**R&D Document: Configuring NSG & ASG for Specific IP Access and Denial of Public Internet Access**

**Table of Contents**

1. **Introduction**
2. **Prerequisites**
3. **Overview of NSG and ASG**
4. **Configuring NSG to Allow Specific IPs**
5. **Configuring ASG for Enhanced Security**
6. **Denying Internet Access**
7. **Static vs. Dynamic IPs**
8. **Using Service Tags**
9. **Best Practices**
10. **Conclusion**

### 1. Introduction

This document provides guidance on configuring Network Security Groups (NSG) and Application Security Groups (ASG) to control access to Azure Virtual Machines (VMs). It includes steps to allow access from specific IP addresses while denying access from the public internet. Additionally, it covers handling static and dynamic IPs and leveraging Azure service tags for security.

### 2. Prerequisites

* An active Azure subscription.
* Basic understanding of Azure Virtual Networks (VNet), Network Security Groups (NSG), and Application Security Groups (ASG).
* Azure CLI or Azure PowerShell installed, or access to the Azure Portal.

### 3. Overview of NSG and ASG

**Network Security Groups (NSG)**: NSGs contain security rules that allow or deny inbound and outbound traffic to and from several types of Azure resources, including VMs and subnets.

**Application Security Groups (ASG)**: ASGs help simplify the management of security rules by grouping VMs and applying NSG rules to these groups.

### 4. Configuring NSG to Allow Specific IPs

To allow access to specific IP addresses, you need to create NSG rules.

#### Using Azure Portal

1. Navigate to your NSG in the Azure Portal.
2. Go to **Inbound security rules** and click **Add**.
3. Set the following:
   * **Source**: IP Addresses
   * **Source IP addresses/CIDR ranges**: Specific IPs (e.g., 203.0.113.5 or 203.0.113.0/24)
   * **Source port ranges**: \* (or specific port if needed)
   * **Destination**: Any (or specific VNet/subnet)
   * **Destination port ranges**: \* (or specific port if needed)
   * **Protocol**: Any
   * **Action**: Allow
   * **Priority**: A number lower than the deny rule
   * **Name**: AllowSpecificIPs
4. Click **Add** to create the rule

#### Using Azure CLI

sh

Copy code

az network nsg rule create \

--resource-group <ResourceGroupName> \

--nsg-name <NSGName> \

--name AllowSpecificIPs \

--priority 1000 \

--source-address-prefixes 203.0.113.5 203.0.113.0/24 \

--destination-port-ranges '\*' \

--direction Inbound \

--access Allow \

--protocol '\*'

### 5. Configuring ASG for Enhanced Security

ASGs allow you to group VMs and apply NSG rules to the group instead of individual VMs.

#### Creating an ASG

1. Navigate to **Application security groups** in the Azure Portal.
2. Click **Add**.
3. Fill in the details and create the ASG.

#### Associating VMs with an ASG

1. Navigate to your VM.
2. Go to **Networking**.
3. Under **Configure network security group**, click **Application security groups**.
4. Add your VM to the created ASG.

### 6. Denying Internet Access

To deny public internet access while allowing specific IPs, create a deny rule.

#### Using Azure Portal

1. Go to **Inbound security rules** and click **Add**.
2. Set the following:
   * **Source**: Any
   * **Source port ranges**: \*
   * **Destination**: Any
   * **Destination port ranges**: \*
   * **Protocol**: Any
   * **Action**: Deny
   * **Priority**: A number higher than the allow rule
   * **Name**: DenyInternetAccess
3. Click **Add** to create the rule.

#### Using Azure CLI

sh

az network nsg rule create \

--resource-group <ResourceGroupName> \

--nsg-name <NSGName> \

--name DenyInternetAccess \

--priority 2000 \

--source-address-prefixes '\*' \

--destination-port-ranges '\*' \

--direction Inbound \

--access Deny \

--protocol '\*'

### 7. Static vs. Dynamic IPs

* **Static IP**: An IP address that does not change over time.
* **Dynamic IP**: An IP address that can change periodically.

To handle dynamic IPs, consider using DNS names or dynamic DNS services that map to the current IP address.

### 8. Using Service Tags

Service tags represent a group of IP address prefixes from a specific Azure service. You can use them in NSG rules to simplify management.

#### Example: Allow AzureLoadBalancer

sh

Copy code

az network nsg rule create \

--resource-group <ResourceGroupName> \

--nsg-name <NSGName> \

--name AllowAzureLoadBalancer \

--priority 1100 \

--source-address-prefixes AzureLoadBalancer \

--destination-port-ranges '\*' \

--direction Inbound \

--access Allow \

--protocol '\*'

### 9. Best Practices

* Use **least privilege** principles when creating NSG rules.
* Regularly review and update your NSG and ASG configurations.
* Use **logging and monitoring** to track access and identify potential security issues.
* Leverage **service tags** to simplify rule management and stay updated with Azure service IP changes.

### 10. Conclusion

This document provides a comprehensive guide to configuring NSG and ASG in Azure to allow access from specific IPs while denying public internet access. By following these steps and best practices, you can enhance the security of your Azure VMs.

### References:

* [Azure NSG Documentation](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview)
* [Azure ASG Documentation](https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups)
* [Azure Service Tags](https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview)