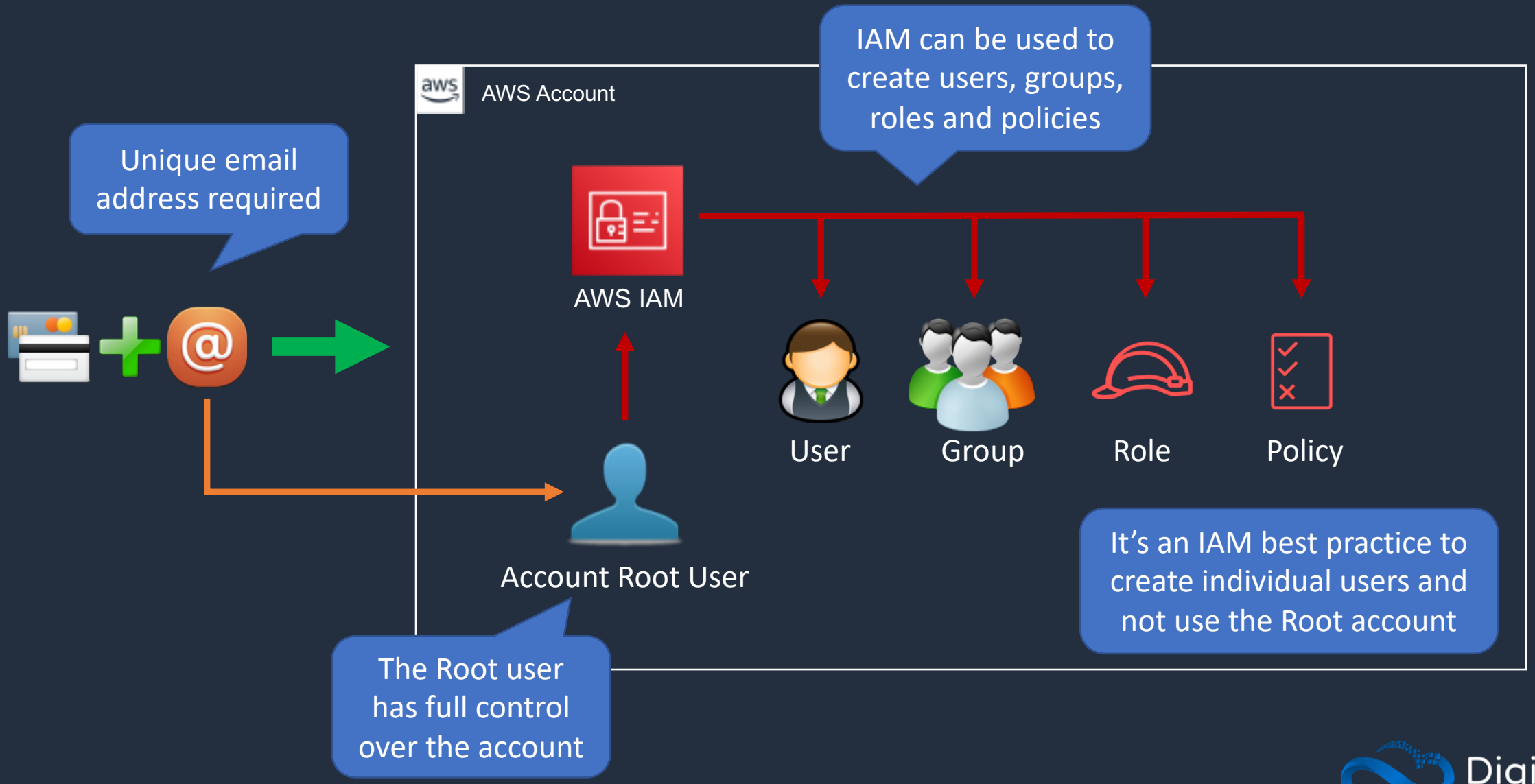
SECTION 2

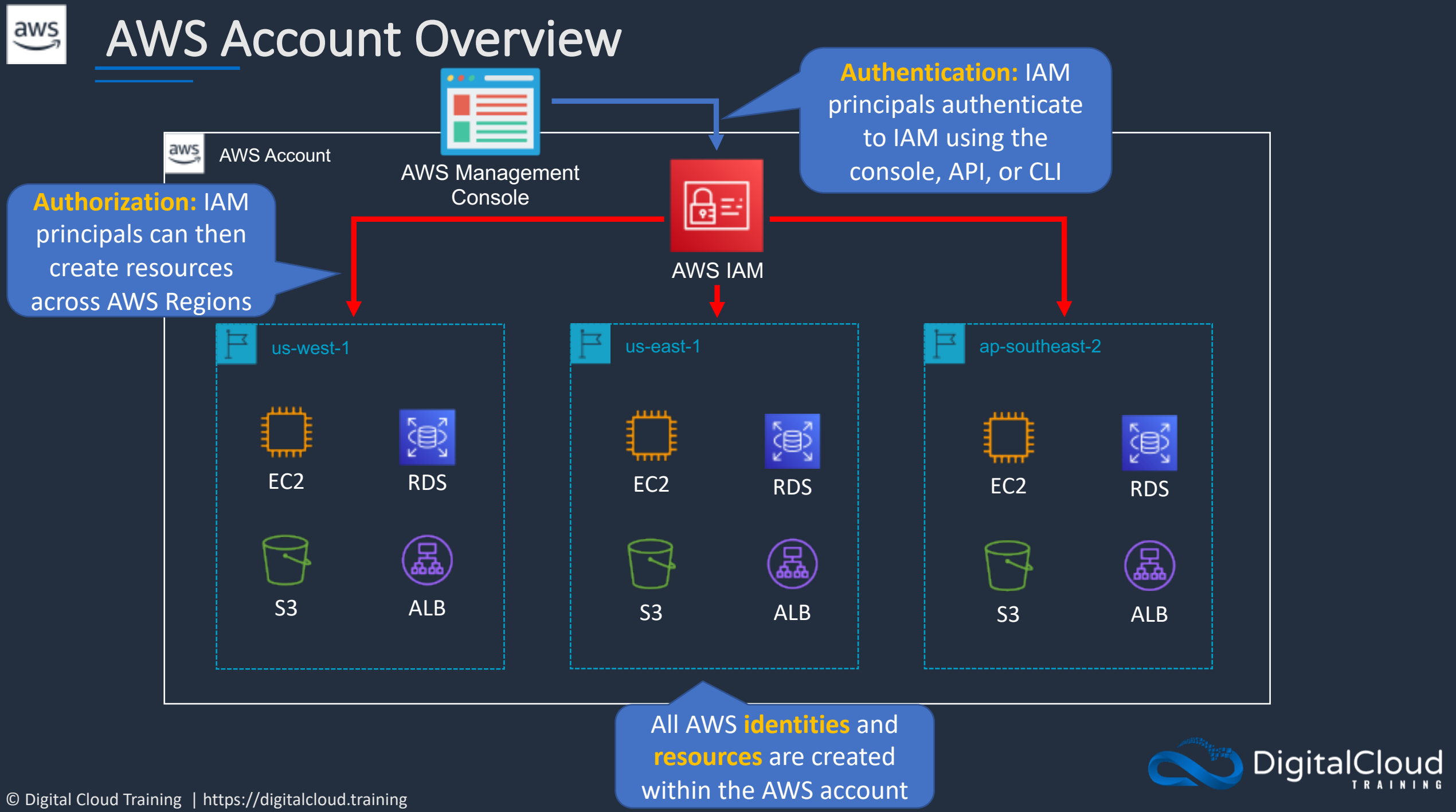
Getting Started – Setup AWS Account

AWS Account Overview

AWS Account Overview



AWS Account Overview



DigitalCloud TRAINING

Create Management AWS Account

What you need…

Credit card for setting up the account and paying any bills

Unique email address for this account

Check if you can use an alias with an existing email address (e.g dynamic aliases in Gmail / O365)

john@example.com

john+dctmanagement@example.com

john+dctprod@example.com

AWS account name – mine will be DCT-MANAGEMENT

Phone to receive an SMS verification code

Configure Account and Setup Billing Alarms

Install Tools (AWS CLI and VS Code)

SECTION 3

Networking Fundamentals

Networking in the Cloud

DigitalCloud TRAINING

Clients and Servers

Cloud Computing

Servers

Servers running in the cloud offer **services** which include the **application**, **processing** and **data storage**

Client devices are connected via the **Internet**

Cloud Networking

Client Devices

Client devices require connectivity via **wired**, **wireless** or **cellular** networks

DigitalCloud TRAINING

Connecting to Services

The client application finds the server by **IP address**

Web Server

Port: 80

Protocol: HTTP

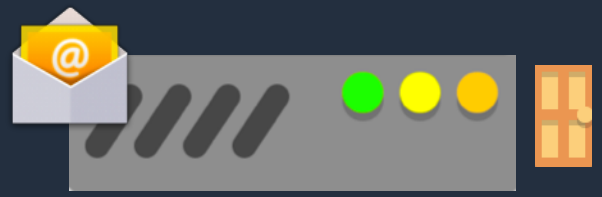
A **port** is like a door into the server

File Server

Port: 445

Protocol: SMB

SMB/CIFS is used by Microsoft file servers and clients



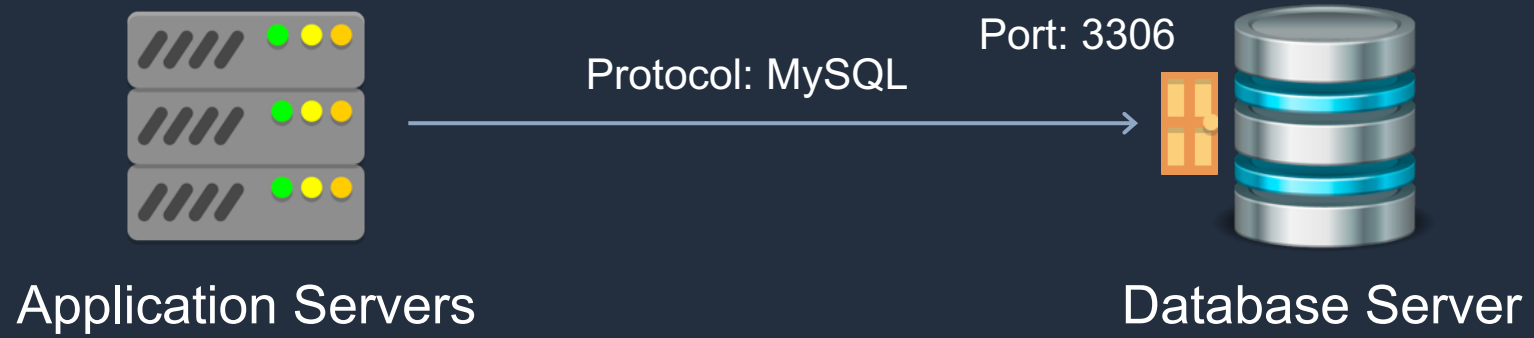
Email Server

Port: 25

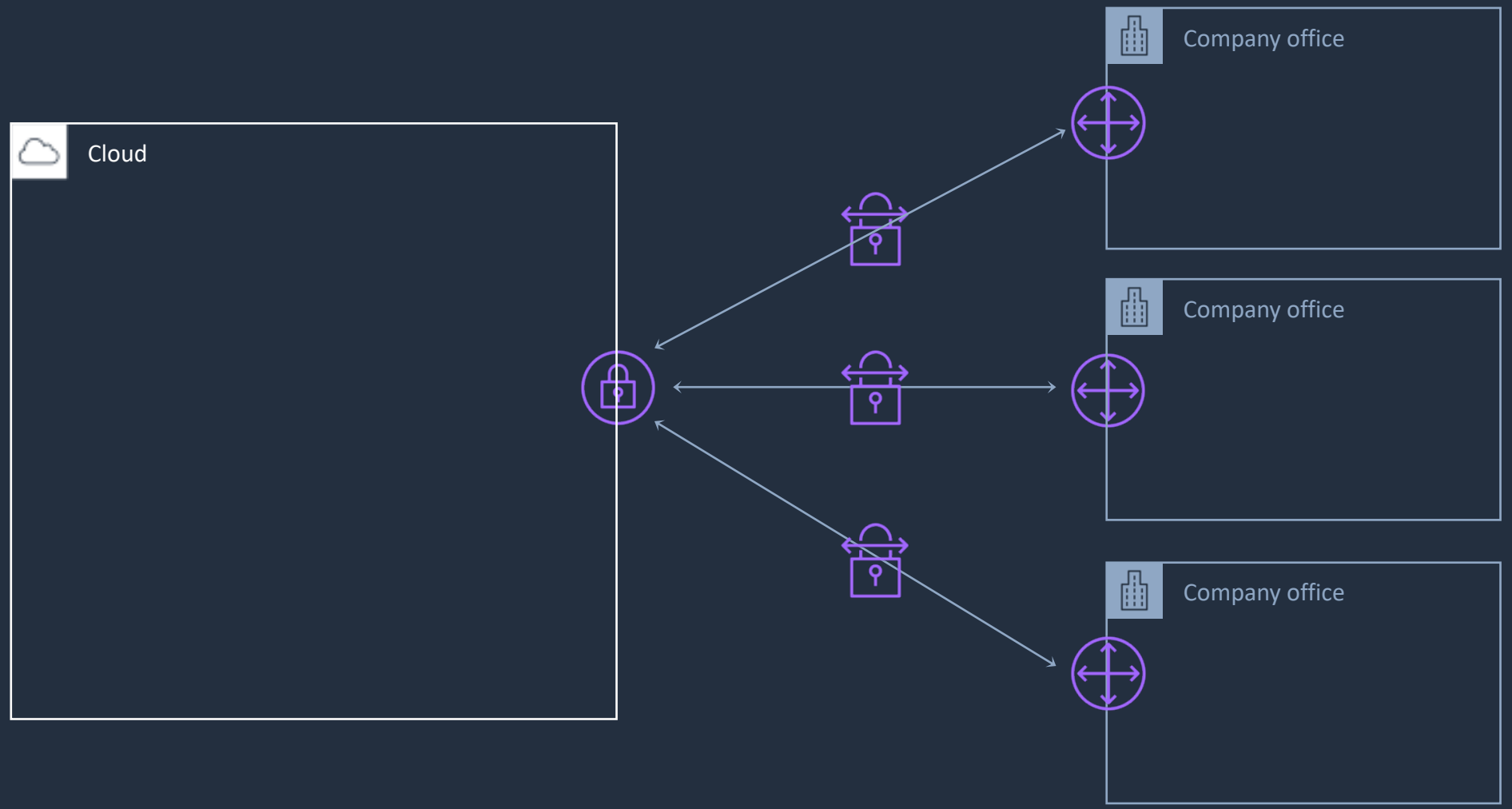
Protocol: SMTP

DigitalCloud TRAINING

Server to Server Connectivity

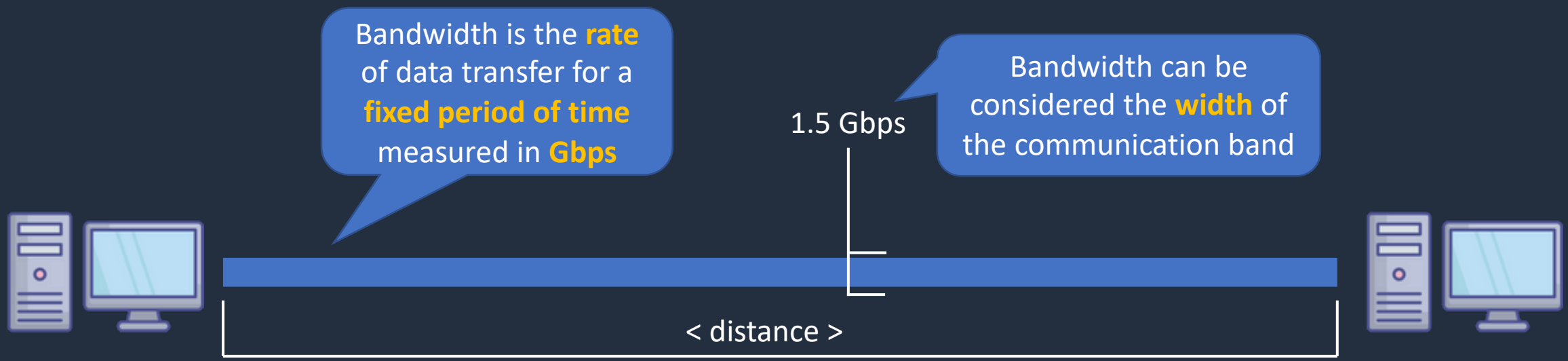


Site to Site Connectivity

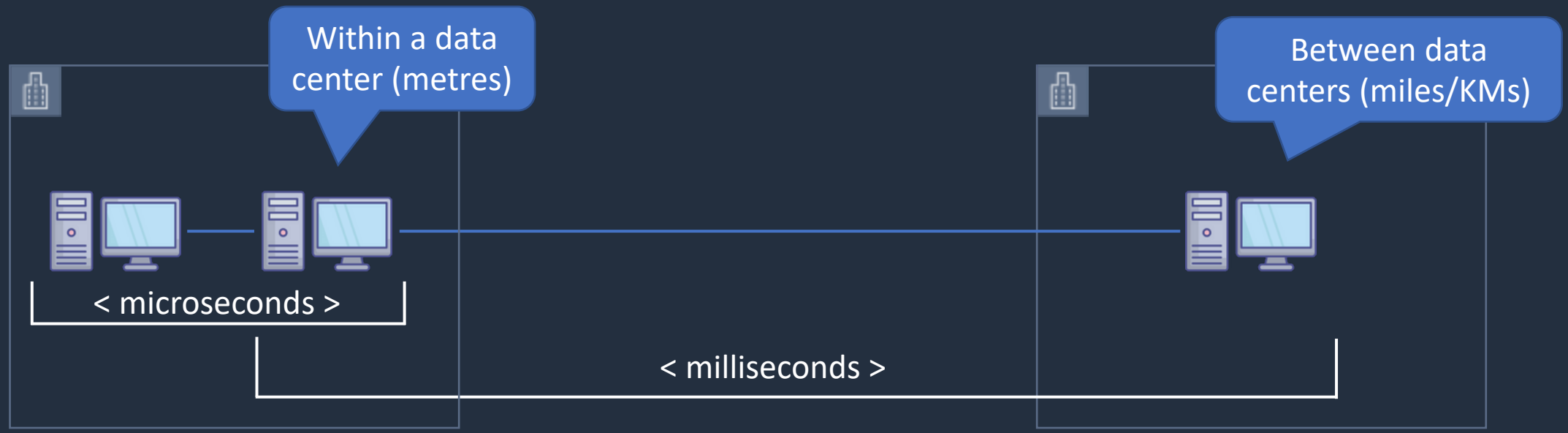


Bandwidth and Latency

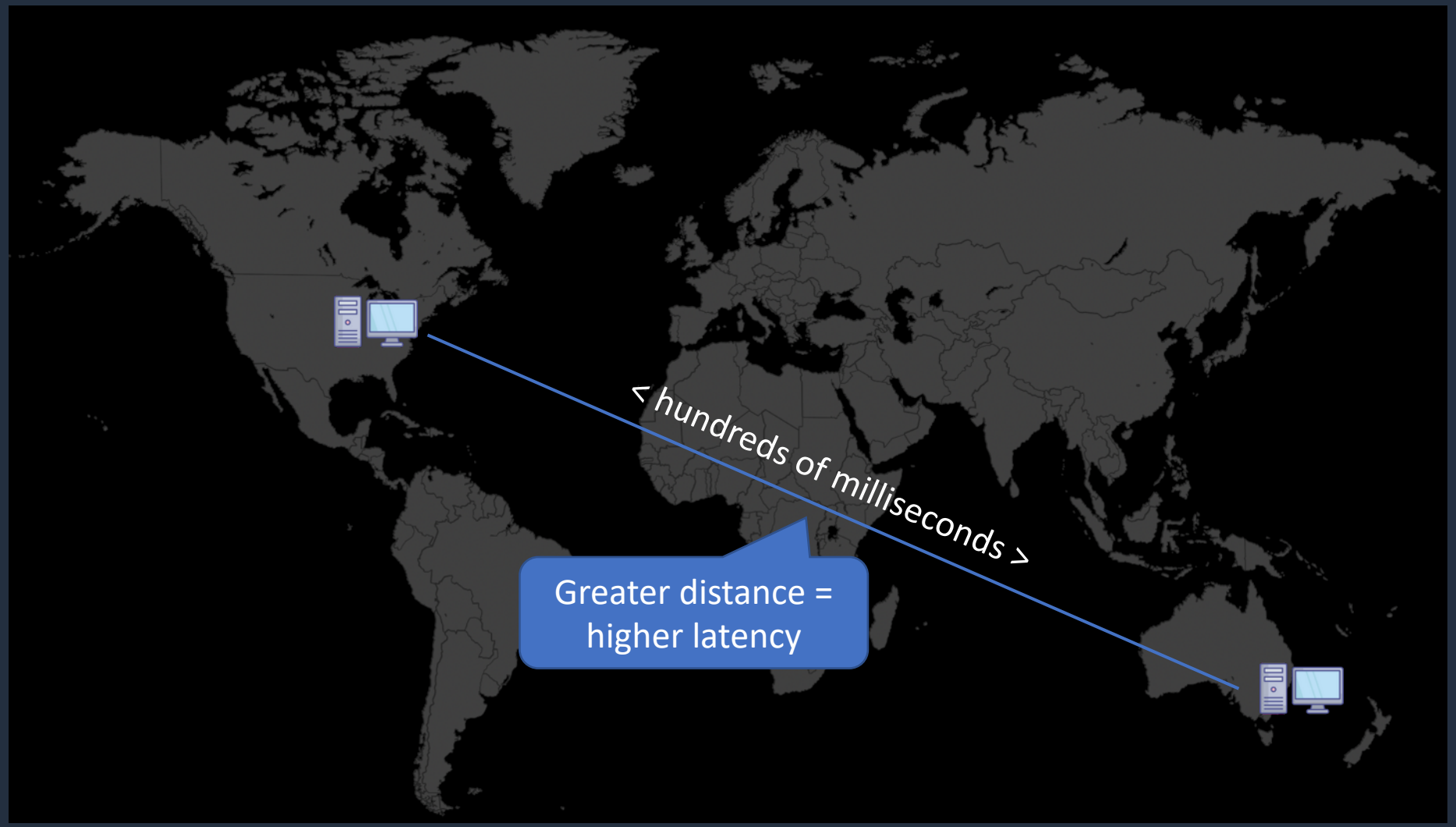
Bandwidth and Latency



Bandwidth and Latency



Bandwidth and Latency

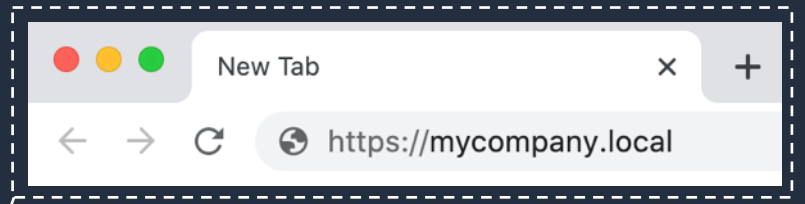


IP Addressing Basics (IPv4)

DigitalCloud TRAINING

IP Addressing Basics

User enters website address in browser



Name	Type	Value
mycompany.local	A	192.168.0.1
emailserver.local	A	192.168.0.2

DNS Server

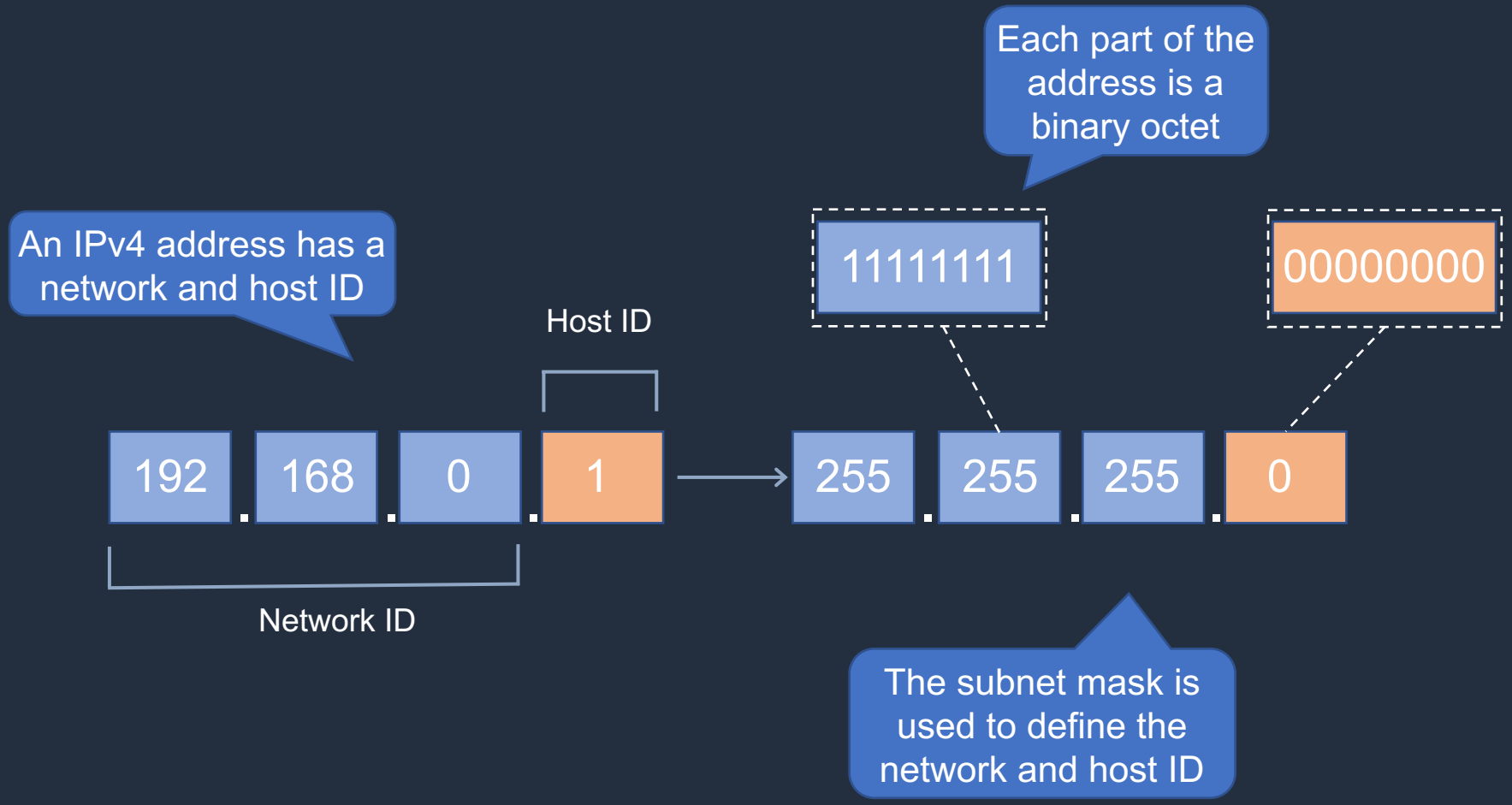
Domain name is resolved to the IP address of the webserver

Computer connects to 192.168.0.1

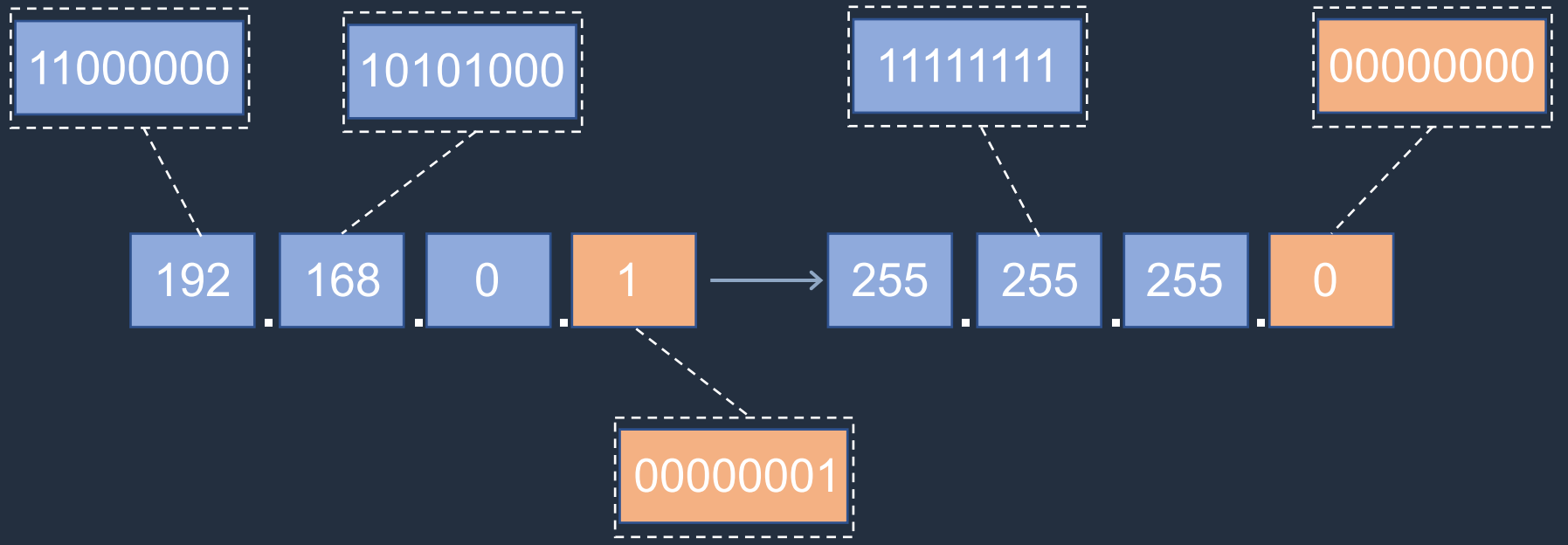
Web Server

DigitalCloud TRAINING

IP Addressing Basics



IP Addressing Basics



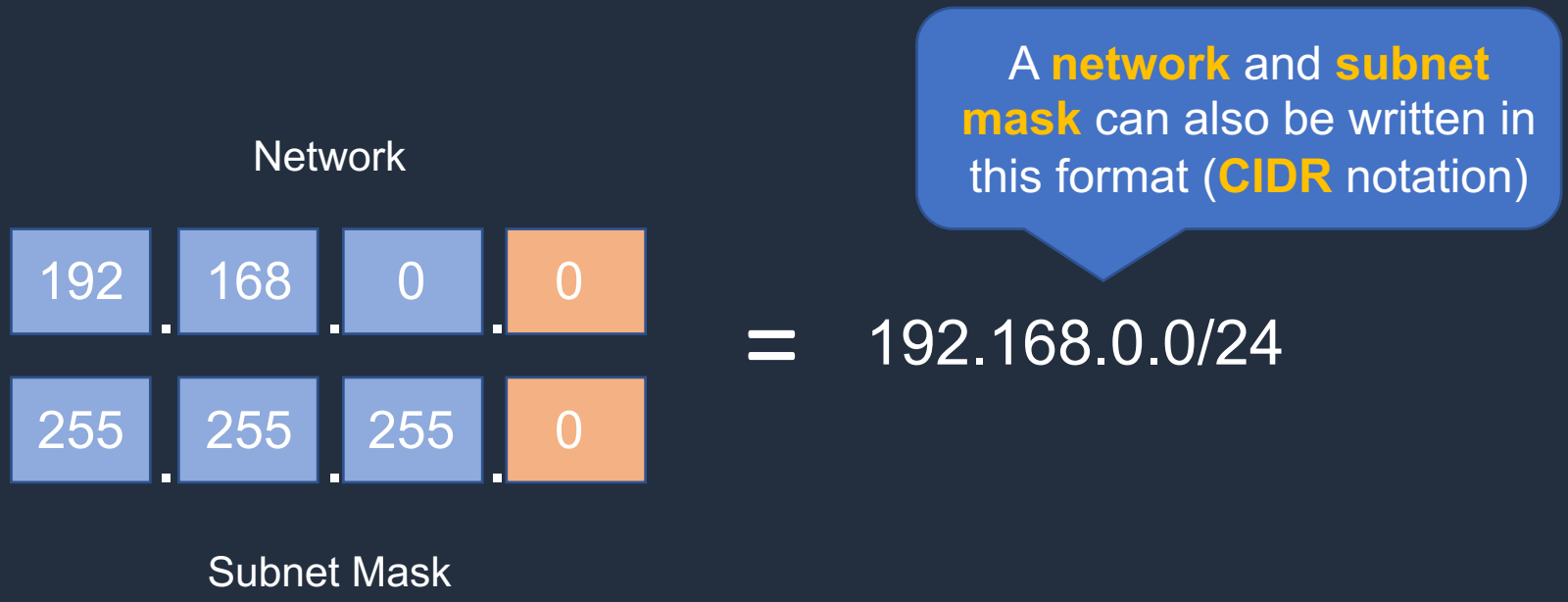
Most significant bit ⟶

1	1	1	1	1	1	1	1
128	64	32	16	8	4	2	1

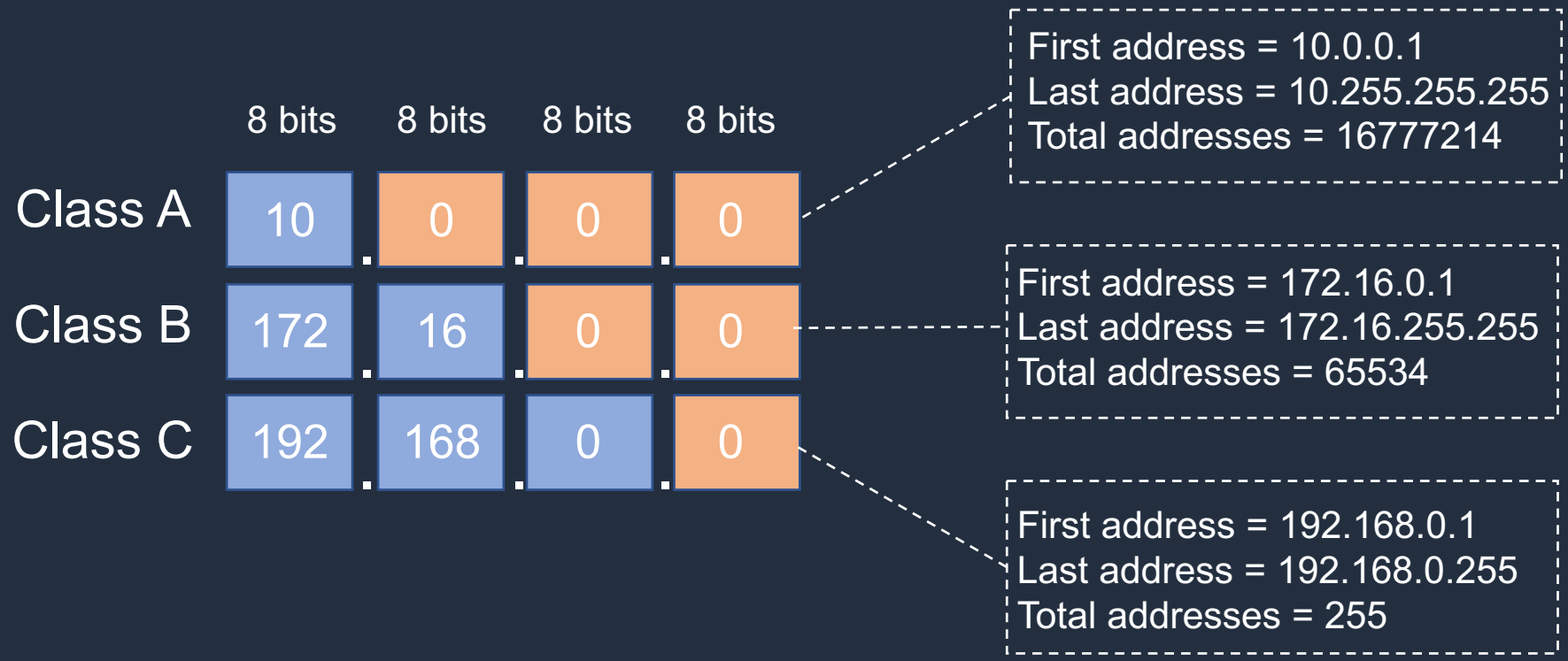
⟵ Least significant bit

Binary Values

IP Addressing Basics



IP Addressing Basics



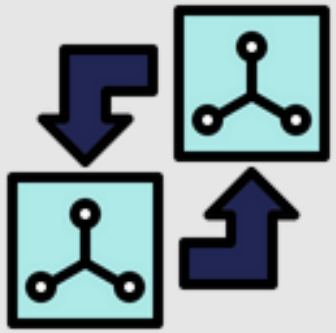
Private IP Addresses

- There are several ranges of addresses reserved for **private usage** as defined in **RFC 1918**
- These are:

