AWS Networking Tutorial

41492 – Engenharia de Software, Nuno Sá Couto e Rafael Direito
October 14th 2024

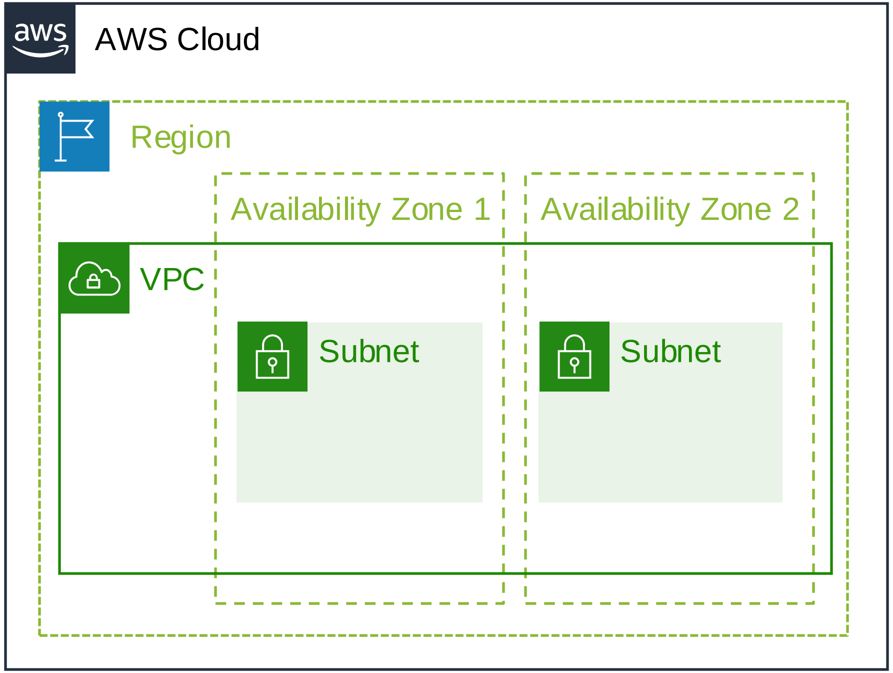
Amazon VPC

Amazon VPC

- Enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define
- Gives you control over your virtual networking resources, including:
  - Selection of IP address range
  - Creation of subnets
  - Configuration of route tables and network gateways
- Enables you to customize the network configuration for your VPC
- Enables you to use multiple layers of security

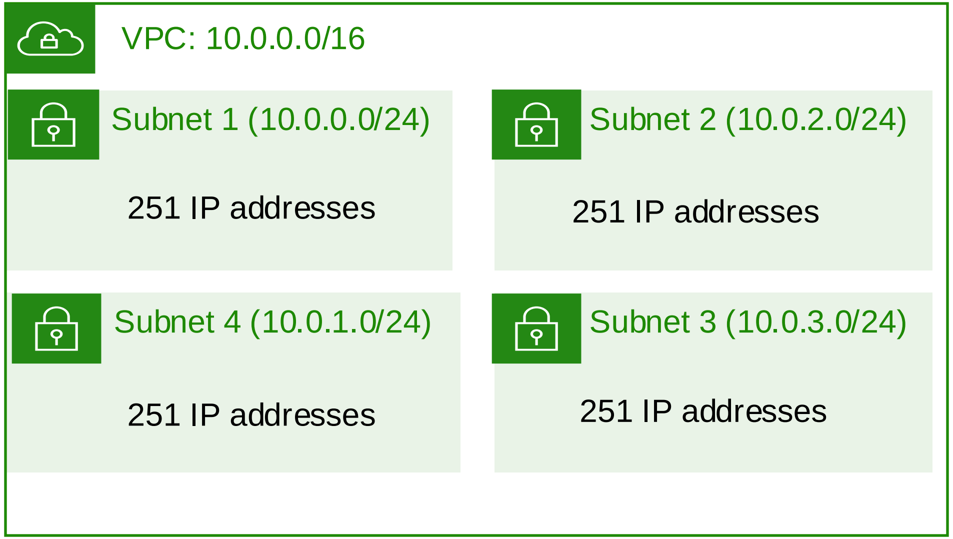
VPCs and subnets

- VPCs:
  - Logically isolated from other VPCs
  - Dedicated to your AWS account
  - Belong to a single AWS Region and can span multiple Availability Zones
- Subnets:
  - Range of IP addresses that divide a VPC
  - Belong to a single Availability Zone
  - Classified as public or private



Reserved IP addresses

Example: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four equal-sized subnets. Only 251 IP addresses are available for use by each subnet.



VPC: 10.0.0.0/16

Subnet 1 (10.0.0.0/24)

251 IP addresses

Subnet 2 (10.0.2.0/24)

251 IP addresses

Subnet 4 (10.0.1.0/24)

251 IP addresses

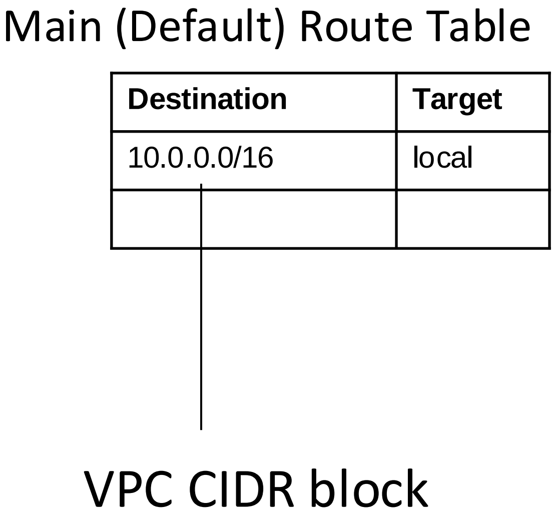
Subnet 3 (10.0.3.0/24)

251 IP addresses

IP Addresses for CIDR block 10.0.0.0/24	Reserved for
10.0.0.0	Network address
10.0.0.1	Internal communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future use
10.0.0.255	Network broadcast address

Route tables and routes

- A route table contains a set of rules (or routes) that you can configure to direct network traffic from your subnet.
- Each route specifies a destination and a target.
- By default, every route table contains a local route for communication within the VPC.
- Each subnet must be associated with a route table (at most one).

