AWS Academy Cloud Foundations

Module 5: Networking and Content Delivery

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

aws academy

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

Networks

Number System

Protocol

IP Addressing

Networks

Number System :-

- Decimal
- Roman
- Binary
- Octal
- HexaDecimal

Networks

0 1 2 3 4 5 6 7 8 9 A B C D E F - Hexadecimal

0 1 - Binary

0	10	100
1	11	101
		110
		111

0	0	10	10	20	20	90	
1	1	11	11	21	21	91	100
2	2	12	12	2	12	92	101
3	3	13	13	3	13	93	102
4	4	14	14	4	14	94	103
5	5	15	15	5	15	95	4
6	6	16	16	6	16	96	5
7	7	17	17	7	27	97	6
8		18		8		98	7
9		19		29		99	8
							109

aws academy

Conversion of Number from one number system to another

- Decimal to Binary
- Binary to Decimal

Networks

Protocol

Network protocols:

- TCP/IP - DOD
- IPx/SPx - Novell
- AppleTalk - Apple
- NetBIOS - Microsoft
- OSI – ISO

IP addresses

192	.	0	.	2	.	0
↓		↓		↓		↓
11000000		00000000		00000010		00000000

IP addresses

Range of IP Address

RANGE OF IPv4 ADDRESS

Taking example as all 0's and all 1's

0 0 0 0 0 0 0 0 = 0

0 0 0 0 0 0 0 1 = 1

0 0 0 0 0 0 1 0 = 2

0 0 0 0 0 0 1 1 = 3

0 0 0 0 0 1 0 0 = 4

1 1 1 1 1 1 1 1 = 255

Total IP Address Range: 0.0.0.0 to 255.255.255.255

IPv4 and IPv6 addresses

IPv4 (32-bit) address: 192.0.2.0

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

IP Address Classification

IP ADDRESS CLASSIFICATION

IP ADDRESS are divided into 5 classes

CLASS A 0 - 127
CLASS B 128 - 191
CLASS C 192 - 223
CLASS D 224 – 239
CLASS E 240 – 255
CLAS A, B, C used in LAN & WAN
CLASS D reserved for multicasting
CLASS E reserved for research & development and for future use

Public IP address And Private IP Address

- Public IP Address

- External (global) reach
- Used for communicating outside your private network, over the internet
- A unique numeric code never reused by other devices
- Found by Googling: "What is my IP address?“
- Assigned and controlled by your internet service provider
- Not free

- Private IP Address

- Internal (local) reach
- Used for communicating within your private network, with other devices in your home or office
- A non-unique numeric code that may be reused by other devices in other private networks
- Found via your device’s internal settings
- Assigned to your specific device within a private network

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

Private IP address Class

NETWORK AND HOST PORTIONS

IP Address is divided into Network & Host Portion.

CLASS A	N.H.H.H
CLASS B	N.N.H.H
CLASS C	N.N.N.H

Host: specific a device in the network.
Network: set of devices

Private IP address Class

aws academy

PRIVATE IP ADDRESS

There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.

CLASS A

10.0.0.0 to 10.255.255.255 (10.X.X.X)

CLASS B

172.16.0.0 to 172.31.255.255

CLASS C

192.169.0.0 to 192.168.255.255 (192.168.X.X)

Classless Inter-Domain Routing (CIDR)

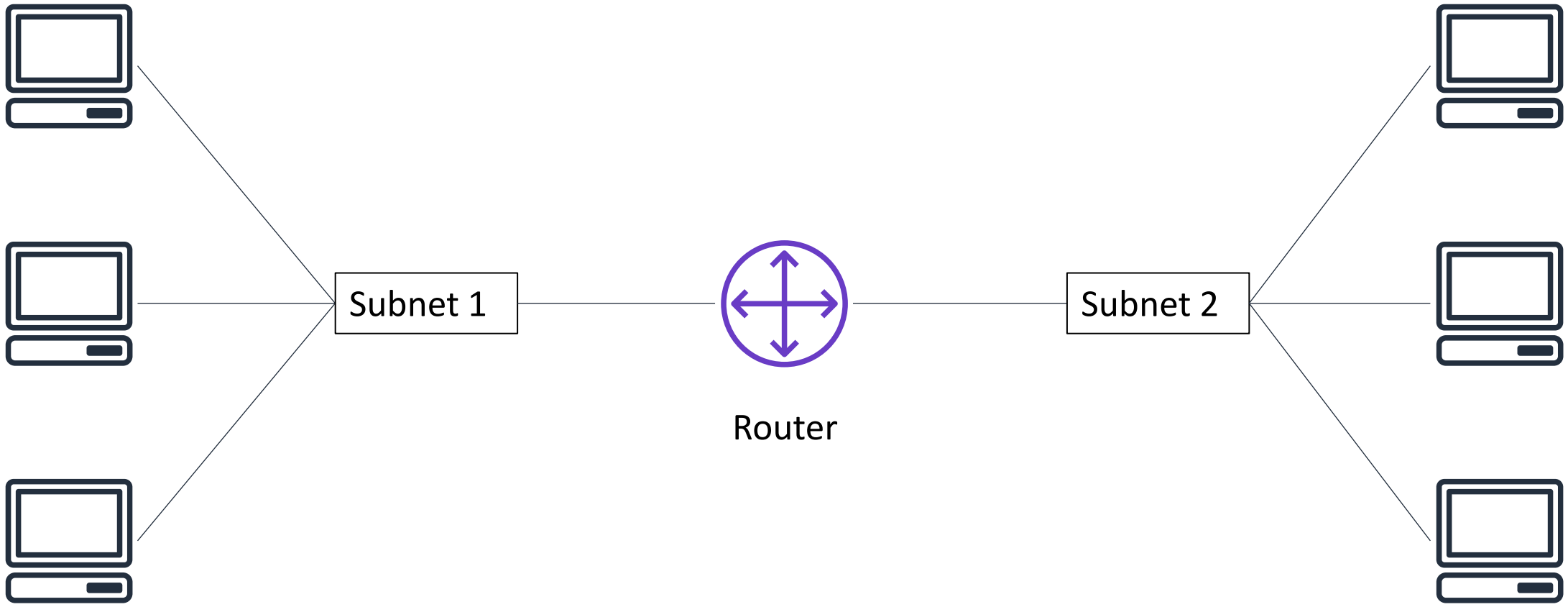
Network identifier (routing prefix) | Host identifier

192 . 0 . 2 . 0 / 24

192	0	2	0
11000000	00000000	00000010	00000000 to 11111111
Fixed	Fixed	Fixed	Flexible

