ENGENHARIA DE SOFTWARE

41492-ES

Nuno Sá Couto / Rafael Direito

(nuno.sacouto@ua.pt / rafael.neves.direito@ua.pt)

Department of Electronics, Telecommunications and Informatics (DETI)

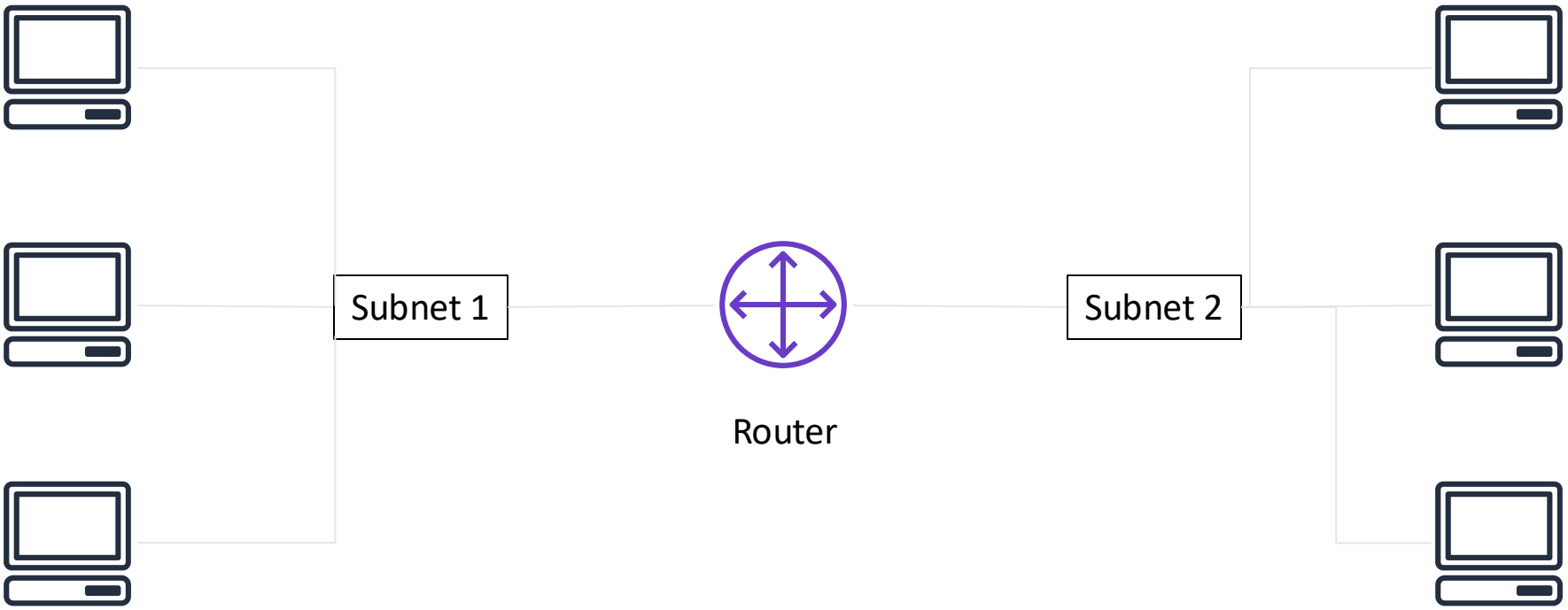
UNIVERSITY OF AVEIRO (UA), PORTUGAL

2024

Module 5: Networking and Content Delivery

SECTION 1: NETWORKING BASICS

Networks



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

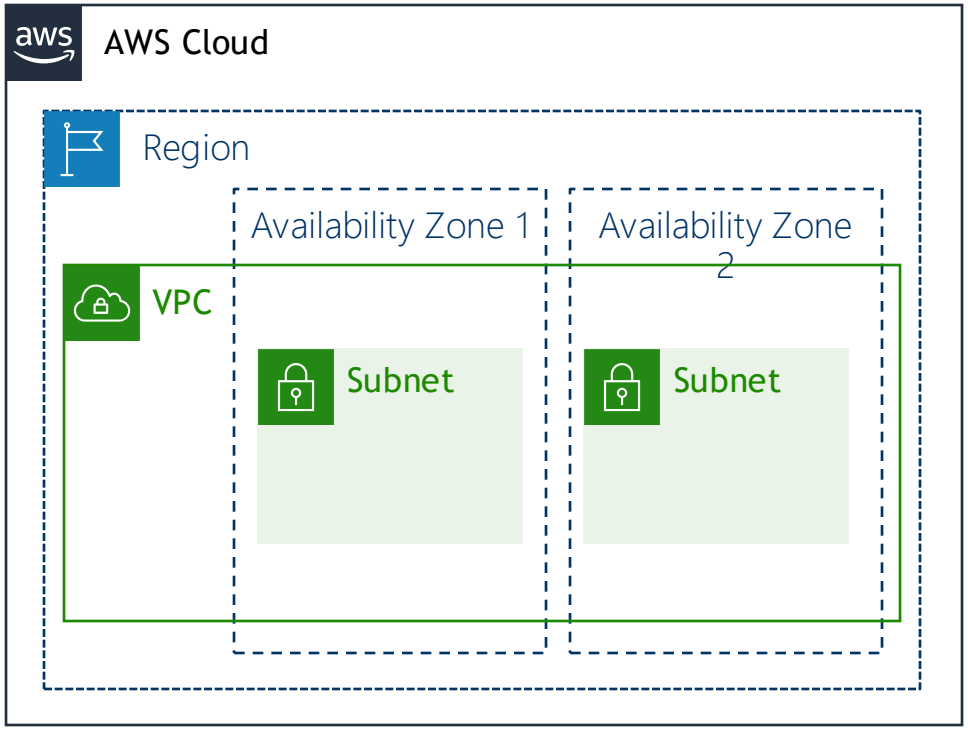
Amazon VPC

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

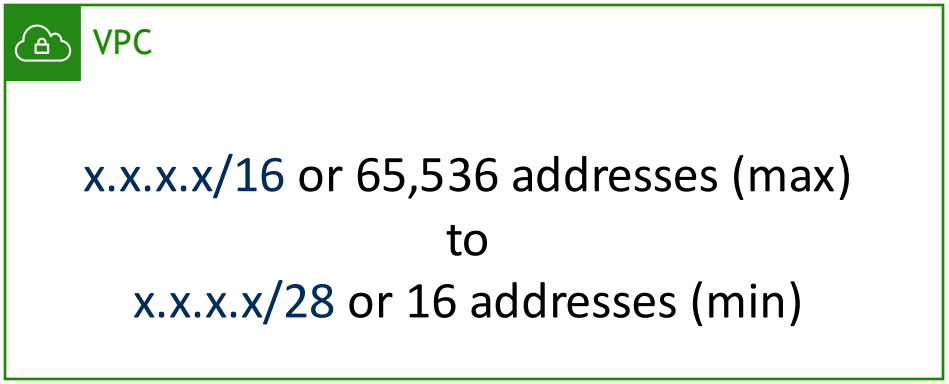
VPCs and subnets

- 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



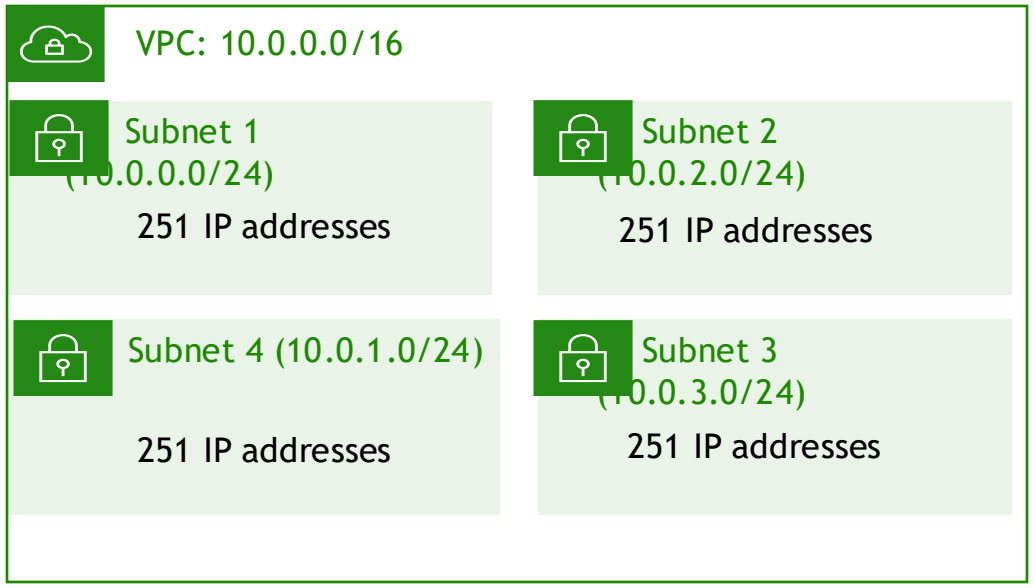
IP addressing

- 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.



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

Public IP address types

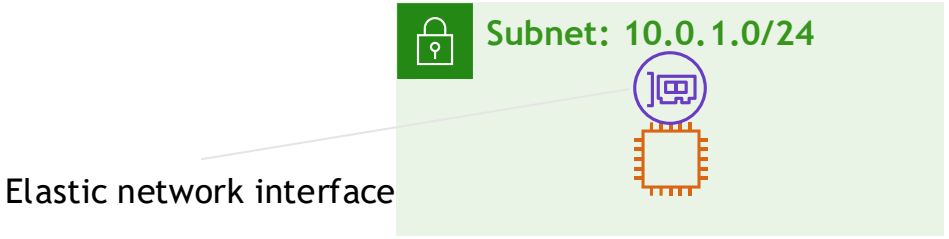
- Add content text
  - Second level
    - Third level
      - Avoid using fourth level
        - Avoid using fifth level

Public IPv4 address

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

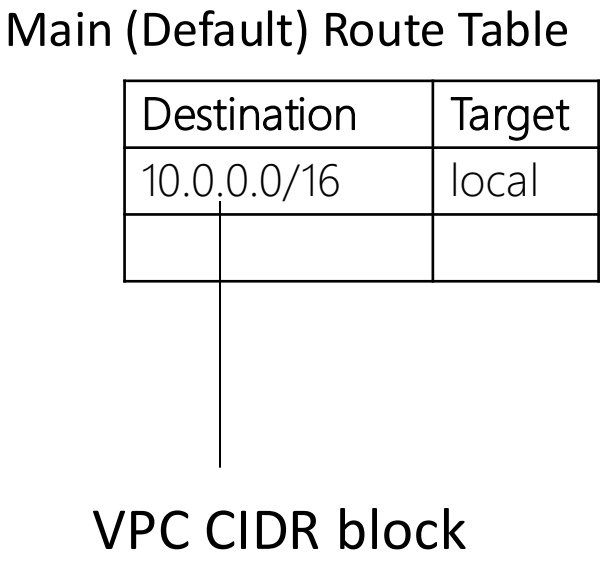
Elastic network interface

- 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

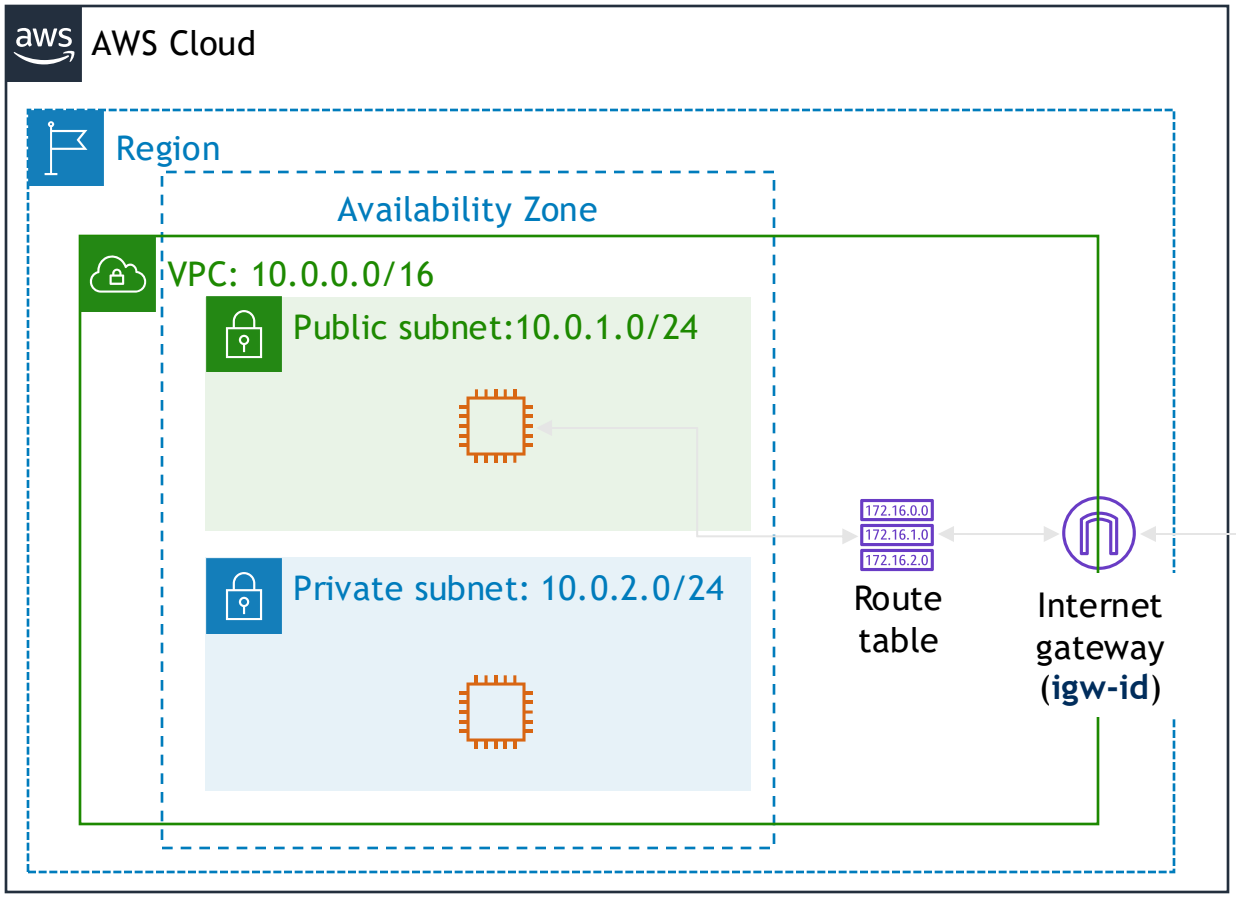
- A route table contains a set of rules (or routes) that you can configure to direct network traffic from your subnet.
- Each route specifies a destination and a target.
- By default, every route table contains a local route for communication within the VPC.
- Each subnet must be associated with a route table (at most one).



