AWS Solution Architect—Associate Level

Lesson 4: Amazon Virtual Private Cloud (VPC)

What You'll Learn

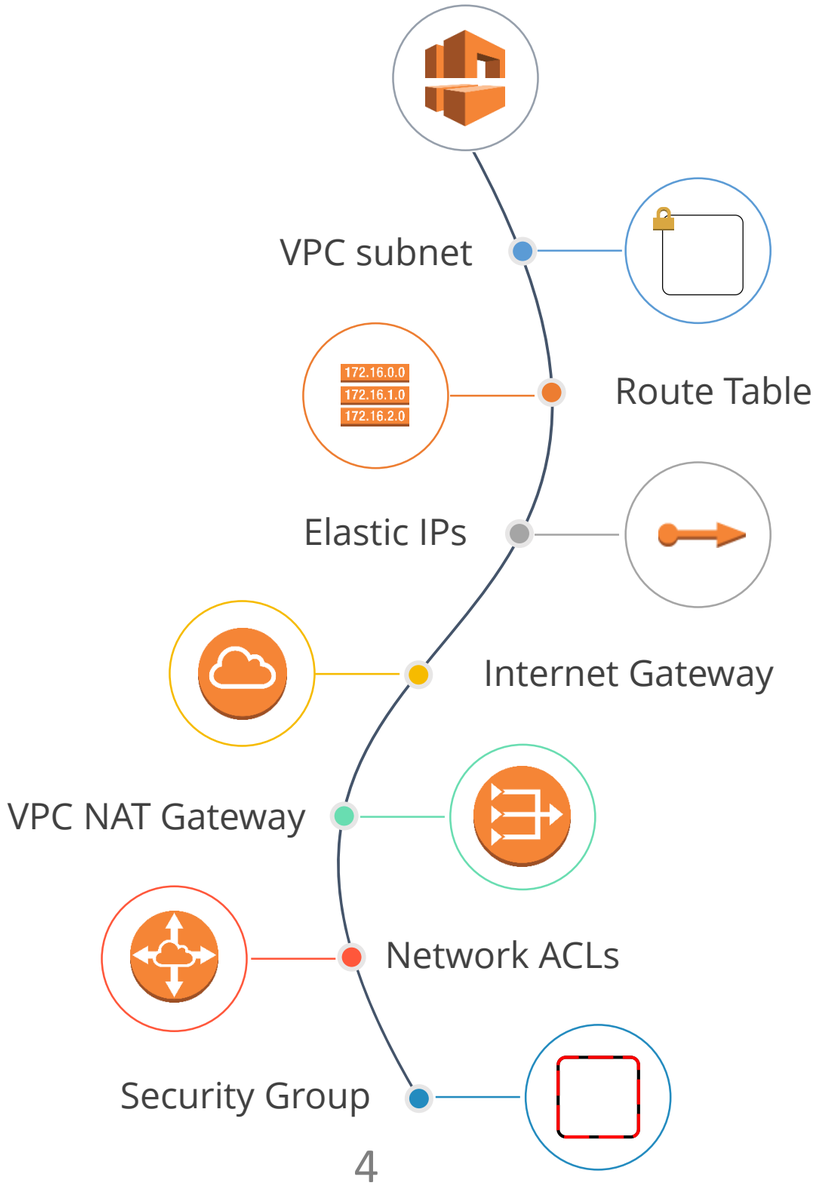
- Virtual Private Cloud
- Public, Private, and Elastic IP addresses
- Public and Private Subnets
- Internet Gateway
- Route Tables
- NAT Gateway
- Security Groups
- Network ACLs
- VPC Best Practices

Amazon VPC Overview

Overview of Virtual Private Cloud Concepts

Amazon VPC Terminology

The following are the terms that are used in VPCs:



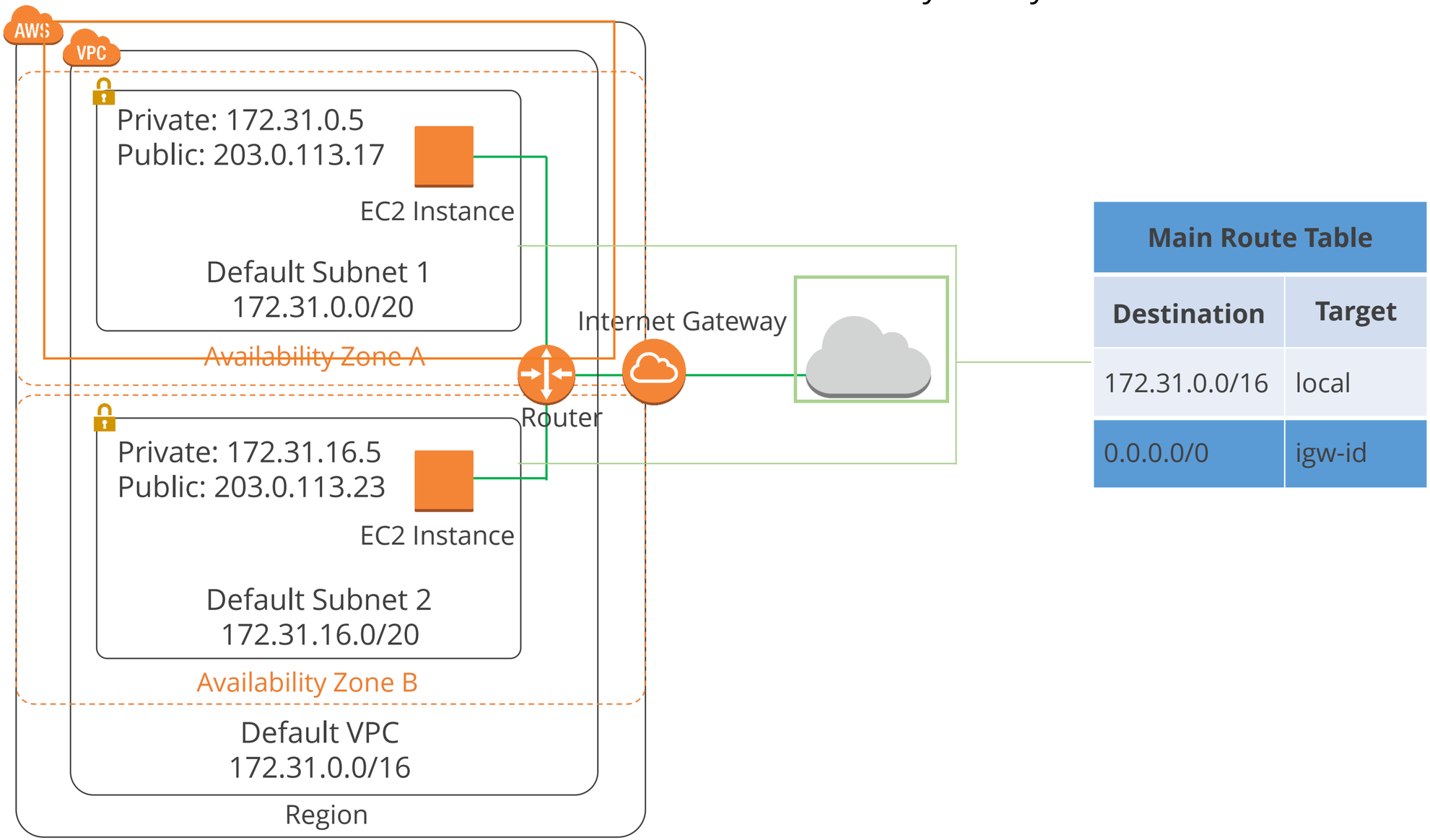
Amazon VPC Definition

Amazon’s definition of a VPC:

“Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.”

Amazon VPC Diagram

A VPC is your own virtual network in the Amazon cloud used as the network layer for your EC2 resources.



Main Route Table	
Destination	**Target**
172.31.0.0/16	local
0.0.0.0/0	igw-id

Knowledge Check

KNOWLEDGE CHECK	Amazon VPC is a component of which AWS service?

a. Compute

b. Analytics

c. Networking

d. Databases

KNOWLEDGE CHECK

Amazon VPC is a component of which AWS service?

a. Compute

b. Analytics

c. Networking

d. Databases

The correct answer is **c**.

Amazon VPC is a component of the Networking service.

KNOWLEDGE CHECK

Amazon VPC allows you to _____.

a. control the IP addresses used in your local data center

b. launch resources into a virtual network that you've defined

c. create physical networks wherever you want

d. associate Security Groups with your IAM users

KNOWLEDGE CHECK

Amazon VPC allows you to _____.

a. control the IP addresses used in your local data center

b. launch resources into a virtual network that you've defined

c. create physical networks wherever you want

d. associate Security Groups with your IAM users

The correct answer is **b.**

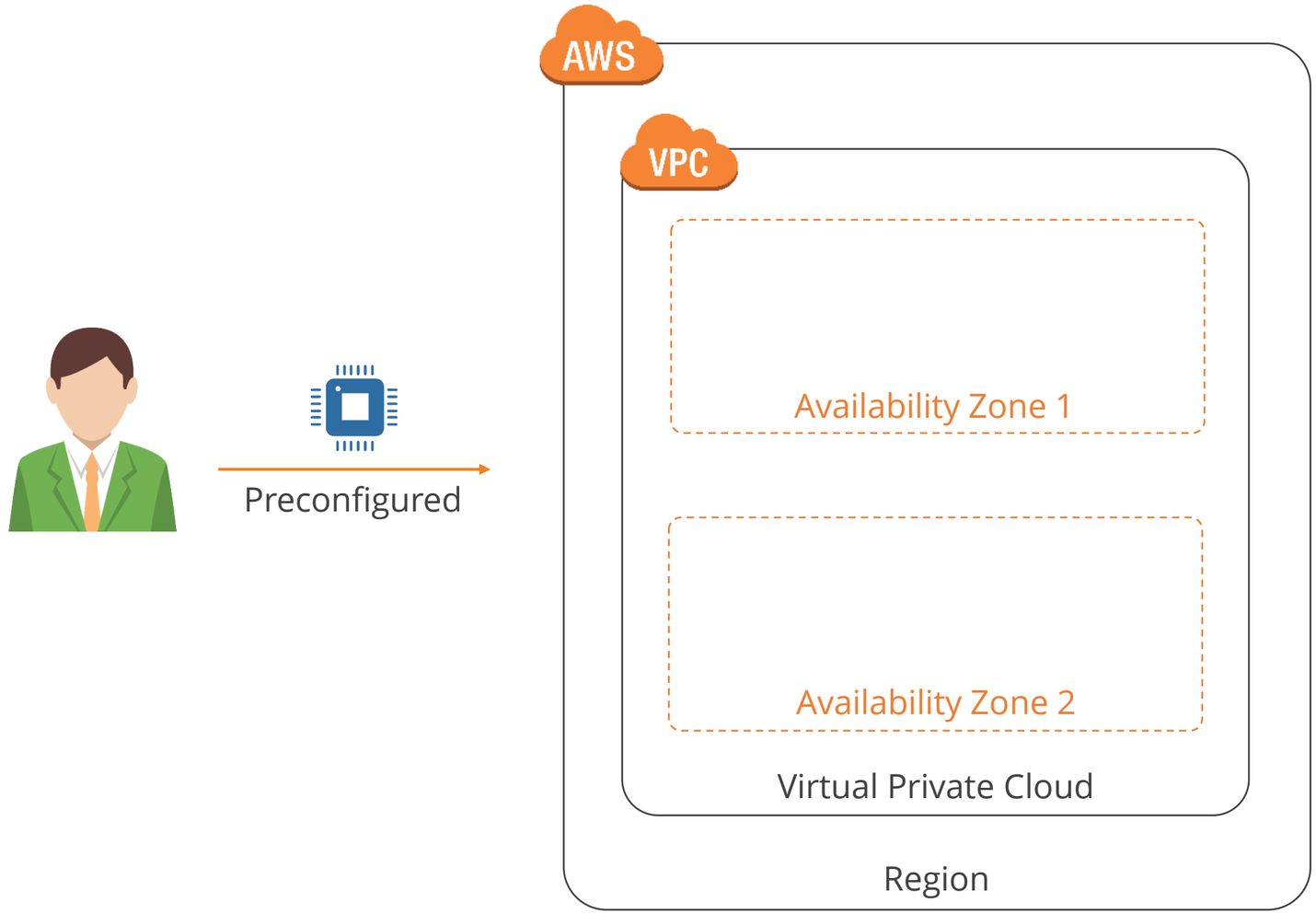
Amazon Virtual Private Cloud (Amazon VPC) allows you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined.

