St. JOSEPH'S GROUP OF INSTITUTIONS
OMR, CHENNAI - 119

aws

Placement Empowerment Program

Cloud Computing and DevOps Centre

Create a virtual private network in cloud:Add a subnets and configure routetable between the subnets.

Name:Anumitha M

Department : AML

St. JOSEPH'S COLLEGE OF ENGINEERING | St. JOSEPH'S INSTITUTE OF TECHNOLOGY

AUTONOMOUS INSTITUTIONS, AFFILIATED TO ANNA UNIVERSITY

Introduction:

Creating a Virtual Private Network (VPN) in the cloud involves setting up a Virtual Network (VNet) to securely connect cloud resources with on-premises infrastructure. By dividing the VNet into multiple subnets, you can organize resources based on their functionality (e.g., web servers, application servers, and databases) while applying security controls to each subnet. Configuring route tables is essential to manage traffic flow, enabling communication between subnets and directing traffic to external destinations, like the internet or on-premises networks through a VPN Gateway. This setup ensures secure, efficient, and scalable network traffic management, facilitating a hybrid architecture that integrates on-premises and cloud resources.

Objective:

The goal is to:

Set up a Virtual Network (VNet) in the cloud to provide secure communication between cloud resources.

Divide the VNet into subnets to logically separate resources based on their functionality (e.g., web, app, database servers).

Configure route tables to control and manage traffic flow between subnets and external networks.

Enable secure communication between on-premises infrastructure and cloud resources via a VPN Gateway.

Apply security policies like Network Security Groups (NSGs) to control access and traffic within each subnet.

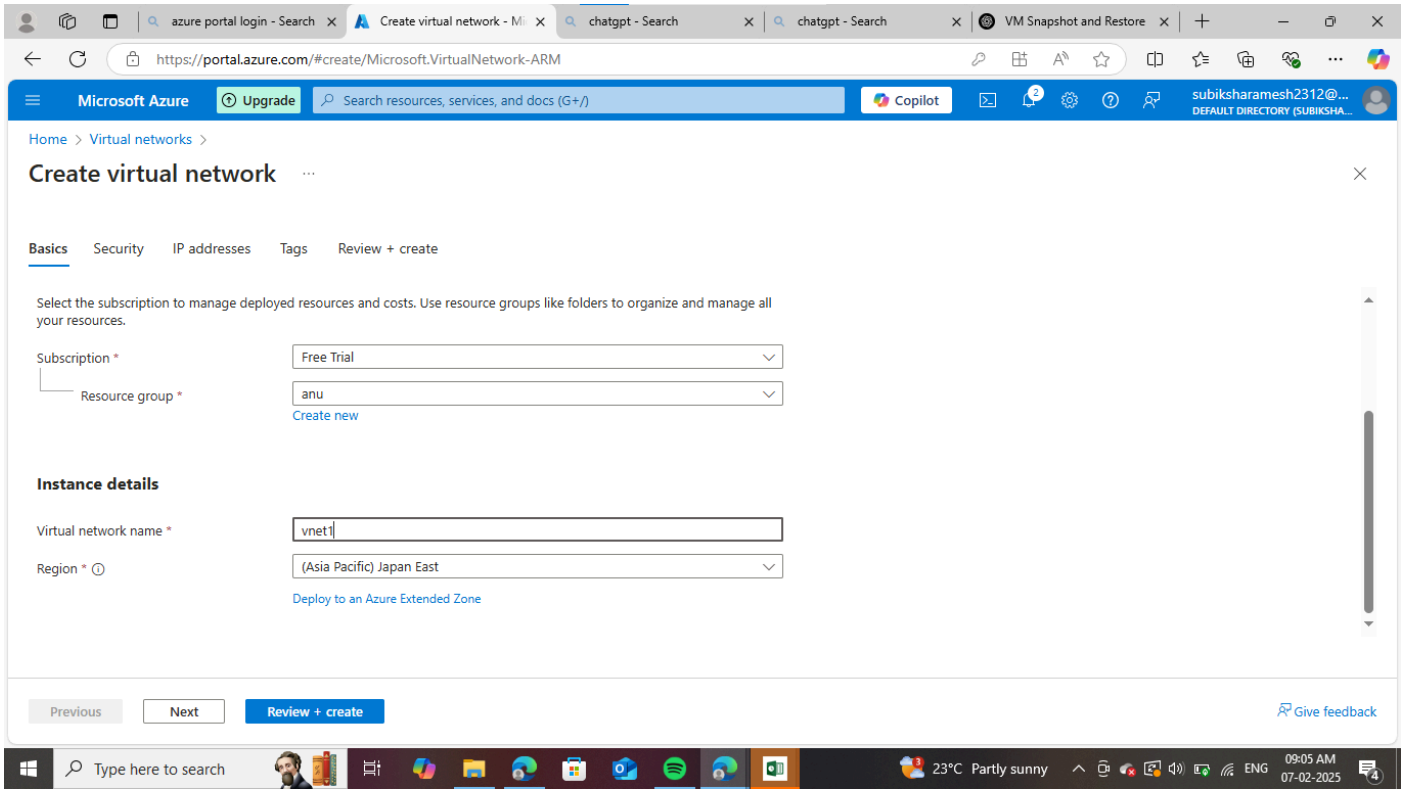
Optimize network performance by organizing resources into subnets and routing traffic efficiently based on business needs.

Ensure scalability and flexibility in network design to support growing cloud-based applications and hybrid architectures.

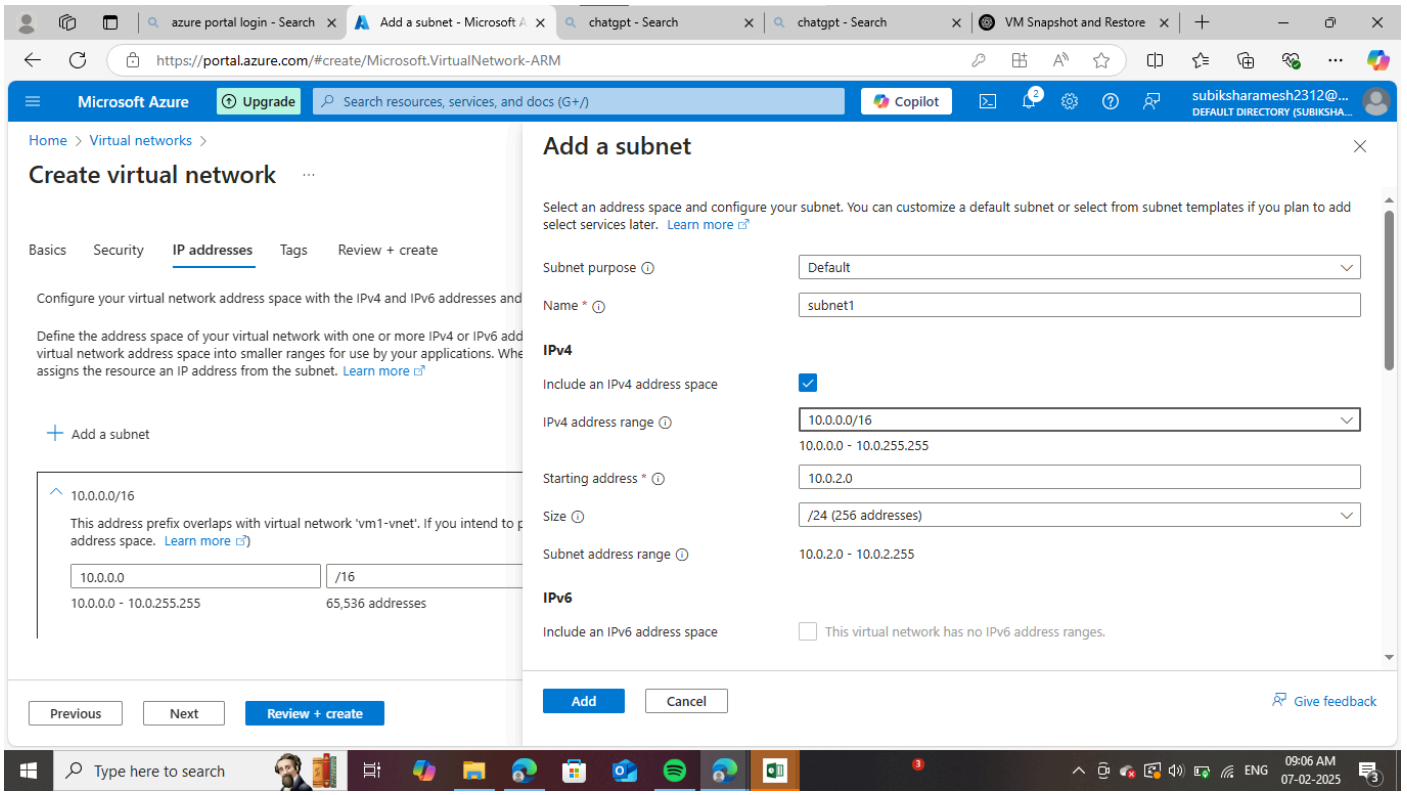
Provide hybrid connectivity for integrating on-premises networks with cloud environments securely.

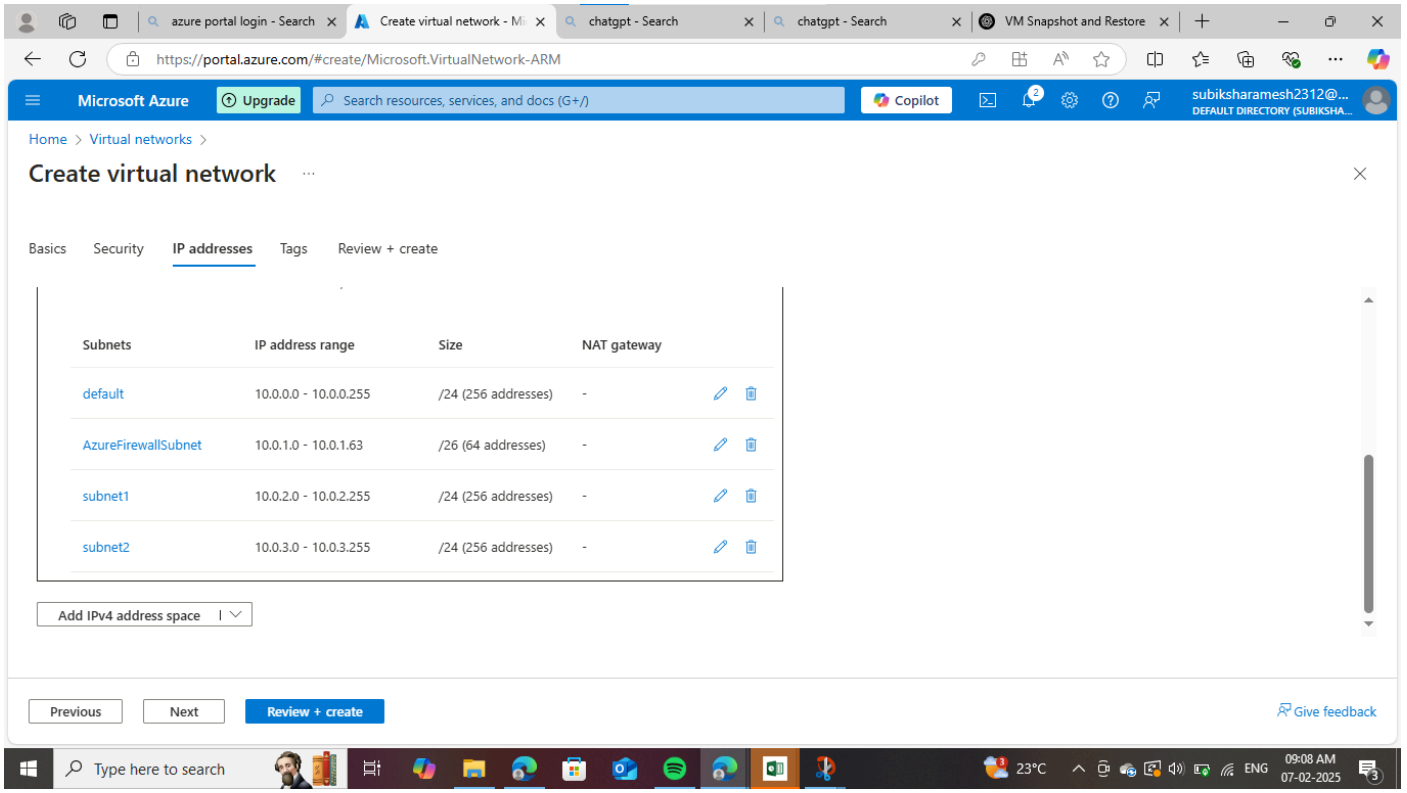
Step-by-Step Procedure:

