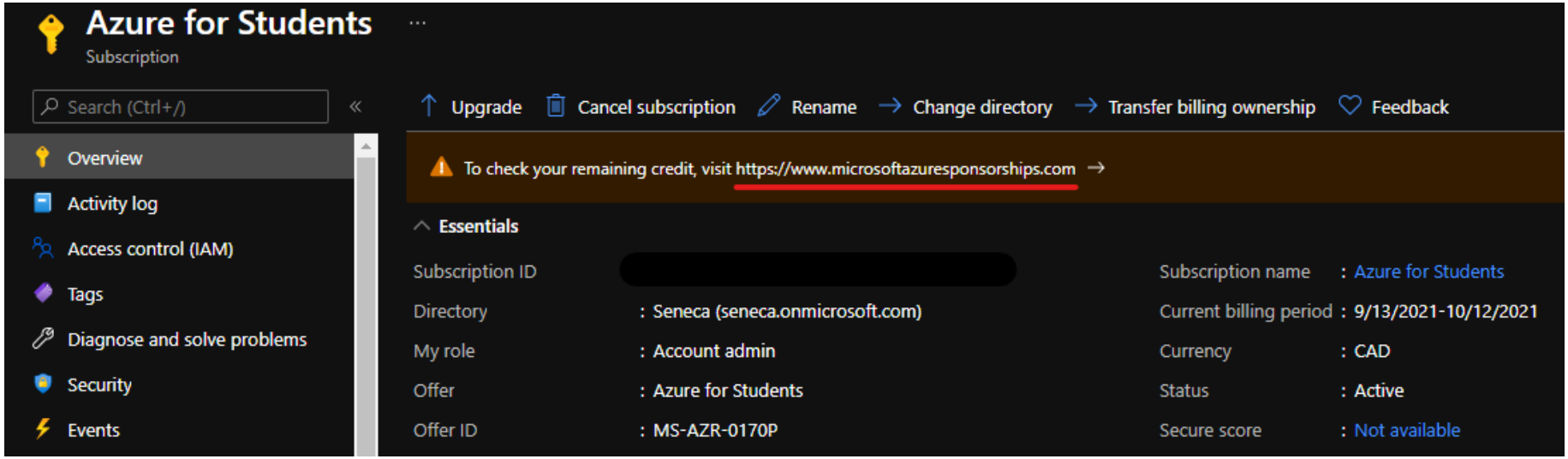
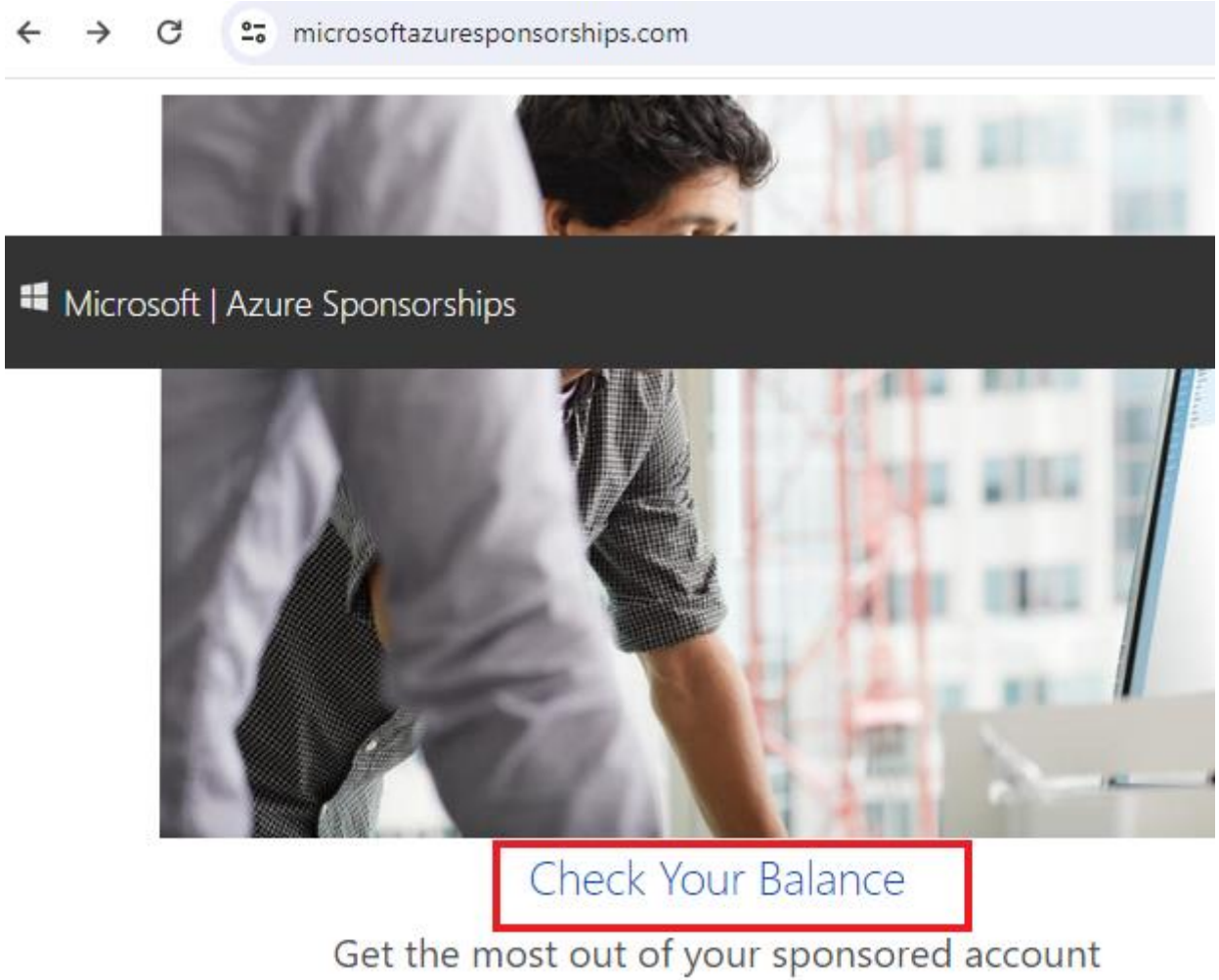
Seneca

Lab 13: Secure network traffic

At the end of each lab, any resources you created in your account will be preserved. Some Azure resources, such as VM instances, may be automatically shut down, while other resources, such as storage services will be left running. Keep in mind that some Azure features cannot be stopped and can still incur charges (i.e. Azure Bastion). To minimize your costs, delete all resources and recreate them as needed to test your work during a session.





Reference: [AZ-900T0X-MICROSOFTAZUREFUNDAMENTALS]

13 - Secure network traffic

In this walk-through, we will configure a network security group.

Task 1: Create a virtual machine (10 min)

In this task, we will create a Windows Server 2019 Datacenter virtual machine.

1. Sign in to the Azure portal with your **odl_user_xxx** azure account
2. From the **All services** blade, search for and select **Virtual machines**, and then click **+ Create** and **Azure virtual machine**.
3. On the **Basics** tab, fill in the following information (leave the defaults for everything else):

Settings	Values
Subscription	**Choose your subscription** (you should see “Seneca College : <course name>”)
Resource group	**myRGSecure** (create new)
Virtual machine name	**<student ID>WinVM (example: smore1WinVM)**
Location	**(US) East US**
Availability options	**No infrastructure redundancy required**
Security Type	**Standard**
Image	**Windows Server 2019 Datacenter – x64 Gen2**
Size	**Standard D2s v3**

Settings	Values
Administrator account username	**azureuser**
Administrator account password	**Pa$$w0rd1234**
Public Inbound port rules	**None**

4. Switch to the **Disk** tab, and configure the following setting:

Settings	Values
OS disk type	**Standard HDD (locally-redundant storage)**

5. Switch to the **Networking** tab, and configure the following setting:

Settings	Values
NIC network security group	**None**

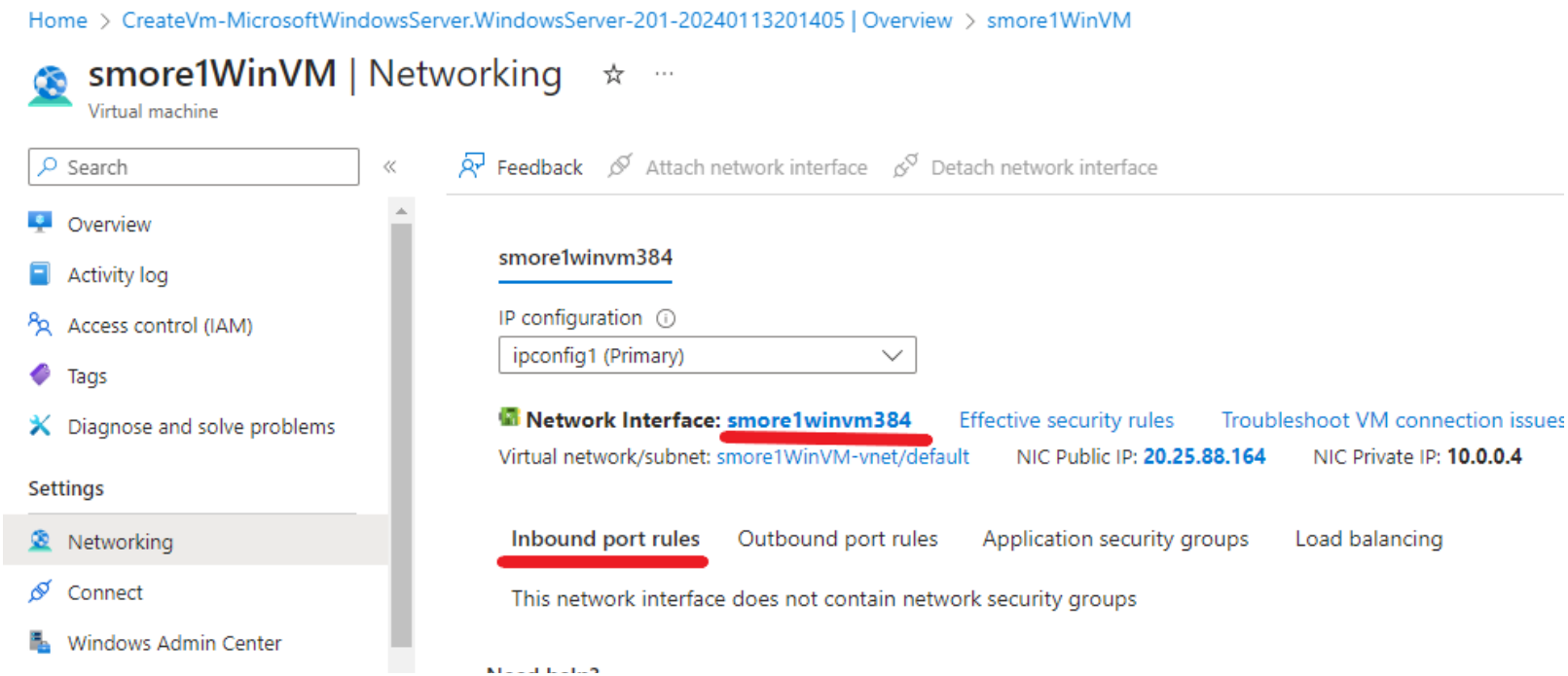
6. Switch to the **Monitoring** tab, select the following setting:

Settings	Values
Boot diagnostics	**Disable**

Settings	Values

7. Leave the remaining defaults and then click the **Review + create** button at the bottom of the page.
8. Once Validation is passed click the **Create** button. It can take about five minutes to deploy the virtual machine.
9. Monitor the deployment. It may take a few minutes for the resource group and virtual machine to be created.
10. From the deployment blade or from the Notification area, click **Go to resource**.
11. On VM **(example: smore1WinVM)** , click **Networking**, review the **Inbound port rules** tab, and note that there is no network security group associated with the network interface of the virtual machine or the subnet to which the network interface is attached.