CIDR	First Address	Last Address
10.0.0.0/8	10.0.0.0	10.255.255.255
172.16.0.0/12	172.16.0.0	172.31.255.255
192.168.0.0/16	192.168.0.0	192.168.255.255

- Private addresses are NOT routable on the Internet

The OSI Model



DigitalCloud TRAINING

The OSI Model

Network services to end user applications

Application Layer	Data	HTTP, FTP, SSH, DNS
Presentation Layer	Data	SSL, FTP, SSH, HTML
Session Layer	Data	TCP, RPC
Transport Layer	Segments	TCP, UDP, TLS
Network Layer	Packets	IP, IPSec, ICMP
Data Link Layer	Frames	Ethernet, 802.11
Physical Layer	Bits	Coax, Fiber, Wireless

Data representation and encryption

Interhost communication

End-to-end connections and reliability

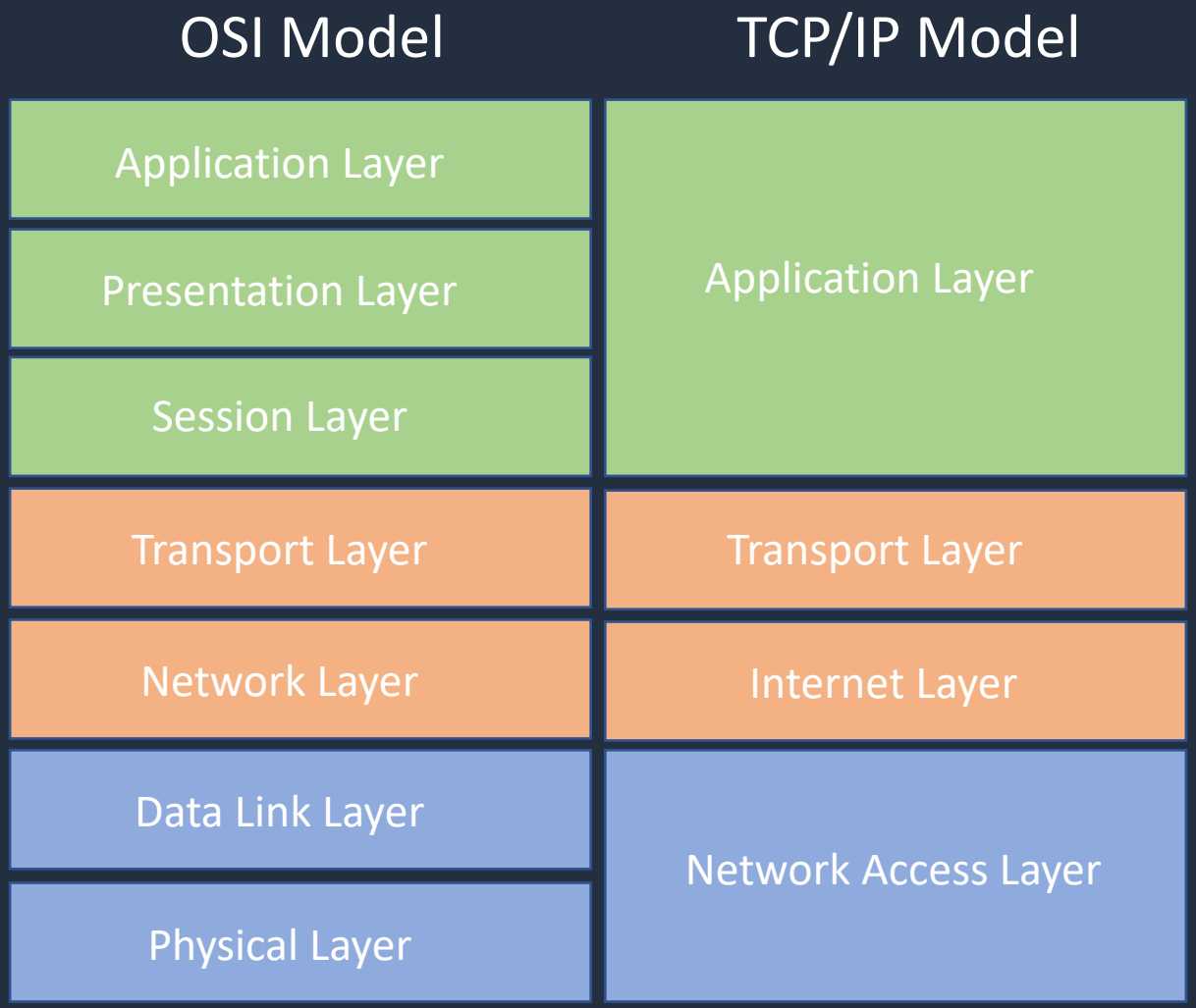
Path determination (e.g. routing)

Physical addressing (e.g. MAC and LLC)

Media, signal, binary transmission

DigitalCloud TRAINING

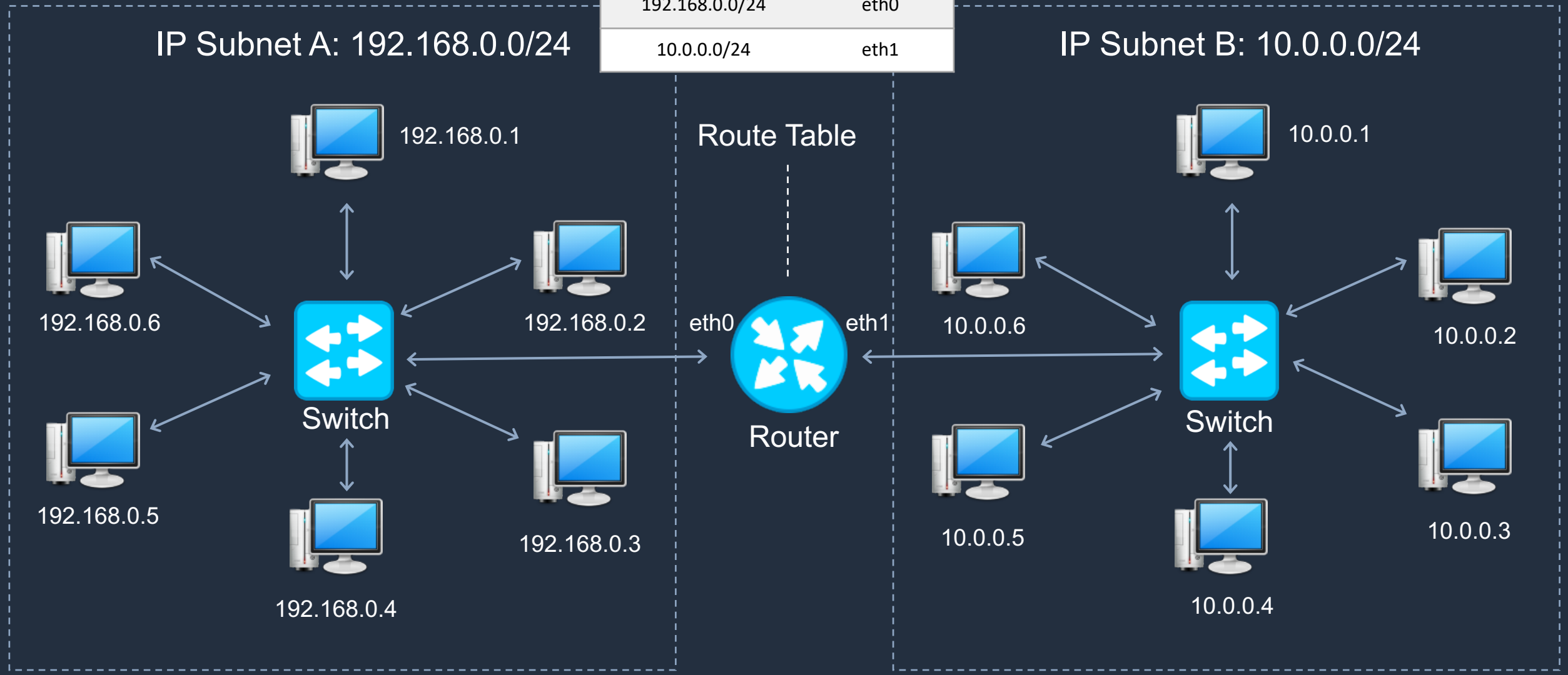
The OSI Model



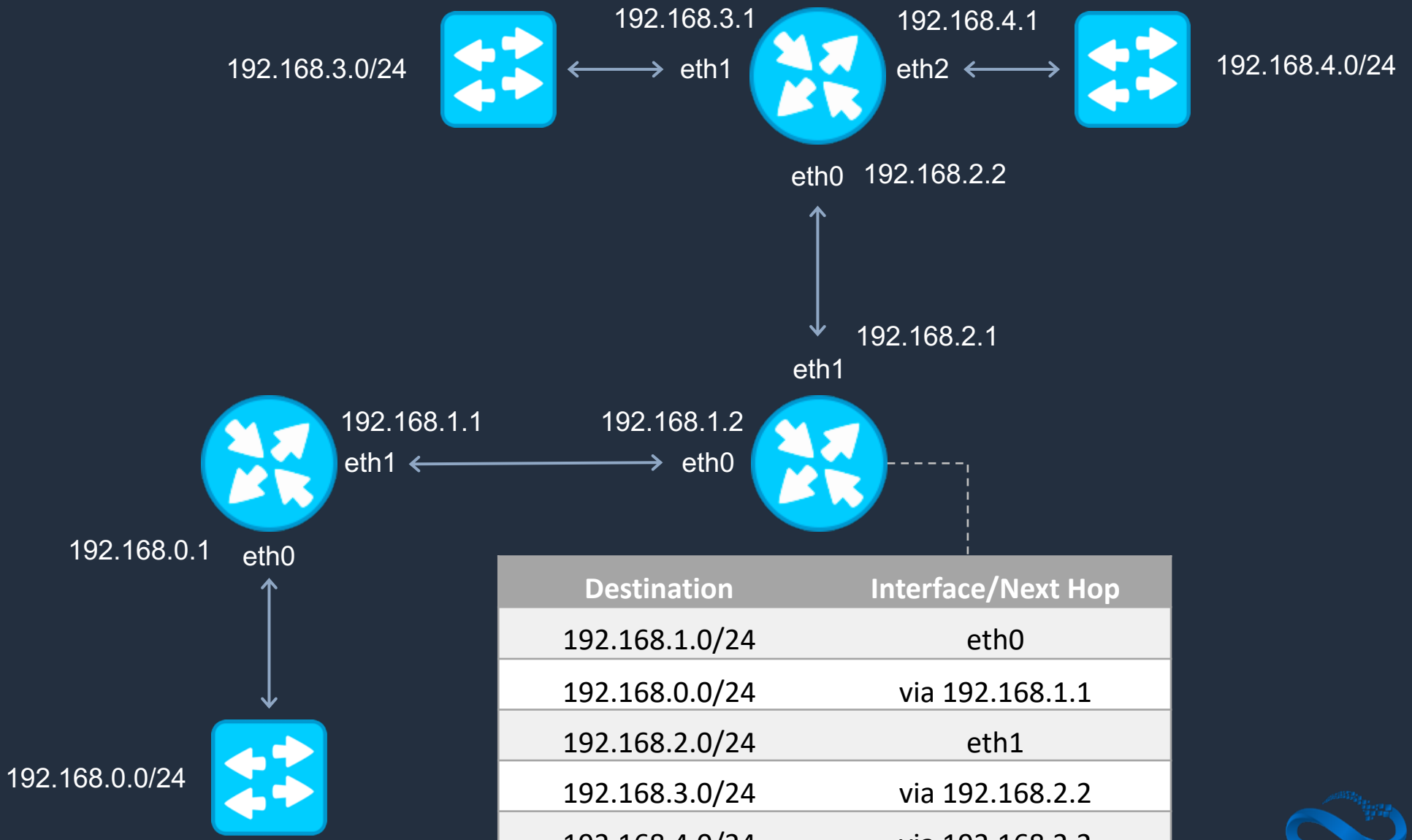
Routing and Switching

Routers and Switches

Destination	Interface
192.168.0.0/24	eth0
10.0.0.0/24	eth1



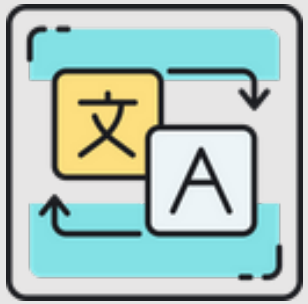
Route Tables



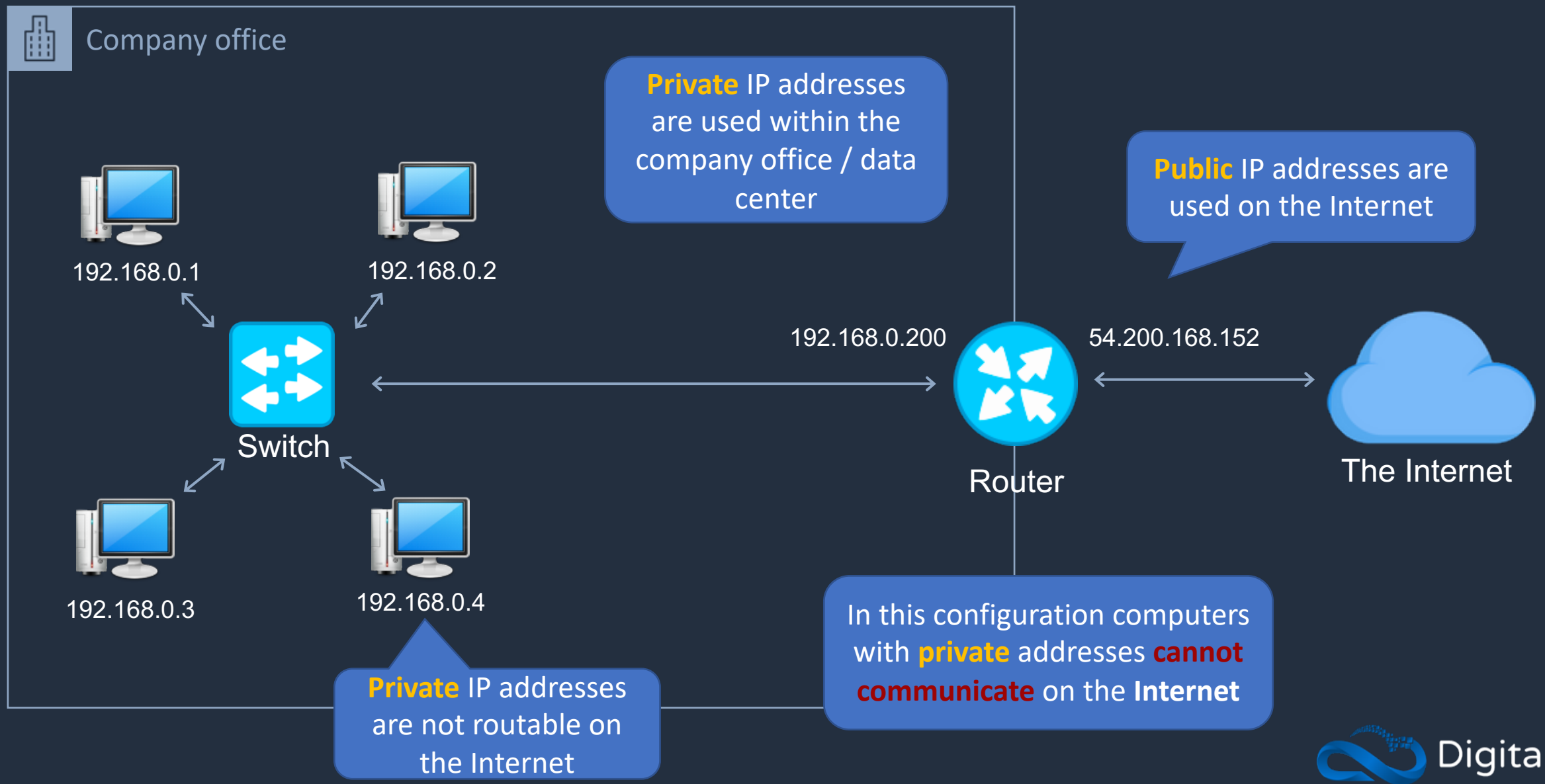
Destination	Interface/Next Hop
192.168.1.0/24	eth0
192.168.0.0/24	via 192.168.1.1
192.168.2.0/24	eth1
192.168.3.0/24	via 192.168.2.2
192.168.4.0/24	via 192.168.2.2

DigitalCloud TRAINING

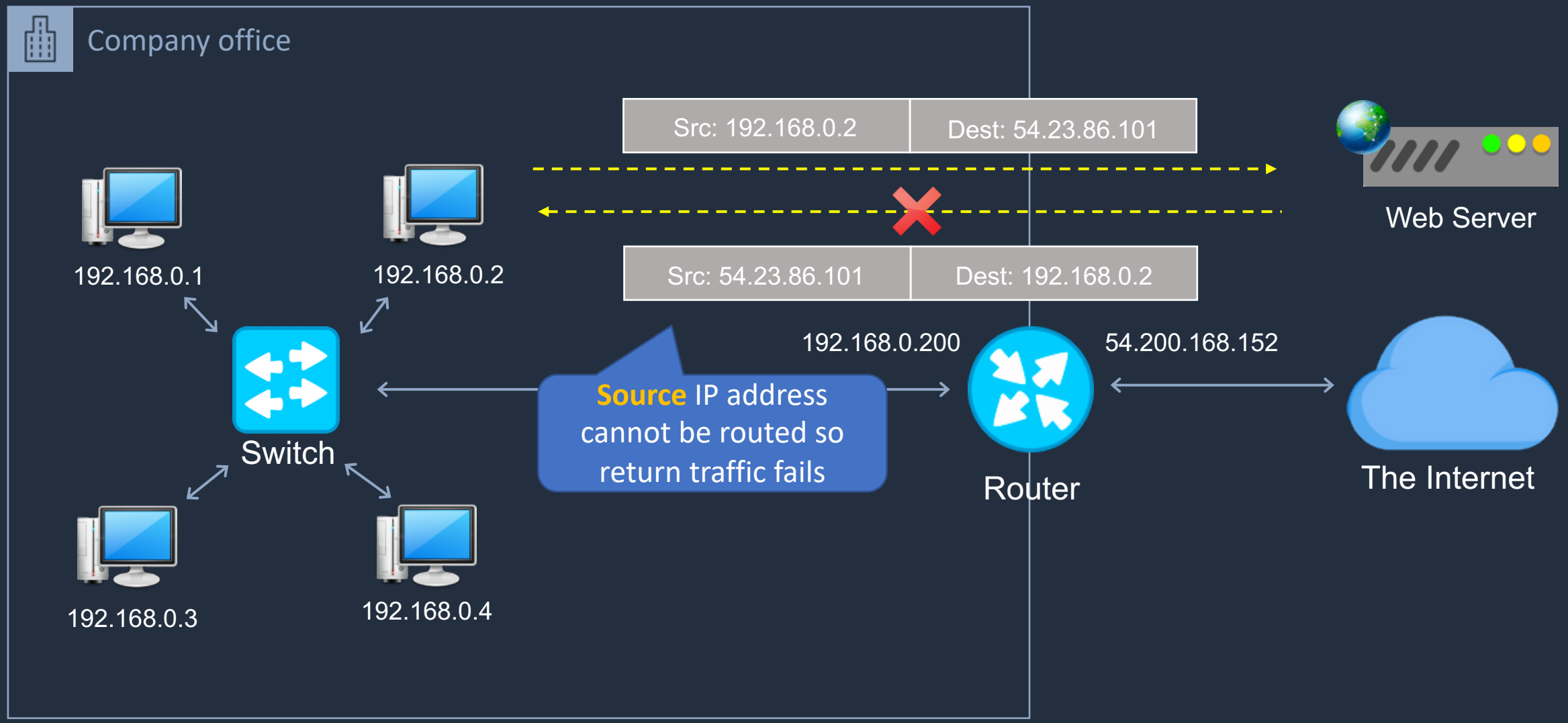
Network Address Translation



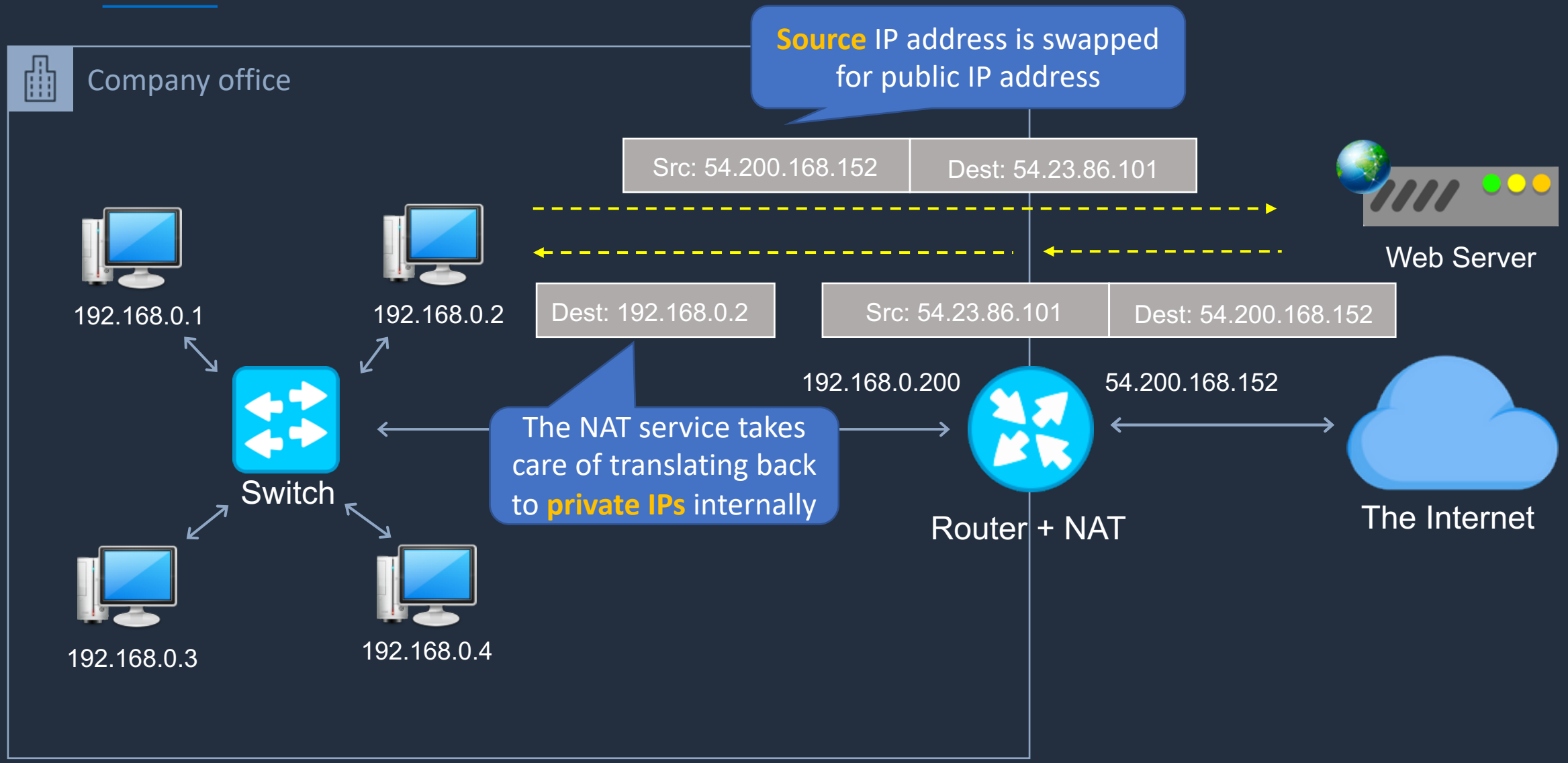
Without Network Address Translation (NAT)



Without Network Address Translation (NAT)



With Network Address Translation (NAT)



Firewalls

Firewalls

POLICY	PROTOCOL	PORT	DESTINATION	SOURCE
ALLOW	HTTP	80	INTERNAL	ANY
ALLOW	HTTPS	443	INTERNAL	ANY
DENY	ANY	ANY	INTERNAL	ANY

Firewall Rules

IP Subnet A

IP Subnet B

Database Server

Application Server

Web Server

Firewall

Firewall

Firewall

The Internet

Database Server

Application Server

Web Server

DigitalCloud TRAINING

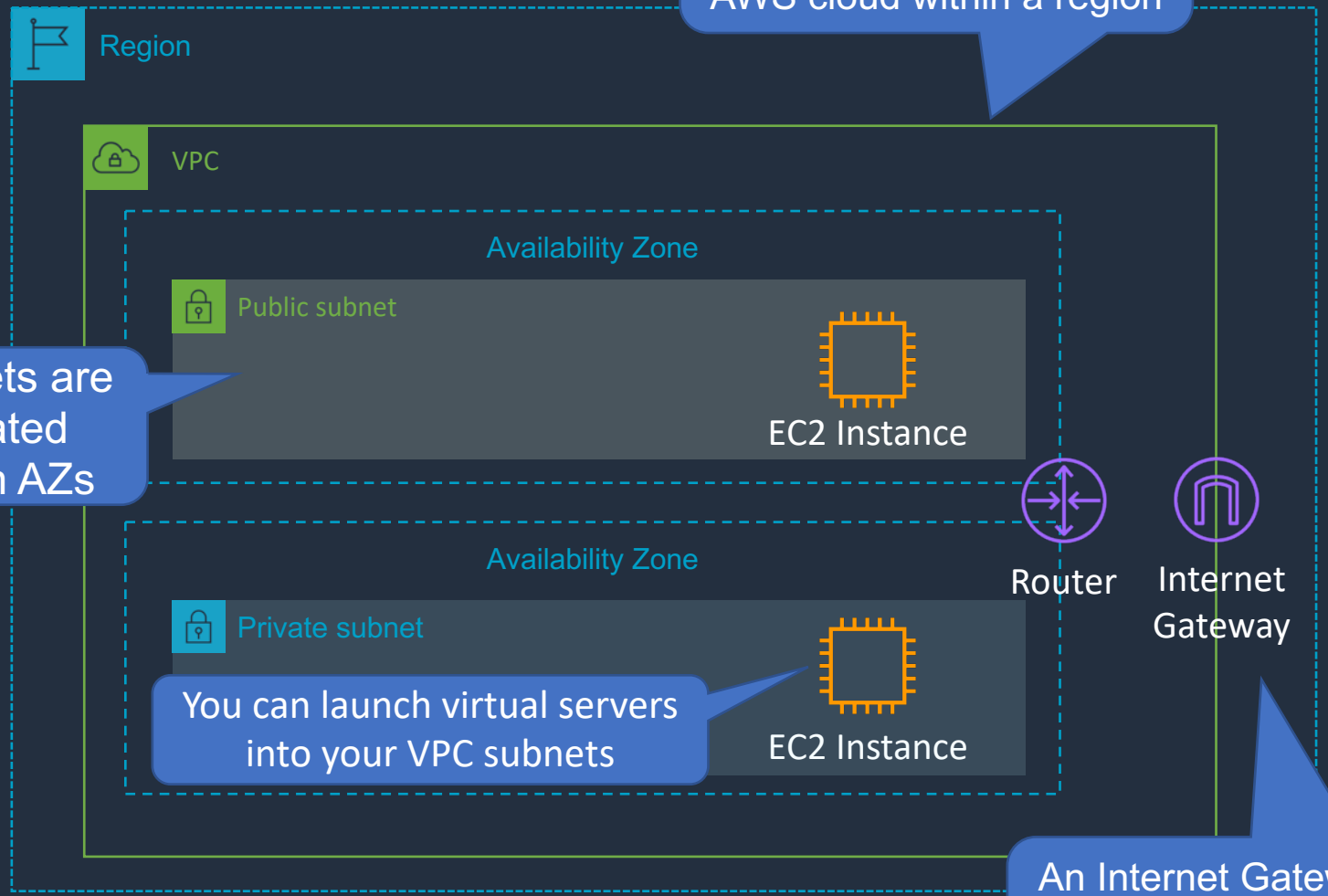
SECTION 4

Amazon Virtual Private Cloud (VPC)

Amazon VPC Overview

Amazon VPC Overview

A VPC is a logically isolated portion of the AWS cloud within a region



Subnets are created within AZs

You can launch virtual servers into your VPC subnets

An Internet Gateway is used to connect to the Internet

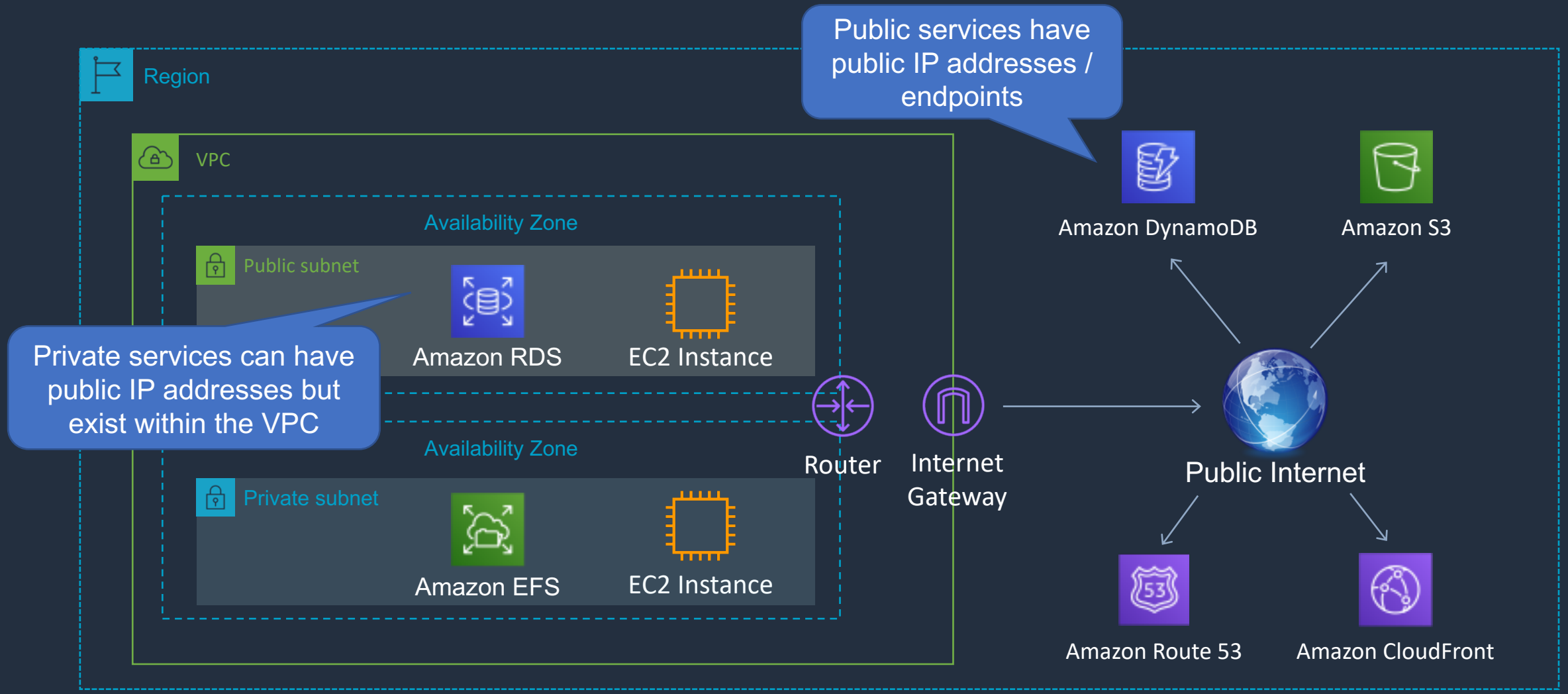
Main Route Table

Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	igw-id

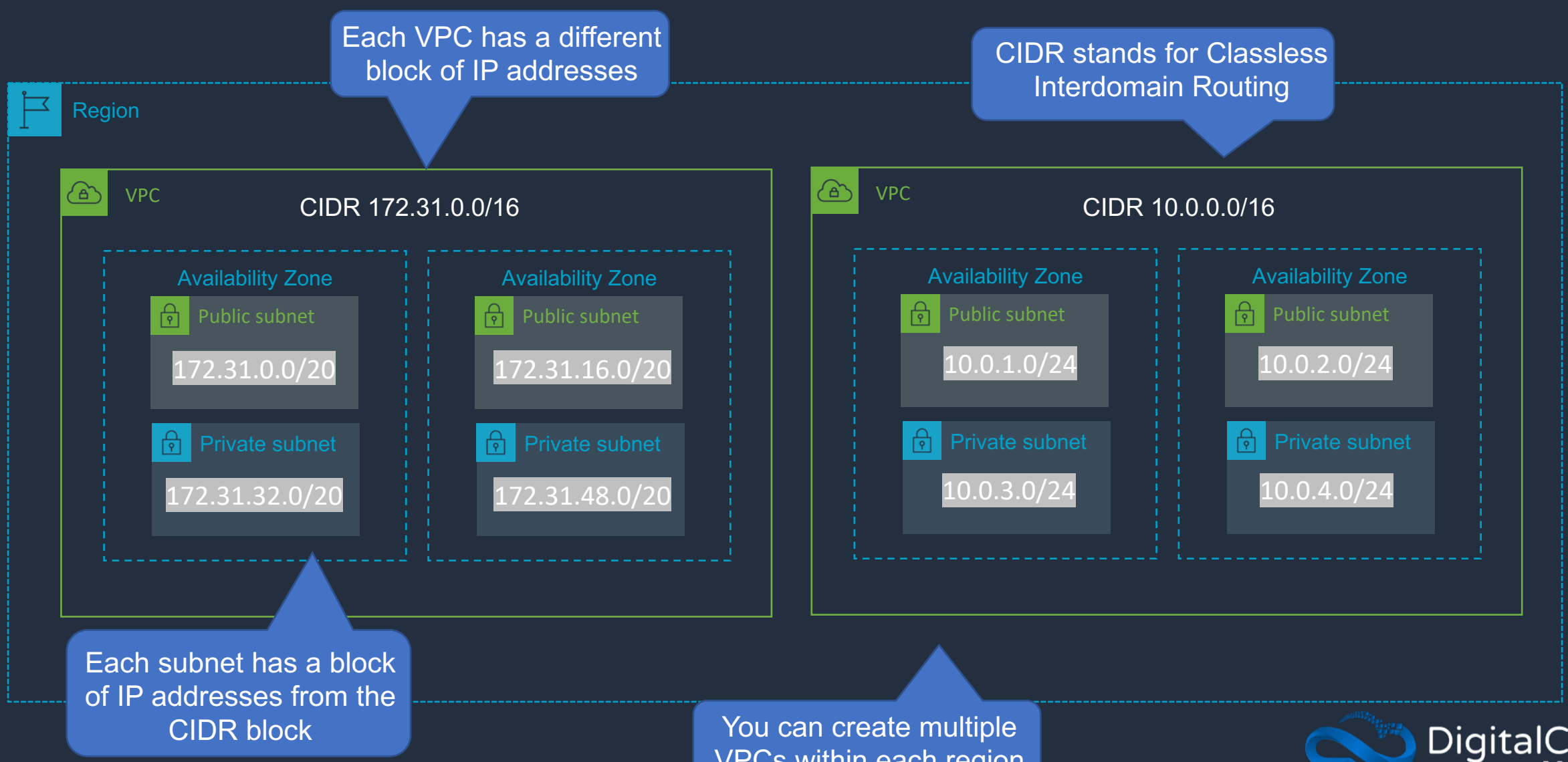
The route table is used to configure the VPC router

