**Placement Empowerment Program**

**Cloud Computing and DevOps Centre**

**Set Up a Private Network in the Cloud**

**“*Create a Virtual Private Cloud (VPC) with subnets for your instances. Configure routing for internal communication between subnets...*”**

Name: **DHARSHINI P** DEPARTMENT: **IT**



**Introduction**

In cloud environments, isolating resources within a secure network is crucial for performance, security, and scalability. A **Virtual Private Cloud (VPC)** provides a logically isolated network where cloud instances can communicate securely. By configuring **subnets, route tables, and security groups**, you can control traffic flow within your cloud infrastructure.

**Overview**

**VPC (Virtual Private Cloud)** allows you to define a private network within a cloud provider like **AWS, Azure, or Google Cloud**. Within a VPC, you can create **subnets** (smaller network segments) to organize and control internal communication. Routing and security rules dictate how instances communicate within the network and with external resources

**Objective**

**The primary objectives of this POC are:**

* Create a **VPC** to isolate cloud instances in a private network.
* Set up **subnets** for organizing resources (e.g., public and private subnets).
* Configure **internal routing** to allow secure communication between subnets.
* Implement **security controls** to manage traffic flow and access

**Important**

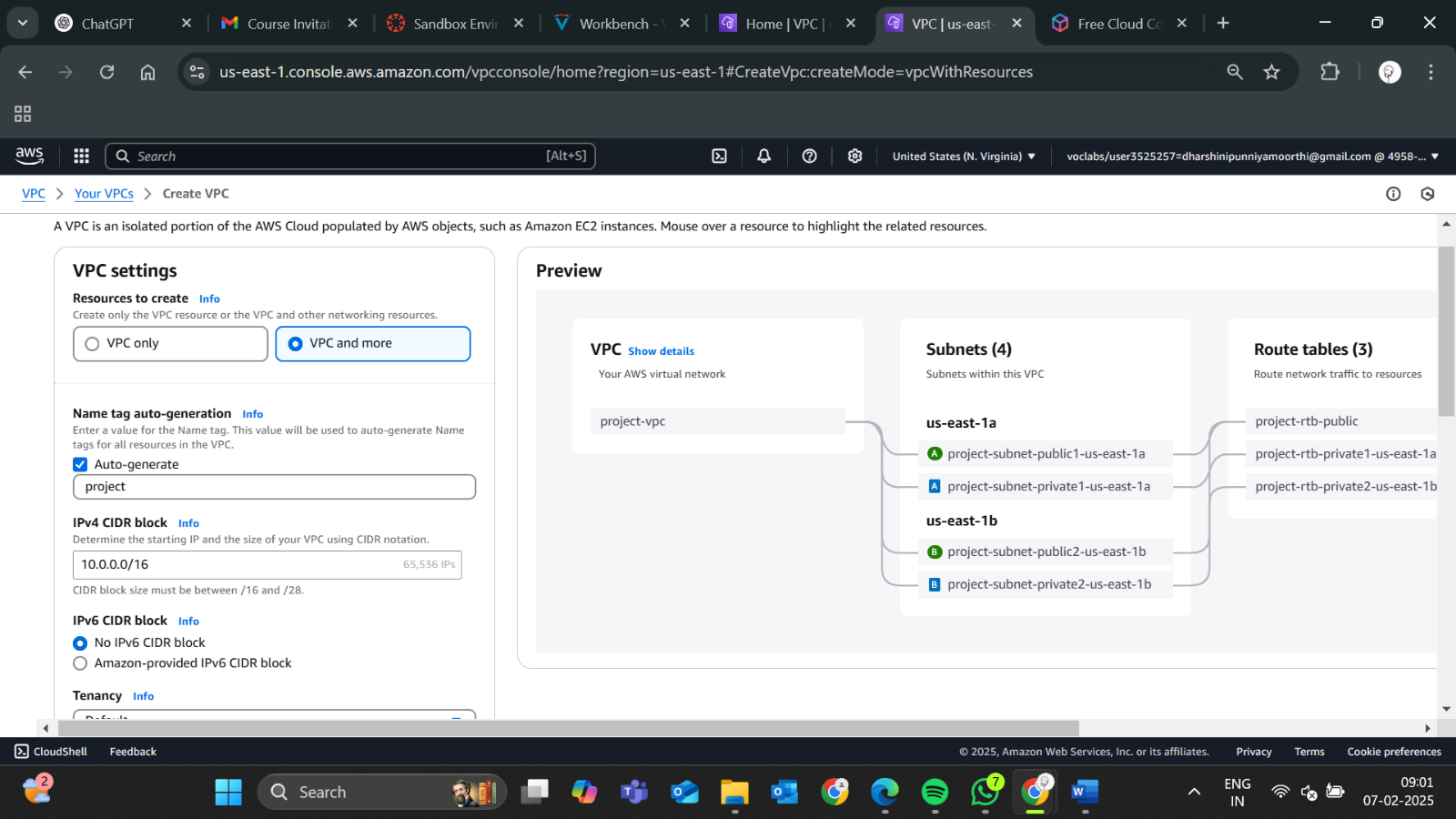
* **Enhanced Security** – Keeps internal resources private and limits exposure to the public internet.
* **Better Network Organization** – Segregates workloads using subnets for efficient management.
* **Improved Performance** – Reduces latency by enabling direct internal communication.
* **Controlled Access** – Configures firewalls and security groups for precise traffic control.
* **Scalability** – Easily expand the network by adding more subnets and instances

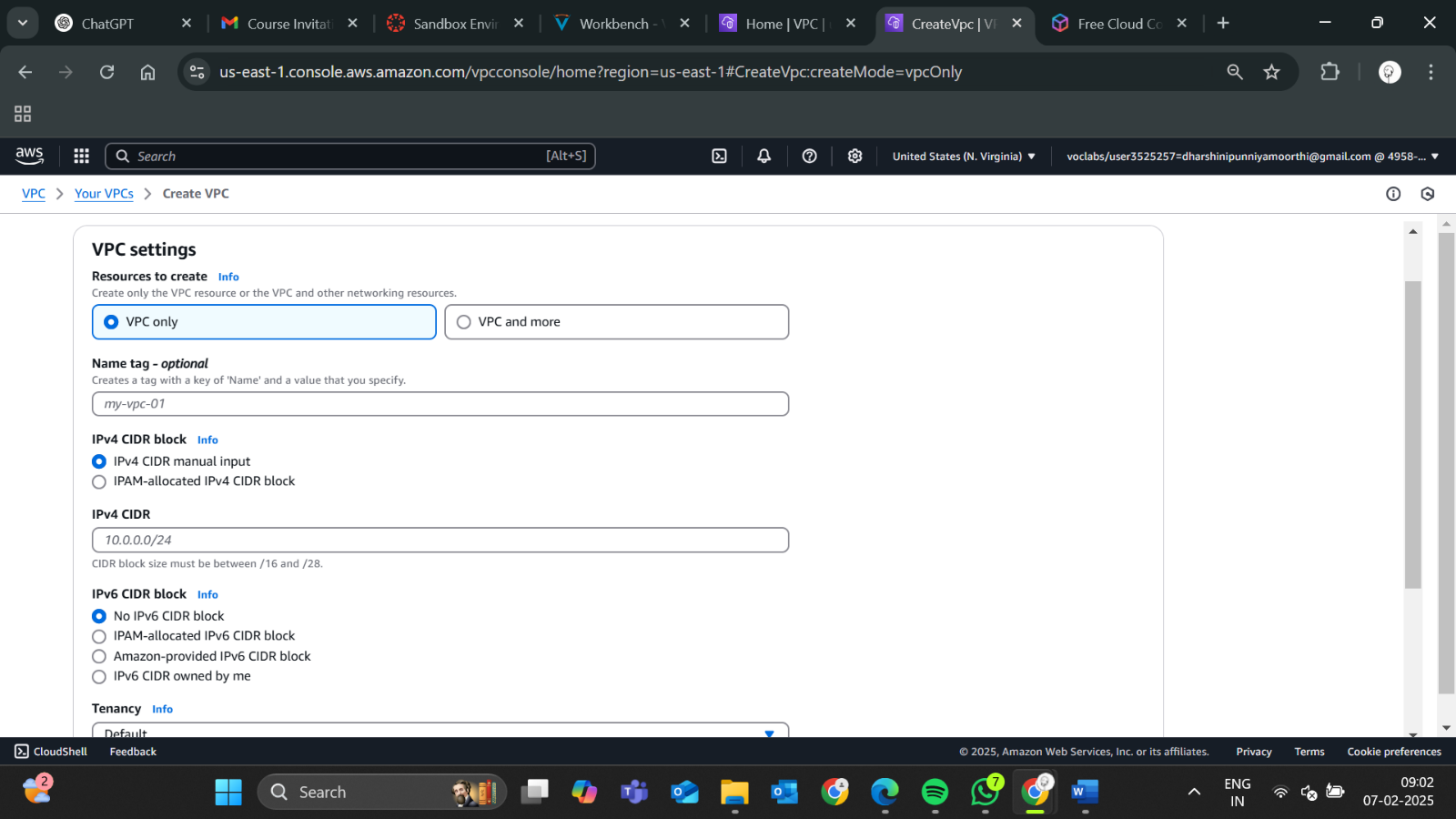
**Steps to Set Up a Private Network in the Cloud**

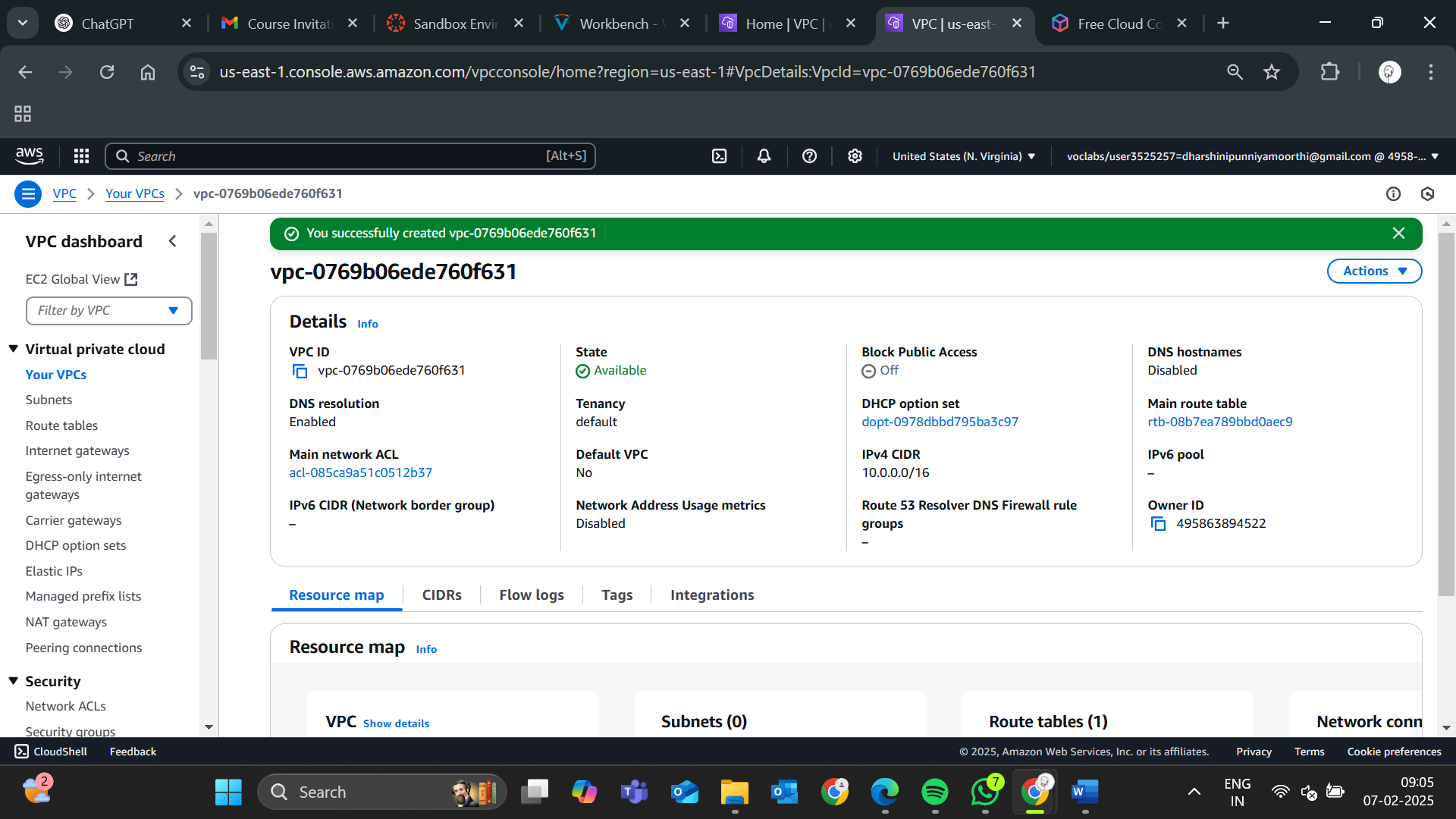
**Step 1:**

**Create a VPC**

* In your cloud provider’s **VPC dashboard**, create a new **VPC**.
* Define a **CIDR block** (IP range) for the VPC (e.g., 10.0.0.0/16).



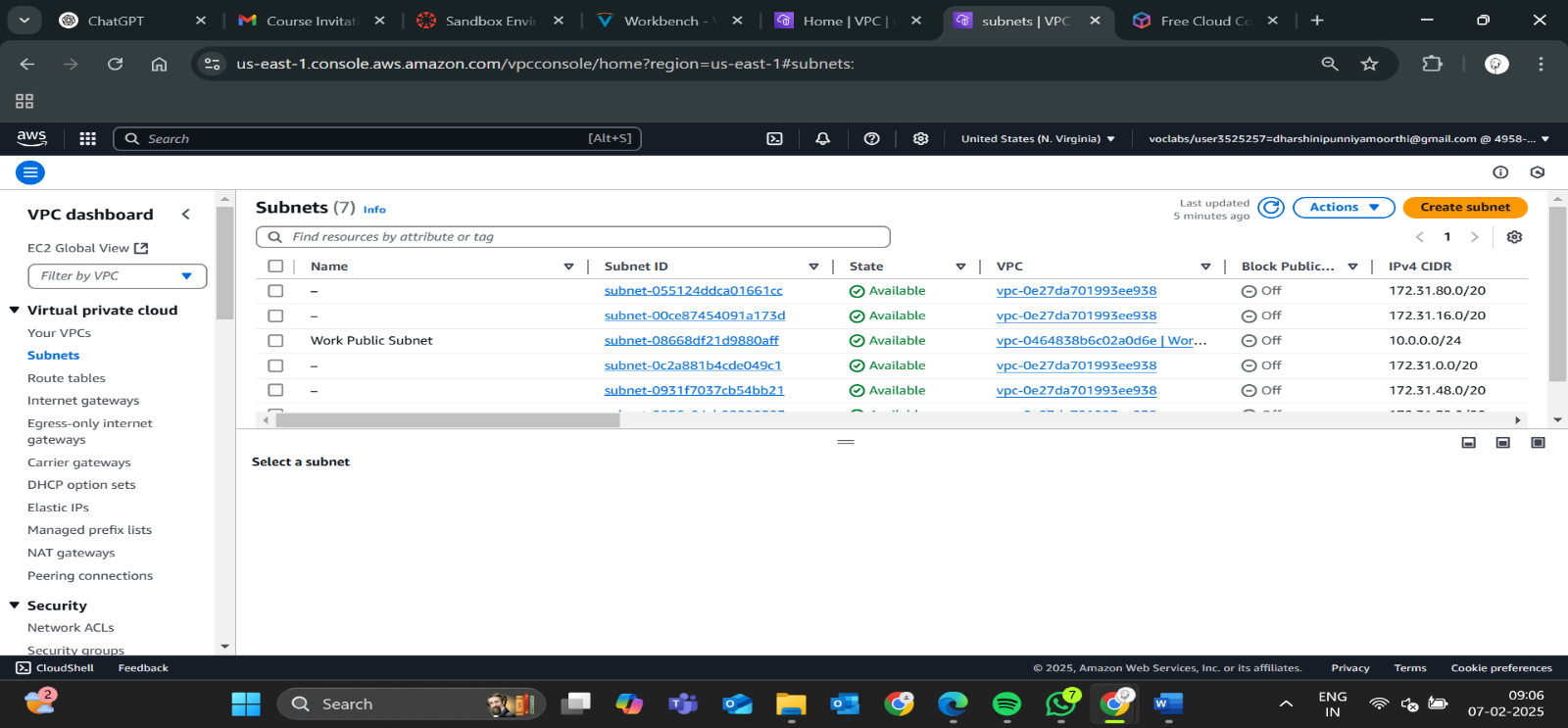


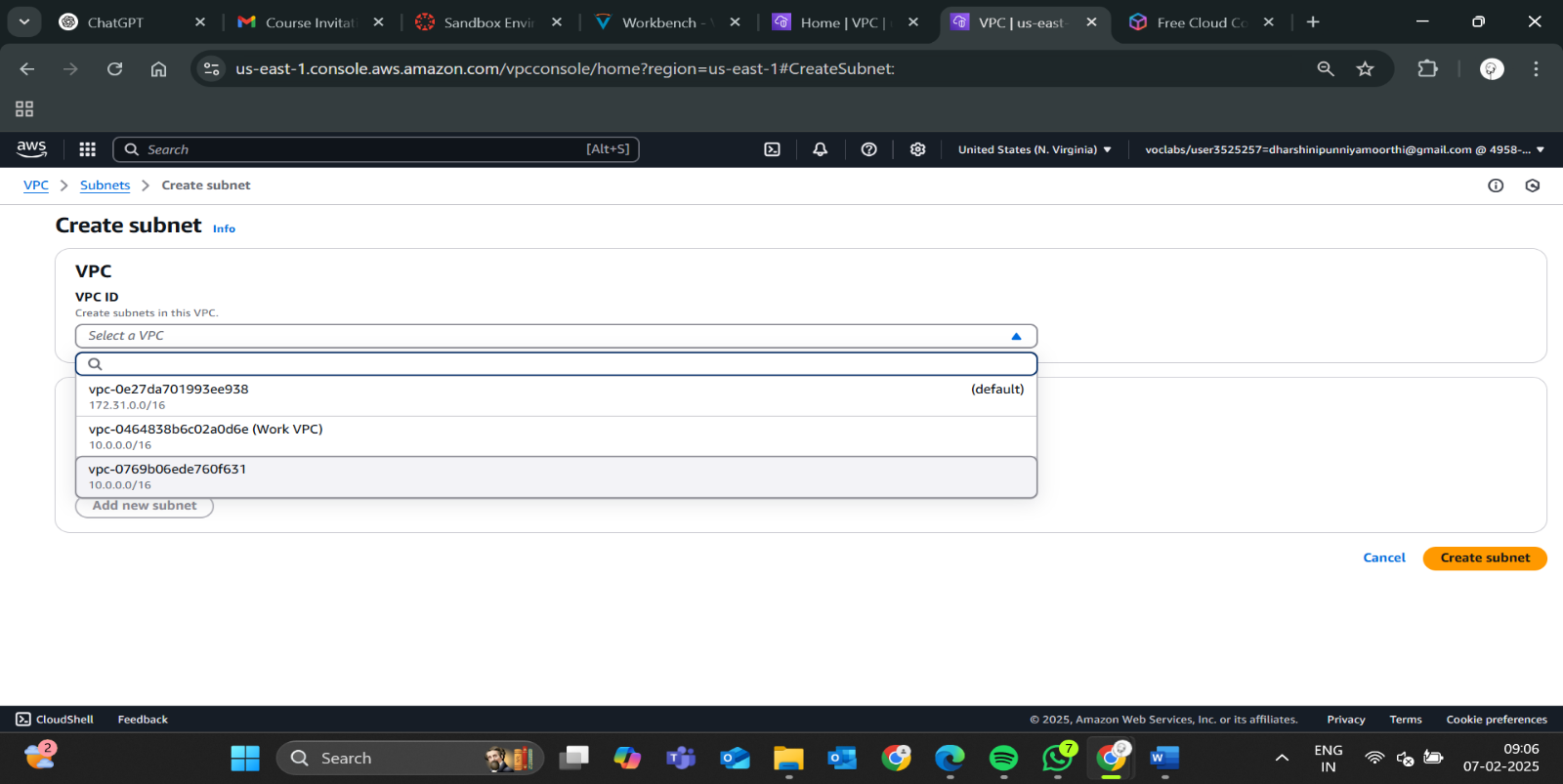


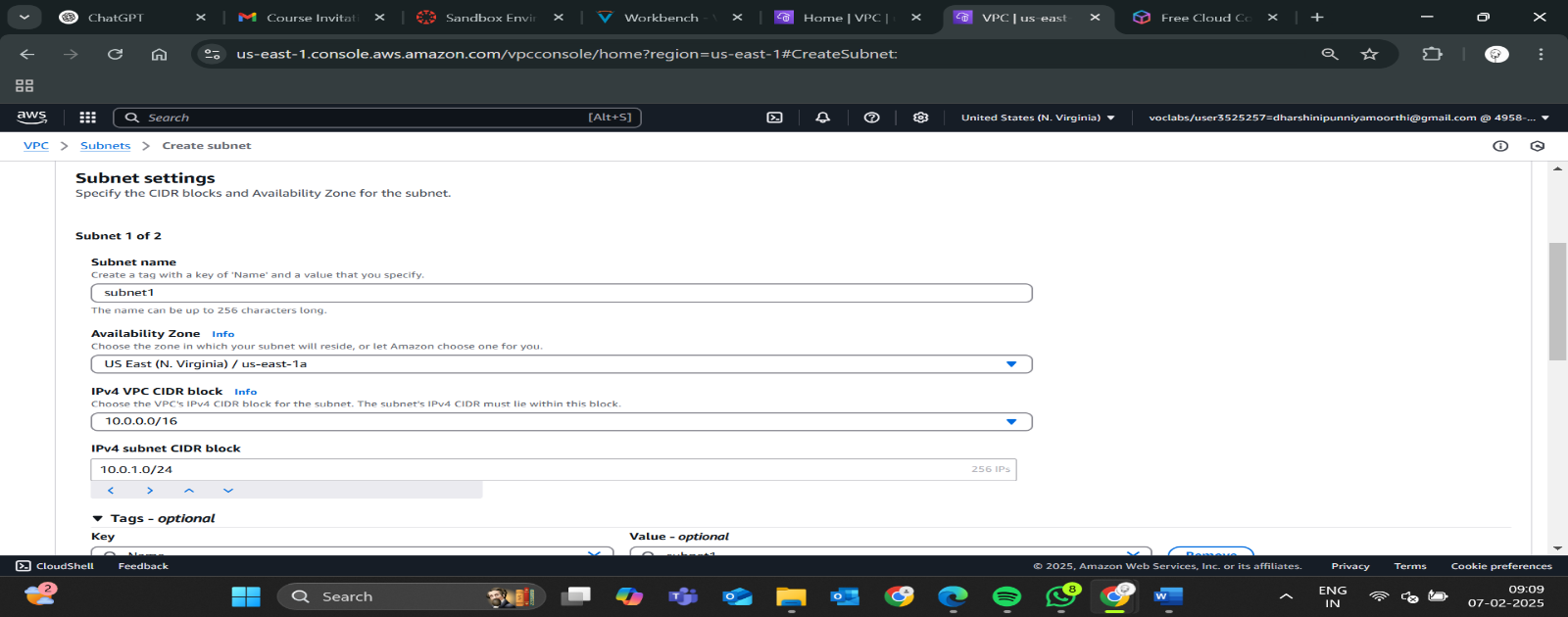
**Step 2:**

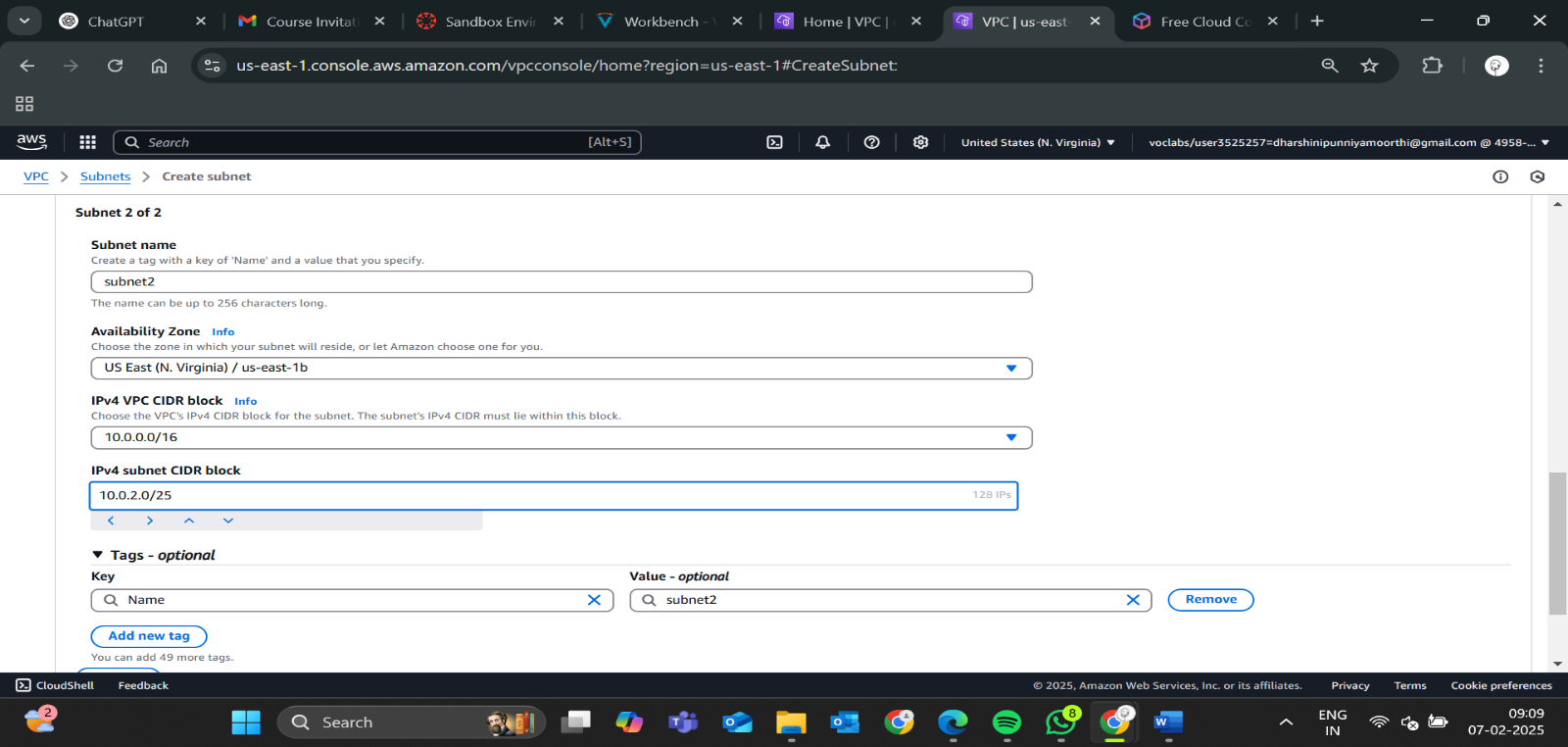
**Create Subnets**

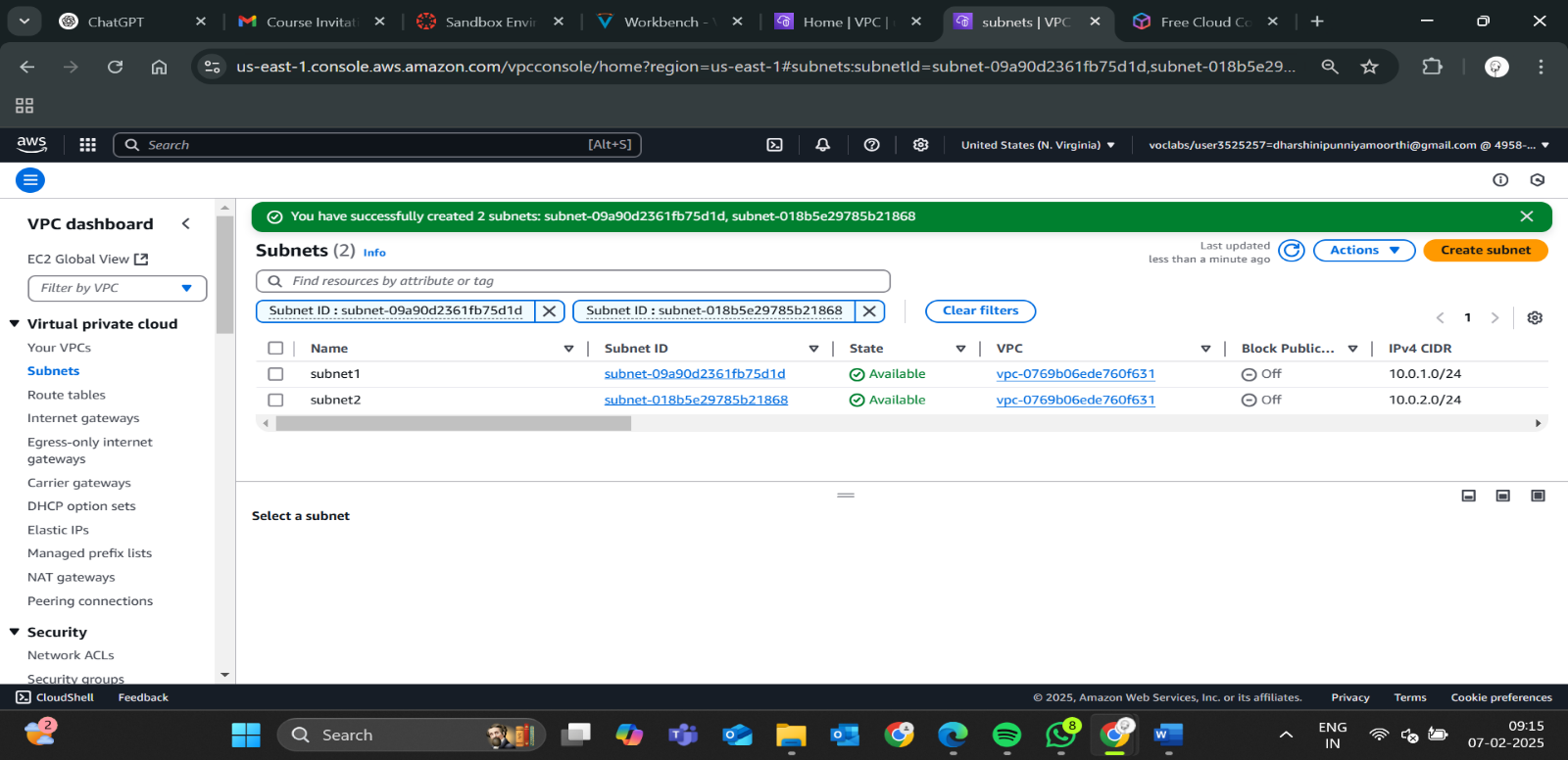
* Create multiple **subnets** within the VPC (e.g., **public** and **private** subnets).
  + **Public subnet**: Used for instances that need internet access.
  + **Private subnet**: Used for internal services like databases.







