

## Module 2: Azure Virtual Machines And Networking

---

### Demo 5

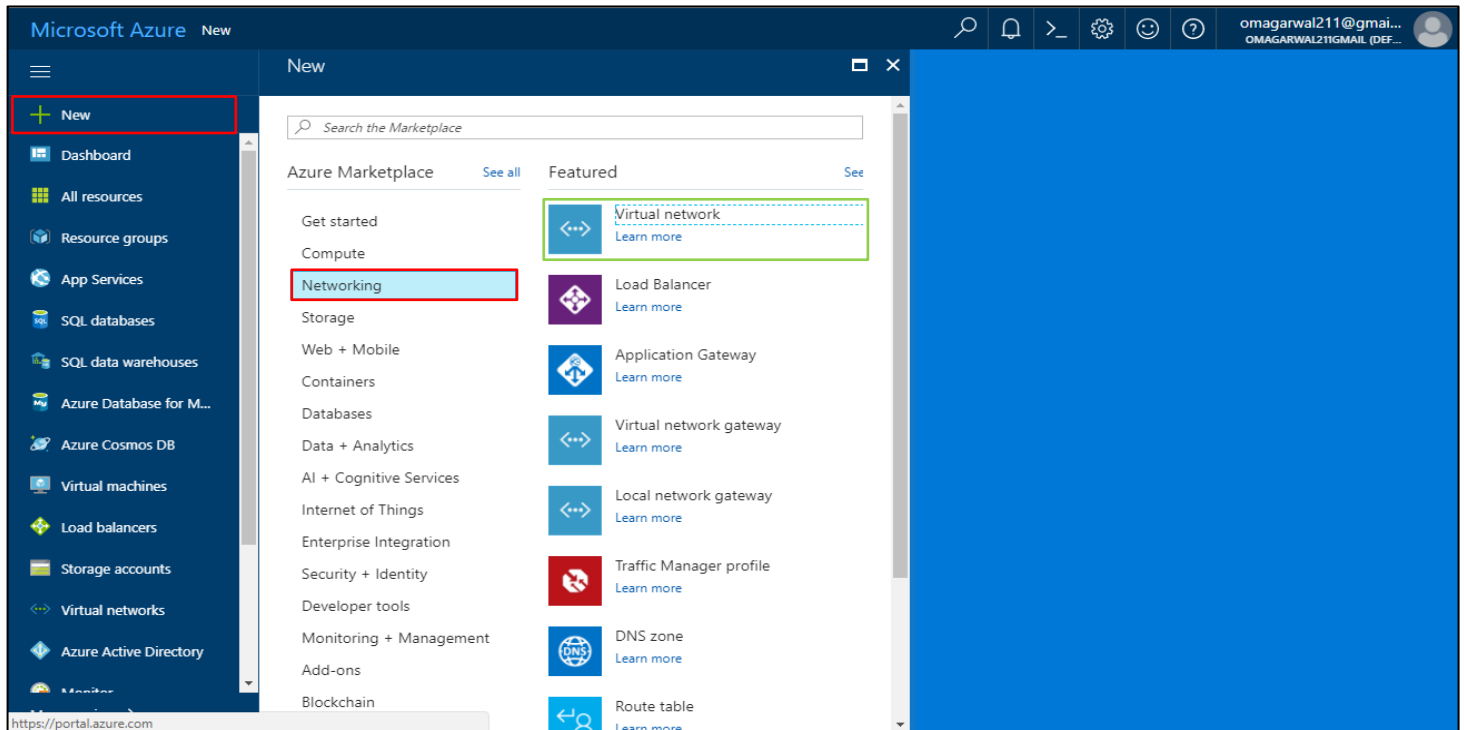
edureka!

**edureka!**

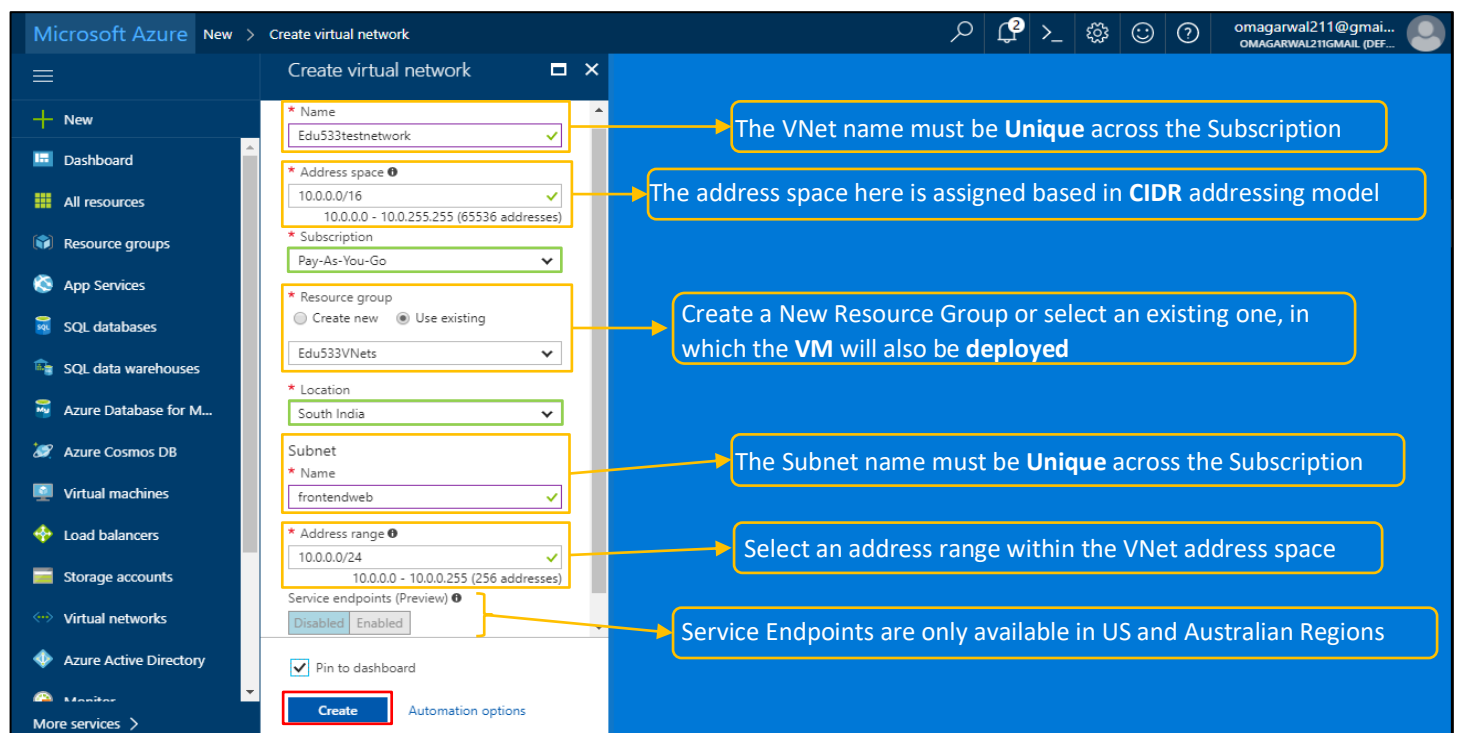
## Demo 5 – Configure Azure Networking

### 1. Create Virtual Network:

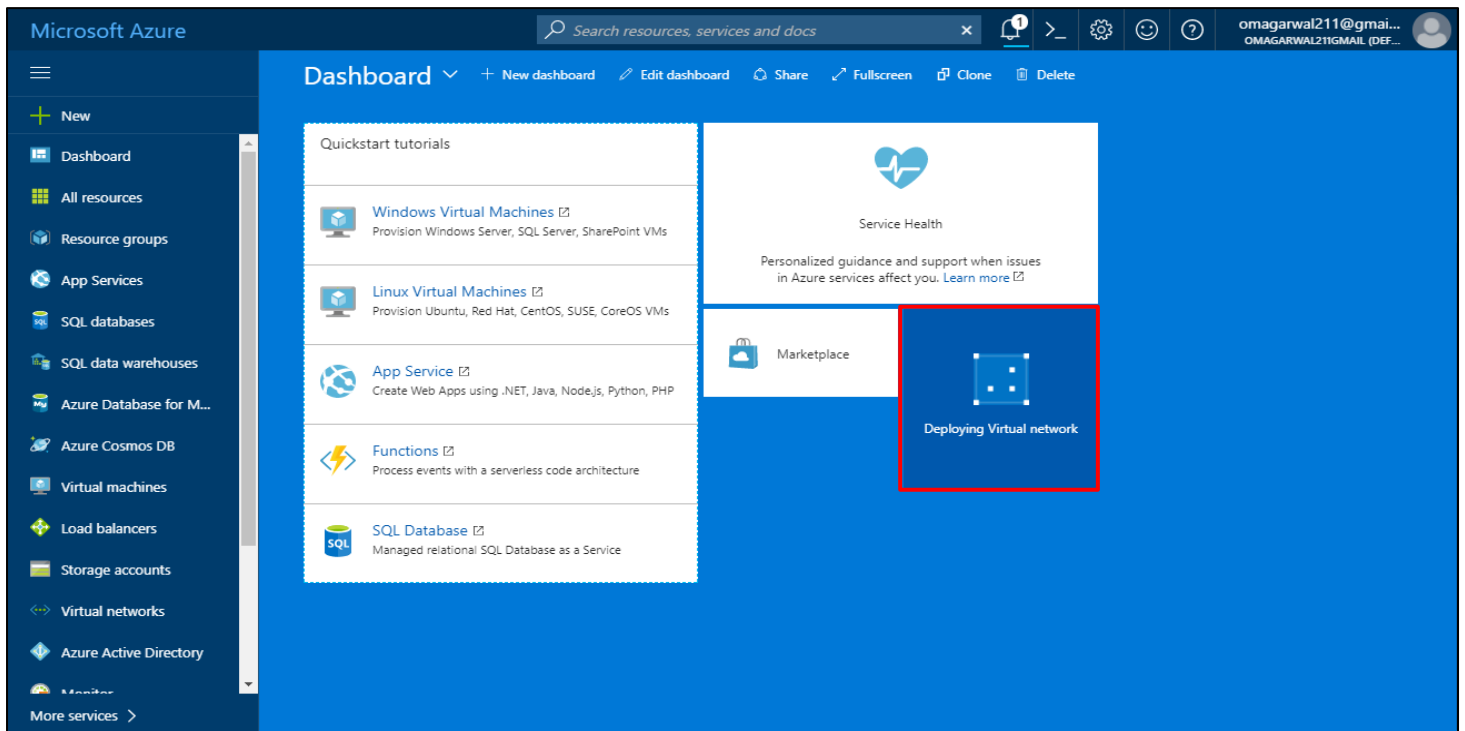
**Step 1:** In the Portal, Goto: +New > Networking > Click on **Virtual Network**:



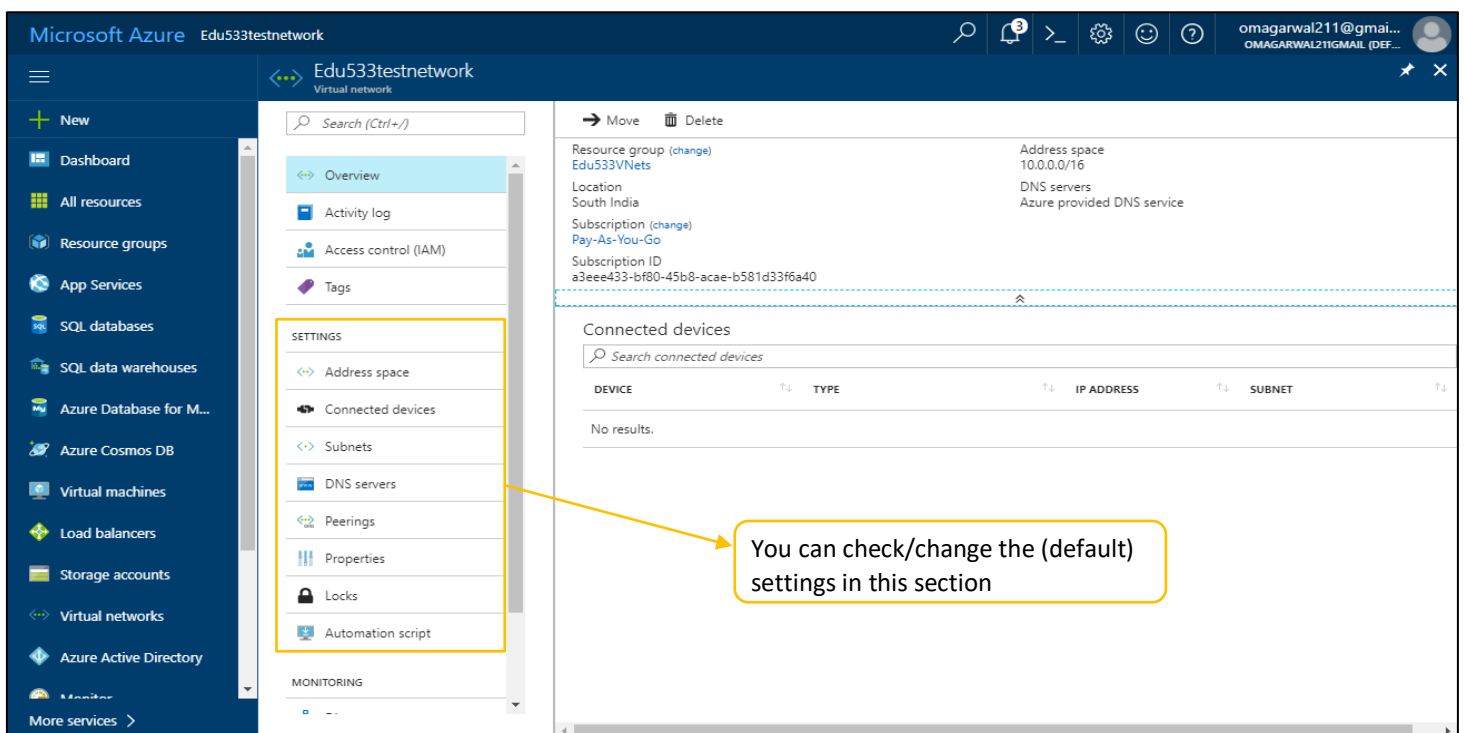
**Step 2:** In the Virtual Network blade, fill the details as shown below and Click **Create** :



