**NSG can apply to subnet of NIC, we have one more security solution that we can apply on group of VM reoffered as ASG**

**What is an ASG?**

An **Application Security Group (ASG)** is a feature in Azure Network Security that allows users to group virtual machines (VMs) logically and define network security policies based on those groups. ASGs simplify the management of **Network Security Group (NSG)** rules by enabling logical references to VMs, rather than relying on static IP addresses.

**Key Features of ASGs**

* **Logical Grouping:** Group VMs by application tier or function (e.g., web, app, database).
* **Integration with NSGs:** Use ASGs within NSG rules to control inbound and outbound traffic.
* **IP Management Simplified:** Avoid manual IP tracking—use ASG names instead.
* **Dynamic Association:** Add or remove VMs from ASGs without updating NSG rules.

**Example Use Case**

Consider a 3-tier architecture with the following components:

* Web Servers
* Application Servers
* Database Servers

**Step 1: Create ASGs**

* asg-web
* asg-app
* asg-db

**Step 2: Define NSG Rules**

* **Allow** traffic from asg-web to asg-app on port **80**
* **Allow** traffic from asg-app to asg-db on port **1433**
* **Deny** all other traffic

This setup allows secure and structured communication across different tiers while minimizing manual configuration.

**How to Use ASGs**

1. **Create ASGs**  
   Use the Azure Portal, CLI, ARM templates, Bicep, or Terraform.
2. **Associate ASGs with VMs or NICs**  
   Attach the VM’s network interface (NIC) to an ASG.
3. **Reference ASGs in NSG Rules**  
   Use ASGs as either the **source** or **destination** in network rules.