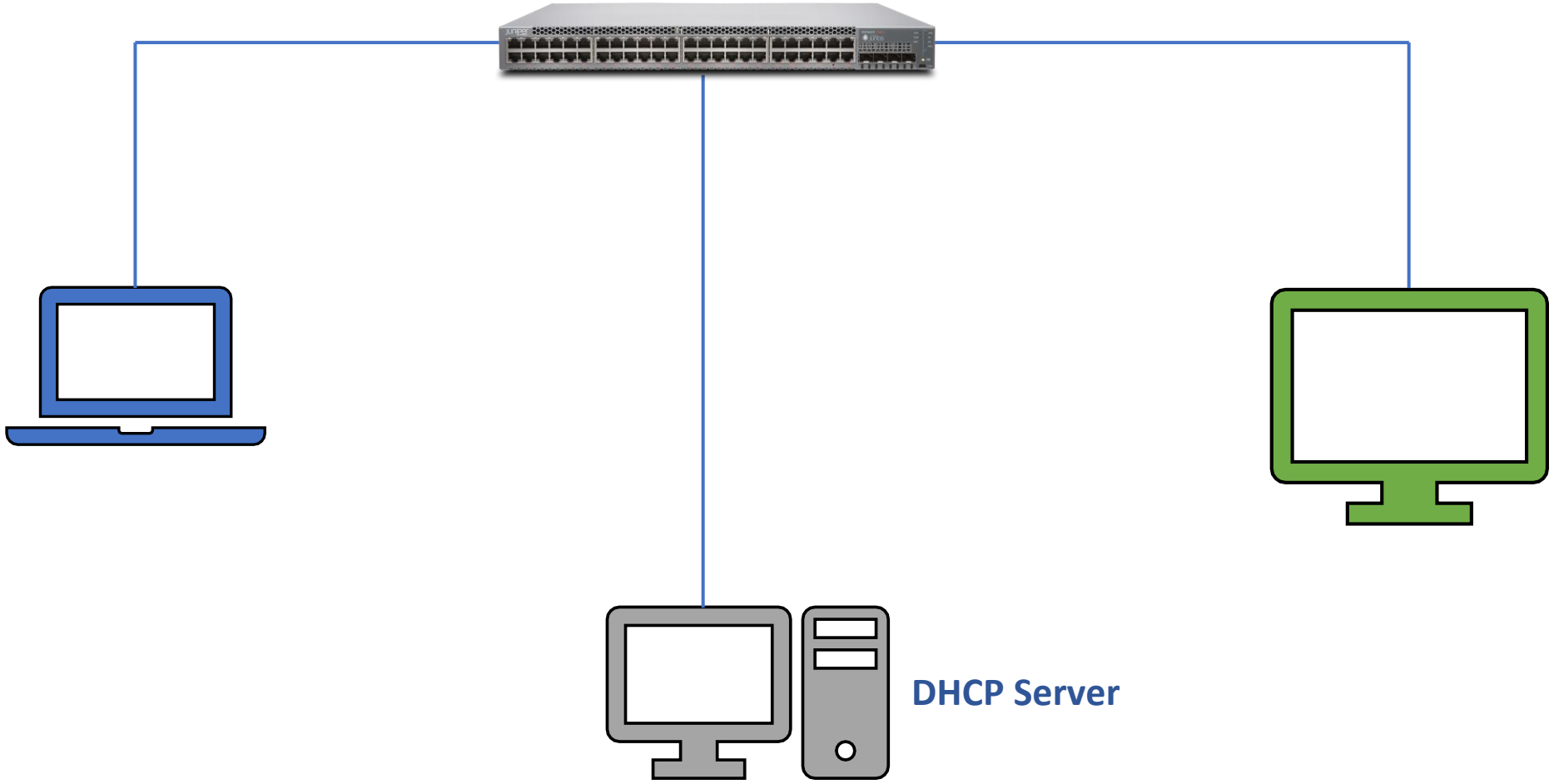

aws certified
Cloud Practitioner
AWS Networking and VPC

Networking Core Concepts

1. Network
2. Switch
3. NIC and MAC Address
4. IP Address
5. DHCP Server
6. CIDR
7. Subnet
8. Routers
9. Gateway
10. DNS Server

Computer Networks

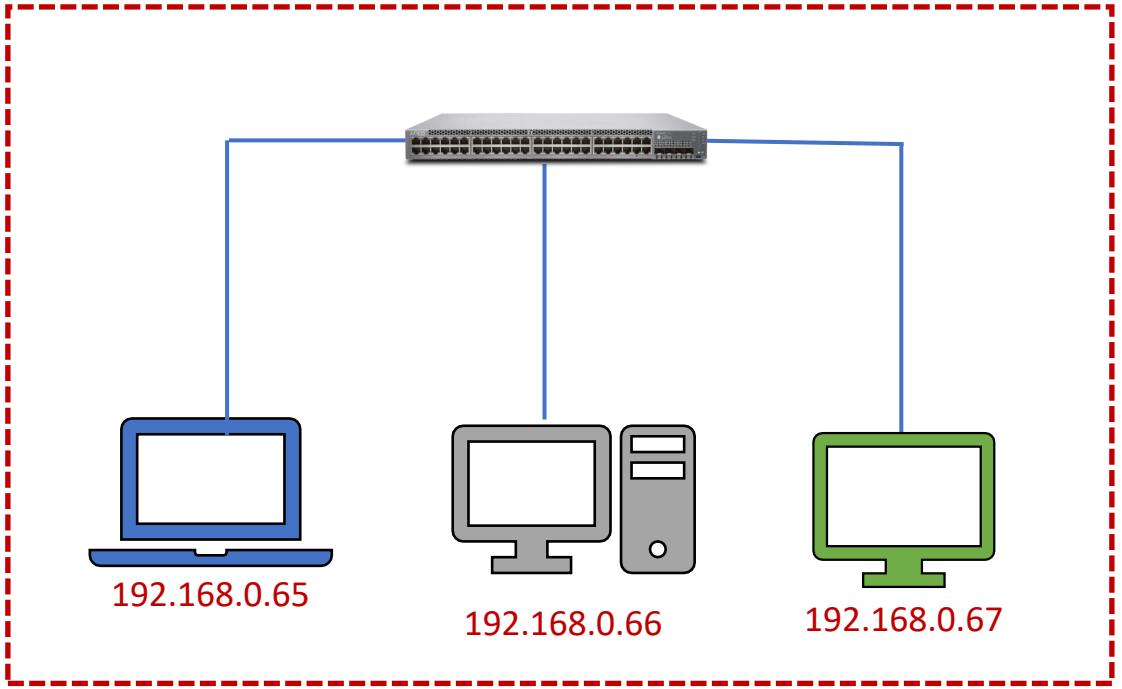
1. MAC Address – 00:1B:44:11:3A:B7
2. IP Address – 192.158.1.38



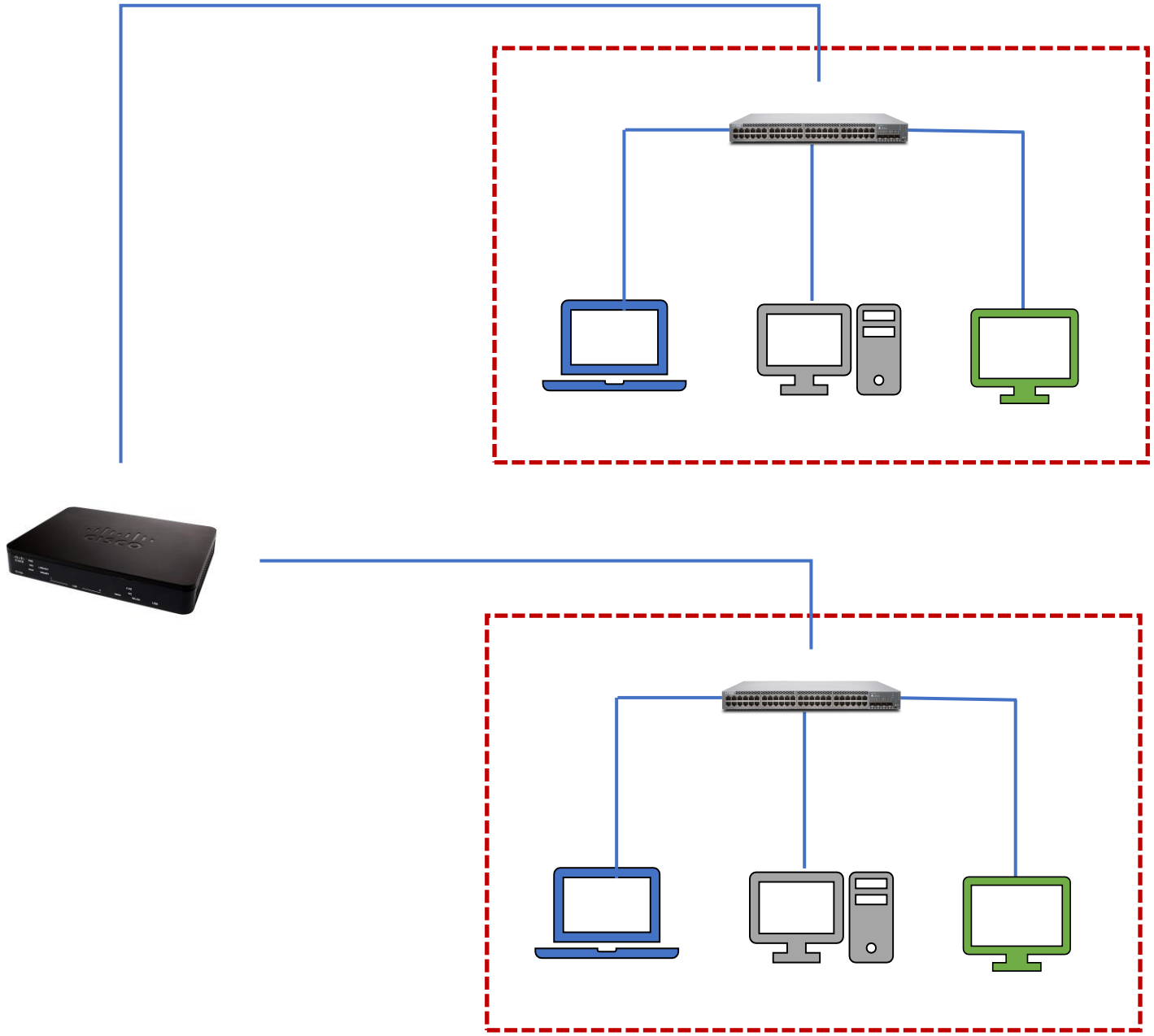
CIDR Block

Class A – 10.0.0.1/8 -> 16777214 devices
Class B – 172.16.0.1/16 -> 65534 devices
Class C – l192.168.0.1/24 -> 254 devices

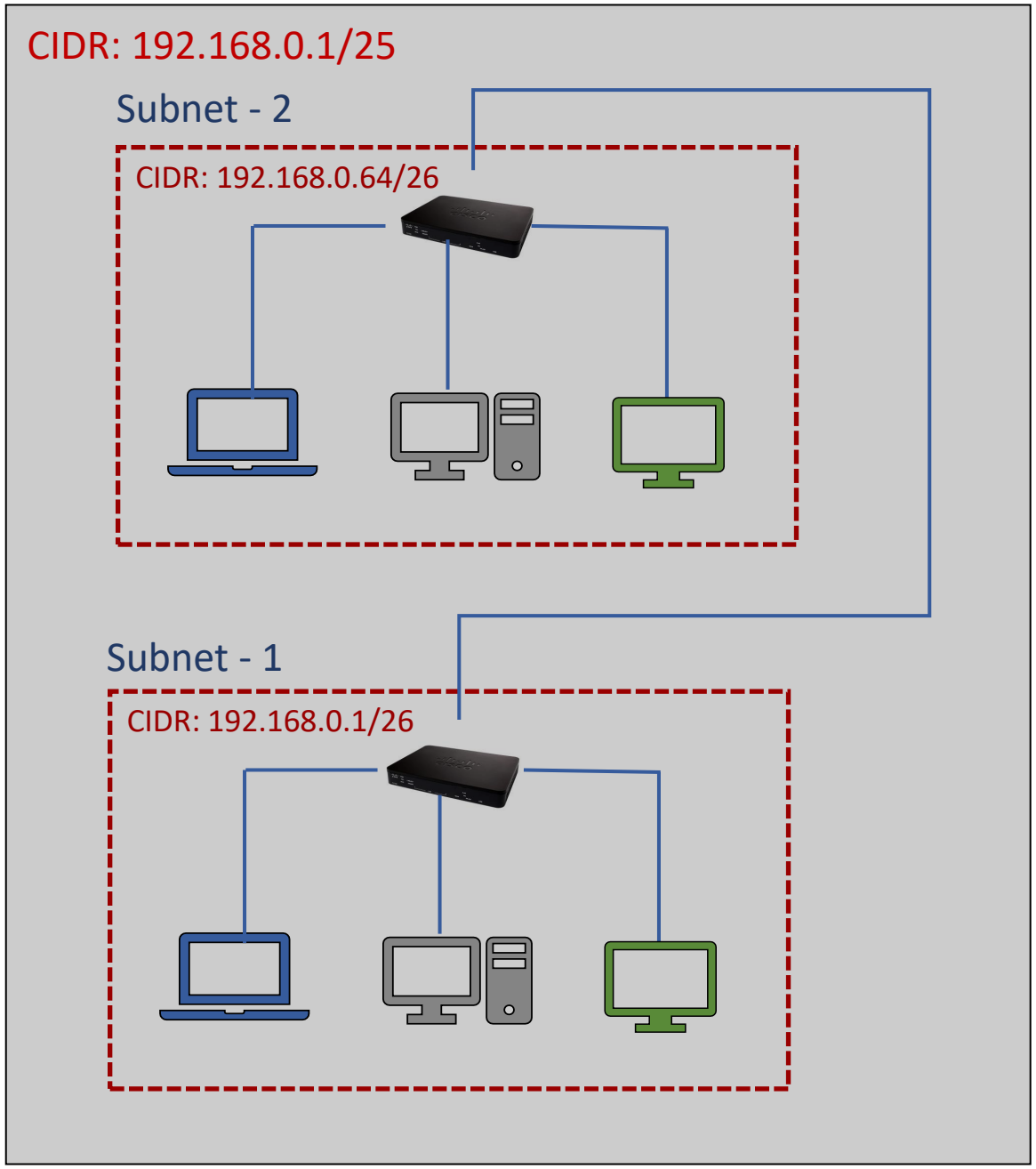
https://www.subnet-calculator.com/



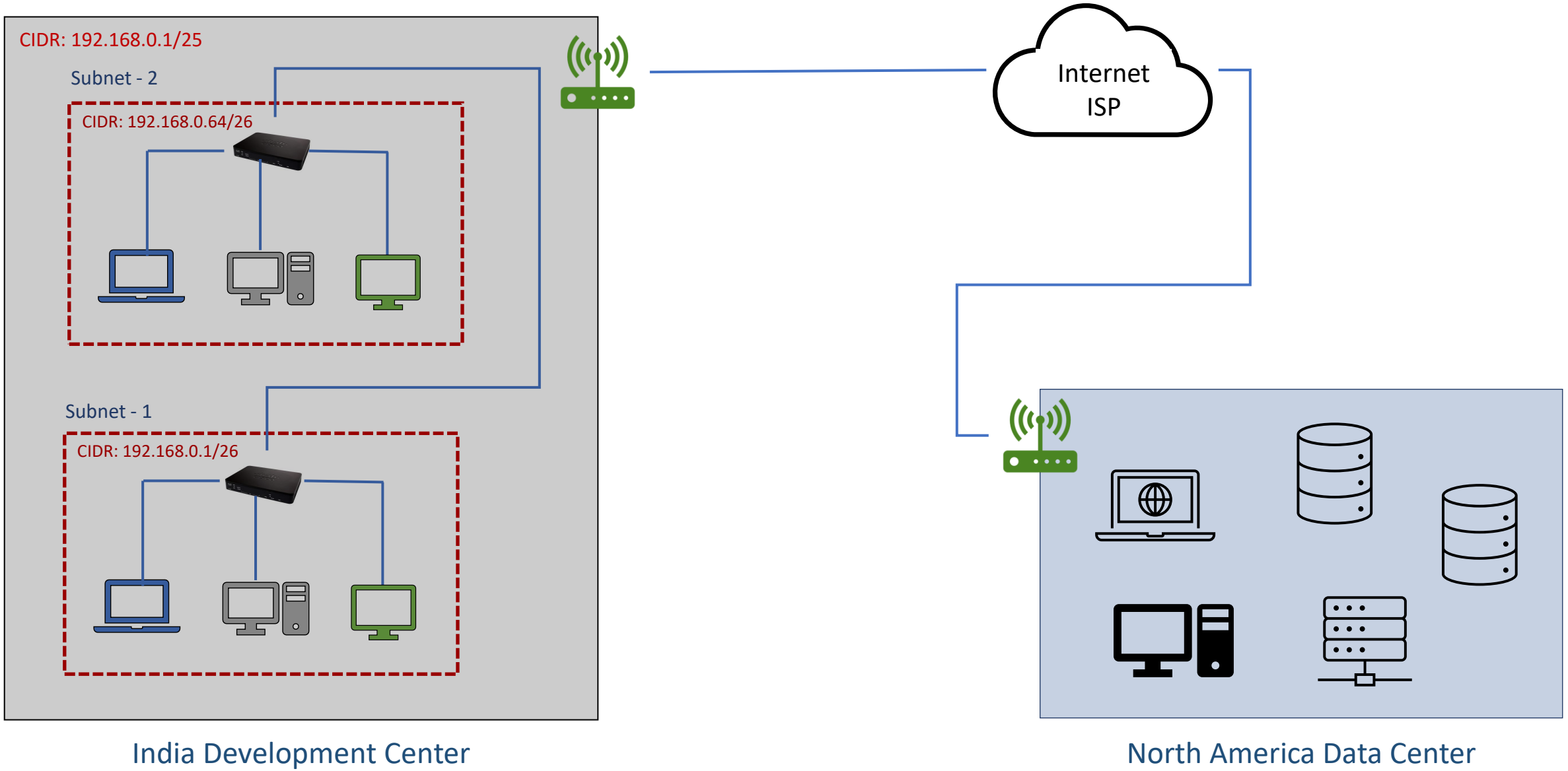
Subnet & Routers



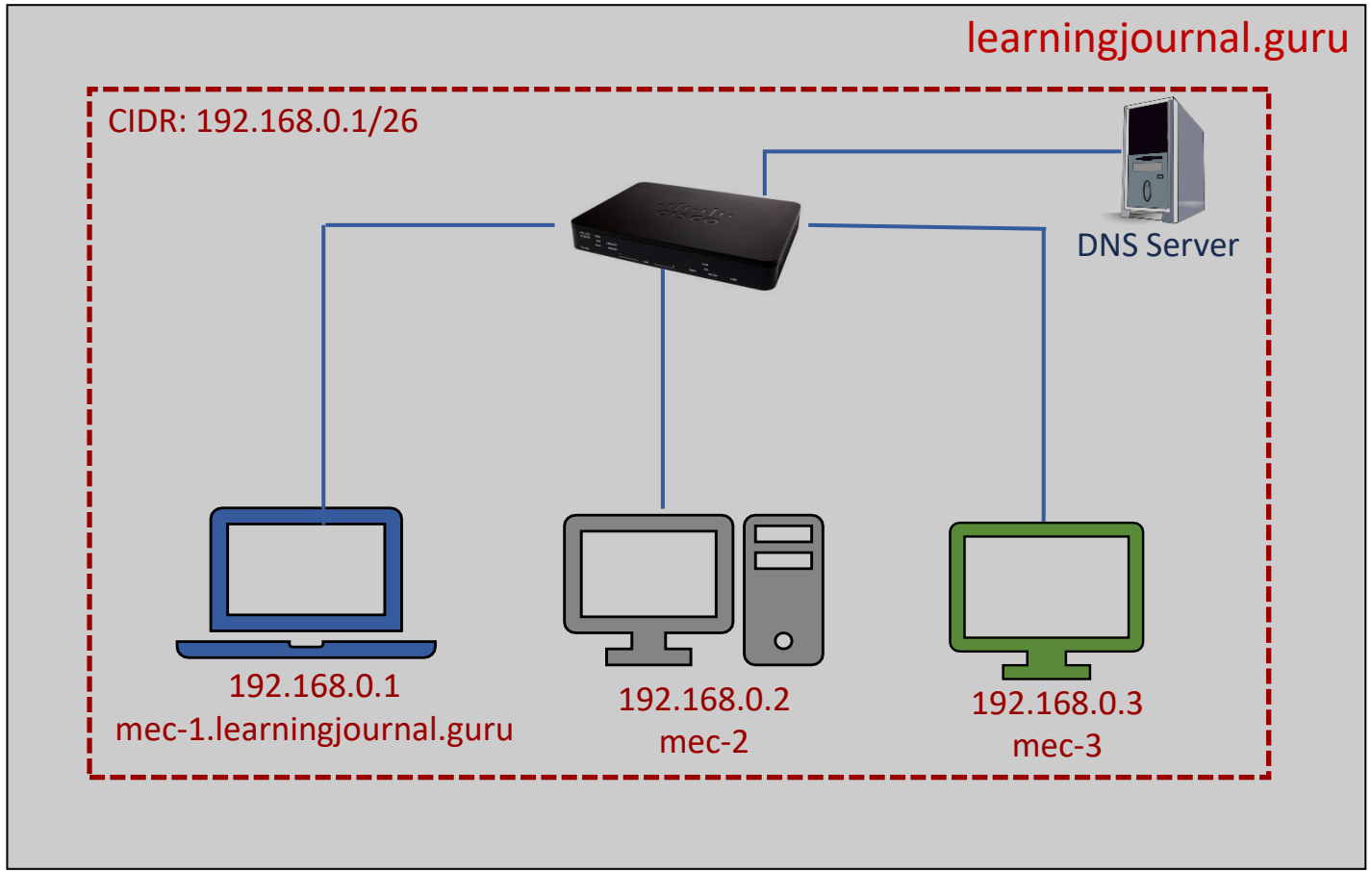
Subnet and CIDR



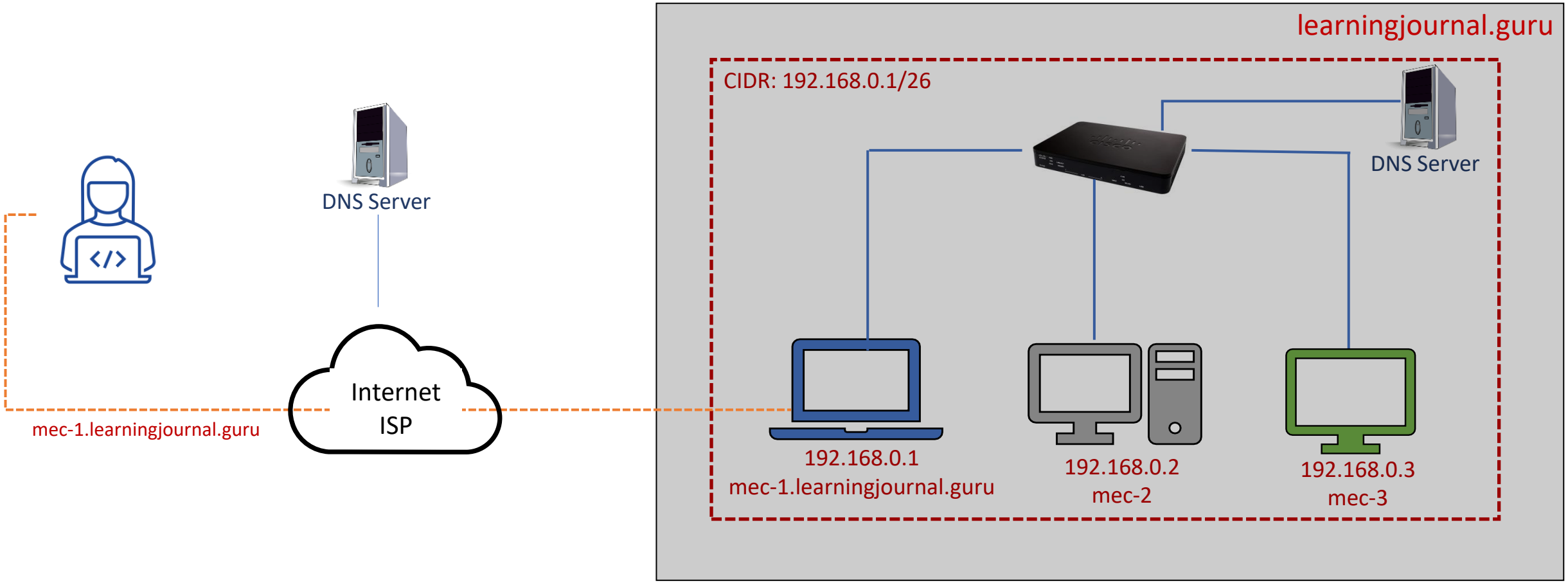
Internet Gateway



Hostname and Domain Name



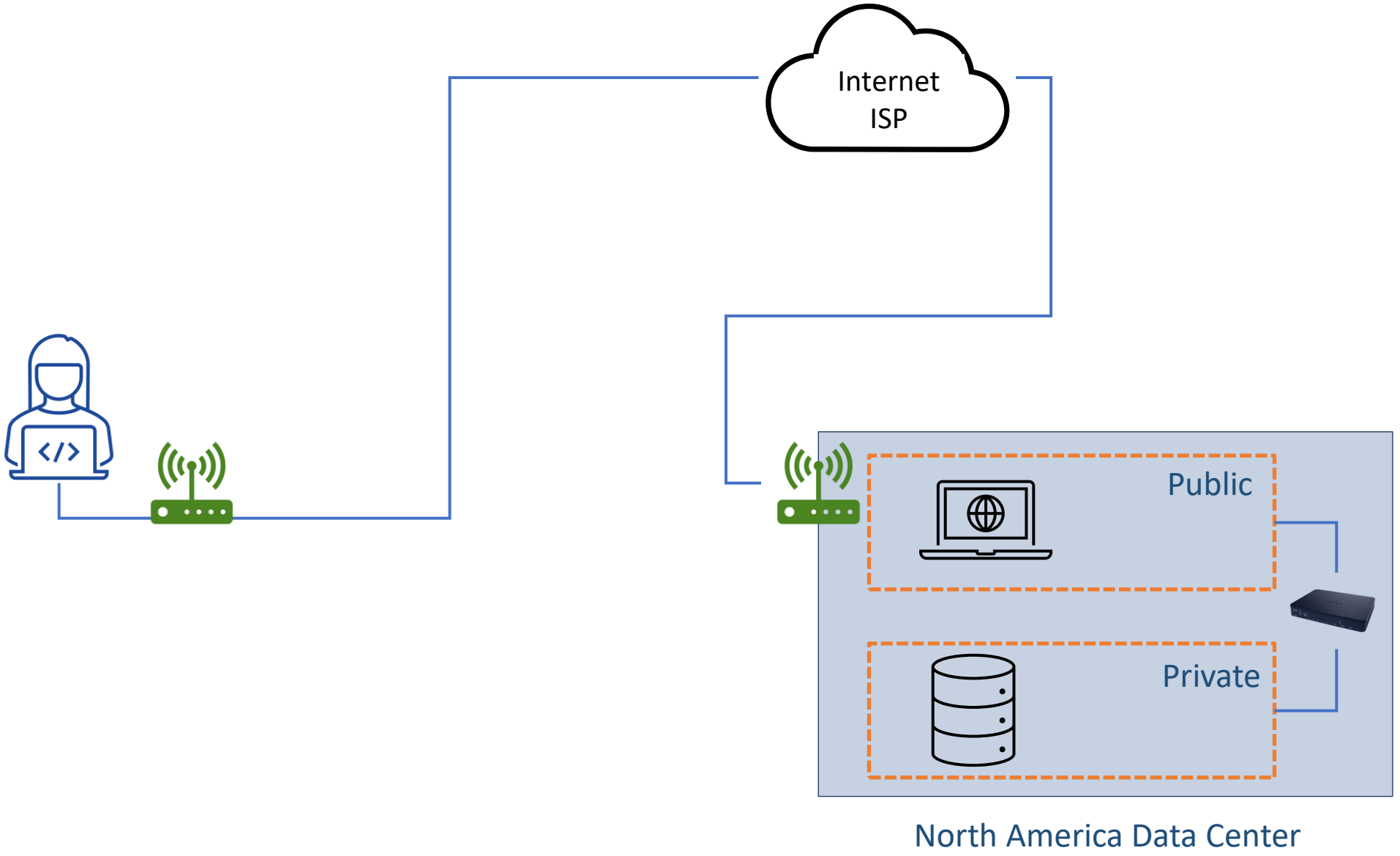
Public and Private DNS Server

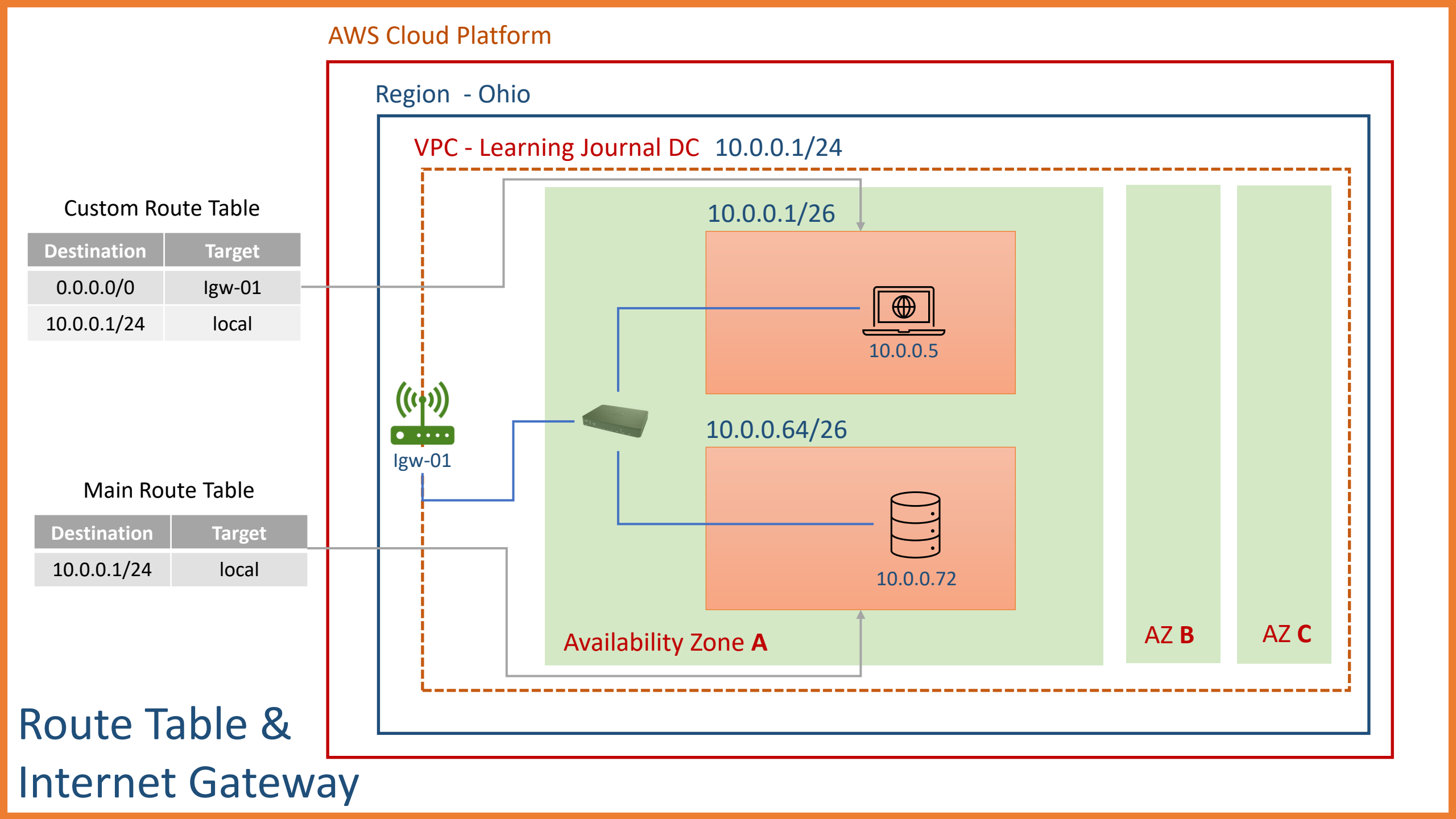


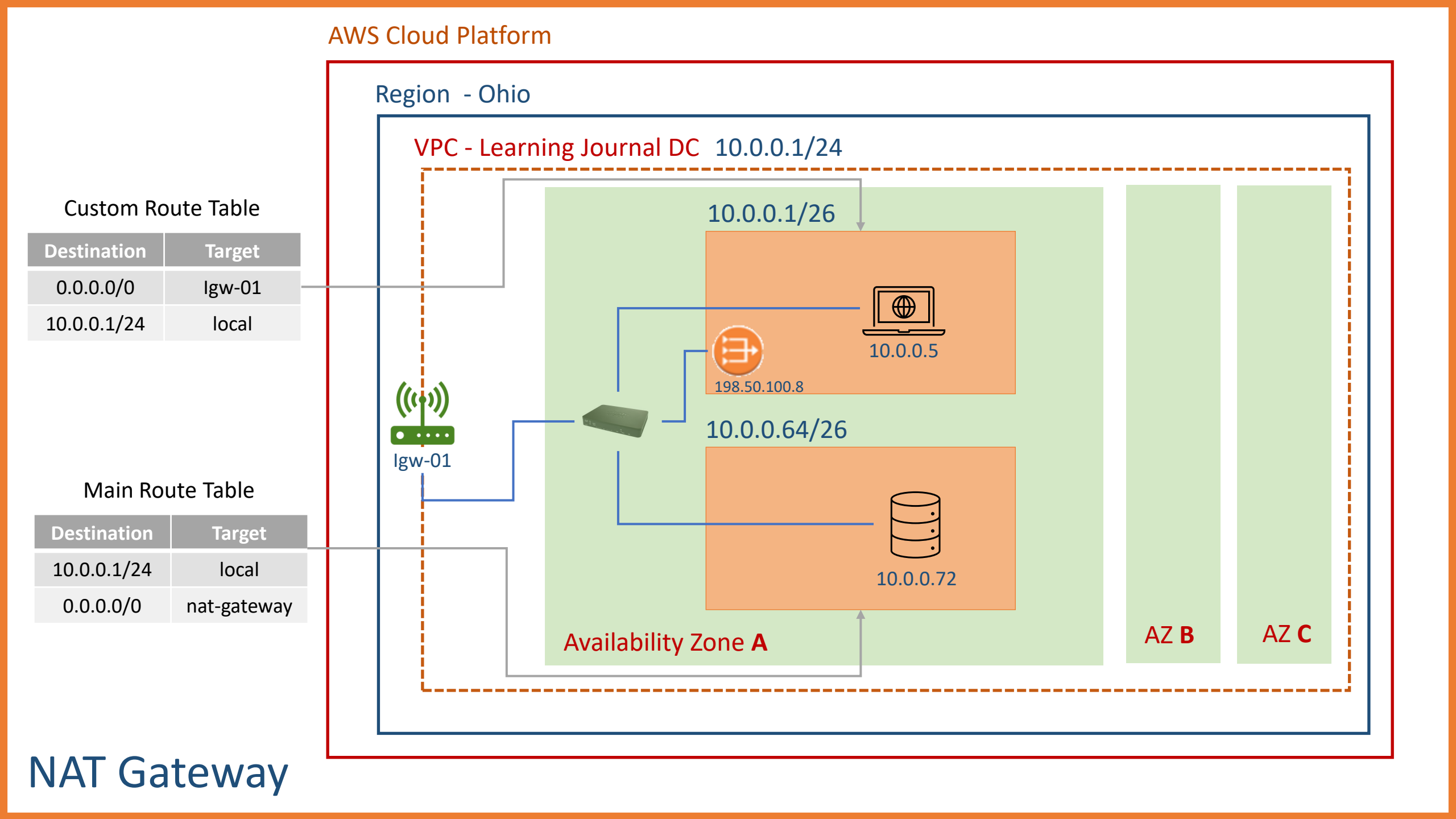
Benefits of Cloud

North America | South America | Europe/Middle East/Africa | Asia Pacific

Public and Private Subnet