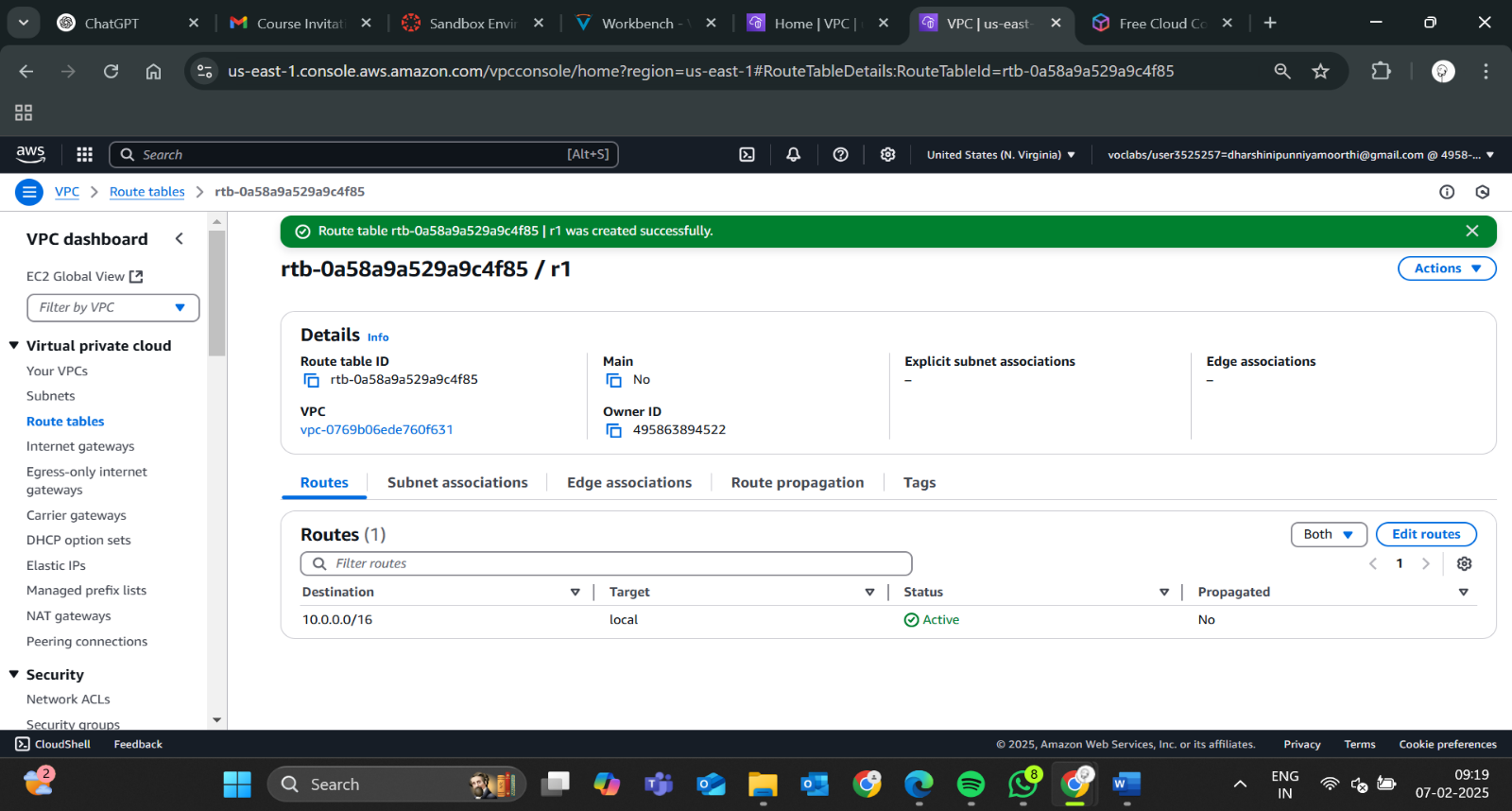


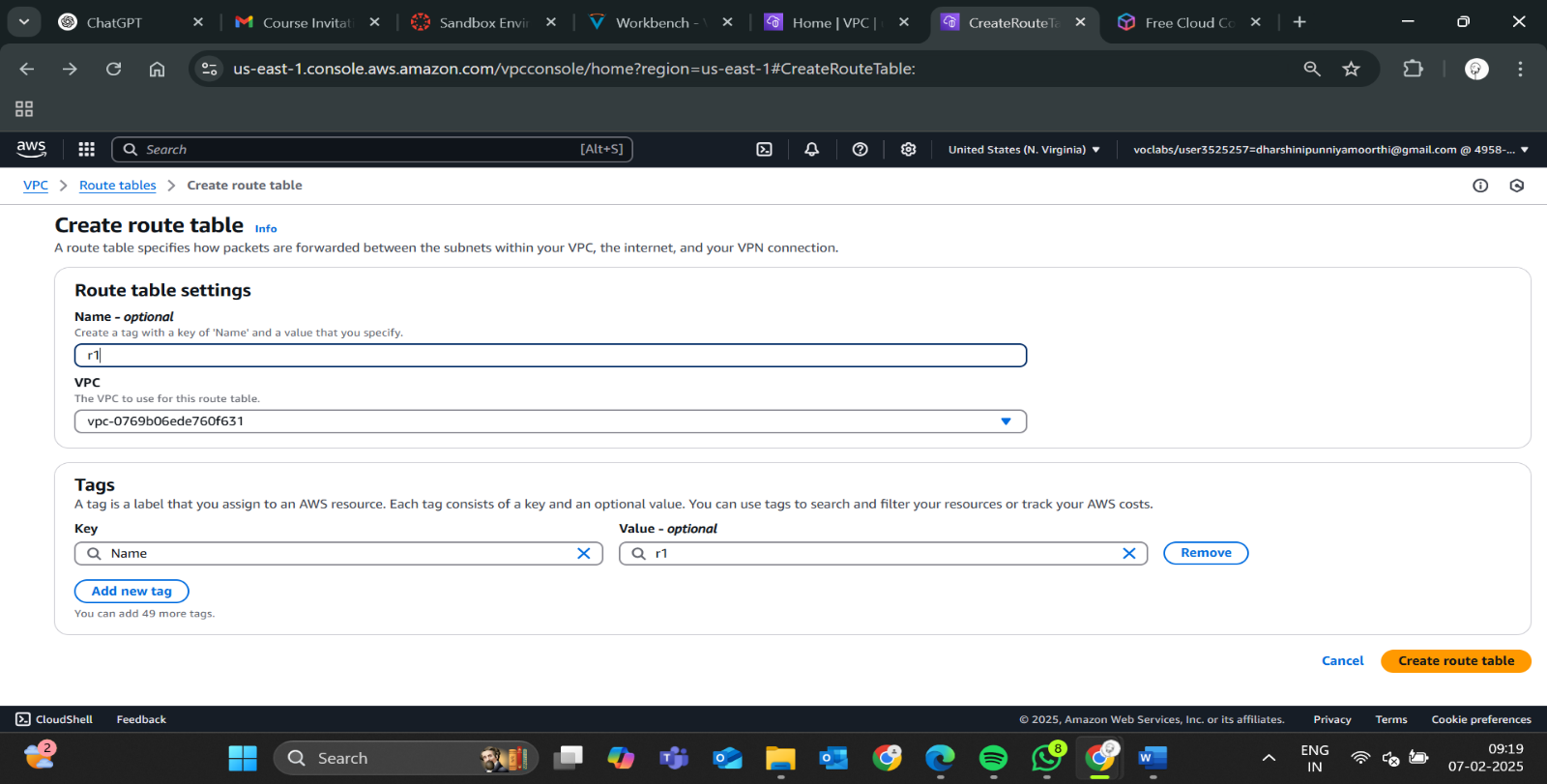


**Step 3:**

**Configure Routing Tables**

* Create a **route table** for each subnet.
* Define routing rules:
  + Public subnet → **Route traffic to the internet via an Internet Gateway (IGW)**.
  + Private subnet → **Allow internal communication and route external traffic through a NAT Gateway or NAT Instance**.

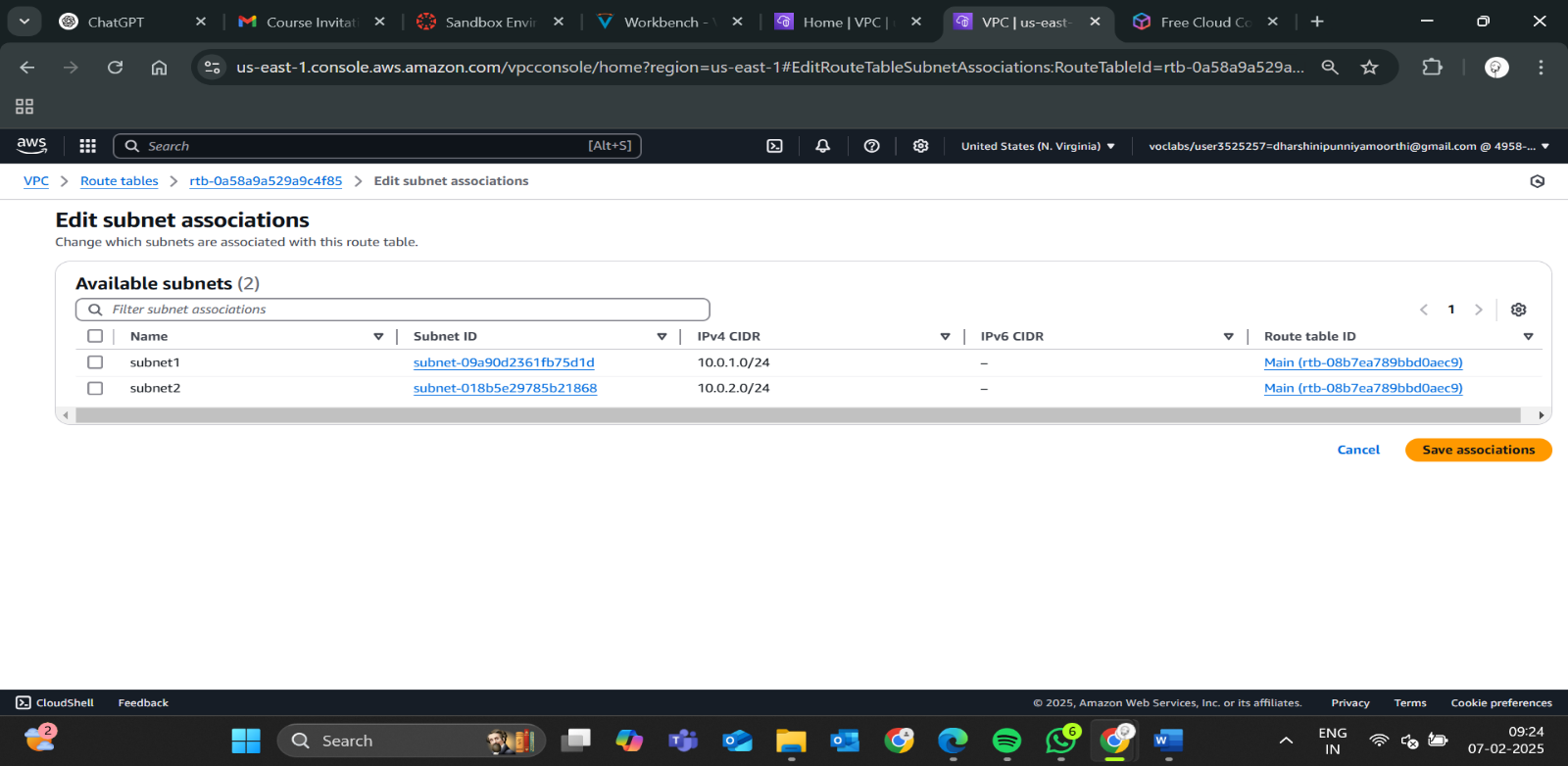


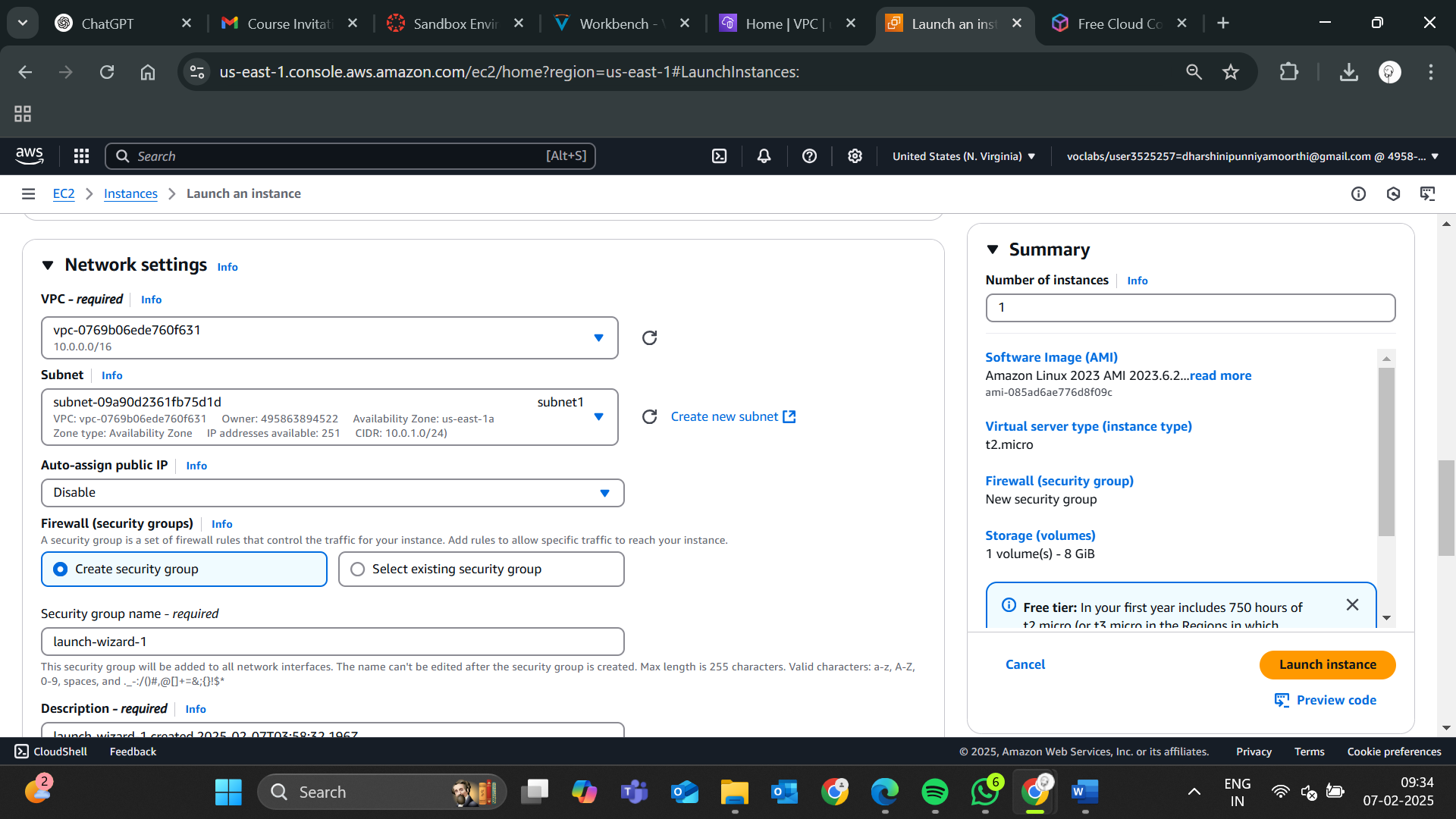


**Step 4:**

**Set Up Security Groups & Network ACLs**

* **Security Groups**: Control inbound and outbound traffic for instances.
* **Network ACLs (Access Control Lists)**: Define rules for subnet-level traffic filtering.

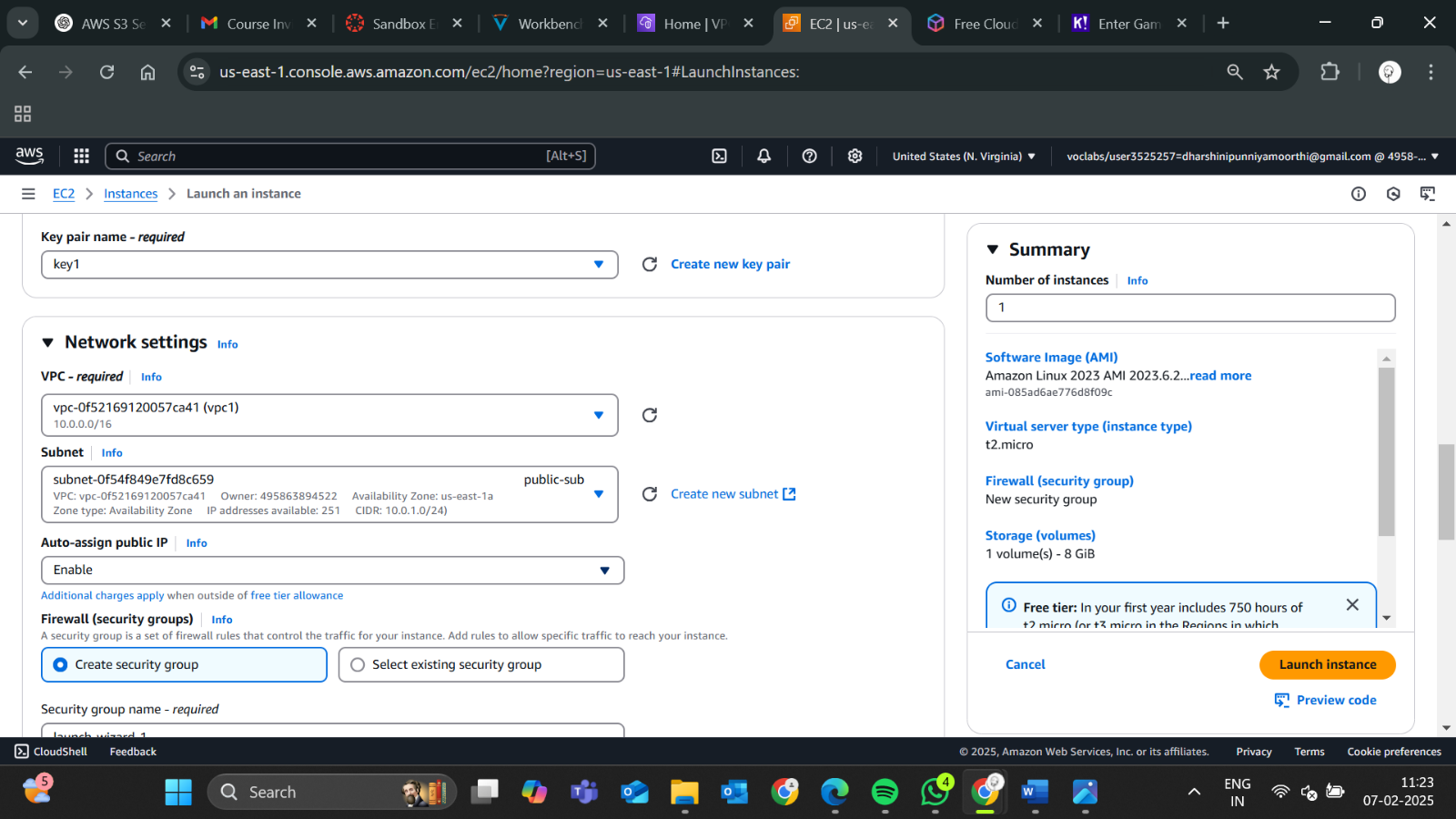


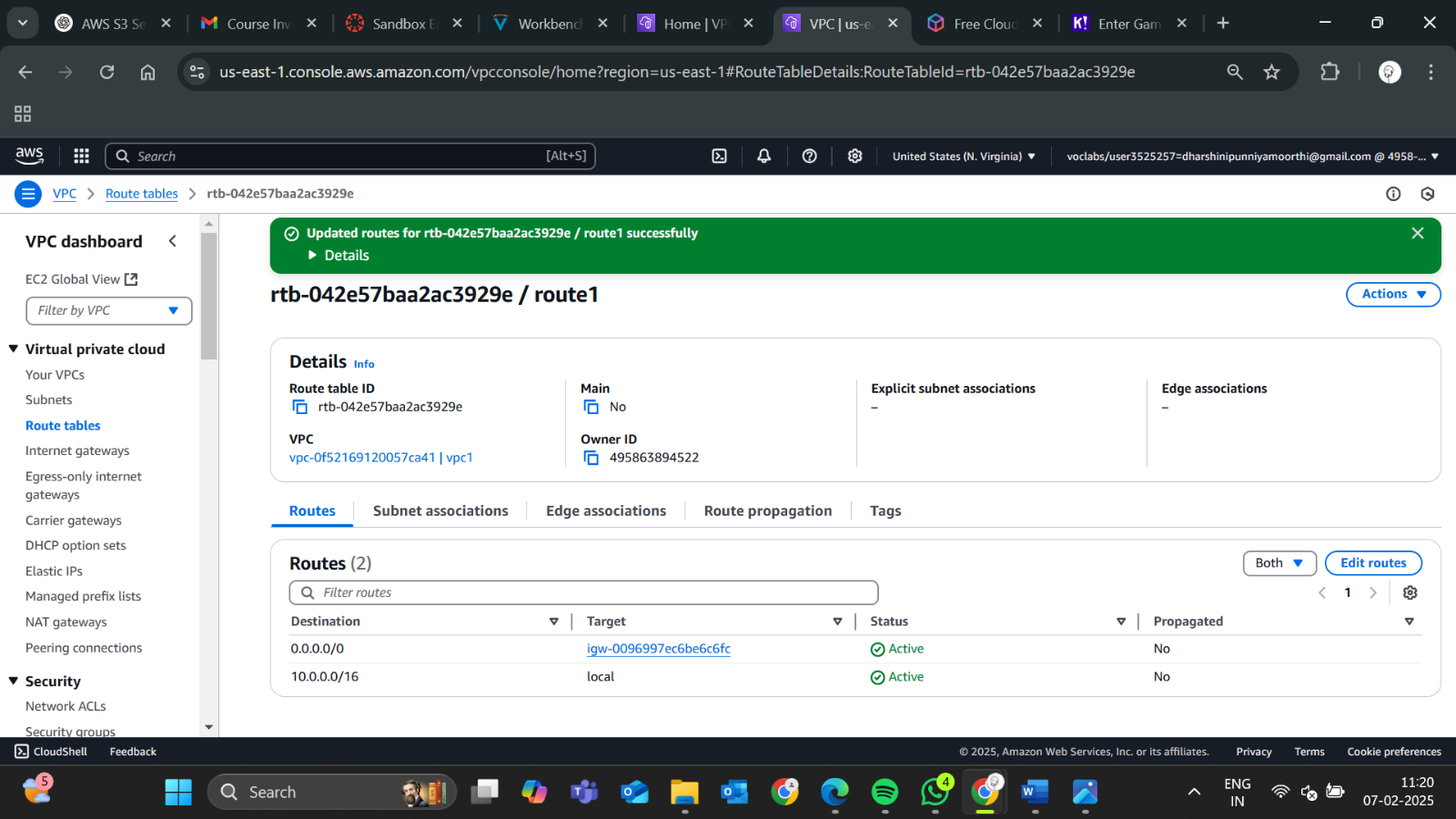


**Step 5:**

**Launch Instances in the Subnets**

* Deploy cloud instances (VMs) in the configured **public** and **private subnets**.
* Assign private IP addresses to enable internal communication.





**Step 6:**

**Test Internal Connectivity**

* Use tools like **ping** or **telnet** to verify internal communication between instances.
* Ensure security groups allow the required traffic between subnets.

**Expected Outcome:**

**By completing this POC, you will:**

* A **secure, private cloud network** with controlled access.
* **Internal communication** between instances in different subnets.
* **Isolated workloads** (e.g., public-facing web apps in the public subnet, databases in the private subnet).
* **Optimized network performance** with reduced exposure to the public internet.