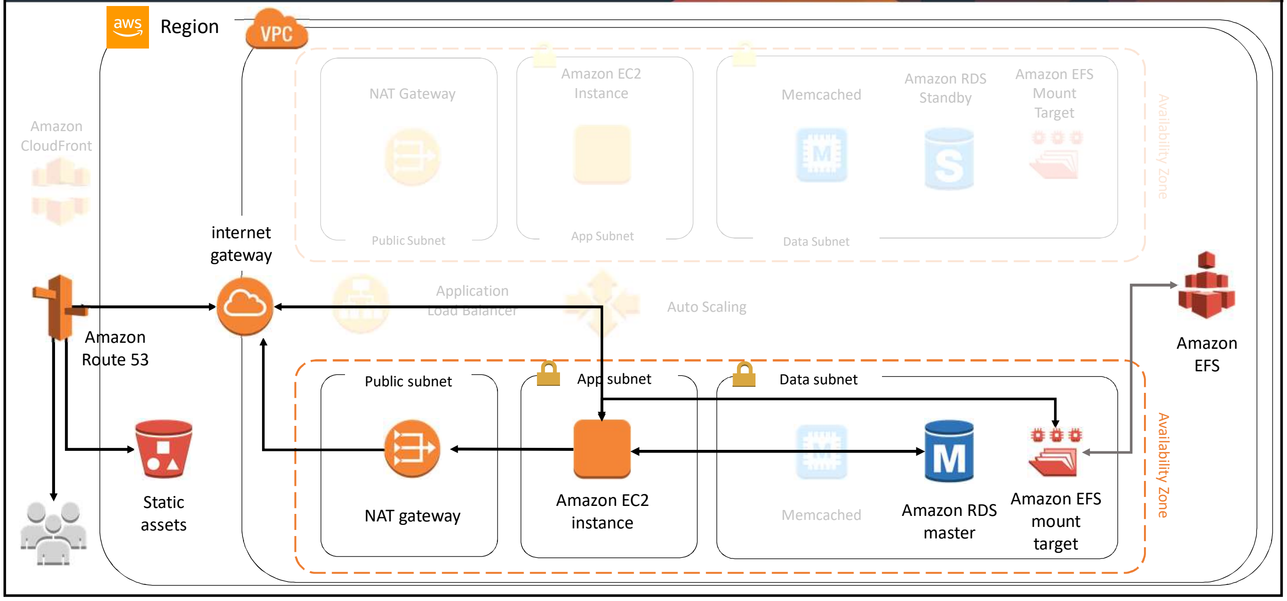
aws training and certification

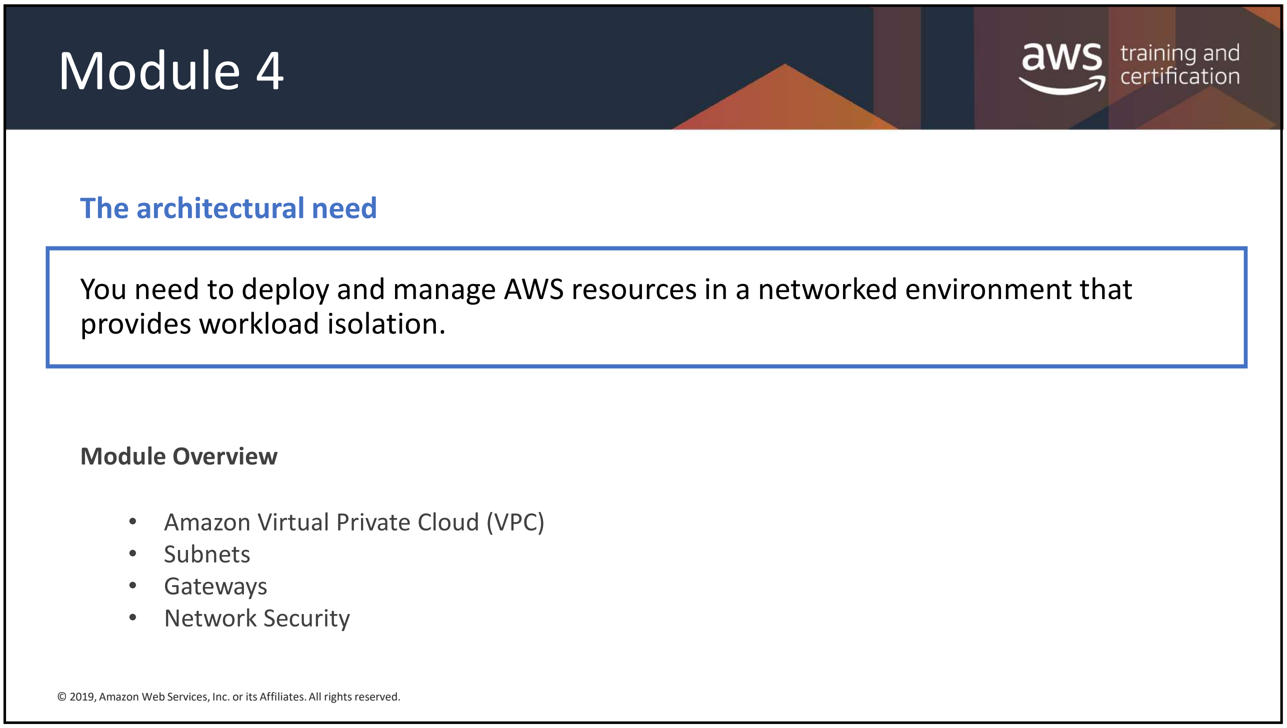
Networking In AWS Part 1

Module 4

Networking Layer

aws training and certification





Module 4

aws training and certification

The architectural need

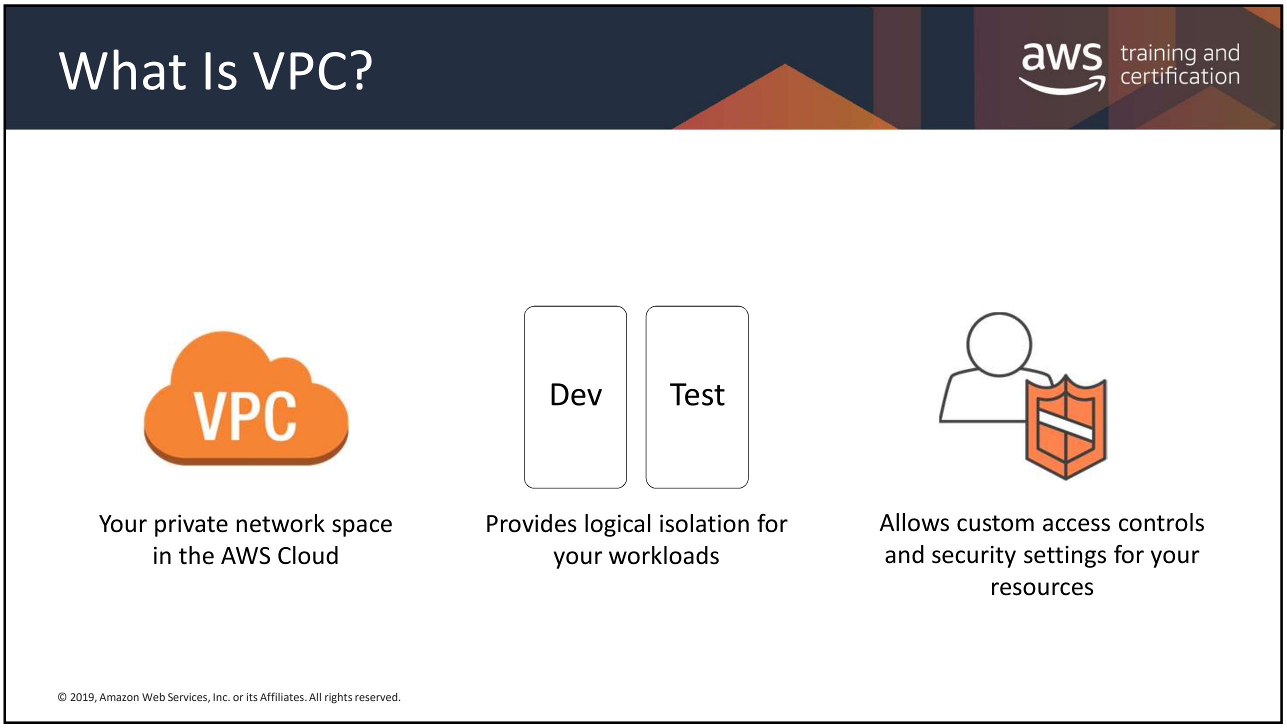
You need to deploy and manage AWS resources in a networked environment that provides workload isolation.

Module Overview

- Amazon Virtual Private Cloud (VPC)
- Subnets
- Gateways
- Network Security

aws training and certification

Amazon Virtual Private Cloud (VPC)



What Is VPC?

VPC

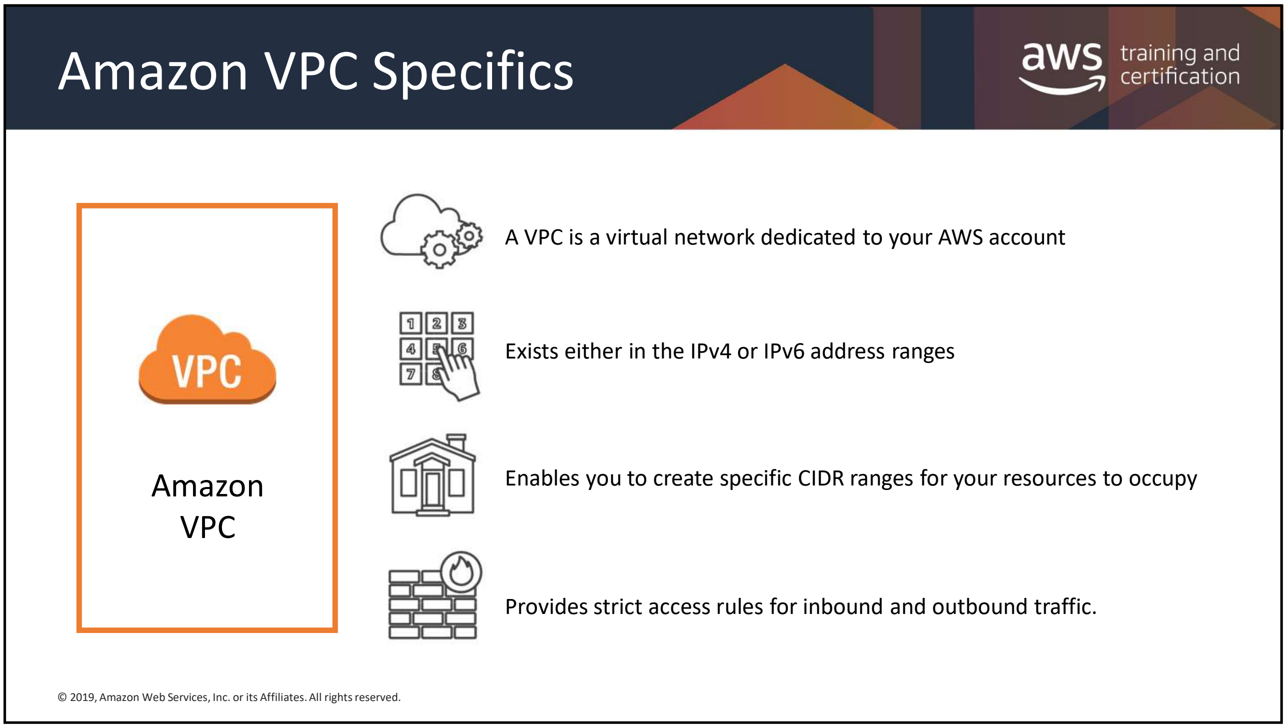
Your private network space in the AWS Cloud

Dev

Test

Provides logical isolation for your workloads

Allows custom access controls and security settings for your resources



Amazon VPC Specifics

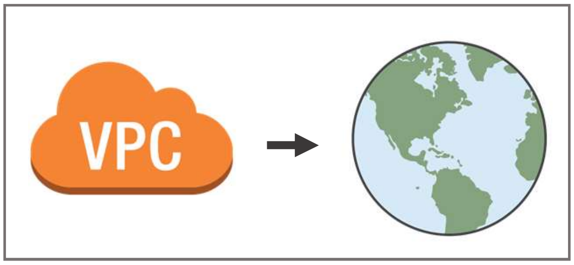
VPC

Amazon VPC

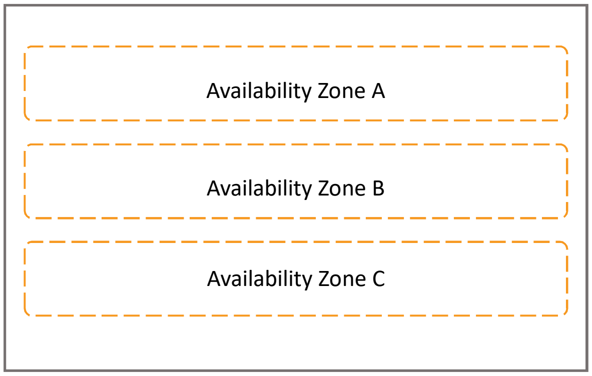
- A VPC is a virtual network dedicated to your AWS account
- Exists either in the IPv4 or IPv6 address ranges
- Enables you to create specific CIDR ranges for your resources to occupy
- Provides strict access rules for inbound and outbound traffic.

Deploying A VPC

aws training and certification



VPCs deploy into **1** of the **18** AWS Regions



A VPC can host resources from **any** Availability Zone within its region

Using One VPC

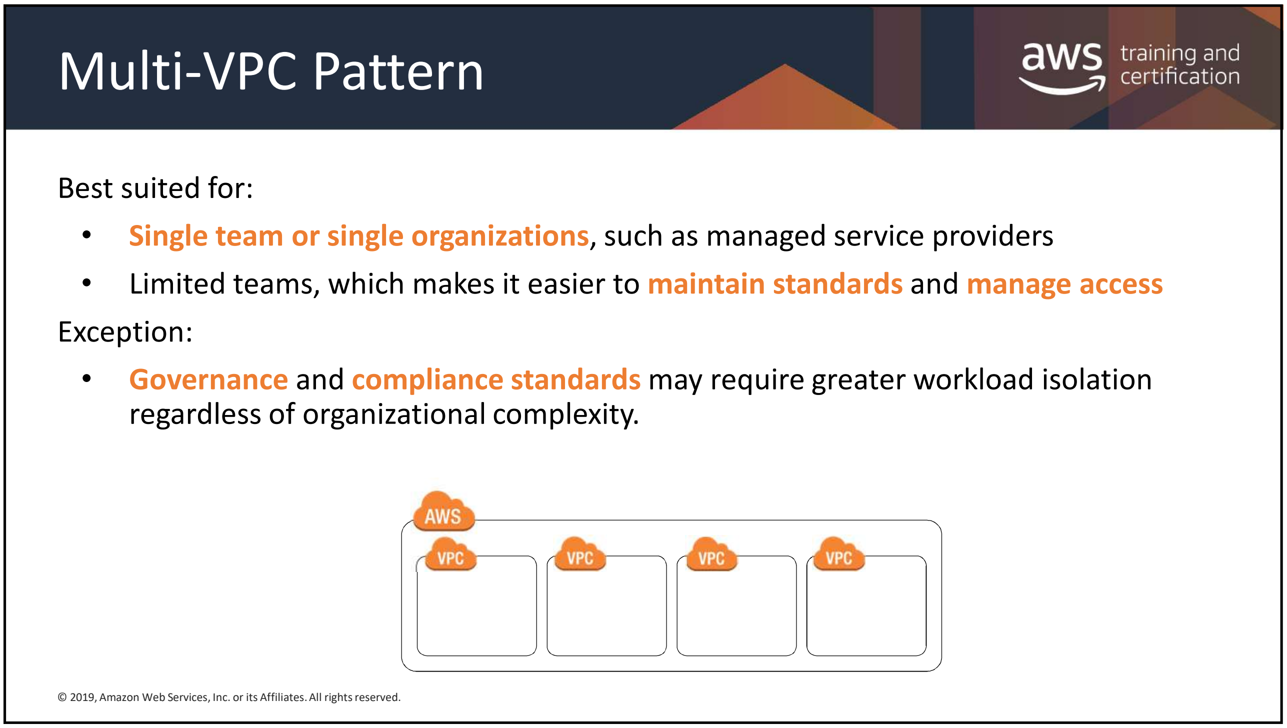
aws training and certification

There are **limited** use cases where one VPC could be appropriate:

- Small, single applications managed by one person or a very small team
- High-performance computing
- Identity management

For **most** use cases, there are two primary patterns for organizing your infrastructure:

Multi-VPC and **multi-account**



Multi-VPC Pattern

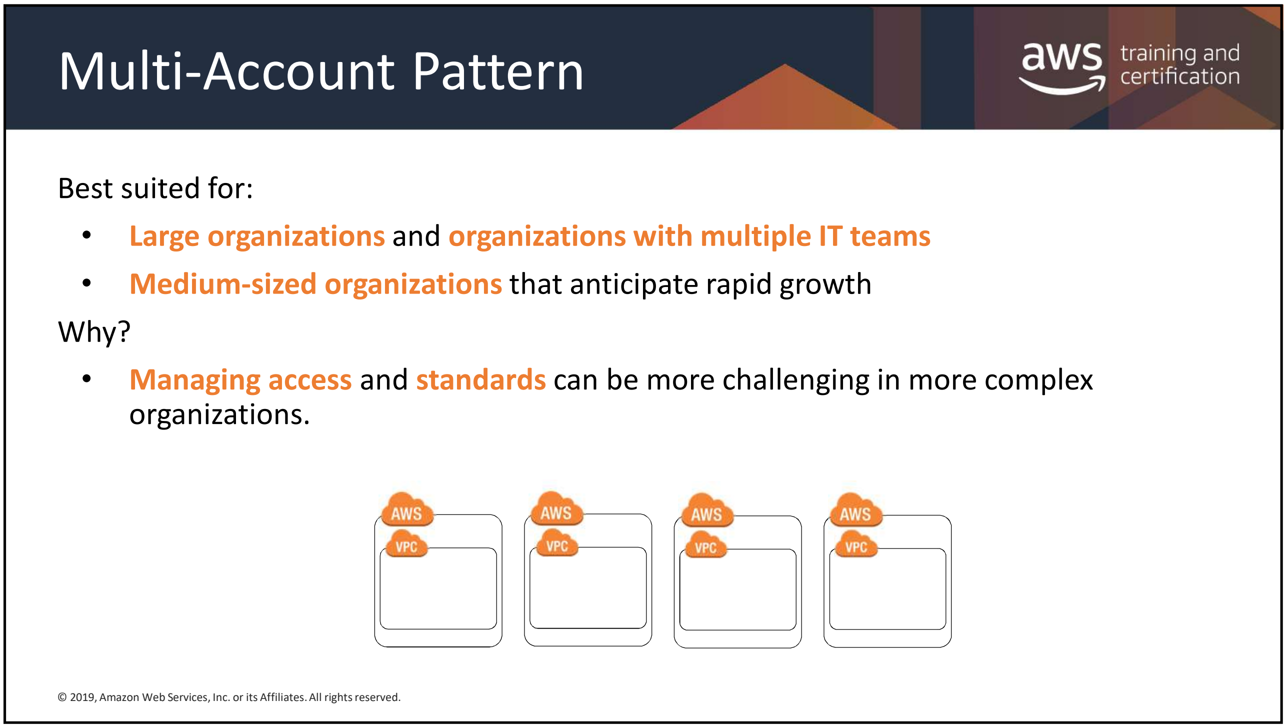
Best suited for:

- **Single team or single organizations**, such as managed service providers
- Limited teams, which makes it easier to **maintain standards** and **manage access**

Exception:

- **Governance** and **compliance standards** may require greater workload isolation regardless of organizational complexity.

AWS
VPC
VPC
VPC
VPC



Multi-Account Pattern

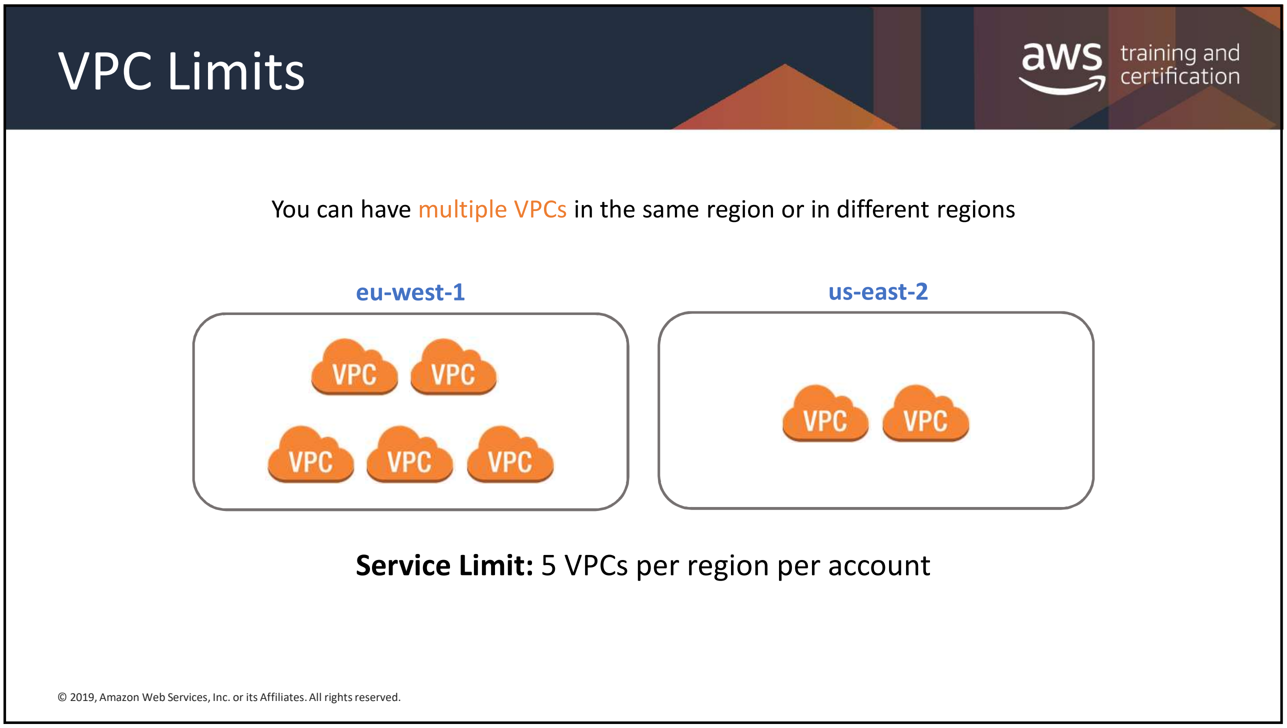
Best suited for:

- **Large organizations** and **organizations with multiple IT teams**
- **Medium-sized organizations** that anticipate rapid growth

Why?

- **Managing access** and **standards** can be more challenging in more complex organizations.

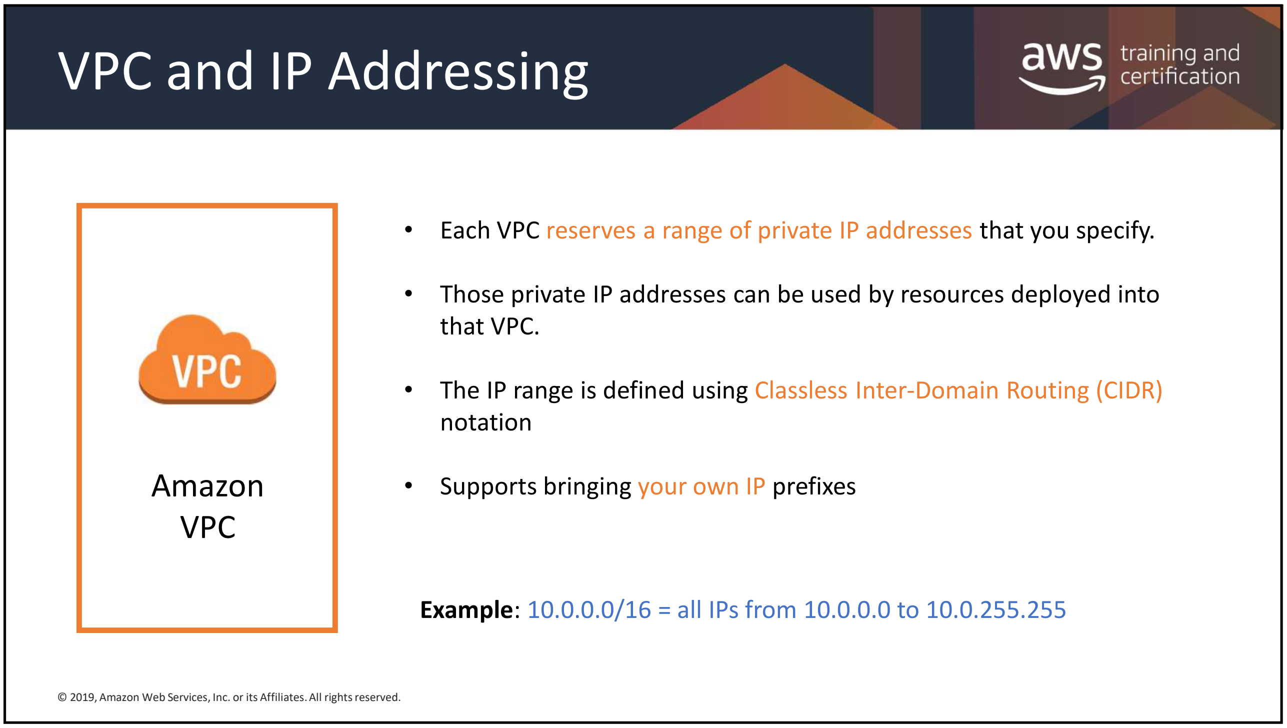
AWS
VPC
AWS
VPC
AWS
VPC
AWS
VPC



VPC Limits

You can have multiple VPCs in the same region or in different regions

Service Limit: 5 VPCs per region per account

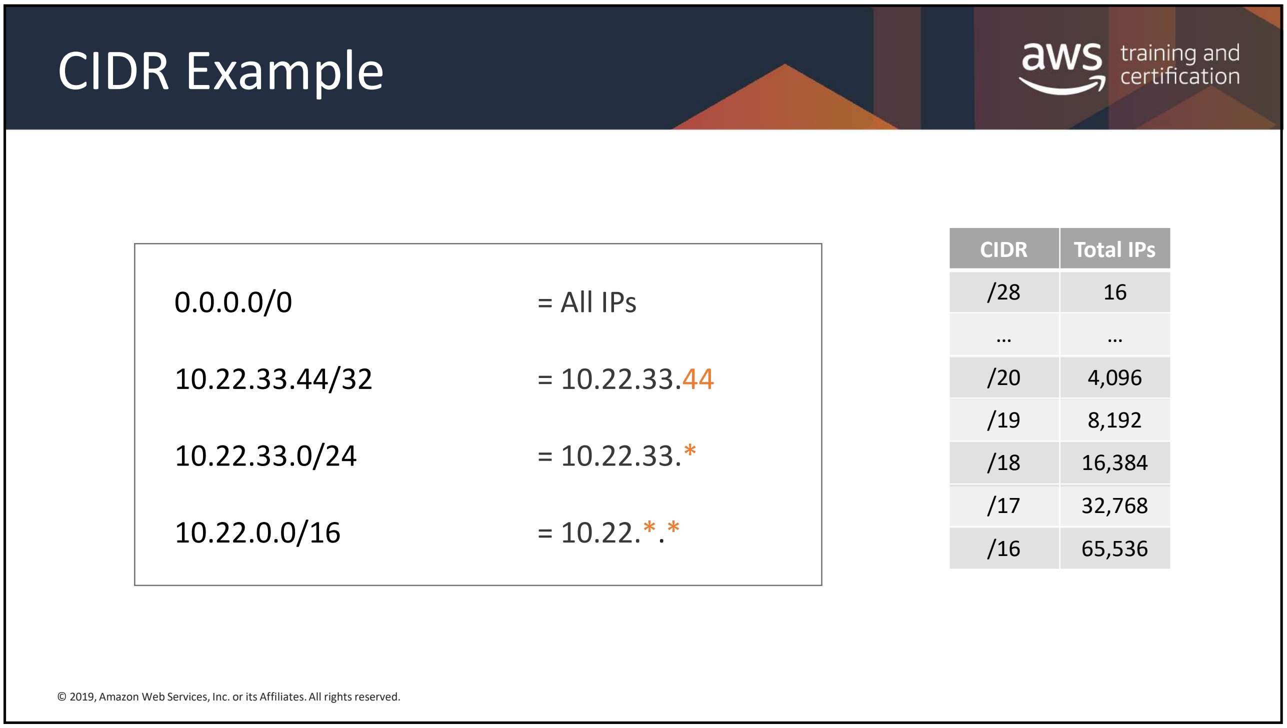


VPC and IP Addressing

VPC
Amazon VPC

- Each VPC reserves a range of private IP addresses that you specify.
- Those private IP addresses can be used by resources deployed into that VPC.
- The IP range is defined using Classless Inter-Domain Routing (CIDR) notation
- Supports bringing your own IP prefixes

Example: 10.0.0.0/16 = all IPs from 10.0.0.0 to 10.0.255.255

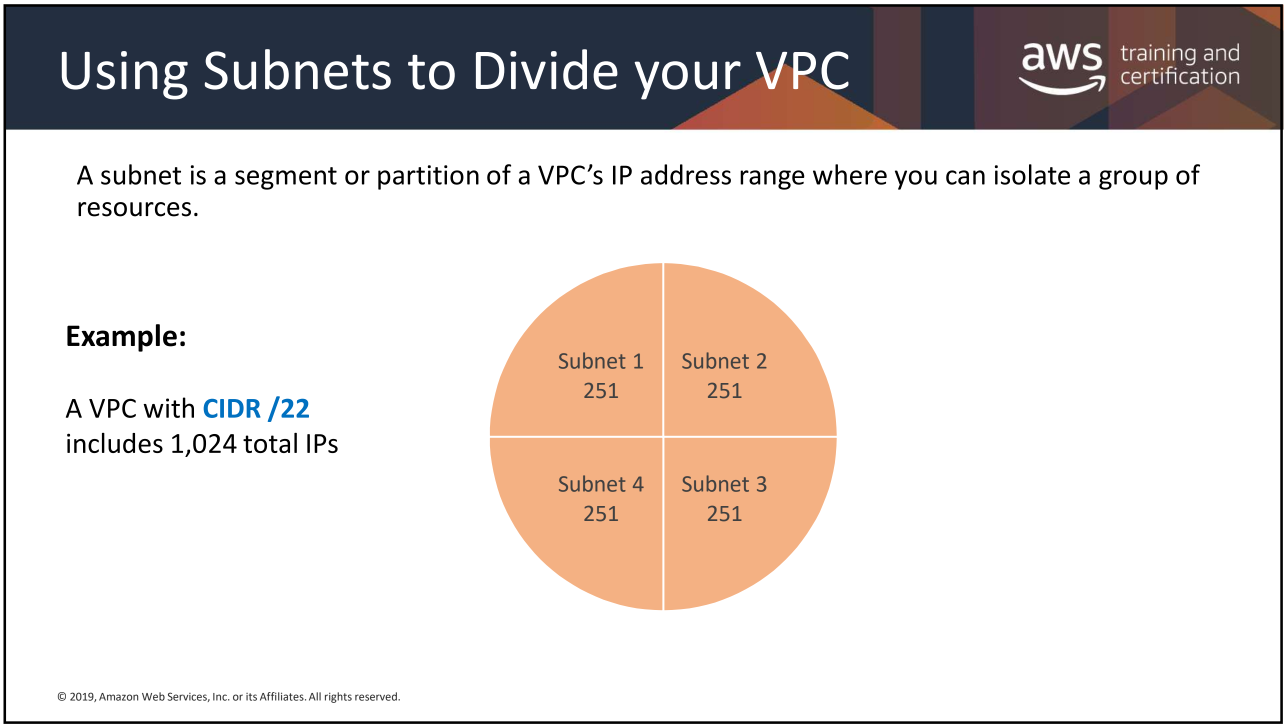


CIDR Example

aws training and certification

0.0.0.0/0	= All IPs
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	Total IPs
/28	16
…	…
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536



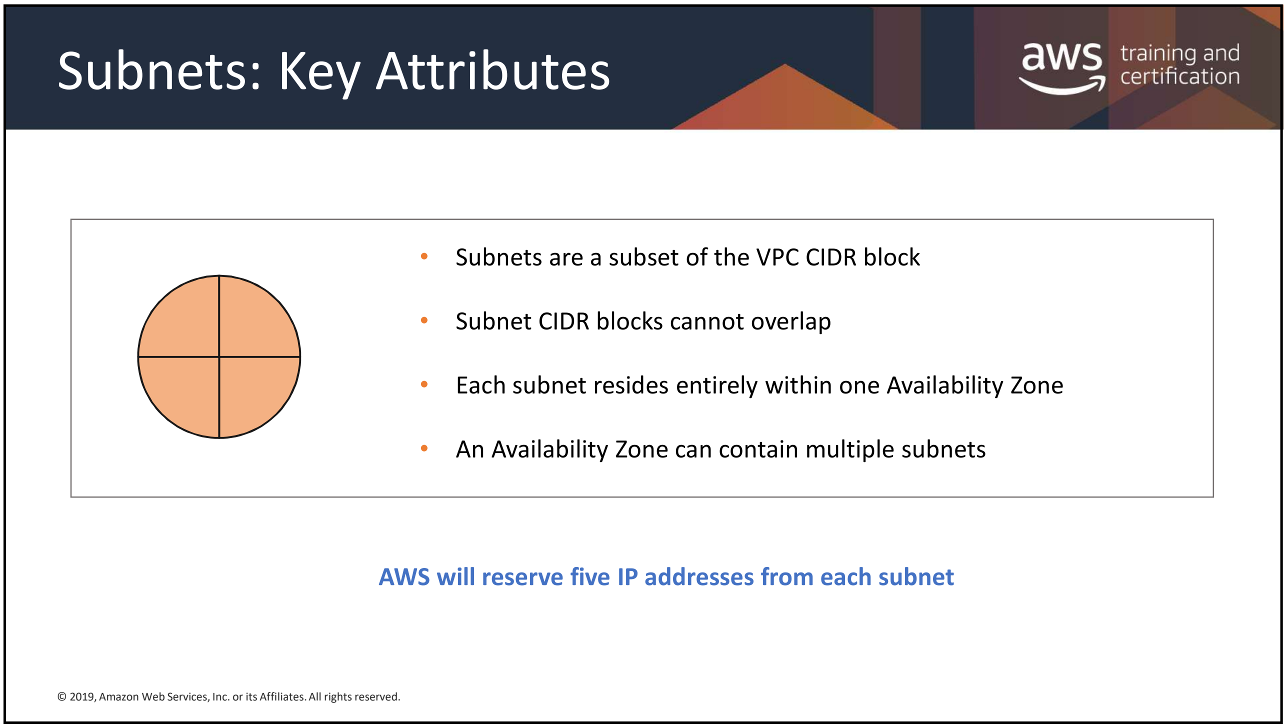
Using Subnets to Divide your VPC

aws training and certification

A subnet is a segment or partition of a VPC's IP address range where you can isolate a group of resources.

Example:

A VPC with **CIDR /22** includes 1,024 total IPs

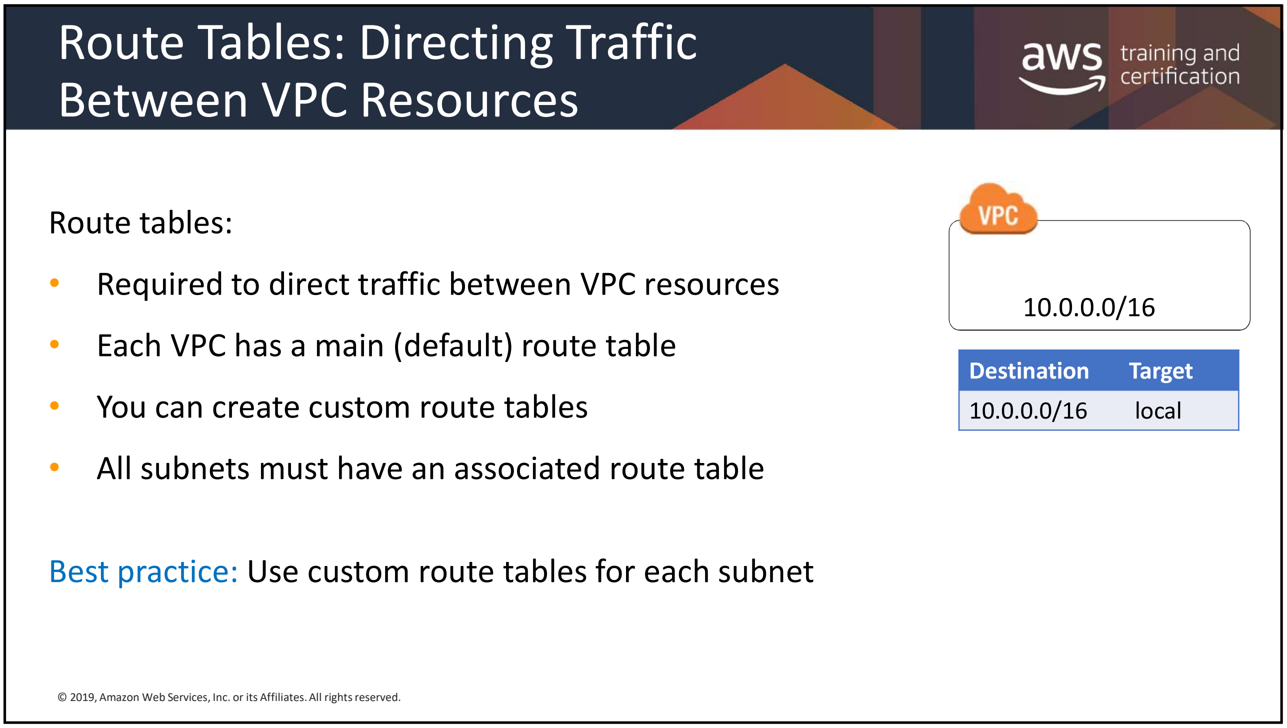


Subnets: Key Attributes

aws training and certification

- Subnets are a subset of the VPC CIDR block
- Subnet CIDR blocks cannot overlap
- Each subnet resides entirely within one Availability Zone
- An Availability Zone can contain multiple subnets

AWS will reserve five IP addresses from each subnet



Route Tables: Directing Traffic Between VPC Resources

aws training and certification

Route tables:

- Required to direct traffic between VPC resources
- Each VPC has a main (default) route table
- You can create custom route tables
- All subnets must have an associated route table

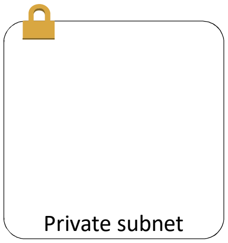
Best practice: Use custom route tables for each subnet

VPC
10.0.0.0/16

Destination	Target
10.0.0.0/16	local

Subnets Allow Different Levels of Network Isolation

aws training and certification



Use subnets to define internet accessibility.

Public subnets

- Include a routing table entry to an internet gateway to support inbound/outbound access to the public internet

Private subnets

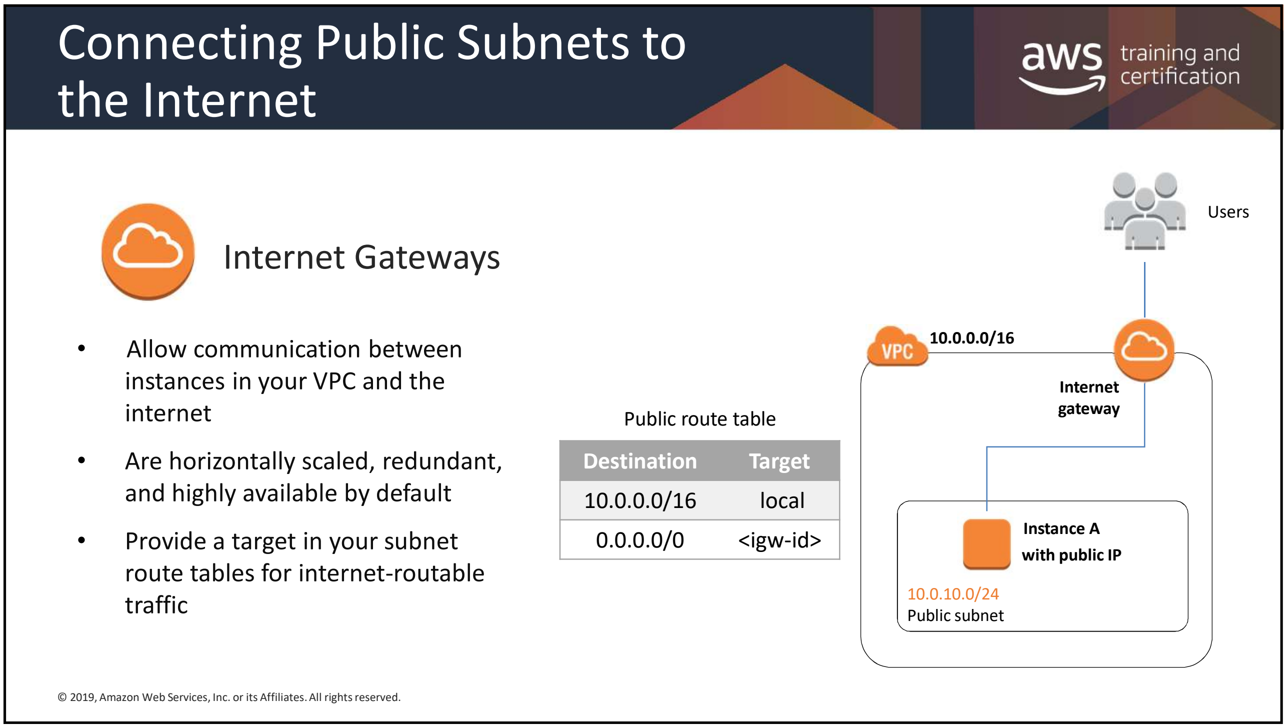
- Do not have a routing table entry to an internet gateway
- Are not directly accessible from the public internet
- Typically use a NAT gateway to support restricted, outbound public internet access

Connecting Public Subnets to the Internet

aws training and certification

Internet Gateways

- Allow communication between instances in your VPC and the internet
- Are horizontally scaled, redundant, and highly available by default
- Provide a target in your subnet route tables for internet-routable traffic



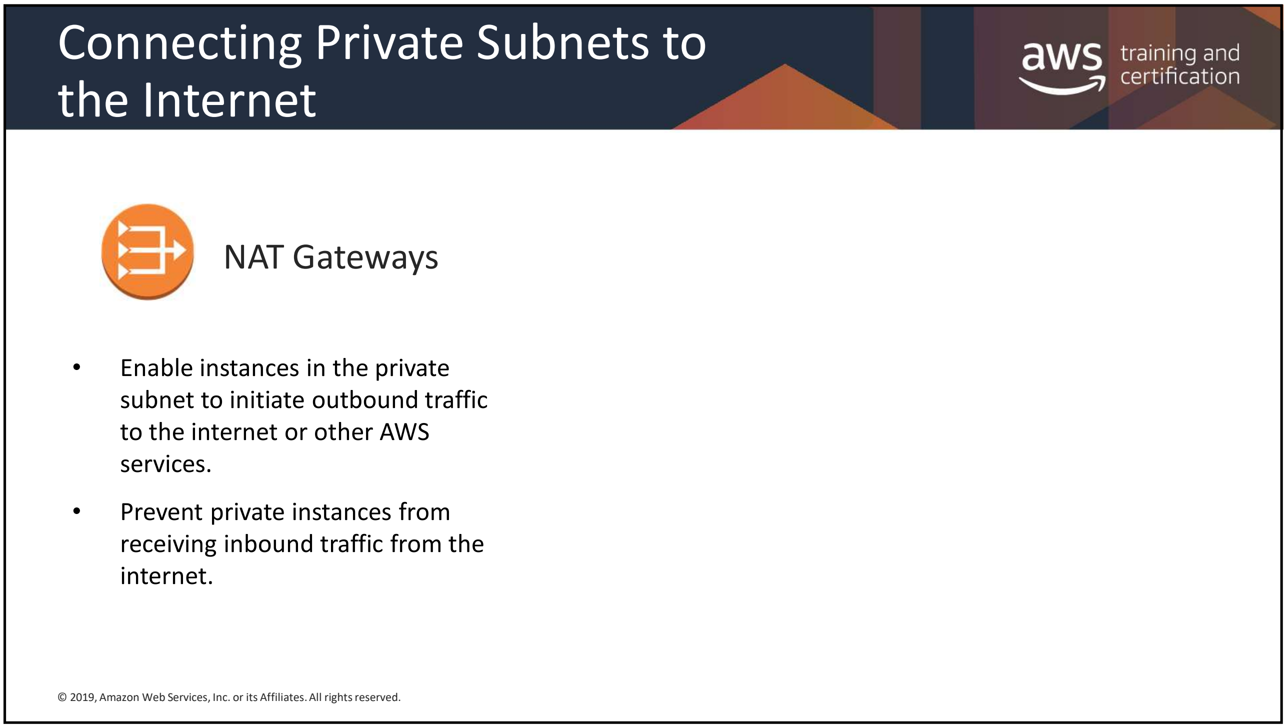
Connecting Public Subnets to the Internet

Internet Gateways

- Allow communication between instances in your VPC and the internet
- Are horizontally scaled, redundant, and highly available by default
- Provide a target in your subnet route tables for internet-routable traffic

Public route table

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

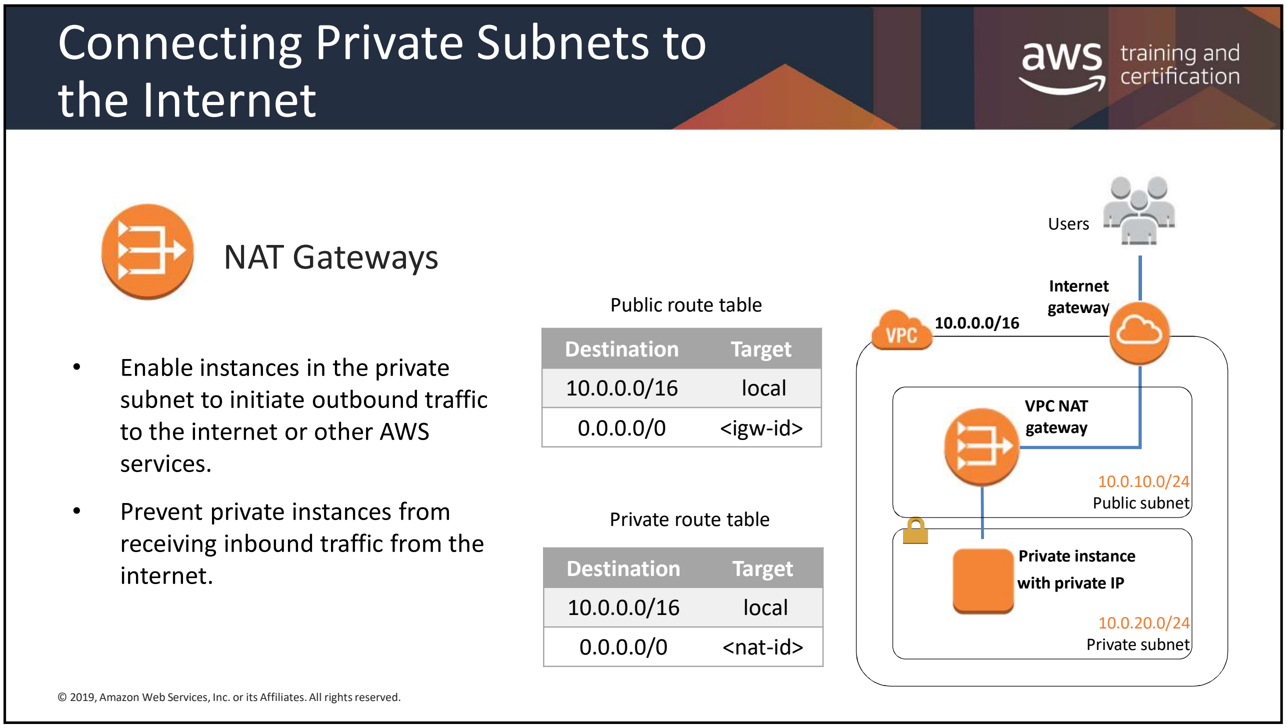


Connecting Private Subnets to the Internet

aws training and certification

NAT Gateways

- Enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services.
- Prevent private instances from receiving inbound traffic from the internet.



Connecting Private Subnets to the Internet

NAT Gateways

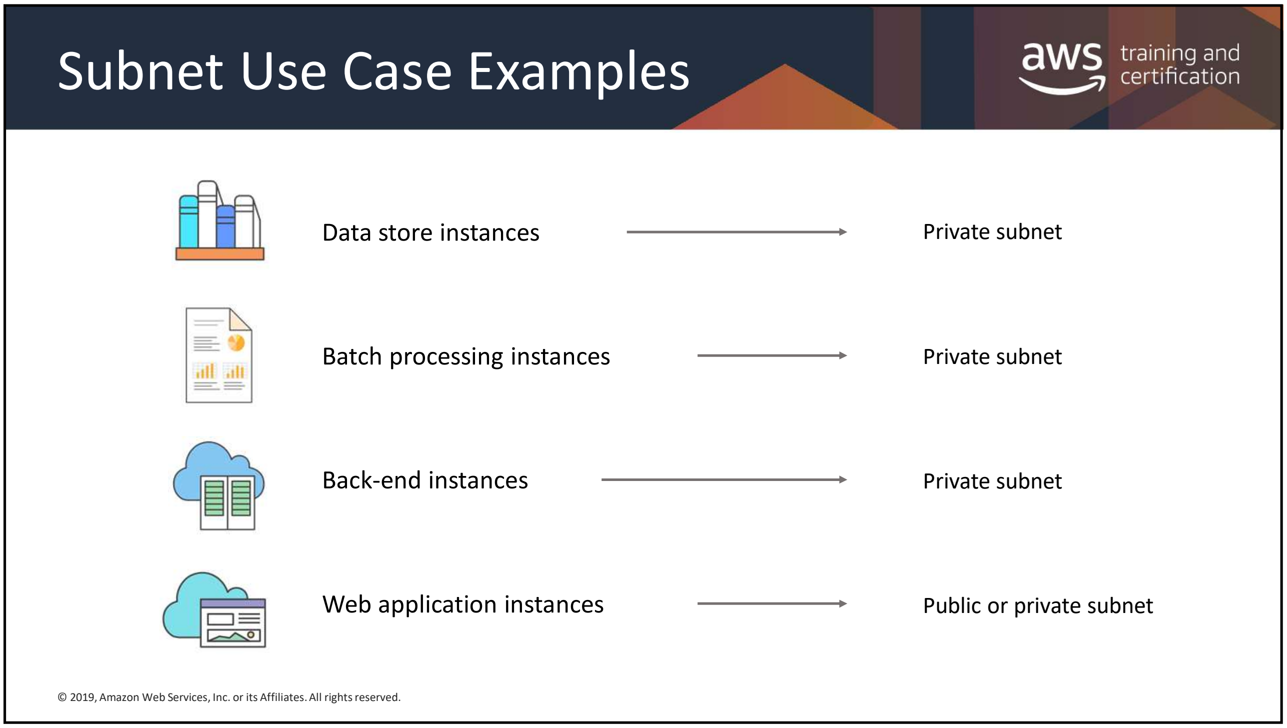
- Enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services.
- Prevent private instances from receiving inbound traffic from the internet.

Public route table

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

Private route table

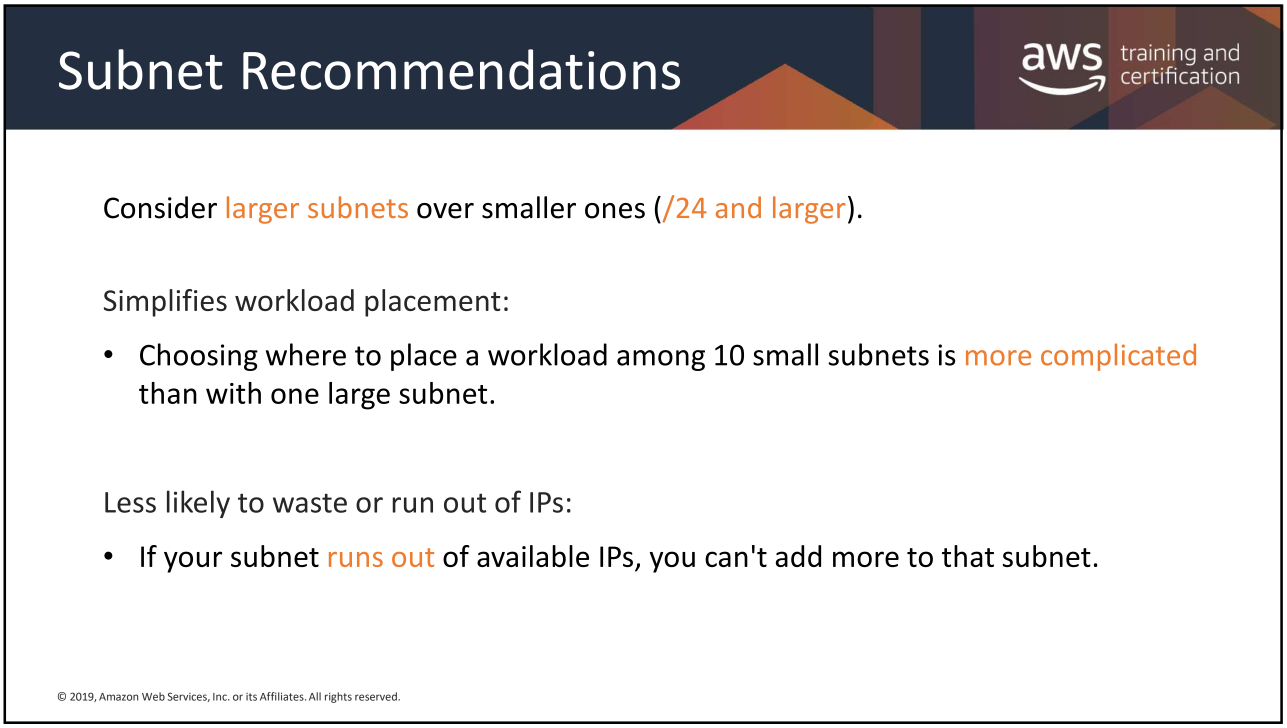
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



Subnet Use Case Examples

aws training and certification

Data store instances →	Private subnet
Batch processing instances →	Private subnet
Back-end instances →	Private subnet
Web application instances →	Public or private subnet