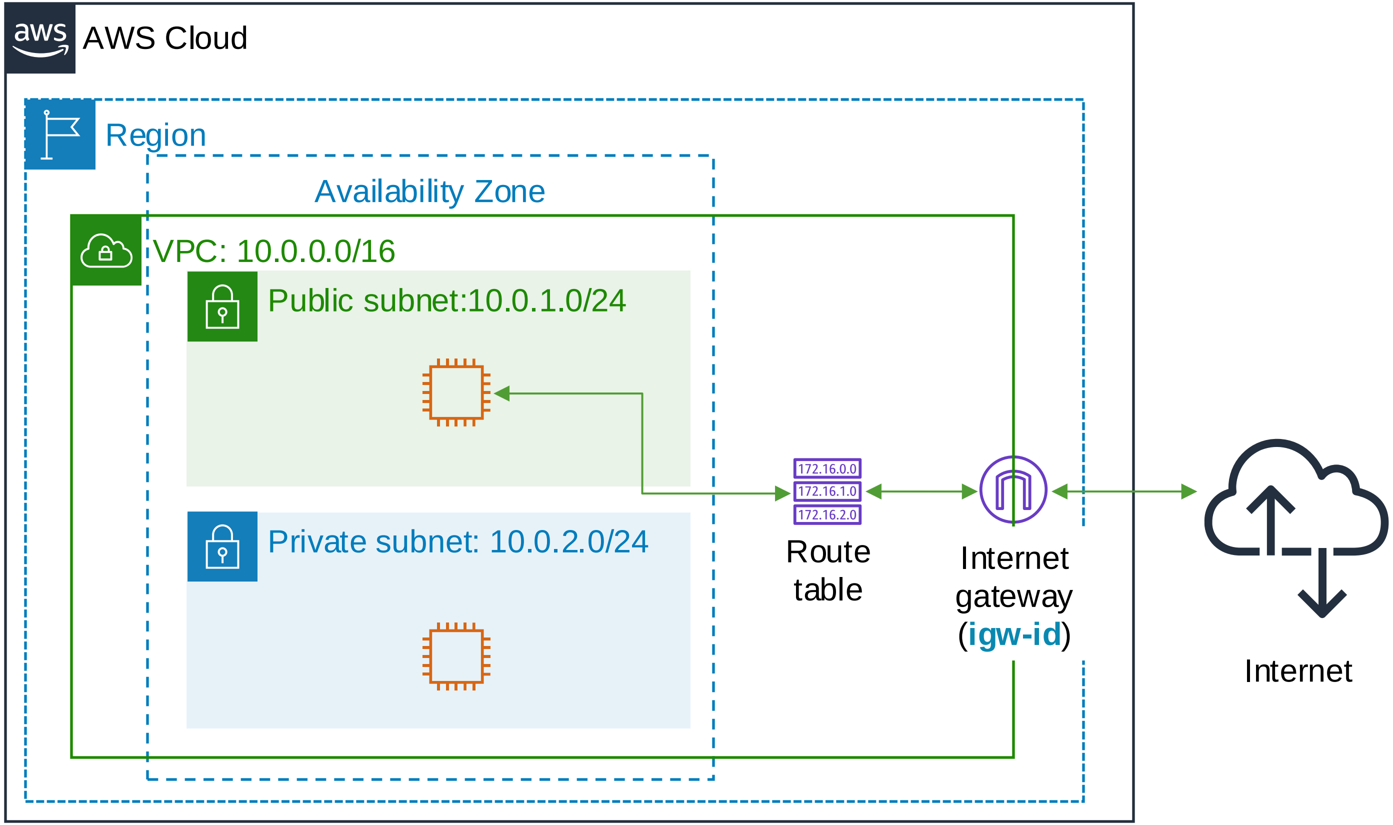


Main (Default) Route Table

Destination	Target
10.0.0.0/16	local

VPC CIDR block

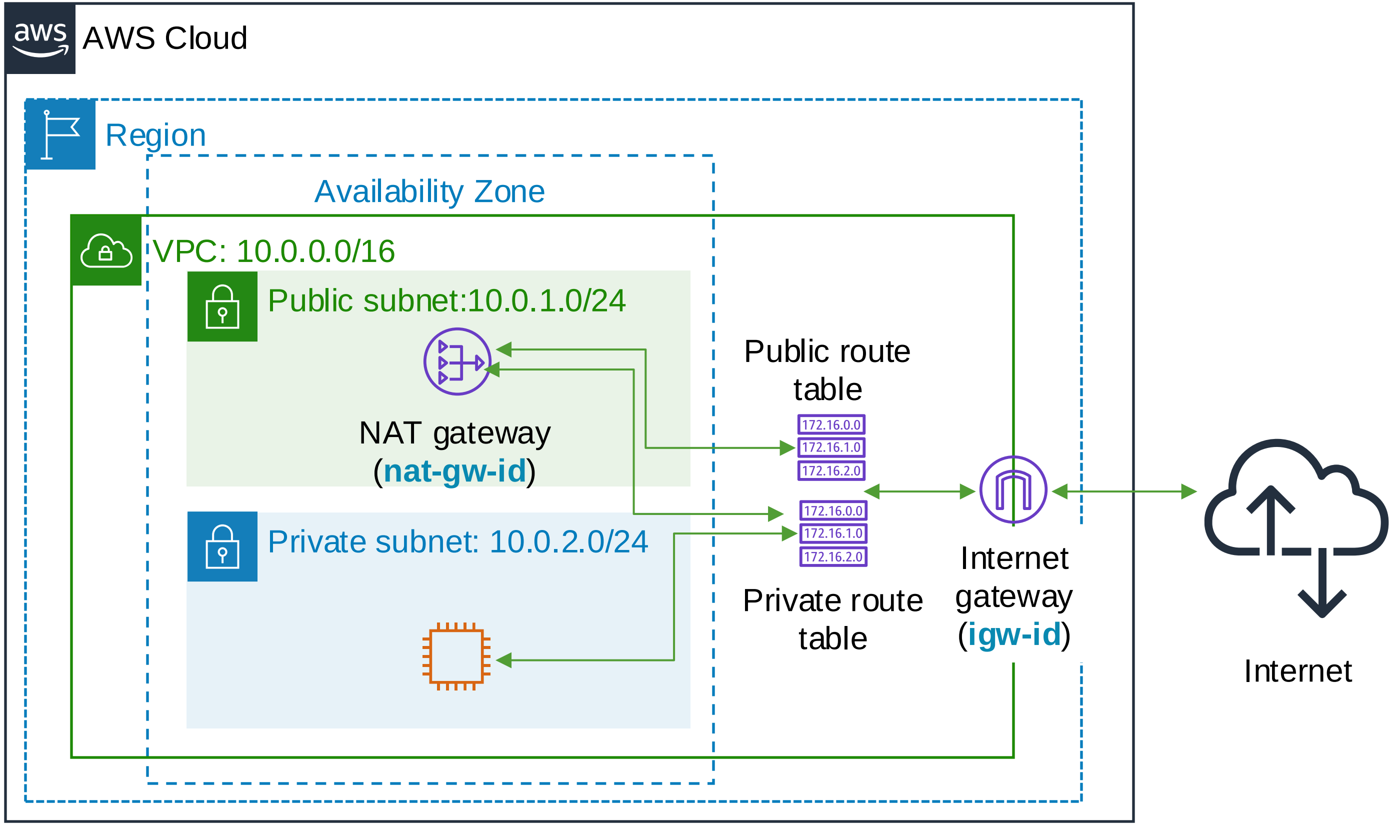
Internet gateway



Public Subnet Route Table

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

Network address translation (NAT) gateway



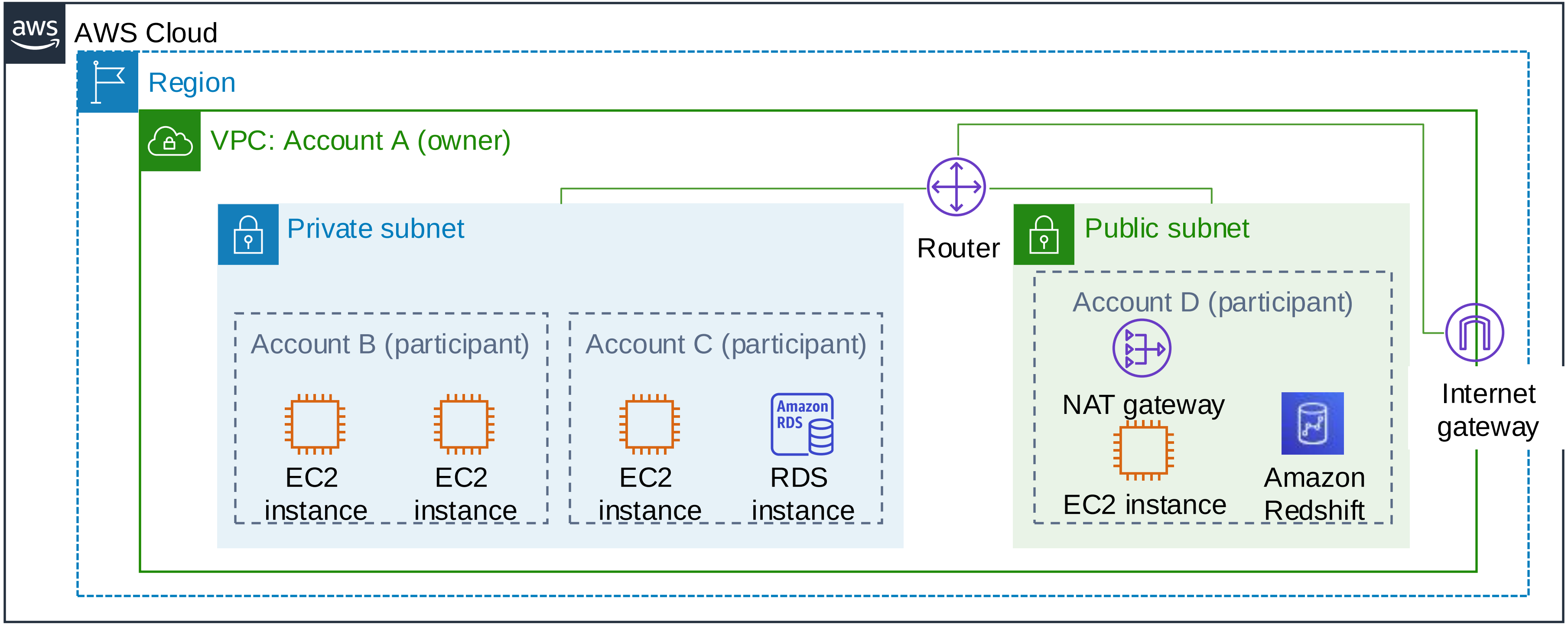
Public Subnet Route Table

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

Private Subnet Route Table

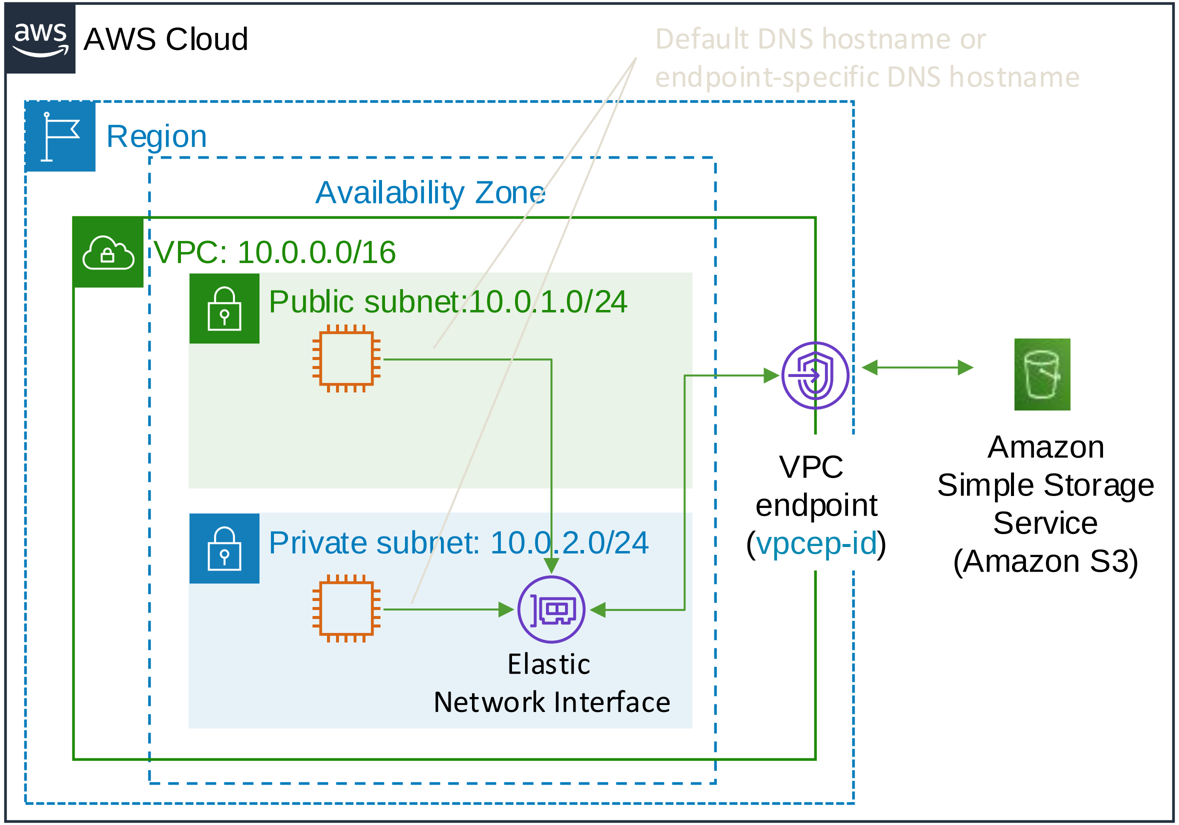
Destination	**Target**
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

VPC sharing



AWS Cloud
Region
VPC: Account A (owner)
Router
Private subnet
Account B (participant)
EC2 instance
EC2 instance
