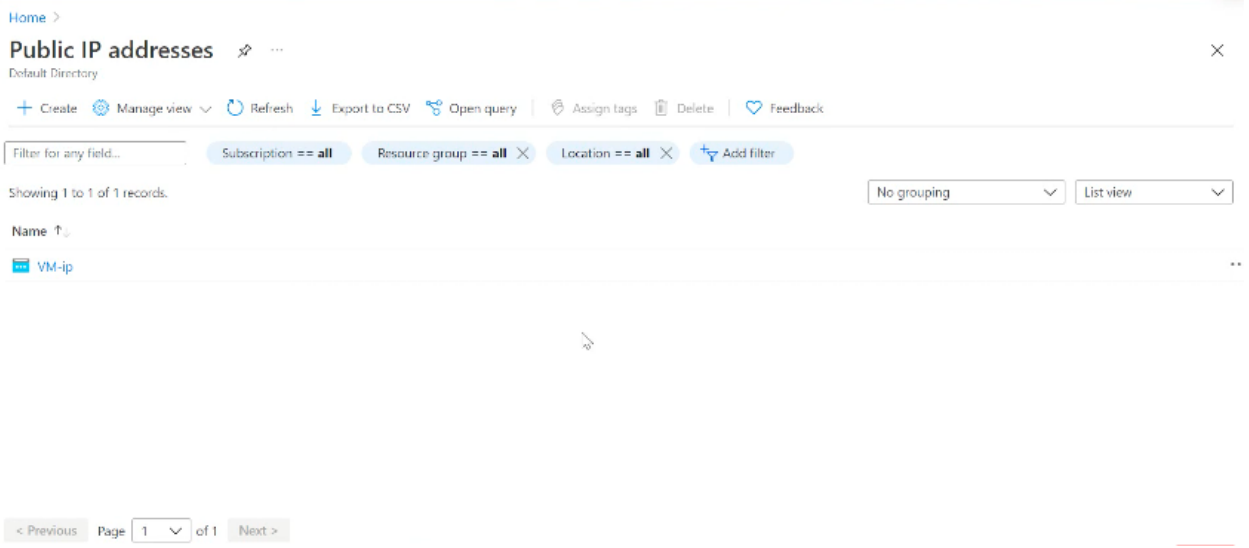
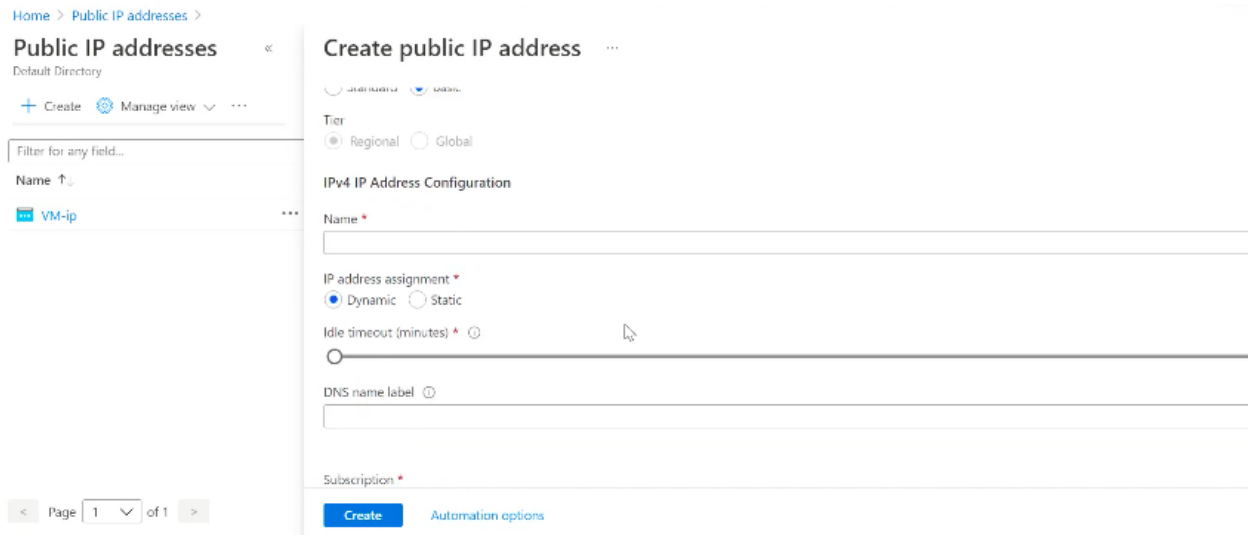
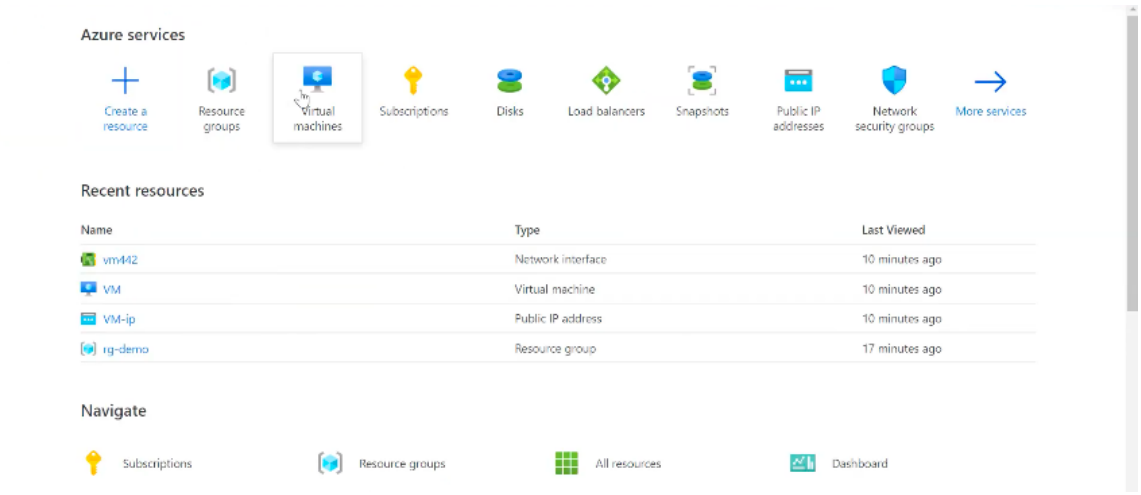
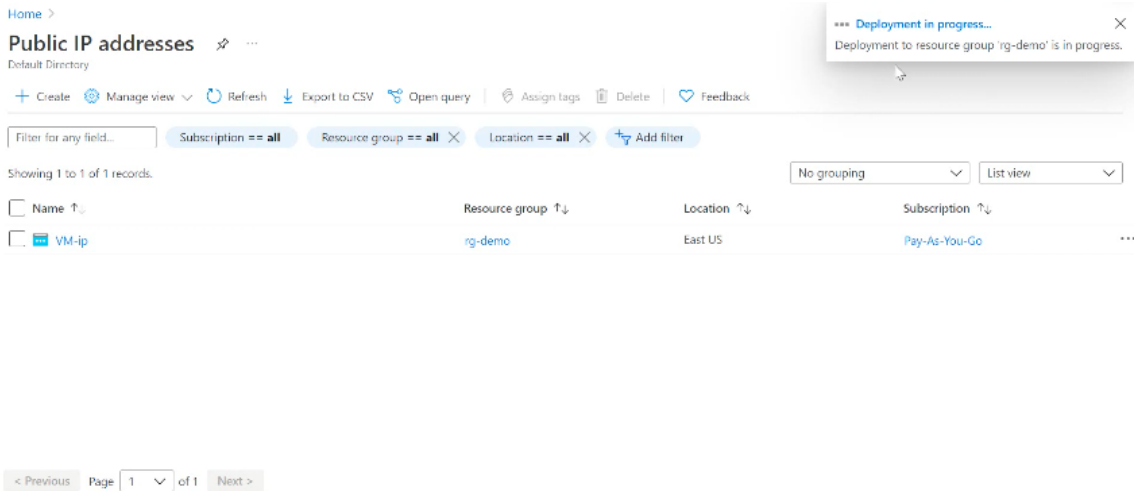
Network Security Groups (NSGs) in Azure

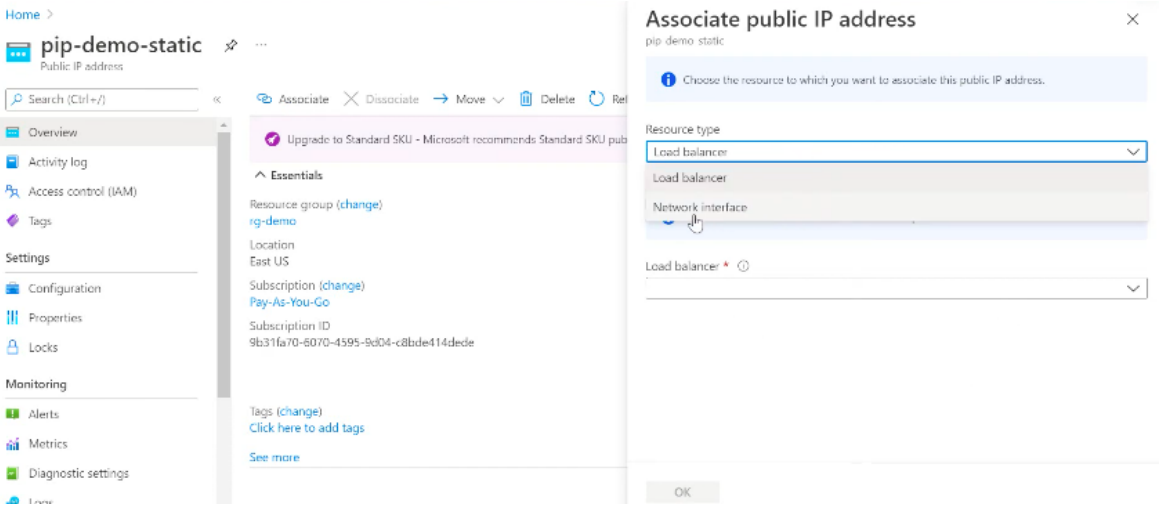
Azure Network Security Groups (NSGs) are an essential component for managing and filtering network traffic to and from resources within an Azure Virtual Network. They provide a robust mechanism for controlling access to and from virtual machines and other resources, ensuring that only authorized traffic is permitted.

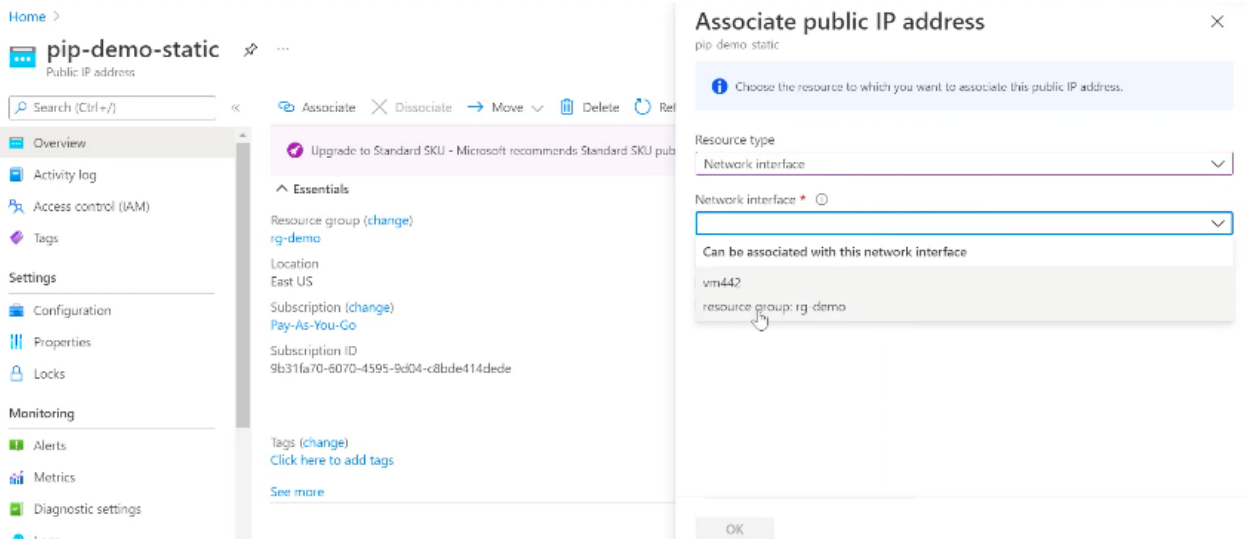


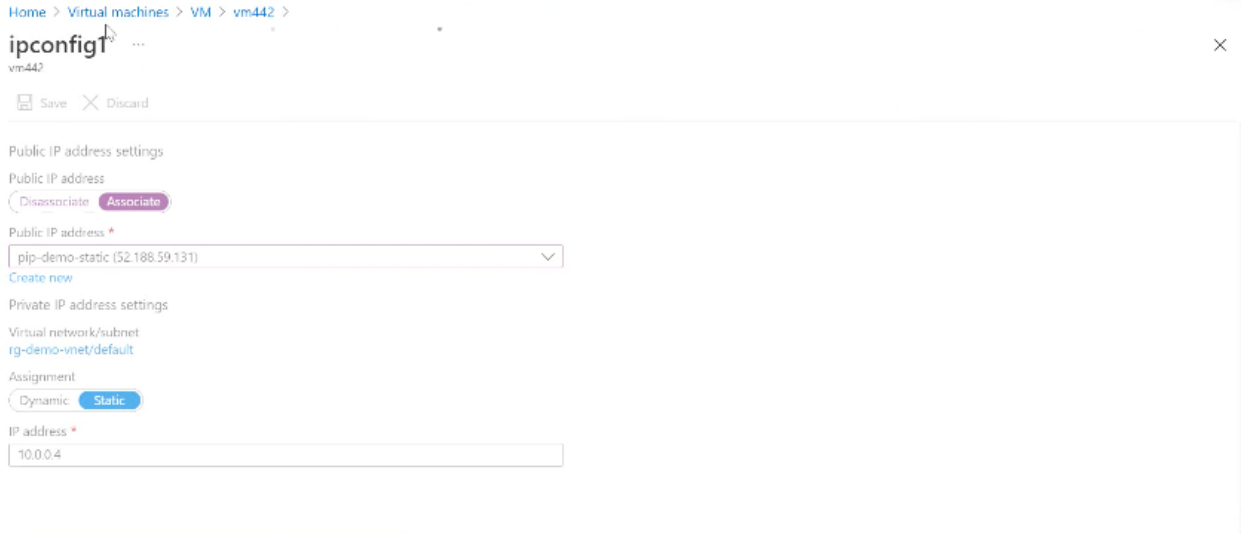



Azure services
Create a resource
Resource groups
Virtual machines
Subscriptions
Disks
Load balancers
Snapshots
Public IP addresses
Network security groups
More services
Recent resources
Name
Type
Last Viewed
vm442
Network interface
10 minutes ago
VM
Virtual machine
10 minutes ago
VM-ip
Public IP address
10 minutes ago
rg-demo
Resource group
17 minutes ago
Navigate
Subscriptions
Resource groups
All resources
Dashboard


Home
Public IP addresses
Default Directory
Deployment in progress...
Deployment to resource group 'rg-demo' is in progress.
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
Feedback
Filter for any field...
Subscription == all
Resource group == all
Location == all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Resource group
Location
Subscription
VM-ip
rg-demo
East US
Pay-As-You-Go
< Previous
Page 1 of 1
Next >


Home
pip-demo-static
Public IP address
Search (Ctrl+/)
Associate
Dissociate
Move
Delete
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Upgrade to Standard SKU - Microsoft recommends Standard SKU pub
Essentials
Resource group (change)
rg-demo
Location
East US
Subscription (change)
Pay-As-You-Go
Subscription ID
9b31fa70-6070-4595-9d04-c8bde414dede
Tags (change)
Click here to add tags
See more
Associate public IP address
pip-demo-static
Choose the resource to which you want to associate this public IP address.
Resource type
Load balancer
Load balancer
Network interface
Load balancer *
OK


