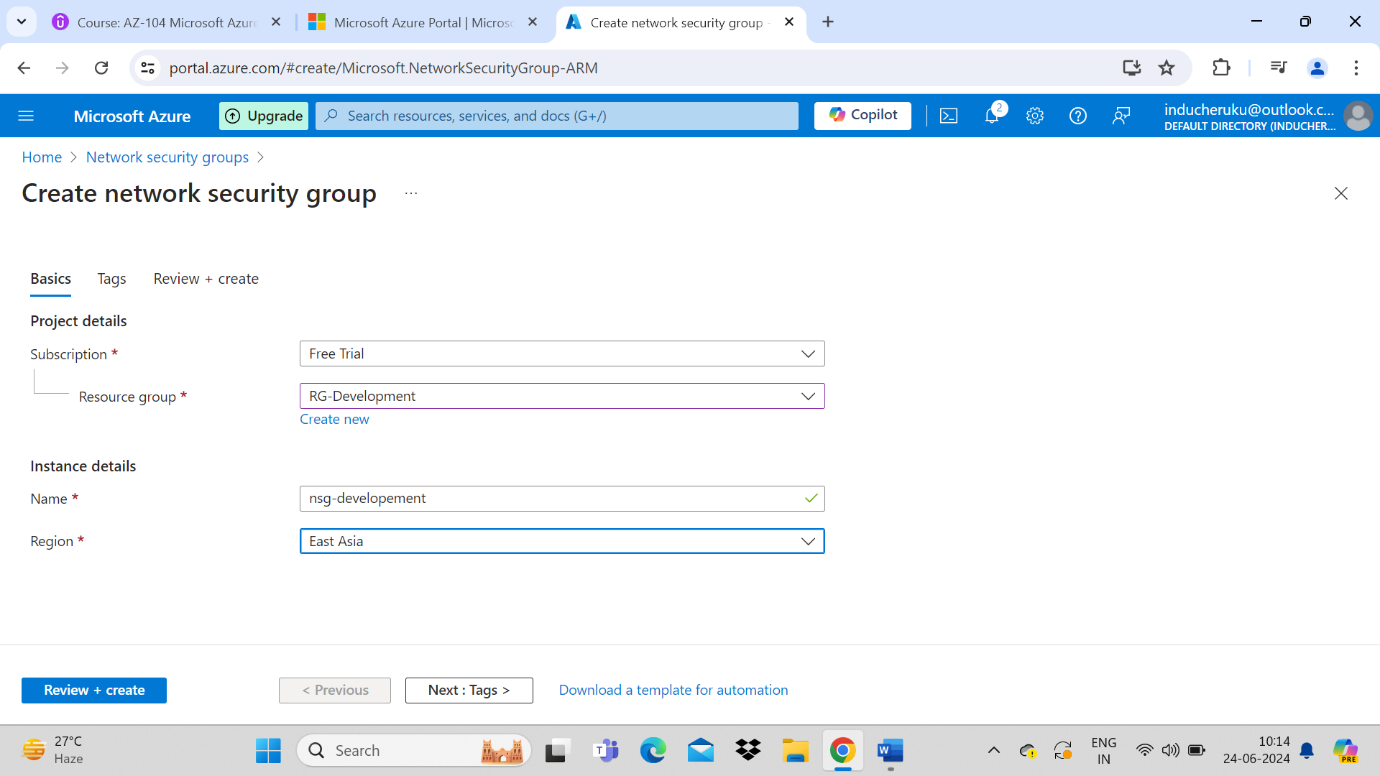
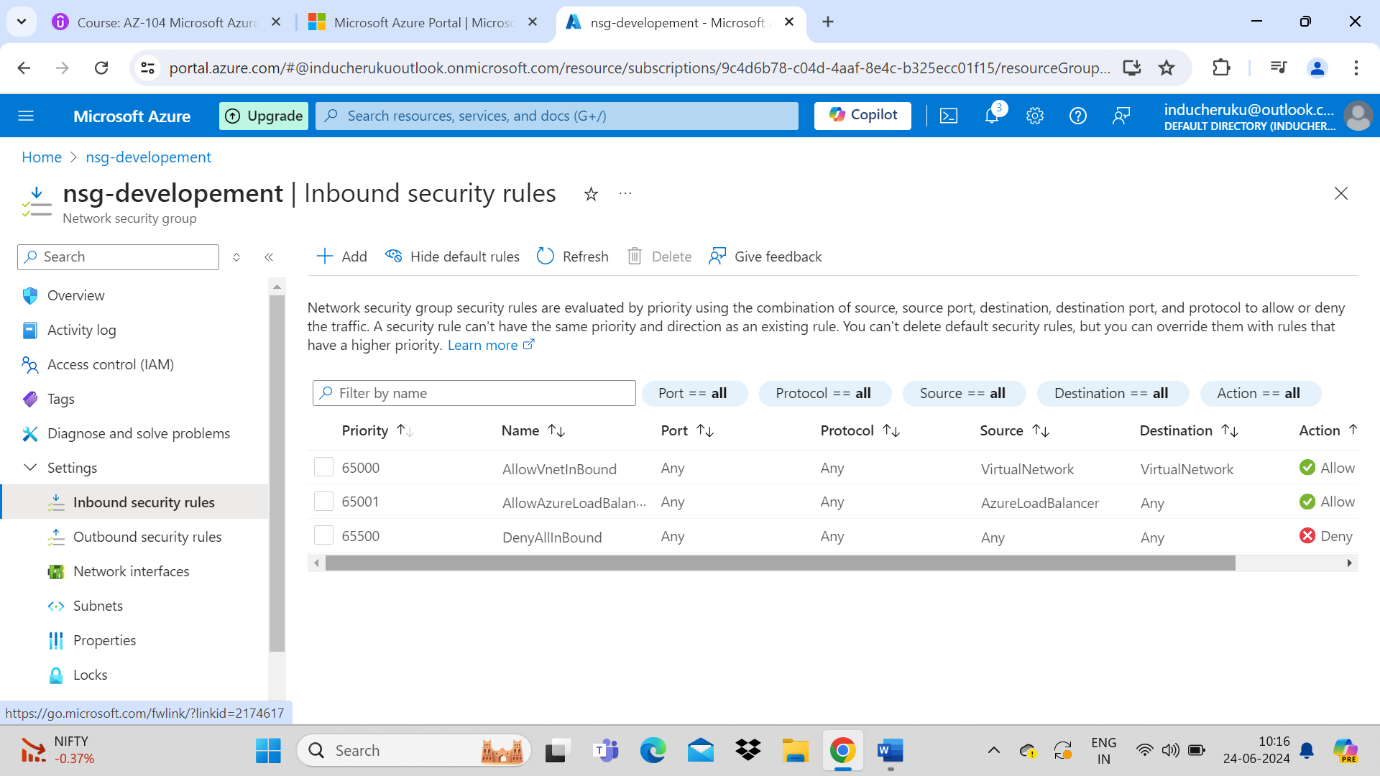
Network security group’s :

Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets.

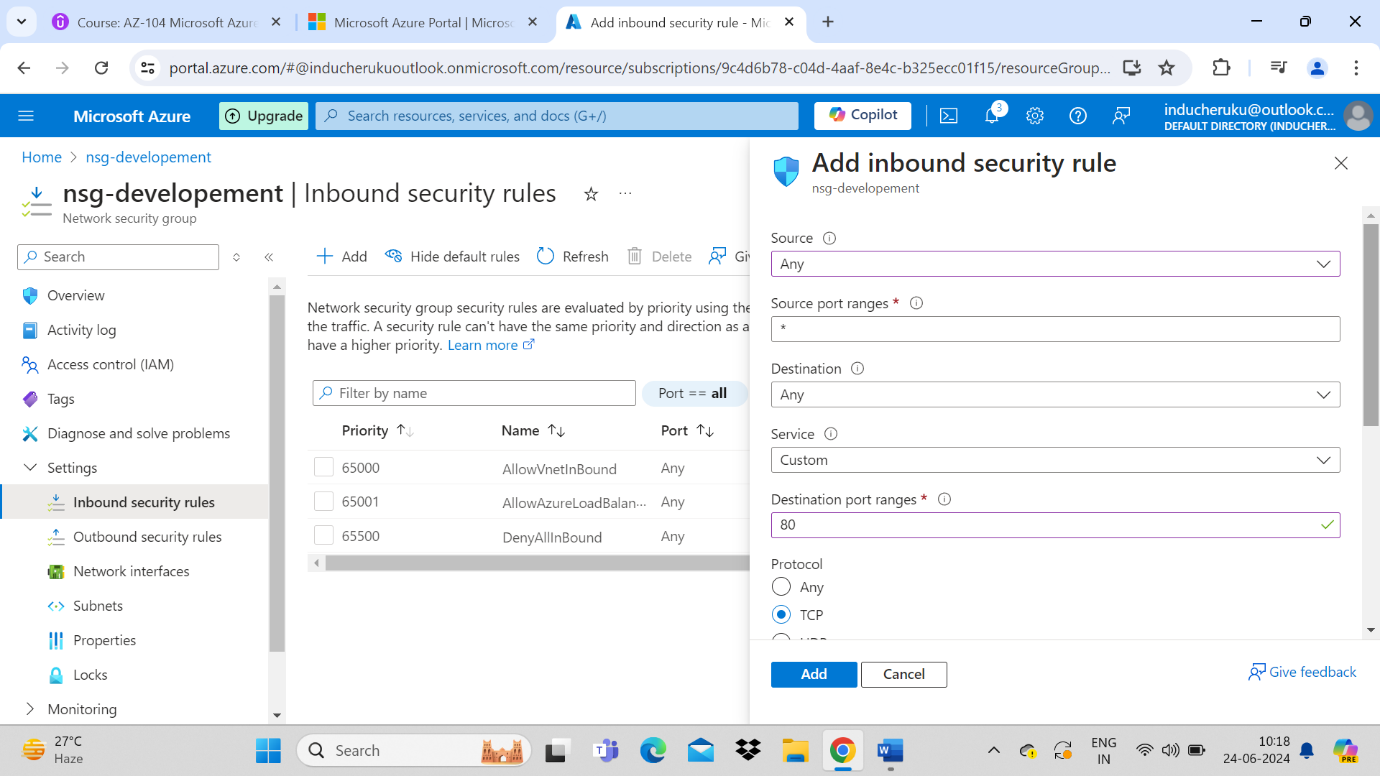
1. Go to Azure portal and search for NSG

