Research & Development on Azure Networking Concepts

Objective

To explore and implement advanced Azure Networking tasks such as configuring NSG (Network Security Group), ASG (Application Security Group), assigning public IPs, controlling IP access, and managing network interfaces in a secure and efficient way.

PREPARED BY:

Richa Budhori

---

1. Network Security Group (NSG)

What is NSG?

An NSG is a firewall that controls inbound and outbound traffic at the subnet or NIC (Network Interface Card) level.

They are used to filter network traffic to and from azure resources within a virtual network.

Key Features:

- Contains security rules that allow or deny traffic based on 5-tuple rules: Source IP, Source Port, Destination IP, Destination Port, Protocol.

- It supports Service Tags and Application Security Groups.

- Acts like a stateless firewall (return traffic is automatically allowed for allowed traffic).

NSG Rule Types:

Rule	**Description**
Inbound Rules	Traffic entering VM/Subnet
Outbound Rules	Traffic leaving VM/Subnet

Priority:

Lower priority numbers are evaluated first. Rules are processed in order.

2. Application Security Group (ASG)

What is ASG?

An ASG simplifies management of security by grouping virtual machines (VMs) based on logical applications (e.g., web servers, backend APIs), and allowing to apply NSG rules to the group instead of individual IPs.

This makes it easier to manage large environments.

3. Allowing Specific IPs to Access VMs

To allow only specific IPs (e.g., developer machines or office static IPs):

1. Go to the NSG , then Inbound Security Rules
2. Create a rule:
   - Source: IP Addresses
   - Source IP Ranges: `203.0.113.5/32`
   - Destination Port: 22 (SSH) or 3389 (RDP)
   - Action: Allow

NSG rules are processed in order of priority (lower numbers first). A deny rule with higher priority will override subsequent allow rules.

4. Denying Internet Access Using NSG

To deny internet access: Add a rule with "Service Tag: Internet" as the source, set action to "Deny", and assign a higher priority (lower number) than allow rules:

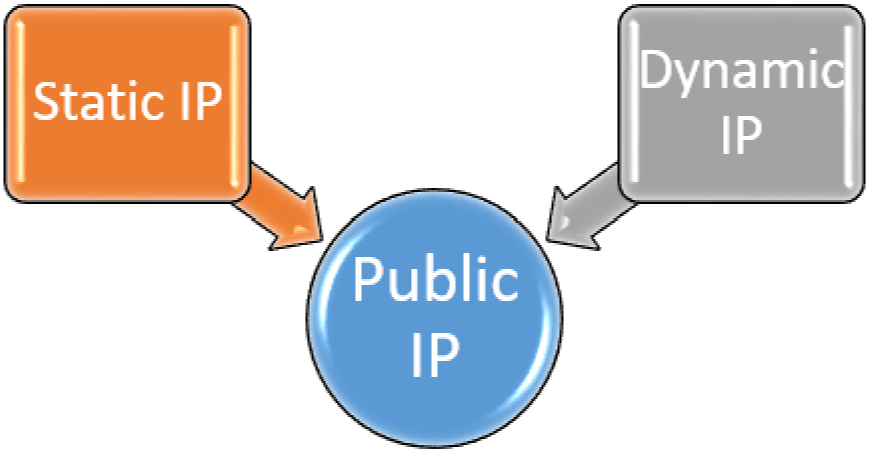
1. Go to NSG => **Outbound Rules**
2. Add a rule:
   - **Destination**: Service Tag = Internet
   - **Action**: Deny
   - **Priority**: Lower than default allow rule (e.g., 100)
   - **Port**: *
   - **Protocol**: Any

5. Public IPs and Their Types

What is a Public IP?

A **Public IP** enables internet connectivity to Azure resources.

Types of Public IPs:



6. Static vs Dynamic IP Allocation

Type	Static	Dynamic
Assignment	Fixed at creation	Assigned on association
Change on restart	No	Yes
Use cases	DNS, Firewall rules, TLS	Non-critical, temporary
Supported SKUs	Standard (IPv4/ IPv6), Basic (IPv4)	Basic(IPv4/IPv6)

- Static IPs are recommended for scenarios where IP consistency is required, such as DNS records, firewall rules, or certificate binding.
- Dynamic IPs are suitable where IP changes are acceptable, and are released/reassigned when the VM stops or restarts.

7. Service Tags

What are Service Tags?

Service Tags are predefined identifiers in NSG rules that represent a group of IP address prefixes for specific microsoft services like:

- Internet
- VirtualNetwork
- AzureLoadBalancer
- Storage.region

They simplify NSG rule creation management by avoiding manual IP range updates.

8. Allocating Static IPs to All VMs

To assign a static **private IP** to VMs:

1. Go to VM => Networking => Network Interface
2. Select IP Configurations
3. Change Assignment from Dynamic to Static
4. Enter desired IP (within subnet range)

For static **public IP**:

- Create a new Public IP with Static SKU
- Associate with VM (see below)

9. Creating a Network Security Group

Steps:

1. Go to Azure Portal and search "Network Security Group"
2. Click Create
   - Resource Group: Choose existing/new
   - Name: nsg-web
   - Region: Match VM/Subnet
3. Add Inbound/Outbound rules
4. Associate NSG to Subnet or Network Interface and finally review + create.

10. Creating Public IP

Steps:

1. Go to Azure Portal => Create Resource => Search Public IP address
2. Click Create
   - Name: publicIP-vm1
   - SKU: Basic or Standard
   - Assignment: Static or Dynamic
   - IP Version: IPv4
3. Click Review + Create

11. Associating / De-associating Public IP with VM

Associating:

1. VM > Networking > Network Interface > IP Configurations
2. Click IP config (e.g., ipconfig1)
3. Under Public IP Address, select your Public IP
4. Save

De-associating:

- Set Public IP to None and Save

12. Creating a Network Interface (NIC)

What is NIC?

A Network Interface connects your VM to a Virtual Network.

Steps:

1. Go to Azure Portal => Search Network Interface
2. Click Create
   - Name: nic-web
   - VNet/Subnet: Choose existing
   - NSG: Optional
   - IP Config: Set static if needed
3. Assign NIC to a new VM or during VM creation

Conclusion

Understanding how **NSGs**, **ASGs**, **IP allocation**, and **Public IPs** work is essential for securing and managing Azure VMs efficiently.These elements are critical in deploying secure cloud applications.