R&D Report on NSG, ASG, Public IP Configuration, and Network Interface Management in Microsoft Azure

Prepared by: Virat Pandey

Celebal Technology

Cloud Infrastructure & Security Internship

Research & Development Document

July, 2025

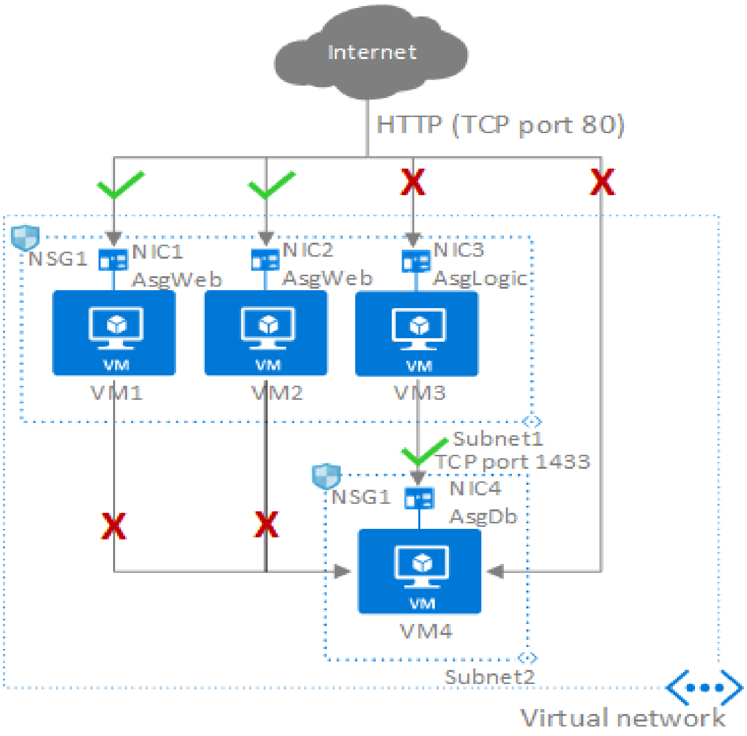
Table of Contents

1. Introduction

As organizations migrate to the cloud, maintaining control over network access and traffic becomes a top priority. Microsoft Azure offers a range of built-in tools that help administrators define and enforce security boundaries, ensure compliant network architecture, and manage connectivity with flexibility.

In this context, **Network Security Groups (NSGs)** and **Application Security Groups (ASGs)** are essential for implementing firewall-like rule sets at both subnet and NIC levels. These allow cloud architects to control which traffic is permitted or denied across Azure resources. **Public IPs**, on the other hand, enable access from the internet, while **Service Tags** help simplify rule creation for trusted Azure services.

This report provides an in-depth understanding of how these networking features operate within Azure. It also includes practical insights on how to allow or restrict access to specific IPs, assign static or dynamic IP addresses to VMs, create NSGs and Public IPs, and associate them correctly with virtual machines and network interfaces.



2. Working of Network Security Groups (NSG)

A **Network Security Group (NSG)** is a fundamental security component in Azure that acts like a virtual firewall. It contains a list of **security rules** that determine whether network traffic is **allowed or denied** to Azure resources based on:

- **Source & Destination IP address**
- **Port number**
- **Protocol (TCP/UDP)**
- **Direction (Inbound/Outbound)**

NSGs can be associated with:

- **Subnets**: Rules apply to all resources in that subnet.
- **Network interfaces (NICs)**: Rules apply only to the specific VM.

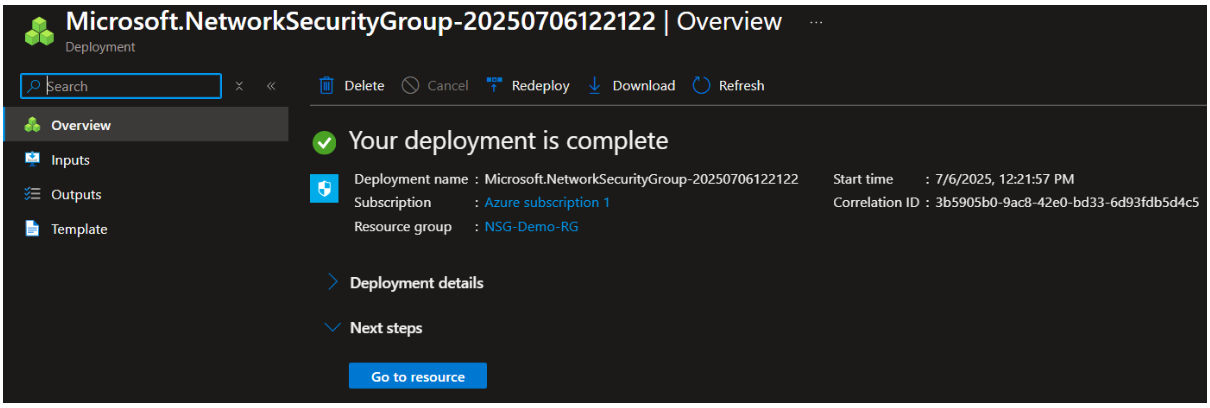
Each rule has a **priority number** (100–4096); **lower values = higher priority**. Rules are evaluated in order, and the first match is applied.

NSG Evaluation Logic (Example):

- Allow SSH (Port 22) from specific IP
- Deny all outbound internet traffic
- Allow VM-to-VM internal communication

Use Cases

- Allowing RDP to Windows VMs only from your home IP
- Blocking all traffic to a sensitive backend subnet
- Creating isolated dev/test environments using NSGs



Microsoft.NetworkSecurityGroup-20250706122122 | Overview

Deployment

Your deployment is complete

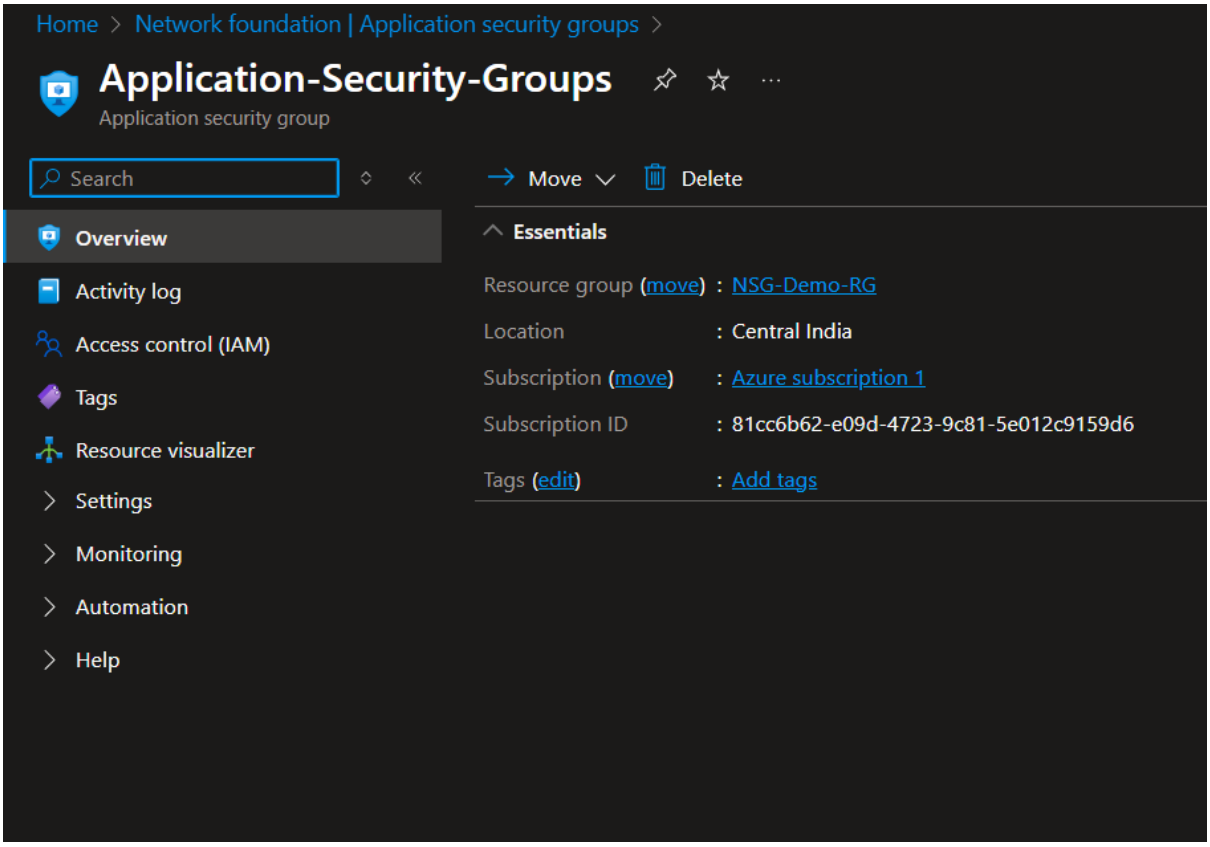
Deployment name : Microsoft.NetworkSecurityGroup-20250706122122
Subscription : Azure subscription 1
Resource group : NSG-Demo-RG
Start time : 7/6/2025, 12:21:57 PM
Correlation ID : 3b5905b0-9ac8-42e0-bd33-6d93fdb5d4c5

3. Working of ASG

An **Application Security Group (ASG)** allows the grouping of virtual machines with similar roles (e.g., web servers, database servers) for easier network security rule management.

In this implementation, an ASG named asg-web was created to represent a group of VMs that serve as the web tier. Instead of assigning NSG rules to specific IPs or NICs, rules can now target this logical group. This improves clarity and maintainability in large deployments.

For example, to allow traffic from web servers to database servers, you can simply allow traffic from asg-web to asg-db on port 1433 (SQL), rather than managing each IP individually.



Essentials

Resource group (move) : NSG-Demo-RG

Location : Central India

Subscription (move) : Azure subscription 1

Subscription ID : 81cc6b62-e09d-4723-9c81-5e012c9159d6

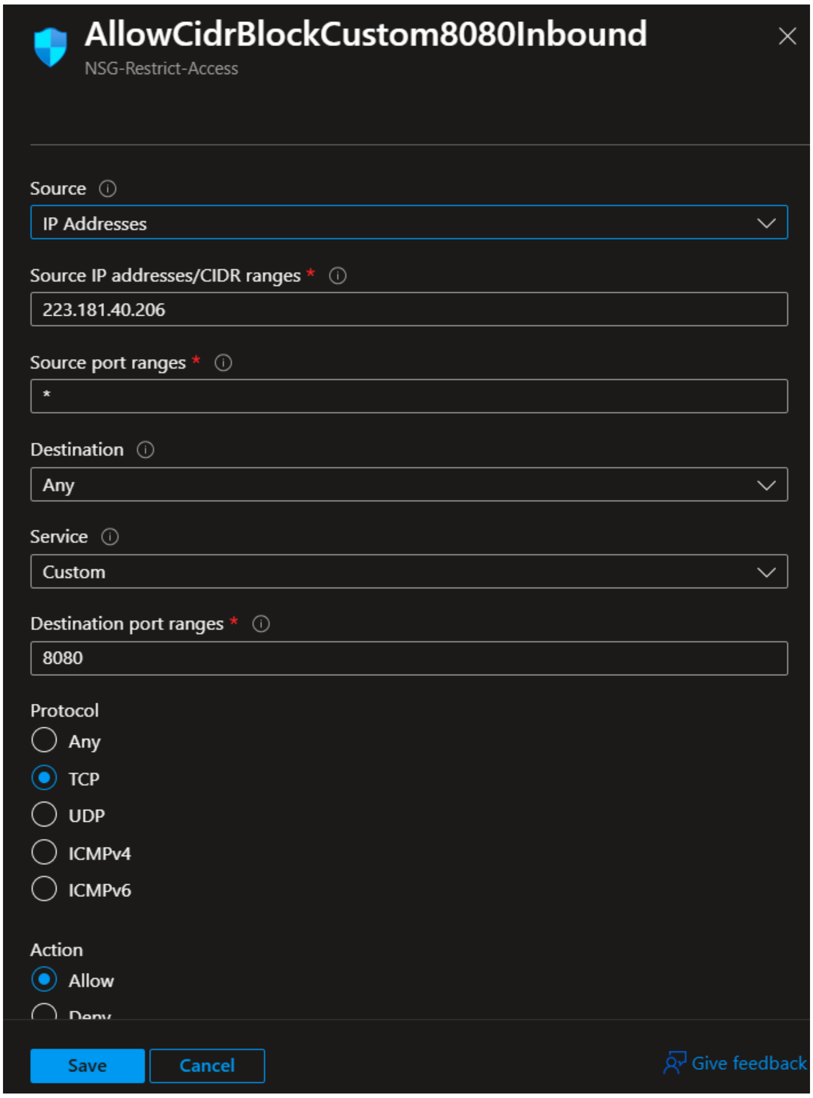
Tags (edit) : Add tags

Figure: Application Security Group asg-web created in Central India region.

4. Allowing specific IPs and denying internet using NSG

To enhance security, access to the VM was restricted to a single public IP address by creating a custom inbound rule in the NSG. This rule allowed traffic only from IP 223.181.40.206 on TCP port 8080.

In addition, an outbound rule was configured to deny all internet traffic from the VM. This was done using the Internet service tag as the destination and setting the action to Deny. This ensures that the VM cannot reach public networks, adding a layer of data security.



AllowCidrBlockCustom8080Inbound

NSG-Restrict-Access

Source: IP Addresses

Source IP addresses/CIDR ranges *: 223.181.40.206

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 8080

Protocol

○ Any
● TCP
○ UDP
○ ICMPv4
○ ICMPv6

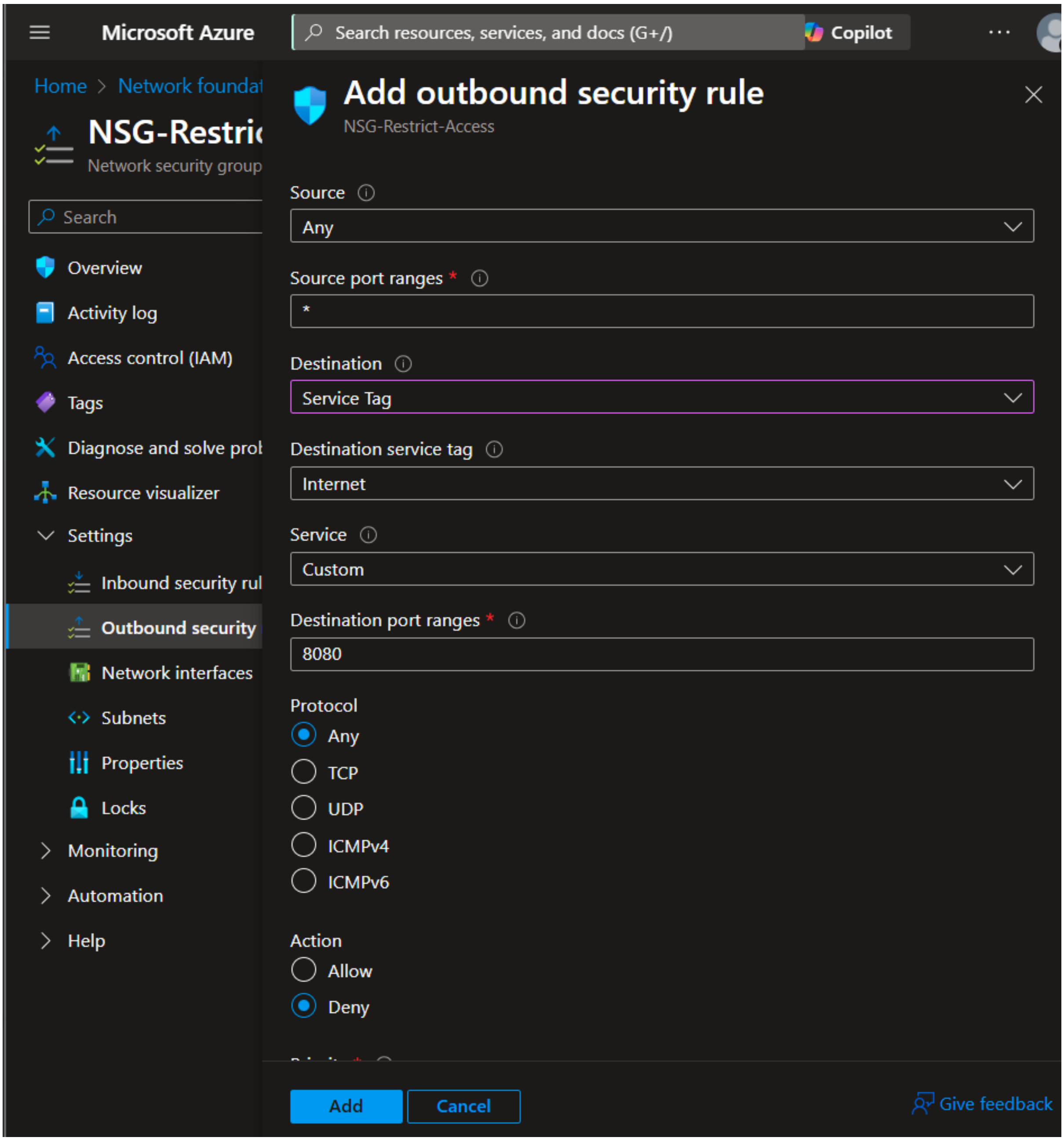
Action

● Allow
○ Deny

Inbound Rule — allowing specific IP

A custom outbound rule was created within the NSG to block all internet-bound traffic from the virtual machine. This rule used the **Internet service tag** as the destination, which represents all public IP addresses.

By setting the action to **Deny**, and the protocol and port range to **Any**, this rule ensures that the VM cannot initiate any outbound connections to the internet. Such restrictions are critical in environments where outbound traffic needs to be tightly controlled, such as backend servers or internal-only applications.