    Note: Identify the name of the network interface. You will need it in the next task.



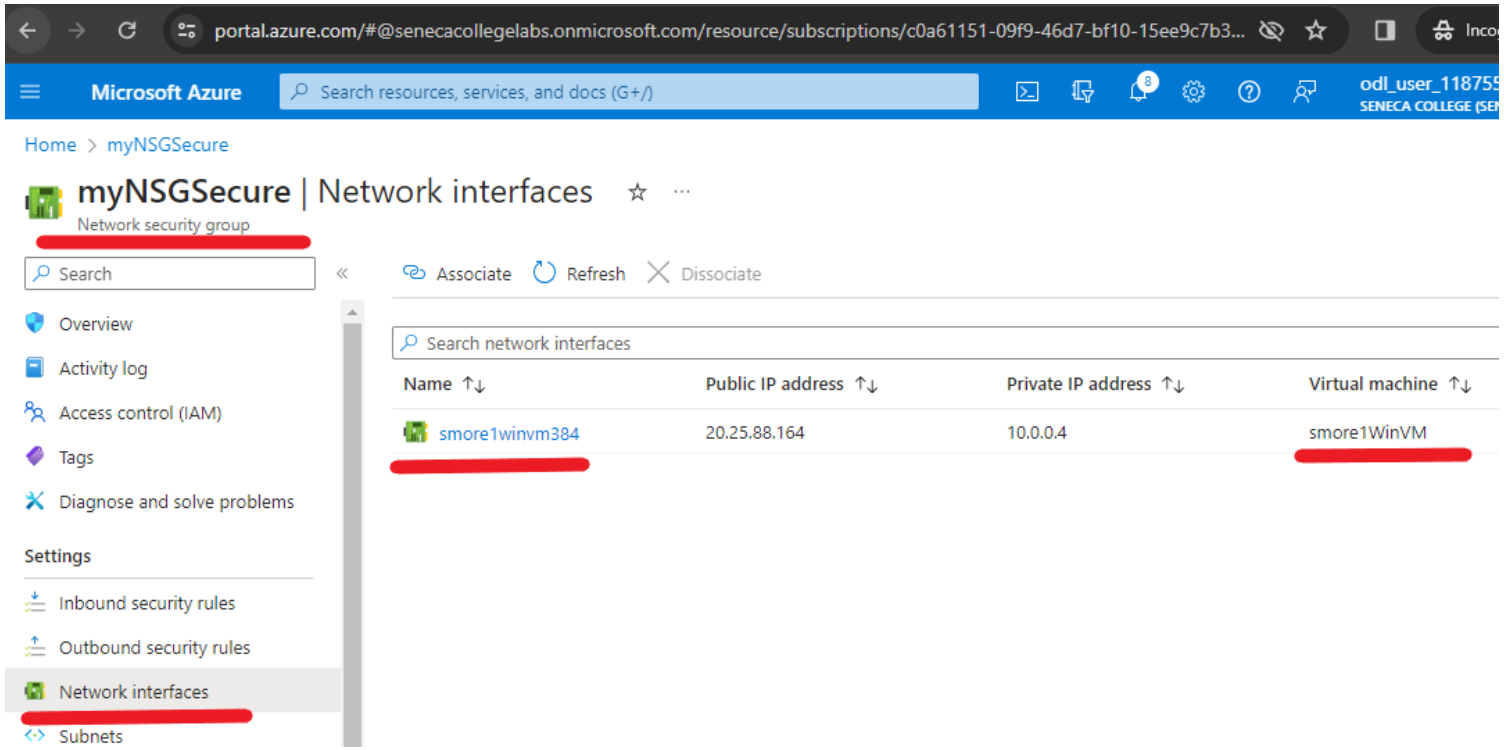
Task 2: Create a network security group

In this task, we will create a network security group and associate it with the network interface.

