AWS Academy Cloud Foundations

Module 5: Networking and Content Delivery

aws academy

Module overview

Topics

- Networking basics

- Amazon VPC

- VPC networking

- VPC security

- Amazon Route 53

- Amazon CloudFront

Activities

- Label a network diagram

- Design a basic VPC architecture

Demo

- VPC demonstration

Lab

- Build your VPC and launch a web server

Knowledge check

Module objectives

After completing this module, you should be able to:

- Recognize the basics of networking
- Describe virtual networking in the cloud with Amazon VPC
- Label a network diagram
- Design a basic VPC architecture
- Indicate the steps to build a VPC
- Identify security groups
- Create your own VPC and add additional components to it to produce a customized network
- Identify the fundamentals of Amazon Route 53
- Recognize the benefits of Amazon CloudFront

Module 5: Networking and Content Delivery

Section 1: Networking basics

aws academy

Networks

Subnet 1

Router

Subnet 2
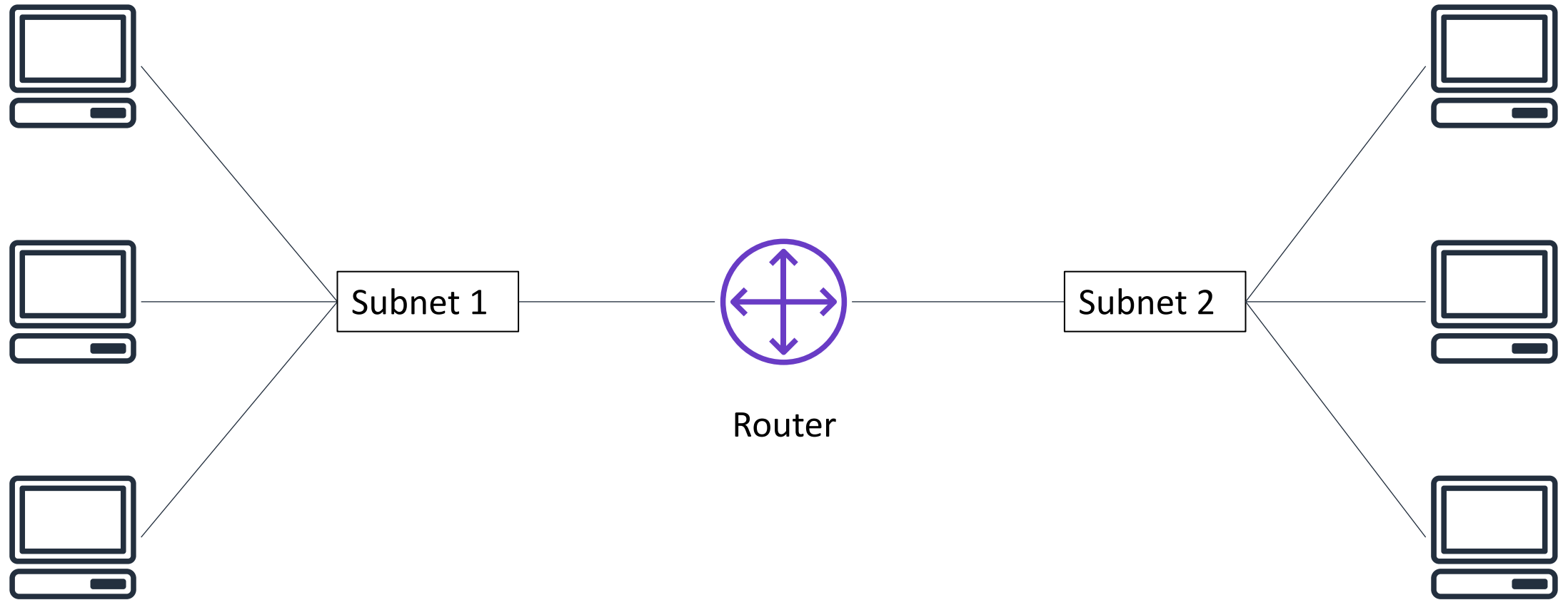
IP addresses

192 . 0 . 2 . 0

11000000   00000000   00000010   00000000

IPv4 and IPv6 addresses

IPv4 (32-bit) address: 192.0.2.0

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

Classless Inter-Domain Routing (CIDR)

Network identifier (routing prefix)   Host identifier

| 192 | . | 0 | . | 2 | . | 0 | / | 24 |

Tells you how many bits are fixed

11000000   00000000   00000010   00000000
to 11111111

Fixed   Fixed   Fixed   Flexible

Open Systems Interconnection (OSI) model

Layer	Number	Function	Protocol/Address
Application	7	Means for an application to access a computer network	HTTP(S), FTP, DHCP, LDAP
Presentation	6	• Ensures that the application layer can read the data • Encryption	ASCI, ICA
Session	5	Enables orderly exchange of data	NetBIOS, RPC
Transport	4	Provides protocols to support host-to-host communication	TCP, UDP
Network	3	Routing and packet forwarding (routers)	IP
Data link	2	Transfer data in the same LAN network (hubs and switches)	MAC
Physical	1	Transmission and reception of raw bitstreams over a physical medium	Signals (1s and 0s)

Module 5: Networking and Content Delivery

Section 2: Amazon VPC

Amazon VPC

Amazon
VPC

- Enables you to provision a **logically isolated** section of the AWS Cloud where you can launch AWS resources in a virtual network that you define

- Gives you **control over your virtual networking resources**, including:
  - Selection of IP address range
  - Creation of subnets
  - Configuration of route tables and network gateways

- Enables you to **customize the network configuration** for your VPC

- Enables you to use **multiple layers of security**

VPCs and subnets

- VPCs:
  - **Logically isolated** from other VPCs
  - **Dedicated** to your AWS account
  - Belong to a single **AWS Region** and can span multiple Availability Zones

- Subnets:
  - **Range of IP addresses** that divide a VPC
  - Belong to a single **Availability Zone**
  - Classified as **public** or **private**

aws AWS Cloud

Region

VPC

Availability Zone 1
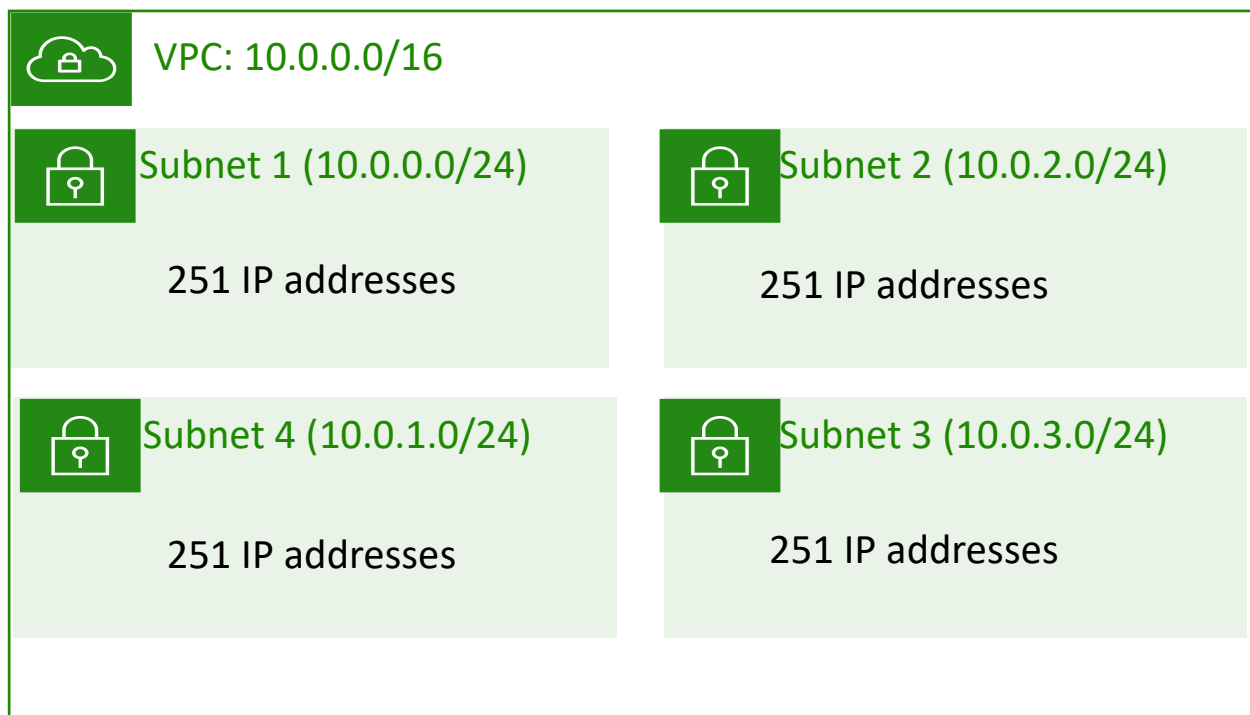
Availability Zone 2

Subnet

Subnet

IP addressing
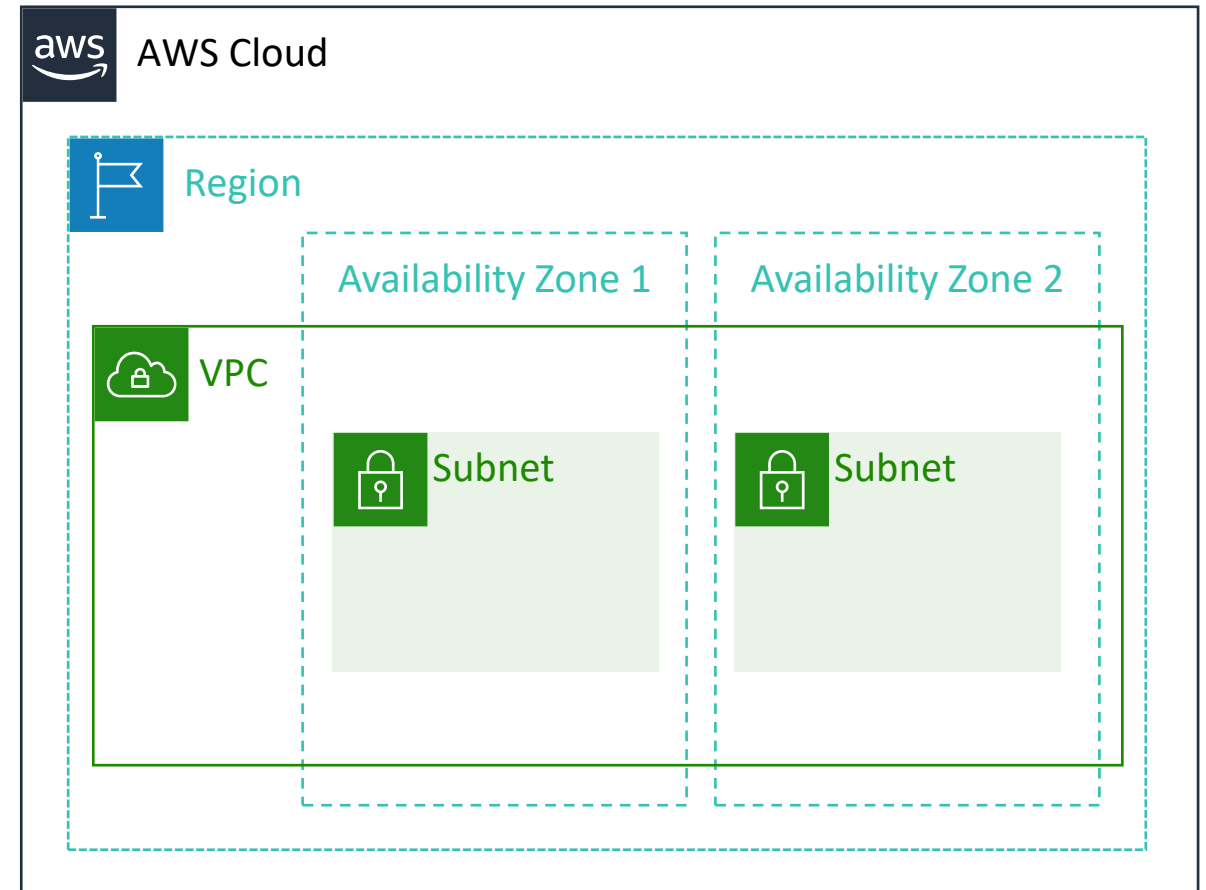
- When you create a VPC, you assign it to an IPv4 **CIDR block** (range of **private** IPv4 addresses).

