NSG & ASG

1. Network Security Group (NSG)

A Network Security Group (NSG) is a fundamental security feature within Microsoft Azure, used to enforce access controls at both the subnet and individual network interface (NIC) level. It acts as a stateful, rule-based firewall that governs inbound and outbound traffic to Azure resources, ensuring that only authorized network communications are permitted within a virtual network.

Core Components:

- **Security Rules:** Each NSG contains a list of rules that define allowed or denied traffic. These rules apply to both **inbound** (incoming) and **outbound** (outgoing) traffic directions.

- **Priority:** Each rule is assigned a priority between 100 and 4096. Rules are evaluated in ascending order, lower numbers take precedence. If a packet matches a rule, the defined action is taken, and subsequent rules are ignored.

- **Rule Properties:**
    - **Direction:** Whether the rule applies to traffic entering (*Inbound*) or leaving (*Outbound*) the resource.
    - **Port Range:** Specific port(s) to which the rule applies, such as 22 (SSH) or 443 (HTTPS).
    - **Protocol:** Supported values include TCP, UDP, or Any.
    - **Source & Destination:** Can be defined using IP addresses, subnets, service tags, or Application Security Groups (ASG).
    - **Action:** Indicates whether the traffic is **Allowed** or **Denied**.

How NSGs Work:

When a packet is received, Azure evaluates the NSG rules in order of priority. The first rule that matches the traffic pattern determines the fate of the packet. This evaluation ensures optimal performance and a predictable security outcome. If no user-defined rules match, Azure applies default rules which are always present in every NSG.

These default rules are non-editable and provide a baseline level of protection. Custom rules must have a lower priority (numerically higher) to override these.

Common Use Cases:

1. **Restrict Internet Access:**
    - Create an outbound rule with destination set to the `Internet` service tag.
    - Set action to **Deny** and assign a priority lower than the default rule (e.g., 100).
    - This effectively blocks all VMs/subnets from making outbound connections to the internet.

2. **Permit Access from Specific IPs/Subnets:**
    - Add inbound rules that allow access only from defined public IP addresses or internal subnets.
    - Useful for limiting management access (e.g., SSH/RDP) to corporate IPs only.

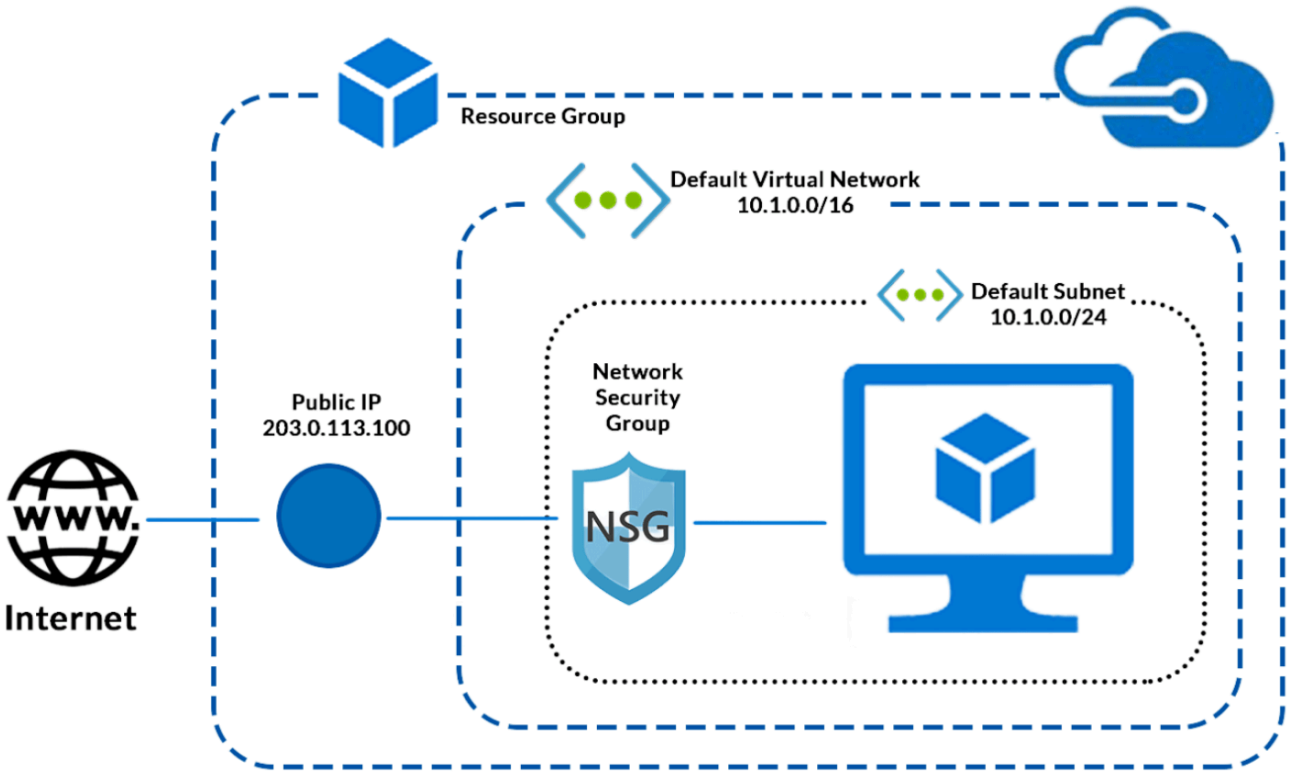
3. **Subnet Isolation:**
    - Apply different NSGs to different subnets to enforce strict communication boundaries.
    - For example, prevent the web tier from accessing the database tier directly.

4. **Granular Application Control:**
    - Combine NSGs with Application Security Groups to manage large-scale environments.
    - Enables grouping of VM roles (Web, App, DB) and simplifies rule creation.

5. **Secure Hybrid Connectivity:**
    - When using ExpressRoute or VPN Gateway, NSGs can be configured to restrict on-premises traffic to specific Azure resources.

Best Practices:

- Use **ASGs** and **service tags** instead of hardcoded IP addresses where possible.
- Implement **least privilege** principles: allow only what's necessary and deny everything else.
- Regularly **audit NSG rules** to remove outdated or overly permissive configurations.
- Apply NSGs at the **subnet level** for broader control and at the **NIC level** for fine-grained exceptions.



2. Application Security Group (ASG)

An Application Security Group (ASG) in Azure is a logical container that allows virtual machines (VMs) with similar functions such as web servers, application servers, or database servers, to be grouped together. This enables role-based segmentation of workloads and significantly simplifies the management of security rules in Network Security Groups (NSGs). Instead of assigning IP addresses or subnets directly in NSG rules, you can reference ASGs, making the configuration more scalable, maintainable, and intuitive.

How It Works:

- **NSG Integration:** ASGs can be used as the source and/or destination in NSG rules. This allows administrators to define access policies between workload tiers based on logical groupings rather than static IP addresses.

- **Dynamic Membership:** Virtual machines are added to ASGs by associating their Network Interface (NIC) with one or more ASGs. The VM automatically inherits the access rules defined via NSGs referencing the ASG, there's no need to update the rules manually if VMs are added or removed.

- **Decouples IP Management:** Because ASGs abstract away individual IPs, they eliminate the need to track or modify rules when IP addresses change, especially in environments using dynamic addressing.

Use Case Example:

Imagine a three-tier application architecture with separate VMs for web, application, and database roles:

- Create an ASG named `Web-ASG` for web servers
- Create another ASG named `DB-ASG` for database servers
- In the NSG, define an inbound rule that allows only `Web-ASG` to initiate connections to `DB-ASG` on port 1433 (SQL Server)

This setup ensures that only web servers can access the database layer, while other resources within the virtual network remain isolated, following the principle of least privilege.

Benefits:

- Simplifies rule management in environments with many VMs
- Enhances readability and intent of security policies
- Adapts well to dynamic scaling and automation workflows
- Reduces risk of misconfiguration due to static IP dependency

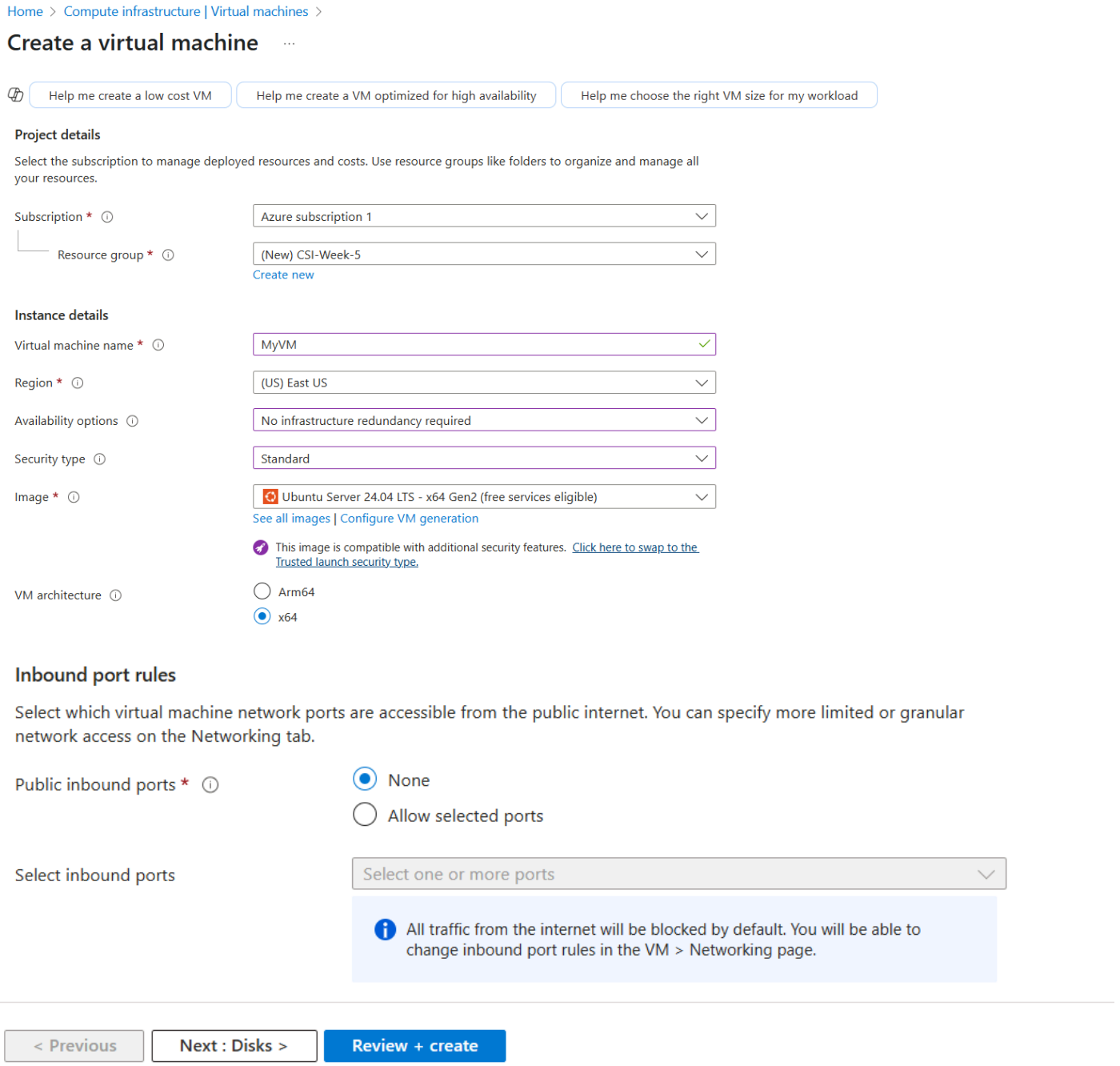
Best Practice:

- Use ASGs in every environment with tiered or role-based application design
- Combine ASGs with NSGs for layered security control
- Keep ASG naming consistent and role-specific (e.g., `web-tier-asg`, `db-tier-asg`)

3. Implementation Steps(on Azure Cloud)

1. Create a Virtual Machine (VM)

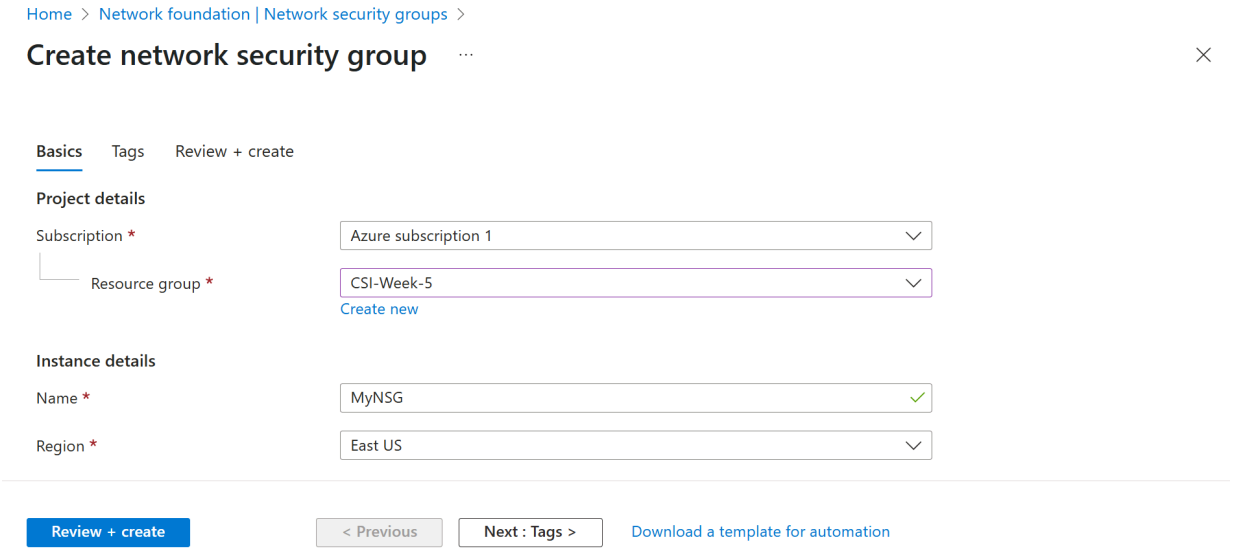
- Go to Virtual Machines > Create
- Select:
  - Subscription, Resource Group
  - VM Name (e.g., `MyVM`)
  - Region (e.g., US East)
- Image: Choose Ubuntu or Windows
- Size: Choose a small size (e.g., `B1s`)
- Authentication: Choose password or SSH
- Public inbound ports: Select None (We'll allow specific IPs later)
- Click Next through all tabs and click **Create**



Now, you have a VM created without internet access or open ports.

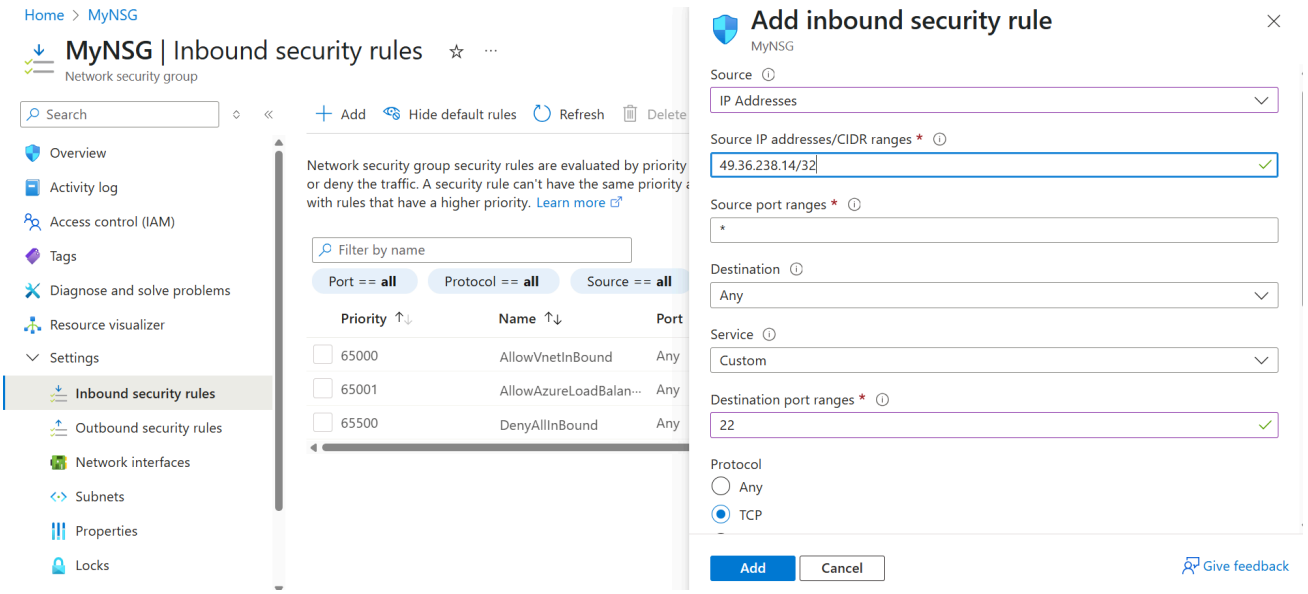
2. Create a Network Security Group (NSG)

- Search Network Security Groups > Create
- Fill in:
  - Name: `MyNSG`
  - Region: same as VM
  - Resource group: same as VM
- Click Review + Create > Create



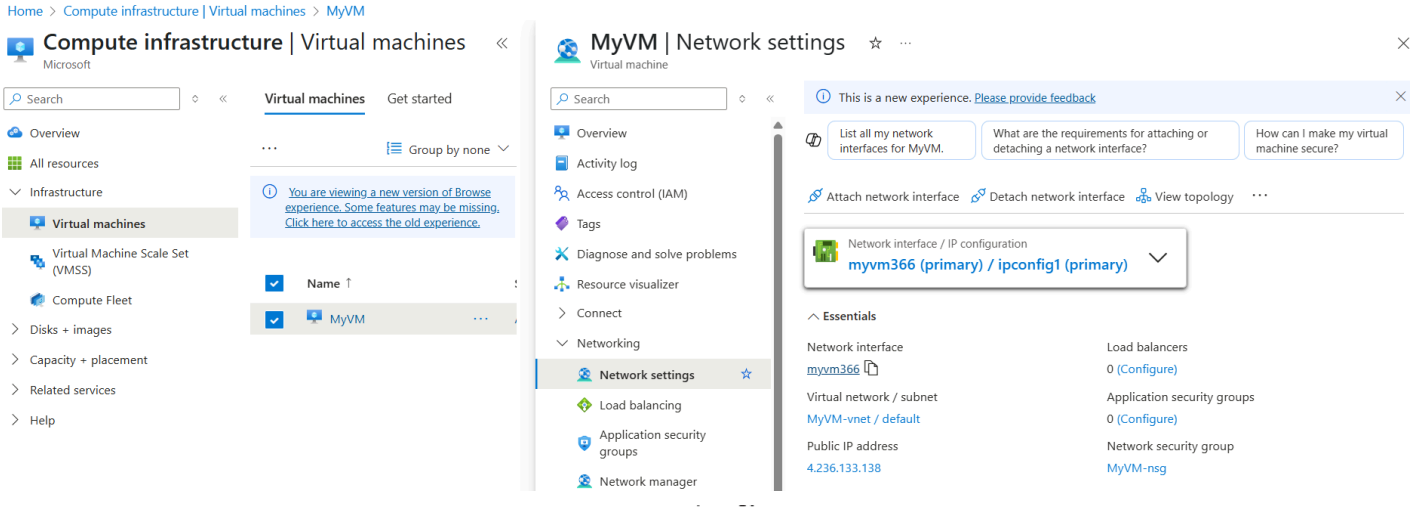
3. Add Inbound Rule to Allow a Specific IP (e.g., your laptop)

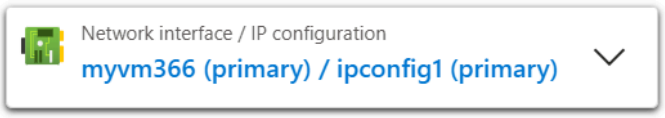
- Go to your NSG > Inbound security rules
- Click + Add
  - Source: **IP Addresses**
  - Source IP: e.g., `203.0.113.5` (or use https://whatismyipaddress.com to get your IP)
  - Protocol: **TCP**
  - Port: `22` (Linux) or `3389` (Windows)
  - Action: **Allow**
  - Priority: `100`
  - Name: `AllowSSHFromMyIP`
- Click Add

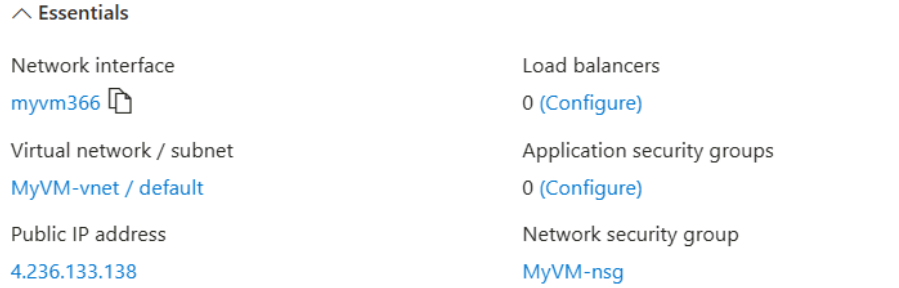


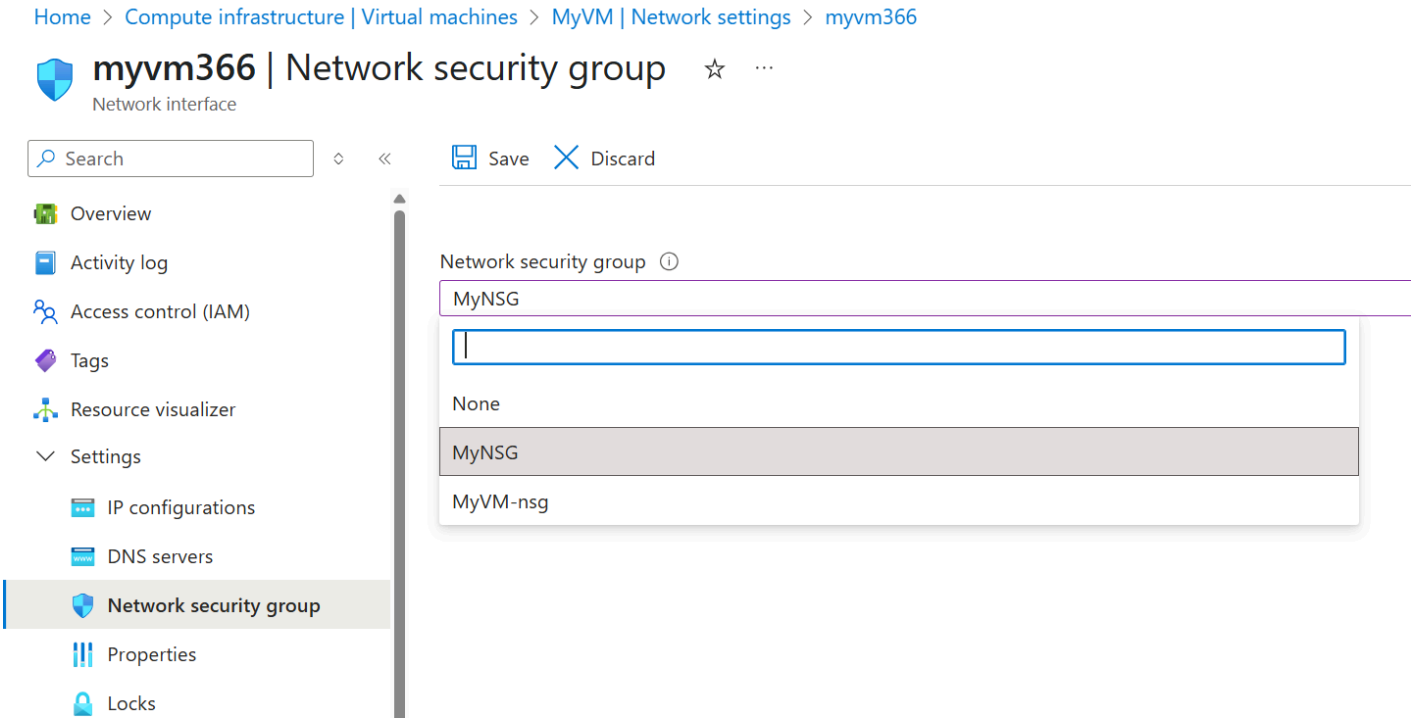
4. Associate NSG with the VM's Network Interface

- Go to your Virtual Machine > Networking
- Click the Network Interface (NIC) name
- In the NIC pane, go to Network Security Group
- Click Associate NSG > Select `MyNSG`



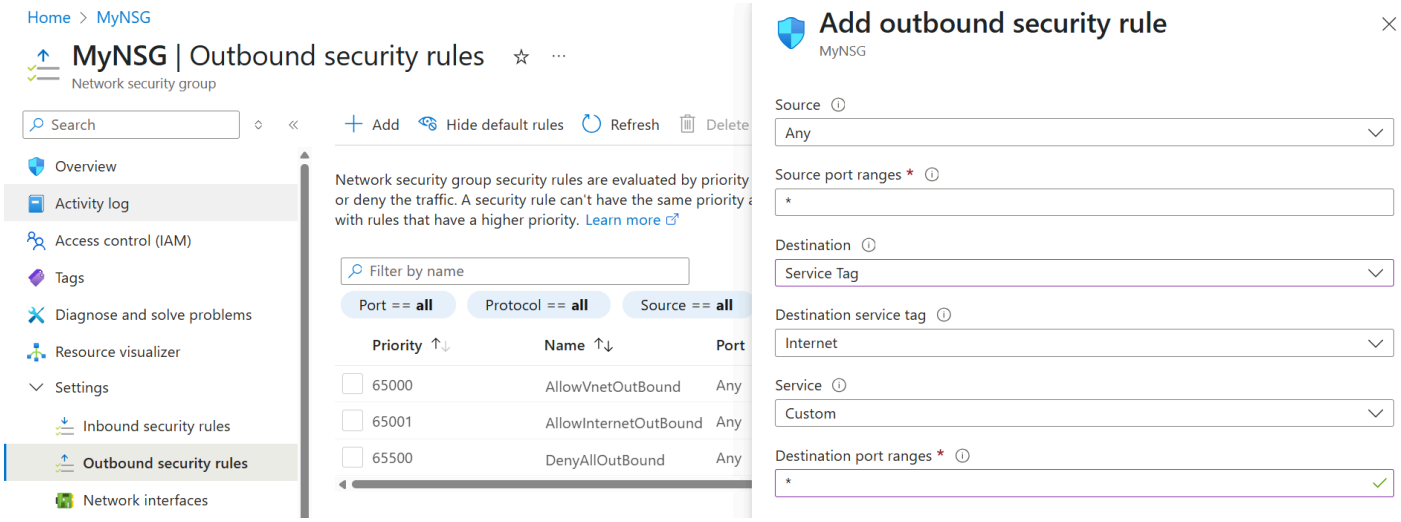


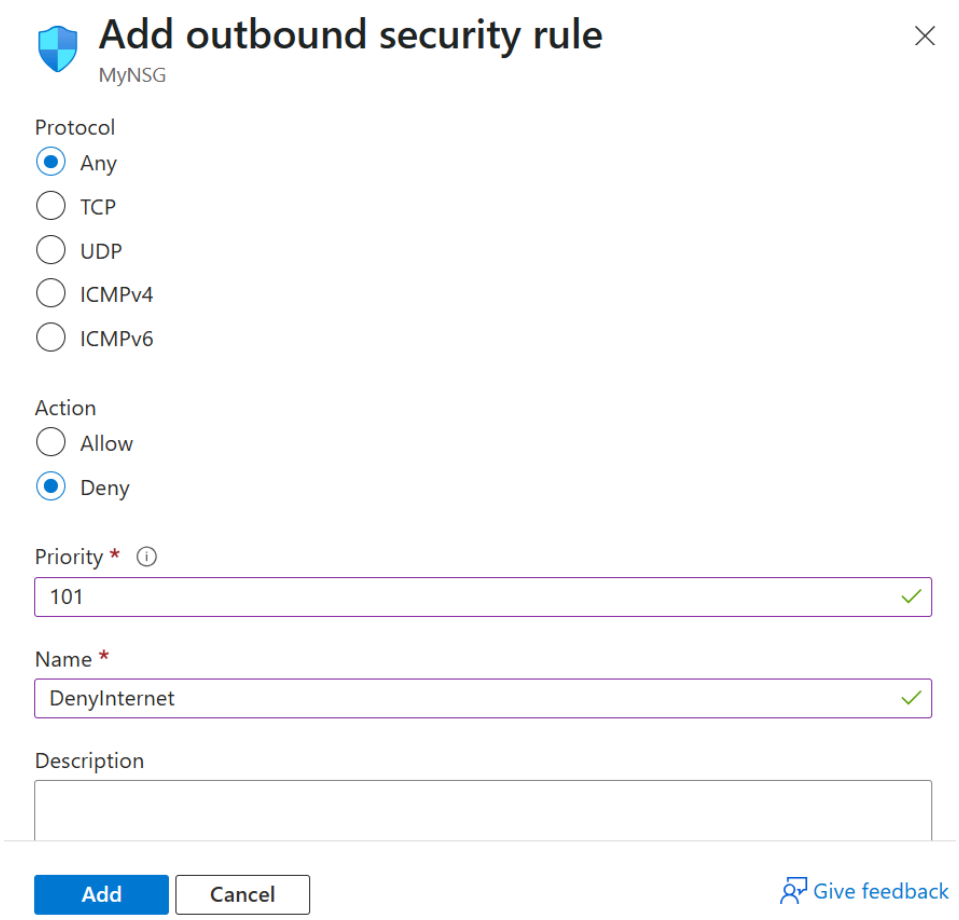




5. Deny Internet Access via NSG (Outbound Rule)

- Go to `MyNSG` > Outbound security rules
- Click + Add
  - Destination: **Service Tag**
  - Tag: `Internet`
  - Protocol: **Any**
  - Port Range: `*`
  - Action: **Deny**
  - Priority: `101`
  - Name: `DenyInternet`
- Click Add

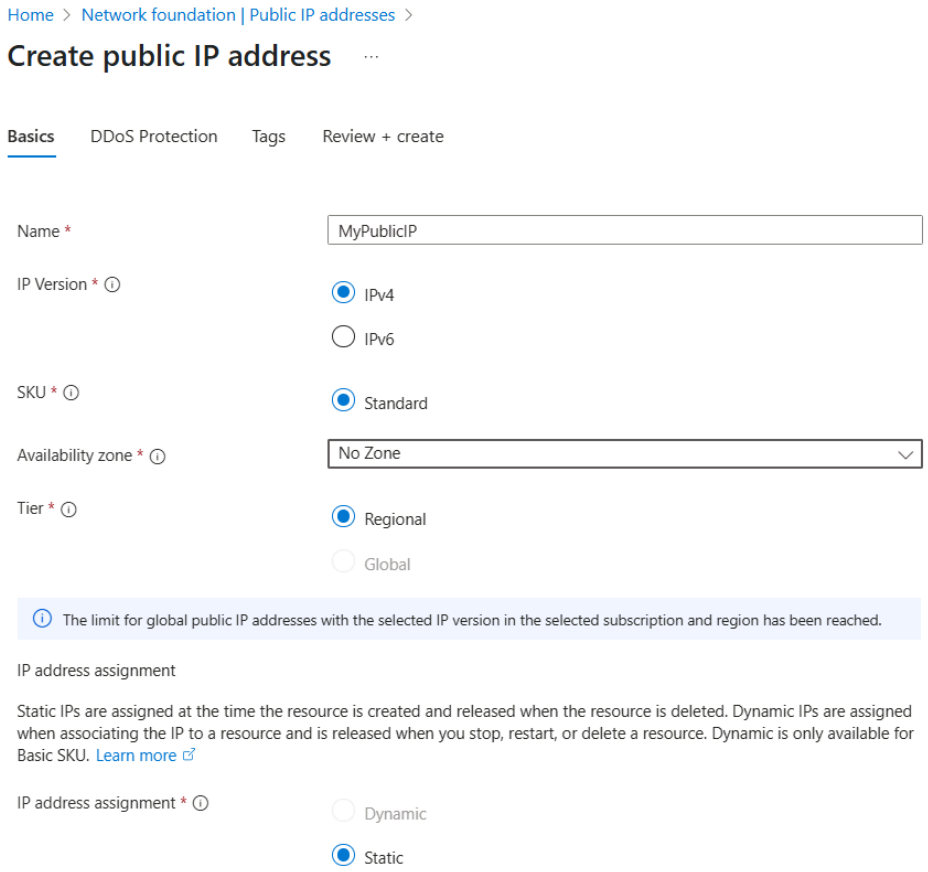




Now your VM cannot reach the internet, but can still be accessed from your IP.

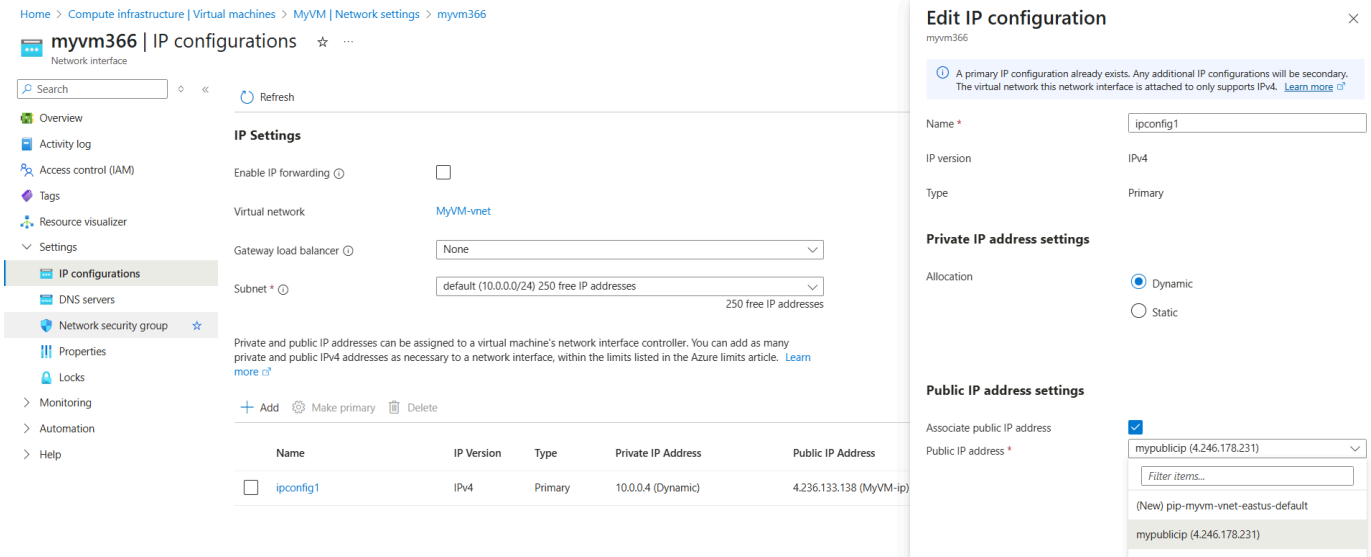
6. Create a Static Public IP

- Search Public IP Addresses > Create
- Fill:
  - Name: `MyPublicIP`
  - SKU: **Standard**
  - Assignment: **Static**
- Click Review + Create > Create



7. Associate Public IP to the VM's NIC

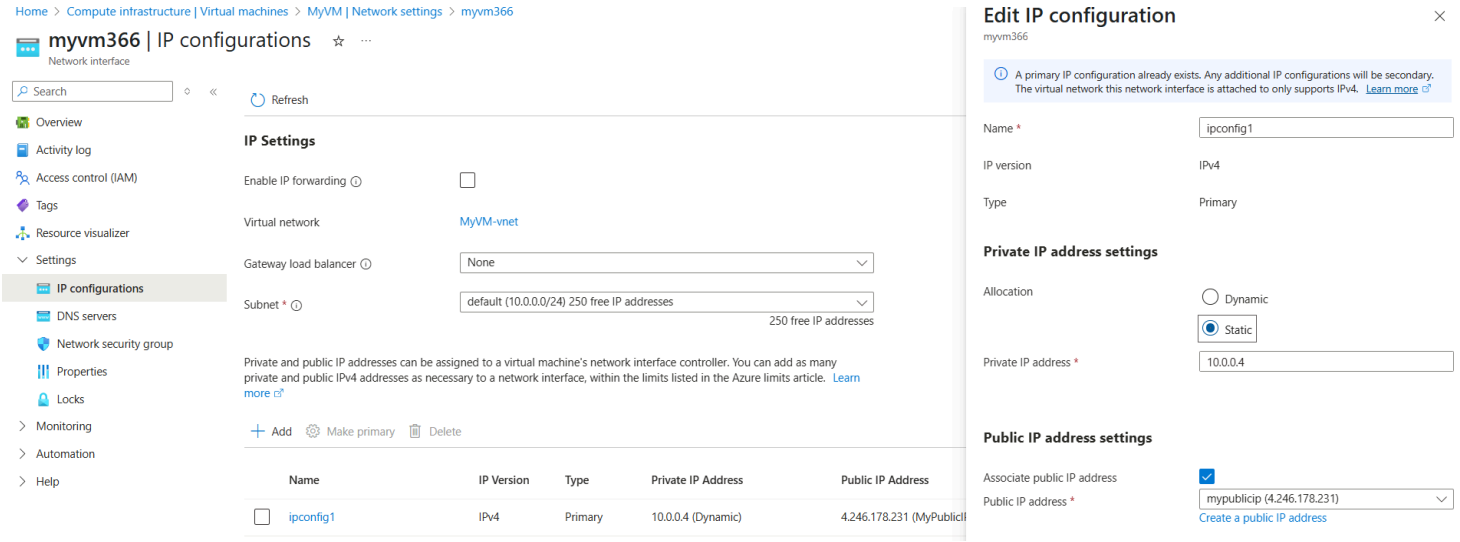
- Go to Virtual Machine > Networking > NIC
- Click IP Configurations > Select the config (usually `ipconfig1`)
- Click Associate public IP > Choose `MyPublicIP`



Your VM now has a static public IP, but only accessible from the IP you allowed earlier.

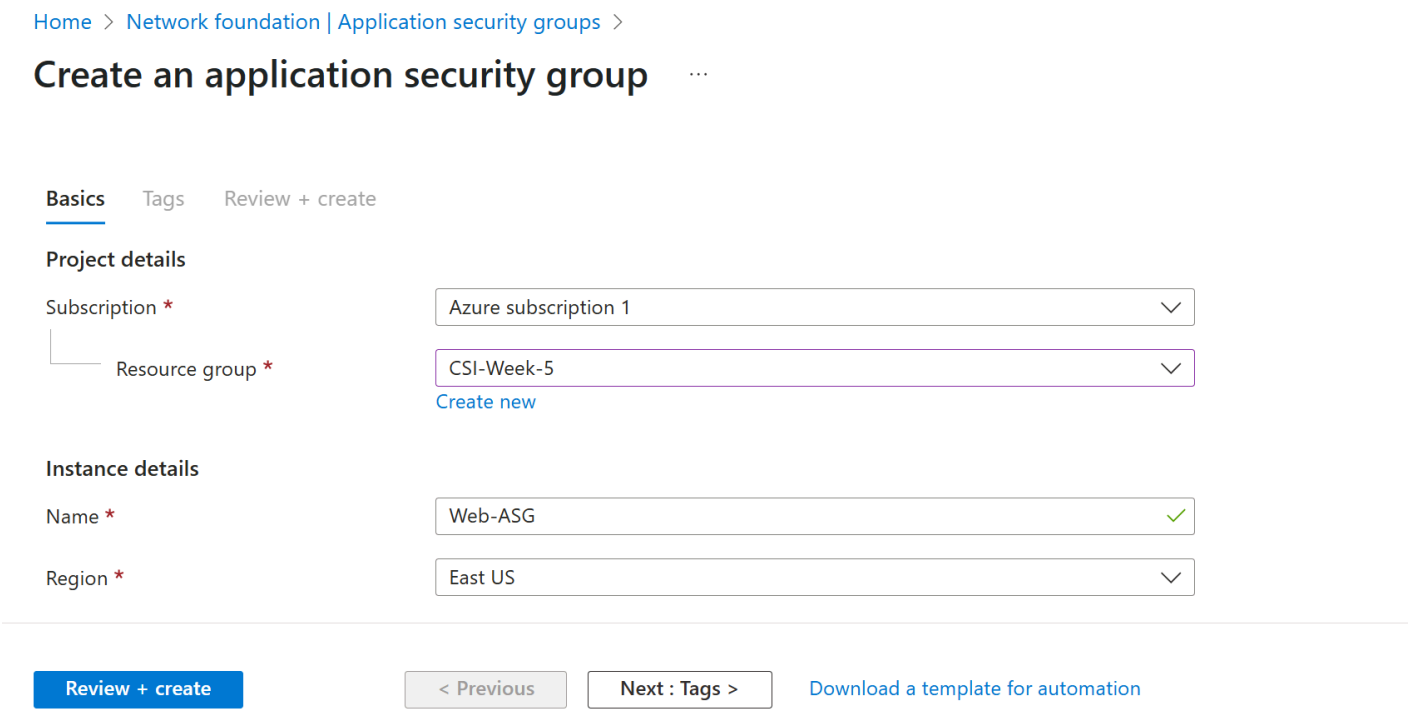
8. Create a Static Private IP for the VM

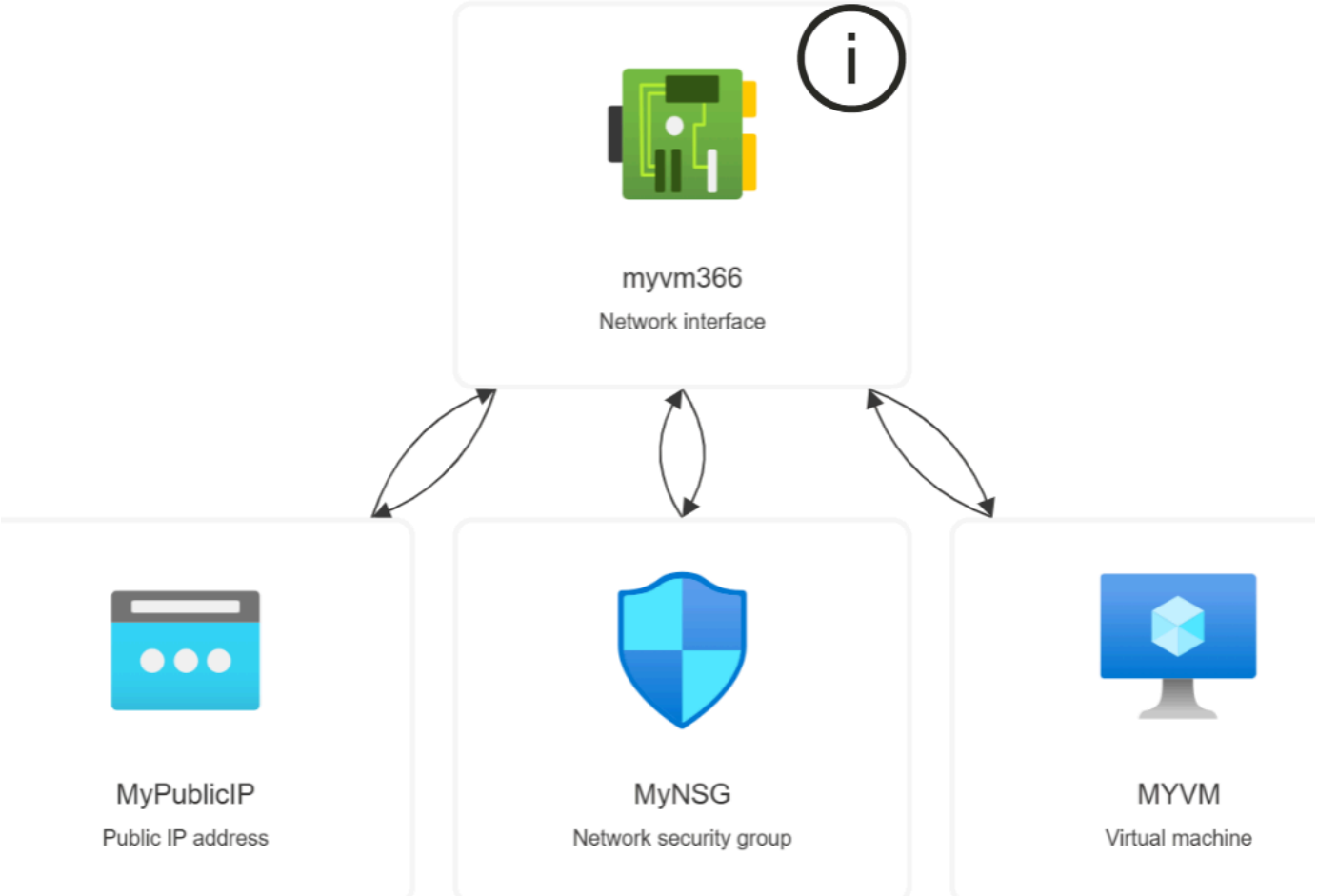
- Go to Virtual Machine > Networking > NIC
- Click IP Configurations > `ipconfig1`
- Change Private IP assignment from Dynamic to Static
- Retain the current IP or set a custom one in the subnet range
- Click Save



9. Create an Application Security Group (ASG)

- Search Application Security Groups > Create
- Fill in:
  - Name: `Web-ASG` (for example)
  - Resource Group: same as VM
  - Region: same as VM
- Click Create






```
C:\Users\ayush\Downloads> ssh -i MyVM_key.pem azureuser@4.246.178.231
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1017-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Jul  6 10:12:31 UTC 2025

  System load:  0.0               Processes:             110
  Usage of /:   5.5% of 28.02GB   Users logged in:       0
  Memory usage: 26%               IPv4 address for eth0: 10.0.0.4
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Sun Jul  6 10:12:32 2025 from 49.36.238.14
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@MyVM:~$ |
```