

# **R&D Document: Azure Networking – NSG, ASG, IP Management & Public Access**

Tushar Bhosale

July 6, 2025

## **Contents**

<b>1</b>	<b>Network Security Group (NSG)</b>	<b>2</b>
<b>2</b>	<b>Application Security Group (ASG)</b>	<b>3</b>
<b>3</b>	<b>Allowing Specific IPs to Access VM</b>	<b>4</b>
<b>4</b>	<b>Deny Internet Access to VM Using NSG</b>	<b>5</b>
<b>5</b>	<b>Public IPs and Their Types</b>	<b>5</b>
<b>6</b>	<b>Allocate Static IPs to All VMs</b>	<b>5</b>
<b>7</b>	<b>Service Tags</b>	<b>5</b>
<b>8</b>	<b>Associate/De-associate Public IP with VM</b>	<b>6</b>
<b>9</b>	<b>Create a Network Interface</b>	<b>6</b>

# 1 Network Security Group (NSG)

## Purpose

Controls inbound and outbound traffic to/from Azure resources at subnet or NIC level.

## Working

- NSG contains **security rules** with Allow or Deny actions.
- Rules have priorities; lower numbers are higher priority.
- Azure processes rules in order until a match is found.

## Creation Steps

1. Go to Azure Portal → Search for *Network Security Groups* → Click **Create**.
2. Assign Subscription, Resource Group, Region, and Name.
3. Associate the NSG with either a Subnet or Network Interface (NIC).

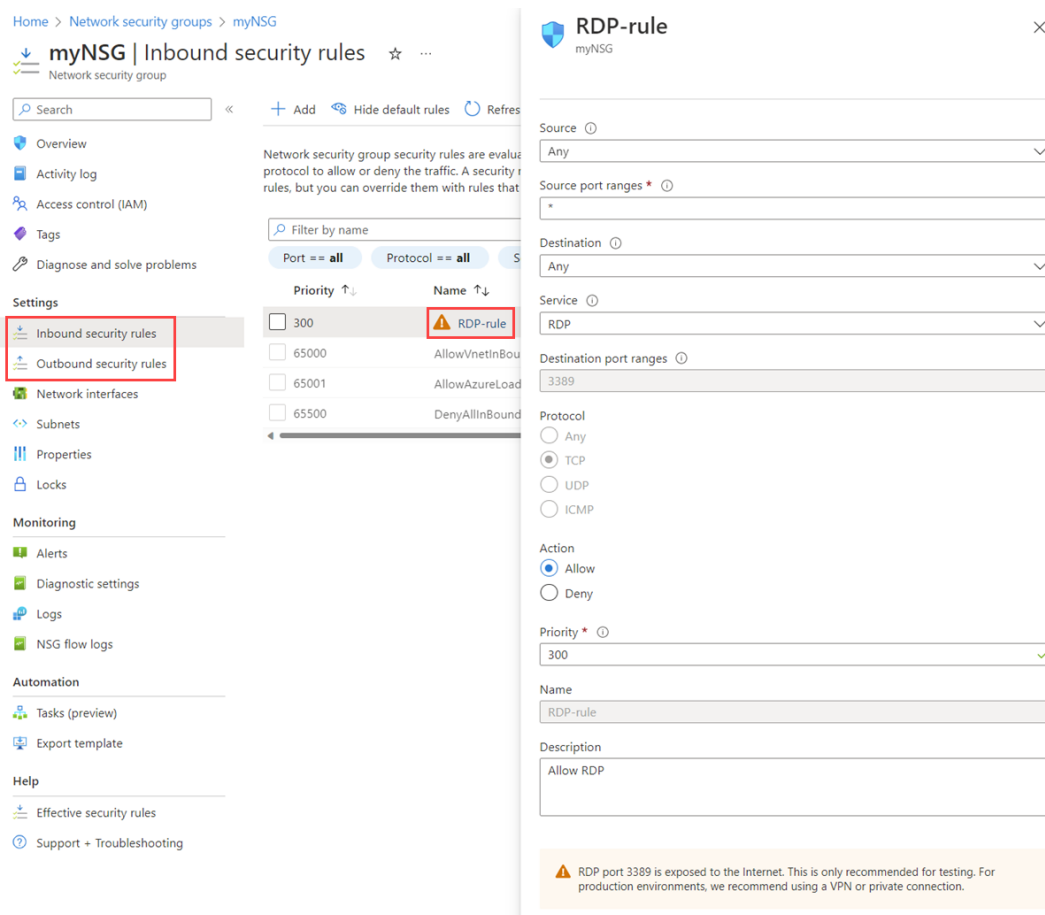


Figure 1: Creating a Network Security Group (NSG)

## 2 Application Security Group (ASG)

### Purpose

Logical grouping of virtual machines (VMs) for simplified NSG rule management.

### Working

- Create ASGs and assign them to NICs of VMs.
- Use ASGs in NSG rules instead of individual IPs.

### Example

- Create ASGs: *Web-ASG* and *DB-ASG*.
- Allow Web-ASG to access DB-ASG on port 1433 (SQL).

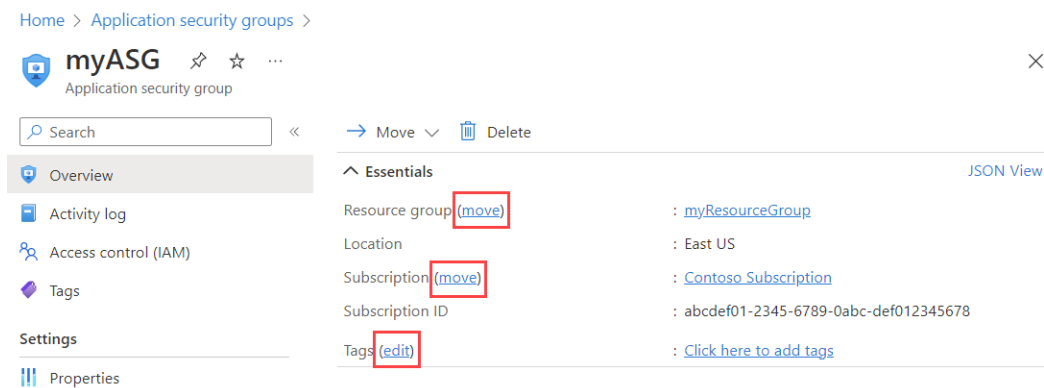


Figure 2: Assigning ASG and Using it in NSG Rule

### 3 Allowing Specific IPs to Access VM

#### Use Case

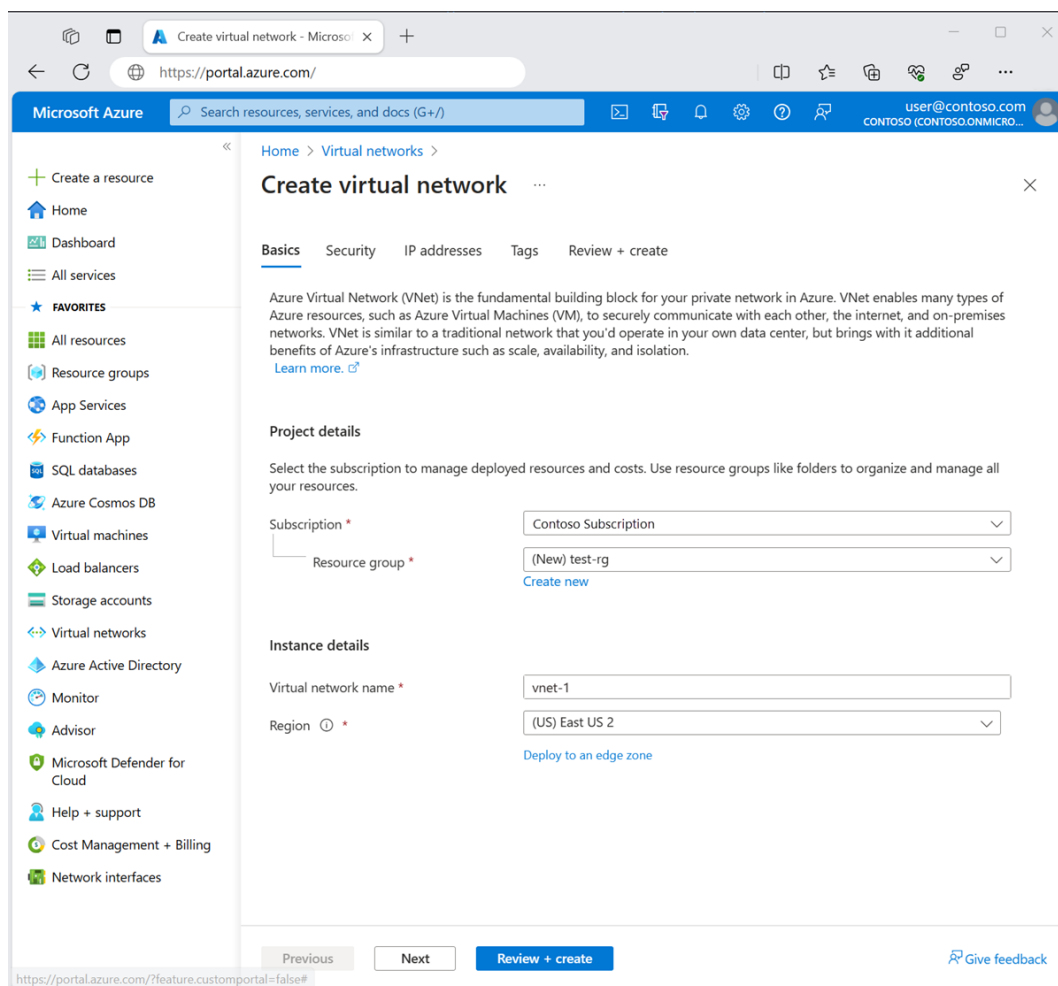
Restrict SSH/RDP/HTTP access to known IPs like your home/office.

#### Steps

1. In NSG → Inbound Rules → Add Rule.
2. Source: *IP Addresses*, Source IP: e.g., 203.0.113.5.
3. Destination Port Range: 3389 (RDP) or 22 (SSH).
4. Action: **Allow**, Priority: e.g., 100.

#### Deny Others

Use the default `DenyAllInbound` rule or create a custom Deny rule below the Allow rule.



The screenshot shows the Microsoft Azure portal interface for creating a new virtual network. The left sidebar contains navigation links for various Azure services. The main content area is titled 'Create virtual network' and includes tabs for 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create'. The 'Basics' tab is active, displaying the following information:

- Project details:** Subscription is set to 'Contoso Subscription' and the Resource group is '(New) test-rg'.
- Instance details:** The Virtual network name is 'vnet-1' and the Region is '(US) East US 2'.

At the bottom of the form, there are buttons for 'Previous', 'Next', and 'Review + create'. A 'Give feedback' link is also present in the bottom right corner.

Figure 3: NSG Rule Allowing Specific IP

## 4 Deny Internet Access to VM Using NSG

### Steps

- Remove or Deny outbound rule to **Internet**.
- Ensure outbound rules only allow trusted internal IP ranges like 10.0.0.0/8.

### Result

The VM can communicate within the VNet but not with the external internet.

## 5 Public IPs and Their Types

### Types

- **Dynamic:** Assigned when VM is started, may change.
- **Static:** Fixed, reserved IP address.

### Steps to Create

1. Go to Azure Portal → Public IP Address → Create.
2. Choose SKU: *Basic/Standard*.
3. Choose IP Type: *Static/Dynamic*.
4. Associate with a VM or leave unattached for later.

## 6 Allocate Static IPs to All VMs

- Go to VM → Networking → Network Interface.
- Click on IP Configurations → Set Private IP as **Static**.
- Save and repeat for all VMs.

## 7 Service Tags

### Definition

Predefined tags representing groups of IP addresses for Microsoft services.

## Examples

- **Internet:** All public IP addresses.
- **VirtualNetwork:** All resources in the same virtual network.
- **AzureLoadBalancer:** Azure's internal LB IPs.

## Usage

Use these tags in NSG rules to simplify and secure access.

## 8 Associate/De-associate Public IP with VM

### Associate

1. Go to VM → Networking → Network Interface → IP Configurations.
2. Click existing configuration and assign public IP.

### De-associate

- In same panel, select Public IP: *None*.

## 9 Create a Network Interface

### Steps

1. Azure Portal → Search *Network Interfaces* → Create.
2. Provide:
  - Name
  - Virtual Network and Subnet
  - NSG (optional)
  - IP Configuration (Static/Dynamic)
3. Associate with VM during or after creation.

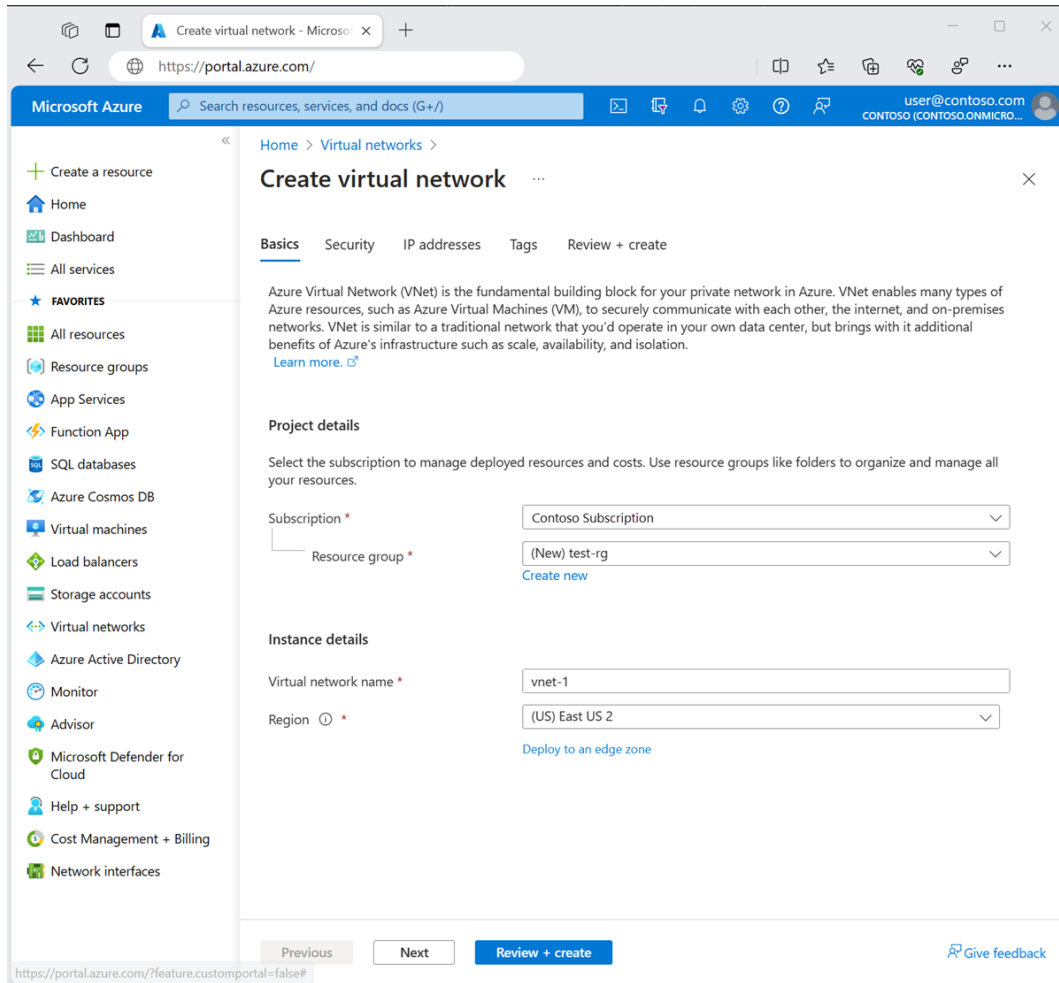


Figure 4: Outbound Rule to Deny Internet Access