R&D Document: NSG, ASG, Public IPs, and Network Interfaces

Intern Name: Tejasvi Avhad
Company Name: Celebal Technologies
Department: Cloud Infra and Security

Introduction:

In today's cloud-based infrastructure, securing and managing network access to resources such as virtual machines is critical. Microsoft Azure provides robust tools and features to control traffic, enforce access control, and simplify IP management. These features include Network Security Groups (NSG), Application Security Groups (ASG), Public IP address assignments, and Network Interfaces (NIC).

We will:

- Understand how to control and monitor network traffic.
- Allow or deny access to specific IP addresses.
- Configure public and private IP settings.
- Use service tags for simplified access control.
- Implement and test these settings in a real-world cloud environment.

This guide ensures a hands-on learning experience while maintaining clarity and simplicity throughout.

Objective:

To understand and practically implement key Azure networking components such as:

- Network Security Groups (NSG)
- Application Security Groups (ASG)
- Public IP addresses (Static & Dynamic)
- Allowing specific IPs and denying Internet access
- Allocating static IPs to VMs
- Creating Network Interface Cards (NIC)

1. Network Security Group (NSG)

- Network Security Group is a security feature in Microsoft Azure that acts like a virtual firewall to control incoming and outgoing traffic to Azure resources.
- NSG contains a list of security rules that allow or deny network traffic to resources.

- Rules are evaluated in order of priority, and each rule defines:
  - Priority Number: Lower number = higher priority
  - Source and Destination IP Addresses
  - Port Numbers
  - Protocols (TCP/UDP)
  - Access (Allow/Deny)

Purpose:

- Restrict access to virtual machines.
- Allow only selected IPs or services.
- Protect your virtual network from threats.

Where NSG can be applied:

- On Subnets: Controls traffic for all VMs in that subnet.
- On Network Interfaces (NICs): Controls traffic for the associated VM.

2. Application Security Group (ASG)

- ASG is used to logically group VMs based on their function (e.g., WebServers, DBServers).
- NSG rules can then target ASGs rather than individual IP addresses.
- It simplifies management when working with a large number of VMs.

Purpose:

- To apply NSG rules dynamically based on group names instead of IPs.
- Enhance scalability and manageability.

Example:

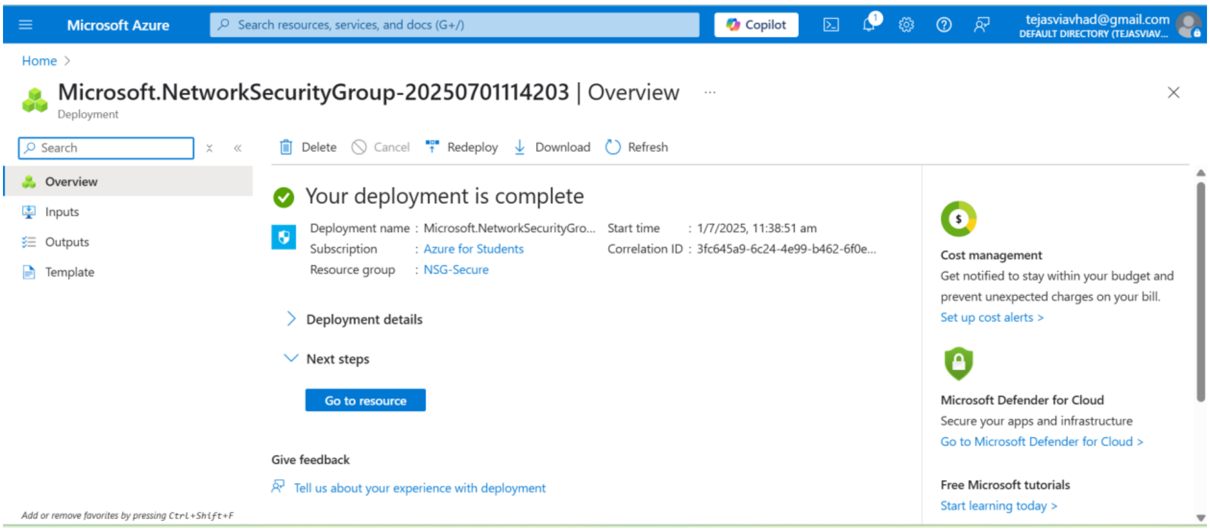
- Group all web VMs in Web-ASG.
- Allow only App-ASG to talk to Web-ASG on port 80.