Account C (participant)
EC2 instance
Amazon RDS
RDS instance
Public subnet
Account D (participant)
NAT gateway
EC2 instance
Amazon Redshift
Internet gateway

VPC endpoints


AWS Cloud
Default DNS hostname or endpoint-specific DNS hostname
Region
Availability Zone
VPC: 10.0.0.0/16
Public subnet:10.0.1.0/24
Private subnet: 10.0.2.0/24
Elastic Network Interface
VPC endpoint (vpcep-id)
Amazon Simple Storage Service (Amazon S3)

Public Subnet Route Table

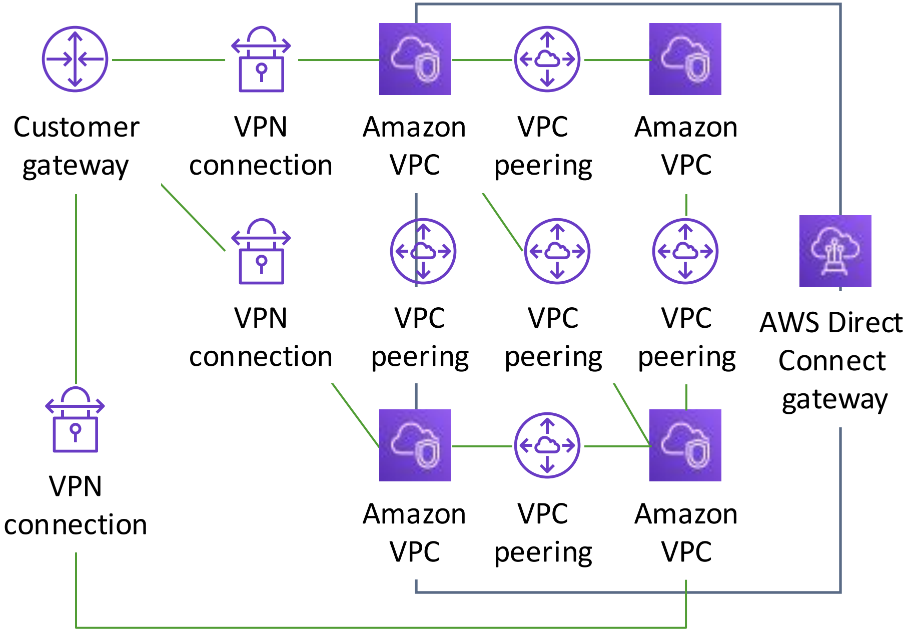
Destination	Target
10.0.0.0/16	local
Amazon S3 ID	vpcep-id

Two types of endpoints:

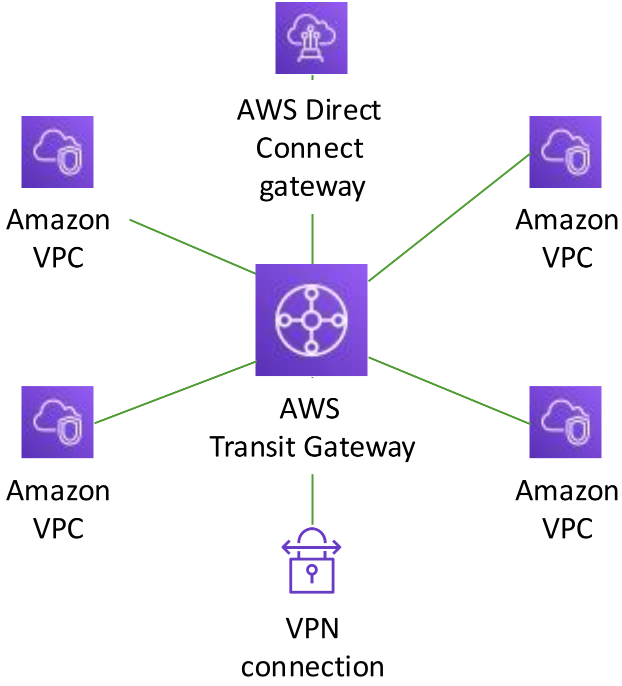
- **Interface** endpoints (powered by AWS PrivateLink)
- **Gateway** endpoints (Amazon S3 and Amazon DynamoDB)

AWS Transit Gateway

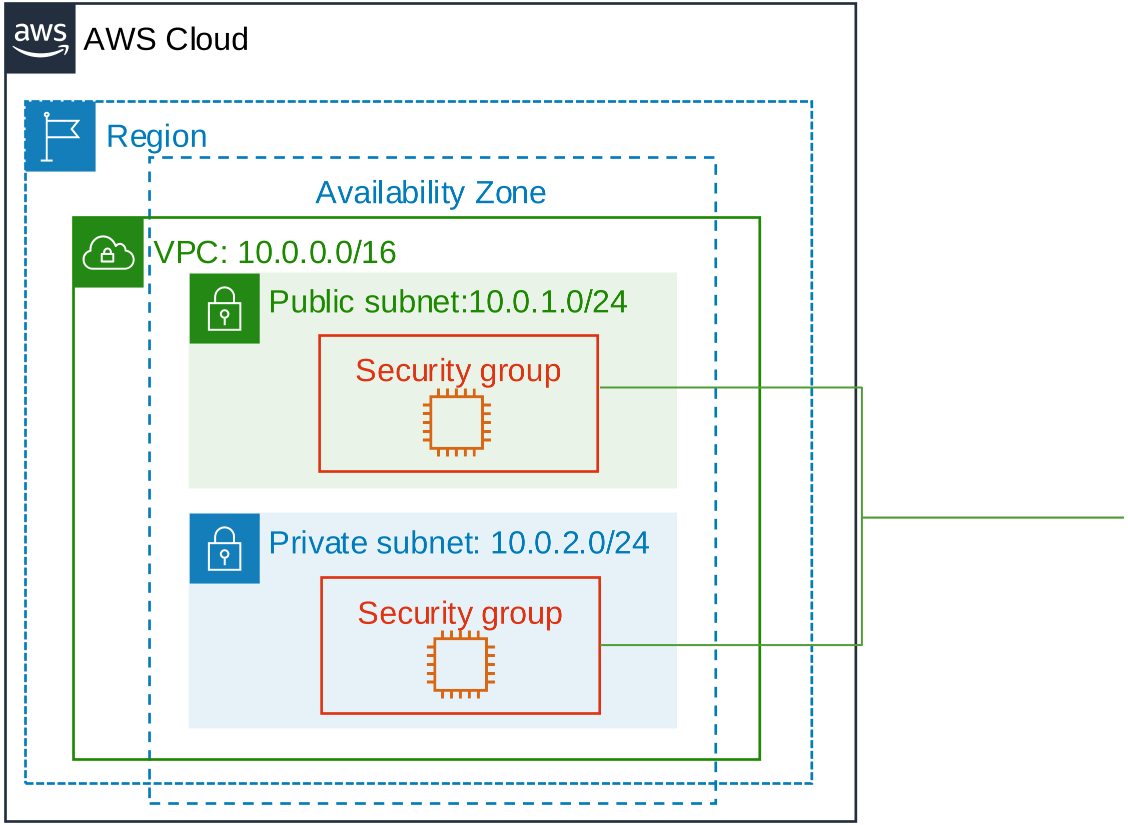
From this…



To this…



Security groups (1 of 2)



Security groups act at the instance level.

Security groups (2 of 2)

- Security groups have rules that control inbound and outbound instance traffic.
- Default security groups deny all inbound traffic and allow all outbound traffic.
- Security groups are stateful.

Inbound			
Source	**Protocol**	**Port Range**	**Description**
sg-*xxxxxxxx*	All	All	Allow inbound traffic from network interfaces assigned to the same security group.

Outbound			
Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic.

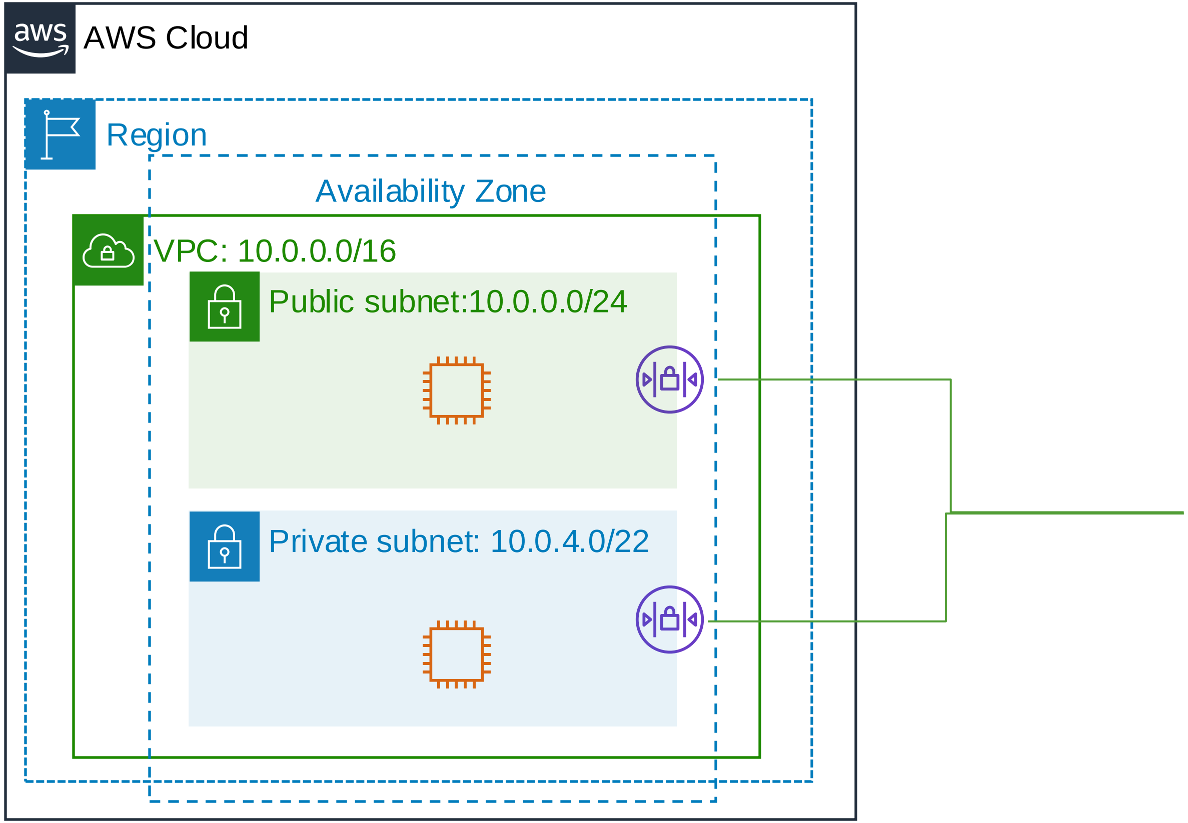
Custom security group examples

- You can **specify allow** rules, but not deny rules.
- **All rules are evaluated** before the decision to allow traffic.

Inbound			
Source	**Protocol**	**Port Range**	**Description**
0.0.0.0/0	TCP	80	Allow inbound HTTP access from all IPv4 addresses
0.0.0.0/0	TCP	443	Allow inbound HTTPS access from all IPv4 addresses
Your network's public IPv4 address range	TCP	22	Allow inbound SSH access to Linux instances from IPv4 IP addresses in your network (over the internet gateway)

Outbound			
Destination	Protocol	Port Range	Description
The ID of the security group for your Microsoft SQL Server database servers	TCP	1433	Allow outbound Microsoft SQL Server access to instances in the specified security group

Network access control lists (network ACLs 1 of 2)



Network ACLs act at the **subnet level**.

Network access control lists (network ACLs 2 of 2)

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Default network ACLs allow all inbound and outbound IPv4 traffic.
- Network ACLs are stateless.

Inbound					
Rule	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound					
Rule	**Type**	**Protocol**	**Port Range**	**Destination**	**Allow/Deny**
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Lab 2: Scenario

In this lab, you use Amazon VPC to create your own VPC and add some components to produce a customized network. You create a security group for your VPC. You also create an EC2 instance and configure it to run a web server and to use the security group. You then launch the EC2 instance into the VPC.

Amazon VPC

Amazon EC2

Lab 2: Tasks

- Create a VPC.
- Create additional subnets.
- Create a VPC security group.
- Launch a web server instance.

Security group

[RECAP] Concepts/Components

Describe the following AWS components and the functionality they provide:

- **VPC**
- **Region**
- **Availability Zone**
- **Private Network**
- **Public Network**
- **NAT**
- **Internet Gateway**
- **Security Group**

[RECAP] Concepts/Components

VPC

- An AWS VPC allows you to create an **isolated section of the AWS cloud where you can define your own virtual network**. It provides control over IP address ranges, subnets, route tables, and network gateways within that virtual environment.

Region

- **An AWS region is a physical geographical location that has multiple, independent data centers called Availability Zones.** Each AWS region is fully isolated to ensure maximum resilience and fault tolerance.

Availability Zone (AZ)

- **Availability Zones are individual data centers within a region, each isolated but connected with low-latency networking.** An AZ is physically separated from other AZs, reducing the risk of data loss in case of an outage in one AZ.

[RECAP] Concepts/Components

Private Network

- A Private Network within a VPC refers to **subnets and resources that are not directly accessible from the internet**, often used for backend services, databases, or sensitive applications.

Public Network

- In AWS, a public network is typically a **subnet that allows resources to communicate with the internet via an Internet Gateway**. **Resources in public networks can be accessed directly from the internet** if appropriately configured.

NAT (Network Address Translation) Gateway:

- A NAT Gateway **allows instances in a private subnet to connect to the internet or other AWS services but prevents external systems from initiating a connection back** to those instances.

[RECAP] Concepts/Components

Internet Gateway

- An Internet Gateway is a component that **enables internet communication for instances within VPC public subnets**. It connects the VPC to the internet and manages traffic flow in and out of the VPC.

Security Group

- Security Groups in AWS act as **virtual firewalls for your instances to control both inbound and outbound traffic**. They are associated with resources like EC2 instances, allowing you to specify permitted traffic based on protocols, ports, and IP ranges.

