**ASSIGNMENT 5**

* **Overview**

This document explains essential Azure networking components such as **NSG (Network Security Group)**, **ASG (Application Security Group)**, **Public IPs**, **Service Tags**, and other key configurations like creating a **Network Interface**, assigning **Static IPs**, and managing **Public IP associations**. All explanations are kept beginner-friendly and structured with examples where necessary.

**1. Understanding Network Security Groups (NSG) and Application Security Groups (ASG)**

**2.1. Network Security Group (NSG)**

**Definition:** An NSG acts as a virtual firewall for your Azure resources, controlling inbound and outbound network traffic. It contains a set of security rules that allow or deny traffic based on various properties like source/destination IP address, port, and protocol.

**Working Principle:** NSGs operate at Layer 4 (Transport Layer) of the OSI model. When network traffic flows to or from a resource associated with an NSG, all rules within that NSG are evaluated in order of priority. The first rule that matches the traffic flow is applied.

**Components of an NSG Rule:**

* Priority: A number between 100 and 4096 (lower numbers have higher priority).
* Source/Destination: IP address (individual, CIDR block), Service Tag, or Application Security Group.
* Source/Destination Port Ranges: Specific ports (e.g., 80, 443), ranges (e.g., 22-25), or \* for all ports.
* Protocol: TCP, UDP, ICMP, ESP, AH, or \* for all protocols.
* Direction: Inbound or Outbound.
* Action: Allow or Deny.

**Association Levels:** NSGs can be associated with:

* Network Interfaces (NICs): Rules apply to all traffic flowing through that specific NIC.
* Subnets: Rules apply to all resources within that subnet.

**Default Security Rules:** Azure pre-populates every NSG with a set of default rules. These rules cannot be deleted but have the lowest priority, allowing user-defined rules to override them.

* Inbound: Deny all inbound, Allow VNet inbound, Allow Azure Load Balancer inbound.
* Outbound: Allow VNet outbound, Allow Internet outbound, Deny all outbound.

**2.2. Application Security Group (ASG)**

**Definition:** An ASG allows you to group VMs logically based on their application workload, rather than by explicit IP addresses. This simplifies security rule management, especially in large-scale deployments.

**Working Principle:** Instead of specifying individual IP addresses in NSG rules, you can refer to an ASG. When a VM's network interface is associated with an ASG, it effectively inherits the security rules defined for that ASG.

**Benefits:**

* Simplified rule management: No need to update NSG rules when VMs are added or removed from an application tier.
* Improved readability: NSG rules become more intuitive (e.g., "Allow Web traffic to Web-ASG").
* Scalability: Easily add new VMs to an application tier without reconfiguring NSGs.

**3. Allowing Specific IPs and Denying Internet Access using NSG**

This section details how to configure an NSG to restrict access to VMs to specific IP addresses while blocking general internet access.

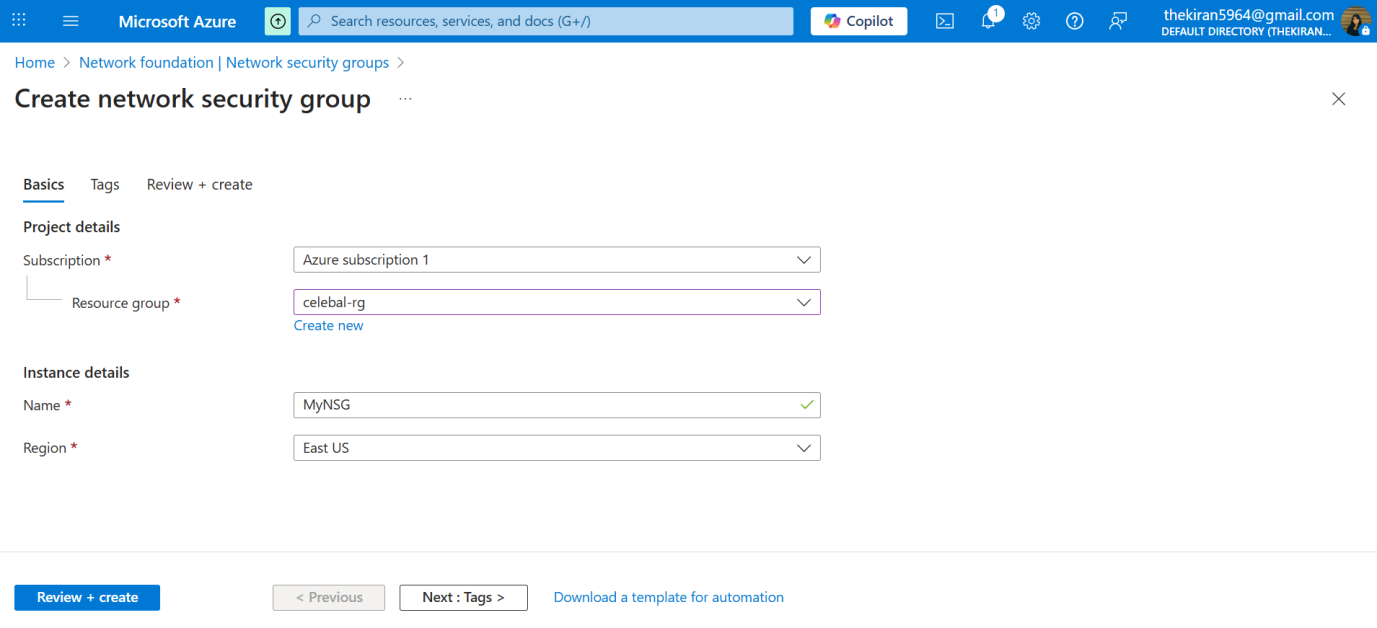
**3.1. Scenario: Allow Specific Management IPs, Deny Internet for VMs**

**Objective:** Allow SSH (port 22) or RDP (port 3389) access from a specific set of administrative IP addresses to VMs, while preventing outbound internet access from the VMs (e.g., for backend servers).

**Steps:**

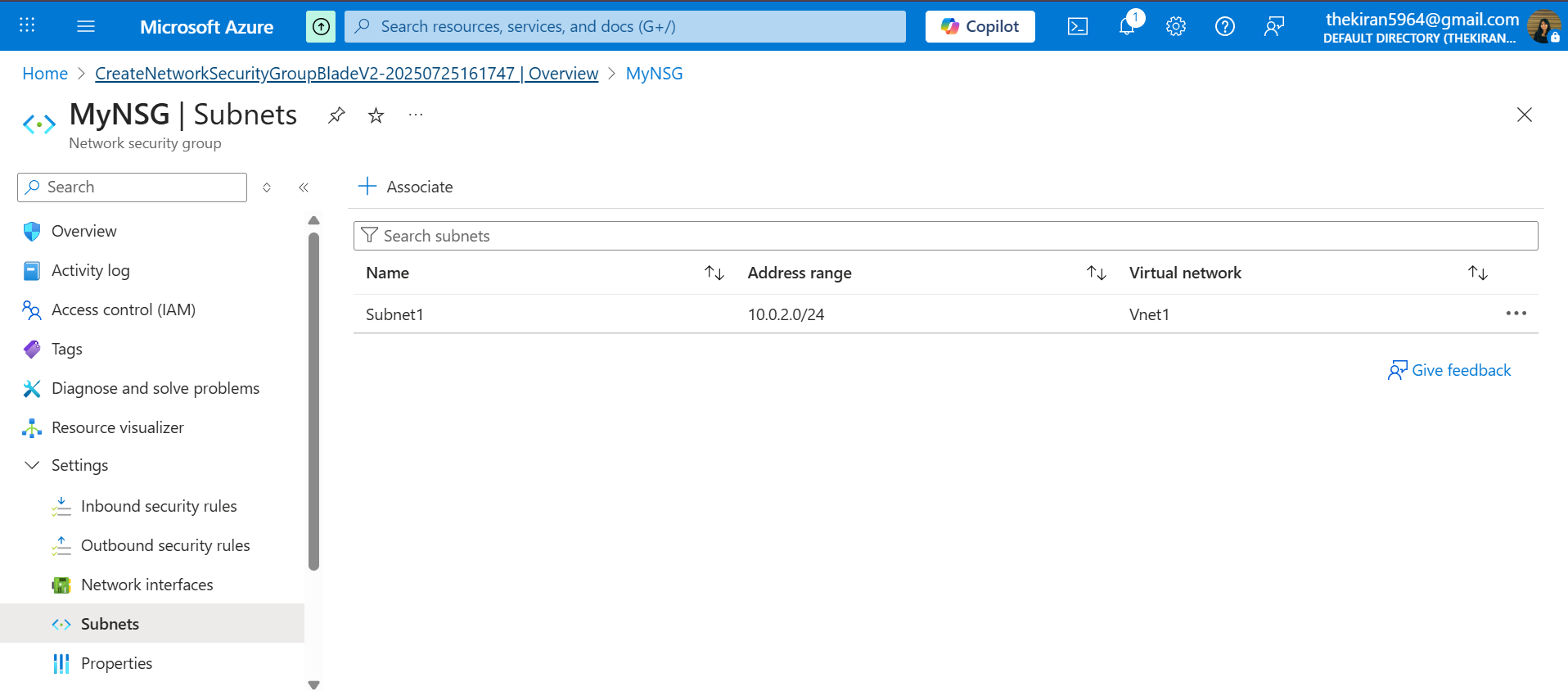
**Create an NSG:**

* Go to Azure Portal -> Network Security Groups -> Create.
* Provide a Name, Resource Group, and Region.



**Associate NSG (to Subnet or NIC):**

* For subnet association: Go to Virtual Networks -> your VNet -> Subnets -> your Subnet -> Network security group -> Select your NSG.
* For NIC association: Go to Virtual Machines -> your VM -> Networking -> Network Interface -> Network security group -> Select your NSG.



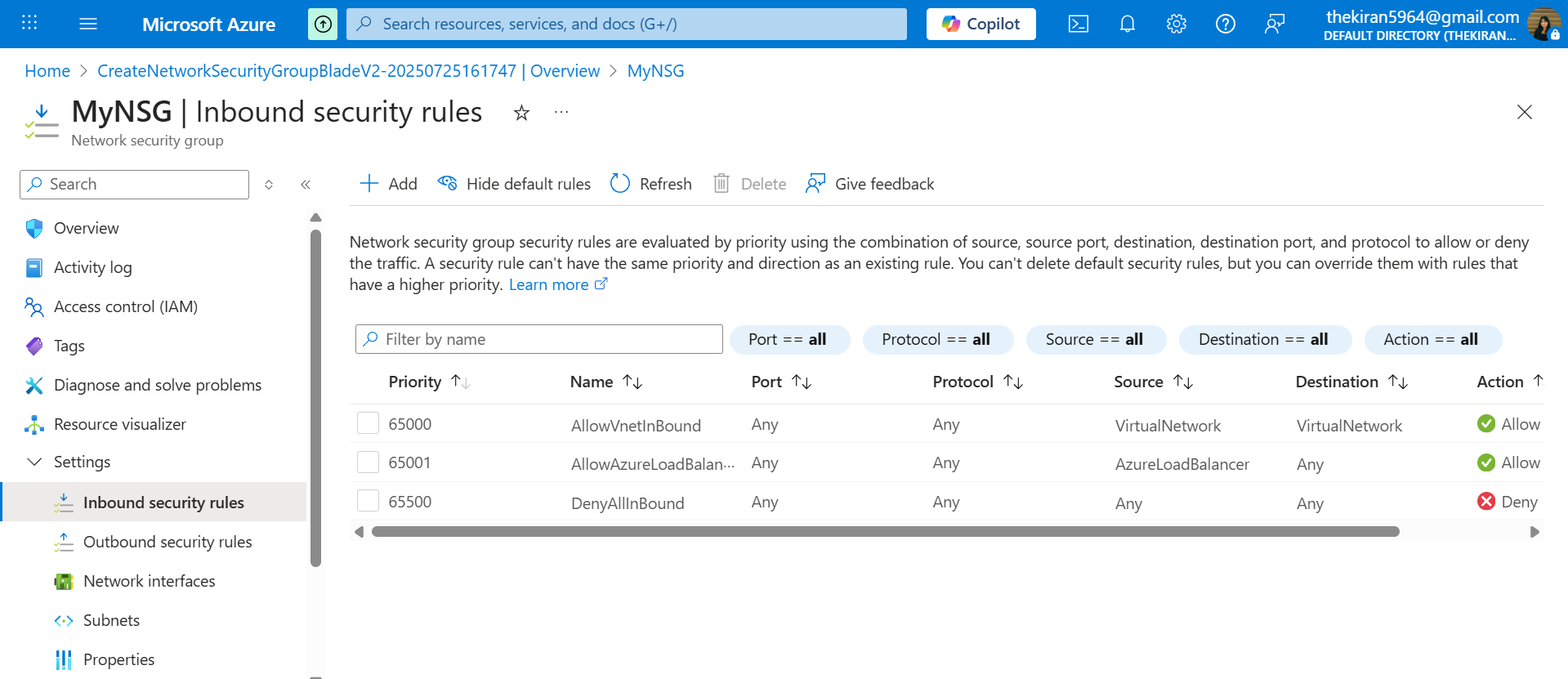
**Configure Inbound Security Rules (Allow Specific IPs):**

**Rule 1: Allow Management Access (e.g., SSH/RDP)**

* Priority: 100 (or lower than any Deny rule)
* Source: IP Addresses (your administrative IP range, e.g., 203.0.113.0/24)
* Source port ranges: \*
* Destination: Any
* Destination port ranges: 22 (for SSH) or 3389 (for RDP)
* Protocol: TCP
* Action: Allow
* Direction: Inbound
* Name: Allow-Admin-Access

**Rule 2: Deny All Other Inbound Traffic (if not already covered by default rules)**

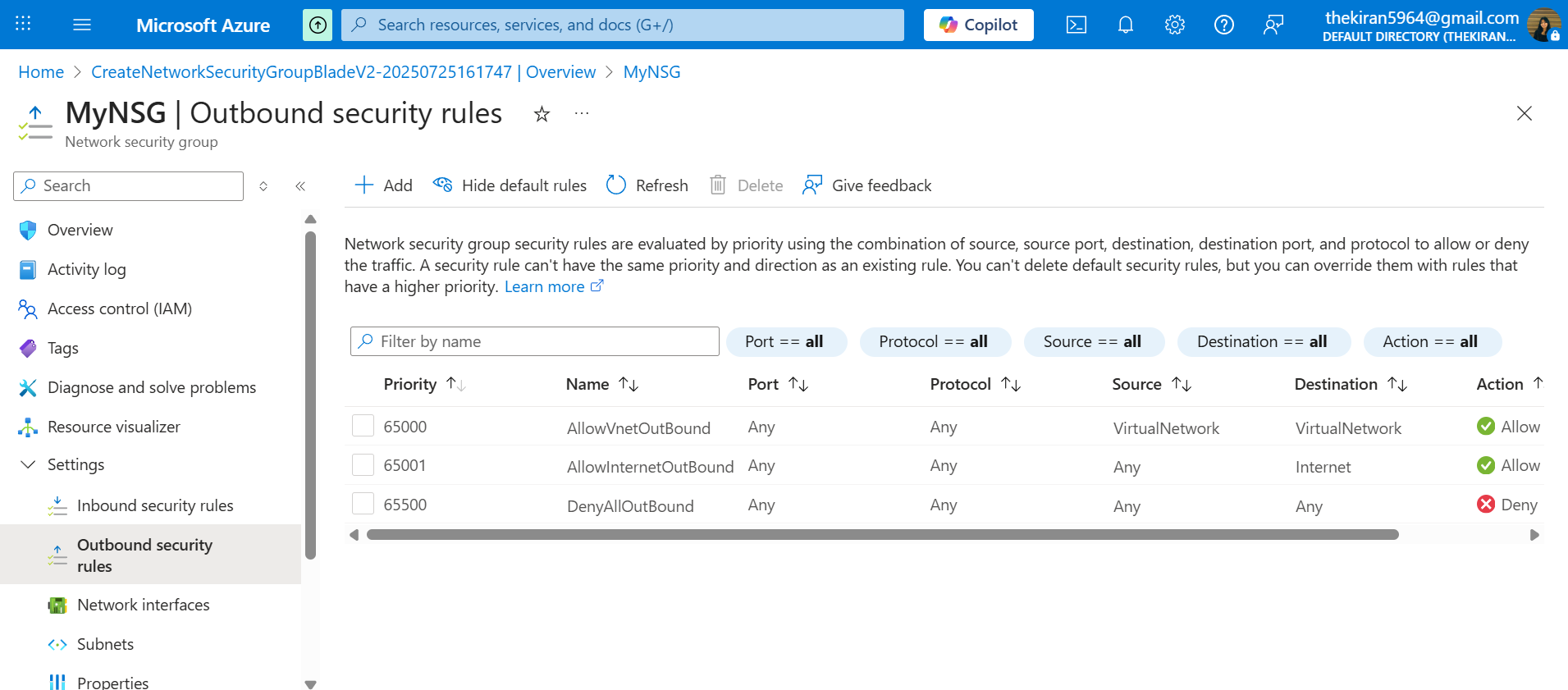
* Priority: 200 (higher than default Deny, lower than your Allow rule)
* Source: Any
* Source port ranges: \*
* Destination: Any
* Destination port ranges: \*
* Protocol: Any
* Action: Deny
* Direction: Inbound
* Name: Deny-All-Inbound-Except-Admin



**Configure Outbound Security Rules (Deny Internet):**

**Rule 1: Deny Outbound Internet Access**

* Priority: 100 (or lower than any other Allow outbound rule)
* Source: Any
* Source port ranges: \*
* Destination: Internet (Service Tag)
* Destination port ranges: \*
* Protocol: Any
* Action: Deny
* Direction: Outbound
* Name: Deny-Outbound-Internet



**Note:** Default NSG rules have AllowVNetOutBound and AllowInternetOutBound with priorities 65000 and 65001 respectively. By creating a Deny-Outbound-Internet rule with a lower priority (e.g., 100), you override the default AllowInternetOutBound rule. Ensure that AllowVNetOutBound (default priority 65000) remains effective if VMs need to communicate within the VNet.

**4. Public IPs and Types**

**4.1. Definition: Public IP Address**

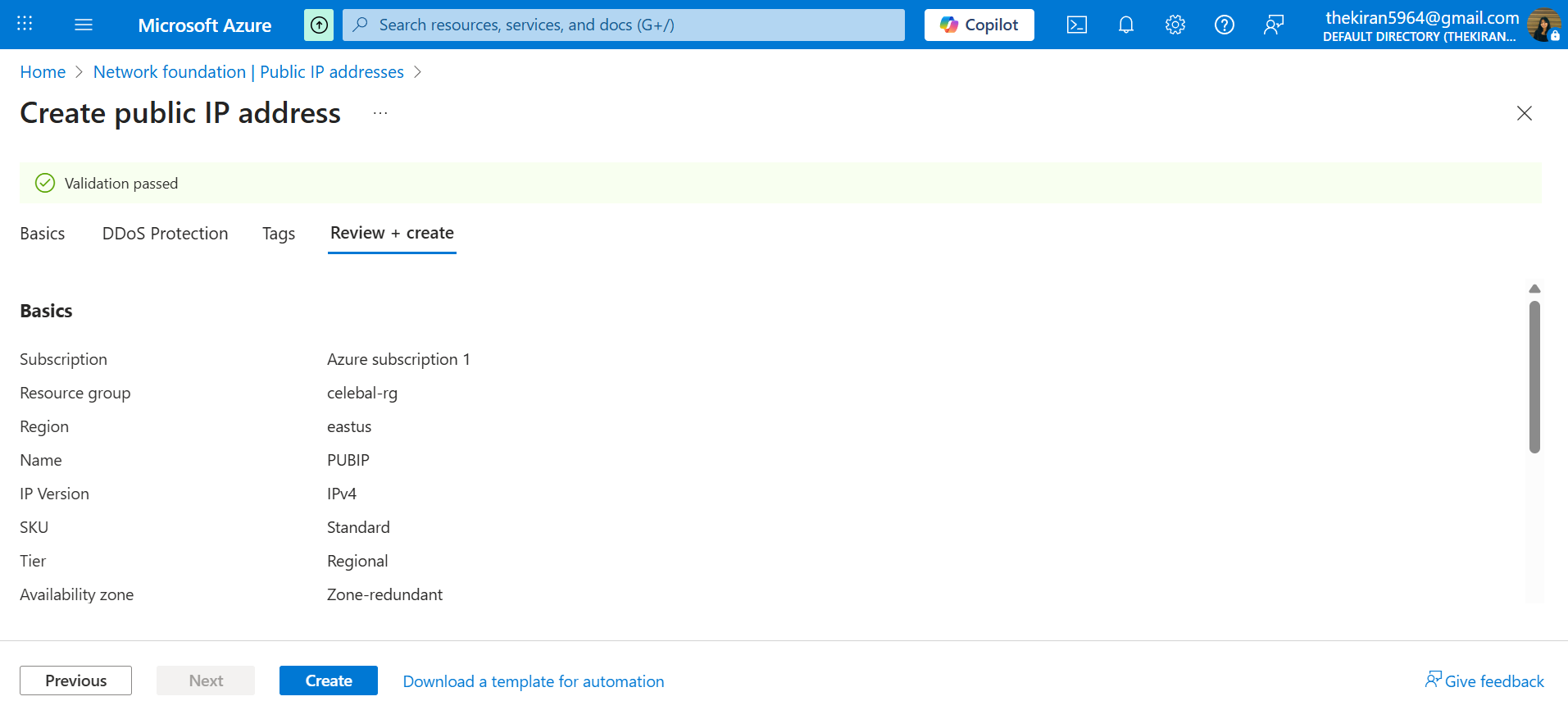
A Public IP address in Azure enables internet-facing communication for Azure resources. It allows resources like VMs, Load Balancers, and Application Gateways to be accessible from the internet.

**4.2. Public IP SKUs: Basic:**

* **Allocation Method:** Dynamic by default, but can be Static.
* **Features:** Basic functionality, no zone redundancy.
* **Use Cases:** Non-critical applications, dev/test environments.

**Standard:**

* **Allocation Method:** Always Static.
* **Features:** Zone-redundant (if deployed in a region with Availability Zones), secure by default (closed to inbound traffic unless explicitly allowed by NSG), supports inbound SNAT, outbound rules.
* **Use Cases:** Production workloads, high-availability scenarios, services requiring zone redundancy.



**4.3. Public IP Allocation Methods:**

**Dynamic:**

* The IP address is assigned from a pool of available addresses and can change if the associated resource is stopped and deallocated.
* Cost-effective for resources that don't require a persistent public IP.

**Static:**

* The IP address is assigned permanently to the resource and remains the same even if the resource is stopped and deallocated.
* Essential for services that require a consistent public IP, such as DNS records, VPN gateways, or public-facing web servers.

**5. Service Tags**

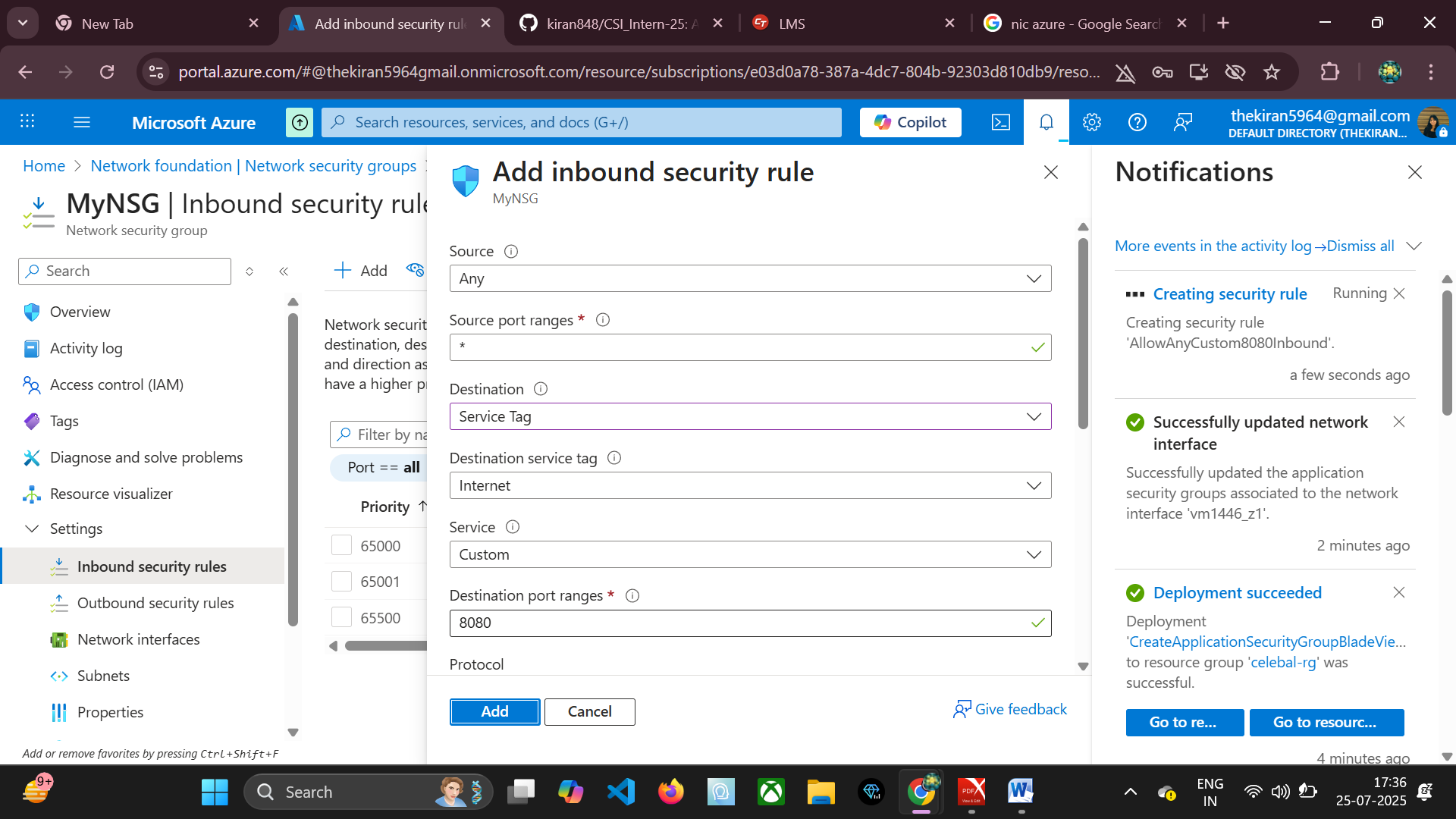
**Definition:** Service Tags represent a group of IP address prefixes for a given Azure service or a set of IP ranges within a specific region. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change.

**Benefits:**

* Simplifies NSG rule creation: Instead of specifying individual CIDR blocks, you can use a service tag (e.g., VirtualNetwork, AzureLoadBalancer, Internet, Storage, Sql).
* Reduced management overhead: Azure automatically updates the IP ranges associated with service tags, so you don't need to manually keep track of changes.

**Common Service Tags:**

* VirtualNetwork: Represents the address space of the virtual network.
* AzureLoadBalancer: Represents Azure's infrastructure load balancer.
* Internet: Represents the public IP address space.
* Storage: Represents Azure Storage public IP addresses.
* Sql: Represents Azure SQL Database public IP addresses.



**6. Allocate Static IPs to all VMs**

While you can allocate a Public Static IP to a VM's NIC, it's more common and recommended to use Private Static IPs for VMs within a VNet, unless the VM explicitly needs to be directly accessible from the internet via its own public IP.

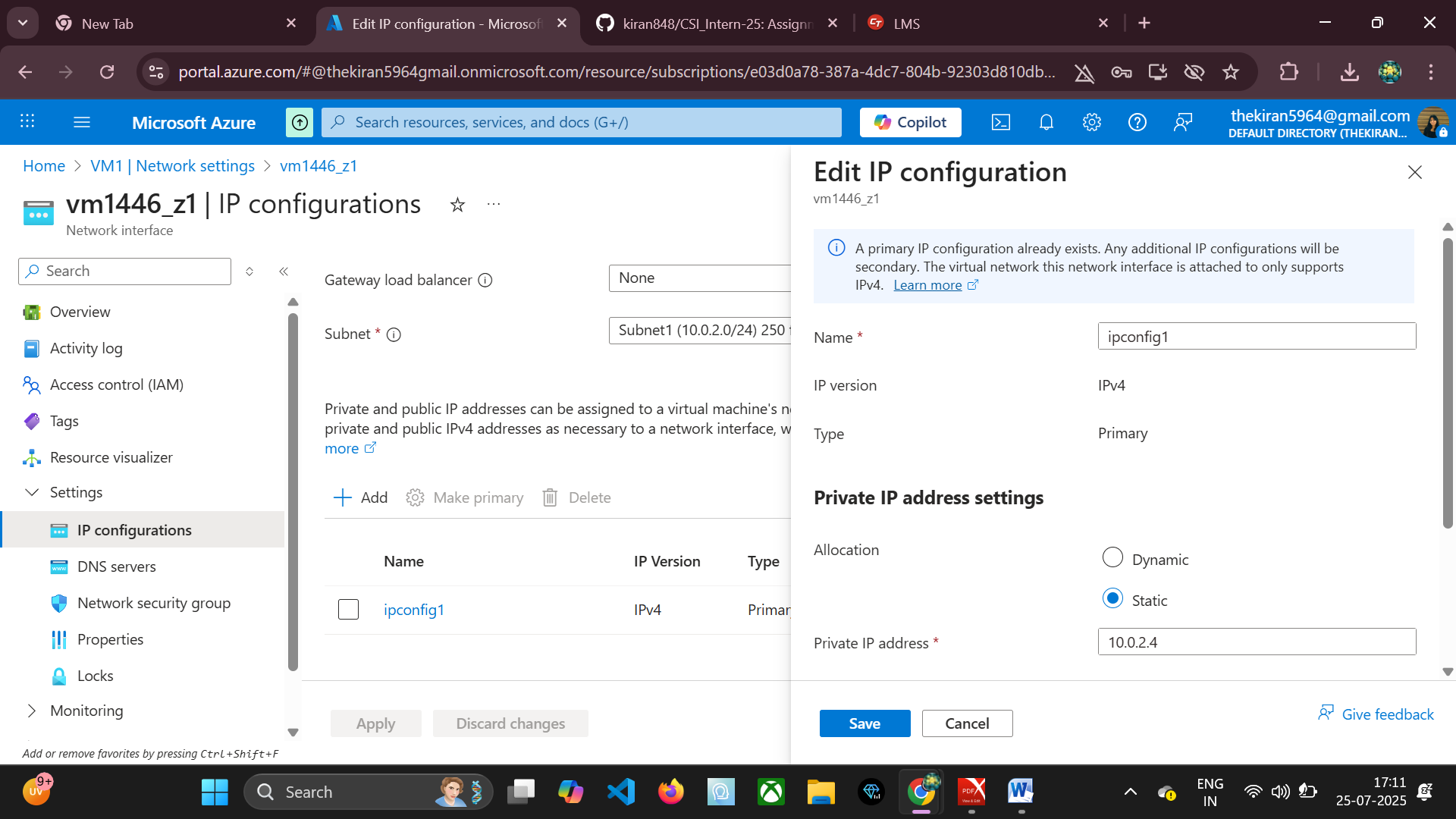
**6.1. Allocating a Private Static IP to a VM**

**Purpose:** Ensures the VM always retains the same private IP address within its subnet, which is crucial for applications that rely on fixed internal IP addresses (e.g., domain controllers, database servers, internal DNS).

**Steps:**

* Go to Azure Portal -> Virtual Machines -> your VM -> Networking -> Network Interface.
* Click on "IP configurations".
* Click on the existing IP configuration (e.g., ipconfig1).
* Under "Private IP address settings", select Static for the "Allocation" method.
* Enter a specific IP address within the subnet's address range. Ensure it's not already in use.
* Click "Save".

**Note:** If the VM is running, it may require a reboot or network refresh for the change to take full effect.

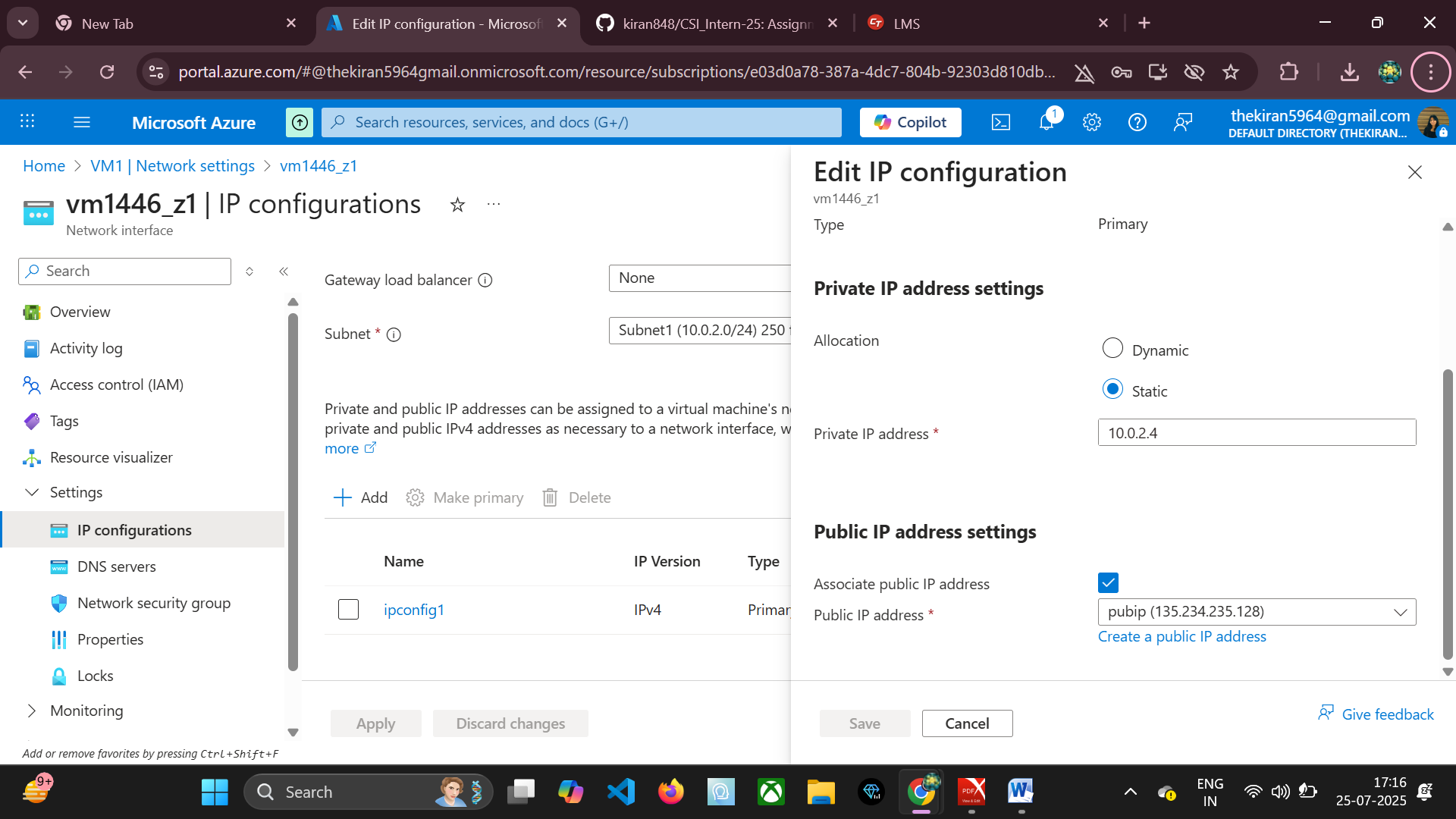


**6.2. Allocating a Public Static IP to a VM**

**Purpose:** For VMs that require direct and persistent internet accessibility (e.g., a public web server).

**Steps (assuming Public IP already created - see Section 8):**

* Go to Azure Portal -> Virtual Machines -> your VM -> Networking -> Network Interface.
* Click on "IP configurations".
* Click on the existing IP configuration.
* Under "Public IP address", select "Associate".
* Choose an existing Static Public IP address from the dropdown or create a new one (select Standard SKU for Static).
* Click "Save".



### ****7. Creating an Application Security Group (ASG)****

This section provides a step-by-step guide to creating an **Application Security Group (ASG)** in the Azure Portal.

**Steps:**

**Sign in to Azure Portal:**  
Go to <https://portal.azure.com>

**Search for "Application Security Groups":**  
In the search bar at the top, type **"Application Security Groups"** and select it from the results.

**Click "Create":**  
On the Application Security Groups blade, click the **"+ Create"** button.

**Basics Tab:**

* **Subscription:** Select your Azure subscription.
* **Resource group:** Choose an existing resource group or create a new one.
* **Name:** Enter a unique name for your ASG (e.g., web-asg).
* **Region:** Select the Azure region where your ASG will be deployed.

⚠️ **Note:** The ASG and the virtual machines that will use it must be in the **same region**.

**Review + create Tab:**

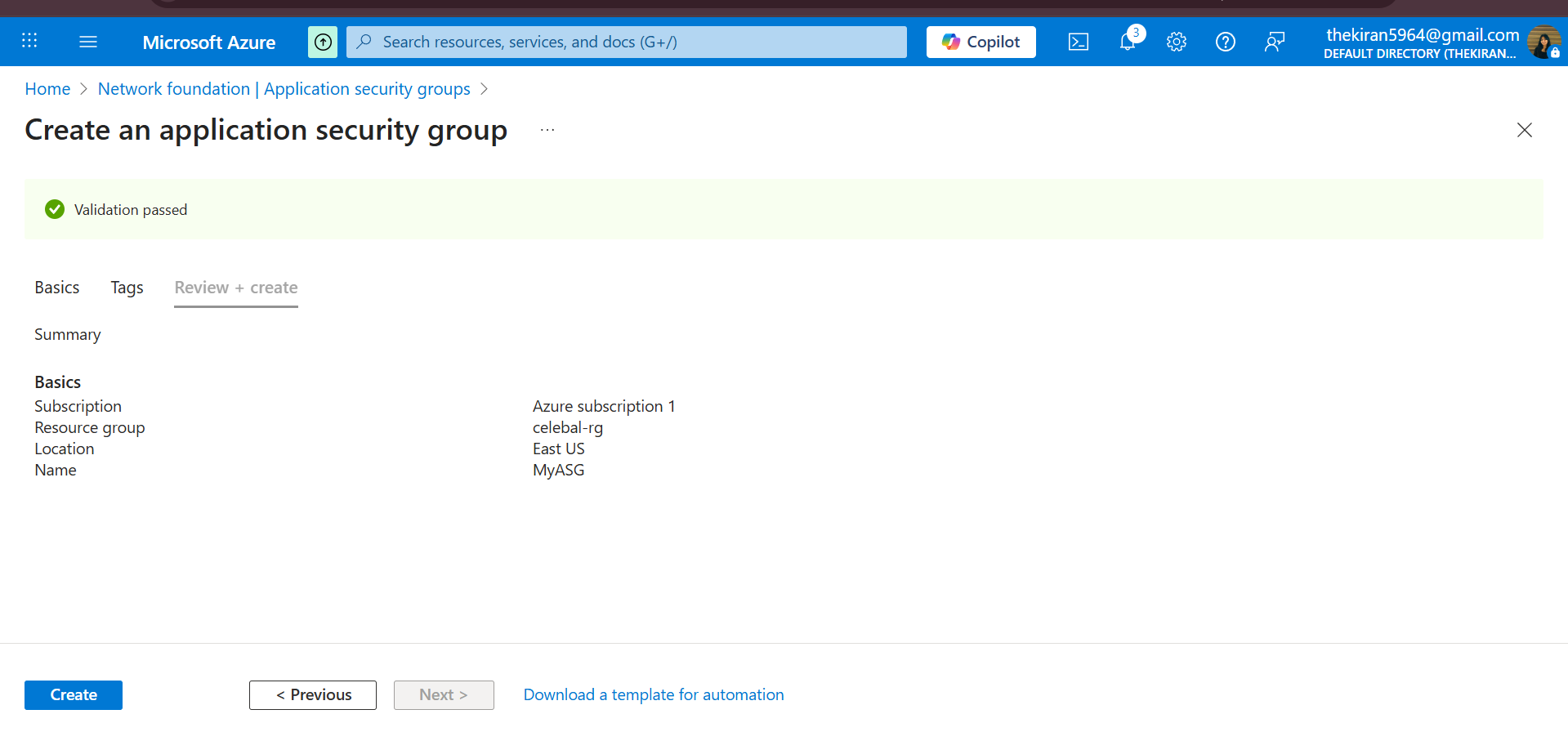
* **Review your settings.**
* **Click "Create":** Once validation passes, click **"Create"**.

