Microsoft ADC Cybersecurity Skilling Program

Week 7 Assignment 13 LAB

Student Name: DEBORAH BINYANYA NYATICHI

Student ID: ADC-CSS02-25051

Introduction

In this lab, we explore the configuration and functionality of Azure Firewall, a cloud-native and intelligent network security service that protects Azure Virtual Network resources. This lab is designed as part of the AZ-500: Microsoft Azure Security Technologies course, and it focuses on equipping learners with hands-on experience in deploying and managing Azure Firewall to control both inbound and outbound traffic through defined rules and routing. Throughout the lab, we will deploy a pre-configured environment using an ARM template, then proceed to set up an Azure Firewall to enforce security controls. Key tasks include creating default routes, configuring application and network rules, specifying custom DNS settings, and validating the firewall's effectiveness through comprehensive testing. These tasks demonstrate how Azure Firewall integrates with other Azure services to provide centralized traffic inspection and threat intelligence-based filtering, which are essential in safeguarding cloud environments against modern security threats.This lab not only reinforces theoretical knowledge but also provides practical skills needed for securing Azure networks in real-world scenarios.

Tasks Completed

Required Lab Setup

Hello Deborah, on SEA-Dev click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.

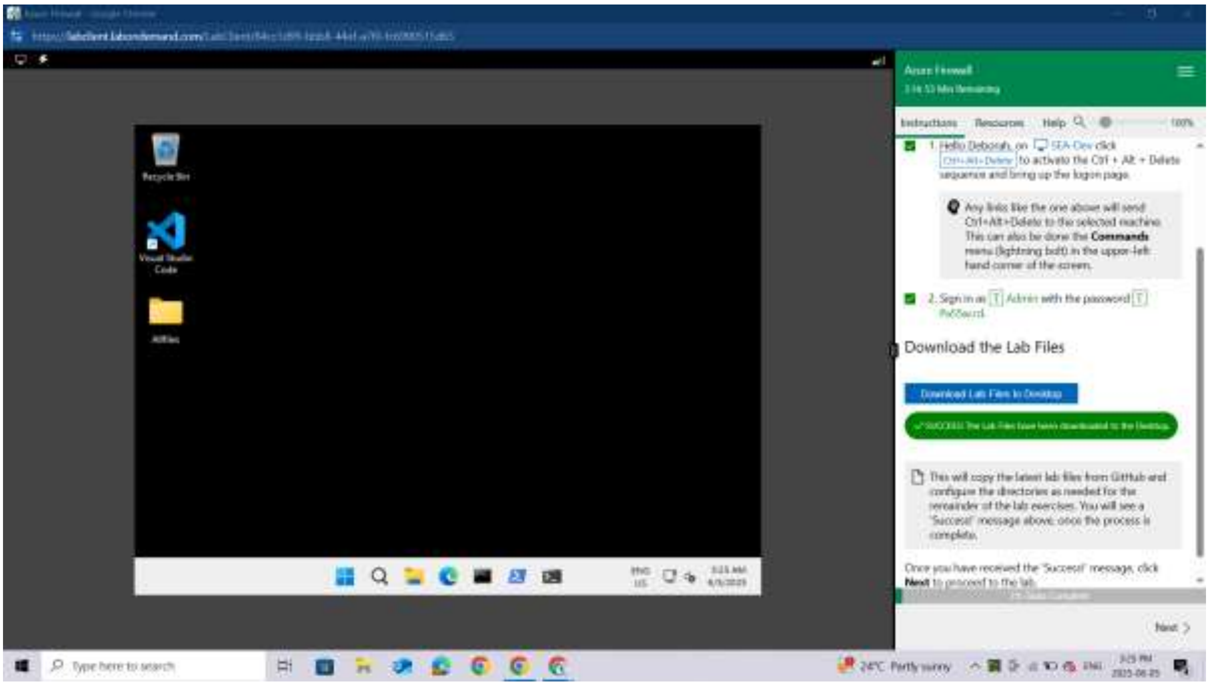
*Any links like the one above will send Ctrl+Alt+Delete to the selected machine. This can also be done the **Commands** menu (lightning bolt) in the upper-left hand corner of the screen.*

Sign in as Admin with the password Pa55w.rd.

Download the Lab Files

This will copy the latest lab files from GitHub and configure the directories as needed for the remainder of the lab exercises. You will see a 'Success!' message above, once the process is complete.

Once you have received the 'Success!' message, click **Next** to proceed to the lab.



1. Hello Deborah, on SEA-Dev click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.

Any links like the one above will send Ctrl+Alt+Delete to the selected machine. This can also be done the **Commands** menu (lightning bolt) in the upper-left hand corner of the screen.

2. Sign in as Admin with the password Pa55w.rd.

Download the Lab Files

Download Lab Files to Desktop

✓ SUCCESS: The Lab Files have been downloaded to the Desktop.

This will copy the latest lab files from GitHub and configure the directories as needed for the remainder of the lab exercises. You will see a 'Success!' message above, once the process is complete.

Once you have received the 'Success!' message, click **Next** to proceed to the lab.

Lab 03: Azure Firewall

Student lab manual

Lab scenario

You have been asked to install Azure Firewall. This will help your organization control inbound and outbound network access which is an important part of an overall network security plan. Specifically, you would like to create and test the following infrastructure components:

- A virtual network with a workload subnet and a jump host subnet.
- A virtual machine is each subnet.
- A custom route that ensures all outbound workload traffic from the workload subnet must use the firewall.
- Firewall Application rules that only allow outbound traffic to www.bing.com.
- Firewall Network rules that allow external DNS server lookups.

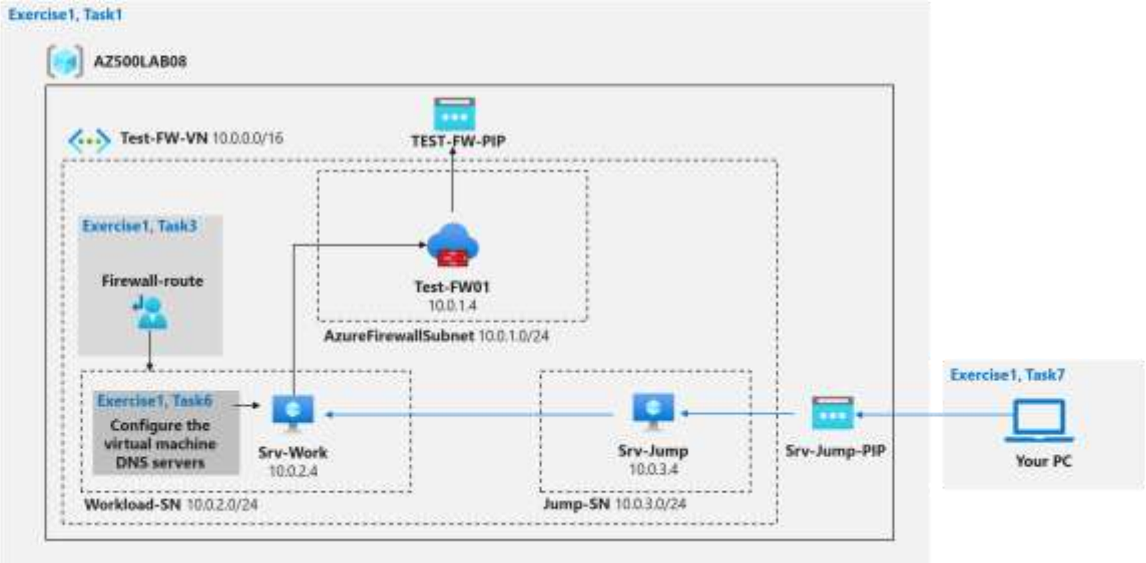
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

Lab objectives

In this lab, you will complete the following exercise:

- Exercise 1: Deploy and test an Azure Firewall

Azure Firewall diagram



Instructions

Lab files:

- *\Allfiles\Labs\08\template.json*

Exercise 1: Deploy and test an Azure Firewall

Estimated timing: 40 minutes

In this exercise, you will complete the following tasks:

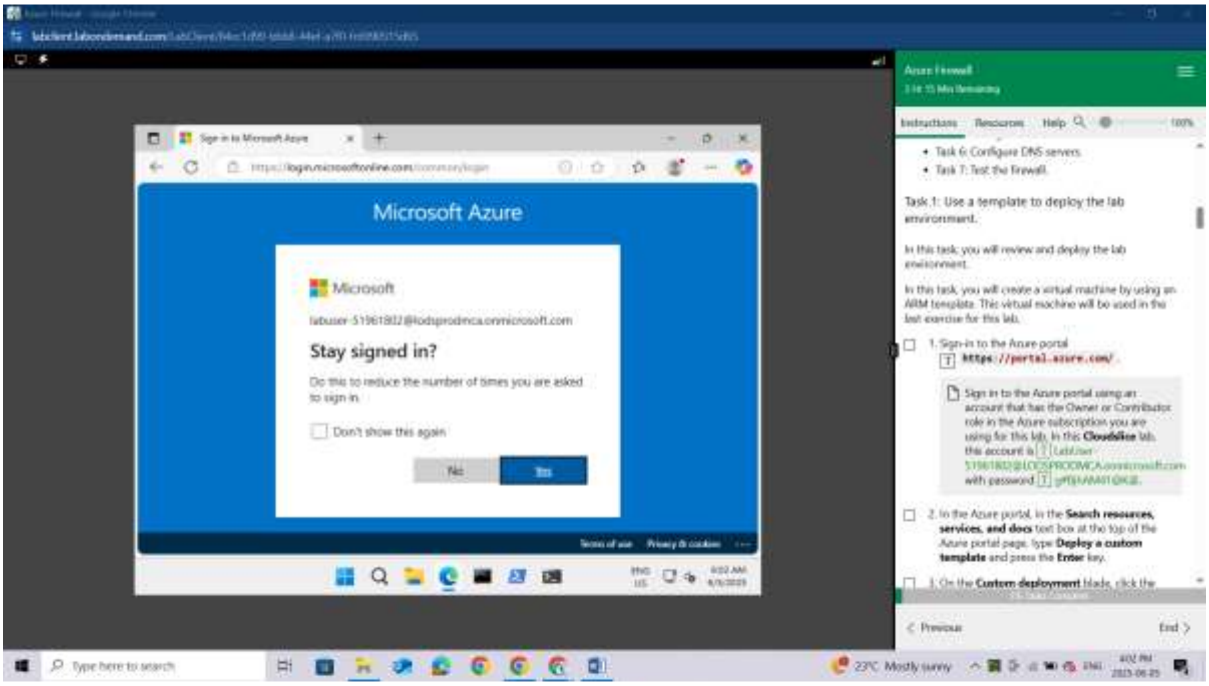
- Task 1: Use a template to deploy the lab environment.
- Task 2: Deploy an Azure firewall.
- Task 3: Create a default route.
- Task 4: Configure an application rule.
- Task 5: Configure a network rule.
- Task 6: Configure DNS servers.
- Task 7: Test the firewall.

Task 1: Use a template to deploy the lab environment.

In this task, you will review and deploy the lab environment.

In this task, you will create a virtual machine by using an ARM template. This virtual machine will be used in the last exercise for this lab.

Sign-in to the Azure portal **https://portal.azure.com/**



Microsoft Azure

Microsoft

labuser-51961802@lodsprodmca.onmicrosoft.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

Azure Firewall

Instructions Resources Help

- Task 6: Configure DNS servers.
- Task 7: Test the firewall.

Task 1: Use a template to deploy the lab environment.

In this task, you will review and deploy the lab environment.

In this task, you will create a virtual machine by using an ARM template. This virtual machine will be used in the last exercise for this lab.

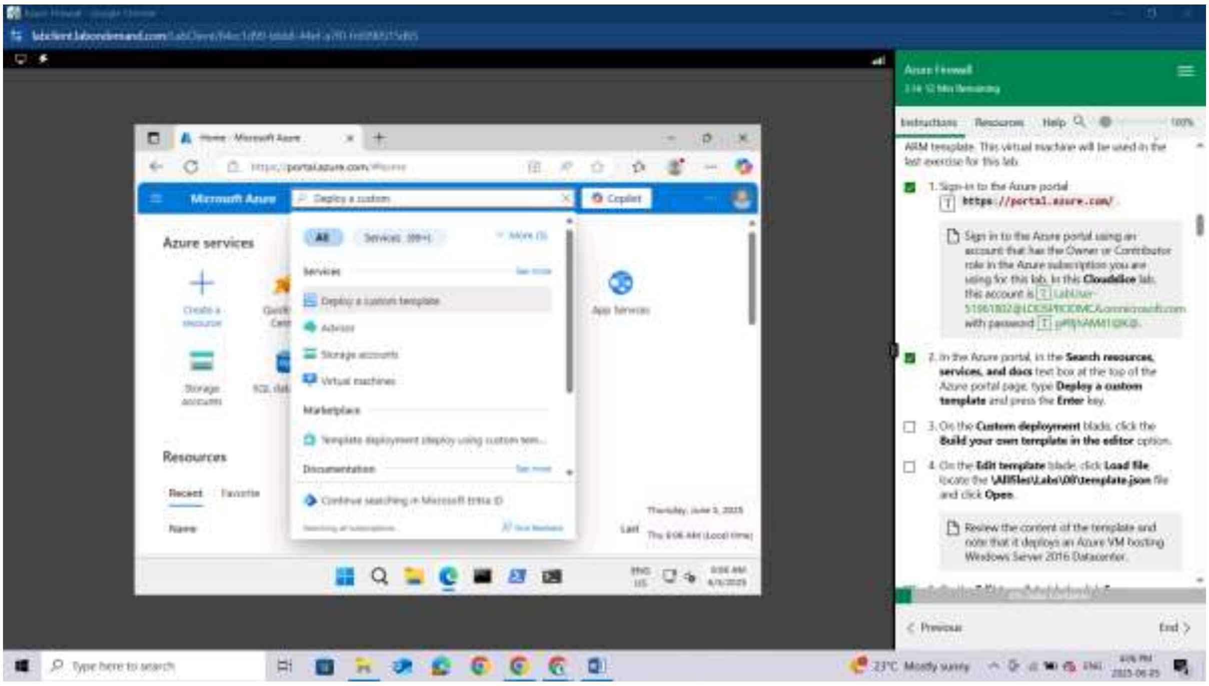
□ 1. Sign-in to the Azure portal `https://portal.azure.com/`.

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-51961802@LODSPRODMCA.onmicrosoft.com with password [illegible].

□ 2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key.

□ 3. On the **Custom deployment** blade, click the

In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key.



Azure Firewall

ARM template. This virtual machine will be used in the last exercise for this lab.

☑ 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-51961802@LODSPRODMCA.onmicrosoft.com with password [illegible].

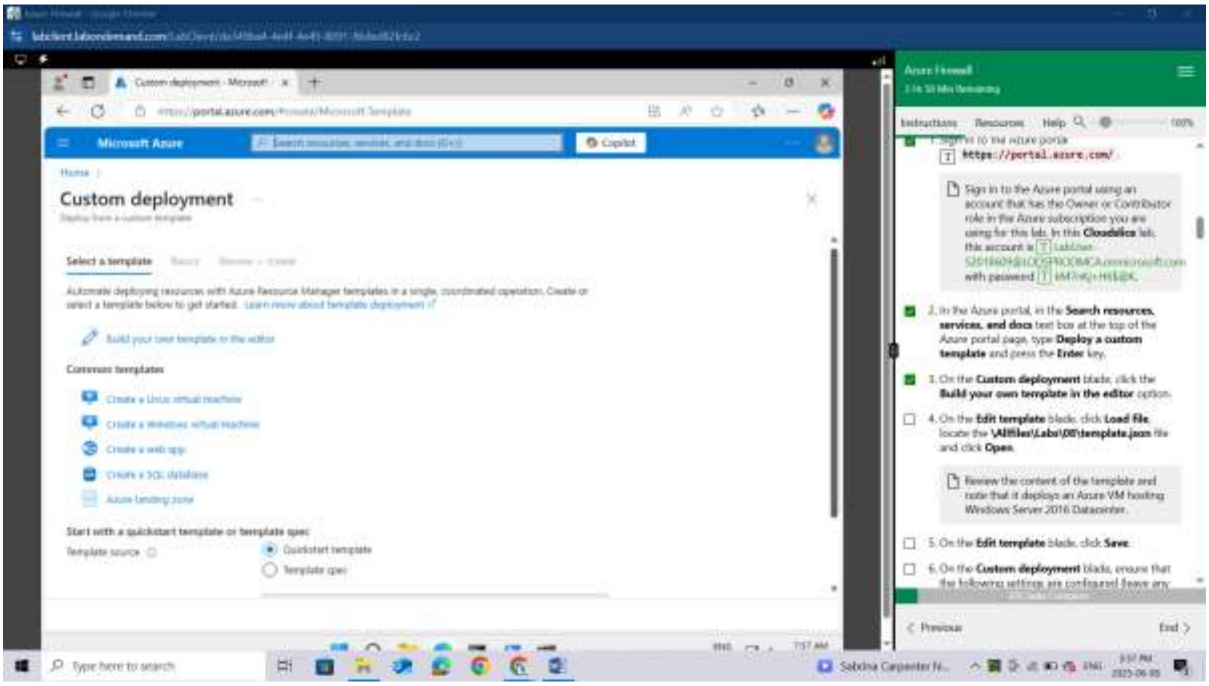
☑ 2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key.

□ 3. On the **Custom deployment** blade, click the **Build your own template in the editor** option.

□ 4. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**.

Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2016 Datacenter.

On the **Custom deployment** blade, click the **Build your own template in the editor** option.



Custom deployment

Deploy from a custom template

Select a template | Basics | Review + create

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started. Learn more about template deployment

Build your own template in the editor

Common templates

- Create a Linux virtual machine
- Create a Windows virtual machine
- Create a web app
- Create a SQL database
- Azure landing zone

Start with a quickstart template or template spec

Template source ● Quickstart template ○ Template spec

Azure Firewall

☑ 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 [illegible] with password [illegible].

☑ 2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key.

☑ 3. On the **Custom deployment** blade, click the **Build your own template in the editor** option.

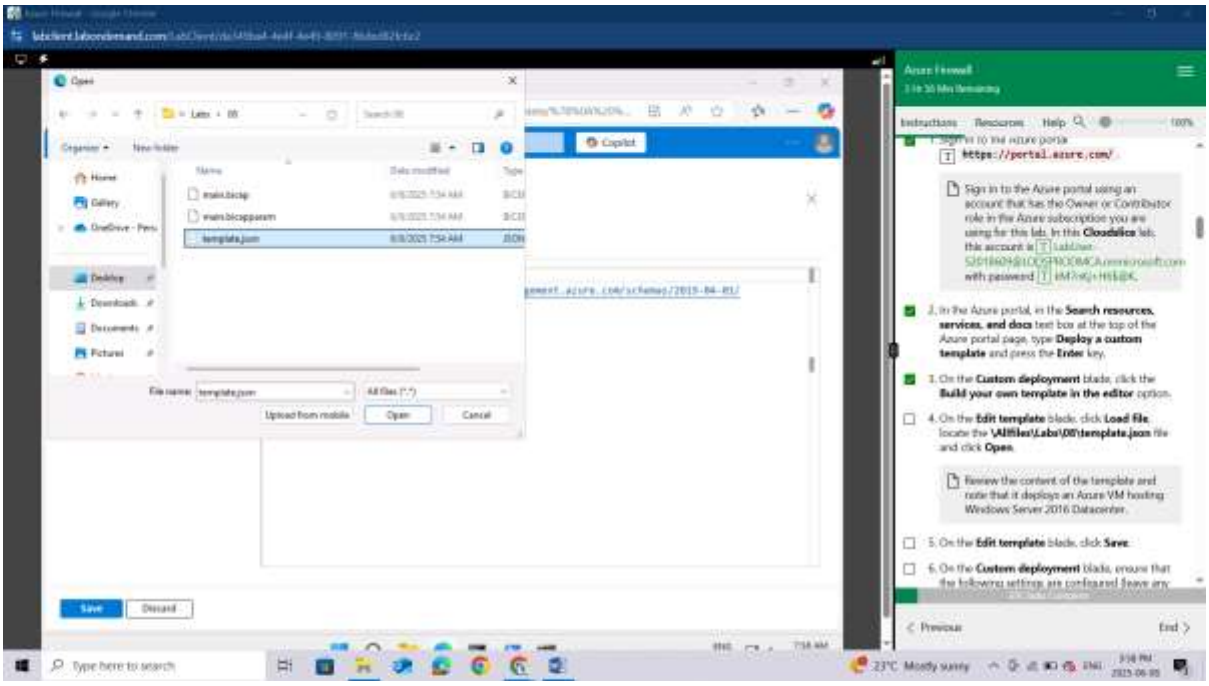
□ 4. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**.

Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2016 Datacenter.

□ 5. On the **Edit template** blade, click **Save**.

□ 6. On the **Custom deployment** blade, ensure that the following settings are configured (leave any

On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**.



Open

Labs › 08

Name	Date modified	Type
main.bicep	6/5/2025 7:54 AM	BICEP
main.bicepparam	6/5/2025 7:54 AM	BICEP
template.json	6/5/2025 7:54 AM	JSON

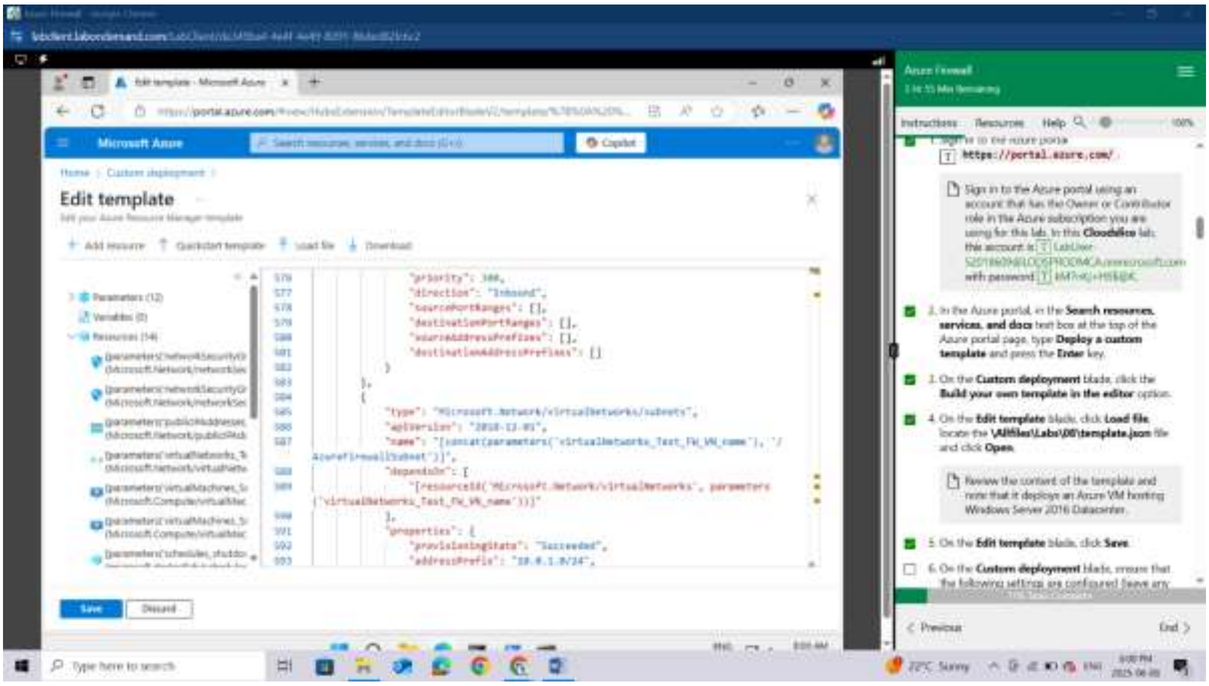
File name: template.json | All files (*.*)

Upload from mobile | Open | Cancel

Save | Discard

Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2016 Datacenter.

On the **Edit template** blade, click **Save**.



Edit template

Edit your Azure Resource Manager template

```
                "priority": 100,
                "direction": "Inbound",
                "sourcePortRanges": [],
                "destinationPortRanges": [],
                "sourceAddressPrefixes": [],
                "destinationAddressPrefixes": []
            }
        },
        {
            "type": "Microsoft.Network/virtualNetworks/subnets",
            "apiVersion": "2018-12-01",
            "name": "[concat(parameters('virtualNetworks_Test_FW_VN_name'), '/AzureFirewallSubnet')]",
            "dependsOn": [
                "[resourceId('Microsoft.Network/virtualNetworks', parameters('virtualNetworks_Test_FW_VN_name'))]"
            ],
            "properties": {
                "provisioningState": "Succeeded",
                "addressPrefix": "10.0.1.0/24",
```

☑ 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 [illegible] with password [illegible]

☑ 2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key.

☑ 3. On the **Custom deployment** blade, click the **Build your own template in the editor** option.

☑ 4. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**.

Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2016 Datacenter.

☑ 5. On the **Edit template** blade, click **Save**.

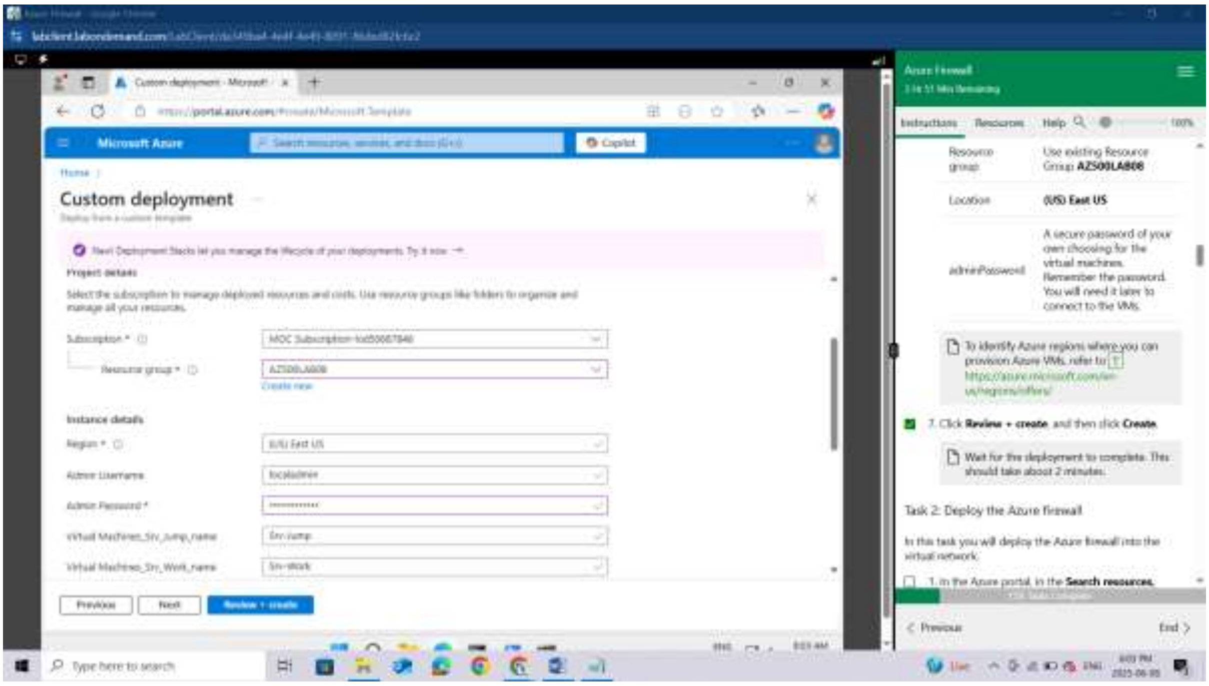
☐ 6. On the **Custom deployment** blade, ensure that the following settings are configured (leave any

On the **Custom deployment** blade, ensure that the following settings are configured (leave any others with their default values):

Setting	Value
Subscription	the name of the Azure subscription you will be using in this lab
Resource group	Use existing Resource Group **AZ500LAB08**
Location	**(US) East US**
adminPassword	A secure password of your own choosing for the virtual machines. Remember the password. You will need it later to connect to the VMs.

To identify Azure regions where you can provision Azure VMs, refer to https://azure.microsoft.com/en-us/regions/offers/

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



Custom deployment

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : MOC Subscription-lod50667846

Resource group * : AZ500LAB08

Instance details

Region * : (US) East US

Admin Username : localadmin

Admin Password * : ••••••••••••

Virtual Machines_Srv_Jump_name : Srv-Jump

Virtual Machines_Srv_Work_name : Srv-Work

Azure Firewall

Resource group	Use existing Resource Group **AZ500LAB08**
Location	**(US) East US**
adminPassword	A secure password of your own choosing for the virtual machines. Remember the password. You will need it later to connect to the VMs.

To identify Azure regions where you can provision Azure VMs, refer to https://azure.microsoft.com/en-us/regions/offers/

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

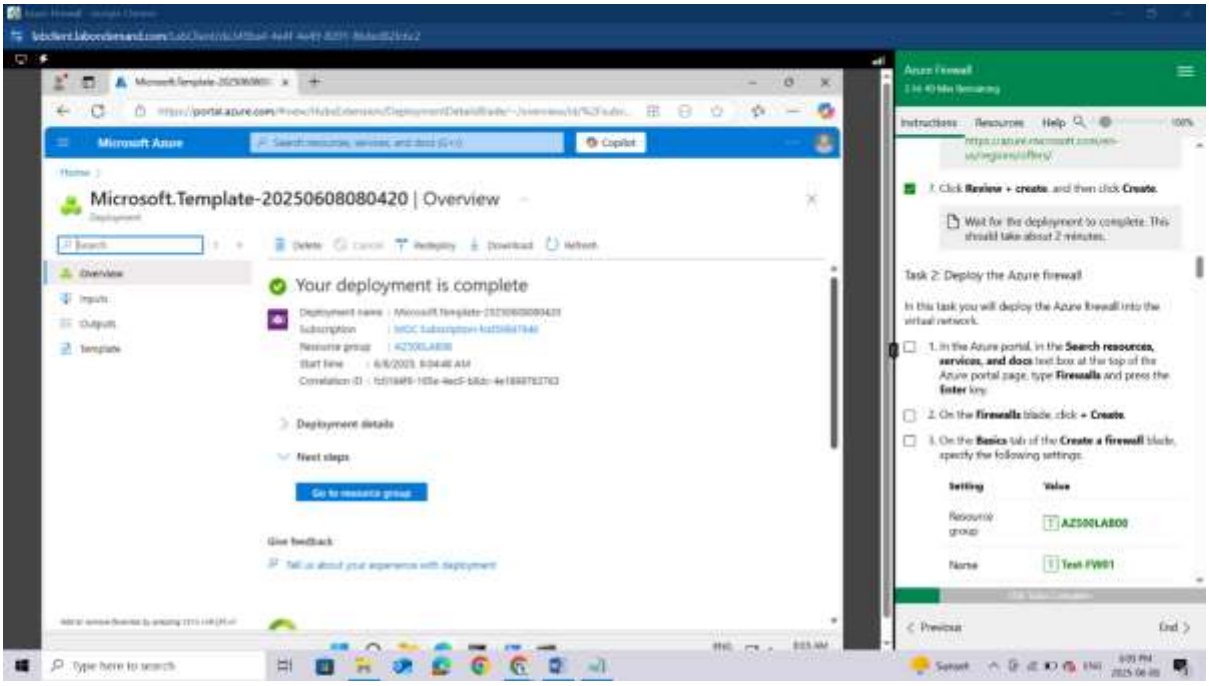
Wait for the deployment to complete. This should take about 2 minutes.

Task 2: Deploy the Azure firewall

In this task you will deploy the Azure firewall into the virtual network.

□ 1. In the Azure portal, in the **Search resources,**

Wait for the deployment to complete. This should take about 2 minutes.



Microsoft.Template-20250608080420 | Overview

Your deployment is complete

Deployment name : Microsoft.Template-20250608080420

Subscription : MOC Subscription-lod50667846

Resource group : AZ500LAB08

Start time : 6/8/2025, 8:04:48 AM

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

Wait for the deployment to complete. This should take about 2 minutes.

Task 2: Deploy the Azure firewall

In this task you will deploy the Azure firewall into the virtual network.

□ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Firewalls** and press the **Enter** key.

□ 2. On the **Firewalls** blade, click **+ Create**.

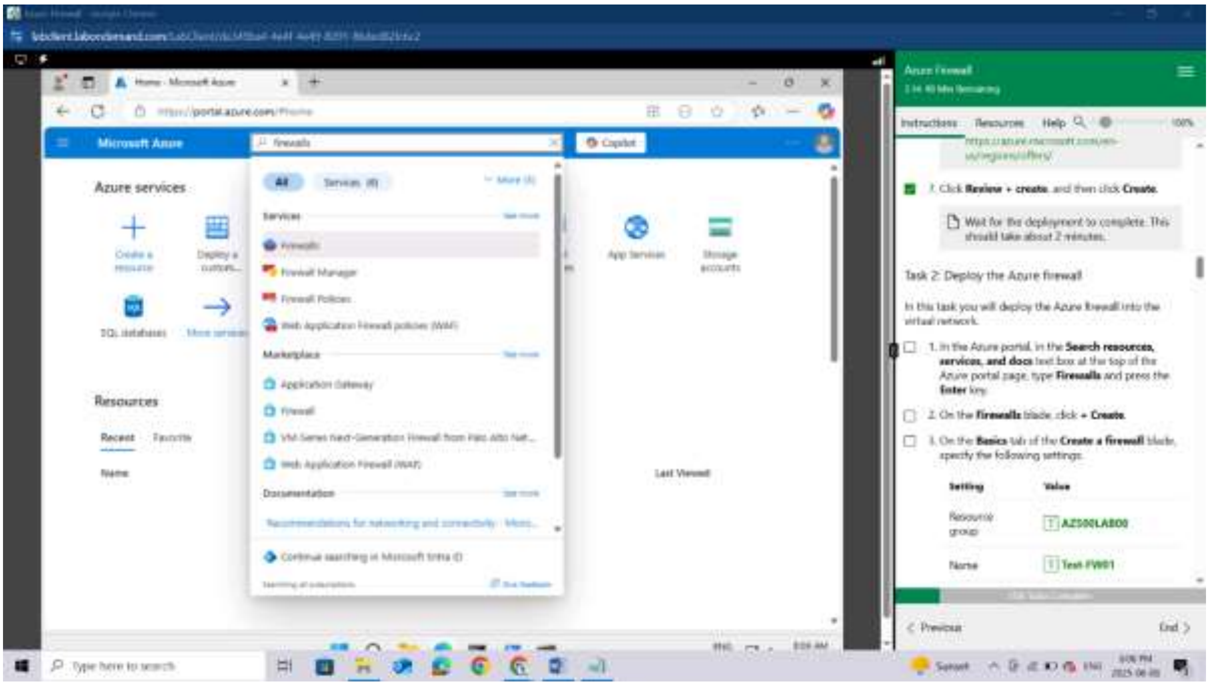
□ 3. On the **Basics** tab of the **Create a firewall** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB08
Name	Test-FW01

Task 2: Deploy the Azure firewall

In this task you will deploy the Azure firewall into the virtual network.

In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Firewalls** and press the **Enter** key.



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

Wait for the deployment to complete. This should take about 2 minutes.

Task 2: Deploy the Azure firewall

In this task you will deploy the Azure firewall into the virtual network.

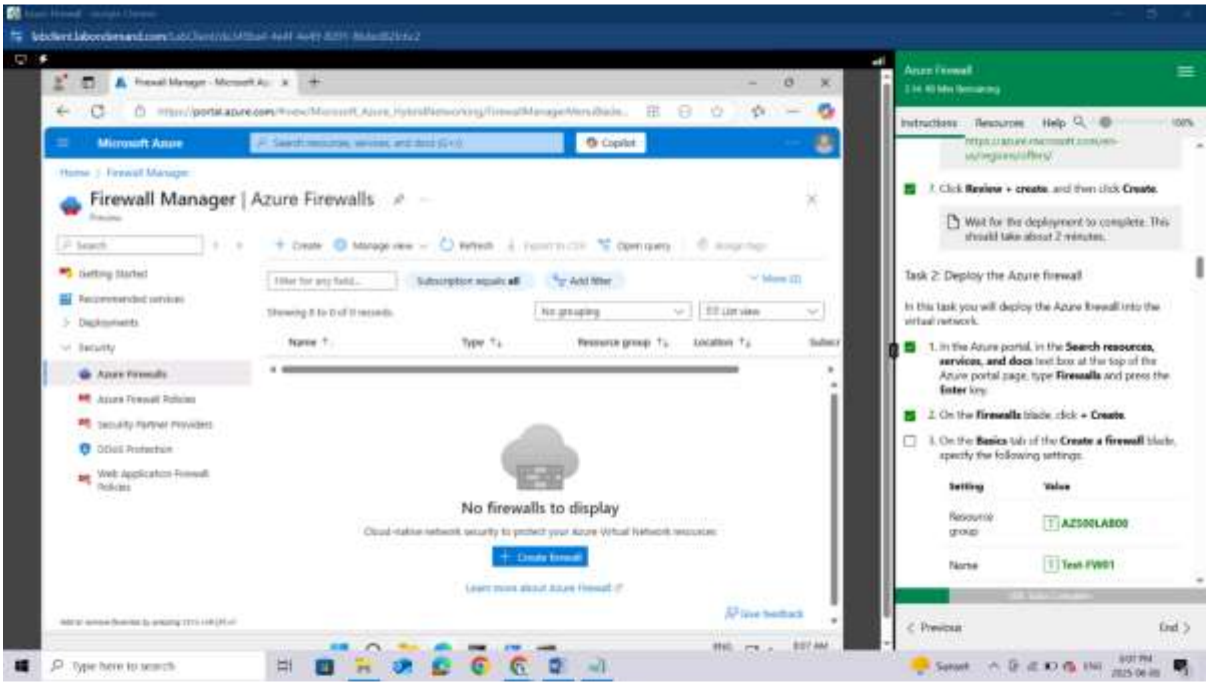
☐ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Firewalls** and press the **Enter** key.

☐ 2. On the **Firewalls** blade, click **+ Create**.

☐ 3. On the **Basics** tab of the **Create a firewall** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB08
Name	Test-FW01

On the **Firewalls** blade, click **+ Create**.



☑ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Firewalls** and press the **Enter** key.

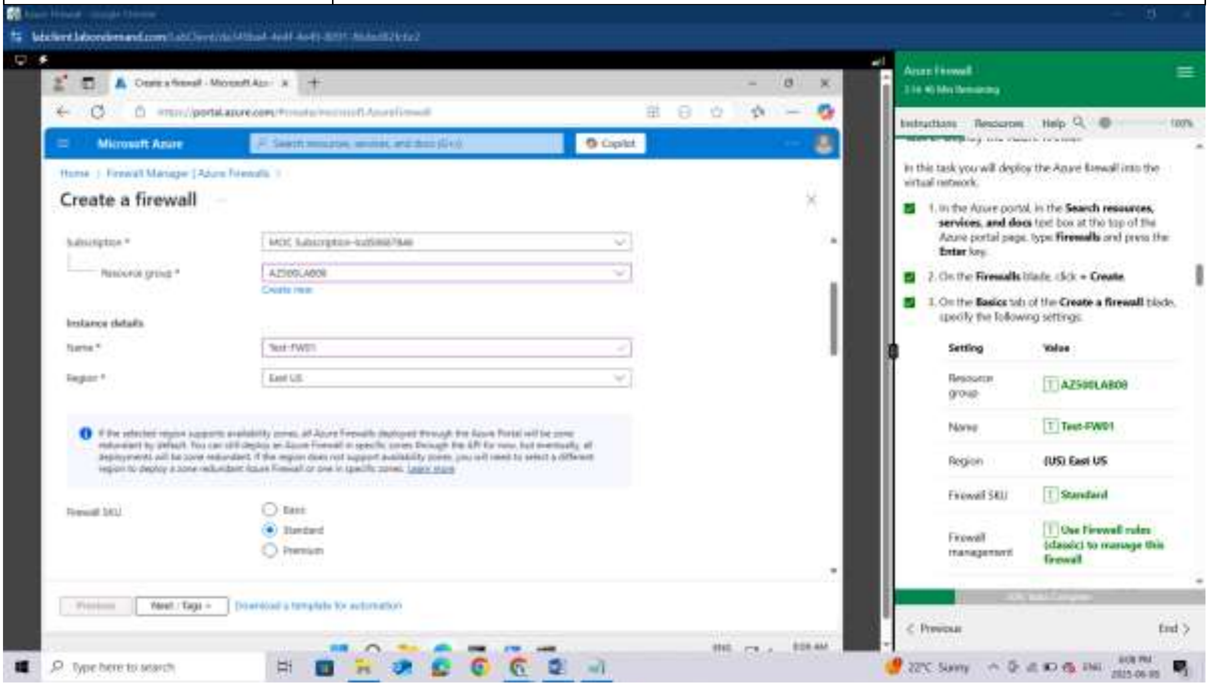
☑ 2. On the **Firewalls** blade, click **+ Create**.

☐ 3. On the **Basics** tab of the **Create a firewall** blade, specify the following settings:

On the **Basics** tab of the **Create a firewall** blade, specify the following settings:

Setting	Value
Resource group	**AZ500LAB08**
Name	**Test-FW01**
Region	**(US) East US**

Setting	Value
Firewall SKU	**Standard**
Firewall management	**Use Firewall rules (classic) to manage this firewall**
Choose a virtual network	click the **Use existing** option and, in the drop-down list, select **Test-FW-VN**
Firewall Management NIC	To disable this feature, **deselect** the **Enable Firewall Management NIC** option.
Public IP address	clck **Add new** and type the name **TEST-FW-PIP** and click **OK**



Create a firewall

Subscription * MOC Subscription-[illegible]

Resource group * AZ500LAB08

Instance details

Name * Test-FW01

Region * East US

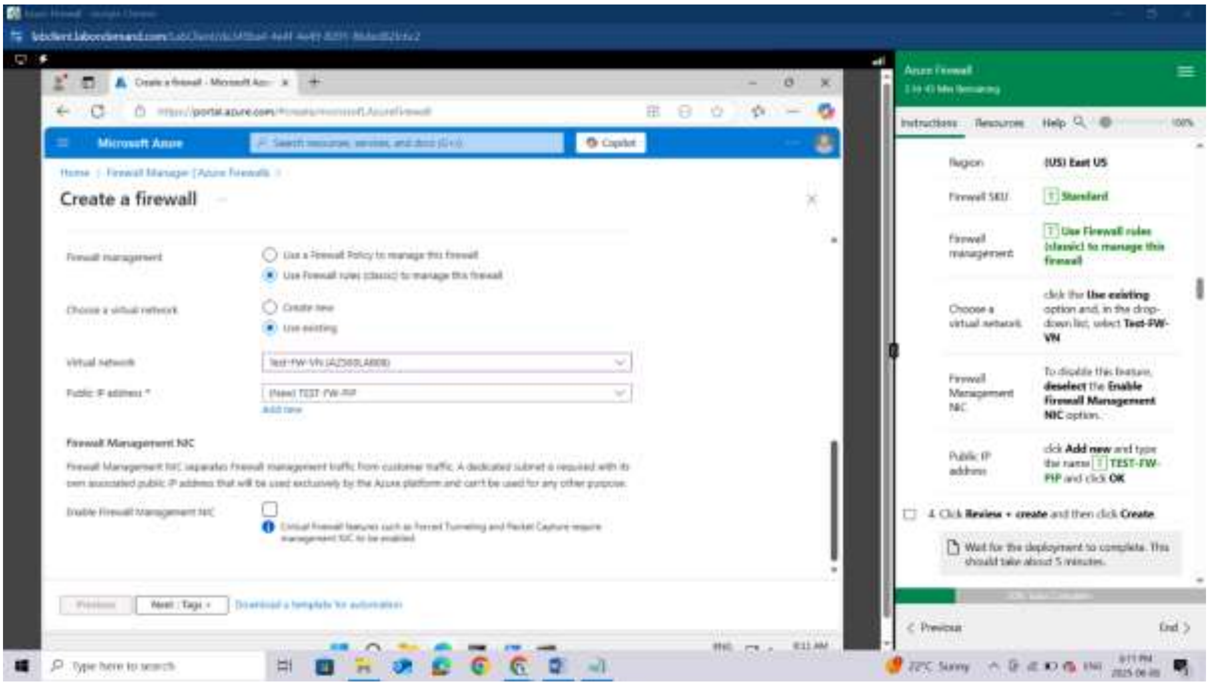
If the selected region supports availability zones, all Azure Firewalls deployed through the Azure Portal will be zone redundant by default. You can still deploy an Azure Firewall in specific zones through the API for now, but eventually, all deployments will be zone redundant. If the region does not support availability zones, you will need to select a different region to deploy a zone redundant Azure Firewall or one in specific zones. Learn more

Firewall SKU ○ Basic ● Standard ○ Premium

In this task you will deploy the Azure firewall into the virtual network.

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **firewalls** and press the **Enter** key.
2. On the **Firewalls** blade, click **+ Create**.
3. On the **Basics** tab of the **Create a firewall** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB08
Name	Test-FW01
Region	(US) East US
Firewall SKU	Standard
Firewall management	Use Firewall rules (classic) to manage this firewall



Create a firewall

Firewall management
○ Use a Firewall Policy to manage this firewall
● Use Firewall rules (classic) to manage this firewall

Choose a virtual network
○ Create new
● Use existing

Virtual network: Test-FW-VN (AZ500LAB08)

Public IP address *: (New) TEST-FW-PIP
Add new

Firewall Management NIC

Firewall Management NIC separates Firewall management traffic from customer traffic. A dedicated subnet is required with its own associated public IP address that will be used exclusively by the Azure platform and can't be used for any other purpose.

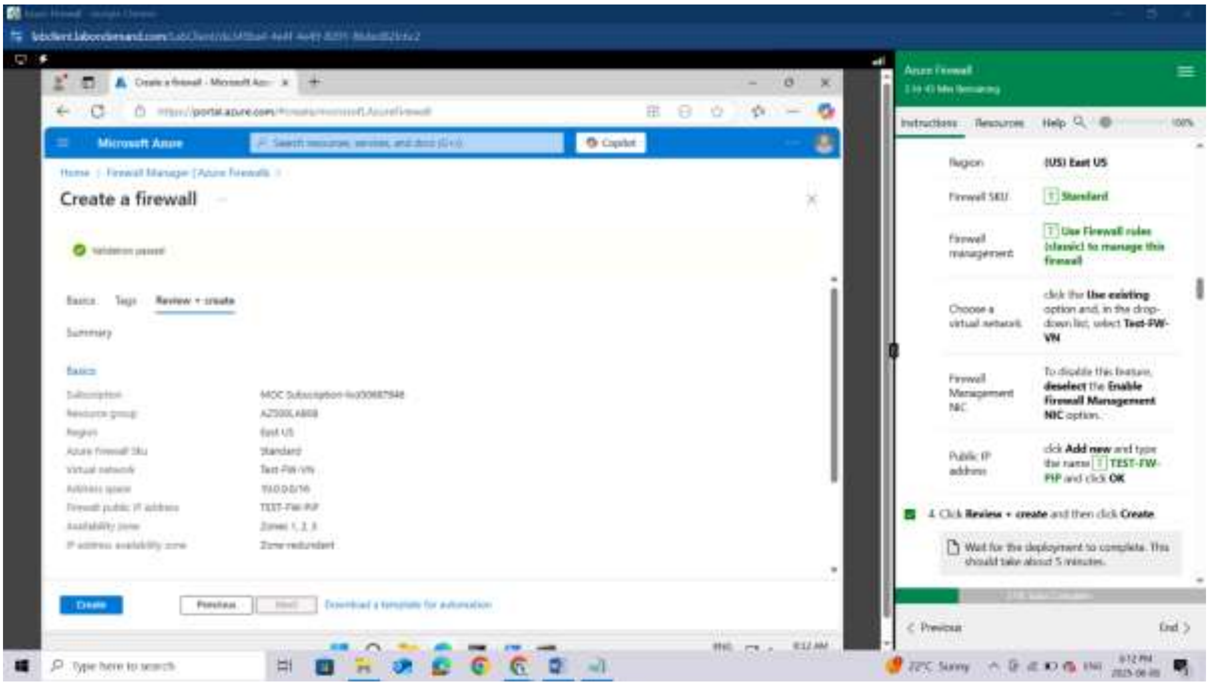
Enable Firewall Management NIC □
Critical Firewall features such as Forced Tunneling and Packet Capture require management NIC to be enabled.

Region	**(US) East US**
Firewall SKU	**Standard**
Firewall management	**Use Firewall rules (classic) to manage this firewall**
Choose a virtual network	click the **Use existing** option and, in the drop-down list, select **Test-FW-VN**
Firewall Management NIC	To disable this feature, **deselect** the **Enable Firewall Management NIC** option.
Public IP address	click **Add new** and type the name **TEST-FW-PIP** and click **OK**

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

Wait for the deployment to complete. This should take about 5 minutes.

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



Create a firewall

Validation passed

Summary

Basics

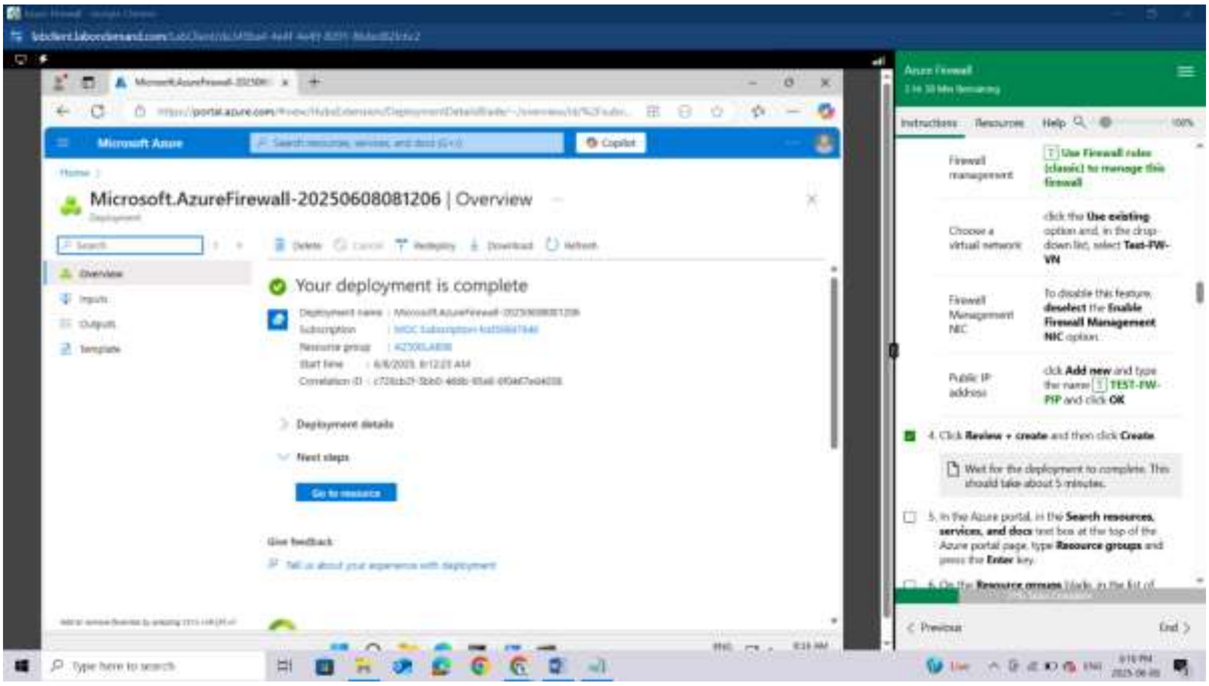
Subscription	MOC Subscription-lod30687946
Resource group	AZ500LAB08
Region	East US
Azure Firewall Sku	Standard
Virtual network	Test-FW-VN
Address space	10.0.0.0/16
Firewall public IP address	TEST-FW-PIP
Availability zone	Zones 1, 2, 3
IP address availability zone	Zone-redundant

Region	**(US) East US**
Firewall SKU	**Standard**
Firewall management	**Use Firewall rules (classic) to manage this firewall**
Choose a virtual network	click the **Use existing** option and, in the drop-down list, select **Test-FW-VN**
Firewall Management NIC	To disable this feature, **deselect** the **Enable Firewall Management NIC** option.
Public IP address	click **Add new** and type the name **TEST-FW-PIP** and click **OK**

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

Wait for the deployment to complete. This should take about 5 minutes.

Wait for the deployment to complete. This should take about 5 minutes.



Microsoft.AzureFirewall-20250608081206 | Overview

Your deployment is complete

Deployment name : Microsoft.AzureFirewall-20250608081206
Subscription : MOC Subscription-lod[illegible]
Resource group : AZ500LAB08
Start time : 6/8/2025, 8:12:23 AM

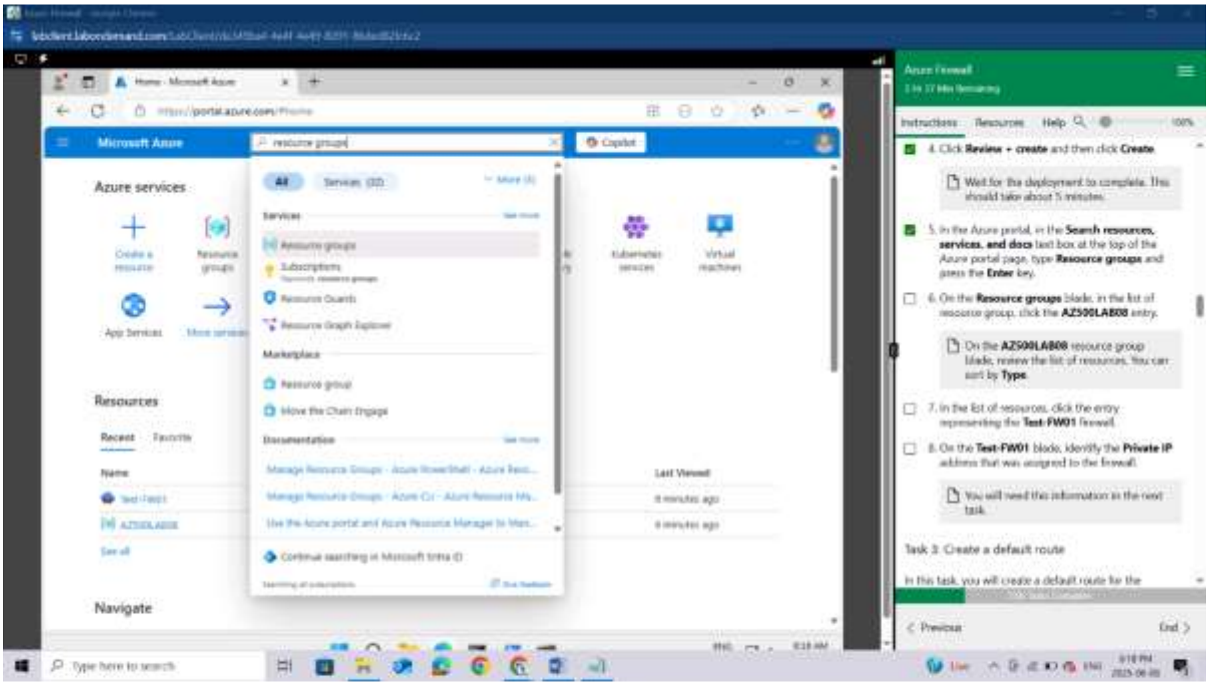
Firewall management	Use Firewall rules (classic) to manage this firewall
Choose a virtual network	click the **Use existing** option and, in the drop-down list, select **Test-FW-VN**
Firewall Management NIC	To disable this feature, **deselect** the **Enable Firewall Management NIC** option.
Public IP address	click **Add new** and type the name TEST-FW-PIP and click **OK**

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

Wait for the deployment to complete. This should take about 5 minutes.

□ 5. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.

In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.



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

Wait for the deployment to complete. This should take about 5 minutes.

☑ 5. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.

□ 6. On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB08** entry.

On the **AZ500LAB08** resource group blade, review the list of resources. You can sort by **Type**.

□ 7. In the list of resources, click the entry representing the **Test-FW01** firewall.

□ 8. On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

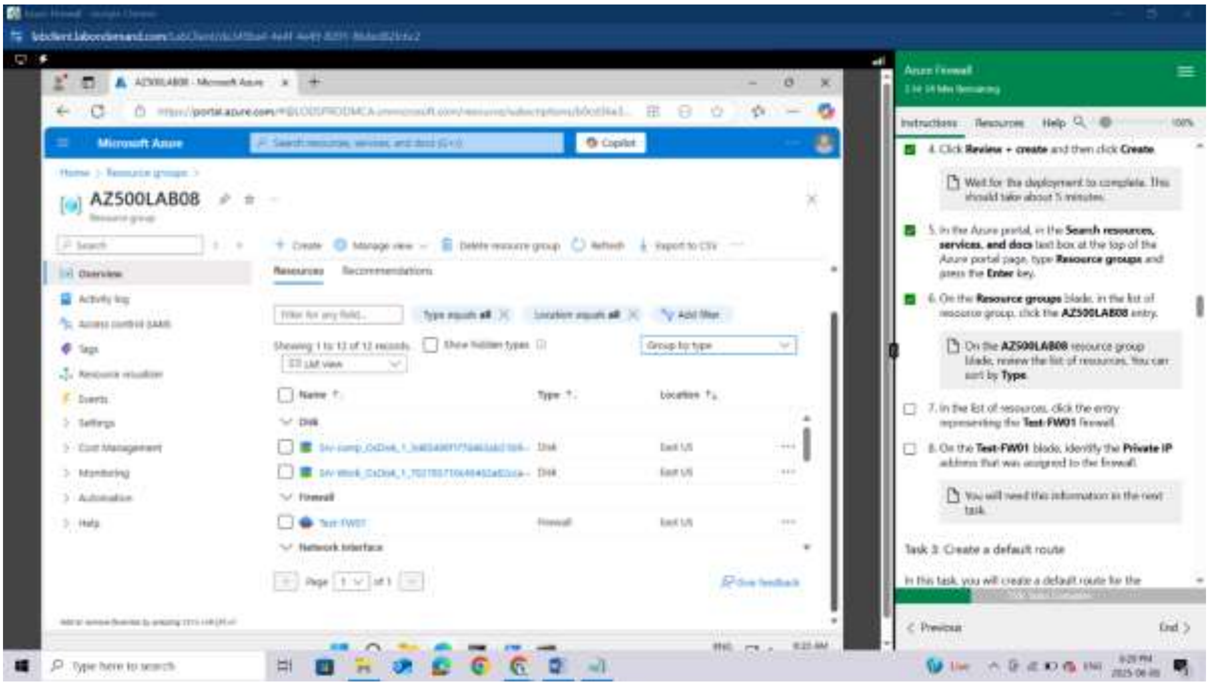
You will need this information in the next task.

Task 3: Create a default route

In this task, you will create a default route for the

On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB08** entry.

*On the **AZ500LAB08** resource group blade, review the list of resources. You can sort by **Type**.*



Azure Firewall

Instructions | Resources | Help

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

Wait for the deployment to complete. This should take about 5 minutes.

☑ 5. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.

☑ 6. On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB08** entry.

On the **AZ500LAB08** resource group blade, review the list of resources. You can sort by **Type**.

□ 7. In the list of resources, click the entry representing the **Test-FW01** firewall.

□ 8. On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

You will need this information in the next task.

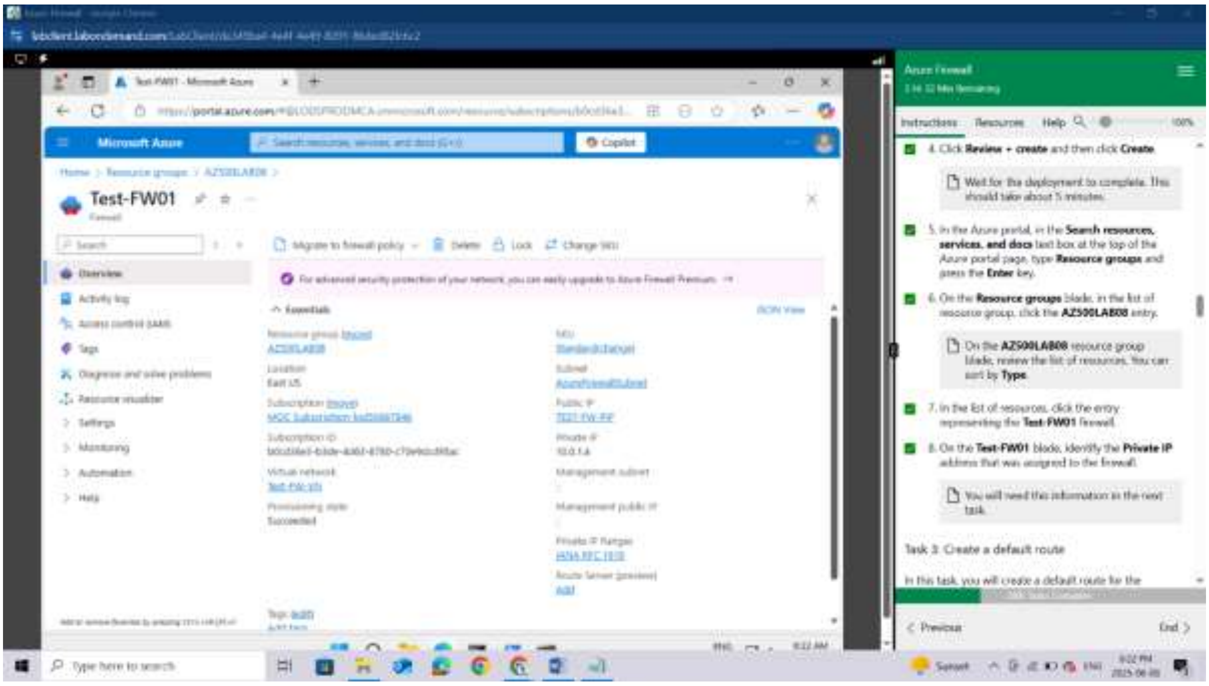
Task 3: Create a default route

In this task, you will create a default route for the

In the list of resources, click the entry representing the **Test-FW01** firewall.

On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

You will need this information in the next task.



Test-FW01

Essentials

Resource group: AZ500LAB08

Location: East US

Virtual network: Test-FW-VN

Provisioning state: Succeeded

SKU: Standard

Subnet: AzureFirewallSubnet

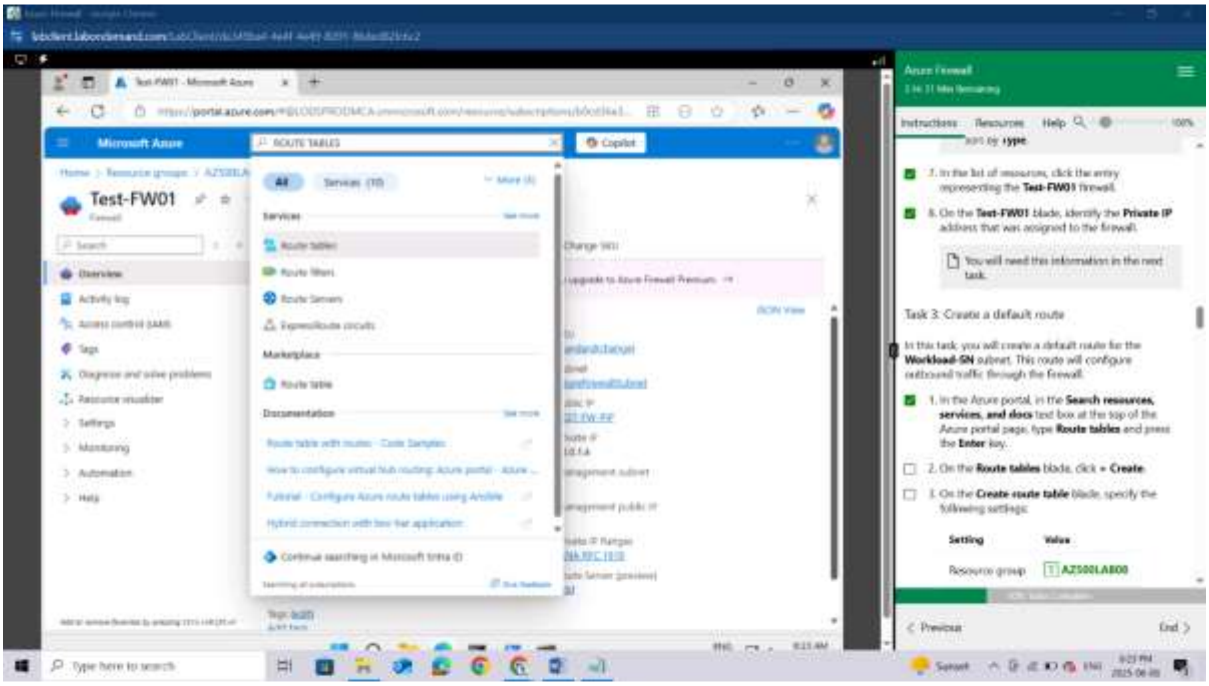
Public IP: TEST-FW-PIP

Private IP: 10.0.1.4

Private IP Ranges: IANA RFC 1918

Task 3: Create a default route

In this task, you will create a default route for the **Workload-SN** subnet. This route will configure outbound traffic through the firewall.



Azure Firewall

Instructions Resources Help

☑ 7. In the list of resources, click the entry representing the **Test-FW01** firewall.

☑ 8. On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

You will need this information in the next task.

Task 3: Create a default route

In this task, you will create a default route for the **Workload-SN** subnet. This route will configure outbound traffic through the firewall.

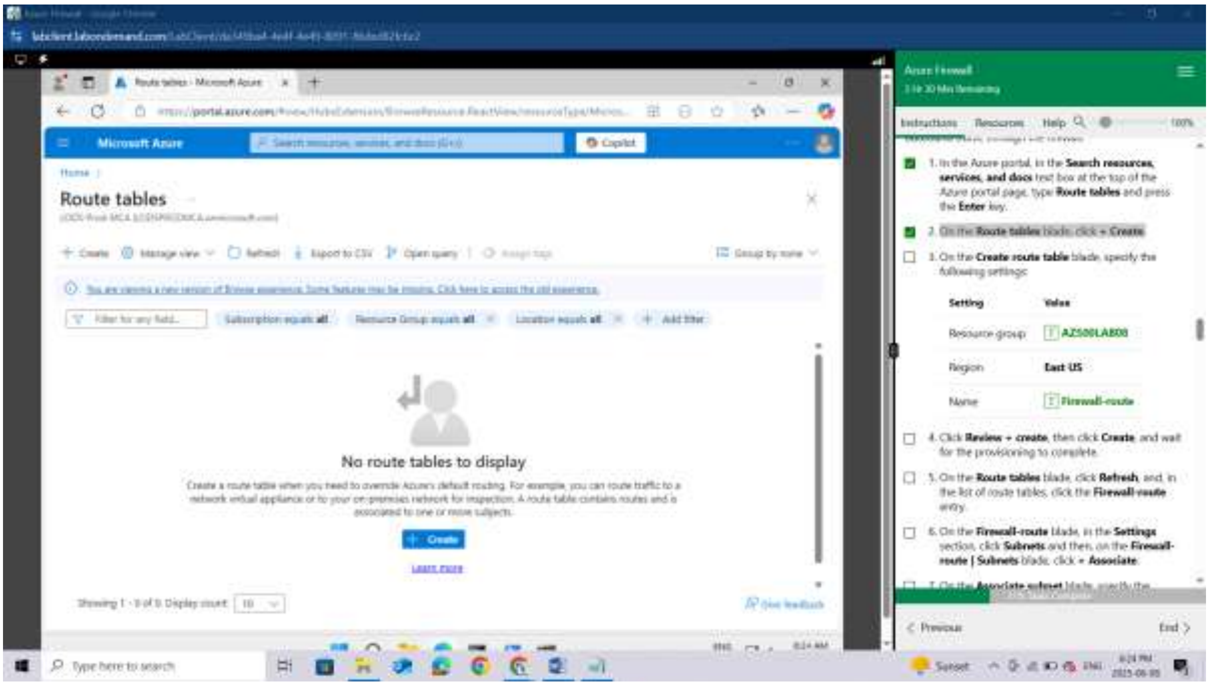
☑ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.

□ 2. On the **Route tables** blade, click **+ Create**.

□ 3. On the **Create route table** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB08

On the **Route tables** blade, click **+ Create**.



Azure Firewall

Instructions Resources Help

☑ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.

☑ 2. On the **Route tables** blade, click **+ Create**.

□ 3. On the **Create route table** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB08
Region	East US
Name	Firewall-route

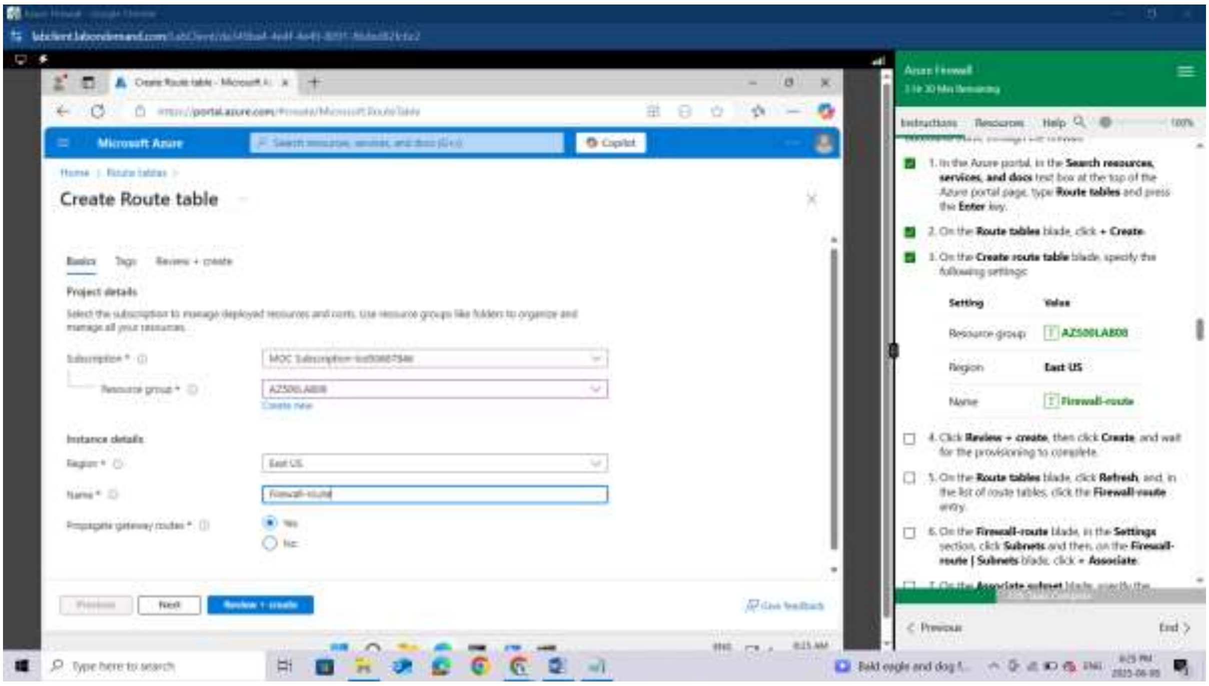
□ 4. Click **Review + create**, then click **Create**, and wait for the provisioning to complete.

□ 5. On the **Route tables** blade, click **Refresh**, and, in the list of route tables, click the **Firewall-route** entry.

□ 6. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.

On the **Create route table** blade, specify the following settings:

Setting	Value
Resource group	**AZ500LAB08**
Region	**East US**
Name	**Firewall-route**



Create Route table

Basics | Tags | Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : MOC Subscription-lod50887946

Resource group * : AZ500LAB08

Instance details

Region * : East US

Name * : Firewall-route

Propagate gateway routes * : ● Yes ○ No

Azure Firewall
3 Hr 30 Min Remaining

☑ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.

☑ 2. On the **Route tables** blade, click **+ Create**.

☑ 3. On the **Create route table** blade, specify the following settings:

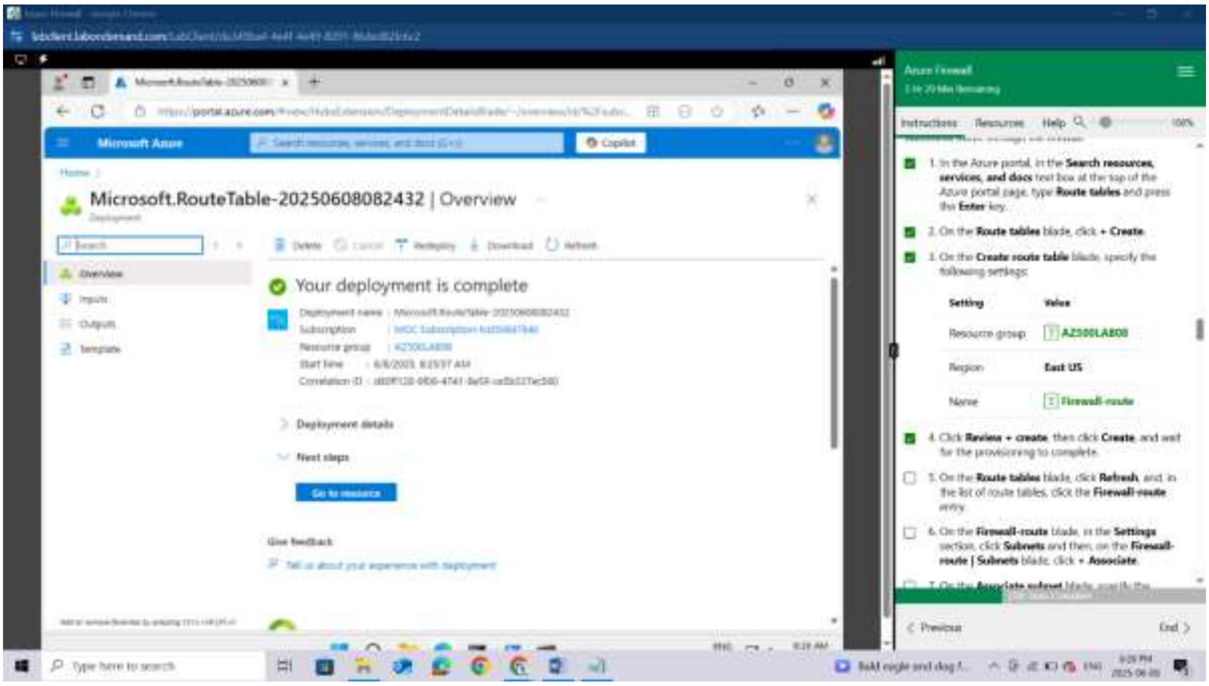
Setting	Value
Resource group	AZ500LAB08
Region	East US
Name	Firewall-route

□ 4. Click **Review + create**, then click **Create**, and wait for the provisioning to complete.

□ 5. On the **Route tables** blade, click **Refresh**, and, in the list of route tables, click the **Firewall-route** entry.

□ 6. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.

Click **Review + create**, then click **Create**, and wait for the provisioning to complete.



Microsoft.RouteTable-20250608082432 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.RouteTable-20250608082432
Subscription : MOC Subscription-lod50887946
Resource group : AZ500LAB08
Start time : 6/8/2025, 8:25:37 AM
Correlation ID : [illegible]

Azure Firewall

☑ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.

☑ 2. On the **Route tables** blade, click **+ Create**.

☑ 3. On the **Create route table** blade, specify the following settings:

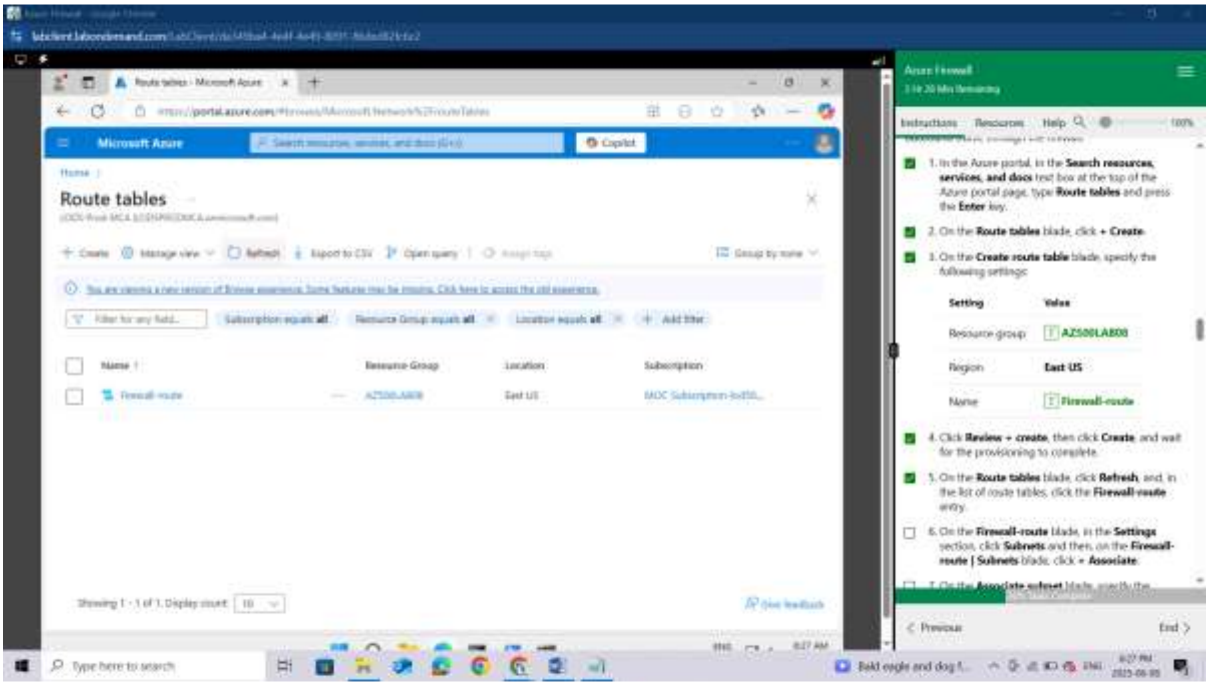
Setting	Value
Resource group	AZ500LAB08
Region	East US
Name	Firewall-route

☑ 4. Click **Review + create**, then click **Create**, and wait for the provisioning to complete.

□ 5. On the **Route tables** blade, click **Refresh**, and, in the list of route tables, click the **Firewall-route** entry.

□ 6. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.

On the **Route tables** blade, click **Refresh**, and, in the list of route tables, click the **Firewall-route** entry.



Route tables

Name	Resource Group	Location	Subscription
Firewall-route	AZ500LAB08	East US	MOC Subscription-lod5...

Azure Firewall

☑ 1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.

☑ 2. On the **Route tables** blade, click **+ Create**.

☑ 3. On the **Create route table** blade, specify the following settings:

Setting	Value
Resource group	AZ500LAB08
Region	East US
Name	Firewall-route

☑ 4. Click **Review + create**, then click **Create**, and wait for the provisioning to complete.

☑ 5. On the **Route tables** blade, click **Refresh**, and, in the list of route tables, click the **Firewall-route** entry.

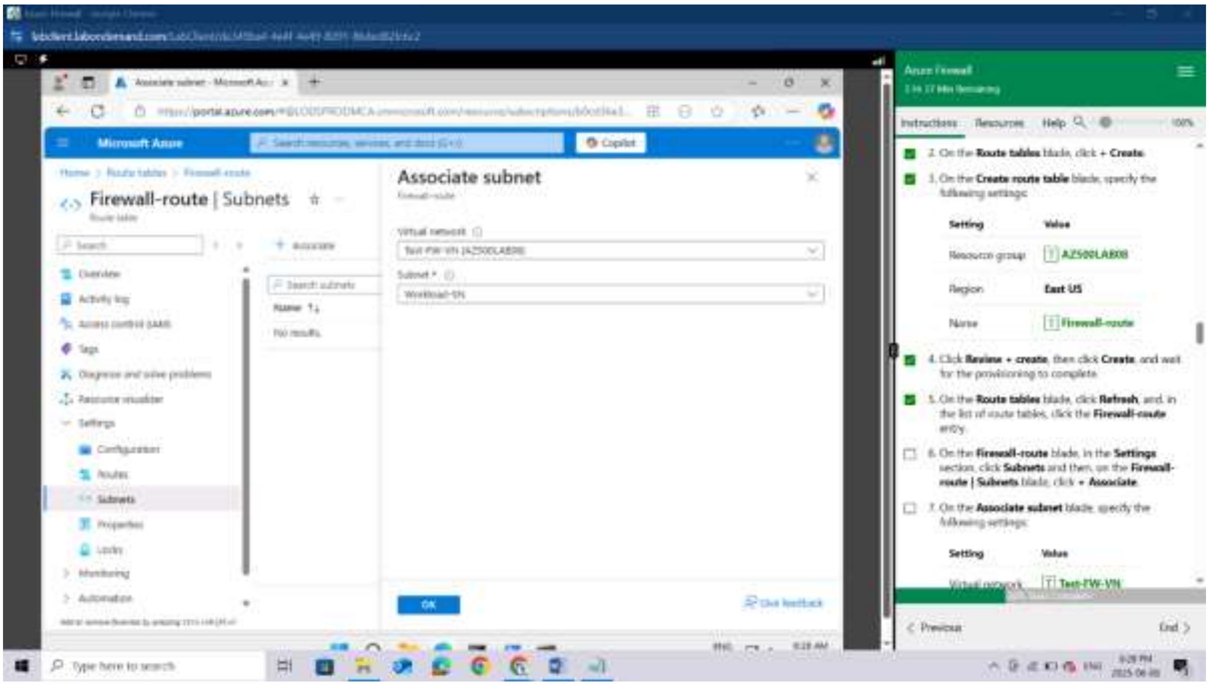
□ 6. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.

On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.

On the **Associate subnet** blade, specify the following settings:

Setting	Value
Virtual network	**Test-FW-VN**
Subnet	**Workload-SN**

*Ensure the **Workload-SN** subnet is selected for this route, otherwise the firewall won't work correctly.*



Firewall-route | Subnets

Associate subnet

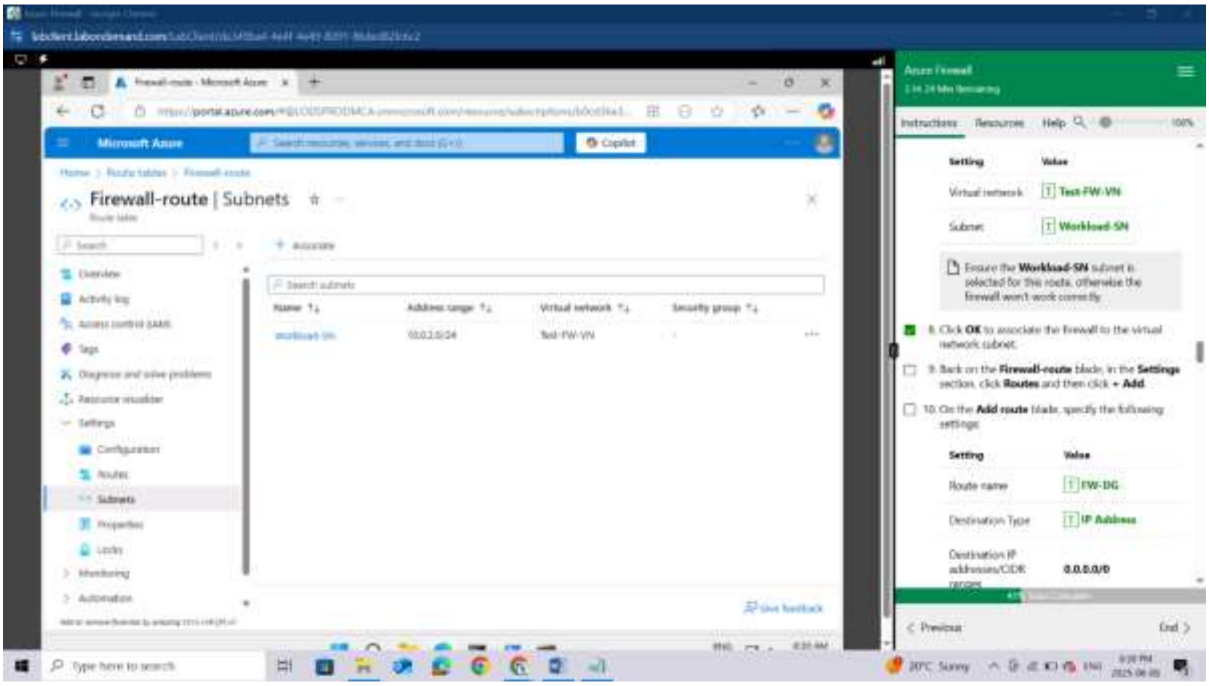
Virtual network: Test-FW-VN (AZ500LAB08)

Subnet *: Workload-SN

□ 7. On the **Associate subnet** blade, specify the following settings:

Setting	Value
Virtual network	Test-FW-VN

Click **OK** to associate the firewall to the virtual network subnet.



Firewall-route | Subnets

Route table

Name	Address range	Virtual network	Security group
Workload-SN	10.0.2.0/24	Test-FW-VN	-

Azure Firewall

Setting	Value
Virtual network	Test-FW-VN
Subnet	Workload-SN

Ensure the **Workload-SN** subnet is selected for this route, otherwise the firewall won't work correctly.

☑ 8. Click **OK** to associate the firewall to the virtual network subnet.

☐ 9. Back on the **Firewall-route** blade, in the **Settings** section, click **Routes** and then click **+ Add**.

☐ 10. On the **Add route** blade, specify the following settings:

Setting	Value
Route name	FW-DG
Destination Type	IP Address
Destination IP addresses/CIDR ranges	0.0.0.0/0

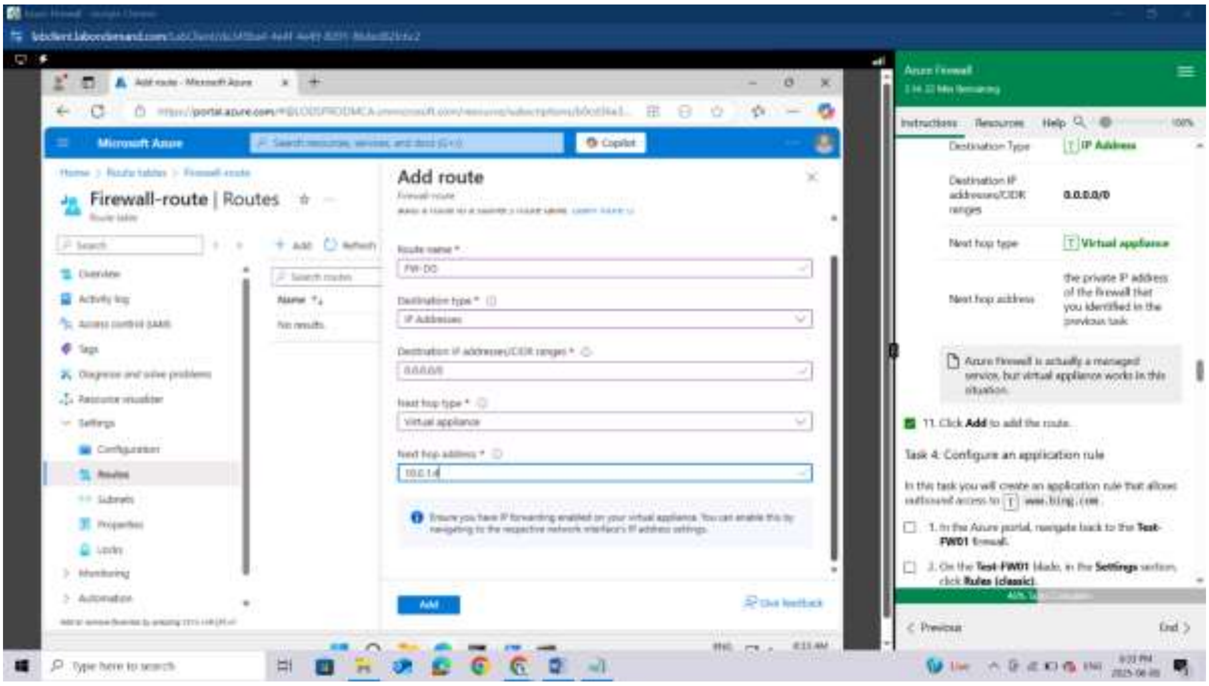
Back on the **Firewall-route** blade, in the **Settings** section, click **Routes** and then click **+ Add**.

On the **Add route** blade, specify the following settings:

Setting	Value
Route name	**FW-DG**
Destination Type	**IP Address**
Destination IP addresses/CIDR ranges	**0.0.0.0/0**
Next hop type	**Virtual appliance**
Next hop address	the private IP address of the firewall that you identified in the previous task

Azure Firewall is actually a managed service, but virtual appliance works in this situation.

Click **Add** to add the route.



Add route

Route name * FW-DG

Destination type * IP Addresses

Destination IP addresses/CIDR ranges * 0.0.0.0/0

Next hop type * Virtual appliance

Next hop address * 10.0.1.4

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Azure Firewall

Destination Type	IP Address
Destination IP addresses/CIDR ranges	0.0.0.0/0
Next hop type	Virtual appliance
Next hop address	the private IP address of the firewall that you identified in the previous task

Azure Firewall is actually a managed service, but virtual appliance works in this situation.

☑ 11. Click **Add** to add the route.

Task 4: Configure an application rule

In this task you will create an application rule that allows outbound access to www.bing.com.

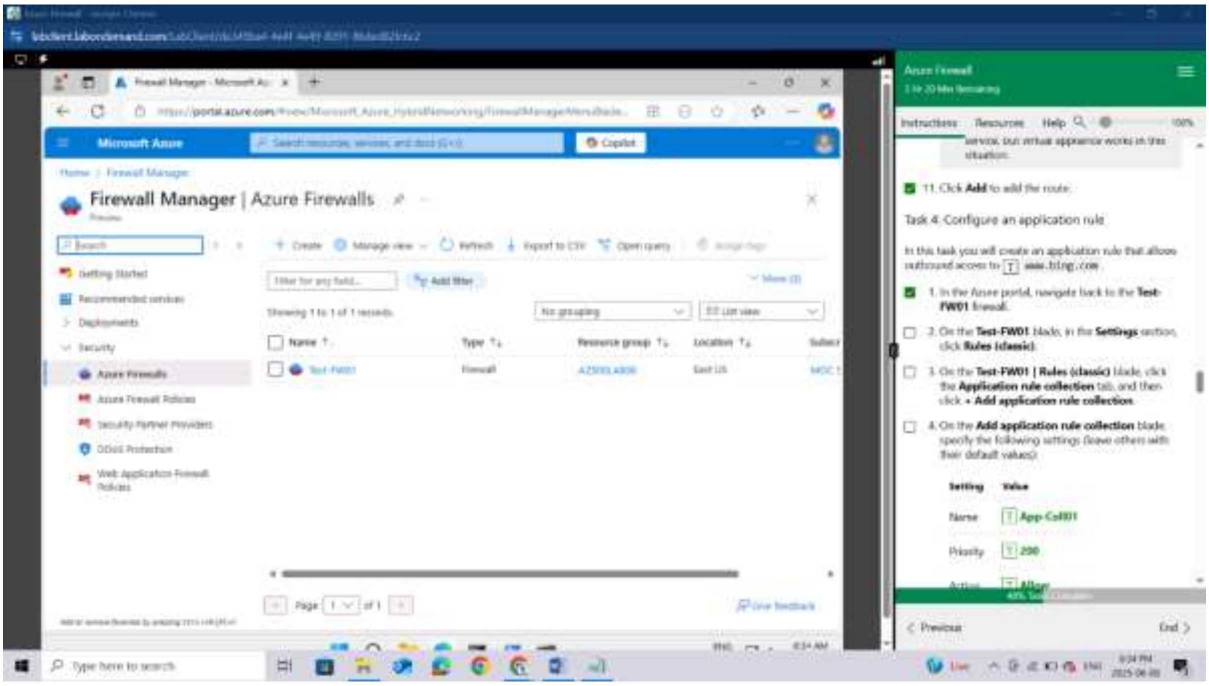
☐ 1. In the Azure portal, navigate back to the **Test-FW01** firewall.

☐ 2. On the **Test-FW01** blade, in the **Settings** section, click **Rules (classic)**.

Task 4: Configure an application rule

In this task you will create an application rule that allows outbound access to www.bing.com.

In the Azure portal, navigate back to the **Test-FW01** firewall.



Firewall Manager | Azure Firewalls

Name	Type	Resource group	Location
Test-FW01	Firewall	AZ500LAB08	East US

Azure Firewall

☑ 11. Click **Add** to add the route.

Task 4: Configure an application rule

In this task you will create an application rule that allows outbound access to www.bing.com.

☑ 1. In the Azure portal, navigate back to the **Test-FW01** firewall.

☐ 2. On the **Test-FW01** blade, in the **Settings** section, click **Rules (classic)**.

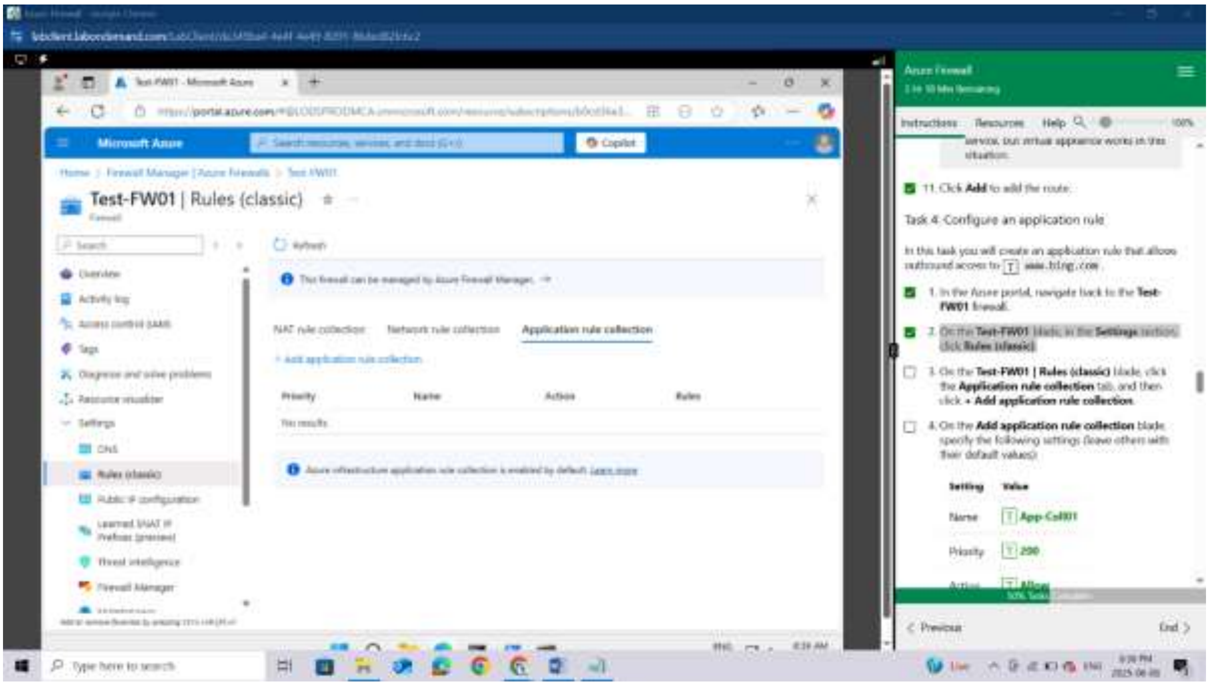
☐ 3. On the **Test-FW01 | Rules (classic)** blade, click the **Application rule collection** tab, and then click **+ Add application rule collection**.

☐ 4. On the **Add application rule collection** blade, specify the following settings (leave others with their default values):

Setting	Value
Name	App-Coll01
Priority	200
Action	Allow

On the **Test-FW01** blade, in the **Settings** section, click **Rules (classic)**.

On the **Test-FW01 | Rules (classic)** blade, click the **Application rule collection** tab, and then click **+ Add application rule collection**.



☑ 11. Click **Add** to add the route.

Task 4: Configure an application rule

In this task you will create an application rule that allows outbound access to www.bing.com.

☑ 1. In the Azure portal, navigate back to the **Test-FW01** firewall.

☑ 2. On the **Test-FW01** blade, in the **Settings** section, click **Rules (classic)**.

□ 3. On the **Test-FW01 | Rules (classic)** blade, click the **Application rule collection** tab, and then click **+ Add application rule collection**.

□ 4. On the **Add application rule collection** blade specify the following settings (leave others with their default values):

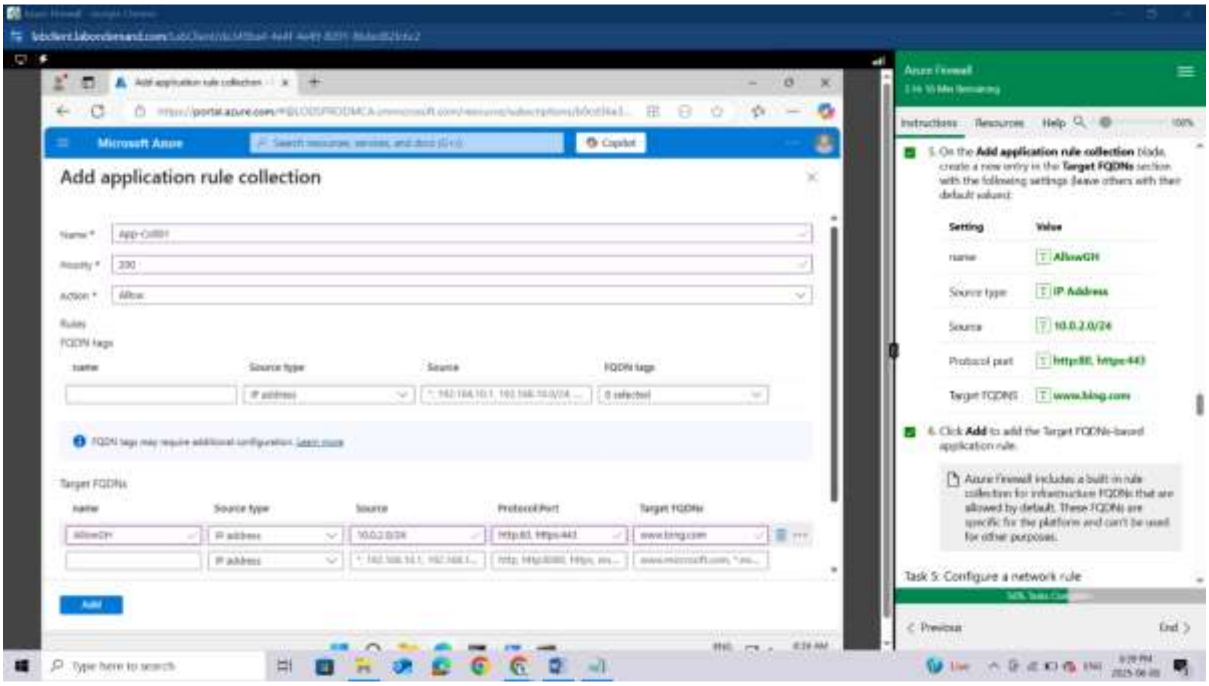
Setting	Value
Name	App-Coll01
Priority	200
Action	Allow

On the **Add application rule collection** blade, specify the following settings (leave others with their default values):

Setting	Value
Name	**App-Coll01**
Priority	**200**
Action	**Allow**

On the **Add application rule collection** blade, create a new entry in the **Target FQDNs** section with the following settings (leave others with their default values):

Setting	Value
name	**AllowGH**
Source type	**IP Address**
Source	**10.0.2.0/24**
Protocol port	**http:80, https:443**
Target FQDNS	**www.bing.com**



Add application rule collection

Name * App-Coll01

Priority * 200

Action * Allow

Target FQDNs

name	Source type	Source	Protocol:Port	Target FQDNs
AllowGH	IP address	10.0.2.0/24	http:80, https:443	www.bing.com

5. On the **Add application rule collection** blade, create a new entry in the **Target FQDNs** section with the following settings (leave others with their default values):

Setting	Value
name	AllowGH
Source type	IP Address
Source	10.0.2.0/24
Protocol port	http:80, https:443
Target FQDNS	www.bing.com

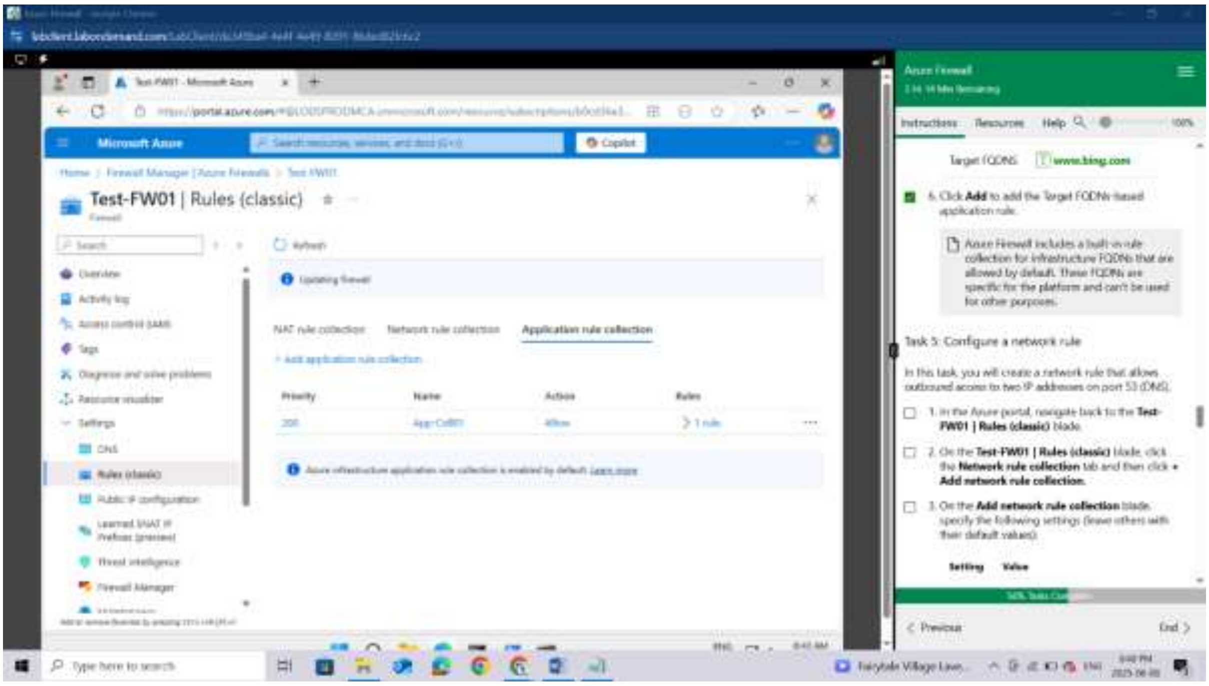
6. Click **Add** to add the Target FQDNs-based application rule.

Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes.

Task 5: Configure a network rule

Click **Add** to add the Target FQDNs-based application rule.

Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes.



Test-FW01 | Rules (classic)

Updating firewall

Priority	Name	Action	Rules
200	App-Coll01	Allow	1 rule

Task 5: Configure a network rule

In this task, you will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

1. In the Azure portal, navigate back to the **Test-FW01 | Rules (classic)** blade.
2. On the **Test-FW01 | Rules (classic)** blade, click the **Network rule collection** tab and then click **+ Add network rule collection**.
3. On the **Add network rule collection** blade, specify the following settings (leave others with their default values):

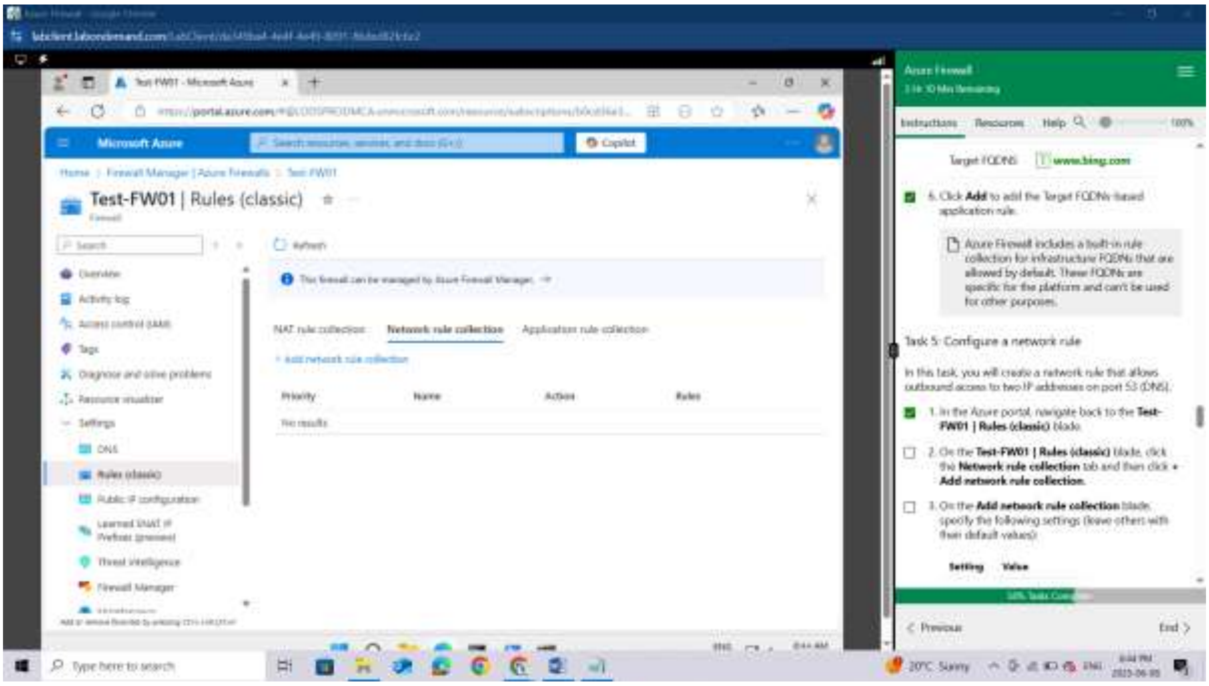
NAT rule collection
Network rule collection
Application rule collection
+ Add application rule collection

Task 5: Configure a network rule

In this task, you will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

In the Azure portal, navigate back to the **Test-FW01 | Rules (classic)** blade.

On the **Test-FW01 | Rules (classic)** blade, click the **Network rule collection** tab and then click **+ Add network rule collection**.



Target FQDNS www.bing.com

☑ 6. Click **Add** to add the Target FQDNs-based application rule.

Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes.

Task 5: Configure a network rule

In this task, you will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

☑ 1. In the Azure portal, navigate back to the **Test-FW01 | Rules (classic)** blade.

☐ 2. On the **Test-FW01 | Rules (classic)** blade, click the **Network rule collection** tab and then click **+ Add network rule collection**.

☐ 3. On the **Add network rule collection** blade, specify the following settings (leave others with their default values):

Setting **Value**

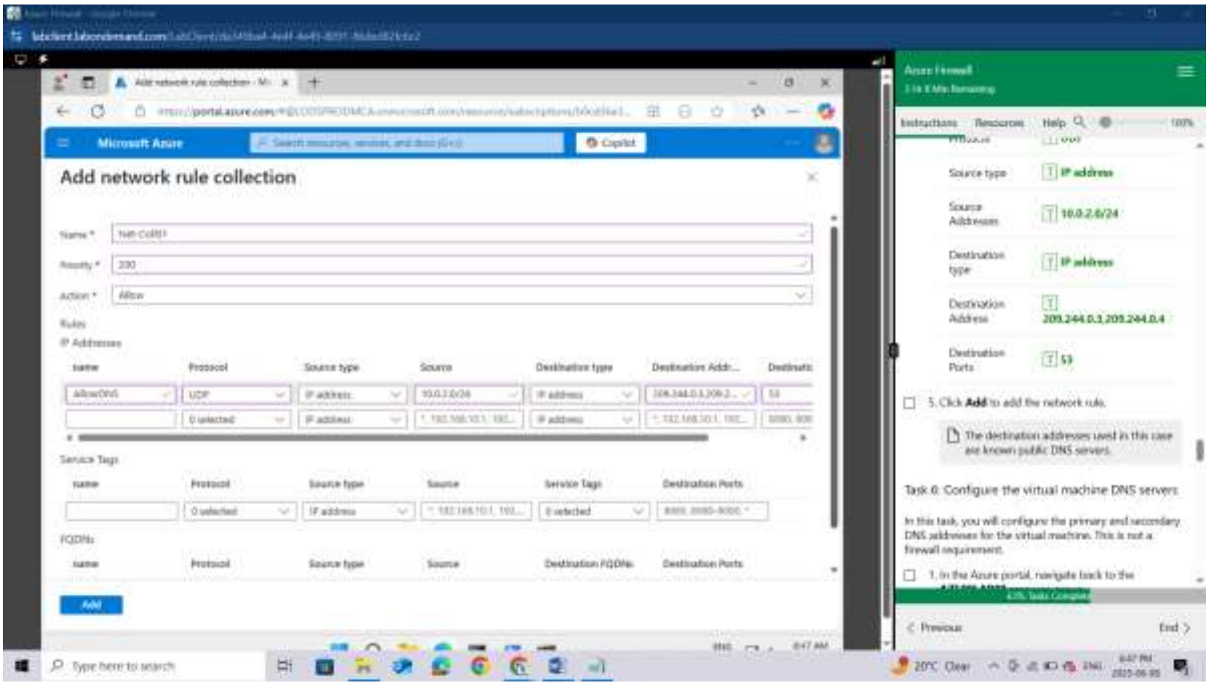
On the **Add network rule collection** blade, specify the following settings (leave others with their default values):

Setting	Value
Name	**Net-Coll01**
Priority	**200**
Action	**Allow**

On the **Add network rule collection** blade, create a new entry in the **IP Addresses** section with the following settings (leave others with their default values):

Setting	Value
Name	**AllowDNS**
Protocol	**UDP**
Source type	**IP address**
Source Addresses	**10.0.2.0/24**
Destination type	**IP address**

Setting	Value
Destination Address	209.244.0.3,209.244.0.4
Destination Ports	53



Add network rule collection

Name * Net-Coll01

Priority * 200

Action * Allow

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addr...	Destinatio
AllowDNS	UDP	IP address	10.0.2.0/24	IP address	209.244.0.3,209.2...	53

Add

Source type IP address

Source Addresses 10.0.2.0/24

Destination type IP address

Destination Address 209.244.0.3,209.244.0.4

Destination Ports 53

□ 5. Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.

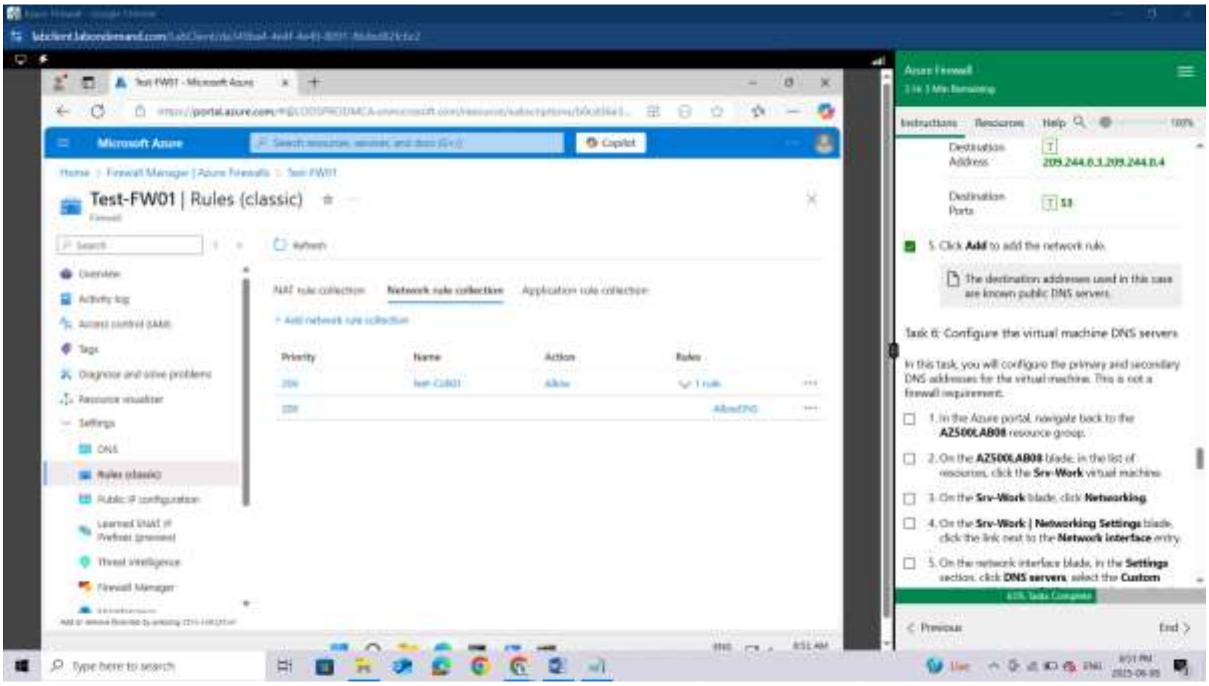
Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

□ 1. In the Azure portal, navigate back to the

Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.



Test-FW01 | Rules (classic)

NAT rule collection | Network rule collection | Application rule collection

+ Add network rule collection

Priority	Name	Action	Rules
200	Net-Coll01	Allow	1 rule
200			AllowDNS

Destination Address 209.244.0.3,209.244.0.4

Destination Ports 53

☑ 5. Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.

Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

□ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

□ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Work** virtual machine.

□ 3. On the **Srv-Work** blade, click **Networking**.

□ 4. On the **Srv-Work | Networking Settings** blade, click the link next to the **Network interface** entry.

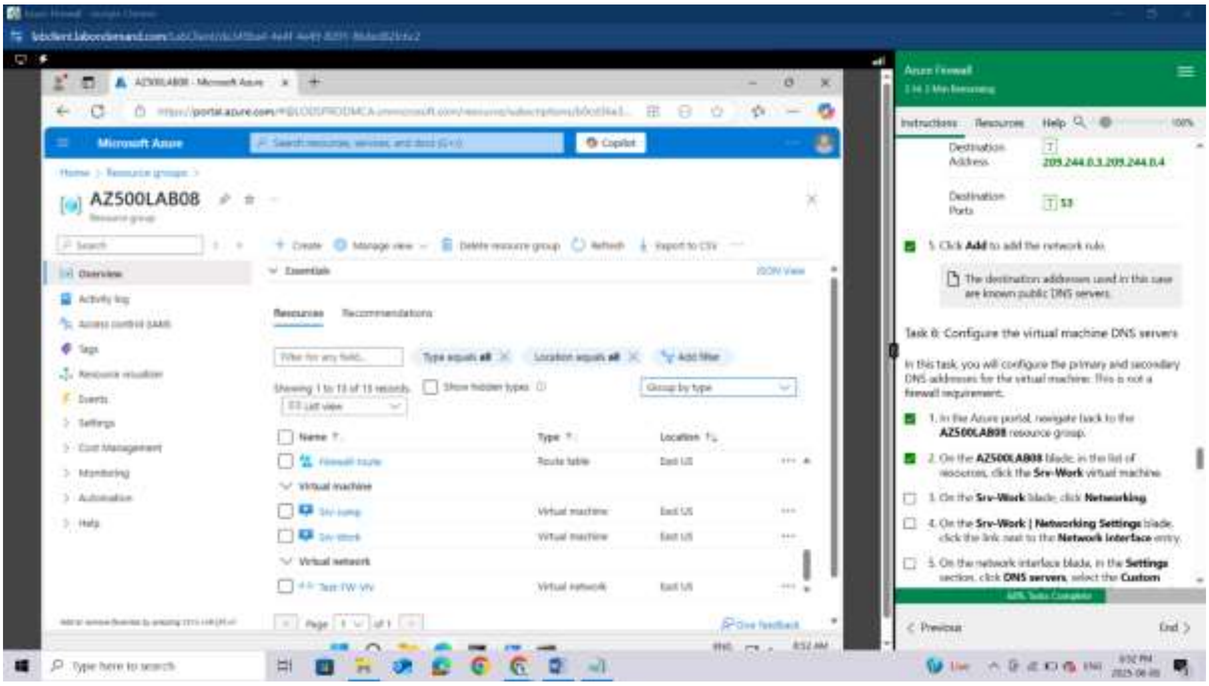
□ 5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom**

Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

In the Azure portal, navigate back to the **AZ500LAB08** resource group.

On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Work** virtual machine.



AZ500LAB08

Resource group

Showing 1 to 13 of 13 records.

Name	Type	Location
Firewall route	Route table	East US
Virtual machine		
Srv-Jump	Virtual machine	East US
Srv-Work	Virtual machine	East US
Virtual network		
Test-FW-VN	Virtual network	East US

Azure Firewall

Destination Address: 209.244.0.3,209.244.0.4

Destination Ports: 53

☑ 5. Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.

Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

☑ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☑ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Work** virtual machine.

☐ 3. On the **Srv-Work** blade, click **Networking**.

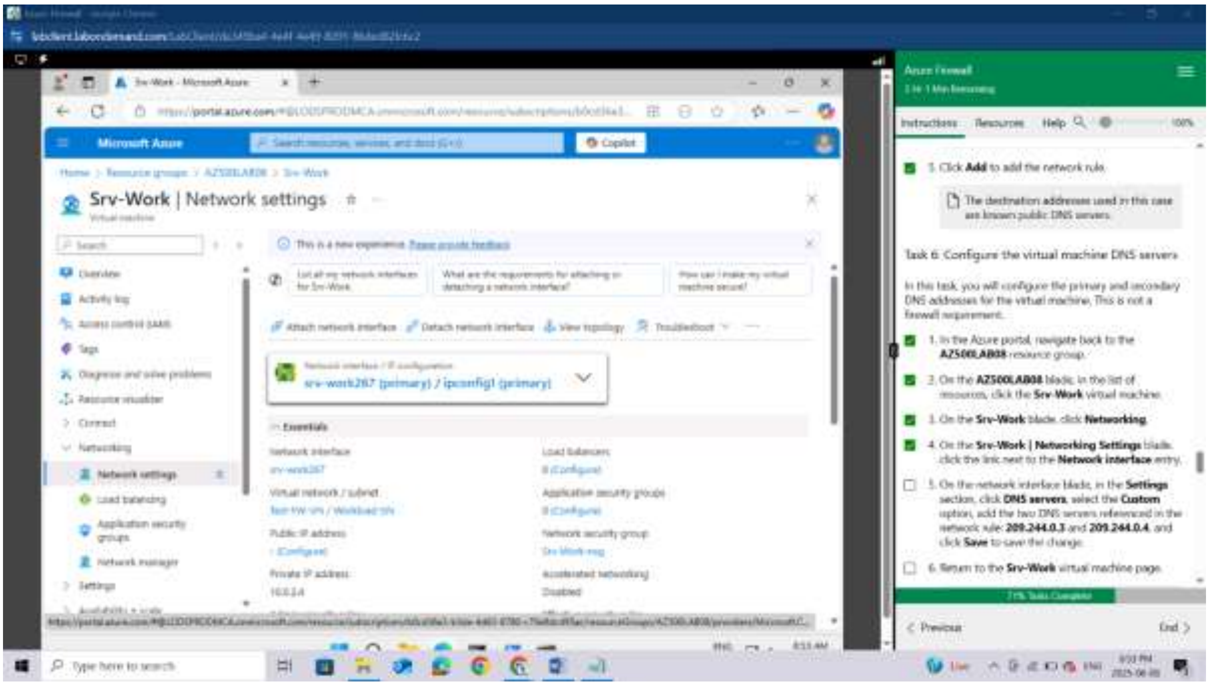
☐ 4. On the **Srv-Work | Networking Settings** blade, click the link next to the **Network interface** entry.

☐ 5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom**

68% Tasks Complete

On the **Srv-Work** blade, click **Networking**.

On the **Srv-Work | Networking Settings** blade, click the link next to the **Network interface** entry.



Srv-Work | Network settings

Virtual machine

This is a new experience. Please provide feedback

List all my network interfaces for Srv-Work

What are the requirements for attaching or detaching a network interface?

How can I make my virtual machine secure?

Network interface / IP configuration: srv-work267 (primary) / ipconfig1 (primary)

Essentials

Network interface: srv-work267

Load balancers: 0 (Configure)

Virtual network / subnet: Test-FW-VN / Workload-SN

Application security groups: 0 (Configure)

Public IP address: - (Configure)

Network security group: Srv-Work-nsg

Private IP address: 10.0.2.4

Accelerated networking: Disabled

Azure Firewall

☑ 5. Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.

Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

☑ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☑ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Work** virtual machine.

☑ 3. On the **Srv-Work** blade, click **Networking**.

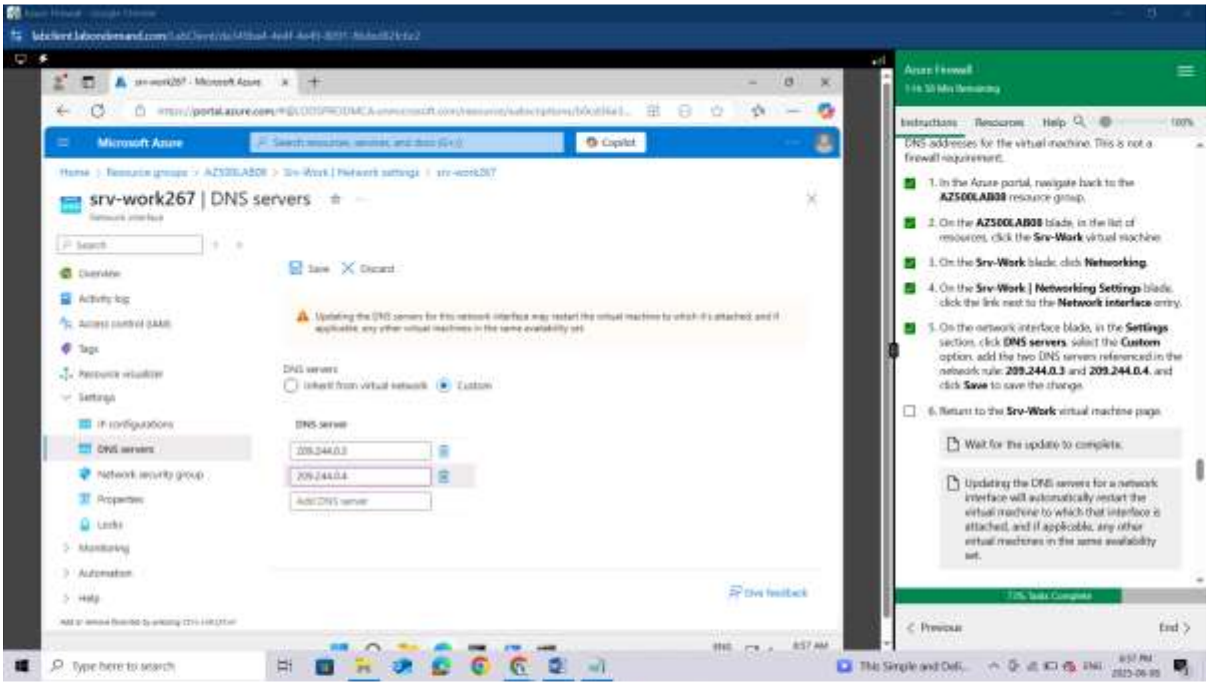
☑ 4. On the **Srv-Work | Networking Settings** blade, click the link next to the **Network interface** entry.

☐ 5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom** option, add the two DNS servers referenced in the network rule: **209.244.0.3** and **209.244.0.4**, and click **Save** to save the change.

☐ 6. Return to the **Srv-Work** virtual machine page.

71% Tasks Complete

On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom** option, add the two DNS servers referenced in the network rule: **209.244.0.3** and **209.244.0.4**, and click **Save** to save the change.



Home > Resource groups > AZ500LAB08 > Srv-Work | Network settings > srv-work267

srv-work267 | DNS servers

Network interface

Save Discard

Updating the DNS servers for this network interface may restart the virtual machine to which it's attached, and if applicable, any other virtual machines in the same availability set.

DNS servers

○ Inherit from virtual network ● Custom

DNS server

209.244.0.3

209.244.0.4

Add DNS server

Azure Firewall

Instructions Resources Help

DNS addresses for the virtual machine. This is not a firewall requirement.

☑ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☑ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Work** virtual machine.

☑ 3. On the **Srv-Work** blade, click **Networking**.

☑ 4. On the **Srv-Work | Networking Settings** blade, click the link next to the **Network interface** entry.

☑ 5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom** option, add the two DNS servers referenced in the network rule: **209.244.0.3** and **209.244.0.4**, and click **Save** to save the change.

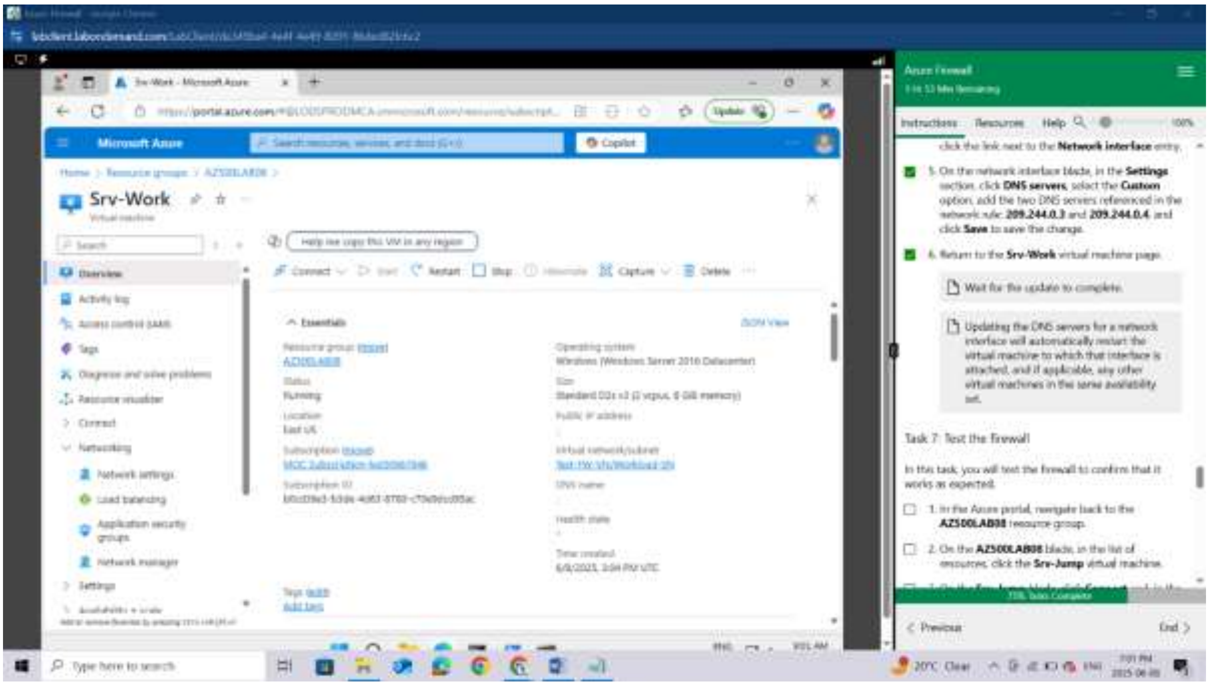
□ 6. Return to the **Srv-Work** virtual machine page.

Wait for the update to complete.

Updating the DNS servers for a network interface will automatically restart the virtual machine to which that interface is attached, and if applicable, any other virtual machines in the same availability set.

Return to the **Srv-Work** virtual machine page.

Wait for the update to complete.
Updating the DNS servers for a network interface will automatically restart the virtual machine to which that interface is attached, and if applicable, any other virtual machines in the same availability set.



Home > Resource groups > AZ500LAB08 >

Srv-Work

Virtual machine

Essentials

Resource group (move): AZ500LAB08

Status: Running

Location: East US

Subscription ID: b0cd39e3-53d4-4083-8780-c70e0ecd95ac

Operating system: Windows (Windows Server 2016 Datacenter)

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

Time created: 6/5/2025, 3:04 PM UTC

Azure Firewall

Instructions Resources Help

click the link next to the **Network interface** entry.

☑ 5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom** option, add the two DNS servers referenced in the network rule: **209.244.0.3** and **209.244.0.4**, and click **Save** to save the change.

☑ 6. Return to the **Srv-Work** virtual machine page.

Wait for the update to complete.

Updating the DNS servers for a network interface will automatically restart the virtual machine to which that interface is attached, and if applicable, any other virtual machines in the same availability set.

Task 7: Test the firewall

In this task, you will test the firewall to confirm that it works as expected.

□ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

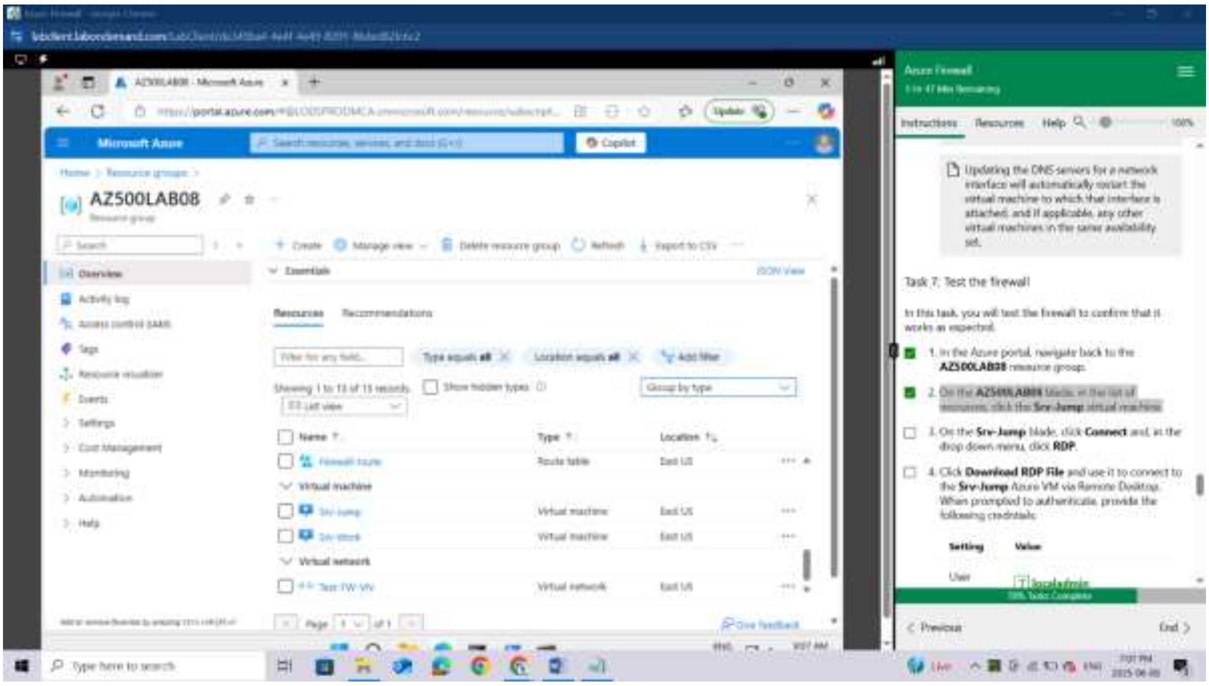
□ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.

Task 7: Test the firewall

In this task, you will test the firewall to confirm that it works as expected.

In the Azure portal, navigate back to the **AZ500LAB08** resource group.

On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.



AZ500LAB08

Resource group

Showing 1 to 13 of 13 records.

Name	Type	Location
Firewall route	Route table	East US
Srv-Jump	Virtual machine	East US
Srv-Work	Virtual machine	East US
Test-FW-VN	Virtual network	East US

Azure Firewall

Instructions Resources Help 100%

Updating the DNS servers for a network interface will automatically restart the virtual machine to which that interface is attached, and if applicable, any other virtual machines in the same availability set.

Task 7: Test the firewall

In this task, you will test the firewall to confirm that it works as expected.

☑ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☑ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.

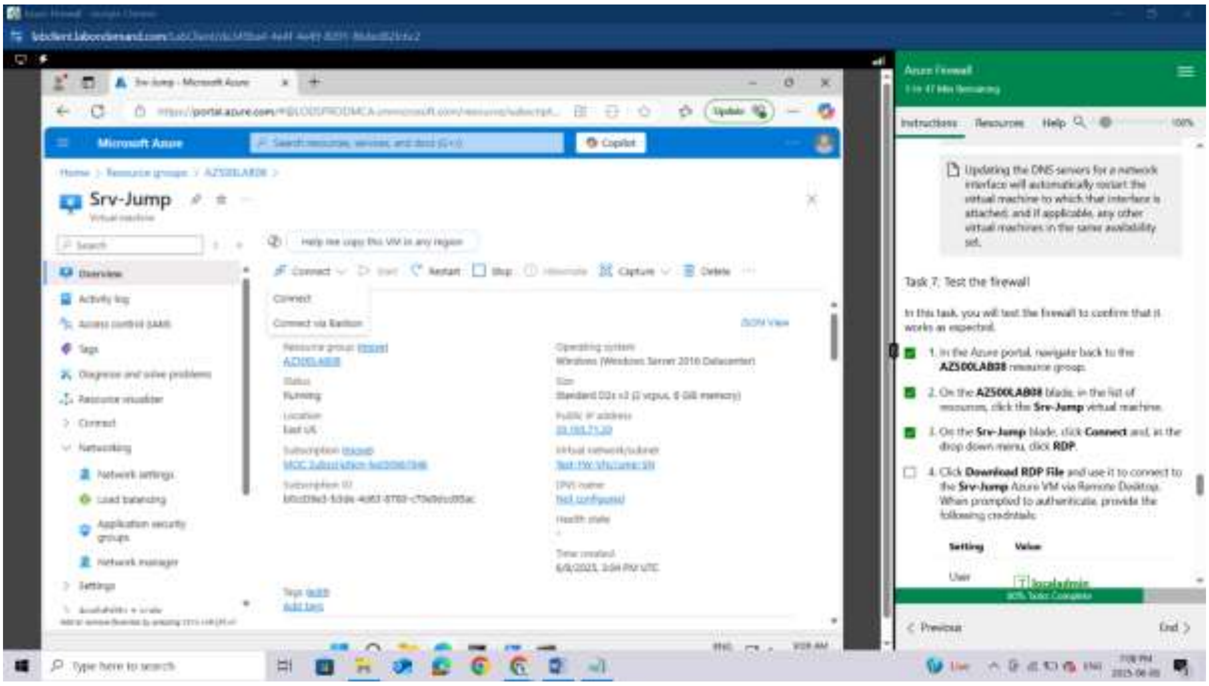
☐ 3. On the **Srv-Jump** blade, click **Connect** and, in the drop down menu, click **RDP**.

☐ 4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credentials:

Setting	Value
User	localadmin

< Previous End >

On the **Srv-Jump** blade, click **Connect** and, in the drop down menu, click **Connect**.



Srv-Jump

Virtual machine

Connect

Connect via Bastion

Resource group (move) : AZ500LAB08

Status : Running

Location : East US

Operating system : Windows (Windows Server 2016 Datacenter)

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

Azure Firewall

Instructions Resources Help 100%

Updating the DNS servers for a network interface will automatically restart the virtual machine to which that interface is attached, and if applicable, any other virtual machines in the same availability set.

Task 7: Test the firewall

In this task, you will test the firewall to confirm that it works as expected.

☑ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☑ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.

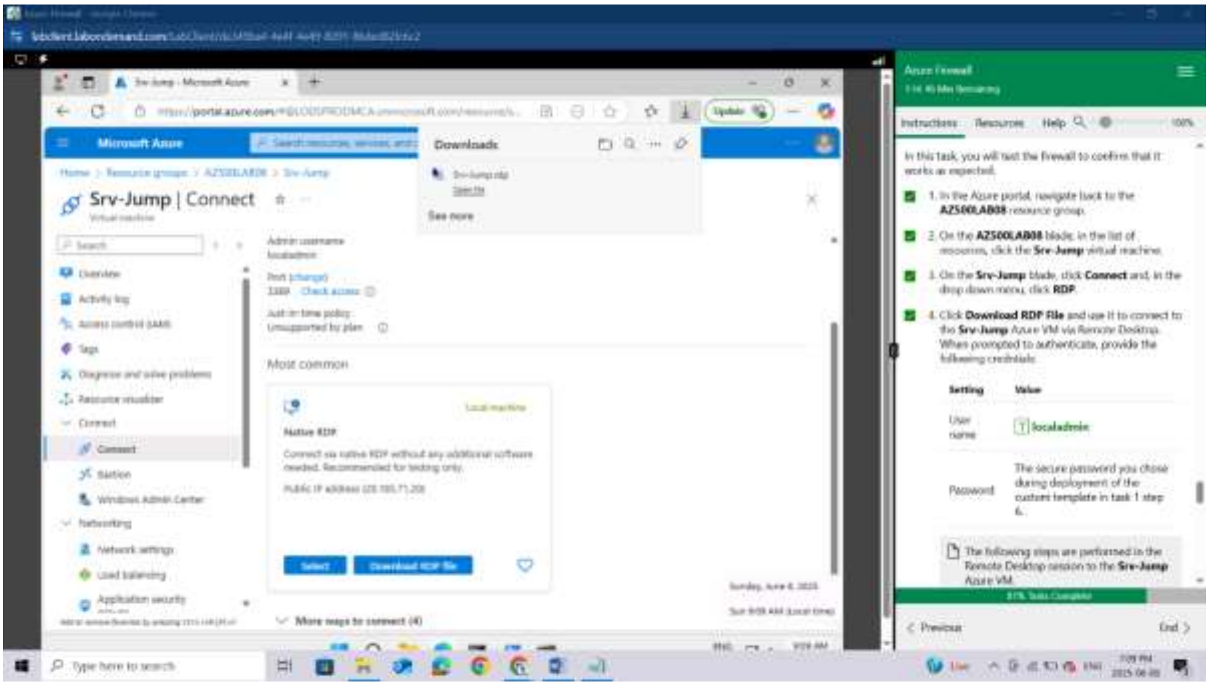
☑ 3. On the **Srv-Jump** blade, click **Connect** and, in the drop down menu, click **RDP**.

☐ 4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credentials:

Setting	Value
User	localadmin

< Previous End >

Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop.



Srv-Jump | Connect

Virtual machine

Home > Resource groups > AZ500LAB08 > Srv-Jump

Admin username
localadmin

Port (change)
3389 Check access

Just-in-time policy
Unsupported by plan

Most common

Native RDP

Local machine

Connect via native RDP without any additional software needed. Recommended for testing only.

Public IP address

Downloads

Srv-Jump.rdp

Azure Firewall

In this task, you will test the firewall to confirm that it works as expected.

☑ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☑ 2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.

☑ 3. On the **Srv-Jump** blade, click **Connect** and, in the drop down menu, click **RDP**.

☑ 4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

Setting	Value
User name	localadmin
Password	The secure password you chose during deployment of the custom template in task 1 step 6.

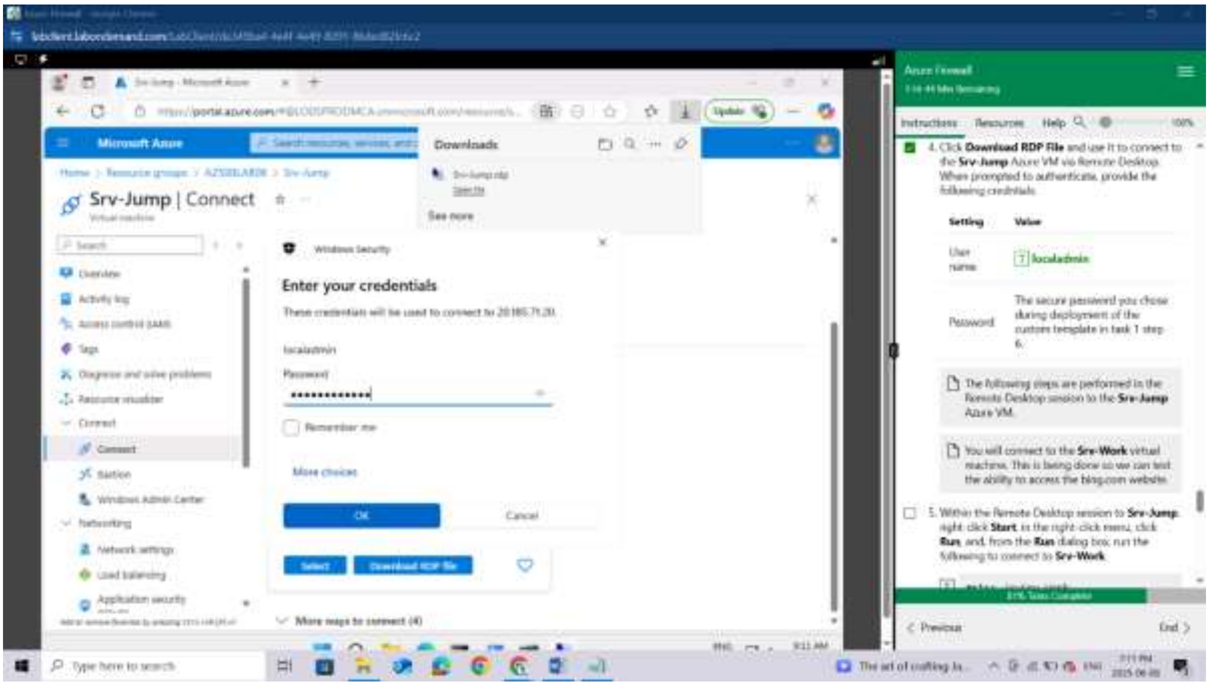
The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.

When prompted to authenticate, provide the following credntials:

Setting	Value
User name	**localadmin**
Password	The secure password you chose during deployment of the custom template in task 1 step 6.

*The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.*

*You will connect to the **Srv-Work** virtual machine. This is being done so we can test the ability to access the bing.com website.*



Windows Security

Enter your credentials

These credentials will be used to connect to 20.185.71.20.

localadmin

Password

•••••••••••••

□ Remember me

More choices

OK Cancel

Azure Firewall

Instructions Resources Help

☑ 4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credentials:

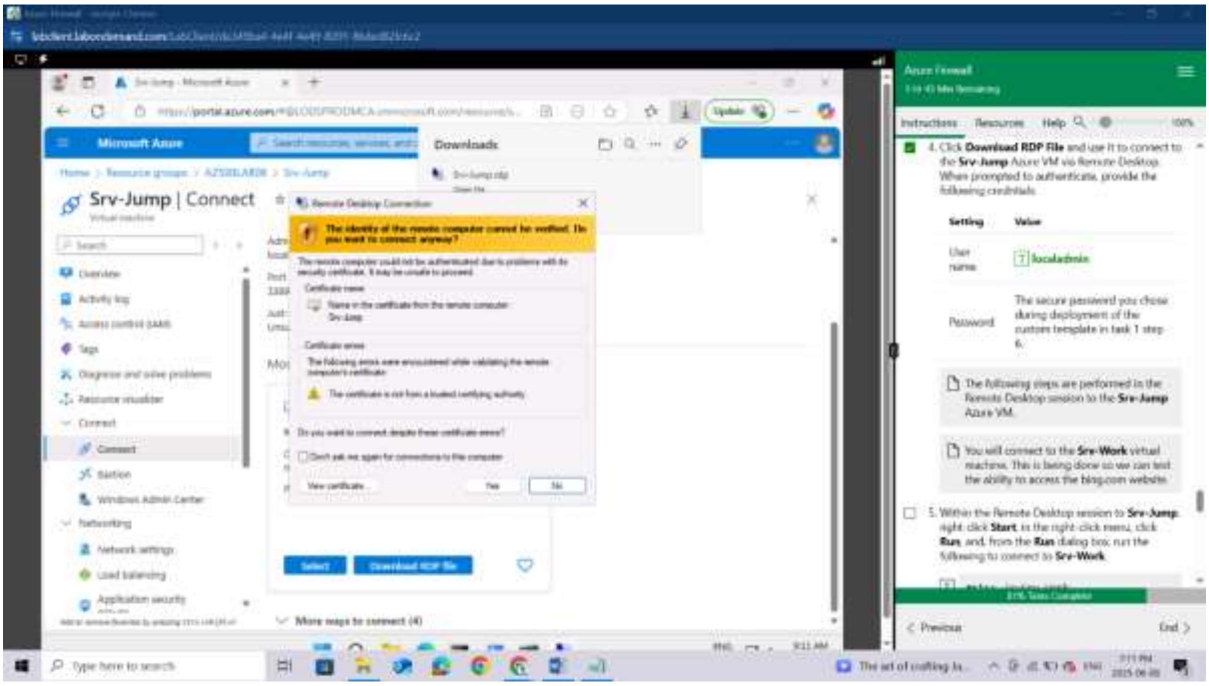
Setting	Value
User name	localadmin
Password	The secure password you chose during deployment of the custom template in task 1 step 6.

The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.

You will connect to the **Srv-Work** virtual machine. This is being done so we can test the ability to access the bing.com website.

□ 5. Within the Remote Desktop session to **Srv-Jump**, right-click **Start**, in the right-click menu, click **Run**, and, from the **Run** dialog box, run the following to connect to **Srv-Work**.

When prompted click **YES**



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Srv-Jump

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

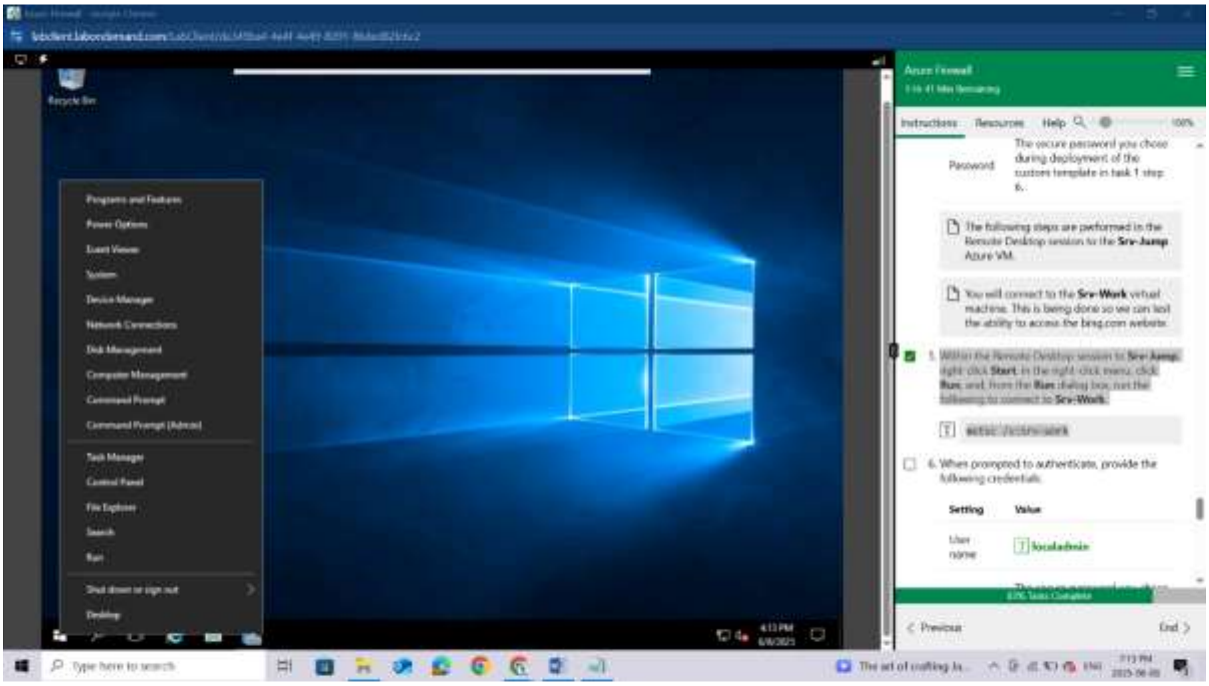
The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

View certificate... Yes No

Within the Remote Desktop session to **Srv-Jump**, right-click **Start**, in the right-click menu, click **Run**,



Password	The secure password you chose during deployment of the custom template in task 1 step 6..

The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.

You will connect to the **Srv-Work** virtual machine. This is being done so we can test the ability to access the bing.com website.

☑ 5. Within the Remote Desktop session to **Srv-Jump**, right-click **Start**, in the right-click menu, click **Run**, and, from the **Run** dialog box, run the following to connect to **Srv-Work**.

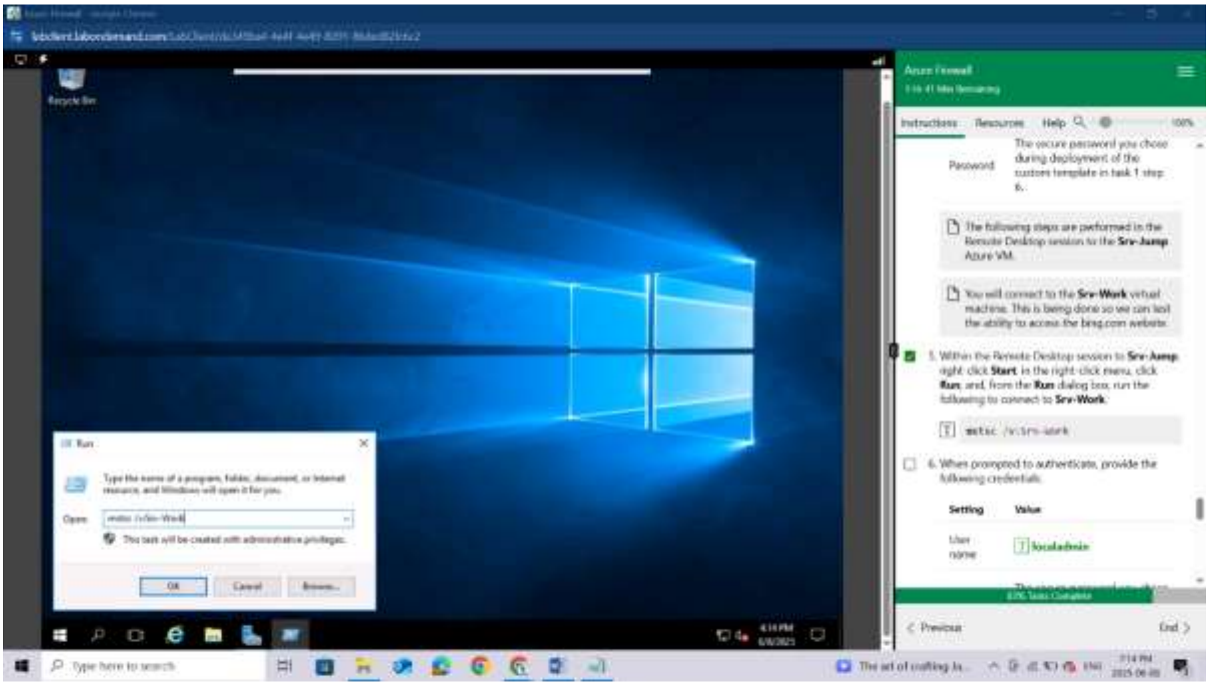
```
mstsc /v:Srv-Work
```

□ 6. When prompted to authenticate, provide the following credentials:

Setting	Value
User name	localadmin

and, from the **Run** dialog box, run the following to connect to **Srv-Work**.

mstsc /v:Srv-Work



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mstsc /v:Srv-Work

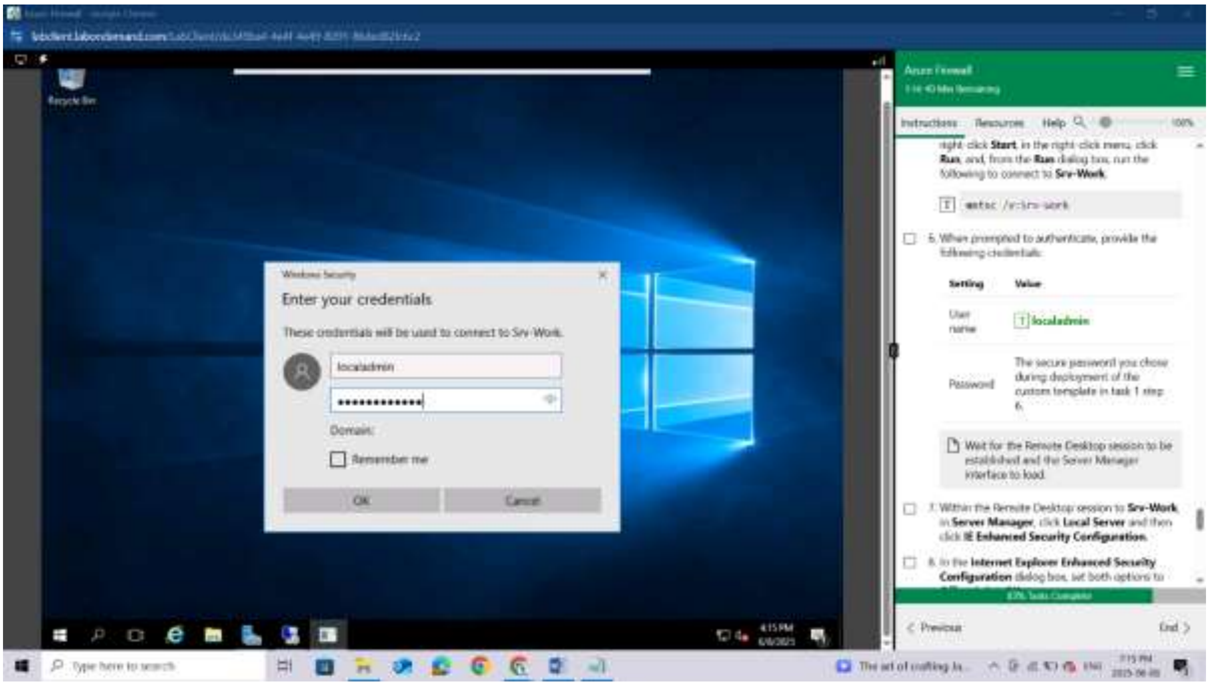
This task will be created with administrative privileges.

When prompted to authenticate, provide the following credentials:

Setting	Value
User name	**localadmin**

Setting	Value
Password	The secure password you chose during deployment of the custom template in task 1 step 6.

Wait for the Remote Desktop session to be established and the Server Manager interface to load.



Windows Security

Enter your credentials

These credentials will be used to connect to Srv-Work.

localadmin

••••••••••••

Domain:

□ Remember me

OK Cancel

right-click **Start**, in the right-click menu, click **Run**, and, from the **Run** dialog box, run the following to connect to **Srv-Work**.

```
mstsc /v:Srv-Work
```

□ 6. When prompted to authenticate, provide the following credentials:

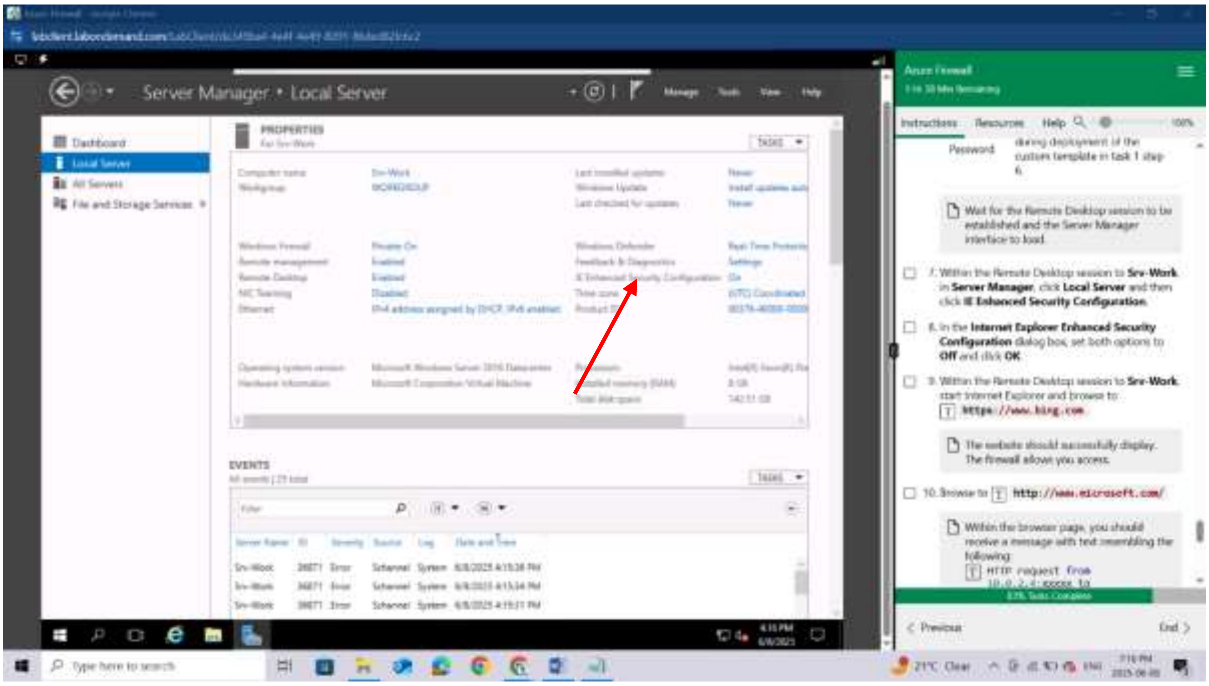
Setting	Value
User name	localadmin
Password	The secure password you chose during deployment of the custom template in task 1 step 6.

Wait for the Remote Desktop session to be established and the Server Manager interface to load.

□ 7. Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.

□ 8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to

Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.



Computer name	Srv-Work	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Install updates automatically
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Defender	Real-Time Protection
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	[illegible]
Operating system version	Microsoft Windows Server 2016 Datacenter	Processors	Intel(R) Xeon(R)
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	8 GB
		Total disk space	[illegible]

Password — during deployment of the custom template in task 1 step 6.

Wait for the Remote Desktop session to be established and the Server Manager interface to load.

□ 7. Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.

□ 8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.

□ 9. Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to

```
https://www.bing.com
```

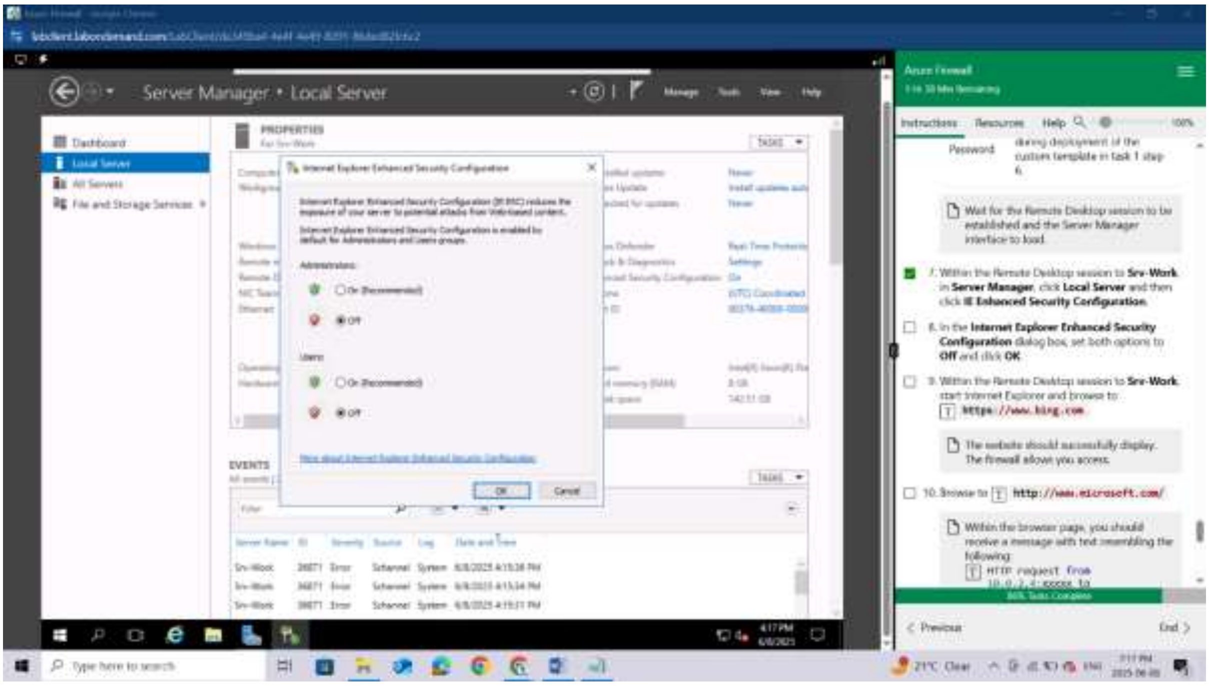
The website should successfully display. The firewall allows you access.

□ 10. Browse to `http://www.microsoft.com/`

Within the browser page, you should receive a message with text resembling the following:

```
HTTP request from 10.0.2.4:xxxxx to
```

In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.



Server Manager • Local Server

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

○ On (Recommended)

● Off

OK Cancel

Server Name	ID	Severity	Source	Log	Date and Time
Srv-Work	36871	Error	Schannel	System	6/8/2025 4:15:38 PM
Srv-Work	36871	Error	Schannel	System	6/8/2025 4:15:34 PM
Srv-Work	36871	Error	Schannel	System	6/8/2025 4:15:31 PM

Azure Firewall

Password — during deployment of the custom template in task 1 step 6.

Wait for the Remote Desktop session to be established and the Server Manager interface to load.

☑ 7. Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.

☐ 8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.

☐ 9. Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to `https://www.bing.com`

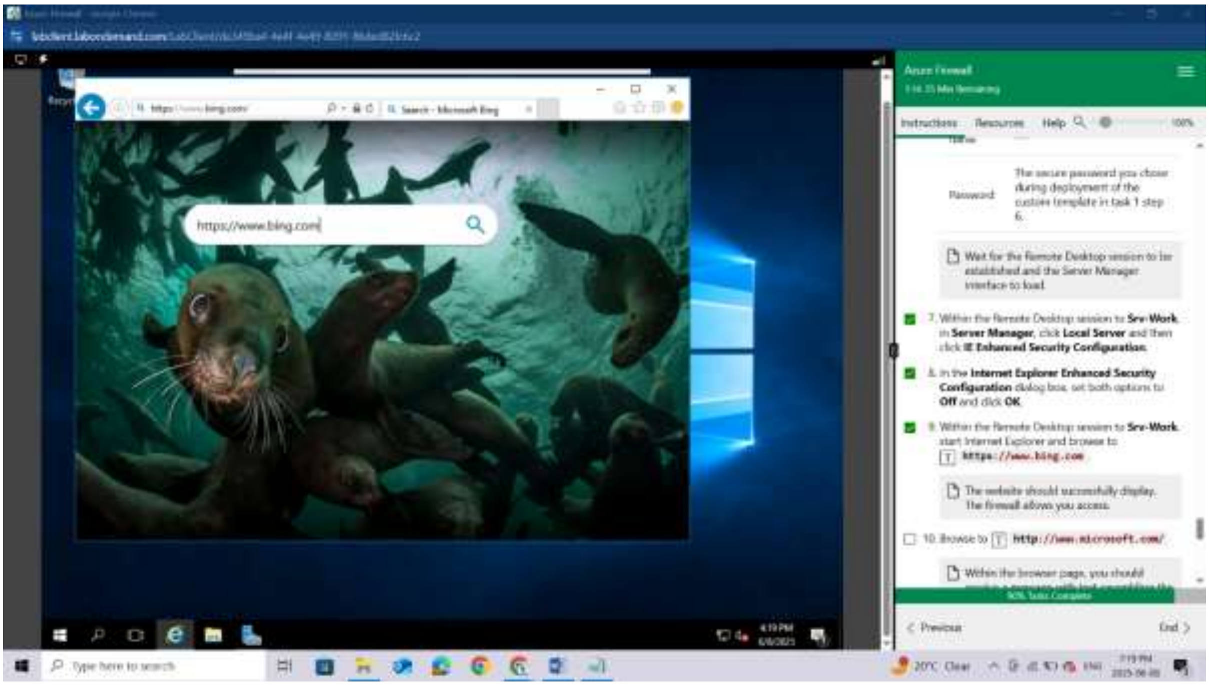
The website should successfully display. The firewall allows you access.

☐ 10. Browse to `http://www.microsoft.com/`

Within the browser page, you should receive a message with text resembling the following: `HTTP request from 10.0.2.4:xxxxx to`

Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to https://www.bing.com.

The website should successfully display. The firewall allows you access.



https://www.bing.com

Azure Firewall

Password — The secure password you chose during deployment of the custom template in task 1 step 6.

Wait for the Remote Desktop session to be established and the Server Manager interface to load.

☑ 7. Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.

☑ 8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.

☑ 9. Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to `https://www.bing.com`

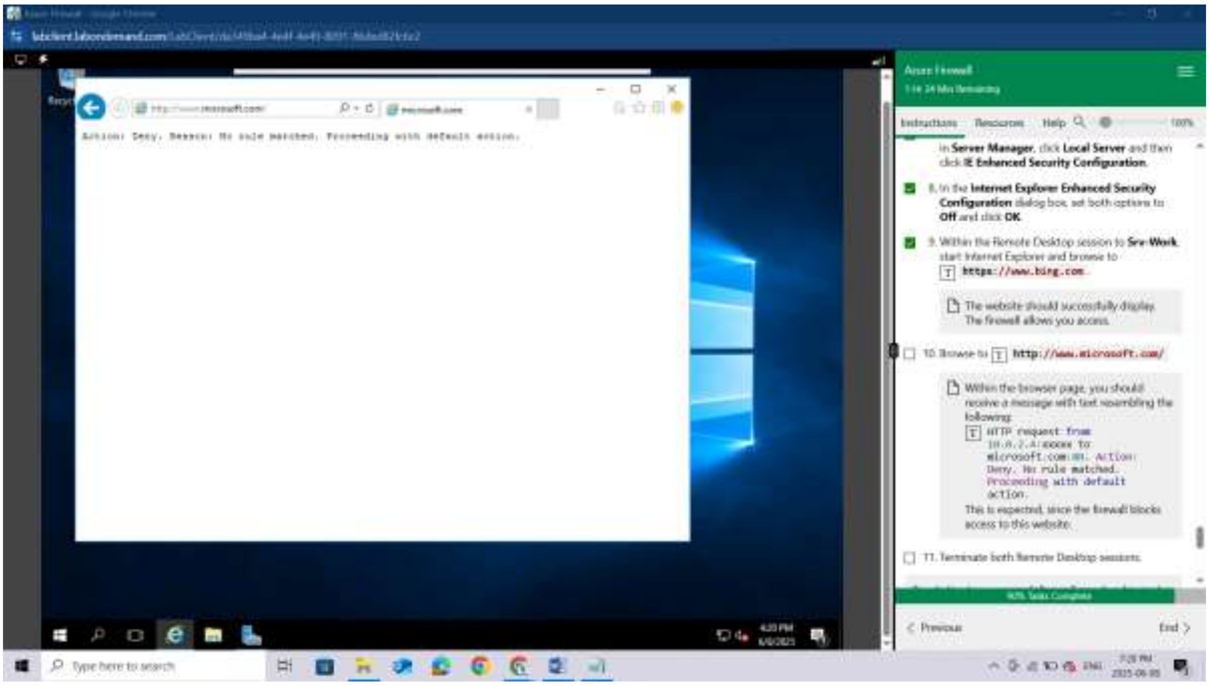
The website should successfully display. The firewall allows you access.

☐ 10. Browse to `http://www.microsoft.com/`

Within the browser page, you should

Browse to **http://www.microsoft.com/**

Within the browser page, you should receive a message with text resembling the following: HTTP request from 10.0.2.4:xxxxx to microsoft.com:80. Action: Deny. No rule matched. Proceeding with default action. This is expected, since the firewall blocks access to this website.



http://www.microsoft.com/

```
Action: Deny. Reason: No rule matched. Proceeding with default action.
```

Azure Firewall

Instructions Resources Help

In **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.

☑ 8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.

☑ 9. Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to `https://www.bing.com`.

The website should successfully display. The firewall allows you access.

□ 10. Browse to `http://www.microsoft.com/`

Within the browser page, you should receive a message with text resembling the following:

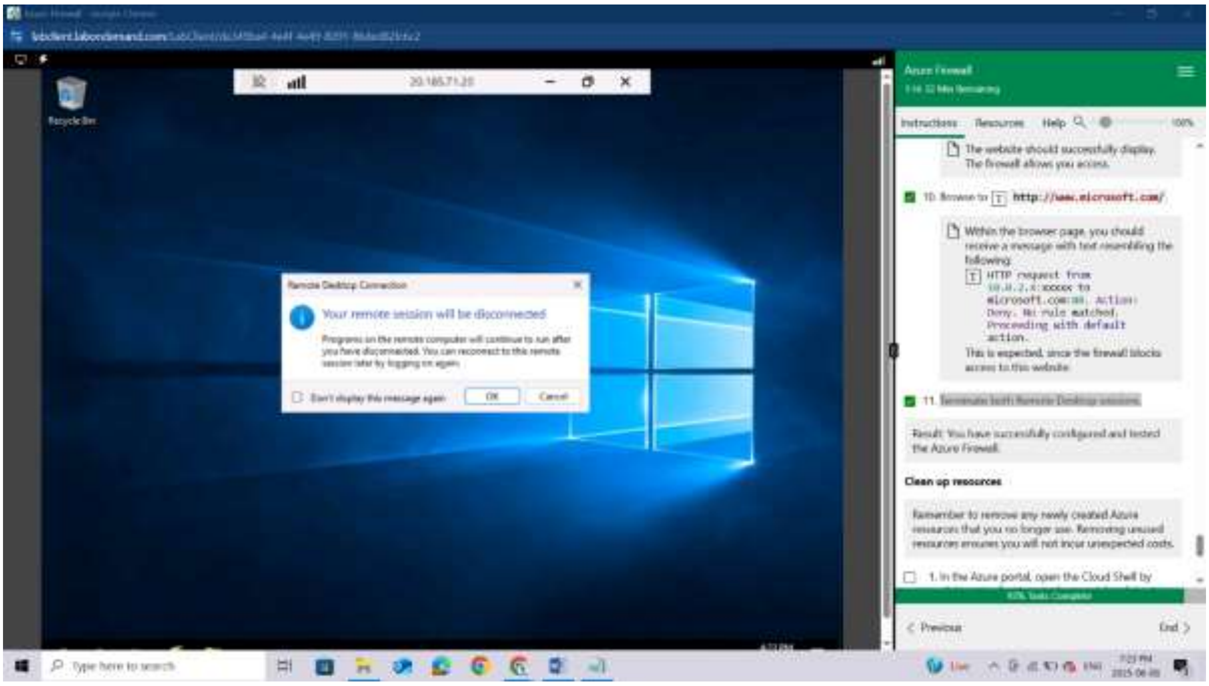
```
HTTP request from
10.0.2.4:xxxxx to
microsoft.com:80. Action:
Deny. No rule matched.
Proceeding with default
action.
```

This is expected, since the firewall blocks access to this website.

□ 11. Terminate both Remote Desktop sessions.

Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.



Remote Desktop Connection

Your remote session will be disconnected

Programs on the remote computer will continue to run after you have disconnected. You can reconnect to this remote session later by logging on again.

□ Don't display this message again OK Cancel

Azure Firewall

The website should successfully display. The firewall allows you access.

☑ 10. Browse to `http://www.microsoft.com/`

Within the browser page, you should receive a message with text resembling the following:

```
HTTP request from
10.0.2.4:xxxxx to
microsoft.com:80. Action:
Deny. No rule matched.
Proceeding with default
action.
```

This is expected, since the firewall blocks access to this website.

☑ 11. Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.

Clean up resources

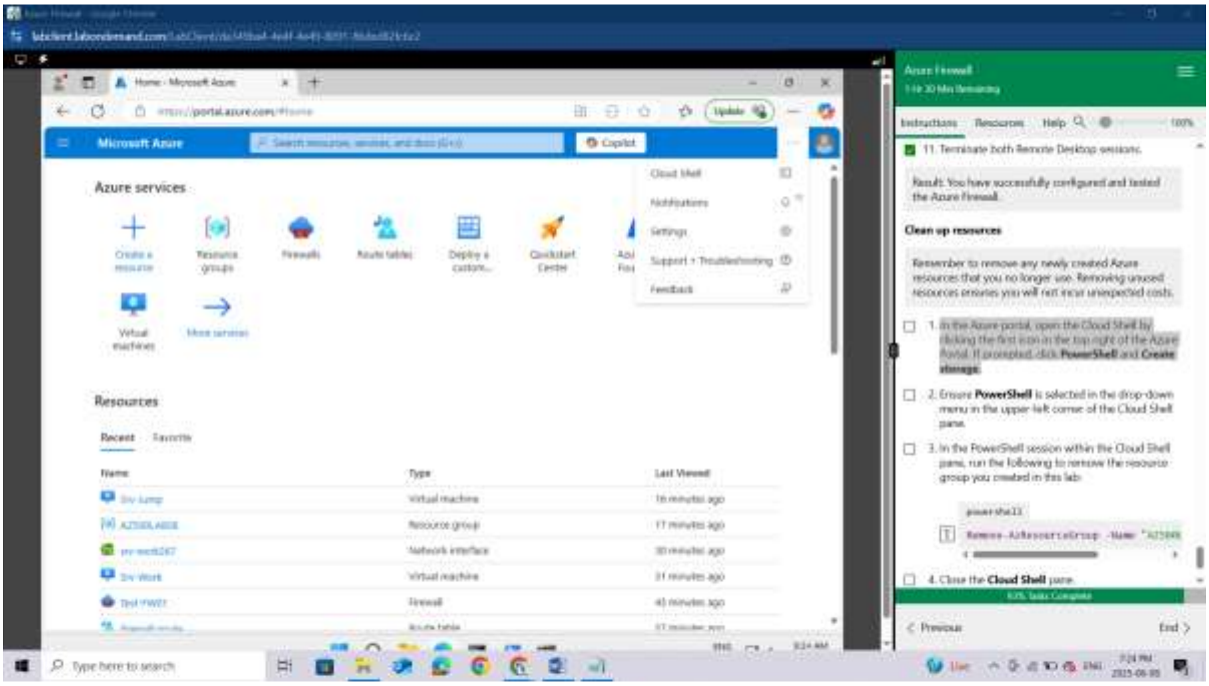
Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not incur unexpected costs.

□ 1. In the Azure portal, open the Cloud Shell by

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.

In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal.



Name	Type	Last Viewed
Srv-Jump	Virtual machine	16 minutes ago
AZ500LAB08	Resource group	17 minutes ago
srv-work287	Network interface	30 minutes ago
Srv-Work	Virtual machine	31 minutes ago
Test-FW01	Firewall	40 minutes ago

Azure Firewall
1 Hr 30 Min Remaining

Instructions Resources Help 100%

☑ 11. Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.

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. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

☐ 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:

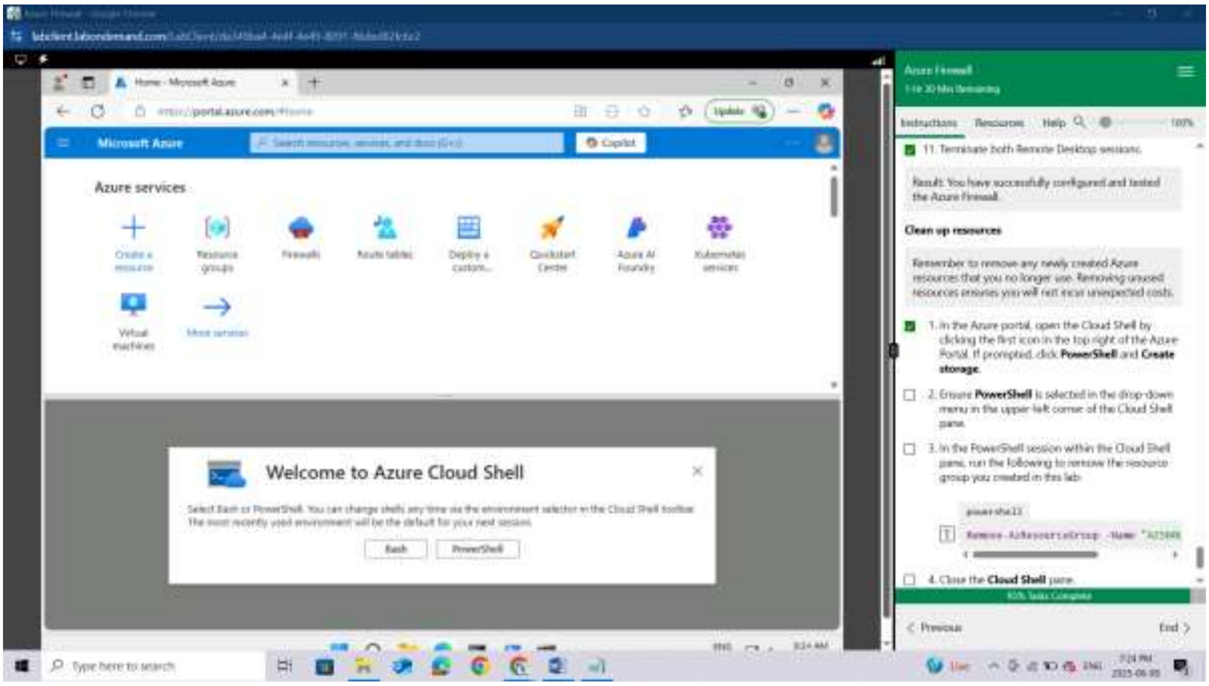
```
Remove-AzResourceGroup -Name "AZ500L
```

☐ 4. Close the **Cloud Shell** pane.

93% Tasks Complete

< Previous End >

If prompted, click **PowerShell** and **Create storage**.



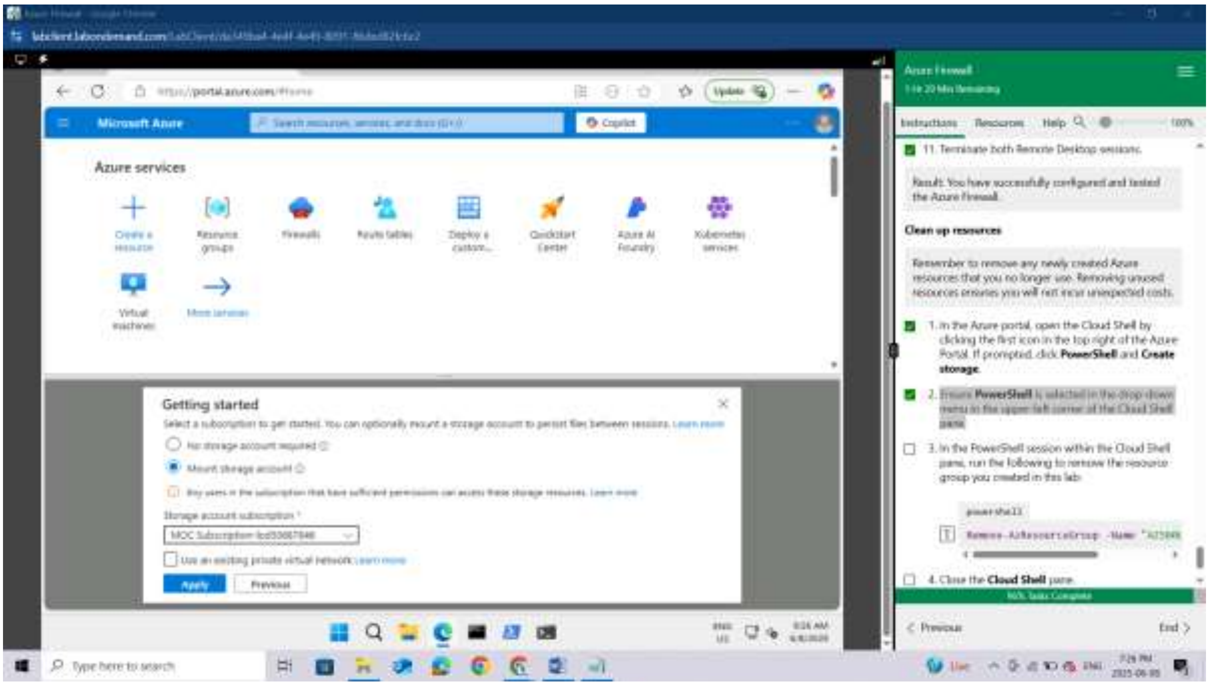
Welcome to Azure Cloud Shell

Select Bash or PowerShell. You can change shells any time via the environment selector in the Cloud Shell toolbar. The most recently used environment will be the default for your next session.

Bash PowerShell

☑ 1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

I will guide through the process of creating your storage



https://portal.azure.com/#home

Microsoft Azure

Azure services

Getting started

Select a subscription to get started. You can optionally mount a storage account to persist files between sessions. Learn more

○ No storage account required

● Mount storage account

Any users in the subscription that have sufficient permissions can access these storage resources. Learn more

Storage account subscription *

MOC Subscription-lod53087848

□ Use an existing private virtual network. Learn more

Azure Firewall

1 Hr 20 Min Remaining

☑ 11. Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.

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. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

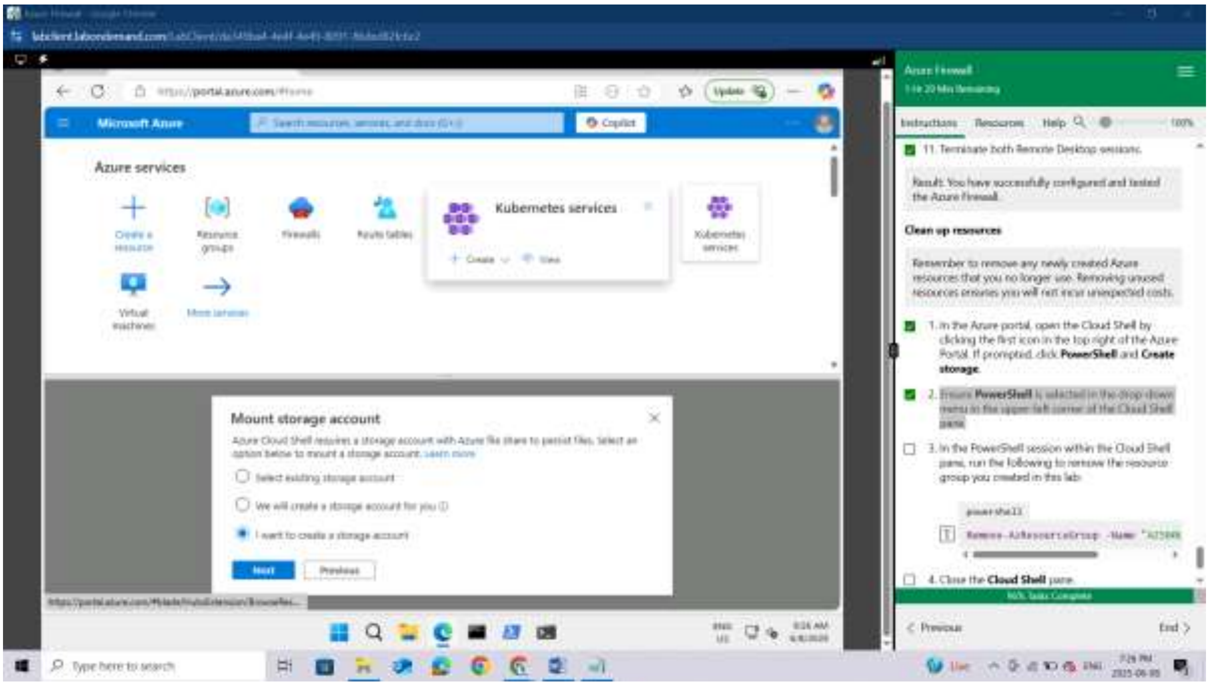
☑ 2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

□ 3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

```
powershell
Remove-AzResourceGroup -Name "AZ500
```

□ 4. Close the **Cloud Shell** pane.

90% Tasks Complete



https://portal.azure.com/#home

Microsoft Azure

Azure services

Mount storage account

Azure Cloud Shell requires a storage account with Azure file share to persist files. Select an option below to mount a storage account. Learn more

○ Select existing storage account

○ We will create a storage account for you

● I want to create a storage account

Azure Firewall

1 Hr 20 Min Remaining

☑ 11. Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.

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. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

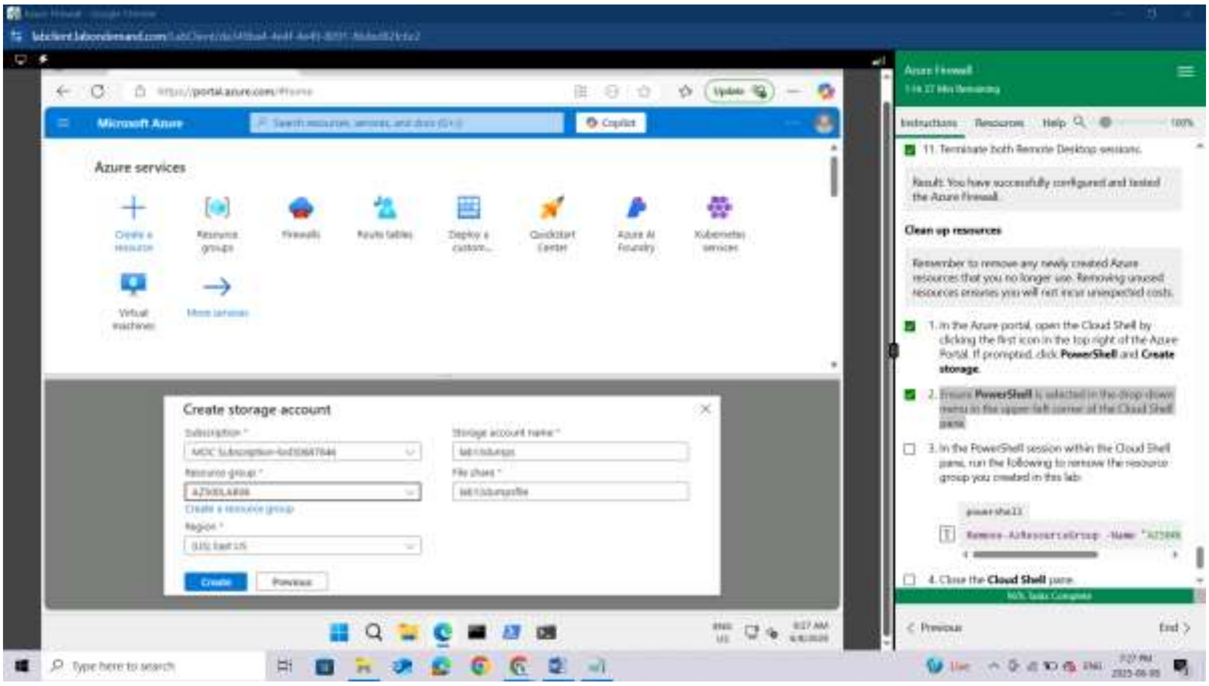
☑ 2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

□ 3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

powershell
Remove-AzResourceGroup -Name "AZ500

□ 4. Close the **Cloud Shell** pane.

90% Tasks Complete



Create storage account

Subscription *: MOC Subscription-[illegible]

Resource group *: AZ500LAB08

Create a resource group

Region *: (US) East US

Storage account name *: [illegible]

File share *: [illegible]

Create Previous

Azure Firewall

11. Terminate both Remote Desktop sessions.

Result: You have successfully configured and tested the Azure Firewall.

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. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

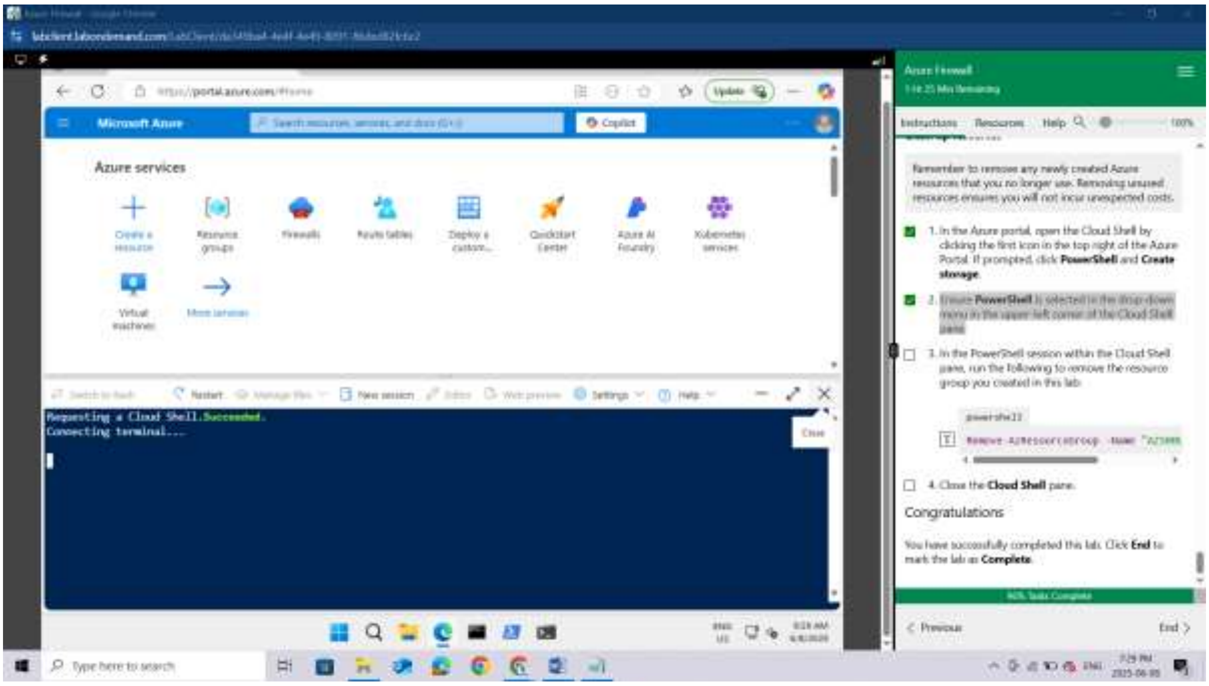
☑ 2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

□ 3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

```
powershell
Remove-AzResourceGroup -Name "AZ500
```

□ 4. Close the **Cloud Shell** pane.

Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.



```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...
```

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

☑ 1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

☑ 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:

```
powershell
Remove-AzResourceGroup -Name "AZ500
```

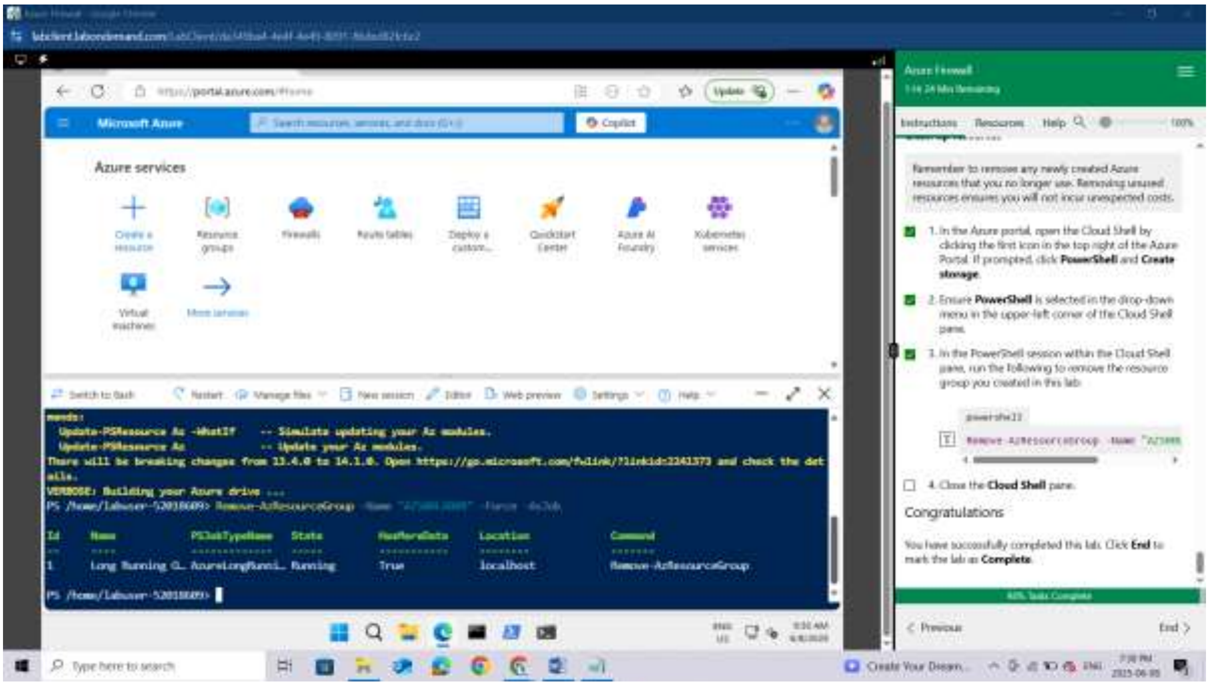
□ 4. Close the **Cloud Shell** pane.

Congratulations

You have successfully completed this lab. Click **End** to mark the lab as **Complete**.

In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

```
powershell
Remove-AzResourceGroup -Name "AZ500LAB08" -Force -AsJob
```



```
mands:
  Update-PSResource Az -WhatIf    -- Simulate updating your Az modules.
  Update-PSResource Az            -- Update your Az modules.
There will be breaking changes from 13.4.0 to 14.1.0. Open https://go.microsoft.com/fwlink/?linkid=2241373 and check the det
ails.
VERBOSE: Building your Azure drive ...
PS /home/labuser-52018609> Remove-AzResourceGroup -Name "AZ500LAB08" -Force -AsJob

Id     Name            PSJobTypeName     State         HasMoreData     Location             Command
--     ----            -------------     -----         -----------     --------             -------
1      Long Running O… AzureLongRunni… Running       True            localhost            Remove-AzResourceGroup

PS /home/labuser-52018609> 
```

Azure Firewall
1:14 24 Min Remaining

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

☑ 1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

☑ 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:

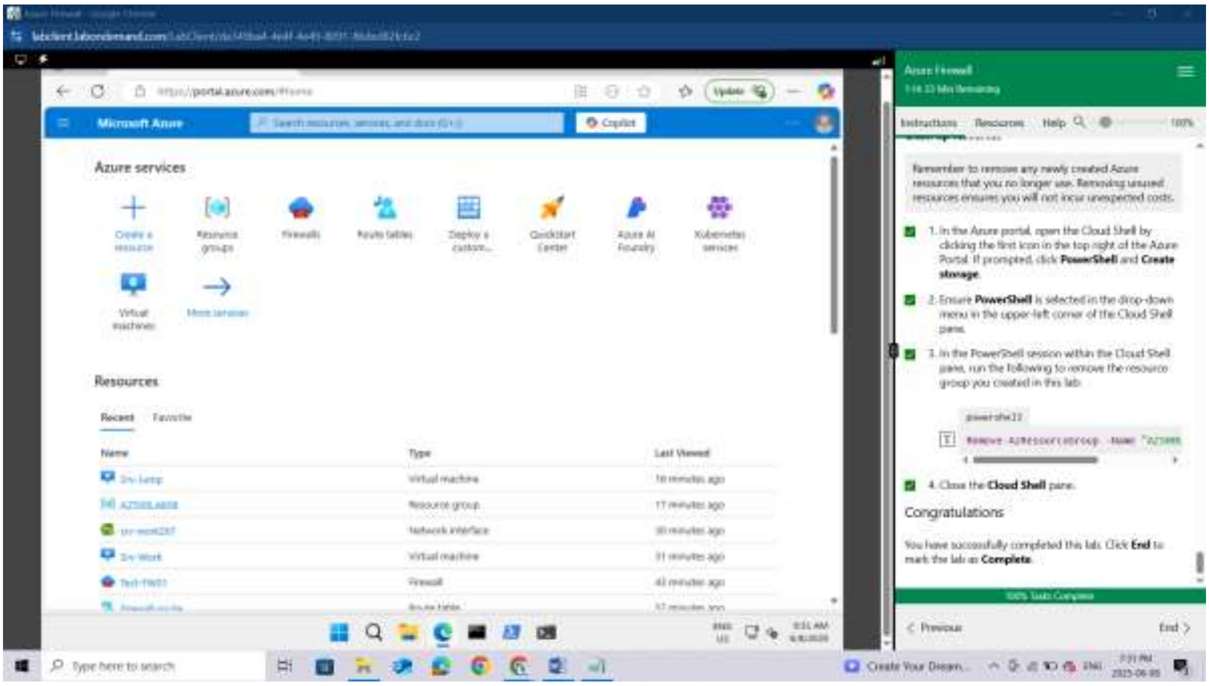
```
powershell
Remove-AzResourceGroup -Name "AZ500
```

□ 4. Close the **Cloud Shell** pane.

Congratulations

You have successfully completed this lab. Click **End** to mark the lab as **Complete**.

Close the **Cloud Shell** pane.



Resources

Name	Type	Last Viewed
Srv-Jump	Virtual machine	16 minutes ago
AZ500LAB08	Resource group	17 minutes ago
srv-work287	Network interface	30 minutes ago
Srv-Work	Virtual machine	31 minutes ago
Test-FW01	Firewall	43 minutes ago
Firewall-route	Route table	57 minutes ago

Azure Firewall
1:14 23 Min Remaining

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

☑ 1. In the Azure portal, open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, click **PowerShell** and **Create storage**.

☑ 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:

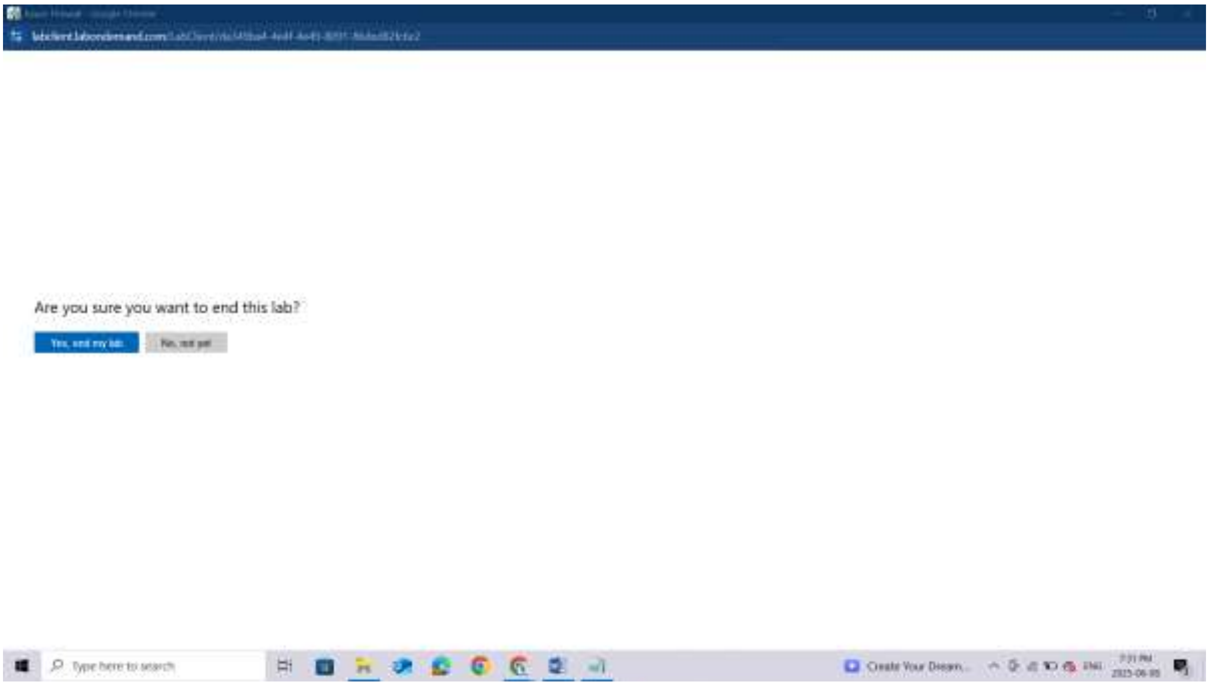
powershell
Remove-AzResourceGroup -Name "AZ500

☑ 4. Close the **Cloud Shell** pane.

Congratulations

You have successfully completed this lab. Click **End** to mark the lab as **Complete**.

Congratulations. You have successfully completed this lab. Click **End** to mark the lab as **Complete**.



Are you sure you want to end this lab?

Conclusion

Completing this lab provided valuable hands-on experience with **Azure Firewall**, reinforcing its role as a critical component in securing Azure network infrastructure. By deploying the firewall, configuring routing, setting up application and network rules, and customizing DNS settings, we gained a deeper understanding of how traffic can be effectively controlled and monitored within a cloud environment. Through testing, we validated the firewall's ability to enforce security policies and restrict unauthorized access, demonstrating its effectiveness in protecting Azure resources. This lab not only enhanced our technical skills in managing Azure Firewall but also emphasized best practices in network security—essential for any organization operating in the cloud. Overall, the lab served as a practical and insightful step toward mastering Azure security technologies and preparing for real-world implementation scenarios.