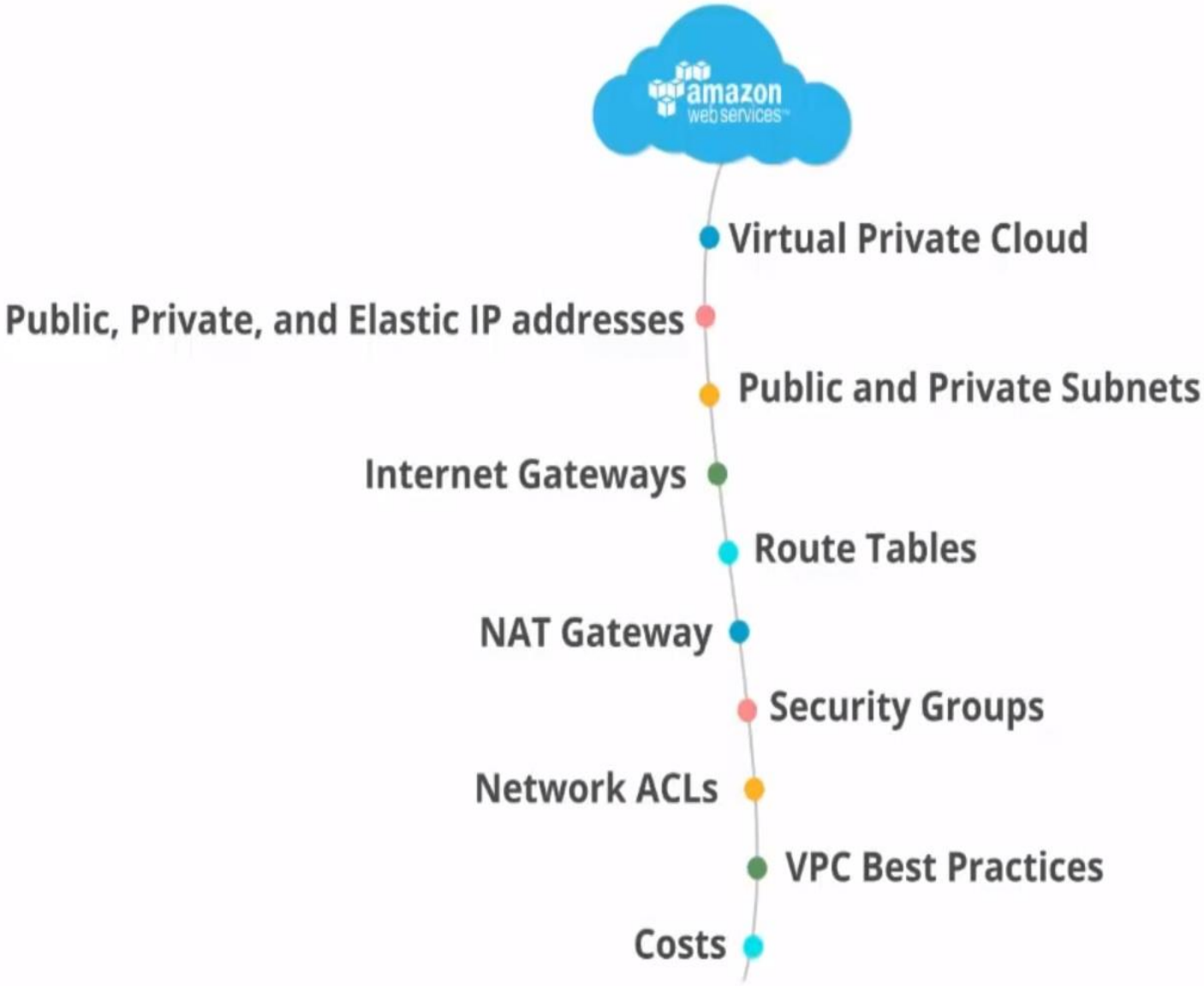
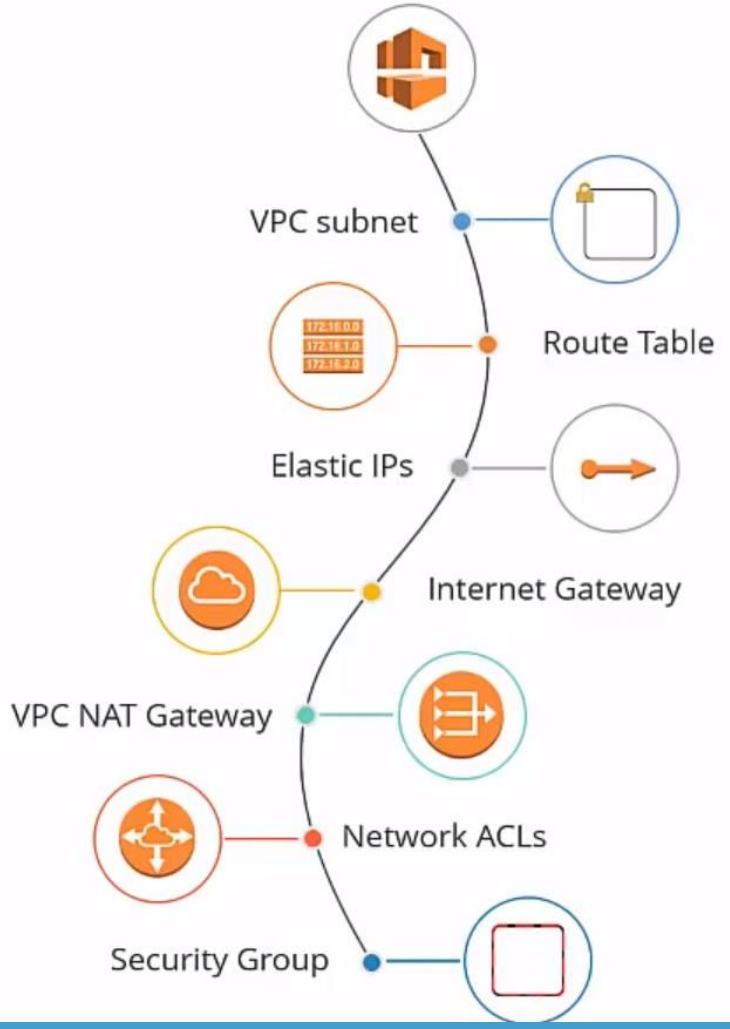
Amazon VPC Definition

Amazon's definition of a VPC:

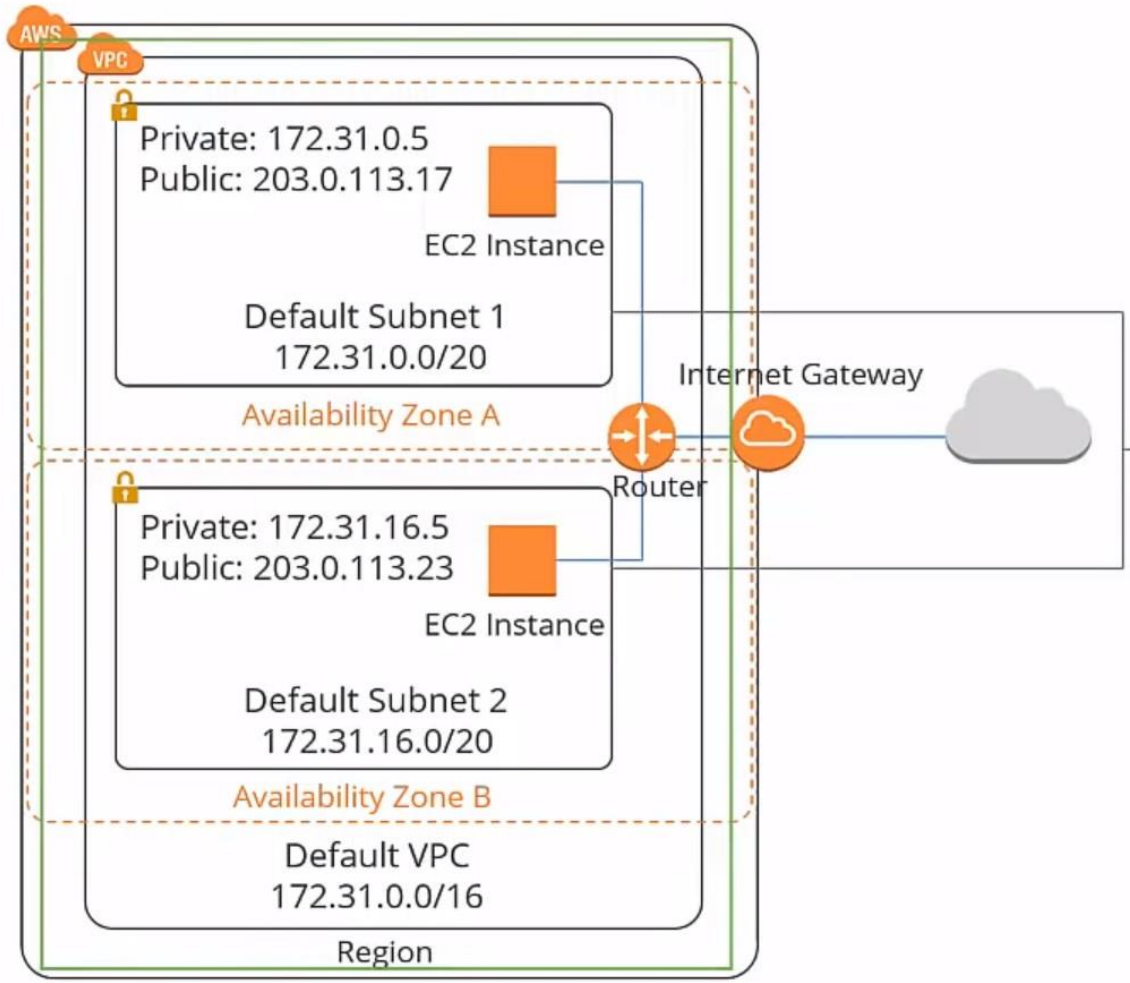
"Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure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


