CS 4037
Introduction to Cloud Computing
Lecture 25

Danyal Farhat

FAST School of Computing

NUCES Lahore

AWS Networking and Content Delivery

Lecture’s Agenda

- **Amazon Virtual Private Cloud**
- VPC Networking
- VPC Security
- Amazon Route 53 and CloudFront

Amazon Virtual Private Cloud

- “Enables to provision a logically isolated section of the AWS Cloud where user can launch resources in a virtual network.”

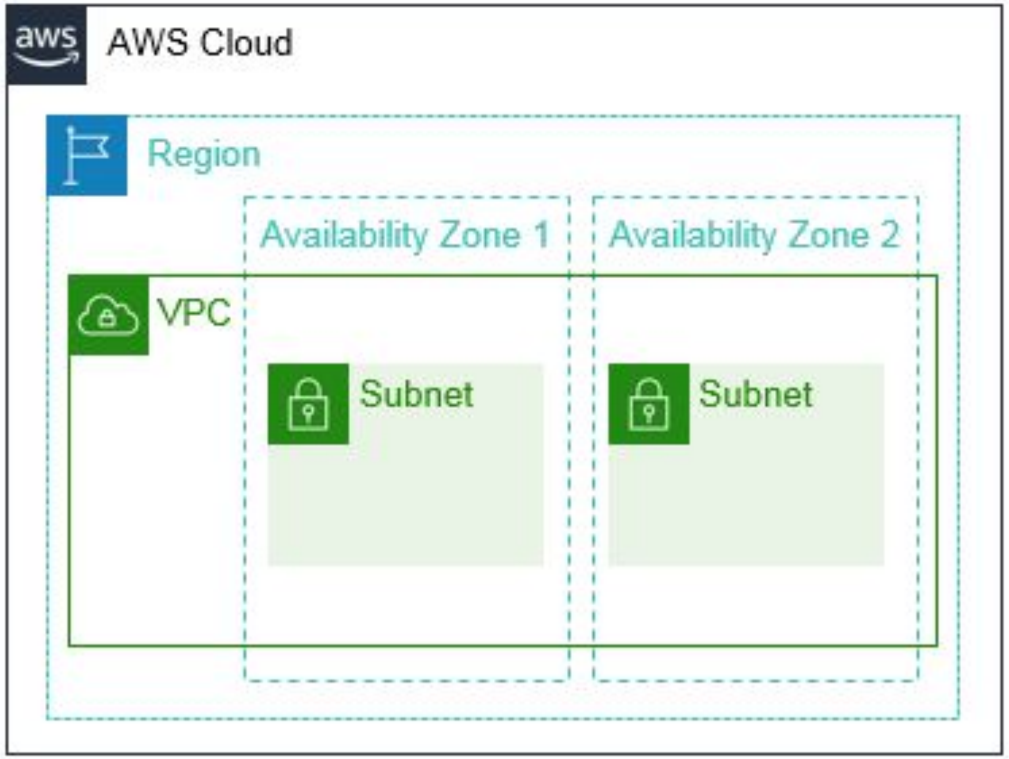
Amazon VPC

- Gives control over virtual networking resources, including:
  - Selection of IP address range
  - Creation of subnets
  - Configuration of route tables and network gateways
- Enables to use multiple layers of security
  - Instance level (Security Group) and Subnet level (Access Control List)

Virtual Private Cloud and Subnets

Virtual Private Cloud:

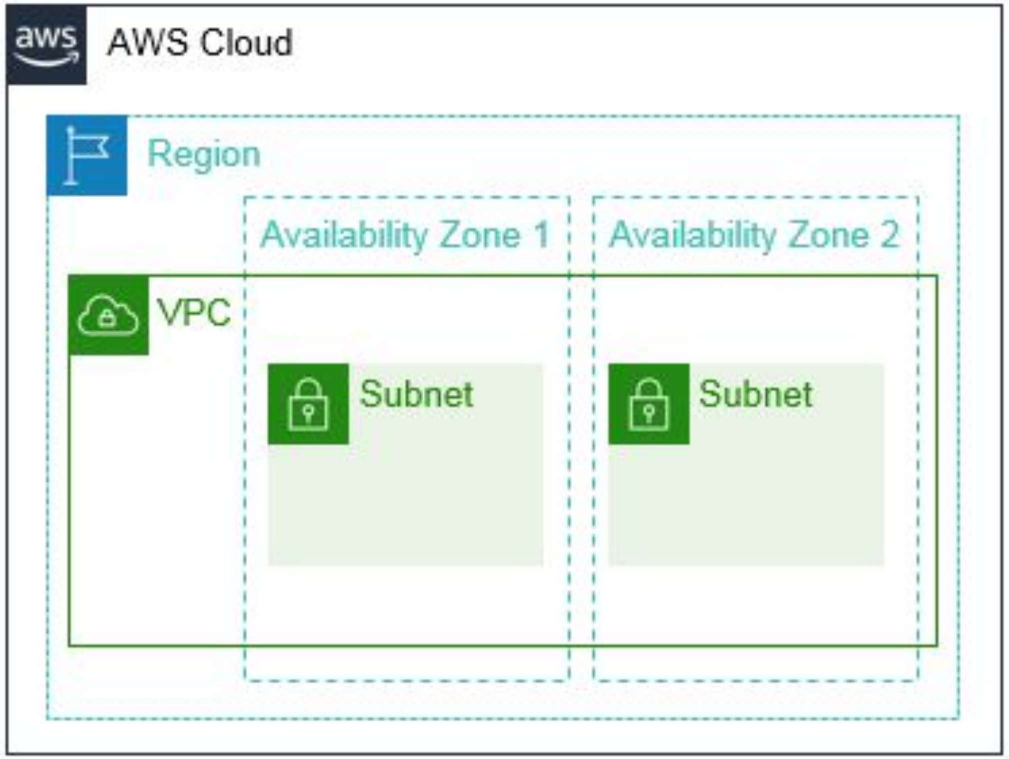
- Logically **isolated** from other VPCs
- **Dedicated** to user's AWS account
- Belong to a **single AWS Region** and can span multiple Availability Zones



Virtual Private Cloud and Subnet (Cont.)

Subnet:

- Range of IP addresses that divide a VPC
- Belong to a single Availability Zone
- Classified as public or private
  - Public subnets have direct access to the internet, but private subnets do not.

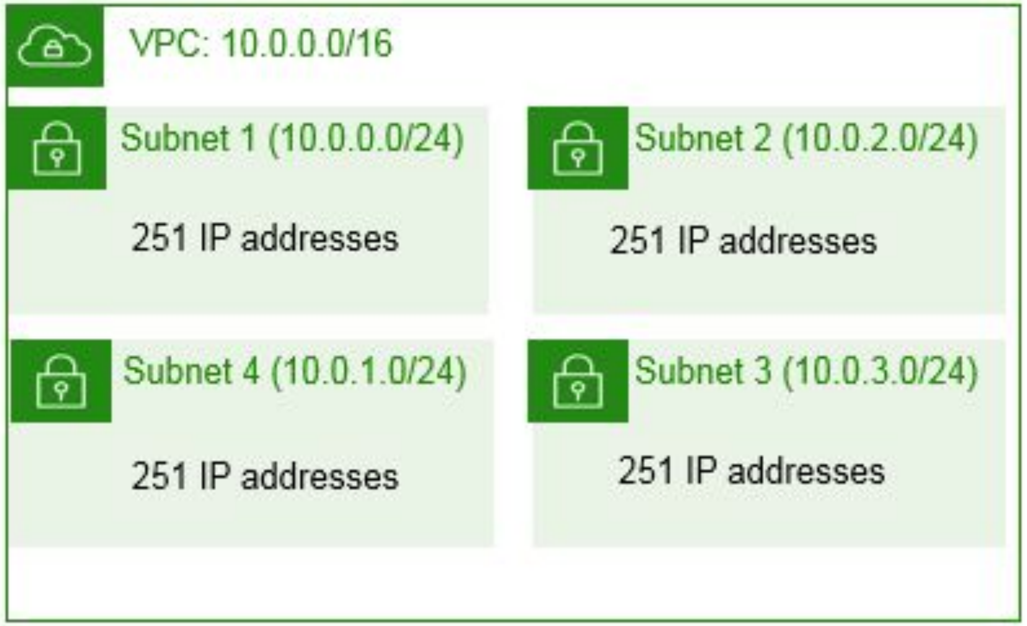


IP Addressing

- When customer creates a VPC, he/she assign it to an IPv4 CIDR block (range of private IPv4 addresses)
- Address range cannot be changed after the creation of VPC
  - The largest IPv4 CIDR block size is /16 (65,536 addresses)
  - The smallest IPv4 CIDR block size is /28 (16 addresses)
- IPv6 is also supported with a different block size limit
- CIDR blocks of subnets cannot overlap
- Duplicate IP addresses in the same VPC are not allowed

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 because five IPs are reserved.



VPC: 10.0.0.0/16

Subnet 1 (10.0.0.0/24)

251 IP addresses

Subnet 2 (10.0.2.0/24)

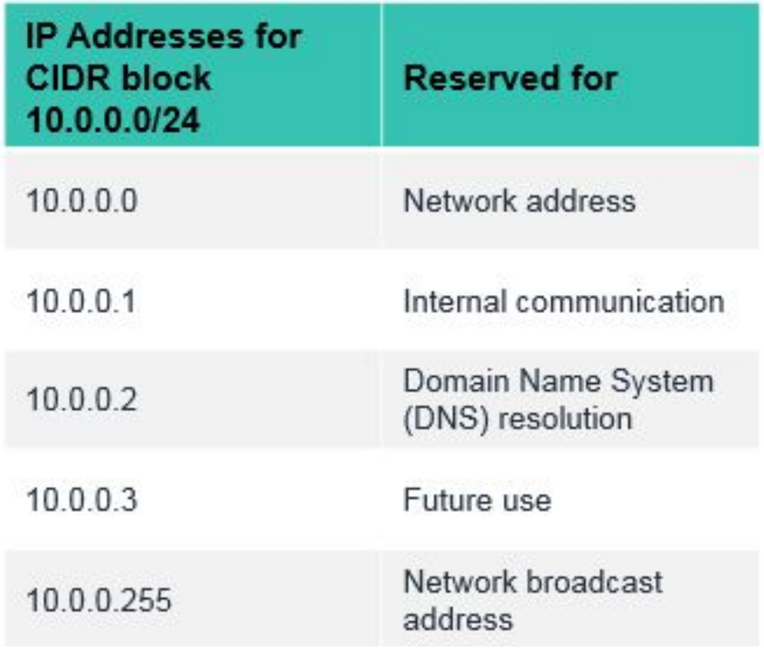
251 IP addresses

Subnet 4 (10.0.1.0/24)

251 IP addresses

Subnet 3 (10.0.3.0/24)

251 IP addresses



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 Assignment Types

Manually Assigned:

- Manually assigned through an Elastic IP address

Automatically Assigned:

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

- When you create a VPC, every instance in that VPC gets a private IP address automatically

Elastic IP Address

- Static public IPV4 address

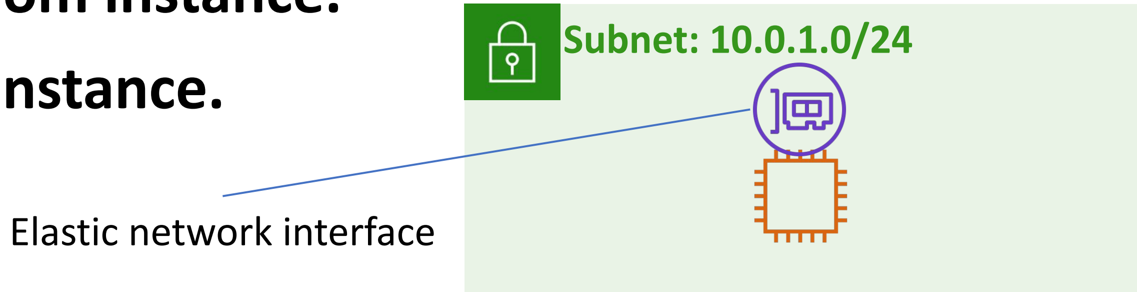
- Associated with an AWS account
  - □ Independent resource in the AWS account

- Can be allocated and remapped anytime

- Additional cost do apply

Elastic Network Interface

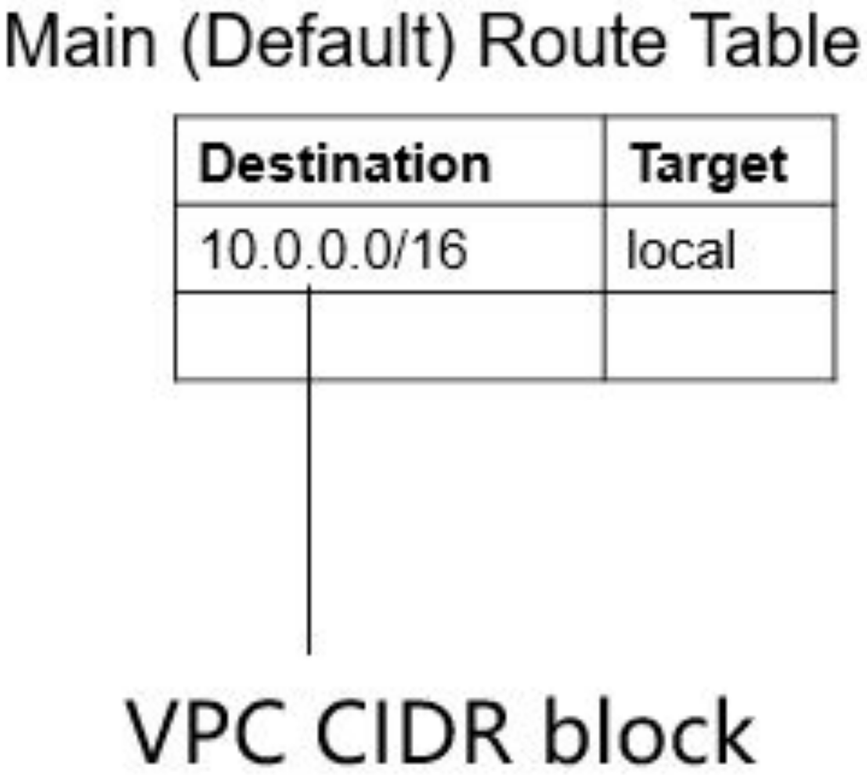
- An elastic network interface is a virtual network interface that can be:
  - Attach to an instance
  - Detach from the instance, and attach to another instance to redirect network traffic
- Its attributes follow when it is reattached to a new instance
- Each instance in VPC has a default (primary) network interface that is assigned a private IPv4 address from the IPv4 address range of the VPC
- User cannot detach primary NIC from instance.
- User can attach additional NIC to instance.



Route Table

- A route table contains a set of rules that user can configure to direct network traffic from the subnet

- Each route specifies a destination and a target
  - Destination is the CIDR block where user wants traffic from the subnet to go.
  - The target is the processing resource where the traffic is sent through.



Main (Default) Route Table

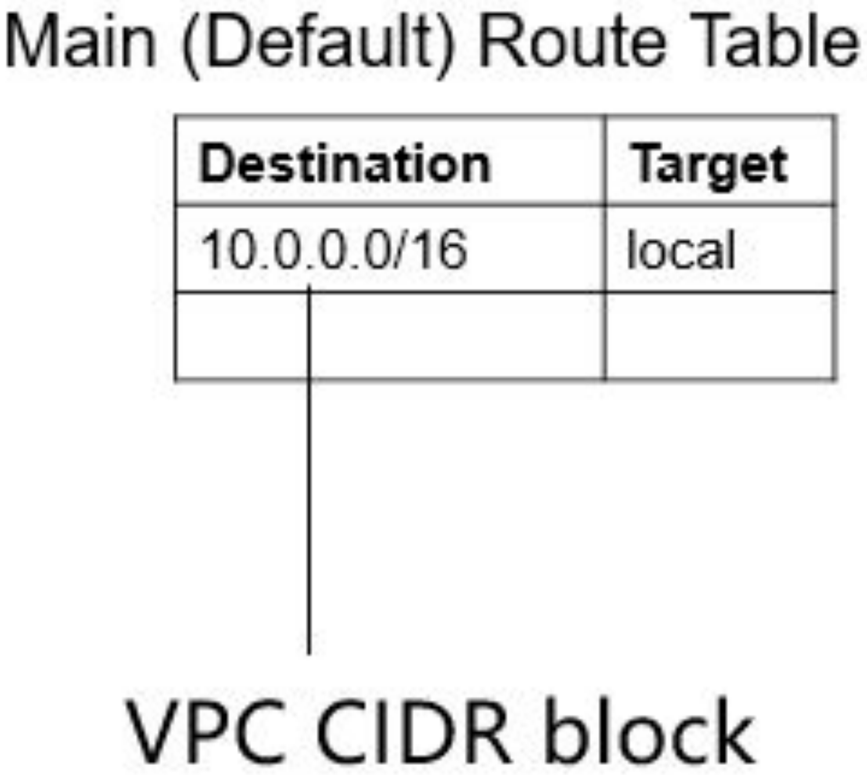
Destination	Target
10.0.0.0/16	local

VPC CIDR block

Route Table (Cont.)

- Every route table contains a local route for communication within VPC
  - User can customize route tables by adding routes
  - User cannot delete the local route entry that is used for internal communications

- Each subnet must be associated with a route table (at most one)



Main (Default) Route Table

Destination	Target
10.0.0.0/16	local

VPC CIDR block

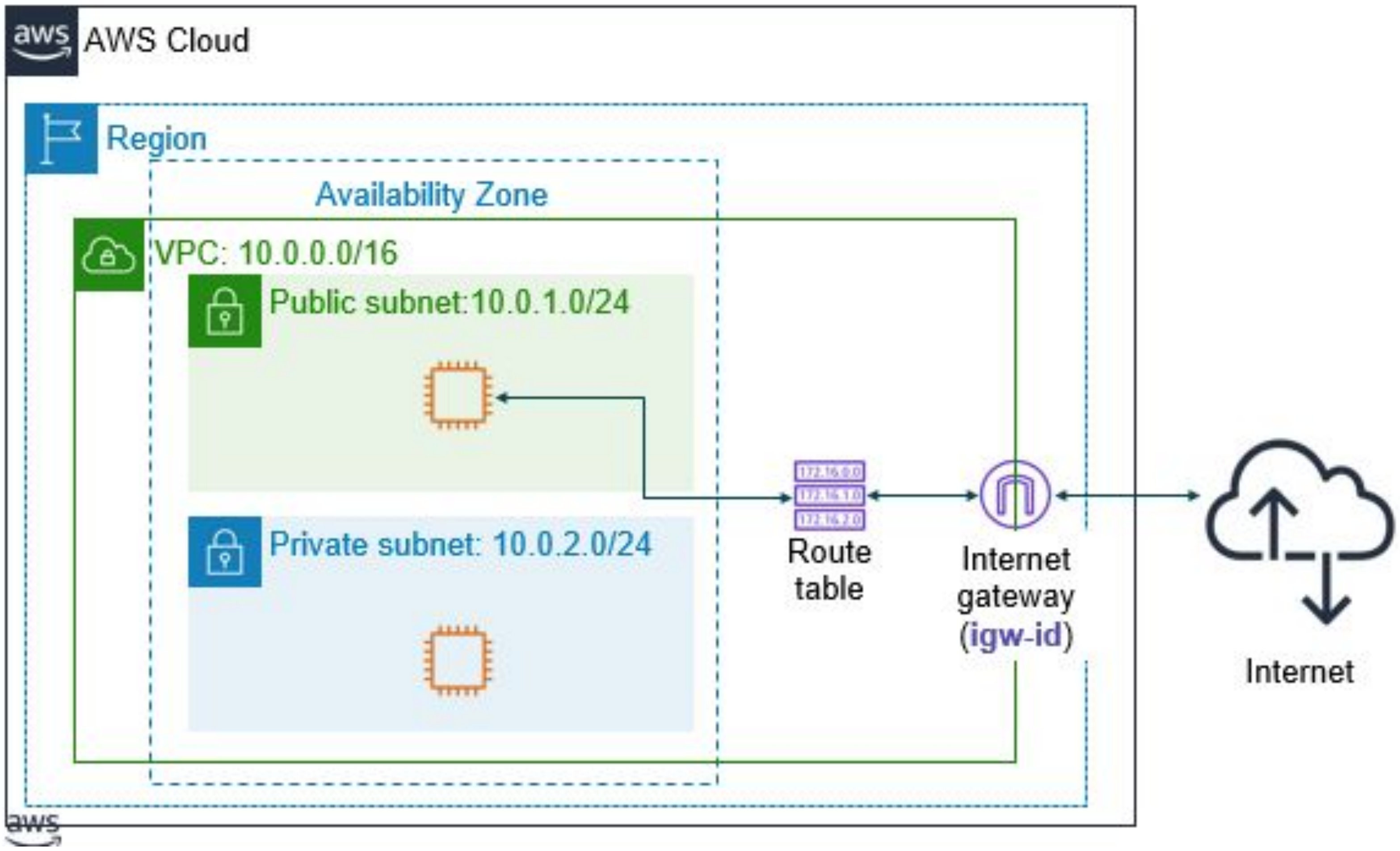
Lecture's Agenda

- Amazon Virtual Private Cloud
- **VPC Networking**
- VPC Security
- Amazon Route 53 and CloudFront

Internet Gateway

- "An internet gateway is a VPC component that allows communication between instances in the VPC and the internet."
- An internet gateway serves two purposes:
  - Provide a target in your VPC route tables for internet-routable traffic
  - Perform network address translation for instances that were assigned public IPv4 addresses
- To make a subnet public, user attach an internet gateway to the VPC and add a route to the route table to send non-local traffic through the internet gateway to the internet (0.0.0.0/0).