Module 5: Networking and Content Delivery

SECTION 3: VPC NETWORKING

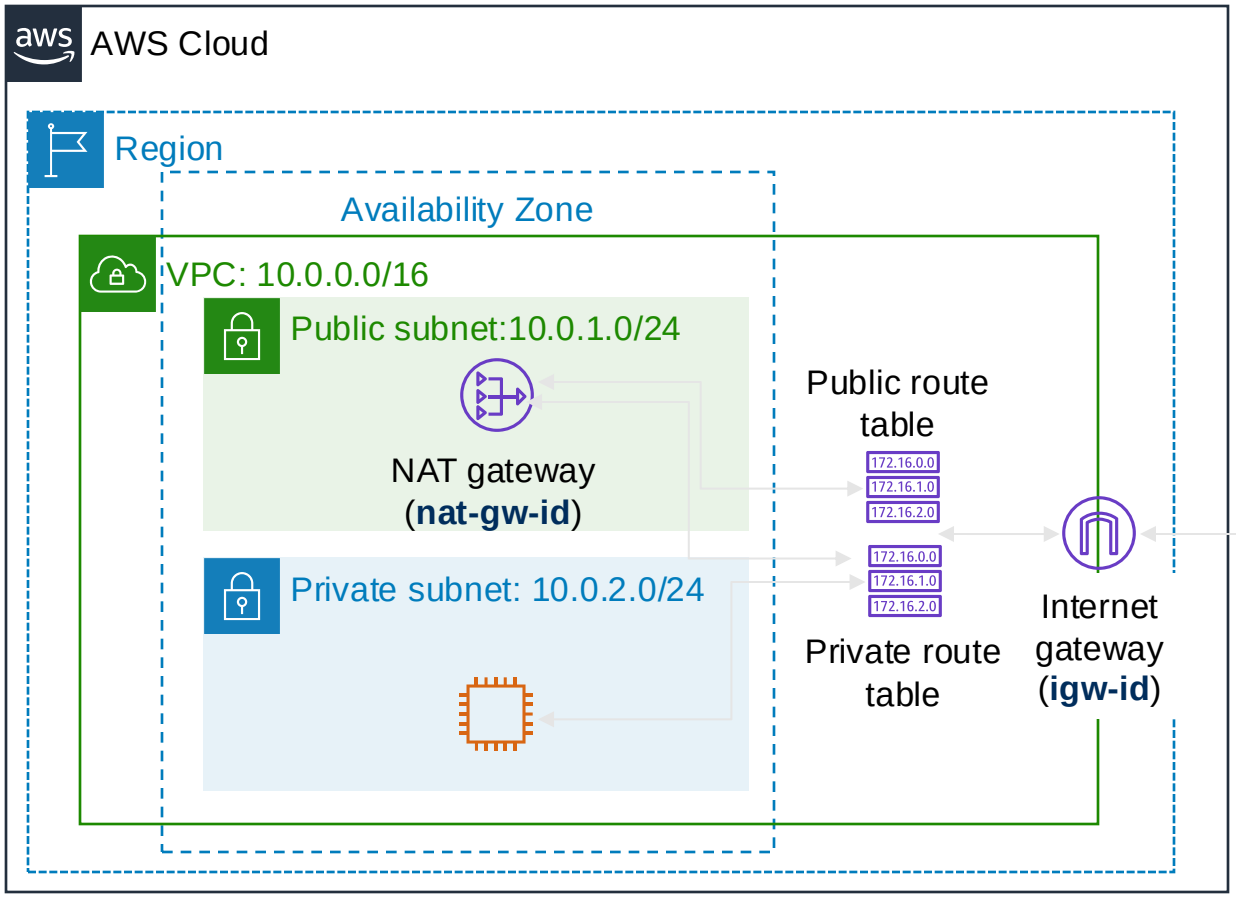
Internet gateway



Public Subnet Route Table

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

Network address translation (NAT) gateway



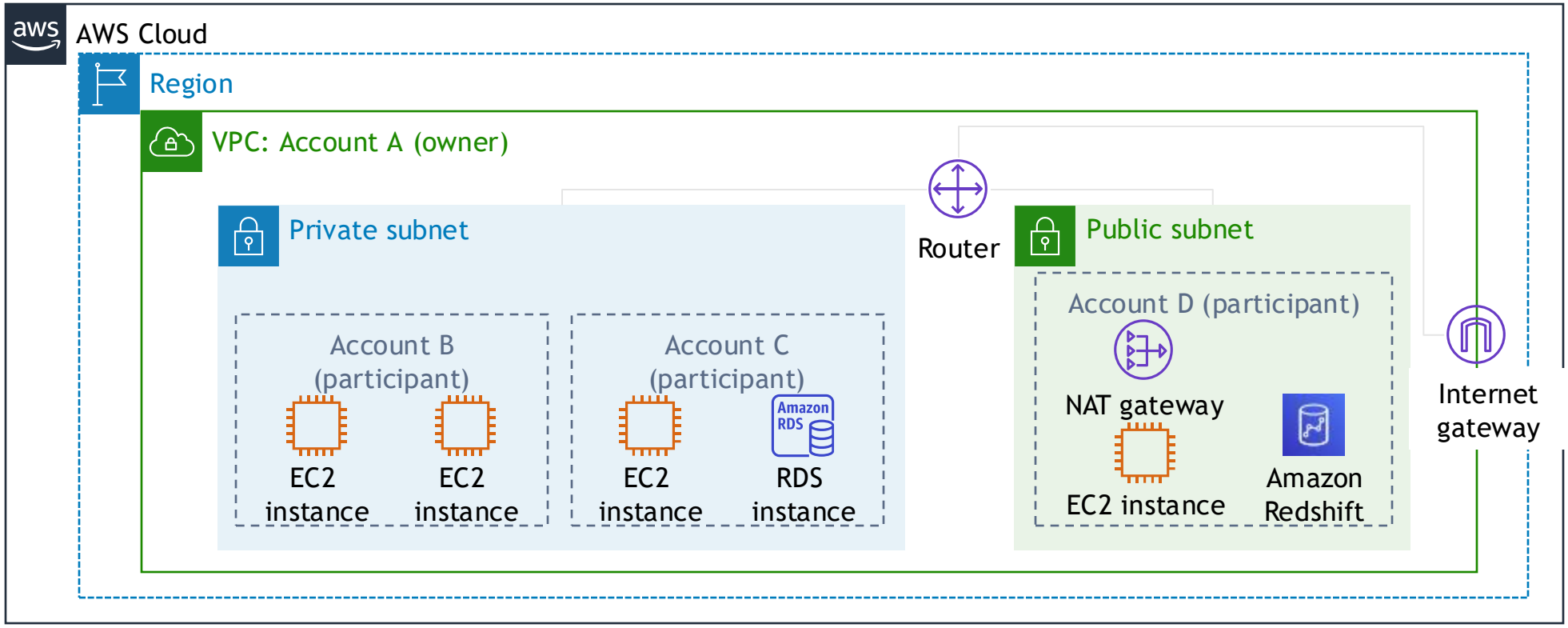
