Key Points

- Research suggests NSGs filter traffic to Azure resources, while ASGs group VMs for security policies.

- It seems likely that specific IPs can access VMs via NSG rules, and internet access can be denied using NSG outbound rules.

- The evidence leans toward public IPs having Basic and Standard types, with static and dynamic allocation options.

- Service tags simplify NSG rules by representing Azure service IP ranges, and static IPs can be allocated to VMs for consistent addressing.

Network Security Groups (NSG)

NSGs help filter network traffic to and from Azure resources, like virtual machines, by allowing or denying traffic based on rules. These rules consider source, destination, port, and protocol, making them essential for securing your Azure environment.

Application Security Groups (ASG)

ASGs let you group VMs logically, applying security policies based on these groups rather than individual IPs. This simplifies management, especially in complex setups, by reusing policies at scale.

Allowing Specific IPs and Denying Internet Access

To allow specific IPs to access a VM, create an NSG inbound rule for the desired IP and port, like 3389 for RDP. To deny internet access, add an outbound NSG rule blocking traffic to the "Internet" service tag, ensuring necessary Azure services are still allowed.

Public IPs, Types, and Allocation

Public IPs enable internet communication with Azure resources. They come in Basic and Standard SKUs, with Standard recommended for production. IPs can be static (fixed) or dynamic (may change), depending on your needs for consistency, like DNS or firewall updates.

Service Tags and Static IP Allocation

Service tags represent Azure service IP ranges, simplifying NSG rules. To allocate static IPs to VMs, assign them during VM creation or associate them later, ensuring consistent addressing for services like web servers.

Creating and Managing Network Components

Creating an NSG involves setting up basic details in the Azure portal. Public IPs and network interfaces follow similar processes, with options for static or dynamic allocation. Associating or de-associating public IPs with VMs adjusts internet accessibility as needed.

Survey Note: Detailed Analysis of Azure Networking Concepts

This section provides an in-depth exploration of Azure networking components, including Network Security Groups (NSG), Application Security Groups (ASG), public IP addresses, and network interfaces, as requested. The analysis is based on authoritative sources from Microsoft Learn and other technical documentation, ensuring accuracy and relevance as of June 22, 2025.

1. Network Security Groups (NSG)

Network Security Groups (NSGs) are fundamental for filtering network traffic to and from Azure resources within a virtual network. They contain security rules that allow or deny inbound and outbound traffic based on a five-tuple: source, source port, destination, destination port, and protocol. NSGs can be associated with subnets or individual network interfaces, providing flexibility in traffic management.

- Key Features and Functionalities:

  - Association: NSGs can be linked to subnets or network interfaces, affecting all resources within the subnet or specific VMs.

  - Rule Properties: Each rule has a name, priority (100-4096, lower numbers processed first), source/destination (IP, CIDR, service tag, or ASG), protocol (TCP, UDP, ICMP, etc.), direction (inbound/outbound), port range, and action (allow/deny).

- Default Rules: Include AllowVNetInBound, AllowAzureLoadBalancerInBound, DenyAllInbound for inbound, and AllowVnetOutBound, AllowInternetOutBound, DenyAllOutBound for outbound. These cannot be deleted but can be overridden by higher-priority custom rules.

- Augmented Security Rules: Available in the Resource Manager model, these simplify policies by combining multiple ports, IPs, or ranges into one rule, enhancing manageability.

- Flow Timeout: Configurable via the Azure portal or command line, affecting how long flow records remain active before expiring, detailed in [NSG flow logs overview](https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logs-overview?tabs=Americas#non-default-inbound-tcp-rules).

- Use Case: For example, to secure a web server, you might create an NSG rule allowing HTTP (port 80) and HTTPS (port 443) from the "Internet" service tag, while denying all other inbound traffic.

- Steps to Create an NSG:

1. Sign in to the [Azure portal](https://portal.azure.com).
2. Search for "Network security groups" and select it.
3. Select "+ Create".
4. Configure: Subscription, Resource group, Name, Region.
5. Select "Review + create", then "Create" after validation.

2. Application Security Groups (ASG)

Application Security Groups (ASGs) enhance network security by grouping virtual machines and defining policies based on these groups, reducing the need for manual IP address maintenance. This is particularly useful for scaling and managing complex application architectures.

- Key Features and Functionalities:

- Flexibility: A network interface can belong to multiple ASGs, up to Azure limits, as detailed in [Azure limits](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-subscription-service-limits?toc=/azure/virtual-network/toc.json#azure-resource-manager-virtual-networking-limits).

- Rule Application: NSG rules apply only to network interfaces in the specified ASG, not affecting non-members even if the NSG is associated with the subnet.

- Constraints: All network interfaces in an ASG must be in the same virtual network, and source/destination ASGs in a rule must share the same virtual network.

- Best Practice: Plan ASGs to minimize rules, using service tags or ASGs instead of individual IPs for efficiency.

- Use Case: Group all web servers into an "AsgWeb" ASG and apply an NSG rule allowing HTTP/HTTPS traffic, simplifying policy management across multiple VMs.

3. Allowing Specific IPs to Access VMs

To allow specific IPs to access VMs, create NSG inbound rules specifying the source IP or CIDR range. This is crucial for securing remote access, such as RDP or SSH, to VMs.

- Steps:

1. Create or edit an NSG associated with the VM's subnet or network interface.
2. Add an inbound rule:
   - Source: Specific IP (e.g., 192.168.1.10/32) or CIDR range.
   - Destination: Any or VM's IP.
   - Port: Desired port (e.g., 3389 for RDP).
   - Action: Allow.
   - Priority: Set higher than default deny rules (e.g., 100).
3. Save the rule.