Home
pip-demo-static
Public IP address
Search (Ctrl+/)
Associate
Dissociate
Move
Delete
Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Upgrade to Standard SKU - Microsoft recommends Standard SKU pub
Essentials
Resource group (change)
rg-demo
Location
East US
Subscription (change)
Pay-As-You-Go
Subscription ID
9b31fa70-6070-4595-9d04-c8bde414dede
Tags (change)
Click here to add tags
See more
Associate public IP address
pip-demo-static
Choose the resource to which you want to associate this public IP address.
Resource type
Network interface
Network interface *
Can be associated with this network interface
vm442
resource group: rg-demo
OK


Home > Virtual machines > VM > vm442 >
ipconfig1
vm442
Save
Discard
Public IP address settings
Public IP address
Disassociate
Associate
Public IP address *
pip-demo-static (52.188.59.131)
Create new
Private IP address settings
Virtual network/subnet
rg-demo-vnet/default
Assignment
Dynamic
Static
IP address *
10.0.0.4

This comprehensive article will cover the following aspects of NSGs:
1. **Security Rules**: Explanation of the properties and functionalities of security rules within NSGs.
2. **Default Security Rules**: Overview of the default rules created by Azure.
3. **Augmented Security Rules**: Details on creating complex security rules.
4. **Service Tags and Application Security Groups**: Explanation of service tags and application security groups to simplify security management.
5. **Azure Platform Considerations**: Special considerations for Azure infrastructure and services.
6. **Email Sending Rules**: Specific guidelines and rules for sending emails from Azure VMs.
7. **Next Steps**: Guidance on additional resources and tutorials for managing NSGs.

Security Rules

A Network Security Group contains multiple security rules, each defined by several properties. These properties allow precise control over the traffic allowed or denied by the NSG:

1. **Name**:
   - A unique identifier for the rule within the NSG.
   - Can be up to 80 characters long.
   - Must start with a word character and end with a word character or an underscore (`_`).
   - May contain word characters (`a-z`, `A-Z`, `0-9`), dots (`.`), hyphens (`-`), and underscores (`_`).

2. **Priority**:
   - A number between 100 and 4096.
   - Determines the order in which rules are processed, with lower numbers having higher priority.
   - Once traffic matches a rule, processing stops, ensuring no further rules are evaluated for that traffic.

3. **Source or Destination**:
   - Can be specified as an individual IP address, a CIDR block (e.g., `10.0.0.0/24`), a service tag, or an application security group.
   - For Azure resources, specify the private IP address assigned to the resource.
   - Network security groups process traffic after Azure translates public IP addresses to private IP addresses (for inbound traffic) and before translating private IP addresses to public IP addresses (for outbound traffic).

4. **Protocol**:
   - Can be TCP, UDP, ICMP, ESP, AH, or Any.
   - ESP (Encapsulating Security Payload) and AH (Authentication Header) protocols are not currently available via the Azure portal but can be configured using ARM templates.

5. **Direction**:
   - Indicates whether the rule applies to inbound or outbound traffic.

6. **Port Range**:
   - Specifies an individual port or a range of ports (e.g., 80 or 10000-10005).
   - Allows for creating fewer security rules by specifying port ranges.

7. **Action**:
   - Can either allow or deny the specified traffic.

Security rules in NSGs are evaluated and applied based on the five-tuple information (source IP, source port, destination IP, destination port, and protocol). The stateful nature of NSGs means that once a connection is allowed, its subsequent packets are allowed automatically without re-evaluation, unless the rule set changes.

Default Security Rules

Azure creates several default security rules in each NSG, which you cannot remove but can override by creating higher-priority rules:

1. **Inbound Rules**:
   - **AllowVNetInBound**:
     - Priority: 65000
     - Source: VirtualNetwork
     - Source Ports: 0-65535
     - Destination: VirtualNetwork
     - Destination Ports: 0-65535
     - Protocol: Any
     - Action: Allow

   - **AllowAzureLoadBalancerInBound**:
     - Priority: 65001
     - Source: AzureLoadBalancer
     - Source Ports: 0-65535
     - Destination: 0.0.0.0/0
     - Destination Ports: 0-65535
     - Protocol: Any
     - Action: Allow

   - **DenyAllInbound**:
     - Priority: 65500
     - Source: 0.0.0.0/0
     - Source Ports: 0-65535
     - Destination: 0.0.0.0/0
     - Destination Ports: 0-65535
     - Protocol: Any
     - Action: Deny

2. **Outbound Rules**:
   - **AllowVNetOutBound**:
     - Priority: 65000
     - Source: VirtualNetwork
     - Source Ports: 0-65535
     - Destination: VirtualNetwork
     - Destination Ports: 0-65535
     - Protocol: Any
     - Action: Allow

   - **AllowInternetOutBound**:
     - Priority: 65001
     - Source: 0.0.0.0/0
     - Source Ports: 0-65535
     - Destination: Internet
     - Destination Ports: 0-65535
     - Protocol: Any
     - Action: Allow

   - **DenyAllOutBound**:
     - Priority: 65500
     - Source: 0.0.0.0/0
     - Source Ports: 0-65535
     - Destination: 0.0.0.0/0
     - Destination Ports: 0-65535
     - Protocol: Any
     - Action: Deny

In the Source and Destination columns, service tags like VirtualNetwork, AzureLoadBalancer, and Internet are used rather than specific IP addresses. The protocol column can be Any, encompassing TCP, UDP, and ICMP.

Augmented Security Rules

Augmented security rules are designed to simplify the definition of complex security policies by allowing the combination of multiple ports and IP addresses into a single rule. This reduces the number of rules needed and simplifies management. These rules can only be created in NSGs through the Resource Manager deployment model and allow specifying multiple ports and IP ranges in a single rule.

Service Tags and Application Security Groups

- **Service Tags**: Represent a group of IP address prefixes from specific Azure services, minimizing the need for frequent updates to network security rules. Examples include tags for Azure services like Storage, SQL, and Cosmos DB.

- **Application Security Groups**: Allow grouping of virtual machines and defining network security policies based on these groups, facilitating scalable and manageable security configurations. Application security groups help avoid the need for manual IP address maintenance.

Azure Platform Considerations

When configuring NSGs, it's essential to consider certain Azure platform specifics:

1. **Virtual IP of the Host Node**: Basic infrastructure services like DHCP, DNS, IMDS, and health monitoring use specific virtualized IP addresses (168.63.129.16 and 169.254.169.254). These addresses are used across all Azure regions and are not typically subject to NSG rules unless explicitly targeted.

2. **Licensing (Key Management Service)**: VMs need to communicate with Key Management Service (KMS) servers for licensing via port 1688. In deployments using the default route configuration (0.0.0.0/0), this rule is disabled by default.

3. **Virtual Machines in Load-Balanced Pools**: The source port and address range applied are from the originating computer, not the load balancer. The destination port and address range are for the destination computer.

4. **Azure Service Instances**: Instances of several Azure services (e.g., HDInsight, Application Service Environments, Virtual Machine Scale Sets) are deployed in virtual network subnets. It is crucial to understand the port requirements for these services before applying NSGs.

5. **Sending Outbound Email**: Azure recommends using authenticated SMTP relay services for sending emails from VMs. Depending on your subscription type, outbound communication over port 25 might be restricted:

   - **Enterprise Agreement**: Typically allows outbound SMTP connections on port 25, but with potential restrictions.
   - **Other Subscriptions**: Often block port 25, requiring the use of SMTP relay services like Exchange Online Protection or SendGrid.

Next Steps

To continue exploring and managing NSGs effectively, consider the following resources and tutorials:

1. **Virtual Network Integration for Azure Services**: Learn which Azure resources can be deployed into a virtual network and associated with NSGs.
2. **How Network Security Groups Work**: Understand the detailed mechanics of how NSGs evaluate and process traffic.
3. **Creating and Managing NSGs**: Use Azure portal, CLI, or PowerShell to create and

manage NSGs.
4. **Troubleshooting**: Diagnose communication issues related to NSGs.
5. **Flow Logs**: Enable NSG flow logs to analyze network traffic to and from resources with associated NSGs.

By effectively configuring and managing Network Security Groups, you can enhance the security and compliance of your Azure environment, ensuring that network traffic is strictly controlled and monitored according to your organizational policies.