Add outbound security rule

NSG-Restrict-Access

Source: Any

Source port ranges *: *

Destination: Service Tag

Destination service tag: Internet

Service: Custom

Destination port ranges *: 8080

Protocol
● Any
○ TCP
○ UDP
○ ICMPv4
○ ICMPv6

Action
○ Allow
● Deny

Outbound Rule — deny Internet

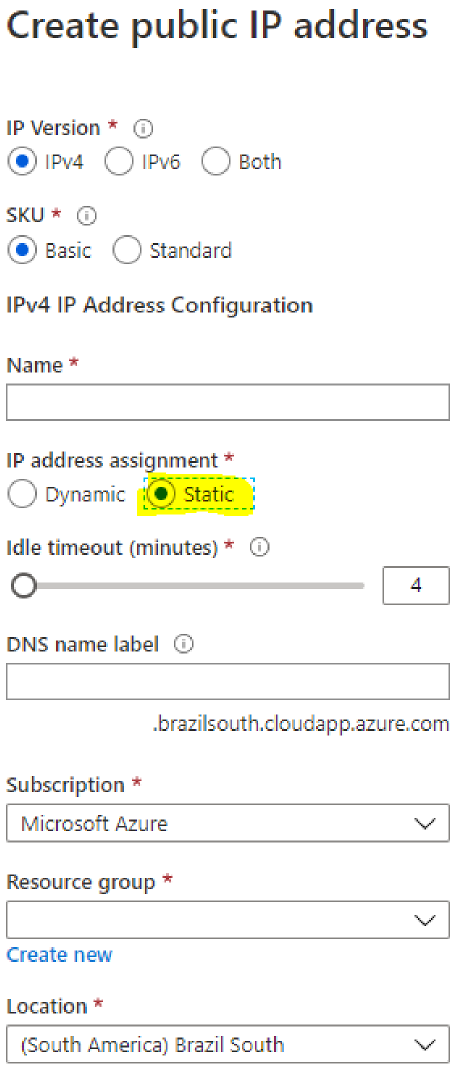
5. Public IPs in azure

5.1 Static vs Dynamic Public IP

In Azure, a **Public IP address** allows external users and services to connect to Azure resources like virtual machines. Azure provides two types of public IPs: **Static** and **Dynamic**.

- **Static Public IP**: The IP address is reserved and does not change, even if the resource is stopped or restarted. Ideal for DNS mapping and production environments.
- **Dynamic Public IP**: The IP is assigned when the resource is started and may change if the resource is stopped and started again.

Static IPs offer consistency while dynamic IPs are more suited for short-lived or test workloads where permanent addressing isn't required.



Create public IP address

IP Version *
● IPv4 ○ IPv6 ○ Both

SKU *
● Basic ○ Standard

IPv4 IP Address Configuration

Name *

IP address assignment *
○ Dynamic ● Static

Idle timeout (minutes) *
4

DNS name label
.brazilsouth.cloudapp.azure.com

Subscription *
Microsoft Azure

Resource group *

Create new

Location *
(South America) Brazil South

5.2 Creating and Managing Public IPs in Azure

Public IP addresses in Azure can be created independently or during the deployment of a resource such as a virtual machine or load balancer.

When creating a Public IP manually, Azure allows you to choose:

- **SKU**: Basic or Standard
- **Assignment**: Static or Dynamic
- **IP Version**: IPv4 (default) or IPv6

A public IP can then be **associated** with a VM's network interface (NIC) to enable internet access, or **disassociated** when internet exposure is no longer needed.

These IPs can also be **named and reused** across services within the same region and subscription.

5.3 Associating/De-associating Public IPs with Virtual Machines

In Azure, a public IP address can be associated with a **network interface (NIC)** to provide external access to a virtual machine. This is essential for scenarios like remote access (SSH/RDP) or exposing web services to the internet.

When a VM is deployed, a public IP can be **automatically assigned**, or you can manually associate an existing Public IP with the VM's NIC through the Azure Portal.

Conversely, you can also **de-associate the public IP** from the NIC to cut off internet access to the VM without deleting the VM itself. This is useful when a resource is being moved to a private-only environment or when shutting down access temporarily.