- Example: To restrict RDP access, create a rule allowing traffic from your office IP (e.g., 203.0.113.5/32) on port 3389, ensuring only authorized access.

- Reference: For detailed steps, see [Tutorial: Filter network traffic with a network security group (NSG)](https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic).

4. Denying Internet Access Using NSG

Denying internet access involves creating an outbound NSG rule to block traffic to the "Internet" service tag, ensuring VMs cannot access external resources unless explicitly allowed.

- Steps:

1. Create or edit an NSG.

2. Add an outbound rule:

   - Source: Any.

   - Destination: Internet (service tag).

   - Protocol: Any.

   - Action: Deny.

   - Priority: Set high (e.g., 4096) to allow exceptions with lower priorities.

3. Create allow rules for necessary Azure services using service tags (e.g., "Storage.WestEurope" for Azure Storage access):

   - Source: Virtual Network.

   - Destination: Specific service tag (e.g., Storage.WestEurope).

   - Action: Allow.

   - Priority: Lower than deny rule (e.g., 100 for Storage, 200 for SQL).

5. Public IP Addresses and Types

Public IP addresses enable internet communication with Azure resources, such as VMs, load balancers, and application gateways. They are available in two SKUs: Basic and Standard, with Standard recommended for production due to advanced features.

- Types:

  - Basic SKU: Basic features, being retired on September 30, 2025, per [official announcement](https://azure.microsoft.com/updates/upgrade-to-standard-sku-public-ip-addresses-in-azure-by-30-september-2025-basic-sku-will-be-retired/).

  - Standard SKU: Zone-redundant by default, required for Standard load balancers, and supports advanced scenarios.

- Allocation Methods:

  - Static: Assigned at creation, remains fixed until resource deletion, used for DNS, firewall updates, and IP-based security.

  - Dynamic: Assigned on association, can change on stop/delete, suitable for non-critical scenarios.

- Steps to Create a Public IP:

  1. Sign in to the [Azure portal](https://portal.azure.com).

  2. Search for "Public IP addresses" and select it.

  3. Select "+ Create".

  4. Configure: Subscription, Resource group, Name, Region, IP Version (IPv4/IPv6), SKU (Standard), Assignment (Static/Dynamic), etc.

  5. Select "Review + create", then "Create".

- Reference: See [Quickstart: Create a public IP address - Azure portal](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/create-public-ip-portal).

6. Static vs Dynamic IPs

- Static IPs: Assigned at creation, released only on deletion, ensuring consistency for DNS, firewall rules, and TLS/SSL certificates. Cannot specify exact IP; Azure assigns from a pool.

- Dynamic IPs: Assigned on resource start, released on stop/delete, suitable for scenarios without IP dependency, like temporary testing VMs.

- Use Case: For a web server requiring consistent access, use static IPs; for a development VM, dynamic IPs may suffice.

7. Service Tags

Service tags represent groups of IP address prefixes from Azure services, managed and updated by Microsoft. They simplify NSG rule creation by allowing traffic to/from entire services instead of individual IPs.

- Key Features:

  - Predefined: Examples include "Internet", "AzureCloud", "Storage.WestUS".

  - Automatic Updates: Microsoft updates IP ranges weekly, ensuring rules remain current.

  - Usage: Used in NSGs, Azure Firewall, and user-defined routes for access control.

- Discovery Methods:

  - API: Use PowerShell, e.g., `Get-AzNetworkServiceTag -Location eastus2`, takes up to 4 weeks for new data propagation.

  - JSON Files: Weekly updated, locations vary by cloud, in CIDR notation, e.g., AzureCloud.centralfrance.

- Use Case: To allow traffic to Azure Storage, use the "Storage" service tag in an NSG rule, reducing manual IP management.

- Reference: See [Azure service tags overview](https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview).

8. Allocating Static IPs to All VMs

Allocating static IPs to VMs ensures consistent addressing, crucial for services like web servers or DNS resolution.

- Steps:

  - During VM creation, in the Networking tab, create a new public IP with Static assignment.

  - For existing VMs, follow Section 5 (Associating Public IP) to associate a static public IP.

- Reference: See [Create a VM with a static public IP address](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-static-public-ip).

9. Creating a Network Security Group

Creating an NSG involves setting up basic details and configuring rules as needed.

- Steps:

  1. Sign in to the [Azure portal](https://portal.azure.com).

  2. Search for "Network security groups" and select it.

  3. Select "+ Create".

  4. Configure: Subscription, Resource group, Name, Region.

  5. Select "Review + create", then "Create" after validation.

- Reference: See [Create, change, or delete an Azure network security group](https://learn.microsoft.com/en-us/azure/virtual-network/manage-network-security-group).

10. Creating a Public IP

Covered in Section 5, with steps to create a public IP using the Azure portal, ensuring static or dynamic allocation as needed.

11. Associating/De-associating Public IP with a VM

- Associating: Follow Section 5 steps, selecting the public IP in the VM's IP configuration.

- De-associating: Remove the public IP association in the IP configuration, saving changes.

- Reference: See [Associate a public IP address to a virtual machine](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/associate-public-ip-address-vm).

12. Creating a Network Interface

A network interface (NIC) connects VMs to virtual networks for communication.

- Steps:

1. Sign in to the [Azure portal](https://portal.azure.com).

2. Search for "network interfaces" and select it.

3. Select "+ Create".

4. Configure: Subscription, Resource group, Name, Region, Virtual network, Subnet, IP version, Private IP assignment.

5. Select "Review + create", then "Create".

- Reference: See [Create, change, or delete an Azure network interface](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface).