

Build Your VPC and Launch a Web Server

Objectives

After completing this lab, you should be able to:

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

Duration

This lab takes approximately **45 minutes** to complete.

Scenario

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:

Customer diagram

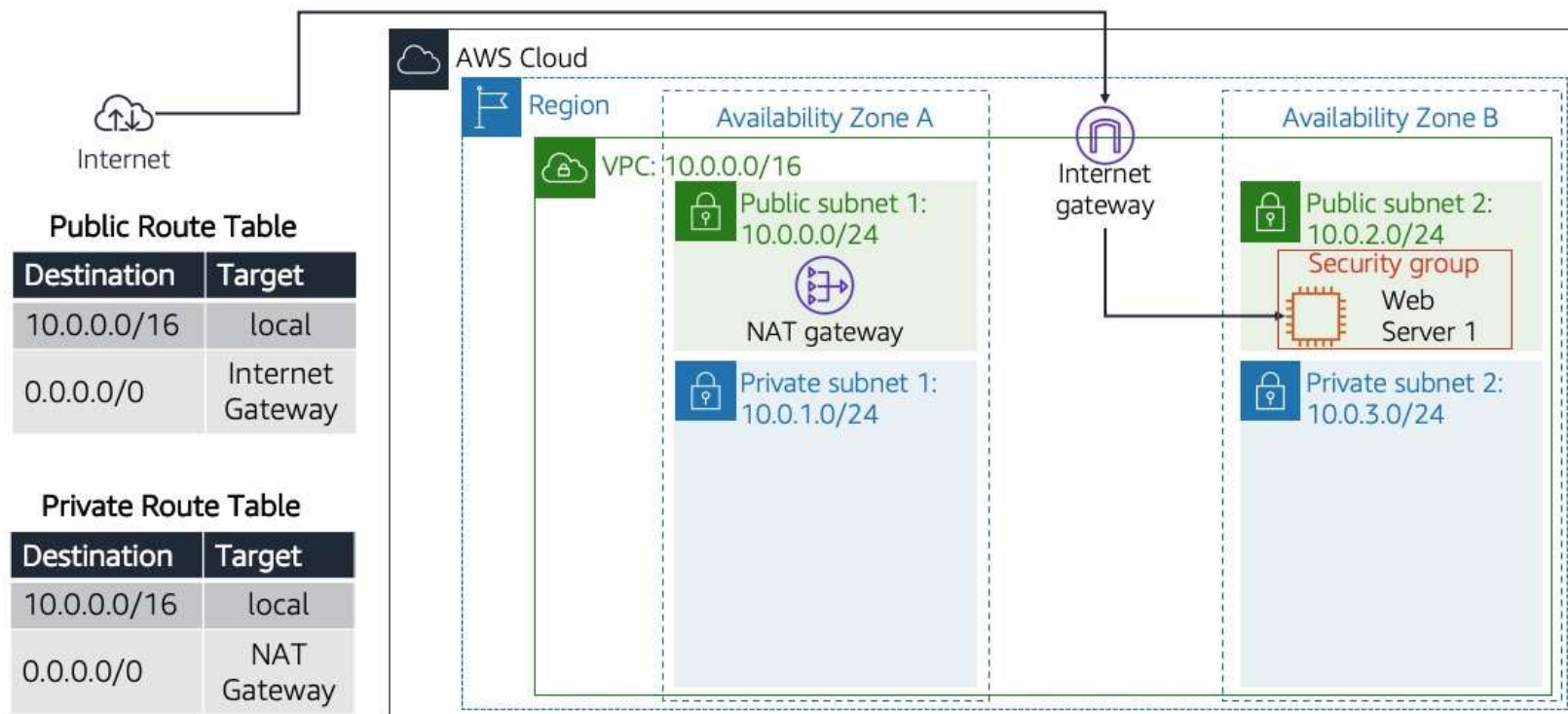


Figure: The customer is requesting the build of this architecture to launch their web server successfully.

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that you need to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that this lab describes.

Accessing the AWS Management Console

1. At the top of these instructions, choose **Start Lab** to launch this lab.

A **Start Lab** panel opens and displays the lab status.

i Tip: If you need more time to complete the lab, restart the timer for the environment by choosing the **Start Lab** button again.

2. Wait until you see the message **Lab status: ready**, and then choose the **X** to close the **Start Lab** panel.

3. At the top of these instructions, choose **AWS**

This option opens the AWS Management Console in a new browser tab. The system automatically signs you in.

i Tip: If a new browser tab does not open, a banner or icon at the top of your browser will indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

Task 1: Create your VPC

In this task, you 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.

4. In the AWS Management Console, select the **Services** menu, and then select **VPC** under **Networking & Content Delivery**.

5. In the left navigation menu, choose **Elastic IPs**.

6. Choose **Allocate Elastic IP address**.

7. On the **Allocate Elastic IP address** page, leave the settings as is, and choose **Allocate**.

8. In the left navigation menu, choose **VPC Dashboard**.

9. Choose **Launch VPC Wizard**.

10. For **Step 1: Select a VPC Configuration**, choose **VPC with Public and Private Subnets**.

11. Choose **Select**.

12. For **Step 2: VPC with Public and Private Subnets**, configure the following options:

- **VPC name:** Enter **Lab VPC**
- **Availability Zone:** From the dropdown list, choose the first Availability Zone.
- **Public subnet name:** Enter **Public Subnet 1**
- **Availability Zone:** From the dropdown list, choose the first Availability Zone (the same as used above).
- **Private subnet name:** Enter **Private Subnet 1**
- **Elastic IP Allocation ID:** Select the box, and select the displayed IP address.

13. Choose **Create VPC**. It may take a few minutes for the VPC to become available.

14. On the **VPC Successfully Created** page, choose **OK**.

The wizard has provisioned a VPC with a public subnet and a private subnet in the same Availability Zone together with route tables for each subnet:

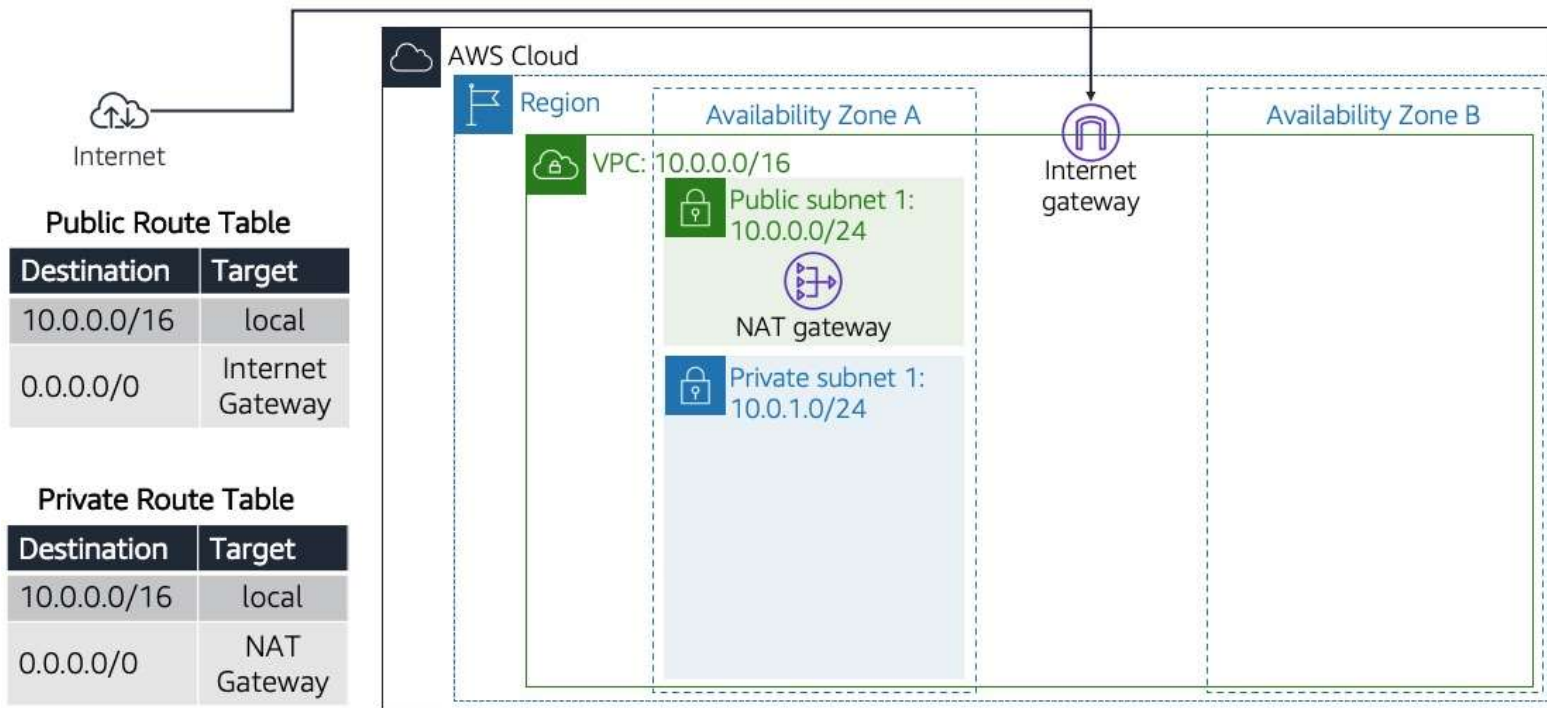


Figure: The VPCs, CIDRs, and the creation of public and private route tables. You created these options using the VPC Wizard.

The public subnet has a Classless Inter-Domain Routing (CIDR) of **10.0.0.0/24**, which means that it contains all IP addresses starting with **10.0.0.x**.

The private subnet has a CIDR of **10.0.1.0/24**, which means that it contains all IP addresses starting with **10.0.1.x**.

Task 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:
 - VPC ID:** From the dropdown list, choose **Lab VPC**.
 - Subnet name:** Enter `Public Subnet 2`
 - Availability Zone:** From the dropdown list, choose the second Availability Zone.
 - IPv4 CIDR block:** Enter `10.0.2.0/24`

17. Choose **Create subnet**.

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

- 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:** From the dropdown list, choose the second Availability Zone.
 - IPv4 CIDR block:** Enter `10.0.3.0/24`

19. Choose **Create subnet**.

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


Task 3: Create a route table

You now configure the private subnets to route internet-bound traffic to the NAT gateway so that resources in the private subnet are able to connect to the internet while still keeping the resources private. To do this, you configure a route table.

Recall that a route table contains a set of rules, called routes, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table controls routing for the subnet.


20. In the left navigation pane, choose **Route Tables**.
21. Select the check box for the route table with **Yes** in the **Main** column and **Lab VPC** in the **VPC** column. (Expand the **VPC** column if necessary to view the VPC name.)
22. In the lower pane, choose the **Routes** tab.

Recall that **Destination 0.0.0.0/0** is set to **Target nat-xxxxxxx**. This means that traffic destined for the internet (0.0.0.0/0) will be sent to the NAT gateway. The NAT gateway will then forward the traffic to the internet.

This route table is therefore being used to route traffic from private subnets.
23. In the **Name** column for this route table, choose the pencil , enter `Private Route Table` and then choose **Save**.

Task 4: Associate the subnets and add routes

24. In the lower pane, choose the **Subnet associations** tab.
25. Under **Subnets without explicit associations**, choose **Edit subnet associations**.
26. Select the check boxes for both **Private Subnet 1** and **Private Subnet 2**.
27. Choose **Save associations**.

You now configure the route table that is used by the public subnets.
28. Select the check box for the route table with **No** in the **Main** column and **Lab VPC** in the **VPC** column, and clear the check boxes for any other route tables.
29. In the **Name** column for this route table, choose the pencil , enter `Public Route Table` and then choose **Save**.
30. In the lower pane, choose the **Routes** tab.

Note that **Destination 0.0.0.0/0** is set to **Target igw-xxxxxxx**, which is the internet gateway. This means that internet-bound traffic will be sent straight to the internet via the internet gateway.

You now associate this route table to the public subnets.
31. Choose the **Subnet associations** tab.
32. In the **Subnets without explicit associations** section, choose **Edit subnet associations**.
33. Select the check boxes for both **Public Subnet 1** and **Public Subnet 2**.
34. Choose **Save associations**.

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

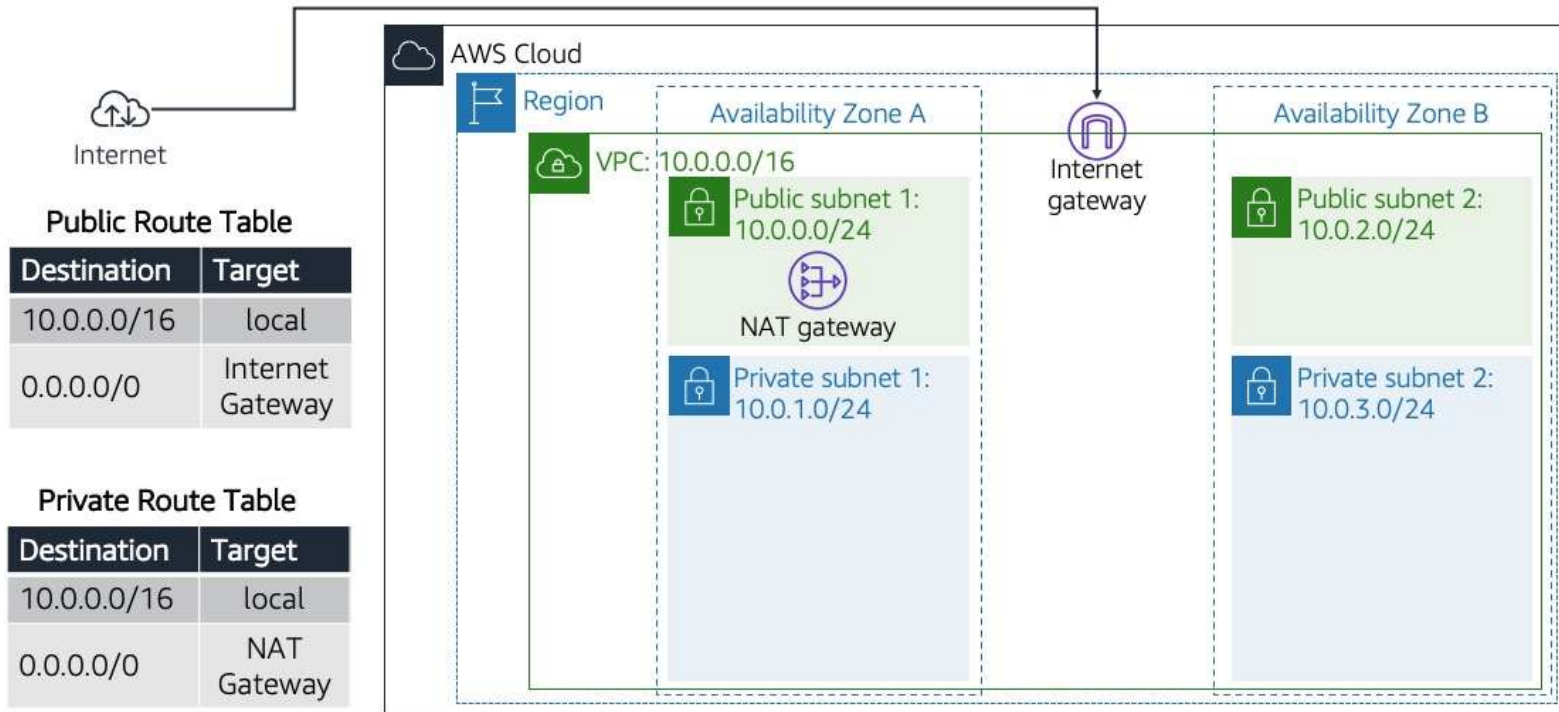


Figure: The creation of the networking resources and routing components and attachment of these resources that make the VPC functional as a network.

Task 5: 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.

35. In the left navigation pane, choose **Security Groups**.

36. Choose **Create security group**.

37. Configure the security group with the following options:

- **Security group name:** Enter `Web Security Group`
- **Description:** Enter `Enable HTTP access`
- **VPC:** Choose **Lab VPC**.

38. Choose **Create security group**.

You now add a rule to the security group to permit inbound web requests.

39. Choose the **Inbound rules** tab.

40. Choose **Edit inbound rules**

41. Choose **Add rule**.

42. Configure the following options:

- **Type:** Choose **HTTP**.
- **Source:** Choose **Anywhere**.
- **Description:** Enter `Permit web requests`

43. Choose **Save rules**.

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

Task 6: Launch a web server instance

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

44. In the AWS Management Console, select the  **Services** menu, and then select **EC2** under **Compute**.

45. Choose **Launch instances**

First, you choose an **Amazon Machine Image (AMI)**, which contains the desired operating system.

46. For **Step 1: Choose an Amazon Machine Image (AMI)**, choose **Select** for **Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type**.

The instance type defines the hardware resources assigned to the instance.

47. For **Step 2: Choose an Instance Type**, choose the check box for **t2.micro**.

48. Choose **Next: Configure Instance Details**

You now configure the instance to launch in a public subnet of the new VPC.

49. For **Step 3: Configure Instance Details**, configure the following settings:

- **Network:** Choose **Lab VPC**.
- **Subnet:** Choose **Public Subnet 2**. (Be careful not to choose the private subnet.)
- **Auto-assign Public IP:** Choose **Enable**.

