Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module overview

Topics

- Networking basics
- Amazon VPC
- VPC networking
- VPC security
- Amazon Route 53
- Amazon CloudFront

Knowledge check

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module objectives

After completing this module, you should be able to:

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

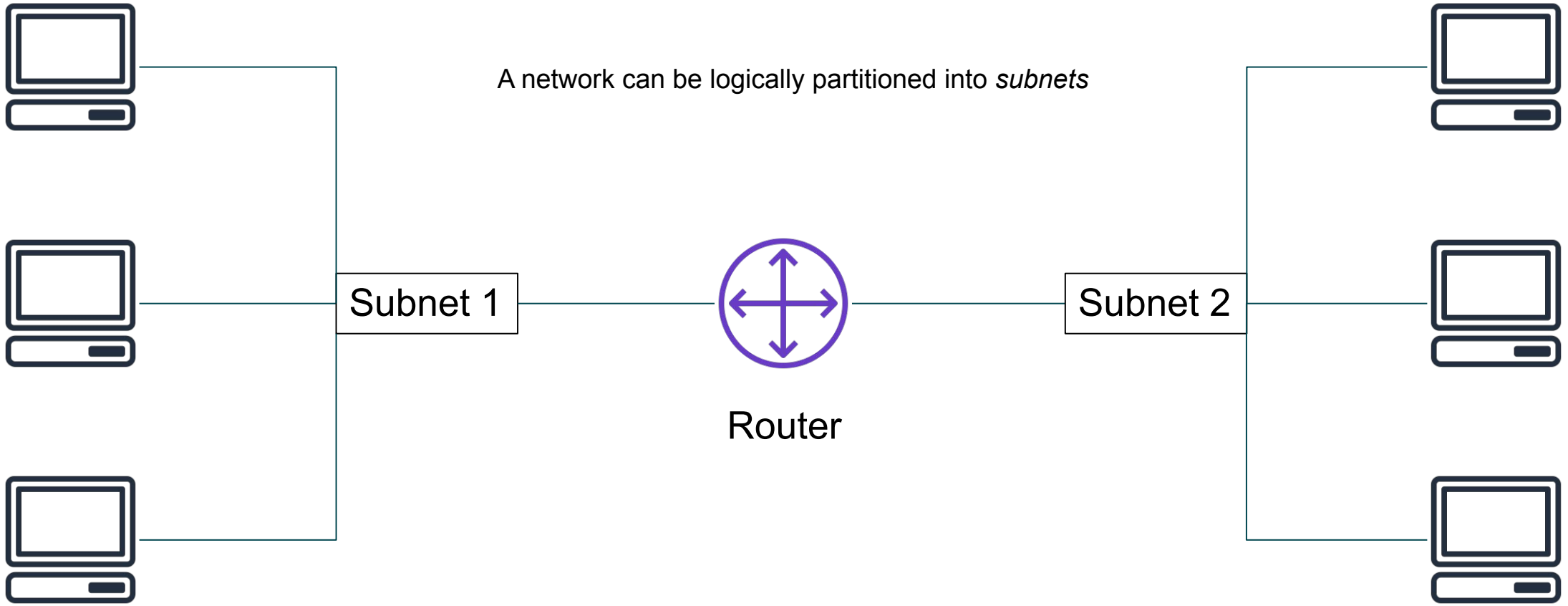
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 1: Networking basics

Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

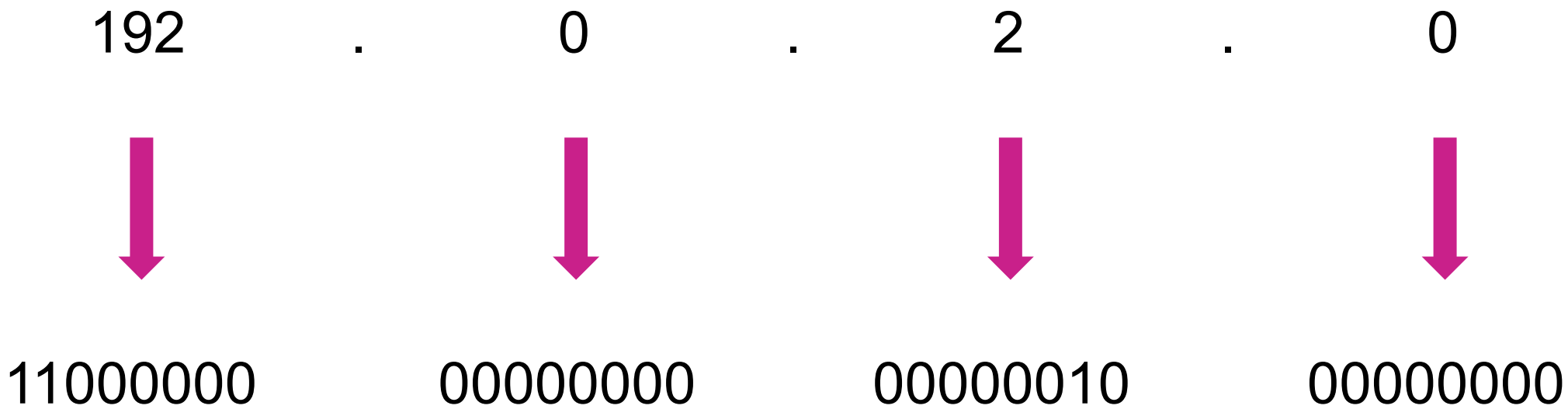
Networks



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IP addresses

An IP address is a numerical label in decimal format. Machines convert that decimal number to a binary format.



The IP address is 192.0.2.0. Each of the four dot (.)-separated numbers of the IP address represents 8 bits in octal number format. That means each of the four numbers can be anything from 0 to 255. The combined total of the four numbers for an IP address is 32 bits in binary format

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

IPv4 and IPv6 addresses

IPv4 (32-bit) address:
192.0.2.0

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

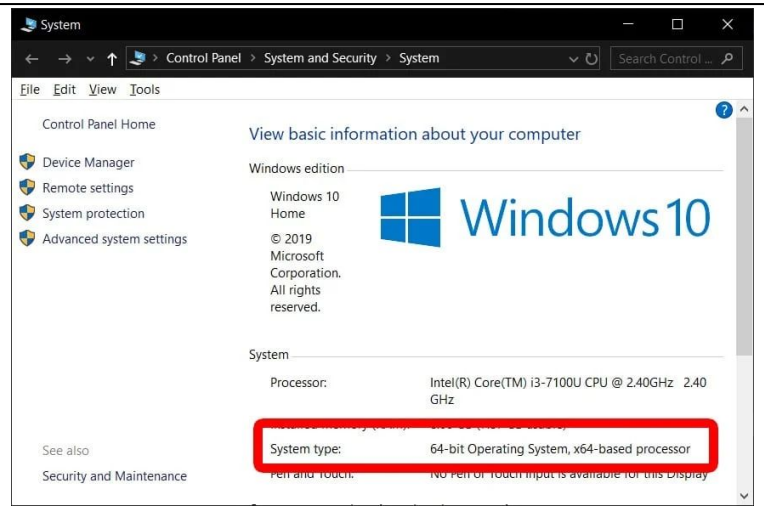
An IPv6 address is composed of eight groups of four letters and numbers that are separated by colons (:). Each of the eight colon-separated groups of the IPv6 address represents 16 bits in hexadecimal number format. That means each of the eight groups can be anything from 0 to FFFF. The combined total of the eight groups for an IPv6 address is 128 bits in binary format.

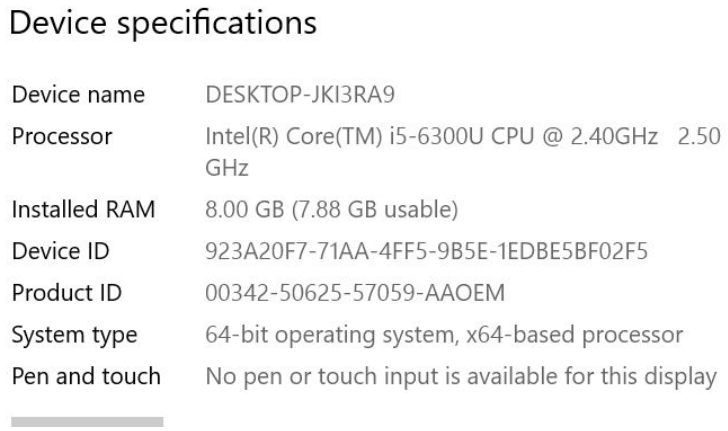
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Difference Between Network Bits and Processor Bits

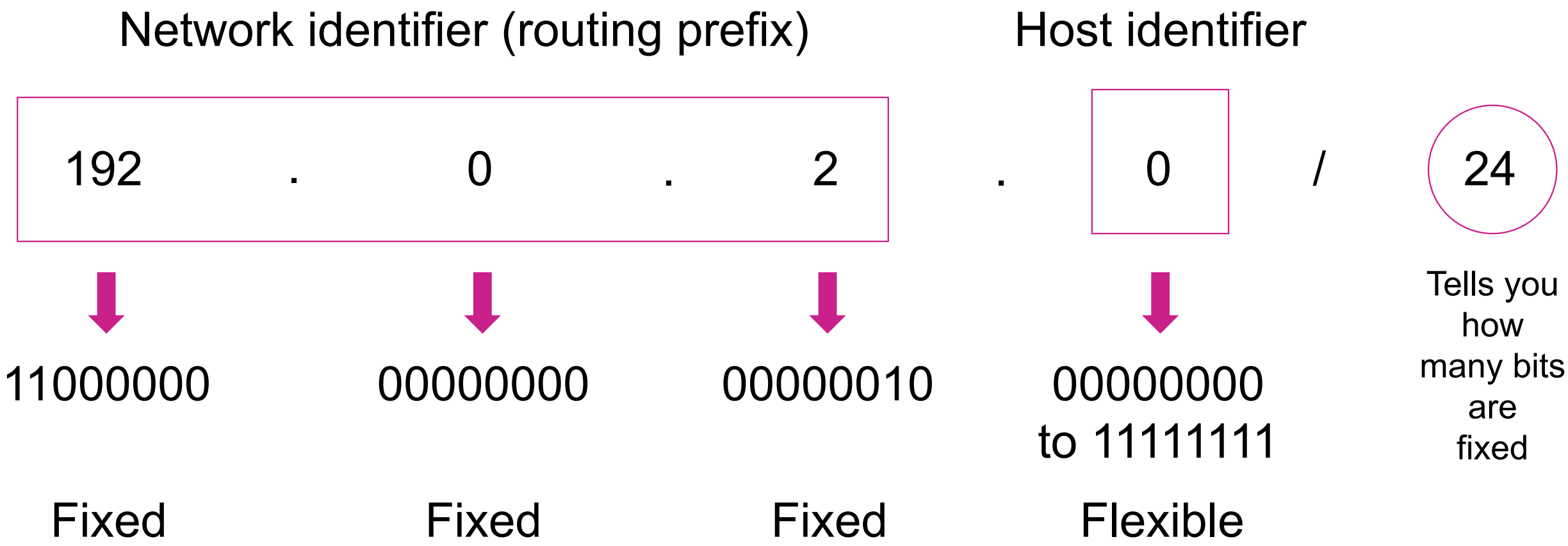
Network Bits	Processor Bits
The IPv4 address is a 32-bit number that uniquely identifies a network interface on a machine. An IPv4 address is typically written in decimal digits, formatted as four 8-bit fields that are separated by periods. Each 8-bit field represents a byte of the IPv4 address.	What is a 64-bit processor (64-bit computing) A 64-bit processor refers to a microprocessor that can process data and instructions in chunks of 64 bits. Microprocessors that can handle 64 bits perform a larger number of calculations per second compared to 32-bit processors.





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Classless Inter-Domain Routing (CIDR)

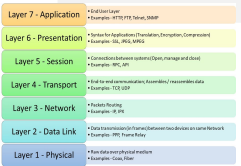


- Fixed IP addresses, in which every bit is fixed, represent a single IP address (for example, *192.0.2.0/32*). This type of address is helpful when you want to set up a firewall rule and give access to a specific host. **0.0.0.0/0 = internet**
- **32 bits = /24 = 8 = 2^8 = 256 IP address, 32 bits = /28 = 4 = 2^4 = 16 Ip address, 32 bits = /16 = 16 = 2^16 = 65,536 Ip**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 2: Amazon VPC

Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC

Amazon VPC

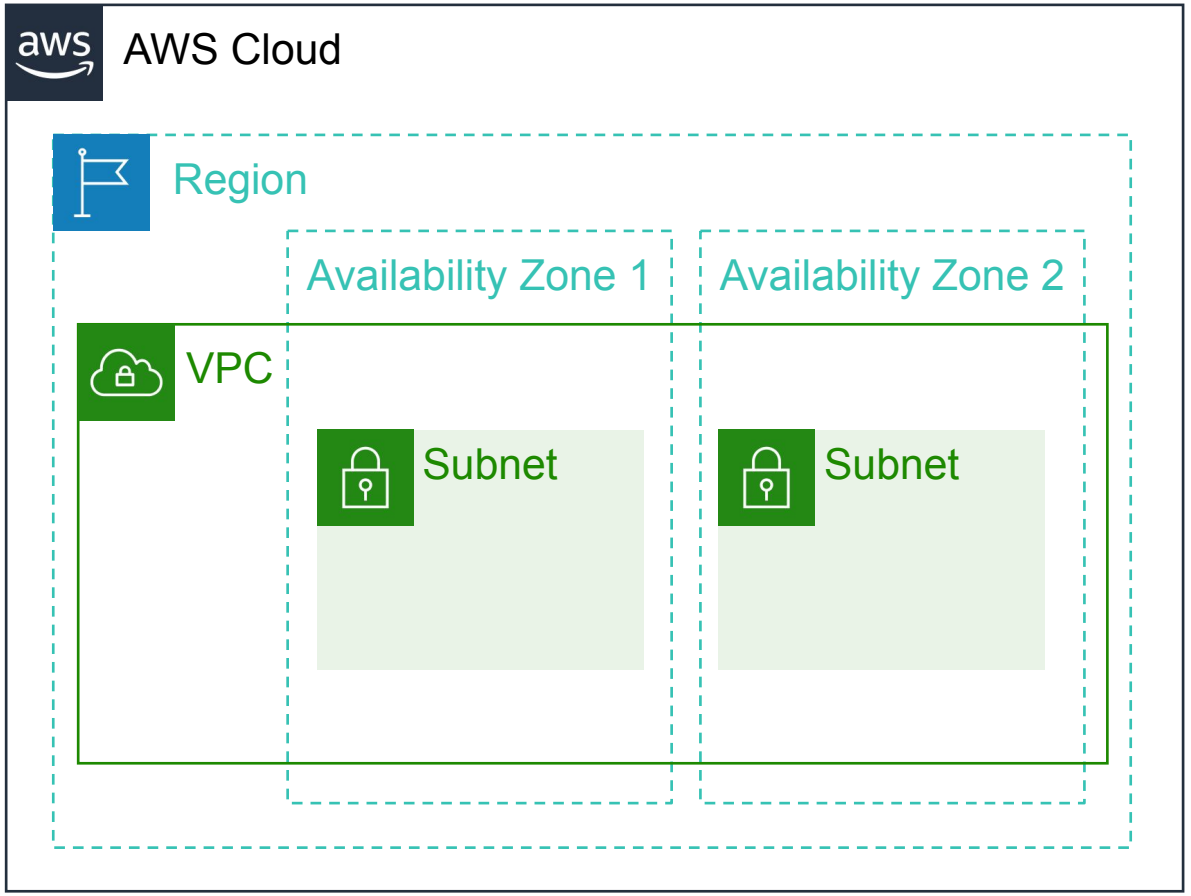
- Enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define
- Gives you control over your virtual networking resources, including:
  - Selection of IP address range
  - Creation of subnets
  - Configuration of route tables and network gateways
- Enables you to customize the network configuration for your VPC
- Enables you to use multiple layers of security

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPCs and subnets

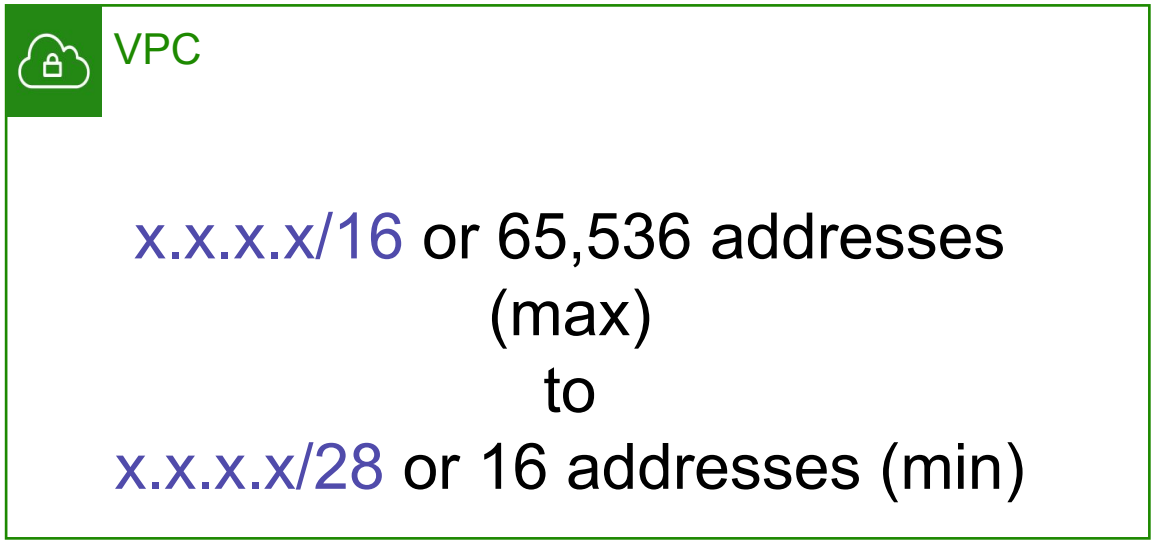
- VPCs:
  - Logically isolated from other VPCs
  - Dedicated to your AWS account
  - Belong to a single AWS Region and can span multiple Availability Zones
- Subnets:
  - Range of IP addresses that divide a VPC
  - Belong to a single Availability Zone
  - Classified as public or private



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.



192.2.0.0/16

192.2.1.0/16

32 bits = /24 = 8 = 2^8 = 256 Ip address are available

32 bits = /28 = 4 = 2^4 = 16 Ip address are available

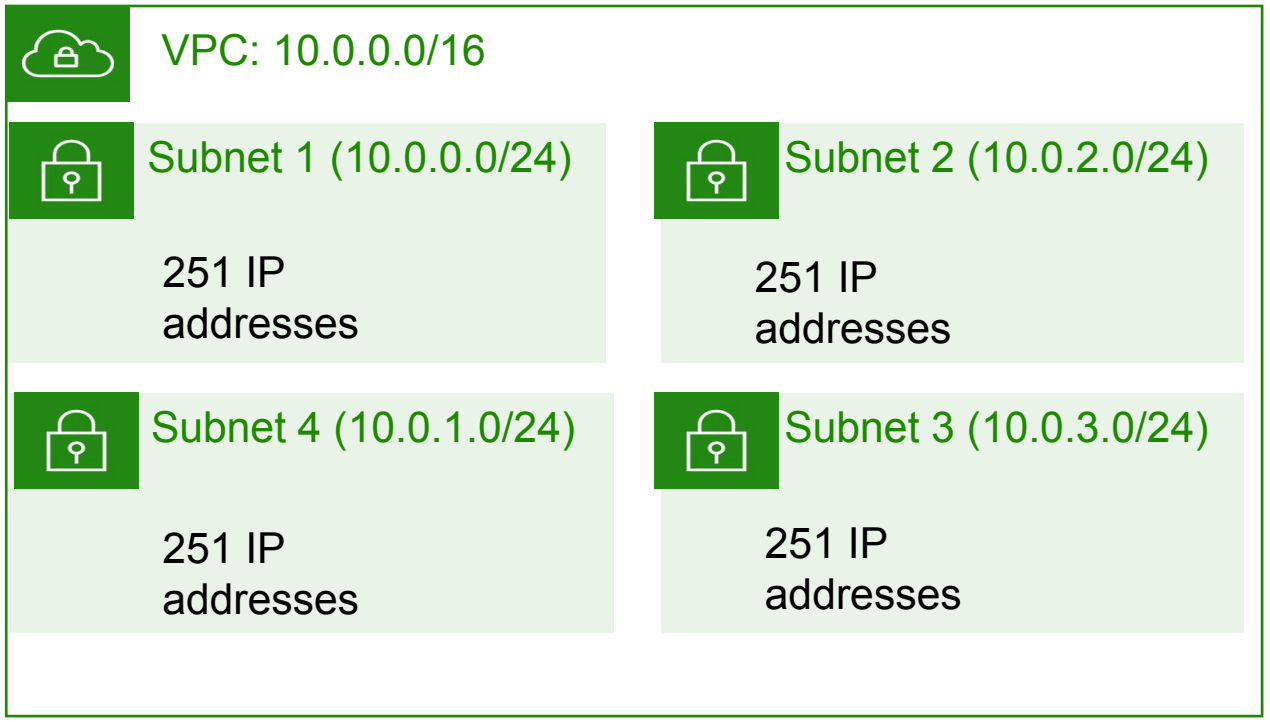
32 bits = /16 = 16 = 2^16 = 65,536 Ip addresses are available

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reserved IP addresses

65536 - 251 * 4 = 1004 = 64531 Ip address still available

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

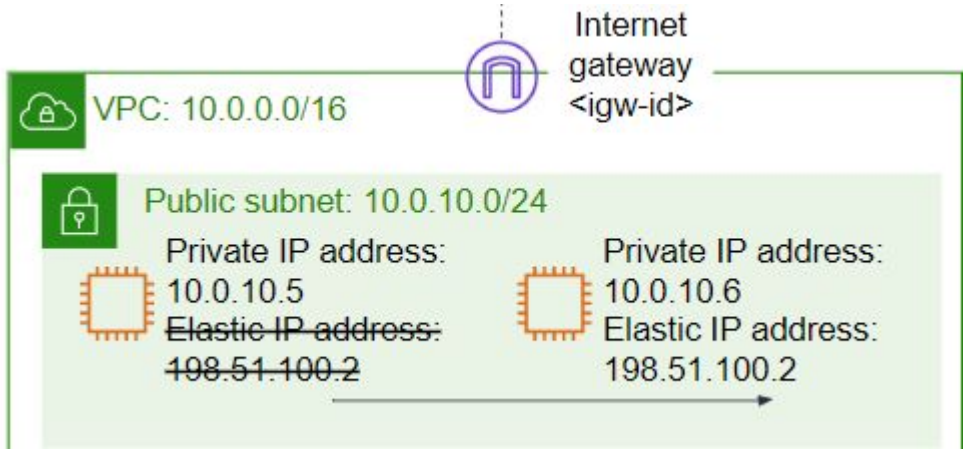
Public IP address types

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

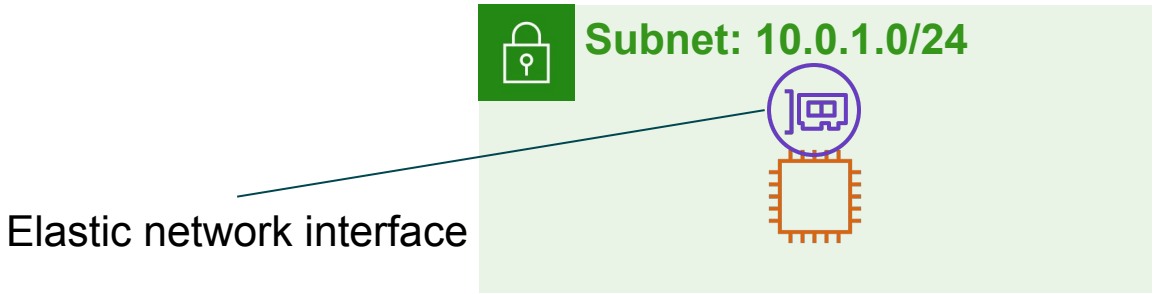
- Associated with an AWS account
- Can be allocated and remapped anytime
- Additional costs might apply



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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). Also a route table can have multiple subnets

Main (Default) Route Table

Destination	Target
10.0.0.0/16	local

VPC CIDR block

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

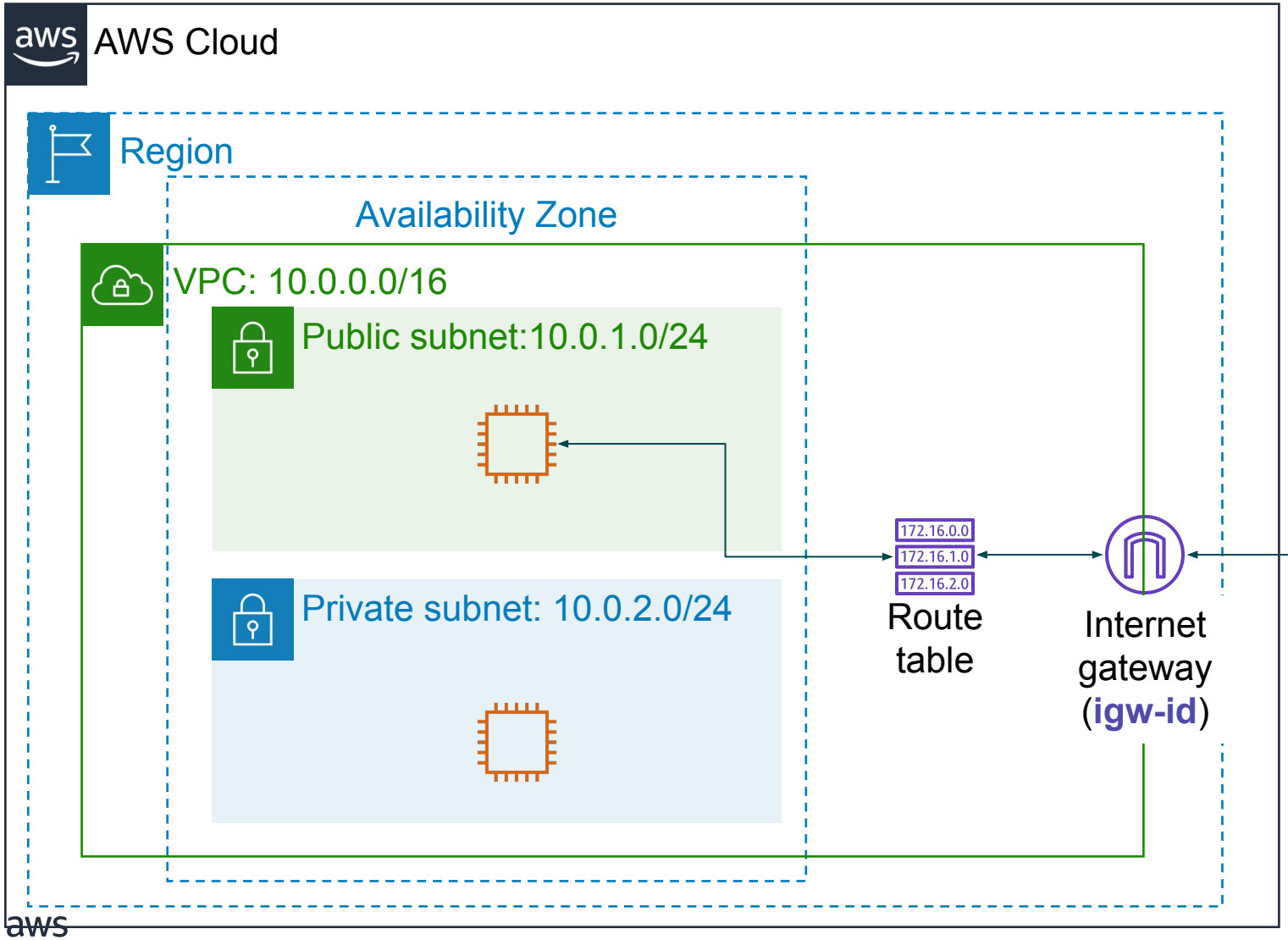
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 3: VPC networking

Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Internet gateway

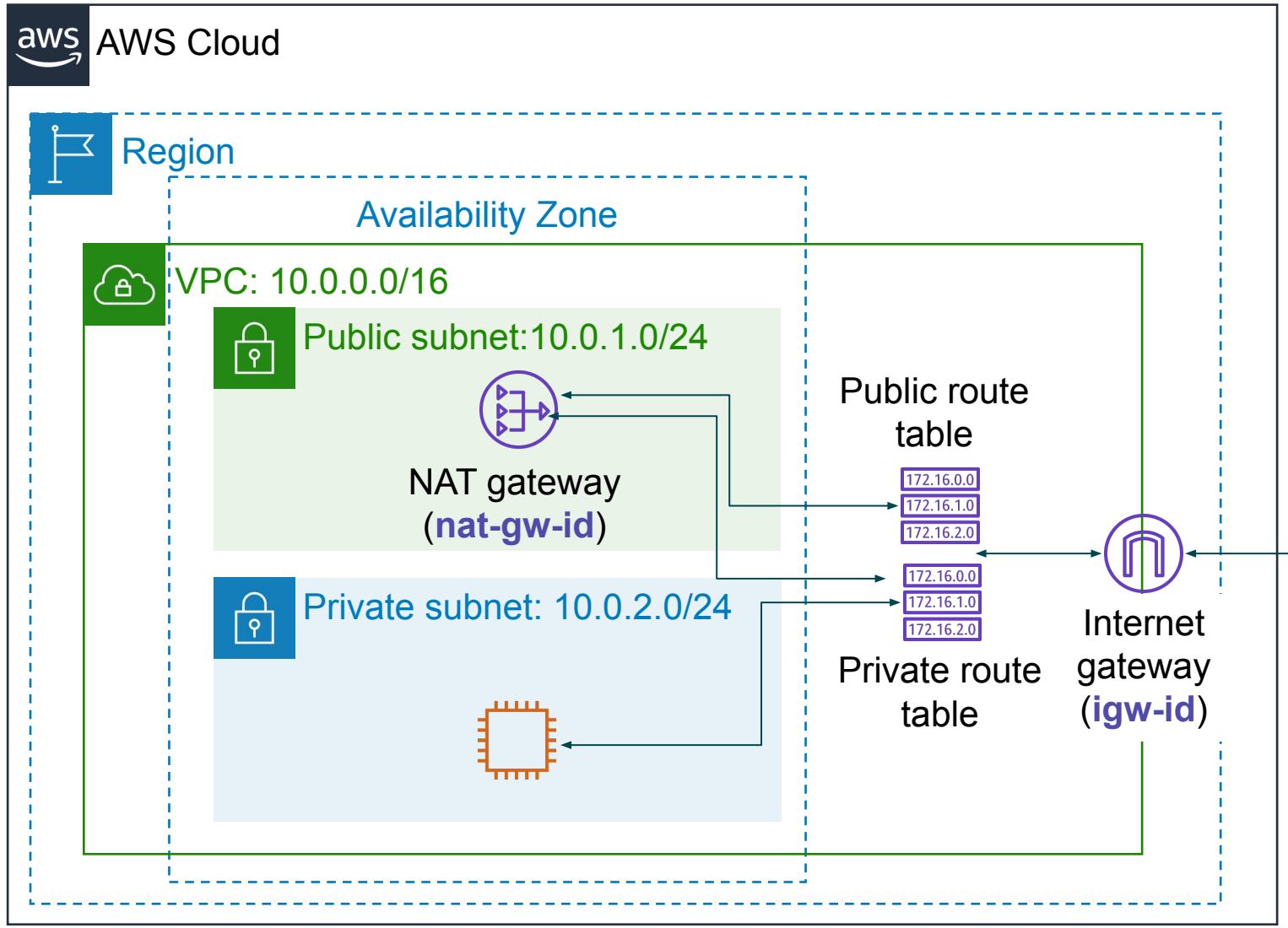


Public Subnet Route Table

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network address translation (NAT) gateway



Public Subnet Route Table

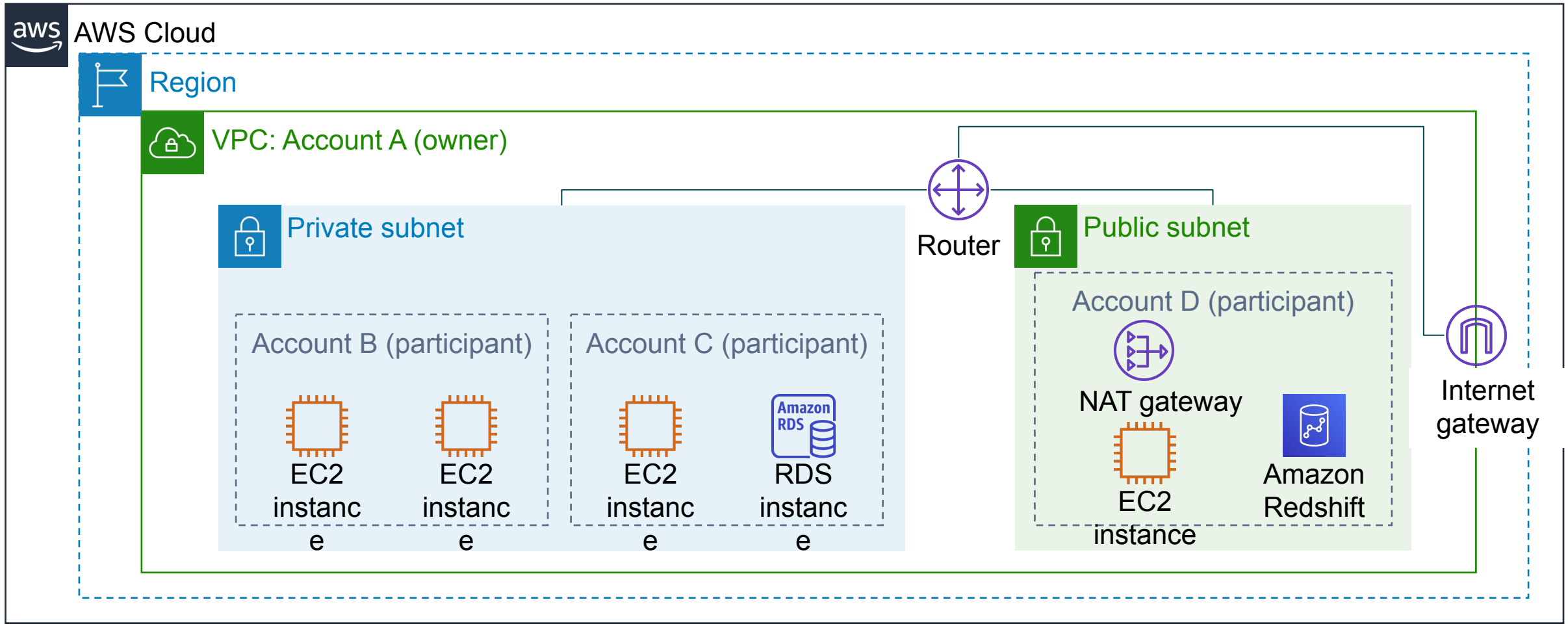
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private Subnet Route Table

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

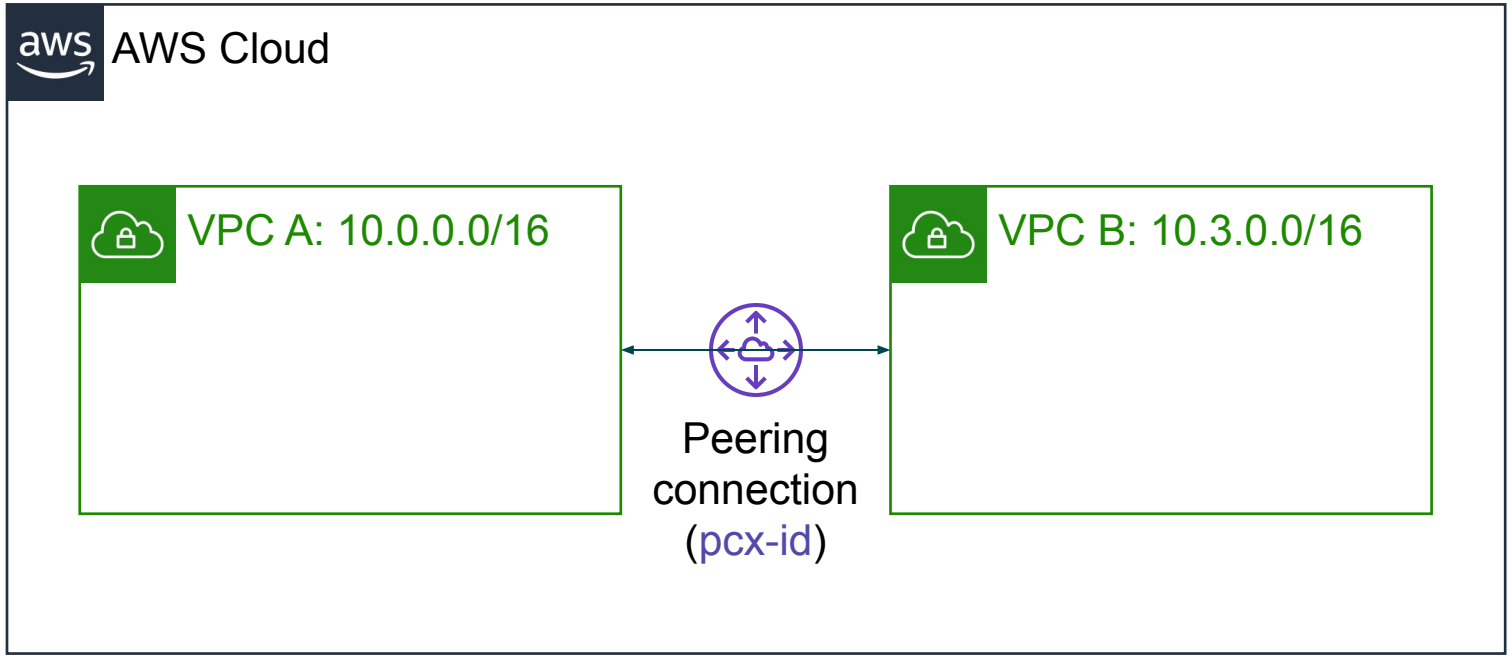
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC sharing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC peering



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

Restrictions:

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

Route Table for VPC A

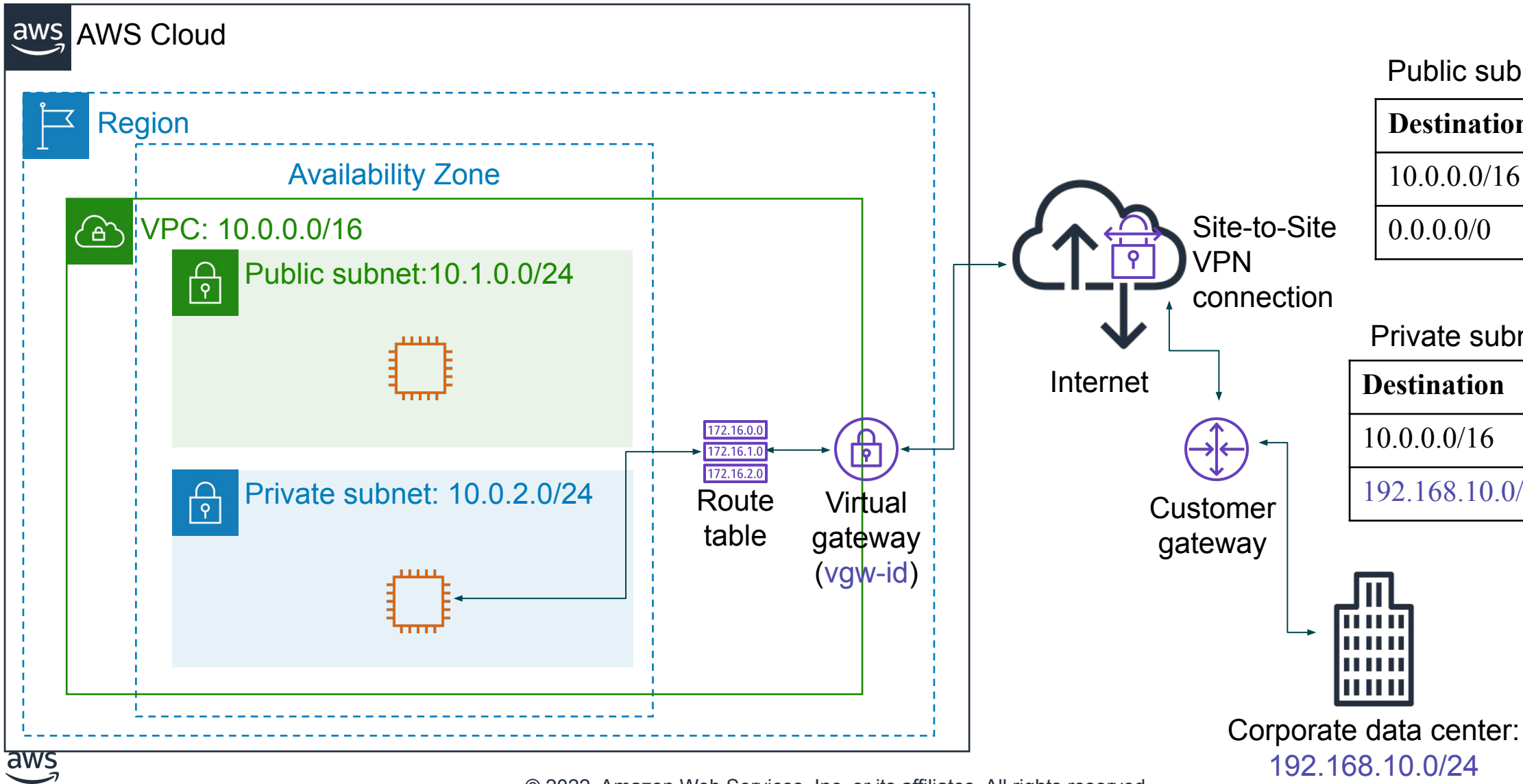
Destination	Target
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Route Table for VPC B

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Site-to-Site VPN



Public subnet route table

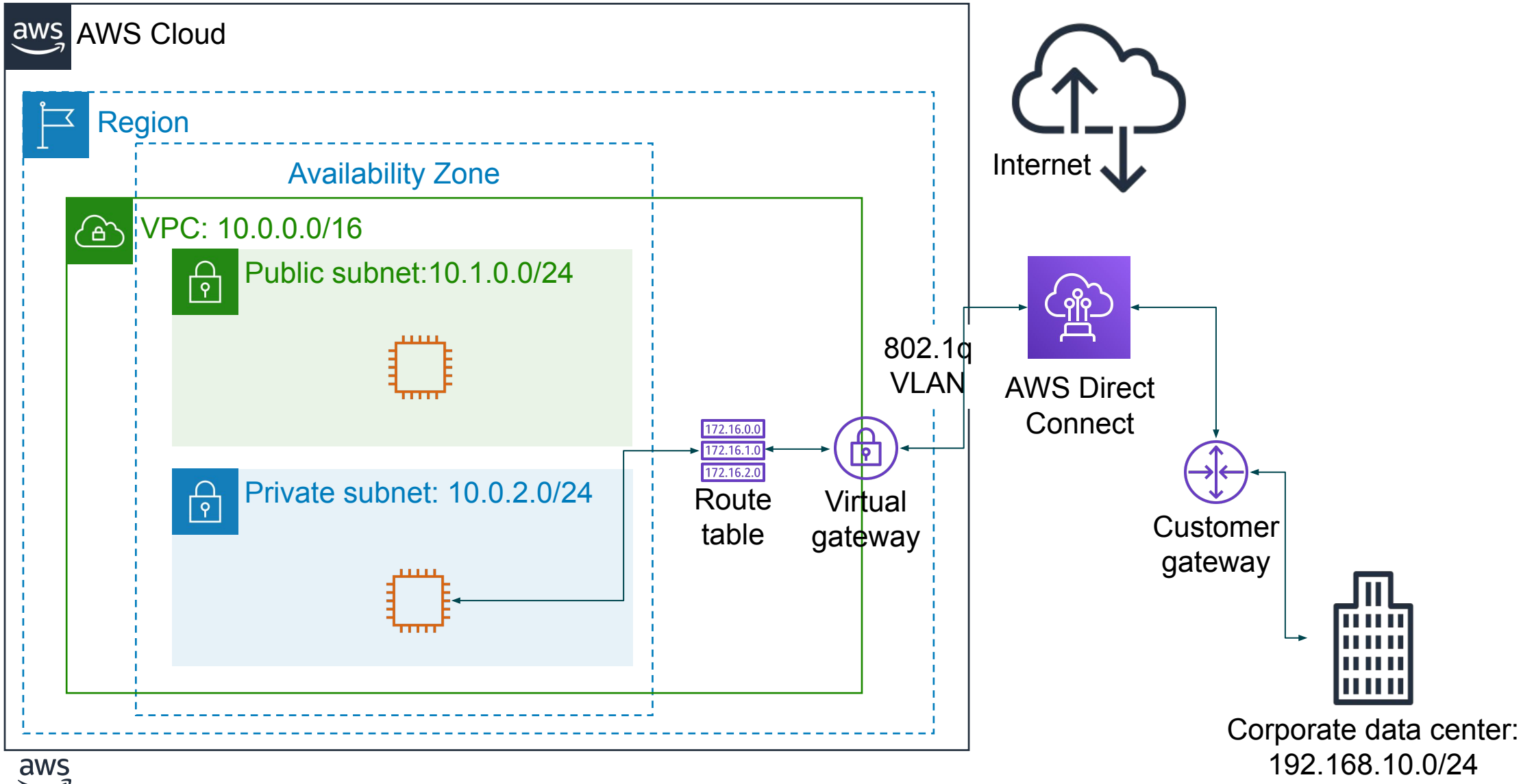
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private subnet route table

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

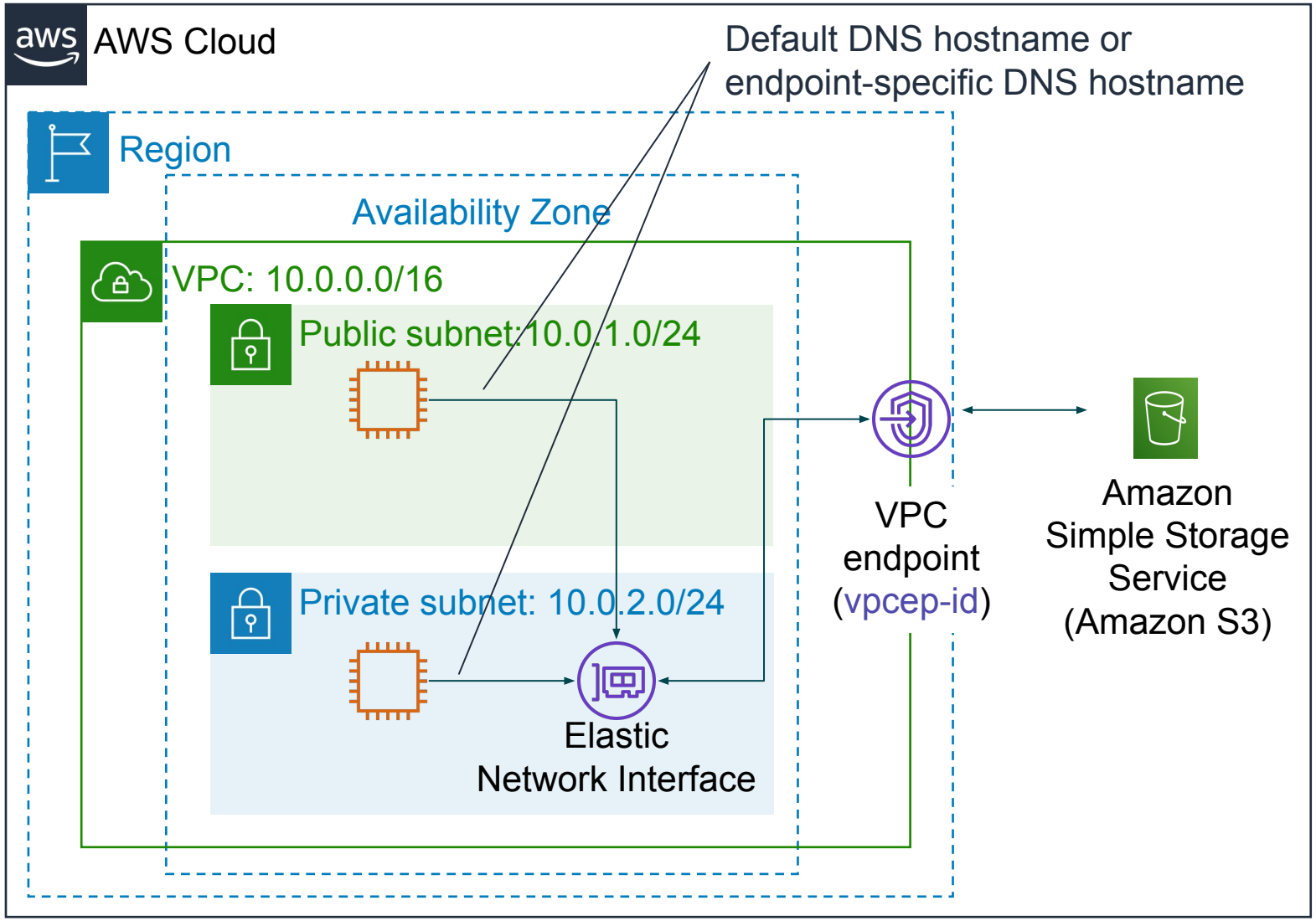
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Direct Connect



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

VPC endpoints



Public Subnet Route Table

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

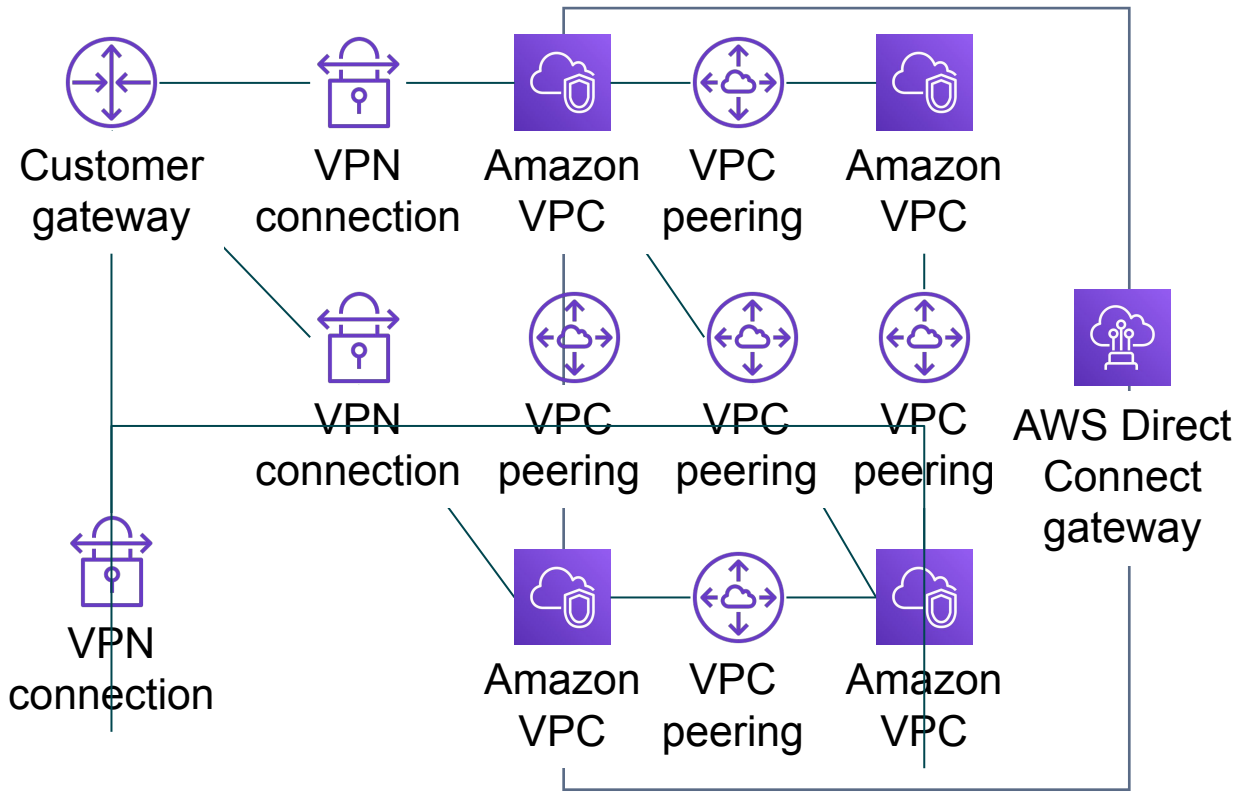
Two types of endpoints:

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

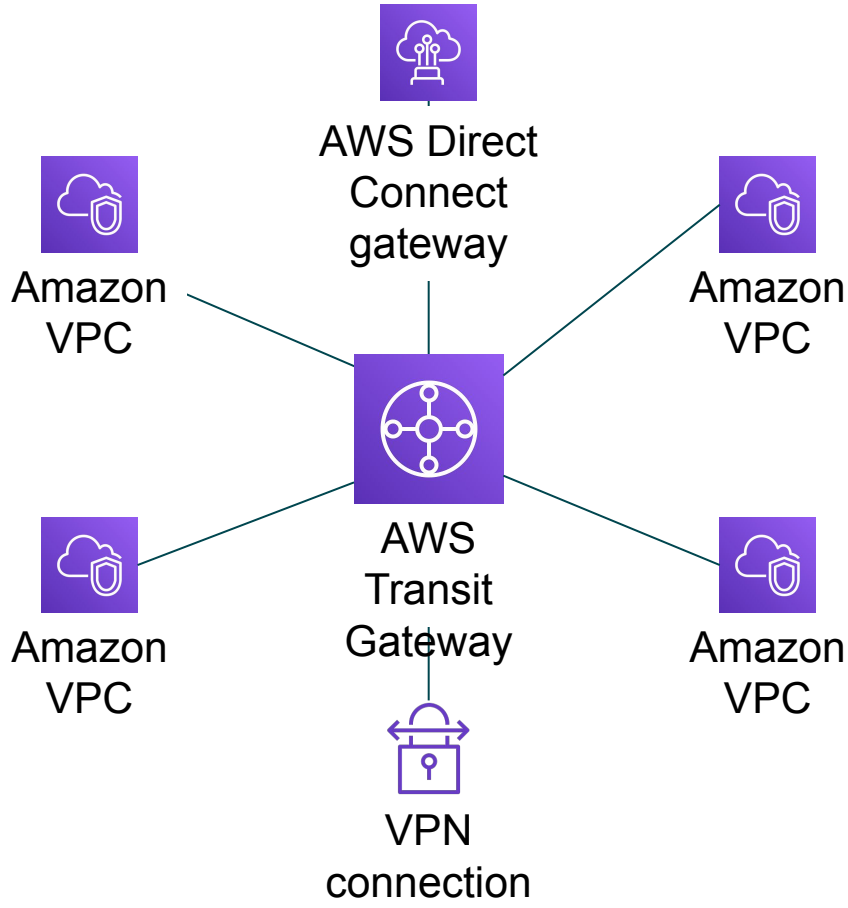
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Transit Gateway

From this…

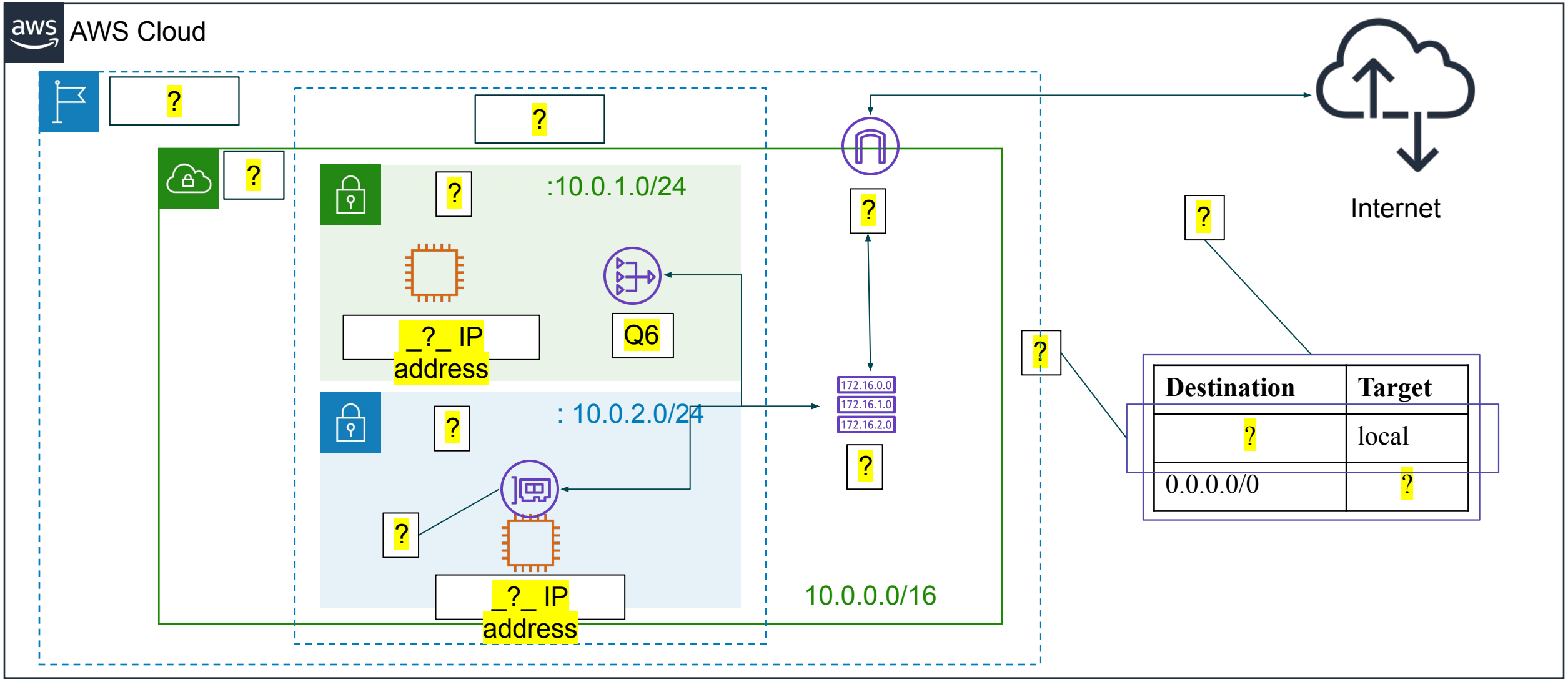


To this…



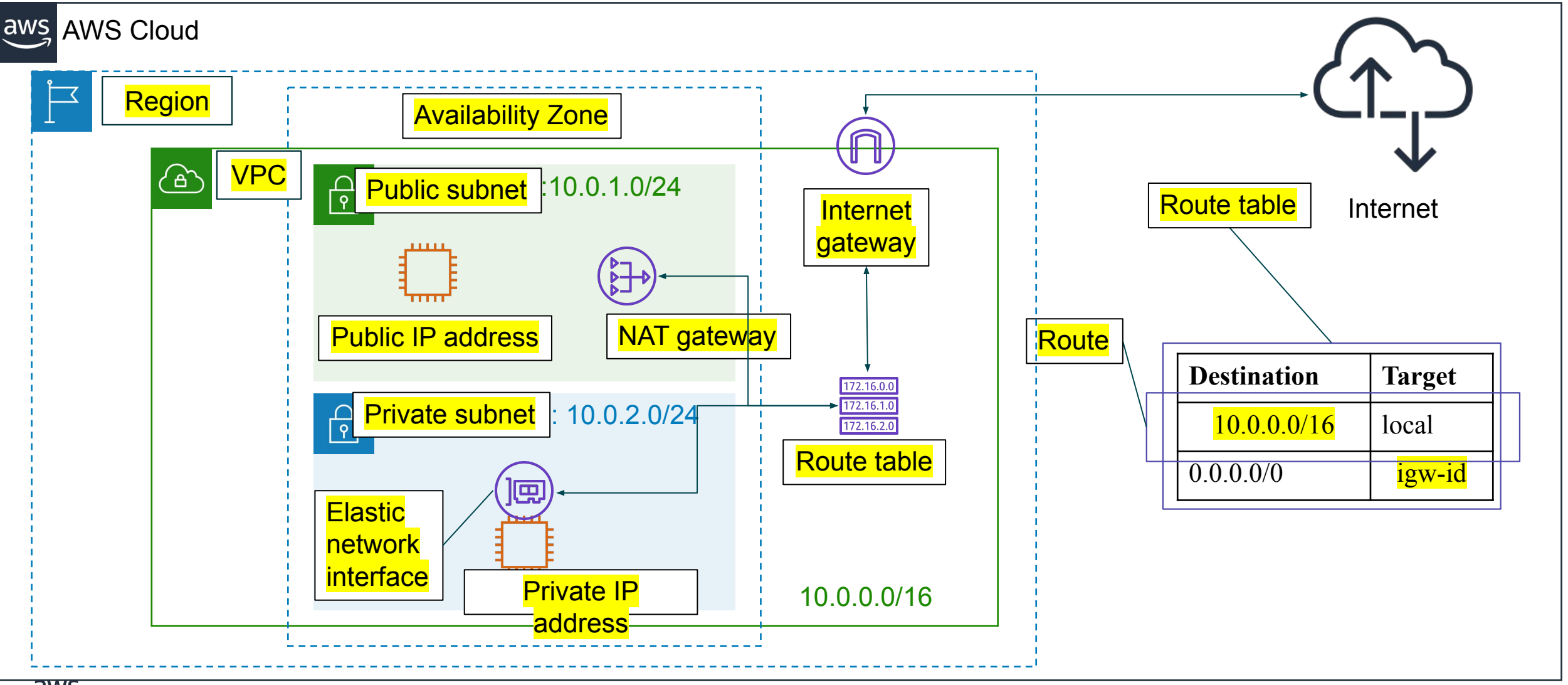
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Activity: Label this network diagram



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Activity: Solution



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

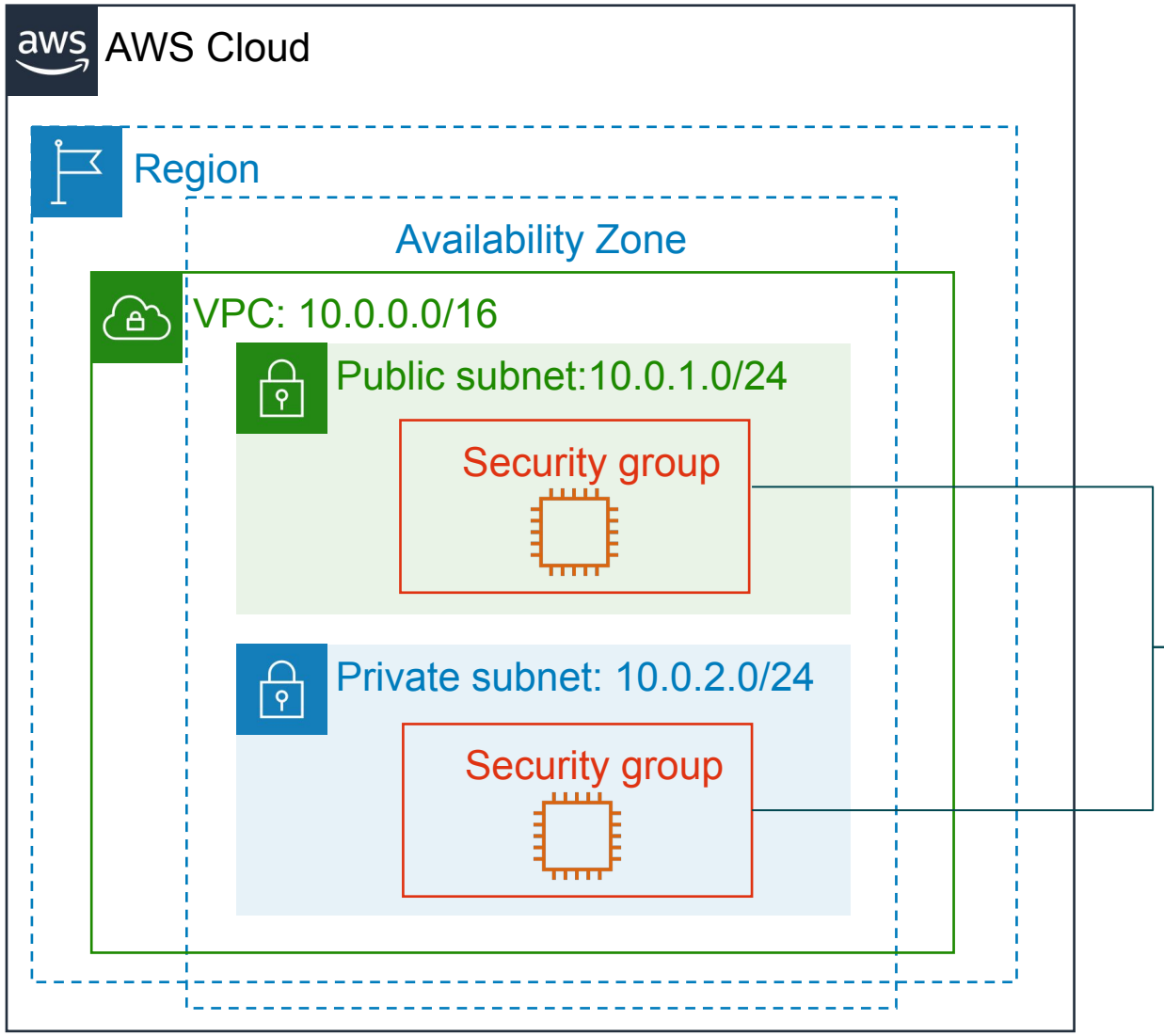
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 4: VPC security

Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security groups (1 of 2)



Security groups act at the instance level.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Custom security group examples

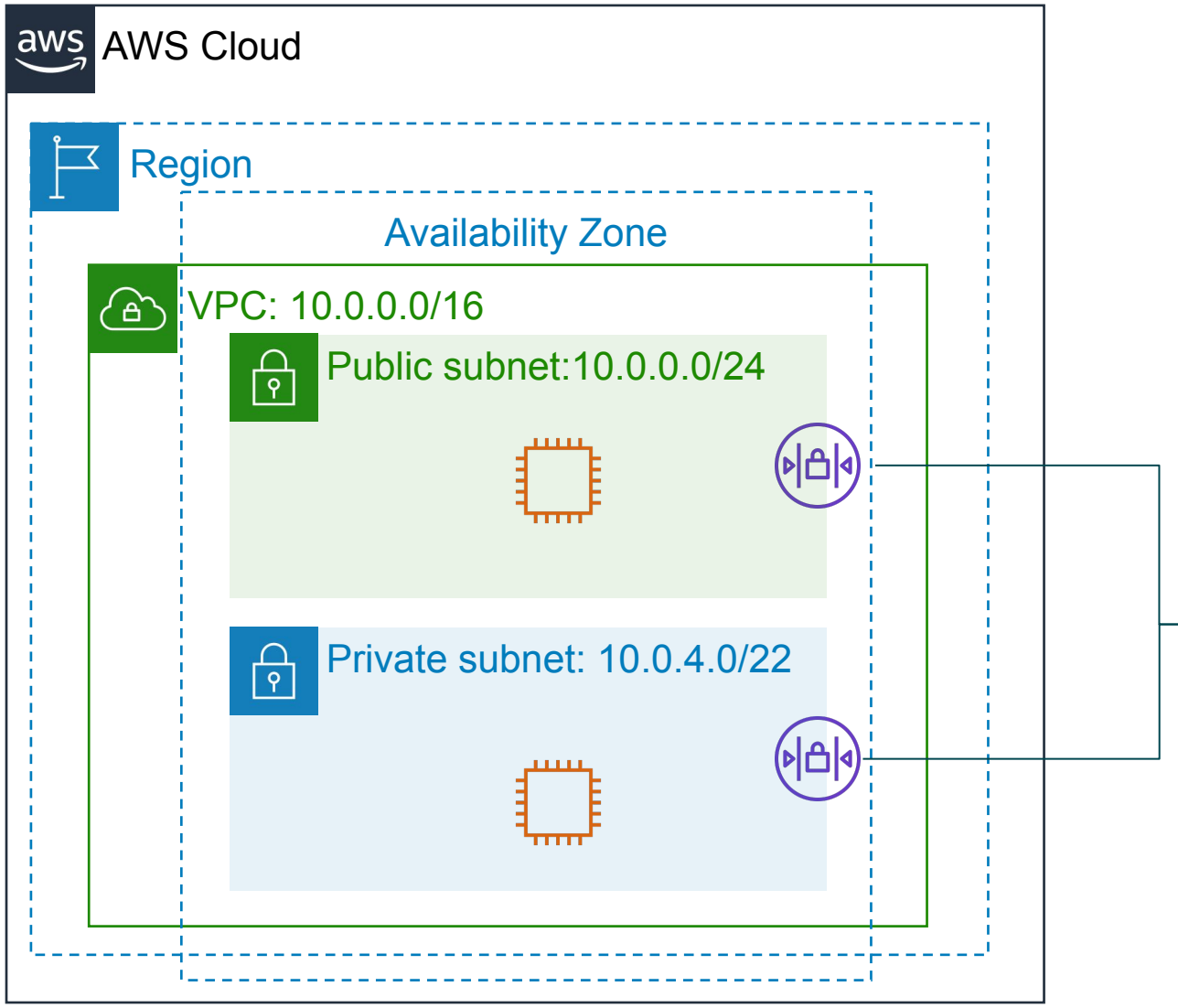
- You can **specify allow** rules, but not deny rules.
- **All rules are evaluated** before the decision to allow traffic.

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

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network access control lists (network ACLs 1 of 2)



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

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

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 4 key takeaways

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 5: Amazon Route 53

Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

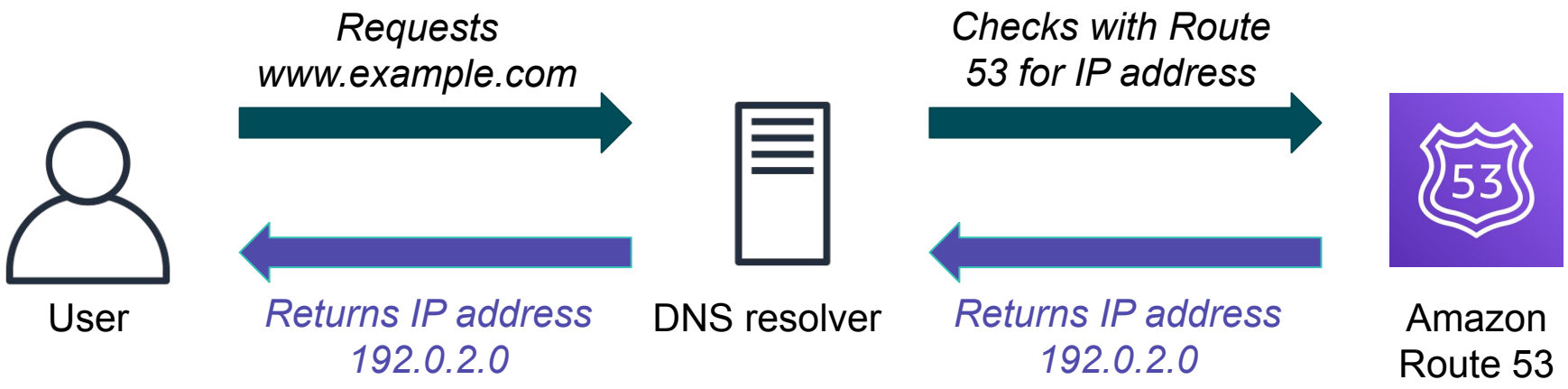
Amazon Route 53

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Route 53 DNS resolution



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

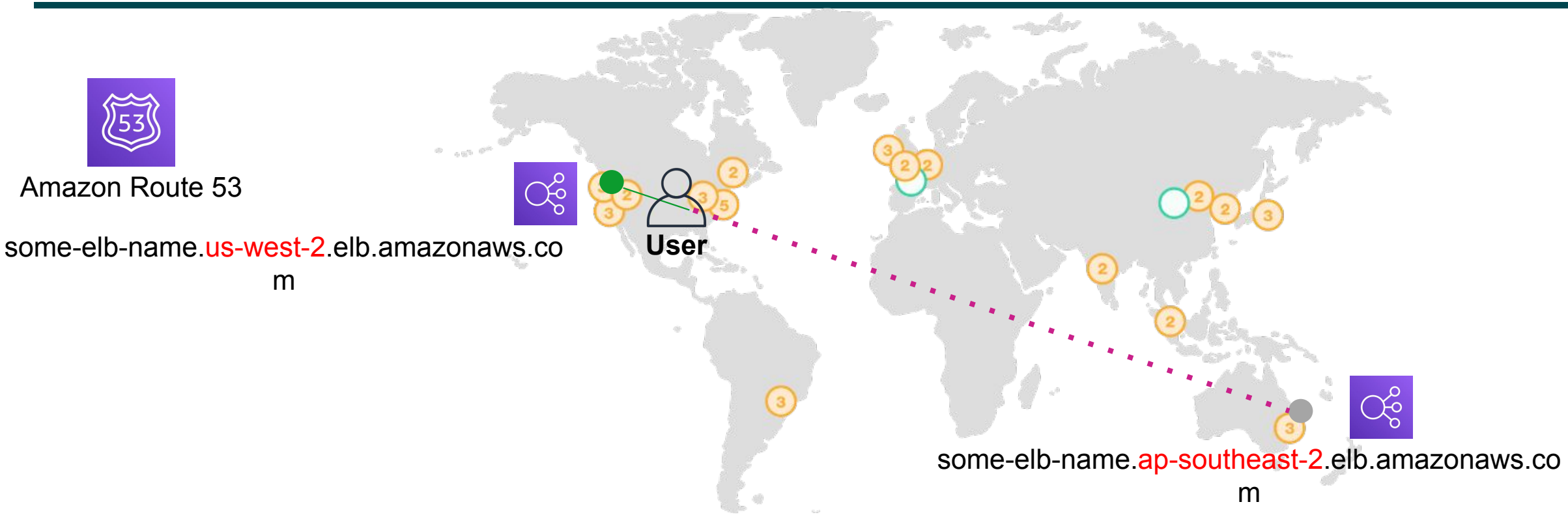
Amazon Route 53 supported routing

- 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

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use case: Multi-region deployment



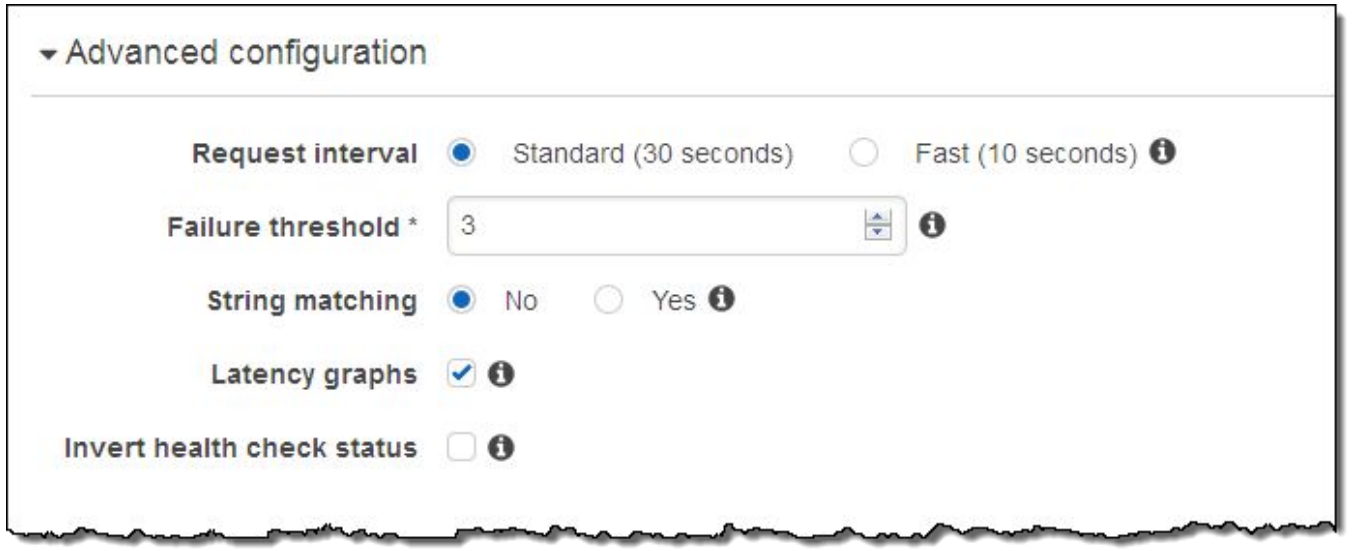
Name	Type	Value
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Route 53 DNS failover

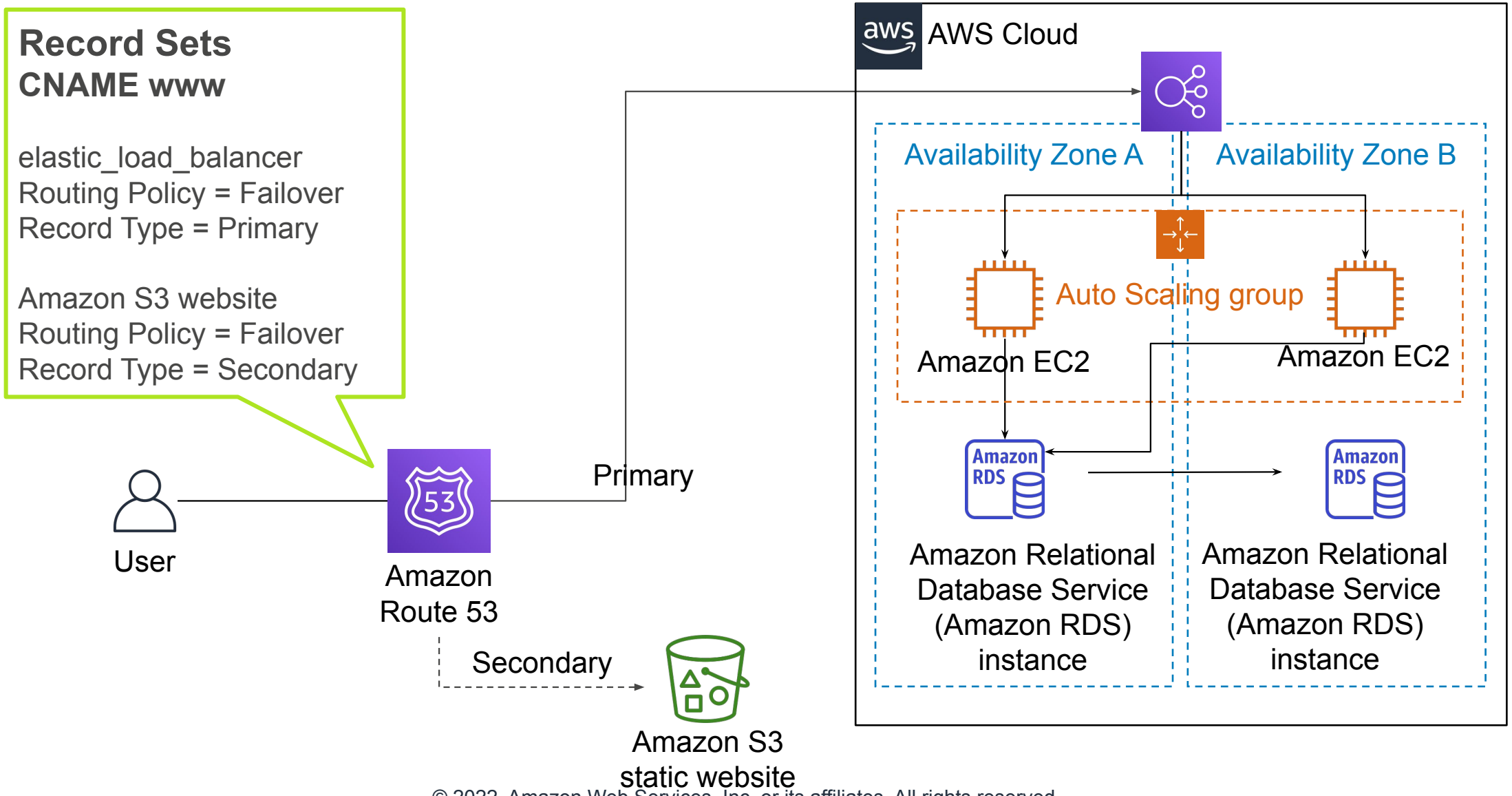
Improve the availability of your applications that run on AWS by:

- Configuring backup and failover scenarios for your own applications
- Enabling highly available multi-region architectures on AWS
- Creating health checks



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DNS failover for a multi-tiered web application



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 5 key takeaways

- Amazon Route 53 is a highly available and scalable cloud DNS web service that translates domain names into numeric IP addresses.
- Amazon Route 53 supports several types of routing policies.
- Multi-Region deployment improves your application's performance for a global audience.
- You can use Amazon Route 53 failover to improve the availability of your applications.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 6: Amazon CloudFront

Module 5: Networking and Content Delivery

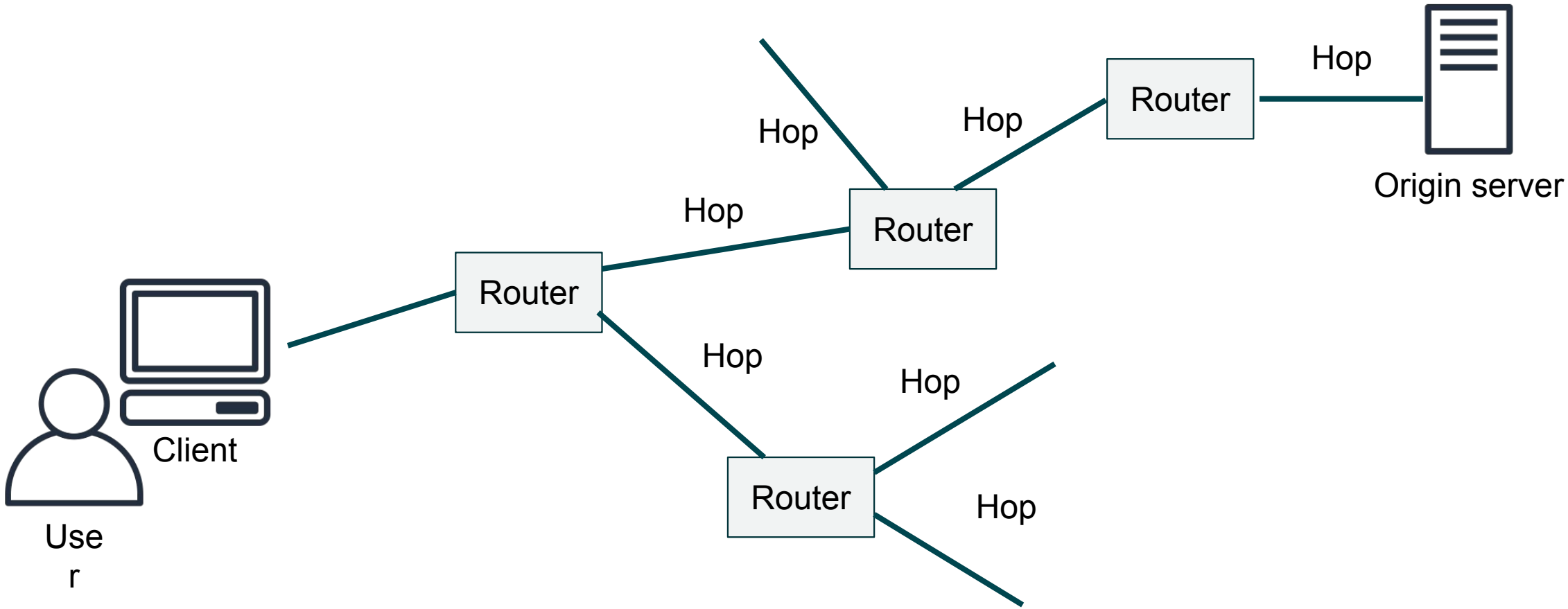
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Content delivery and network latency



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudFront

Amazon CloudFront

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

aws

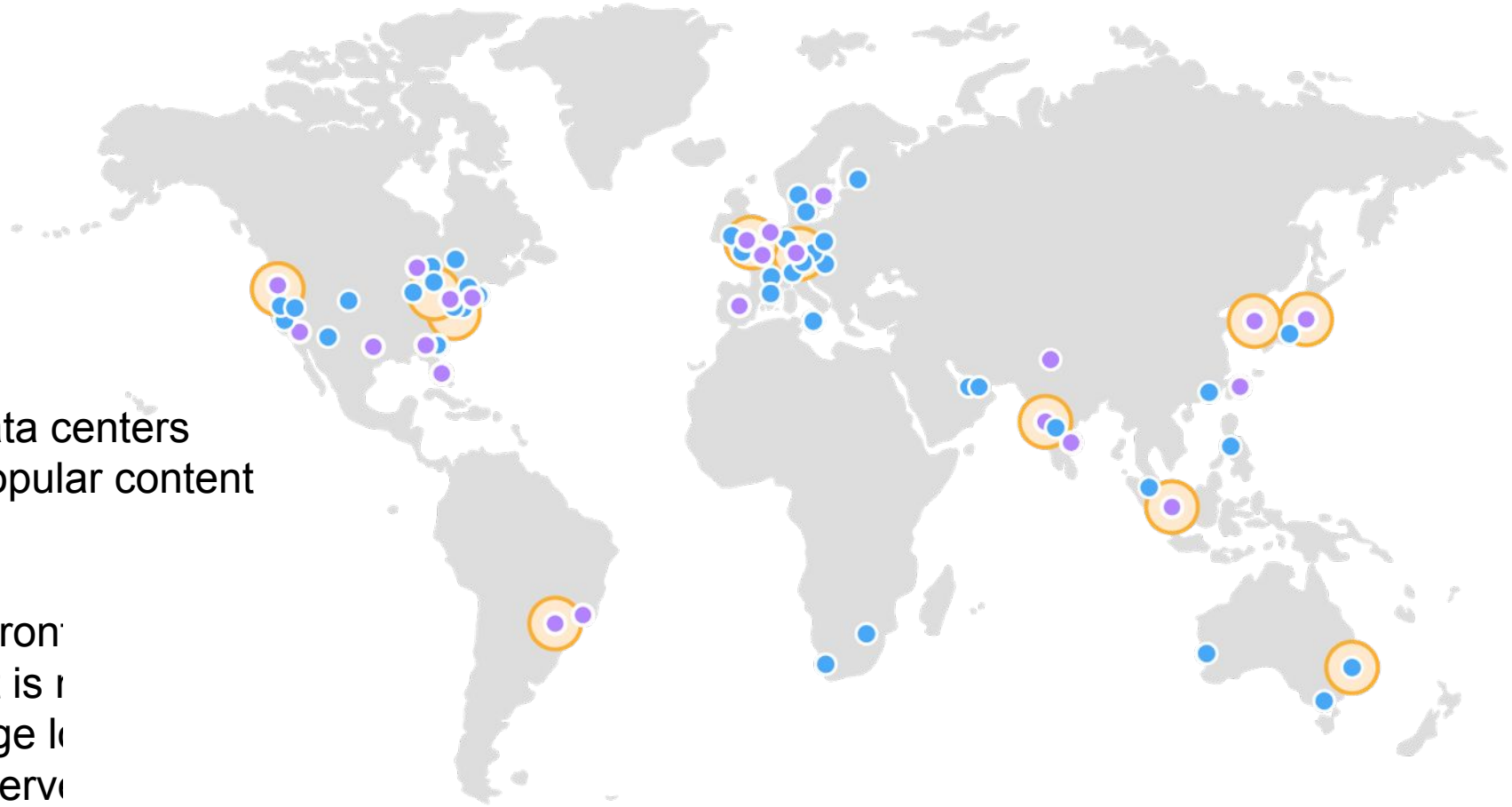
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudFront infrastructure

Edge locations

Multiple edge locations

Regional edge caches



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon CloudFront benefits

- Fast and global
- Security at the edge
- Highly programmable
- Deeply integrated with AWS
- Cost-effective

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Section 6 key takeaways

- A CDN is a globally distributed system of caching servers that accelerates delivery of content.
- Amazon CloudFront is a fast CDN service that securely delivers data, videos, applications, and APIs over a global infrastructure with low latency and high transfer speeds.
- Amazon CloudFront offers many benefits.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module wrap-up

Module 5: Networking and Content Delivery

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Module summary

In summary, in this module you learned how to:

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Complete the knowledge check

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample exam question

Which AWS networking service enables a company to create a virtual network within AWS?

Choice	Response
A	AWS Config
B	Amazon Route 53
C	AWS Direct Connect
D	Amazon VPC

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sample exam question answer

Which AWS networking service enables a company to create a virtual network within AWS?

The correct answer is D.

The keywords in the question are “AWS networking service” and “create a virtual network”.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Additional resources

- Amazon VPC Overview pag: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Amazon Virtual Private Cloud Connectivity Options whitepaper: https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/introduction.html
- One to Many: Evolving VPC Design AWS Architecture blog post: https://aws.amazon.com/blogs/architecture/one-to-many-evolving-vpc-design/
- Amazon VPC User Guide: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Amazon CloudFront overview page: https://aws.amazon.com/cloudfront/?nc=sn&loc=1

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you

Corrections, feedback, or other questions?
Contact us at https://support.aws.amazon.com/#/contacts/aws-academy.
All trademarks are the property of their owners.

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.