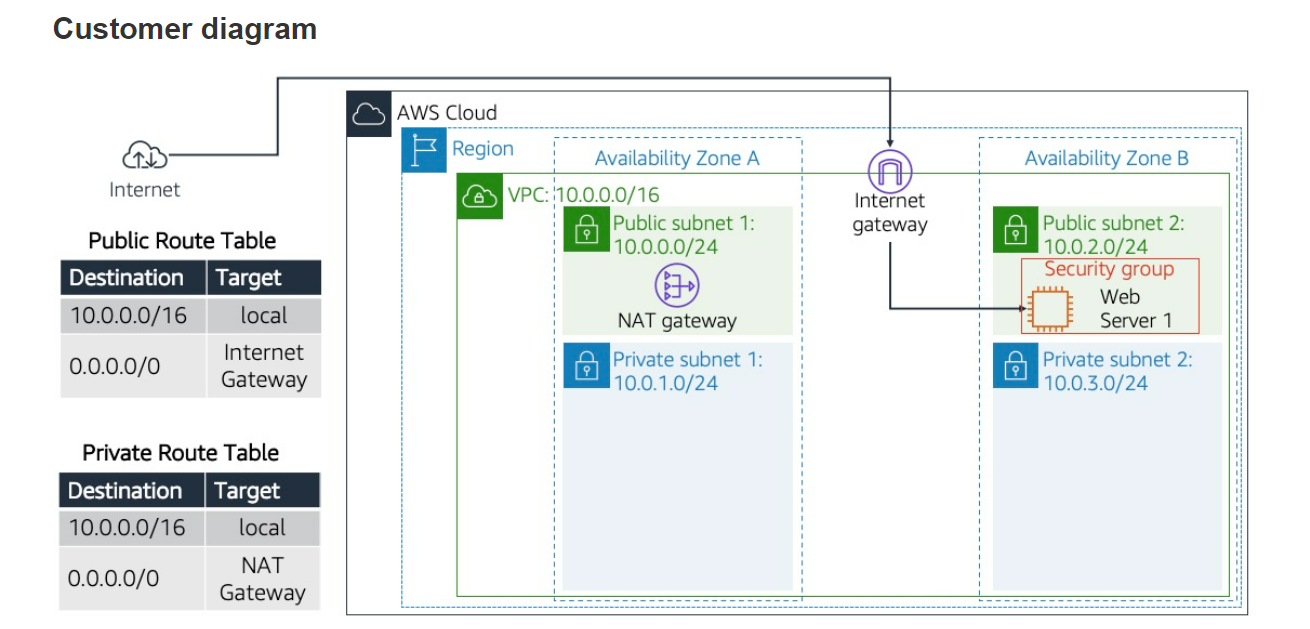
**[Mohamed Mourad](Mohamed%20Mourad%20%20%20Linkedn)**

**Follow me:** [**Linkedn**](inkedin.com/in/mohamed-0mourad/)

**Build Your VPC and Launch a Web Server**

* Create a virtual private cloud (VPC)
* Create subnets
* Configure a security group
* Launch an Amazon Elastic Compute Cloud (Amazon EC2) instance into a VPC

In this lab, you use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to produce a customized network for a Fortune 100 customer. You also create security groups for your EC2 instance. You then configure and customize an EC2 instance to run a web server and launch it into the VPC that looks like the following customer diagram:



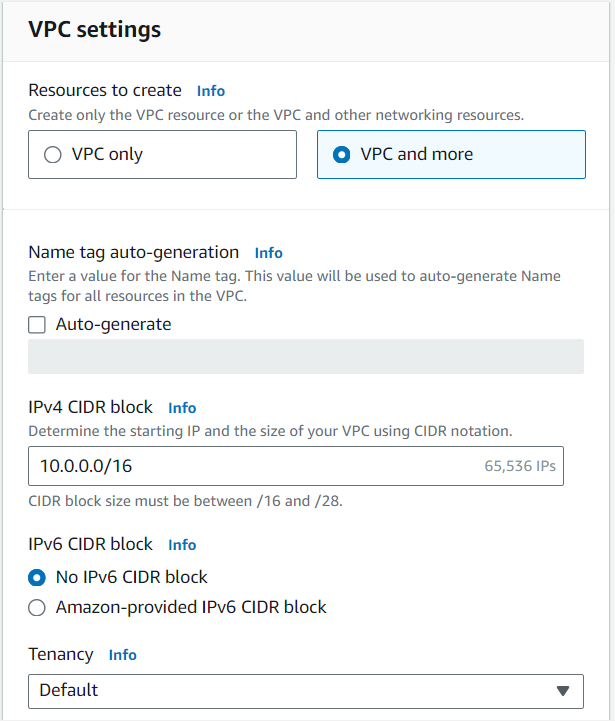
**1: Create your VPC**

We use the VPC Wizard to create a VPC, an internet gateway, and two subnets in a single Availability Zone. An internet gateway is a VPC component that allows communication between instances in your VPC and the internet.

After creating a VPC, you can add subnets. Each subnet resides entirely within one Availability Zone and cannot span zones. If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. If a subnet does not have a route to the internet gateway, the subnet is known as a private subnet.

The wizard also creates a NAT gateway, which is used to provide internet connectivity to EC2 instances in private subnets.

* Once you are in the AWS console, type and search for VPC in the search bar at the top. Select VPC from the list.
* You are now in the Amazon VPC dashboard. You use the Amazon Virtual Private Cloud (Amazon VPC) service to build your VPC.
* Choose **Create VPC** and configure the following options:
  + **Resources to create:** Choose **VPC and more**
  + **Name tag auto-generation**: UnCheck the box **Auto-generate**
  + **IPv4 CIDR:** Enter 10.0.0.0/16
  + **IPv6 CIDR block:** Choose **No IPv6 CIDR block**.
  + **Tenancy:** Choose **Default**.





* + **Number of Availability Zones (AZs)** : **1**
  + **Number of public subnets**: **1**
  + **Number of private subnets**: **1**
  + Expand **Customize subnets CIDR blocks**
    - **Public subnet CIDR block in us-west-2a**: 10.0.0.0/24
    - **Private subnet CIDR block in us-west-2a**: 10.0.1.0/24
  + **NAT gateways**: Choose **In 1 AZ**
  + **VPC endpoints**: Choose **None**
  + A screenshot of a computer

    Description automatically generated



* On the **Preview** pane, name the resources as follows:
  + VPC: Lab VPC
  + Subnets (2)
    - First box, *Public subnet one without name tag*: Public Subnet 1
    - Second box, *Private subnet one without name tag*: Private Subnet 1
  + Route tables (2)
    - First box, *Public route table without name tag*: Public Route Table
    - Second box, *Private route table without name tag*: Private Route Table

A screenshot of a computer

Description automatically generated



* Choose **Create VPC**.

On the next screen, *Success* message is displayed with VPC details.

* Choose **View VPC**.

*Lab VPC* details are displayed as per configuration.

**2.Create additional subnets**

In this task, you create two additional subnets in a second Availability Zone. This option is useful for creating resources in multiple Availability Zones to provide high availability.

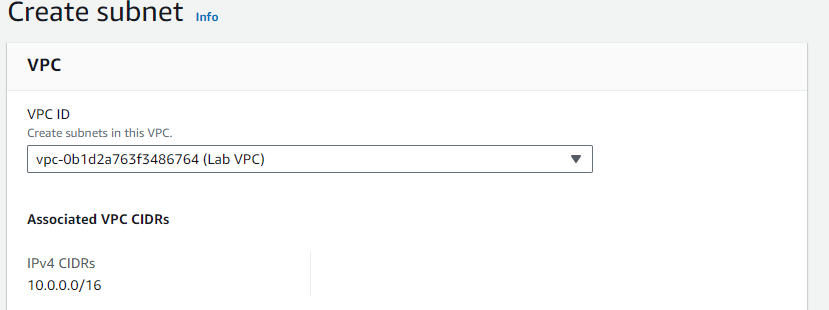
* In the left navigation pane, choose **Subnets**.
* To configure the second public subnet, choose **Create subnet** and configure the following options:
* A screenshot of a computer