Internet Gateway (Cont.)



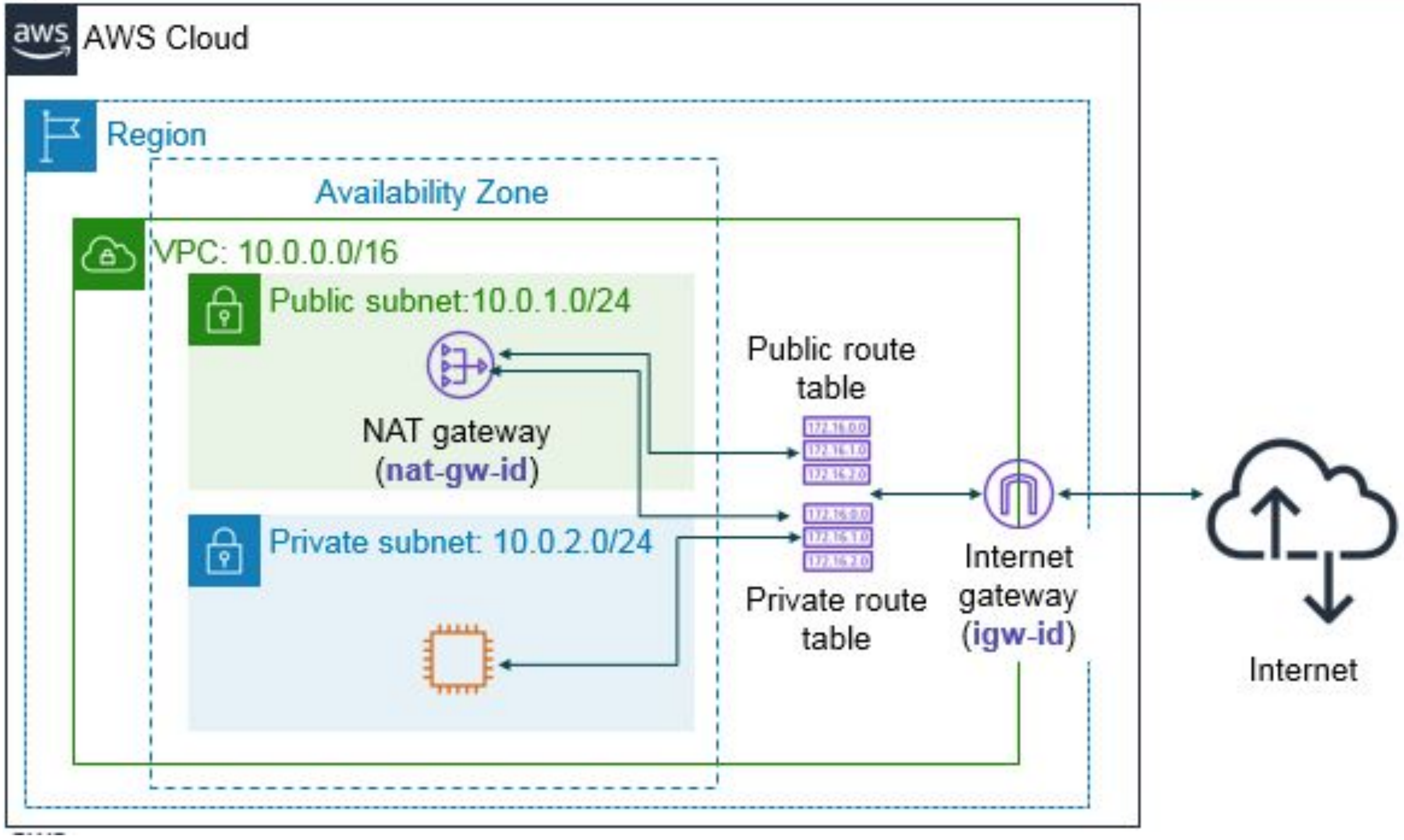
Public Subnet Route Table

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

NAT Gateway

- "A network address translation (NAT) gateway enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating a connection with those instances."
- To create a NAT gateway, user must specify the public subnet in which the NAT gateway should reside.
- User must also specify an Elastic IP address to associate with the NAT gateway.

NAT Gateway (Cont.)



Public Subnet Route Table

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

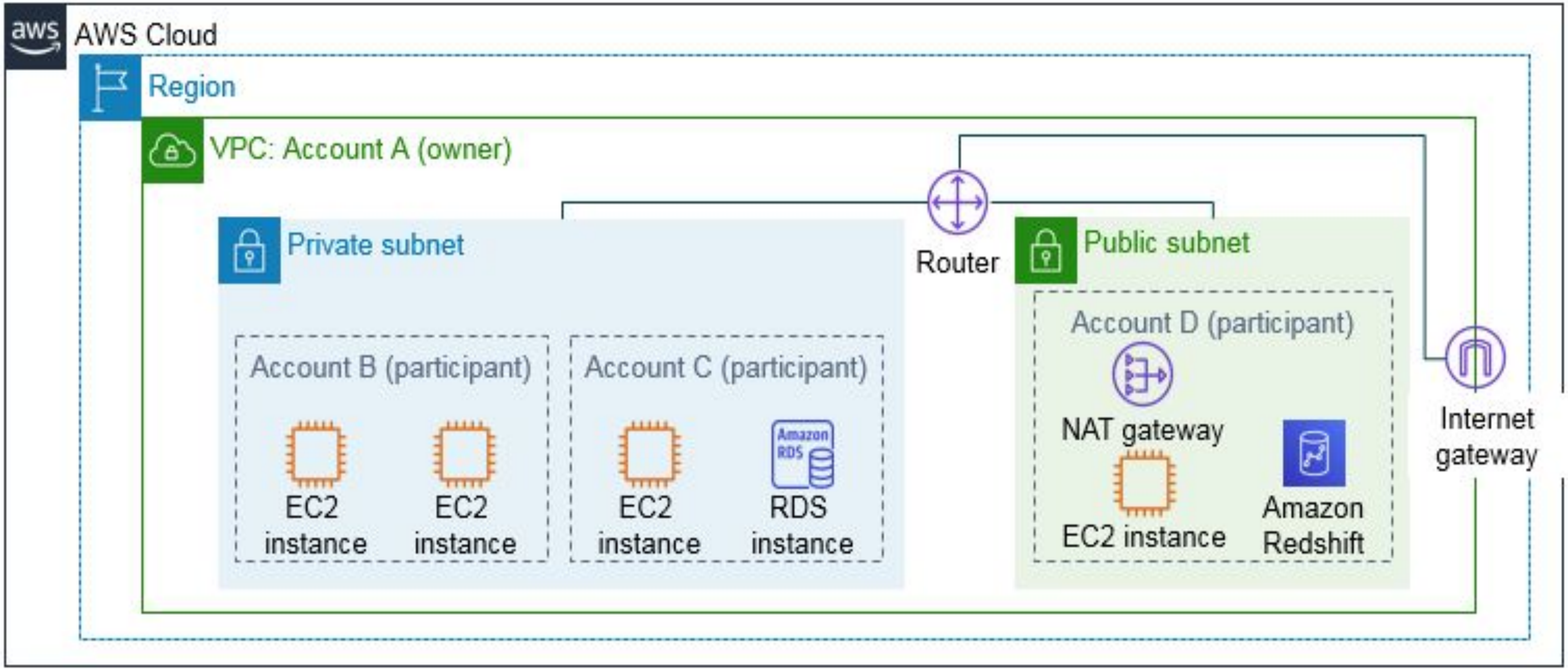
Private Subnet Route Table

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

VPC Sharing

- “VPC sharing enables customers to share subnets with other AWS accounts in the same organization.”
- In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization.
- After a subnet is shared
  - Participants can view, create, modify, and delete their application resources in the subnets that are shared with them.
  - Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner.

VPC Sharing (Cont.)



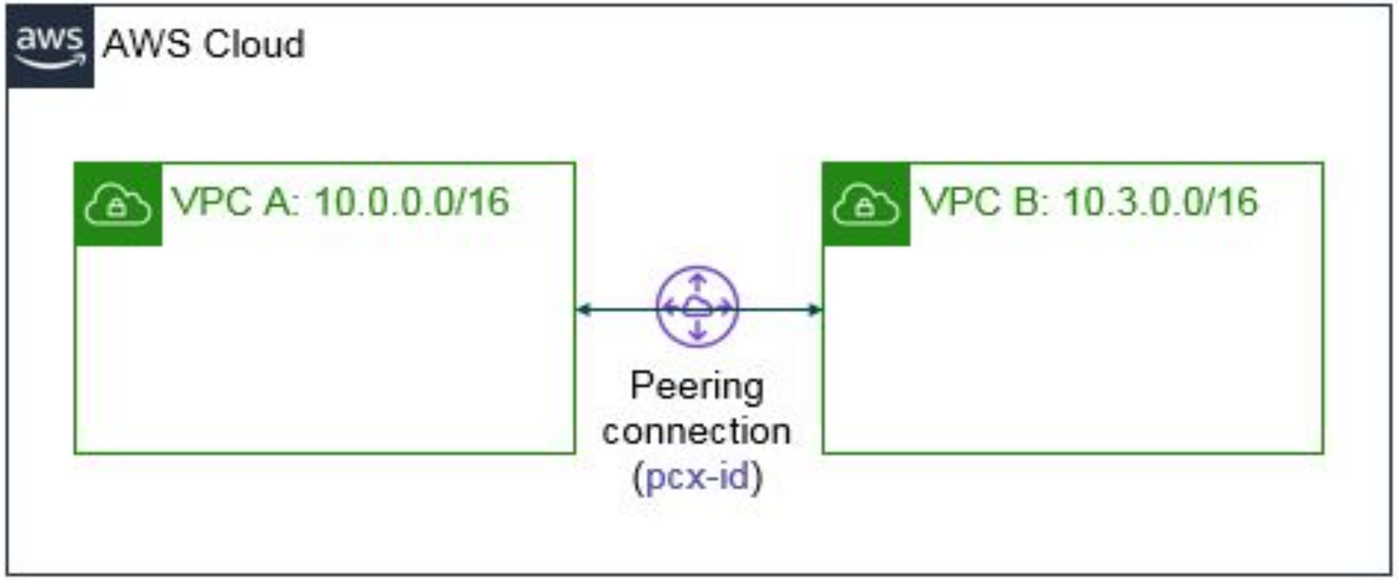
VPC Peering

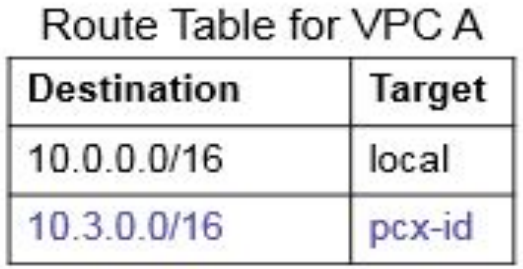
- "A networking connection between two VPCs that enables user to route traffic between them privately."
- Customer can connect VPCs in own AWS account, between AWS accounts, or between AWS Regions

Restrictions:

- IP spaces (range) cannot overlap
- Transitive peering is not supported. A=>B=>C != A=>C
- Customer can only have one peering resource between the same two VPCs

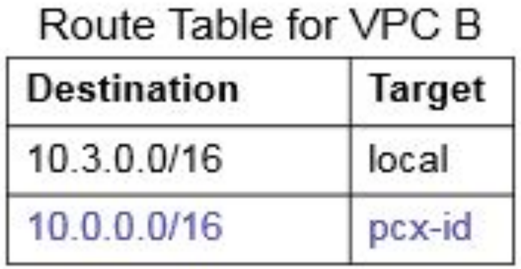
VPC Peering (Cont.)





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

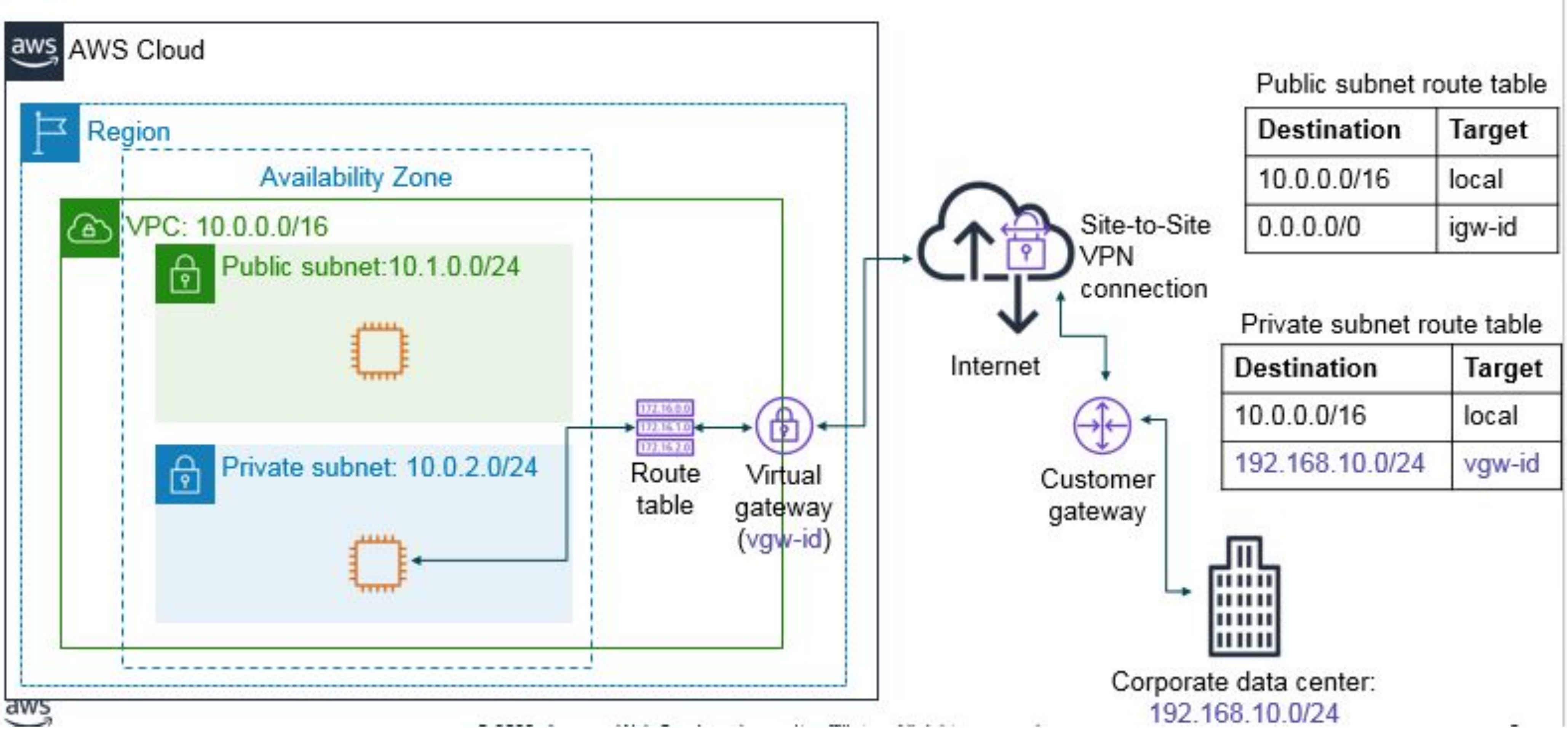
Destination	Target
10.3.0.0/16	local
10.0.0.0/16	pcx-id

AWS Site-to-Site VPN

- By default, instances that customer launch into a VPC cannot communicate with a remote network

- To connect a VPC to a remote network, customer needs to:
  - Create a new VPN gateway and attach it to the VPC
  - Define the configuration of the VPN gateway and the customer gateway
  - Establish a Site-to-Site VPN connection to link the two systems together
  - Configure routing to pass traffic through the connection

AWS Site-to-Site VPN (Cont.)


AWS Cloud
Region
Availability Zone
VPC: 10.0.0.0/16
Public subnet:10.1.0.0/24
Private subnet: 10.0.2.0/24
Route table
Virtual gateway (vgw-id)
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

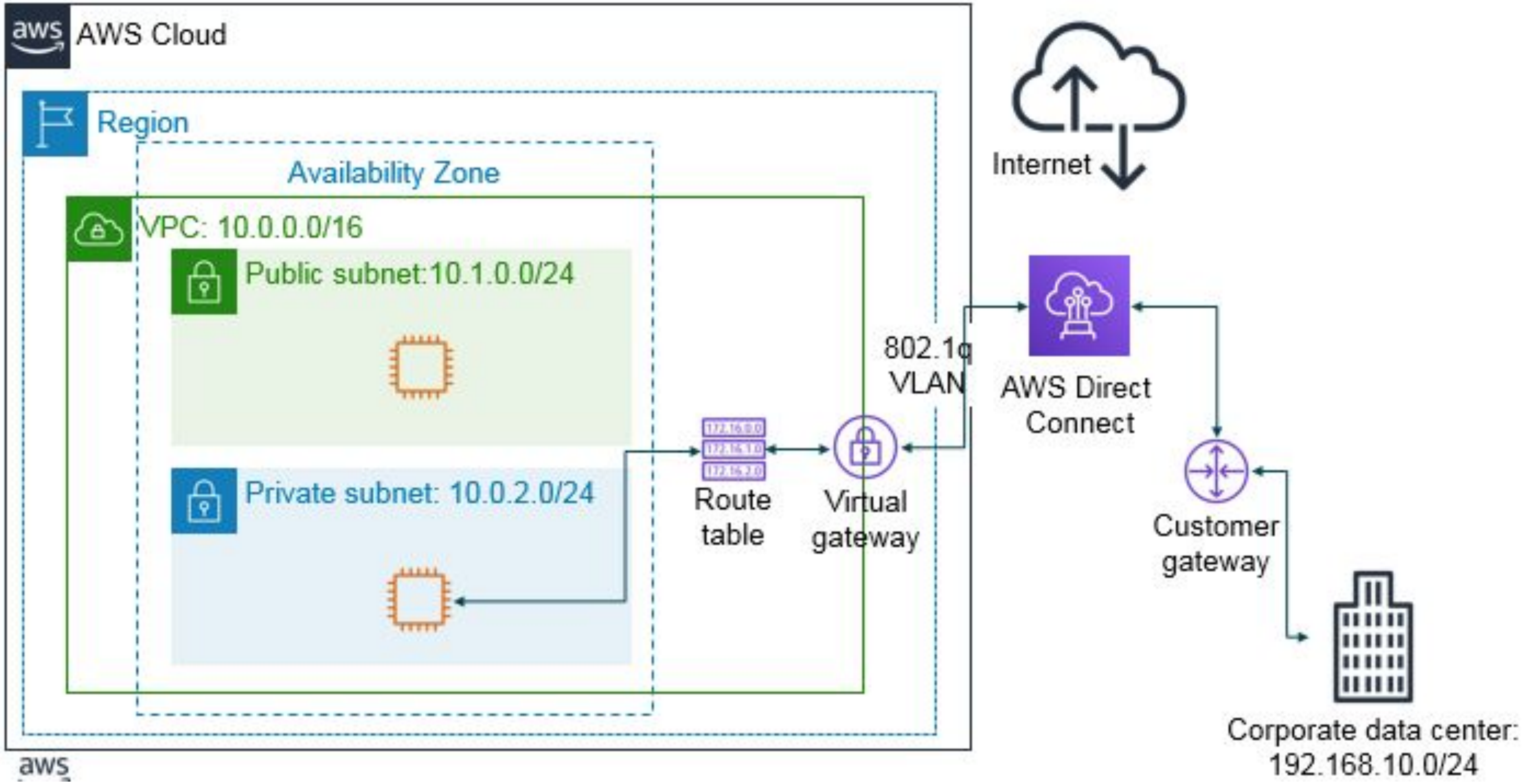
Private subnet route table

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

AWS Direct Connect

- “AWS Direct Connect enables to establish a dedicated, private network connection between corporate network and one of the AWS direct connect (DX) locations.”
- Increases bandwidth throughput
- Provide better and consistent network experience than internet-based connections
- DX uses open standard 802.1q Virtual Local Area Networks

