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

Week 8 Assignment 1: Azure Firewall

Introduction

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. One can **centrally** create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. It also integrates with threat intelligence, allowing one to detect and block malicious IPs and domains that have been discovered through threat intelligence research.

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 jump host is typically placed in a public subnet to be accessible from the internet, allowing it to act as a secure gateway to reach servers in private subnets).
- A virtual machine in 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.

Lab objectives

In this lab, you will complete the following exercise:

- Exercise 1: Deploy and test an Azure Firewall

Instructions

Lab files:

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

Exercise 1: Deploy and test an Azure Firewall

In this exercise, you will complete the following tasks:

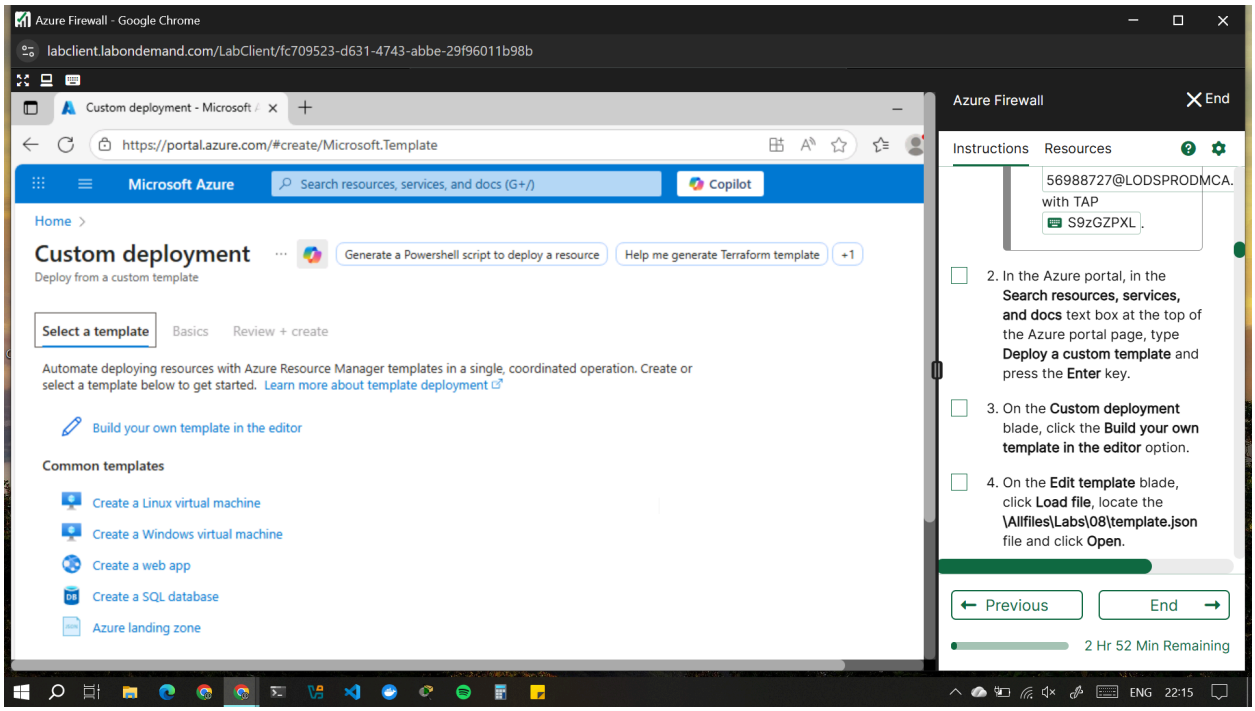
- Task 1: Use a template to deploy the lab environment.
- Task 2: Deploy an Azure firewall.
- Task 3: Create a default route.
- Task 4: Configure an application rule.
- Task 5: Configure a network rule.
- Task 6: Configure DNS servers.
- Task 7: Test the firewall.

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

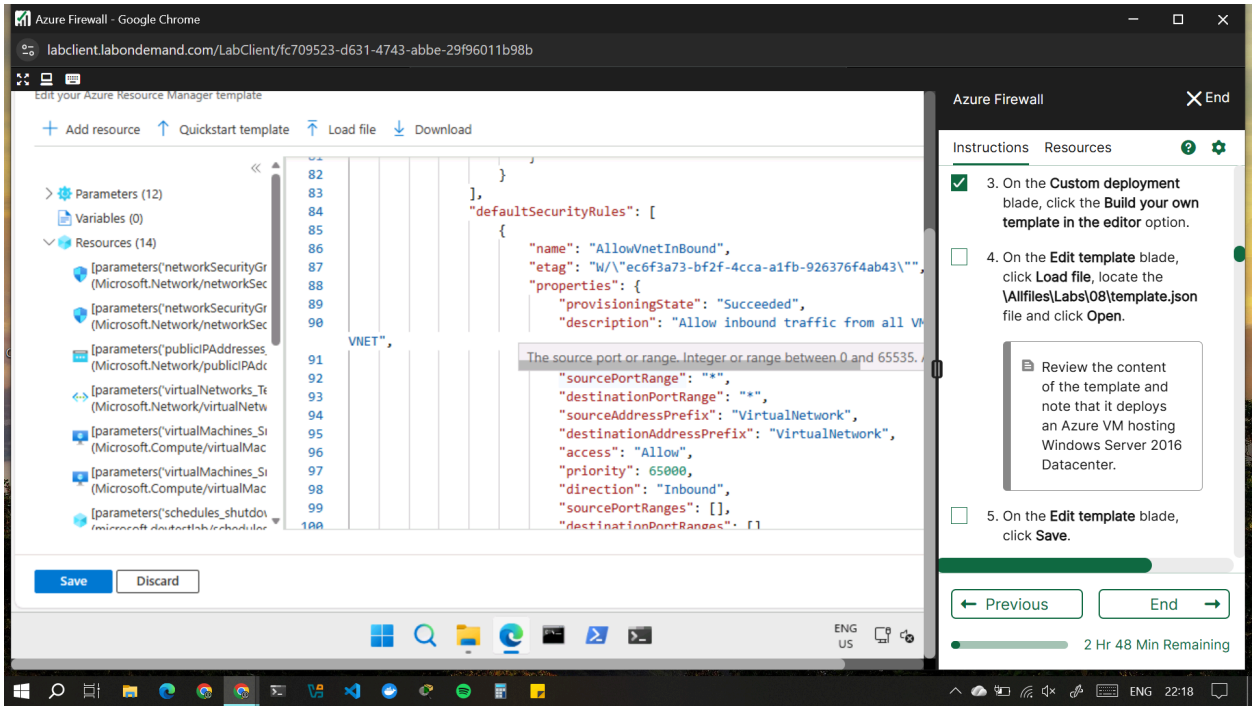
In this task, you will review and deploy the lab environment.

