module 4: networking

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

▼ *What is VPC?*

Virtual Private Cloud - lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.

▼ *What is VPC usually used for?*

For backend services like databases or application servers.

▼ *What is a subnet?*

It's a public or private grouping of resources - ranges of IP addresses in your VPC.

▼ *What sorts of things can you place in a VPC?*

EC2 instances and ELBs , for example

▼ *What is the point of a subnet?*

It's to control whether the resources are either publicly or privately available.

▼ *Can you control the traffic within a subnet?*

Yes - ex: make it public if the service should be able to reach a public website

▼ *How do you allow traffic from the public internet to flow into and out of your VPC?*

By attaching an Internet Gateway (IGW) or a Virtual Private Gateway (VPGW)
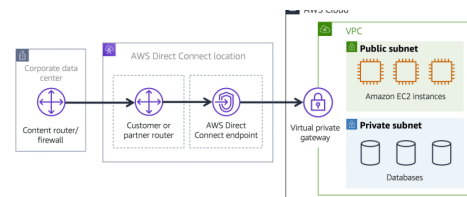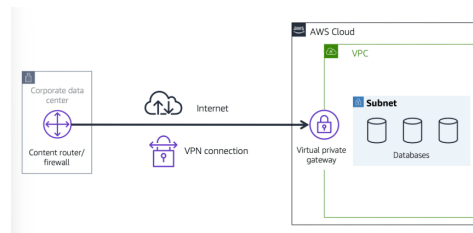
▼ *What is a VPN?*

A Virtual Private Network - private and are encrypted but they still use a regular internet connection that has bandwidth that is being shared by many people using the internet.

▼ *What is AWS Direct Connect?*

It allows you to establish a completely private dedicated fiber - provides a physical line that connects your network to your AWS VPC.
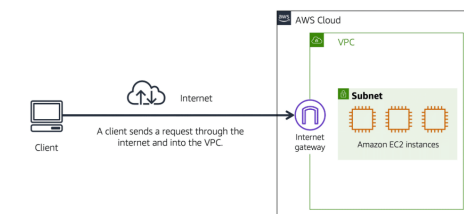
Internet gateway icon attached to a VPC that holds three EC2 instances. An arrow connects the client to the gateway over the internet indicating that the client's request has gained access to the VPC.

▼ *What is the technical reason to use subnets in a VPC?*

To control access to the gateways

▼ *What do public subnets have access to that private subnets don't?*

Internet gateway

▼ *What are packets?*

Messages from the internet

▼ *What is a NACL?*

Network ACL (Access Control List)
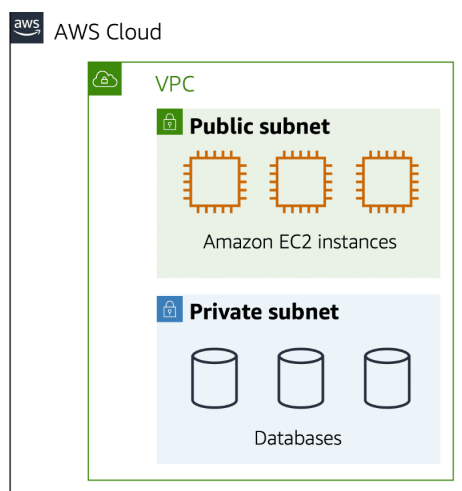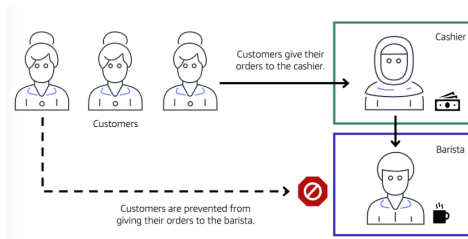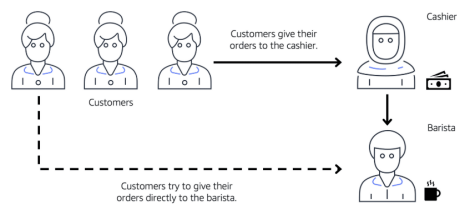
▼ *What is instance level network security?*

It includes security groups that do not allow traffic into the instance at all by default

▼ *What is the difference between security groups and NACLs?*

Security groups are stateful, NACLs are stateless

▼ *Is there any overhead with this?*

No overhead, this will happen instantly as part of how AWS networking ac works.

