Module 3 - Lab 3 - Filtering Network Traffic with Network Security Groups

Overview

In this lab, you will create a virtual network, network security groups and an application security group. From there you will associate several security rules and then create several virtual machines associated with them to test filtering network traffic.

Exercise 1: Create a Virtual Network and Security Groups

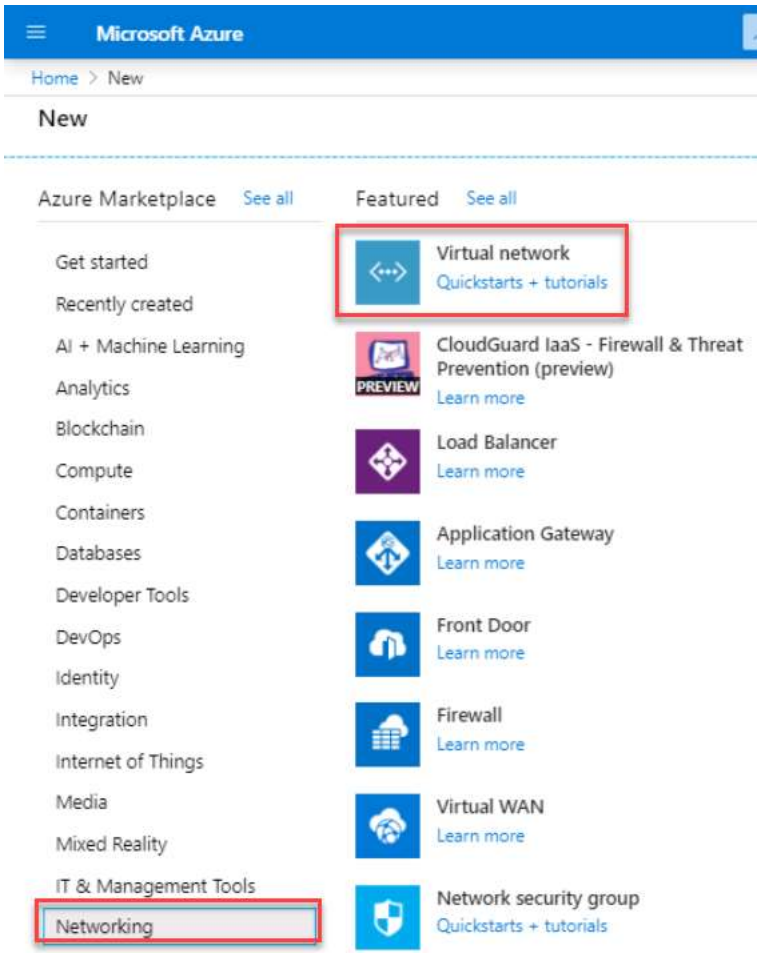
In this exercise, you will create the lab's virtual network as well as application and network security groups.

Task 1: Create a Virtual Network

- [ ] 1. Launch a broswer in the Lab VM and navigate to the URL **https://portal.azure.com** and login with the username **sheikhnasirJV3ZM@gdcs1.com** and password **EvPOwKYcA4jrQ7CO**

- [ ] 2. Expand the portal's left navigation by clicking **Show portal menu** in the top left.

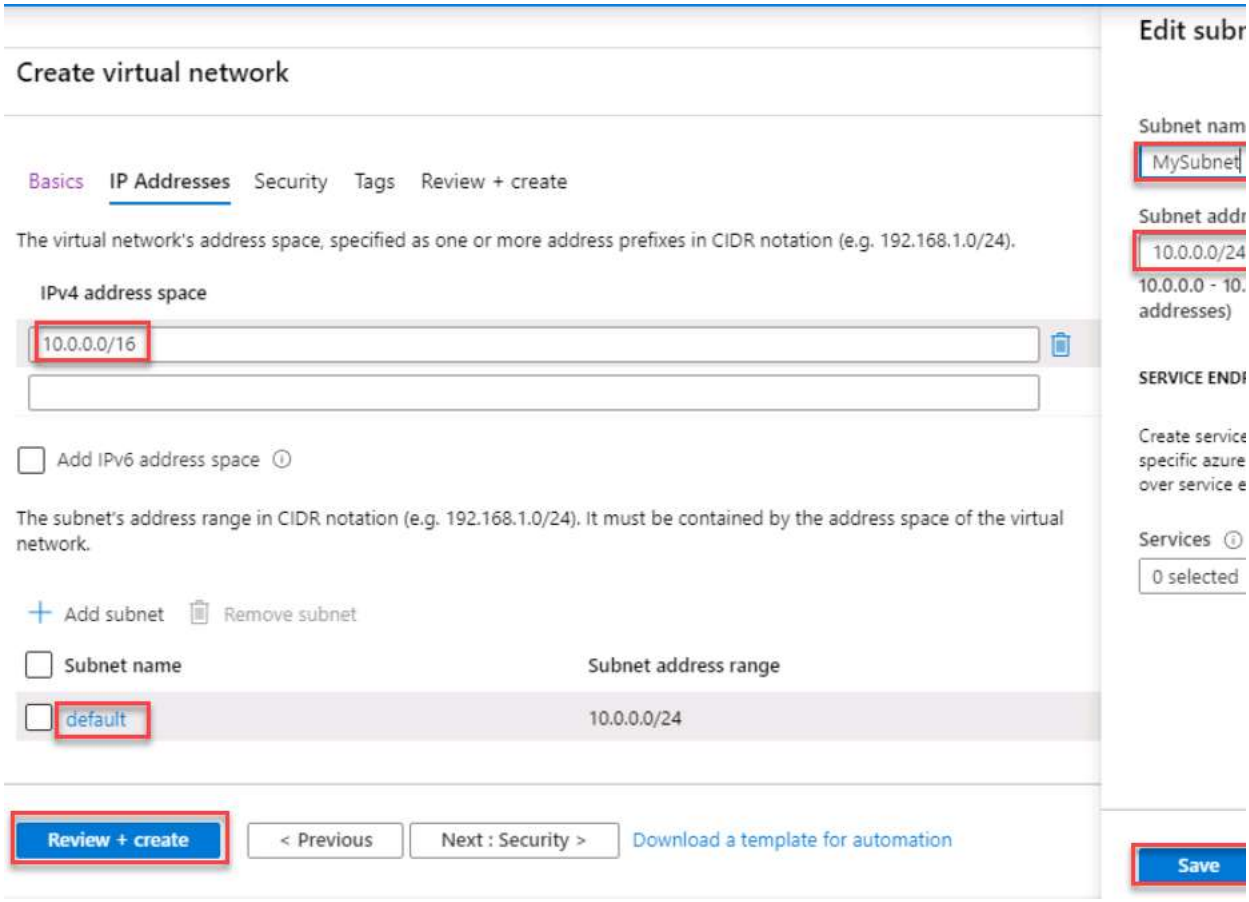
- [ ] 3. Click **+ Create a resource** > **Networking** > **Virtual Network**



- [ ] 4. In the **Create virtual network** blade, enter the following configuration and click **Next: IP Addresses**.
    - Resource Group: **NSGLabRG-DLPOE1DZAR**
    - Name: **NSGLabVN**
    - Region: South Central US

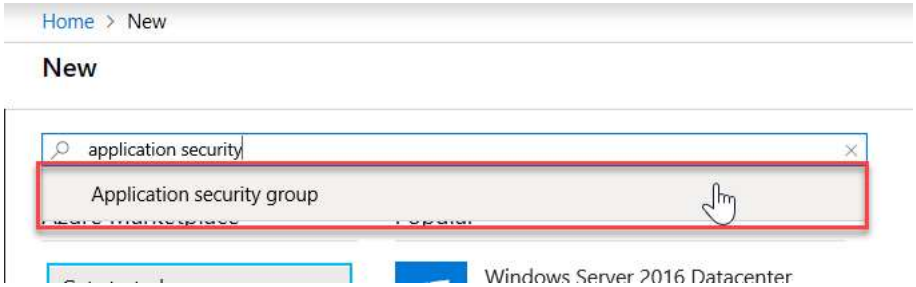
- [ ] 5. In The **IP Addresses** tab, enter the following configuration then click **Review + Create** then **Create**.
    - Address Space: **10.0.0.0/16**
    - Subnet name: Click **default** then enter **MySubnet** in the **Edit Subnet** blade that appears.

- Subnet Address Range: Enter 10.0.0.0/24 in the **Edit Subnet** blade then click **Save**.

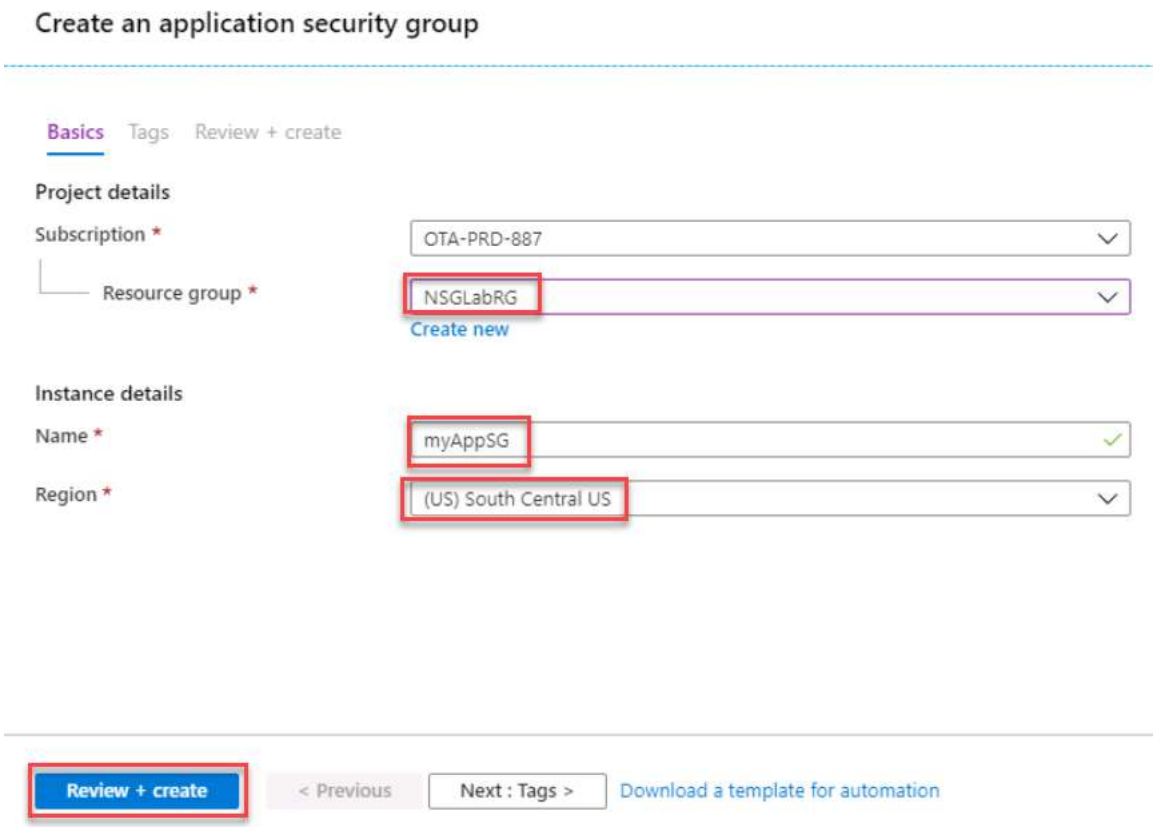


Task 2: Create a Application Security Groups

- [ ] 1. Click **+ Create a resource**
- [ ] 2. Search for and select Application security group