DigitalCloud TRAINING

Amazon VPC Overview



Amazon VPC Overview



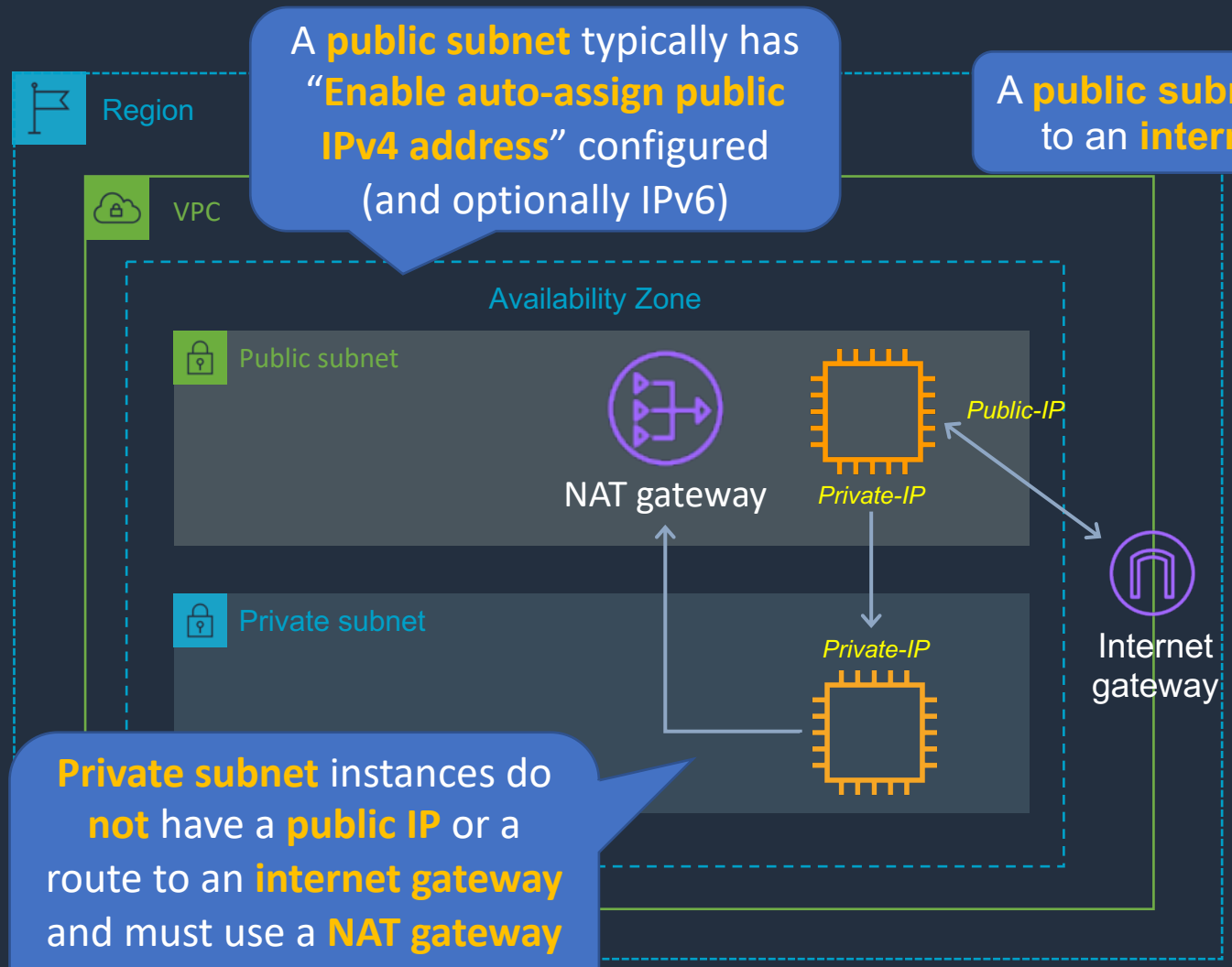
DigitalCloud TRAINING

Default VPC Walkthrough

Public and Private Subnets

DigitalCloud TRAINING

Public and Private Subnets



Public Subnet Route Table

Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	igw-id

Public Internet

Private Subnet Route Table

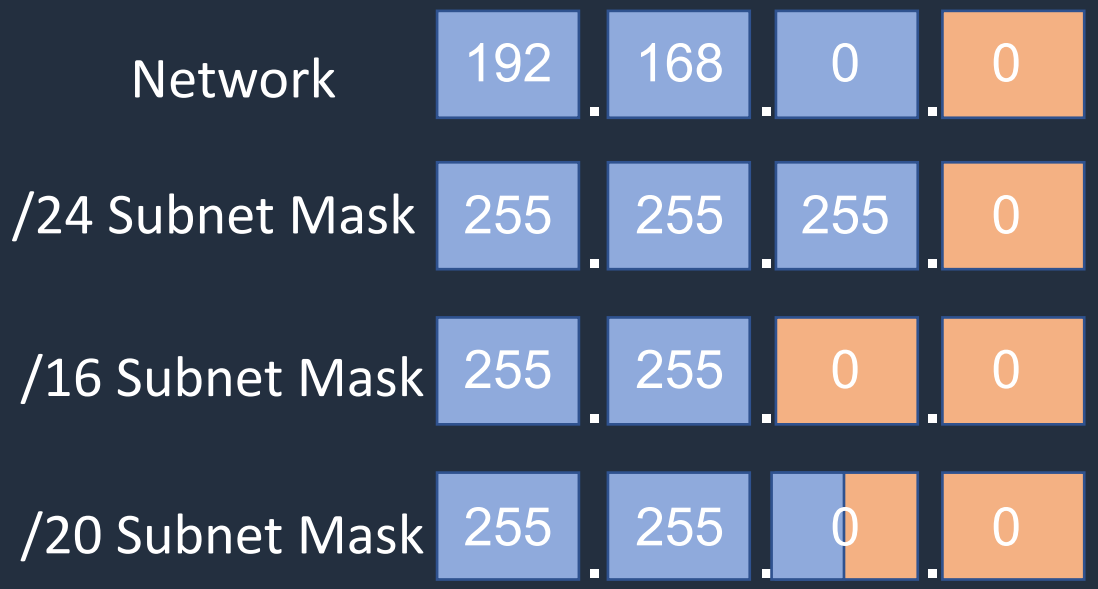
Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	nat-gateway-id

NAT = Network Address Translation

Defining VPC CIDR Blocks

DigitalCloud TRAINING

Defining VPC CIDR Blocks



First Address	Last Address
192.168.0.1	192.168.0.254

8 host bits = 256 addresses

16 host bits = 65536 addresses

First Address	Last Address
192.168.0.1	192.168.255.254

12 host bits = 4096 addresses

First Address	Last Address
192.168.0.1	192.168.15.254

Classless Interdomain Routing (CIDR) uses **variable length subnets masks** (VLSM)

DigitalCloud TRAINING

Rules and Guidelines

- CIDR block size can be between /16 and /28
- The CIDR block must not overlap with any existing CIDR block that's associated with the VPC
- You cannot increase or decrease the size of an existing CIDR block
- The first four and last IP address are not available for use
- AWS recommend you use CIDR blocks from the RFC 1918 ranges:

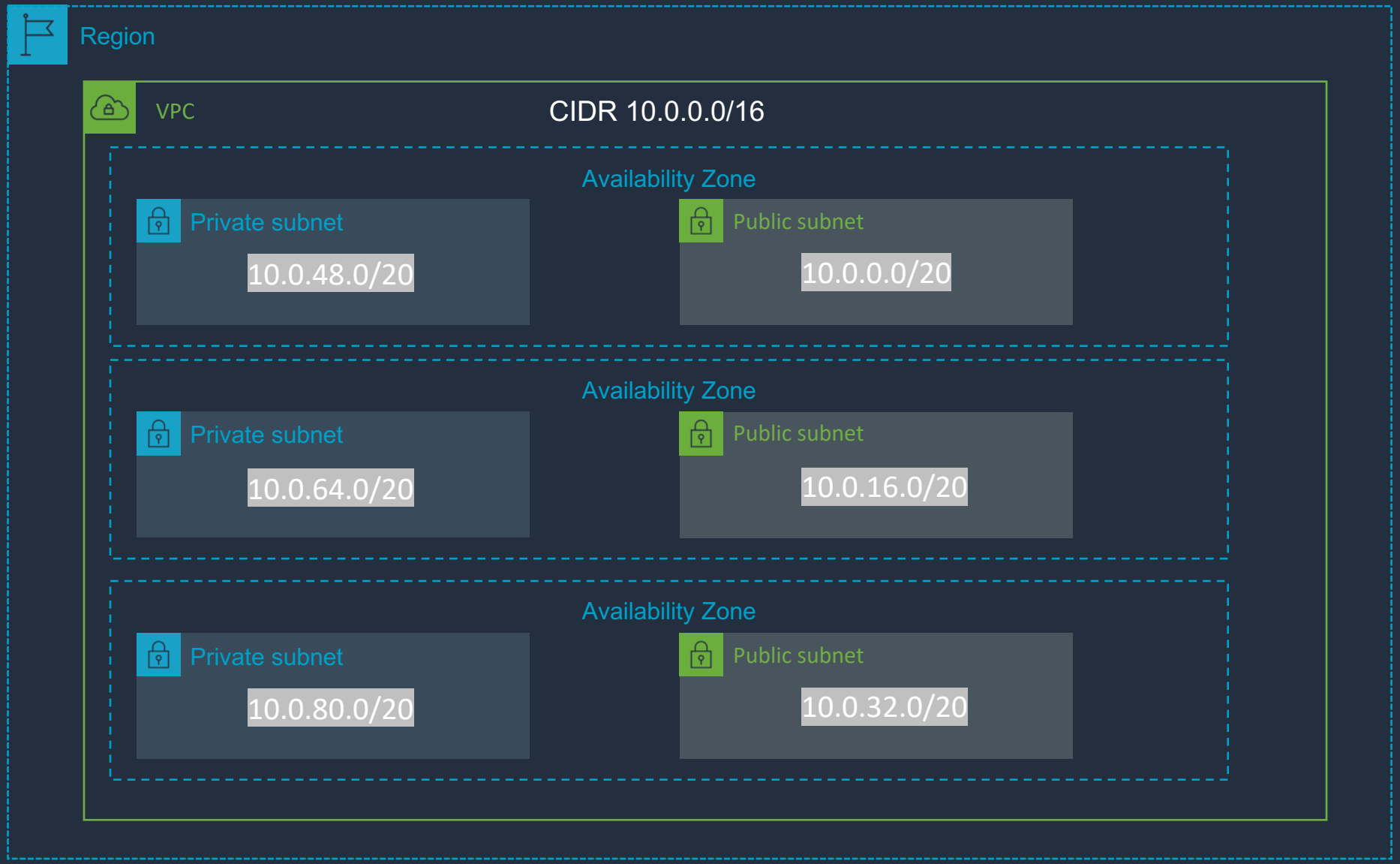
RFC 1918 Range	Example CIDR Block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	Your VPC must be /16 or smaller, for example, 10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	Your VPC must be /16 or smaller, for example, 172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	Your VPC can be smaller, for example 192.168.0.0/20

DigitalCloud TRAINING

Create a Custom VPC with Subnets

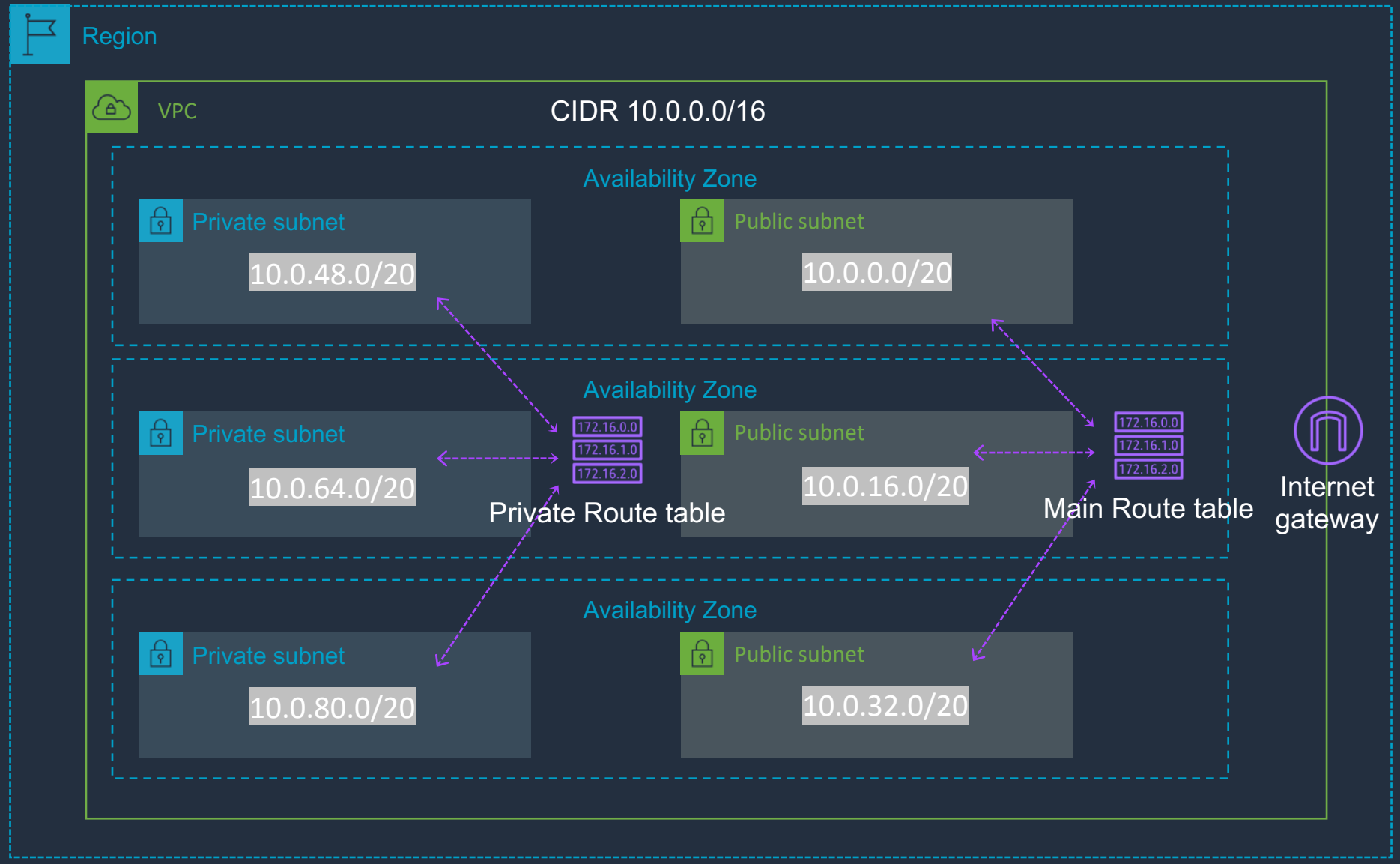
DigitalCloud TRAINING

Create a Custom VPC



Configure Routing

Create a Custom VPC



Main Route Table

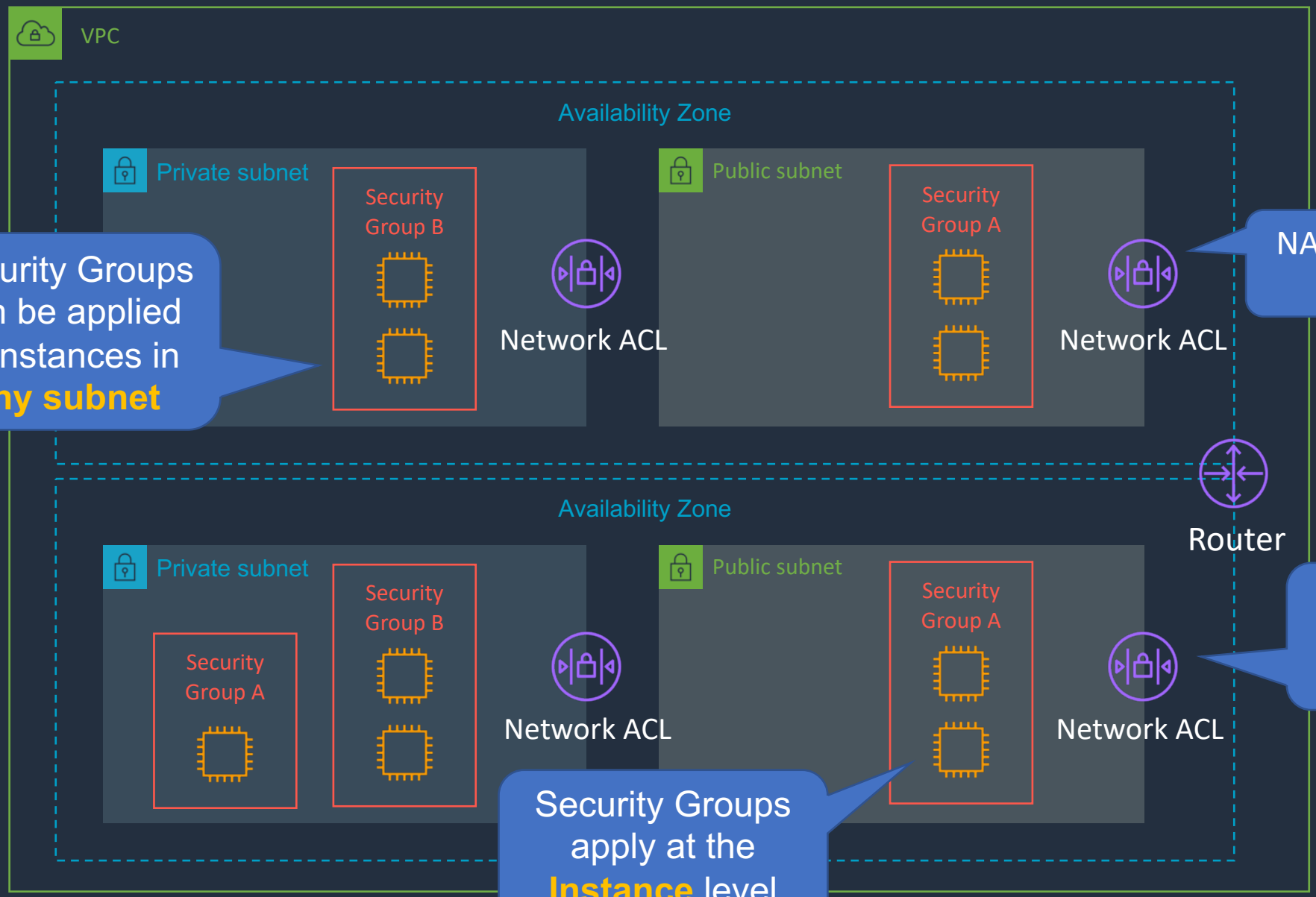
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-id

Private Route Table

Destination	Target
10.0.0.0/16	Local

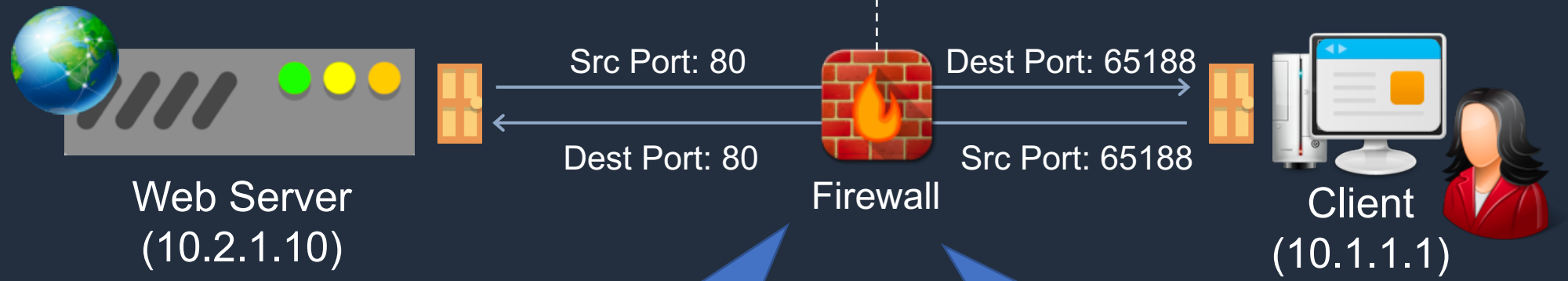
Security Groups and Network ACLs

Security Groups and Network ACLs



Stateful vs Stateless Firewalls

PROTOCOL	SOURCE IP	DESTINATION IP	SOURCE PORT	DESTINATION PORT
HTTP	10.1.1.1	10.2.1.10	65188	80
HTTP	10.2.1.10	10.1.1.1	80	65188



A stateful firewall allows the return traffic automatically

A stateless firewall checks for an allow rule for both connections

Security Group Rules

Security groups support **allow** rules only

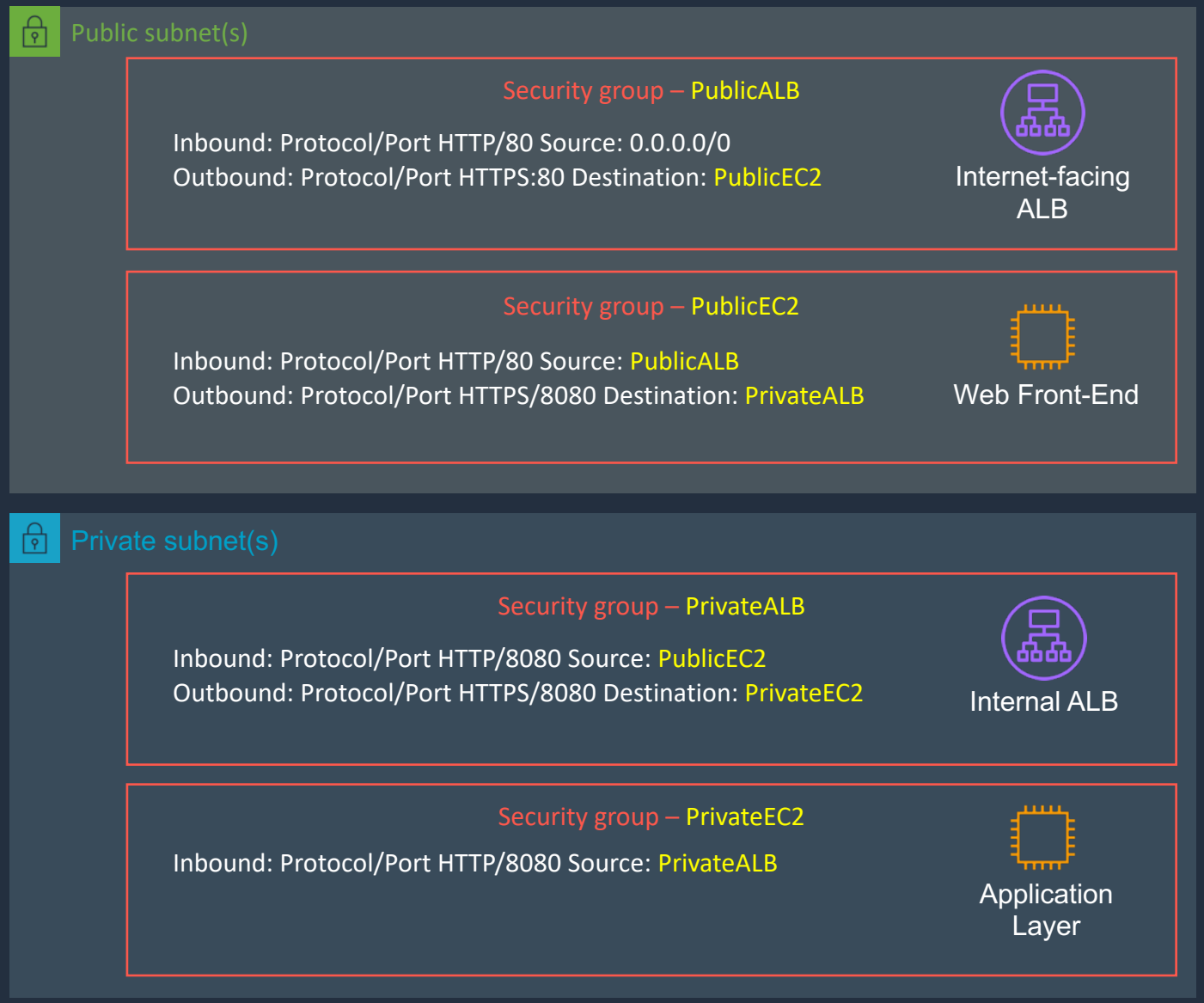
Inbound rules

Type	Protocol	Port range	Source
SSH	TCP	22	0.0.0.0/0
RDP	TCP	3389	0.0.0.0/0
RDP	TCP	3389	::/0
HTTPS	TCP	443	0.0.0.0/0
HTTPS	TCP	443	::/0
All ICMP - IPv4	ICMP	All	0.0.0.0/0

Separate rules are defined for outbound traffic

A source can be an **IP address** or **security group ID**

Security Groups Best Practice



Network ACLs

Inbound Rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

Outbound Rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
101	ALL Traffic	ALL	ALL	::/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
*	ALL Traffic	ALL	ALL	::/0	DENY

NACLs have an explicit deny

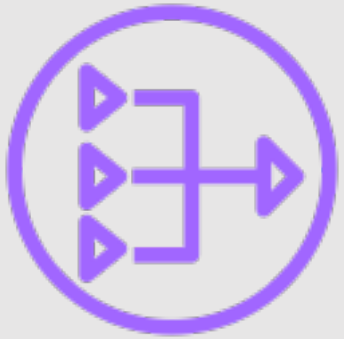
Rules are processed in order

DigitalCloud TRAINING

Setup Security Groups and NACLs

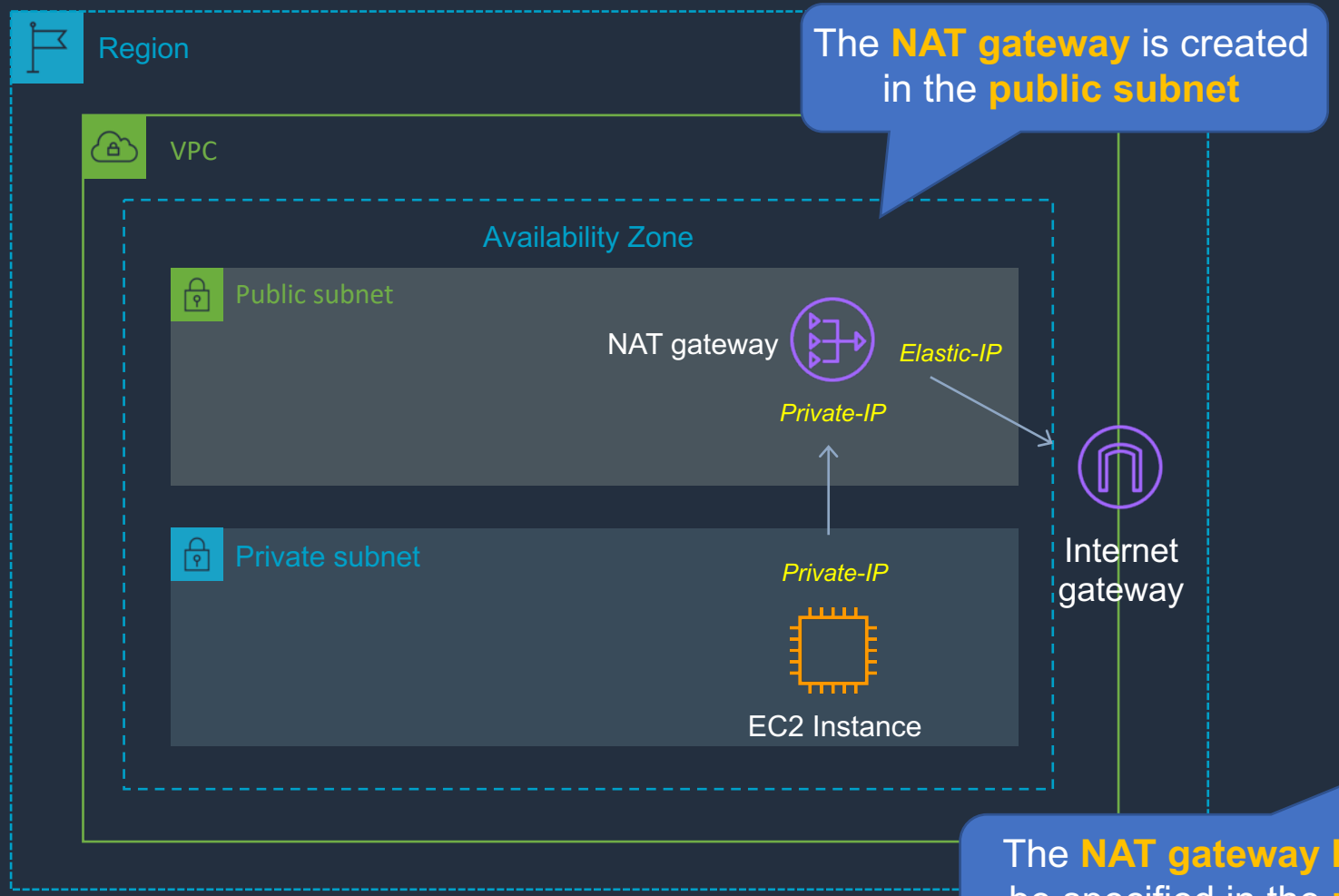
Launch Instances into Subnets

NAT Gateways and NAT Instances



DigitalCloud TRAINING

NAT Gateways



The **NAT gateway** is created in the **public subnet**

Main Route Table

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

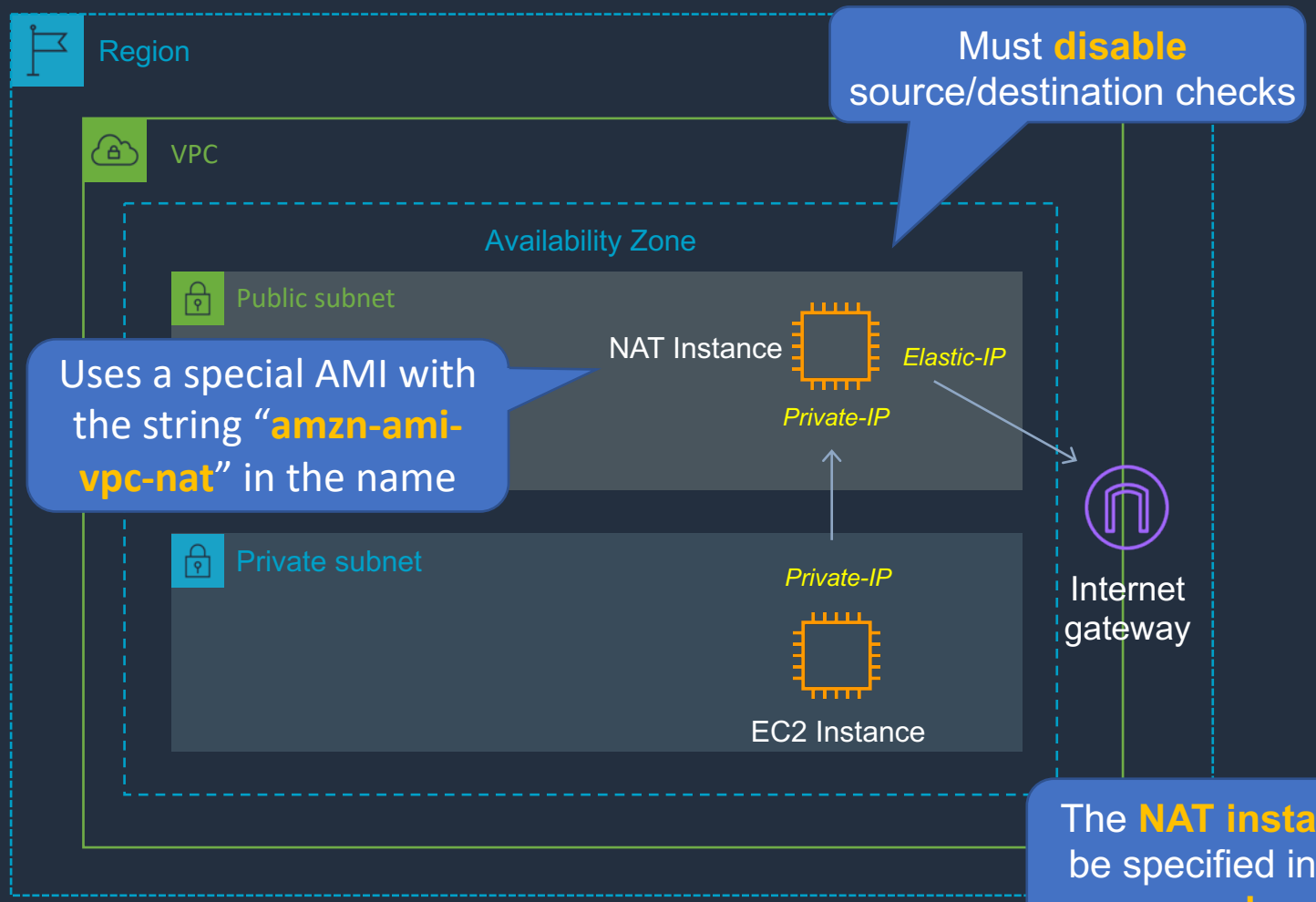
Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-gateway-id

The **NAT gateway ID** must be specified in the **private subnet** RT

DigitalCloud TRAINING

NAT Instances



Main Route Table

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

Private Route Table

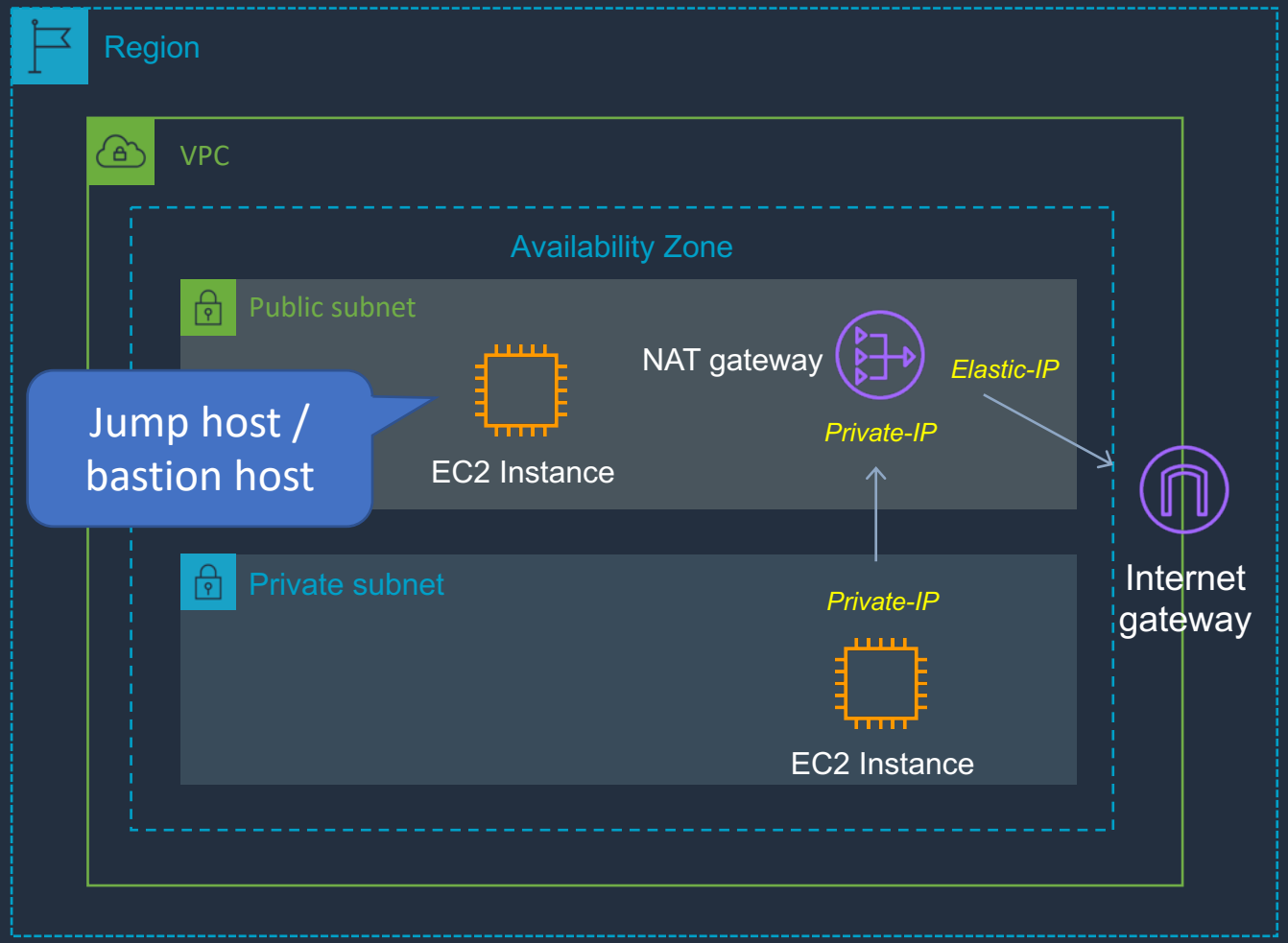
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-instance-id

NAT Instance vs NAT Gateway

NAT Instance	NAT Gateway
Managed by you (e.g. software updates)	Managed by AWS
Scale up (instance type) manually and use enhanced networking	Elastic scalability up to 45 Gbps
No high availability – scripted/auto-scaled HA possible using multiple NATs in multiple subnets	Provides automatic high availability within an AZ and can be placed in multiple AZs
Need to assign Security Group	No Security Groups
Can use as a bastion host	Cannot access through SSH
Use an Elastic IP address or a public IP address with a NAT instance	Choose the Elastic IP address to associate with a NAT gateway at creation
Can implement port forwarding through manual customisation	Does not support port forwarding

Create NAT Gateway

NAT Gateways



Main Route Table

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

Private Route Table

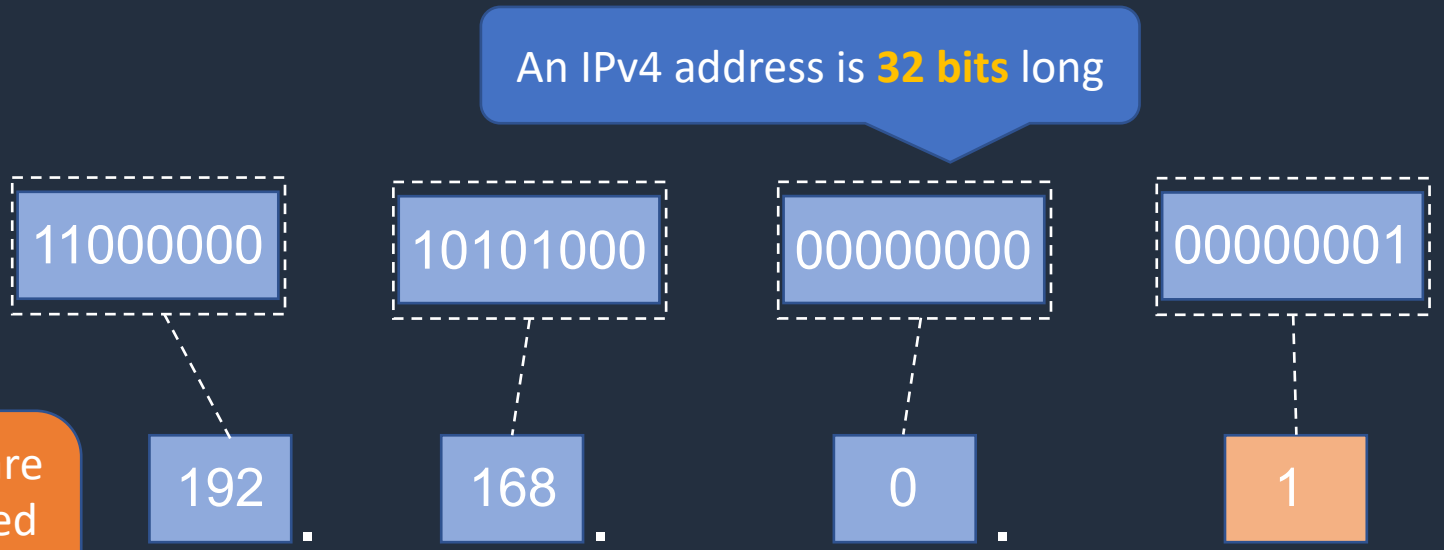
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	nat-gateway-id

DigitalCloud TRAINING

Using IPv6 in a VPC

DigitalCloud TRAINING

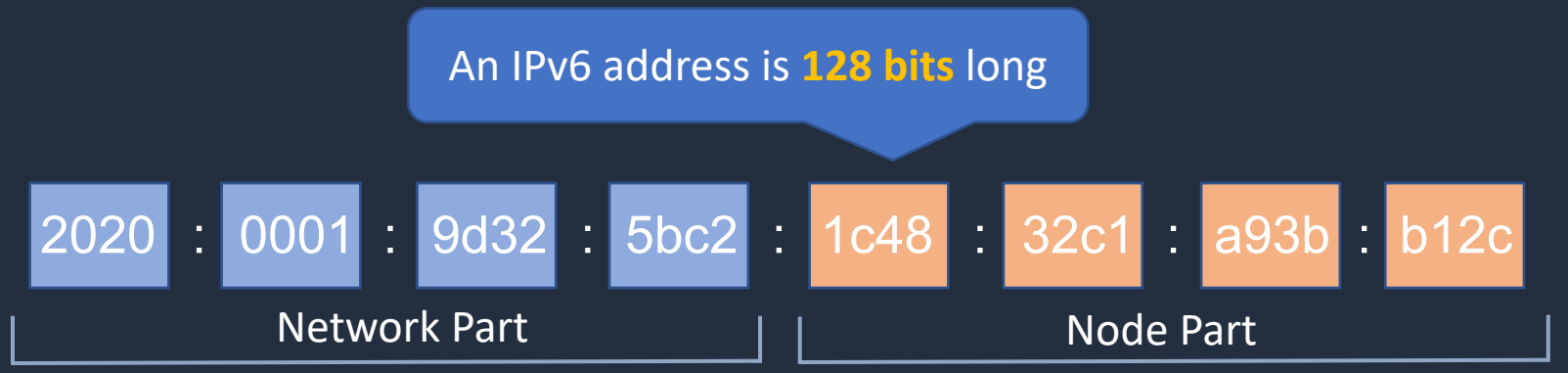
Using IPv6 in a VPC



Public **IPv4** addresses are close to being exhausted and **NAT** must be used extensively

IPv4 provides approximately **4.3 billon** addresses

Using IPv6 in a VPC



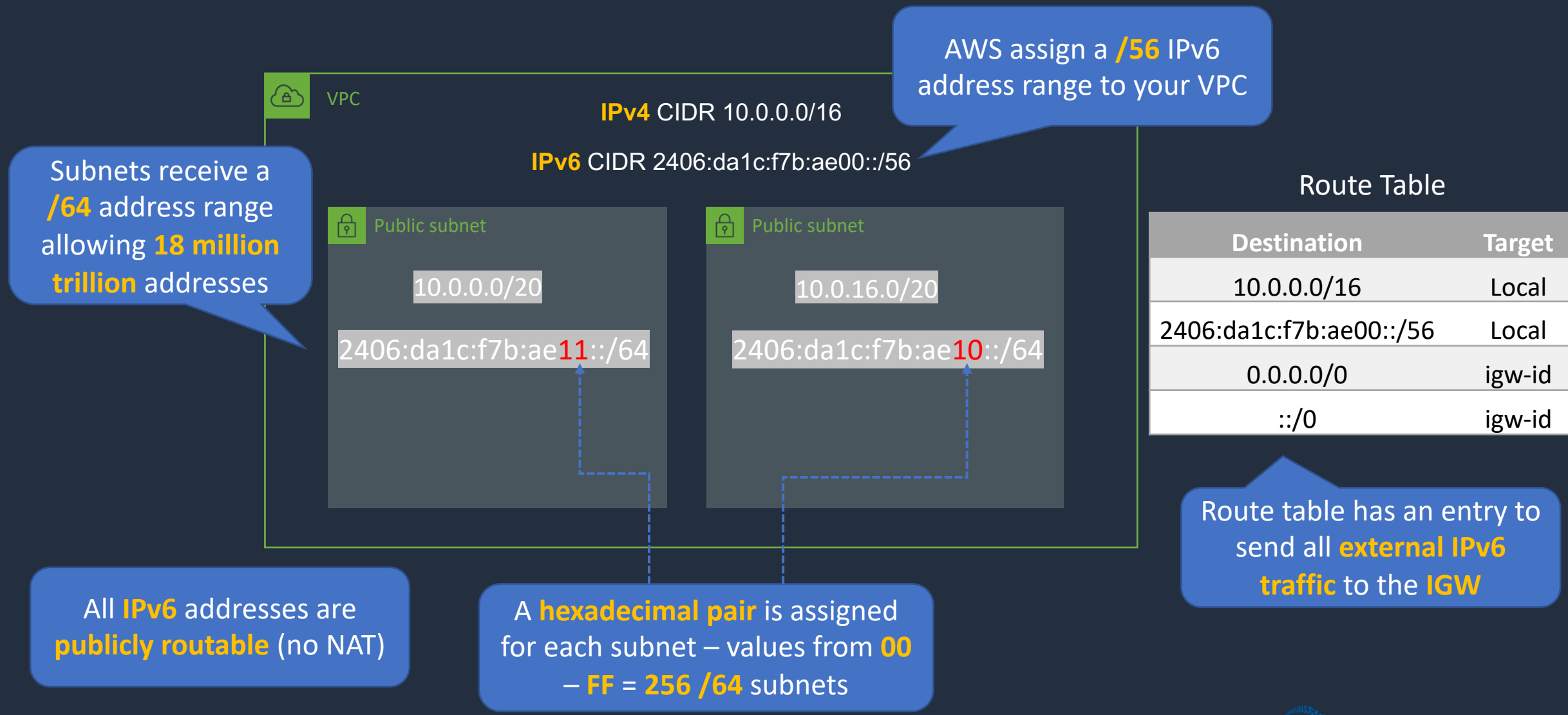
An IPv6 addresses use **hexadecimal** whereas **IPv4** addresses use **dotted decimal**

That's enough to assign more than **100 IPv6 addresses** to **every atom** on earth!!!

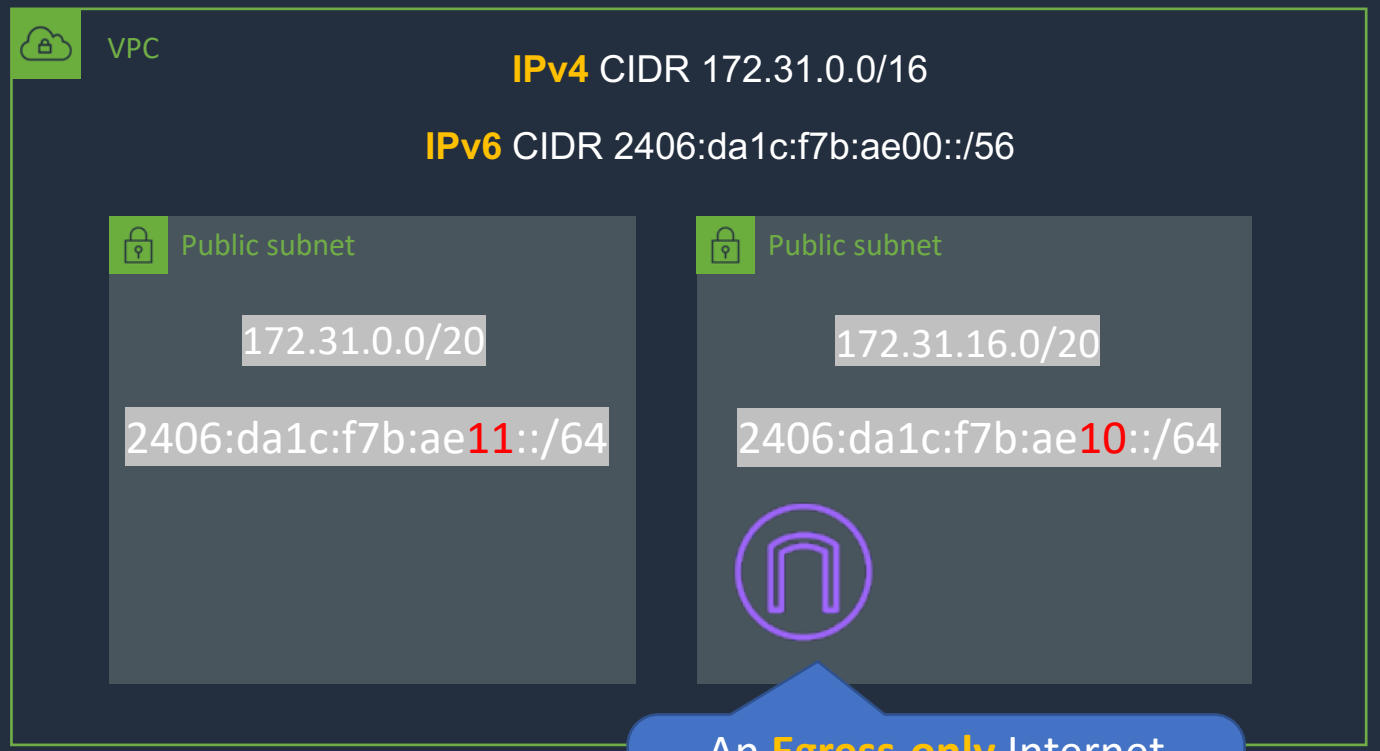
IPv6 provides **340,282,366,920,938,463,463,374,607,431,768,211,456** addresses

DigitalCloud TRAINING

Using IPv6 in a VPC



Using IPv6 in a VPC



Route Table

Destination	Target
172.31.0.0/16	Local
0.0.0.0/0	igw-id
::/0	eo-igw-id

All **IPv6** addresses are **publicly routable** (no NAT)

An **Egress-only** Internet Gateway allows IPv6 traffic **outbound** but **not inbound**

Configure IPv6

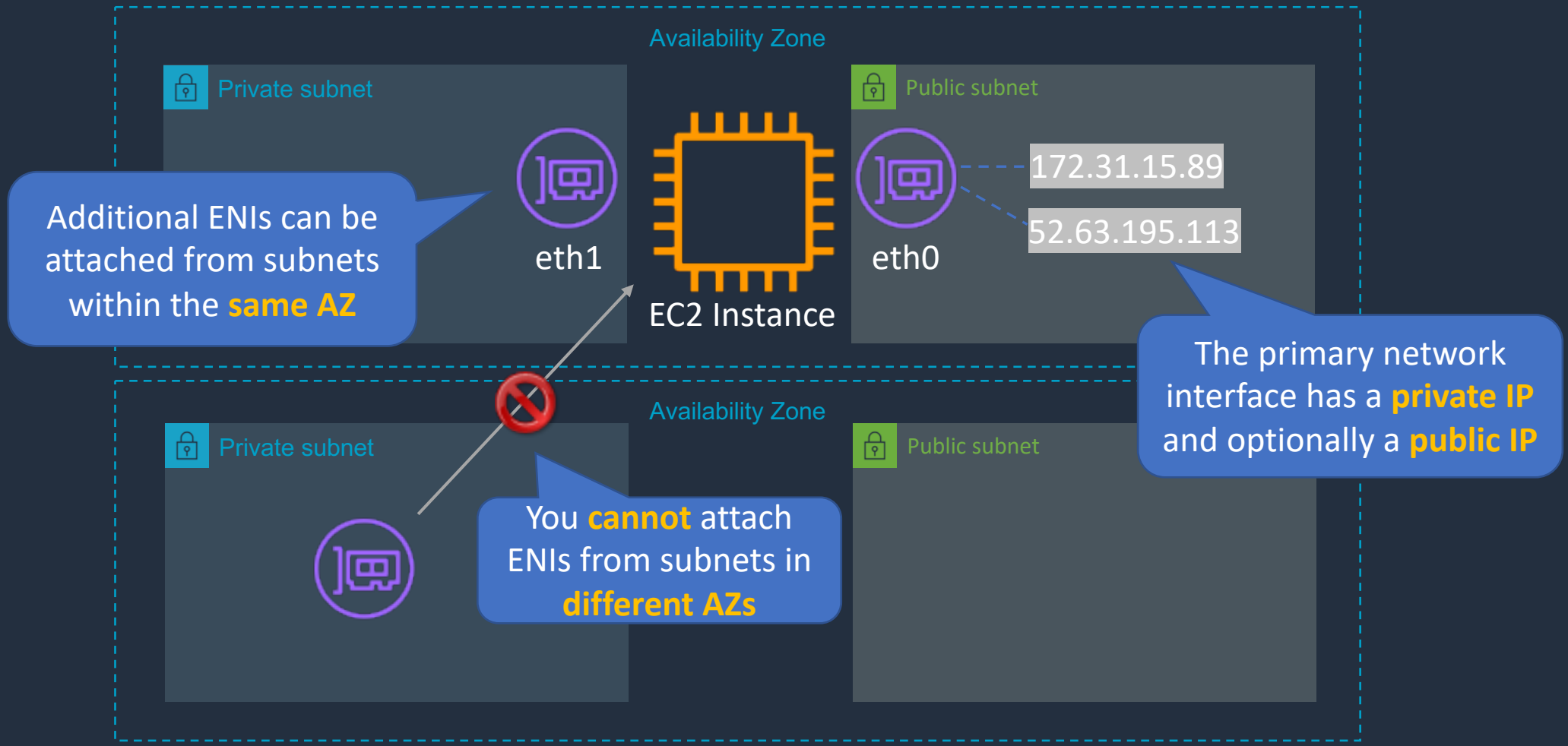
Additional Settings

SECTION 5

Amazon EC2 Networking

Network Interfaces (ENI, ENA, EFA)

Network Interfaces (ENI, ENA, EFA)



Network Interfaces (ENI, ENA, EFA)

Elastic network interface

- Basic adapter type for when you don’t have any high-performance requirements
- Can use with all instance types

Elastic network adapter

- Enhanced networking performance
- Higher bandwidth and lower inter-instance latency
- Must choose supported instance type

Elastic Fabric Adapter

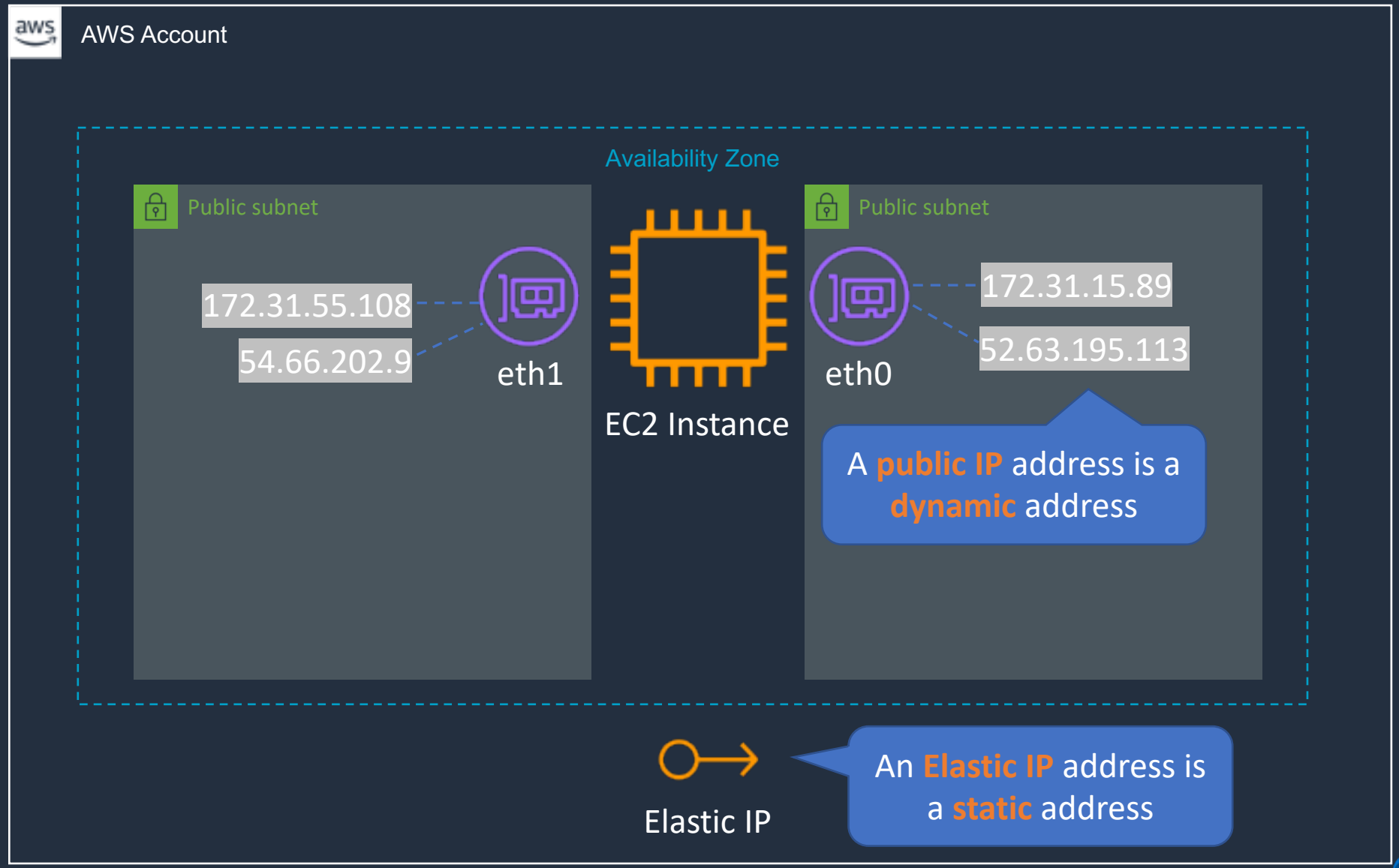
- Use with High Performance Computing and MPI and ML use cases
- Tightly coupled applications
- Can use with all instance types

Working with ENIs

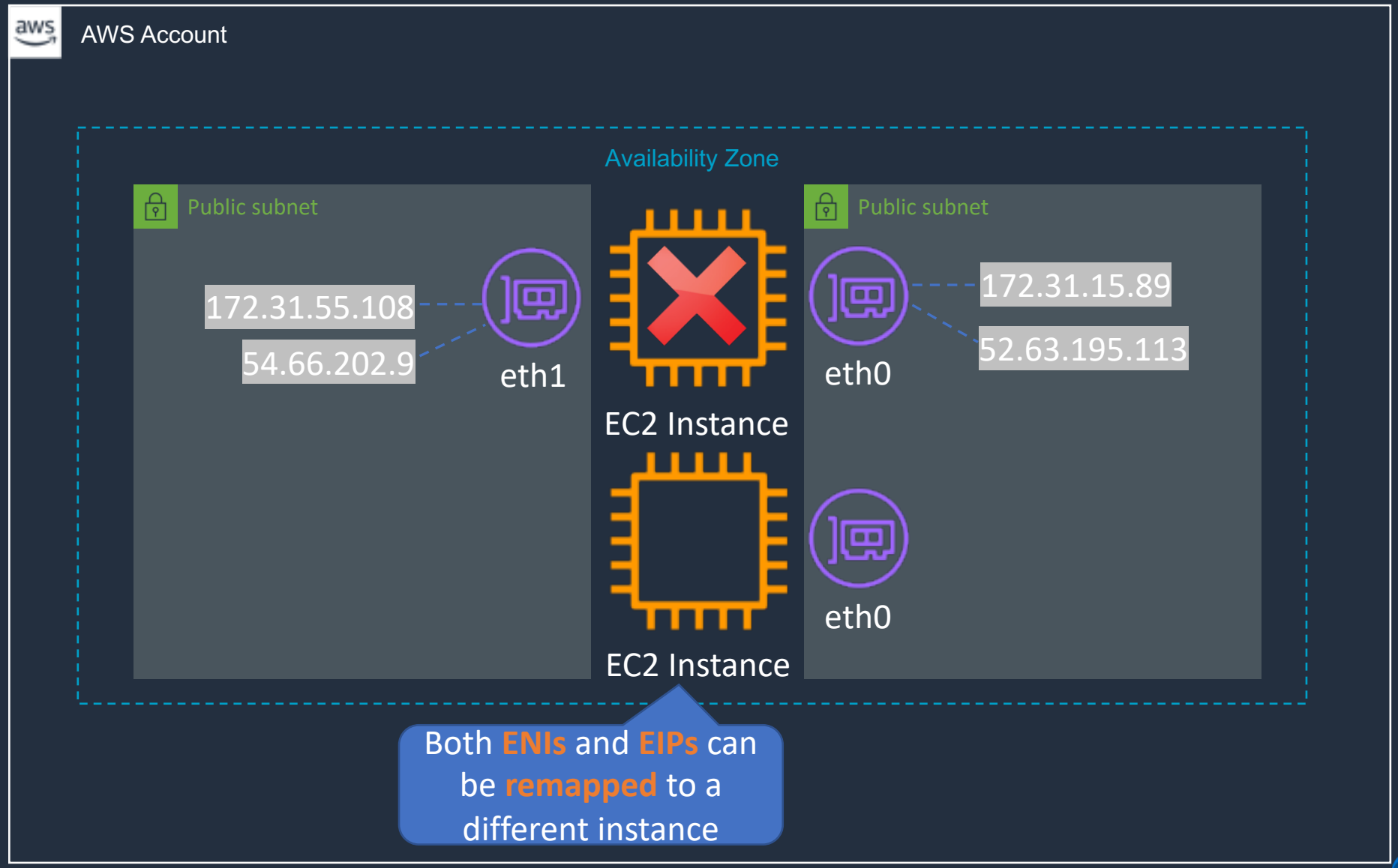
Public, Private and Elastic IP Addresses

DigitalCloud TRAINING

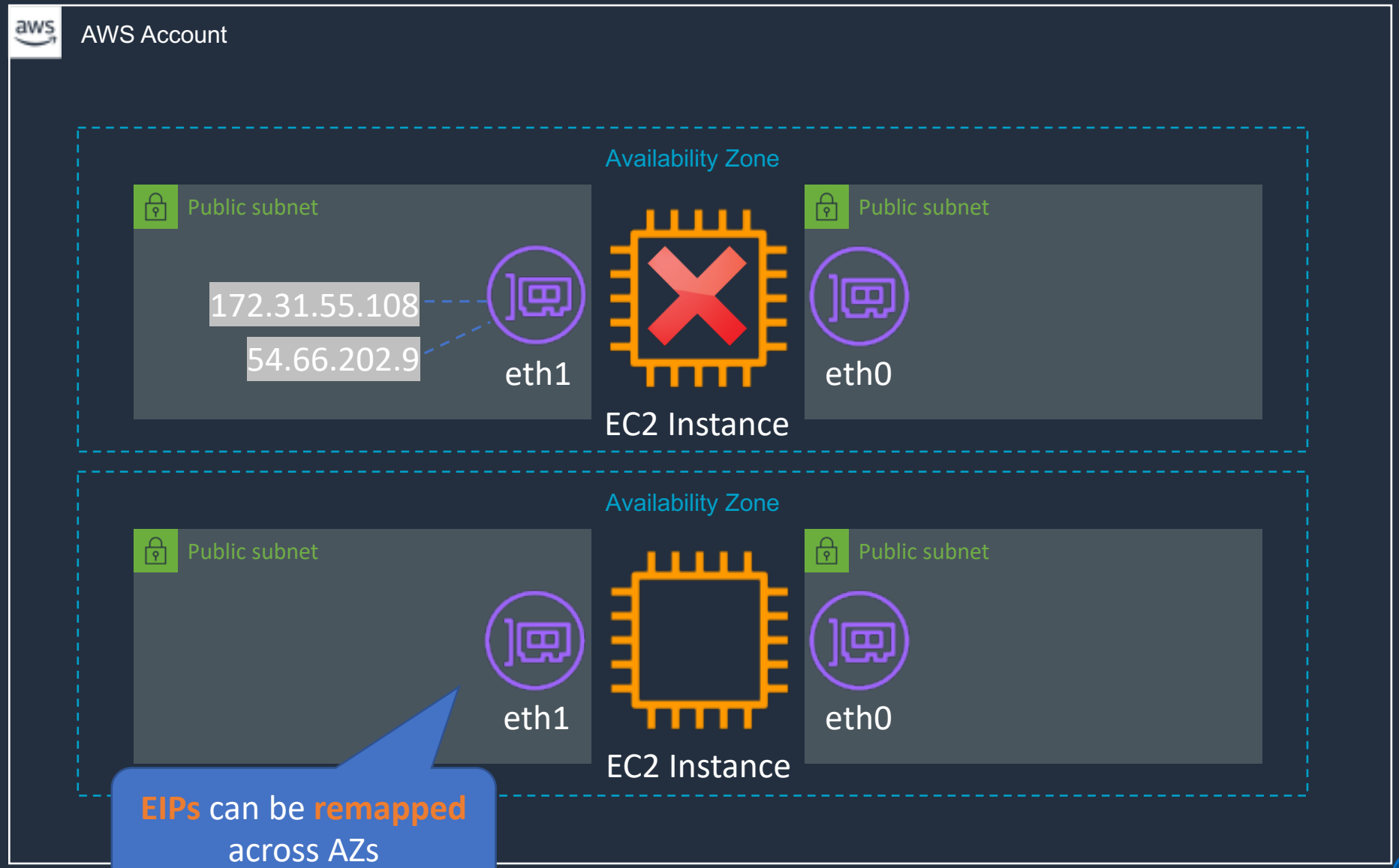
Public, Private and Elastic IP Addresses



Public, Private and Elastic IP Addresses



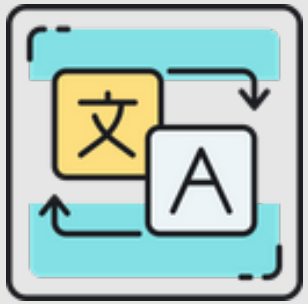
Public, Private and Elastic IP Addresses



Public, Private and Elastic IP addresses

Name	Description
Public IP address	Lost when the instance is stopped Used in Public Subnets No charge Associated with a private IP address on the instance Cannot be moved between instances
Private IP address	Retained when the instance is stopped Used in Public and Private Subnets
Elastic IP address	Static Public IP address You are charged if not used Associated with a private IP address on the instance Can be moved between instances and Elastic Network Adapters

NAT for Public Addresses



NAT for Public Addresses

```
[ec2-user@ip-172-31-32-63 ~]$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast sta
te UP group default qlen 1000
    link/ether 06:06:db:ad:56:28 brd ff:ff:ff:ff:ff:ff
    inet 172.31.32.63/20 brd 172.31.47.255 scope global dynamic eth0
       valid_lft 3330sec preferred_lft 3330sec
    inet6 fe80::406:dbff:fead:5628/64 scope link
       valid_lft forever preferred_lft forever
```

Src: 3.104.75.244	Dest: 54.23.86.101

Src: 54.23.86.101	Dest: 3.104.75.244

Src: 172.31.32.63	Dest: 54.23.86.101

Src: 54.23.86.101	Dest: 172.31.32.63

172.31.32.63

eth0

3.104.75.244

Public / Elastic

Association

IGW performs 1:1 NAT

Internet gateway

The Internet Gateway performs **NAT**

DigitalCloud TRAINING

Working with EC2 IP addresses

DigitalCloud TRAINING

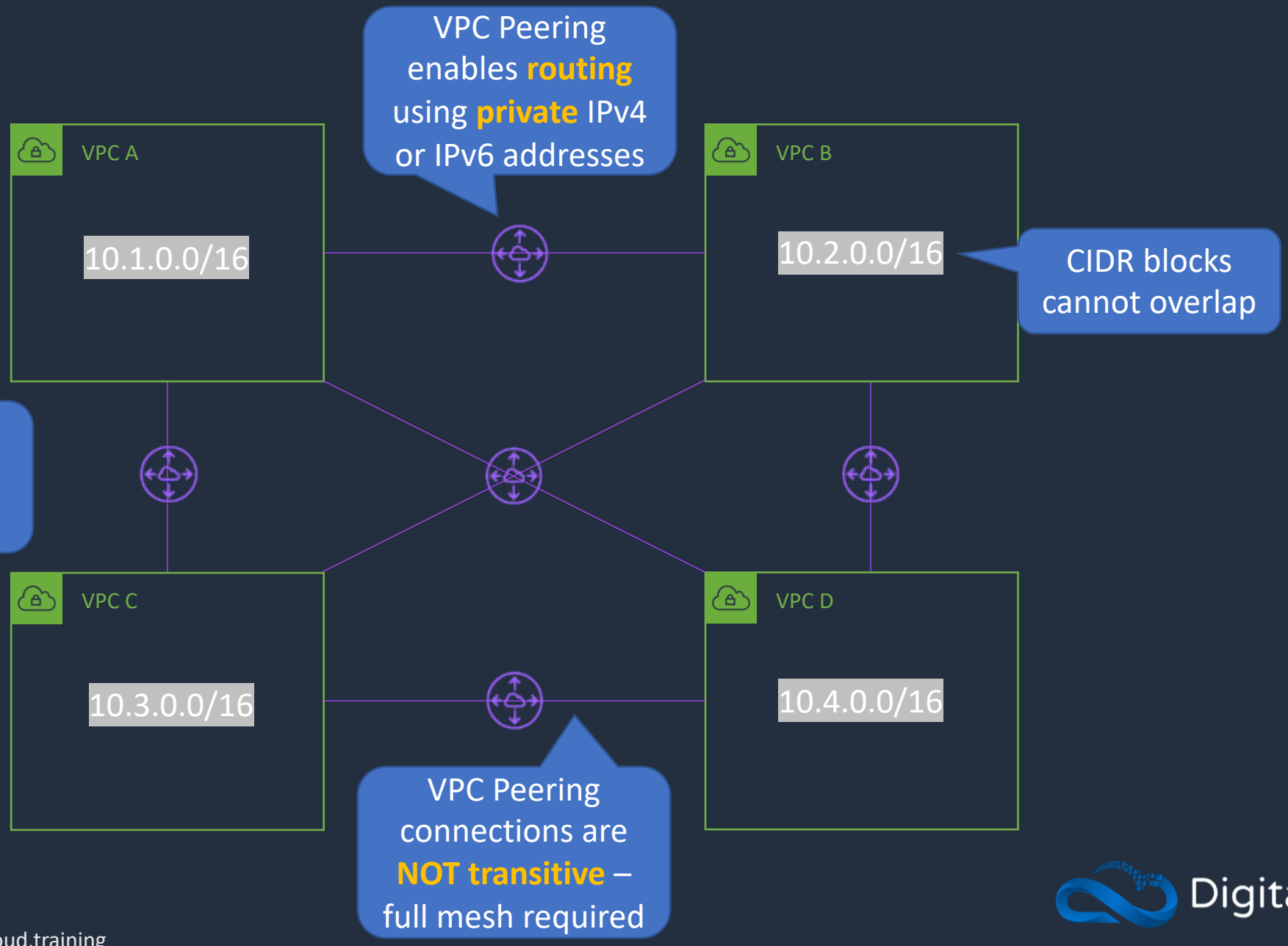
SECTION 6

Amazon VPC Connectivity and DNS

Create Second AWS Account

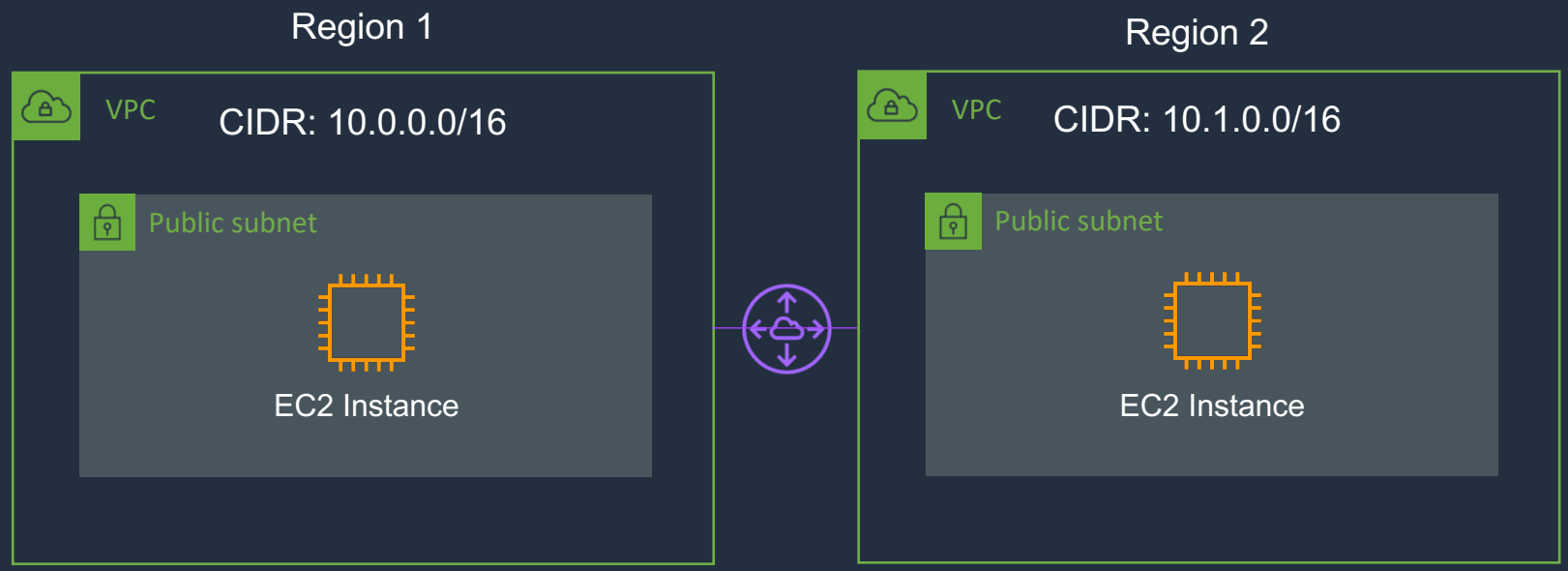
VPC Peering

VPC Peering



DigitalCloud TRAINING

VPC Peering



Security group (Region1-SG)

