**Working of NSG & ASG:**

* NSG's (Network Security Group) & ASG's (Application Security Group) are the main Azure Resources that are used to administrate and control network traffic within a virtual network (VNet).
* Network Security Group is the Azure Resource that you will use to enforce and control the network traffic with, whereas Application Security Group is an object reference within a Network Security Group.

**Network Security Group:**

* NSG is like a firewall for your Azure resources.
* NSG is a group of Access Control List rules that either allow or deny network traffic to a specific destination located on your VNet.
* They can be applied either on a virtual machine or subnet (one NSG can be applied to multiple subnets or virtual machines):

1. Virtual Machines: the rules will only get applied to Virtual Machines that are associated.
2. Subnets: All virtual machines within the specified subnet will get the applied rules.

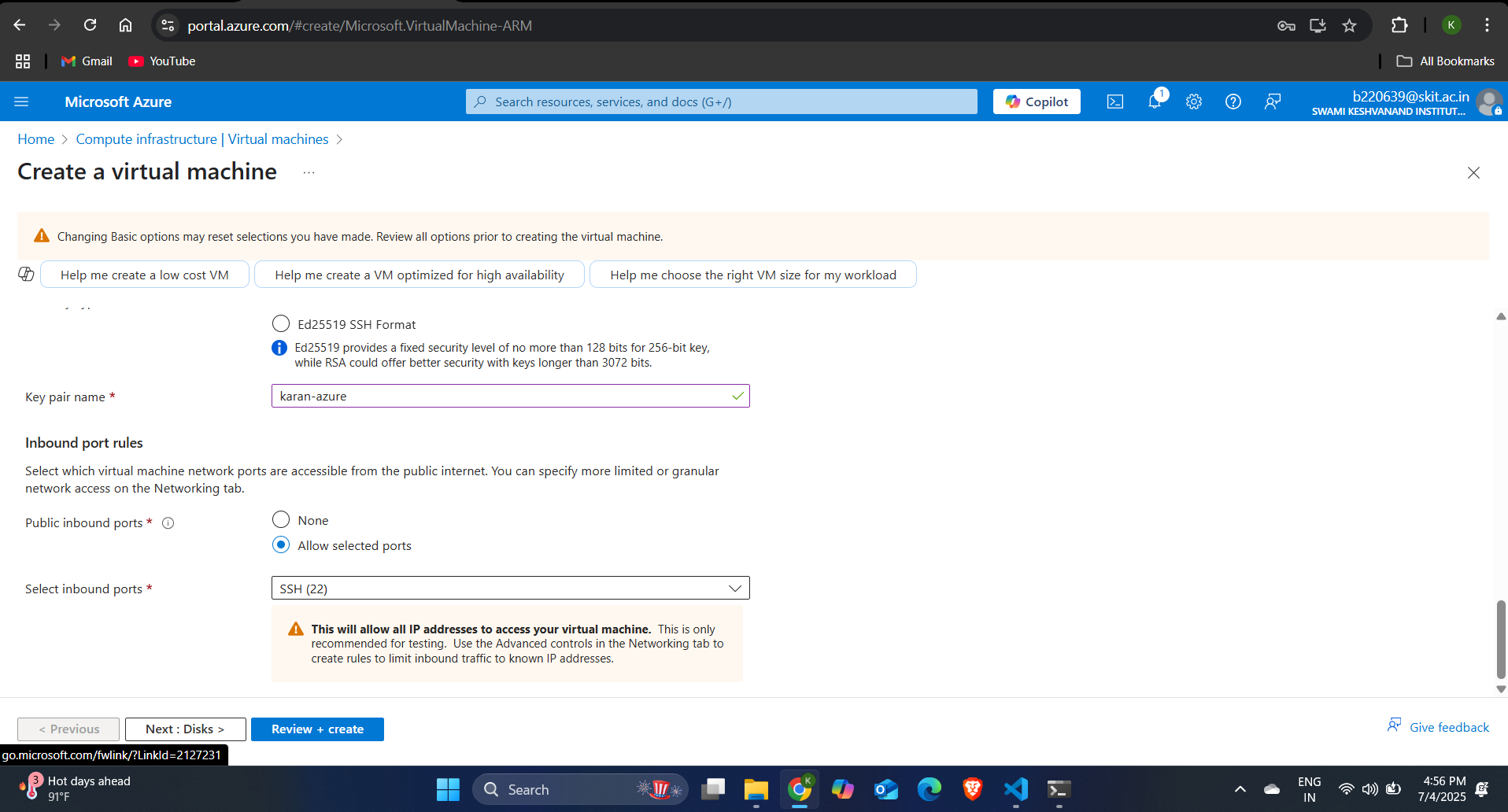
* Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces.

**Application Security Group (ASG):**

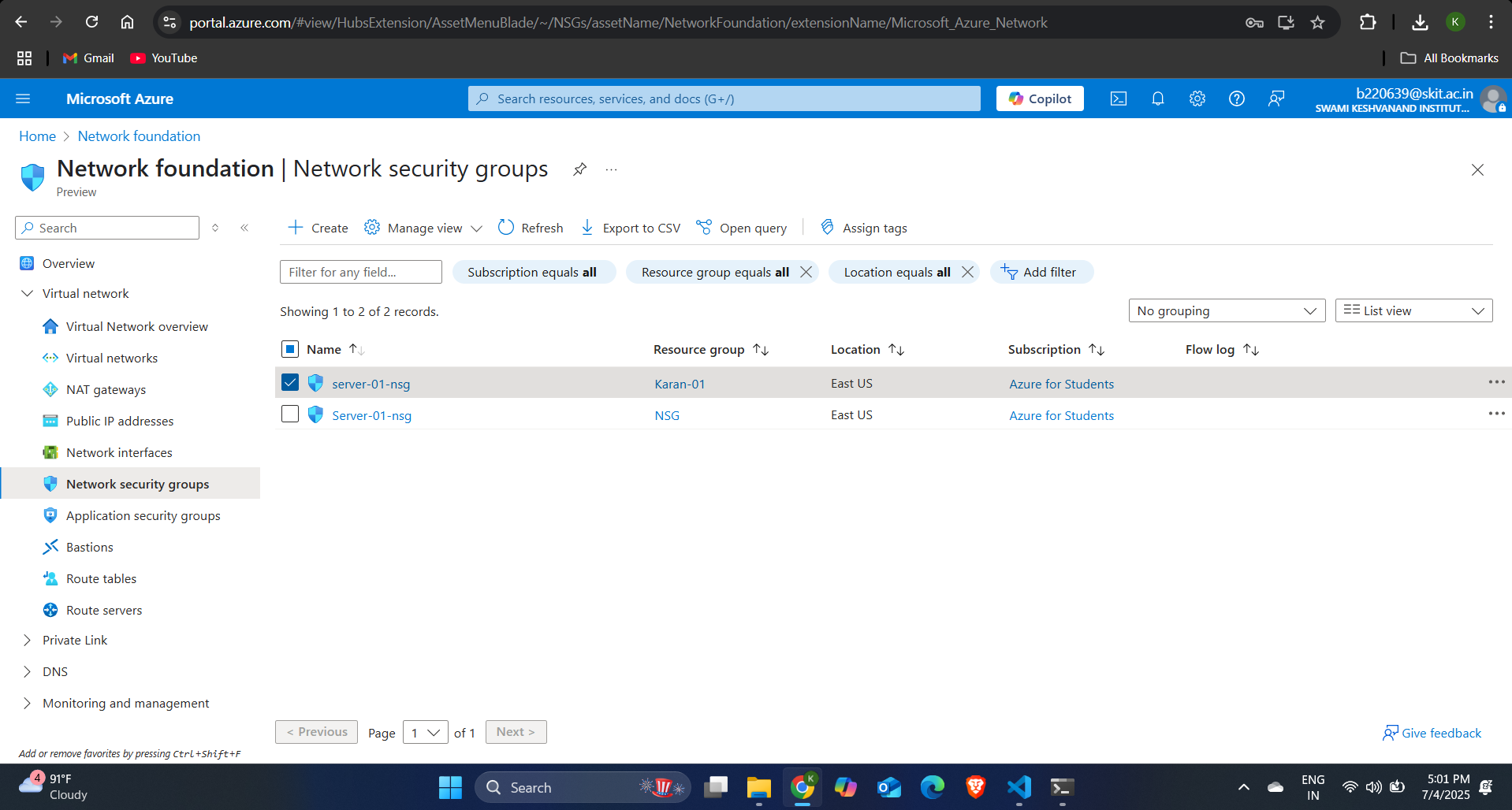
* ASG is like a tag or logical grouping of VMs for security rules.
* Instead of writing NSG rules using IP addresses, you use ASG names.
* Easier management of NSG rules for large environments.
* For example, group all web servers in an ASG called “Web Servers” and allow traffic to/from them without worrying about their IPs.

Allowing specific IPs to access VMs and Deny Internet using NSG:

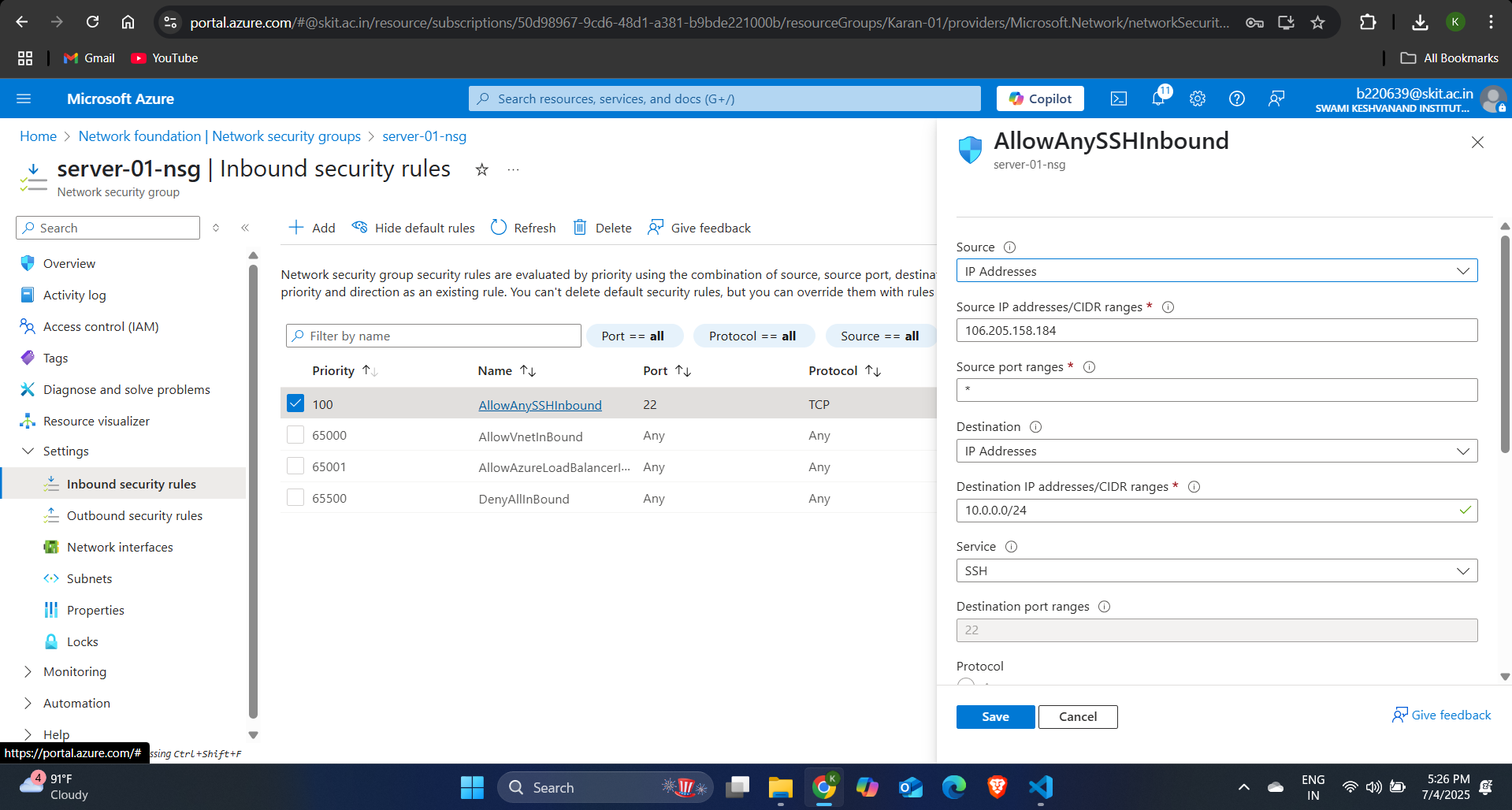
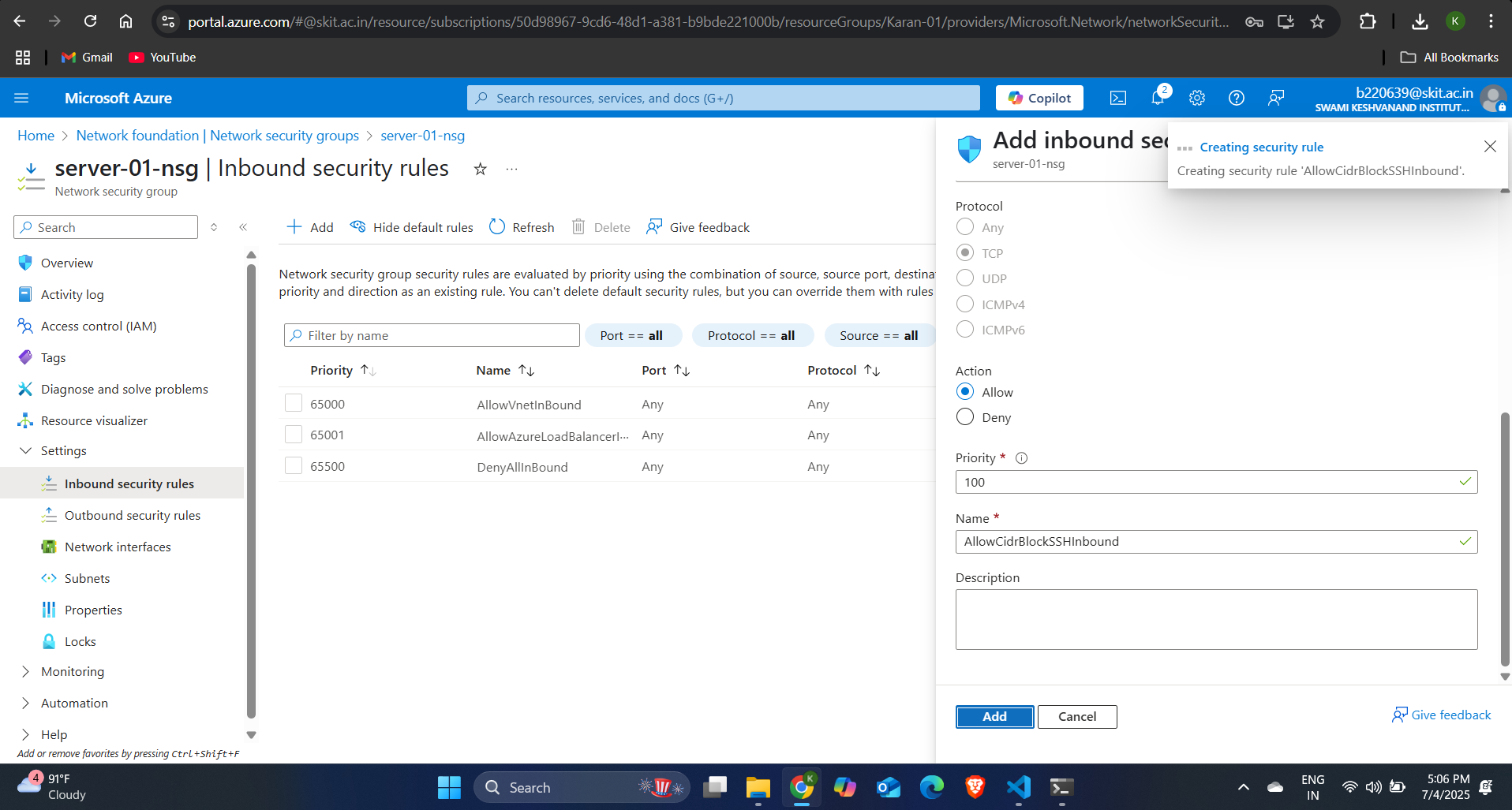
Step-1: We will create a virtual machine in which we allow only SSH access to virtual machine, so every public IP will be able to access the virtual machine through SSH.



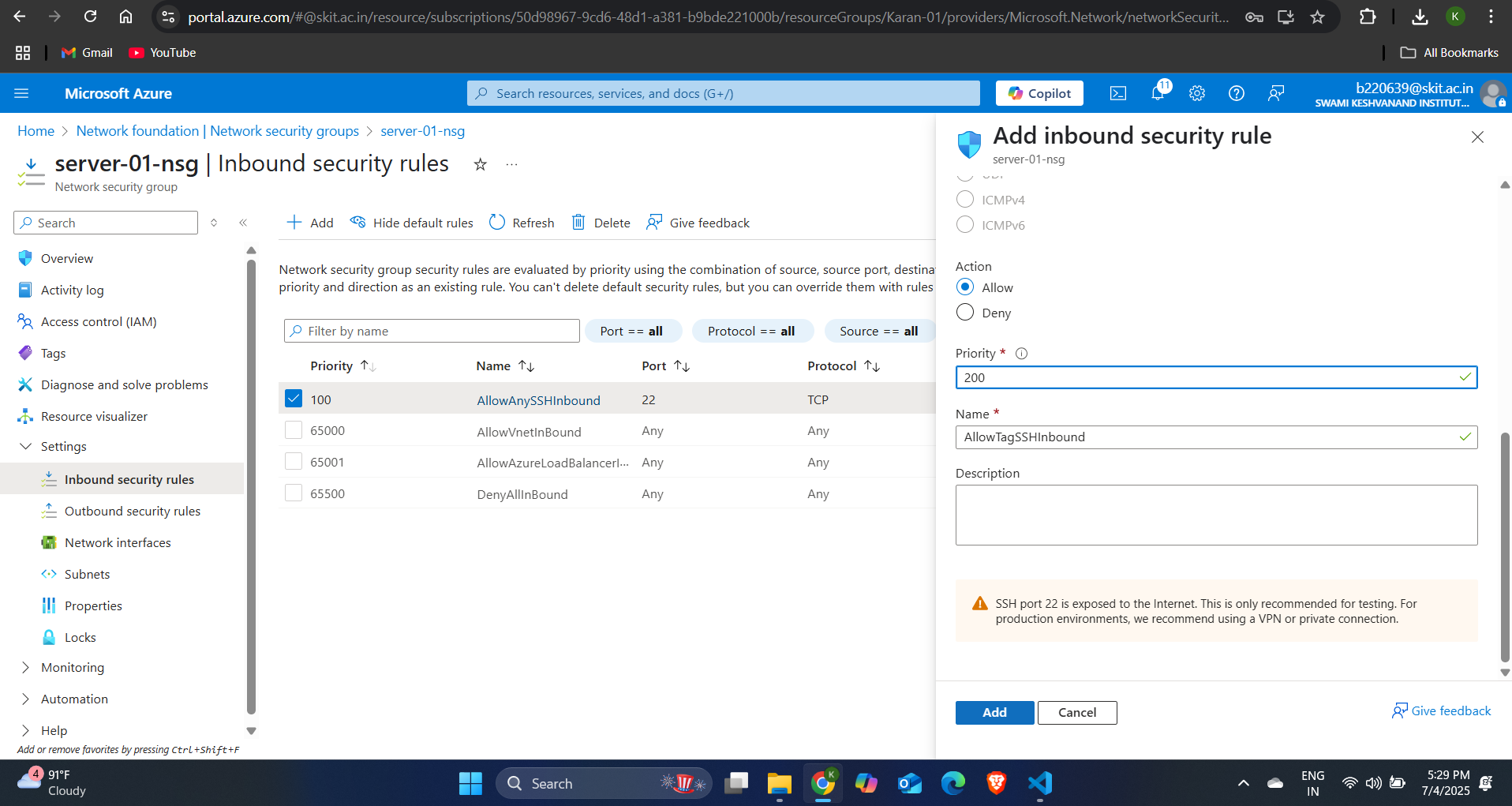
Step-2: Then go to network security group and access the NSG of virtual machine that you created.



Step-3: Click on add rule and now we have to allow only our IP address to access the virtual machine through SSH so we will specify the source address IP address as your own IP address and destination IP address as the CIDR range of the subnet in which the VM is present and also set the priority of the rule, priority values range from 100 to 4096. The smaller the priority number, the higher the priority of the rule. Shown below in the screenshot.



Step-4: Since we have to deny Internet to the virtual machine create another rule and enter the source as Internet and destination as the CIDR range of the subnet in which the virtual machine is present and set the priority of the rule lower than the rule created above so that your IP can access the virtual machine through SSH and select the action as Deny.



Static IP Address:

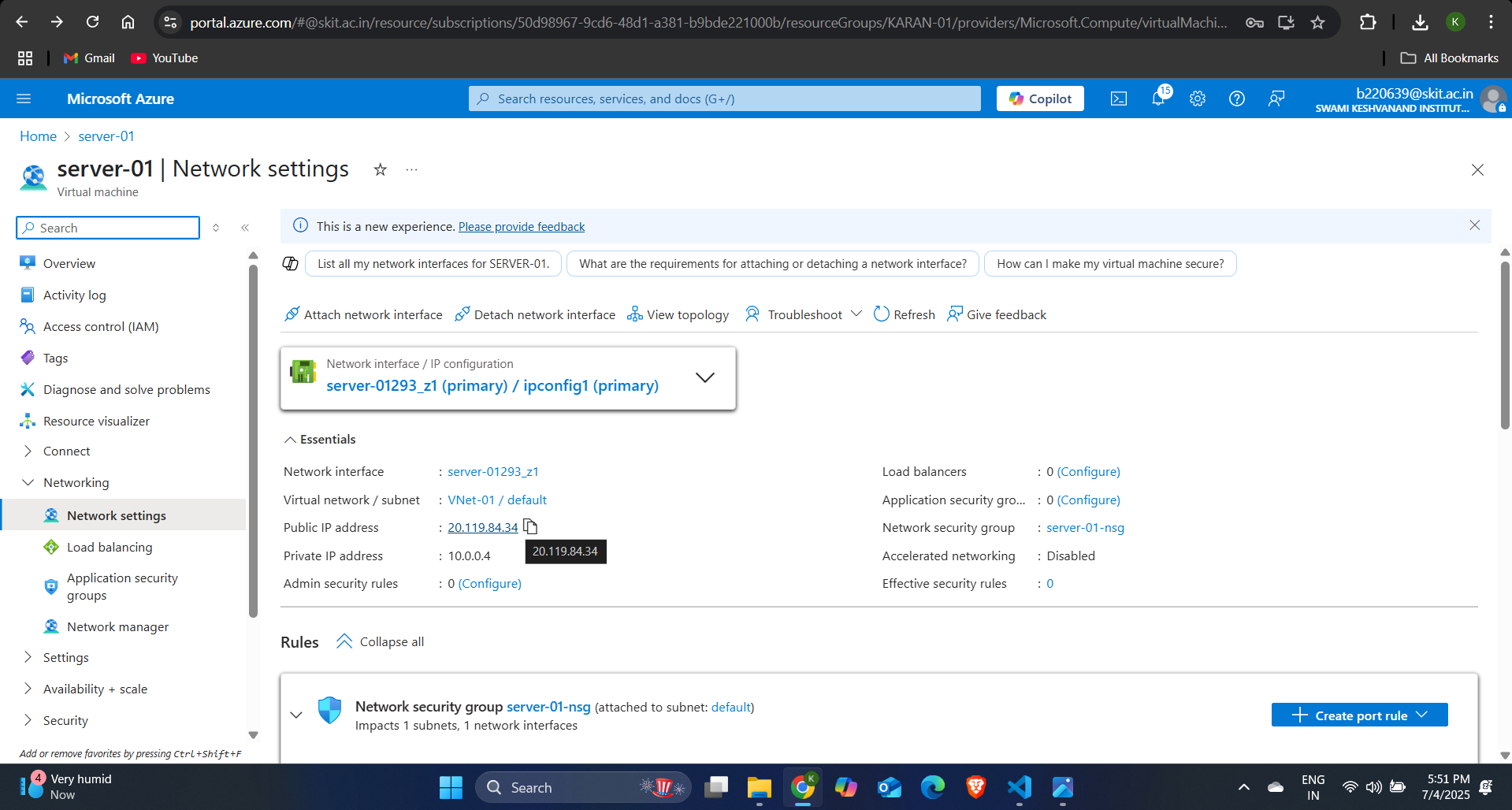
* A Static IP address is an IP address that does not change over time. It is manually assigned and remains constant, unlike a dynamic IP which can change when resources are restarted.
* Static IP address can be assigned to virtual machines, load balancers, Application Gateways.
* It is useful for:
  + DNS configurations.
  + Application dependencies needing specific IPs.
  + Firewall rules.
* Static IP is actually applied to the NIC instead of the virtual machine since virtual machine uses the IP configuration of NIC and virtual machine do not have IP configurations.

