



CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Harsh Tongariya

College: Arya College of Engineering Information
Technology

Domain: Cloud Infra & Security

Student ID: CT_CSI_CI_1160

Research & Development Document

In-Depth R&D on NSG, ASG, Public IP, and VM Networking in Azure

1. Network Security Group (NSG)

What is NSG?

- Think of NSG as a virtual firewall that controls traffic at Layer 3 & 4 (IP + TCP/UDP).
- It can be applied at:
 - Subnet level → Controls traffic for all VMs in the subnet.
 - NIC level → Controls traffic for specific VM.

NSG Rule Components:

Field	Description
Priority	100 (high) to 4096 (low). First match is applied
Name	Unique identifier for the rule
Source/Destination	IP address, CIDR, service tag, ASG
Protocol	TCP, UDP, or Any
Port range	e.g. 80, 3389, 22
Action	Allow or Deny
Direction	Inbound or Outbound

Default Rules in NSG:

Priority	Name	Direction	Source	Destination	Port	Action
65000	AllowVnetInBound	Inbound	VirtualNetwork	VirtualNetwork	Any	Allow
65001	AllowAzureLoadBalancerInBound	Inbound	AzureLoadBalancer	Any	Any	Allow
65500	DenyAllInBound	Inbound	Any	Any	Any	Deny
65000	AllowVnetOutBound	Outbound	VirtualNetwork	VirtualNetwork	Any	Allow
65001	AllowInternetOutBound	Outbound	Any	Internet	Any	Allow
65500	DenyAllOutBound	Outbound	Any	Any	Any	Deny

2. Application Security Group (ASG)

What is ASG?

- ASG groups VMs logically.
- Instead of writing rules for individual IPs → apply to ASG (e.g., all Web VMs).

Use case:

- You have Web-ASG (frontend VMs) & DB-ASG (backend VMs)
- NSG rule → Allow Web-ASG to talk to DB-ASG on port 1433 (SQL).
- Advantages:
 - Simplifies management as your app scales (add/remove VMs in ASG, no NSG update needed).
 - Dynamic security for microservices architecture.

3. Allow Specific IPs + Deny Internet

Scenario: Allow your office IP 203.0.113.10 → Deny all else

Example NSG Inbound Rules:

Priority	Source	Port	Protocol	Action
100	203.0.113.10/32	3389	TCP	Allow
200	Any	3389	TCP	Deny

Example NSG Outbound Rules (Block Internet):

Priority	Destination	Port	Protocol	Action
100	Internet	Any	Any	Deny
200	VirtualNetwork	Any	Any	Allow

4. Public IP Types

Type	When Assigned	IP Changes?	Example Use Case
Dynamic	On VM start	Yes	Dev/test VMs
Static	Reserved	No	DNS mappings, production endpoints

SKU:

- Basic → No zone resiliency, open unless NSG denies
- Standard → Secure by default, zone-aware

5. Service Tags

Pre-defined tags representing Azure IP ranges.

Examples:

Tag	Represents
Internet	All public IP addresses
VirtualNetwork	All VMs in the same VNet
AzureLoadBalancer	IPs of Azure LB
Storage, SQL	Azure service endpoints

6. Allocate Static IPs to VMs

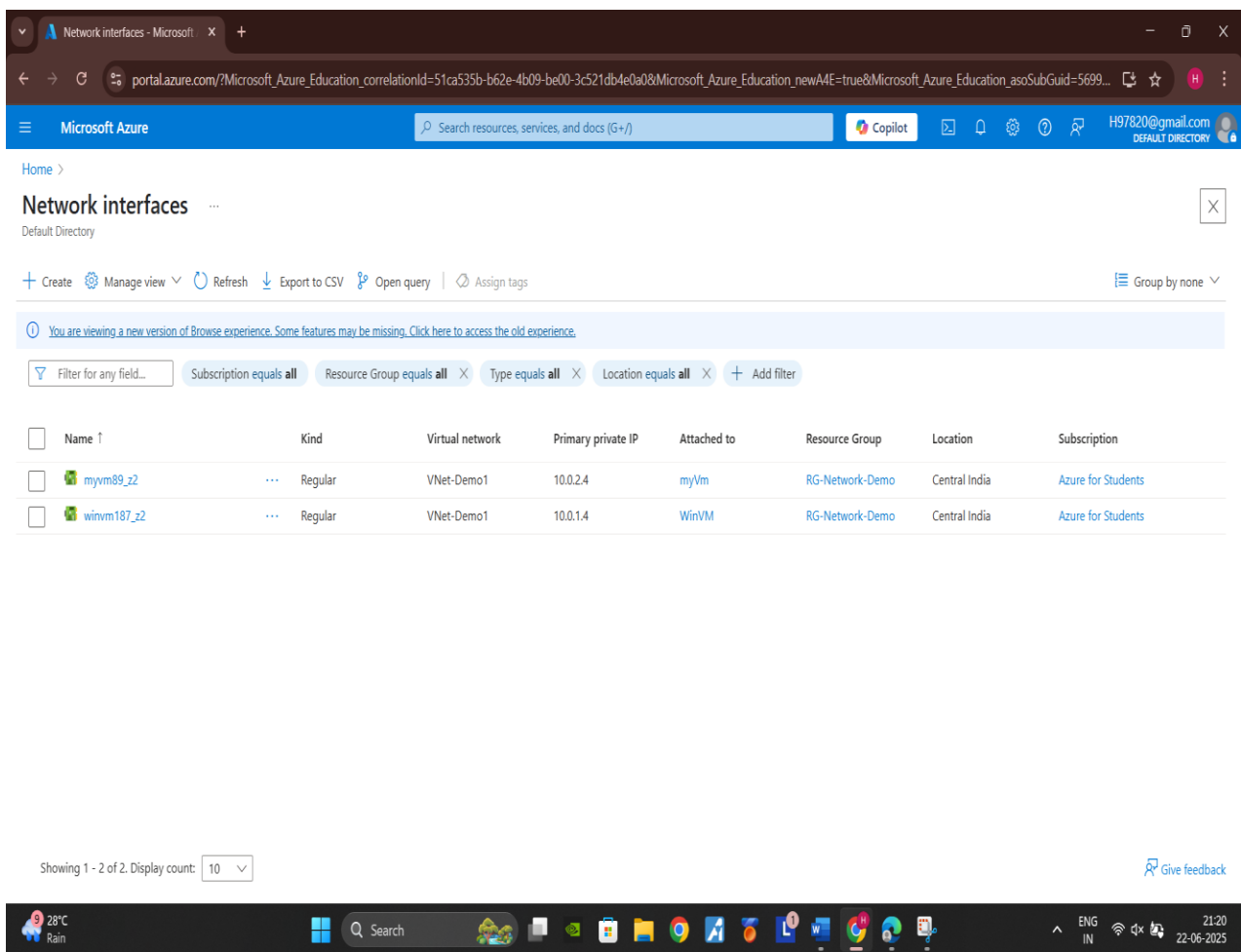
- Public Static IP:
VM → Networking → Public IP → Configuration → Change assignment to *Static*
- Private Static IP :
VM → NIC → IP configurations → Private IP → Change to *Static*

7. Create NSG (Azure Portal)

Go to Networking > Network security groups > + Create

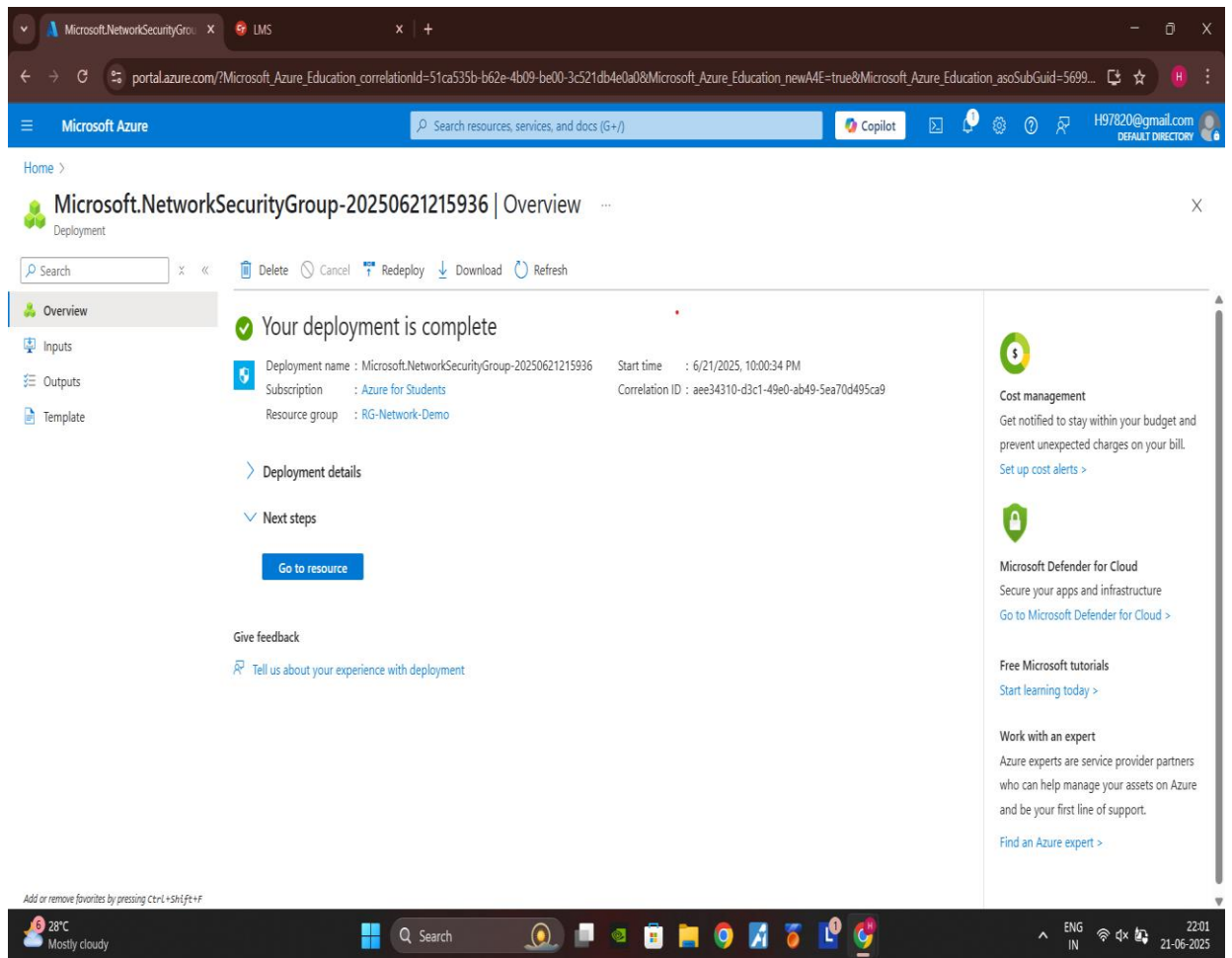
→ Enter:

- Name
- Region
- Resource group
 - Add inbound/outbound rules
 - Associate to subnet/NIC



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The main content area is titled 'Network interfaces' and shows a table of existing interfaces. The table has columns for Name, Kind, Virtual network, Primary private IP, Attached to, Resource Group, Location, and Subscription. Two interfaces are listed: 'myvm89_z2' and 'winvm187_z2', both connected to 'VNet-Demo1' and located in 'Central India'.

Name	Kind	Virtual network	Primary private IP	Attached to	Resource Group	Location	Subscription
myvm89_z2	Regular	VNet-Demo1	10.0.2.4	myVm	RG-Network-Demo	Central India	Azure for Students
winvm187_z2	Regular	VNet-Demo1	10.0.1.4	WinVM	RG-Network-Demo	Central India	Azure for Students



8. Create Public IP (Azure Portal)

Go to Networking > Public IP addresses > + Create
→ Enter:

- Name
- SKU (Basic/Standard)

- Assignment: Static / Dynamic

The screenshot shows the 'Create public IP address' wizard in the Microsoft Azure portal. The 'Basics' tab is active, displaying the following configuration details:

- Resource group:** RS-NETWORK-LEMO (with a 'Create new' link)
- Region:** (Asia Pacific) Central India (with a 'Deploy to an Azure Extended Zone' link)
- Name:** MyPublicIP
- IP Version:** IPv4 (selected), IPv6 (unselected)
- SKU:** Standard (selected)

At the bottom of the wizard, there are three buttons: 'Previous', 'Next', and 'Review + create'. The 'Review + create' button is highlighted in blue. The bottom of the screen shows the Windows taskbar with the date 21-06-2025 and time 22:03.

