**CSI ASSIGNMENT 5**

**AZURE NETWORKING**

# 1. Network Security Groups (NSG)

## Definition:

A Network Security Group (NSG) is a critical Azure component that acts as a firewall, controlling both inbound and outbound traffic to Azure resources. It enables granular filtering of traffic at both the subnet and the network interface card (NIC) level.

In Azure, a Network Security Group (NSG) acts as a virtual firewall that filters network traffic to and from Azure resources within a virtual network. It controls inbound and outbound traffic based on security rules defined by the user. These rules specify allowed or denied traffic based on criteria like IP addresses, ports, and protocols.

## Features:

- Supports 1000 rules per NSG
- Prioritized rule evaluation (lower number = higher priority)
- Supports service tags and application security groups

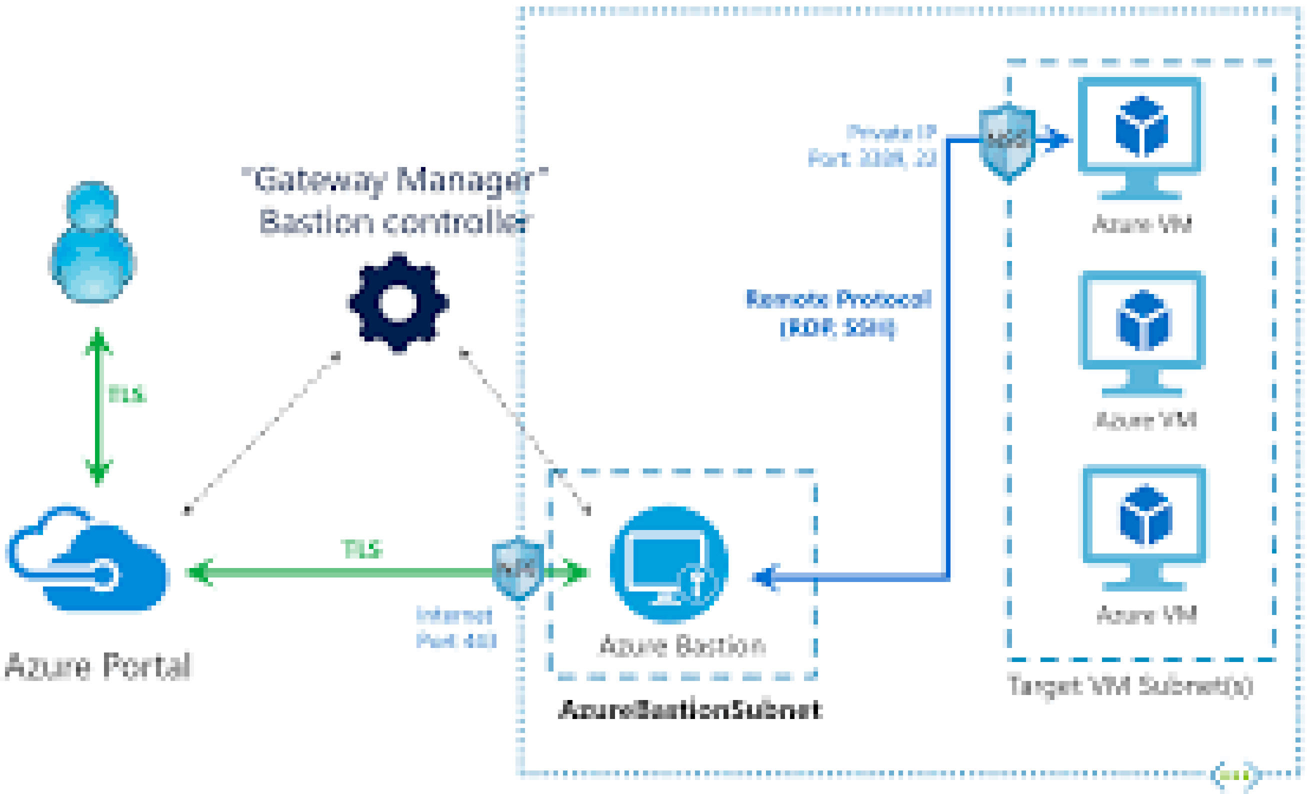
## Steps to Create NSG:

1. Navigate to **Azure Portal > Networking > Network Security Groups**.
2. Click **+ Create** to begin the wizard.
3. Select the appropriate **Subscription** and **Resource Group**.
4. Enter a **name** for the NSG (e.g., Prod-VM-NSG).
5. Choose the **Region** matching your VMs.
6. Click **Review + Create**, then **Create** to deploy the NSG.

## Best Practices:

- Apply NSG at the subnet level for broad controls.
- Use NIC-level NSGs for specific VM control.
- Always document rules for audit and debugging purposes.

Working  of NGS:



## 2. Application Security Groups (ASG)

### Definition:

Application Security Groups (ASGs) allow you to group VMs logically and apply security rules collectively through NSGs. ASGs remove the need to maintain individual IP addresses in rules.

An application group controls access to a full desktop or a logical grouping of applications that are available on session hosts in a single host pool. Users can be assigned to multiple application groups across multiple host pools, which enable you to vary the applications and desktops that users can access.

## Benefits:

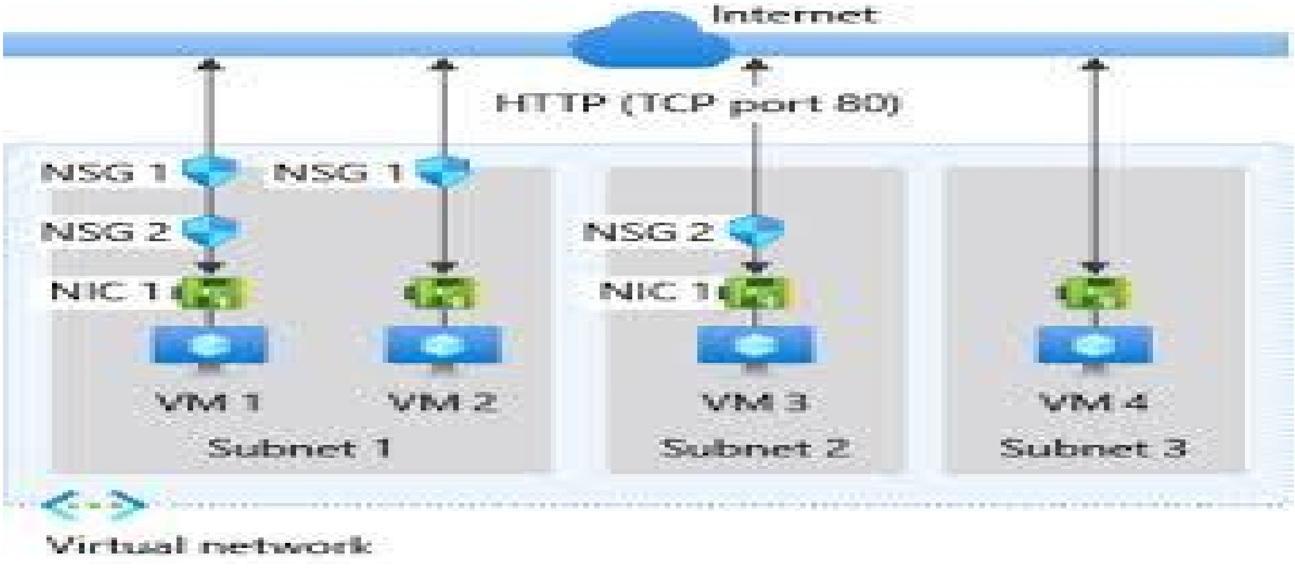
- Simplified management of security rules
- Logical groupings that reflect application architecture

## Steps to Create ASG:

1. Go to **Azure Portal > Networking > Application Security Groups**.
2. Click **+ Create**.
3. Select **Subscription**, **Resource Group**, and a meaningful **Name** (e.g., `WebTierASG`).
4. Choose the **Region** of your VMs.
5. Click **Review + Create**, then **Create**.

## Adding VMs to ASG:

1. Navigate to the VM's **Networking blade**.
2. Under **Network Interface**, click **IP Configurations**.
3. Select **Application security group** and choose your ASG.
4. Save changes.



# 3. Allow Specific IPs to Access VMs Using NSG

## Scenario:

You want to restrict VM access to a specific corporate office IP (e.g., `203.0.113.5`).

## Steps:

1. Go to the NSG associated with the VM or subnet.
2. Select **Inbound Security Rules > + Add**.
3. Set the following fields:
   - **Source**: IP Addresses
   - **Source IP addresses/CIDR ranges**: `203.0.113.5/32`
   - **Destination**: Any (or a specific IP if needed)
   - **Destination port ranges**: `22` for SSH or `3389` for RDP
   - **Protocol**: TCP
   - **Action**: Allow
   - **Priority**: e.g., `100`
   - **Name**: `Allow-Corp-IP`
4. Click **Add**.

## Validation:

Test access from the specified IP and confirm the connection. Ensure default deny rules are in place.

# 4. Deny Internet Access Using NSG

## Scenario:

Block all outbound internet traffic while allowing internal communication.

## Steps:

1. Navigate to the NSG and open **Outbound Security Rules**.
2. Click **+ Add**.
3. Set the rule to:
    - **Source**: Any
    - **Destination**: Service Tag > `Internet`
    - **Protocol**: Any
    - **Port range**: `*`
    - **Action**: Deny
    - **Priority**: `100`
    - **Name**: `Deny-Internet`
4. Save the rule.

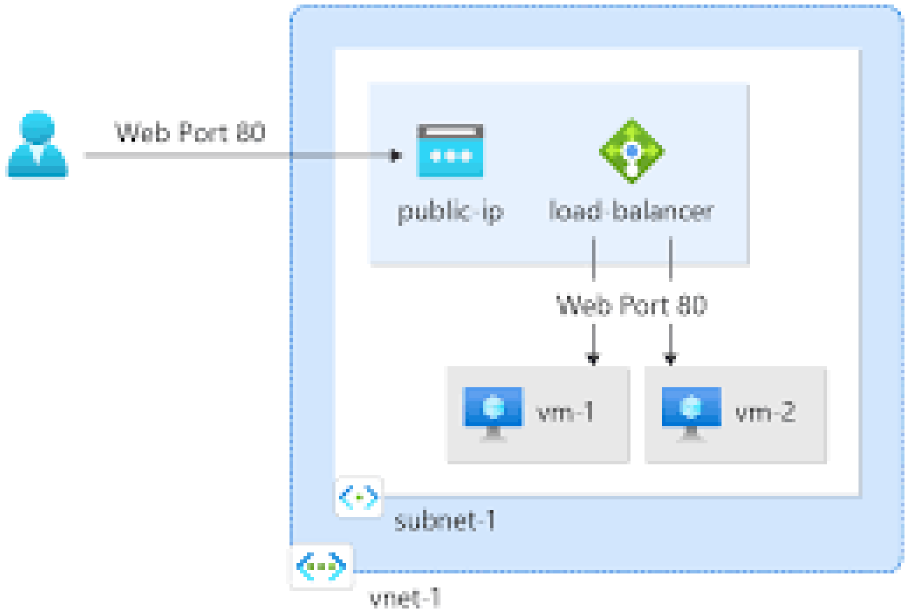
# 5. Public IPs in Azure

## What is a Public IP?

A Public IP allows Azure resources to communicate over the internet. It can be attached to VMs, Load Balancers, and Azure Firewalls.

## Use Cases:

- Remote access to VMs
- Hosting public-facing services
- NAT (Network Address Translation)



## 6. Types of Public IPs: Static vs Dynamic

| Type | Behavior | Use Case |
|---|---|---|
| Static | IP remains constant throughout resource life | DNS configuration, white-listing |
| Dynamic | IP may change on deallocation | Temporary VMs or dev use |

### How to Choose:

- Use **Static** for production and critical apps
- Use **Dynamic** for short-lived or internal-only apps

# 7. Service Tags in Azure

## What are Service Tags?

Service Tags represent a group of IP address prefixes from Azure services like Storage, SQL, and AzureMonitor.