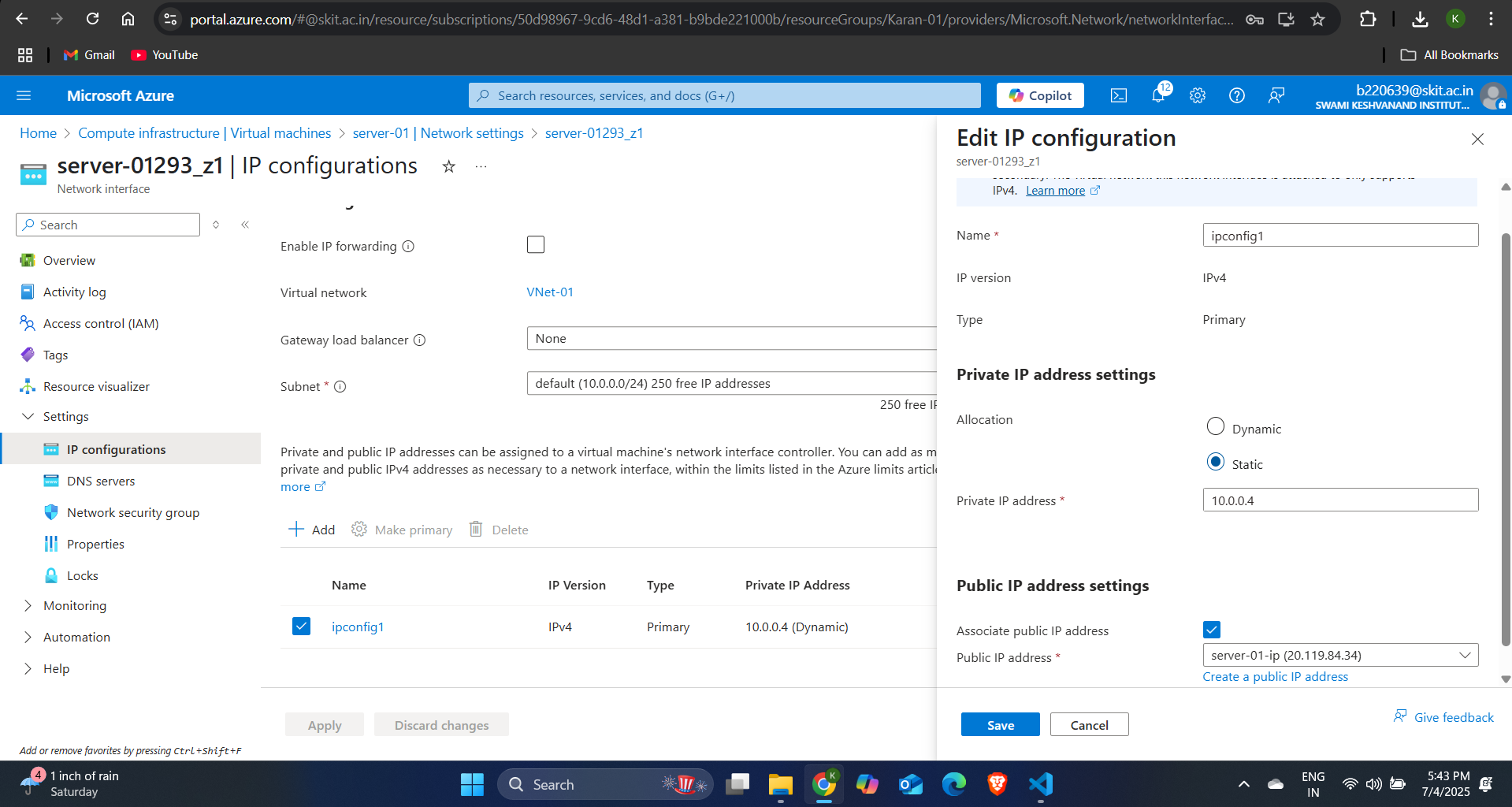
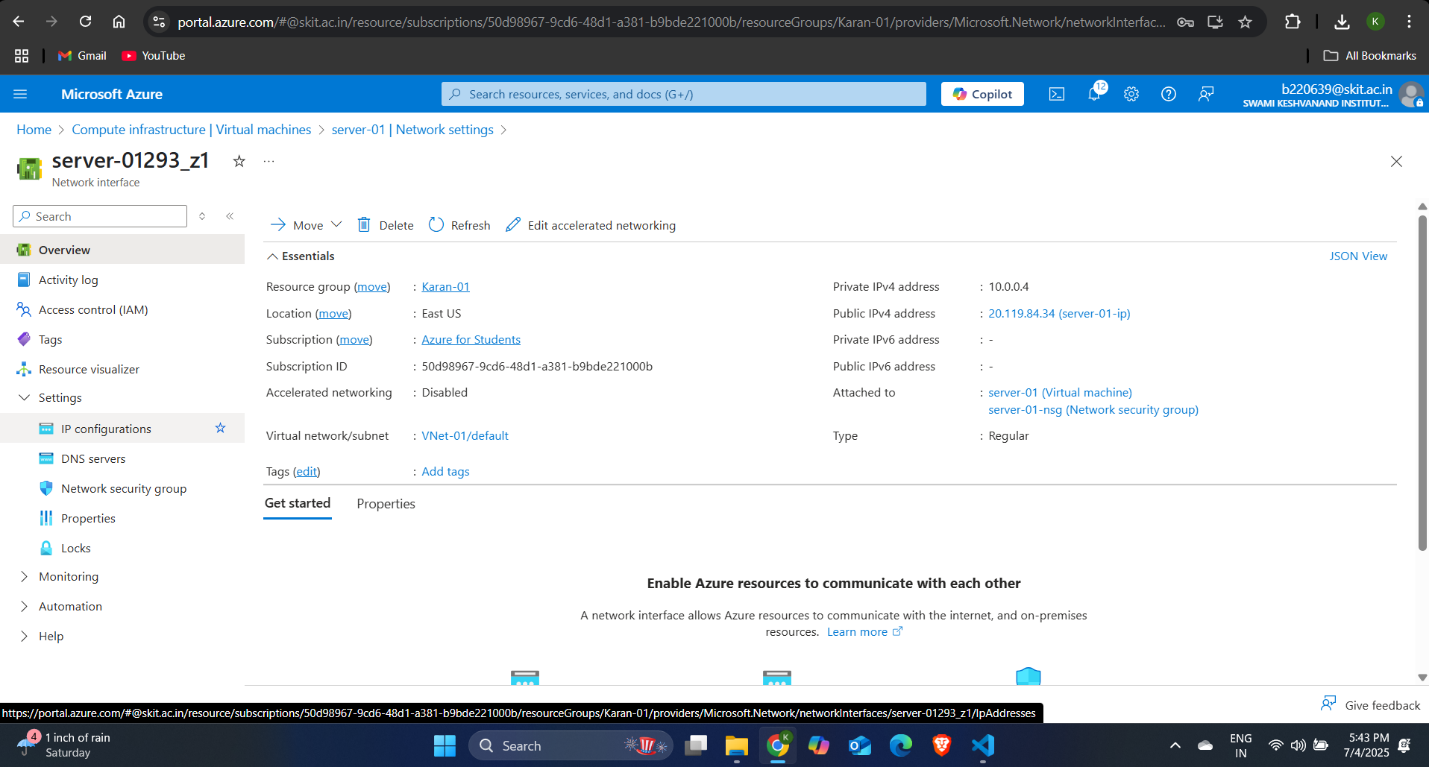
**Dynamic IP address:**

* A Dynamic IP address is an IP address that is automatically assigned by Azure from a pool of available IP addresses. It can change under certain conditions.
* When we assign a dynamic IP address to a virtual machine and then we restart the virtual machine then the IP address of the virtual machine changes. So, we use Static IP address and the IP address of the virtual machine will not change.
* By default, when you create a VM or resource within a VNet, Azure assigns a dynamic private IP.
* However, it does not change as long as the VM is running or stopped (but not deallocated).

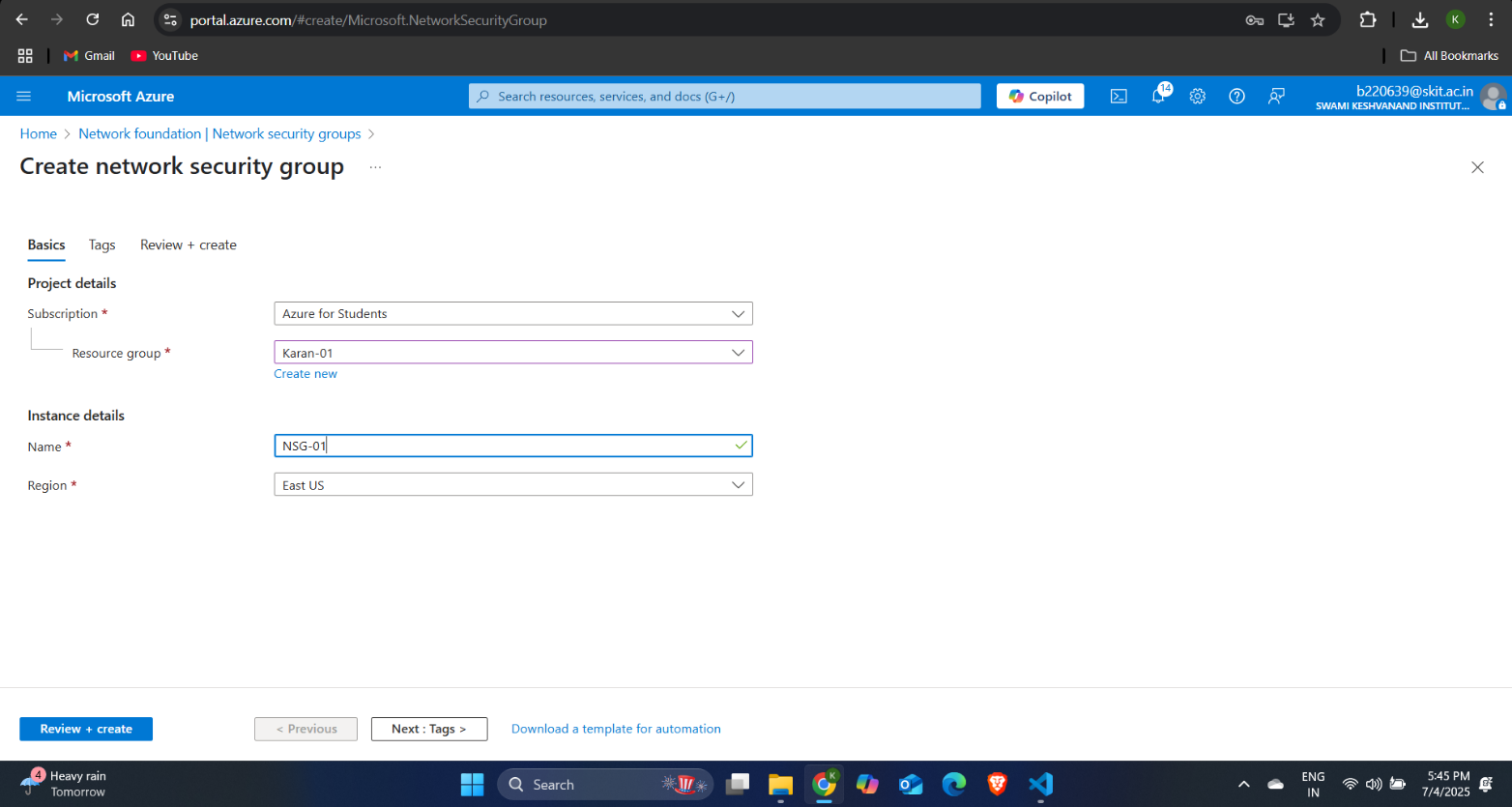
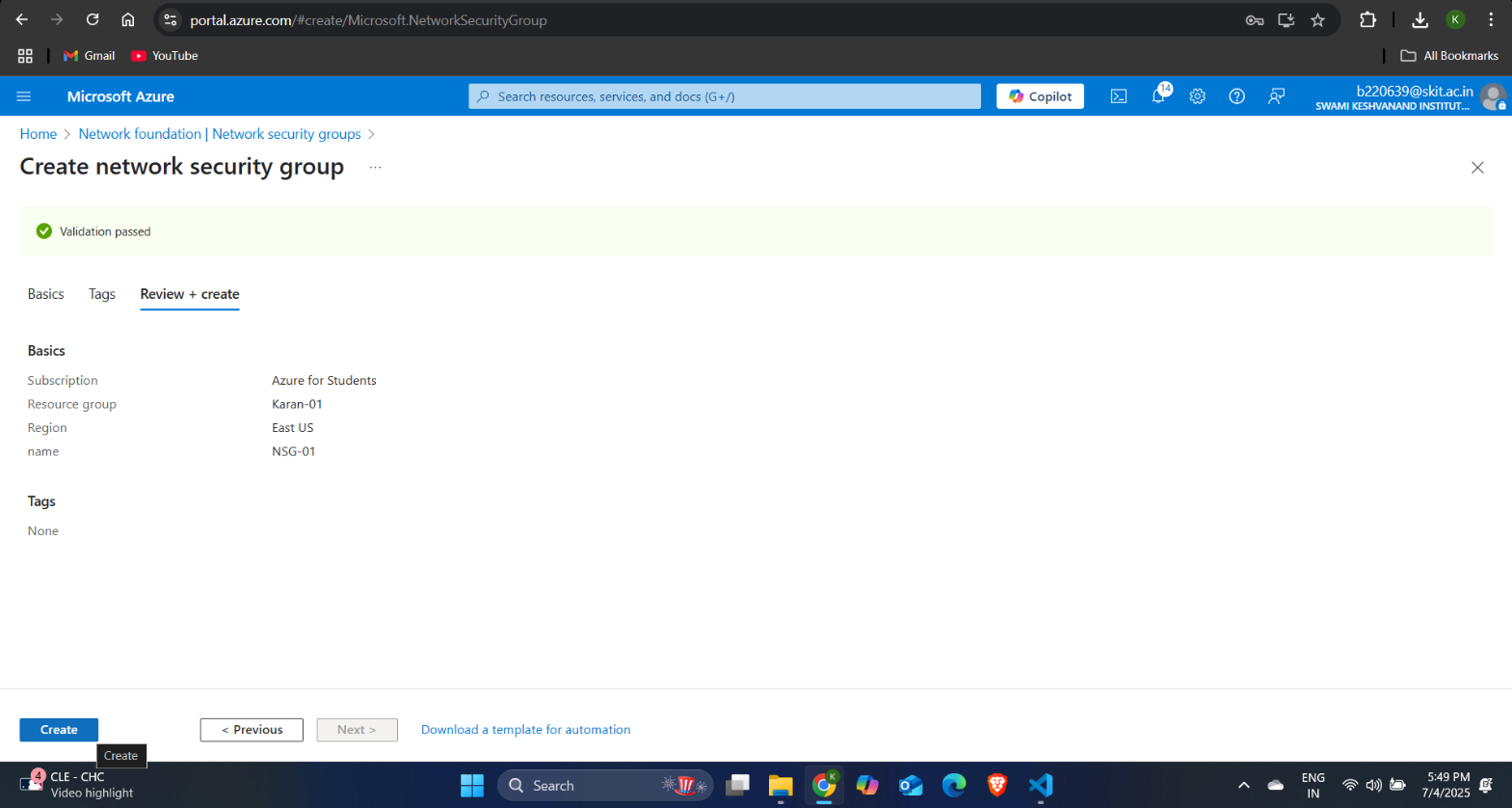
**Allocate Static IPs to all VM's:**

Step-1: Go the virtual machine for which you want to allocate the static IP address. And then select the NIC (Network Interface) of the virtual machine. Then, go to the settings sections and under the settings section go to IP configurations and click on ipconfig1 and select the allocation as Static.

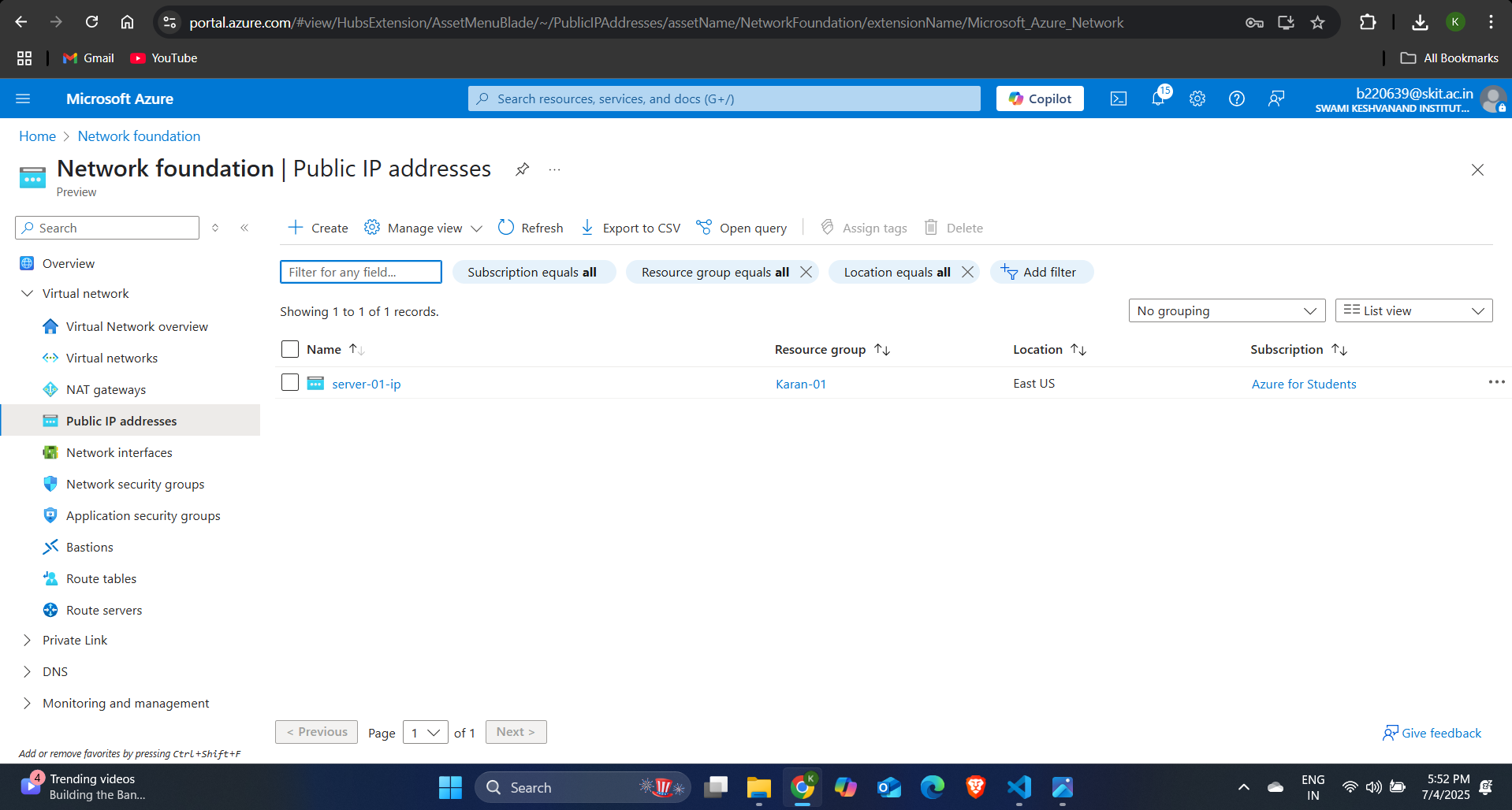


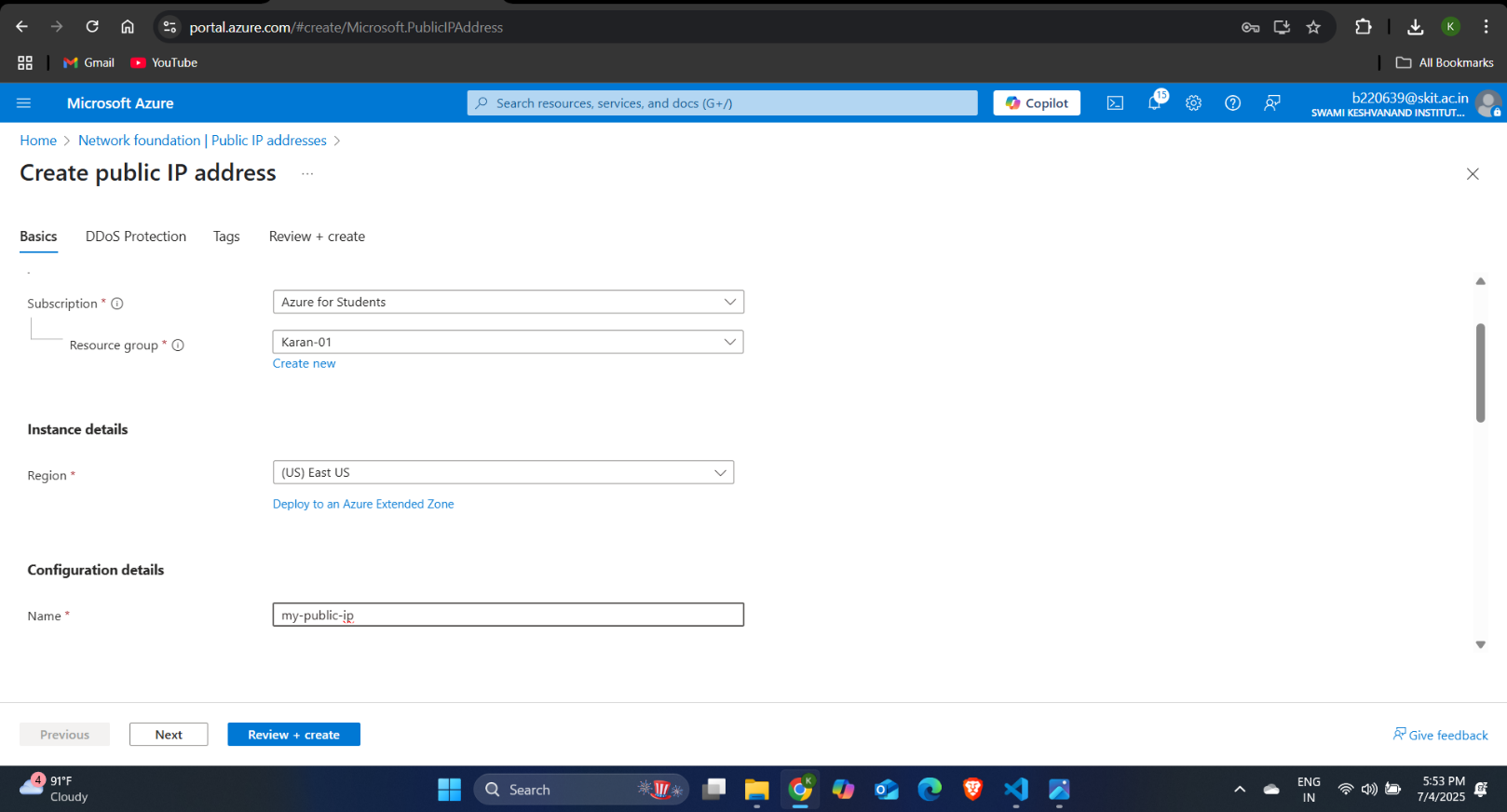


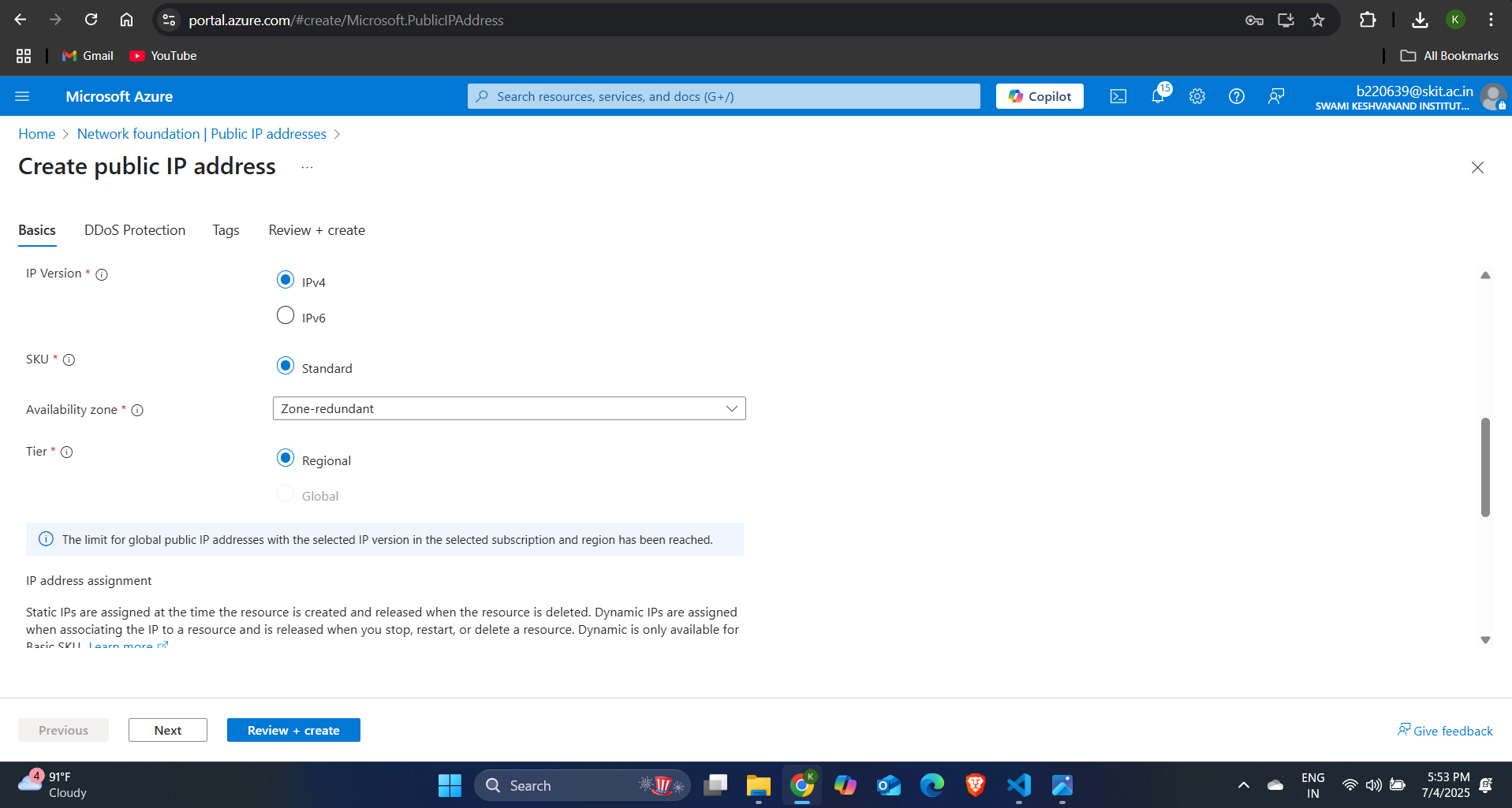
**Creating a Network Security Group:**

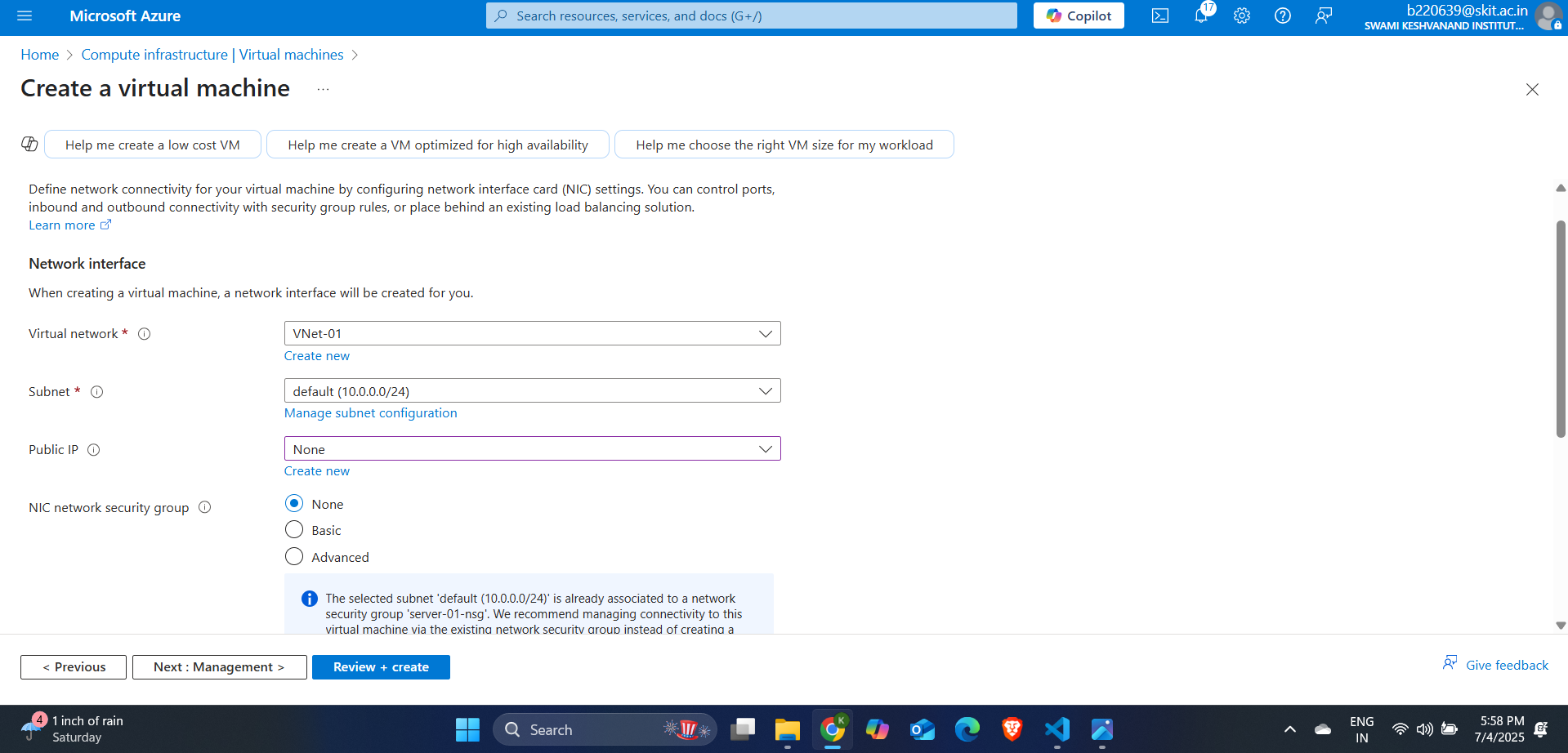
**Step-1: Search for network security group and click on create. Specify the name of your NSG and then click on review + create and your NSG will be created.**

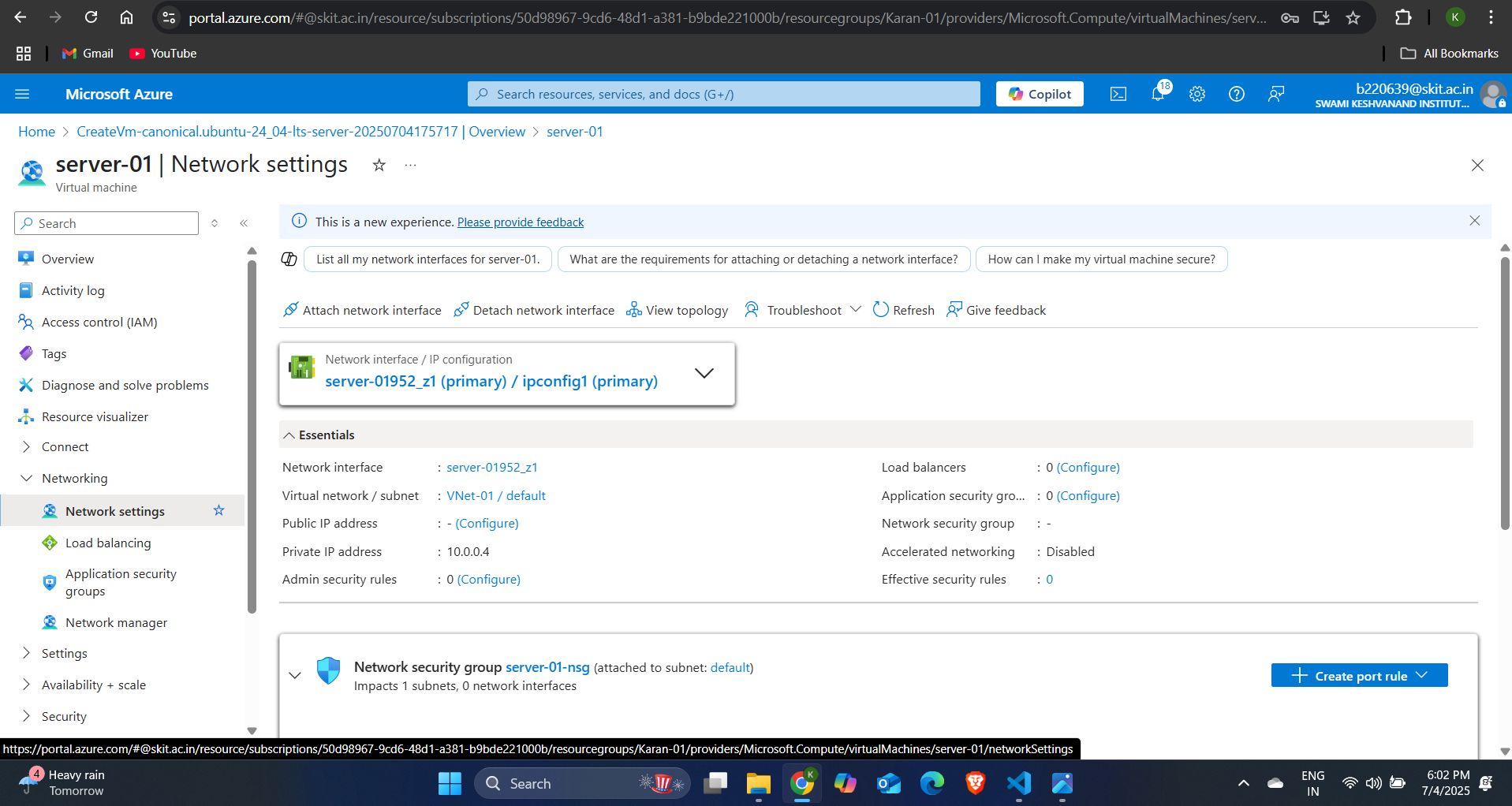
**Creating Public IP:**

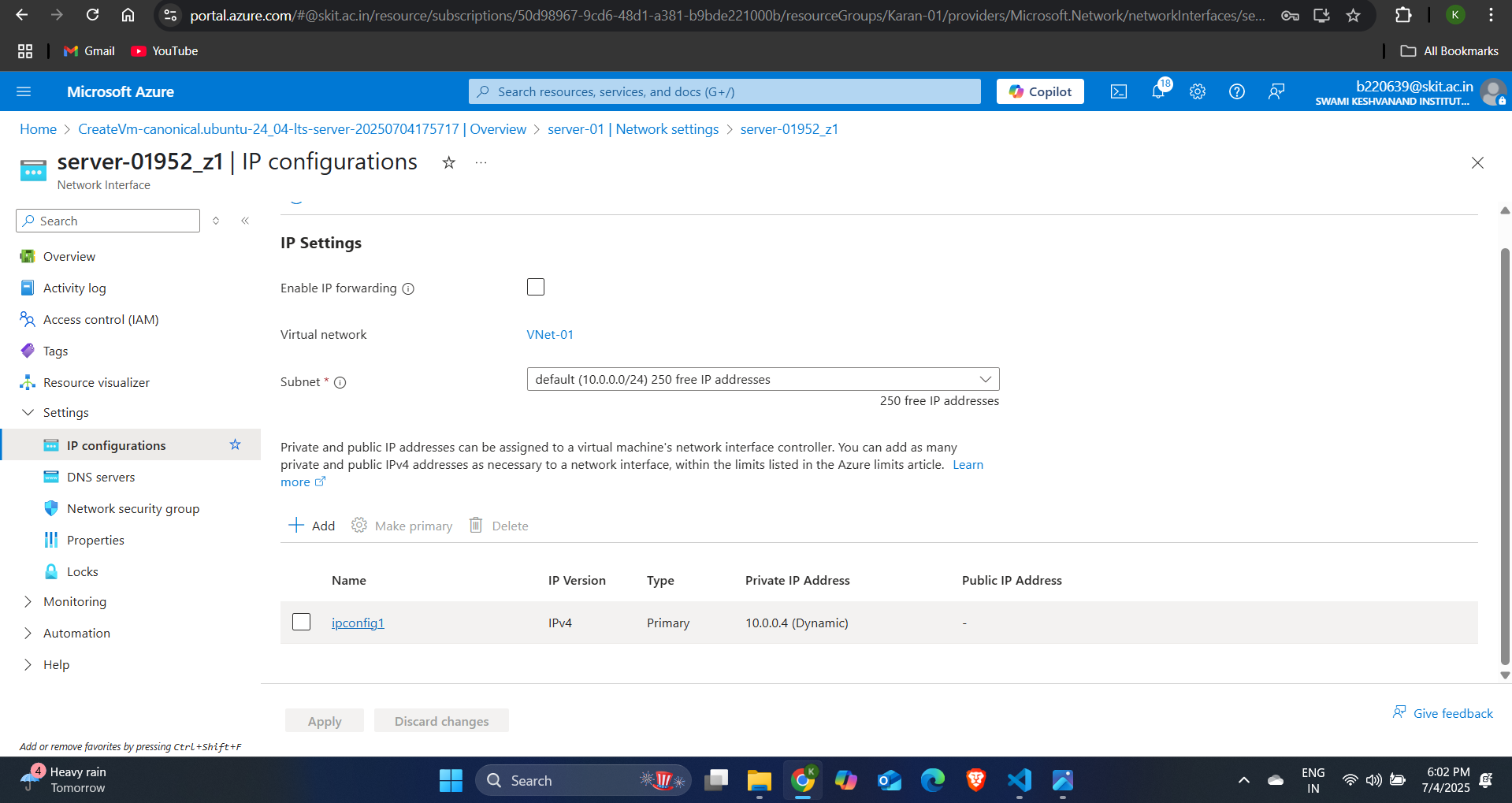
Step-1: Search for Public IP in azure and click on create.

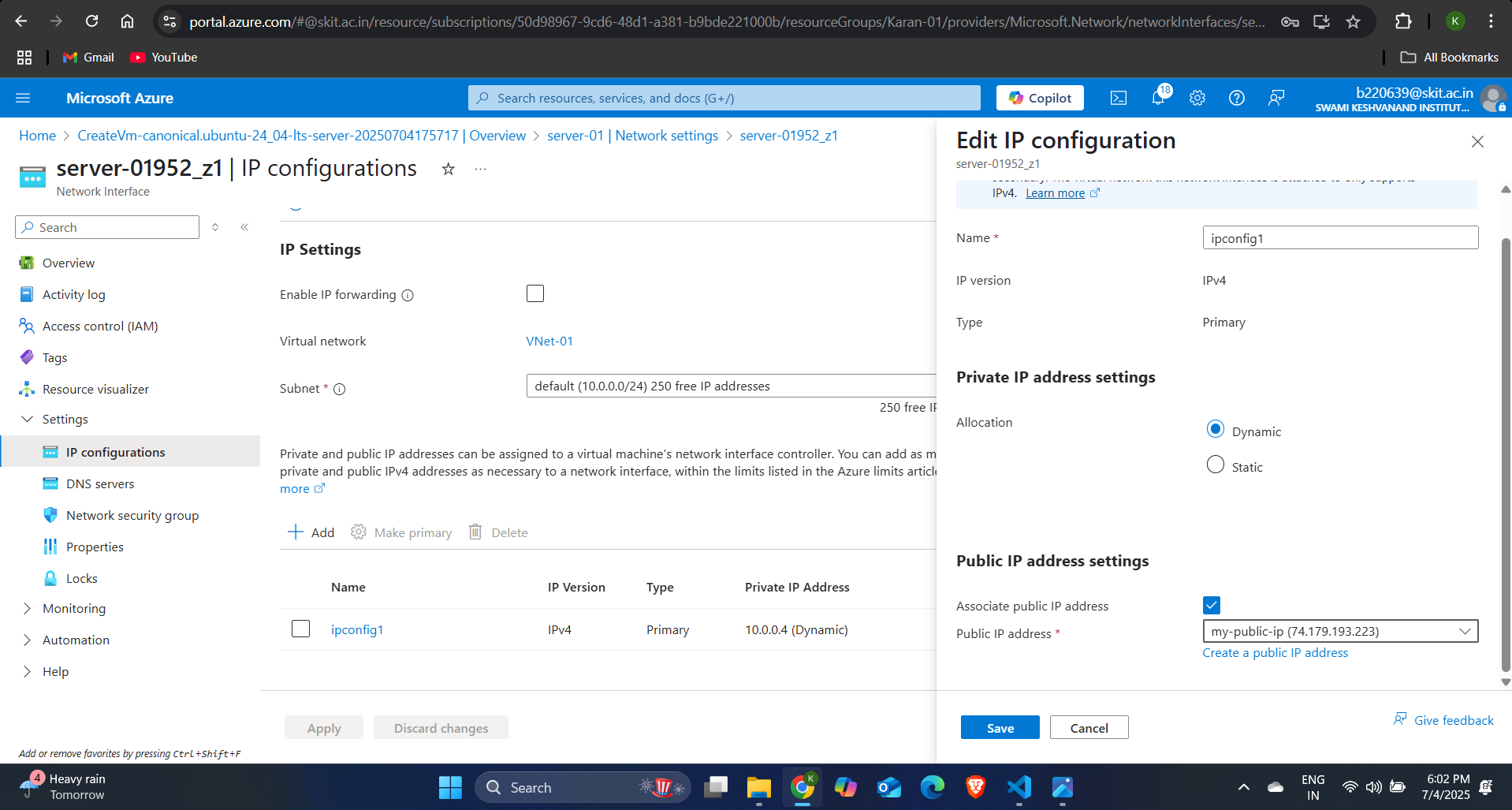
Step-2: Specify the name of the Public IP address then select the version of IP address as IPv4 and select the IP address assignment as Static and click on review + create.

**Associating/De-associating Public IP with virtual machine:**

****Step-1: Create a virtual machine and deploy it in a subnet of a virtual network and assign the Public IP as none, so it will not get a Public IP address.

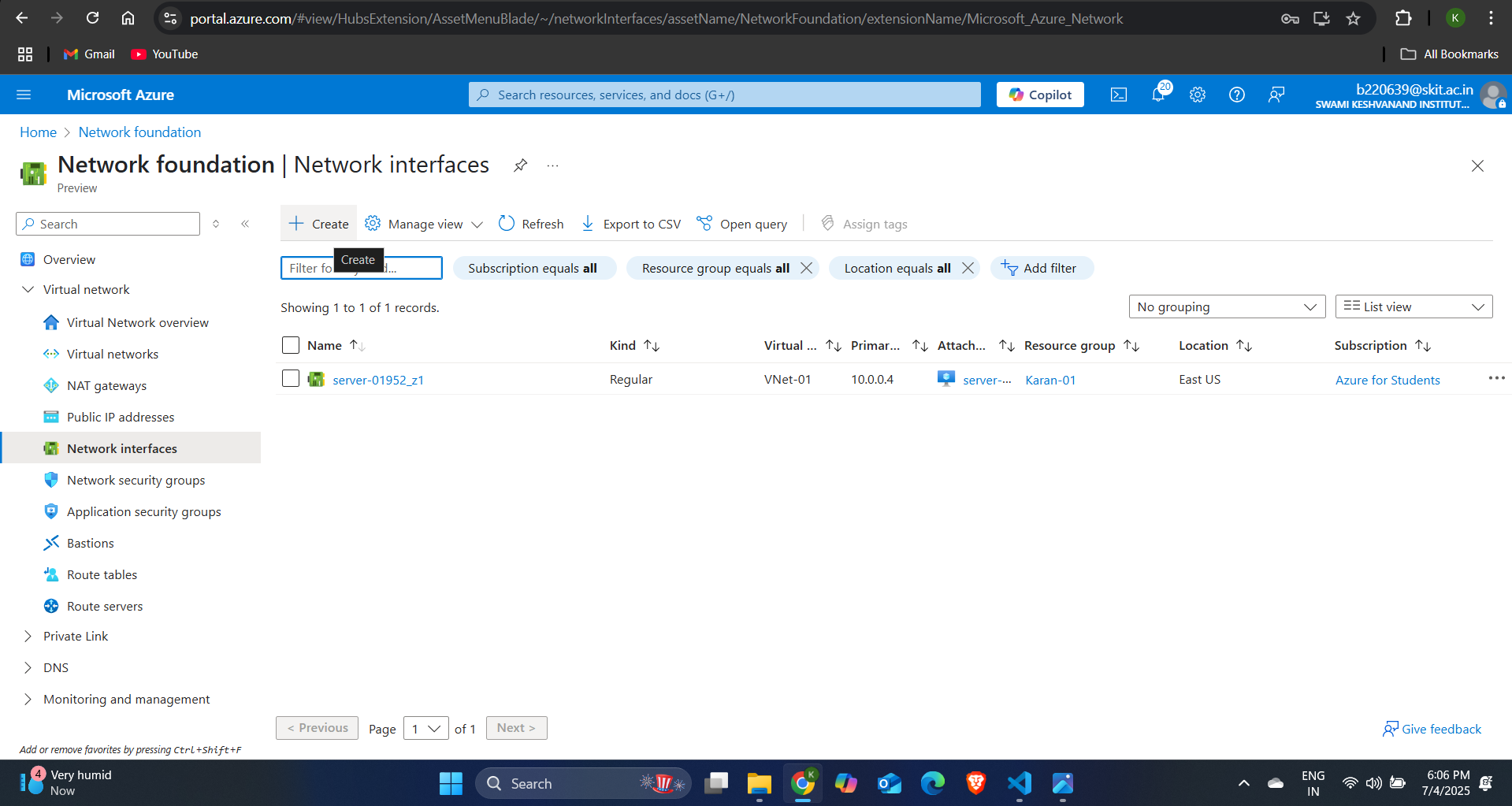
Step-2: Go to the Networking section and then go to Network Settings and click on the network interface link.

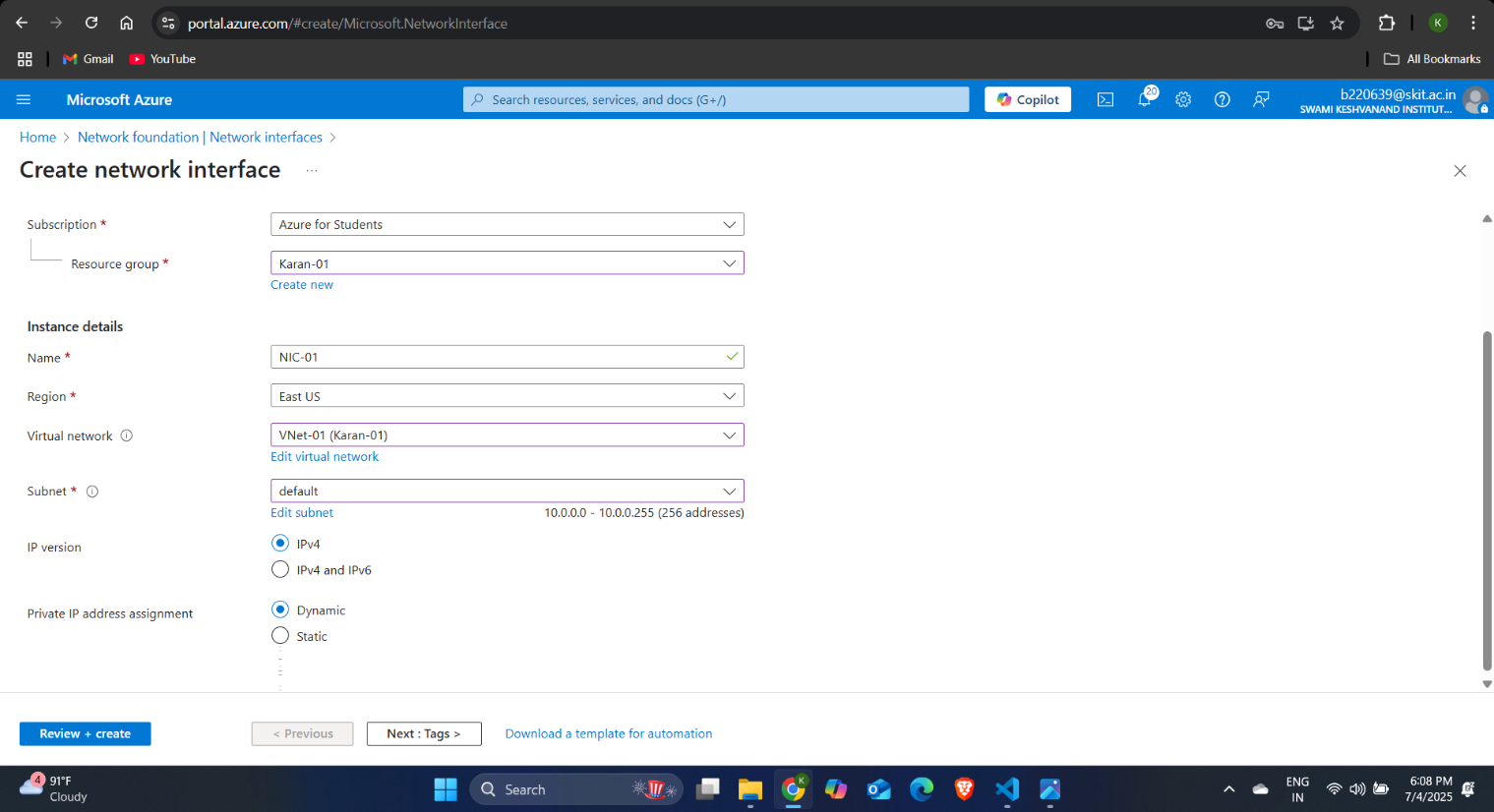
Step-3: Go to the settings section of the NIC and then click on IP configurations and then click on ipconfig1 and select the box of associate public IP address and then select the public IP address that you created and click on save.



Step-4: Now to de-associate the public IP address, again follow the above procedure and uncheck the associate Ip address box and your IP address will be de-associated.

**Creation of Network Interface:**

Step-1: Search for Network Interface in Azure portal and click on create.

Step-2: Then specify the name for your NIC and select the virtual network and subnet in which you want to deploy the NIC and select the private IP address assignment as dynamic or static and click on review + create.