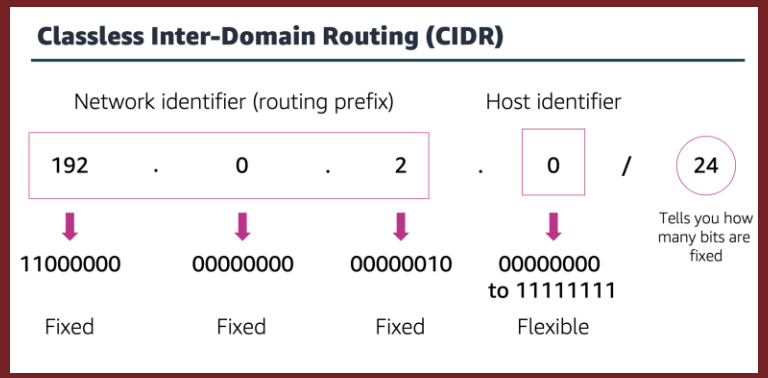
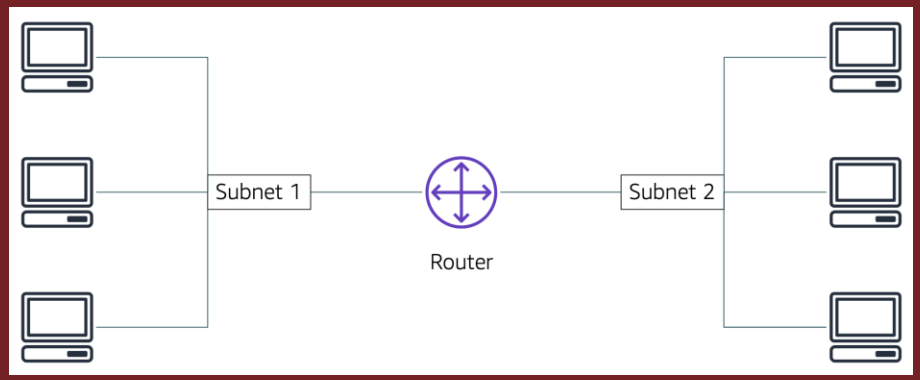
NETWORKING AND CONTENT DELIVERY

NETWORKING BASICS

- A network is two or more client machines connected to share resources
- Each client machine has an IP address (4 sets of binary numbers)
- IPv4 = 32-bit IPv6 = 128-bit
- Classless Inter-domain Routing is another way to describe networks
- CIDR list the IP address, and fixed bits



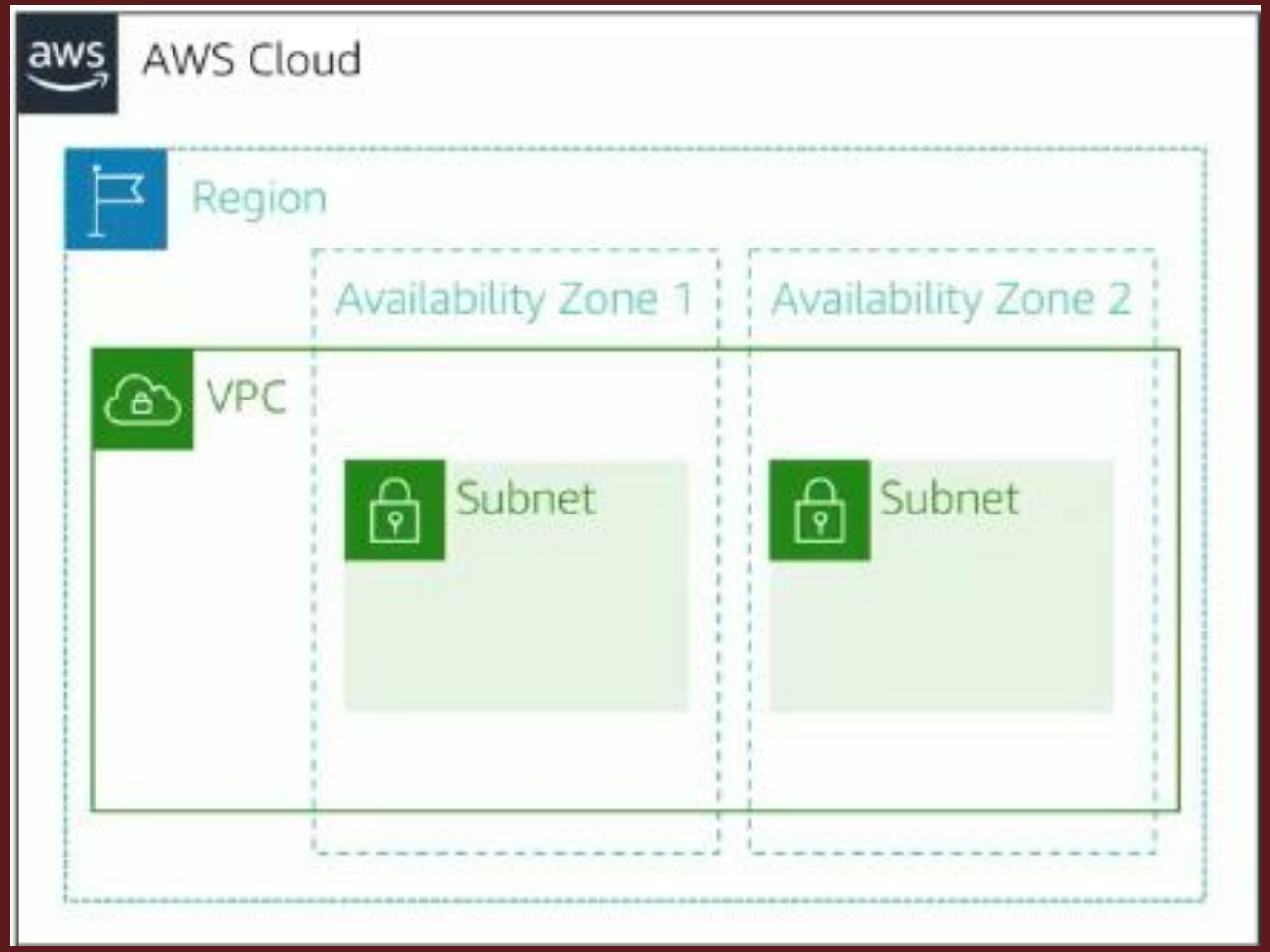


IPv4 (32-bit) address: 192.0.2.0

IPv6 (128-bit) address:
2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

AMAZON VPC

- Allows you to launch and control AWS resources on a virtual network
- Selection of IP address range
- Allows you to create subnets
- Allows you to customize network configuration
- Allows you to use multiple layers of the network
- You can use both IPv4 and IPv6 on VPC
- Subnets:
    - Range of IP address that divide the VPC
    - Each subnet belongs to one availability zone
    - Each subnet can be classified at private or public



IP ADDRESSING

- When you make a new VPC you assign it to a IPv4 CIDR block
- You get to assign the range of IP addresses
- After the VPC is created you cannot change the IP address range
- CIDR block of subnets cannot overlap
- When you make a subnet there are 5 IP addresses that you cannot use because they are reserved

- 5 reserved IP addresses
  - 10.0.0.0 - network address
  - 10.0.0.1 - internal communication
  - 10.0.0.2 - Domain name system
  - 10.0.0.3 - Future use
  - 10.0.0.225 - network broadcast

PUBLIC IP ADDRESSING TYPES

- Public IPv4 address
  - Manually assigned through Elastic IP address
  - Automatically assigned through auto-assign public IP address settings.
- Elastic IP address
  - Associated with AWS accounts
  - Additional cost added to use this

ELASTIC NETWORK INTERFACE AND ROUTE TABLES +ROUTES

This is a virtual network interface that you can use to attach and detach to an instance.

Its attributes follow it what attached to a new instance

Each instance in a VPC has a default network interface

A route table is a set of rules that you can configure to direct network traffic in your subnet

A route specifies a destination for the traffic

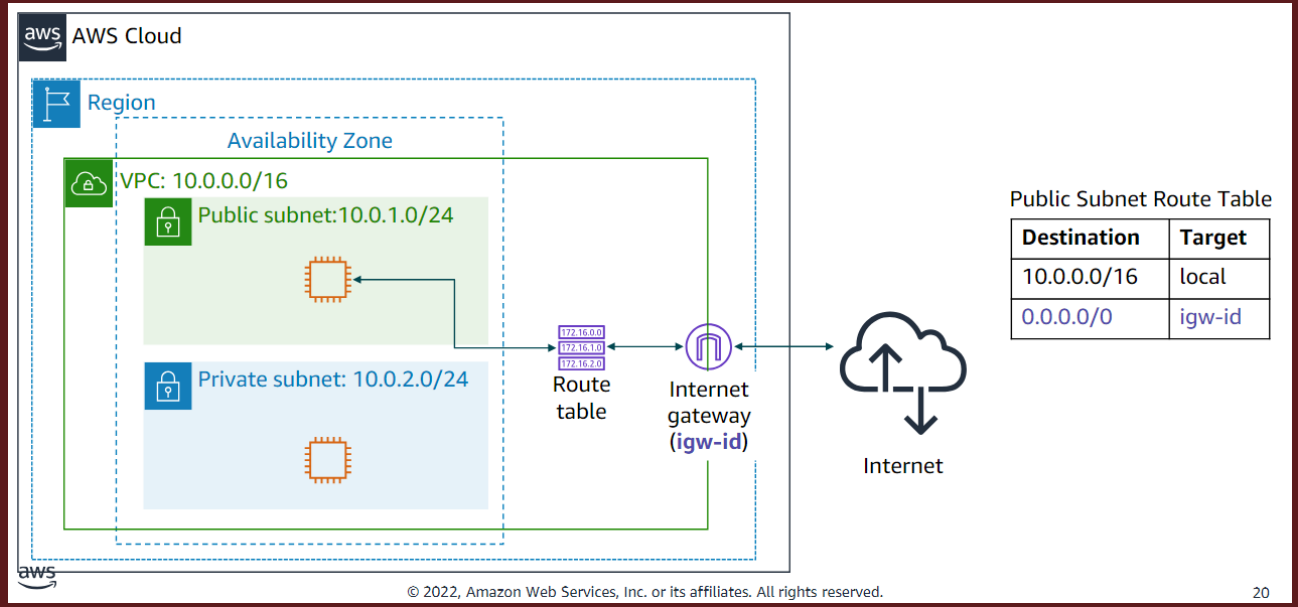
Each subnet must have one route table

INTERNET GATEWAY

An internet gateway is a VPC component that allows communication between instances in your VPC

An internet gateway does two things:

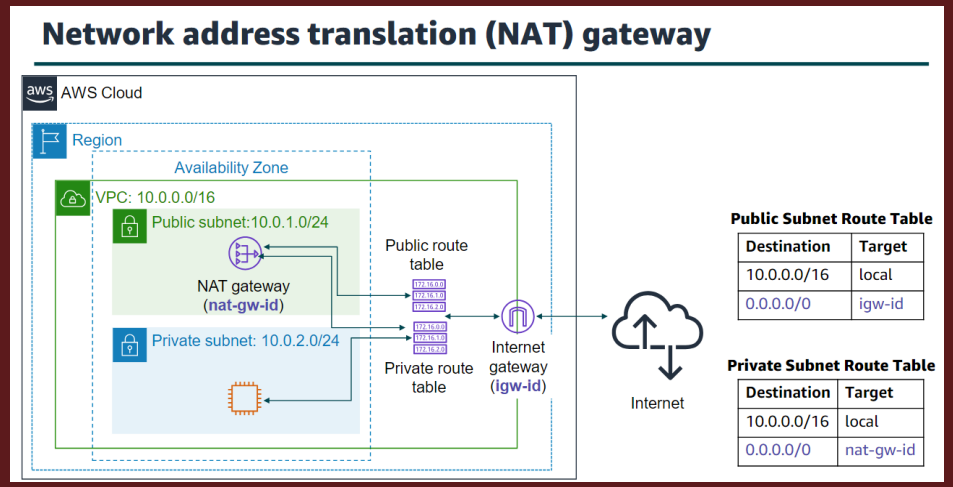
- Provides a target for route tables to direct network traffic to
- Translates network addresses for instances that were assigned with public IPv4 addresses



NETWORK ADDRESS TRANSLATION GATEWAY

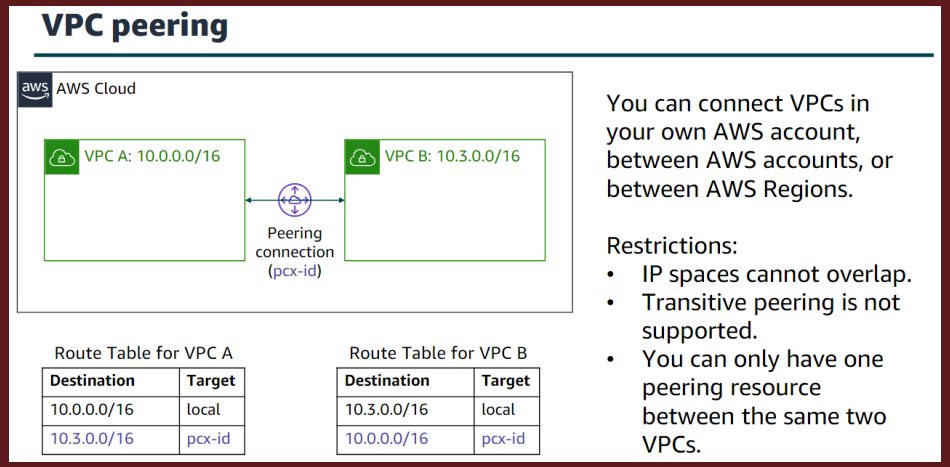
NAT gateways allows instances in a private subnet to connect to the internet or other AWS services but does not allow the internet to initiate a connection with those instances.

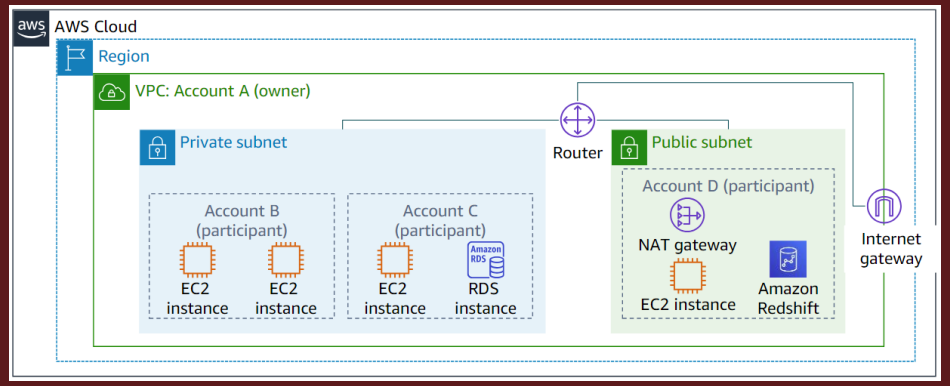
You can use a NAT instance in a public subnet instead of a NAT gateway



VPC SHARING AND PEERING

- VPC sharing:
  - Allows users to share subnets with other AWS accounts
  - Allow users to decouple accounts and networks so that you have fewer and centrally managed VPCs
- VPC peering:
  - Allows users to privately route traffic between two VPCs
  - Instances can easily communicate with each other if they are in the same network

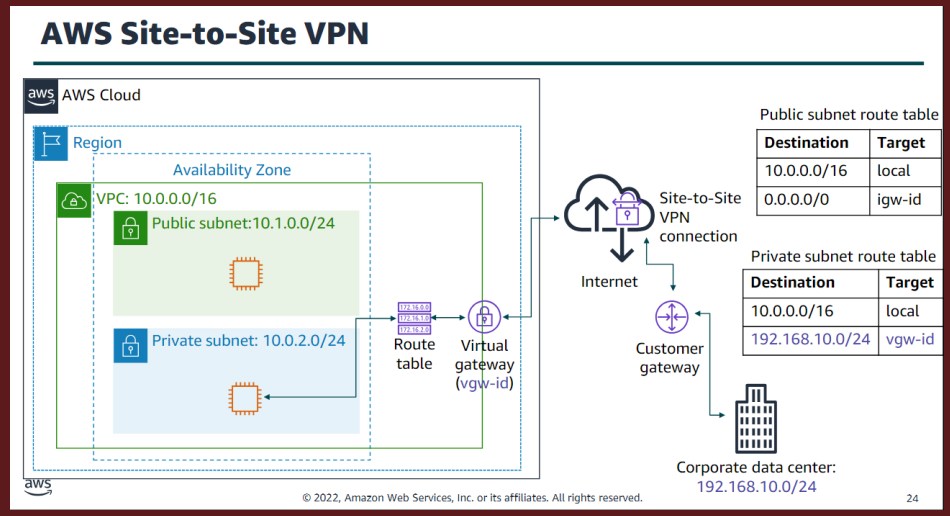




AWS SITE-TO-SITE VPN

How to make a VPN:

- Create a new virtual gateway device and attach it to your VPC
- Define the configuration of the VPC device
- Create a custom route table to route data traffic to the VPN gateway
- Establish a VPN connection to link the systems together
- Configure routing to pass traffic through the connection

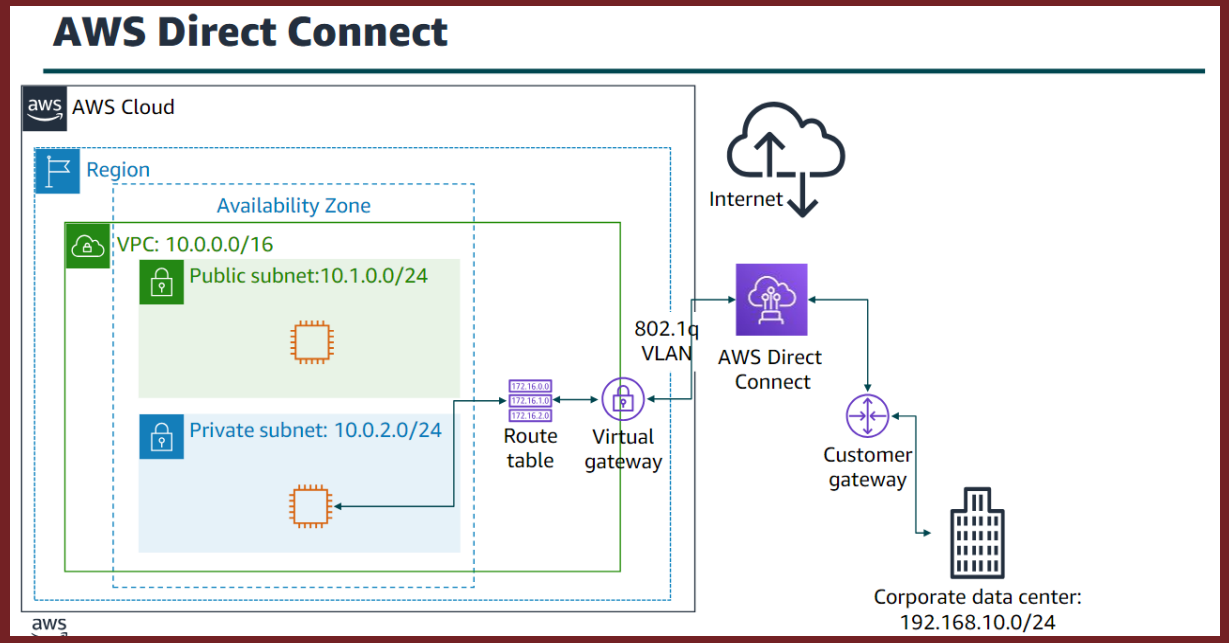


AWS DIRECT CONNECT

Allows the user to establish a private network connection between one of your networks

This private connection can reduce network cost

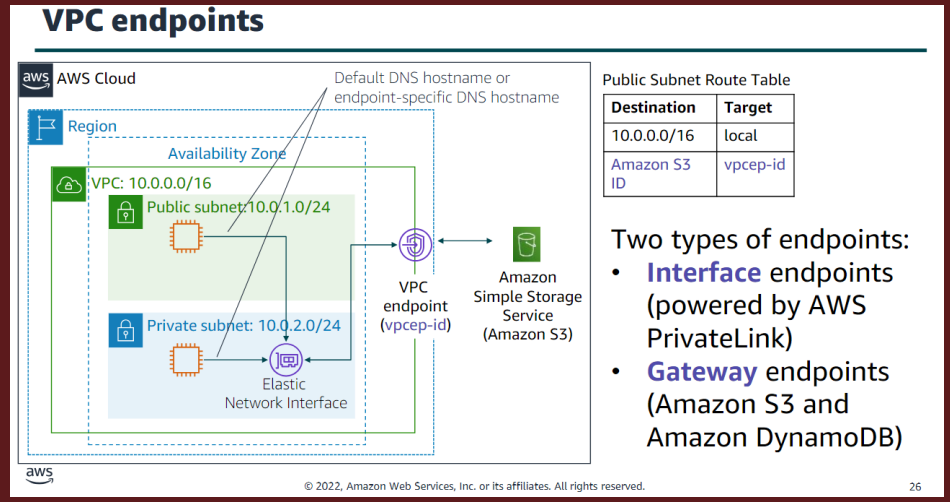
DX uses open standard 802.1q virtual local area networks (VLANs)



VPC ENDPOINT

It is a virtual device that enables you to privately connect your VPC to supported AWS services and VPC endpoint services that are powered by AWS PrivateLink