A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

### Examples:

- `VirtualNetwork`
- `AzureLoadBalancer`
- `Internet`
- `Storage`

### Benefits:

- Automatically updated by Microsoft
- Avoids hard-coding IP ranges in NSG rules

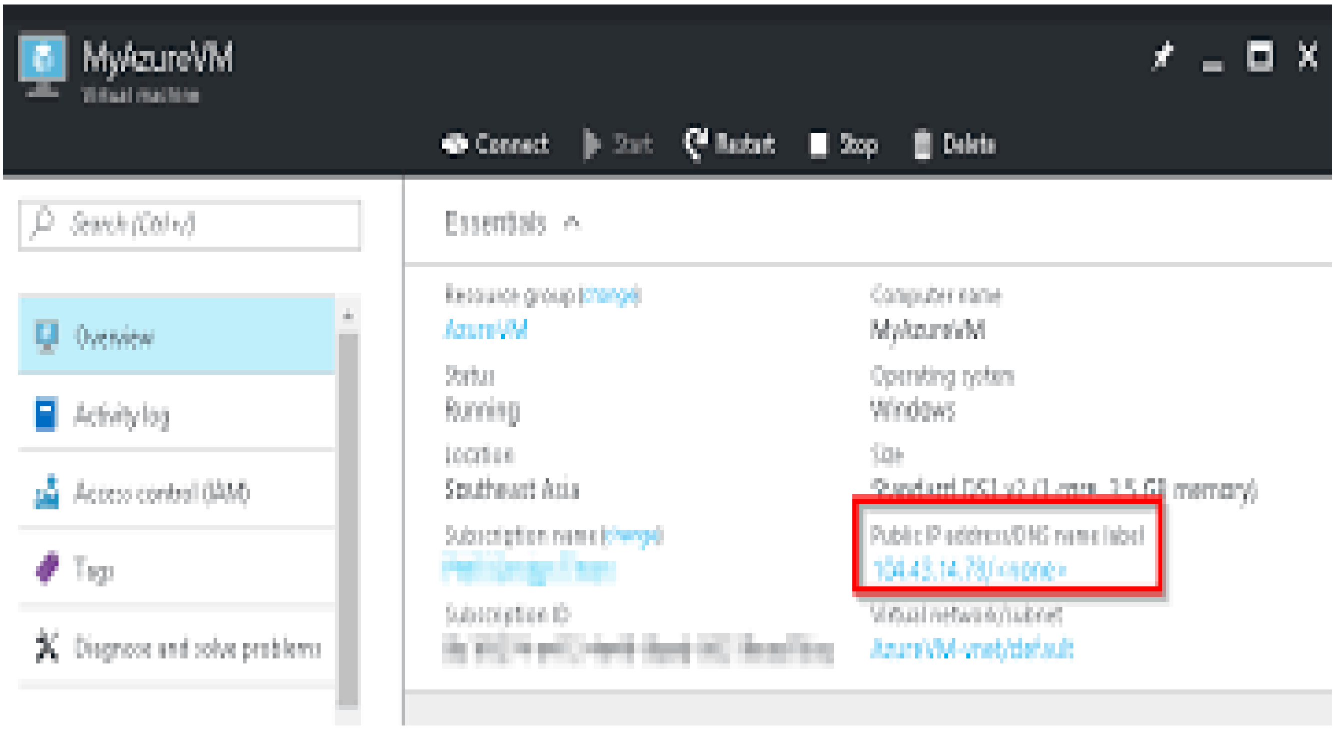
### How to Use:

1. In NSG rule creation, select **Destination** as **Service Tag**
2. Choose from available tags

# 8. Allocate Static IPs to VMs

## Steps:

1. Navigate to the **Virtual Machine > Networking > Network Interface**.
2. Click on the associated NIC.
3. Go to **IP Configurations**.
4. Select the current configuration.
5. Change **Assignment** to Static.
6. Enter a valid IP address (from subnet range).
7. Save the configuration.



Resource group (change)
AzureVM

Computer name
MyAzureVM

Status
Running

Operating system
Windows

Location
Southeast Asia

Size
Standard DS1 v2 (1 core, 3.5 GB memory)

Subscription name (change)
[redacted]

Public IP address/DNS name label
104.43.14.78/<none>

Subscription ID
[redacted]

Virtual network/subnet
AzureVM-vnet/default

# 10. Creating a Public IP Address

## Steps:

1. Navigate to **Azure Portal > Networking > Public IP Addresses**.
2. Click **+ Create**.
3. Fill in the following:
   - **Name**: `MyPublicIP`
   - **SKU**: Standard
   - **Assignment**: Static or Dynamic
   - **IP Version**: IPv4 (default)
   - **DNS name label** (optional)
4. Assign to a **Resource Group** and Region.
5. Click **Review + Create**, then **Create**.

# 11. Associating / De-associating Public IP with a Virtual Machine

## To Associate:

1. Go to **Virtual Machine > Networking**.
2. Click on the **Network Interface** link.
3. Navigate to **IP Configurations**.
4. Click on the current configuration.
5. Under Public IP, click **Associate** and select an existing Public IP or create a new one.

### To De-associate:

1. Open the NIC configuration as above.
2. Under Public IP, click **None** to remove association.

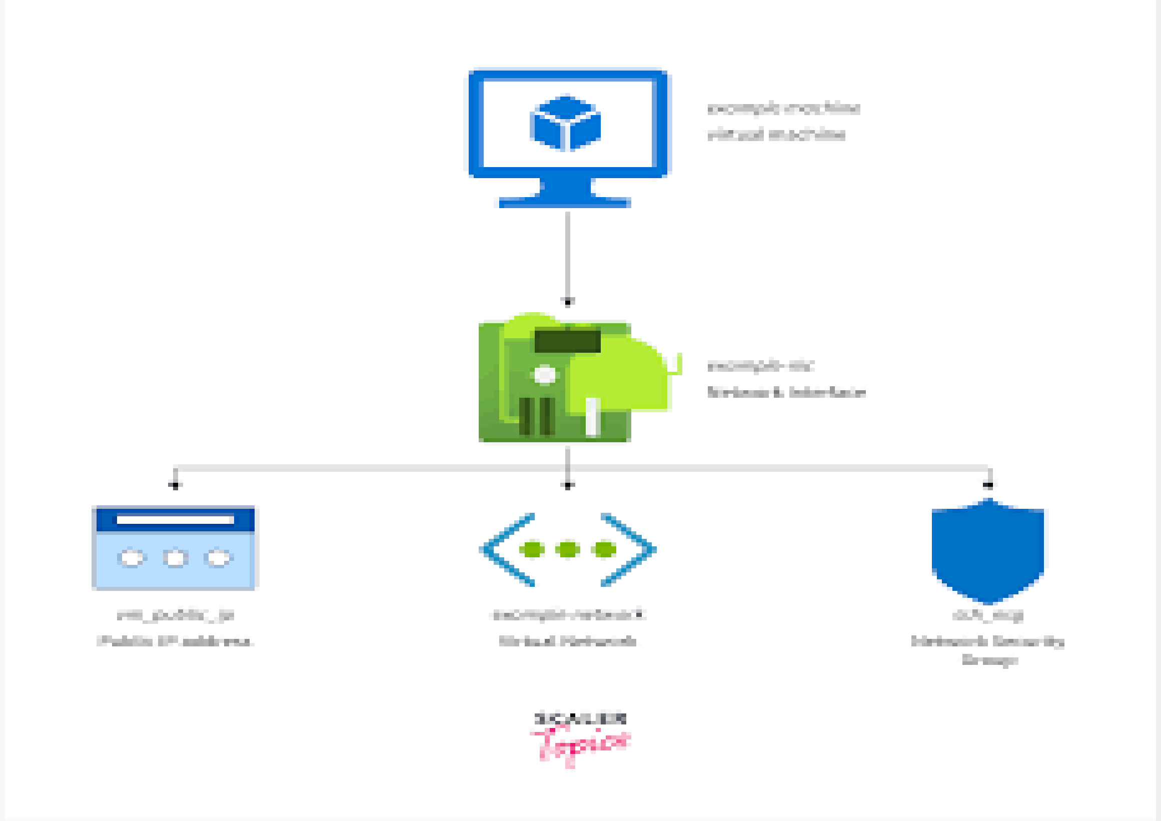
CSI ASSIGNMENT 5

AZURE NETWORKING

# 12. Creating a Network Interface (NIC) in Azure

## Steps:

1. Go to **Azure Portal > Networking > Network Interfaces**.
2. Click **+ Create**.
3. Fill in the following:
    - **Name**: `WebServerNIC`
    - **Virtual Network**: Select existing VNet
    - **Subnet**: Choose subnet
    - **NSG**: Attach a security group
    - **Private IP**: Static or Dynamic
    - **Public IP**: Optional
4. Assign to **Resource Group** and Region.
5. Click **Review + Create**.


example-machine
virtual machine
example-nic
Network Interface
vm_public_ip
Public IP address
example-network
Virtual Network
Network Security Group
SCALER Topics