3. How to Allow Specific IPs and Deny Internet Access using NSG?

- You can configure NSG to allow only a particular IP address (like your office IP) to access your VM.
- You can also deny all outbound traffic to the Internet for a secure environment.

Steps on Azure Portal:

1. Go to Azure Portal > Search "Network Security Groups" > Click + Create.
2. Enter:
   - Name: NSG-Secure
   - Resource Group and Region.
3. Click Create.



Microsoft.NetworkSecurityGroup-20250701114203 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGro...
Subscription : Azure for Students
Resource group : NSG-Secure
Start time : 1/7/2025, 11:38:51 am
Correlation ID : 3fc645a9-6c24-4e99-b462-6f0e...

Deployment details

Next steps

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

Microsoft Defender for Cloud

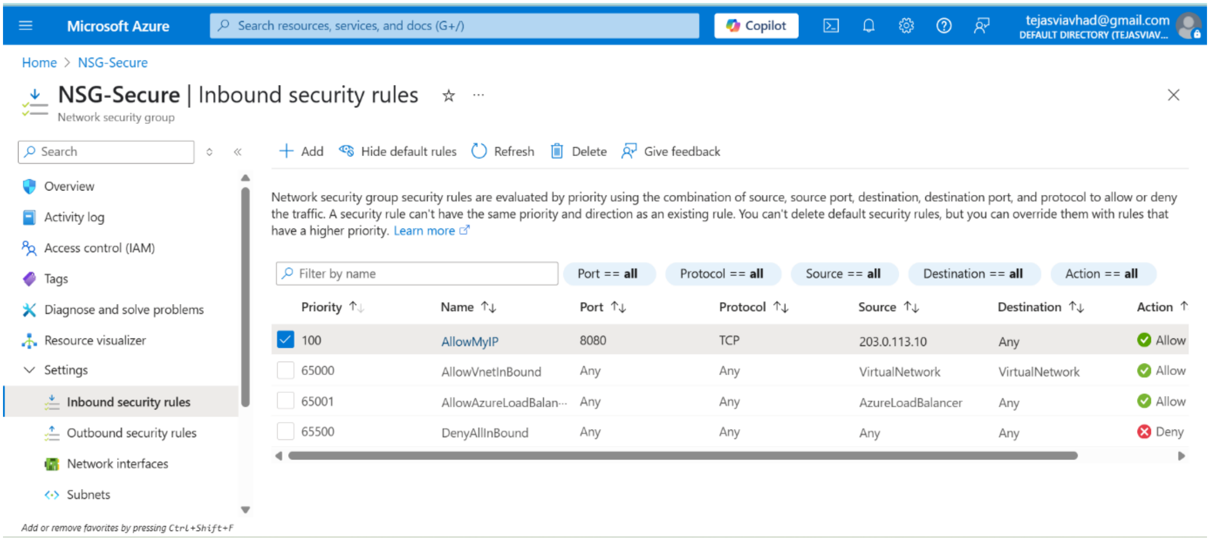
Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

4. Go to Inbound Security Rules > Click + Add.
   - Priority: 100
   - Source: IP Addresses (enter your IP, e.g., 203.0.113.10)
   - Port: 22 (SSH) or 3389 (RDP)
   - Protocol: TCP
   - Action: Allow
   - Name: AllowMyIP



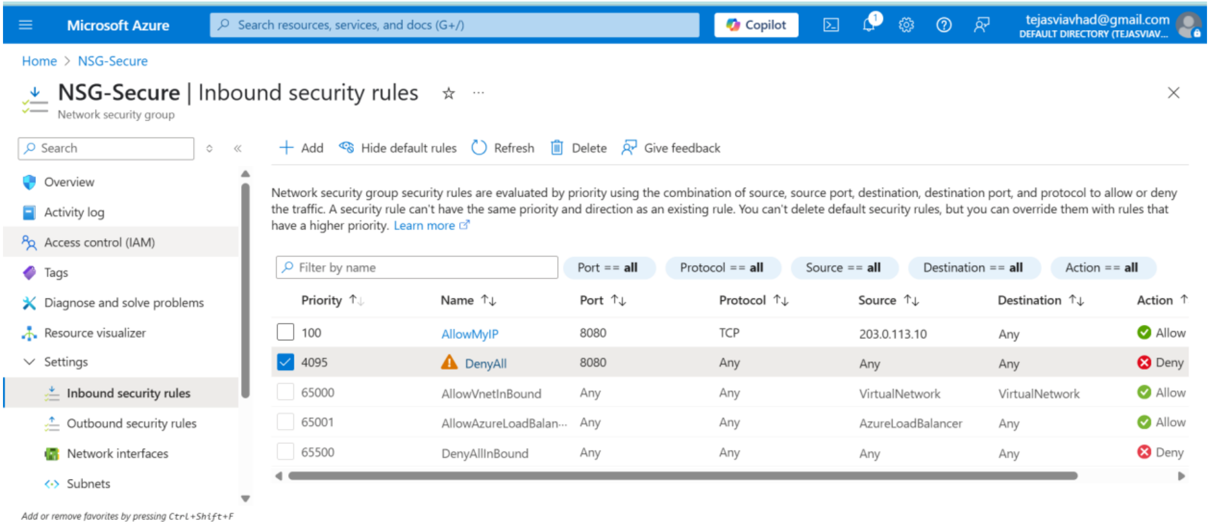
NSG-Secure | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source	Destination	Action
☑	100	AllowMyIP	8080	TCP	203.0.113.10	Any	✓ Allow
□	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
□	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
□	65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

5. Add a Deny rule:
    - Priority: 4095
    - Source: Any
    - Destination: Any
    - Port: Any
    - Protocol: Any
    - Action: Deny
    - Name: DenyAll



NSG-Secure | Inbound security rules

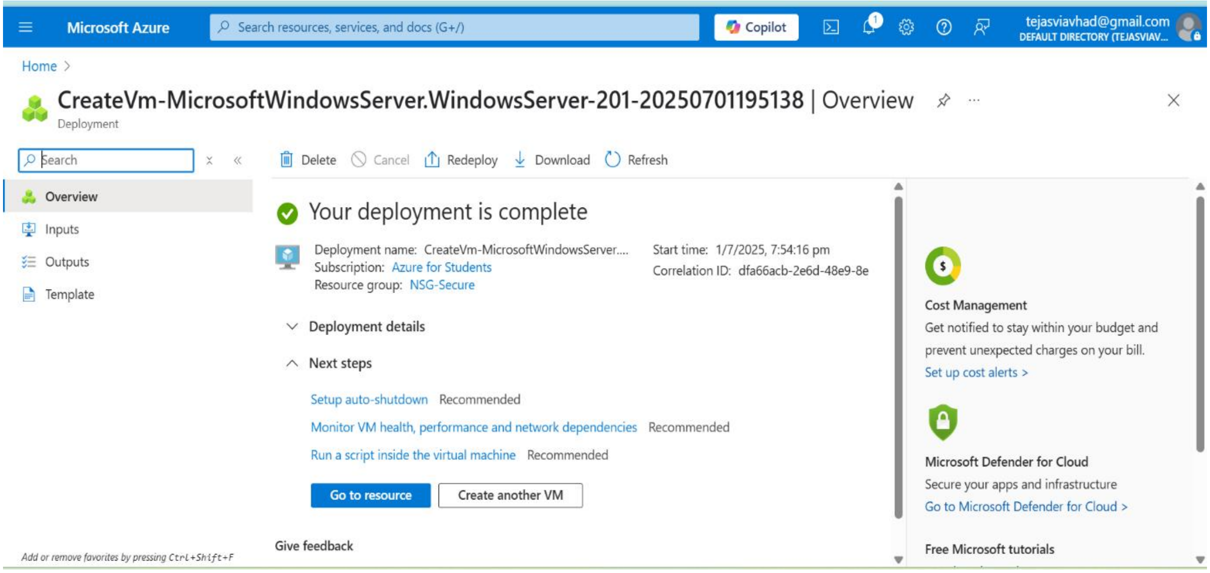
Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source	Destination	Action
□	100	AllowMyIP	8080	TCP	203.0.113.10	Any	✓ Allow
☑	4095	⚠ DenyAll	8080	Any	Any	Any	✗ Deny
□	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
□	65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
□	65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