**Step 3:** Once you click on Create, your VNet deployment progress is displayed on the dashboard:

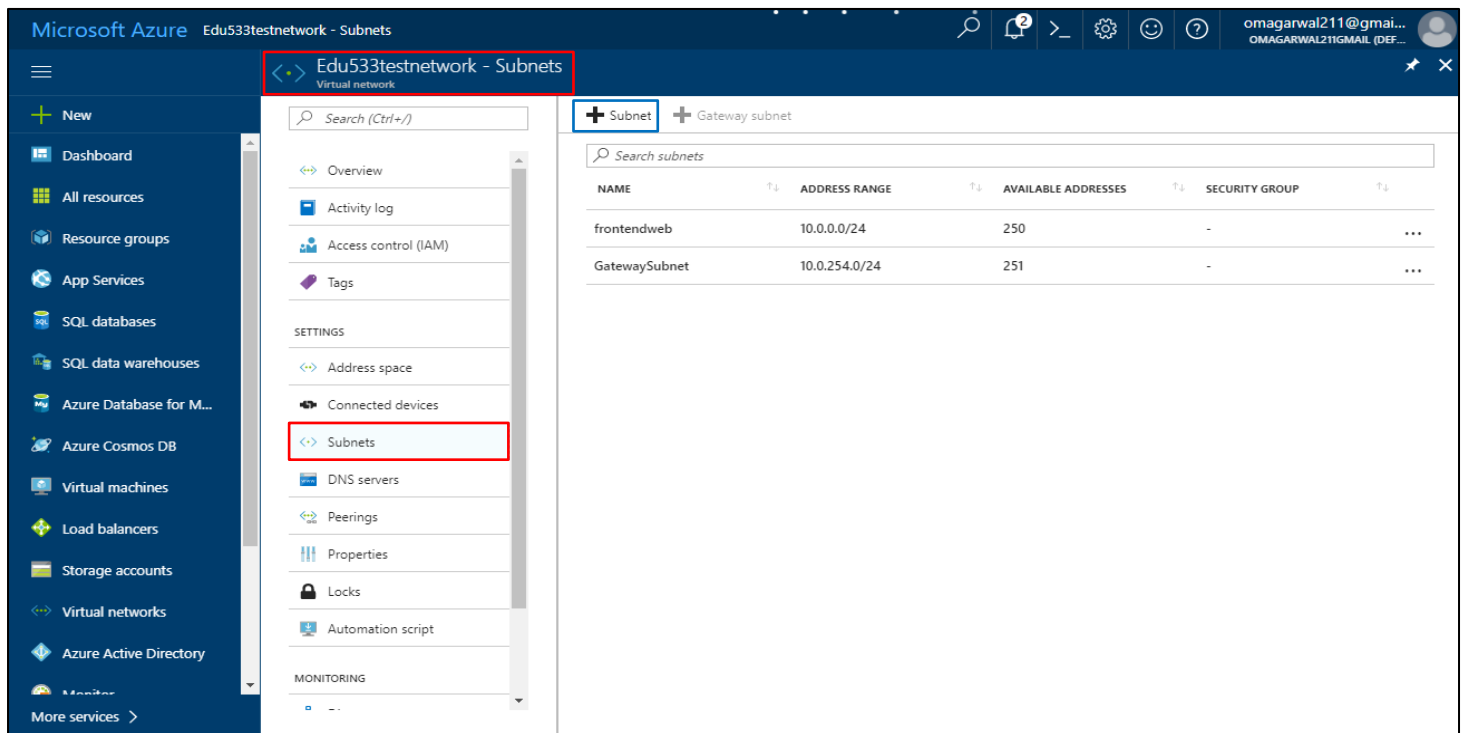


**Step 4:** Once deployed, an overview window of your VNet will be displayed:

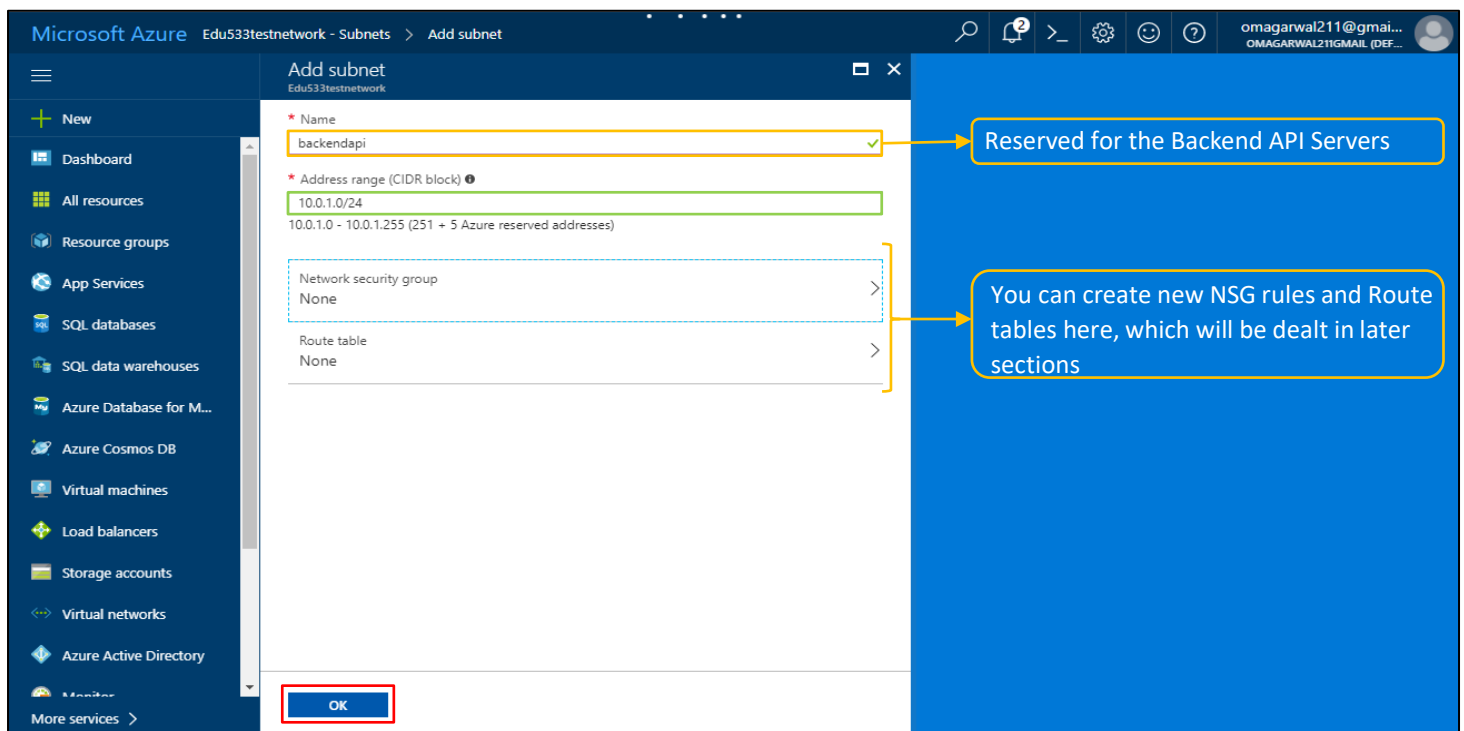


## 2. Configure Subnets:

**Step 1:** In the Virtual Network window, Goto: Subnets > **+Subnet** to create a new Subnet:



**Step 2:** Once you click on the +Subnet, configure the subnet as shown below:



Step 3: The main purpose of the subnet is Security such as the below scenario:

Microsoft Azure

Edu533testnetwork - Subnets

omagarwal211@gmail...  
OMAGARWAL211GMAIL (DEF...

New

Dashboard

All resources

Resource groups

App Services

SQL databases

SQL data warehouses

Azure Database for M...

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

More services >

Edu533testnetwork - Subnets

Virtual network

Overview

Activity log

Access control (IAM)

Tags

SETTINGS

Address space

Connected devices

Subnets

DNS servers

Peerings

Properties

Locks

Automation script

MONITORING

+ Subnet

+ Gateway subnet

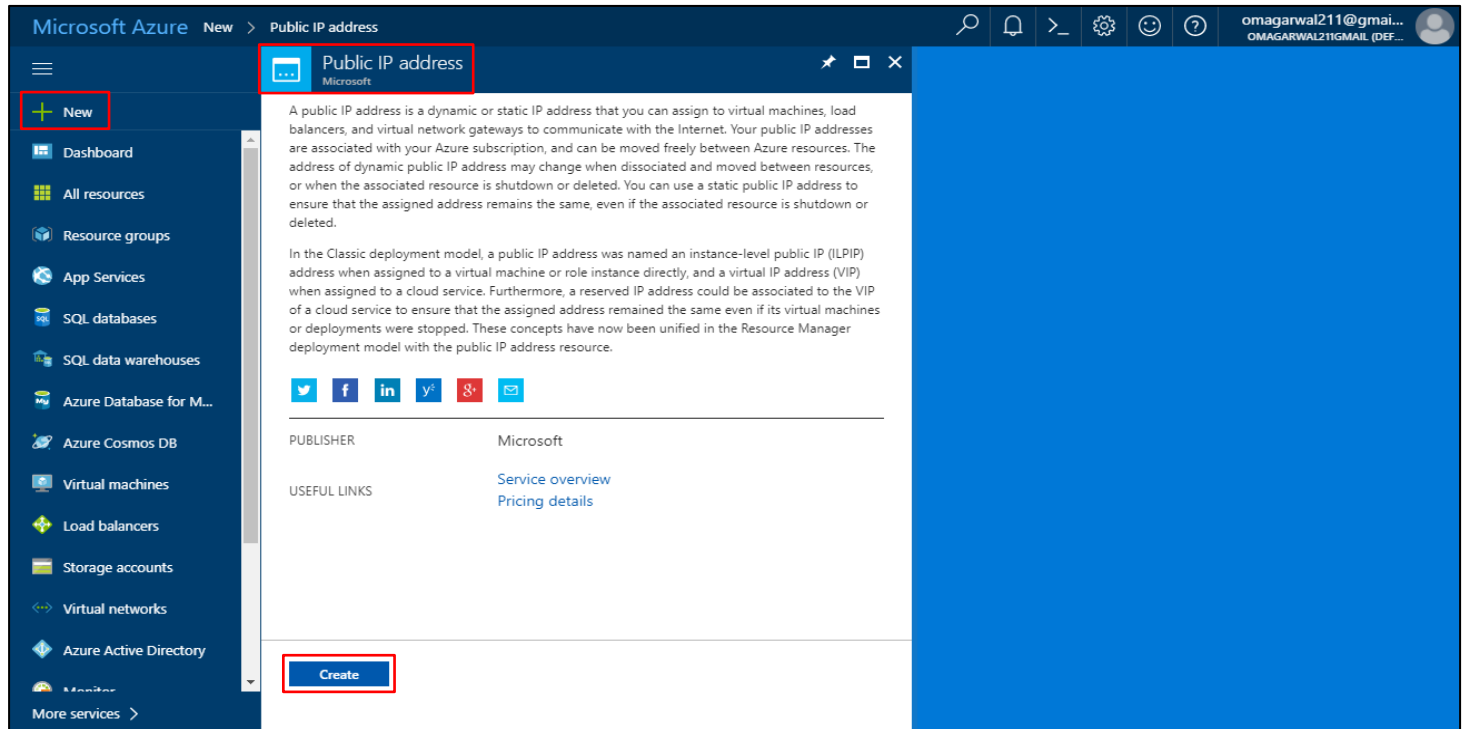
Search subnets

NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
frontendweb	10.0.0.0/24	250	-
GatewaySubnet	10.0.254.0/24	251	-
backendapi	10.0.1.0/24	251	-

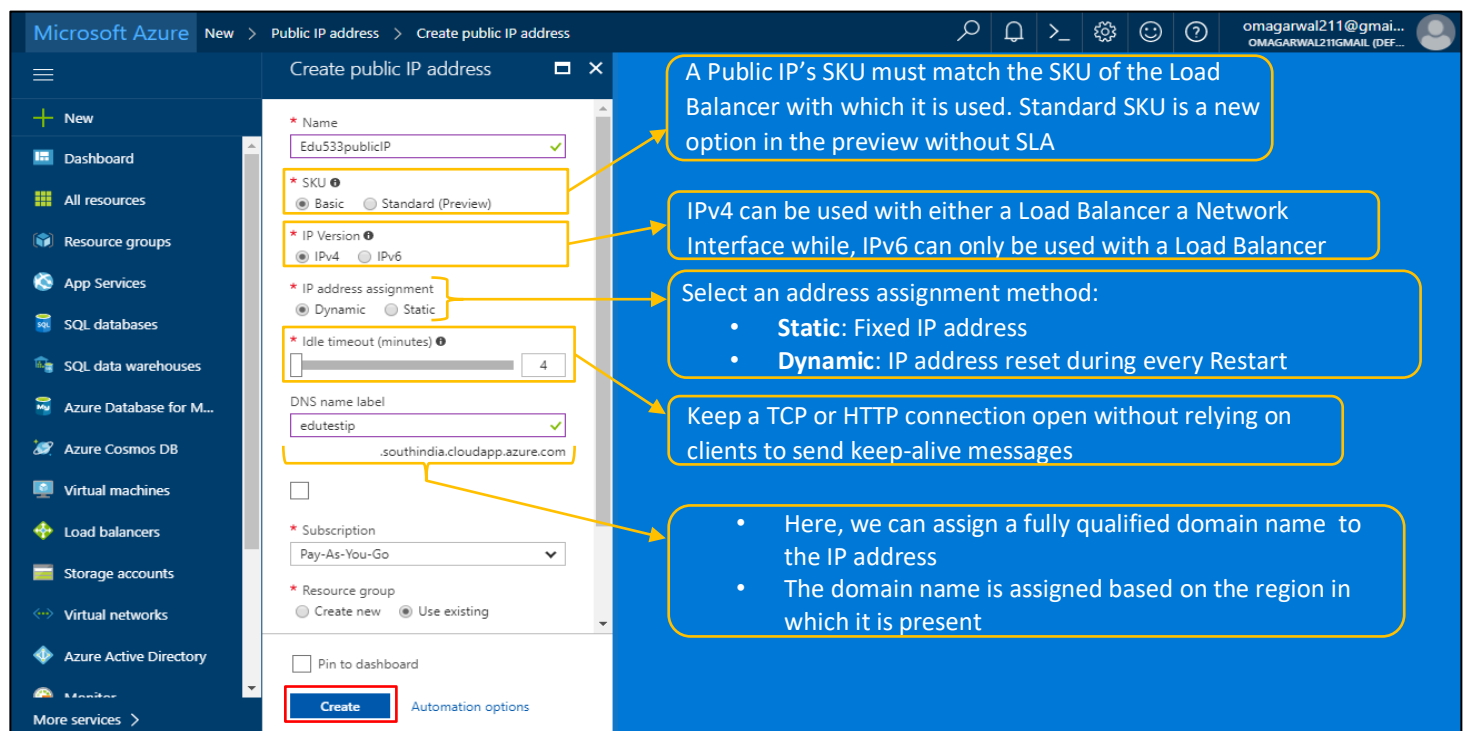
The Public internet traffic that is allowed in the **frontend** web address space but the same can be stopped to flow into the **backend** network space

### 3. Configure Static, Public and Private IP Addresses:

**Step 1:** In the Portal, Goto: +New > Search for **Public IP Address** > Click on **Create**:

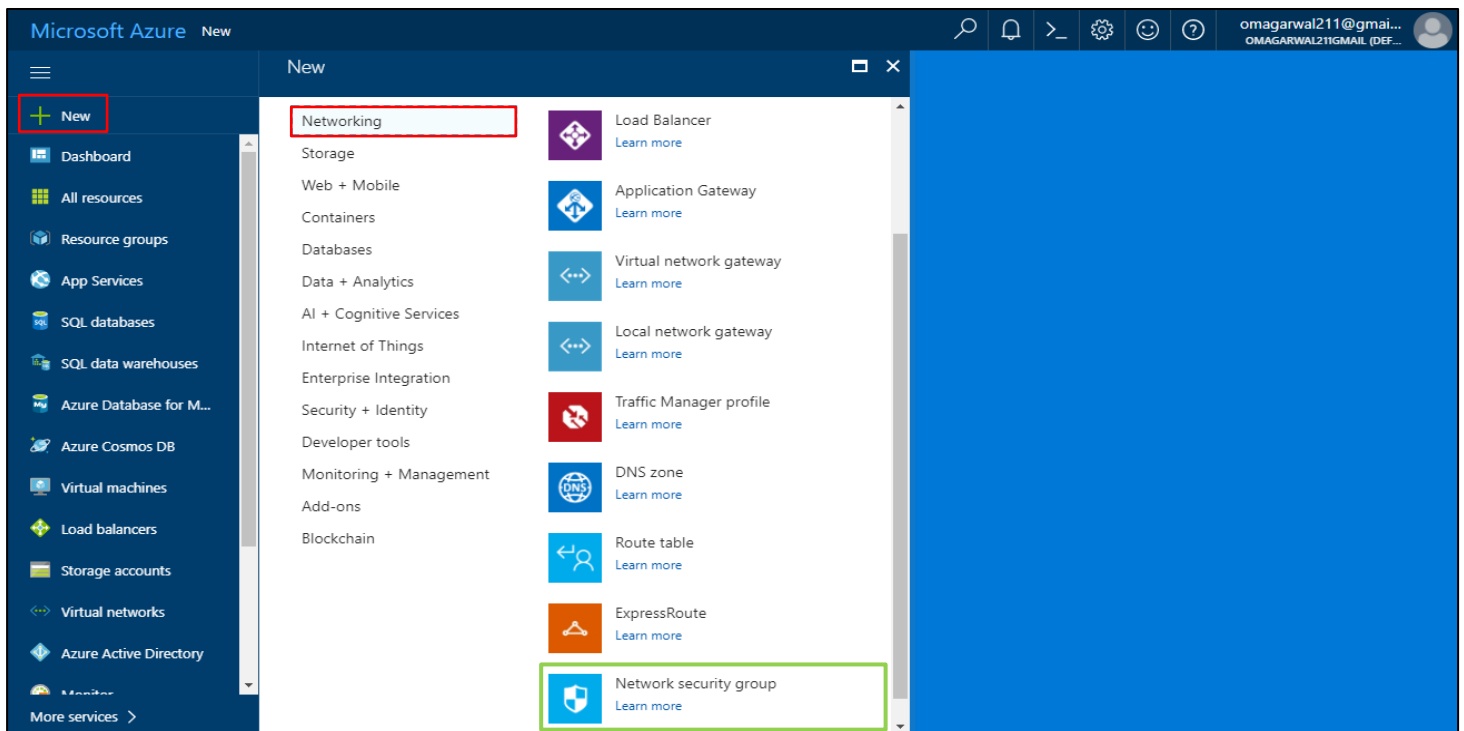


**Step 2:** Once you click Create, configure the Public IP address as shown below on the blade:

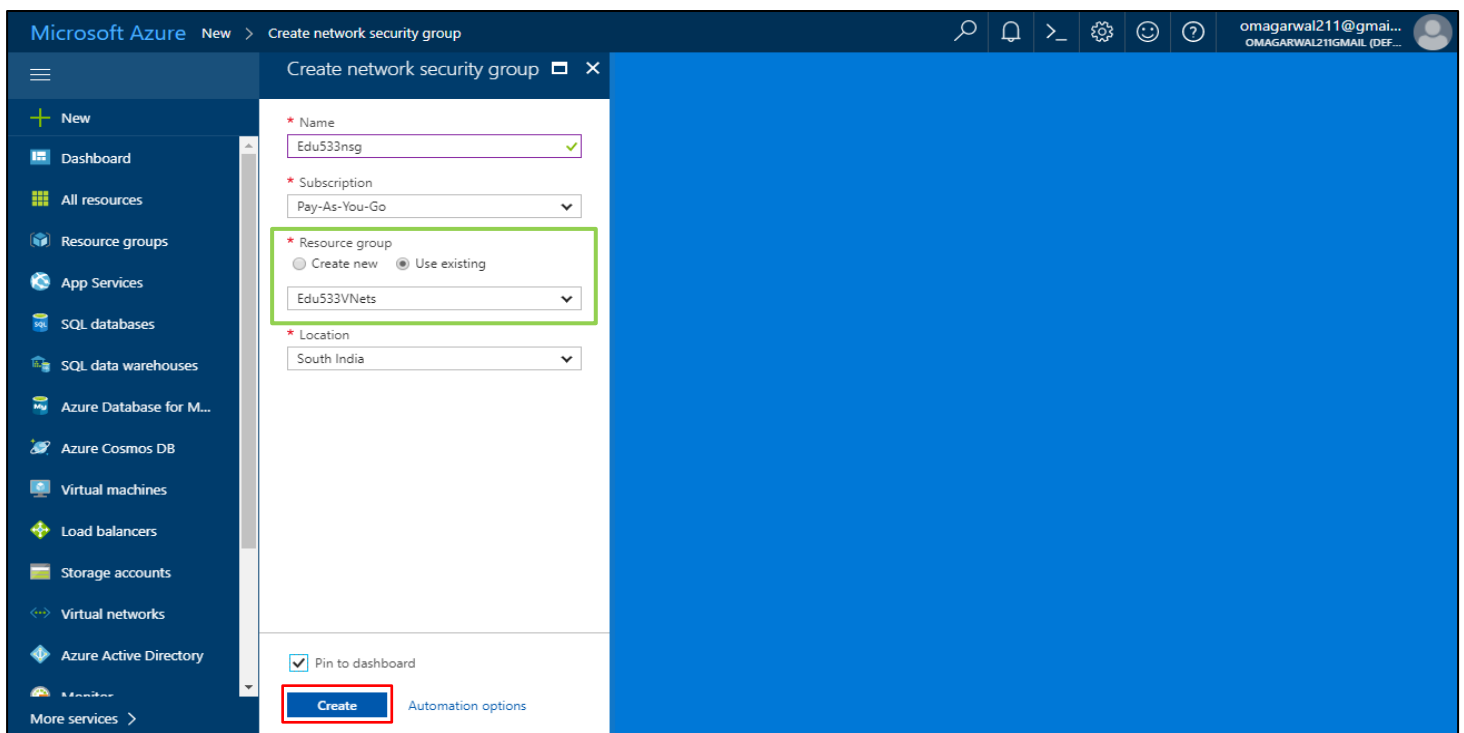


#### 4. Setup Network Security Groups (NSGs):

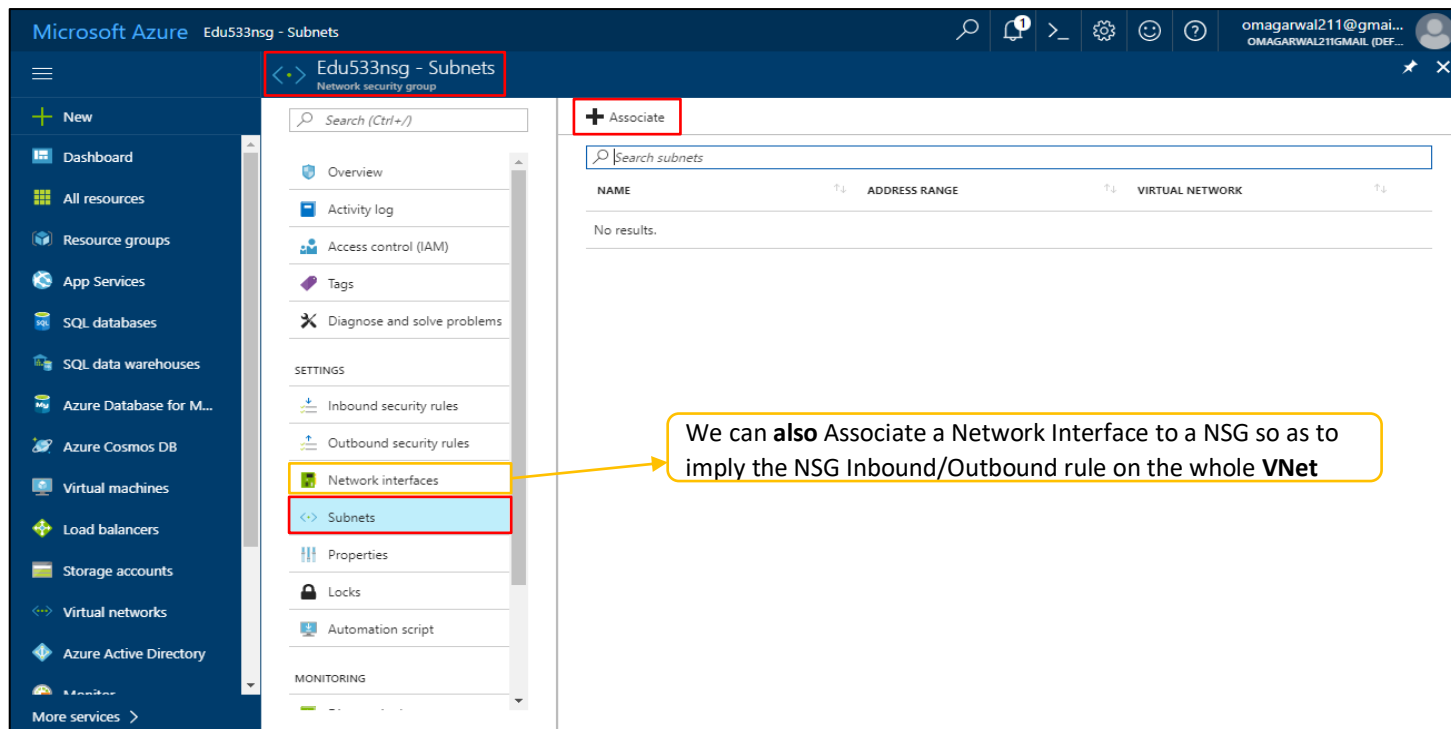
**Step 1:** In the Portal, Goto: **+New** > Networking > Click on **Networking Security Group**:



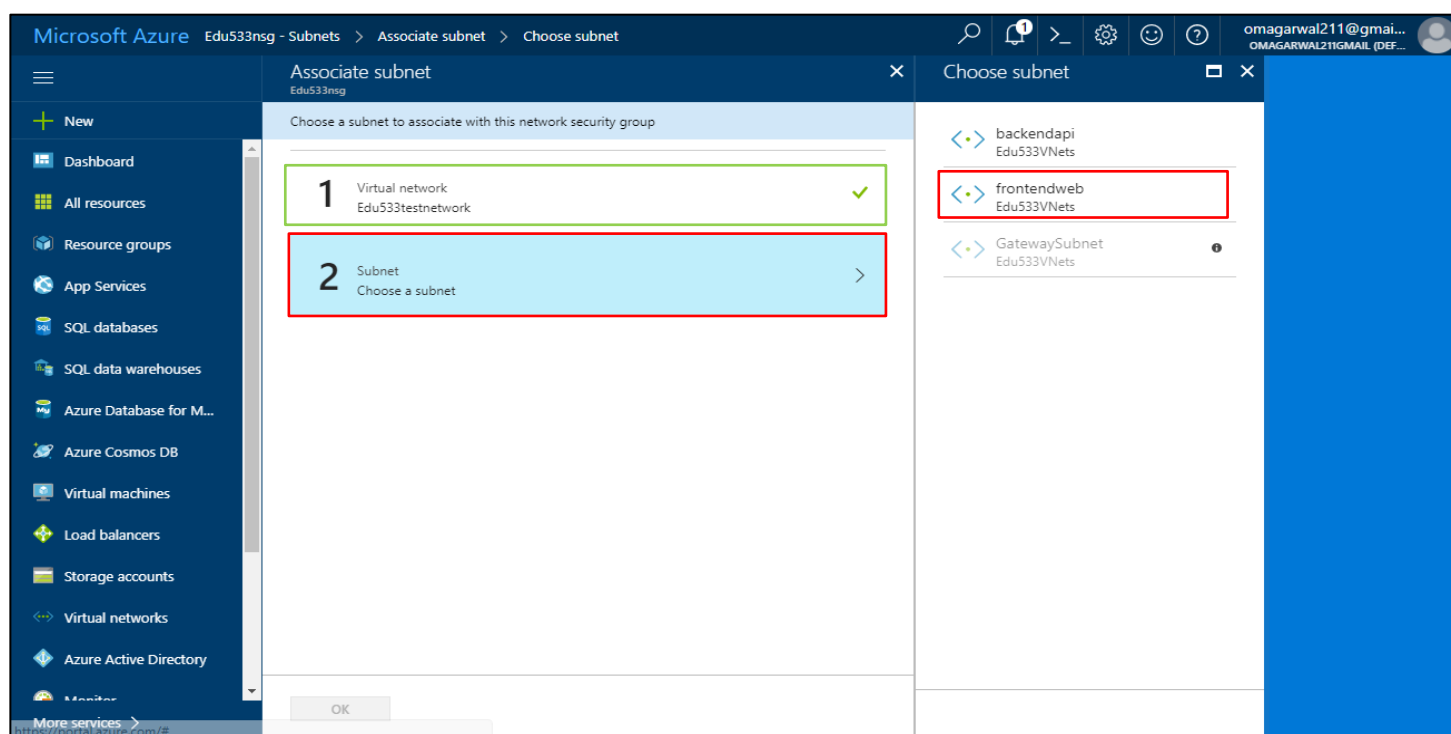
**Step 2:** Once you click on NSG, add the NSG to a Resource Group as shown below and click **Create**:



**Step 3:** In the NSG window, Select **Subnets** in the menu > Click on **+Associate** to select a subnet:



**Step 4:** In the +Associate blade, Select Virtual Network in which the Subnet is present > Click on desired **Subnet** > **OK**:





**Step 5:** Once you associate the Subnet, Click on the **Inbound Rules** in the menu to configure them:

The screenshot shows the 'Inbound security rules' configuration page for a Network Security Group (NSG) named 'Edu533nsg'. The 'Default rules' tab is selected, displaying a table of rules. A yellow box highlights the first three rules, and a yellow arrow points from this box to a callout box containing three points.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBala...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

1. Traffic from a **different** VNet to the Current VNet is **allowed**

2. Traffic from the **Azure Load Balancer** to the current subnet is **allowed**

3. Traffic from the **Public Internet** is **not** allowed

**Step 6:** To create an Inbound Security rule specifically for the HTTP traffic, Click on **+Add** in Inbound Security rules blade:

The screenshot shows the 'Inbound security rules' configuration page for a Network Security Group (NSG) named 'Edu533nsg'. The '+ Add' button is highlighted with a red box, indicating the next step in the process.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBala...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

**Step 7:** Once you click **+Add**, configure the rule as shown below:

Microsoft Azure Edu533nsg - Inbound security rules > Add inbound security rule

Basic

\* Source Any

\* Source port range \*

\* Destination Any

\* Destination port range 80

\* Protocol Any TCP UDP

\* Action Allow Deny

\* Priority 100

\* Name WebTraffic

Description

OK

Specifies the incoming traffic from a specific source IP address range that will be allowed or denied in this rule

