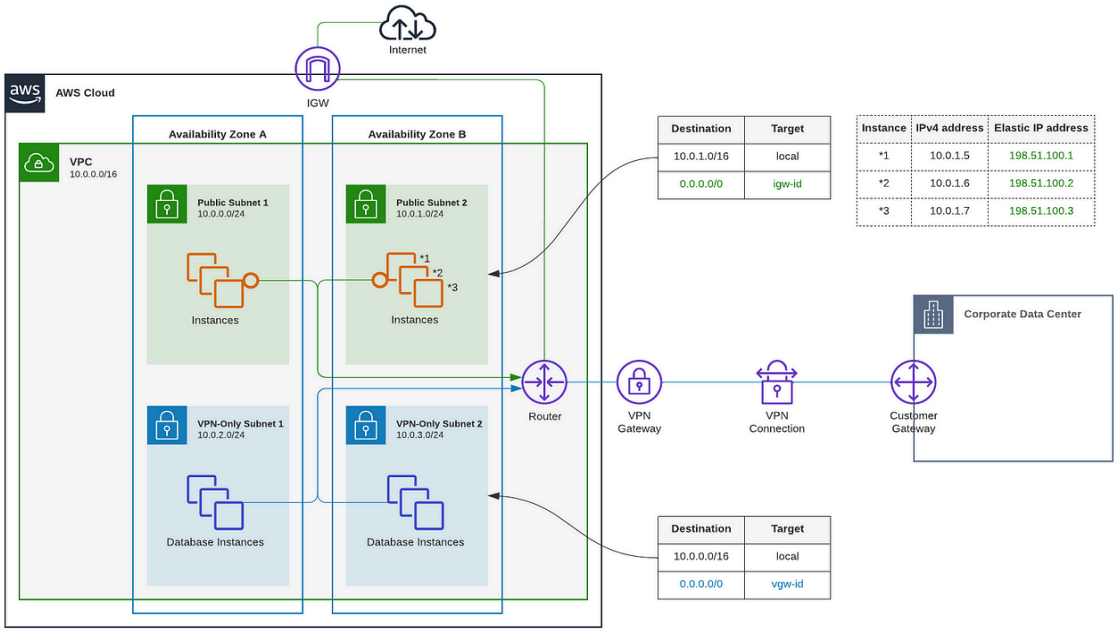
JTT24 Assignment
Cletus Adodo

Task 1.



Components of the VPC and Inter-connectivity

The components of the VPC and Inter-connectivity in the architectural diagram below can be identified and described as follows:

1. **VPC** (10.0.0.0/16):
   The VPC was created within a particular region of the AWS account and with a cidr block of /16.

2. **Subnets**:
   Subnets which stands for sub network can also be identified in the diagram. Subnets are always created within the availability zone of a region and in the above diagram, there are two availability zones which are zone A and Zone B.

   In availability zone A, there are two subnet. One public subnet with IP address 10.0.0.0/24 which means it is on cidr block /24. There is also a private subnet in availability zone A with IP address 10.0.2.0/24.

In availability zone B, there are also two subnets. One public subnet with IP address 10.0.1.0/24 and a private subnet with IP address 10.0.3.0/24

3. **Internet Gateway (IGW)**:
   There is an Internet gateway that connects the VPC to the internet, which also allows the instances in the public subnets to communicate with the outside world or accessible to the internet.

4. **Instances in Public Subnets**:
   There are three instances in the public subnet 2, each with private IPs (`10.0.1.5`, `10.0.1.6`, and `10.0.1.7`) and Elastic IPs (`198.51.100.1`, `198.51.100.2`, and `198.51.100.3`). The Elastic IP addresses which can also be referred to as the public IP enables them to be accessible from the internet.

   I also think the three instances in public subnet 1 is a mirror of what is in public subnet2 hence the reason why a separate IP addresses were not allocated.

5. **Route Tables**:
   There two route tables that has been identified in the diagram which are:
   The public route table and the Private/VPN route table.

   The public route table which is assigned to public subnets directs traffic for the VPC CIDR (`10.0.0.0/16`) locally, while traffic destined for the internet (`0.0.0.0/0`) is routed through the IGW. while the private route table route traffic for the VPN-only subnets for the VPC CIDR locally and traffic destined for external networks such as the on-premises data centre (`0.0.0.0/0`) is routed through the Virtual Private Gateway (VGW).

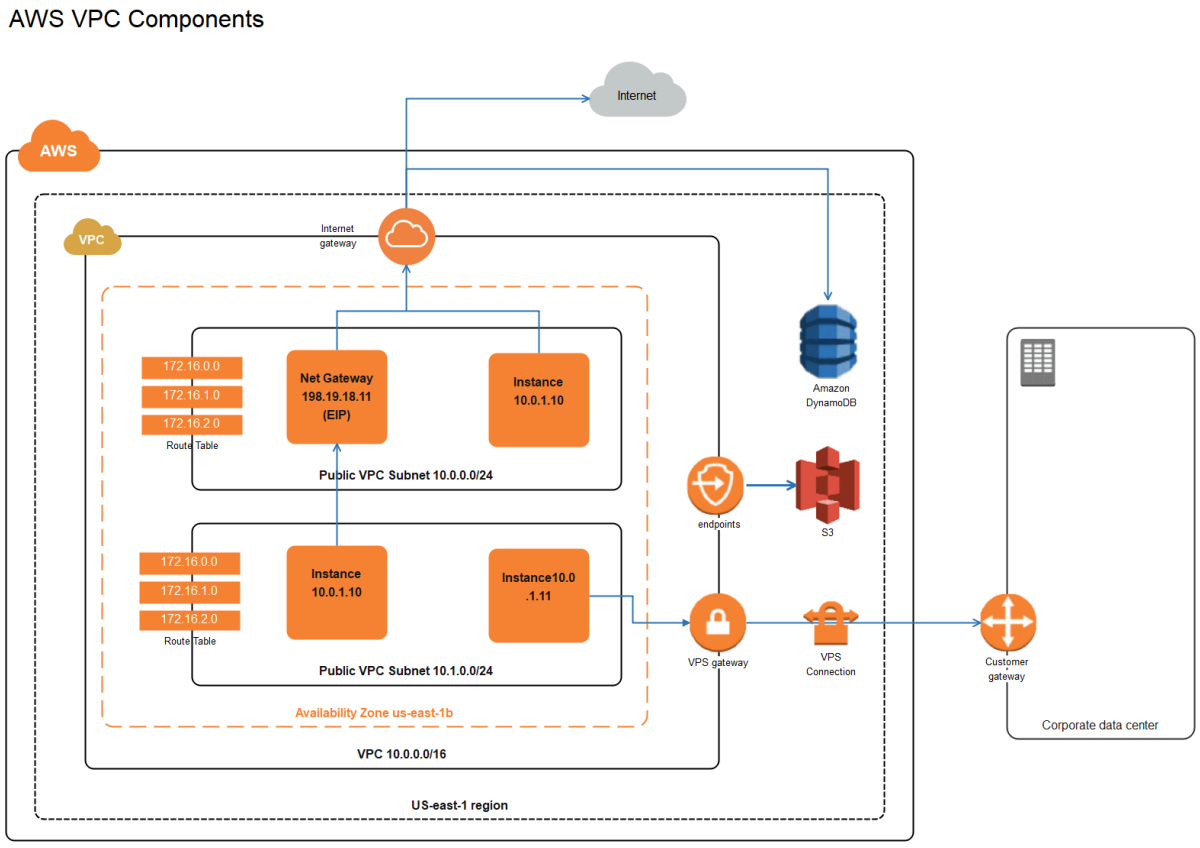
6. **VPN Gateway (VGW)**:
   The VPN Gateway allows secure communication between the VPC and the on-premises corporate data center via the VPN/tunneled connection.

7. **VPN Connection**:
   The encrypted link or tunel between the VPN Gateway (VGW) and the Customer Gateway, allows secure data transfer between the private VPC and the on-premises network enabling traffic between on cloud database and the on-prem data centre.

8. **Customer Gateway**:
   The on-premises side of the VPN connection, located at the corporate data center. It allows resources within the corporate data center to communicate securely with resources in the VPC.
   Kindly note the Customer gateway is on the On-prem-side while the VGW is on the subnet side. This can also be referred to as site-to site VPN connection.

9. **Router**:
   The router manages traffic within the VPC, directing data between subnets and to external networks that is via the IGW for internet-bound traffic and the VPN Gateway for VPN-bound traffic.

Task 2



Components of the VPC and Inter-connectivity

The components of the VPC and Inter-connectivity in the architectural diagram below can be identified and described as follows:

1. **VPC (10.0.0.0/16):**
   The VPC was created within us-east-1 region of the AWS account and with a cidr block of /16.

2. **Subnets:**
   There are two public subnet created within the VPC, which are:
   Public Subnet 1 with IP address 10.0.0.0/24 and another Public Subnet 2 with Ip address 10.1.0.0/24.

3. **Instances:**
   Two instances have been identified in the diagram, both subnets can be access the internet. The first instance as an IP address 10.0.1.10 and it is located in public subnet 1 and connected to the internet via NAT Gateway and Internet Gateway. The second instance is has the IP address 10.0.1.11 and it is located in the subnet 2 and can only access the internet via the Internet Gateway

4. **NAT Gateway 198.19.18.11:**
   The (NAT) Gateway identified in the diagram is assigned an Elastic IP 198.19.18.11 and enables outbound internet traffic from instances in private subnets although there is no private subnets shown in this diagram.

5. **Internet Gateway:**
   The Internet Gateway connects the public subnets to the internet, allowing instances in the public subnet to send and receive internet traffic.

6. **Route Tables:**
   There is only one route table identified in the above diagram and it is associated with both public subnets. It includes routes directing internet-bound traffic (0.0.0.0/0) through the Internet Gateway, allowing instances to communicate with external resources on the internet.

7. **Amazon S3:**
   S3 is an AWS service used to store and retrieve data. The diagram shows that there an endpoint within the VPC for the S3 bucket, this allows a secure, private access to S3 buckets without passing through the public internet. Kindly note the end point is situated outside of the subnet and the availability zone but it is within the VPC.

8. **Amazon DynamoDB:**
   DynamoDB is a fully managed NoSQL database service. The diagram shows an endpoint for DynamoDB, which also enables private access to the service within the VPC.

9. **VPC Gateway & VPN Connection:**
   The VPC Gateway enables a VPN Connection to the on-premises Corporate Data Center. This allows secure communication between the on-premises network and the public subnet.
   The Customer Gateway represents the device on the corporate data center's side of the VPN connection.