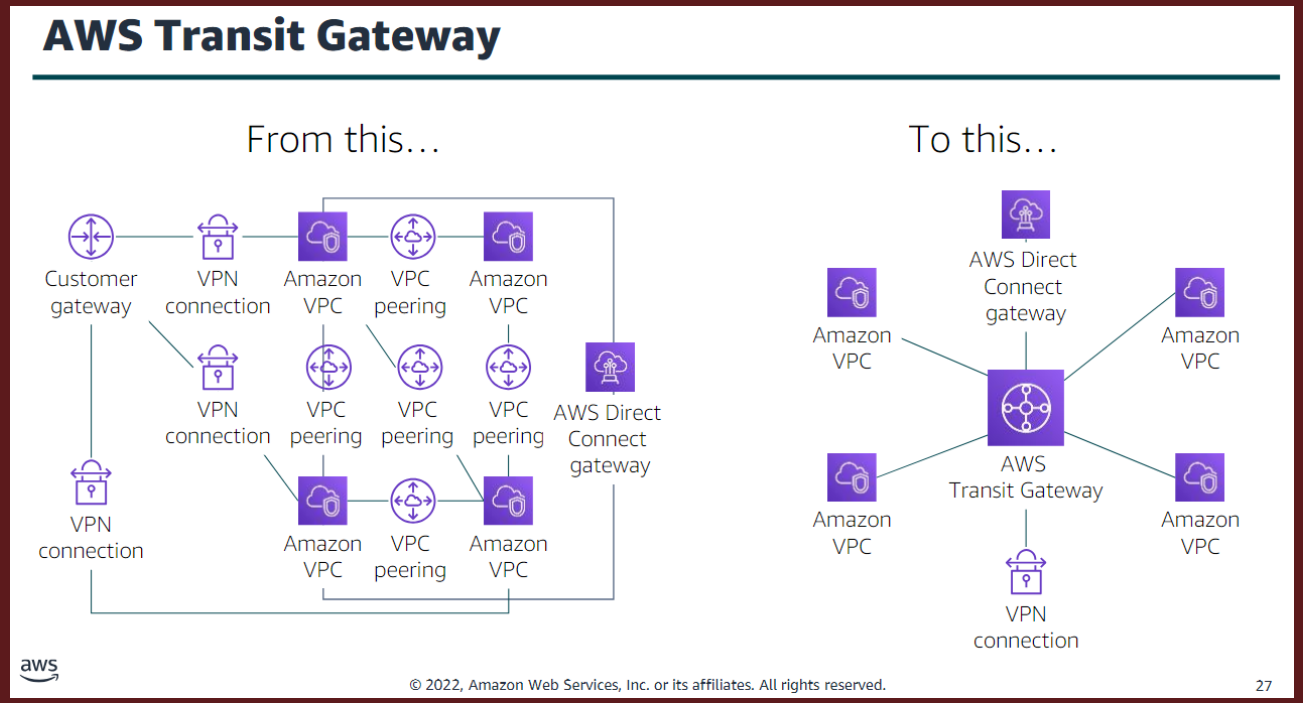
- Interface endpoint:
  - Allows you to connect to services that are powered by AWS PrivateLink
- Gateway endpoint:
  - Gateway endpoint does not add any additional charges
  - Uses standard charges for data transfer



AWS TRANSIT GATEWAY

This allows you to simplify your networking model.

You only need to manage one connection between the central gateway and each VPC.



VPC SECURITY GROUPS

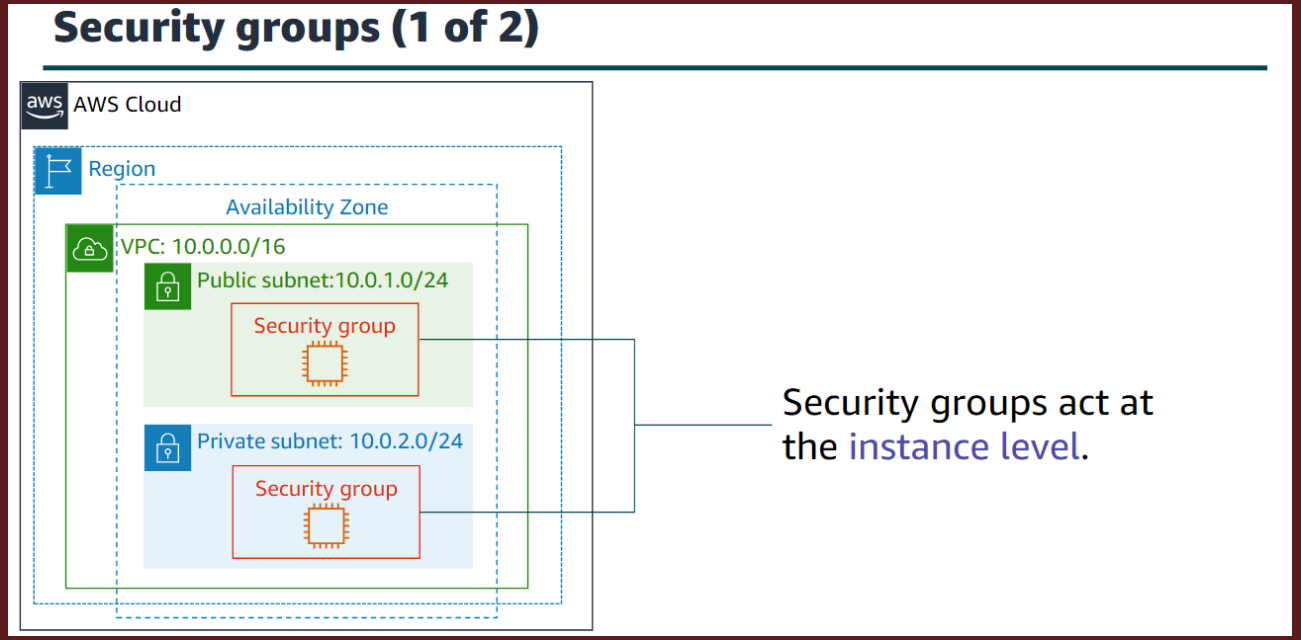
These security groups act as a virtual firewall for your instances

It also controls inbound and outbound traffic

Security groups act at the instance level not at the subnet level

Default security groups do not allow all inbound traffic and allows all outbound traffic

You can specifically allow rules, but not deny rules



NETWORK ACCESS CONTROL LIST

Network ACLs act at the subnet level

Optional layer of security

Each subnet in your VPC must be associated with a network ACL

Allows you to focus more on security groups

Rules can be allowed and denied

Rules are evaluated in numerical order

Attribute	Security Groups	Network ACLs
Scope	Instance level	Subnet level
Supported Rules	Allow rules only	Allow and deny rules
State	Stateful (return traffic is automatically allowed, regardless of rules)	Stateless (return traffic must be explicitly allowed by rules)
Order of Rules	All rules are evaluated before decision to allow traffic	Rules are evaluated in number order before decision to allow traffic

AMAZON ROUTE 53

This service routes end-users to internet applications

It is fully compliant with IPv4 and IPv6

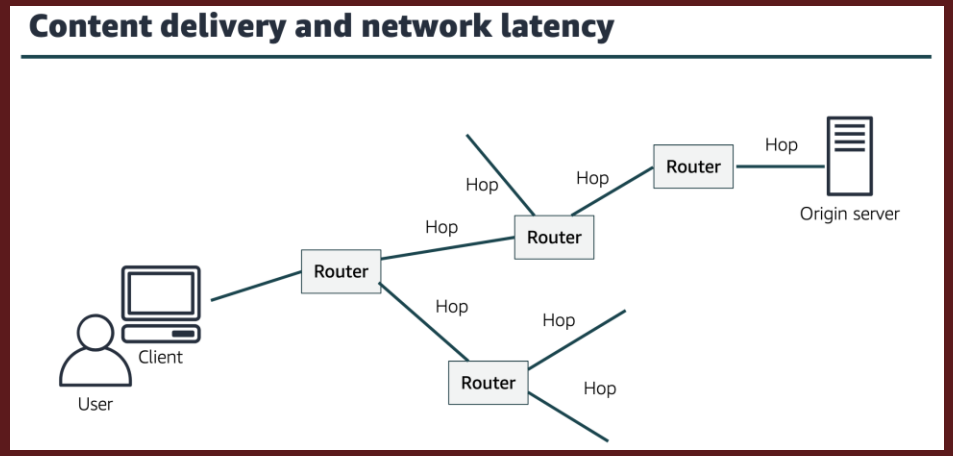
Allows you to enable domain names

Supported routing includes:

- Simple routing – single server
- Weighted round robin routing – applies weights to resource records to specify frequency
- Latency routing – helps improve global apps
- Geolocation routing – directs traffic based on user
- Geoproximity routing – directs traffic based on resource
- Failover routing – backup site if primary site fails
- Multivalue answer routing – respond to domain name system (DNS) queries

CONTENT DELIVERY NETWORK (CDN)

- Globally distributed system of cache servers
- Delivers local copy of requested content
- Accelerated delivery of dynamic content
- Improves application performance



AMAZON CLOUDFRONT

- Fast, global, and secure CDN service
- Global network of edge locations
- Self-service model
- Allows application performance to run much smoother
- Pay-as-you-go pricing
- Relies on route 53 Geoloaction routing
- As data becomes stale, it gets removed from cache to make room for new content