6. Create Virtual Machine.

- Go to Azure Portal → Virtual Machines → + Create.
- Select your Subscription and Resource Group.
- Enter a VM name and select Region and Image (Windows/Linux).
- Choose a Size (Free tier if available).
- Set username and password/SSH key.
- Under Inbound ports, allow SSH (22) or RDP (3389).
- Click Review + Create → then Create.



CreateVm-MicrosoftWindowsServer.WindowsServer-201-20250701195138 | Overview

Deployment

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer....
Subscription: Azure for Students
Resource group: NSG-Secure

Start time: 1/7/2025, 7:54:16 pm
Correlation ID: dfa66acb-2e6d-48e9-8e

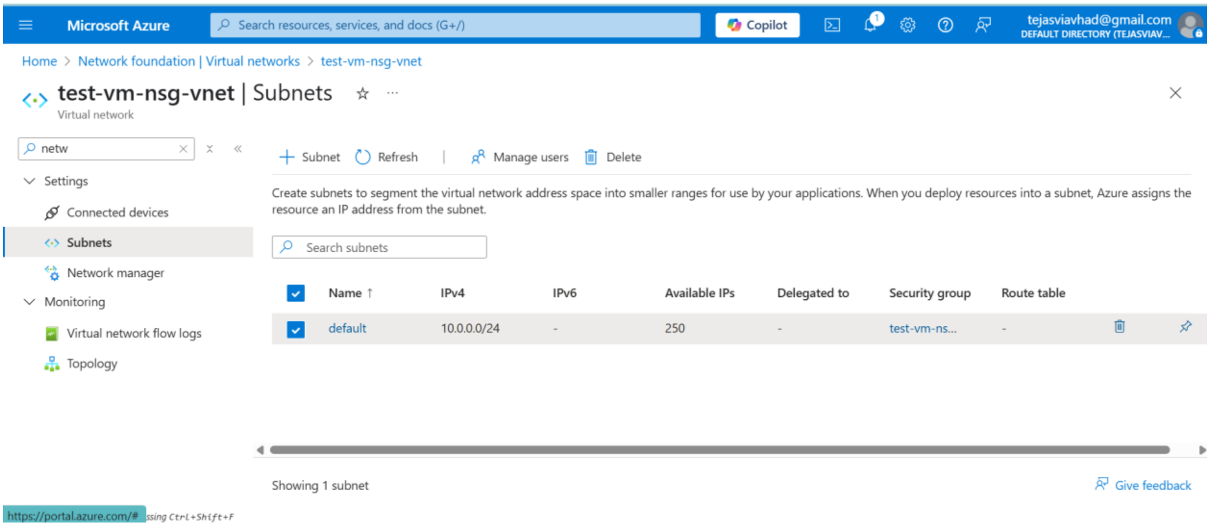
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

7. Attach NSG to a Subnet
   - Go to Azure Portal > Search Virtual Networks.
   - Select your virtual network > Click on Subnets in the left menu.
   - Click on the subnet name.
   - In the subnet settings, under Network Security Group, click Associate.
   - Select your NSG from the dropdown list.
   - Click Save.



test-vm-nsg-vnet | Subnets

Virtual network

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

☑	Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
☑	default	10.0.0.0/24	-	250	-	test-vm-ns...	-

Showing 1 subnet

4. Public IP Addresses in Azure

- A Public IP is used to communicate with Azure resources over the internet.
- Assigned to virtual machines, load balancers, and other network resources.

Types of Public IPs:

1. Dynamic IP:
   - Automatically assigned when VM starts.
   - May change after VM stops and restarts.
2. Static IP:
   - Manually reserved.
   - Remains fixed even after stopping/restarting VM.
   - Recommended for production workloads.

Use Cases:

- SSH/RDP access.
- Hosting web applications.
- Fixed DNS mapping.

5. Service Tags in Azure

- Service tags simplify NSG rule definitions.
- Instead of using IP ranges, we use service tags.

Examples:

- Internet: All external IP addresses.
- VirtualNetwork: All resources in your VNet.
- AzureLoadBalancer: IPs used by Azure's load balancer.

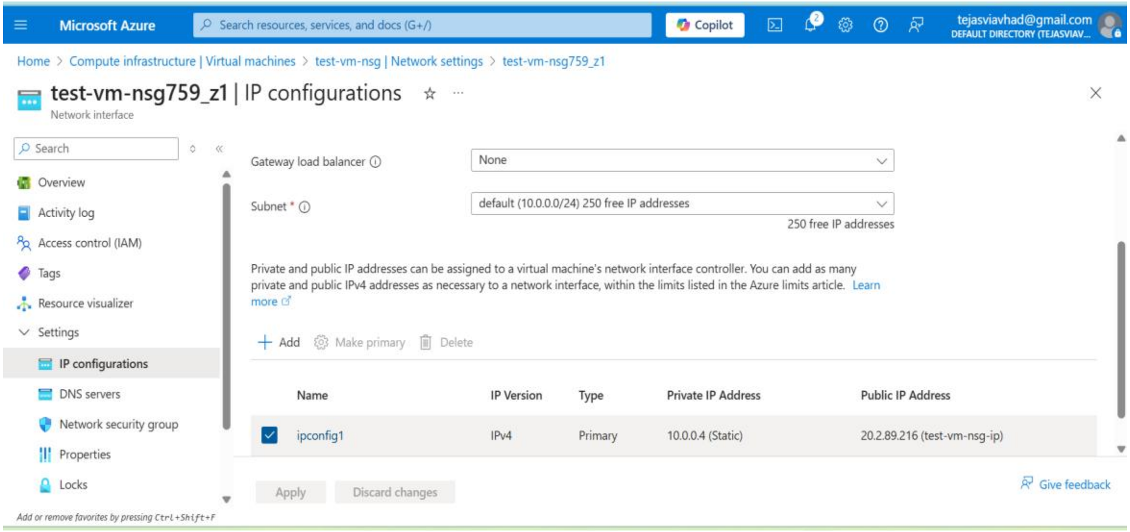
Purpose:

- Reduce complexity.
- Improve manageability.

6. Allocating Static Private and Public IPs to a VM

Steps to Assign Static Private IP:

1. Azure Portal > VM > Networking > Click NIC name.
2. Go to IP configurations > Click on IP config name.
3. Set Private IP address to Static.
4. Save the settings.



Home > Compute infrastructure | Virtual machines > test-vm-nsg | Network settings > test-vm-nsg759_z1

test-vm-nsg759_z1 | IP configurations

Network interface

Gateway load balancer: None

Subnet *: default (10.0.0.0/24) 250 free IP addresses

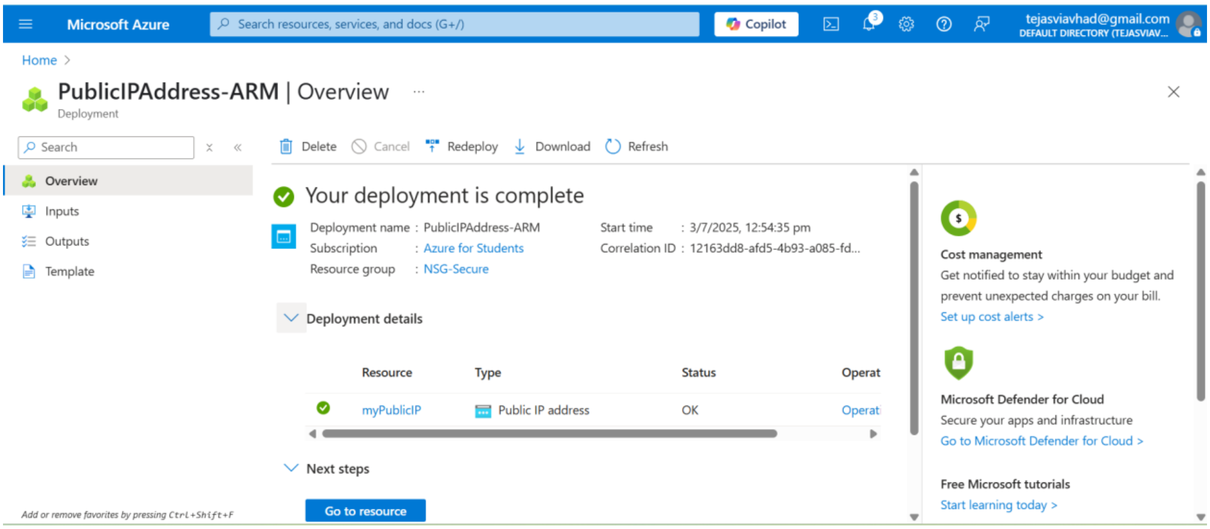
250 free IP addresses

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. Learn more

	Name	IP Version	Type	Private IP Address	Public IP Address
☑	ipconfig1	IPv4	Primary	10.0.0.4 (Static)	20.2.89.216 (test-vm-nsg-ip)

Steps to Assign an Existing Static Public IP

- In Azure Portal, search for Public IP addresses.
- Click + Create to make a new Public IP.
- Set the following:
  1. Name: myPublicIP
  2. SKU: Basic or Standard
  3. Assignment: Static
  4. Location: Same as your VM
  5. Resource Group: Same as your VM
- Click Review + Create, then Create.



Home >

PublicIPAddress-ARM | Overview

Deployment

Your deployment is complete

Deployment name : PublicIPAddress-ARM
Subscription : Azure for Students
Resource group : NSG-Secure
Start time : 3/7/2025, 12:54:35 pm
Correlation ID : 12163dd8-afd5-4b93-a085-fd...

Deployment details

Resource	Type	Status	Operat
myPublicIP	Public IP address	OK	Operat

Next steps

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

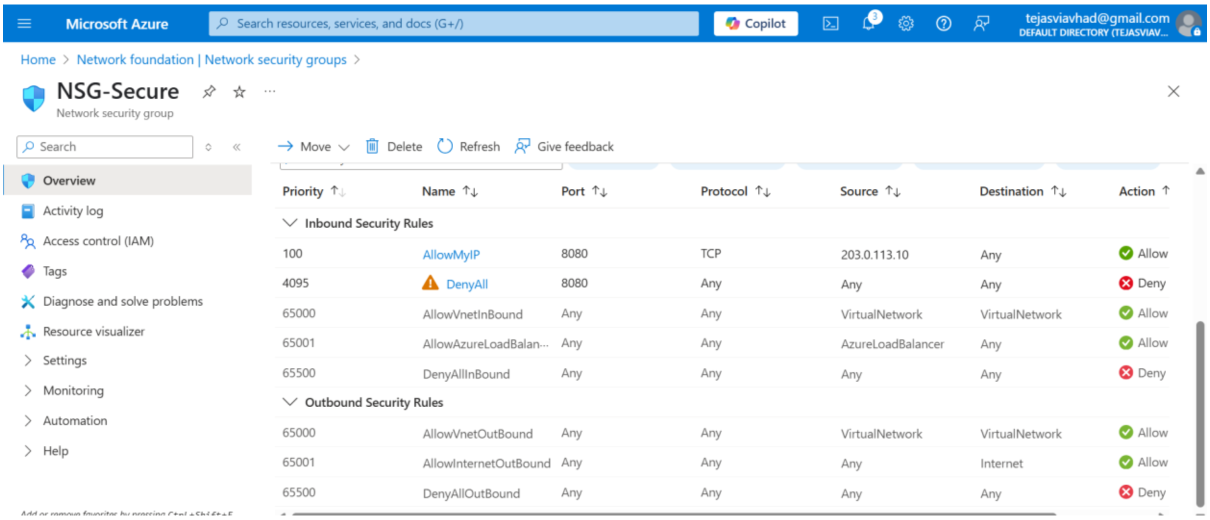
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

7. How to Create a Network Security Group (NSG)?

Steps:

1. Azure Portal > Search "Network Security Groups" > Click + Create.
2. Fill in:
   - Name: NSG-Secure
   - Resource Group
   - Region
3. Click Review + Create > Create.
4. Go to the created NSG > Add Inbound or Outbound rules as required.

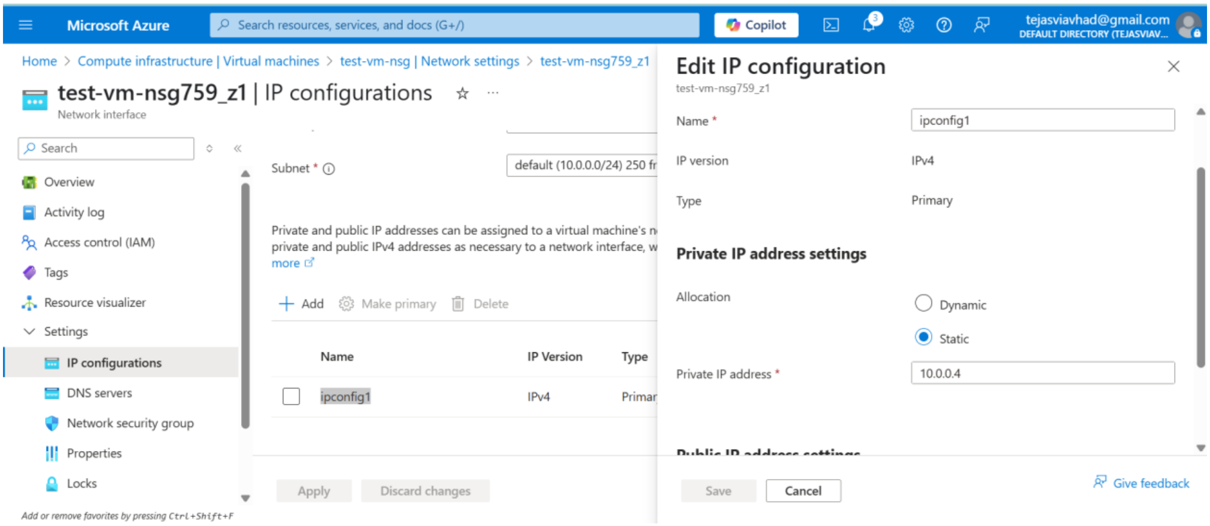


Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
100	AllowMyIP	8080	TCP	203.0.113.10	Any	✓ Allow
4095	⚠ DenyAll	8080	Any	Any	Any	✗ Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

8. How to Associate or De-associate Public IP with a VM?

To Associate Public IP:

1. Go to VM > Networking > Click NIC name.
2. Click IP Configurations.
3. Click IP configuration name.
4. Under Public IP, select your static IP.
5. Save changes.



test-vm-nsg759_z1 | IP configurations

Subnet * default (10.0.0.0/24) 250 fr

Private and public IP addresses can be assigned to a virtual machine's n
private and public IPv4 addresses as necessary to a network interface, w
more