Protocol	Port	Source
ICMP	All	10.1.0.0/16
TCP	22	0.0.0.0/0

Security group (Region2-SG)

Protocol	Port	Source
ICMP	All	10.0.0.0/16
TCP	22	0.0.0.0/0

Route Table

Destination	Target
10.1.0.0/16	peering-id

Route Table

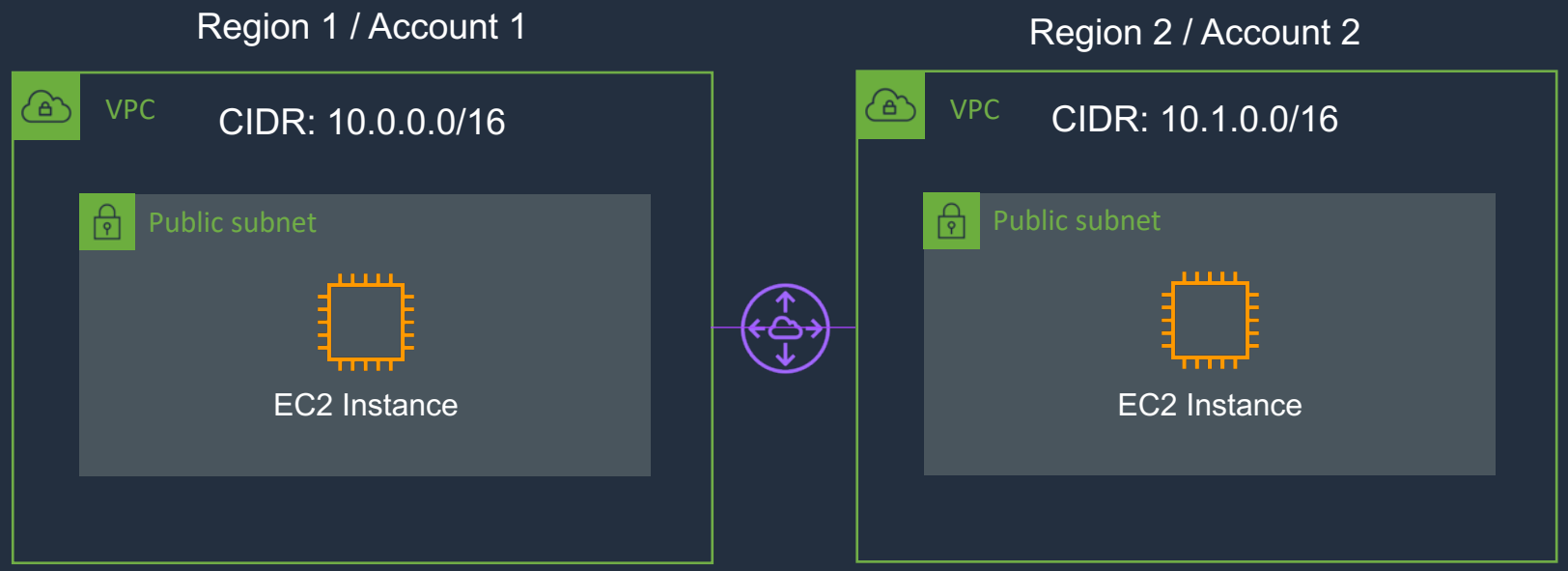
Destination	Target
10.0.0.0/16	peering-id

Setup VPC in Second Account

Create VPC Peering Connection

DigitalCloud TRAINING

Create VPC Peering Connection



Security group (Region1-SG)

Protocol	Port	Source
ICMP	All	10.1.0.0/16
TCP	22	0.0.0.0/0

Security group (Region2-SG)

Protocol	Port	Source
ICMP	All	10.0.0.0/16
TCP	22	0.0.0.0/0

Route Table

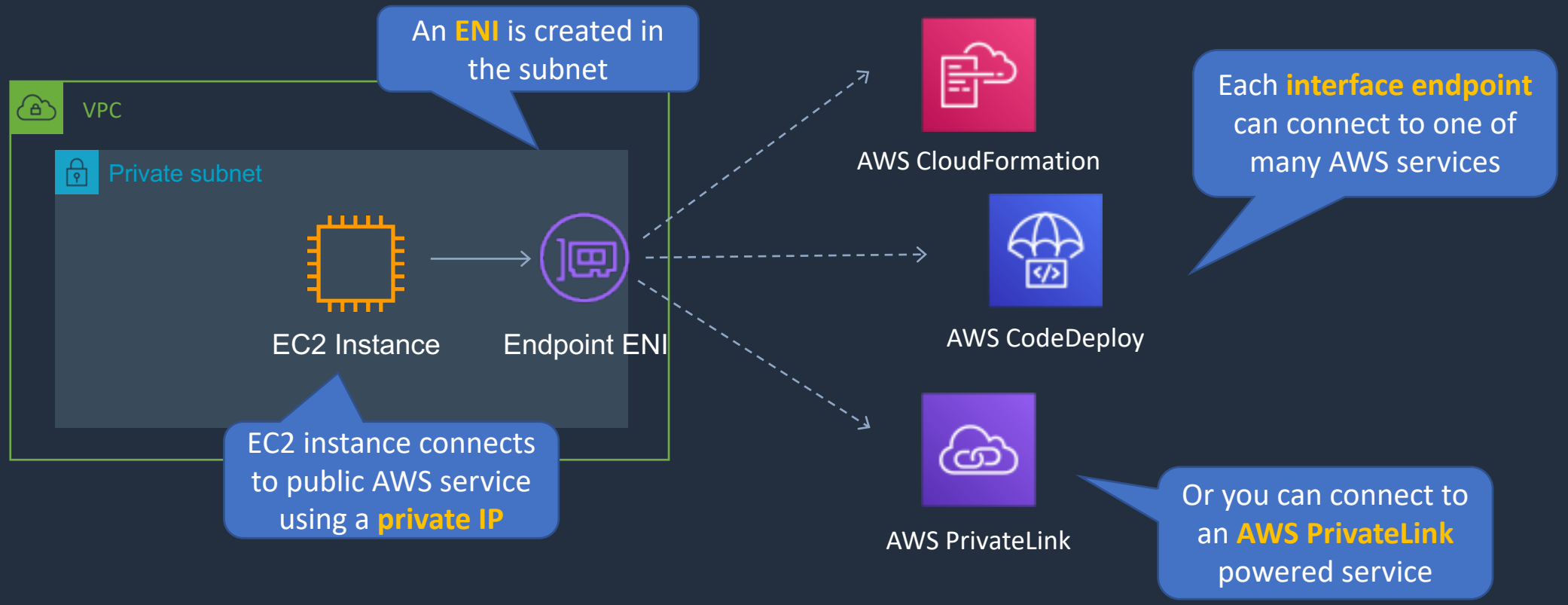
Destination	Target
10.1.0.0/16	peering-id

Route Table

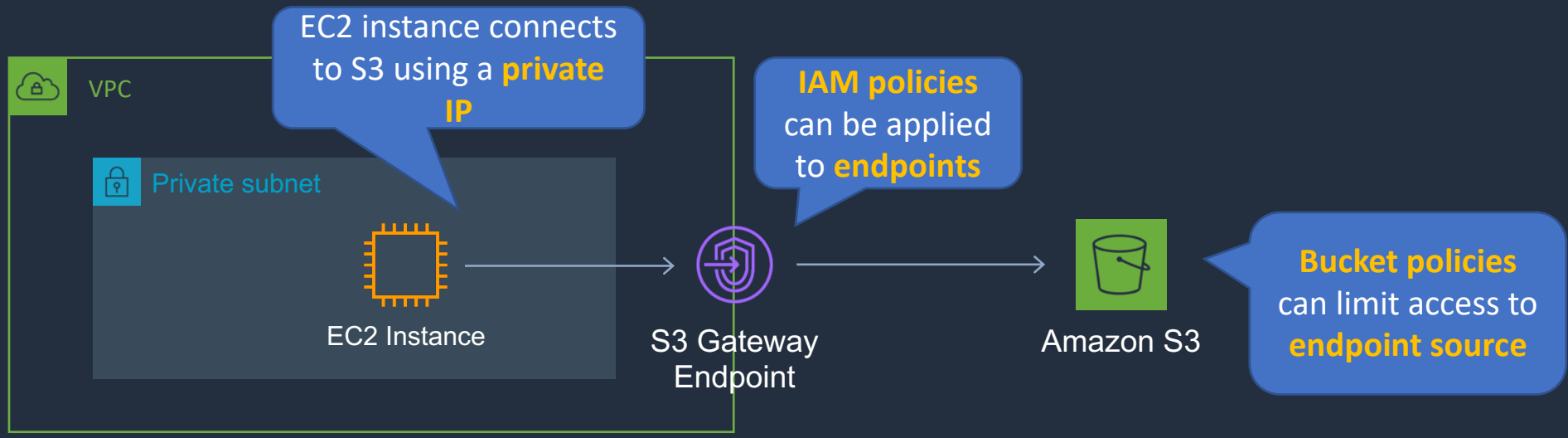
Destination	Target
10.0.0.0/16	peering-id

VPC Endpoints

VPC Interface Endpoints



VPC Gateway Endpoints



Route Table

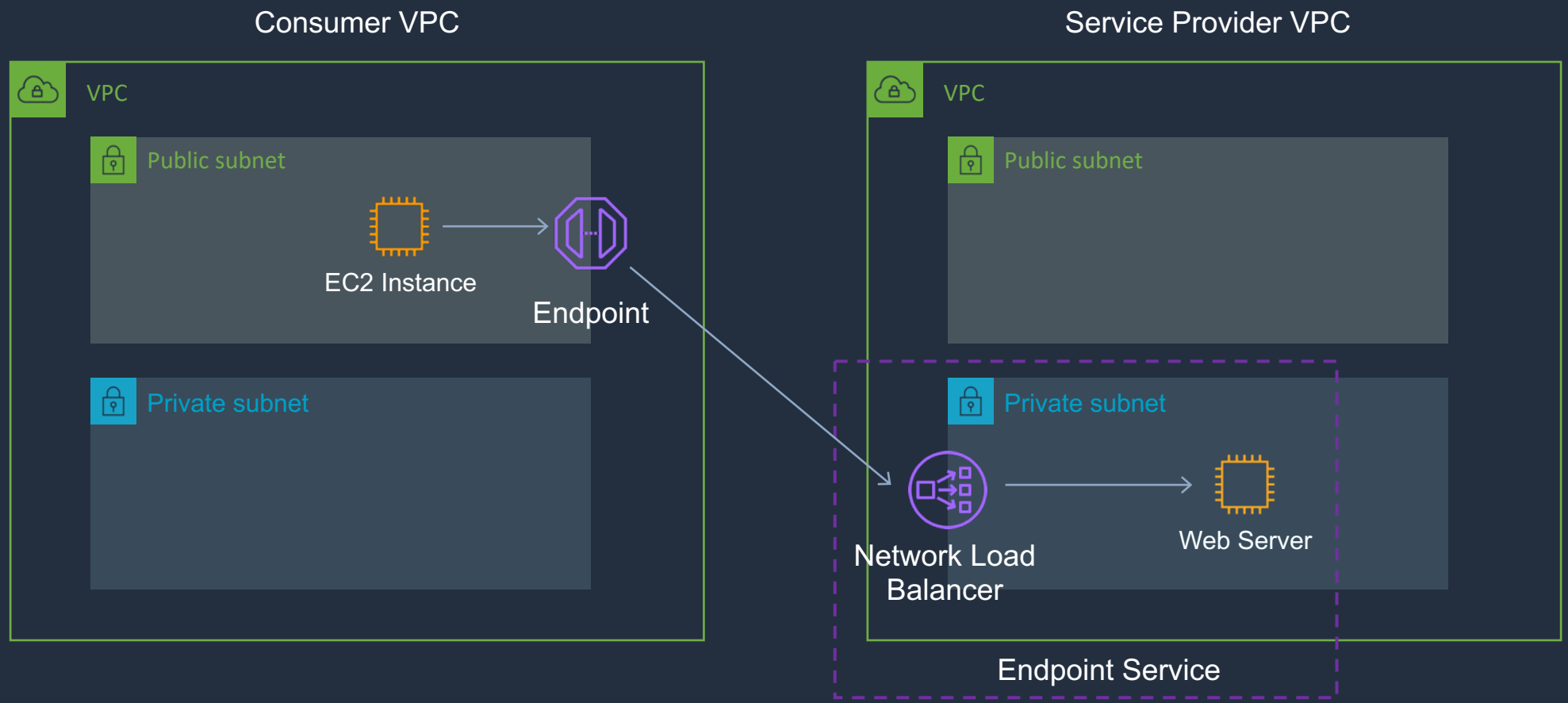
Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	*vpce-ID*

A **route table** entry is required with the prefix list for S3 and the **gateway ID**

VPC Endpoints

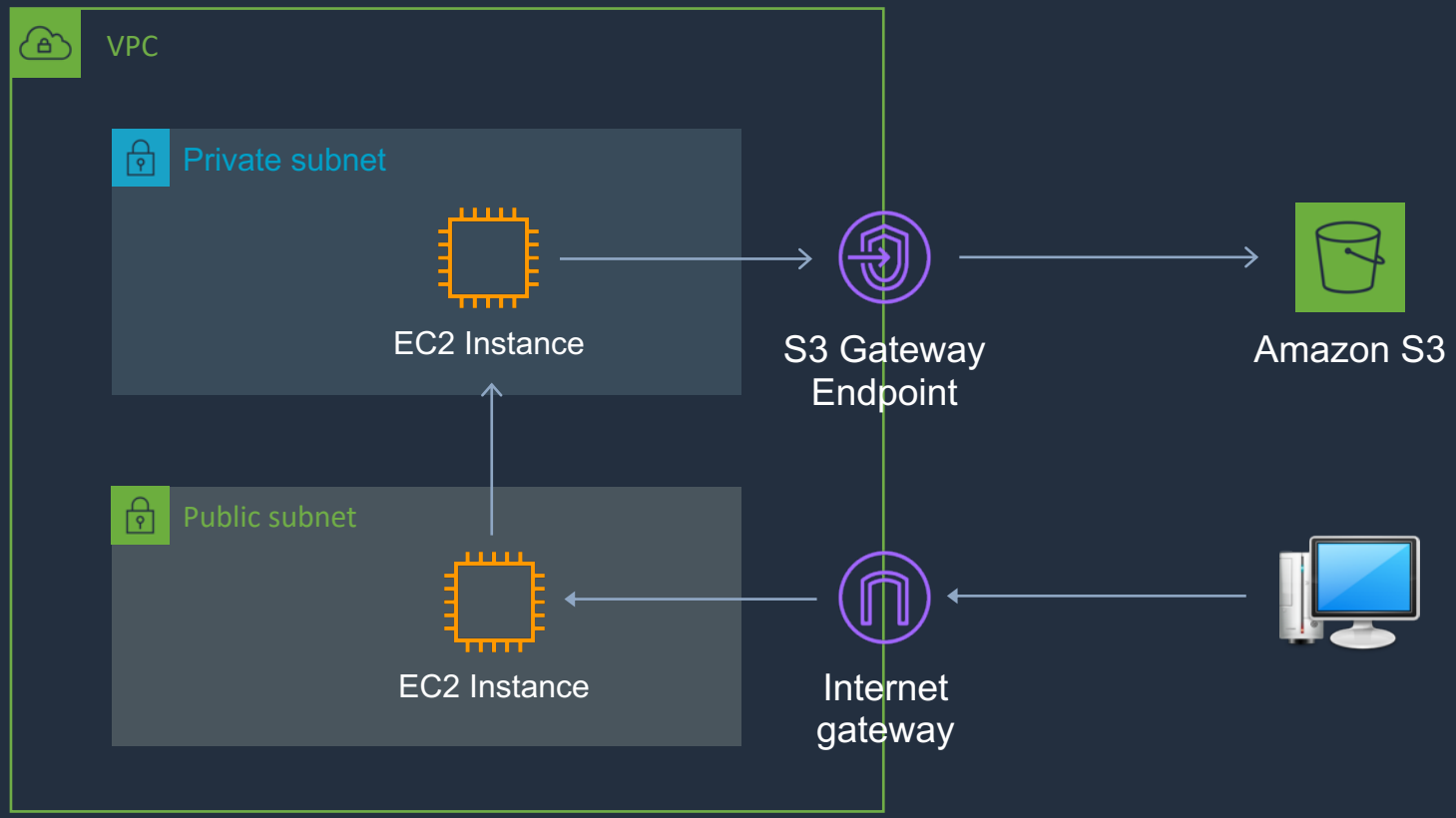
	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

Service Provider Model



Create VPC Endpoint

VPC Gateway Endpoints



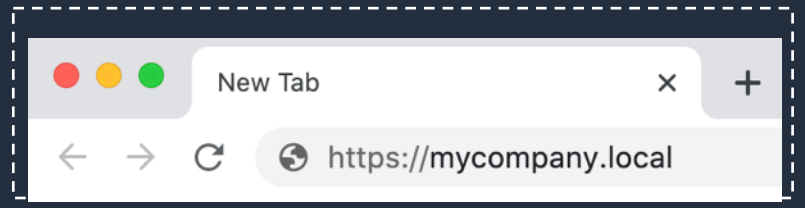
Private Subnet Route Table

Destination	Target
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 54.231.248.0/22, 54.231.252.0/24, 52.95.128.0/21)	*vpce-ID*

Amazon Route 53

Domain Name Service (DNS)

User enters website address in browser



Name	Type	Value
mycompany.local	A	192.168.0.1
emailserver.local	MX	192.168.0.2

DNS Server

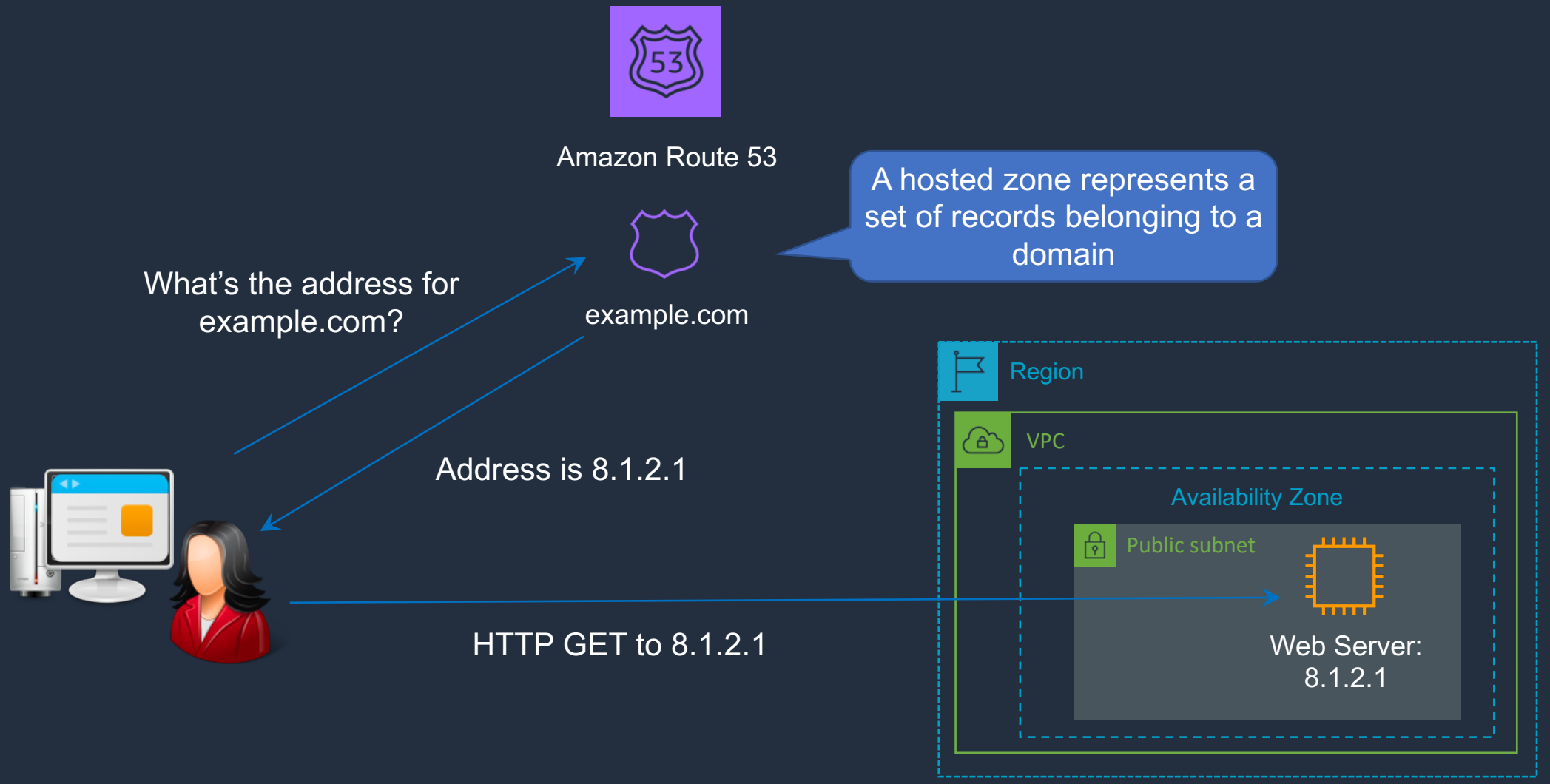
Domain name is resolved to the IP address of the webserver

Computer connects to 192.168.0.1

Web Server

DigitalCloud TRAINING

Amazon Route 53

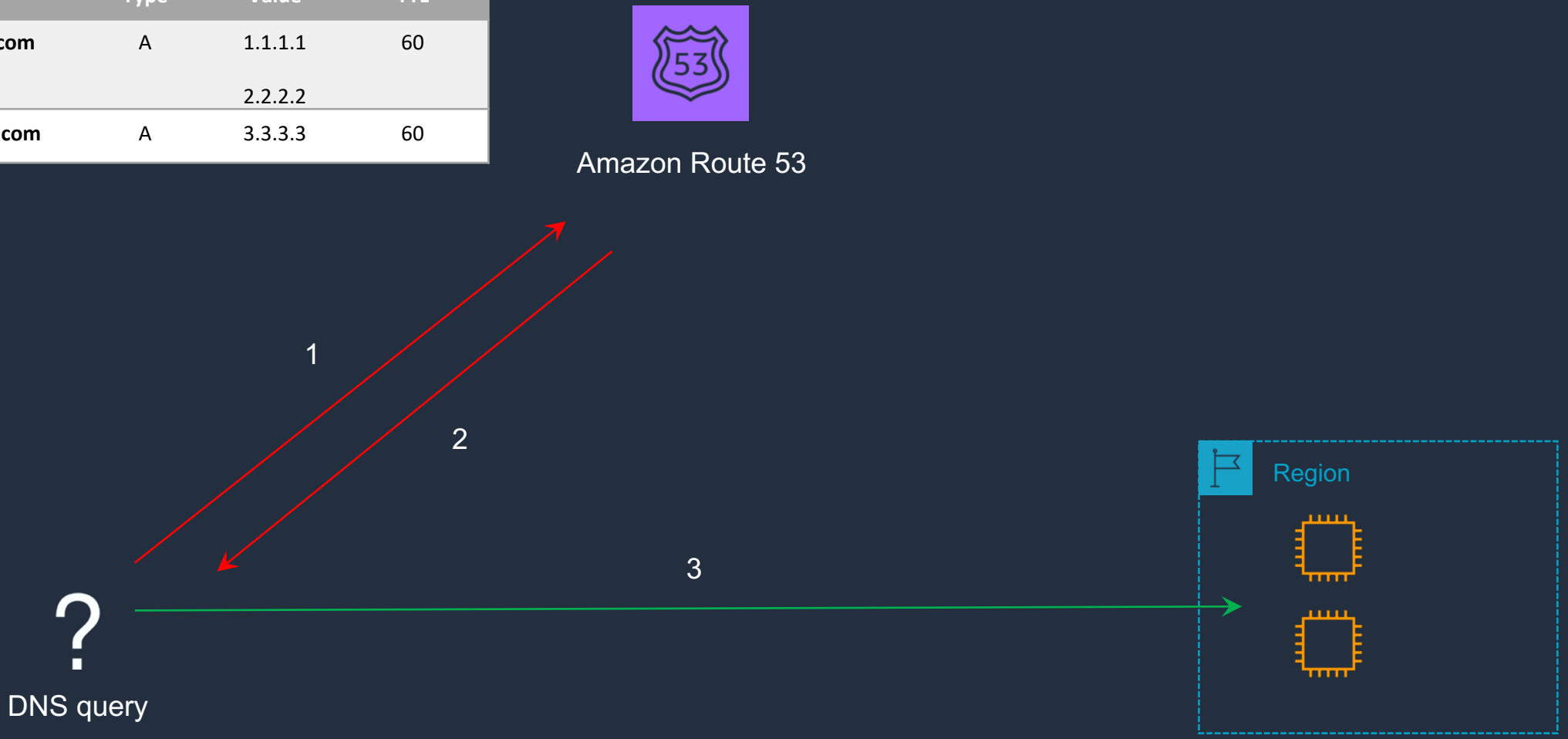


Amazon Route 53 Routing Policies

Routing Policy	What it does
Simple	Simple DNS response providing the IP address associated with a name
Failover	If primary is down (based on health checks), routes to secondary destination
Geolocation	Uses geographic location you're in (e.g. Europe) to route you to the closest region
Geoproximity	Routes you to the closest region within a geographic area
Latency	Directs you based on the lowest latency route to resources
Multivalue answer	Returns several IP addresses and functions as a basic load balancer
Weighted	Uses the relative weights assigned to resources to determine which to route to

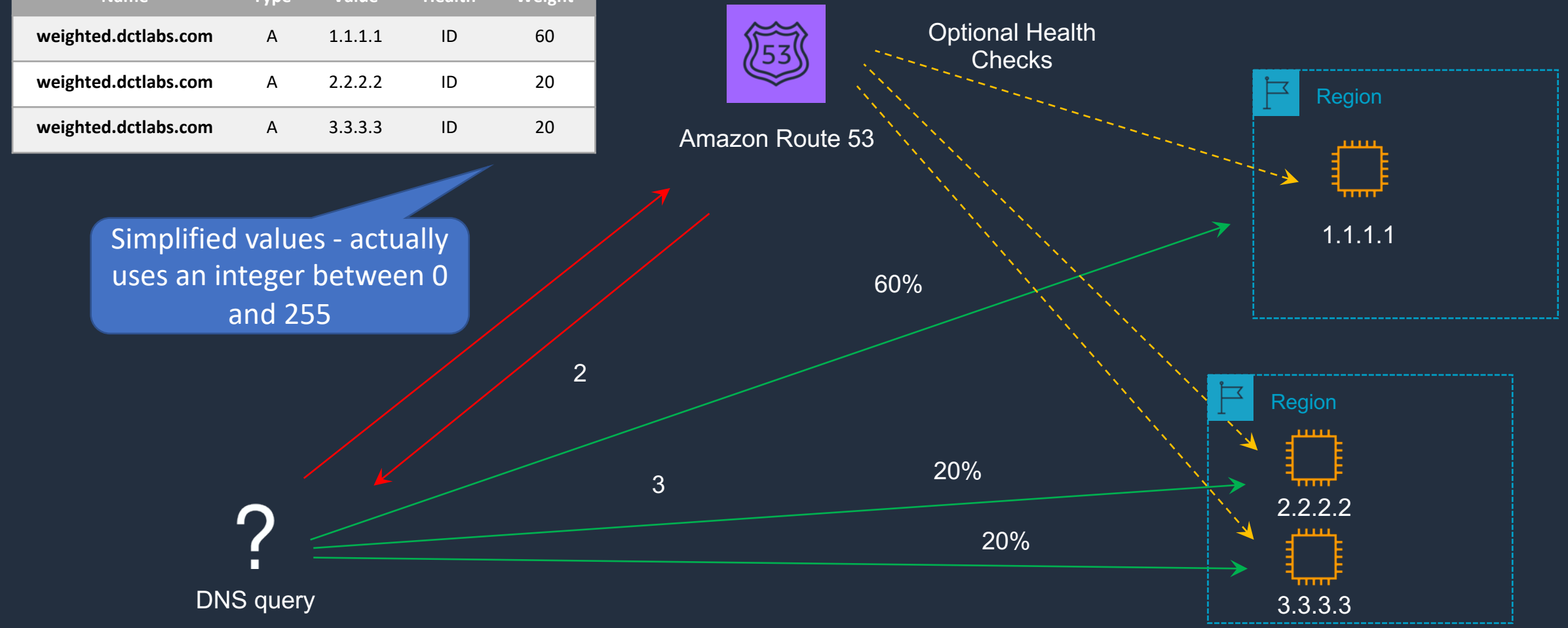
Amazon Route 53 – Simple Routing Policy

Name	Type	Value	TTL
simple.dctlabs.com	A	1.1.1.1 2.2.2.2	60
simple2.dctlabs.com	A	3.3.3.3	60



Amazon Route 53 – Weighted Routing Policy

Name	Type	Value	Health	Weight
weighted.dctlabs.com	A	1.1.1.1	ID	60
weighted.dctlabs.com	A	2.2.2.2	ID	20
weighted.dctlabs.com	A	3.3.3.3	ID	20



Amazon Route 53 – Latency Routing Policy

Name	Type	Value	Health	Region
latency.dctlabs.com	A	1.1.1.1	ID	ap-southeast-1
latency.dctlabs.com	A	2.2.2.2	ID	us-east-1
latency.dctlabs.com	A	alb-id	ID	ap-southeast-2

Amazon Route 53

Optional Health Checks

Singapore

?

DNS query

Region – ap-southeast-1

1.1.1.1

Region – us-east-1

2.2.2.2

Sydney

?

DNS query

Region – ap-southeast-2

ALB

New York

?

DNS query

DigitalCloud TRAINING

Amazon Route 53 – Failover Routing Policy

Name	Type	Value	Health	Record Type
failover.dctlabs.com	A	1.1.1.1	ID	Primary
failover.dctlabs.com	A	alb-id		Secondary

Amazon Route 53

Health check is **required** on Primary

Region – us-east-1

1.1.1.1

?

DNS query

Region – ap-southeast-2

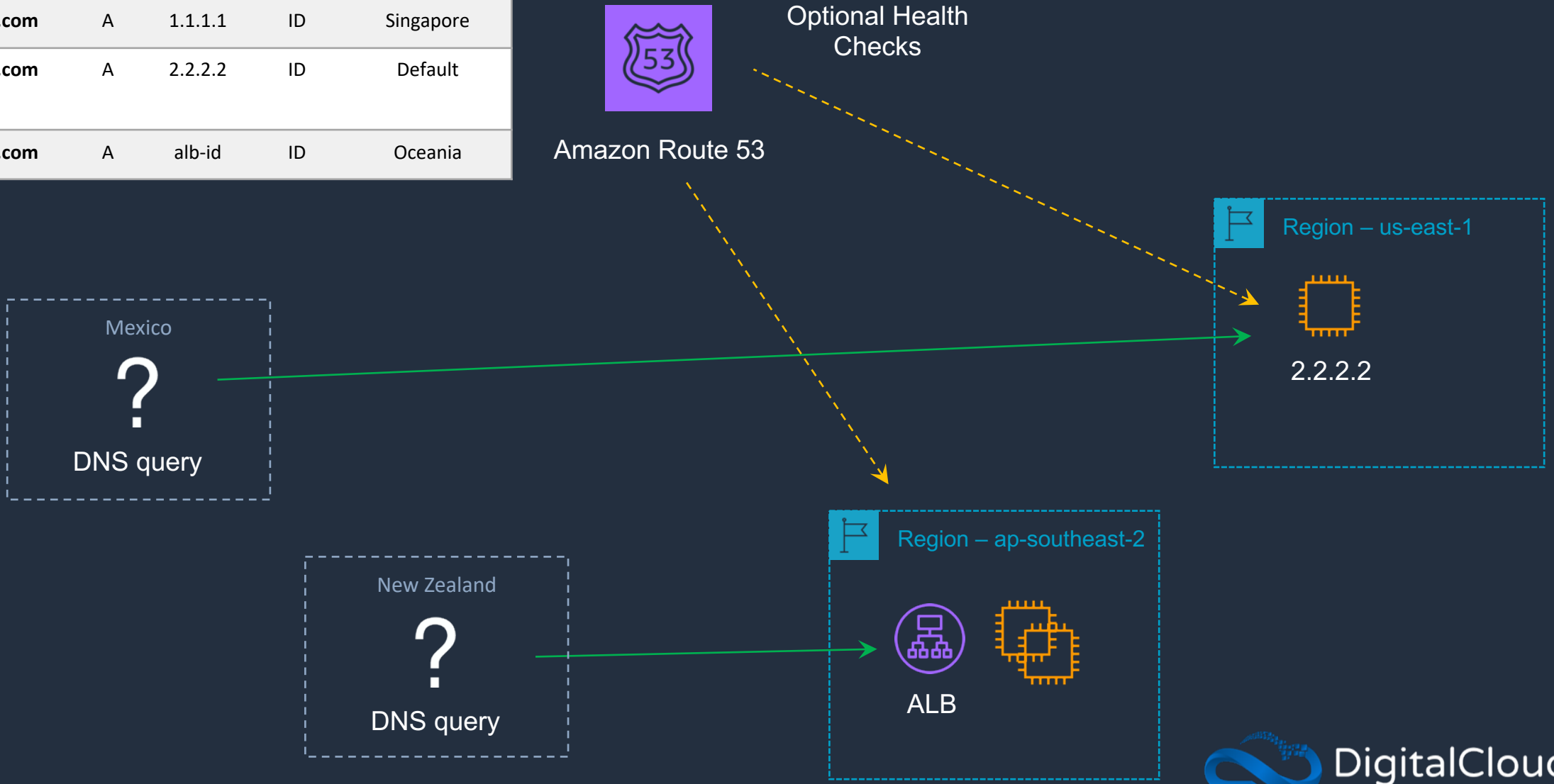
ALB

ap-southeast-2 is the **secondary** Region

DigitalCloud TRAINING

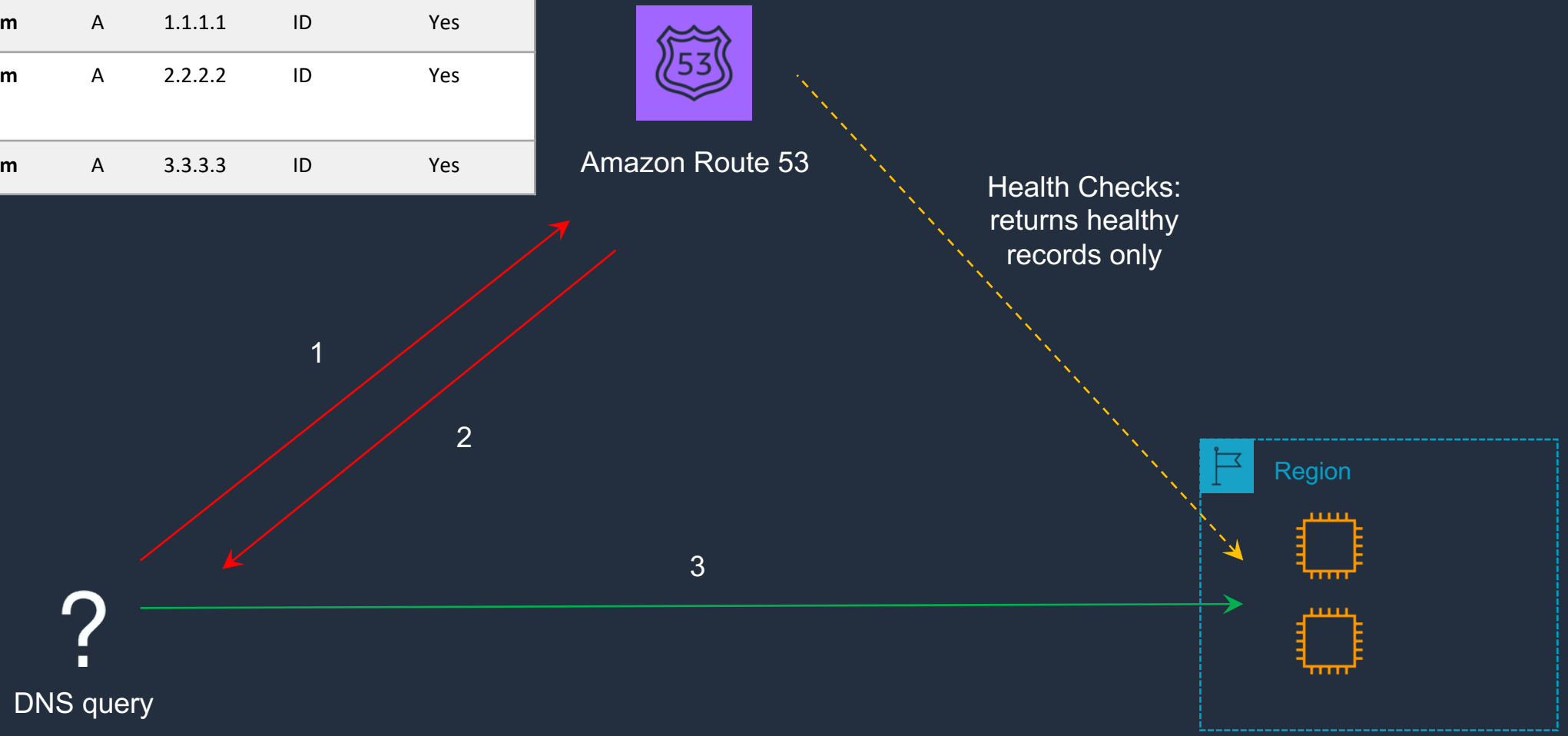
Amazon Route 53 – Geolocation Routing Policy

Name	Type	Value	Health	Geolocation
geolocation.dctlabs.com	A	1.1.1.1	ID	Singapore
geolocation.dctlabs.com	A	2.2.2.2	ID	Default
geolocation.dctlabs.com	A	alb-id	ID	Oceania



Amazon Route 53 – Multivalue Routing Policy

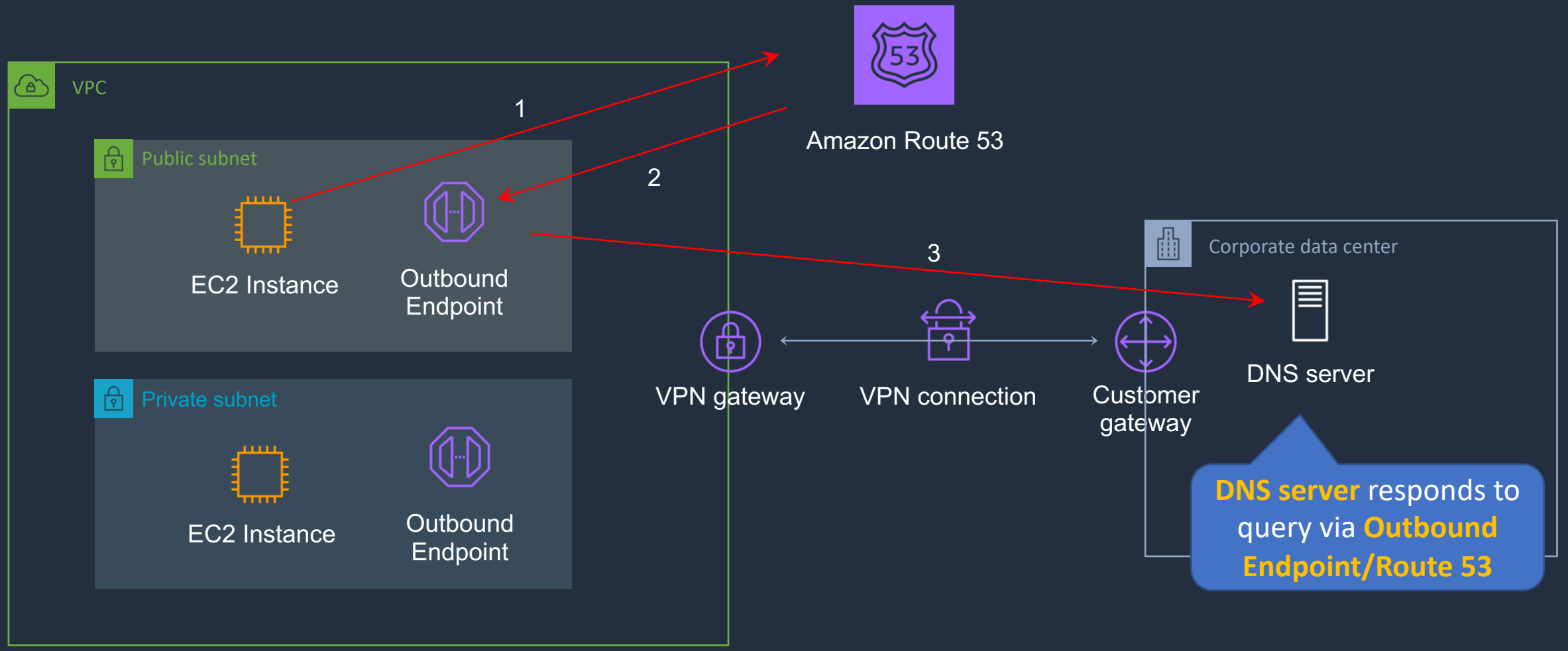
Name	Type	Value	Health	Multi Value
multivalue.dctlabs.com	A	1.1.1.1	ID	Yes
multivalue.dctlabs.com	A	2.2.2.2	ID	Yes
multivalue.dctlabs.com	A	3.3.3.3	ID	Yes



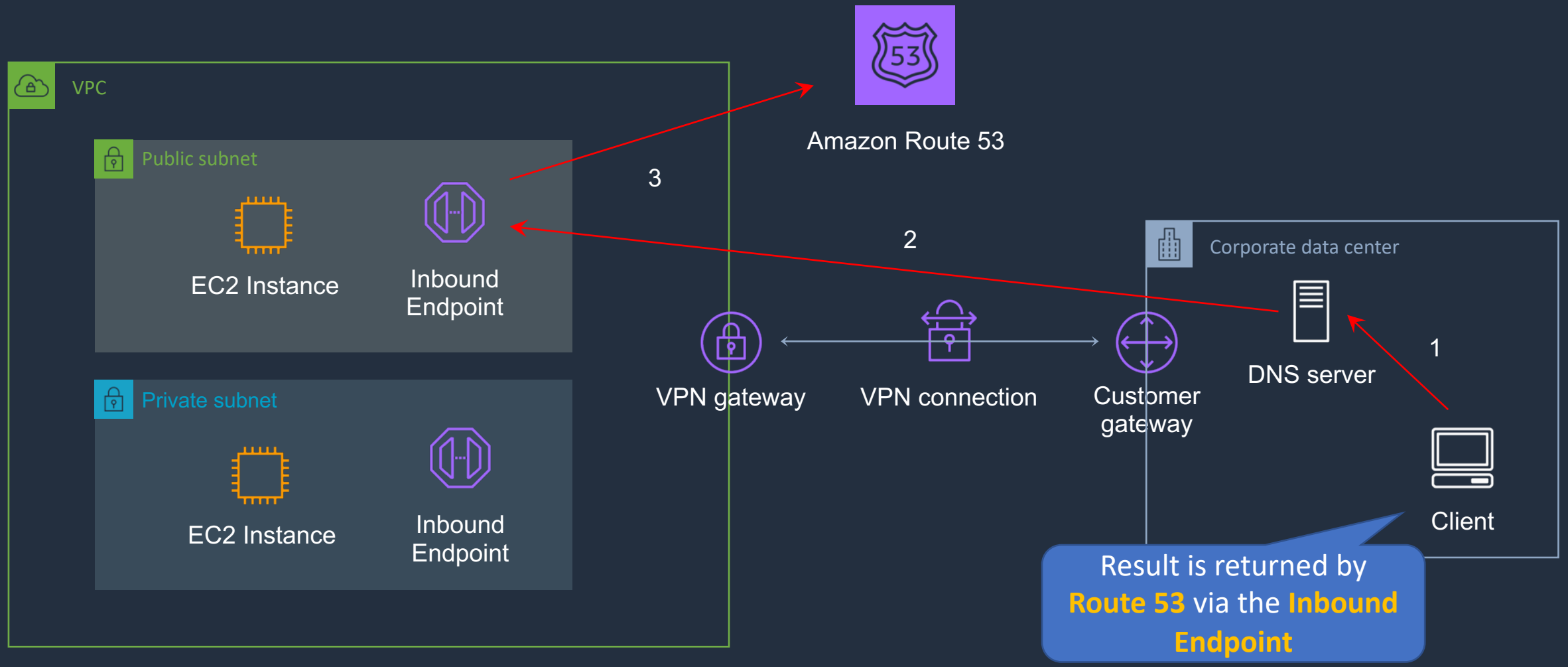
Test Route 53 Routing Policies

Amazon Route 53 Resolver

Route 53 Resolver – Outbound Endpoints



Route 53 Resolver – Inbound Endpoints

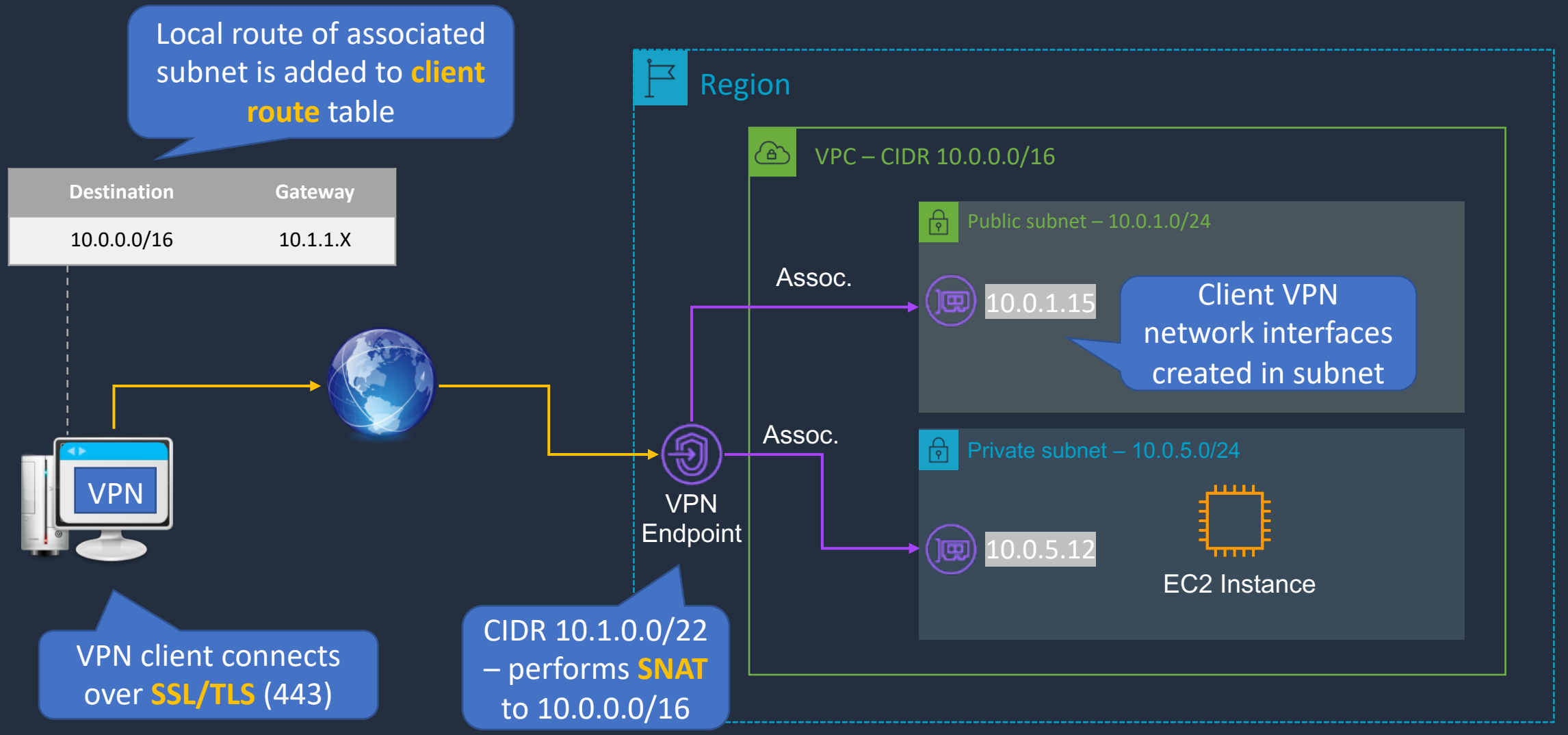


SECTION 7

Hybrid Connectivity

AWS Client VPN

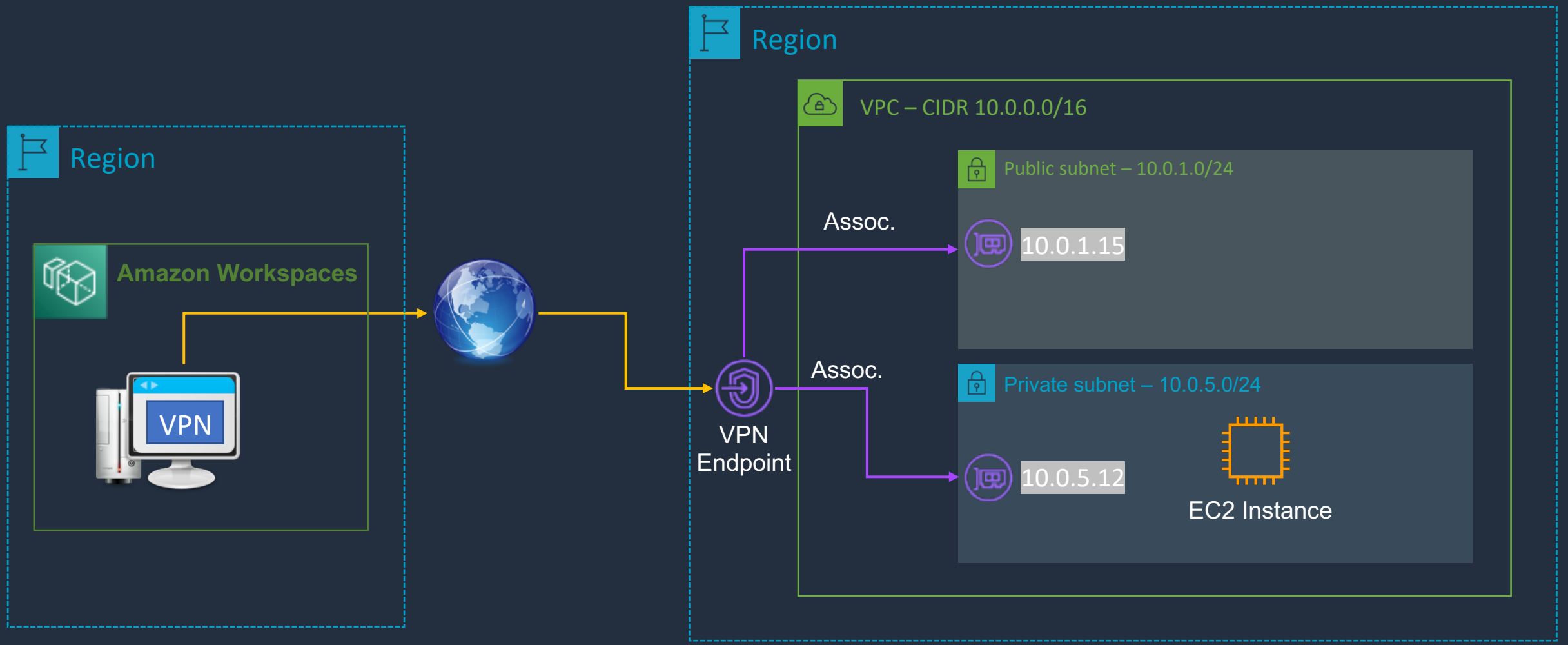
AWS Client VPN



Deploy AWS Client VPN

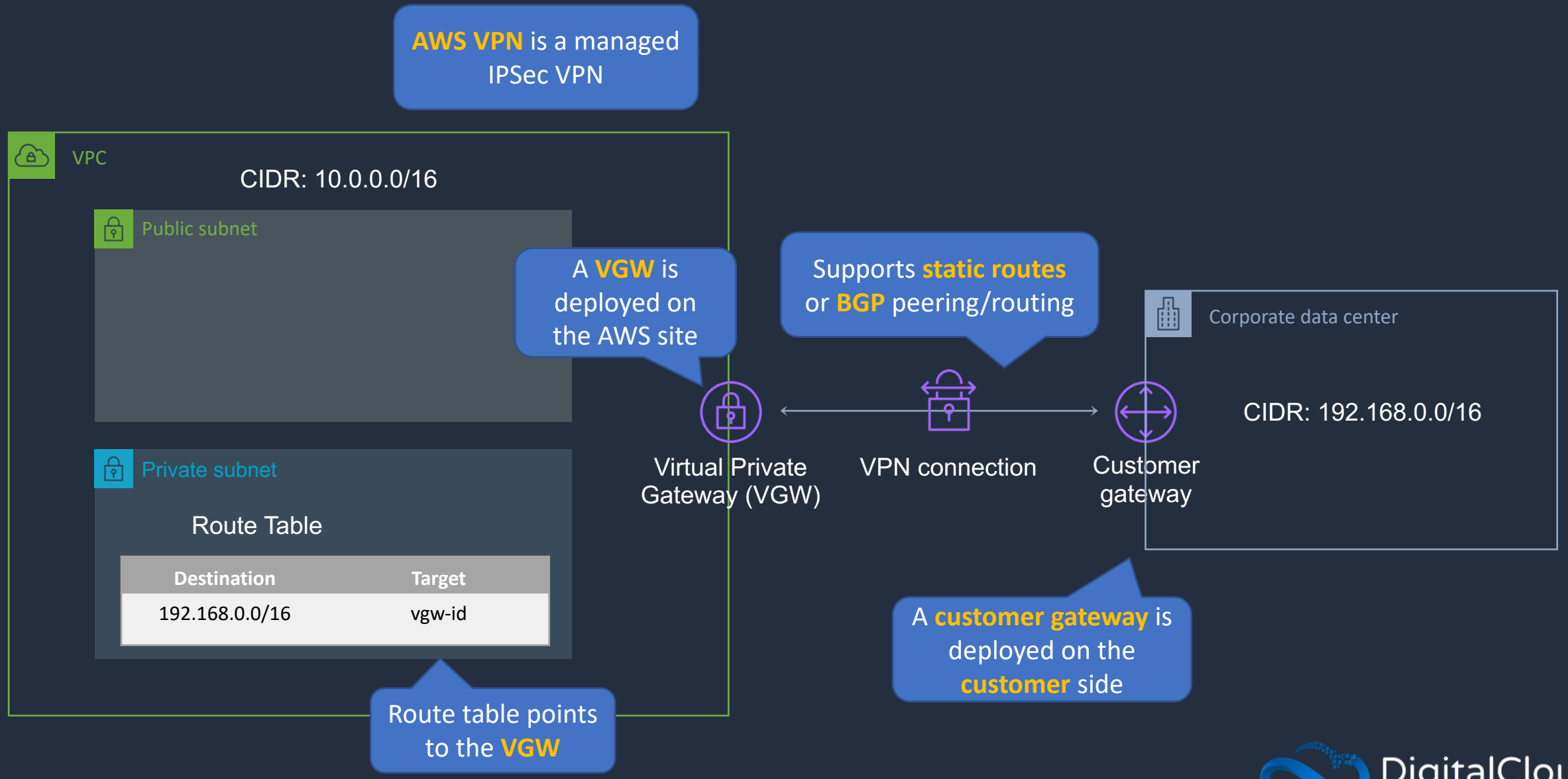
DigitalCloud TRAINING

AWS Client VPN – Hands-On



AWS Site-to-Site VPN

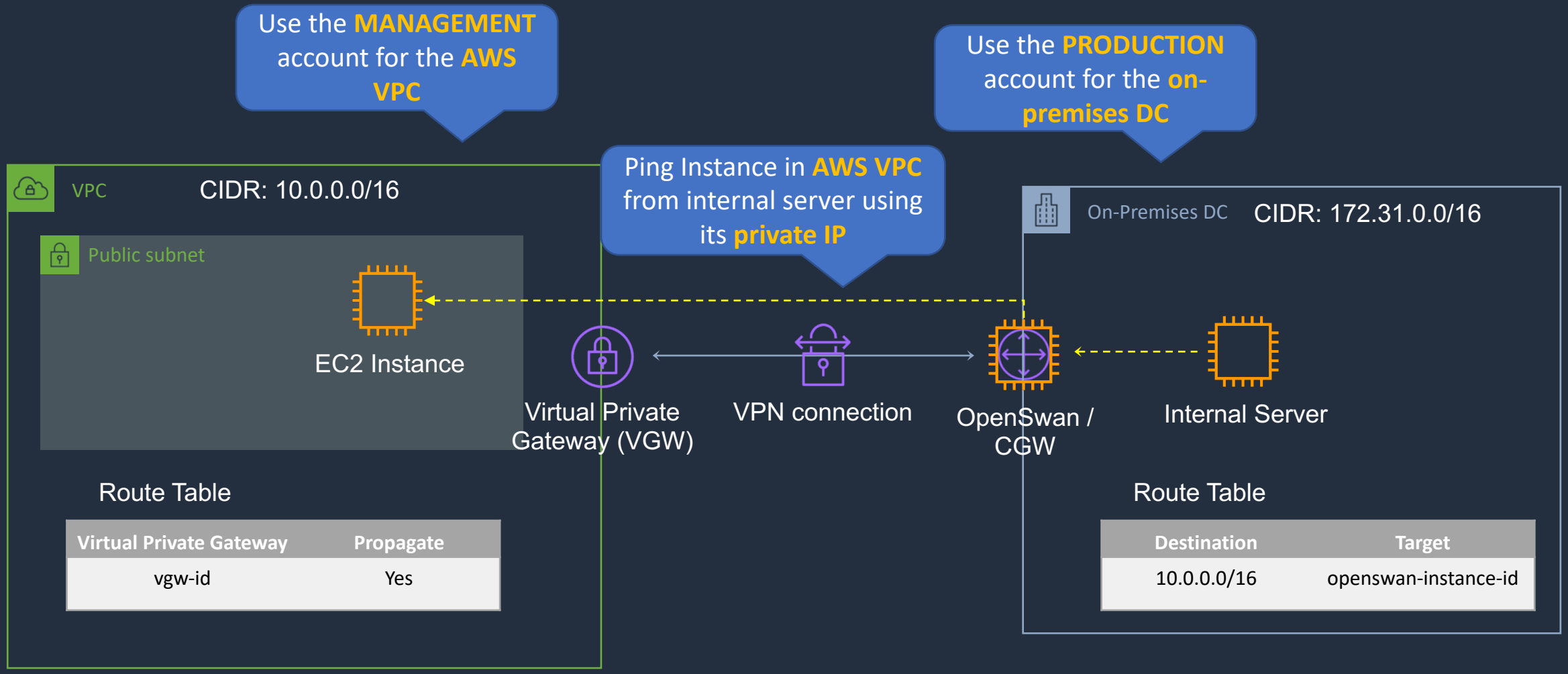
AWS Site-to-Site VPN



Deploy AWS Site-to-Site VPN

DigitalCloud TRAINING

AWS Site-to-Site VPN – Hands-On



Route Table

Virtual Private Gateway	Propagate
vgw-id	Yes

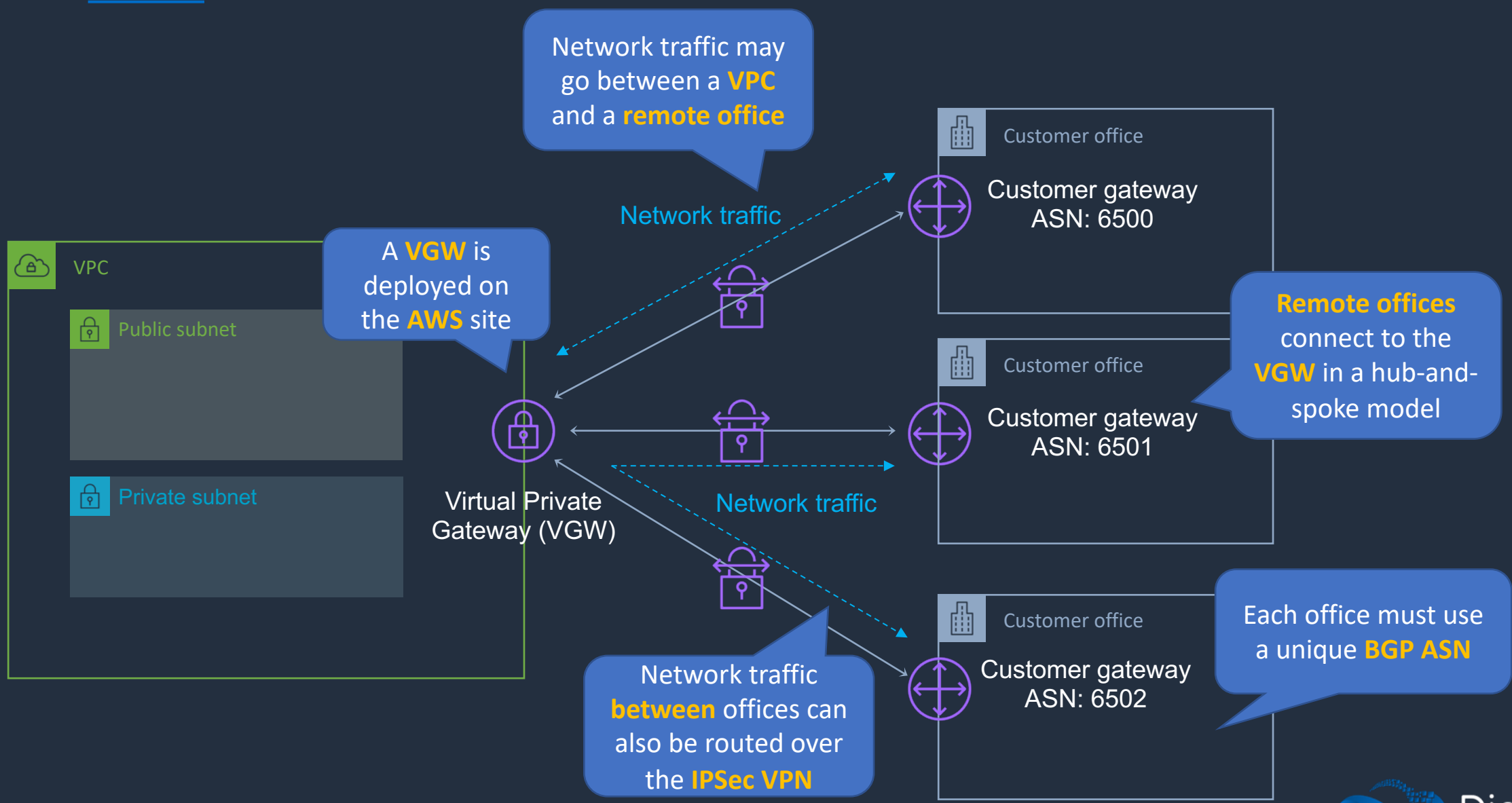
Route Table

Destination	Target
10.0.0.0/16	openswan-instance-id

DigitalCloud TRAINING

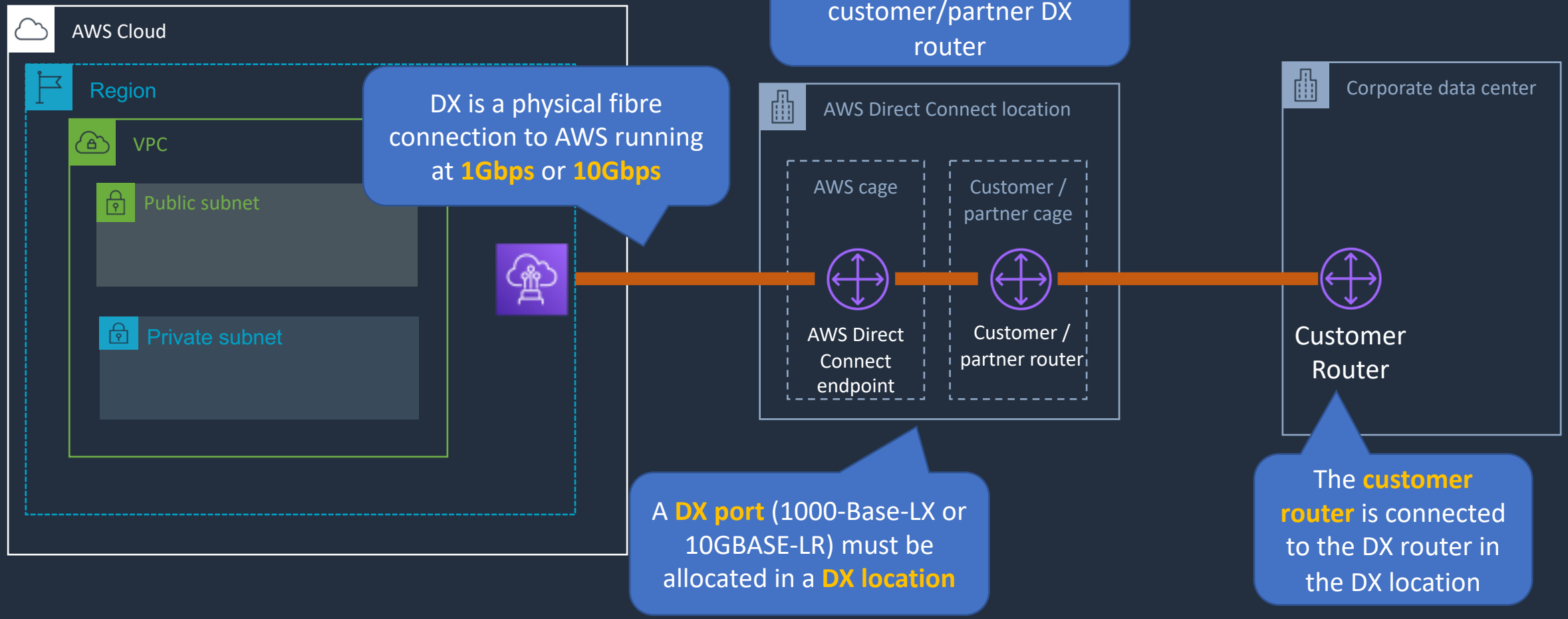
AWS VPN CloudHub

AWS VPN CloudHub



AWS Direct Connect (DX)

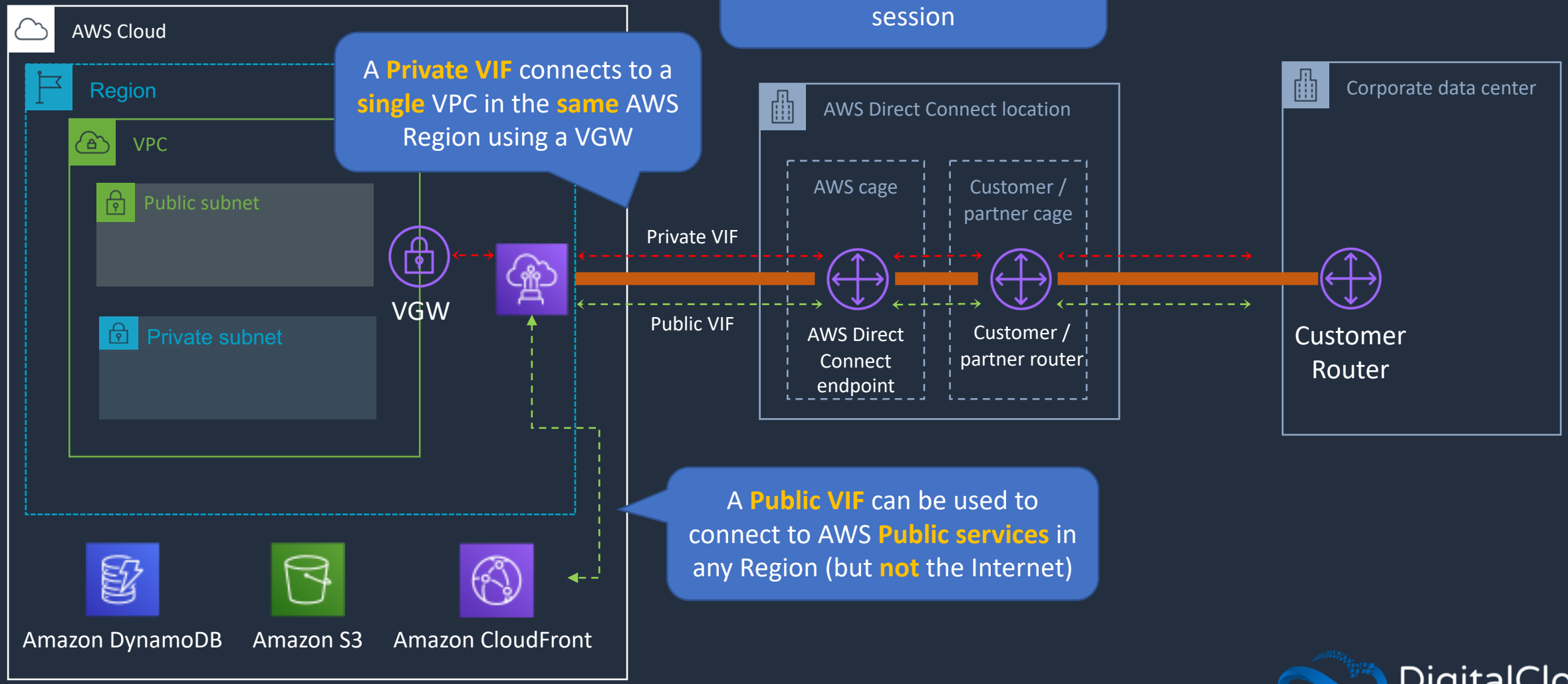
AWS Direct Connect (DX)



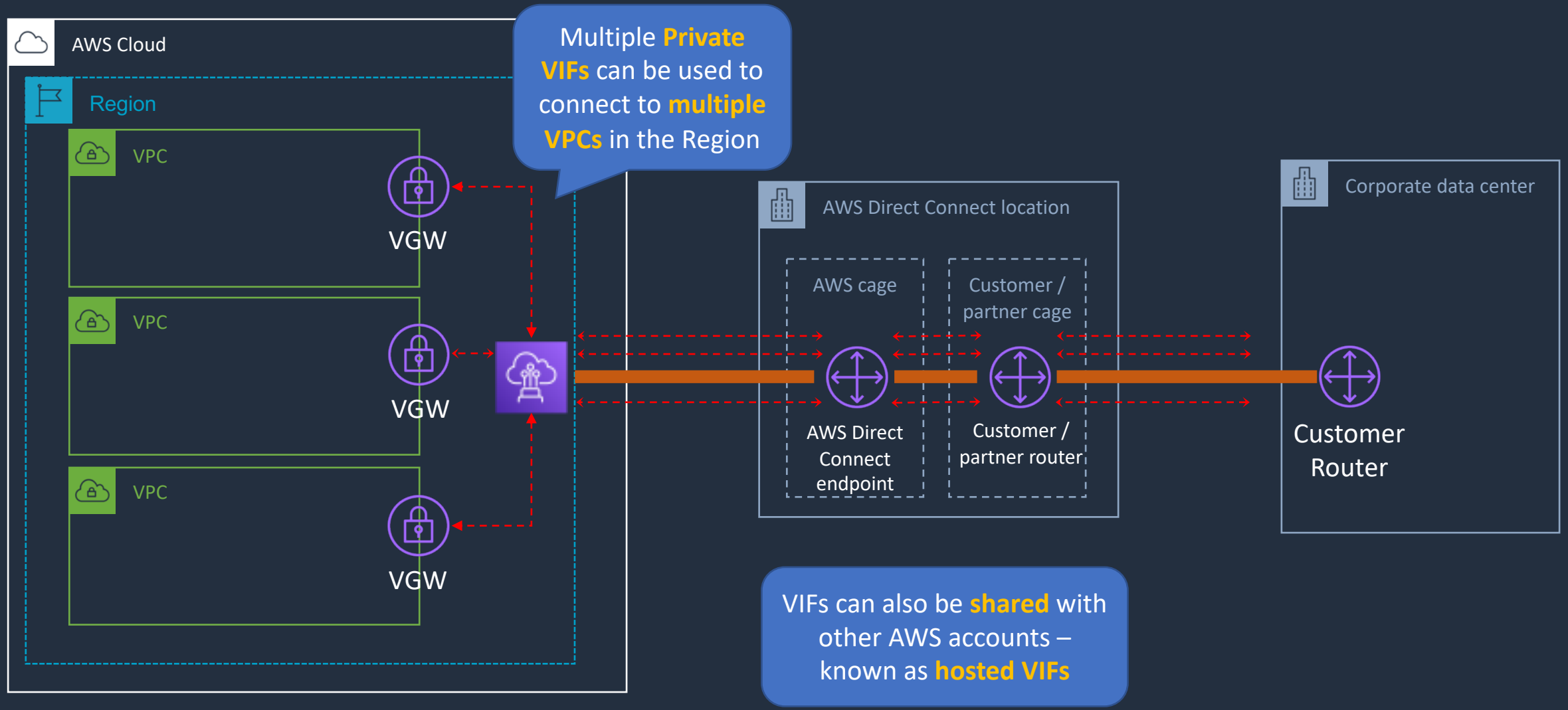
AWS Direct Connect Benefits

- **Private** connectivity between AWS and your data center / office
- Consistent network experience – increased **speed/latency** & **bandwidth/throughput**
- Lower costs for organizations that transfer **large** volumes of data

