**Research and Development Document**

**ON**

**Azure Networking - Network & Application Security Groups**

****

****

**By**

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

**Under**

**Celebal Summer Internship**

**in**

**Cloud Infra & Security**

**Table of Contents**

[**Azure Network Security Groups**](#_heading=h.67ho4h9dmith) **3**

Azure Network Security Rules**5**

[**Azure Application security groups 5**](#_heading=h.wsba14yifqzv)

**Assignment 6**

**References 12**

**Azure Network Security Group**

Azure network security group is used to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

NSG is a tool for activating rules that manage traffic to the Virtual networks. Within NSG, an inbound rule refers to incoming traffic requests, while an outbound rule relates to outgoing traffic requests. These rules align with our organizational policy, dictating the permissions for both incoming and outgoing access.

After the creation of NSG, there are default security rules that we can't change, but we can override those rules with custom rules. By default, NSG allows inbound and outbound traffic from the same virtual network.

## **Azure Network Security Rules**

Azure Network security provides custom control over the inbound and outbound traffic to the Azure services. It facilitates secure cloud networks by defining the network security groups with customized rules specifying what protocol, IP address, ports-based traffic are allowed to Azure services.

**Properties of Security Rules:**

|  |  |
| --- | --- |
| Property | Explanation |
| Name | A unique name within the network security group. The name can be up to 80 characters long. It must begin with a word character, and it must end with a word character or with \_. The name can contain word characters or ., -, \\_. |
| Priority | A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. |
| Source or destination | You can specify Any, an individual IP address, a CIDR block (for example, 10.0.0.0/24), a service tag, or an application security group. For Azure resources, use the private IP address assigned to the resource. Network security groups process traffic after Azure translates public IP addresses to private IP addresses for inbound traffic. They process traffic before translating private IP addresses to public IP addresses for outbound traffic. Enter a range, service tag, or application security group to reduce the number of security rules needed. |
| Protocol | TCP, UDP, ICMP, or Any. |
| Direction | Whether the rule applies to **inbound**, or **outbound** traffic. |
| Port range | Wecan specify an individual or range of ports. For example, you could specify 80 or 10000-10005. Specifying ranges enables you to create fewer security rules. |
| Action | Allow or deny |

**Default Security Groups:**

Azure provides the default security rules for both incoming and outcoming traffic in each network security group that we create:

**Inbound**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

##### **Inbound Load Balancer**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65001 | AzureLoadBalancer | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Allow |

##### **Destination Inbound**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Outbound**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

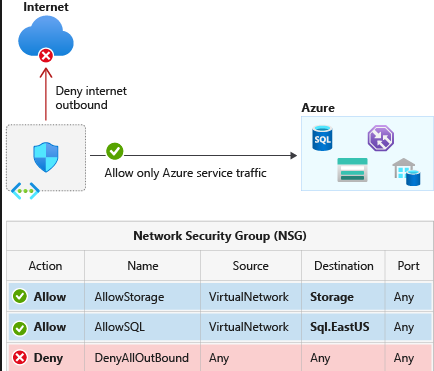
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65001 | 0.0.0.0/0 | 0-65535 | Internet | 0-65535 | Any | Allow |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Source** | **Source ports** | **Destination** | **Destination ports** | **Protocol** | **Access** |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

### **Augmented security rules**

Augmented security rules simplify security definition for virtual networks, allowing you to define larger and complex network security policies, with fewer rules. You can combine multiple ports and multiple explicit IP addresses and ranges into a single, easily understood security rule. Use augmented rules in the source, destination, and port fields of a rule.

**Service tags**

A service tag represents a group of IP address prefixes from a given Azure service. It helps to minimize the complexity of frequent updates on network security rules.

#### **Application security groups**

Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses.

**Types of IP:**

|  |  |  |
| --- | --- | --- |
| **Static** | IP doesn’t change | Production, DNS mapping |
| **Dynamic** | IP changes on stop/start | Testing or temporary services |

# **Azure Application security groups**

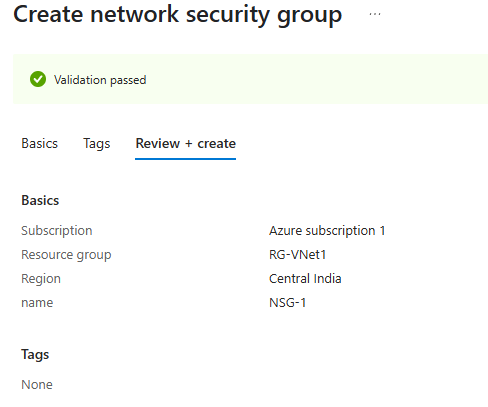
Application Security Group (ASG) is a networking feature that allows you to group Azure virtual machines (VMs) based on the application to which they belong. ASGs enable network security group (NSG) policies to be defined using logical application groupings rather than individual VM IP addresses. This simplifies network security rule management, especially when multiple VMs belong to the same application or service. Application Security Groups are especially useful in complicated and distributed application architectures where VMs must safely communicate across network boundaries. You can use ASGs to ease the maintenance of network security rules, improve security, and simplify application deployment in Azure.

**ASSIGNMENT**

1. **Create Network Security Group:**

Azure Portal > Network Security Groups.

Click Create.

