Prepared by: Nandini Goyal

Intern at Celebal Technologies

Department: Cloud Infra & Security

Date: 5 July 2025

R&D Document

Network Security Groups, Application Security Groups & IP Management in Azure

Table of Contents

1. Introduction

Cloud environments demand advanced control over traffic flow, both inbound and outbound. In Microsoft Azure, Network Security Groups (NSG) and Application Security Groups (ASG) are essential tools for managing access, defining security boundaries, and enforcing communication policies.

This R&D document provides a detailed explanation of the key components involved in managing Azure Virtual Network security. It also covers the concepts of public IPs, service tags, and network interfaces with step-by-step implementation.

2. Network Security Group (NSG)

2.1 Overview of NSG

A Network Security Group (NSG) is a logical firewall in Azure. It controls access to network interfaces (NICs) and subnets by evaluating inbound and outbound traffic based on defined security rules.

2.2 Components of NSG Rules

Each NSG contains a set of rules that define:

- **Priority:** Determines rule evaluation order (lower number = higher priority).
- **Name:** A unique identifier for the rule.
- **Port/Protocol:** Specifies what traffic is allowed or denied.
- **Source/Destination:** Defines IP ranges or service tags involved.
- **Action:** Either Allow or Deny.

2.3 Default Rules in NSG

Azure automatically includes several default rules in every NSG:

- Allow traffic within the VNet.
- Allow Azure load balancer traffic.
- Deny all inbound internet traffic by default.

2.4 Custom Rules and Priorities

Custom rules can be created to override the default behavior. These should be assigned priorities lower than 65000. For example, a custom rule to allow RDP (port 3389) may use priority 100.

3. Application Security Groups (ASG)

3.1 Overview of ASG

Application Security Groups are used to group virtual machine network interfaces logically. ASGs simplify network rule definitions when working with large environments.

3.2 Use Case of ASG

Instead of specifying IP addresses of multiple VMs in NSG rules, you attach them to an ASG and reference the group in the rule.

For example:

"Allow traffic from ASG ‘WebServers’ to ASG ‘DBServers’ on port 1433 (SQL Server).”

3.3 ASG vs NSG

Feature	NSG	ASG
Function	Rule container	VM grouping
Use Case	Define access	Reference in NSG rules
Scope	Subnet/NIC	VM NIC only

