

Cyber Shujaa

Cloud Security Specialist

Assignment 11: Lab - Security for virtual networks

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this lab scenario, we will implement the network security capabilities such as Network Security Groups and Application Security Groups used in securing Azure Virtual Networks. We will use Network security group rules to control network access, while Application Security Groups to secure two groups of servers: web server and management servers.

Create the virtual networking infrastructure

In this task, we will create a virtual network, two application security groups, and network security groups. We will then associate the network security groups with the virtual network subnet.

The screenshot displays the Microsoft Azure portal interface. On the left, the 'myVirtualNetwork-1747165946166 | Overview' blade is open, showing deployment details for a virtual network. A red box highlights the title bar of this blade. Below the title, the deployment status is 'OK' for the 'myVirtualNetwork' resource. Another red box highlights the table containing this resource information.

Resource	Type	Status	Operation details
myVirtualNetwork	Virtual network	OK	Operation details

On the right, a task list titled 'Task 2: Create application security groups' is visible. It includes instructions for creating an application security group and a progress bar indicating '13% Tasks Complete'.

- 6. Back on the **IP addresses** tab of the **Create virtual network** blade, click **Review + create**.
- 7. On the **Review + create** tab of the **Create virtual network** blade, click **Create**.

Task 2: Create application security groups

In this task, you will create an application security group.

- 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Application security groups** and press the **Enter** key.
- 2. On the **Application security groups** blade, click **+ Create**.
- 3. On the **Basics** tab of the **Create an application security group** blade, specify the following

13% Tasks Complete

< Previous End >

We then create the web server and management server ASGs

The first screenshot shows the 'Create an application security group' blade in the Microsoft Azure portal. The 'Basics' tab is selected, and the 'Create' button is highlighted with a red box. The 'Summary' section shows the following details:

Summary	
Subscription	MOC Subscription-lod50572803
Resource group	AZ500LAB07
Location	East US
Name	myAsgWebServers

The second screenshot shows the 'myAsgMgmtServers' ASG page. The 'myAsgMgmtServers' name is highlighted with a red box. The 'Essentials' section shows the following details:

Essentials	
Resource group	(move) AZ500LAB07
Location	East US
Subscription	(move) MOC Subscription-lod50572803
Subscription ID	e0e29af2-ccfa-47e0-ba4f-bd1cf0826a3a
Tags	(edit) Add tags

We create the NSG.

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/18e8948f-bdf8-47c0-b001-013d04c7dceb

Create network security group - Microsoft Azure

https://portal.azure.com/#create/Microsoft.Network...

Microsoft Azure Search resources, services, and docs (G+)

Copilot

Validation passed

Basics Tags Review + create

Basics

Subscription	MOC Subscription-lod50572803
Resource group	AZ500LAB07
Region	East US
name	myNsg

Tags

None

Create < Previous Next > Download a template for automation

Network Security Groups and Application Security G... 55 Minutes Remaining

Instructions Resources Help 100%

Resource group AZ500LAB07

Name myNsg

Region East US

4. Click Review + create and then click Create.

5. In the Azure portal, navigate back to the Network security groups blade and click the myNsg entry.

6. On the myNsg blade, in the Settings section, click Subnets and then click + Associate.

7. On the Associate subnet blade, specify the following settings and click OK:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

26% Tasks Complete

< Previous End >

We associate the NSG created above to a subnet

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/18e8948f-bdf8-47c0-b001-013d04c7dceb

Associate subnet - Microsoft Azure

https://portal.azure.com/#@L0D5PRODMDCA.onmicr...

Microsoft Azure Search resources, services, and docs (G+)

Copilot

Home > myNsg

myNsg | Subnets

Network security group

+ Associate

Search subnets

Name

No results.

Virtual network myVirtualNetwork (AZ500LAB07)

Subnet default

OK

Network Security Groups and Application Security G... 46 Minutes Remaining

Instructions Resources Help 100%

Resource group AZ500LAB07

Name myNsg

Region East US

4. Click Review + create and then click Create.

5. In the Azure portal, navigate back to the Network security groups blade and click the myNsg entry.

6. On the myNsg blade, in the Settings section, click Subnets and then click + Associate.

7. On the Associate subnet blade, specify the following settings and click OK:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

32% Tasks Complete

< Previous End >

Inside our NSG, we create two inbound rule with management server and web server as their destinations on ports 80, and 443 for web server and 3389 for management server.

myNsg | Inbound security rules

Network security group

Filter by name

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

Priority	Name	Port	Protocol	Source
100	Allow-Web-All	80,443	TCP	Any
110	Allow-RDP-All	3389	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer

7. On the **Add inbound security rule** blade, click **Add** to create the new inbound rule.

Result: You have deployed a virtual network, network security with inbound security rules, and two application security groups.

Exercise 2: Deploy virtual machines and test network filters

Estimated timing: 25 minutes

In this exercise, you will complete the following tasks:

- Task 1: Create a virtual machine to use as a web server.
- Task 2: Create a virtual machine to use as a management server.

46% Tasks Complete

< Previous End >

Deploy virtual machines and test network filters

In this task, we will spin up two VMs: a web server and a management server, and then associate each machine's network interface with its application security.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual machines' blade is selected, displaying a table of virtual machines. A red box highlights the 'myVMgmt' and 'myVmWeb' VMs. On the right, a task pane titled 'Network Security Groups and Application Security Groups' is visible, showing instructions for associating VMs with ASGs. The task pane includes a progress bar and a '1 Minute Remaining' timer.

Name	Subscription	Resource Group	Location	Status
myVMgmt	MOC Subscripti...	AZ500LA807	East US	Running
myVmWeb	MOC Subscripti...	AZ500LA807	East US	Running

Task 3: Associate each virtual machines network interface to its application security group.

In this task, you will associate each virtual machines network interface with the corresponding application security group. The myVMWeb virtual machine interface will be associated to the myAsgWebServers ASG. The myVMgmt virtual machine interface will be associated to the myAsgMgmtServers ASG.

1. In the Azure portal, navigate back to the **Virtual machines** blade and verify that both virtual machines are listed with the **Running** status.
2. In the list of virtual machines, click the...

69% Tasks Complete

Associating the VMs with respective ASGs

The screenshot shows the Microsoft Azure portal interface. On the left, the 'myVMgmt' virtual machine blade is selected, displaying the 'Application security groups' section. A red box highlights the 'myAsgMgmtServers' ASG. On the right, a task pane titled 'Network Security Groups and Application Security Groups' is visible, showing instructions for testing network traffic filtering. The task pane includes a progress bar and a '1 Hr 2 Min Remaining' timer.

myVMgmt | Application security groups

Network interface / IP configuration

myvmgmt416 (primary) / ipconfig1 (primary)

Name	Resource group
myAsgMgmtServers	AZ500LA807

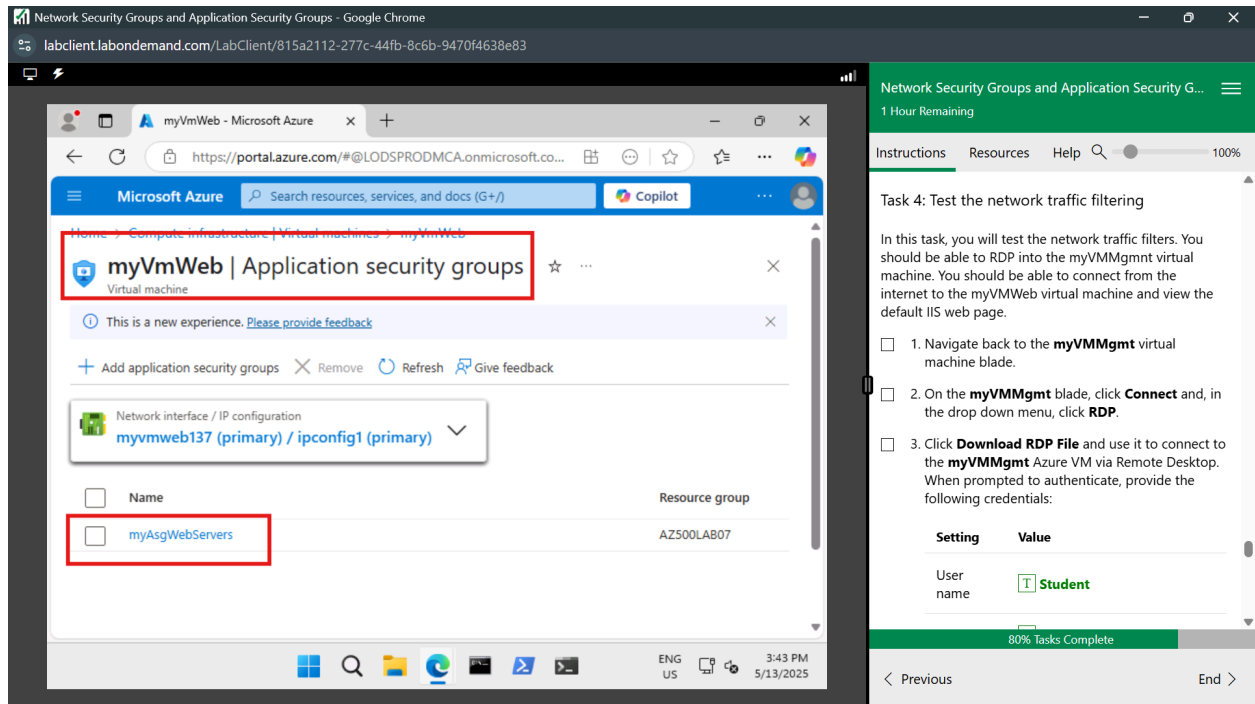
Task 4: Test the network traffic filtering

In this task, you will test the network traffic filters. You should be able to RDP into the myVMgmt virtual machine. You should be able to connect from the internet to the myVmWeb virtual machine and view the default IIS web page.

1. Navigate back to the **myVMgmt** virtual machine blade.
2. On the **myVMgmt** blade, click **Connect** and, in the drop down menu, click **RDP**.
3. Click **Download RDP File** and use it to connect to the **myVMgmt** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credentials:

Setting	Value
User name	T Student

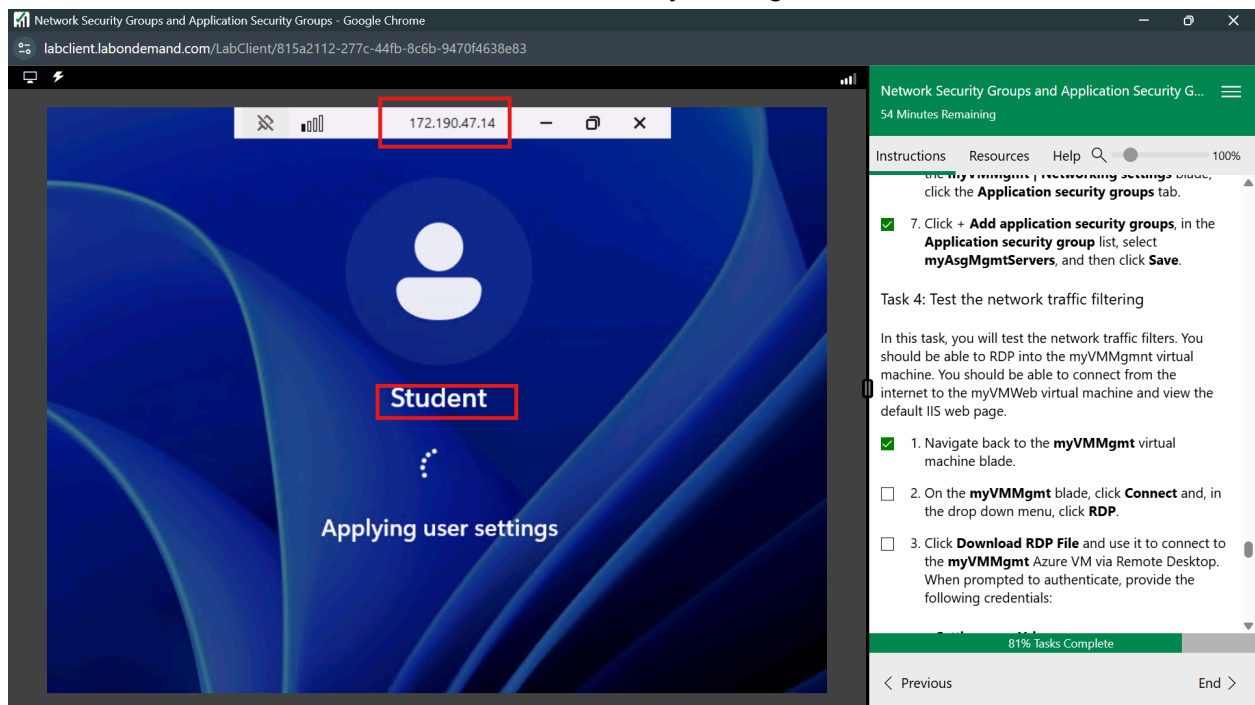
80% Tasks Complete



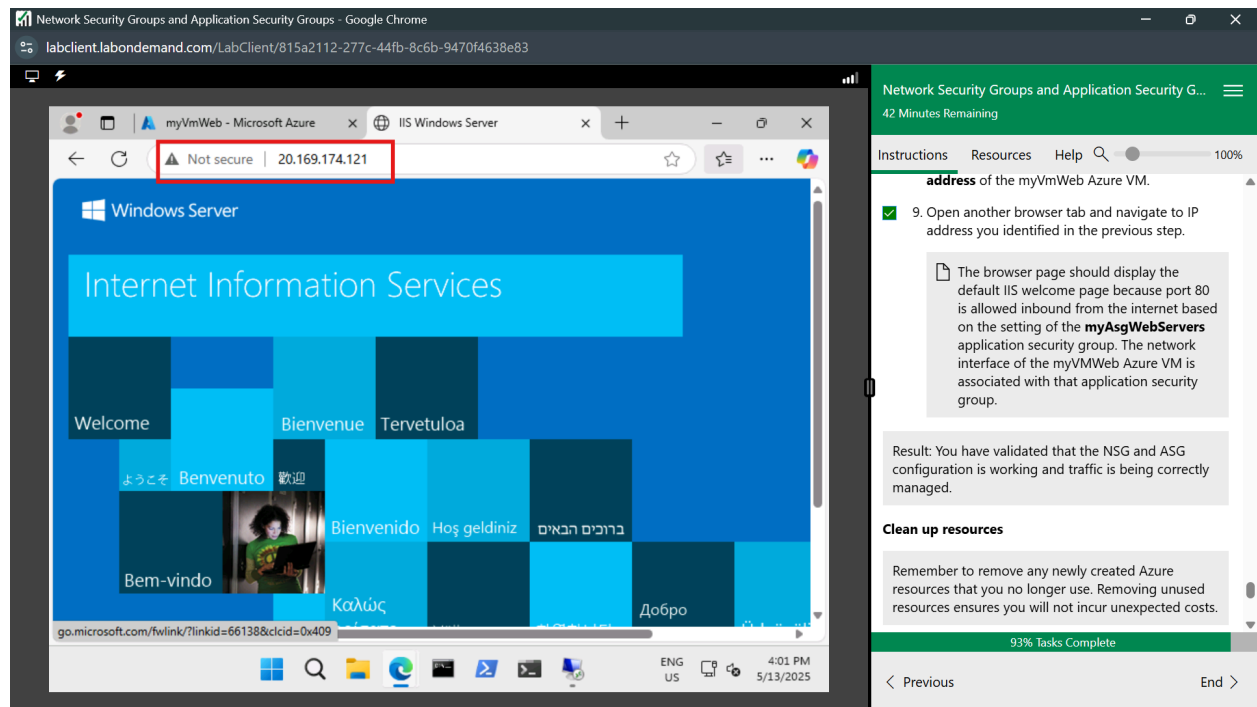
Test the network traffic filtering

In this task, we will test our configurations. We should be able to RDP into the myVMMgmt virtual machine. We should be able to connect from the internet to the myVMWeb virtual machine and view the default IIS web page.

The screenshot shows we were able to RDP into myVMMngt.



The following screenshot shows that we were able to install a web server and using its public IP to access its default IIS welcome page as shown.



Conclusion

To conclude, we have implemented the network security of Azure virtual networks using Application Security Groups and Network Security Groups attached to VMs and Subnets, respectively. We were able to demonstrate how the network traffic was filtered to avoid unwanted traffic.