The association and disassociation process can be done through:

- The **NIC settings** in the Azure Portal
- Or via **PowerShell / CLI** in automated environments

6. Service tags in azure NSG

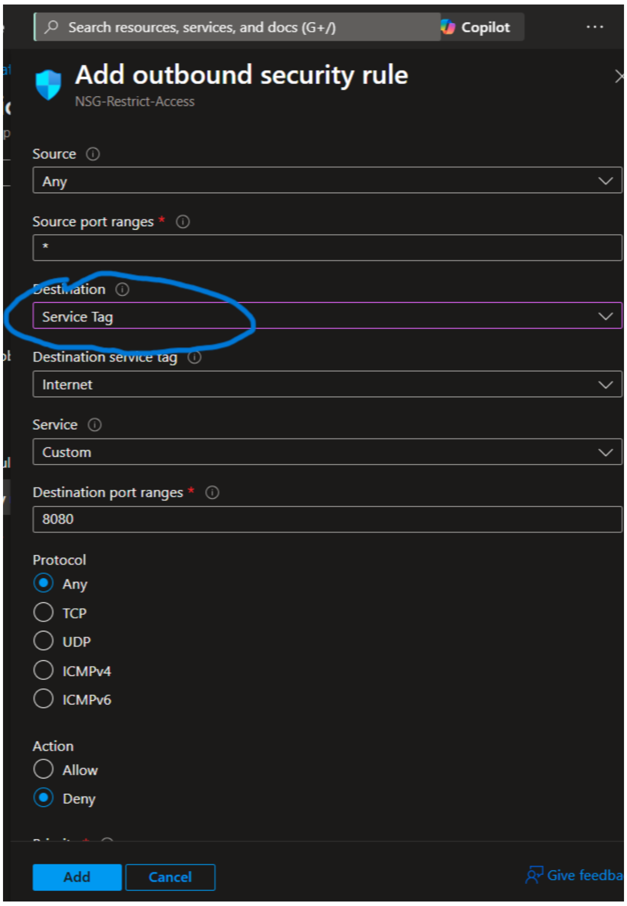
Service Tags in Azure are predefined labels that represent a group of IP address ranges for specific Azure services. They simplify NSG rule management by allowing you to reference a service instead of managing individual IPs or CIDRs.

For example, instead of entering all IP ranges for Azure Load Balancer, you can simply use the service tag AzureLoadBalancer in the destination field of an NSG rule.

Commonly used service tags include:

- Internet – All public IPs not part of Azure
- VirtualNetwork – All IPs within the connected VNets
- AzureCloud, Storage, SQL, etc.

These tags are regularly updated by Microsoft and help reduce the operational overhead of manually tracking IP changes.



Add outbound security rule

NSG-Restrict-Access

Source: Any

Source port ranges *: *

Destination: Service Tag

Destination service tag: Internet

Service: Custom

Destination port ranges *: 8080

Protocol

● Any
○ TCP
○ UDP
○ ICMPv4
○ ICMPv6

Action

○ Allow
● Deny

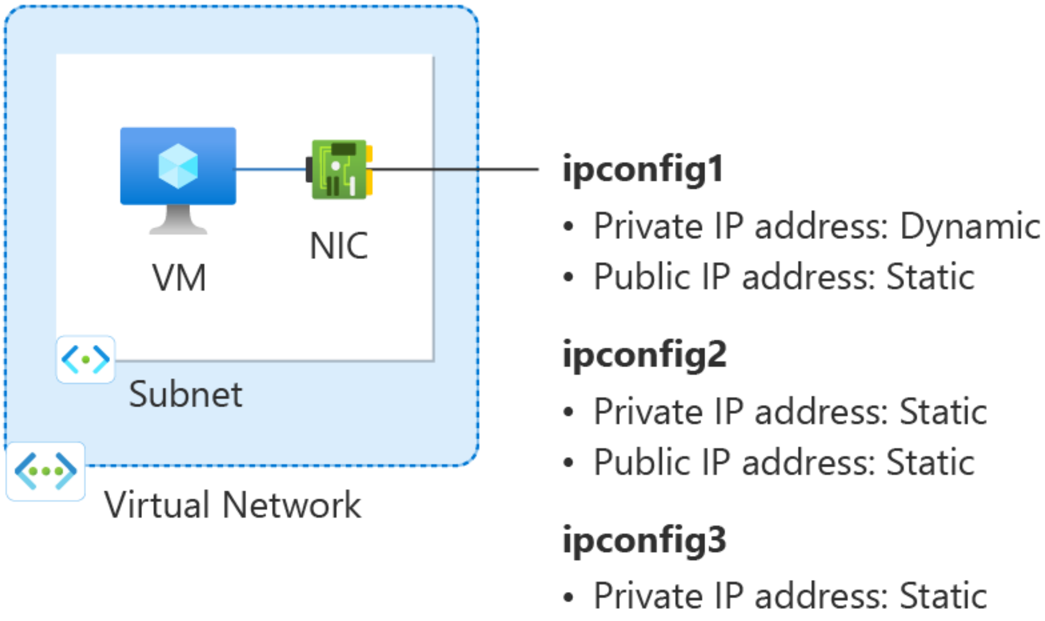
7. Allocating Static IPs to All VMs

In Azure, each virtual machine receives a **dynamic private IP** by default, which may change if the VM is stopped or deallocated. To ensure consistency in networking (especially for DNS, firewall rules, or peering), you can assign a **static private IP** to a VM.