1. From the **All services** blade, search for and select **Network security groups** and then click **+ Create**
2. On the **Basics** tab of the **Create network security group** blade, specify the following settings.

Setting	Value
Subscription	**Choose your subscription** (you should see “Seneca College : <course name>”)
Resource group	**myRGSecure**
Name	**myNSGSecure**
Region	**(US) East US**

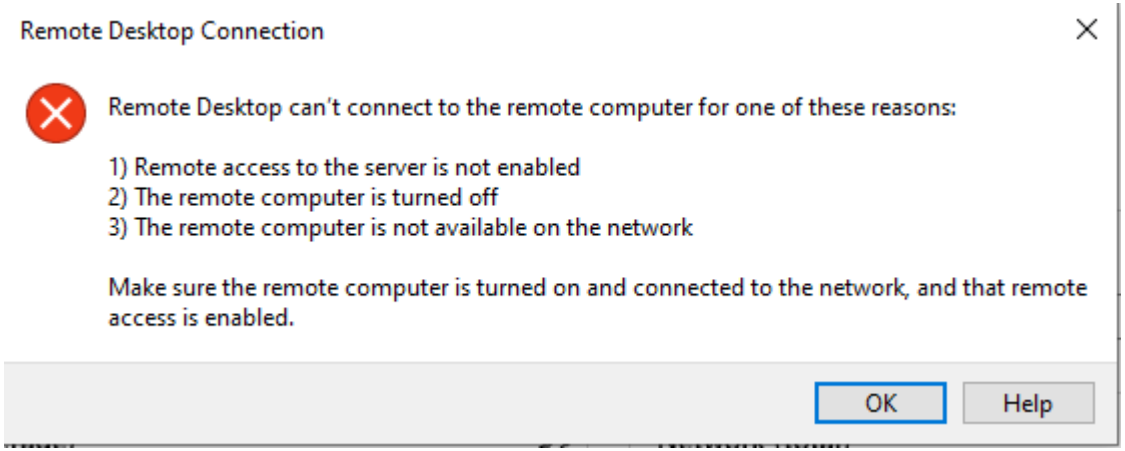
3. Click **Review + create** and then after the validation click **Create**.
4. After the NSG is created, click **Go to resource**.
5. Under **Settings** click **Network interfaces** and then **+ Associate**.
6. Select the network interace you identified in the previous task.


portal.azure.com/#@senecacollegelabs.onmicrosoft.com/resource/subscriptions/c0a61151-09f9-46d7-bf10-15ee9c7b3...
Microsoft Azure
Search resources, services, and docs (G+/)
odl_user_118755
SENECA COLLEGE (SE
Home > myNSGSecure
myNSGSecure | Network interfaces
Network security group
Search
Associate
Refresh
Dissociate
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Search network interfaces
Name
Public IP address
Private IP address
Virtual machine
smore1winvm384
20.25.88.164
10.0.0.4
smore1WinVM

Task 3: Configure an inbound security port rule to allow RDP

In this task, we will allow RDP traffc to the virtual machine by configuring an inbound security port rule.

1. In the Azure portal, navigate to the blade of the virtual machine **(example: smore1WinVM)**
2. On the **Overview** pane, click **Connect**.
3. Attempt to connect to the virutal machine using RDP. By default the network security group does not allow RDP. Close the error window.



4. On the virtual machine blade, scroll down to the **Settings** section, click on **Networking**, and notice the inbound rules for the **myNSGSecure (attached to network interface: myVMNic)** network security group deny all inbound traffic except traffic within the virtual network and load balancer probes.
5. On the **Inbound port rules** tab, click **Add inbound port rule** . Click **Add** when you are done.