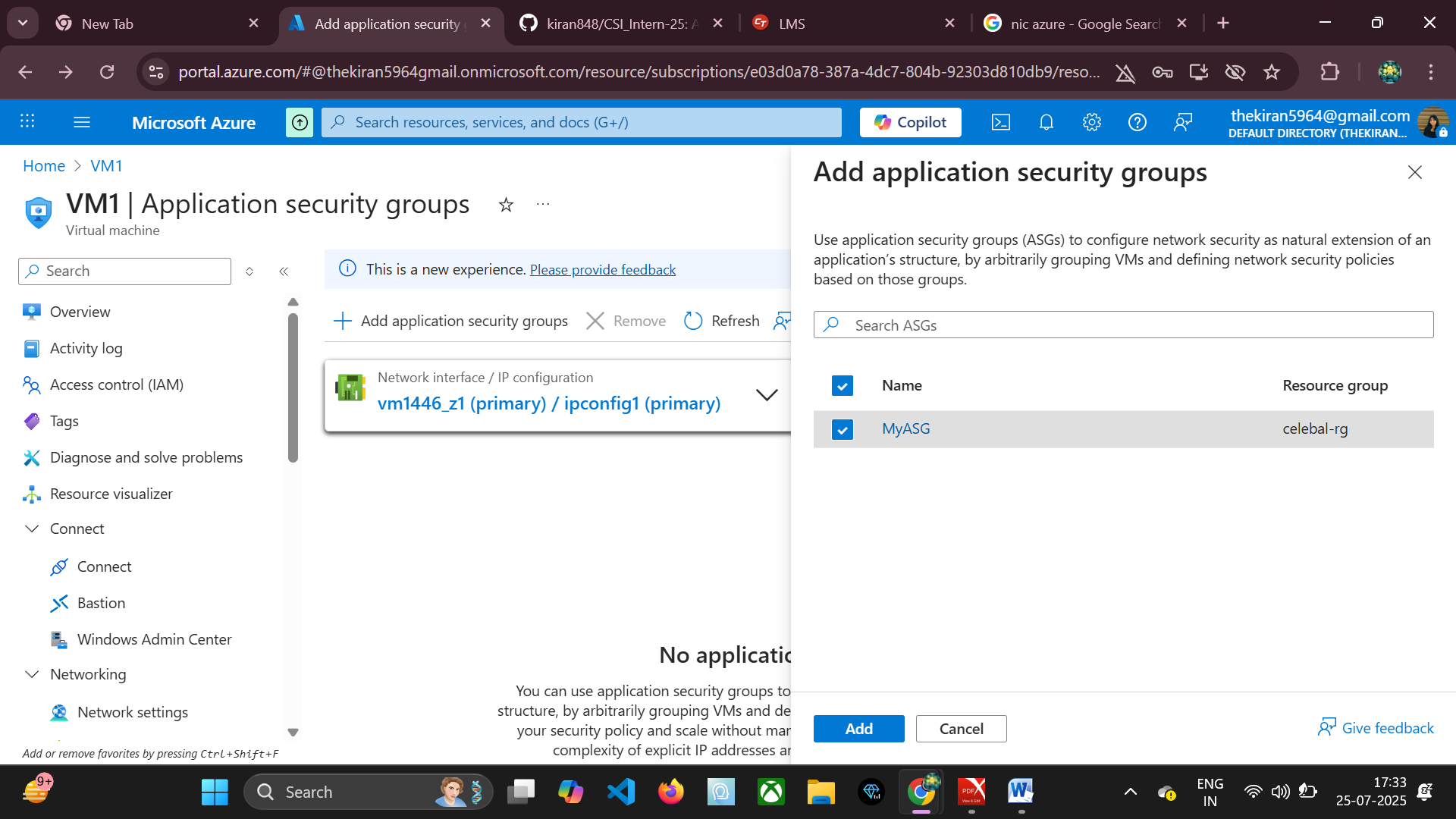
**Deployment:**  
Azure will deploy the ASG. You will receive a notification when the deployment is complete.

**Associate ASG with a VM:**  
After creation, associate the ASG with a VM’s Network Interface:

* Go to **Virtual Machines** → your VM → **Networking**.
* Click on the **Network Interface**.
* Under **Application Security Groups**, click **+ Associate**.
* Select your newly created ASG.
* Click **Save**.

Once associated, this ASG can be used in **NSG rules** as a **source or destination** to allow or deny traffic between groups of VMs logically.





**8. Creating Public IP**

This section provides a step-by-step guide to creating a Public IP address in the Azure Portal.

**Steps:**

**Sign in to Azure Portal:** Go to portal.azure.com.

**Search for "Public IP addresses":** In the search bar, type "Public IP addresses" and select it.

**Click "Create":** On the Public IP addresses blade, click the "+ Create" button.

**Basics Tab:**

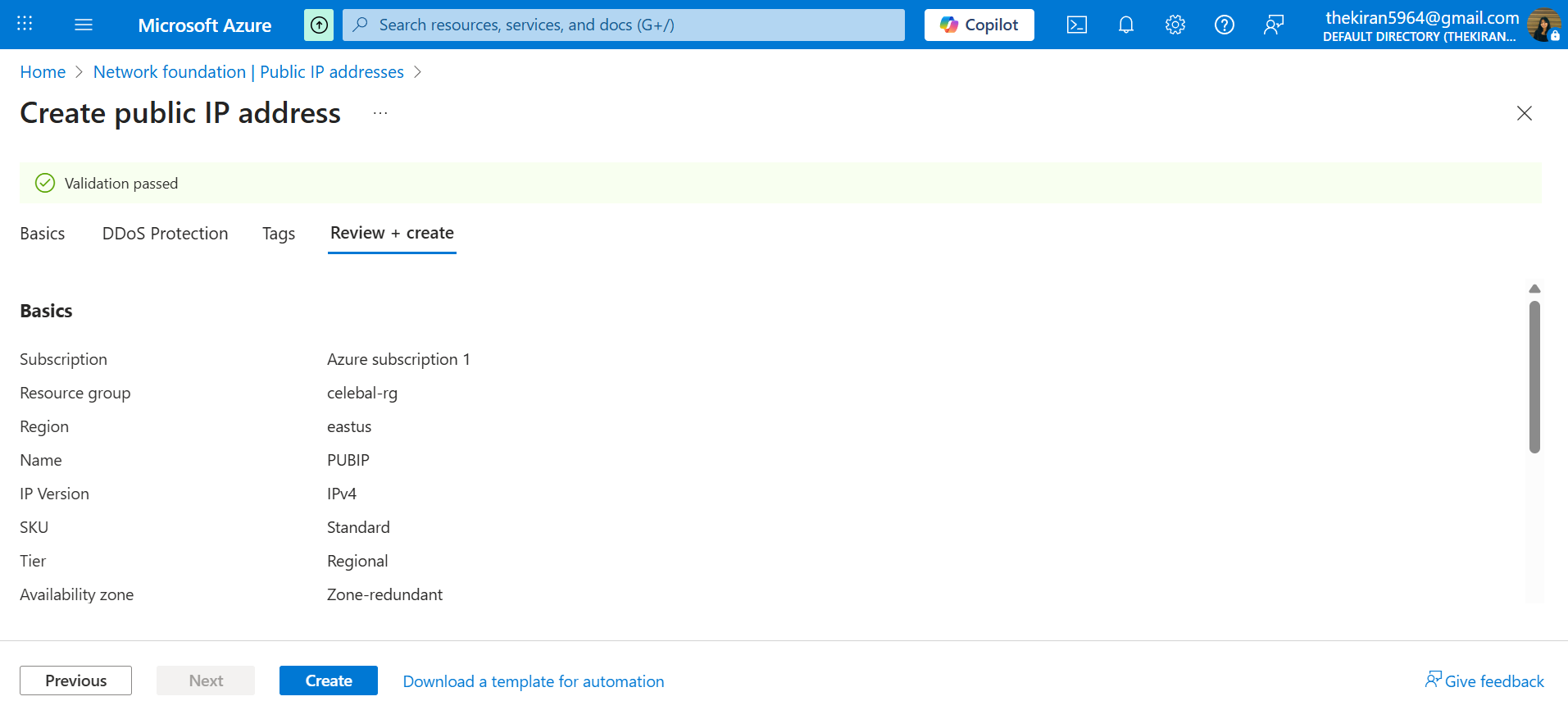
* **Subscription:** Select your Azure subscription.
* **Resource group:** Choose an existing resource group or create a new one.
* **Region:** Select the Azure region.
* **Name:** Enter a unique name for your Public IP (e.g., my-vm-public-ip).
* **IP version:** IPv4 (most common) or IPv6.
* **SKU:** Choose Standard (recommended for production, always static) or Basic (can be static or dynamic).
* **Tier:** Regional (default) or Global (for cross-region load balancing).
* **Allocation:** Static (recommended for consistent IP) or Dynamic (only available for Basic SKU).
* **Availability zone:** (Only for Standard SKU) Choose Zone-redundant, Zoned (select a specific zone), or No zone.
* **DNS name label (optional):** Enter a unique DNS name label (e.g., myvmweb). This will create a FQDN like myvmweb.region.cloudapp.azure.com.

**Tags Tab (optional):** Add tags for categorization.

**Review + create Tab:** Review your settings.

**Click "Create":** Once validation passes, click "Create".

**Deployment:** Azure will deploy the Public IP.



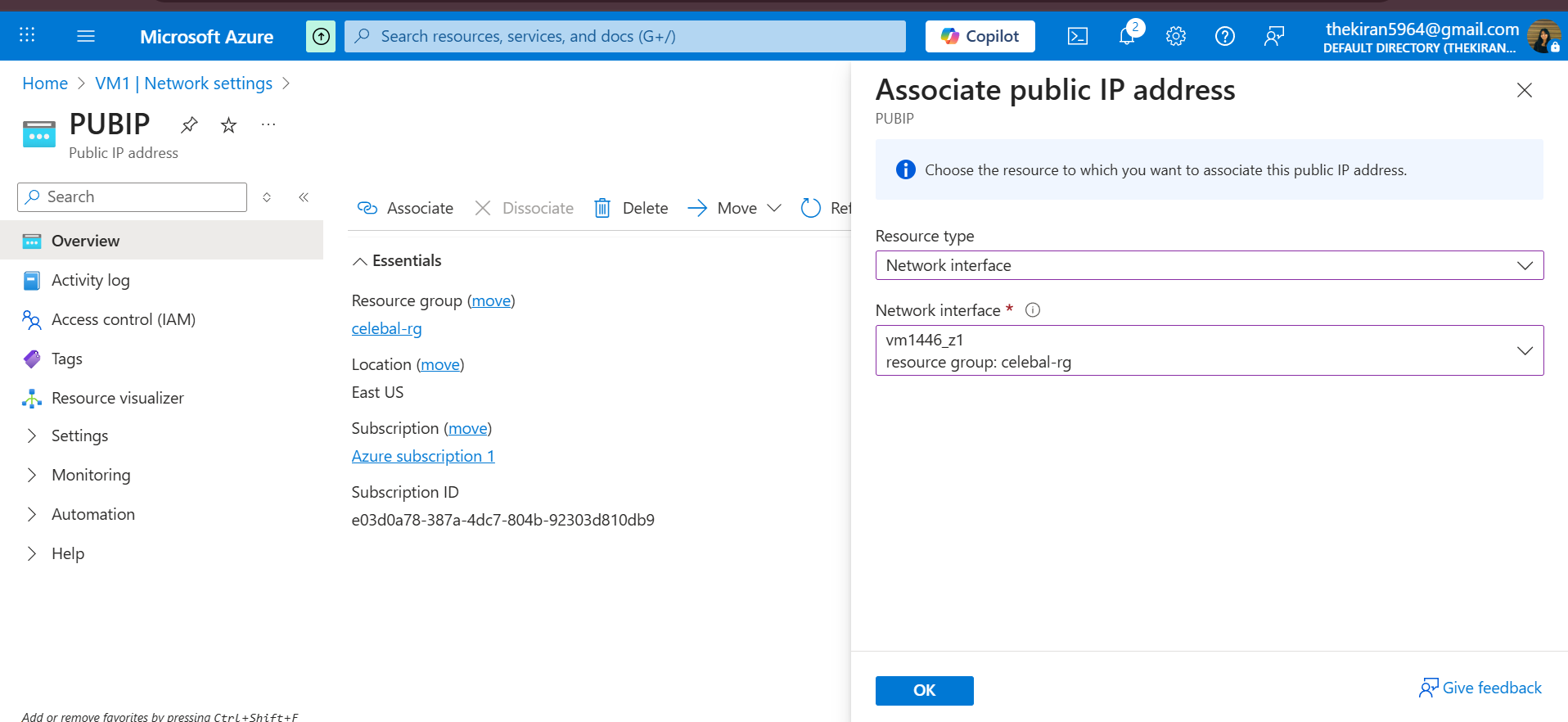
**9. Associating/De-associating Public IP with Virtual Machine**

**9.1. Associating Public IP with a VM**

**Prerequisites:** A Public IP address and a Virtual Machine with a Network Interface.

**Steps:**

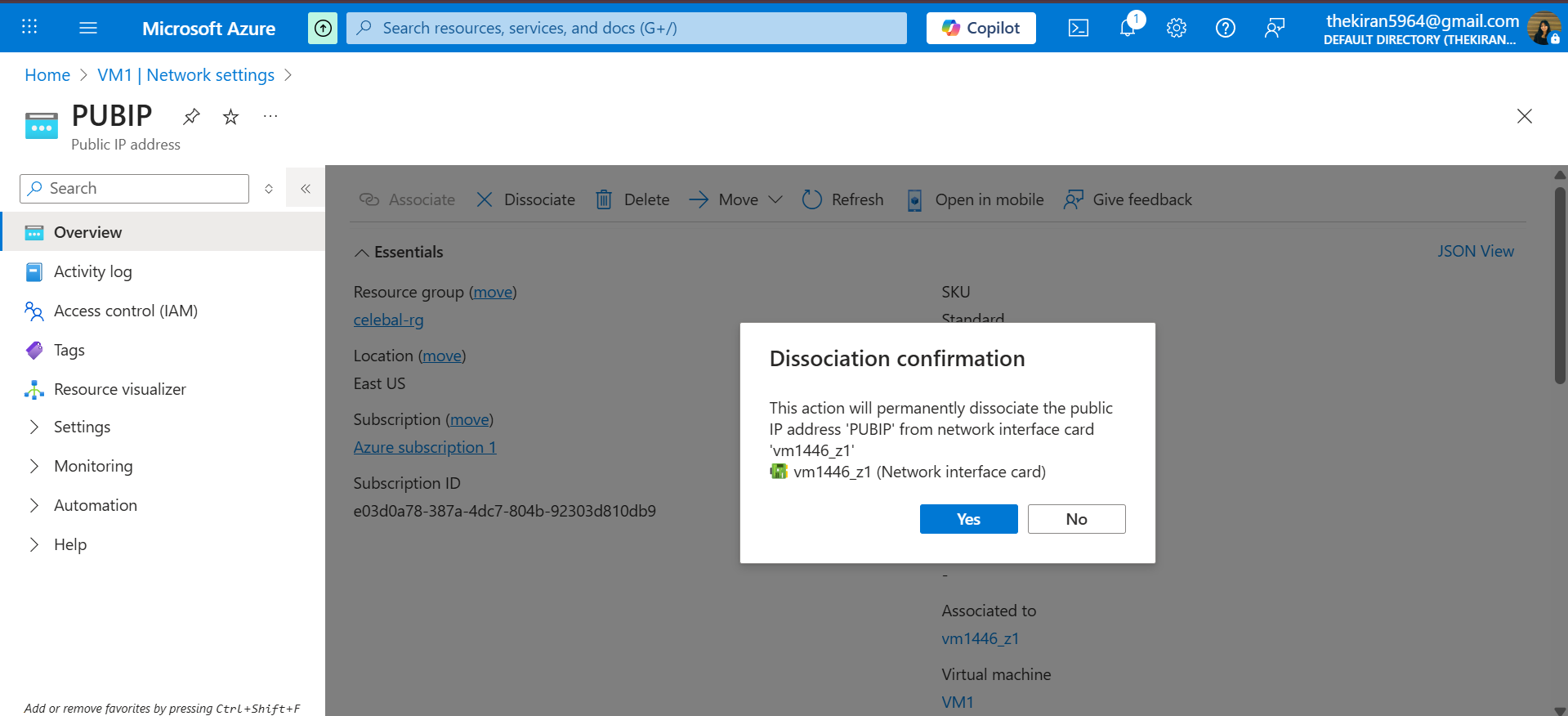
* Go to Azure Portal -> Virtual Machines -> your VM.
* In the left-hand menu, select "Networking".
* Click on the "Network Interface" for your VM.
* In the left-hand menu of the Network Interface blade, select "IP configurations".
* Click on the IP configuration you want to associate the Public IP with (usually ipconfig1).
* Under "Public IP address", click "Associate".
* From the dropdown list, select the Public IP address you want to associate.
* Click "Save".



**9.2. De-associating Public IP from a VM**

**Steps:**

* Go to Azure Portal -> Virtual Machines -> your VM.
* In the left-hand menu, select "Networking".
* Click on the "Network Interface" for your VM.
* In the left-hand menu of the Network Interface blade, select "IP configurations".
* Click on the IP configuration that has the associated Public IP.
* Under "Public IP address", click "Disassociate".
* Confirm the de-association.
* Click "Save".



**Note:** The Public IP address will still exist after de-association and can be associated with another resource. You must explicitly delete it if it's no longer needed.

**10. Creation of Network Interface (NIC)**

Network Interfaces (NICs) are the fundamental components that enable a VM to connect to a virtual network. Every VM in Azure has at least one NIC.

**10.1. When to create a NIC explicitly?**

Typically, when you create a new VM, a NIC is automatically created and attached to it.

You might explicitly create a NIC if you need to:

* Add a second (or more) NIC to an existing VM (for multi-homing).
* Pre-provision a NIC before VM creation.
* Attach an existing NIC to a different VM (though this is less common and has specific considerations).

**10.2. Steps to Create a Network Interface**

**Sign in to Azure Portal:** Go to portal.azure.com.

**Search for "Network Interfaces":** In the search bar, type "Network Interfaces" and select it.

**Click "Create":** On the Network Interfaces blade, click the "+ Create" button.

**Basics Tab:**

* **Subscription:** Select your Azure subscription.
* **Resource group:** Choose an existing resource group or create a new one.
* **Name:** Enter a unique name for your NIC (e.g., my-vm-nic-02).
* **Region:** Select the Azure region.
* **Virtual network:** Select the VNet to which this NIC will connect.
* **Subnet:** Select the specific subnet within the VNet.
* **Network security group (NSG):** (Optional) You can associate an existing NSG here or leave it blank and associate later.
* **DNS server:** (Optional) Inherit from VNet, or custom.
* **IP forwardling:** Disabled (default) or Enabled.

**IP Configurations Tab:**

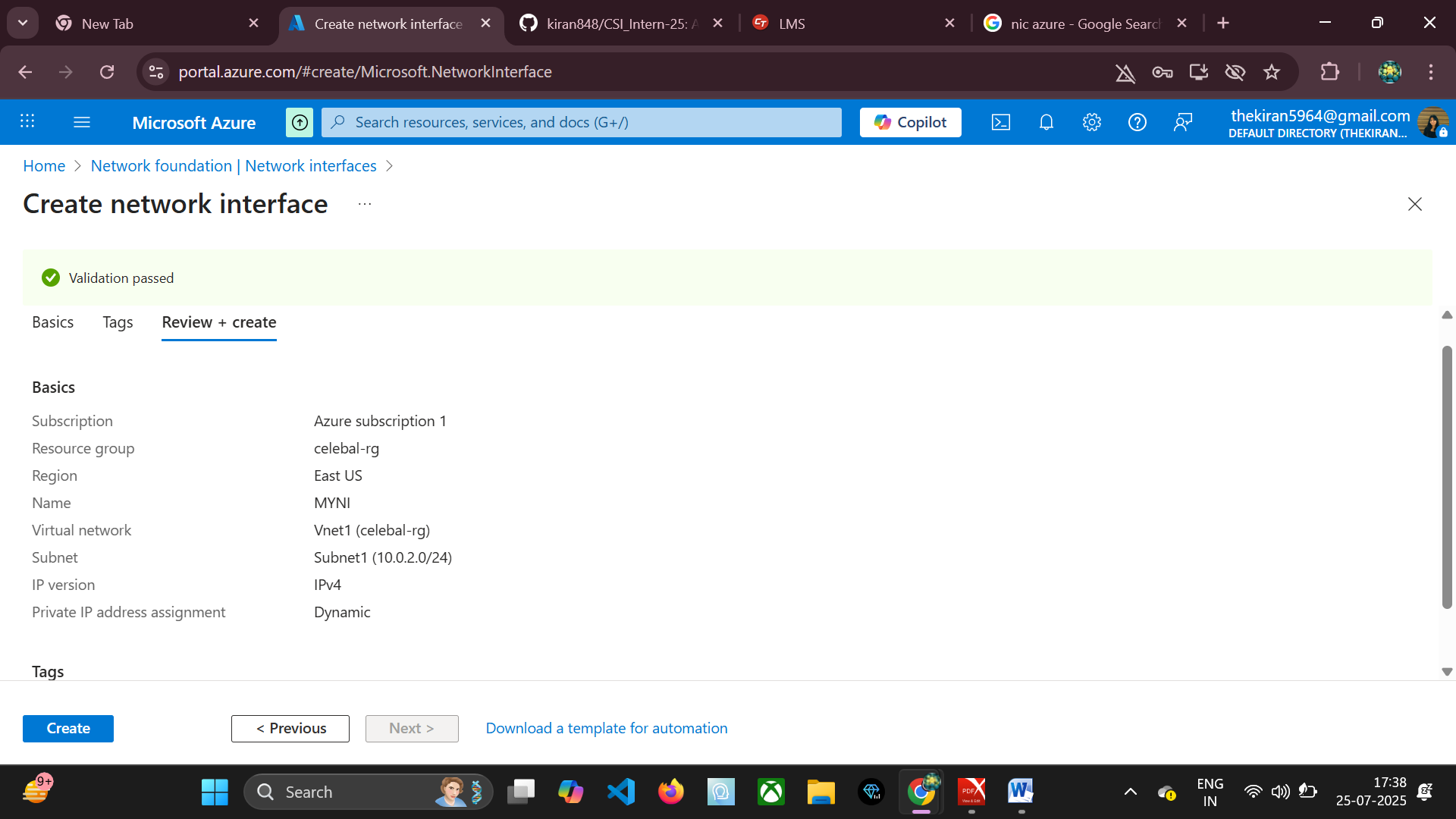
* An initial IP configuration (ipconfig1) is created by default.
* You can configure its Private IP allocation (Dynamic or Static).
* You can also choose to Associate Public IP address at this stage.

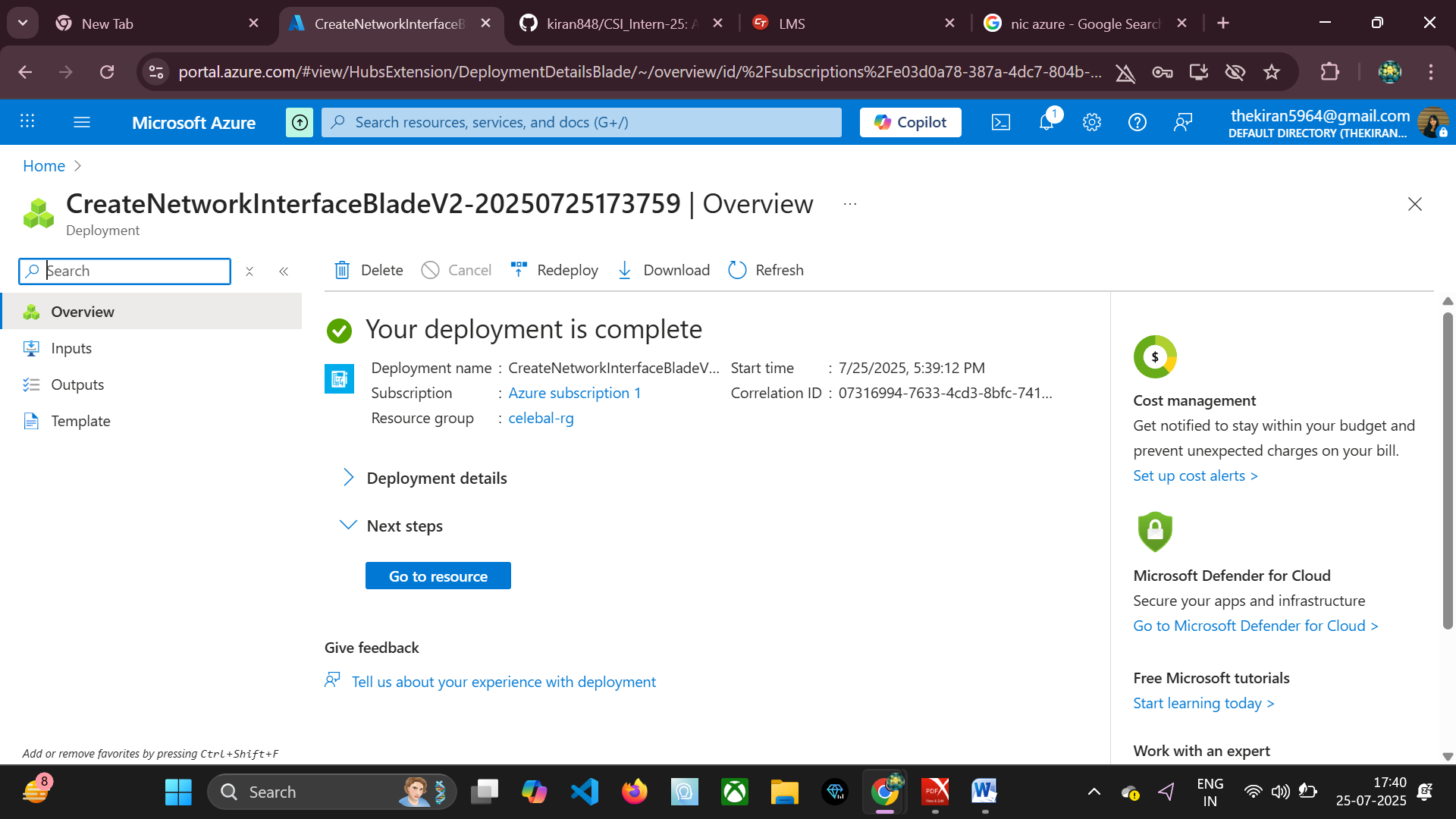
**Management, DNS, Tags Tabs (Optional):** Configure as needed.

**Review + create Tab:** Review your settings.

**Click "Create":** Once validation passes, click "Create".

**Deployment:** Azure will deploy the Network Interface.





**Conclusion**

This document has provided a foundational understanding of Azure's network security and IP management capabilities. By effectively leveraging NSGs, ASGs, and proper IP allocation, organizations can build secure, scalable, and highly available cloud environments. Implementing the practices outlined here is crucial for protecting your Azure resources from unauthorized access and ensuring efficient network communication.