Public Subnet Route Table

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

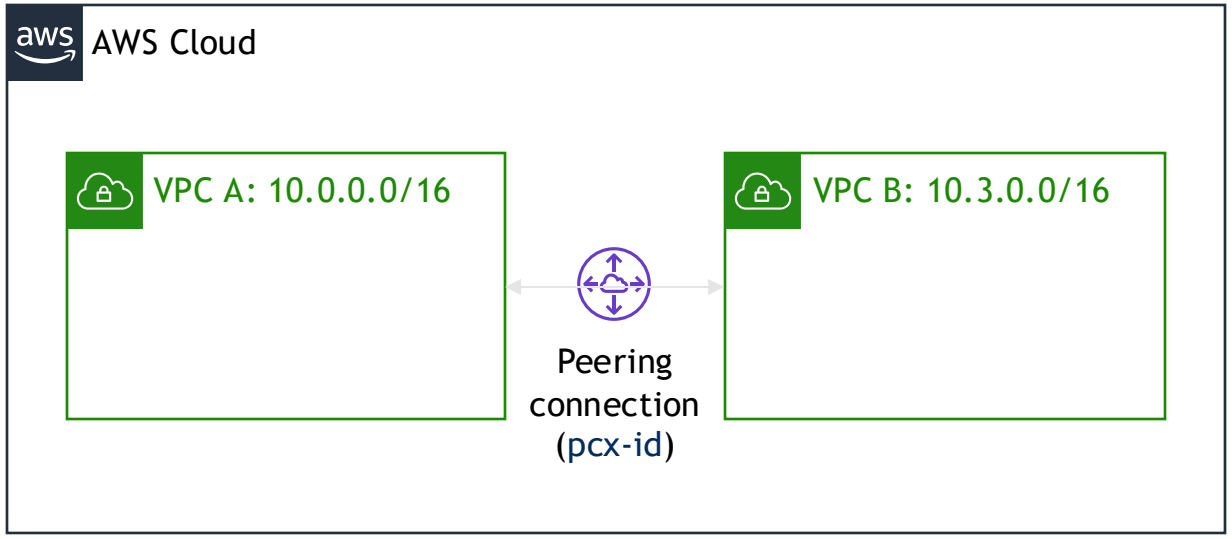
Private Subnet Route Table

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

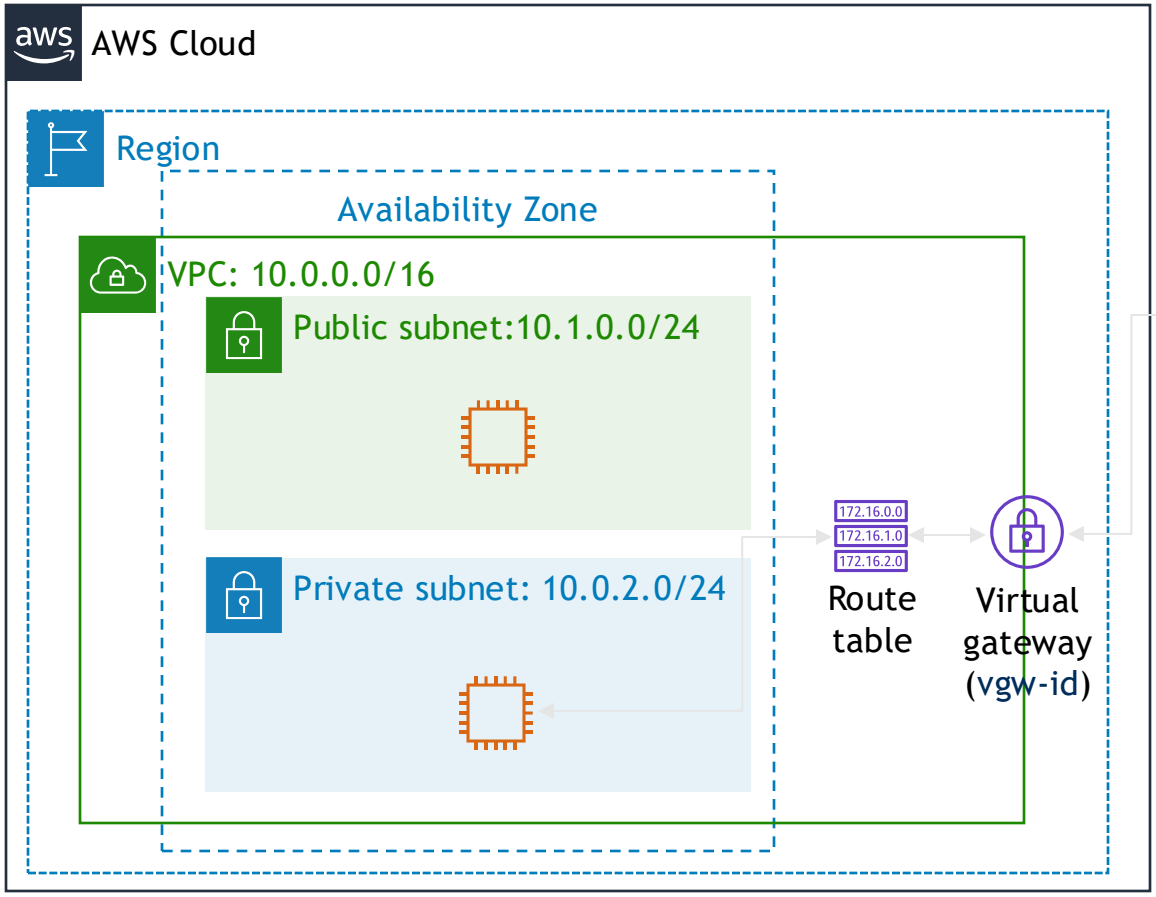
Destination	Target
10.3.0.0/16	local
10.0.0.0/16	pcx-id

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



Site-to-Site VPN connection

Internet

Customer gateway

Corporate data center: 192.168.10.0/24

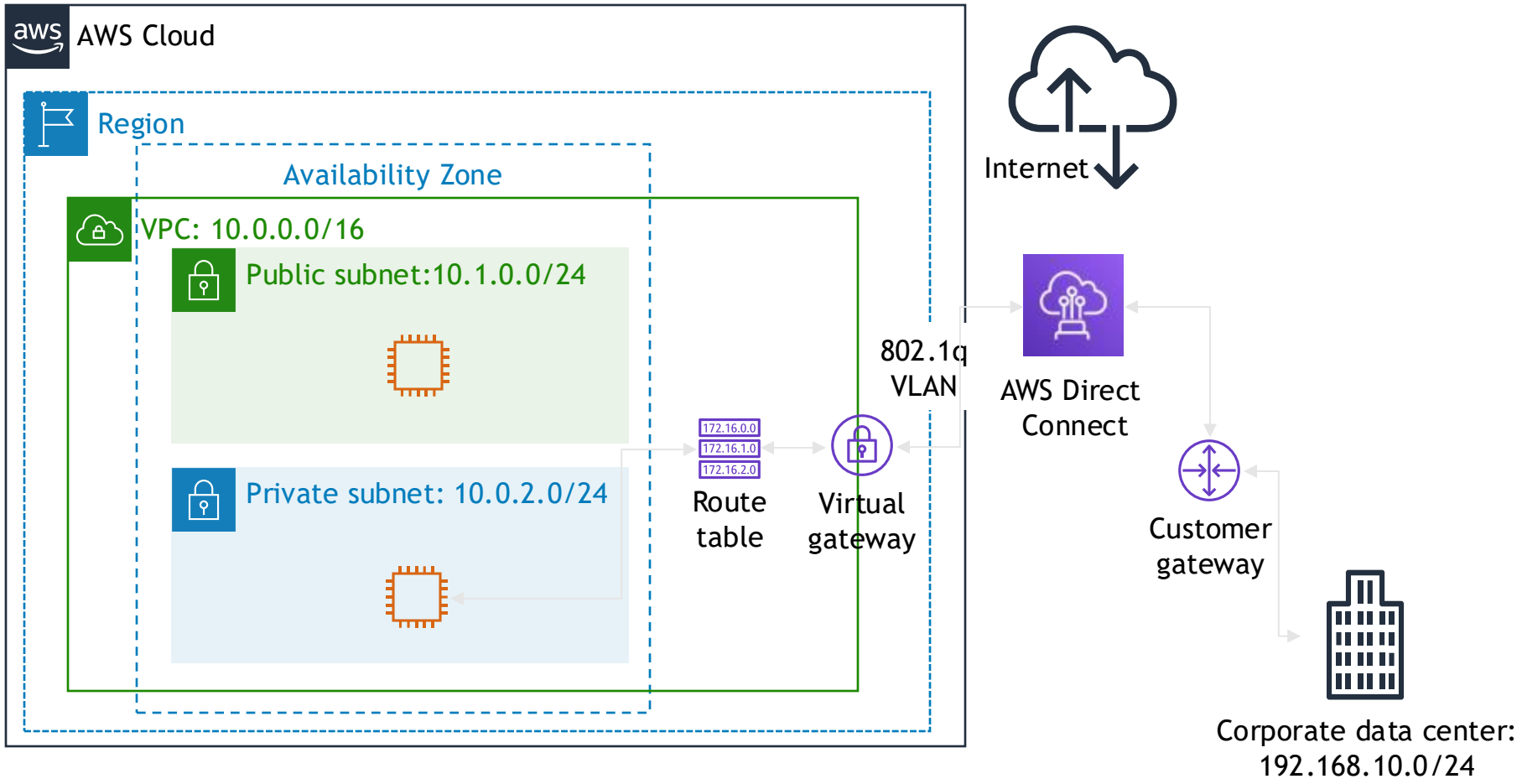
Public subnet route table

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

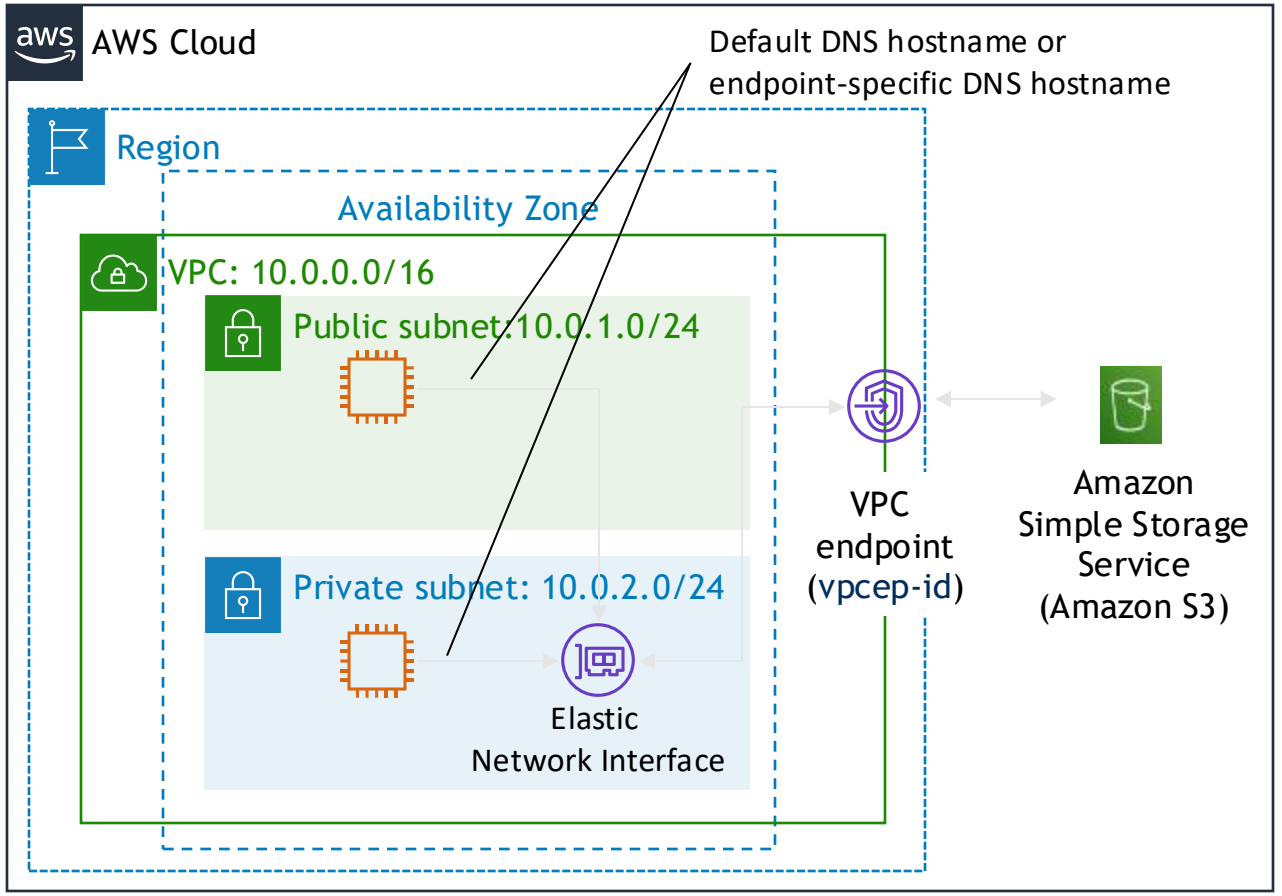
Private subnet route table

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

AWS Direct Connect



VPC endpoints



Public Subnet Route Table

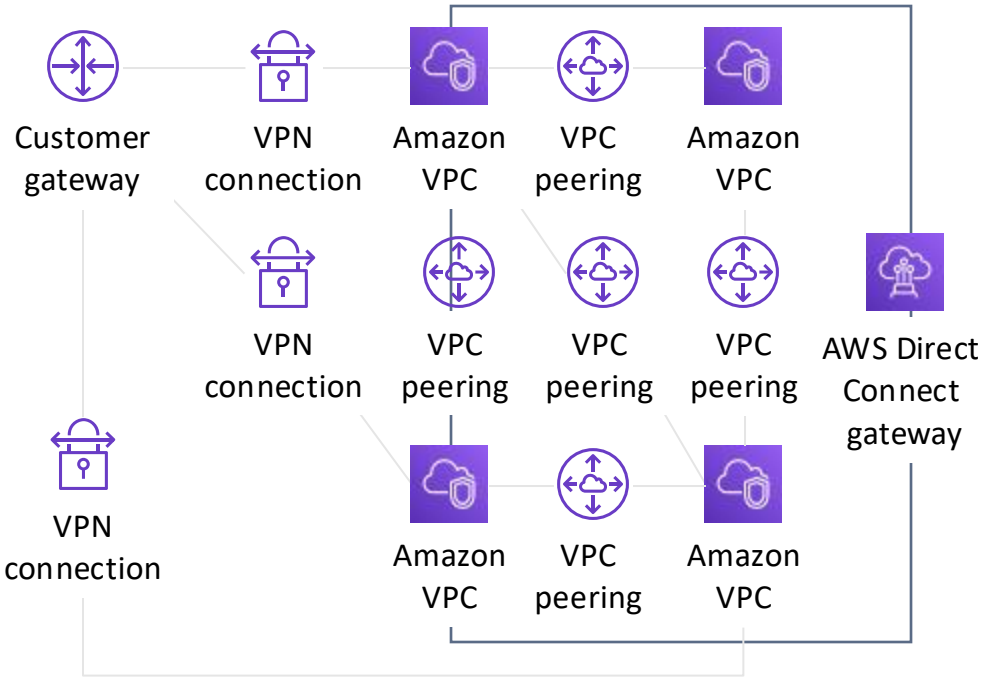
Destination	Target
10.0.0.0/16	local
Amazon S3 ID	vpcep-id

Two types of endpoints:

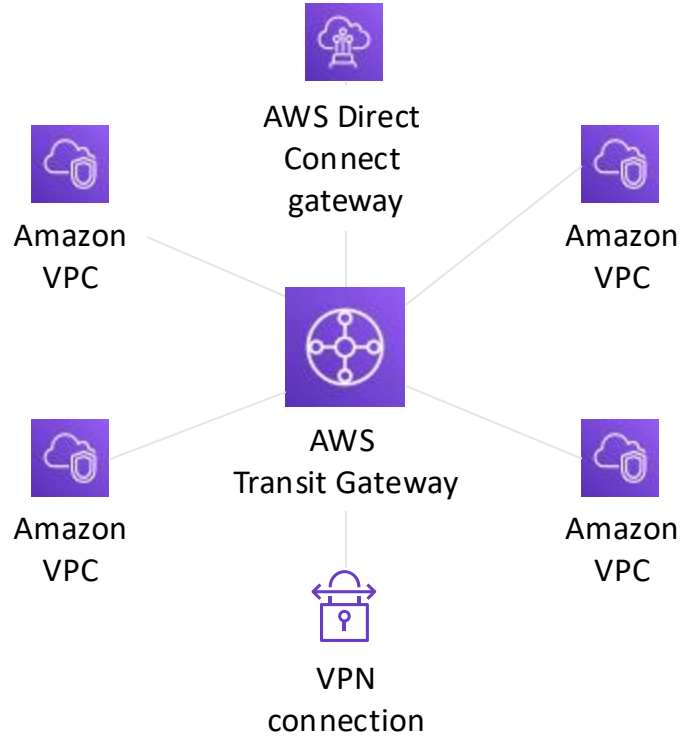
- **Interface** endpoints (powered by AWS PrivateLink)
- **Gateway** endpoints (Amazon S3 and Amazon DynamoDB)