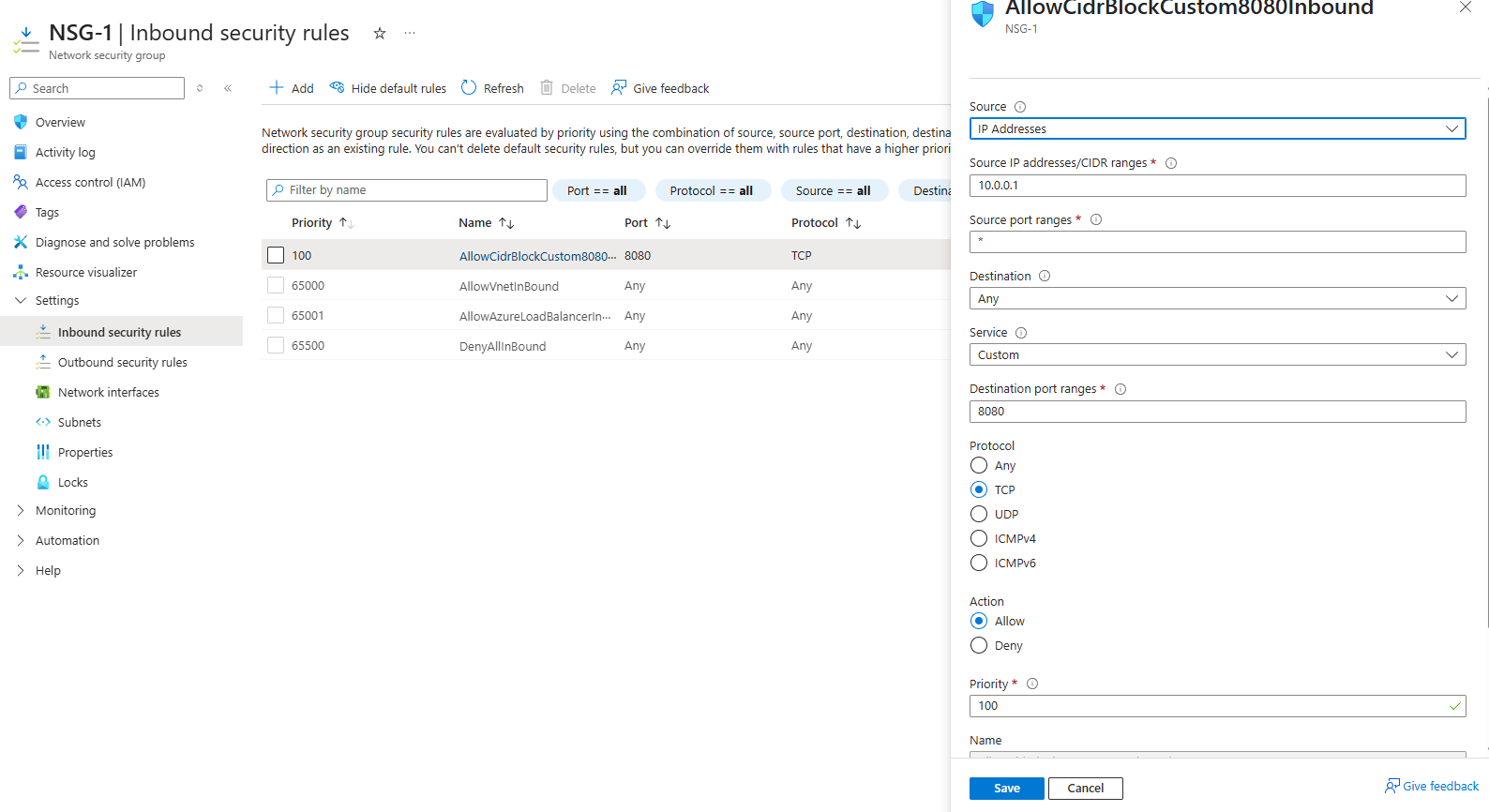
****

1. **Adding INBOUND RULE :**

NSG > Inbound Security Rules > Click + Add.