This is done through the **Network Interface (NIC)** of the VM:

1. Go to the VM's NIC
2. Select **IP Configurations**
3. Click on the assigned configuration
4. Change **Assignment** from Dynamic to Static
5. Choose the desired private IP within the subnet range

This ensures the VM always retains the same private IP across restarts and redeployments.


VM
NIC
Subnet
Virtual Network
ipconfig1
• Private IP address: Dynamic
• Public IP address: Static
ipconfig2
• Private IP address: Static
• Public IP address: Static
ipconfig3
• Private IP address: Static

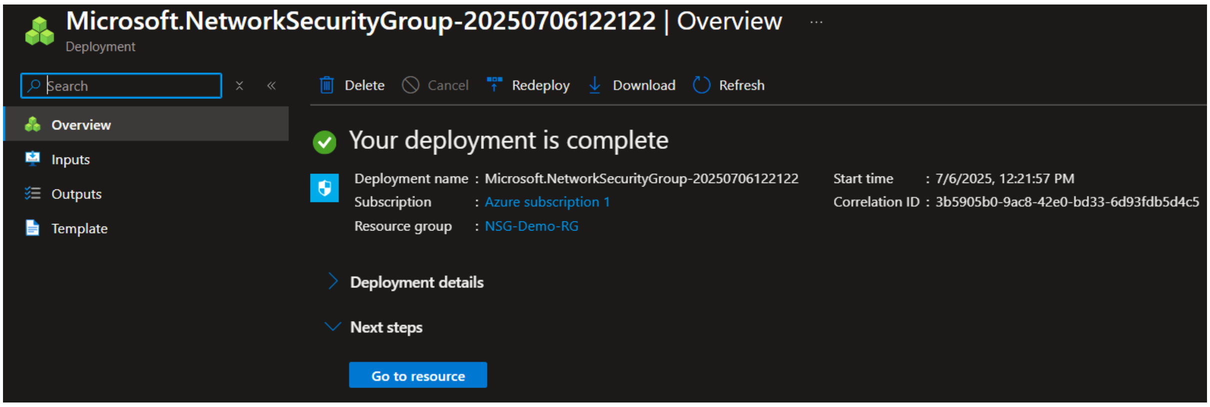
8. Creating NSG

A **Network Security Group (NSG)** in Azure is a virtual firewall that controls inbound and outbound traffic for resources such as VMs, subnets, and NICs.

In this implementation, an NSG named **NSG-Restrict-Access** was created and attached to the network interface of the VM.
It contains custom rules to:

- Allow traffic only from a specific public IP on port 8080
- Deny all outbound traffic to the internet

NSGs are essential for enforcing granular access control in Azure and are commonly applied at both subnet and NIC levels.



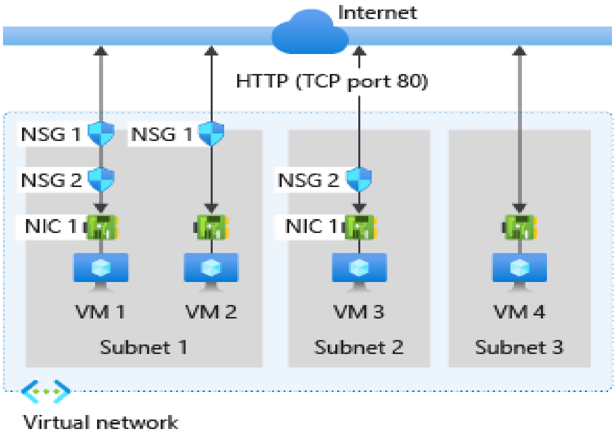
Microsoft.NetworkSecurityGroup-20250706122122 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.NetworkSecurityGroup-20250706122122
Subscription : Azure subscription 1
Resource group : NSG-Demo-RG
Start time : 7/6/2025, 12:21:57 PM
Correlation ID : 3b5905b0-9ac8-42e0-bd33-6d93fdb5d4c5

Figure: Network Security Group NSG-Restrict-Access created in Central India region



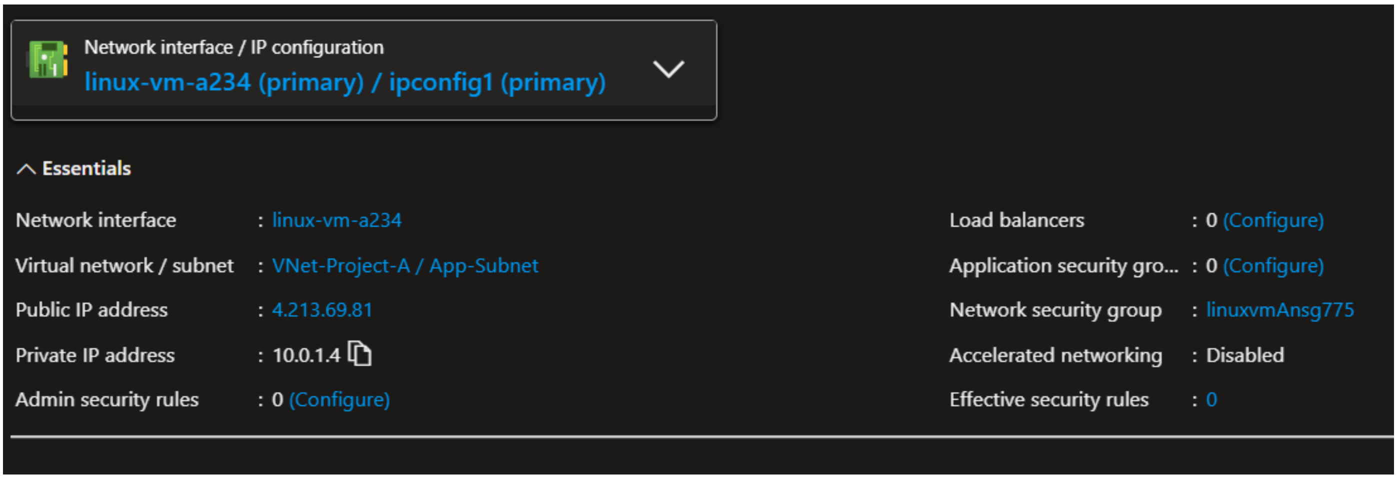
9. Creating a Network Interface

A **Network Interface (NIC)** in Azure is a virtual adapter that connects a virtual machine to a virtual network. It holds IP configuration details such as:

- Private IP address
- Public IP address (if any)
- NSG association
- ASG membership

Each VM must have at least one NIC, and NICs can be created independently or automatically during VM creation.

In this implementation, the NICs were automatically generated when the VMs were created, but their settings (such as static IP, NSG assignment) were modified later through the portal for better control.



Network interface / IP configuration
linux-vm-a234 (primary) / ipconfig1 (primary)

Essentials

Network interface	: linux-vm-a234	Load balancers	: 0 (Configure)
Virtual network / subnet	: VNet-Project-A / App-Subnet	Application security gro...	: 0 (Configure)
Public IP address	: 4.213.69.81	Network security group	: linuxvmAnsg775
Private IP address	: 10.0.1.4	Accelerated networking	: Disabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Conclusion

This report explored and implemented critical components of Azure's virtual networking and security architecture. Through both theoretical research and practical application, we examined how **Network Security Groups (NSGs)** and **Application Security Groups (ASGs)** are used to control traffic at a granular level, ensuring secure and organized network access to virtual machines.

By configuring **inbound rules** to allow specific public IPs and **outbound rules** to deny internet access, we demonstrated how NSGs can restrict communication in and out of the cloud environment. Additionally, **Service Tags** were used to simplify IP-based rules, while **static IP allocation** ensured consistency in VM addressing across restarts and deployments.

The creation and management of **public IPs**, both static and dynamic, as well as the manual association/disassociation of these IPs with virtual machines, reinforced the importance of access control and external connectivity planning. The report also emphasized the role of **Network Interfaces (NICs)** in binding VMs to the network and applying NSGs and IP configurations effectively.

Overall, this assignment deepened the understanding of Azure networking fundamentals, promoted hands-on learning of best practices, and showcased how modern cloud infrastructures rely on precise control over connectivity and security boundaries.

References

□ Microsoft Learn – How Network Security Groups (NSG) Work
https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

□ Microsoft Learn – Assign Multiple IP Addresses to Azure NICs
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-multiple-ip-addresses-portal

□ Microsoft Learn – Virtual Network Overview
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

□ Microsoft Learn – Virtual Network Peering
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

□ Microsoft Learn – Public IP Address in Azure
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses

□ Microsoft Learn – Application Security Groups
https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups

□ Microsoft Learn – Create and manage a network interface
https://learn.microsoft.com/en-us/azure/virtual-network/create-network-interface