  Description automatically generated



* + **VPC ID:** From the dropdown list, choose **Lab VPC**.
  + **Subnet name:** Enter Public Subnet 2
  + **Availability Zone:** No preference
  + **IPv4 CIDR block:** Enter 10.0.2.0/24
* Choose **Create subnet**.

The subnet will have all IP addresses starting with **10.0.2.x**.





A screenshot of a computer

Description automatically generated



* To configure the second private subnet, choose **Create subnet** and configure the following options:
  + **VPC ID:** From the dropdown list, choose **Lab VPC**.
  + **Subnet name:** Enter Private Subnet 2
  + **Availability Zone:** No preference
  + **IPv4 CIDR block:** Enter 10.0.3.0/24
* Choose **Create subnet**.

The subnet will have all IP addresses starting with **10.0.3.x**.

**3: Associate the subnets and add routes**

* In the left navigation pane, choose **Route Tables**.
* Choose **Public Route Table**
* In the lower pane, choose the **Subnet associations** tab.

A screenshot of a computer

Description automatically generated



* Under **Subnets without explicit associations**, choose **Edit subnet associations**.
* Select the check boxes for **Public Subnet 2**.
* Choose **Save associations**.

A screenshot of a computer

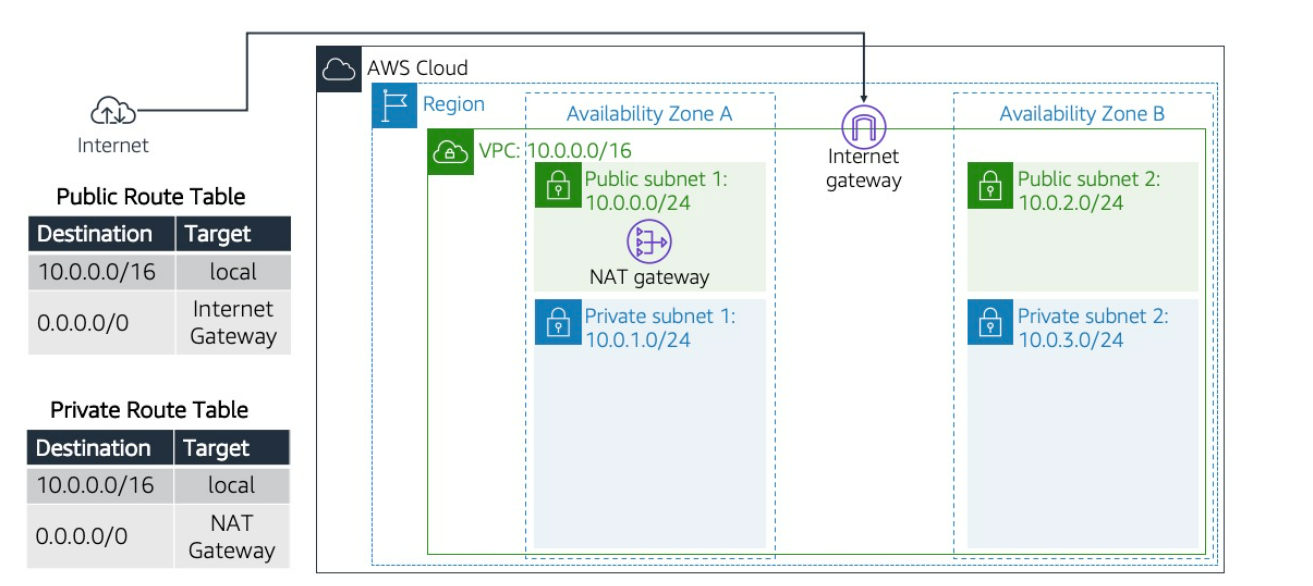
Description automatically generated



You now configure the route table that is used by the private subnets.

