-Om Wabale

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

An **NSG** is a virtual firewall for Azure subnets or NICs. It filters inbound/outbound traffic based on rules matching source/destination IP, port, and protocol. NSGs are **stateful**: once a session is allowed, return traffic is automatically permitted. Each NSG rule has a priority (100–4096; lower number = higher priority) and is processed in order. Azure creates default rules in every NSG (e.g. *AllowVNetInbound*, *AllowAzureLoadBalancerInbound*, *DenyAllInbound*) so that intra-VNet traffic is permitted and all other inbound traffic is denied by default. You can override defaults by adding higher-priority rules.

Application Security Groups (ASGs) let you group virtual machine NICs by workload or role. You then write NSG rules referring to an ASG instead of explicit IPs. For example, you might have ASGs named *AsgWeb*, *AsgLogic*, and *AsgDb* containing different VM NICs. An NSG rule could allow HTTP from **Internet** to *AsgWeb* and deny other inbound traffic, or allow only *AsgLogic* to reach *AsgDb*. ASGs enable scaling security policies without renumbering IPs. The diagram below illustrates NICs in three ASGs under one NSG that permits only specific flows. ASGs simplify network rules by grouping NICs and treating each group as a single entity.

Figure: Example of Application Security Groups (AsgWeb, AsgLogic, AsgDb) with an NSG. NICs 1–2 are in AsgWeb, NIC3 in AsgLogic, NIC4 in AsgDb. The NSG has rules (e.g., allow HTTP from Internet to AsgWeb) that apply to all NICs in each ASG.

Service Tags are labels for well-known IP address ranges of Azure services. Using a service tag (like VirtualNetwork, Internet, Storage, etc.) in an NSG rule replaces specifying multiple IP ranges. For example, the default NSG rules use the tag **VirtualNetwork** to mean “all IPs in the virtual network” and **AzureLoadBalancer** for Azure’s load balancer addresses. The **Internet** tag represents all public IPs outside the VNet. Service tags minimize rule updates: when a service’s IP ranges change, Azure updates the tag automatically. A service tag is essentially a set of IP prefixes for an Azure service.

Restricting VM Access with NSGs

To allow only specific clients to reach a VM and block all other Internet traffic, use NSG rules with precise sources and priorities. For example, create an **Allow** inbound rule with **Source = your specific IP (or CIDR)** and **Destination = VM’s subnet/NIC**, on the required port. Give it a higher priority (lower number) than the default deny. All other sources will hit the default **DenyAllInbound** rule (priority 65500) and be blocked. If you prefer explicitly blocking external traffic, you can add a rule with source = **“Internet”** (service tag) and Action = Deny. Because NSGs are stateful, once an allowed connection is established, return traffic is automatically permitted. The key is rule ordering: custom allow rules must have a higher priority than any deny for the same traffic. In practice, to permit RDP from one IP and deny all else, put the allow rule above the deny-all rule.

Azure Public IP Addresses

A **Public IP address** in Azure is a resource that you assign to enable inbound Internet access to Azure services (VMs, load balancers, Application Gateways, etc.) and to give predictable outbound connectivity. Public IPs come in two SKUs: **Basic** and **Standard**. Standard SKU is recommended for production (it supports Availability Zones and is zone-redundant by default). Basic SKU is older and cannot be changed to Standard; it does not support zones and provides limited features. Each public IP also has a **tier**: *Regional* (default) or *Global* (preview feature used for cross-region load balancers). When you create a public IP, you choose the IP version (IPv4 or IPv6) and an assignment method: **Static** or **Dynamic**. Static assignment reserves the IP at creation time and it persists until the resource is deleted; dynamic means Azure allocates the IP from the region’s pool when the associated resource (e.g. VM) starts. A static IPv4 address will never change, while a dynamic IPv4 address can change if you stop-deallocate the VM. (Note: IPv6 addresses under Basic SKU must be dynamic, and Standard SKUs are static by default for IPv4/IPv6.)

Public IP routing: By default, Azure routes traffic over Microsoft’s global network, but you can set the routing preference to *Internet* to use ISP transit (possibly lower latency). This is chosen at creation and cannot be changed later.

Static vs. Dynamic IP Addresses

The terms *static* and *dynamic* apply both to public and private (VM) IPs. For **public IPs**, static means the address is allocated at creation (e.g. 52.165.10.5) and stays fixed; dynamic means the address is assigned on VM start and may change on deallocation. For **VM private IPs**, the default is dynamic: Azure automatically gives the next available address from the subnet, and it is retained by the VM until it’s deleted or deallocated. To make a VM’s private IP static, you modify its network interface (NIC) configuration to static assignment. In the portal or CLI, set the NIC’s IP config *Allocation* to **Static** and specify the address. This reserves that IP for the VM. Static private IPs are useful for stable internal addressing (for example, when IP-to-IP licensing or firewall rules require fixed addresses).

Creating a Network Security Group

To create an NSG in the Azure portal: go to **Network security groups** and click **+ Create**. On the Basics tab, specify your Subscription and Resource Group, give the NSG a **Name**, and pick a **Region**. Then click *Review + create* and *Create*. This makes an empty NSG (with default rules). You can then add your own **Inbound/Outbound security rules** under the NSG's *Settings* to allow or deny specific traffic.

Creating a Public IP Address

To create a public IP in the portal, search for **Public IP addresses** and click **Create**. On the Basics tab, choose your Subscription and Resource Group, enter a **Name** for the IP resource, select the **IP Version** (IPv4 or IPv6), the **SKU** (Standard or Basic), and set the **Assignment** method (Static or Dynamic). For a Standard SKU IPv4, the assignment is static by default. You can also select an Availability Zone or make it Zone-Redundant if needed. After filling in these fields, click *Review + create* then *Create* to allocate the public IP. The new public IP resource can then be associated with VMs or other services.

Associating a Public IP with a VM

Each public IP is attached to a VM by associating it to that VM's network interface configuration. In the portal, open the VM's **Networking** tab and click the network interface. Under **Settings → IP configurations**, edit the primary IP configuration. Choose **Associate** next to Public IP address, then pick an existing public IP from the dropdown (or create a new one). Save the changes. The VM will then be reachable at that public IP (provided you open the necessary ports in the NSG). You can also do this via CLI or PowerShell using az network nic ip-config update with the --public-ip-address parameter.

Disassociating a Public IP from a VM

To remove a public IP, simply disassociate it from the VM's NIC. In the portal's Network Interface IP configuration, click **Dissociate** (or remove the public IP setting). This frees the public IP address (though it remains as a resource until you delete it). After dissociation, you can delete the public IP resource if it's no longer needed. (CLI/PowerShell methods also exist: e.g. az network nic ip-config update with --remove public-ip-address and then az network public-ip delete.)

Network Interfaces (NIC) and IP Configuration

A **Network Interface (NIC)** is the logical network card attached to a VM that connects it to a virtual network. When you create a VM in the portal, Azure automatically makes one NIC with default settings. You can also create NICs manually (for example, to attach multiple NICs to a VM). In the portal, go to **Network interfaces → +Add**, and fill in the fields: Name, Resource Group, Region. Then select the **Virtual network** and **Subnet** where it will reside. Choose the **IP version** (IPv4 or IPv6) and whether to allocate its private IP **Dynamic** or **Static**. If you pick

Static, you must enter an unused IP address from that subnet. The portal does not allow assigning a public IP at NIC creation time, but you can add one afterward.

Each NIC has an IP configuration. By default a NIC has one **Primary** configuration with a private IP. You can add **Secondary** IP configurations if needed. Both private and public IPs attach here. To set or change the private IP: go to the NIC's **IP configurations**, edit the entry, and for *Private IP address assignment* choose **Static** (and enter the address) or **Dynamic**. To associate a public IP to a NIC, in the same place choose **Associate** under *Public IP address* and select an existing or new public IP.

In summary, Azure NSGs and ASGs provide flexible, scalable network filtering (using explicit IPs, CIDRs, ASGs, and service tags). By combining NSG rule priorities, static IP assignments, service tags, and careful configuration of public IPs and NICs, you can tightly control which clients access your VMs and how VMs reach the Internet.

1. Overview of NSG & ASG

Network Security Group (NSG):

- Acts as a virtual firewall controlling inbound and outbound traffic for Azure resources.
- Rules filter traffic based on source/destination IP, port, and protocol.
- Can be associated with subnets or individual NICs.
- Stateful: return traffic is automatically allowed.

Application Security Group (ASG):

- Logical grouping of NICs.
- Enables simplified management by grouping VMs by role (e.g., Web, DB).
- NSG rules can refer to ASG names instead of specific IPs.

2. Allowing Specific IPs and Denying Internet via NSG

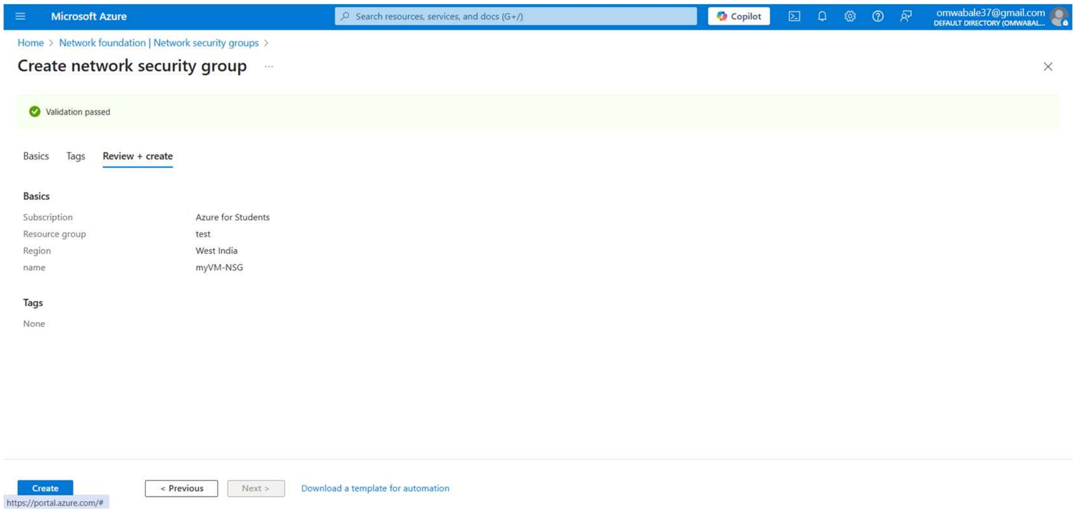
Objective:

- Allow access to VM from specific IP(s).
- Block all other internet traffic.

Steps:

1. Go to **Network Security Groups** in the Azure portal.
2. Open NSG > Inbound Security Rules > Add rule.

3. **Source**: IP Addresses
4. **Source IP**: Enter the allowed IP (e.g., 203.0.113.5).
5. **Destination**: Any or specific VM NIC/subnet.
6. **Port**: Enter required port (e.g., 22 for SSH).
7. **Action**: Allow
8. **Priority**: e.g., 100 (lower = higher priority)
9. Add a **Deny** rule with **Source = Internet** and higher priority number


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
omwabale37@gmail.com
DEFAULT DIRECTORY (OMWABAL...
Home > Network foundation | Network security groups >

