# Research and Development Document: Networking and Security in Microsoft Azure

This document provides a comprehensive overview of key Azure networking and security components, including Network Security Groups (NSGs), Application Security Groups (ASGs), public IP addresses, static and dynamic IP allocation, service tags, and network interfaces. It addresses how to configure these components to allow specific IPs to access virtual machines (VMs), deny internet access, and manage IP assignments, with practical guidance for implementation.

## 1. Network Security Groups (NSGs)

### Overview

Network Security Groups (NSGs) are Azure resources that filter network traffic to and from resources within a virtual network (VNet). They contain security rules that allow or deny traffic based on a 5-tuple: source, source port, destination, destination port, and protocol. NSGs operate at Layer 4 of the OSI model and can be associated with subnets or individual network interfaces (NICs).

### How NSGs Work

- **Association**: NSGs can be applied to a subnet (affecting all resources in it) or a NIC (affecting a specific VM).
- **Rule Evaluation**: Rules are processed in priority order (100 to 4096, lower numbers = higher priority).
- **Default Rules**: Azure provides default rules that cannot be deleted but can be overridden by custom rules with higher priority.

### Default Security Rules

The following table outlines the default NSG rules:

| Rule Name | Priority | Source | Source Ports | Destination | Destination Ports | Protocol | Access |
|---|---|---|---|---|---|---|---|
| **Inbound Rules** | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AllowVNetInBound | 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |
| AllowAzureLoadBalancerInBound | 65001 | AzureLoadBalancer | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Allow |
| DenyAllInbound | 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |
| **Outbound Rules** | | | | | | | |
| AllowVNetOutBound | 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |
| AllowInternetOutBound | 65001 | 0.0.0.0/0 | 0-65535 | Internet | 0-65535 | Any | Allow |
| DenyAllOutBound | 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

- **Notes**:
  - "VirtualNetwork," "AzureLoadBalancer," and "Internet" are service tags, not specific IPs.
  - Protocol "Any" includes TCP, UDP, and ICMP.
  - Custom rules must have priorities between 100 and 4096 to override defaults.

## Creating an NSG

1. In the Azure portal, search for "Network Security Groups."
2. Click "Create."
3. Specify subscription, resource group, name, and region.
4. Click "Review + create," then "Create."
5. After creation, add rules via the "Inbound security rules" or "Outbound security rules" sections.

## Associating an NSG

6. **With a Subnet**: Navigate to the VNet, select the subnet, and under "Network security group," choose the NSG.
7. **With a NIC**: In the VM's NIC settings, under "Network security group," select the NSG.

*Reference*: Azure Network Security Groups Overview

## 2. Application Security Groups (ASGs)

### Overview

Application Security Groups (ASGs) simplify NSG rule management by grouping VMs based on application roles (e.g., web servers, database servers). ASGs are referenced in NSG rules as source or destination, reducing the need to manage individual IP addresses.

### How ASGs Work

- **Grouping**: Assign NICs of VMs to an ASG.
- **Integration with NSGs**: Use ASGs in NSG rules to apply policies to all VMs in the group.
- **Scalability**: ASGs are particularly useful for complex applications with multiple VMs, as they allow reusable security policies.

### Creating an ASG

1. In the Azure portal, search for "Application Security Groups."
2. Click "Create."
3. Provide name, subscription, resource group, and location.
4. Click "Review + create," then "Create."

### Assigning VMs to ASGs

5. In the NIC settings of a VM, under "Application security groups," select the ASG.
6. A NIC can belong to multiple ASGs, up to Azure's limits.

*Example*: Create an ASG named "WebServers" for web VMs and another named "DatabaseServers" for database VMs. Then, create an NSG rule allowing traffic from "WebServers" to "DatabaseServers" on port 1433 (SQL).

*Reference*: Azure Application Security Groups Overview

## 3. Allowing Specific IPs to Access VMs

To allow specific IP addresses to access VMs, create inbound NSG rules specifying the source IP and desired port.

### Example Rule (Allow SSH from Specific IP)

- **Priority**: 100

- **Source**: 203.0.113.5 (specific IP)
- **Source Port**: * (any)
- **Destination**: VirtualNetwork or VM’s private IP
- **Destination Port**: 22 (SSH)
- **Protocol**: TCP
- **Action**: Allow

### Steps

1. In the NSG’s "Inbound security rules" section, click "Add."
2. Configure the rule with the above parameters.
3. Save and apply the rule.

This ensures only the specified IP can access the VM on the designated port, while the default "DenyAllInbound" rule blocks other traffic.

## 4. Denying Internet Access Using NSGs

To prevent VMs from accessing the internet, create an outbound NSG rule to deny traffic to the "Internet" service tag, overriding the default "AllowInternetOutBound" rule (priority 65001).

### Example Rule (Deny Internet Access)

- **Priority**: 100
- **Source**: Any
- **Source Port**: * (any)
- **Destination**: Internet (service tag)
- **Destination Port**: * (any)
- **Protocol**: Any
- **Action**: Deny

### Steps

1. In the NSG’s "Outbound security rules" section, click "Add."
2. Configure the rule with the above parameters.
3. Save and apply the rule.

### Best Practice

- Ensure necessary Azure services (e.g., Storage, Azure Monitor) are allowed using specific service tags to avoid disrupting VM functionality.

## 5. Public IP Addresses in Azure

### Overview

Public IP addresses enable Azure resources to communicate with the internet and public-facing Azure services. They are dedicated to a resource until unassigned.

### Types and SKUs

- **SKUs**:
  - **Basic**: Supports dynamic or static IPv4, dynamic-only IPv6. Being retired by 30 September 2025.
  - **Standard**: Supports static-only IPv4 and IPv6, recommended for production workloads.
- **IP Versions**: IPv4, IPv6, or dual-stack.

### Allocation Methods

- **Dynamic**: IP is assigned when the resource starts and may change if stopped or deleted.
- **Static**: IP is fixed at creation and remains until the public IP resource is deleted.

### Creating a Public IP

1. In the Azure portal, search for "Public IP addresses."
2. Click "Create."
3. Select SKU (Standard recommended), IP version, name, and allocation method (static or dynamic).
4. Optionally, configure a domain name label (e.g., contoso.westus.cloudapp.azure.com).
5. Click "Review + create," then "Create."

### Associating/De-associating Public IP with a VM

- **During VM Creation**: In the networking tab, select or create a public IP.
- **For Existing VMs**:
  1. Navigate to the VM’s NIC, go to "IP configurations."
  2. Add a public IP by selecting an existing one or creating a new one.
  3. To disassociate, remove the public IP from the IP configuration.

*Reference*: Public IP Addresses in Azure

## 6. Static and Dynamic IPs

### Public IPs

- **Static**: Fixed IP, ideal for scenarios requiring consistent addressing (e.g., DNS records).
- **Dynamic**: IP may change, suitable for non-critical applications.

### Private IPs

- **Static**: Manually assigned IP within the subnet’s range, ensuring consistency.
- **Dynamic**: Assigned by Azure’s DHCP, may change on VM restart.

### Assigning Static IPs

- **Public**: Set allocation method to static when creating the public IP.
- **Private**: In the NIC's IP configuration, set "Private IP address settings" to static and specify an IP within the subnet.

## 7. Service Tags in NSGs

### Overview

Service tags are predefined identifiers for Azure services, representing their IP ranges. They simplify NSG rules by eliminating the need to manage specific IPs.

### Common Service Tags

- **Internet**: Public internet addresses.
- **VirtualNetwork**: All VNets in the subscription.
- **AzureLoadBalancer**: Azure's load balancer service.
- **Storage**: Azure Storage services.
- **SQL**: Azure SQL Database.

### Usage

In NSG rules, select a service tag as the source or destination instead of an IP range. For example, allow traffic to "Storage" for VMs accessing Azure Storage.

*Reference*: Azure Service Tags Overview

## 8. Allocating Static IPs to All VMs

### Public Static IPs

1. For each VM, create a public IP with static allocation (see Section 5).
2. Associate the public IP with the VM's NIC during creation or via IP configurations.

### Private Static IPs

1. In the VM's NIC settings, go to "IP configurations."
2. Set "Assignment" to static and specify an available IP within the subnet's range.
3. Repeat for all VMs.

### Considerations

- Assigning public static IPs to all VMs may not be necessary unless direct internet access is required. Consider using a load balancer or NAT gateway for outbound traffic.
- Ensure private IPs are unique within the subnet.

# 9. Creating a Network Interface

### Overview

A network interface (NIC) connects a VM to a VNet, enabling communication with other resources. Each VM requires at least one NIC, and some VM sizes support multiple NICs.

### Creating a NIC

1. In the Azure portal, search for "Network interfaces."
2. Click "Create."
3. Specify name, VNet, subnet, private IP settings (static or dynamic), and optionally associate a public IP or NSG.
4. Click "Review + create," then "Create."

### Attaching to a VM

- **During VM Creation**: Select or create a NIC in the networking tab.
- **For Existing VMs**: Add a NIC via the VM’s "Networking" settings, ensuring the VM size supports multiple NICs.

*Reference*: Create, Change, or Delete an Azure Network Interface

# Best Practices

- **NSGs**: Associate at the subnet level for easier management, unless specific VM-level rules are needed.
- **ASGs**: Use descriptive names (e.g., "WebServers") and regularly update memberships to reflect infrastructure changes.
- **Public IPs**: Use Standard SKU for production and static allocation for persistent IPs. Be aware of costs, as public IPs incur charges.
- **Service Tags**: Use to simplify rules, but verify availability in your region.
- **Security**: Follow the least-privilege principle, allowing only necessary traffic.
- **Monitoring**: Regularly audit NSG and ASG configurations for compliance.

# Citations

- Azure Network Security Groups Overview
- Azure Application Security Groups Overview
- Public IP Addresses in Azure
- Create, Change, or Delete an Azure Network Interface
- Azure Service Tags Overview