4. Working of NSGs and ASGs

4.1 Flow of Evaluation

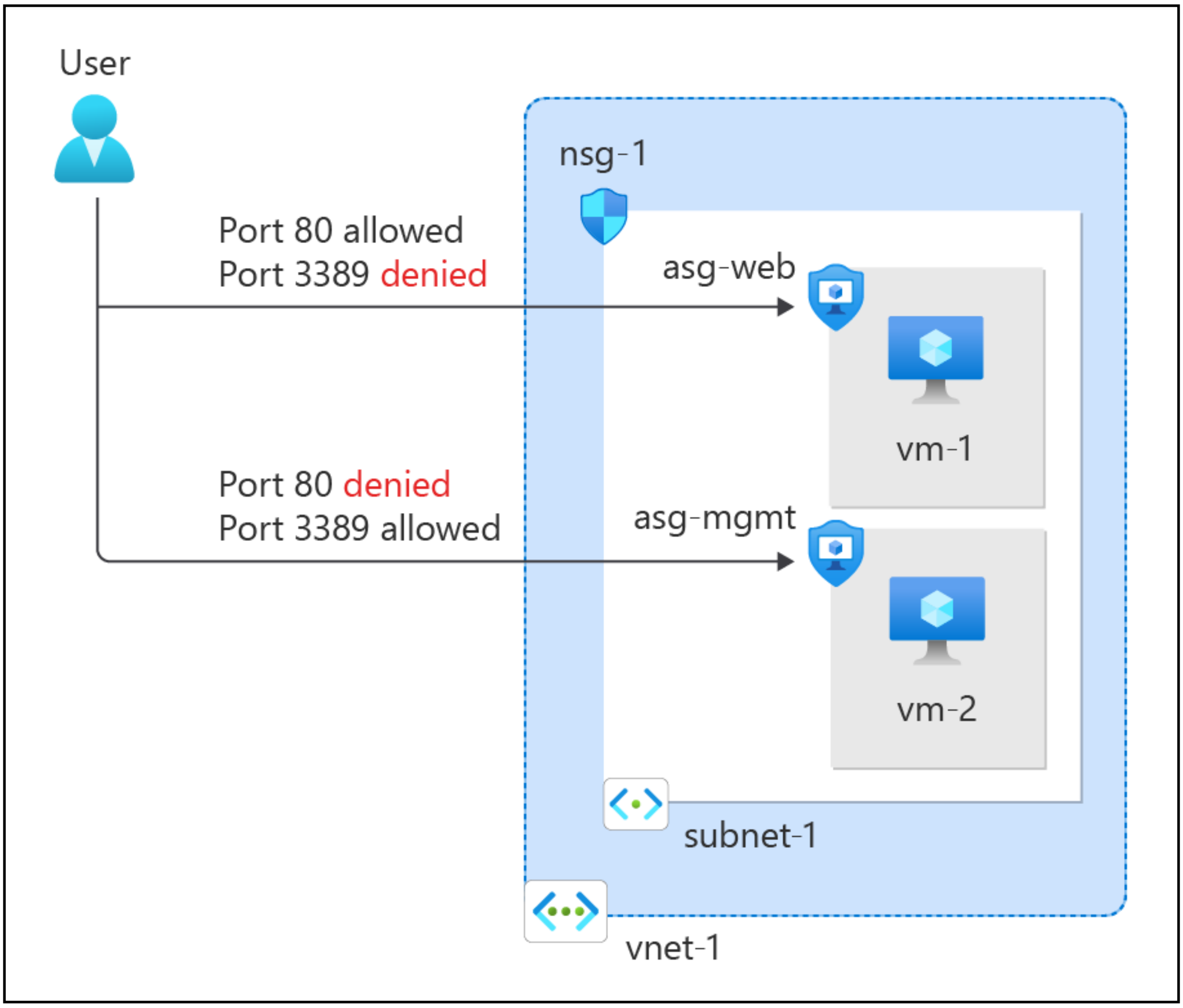
When a packet enters or leaves a VM, the following evaluation takes place:

- NSG rules at the **NIC level** are evaluated.
- NSG rules at the **subnet level** are evaluated.
- The rule with the **lowest priority number** is applied.

4.2 Practical Example of NSG + ASG

- VM1 (Web Server) is in ASG: Web-ASG
- VM2 (Database Server) is in ASG: DB-ASG
- NSG rule allows traffic from Web-ASG to DB-ASG on port 1433 (SQL)

This setup allows logical and scalable access management.



5. Allowing Specific IPs via NSG

5.1 Why Restrict by IP

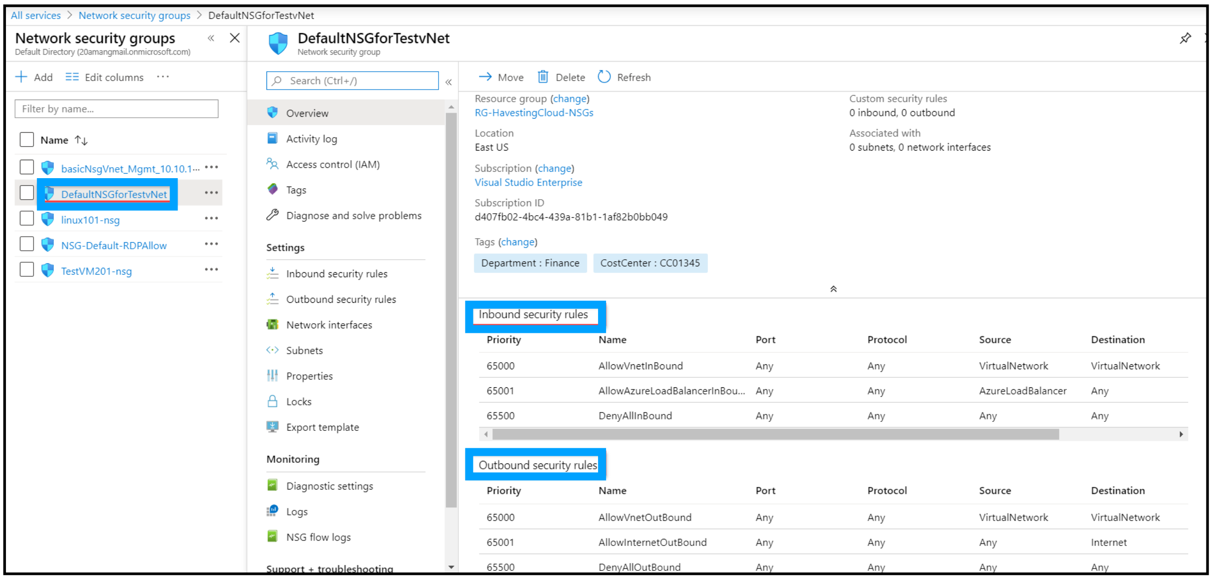
Allowing only specific IPs (e.g., admin machines) enhances security by preventing unauthorised users from accessing cloud resources.

5.2 How to Configure IP Restrictions

Steps:

1. Go to NSG → Inbound Rules → Add
2. Source: IP Address
3. Value: (e.g., 103.22.12.55)
4. Destination: VM
5. Port: 22 (Linux), 3389 (Windows)
6. Protocol: TCP
7. Action: Allow

8. Priority: 100



Resource group (change)
RG-HavestingCloud-NSGs

Location
East US

Subscription (change)
Visual Studio Enterprise

Subscription ID
d407fb02-4bc4-439a-81b1-1af82b0bb049

Tags (change)
Department : Finance
CostCenter : CC01345

Custom security rules
0 inbound, 0 outbound

Associated with
0 subnets, 0 network interfaces

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBou...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

5.3 Use Case for Secure Admin Access

This method is typically used to allow only IT administrators to SSH/RDP into VMs.

6. Denying Internet Access via NSG

6.1 Why Block Internet Access

In secured enterprise environments, some VMs (like backend or internal apps) should not have internet access.

6.2 Creating a Deny Rule

Steps:

1. Go to NSG → Outbound Rules → Add
2. Destination: 0.0.0.0/0 (entire internet)
3. Protocol: Any
4. Port: Any
5. Action: Deny
6. Priority: 100

6.3 Testing and Verification

Try accessing websites or performing a ping. It should fail due to the outbound restriction.

7. Public IPs in Azure

7.1 Overview

Public IPs allow Azure resources to be accessed from outside the Azure VNet.

7.2 Static vs Dynamic IPs

- **Static IPs** remain constant.
- **Dynamic IPs** may change after VM restart.

7.3 Choosing the Right IP Type

Use **Static** for production, DNS mapping, or when predictable IPs are required.

8. Azure Service Tags

8.1 What are Service Tags

Service Tags are abstracted labels representing groups of IPs, managed by Azure.

8.2 Common Service Tags

- Internet: Represents all external IPs.
- VirtualNetwork: IPs within the same VNet.
- AzureLoadBalancer: Azure's default load balancer traffic.

8.3 Benefits of Using Tags

They reduce complexity and keep NSG rules maintainable. No need to manually track IP ranges.

9. Allocating Static IPs to VMs

9.1 Static IP during Creation

While creating a VM:

- Go to "Networking"
- Under IP settings, select “Static”

9.2 Converting Dynamic to Static

Post-creation:

- Go to VM → Networking → NIC
- Open IP Configuration
- Change Assignment from “Dynamic” to “Static”

10. Creating Network Security Group (NSG)

10.1 Steps to Create

1. Azure Portal → Create a Resource → Network Security Group
2. Provide name, region, and resource group
3. Create

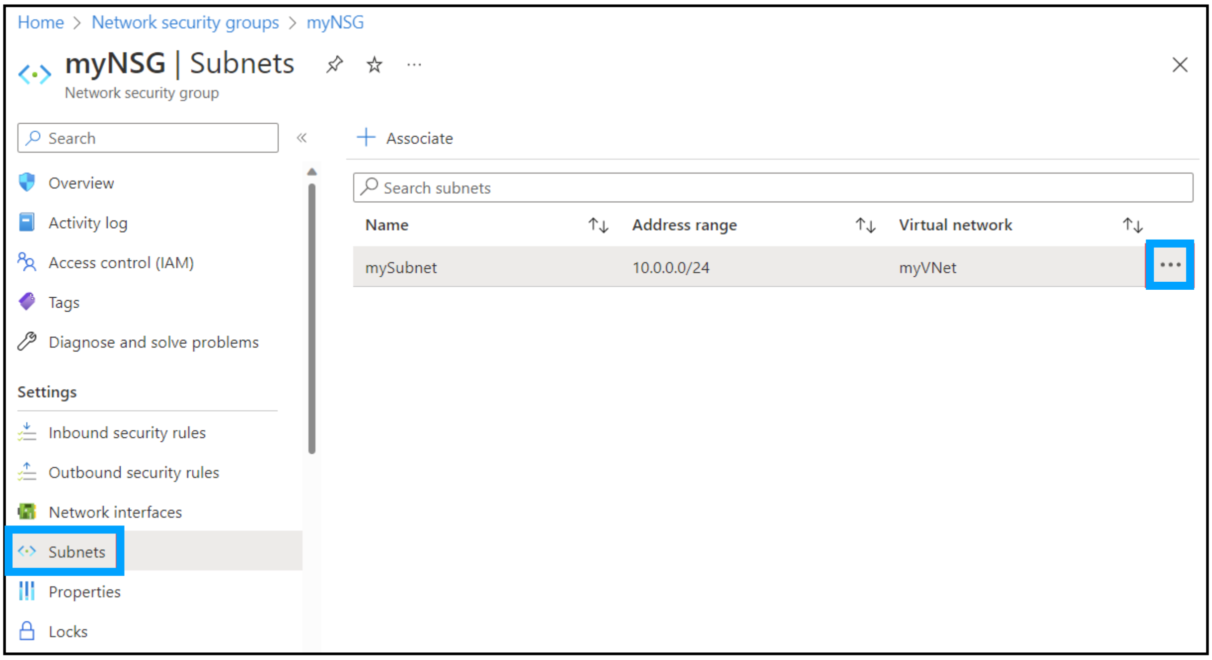
10.2 Associating NSG with Subnet or NIC

- To apply at subnet level:

  VNet → Subnet → NSG → Associate

- To apply at NIC level:

  VM → Networking → NIC → NSG → Associate



Name	Address range	Virtual network
mySubnet	10.0.0.0/24	myVNet

11. Creating and Associating Public IP

11.1 Steps to Create

1. Azure Portal → Create Resource → Networking → Public IP
2. Choose:
   - Assignment: Static
   - SKU: Basic or Standard

11.2 Steps to Associate

1. VM → Networking

2. Click on NIC → IP Config
3. Assign created Public IP

12. De-associating a Public IP

12.1 Use Case for De-association

To restrict the VM to internal-only communication (e.g., internal APIs).

12.2 Steps

1. VM → Networking → NIC
2. Open IP Config
3. Set Public IP = None → Save

13. Creating a Network Interface (NIC)

13.1 Purpose of NIC

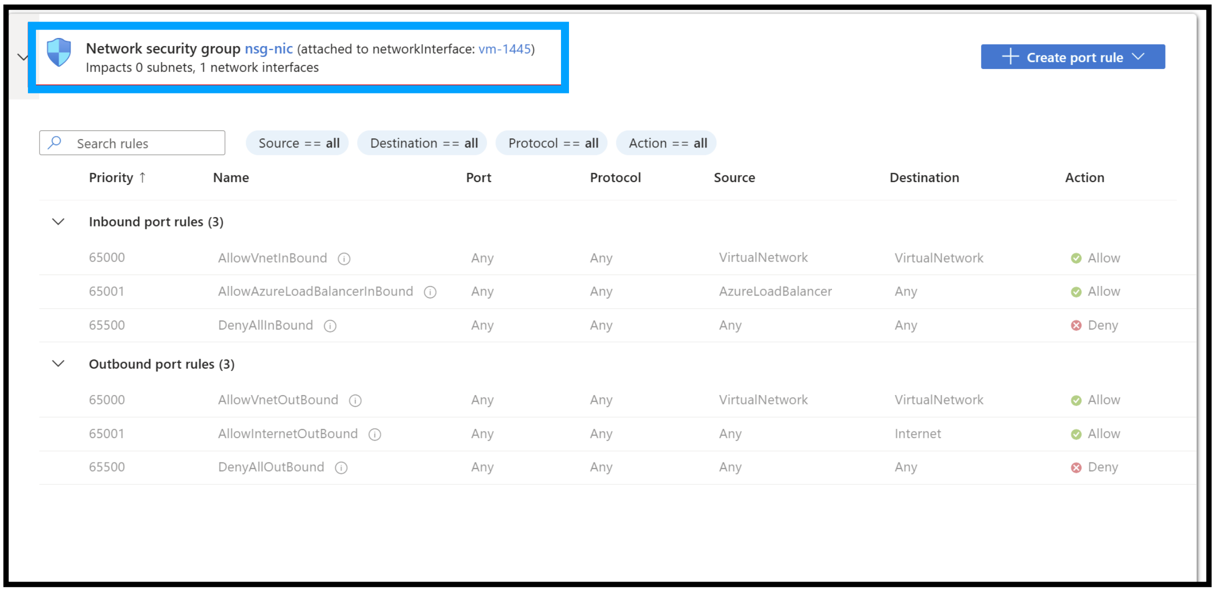
A NIC is required for any VM to communicate. Each NIC is assigned private/public IPs and security rules.

13.2 Steps to Create NIC

1. Azure Portal → Create → Networking → Network Interface
2. Provide name, VNet, Subnet
3. Associate NSG and IP Config
4. Save

14. Practical Implementation Steps

1. Create two VMs (Linux + Windows) in the same VNet.
2. Assign Static Public IPs to both.
3. Create NSGs and attach to each VM's NIC.
4. Add inbound rule allowing only specific IPs.
5. Add outbound rule denying internet on one VM.
6. Create ASGs, assign VMs.
7. Create NSG rules based on ASG communication.
8. Test SSH/RDP and Internet access.
9. Create a separate NIC and assign it to a VM.



Network security group nsg-nic (attached to networkInterface: vm-1445)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (3)						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound port rules (3)						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

15. Conclusion

In this week's task, we explored network security capabilities in Azure through NSGs, ASGs, and public IP configurations. We learned how to allow selective access, block internet traffic, manage IP assignments, and apply group-based security using ASGs. These tools form the foundation of secure, scalable, and well-governed cloud environments.

16. References

1. Azure NSG Documentation
   https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview
2. Azure ASG Documentation
   https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups
3. IP Address Types in Azure
   https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-ip-addresses-overview-arm
4. Service Tags in Azure
   https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview
5. Create and Manage Azure NICs
   https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface