Azure Network Security Groups (NSG) & Application Security Groups (ASG)

Research & Development Document

Document Version: 1.0

Last Updated: June 2025

Document Classification: Technical Reference

Prepared By: Cloud Infrastructure R&D Team

Table of Contents

Executive Summary

This research and development document provides comprehensive coverage of Azure's network security mechanisms, focusing on Network Security Groups (NSGs), Application Security Groups (ASGs), IP address management, and related networking components. The document serves as both a technical reference and implementation guide for securing Azure virtual machines and network infrastructure.

Key Objectives

- Understand the architecture and functionality of NSGs and ASGs
- Implement secure network access controls for Azure VMs
- Manage static and dynamic IP addresses effectively
- Configure network interfaces and public IP associations
- Apply best practices for network security and cost optimization

Network Security Groups (NSG) Overview

Definition and Purpose

Network Security Groups (NSGs) act as cloud-based firewalls that control inbound and outbound network traffic to Azure resources. They contain security rules that allow or deny network traffic based on source/destination IP addresses, ports, and protocols.

Key Components

Security Rules Structure

Component	Description	Values/Range
Priority	Rule processing order	100-4096 (lower = higher priority)
Name	Descriptive identifier	User-defined string
Protocol	Network protocol	TCP, UDP, ICMP, ESP, AH, Any
Source/Destination	Traffic origin/target	IP addresses, CIDR, service tags, ASGs
Port Ranges	Network ports	1-65535 (specific or ranges)
Action	Traffic handling	Allow or Deny

Default Rules

Inbound Default Rules

- **AllowVnetInBound** (Priority 65000): Allows traffic within VNet

- **AllowAzureLoadBalancerInBound** (Priority 65001): Allows Azure Load Balancer probes
- **DenyAllInBound** (Priority 65500): Denies all other inbound traffic

Outbound Default Rules

- **AllowVnetOutBound** (Priority 65000): Allows outbound VNet traffic
- **AllowInternetOutBound** (Priority 65001): Allows outbound internet traffic
- **DenyAllOutBound** (Priority 65500): Denies all other outbound traffic

NSG Association Levels

Subnet Level

- Applied to all resources within the subnet
- More efficient for broad security policies
- Single point of management for multiple VMs
- Ideal for implementing network segmentation

Network Interface Level

- Applied to specific VM network interfaces
- Granular control per VM
- Takes precedence over subnet-level NSGs
- Suitable for VM-specific security requirements

Application Security Groups (ASG) Overview

Definition and Purpose

Application Security Groups (ASGs) enable network security policies based on application workloads rather than explicit IP addresses. They provide a more dynamic and scalable approach to network security by grouping VMs logically according to their function or role in the application architecture.

Key Features

Logical Grouping

- Group VMs by function (web servers, database servers, application servers)
- Independent of IP addresses or subnet boundaries
- Simplified rule management and maintenance
- Support for complex application topologies

Dynamic Membership

- VMs can be added/removed from ASGs without changing security rules
- Rules automatically apply to all ASG members
- Supports micro-segmentation strategies
- Enables scalable security architectures

ASG vs NSG Comparison

Feature	NSG	ASG
Scope	IP-based rules	Application-based grouping
Scalability	Limited by IP management	Highly scalable
Maintenance	Manual IP updates required	Automatic through logical grouping
Use Case	Traditional firewall rules	Modern application security
Management Complexity	Increases with scale	Remains consistent

IP Address Management in Azure

Public IP Address Types

Static Public IP

Characteristics

- Fixed IP address that doesn't change throughout the resource lifecycle
- Reserved even when the associated resource is stopped
- Consistent network identity for external access

Use Cases

- Production servers requiring consistent external access
- Domain name mapping and DNS configurations
- SSL certificates tied to specific IP addresses
- Firewall rules and security policies

Billing Implications

- Charged continuously whether attached to a resource or not
- Higher cost compared to dynamic IPs
- Available in both Basic and Standard SKUs

Dynamic Public IP

Characteristics

- IP address assigned when VM starts
- Released when VM is stopped (deallocated)
- May change between VM restarts

Use Cases

- Development and testing environments
- Temporary or short-lived resources
- Cost-sensitive deployments

Limitations

- Only available with Basic SKU
- IP address changes on VM restart
- Not suitable for production workloads requiring consistent access

Private IP Address Types

Static Private IP

- Manually assigned within subnet IP range
- Persistent across VM restarts and redeployments
- Required for infrastructure services (domain controllers, DNS servers)
- Enables predictable internal network addressing

Dynamic Private IP

- Automatically assigned by Azure DHCP service
- Default option for most VM deployments
- Can change during VM restart (though rarely in practice)
- Suitable for most application workloads

Service Tags

Service tags represent groups of IP address prefixes from specific Azure services, significantly simplifying security rule creation and maintenance.

Common Service Tags

Service Tag	Description	Use Case
Internet	All public internet addresses	Allow/deny general internet access
VirtualNetwork	All virtual network address space	Internal VNet communication
AzureLoadBalancer	Azure load balancer infrastructure	Health probe access
Storage	Azure Storage service IP ranges	Access to storage accounts
Sql	Azure SQL Database IP ranges	Database connectivity
AzureActiveDirectory	Azure AD IP ranges	Authentication services

Implementation Scenarios

Scenario 1: Allowing Specific IPs to Access VMs

Business Case

Restrict VM access to specific corporate IP addresses, management systems, or trusted partner networks to enhance security posture and comply with regulatory requirements.

Implementation Strategy

1. Identify all legitimate source IP addresses or CIDR blocks
2. Create NSG with custom inbound rules for each IP range
3. Define specific allowed ports and protocols (SSH, RDP, HTTP/HTTPS)
4. Set appropriate rule priorities to ensure proper processing order
5. Associate NSG with target subnet or specific network interfaces
6. Test connectivity from allowed and blocked sources

Important Considerations

- Ensure backup access methods are available before implementing restrictions
- Consider dynamic IP ranges for remote workers
- Plan for emergency access scenarios
- Document all approved IP ranges and their business justification

Scenario 2: Denying Internet Access Using NSG

Business Case

Prevent VMs from accessing the internet to meet security compliance requirements, protect against data exfiltration, and reduce the attack surface of critical systems.

Implementation Strategy

1. Create outbound NSG rules with higher priority than default rules
2. Add explicit deny rule for destination "Internet" service tag
3. Allow specific outbound traffic if required (Windows Updates, package repositories)
4. Configure Azure Update Management for patch management
5. Implement NAT Gateway or proxy for necessary external access
6. Monitor applications for unexpected internet dependencies

Scenario 3: Multi-Tier Application Security with ASG

Business Case

Implement micro-segmentation for a multi-tier application architecture with web servers, application servers, and database servers, ensuring each tier can only communicate with authorized adjacent tiers.

Implementation Strategy

1. Create ASGs for each application tier (WebTier, AppTier, DBTier)
2. Assign VMs to appropriate ASGs based on their function
3. Create NSG rules using ASGs as source and destination
4. Implement least-privilege access between tiers
5. Configure monitoring and logging for inter-tier communication
6. Test application functionality across all tiers

Step-by-Step Implementation Guide

Creating a Network Security Group

Azure Portal Method

1. Navigate to "Create a resource" → "Networking" → "Network security group"
2. Configure basic settings:
    3. Select appropriate subscription and resource group
    4. Provide descriptive name following naming conventions
    5. Choose target region
    6. Add relevant tags for organization and billing
7. Review configuration settings and create the NSG
8. Navigate to the created NSG and add custom security rules
9. Configure inbound and outbound rules based on requirements
10. Associate NSG with target subnets or network interfaces

Azure CLI Method

```
# Create NSG
az network nsg create \
    --resource-group myResourceGroup \
    --name myNSG \
    --location eastus \
    --tags environment=production

# Add inbound security rule for SSH
az network nsg rule create \
```

```
    --resource-group myResourceGroup \
    --nsg-name myNSG \
    --name AllowSSH \
    --protocol tcp \
    --priority 1000 \
    --destination-port-range 22 \
    --access allow \
    --source-address-prefixes 10.0.0.0/16

# Add outbound rule to deny internet access
az network nsg rule create \
    --resource-group myResourceGroup \
    --nsg-name myNSG \
    --name DenyInternet \
    --protocol * \
    --priority 1000 \
    --destination-address-prefixes Internet \
    --access deny \
    --direction outbound
```

