**Azure Virtual Networks and Virtual Machines**

1. Create an ARM Template for a virtual network with subnets and Network Security Group with Inbound Outbound rules

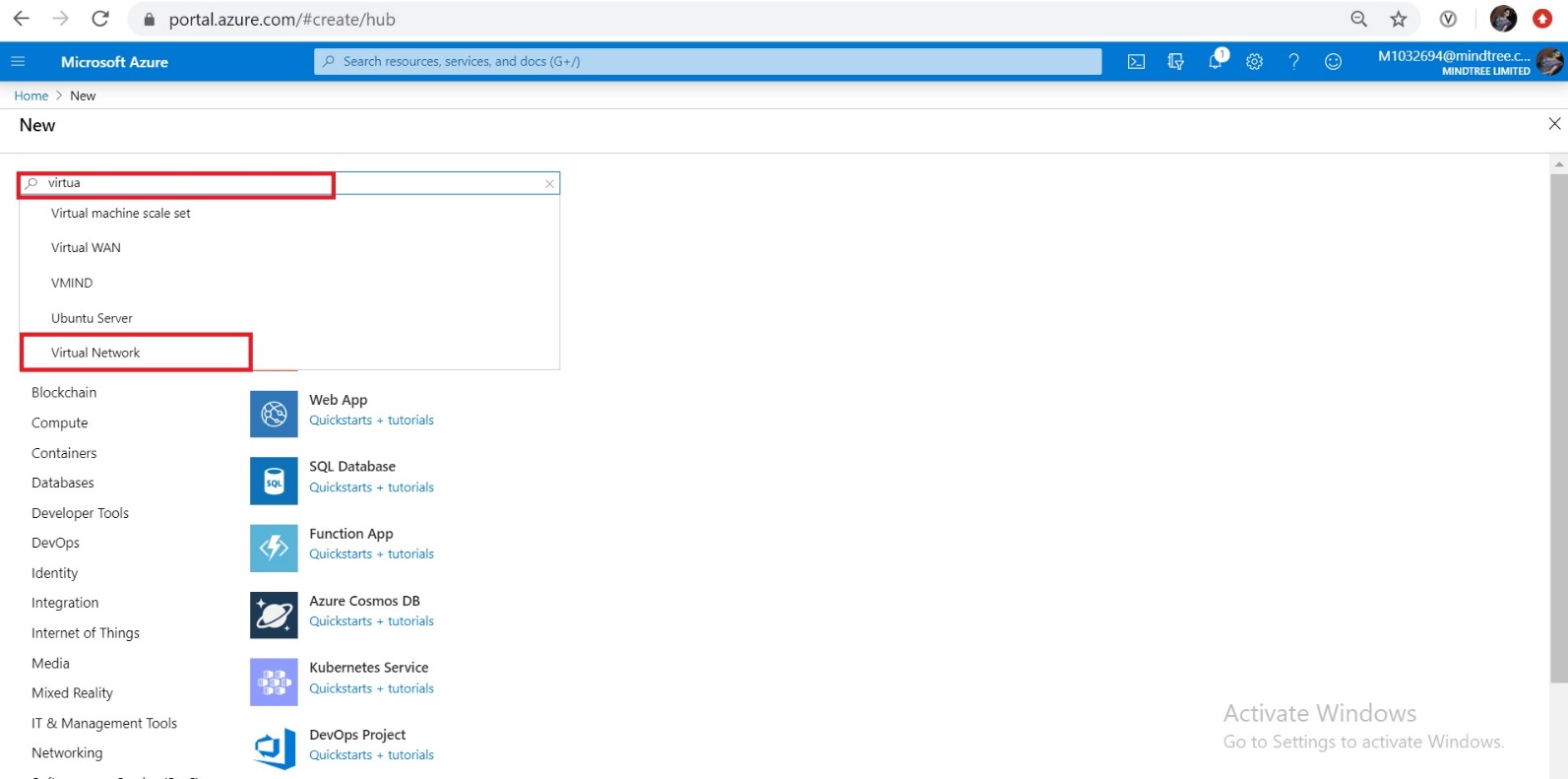
2. Write an ARM Template to deploy windows VM using the existing VNets and NSGs

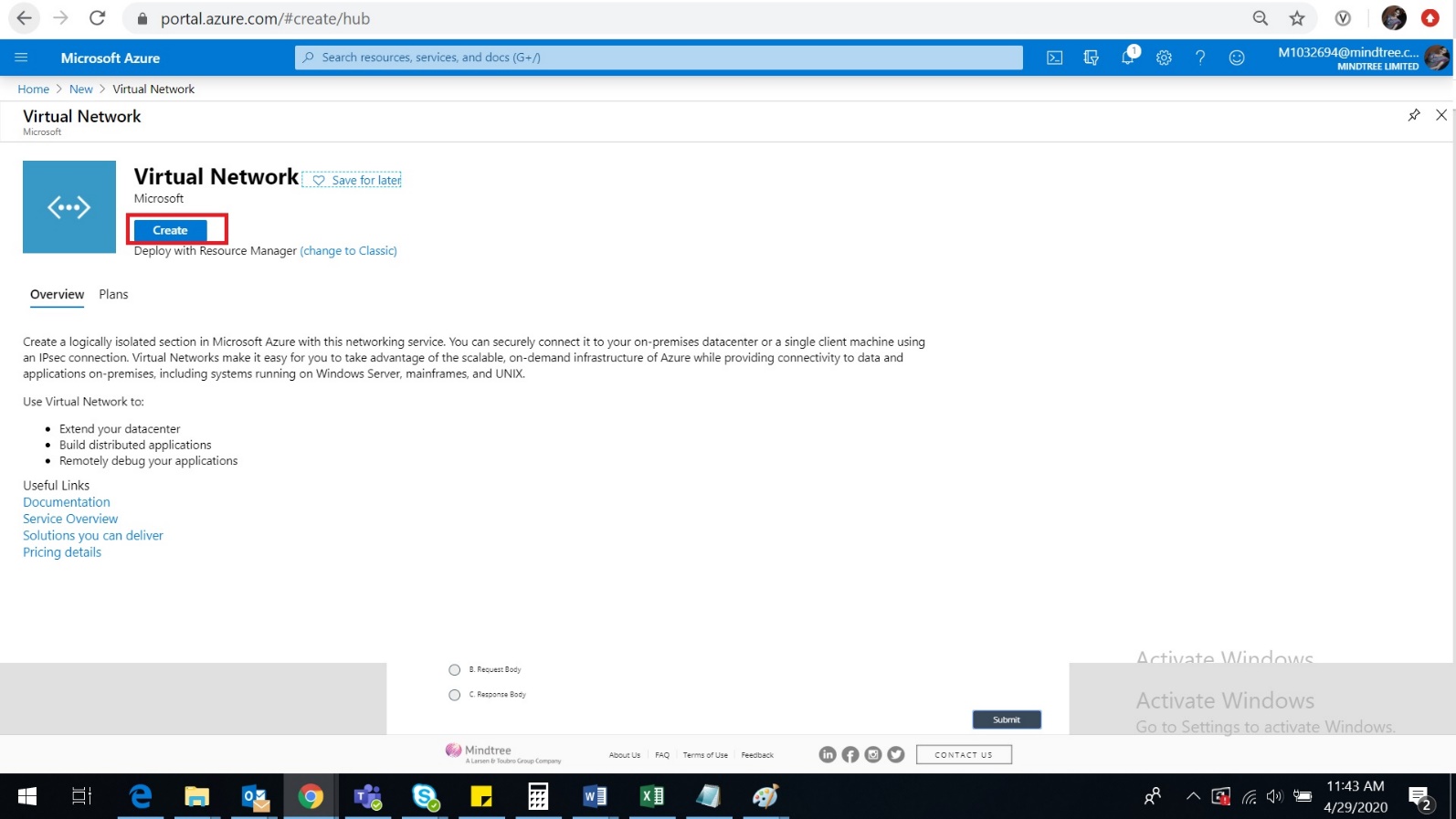
3. Deploy an application in the VM and access using the public IP

I am using the same resource group “AzureSKURestrictionsResourceGroup”, which is used in the previous assignment as a part of creation of virtual network.

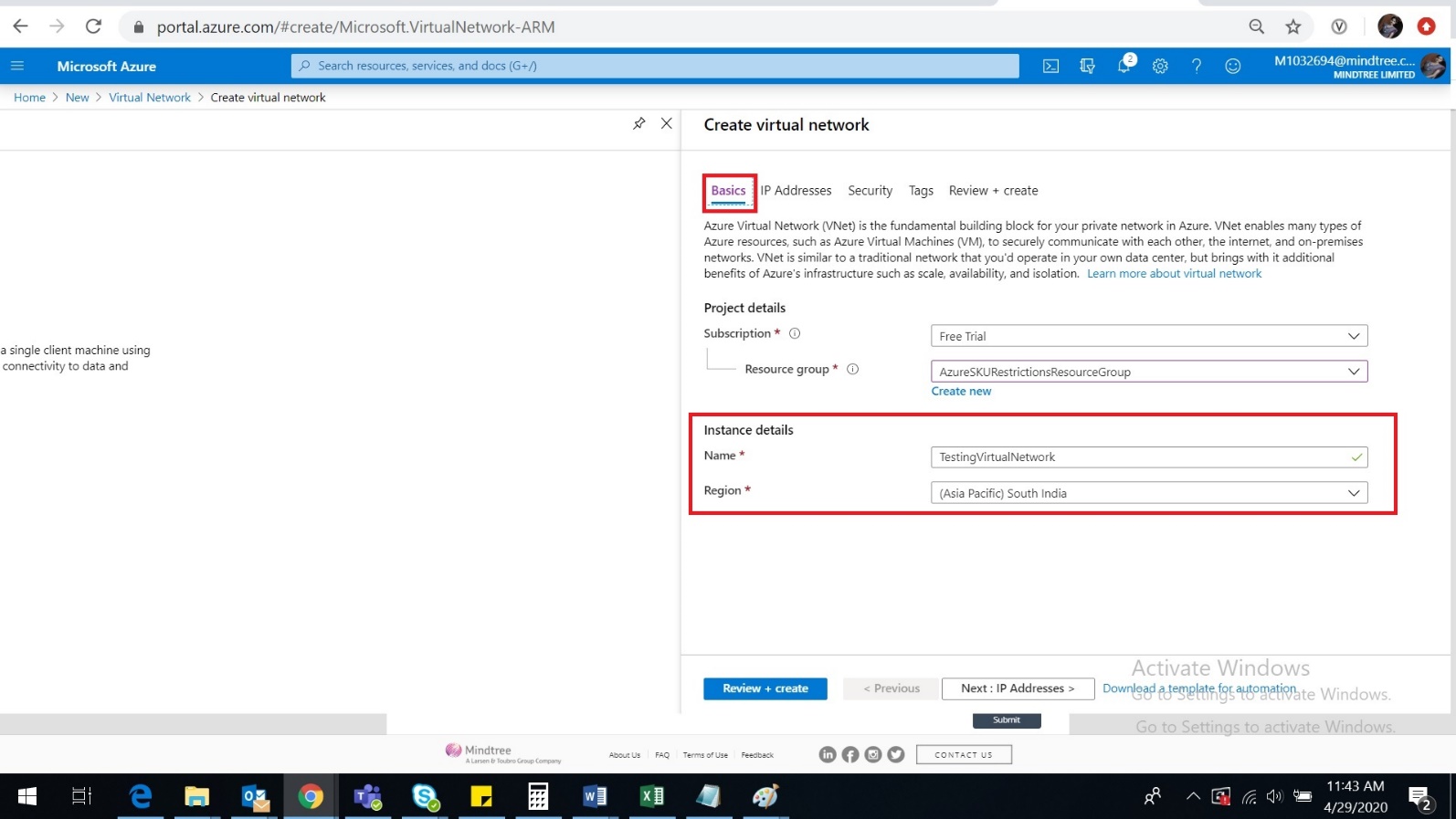
An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azurecloud dedicated to your subscription. ... S2S VPNs use IPSEC to provide a secure connection between your corporate VPN gateway and Azure.

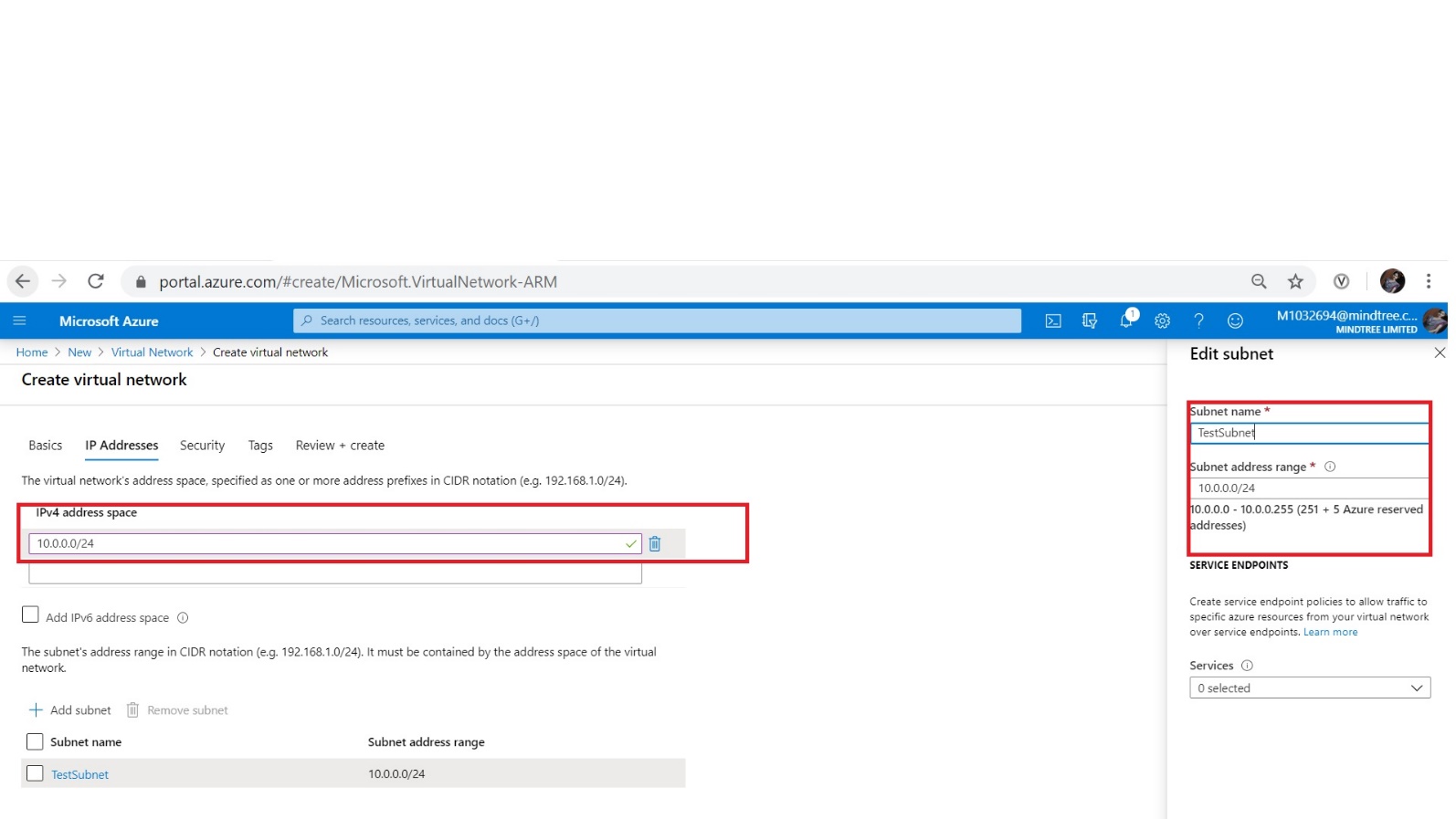
The below screen shots shows how to create the virtual networks which subnet and with network security.