Create network security group

Validation passed

Basics
Tags
Review + create

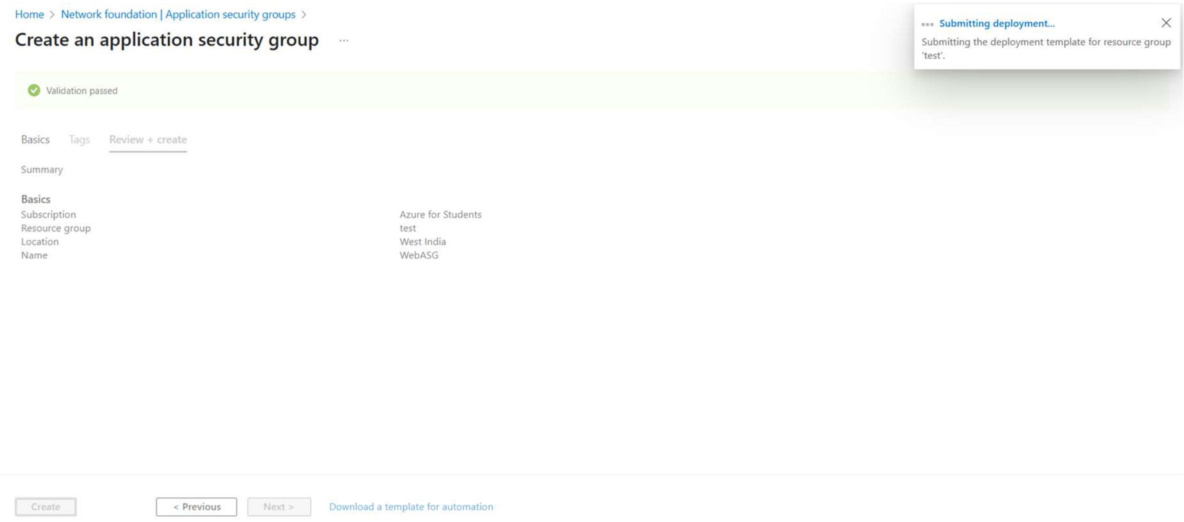
Basics

Subscription: Azure for Students
Resource group: test
Region: West India
name: myVM-NSG

Tags

None

Create
https://portal.azure.com/#
< Previous
Next >
Download a template for automation


Home > Network foundation | Application security groups >

Create an application security group

Submitting deployment...

Submitting the deployment template for resource group 'test'.

Validation passed

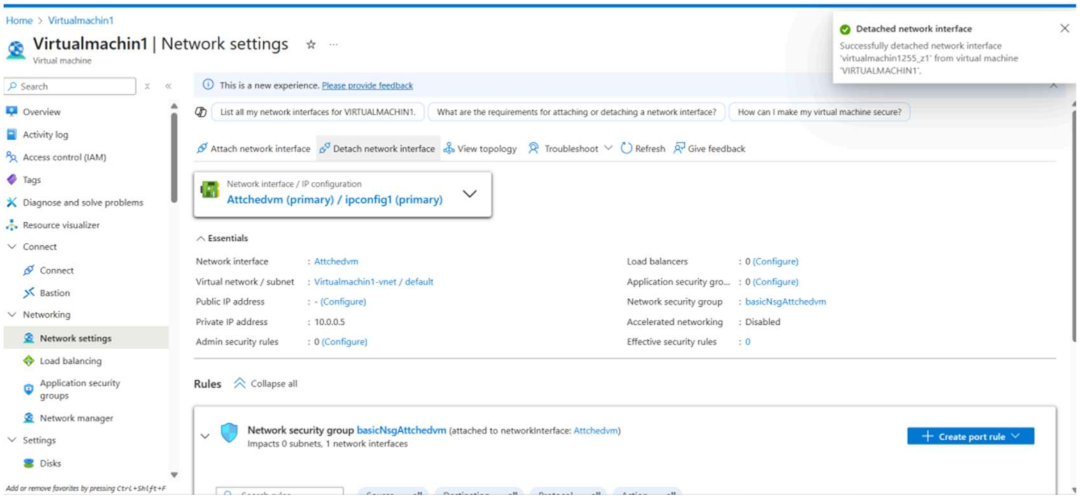
Basics
Tags
Review + create

Summary

Basics

Subscription: Azure for Students
Resource group: test
Location: West India
Name: WebASG

Create
< Previous
Next >
Download a template for automation



Virtualmachin1 | Network settings

Virtual machine

Detached network interface

Successfully detached network interface 'virtualmachin1255_z1' from virtual machine 'VIRTUALMACHIN1'.

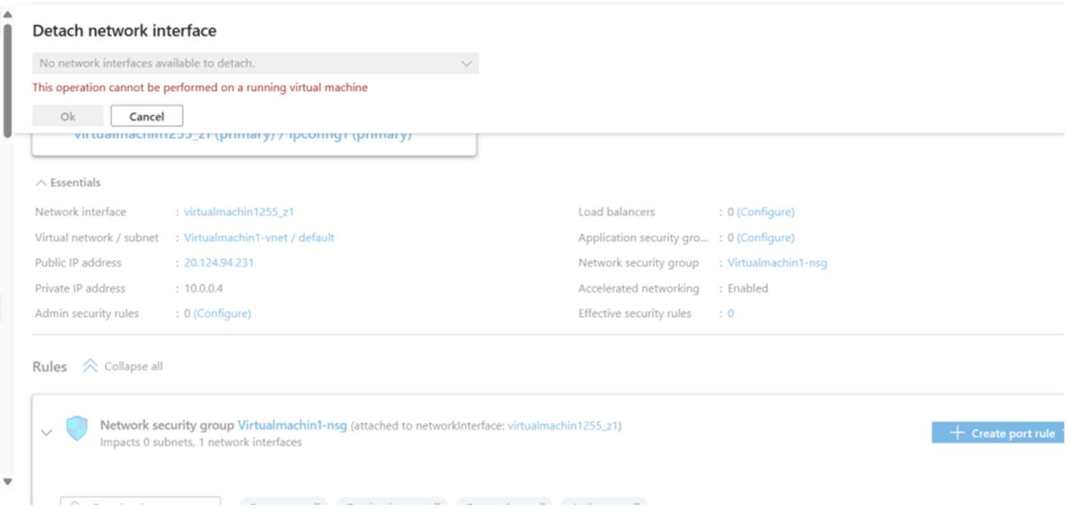
This is a new experience. Please provide feedback

Network interface / IP configuration: Attchedvm (primary) / ipconfig1 (primary)

Essentials

Network interface	: Attchedvm	Load balancers	: 0 (Configure)
Virtual network / subnet	: Virtualmachin1-vnet / default	Application security gro...	: 0 (Configure)
Public IP address	: - (Configure)	Network security group	: basicNsgAttchedvm
Private IP address	: 10.0.0.5	Accelerated networking	: Disabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Network security group basicNsgAttchedvm (attached to networkInterface: Attchedvm)
Impacts 0 subnets, 1 network interfaces



Detach network interface

No network interfaces available to detach.

This operation cannot be performed on a running virtual machine

virtualmachin1255_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface	: virtualmachin1255_z1	Load balancers	: 0 (Configure)
Virtual network / subnet	: Virtualmachin1-vnet / default	Application security gro...	: 0 (Configure)
Public IP address	: 20.124.94.231	Network security group	: Virtualmachin1-nsg
Private IP address	: 10.0.0.4	Accelerated networking	: Enabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Network security group Virtualmachin1-nsg (attached to networkInterface: virtualmachin1255_z1)
Impacts 0 subnets, 1 network interfaces

3. Public IPs: Types and Assignment

Static Public IP:

- Assigned at creation and never changes.
- Required for DNS mappings, production apps.

Dynamic Public IP:

- Assigned when resource starts.
- May change on VM deallocation.

SKU:

- **Basic**: Limited functionality, no availability zones.
- **Standard**: Zone-redundant, more secure and recommended.

4. Service Tags in NSG

Definition:

- Predefined labels for IP ranges of Azure services.
- Examples: Internet, VirtualNetwork, AzureLoadBalancer, Storage.

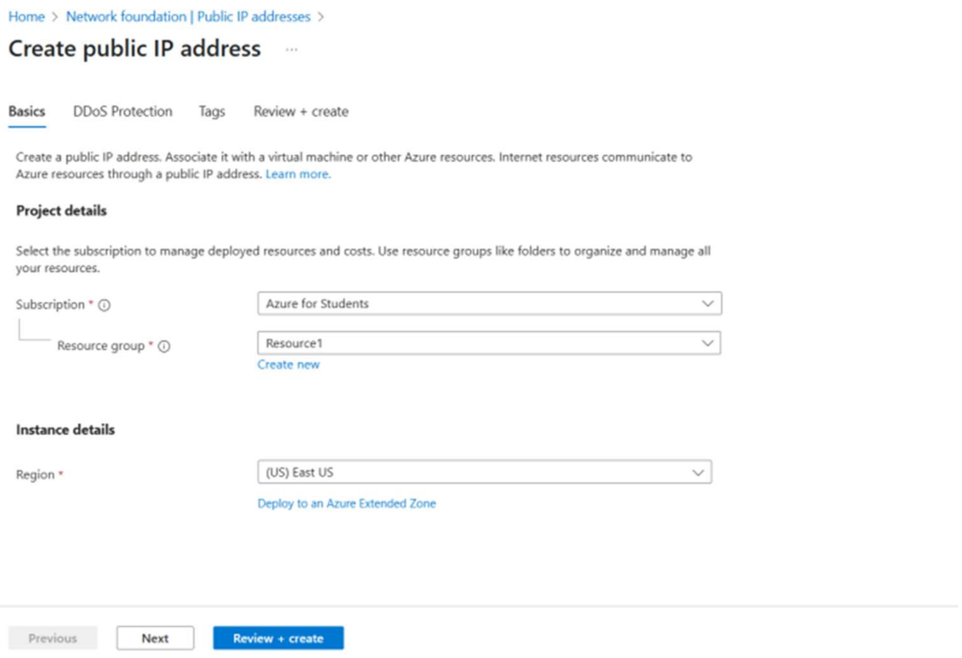
Usage:

- In NSG rules, select Service Tag instead of IP ranges.

5. Allocating Static IPs to All VMs (Private IP)

Steps:

1. Go to VM > Networking > Click NIC.
2. Under Settings > IP configurations > Click on primary IP config.
3. Set **Private IP assignment** to **Static**.
4. Assign unused IP within subnet range.
5. Save configuration.



Create public IP address ...

Create a public IP address. Associate it with a virtual machine or other Azure resources. Internet resources communicate to Azure resources through a public IP address. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure for Students

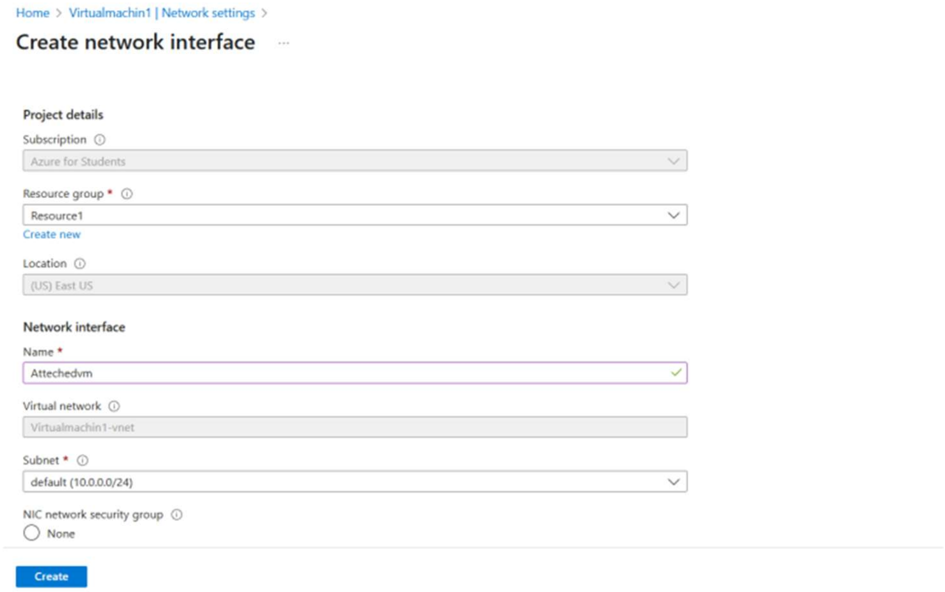
Resource group * : Resource1

Create new

Instance details

Region * : (US) East US

Deploy to an Azure Extended Zone


Home > Virtualmachin1 | Network settings >

Create network interface ...

Project details

Subscription: Azure for Students

Resource group *: Resource1

Create new

Location: (US) East US

Network interface

Name *: Attechedvm

Virtual network: Virtualmachin1-vnet

Subnet *: default (10.0.0.0/24)

NIC network security group: ○ None

6. Creating a Network Security Group (NSG)

Steps:

1. Go to **Network Security Groups** > **+ Create**.
2. Enter:
   - Subscription
   - Resource Group
   - NSG Name
   - Region
3. Click **Review + create** > **Create**.

7. Creating a Public IP

Steps:

1. Go to **Public IP addresses** > **+ Create**.
2. Enter:
   - Name
   - SKU: Standard or Basic

- Assignment: Static or Dynamic
- IP Version: IPv4 or IPv6

3. Click **Review + create** > **Create**.

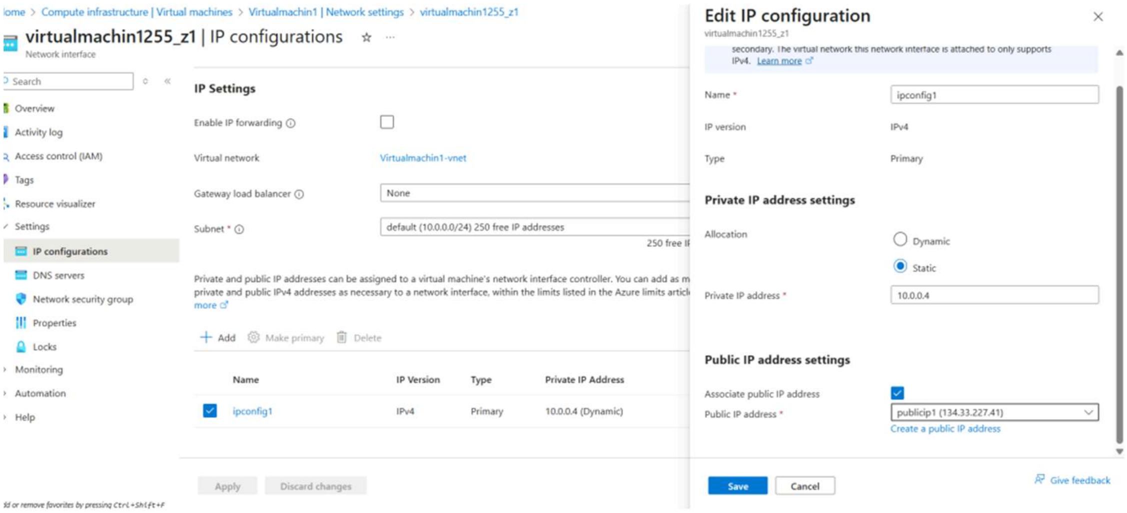
8. Associating/De-associating Public IP with VM

Associate:

1. Go to **VM > Networking**.
2. Click the NIC > IP configurations.
3. Edit primary IP config.
4. Under Public IP address, click **Associate**.
5. Select existing or new Public IP.

De-associate:

1. Open NIC > IP configurations.
2. Edit primary IP config.
3. Click **Dissociate** or set Public IP to None.



virtualmachin1255_z1 | IP configurations

Network interface

IP Settings

Enable IP forwarding ⓘ ☐

Virtual network: Virtualmachin1-vnet

Gateway load balancer ⓘ: None

Subnet * ⓘ: default (10.0.0.0/24) 250 free IP addresses

250 free I

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as m private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits articl more

	Name	IP Version	Type	Private IP Address
☑	ipconfig1	IPv4	Primary	10.0.0.4 (Dynamic)

Edit IP configuration

virtualmachin1255_z1

secondary. The virtual network this network interface is attached to only supports IPv4. Learn more

Name *: ipconfig1

IP version: IPv4

Type: Primary

Private IP address settings

Allocation: ○ Dynamic ● Static

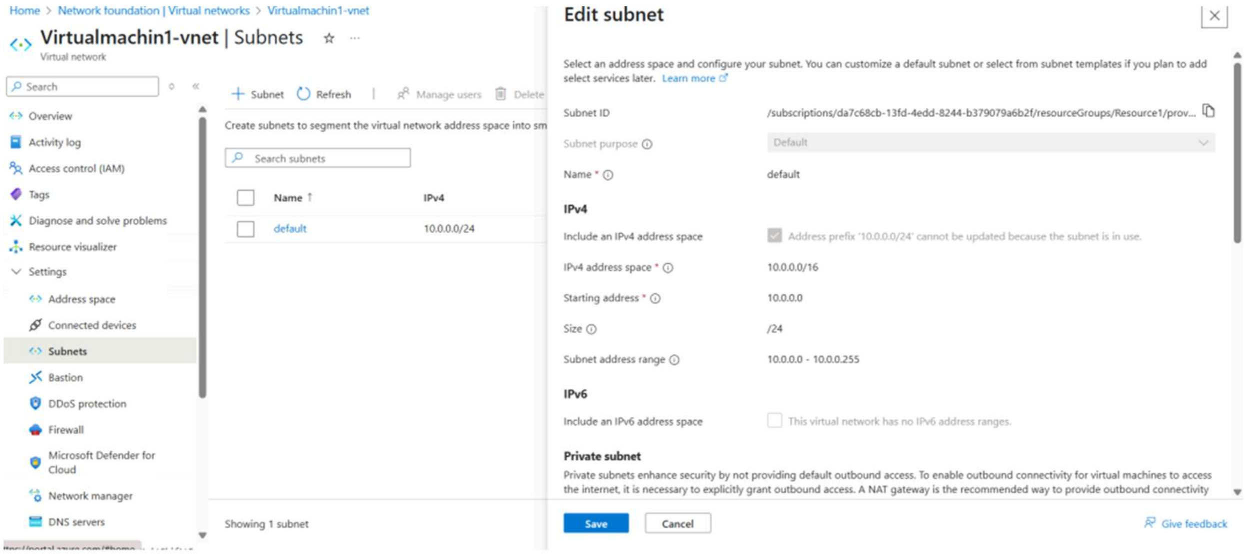
Private IP address *: 10.0.0.4

Public IP address settings

Associate public IP address ☑

Public IP address *: publicip1 (134.33.227.41)

Create a public IP address



Create subnets to segment the virtual network address space into sm

Name ↑	IPv4
default	10.0.0.0/24

Showing 1 subnet

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet ID: /subscriptions/da7c68cb-13fd-4edd-8244-b379079a6b2f/resourceGroups/Resource1/prov...

Subnet purpose: Default

Name *: default

IPv4

Include an IPv4 address space: ☑ Address prefix '10.0.0.0/24' cannot be updated because the subnet is in use.

IPv4 address space *: 10.0.0.0/16

Starting address *: 10.0.0.0

Size: /24

Subnet address range: 10.0.0.0 - 10.0.0.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity

9. Creating a Network Interface (NIC)

Steps:

1. Go to **Network interfaces** > **+ Add**.
2. Enter:
   - Name
   - Resource Group
   - Region
   - Virtual Network & Subnet
   - Private IP: Static or Dynamic
3. Click **Review + create** > **Create**.

Conclusion

With NSGs, ASGs, and proper IP configurations, Azure allows fine-grained access control to VMs. This architecture ensures secure exposure of services while maintaining internal network flexibility using ASGs and service tags.