PowerShell Method

```
# Create NSG
$nsg = New-AzNetworkSecurityGroup `
    -ResourceGroupName "myResourceGroup" `
    -Location "East US" `
    -Name "myNSG" `
    -Tag @{Environment="Production"}

# Add SSH security rule
Add-AzNetworkSecurityRuleConfig `
    -NetworkSecurityGroup $nsg `
    -Name "AllowSSH" `
    -Description "Allow SSH access" `
    -Access Allow `
    -Protocol Tcp `
    -Direction Inbound `
    -Priority 1000 `
```

```
    -SourceAddressPrefix "10.0.0.0/16" `
    -SourcePortRange * `
    -DestinationAddressPrefix * `
    -DestinationPortRange 22

# Update NSG with new rules
Set-AzNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

Creating Public IP Address

Static Public IP Creation

1. Navigate to "Create a resource" → "Networking" → "Public IP address"
2. Configure basic settings:
    3. Provide descriptive name
    4. Select resource group and region
    5. Choose SKU: Standard (for static IP)
    6. Set IP Version: IPv4 or IPv6
    7. Select IP address assignment: Static
    8. Configure DNS name label (optional but recommended)
9. Configure advanced settings if needed:
    10. Availability zone preferences
    11. Routing preference settings
    12. Security settings
13. Add appropriate tags for resource management
14. Review and create the public IP resource

Allocating Static IPs to VMs

For New Virtual Machines

1. During VM creation process, navigate to the "Networking" tab
2. Under "Public IP" section, click "Create new"
3. Configure static IP settings:
    4. Name the public IP resource
    5. Select Standard SKU
    6. Choose Static assignment
    7. Set DNS name label
8. Configure network security group settings
9. Complete VM creation process
10. Verify static IP assignment post-deployment

For Existing Virtual Machines

1. Stop the target VM (required for dynamic to static conversion)
2. Navigate to the VM's networking configuration
3. Select the network interface
4. Go to "IP configurations" section
5. Click on the primary IP configuration
6. Change assignment from "Dynamic" to "Static"
7. Specify the desired static IP address (within subnet range)
8. Save changes and restart the VM
9. Verify connectivity and static IP assignment

Creating Application Security Groups

Azure Portal Method

1. Navigate to "Create a resource" → "Networking" → "Application security group"
2. Configure basic settings:
    3. Select subscription and resource group
    4. Provide descriptive name (e.g., "WebTier-ASG", "DatabaseTier-ASG")
    5. Choose appropriate region
    6. Add relevant tags
7. Review and create the ASG
8. Assign VMs to the ASG through their network interfaces
9. Configure NSG rules to use the ASG as source or destination

Using ASGs in NSG Rules

1. Create or edit an existing NSG rule
2. In the source or destination field, select "Application security group"
3. Choose the appropriate ASG from the dropdown
4. Configure remaining rule parameters (ports, protocols, action)
5. Set appropriate priority level
6. Save the rule and test connectivity

Associating/De-associating Public IP with VM

Association Process

1. Navigate to the target VM in Azure Portal

2. Go to the "Networking" section
3. Click on the Network Interface name
4. Select "IP configurations" from the menu
5. Click on the primary IP configuration
6. Enable "Public IP address" option
7. Either create a new public IP or select an existing one
8. Configure public IP settings if creating new
9. Save changes and wait for deployment completion
10. Verify public IP association and connectivity

De-association Process

1. Follow steps 1-5 from the association process
2. Disable the "Public IP address" option
3. Confirm the de-association action
4. Save changes
5. Verify that public IP is no longer associated

PowerShell Automation

```
# Associate Public IP with VM
$vm = Get-AzVM -ResourceGroupName "myRG" -Name "myVM"
$publicIP = Get-AzPublicIpAddress -ResourceGroupName "myRG" -Name
"myPublicIP"
$nic = Get-AzNetworkInterface -ResourceGroupName "myRG" -Name
$vm.NetworkProfile.NetworkInterfaces[0].Id.Split('/')[-1]

$nic.IpConfigurations[0].PublicIpAddress = $publicIP
Set-AzNetworkInterface -NetworkInterface $nic
```

```
# De-associate Public IP from VM
$nic.IpConfigurations[0].PublicIpAddress = $null
Set-AzNetworkInterface -NetworkInterface $nic

# Verify association status
Get-AzNetworkInterface -ResourceGroupName "myRG" -Name $nic.Name |
    Select-Object -ExpandProperty IpConfigurations |
    Select-Object Name, PublicIpAddress
```

Creating Network Interface

Azure Portal Method

1. Navigate to "Create a resource" → "Networking" → "Network interface"
2. Configure basic settings:
    3. Provide descriptive name
    4. Select resource group and region
    5. Choose target virtual network and subnet
6. Configure IP settings:
    7. Private IP assignment (Dynamic or Static)
    8. Network security group association
    9. Public IP address (optional)
10. Advanced configuration options:
    11. Enable IP forwarding for routing scenarios
    12. Configure custom DNS servers
    13. Enable accelerated networking for performance
14. Add resource tags for organization
15. Review and create the network interface

Azure CLI Method

```
# Create network interface with static private IP
az network nic create \
    --resource-group myResourceGroup \
    --name myNIC \
    --vnet-name myVNet \
    --subnet mySubnet \
    --private-ip-address 10.0.1.10 \
    --network-security-group myNSG \
    --public-ip-address myPublicIP \
    --accelerated-networking true

# Create network interface with dynamic IP
az network nic create \
    --resource-group myResourceGroup \
    --name myNIC-Dynamic \
    --vnet-name myVNet \
    --subnet mySubnet \
    --network-security-group myNSG
```

Best Practices and Recommendations

NSG Design Principles

Rule Organization Strategy

Naming Conventions

- Use descriptive, consistent names that indicate purpose
- Include direction, protocol, and source/destination information
- Examples: "Allow-SSH-FromCorpNetwork", "Deny-HTTP-ToInternet"

Rule Documentation

- Document business justification for each rule
- Include change management information
- Maintain rule ownership and review schedules
- Use rule descriptions effectively

Priority Management Framework

Priority Range	Rule Type	Examples
100-500	Critical Security Rules	Emergency access, security overrides
500-1000	Application-Specific Rules	Database access, web server rules
1000-2000	Management and Monitoring	Backup agents, monitoring tools
2000-3000	General Access Rules	User access, development tools

Priority Range	Rule Type	Examples
3000+	Temporary/Testing Rules	Troubleshooting, temporary access

Service Tag Utilization

Benefits of Service Tags

- Automatically maintained by Microsoft
- Reduce rule complexity and maintenance overhead
- Improve rule readability and understanding
- Support for regional and global service ranges

Implementation Guidelines

- Prefer service tags over hardcoded IP ranges when available
- Use regional service tags for better performance and security
- Combine service tags with port restrictions for granular control
- Monitor for new service tags that could simplify existing rules

ASG Implementation Strategy

Logical Grouping Principles

- Align ASGs with application architecture and data flow
- Create ASGs for each security zone and trust boundary
- Consider both horizontal scaling (multiple instances) and vertical scaling (different tiers)
- Plan for hybrid cloud scenarios with on-premises integration

Naming Convention Framework

Recommended Naming Pattern

```
{Environment}-{Application}-{Tier}-{Function}-ASG
```

Examples

- "prod-ecommerce-web-frontend-ASG"
- "dev-analytics-data-processing-ASG"
- "test-crm-database-backend-ASG"

IP Address Management Best Practices

Static IP Allocation Guidelines

When to Use Static IPs

- Infrastructure services (DNS, domain controllers, monitoring)
- Load balancers and application gateways
- VPN gateways and network virtual appliances
- Production databases requiring consistent connectivity

Static IP Management

- Maintain comprehensive IP address documentation
- Implement IP address management (IPAM) solutions
- Plan for IP address space growth and scalability
- Monitor regional IP availability and quotas

Dynamic IP Usage Strategy

- Use for development and testing environments

- Implement for temporary or ephemeral workloads
- Apply to auto-scaling compute resources
- Ensure proper DNS naming strategies for dynamic resources

Troubleshooting and Monitoring

Common NSG Issues and Solutions

Connectivity Problems

Issue	Symptoms	Troubleshooting Steps
Rule Priority Conflicts	Unexpected traffic blocking/allowing	Review rule priorities, check for overlapping rules
Incorrect Source/Destination	Legitimate traffic blocked	Verify IP ranges, service tags, ASG memberships
Default Rule Impact	Unexpected default behavior	Understand default rule implications, add explicit rules
Subnet vs NIC Association	Rules not applying as expected	Check NSG association levels, understand precedence

Performance Optimization

Rule Optimization Strategies

- Order rules by frequency of use (most common first)
- Consolidate similar rules to reduce processing overhead
- Use service tags instead of multiple IP ranges
- Remove unused or redundant rules regularly

Performance Monitoring

- Monitor NSG processing metrics in Azure Monitor

- Track rule hit counts and usage patterns
- Analyze flow logs for performance insights
- Set up alerts for unusual traffic patterns

Monitoring and Logging

NSG Flow Logs Configuration

1. Enable NSG Flow Logs for compliance and troubleshooting
2. Configure storage account with appropriate retention policies
3. Set up Log Analytics workspace for advanced querying and analysis
4. Implement automated alerting for suspicious traffic patterns
5. Create dashboards for security and operational monitoring

Azure Monitor Integration

Key Metrics to Monitor

- NSG rule hit counts and patterns
- Blocked vs allowed traffic ratios
- Public IP usage and associated costs
- Network interface performance metrics
- Security group membership changes

Alerting Strategies

- Set up alerts for rule violations and unusual patterns
- Monitor for unauthorized network access attempts
- Track changes to security group configurations

- Alert on public IP allocation and de-allocation events

Diagnostic Tools

Network Watcher Capabilities

Tool	Purpose	Use Case
IP Flow Verify	Test NSG rule application	Validate rule configuration and troubleshoot connectivity
Next Hop Analysis	Routing path investigation	Understand traffic routing and identify bottlenecks
Security Group View	Applied rules visualization	See all effective security rules for a network interface
Connection Troubleshoot	End-to-end connectivity testing	Diagnose complex connectivity issues across multiple hops

Azure Resource Graph Queries

```
// Query all NSGs with specific rules
Resources
| where type == "microsoft.network/networksecuritygroups"
| extend rules = properties.securityRules
| mvexpand rules
| where rules.properties.access == "Allow"
| project name, resourceGroup, ruleName = rules.name,
          sourceAddressPrefix = rules.properties.sourceAddressPrefix

// Find unused public IPs
Resources
| where type == "microsoft.network/publicipaddresses"
| where properties.ipConfiguration == ""
```

```
| project name, resourceGroup, ipAddress = properties.ipAddress,
          sku = properties.sku.name
```

Cost Optimization

Public IP Cost Management

Cost Optimization Strategies

Immediate Cost Reduction

- Use dynamic IPs for non-production environments
- Implement IP sharing through load balancers and application gateways
- Regular audit and cleanup of unused public IP addresses
- Consider NAT Gateway for outbound-only internet access scenarios

Long-term Cost Management

- Implement automated IP lifecycle management
- Use Azure Policy to enforce IP allocation standards
- Plan for reserved IP addresses where predictable usage exists
- Optimize IP SKU selection based on requirements

Monitoring and Alerting for Cost Control

1. Set up billing alerts for public IP costs
2. Track IP utilization metrics and trends
3. Implement automated cleanup policies for unused resources
4. Use resource tags for accurate cost allocation and chargeback
5. Regular review of IP allocation against business requirements

NSG and ASG Cost Considerations

Resource Efficiency Optimization

NSG Consolidation

- Consolidate NSGs where security requirements allow
- Use subnet-level NSGs for broader policy application
- Optimize rule complexity to reduce processing overhead
- Plan NSG architecture for scalability and maintainability

ASG Efficiency

- Design ASGs for optimal reusability across environments
- Minimize the number of ASGs while maintaining security boundaries
- Use consistent ASG patterns to reduce management complexity

Conclusion

Network Security Groups and Application Security Groups provide comprehensive network security capabilities for Azure environments, enabling organizations to implement robust security controls while maintaining operational efficiency. The successful implementation of these technologies requires careful planning, consistent application of best practices, and ongoing monitoring and optimization.

Key Success Factors

Strategic Implementation

- **Least-Privilege Principle:** Implement security rules that provide minimum necessary access
- **Scalable Architecture:** Design NSG and ASG strategies that support organizational growth
- **Automation Integration:** Leverage service tags and ASGs for reduced maintenance overhead
- **Consistent Standards:** Follow established naming conventions and documentation practices

Operational Excellence

Achieving operational excellence with Azure network security requires a combination of technical implementation and organizational processes:

- **Continuous Monitoring:** Implement comprehensive logging and alerting to detect security issues and performance problems
- **Regular Reviews:** Conduct periodic reviews of security rules and access patterns to ensure continued relevance

- **Change Management:** Establish formal processes for security rule changes and documentation updates
- **Cost Optimization:** Regularly assess and optimize IP address usage and security group configurations

Future Considerations

Organizations should consider emerging trends and capabilities in Azure networking:

- Integration with Azure Security Center and Microsoft Sentinel for advanced threat detection
- Adoption of Zero Trust networking principles and micro-segmentation strategies
- Hybrid cloud connectivity patterns and security boundary management
- Automation and Infrastructure as Code (IaC) for security configuration management

Critical Reminders

- Always test security rule changes in non-production environments first
- Maintain backup access methods before implementing restrictive security rules
- Document all security rules with business justification and ownership information
- Regularly review and update security configurations to address evolving threats

This document serves as a comprehensive foundation for implementing robust network security in Azure environments while maintaining operational efficiency and cost-effectiveness. The combination of NSGs, ASGs, and proper IP address management provides the building blocks for secure, scalable, and manageable cloud infrastructure.

Document Information

Version: 1.0 | Last Updated: June 2025 | Classification: Technical Reference

Prepared by: Cloud Infrastructure R&D Team