AWS Cloud Platform
Region - Ohio
VPC - Learning Journal DC 10.0.0.1/24
Custom Route Table
Destination
Target
0.0.0.0/0
Igw-01
10.0.0.1/24
local
10.0.0.1/26
10.0.0.5
Igw-01
10.0.0.64/26
10.0.0.72
Main Route Table
Destination
Target
10.0.0.1/24
local
Availability Zone A
AZ B
AZ C
Route Table &
Internet Gateway



Custom Route Table

Destination	Target
0.0.0.0/0	Igw-01
10.0.0.1/24	local

Main Route Table

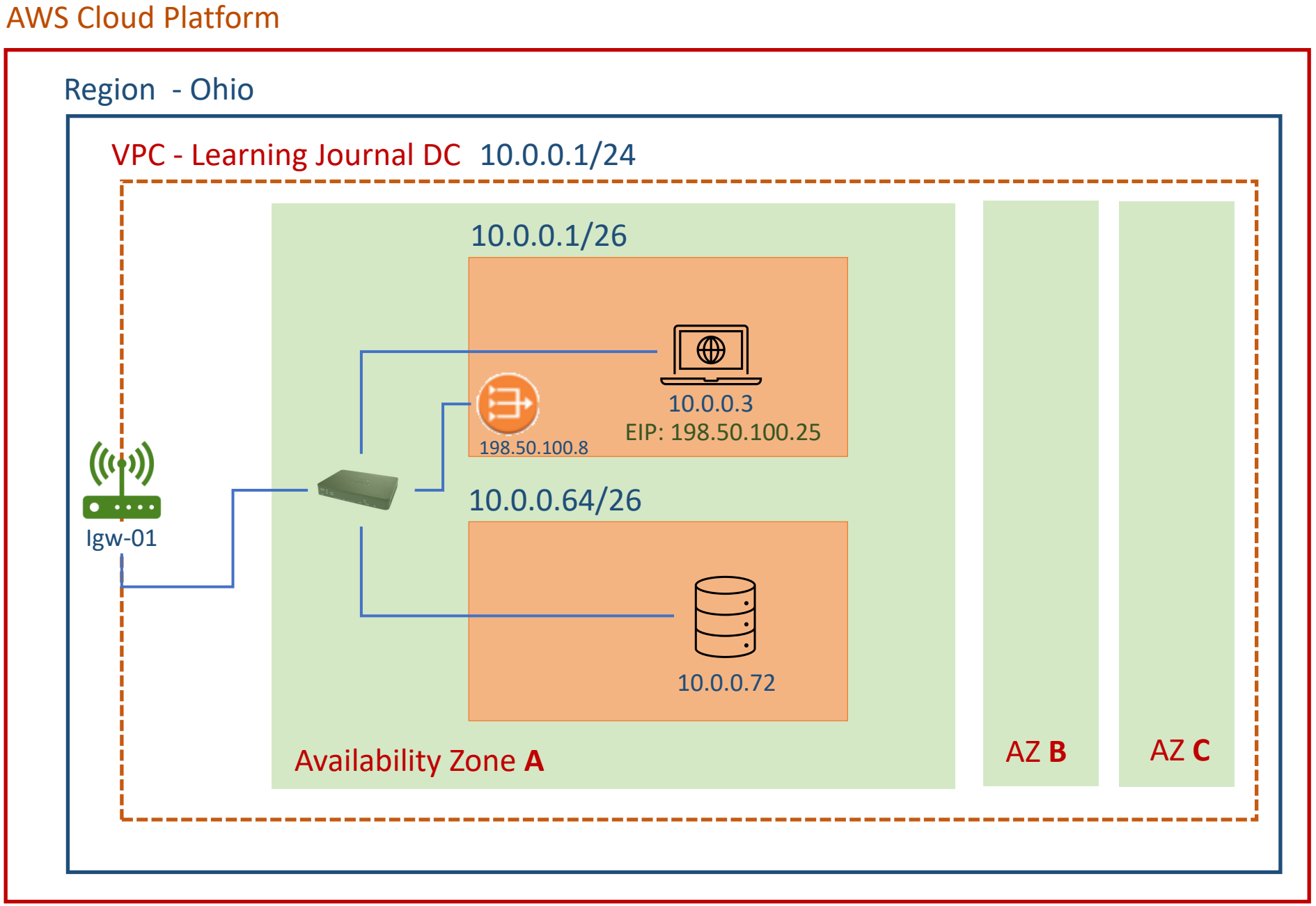
Destination	Target
10.0.0.1/24	local
0.0.0.0/0	nat-gateway

NAT Gateway

1. Private IP Address
2. Public IP Address
3. Elastic IP Address

Elastic IP Address

- Available on rent from AWS
- Bring your own IP Address
- Get Up to 5 Elastic IP Address per VPC
- Release back when not needed


AWS Cloud Platform
Region - Ohio
VPC - Learning Journal DC 10.0.0.1/24
10.0.0.1/26
10.0.0.3
EIP: 198.50.100.25
198.50.100.8
10.0.0.64/26
10.0.0.72
Igw-01
Availability Zone A
AZ B
AZ C

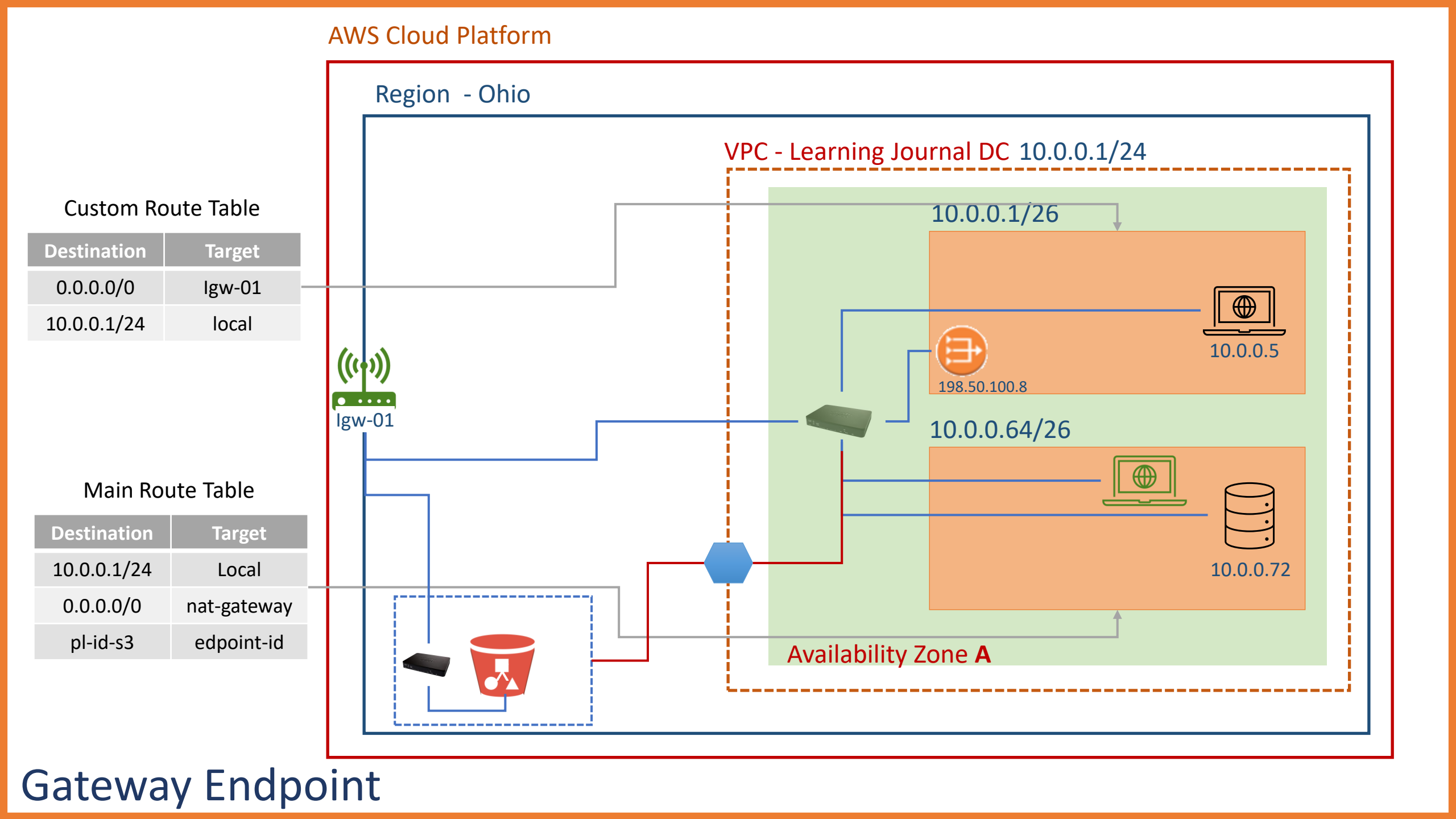
Elastic IP

AWS Private Link Technology

- Create new AWS PrivateLink-powered service
- Private Connection to AWS services without internet