amazon
web services
Virtual Private Cloud
Public, Private, and Elastic IP addresses
Public and Private Subnets
Internet Gateways
Route Tables
NAT Gateway
Security Groups
Network ACLs
VPC Best Practices
Costs

Amazon VPC Terminology

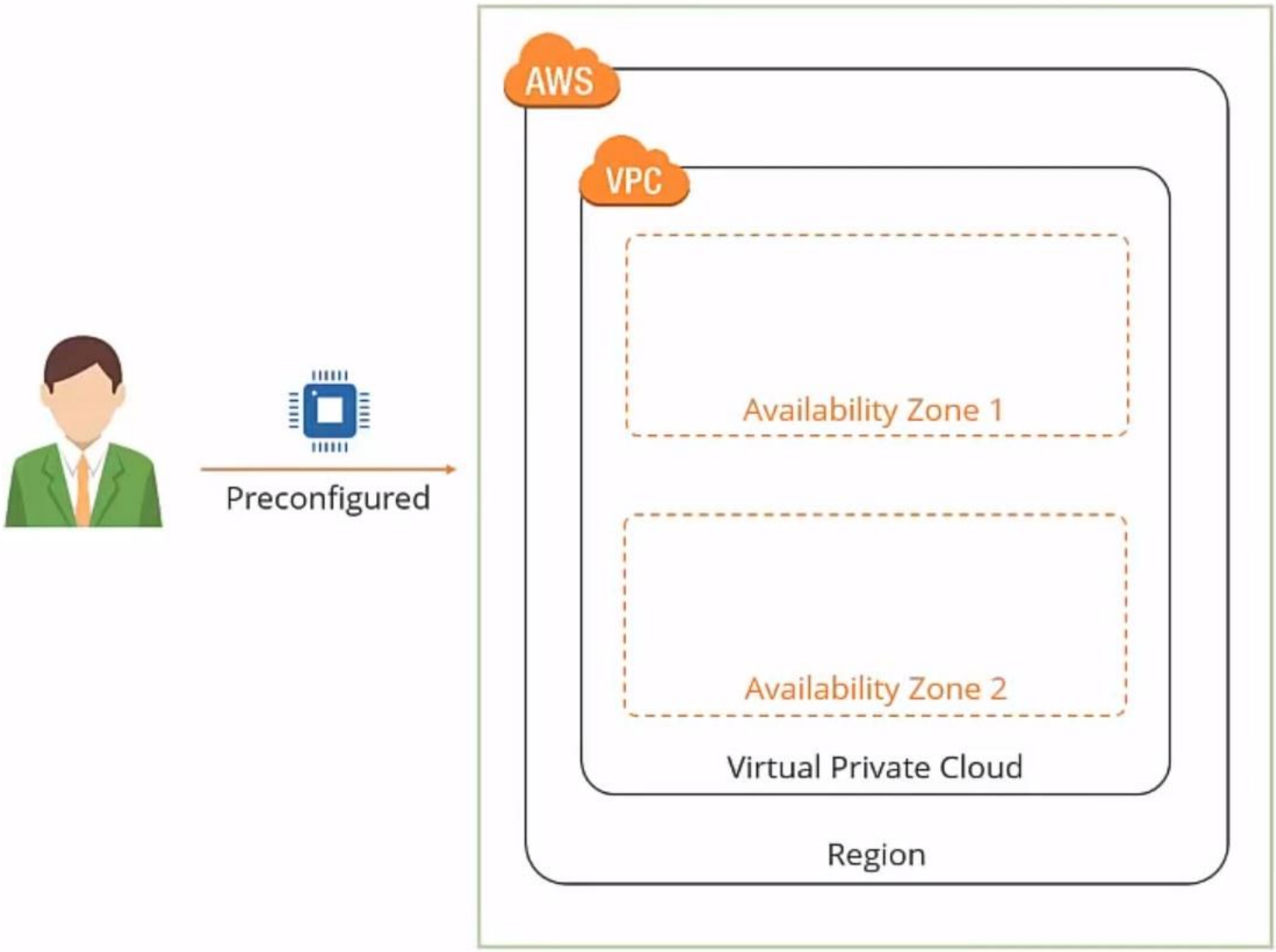


Amazon VPC Diagram

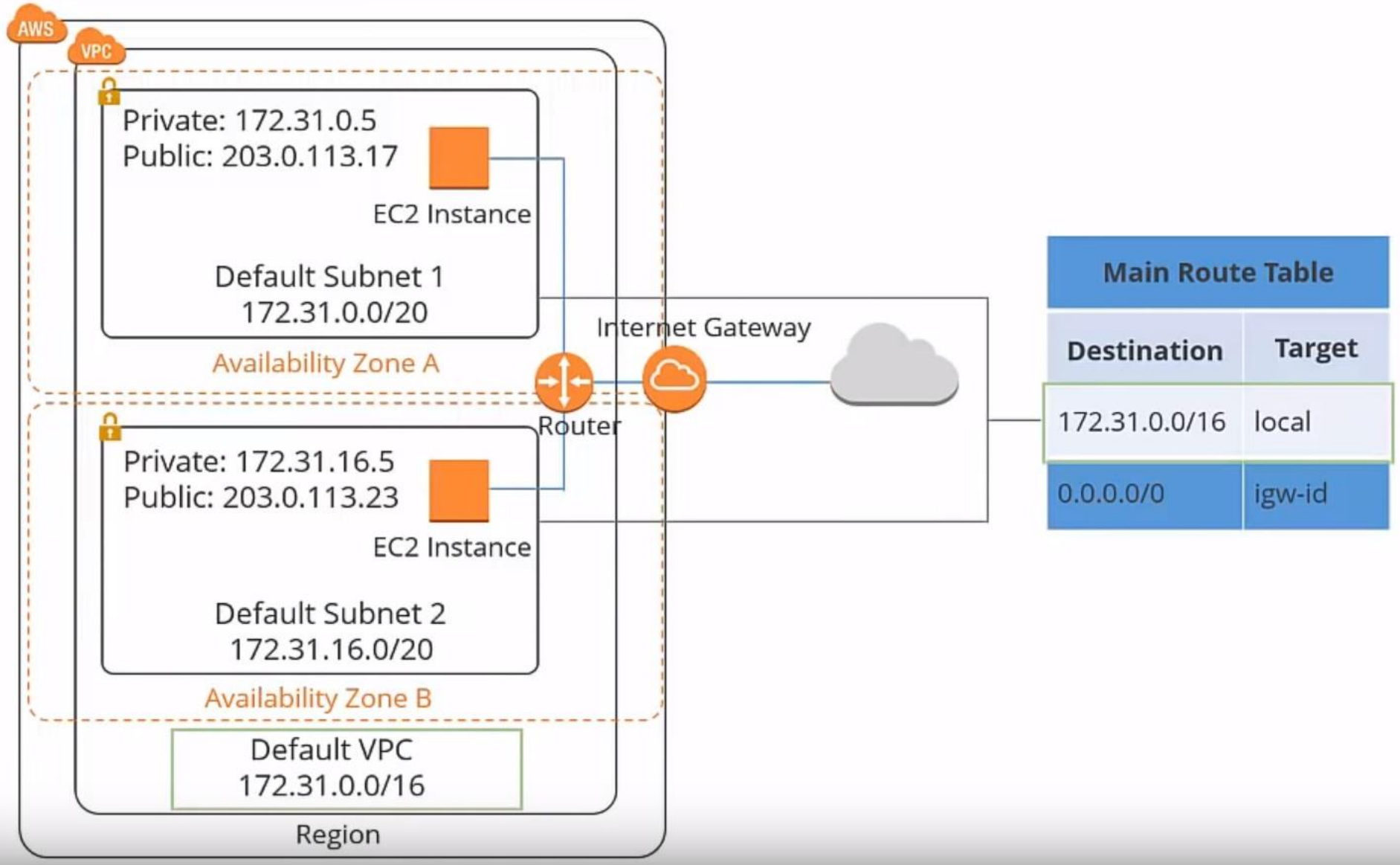


Main Route Table	
Destination	**Target**
172.31.0.0/16	local
0.0.0.0/0	igw-id

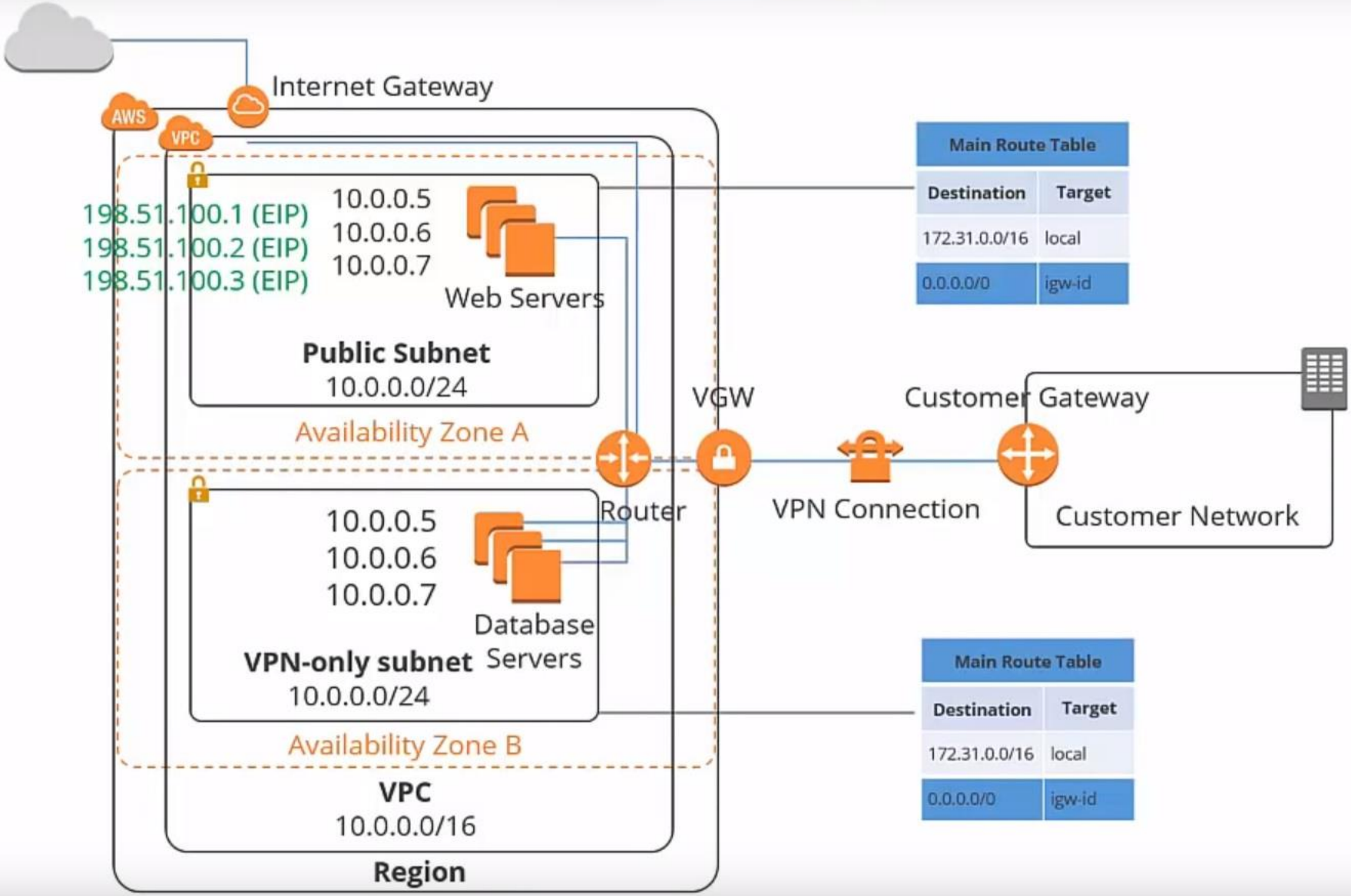
Default Amazon VPC



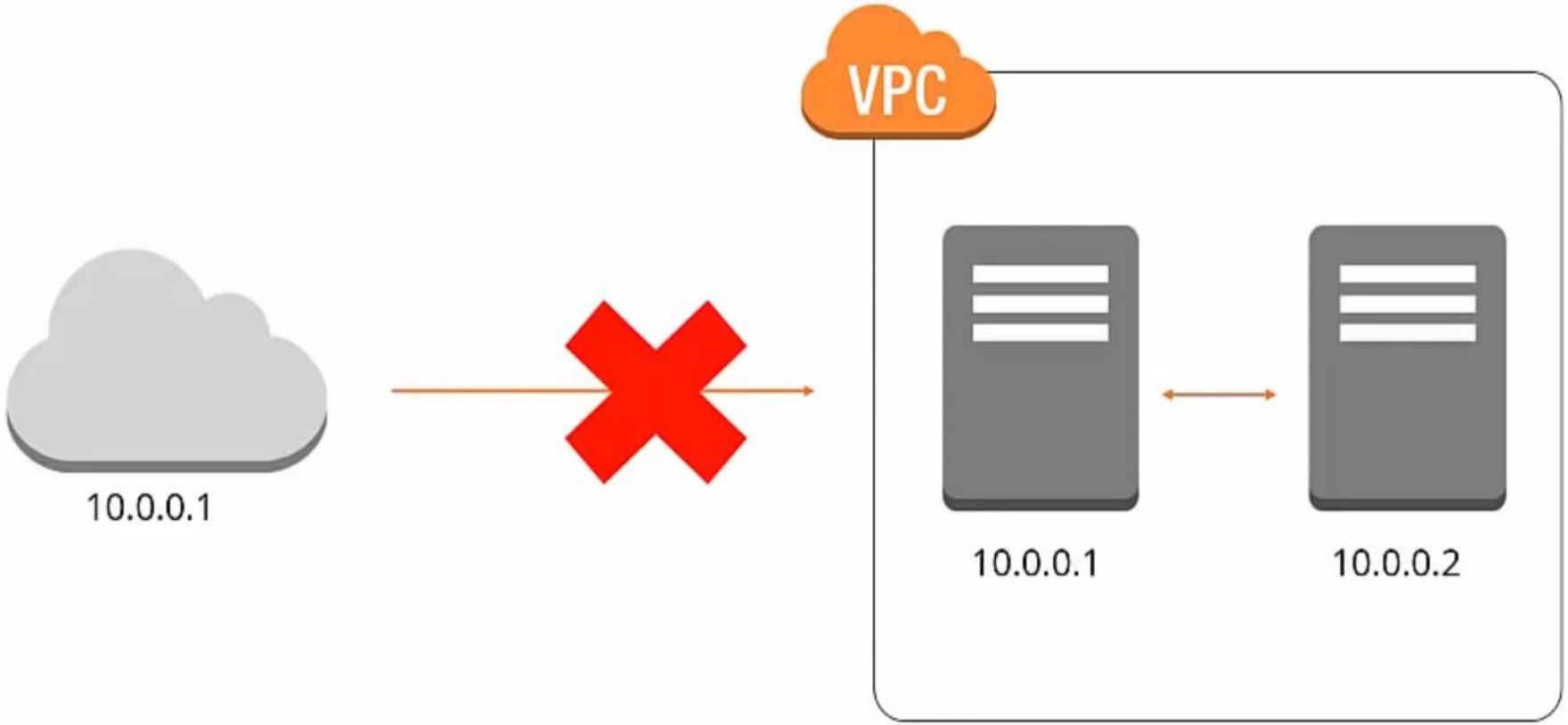
Default Amazon VPC



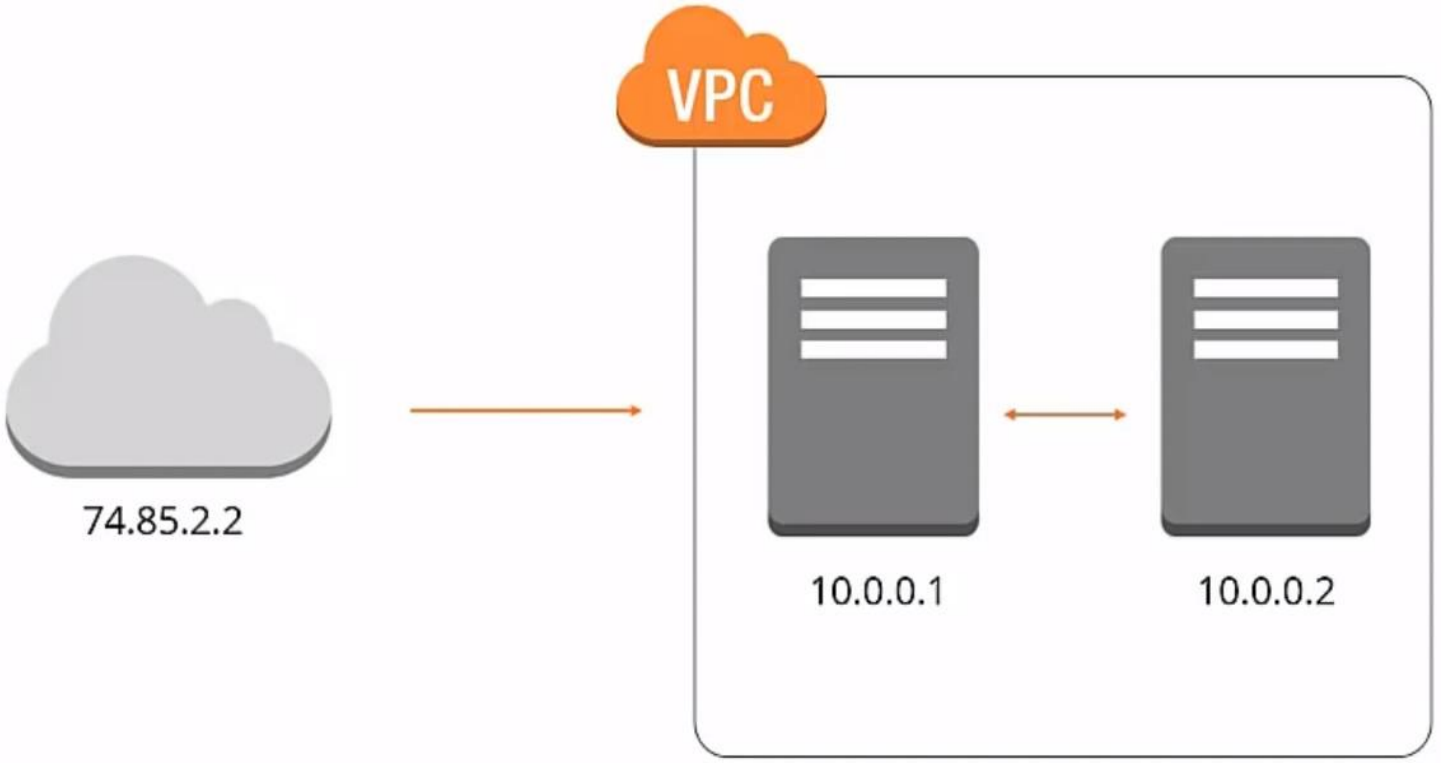
Custom VPC


Internet Gateway
AWS
VPC
198.51.100.1 (EIP)
198.51.100.2 (EIP)
198.51.100.3 (EIP)
10.0.0.5
10.0.0.6
10.0.0.7
Web Servers
Public Subnet
10.0.0.0/24
Availability Zone A
Main Route Table
Destination
Target
172.31.0.0/16
local
0.0.0.0/0
igw-id
VGW
Customer Gateway
Router
VPN Connection
Customer Network
10.0.0.5
10.0.0.6
10.0.0.7
Database Servers
VPN-only subnet
10.0.0.0/24
Availability Zone B
Main Route Table
Destination
Target
172.31.0.0/16
local
0.0.0.0/0
igw-id
VPC
10.0.0.0/16
Region

Private IP Addresses



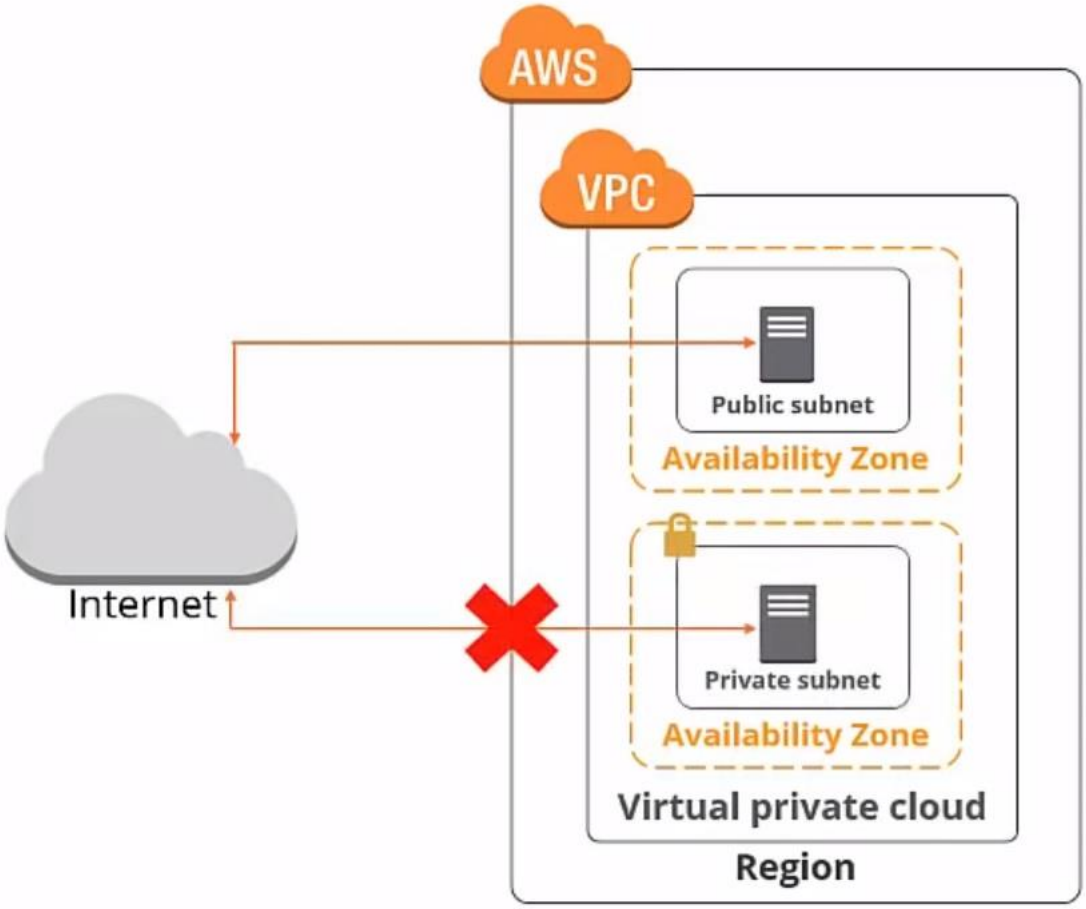
Public IP Addresses



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."

Public and Private Subnets

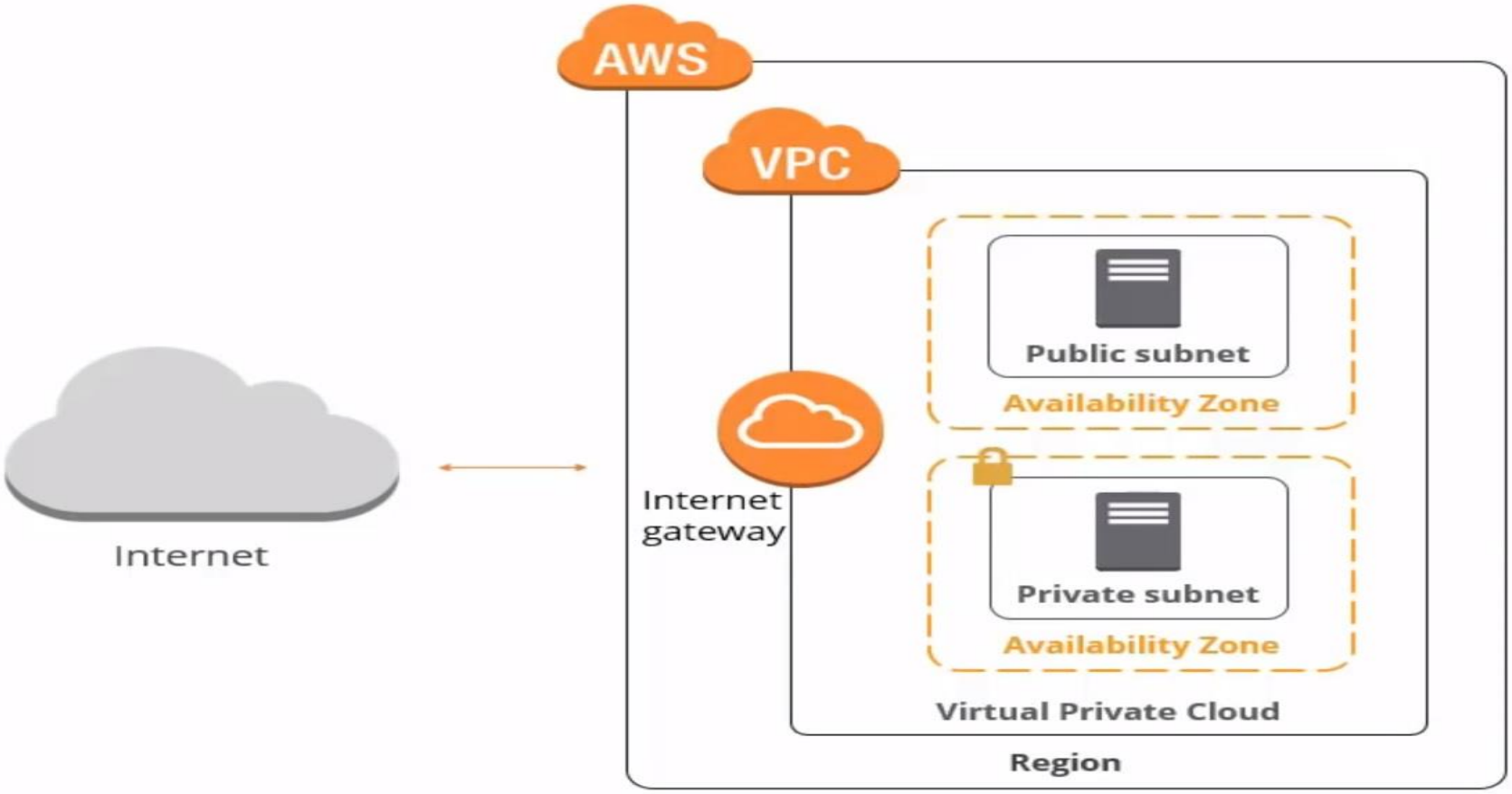


Internet Gateway Definition

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



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.

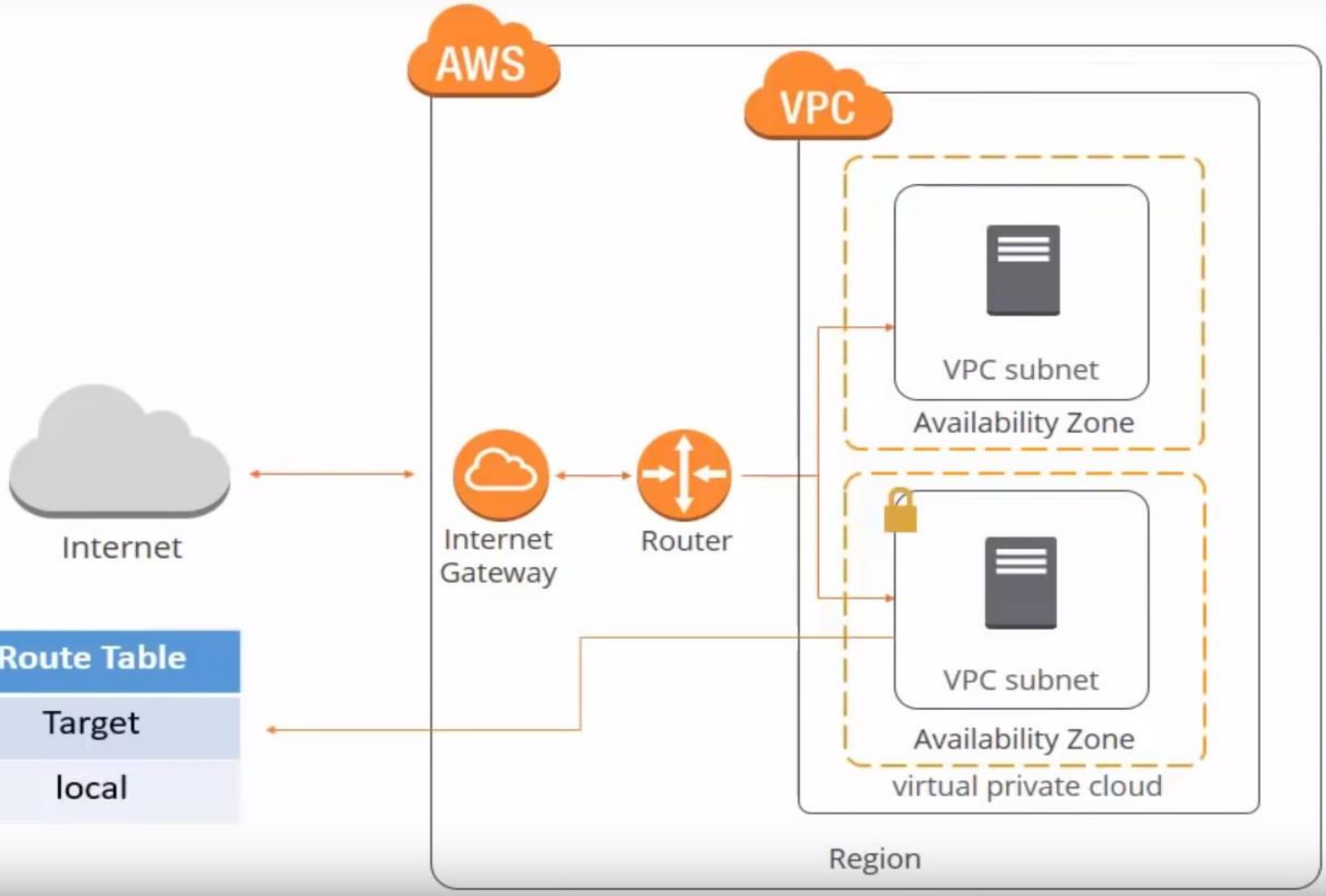
Route Table Overview

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

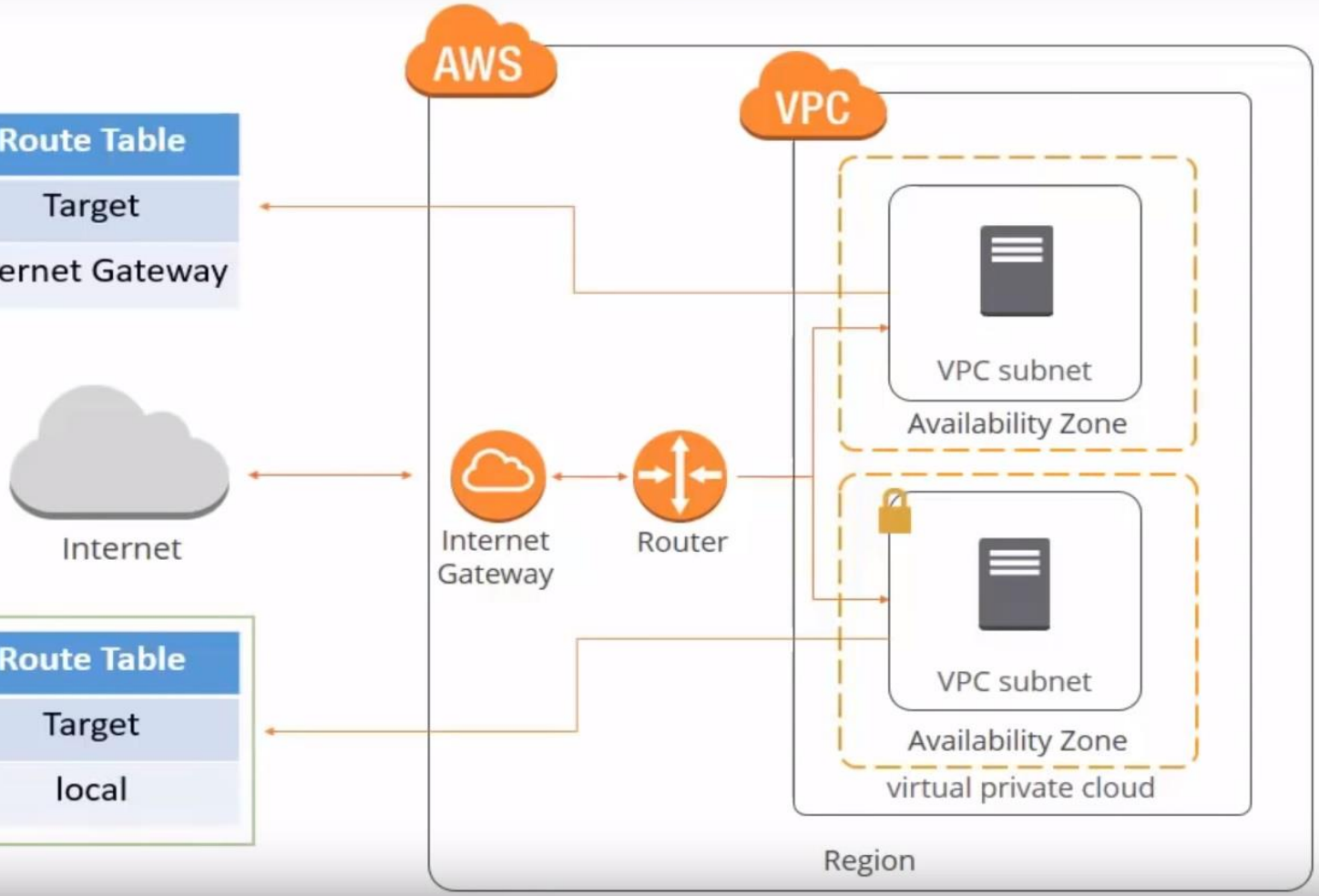
Route Table Diagram



Main	Route Table
Destination	Target
10.0.0.0/16	local

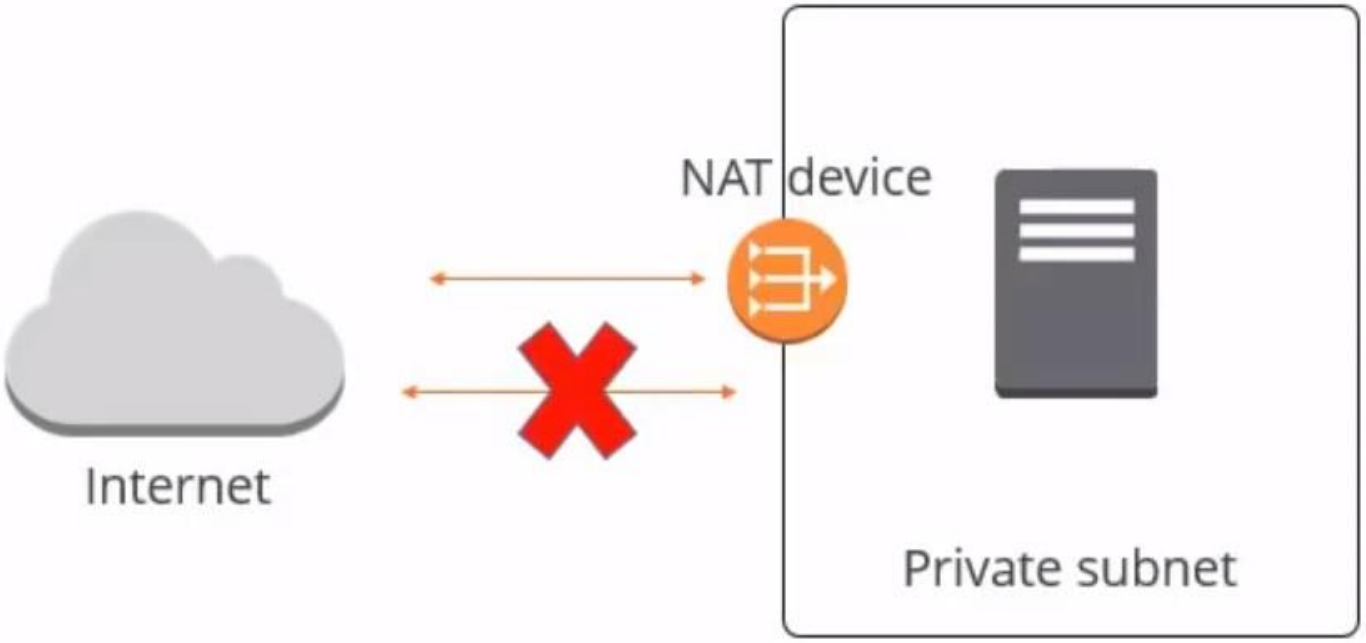
Route Table Diagram

Custom	Route Table
Destination	Target
0.0.0.0/0	Internet Gateway



Main	Route Table
Destination	Target
10.0.0.0/16	local

NAT Devices Overview



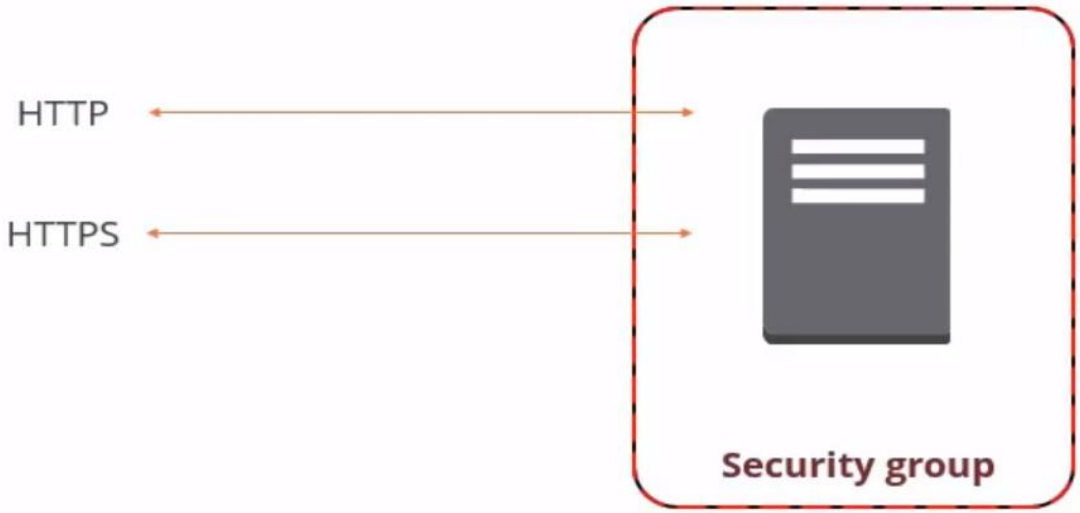
Security Groups Overview

Amazon's definition of a Security Group:

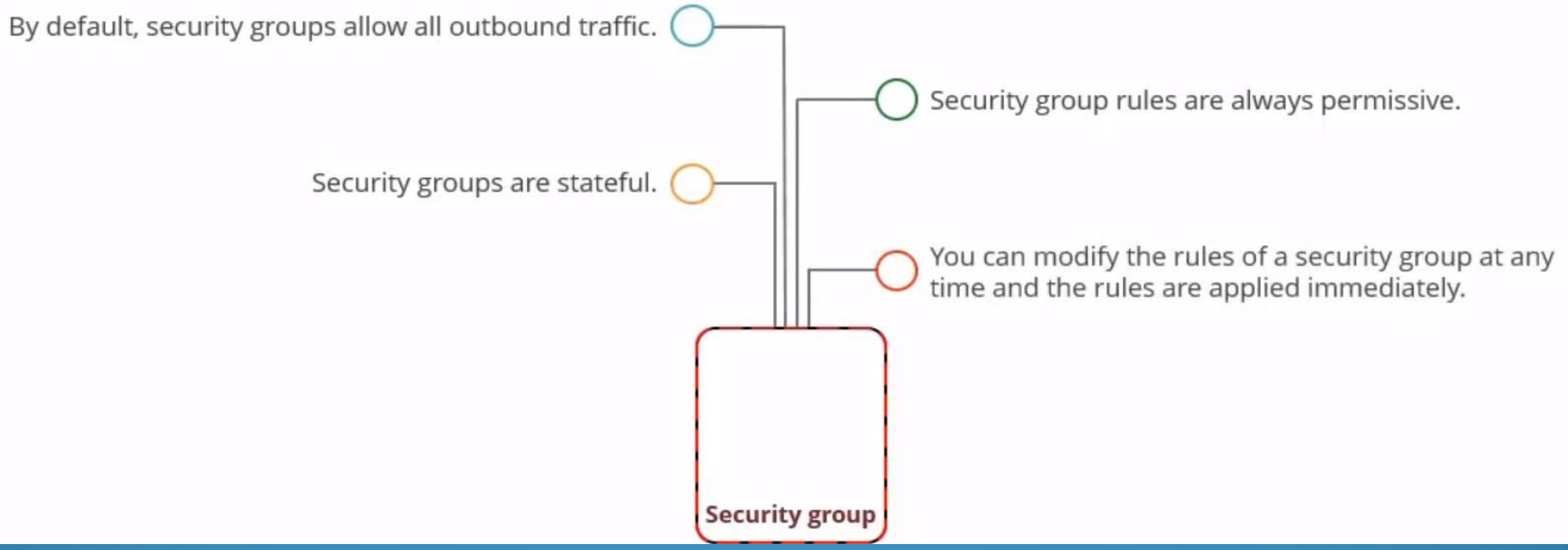
"A security group acts as a virtual firewall that controls the traffic for one or more instances. You add rules to each security group that allow traffic to or from its associated instances."

Security Groups for Webservers

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



Security Groups Rules

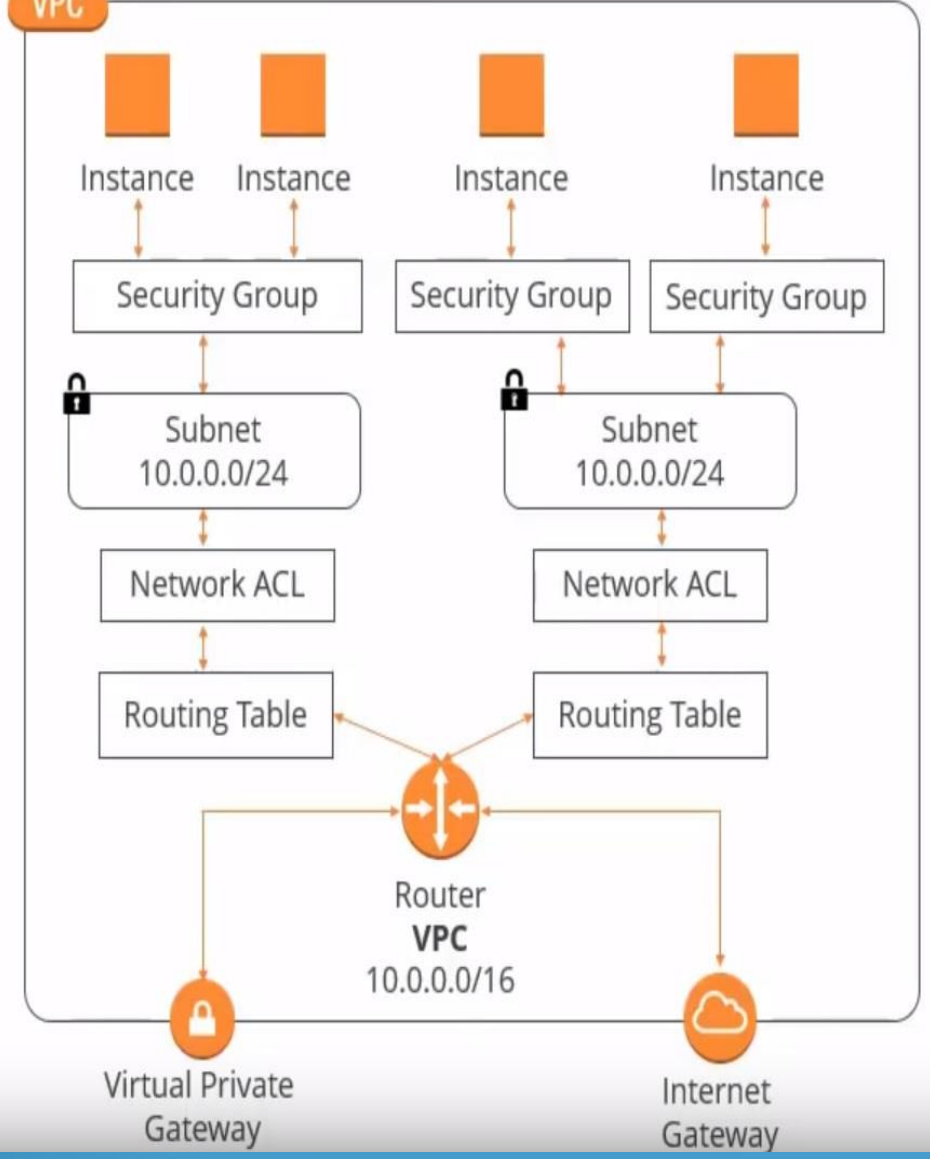


Network ACL Overview

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."



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

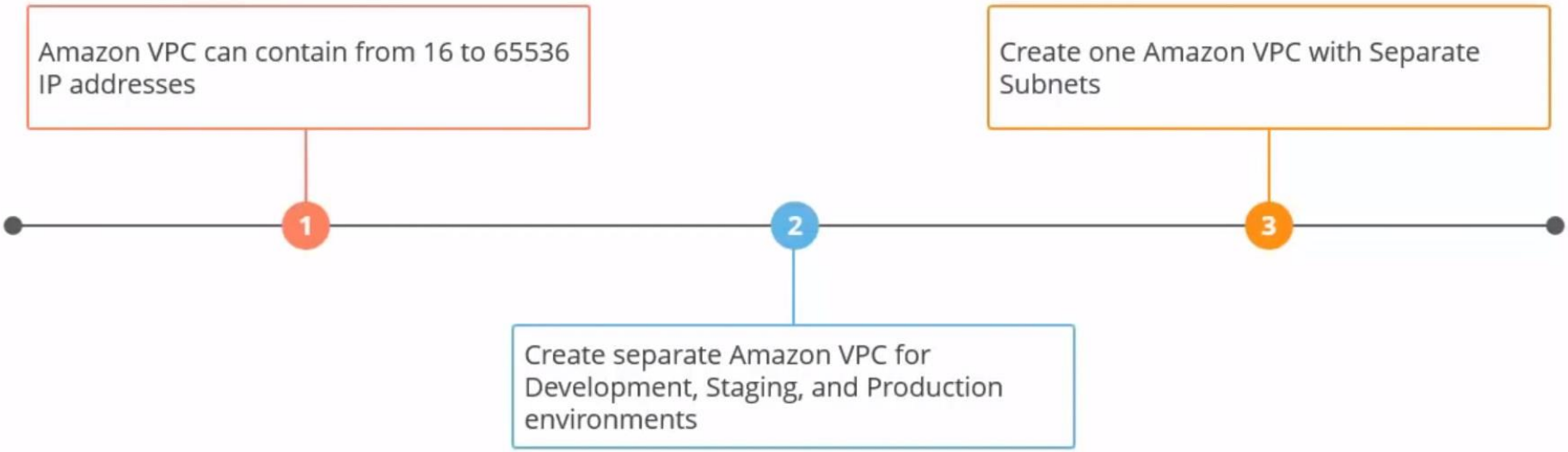
ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic.

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

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

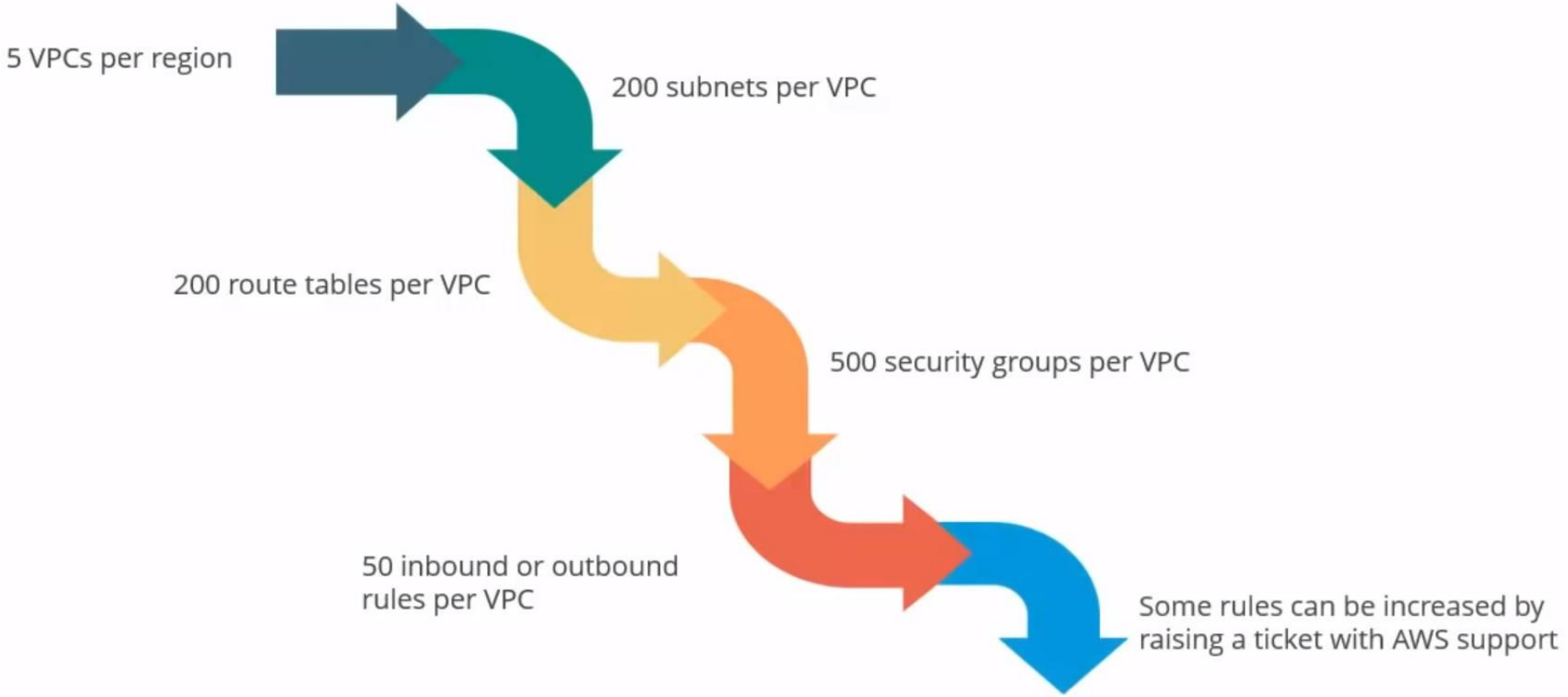
A subnet can only be associated with one ACL. However, an ACL can be associated with multiple subnets.

Choose CIDR blocks



Understand Amazon VPC Limits

AWS has various limitations on the VPC components:



Key Takeaways

1. Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defin 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.
2. Private IP address is an IP address that's not reachable over the Internet.
3. Public IP address is reachable from the Internet.
4. Elastic IP address is a static or public persistent IP address.
5. 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.

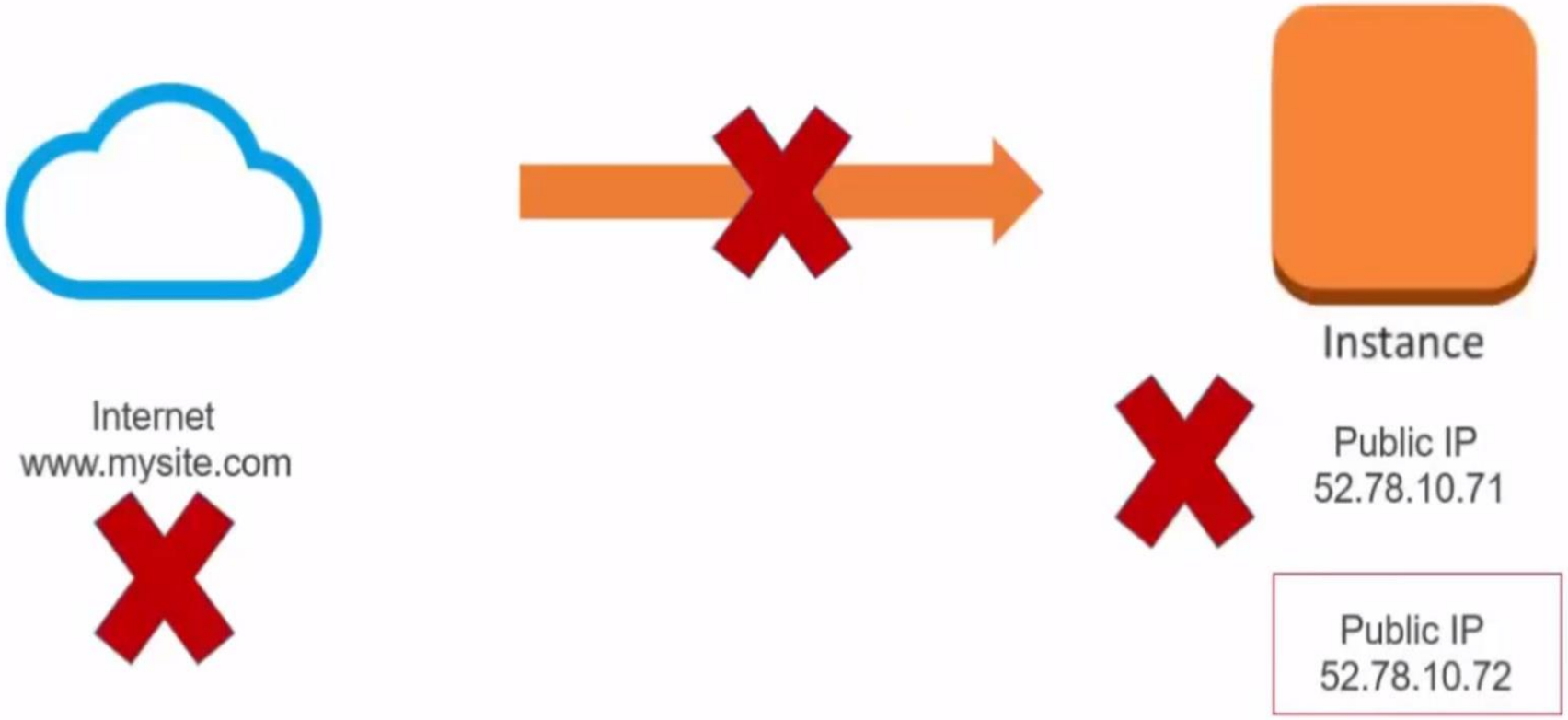
Amazon Web Services – Elastic IP

Static IP allocated to an EC2 instance

Associated with your AWS Account

At any point associate the IP with another EC2 instance

Why Elastic IP



Elastic IP is nothing but the static IP

Allocate a new Elastic IP to your account

Associate the address to an EC2 instance