STEP 1: *Create a virtual private network*

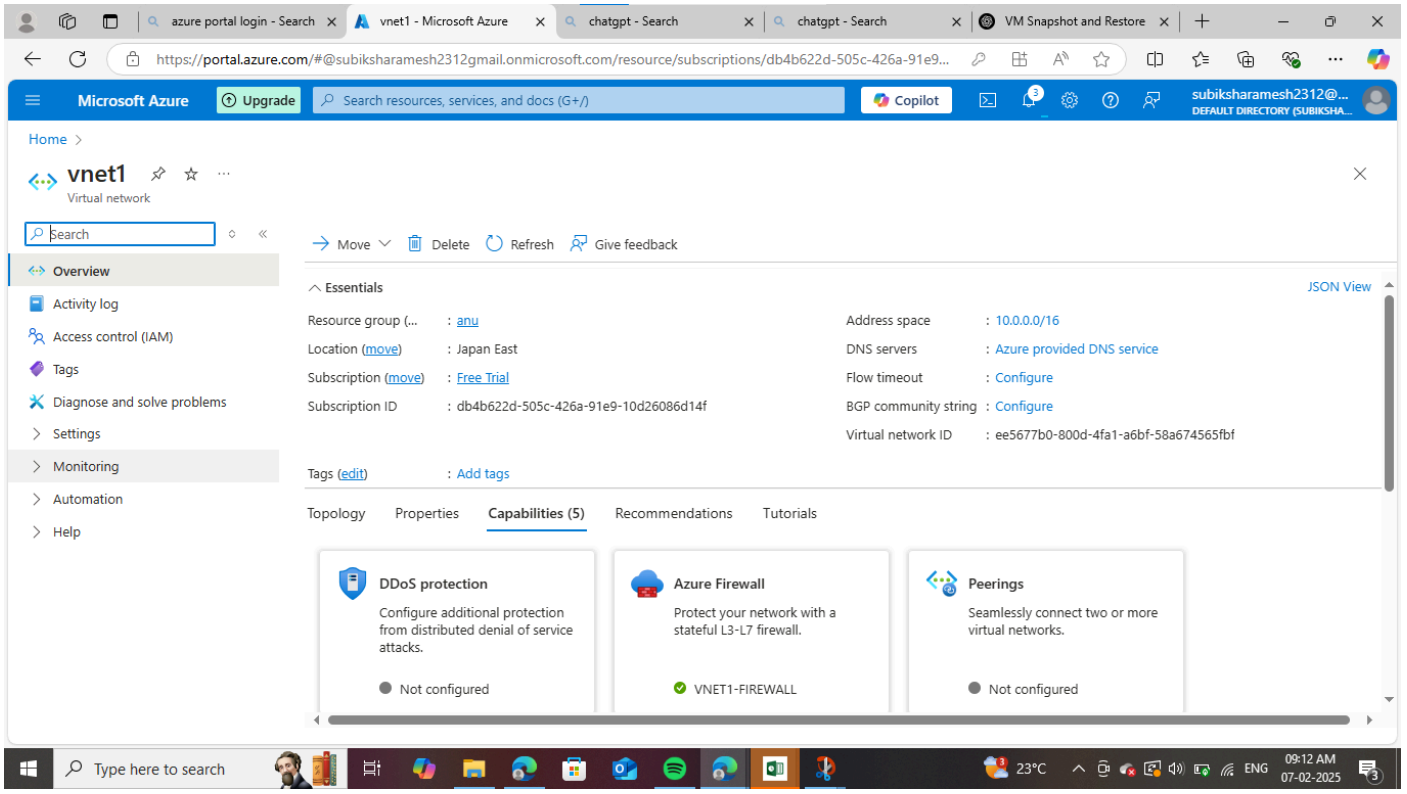


*STEP 2:*Add two subnets with two different ip-address