* Choose **Private Route Table**
* In the lower pane, choose the **Subnet associations** tab.
* Under **Subnets without explicit associations**, choose **Edit subnet associations**.
* Select the check boxes for **Private Subnet 2**.
* Choose **Save associations**.

Your VPC now has public and private subnets configured in two Availability Zones:



**4: Create a VPC security group**

In this task, you create a VPC security group, which acts as a virtual firewall for your instance. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

* In the left navigation pane, choose **Security Groups**.
* Choose **Create security group**.
* Configure the security group with the following options:
  + **Security group name:** Enter Web Security Group
  + **Description:** Enter Enable HTTP access
  + **VPC:** Choose **Lab VPC**.
* Under **Inbound rules**, choose **Add rule**.
* Configure the following options:
  + **Type:** Choose **HTTP**.
  + **Source:** Choose **Anywhere IPv4**.
  + **Description:** Enter Permit web requests
* Choose **Create security group**.

A screenshot of a computer

Description automatically generated



You use this security group in the next task when launching an EC2 instance.

**5: Launch a web server instance**

[**Check this detailed file**](https://www.linkedin.com/posts/mohamed-0mourad_amazon-ec2-instance-activity-7242198512656932864-6q0M?utm_source=share&utm_medium=member_desktop)

In this task, you launch an EC2 instance into the new VPC. You configure the instance to act as a web server.

* On the AWS Management Console, in the **Search** bar, enter and choose EC2 to go to the **EC2**
* In the left navigation pane, choose **Instances**.
* Choose **Launch instances** and configure the following options:
* In the **Name and tags** section, **Name:** Web Server 1.
* In the **Application and OS Images (Amazon Machine Image)** section, configure the following options:
  + **Quick Start:** Choose **Amazon Linux**.
  + **Amazon Machine Image (AMI):** From dropdown, Choose **Amazon Linux 2 AMI (HVM)**.
* In the **Instance type** section, choose **t3.micro**.
* In the **Key pair (login)** section, choose **vockey**.
* In the **Network settings** section, choose Edit and configure the following options:
* **VPC - *required*:** Choose **Lab VPC**.
* **Subnet:** Choose **Public Subnet 2**.
* **Auto-assign public IP:** Choose **Enable**.
* **Firewall (security groups):** Choose **Select existing security group**.
  + Choose **Web Security Group**.

A screenshot of a computer

Description automatically generated



* Expand **Advanced details**
* Under **User data**, copy and paste the following code

#!/bin/bash

#Install Apache Web Server and PHP

yum install -y httpd mysql php

#Download Lab files

wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-RESTRT-1/267-lab-NF-build-vpc-web-server/s3/lab-app.zip

unzip lab-app.zip -d /var/www/html/

#Turn on web server

chkconfig httpd on

service httpd start

* Choose **Launch instance**.

A screenshot of a computer

Description automatically generated



* To display the launched instance, choose **View all instances**.
* Wait until the **Web Server 1** shows **2/2 checks passed** in the **Status check** column.
* This may take a few minutes. To update the page, choose refresh at the top of the page.

A screenshot of a computer

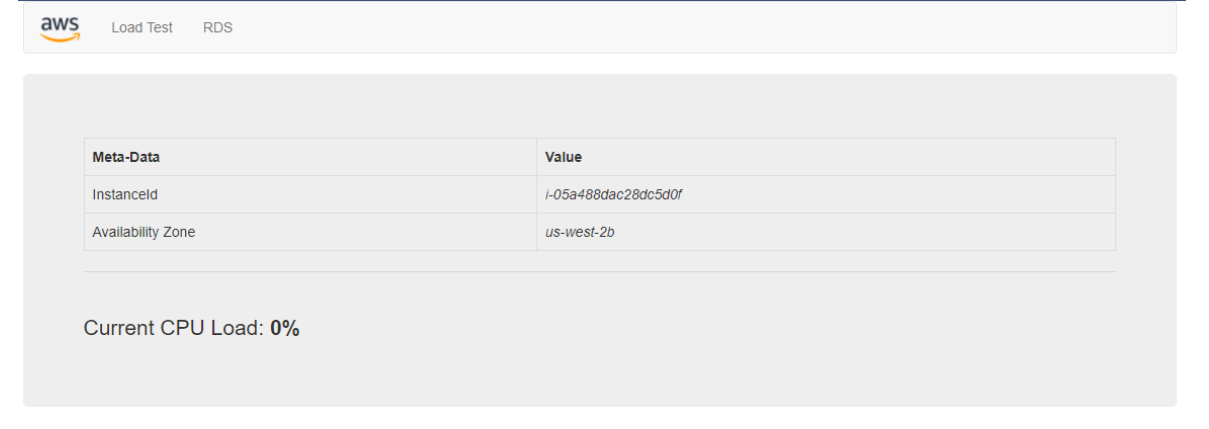
Description automatically generated



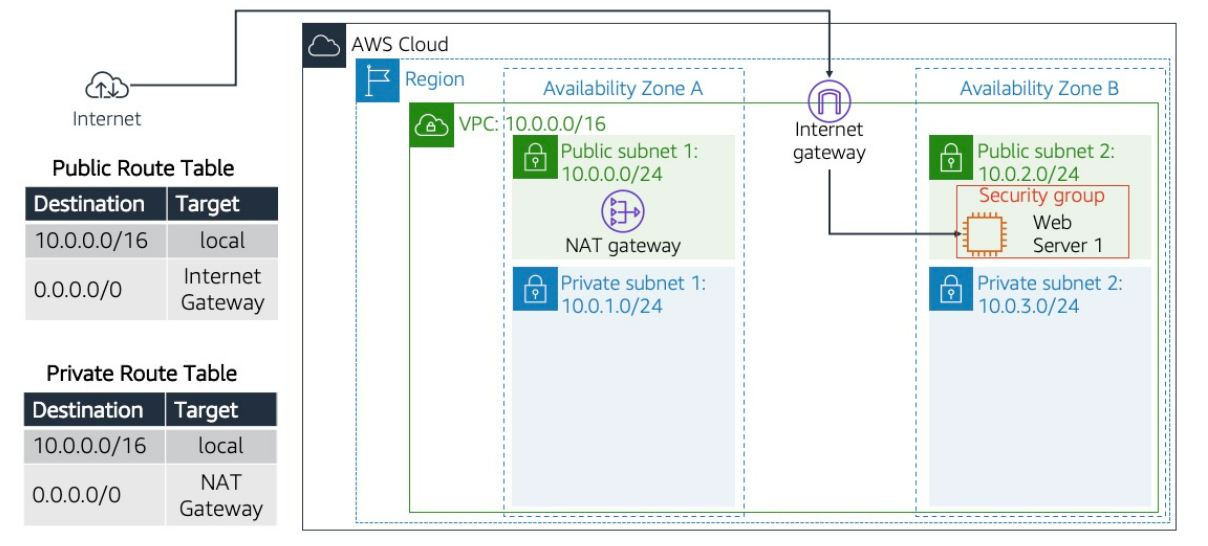
You now connect to the web server running on the EC2 instance.

* Select the check box for the instance, and choose the **Details** tab.
* Copy the **Public IPv4 DNS** value.
* Open a new web browser tab, paste the **Public IPv4 DNS** value, and press Enter.

When successful, the page should look like the following:



The following is the complete architecture that we deployed:



**Thank you for your time**

**نسألكم الدعاء**

**لا تنسوا اخواتنا في غزة والسودان بالدعاء**