

Course: Cloud and Network Security
Name: Neville Ngothe Iregi
Student No.: CS-CNS10-25054
Date: Tuesday, 11 November 2025

Week 8 Assignment 2: Network Security Groups and Application Security Groups

Introduction

A Network Security Group (NSG) is a decentralized, basic firewall that controls inbound and outbound traffic to Azure resources. It contains zero or multiple inbound and outbound security rules that enable one to filter traffic to and from cloud resources. They specify five-tuple information i.e source port, source IP, destination IP, destination port, and the protocol. NSG can be associated with either a subnet or individual network interfaces. They are also stateless; traffic must be explicitly given permission unless there is a setting to automatically handle the traffic by rules set.

ASGs are used within a NSG to apply a network security rule to a specific workload or group of VMs — defined by ASG worked as being the “network object” & explicit IP addresses are added to this object. This provides the capability to group VMs into associated groups or workloads, simplifying the NSG rule definition process. Another great use of this is for scalability, creating the virtual machine and assigning the newly created virtual machine to its ASG will provide it with all the NSG rules in place for that specific ASG

Lab scenario

You have been asked to implement your organization's virtual networking infrastructure and test to ensure it is working correctly. In particular:

- The organization has two groups of servers: Web Servers and Management Servers.
- Each group of servers should be in its own Application Security Group.
- You should be able to RDP into the Management Servers, but not the Web Servers.
- The Web Servers should display the IIS web page when accessed from the internet.
- Network security group rules should be used to control network access.

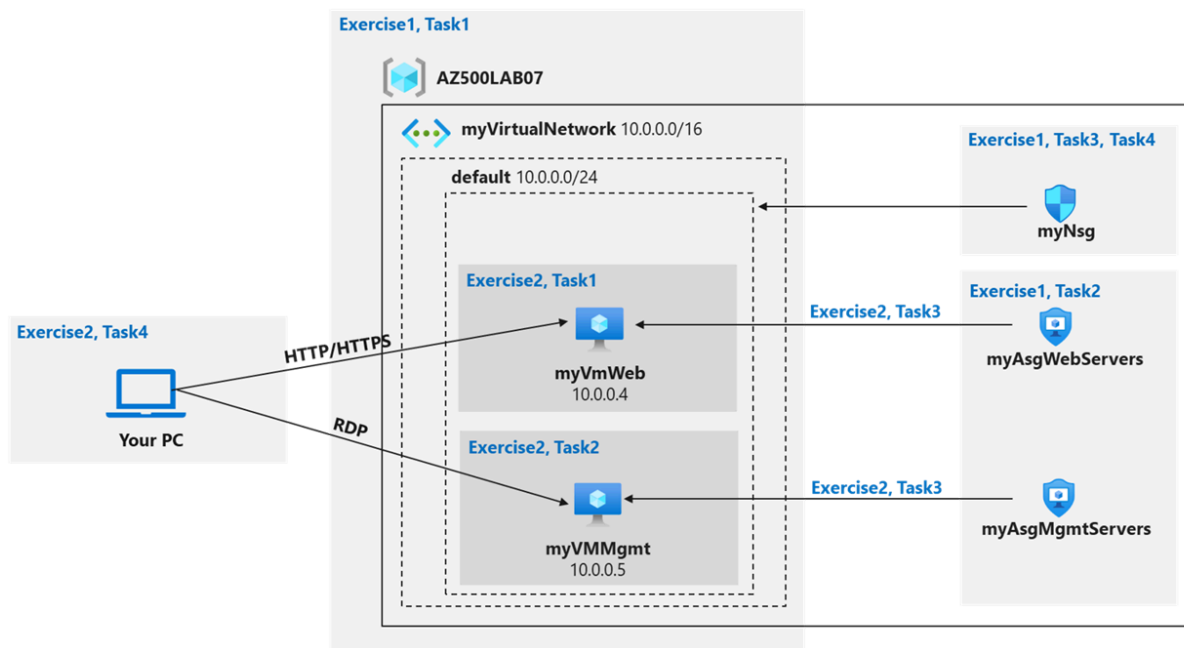
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Lab objectives

In this lab, you will complete the following exercises:

- Exercise 1: Create the virtual networking infrastructure
- Exercise 2: Deploy virtual machines and test the network filters

Network and Application Security Groups diagram



Instructions

Exercise 1: Create the virtual networking infrastructure

Estimated timing: 20 minutes

For all the resources in this lab, we are using the **East (US)** region. Verify with your instructor this is the region to use for your class.

In this exercise, you will complete the following tasks:

- Task 1: Create a virtual network with one subnet.
- Task 2: Create two application security groups.
- Task 3: Create a network security group and associate it with the virtual network subnet.
- Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the management servers.

Task 1: Create a virtual network

A Virtual Network is the fundamental building block for private communications in Azure and it enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks

In this task, you will create a virtual network to use with the network and application security groups.

1. Sign-in to the Azure portal <https://portal.azure.com/>.
Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab. In this **Cloudslice** lab, this account is LabUser-57057525@LODSPRODMCA.onmicrosoft.com with TAP @E46\$BH4.
2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type Virtual networks and press the **Enter** key.
3. On the **Virtual networks** blade, click **+ Create**.
4. On the **Basics** tab of the **Create virtual network** blade, specify the following settings (leave others with their default values) and click **Next: IP Addresses**:

Setting	Value
Subscription	Name of the Azure subscription you are using in this lab
Resource group	Use the provided Resource Group named AZ500LAB07
Name	myVirtualNetwork
Region	East US

5. On the **IP addresses** tab of the **Create virtual network** blade, set the **IPv4 address space** to **10.0.0.0/16**, and, if needed, in the **Subnet name** column, click **default**, on the **Edit subnet** blade, specify the following settings and click **Save**:

Setting	Value
Subnet name	default
Subnet address range	10.0.0.0/24

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

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

Create virtual network - Microsoft Azure

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

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

Validation passed

Basics Security IP addresses Tags Review + create

View automation template

Basics

Subscription MOC Subscription-Iod51697973

Resource Group AZ500LAB07

Name myVirtualNetwork

Region East US

Security

Previous Next Create Download a template for automation Give feedback

Network Security Groups and Application Security Groups

Instructions Resources

needed, in the Subnet name column, click default, on the Edit subnet blade, specify the following settings and click Save:

Setting	Value
Subnet name	default
Subnet address range	10.0.0.0/24

6. Back on the IP addresses tab of the Create virtual network screen, click Review + create.

7. On the Review + create tab of the Create virtual network screen, click Create.

Task 2: Create application security groups

Previous End

1 Hr 4 Min Remaining

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

myVirtualNetwork-1764150085770

Deployment

Deployment succeeded

Deployment 'myVirtualNetwork-1764150085770' to resource group 'AZ500LAB07' was successful.

Go to resource Pin to dashboard

Deployment is in progress

Deployment name : myVirtualNetwork-1764150085770

Subscription : MOC Subscription-Iod51697973

Resource group : AZ500LAB07

Start time : 11/26/2025, 1:41:21 AM

Correlation ID : 01876d63-149f-48c9-99c7-74ac1ad1363e

Deployment details

Resource	Type	St.
myVirtualNetwork-1764150085770	Microsoft.Network.VirtualNetwork	Created

Network Security Groups and Application Security Groups

Instructions Resources

needed, in the Subnet name column, click default, on the Edit subnet blade, specify the following settings and click Save:

Setting	Value
Subnet name	default
Subnet address range	10.0.0.0/24

6. Back on the IP addresses tab of the Create virtual network screen, click Review + create.

7. On the Review + create tab of the Create virtual network screen, click Create.

Task 2: Create application security groups

Previous End

1 Hr 3 Min Remaining

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 settings:

Setting	Value
Resource group	AZ500LAB07
Name	myAsgWebServers
Region	East US

4.
This group will be for the web servers.
5. Click **Review + create** and then click **Create**.
6. Navigate back to the **Application security groups** blade and click **+ Create**.
7. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB07
Name	myAsgMgmtServers
Region	East US

8.

This group will be for the management servers.

9. Click **Review + create** and then click **Create**.

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

Create an application security group

Validation passed

Basics Tags Review + create

Basics

Subscription MOC Subscription-lod51697973

Resource group AZ500LAB07

Location East US

Name myAsgWebServers

Create

Previous Next > Download a template for auto

Wednesday, November 26, 2025

Wed 1:44 AM (Local time)

What is the difference between application security group and service tag in Azure?

Network Security Groups and Application Security Groups

Instructions Resources

Resource group AZ500LAB07

Name myAsgWebServers

Region East US

This group will be for the web servers.

4. Click **Review + create** and then click **Create**.

5. Navigate back to the **Application security groups** blade and click **+ Create**.

6. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:

Previous End

1 Hour Remaining

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

CreateApplicationSecurityGroupBladeViewModel

Deployment

Deployment succeeded

Deployment 'CreateApplicationSecurityGroupBladeViewModel' to resource group 'AZ500LAB07' was successful.

Go to resource Go to resource group

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name : CreateApplicationSecurityGroupBladeViewModel

Subscription : MOC Subscription-lod51697973

Resource group : AZ500LAB07

Start time : 11/26/2025, 1:45:04 AM

Correlation ID : 1c6c15a2-fdd1-4f57-a996-05e9d51945dd

Deployment details

Next steps

Go to resource

Add or remove favorites by pressing Ctrl+Shift+F

Network Security Groups and Application Security Groups

Instructions Resources

Resource group AZ500LAB07

Name myAsgWebServers

Region East US

This group will be for the web servers.

4. Click **Review + create** and then click **Create**.

5. Navigate back to the **Application security groups** blade and click **+ Create**.

6. On the **Basics** tab of the **Create an application security group** blade, specify the following settings:

Previous End

59 Minutes Remaining

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

CreateApplicationSecurityGroupBladeViewModel

Deployment

Deployment succeeded

Deployment 'CreateApplicationSecurityGroupBladeViewModel' to resource group 'AZ500LAB07' was successful.

Go to resource Go to resource group

Your deployment is complete

Deployment name : CreateApplicationSecurityGroupBladeViewModel

Subscription : MOC Subscription-Iod51697973

Resource group : AZ500LAB07

Start time : 11/26/2025, 1:46:49 AM

Correlation ID : e9951113-a51f-48f3-b992-815a1ce12066

Deployment details

Next steps

Go to resource

Network Security Groups and Application Security Groups

Instructions Resources

Setting	Value
Resource group	AZ500LAB07
Name	myAsgMgmtServers
Region	East US

This group will be for the management servers.

7. Click **Review + create** and then click **Create**.

Task 3: Create a network security group and associate the NSG to the subnet

Previous End

57 Minutes Remaining

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

Network foundation - Microsoft

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security groups

Application security groups

Bastions

Route tables

Route servers

You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field...

Subscription equals all Resource Group equals all

Location equals all Add filter

Name	Network interf...	Virtual netwo
myAsgMgmtServers	0	-
myAsgWebServers	0	-

Network Security Groups and Application Security Groups

Instructions Resources

Setting	Value
Resource group	AZ500LAB07
Name	myAsgMgmtServers
Region	East US

This group will be for the management servers.

7. Click **Review + create** and then click **Create**.

Task 3: Create a network security group and associate the NSG to the subnet

Previous End

57 Minutes Remaining

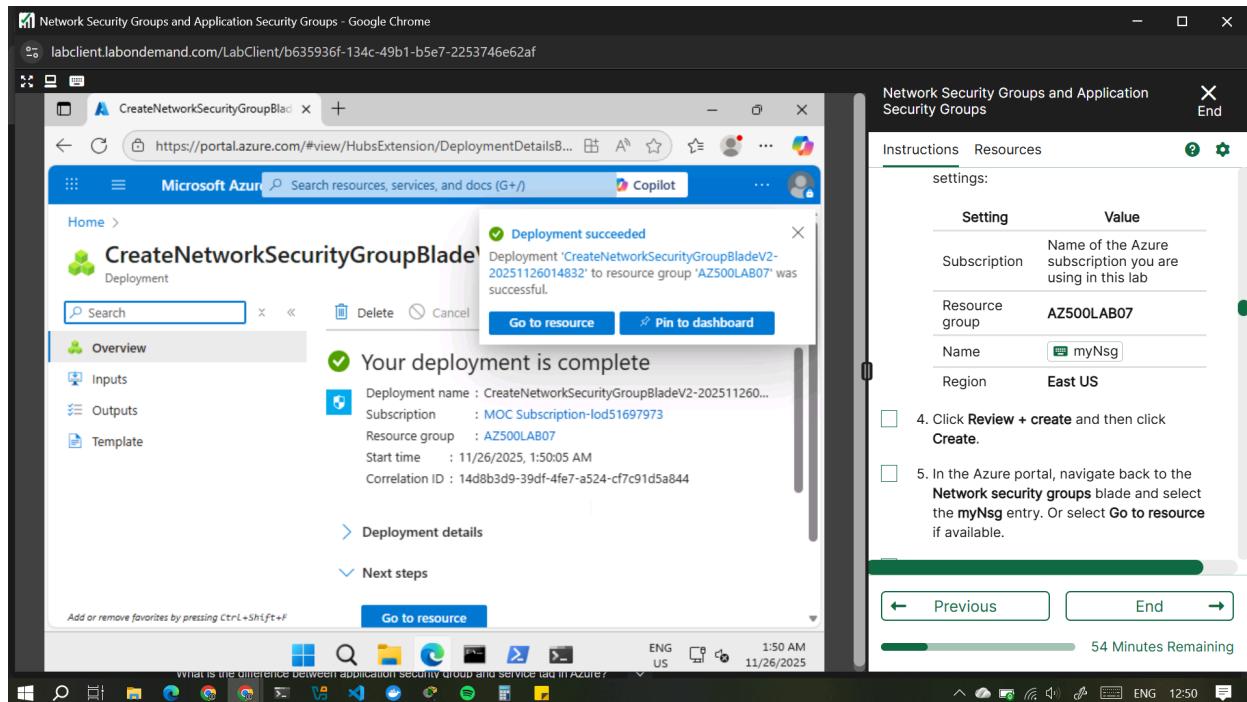
Task 3: Create a network security group and associate the NSG to the subnet

In this task, you will create a network 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 Network security groups and press the **Enter** key.
2. On the **Network security groups** blade, click **+ Create**.
3. On the **Basics** tab of the **Create network security group** blade, specify the following settings:

Setting	Value
Subscription	Name of the Azure subscription you are using in this lab
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 select the **myNsg** entry. Or select **Go to resource** if available.
6. On the **myNsg** blade, in the **Settings** section, click **Subnets** and then select **+ Associate**.
7. On the **Associate subnet** blade, specify the following settings and select **OK**:

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

Associate subnet - Microsoft Azure

myNsg | Subnet

Virtual network: myVirtualNetwork (AZ500LAB07)

Subnet: default

OK

Network Security Groups and Application Security Groups

Instructions Resources

Network security groups blade and select the myNsg entry. Or select Go to resource if available.

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

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

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the servers.

Previous End

53 Minutes Remaining

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e62af

myNsg | Subnets

Saving subnet

Successfully saved network security group for subnet 'default'.

Name	Address range	Virtual network
default	10.0.0.0/24	myVirtualNetwork

Give feedback

Network Security Groups and Application Security Groups

Instructions Resources

Network security groups blade and select the myNsg entry. Or select Go to resource if available.

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

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

Setting	Value
Virtual network	myVirtualNetwork
Subnet	default

Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the servers.

Previous End

52 Minutes Remaining

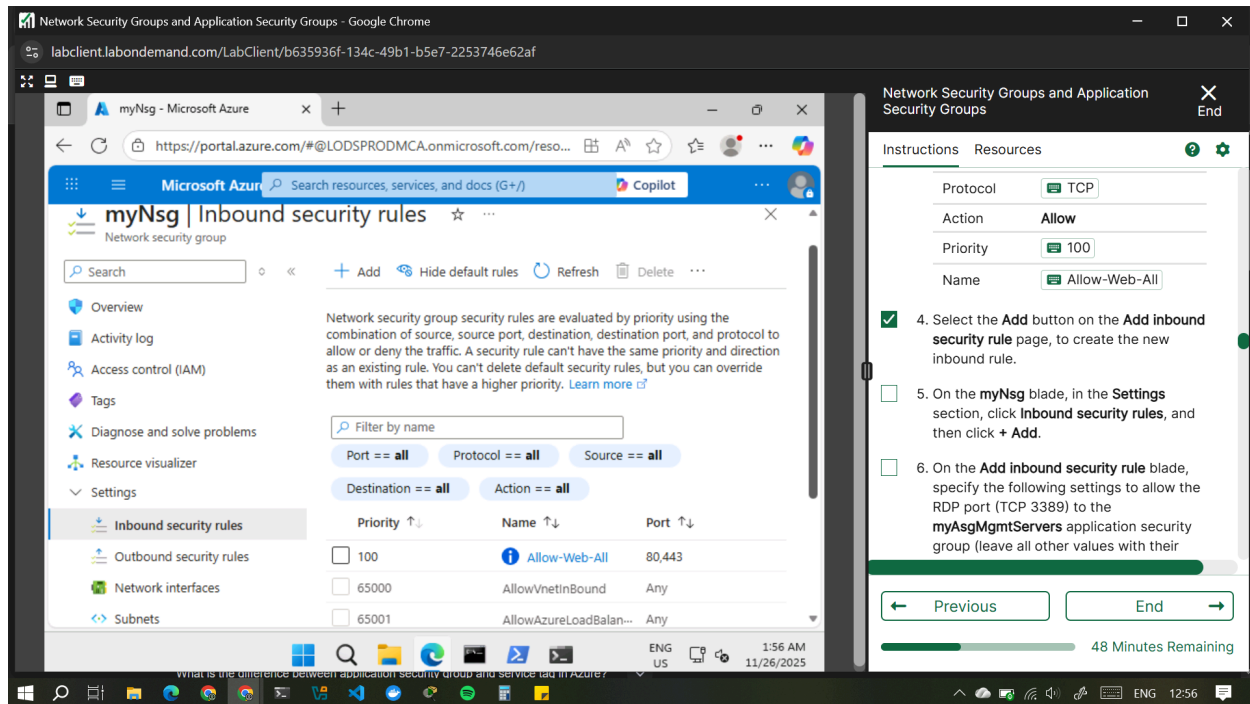
Task 4: Create inbound NSG security rules to all traffic to web servers and RDP to the servers.

1. On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**.

-
2. Review the default inbound security rules and then click **+ Add**.
 3. On the **Add inbound security rule** blade, specify the following settings to allow TCP ports 80 and 443 to the **myAsgWebServers** application security group (leave all other values with their default values):

Setting	Value
Source	Any
Source port ranges	*
Destination	in the drop-down list, select Application security group and then click myAsgWebServers
Service	Custom
Destination port ranges	80,443
Protocol	TCP
Action	Allow
Priority	100
Name	Allow-Web-All

4. Select the **Add** button on the **Add inbound security rule** page, to create the new inbound rule.



5. On the **myNsg** blade, in the **Settings** section, click **Inbound security rules**, and then click **+ Add**.
6. On the **Add inbound security rule** blade, specify the following settings to allow the RDP port (TCP 3389) to the **myAsgMgmtServers** application security group (leave all other values with their default values):

Setting	Value
Source	Any
Source port ranges	*
Destination	in the drop-down list, select Application security group and then click myAsgMgmtServers
Service	Custom

Destination port ranges 3389

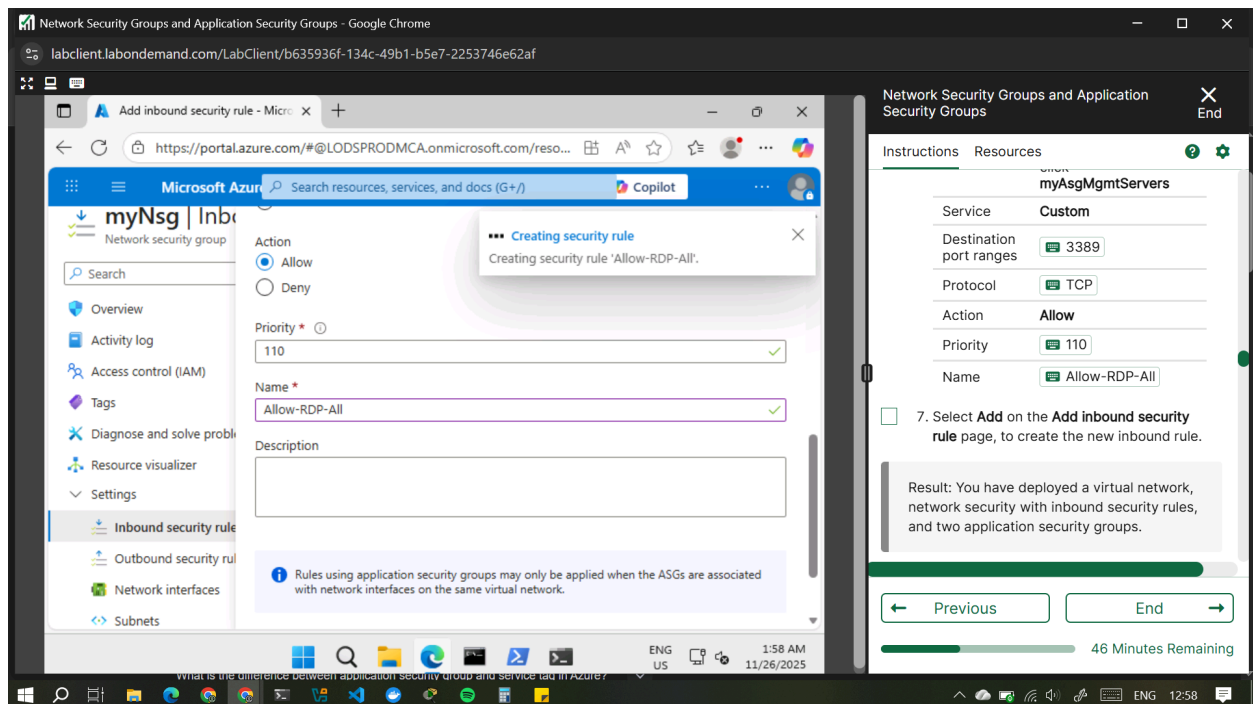
Protocol TCP

Action **Allow**

Priority 110

Name Allow-RDP-All

7. Select **Add** on the **Add inbound security rule** page, 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.
- Task 3: Associate each virtual machines network interface to it's application security group.
- Task 4: Test the network traffic filtering.

Task 1: Create a virtual machine to use as a web server

In this task, you will create a virtual machine to use as a web server.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type Virtual machines and press the **Enter** key.
2. On the **Virtual machines** blade, click **+ Create** and, in the dropdown list, click **Virtual machine**.
3. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you will be using in this lab
Resource group	AZ500LAB07
Virtual machine name	myVmWeb

Region	(US)East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2022 Datacenter: Azure Edition- x64 Gen2
Size	Standard D2s v3
Username	Student
Password	Please create your own password and record it for future reference in subsequent labs
Confirm password	Retype your password
Public inbound ports	None
Would you like to use an existing Windows Server License	No

4.

For public inbound ports, we will rely on the precreated NSG.

5. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.
6. On the **Networking** tab of the **Create a virtual machine** blade, select the previously created network **myVirtualNetwork** and the **default (10.0.0.0/24)** subnet.
7. Under **NIC network security group** select **None**.

8. Click **Next: Management >**, then click **Next: Monitoring >**. On the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:

Setting	Value
Boot diagnostics	Enabled with managed storage account (recommended)

9. Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create**.

The screenshot shows the Microsoft Azure portal interface. The main content area displays a deployment summary for 'CreateVm-MicrosoftWindowsServer.WindowsServer...'. The deployment is marked as complete with a green checkmark. Key details include: Subscription: MOC Subscription-lod51697973, Resource group: AZ500LAB07, Start time: 11/26/2025, 2:18:34 AM, and Correlation ID: 776f34cb-5453-4e63-8c24-c127d7a09cd8. Below the summary, there are sections for 'Deployment details' and 'Next steps', which include links for 'Setup auto-shutdown' and 'Monitor VM health, performance and network dependencies'.

On the right side, a task instruction panel titled 'Network Security Groups and Application Security Groups' is visible. It contains a list of instructions:

- 7. In the Azure portal, navigate back to the myVMWeb blade.
- 8. On the myVMWeb blade, identify the Public IP address of the myVmWeb Azure VM.
- 9. Open another browser tab and navigate to IP address you identified in the previous step.

A callout box provides additional context: 'The browser page should display the default IIS welcome page because port 80 is allowed inbound from the internet based on the setting of the myAsgWebServers application security group. The network security group...'.

The screenshot shows the Microsoft Azure portal interface, specifically the 'Virtual machines' blade. The left sidebar shows the navigation menu with 'Virtual machines' selected. The main content area displays a list of virtual machines. A table shows the following information:

Name	Subscription	Resource Gro
myVmWeb	MOC Subscripti...	AZ500LAB07

Below the table, it indicates 'Showing 1 - 1 of 1. Display count: auto'. A 'Give feedback' link is also present.

On the right side, a task instruction panel titled 'Network Security Groups and Application Security Groups' is visible. It contains a list of instructions:

- 1. In the Azure portal, navigate back to the Virtual machines blade, click + Create, and, in the dropdown list, click Virtual machine.
- 2. On the Basics tab of the Create a virtual machine blade, specify the following settings (leave others with their default values):

A table with 'Setting' and 'Value' columns is partially visible, showing the name of the VM.

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

In this task, you will create a virtual machine to use as a management server.

-
1. In the Azure portal, navigate back to the **Virtual machines** blade, click **+** **Create**, and, in the dropdown list, click **Virtual machine**.
 2. On the **Basics** tab of the **Create a virtual machine** blade, specify the following settings (leave others with their default values):

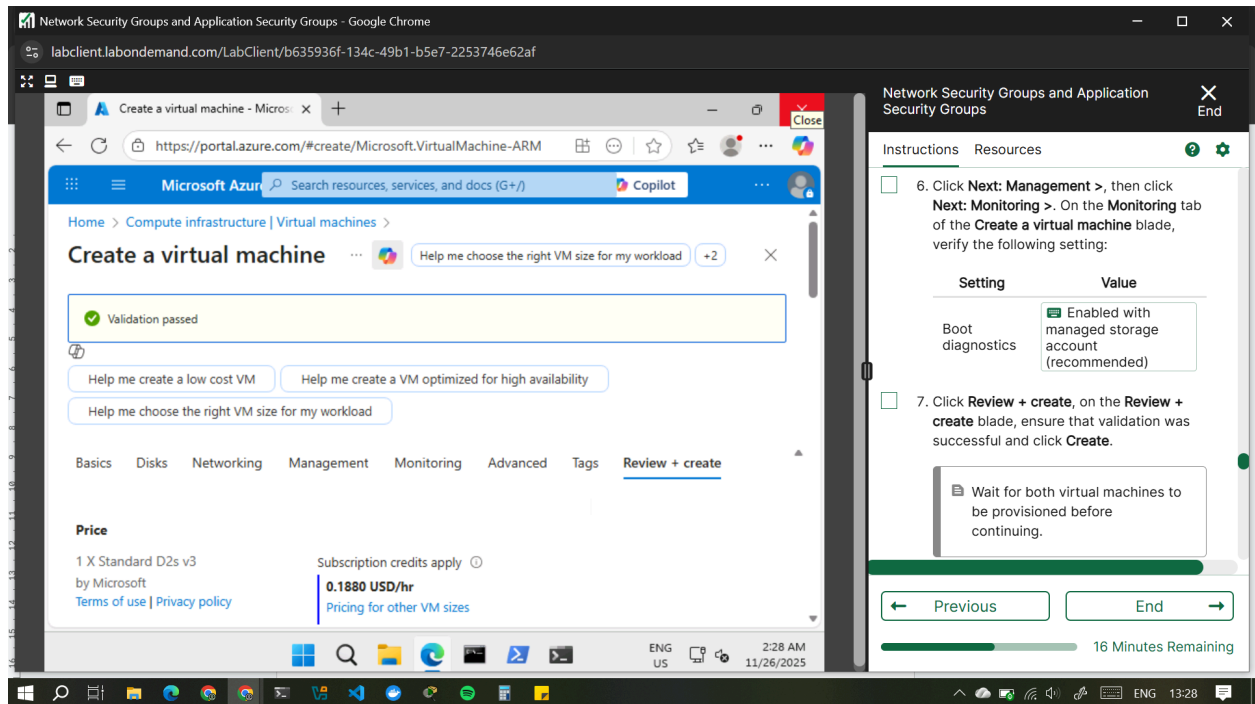
Setting	Value
Subscription	the name of the Azure subscription you will be using in this lab
Resource group	AZ500LAB07
Virtual machine name	myVMMgmt
Region	(US)East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2022 Datacenter: Azure Edition - x64 Gen2
Size	Standard D2s v3
Username	Student
Password	Please use your personal password created in Lab 02 > Exercise 2 > Task 1 > Step 3.
Public inbound ports	None

Already have a Windows Server license No

3.
For public inbound ports, we will rely on the precreated NSG.
4. Click **Next: Disks >** and, on the **Disks** tab of the **Create a virtual machine** blade, set the **OS disk type** to **Standard HDD** and click **Next: Networking >**.
5. On the **Networking** tab of the **Create a virtual machine** blade, select the previously created network **myVirtualNetwork** and the **default (10.0.0.0/24)** subnet.
6. Under **NIC network security group** select **None**.
7. Click **Next: Management >**, then click **Next: Monitoring >**. On the **Monitoring** tab of the **Create a virtual machine** blade, verify the following setting:

Setting	Value
Boot diagnostics	Enabled with managed storage account (recommended)

8. Click **Review + create**, on the **Review + create** blade, ensure that validation was successful and click **Create**.

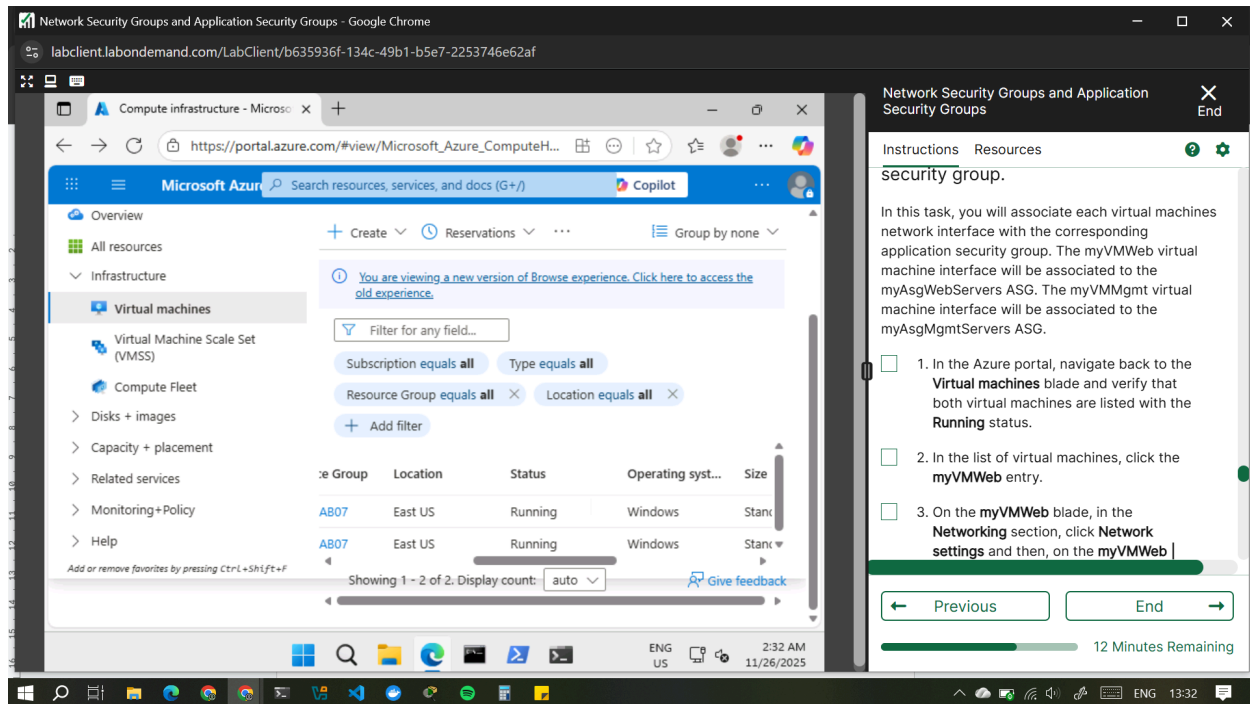


Wait for both virtual machines to be provisioned before continuing.

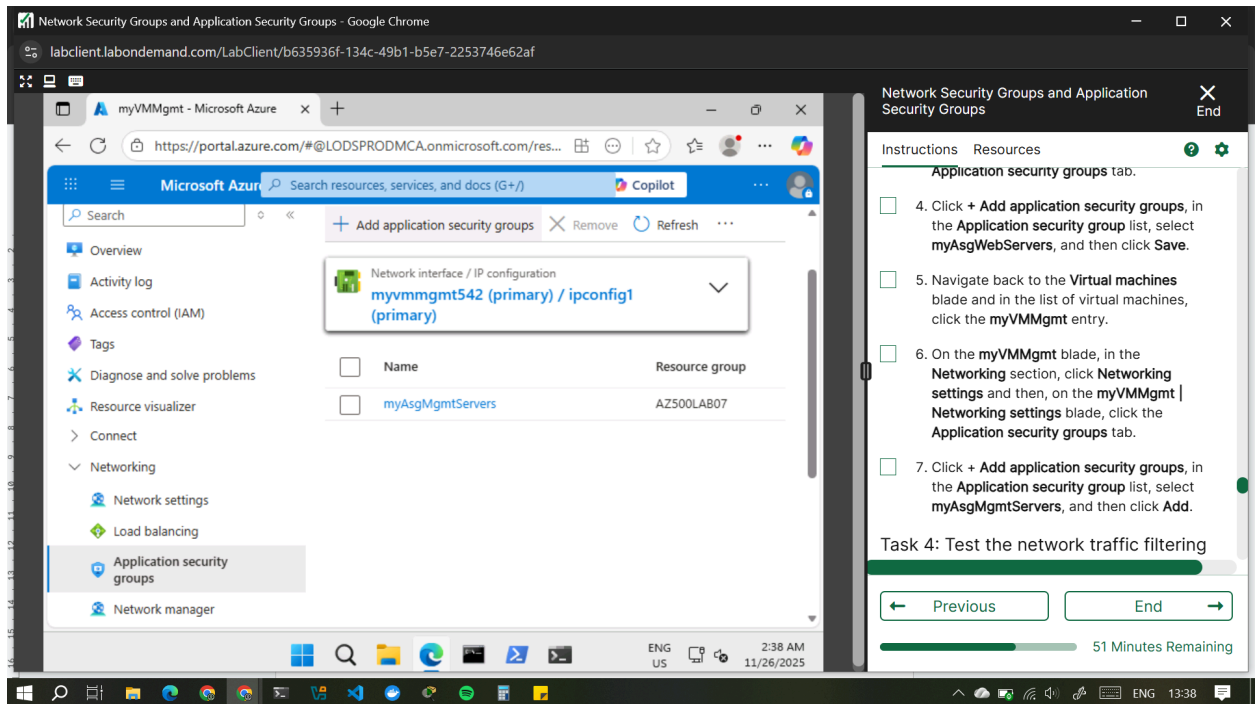
Task 3: Associate each virtual machine's network interface to its application security group.

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 myVMMgmt 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 **myVMWeb** entry.
3. On the **myVMWeb** blade, in the **Networking** section, click **Network settings** and then, on the **myVMWeb | Networking settings** blade, click the **Application security groups** tab.
4. Click **+ Add application security groups**, in the **Application security group** list, select **myAsgWebServers**, and then click **Save**.
5. Navigate back to the **Virtual machines** blade and in the list of virtual machines, click the **myVMMgmt** entry.
6. On the **myVMMgmt** blade, in the **Networking** section, click **Networking settings** and then, on the **myVMMgmt | Networking settings** blade, click the **Application security groups** tab.
7. Click **+ Add application security groups**, in the **Application security group** list, select **myAsgMgmtServers**, and then click **Add**.



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 myVMMgmt virtual machine. You should be able to connect from the internet to the myVMWeb virtual machine and view the default IIS web page.

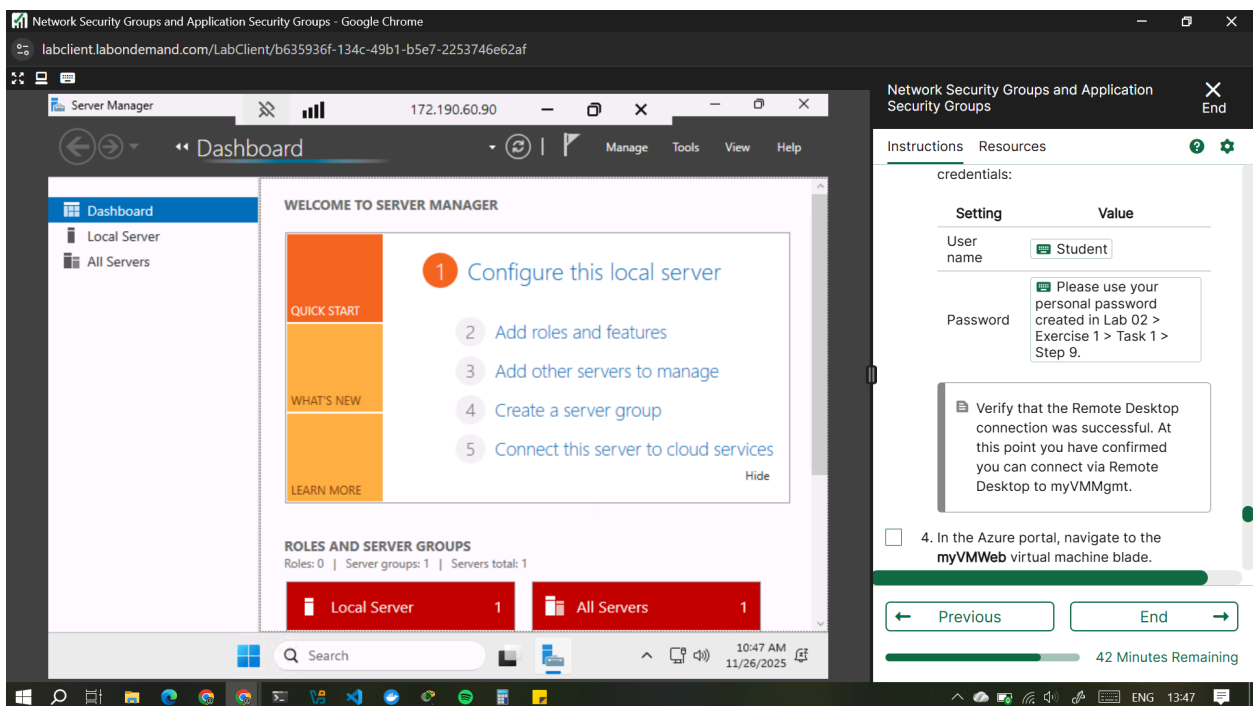
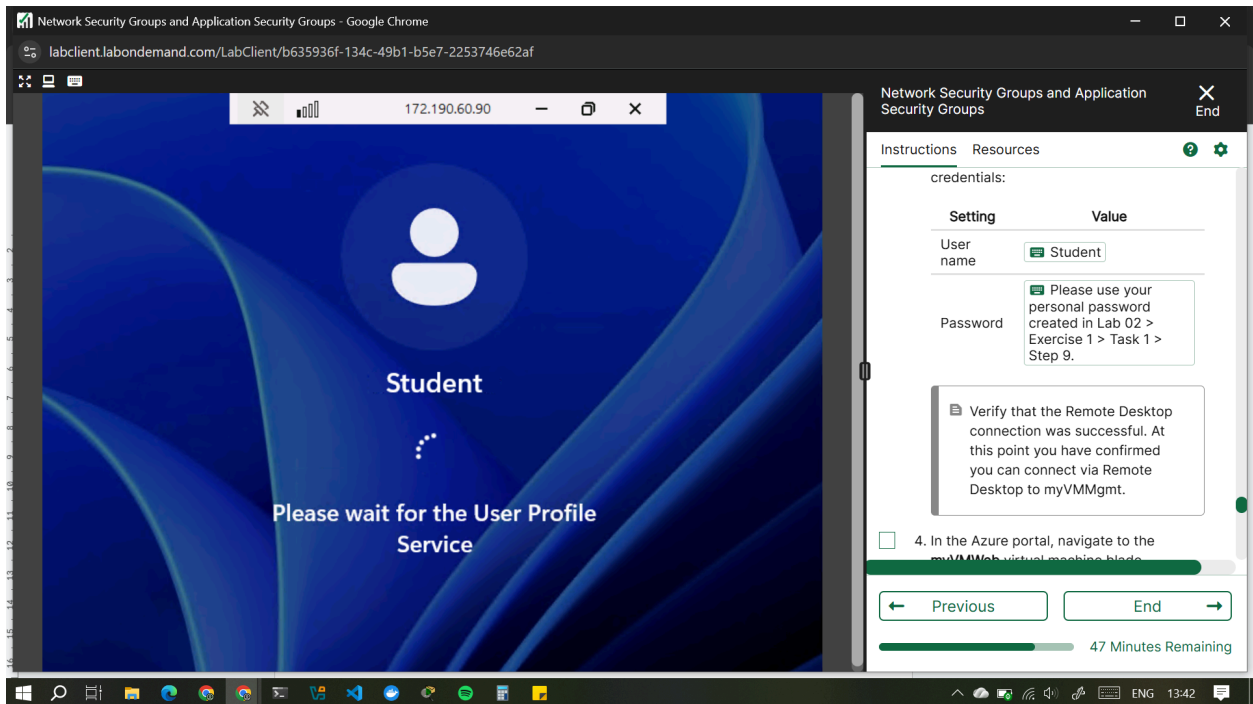
1. Navigate back to the **myVMMgmt** virtual machine blade.
2. On the **myVMMgmt** Overview blade, click **Connect** and, in the drop down menu, click **Connect**.
3. Download the RDP file and use it to connect to the **myVMMgmt** Azure VM via Remote Desktop. When prompted to authenticate, provide the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

Setting	Value
---------	-------

User name	Student
-----------	---------

Password Please use your personal password created in Lab 02 >
Exercise 1 > Task 1 > Step 9.

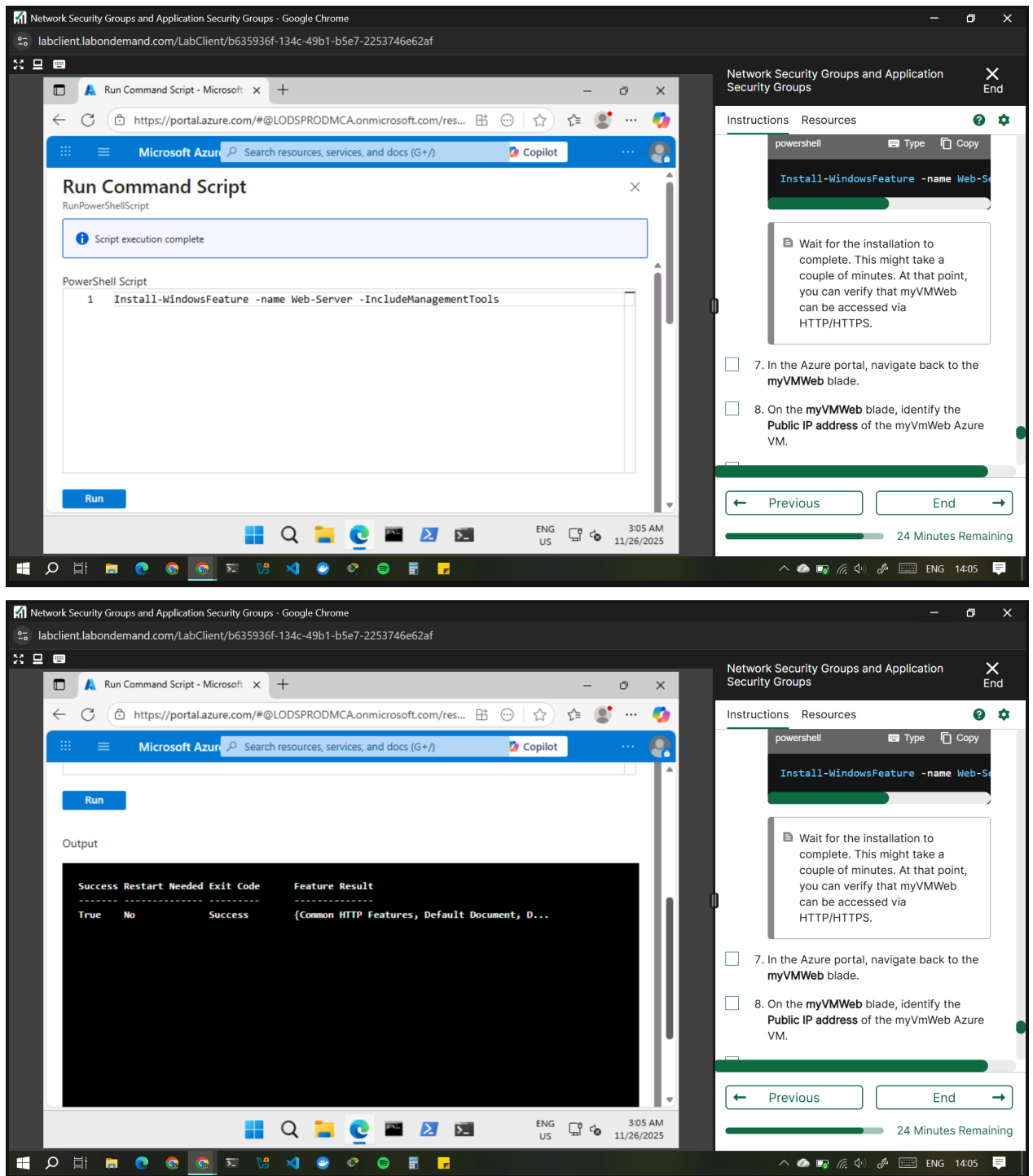
4. Verify that the Remote Desktop connection was successful. At this point you have confirmed you can connect via Remote Desktop to myVMMgmt.



5. In the Azure portal, navigate to the **myVMWeb** virtual machine blade.
6. On the **myVMWeb** blade, in the **Operations** section, click **Run command** and then click **RunPowerShellScript**.

-
7. On the **Run Command Script** pane, run the following to install the Web server role on **myVmWeb**:

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



8. Wait for the installation to complete. This might take a couple of minutes. At that point, you can verify that myVMWeb can be accessed via HTTP/HTTPS.
9. In the Azure portal, navigate back to the **myVMWeb** blade.

10. On the **myVMWeb** blade, identify the **Public IP address** of the myVmWeb Azure VM.

11. Open another browser tab and navigate to IP address you identified in the previous step.

The browser page should display the default IIS welcome page because port 80 is allowed inbound from the internet based on the setting of the **myAsgWebServers** application security group. The network interface of the myVMWeb Azure VM is associated with that application security group.

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e2af

myVmWeb - Microsoft Azure

https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.co...

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

Network settings Location East US

Load balancing Subscription (move) MOC Subscription-lod51697973

Application security groups Subscription ID eef4cd23-9a23-4741-8561-d6b6663a34db

Network manager Operating system Windows (Windows Server 2025 Datacenter Azure Edition)

Settings Size Standard D2s v3 (2 vcpus, 8 GiB memory)

Availability + scale Primary NIC public IP 40.71.206.44

Security 1 associated public IPs

Backup + disaster recovery Virtual network/subnet myVirtualNetwork/default

Operations Auto-shutdown DNS name Not configured

Run command Health state

Updates

Health monitoring

Instructions Resources

Install-WindowsFeature -name Web-S

Wait for the installation to complete. This might take a couple of minutes. At that point, you can verify that myVmWeb can be accessed via HTTP/HTTPS.

7. In the Azure portal, navigate back to the myVmWeb blade.

8. On the myVmWeb blade, identify the Public IP address of the myVmWeb Azure VM.

9. Open another browser tab and navigate to IP address you identified in the previous

Previous End

23 Minutes Remaining

Network Security Groups and Application Security Groups - Google Chrome

labclient.labondemand.com/LabClient/b635936f-134c-49b1-b5e7-2253746e2af

myVmWeb - Microsoft Azure

IIS Windows Server

Not secure 40.71.206.44

Windows Server

Internet Information Services

Welcome Bienvenue Tervetuloa

ようこそ Benvenuto 歡迎

Bienvenido Hoş geldiniz ברוכים הבאים

Bem-vindo Καλώς Добро

go.microsoft.com/fwlink/?linkid=66138&clcid=0x409

Instructions Resources

Public IP address of the myVmWeb Azure VM.

9. Open another browser tab and navigate to IP address you identified in the previous step.

The browser page should display the default IIS welcome page because port 80 is allowed inbound from the internet based on the setting of the myAsgWebServers application security group. The network interface of the myVmWeb Azure VM is associated with that application security group.

Result: You have validated that the NSG and

Previous End

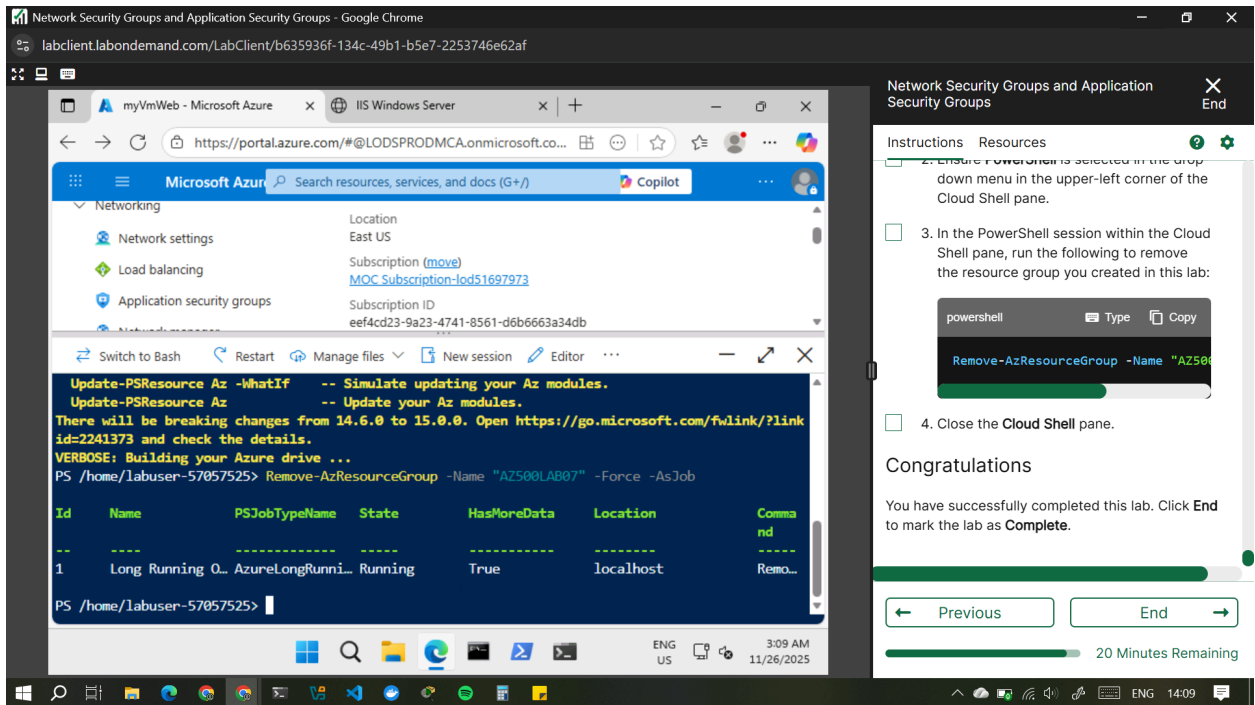
22 Minutes Remaining

Result: You have validated that the NSG and ASG configuration is working and traffic is being correctly managed.

Clean up resources

Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

1. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell** and **No storage account required**, select the name of your subscription, and then select **Apply**.
2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.
3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:
4. 
5. `Remove-AzResourceGroup -Name "AZ500LAB07" -Force -AsJob`
6. Close the **Cloud Shell** pane.



The screenshot shows the Azure Portal interface. On the left, the 'Network Security Groups and Application Security Groups' page is visible, showing a list of resources. The main pane displays the Cloud Shell session, which is running PowerShell. The session output shows the command `Remove-AzResourceGroup -Name "AZ500LAB07" -Force -AsJob` being executed. The right pane shows the 'Instructions' section for the lab, which includes steps 2, 3, and 4. Step 3 is highlighted, showing the command `Remove-AzResourceGroup -Name "AZ500LAB07" -Force -AsJob`. The 'Congratulations' section at the bottom of the right pane indicates that the lab has been successfully completed and provides a progress bar showing 20 minutes remaining.

Conclusion

In this lab, I successfully designed, deployed, and tested a secure virtual networking environment in Azure using **Network Security Groups (NSGs)** and **Application Security Groups (ASGs)**. By creating a virtual network, defining ASGs for workload-based grouping, and applying NSG rules at the subnet level, I demonstrated how Azure enables granular control over inbound and outbound traffic. The deployment of two virtual machines—one acting as a web server and the other as a management server—allowed me to validate the effectiveness of the configured security rules.

I confirmed that **RDP access** was only permitted to the management server through the ASG-based filtering and that the **web server** was safely exposed to the internet through ports **80 and 443**. The successful display of the IIS welcome page verified correct configuration of web traffic rules. This exercise highlighted the importance of segmentation, least-privilege network access, and scalable security management in cloud environments. Overall, the lab demonstrated how NSGs and ASGs work together to provide structured, efficient, and secure network traffic control within Azure.