Recap Quiz

What is the purpose of an Internet Gateway in a VPC?

a) To allow communication between subnets
● b) To enable instances in a public subnet to connect to the internet
c) To provide NAT services for private subnets
d) To connect multiple VPCs

Which of the following is true about security groups?

a) They operate at the subnet level
b) They are stateless
● c) They support allow rules only
d) They can only have outbound rules

What is the main difference between a NAT Gateway and an Internet Gateway?

● a) NAT Gateway allows internet access for private instances, while Internet Gateway is for public instances
b) NAT Gateway is used for VPC peering, while Internet Gateway is for internet access
c) NAT Gateway is cheaper than Internet Gateway
d) There is no difference; they serve the same purpose

Recap Quiz

What is the primary function of a Network Access Control List (NACL) in a VPC?

a) To provide instance-level security
● b) To filter traffic at the subnet level
c) To route traffic between public and private subnets
d) To manage access to internet gateways

Which of the following is a key difference between Security Groups and Network Access Control Lists (NACLs)?

a) Security groups are stateless, while NACLs are stateful
b) Security groups operate at the subnet level, while NACLs operate at the instance level
● c) Security groups only support allow rules, while NACLs support both allow and deny rules
d) Security groups are associated with NAT Gateways, while NACLs are associated with Internet Gateways

Group Discussion

An enterprise is deploying a three-tier application (web, application, and database tiers) across multiple Availability Zones for high availability.
Explain how you would design the VPC architecture to support this setup.

Topics to address:

- VPC and Subnets (Public and Private)
- Availability Zones
- Internet Access, if needed
- Routing
- Security (Security Groups and NACLs)

Group Discussion

VPC and Subnets:

- Use multiple AZs for high availability. For example, if you have three AZs (AZ-A, AZ-B, AZ-C), create one subnet per tier in each AZ.
- Public Subnets for the Web Tier: Place the web servers in public subnets to make them accessible to the internet.
- Private Subnets for the Application and Database Tiers: Place application and database servers in private subnets to restrict direct internet access.

Internet and NAT Gateways:

- Attach an internet gateway to the VPC for instances in public subnets to communicate with the internet.
- Deploy a NAT gateway in each public subnet in different AZs. This allows instances in private subnets to access the internet (e.g., for updates) without exposing them directly to incoming internet traffic.

Group Discussion

Routing:

- Public Subnet Route Tables: Associate route tables with public subnets to route internet-bound traffic through the internet gateway.
- Private Subnet Route Tables: Associate route tables with private subnets (application and database tiers) to route internet-bound traffic through the NAT gateways, keeping incoming traffic secure.

Security:

- Web Tier Security Group: Allows HTTP/HTTPS traffic from the internet to the web servers.
- Application Tier Security Group: Allows traffic from the web tier security group on specific ports (e.g., HTTP on port 80 if using HTTP internally).
- Database Tier Security Group: Allows only traffic from the application tier on the database port (e.g., MySQL on port 3306).
- Optionally, configure Network ACLs for additional security at the subnet level, defining rules for inbound and outbound traffic.

Group Discussion

Load Balancing and High Availability:

- Application Load Balancer (ALB): Deploy an ALB in the public subnets across all AZs to balance traffic across the web servers. This allows users to access the application from the internet.
- Auto Scaling Groups: Set up auto-scaling groups for both the web and application tiers, spanning multiple AZs. This ensures high availability and scales the application to handle varying loads.

Database High Availability:

- Amazon RDS Multi-AZ: For the database tier, use Amazon RDS with Multi-AZ deployment or Amazon Aurora for high availability and automatic failover. This ensures that the database is available even if one AZ fails.

Cloud Network Planning

Lab - Configure your VPC

- The VPC must have **1 Public Network**
  - VMs should be automatically assigned a public IP
  - VMs should be able to access other VMs on the Private Network
  - VMs should be able to access the internet
  - VMs should be accessible from the internet
- The VPC must have **1 Private Network**
  - VMs should be able to access other VMs on the Public Network
  - VMs should be able to access the internet
  - VMs cannot be accessible from the internet

Cloud Network Planning

Exercise: Configure your VPC

- The VPC must have **1 Public Network**
  - VMs should be automatically assigned a public IP
  - VMs should be able to access other VMs on the Private Network
    - **How to enforce this?**
  - VMs should be able to access the internet
    - **How to enforce this?**
  - VMs should be accessible from the internet
    - **How to enforce this?**

Which Components do you have to configure?

Why?

Cloud Network Planning

Exercise: Configure your VPC

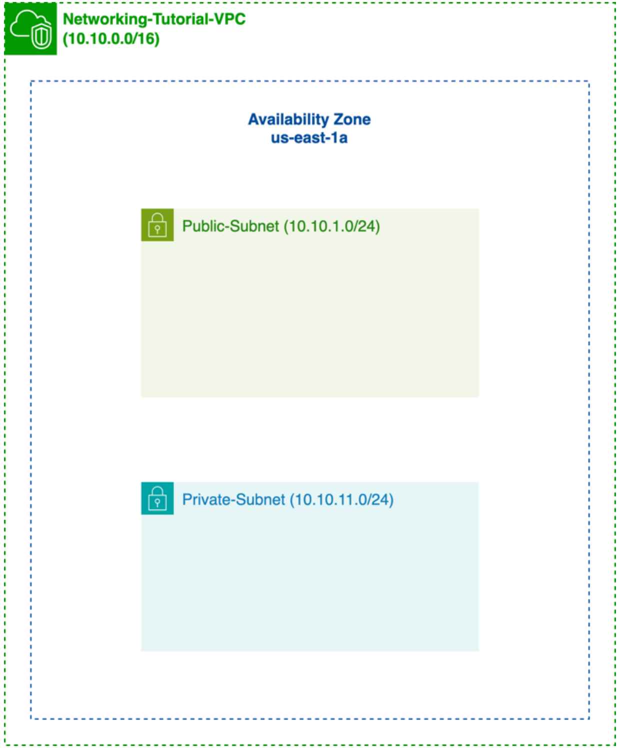
- The VPC must have **1 Private Network**
  - VMs should be able to access other VMs on the Public Network
    - **How to enforce this?**
  - VMs should be able to access the internet
    - **How to enforce this?**
  - VMs cannot be accessible from the internet
    - **How to enforce this?**

Which Components do you have to configure?

Why?

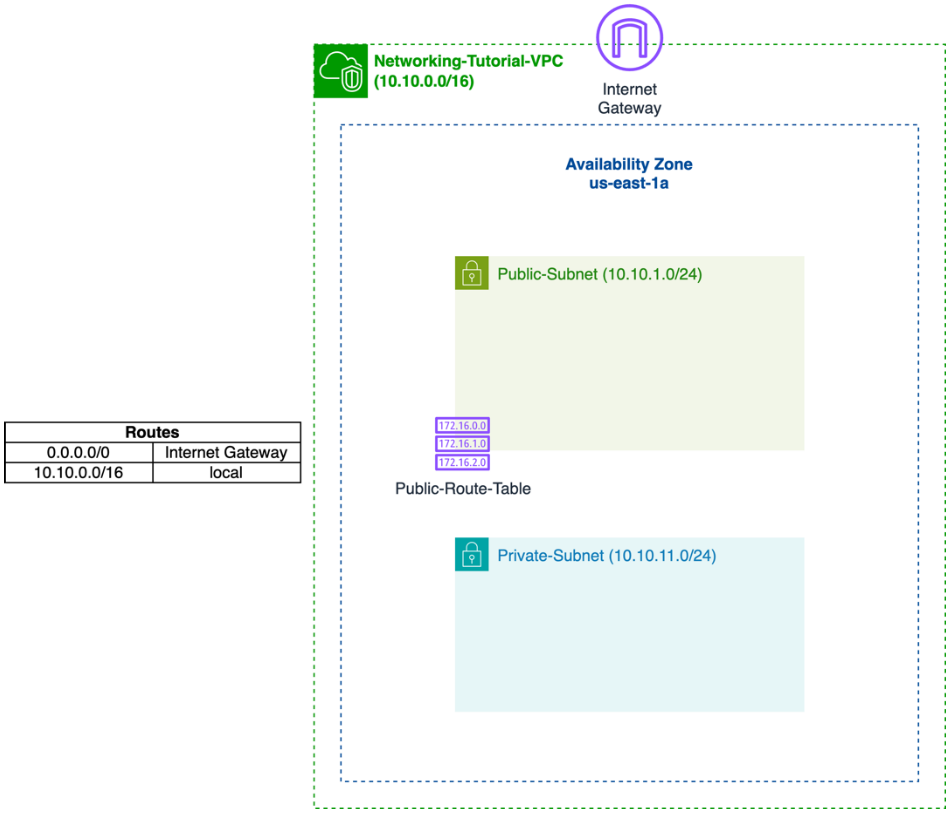
Cloud Network Planning

Base Scenario



Cloud Network Planning

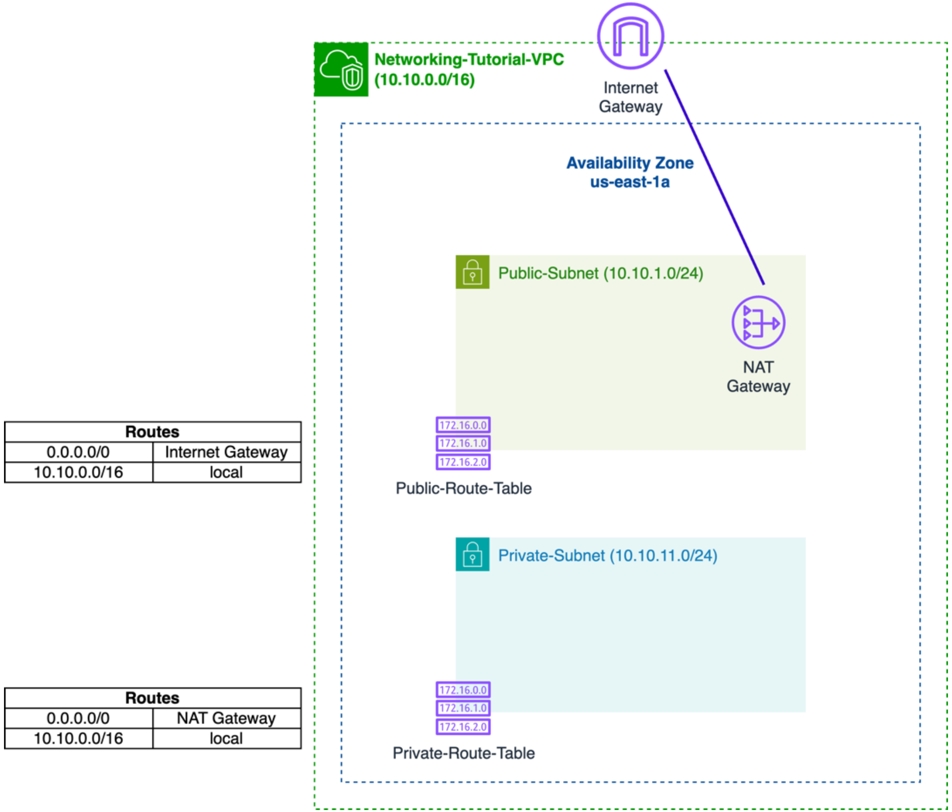
- VMs on the Public Subnet can access the Internet
- Communication between VMs on the Private and Public Subnets is possible
- VMs on the Public Subnet are accessible from the Internet



Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Cloud Network Planning

- VMs on the Public Subnet can access the Internet
- Communication between VMs on the Private and Public Subnets is possible
- VMs on the Public Subnet are accessible from the Internet
- VMs on the Private Subnet can reach the Internet
- VMs on the Private Subnet cannot be reached from the internet



Networking-Tutorial-VPC (10.10.0.0/16)
Internet Gateway
Availability Zone us-east-1a
Public-Subnet (10.10.1.0/24)
NAT Gateway
172.16.0.0
172.16.1.0
172.16.2.0
Public-Route-Table
Private-Subnet (10.10.11.0/24)
172.16.0.0
172.16.1.0
172.16.2.0
Private-Route-Table

Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway
10.10.0.0/16	local

Implementation

1 - Create Your VPC

Resources to Create	VPC Only
Name	networking-tutorial
IPv4 CIDR block	10.10.0.0/16
IPv6 CIDR block	No
Tenancy	Default

2 - Create a Private Subnet

VPC	networking-tutorial
Name	private-subnet-us-east-1a
Availability Zone	us-east-1a
IPv4 CIDR block	10.10.11.0/24

Implementation

3 - Create a Public Network

VPC	networking-tutorial
Name	public-subnet-us-east-1a
Availability Zone	us-east-1a
IPv4 CIDR block	10.10.1.0/24

4 - Edit the Public Subnet to enable Public IPv4 Auto-Assignment

Actions > Edit Subnet Settings
Check : Enable auto-assign public IPv4 address

Implementation

5 - Create an Internet Gateway

Name	Internet-gw

After its creation, attach it to the networking-tutorial VPC

6 - Create a VPC Endpoint

VPC	networking-tutorial
Name	ec2-endpoint
Service Category	EC2 Instance Connect Point
Security Groups	VPC Default Security Group (Allow ALL) - INSECURE
Subnet	public-subnet-us-east-1a (Must be on public network, with a public IP)

Not required when using AWS Academy

Implementation

7 - Create a Route Table for the Public Subnet

Name	public-route-table
VPC	networking-tutorial
Subnet Associations	public-subnet-us-east-1a
Routes	Destination: 0.0.0.0/0 Target: Internet Gateway Internet Gateway: internet-gw

Public Network - Testing

PubN - T1 - Create a Security Group for EC2 Instance

Security Group Name	all_open
Description	This Security Group is VERY INSECURE
VPC	networking-tutorial
Outbound Rules	(Leave as is)
Inbound Rules	Type: All Traffic Source: Anywhere-IPv4

PubN – T2 - Create a SSH Key To Access EC2 Instances

Name	ec2-key
Key Pair Type	RSA
File Format	.pem

Save the key locally !

Public Network - Testing

PubN – T3 - Create a Public EC2 Instance

Name	public-ec2-1
Amazon Machine Image	Ubuntu
Architecture	64-bit
Instance Type	t2.micro
VPC	networking-tutorial
Subnet	public-subnet-us-east-1a
Key Pair	ec2-key
Auto-assign public IP	Enable
Security Group	all_open
Storage	8GiB

Advanced Details > User Data:

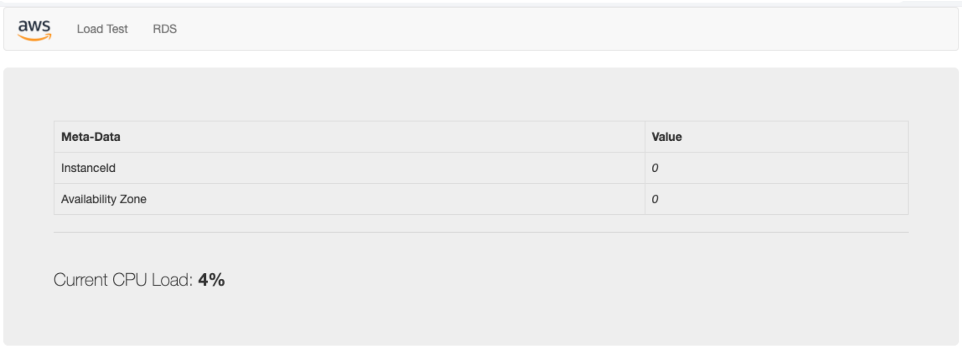
```
#! /bin/bash
apt update
apt install -y apache2 wget php mariadb-server unzip -y
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
service apache2 start
```

This script should bootstrap an Apache2 server inside the VM.
You may access the webserver via http://<public_ip>/index.php

Public Network - Testing

PubN – T4 - Validate the Public EC2 Instance

- Confirm that the EC2 Instance was assigned a Public IP
- Ping the VM's Public IP from your PC (should work!) - This means that Internet Traffic can reach the VM
- Connect to the instance via the EC2 Instance via EC2 Instance Connect (username: ubuntu)
- Validate that the apache2 webserver is running (sudo service apache2 status) If the server is running, try to access it through your browser (http://<public_ip>/index.php). You should see something like this:



Meta-Data	Value
InstanceId	*0*
Availability Zone	*0*

Current CPU Load: **4%**

Public Network - Testing

PubN – T4 - Validate the Public EC2 Instance

- Try to access the VM from your local machine (via SSH)
- You will need the .pem key that you previously created (ec2-key.pem)
- In your machine:

```
sudo chmod 400  ~/Downloads/ec2-key.pem
ssh -i ~/Downloads/ec2-key.pem ubuntu@34.228.167.2
```

Implementation

8 - Create NAT Gateway for the Private Subnet

Name	nat-gw
Subnet	public-subnet-us-east-1a (The NAT must have a public IP!)
Connectivity Type	Public
Elastic IP Allocation ID	Allocate a new Elastic IP

9 - Create a Route Table for the Private Subnet

Name	private-route-table
VPC	networking-tutorial
Subnet Associations	private-subnet-us-east-1a
Routes	Destination: 0.0.0.0/0 Target: NAT GW Internet Gateway: nat-gw

Private Network - Testing

PrivN – T1 - Create a Public EC2 Instance

Name	private-ec2-1
Amazon Machine Image	Ubuntu
Architecture	64-bit
Instance Type	t2.micro
VPC	networking-tutorial
Subnet	private-subnet-us-east-1a
Key Pair	ec2-key
Security Group	all_open
Storage	8GiB

In AWS Academy, to be able to access a private instance, you have to attach an IAM Role to it.

Advanced Details > IAM Instance Profile (Select LabInstanceProfile)

You must do this while creating the instance!

Private Network - Testing

PrivN – T2 - Connect to the private EC2 Instance

Connection Type	Connect using EC2 Instance Connect Endpoint
EC2 Instance Connect Endpoint	ec2-endpoint
Username	ubuntu

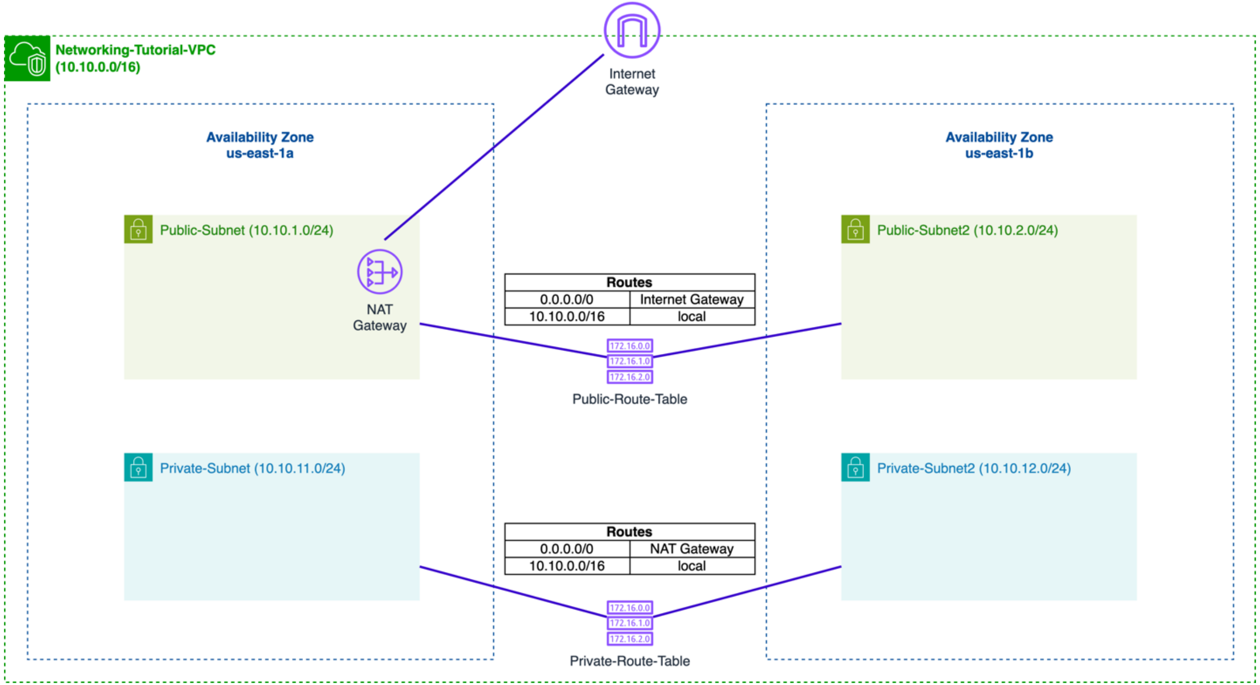
In AWS Academy, the connection will be achieved through the Session Manager, and not the EC2 Instance Connect Endpoint

PrivN – T3 - Connectivity Validation

- Validate that you can access the internet (ping 1.1.1.1)
- Validate that you can access the public network (ping <private_ip_of_public_vm>)

Cloud Network Planning – 2 AZs

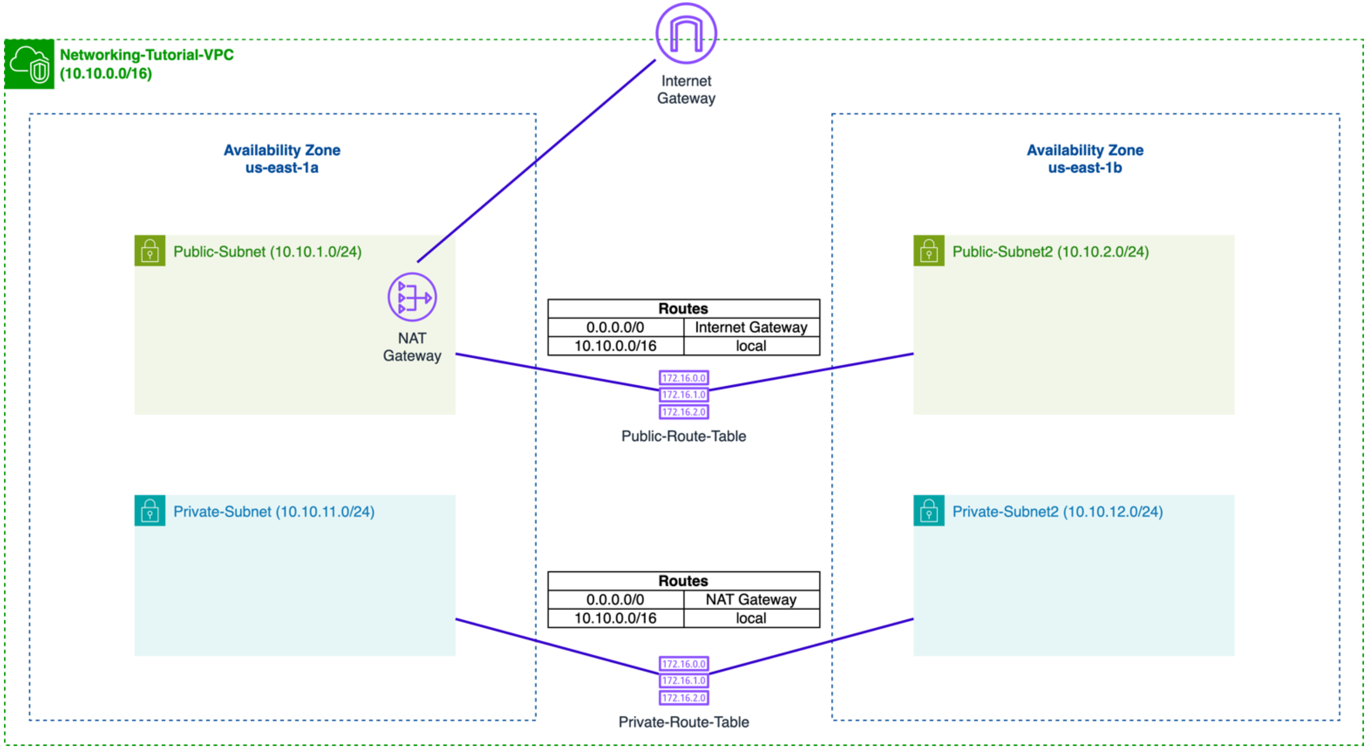
- VMs on the Public Subnet can access the Internet
- Communication between VMs on the Private and Public Subnets is possible
- VMs on the Public Subnet are accessible from the Internet
- VMs on the Private Subnet can reach the Internet
- VMs on the Private Subnet cannot be reached from the internet
- VMs can communicate with other VMs in other Availability Zones



Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway
10.10.0.0/16	local

Cloud Network Planning – 2 AZs

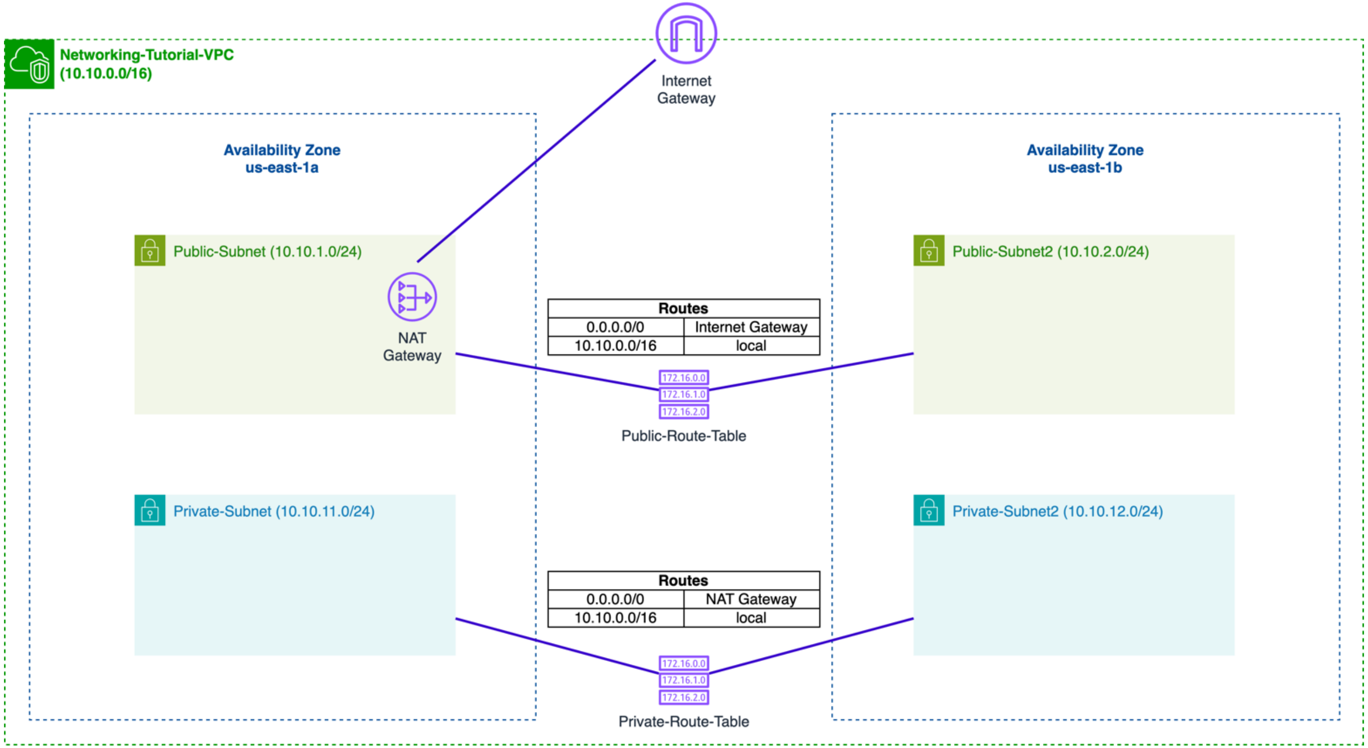


Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway
10.10.0.0/16	local

Is this architecture OK? Why?

Cloud Network Planning – 2 AZs

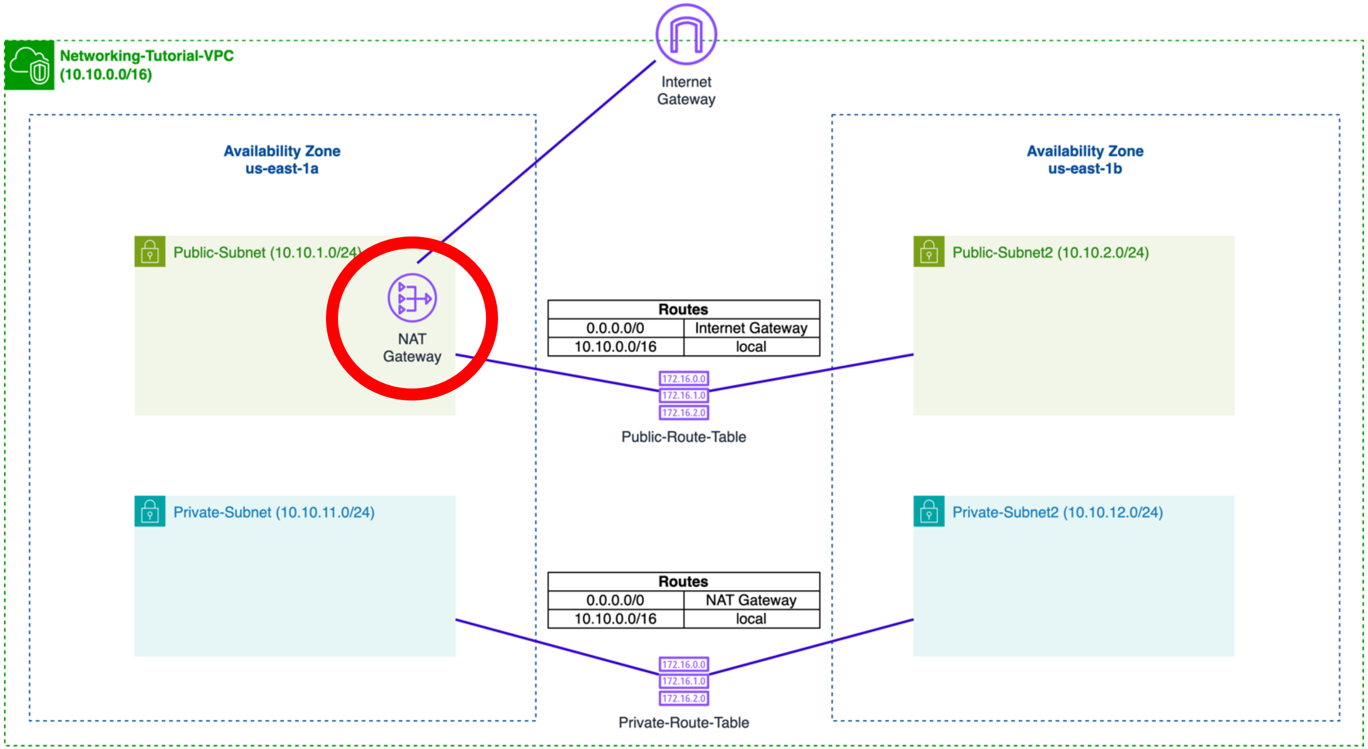


Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway
10.10.0.0/16	local

What happens if you lose AZ us-east-1-a ?

Cloud Network Planning – 2 AZs

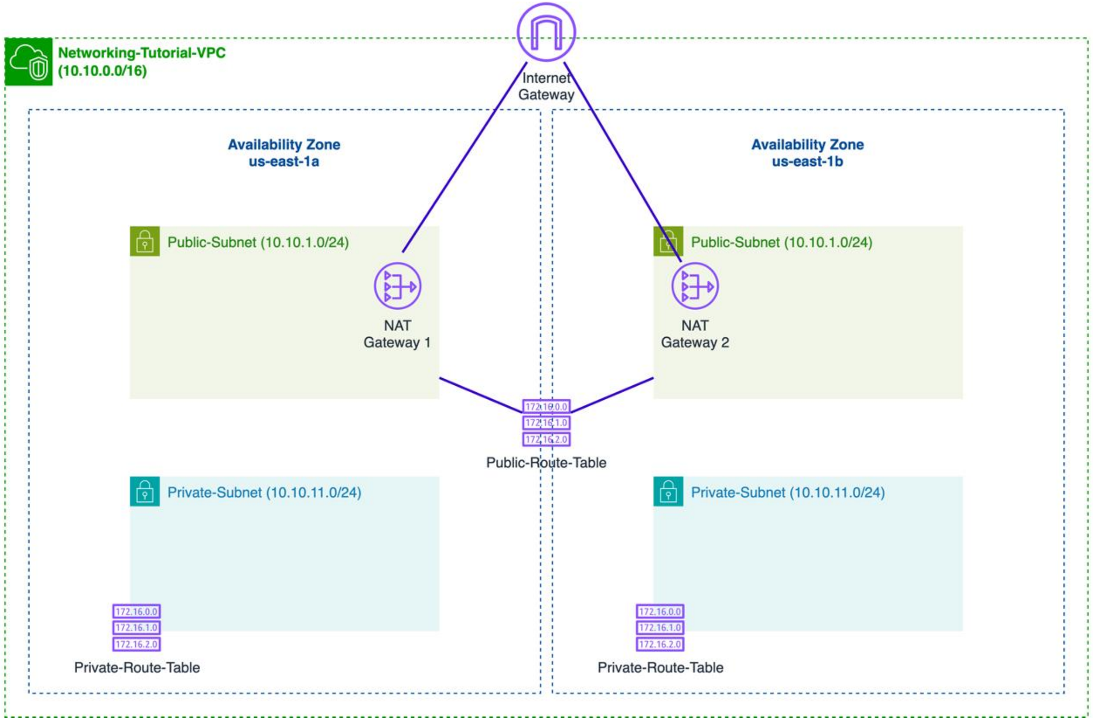


Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway
10.10.0.0/16	local

What happens if you lose AZ us-east-1-a ?

Cloud Network Planning – 2 AZs (Fixed)



Routes	
0.0.0.0/0	Internet Gateway
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway 1
10.10.0.0/16	local

Routes	
0.0.0.0/0	NAT Gateway 2
10.10.0.0/16	local

Better now (High Availability, Fault Tolerance, Security)

How to automate the creation of these resources?

HashiCorp Terraform

aws Cloud Development Kit

Pulumi

AWS CloudFormation

ANSIBLE