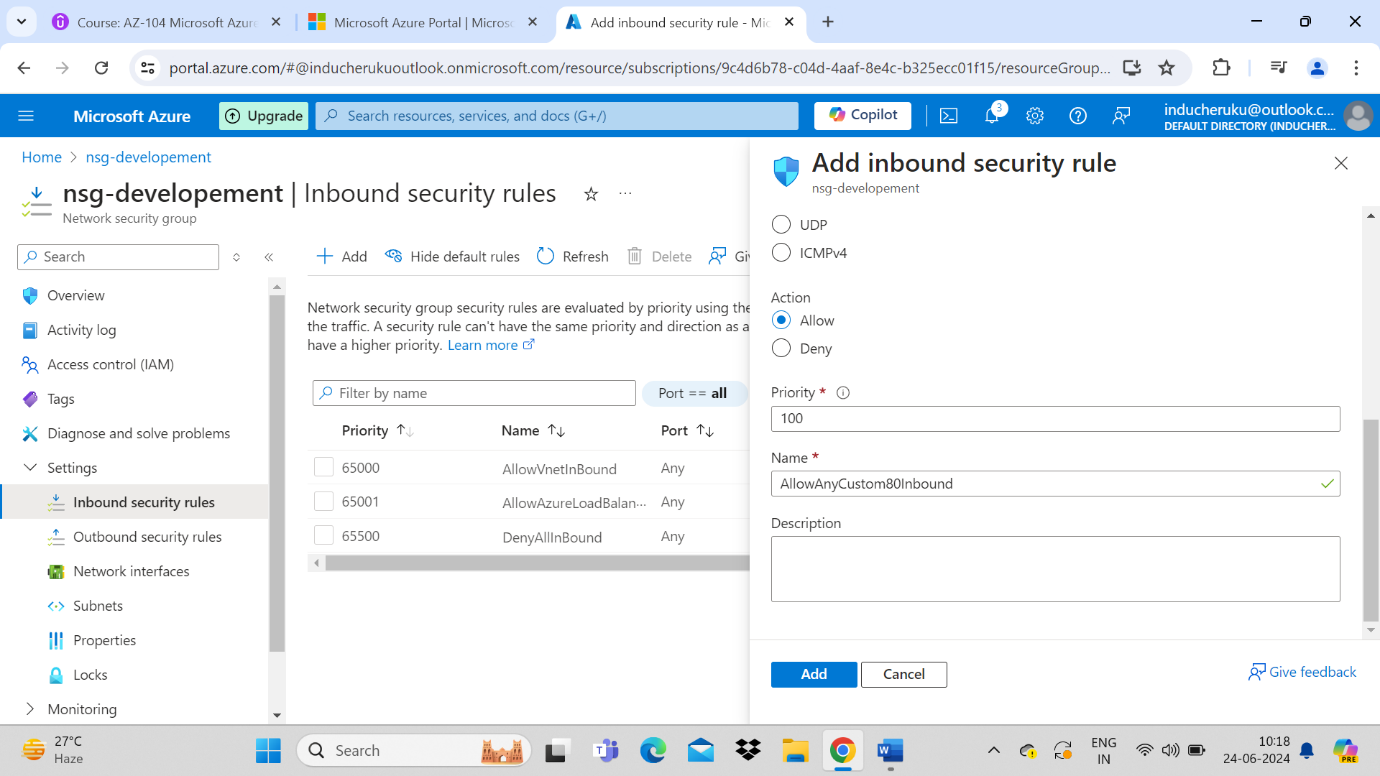


1. Review + Create
2. Add new inbound/outbound rules to NSG

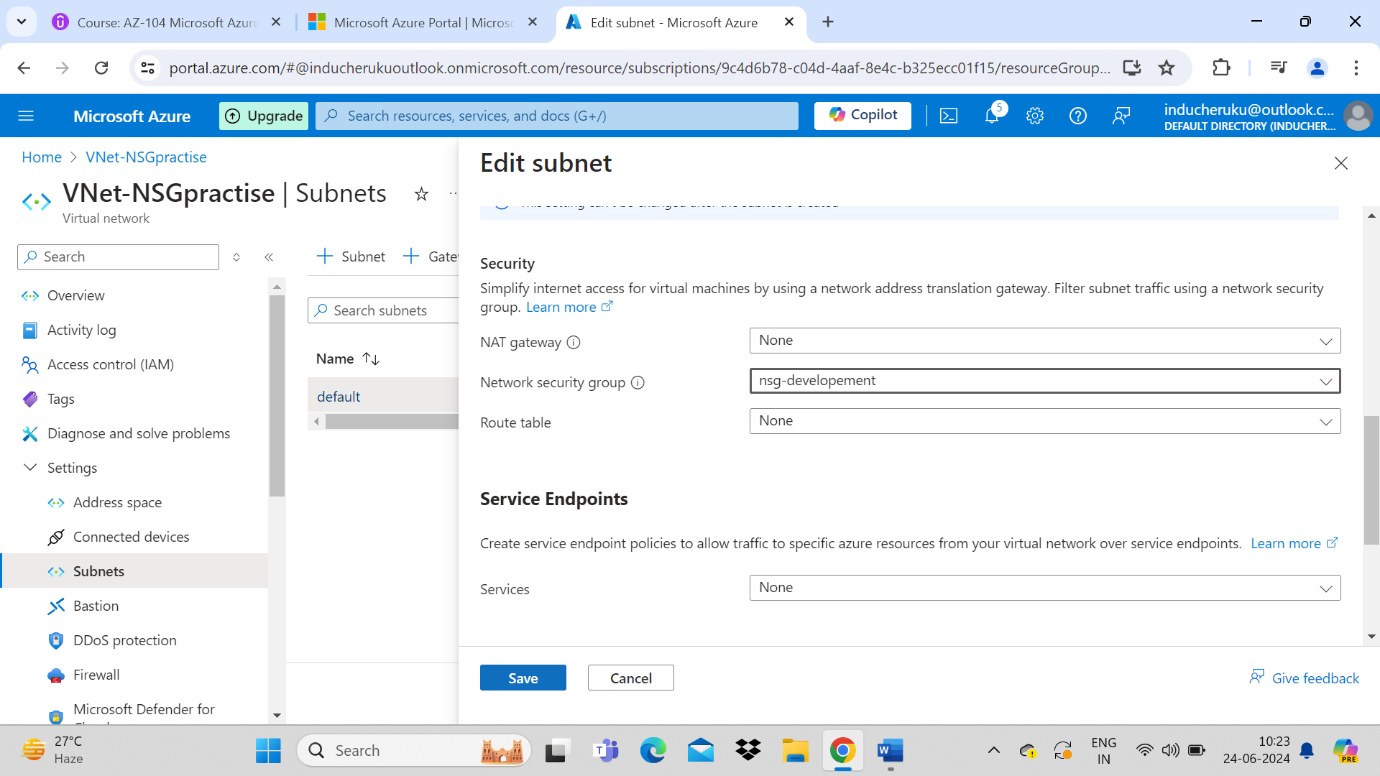


1. Select Inbound security rules from the left side menu

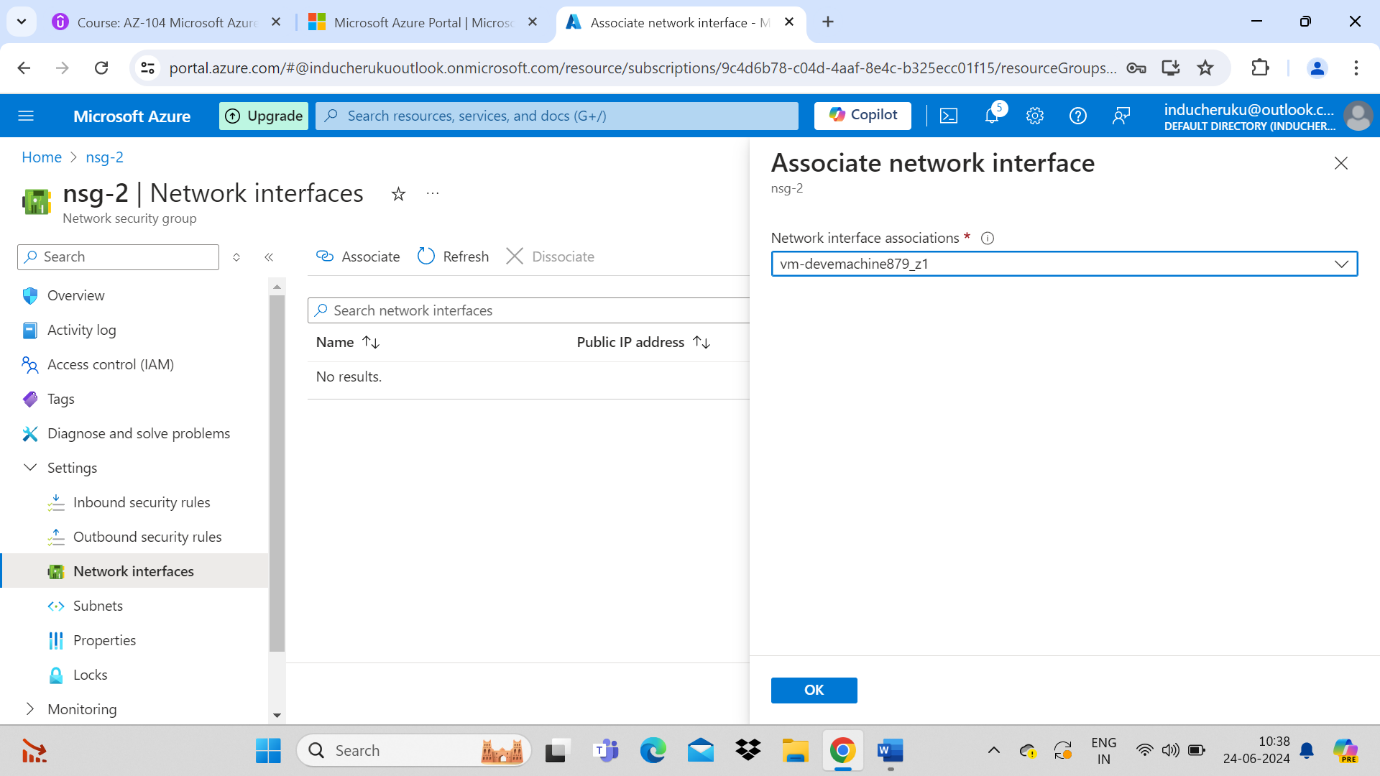




1. Apply a NSG to subnetwork
2. Go to respective VNet and go to subnet section in left side menu
3. Select the respective subject (Eg: select default subject ) scroll down and find the NSG option dropdown to select