Tells you how many bits are fixed

Networks



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

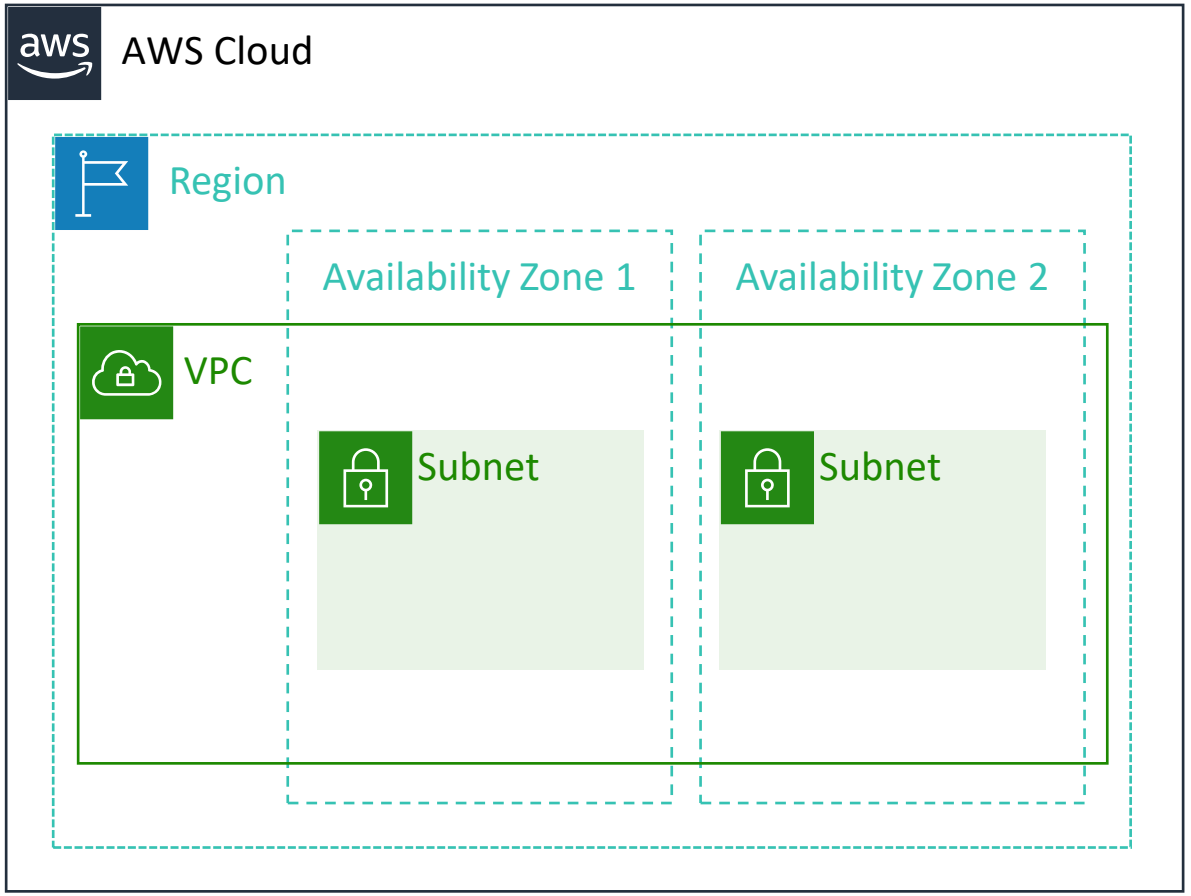
Amazon VPC

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**



IP addressing

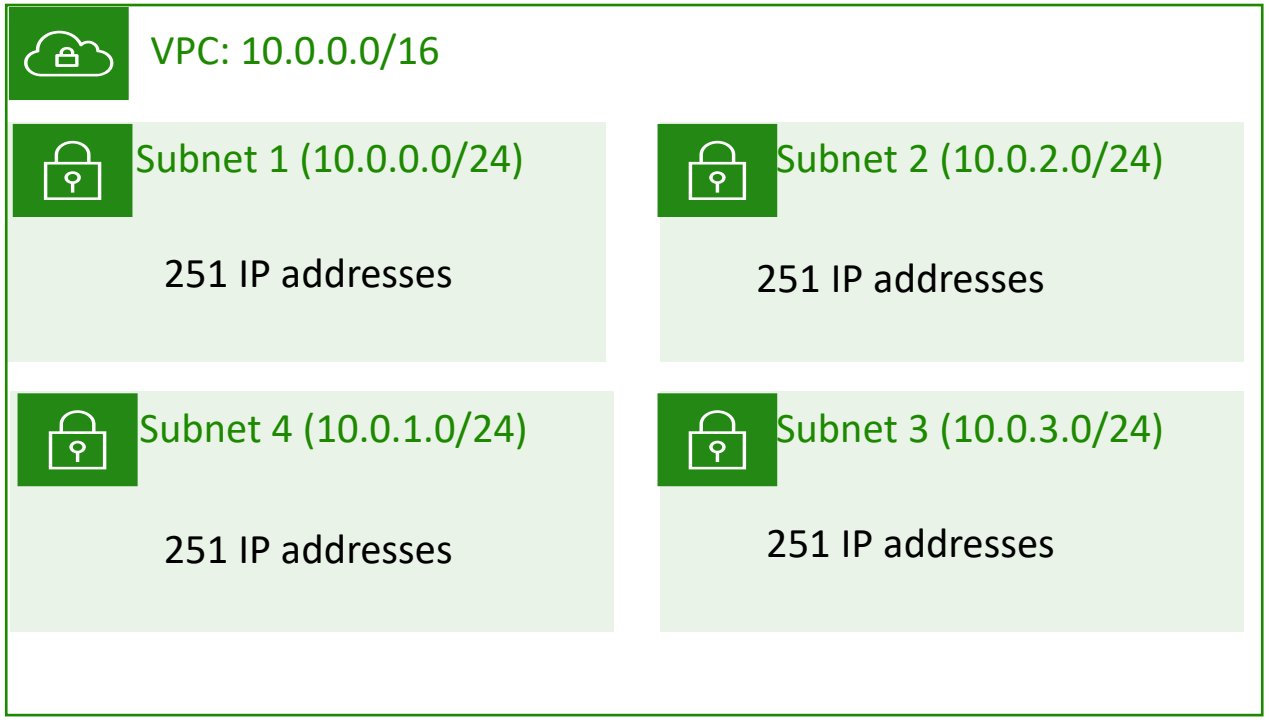
- When you create a VPC, you assign it to an IPv4 **CIDR block** (range of **private** IPv4 addresses).
- You **cannot change the address range** after you create the VPC.
- The **largest** IPv4 CIDR block size is **/16**.
- The **smallest** IPv4 CIDR block size is **/28**.
- IPv6 is also supported (with 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

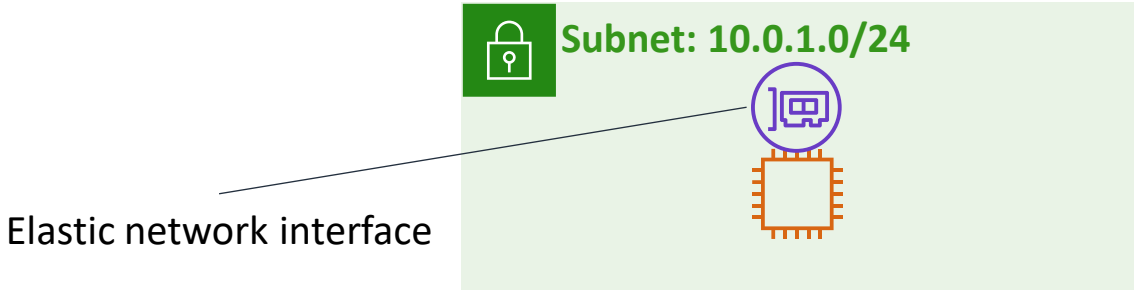
Example: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four equal-sized subnets. Only 251 IP addresses are available for use by each subnet.