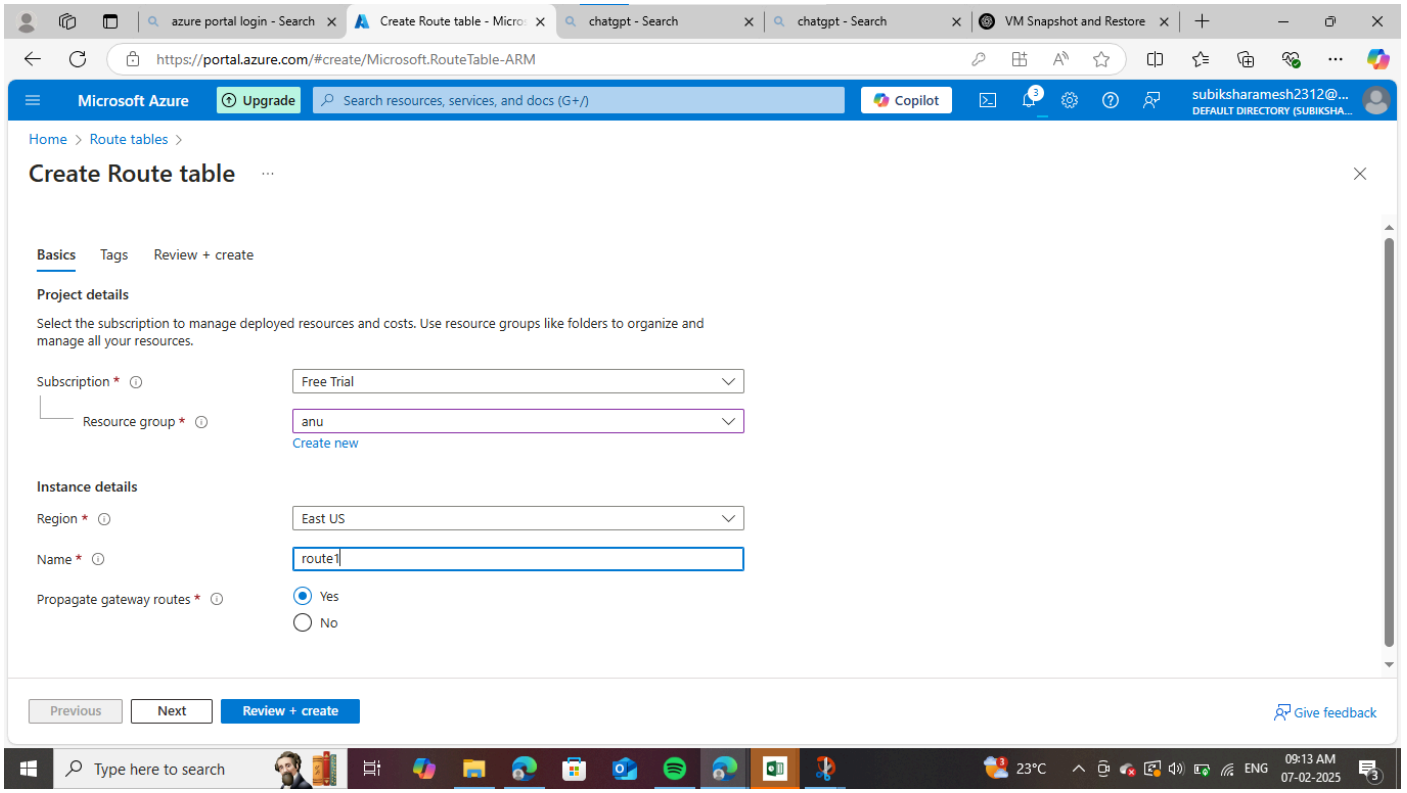




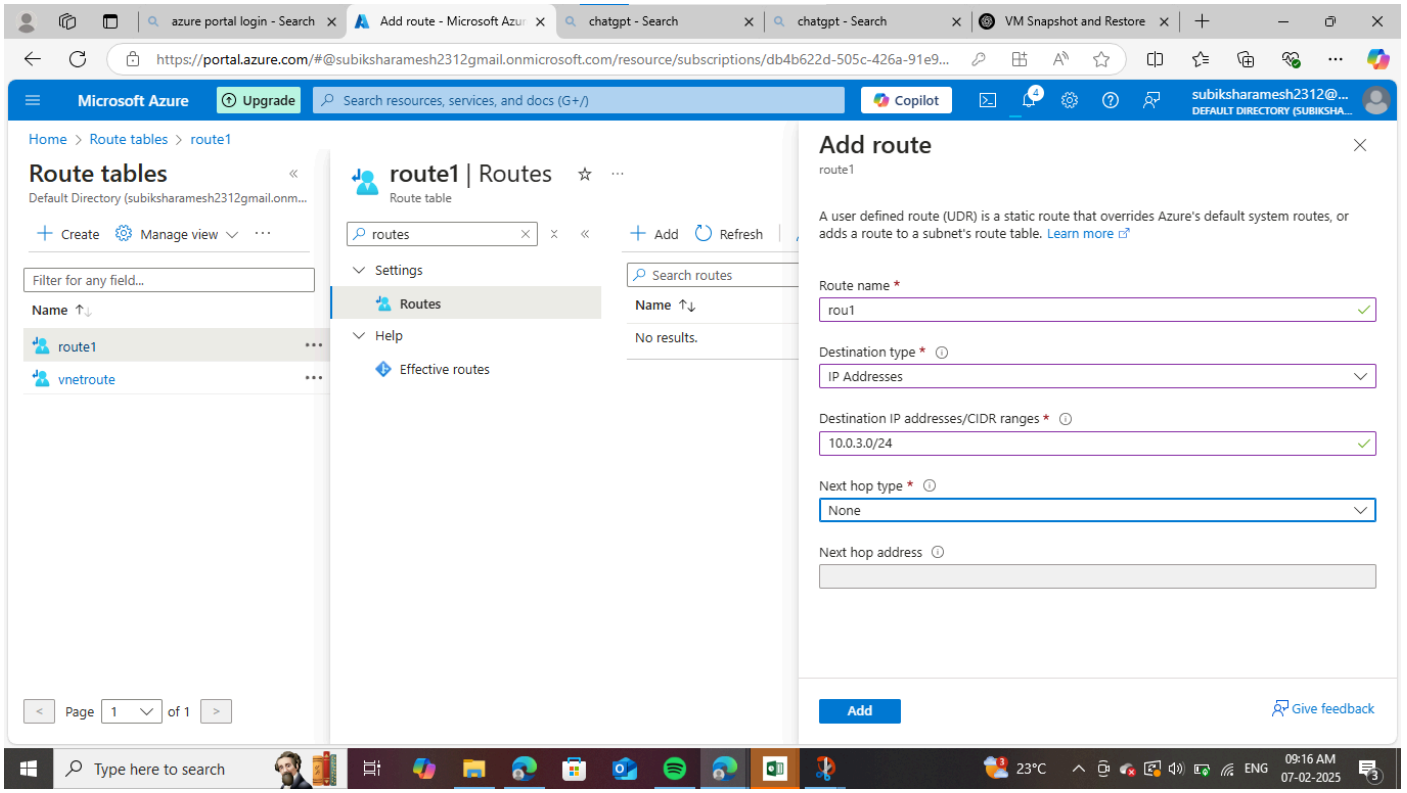
STEP 3:deploy the vnet and configure the changes

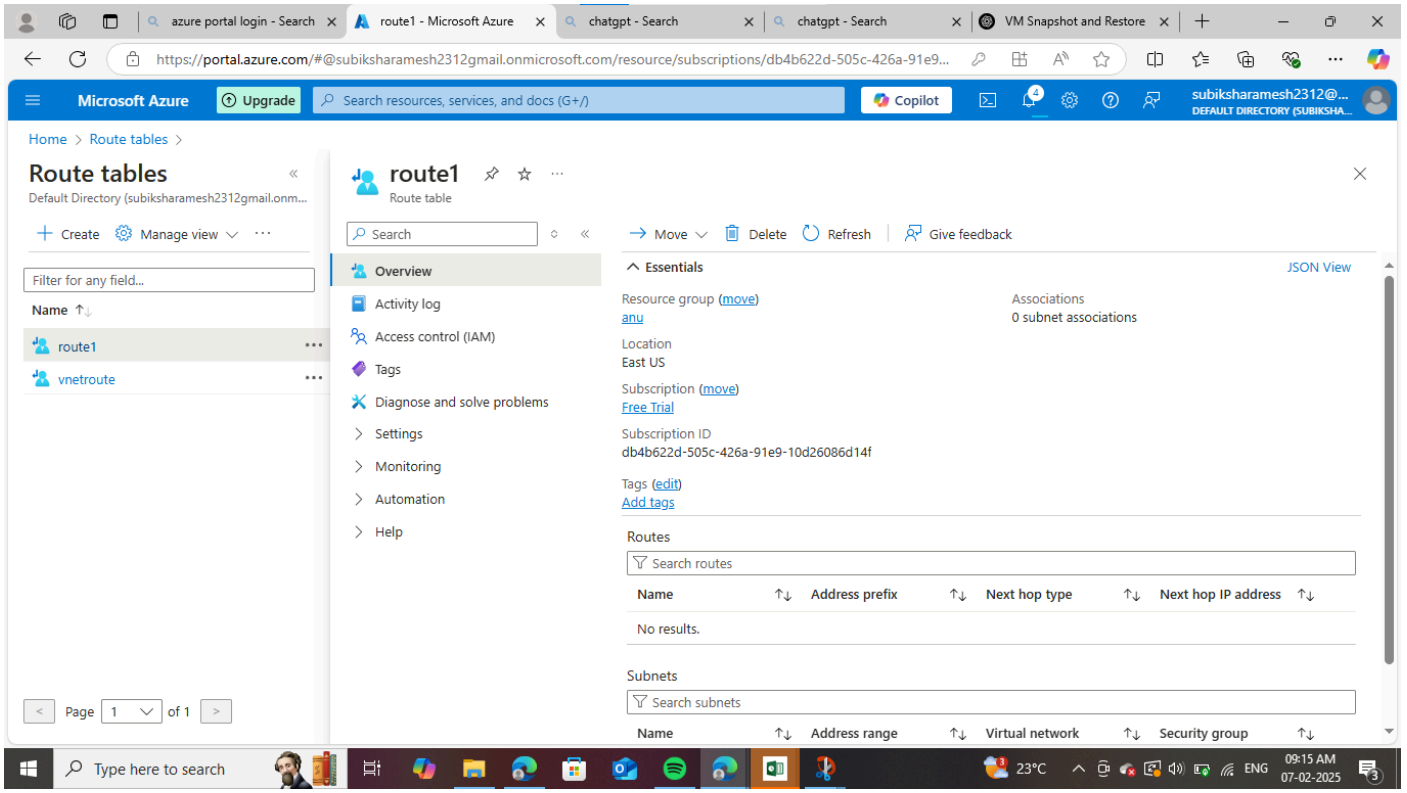


STEP 4:create a route table to connect two subnets inside that to partition the network among the subnets to manage the incoming traffic

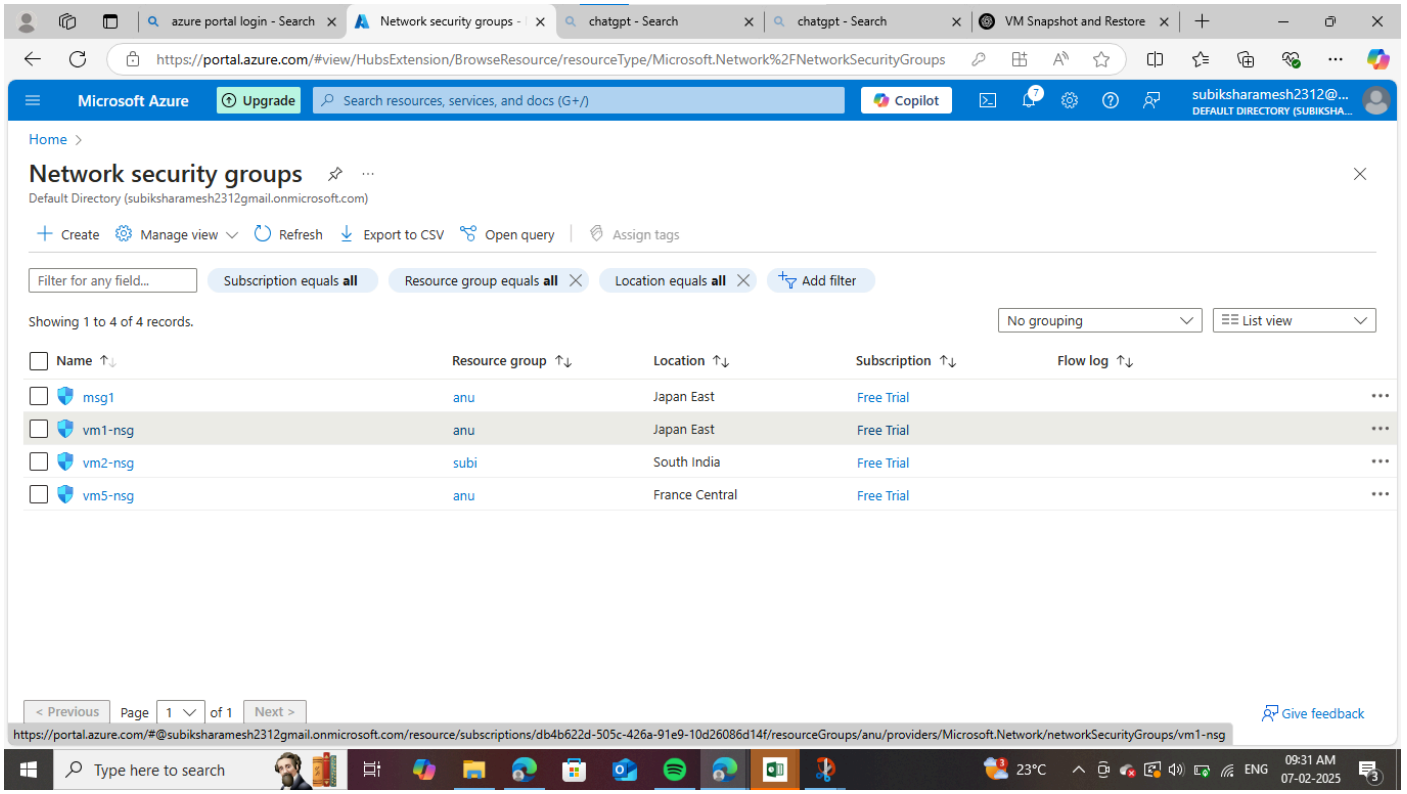


STEP 5:add routes ,give the subnet2-ip in the destination port

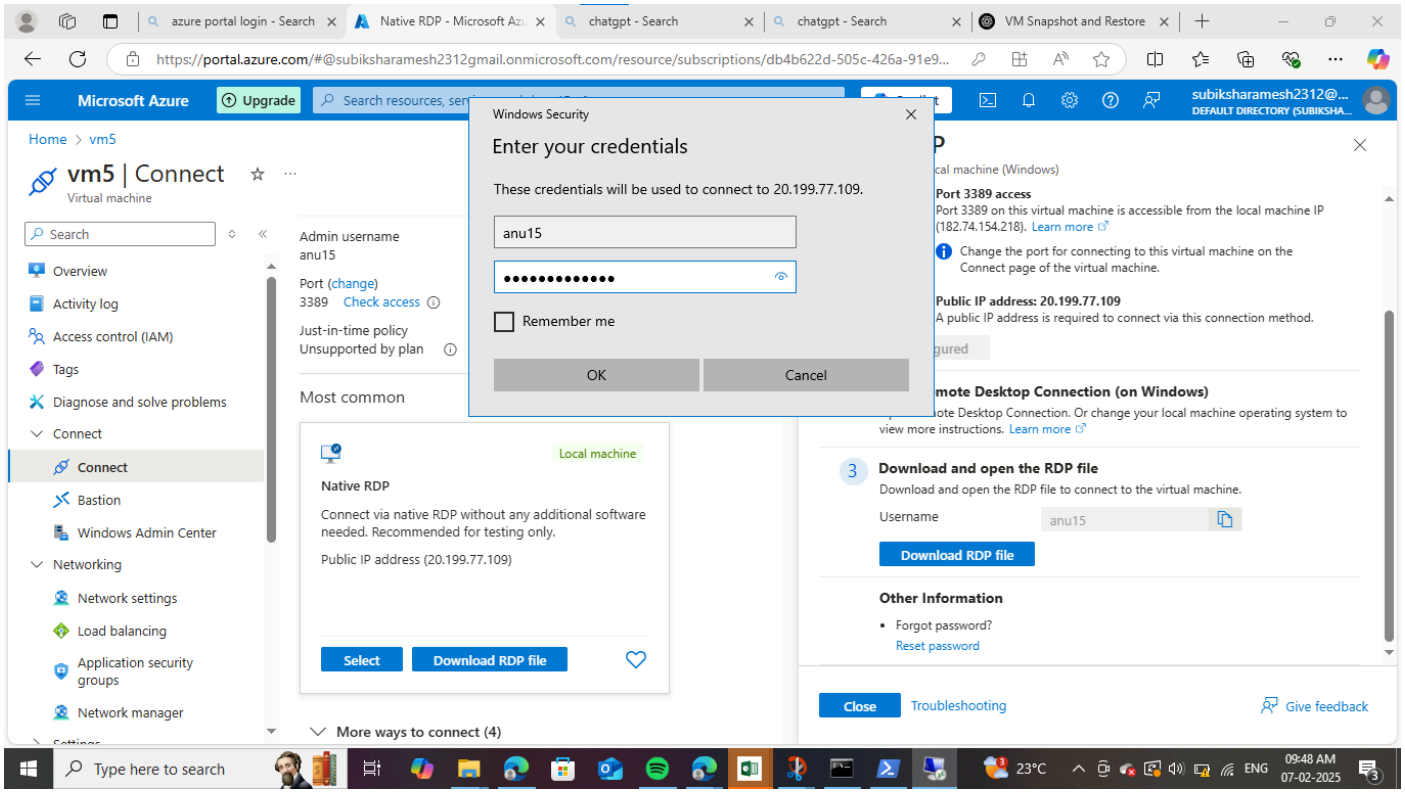




STEP 6:Attach network-security groups to allow the incoming traffic in the vnet,add icamp rule port



STEP 7:Connect the created vm inside the vnet to remote-desktop connection using your credentials



Outcome:

By completing this task, I learned:

Secure Connectivity: Establish a secure connection between cloud resources and on-premises infrastructure through a VPN Gateway.

Network Segmentation: Efficiently segment cloud resources into subnets, enhancing security, and improving traffic management by isolating different parts of the network.

Controlled Traffic Flow: Effective routing of traffic between subnets and external networks, ensuring optimized data flow and proper access control.

Enhanced Security: Implement security controls such as Network Security Groups (NSGs) and route tables to enforce access restrictions and secure communication.

Scalable Architecture: Ability to scale the network design to accommodate growing cloud workloads while maintaining high availability and security.

Hybrid Network Integration: Seamless integration of on-premises and cloud networks, enabling a hybrid environment with secure communication across both infrastructures.

Simplified Network Management: Clear organization of resources and traffic flow, improving manageability and troubleshooting of network issues.