**Question 3. Why is it important to deny inbound traffic from the public internet for certain VMs? Describe how you can configure an NSG to achieve this.**

**Answer:**

Denying inbound traffic from the public internet for the certain virtual machine is important because of the following reasons:

**Security:** VMs are often targeted by malicious actors looking to exploit vulnerabilities, launch attacks, or gain unauthorized access. Denying inbound traffic helps mitigate these risks by reducing the attack surface and preventing unauthorized entry points.

**Data Protection:** Many VMs host sensitive or critical data, such as personal information, financial records, or intellectual property. Restricting inbound traffic ensures that only authorized users or systems can access this data, minimizing the risk of data breaches or leaks.

**Compliance Requirements:** Various regulations and industry standards mandate strict controls over access to sensitive systems and data. Denying inbound traffic helps organizations comply with these requirements by ensuring that access is limited to authorized entities only.

**Resource Optimization:** Allowing unrestricted inbound traffic can strain system resources, such as bandwidth, processing power, and memory. By denying unnecessary traffic, organizations can optimize resource utilization and maintain the performance and availability of their VMs.

**Prevention of Service Disruption:** Malicious or excessive inbound traffic, such as Distributed Denial of Service (DDoS) attacks, can disrupt the normal operation of VMs and associated services. Denying inbound traffic helps prevent such disruptions and ensures the continuity of business operations.

**Protection against Exploits:** Vulnerable VMs can be exploited by attackers to launch further attacks within an organization's network or against external targets. Denying inbound traffic helps contain the impact of potential exploits and limit the spread of malicious activity.

Configuring an NSG to achieve this involves setting up some security rules within the NSG. Which involves the following steps:

* Firstly, create or select an network security group.
* Then add an inbound security rule.
* Configure the rule by specifying source, source port range, destination, destination port range, protocol, action, name etc.

**Example:** There is a VM suppose “webserver”, which host a website that should only be accessible within an organization’s network. We have to configure an NSG to deny all inbound traffic from the public internet to this VM. For this we follow the following:

Step 1: Access Azure Portal

Firstly, Log in to the Azure Portal

Step 2: Navigate to Network Security Groups

Go to the Networking section in the Azure Portal and select Network security groups.

Step 3: Create or Select an NSG

Click on Add to create a new NSG.

Step 4: Configure Inbound Security Rule

In the selected NSG, go to the Inbound security rules section and click on add to create a new rule.

Step 5: Define the Rule Parameters

Source: Set the source to your organization's IP address range or specific IP addresses that should have access to the VM. For this example, let's assume organization's IP range is 10.0.0.0/24.

Source port ranges: Set to \* to apply the rule to all source ports.

Destination: Set to \* to apply the rule to all destinations.

Destination port ranges: Set to \* to apply the rule to all destination ports.

Protocol: Choose the appropriate protocol. If you want to restrict access to HTTP traffic, select TCP and specify port 80.

Action: Set the action to Deny to block the traffic.

Priority: Assign priority to the rule. For simplicity, let's set it to 100.

Name: Enter a descriptive name for the rule, such as "DenyPublicInboundHTTP."

Step 6: Save the Rule:

Click on Save to save the rule.

Step 7: Associate NSG with VM:

Go to the Network interfaces section within the NSG settings.

Click on Associate and select the network interface associated with the "WebServer" VM.