AWS Direct Connect (DX)



AWS Direct Connect (DX)

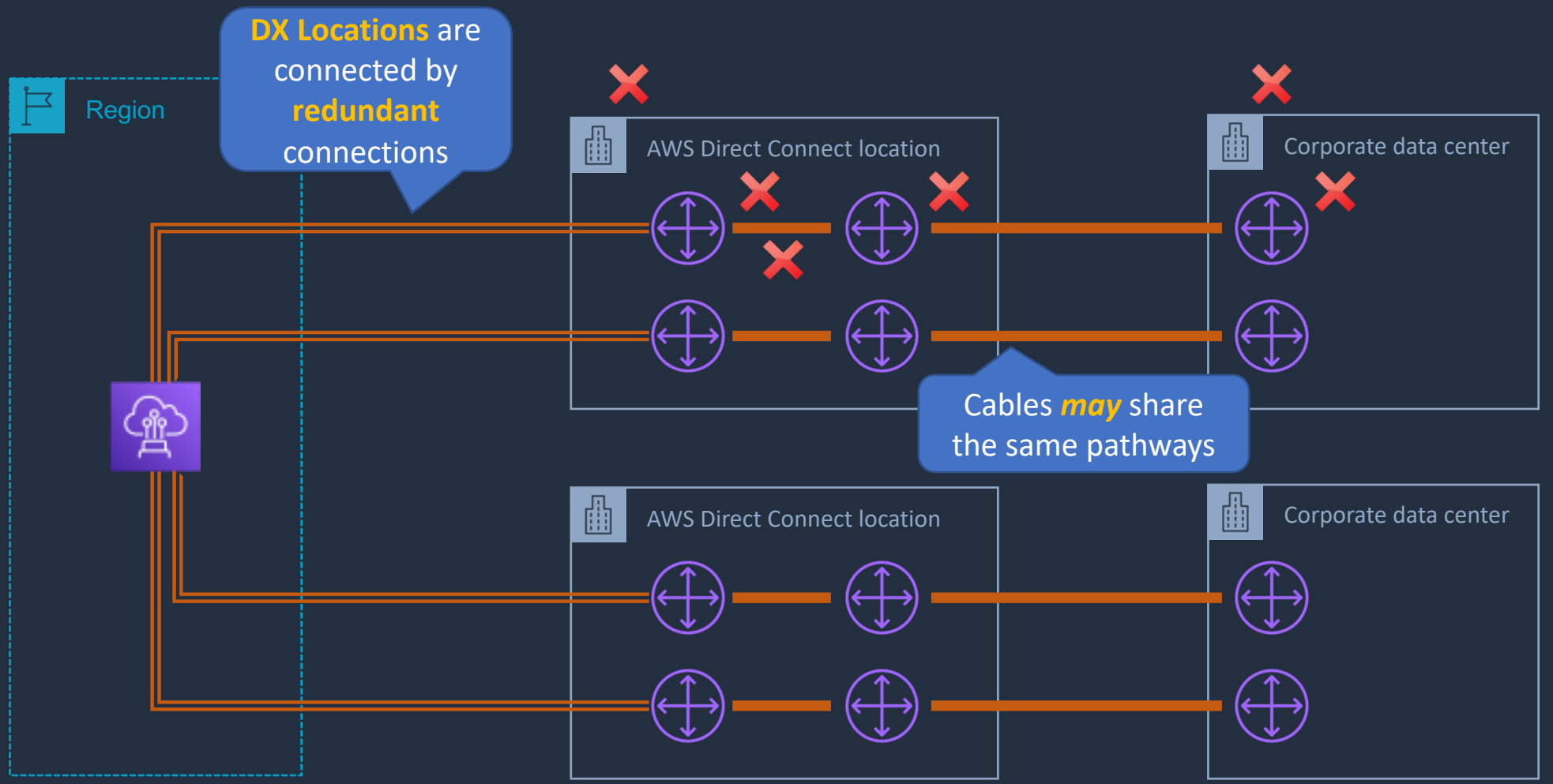


AWS Direct Connect (DX)

- Speeds from 50Mbps to 500Mbps can also be accessed via an APN partner (uses hosted VIFs or hosted connections):
  - A ***hosted VIF*** is a single VIF that is shared with other customers (shared bandwidth)
  - A ***hosted connection*** is a DX connection with a single VIF dedicated to you
- DX Connections are **NOT** encrypted!
- Use an **IPSec S2S VPN** connection over a VIF to add encryption in transit
- Link aggregation groups (**LAG**s) can be used to combine multiple **physical** connections into a single **logical** connection using **LACP** – provides improved **speed**

DigitalCloud TRAINING

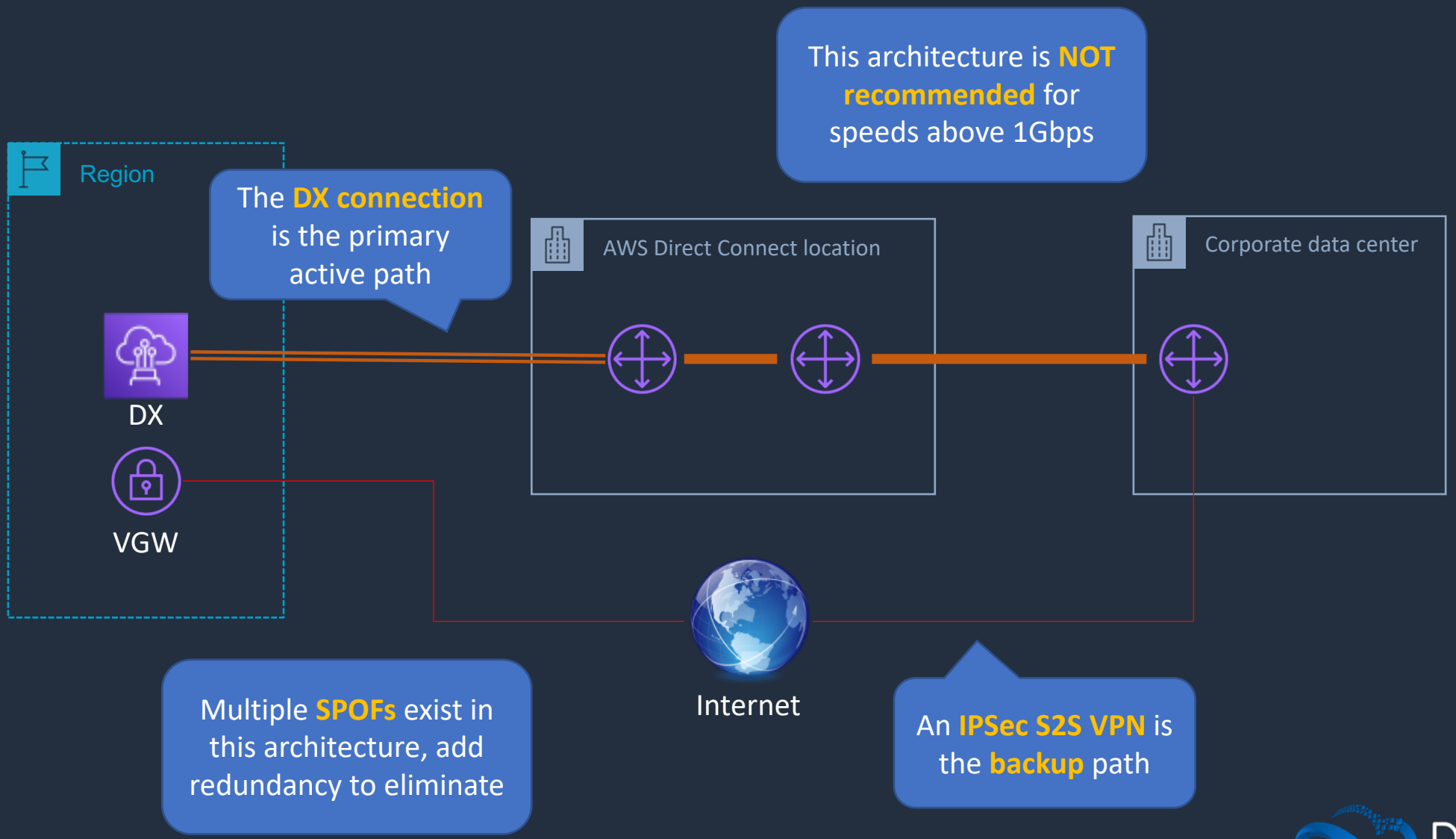
DX - Native High Availability



✕ = Single Point of Failure

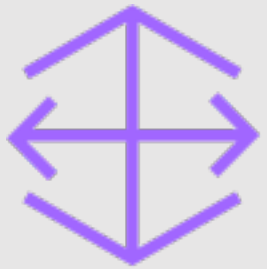
DigitalCloud TRAINING

Direct Connect + IPSec S2S VPN

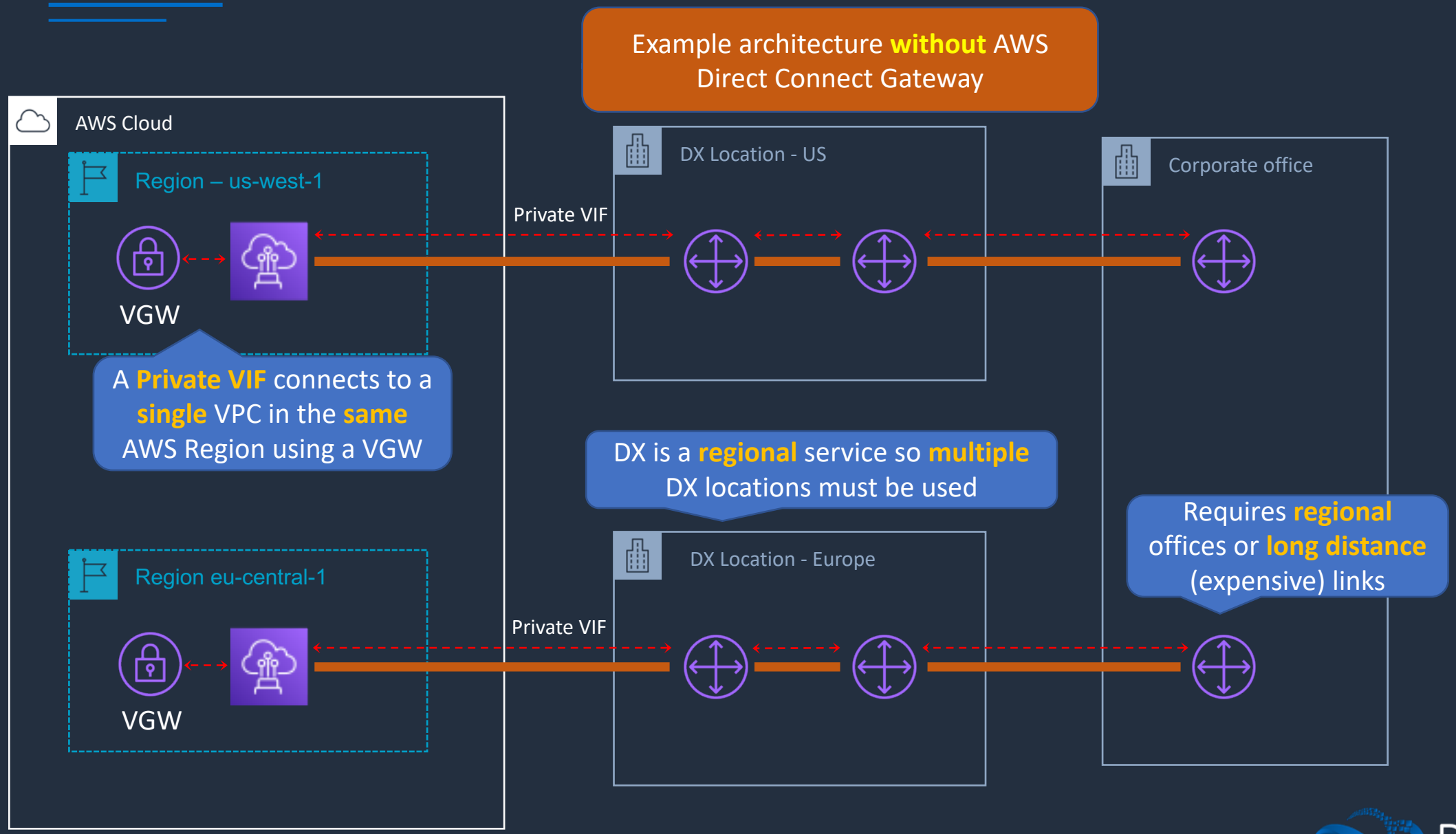


Create Direct Connect Connection

AWS Direct Connect Gateway

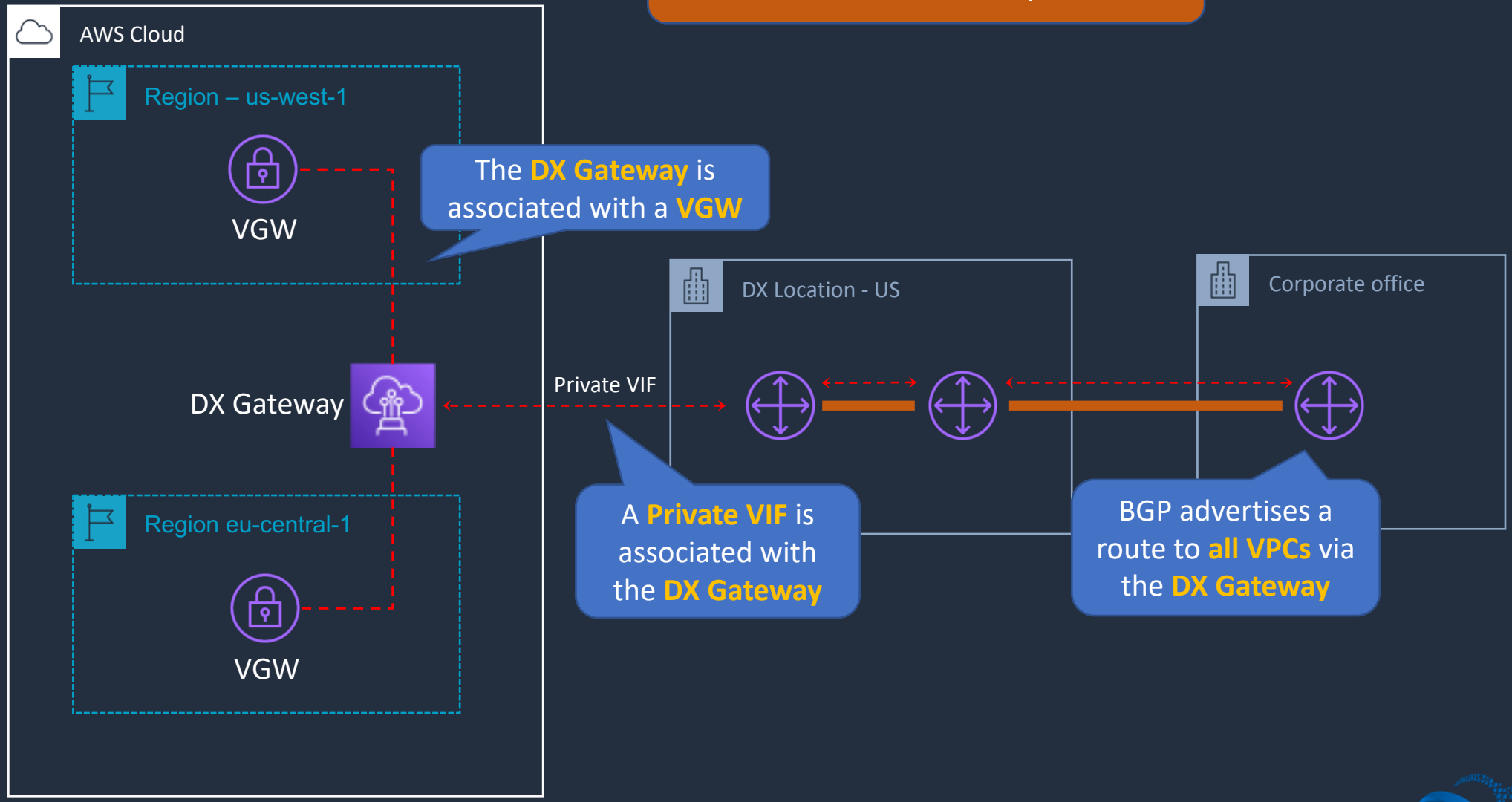


Direct Connect - Multiple Regions



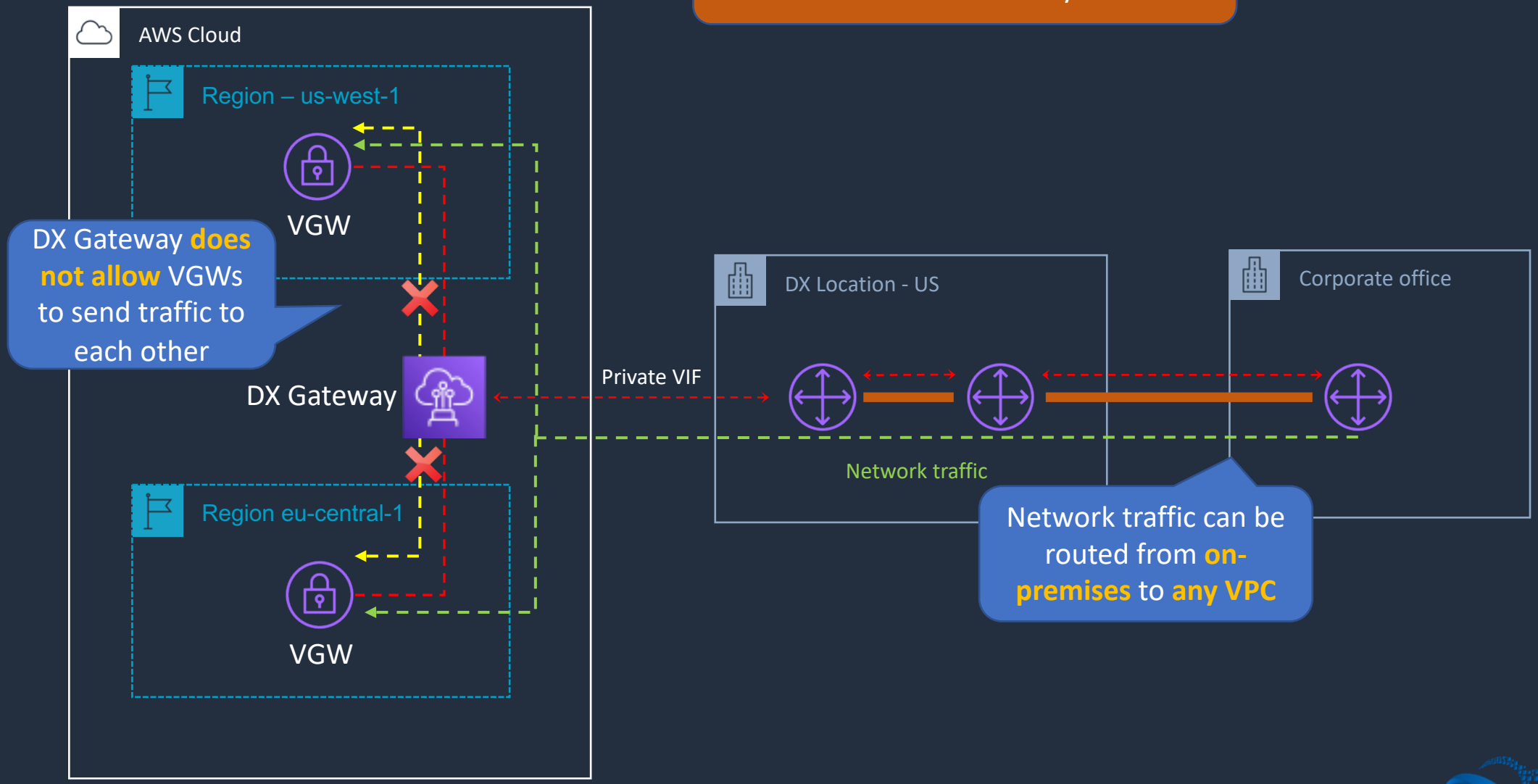
Direct Connect - Multiple Regions

Example architecture **with** AWS Direct Connect Gateway



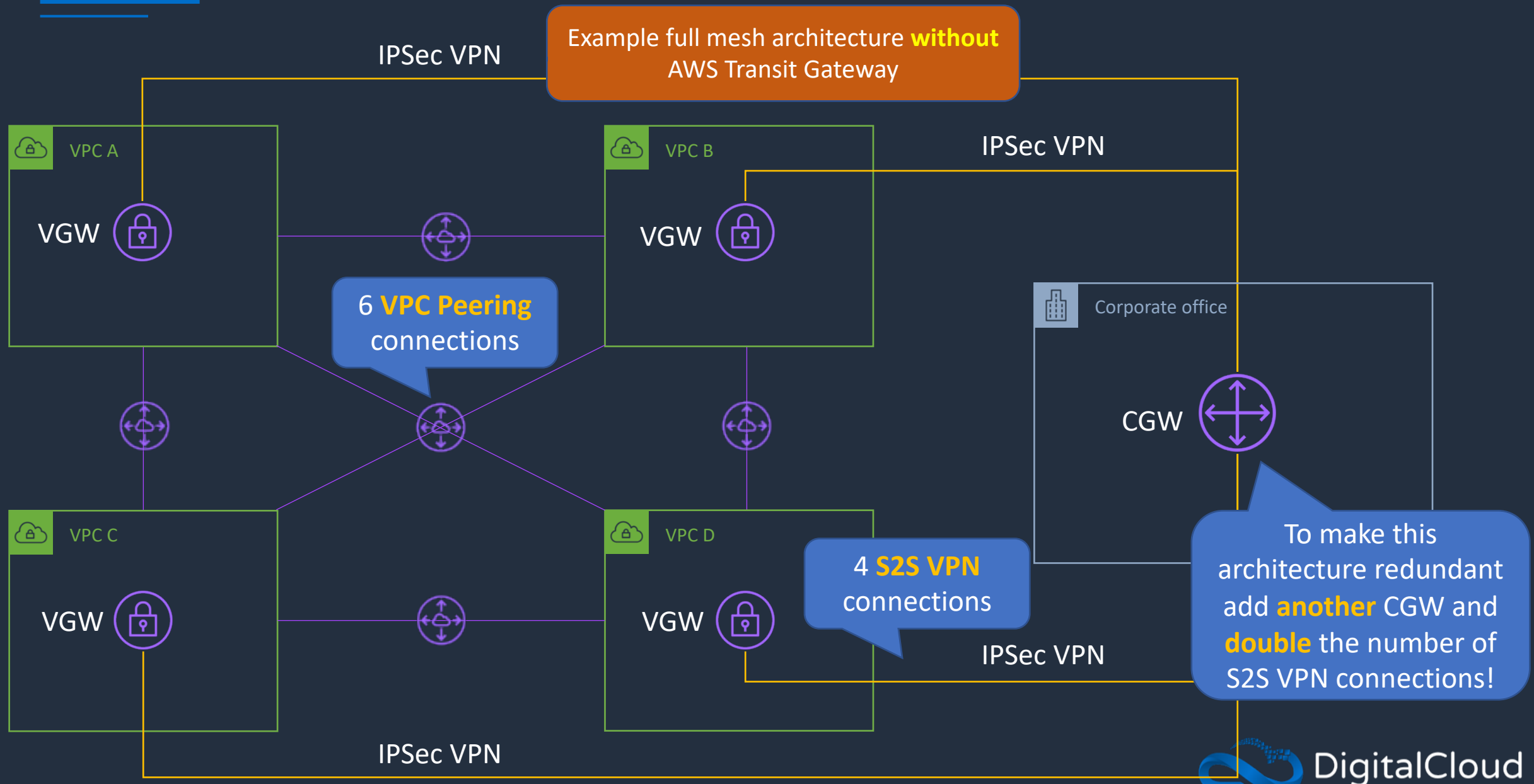
Direct Connect - Multiple Regions

Example architecture **with** AWS Direct Connect Gateway



AWS Transit Gateway

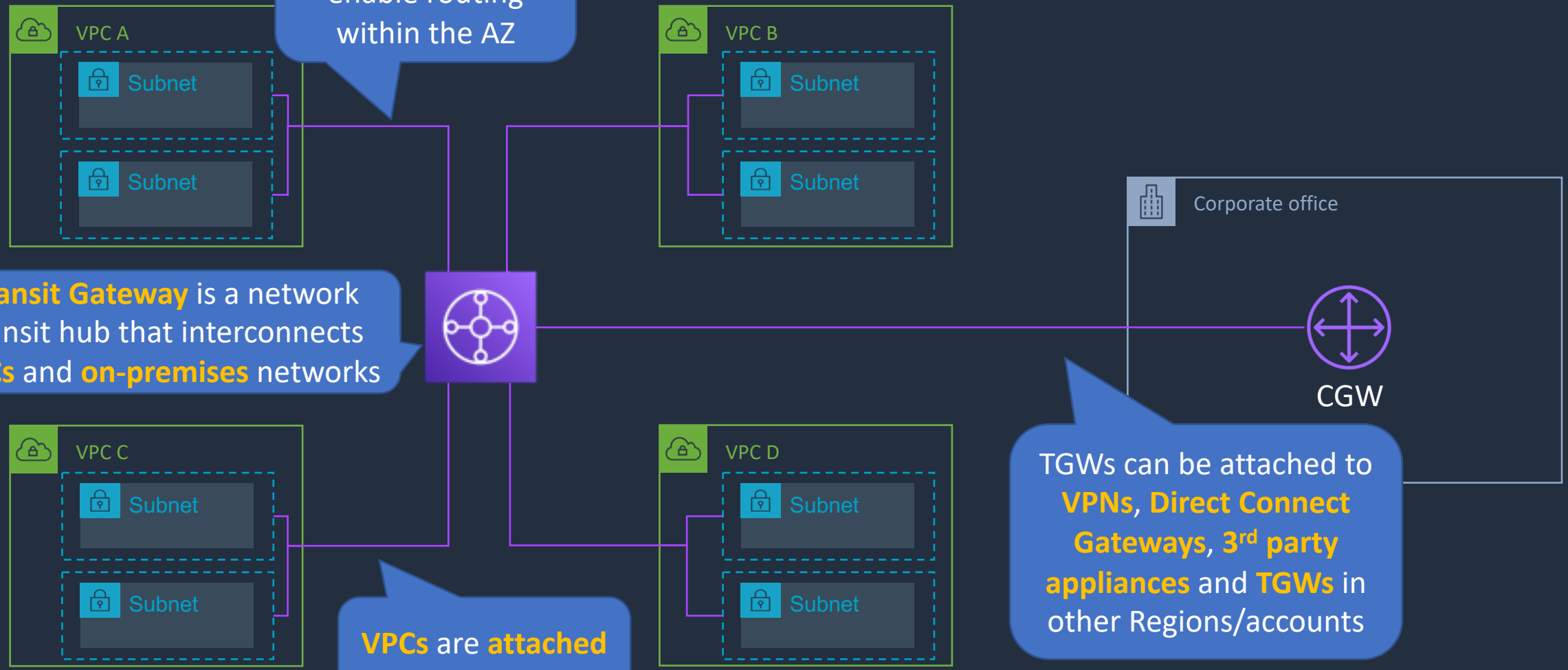
AWS Transit Gateway



AWS Transit Gateway

Specify **one subnet** from **each AZ** to enable routing within the AZ

Example full mesh architecture **with** AWS Transit Gateway



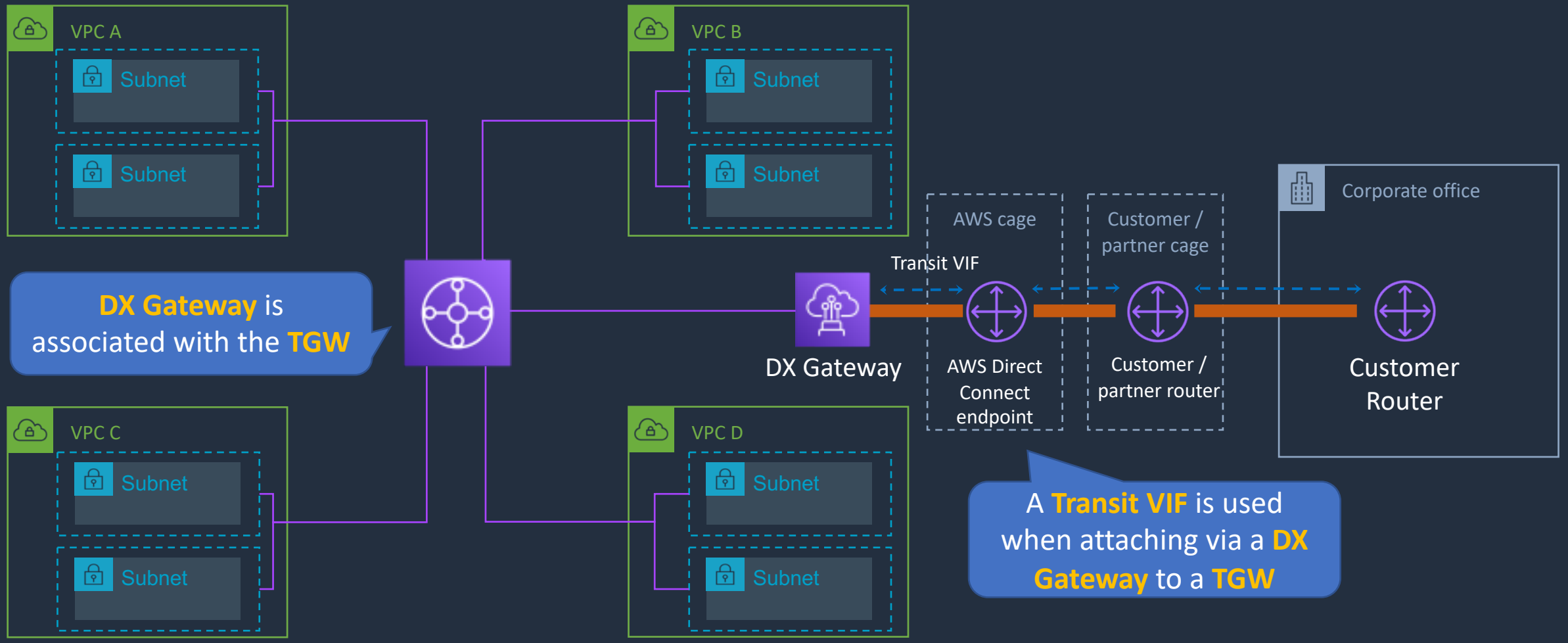
Transit Gateway is a network transit hub that interconnects **VPCs** and **on-premises** networks

VPCs are **attached** to Transit Gateway

TGWs can be attached to **VPNs**, **Direct Connect Gateways**, **3rd party appliances** and **TGWs** in other Regions/accounts

AWS TGW + DX Gateway

This architecture supports **full transitive** routing between **on-premises**, **TGW** and **VPCs**



DX Gateway is associated with the **TGW**

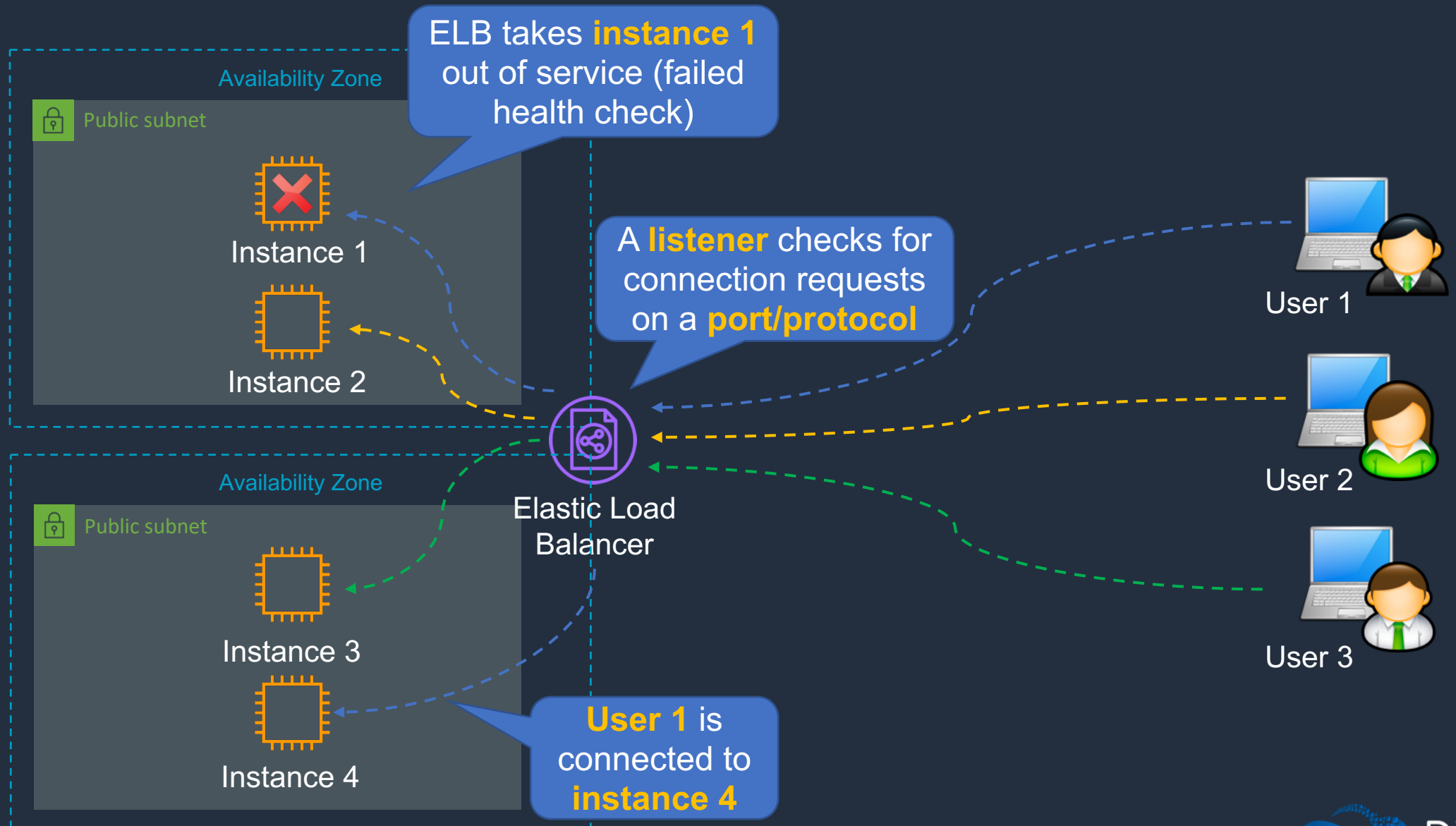
A **Transit VIF** is used when attaching via a **DX Gateway** to a **TGW**

SECTION 8

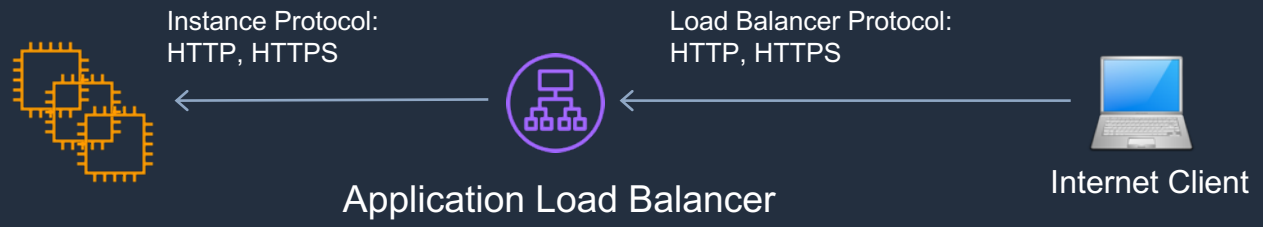
Load Balancing and Acceleration

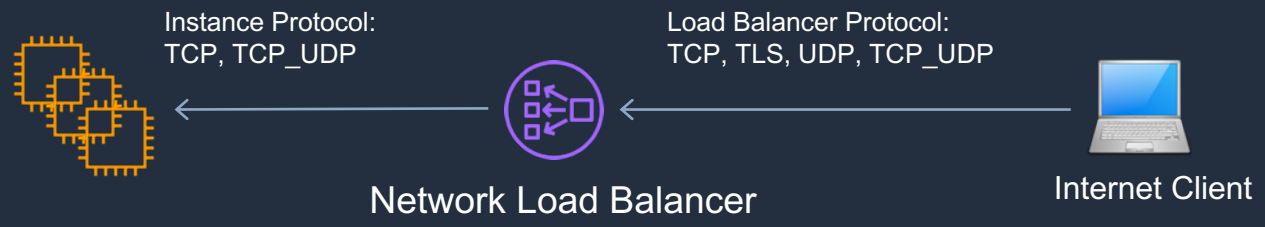
Elastic Load Balancing

Elastic Load Balancing



Elastic Load Balancing





Application Load Balancer

- Operates at the request level
- Routes based on the content of the request (layer 7)
- Supports path-based routing, host-based routing, query string parameter-based routing, and source IP address-based routing
- Supports instances, IP addresses, Lambda functions and containers as targets