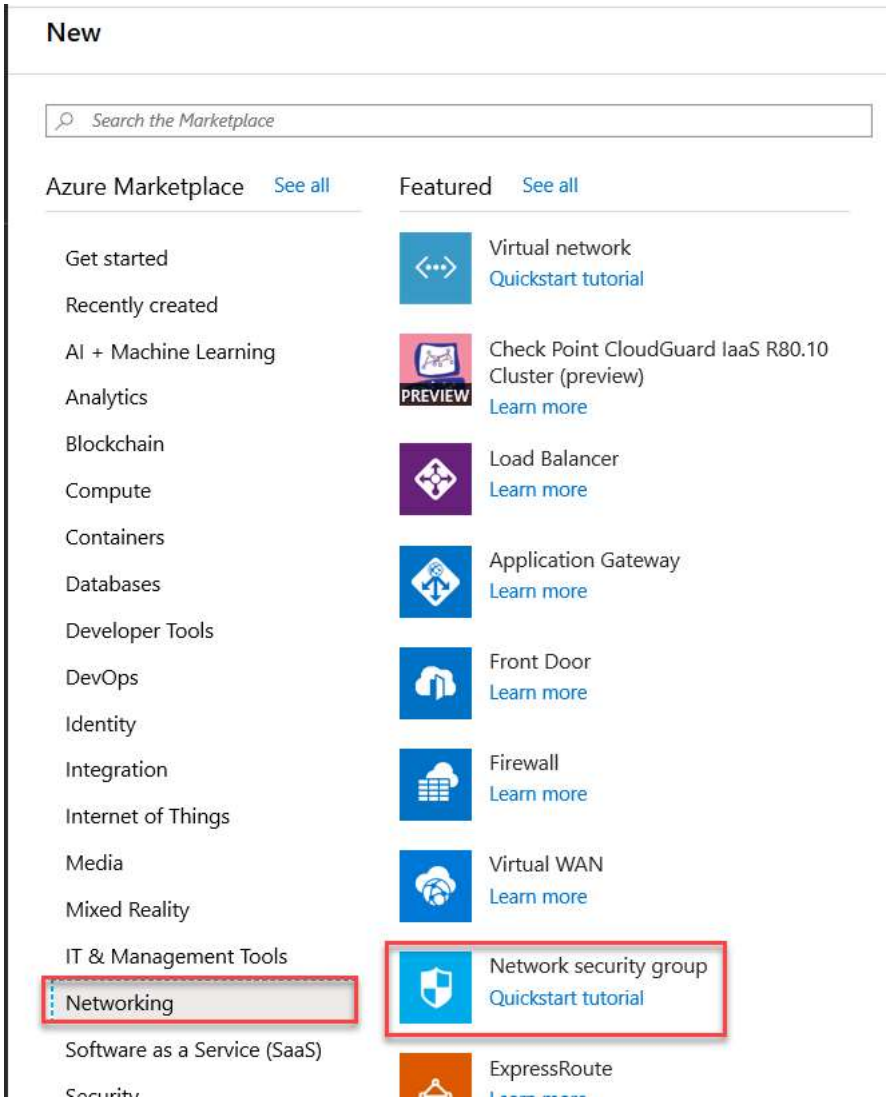
- [ ] 3. Click **Create**
- [ ] 4. In the **Create an application security group** blade, enter the following configuration then click **Review + Create** then **Create**.
  - Resource Group: NSGLabRG-DLPOE1DZAR
  - Name: myAppSG
  - Region: **Select the same region you used previously**



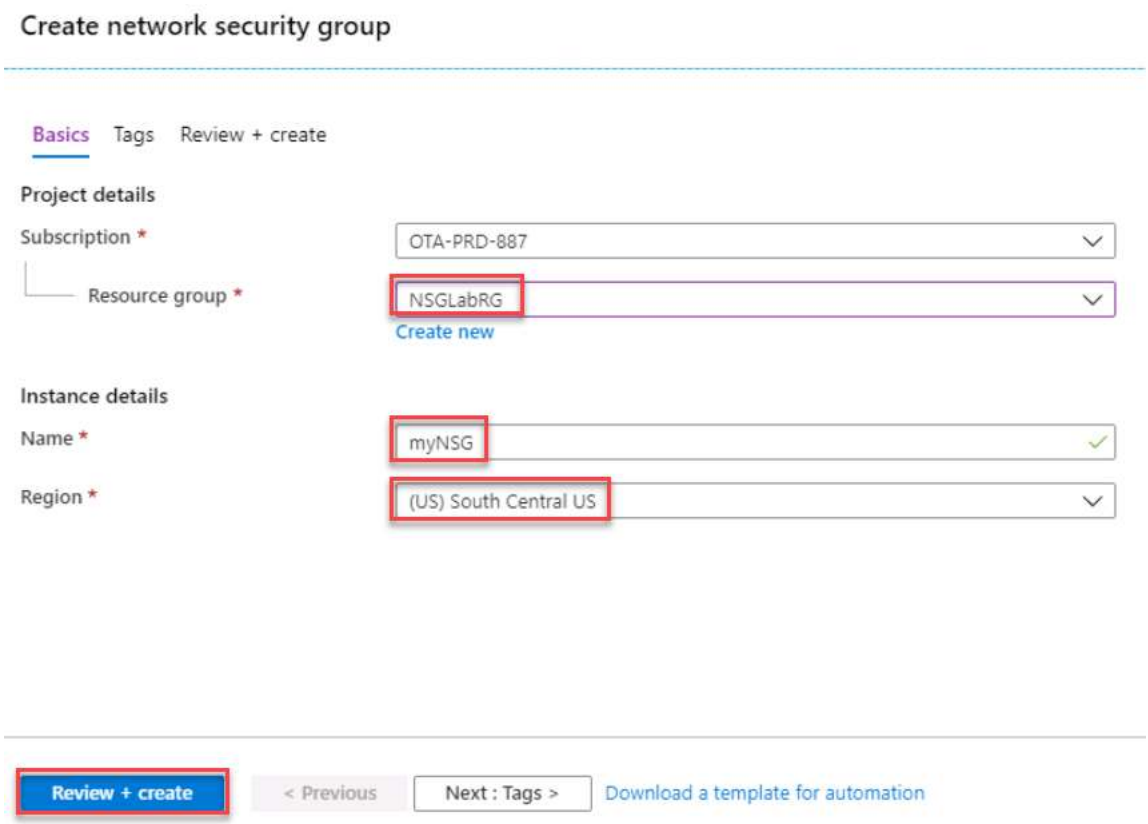
- [ ] 5. Repeat steps 1-3 then enter the following configuration. Click **Review + Create** then **Create**.
    - Resource Group: **NSGLabRG-DLPOE1DZAR**
    - Name: **myMgmtSG**
    - Region: **Select the same region as you used previously**
- [ ] 6. This will enable you to group together servers with similar functions.

Task 3: Create a Network Security Group

- [ ] 1. Click **+ Create a resource** > **Networking** > **Network security group**



- [ ] 2. In the **Create network security group** blade, enter the following configuration then click **Review + Create** then **Create**.
    - Resource Group: **NSGLabRG-DLPOE1DZAR**
    - Name: **myNSG**
    - Location: **Select the same region you used previously**



✓ **Results**: In this exercise, you successfully created a virtual network along with application security groups and a network security group.