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

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.



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

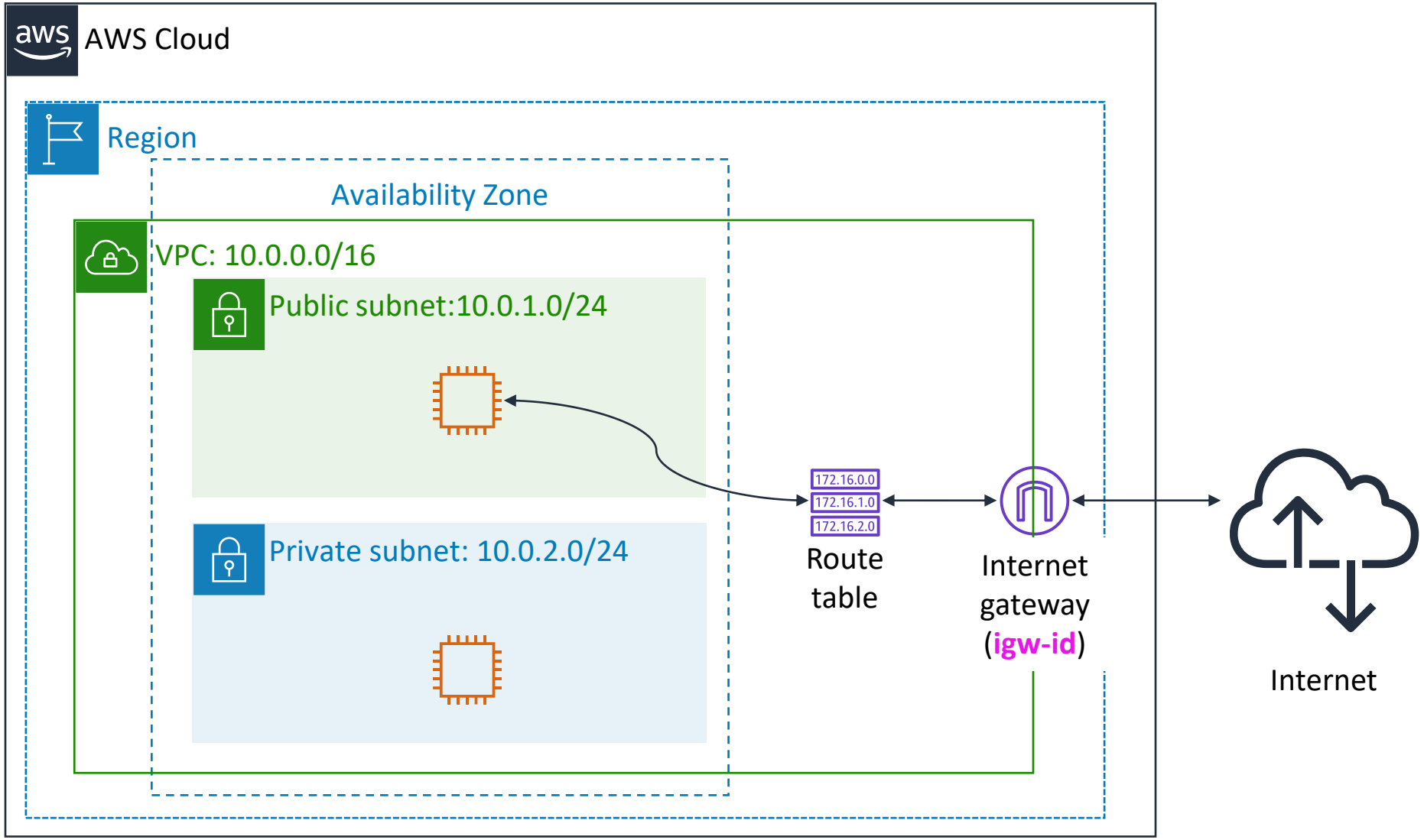
Section 2 key takeaways

- 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

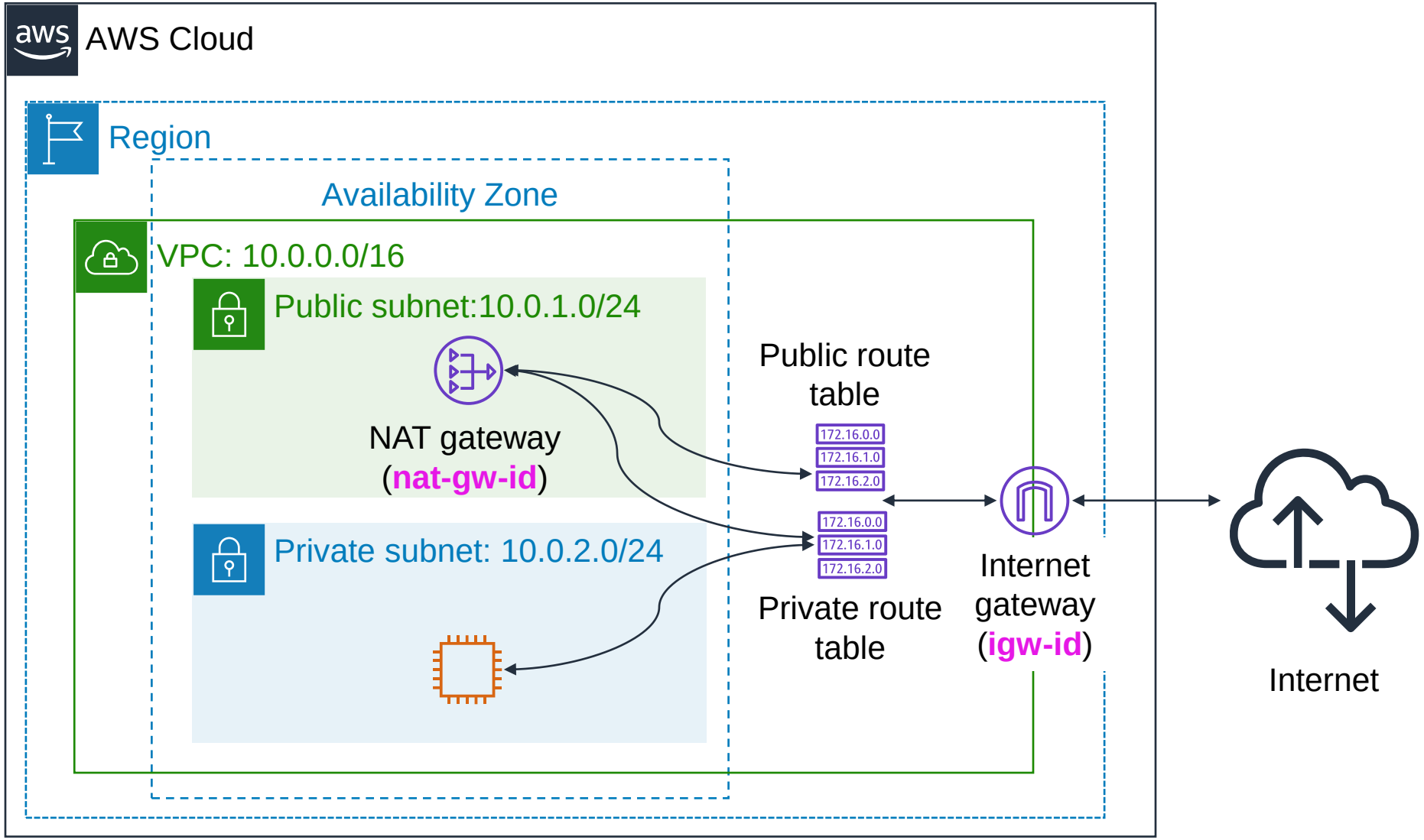
Internet gateway



Public Subnet Route Table

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

Network address translation (NAT) gateway



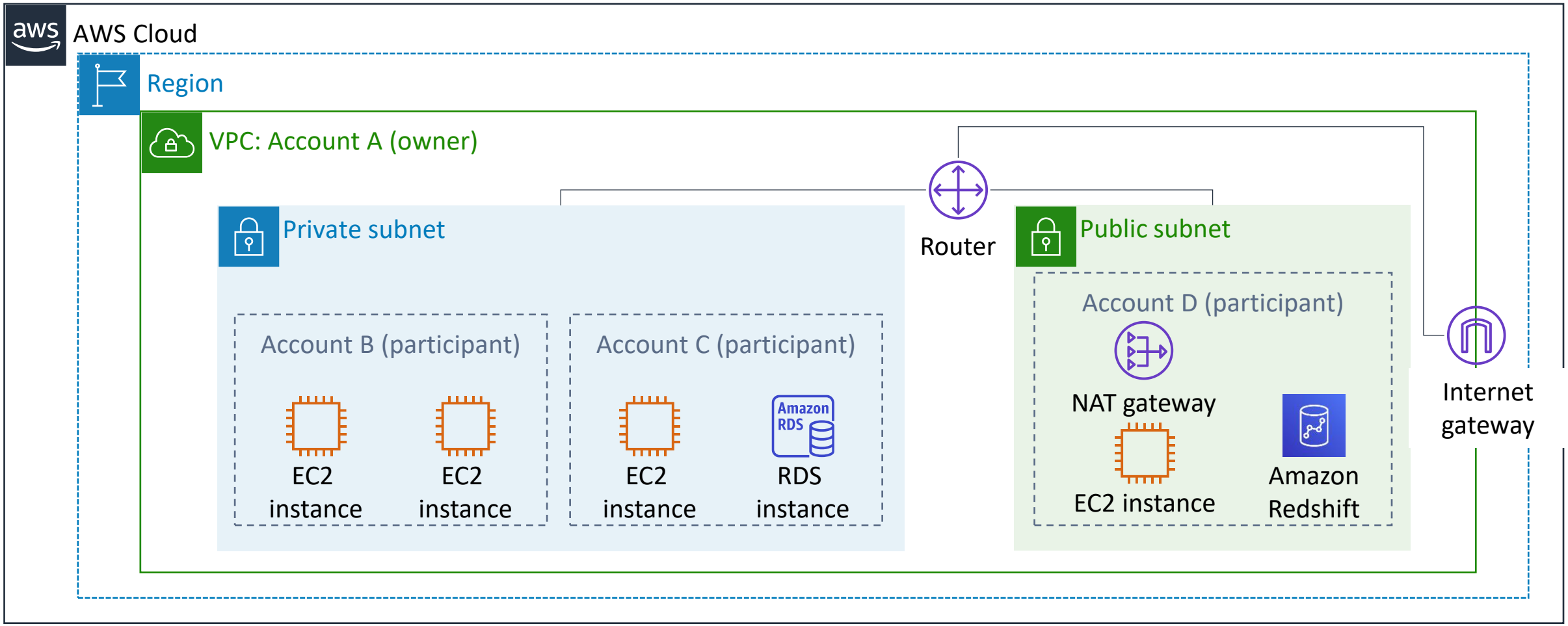
Public Subnet Route Table

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

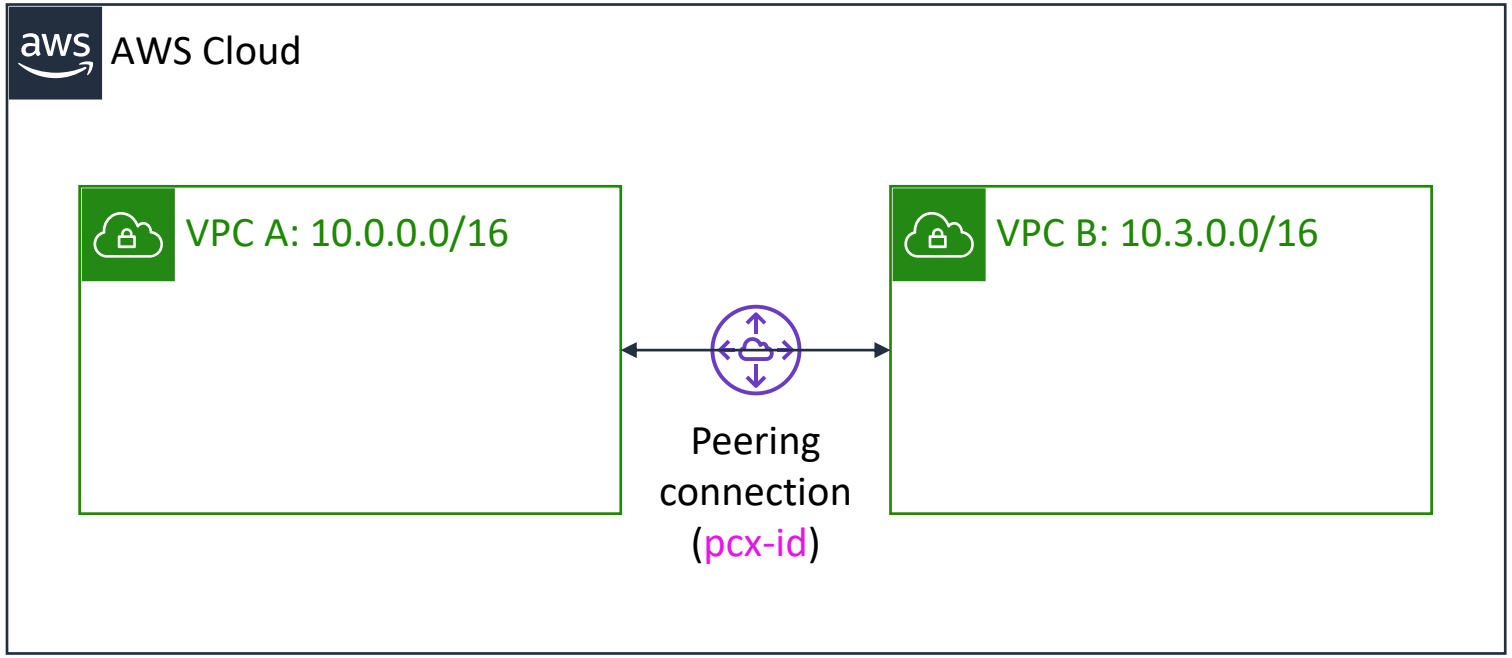
Private Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