Subnet Recommendations

aws training and certification

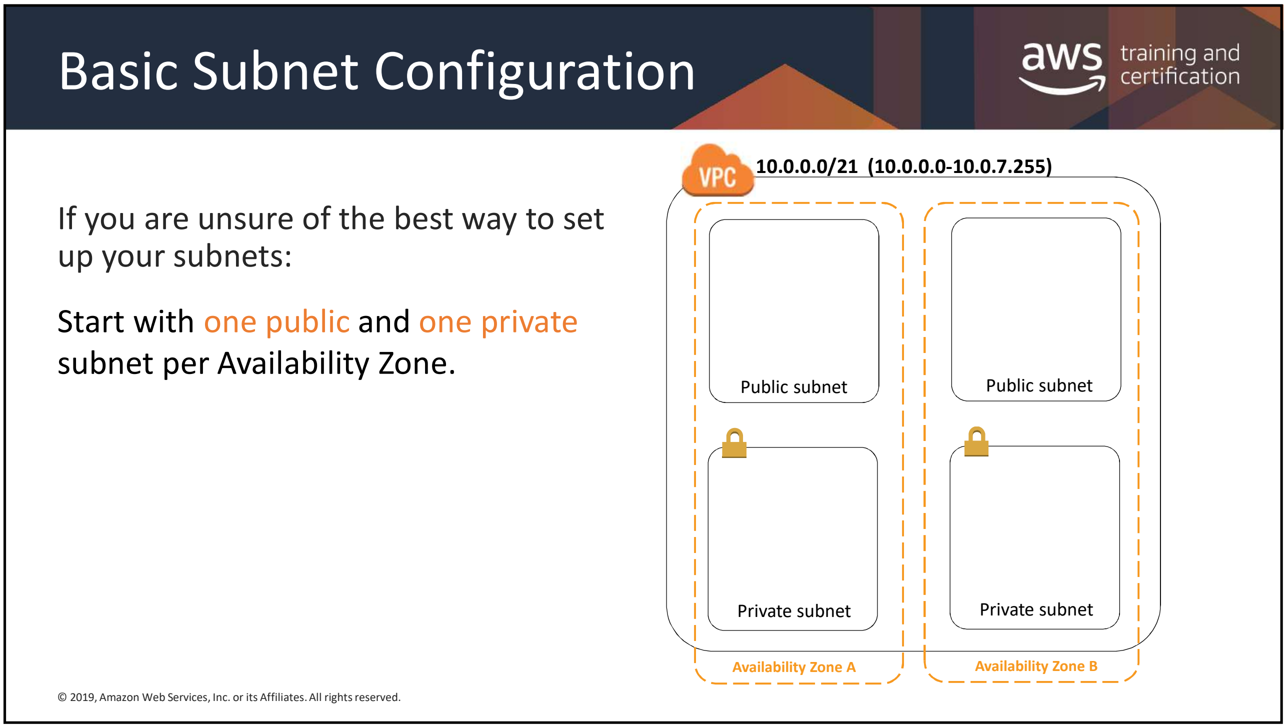
Consider larger subnets over smaller ones (/24 and larger).

Simplifies workload placement:

- Choosing where to place a workload among 10 small subnets is more complicated than with one large subnet.

Less likely to waste or run out of IPs:

- If your subnet runs out of available IPs, you can't add more to that subnet.



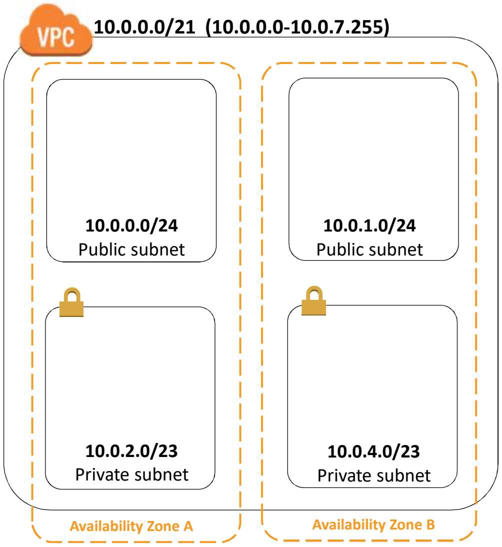
Basic Subnet Configuration

aws training and certification

If you are unsure of the best way to set up your subnets:

Start with one public and one private subnet per Availability Zone.

Basic Subnet Configuration



VPC

10.0.0.0/21 (10.0.0.0-10.0.7.255)

10.0.0.0/24
Public subnet

10.0.1.0/24
Public subnet

10.0.2.0/23
Private subnet

10.0.4.0/23
Private subnet

Availability Zone A

Availability Zone B

Most architectures have significantly more private resources than public resources.

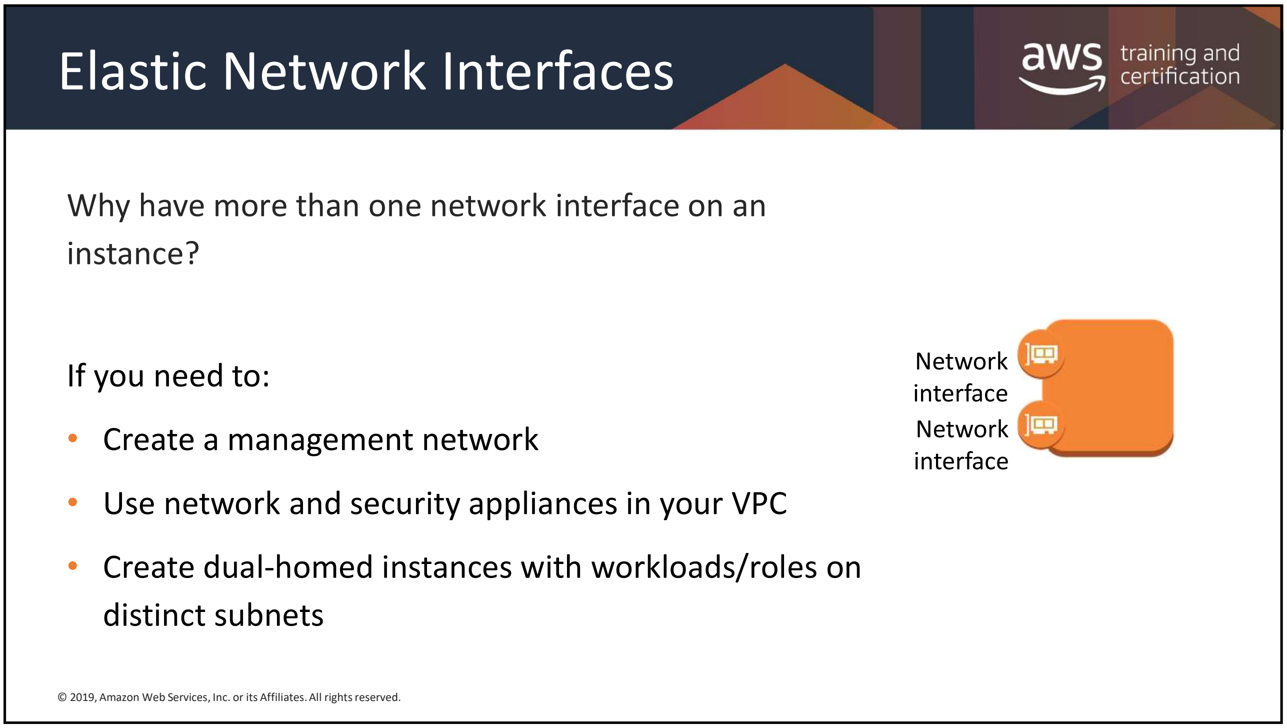
Allocate substantially more IPs for private subnets than for public subnets.

Elastic Network Interfaces

An elastic network interface is a
virtual network interface
that can be moved across EC2 instances
in the same Availability Zone.

When moved to a new instance, a network interface maintains its:

- Private IP address
- Elastic IP address
- MAC address



Elastic Network Interfaces

aws training and certification

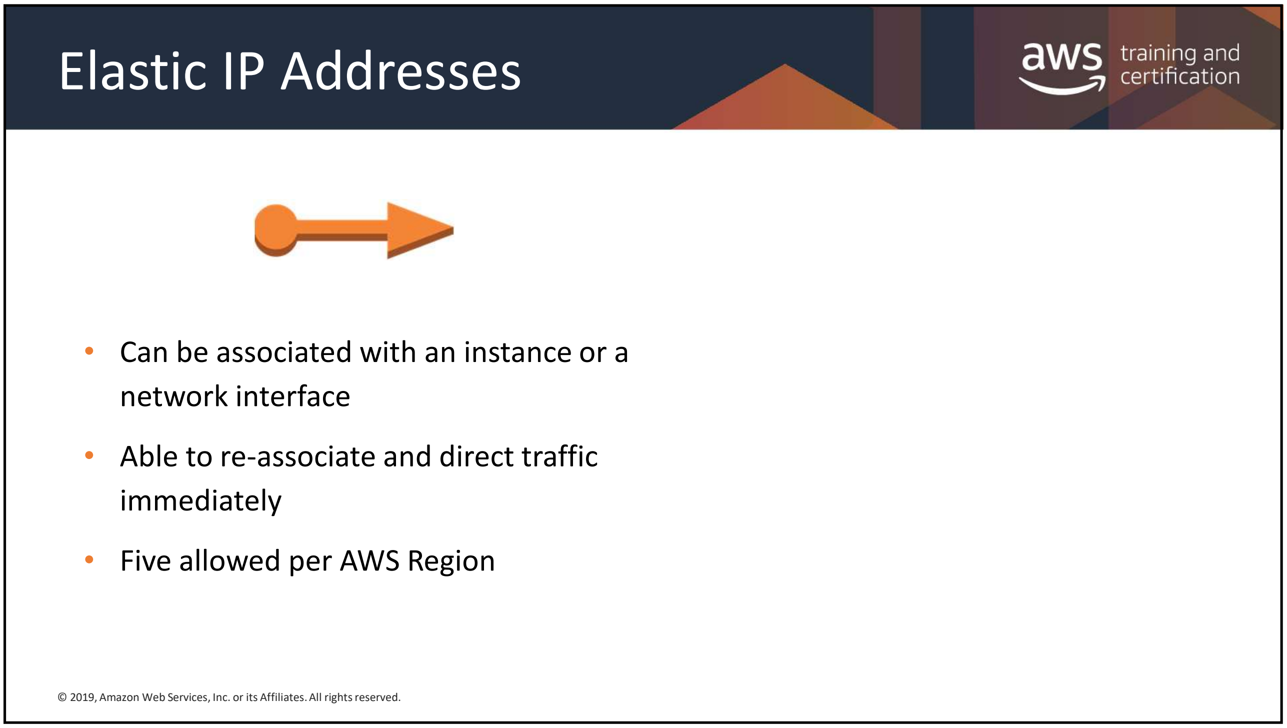
Why have more than one network interface on an instance?

If you need to:

- Create a management network
- Use network and security appliances in your VPC
- Create dual-homed instances with workloads/roles on distinct subnets

Network interface

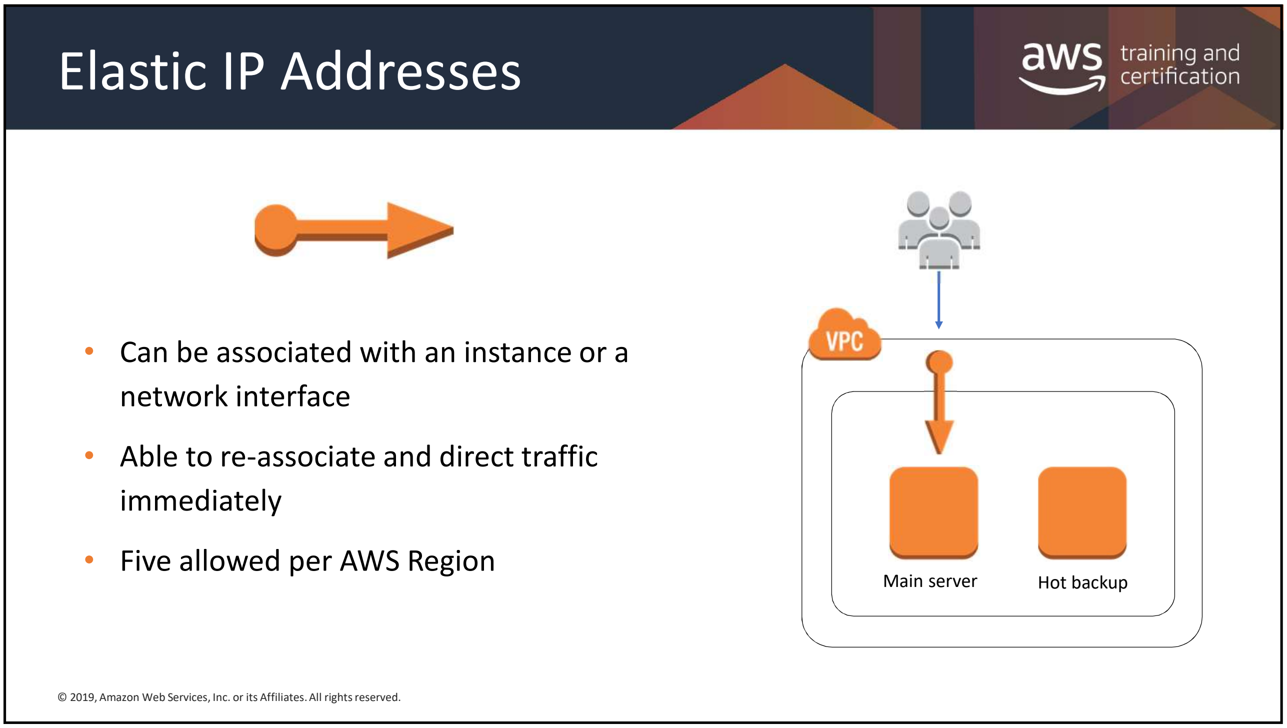
Network interface



Elastic IP Addresses

aws training and certification

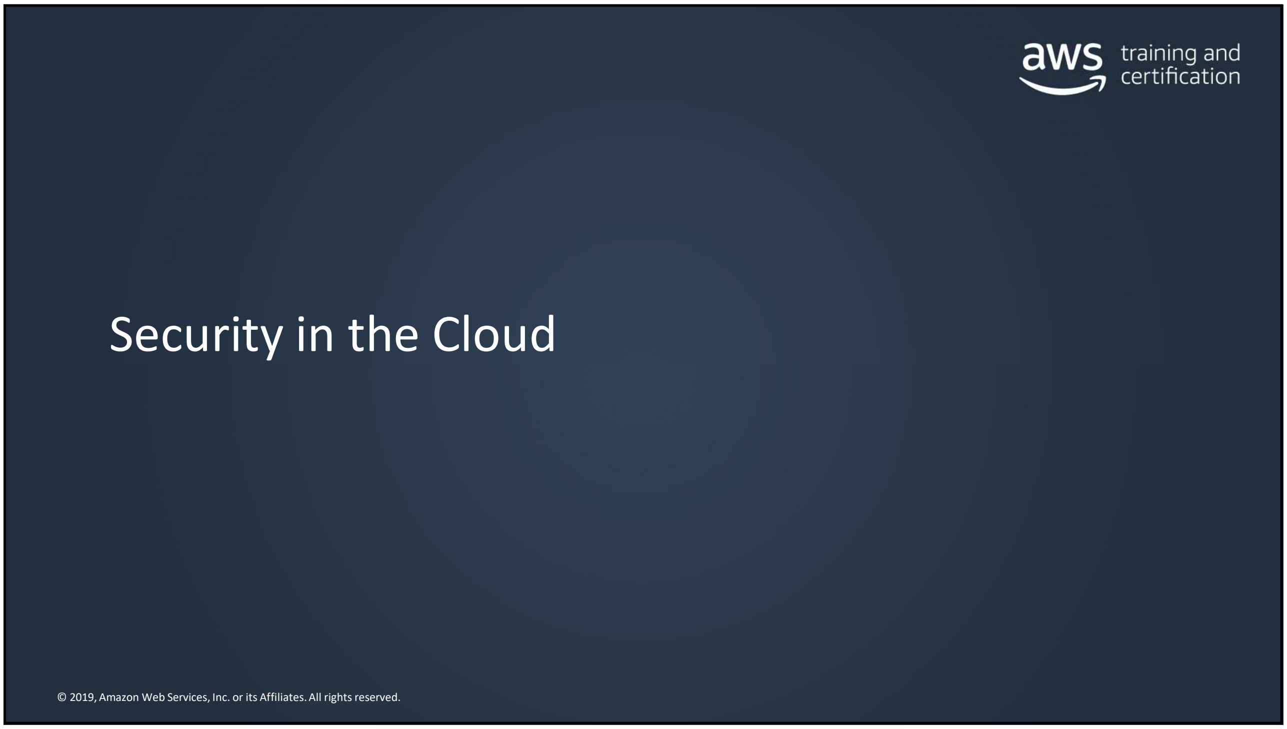
- Can be associated with an instance or a network interface
- Able to re-associate and direct traffic immediately
- Five allowed per AWS Region



Elastic IP Addresses

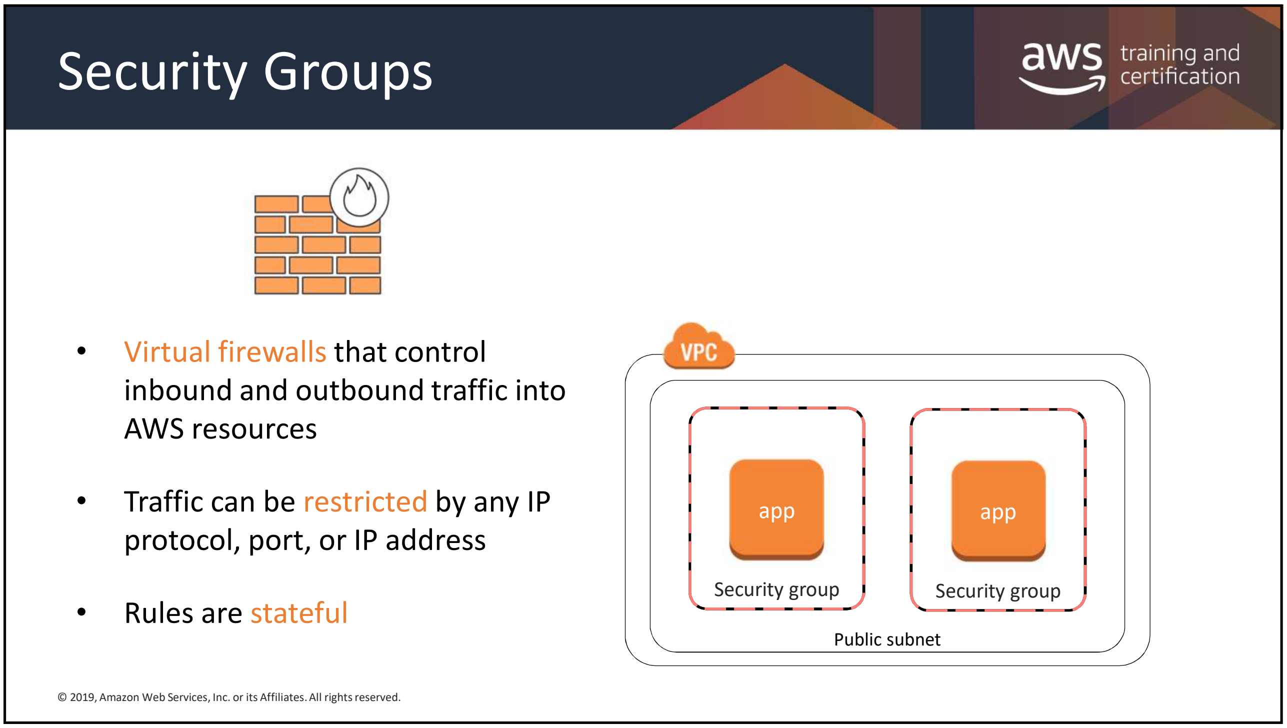
aws training and certification

- Can be associated with an instance or a network interface
- Able to re-associate and direct traffic immediately
- Five allowed per AWS Region



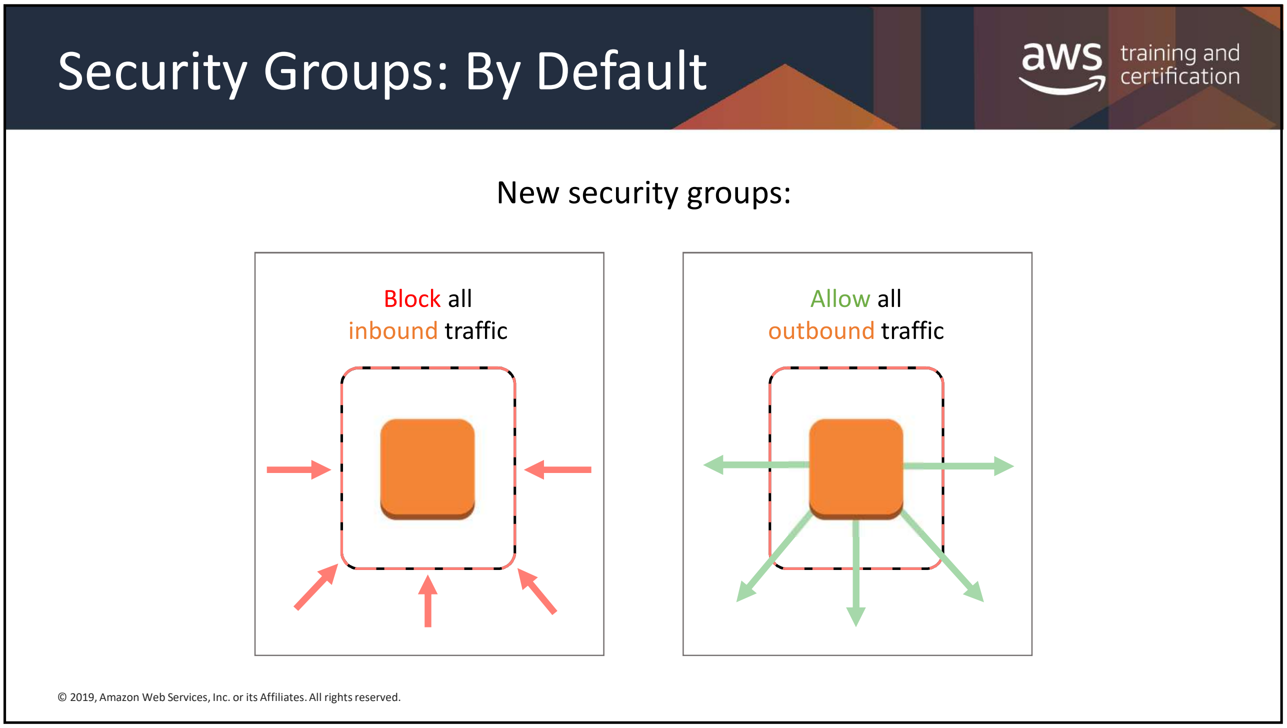
aws training and certification

Security in the Cloud



Security Groups

- Virtual firewalls that control inbound and outbound traffic into AWS resources
- Traffic can be restricted by any IP protocol, port, or IP address
- Rules are stateful



Security Groups: By Default

New security groups:

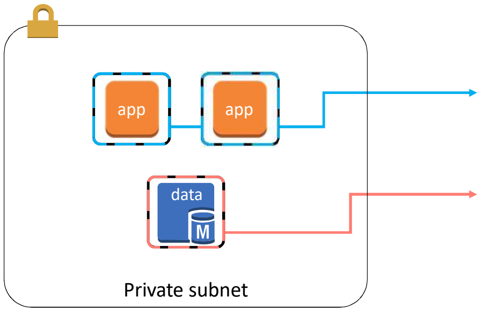
Block all inbound traffic

Allow all outbound traffic

Security Groups: Controlling Traffic

aws training and certification

Most cloud organizations create security groups with inbound rules for each functional tier.

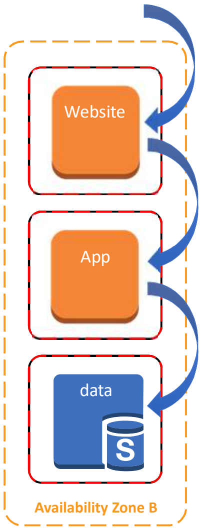


App tier security group

Data tier security group

Security Groups: Chaining Diagram

aws training and certification



Web tier
Security group

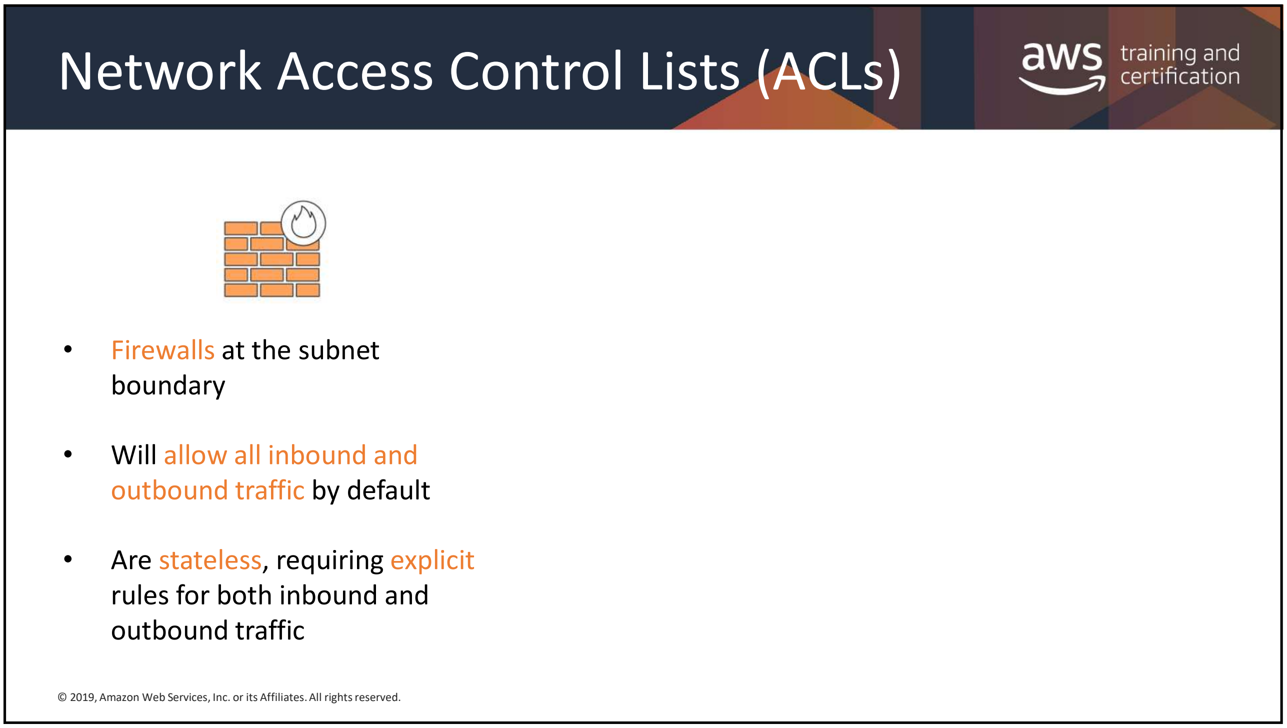
Application
Security group

Database
Security group

Inbound rule
Allow HTTPS port 443
Source: 0.0.0.0/0 (any)

