**Lab06: Filter network traffic with a network security group using the Azure portal**

|  |  |
| --- | --- |
| **Name** | **Student ID** |
|  |  |

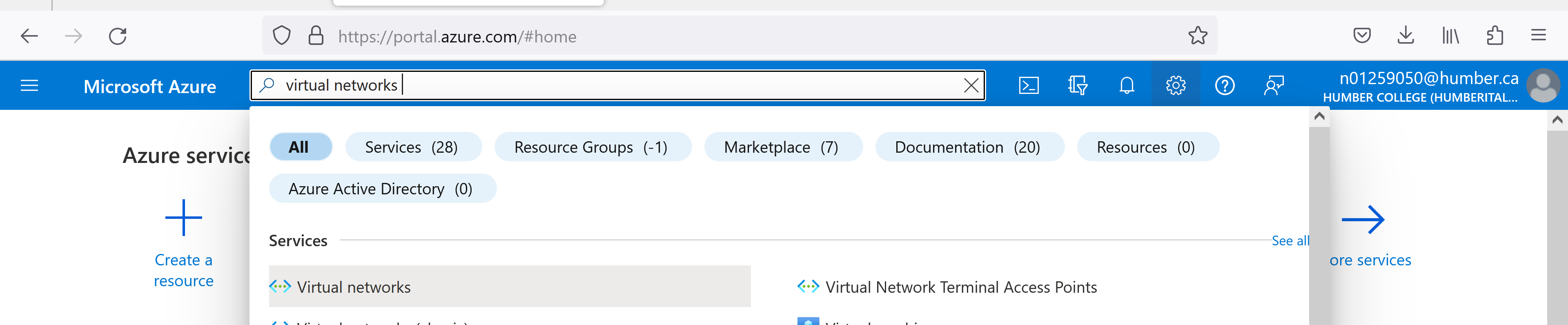
**Sign in to Azure**

Sign in to the Azure portal at [https://portal.azure.com](https://portal.azure.com/).

**Important Note**: All name in this lab are generic, so when you are creating the lab, you need to use the name conventions by using expression **ao123-** followed by the resource ( VM, Vnet, subnet, … etc); where (a) is first letter of student first name, (o) is first letter of student last name, and 123 are last three digits of Humber student.

**Create a virtual network**

1. On the Azure portal menu or from the **Home** page, write **Virtual networks** in the search bar and click **Enter.**



1. Enter, or select, the following information, accept the defaults for the remaining settings, and then select **Create**:

| **Setting** | **Value** |
| --- | --- |
| Name | ao123-Vnet |
| Address space | 10.0.0.0/16 |
| Subscription | Select your subscription. |
| Resource group | Select **Create new** and enter ***ao123-Rsg***. |
| Location | Canada Central. |
| Subnet- Name | ao123-Subnet, modify the default by change the name only or  delete the default subnet and create a new one. |
| Subnet - Address range | 10.0.0.0/24 |

**Create application security groups**

An application security group enables you to group together servers with similar functions, such as web servers.

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. In the **Search the Marketplace** box, enter *Application security group*. When **Application security group** appears in the search results, select it, select **Application security group** again under **Everything**, and then select **Create**.
3. Enter, or select, the following information, and then select **Create**:

| **Setting** | **Value** |
| --- | --- |
| Name | ao123-AsgWebSer |
| Subscription | Select your subscription. |
| Resource group | Select **Use existing** and then select ***ao123-Rsg***. |
| Location | Canada Central |

1. Complete step 3 again, specifying the following values:

| **Setting** | **Value** |
| --- | --- |
| Name | ao123-AsgMangSer |
| Subscription | Select your subscription. |
| Resource group | Select **Use existing** and then select ***ao123-Rsg***. |
| Location | Canada Central |

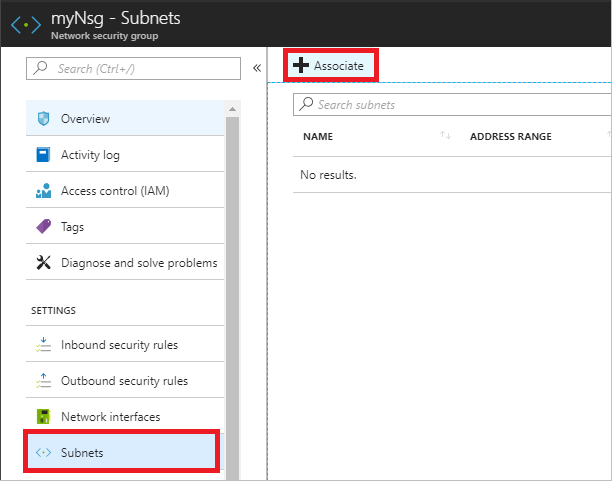
**Create a network security group**

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Select **Networking**, and then select **Network security group**.
3. Enter, or select, the following information, and then select **Create**:

| **Setting** | **Value** |
| --- | --- |
| Name | ao123-Nsg |
| Subscription | Select your subscription. |
| Resource group | Select **Use existing** and then select ***ao123-Rsg***. |
| Location | Canada Central |

**Associate network security group to subnet**

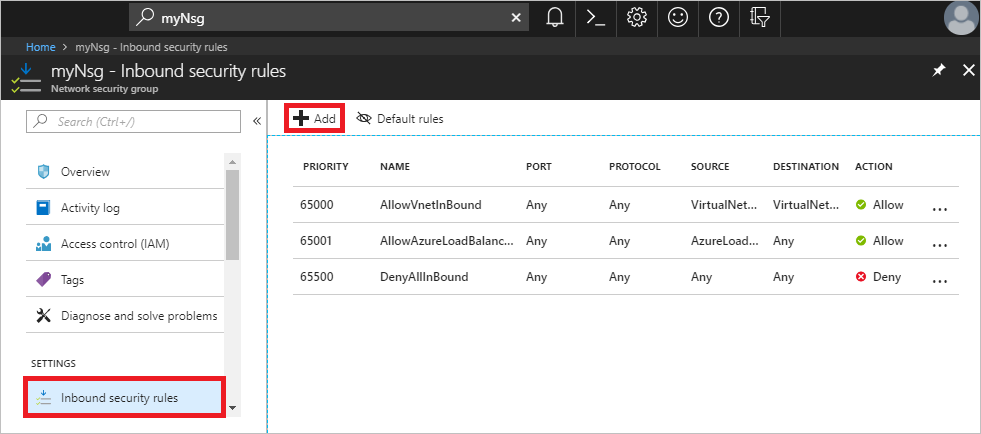
1. In the *Search resources, services, and docs* box at the top of the portal, begin typing *ao123-Nsg*. When **ao123-Nsg** appears in the search results, select it.
2. Under **SETTINGS**, select **Subnets** and then select **+ Associate**, as shown in the following picture:



1. Under **Associate subnet**, select **Virtual network** and then select **ao123-Vnet**. Select **Subnet**, select **ao123-Subnet**, and then select **OK**.

**Create security rules**

1. Under **SETTINGS**, select **Inbound security rules** and then select **+ Add**, as shown in the following picture:



1. Create a security rule that allows ports 80 and 443 to the **ao123-AsgWebSer** application security group. Under **Add inbound security rule**, enter, or select the following values, accept the remaining defaults, and then select **Add**:

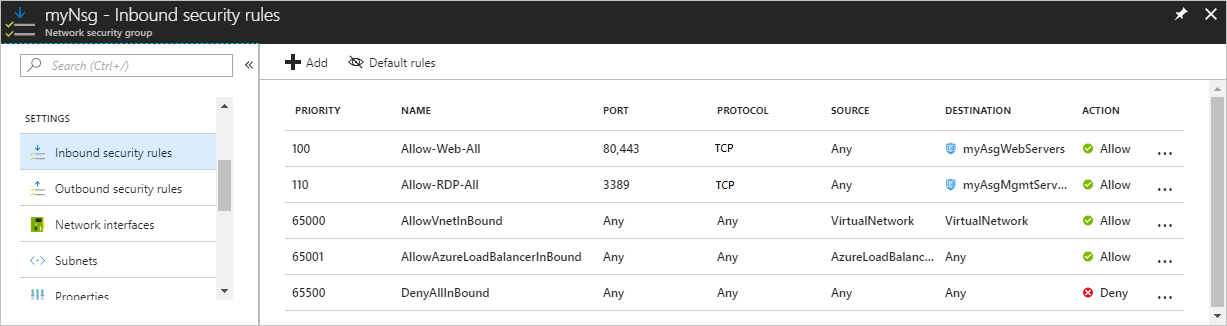
| **Setting** | **Value** |
| --- | --- |
| Destination | Select **Application security group**, and then select **ao123-AsgWebSer** for  **Application security group**. |
| Destination port ranges | Enter 80,443 |
| Protocol | Select TCP |
| Name | Allow-Web-All |

