Research & Development Document: Azure Networking - NSG, ASG, Public IPs, and VM Connectivity

Table of Contents

8. **Troubleshooting Common Issues**
9. **Conclusion**
10. **References**

---

1. Introduction to Azure Networking Security

Azure provides multiple layers of network security:

- **Network Security Groups (NSG)**: Firewall for Azure resources.
- **Application Security Groups (ASG)**: Logical grouping of VMs for granular security.
- **Public IPs**: Enables internet-facing access.
- **Service Tags**: Simplify NSG rules by grouping Azure services.

---

2. Network Security Groups (NSG)

2.1 What is an NSG?

- A **virtual firewall** that controls inbound/outbound traffic.
- Applied at **Subnet** or **Network Interface (NIC)** level.

2.2 How NSG Works

- Evaluates traffic based on **5-tuple rules**:
    - Source/Destination IP
    - Source/Destination Port
    - Protocol (TCP/UDP/ICMP)
- Rules processed in **priority order** (lower number = higher priority).

2.3 Default NSG Rules

Priority	Rule	Description
65000	AllowVNetInBound	Allows all traffic within VNet
65001	AllowAzureLoadBalancerInBound	Allows Azure LB health probes
65500	DenyAllInBound	Blocks all other inbound traffic

2.4 Creating an NSG

1. Go to **Azure Portal** → **Create Resource** → **Network Security Group**.
2. Configure:
    - **Name**: nsg-webserver
    - **Resource Group**: rg-networking

2.5 Applying NSG to Subnets/NICs

- **Subnet-Level**: Applies to all VMs in the subnet.
- **NIC-Level**: Overrides subnet NSG for specific VMs.

---

3. Application Security Groups (ASG)

3.1 What is an ASG?

- Logical grouping of VMs (e.g., "WebServers", "DatabaseServers").
- Used in **NSG rules** to apply policies to multiple VMs.

3.2 ASG vs NSG

Feature	NSG	ASG
Purpose	Filters traffic	Groups VMs for NSG rules
Scope	Subnet/NIC	VM NICs
Rule Target	IPs/Ports	Logical VM groups

3.3 Implementing ASG in NSG Rules

1. **Create ASG**:
    - Name: asg-webservers
2. **Assign VMs** to ASG via NIC configuration.
3. **Add NSG Rule**:
    - Source: Internet
    - Destination: asg-webservers
    - Port: 80,443

4. Public IP Addresses

4.1 Public IP Types

Type	Description	Use Case
Static	Fixed IP (Doesn't change)	Production workloads
Dynamic	Changes on VM stop/start	Dev/Test environments

4.2 Creating & Assigning Public IPs

1. **Create Public IP**:
    - Name: pip-web-vm1
    - Type: **Static**
2. **Assign to VM**:
    - Attach during VM creation or via NIC settings.

4.3 Associating/Disassociating Public IPs

- **Associate**:
  NIC → IP Configurations → Add Public IP
- **Disassociate**:
  NIC → IP Configurations → Remove Public IP

---

5. Restricting Access Using NSGs

5.1 Allowing Specific IPs to Access VMs

1. **Add Inbound Rule**:
    - Source: Specific IP (e.g., 203.0.113.5)
    - Destination: VM Private IP
    - Port: 3389 (RDP) / 22 (SSH)

5.2 Blocking Internet Access Using NSG

1. **Add Outbound Rule**:
    - Source: Any
    - Destination: Internet
    - Action: **Deny**

6. Service Tags in Azure

6.1 What are Service Tags?

- Represents **groups of Azure service IPs** (e.g., AzureCloud, AzureLoadBalancer).
- Simplifies NSG rules by avoiding manual IP listing.

6.2 Common Azure Service Tags

Tag	Description
VirtualNetwork	All VNet IPs
AzureLoadBalancer	Azure LB health probes
Internet	Public internet

7. Step-by-Step Implementation

7.1 Creating a Network Security Group

1. Azure Portal → **Create NSG** (nsg-main).
2. Add rules:
    - Allow SSH (Port 22) from MyOfficeIP.
    - Deny all inbound internet traffic.

7.2 Allocating Static Public IPs to VMs

1. Create **Static Public IP** (pip-vm1).
2. Assign to vm1 during creation.

7.3 Creating & Attaching Network Interfaces

1. **Create NIC**:
    - Attach to vnet-main/subnet1.
    - Assign pip-vm1.
2. **Attach to VM**.

7.4 Configuring NSG Rules for Specific Access

plaintext

Copy

Download

Rule 1: Allow RDP (3389) from 203.0.113.5

Rule 2: Deny all inbound from Internet

---

8. Troubleshooting Common Issues

❌ **Can't connect to VM?**

- Check **NSG rules** and **Public IP association**.
- Verify **VM firewall settings**.

❌ **IP address changed?**

- Ensure **Static Public IP** is used.

---

9. Conclusion

- **NSGs** provide granular traffic control.
- **ASGs** simplify security management for VM groups.
- **Public IPs** enable external access (Static for production).
- **Service Tags** reduce manual IP management.

---

10. References

- Azure NSG Documentation
- Public IP Addresses