Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud

simplilearn

Cloud

Caltech | Center for Technology & Management Education

AWS Solution Architect: Associate Level

simplilearn

Amazon Virtual Private Cloud

Learning Objectives

By the end of the lesson, you will be able to:

- Explain Amazon Virtual Private Cloud (VPC)
- Illustrate the VPC components
- Create a public and private subnet
- Create route tables and security groups
- Set up a VPC peering connection
- Demonstrate a VPN connection
- Demonstrate load balancing

Introduction to Amazon Virtual Private Cloud (VPC)

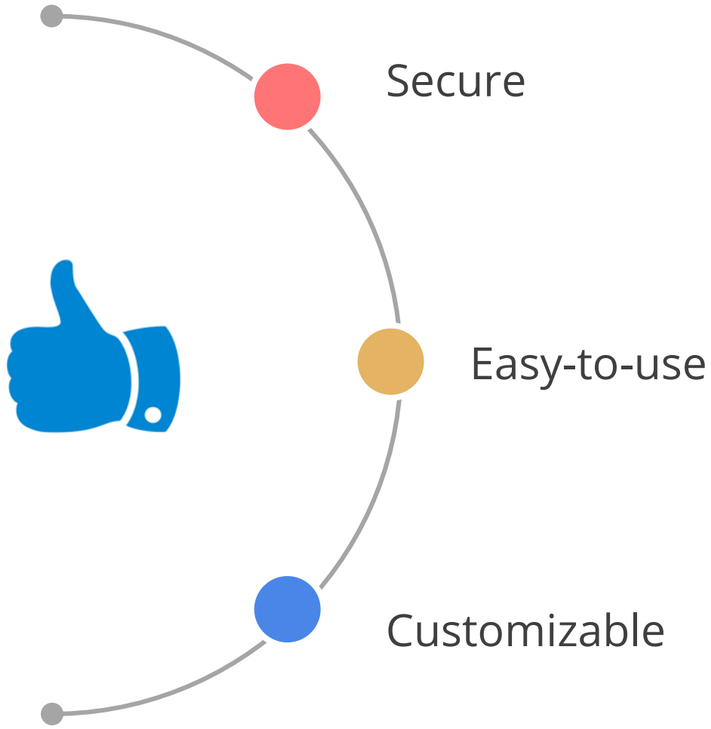
Amazon Virtual Private Cloud

Amazon Virtual Private Cloud (VPC) enables the user to launch AWS resources into a virtual network.

Amazon Virtual Private Cloud (VPC)

Benefits of Amazon Virtual Private Cloud (VPC)

Here are some benefits of Amazon Virtual Private Cloud (VPC):



Use Cases of Amazon Virtual Private Cloud (VPC)

Here are some use cases of Amazon Virtual Private Cloud (VPC):

01	Host a simple and public-facing website
02	Host multi-tier web applications
03	Recovery from disaster
04	Extend the corporate network into the cloud
05	Securely connect cloud applications to the data center
06	Out-of-band and inline traffic inspection

Functionality of Amazon Virtual Private Cloud (VPC)

With Amazon Virtual Private Cloud (Amazon VPC), the users can:

- Store data in Amazon S3 and set permissions such that the data can only be accessed from within the Amazon VPC
- Assign multiple IP addresses and attach multiple elastic network interfaces to instances in the VPC
- Control inbound and outbound access to and from individual subnets using network access control lists
- Expand the VPC by adding secondary IP ranges

Functionality of Amazon Virtual Private Cloud (VPC)

With Amazon Virtual Private Cloud (Amazon VPC), the users can:

- Bridge the Amazon VPC and the on-site IT infrastructure with AWS Site-to-Site VPN
- Associate VPC security groups with instances on EC2-Classic
- Enable both IPv4 and IPv6 in the VPC
- Use Amazon VPC traffic mirroring to capture and mirror network traffic for Amazon EC2 instances
- Intercept and analyze ingress and egress traffic using a network and security appliance, including third-party offerings

Types of Amazon Virtual Private Cloud (VPC)

The following are the types of Amazon Virtual Private Cloud (VPC):

1

Default VPC

It gets automatically created in every region along with the account creation.

2

Custom VPC

Custom VPCs are created by the user.

Default VPC Overview

- A default VPC is ready for the users to use so that they don't have to create and configure into their own VPC.
- The users can immediately launch the Amazon EC2 instances into their default VPC.
- The users can also use services such as Elastic Load Balancing, Amazon RDS, and Amazon EMR in their default VPC.
- A default VPC is suitable for getting started quickly, and for launching public instances such as a blog or simple website.
- The users can modify the components of their default VPC as needed.

Default VPC Overview

Default VPC allows the users to:

- Add additional non default subnets
- Modify the main route table
- Add additional route tables
- Associate additional security groups
- Update the rules of the default security group
- Add AWS Site-to-Site VPN connections
- Add more IPv4 CIDR blocks
- Access VPCs in a remote region by using a Direct Connect gateway

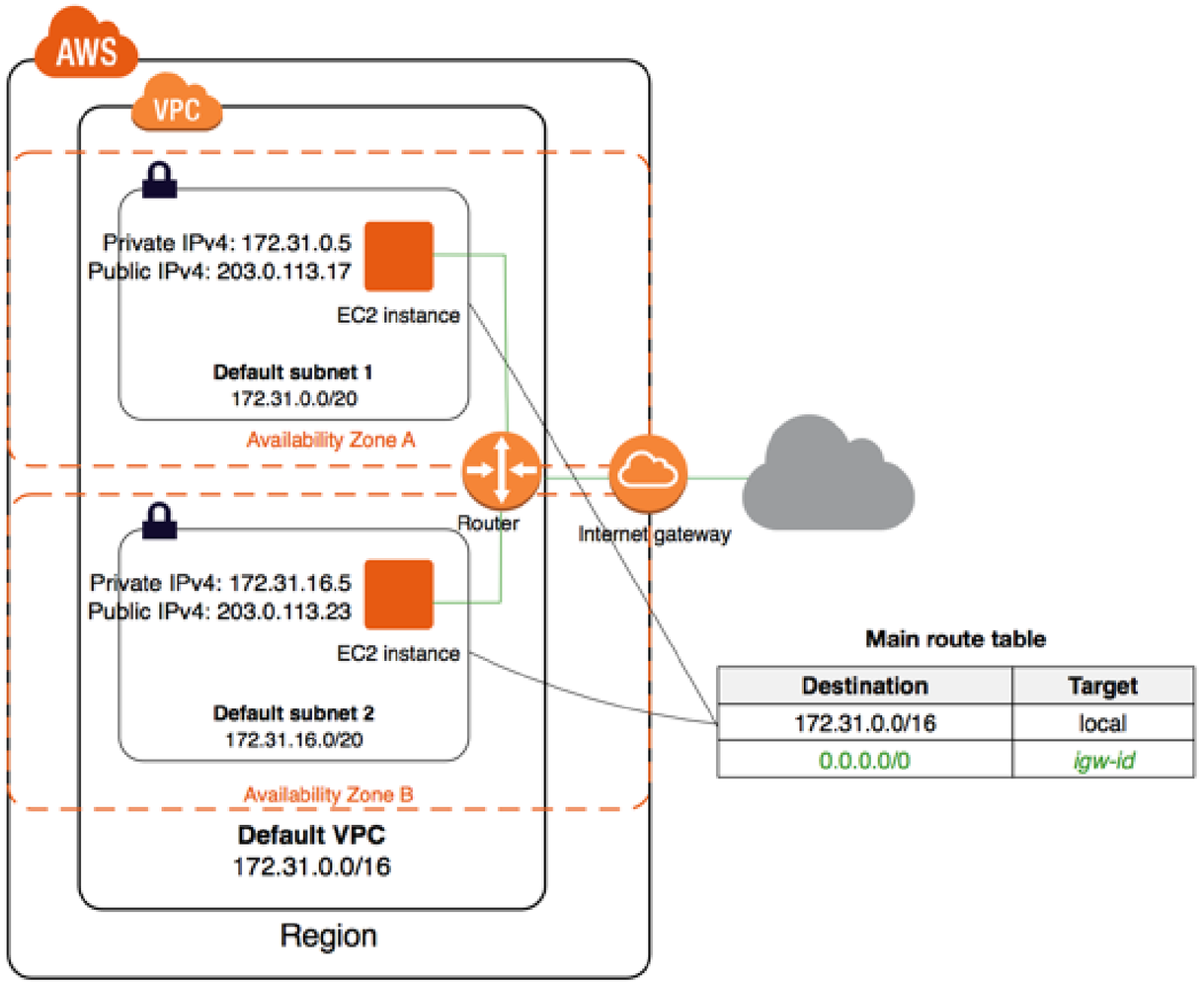
Default VPC Components

The following are the components that Amazon sets up for the users while creating a default VPC:

- Create a VPC with a size /16 IPv4 CIDR block (172.31.0.0/16)
- Create a size /20 default subnet in each Availability Zone
- Create an internet gateway and connect it to the default VPC
- Create a default security group and associate it with the default VPC
- Create a default network access control list (ACL) and associate it with the default VPC

Default VPC Components

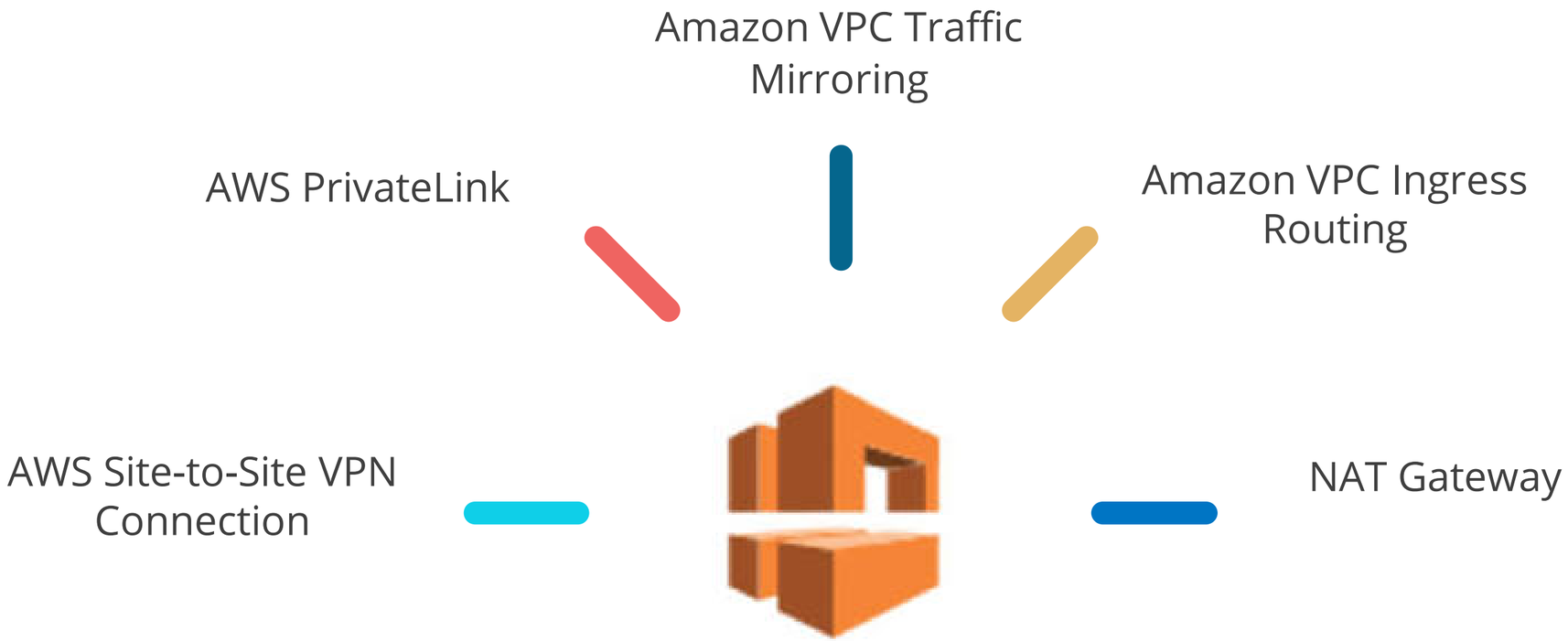
The following figure illustrates the key components that Amazon sets up for a default VPC:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/default-vpc.html

Amazon Virtual Private Cloud (VPC) Costs

The following are the costs associated with Amazon Virtual Private Cloud (VPC):



Assisted Practice

Create a Custom VPC

Duration: 10 min.

Problem Statement:

You are given a project to create a Custom VPC.

Assisted Practice: Guidelines to Create a Custom VPC

Steps to perform:

1. Go to your Amazon Console
2. Open the VPC dashboard
3. Click on the Launch VPC Wizard button
4. Choose VPC with Single Public Subnet
5. Skip to the review page and click on the Create VPC button

Amazon VPC Components

Amazon VPC Components

1

Virtual Private Cloud (VPC)

It is a virtual network dedicated to the user's AWS account.

2

Subnet

It is a range of IP addresses in the user's VPC.

3

Route table

It contains a set of rules, called routes, that are used to determine where the network traffic is directed.

Amazon VPC Components

4

Internet gateway

It is a gateway that the users attach to their VPC to enable communication between resources in their VPC and the internet.

5

VPC endpoint

It enables the users to privately connect their VPC to supported AWS and VPC endpoint services without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

Amazon VPC Components

6

NAT gateway

It is a highly available and managed Network Address Translation (NAT) service for the resources in a private subnet to access the internet.

7

Peering connection

It is a peering connection that enables the users to route traffic via private IP addresses between two peered VPCs.

8

Egress-only internet gateway

It is a stateful gateway to provide egress only access for IPv6 traffic from the VPC to the internet.

IP Addresses

IP Addresses

The following are the types of IP Addresses in Amazon VPC:

Private IP Address	• A private IP address is not reachable over the internet.
Public IP Address	• The users can use private IP address to communicate between instances in the same VPC.
Elastic IP Address	• Public IP will get released whenever the user spot and instance.

IP Addresses

The following are the types of IP Addresses in Amazon VPC:

- Private IP Address
- Public IP Address
- Elastic IP Address

- A public IP address is reachable from the internet.
- The users can use public IP address to communicate between the instances and the internet.

IP Addresses

The following are the types of IP Addresses in Amazon VPC:

- Private IP Address
- Public IP Address
- Elastic IP Address

- An Elastic IP address is a public IP address that the users can allocate to their account.
- The users can associate it to and from the instances as they require, and it remains allocated to their account until they choose to release it.

Multiple IP Addresses

It can be useful to assign multiple IP addresses to an instance in the VPC to do the following:

- Host multiple websites on a single server by using multiple SSL certificates on a single server and associating each certificate with a specific IP address
- Operate network appliances, such as firewalls or load balancers, that have multiple IP addresses for each network interface
- Redirect internal traffic to a standby instance in case the instance fails, by reassigning the secondary IP address to the standby instance

Elastic Network Interface

Elastic Network Interface

An elastic network interface is a virtual network interface that includes the following attributes:

- A primary private IPv4 address
- One or more secondary private IPv4 addresses
- One Elastic IP address per private IPv4 address
- One public IPv4 address, which can be auto-assigned to the network interface for eth0 when the users launch an instance
- One or more IPv6 addresses
- One or more security groups
- A MAC address
- A source or destination check flag

Elastic Network Interface

Attaching multiple network interfaces to an instance is useful when the user wants to:

Create a management network

Use network and security appliances in the VPC

Create dual-homed instances with workloads or roles on distinct subnets

Create a low-budget, high-availability solution

VPCs and Subnets

VPCs and Subnets

The following are the types of subnets in Amazon VPC:

Public Subnet

- A subnet that is associated with a route table that has a route to an internet gateway

Private Subnet

- Provides 256 private IPv4 addresses

VPCs and Subnets

The following are the types of subnets in Amazon VPC:

Public Subnet

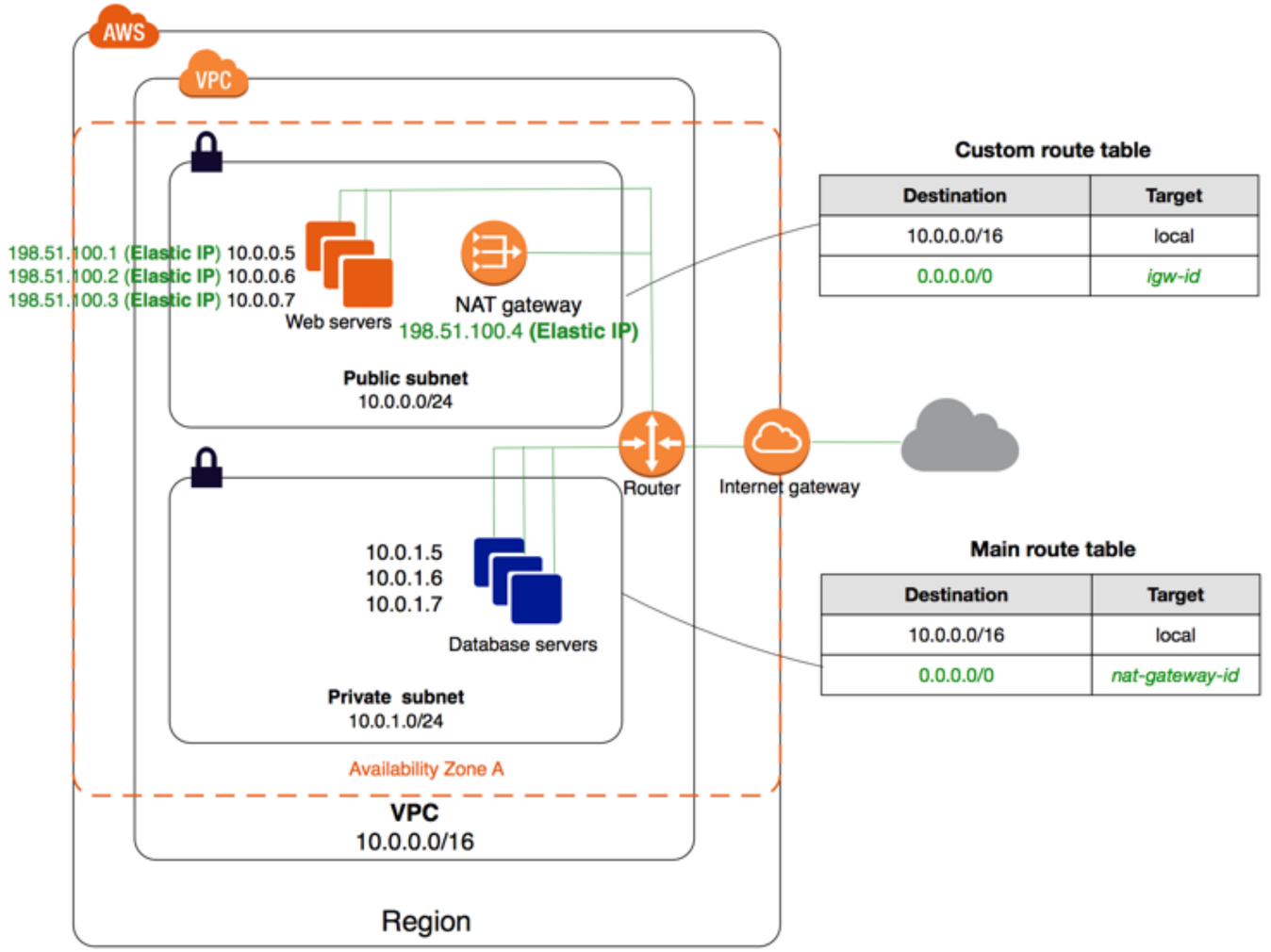
- A private subnet with a size per 24 IPv4 Classless Inter-Domain Routing (CIDR) block (example: 10.0.1.0/24)

Private Subnet

- Provides 256 private IPv4 addresses

VPCs and Subnets

The following diagram shows the key components of the configuration for the VPCs and the subnets:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Scenario2.html

Internet Gateways

Internet Gateways

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between the VPC and the internet.

An internet gateway serves two purposes:

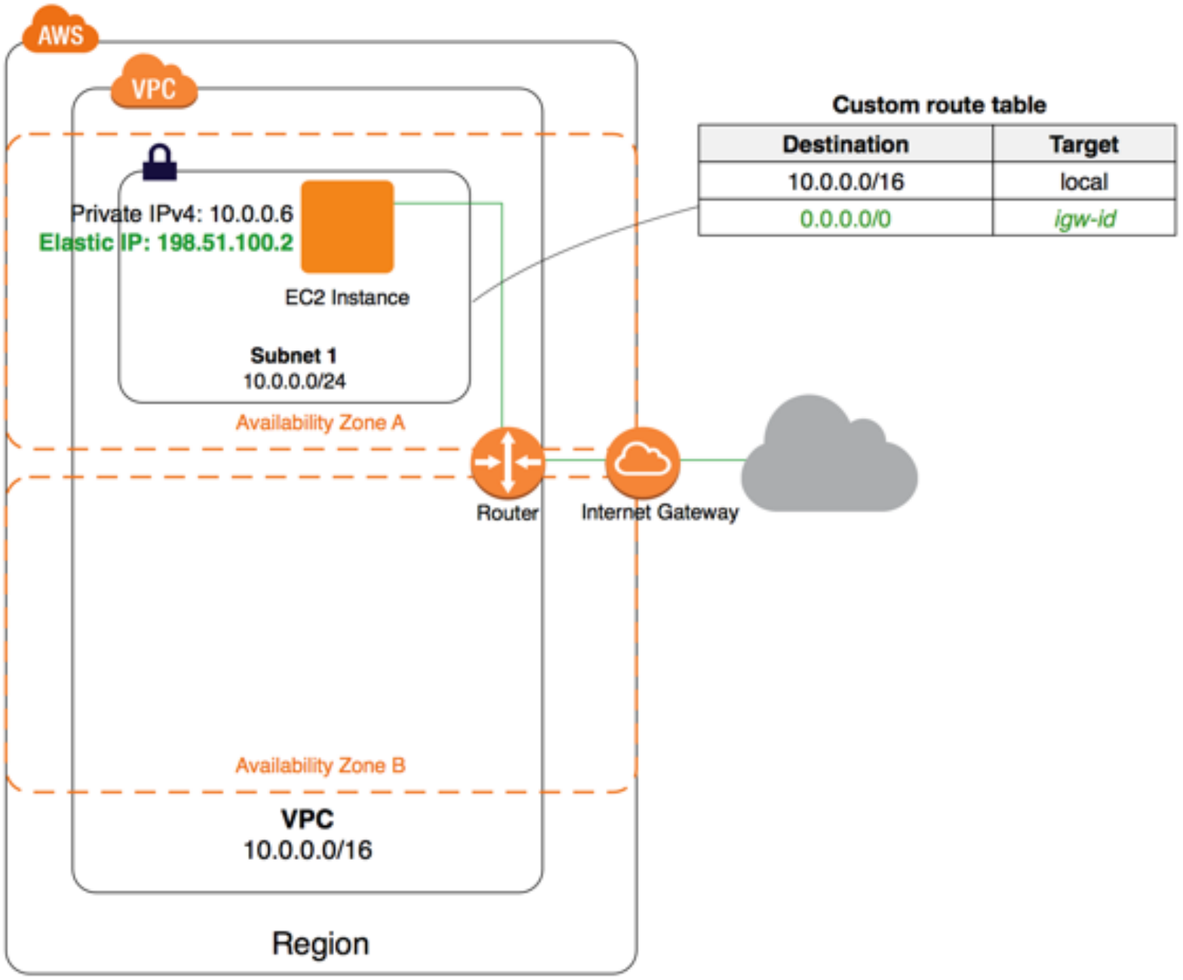
01	It provides a target in the VPC route tables for internet-routable traffic.
02	It performs network address translation (NAT) for instances that have been assigned public IPv4 addresses.

Note

An internet gateway supports IPv4 and IPv6 traffic.

Internet Gateways

The following diagram shows the communication between the Elastic IP address and the internet:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Egress-Only Internet Gateways

- An egress-only internet gateway is a horizontally scaled, redundant, and highly available VPC component.
- It allows outbound communication over IPv6 from instances in the VPC to the internet.
- It prevents the internet from initiating an IPv6 connection with the instances.

Note

An egress-only internet gateway is for use with IPv6 traffic only.

