1. Objective – Create security rules

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. At the top of the resource group window select **+ Add**, search for and select "*network security group*", then choose **Create.** Enter the following configuration information. If not noted below, use the defaults:

   Resource group: *oreilly-az104*

   Name: *nsg-frontend-westus*

   Location: *West US*

3. Select **Review + create**, then **Create**
1. If needed, select the notification bell in the top right-hand corner to view deployment progress as the network security group is created. It takes a minute or two to create the resource.
4. When ready, select **Go to resource**
5. Look at the default inbound and outbound security rules. These rules take effect if you don't define any higher-priority rules. The lower the integer value of the priority, the higher the priority. When an explicit allow or deny rule is reached, the processing of rules stops.
6. Select **Inbound security rules** from the menu on the left-hand side, then **+ Add.** Enter the following configuration information. If not noted below, use the defaults:

   Look at **Source** options, leave as *Any*

   Destination: *Any*

   Destination port ranges: *80*

   Protocol: *TCP*

   Action: *Allow*

   Priority: *100*

   Name: *Port_80*

7. When ready, select **Add**

2. Objective – Associate NSG to a subnet or network interface

1. From your *nsg-frontend-westus* resource, select **Subnets** from the menu on the left-hand side.
2. Select **+ Associate**, then choose the *vnet-westus* virtual network.
3. Choose the *frontend-subnet*, and note that the *GatewaySubnet* is unavailable.
4. When ready, select **OK**