Exercise 2: Associate Network Security Groups to a Subnet and Create Security Rules.

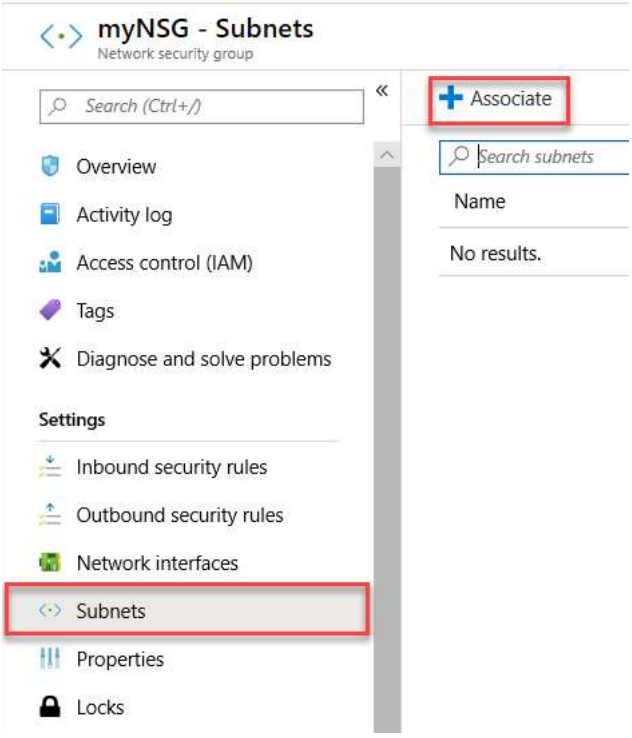
In this exercise, you will associate the network security group created previously to the subnet and then create security rules.

Time Estimate

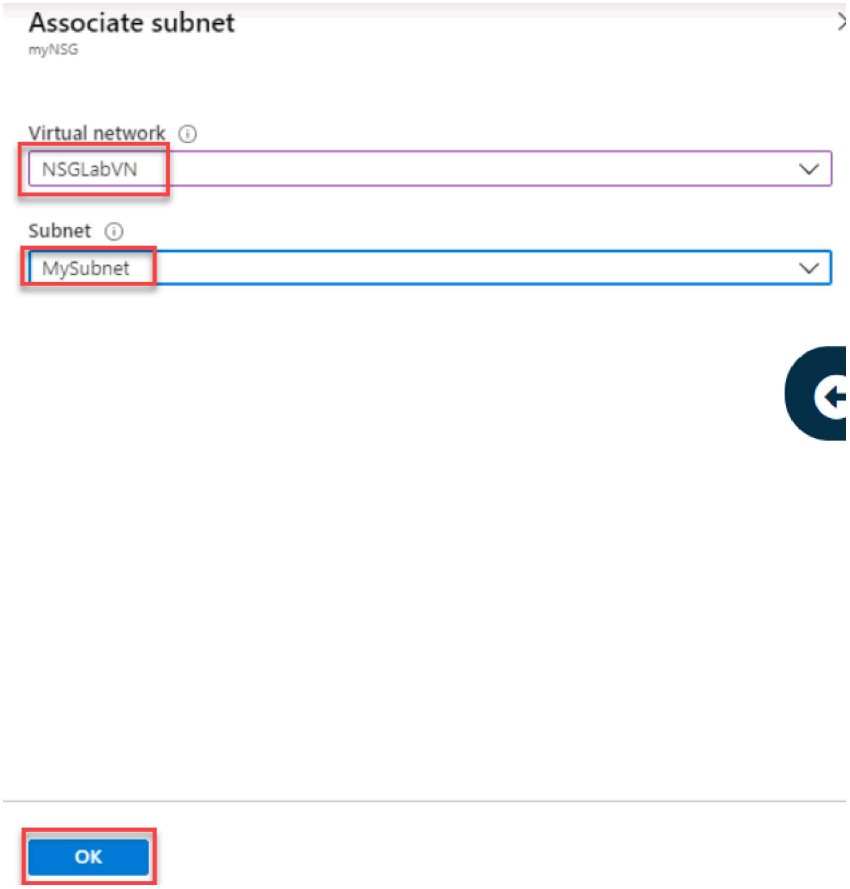
- 20 minutes

Task 1: Associate the Network Security Group to a Subnet

- [ ] 1. Navigate to your network security group in the portal.
- [ ] 2. Under **Settings**, click **Subnets** Then click **+ Associate**.