AWS Transit Gateway

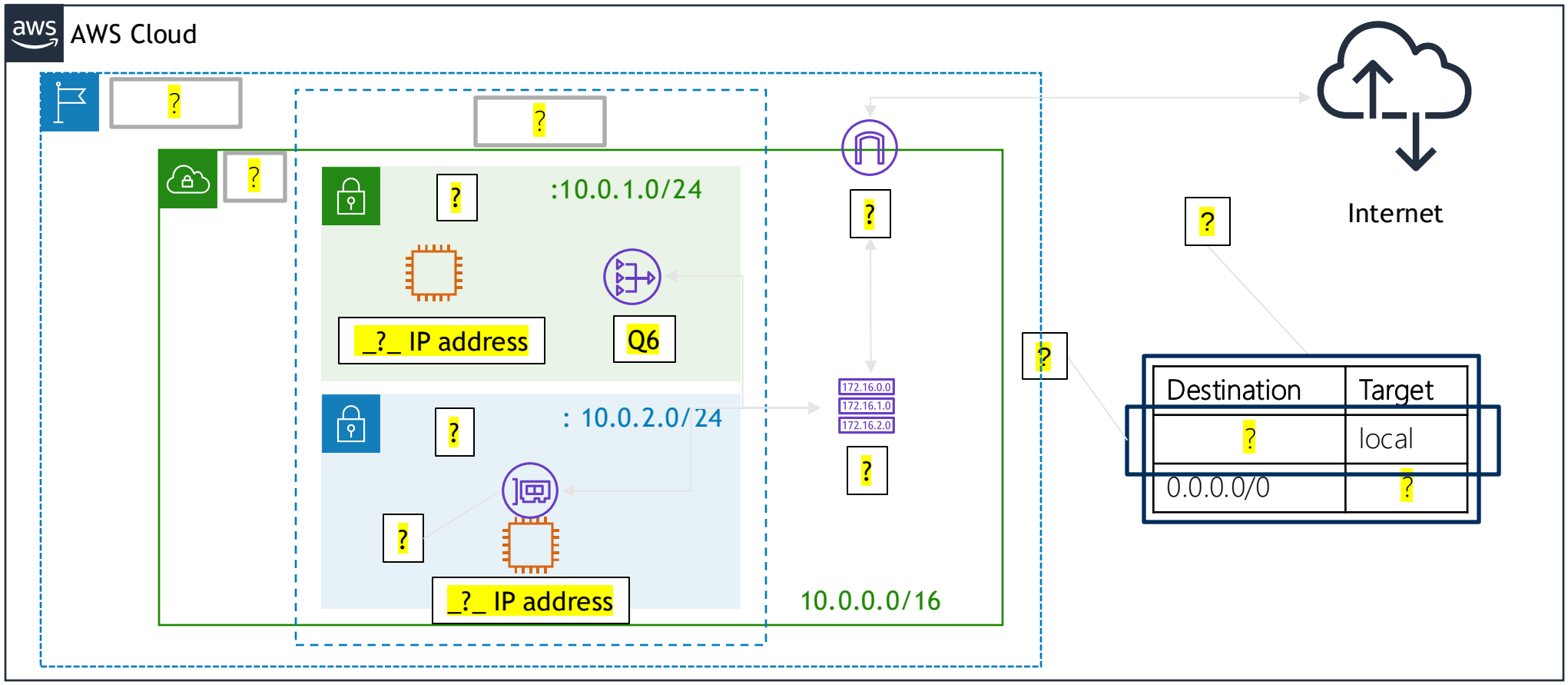
From this…



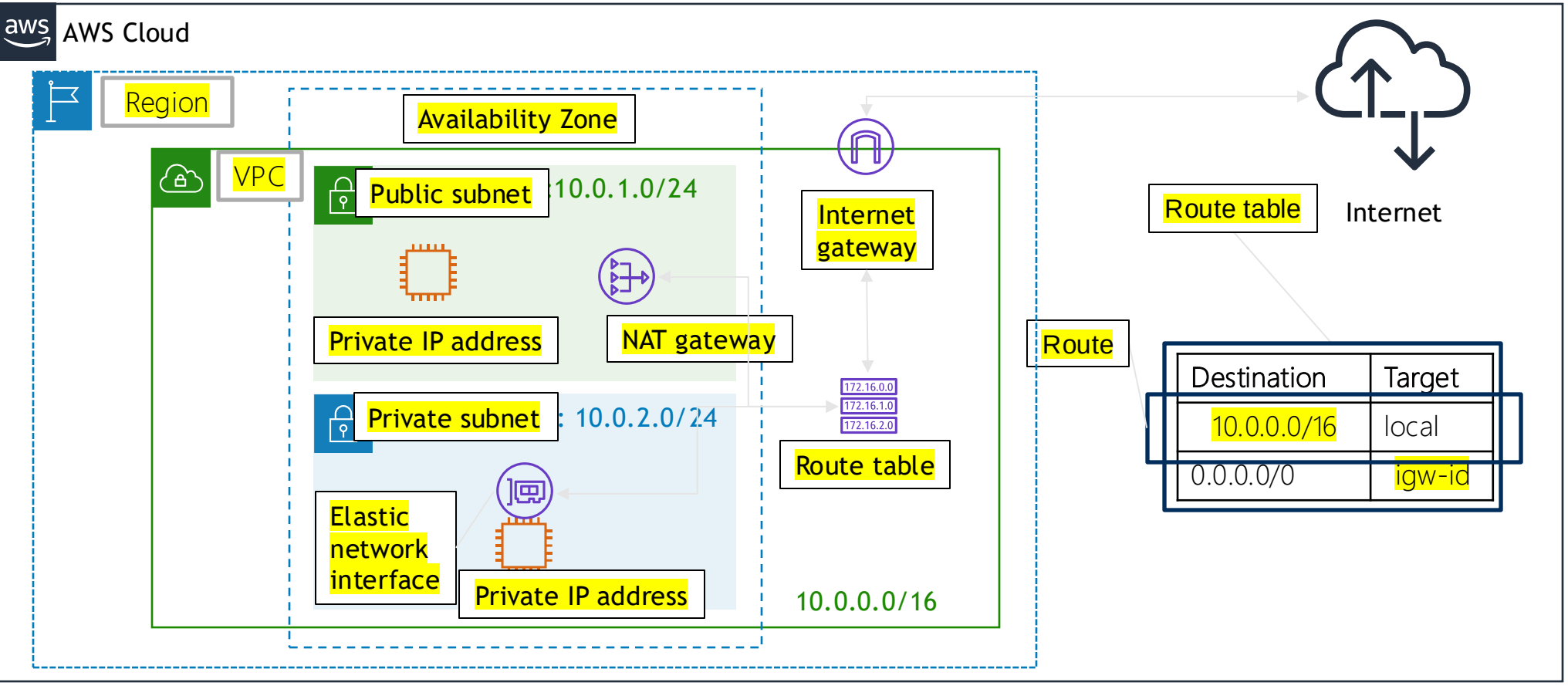
To this…



Activity: Label this network diagram



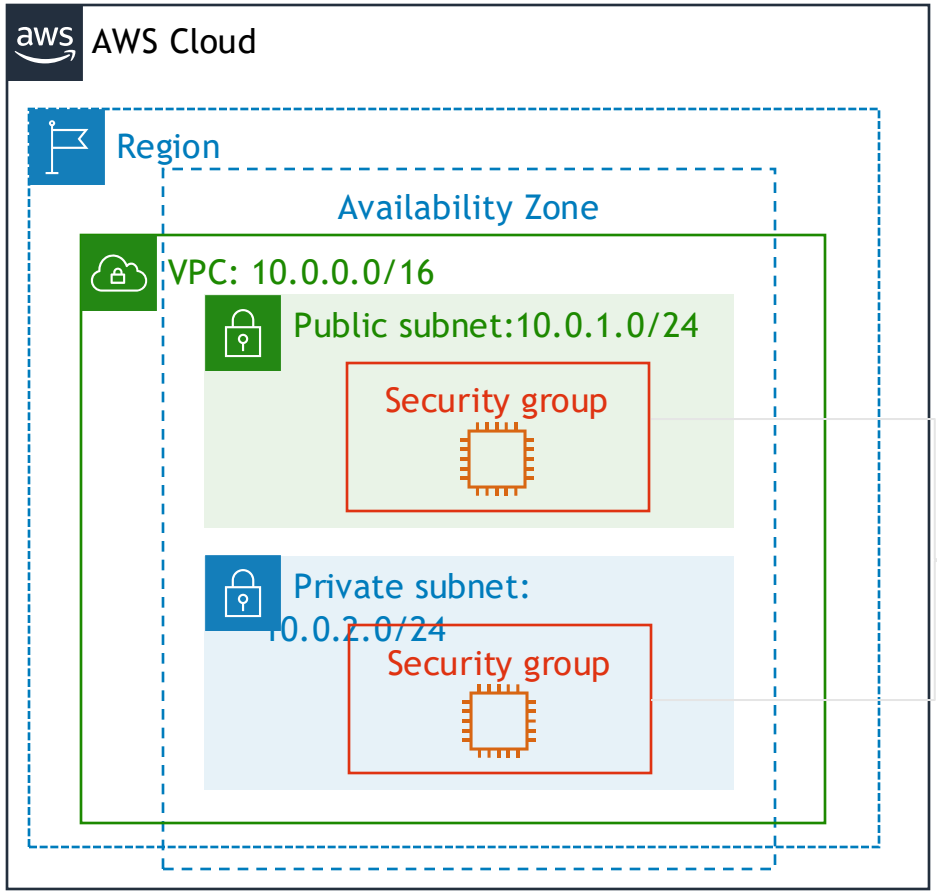
Activity: Solution



Module 5: Networking and Content Delivery

SECTION 4: VPC SECURITY

Security groups (1 of 2)



Security groups act at the instance level.

Security groups (2 of 2)

- 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.

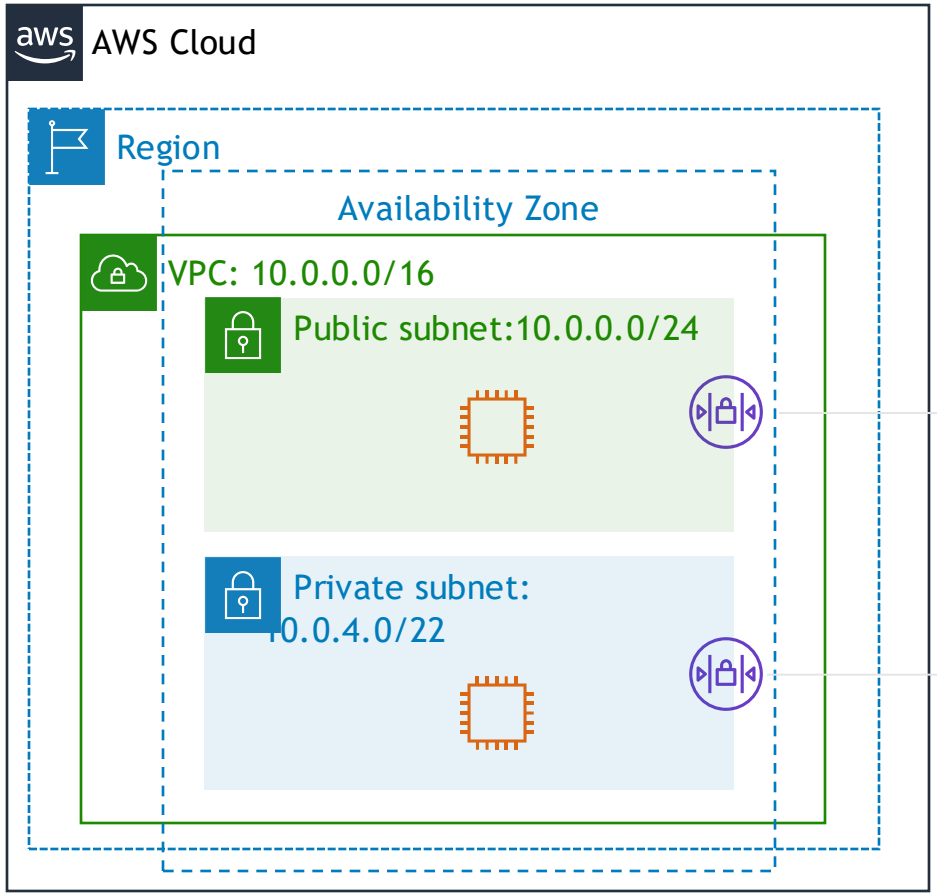
Inbound

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	TCP	22	Allow inbound SSH access to Linux instances from

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 1 of 2)



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

Network access control lists (network ACLs 2 of 2)

- 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

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.

