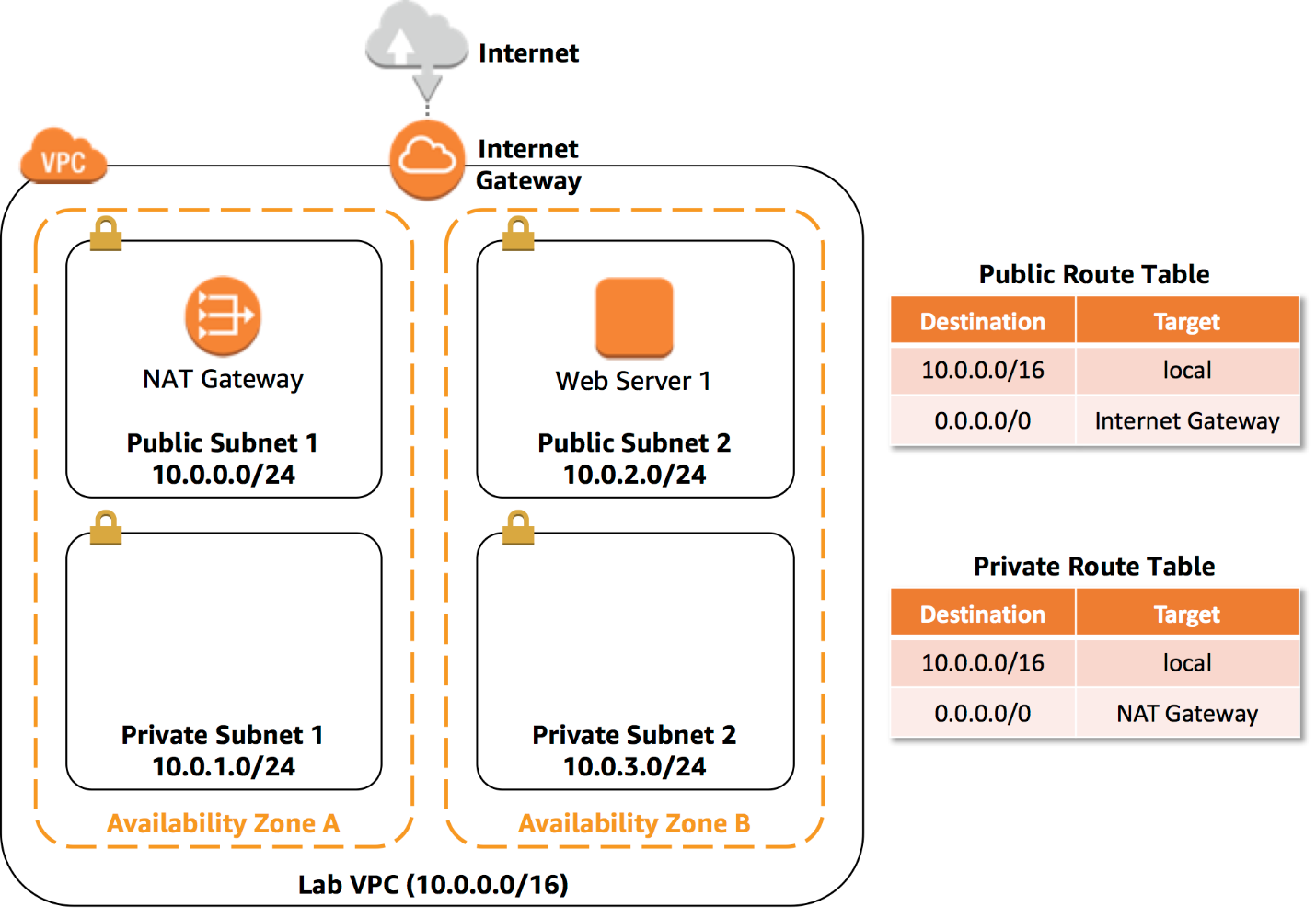
AWS Training and certification  
  
Amazon Virtual Private Clou (Amazon VPC) enables you to launch Amazon Web services (AWS) resources into a virtual network that you defined. This Virtual network closely resembles a traditional network that you would operate in your own data center. with the benefits of using the scalable infrastructure of AWS.



With this lab you can:

* Create a VPC.
* Create subnets.
* Configure a Security group.
* Launch an EC2 instance into a VPC.

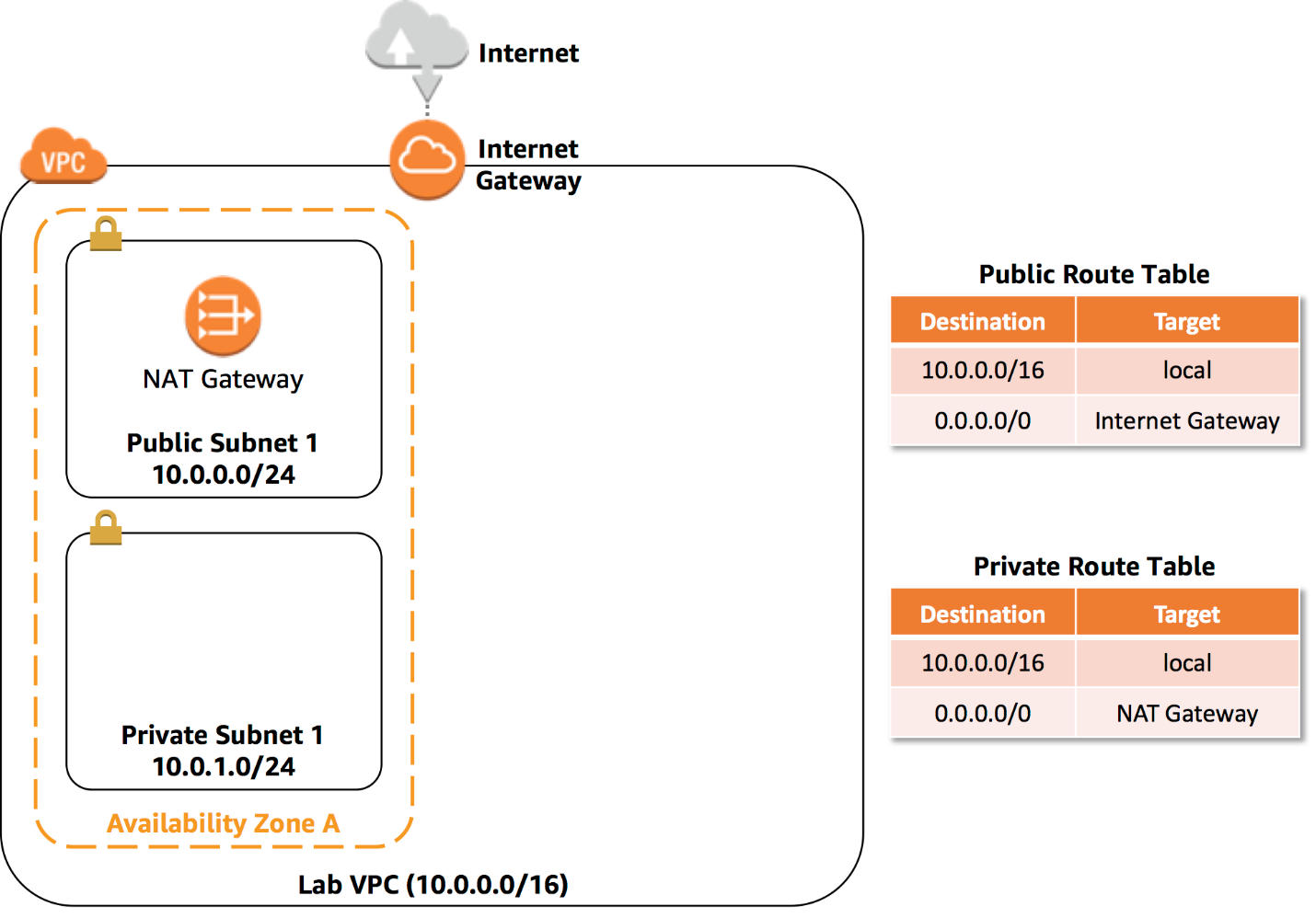
**CREATE YOUR VPC**

In this task, you will use the VPC Wizard to create a VPC, an Internet Gateway and two subnets in a single Availability Zone. An Internet gateway (IGW) is a VPCcomponent 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 will also create a NAT Gateway, which is used to provide internet connectivity to EC2 instances in the private subnets.

1. In the **AWS Managment Console,** on the “Services” menu, click **VPC**
2. Click “*Launch VPC Wizard”* button
3. In the left navigation pane. click **VPC with Public and Private Subnets** (the second option).
4. Click”*Select”* button and then configure:  
   - **VPC name:** Lab VPC  
   - **Availability Zone:** Select the *first* Availability Zone  
   - **Public subnet name:** Public Subnet 1   
   - **Availability Zone:** Select the *first* Abailability Zone (the same as used above)  
   - **Private subnet name:** Private Subnet 1   
   - **Elastic IP Allocation ID:** Click n the box and select the displayed IP address
5. Click **Create VPC** button  
   The wizzardwill create your VPC.
6. Once it is complete, click “**ok**” button   
     
   The wizzard has provisioned a VPC with a public subnet and a private subnet in the same Availability Zone, together with route tables for each subnet:



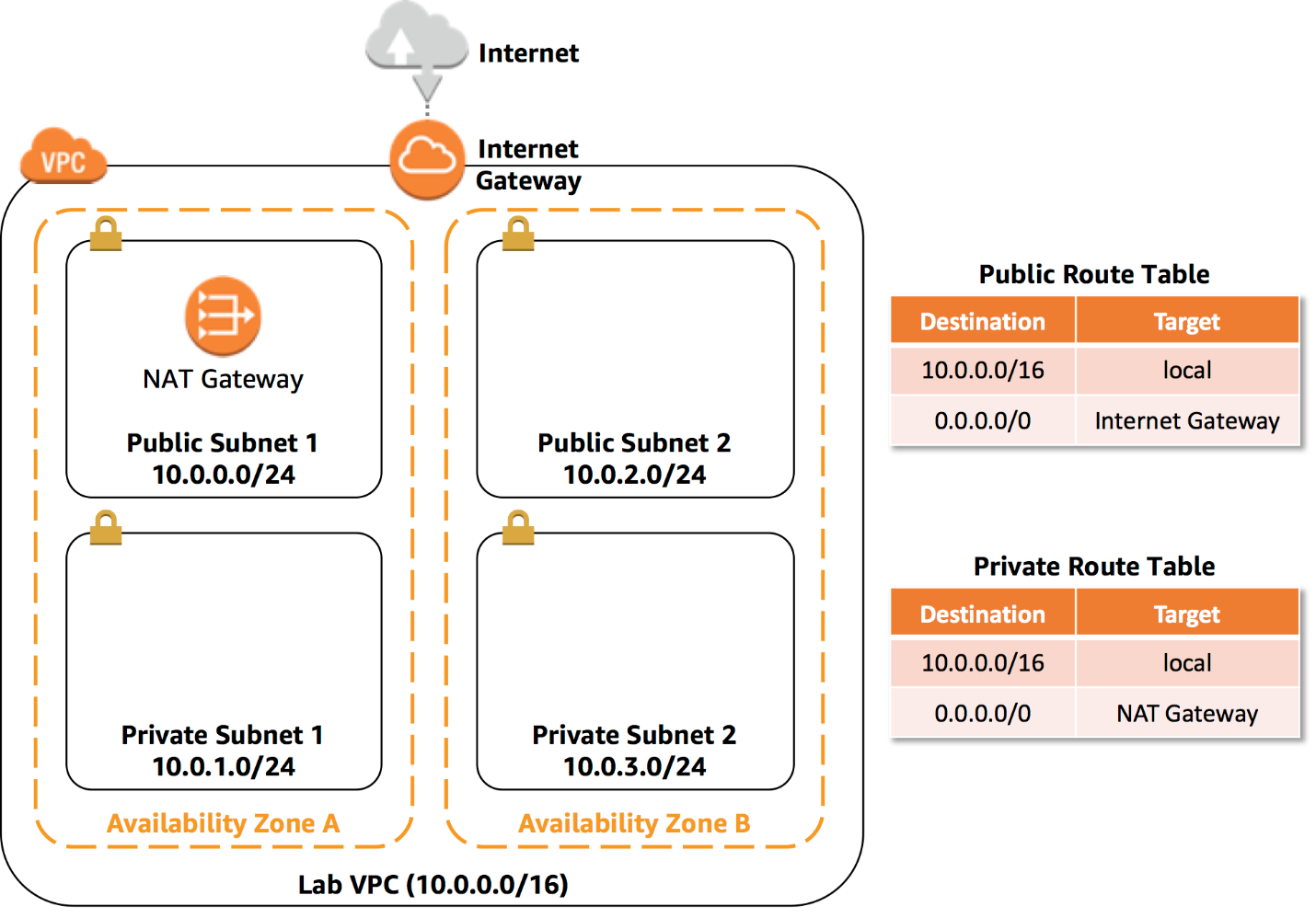
The public Subnet has a CDIR of **10.0.0.0/24,**which means that it contains all IP addresses starting with **10.0.0.x**

The Private Subnet has a CDIR 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 will create two additional subnets in a second Availability Zone. This is iseful for creating resources in multiple Availability Zones to provide *High Availability.*

1. In the left navigation pane. click **Subnets.**  
   First, you will create a second Public Subnet.
2. Click “Create subnet” then configure:  
     
   - **VPC ID:** Lab *VPC*  
   - **Name tag:** Public Subnet 2  
   - **Availability Zone:** Select the *second* Availability Zone  
   - **IPv4 CIDR block:** 10.0.2.0/24  
     
     
   The subnet will have all IP addresses starting with **10.0.2.x.**
3. Click “Create Subnet” button.  
     
   You will now create a second Private Subnet.
4. Click “Create subet” then configure:   
     
   - **VPC ID:** *Lab VPC*  
   - **Subnet name:** Private Subnet 2   
   - **Availability Zone:** Select the *second* Availability Zone  
   - **CIDR lock:** 10.0.3.0/24  
     
   The subnet will have all the IP addresses starting wih **10.0.3.x.**
5. Click “Create Subnet “ button.  
     
   You will now configure the Private Subnets to route internet-bound trafic to the NAT Gateway so that resources in the Private Subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring *Route Table.*  
     
   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.
6. In the left navigation pane, click **Route Tables.**
7. Select the “marck check” the route table with **Main = Yes** and **VPC.** (Expand the VPC ID column if necessary to view the VPC name.)
8. In the Lower pane, click the **Routes** tab.  
     
   Note that **Destination 0.0.0.0/0** is set to **Target nat-xxxxxxxx.** 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 Priavate Subnets. You will now add a name to the Route Table to make this easier to recognize in the future.
9. In the **Name** column for this route table, click the pencil and then type “ Private Route Table and click.
10. In the lower pane, click the **Subnet Associations** tab.   
      
    You will now associate this route tabe to the Private Subnets.
11. Click **Edit subnet associations**
12. Select both **Private Subnet 1** and **Private Subnet 2.**  
      
    You can expand the *Subnet ID* column to view the Subnet names.
13. Click “*Save”* button  
      
    You will now configure the Route Table that is used by the Public subnets.
14. Select the route table with **Main = No** and **VPC = Lab VPC** (and deselect any other subnets).
15. In the **Name** column for this route table, click the pencil and then type “Public Route Table, and click the check.
16. In the lower pane, click the **Routes** tab.   
      
    Note that **Destination 0.0.0.0/0** is set to **Target igw-xxxxxxxx,** which is the Internet Gateway. This means that internet-bound raffic will be sent straight to the internet via the Internet Gateway.  
      
    You will now associate this route table to the Public Subnets.
17. Click the **Subnet Associations** tab.
18. CLick “**Edit subnet associations”** button.
19. Select checkmark both **Public Subnet 1** and **Public Subnet 2.**
20. Click “Save” button.  
      
    Your VPC now has public and private subnets configured in two Availability Zones:



**TASK 3: CRATE A VPC SECURITY GROUP**

In this task, you will create a VPC security group, which acts as a virtual firewall. 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 rom its associated instances.