Source: IP Addresses  
Configure as per requirements

Click Add

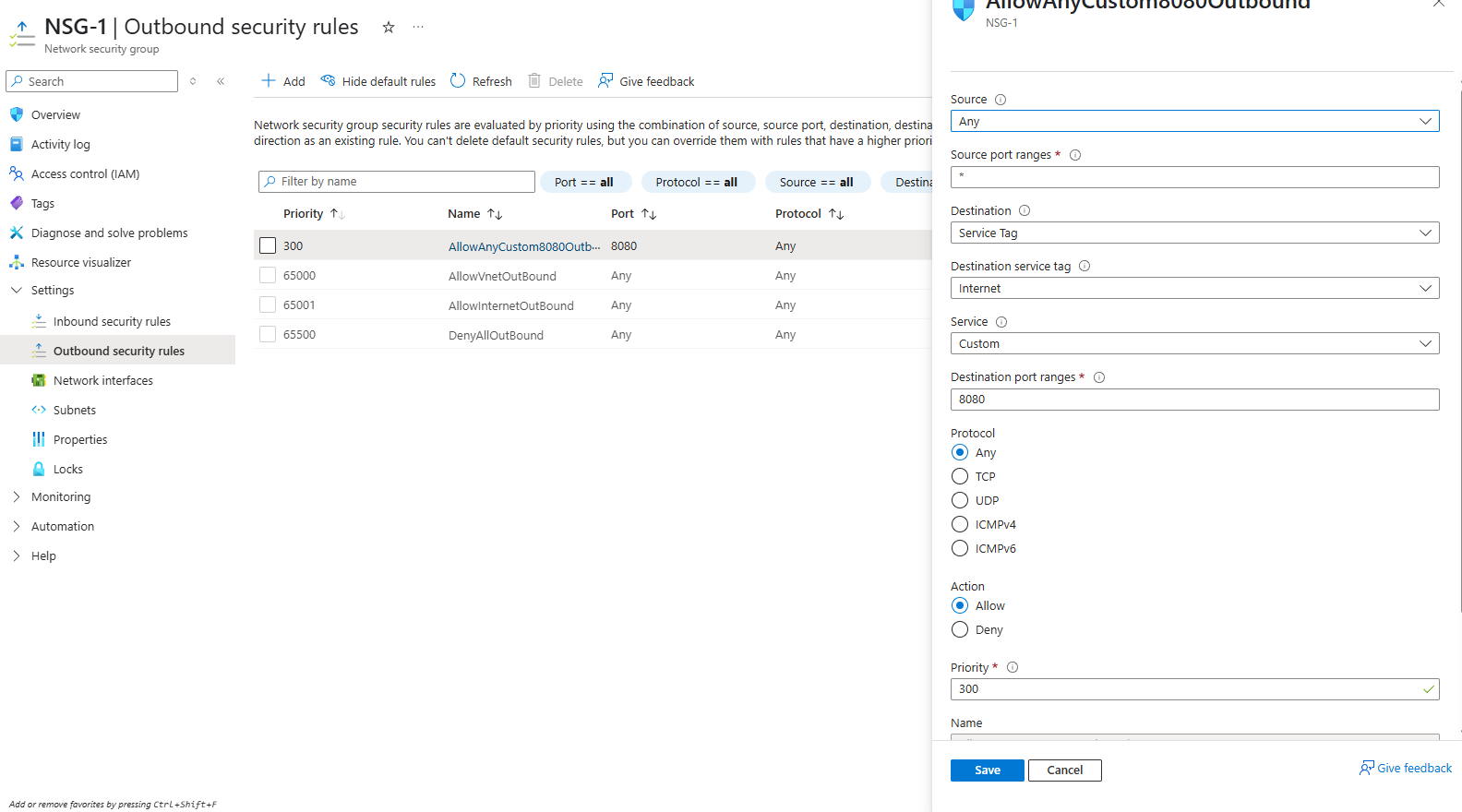
****

1. **Adding OUTBOUND rule :**

NSG > Outbound Security Rules > Click + Add.

Source: IP Addresses  
Configure as per requirements

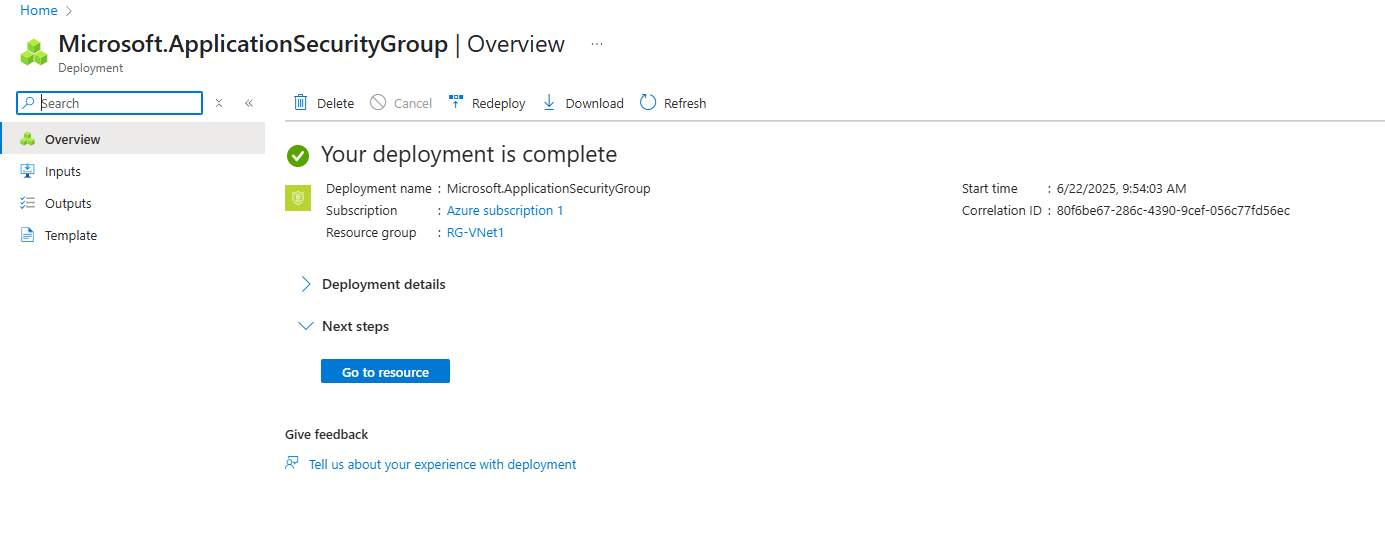
Click Add