Module 5: Networking and Content Delivery

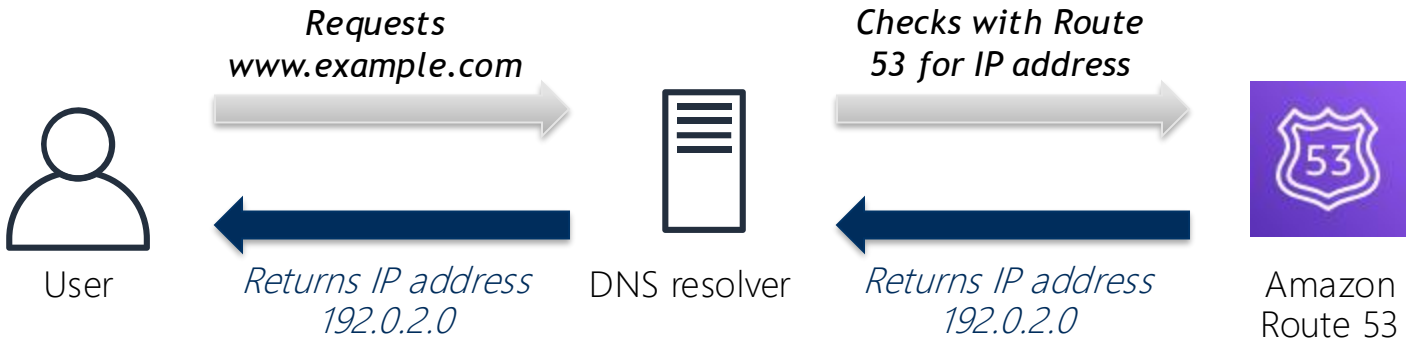
SECTION 5: AMAZON ROUTE 53

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

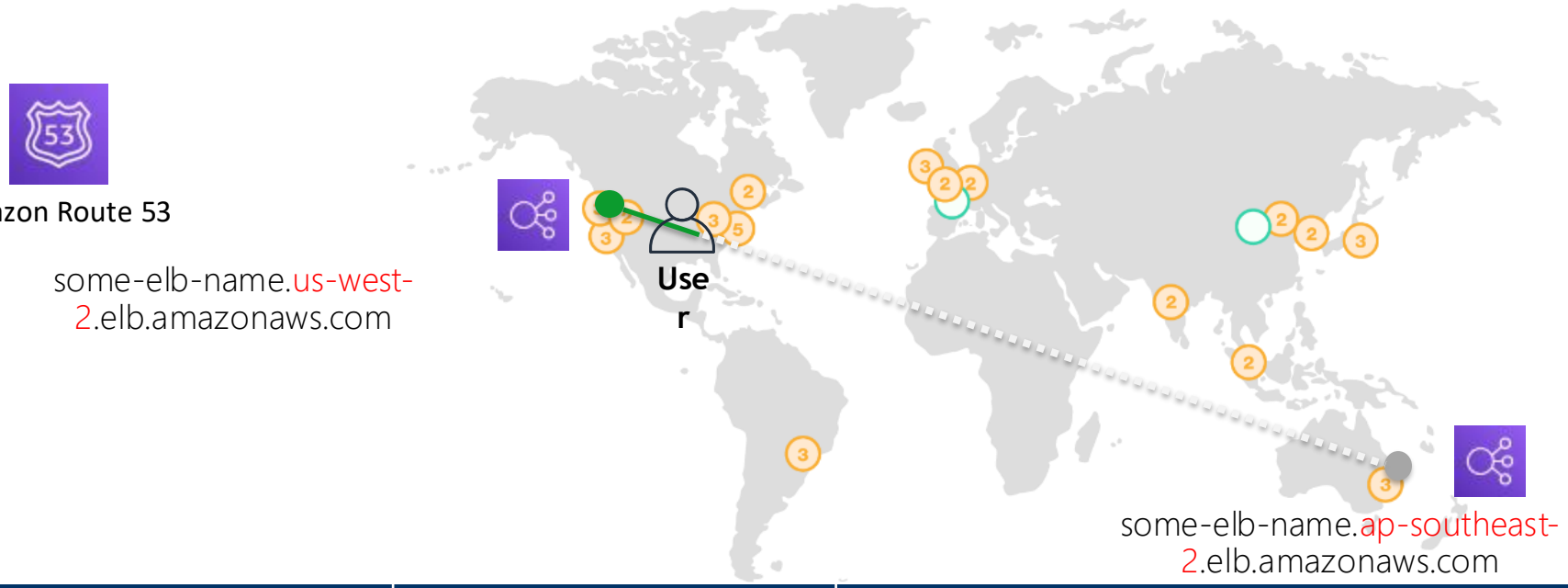
Amazon Route 53 DNS resolution



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



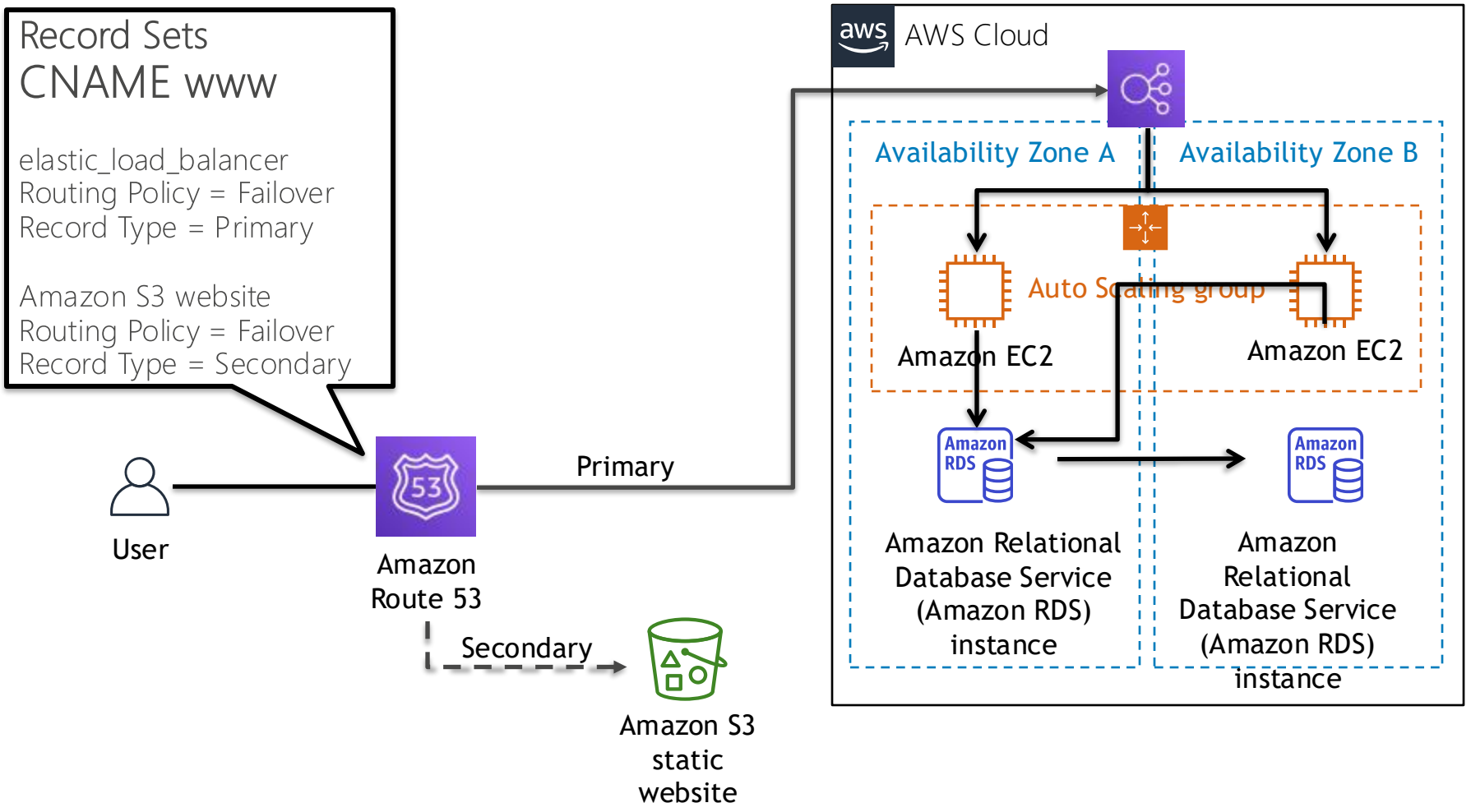
Name	Type	Value
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

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 h

DNS failover for a multi-tiered web application



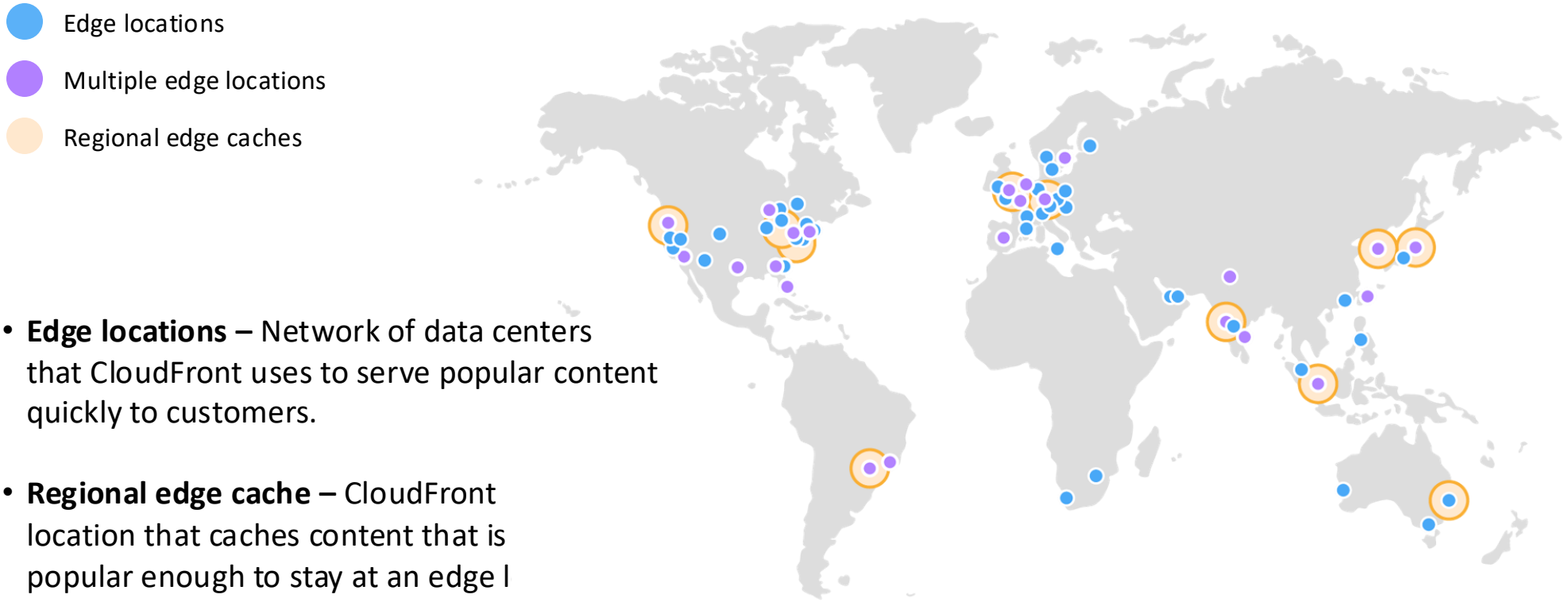
Module 5: Networking and Content Delivery

SECTION 6: AMAZON CLOUDFRONT

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 infrastructure



- **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 popular enough to stay at an edge l It is located between the origin serv 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.