Inbound rule
Allow HTTP port 80
Source: Web tier

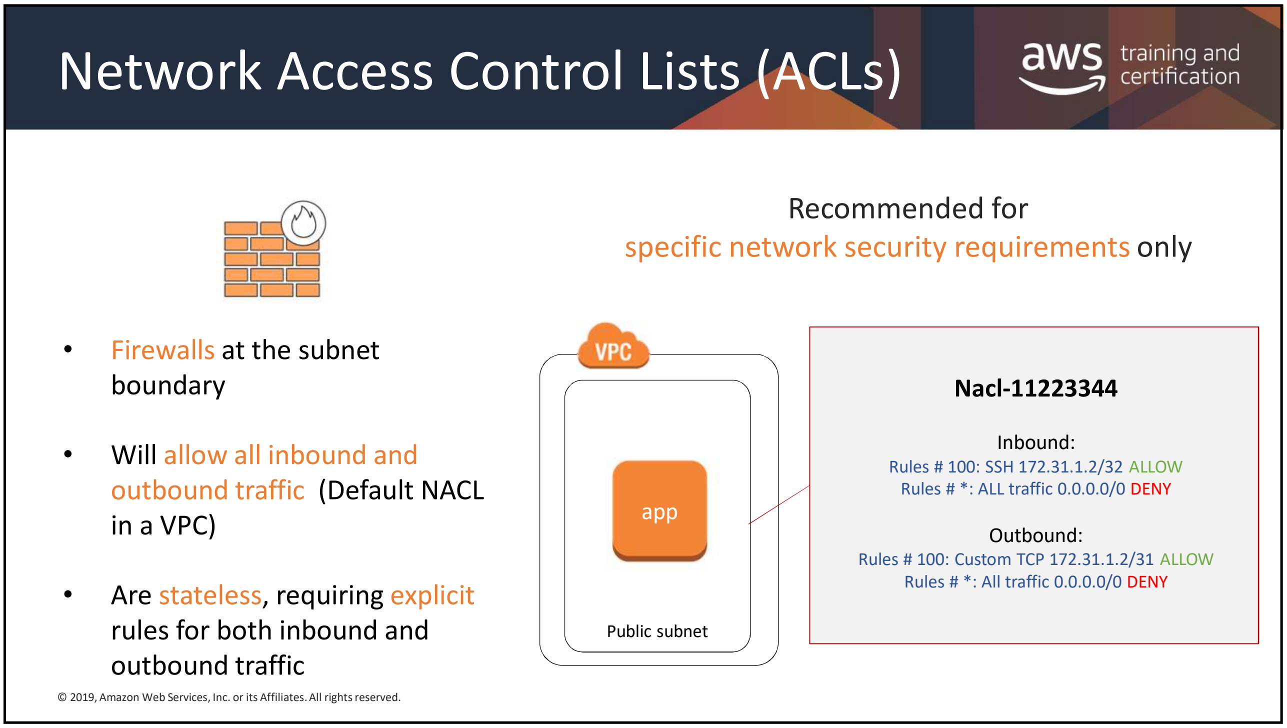
Inbound rule
Allow TCP port 3306
Source: App tier



Network Access Control Lists (ACLs)

aws training and certification

- Firewalls at the subnet boundary
- Will allow all inbound and outbound traffic by default
- Are stateless, requiring explicit rules for both inbound and outbound traffic



Network Access Control Lists (ACLs)

aws training and certification

- Firewalls at the subnet boundary
- Will allow all inbound and outbound traffic (Default NACL in a VPC)
- Are stateless, requiring explicit rules for both inbound and outbound traffic

Recommended for specific network security requirements only

Nacl-11223344

Inbound:
Rules # 100: SSH 172.31.1.2/32 ALLOW
Rules # *: ALL traffic 0.0.0.0/0 DENY

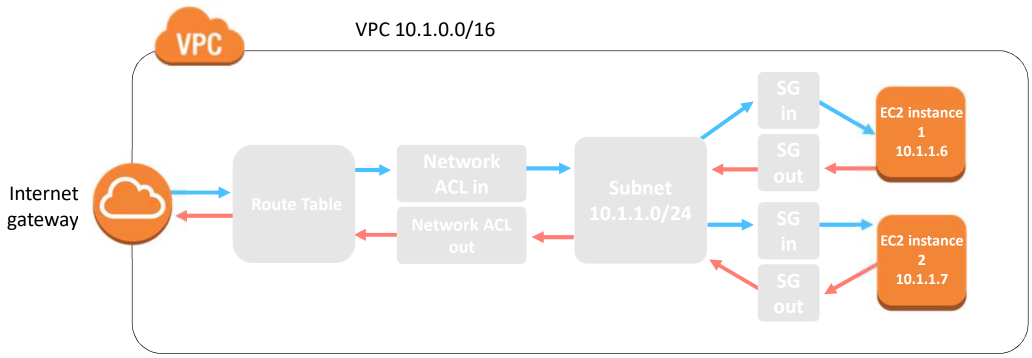
Outbound:
Rules # 100: Custom TCP 172.31.1.2/31 ALLOW
Rules # *: All traffic 0.0.0.0/0 DENY

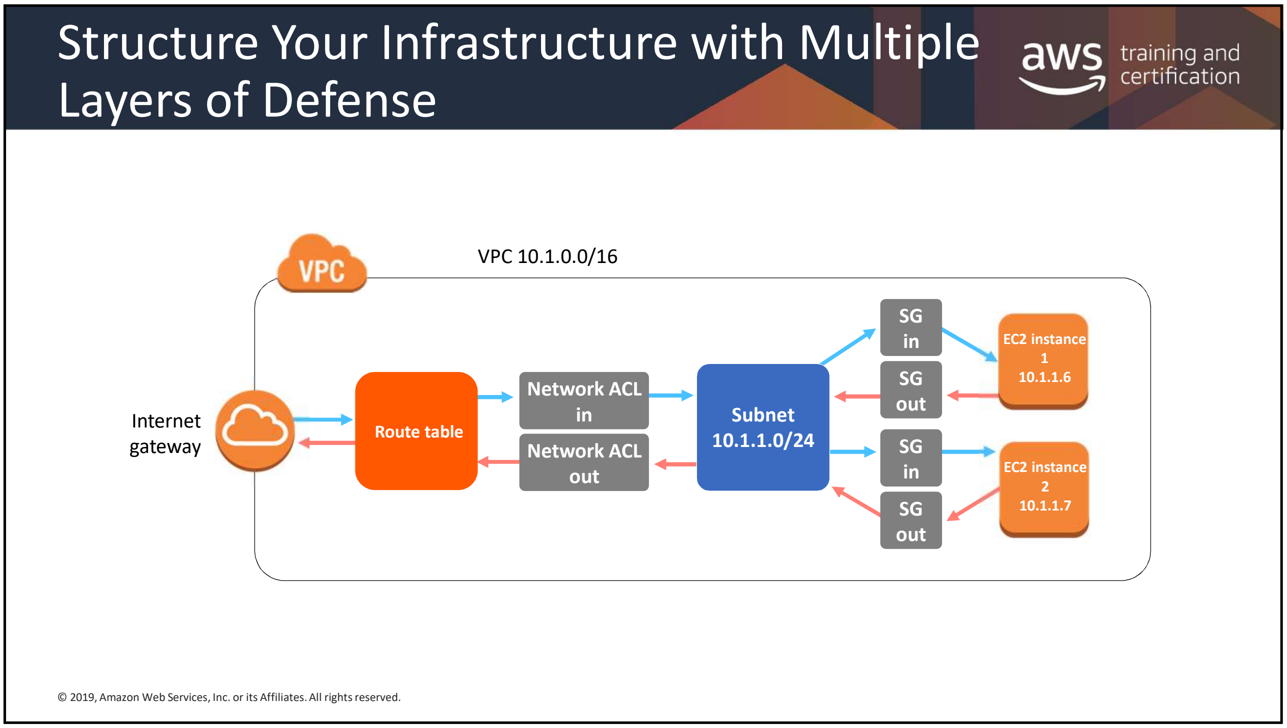
aws training and certification

Review

Structure Your Infrastructure with Multiple Layers of Defense

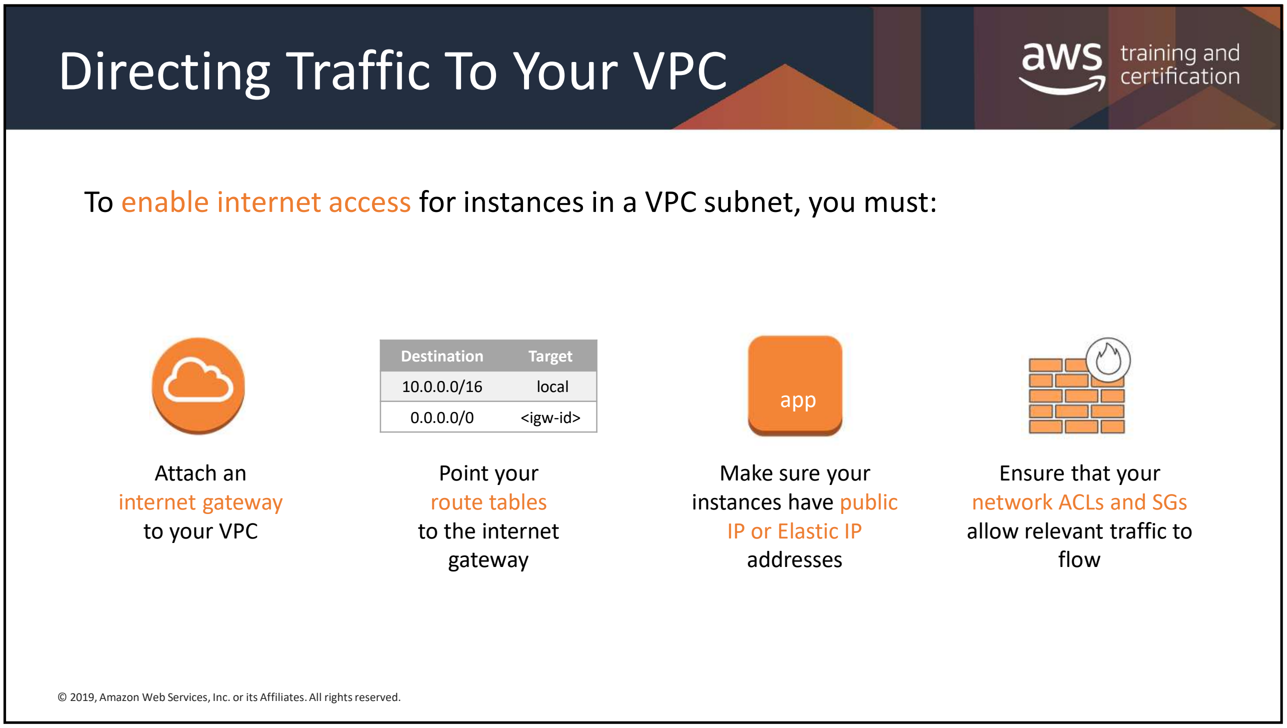
aws training and certification





Structure Your Infrastructure with Multiple Layers of Defense

aws training and certification



Directing Traffic To Your VPC

aws training and certification

To enable internet access for instances in a VPC subnet, you must:

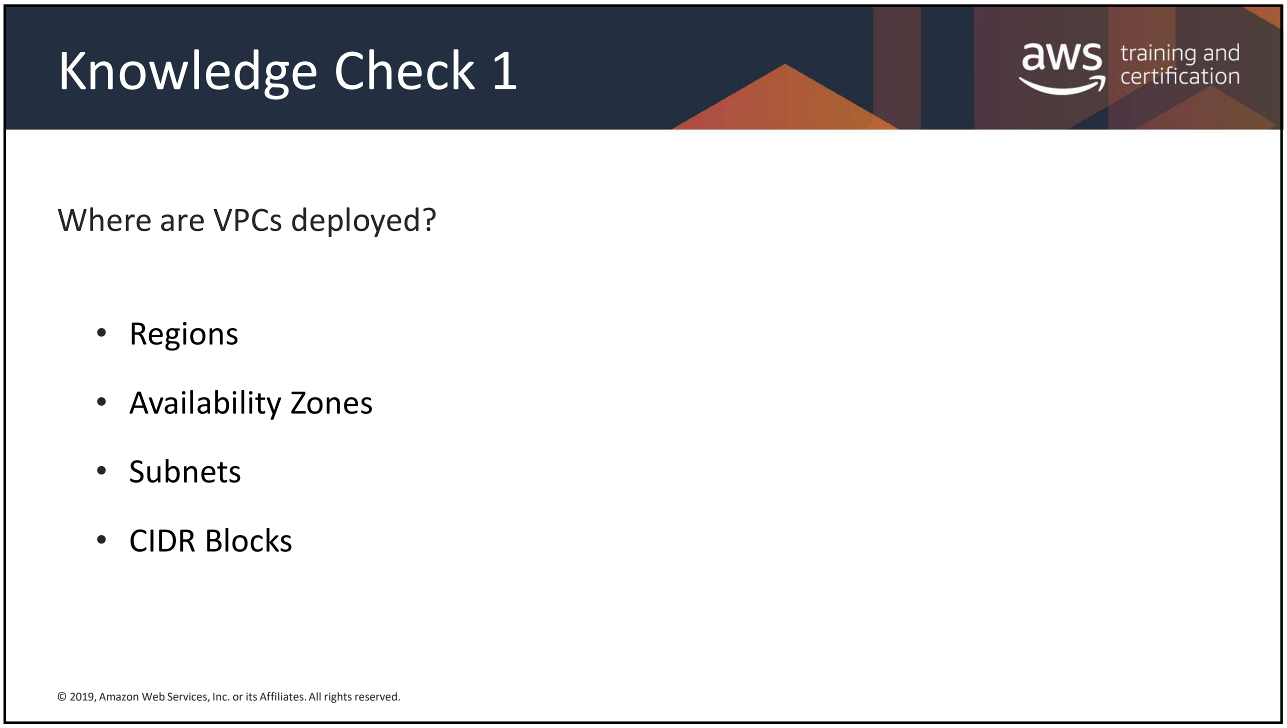
Attach an internet gateway to your VPC

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

Point your route tables to the internet gateway

Make sure your instances have public IP or Elastic IP addresses

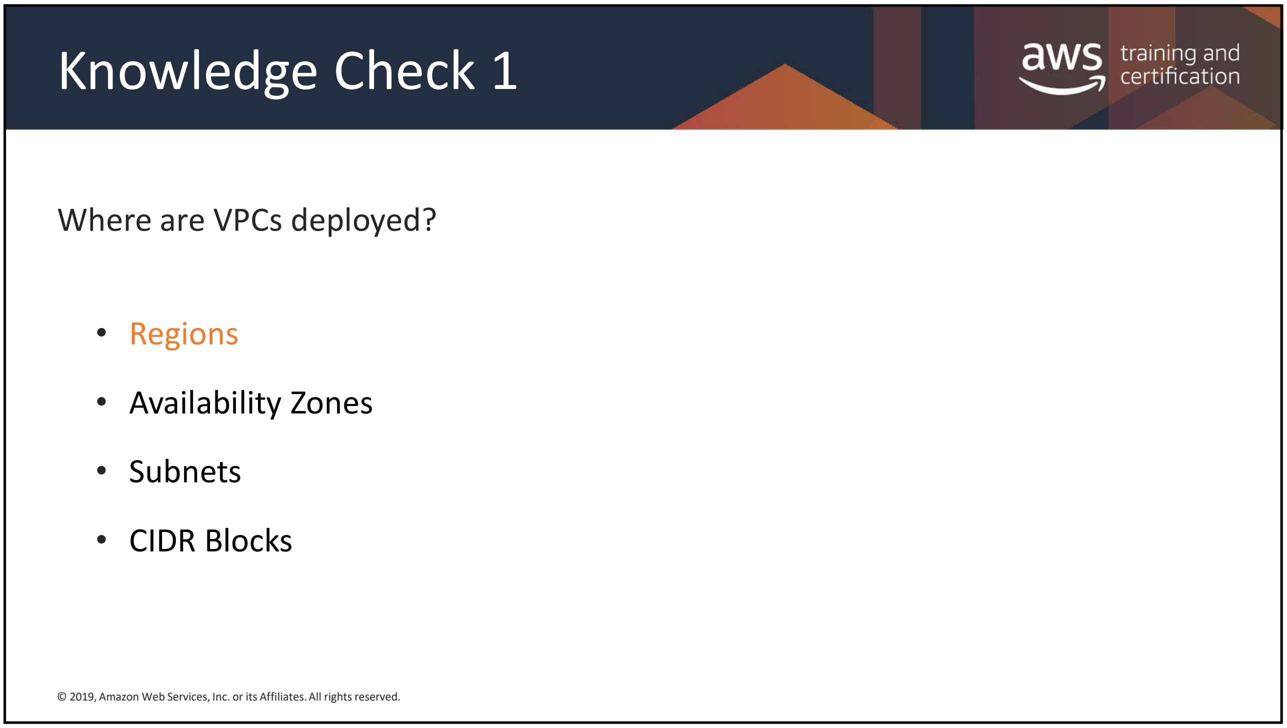
Ensure that your network ACLs and SGs allow relevant traffic to flow



Knowledge Check 1

Where are VPCs deployed?

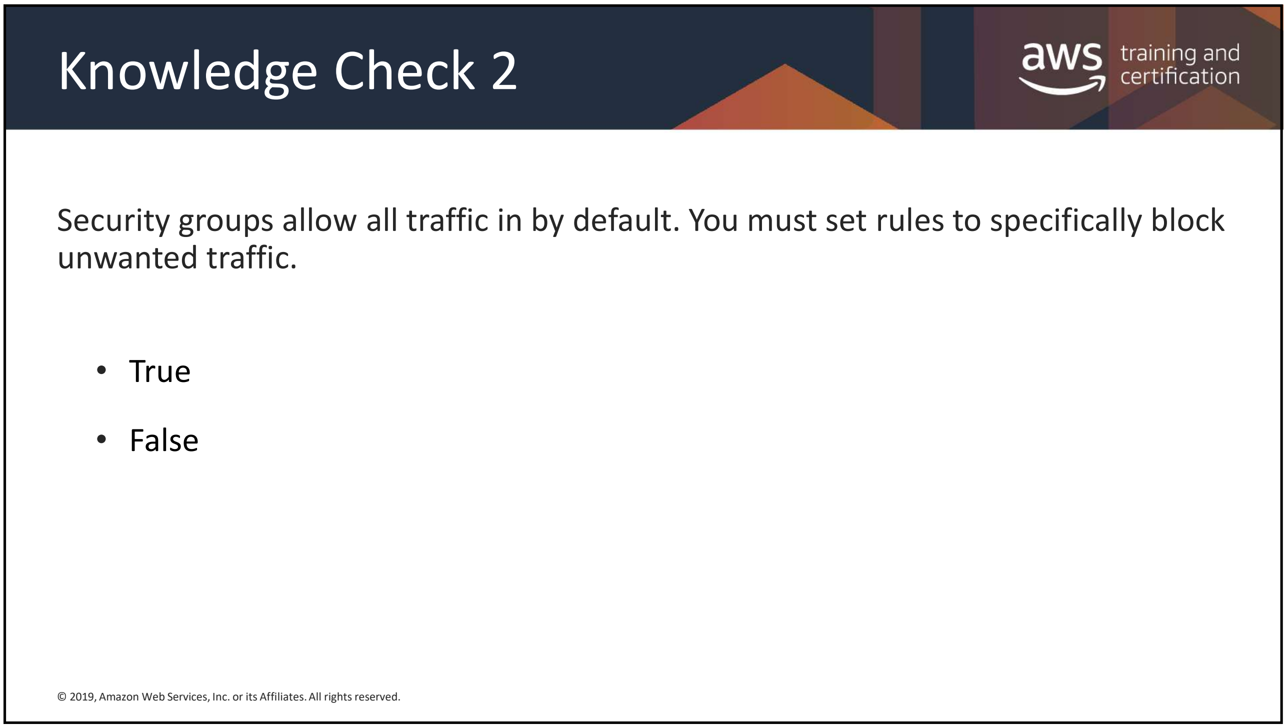
- Regions
- Availability Zones
- Subnets
- CIDR Blocks



Knowledge Check 1

Where are VPCs deployed?

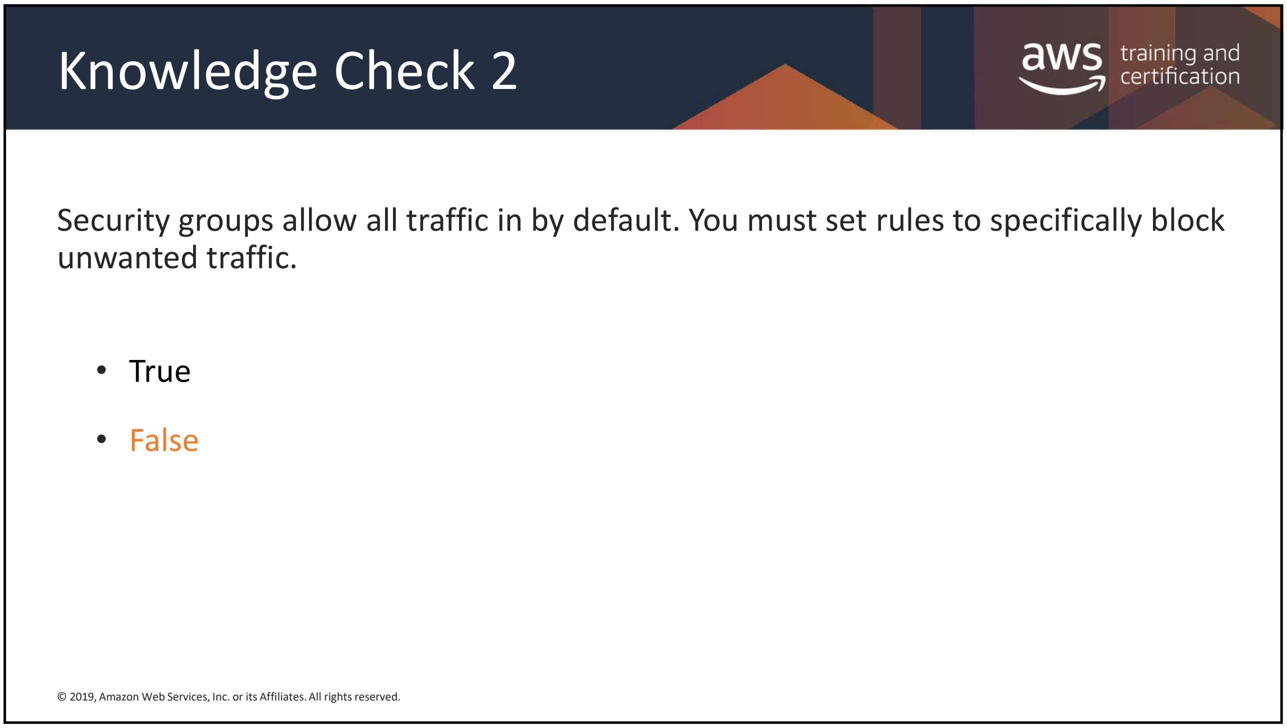
- **Regions**
- Availability Zones
- Subnets
- CIDR Blocks



Knowledge Check 2

Security groups allow all traffic in by default. You must set rules to specifically block unwanted traffic.

- True
- False



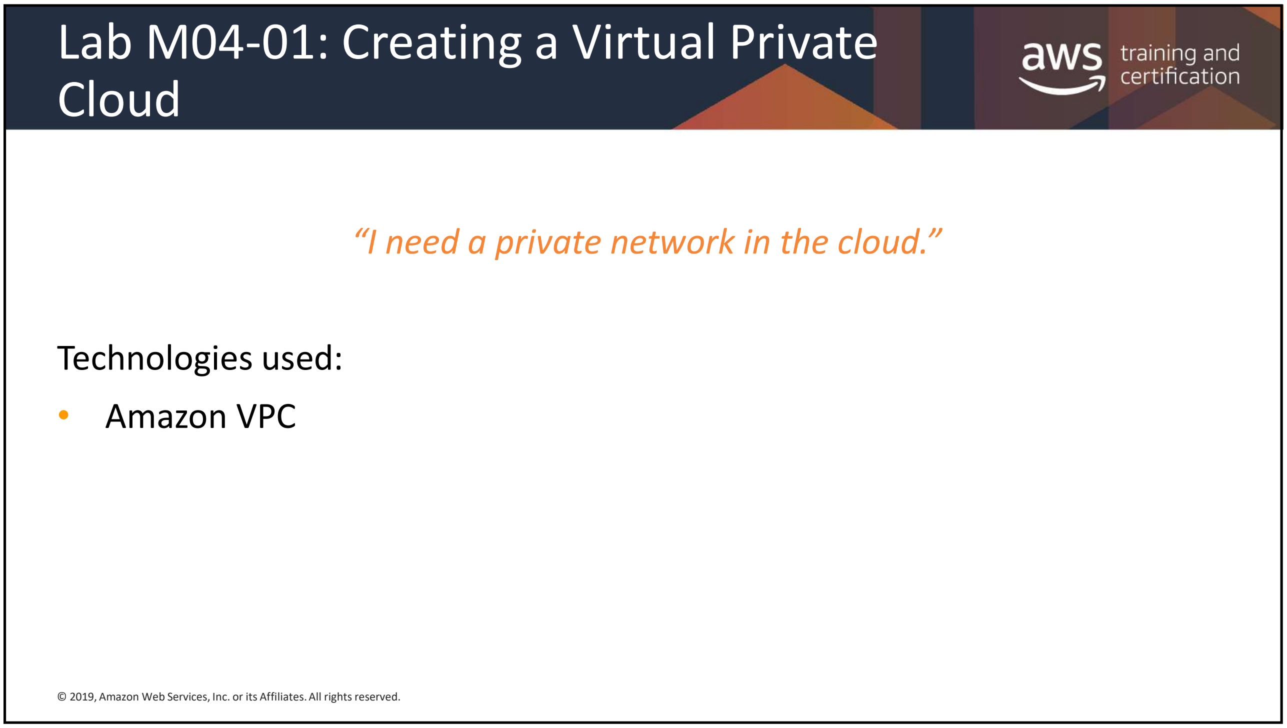
Knowledge Check 2

Security groups allow all traffic in by default. You must set rules to specifically block unwanted traffic.

- True
- False

aws training and certification

Lab M04-01: Creating a Virtual Private Cloud



Lab M04-01: Creating a Virtual Private Cloud

aws training and certification

“I need a private network in the cloud.”

Technologies used:

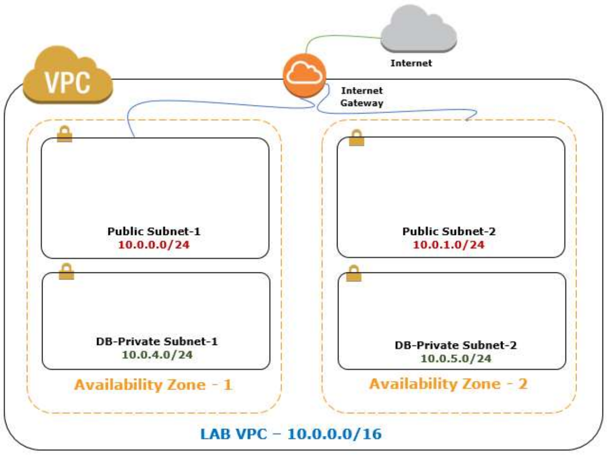
- Amazon VPC

Lab M04-01: Creating a Virtual Private Cloud

aws training and certification

You will create a VPC with:

- An internet gateway
- A public subnet
- A private subnet
- Route tables for each subnet



Duration: 20m

aws training and certification

Thank You