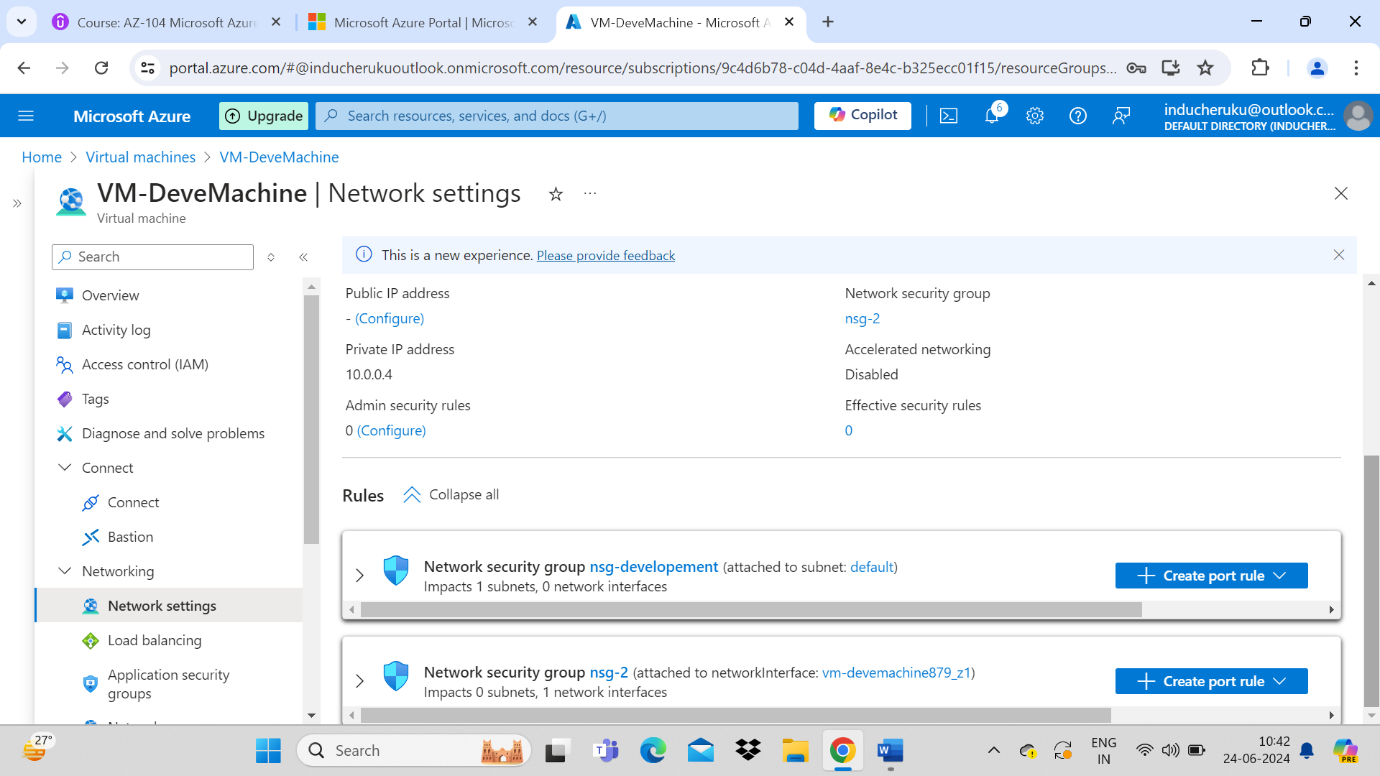


1. Now Create a new VM and add VM Level security by adding new nsg/rules to created virtual machine
2. Create a new NSG with name NSG-02. Go to NSG-02 -> select network interfaces from left side menu -> Click associate > select NIC (vm related) from the drop down -> click ok



Now go VM -> network setting – we can see two NSG’S

1. One NSG is attached via subnet level NSG for allow 8080 security
2. Second one is attached VM level NSG for default inbound and outbound security. PFA pic



Like wise . we can add single NSG to multiple VM’s and the security will apply to all the connection Virtual machine network interface cards.

