Workshop #3 - Networking

Last Workshop - Storage

Learning Objectives

- Describe the basic concepts of networking.
- Describe the difference between public and private networking resources.
- Explain a virtual private gateway using a real life scenario.
- Explain a virtual private network (VPN) using a real life scenario.
- Describe the benefit of AWS Direct Connect.
- Describe the benefit of hybrid deployments.
- Describe the layers of security used in an IT strategy.
- Describe the services customers use to interact with the AWS global network.

Virtual Private Cloud (VPC)

VPC's enables you to provision an isolated section of the AWS Cloud.

Everything goes inside a VPC.

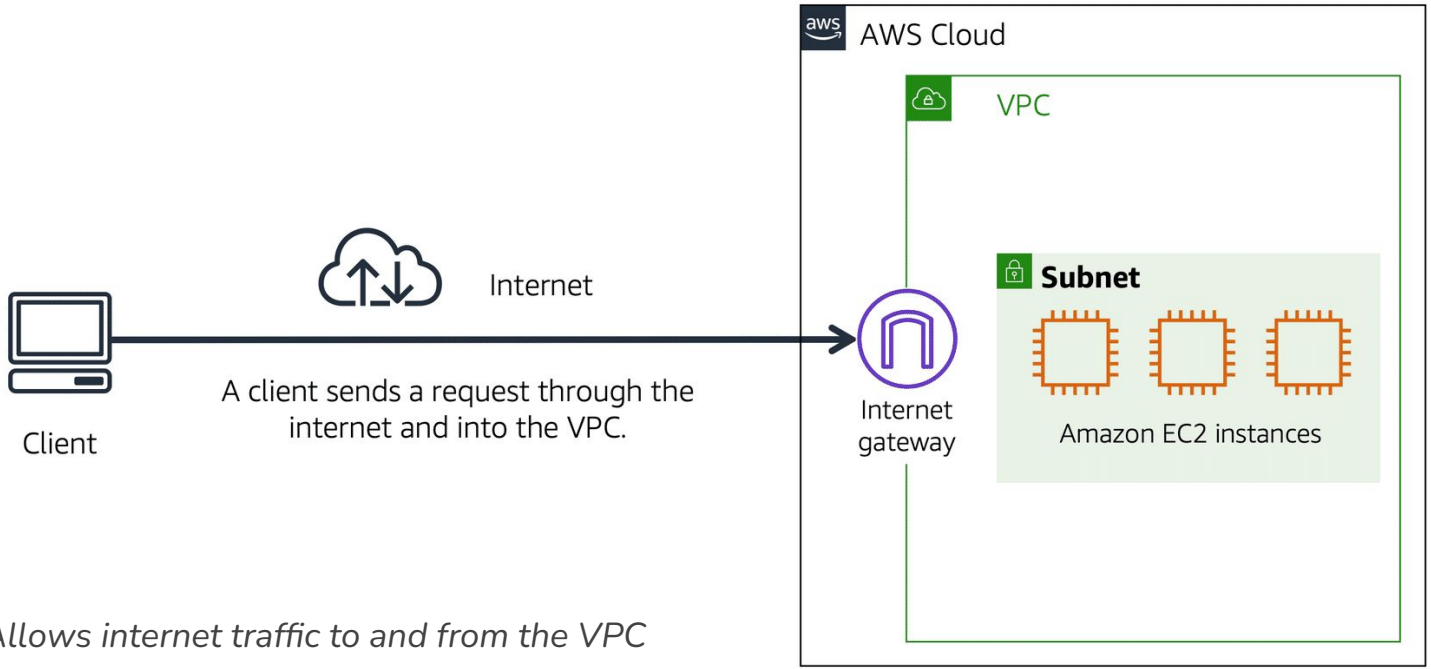
You can control networking using a VPC.

Within a VPC, you can have subnets for fine grained control.

Networking - How you control the connections into and out of your servers

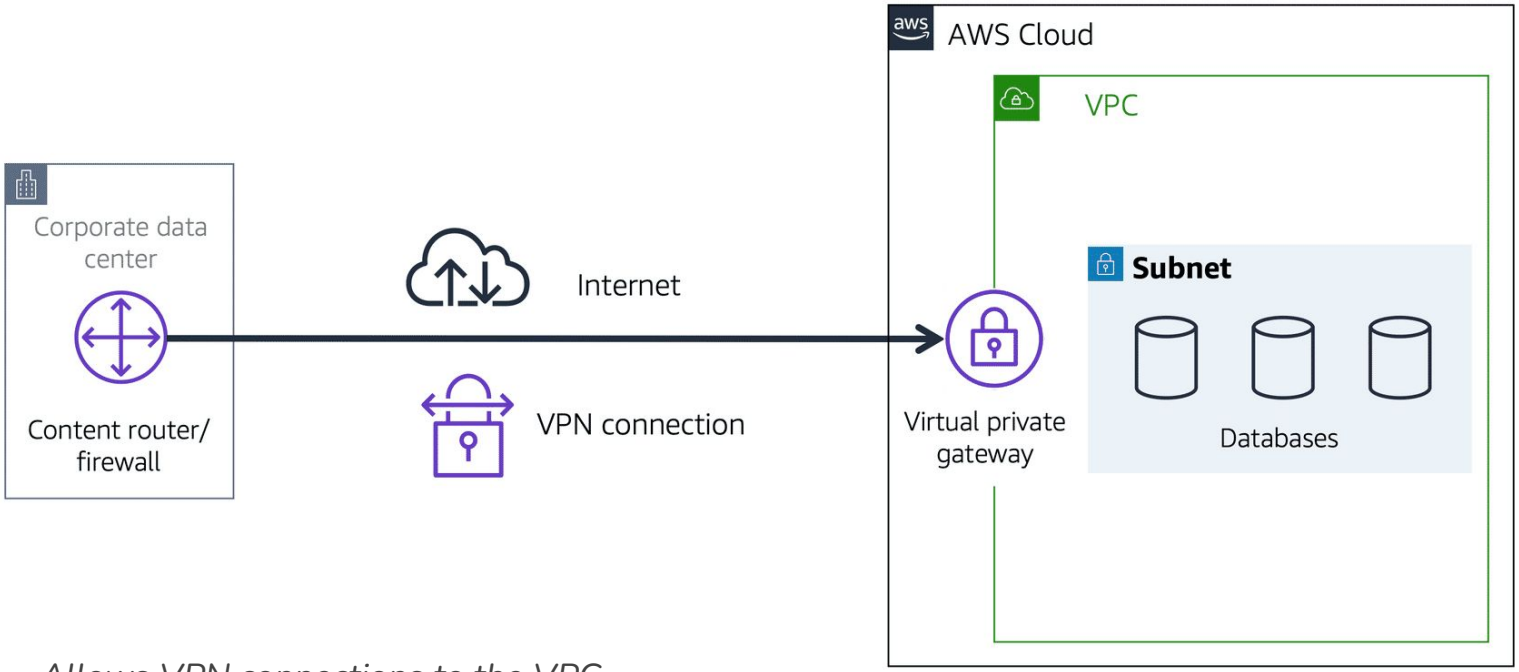

Region 1
VPC Subnet in AZ 1
Amazon EC2
Instance
Amazon EC2
Instance
VPC Subnet in AZ 2
Amazon EC2
Instance
Amazon EC2
Instance
Region 2
VPC Subnet in AZ 1
Amazon EC2
Instance
Amazon EC2
Instance
VPC Subnet in AZ 2
Amazon EC2
Instance
Amazon EC2
Instance

Internet Gateways



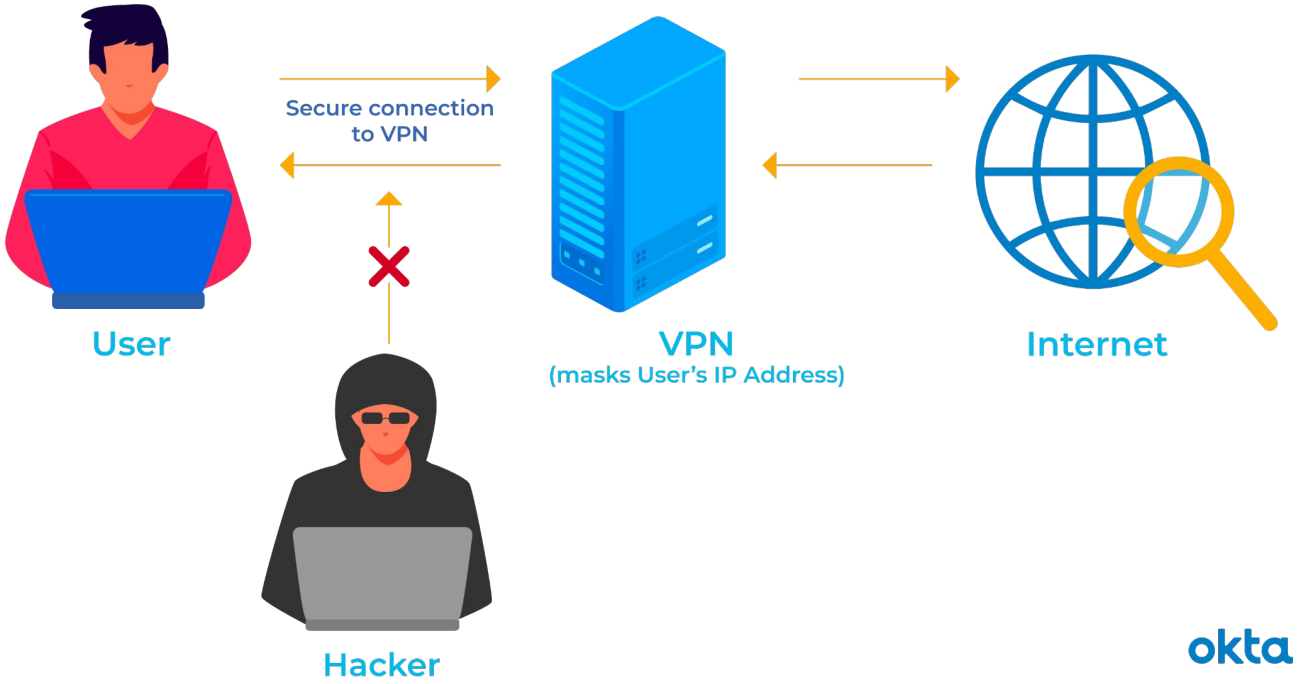
Allows internet traffic to and from the VPC

Virtual Private Gateway



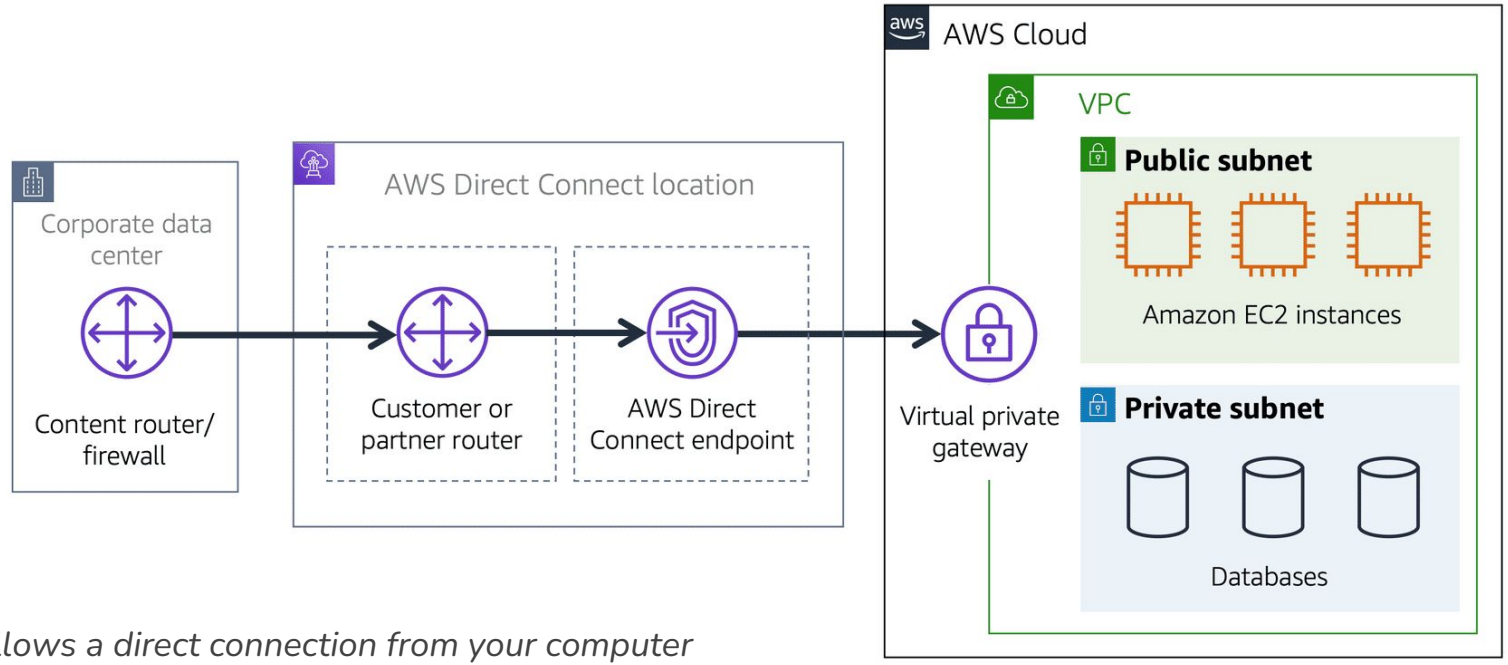
Allows VPN connections to the VPC

What is a VPN?



okta

AWS Direct Connect



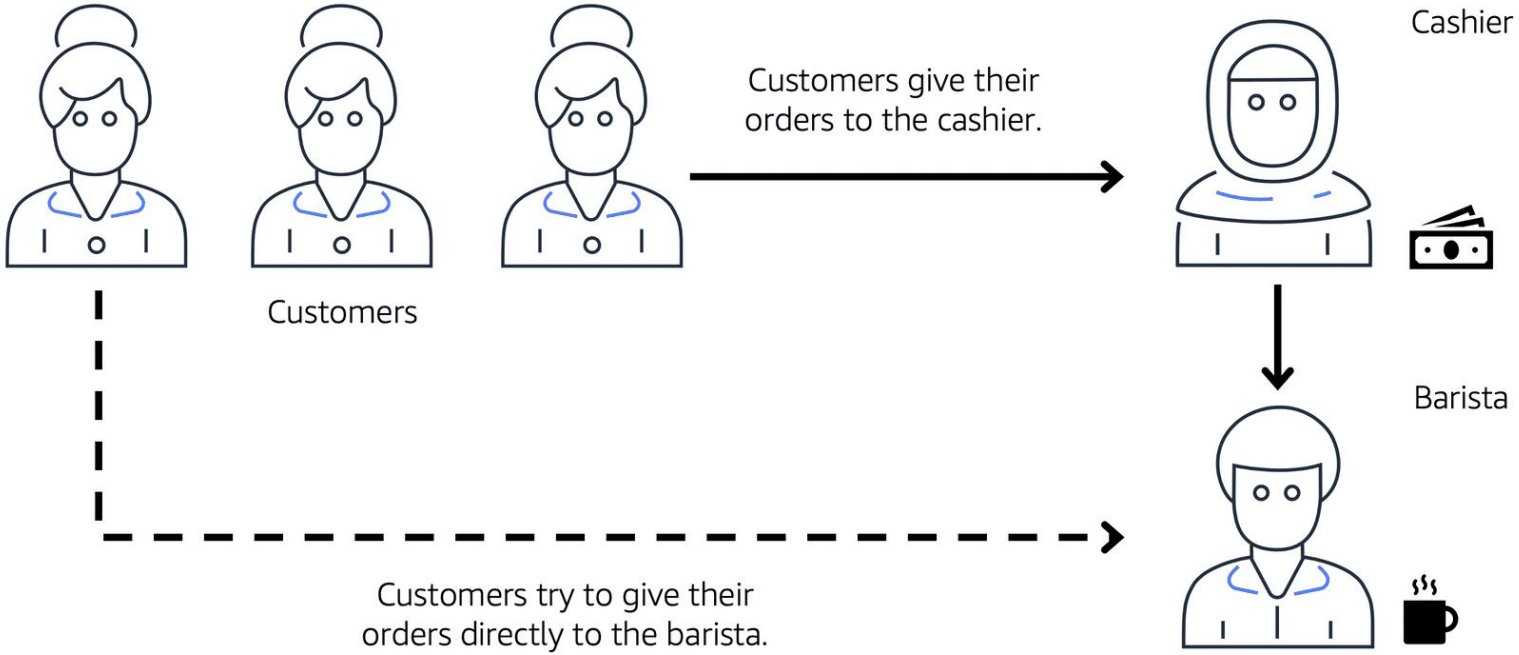
Allows a direct connection from your computer to AWS, without needing to travel the internet

Example Question

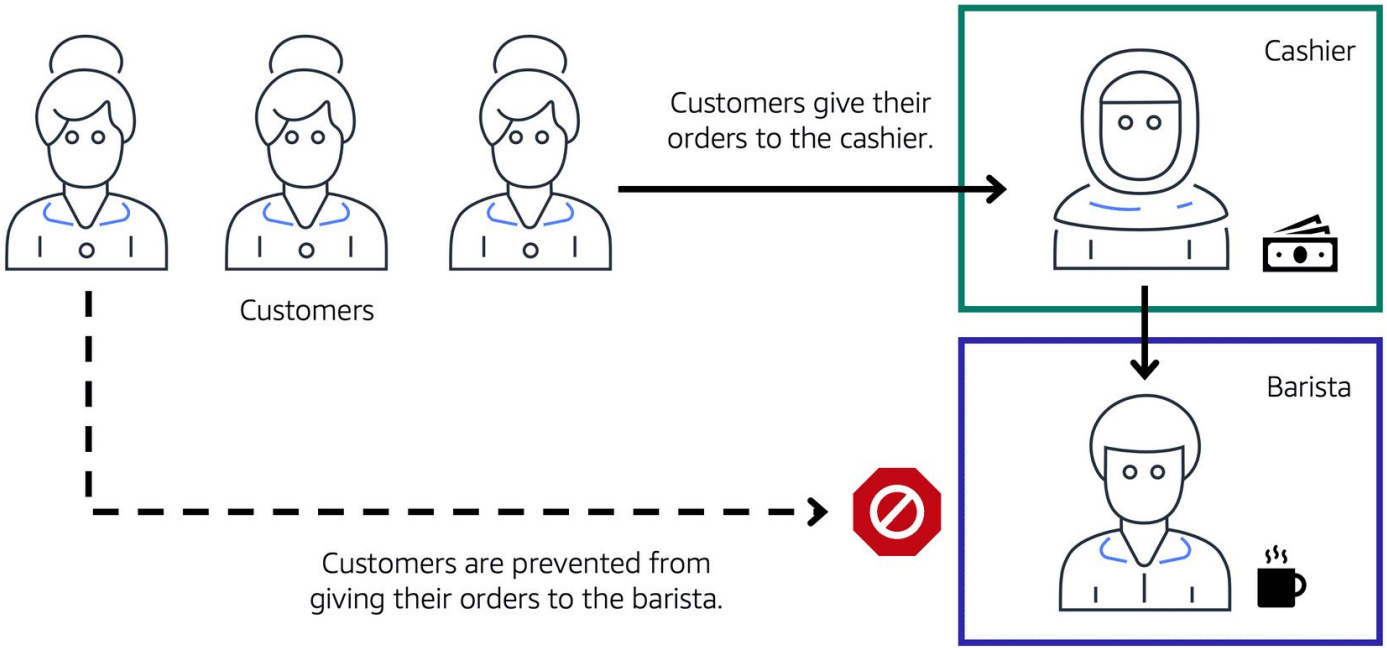
4) Which AWS networking service enables a company to create a virtual network within AWS?

A) AWS Config
B) Amazon Route 53
C) AWS Direct Connect
D) Amazon Virtual Private Cloud (Amazon VPC)

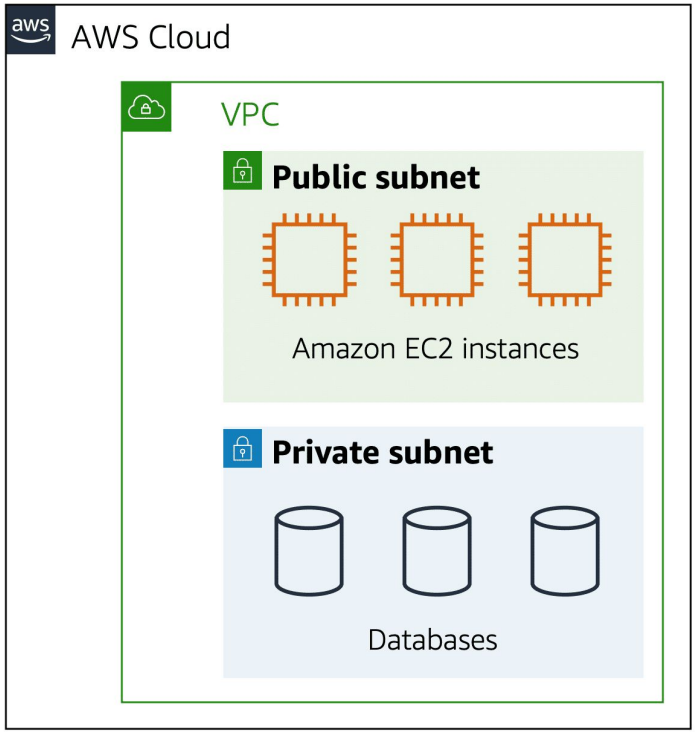
Subnets


Customers give their orders to the cashier.
Cashier
Customers
Barista
Customers try to give their orders directly to the barista.

Subnets


Customers give their orders to the cashier.
Cashier
Customers
Barista
Customers are prevented from giving their orders to the barista.

Subnets



Public Subnets - Contains resources accessible to the public

Private Subnets - Contains resources that should only be accessed privately, like databases. Think private information.

How do we actually control who can enter and who can exit?

2 Ways

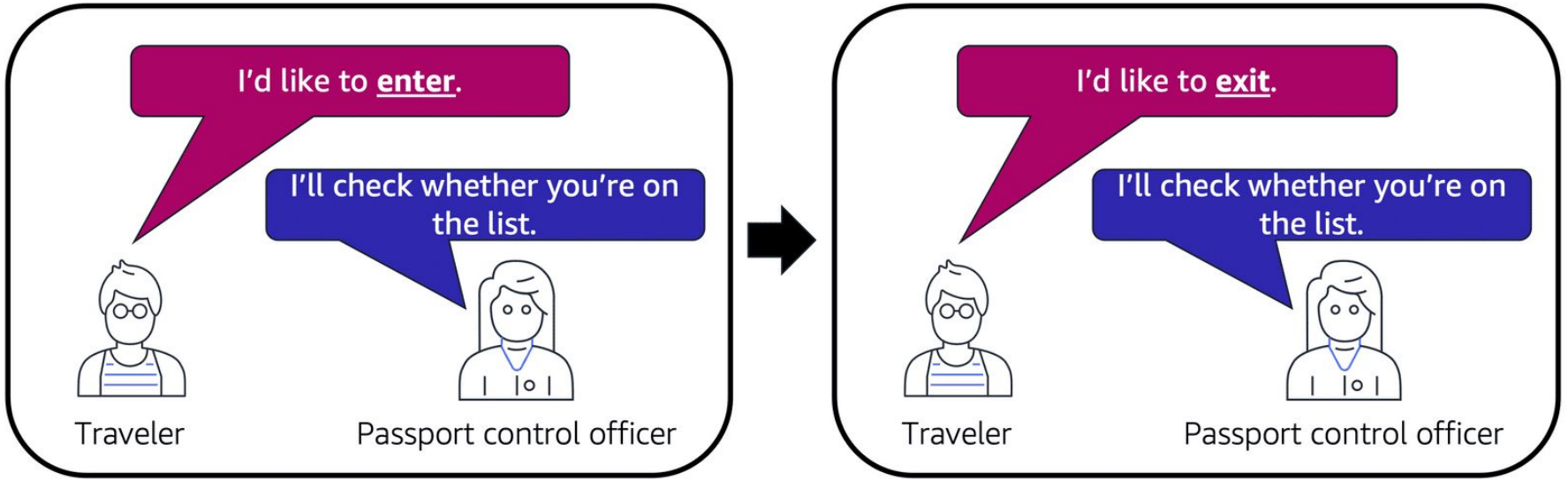
Network access control lists (NACLs)

- Stateless
- You can Allow or Deny
- You can control both inbound and outbound traffic

Security Groups

- Stateful
- You can only Allow
- You can control only inbound and traffic (outbound is done automatically)

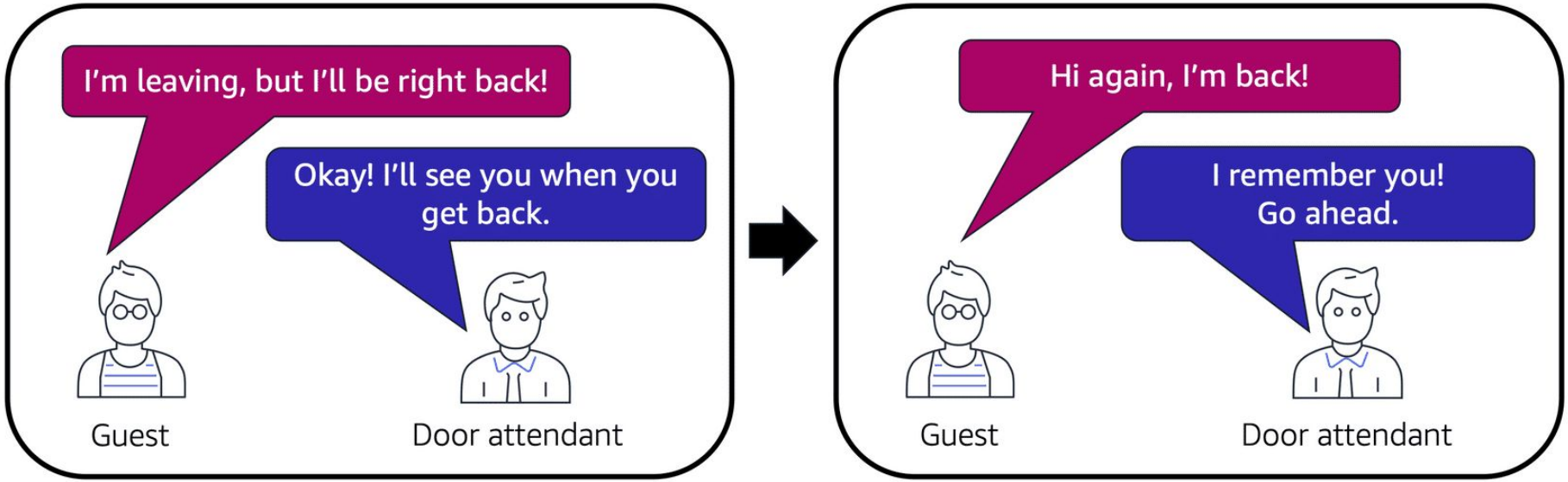
NACLs



Fine-grained control: Allow/Deny, Inbound/Outbound

This is called Stateless

Security Groups



*Can only **Allow** inbound traffic*

This is called Stateful

Recap

Network access control lists (NACLs)

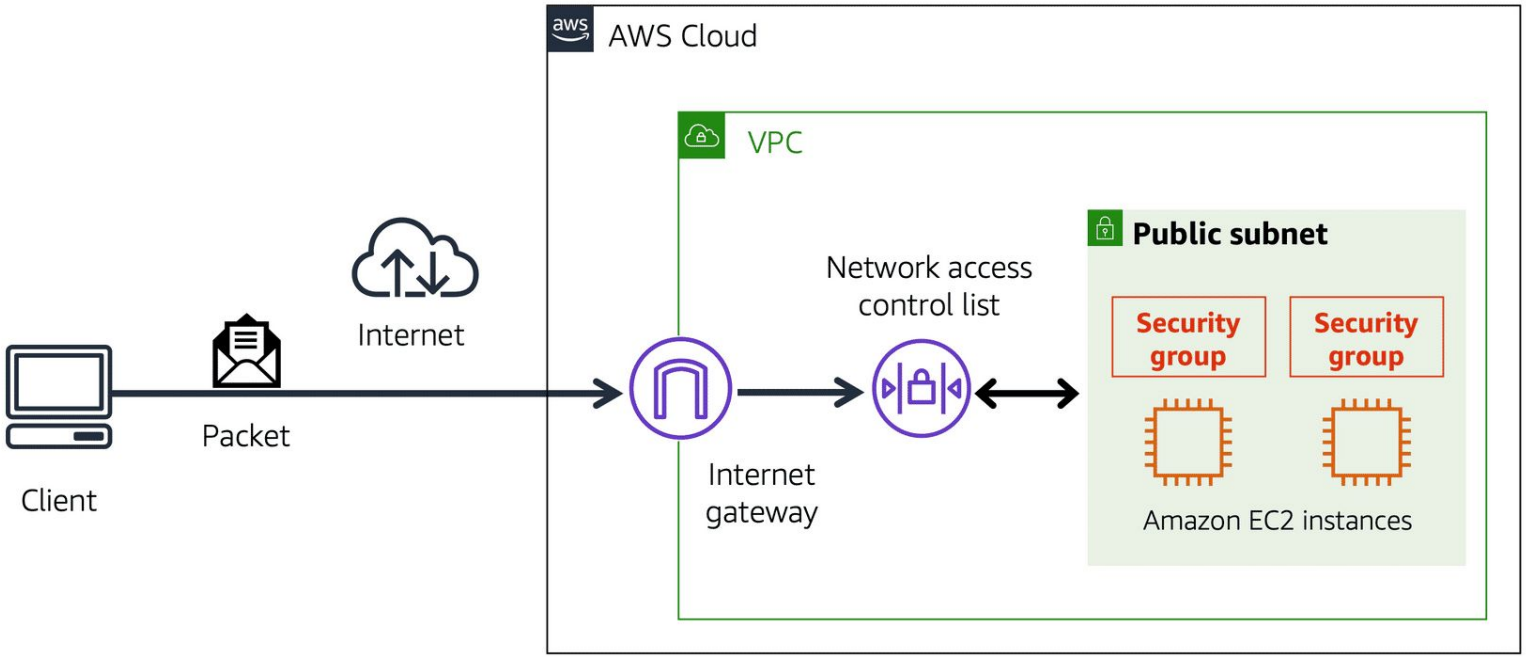
- Stateless
- You can Allow or Deny
- You can control both inbound and outbound traffic

Security Groups

- Stateful
- You can only Allow
- You can control only inbound and traffic (outbound is done automatically)

BOTH NACLs and Security Groups are used to protect a VPC, not one or the other

Recap


AWS Cloud
VPC
Public subnet
Network access control list
Security group
Security group
Internet
Packet
Client
Internet gateway
Amazon EC2 instances

Global Networking

Global Infrastructure Overview

AWS Global Infrastructure is made up of:

- 31 Launched Regions
- 99 Availability Zones
- 450+ Points of Presence
- 32 Local Zones
- 29 Wavelength Zones

Regions

Geographically distinct locations consisting of one or more Availability Zones

Every region is **physically isolated** from every other region in terms of:

- Location
- Power
- Water Supply

Availability Zones

Physical location made up of one or more data center

Datacenter - Secured building containing hundreds of thousands of computers

High Availability is often achieved by running workloads in at least 3 AZs

Points of Presence

Data centers owned by **AWS or a trusted partner** that is utilized by AWS Services for **content delivery or expedited upload**

PoP resources are:

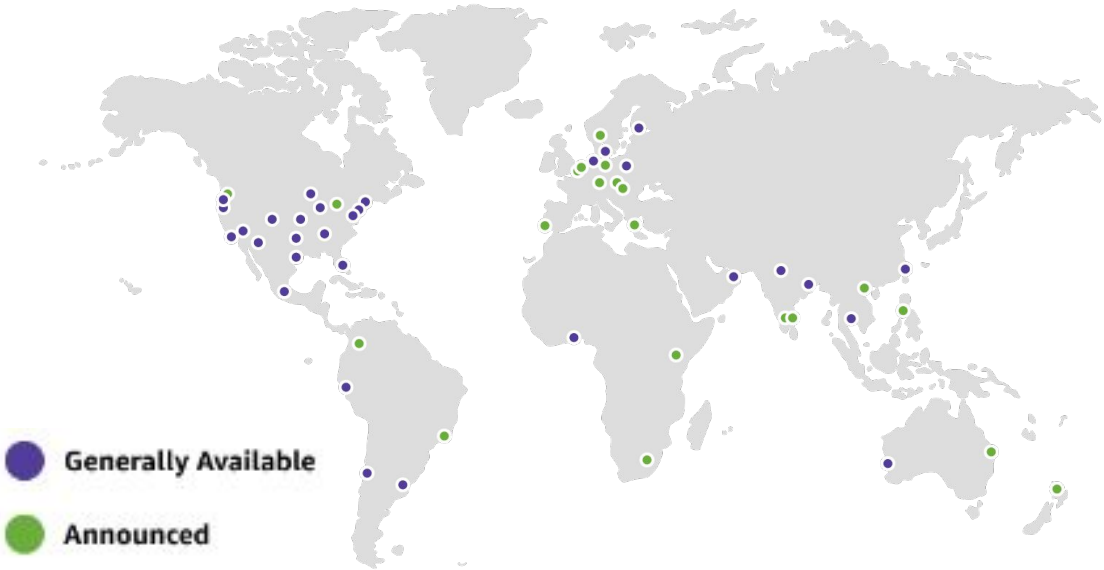
- **Edge Locations**
- **Regional Caches**

Edge Locations - data centers holding caches of popular files (web pages, images, videos), so that delivery distance is reduced and speed is increased

Regional Edge Locations - data centers holding much larger caches of less popular files

Local Zones

Data centers located very close to densely populated areas, providing low latency performance for that area

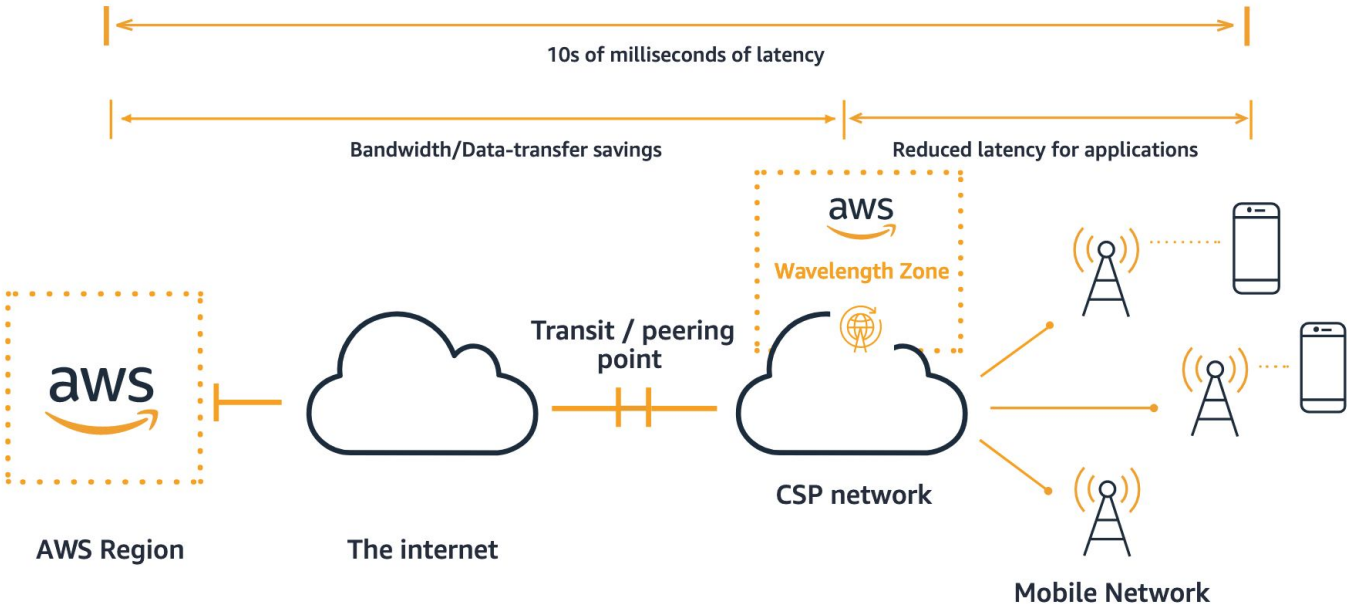


Only specific AWS Services made available:

- EC2 Instance Types
- EVS
- Amazon FSx
- Application Load Balancer
- Amazon VPC

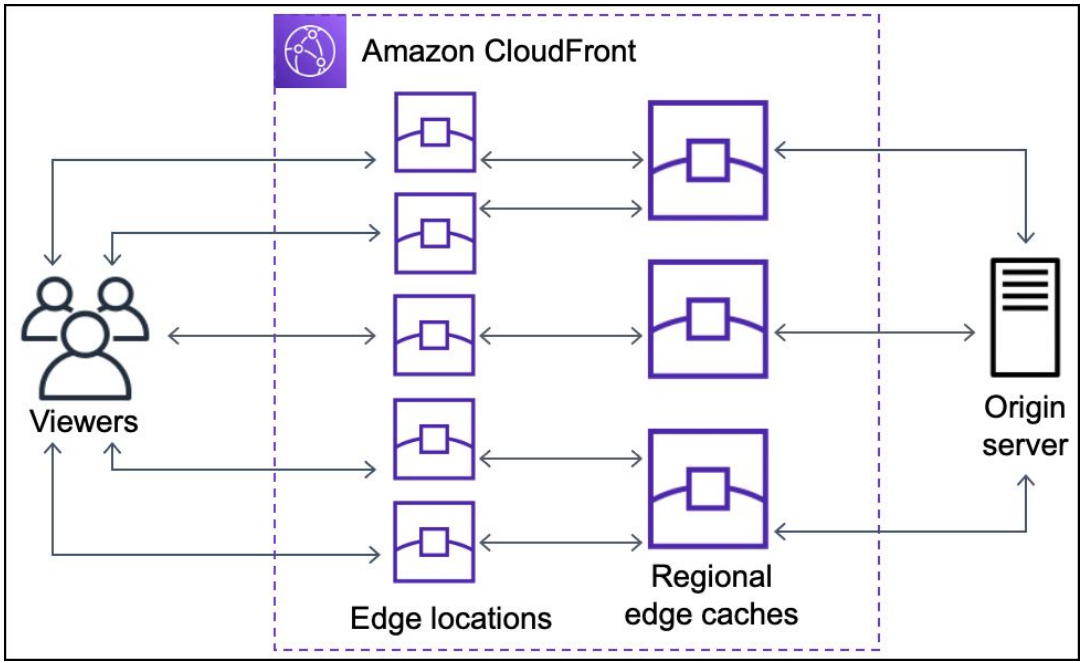
Wavelength Zones

AWS Wavelength Zones allow for ultra-low latency for end users on 5G Networks



CloudFront

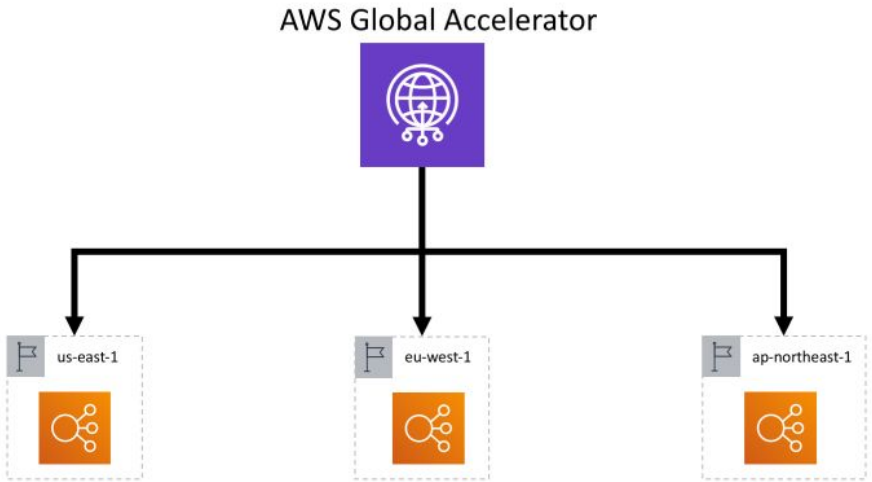
Content Delivery Network (CDN)



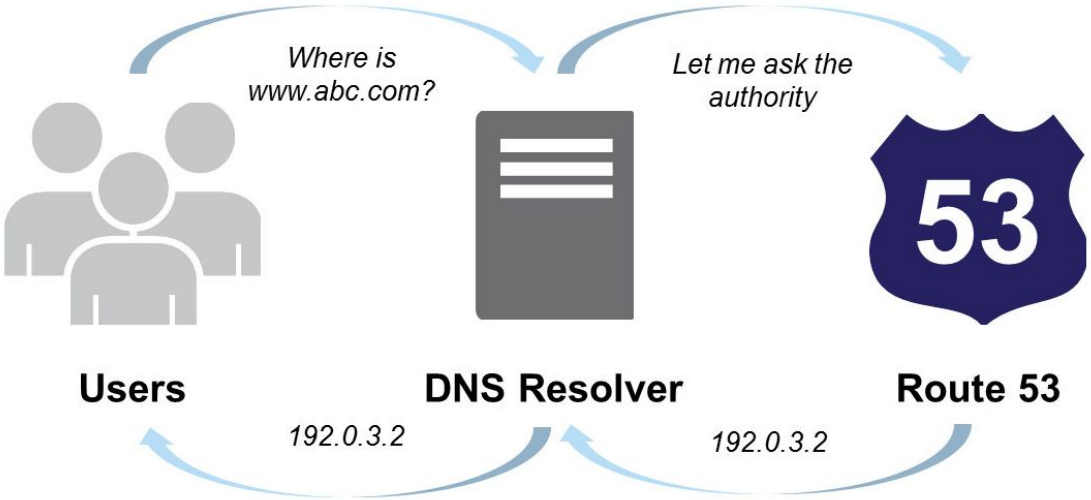
- Routes website requests to the nearest **Edge Location Cache**
- Allows you to choose **origin** as source of cached content
- Caches content from origin to Edge Locations around the world

AWS Global Accelerator

Finds the optimal path from end user to your web-servers



Route 53



Amazon Route 53 is a highly available and scalable **Domain Name System (DNS)** web service.

It connects user requests to internet applications running on AWS or on-premises.

AWS Outposts

What is Data Residency?

The geographic location of where an organization's data resides

What are Compliance Boundaries?

Legal requirements describing where data is allowed to reside

What is Data Sovereignty?

Jurisdictional control over data due to its physical location

AWS Outposts

Physical server rack allowing you to control where your data geographically resides

Example Question

6) Which component of the AWS global infrastructure does Amazon CloudFront use to ensure low-latency delivery?

A) AWS Regions
B) Edge locations
C) Availability Zones
D) Virtual Private Cloud (VPC)

Example Question

6) Which component of the AWS global infrastructure does Amazon CloudFront use to ensure low-latency delivery?

A) AWS Regions
B) Edge locations
C) Availability Zones
D) Virtual Private Cloud (VPC)

Hands-On Demo

Thank You!