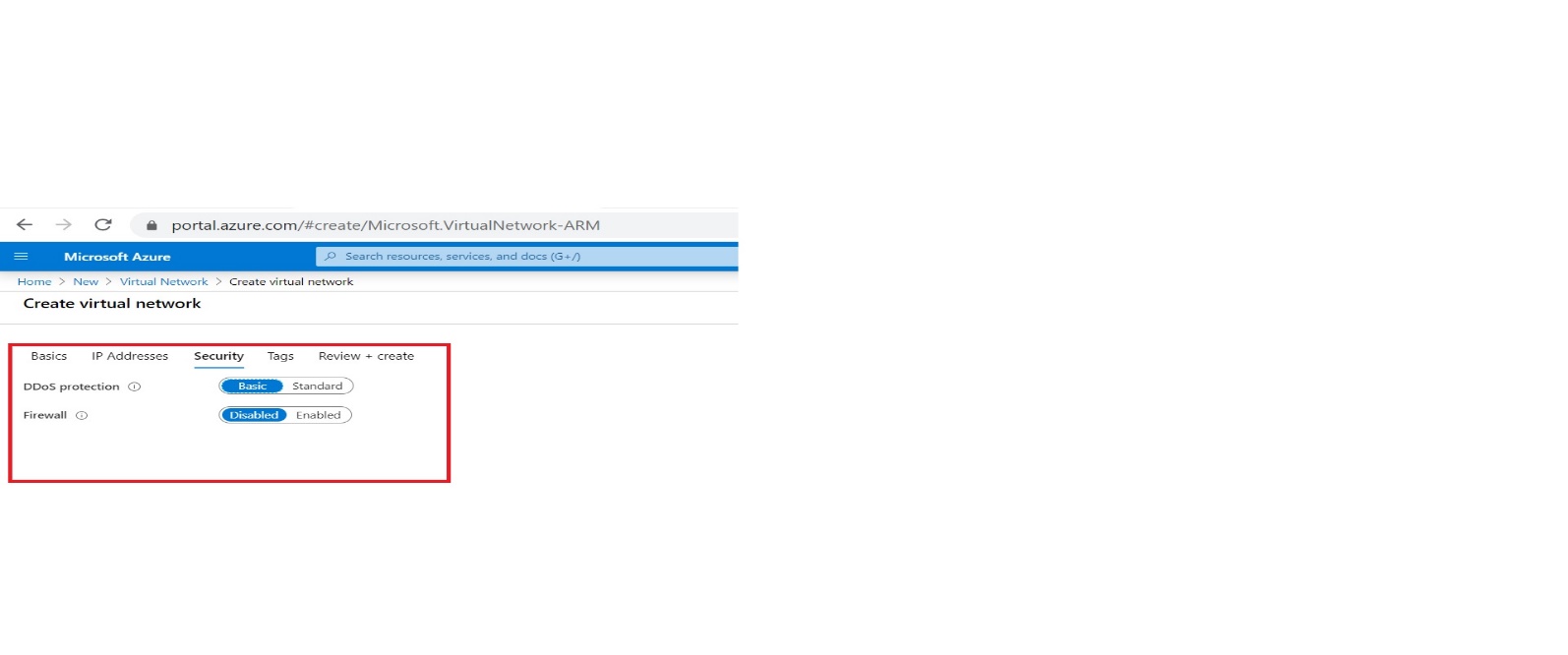


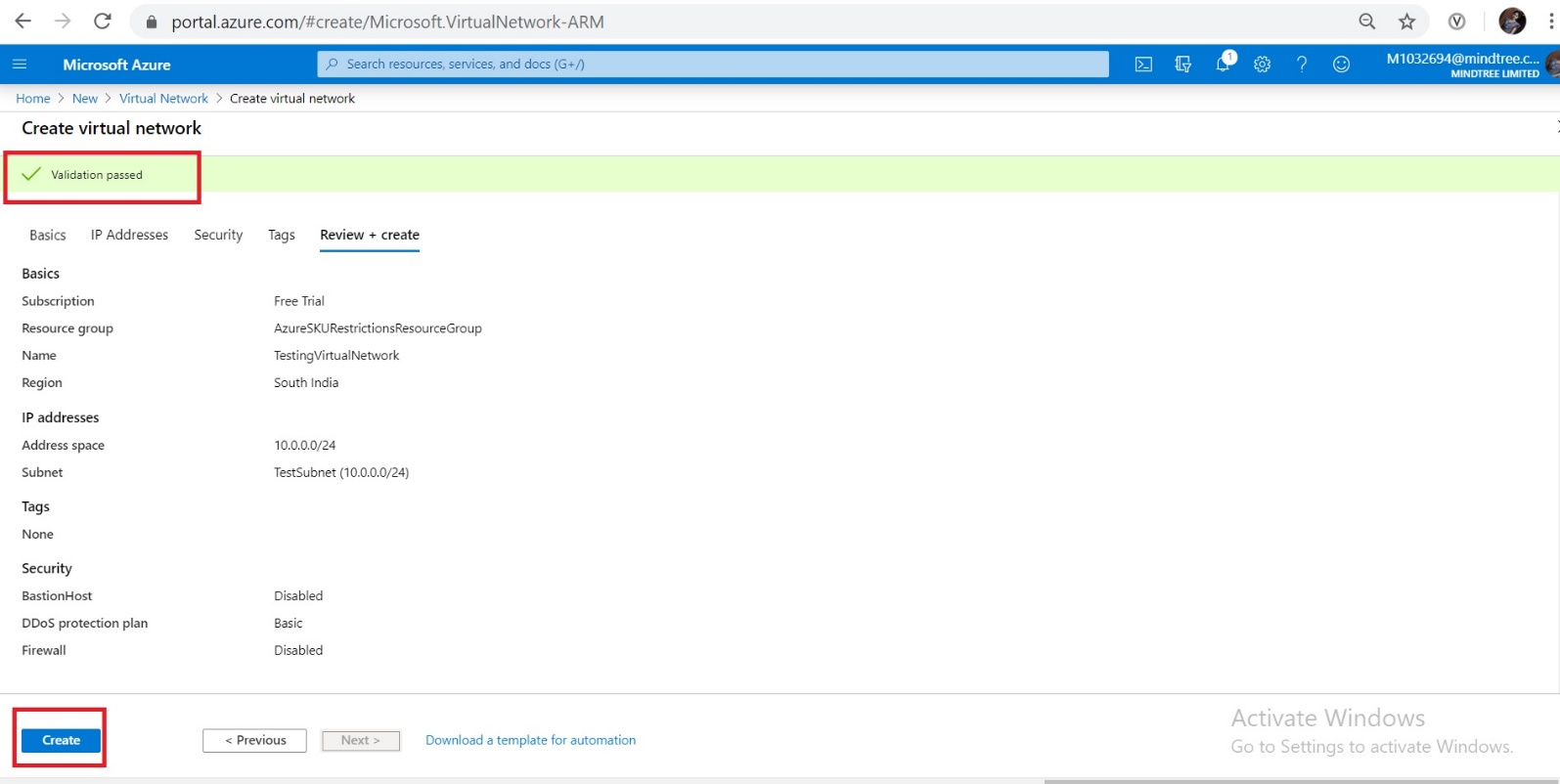


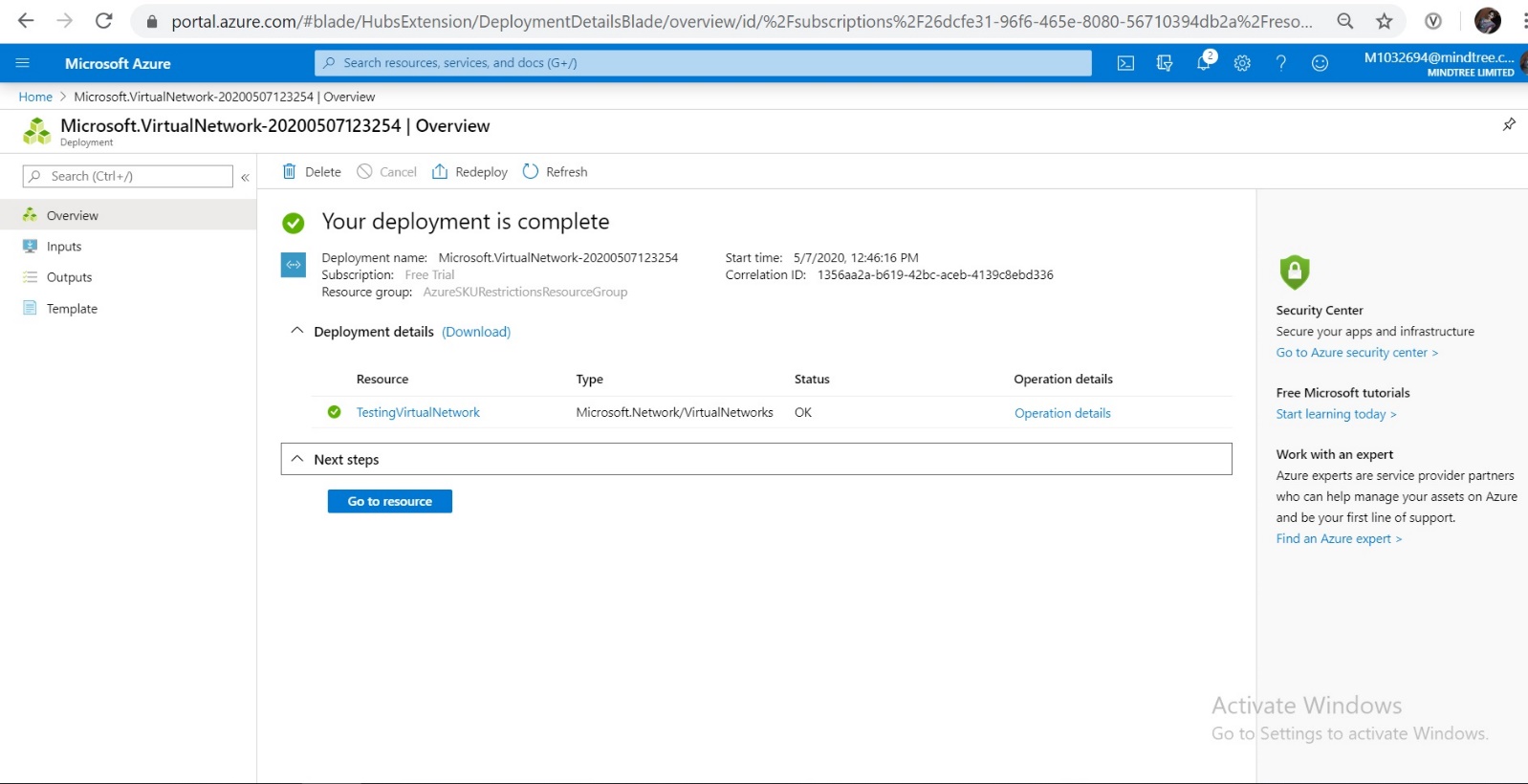
In the below Create virtual network window fill all the details and click on the create button



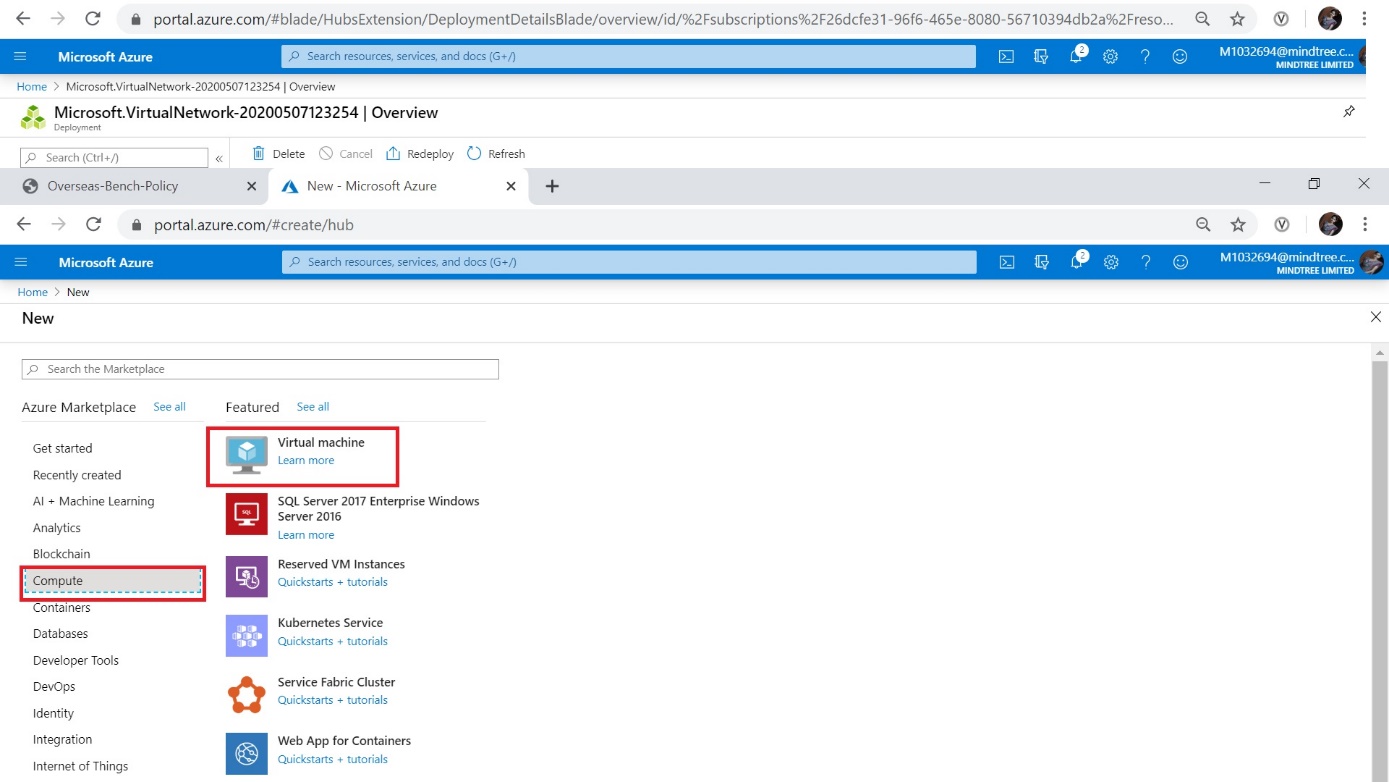


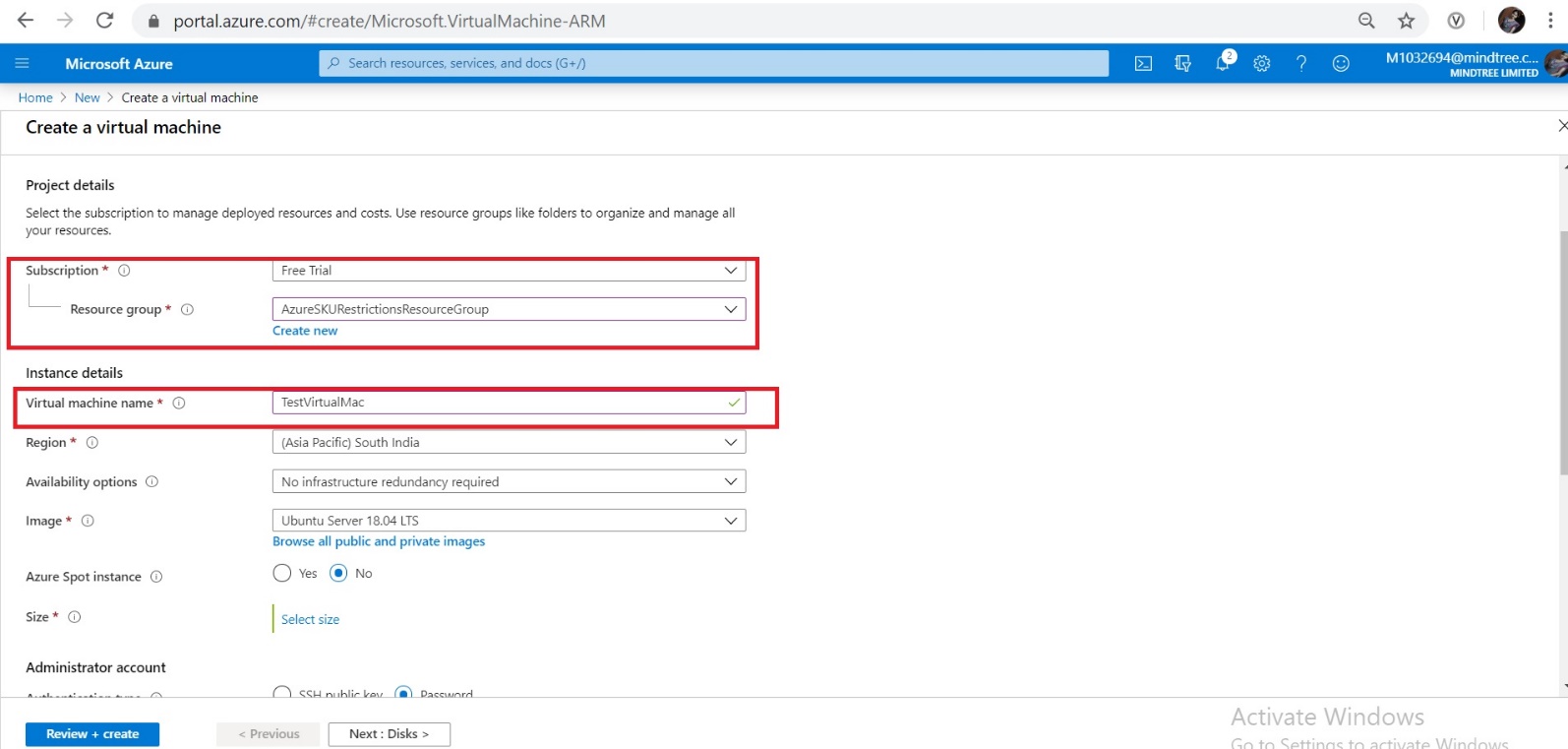


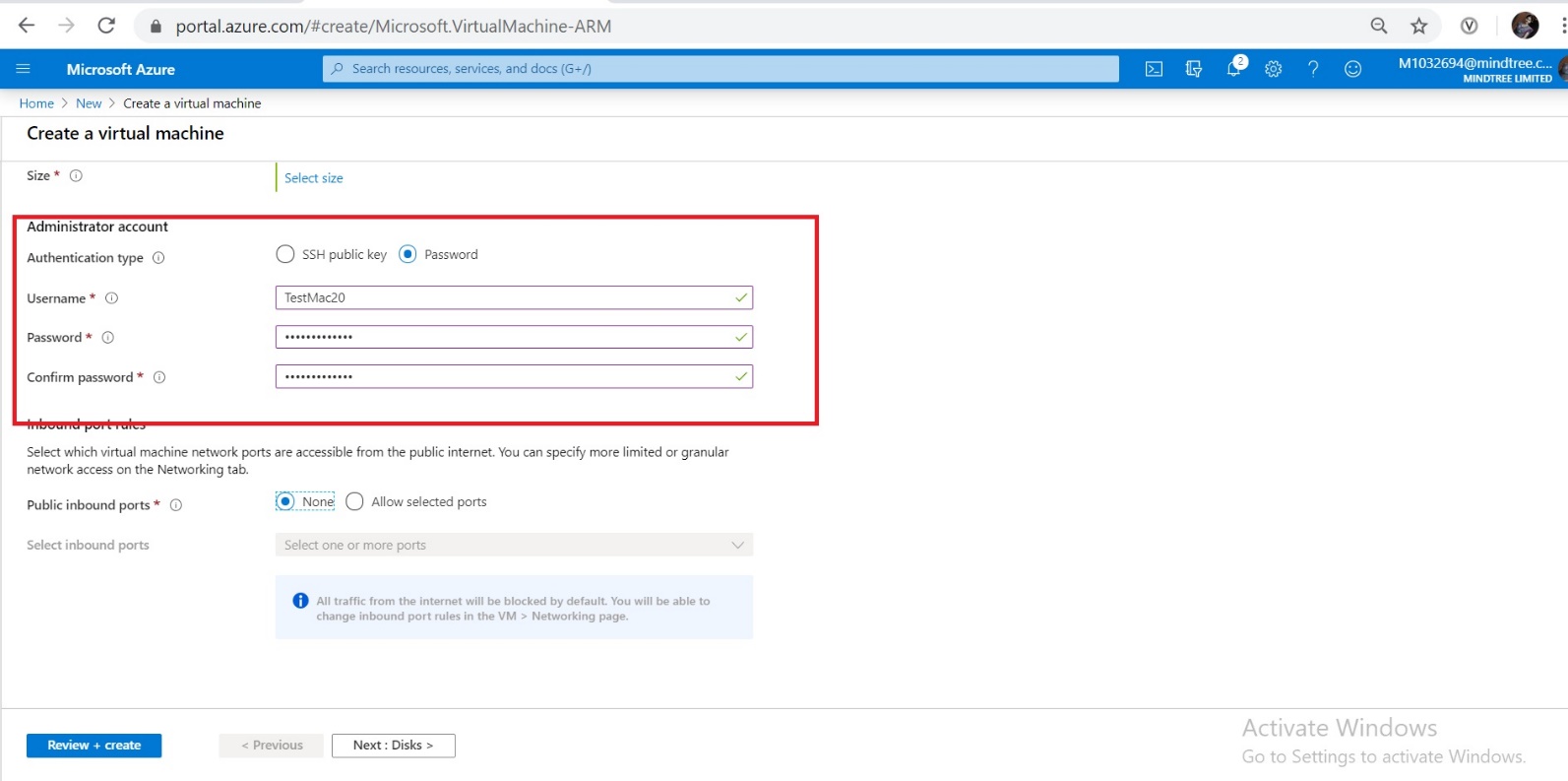


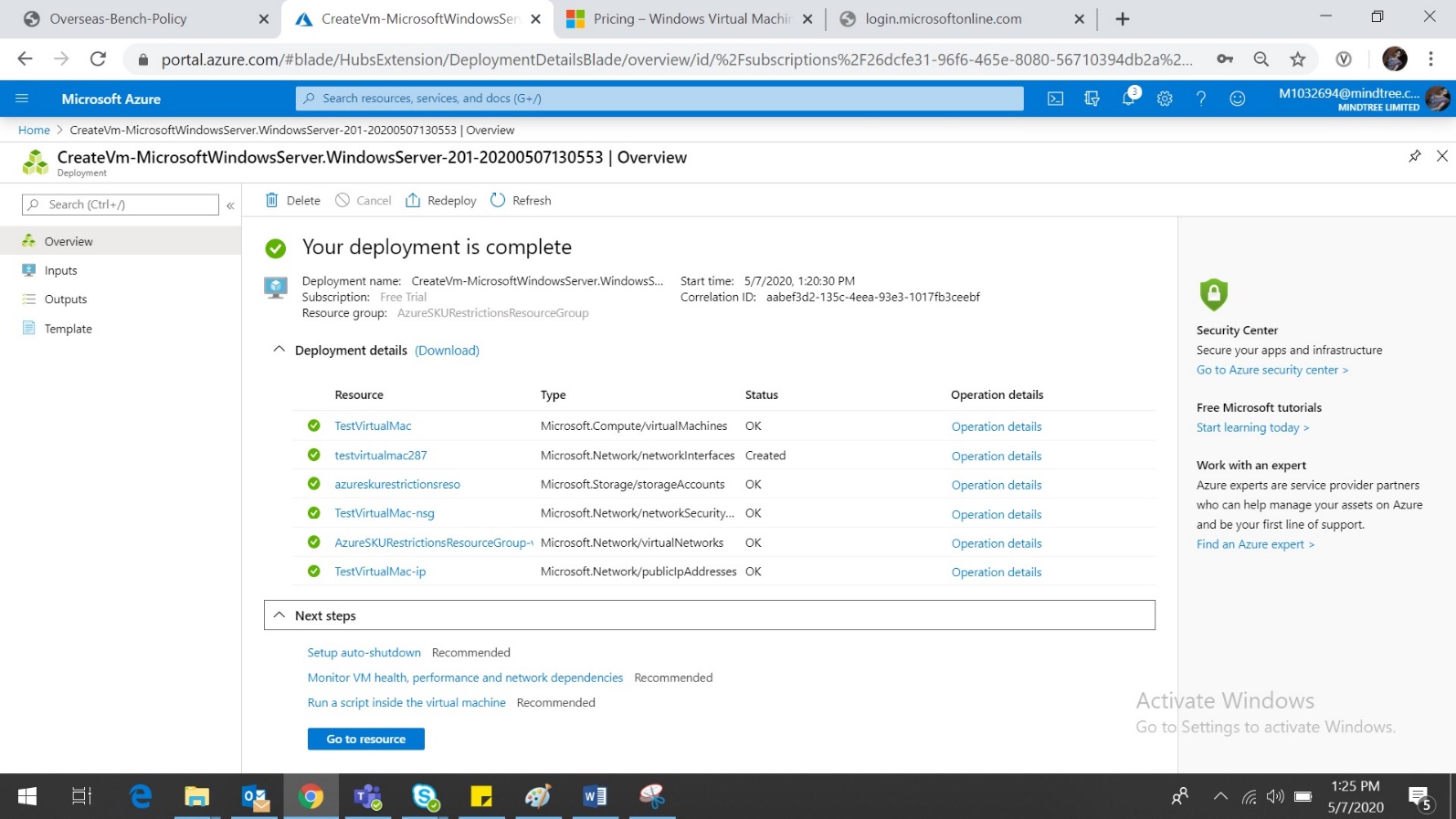


Below Screen shots show creating Virtual Machine









A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager)

We can filter the network traffic to and azure resources in azure network with a network security group. A network security group contains security rules that allow or deny inbound or outbound traffic from several types of azure resources.

Below is the Inbound and Outbound rules which I have created for my virtual network in the nework security group. I have enabled the http port to access the application deployed in the remote server. PFB the screenshots for the same.

Below are the credentials for the virtual machine, which I have created.

Public IP: 52.228.63.113

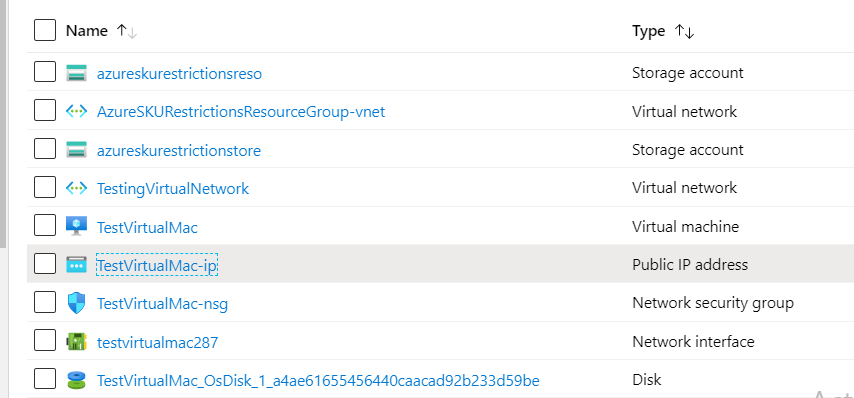
User name: TestMac20

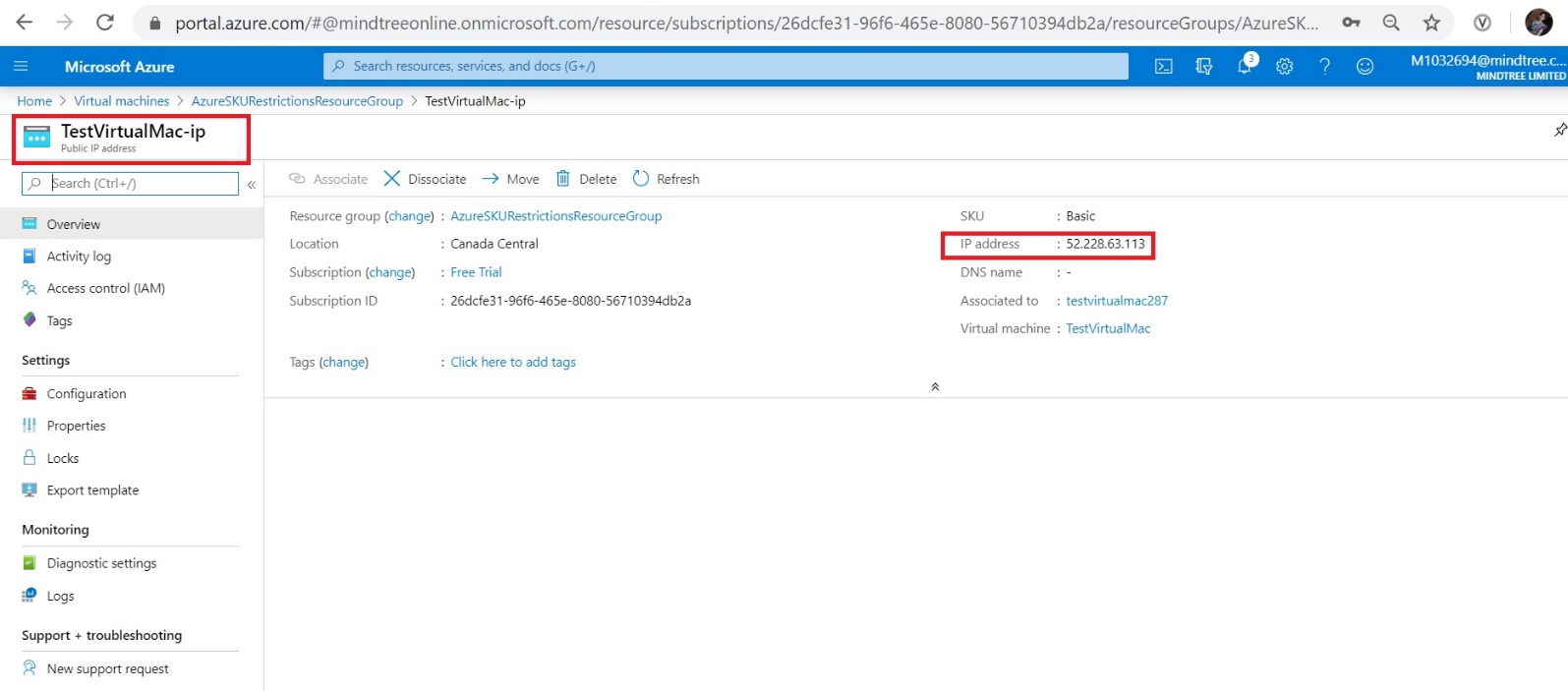
Password: Mahaarvi@2020

Allowed the traffic in port: 80(http)

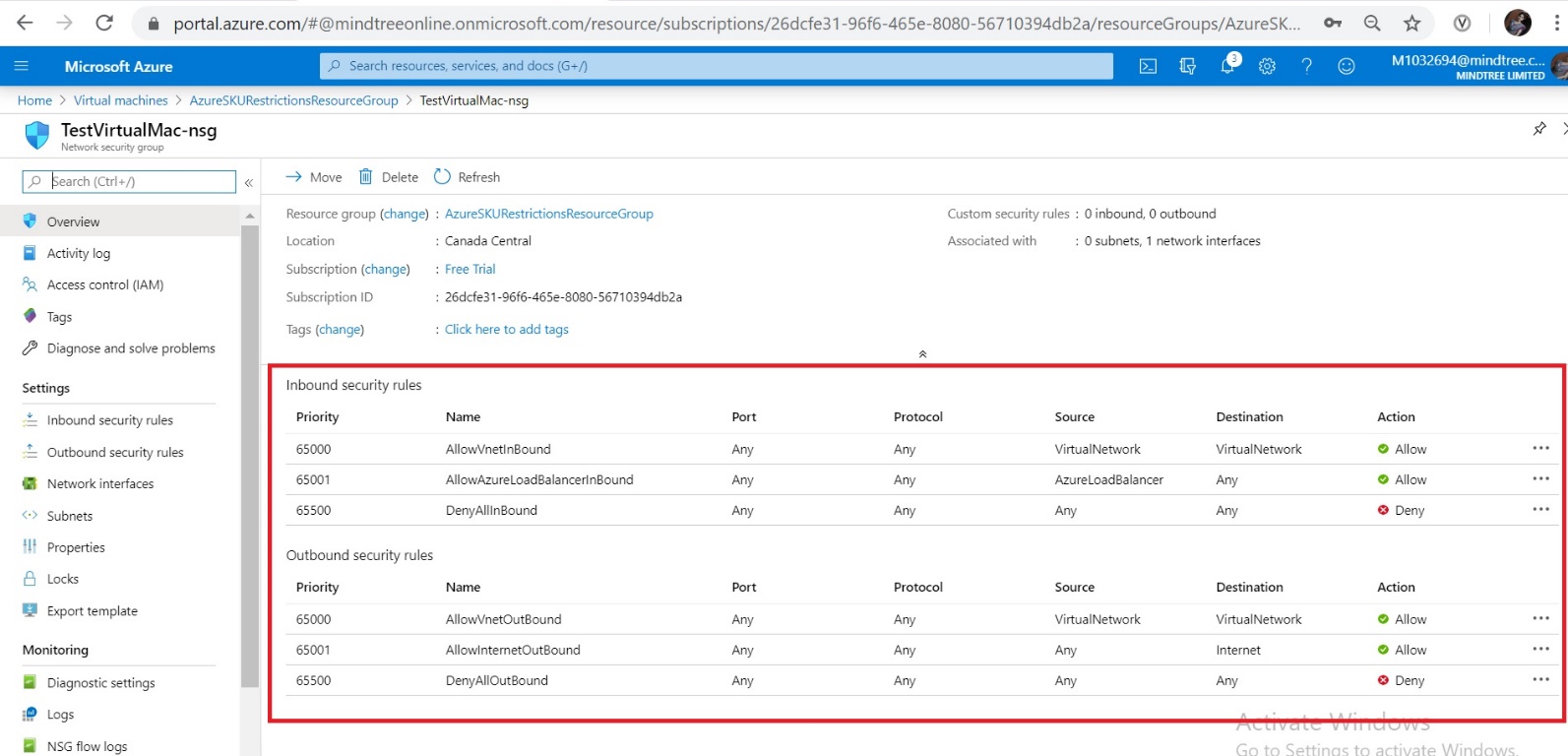
Denied the traffic in port: 443(https)

<http://52.228.63.113/helloworld.html> is the application, which is deployed in virtual machine.





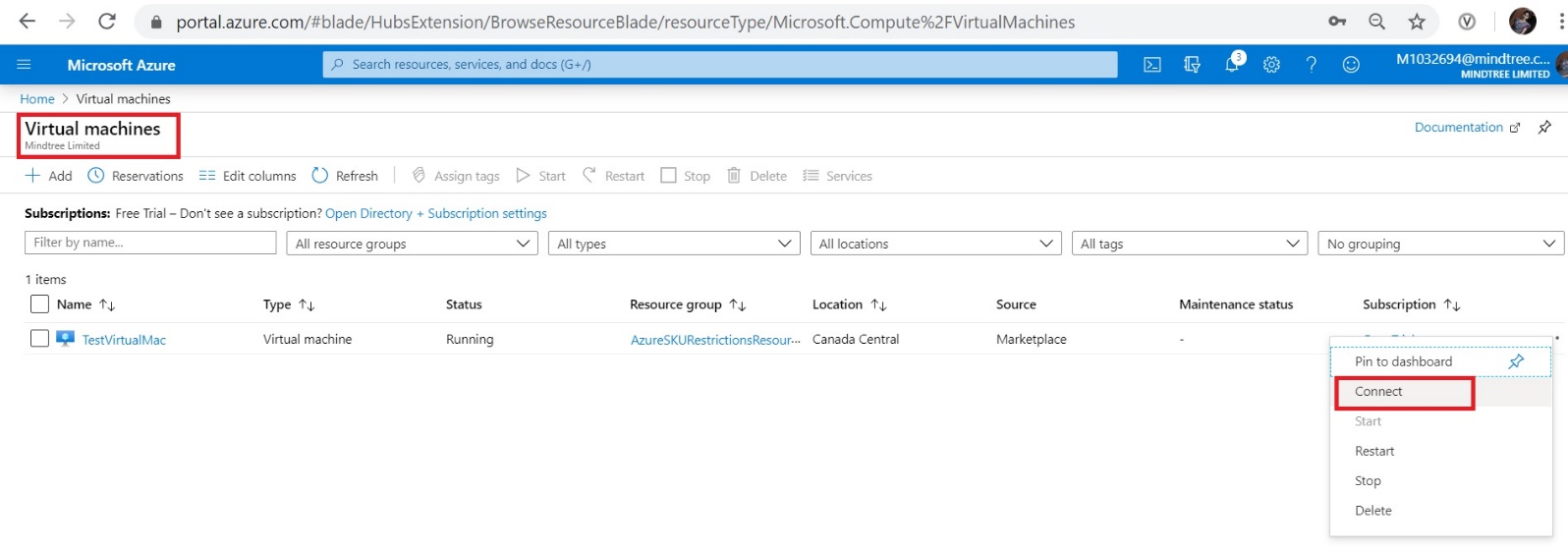
Inbound and out rules:



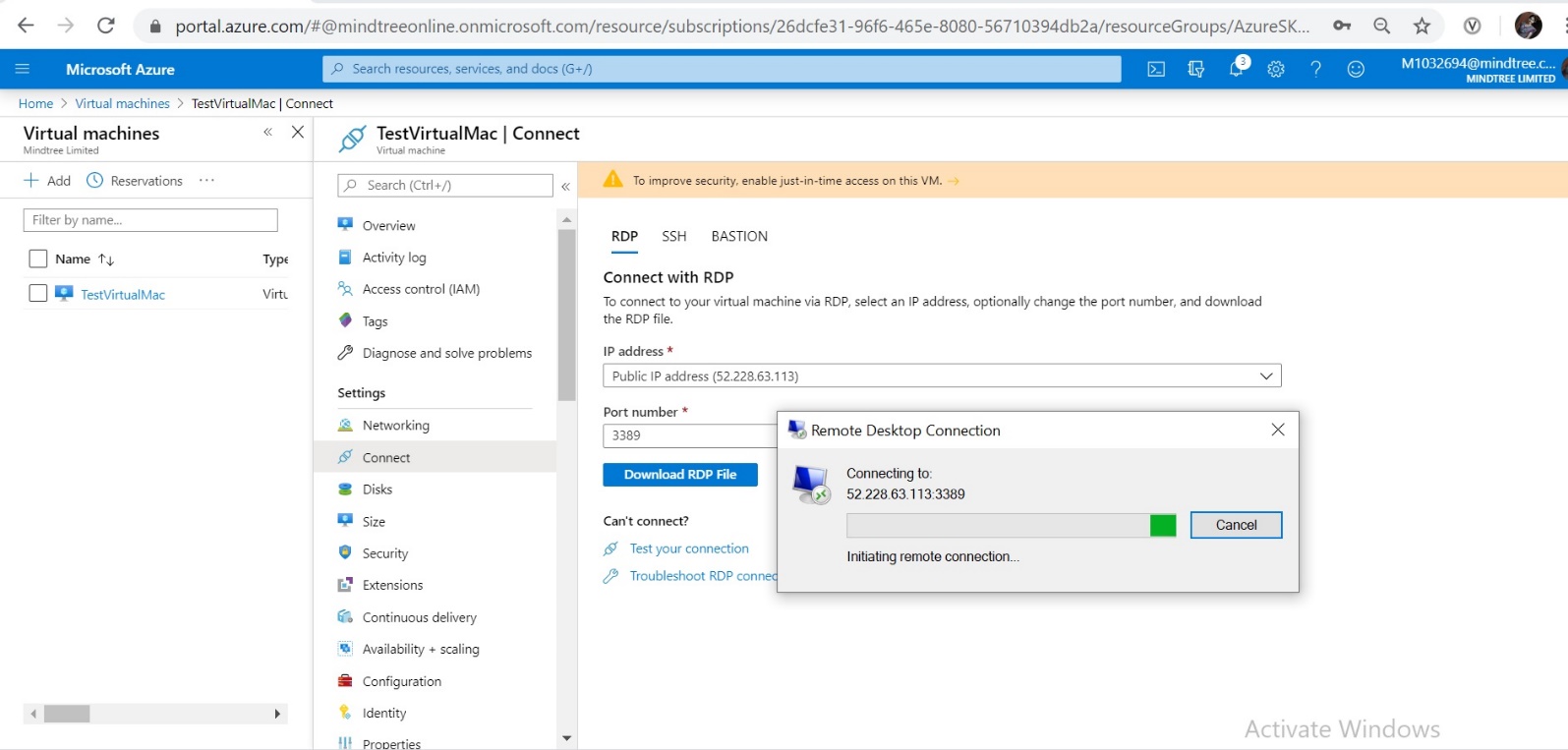
Configured II S in the remote machine and deployed the application. PFB screenshots.

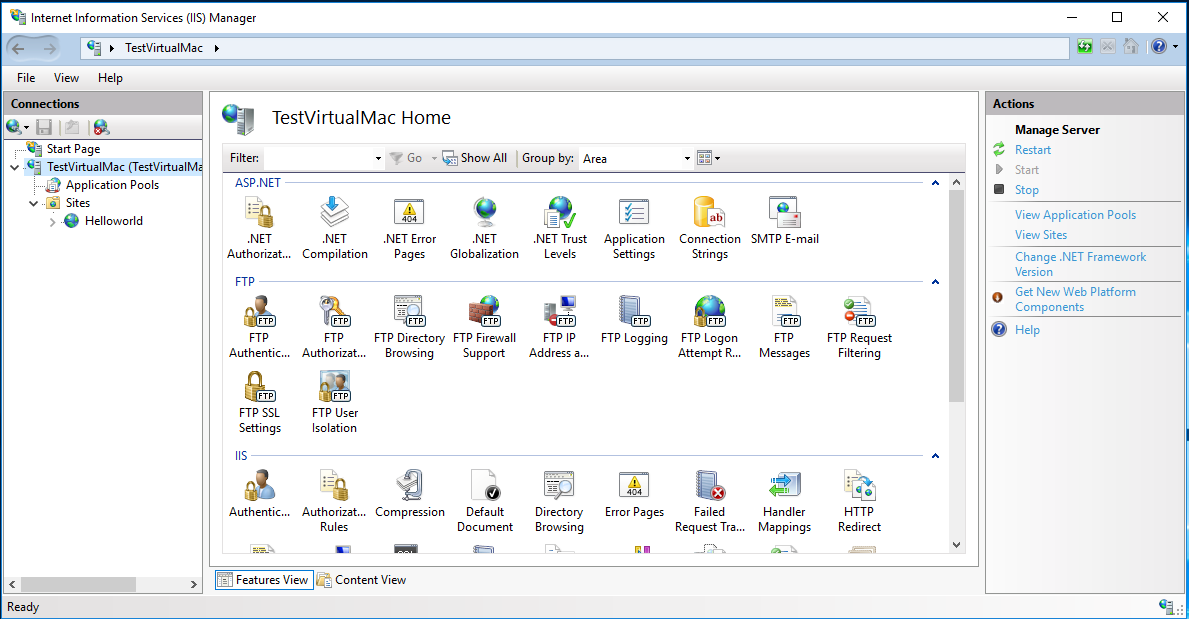
<http://52.228.63.113/helloworld.html> is the application, which deployed in virtual machine.

Go to virtual machine, right click on virtual machine which is required to connect and select the connect option from the popup



Once we click on connect will get an RDP file, Please double click on that file and enter you credentials to login to your Virtual machine and then deploy application. Below screen shots shows the same





<http://52.228.63.113/helloworld.html>

