CMPT 489

Assignment 9

Marcelo Ollin Paco Zepeda
301180252

Table of Contents

Part 1: Amazon VPC

Task 1:

What is the range of the IPs in the VPC you just created?

The netmask that we used was 10.0.0.0/16 therefore, the range of the IPs in the VPC are from **10.0.0.0** to **10.0.255.255.**

Task 2:

What is the difference between a VPC and a Virtual Private Network (VPN)?

Aside from both having virtual and private in their names, VPC and VPC are quite different from one another. A virtual private cloud (VPC) is an on-demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations – denoted as users hereafter – using the resources. Where as a virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Note that the V (virtual) in the acronyms emphasizes that the VPN or VPC is created by means of virtualizations. The hardware they rely on is virtual and separated from the underlying physical hardware resources. The P (private) in the acronym implies that these resources can only be accessed by permitted users.

Part 2: Subnets

Task 3:

What are the IP ranges of the two subnets you created?

For the subnet mask 10.0.1.0/24, the IP ranges start from **10.0.1.0** and go up to **10.0.1.255**. For the subnet mask 10.0.2.0/24, the IP ranges from **10.0.2.0** and go up to **10.0.2.255**.

Task 4:

Why would someone create a public and a private subnet? What are the uses of each of them? Provide an example.

Using the virtual private cloud with public and private subnets (NAT) could be done for multiple reasons. A reason that this would be done is if a user wants to run a public-facing web application, while maintaining the back-end servers that aren't publicly accessible. A common example is a multi-tier website, with the web servers in a public subnet and the database servers in private subnet. A user can set up security and routing so that the web server can communicate with the database servers. Moreover, the instances in the public subnet can send outbound traffic directly to the internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the internet by using a network address translation (NAT) gateway that resides in the public subnet. The database servers can connect to the internet for software updates using the NAT gateway, but the internet cannon establish connections to the database servers.

Part 3: Running a Web App on EC2

Task 5:

If we launch two instances, one in the public subnet and one in the private subnet, the one in the private one will not have internet access. How is it possible to connect through SSH to the instance in the private subnet?

SSHing to the instance in the private subnet is possible because of the network address translation (NAT) instance in the VPC that is provided by the internet gateway. A test can be done to check if an instance in the private subnet can access the internet through the NAT instance by using the NAT instance as a bastion server. This can be done by updating the NAT instance's security group rules to allow inbound and outbound ICMP traffic and allow outbound SSH traffic, launch an instance into the private subnet, configure SSH forwarding to access instances in the private subnet, connect to the instances and then to test the internet connectivity.

For more information see the following:
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html

Task 6:

If we wanted to give Internet access to the private subnet this can be done by creating a NAT Gateway. What is the difference between the NAT Gateway and the Internet Gateway?

The difference between the NAT gateway and the internet gateway is that attaching an internet gateway to a virtual private cloud allows instances with public IPs to access the internet. While a NAT gateway allows instances with not public IPs to access the internet.

Task 7:

What are the steps needed to be taken in order to create a NAT Gateway into the public subnet that can provide the private subnet with internet access? You can try it by launching two instances and experimenting with the NAT Gateway.

The following was take from: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

Creating a NAT Gateway

To create a NAT gateway, you must specify a subnet and an Elastic IP address. Ensure that the Elastic IP address is currently not associated with an instance or a network interface. If you are migrating from a NAT instance to a NAT gateway and you want to reuse the NAT instance's Elastic IP address, you must first disassociate the address from your NAT instance.

To create a NAT gateway

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **NAT Gateways**, **Create NAT Gateway**.
3. Specify the subnet in which to create the NAT gateway, and select the allocation ID of an Elastic IP address to associate with the NAT gateway. When you're done, choose **Create a NAT Gateway**.
4. The NAT gateway displays in the console. After a few moments, its status changes to `Available`, after which it's ready for you to use.

If the NAT gateway goes to a status of `Failed`, there was an error during creation. For more information, see NAT Gateway Goes to a Status of Failed.

Note: to create a NAT gateway, the user must specify the public subnet in which the NAT gateway should reside. After the NAT gateway is created, the user must update the route table associated with one or more of their private subnets to point internet-bound traffic to the NAT gateway. This enables instances in the private subnets to communicate with the internet.

Part 4: Security Groups

Task 8:

In VPC under Security there is another module called Network ACL. What is the difference between Network ACL and Security Groups?

The difference between security group and ACLs is that, security group acts as a firewall associated with Amazon EC2 instances, controlling both the inbound and outbound traffic at the instance level, while ACLs act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.

Task 9:

Report the steps required to create a Network ACL and how would you integrate it in the public subnet you previously created?

The following was taken from: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Creating a Network ACL

You can create a custom network ACL for your VPC. By default, a network ACL that you create blocks all inbound and outbound traffic until you add rules, and is not associated with a subnet until you explicitly associate it with one.

To create a network ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Network ACLs**.
3. Choose **Create Network ACL**.
4. In the **Create Network ACL** dialog box, optionally name your network ACL, and then select the ID of your VPC from the **VPC** list, and choose **Yes, Create**.

Associating a Subnet with a Network ACL

To apply the rules of a network ACL to a particular subnet, you must associate the subnet with the network ACL. You can associate a network ACL with multiple subnets; however, a subnet can be associated with only one network ACL. Any subnet not associated with a particular ACL is associated with the default network ACL by default.

To associate a subnet with a network ACL

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Network ACLs**, and then select the network ACL.
3. In the details pane, on the **Subnet Associations** tab, choose **Edit**. Select the **Associate** check box for the subnet to associate with the network ACL, and then choose **Save**. (**Here is where we would put the public subnet that we previously created**)