AWS Private Link Connections

- Gateway Endpoint (S3, DynamoDB)
- Interface Endpoint (all other services)
- Gateway Load Balancer Endpoint (Virtual Appliances)



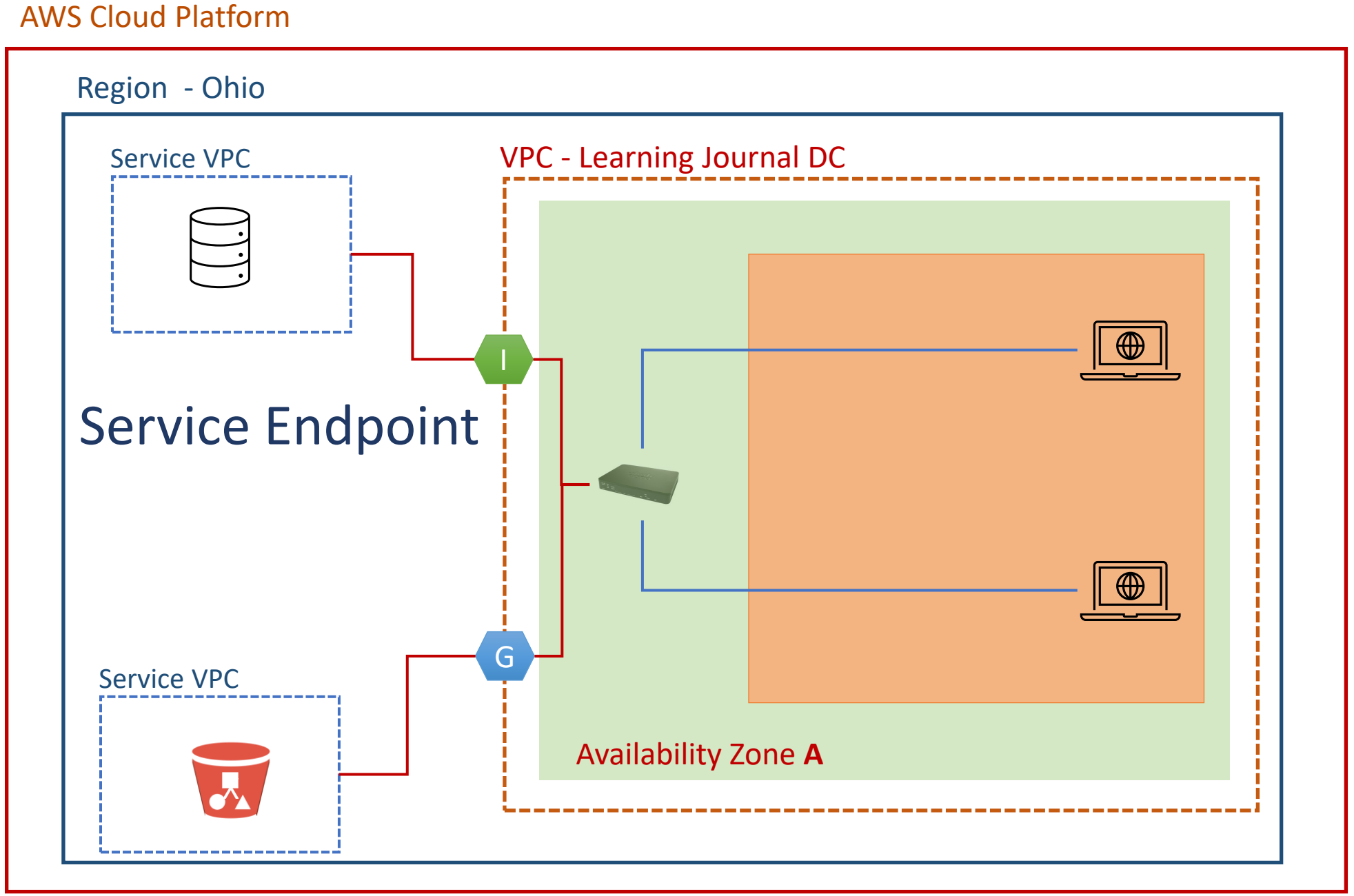
Custom Route Table

Destination	Target
0.0.0.0/0	lgw-01
10.0.0.1/24	local

Main Route Table

Destination	Target
10.0.0.1/24	Local
0.0.0.0/0	nat-gateway
pl-id-s3	edpoint-id

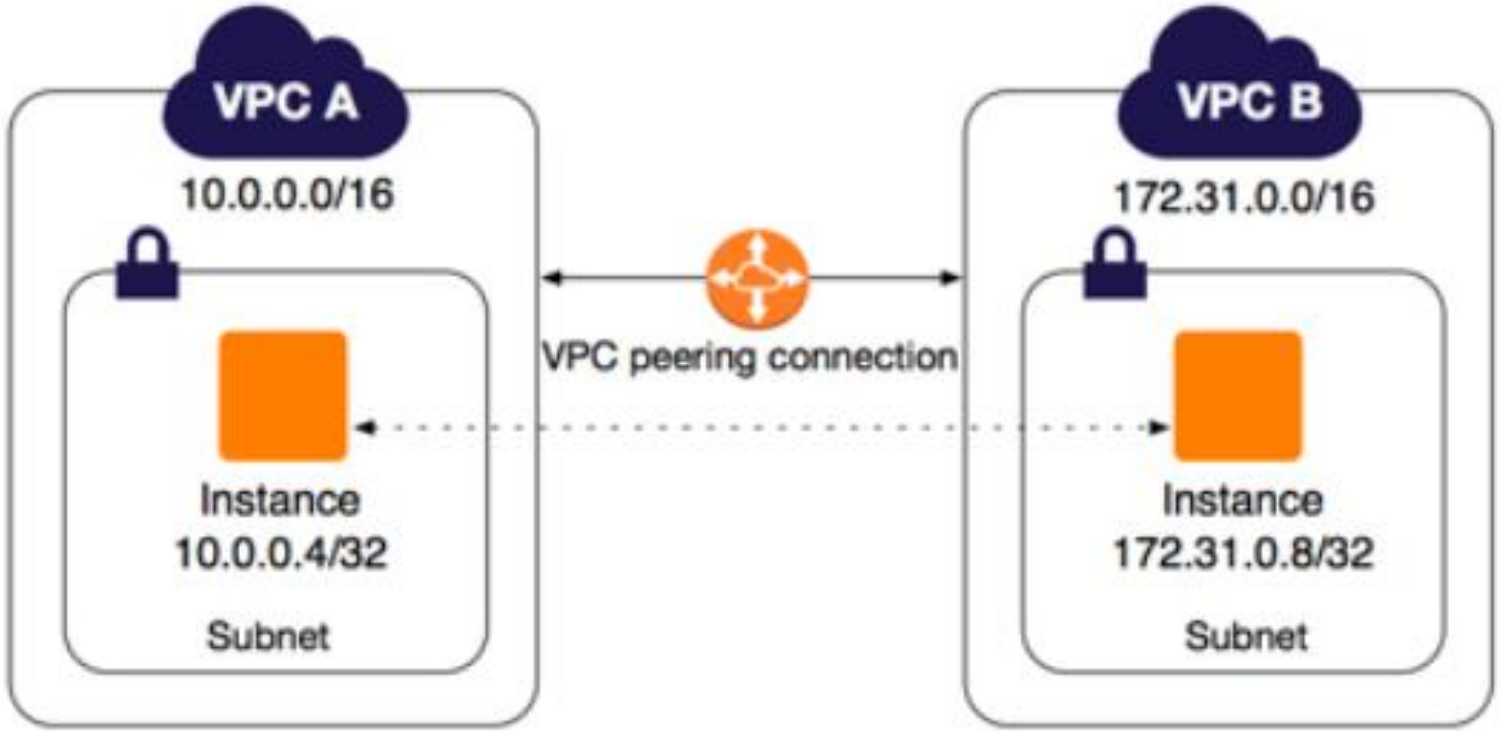
Gateway Endpoint


AWS Cloud Platform
Region - Ohio
Service VPC
VPC - Learning Journal DC
I
Service Endpoint
G
Service VPC
Availability Zone A

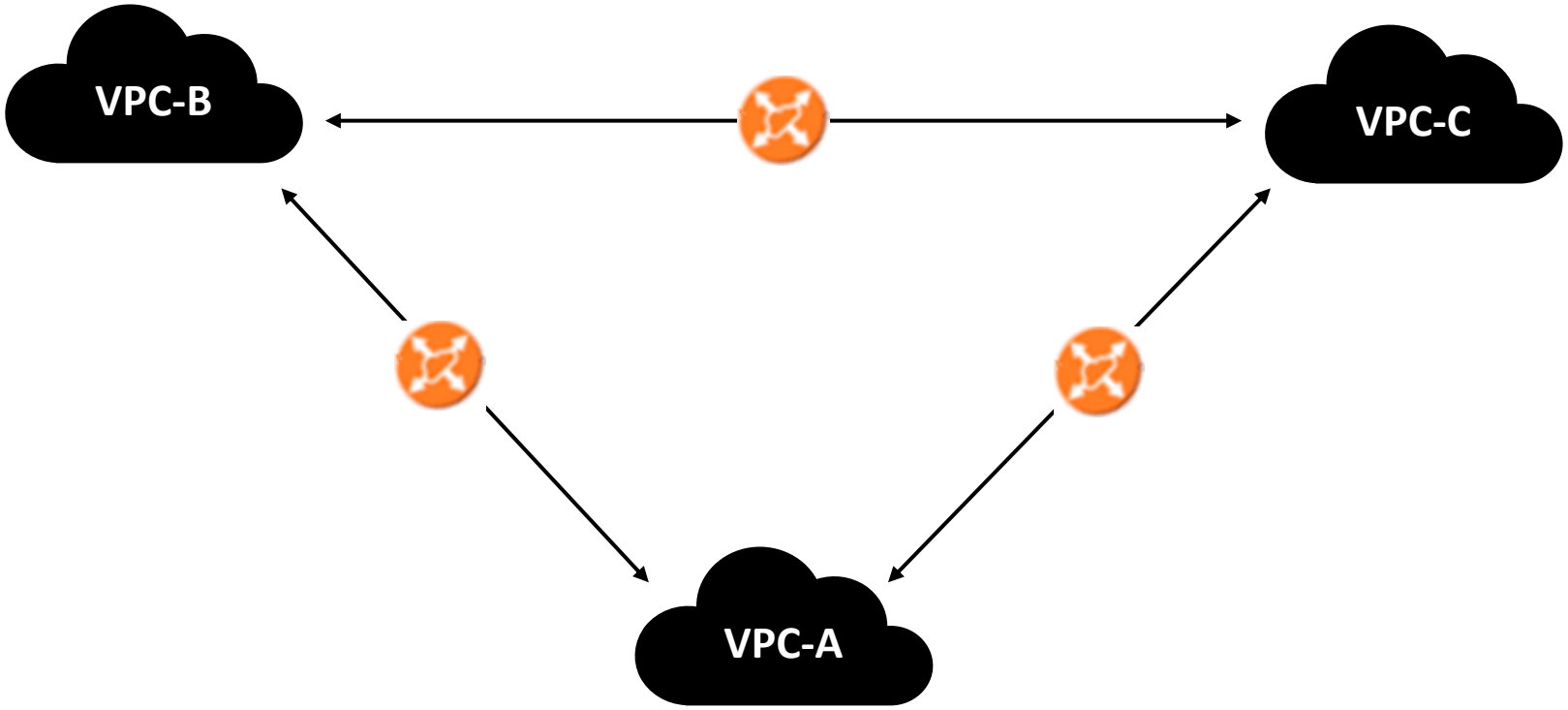
Connecting Multiple VPC?

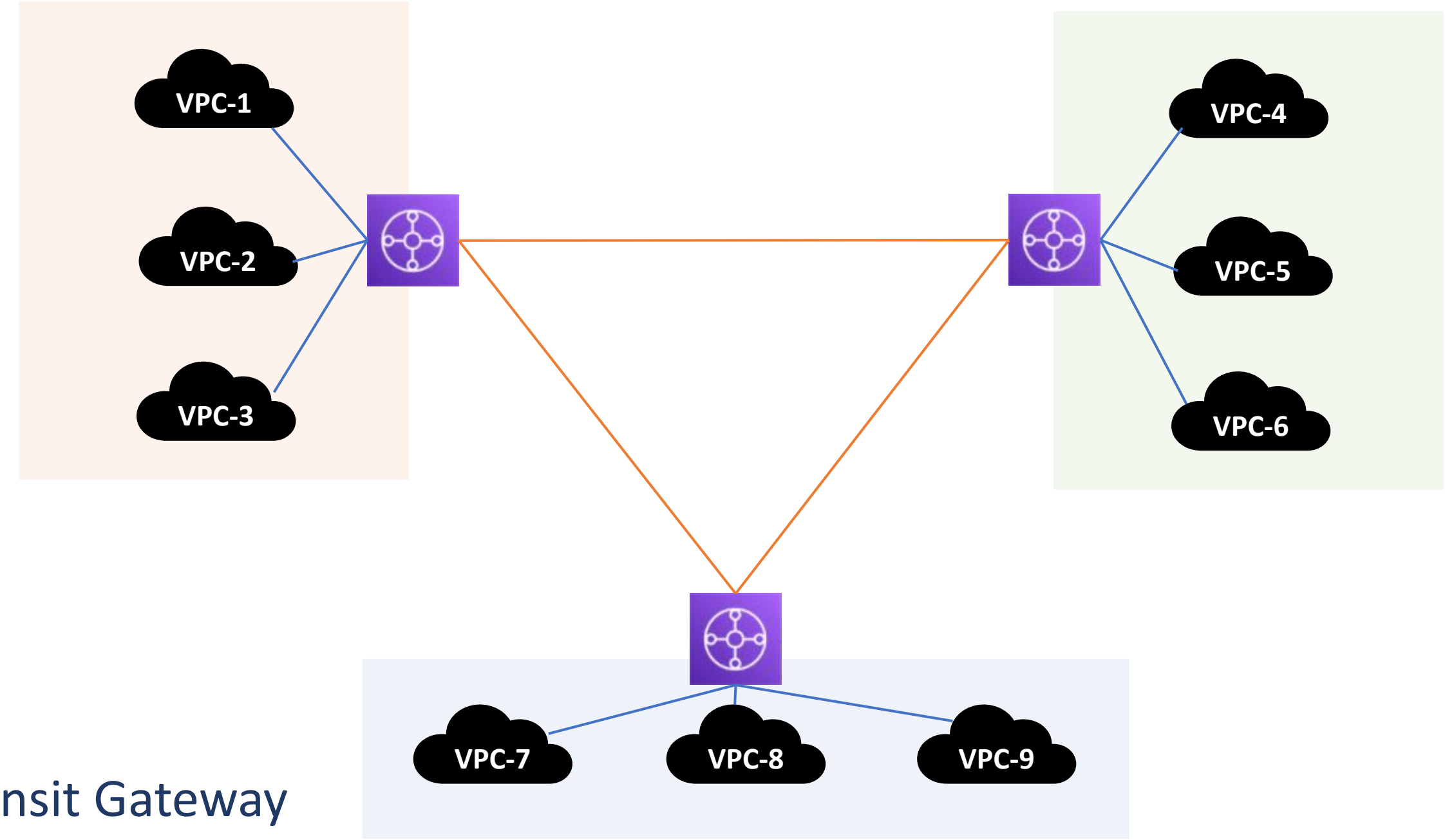
1. VPC Peering
2. AWS Transit Gateway

VPC Peering


VPC A
10.0.0.0/16
Instance
10.0.0.4/32
Subnet
VPC peering connection
VPC B
172.31.0.0/16
Instance
172.31.0.8/32
Subnet

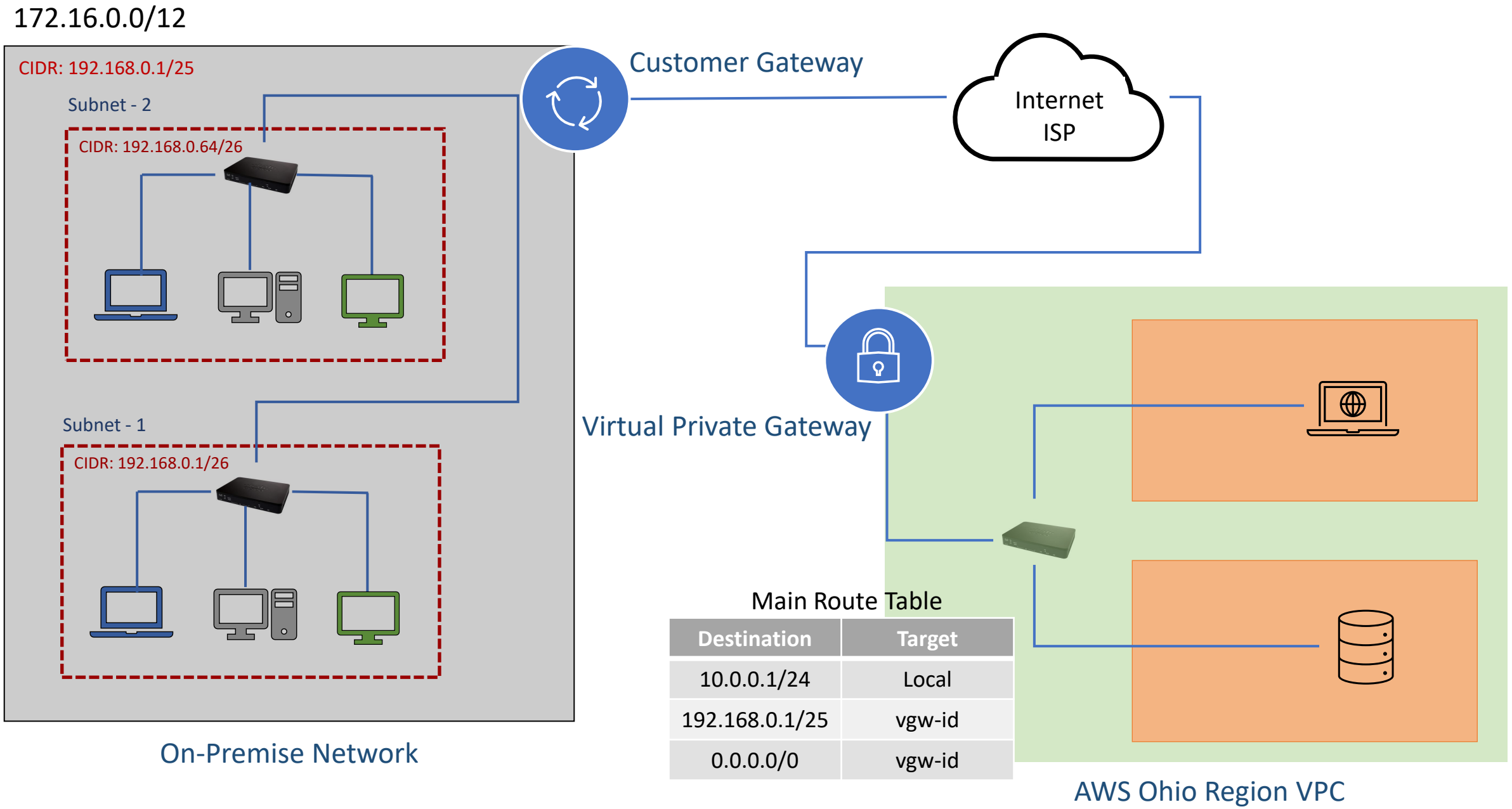
VPC Peering





Transit Gateway

Site-to-Site VPN



Customer Gateway

1. Customer Gateway Device
2. Customer Gateway Configuration

- Check Point Security Gateway running R77.10 (or later) software
- Cisco ASA running Cisco ASA 8.2 (or later) software
- SonicWALL running SonicOS 5.9 (or later) software
- Juniper SRX running JunOS 11.0 (or later) software
- Microsoft Windows Server 2012 R2 (or later) software

Connecting Multiple VPC?

1. VPC Peering
2. AWS Transit Gateway

AWS VPC to On-Premise connection

1. AWS Managed VPN (Site-to-Site VPN)
2. AWS Direct Connect (AWS DX)

Shared responsibility Model?

1. Security of the Cloud
2. Security in the cloud

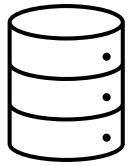
Security in the cloud?

Amazon EC2

Your Responsibilities

- Install OS
- Update OS
- Install OS Security Patch
- Install Other Software
- Install Security patch for other software
- Configure Firewall
- Manage User Access and Permissions
- Generate and Monitor Audit Logs

Security in the cloud?



Dynamo DB

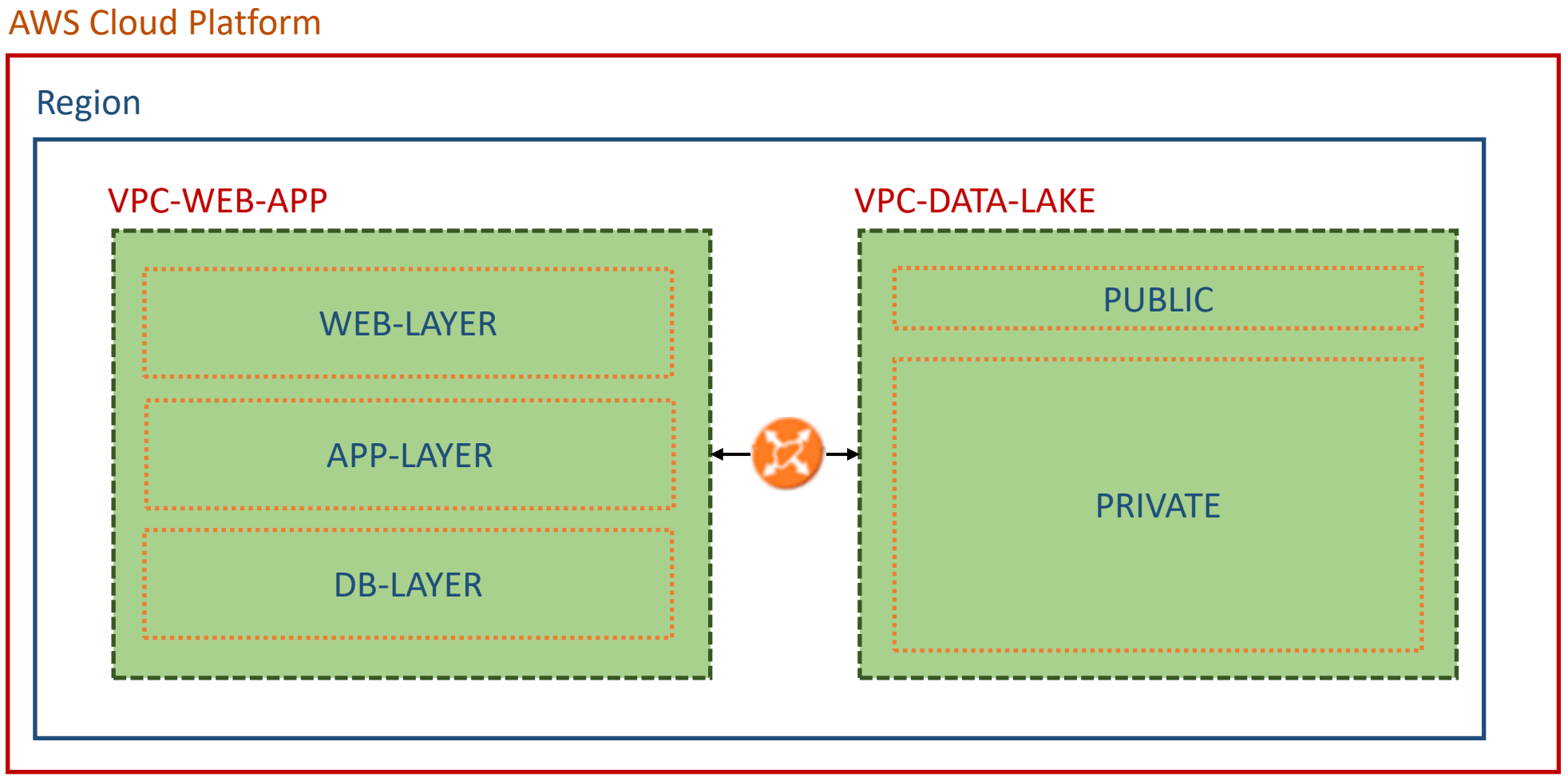
AWS Responsibilities

- Install OS
- Update OS
- Install OS Security Patch
- Install Database
- Install Security patch for Database

Your Responsibilities

- Manage User Access and Permissions
- Configure Firewall
- Data Encryption

Network Isolation?



Internetwork traffic security

1. Security groups
2. Network access control lists or NACLs
3. Flow logs

Security group

1. Is a firewall
2. Applies to an instance
3. Up to 5 SG per instance (this limit can be increased)
4. Supports only allow rule
5. Stateful

Network ACL - NACLs

1. Is a firewall
2. Applies to a subnet
3. All subnets must have a NACL
4. Subnet can have one NACL
5. NACL supports allow and deny rules
6. Stateless
7. NACL rules are evaluated in increasing order

Security Group Vs Network ACL

S. No.	Security Group	Network ACL
1.	Operates at the instance level	Operate at the subnet level
2.	Supports allow-rules only	Supports allow-rules and deny rules
3.	Stateful	Stateless
4.	Evaluates all rules before deciding allow/deny	Process rules in order

Flow Logs

Capture information about the IP traffic
Log levels – VPC, subnet, network interface
Published to – Cloud Watch or S3

Purpose of Flow Logs

1. Troubleshooting connectivity issues
2. Intrusion detection
3. Anomaly detection
4. Archival for compliance purposes
5. Monitoring and metrics collection for your application