50. At the bottom of the page, expand the **Advanced Details** section.

51. Copy and paste the following code into the **User data** box:

```
#!/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-RESTR-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
```

This script runs automatically when the instance launches for the first time. The script loads and configures a PHP web application.

52. Choose **Next: Add Storage**

53. For **Step 4: Add Storage**, you use the default settings for storage. Choose **Next: Add Tags** to move onto the next step.

Tags can be used to identify resources. You use a tag to assign a name to the instance.

54. For **Step 5: Add Tags**, choose **Add Tag**

55. Configure the following options:

- **Key:** Enter **Name**
- **Value:** Enter **web Server 1**

56. Choose **Next: Configure Security Group**

You configure the instance to use the **Web Security Group** that you created earlier.

57. For **Step 6: Configure Security Group**, for **Assign a security group**, select  **Select an existing security group**.


58. Select the check box for the ☒ **vockey | RSA** security group.

This is the security group that you created in the previous task. It permits HTTP access to the instance.

59. Choose **Review and Launch**

60. When prompted with a warning that you will not be able to connect to the instance through port 22, choose **Continue**

61. For **Step 7: Review Instance Launch**, review the instance information, and choose **Launch**
62. In the **Select an existing key pair or create a new key pair** window, select the check box next to ☒ **I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.**
63. Choose **Launch Instances**
64. Choose **View Instances**
65. 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.

You now connect to the web server running on the EC2 instance.
66. Select the check box for the instance, and choose the **Details** tab.
67. Copy the **Public IPv4 DNS** value.
68. Open a new web browser tab, paste the **Public IPv4 DNS** value, and press Enter.
- When successful, the page should look like the following:

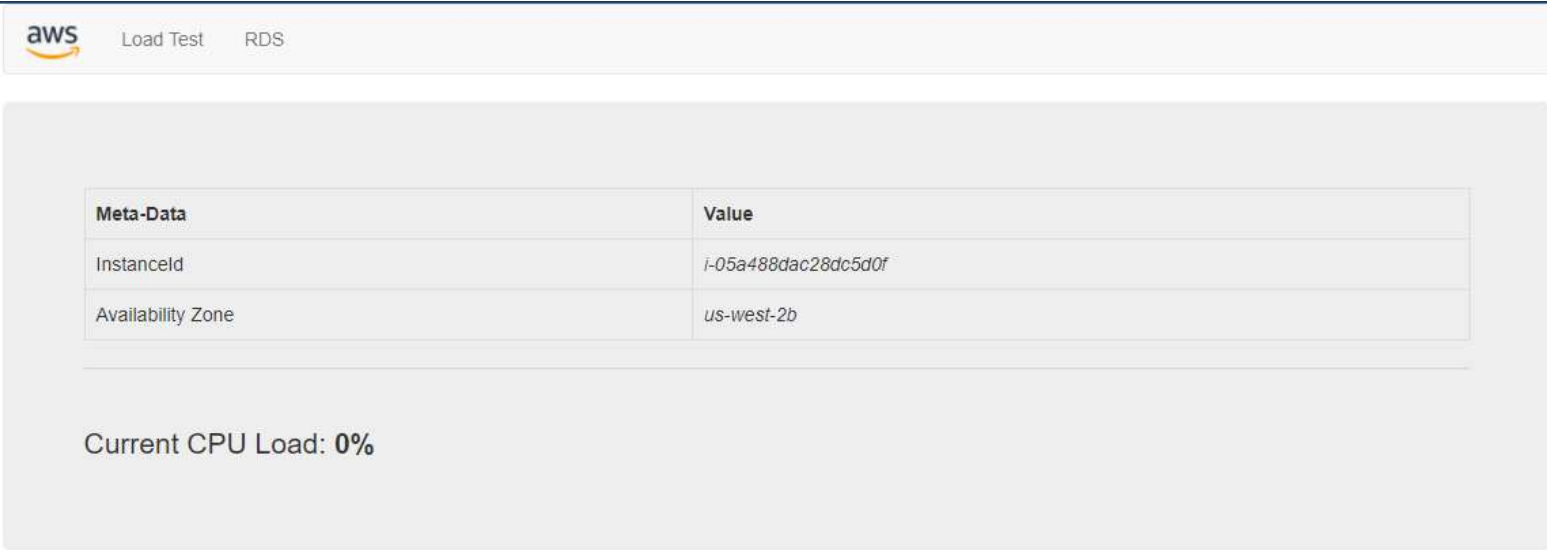


Figure: The success page when the web server is launched.