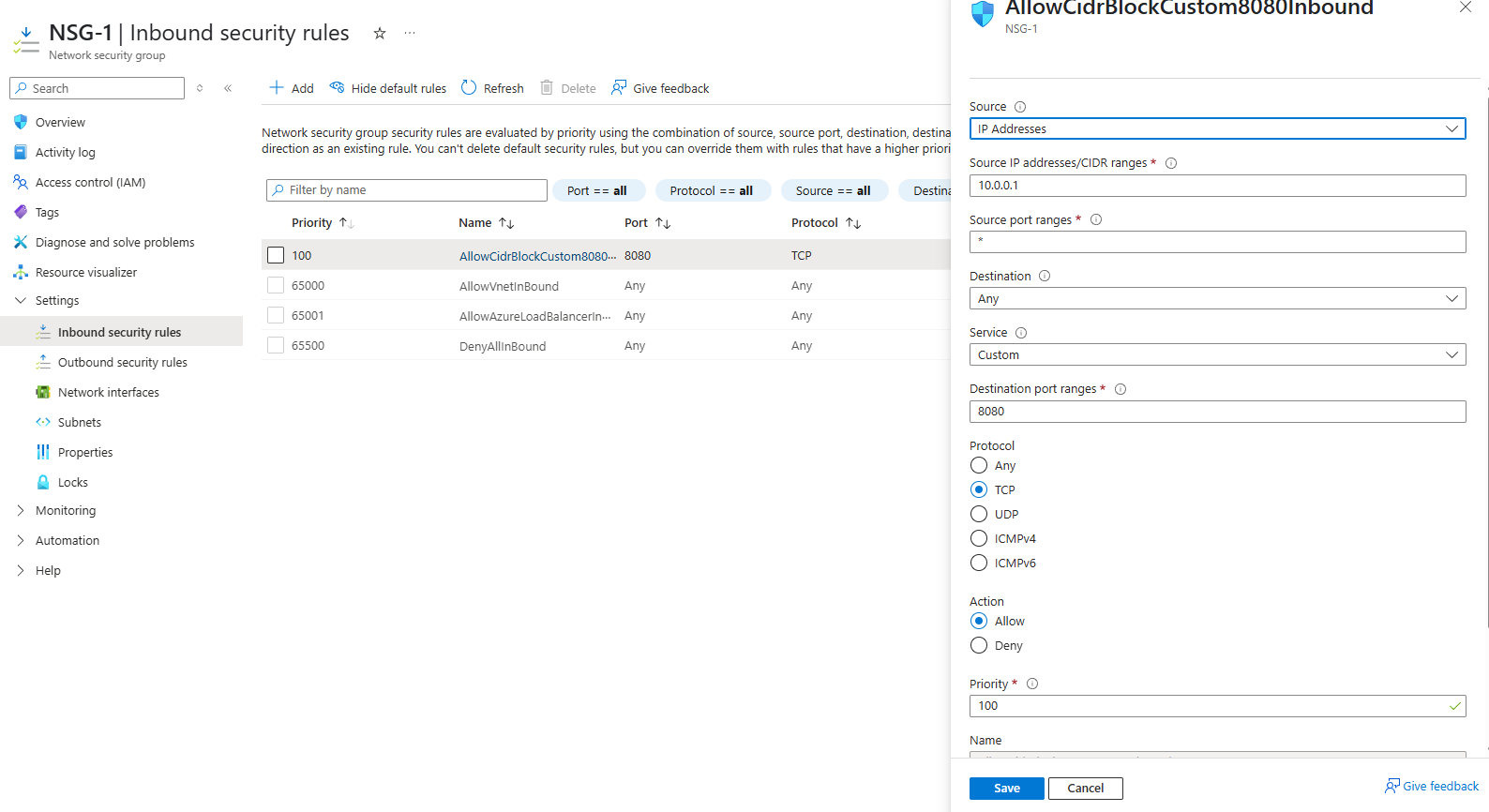
****

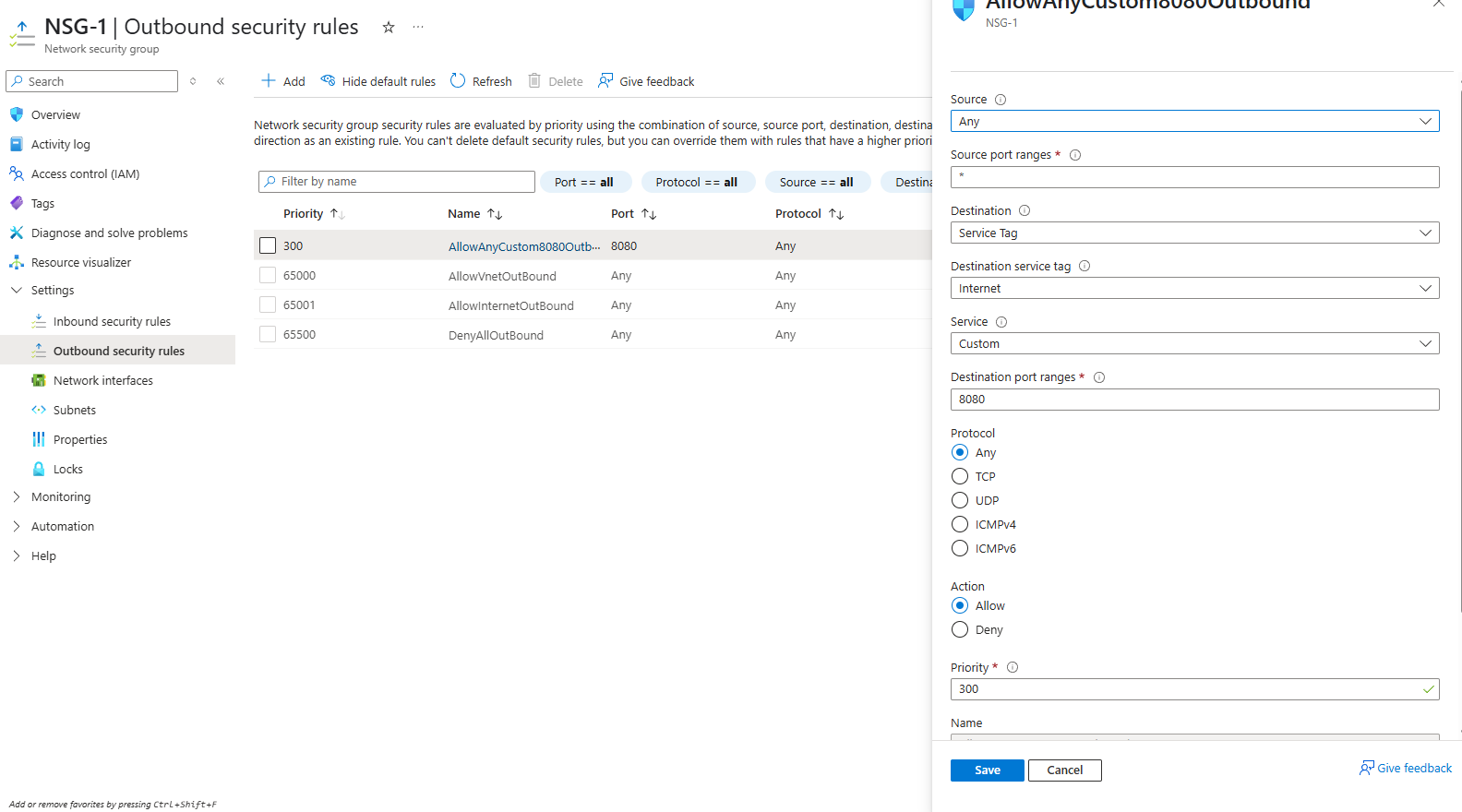
1. **Creating Application Security Groups:**

Azure Portal > Search Application Security Groups.

Click Create.

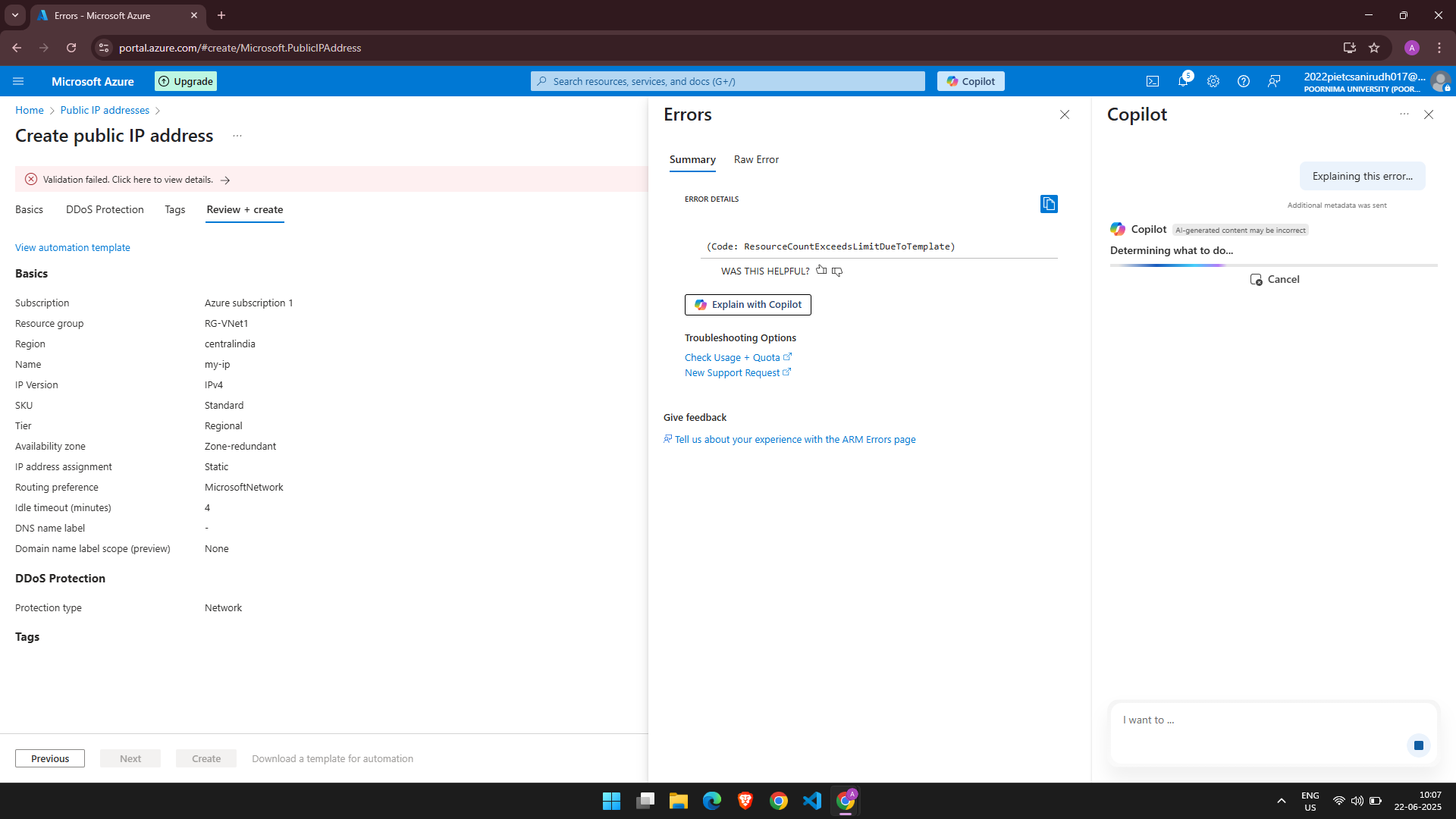
****

1. **Allow Specific IP to Access VMs:** 
2. **Deny Internet Access Using NSG:**

****

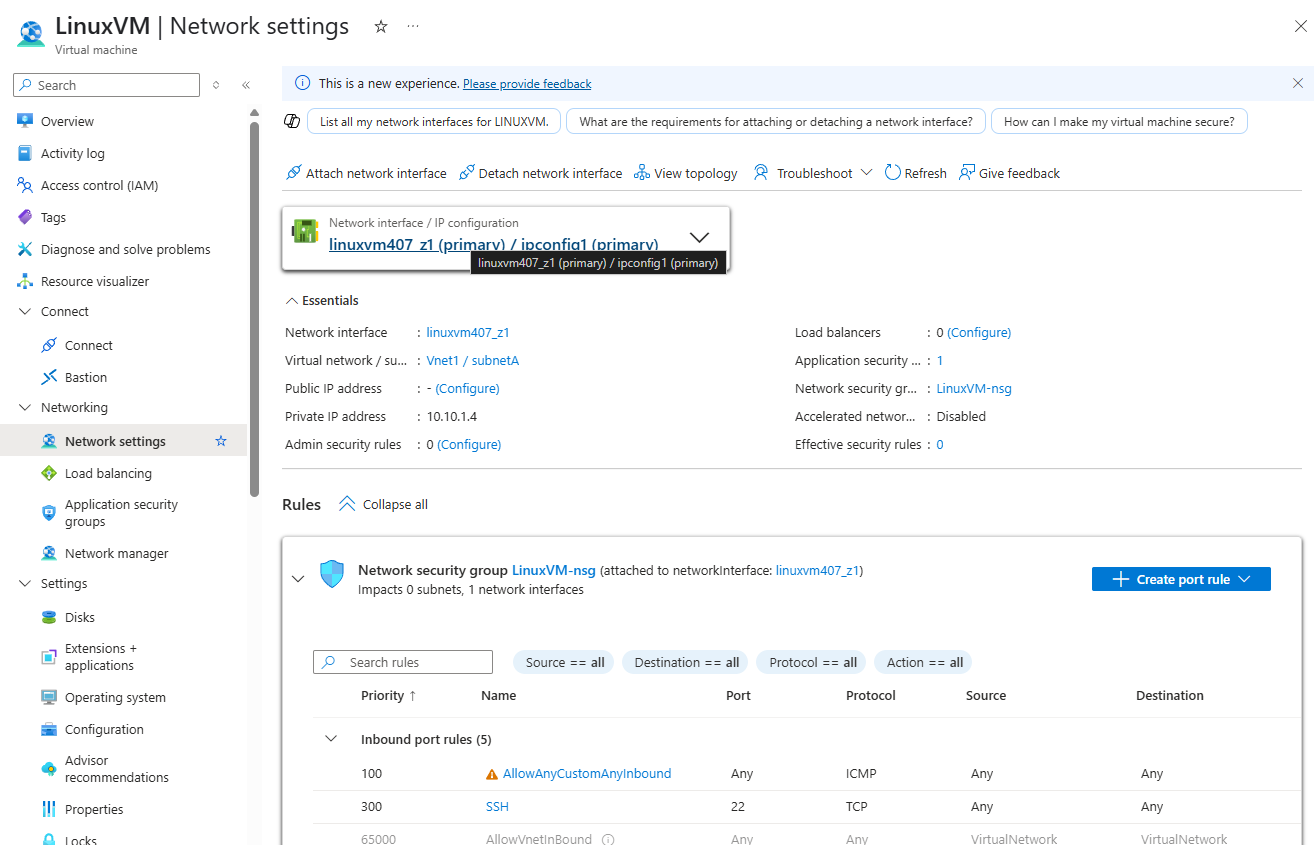
1. **Creating Public IPs:**

Azure Portal > Search Public IP addresses > Create.  
Click Create

****

1. **Associate/De-associate Public IP with VM:**

VM > Networking > Network Interface > IP Configurations  
Click ip> Under Public IP Address, click Associate/Diassociate  
Choose or create Public IP

****

1. **Allocate Static Private IP to VM:**

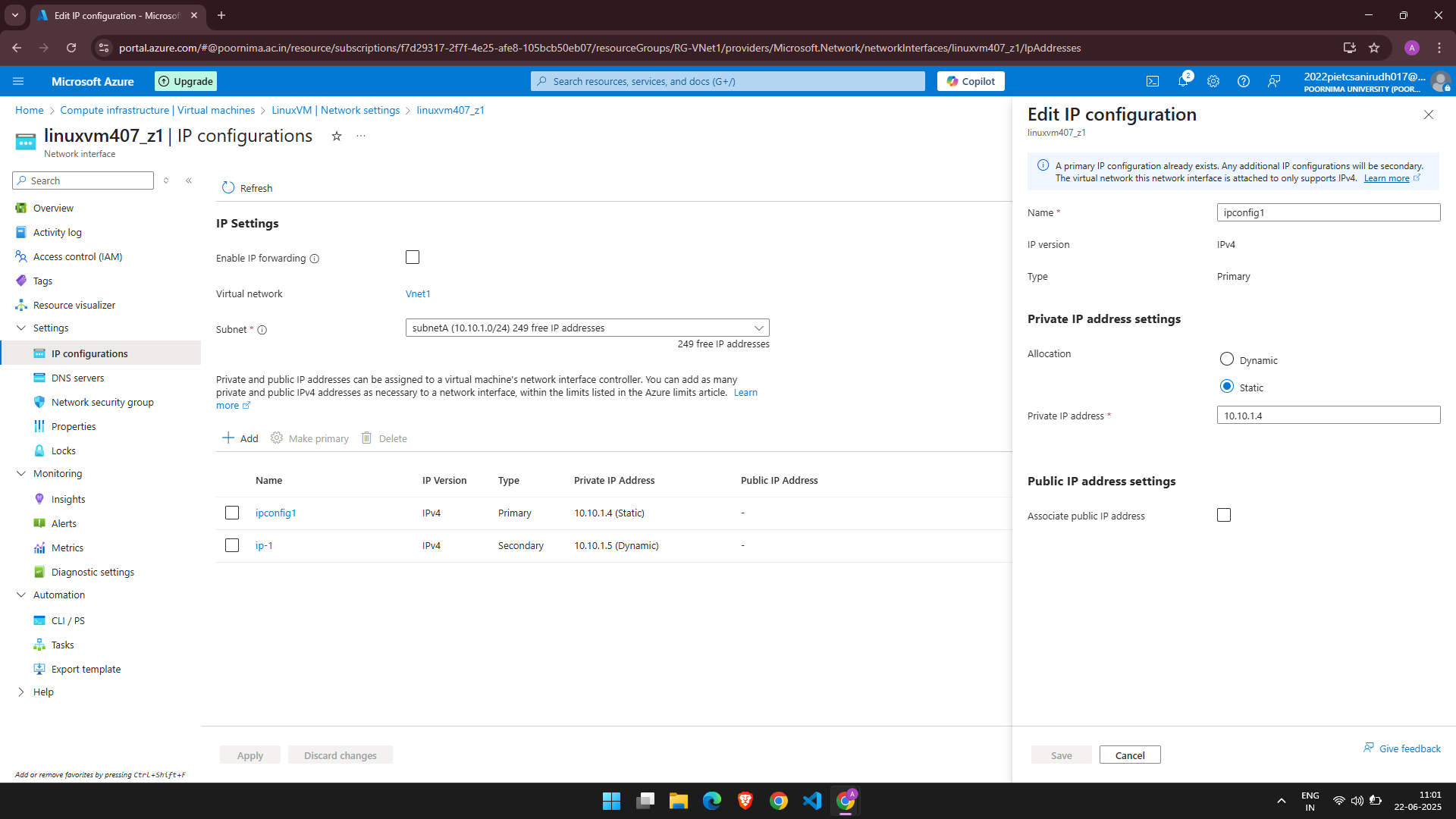
VM > Networking > Network Interface

Click on IP Configuration

Change IP Assignment to Static

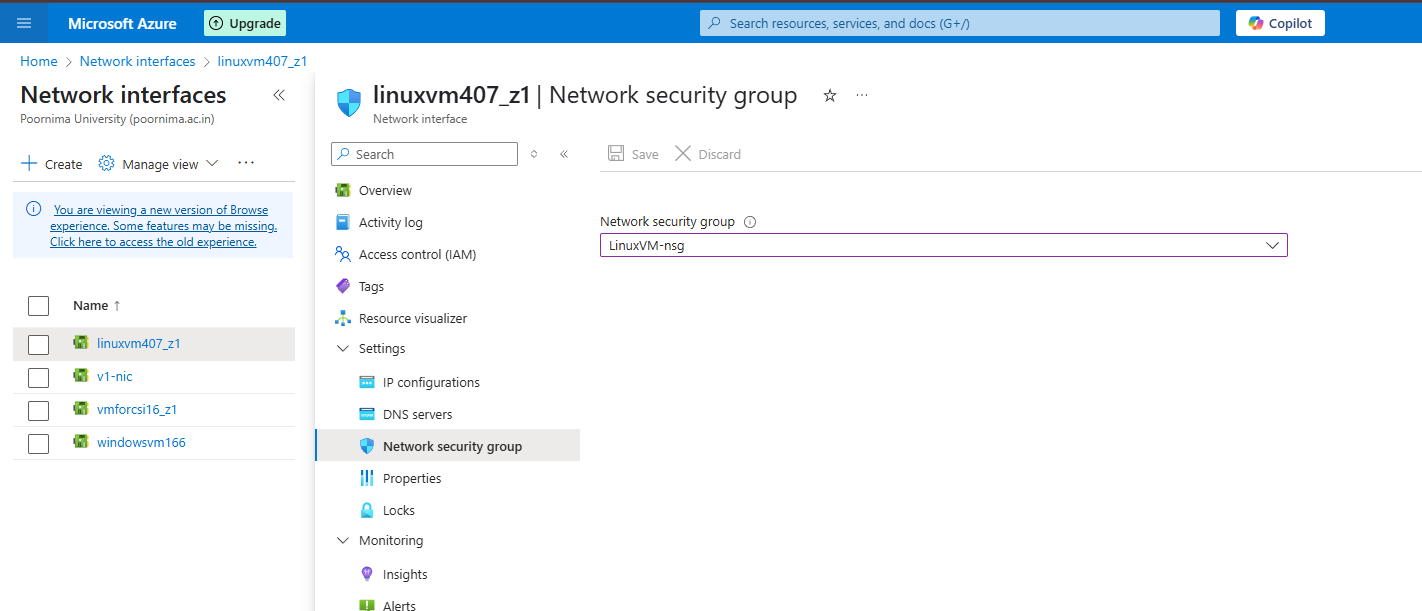
Enter available IP from subnet range

Click Save

****

**10.Attach NSG to NIC:**

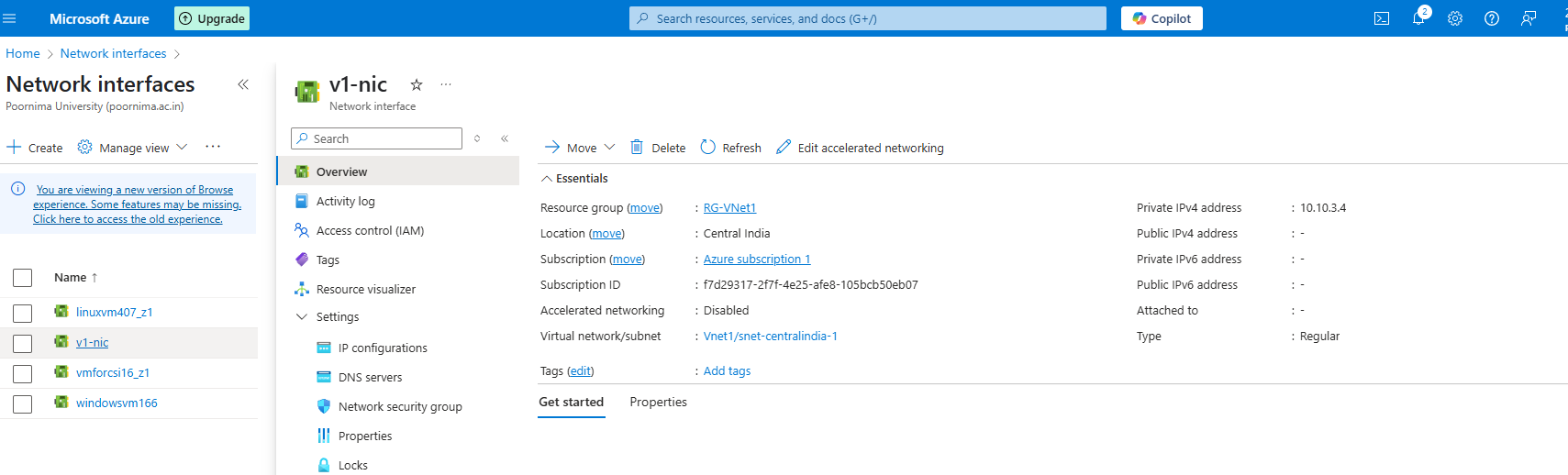
Network Interface > Network Security Group  