Amazon VPC

Using Virtual Private Clouds in AWS

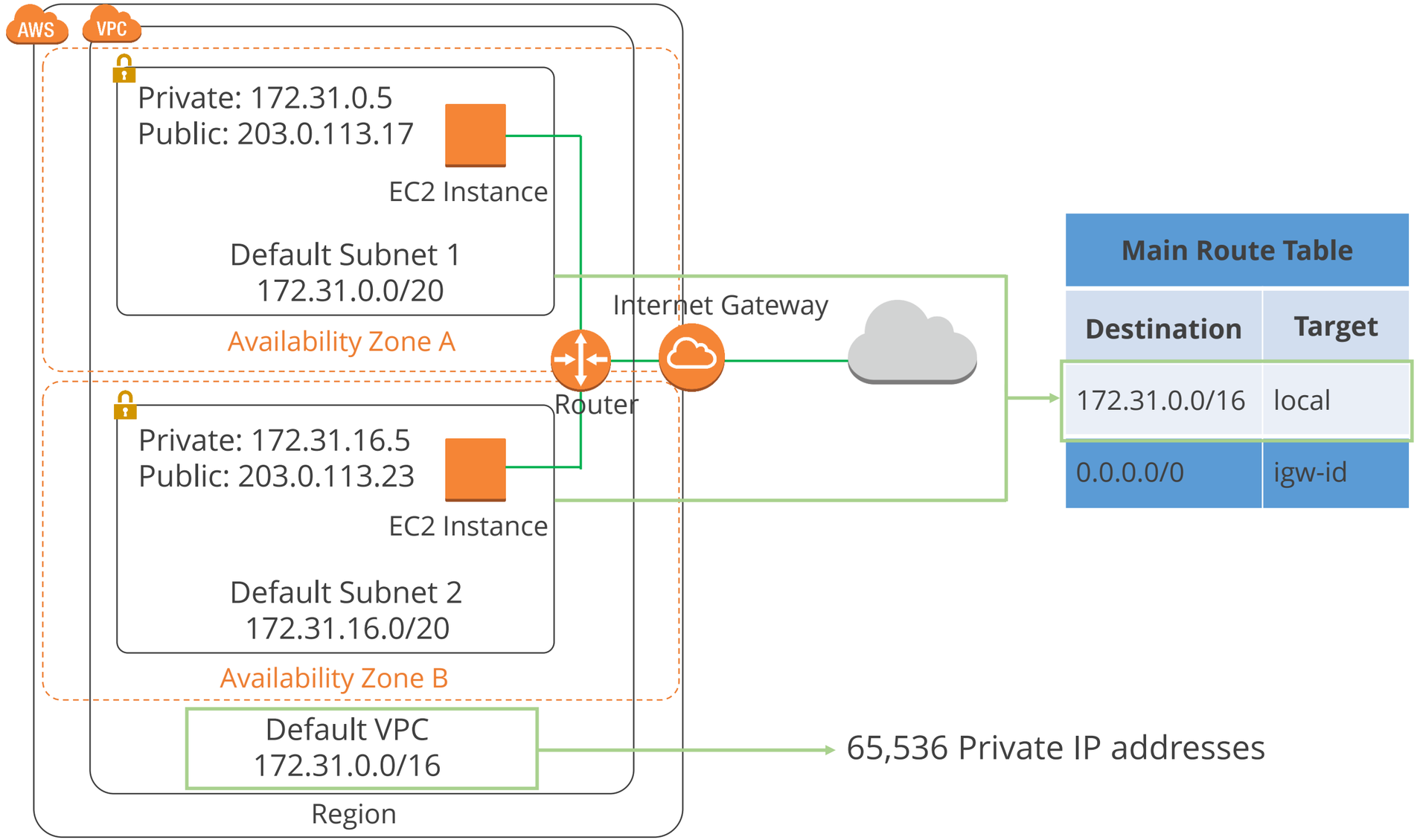
Default Amazon VPC

Each Amazon account comes with a default VPC that is preconfigured for you to start using straight away.



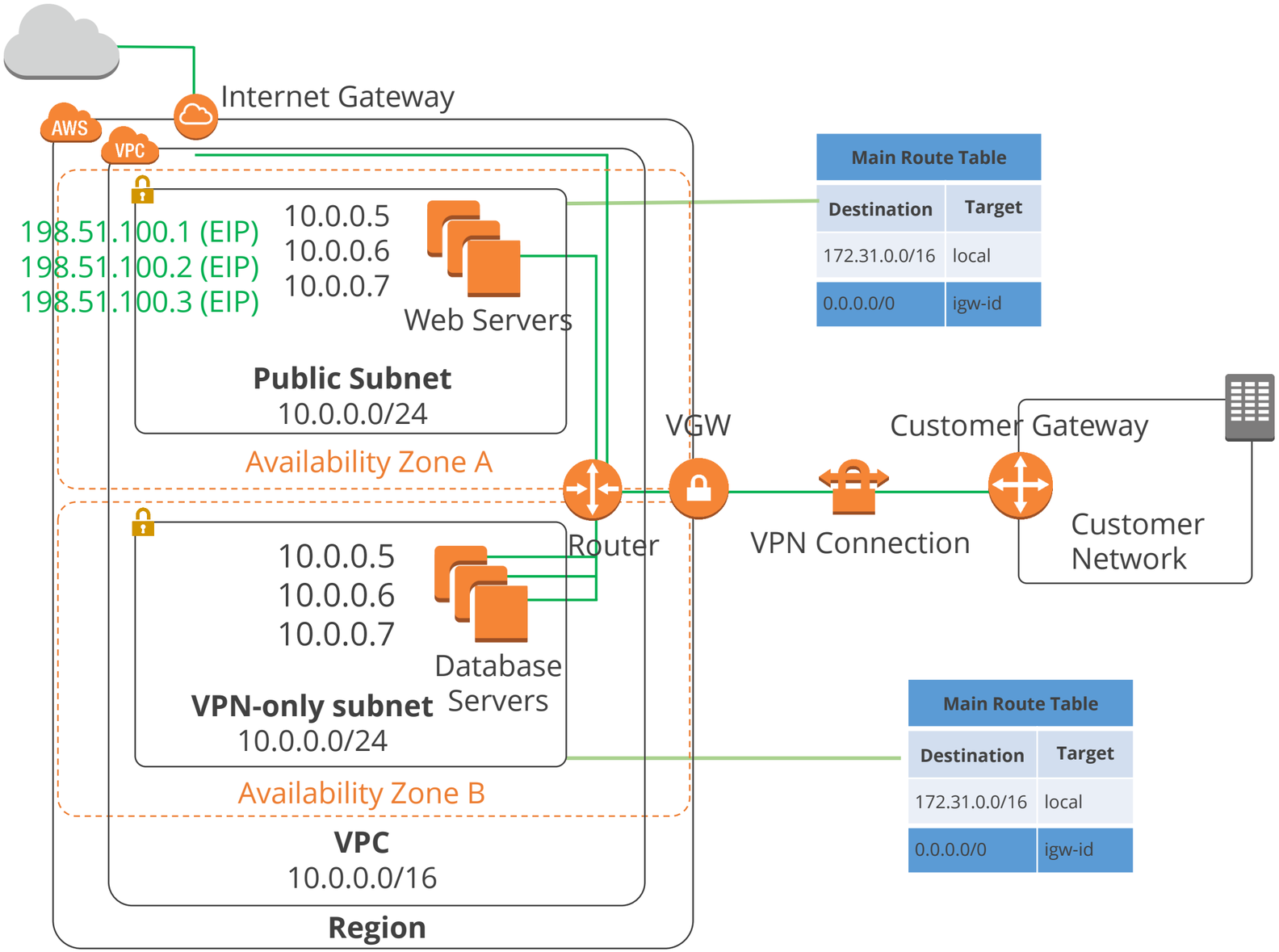
Default Amazon VPC (contd.)

The CIDR (Classless Inter-Domain Routing) block for a default VPC is always a /16 netmask, for example, 172.31.0.0/16.



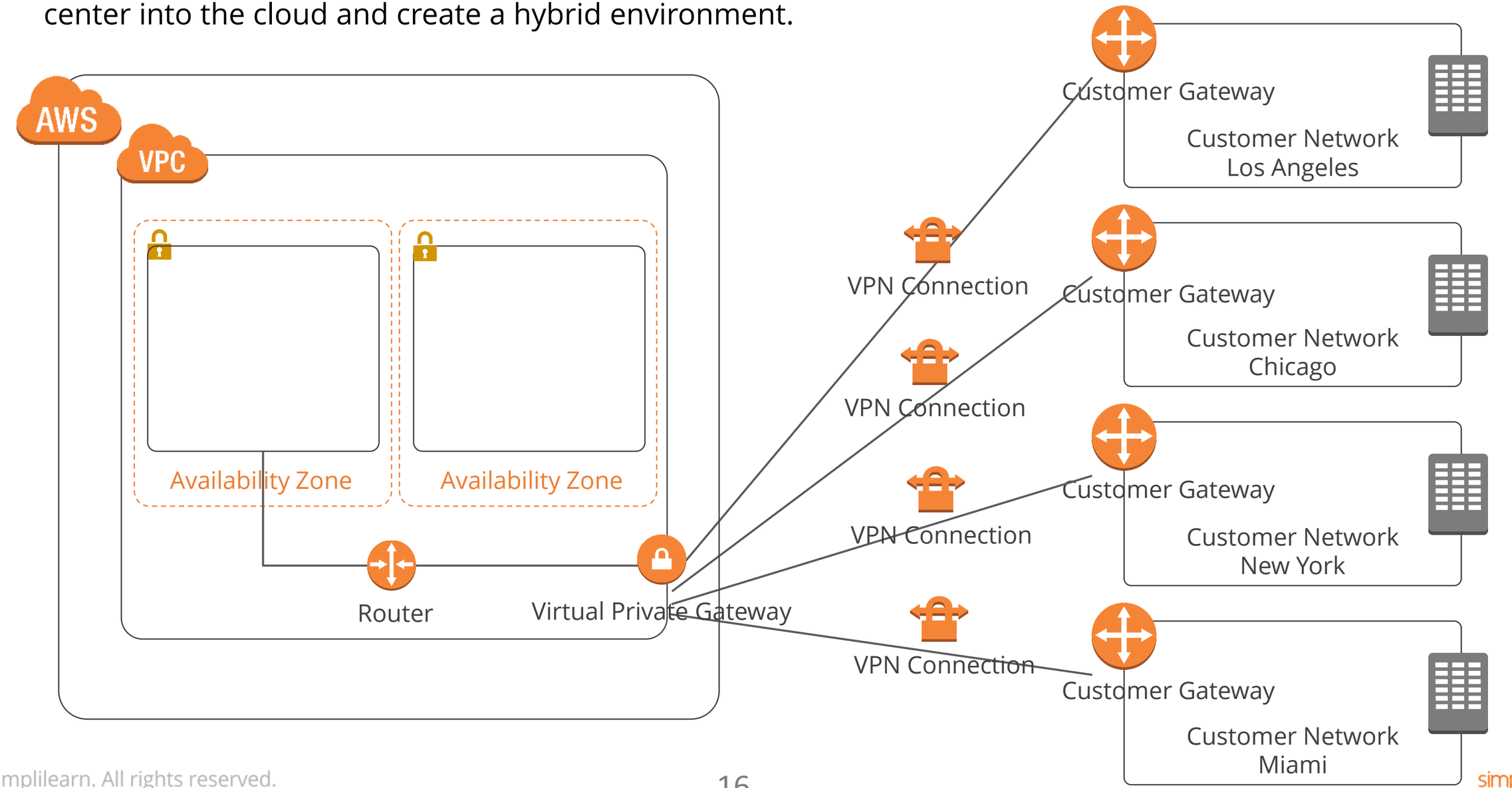
Custom VPC

The default VPC is great for launching new instances when you are testing AWS, but creating a custom VPC allows you to secure your resources.



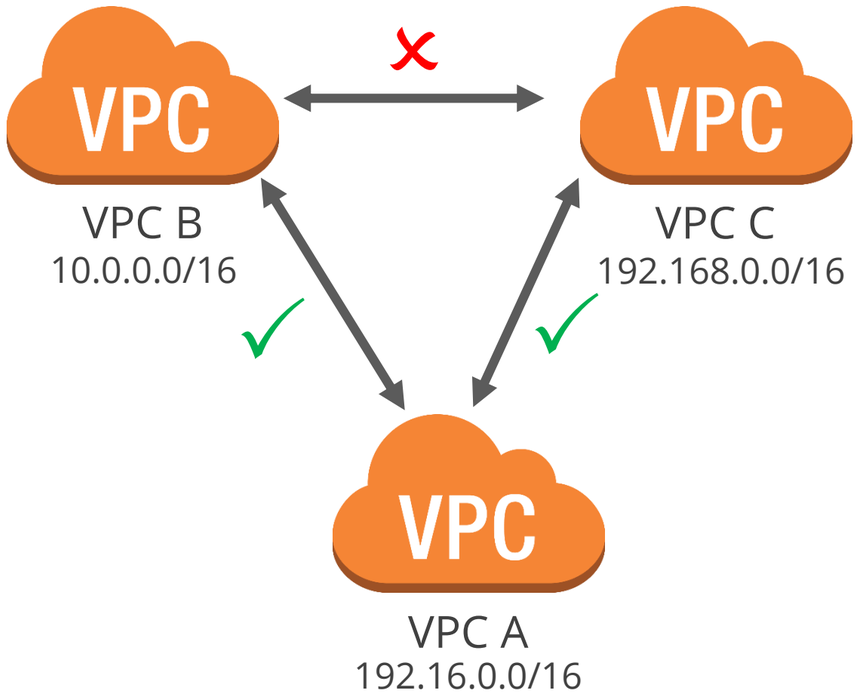
Hardware VPN Access

Connect your VPCs to your existing data center using Hardware VPN Access so you can extend your data center into the cloud and create a hybrid environment.



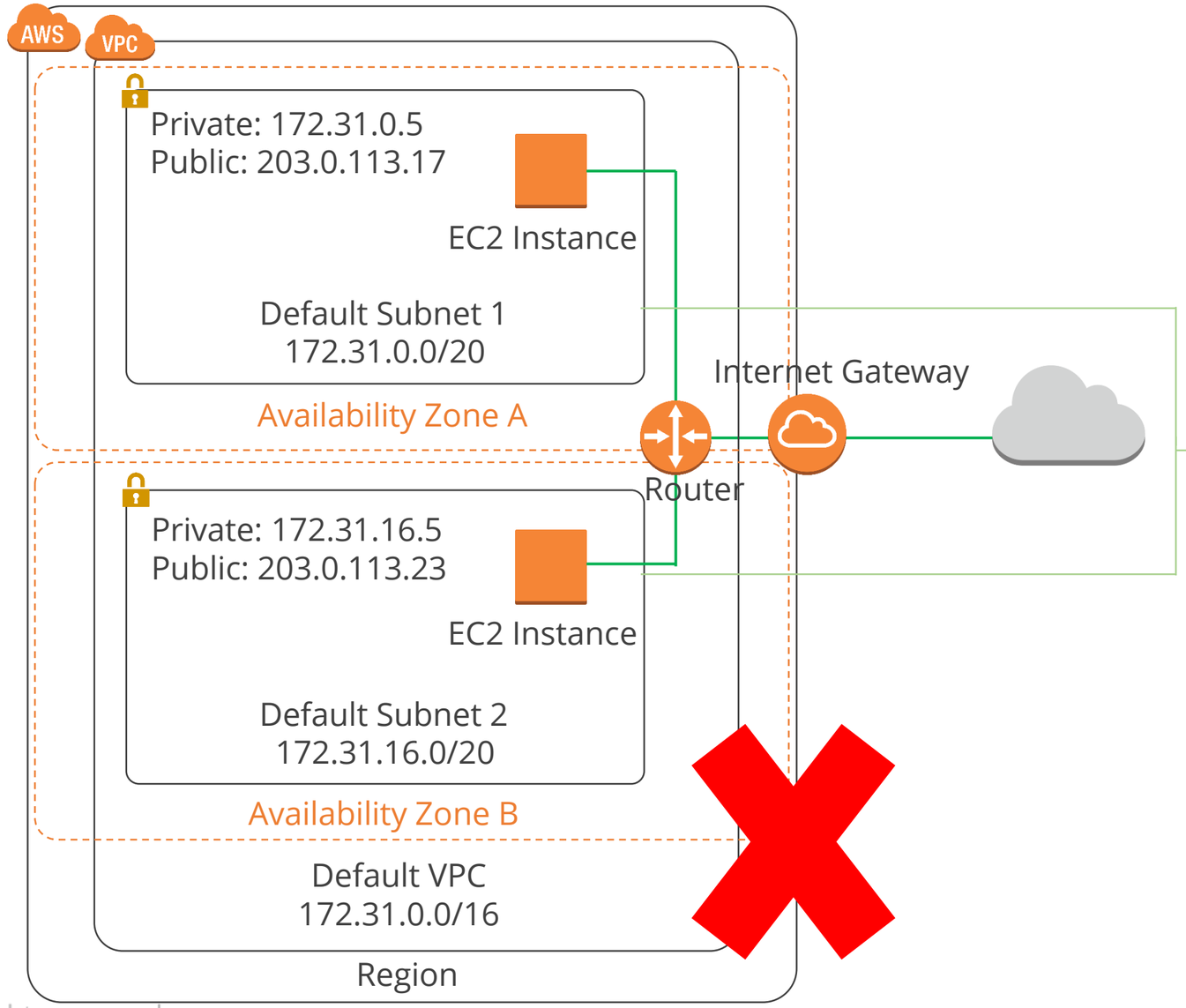
VPC Peering

VPC Peering - A peering connection allows you to route traffic between two VPCs using the private IP addresses so EC2 instances in either network can communicate directly with each other.



Default VPC Deletion

If you delete the default VPC, you have to contact AWS Support to get it restored.



Main Route Table	
Destination	**Target**
172.31.0.0/16	local
0.0.0.0/0	igw-id

Demo 1: Creating a custom VPC

Demonstrate how to create a custom VPC.

Knowledge Check

KNOWLEDGE CHECK

What is attached to the default VPC?

a. Availability Zone

b. VPC Peering Connection

c. Internet Gateway

d. None of the above

KNOWLEDGE CHECK

What is attached to the default VPC?

a. Availability Zone

b. VPC Peering Connection

c. Internet Gateway

d. None of the above

The correct answer is **c.**

The default VPC has an IGW attached, meaning that each subnet is public or has Internet access. Any EC2 instance launched into the default VPC will have both a public and private IP address attached.

KNOWLEDGE CHECK	Why would you create a custom VPC?

a. To customize the VPC to your own configuration

b. To save money

c. To avoid AWS from having access to your EC2 instances

d. To make allowances for cases where you delete the default VPC

KNOWLEDGE CHECK	Why would you create a custom VPC?

a. To customize the VPC to your own configuration

b. To save money

c. To avoid AWS from having access to your EC2 instances

d. To make allowances for cases where you delete the default VPC

The correct answer is **a**.

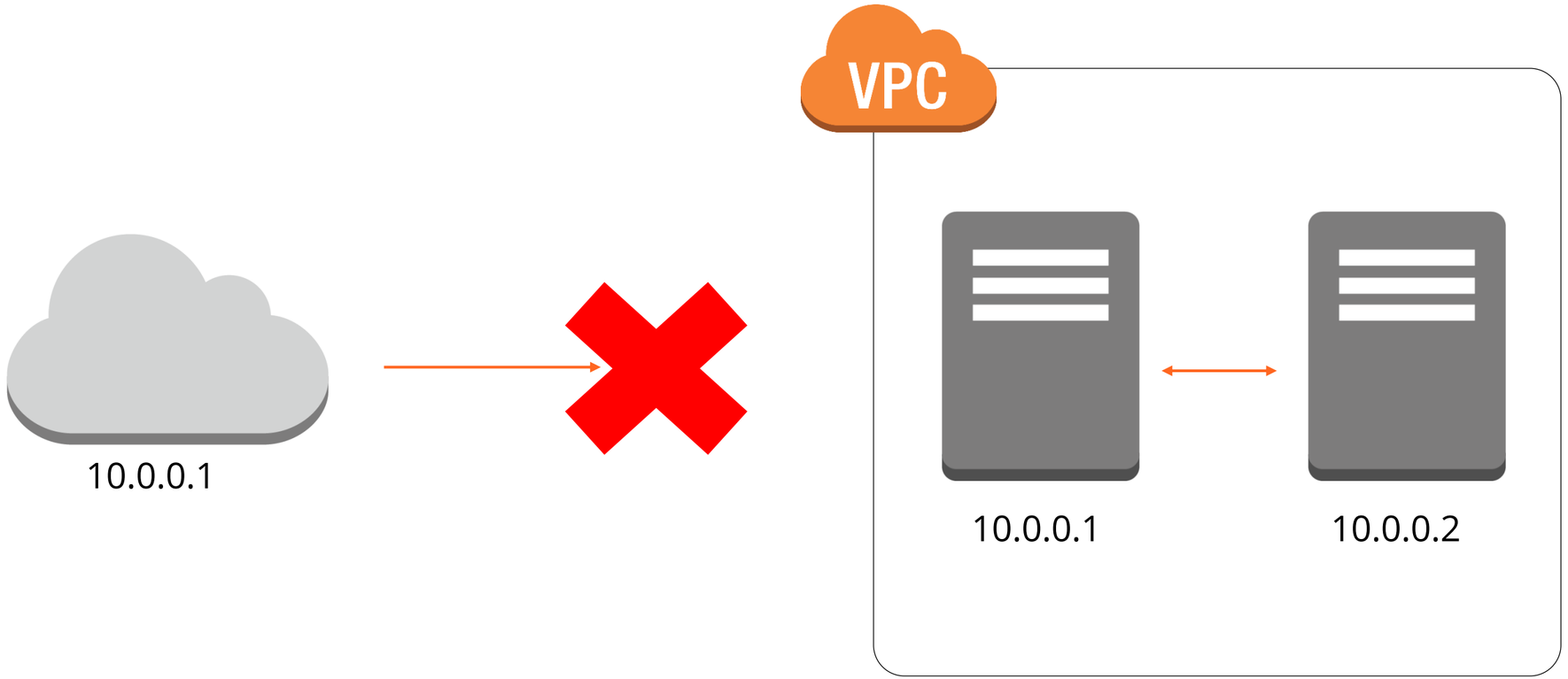
Creating a custom VPC allows you to customize your virtual network by defining your own IP address range, create subnets that are both private and public, and strengthen your security settings.

IP Addresses

Using IP Addresses in Amazon VPC

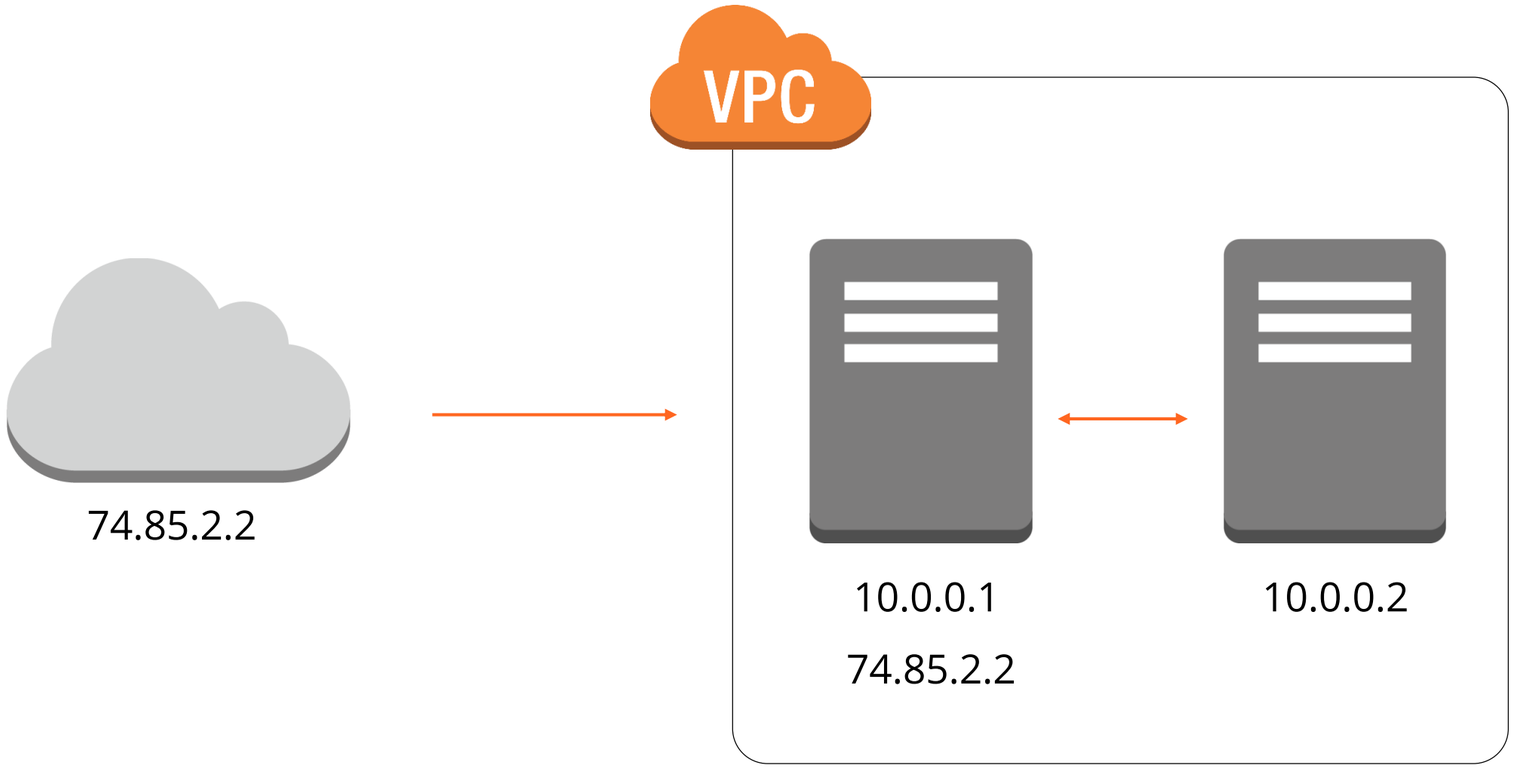
Private IP Addresses

Private IP address is not reachable over the Internet.
It is used for communication between instances in the same network. When you launch a new instance, it's given a private IP address and an internal DNS host name that resolves to the private IP address of the instance.



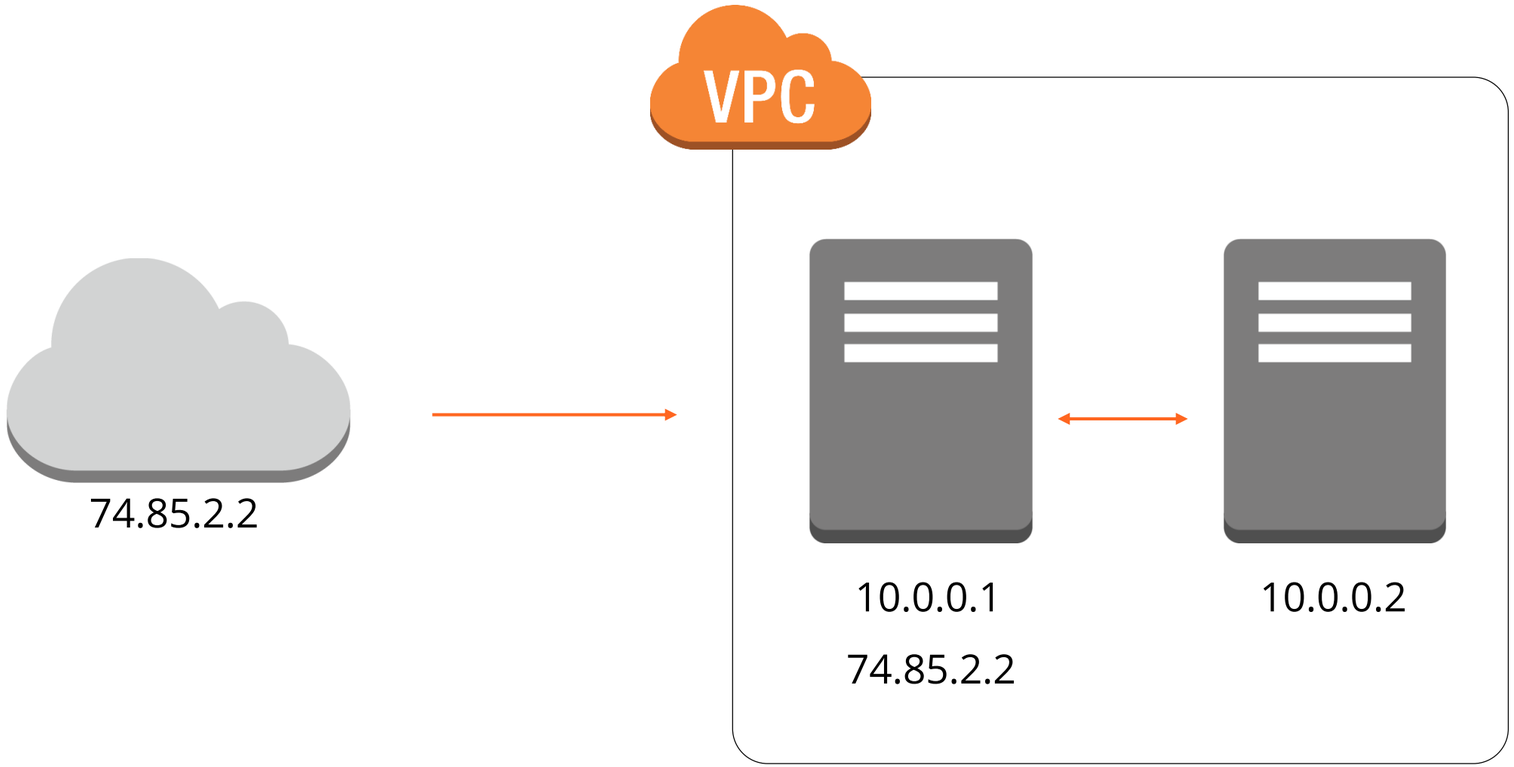
Public IP Addresses

A public IP address is reachable from the Internet. You can use public IP addresses for communication between your instances and the Internet.



Elastic IP Addresses

Elastic IP address is a static/public persistent public IP address that is allocated to your account and can be associated to and from your instances as required.



Demo 2: Creating an Elastic IP Address

Demonstrate how to create an Elastic IP Address.

Knowledge Check

KNOWLEDGE CHECK

When is an Elastic IP address released from your account?

a. When the EC2 instance it is attached to is restarted

b. When the EC2 instance it is attached to is terminated

c. Until you choose to release it

d. Until you delete the default VPC

KNOWLEDGE CHECK

When is an Elastic IP address released from your account?

a. When the EC2 instance it is attached to is restarted

b. When the EC2 instance it is attached to is terminated

c. Until you choose to release it

d. Until you delete the default VPC

The correct answer is **c**.

It remains in your account until you choose to release it; till then it can be associated with and from your instances as required.

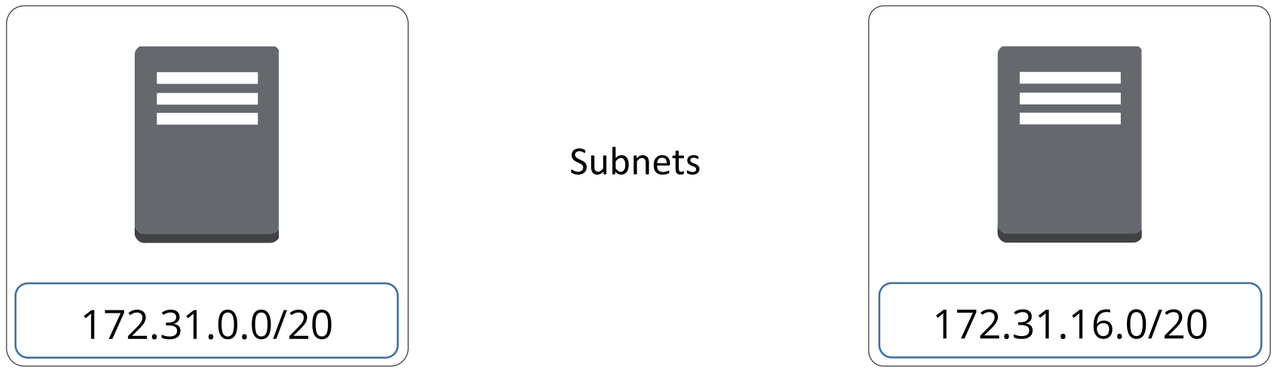
Subnets

Using subnets in Amazon VPC

Subnet Definition

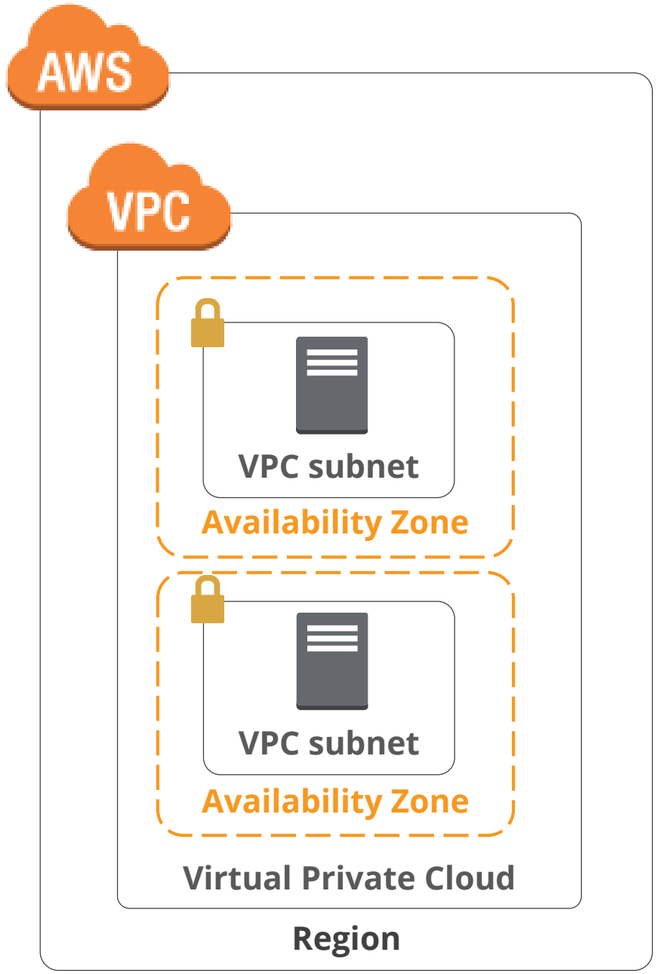
Amazon’s definition of a Subnet:

“A range of IP addresses in your VPC; you can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet and a private subnet for resources that won't be connected to the Internet.”



Subnet Diagram

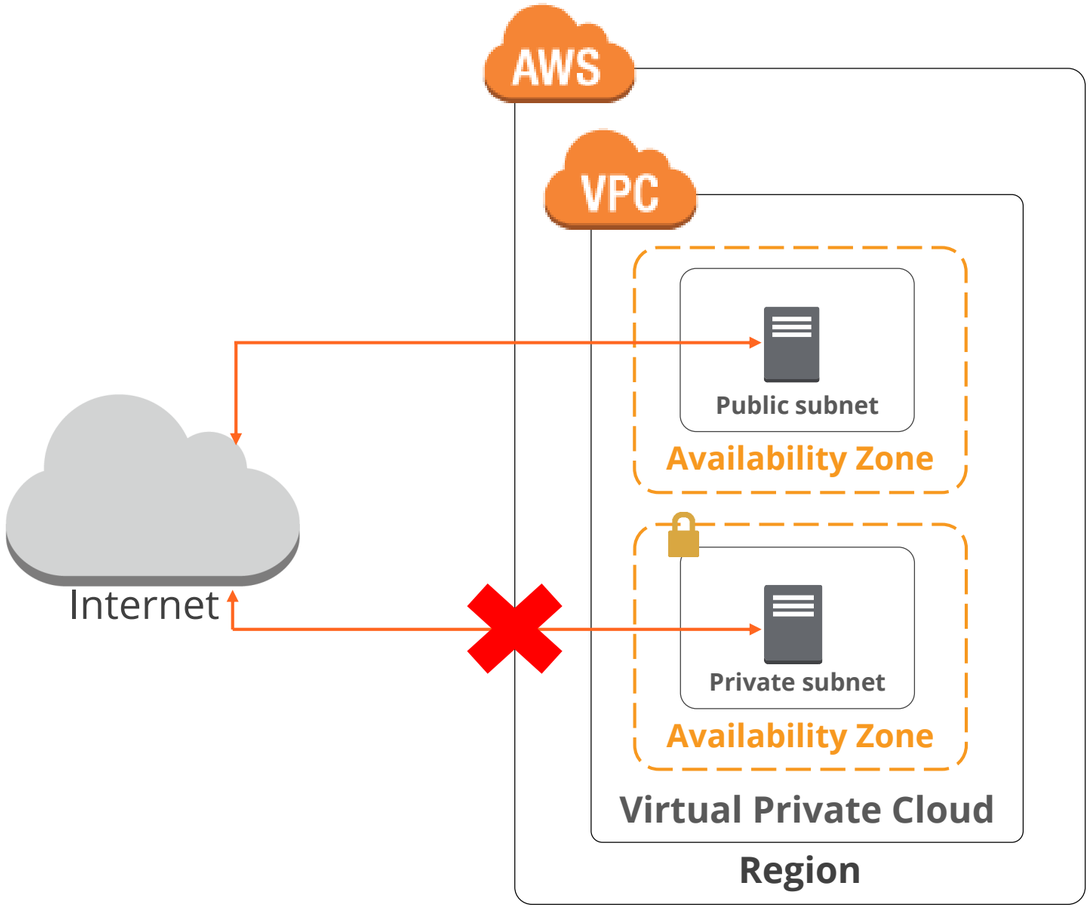
A VPC can span multiple Availability Zones, but a subnet is always mapped to a single Availability Zone.



Public and Private Subnets

Public subnets are used for resources that need to be connected to the Internet.

Private subnets are resources that don't need an Internet connection or those that you want to protect from the Internet.



Demo 3: Creating Subnets

Demonstrate how to create a public and private subnet.

Knowledge Check

KNOWLEDGE CHECK	A subnet can _____.

a. span multiple Availability Zones

b. span multiple Regions

c. provide up to 65,536 private IP addresses by default

d. only be mapped to one Availability Zone

KNOWLEDGE CHECK	A subnet can _____.

a. span multiple Availability Zones

b. span multiple Regions

c. provide up to 65,536 private IP addresses by default

d. only be mapped to one Availability Zone

The correct answer is **d**.

A subnet can only be mapped to one Availability Zone and the default subnet is always /20, which provides up to 4,096 addresses per subnet, a few of which are reserved for AWS use.

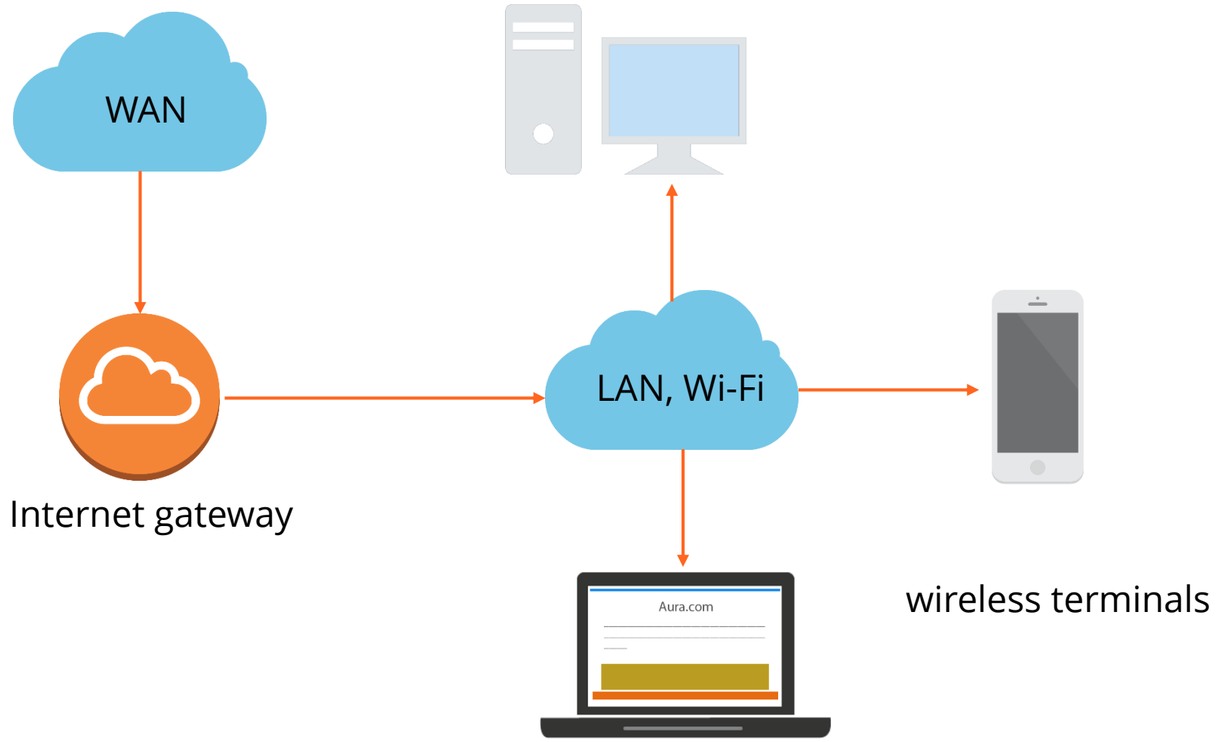
Internet Gateways

Using Internet Gateways in Amazon VPC

Internet Gateway Definition

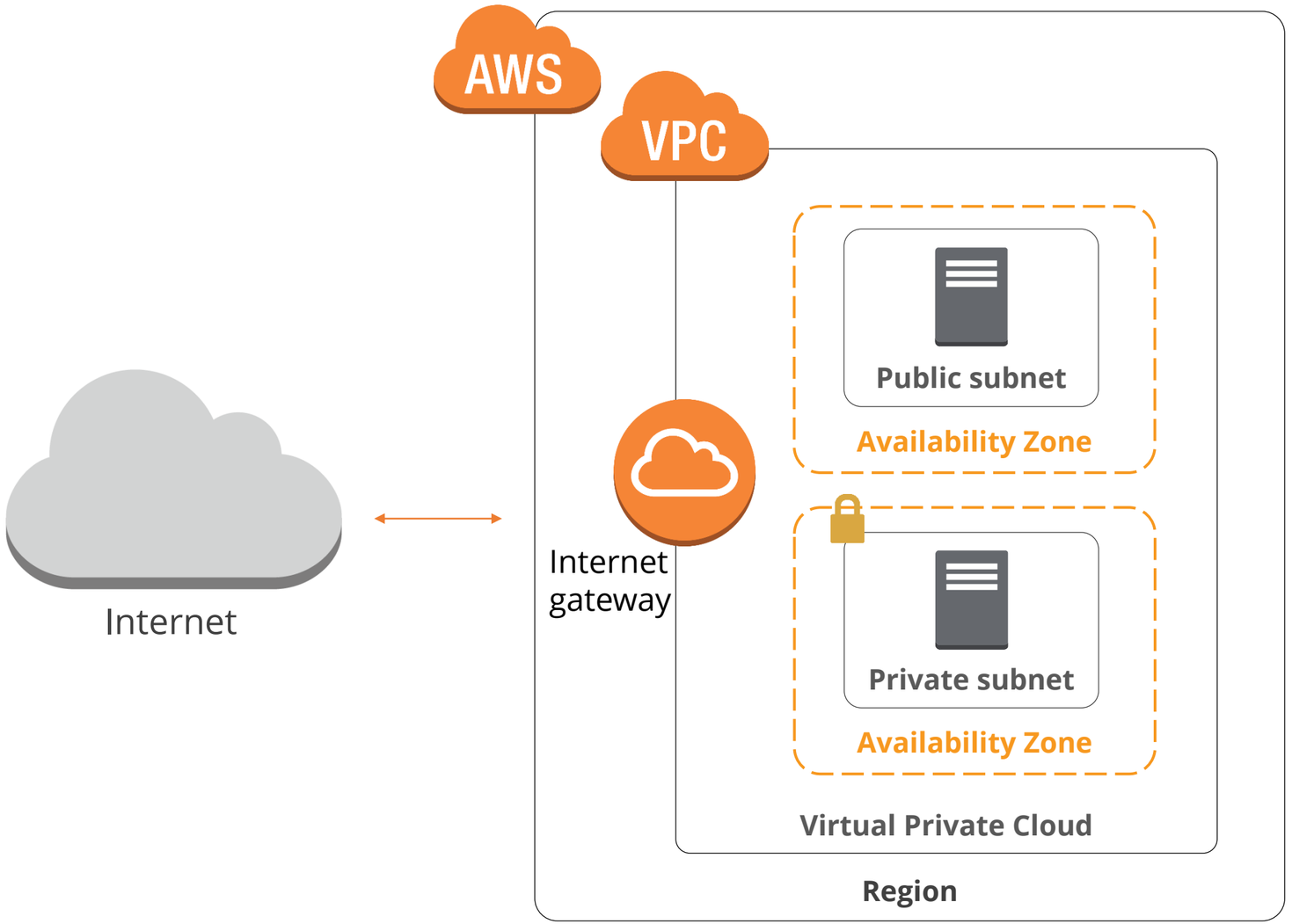
Amazon's definition of an Internet Gateway:

"An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic."



Internet Gateway Diagram

To allow your VPC the ability to connect to the Internet, you need to attach an Internet Gateway.



Internet Gateway Requirements

1. An Internet gateway must be attached to your VPC.
2. All instances in your subnet must have either a public IP address or an Elastic IP address.
3. Your subnet's route table must point to the Internet gateway.
4. All network access control and security group rules must be configured to allow the required traffic to and from your instance.

Demo 4: Creating Internet Gateways

Demonstrate how to create an Internet Gateway.

Knowledge Check

KNOWLEDGE CHECK	An Internet Gateway allows _____.

a. Internet access to your VPC as soon as you attach it

b. communication between instances in your VPC and the Internet

c. high bandwidth constraints on your network traffic

d. you to attach one Internet Gateway per subnet

KNOWLEDGE CHECK	An Internet Gateway allows _____.

a. Internet access to your VPC as soon as you attach it

b. communication between instances in your VPC and the Internet

c. high bandwidth constraints on your network traffic

d. you to attach one Internet Gateway per subnet

The correct answer is **b.**

An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic. Once attached to your VPC, there are several other steps that must be met before Internet access is available.

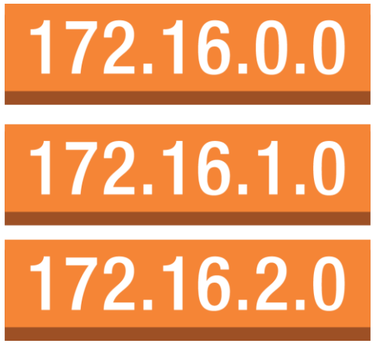
Route Tables

Using Route Tables in Amazon VPC

Route Table Overview

Amazon's definition of a route table:
"A route table contains a set of rules, called routes, which are used to determine where network traffic is directed.

Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table."

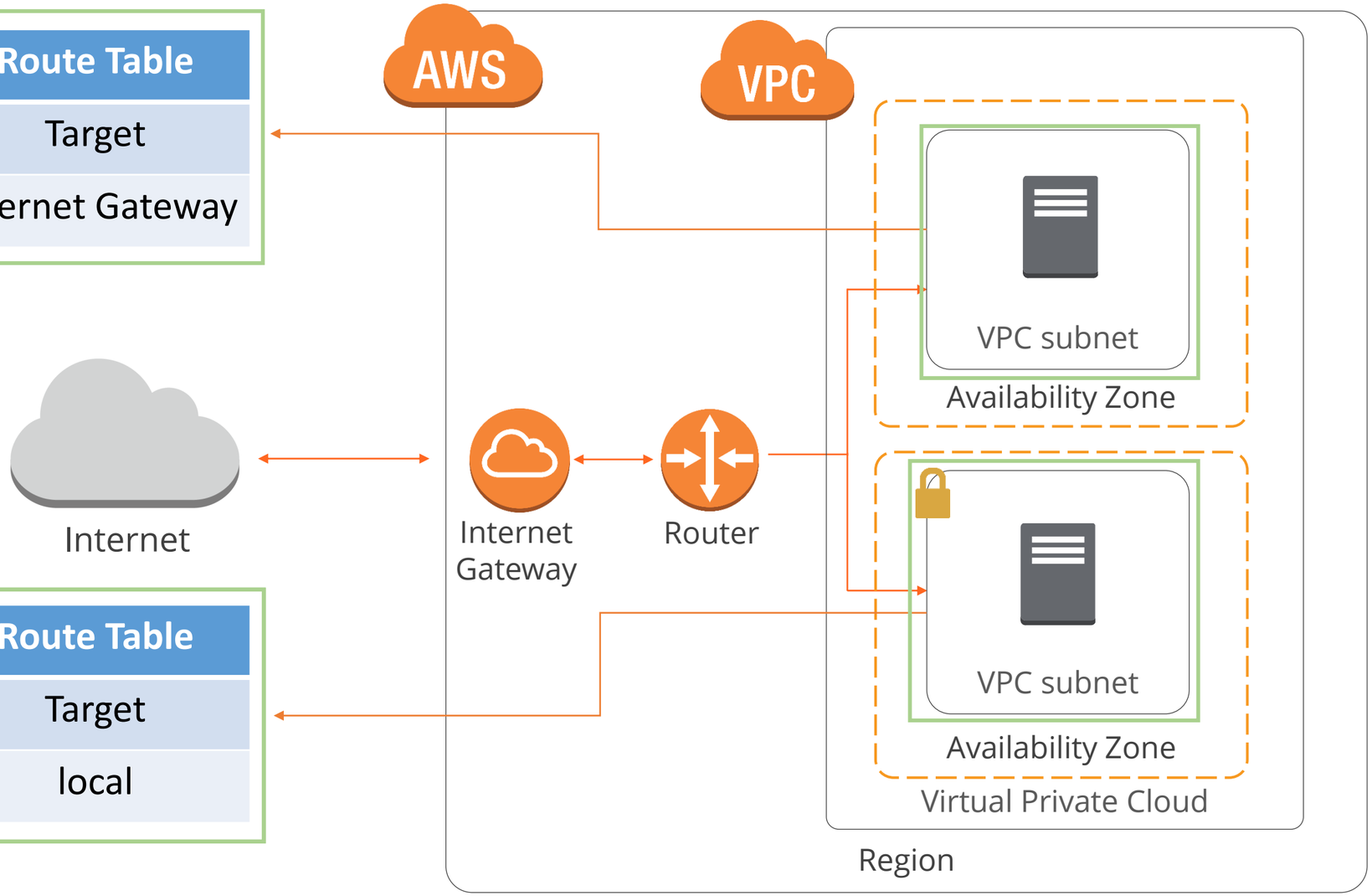


Route Table

Internet Gateway Diagram

Every VPC has a default route table. It is best to leave it in its original state and create a new route table to customize the network traffic routes.

Custom	Route Table
Destination	Target
0.0.0.0/0	Internet Gateway



Main	Route Table
Destination	Target
10.0.0.0/16	local

Demo 5: Creating Route Tables

Demonstrate how to create a custom route table.

Knowledge Check

KNOWLEDGE CHECK	Which of the following is NOT true about route tables?

a. A route table contains a set of rules, called routes, which is used to determine where network traffic is directed.

b. Multiple subnets can be associated with the same route table.

c. It is recommended to only use the default route table.

d. Each subnet in your VPC must be associated with a route table.

KNOWLEDGE CHECK	Which of the following is NOT true about route tables?

a. A route table contains a set of rules, called routes, which is used to determine where network traffic is directed.

b. Multiple subnets can be associated with the same route table.

c. It is recommended to only use the default route table.

d. Each subnet in your VPC must be associated with a route table.

The correct answer is **c.**

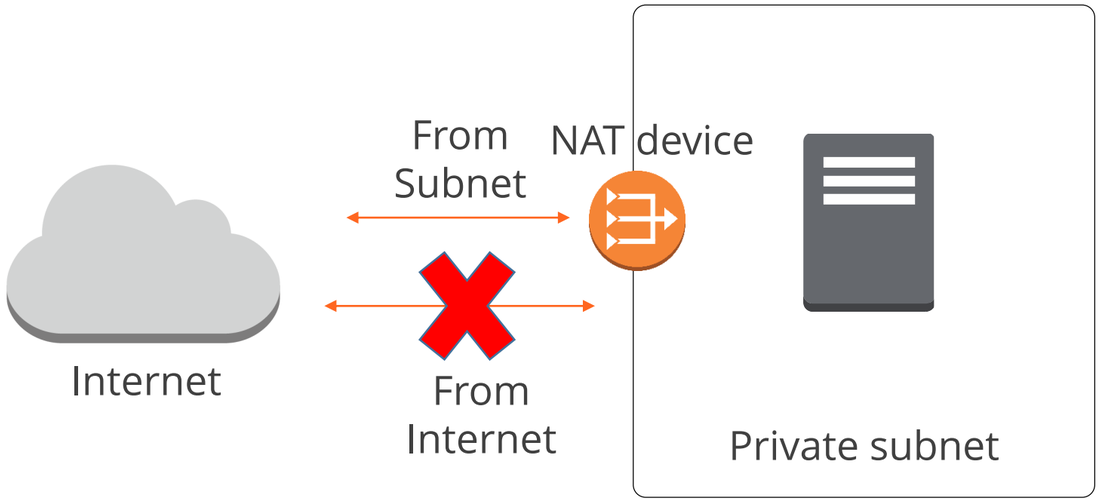
Every VPC has a default route table. It's good practice to leave this in its original state and create a new route table to customize the network traffic routes.

NAT Devices

Using NAT devices in Amazon VPC

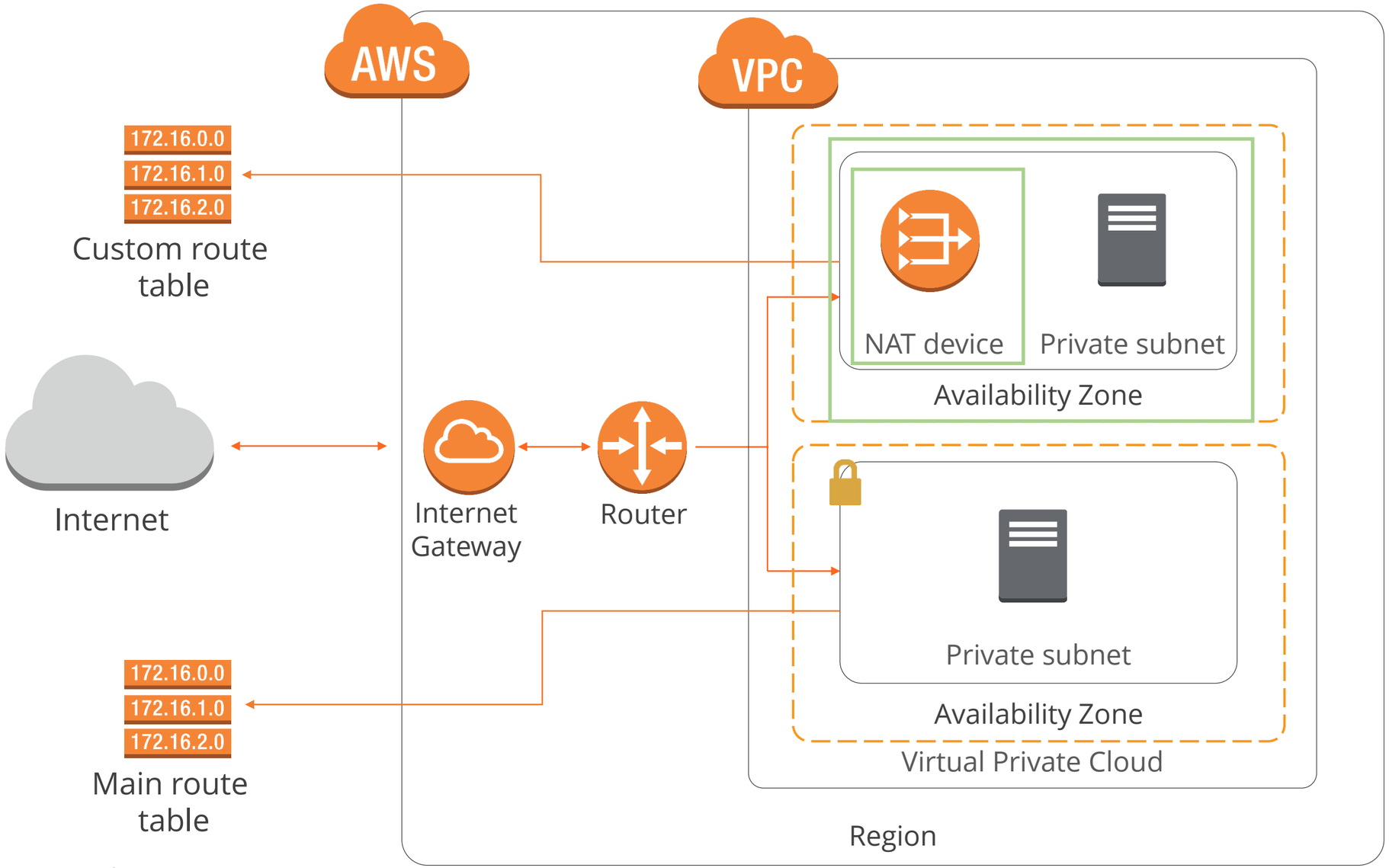
NAT Devices Overview

You can use a Network Address Translation (NAT) device to enable instances in a private subnet to connect to the Internet or other AWS services, but prevents the Internet from initiating connections with the instances.



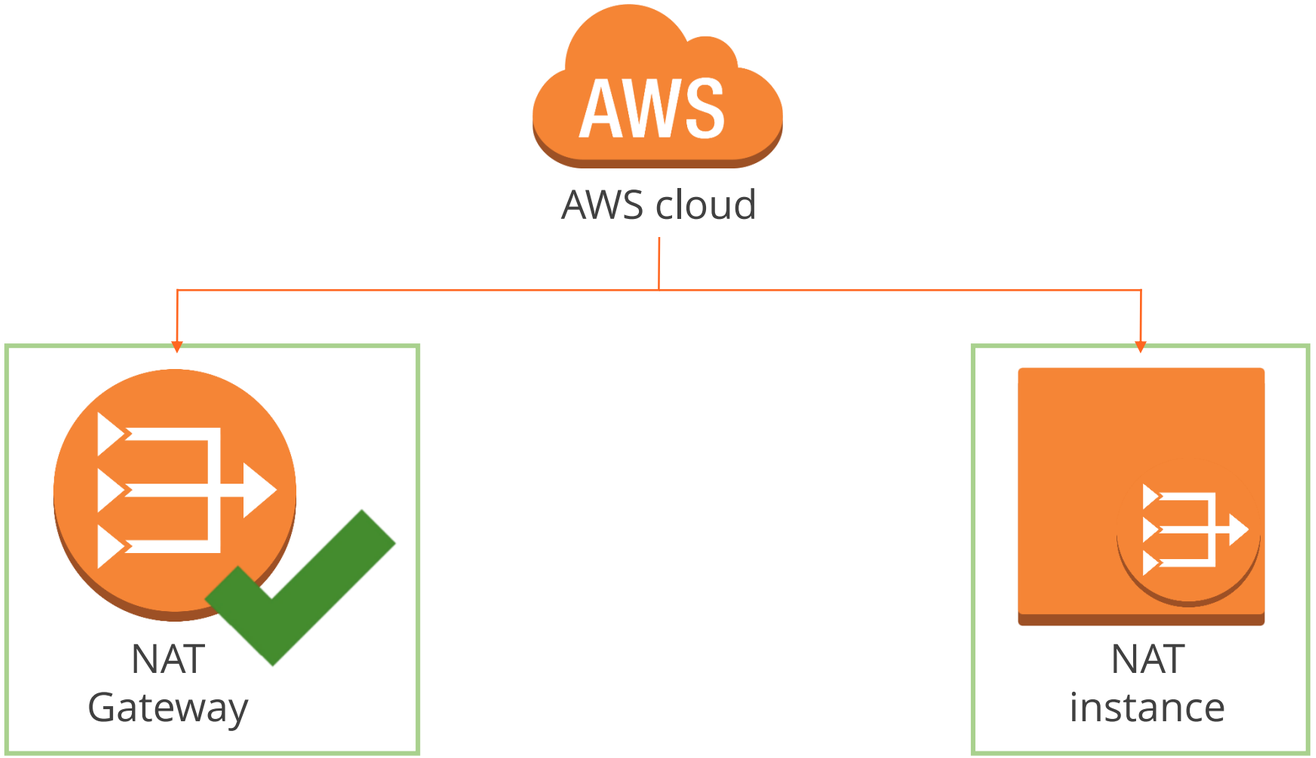
NAT Devices Overview (contd.)

You can connect your private subnet database to other AWS resources if you use a NAT device.



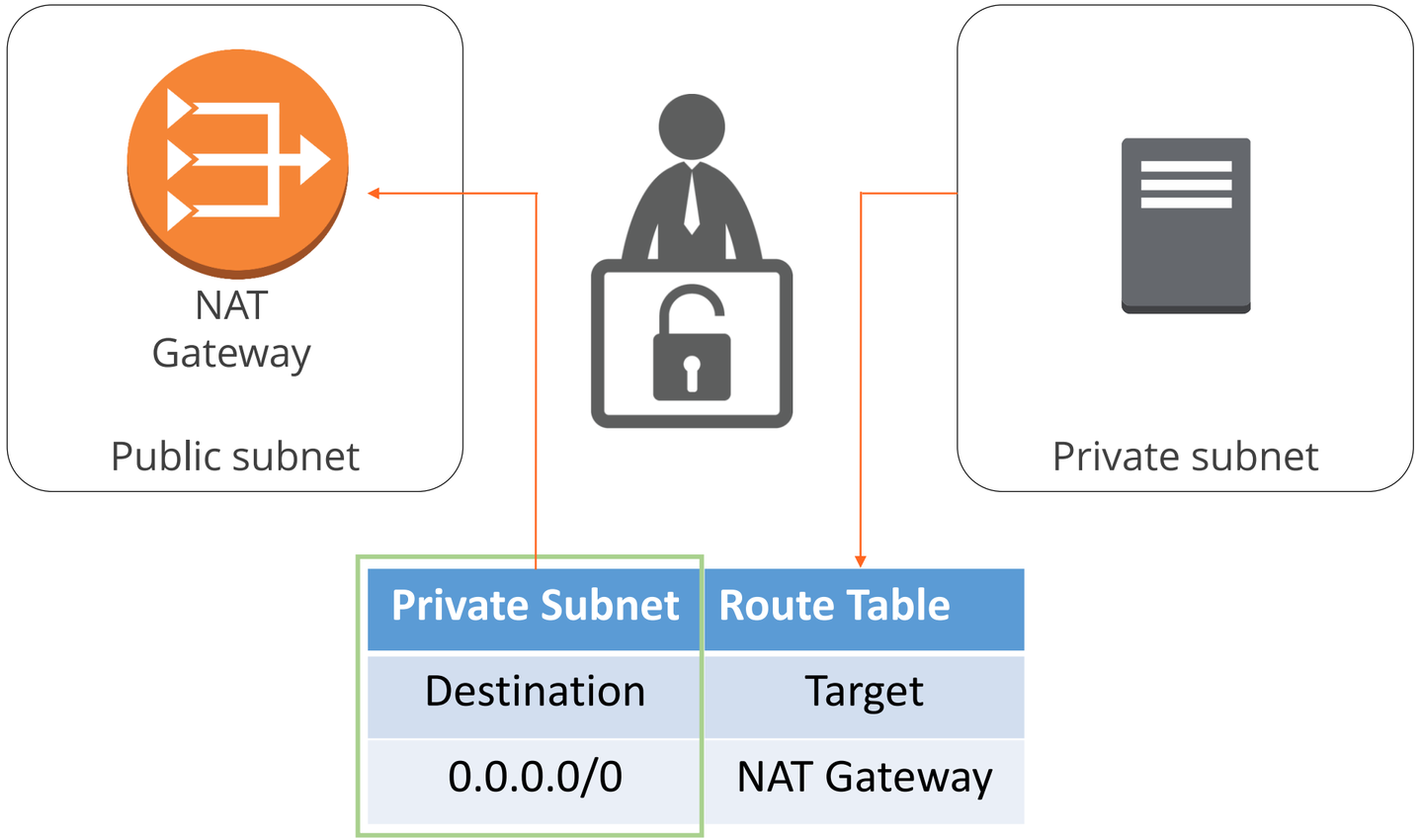
NAT Gateway versus NAT Device

AWS provides two kinds of NAT devices: a NAT gateway or a NAT instance.



NAT Gateway

A NAT Gateway must be launched into a public subnet.



Private Subnet	Route Table
Destination	Target
0.0.0.0/0	NAT Gateway

Demo 6: Creating a NAT Gateway

Demonstrate how to create a NAT Gateway.

Knowledge Check

KNOWLEDGE CHECK	Why does AWS recommend using a NAT Gateway?

a. It’s a managed service.

b. It provides better availability and bandwidth than NAT instances.

c. It provides redundancy in the AZ where it is created.

d. All of the above are correct.

KNOWLEDGE CHECK	Why does AWS recommend using a NAT Gateway?

a. It’s a managed service.

b. It provides better availability and bandwidth than NAT instances.

c. It provides redundancy in the AZ where it is created.

d. All of the above are correct.

The correct answer is **d**.

AWS recommends a NAT Gateway as it’s a managed service that provides better availability and bandwidth than NAT instances. Each NAT gateway is created in a specific Availability Zone and implemented with redundancy in that zone.

KNOWLEDGE CHECK

What does a NAT Gateway require to function properly?

a. To be launched in a private subnet and have an Elastic IP address

b. To be launched in a public subnet and have an Elastic IP address

c. To be launched in a private subnet and have an private IP address

d. To be launched in a public subnet and have an private IP address

KNOWLEDGE CHECK

What does a NAT Gateway require to function properly?

a. To be launched in a private subnet and have an Elastic IP address

b. To be launched in a public subnet and have an Elastic IP address

c. To be launched in a private subnet and have an private IP address

d. To be launched in a public subnet and have an private IP address

The correct answer is **b**.

A NAT Gateway must be launched into a public subnet and have an Elastic IP address as it needs Internet connectivity.

Security Groups

Using Security Groups in Amazon VPC

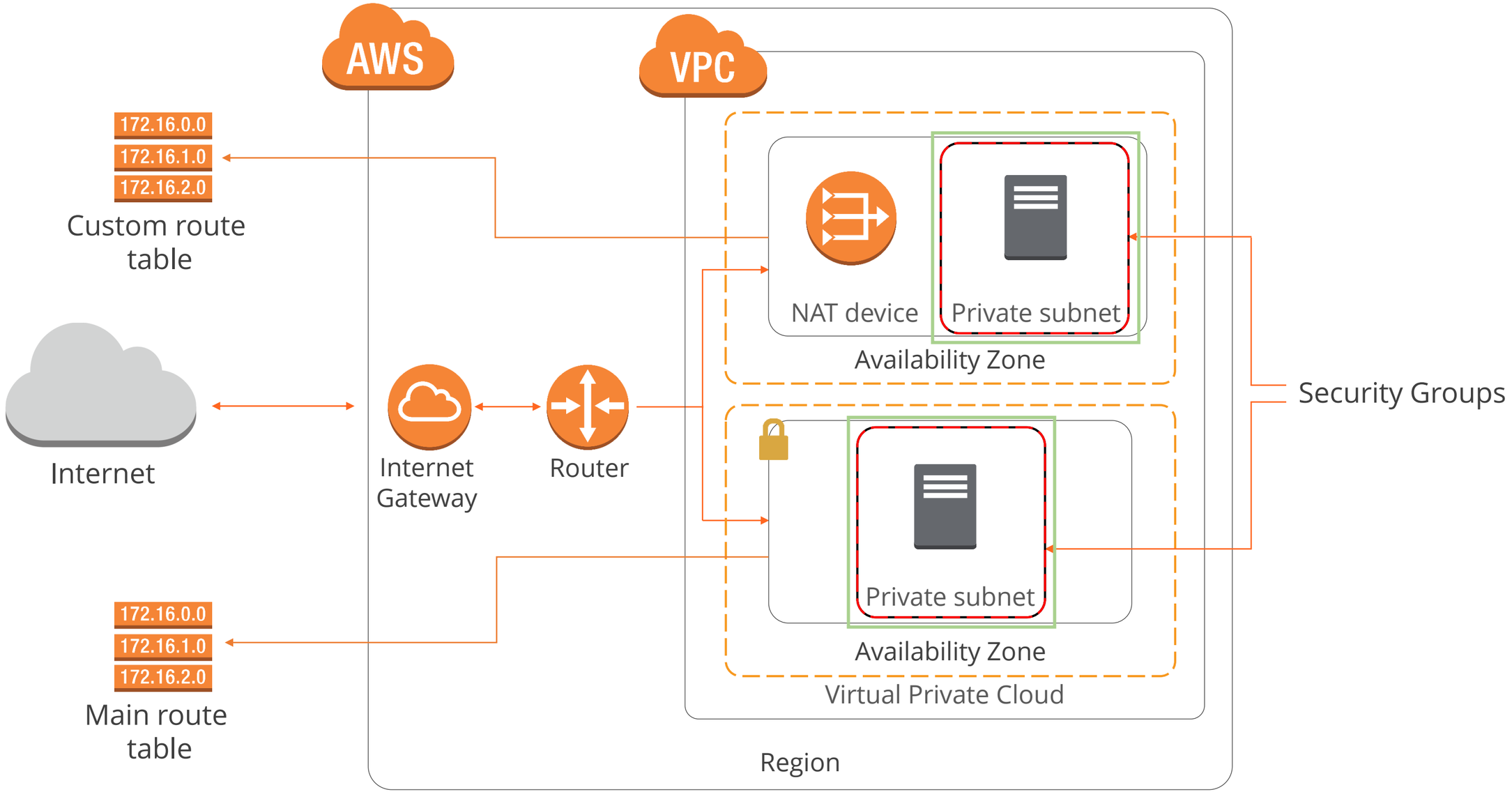
Security Groups Overview

Amazon's definition of a Security Group:

"A security group acts as a virtual firewall that controls the traffic for one or more instances. You add rules to each security group that allow traffic to or from its associated instances."

Security Group Diagram

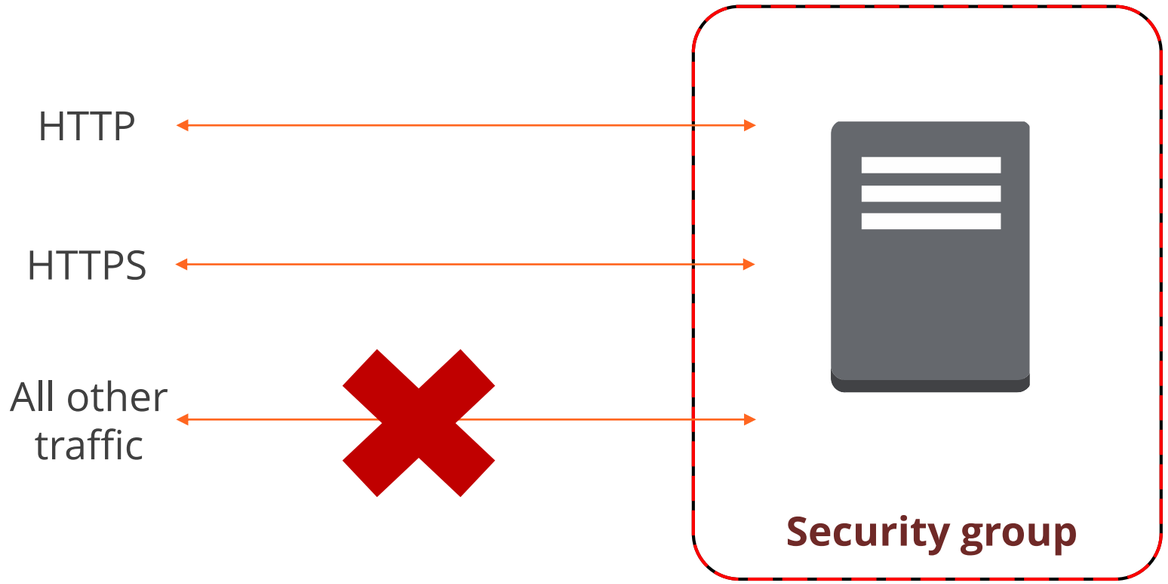
Security Groups control what can and what cannot access our instances that reside in the VPC.



Security Groups for Webservers

Let’s take a look at some examples:
The webserver needs to receive traffic from the Internet on HTTP and HTTPS ports.

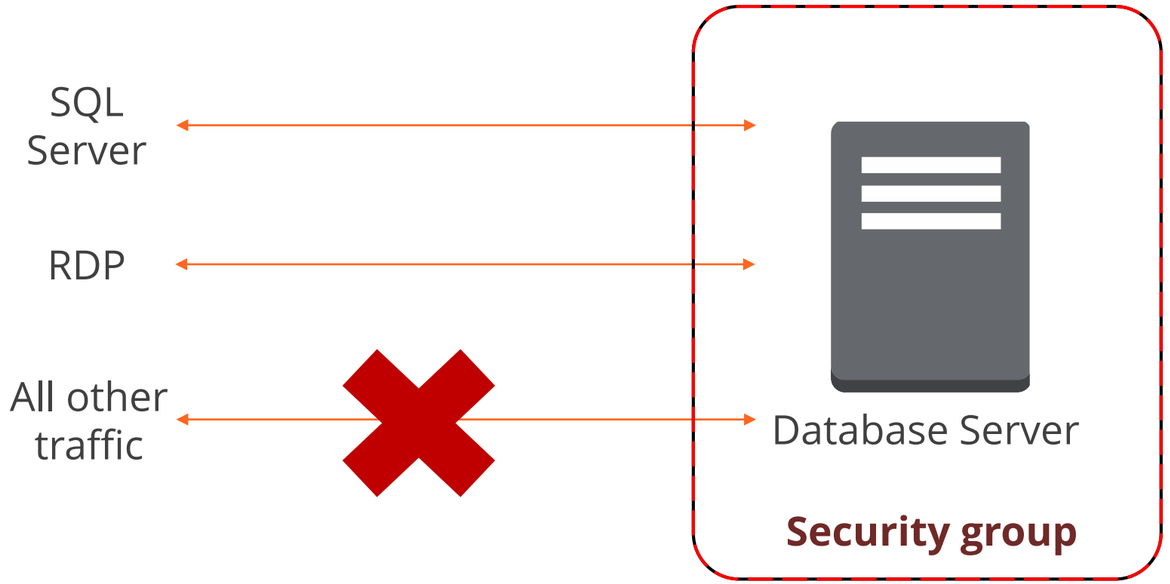
Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0



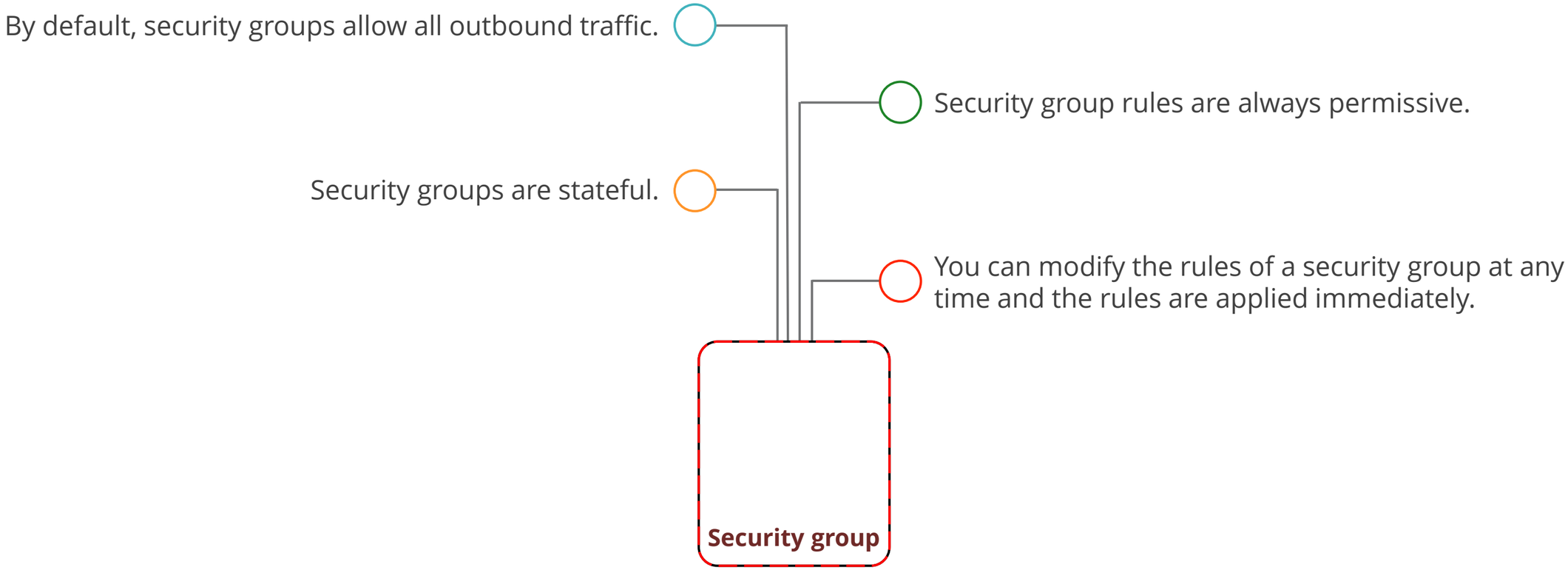
Security Groups for Database Servers

Let’s take a look at a database server security group.

Type	Protocol	Port Range	Source
MS SQL	TCP	1433	0.0.0.0/0
RDP	TCP	3389	10.0.0.0/32



Security Groups Rules



Demo 7: Creating a Security Group

Demonstrate how to create a Security Group.

Knowledge Check

KNOWLEDGE CHECK

Which of the following statements about Security Groups is NOT true?

a. Security group rules are always permissive.

b. Security groups are stateless.

c. Security group rules can be modified at any time.

d. Security Group rules are applied immediately.

KNOWLEDGE CHECK	Which of the following statements about Security Groups is NOT true?

a. Security group rules are always permissive.

b. Security groups are stateless.

c. Security group rules can be modified at any time.

d. Security Group rules are applied immediately.

The correct answer is **b**.

Security groups are stateful—for any request that comes from your instance, the response traffic for that request is automatically allowed to flow in regardless of what inbound security group rules have been configured.

Network ACL

Using Network ACLs in Amazon VPC

Network ACL Overview

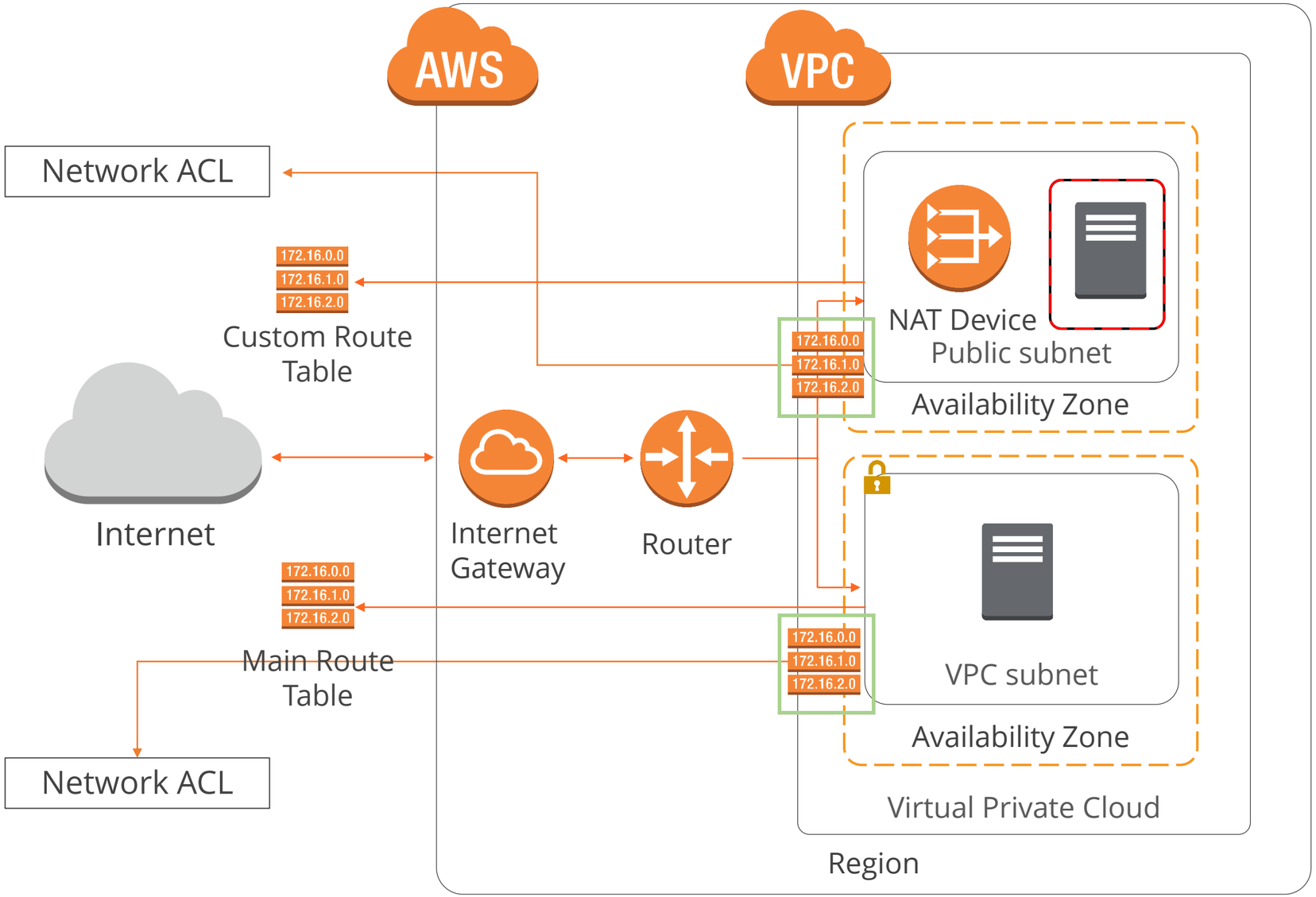
Amazon's definition of a Network ACL:

"A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC."

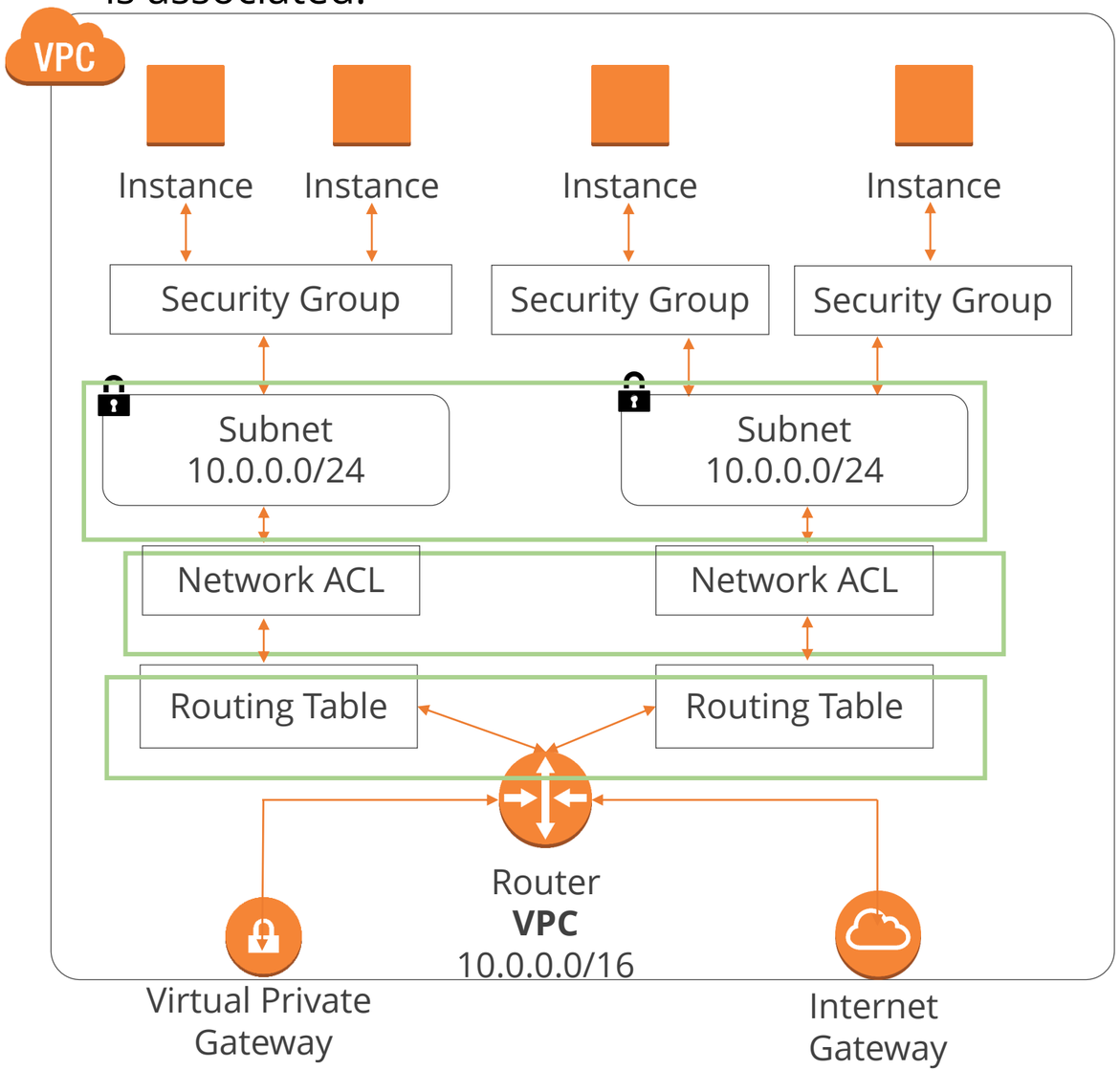
Network ACL Overview (contd.)

A Network ACL is placed between the route table and the Subnet.



Network ACL Overview (contd.)

The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated.



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

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

Network ACL Rules

Each subnet in your VPC must be associated with an ACL.

A subnet can only be associated with one ACL. However, an ACL can be associated with multiple subnets.

An ACL contains a list of numbered rules which are evaluated in order, starting with the lowest.

ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic.

Demo 8: Network ACL Overview

Demonstrate where to look for Network ACL settings.

Knowledge Check

KNOWLEDGE CHECK

Which of the following statements about Network ACLs is NOT true?

a. Each subnet in your VPC must be associated with an ACL.

b. A subnet can only be associated with one ACL; however, an ACL can be associated with multiple subnets.

c. An ACL contains a list of numbered rules which are evaluated in order, starting with the highest.

d. ACLs are stateless.

KNOWLEDGE CHECK

Which of the following statements about Network ACLs is NOT true?

a. Each subnet in your VPC must be associated with an ACL.

b. A subnet can only be associated with one ACL; however, an ACL can be associated with multiple subnets.

c. An ACL contains a list of numbered rules which are evaluated in order, starting with the highest.

d. ACLs are stateless.

The correct answer is **c**.

An ACL contains a list of numbered rules which are evaluated in order, starting with the lowest.

Amazon VPC Best Practices

Overview of Amazon VPC recommended best practices

VPC Best Practices

- Public and Private Subnets
- Provide NAT to Private Subnets
- Choose CIDR Blocks
- Amazon VPC Limits

1. The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated.
2. Use private subnets to secure resources that don't need to be available from the Internet such as database servers.

VPC Best Practices (contd.)

- Public and Private Subnets
- Provide NAT to Private Subnets
- Choose CIDR Blocks
- Amazon VPC Limits

Use NAT Gateway over NAT instances, to provide secure Internet access to your private subnets

VPC Best Practices (contd.)

- Public and Private Subnets
- Provide NAT to Private Subnets
- Choose CIDR Blocks
- Amazon VPC Limits

1. Amazon VPC can contain 16 to 65536 IP addresses.
2. Create separate Amazon VPC for Development, Staging, and Production environments.
3. Create one Amazon VPC with Separate Subnets.

VPC Best Practices (contd.)

- Public and Private Subnets
- Provide NAT to Private Subnets
- Choose CIDR Blocks
- Amazon VPC Limits

1. 5 VPCs per region
2. 200 subnets per VPC
3. 200 route tables per VPC
4. 500 security groups per VPC
5. 50 in/outbound rules per VPC
6. Some rules can be increased by raising a ticket with AWS support

VPC Best Practices (contd.)

- Security Groups and Network ACLs
- Tier Security Groups
- Standardize Security Group Naming Conventions
- Span Amazon VPC

Use Security groups for white list and Network ACLs for blacklist.

VPC Best Practices (contd.)

- Security Groups and Network ACLs
- Tier Security Groups
- Standardize Security Group Naming Conventions
- Span Amazon VPC

1. Create different security groups for different tiers of your infrastructure architecture inside your VPC.
2. If you create Amazon VPC security groups for each and every tier/service separately, it will be easier to open a port to a particular service.

VPC Best Practices (contd.)

- Security Groups and Network ACLs
- Tier Security Groups
- Standardize Security Group Naming Conventions
- Span Amazon VPC

1. Following a security group naming convention inside Amazon VPC will improve operations/management for large scale deployments inside VPC.
2. It avoids manual errors, leaks, and saves cost and time.

VPC Best Practices (contd.)

- Security Groups and Network ACLs
- Tier Security Groups
- Standardize Security Group Naming Conventions
- Span Amazon VPC

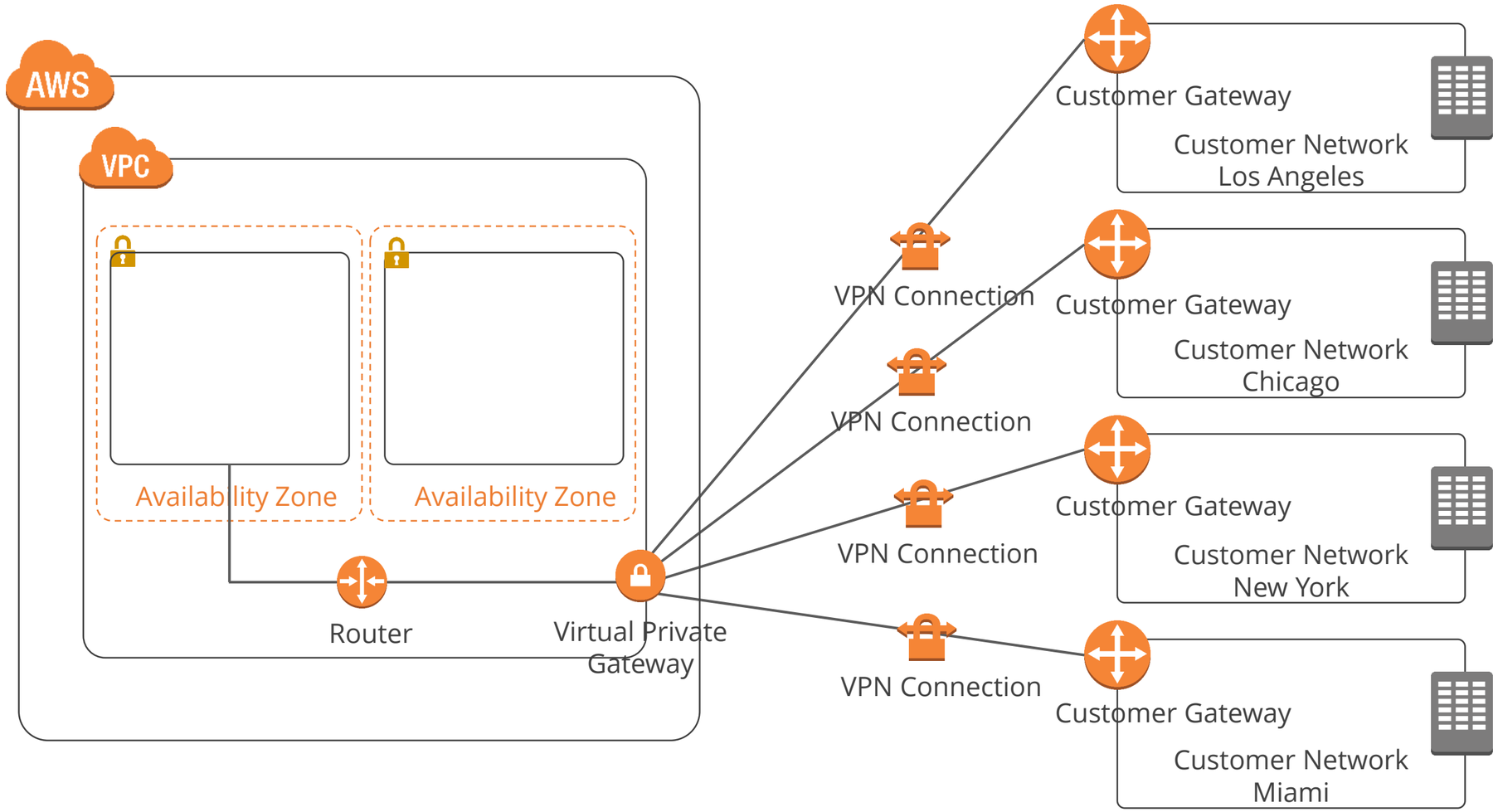
Span your Amazon VPC across multiple subnets in multiple Availability Zones inside a Region. This helps in architecting high availability inside your Amazon VPC.

Amazon VPC Costs

Overview of the Amazon VPC associated costs

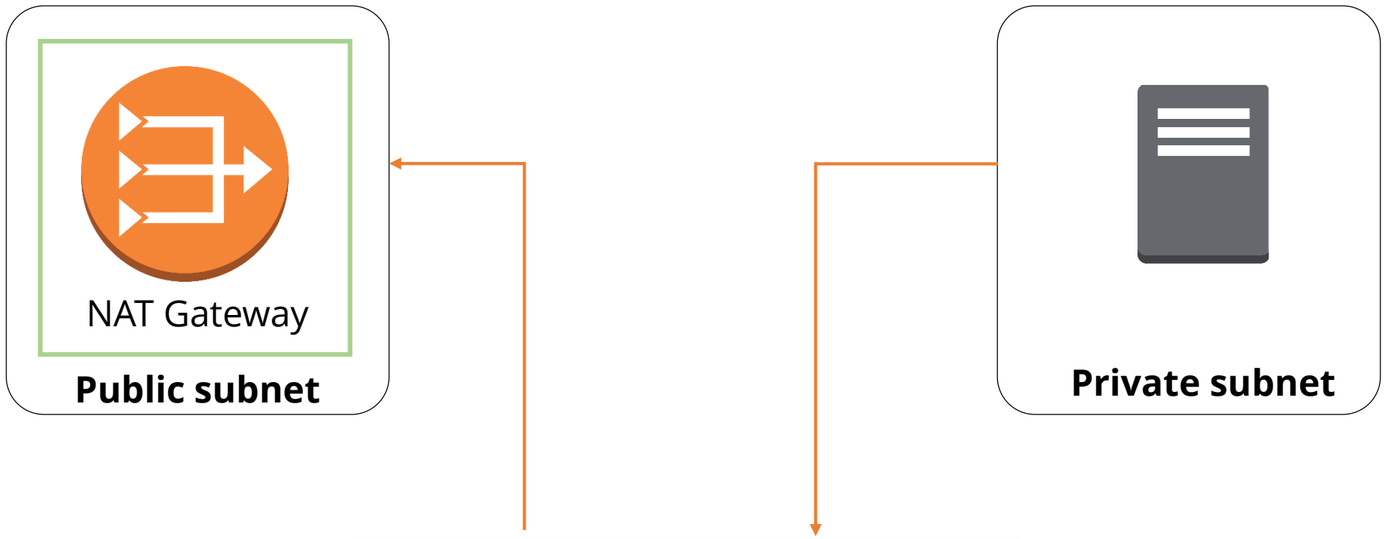
Amazon VPC Costs

If you create a hardware VPN Connection to your VPC using a Virtual Private Gateway, you are charged for each "VPN Connection-hour" that your VPN connection is provisioned and available.



Amazon VPC Costs (contd.)

If you create a NAT gateway in your VPC, you are charged for each “NAT Gateway-hour" that your NAT gateway is provisioned and available.



Private Subnet	Route Table
Destination	Target
0.0.0.0/0	NAT Gateway

Practice Assignment: Designing a Custom VPC

Create a custom VPC using the concepts learned in this lesson

Build a Custom VPC

Using the concepts learned in this lesson, recreate the custom VPC as shown in the demonstrations:

VPC Name: SIMPLILEARN_VPC
CIDR: 10.0.0.0/16
Subnets: 1 public (10.0.1.0) and 1 private (10.0.2.0) placed in separate availability zones
Internet Gateway: 1
NAT Gateway: 1
Route Table: 1 (in the public subnet)
Security Groups: SIMPLILEARN_WEBSERVER_SG and SIMPLILEARN_DBSERVER_SG

Key Takeaways

Key Takeaways

- Amazon’s definition of a VPC: “Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.”
- Private IP address is not reachable over the Internet; it’s used for communication between instances in the same network.
- A public IP address is reachable from the Internet. You can use public IP addresses for communication between your instances and the Internet.
- Elastic IP address is a static/public persistent public IP address that persists after an instance restarts.

Key Takeaways (contd.)

- AWS defines a subnet as a range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. A subnet is always mapped to a single Availability Zone. You can use a public subnet for resources that must be connected to the Internet and a private subnet for resources that won't be connected to the Internet.
- To allow your VPC the ability to connect to the Internet, you need to attach an Internet Gateway. You can only attach one IGW per VPC.
- A route table determines where network traffic is directed. It does this by defining a set of rules.
- Every subnet has to be associated with a route table and a subnet can only be associated with one route table; however, multiple subnets can be associated with the same subnet.
- You can use a NAT device to enable instances in a private subnet to connect to the Internet or other AWS services. However, it will prevent the Internet from initiating connections with the instances.

Key Takeaways (contd.)

- A security group acts as a virtual firewall that controls the traffic for one or more instances.
- You add rules to each security group that allows traffic to or from its associated instances.
- A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

This concludes the lesson “Amazon VPC.”

The next lesson is “Amazon EC2.”