Name	IP Version	Type
□ ipconfig1	IPv4	Primar

Edit IP configuration

test-vm-nsg759_z1

Name * ipconfig1

IP version IPv4

Type Primary

Private IP address settings

Allocation ○ Dynamic ● Static

Private IP address * 10.0.0.4

Public IP address settings

To De-associate Public IP:

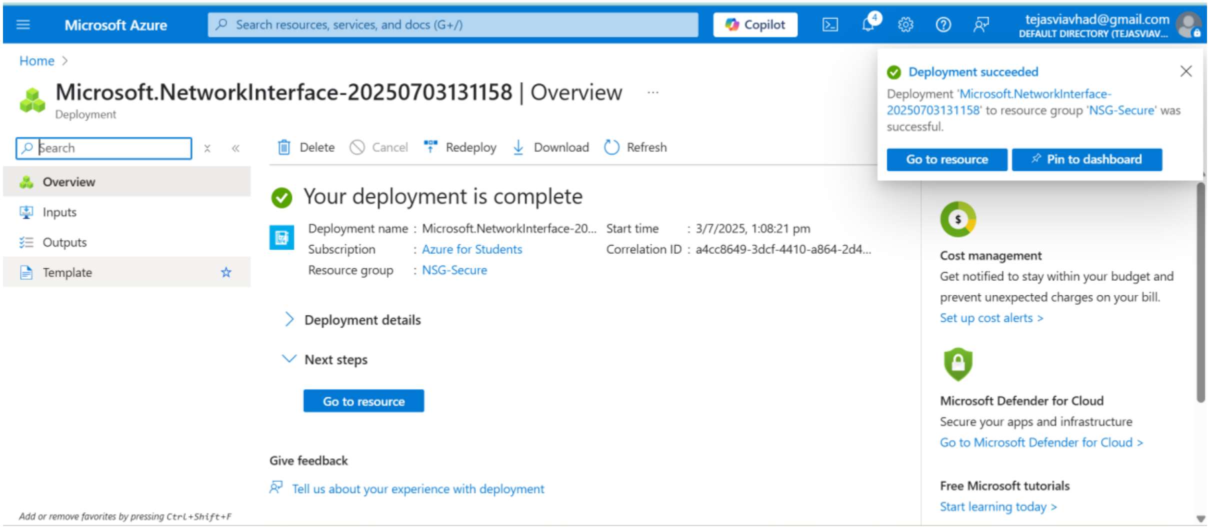
1. Follow the same steps above.
2. Under Public IP, choose None.
3. Click Save.

9. How to Create a Network Interface (NIC)?

- NIC is used to connect a VM to a VNet.
- Each NIC can be assigned:
  - One private IP
  - One public IP (optional)
  - NSG

Steps to Create NIC:

1. Azure Portal > Search "Network Interfaces" > Click + Create.
2. Enter:
   - Name: nic-01
   - Region
   - Virtual Network and Subnet
   - Assign Static or Dynamic IP
3. Optionally assign an NSG and Public IP.
4. Click Review + Create > Create.



Microsoft.NetworkInterface-20250703131158 | Overview

Deployment

Deployment succeeded

Deployment 'Microsoft.NetworkInterface-20250703131158' to resource group 'NSG-Secure' was successful.

Your deployment is complete

Deployment name : Microsoft.NetworkInterface-20...
Subscription : Azure for Students
Resource group : NSG-Secure
Start time : 3/7/2025, 1:08:21 pm
Correlation ID : a4cc8649-3dcf-4410-a864-2d4...

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Microsoft Defender for Cloud

Secure your apps and infrastructure

Free Microsoft tutorials

10. Conclusion

In this document, I learned how to manage network access in Azure using NSG, ASG, static IPs, and public IPs. I also practiced creating a VM, assigning IPs, and connecting rules to NIC and subnet. It helped me understand how to protect virtual machines and allow specific traffic securely. This was a great hands-on experience for learning Azure networking.