Setting	Value
Source	**Any**
Source port ranges	*****

Setting	Value
Destination	**Any**
Destination port ranges	**3389**
Protocol	**TCP**
Action	**Allow**
Priority	**300**
Name	**AllowRDP**

6. Wait for the rule to be provisioned and then try again to RDP into the virtual machine. This time you should be successful. Remember the user is **azureuser** and the password is **Pa$$w0rd1234**.

Task 4: Configure an outbound security port rule to deny Internet access

In this task, we will create a NSG outbound port rule that will deny **Internet access** and then test to ensure the rule is working.

1. Continue in your virtual machine RDP session.
2. After the machine starts, open an **Internet Explorer** browser.
3. Verify that you can access **https://www.bing.com** and then close Internet Explorer. You will need to work through the IE enhanced security pop-ups.

   Note: We will now configure a rule to deny outbound internet access.

4. In the Azure portal, navigate back to the blade of the virtual machine **(example: smore1WinVM)**
5. Under **Settings**, click **Networking**, and then **Outbound port rules**.
6. Notice there is a rule, **AllowInternetOutbound**. This a default rule and cannot be removed.
7. Click **Add outbound port rule** to the right of the **myNSGSecure (attached to network interface: myVMNic)** network security group and configure a new outbound security rule with a higher priority that will deny internet traffic.
   Click **Add** when you are finished.

Setting	Value
Source	**Any**
Source port ranges	*****
Destination	**Service Tag**
Destination service tag	**Internet**
Destination port ranges	*****

Setting	Value
Protocol	**TCP**
Action	**Deny**
Priority	**4000**
Name	**DenyInternet**

8. Return to your RDP session.
9. Browse to **https://www.microsoft.com**. The page should not display. You may need to work through additional IE enhanced security pop-ups.

Note: To avoid additional costs, you can remove all resources in the resource group. Search for resource groups, click your resource group, and then delete the resources within the resource group. **DO NOT DELETE YOUR RESOURCE GROUP.**

Submission Requirements

Submit a screenshot with the following information:

Screenshot #1:

- Virtual machine browser not being able to access www.bing.com
- Both inbound and outbound rules for the network security group
- The Azure Portal with your **CloudLab Account** [requires another browser window]
    - **Note**: underline the above items as described in the below picture

portal.azure.com/#@senecacollegelabs.onmicrosoft.com/resource/subscriptions/c0a61151-09f9-46d7-bf10-15ee...

Microsoft Azure | Search resources, services, and docs (G+/) | odl_user_1187557@sen... SENECA COLLEGE (SENECACOLLE...

Home > Network security groups >

myNSGSecure

Network security group

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Locks

Monitoring

- Alerts
- Diagnostic settings
- Logs
- NSG flow logs

Automation

- CLI / PS
- Tasks (preview)

Move | Delete | Refresh

JSON View

Essentials

Resource group (move)
myRGSecure

Location
East US

Subscription (move)
Seneca College : MST300NAA - 1042

Subscription ID
c0a61151-09f9-46d7-bf10-15ee9c7b37ac

Tags (edit)
Add tags

smore1WinVM - 20.25.88.164:3389 - Remote Desktop Conne...

https://www.bing.com/

Can't reach this page

Can't reach this page

- Make sure the web address is correct
- Search for this site on Bing
- Refresh the page

Filter by name

Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority	Name	Port	Protocol	Source	Destination
Inbound Security Rules					
300	AllowRDP	3389	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any
Outbound Security Rules					
4000	DenyInternet	Any	TCP	Any	Internet
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet

Screenshot #2:

- Successful deletion of all resources within resource group. **DO NOT DELETE YOUR RESOURCE GROUP!**
  - To delete all resources with a resource group, go to "**Resource Group**", select "**myRGSecure**", select all resources within the resource group, and select "**Delete**"