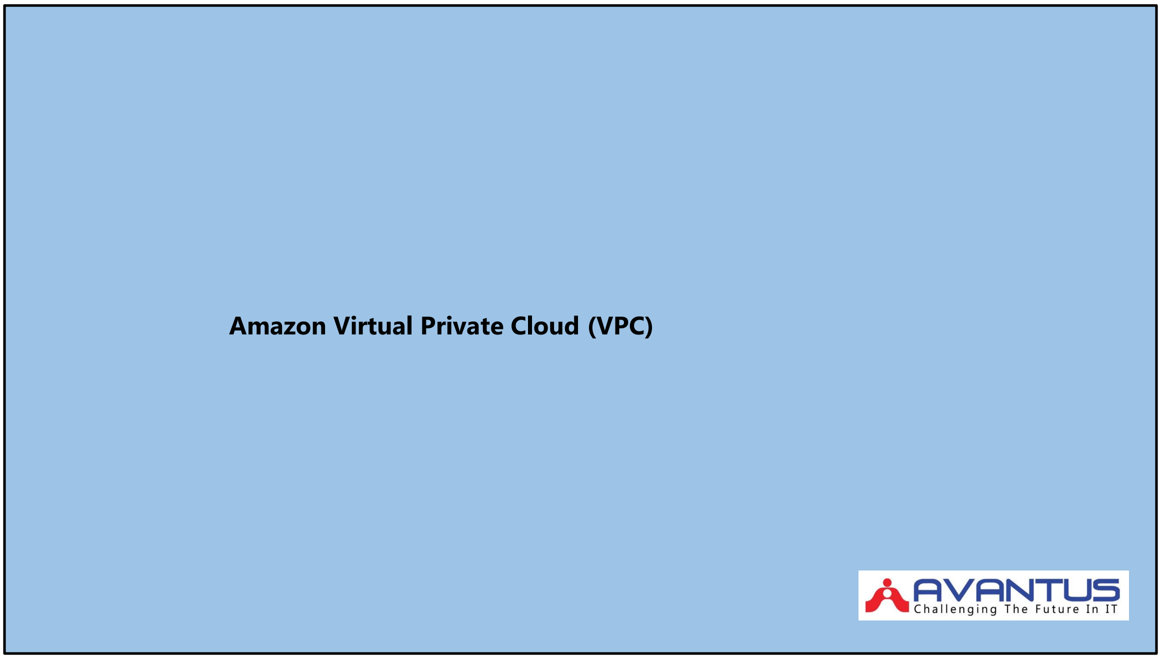
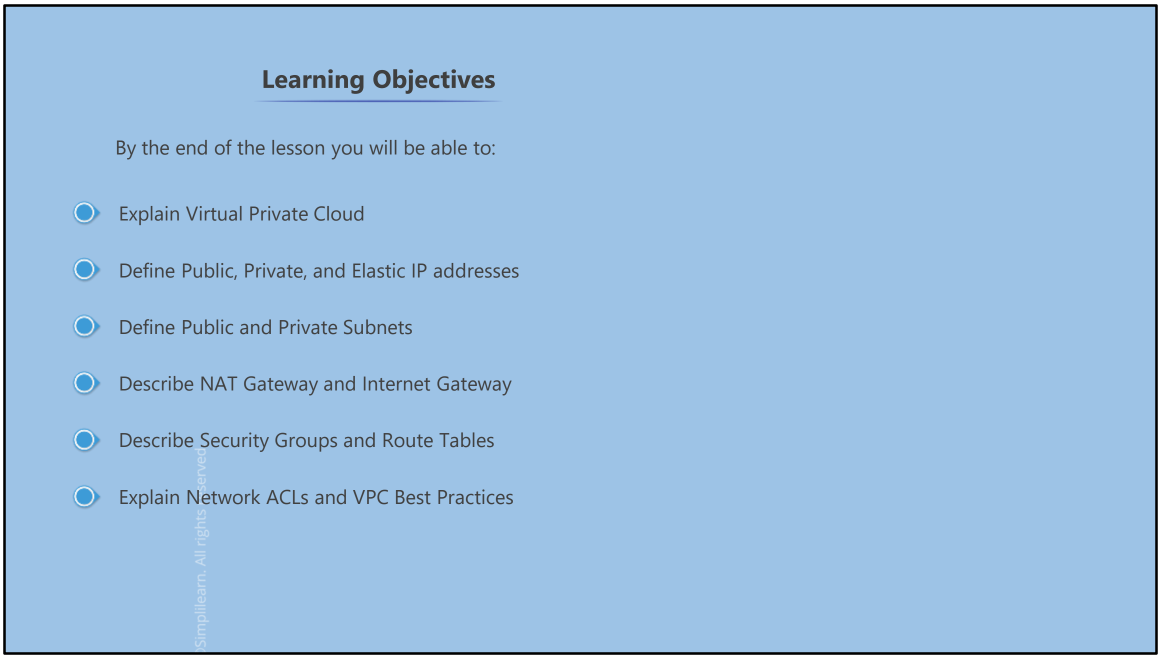


Amazon Virtual Private Cloud (VPC)

Welcome to the fourth lesson of the AWS Solutions Architect Associate level course; Amazon Virtual Private Cloud (VPC).

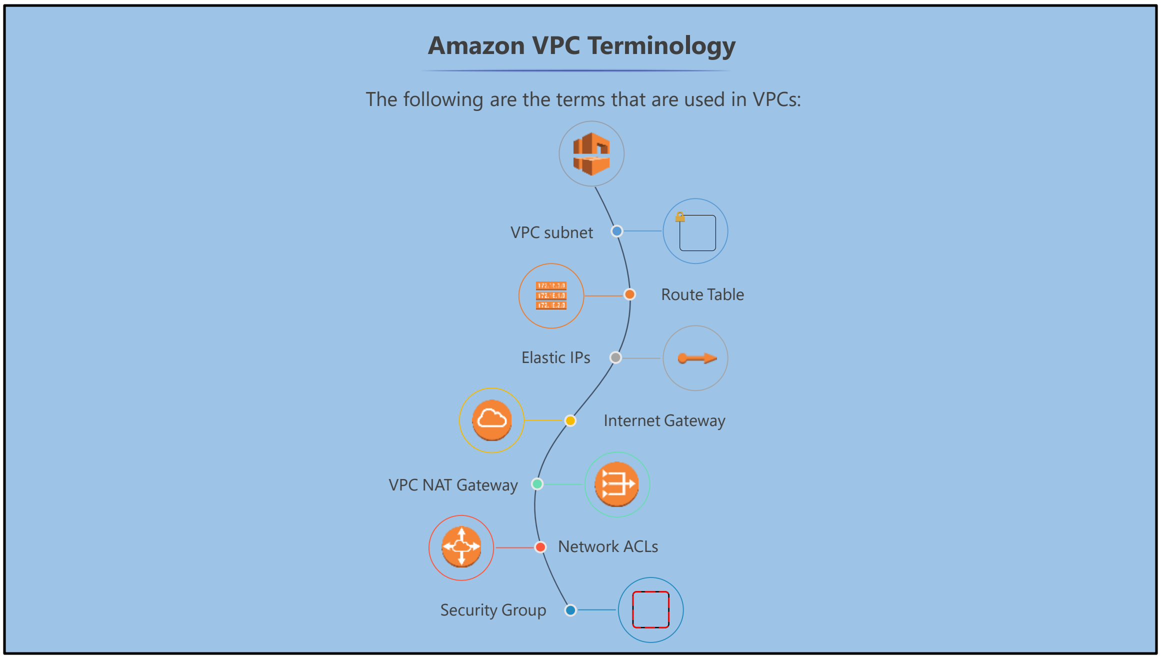


Learning Objectives

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

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

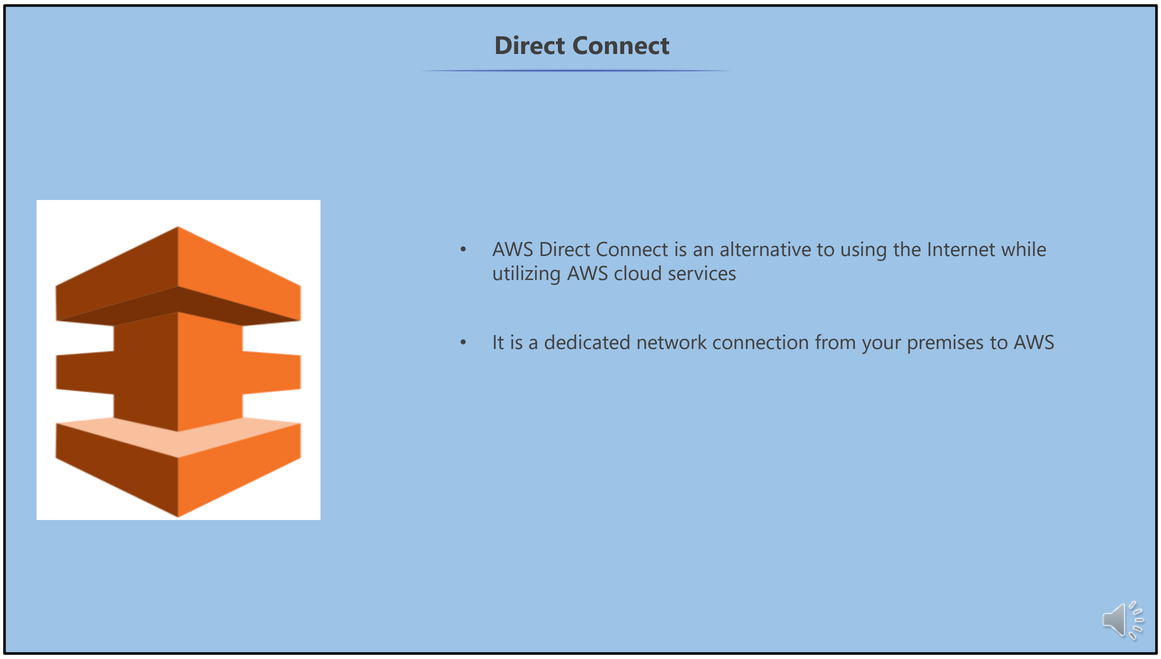
By the end of this lesson you'll be able to:
Have an overview of Virtual Private Clouds and understand the concept
Understand the difference between public, private, and Elastic IP addresses
Learn about public and private subnets
Understand what an Internet Gateway is
Learn how route tables are used
Define what a NAT Gateway is and when it is used
Understand the importance of Security Groups
Describe Network ACLs and their usage
Review VPC best practices and the costs associated with running a VPC



Amazon VPC Terminology

The following are the terms that are used in VPCs:

The following are the terms that are used in VPCs:
Subnets
Route Tables
Elastic IPs
Internet Gateway
NAT Gateways
Network ACLs
Security Groups



Direct Connect

- AWS Direct Connect is an alternative to using the Internet while utilizing AWS cloud services
- It is a dedicated network connection from your premises to AWS

AWS Direct Connect is an alternative to using the Internet to utilize AWS cloud services.

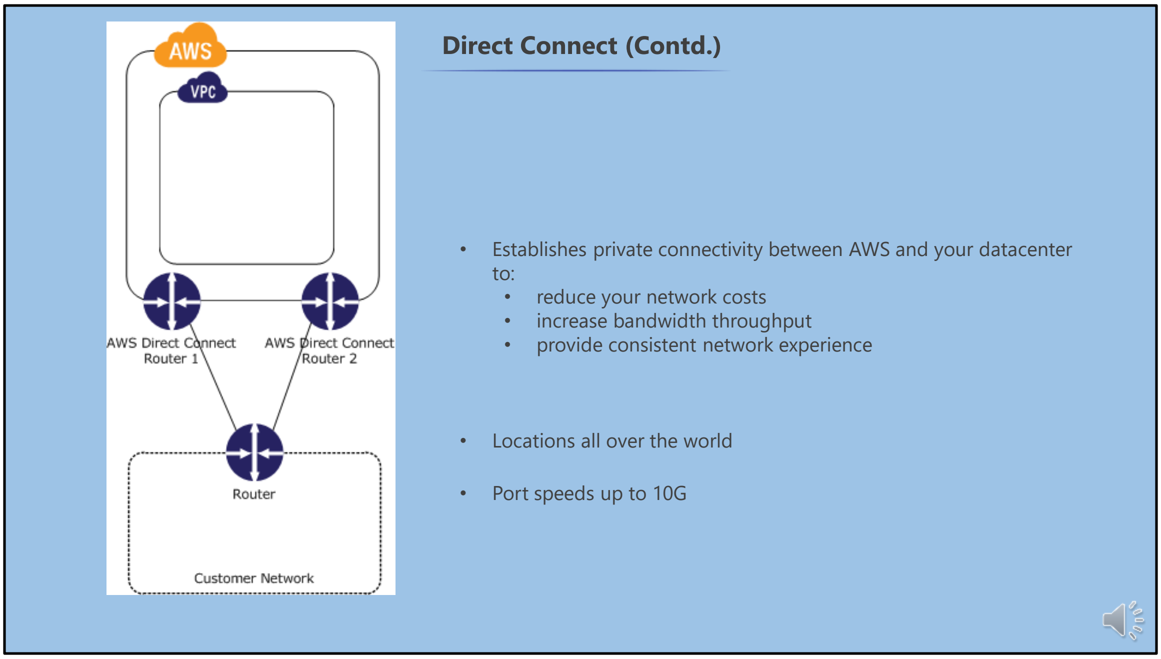
It makes it easy to establish a dedicated network connection from your premises to AWS.

Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Available in a variety of locations all over the world.

Variety of port speeds ranging from 50M to 10G.

More expensive, but better connections.



Direct Connect (Contd.)

- Establishes private connectivity between AWS and your datacenter to:
  - reduce your network costs
  - increase bandwidth throughput
  - provide consistent network experience
- Locations all over the world
- Port speeds up to 10G

AWS Direct Connect is an alternative to using the Internet to utilize AWS cloud services.

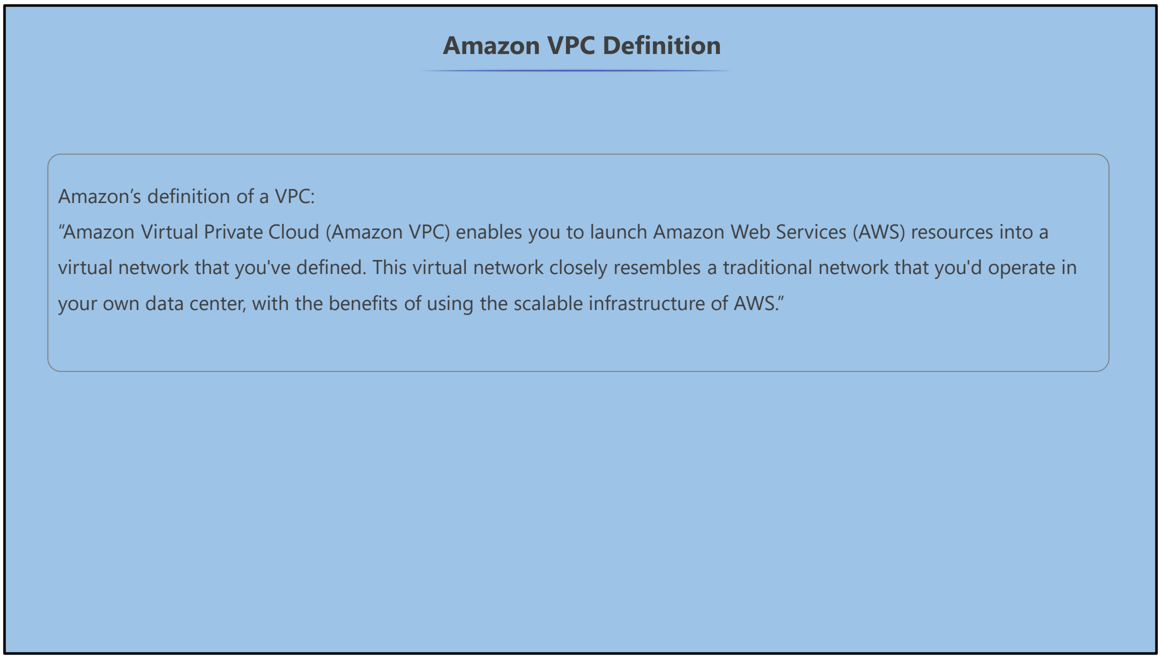
It makes it easy to establish a dedicated network connection from your premises to AWS.

Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Available in a variety of locations all over the world.

Variety of port speeds ranging from 50M to 10G.

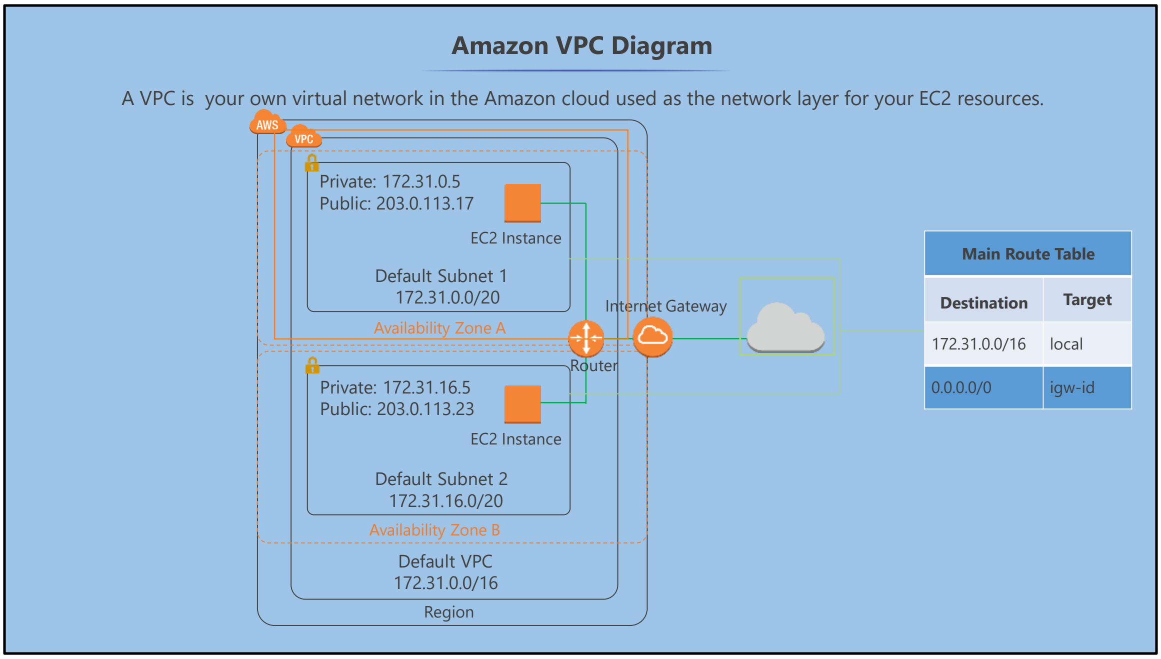
More expensive, but better connections.



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 defines a VPC as:
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.

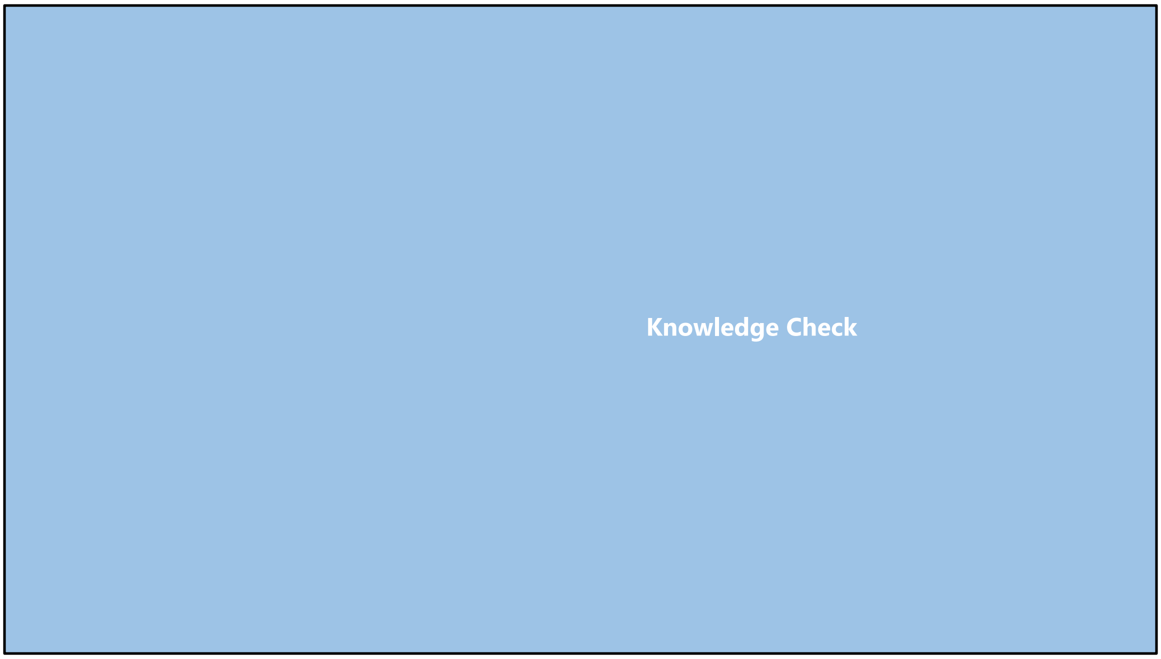
Main Route Table	
Destination	**Target**
172.31.0.0/16	local
0.0.0.0/0	igw-id

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

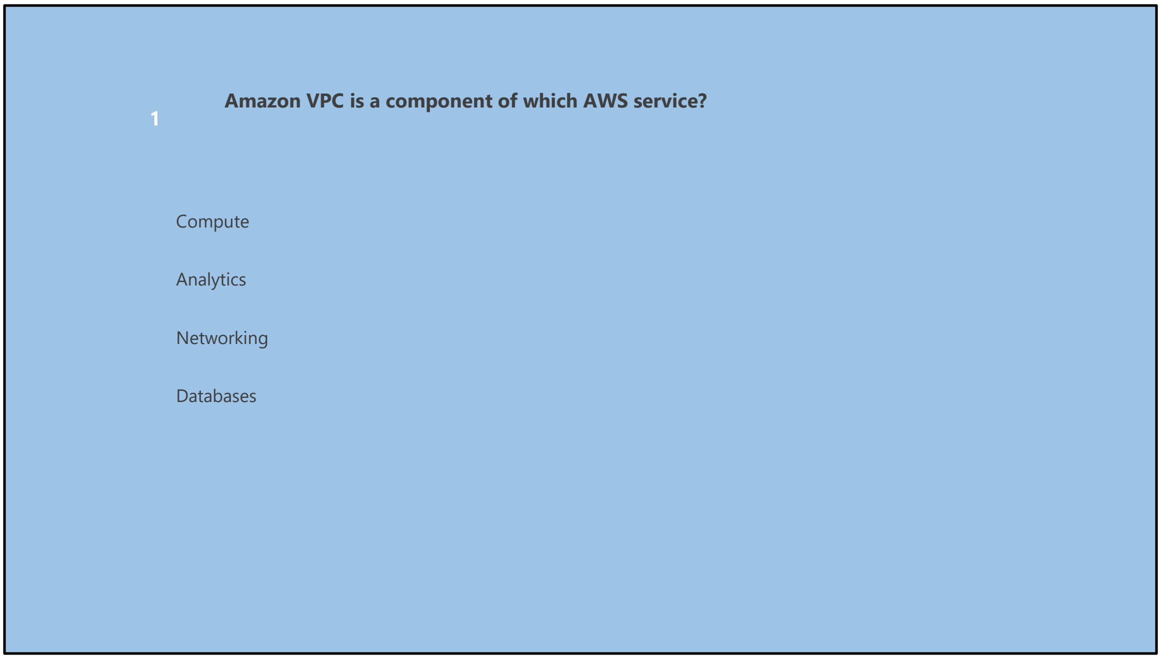
This is a diagram of the default VPC.

VPC is a critical part of the exam and you need to know all the key concepts and how it differs from your own networks. You also need to know how to create your own VPC from scratch. Each VPC that you create is logically isolated from other virtual networks in the AWS cloud.

A VPC is fully customizable. You can select the IP address range, create subnets, configure route tables, set up network gateways, and define security settings using security groups and network access control lists (ACL).



Knowledge Check



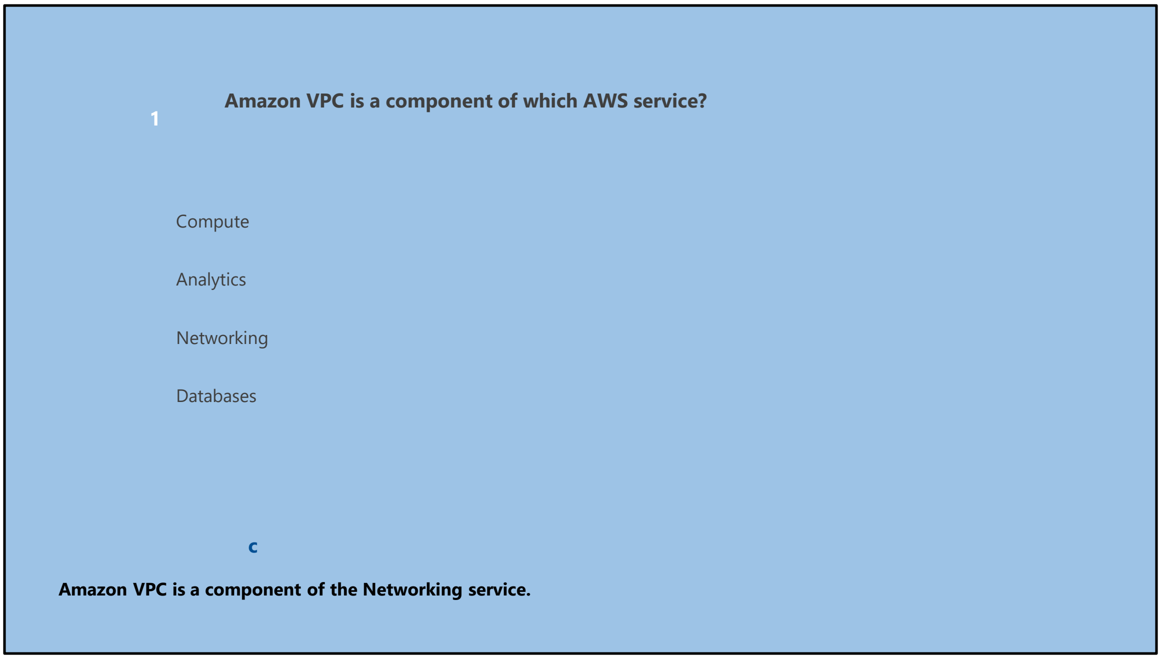
1 **Amazon VPC is a component of which AWS service?**

Compute

Analytics

Networking

Databases



1 **Amazon VPC is a component of which AWS service?**

Compute

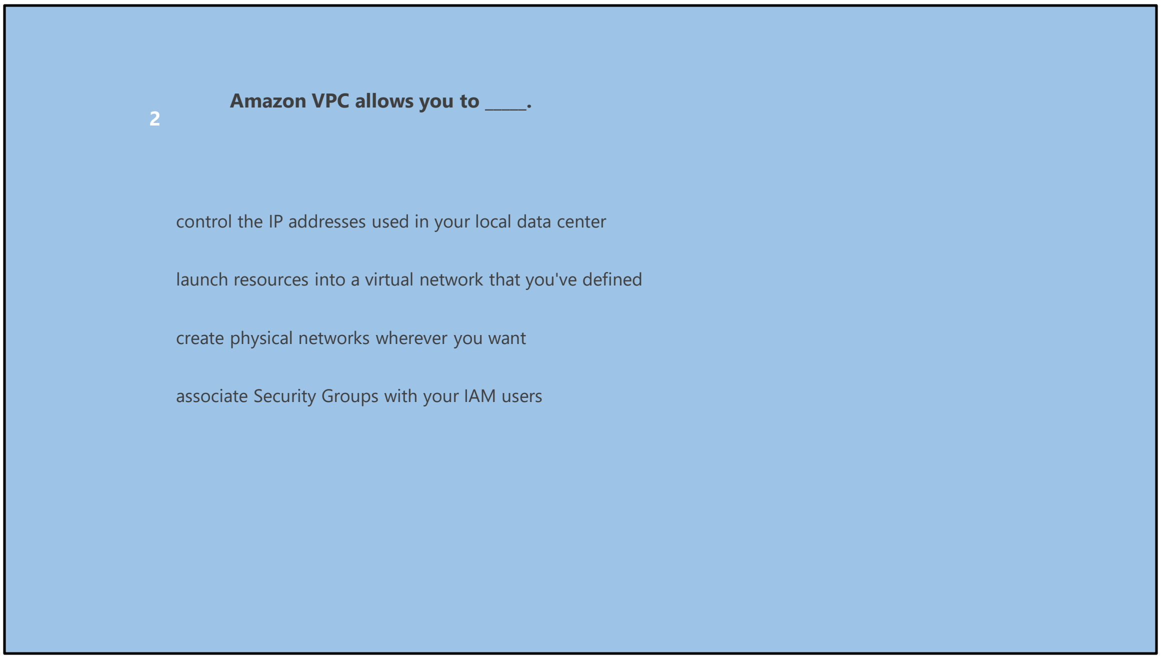
Analytics

Networking

Databases

c

Amazon VPC is a component of the Networking service.



2

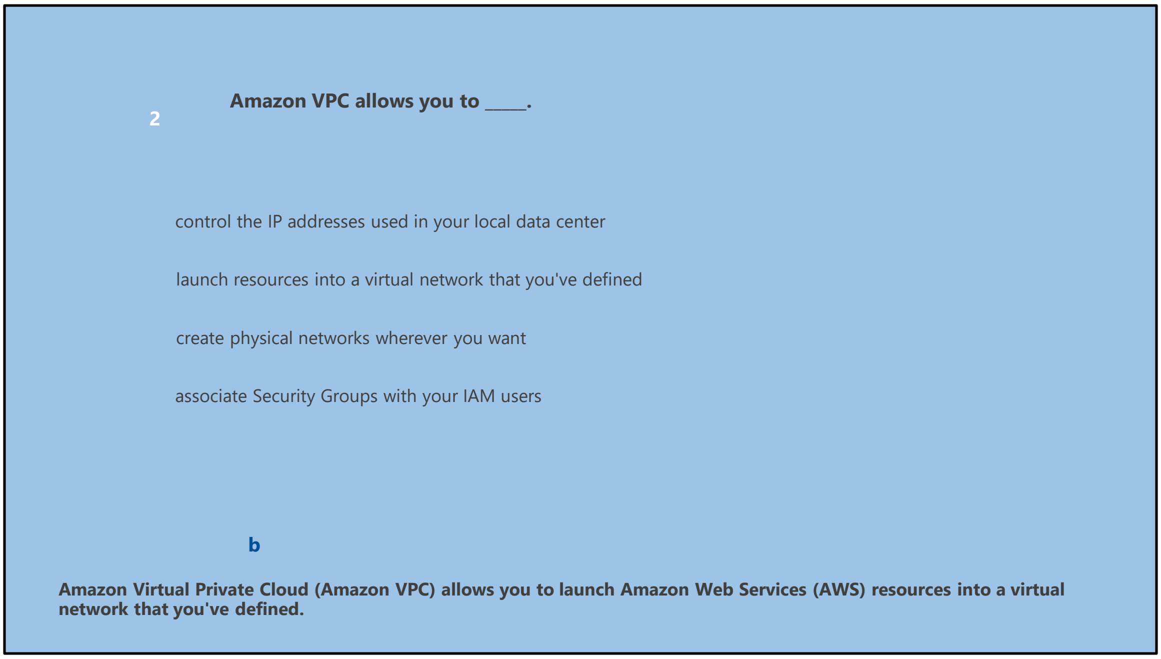
Amazon VPC allows you to _____.

control the IP addresses used in your local data center

launch resources into a virtual network that you've defined

create physical networks wherever you want

associate Security Groups with your IAM users



2

Amazon VPC allows you to _____.

control the IP addresses used in your local data center

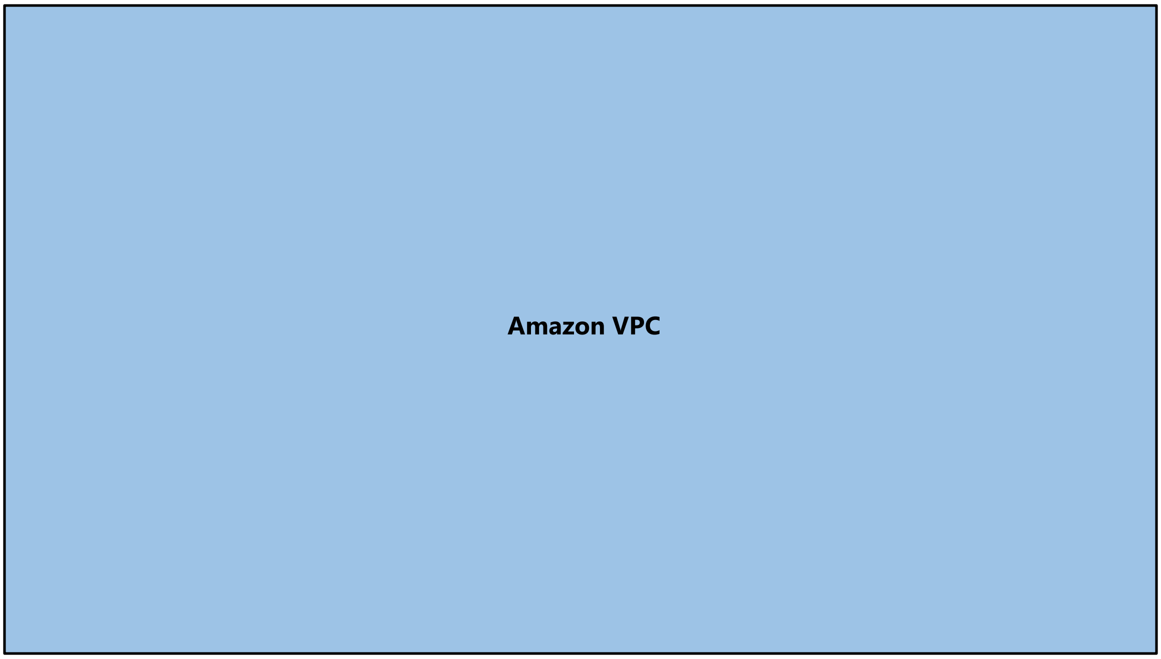
launch resources into a virtual network that you've defined

create physical networks wherever you want

associate Security Groups with your IAM users

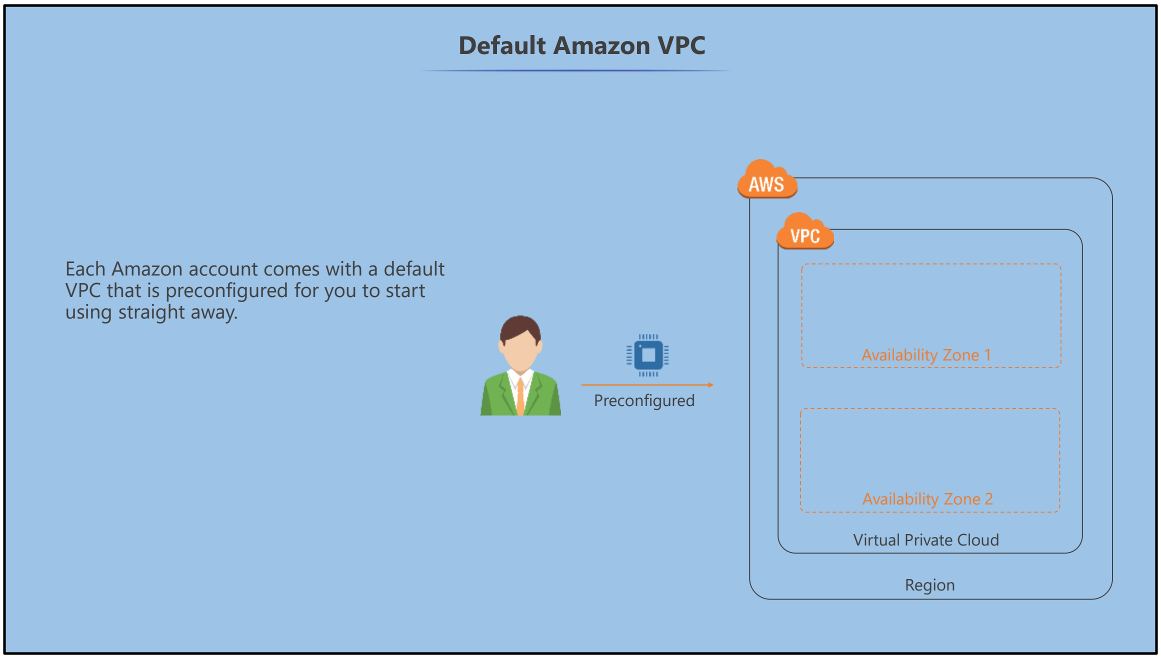
b

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

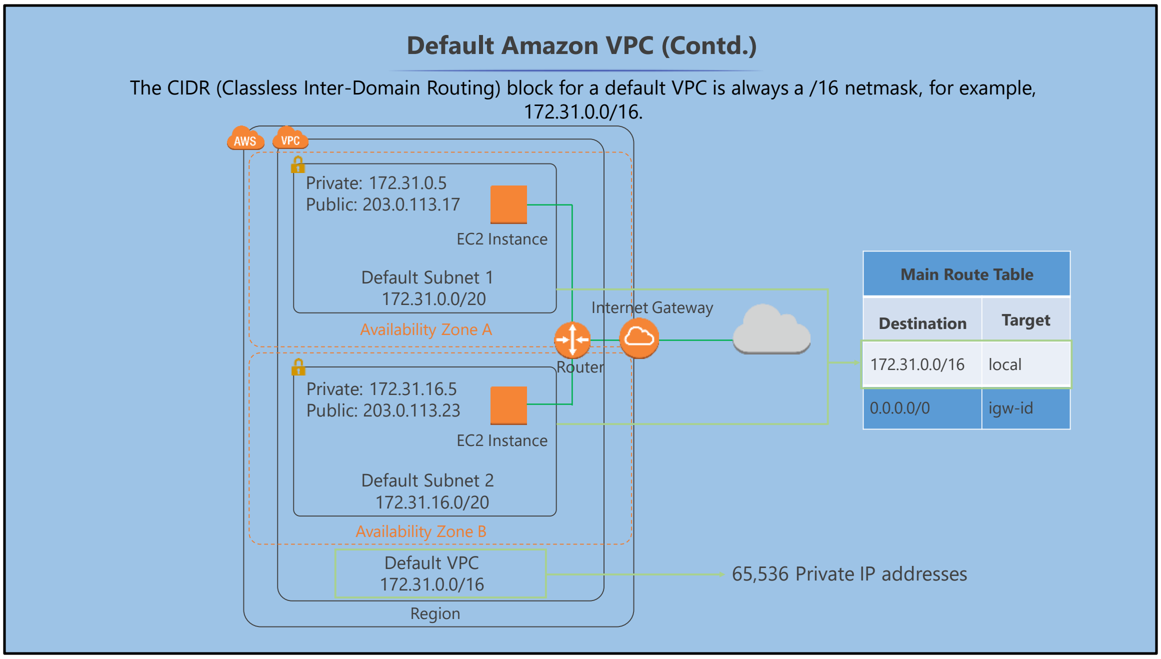
In this section you'll learn how to use Virtual Private Clouds in AWS.



Default Amazon VPC

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

Each Amazon account comes with a default VPC, that is, preconfigured for you to start using straight away. You can launch EC2 instances immediately.
A VPC can span multiple AZs in a region.

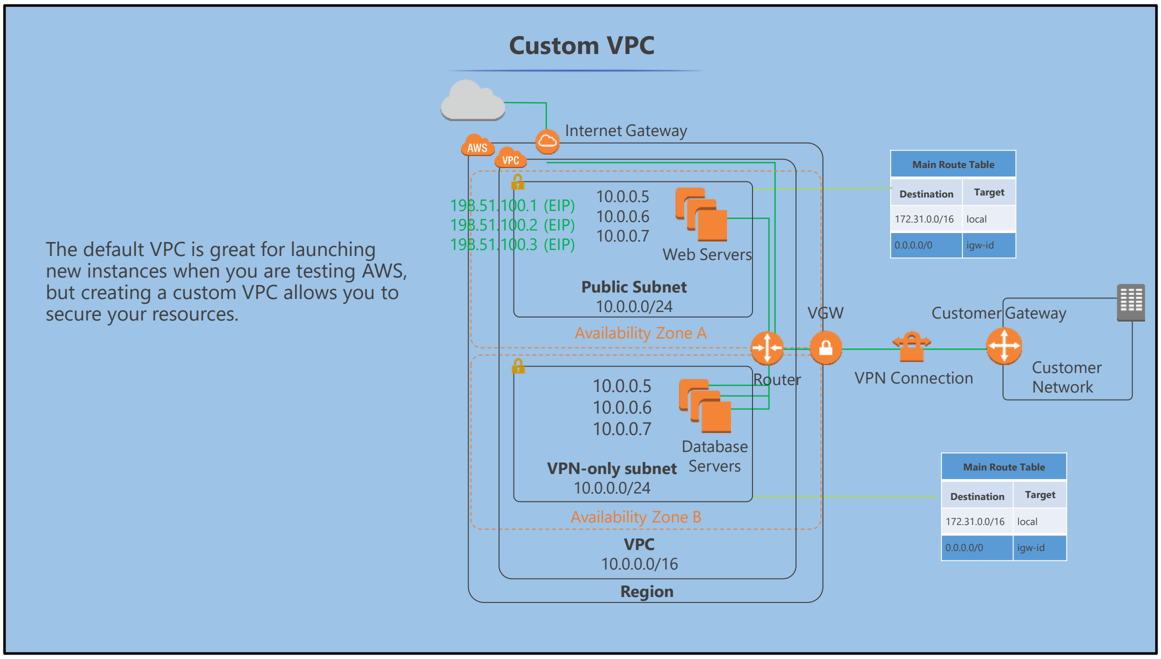


Default Amazon VPC (Contd.)

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

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-id

This is a diagram of the default VPC. The CIDR block for a default VPC is always a /16 netmask, for example, 172.31.0.0/16. This provides up to 65,536 private IP addresses.



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.

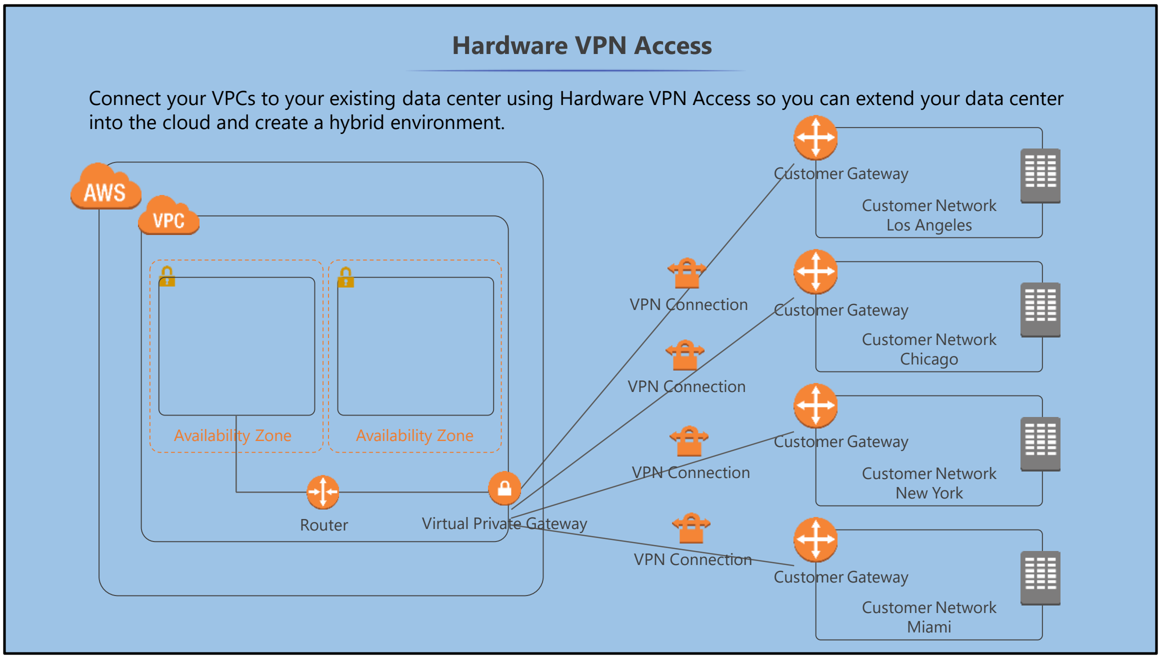
Main Route Table

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-id

Main Route Table

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-id

The default VPC is great for launching new instances when you are testing AWS, but creating a custom VPC allows you to make things more secure. You can also customize your virtual network as you define your own IP address range, create subnets that are both private and public, and strengthen your security settings.



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.

By default, instances that you launch into a virtual private cloud (VPC) can't communicate with your own network.

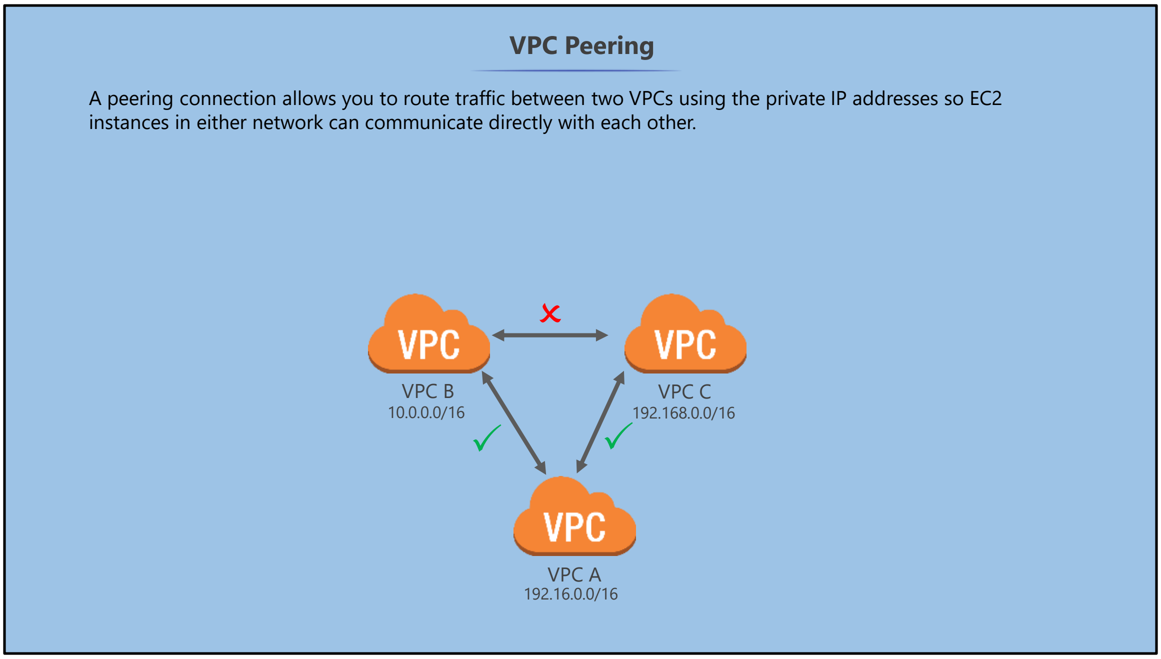
You can connect your VPCs to your existing data center using Hardware VPN Access so you can effectively extend your data center into the cloud, and create a hybrid environment.

Virtual Private Gateway:

A virtual private gateway is the VPN concentrator on the Amazon side of the VPN connection.

Customer Gateway:

A customer gateway is a physical device or software application on your side of the VPN connection. When you create a VPN connection, the VPN tunnel comes up when traffic is generated from your side of the VPN connection.



VPC Peering

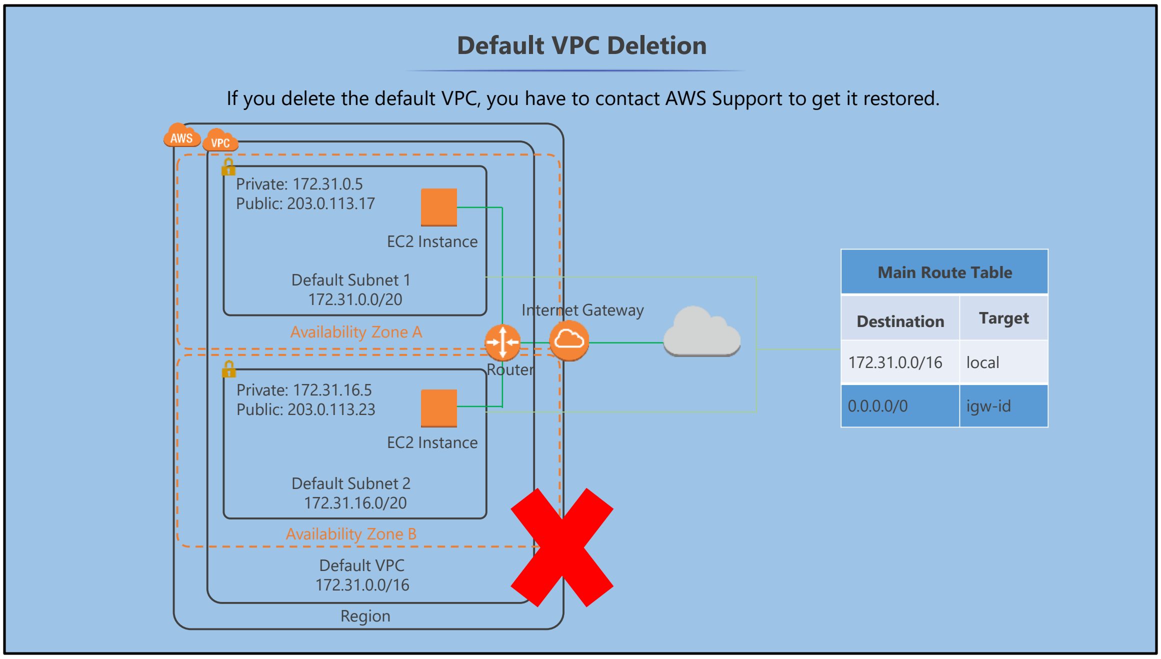
A peering connection allows you to route traffic between two VPCs using the private IP addresses so EC2 instances in either network can communicate directly with each other.

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.

A peering connection can be made between your own VPCs or with a VPC in another AWS account as long as it's in the same region.

VPC peering is a one-to-one relationship. A VPC can have multiple peering connections to other VPCs, but transitive peering is not supported.

In other words, A can connect to B and A can also connect to C, but B cannot connect to C.



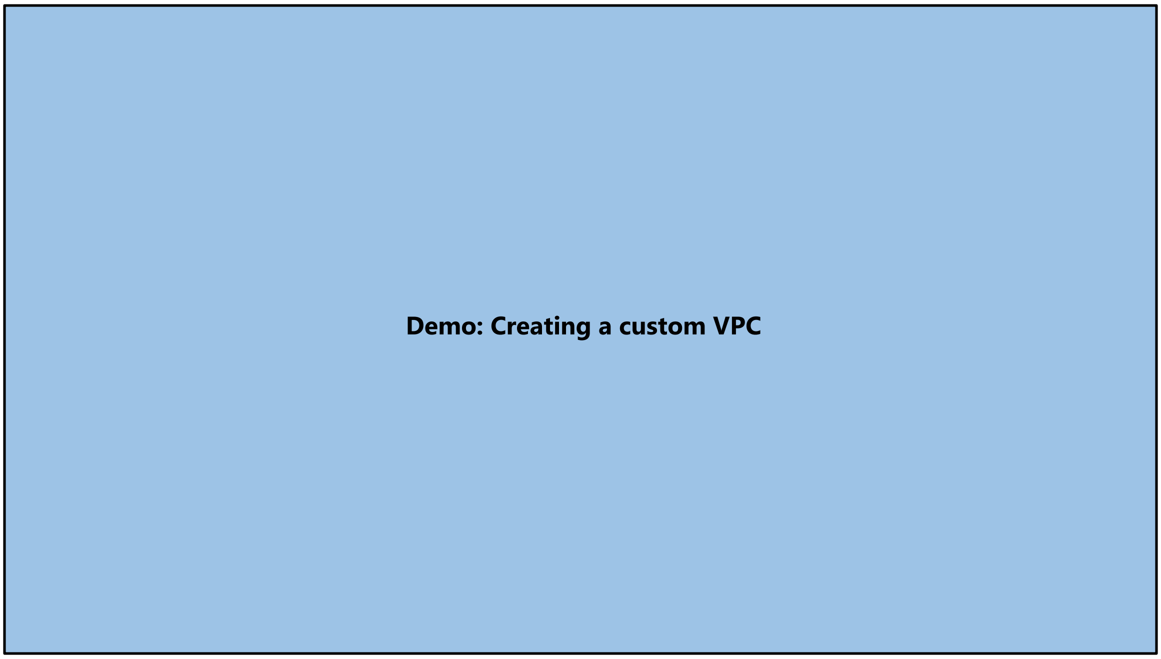
Default VPC Deletion

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

Main Route Table

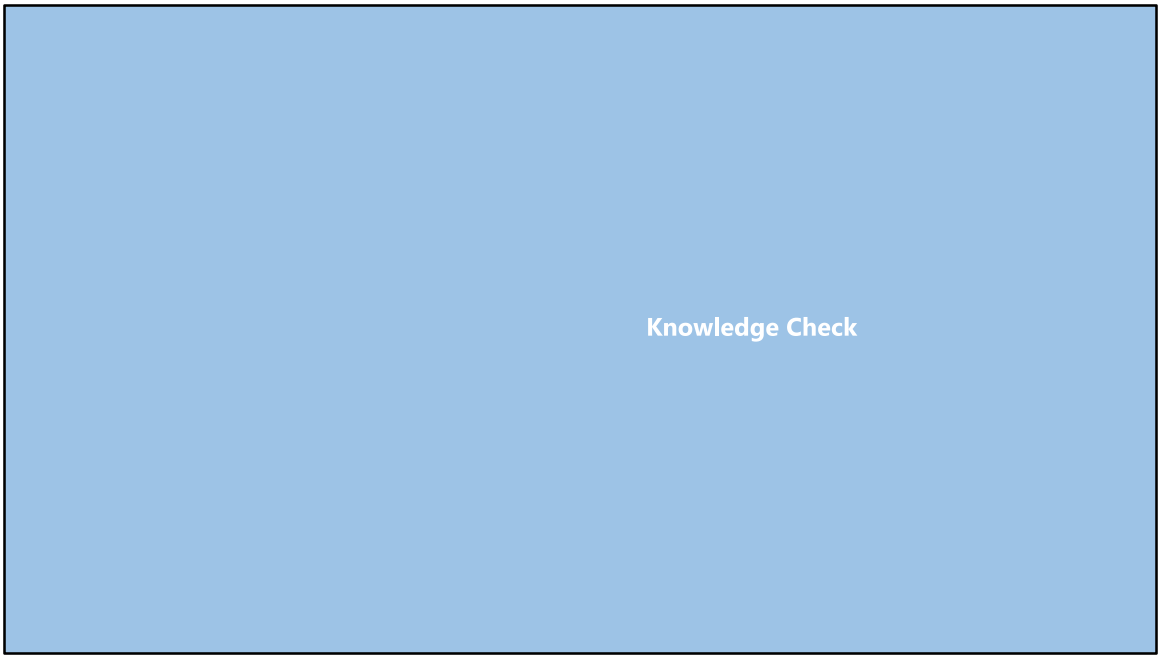
Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-id

If you delete the default VPC, you have to contact AWS Support to get it back. So be careful with it and delete it only if you have a good reason to do so.

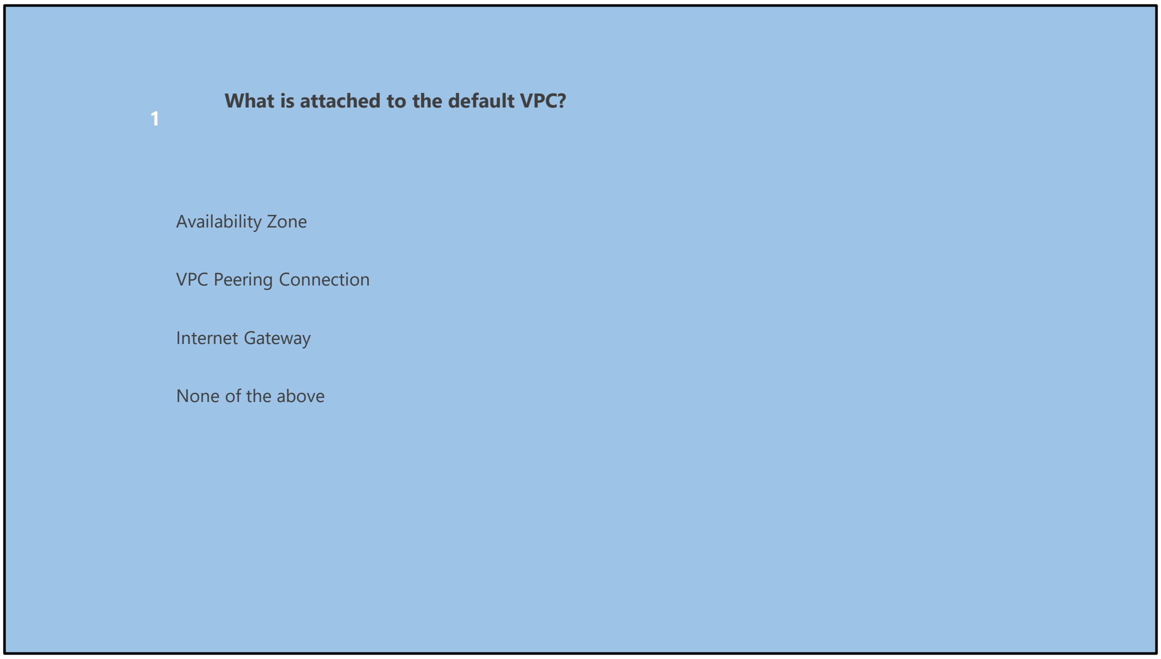


Demo: Creating a custom VPC

In this demonstration you'll learn how to create a custom VPC.



Knowledge Check



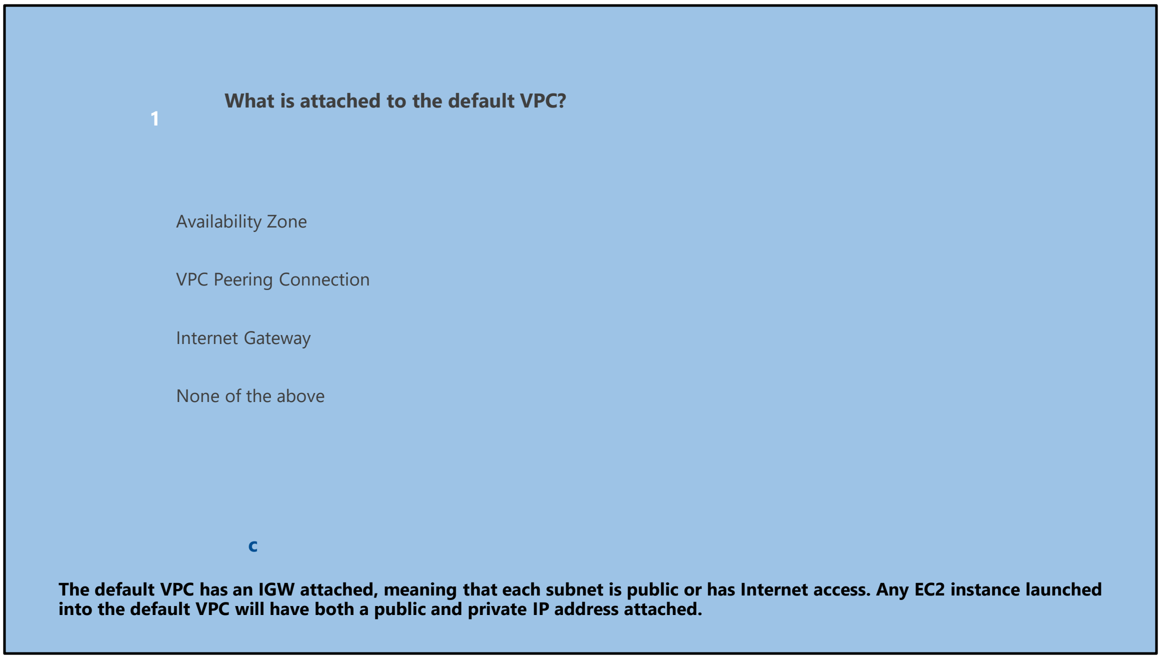
1 **What is attached to the default VPC?**

Availability Zone

VPC Peering Connection

Internet Gateway

None of the above



1 **What is attached to the default VPC?**

Availability Zone

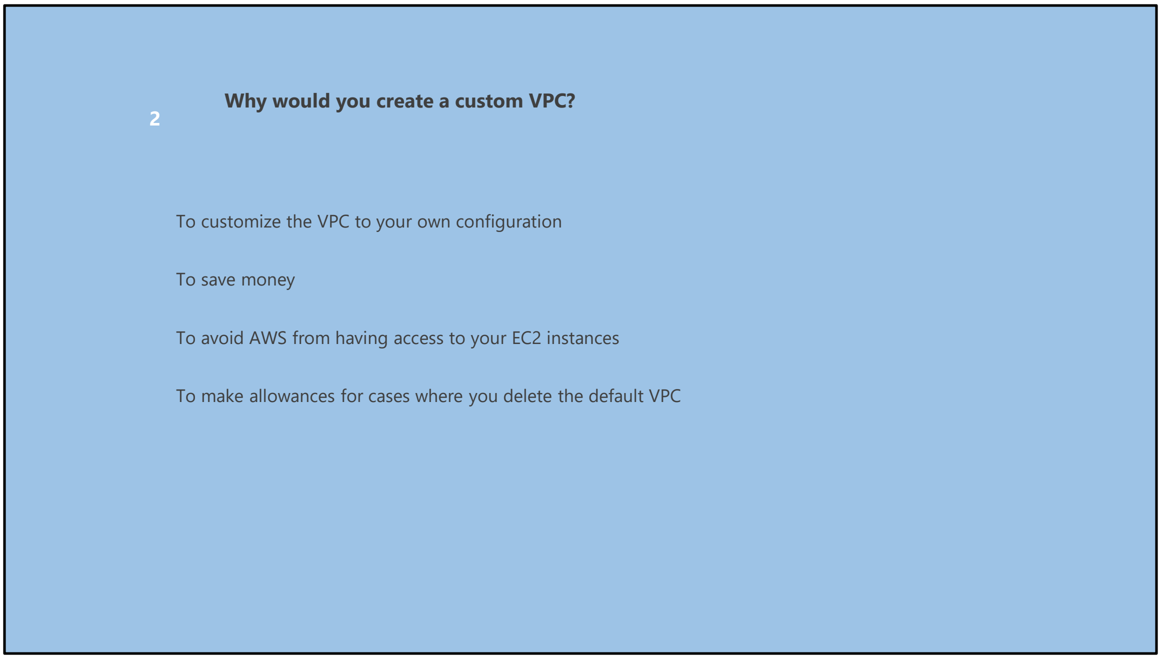
VPC Peering Connection

Internet Gateway

None of the above

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.



2

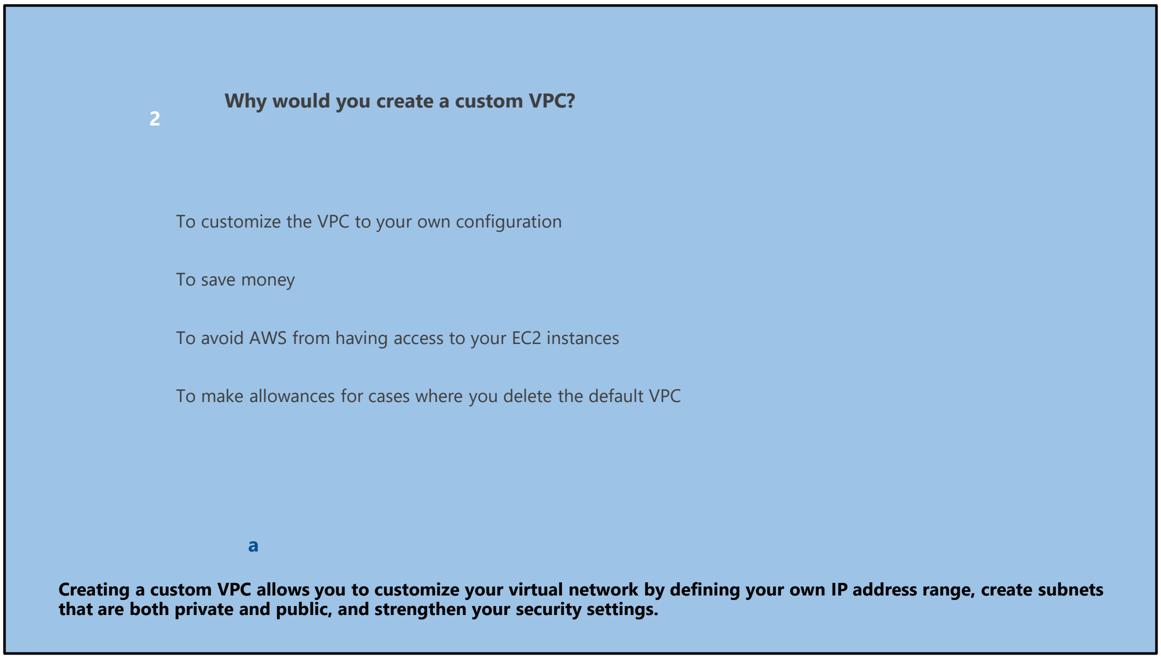
Why would you create a custom VPC?

To customize the VPC to your own configuration

To save money

To avoid AWS from having access to your EC2 instances

To make allowances for cases where you delete the default VPC



2 **Why would you create a custom VPC?**

To customize the VPC to your own configuration

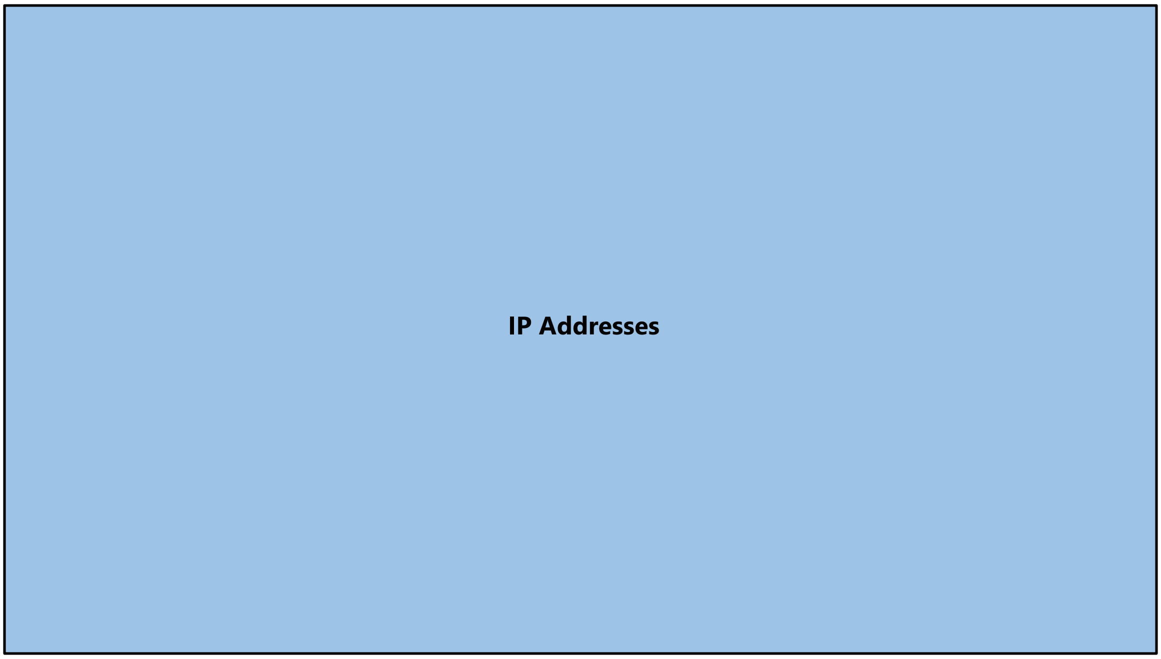
To save money

To avoid AWS from having access to your EC2 instances

To make allowances for cases where you delete the default VPC

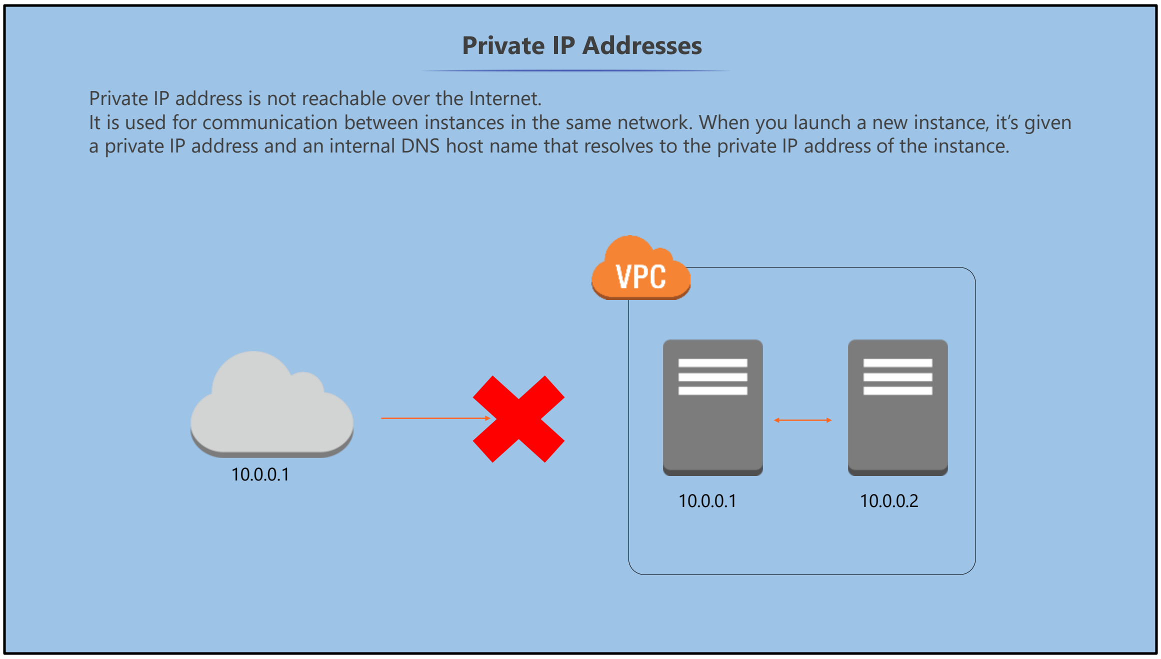
a

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

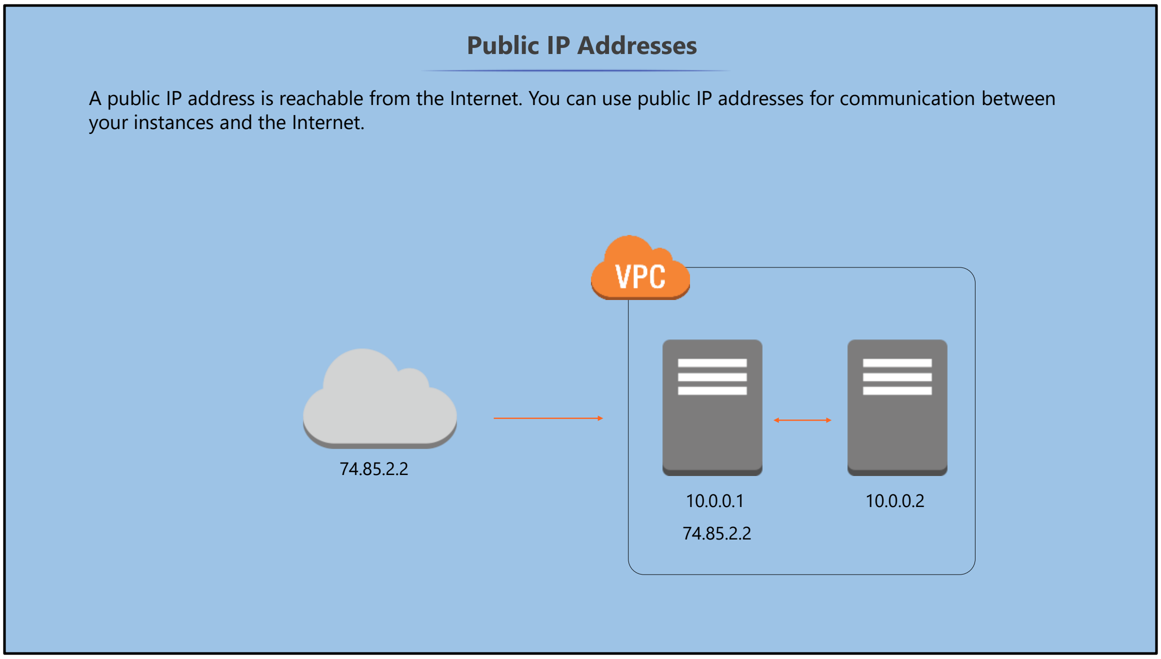
In this section you'll learn how to use IP Addresses in Amazon VPC.



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.

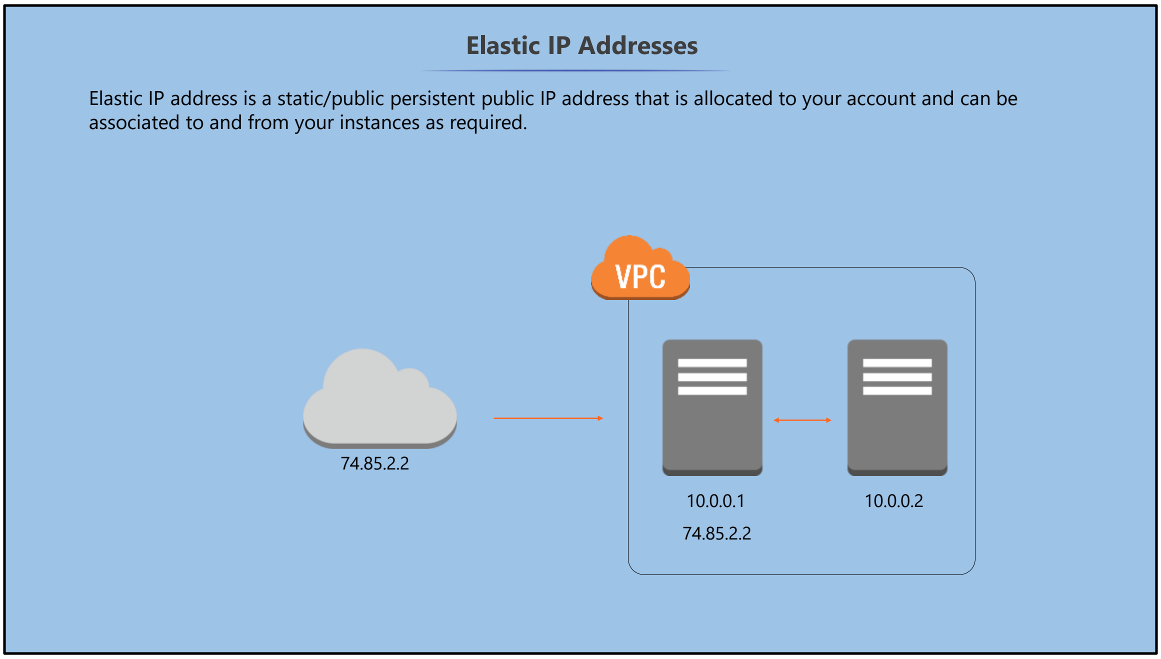
Private IP address: A private IP address is not reachable over the Internet.
It is used for communication between instances in the same network. When you launch a new instance it's given a private IP address and an internal DNS host name that resolves to the private IP address of the instance.



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.

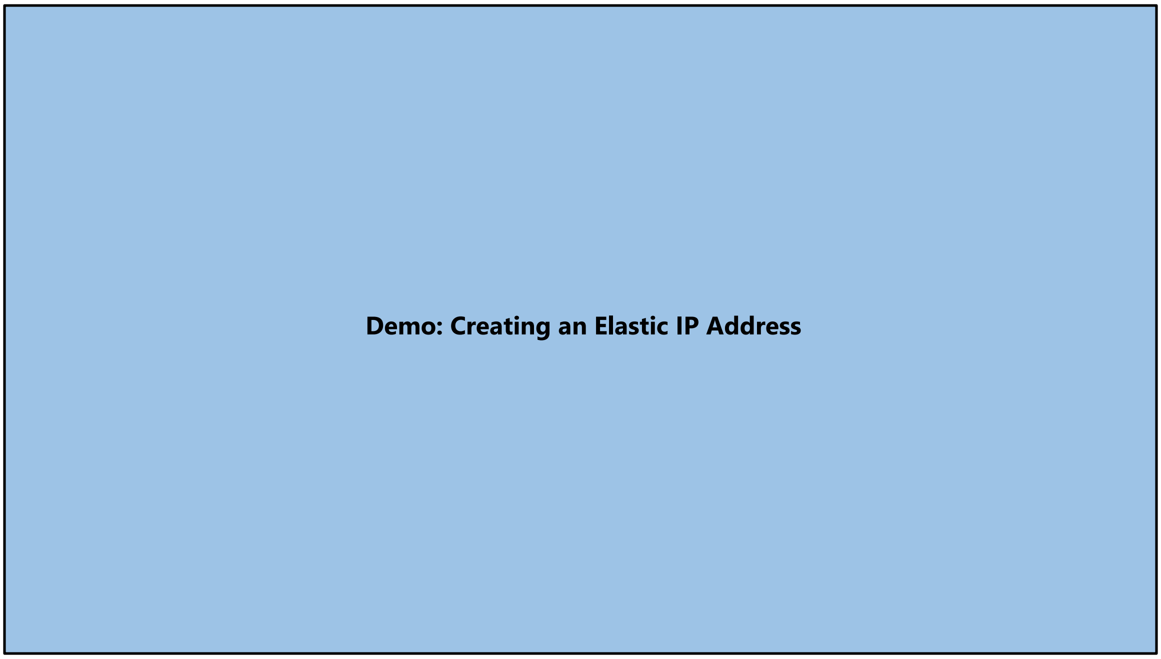
Public IP address: A public IP address is reachable from the Internet. You can use public IP addresses for communication between your instances and the Internet. Each instance that receives a public IP address is also given an external DNS hostname; for example, ec2-203-0-113-25.compute-1.amazonaws.com.
Public IP addresses are associated with your instances from the Amazon pool of public IP addresses. When you stop or terminate your instance, the public IP address is released and a new one is associated when the instance restarts.



Elastic IP Addresses

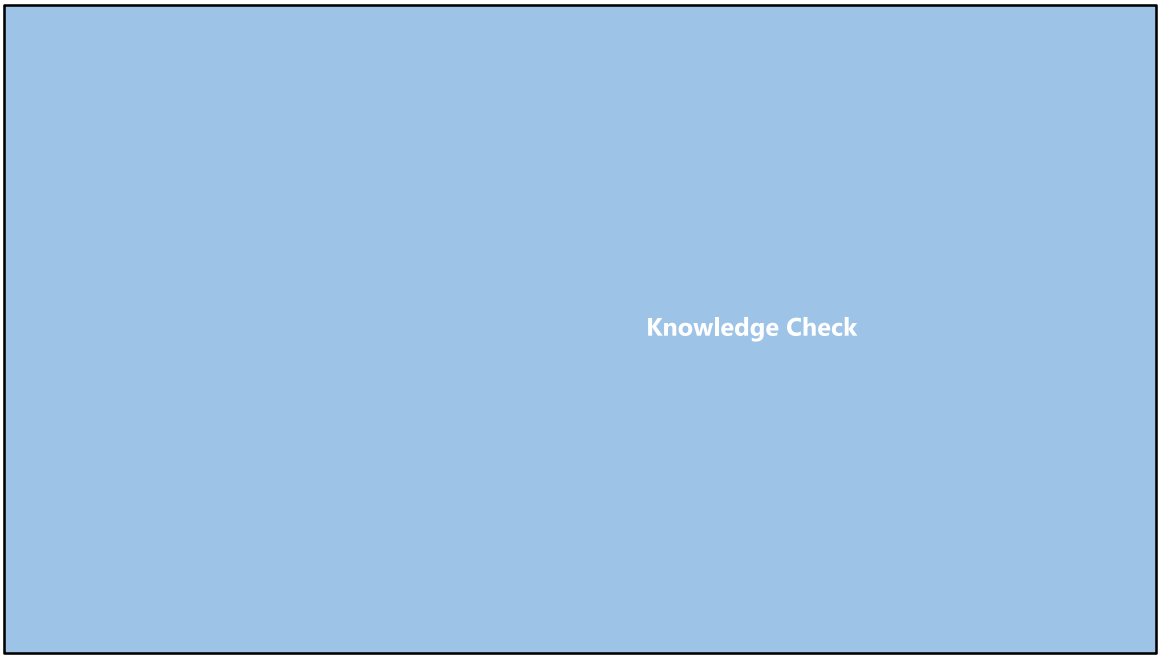
Elastic IP address is a static/public persistent public IP address that is allocated to your account and can be associated to and from your instances as required.

Elastic IP address: 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. It remains in your account until you choose to release it. There is a charge associated with an EIP if it is not allocated to an instance.

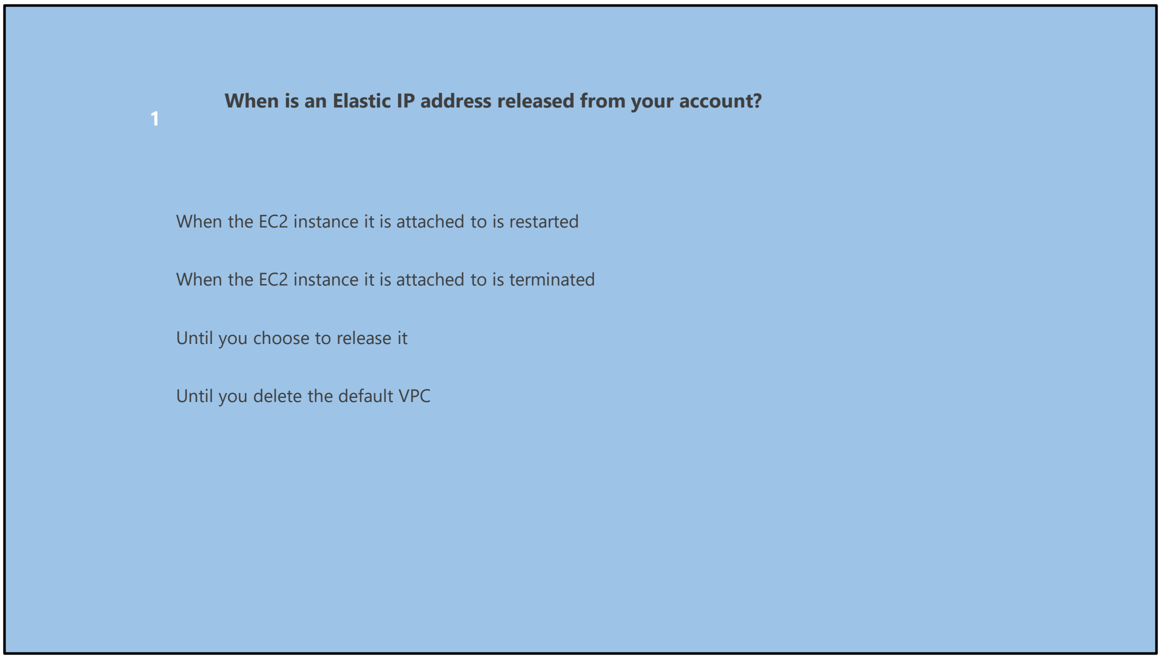


Demo: Creating an Elastic IP Address

In this demonstration you’ll learn how to create an elastic IP address.



Knowledge Check



1

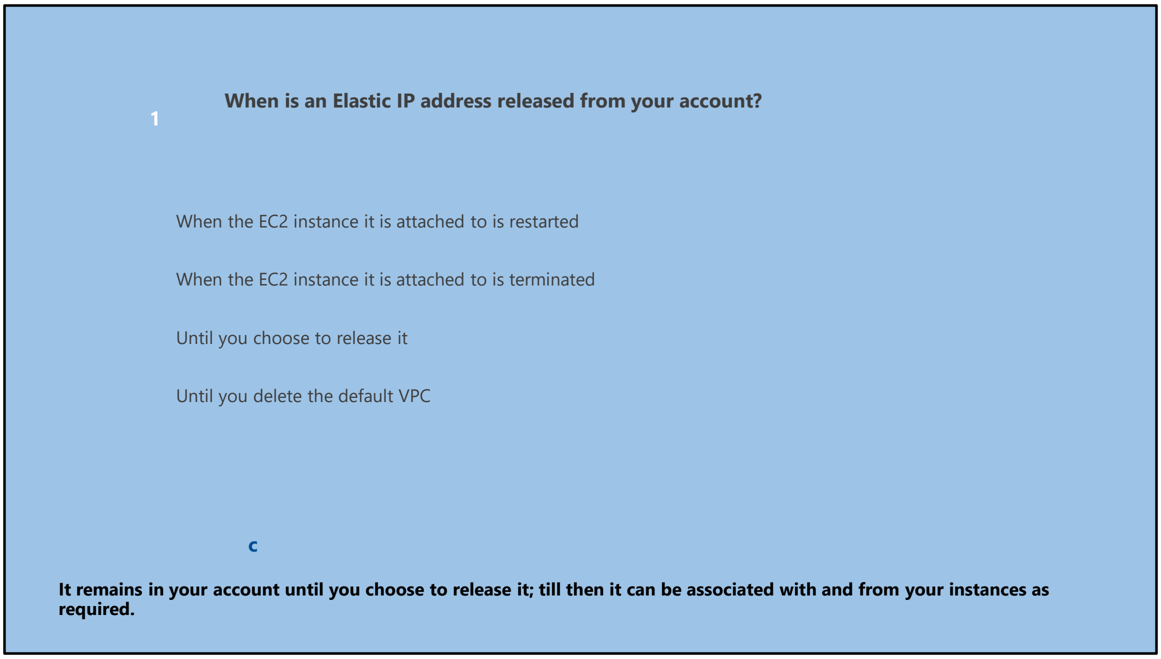
When is an Elastic IP address released from your account?

When the EC2 instance it is attached to is restarted

When the EC2 instance it is attached to is terminated

Until you choose to release it

Until you delete the default VPC



1 **When is an Elastic IP address released from your account?**

When the EC2 instance it is attached to is restarted

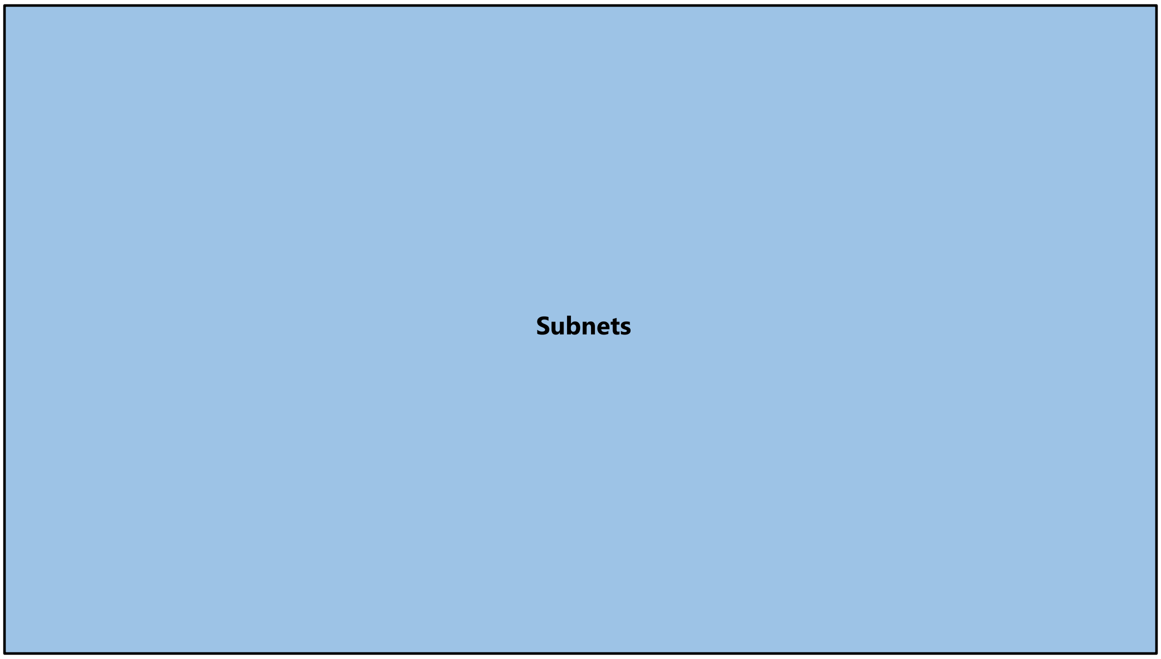
When the EC2 instance it is attached to is terminated

Until you choose to release it

Until you delete the default VPC

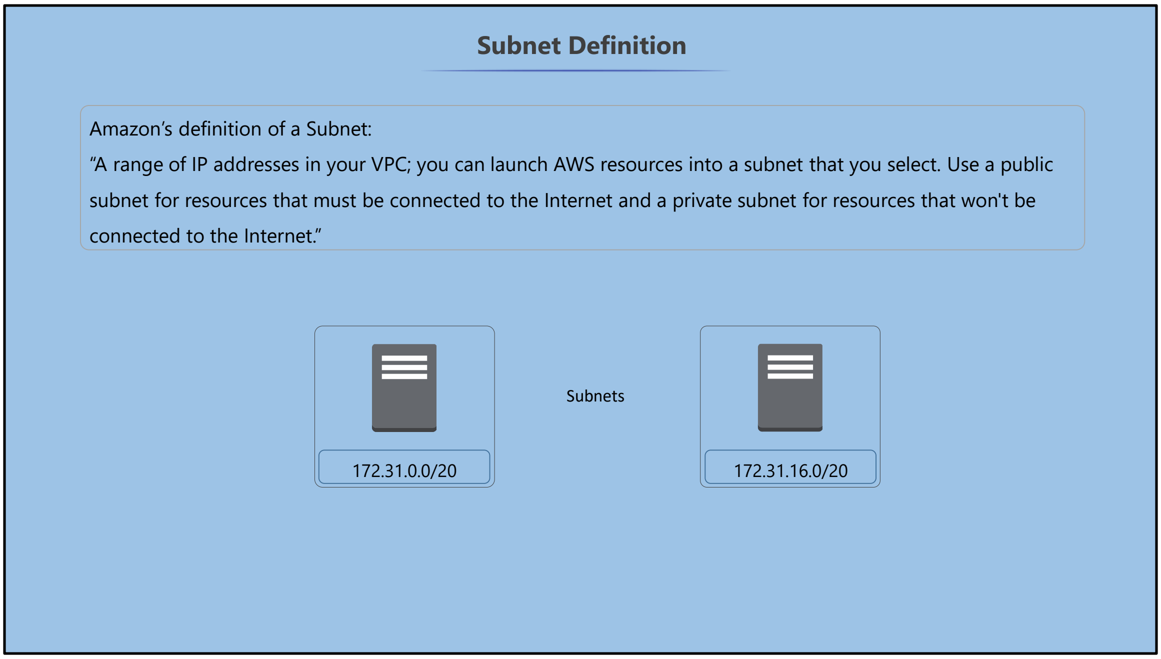
c

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

In this section you'll learn about using subnets in Amazon VPC.



Subnet Definition

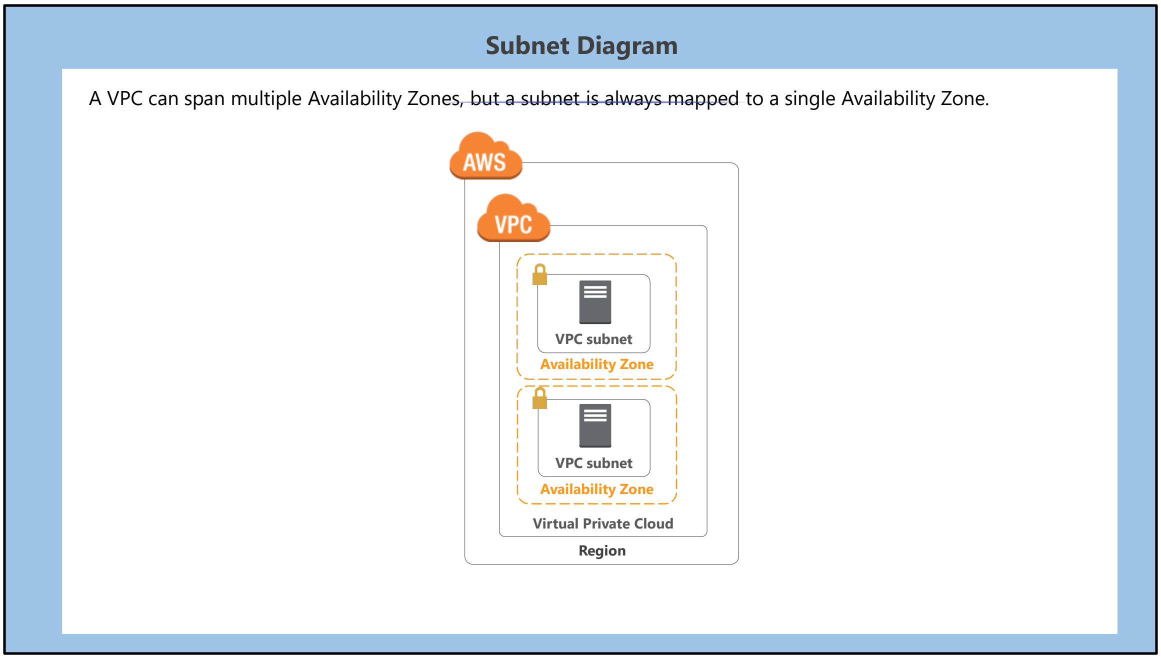
Amazon’s definition of a Subnet:
“A range of IP addresses in your VPC; you can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet and a private subnet for resources that won't be connected to the Internet.”

172.31.0.0/20

Subnets

172.31.16.0/20

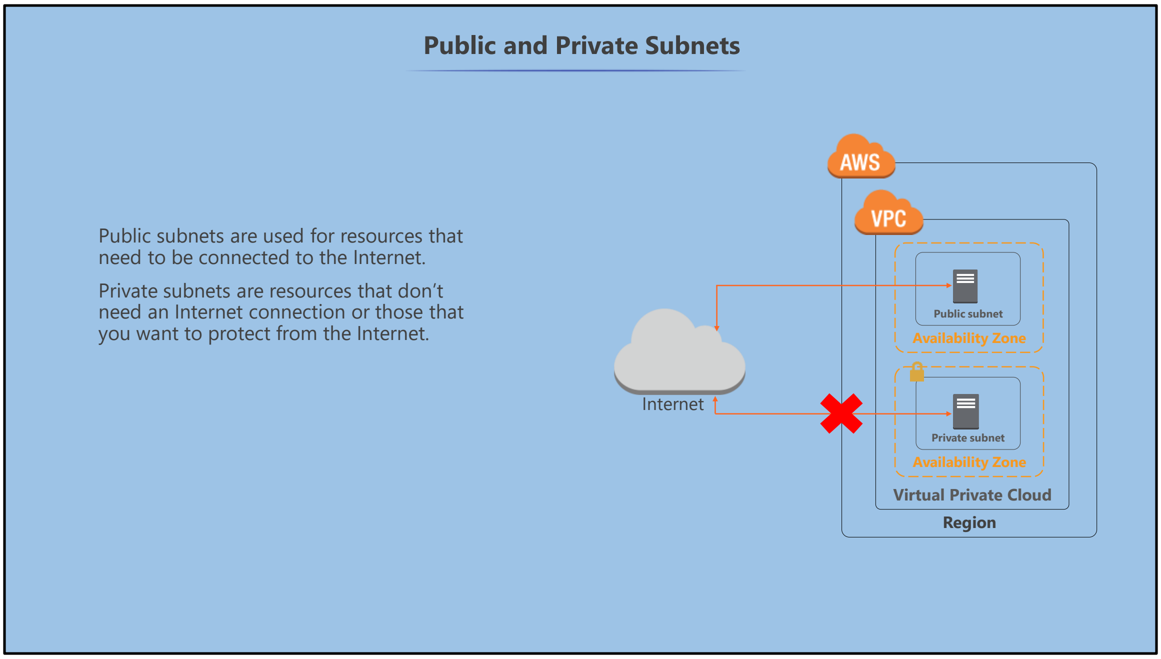
AWS defines a subnet as:
A range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. Use a public subnet for resources that must be connected to the Internet, and a private subnet for resources that won't be connected to the Internet.
The netmask for a default subnet is always /20, which provides up to 4,096 addresses per subnet. However, 5 IP addresses are always reserved by AWS (the first four IPs and the last IP).



Subnet Diagram

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

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



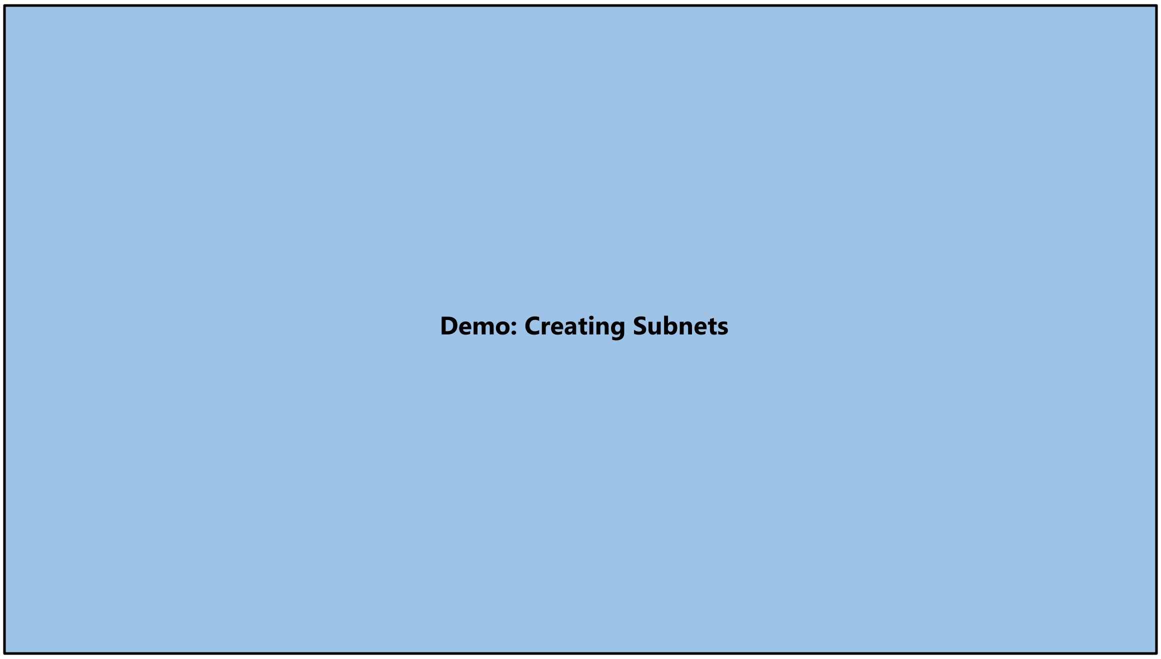
Public and Private Subnets

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.

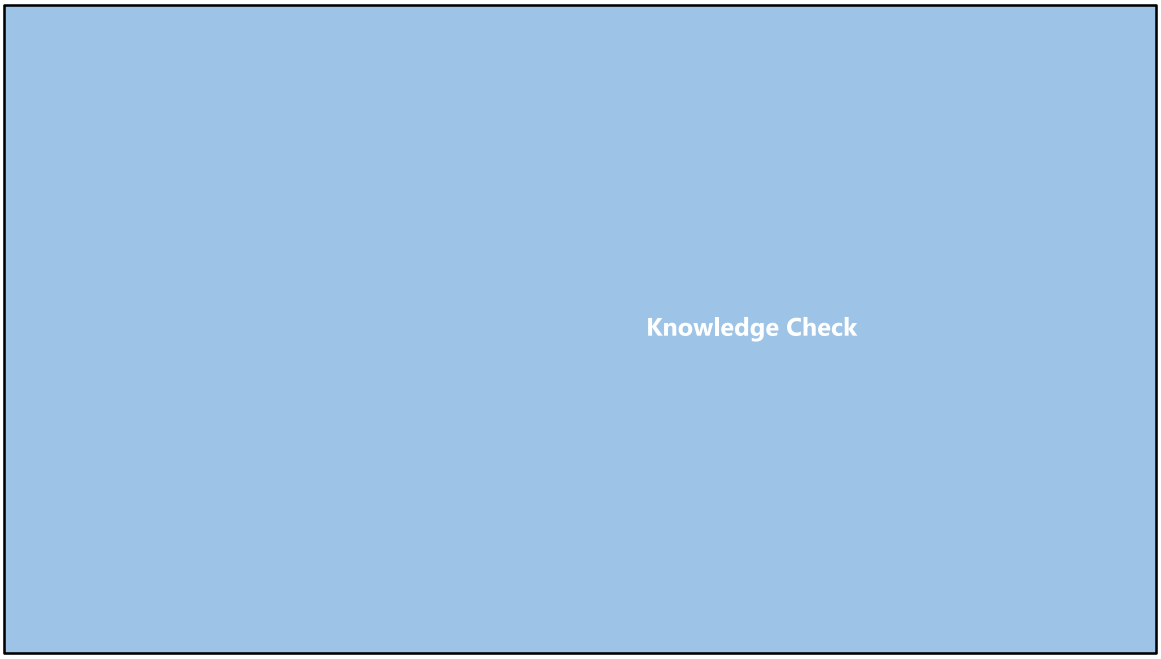
Use a public subnet for resources that must be connected to the Internet, for example, web servers. A public subnet is made public because the main route table sends the subnet's traffic that is destined for the Internet to the Internet gateway.

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

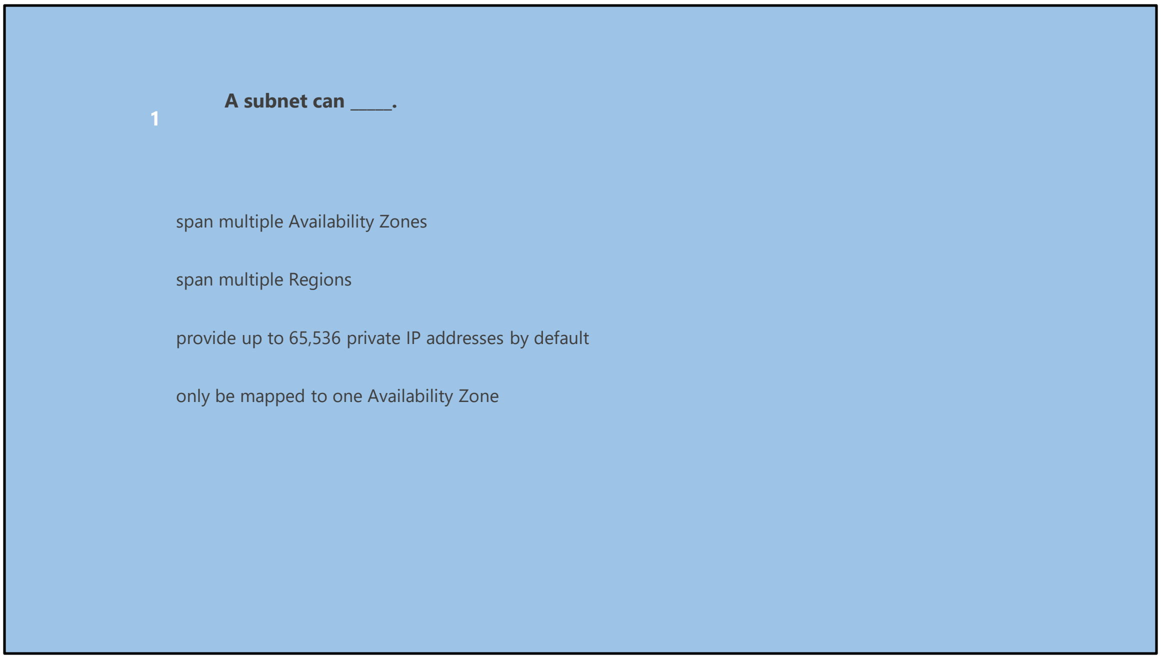


Demo: Creating Subnets

In this demonstration you’ll learn how to create a public and private subnet.



Knowledge Check



1

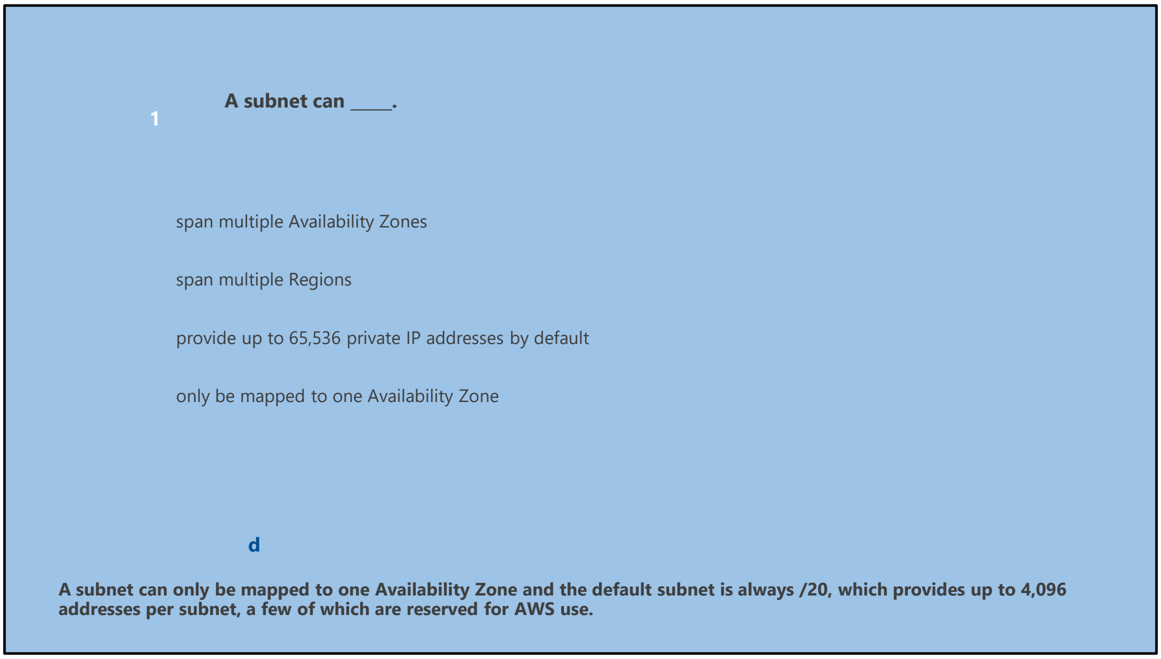
A subnet can _____.

span multiple Availability Zones

span multiple Regions

provide up to 65,536 private IP addresses by default

only be mapped to one Availability Zone



1 **A subnet can _____.**

span multiple Availability Zones

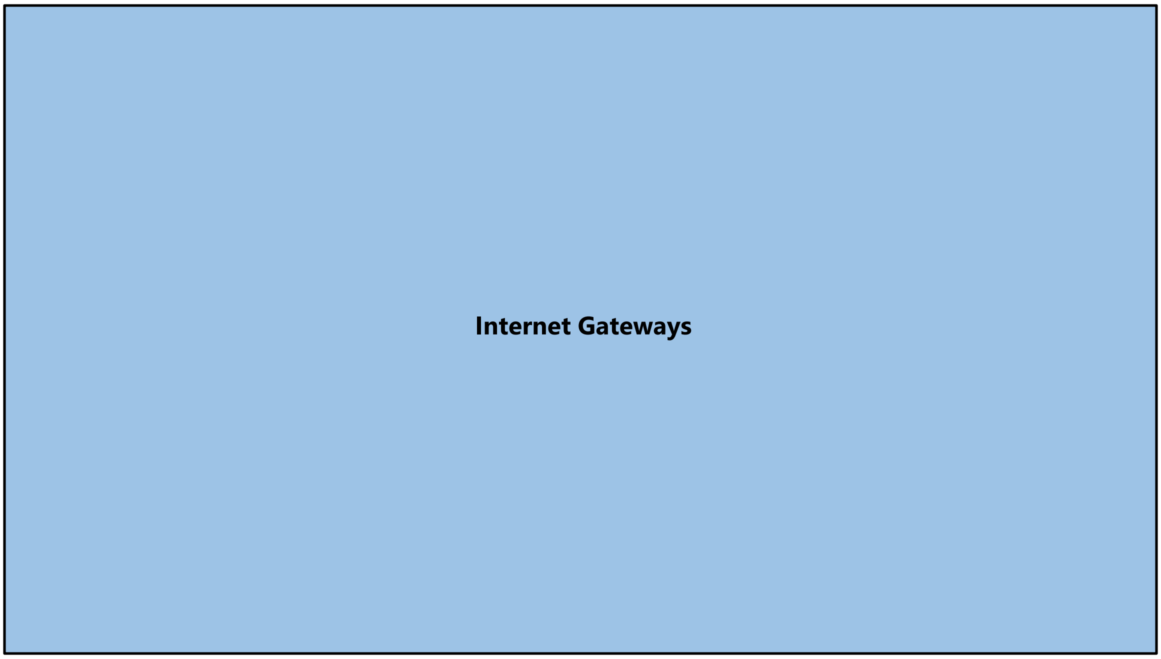
span multiple Regions

provide up to 65,536 private IP addresses by default

only be mapped to one Availability Zone

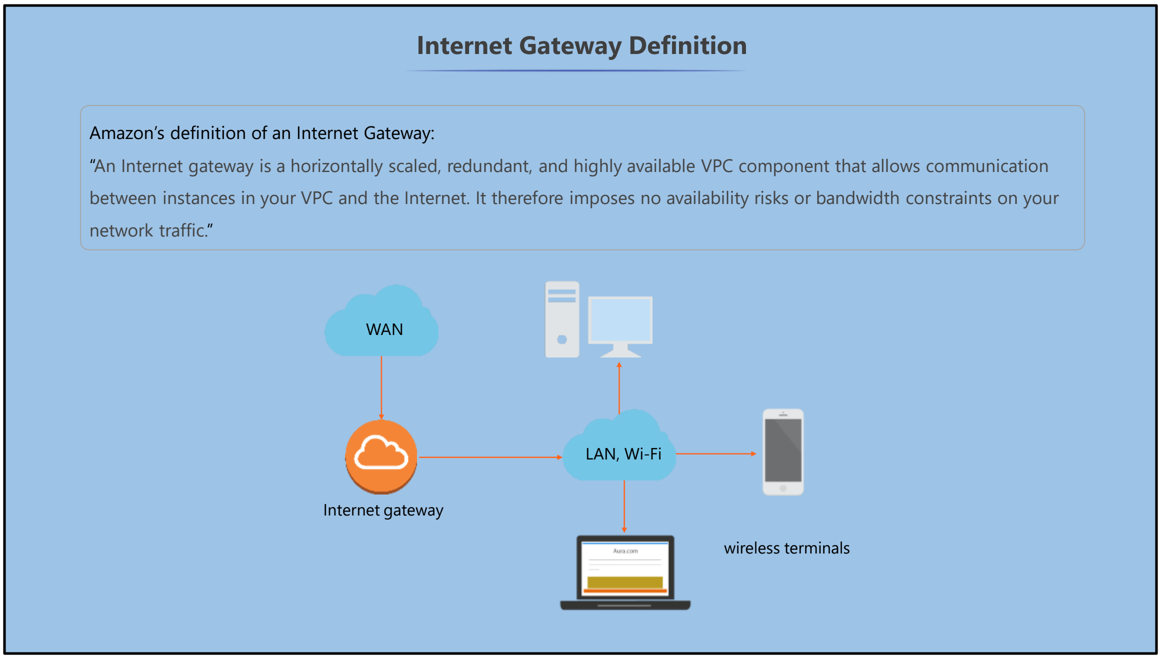
d

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

In this section you’ll learn how to use Internet gateways in Amazon VPC.



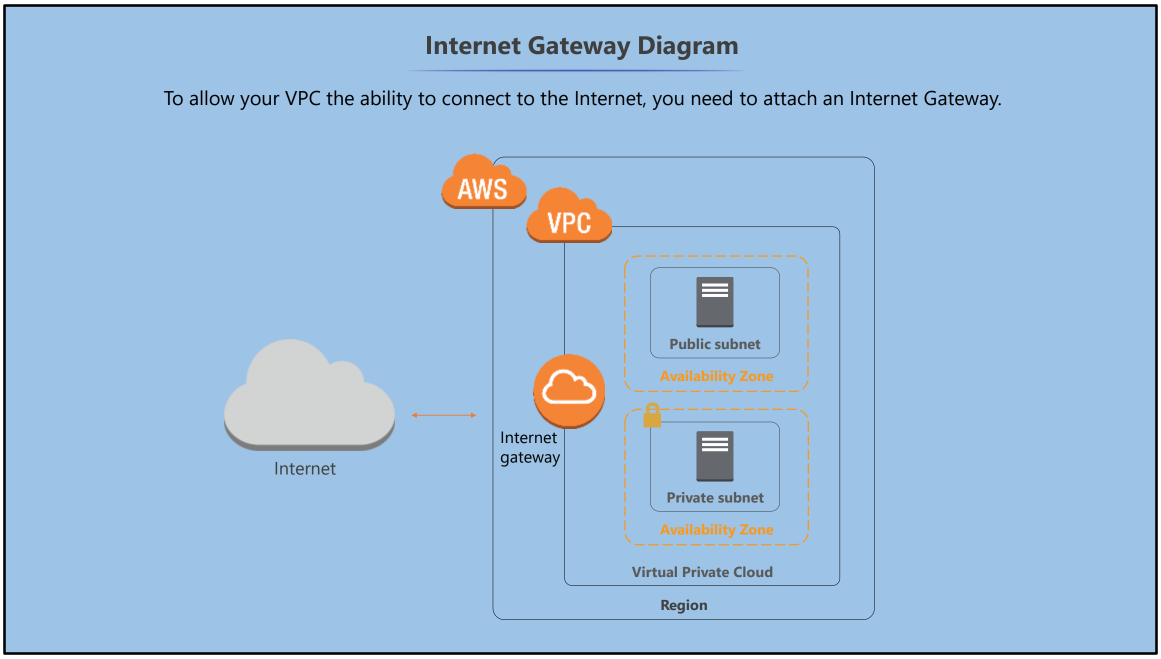
Internet Gateway Definition

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.”

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.

It serves two purposes: to provide a target in your VPC route tables for Internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IP addresses.

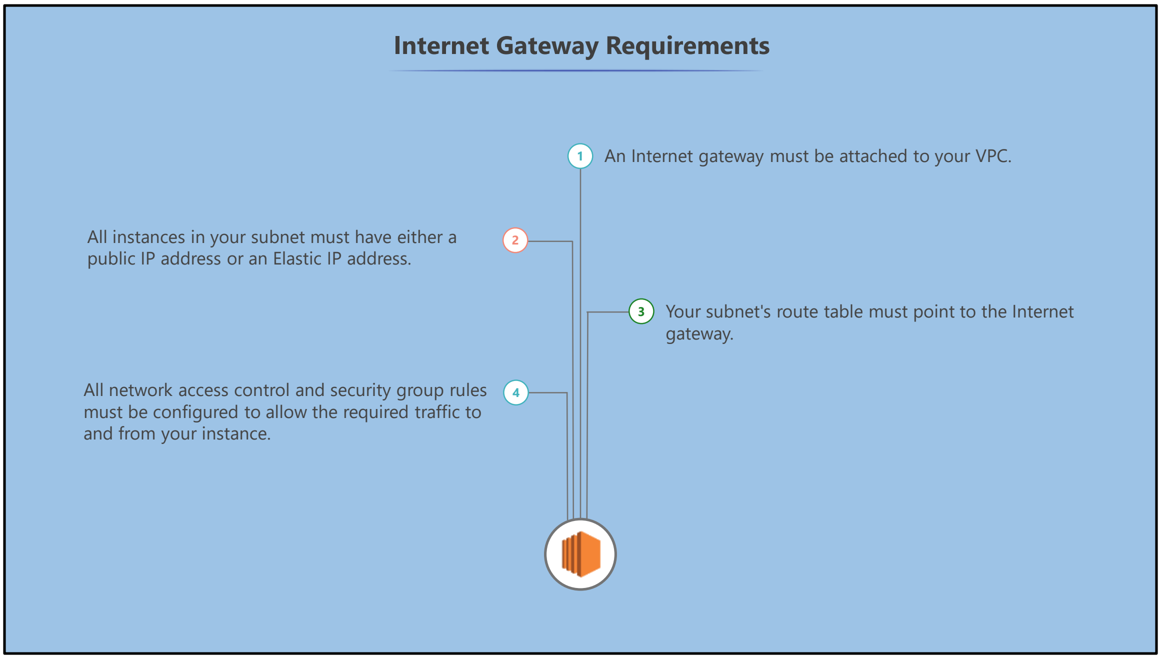


Internet Gateway Diagram

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

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.

Attaching an Internet Gateway is the first stage in permitting Internet access instances in your custom VPC.



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.

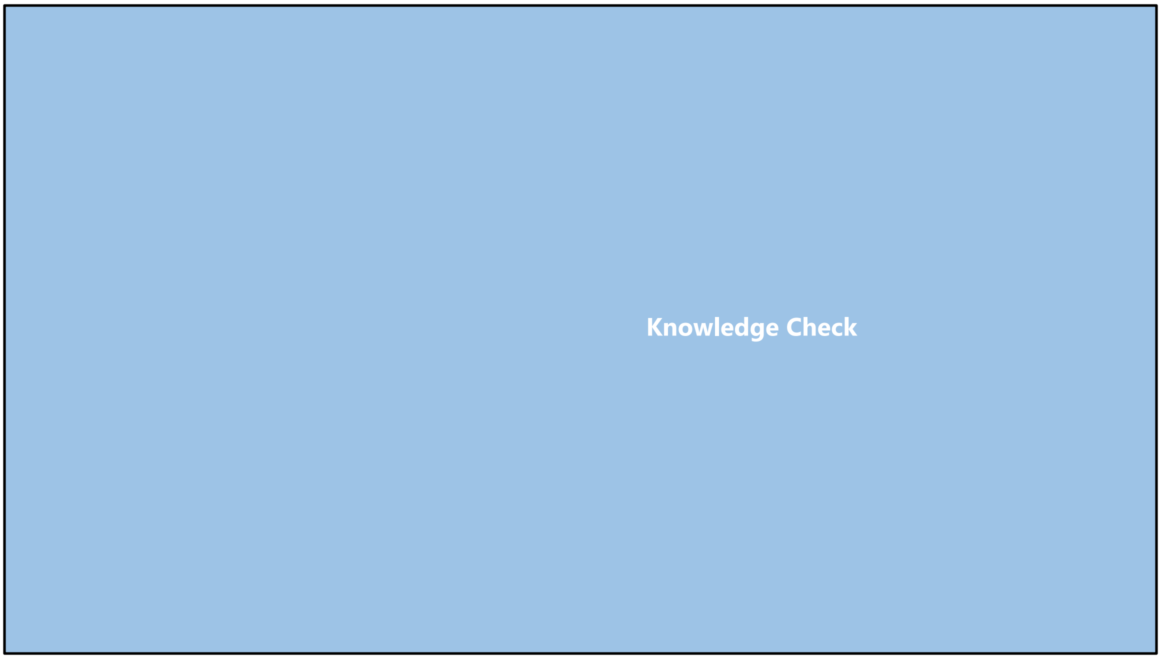
3 Your subnet's route table must point to the Internet gateway.

4 All network access control and security group rules must be configured to allow the required traffic to and from your instance.

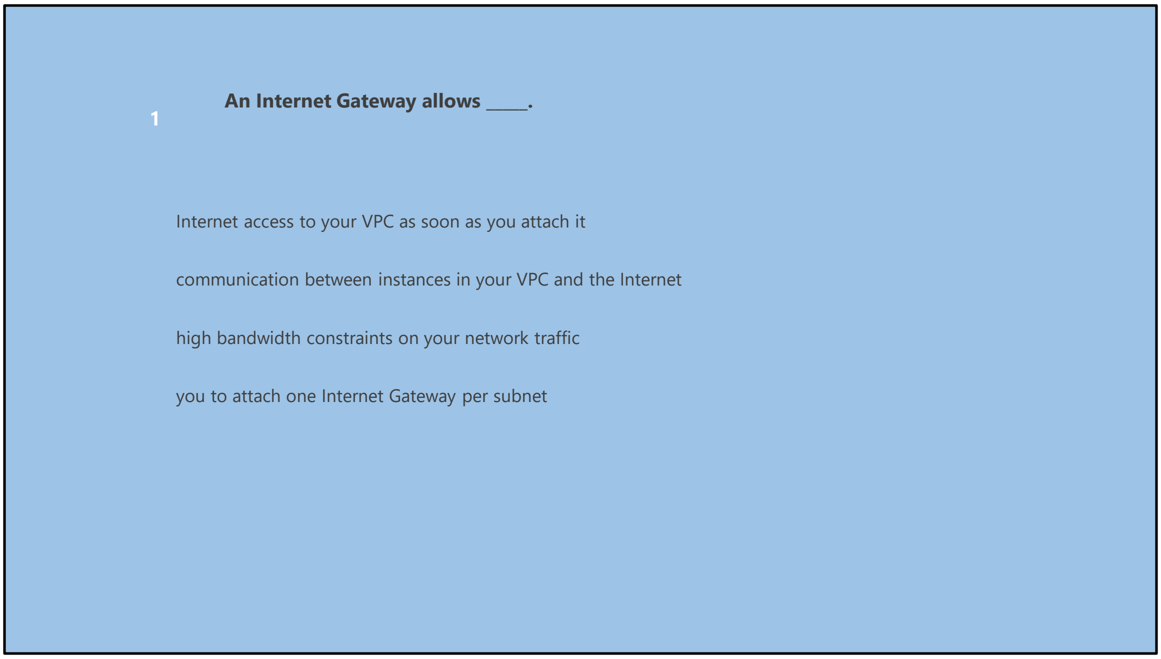
For an EC2 instance to be connected to the internet AWS requires the following:
An Internet gateway must be attached to your VPC.
All instances in your subnet must have either a public IP address or an Elastic IP address.
Your subnet's route table must point to the Internet gateway.
All network access control and security group rules must be configured to allow the required traffic to and from your instance.

Demo: Creating Internet Gateways

In this demonstration you’ll learn how to create an Internet gateway.



Knowledge Check



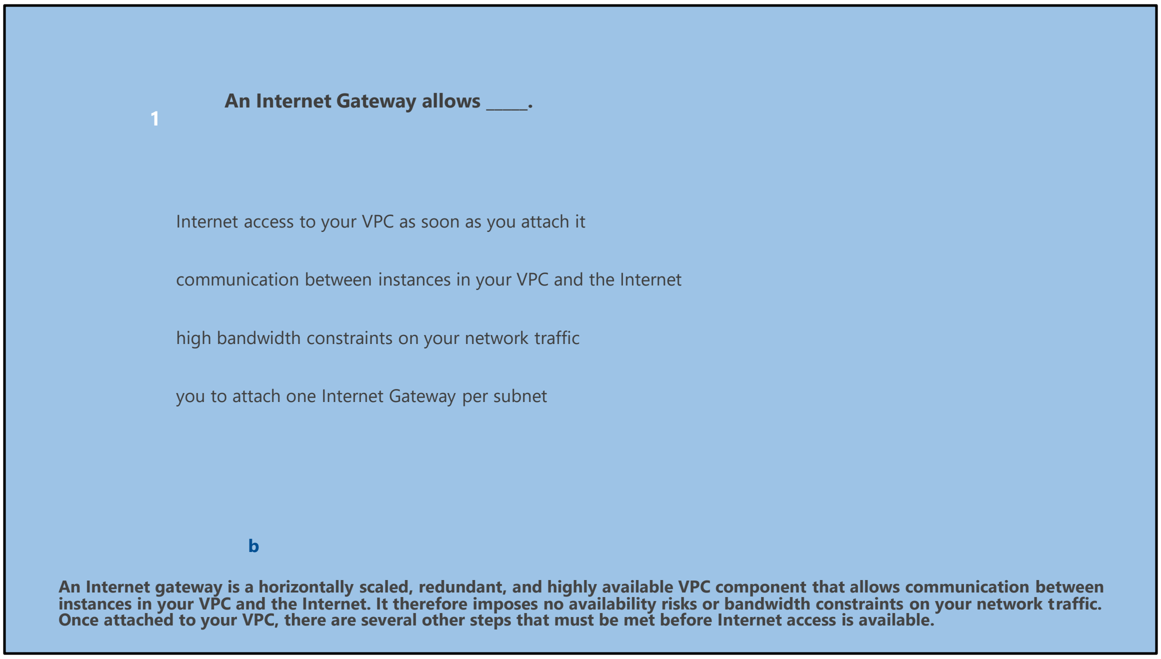
1 **An Internet Gateway allows _____.**

Internet access to your VPC as soon as you attach it

communication between instances in your VPC and the Internet

high bandwidth constraints on your network traffic

you to attach one Internet Gateway per subnet



1 **An Internet Gateway allows _____.**

Internet access to your VPC as soon as you attach it

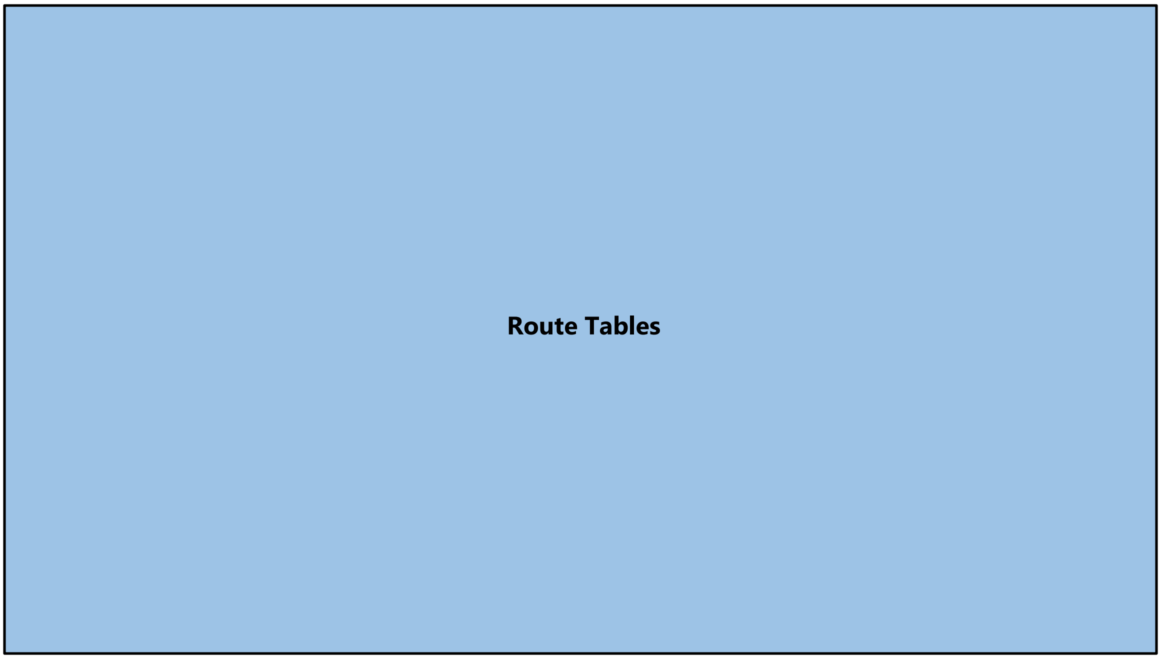
communication between instances in your VPC and the Internet

high bandwidth constraints on your network traffic

you to attach one Internet Gateway per subnet

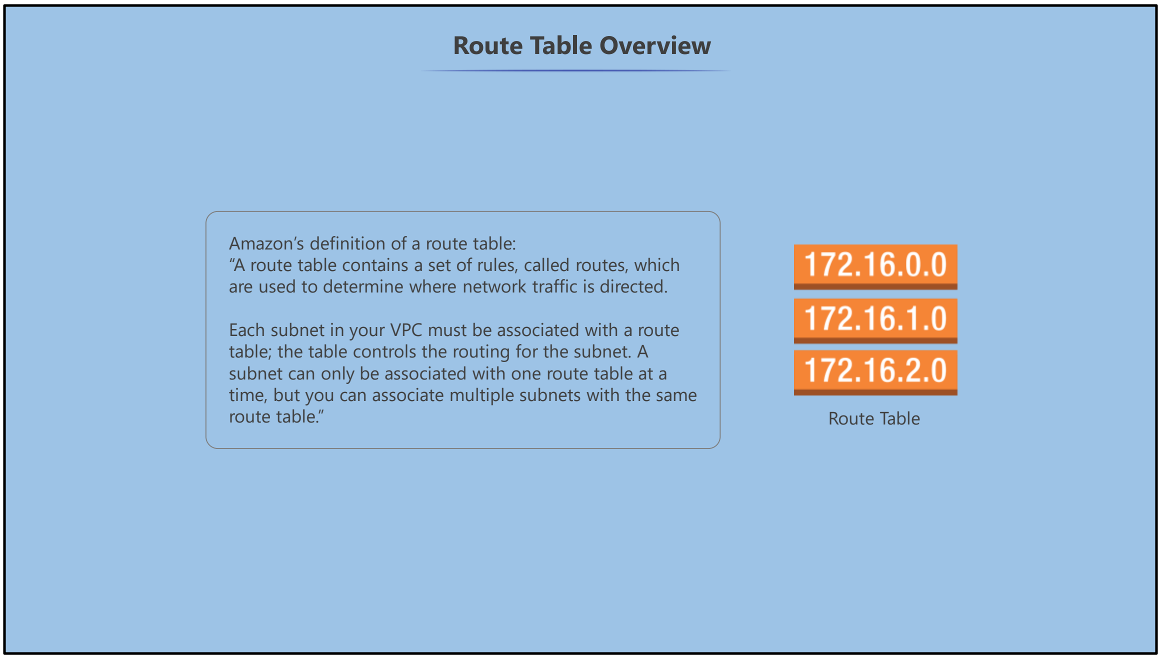
b

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

In this section you’ll learn how to use route tables in Amazon VPC.

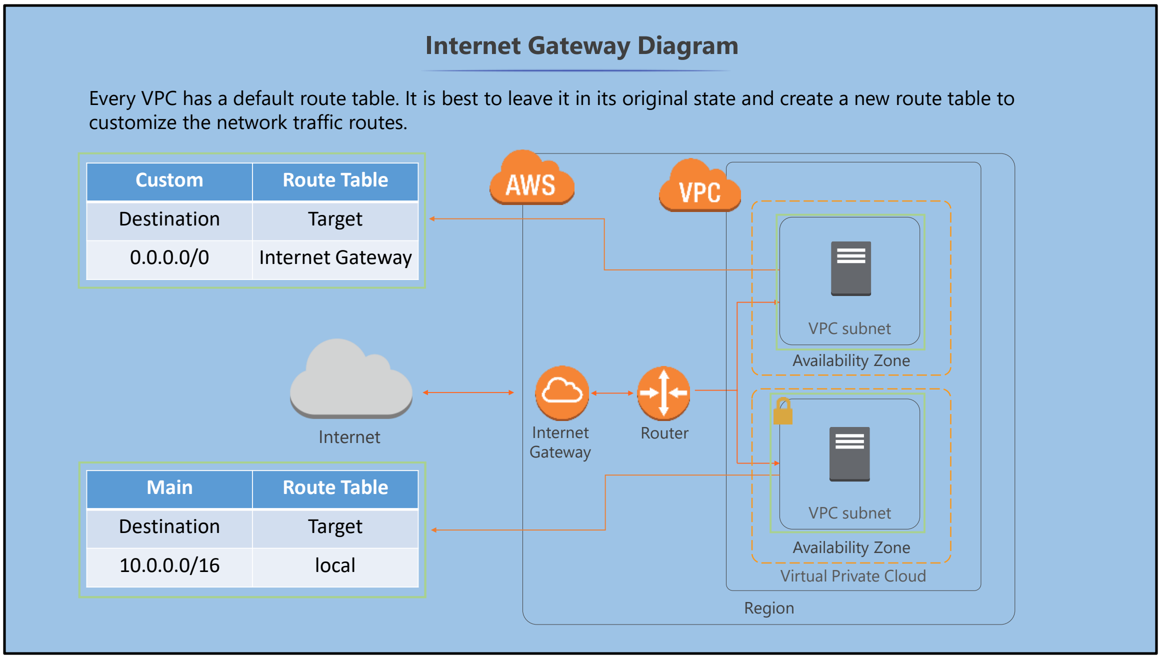


Route Table Overview

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."

A route table determines where network traffic is directed. It does so by defining a set of rules.
Every subnet has to be associated with a route table. A subnet can only be associated with one route table, however, multiple subnets can be associated with the same route table.



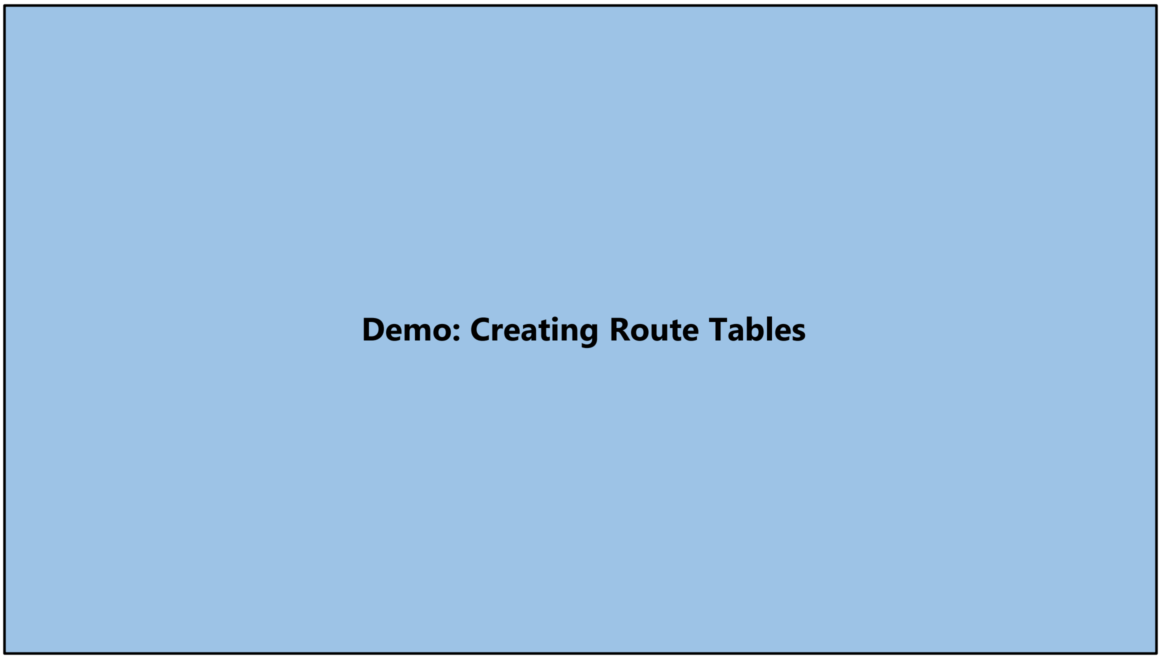
Internet Gateway Diagram

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

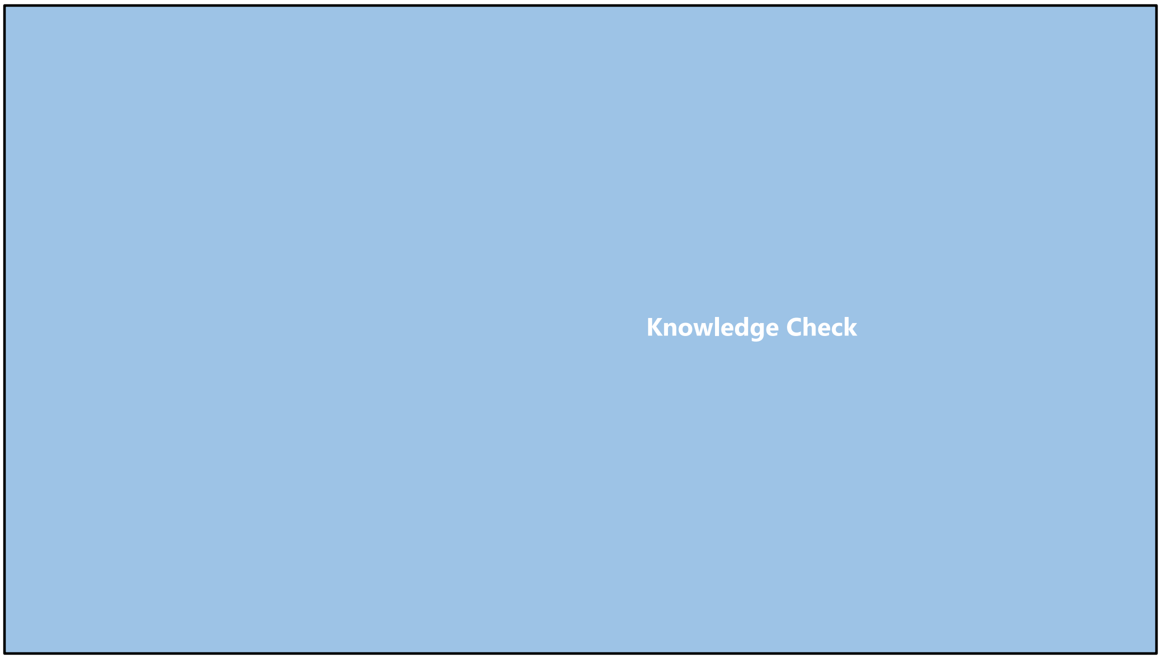
Main	Route Table
Destination	Target
10.0.0.0/16	local

Every VPC has a default route table. It’s good practice to leave it in its original state and create a new Route Table to customize the network traffic routes.
In the example, the new route table informs the Internet Gateway to direct Internet traffic to the public subnet, but the private subnet is still associated to the default route table, which does not allow Internet traffic to it.

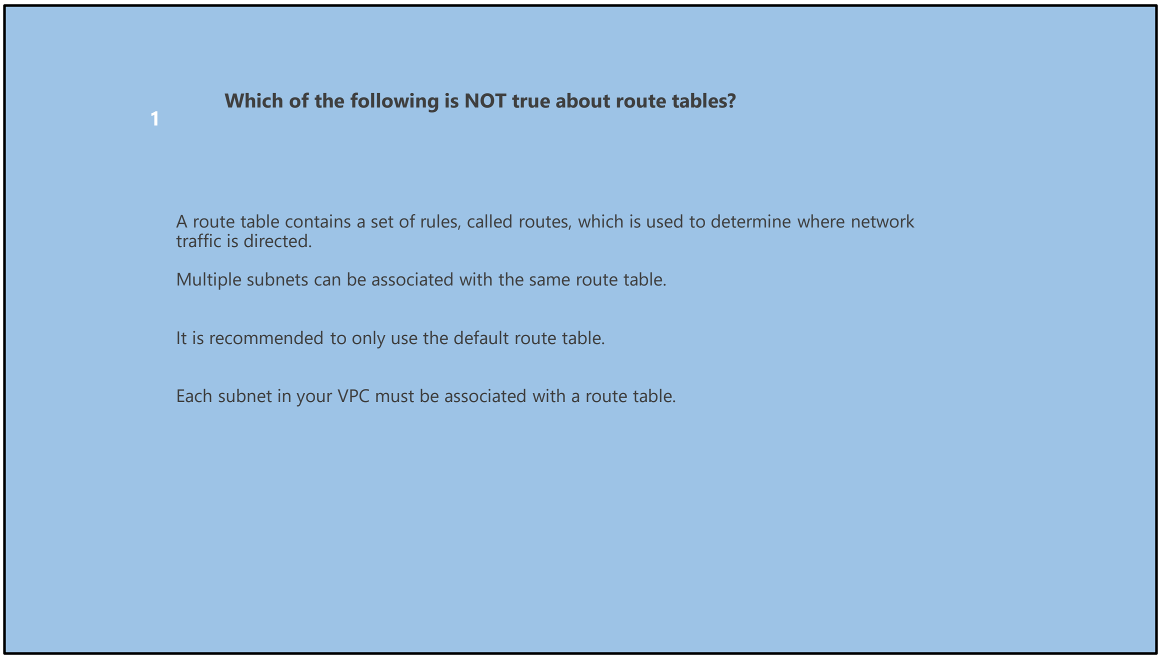


Demo: Creating Route Tables

In this demonstration you’ll learn how to create an custom route table.



Knowledge Check



1

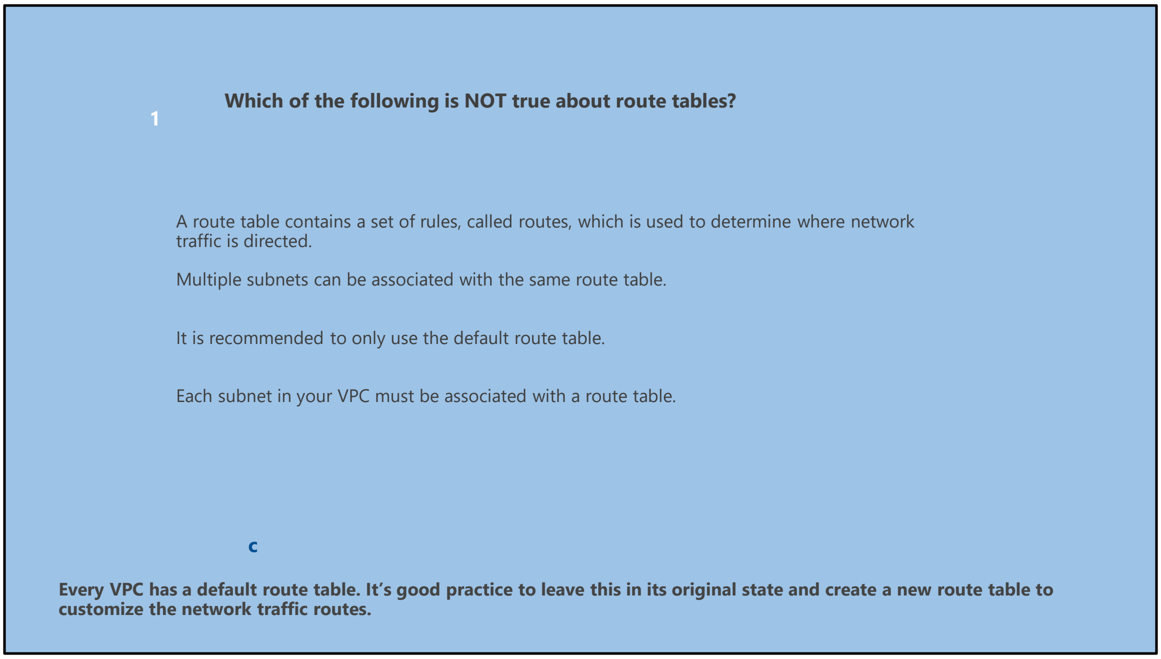
Which of the following is NOT true about route tables?

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

Multiple subnets can be associated with the same route table.

It is recommended to only use the default route table.

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



1

Which of the following is NOT true about route tables?

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

Multiple subnets can be associated with the same route table.

It is recommended to only use the default route table.

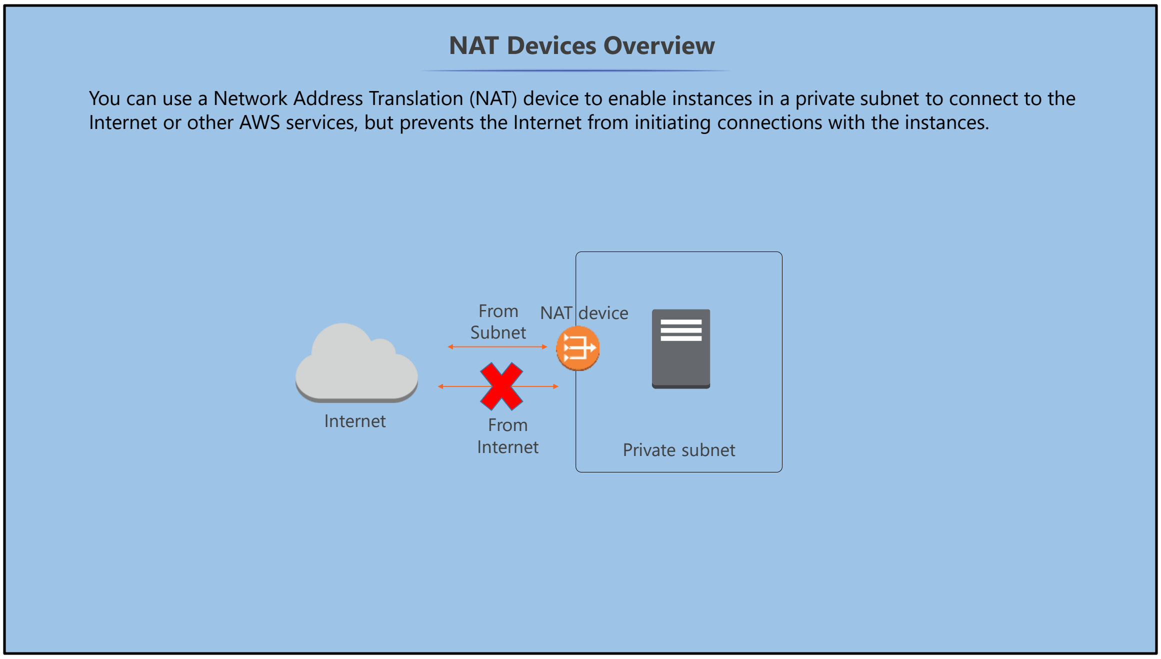
Each subnet in your VPC must be associated with a route table.

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

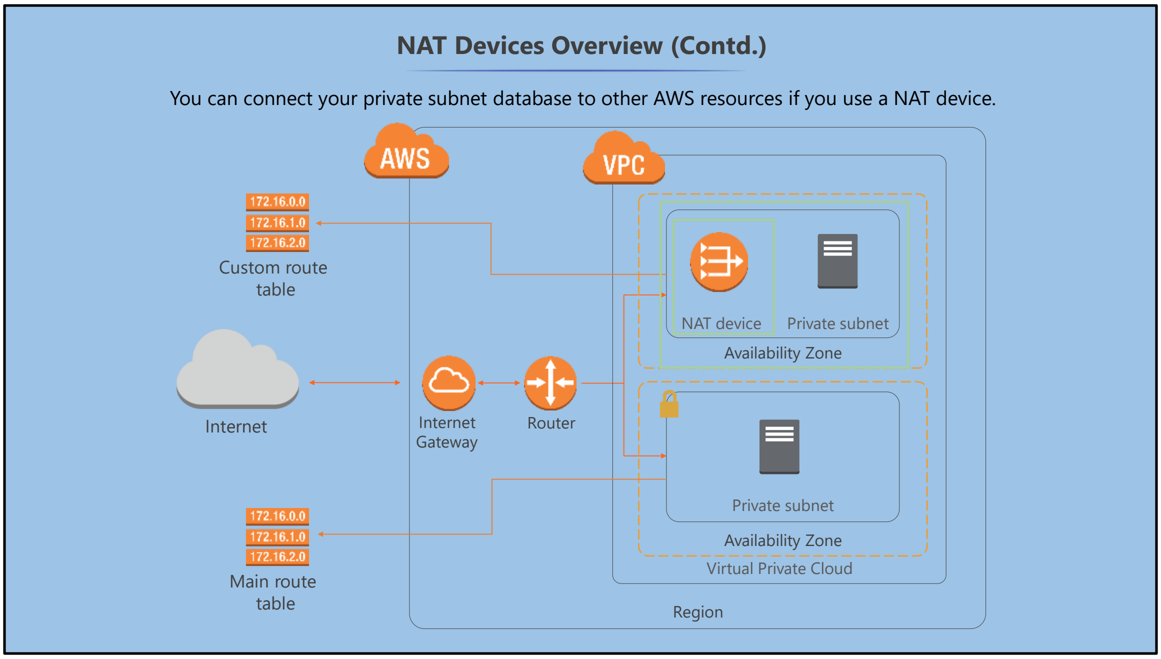
In this section you will learn how to use NAT devices in Amazon VPC.



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.

You can use a NAT device to enable instances in a private subnet to connect to the Internet or other AWS services. However, it prevents the Internet from initiating connections with the instances.



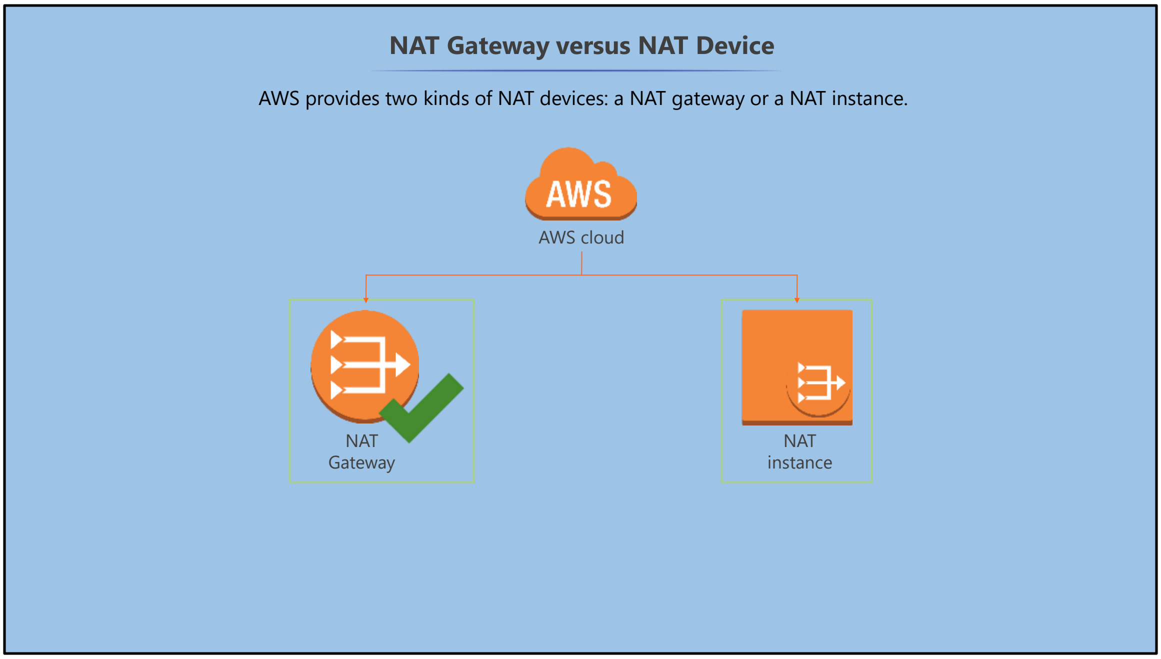
NAT Devices Overview (Contd.)

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

We talked earlier about using public and private subnets to protect assets from being directly connected to the Internet. For example, your web server sits in the public subnet and your database in the private subnet, which does not have Internet connectivity.

However, your private subnet database instance might still need Internet access. It can connect to other AWS resources if you use a Network Address Translation (NAT) device. A NAT device forwards traffic from your private subnet instances to the Internet or other AWS services and then sends the response back to the instances.

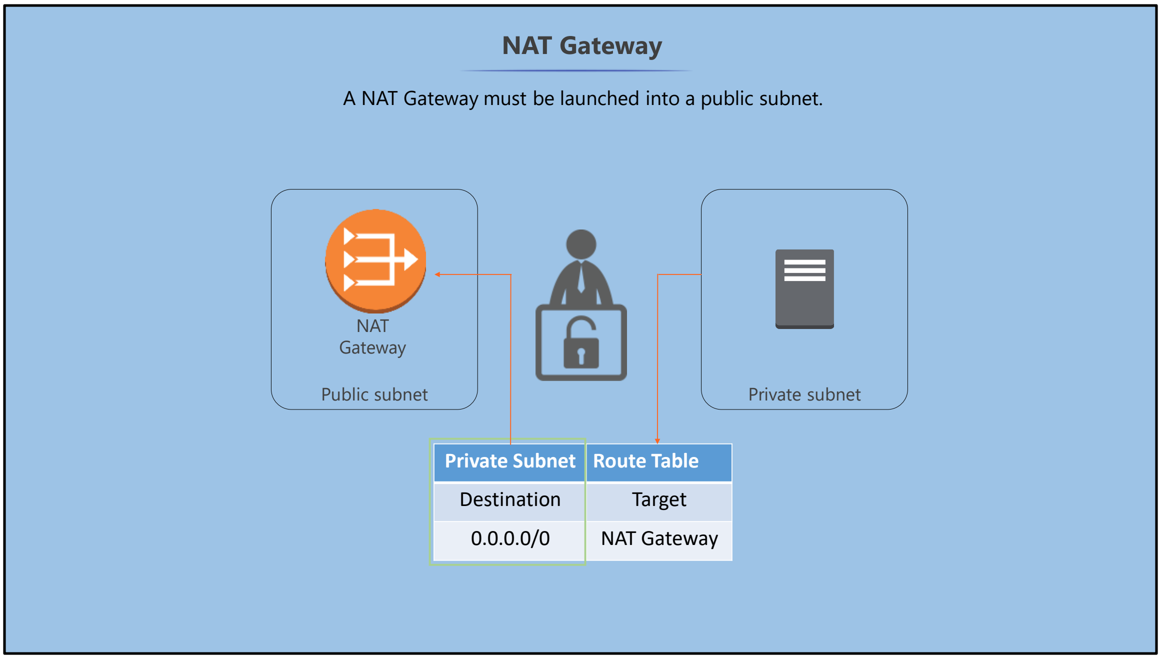
When traffic goes to the Internet, the source IP address of your instance is replaced with the NAT device's address and, when the Internet traffic goes back to your instances, the NAT device translates the address to your instances' private IP addresses.



NAT Gateway versus NAT Device

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

AWS provides two kinds of NAT devices: a NAT gateway or a NAT instance.
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.
A NAT instance is launched from a NAT AMI and runs as an instance in your VPC.

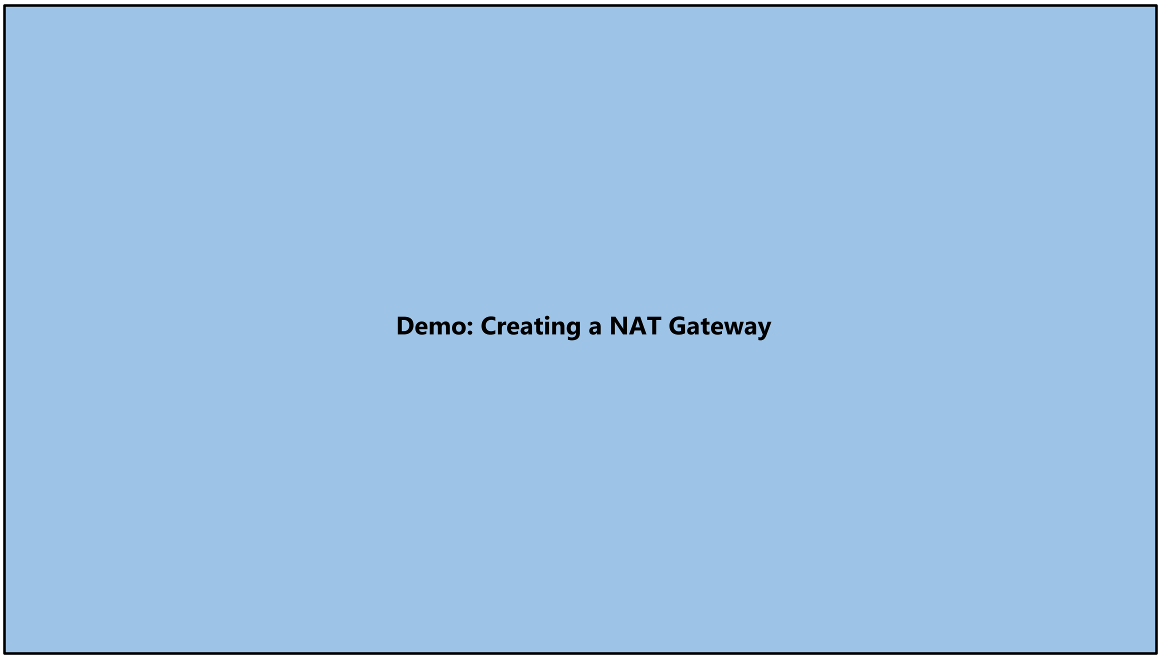


NAT Gateway

A NAT Gateway must be launched into a public subnet.

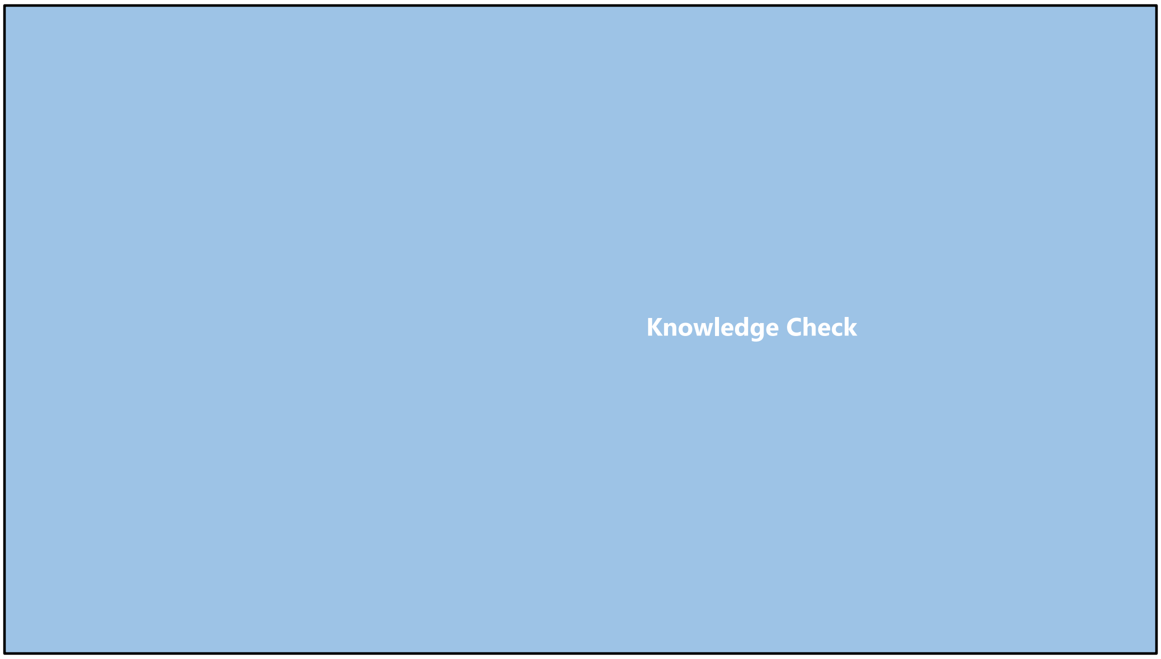
Private Subnet	Route Table
Destination	Target
0.0.0.0/0	NAT Gateway

A NAT Gateway must be launched into a public subnet, as it has Internet connectivity. It also needs an Elastic IP address which you can select at the launch time. Once created, you need to update the route table associated with your private subnet to point Internet-bound traffic to the NAT gateway so that the instances in your private subnets can communicate with the Internet. So, the private subnet also gets Internet.

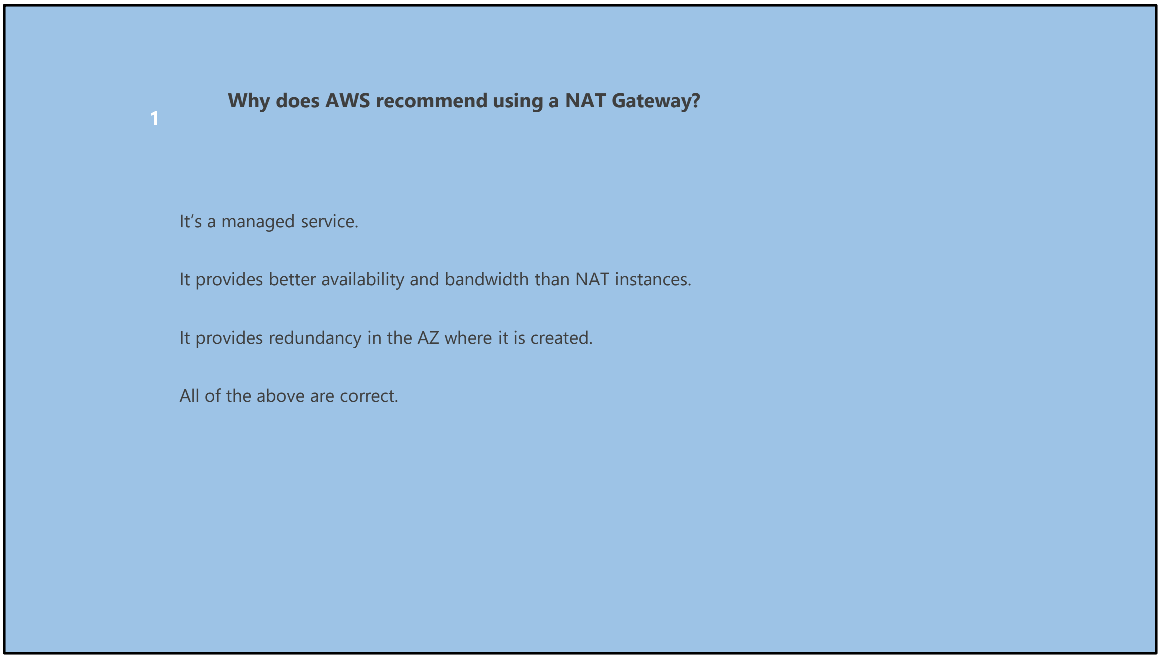


Demo: Creating a NAT Gateway

In this demonstration you’ll learn how to create a NAT gateway.



Knowledge Check



1

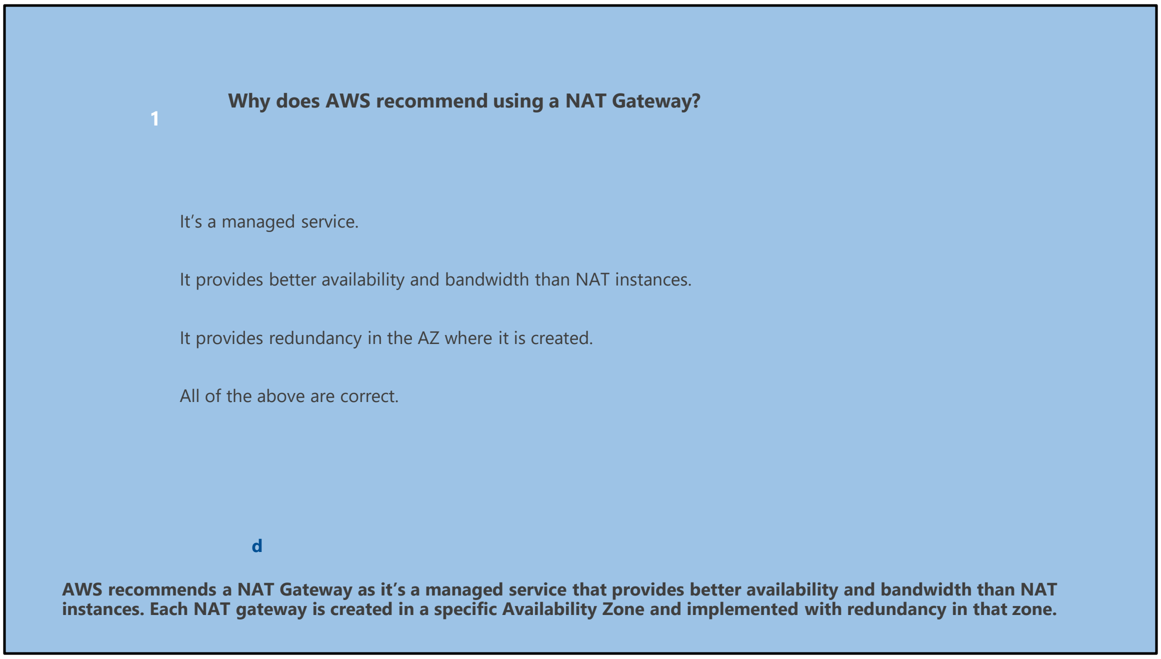
Why does AWS recommend using a NAT Gateway?

It’s a managed service.

It provides better availability and bandwidth than NAT instances.

It provides redundancy in the AZ where it is created.

All of the above are correct.



1

Why does AWS recommend using a NAT Gateway?

It's a managed service.

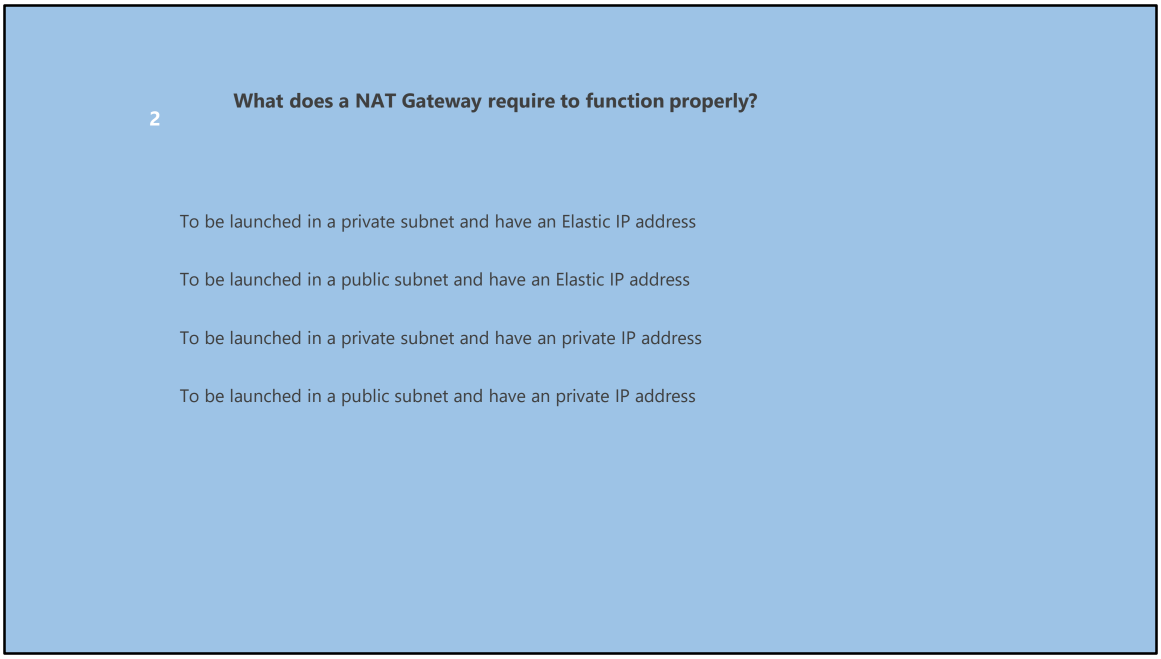
It provides better availability and bandwidth than NAT instances.

It provides redundancy in the AZ where it is created.

All of the above are correct.

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.



2

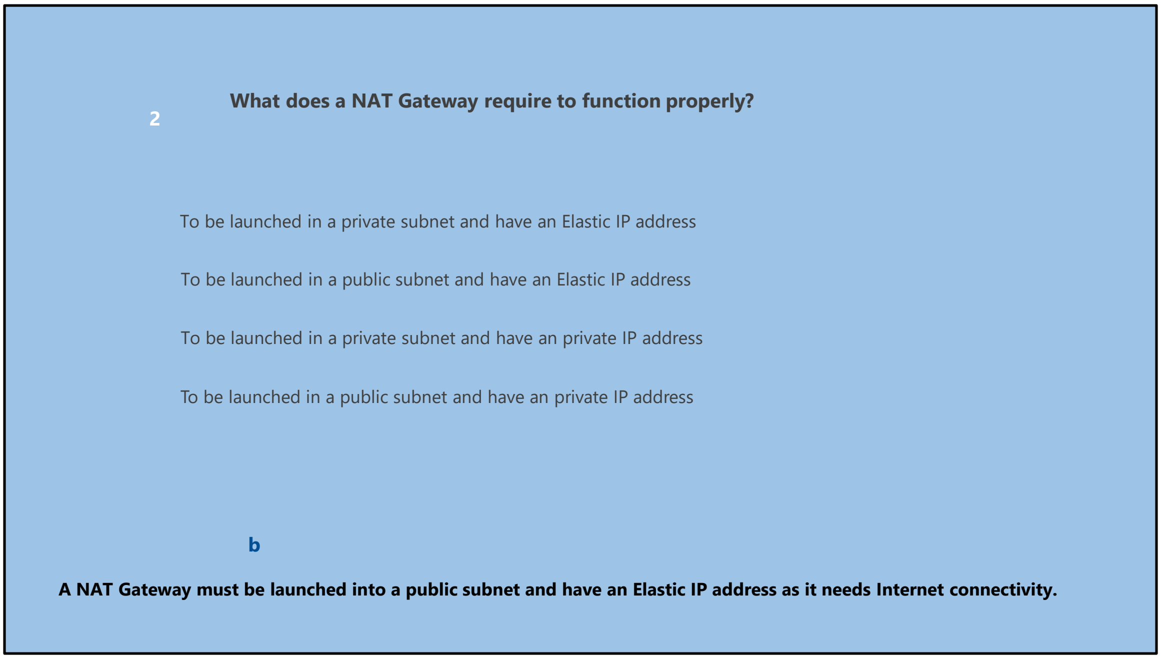
What does a NAT Gateway require to function properly?

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

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

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

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



2

What does a NAT Gateway require to function properly?

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

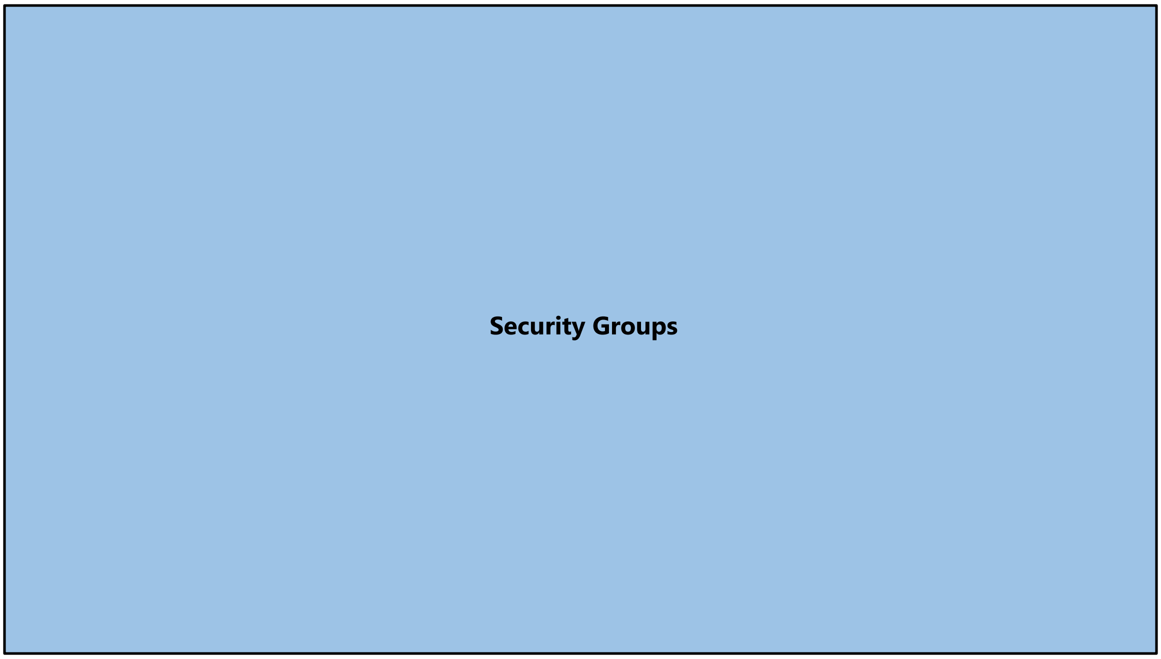
To be launched in a public subnet and have an Elastic IP address

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

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

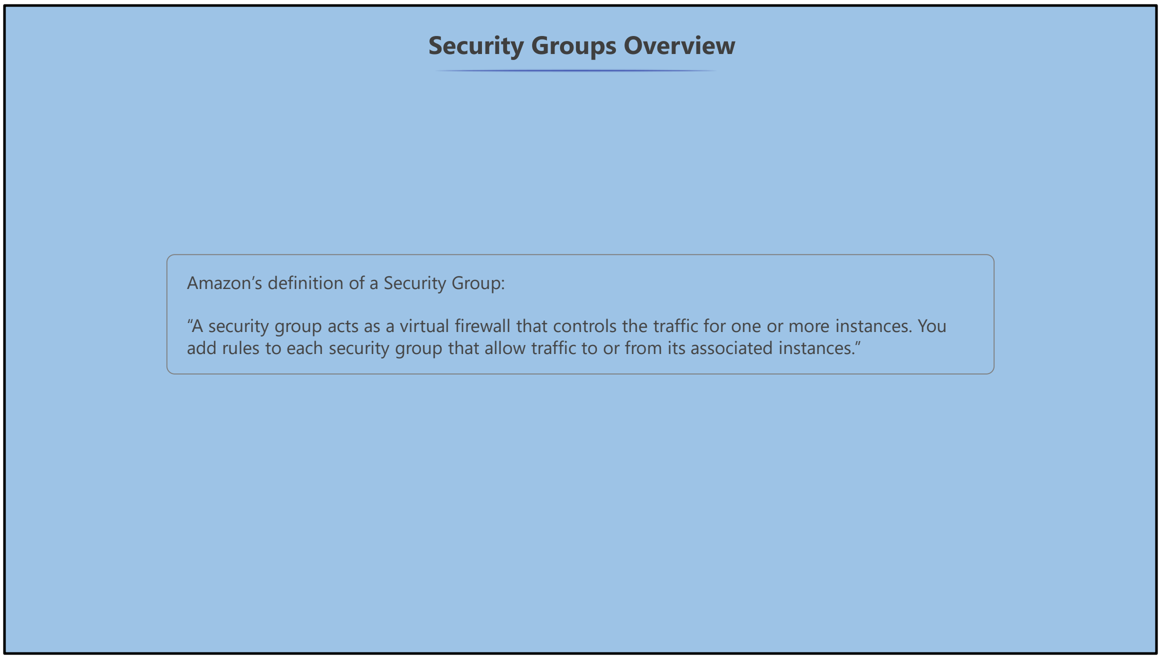
b

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



Security Groups

In this section you'll learn about using security groups in Amazon VPC.

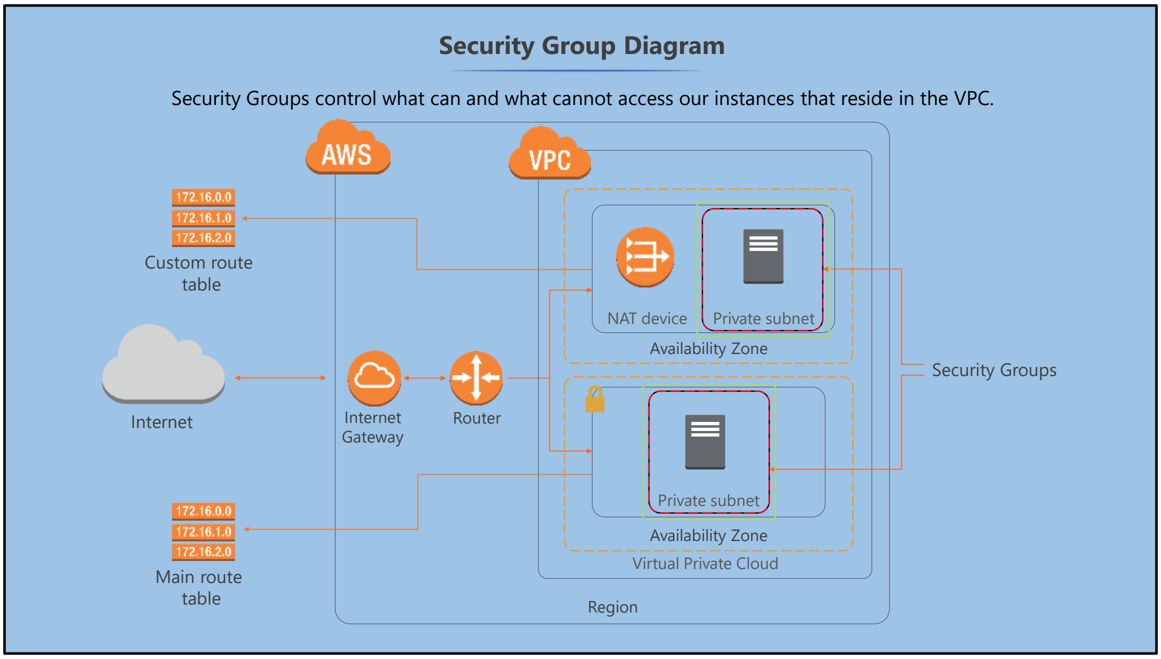


Security Groups Overview

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."

A security group acts as a virtual firewall that controls the traffic for one or more instances.
You can add rules to each security group that allows traffic to or from its associated instances.
A security group can control the inbound and outbound traffic for one or more EC2 instances.
Security Groups can be found on both the EC2 and VPC dashboards in the AWS Web Management Console.



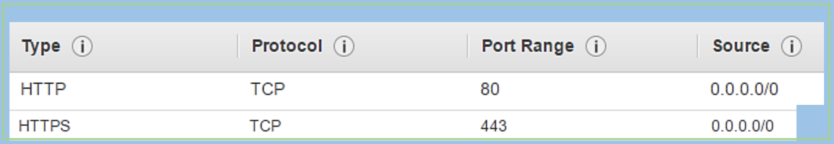
Security Group Diagram

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

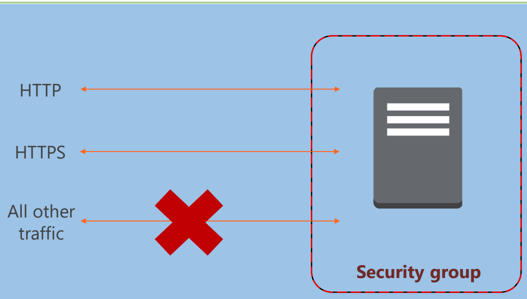
Security Groups control what can and what cannot access our instances that reside in our VPC.

Security Groups for Webservers

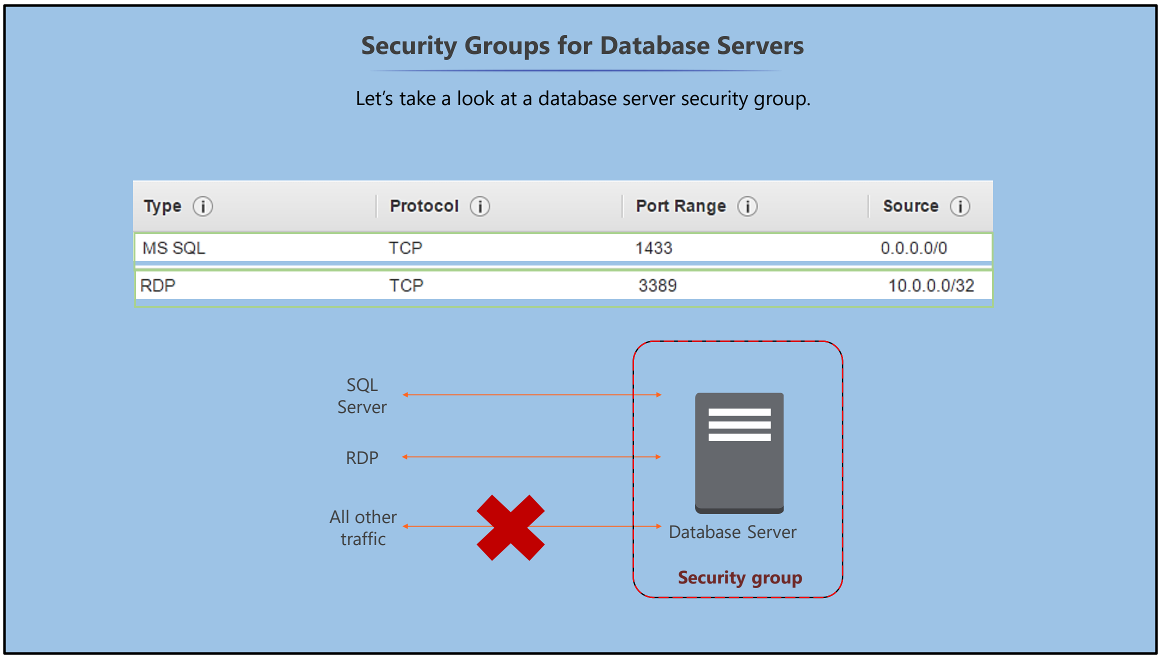
Let’s take a look at some examples:
The webserver needs to receive traffic from the Internet on HTTP and HTTPS ports.



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



Let’s take a look at some examples:
The webserver needs to receive traffic from the Internet on HTTP and HTTPS ports.
The security group table in the example allows http and https and the port and the sources.

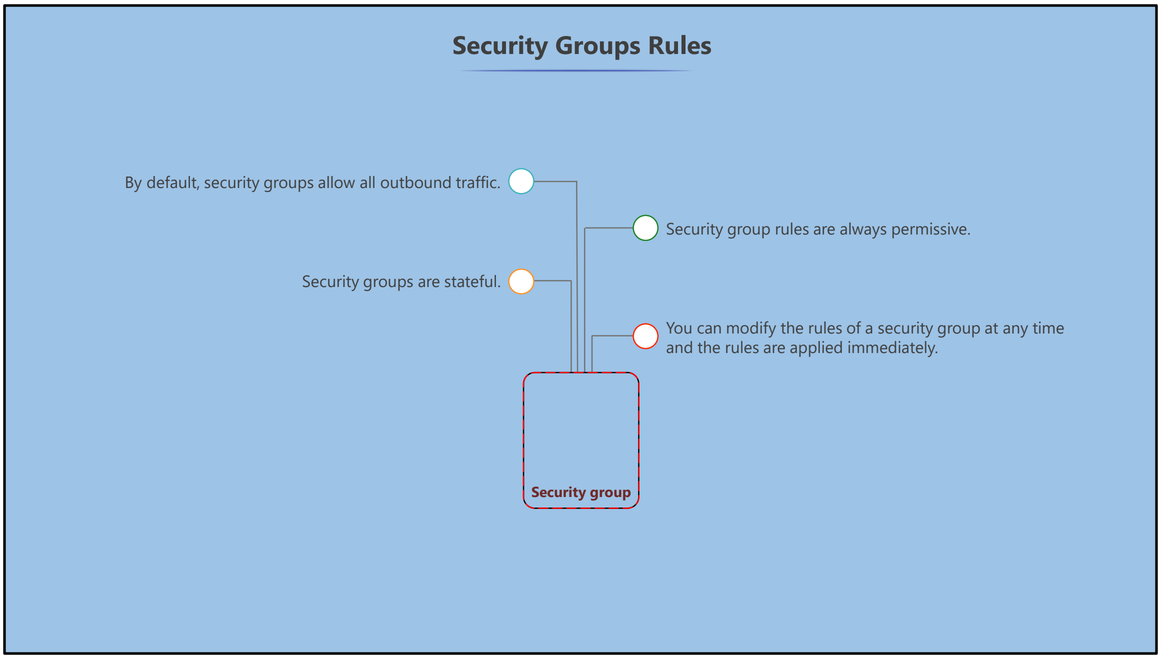


Security Groups for Database Servers

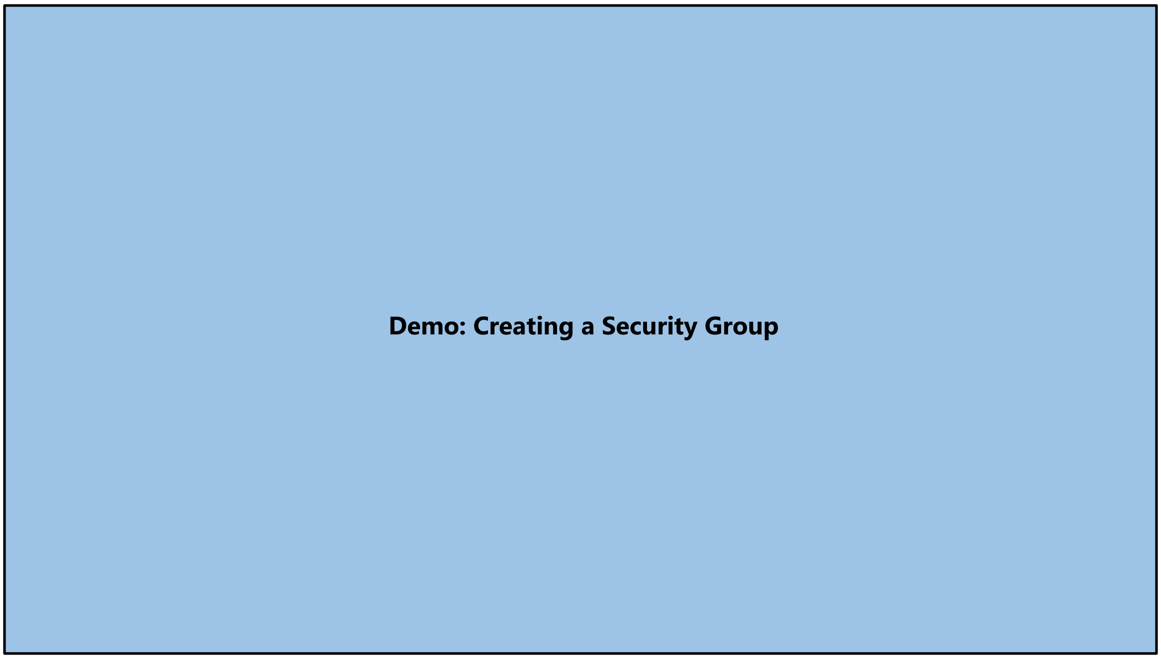
Let's take a look at a database server security group.

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

A database server receives traffic from the webserver on SQL Server port and RDP.
A Windows server receives RDP traffic on RDP port, but only from specified IP ranges.

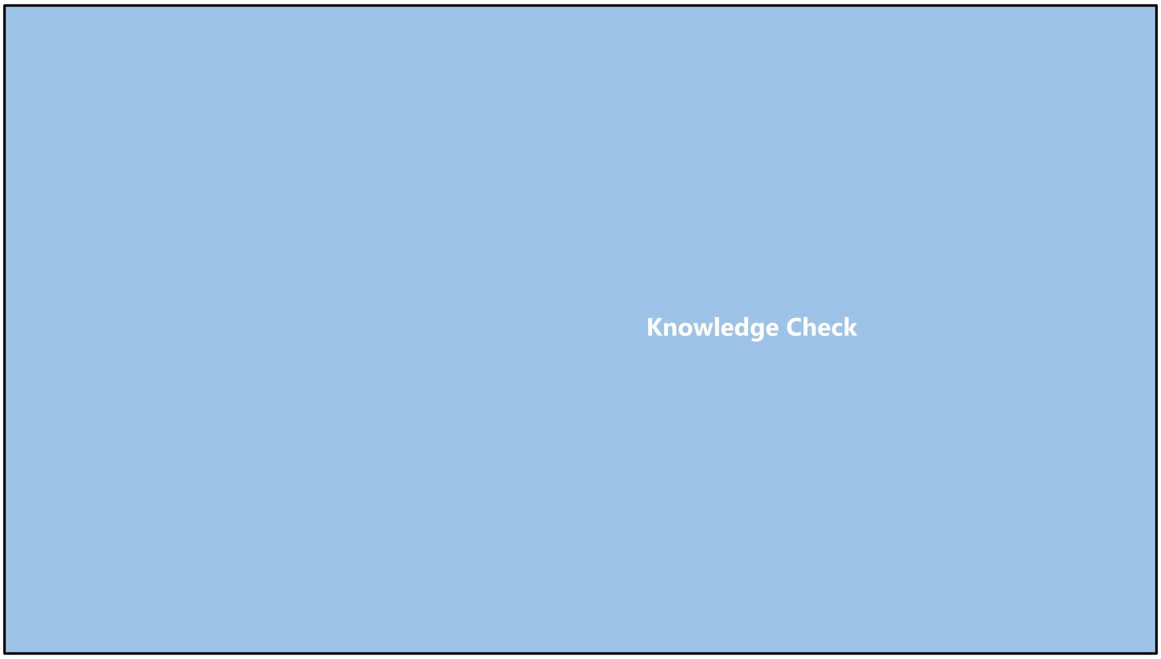

Security Groups Rules
By default, security groups allow all outbound traffic.
Security group rules are always permissive.
Security groups are stateful.
You can modify the rules of a security group at any time and the rules are applied immediately.
Security group

The default setting for security groups is to allow all outbound traffic.
Security group rules are always permissive; you can't create rules that deny access.
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.
You can modify the rules of a security group any time and the rules get applied with immediate effect.

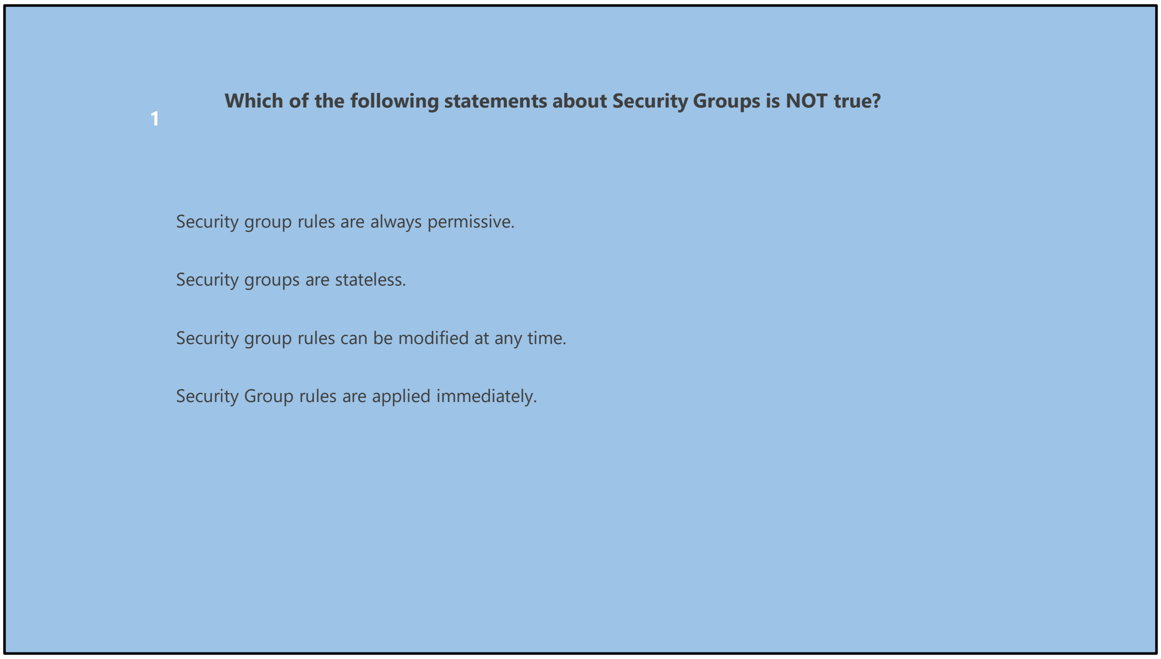


Demo: Creating a Security Group

In this demonstration you’ll learn how to create a security group.



Knowledge Check



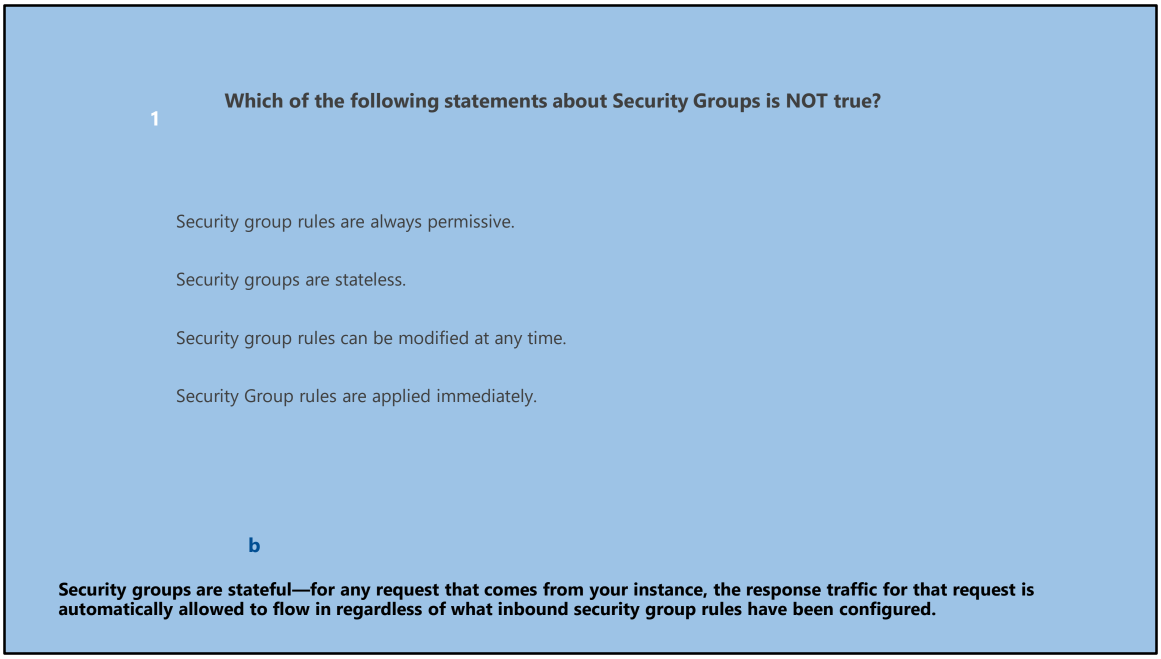
1 **Which of the following statements about Security Groups is NOT true?**

Security group rules are always permissive.

Security groups are stateless.

Security group rules can be modified at any time.

Security Group rules are applied immediately.



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

Security group rules are always permissive.

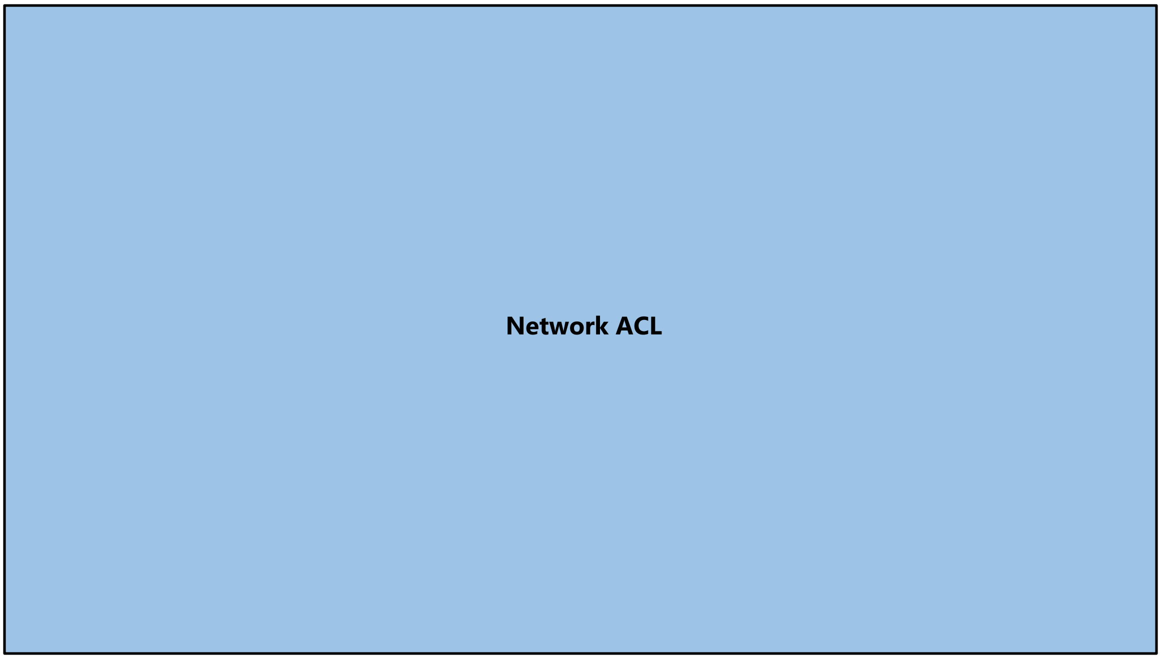
Security groups are stateless.

Security group rules can be modified at any time.

Security Group rules are applied immediately.

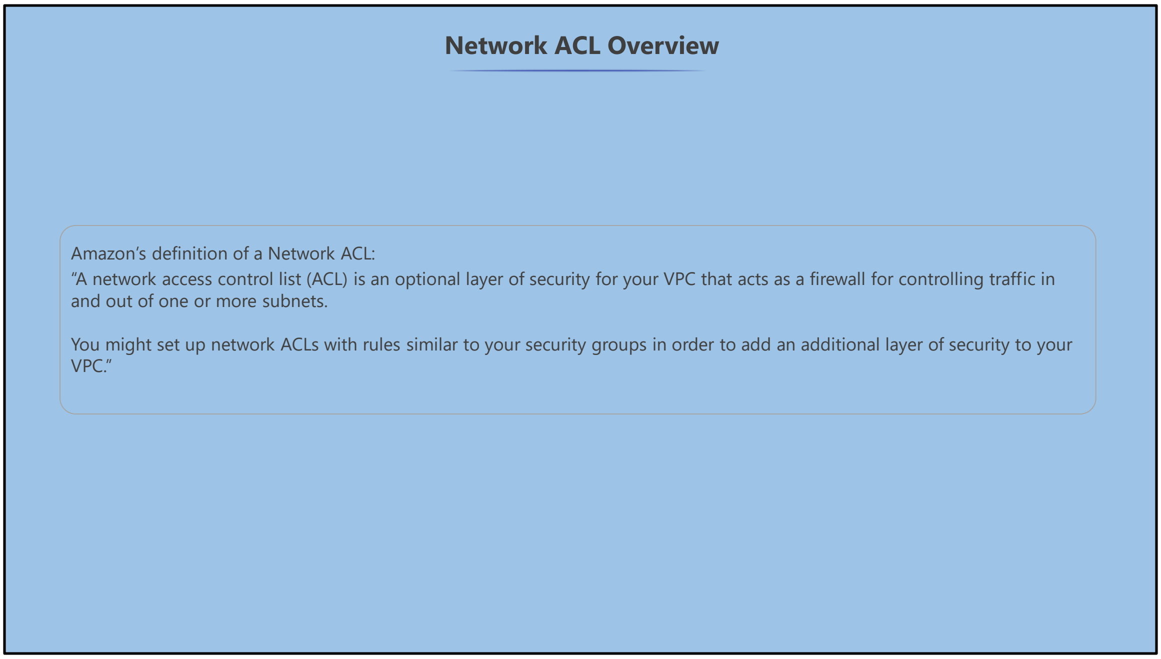
b

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

In this section you’ll learn about using Network ACLs in Amazon VPC.



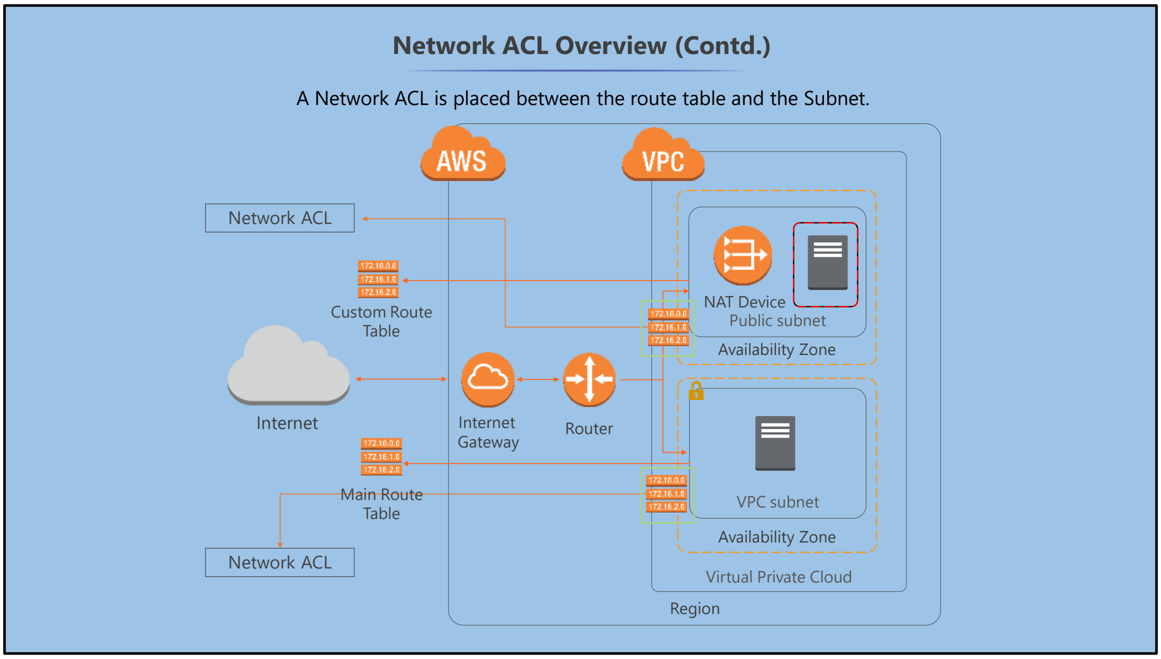
Network ACL Overview

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."

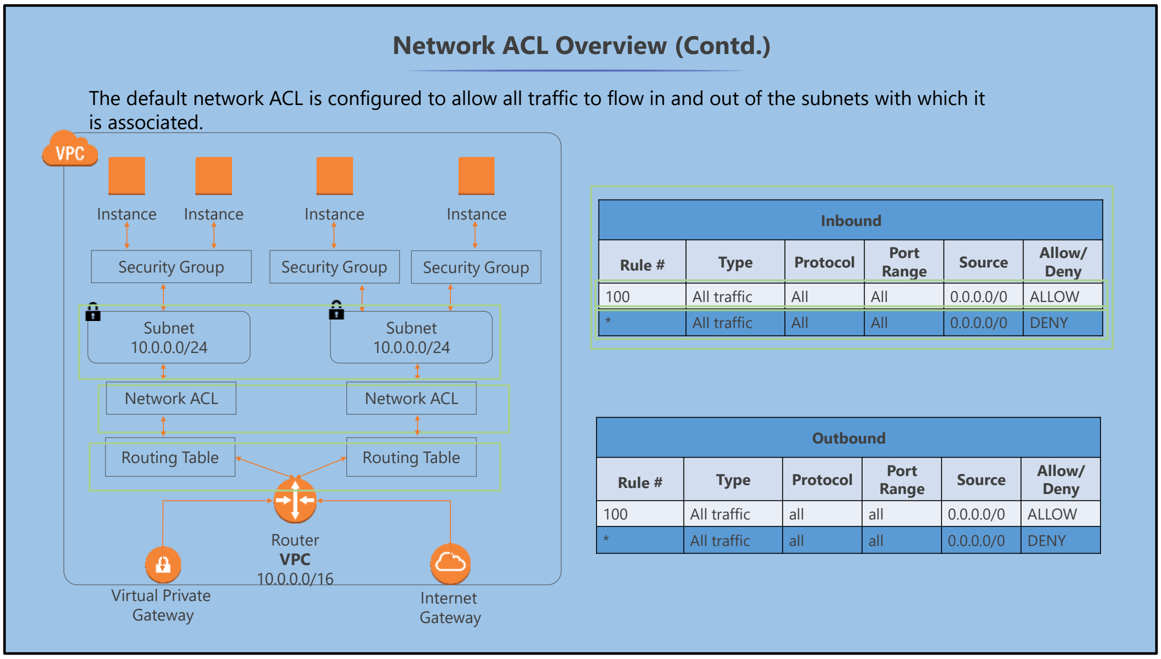
A network Access Control List (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You can set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.



Network ACL Overview (Contd.)

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

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



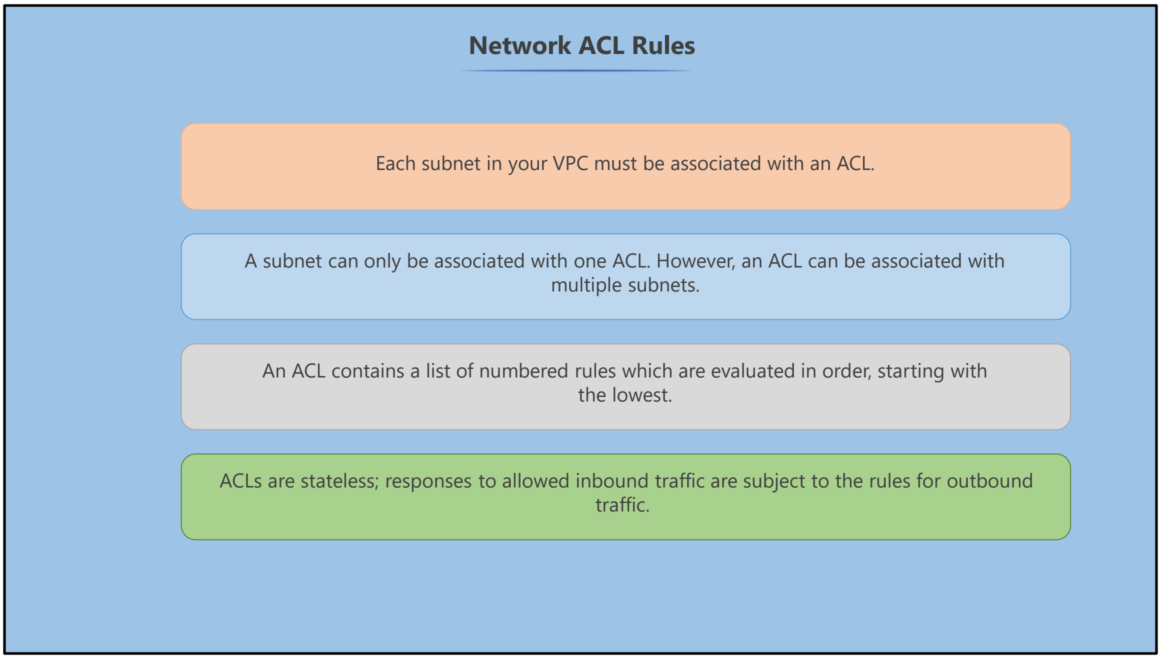
Network ACL Overview (Contd.)

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

A Network ACL is placed between the route table and the Subnet. The default network ACL is configured to allow all traffic to flow in and out of the subnets to which it is associated. Each network ACL includes a rule, where the rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.
In the table “Inbound”, the traffic (will look for/ is routed to/ will be matched to) the first rule, which is 100. This rule allows traffic from all sources. If the rule 100 doesn’t exist, the traffic (will go to/ will be matched to) the asterisk rule, which denies traffic from all sources.



Network ACL Rules

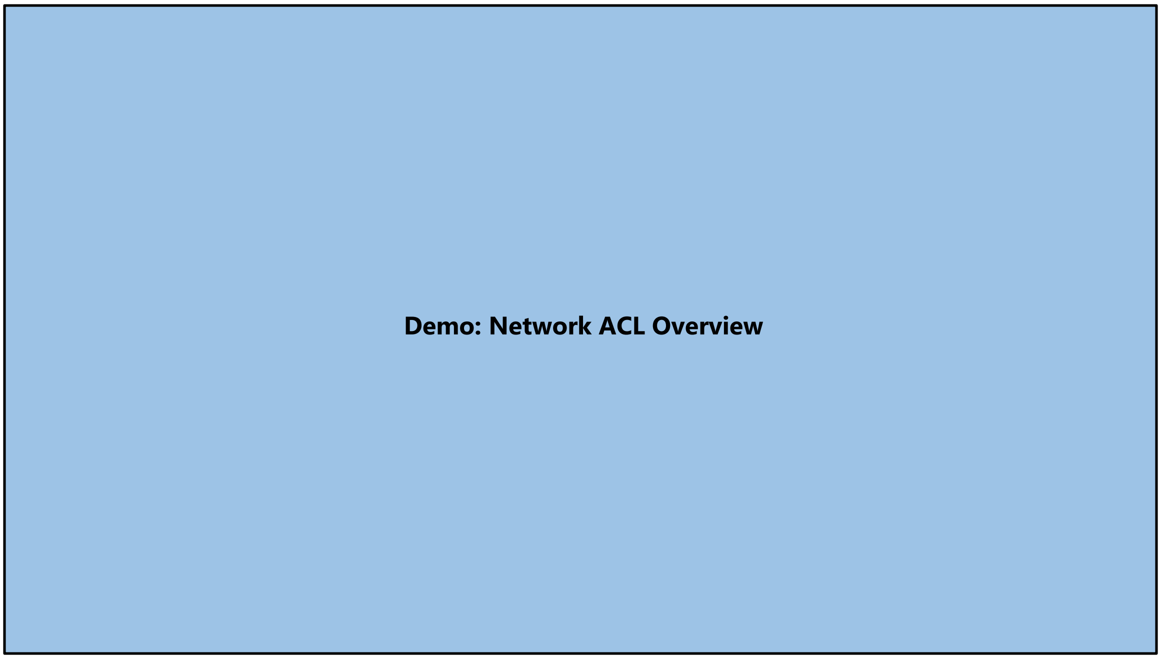
Each subnet in your VPC must be associated with an ACL.

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.

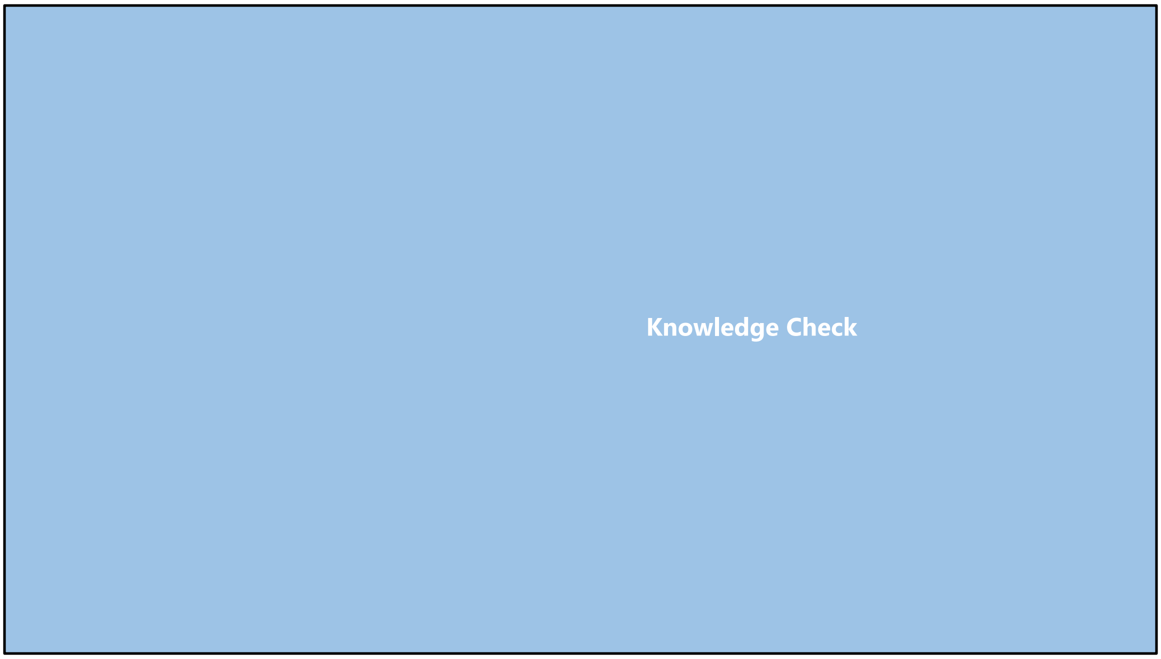
ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic.

Each subnet in your VPC must be associated with an ACL. If you don’t assign it to a custom ACL, it will automatically be associated to your default 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. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that may contradict it. AWS recommends incrementing your rules by a factor of 100, so there is plenty of room to implement new rules at a later date.
Unlike Security Groups, ACLs are stateless; responses to allowed inbound traffic are subject to the rules for outbound traffic.

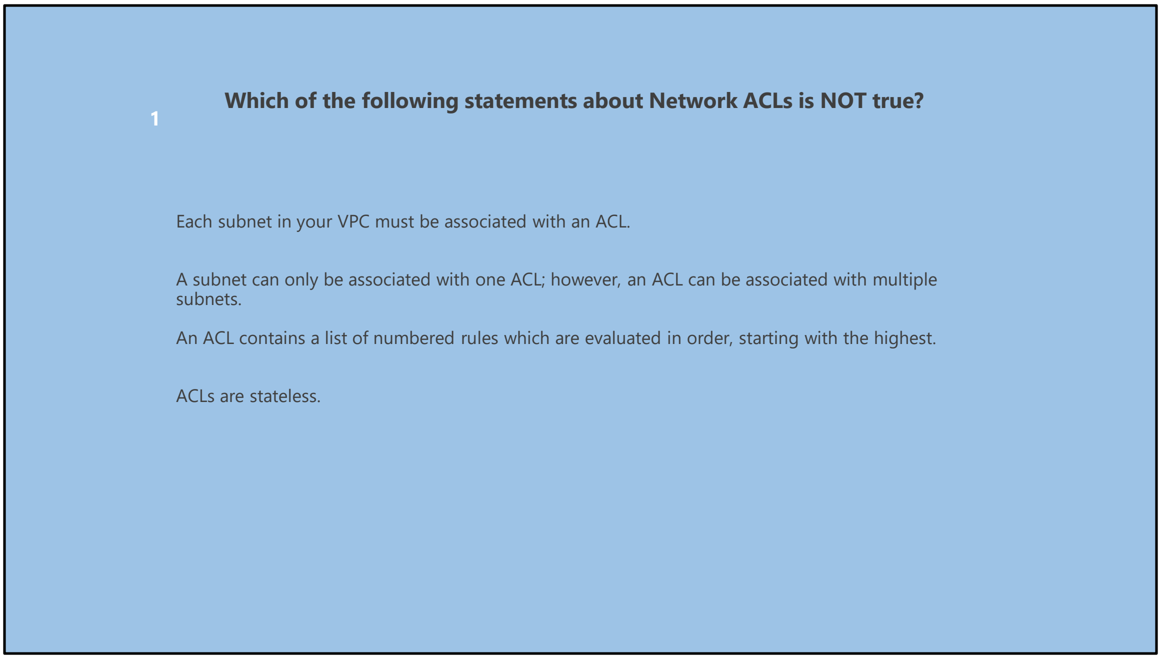


Demo: Network ACL Overview

In this demonstration you’ll learn where to look for Network ACL settings.



Knowledge Check



1

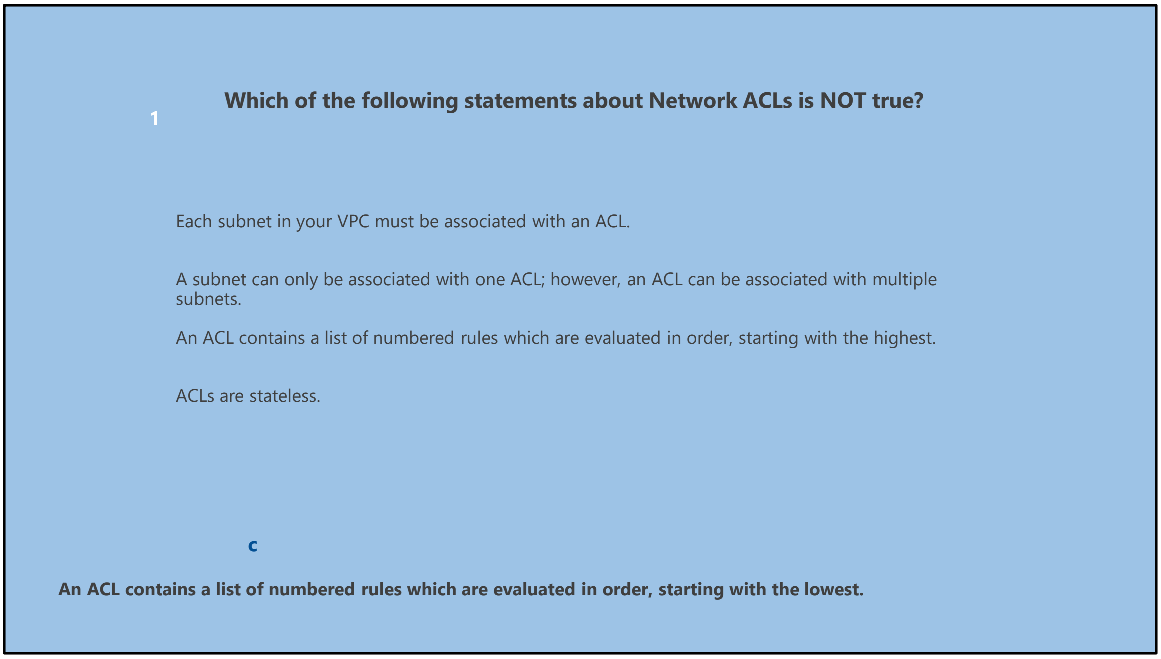
Which of the following statements about Network ACLs is NOT true?

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 highest.

ACLs are stateless.



1

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

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

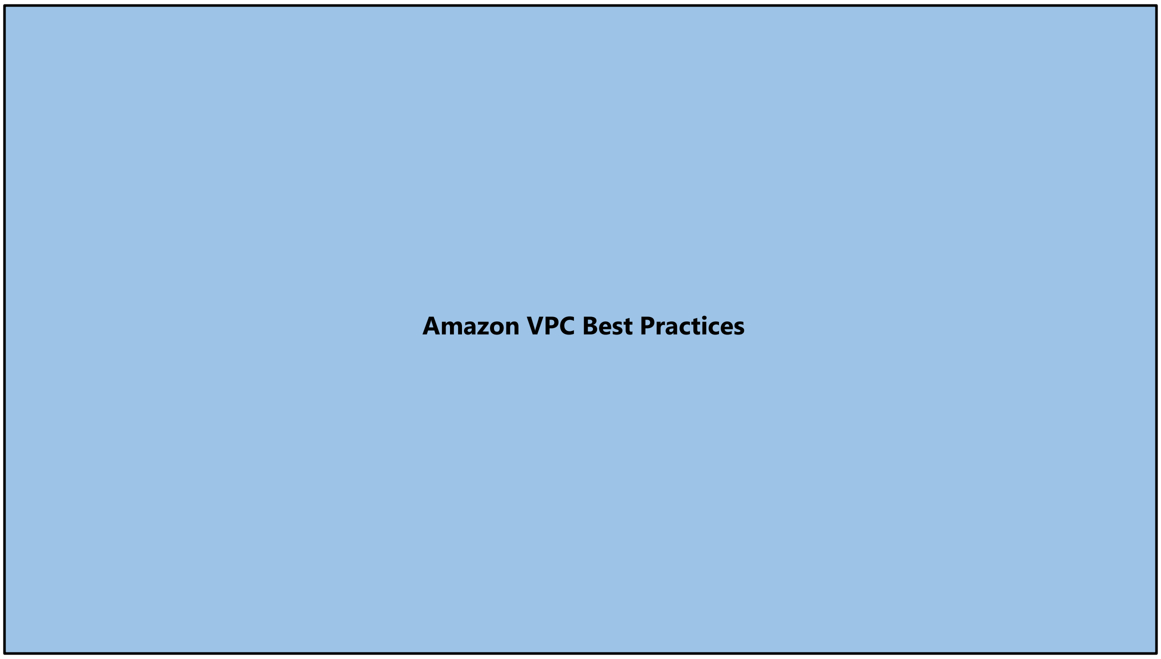
A subnet can only be associated with one ACL; however, an ACL can be associated with multiple subnets.

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

ACLs are stateless.

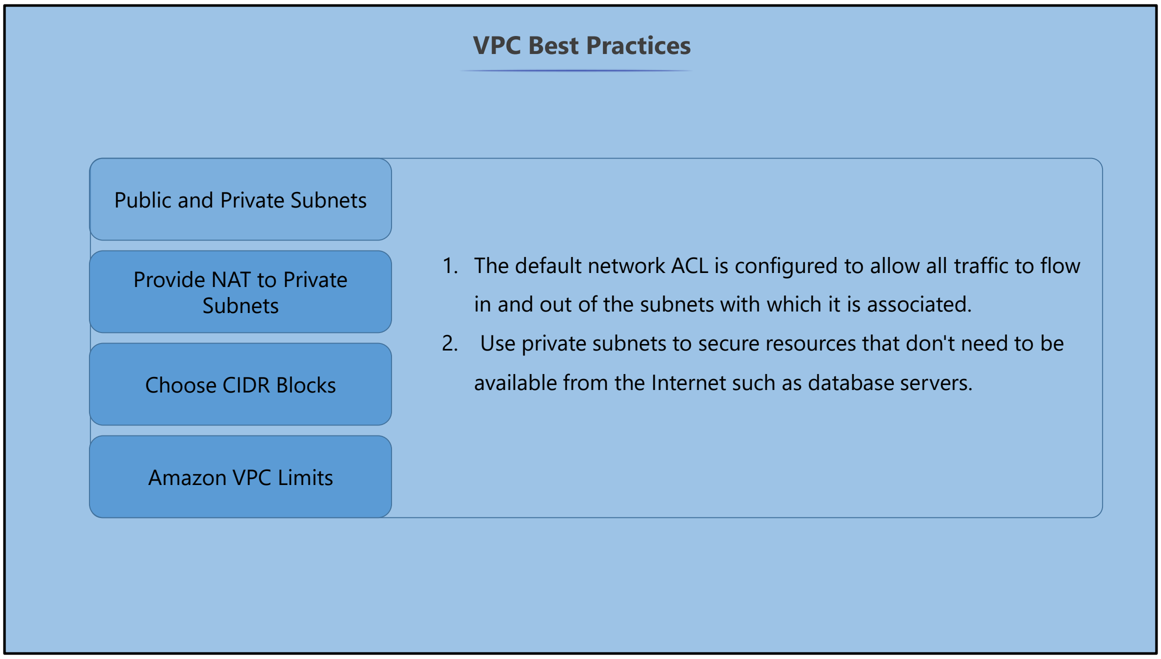
c

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



Amazon VPC Best Practices

In this section you'll learn about the overview of AWS VPC recommended best practices.



VPC Best Practices

Public and Private Subnets

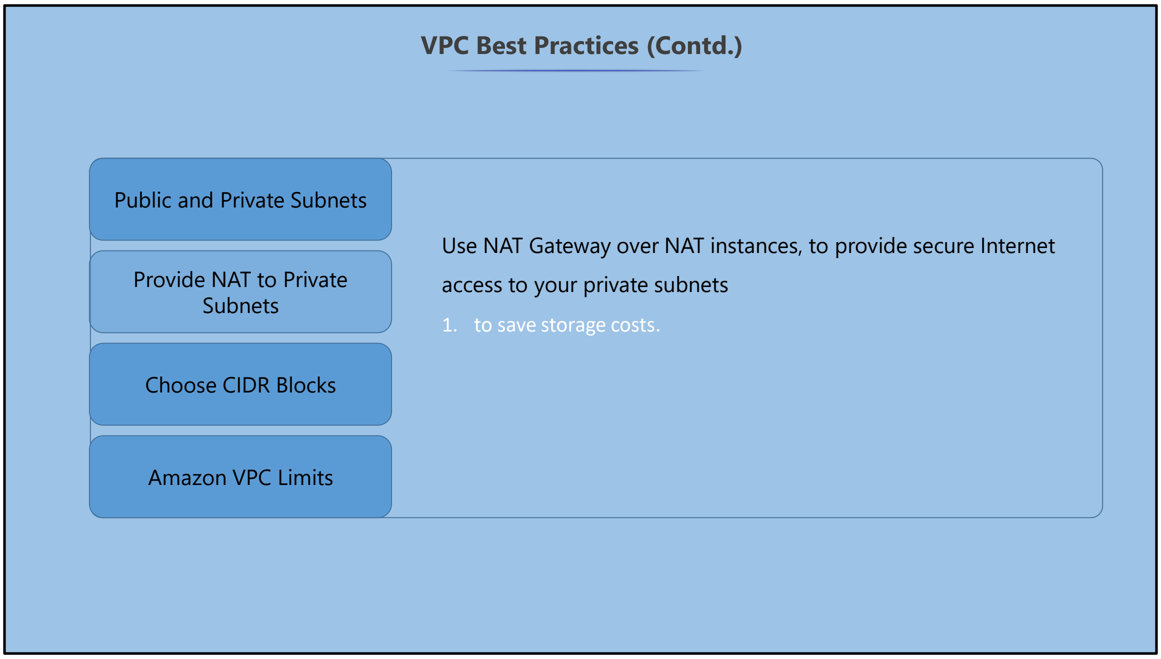
Provide NAT to Private Subnets

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.

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



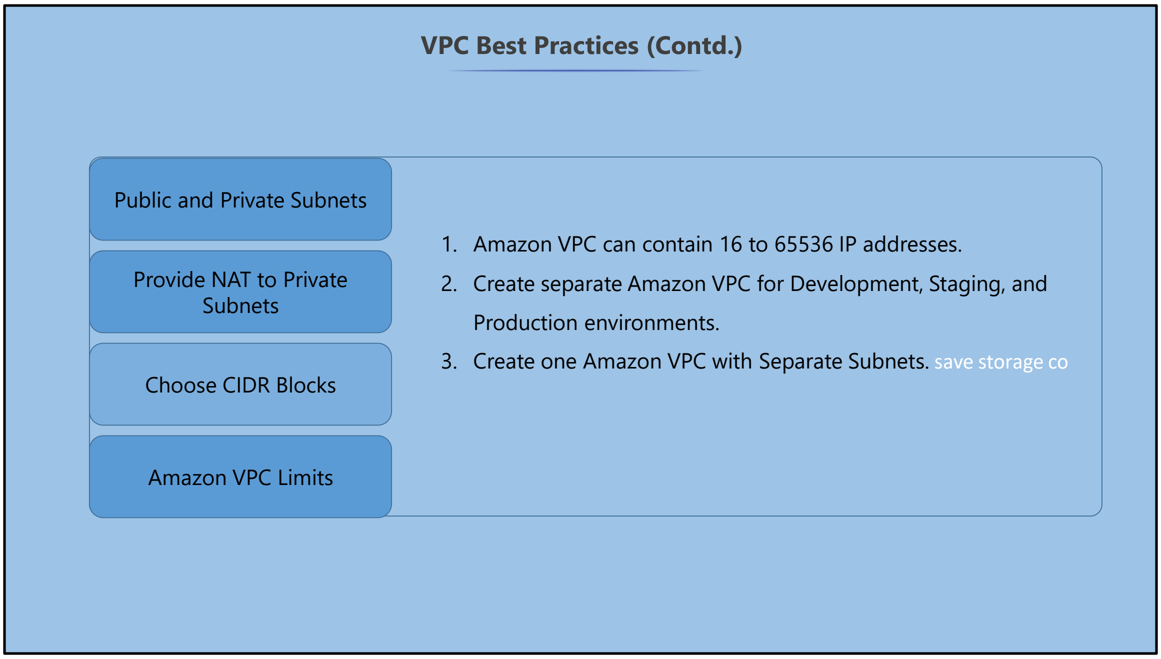
VPC Best Practices (Contd.)

- 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

1. to save storage costs.

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

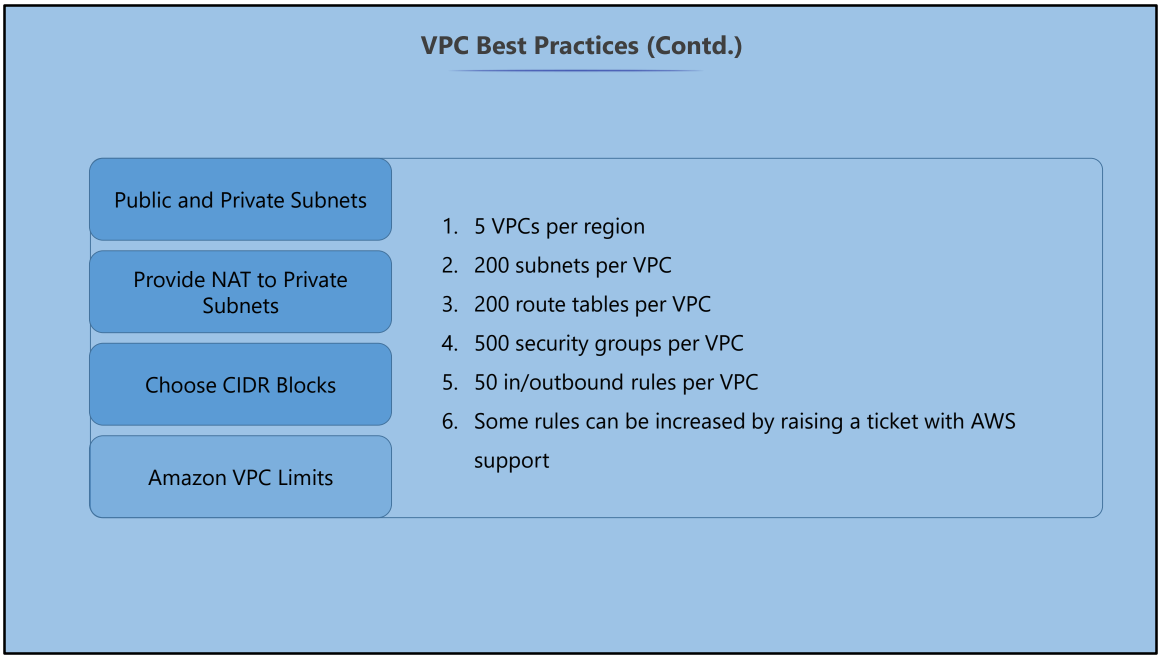


VPC Best Practices (Contd.)

- 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. save storage co

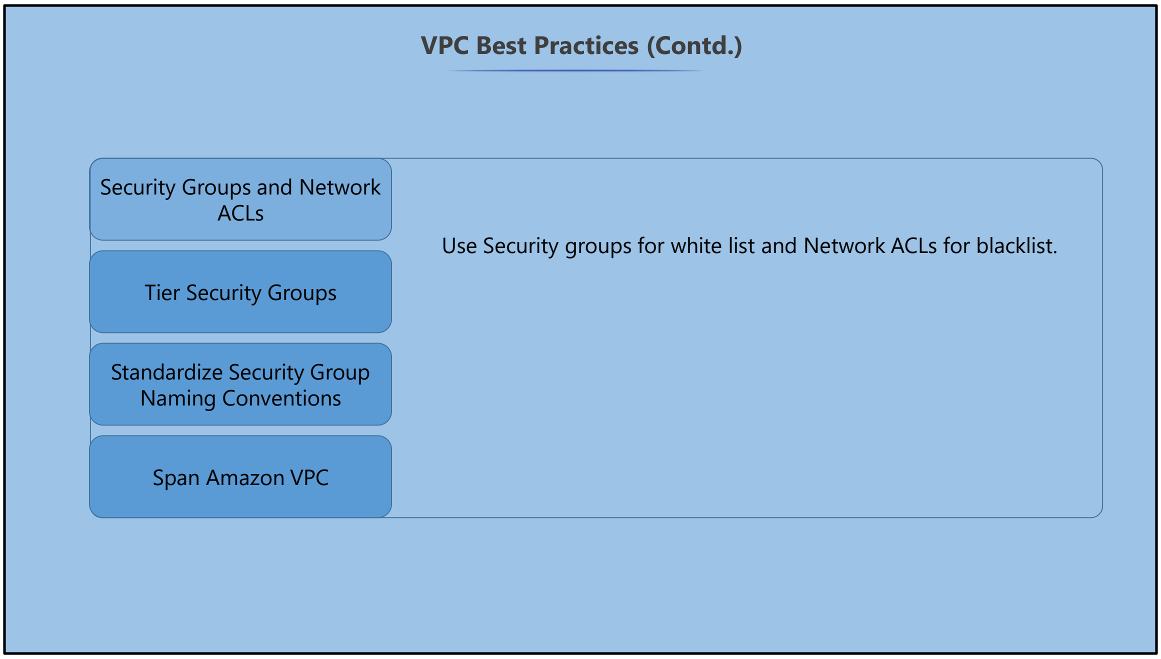
Amazon VPC can contain 16 to 65536 IP addresses. Choose your CIDR block according the number of instances you think you'll need. Also do not overlap CIDR blocks. Select different blocks for both Prod, DR, DEV, test VPCs.
Create separate Amazon VPC for Development, Staging, and Production environment.
Create one Amazon VPC with Separate Subnets NW groups for Production, Staging, and development.



VPC Best Practices (Contd.)

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

Understand Amazon VPC Limits:
Always design the VPC subnets in consideration with the expansion in the future and understand the Amazon VPC's limit. AWS has various limitations on the VPC components:
5 VPCs per region
200 subnets per VPC
200 route tables per VPC
500 security groups per VPC
50 in/outbound rules per VPC
Some rules can be increased by raising a ticket with AWS support.
For example, the number of EIPs per account.



VPC Best Practices (Contd.)

Security Groups and Network ACLs

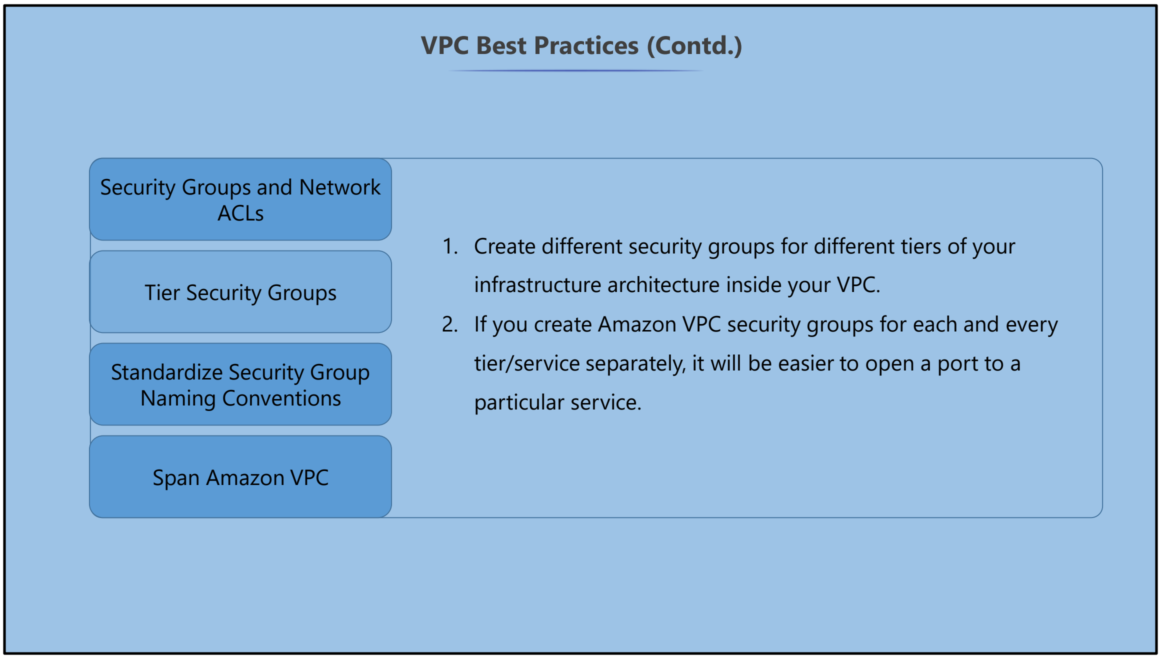
Tier Security Groups

Standardize Security Group Naming Conventions

Span Amazon VPC

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

Use security groups and Network ACLs: Use Security groups for White list and Network ACLs for blacklist.



VPC Best Practices (Contd.)

Security Groups and Network ACLs

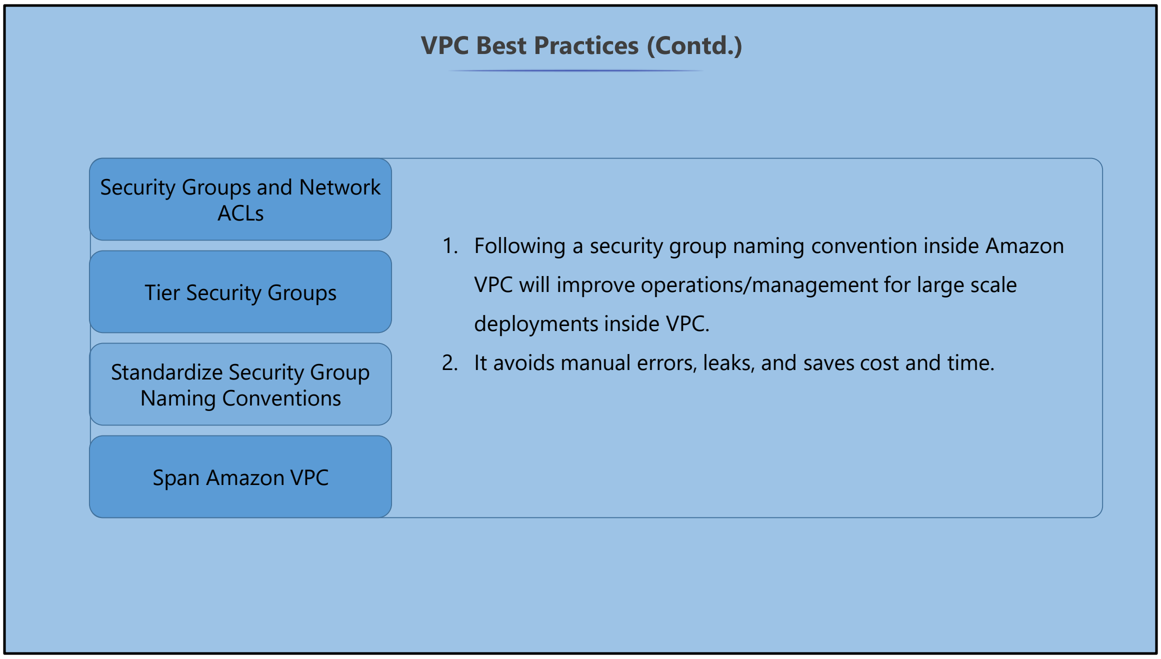
Tier Security Groups

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.

Create tiers for your Security Groups: Create different security groups for different tiers of your infrastructure architecture inside your VPC. If you have Web, App, DB tiers, then create different security group for each of them. Creating tier wise security groups will increase the infrastructure security inside Amazon VPC. EC2 instances in each tier can communicate only on application specified ports and not at all ports. 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. Don't use same security group for multiple tiers of instances.

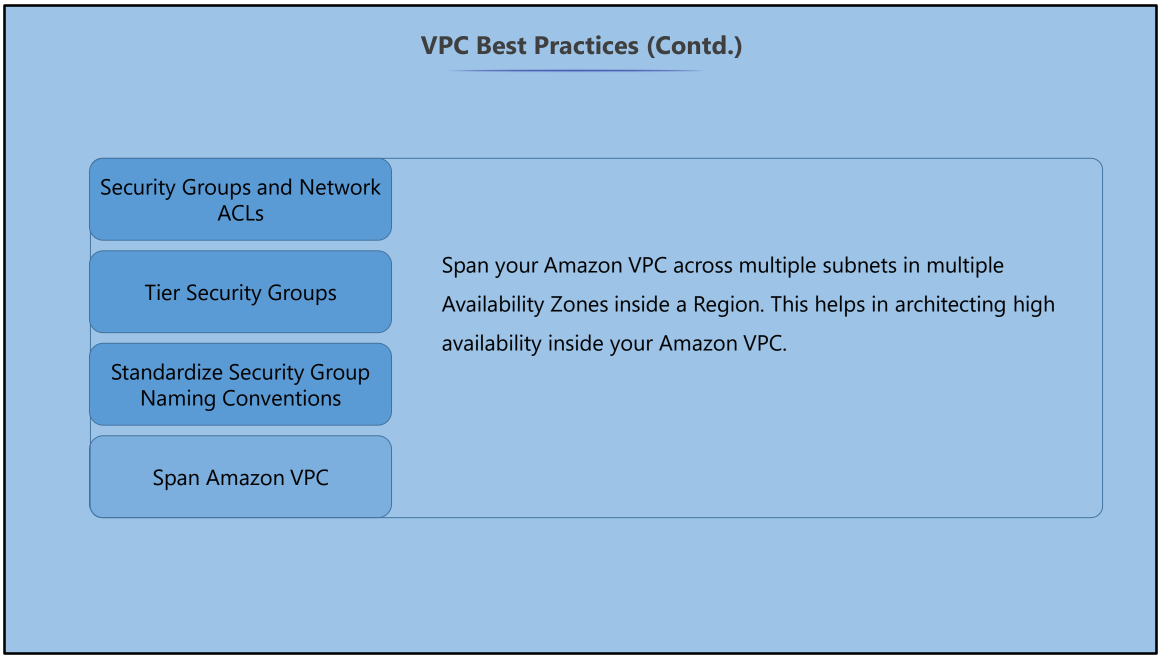


VPC Best Practices (Contd.)

- 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.

Standardize your Security Group Naming conventions: Following a security group naming convention inside Amazon VPC will improve operations/management for large scale deployments inside VPC. It also avoids manual errors, leaks, and saves cost and time.
ELB on Amazon VPC: When using Amazon ELB for Web Applications, put all other EC2 instances (tiers like App, cache, DB, BG, and so on) in private subnets as much as possible. Unless there is a specific requirement where instances need outside world access and EIP attached, put all instances only in private subnet. Only ELBs should be provisioned in Public Subnet as secure practice in Amazon VPC environment.



VPC Best Practices (Contd.)

Security Groups and Network ACLs

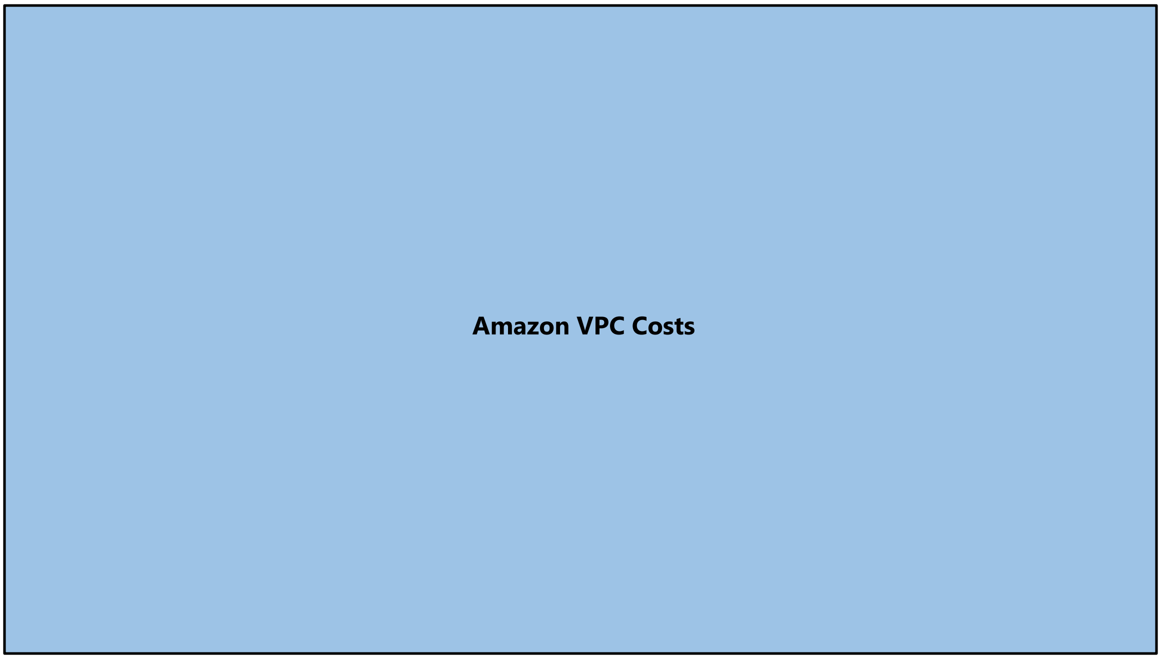
Tier Security Groups

Standardize Security Group Naming Conventions

Span Amazon VPC

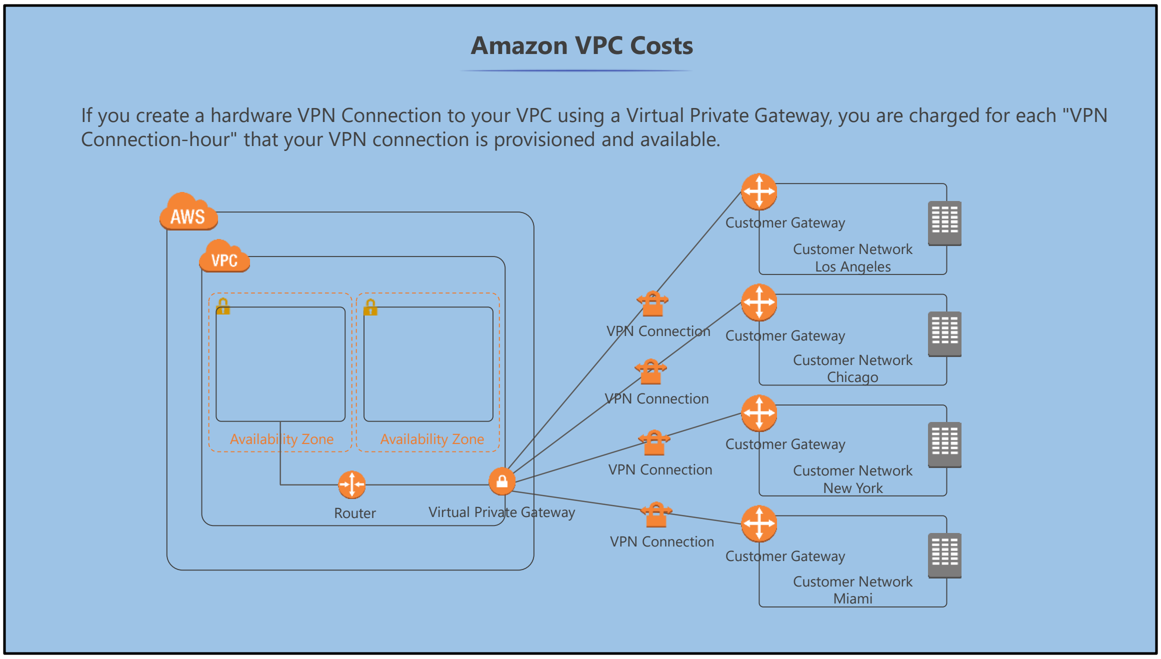
Span your Amazon VPC across multiple subnets in multiple Availability Zones inside a Region. This helps in architecting high availability inside your Amazon VPC.

Always 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

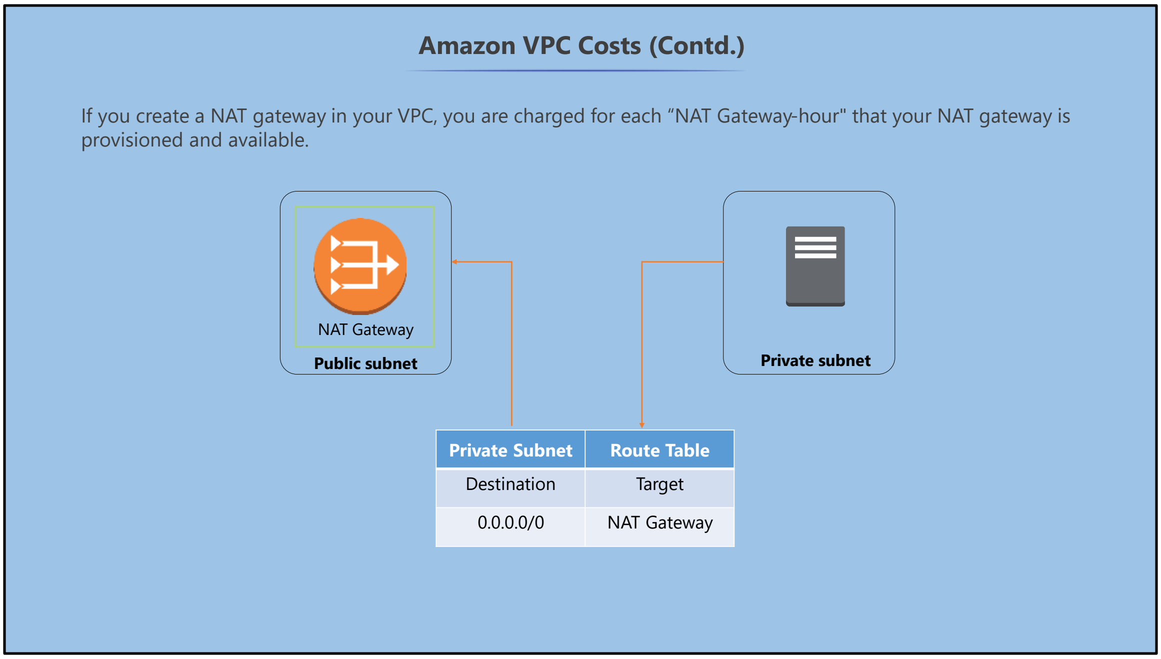
In this section you’ll learn about the costs associated with the Amazon VPC.



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.

If you choose to 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. Each partial VPN Connection-hour consumed is billed as a full hour. You also incur standard AWS data transfer charges for all data transferred via the VPN Connection.

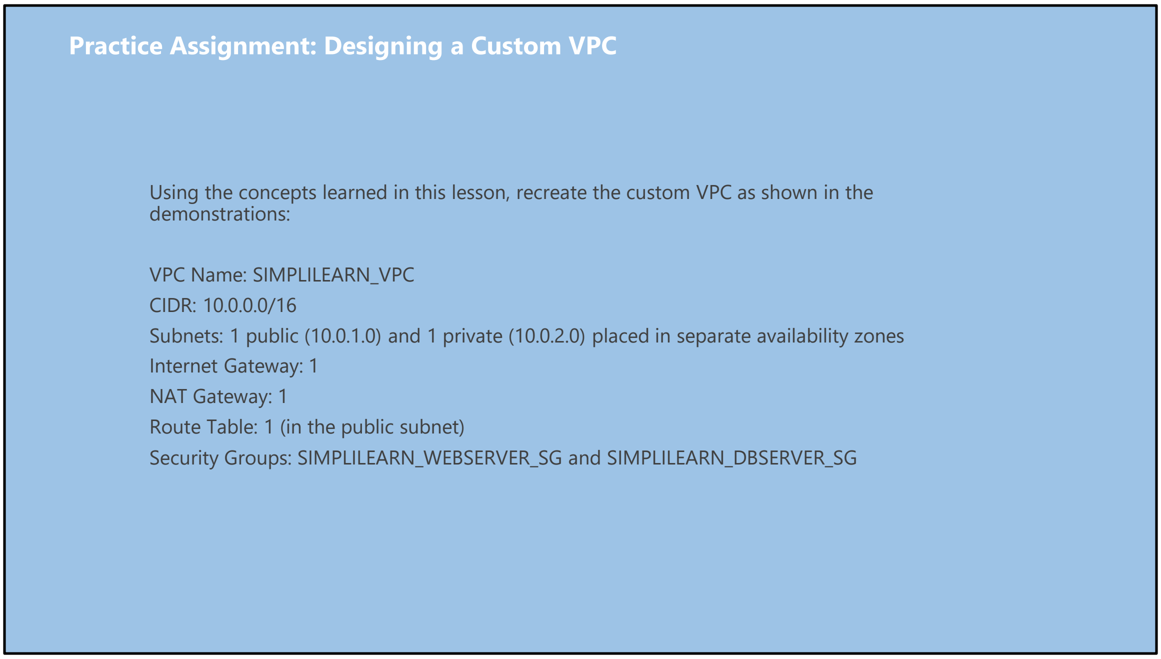


Amazon VPC Costs (Contd.)

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

If you choose to create a NAT gateway in your VPC, you are charged for each “NAT Gateway-hour" that your NAT gateway is provisioned and available. Data processing charges apply for each Gigabyte processed through the NAT gateway. Each partial NAT Gateway-hour consumed is billed as a full hour. You also incur standard AWS data transfer charges for all data transferred via the NAT gateway.



Practice Assignment: Designing 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

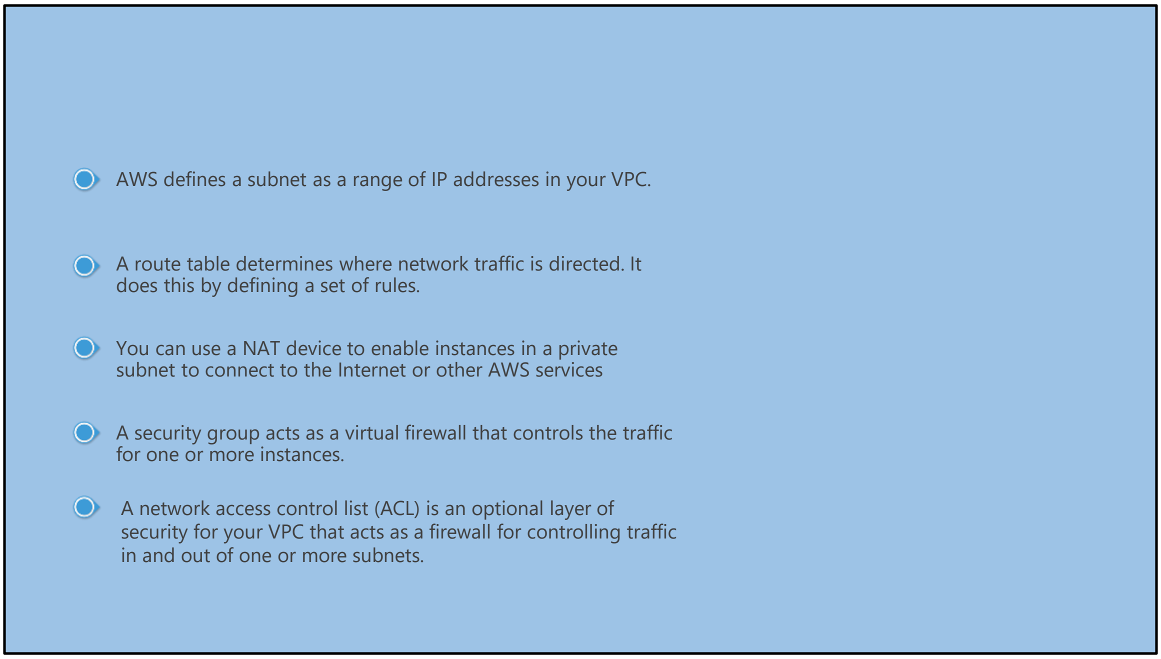
Internet Gateway: 1

NAT Gateway: 1

Route Table: 1 (in the public subnet)

Security Groups: SIMPLILEARN_WEBSERVER_SG and SIMPLILEARN_DBSERVER_SG

In this section you'll create a custom VPC using the concept.s learned in this lesson



- AWS defines a subnet as a range of IP addresses in your VPC.
- A route table determines where network traffic is directed. It does this by defining a set of rules.
- You can use a NAT device to enable instances in a private subnet to connect to the Internet or other AWS services
- A security group acts as a virtual firewall that controls the traffic for one or more 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.

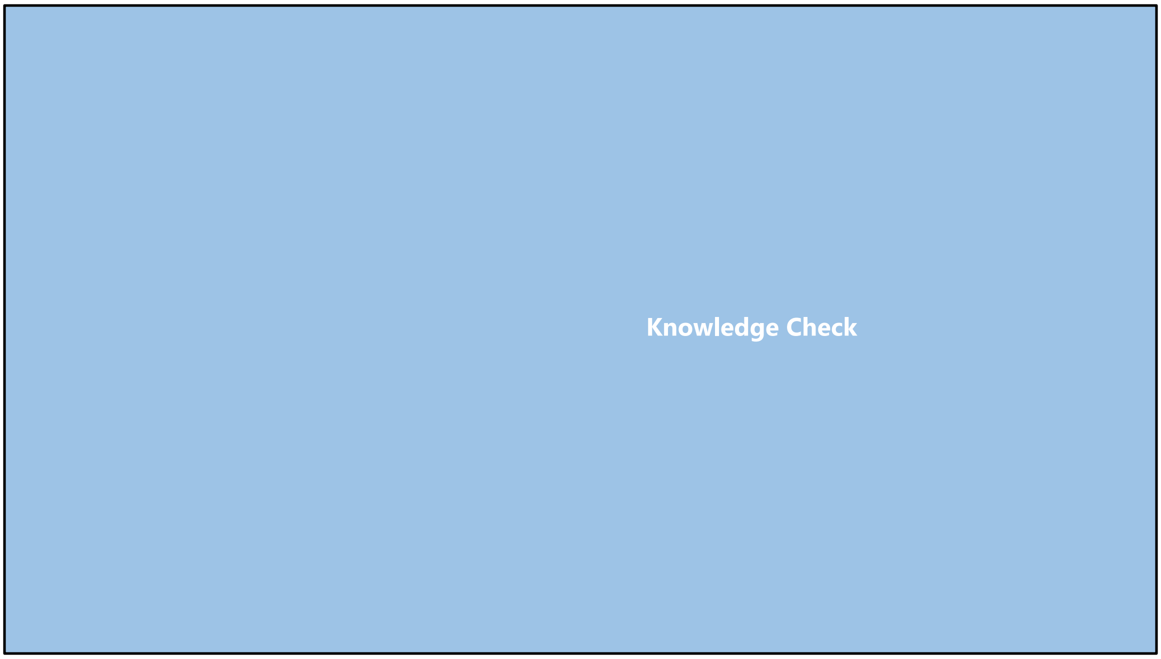
AWS defines a subnet as: A range of IP addresses in your VPC. You can launch AWS resources into a subnet that you select. A subnet is always mapped to a single Availability Zone. You can use a public subnet for resources that must be connected to the Internet and a private subnet for resources that won't 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.

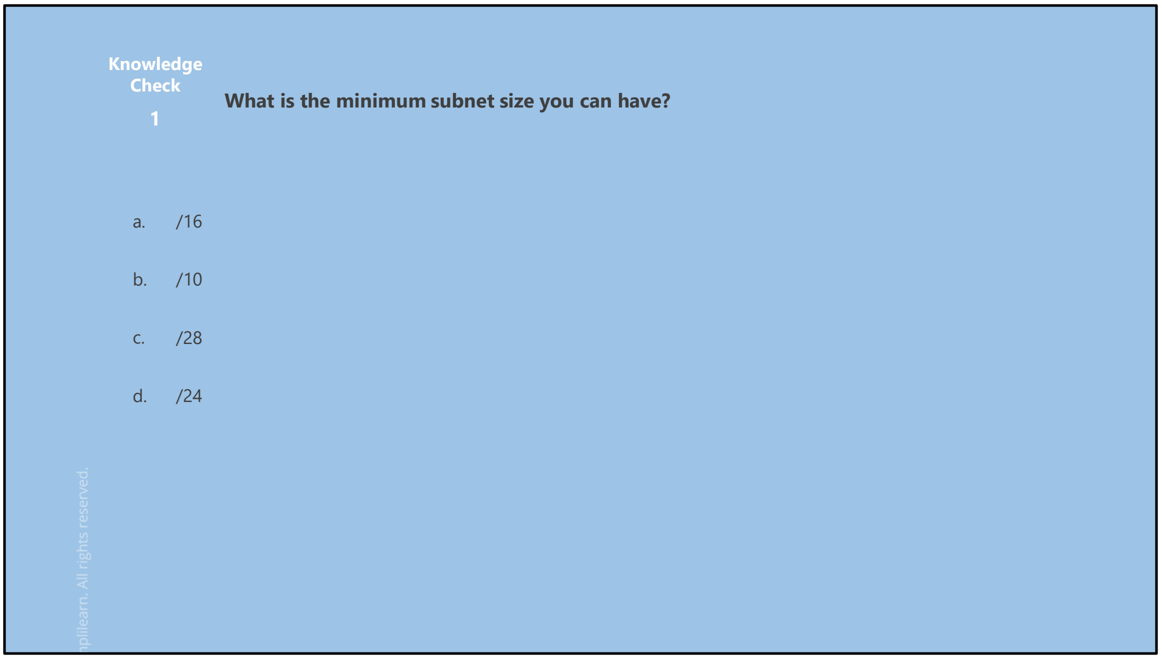


Knowledge Check

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.



Knowledge Check
1

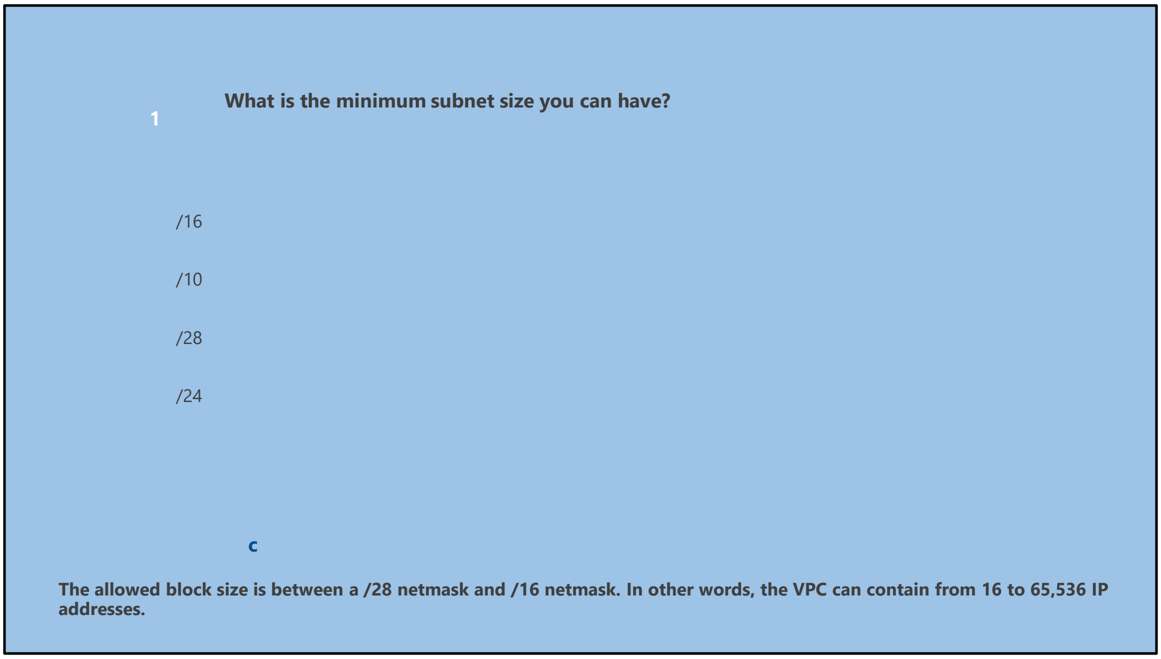
What is the minimum subnet size you can have?

a. /16

b. /10

c. /28

d. /24



1

What is the minimum subnet size you can have?

/16

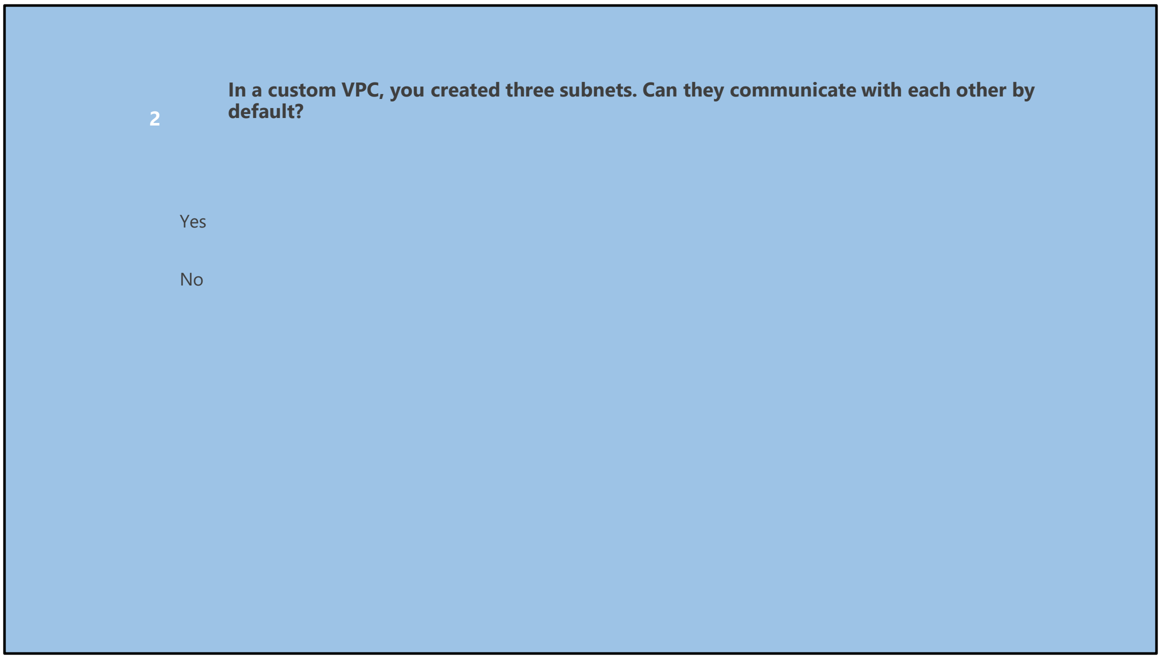
/10

/28

/24

c

The allowed block size is between a /28 netmask and /16 netmask. In other words, the VPC can contain from 16 to 65,536 IP addresses.

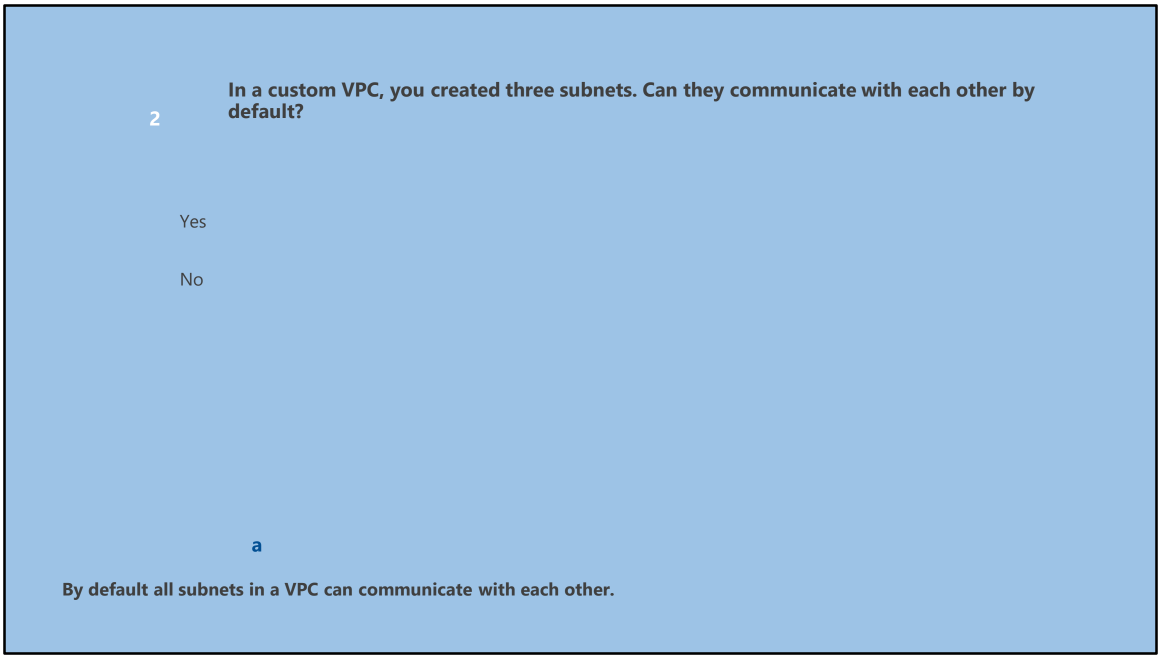


2

In a custom VPC, you created three subnets. Can they communicate with each other by default?

Yes

No



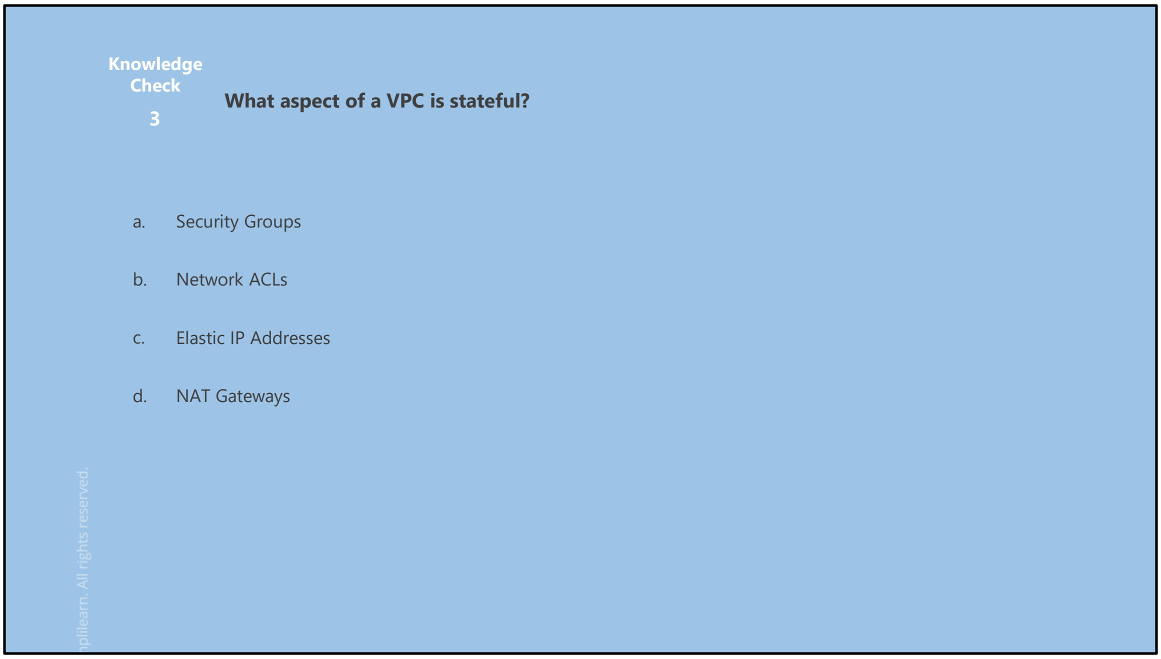
2 In a custom VPC, you created three subnets. Can they communicate with each other by default?

Yes

No

a

By default all subnets in a VPC can communicate with each other.



Knowledge Check 3

What aspect of a VPC is stateful?

a. Security Groups

b. Network ACLs

c. Elastic IP Addresses

d. NAT Gateways

3

What aspect of a VPC is stateful?

Security Groups

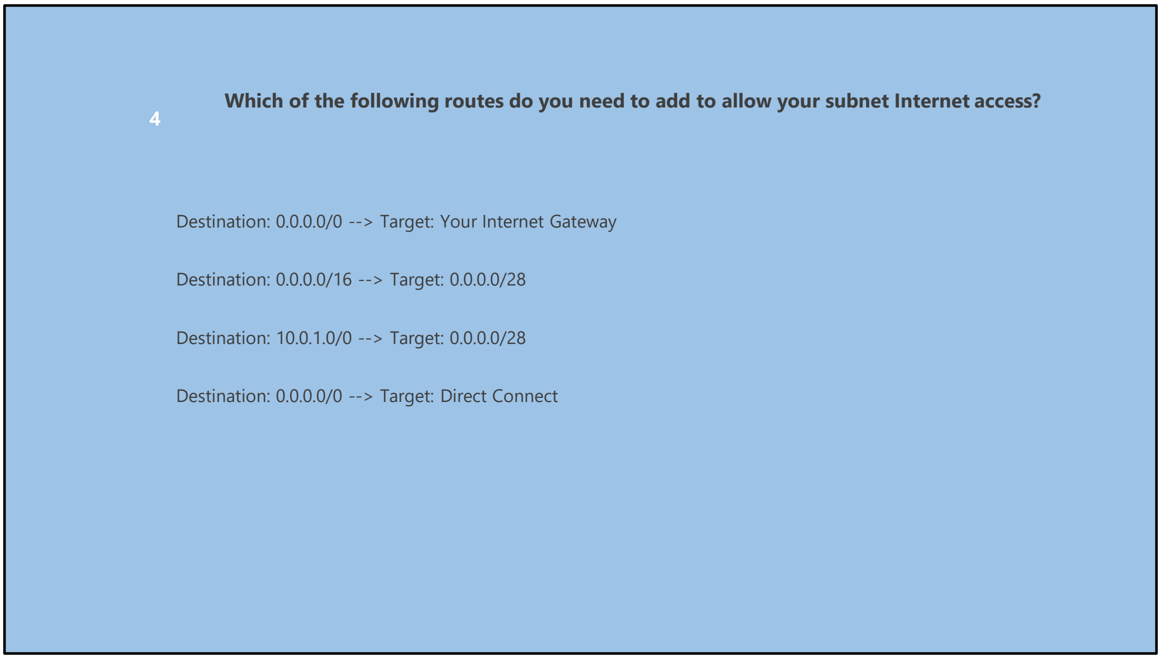
Network ACLs

Elastic IP Addresses

NAT Gateways

a

Security groups are stateful-if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules.



4

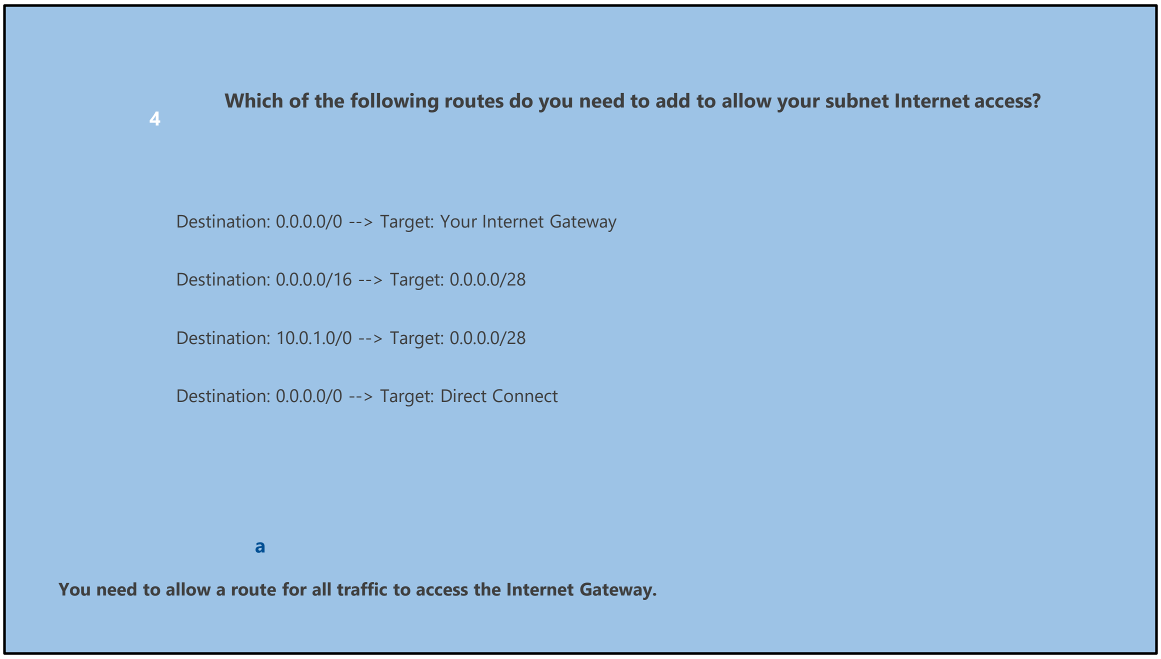
Which of the following routes do you need to add to allow your subnet Internet access?

Destination: 0.0.0.0/0 --> Target: Your Internet Gateway

Destination: 0.0.0.0/16 --> Target: 0.0.0.0/28

Destination: 10.0.1.0/0 --> Target: 0.0.0.0/28

Destination: 0.0.0.0/0 --> Target: Direct Connect



4

Which of the following routes do you need to add to allow your subnet Internet access?

Destination: 0.0.0.0/0 --> Target: Your Internet Gateway

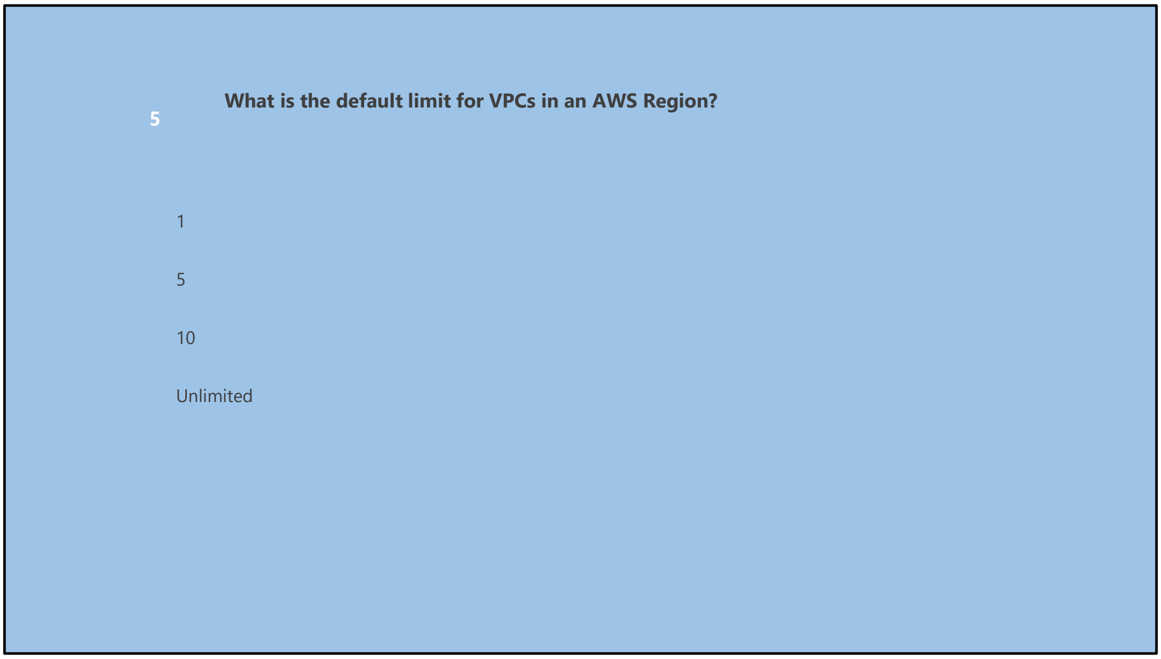
Destination: 0.0.0.0/16 --> Target: 0.0.0.0/28

Destination: 10.0.1.0/0 --> Target: 0.0.0.0/28

Destination: 0.0.0.0/0 --> Target: Direct Connect

a

You need to allow a route for all traffic to access the Internet Gateway.



5 What is the default limit for VPCs in an AWS Region?

1

5

10

Unlimited

5

What is the default limit for VPCs in an AWS Region?

1

5

10

Unlimited

b

By default you can have five VPCs per Region. If you need more, you need to raise a ticket with AWS Support to increase the limit.