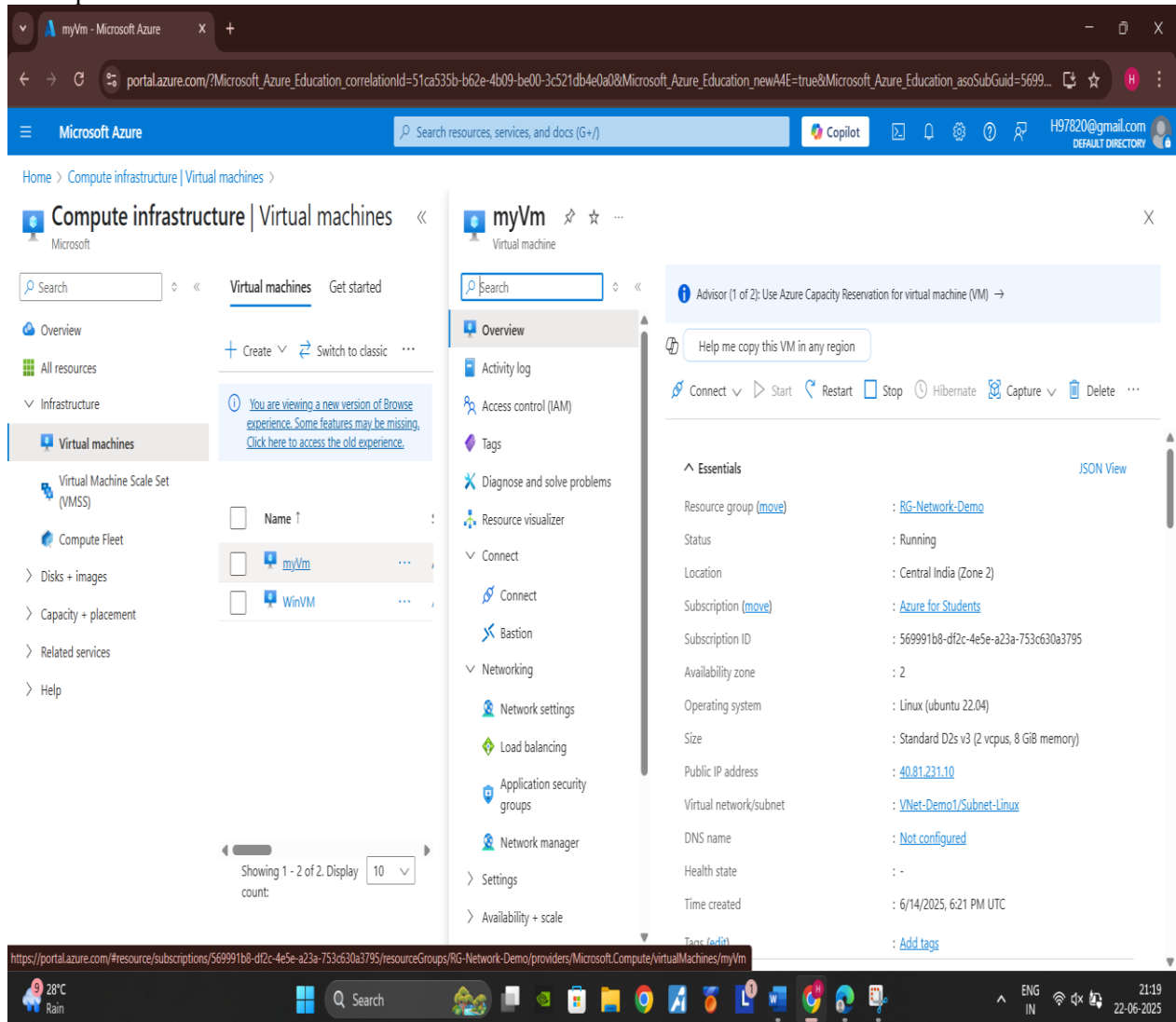
9. Associate / De-associate Public IP

Associate:

- Go to NIC → IP Configurations → Public IP → Associate existing or create new

De-associate:

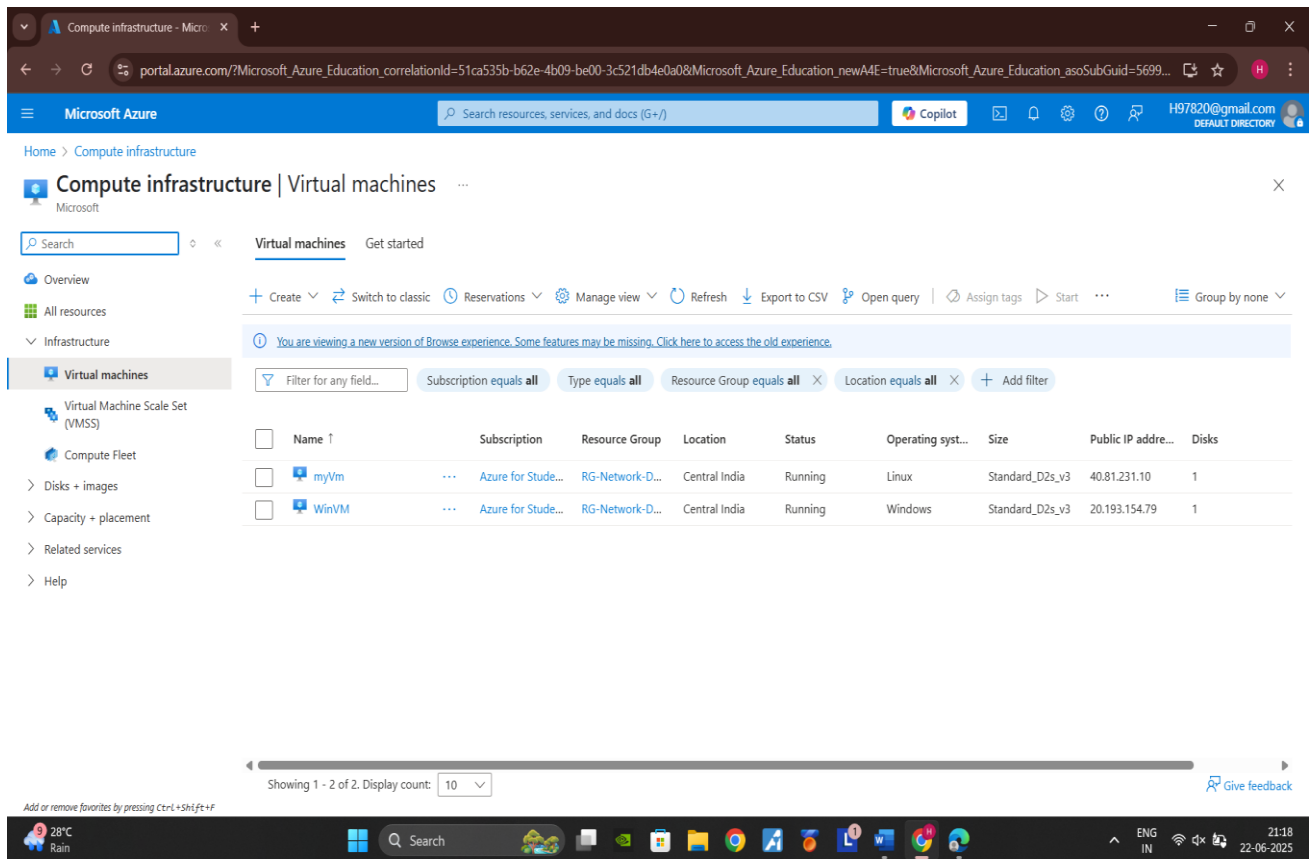
- Same place → Choose *None*



Create Network Interface (NIC)

Go to Networking > Network Interfaces > + Create
→ Enter:

- Name
- VNet + Subnet
- NSG (optional)
- IP assignment: Static/Dynamic
→ Attach NIC to VM



Full Example — Secure VM with NSG + Static IP

Goal:

- VM accessible *only* via RDP from 203.0.113.10
- Deny all internet traffic outbound
- Static Public IP for DNS
- Static Private IP for internal comm
- Steps:
 - Create NSG
 - Add inbound rule (203.0.113.10/32, port 3389, allow)
 - Add inbound rule (Any, port 3389, deny)
 - Add outbound rule (Internet, Any, deny)
 - Create Public IP → Static
 - Assign Public IP to NIC
 - Set NIC private IP to Static