Research & Development Document: Azure Network Security Groups, Application Security Groups, and IP Management

Prepared for: CSI Summer Internship - Celebal Technologies
Prepared By: Hitesh Jangid
Document Classification: Technical Research & Implementation
Date: 03 July 2025

Research Abstract

This comprehensive research document examines Azure's network security architecture, focusing on Network Security Groups (NSGs), Application Security Groups (ASGs), and IP address management strategies. The study provides detailed analysis of security rule implementation, IP allocation methodologies, and practical scenarios for enterprise network security deployment.

Azure's network security model operates on multiple layers, providing granular control over network traffic through rule-based filtering and application-centric security groupings. Understanding these mechanisms becomes essential for implementing robust cloud security architectures that protect resources while maintaining operational efficiency.

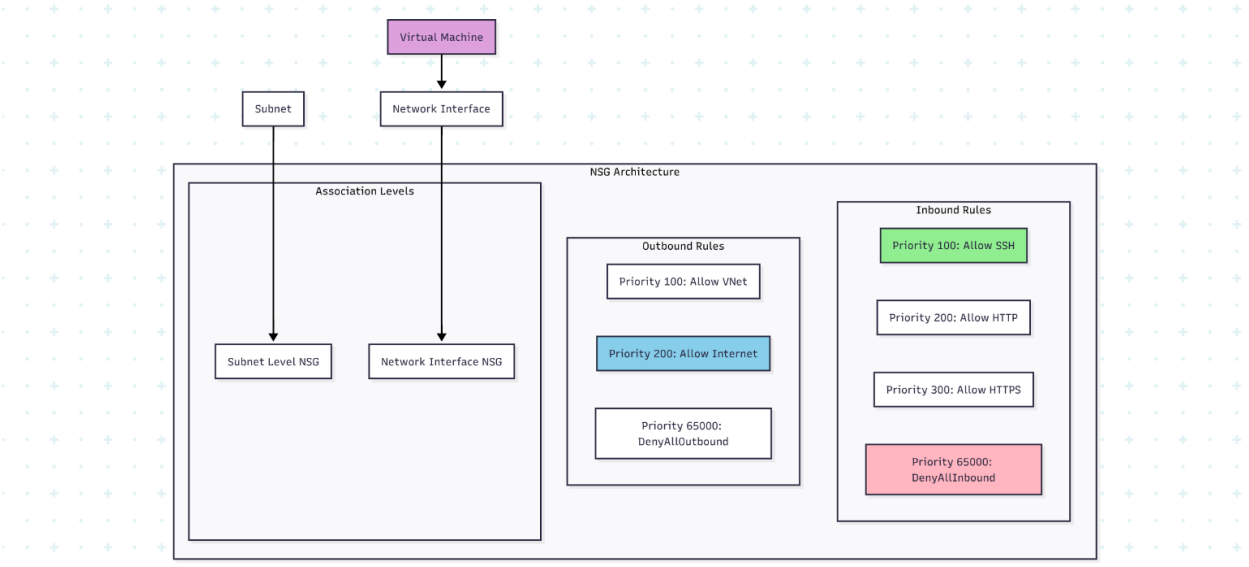
Research Methodology and Scope

This investigation combines theoretical framework analysis with practical implementation testing, examining Microsoft documentation, security best practices, and hands-on laboratory validation. The methodology encompasses architectural review, configuration testing, and security validation to ensure comprehensive understanding of Azure networking security concepts.

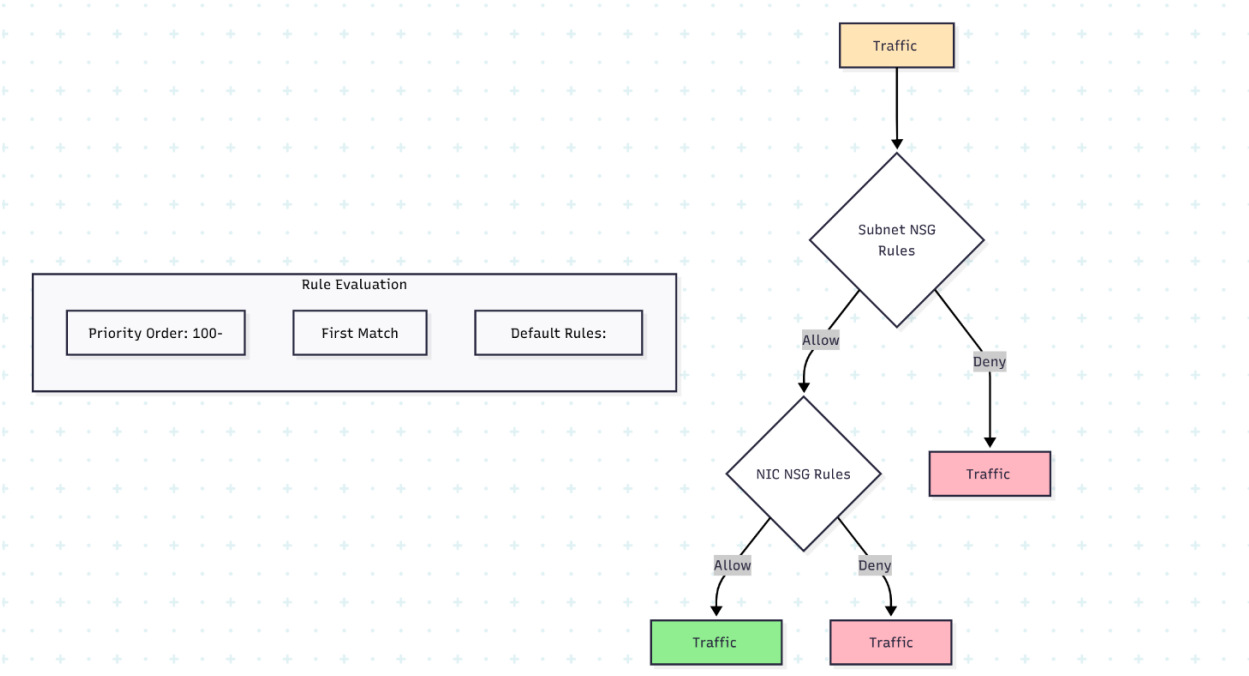
Network Security Groups (NSG) Architecture

Network Security Groups function as virtual firewalls that control inbound and outbound traffic to Azure resources through rule-based filtering. Each NSG contains security rules that allow or deny traffic based on source IP, destination IP, port, and protocol specifications.

The NSG architecture operates at two distinct levels within Azure networking infrastructure. Subnet-level NSGs provide broad network segment protection, while network interface-level NSGs offer granular per-VM security controls. This dual-layer approach enables comprehensive security implementation that addresses both network-wide and resource-specific requirements.



NSG Rule Processing Logic



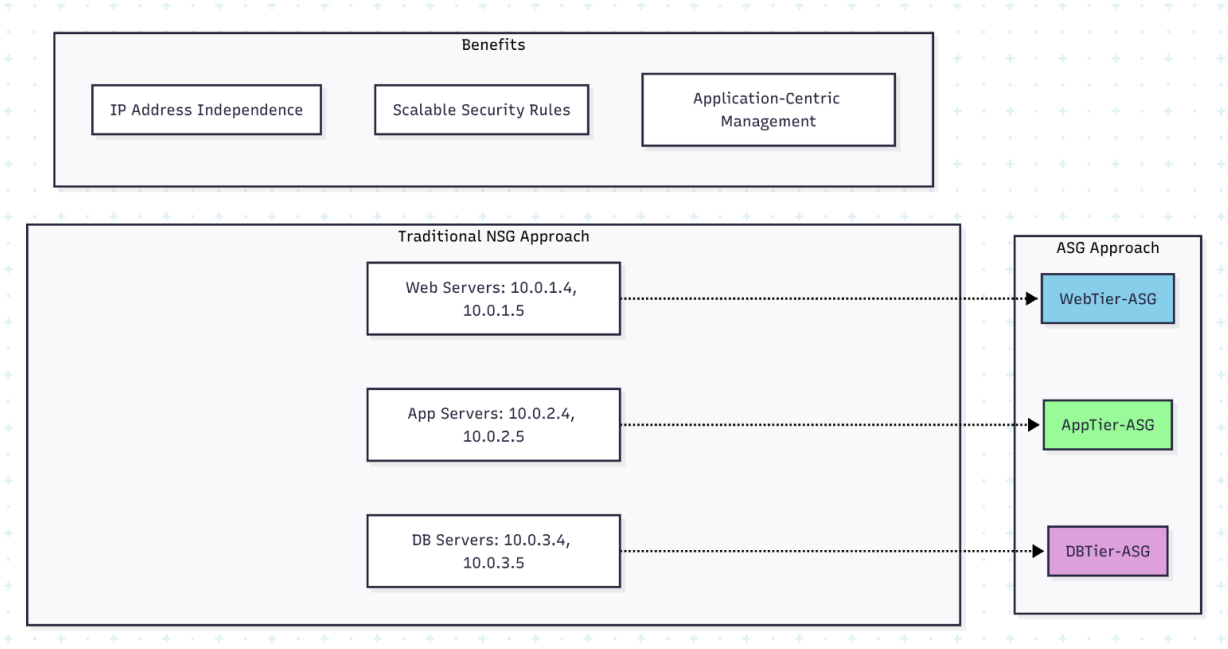
NSG rule processing follows a priority-based evaluation system where lower numerical values indicate higher priority. Rules are evaluated sequentially until a matching condition is found, at which point the associated action (allow or deny) is applied without further rule evaluation.

Default rules provide baseline security policies that cannot be deleted but can be overridden by custom rules with higher priority. These default rules typically allow VNet-

to-VNet communication while blocking unsolicited internet traffic, establishing a secure foundation for network communication.

Application Security Groups (ASG) Implementation

Application Security Groups provide application-centric network security by grouping virtual machines based on their roles or functions rather than their IP addresses. This approach simplifies security rule management and enables dynamic security policies that adapt to infrastructure changes.