VPC sharing



VPC peering



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

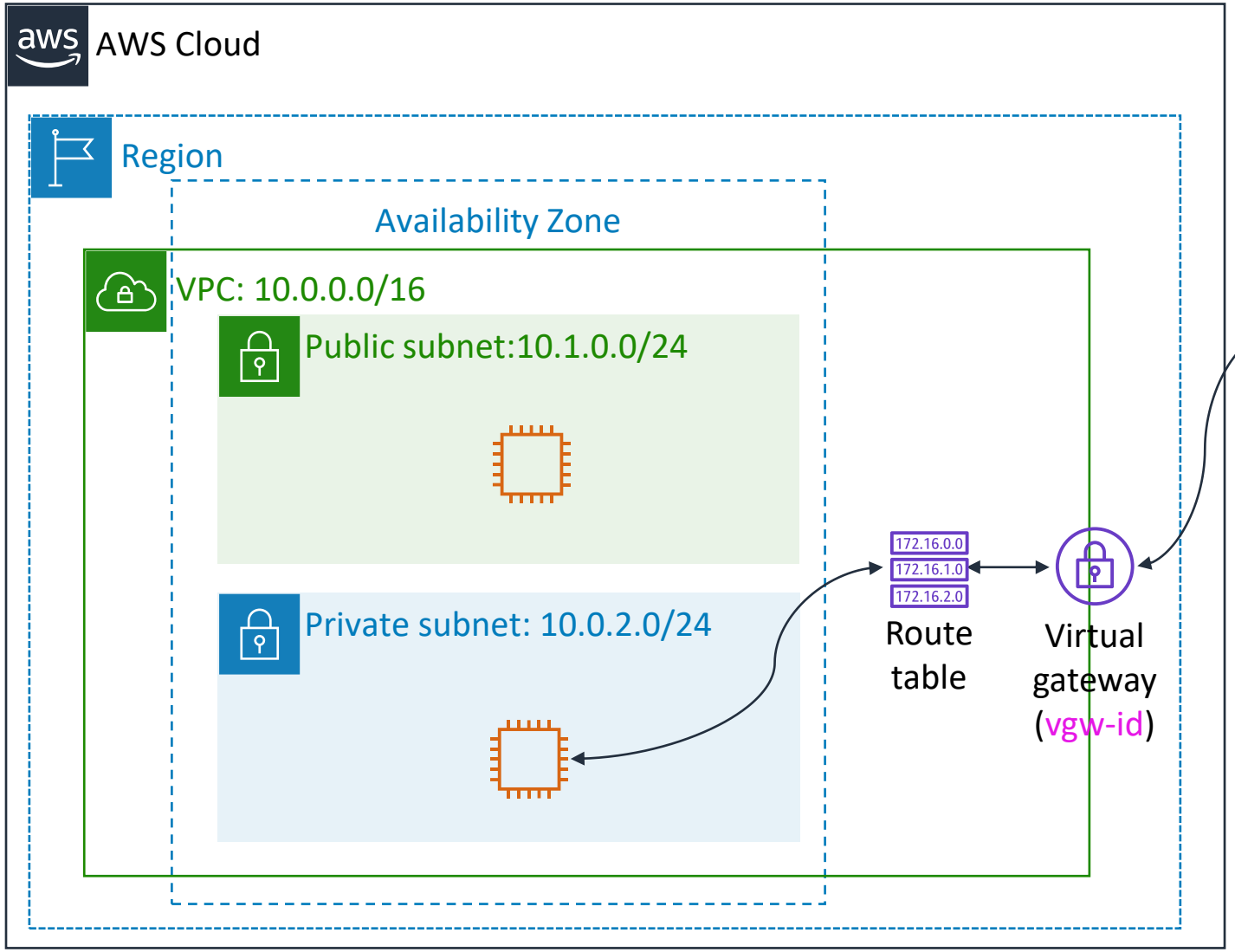
Destination	Target
10.3.0.0/16	local
10.0.0.0/16	pcx-id

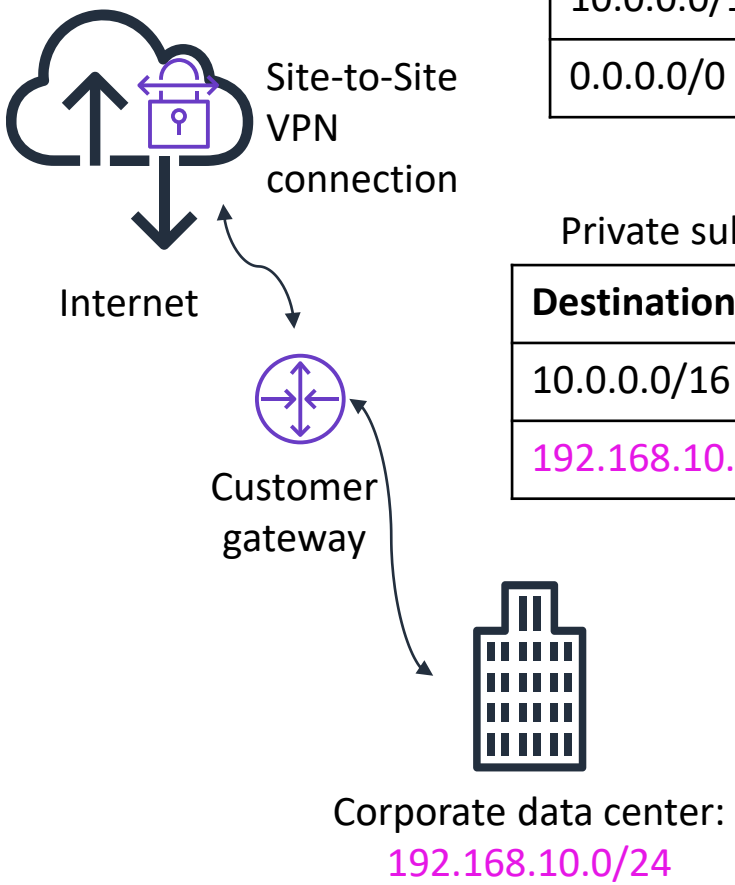
You can connect VPCs in your own AWS account, between AWS accounts, or between AWS Regions.

Restrictions:

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

AWS Site-to-Site VPN





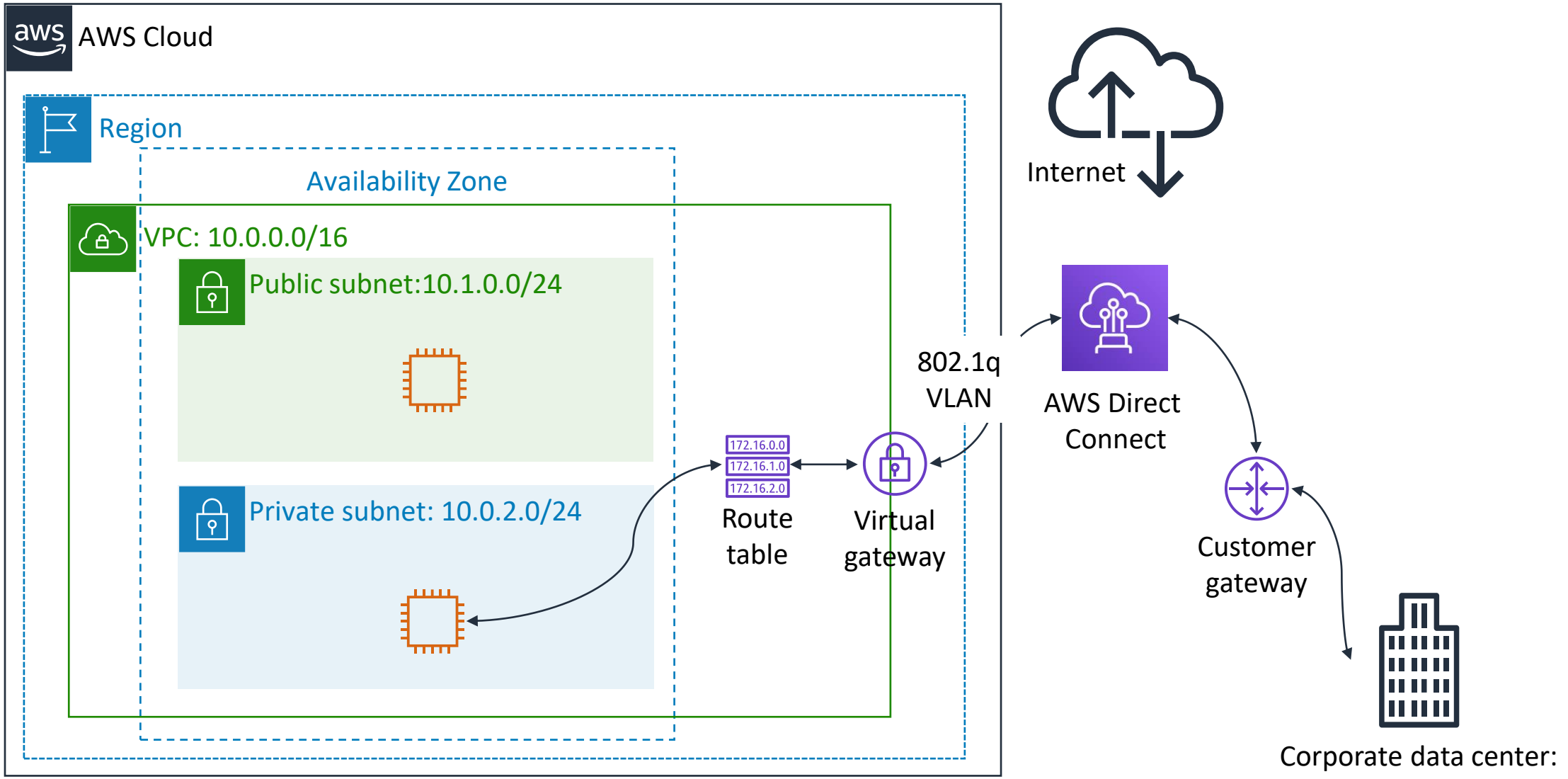
Public subnet route table

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

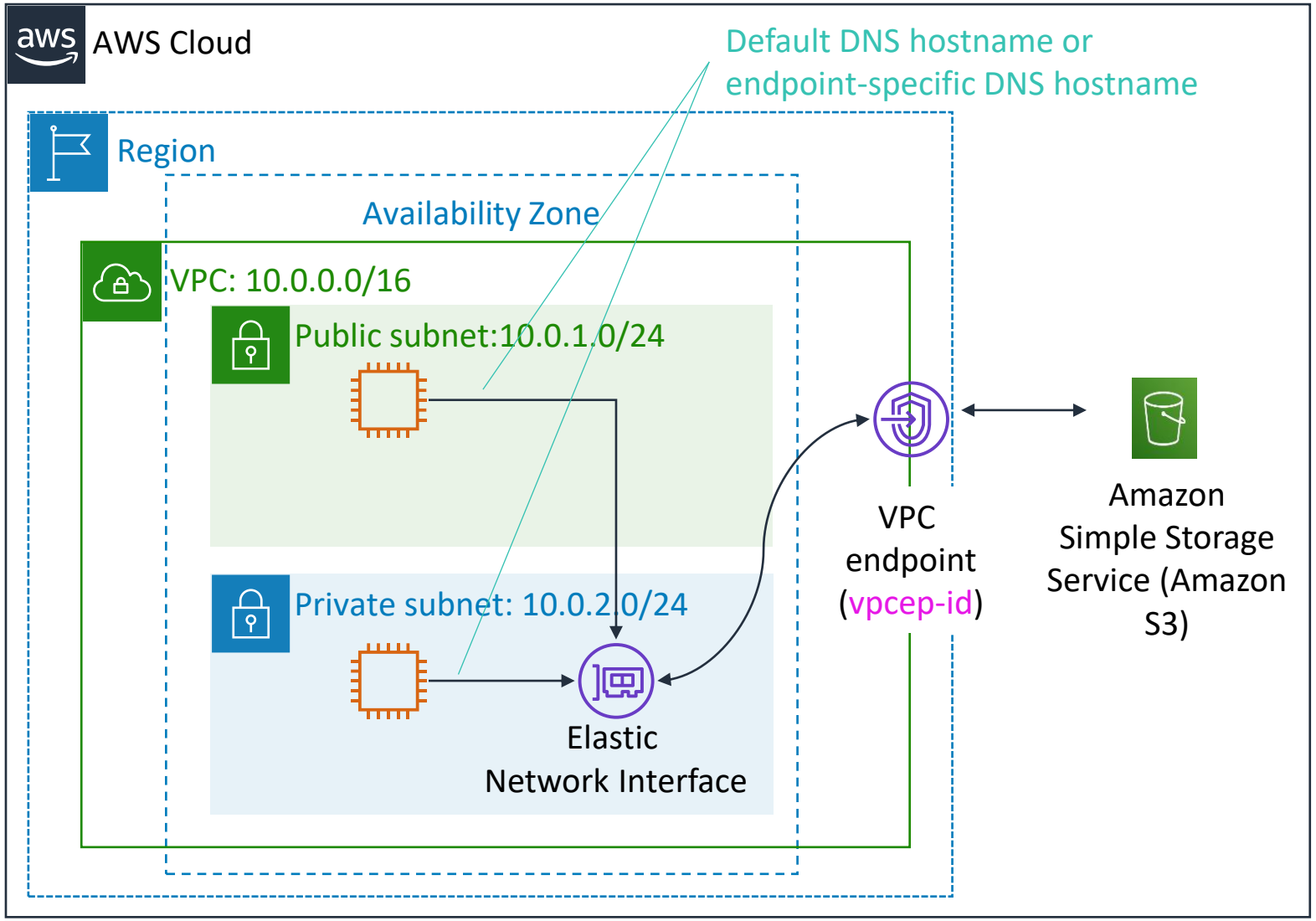
Private subnet route table

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

AWS Direct Connect



VPC endpoints



Public Subnet Route Table

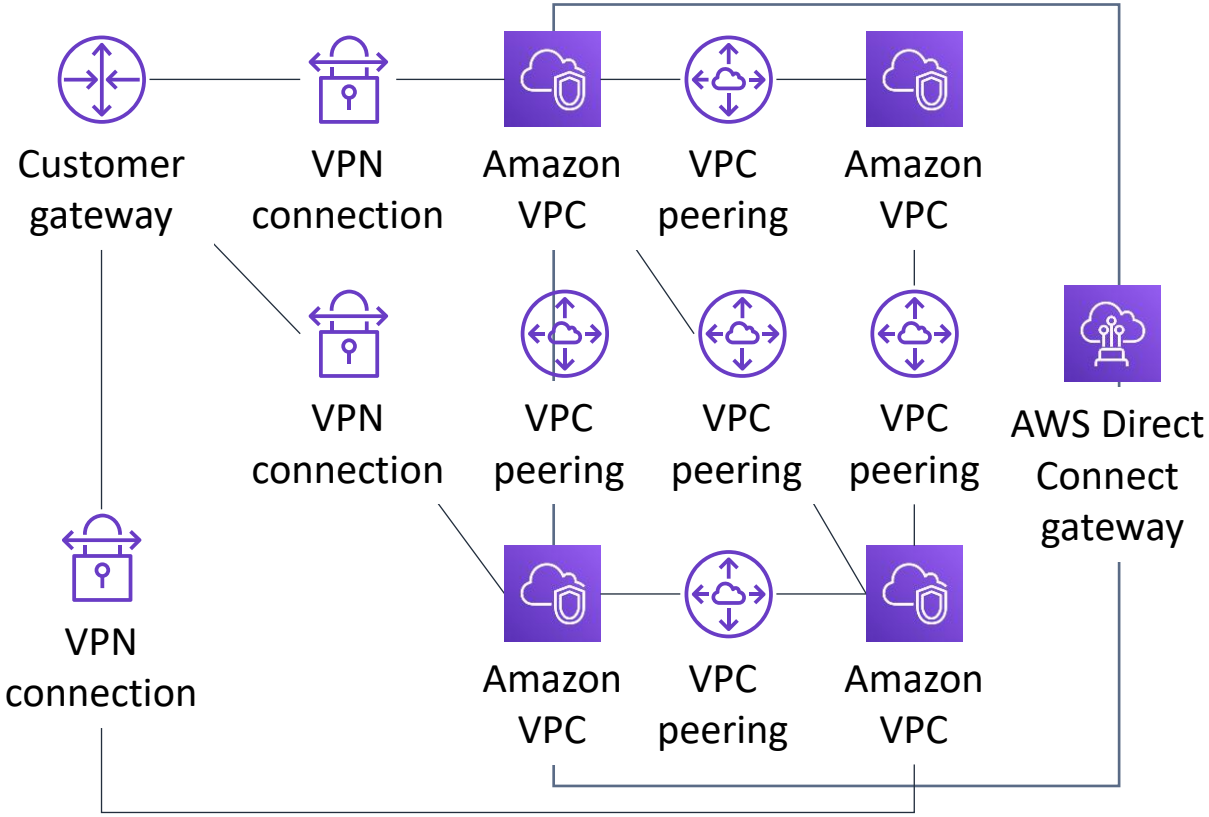
Destination	Target
10.0.0.0/16	local
Amazon S3 ID	vpcep-id

Two types of endpoints:

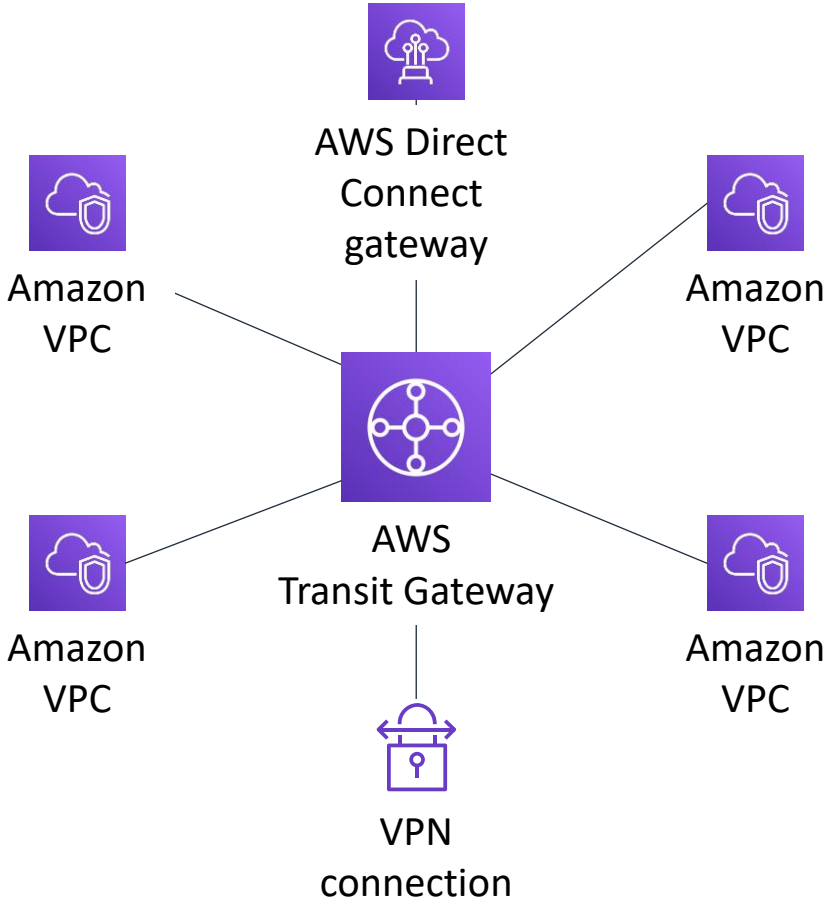
- **Interface** endpoints (powered by AWS PrivateLink)
- **Gateway** endpoints (Amazon S3 and Amazon DynamoDB)

AWS Transit Gateway

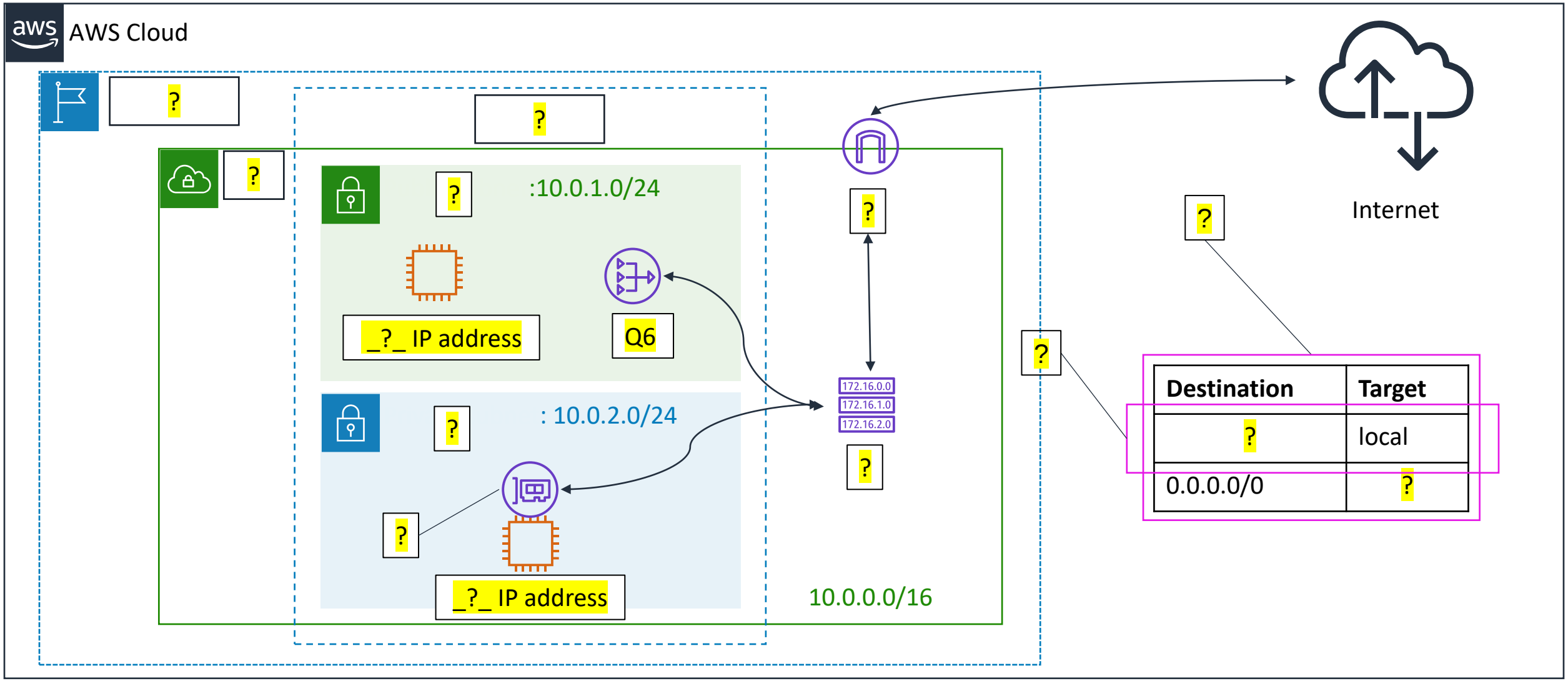
From this…



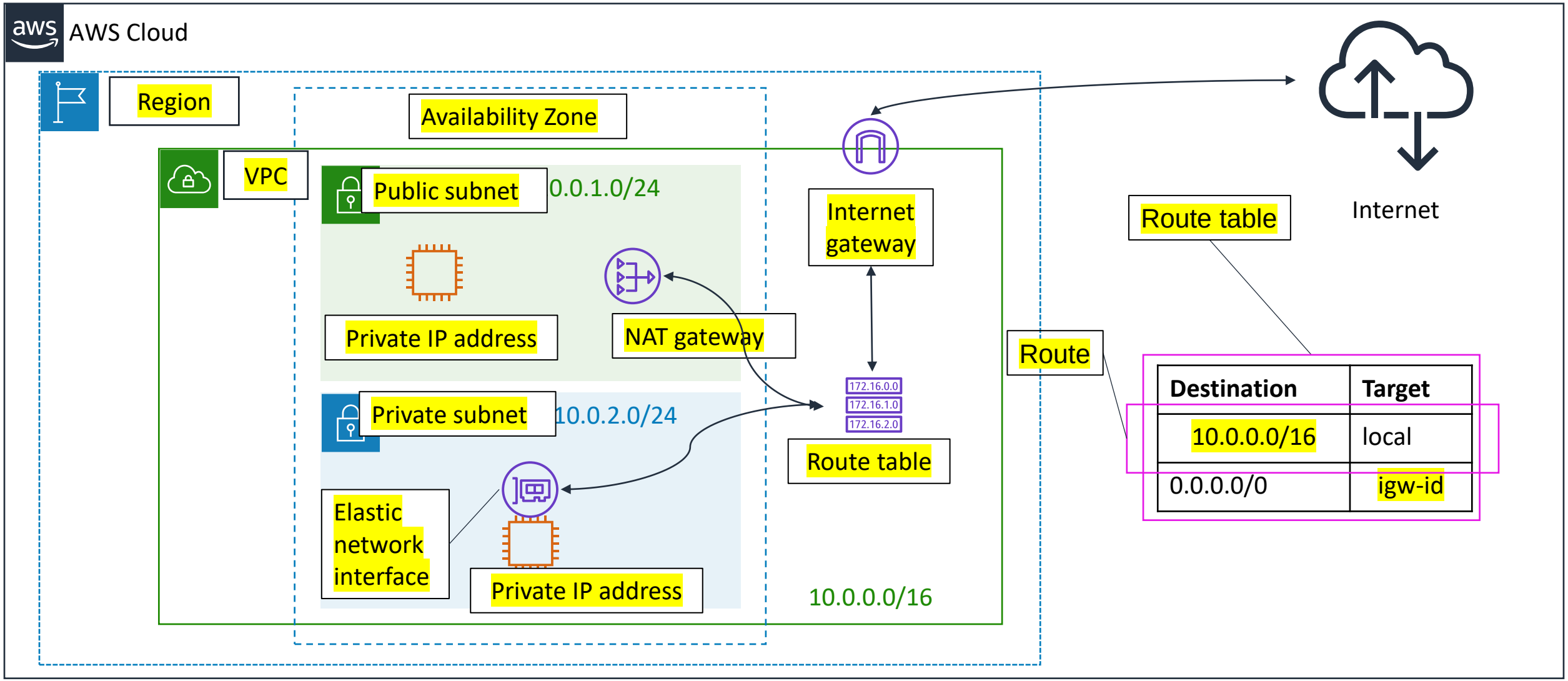
To this…



Activity: Label this network diagram



Activity: Solution



Recorded Amazon VPC demonstration

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.