Select your NSG from dropdown

****

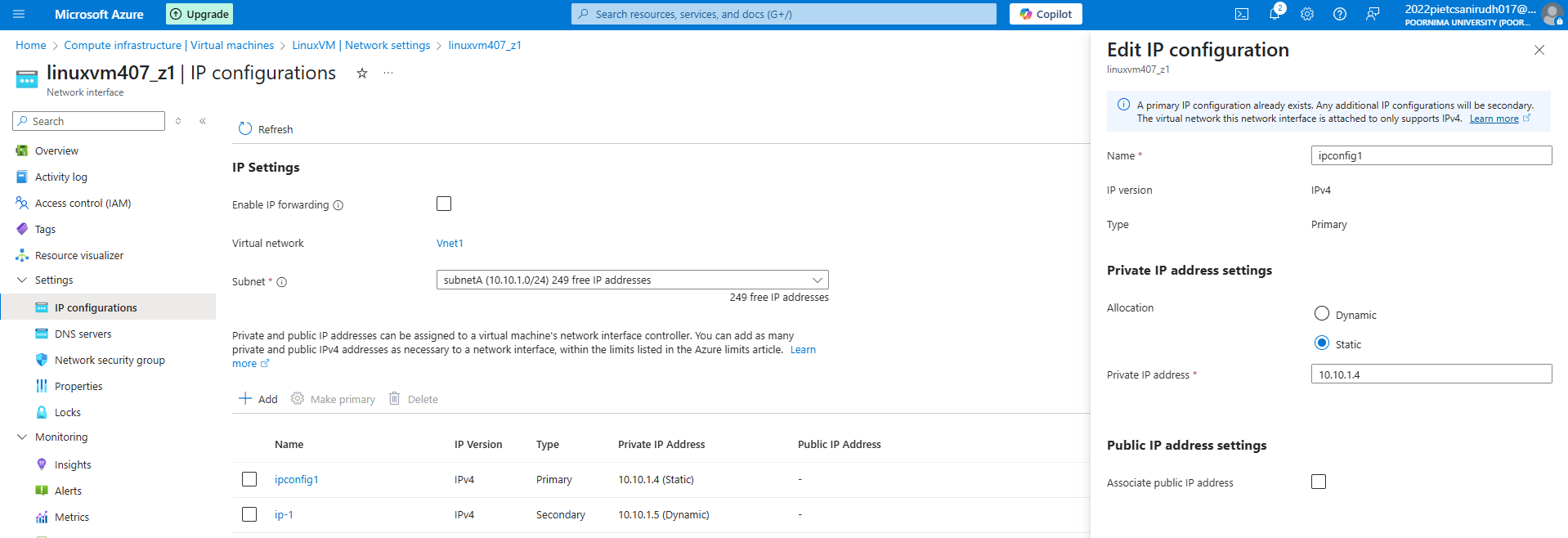
**11.Create a Network Interface (NIC):**

Azure Portal > Create a Resource > Network Interface

Click Create

**12. Assign ASG to a VM:**

VM > Networking > Network Interface  
Click the NIC > Configuration > Application Security Groups  
Select asg> Save

****

**References**

* **Microsoft Azure Documentation**
* **Medium**
* **GeeksForGeeks**