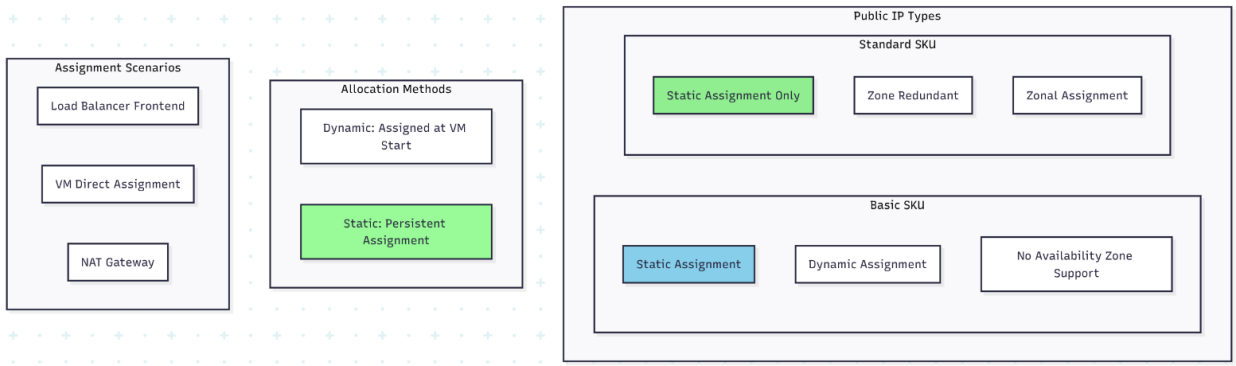
ASGs enable administrators to create security rules that reference application groups rather than specific IP addresses. This abstraction provides significant advantages when scaling applications or implementing infrastructure changes, as security rules remain valid regardless of underlying IP address modifications.

ASG and NSG Integration

The integration between ASGs and NSGs creates powerful security architectures that combine the flexibility of application-centric grouping with the granular control of network-based filtering. NSG rules can reference ASGs as sources or destinations, creating dynamic security policies that automatically apply to group members.

IP Address Management Strategy

Public IP Address Types and Allocation



Azure provides two distinct SKUs for public IP addresses, each offering different capabilities and pricing models. Basic SKU public IPs support both static and dynamic allocation methods, while Standard SKU IPs require static allocation and provide enhanced availability zone support.

Dynamic IP allocation assigns addresses when associated resources start and releases them when resources stop. This method proves cost-effective for development environments but may cause connectivity issues for production systems requiring consistent addressing.

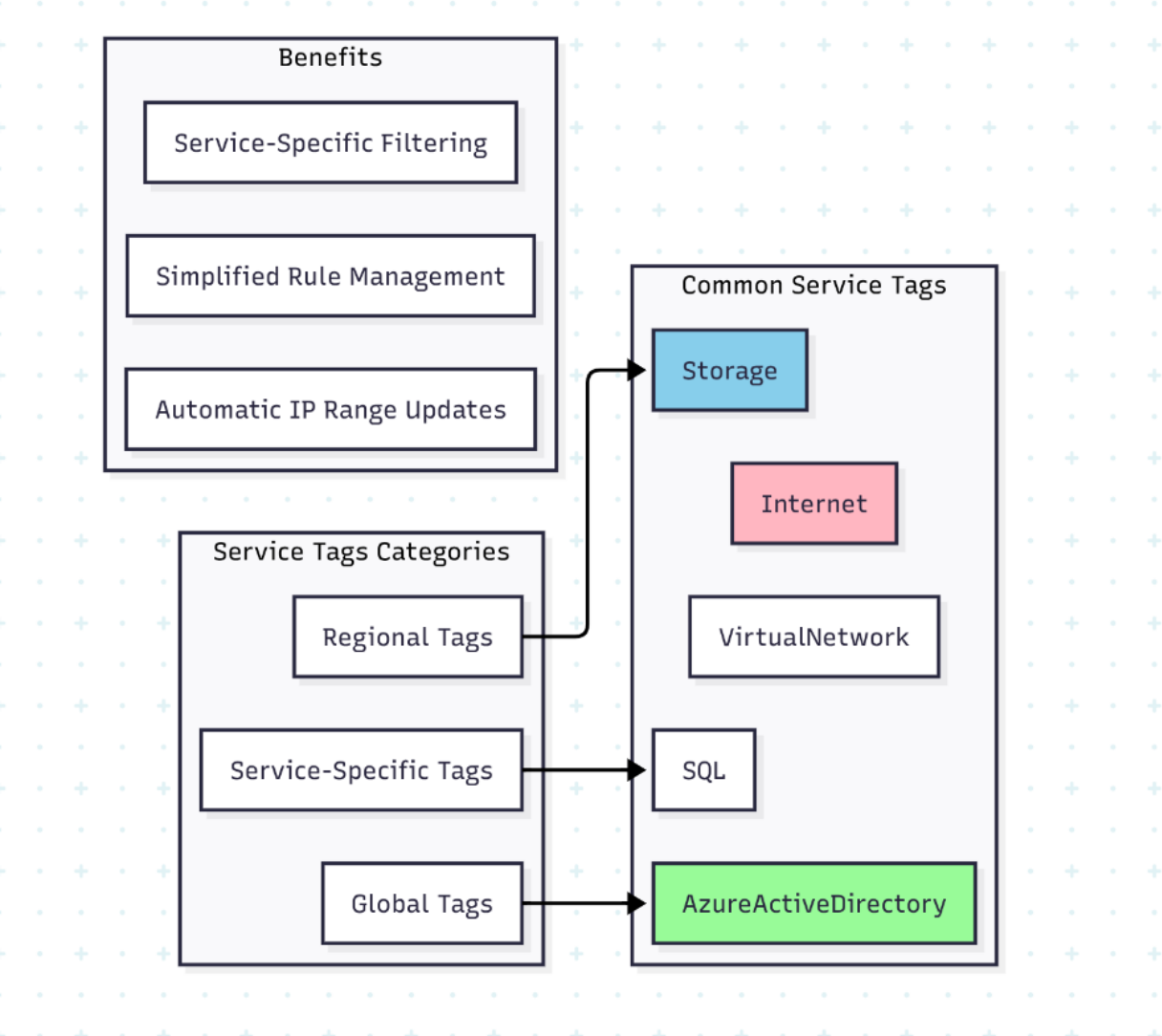
Static IP allocation maintains consistent addresses regardless of resource state changes, making it essential for production systems, DNS configurations, and services requiring predictable connectivity endpoints.

Private IP Address Management

Private IP addresses operate within VNet address spaces and support both dynamic and static allocation methods. Azure's DHCP service manages dynamic allocations, while static assignments require manual configuration and careful coordination to prevent conflicts.

Private IP Allocation Strategies: - Dynamic allocation for standard workloads - Static allocation for domain controllers, DNS servers - Reserved IP ranges for future expansion - Documentation of all static assignments

Service Tags Implementation



Service tags represent groups of IP address prefixes for specific Azure services, simplifying NSG rule creation and maintenance. These tags automatically update when service IP ranges change, eliminating the need for manual rule updates and reducing configuration drift.

Regional service tags provide location-specific IP ranges, enabling rules that allow access only to services within specific Azure regions. This approach improves security by limiting exposure to geographically distant service endpoints.

Practical Implementation Guide

Phase 1: Network Security Group Creation

NSG Configuration Process:

1. **Resource Creation:**
   - NSG Name: Production-Web-NSG
   - Resource Group: RG-Security-Lab
   - Location: East US
   - Tags: Environment=Production, Tier=Web
2. **Inbound Security Rules:**

Rule 1: Allow-HTTP
- Priority: 100
- Source: Any
- Source Port: *
- Destination: Any
- Destination Port: 80
- Protocol: TCP
- Action: Allow

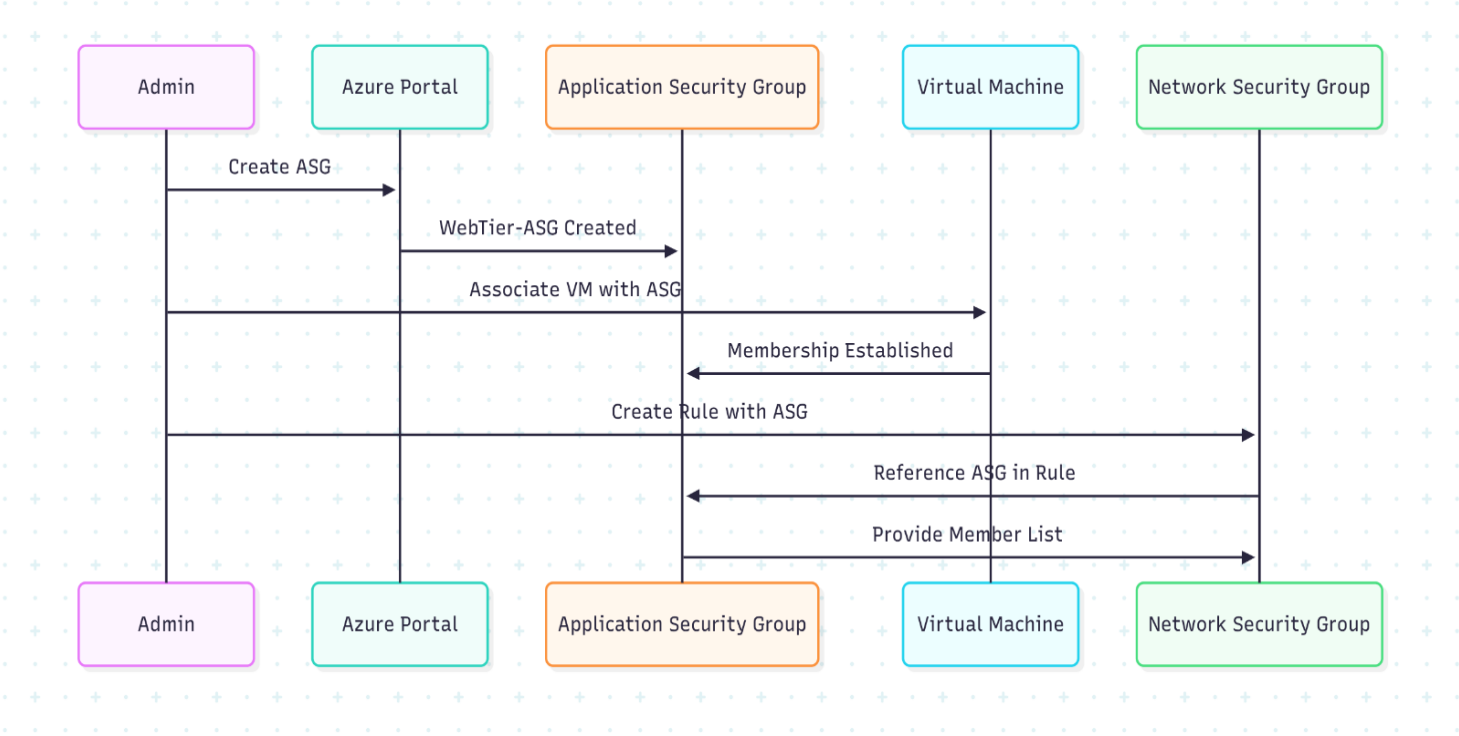
Rule 2: Allow-HTTPS
- Priority: 110
- Source: Any
- Source Port: *
- Destination: Any
- Destination Port: 443
- Protocol: TCP
- Action: Allow

Rule 3: Allow-SSH-Specific-IP
- Priority: 120
- Source: 203.0.113.0/24
- Source Port: *
- Destination: Any
- Destination Port: 22
- Protocol: TCP
- Action: Allow

Rule 4: Deny-Internet
- Priority: 200
- Source: Internet
- Source Port: *
- Destination: Any
- Destination Port: *
- Protocol: Any
- Action: Deny

Phase 2: Application Security Group Implementation

ASG Configuration:



ASG Creation Steps: 1. Create Application Security Groups for each application tier 2. Associate virtual machines with appropriate ASGs 3. Configure NSG rules referencing ASGs instead of IP addresses 4. Validate rule application and traffic flow

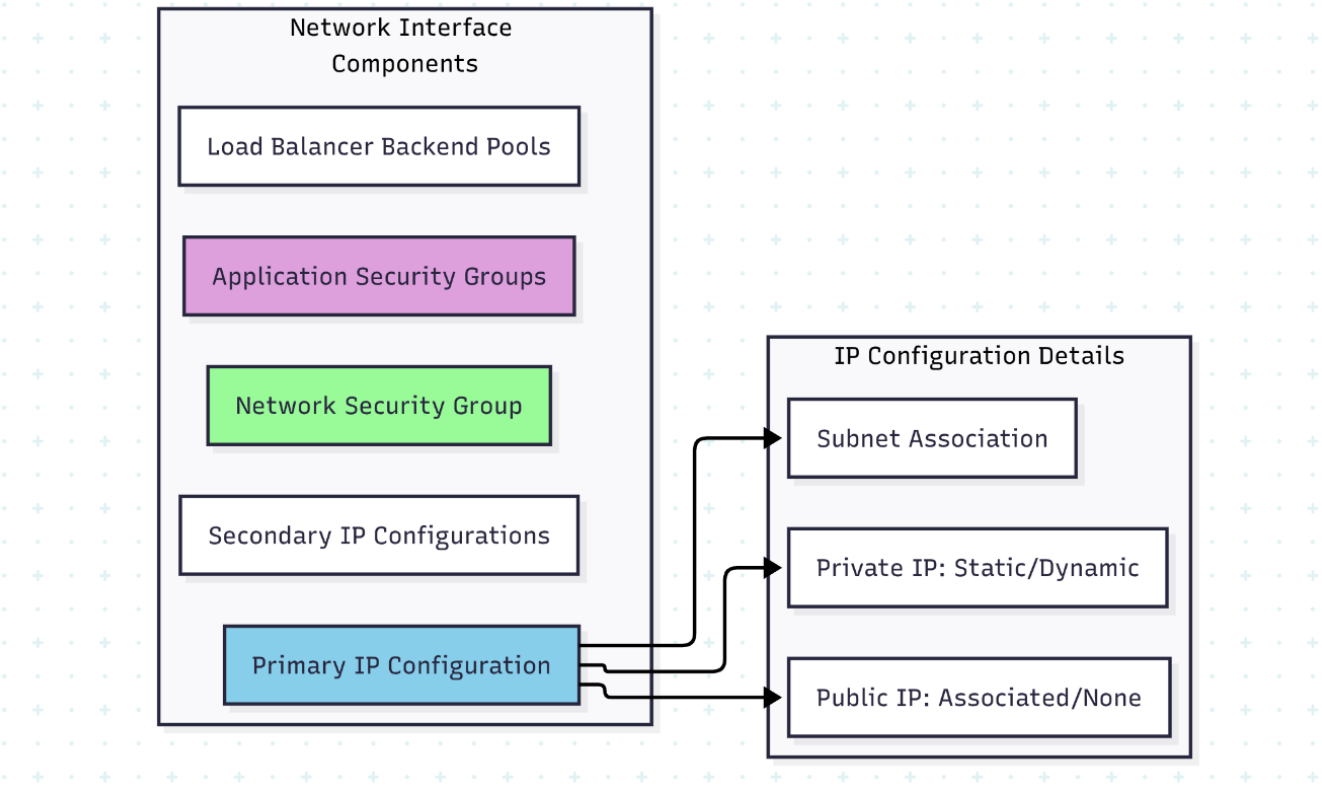
Phase 3: Public IP Address Management

Static Public IP Allocation:

Configuration Parameters: - Public IP Name: VM-WebServer-PIP - SKU: Standard - Assignment: Static - IP Version: IPv4 - DNS Name Label: webserver-prod-001 - Availability Zone: Zone-redundant

Association Process: 1. Create public IP resource with static allocation 2. Configure DNS name label for consistent naming 3. Associate with VM network interface 4. Validate connectivity and DNS resolution 5. Document IP assignment in network inventory

Phase 4: Network Interface Configuration



Network interface creation involves configuring multiple components that determine how virtual machines connect to Azure networks. Each interface supports primary and secondary IP configurations, enabling multi-homed scenarios and advanced networking topologies.

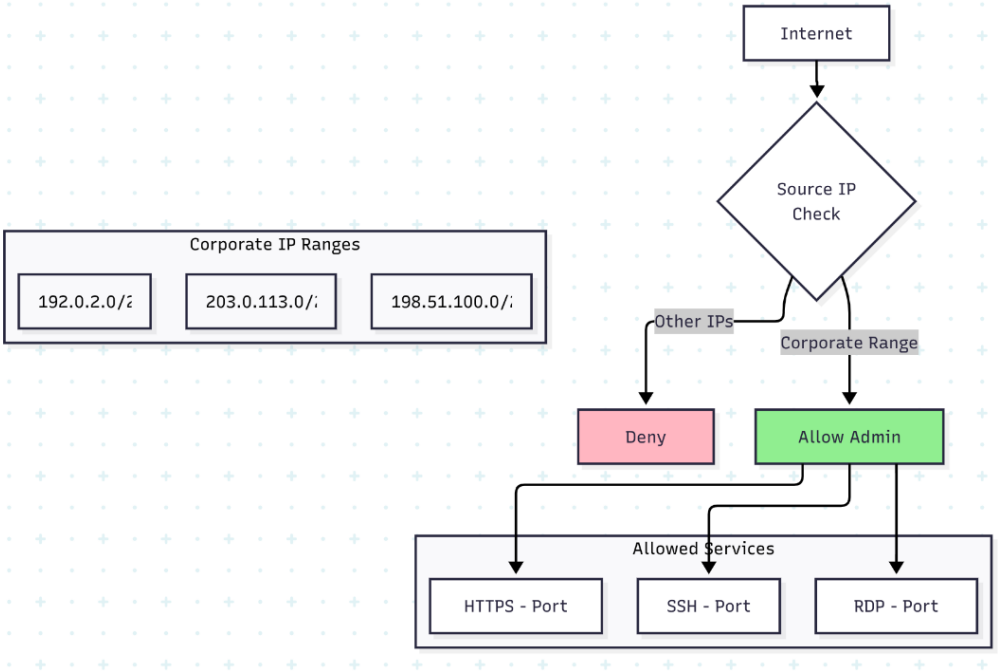
Network Interface Configuration: - Interface Name: VM-WebServer-NIC - Virtual Network: Production-VNet - Subnet: Web-Subnet - Private IP: 10.0.1.100 (Static) - Public IP: VM-WebServer-PIP - NSG: Production-Web-NSG - ASG: WebTier-ASG

Advanced Security Scenarios

Scenario 1: Restricting Access to Specific IP Ranges

Business Requirement: Allow administrative access only from corporate IP ranges while denying all other internet traffic.

Implementation Strategy:



NSG Rule Configuration:

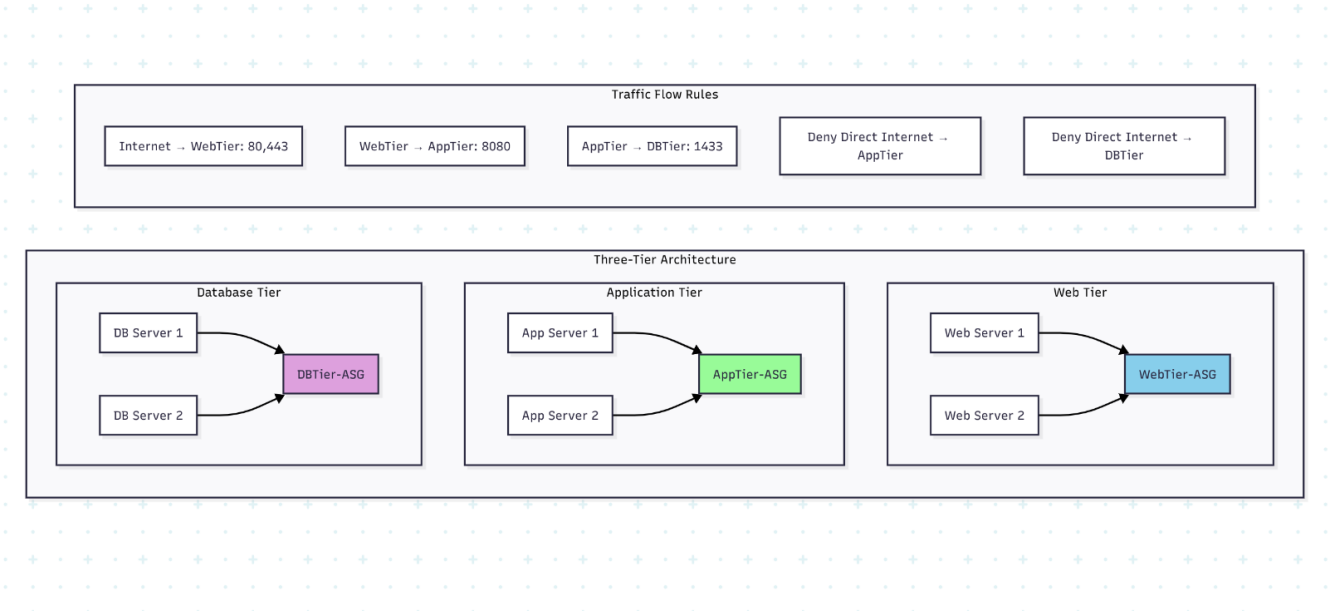
Rule 1: Allow-Corporate-SSH
- Priority: 100
- Source: 203.0.113.0/24,198.51.100.0/24,192.0.2.0/24
- Destination Port: 22
- Action: Allow

Rule 2: Allow-Corporate-RDP
- Priority: 110
- Source: 203.0.113.0/24,198.51.100.0/24,192.0.2.0/24
- Destination Port: 3389
- Action: Allow

Rule 3: Deny-All-Internet
- Priority: 4000
- Source: Internet
- Destination Port: *
- Action: Deny

Scenario 2: Application-Tier Security with ASGs

Architecture Design:



ASG-Based Security Rules:

Rule 1: Internet-to-WebTier
- Source: Internet
- Destination: WebTier-ASG
- Ports: 80, 443
- Action: Allow

Rule 2: WebTier-to-AppTier
- Source: WebTier-ASG
- Destination: AppTier-ASG
- Port: 8080
- Action: Allow

Rule 3: AppTier-to-DBTier
- Source: AppTier-ASG
- Destination: DBTier-ASG
- Port: 1433
- Action: Allow

Rule 4: Deny-Internet-to-AppTier
- Source: Internet
- Destination: AppTier-ASG
- Port: *
- Action: Deny

Static IP Allocation Implementation

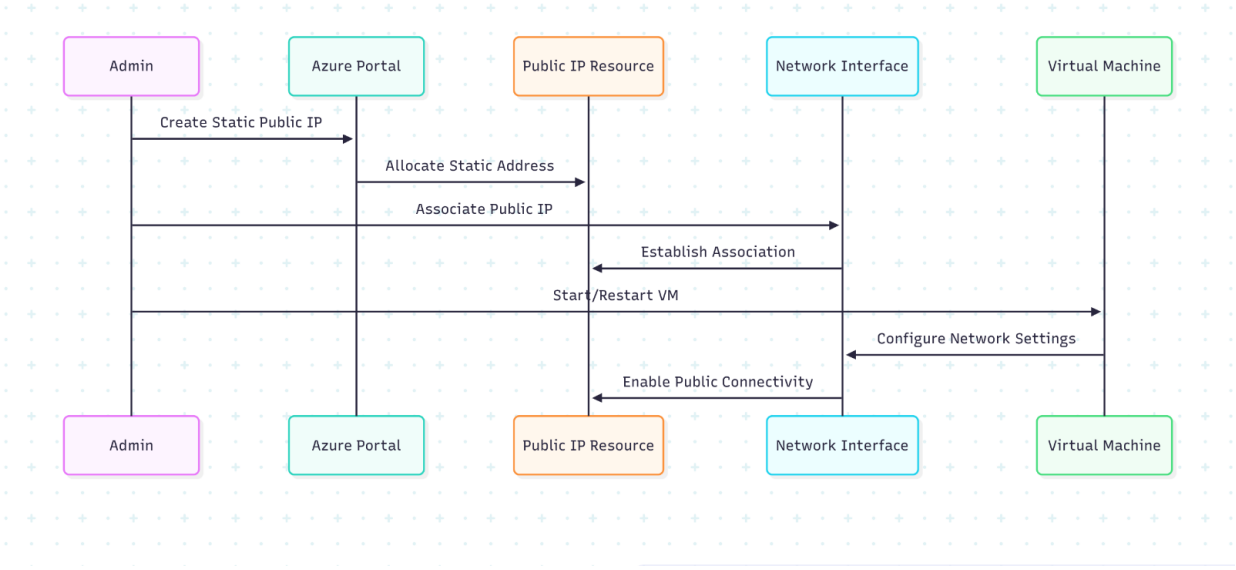
Private IP Static Assignment Process

Step-by-Step Configuration:

1. **VM Power State Management:**
   - Stop virtual machine before IP modification
   - Document current IP configuration
   - Plan static IP assignment within subnet range
2. **Network Interface Modification:**
   - Navigate to VM network interface
   - Select IP configurations
   - Change allocation method to Static
   - Specify desired IP address
   - Validate address availability
3. **Configuration Validation:**
   - Start virtual machine
   - Verify network connectivity
   - Test application functionality
   - Update documentation

Public IP Static Assignment

Configuration Process:



Static Public IP Benefits: - Consistent external connectivity - Simplified DNS configuration - Reliable for external service integrations - Required for certain load balancer configurations

Public IP Association and De-association

Association Process

Prerequisites: - Public IP resource must exist - Network interface must be available - Proper permissions for resource modification

Association Steps: 1. Navigate to VM network interface 2. Select IP configurations 3. Choose public IP resource 4. Apply configuration changes 5. Validate connectivity

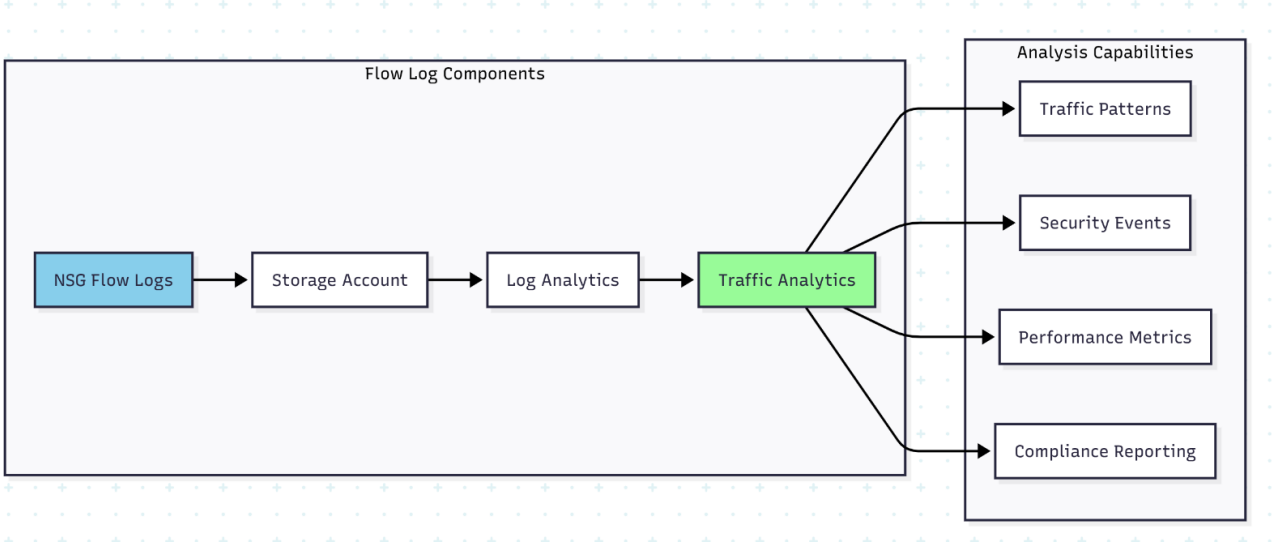
De-association Process

Safety Considerations: - Document current configuration - Notify stakeholders of connectivity changes - Plan for alternative connectivity methods - Schedule during maintenance windows

De-association Steps: 1. Access network interface configuration 2. Remove public IP association 3. Apply configuration changes 4. Verify internal connectivity maintained 5. Update network documentation

Monitoring and Troubleshooting

NSG Flow Logs Analysis



NSG flow logs provide detailed information about network traffic, enabling security analysis, performance monitoring, and compliance reporting. These logs capture information about allowed and denied traffic, helping administrators understand network behavior and identify security issues.

Common Troubleshooting Scenarios

Connectivity Issues: 1. Verify NSG rules allow required traffic 2. Check effective security rules on network interface 3. Validate subnet and NIC-level NSG configurations 4. Confirm service tag and ASG references 5. Analyze flow logs for denied traffic

Performance Problems: 1. Review NSG rule processing overhead 2. Optimize rule priorities for common traffic 3. Consolidate redundant rules 4. Monitor rule evaluation metrics

Security Best Practices and Recommendations

Defense in Depth Strategy

Layer 1: Network Segmentation - Implement subnet-level NSGs for broad protection - Use VNet peering carefully with appropriate NSG rules - Design network topology with security boundaries

Layer 2: Resource-Level Security - Apply NIC-level NSGs for granular control - Implement ASGs for application-centric security - Use service tags for Azure service connectivity

Layer 3: Application Security - Configure application-level authentication - Implement encryption for data in transit - Monitor application logs for security events

Compliance and Governance

Documentation Requirements: - Maintain NSG rule documentation with business justification - Document IP address allocation and usage - Track ASG membership and purposes - Record security configuration changes

Regular Review Processes: - Quarterly NSG rule audits - Annual security architecture reviews - Continuous monitoring of security metrics - Compliance reporting automation

Cost Optimization Strategies

Public IP Cost Management

Cost Factors: - Basic SKU: Lower cost, limited features - Standard SKU: Higher cost, enhanced availability - Reserved IP charges when not associated - Data transfer costs for public IP traffic

Optimization Techniques: - Use dynamic IPs for non-production environments - Implement NAT Gateway for outbound-only scenarios - Consolidate public IPs through load balancers - Regular review of unused public IP resources

NSG and ASG Efficiency

Resource Optimization: - Consolidate similar NSG rules - Use service tags instead of IP ranges - Implement ASGs to reduce rule complexity - Regular cleanup of unused security groups

Research Conclusions and Future Directions

This comprehensive analysis demonstrates the sophisticated network security capabilities available within Azure's infrastructure services. The combination of NSGs, ASGs, and flexible IP management provides organizations with tools necessary to implement robust, scalable security architectures.

Key Research Findings: - NSGs provide effective network-level security controls - ASGs simplify application-centric security management - Static IP allocation supports consistent connectivity requirements - Service tags reduce administrative overhead - Layered security approaches maximize protection effectiveness

Implementation Recommendations: - Start with subnet-level NSGs for broad protection - Implement ASGs for scalable application security - Use static IPs judiciously based on business requirements - Leverage service tags for Azure service connectivity - Establish regular review and maintenance processes

Future Research Opportunities: - Integration with Azure Firewall for advanced threat protection - Automation of security group management through Infrastructure as Code - Advanced analytics and machine learning for security monitoring - Integration with third-party security information and event management systems