An Application Security Group (ASG) in Azure allows you to configure network security as a natural extension of an application’s structure, allowing you to group virtual machines and define security policies based on those groups. Here’s how you can create an ASG and associate it with a virtual machine using the Azure portal.

**Step-by-Step Guide**

**Step 1: Log in to Azure Portal**

1. Go to the [Azure portal](https://portal.azure.com/).
2. Log in with your Azure account credentials.

**Step 2: Create an Application Security Group (ASG)**

1. In the left-hand navigation pane, select **Application security groups**.
2. Click **+ Create**.
3. Fill in the required details:
   * **Subscription**: Select your subscription.
   * **Resource group**: Select an existing resource group or create a new one.
   * **Name**: Enter a name for the ASG.
   * **Region**: Select the region.
4. Click **Review + create**, then **Create**.

**Step 3: Create or Select an Existing Virtual Machine (VM)**

1. In the left-hand navigation pane, select **Virtual machines**.
2. Click **+ Create** to create a new VM, or select an existing VM to modify it.

If creating a new VM:

* + Fill in the required details such as **Subscription**, **Resource group**, **VM name**, **Region**, **Image**, **Size**, **Administrator account**, and **Networking**.
  + Under **Networking**, configure the **Virtual network** and **Subnet**.
  + Click **Next** through the remaining steps and finally click **Create**.

**Step 4: Associate ASG with a Virtual Machine**

1. Go to the **Virtual machines** section in the left-hand navigation pane and select the VM you want to associate with the ASG.
2. In the VM's overview, click on **Networking** under **Settings**.
3. In the **Networking** pane, find the **Network interface** (NIC) attached to the VM and click on it.
4. In the **Network interface** pane, select **IP configurations** under **Settings**.
5. Click on the **IP configuration** name to edit it.
6. In the **IP configurations** pane, under **Application security groups**, click **+ Associate**.
7. Select the ASG you created earlier and click **Save**.

**Step 5: Verify ASG Association**

1. In the **Virtual machines** section, select the VM you associated with the ASG.
2. In the VM's overview, click on **Networking** under **Settings**.
3. Verify that the ASG is listed under the **Application security groups** section.

**Step 6: Create and Apply NSG Rules Using ASG**

1. In the left-hand navigation pane, select **Network security groups**.
2. Select the NSG you want to use, or create a new one by clicking **+ Create** and following the steps for creating an NSG.
3. In the NSG's overview, click on **Inbound security rules** or **Outbound security rules** under **Settings**.
4. Click **+ Add** to create a new rule.
5. Fill in the rule details, using the ASG in the **Source** or **Destination** field as needed:
   * **Source**: Select Application security group and choose the ASG.
   * **Source port ranges**: Specify the port ranges or set to \* for all.
   * **Destination**: Select Application security group and choose the ASG.
   * **Destination port ranges**: Specify the port ranges or set to \* for all.
   * **Protocol**: Choose Any, TCP, or UDP.
   * **Action**: Choose Allow or Deny.
   * **Priority**: Enter a priority number (lower numbers have higher priority).
   * **Name**: Enter a name for the rule.
   * **Description**: Optionally, add a description.
6. Click **Add** to create the rule.

By following these steps, you have created an ASG, associated it with a virtual machine, and applied network security rules using the ASG. This setup allows for more flexible and manageable network security configurations.