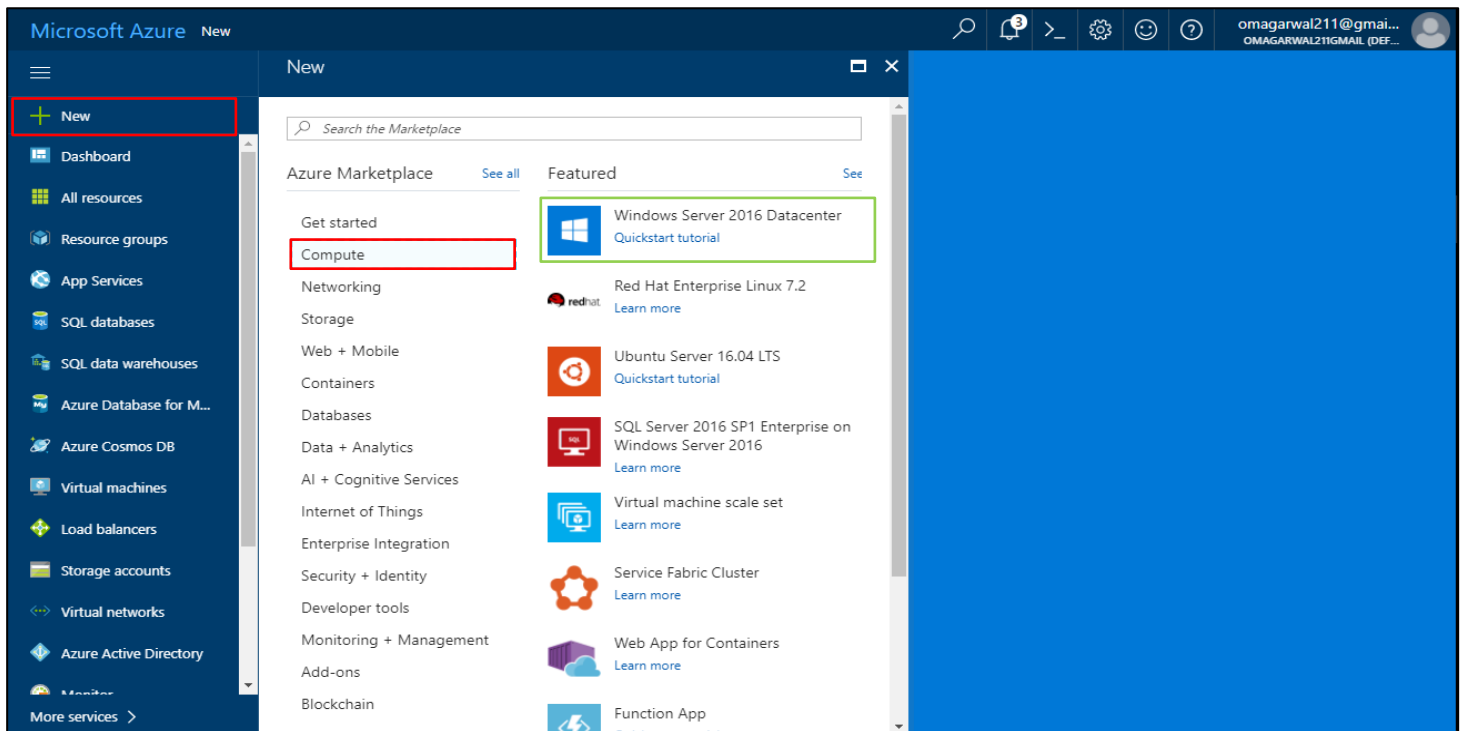
The Source Port range can be single a port, such as 80, or a port range, such as 1024-65535. Asterisk (\*) means from any port.

Lower the value, higher the priority. Leave gaps between rule- 100, 200, 300, etc, -so that its easier to add new rules without having to edit existing ones

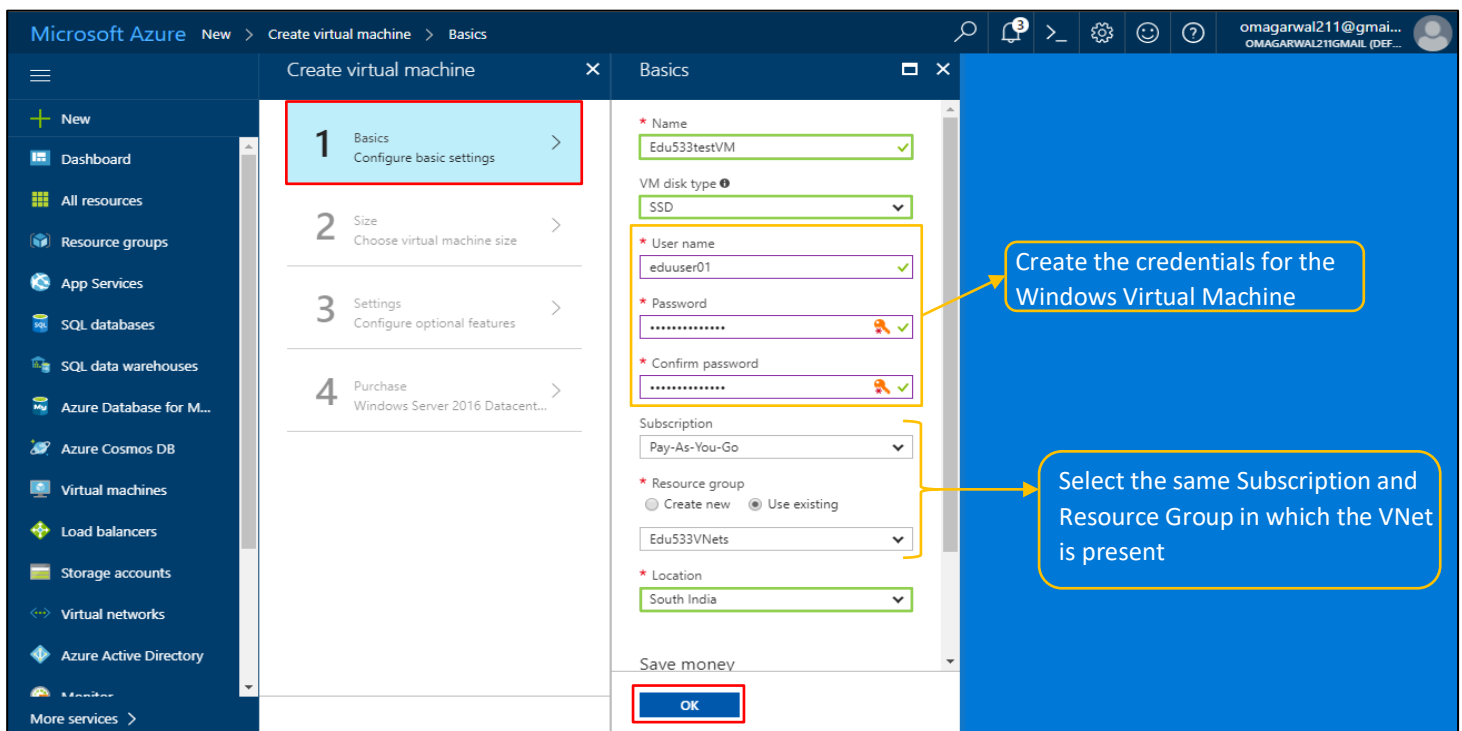
Similarly, you can associate both the inbound/out bound rules to the Backend APIs too

## 5. Onboard a VM to the configured VNet:

**Step 1:** In the Portal, Goto: +New > Compute > Click on **Windows Server 2016 Datacenter**



**Step 2:** Once you click on the Windows VM, fill up the details in the prompted window as shown below and Click **OK**:



**Step 3:** Once you click OK, you will move on to the next blade where you **Select** your desired **VM disk size**:

Microsoft Azure New > Create virtual machine > Choose a size

Create virtual machine

- 1 Basics Done
- 2 Size Choose virtual machine size
- 3 Settings Configure optional features
- 4 Purchase Windows Server 2016 Datacent...

Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

Supported disk type: SSD Minimum vCPUs: 1 Minimum memory (GiB): 0

DS1_V2 Standard	DS2_V2 Standard	DS11_V2 Standard
1 vCPU	2 vCPUs	14 vCPUs
3.5 GB	7 GB	14 GB
2 Data disks	4 Data disks	4 Data disks
3200 Max IOPS	6400 Max IOPS	6400 Max IOPS
7 GB Local SSD	14 GB Local SSD	28 GB Local SSD
Premium disk support	Premium disk support	Premium disk support
Load balancing	Load balancing	Load balancing
6,442.00 INR/MONTH (ESTIMATED)	12,834.83 INR/MONTH (ESTIMATED)	13,867.52 INR/MONTH (ESTIMATED)

Select

**Step 4:** Once you select VM disk, in the Setting blade, all the settings are selected automatically > Just Click **OK**:

Microsoft Azure New > Create virtual machine > Settings

Create virtual machine

- 1 Basics Done
- 2 Size Done
- 3 Settings Configure optional features
- 4 Purchase Windows Server 2016 Datacent...