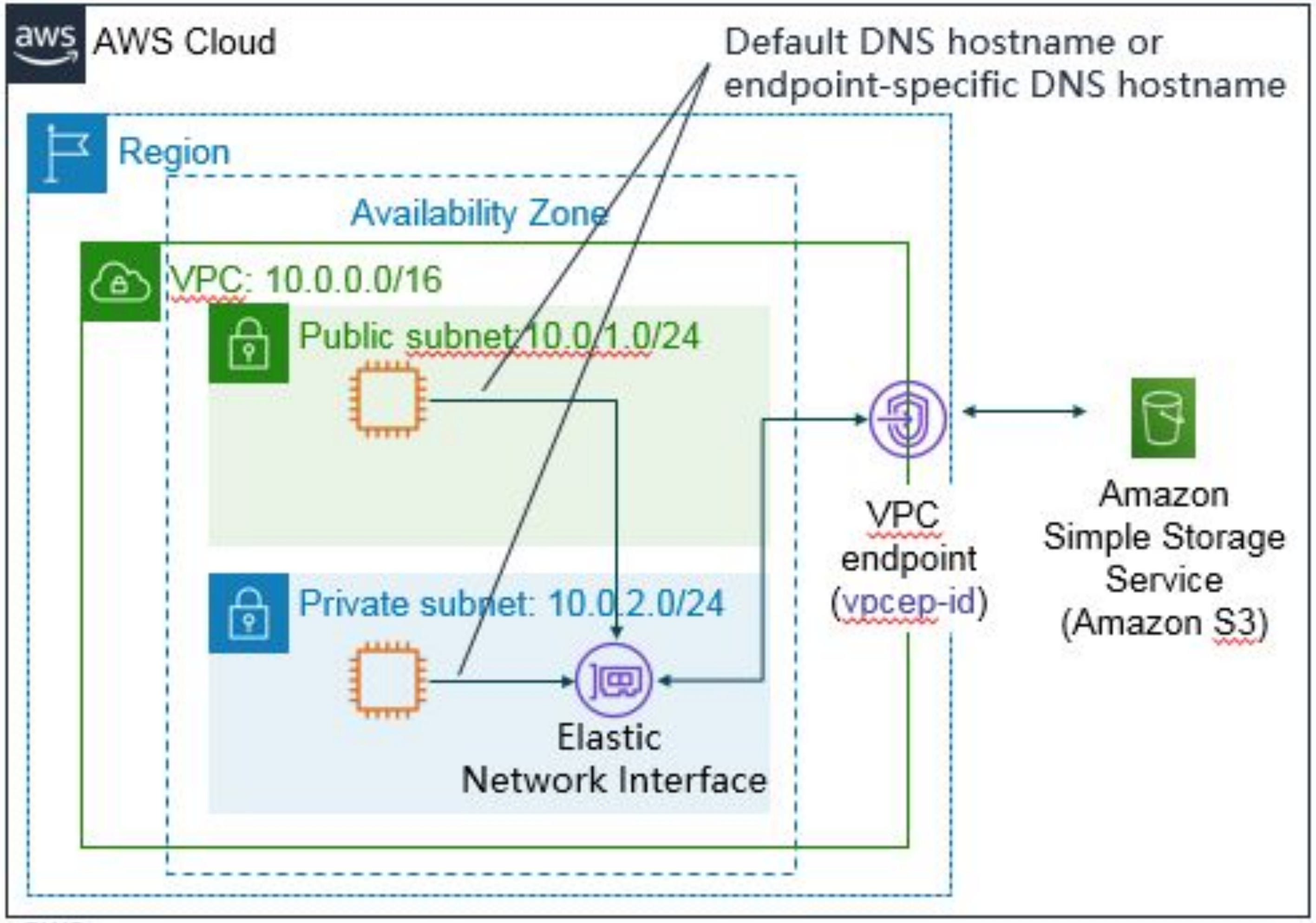
AWS Direct Connect (Cont.)



VPC Endpoints

- "A VPC endpoint is a virtual device that enables to privately connect customer's VPC to supported AWS services and VPC endpoint services that are powered by AWS PrivateLink."
  - PrivateLink is used to connect third party services available on AWS marketplace
- Connection to these services does not require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection
- Instances in the VPC do not require public IP addresses to communicate with resources in the service
- Traffic between the VPC and the other service does not leave the Amazon network

VPC Endpoints (Cont.)


AWS Cloud
Default DNS hostname or endpoint-specific DNS hostname
Region
Availability Zone
VPC: 10.0.0.0/16
Public subnet 10.0.1.0/24
Private subnet: 10.0.2.0/24
Elastic Network Interface
VPC endpoint (vpcep-id)
Amazon Simple Storage Service (Amazon S3)

Public Subnet Route Table

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

Types of VPC Endpoints

Interface Endpoints:

- Powered by AWS PrivateLink
  - Services available on AWS marketplace
  - ThoughtSpot, GitLab Ultimate etc.
- Hourly usage rates and data processing rates apply

Gateway Endpoints:

- AWS supported services
  - Amazon S3, Amazon DynamoDB etc.
- Incurs no additional charge on endpoint connection

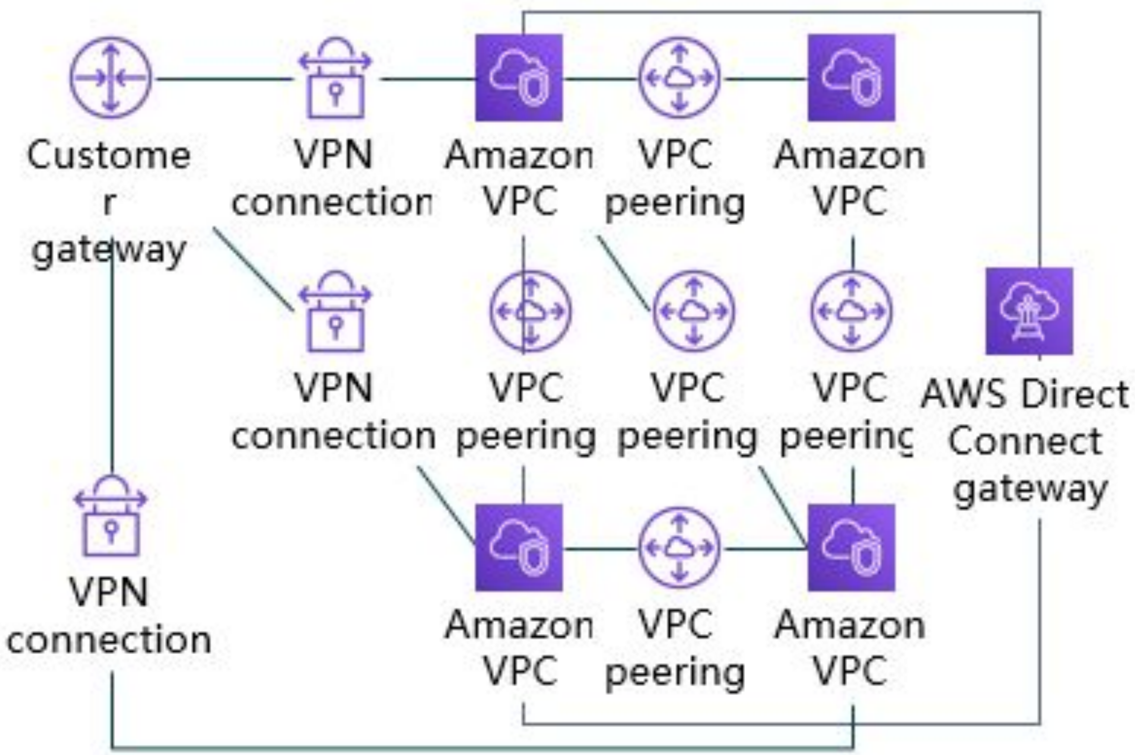
AWS Transit Gateway

- An AWS organization (or customer) can have hundreds of VPCs distributed across AWS accounts and Regions to serve multiple lines of business, teams, projects, and so forth.

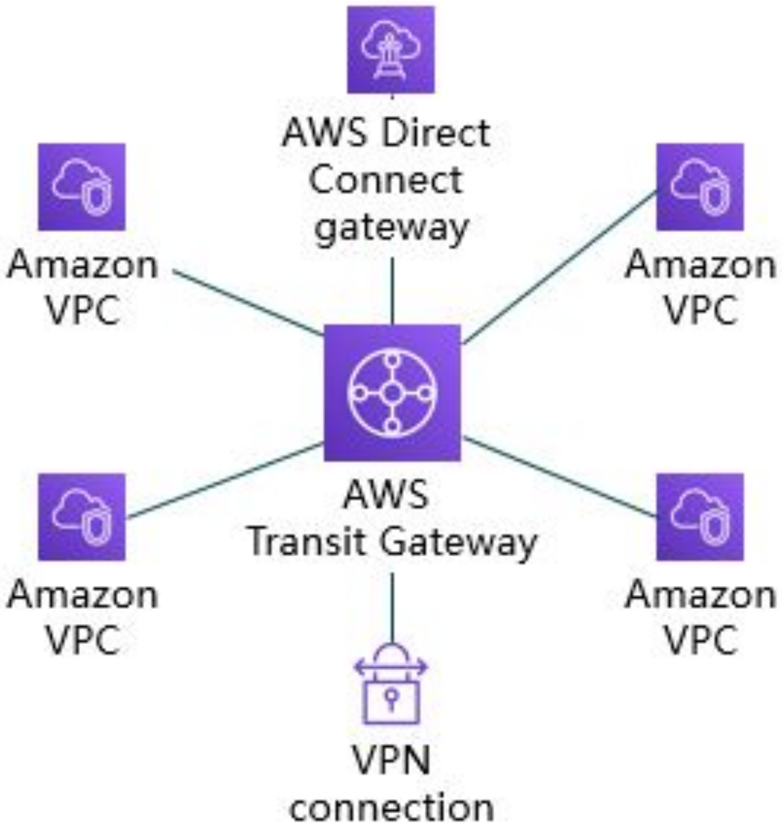
- With AWS Transit Gateway, the customer only need to create and manage a single connection from the central gateway into each VPC, on-premises data center, or remote office across the network.

AWS Transit Gateway

From this...



To this...



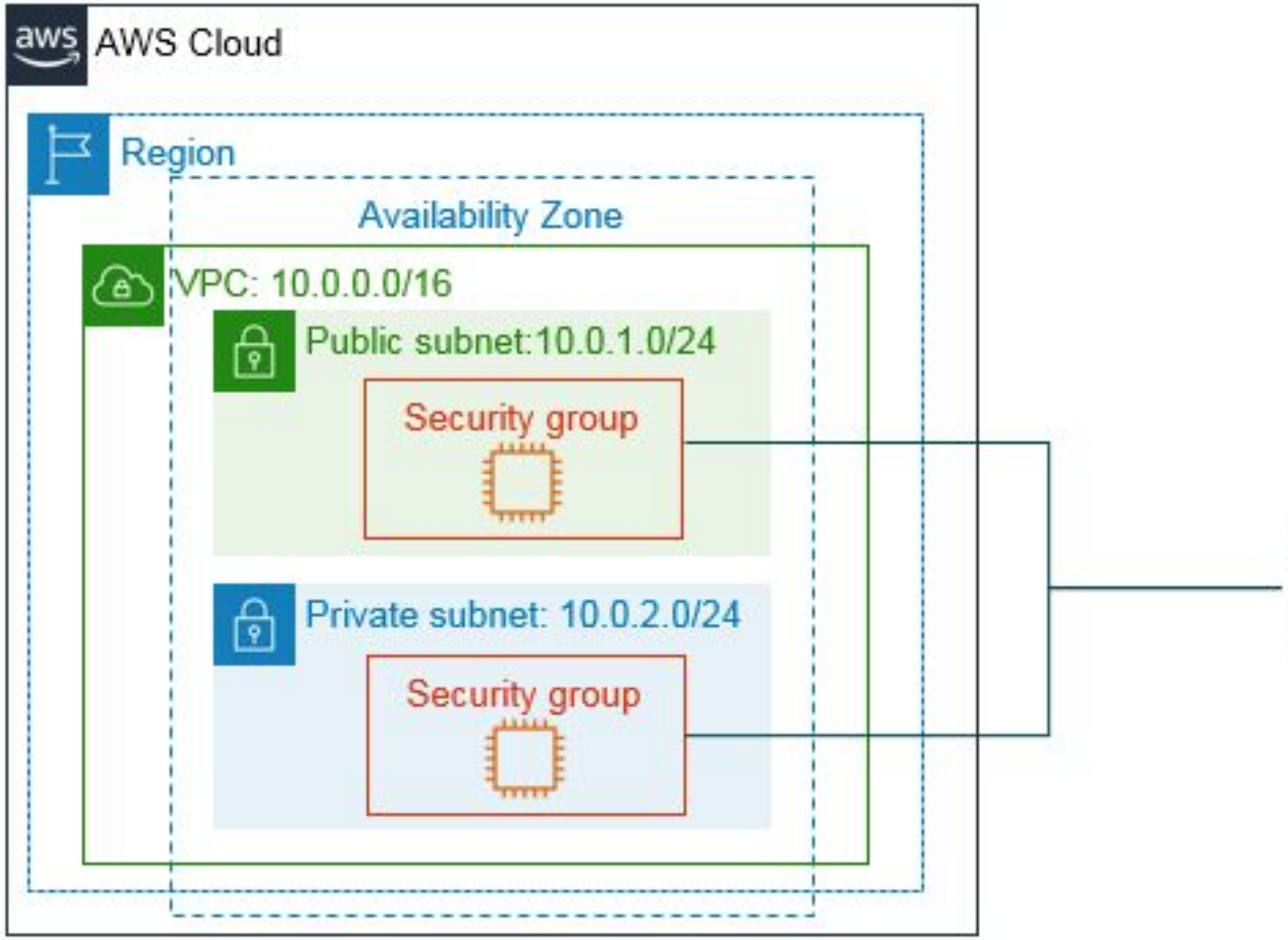
Lecture’s Agenda

- Amazon Virtual Private Cloud
- VPC Networking
- **VPC Security**
- Amazon Route 53 and CloudFront

Security Group

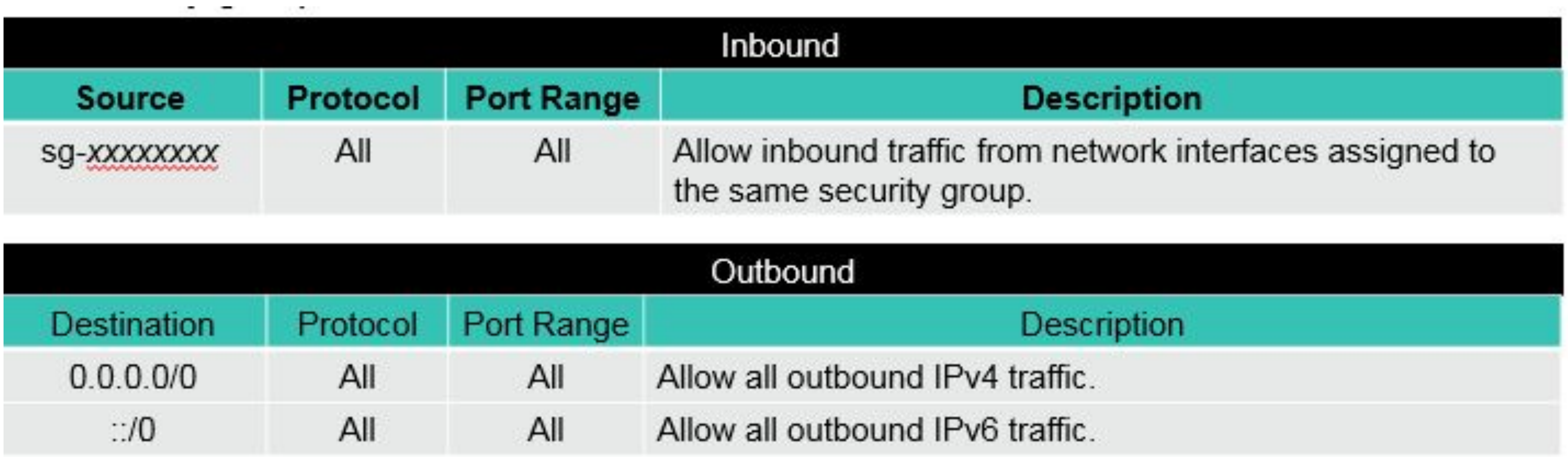
- "A security group is a way for the customer to filter traffic to the instances."
- Acts as a virtual firewall for the instance
- Controls inbound and outbound traffic
- Default security groups deny all inbound traffic and allow all outbound traffic

Security Group (Cont.)



Security groups act at the instance level.

Security Group Unsafe Rules

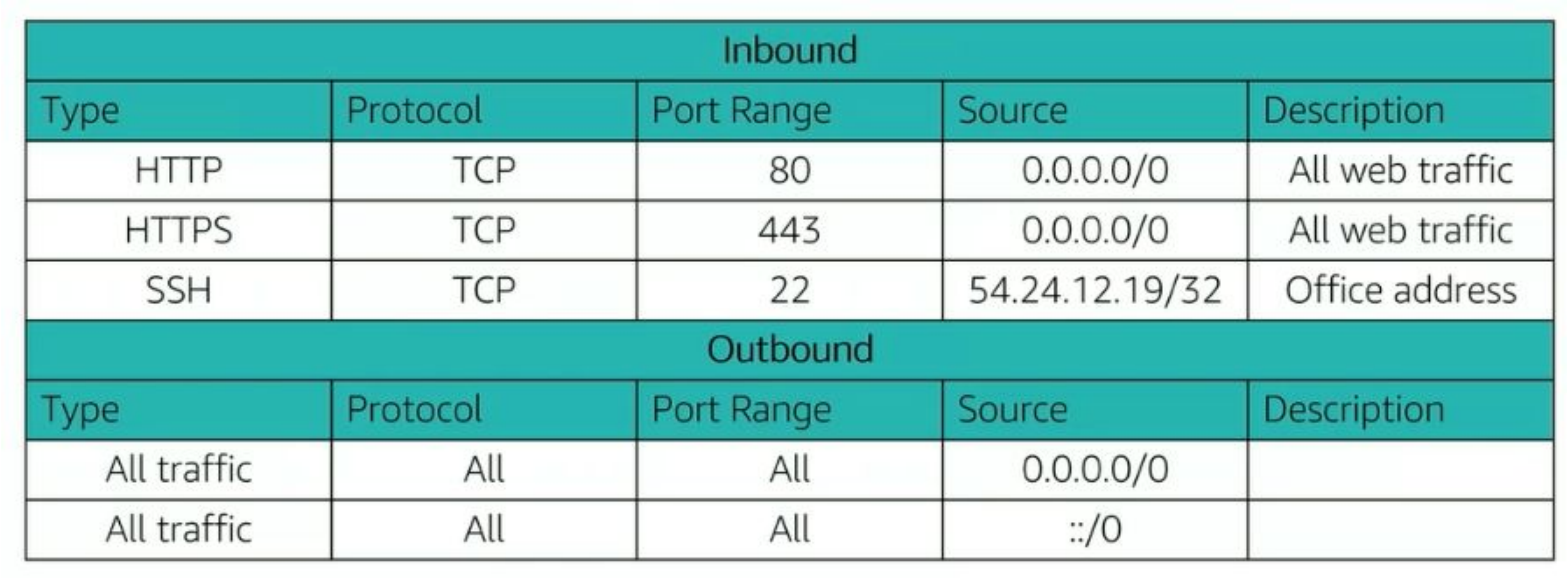


Inbound			
Source	**Protocol**	**Port Range**	**Description**
sg-xxxxxxxx	All	All	Allow inbound traffic from network interfaces assigned to the same security group.

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.

Security Group Custom Rules

All rules are evaluated before decision to allow traffic.

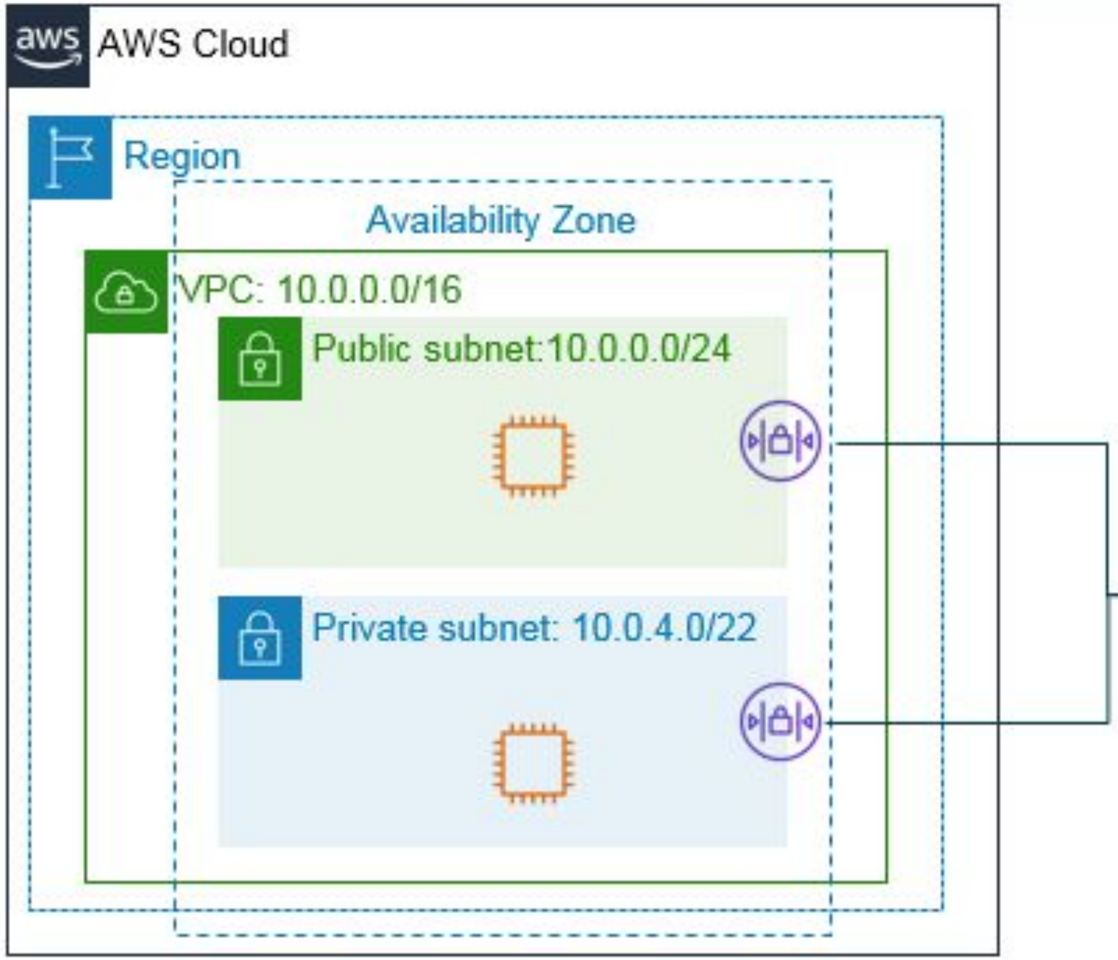


Inbound				
Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	All web traffic
HTTPS	TCP	443	0.0.0.0/0	All web traffic
SSH	TCP	22	54.24.12.19/32	Office address
Outbound				
Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

Network Access Control List (Network ACL)

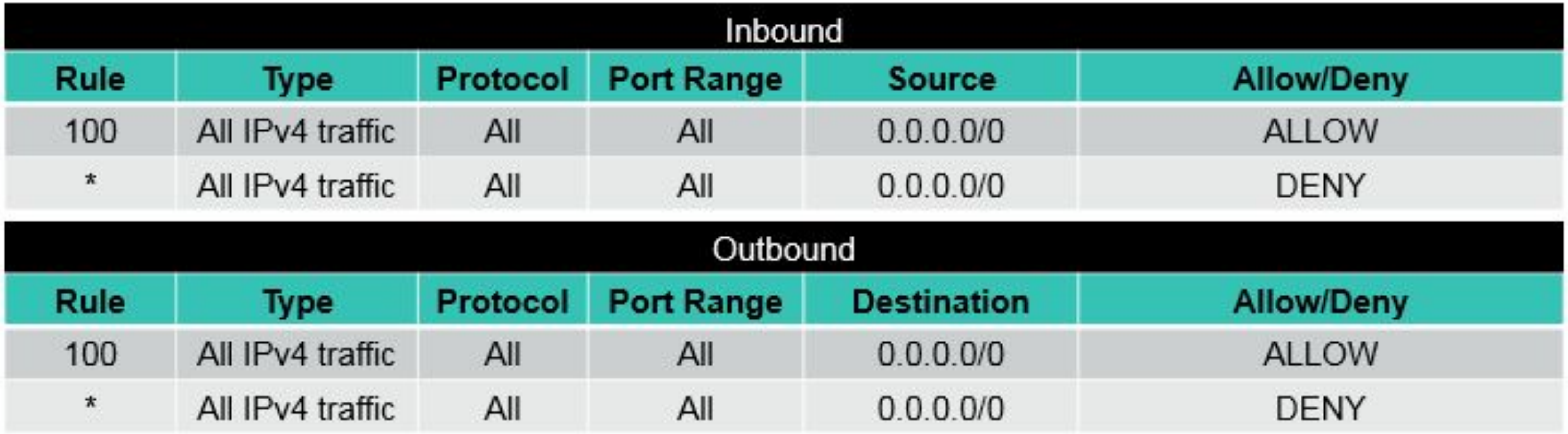
- “A network ACL acts as a firewall for controlling traffic in and out of one or more subnets.”
- Each subnet in VPC must be associated with a network ACL
  - If customer don't explicitly associate a subnet with a network ACL, the subnet is automatically associated with the default network ACL
  - Customer can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL at a time
- Has separate inbound and outbound rules
  - Each rule can either allow or deny traffic
- Default network ACLs allow all inbound and outbound IPv4 traffic

Network ACL (Cont.)



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

Network ACL Unsafe Rules



Inbound

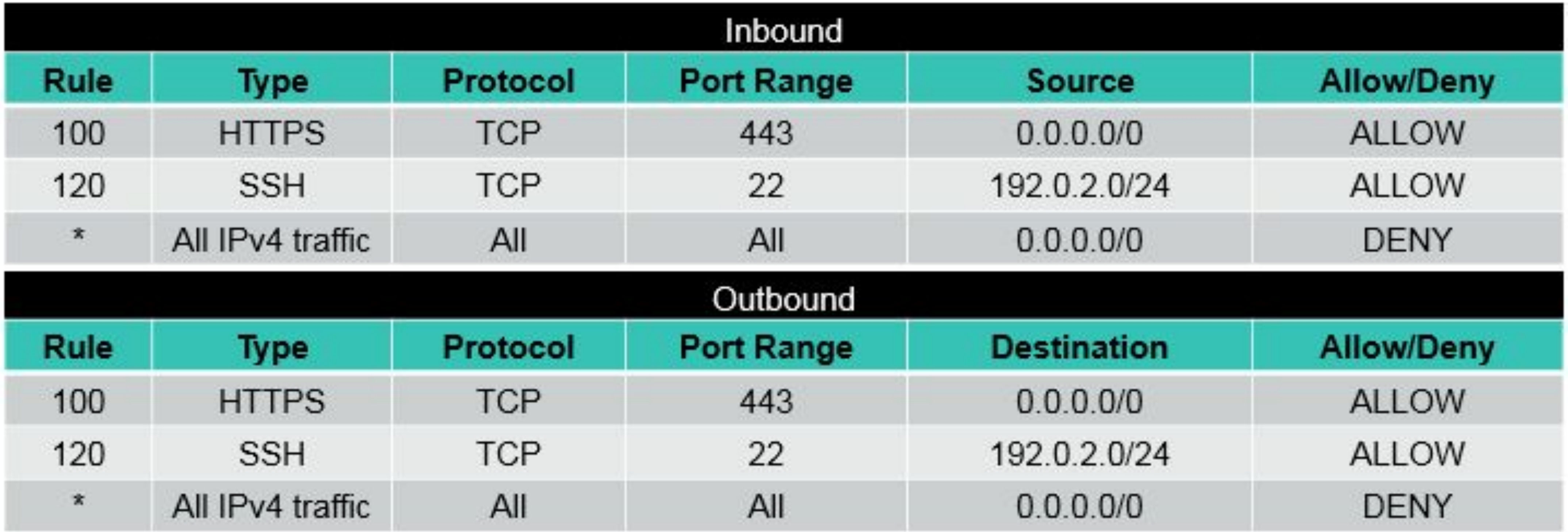
Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

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

Network ACL Custom Rules

Rules are evaluated in number order, starting with the lowest number.



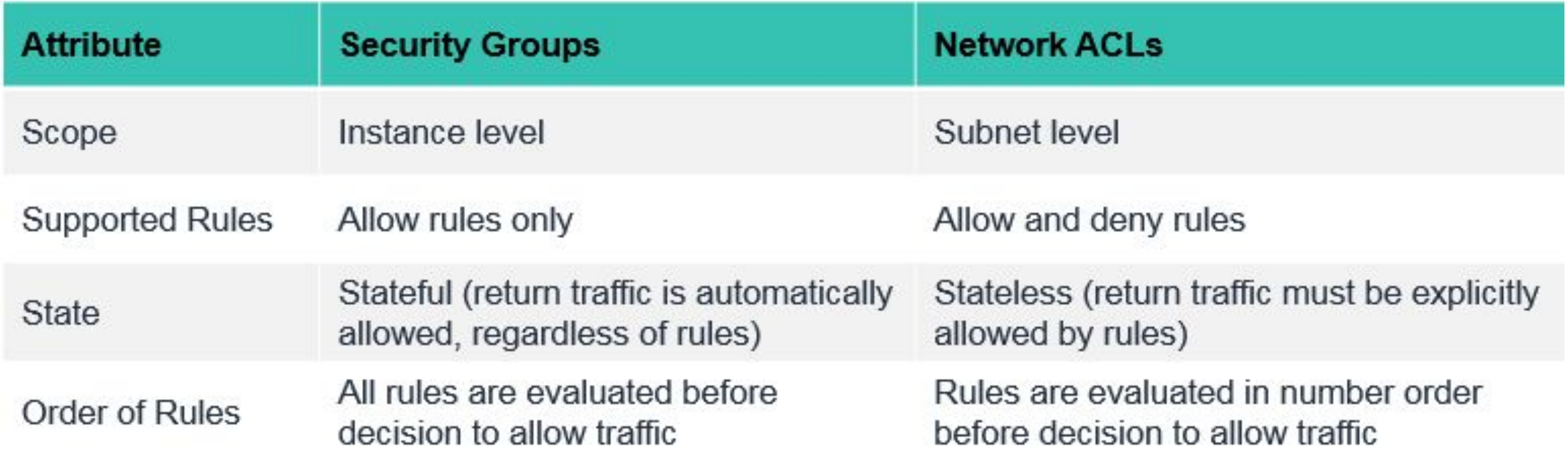
Inbound

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

Lab 2: Build the VPC and Launch a Web Server

Lab 2 Scenario:

- In this lab, you use Amazon VPC to create your own VPC and add some components to produce a customized network. You create a security group for your VPC. You also create an EC2 instance and configure it to run a web server and to use the security group. You then launch the EC2 instance into the VPC.

Amazon VPC

Amazon EC2

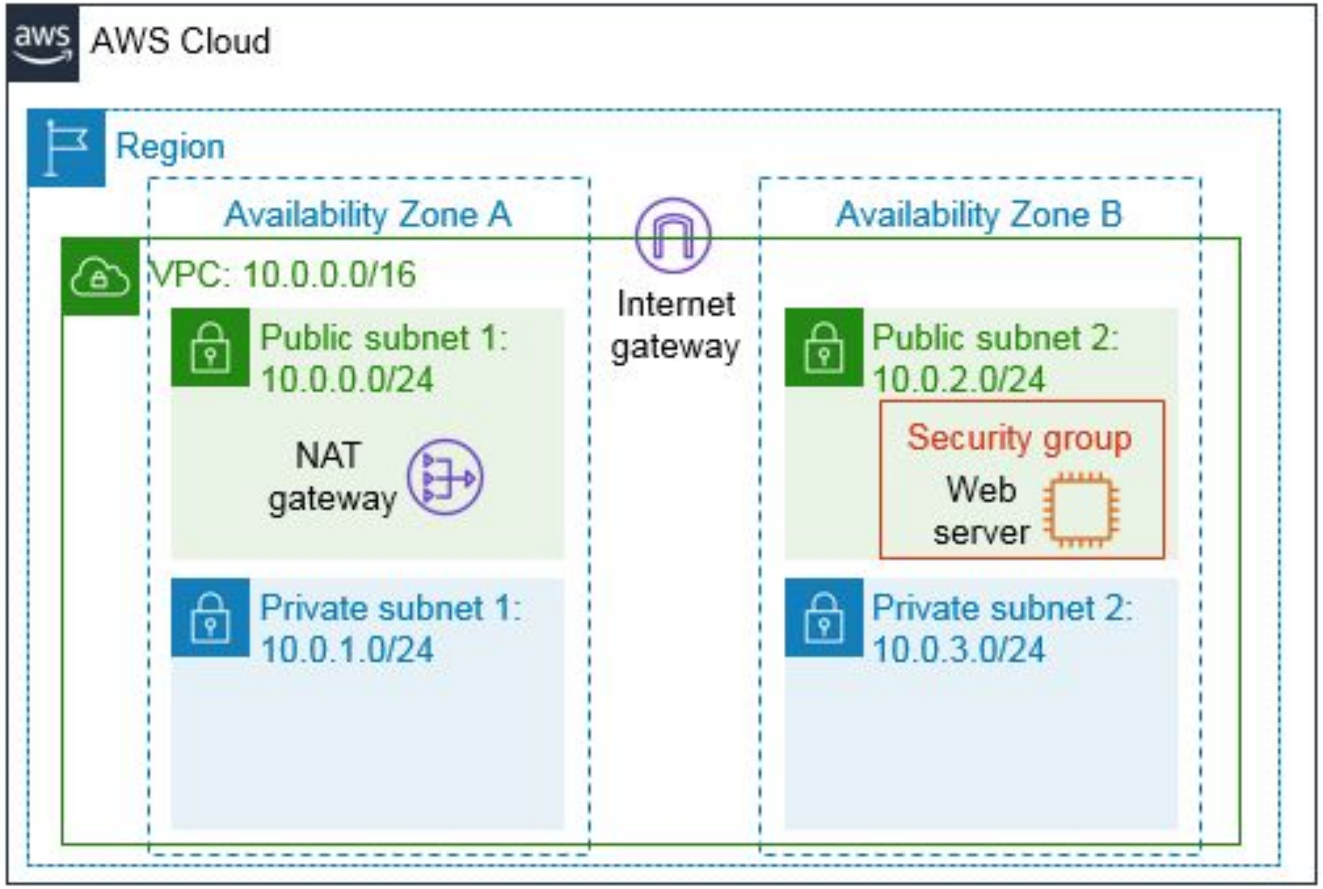
Lab 2: Build the VPC and Launch a Web Server

Lab 2 Tasks:

- Create a VPC
- Create additional subnets
- Create a VPC security group
- Launch a web server instance

Lab 2: Build the VPC and Launch a Web Server

Final Product:



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

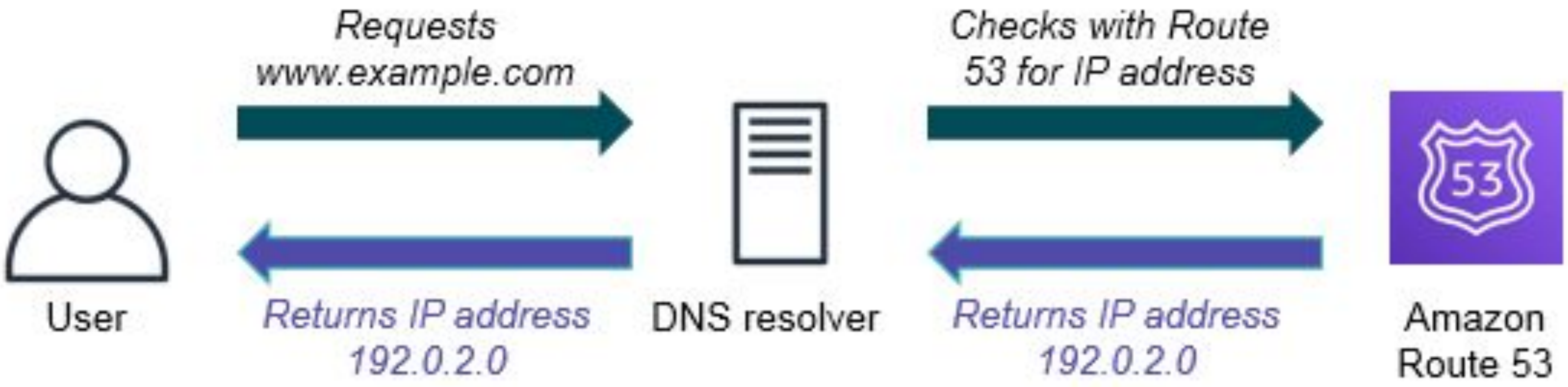
Lecture’s Agenda

- Amazon Virtual Private Cloud
- VPC Networking
- VPC Security
- **Amazon Route 53 and CloudFront**

Amazon Route 53

- Scalable Domain Name System (DNS) web service
- 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
- Enables to register domain names
- Fully compliant with IPv4 and IPv6
- Connects user requests to infrastructure running in AWS and also outside of AWS

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

Amazon Route 53 Supported Routing (Cont.)

Geoproximity Routing:

- Route traffic based on location of your resources

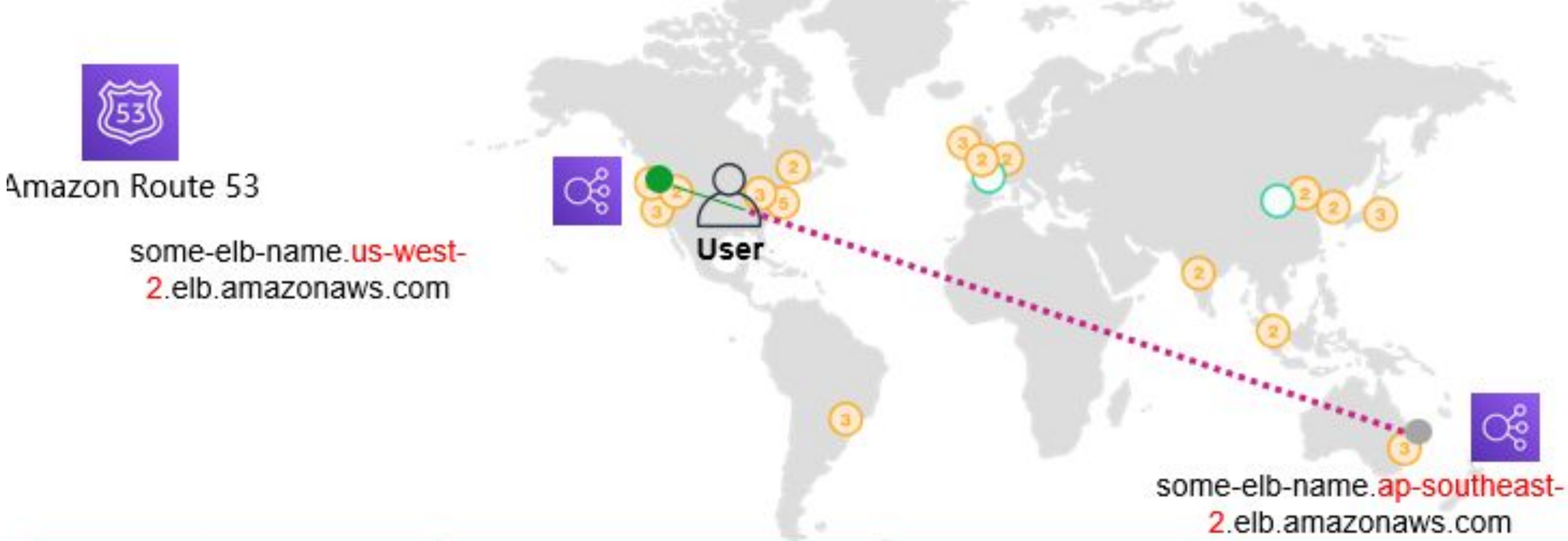
Failover Routing:

- 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



Amazon Route 53

some-elb-name.us-west-2.elb.amazonaws.com

User

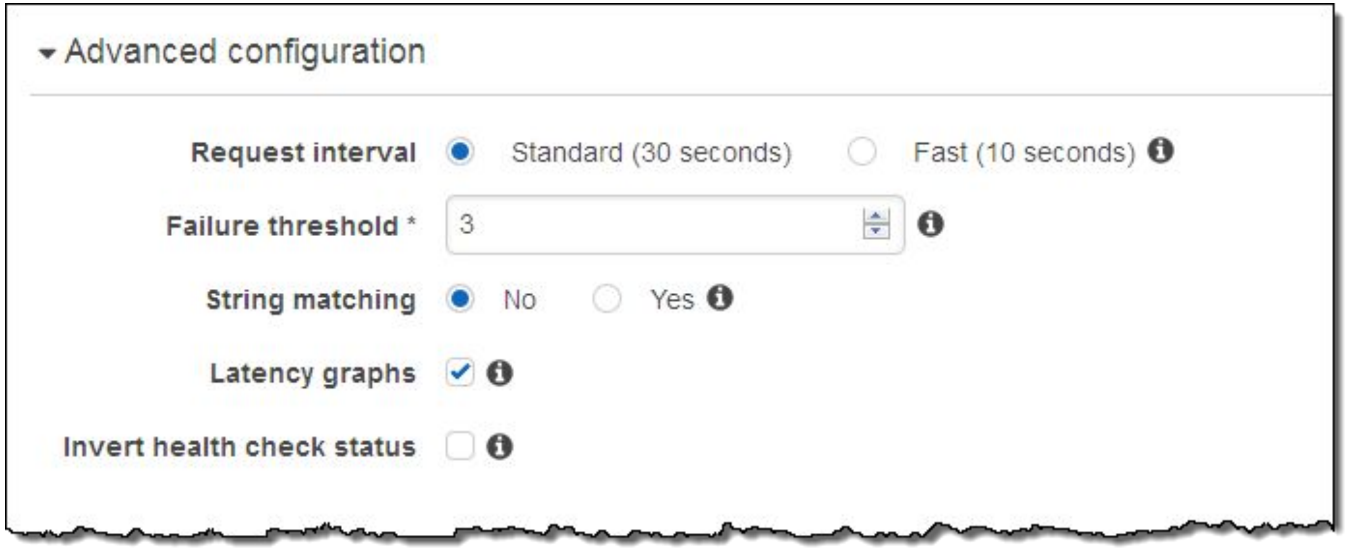
some-elb-name.ap-southeast-2.elb.amazonaws.com

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 applications that run on AWS by:

- Configuring backup and failover scenarios for user’s applications
- Enabling highly available multi-region architectures on AWS
- Creating health checks



▾ Advanced configuration

Request interval ● Standard (30 seconds) ○ Fast (10 seconds)

Failure threshold * 3

String matching ● No ○ Yes

Latency graphs ☑

Invert health check status □

Content Delivery Network (CDN)

- 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

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

Amazon CloudFront

Additional Resources

- **Amazon VPC Overview Page**
  - **https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html**
- **Amazon VPC Connectivity Options Whitepaper**
  - **https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/introduction.html**
- **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**

Questions?