Which statement best describes an AWS account's default network access control list?

- ○ It is stateless and denies all inbound and outbound traffic.
- ○ It is stateful and allows all inbound and outbound traffic.
- ● It is stateless and allows all inbound and outbound traffic.
- ○ It is stateful and denies all inbound and outbound traffic.

▼ *What is DNS resolution?*

Domain Name System - it's a web address into the browser - kinda like a phone book
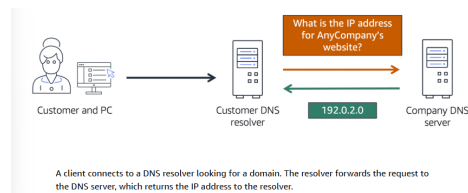
▼ *What is the service provided for DNS?*

Amazon Route 53. It gives developers and businesses a reliable way to route end users to internet apps hosted in AWS

▼ *What does Amazon Route 53 connect user requests to?*

Infrastructure running in AWS as well as infra outside

▼ *What service does Route 53 work with?*

Amazon Cloud Front

▼ *Suppose that a company's app is running on several EC2 instances. They are in an auto scaling group that attaches to an app load balancer. What are the four steps that outline how EC2 and Cloud Front interact?*

1. a customer req data from the app by going to the website

2. 53 uses DNS resolution to identify the IP and the info is sent back to the customer

3. customer's req is sent to the nearest edge location thru Cloud Front

4. Cloud Front connects to the app load balancer which sends the incoming packet to an EC2
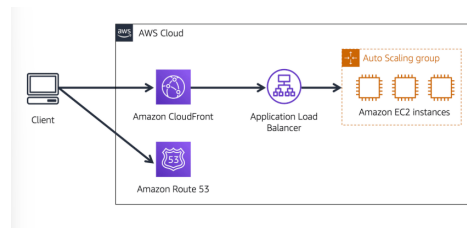
Which statement best describes DNS resolution?

⊗   Launching resources in a virtual network that you define

⊗   Storing local copies of content at edge locations around the world

⊗   Connecting a VPC to the internet

✓   Translating a domain name to an IP address

Your company has an application that uses Amazon EC2 instances to run the customer-facing website and Amazon RDS database instances to store customers' personal information. How should the developer configure the VPC according to best practices?

⊗   Place the Amazon EC2 instances in a private subnet and the Amazon RDS database instances in a public subnet.

✓   Place the Amazon EC2 instances in a public subnet and the Amazon RDS database instances in a private subnet.

⊗   Place the Amazon EC2 instances and the Amazon RDS database instances in a public subnet.

⊗   Place the Amazon EC2 instances and the Amazon RDS database instances in a private subnet.

Which component can be used to establish a private dedicated connection between your company's data center and AWS?

- ⊗ Private subnet

- ⊗ DNS

- ⊙ AWS Direct Connect

- ⊗ Virtual private gateway

Which statement best describes security groups?

- ⊙ They are stateful and deny all inbound traffic by default.

- ⊗ They are stateful and allow all inbound traffic by default.

- ⊗ They are stateless and deny all inbound traffic by default.

- ⊗ They are stateless and allow all inbound traffic by default.

Which component is used to connect a VPC to the internet?

- ⊗ Public subnet

- ⊗ Edge location

- ⊗ Security group

- ⊙ Internet gateway

Which service is used to manage the DNS records for domain names?

- ⊗ Amazon Virtual Private Cloud

- ⊗ AWS Direct Connect

- ⊗ Amazon CloudFront

- ⊘ Amazon Route 53