Creating Networking Resources in an Amazon Virtual Private Cloud (VPC)

Objectives

- **Create a VPC, Internet Gateway, Route Table, Security Group, Network Access List, and EC2 instance to create a routable network within the VPC**

Scenario

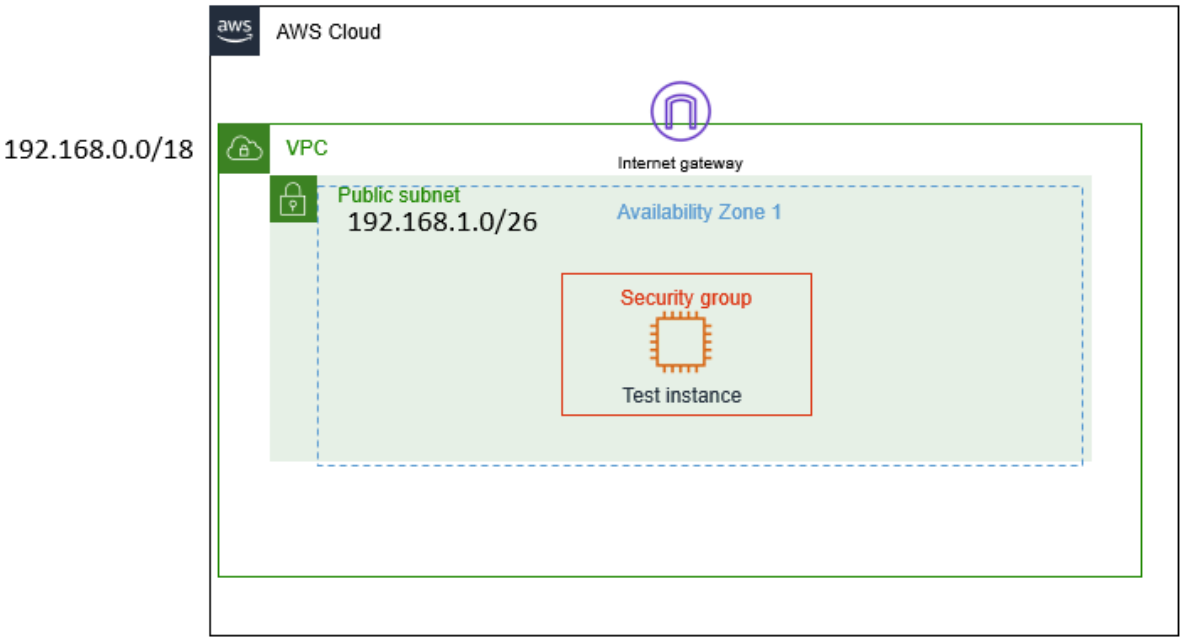
Your role is a Cloud Support Engineer at Amazon Web Services (AWS). During your shift, a customer from a startup company requests assistance regarding a networking issue within their AWS infrastructure. The email and an attachment of their architecture is below.

Email from the customer

Hello Cloud Support!

I previously reached out to you regarding help setting up my VPC. I thought I knew how to attach all the resources to make an internet connection, but I cannot even ping outside the VPC. All I need to do is ping! Can you please help me set up my VPC to where it has network connectivity and can ping? The architecture is below. Thanks!

Brock, startup owner



Steps

Creating the VPC

Name the VPC: Test VPC
IPv4 CIDR block: 192.168.0.0/18

Creating Subnets

Now that the VPC is complete, look at the left navigation pane and select **Subnets**. In the top right corner, select **Create subnet**.

Select Test VPC

Subnet name: Public Subnet

IPv4 CIDR block: 192.168.1.0/28

Create Route Table

Navigate to the left navigation pane, and select **Route Tables**. In the top right corner select **Create route table**.

Route table name: Public Route Table
Select Test VPC

Create Internet Gateway and attach Internet Gateway

From the left navigation pane, select **Internet Gateways**. Create an Internet Gateway (IGW) by selecting **Create internet gateway** at the top right corner.

Name tag : IGW test VPC

Once created, attach the **Internet Gateway** to the VPC by selecting **Actions** at the top right corner and clicking **Attach to VPC**.

Add route to route table and associate subnet to route table

Navigate to the **Route Table** section on the left navigation pane. Select the Public **Route Table**, and then scroll to the bottom and select the **Routes** tab.
Select the Edit routes button located in the routes box.
On the Edit routes page, the first IP address is the local route and cannot be changed.
Select **Add route**.

- In the **Destination** section, type **0.0.0.0/0** in the search box. This is the route to the IGW. You are telling the route table that any traffic that needs

internet connection will use 0.0.0.0/0 to reach the IGW so that it can reach the internet.

- Click in the **Target** section and select **Internet Gateway** since you are targeting any traffic that needs to go to the internet to the IGW. Once you select the IGW, you will see your **TEST VPC IGW** appear. Select that IGW, navigate to the bottom right, and select **Save changes**.

From the Public route table dashboard, select the **Subnet associations** tab. Select the **Edit subnet associations** button.

Select **Save association**

Creating a Network ACL

From the left navigation pane, select **Network ACLs**. Navigate to the top right corner and select **Create network ACL** to create a Network Access Control Lists (NACLs).

Creating a Security Group

From the left navigation pane, select **Security Groups**. Navigate to the top right corner and select **Create security group** to create a security group.

In the VPC portion, remove the current VPC, and select **Test VPC**.

The completed security group is shown below. This indicates that for **Inbound rules** you are allowing SSH, HTTP, and HTTPS types of traffic, each of which has its own protocols and port range. The source from which this traffic reaches your instance can be originating from anywhere. For **Outbound rules**, you are allowing all traffic from outside your instance.

Launch EC2 instance and SSH into instance

In task 2, you will launch an EC2 instance within your Public subnet and test connectivity by running the command **ping**. This will validate that your infrastructure is correct, such as security groups and network ACLs, to ensure that they are not blocking any traffic from your instance to the internet and vice versa. This will validate that you have a route to the IGW via the route table and that the IGW is attached.

Navigate to Services at the top left, and select **EC2**. From the EC2 dashboard, select **Instances**.

Select **Launch instances** from the top right corner. Then complete the following steps:

Choose the AMI: Amazon Linux 2 AMI

Choose the instance type, t3.micro

Edit network settings : choose the Test VPC, public Subnet, enable the "Auto-assign Public IP"

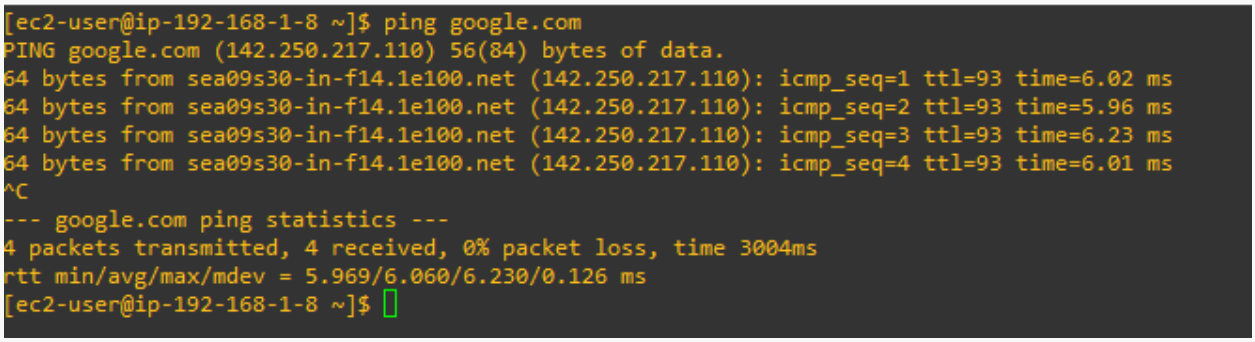
keep at the default storage.

Select an existing key pair , vockey

Use SSH to connect to an Amazon Linux EC2 instance

Use ping to test internet connectivity

Ping google.com



Run ping to test connectivity. The above results are saying you have replies from google.com and have 0% packet loss.
If you are getting replies back, that means that you have connectivity.