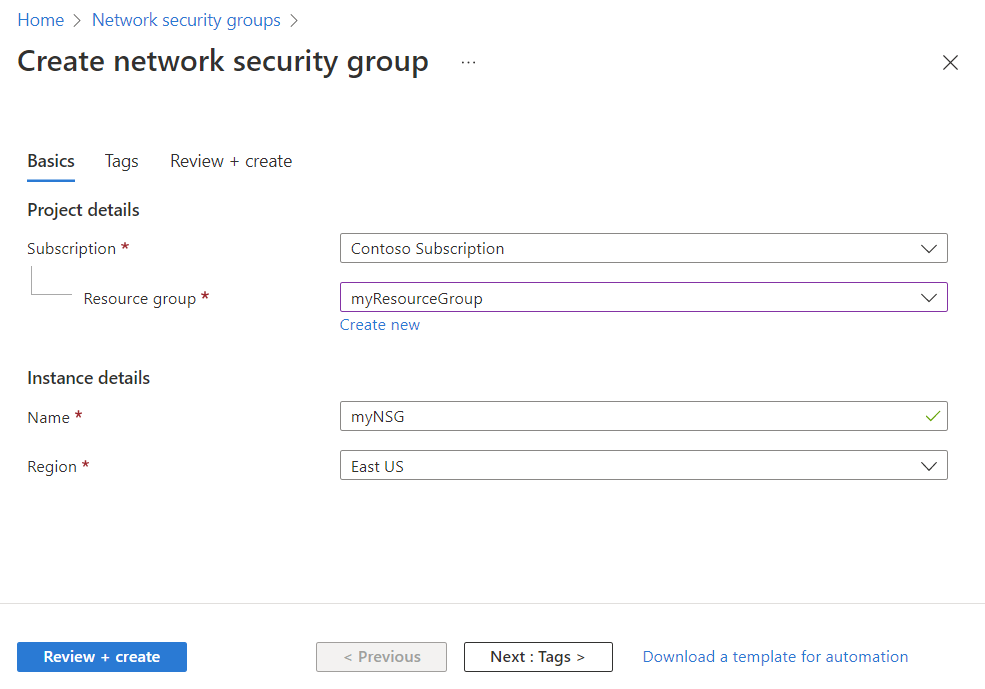
1. Create an NSG:

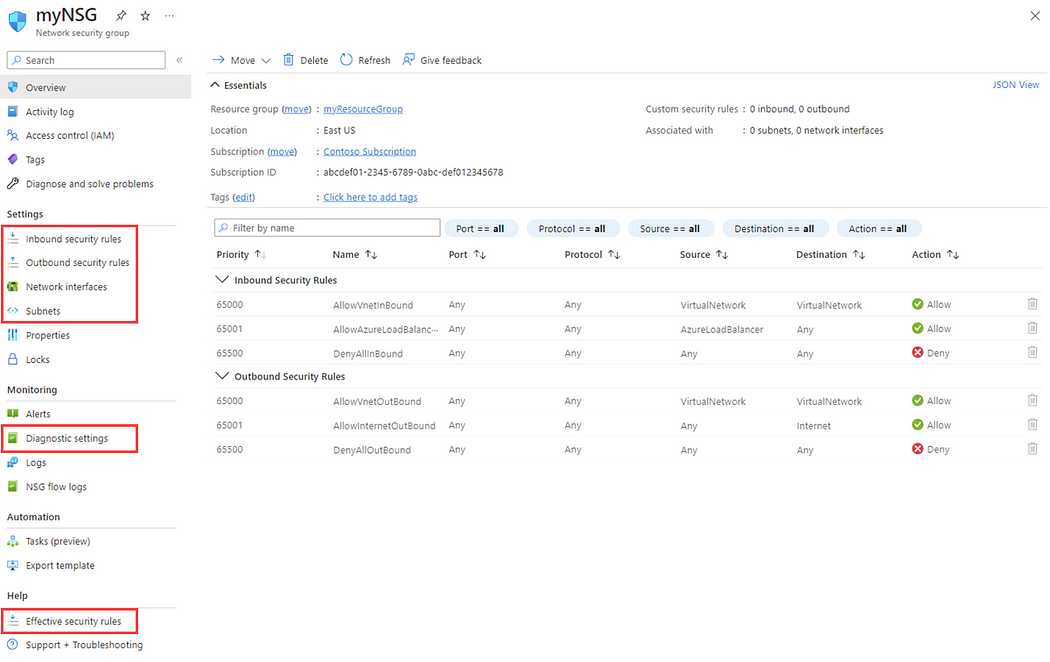
* In the Azure portal, navigate to ‘Network security groups’ and click ‘Add’.
* Provide a name and associate it with a resource group.



Creating an NSG

2. Define Inbound/Outbound Security Rules:

* Under the created NSG, go to the ‘Inbound security rules’ and ‘Outbound security rules’ tabs.
* Add rules to allow or deny traffic based on parameters like source/destination IP address, port, and protocol.



Defining Inbound/Outbound Security Rules

**Example:**

Let’s consider a scenario where we want to allow only HTTP (port 80) and SSH (port 22) traffic to a VM:

* Inbound Rules:

Rule Name: Allow\_HTTP, Priority: 100, Port: 80, Action: Allow

Rule Name: Allow\_SSH, Priority: 110, Port: 22, Action: Allow

* Outbound Rules:

By default, all outbound traffic is allowed. You can define rules as per specific needs.

Associate NSG with Subnet/VM:

* Once rules are defined, navigate to ‘Subnets’ or ‘Network interfaces’ under the NSG.
* Associate the NSG with the previously created VNet subnet or directly to a VM’s NIC.

**4. Testing and Monitoring**

1. Deploy a VM: Deploy a VM within the VNet and verify the connectivity based on your NSG rules.
2. Monitoring: Use Azure’s monitoring and diagnostic features to review the NSG logs and ensure that the traffic is being filtered as per your defined rules.

**5. Best Practices**

* Segregation: Use different VNets for dev/test and production environments.
* Minimal Access: Always adhere to the principle of least privilege. Only open necessary ports and restrict access to specific IP addresses whenever possible.
* Regular Audits: Periodically review and audit NSG rules to ensure compliance with security policies.

**6. Conclusion**

Azure Virtual Network and Network Security Groups provide the foundational network and security capabilities needed for the deployment of applications and data on Azure. Properly configuring VNets and NSGs is crucial to ensuring that your Azure resources remain isolated and secure while still being accessible to authorized entities. Always design with security in mind and make full use of Azure’s rich networking features to keep your deployments safe.