In this task, you will create a virtual machine by using an **ARM template. ARM (Azure Resource Manager) templates** are JSON files that use declarative syntax to define the infrastructure and resources for an Azure deployment, ensuring consistent and repeatable deployments. They allow you to define resources like virtual machines, storage accounts, and networks and their relationships, which are then deployed as a single logical unit called **a resource group**. This infrastructure-as-code approach enables version control and makes it easier to manage complex solutions. 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-56988727@LODSPRODMCA.onmicrosoft.com with TAP S9zGZPXL.
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.



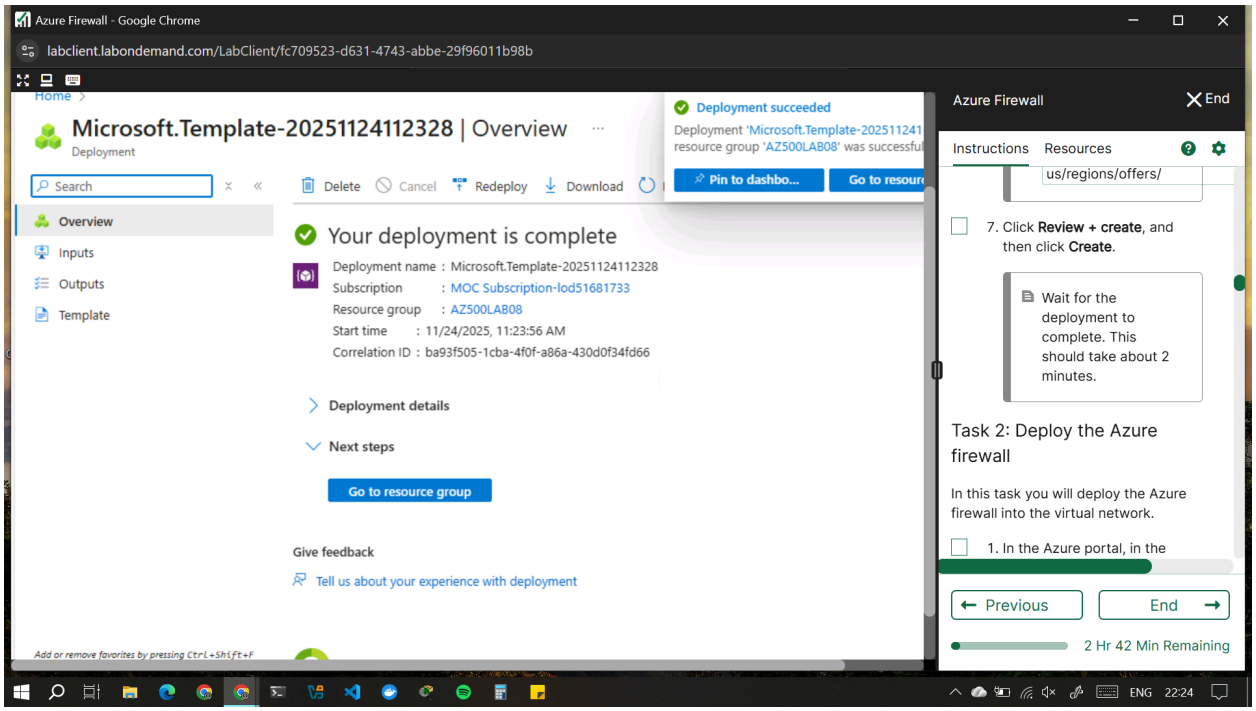
4. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**.
   Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2016 Datacenter.
5. On the **Edit template** blade, click **Save**.