- You **cannot change the address range** after you create the VPC.

- The **largest** IPv4 CIDR block size is **/16**.

- The **smallest** IPv4 CIDR block size is **/28**.

- IPv6 is also supported (with a different block size limit).

- CIDR blocks of subnets **cannot overlap**.

VPC

x.x.x.x/16 or 65,536 addresses (max)
to
x.x.x.x/28 or 16 addresses (min)

Reserved IP addresses

Example: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four equal-sized subnets. Only 251 IP addresses are available for use by each subnet.

VPC: 10.0.0.0/16

Subnet 1 (10.0.0.0/24)

251 IP addresses

Subnet 2 (10.0.2.0/24)

251 IP addresses

Subnet 4 (10.0.1.0/24)

251 IP addresses

Subnet 3 (10.0.3.0/24)

251 IP addresses

| IP Addresses for CIDR block 10.0.0.0/24	Reserved for
10.0.0.0	Network address
10.0.0.1	Internal communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future use
10.0.0.255	Network broadcast address

Public IP address types

Public IPv4 address

- Manually assigned through an Elastic IP address
- Automatically assigned through the auto-assign public IP address settings at the subnet level

Elastic IP address

- Associated with an AWS account
- Can be allocated and remapped anytime
- Additional costs might apply

Elastic network interface

- An elastic network interface is a **virtual network interface** that you can:
  - Attach to an instance.
  - Detach from the instance, and attach to another instance to redirect network traffic.
- Its **attributes follow** when it is reattached to a new instance.
- Each instance in your VPC has a **default network interface** that is assigned a private IPv4 address from the IPv4 address range of your VPC.

Subnet: 10.0.1.0/24

Elastic network interface
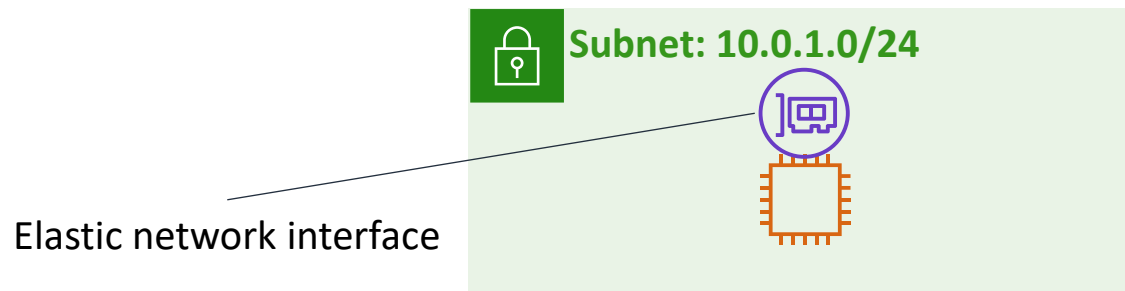
Route tables and routes

- A **route table** contains a set of rules (or routes) that **you can configure** to direct network traffic from your subnet.

- Each **route** specifies a destination and a target.

- By default, every route table contains a **local route** for communication within the VPC.

- Each **subnet must be associated with a route table** (at most one).

Main (Default) Route Table

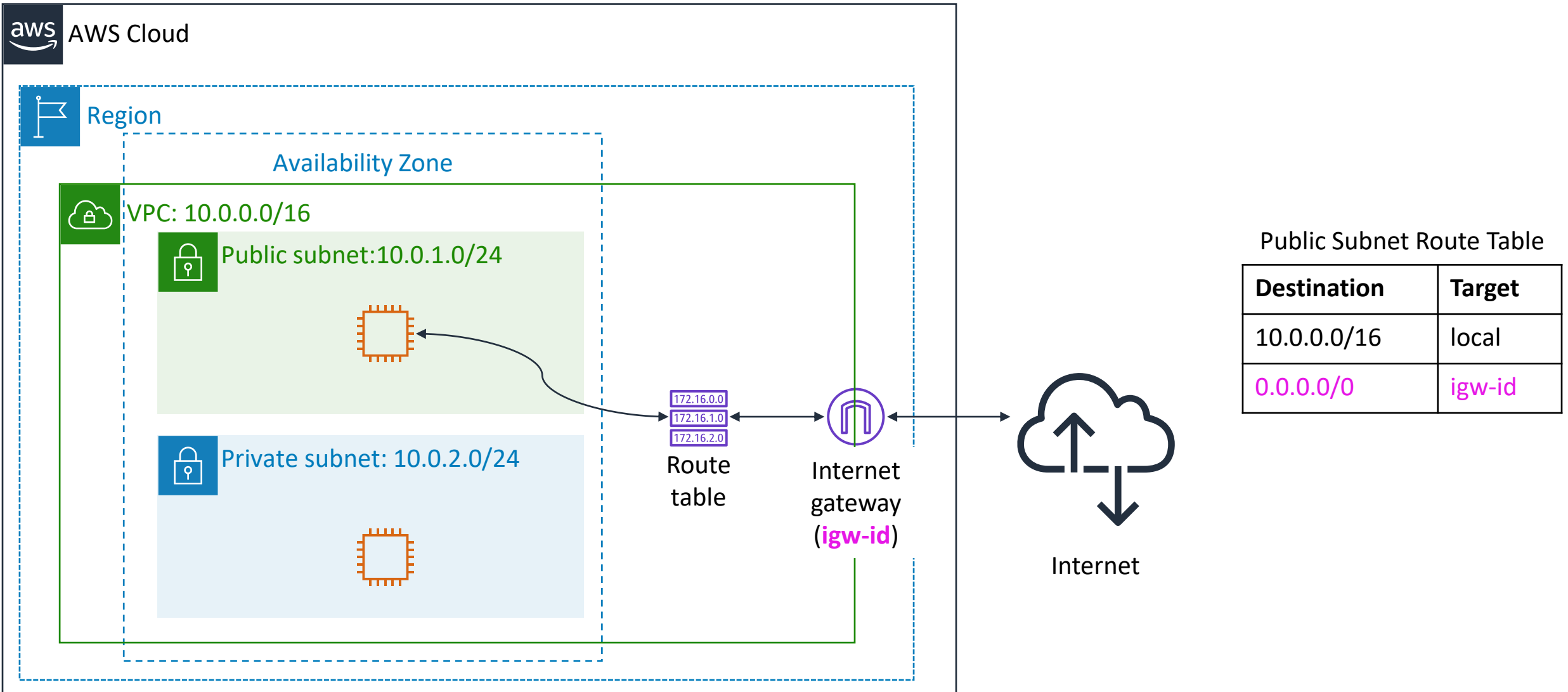| Destination	Target
10.0.0.0/16	local

VPC CIDR block

Section 2 key takeaways

- A VPC is a logically isolated section of the AWS Cloud.
- A VPC belongs to one Region and requires a CIDR block.
- A VPC is subdivided into subnets.
- A subnet belongs to one Availability Zone and requires a CIDR block.
- Route tables control traffic for a subnet.
- Route tables have a built-in local route.
- You add additional routes to the table.
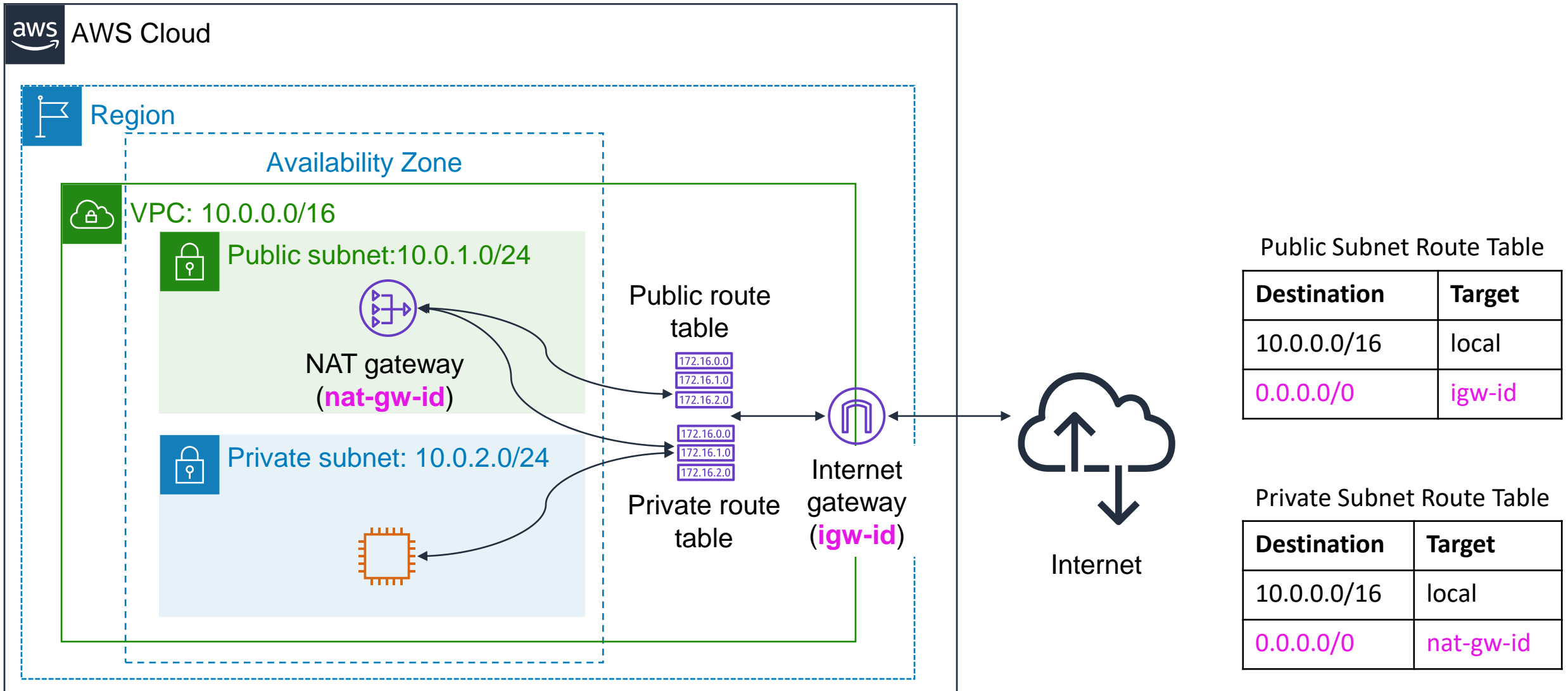- The local route cannot be deleted.

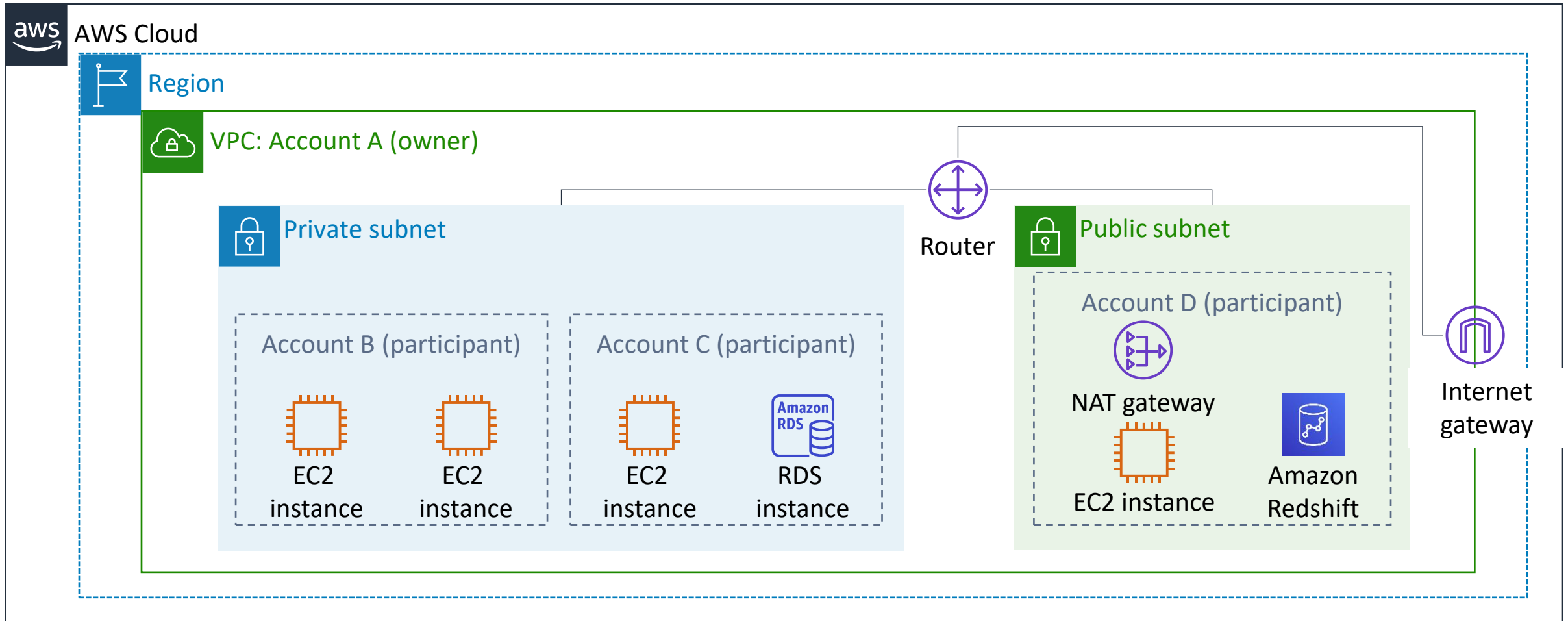Module 5: Networking and Content Delivery

Section 3: VPC networking

Internet gateway

AWS Cloud

Region

Availability Zone

VPC: 10.0.0.0/16

Public subnet:10.0.1.0/24

Private subnet: 10.0.2.0/24

172.16.0.0
172.16.1.0
172.16.2.0

Route table

Internet gateway (**igw-id**)

Internet

Public Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Network address translation (NAT) gateway

VPC sharing

VPC peering

AWS Cloud

VPC A: 10.0.0.0/16

VPC B: 10.3.0.0/16

Peering connection (pcx-id)
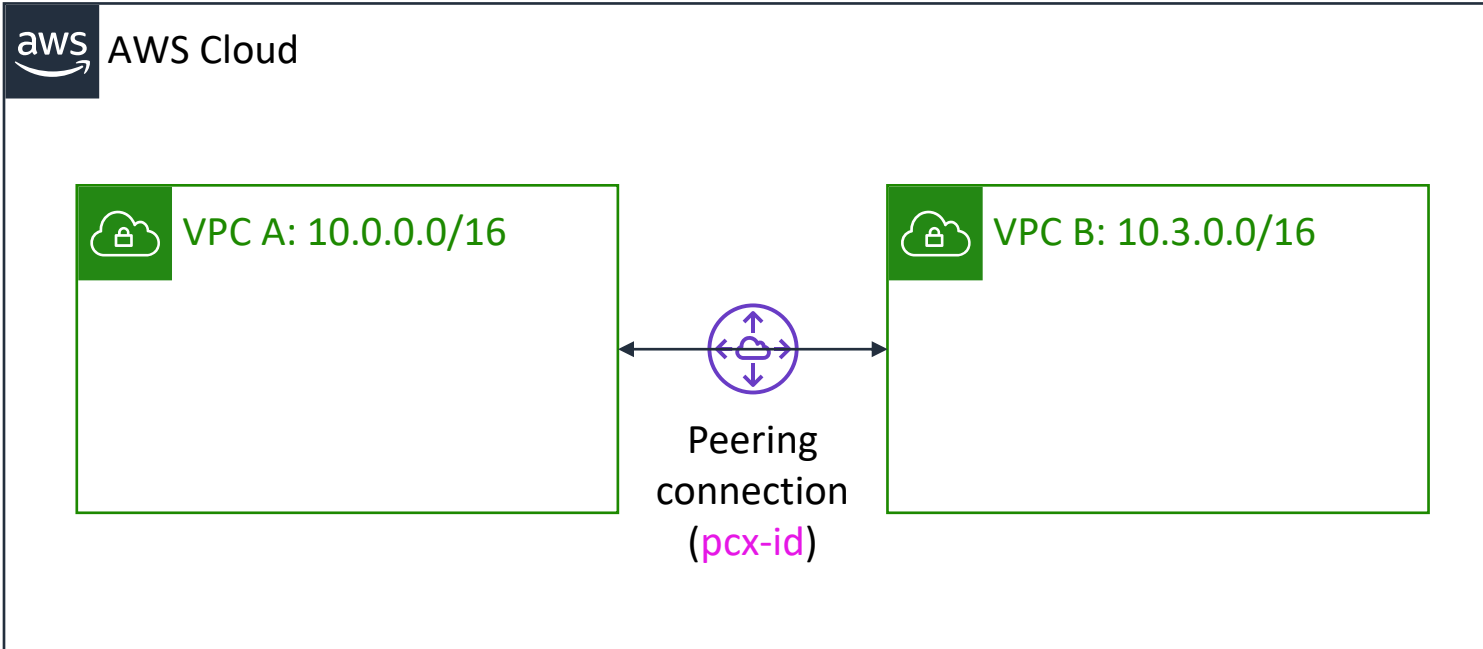
You can connect VPCs in your own AWS account, between AWS accounts, or between AWS Regions.

Restrictions:
- IP spaces cannot overlap.
- Transitive peering is not supported.
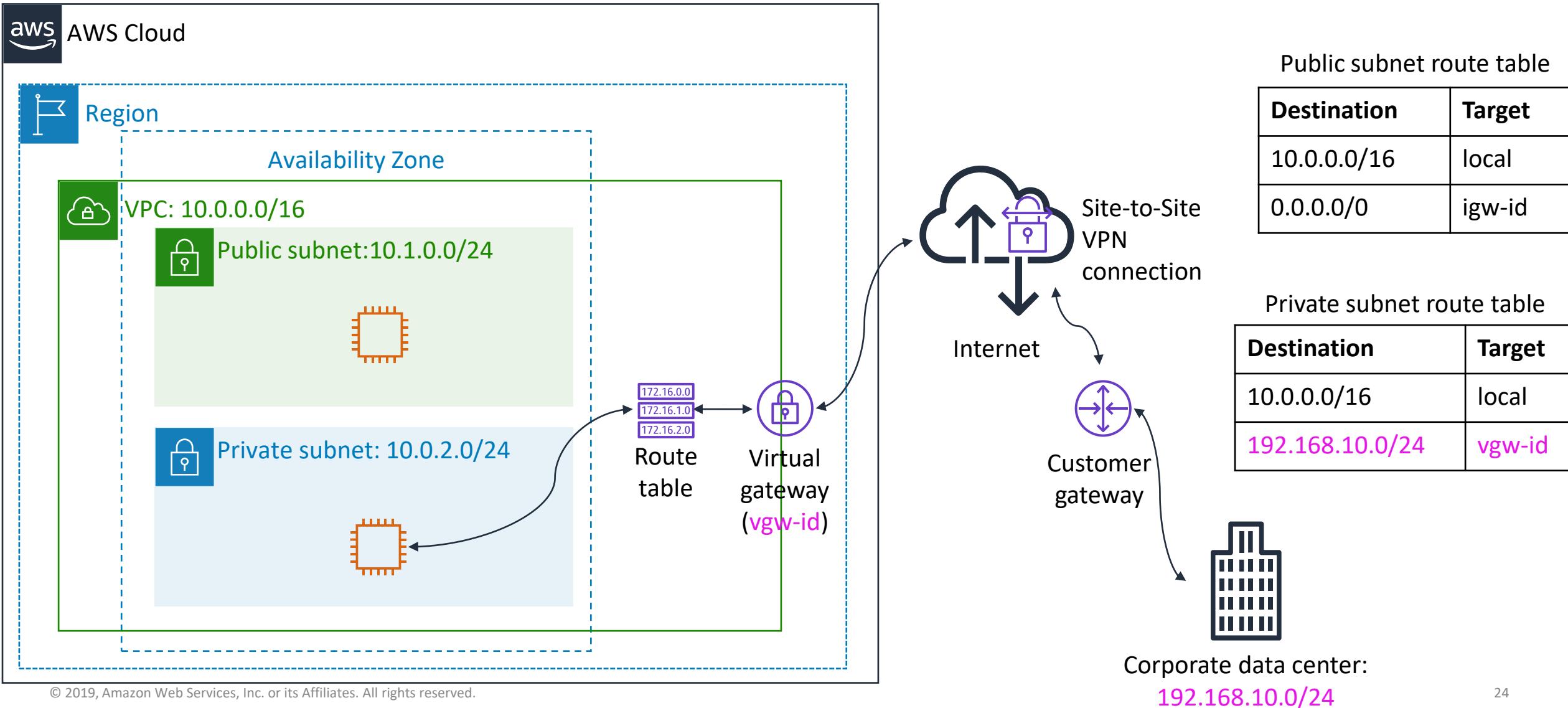- You can only have one peering resource between the same two VPCs.

Route Table for VPC A

Destination	Target
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Route Table for VPC B

Destination	Target
10.3.0.0/16	local
10.0.0.0/16	pcx-id

AWS Site-to-Site VPN

Public subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private subnet route table

Destination	Target
10.0.0.0/16	local
192.168.10.0/24	vgw-id

AWS Direct Connect

VPC endpoints

AWS Cloud

Default DNS hostname or endpoint-specific DNS hostname

Region

Availability Zone

VPC: 10.0.0.0/16

Public subnet:10.0.1.0/24

Private subnet: 10.0.2.0/24

Elastic Network Interface

VPC endpoint (vpcep-id)

Amazon Simple Storage Service (Amazon S3)
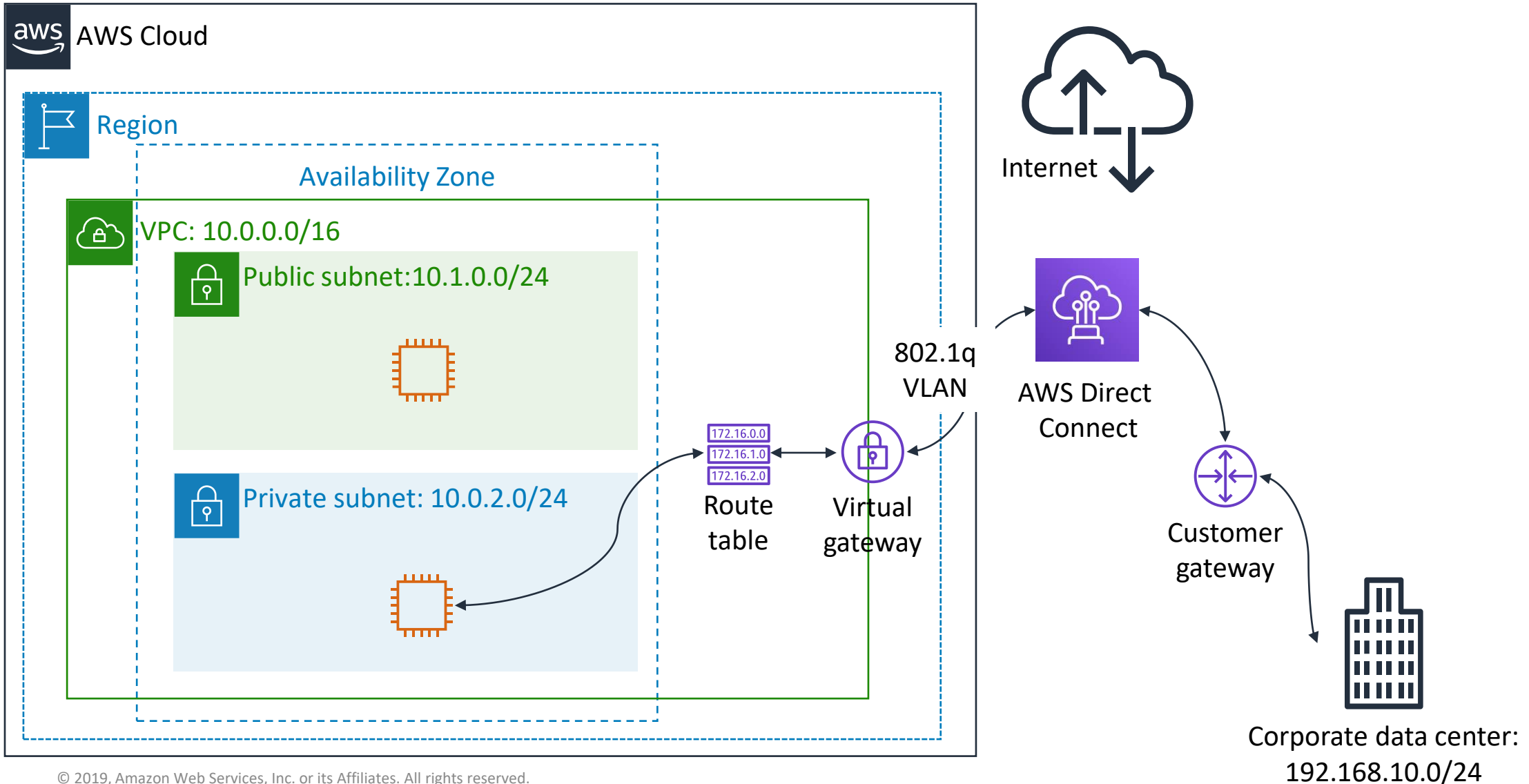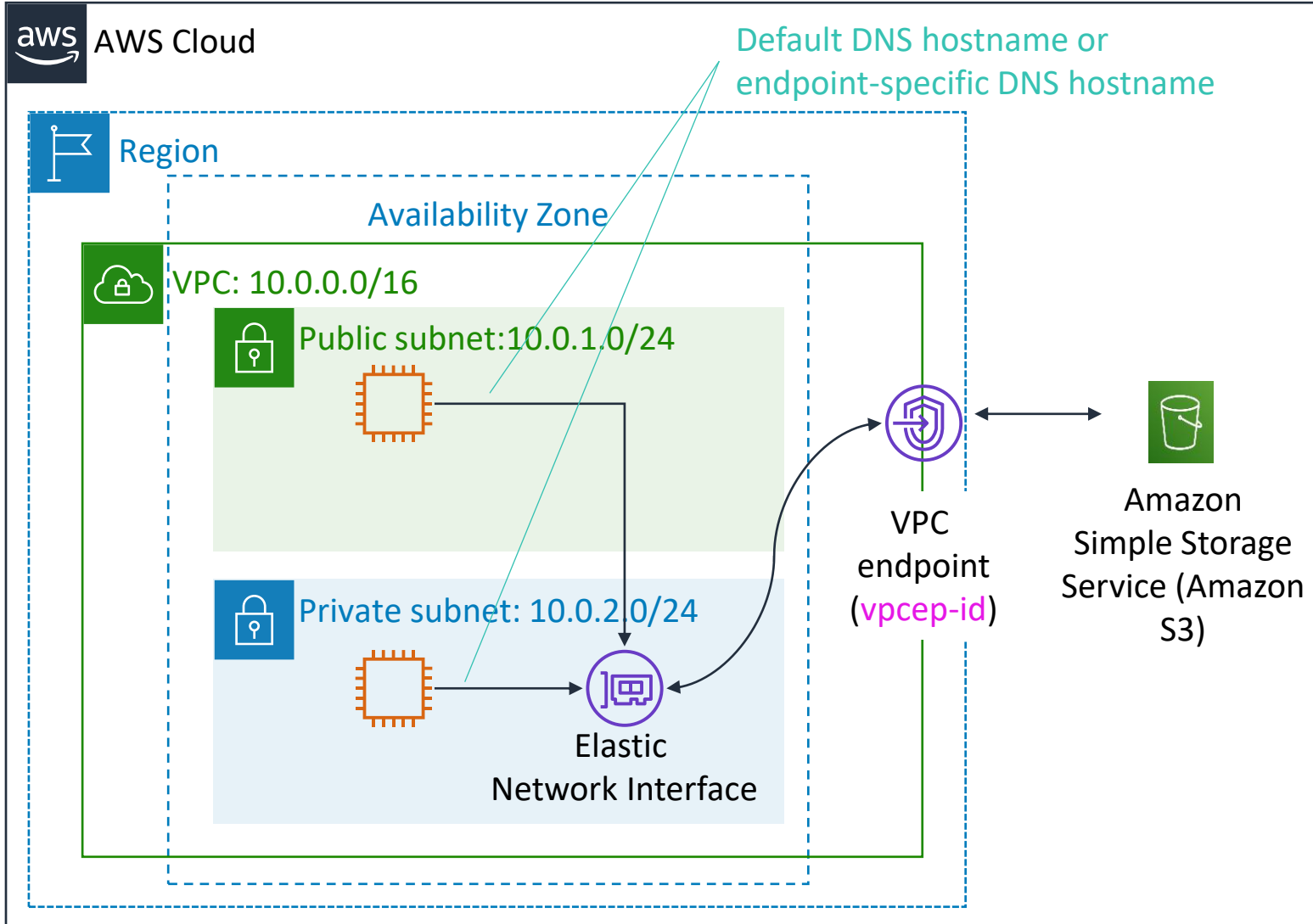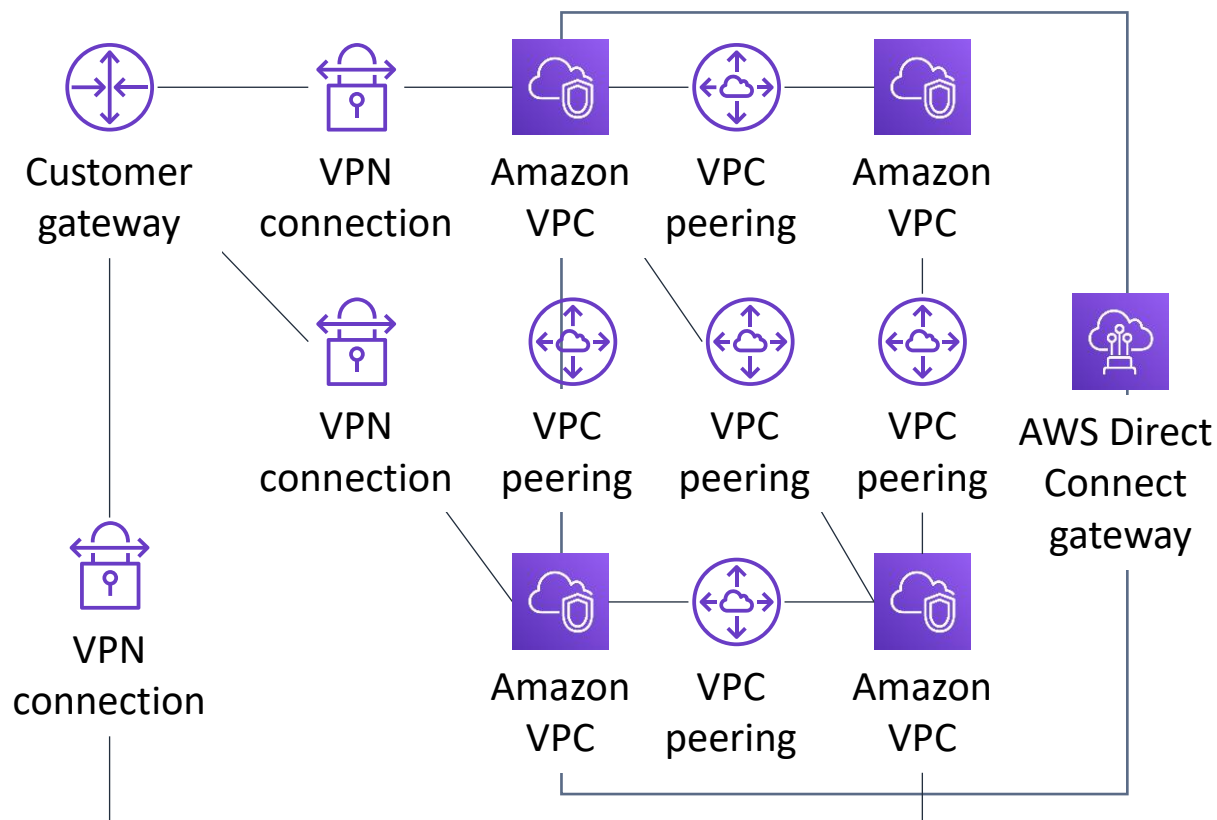
Public Subnet Route Table

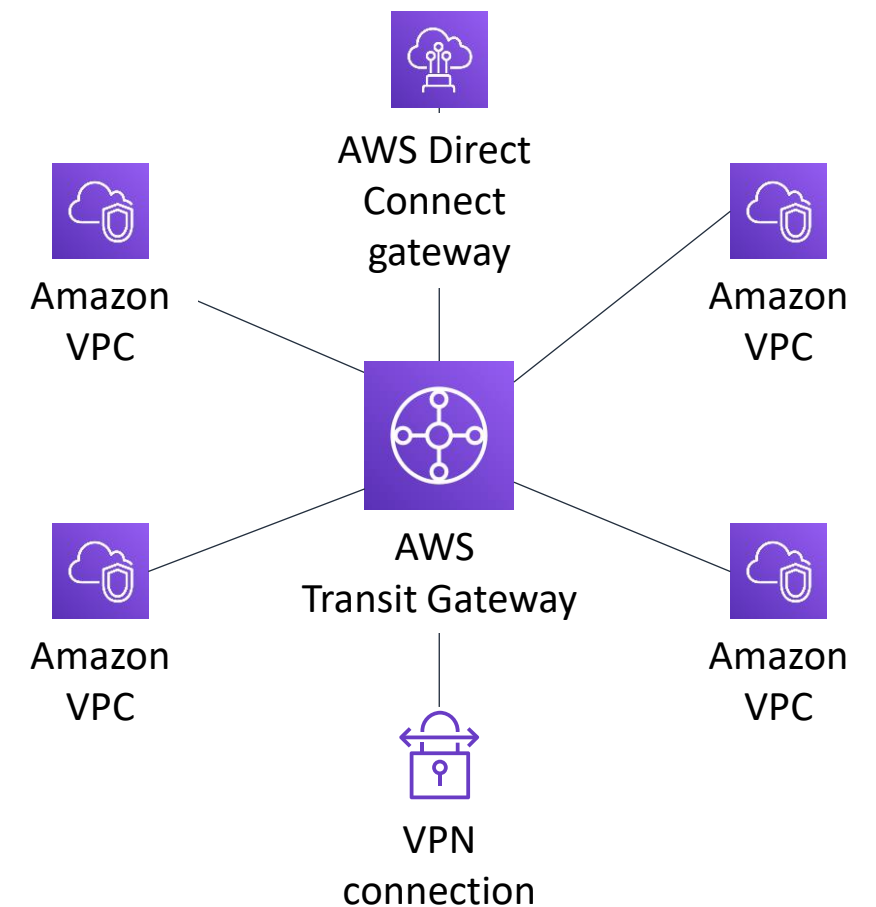| Destination	Target
10.0.0.0/16	local
Amazon S3 ID	vpcep-id

Two types of endpoints:
- **Interface** endpoints (powered by AWS PrivateLink)
- **Gateway** endpoints (Amazon S3 and Amazon DynamoDB)
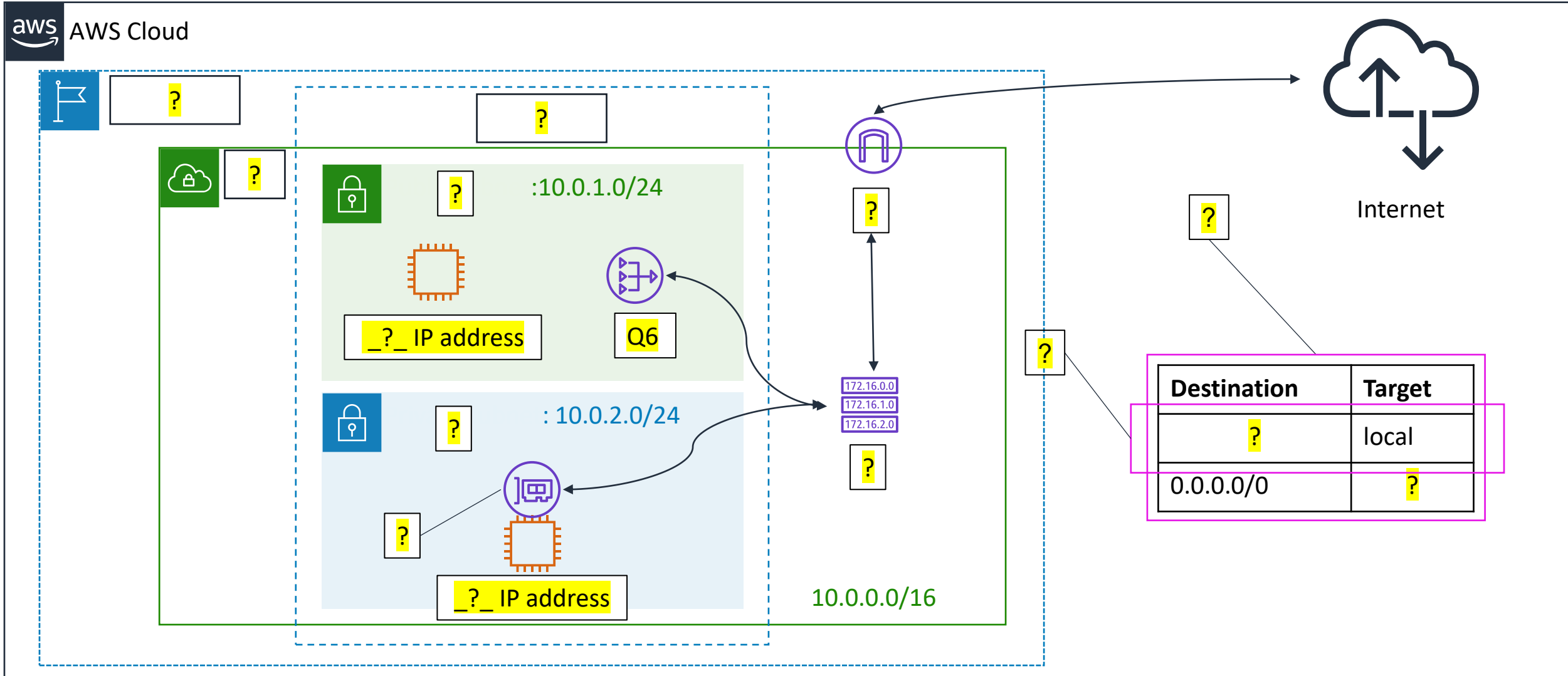
AWS Transit Gateway

From this…

Customer gateway — VPN connection — Amazon VPC — VPC peering — Amazon VPC

VPN connection — VPC peering — VPC peering — VPC peering — AWS Direct Connect gateway

VPN connection — Amazon VPC — VPC peering — Amazon VPC

To this…

Amazon VPC

AWS Direct Connect gateway

Amazon VPC

Amazon VPC

AWS Transit Gateway

Amazon VPC

VPN connection

Activity: Label this network diagram

AWS Cloud

?

?

?

?

?

:10.0.1.0/24

_?_ IP address

Q6

: 10.0.2.0/24

_?_ IP address

172.16.0.0
172.16.1.0
172.16.2.0

?

?

?

?

?

?

Internet

10.0.0.0/16

Destination	Target
?	local
0.0.0.0/0	?

Activity: Solution

AWS Cloud

Region

Availability Zone

VPC

Public subnet   0.0.1.0/24

Private IP address

NAT gateway

Internet gateway

Private subnet   10.0.2.0/24

172.16.0.0
172.16.1.0
172.16.2.0

Route table

Elastic network interface

Private IP address

10.0.0.0/16

Internet

Route table

Route

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Recorded Amazon VPC demonstration

Set up demo
Amazon Virtual Private Cloud (VPC)

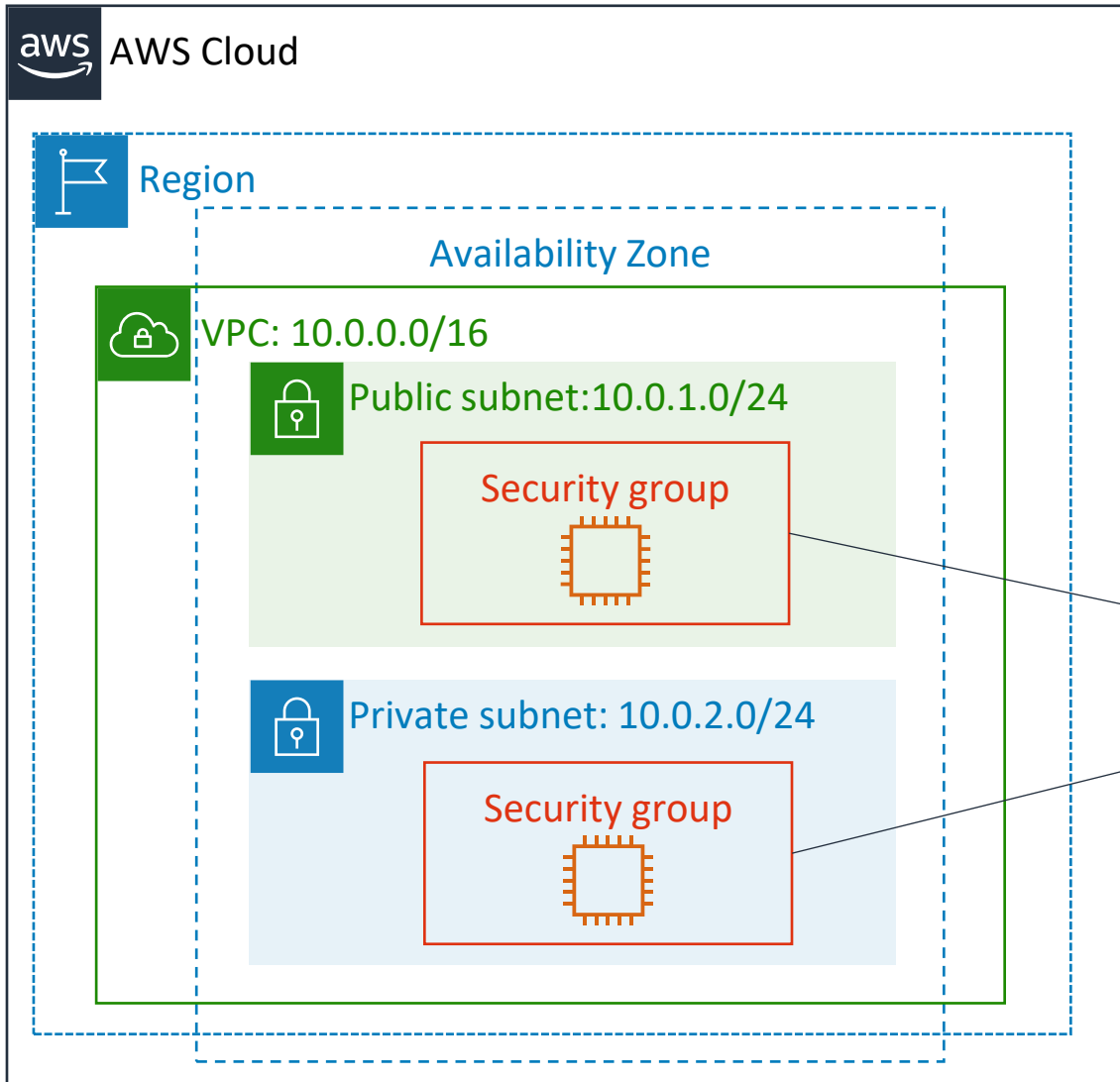# Section 3 key takeaways

- There are several VPC networking options, which include:
  - Internet gateway
  - NAT gateway
  - VPC endpoint
  - VPC peering
  - VPC sharing
  - AWS Site-to-Site VPN
  - AWS Direct Connect
  - AWS Transit Gateway
- You can use the VPC Wizard to implement your design.

Module 5: Networking and Content Delivery

Section 4: VPC security

aws academy

Security groups

Security groups act at the **instance level**.

Security groups

- Security groups have **rules** that control inbound and outbound instance traffic.

- Default security groups **deny all inbound** traffic and **allow all outbound** traffic.

- Security groups are **stateful**.

Inbound			
Source	Protocol	Port Range	Description
sg-*xxxxxxxx*	All	All	Allow inbound traffic from network interfaces assigned to the same security group.

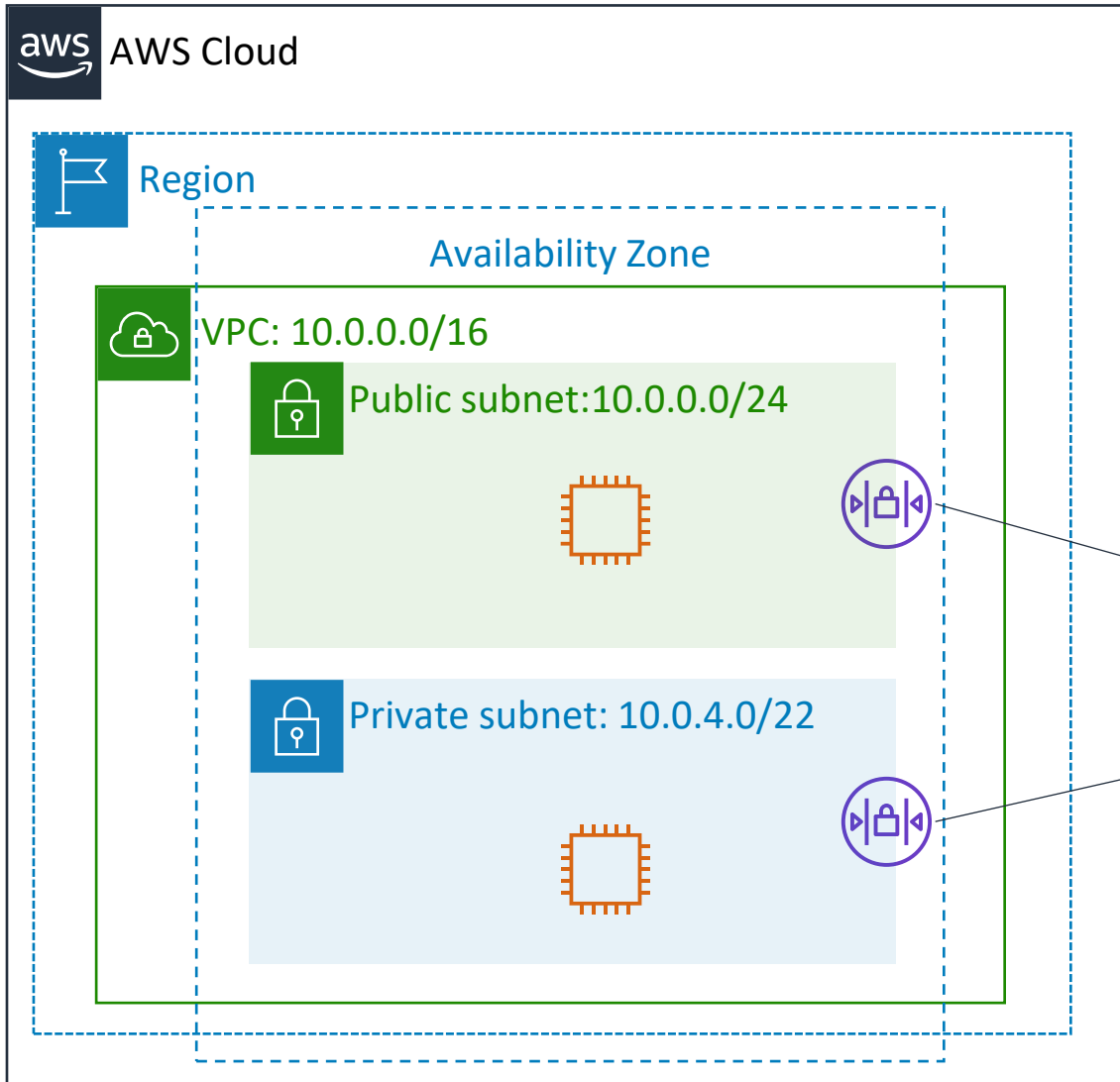| Outbound			
Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic.

Custom security group examples

- You can **specify allow** rules, but not deny rules.
- **All rules are evaluated** before the decision to allow traffic.

Inbound			
Source	Protocol	Port Range	Description
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)

Outbound			
Destination	Protocol	Port Range	Description
The ID of the security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group

Network access control lists (network ACLs)

Network ACLs act at the **subnet level**.

Network access control lists (network ACLs)

- A network ACL has **separate inbound and outbound rules**, and each rule can either **allow or deny traffic**.
- **Default** network ACLs **allow** all inbound and outbound IPv4 traffic.
- Network ACLs are **stateless**.

Inbound					
Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Custom network ACLs examples

- **Custom** network ACLs **deny** all inbound and outbound traffic until you add rules.
- You can specify **both allow and deny** rules.
- Rules are evaluated in number order, starting with the **lowest number**.

Inbound					
Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule	Type	Protocol	Port Range	Destination	Allow/Deny
100	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Security groups versus network ACLs

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

Activity: Design a VPC

Scenario: You have a small business with a website that is hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance. You have customer data that is stored on a backend database that you want to keep private. You want to use Amazon VPC to set up a VPC that meets the following requirements:

- Your web server and database server must be in separate subnets.

- The first address of your network must be 10.0.0.0. Each subnet must have 256 total IPv4 addresses.

- Your customers must always be able to access your web server.

- Your database server must be able to access the internet to make patch updates.

- Your architecture must be highly available and use at least one custom firewall layer.

Section 4 key takeaways

- Build security into your VPC architecture:
  - Isolate subnets if possible.
  - Choose the appropriate gateway device or VPN connection for your needs.
  - Use firewalls.
- Security groups and network ACLs are firewall options that you can use to secure your VPC.

Lab 2:
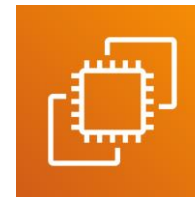# Build Your VPC and Launch a Web Server

Lab 2: Scenario

aws academy

In this lab, you use Amazon VPC to create your own VPC and add some components to produce a customized network. You create a security group for your VPC. You also create an EC2 instance and configure it to run a web server and to use the security group. You then launch the EC2 instance into the VPC.
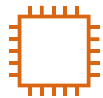
Amazon
VPC

Amazon
EC2

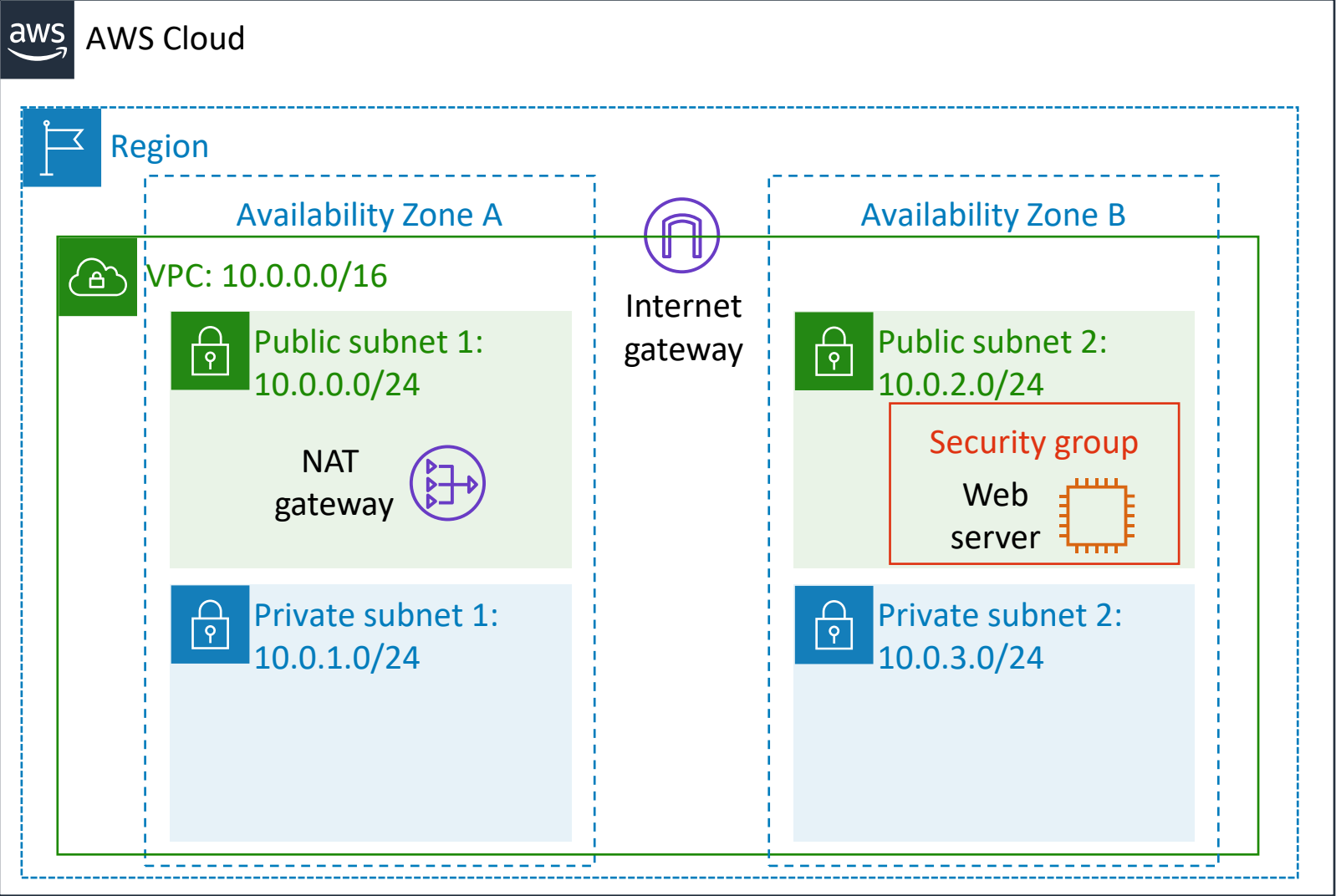# Lab 2: Tasks

- Create a VPC.

- Create additional subnets.

Security group

- Create a VPC security group.

- Launch a web server instance.

Lab 2: Final product

AWS Cloud

Region

VPC: 10.0.0.0/16

Availability Zone A

Public subnet 1: 10.0.0.0/24

NAT gateway

Private subnet 1: 10.0.1.0/24

Internet gateway

Availability Zone B

Public subnet 2: 10.0.2.0/24

Security group

Web server

Private subnet 2: 10.0.3.0/24

Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

~ 30 minutes

Begin Lab 2: Build Your VPC and Launch a Web Server

Lab debrief:
Key takeaways

Module 5: Networking and Content Delivery

Section 5: Amazon Route 53
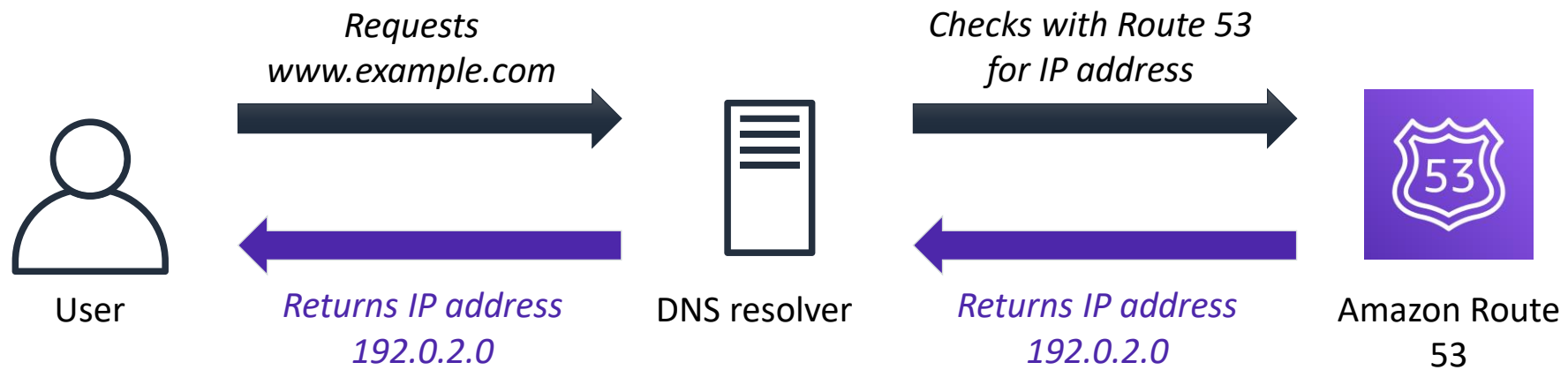
aws academy

Amazon Route 53

Amazon Route 53

- Is a highly available and scalable Domain Name System (DNS) web service
- Is used to route end users to internet applications by translating names (like www.example.com) into numeric IP addresses (like *192.0.2.1*) that computers use to connect to each other
- Is fully compliant with IPv4 and IPv6
- Connects user requests to infrastructure running in AWS and also outside of AWS
- Is used to check the health of your resources
- Features traffic flow
- Enables you to register domain names

Amazon Route 53 DNS resolution

Requests
www.example.com

Checks with Route 53
for IP address

User

*Returns IP address
192.0.2.0*

DNS resolver

*Returns IP address
192.0.2.0*
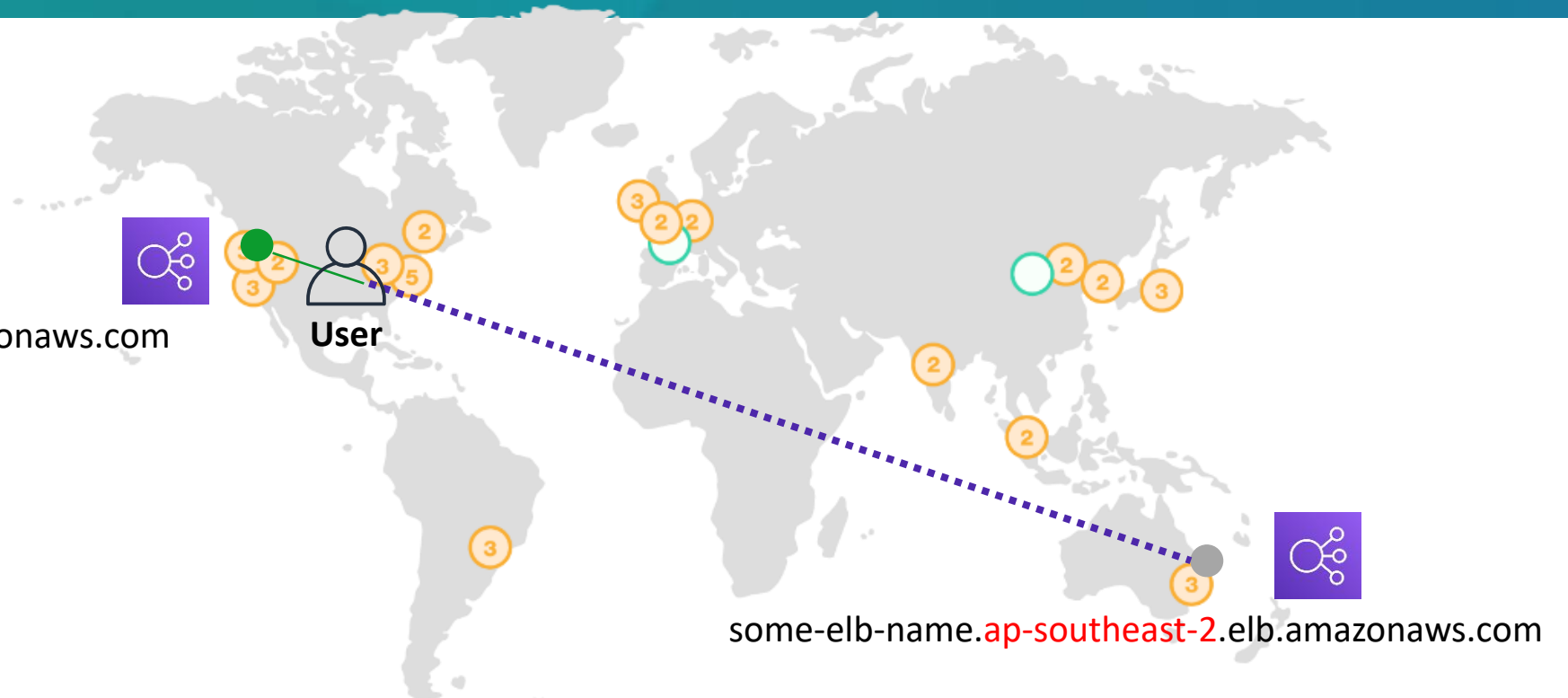
Amazon Route
53

Amazon Route 53 supported routing

- **Simple routing** – Use in single-server environments

- **Weighted round robin routing** – Assign weights to resource record sets to specify the frequency

- **Latency routing** – Help improve your global applications

- **Geolocation routing** – Route traffic based on location of your users

- **Geoproximity routing** – Route traffic based on location of your resources

- **Failover routing** – Fail over to a backup site if your primary site becomes unreachable

- **Multivalue answer routing** – Respond to DNS queries with up to eight healthy records selected at random

Use case: Multi-region deployment

Amazon Route 53

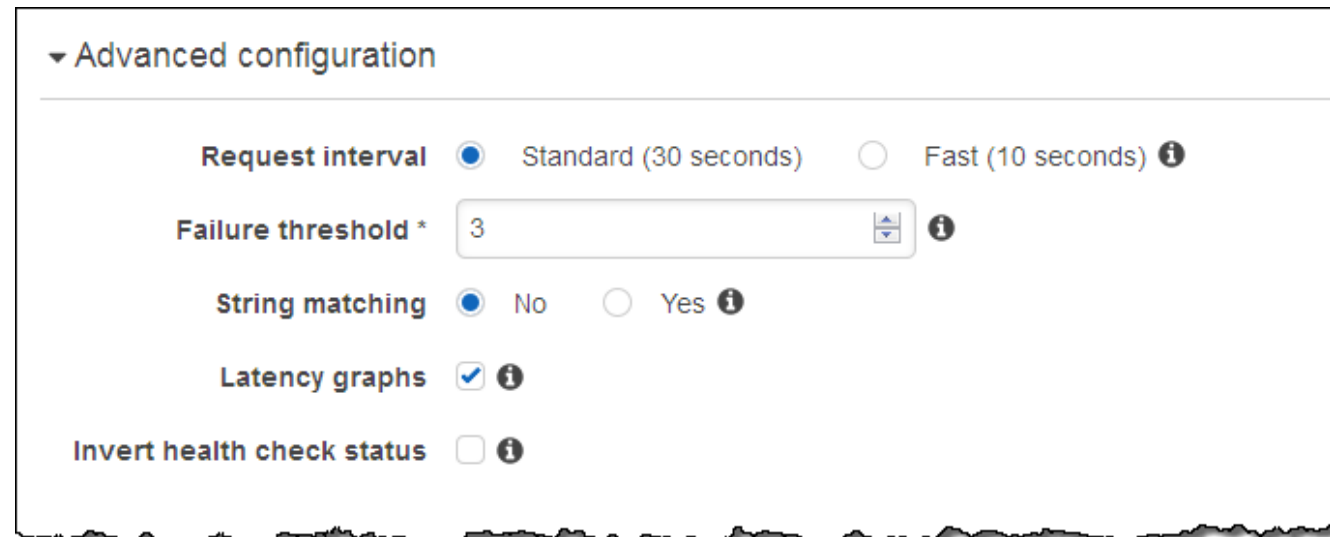some-elb-name.us-west-2.elb.amazonaws.com

User

some-elb-name.ap-southeast-2.elb.amazonaws.com

Name	Type	Value
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

Amazon Route 53 DNS failover

Improve the availability of your applications that run on AWS by:

- Configuring backup and failover scenarios for your own applications

- Enabling highly available multi-region architectures on AWS

- Creating health checks

DNS failover for a multi-tiered web application

Record Sets
CNAME www

elastic_load_balancer
Routing Policy = Failover
Record Type = Primary

Amazon S3 website
Routing Policy = Failover
Record Type = Secondary

User

Amazon Route
53

Primary

Secondary

Amazon S3
static website

aws AWS Cloud

Availability Zone A   Availability Zone B

Auto Scaling group

Amazon EC2   Amazon EC2

Amazon RDS   Amazon RDS

Amazon Relational   Amazon Relational
Database Service   Database Service
(Amazon RDS)   (Amazon RDS)
instance   instance

Section 5 key takeaways

- Amazon Route 53 is a highly available and scalable cloud DNS web service that translates domain names into numeric IP addresses.

- Amazon Route 53 supports several types of routing policies.

- Multi-Region deployment improves your application's performance for a global audience.

- You can use Amazon Route 53 failover to improve the availability of your applications.

Module 5: Networking and Content Delivery

Section 6: Amazon CloudFront

aws academy

Content delivery and network latency
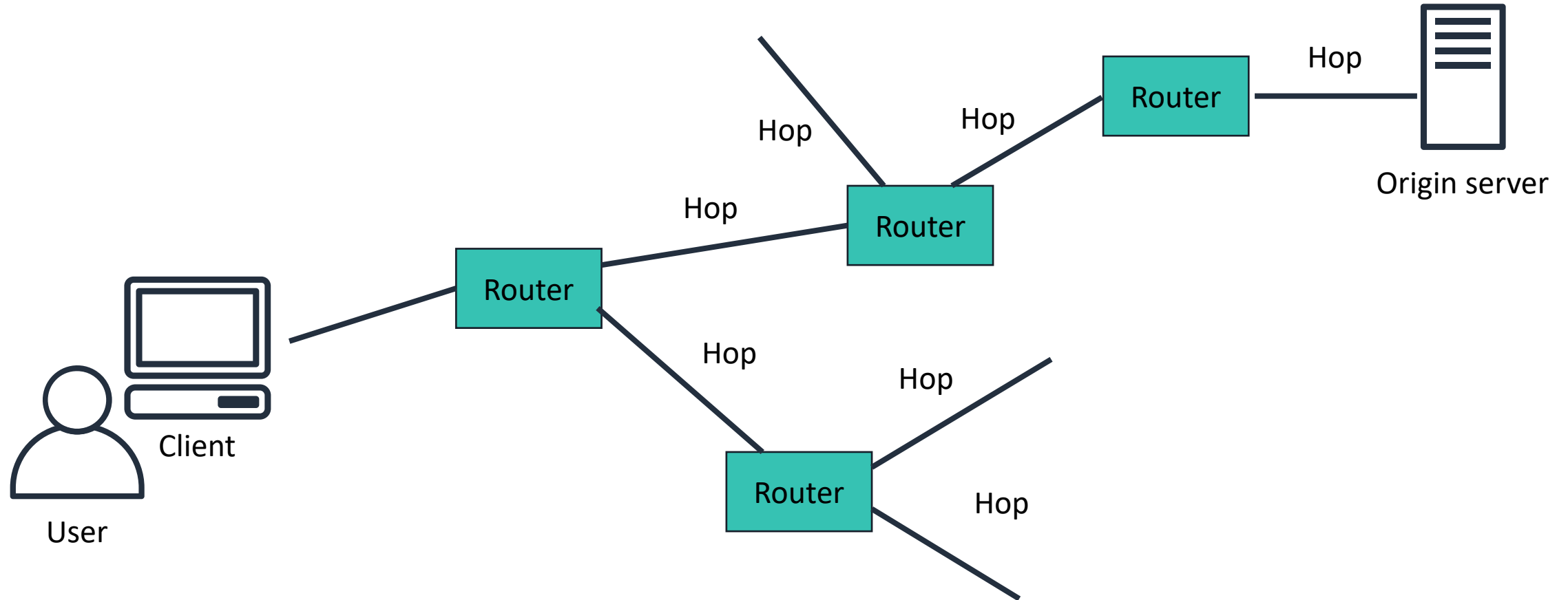
Content delivery network (CDN)

- Is a globally distributed system of caching servers

- Caches copies of commonly requested files (static content)

- Delivers a local copy of the requested content from a nearby cache edge or Point of Presence

- Accelerates delivery of dynamic content

- Improves application performance and scaling

Amazon CloudFront

Amazon CloudFront

- Fast, global, and secure CDN service
- Global network of edge locations and Regional edge caches
- Self-service model
- Pay-as-you-go pricing

Amazon CloudFront infrastructure

- 🔵 Edge locations
- 🟣 Multiple edge locations
- 🟠 Regional edge caches

- **Edge locations –** Network of data centers that CloudFront uses to serve popular content quickly to customers.

- **Regional edge cache –** CloudFront location that caches content that is not popular enough to stay at an edge location. It is located between the origin server and the global edge location.
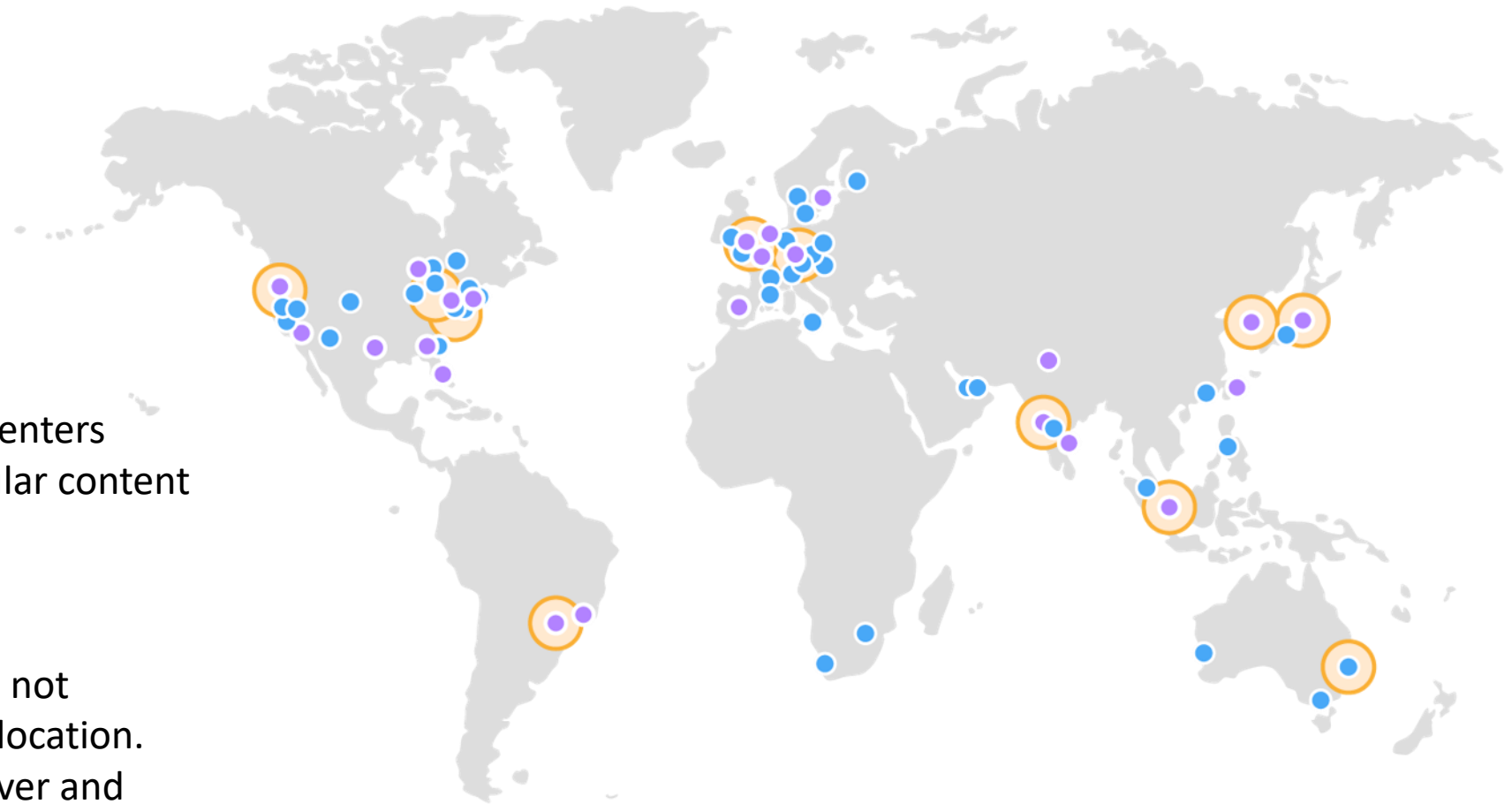
Amazon CloudFront benefits

- Fast and global

- Security at the edge

- Highly programmable

- Deeply integrated with AWS

- Cost-effective

Amazon CloudFront pricing

Data transfer out

- Charged for the volume of data transferred out from Amazon CloudFront edge location to the internet or to your origin.

HTTP(S) requests

- Charged for number of HTTP(S) requests.

Invalidation requests

- No additional charge for the first 1,000 paths that are requested for invalidation each month. Thereafter, $0.005 per path that is requested for invalidation.

Dedicated IP custom SSL

- $600 per month for each custom SSL certificate that is associated with one or more CloudFront distributions that use the Dedicated IP version of custom SSL certificate support.

Section 6 key takeaways

- A CDN is a globally distributed system of caching servers that accelerates delivery of content.

- Amazon CloudFront is a fast CDN service that securely delivers data, videos, applications, and APIs over a global infrastructure with low latency and high transfer speeds.

- Amazon CloudFront offers many benefits.

Module 5: Networking and Content Delivery

Module wrap-up

aws academy

Module summary

In summary, in this module you learned how to:

- Recognize the basics of networking

- Describe virtual networking in the cloud with Amazon VPC

- Label a network diagram

- Design a basic VPC architecture

- Indicate the steps to build a VPC

- Identify security groups

- Create your own VPC and added additional components to it to produce a customized network

- Identify the fundamentals of Amazon Route 53

- Recognize the benefits of Amazon CloudFront

Complete the knowledge check

Sample exam question

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 VPC

Additional resources

- Amazon VPC overview page

- Amazon Virtual Private Cloud Connectivity Options whitepaper

- One to Many: Evolving VPC Design AWS Architecture blog post

- Amazon VPC User Guide

- Amazon CloudFront overview page

Thank you

aws academy