Network Load Balancer

- Operates at the connection level
- Routes connections based on IP protocol data (layer 4)
- Offers ultra high performance, low latency and TLS offloading at scale
- Can have a static IP / Elastic IP
- Supports UDP and static IP addresses as targets

Application Load Balancer (ALB)

Application Load Balancer (ALB)

Requests can also be routed based on the **host** field in the **HTTP header**

A **rule** is configured on the **listener** – ALBs listen on **HTTP/HTTPS**

Requests can be routed based on the **path** in the **URL**

Target groups are used to route requests to registered targets

TG1 TG2 TG3

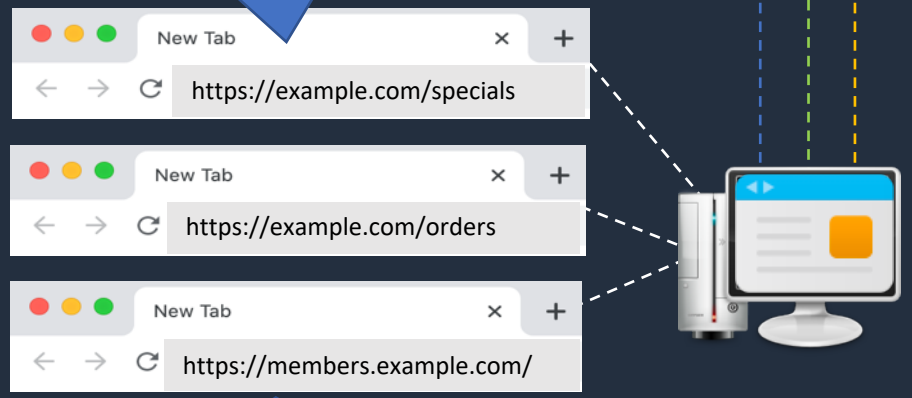
Subnet

Subnet

Subnet

Targets can be EC2 instances, IP addresses, Lambda functions or containers

Path-based routing



Host-based routing

DigitalCloud TRAINING

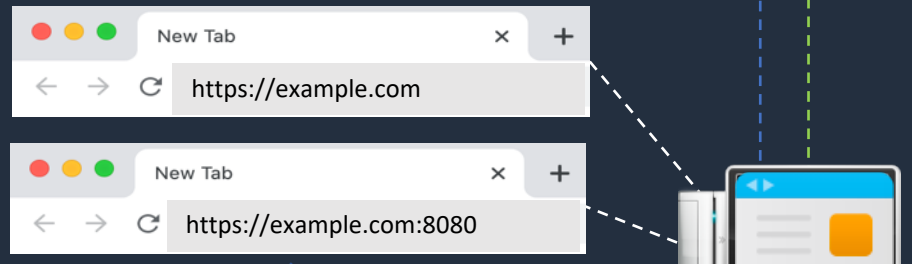
Network Load Balancer (NLB)

Network Load Balancer (NLB)

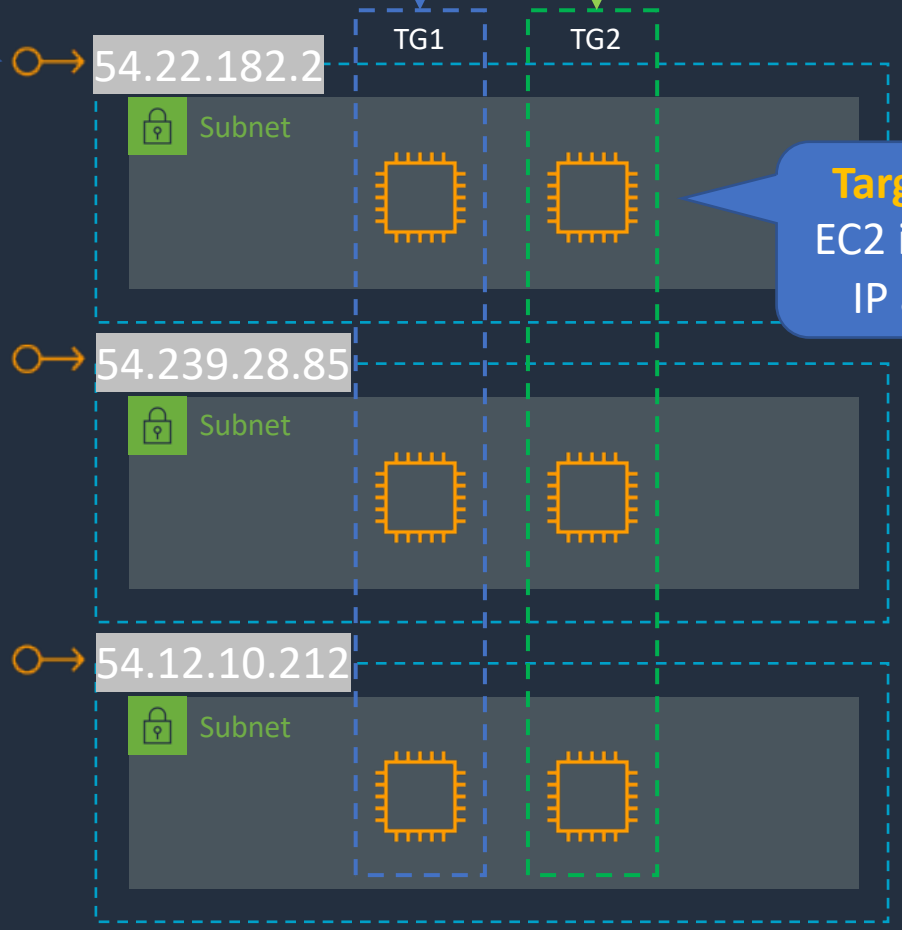
Requests are routed based on **IP protocol** data

NLBs listen on **TCP**, **TLS**, **UDP** or **TCP_UDP**

NLB **nodes** can have **elastic IPs** in each subnet



A **separate** listener on a **unique port** is required for routing



Targets can be EC2 instances or IP addresses

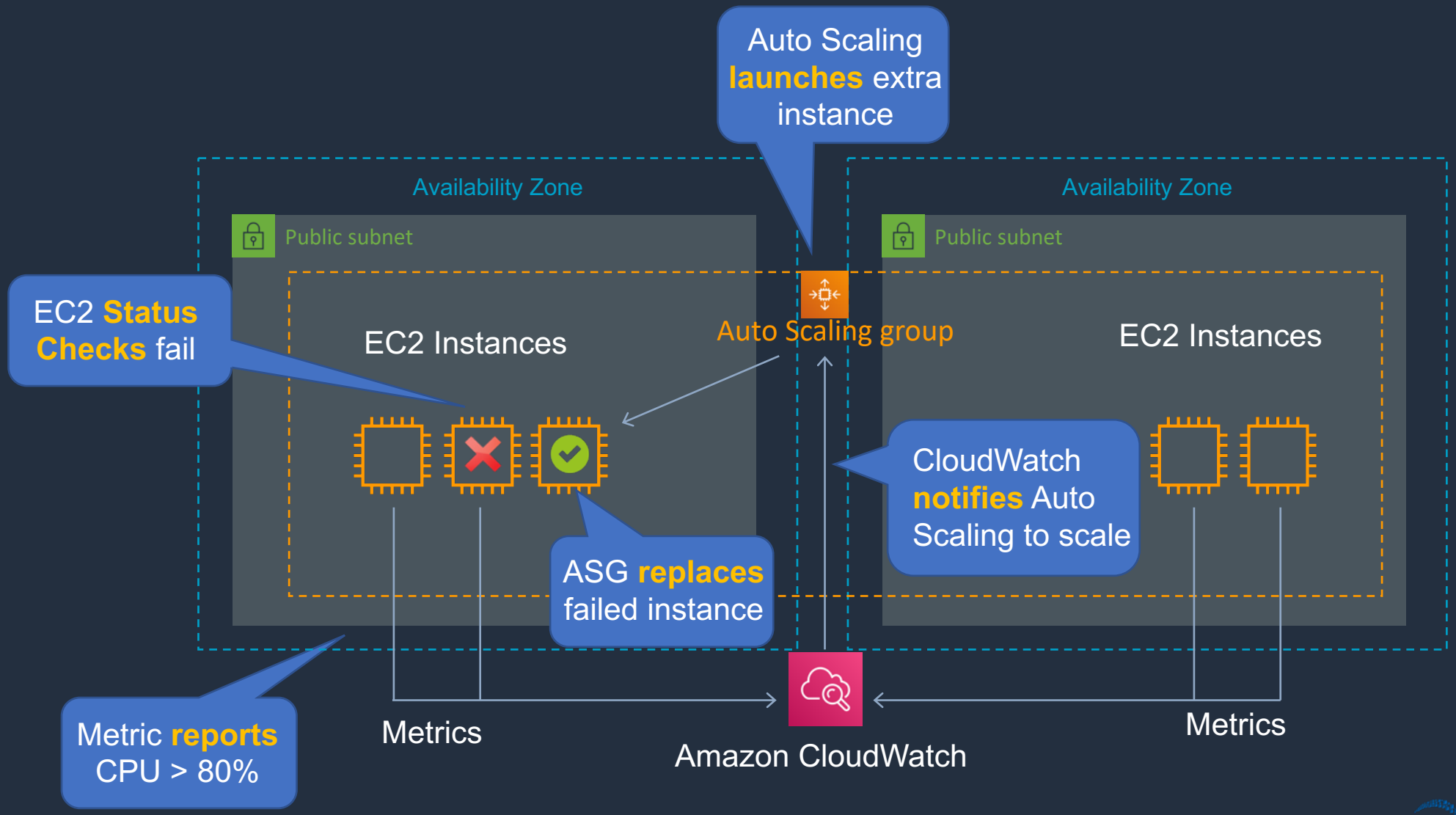
Targets can be outside a VPC (e.g. on-premises)

DigitalCloud TRAINING

Create EC2 Auto Scaling Group for ELB HOL

DigitalCloud TRAINING

Amazon EC2 Auto Scaling

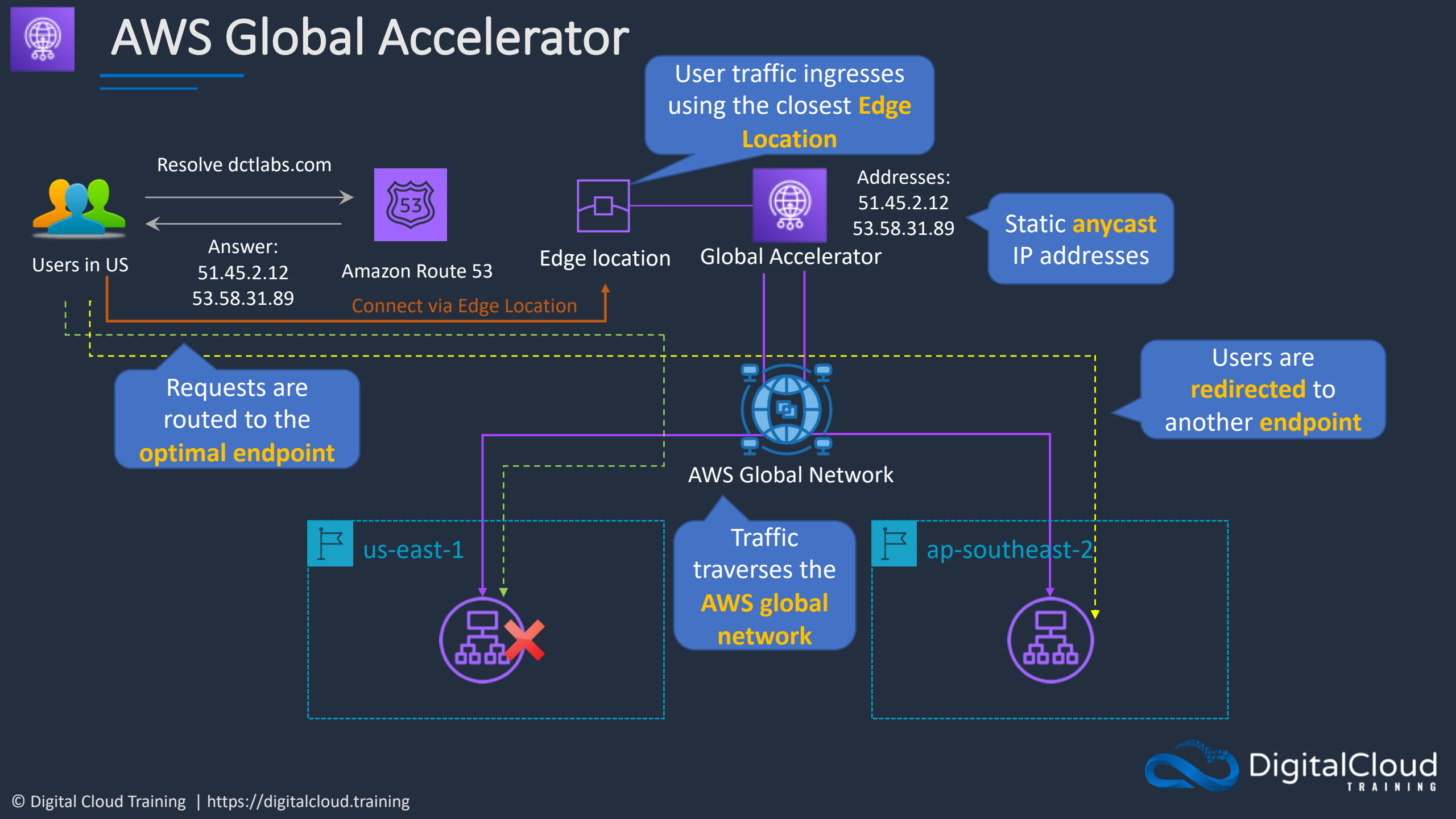


Create Application Load Balancer

Create Network Load Balancer

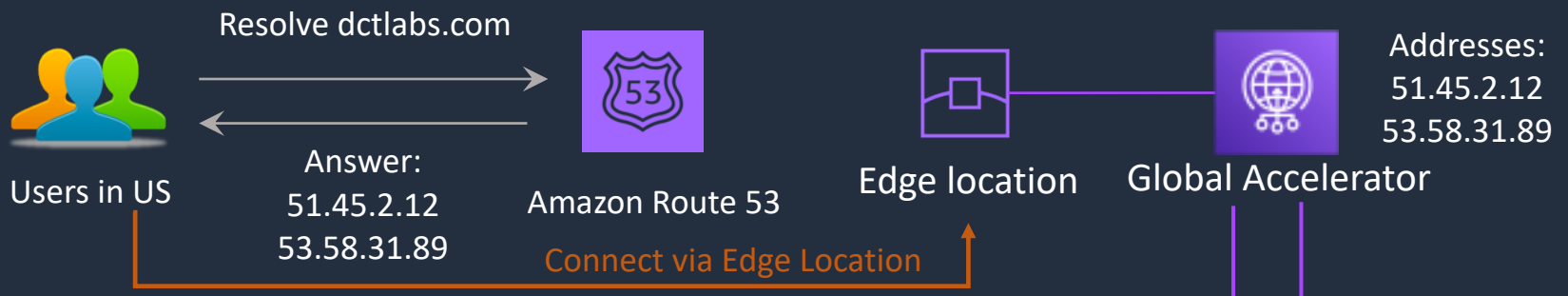
AWS Global Accelerator

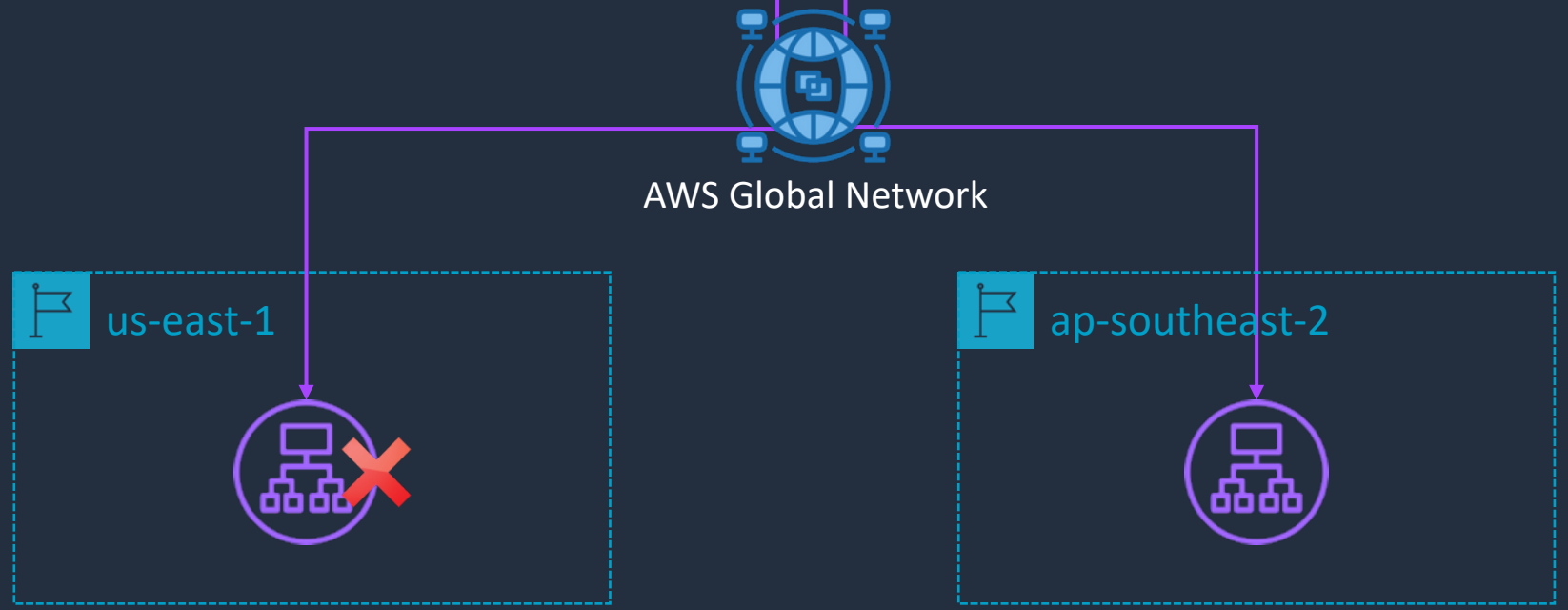
AWS Global Accelerator



Create a Global Accelerator

AWS Global Accelerator



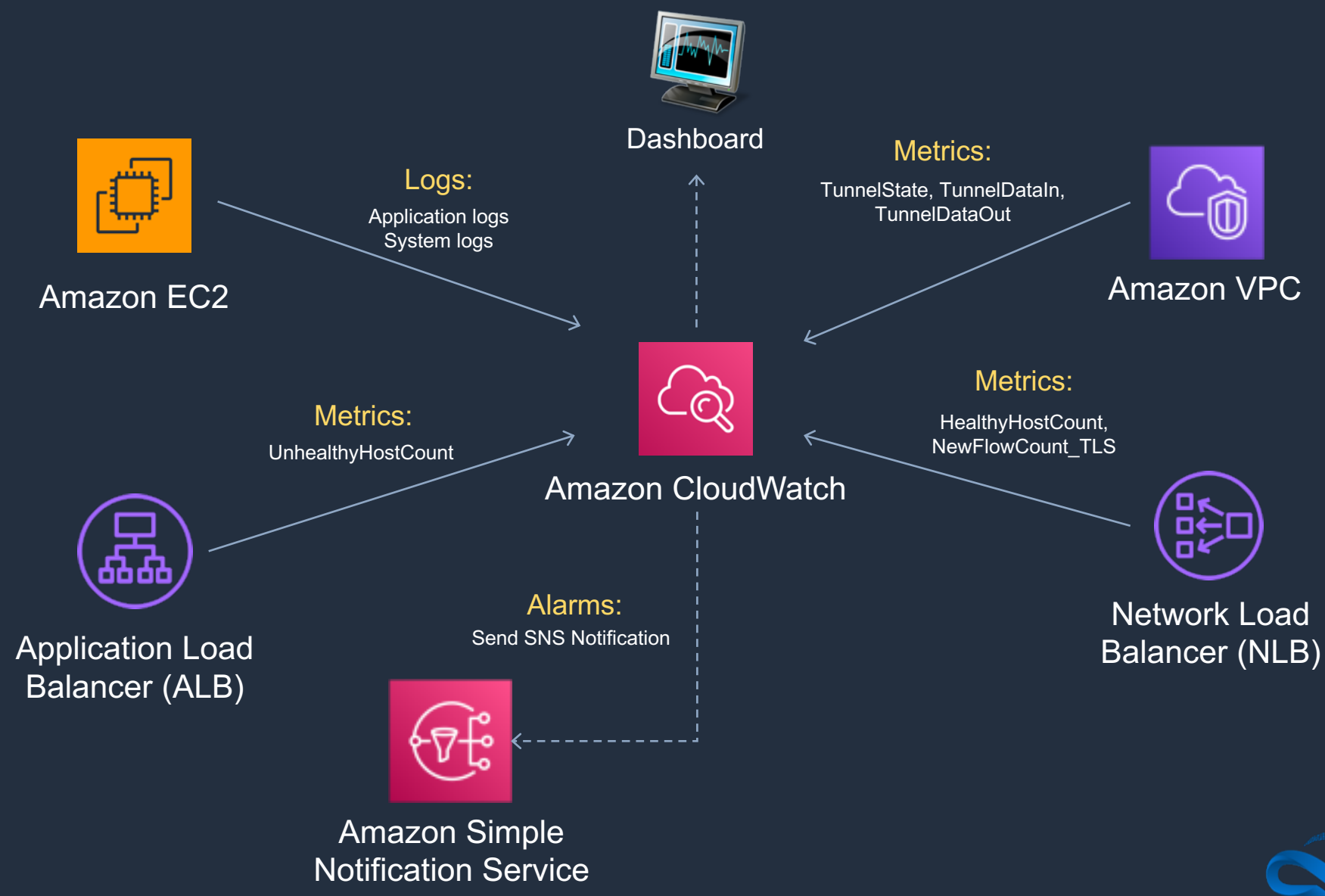


SECTION 9

Monitoring, Auditing and Logging

Monitoring with Amazon CloudWatch

Amazon CloudWatch



DigitalCloud TRAINING

Auditing with AWS CloudTrail

AWS CloudTrail

CloudTrail **audits API actions**

Events can be viewed in the **CloudTrail** console

Dashboard

AWS Direct Connect

API Actions:

CreateBGPPeer,
DeleteVirtualInterface

API Actions:

CreateTransitGatewayVpcAttachment

AWS Transit Gateway

AWS CloudTrail

API Actions:

CreateSecurityGroup

API Actions:

CreateVpcEndpoint,
CreateVpcEndpointServiceConfiguration

Security Group

S3 Bucket

CloudWatch Logs

VPC Endpoint

Events can be delivered to an **S3 bucket**

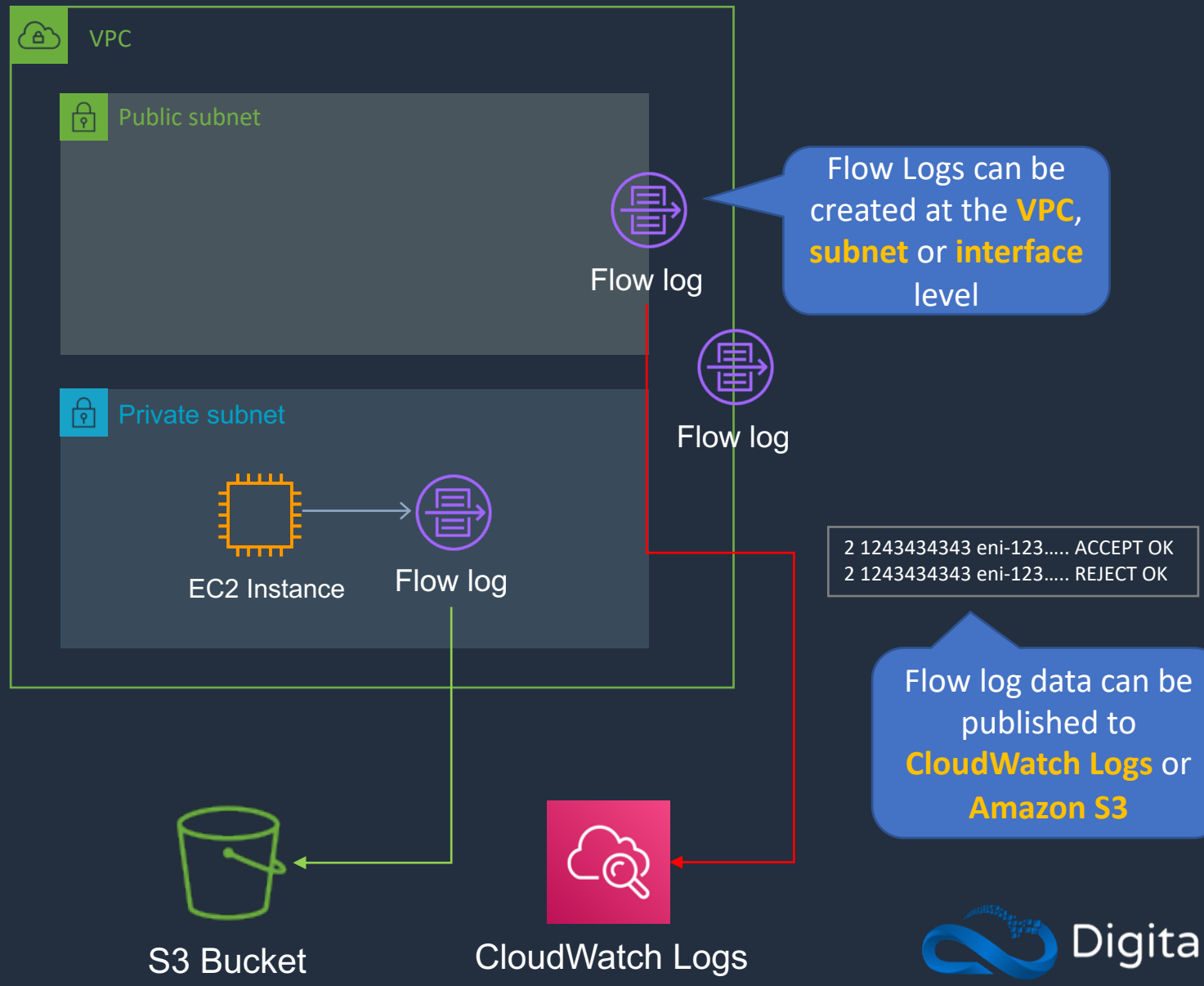
Events can be also be delivered to **CloudWatch Logs**

DigitalCloud TRAINING

VPC Flow Logs

VPC Flow Logs

Flow Logs capture data about **IP traffic** going to and from **networking interfaces** in a VPC



Flow logs capture information about the following:

- Allowed and denied traffic
- Source and destination IP addresses
- Ports
- Protocol number
- Packet and byte counts
- Action taken (accept or reject)

VPC Flow Logs vs ELB Access Logs

VPC Flow Log

version	account-id	interface-id	srcaddr	dstaddr	srcport	dstport	protocol	packets	bytes	start	end	action	log-status
2	55112233445	eni-0f5…	11.200.185.200	10.0.1.15	52933	22	6	1	40	1599…	1599…	ACCEPT	OK
2	55112233445	eni-0f5…	10.0.1.15	11.200.185.200	22	52933	6	1	40	1599…	1599…	ACCEPT	OK
2	55112233445	eni-0f5…	11.200.185.200	10.0.1.15	3624	80	6	1	44	1599…	1599…	REJECT	OK
2	55112233445	eni-0f5…	11.200.185.200	10.0.1.15	3624	80	6	1	44	1599…	1599…	REJECT	OK

ELB Access Log

```
http 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.000 0.001 0.000 200 200 34 366
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067
"Root=1-58337262-36d228ad5d99923122bbe354" "-" "-"
0 2018-07-02T22:22:48.364000Z "forward" "-" "-" 10.0.0.1:80 200 "-" "-"
```

Create VPC Flow Log

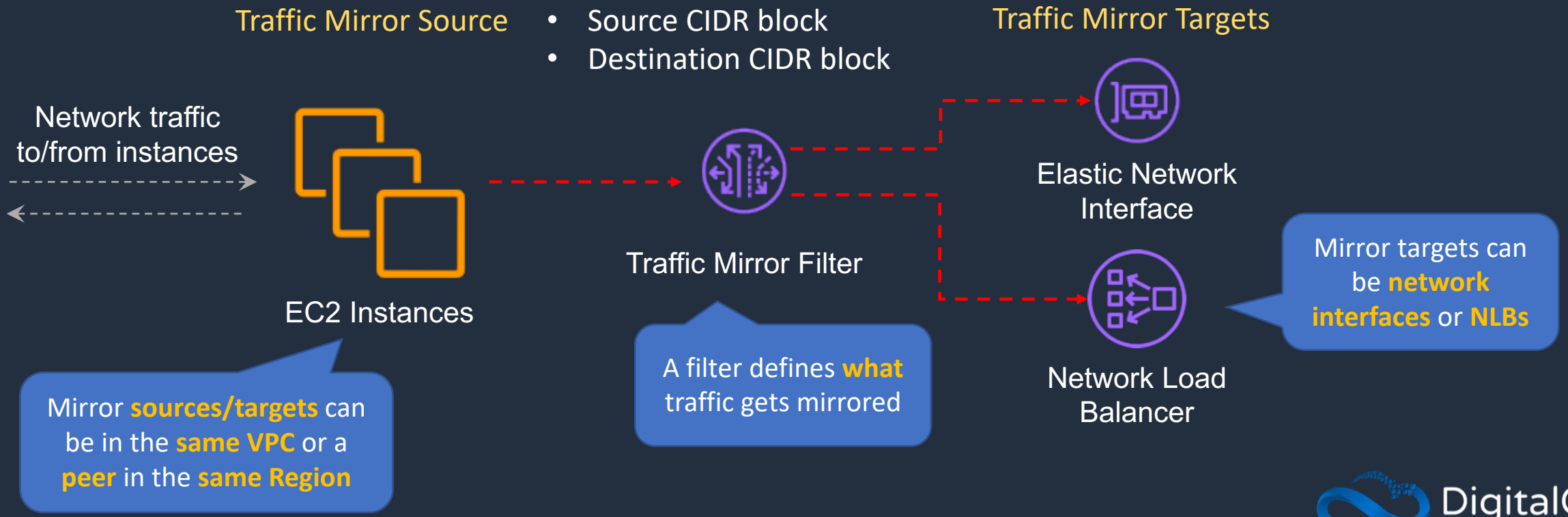
Traffic Mirroring

Traffic Mirroring

The following traffic mirror filter rule parameters are available:

- Traffic direction: Inbound or outbound
- Action: The action to take, either to accept or reject the packet
- Protocol: The L4 protocol
- Source port range
- Destination port range
- Source CIDR block
- Destination CIDR block

Mirrored traffic is encapsulated with a **VXLAN** header



Reachability Analyzer

SECTION 10

Command Line and Automation

Setting up the AWS CLI

Create a VPC and Subnets with AWS CLI

DigitalCloud TRAINING

Launch EC2 instances into subnets with AWS CLI

Introduction to AWS CloudFormation

AWS CloudFormation

CloudFormation **deploys** infrastructure using **code**

template1

Choose template language: JSON YAML

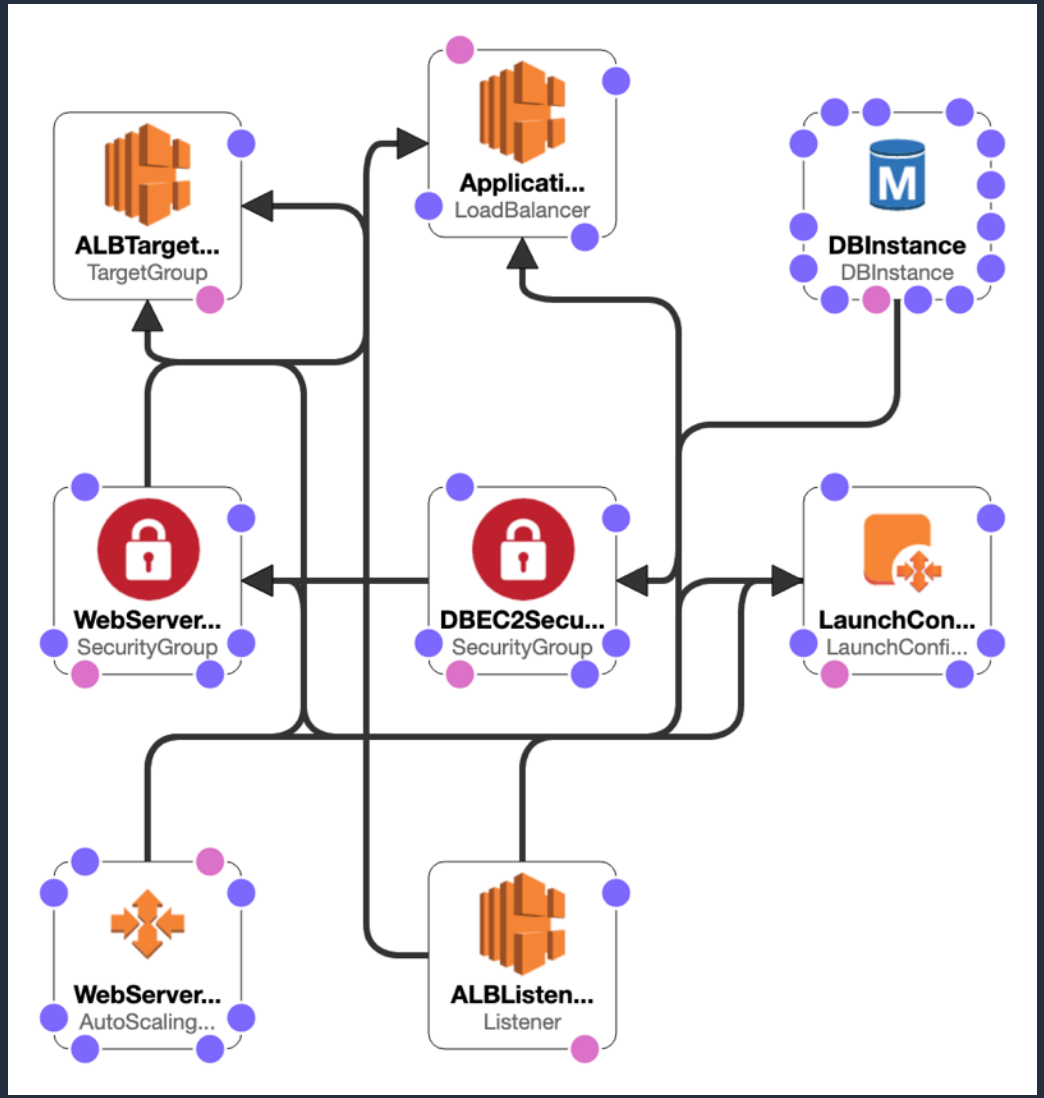
```
{
"AWSTemplateFormatVersion": "2010-09-09",
"Description": "AWS CloudFormation Sample Template LAMP_Single_Instance: Create a LAMP stack using a single EC2 instance a
"Parameters": {
    "KeyName": {
        "Description": "Name of an existing EC2 KeyPair to enable SSH access to the instance",
        "Type": "AWS::EC2::KeyPair::KeyName",
        "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
    },
    "DBName": {
        "Default": "MyDatabase",
        "Description": "MySQL database name",
        "Type": "String",
        "MinLength": "1",
        "MaxLength": "64",
        "AllowedPattern": "[a-zA-Z][a-zA-Z0-9]*",
        "ConstraintDescription": "must begin with a letter and contain only alphanumeric characters."
    },
    "DBUser": {
        "NoEcho": "true",
```

You define the AWS services to create in a **template**

DigitalCloud TRAINING

AWS CloudFormation

CloudFormation creates and configures **resources** according the the **template**



DigitalCloud TRAINING

Create Amazon VPC with CloudFormation

DigitalCloud TRAINING