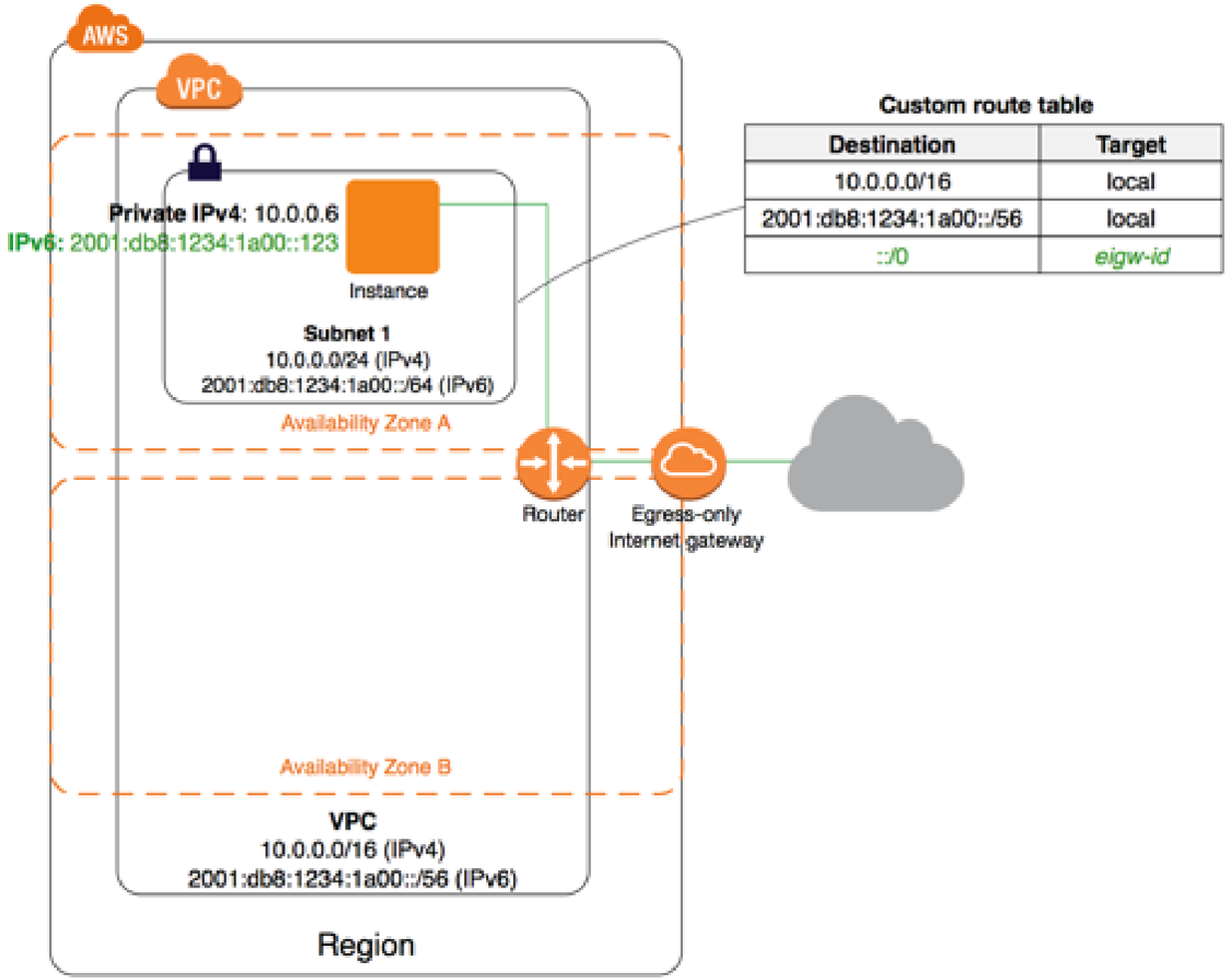
Egress-Only Internet Gateways

The following are the characteristics of egress-only internet gateway:

- The users cannot associate a security group with an egress-only internet gateway.
- The users can use security groups for their instances in the private subnet to control the traffic to and from those instances.
- The users can use a network ACL to control the traffic to and from the subnet for which the egress-only internet gateway routes the traffic.

Egress-Only Internet Gateways

The following diagram illustrates the working of egress-only internet gateway in the VPC:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/egress-only-internet-gateway.html

Carrier Gateways

A carrier gateway serves two purposes:

01	It allows inbound traffic from a carrier network in a specific location.
02	It allows outbound traffic to the carrier network and the internet.

Note

A carrier gateway supports IPv4 traffic.

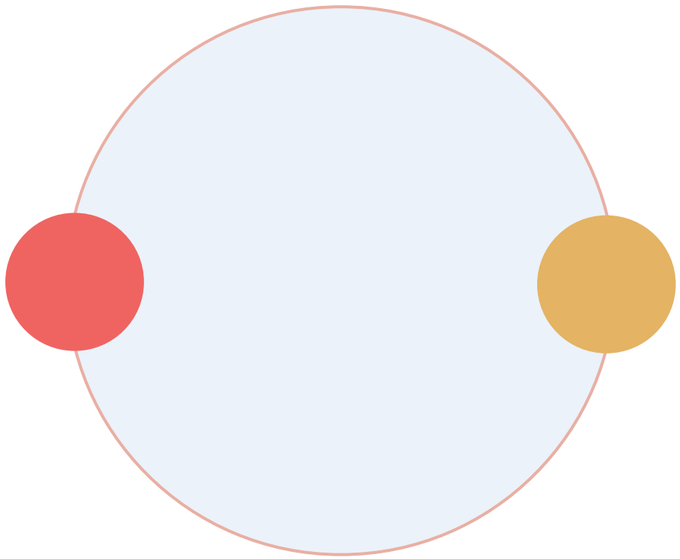
Network Address Translation (NAT) Gateway

Network Address Translation (NAT)

A NAT device is used to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating connections with those instances.

These are the two types of NAT devices:

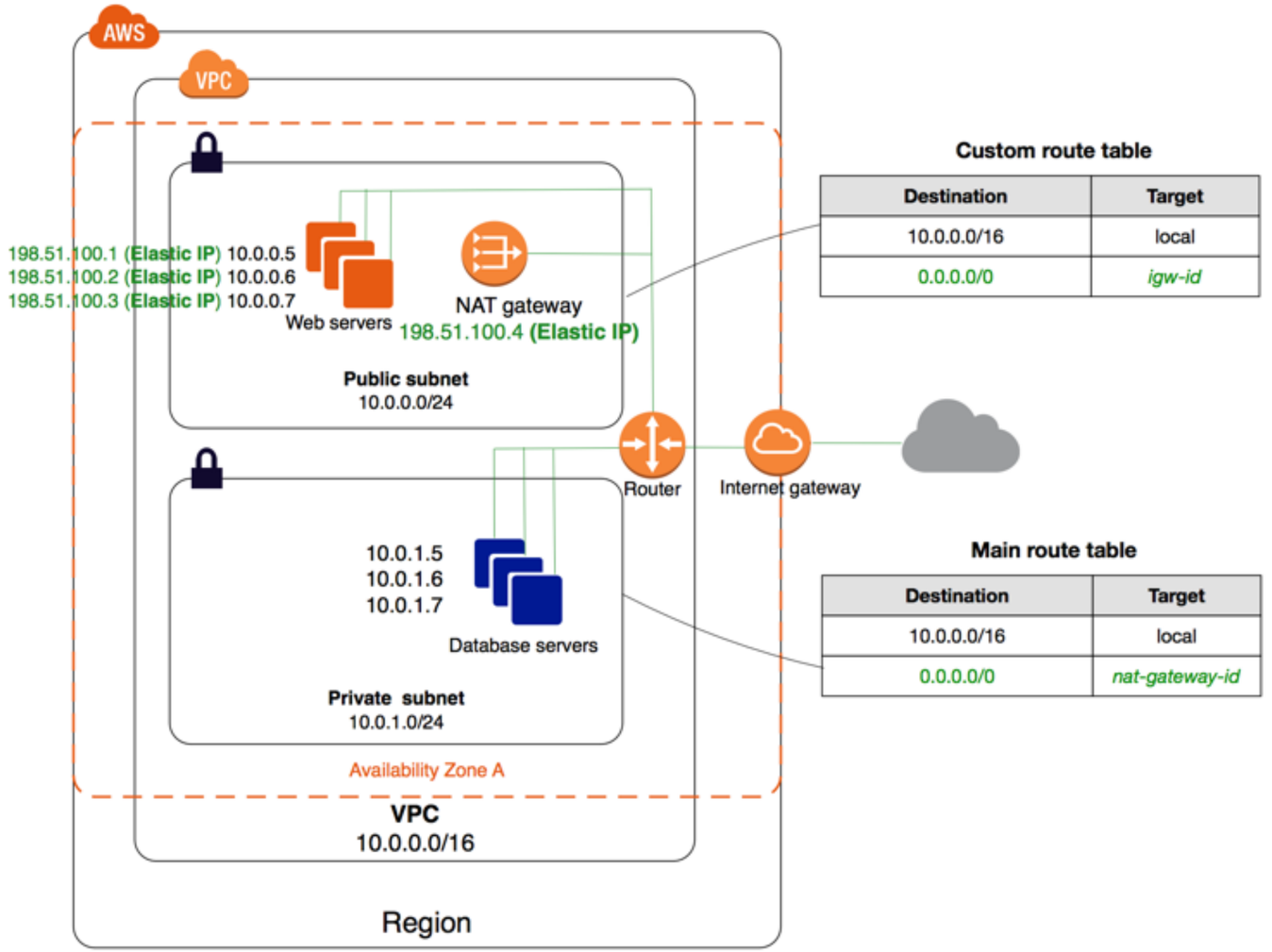
NAT gateway



NAT instance

NAT Gateway

The following diagram illustrates the architecture of a VPC with a NAT gateway:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Characteristics of NAT Gateway

The following are the characteristics of NAT gateway:

- A NAT gateway supports 5 Gbps of bandwidth and automatically scales up to 45 Gbps.
- It supports the TCP, UDP, and ICMP protocols.
- Users can use a network ACL to control the traffic to and from the subnet in which the NAT gateway is located.
- It can support up to 55,000 simultaneous connections to each unique destination.

Limitations of NAT Gateway

The following are the limitations of NAT gateway:

- Users can associate exactly one Elastic IP address with a NAT gateway, but they cannot disassociate an Elastic IP address from a NAT gateway after it is created.
- Users cannot associate a security group with a NAT gateway.
- A NAT gateway cannot be accessed by a ClassicLink connection that is associated with the VPC.
- Users cannot route traffic to a NAT gateway through a VPC peering connection, a Site-to-Site VPN connection, or AWS Direct Connect.

Assisted Practice

Create a Public and Private Subnet

Duration: 25 min.

Problem Statement:

You are given a project to create a public and private subnet.

Assisted Practice: Guidelines to Create a Public and Private Subnet

Steps to perform:

1. Go to your Amazon Console
2. Open the VPC dashboard
3. Click on the Launch VPC Wizard button
4. Choose VPC with Public and Private Subnet
5. Skip to the review page and click on the Create VPC button

Controlling Traffic in Amazon VPC

Internetwork Traffic Privacy in Amazon VPC

Amazon Virtual Private Cloud provides features to increase and monitor the security for the VPC:

01	02	03	04
Security groups	**Network access control lists (ACLs)**	**Flow logs**	**Traffic mirroring**

It acts as a firewall for the associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level.

Internetwork Traffic Privacy in Amazon VPC

Amazon Virtual Private Cloud provides features to increase and monitor the security for the VPC:

01	02	03	04
Security groups	Network access control lists (ACLs)	Flow logs	Traffic mirroring

It acts as a firewall for the associated subnets, controlling both inbound and outbound traffic at the subnet level.

Internetwork Traffic Privacy in Amazon VPC

Amazon Virtual Private Cloud provides features to increase and monitor the security for the VPC:

01	02	03	04
Security groups	Network access control lists (ACLs)	Flow logs	Traffic mirroring

It captures information about the IP traffic going to and from network interfaces in the VPC.

Internetwork Traffic Privacy in Amazon VPC

Amazon Virtual Private Cloud provides features to increase and monitor the security for the VPC:

01	02	03	04
Security groups	Network access control lists (ACLs)	Flow logs	Traffic mirroring

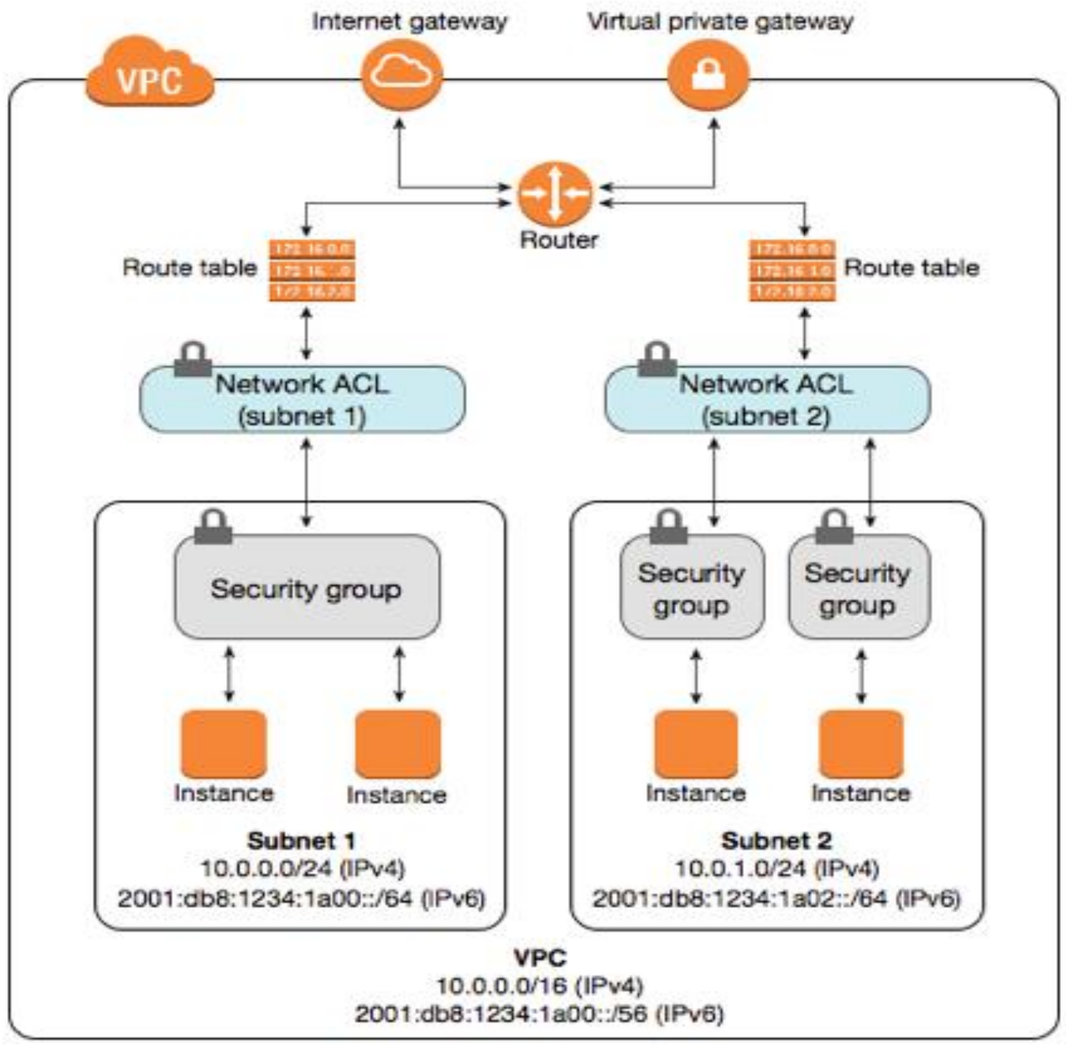
It helps the user to copy network traffic from an elastic network interface of Amazon EC2 instances.

Comparison of Security Groups and Network ACLs

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful, as the return traffic is automatically allowed, regardless of any rules	Is stateless, as the return traffic must be explicitly allowed by rules
Applies to an instance only if the user specifies the security group when launching the instance, or associates the security group with the instance	Automatically applies to all instances in the subnets that it is associated with

Security Groups and Network ACLs

The following diagram illustrates the layers of security provided by security groups and network ACLs:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html

Route Tables

A route table contains a set of rules, called routes, that are used to determine where network traffic from the subnet or gateway is directed.

The following are the key concepts of route tables:

01	Main route table
02	Custom route table
03	Edge association
04	Route table association
05	Subnet route table

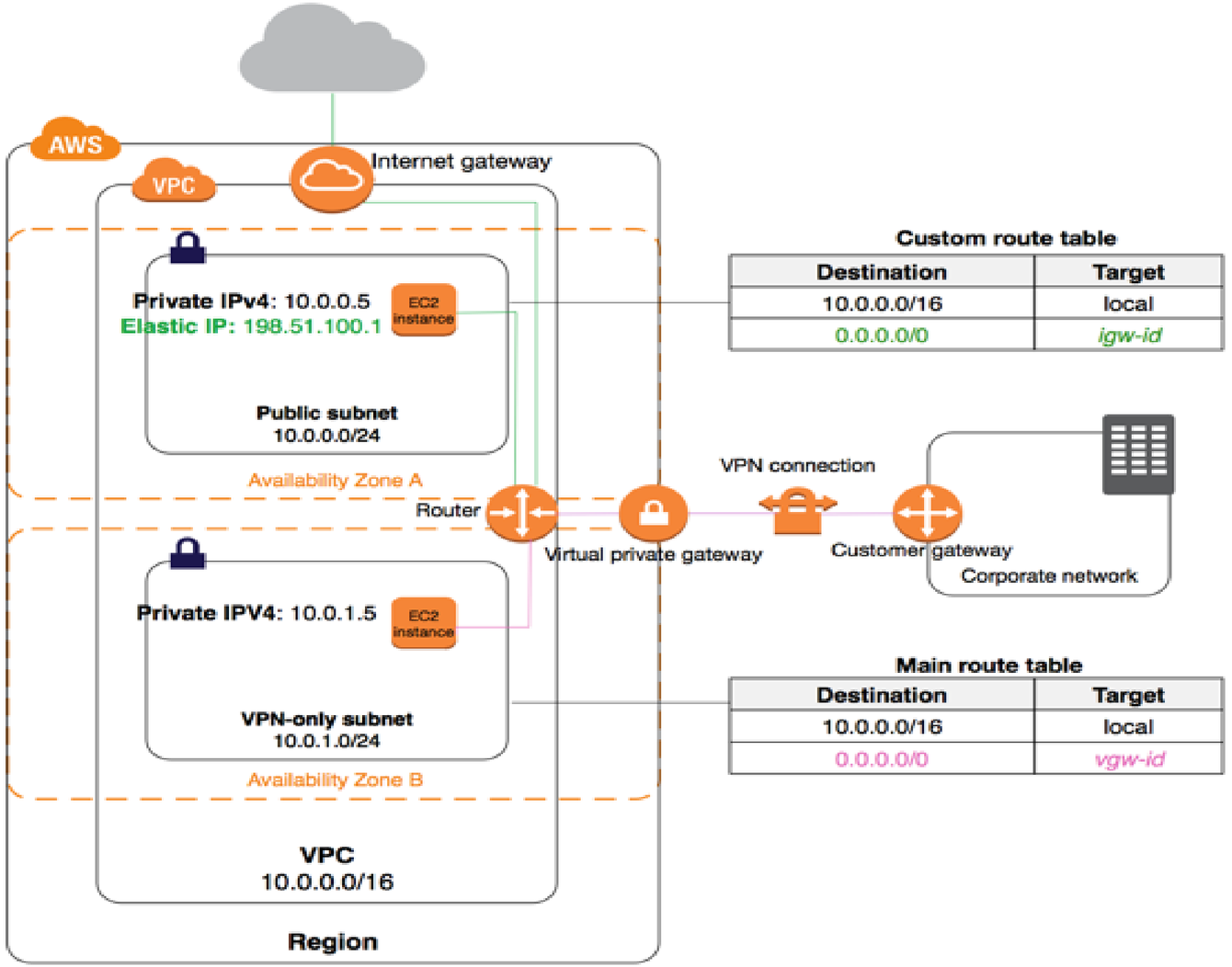
Route Tables

The following are the key concepts of route tables:

06	Gateway route table
07	Local gateway route table
08	Destination
09	Propagation
10	Target
11	Local route

Route Tables

The following diagram shows the routing for a VPC with an internet gateway, a virtual private gateway, a public subnet, and a VPN-only subnet:



Source: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

Assisted Practice

Create and Configure a Custom Route Table

Duration: 15 min.

Problem Statement:

You are given a project to create and configure a custom route table.

Assisted Practice: Guidelines to Create and Configure a Custom Route Table

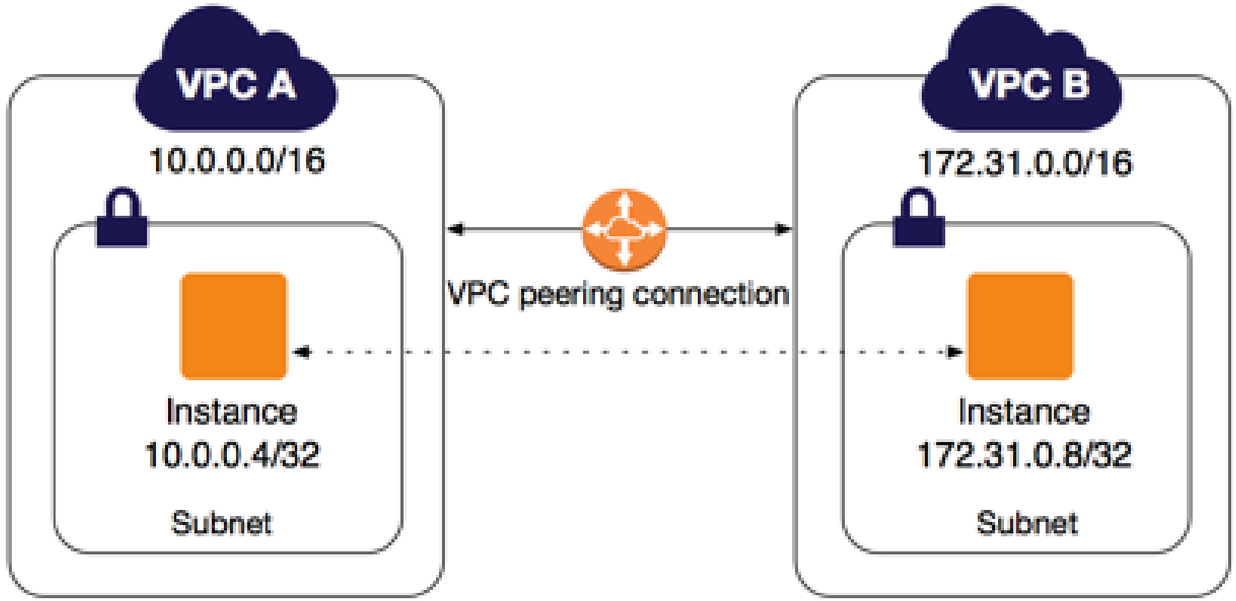
Steps to perform:

1. Go to your Amazon Console
2. Open the VPC dashboard
3. Click on the Create route table button
4. Choose the route table and click on the Add route button
5. Skip to the review page and click on the Create VPC button

VPC Peering

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables the user to route traffic between them using private IPv4 addresses or IPv6 addresses.



VPC peering connection

Source: https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html

VPC Endpoint

A VPC endpoint enables the user to privately connect the VPC to supported AWS services and VPC endpoint services without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.

More about VPC Endpoints:

01	Endpoints are virtual devices.
02	They are horizontally scaled, redundant, and highly available VPC components.
03	They allow communication between instances in the VPC and services without imposing availability risks or bandwidth constraints on the network traffic.

VPC Endpoint

The following are the types of VPC Endpoints:

Interface endpoints	It is an elastic network interface with a private IP address from the IP address range of the subnet that serves as an entry point for traffic destined to a supported service.
Gateway endpoints	

VPC Endpoint

The following are the types of VPC Endpoints:

Interface endpoints	It is a gateway that the user specifies as a target for a route in the route table for traffic destined to a supported AWS service.
Gateway endpoints	The following AWS services are supported: • Amazon S3 • DynamoDB

Working with VPC Endpoints

The user can create, access, and manage VPC endpoints using any of the following:

01	02	03	04
AWS Management console	AWS Command Line Interface (AWS CLI)	AWS SDKs	Query API

It provides a web interface that the user can use to access the VPC endpoints.

Working with VPC Endpoints

The user can create, access, and manage VPC endpoints using any of the following:

01	02	03	04
AWS Management console	AWS Command Line Interface (AWS CLI)	AWS SDKs	Query API

It provides commands for a broad set of AWS services, including Amazon VPC.

Working with VPC Endpoints

The user can create, access, and manage VPC endpoints using any of the following:

01	02	03	04
AWS Management console	AWS Command Line Interface (AWS CLI)	AWS SDKs	Query API

It provides language-specific APIs. The AWS SDKs take care of many of the connection details, such as calculating signatures, handling request retries, and handling errors.

Working with VPC Endpoints

The user can create, access, and manage VPC endpoints using any of the following:

01	02	03	04
AWS Management console	AWS Command Line Interface (AWS CLI)	AWS SDKs	Query API

It provides low-level API actions that the user calls using the HTTPS requests.

Assisted Practice

Create and Accept a VPC Peering Connection

Duration: 20 min.

Problem Statement:

You are given a project to create and accept a VPC peering connection.

Assisted Practice: Guidelines to Create and Accept a VPC Peering Connection

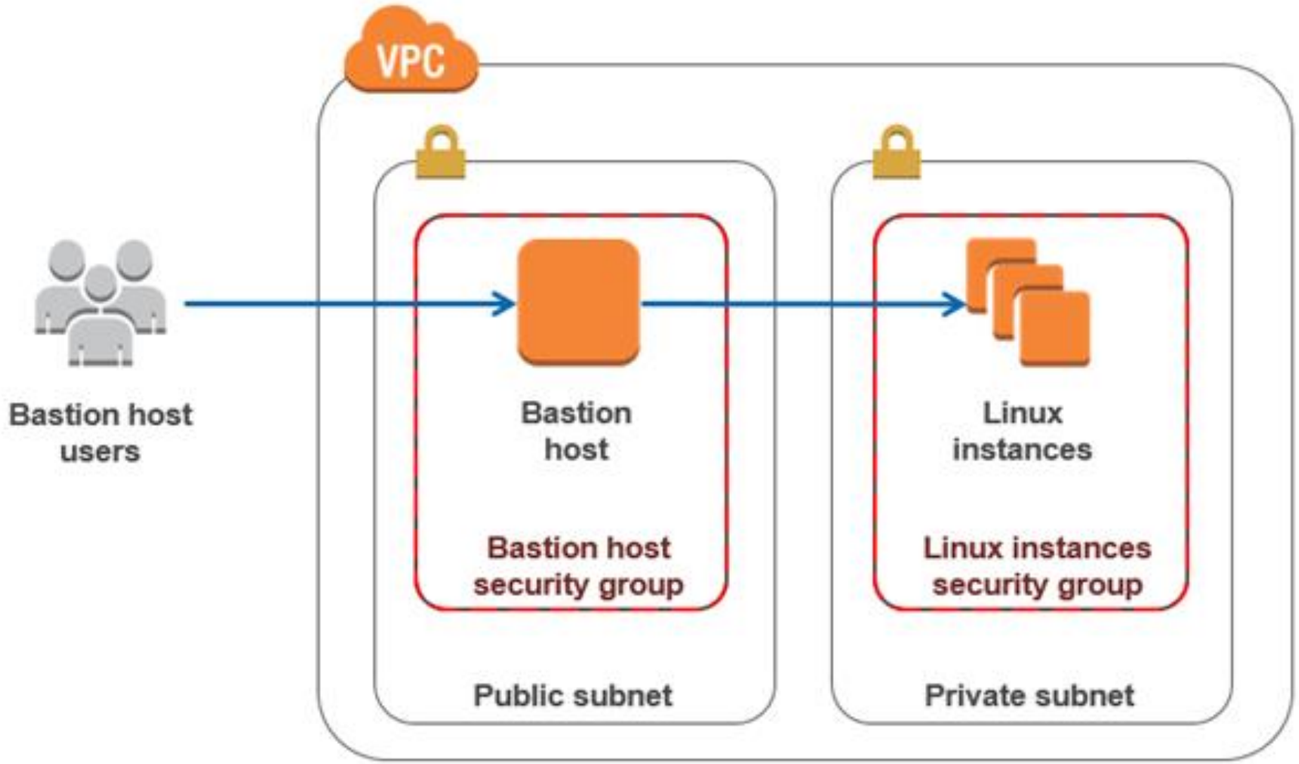
Steps to perform:

1. Go to your Amazon Console
2. Open the VPC dashboard
3. Choose Peering Connections on the left navigation pane
4. Click on the Create Peering Connection button
5. Accept the connection request from the Peering Connections dashboard

Bastion Host

Bastion Host

A bastion host is a server whose purpose is to provide access to a private network from an external network, such as the internet.

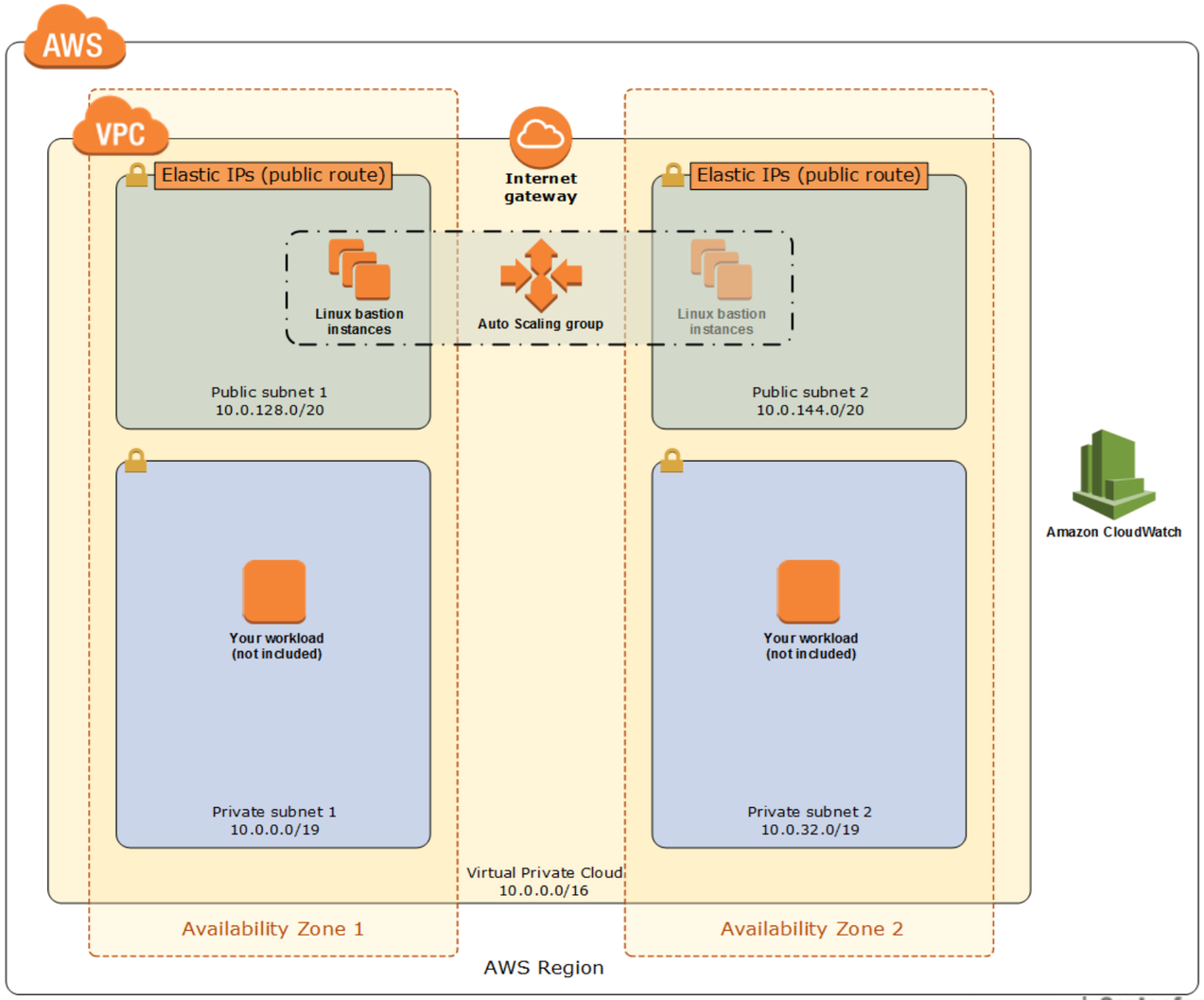


Bastion host

Source: https://aws.amazon.com/blogs/security/how-to-record-ssh-sessions-established-through-a-bastion-host/

Bastion Host: Architecture

The following diagram shows the Linux bastion host architecture on AWS:



Source: https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html

Direct Connect

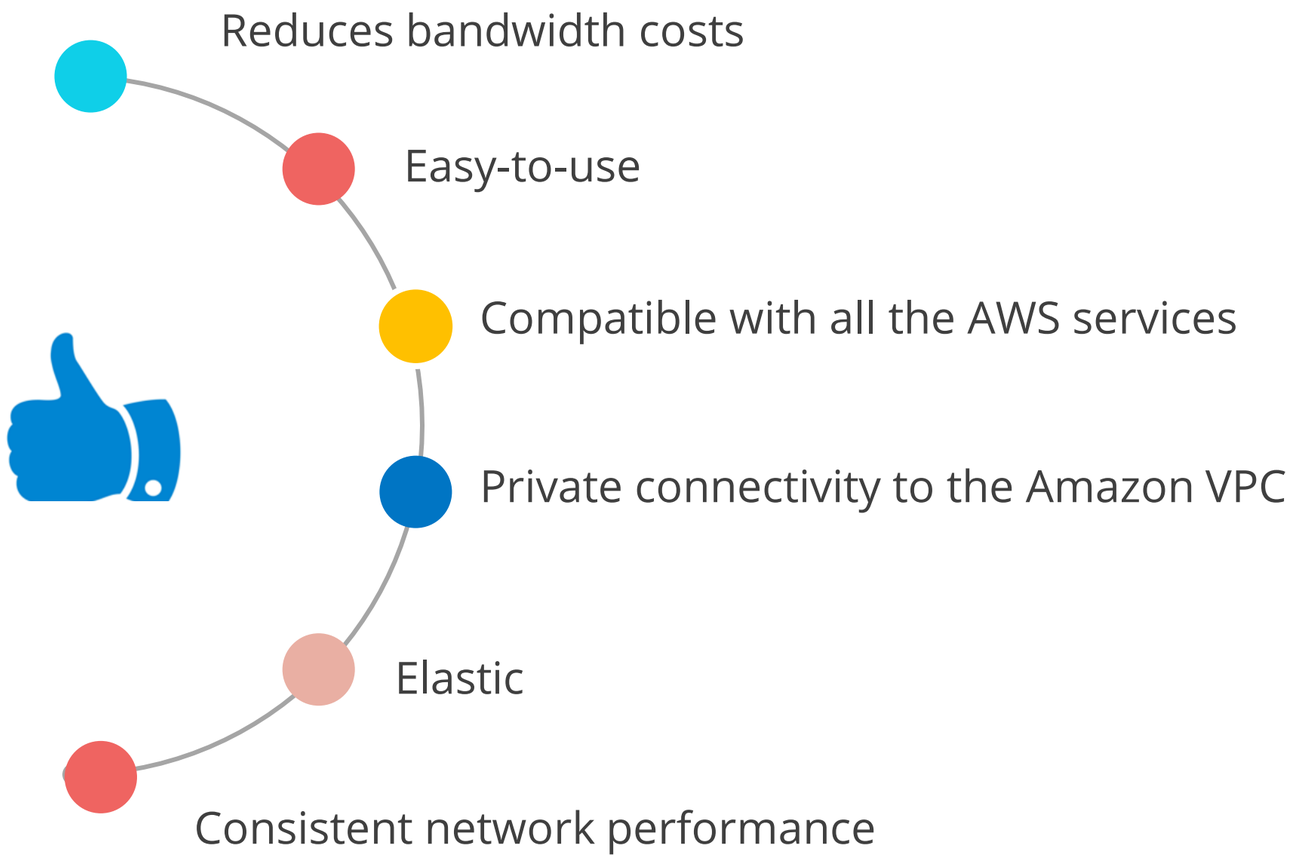
Direct Connect

AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from the user's premises to AWS.

More about Direct Connect:

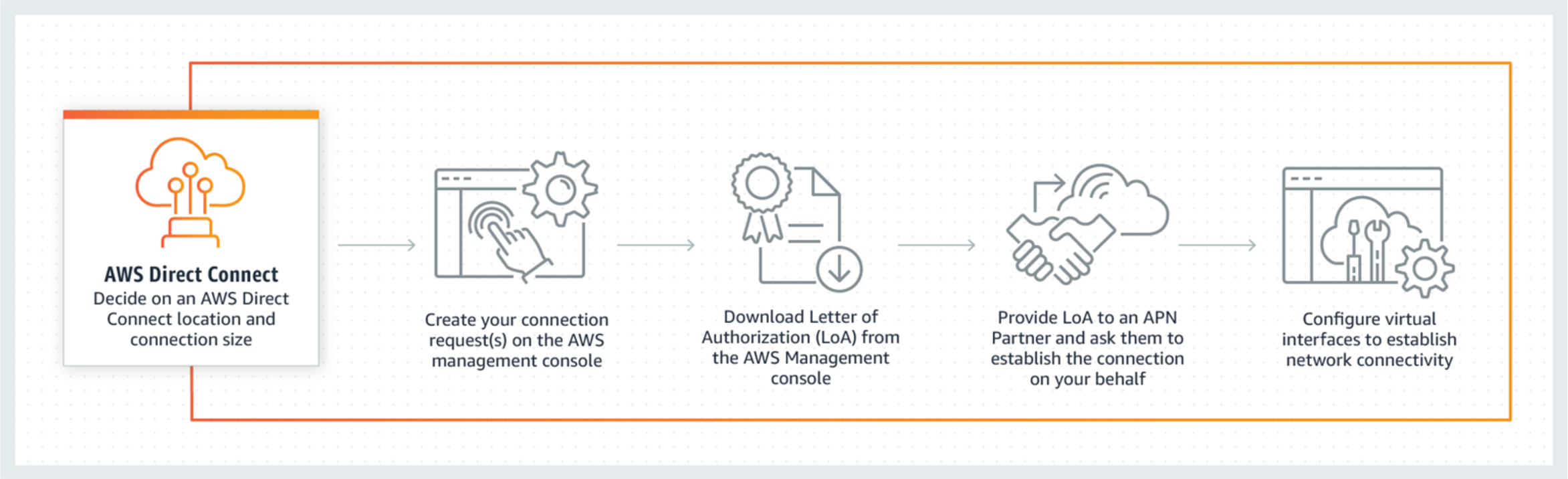
01	It helps to establish private connectivity between AWS and the data center, office, or colocation environment.
02	It helps to establish a dedicated connection between the network and one of the AWS Direct Connect locations.

Benefits of Direct Connect



Working of Direct Connect

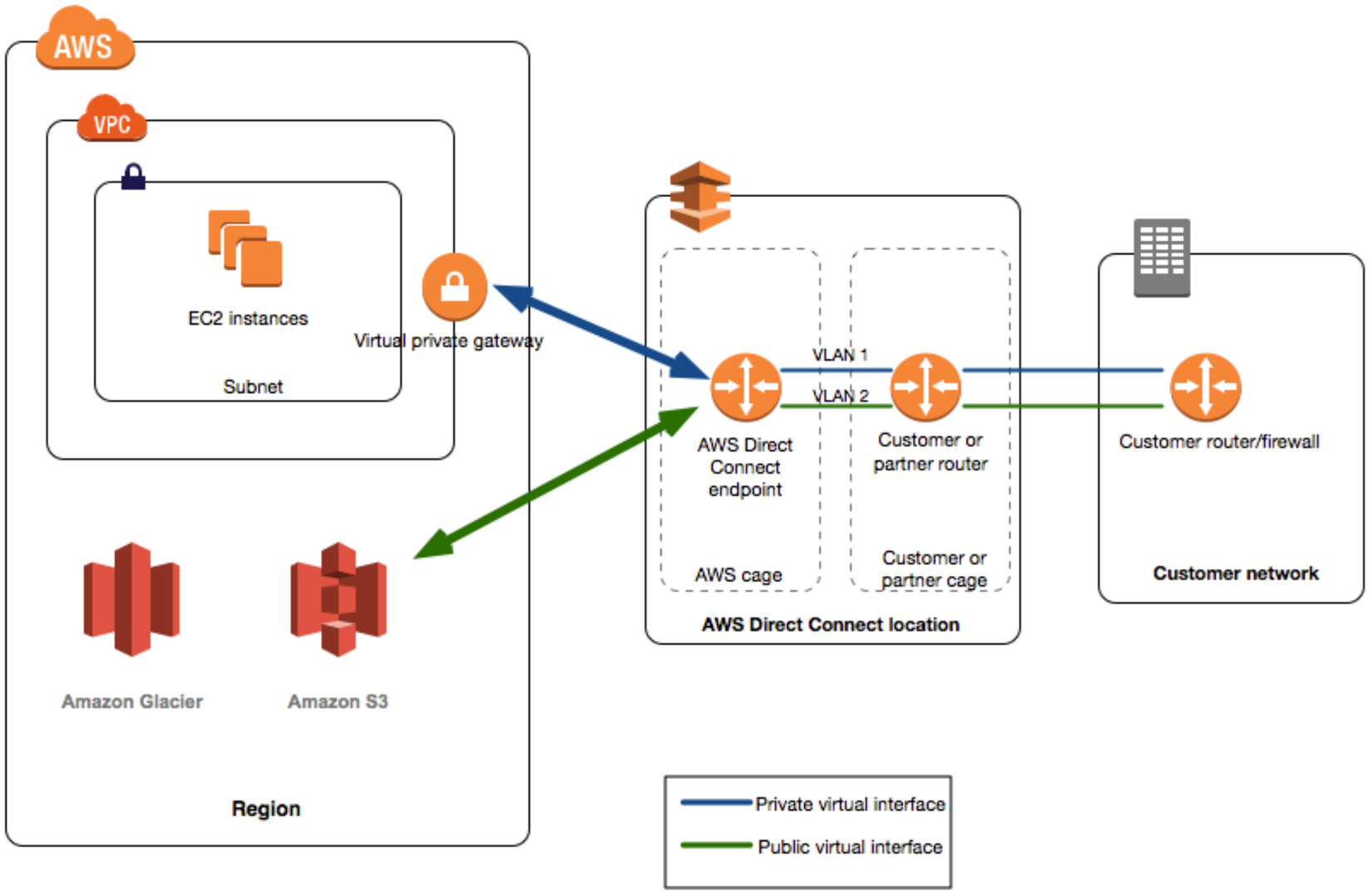
The following diagram shows the working of Direct Connect:



Source: https://aws.amazon.com/directconnect/?nc=sn&loc=1

Working of Direct Connect

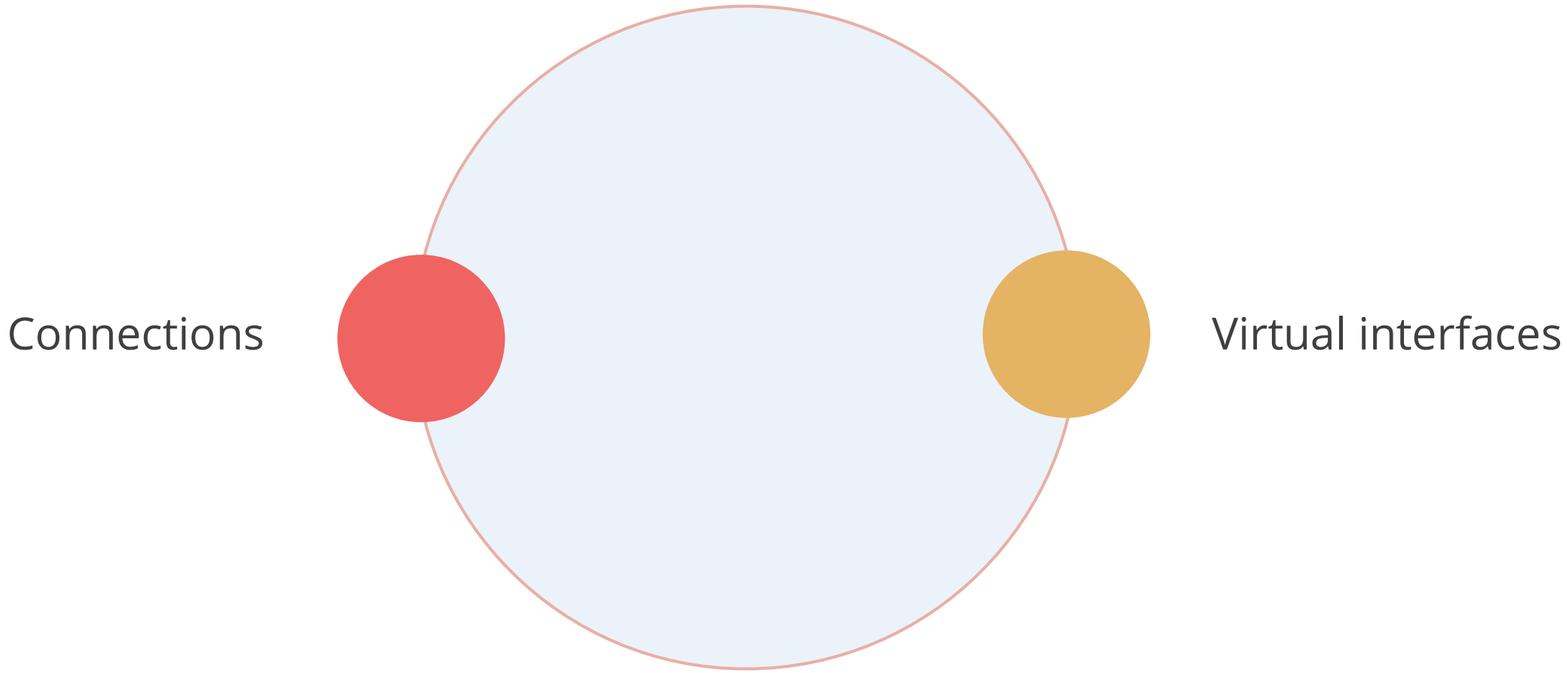
The following diagram shows how AWS Direct Connect interfaces with the network:



Source: https://aws.amazon.com/directconnect/?nc=sn&loc=1

Components of Direct Connect

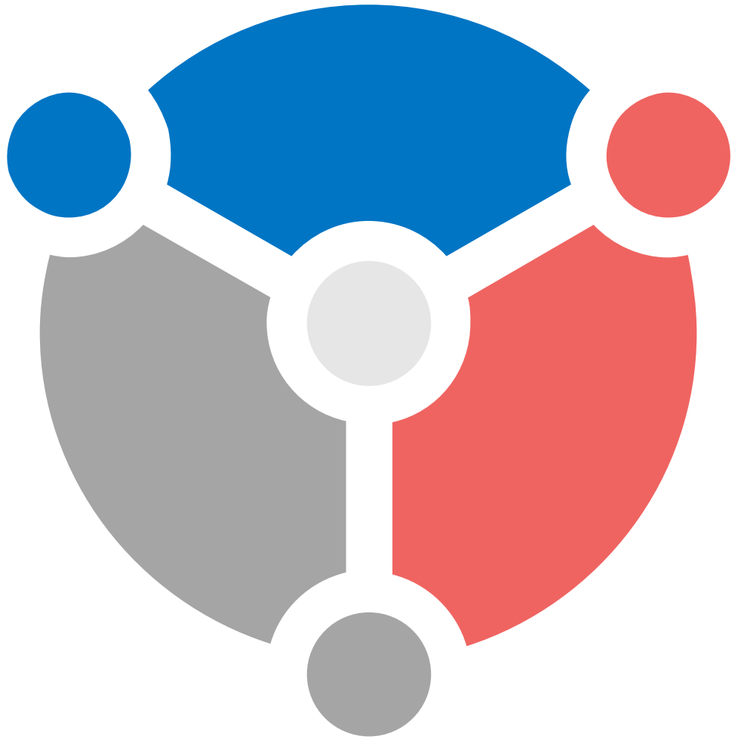
These are the two key components of Direct Connect:



Use Cases of Direct Connect

The following are the use cases of Direct Connect:

Working with large data sets



Real-time data feeds

Hybrid environments

Direct Connect Costs

The following are the costs associated with Direct Connect:

01	Dedicated connections
02	Hosted connections
03	Data transfer
04	TCO calculator
05	AWS pricing calculator
06	Economics resource center

Virtual Private Network (VPN) Connections

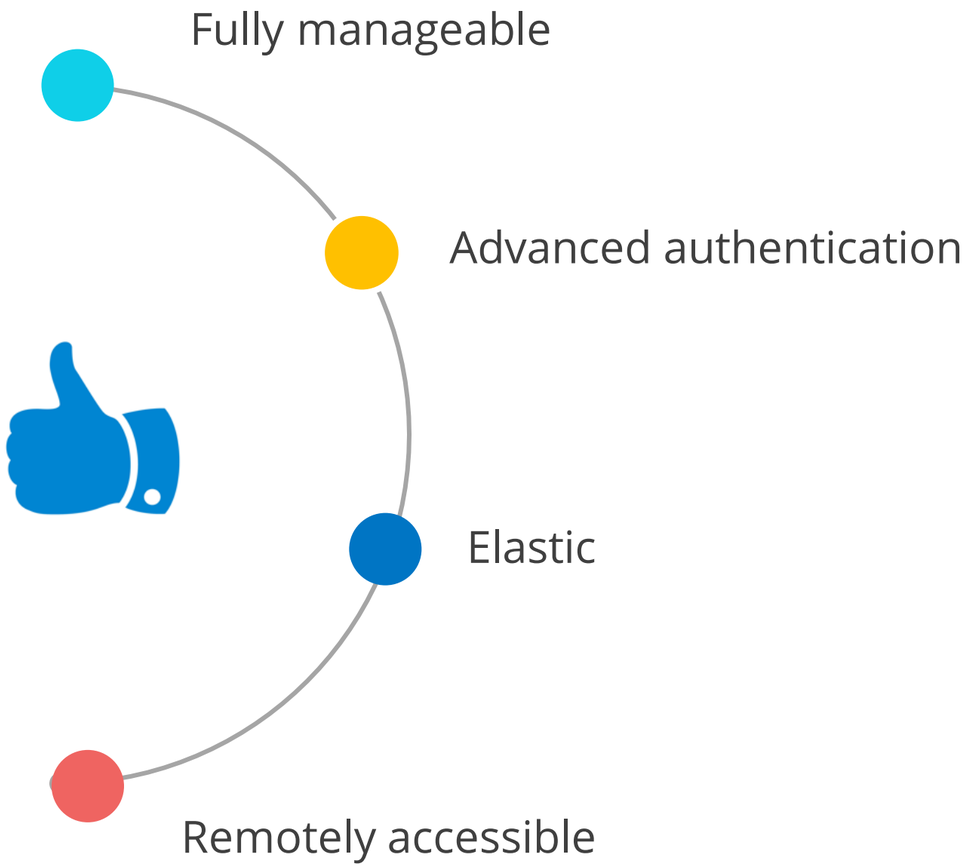
VPN Connections

AWS Virtual Private Network (VPN) solutions establish secure connections between the user's on-premises networks, remote offices, client devices, and the AWS global network.

The following VPN connectivity options help the user to connect the Amazon VPC to remote networks:

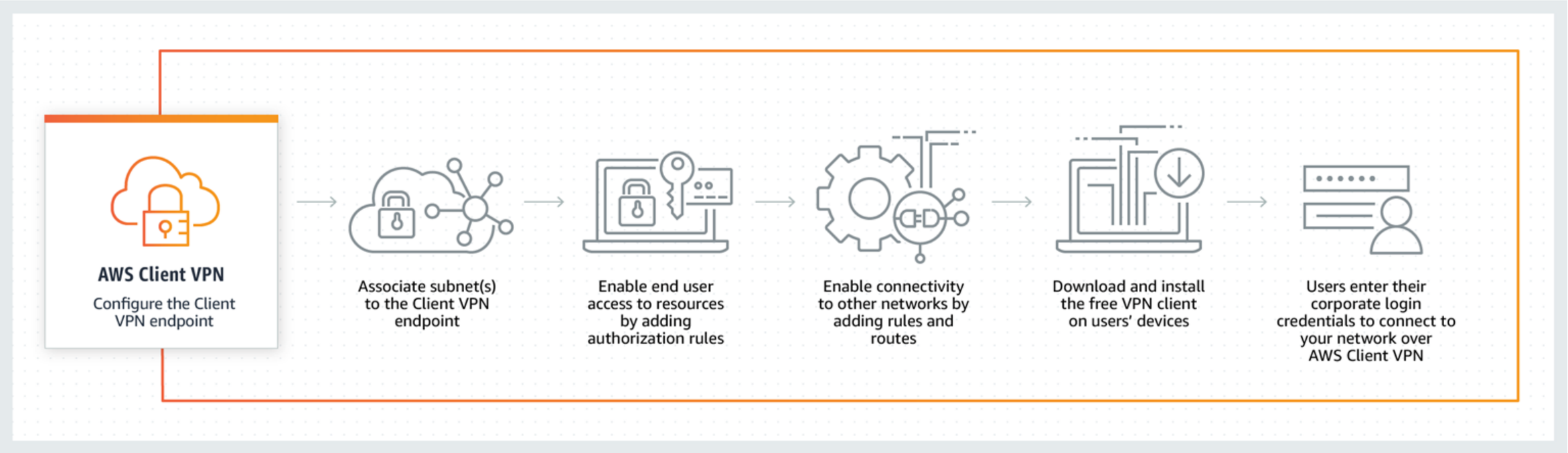
01	AWS Site-to-Site VPN
02	AWS Client VPN
03	AWS VPN CloudHub
04	Third party software VPN appliance

Benefits of VPN Connections



Working of VPN Connections

The following diagram shows the working of VPN connections:

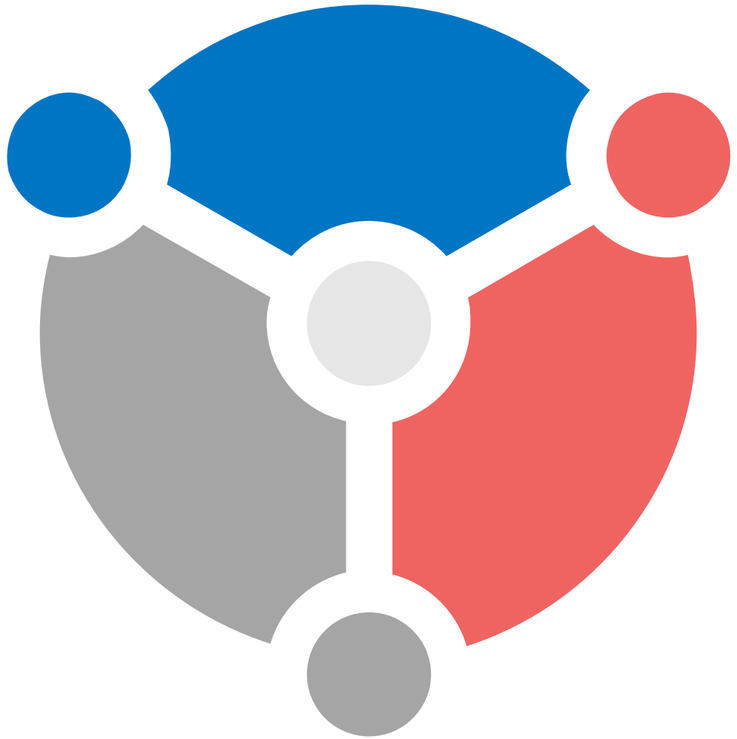


Source: https://aws.amazon.com/vpn/

Use Cases of VPN Connections

The following are the use cases of VPN connections:

Easily access applications in the cloud or on-premises



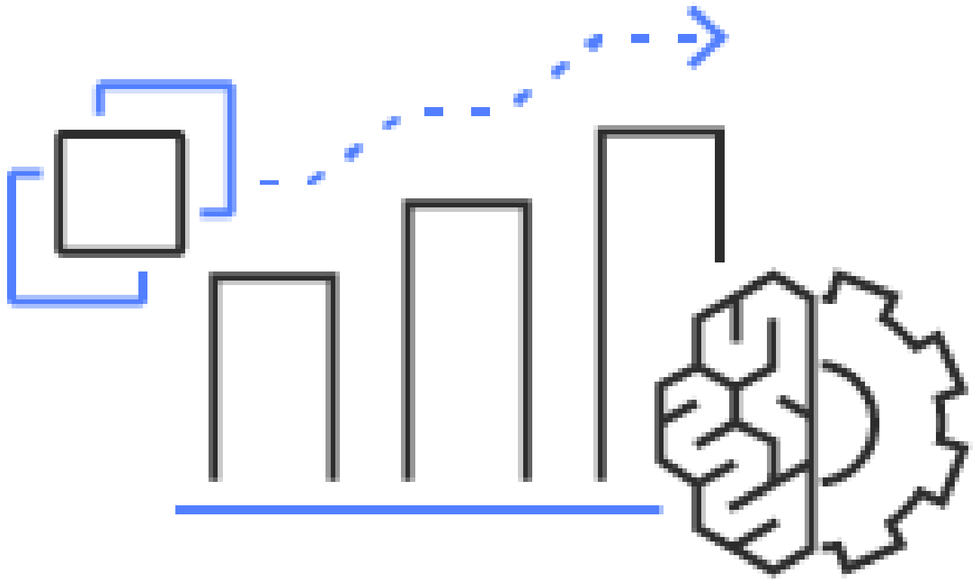
Easily deploy and remove VPN access for temporary workers

Quickly scale remote access

Auto Scaling

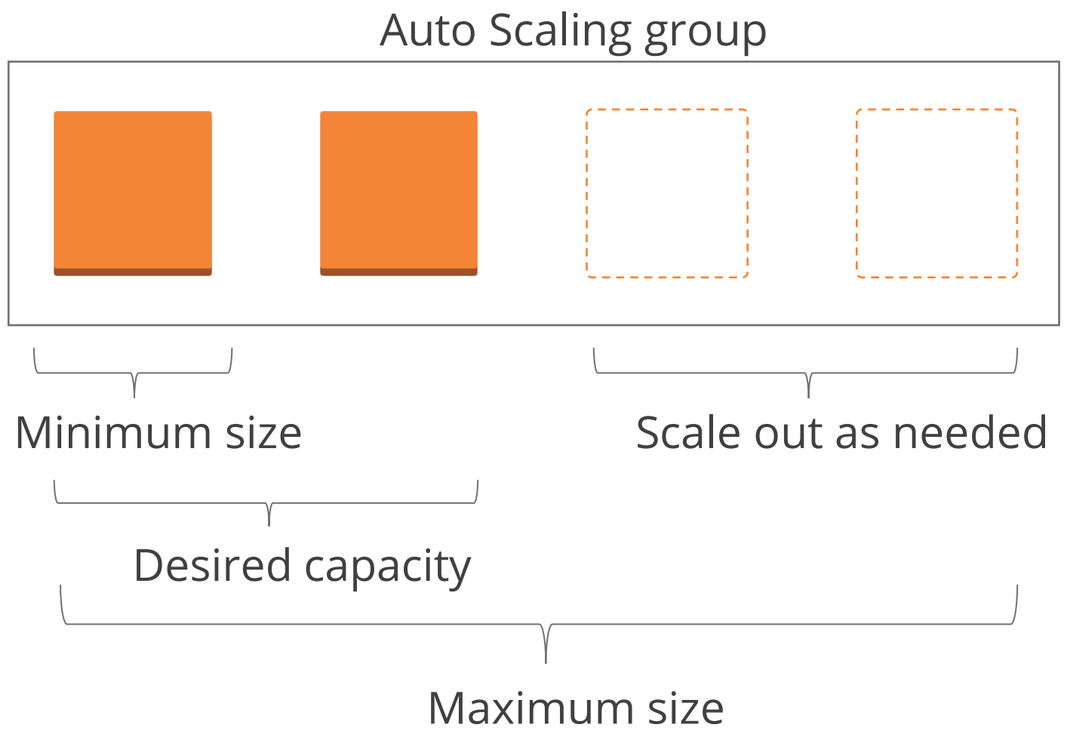
Auto Scaling

Amazon EC2 Auto Scaling helps the users to maintain application availability. It allows them to automatically add or remove EC2 instances according to the conditions defined by them.



Auto Scaling Groups

A collection of EC2 instances is called an Auto Scaling group. Users can specify the minimum number of instances in each group, and Auto Scaling ensures that the group never goes below the minimum size.



Auto Scaling Benefits

- Better fault tolerance
- Increased application availability
- Lower costs

Amazon EC2 Auto Scaling can determine the health of an instance. It can terminate the instance and replace it with a new one.

Auto Scaling Benefits

- Better fault tolerance
- **Increased application availability**
- Lower costs

Amazon EC2 Auto Scaling ensures that the application always has the right amount of computing and proactively provisions capacity with Predictive Scaling.

Auto Scaling Benefits

- Better fault tolerance
- Increased application availability
- Lower costs

Amazon EC2 Auto Scaling adds instances only when needed and it can scale across purchase options to optimize performance and cost.

Amazon Elastic Load Balancer

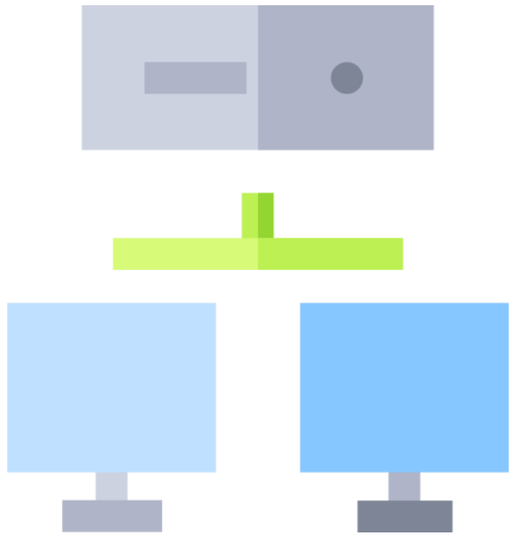
Why Is Load Balancing Needed?

Load balancing is needed to:

01	Prevent traffic overload on any server
02	Improve application responsiveness
03	Increase availability of applications
04	Avoid single point of failure in servers

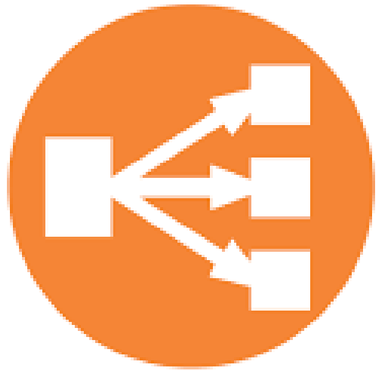
What Is Load Balancing?

Load Balancing refers to the distribution of network traffic across multiple servers or instances of virtual machines that host the application.



What Is Amazon Elastic Load Balancer?

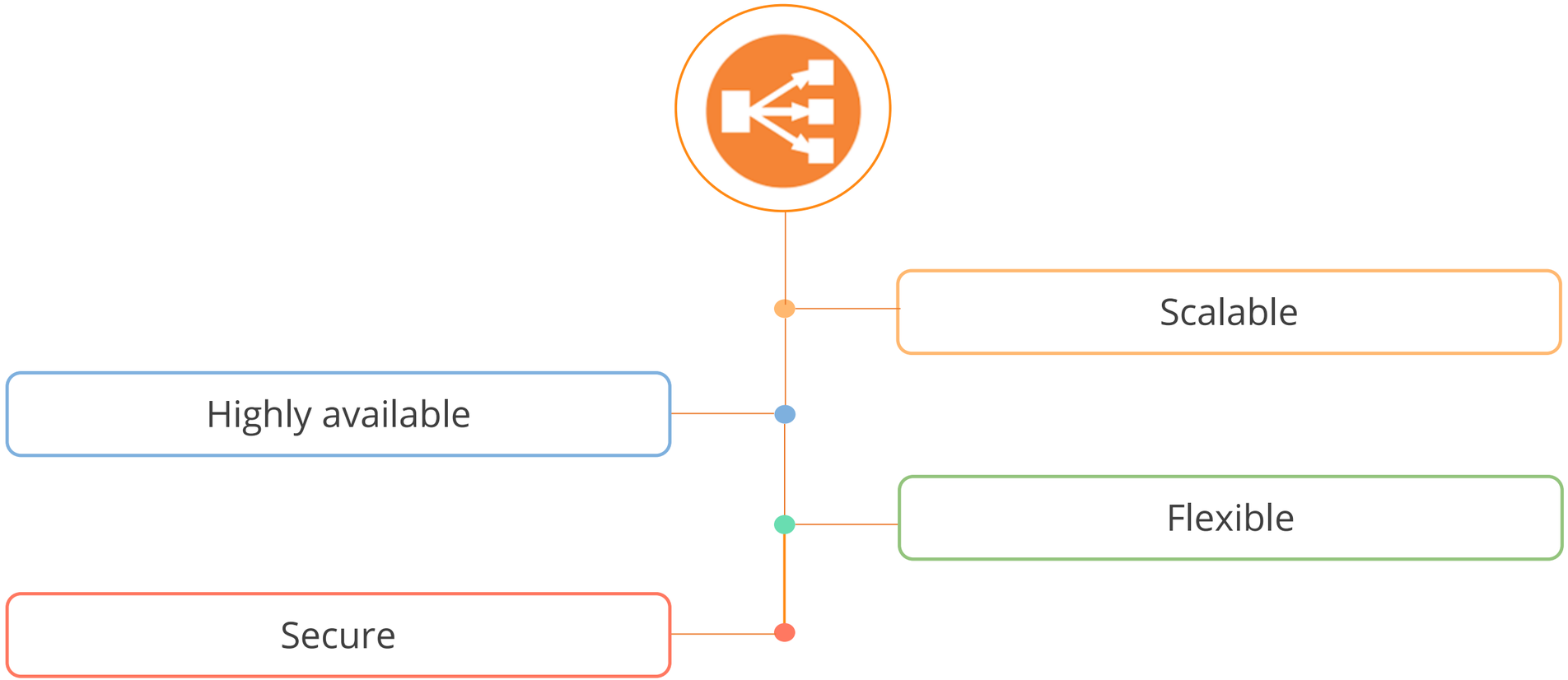
Amazon Elastic Load Balancer (ELB) is a load balancing service offered by AWS that distributes incoming application traffic across multiple targets such as Amazon EC2 instances, containers, and Lambda functions.



Amazon Elastic Load Balancer

Benefits of Amazon ELB

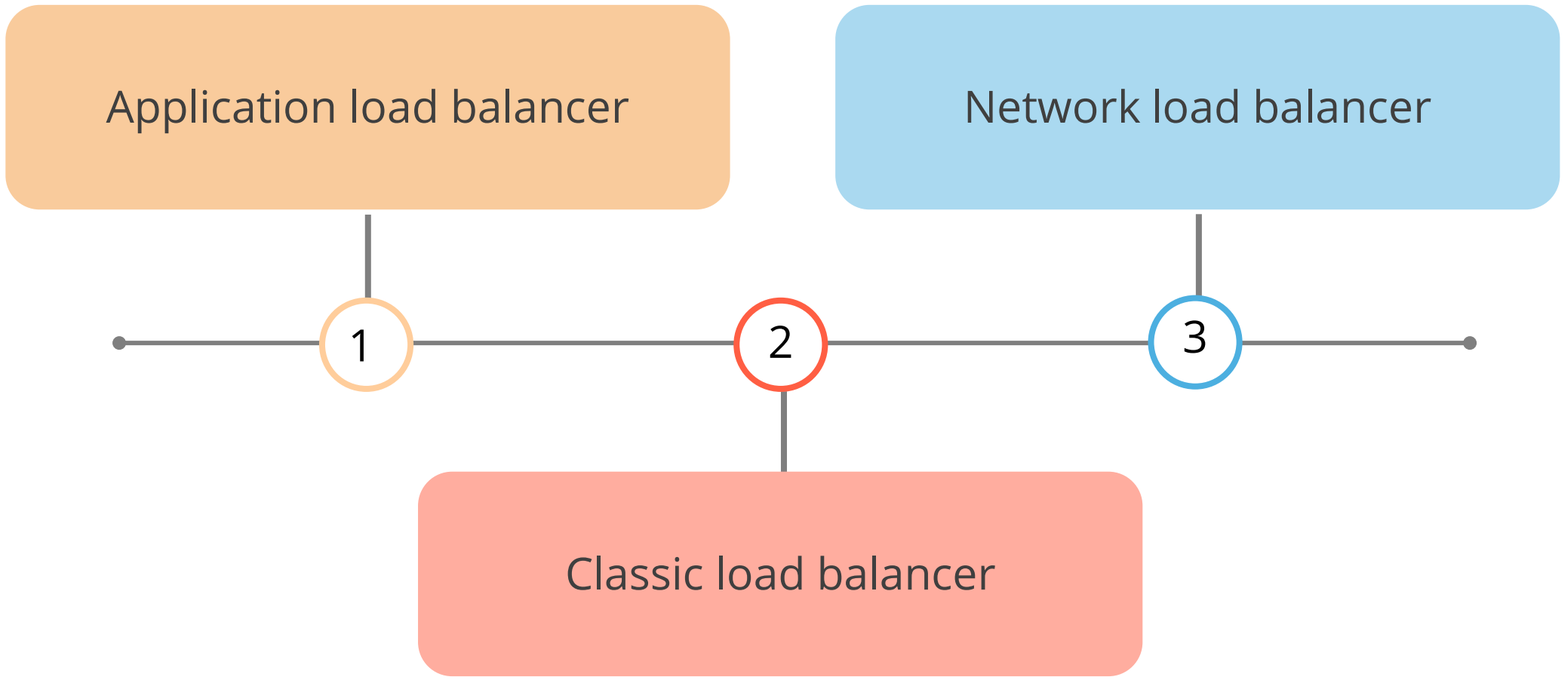
Amazon ELB offers the following benefits:



Types of Amazon Load Balancers

Types of Amazon Load Balancers

Amazon ELB offers the following types of load balancers:



Application Load Balancer

01 Application load balancer is used for load balancing of HTTP and HTTPS traffic.

02 It routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) based on the content of the request.

03 It operates on layer 7.

Network Load Balancer

01 Network load balancer is used for load balancing of TCP, UDP, and TLS traffic.

02 It routes traffic to targets within Amazon Virtual Private Cloud (Amazon VPC) regardless of the content of the request.

03 It operates on Layer 4.

Classic Load Balancer

01 Classic load balancer provides basic load balancing across multiple Amazon EC2 instances.

02 It is best suited for application built on the EC2-Classic network.

03 It operates on both layer 4 and layer 7.

Assisted Practice

Set Up an Autoscaled Environment

Duration: 20 min.

Problem Statement:

You are given a project to set up a autoscaled environment.

Assisted Practice: Guidelines to Set Up an Autoscaled Environment

Steps to perform:

1. Go to your Amazon Console
2. Open the EC2 dashboard
3. Create a launch template
4. Create a launch configuration
5. Create an auto scaling group
6. Enable load balancing

Key Takeaways

- Amazon Virtual Private Cloud (VPC) enables the user to launch AWS resources into a virtual network.
- A route table contains a set of rules, called routes, that are used to determine where network traffic from the subnet or gateway is directed.
- A VPC peering connection is a networking connection between two VPCs that enables the user to route traffic between them using private IPv4 adresses or IPv6 addresses.
- AWS Virtual Private Network (VPN) solutions establish secure connections between the user's on-premises networks, remote offices, client devices, and the AWS global network.

Lesson-End Project

Duration: 60 min.

Set Up Multiple Virtual Networks on the AWS Cloud

Problem Statement:

You have been asked to set up multiple virtual networks on the AWS cloud for various departments in your organization.

Perform the following:

- Open the Amazon VPC dashboard
- Create a VPC with a single subnet for the production team's virtual network
- Create a VPC with two subnets for the development team's virtual network
- Attach the relevant route tables to all the subnets