The following is the complete architecture that you deployed:

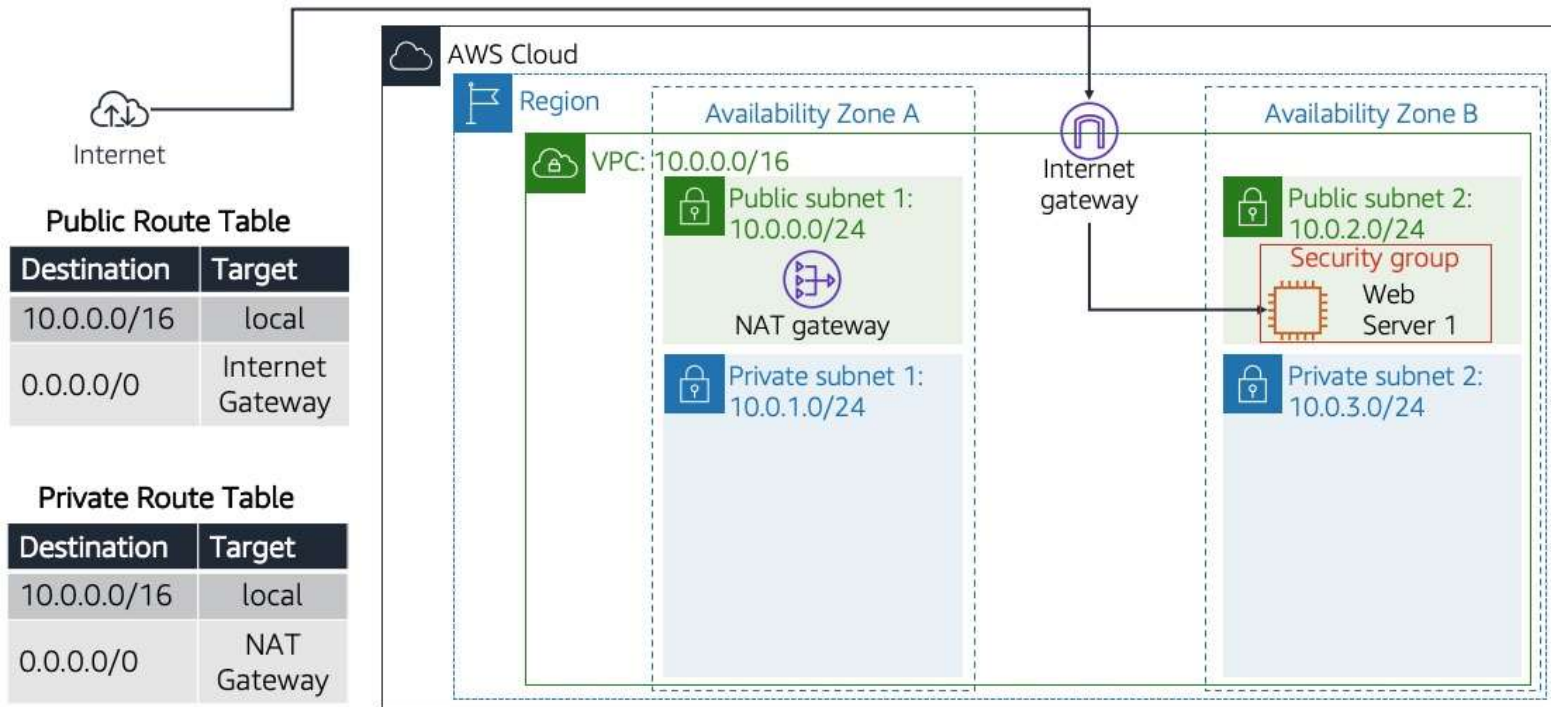


Figure: A picture of the end product, which is the delivery of the exact customer request: a fully functional VPC with its resources (network and security) and a web server.


Recap

► In this lab

Additional resources

- [What is Amazon VPC?](#)

Lab complete

 Congratulations! You have completed the lab.

69. At the top of the page, choose  **End Lab**, and then select  to confirm that you want to end the lab.

A panel appears indicating that **You may close this message box now. Lab resources are terminating ...**

70. In the upper-right corner, choose the **X** to close the **End Lab** panel.

For more information about AWS Training and Certification, see [AWS Training and Certification](#).

Your feedback is welcome and appreciated.

If you would like to share any suggestions or corrections, please provide the details in our [AWS Training and Certification Contact Form](#).

© 2022 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.