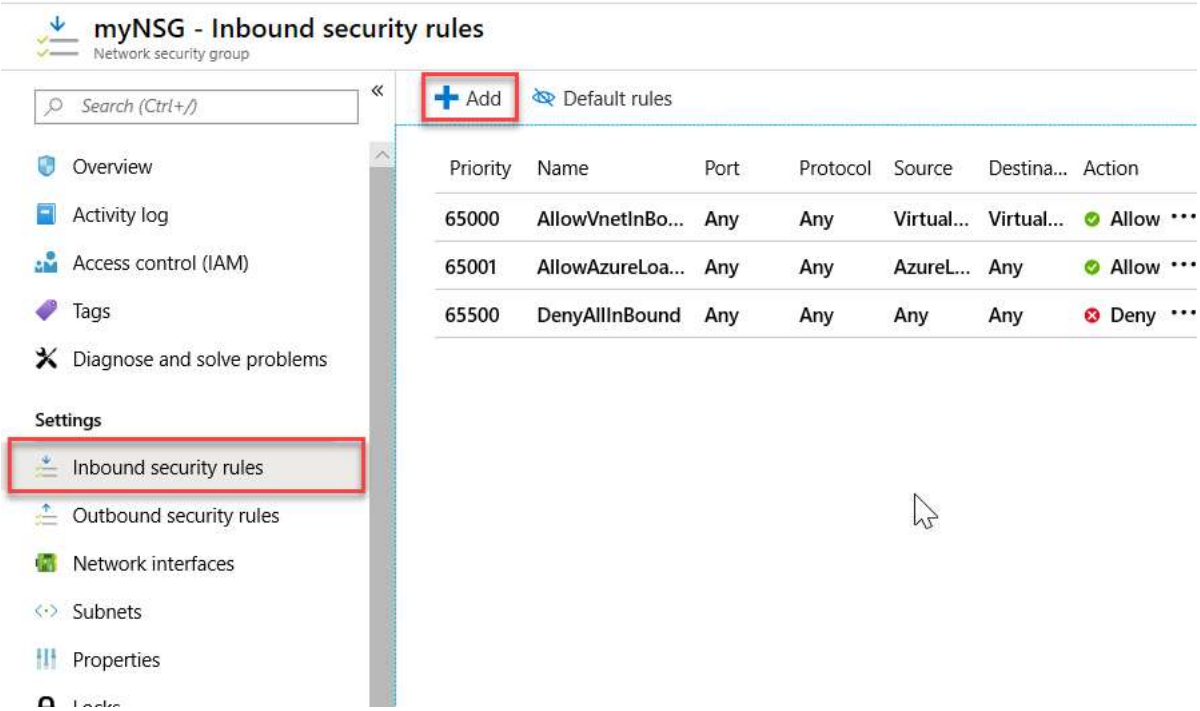


- [ ] 3. In the **Associate subnet** blade, enter the following configuration then click **OK**.
    - Virtual Network: NSGLabVN
    - Subnet: **MySubnet**

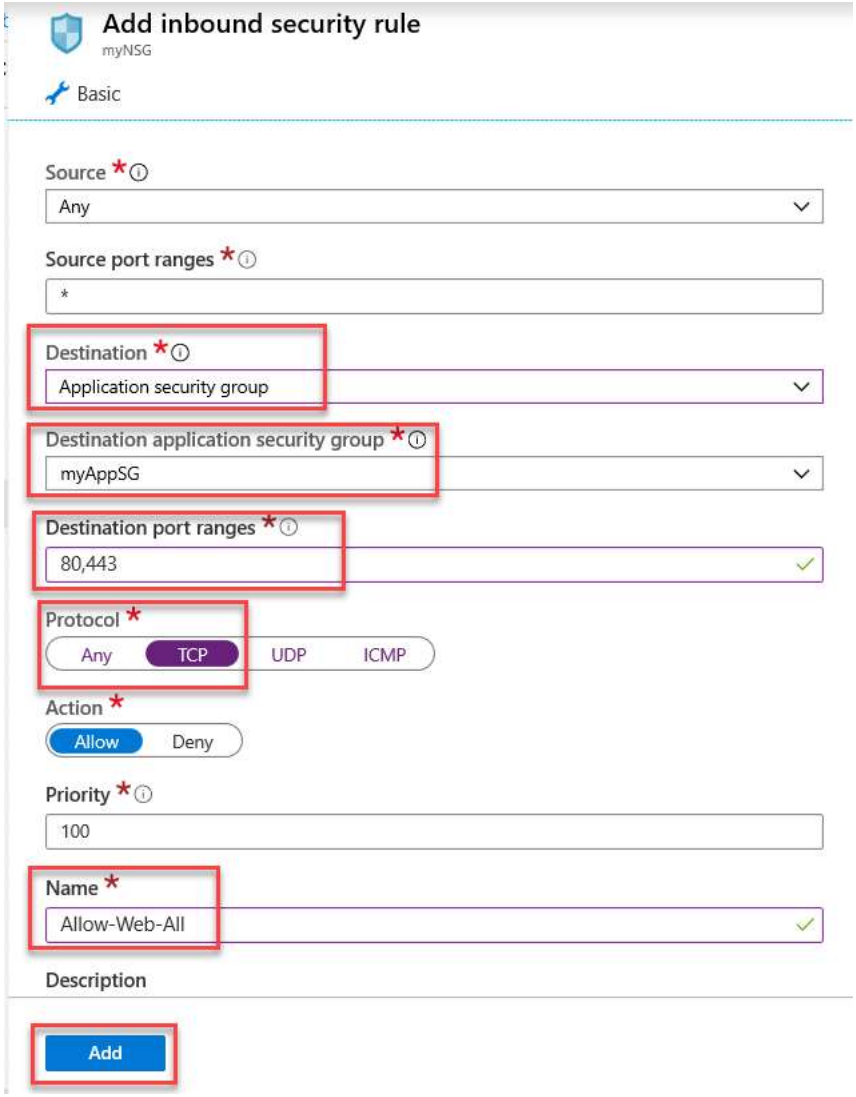


Task 2: Create Security Rules

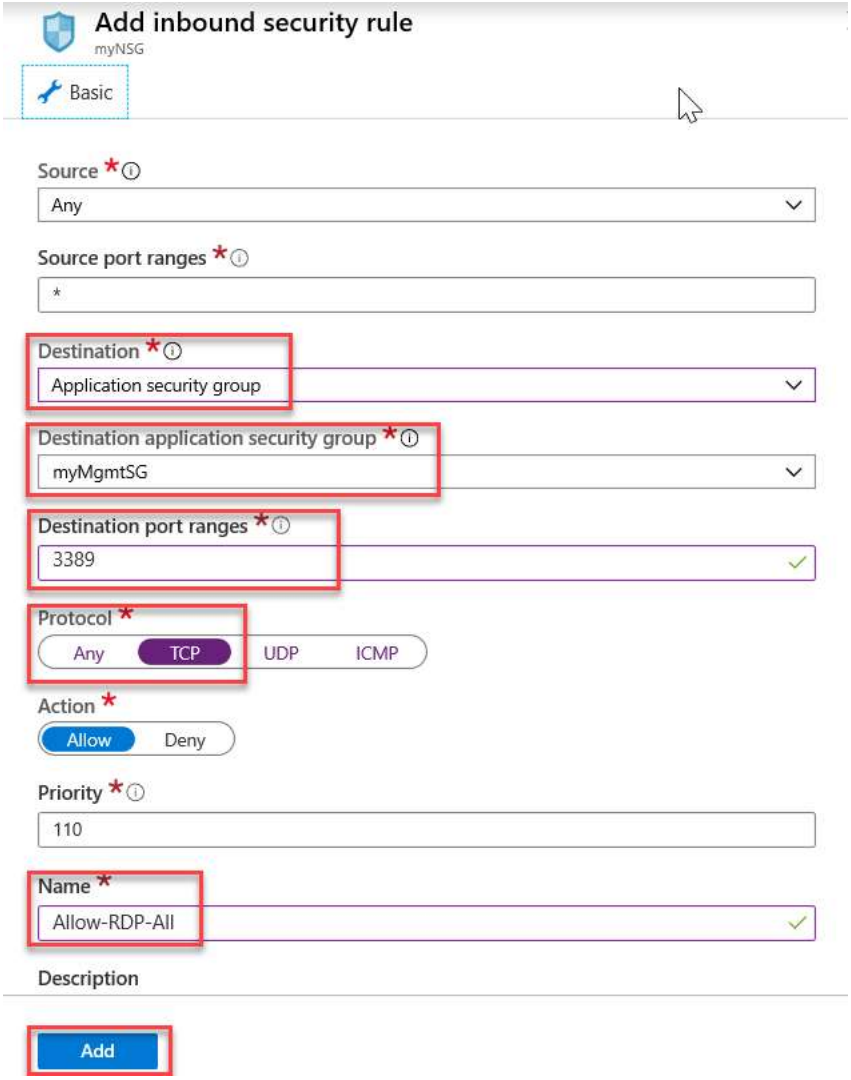
- [ ] 1. Navigate to your network security group in the portal.
- [ ] 2. Under **Settings**, click **Inbound Security Rules** then click **+ Add**



- [ ] 3. In the **Add inbound security rule** blade, enter the following configuration then click **Add**.
    - Destination: **Application security group**
    - Destination application security group: **myAppSG**
    - Destination port ranges: **80,443**
    - Protocol: **TCP**
    - Name: **Allow-Web-All**



- [ ] 4. Click + **Add** again, then enter the following configuration and click **Add**.
    - Destination: **Application security group**
    - Destination application security group: **myMgmtSG**
    - Destination port ranges: **3389**
    - Protocol: **TCP**
    - Name: **Allow-RDP-All**



✓ **Results**: In this exercise, you successfully associated the network security group to the subnet and created security rules.

Exercise 3: Configuring and Testing Traffic Filters

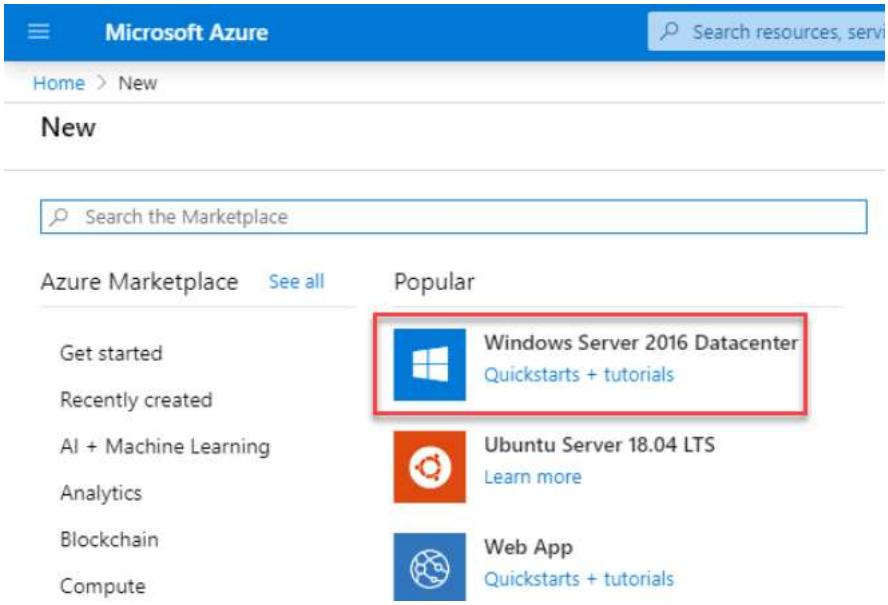
In this exercise, you will create two virtual machines in the virtual network. Then you will add each virtual machine's network interface to the application security groups created earlier. Finally, you will test the traffic filters.

Time Estimate

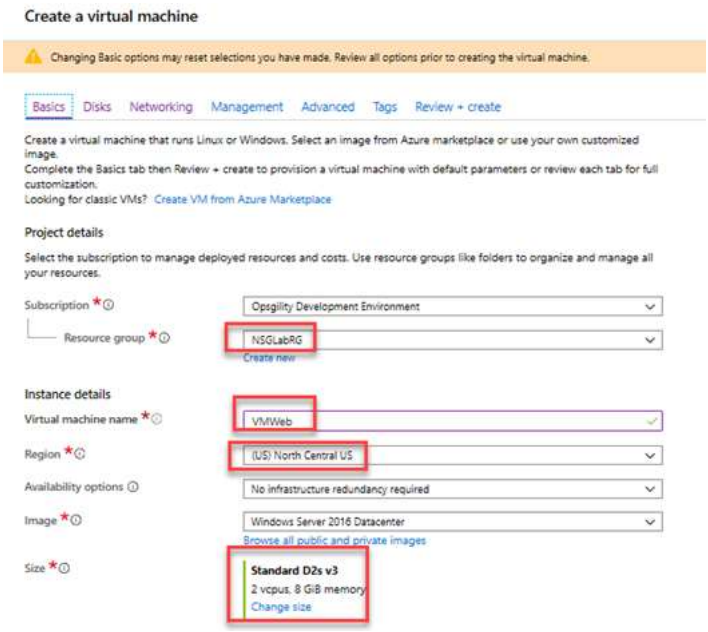
- 30 minutes

Task 1: Create Virtual Machines

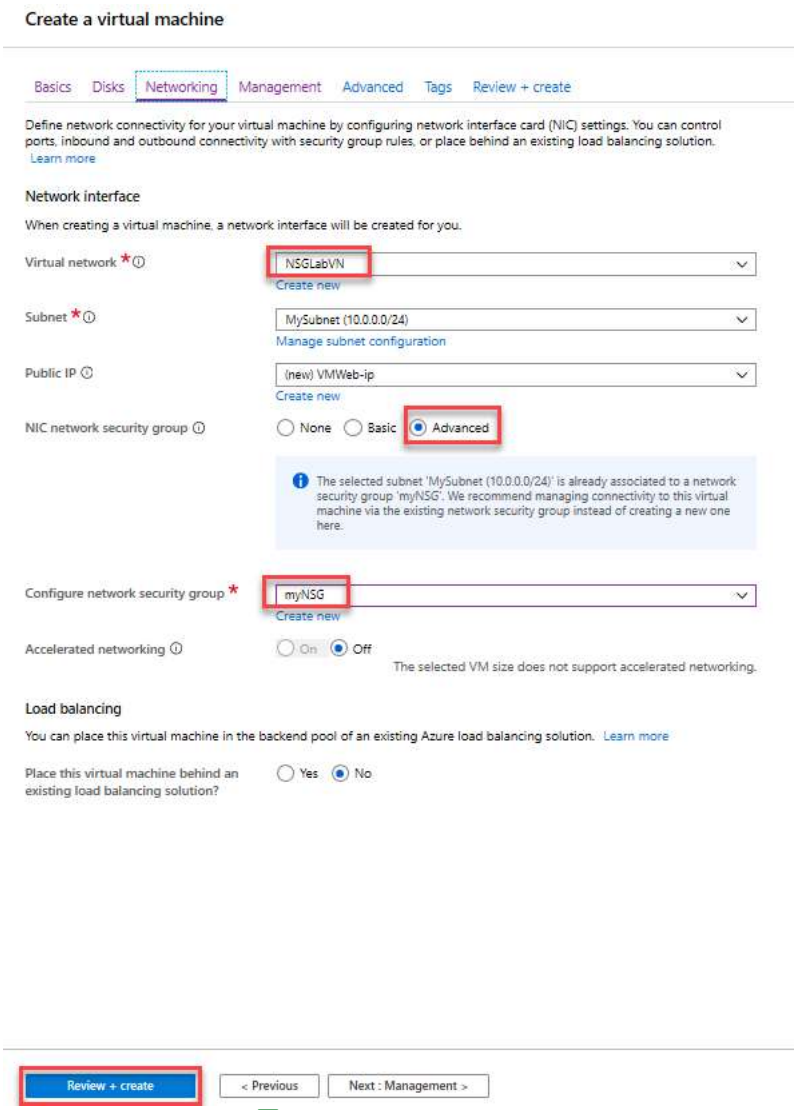
- [ ] 1. Click **+ Create a Resource** search for and select **Windows Server 2016 Datacenter**



- [ ] 2. In the **Create a virtual machine** blade, enter the following configuration then click **Next: Disks** then **Next: Networking**.
    - Resource Group: **NSGLabRG-DLPOE1DZAR**
    - Name: **VMWeb**
    - Region: **Select the same region you've been using**
    - Size: **Standard D2S_V3**
    - Username: **localadmin**
    - Password/Confirm Password: **EvPOwKYcA4jrQ7CO**



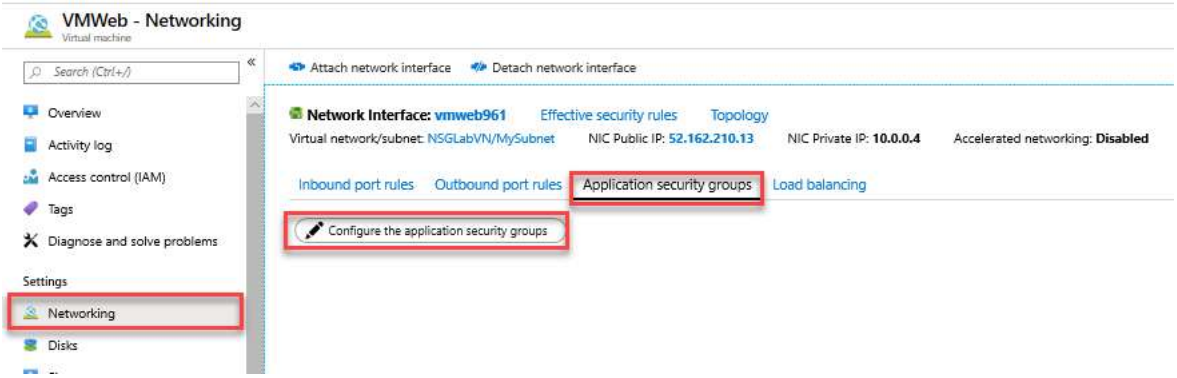
- [ ] 3. On the **Networking** section, enter the following configuration then click **Review + Create** then **Create**.
    - Virtual Network: **NSGLabVN**
    - NIC Network Security Group: **Advanced**
    - Configure Network Security Group: **myNSG**



- [ ] 4. Repeat Steps 1-3 except name the VM **VMMgmt**.
- [ ] 5. Wait for the VMs to be fully deployed before moving to the next task.

Task 2: Associate network interfaces to ASGs

- [ ] 1. Navigate to the **VMWeb** VM.
- [ ] 2. Under **Settings** select **Networking** then click **Application security groups** then **Configure the application security groups**

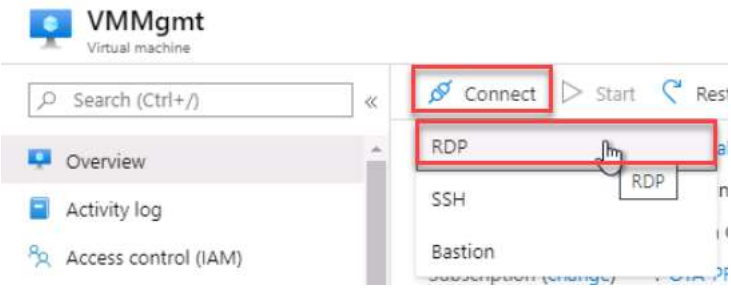


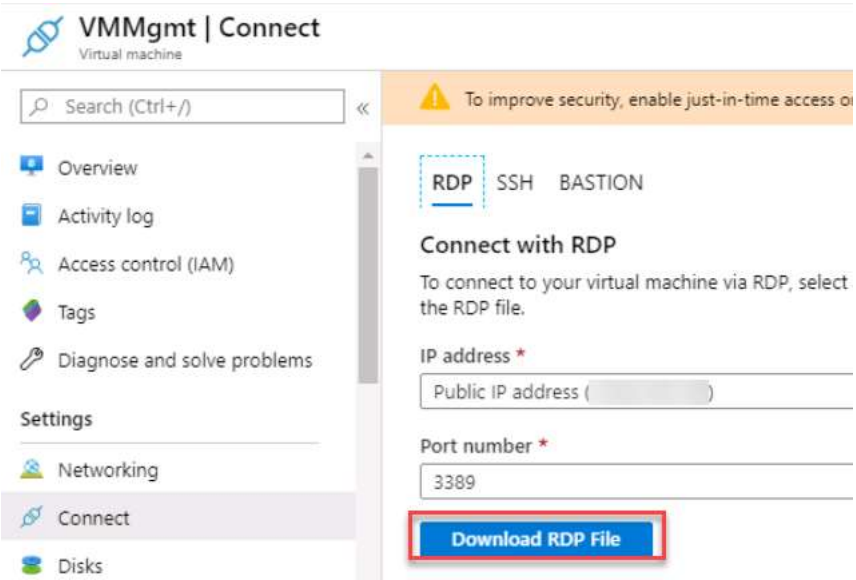
- [ ] 3. In the **Configure application security groups** blade, select **myAppSG** from the dropdown then click **Save**.

- [ ] 4. Repeat steps 1-3 for the **VMMgmt** VM except choose the **myMgmtSG** ASG.

Task 3: Test the Traffic Filters

- [ ] 1. Navigate to the **VMMgmt** VM.
- [ ] 2. Click **Connect** then **RDP**. Then click **Download RDP File**.





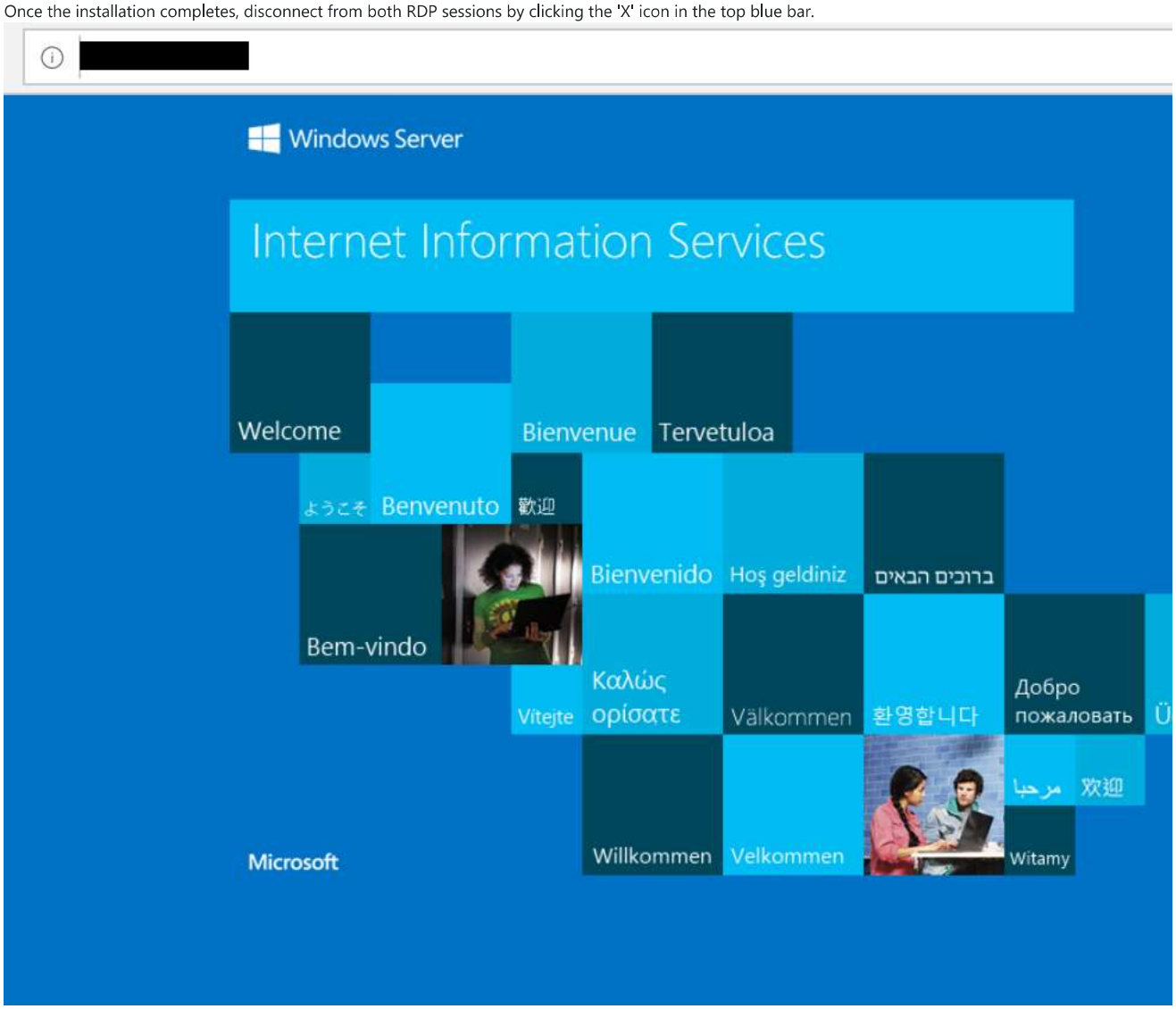
- [ ] 3. Click **Connect** then enter the VM's credentials. Click **Yes** at the next prompt.
  - Username: **localadmin**
  - Password: **EvPOwKYcA4jrQ7CO**
- [ ] 4. Open **PowerShell** from the Start menu then enter the following command.

```
mstsc /v:VMWeb
```

- [ ] 5. Enter the credentials for **VMWeb** and then click **Yes** at the prompt.
  - Username: **localadmin**
  - Password: **EvPOwKYcA4jrQ7CO**
- [ ] 6. You are able to connect to the **VMWeb** VM from the **VMMgmt** VM because the VMs are in the same virtual network. However, you cannot create a remote desktop connection to the **VMWeb** VM from the internet, because the security rule created earlier doesn't allow inbound traffic from the Internet on port 3389 and inbound traffic from the Internet is denied to all resources by default.
- [ ] 7. Open PowerShell on **VMWeb** and install Microsoft IIS using the following command

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

- [ ] 8. Once the installation completes, disconnect from both RDP sessions by clicking the 'X' icon in the top blue bar.



- [ ] 9. Navigate to the **VMWeb** VM in the portal.
- [ ] 10. Copy the public ip address then navigate to it in a new browser tab.
- [ ] 11. You see the IIS welcome screen. This is because inbound traffic from the Internet is allowed on port 80 to the **myAppSG** application security group that the network interface attached to the **VMWeb** VM is in.

✓ **Results**: In this exercise, you created two virtual machines in the virtual network. You then added each virtual machine's network interface to the application security groups created earlier. Finally, you tested the traffic filters.