1. Complete step 2 again, using the following values:

| **Setting** | **Value** |
| --- | --- |
| Destination | Select **Application security group**, and then select **ao123-AsgMangSer** for **Application security group**. |
| Destination port ranges | Enter 3389 |
| Protocol | Select TCP |
| Priority | Enter 110 |
| Name | Allow-RDP-All |

1. In this tutorial, RDP (port 3389) is exposed to the internet for the VM that is assigned to the *ao123-AsgMangSer* application security group. For production environments, instead of exposing port 3389 to the internet, it's recommended that you connect to Azure resources that you want to manage using a VPN or private network connection.

Once you've completed steps 1-3, review the rules you created. Your list should look like the list in the following picture:



**Submit Screenshot**

**Create virtual machines**

Create two VMs in the virtual network.

**Create the first VM**

1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Select **Compute**, and then select **Windows Server 2016 Datacenter**.
3. Enter, or select, the following information, and accept the defaults for the remaining settings:

| **Setting** | **Value** |
| --- | --- |
| Subscription | Select your subscription. |
| Resource group | Select **Use existing** and select **ao123-Rsg**. |
| Name | VMWebSer |
| Location | Select **Canada Central**. |
| User name | Enter a user name of your choosing. |
| Password | Enter a password of your choosing. The password must be at least 12 characters  long and meet the [defined complexity requirements](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/faq?toc=%2fazure%2fvirtual-network%2ftoc.json#what-are-the-password-requirements-when-creating-a-vm). |

1. Select a size for the VM and then select **Select**.
2. Under **Networking**, select the following values, and accept the remaining defaults:

| **Setting** | **Value** |
| --- | --- |
| Virtual network | Select **ao123-Vnet**. |
| NIC network security group | Select **None**. |

1. Select **Review + Create** at the bottom, left corner, select **Create** to start VM deployment.

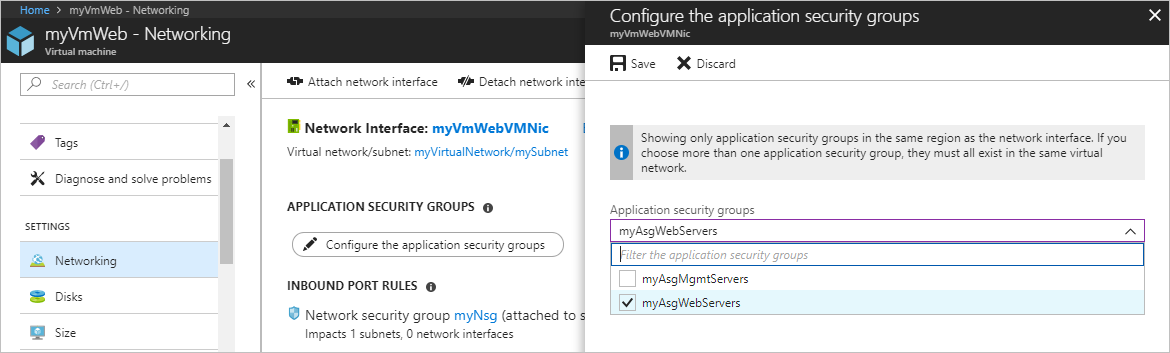
**Create the second VM**

Complete steps 1-6 again, but in step 3, name the VM **VMMangSer**. The VM takes a few minutes to deploy. Do not continue to the next step until the VM is deployed.

**Associate network interfaces to an ASG**

When the portal created the VMs, it created a network interface for each VM, and attached the network interface to the VM. Add the network interface for each VM to one of the application security groups you created previously:

1. In the *Search resources, services, and docs* box at the top of the portal, begin typing ***VMWebSer****.* When the ***VMWebSer*** VM appears in the search results, select it.
2. Under **SETTINGS**, select **Networking**. Click on the  **Configure the application security groups**, select **ao123-AsgWebSer** for **Application security groups**, and then select **Save**, as shown in the following picture:



**Submit Screenshot**

1. Complete steps 1 and 2 again, searching for the ***VMMangSer*** VM and selecting the **ao123-AsgMangSer** ASG.

**Submit Screenshot**

**Test traffic filters**

1. Connect to the ***VMMangSer*** VM. Enter ***VMMangSer*** in the search box at the top of the portal. When ***VMMangSer***appears in the search results, select it. Select the **Connect** button.
2. Select **Download RDP file**.
3. Open the downloaded rdp file and select **Connect**. Enter the user name and password you specified when creating the VM. You may need to select **More choices**, then **Use a different account**, to specify the credentials you entered when you created the VM.
4. Select **OK**.
5. You may receive a certificate warning during the sign-in process. If you receive the warning, select **Yes** or **Continue**, to proceed with the connection.

The connection succeeds, because port 3389 is allowed inbound from the internet to the *ao123-AsgMangSer* application security group that the network interface attached to the ***VMMangSer***VM.

1. Connect to the ***VMWebSer*** VM from the ***VMWebSer*** VM by entering the following command in a PowerShell session:

Copy

mstsc /v:VMWebSer

1. You are able to connect to the ***VMWebSer*** VM from the ***VMMangSer*** VM because VMs in the same virtual network can communicate with each other over any port, by default. You can't however, create a remote desktop connection to the ***VMWebSer*** VM from the internet, because the security rule for the *ao123-AsgWebSer* doesn't allow port 3389 inbound from the internet and inbound traffic from the Internet is denied to all resources by default.

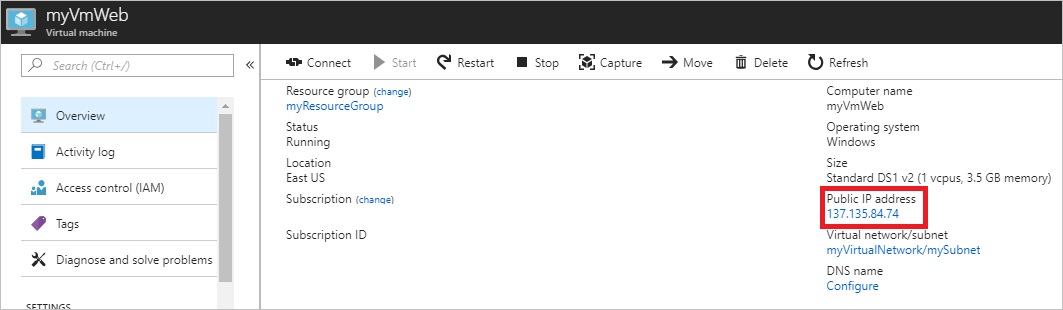
**Submit Screenshot of the error Message**

1. To install Microsoft IIS on the *myVmWeb* VM, enter the following command from a PowerShell session on the *myVmWeb* VM:

PowerShellCopy

Install-WindowsFeature -name Web-Server -IncludeManagementTools

1. After the IIS installation is complete, disconnect from the *myVmWeb* VM, which leaves you in the *myVmMgmt* VM remote desktop connection.
2. Disconnect from the *myVmMgmt* VM.
3. In the *Search resources, services, and docs* box at the top of the Azure portal, begin typing *myVmWeb* from your computer. When **myVmWeb** appears in the search results, select it. Note the **Public IP address** for your VM. The address shown in the following picture is 137.135.84.74, but your address is different:



1. To confirm that you can access the *myVmWeb* web server from the internet, open an internet browser on your computer and browse to http://<public-ip-address-from-previous-step>. You see the IIS welcome screen, because port 80 is allowed inbound from the internet to the *ao123-AsgWebSer* application security group that the network interface attached to the *myVmWeb* VM is in.

**Submit Screenshot of the web page.**

# Clean up resources: ( Important )

When you're done using the virtual network and the VMs, delete the resource group and all of the resources.

**What to submit:**

* A PDF file named after you name\_studentID.
* The PDF file must contain your full name in the first page and must show the required screenshots (5 screenshots) all with visible time and date of your host computer and your Azure account name and identification.