High availability

- \* Availability set: None

Storage

- Use managed disks: No
- \* Storage account: (new) edu533vnetsdisks683

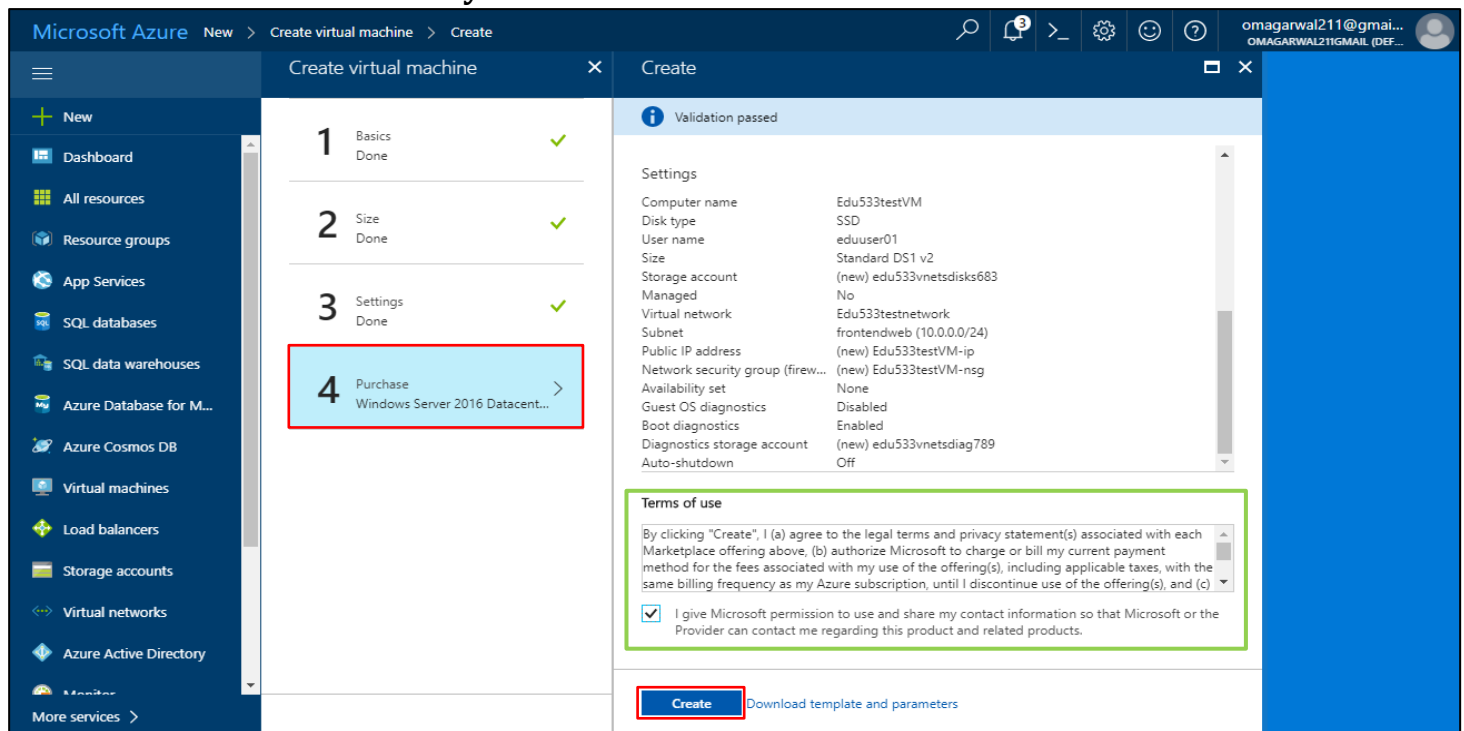
Network

- \* Virtual network: Edu533testnetwork
- \* Subnet: frontendweb (10.0.0.0/24)
- \* Public IP address: (new) Edu533testVM-ip
- \* Network security group (firewall): (new) Edu533testVM-nsg

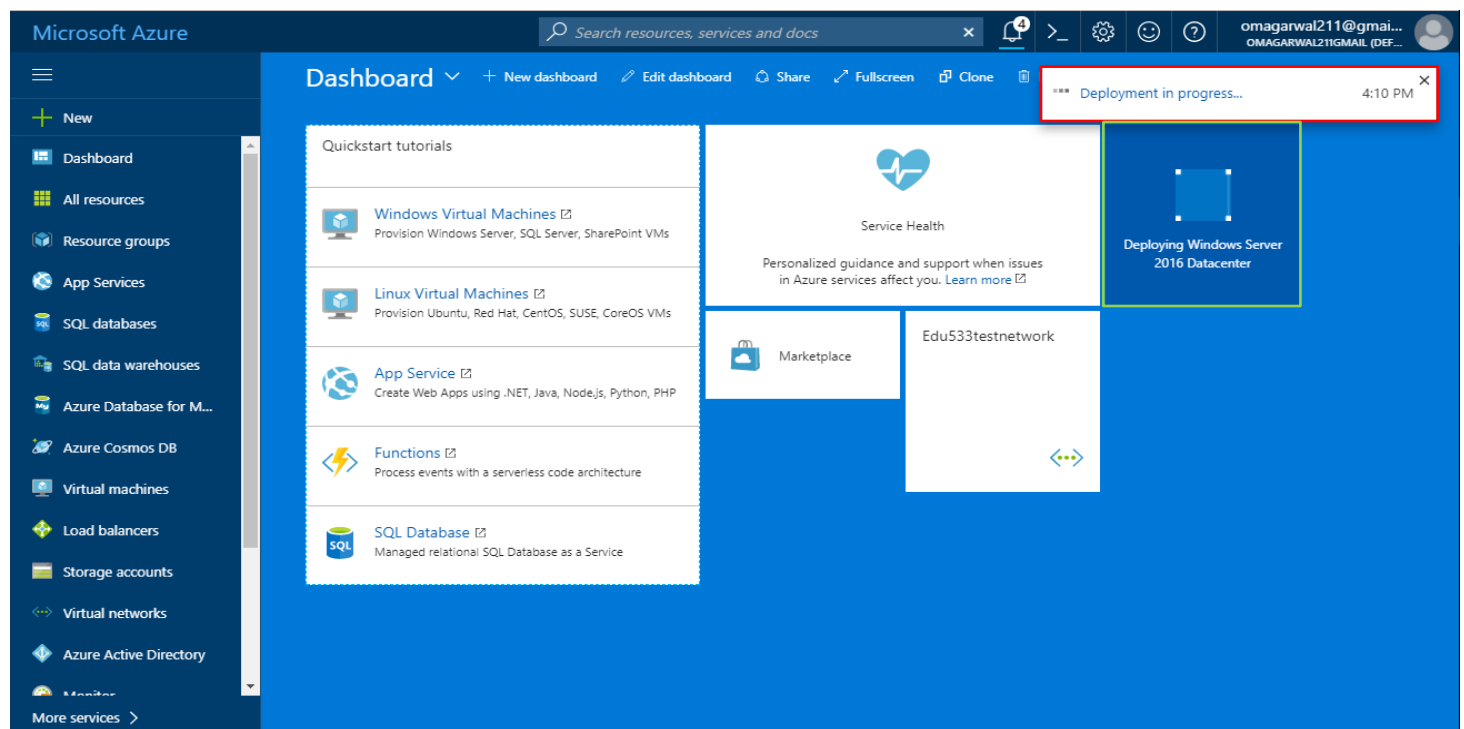
OK

The Virtual Network in which the VM is to be deployed

**Step 5:** After setting up the VM deployment, finalize the procedure in the **Purchase Summary** blade and Click **Create**:



**Step 6:** Once you click Create, you will be redirected to the Home page, where you can check the deployment status:



**Step 7:** Once deployed successfully, you can monitor the VM in the below shown window:

