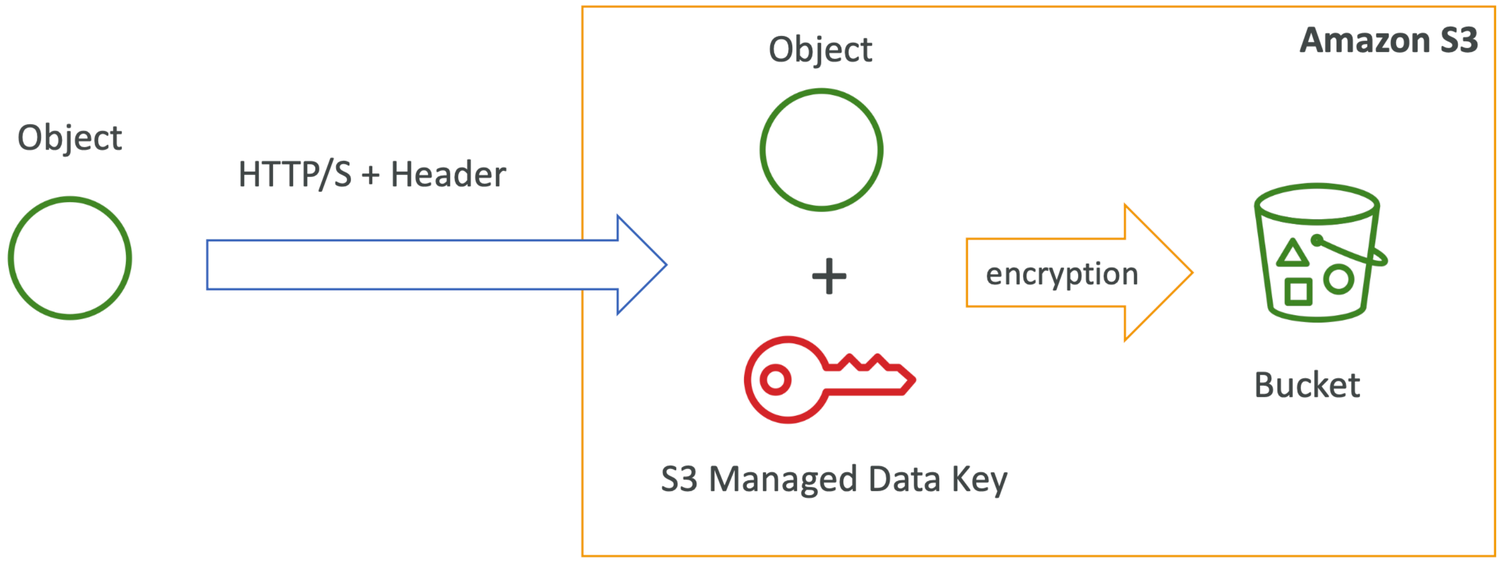
AWS S3 Overview

4 Types of Encryption

- Server Side Encryption (SSE)-S3: encrypts S3 objects using keys handled & managed by AWS
- SSE-KMS: leverage AWS Key Management Service to manage encryption keys
- SSE-Customer (C): customer can own encryption keys
- Client-Side Encryption

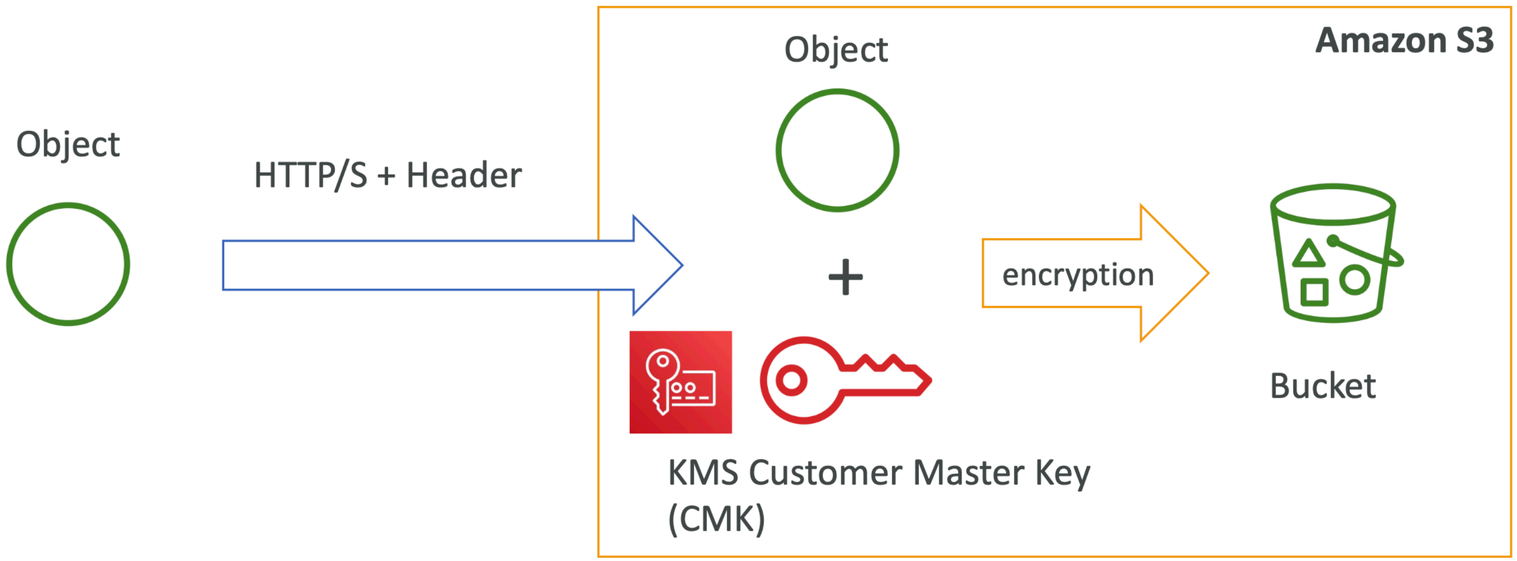
AWS S3 Overview

SSE-S3



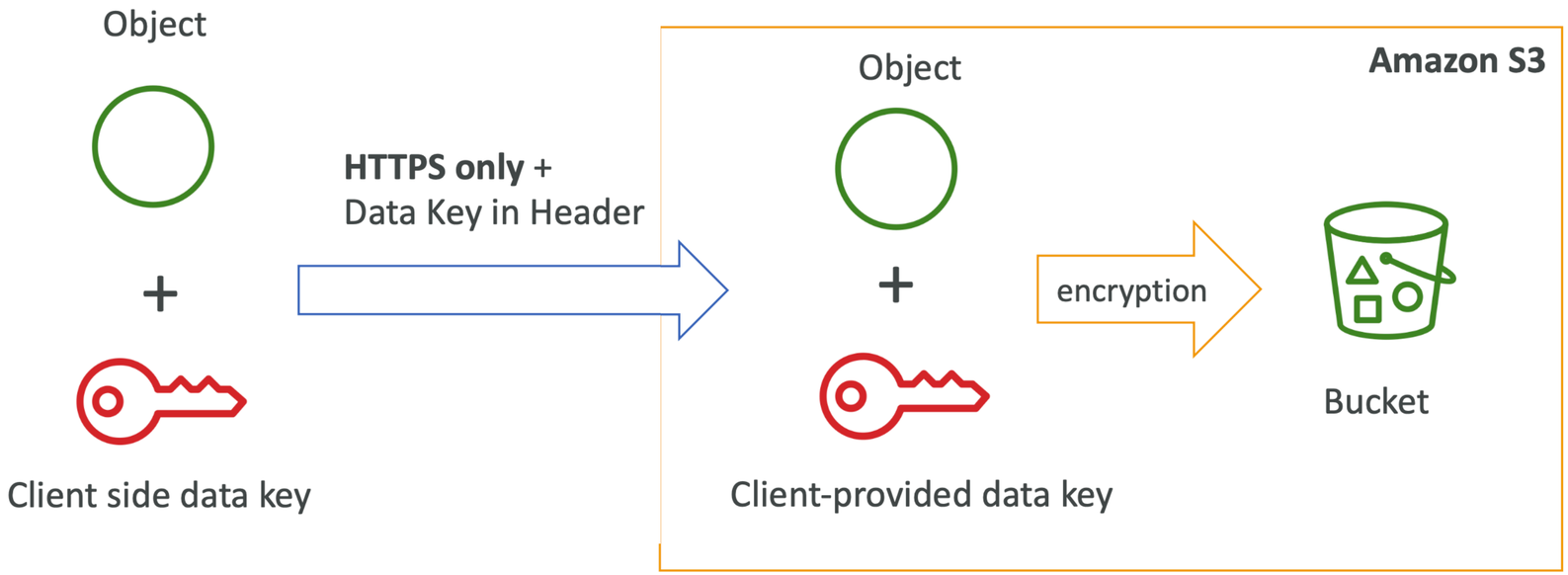
AWS S3 Overview

SSE-KMS



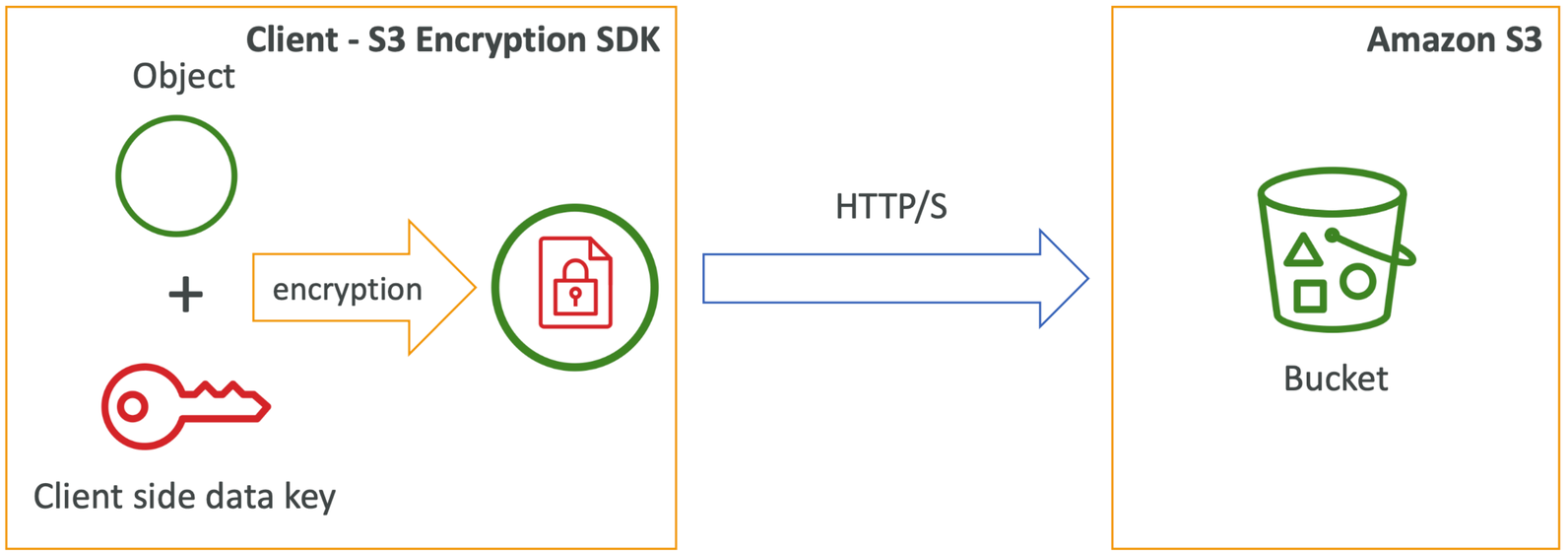
AWS S3 Overview

SSE-C



AWS S3 Overview

Client-Side Encryption



AWS S3 Overview

S3 Web Service

- Amazon S3 exposes:
  - HTTP endpoint: non encrypted
  - HTTPS endpoint: encryption in flight
- HTTPS is mandatory for SSE-C
- Encryption in flight is also called SSL /TLS

AWS S3 Overview

S3 Permissions

- User-based
  - IAM policies - which API calls should be allowed for a specific user from IAM console
- Resource-Based
  - Bucket Policies - bucket-wide rules from the S3 console - allows cross-account
  - Object Access Control List (ACL) – finer grain
  - Bucket Access Control List (ACL) – less common

AWS S3 Overview

Shared Responsibility

- AWS responsibility:
  - Guarantee you get unlimited storage
  - Guarantee you get encryption
  - Ensure separation of the data between different customers
  - Ensure AWS employees can’t access your data

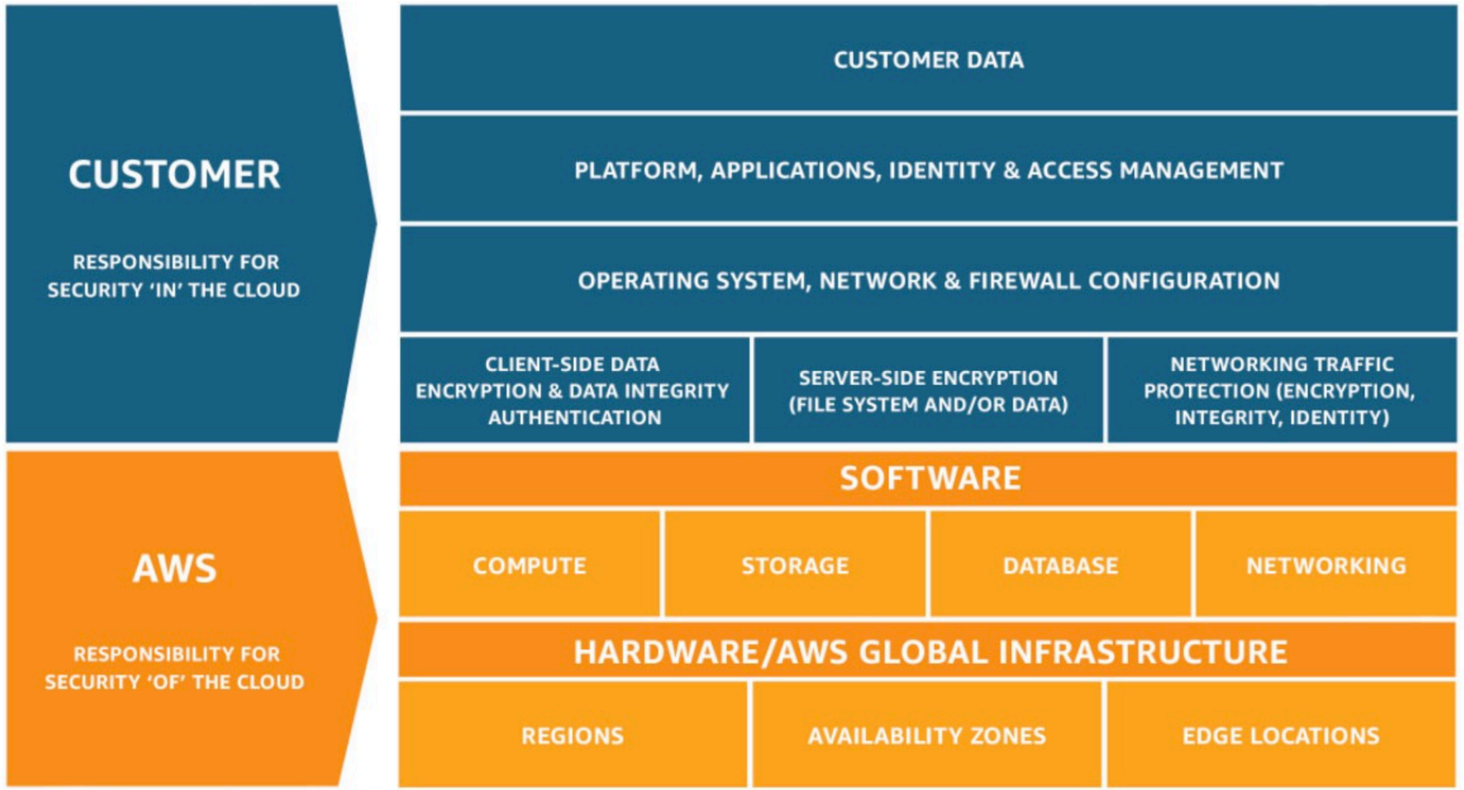
- Your responsibility:
  - Bucket configuration
  - Bucket policy / public setting
  - IAM user and roles
  - Enabling encryption

Security Services

AWS Perspective

Shared Responsibility

https://aws.amazon.com/compliance/shared-responsibility-model/



AWS Inspector

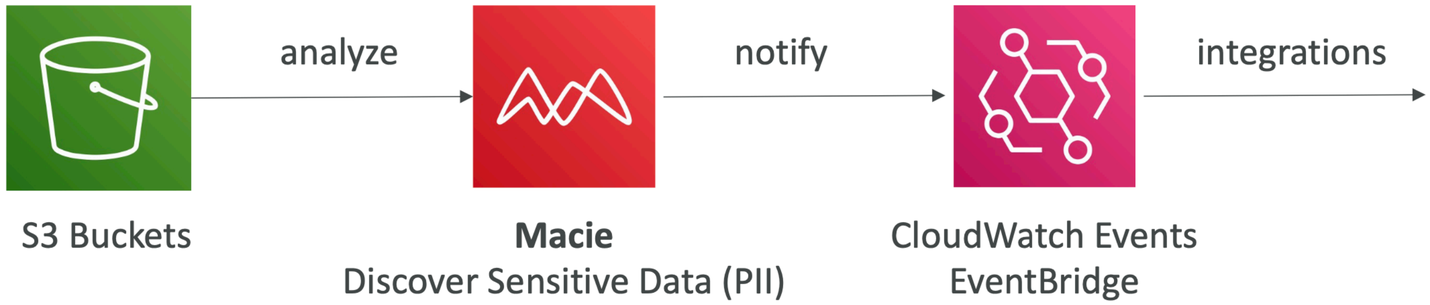
Automated Security Assessments for EC2 Instances and Containers

- For EC2 instances
  - Leveraging the AWS System Manager (SSM)
  - Analyze against unintended network accessibility
  - Analyze the running OS against known vulnerabilities
- For Containers push to Amazon ECR
  - Assessment of containers as they are pushed
- Reporting & integration with AWS Security Hub
- Send findings to Amazon Event Bridge

AWS Macie

Data Security

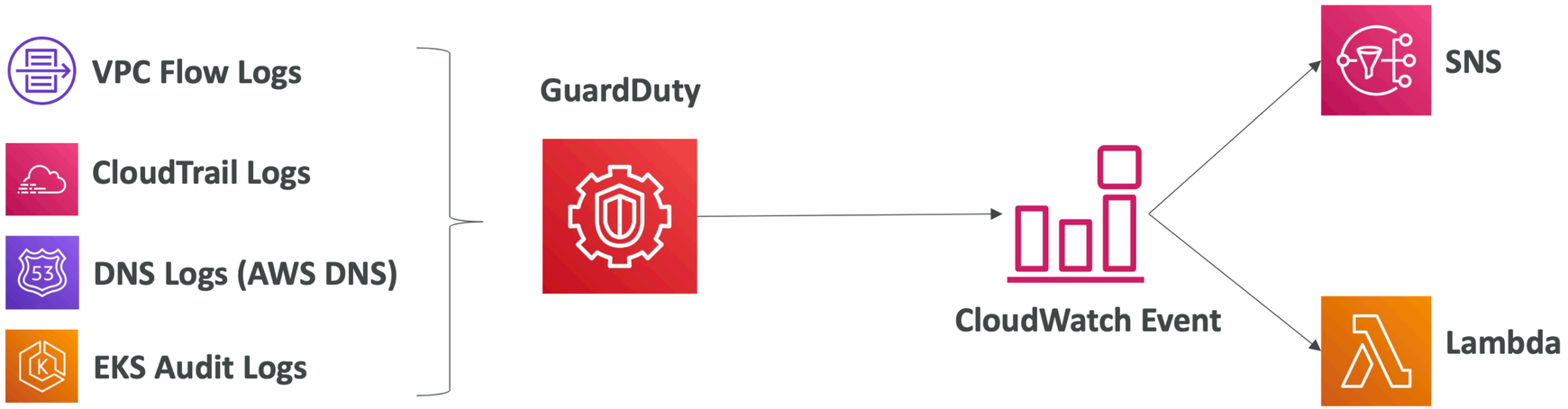
- Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
- Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII)



AWS GuardDuty

Threat Intelligence & Machine Learning based Security

- Intelligent Threat discovery to Protect AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- Integrates with CloudWatch Event rules for alerting



AWS Shield

Denial of Service (DoS) Protection

- **AWS Shield Standard:**
  - Free service that is activated for every AWS customer
  - Provides protection from attacks such as SYN/UDP Floods, Reflection attacks, and other layers 3/layer 4 attacks

- **AWS Shield Advanced:**
  - Optional Distributed DoS mitigation service
  - Protect against more sophisticated attacks on Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, and Route 53
  - 24/7 access to AWS DDoS response team (DRP)
  - Protect against higher fees during usage spikes due to DDoS

AWS WAF

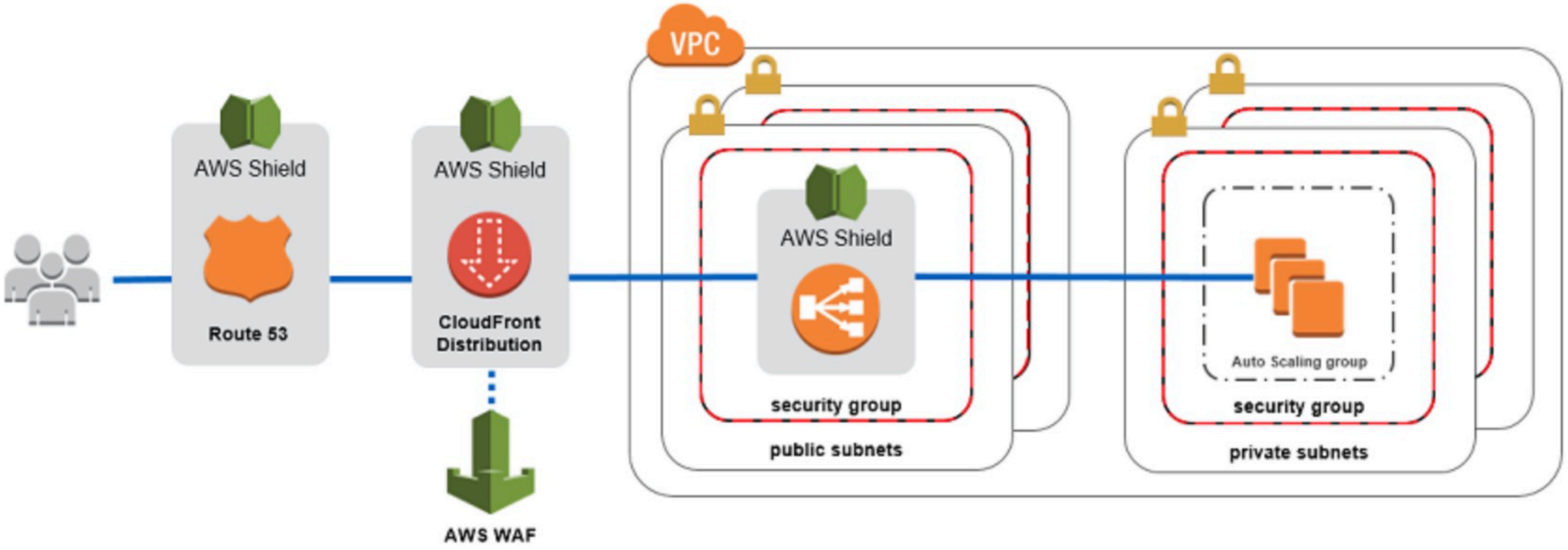
Web Application Firewall

- Protects your web applications from common web exploits (Layer 7)
- Layer 7 is HTTP (vs Layer 4 is TCP)
- Deploy on Application Load Balancer, API Gateway, CloudFront

- Define Web ACL (Web Access Control List):
  - Rules can include: IP addresses, HTTP headers, HTTP body, or URI strings
  - Protects from common attacks - SQL injection and Cross-Site Scripting (XSS)
  - Size constraints, geo-match (block countries)
  - Rate-based rules (to count occurrences of events) – for DDoS protection

DDoS Protection

https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/



What is due?

Homework & Discussions