A R&D report

on

Working of NSG & ASG

Submitted to **Celebal Technologies** in partial fulfillment of the internship task

Week 5

in

Cloud Infra and Security

By

Mr. Ganesh Ghadge

StudentId: CT_CSI_CI_6124

Objective

This document aims to provide a comprehensive understanding of advanced networking configurations in Microsoft Azure, with a focus on controlling and managing network access using Network Security Groups (NSGs), Application Security Groups (ASGs), and Public IP management.

The objectives are:

- Understand the functionality and configuration of Network Security Groups (NSGs) for securing VM-level and subnet-level traffic.
- Learn how Application Security Groups (ASGs) simplify and scale NSG rule management.
- Implement network access control by allowing traffic only from specific IP addresses.
- Deny internet access to virtual machines while still allowing private network traffic.
- Explore Azure Public IPs, their types (Static and Dynamic), and use cases.
- Understand Azure service tags and their role in NSG rules.
- Allocate static Public IPs to virtual machines for consistent access.
- Perform practical deployments such as:
    - Creating NSGs and associating them with subnets or NICs
    - Creating Public IPs (Static and Dynamic)
    - Associating and de-associating Public IPs from VMs
    - Creating and managing Network Interfaces

Introduction

Microsoft Azure provides a highly flexible and secure networking framework for deploying and managing cloud infrastructure. Among the most critical components in Azure networking are **Network Security Groups (NSGs)**, **Application Security Groups (ASGs)**, and **Public IP addressing**, which together help control how and where traffic flows to and from Azure resources.

While Virtual Networks (VNets) and subnets define the structure of your Azure network, **NSGs and ASGs act as firewalls**, determining **who can talk to whom** and under what conditions. With **NSGs**, administrators can allow or deny traffic based on rules defined by **source/destination IPs, ports, protocols, and Azure service tags**. ASGs make rule management easier and more scalable by grouping VMs logically rather than individually by IP.

In modern enterprise environments, it's often necessary to:

- Restrict access to VMs by IP (e.g., allow only corporate IP ranges),
- Prevent virtual machines from accessing the public internet while still communicating within the private network.
- Assign **static public IPs** to maintain consistent external endpoints,
- Use **dynamic public IPs** for cost efficiency when persistence is not needed.

Working of NSG (Network Security Group)

A Network Security Group (NSG) is a virtual firewall in Microsoft Azure that controls inbound and outbound traffic to and from Azure resources. It consists of a set of security rules that allow or deny traffic based on source/destination IP addresses, port numbers, protocols, and service tags.

NSGs can be associated with either of the following:

- Subnets – to control traffic at the subnet level (affects all resources inside).
- Network Interfaces (NICs) – to control traffic for individual VMs or resources.

Key Components

Component	Description
Name	Identifier for the NSG.
Priority	Rule processing order (lower number = higher priority).
Source/Destination	Can be IP addresses, IP ranges, or Azure service tags (e.g., Internet).
Protocol	TCP, UDP, or Any.
Port Range	The destination or source port(s).
Action	Allow or Deny.
Direction	Inbound or Outbound.

Default Rules

Priority	Name	Source	Destination	Protocol	Action	Description
65000	AllowVNetInBound	VirtualNetwork	VirtualNetwork	Any	Allow	Allow traffic within the VNet

65001	AllowAzureLoadBalancer	AzureLoadBalancer	Any	Any	Allow	Required for load balancer health probes
65500	DenyAllInBound	Any	Any	Any	Deny	Deny all other inbound traffic
65000	AllowVNetOutBound	VirtualNetwork	VirtualNetwork	Any	Allow	Allow outbound within the VNet
65001	AllowInternetOutBound	Any	Internet	Any	Allow	Allow outbound to the internet
65500	DenyAllOutBound	Any	Any	Any	Deny	Deny all other outbound traffic

Common Use Cases

- Allow SSH (port 22) from a specific IP to a Linux VM.
- Allow RDP (port 3389) only from a corporate IP to a Windows VM.
- Deny all internet access to a VM (by overriding default outbound rules).
- Allow app-tier VMs to communicate only with DB-tier VMs (using subnet-level NSGs).

Working of ASG (Application Security Group)

An **Application Security Group (ASG)** is a logical grouping of Azure virtual machine **network interfaces (NICs)**, used to simplify the management of **NSG rules**. Instead of writing separate NSG rules for each VM IP, you can assign VMs to ASGs and create NSG rules **targeting ASGs directly**.

ASGs allow for **dynamic, scalable, and tag-based security** without worrying about static IP addresses.

Key Benefits

Feature	Description
Dynamic Membership	VMs can be added/removed from ASGs without updating NSG rules.
Simplified NSG Rules	Write rules based on group names instead of IPs.
Scalability	Manage security policies across large numbers of VMs.
Layered Architecture Support	Define traffic rules between app tiers (web → app → DB) using ASGs.

How ASG Works with NSG

You cannot apply NSGs to ASGs. Instead, you reference ASGs within NSG rules as either the source or destination.
For example:

- Allow traffic from Web-ASG to App-ASG on port 443 (HTTPS).
- Deny traffic from any ASG to DB-ASG except from App-ASG.

ASG Limitations

Limitation	Detail
Same VNet only	ASGs and VMs must be in the same VNet.
No ASG-to-ASG peering	Cannot reference ASGs across VNets using peering.
Only works with NICs	ASGs work at the **NIC level**, not the subnet level.

Controlling Access with NSGs – Allow Specific IPs & Deny Internet

Allowing Specific IPs to Access VMs

To restrict access to VMs (e.g., for SSH or RDP), you can configure **NSG inbound rules** allowing only specific **source IP addresses**. This is critical for securing VMs from unwanted public exposure.

Property	Value
Direction	Inbound
Source	IP Addresses
Source IP	203.0.113.10
Destination	Any
Port	22 (for SSH)
Protocol	TCP
Action	Allow
Priority	100

Denying Internet Access to VMs

By default, outbound traffic to the internet is allowed. To block internet access, override the default outbound rule in the NSG with a higher-priority deny rule:

Property	Value
Direction	Outbound
Destination	Internet
Protocol	Any
Action	Deny
Priority	100

Public IPs – Types (Static/Dynamic), Service Tags, and Static IP Allocation

Public IPs – Static vs. Dynamic

Azure provides Public IP addresses to enable communication between your VMs and the internet or external systems.

Type	Description
Dynamic	Assigned at VM start, may change on reboot. Suitable for non-critical services.
Static	Fixed IP address persists through restarts. Ideal for DNS mapping, firewall allowlists, or production apps.

Service Tags in NSGs

Service Tags are predefined identifiers in NSG rules that represent Azure services or IP ranges, eliminating the need to manually track IPs.

Common Tags:

- Internet – all public IPs
- VirtualNetwork – all IPs within your VNet
- AzureLoadBalancer – used for health probe traffic
- Storage, AppGateway, etc.

Allocating Static IPs to VMs

To ensure consistent addressing:

- Create a Static Public IP:
    - Azure Portal → Public IP Addresses → +Create
    - SKU: Standard (recommended for production)
    - Assignment: Static
- Associate it with a VM's NIC during or after creation.
- Optionally, assign a private static IP from the subnet range by configuring the NIC.

Creating NSG, Public IP, Associating/Deassociating PIP, and NIC

Creating a Network Security Group (NSG)

To create and configure an NSG:

- Go to Azure Portal → Search for Network Security Groups → Click + Create.
- Fill in the basics:
    - Subscription & Resource Group
    - Name: e.g., nsg-web
    - Region: Match your VM/VNet location
- After creation, add inbound/outbound rules (e.g., allow SSH/RDP, deny internet).
- Associate the NSG:
    - To a Subnet (applies to all VMs in it), or
    - To a NIC (applies only to that VM)

Creating a Public IP

Associate / De-associate Public IP from a VM

- To associate a Public IP with a VM:
    - Go to Virtual Machines → Select your VM → Networking tab.
    - Click on the attached NIC → Go to IP Configurations.
    - Click the config (e.g., ipconfig1) → Select your Public IP.
    - Save.
- To remove the Public IP:
    - Set the Public IP to “None” in the IP configuration, then Save.

Creating a Network Interface (NIC)

NICs act as the bridge between a VM and the network. To create a NIC:

- Azure Portal → Search Network Interfaces → + Create.
- Configure:
    - Name: e.g., nic-linuxvm
    - VNet & Subnet
    - Network Security Group (optional)
    - Public IP (optional)
    - Private IP: Static or Dynamic
- Save. This NIC can be attached during VM creation or manually via VM → Networking → Attach network interface.

References

1. Azure Network Security Groups (NSG) Overview
   https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview
2. Public IP Addresses in Azure
   https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses
3. Azure Service Tags
   https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview
4. Create, Change, or Delete a NIC in Azure
   https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface
5. Public IP Addresses in Azure
   https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses