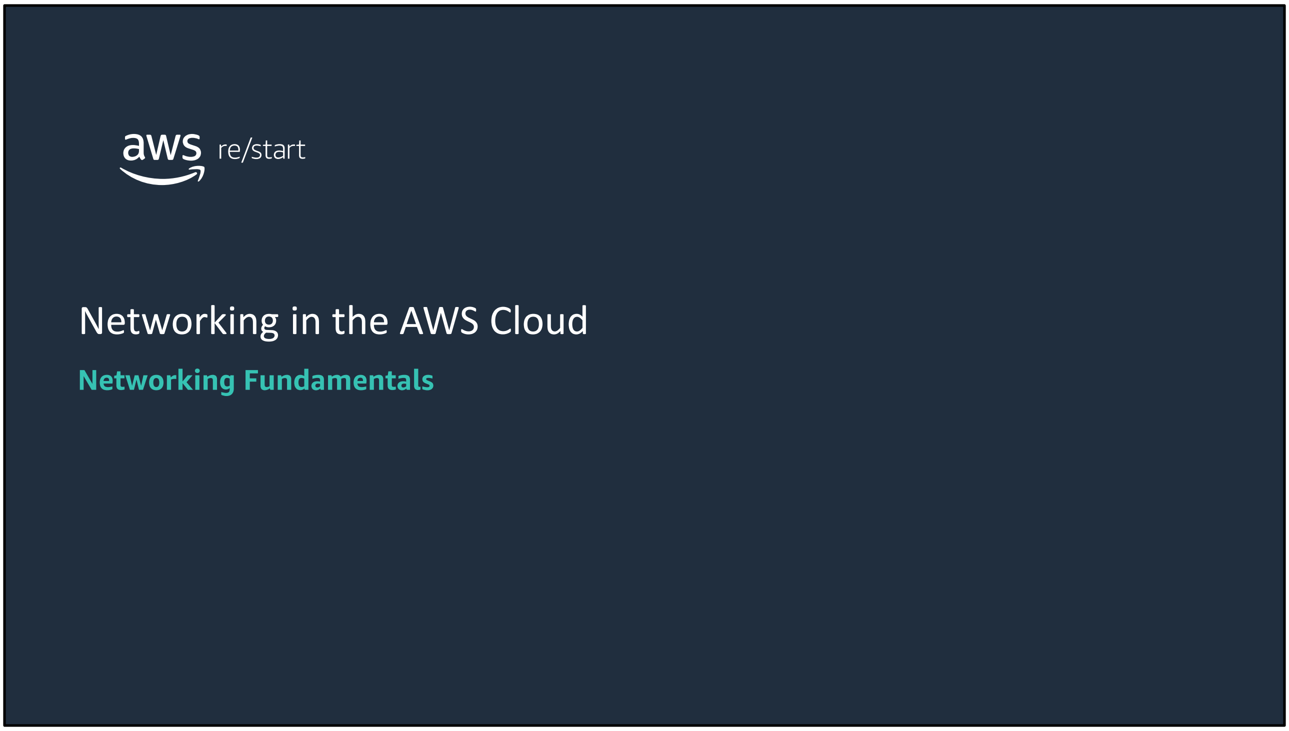
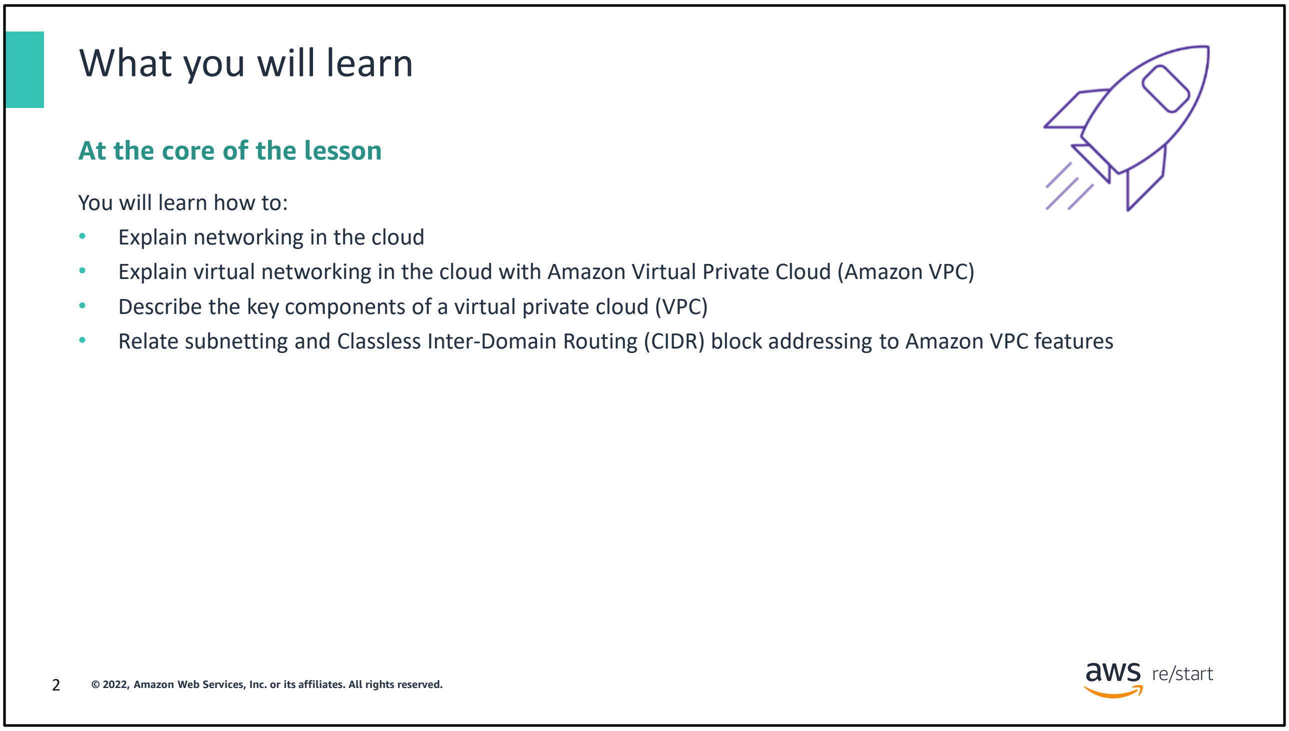


aws re/start

Networking in the AWS Cloud

Networking Fundamentals

Welcome to Networking in the AWS Cloud.



What you will learn

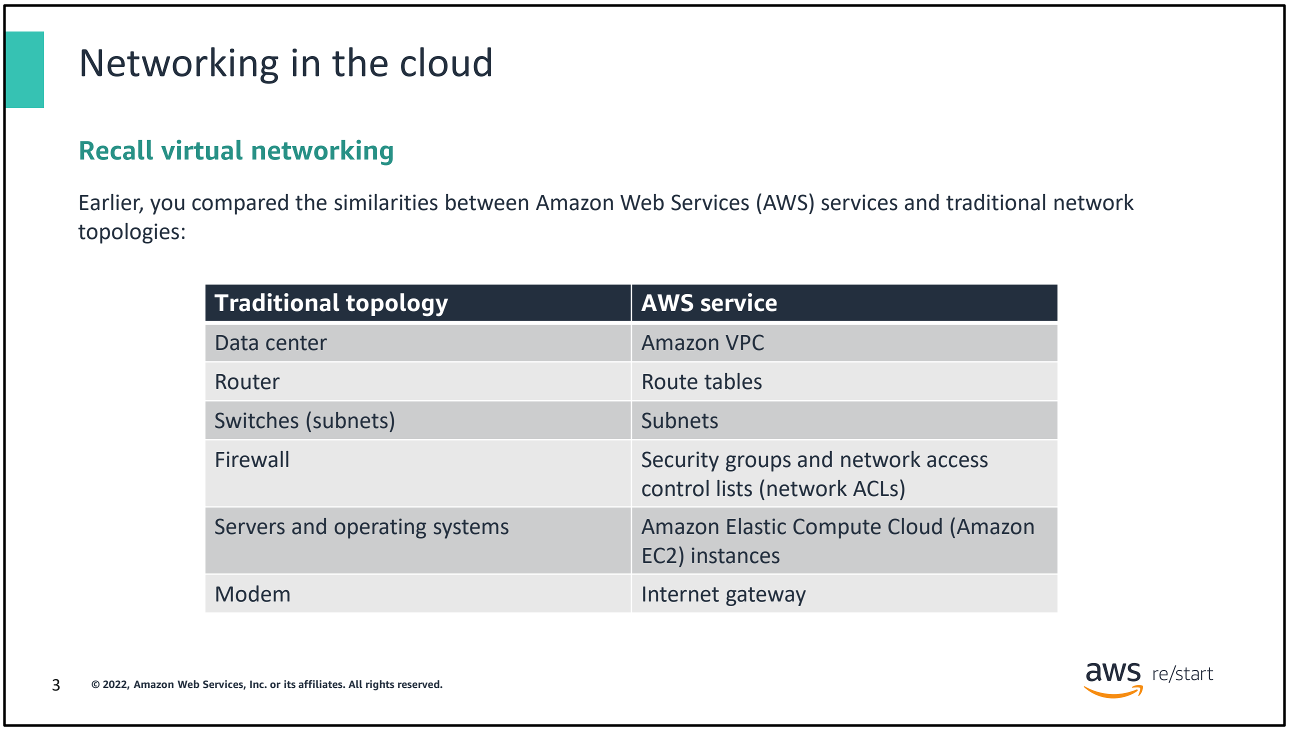
At the core of the lesson

You will learn how to:

- Explain networking in the cloud
- Explain virtual networking in the cloud with Amazon Virtual Private Cloud (Amazon VPC)
- Describe the key components of a virtual private cloud (VPC)
- Relate subnetting and Classless Inter-Domain Routing (CIDR) block addressing to Amazon VPC features

You will learn how to:

- Explain networking in the cloud
- Explain virtual networking in the cloud with Amazon Virtual Private Cloud (Amazon VPC)
- Describe the key components of a virtual private cloud (VPC)
- Relate subnetting and Classless Inter-Domain Routing (CIDR) block addressing to Amazon VPC features



Networking in the cloud

Recall virtual networking

Earlier, you compared the similarities between Amazon Web Services (AWS) services and traditional network topologies:

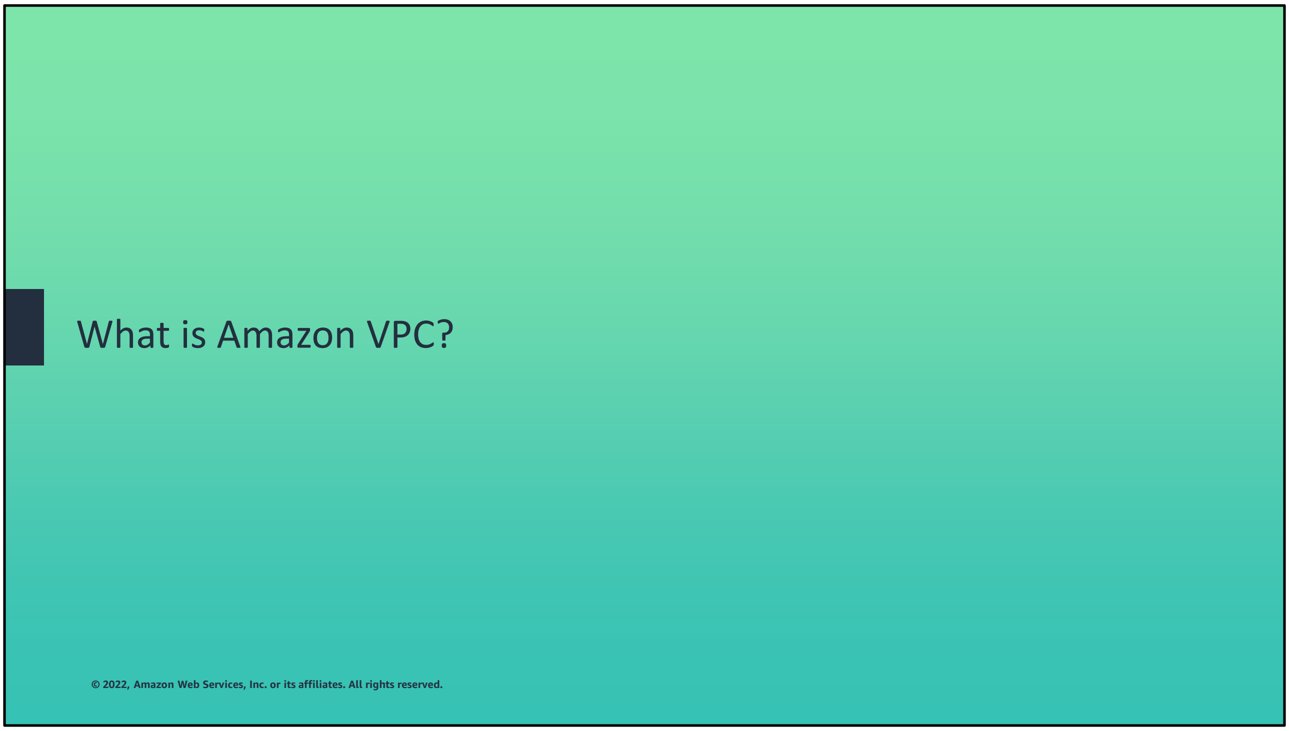
Traditional topology	AWS service
Data center	Amazon VPC
Router	Route tables
Switches (subnets)	Subnets
Firewall	Security groups and network access control lists (network ACLs)
Servers and operating systems	Amazon Elastic Compute Cloud (Amazon EC2) instances
Modem	Internet gateway

As described earlier, networking in the cloud is similar to regular networking in a data center:

- A data center as a whole most closely resembles the function of a VPC. In a VPC, you can launch multiple AWS services that are needed to create a working, scalable network. However, within a VPC, no maintenance is required, and you can create an isolated architecture within minutes.
- A data center involves multiple components: internet, servers, firewalls, switches, and more. Like a data center, a VPC requires the same services to operate.
- A router in a traditional environment has multiple functions, such as filtering packets, routing traffic, and storing them in a route table. In AWS, the service that most closely resembles a router is a route table, where the owner inputs routes within the VPC.
- A switch acts as a subnet and switches data as it comes in. AWS uses subnets in every architecture. Every node (EC2 instance) belongs in a subnet. Although the functions of a switch and an AWS subnet do not match, the functions of a subnet from both work the same architecturally. Subnets are used to logically isolate groups of internet protocols together.
- Firewalls block traffic based on a set of rules. AWS has security groups that block traffic at the node (Amazon EC2 level) and network ACLs that block traffic at the subnet level. These security groups also block traffic based on a set of rules.
- A data center has servers and operating systems. In AWS, you can use an EC2

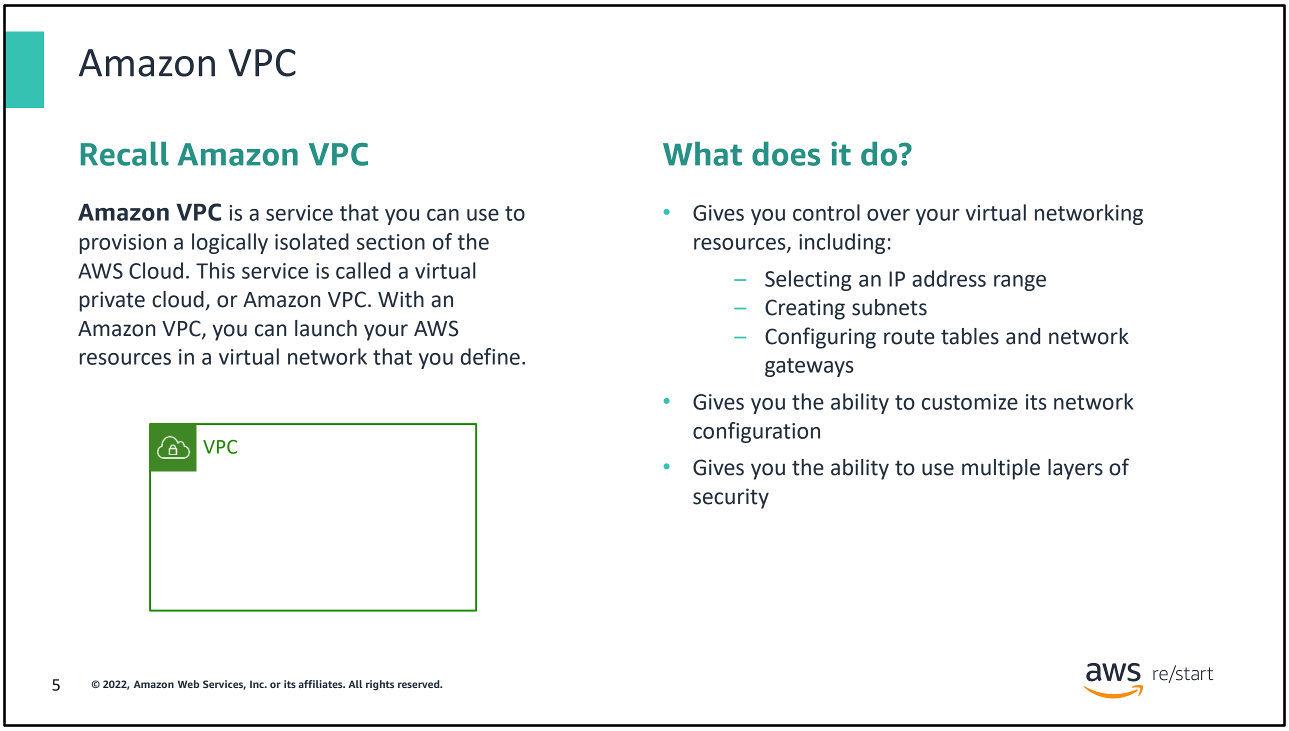
instance to launch an array of servers or operating systems.

- Everything must be connected to the internet through an internet service provider (ISP). One that you might be familiar with is called a modem, where an ISP provides internet to your home. Like a modem, a VPC on AWS and its services receive internet only through an internet gateway.



What is Amazon VPC?

In this section, you will learn what an Amazon VPC is.



Amazon VPC

Recall Amazon VPC

Amazon VPC is a service that you can use to provision a logically isolated section of the AWS Cloud. This service is called a virtual private cloud, or Amazon VPC. With an Amazon VPC, you can launch your AWS resources in a virtual network that you define.

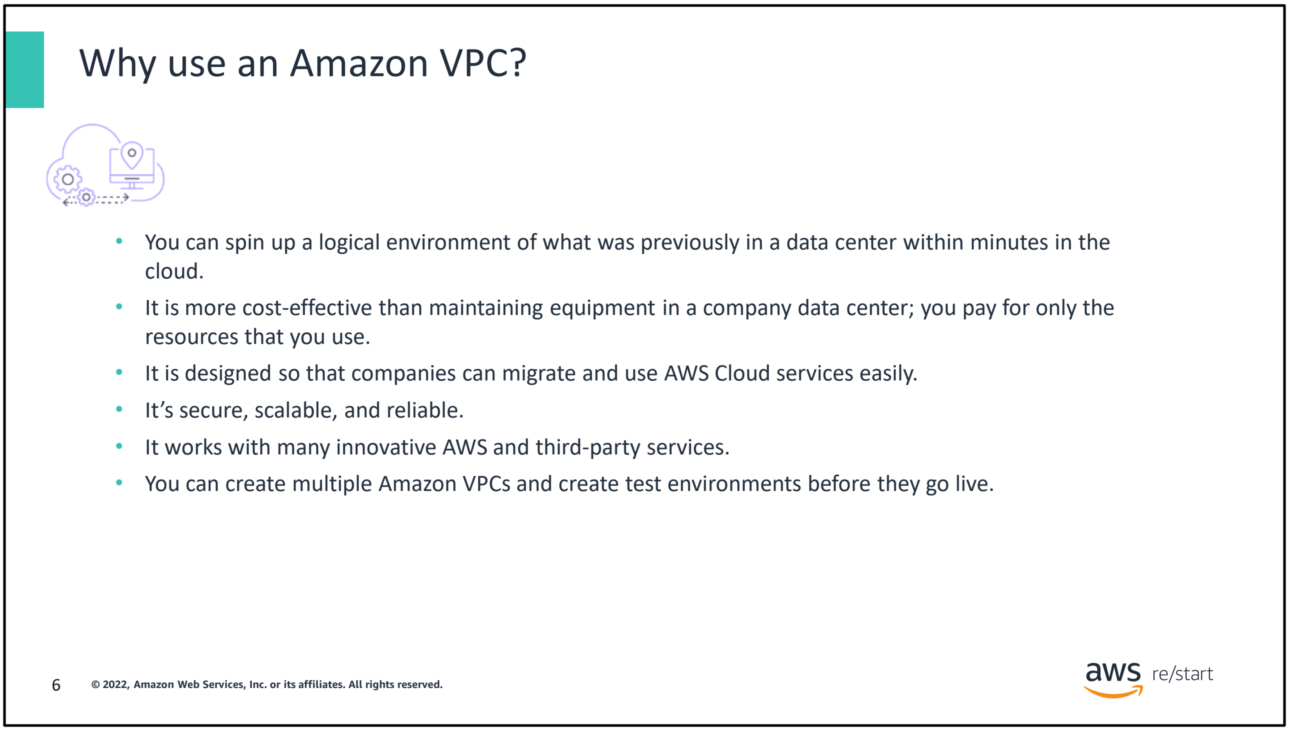
VPC

What does it do?

- Gives you control over your virtual networking resources, including:
  - Selecting an IP address range
  - Creating subnets
  - Configuring route tables and network gateways
- Gives you the ability to customize its network configuration
- Gives you the ability to use multiple layers of security

The Amazon VPC service offers the following benefits:

- You can use Amazon VPC to create a private network in the AWS Cloud that uses many of the same concepts and constructs as an on-premises network.
- Just like an on-premises network, you can select IP address ranges and allocate them by creating subnets.
- All of the physical components of an on-premises network have become virtual. Instead of plugging devices in, in a virtual environment like Amazon VPC, you would attach resources to make a network.
- You can create and provision a fully functional an Amazon VPC in your AWS account within minutes. It offers redundancy and high availability unlike traditional data centers. There are also fewer costs associated with operating within a cloud environment like AWS because there is no upkeep of a traditional data center.

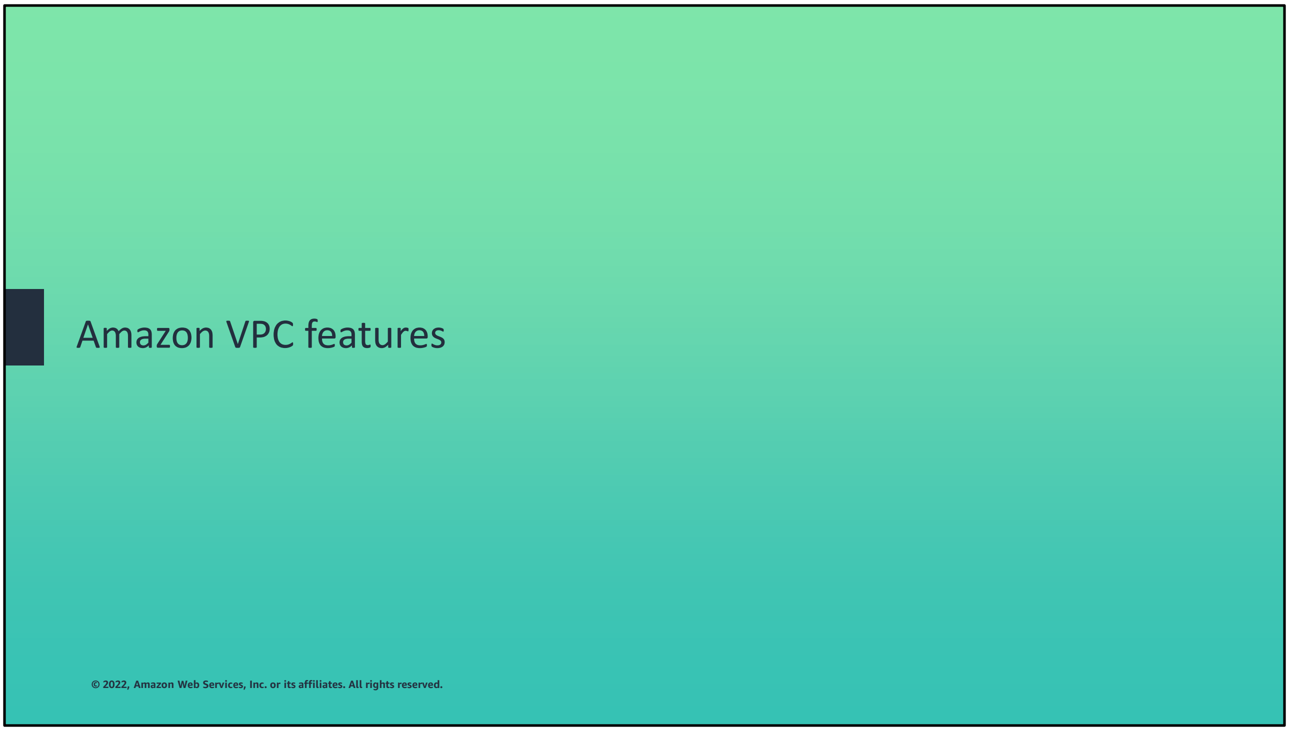


Why use an Amazon VPC?

- You can spin up a logical environment of what was previously in a data center within minutes in the cloud.
- It is more cost-effective than maintaining equipment in a company data center; you pay for only the resources that you use.
- It is designed so that companies can migrate and use AWS Cloud services easily.
- It's secure, scalable, and reliable.
- It works with many innovative AWS and third-party services.
- You can create multiple Amazon VPCs and create test environments before they go live.

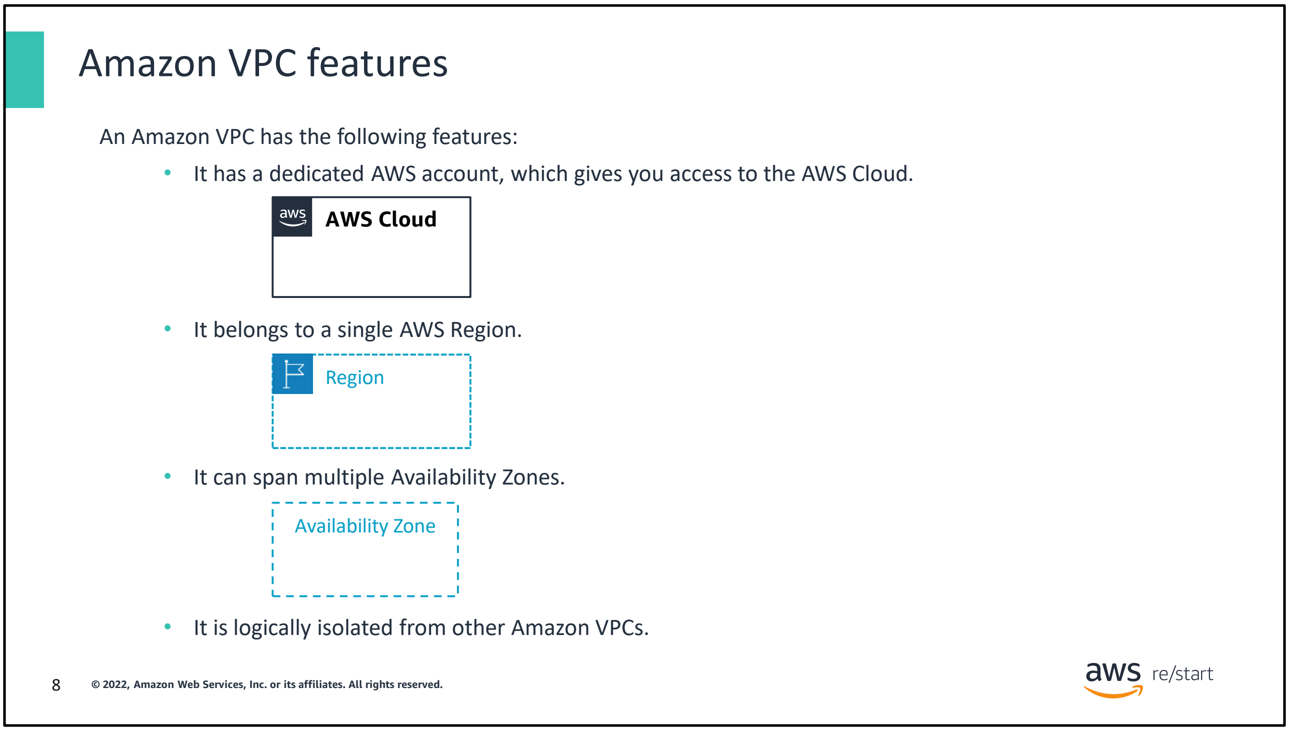
An Amazon VPC offers the following benefits:

- It is more secure, scalable, reliable, cost-effective, and easy to use than a traditional data center.
- It replaces the need for your own data center.
- You can create multiple Amazon VPCs for testing, owning customer accounts, and more.
- It works with many other services through AWS Marketplace (third-party software that is approved through AWS).
- Step-by-step guides are available on how to use an Amazon VPC; everything is well documented.



Amazon VPC features

In this section, you’ll learn about the features of an Amazon VPC.



Amazon VPC features

An Amazon VPC has the following features:

- It has a dedicated AWS account, which gives you access to the AWS Cloud.

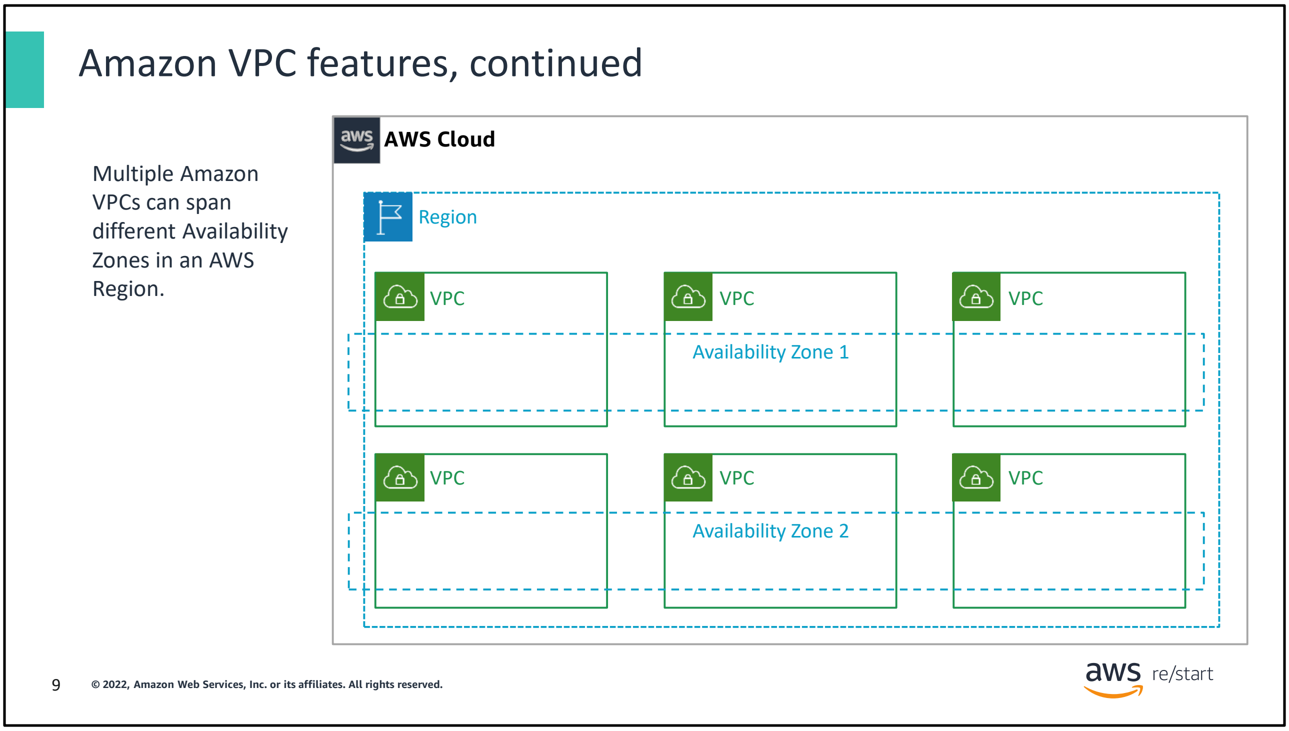
- It belongs to a single AWS Region.

- It can span multiple Availability Zones.

- It is logically isolated from other Amazon VPCs.

An Amazon VPC includes the following features:

- It is dedicated to an AWS account.
- It belongs to a single AWS Region.
- It can span multiple Availability Zones.
- It is logically isolated from other Amazon VPCs.

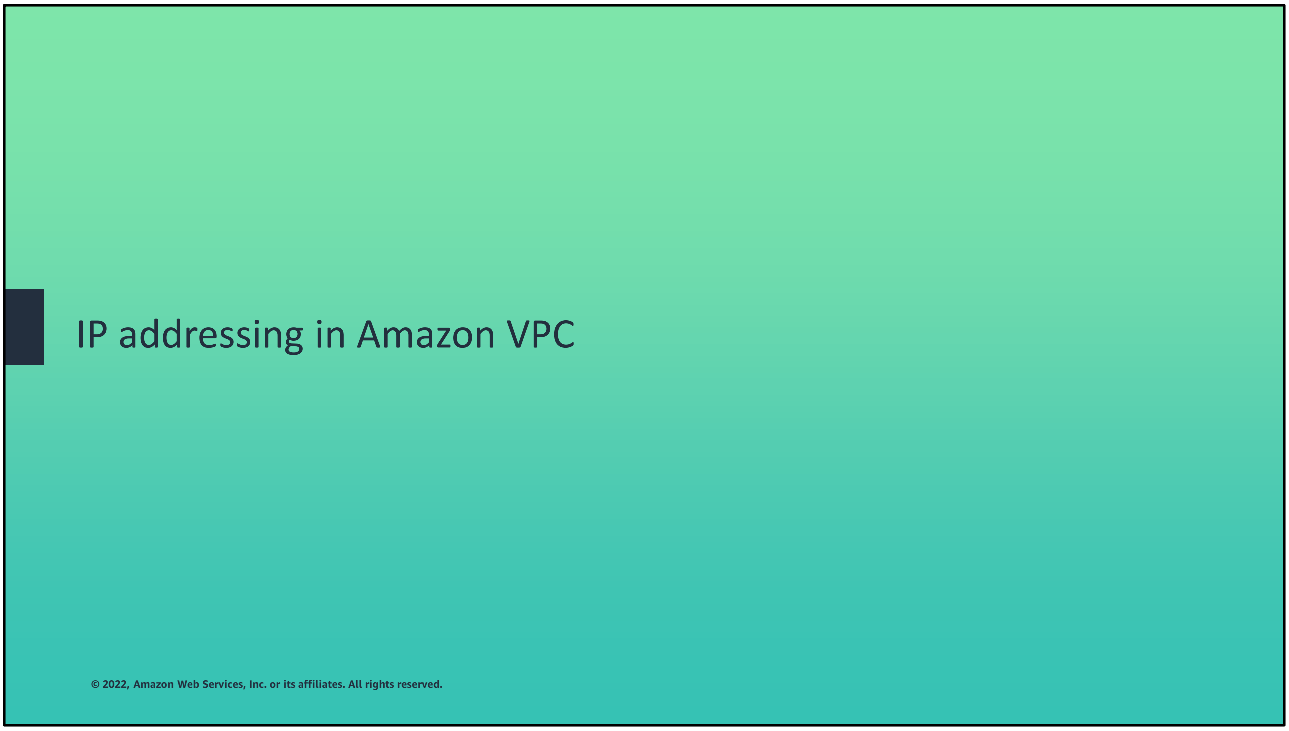


Amazon VPC features, continued

Multiple Amazon VPCs can span different Availability Zones in an AWS Region.

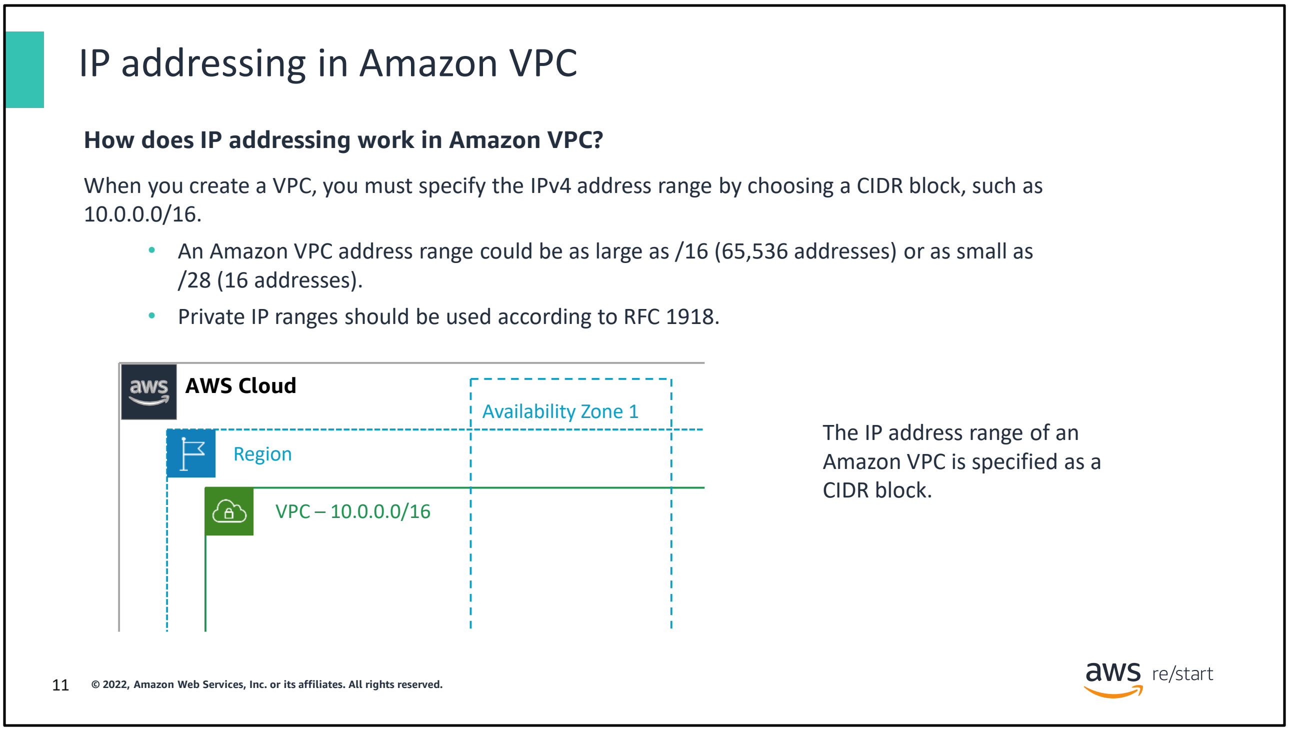
Amazon VPC features offer the following benefits:

- You can create multiple Amazon VPCs in an AWS account to separate networking environments.
- You can create subnets in a VPC; however, fewer subnets are recommended to reduce the complexity of the network topology.



IP addressing in Amazon VPC

In this section, you will learn how IP addressing works within the Amazon VPC.



IP addressing in Amazon VPC

How does IP addressing work in Amazon VPC?

When you create a VPC, you must specify the IPv4 address range by choosing a CIDR block, such as 10.0.0.0/16.

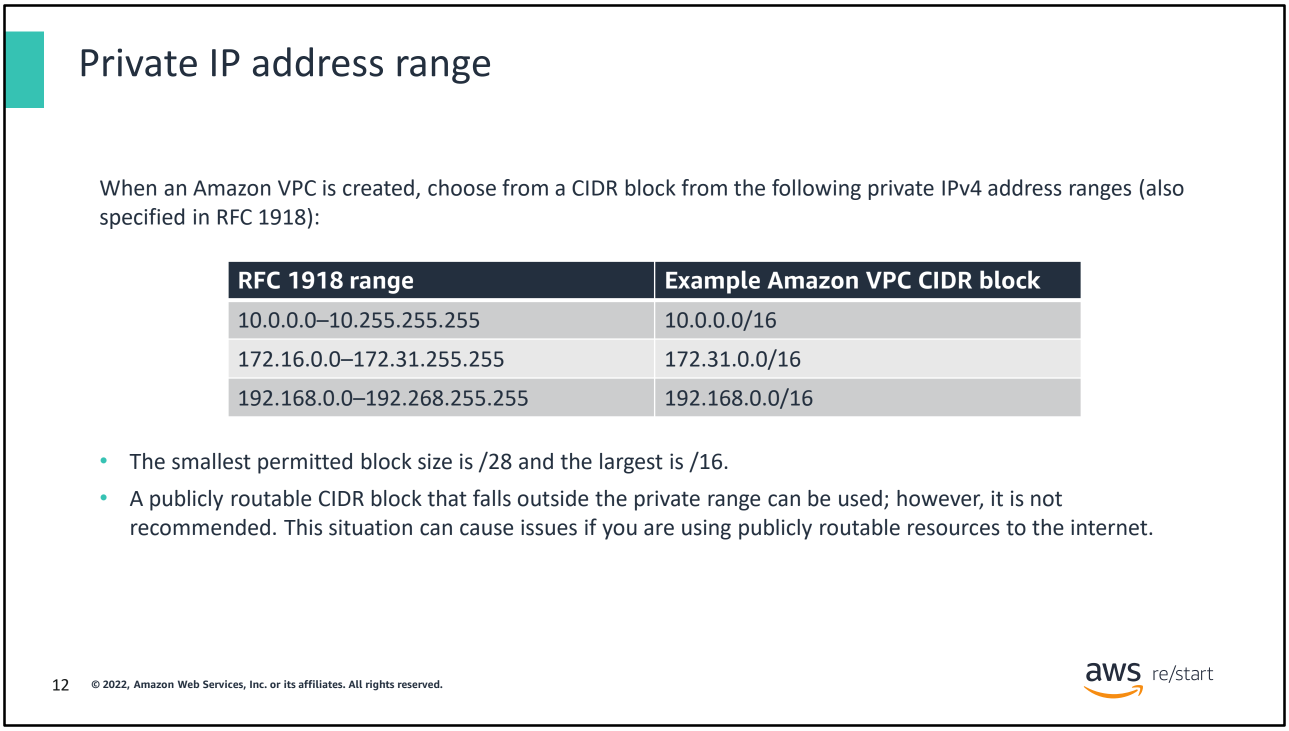
- An Amazon VPC address range could be as large as /16 (65,536 addresses) or as small as /28 (16 addresses).
- Private IP ranges should be used according to RFC 1918.

AWS Cloud
Availability Zone 1
Region
VPC – 10.0.0.0/16

The IP address range of an Amazon VPC is specified as a CIDR block.

IP addressing in Amazon VPC has the following rules:

- Private IP ranges should be used according to RFC 1918 (https://datatracker.ietf.org/doc/html/rfc1918). If private IP ranges are not used, resources within the VPC that have public IPs can get replies back from the internet that do not belong to the Amazon VPC.
- IP addresses should not overlap with the addresses of other networks to which an Amazon VPC is connected.
- The address range of the Amazon VPC cannot be changed after the VPC is created; however, a secondary VPC CIDR can be assigned to the VPC.



Private IP address range

When an Amazon VPC is created, choose from a CIDR block from the following private IPv4 address ranges (also specified in RFC 1918):

RFC 1918 range	Example Amazon VPC CIDR block
10.0.0.0–10.255.255.255	10.0.0.0/16
172.16.0.0–172.31.255.255	172.31.0.0/16
192.168.0.0–192.268.255.255	192.168.0.0/16

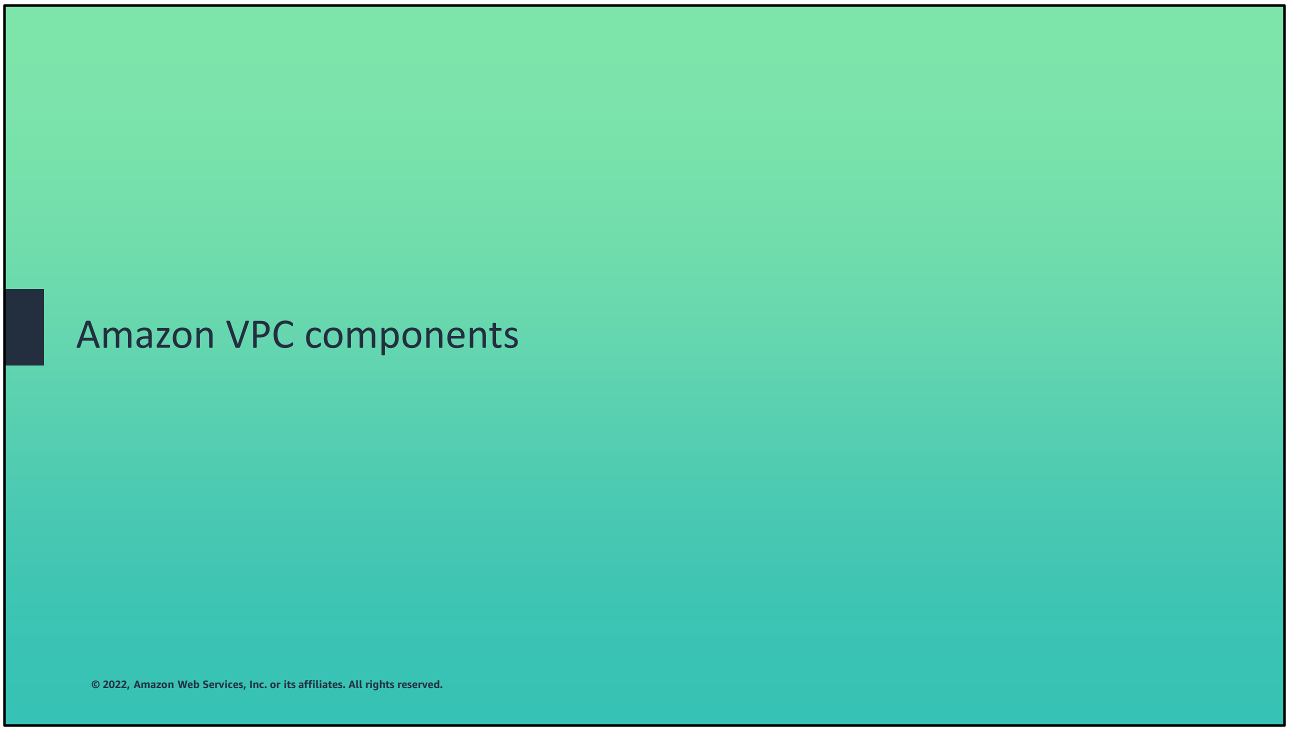
- The smallest permitted block size is /28 and the largest is /16.
- A publicly routable CIDR block that falls outside the private range can be used; however, it is not recommended. This situation can cause issues if you are using publicly routable resources to the internet.

Why is this information important?

- RFC 1918 (https://datatracker.ietf.org/doc/html/rfc1918) shows the private address space and its use case (within enterprise use). However, when the public IP address is enabled or an Elastic IP address is assigned, it gives a public IP address to the instance. This public IP address allows it to be routable on the internet regardless of the private address. This address is unique and is from the Amazon pool of IP addresses.
- It is recommended that you use the private IPv4 address range.
- When using anything outside the IPv4 address range, you run into the possibility of receiving replies from other resources that are not your own resources. These replies might be from other random sources on the internet.
- Some third-party tools can assist in calculating and creating IPv4 subnet and CIDR blocks. Try searching for “subnet calculator” or “CIDR calculator.”
- Within each subnet CIDR block, AWS reserves the first four IP addresses and the last IP address :
    - 10.0.0.0 – Network address
    - 10.0.0.1 – VPC router
    - 10.0.0.2 – Domain Name System (DNS) server
    - 10.0.0.3 – Reserved for future use
    - 10.0.0.255 – Network broadcast, not supported in the VPC, but still reserved

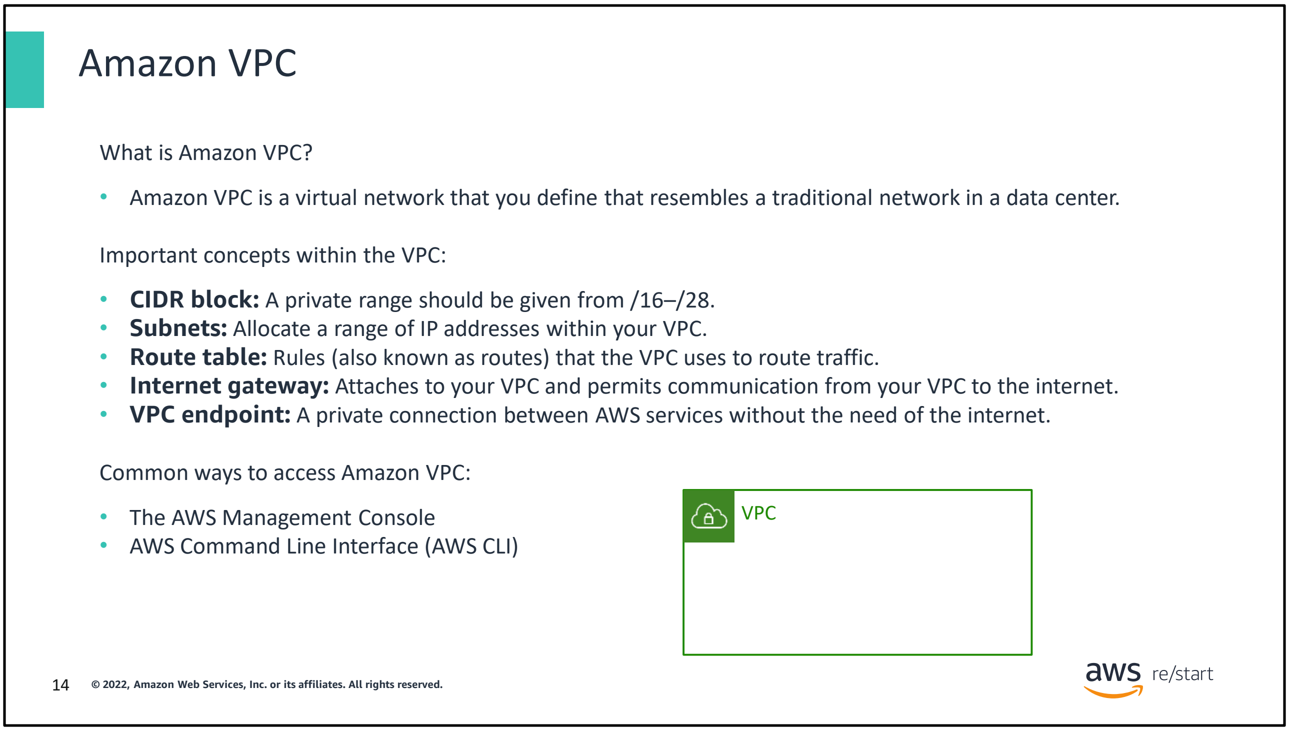
- You can always add a secondary CIDR block to an Amazon VPC.

For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html#vpc-sizing-ipv4.



Amazon VPC components

In this section, you will learn about the components of an Amazon VPC.



Amazon VPC

What is Amazon VPC?

- Amazon VPC is a virtual network that you define that resembles a traditional network in a data center.

Important concepts within the VPC:

- **CIDR block:** A private range should be given from /16–/28.
- **Subnets:** Allocate a range of IP addresses within your VPC.
- **Route table:** Rules (also known as routes) that the VPC uses to route traffic.
- **Internet gateway:** Attaches to your VPC and permits communication from your VPC to the internet.
- **VPC endpoint:** A private connection between AWS services without the need of the internet.

Common ways to access Amazon VPC:

- The AWS Management Console
- AWS Command Line Interface (AWS CLI)

What is Amazon VPC?

- It is a virtual network that you define that resembles a traditional network in a data center.
- For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.

The following concepts are important within the VPC:

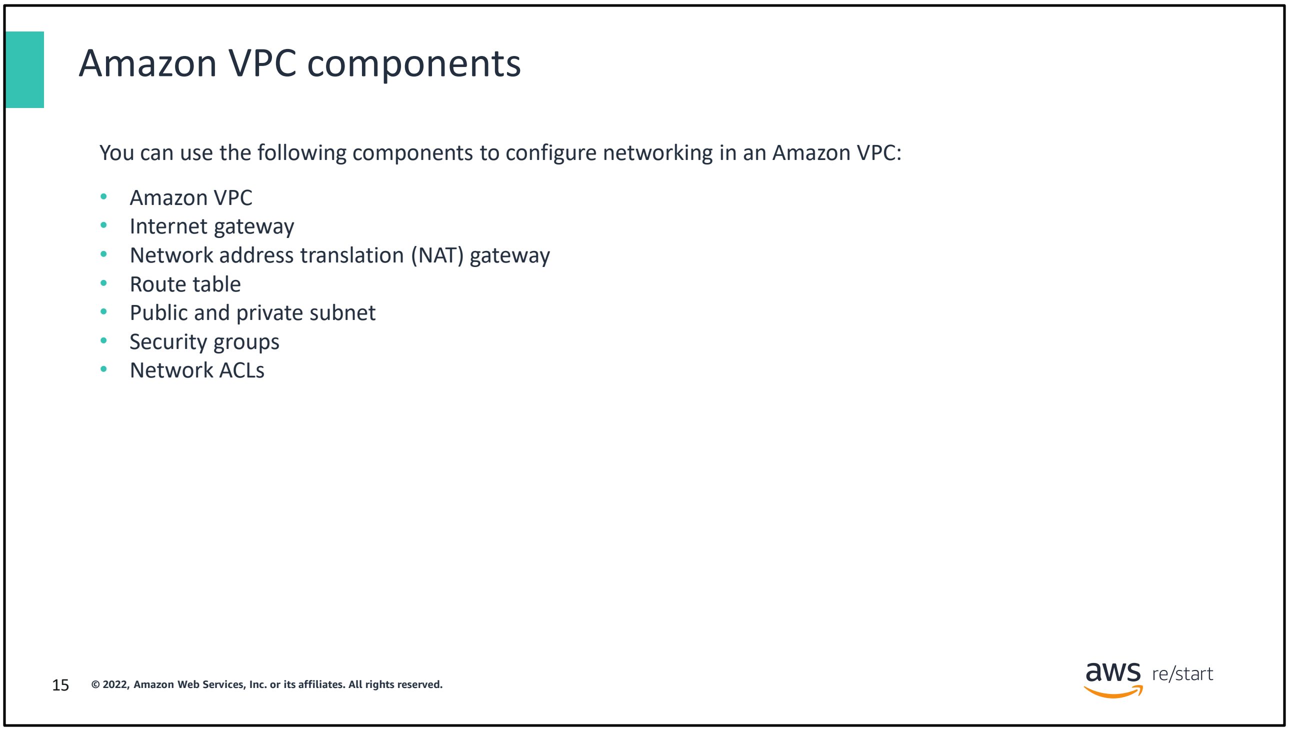
- **CIDR block:** A private range should be given in the range /16–/28. To determine the private IP address range allocation, you can use RFC 1918: https://datatracker.ietf.org/doc/html/rfc1918. To determine the CIDR block and range, various third-party tools are available to determine how many IP addresses can fit into each CIDR range.
- **Subnets:** Subnets allocate a range of IP addresses within your VPC. These subnets are either public or private subnets. Public subnets have the route table with the internet gateway associated with them, but the private subnets do not. Like the VPC CIDR block, subnets need a range. A third-party tool can also be used.
- **Route table:** A route table contains rules (also known as routes) that the VPC uses to route traffic. Targets are services like the internet gateway, VPC endpoint, or NAT gateway. The routes are the specific routes that go to the specific targets.

For example, for the internet gateway (internet gateway), the route will be 0.0.0.0/0 because it is routing to the internet, and the target will be IGW-xxxxxxxx.

- **Internet gateway: An internet gateway a**ttaches to your VPC and allows communication from VPC to internet. This service must be created and attached to the VPC. After it is attached, it must be added to the route table of the public subnet in order for resources to reach the internet.
- **VPC endpoint:** A VPC endpoint is a private connection between AWS services without the need of the internet.

Common ways to access Amazon VPC include:

- AWS Management Console
- AWS Command Line Interface (CLI)



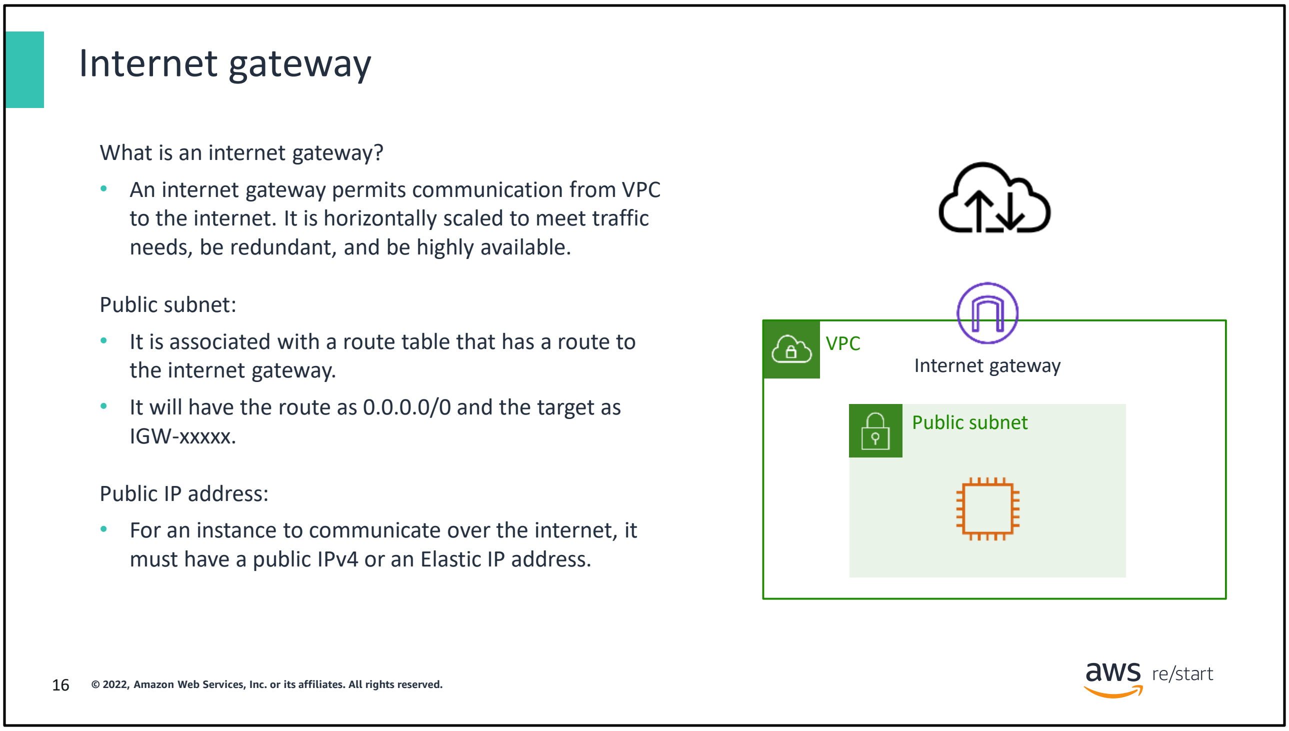
Amazon VPC components

You can use the following components to configure networking in an Amazon VPC:

- Amazon VPC
- Internet gateway
- Network address translation (NAT) gateway
- Route table
- Public and private subnet
- Security groups
- Network ACLs

Amazon VPC components are used to configure networking in a VPC:

- An Amazon VPC is a logically isolated environment for your resources within the cloud. You can choose a Region here.
- The internet gateway gives the Amazon VPC internet connectivity.
- The network address translation (NAT) gateway is attached to the private subnet. It provides network address translation so that the private subnet can reach out to the internet.
- A route table holds the route and target information required to route traffic within the Amazon VPC.
- A public subnet is associated with a route table that has a route to an internet gateway. You can choose Availability Zones here.
- A private subnet does not have an internet gateway on the route table that is associated to it. However, a NAT gateway can be a route on this route table. Like public subnets, Availability Zones can be chosen here.
- Security groups are like firewalls at an EC2 instance level. They are stateful by nature.
- Network ACLs are like firewalls for subnets. They are stateless by nature.



Internet gateway

What is an internet gateway?

- An internet gateway permits communication from VPC to the internet. It is horizontally scaled to meet traffic needs, be redundant, and be highly available.

Public subnet:

- It is associated with a route table that has a route to the internet gateway.
- It will have the route as 0.0.0.0/0 and the target as IGW-xxxxx.

Public IP address:

- For an instance to communicate over the internet, it must have a public IPv4 or an Elastic IP address.

16

aws re/start

How do you enable internet access within the console?

1. Create the internet gateway, and attach it to the VPC.
2. Identify the route table that is associated to the subnet that you want your resources to use to communicate with the internet. Add the route of 0.0.0.0/0 and target of the internet gateway to this route table.
3. Ensure that the resources in the now public subnet have a public IP address or an Elastic IP address.
4. Ensure that security groups around the instances and the network ACLs around the subnets allow traffic to and from the instance and subnet.

Why is this information important?

When troubleshooting, forgetting any of these steps can break internet or network connectivity. Checking the attachment, routes, public IP addresses, and security settings is very important when setting up, maintaining, or testing network configurations within the VPC.

What is an internet gateway?

- It allows communication from VPC to the internet. It is horizontally scaled to meet traffic needs, be redundant, and be highly available.

- Without an internet gateway, you will not be able to reach the internet.

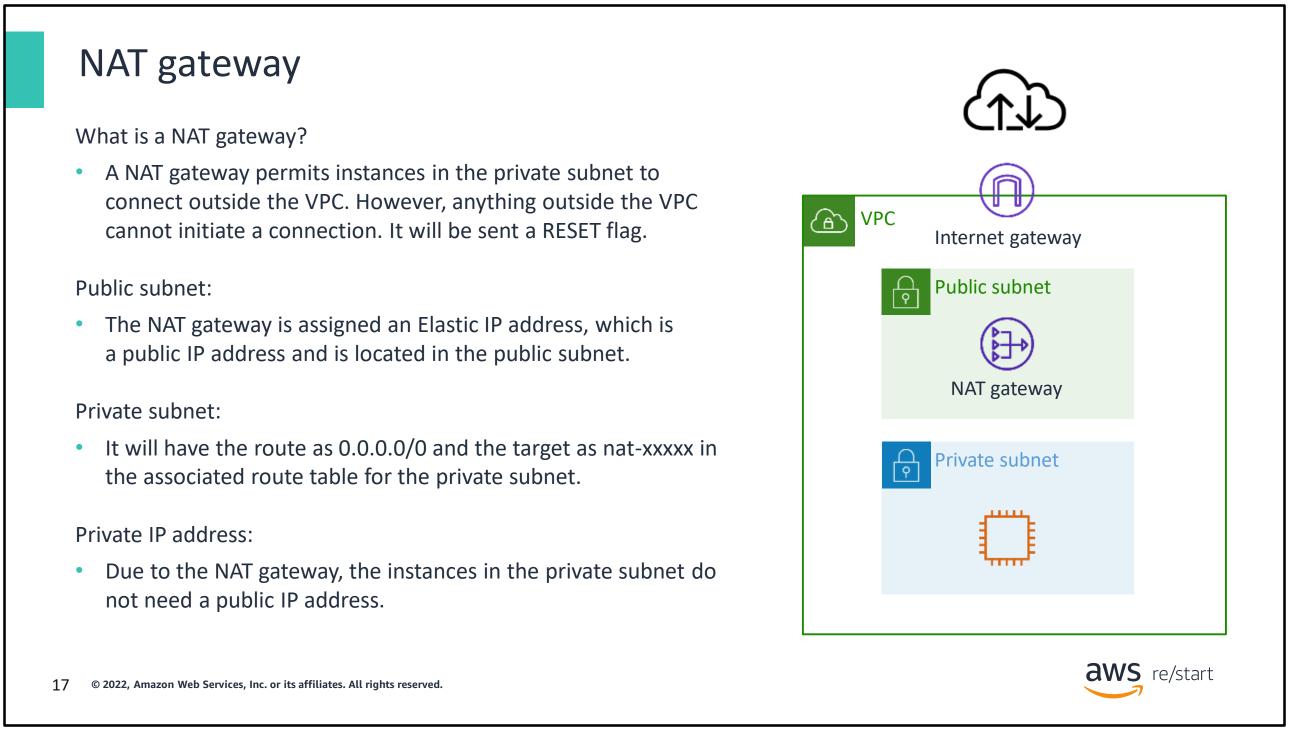
Public subnet:

- A public subnet is associated with a route table that has a route to the internet gateway.
- It will have the route as 0.0.0.0/0 and the target as IGW-xxxxx.

IP address:

- For an instance to communicate over the internet, it must have a public IPv4 (Elastic IP or dynamic) address.

For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html.



NAT gateway

What is a NAT gateway?

- A NAT gateway permits instances in the private subnet to connect outside the VPC. However, anything outside the VPC cannot initiate a connection. It will be sent a RESET flag.

Public subnet:

- The NAT gateway is assigned an Elastic IP address, which is a public IP address and is located in the public subnet.

Private subnet:

- It will have the route as 0.0.0.0/0 and the target as nat-xxxxx in the associated route table for the private subnet.

Private IP address:

- Due to the NAT gateway, the instances in the private subnet do not need a public IP address.

aws re/start

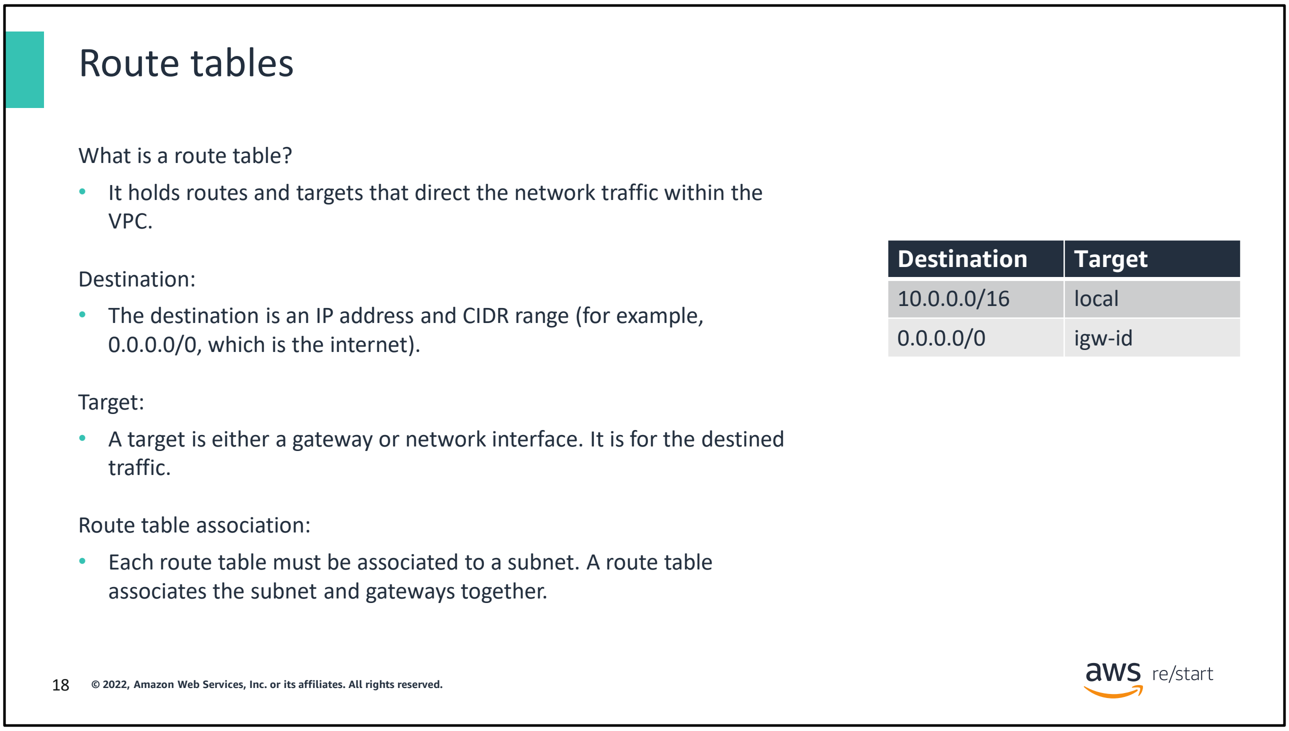
How do you provide internet access to the private subnet?

1. Create the NAT gateway, and select the public subnet in which to place the NAT gateway.
2. The two connectivity types are public and private. Public is for instances within the private subnet to connect to resources outside the VPC, and private is to connect only within the VPC.
3. If the type is public, allocate an Elastic IP address.
4. Identify the route table that is associated to the private subnet that you want your resources to use to communicate with the internet. Add the route of 0.0.0.0/0 and target of the NAT gateway to this route table.
5. Ensure that security groups around the instances and the network ACLs around the subnets allow traffic to and from the instance and subnet.

Why is this information important?

When troubleshooting, forgetting any of these steps can break internet or network connectivity. Checking NAT gateway placement, routes, correct Elastic IP addresses, and security settings is important when setting up, maintaining, or testing network configurations within the VPC.

For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html.



Route tables

What is a route table?

- It holds routes and targets that direct the network traffic within the VPC.

Destination:

- The destination is an IP address and CIDR range (for example, 0.0.0.0/0, which is the internet).

Target:

- A target is either a gateway or network interface. It is for the destined traffic.

Route table association:

- Each route table must be associated to a subnet. A route table associates the subnet and gateways together.

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

Important things to keep in mind when working with route tables in the AWS console:

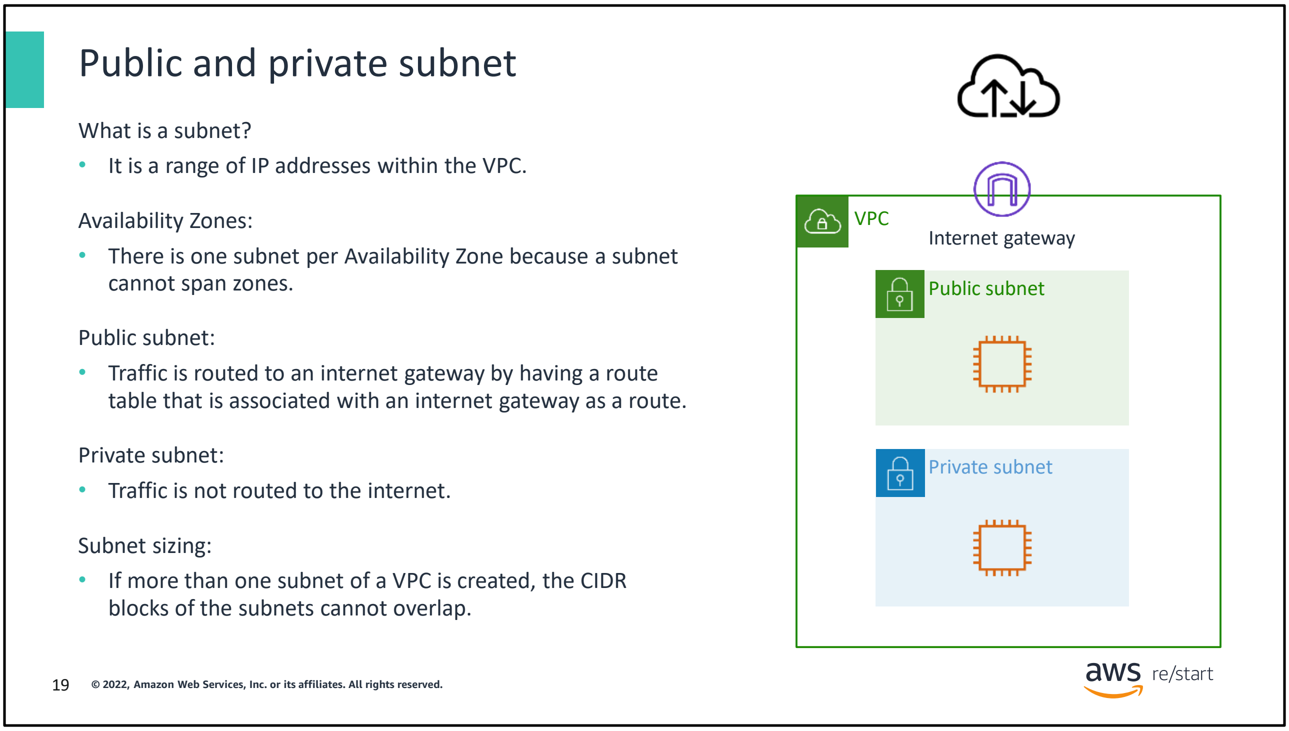
- Associating public route tables to public subnets and naming them the same can assist in organizing when attaching and associating services.
- There are destinations and targets. Destinations hold IP addresses and ranges, and targets hold a service.
- A route table with an internet gateway in it is associated with a subnet that needs internet access and can be accessed by the internet. It will then be called the public subnet.

Why is this information important?

When troubleshooting, forgetting any of these steps can break internet or network connectivity. Checking the correct association to the correct subnets, destination, and targets is crucial to routing within and outside the VPC.

A subnet can be associated with only one route table; however, route tables can be associated to multiple subnets.

For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html.



Public and private subnet

What is a subnet?

- It is a range of IP addresses within the VPC.

Availability Zones:

- There is one subnet per Availability Zone because a subnet cannot span zones.

Public subnet:

- Traffic is routed to an internet gateway by having a route table that is associated with an internet gateway as a route.

Private subnet:

- Traffic is not routed to the internet.

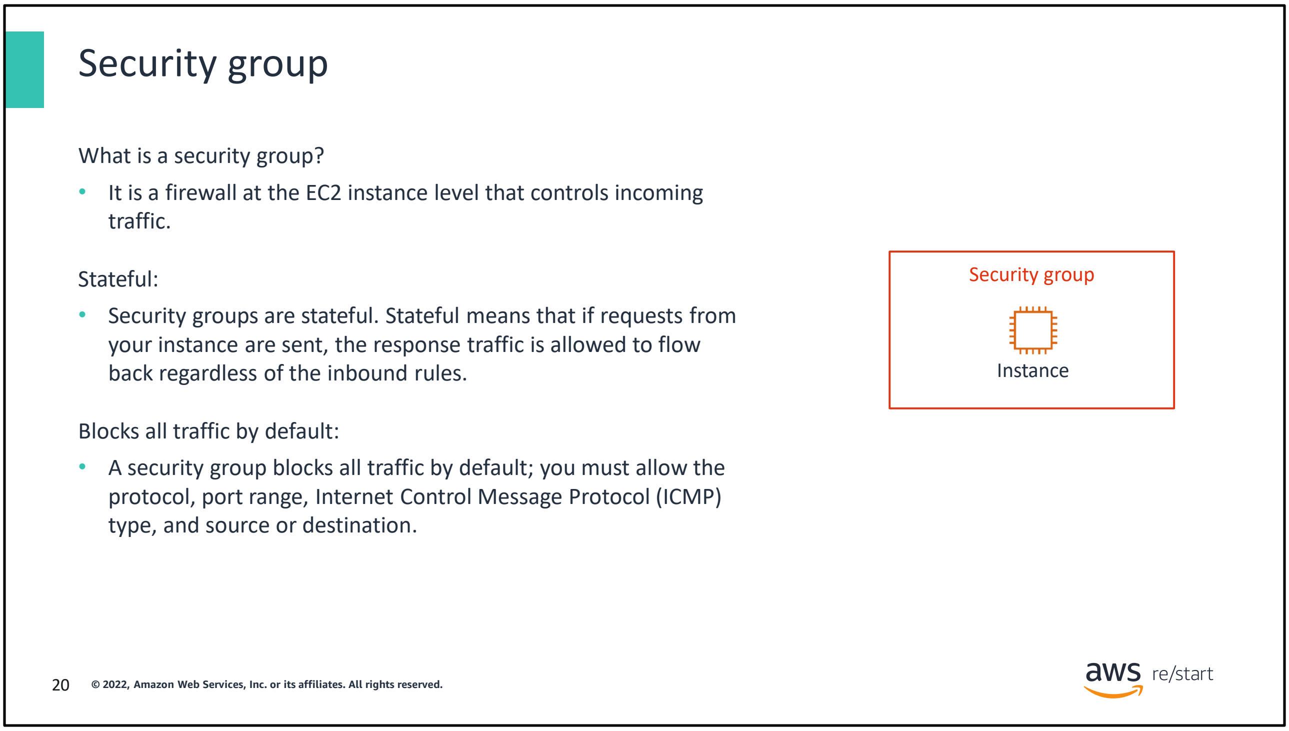
Subnet sizing:

- If more than one subnet of a VPC is created, the CIDR blocks of the subnets cannot overlap.

The following list contains significant information about subnets:

- Each subnet has one Availability Zone.
- A public subnet has an internet gateway and is accessible from the internet and within the VPC.
- A private subnet does not have any traffic routed directly to an internet gateway. However, it can have traffic routed to the NAT gateway from the private subnet. Without a NAT gateway, only VPC traffic is accessible, but with a NAT gateway, a private subnet is able to get updates from the internet.
- AWS reserves the first four IP addresses and the last IP address of every subnet for internal purposes.

For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html#subnet-basics.



Security group

What is a security group?

- It is a firewall at the EC2 instance level that controls incoming traffic.

Stateful:

- Security groups are stateful. Stateful means that if requests from your instance are sent, the response traffic is allowed to flow back regardless of the inbound rules.

Blocks all traffic by default:

- A security group blocks all traffic by default; you must allow the protocol, port range, Internet Control Message Protocol (ICMP) type, and source or destination.

Creating a security group requires specific items:

1. Protocol: You can choose either Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP).
2. Port range: For example, you can choose port 22 to use Secure Shell (SSH) or a range of (0–65,555).
3. ICMP type and code: You can keep the default here.
4. Source or destination: This option can be a specific IP address, a range of IP address, or anywhere (0.0.0.0/0).

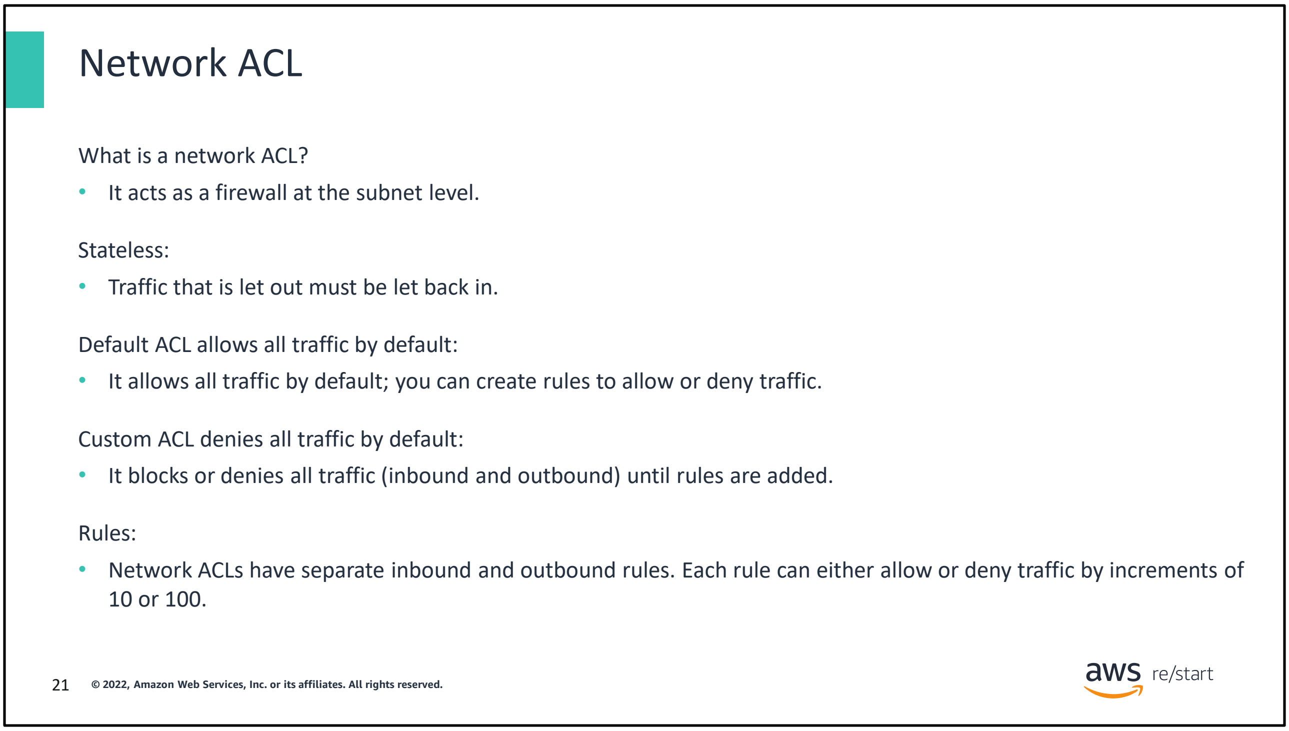
Why is this information important?

When you are troubleshooting, security groups can often be a huge issue. They frequently block ports or certain IP addresses that are easy to miss when you are configuring the networking aspects of the VPC. When everything might seem correct but something is showing as “connection refused,” it’s usually a security group issue.

You can associate multiple security groups to an instance.

You can change these rules at any time, but be mindful of each change because unexpected consequences can occur. Detailing each stage before a change can save a lot of time.

For more information, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html.



Network ACL

What is a network ACL?

- It acts as a firewall at the subnet level.

Stateless:

- Traffic that is let out must be let back in.

Default ACL allows all traffic by default:

- It allows all traffic by default; you can create rules to allow or deny traffic.

Custom ACL denies all traffic by default:

- It blocks or denies all traffic (inbound and outbound) until rules are added.

Rules:

- Network ACLs have separate inbound and outbound rules. Each rule can either allow or deny traffic by increments of 10 or 100.

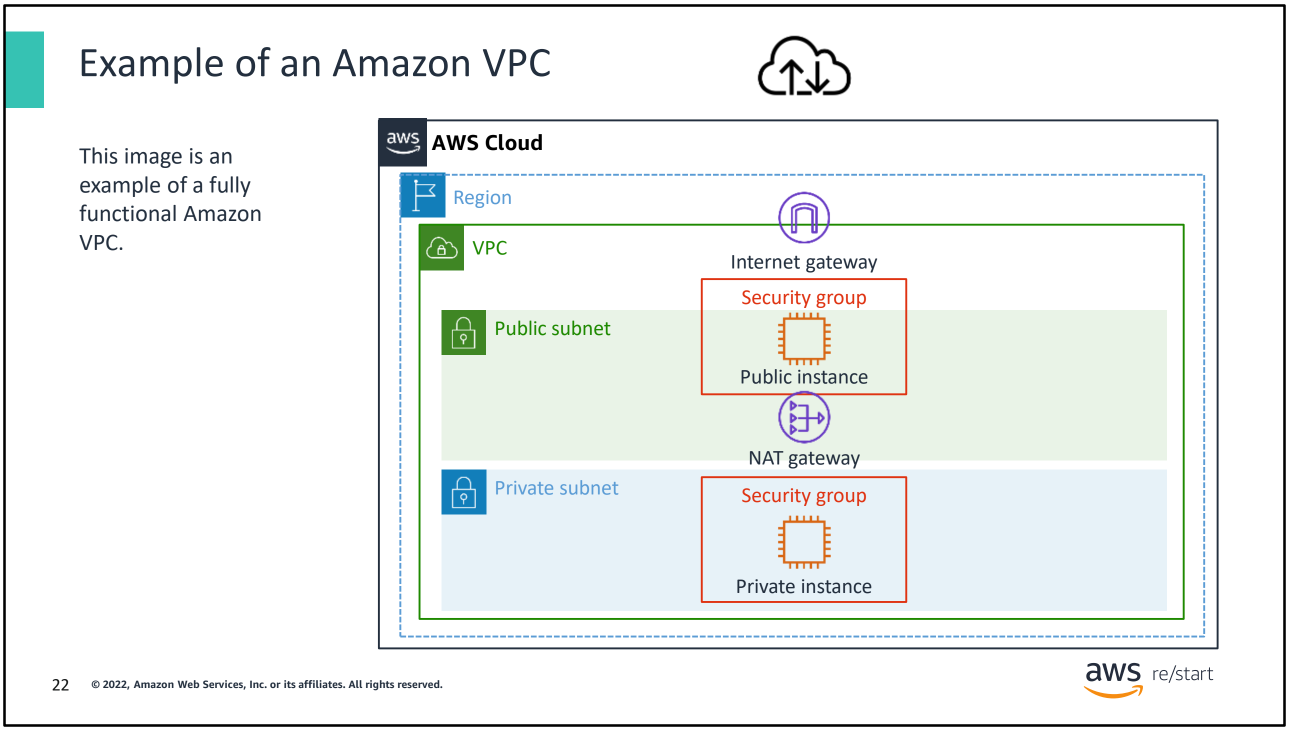
Creating a network ACL requires specific items:

1. Rule number: This option is evaluated with the lowest number first. If a rule matches the traffic, it is applied.
2. Type: For example, this option can be SSH, a range, or all traffic.
3. Protocol: You can specify the ICMP protocol.
4. Port range: For example, this option can be 443 for HTTPS traffic.
5. Source: This option is required only for inbound rules such as the source IP range and CIDR.
6. Destination: This option is required only for outbound rules such as the destination IP range and CIDR.
7. Allow or deny: You can allow or deny the traffic that is specified in the rules.

Why is this information important?

When you are troubleshooting, network ACLs, like security groups, are often an issue when blocking traffic. Checking the deny or allow rules, and the rule number, can further assist you in troubleshooting network ACLs.

For more information, see https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html.

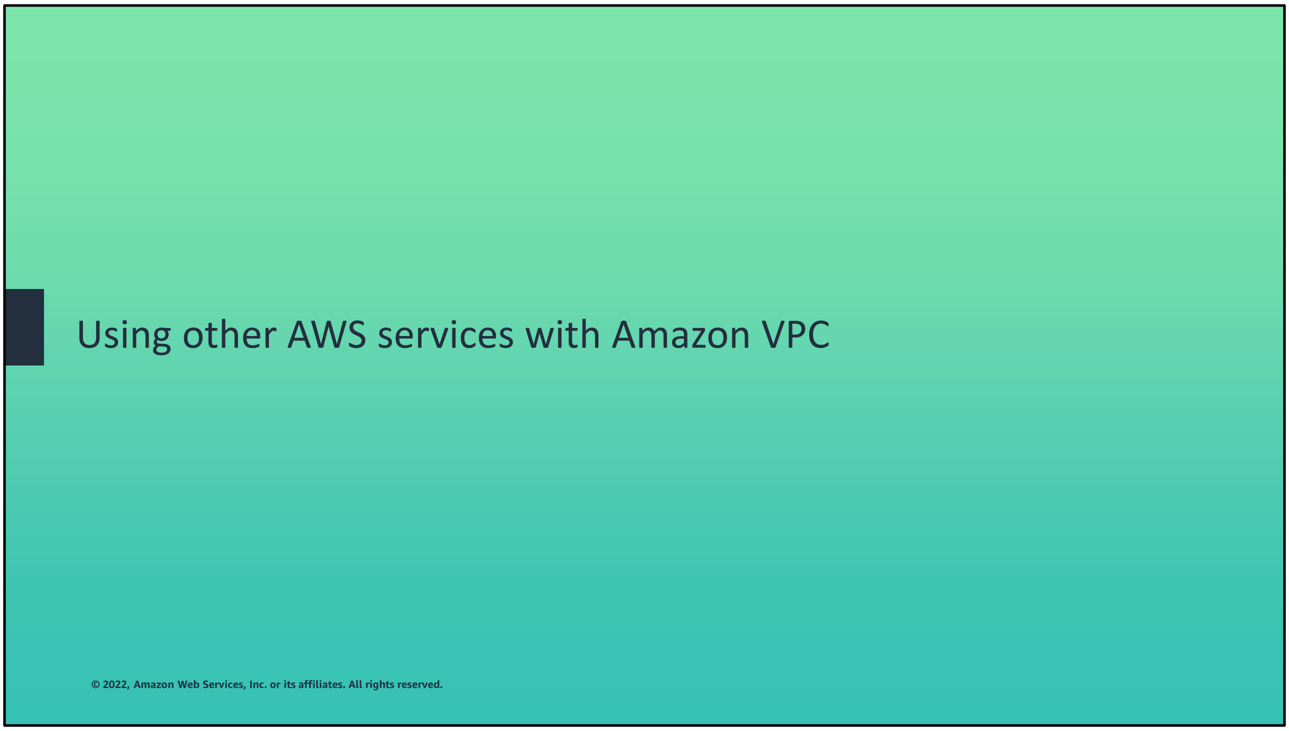


Example of an Amazon VPC

This image is an example of a fully functional Amazon VPC.

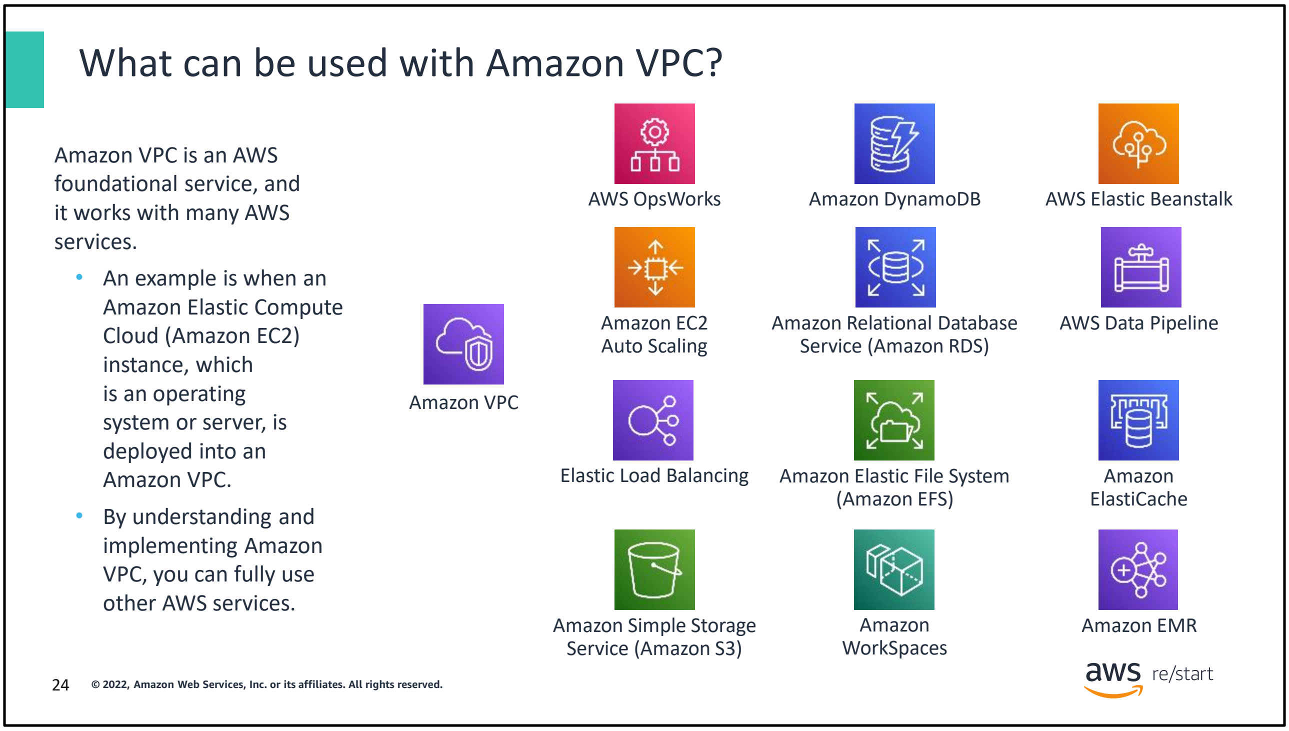
The slide shows an example of a fully functioning Amazon VPC. Starting from the outside and working inward, you have the following components:

- The AWS Cloud environment: This is the account in which you create your Amazon VPC resources.
- The Region: Choose where your logically isolated environment will be provisioned within one of the many Regions in data centers across the US and the world. For a list of Regions, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-available-regions.
- Amazon VPC: This is your logical data center, where resources are provisioned and networked together to reach the outside world.
- Public and private subnet: These are allocated IP ranges for your resources. Public subnets have an internet gateway attached to the route table. Private subnets do not have an internet gateway or public routable address.
- Security groups and network ACLs: These options act as a firewall for your instances and subnets.
- Instances: Instances are operating systems and servers.
- Resources: An internet gateway and NAT gateway are some of the resources that are provisioned within the VPC for it to be routable outside the VPC.



Using other AWS services with Amazon VPC

In this section, you will see examples of additional services that can be used with Amazon VPC.



What can be used with Amazon VPC?

Amazon VPC is an AWS foundational service, and it works with many AWS services.

- An example is when an Amazon Elastic Compute Cloud (Amazon EC2) instance, which is an operating system or server, is deployed into an Amazon VPC.
- By understanding and implementing Amazon VPC, you can fully use other AWS services.

Amazon VPC
AWS OpsWorks
Amazon DynamoDB
AWS Elastic Beanstalk
Amazon EC2 Auto Scaling
Amazon Relational Database Service (Amazon RDS)
AWS Data Pipeline
Elastic Load Balancing
Amazon Elastic File System (Amazon EFS)
Amazon ElastiCache
Amazon Simple Storage Service (Amazon S3)
Amazon WorkSpaces
Amazon EMR
aws re/start

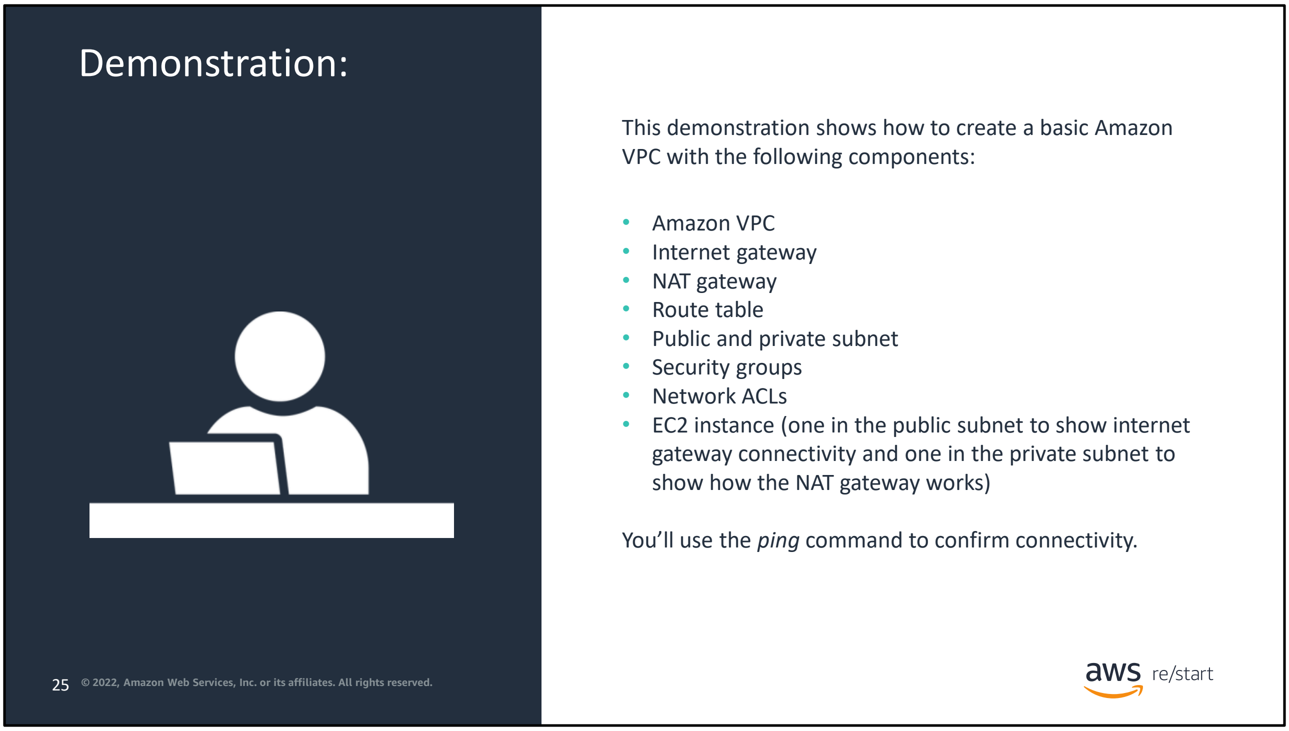
What are some example services that can be used with Amazon VPC?

- **Amazon EC2 Auto Scaling** (https://docs.aws.amazon.com/autoscaling/ec2/userguide/what-is-amazon-ec2-auto-scaling.html): Amazon EC2 Auto Scaling offers scaling to a desired capacity. It ensures a correct number of EC2 instances to handle the load or traffic for your application.
    - Groups of EC2 instances are put into Auto Scaling groups. Within these groups, you set parameters.
    - If there is a scaling policy, Amazon EC2 Auto Scaling can launch or terminate instances on demand for you. This is extremely useful for businesses when they expect a large amount of traffic during a certain time. Depending on the amounts of traffic, Amazon EC2 Auto Scaling can scale to the desired capacity to ensure that the application doesn’t crash.
- **Elastic Load Balancing (ELB)** (https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html): ELB balancers offer fault tolerance by distributing traffic across multiple targets (EC2 instances, IP addresses, or containers) in multiple Availability Zones.
    - It scales with traffic.
    - It is fault tolerant.
    - It monitors the health of registered targets and sends traffic only to

    healthy targets.

    - Types of ELB balancers include Classic Load Balancer, Application Load Balancer, and Network Load Balancer. For information about the benefits of each ELB balancer, see https://aws.amazon.com/elasticloadbalancing/features/#Product_comparisons.

- **Amazon Simple Storage Service (Amazon S3):** Amazon S3 a scalable, secure, and highly available object storage service. For information about the different types of Amazon S3 storage classes, see https://docs.aws.amazon.com/AmazonS3/latest/userguide/storage-class-intro.html#sc-compare.
- **Amazon DynamoDB** (https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html): DynamoDB is a database service that is a fully managed NoSQL database. It offers fast, predictable performance, security, and scalability.
- **Amazon Relational Database Service (Amazon RDS)** (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html): Amazon RDS is a web service that offers the operation and scalability of a relational database in the AWS Cloud.
- **Amazon WorkSpaces** (https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html): You can use this service to provision a virtual desktop (Microsoft Windows or Amazon Linux) for users.



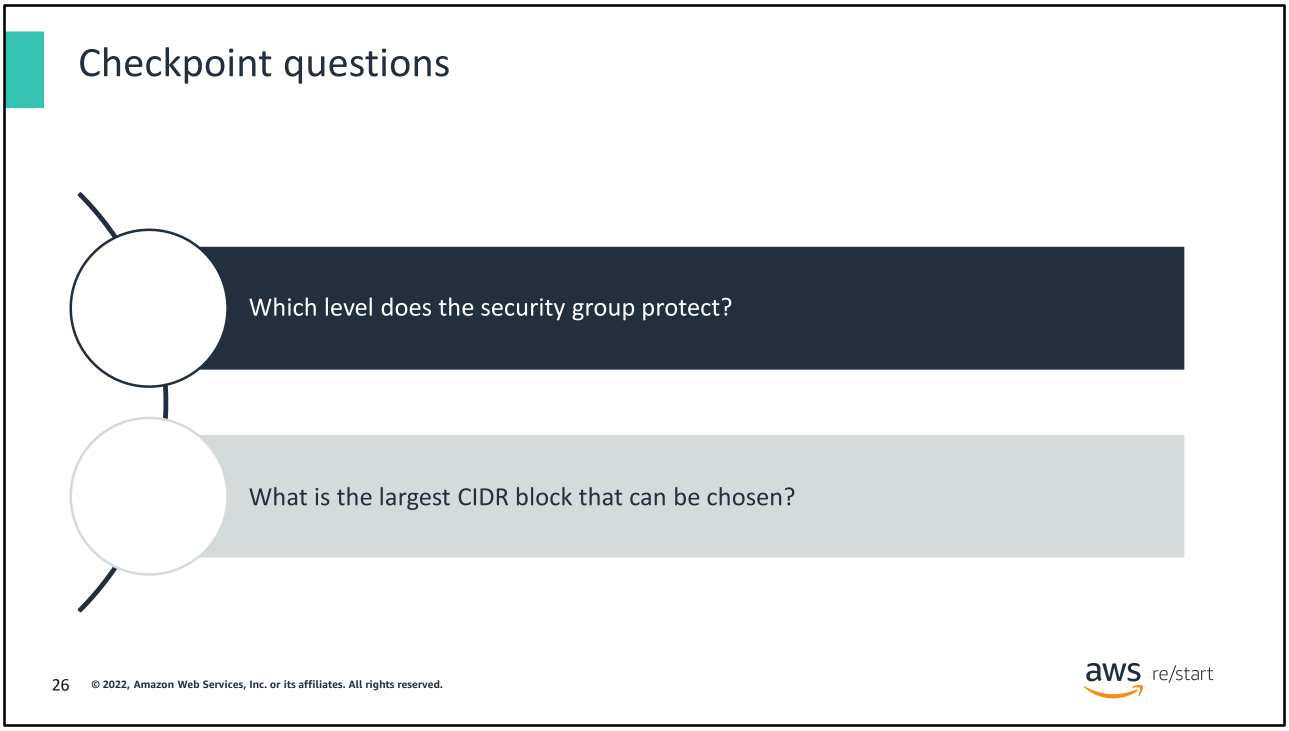
Demonstration:

This demonstration shows how to create a basic Amazon VPC with the following components:

- Amazon VPC
- Internet gateway
- NAT gateway
- Route table
- Public and private subnet
- Security groups
- Network ACLs
- EC2 instance (one in the public subnet to show internet gateway connectivity and one in the private subnet to show how the NAT gateway works)

You'll use the *ping* command to confirm connectivity.

- In the following demonstration, the instructor will demonstrate how to create a basic Amazon VPC with the following components:
  - Amazon VPC
  - Internet gateway
  - NAT gateway
  - Route table
  - Public and private subnet
  - Security groups
  - Network ACLs
  - EC2 instances (one in the public subnet to show internet gateway connectivity and one in the private subnet to show how the NAT gateway works)
- After the Amazon VPC is created, the instructor will then use the *ping* command to test connectivity.
- Please follow along because doing so will help you understand the labs later in the course.



Checkpoint questions

Which level does the security group protect?

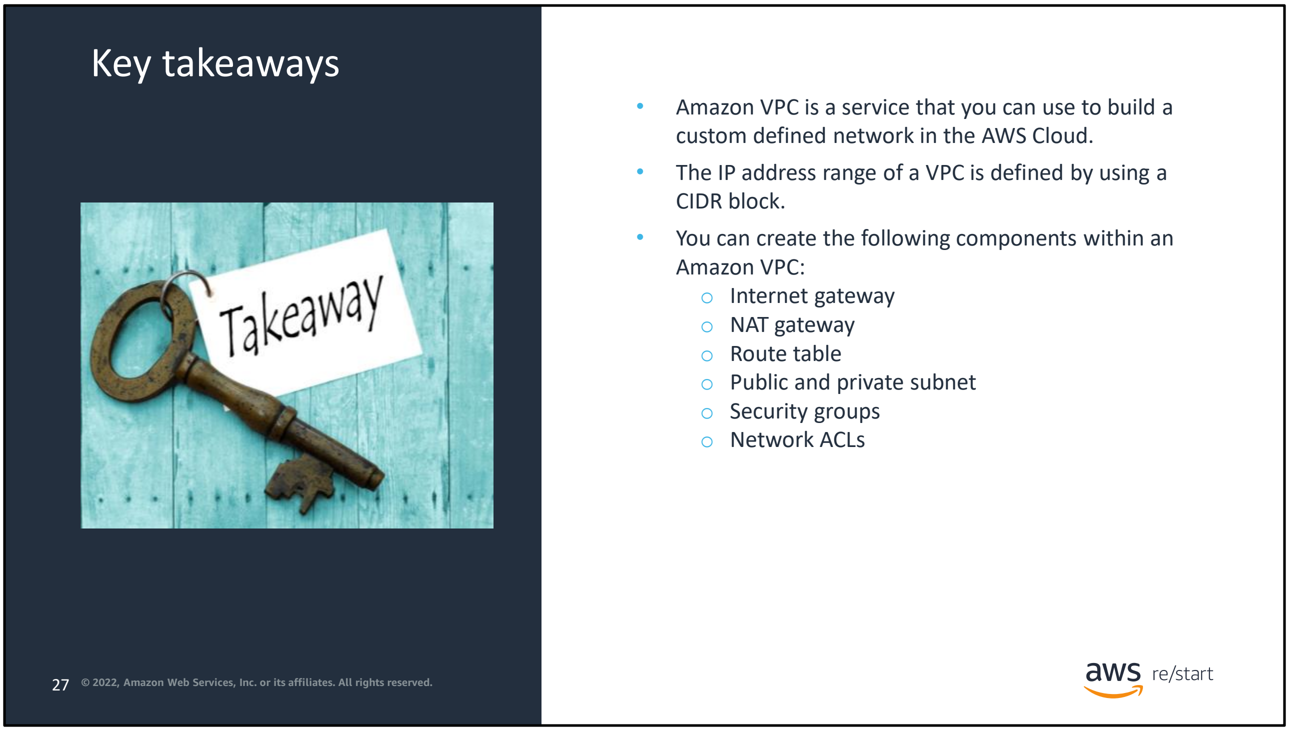
What is the largest CIDR block that can be chosen?

Q1: Which level does the security group protect?

Answer: Instance level

Q2: What is the largest CIDR block that can be chosen?

Answer: /16



Key takeaways

- Amazon VPC is a service that you can use to build a custom defined network in the AWS Cloud.
- The IP address range of a VPC is defined by using a CIDR block.
- You can create the following components within an Amazon VPC:
  - Internet gateway
  - NAT gateway
  - Route table
  - Public and private subnet
  - Security groups
  - Network ACLs

- Amazon VPC is a service that you can use to build a custom defined network in the AWS Cloud.
- The IP address range of a VPC is defined by using a CIDR block.
- You can create the following components within an Amazon VPC:
  - Internet gateway
  - NAT gateway
  - Route table
  - Public and private subnet
  - Security groups
  - Network ACLs

Thank you

Thank you for taking this course.