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

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



Task 2: Deploy the Azure firewall

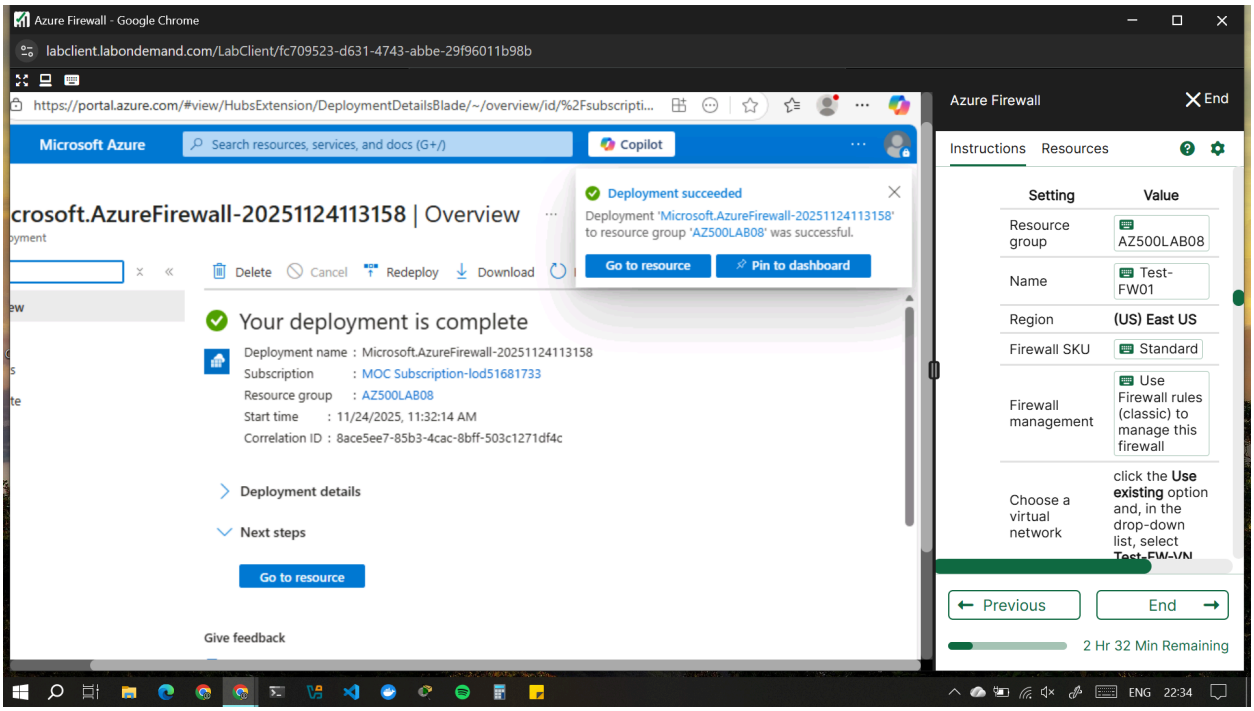
In this task you will deploy the Azure firewall into the virtual network.

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
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**.

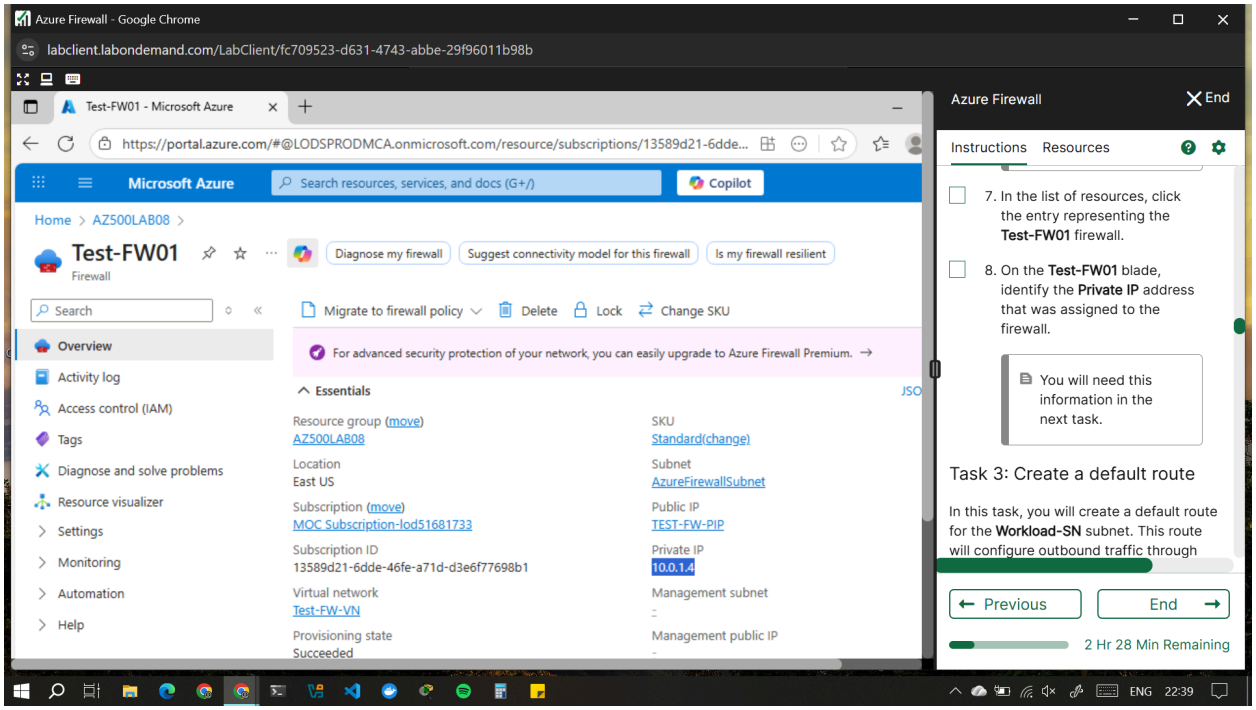
   Wait for the deployment to complete. This should take about 5 minutes.



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 **Workload-SN** subnet. This route will configure outbound traffic through the firewall.

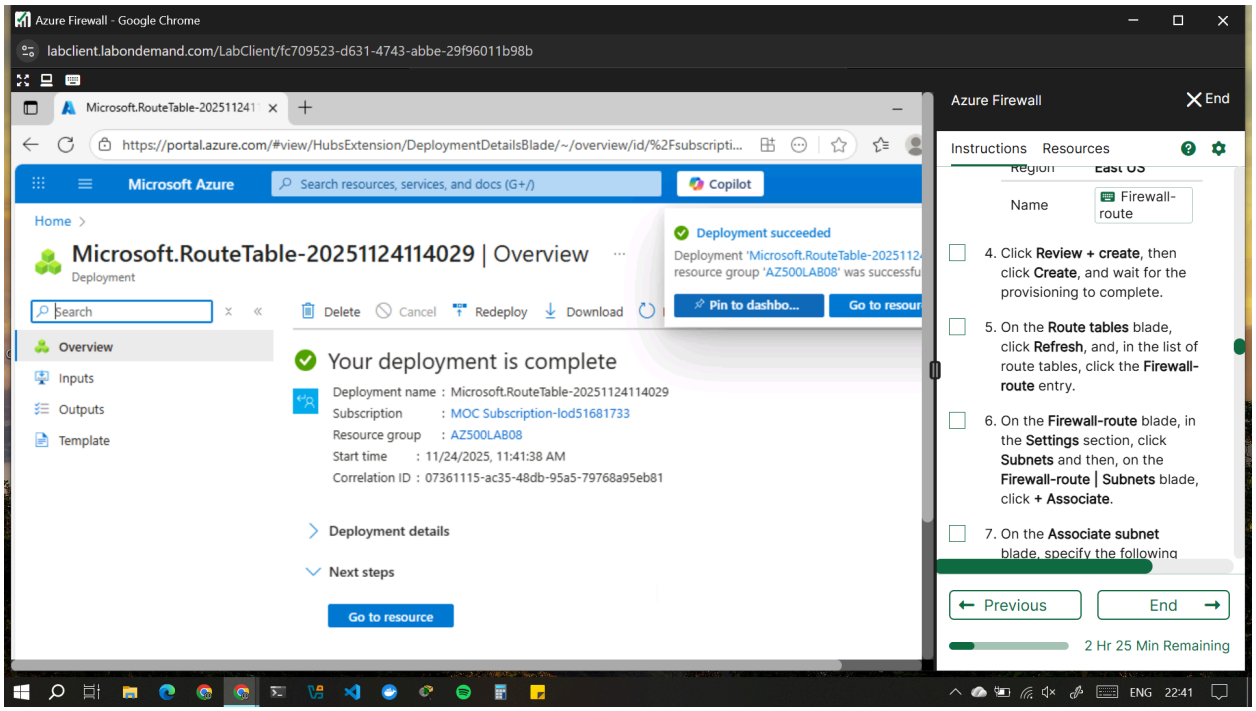
1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Route tables** and press the **Enter** key.
2. On the **Route tables** blade, click **+ Create**.

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

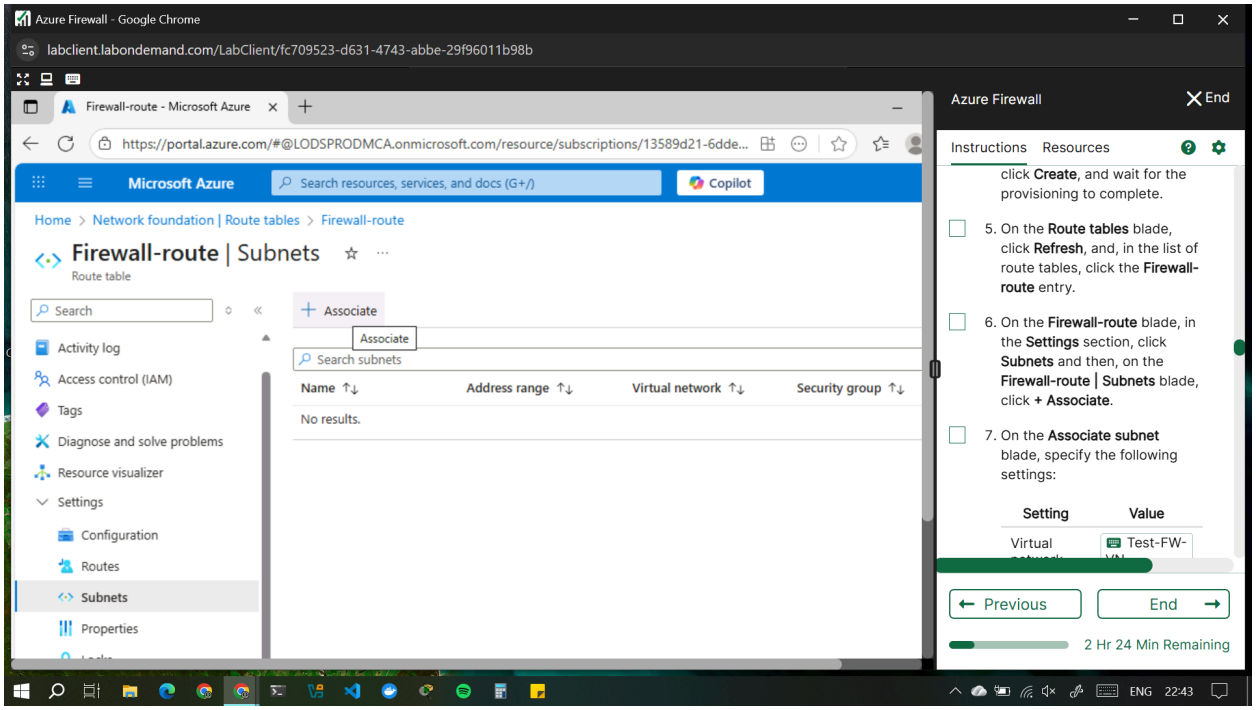
Setting	Value
Resource group	AZ500LAB08
Region	**East US**

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**.



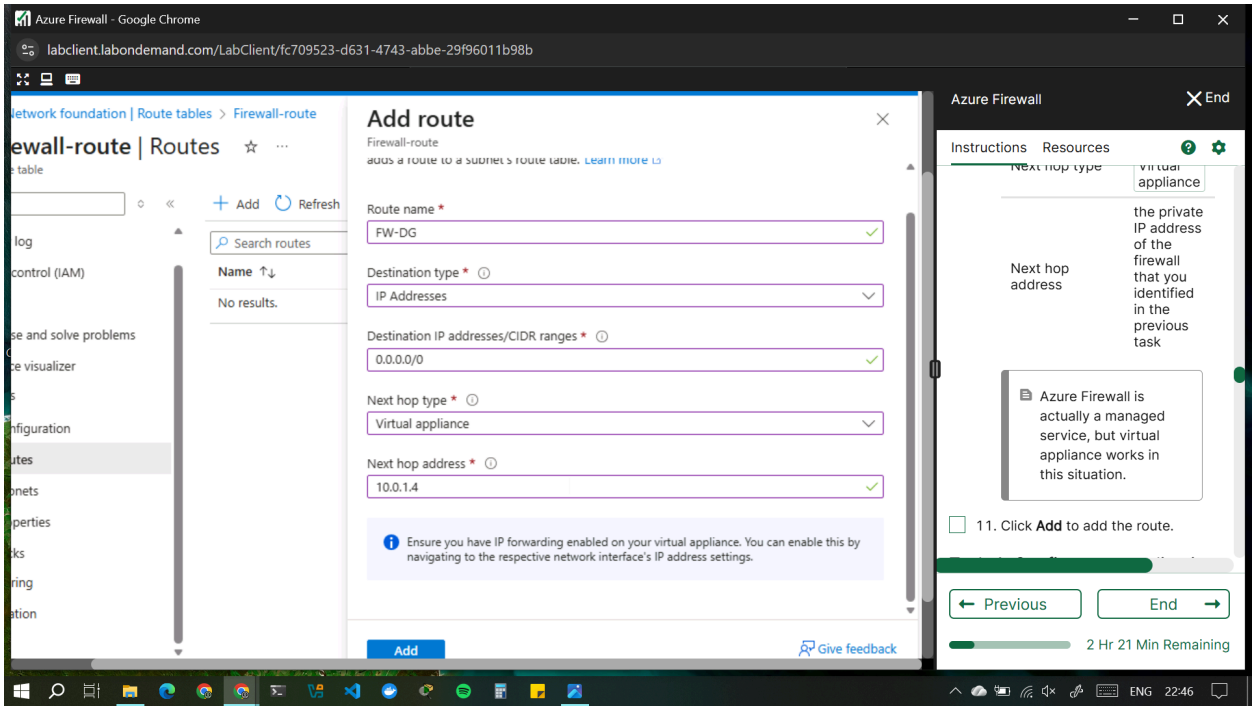
7. On the **Associate subnet** blade, specify the following settings:

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

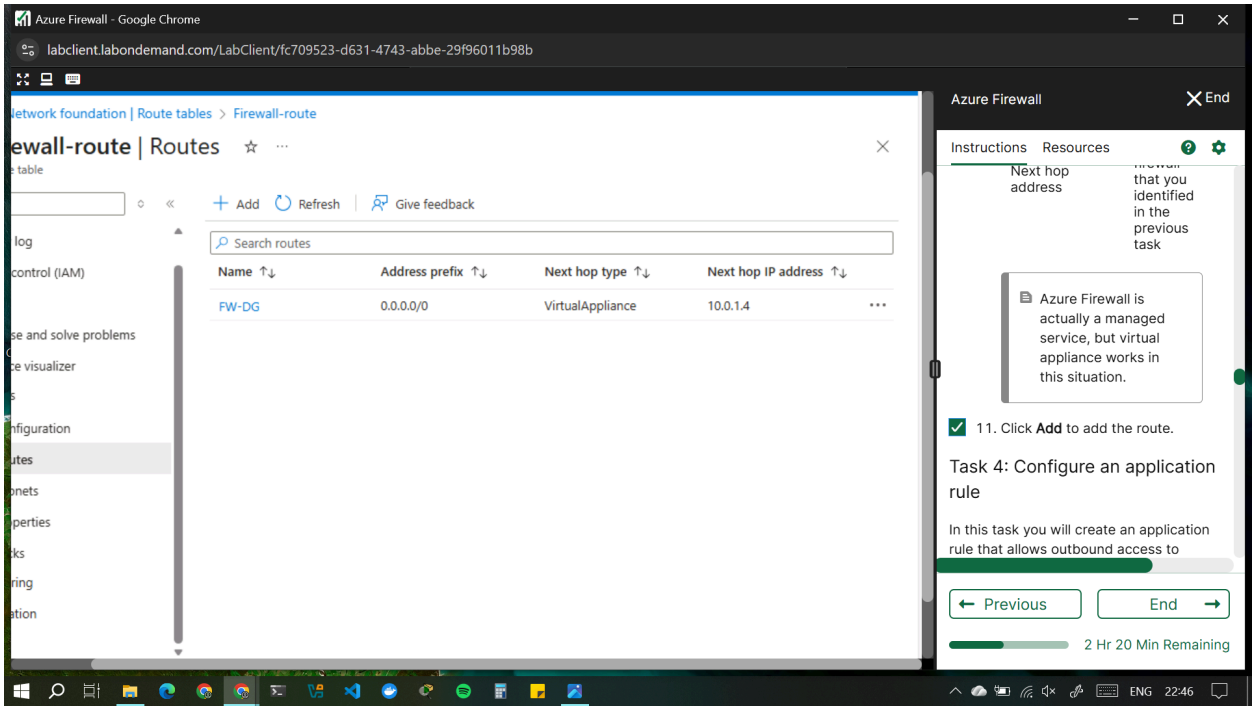
8. Ensure the **Workload-SN** subnet is selected for this route, otherwise the firewall won't work correctly.
9. Click **OK** to associate the firewall to the virtual network subnet.
10. Back on the **Firewall-route** blade, in the **Settings** section, click **Routes** and then click **+ Add**.
11. 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.



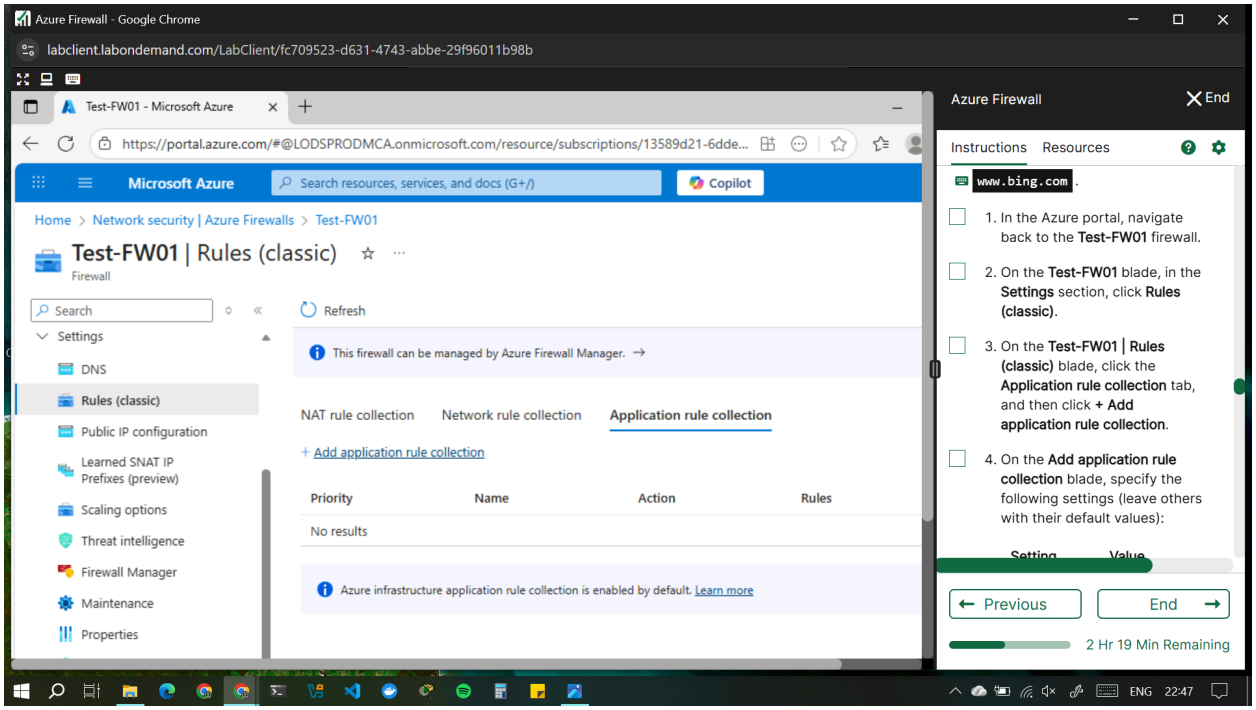
12. Click **Add** to add the route.



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**.

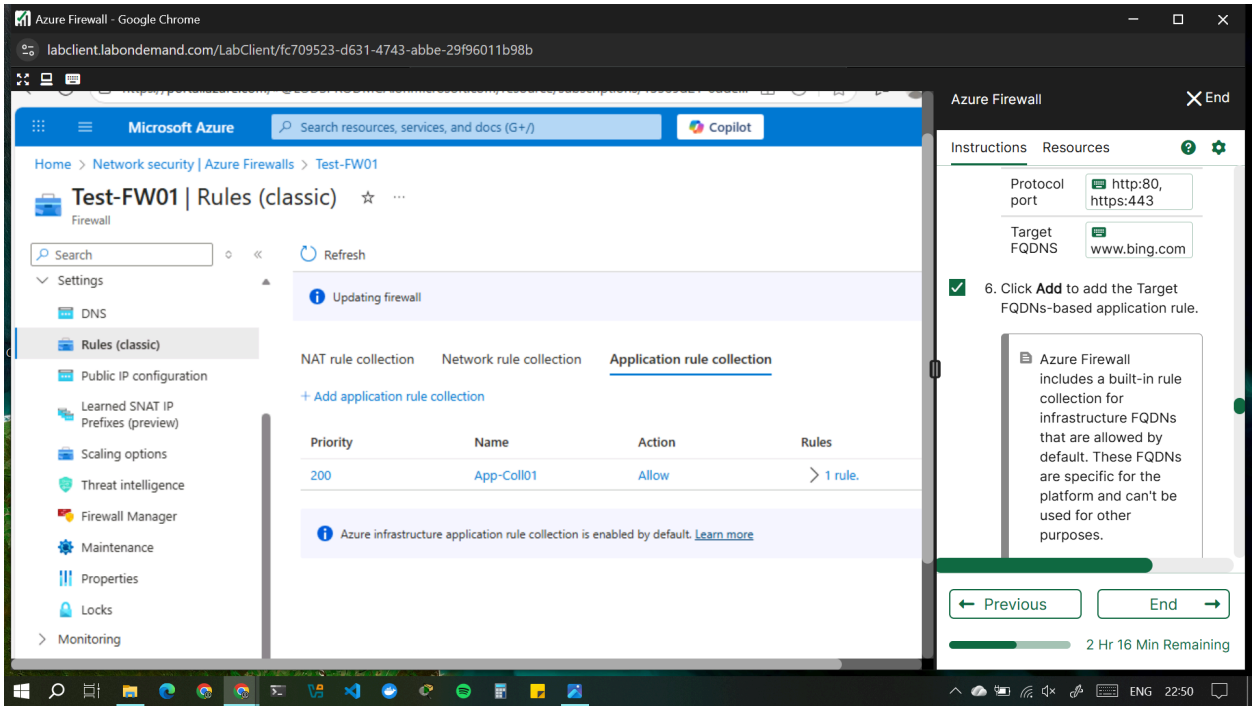
4. On the **Add application rule collection** blade, specify the following settings (leave others with their default values):

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

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.



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):

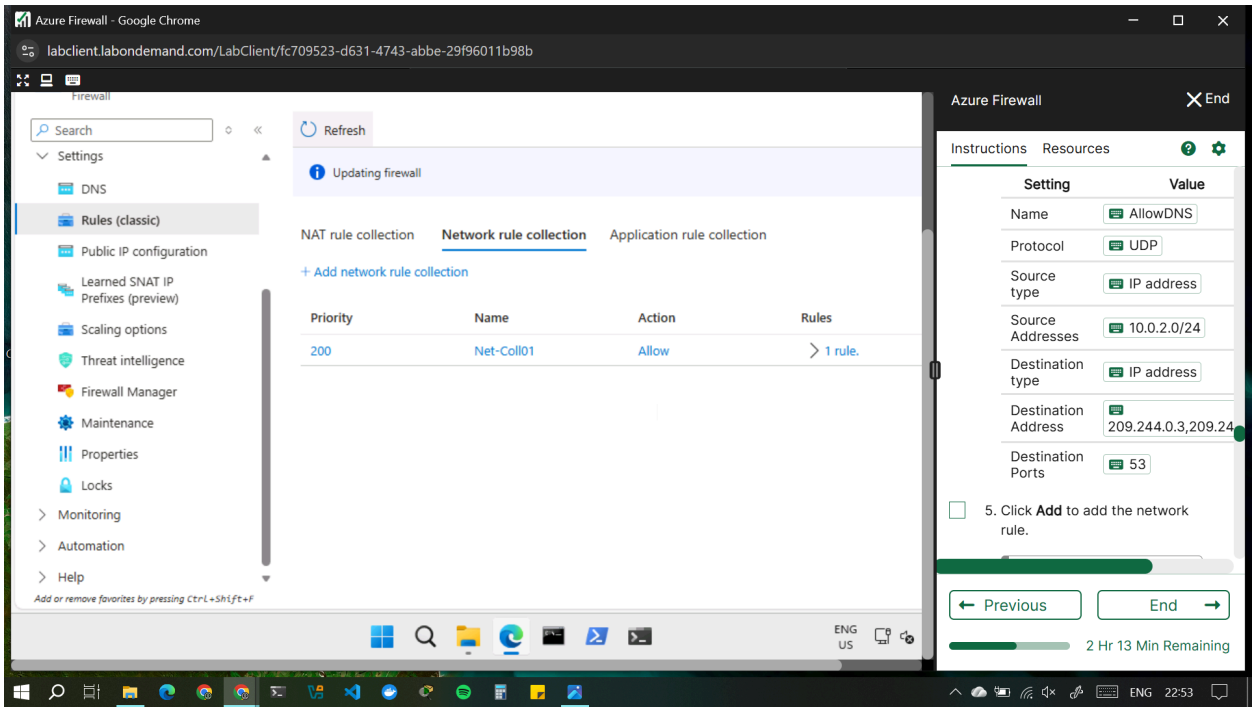
Setting	Value
Name	Net-Coll01
Priority	200
Action	Allow

4. 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
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.

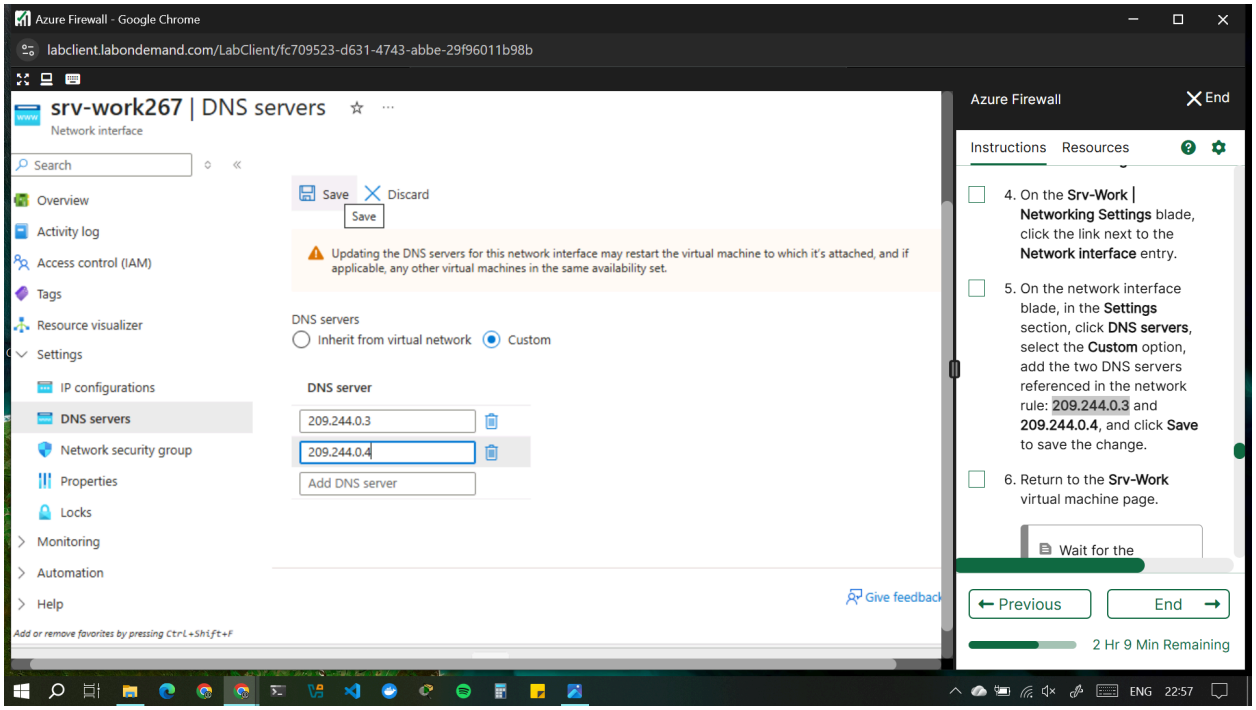


Task 6: Configure the virtual machine DNS servers

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** 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.

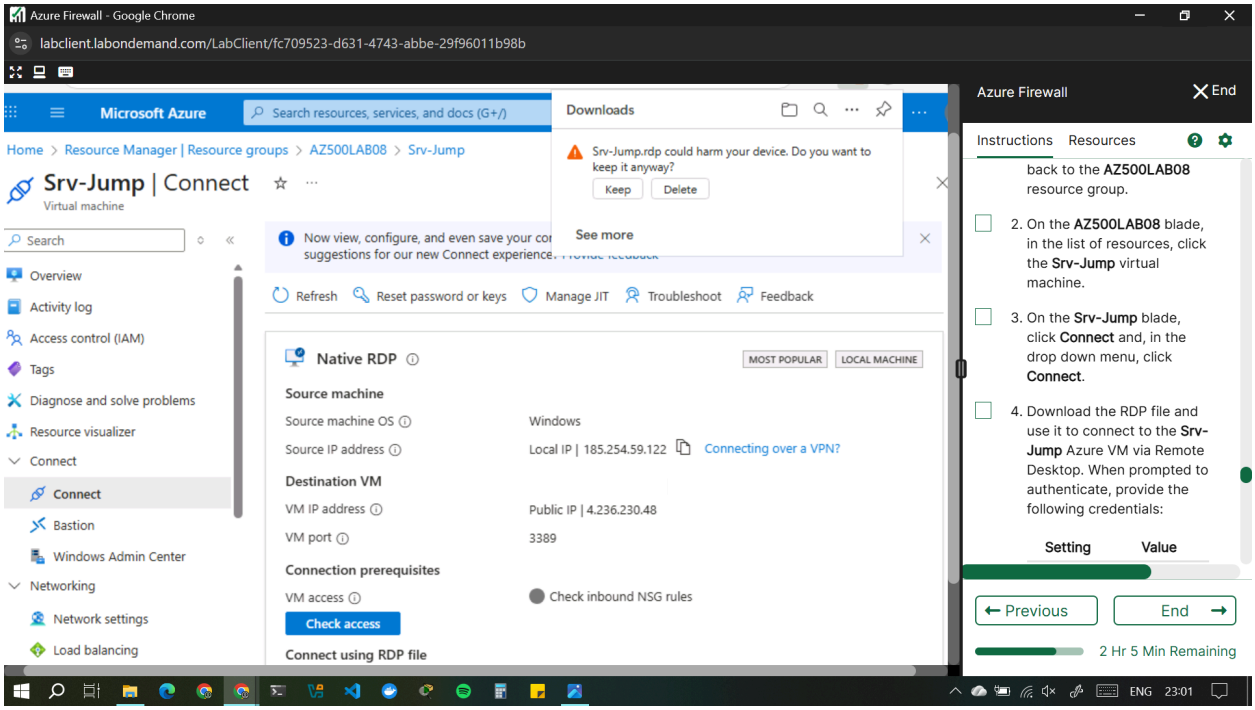
Task 7: Test the firewall

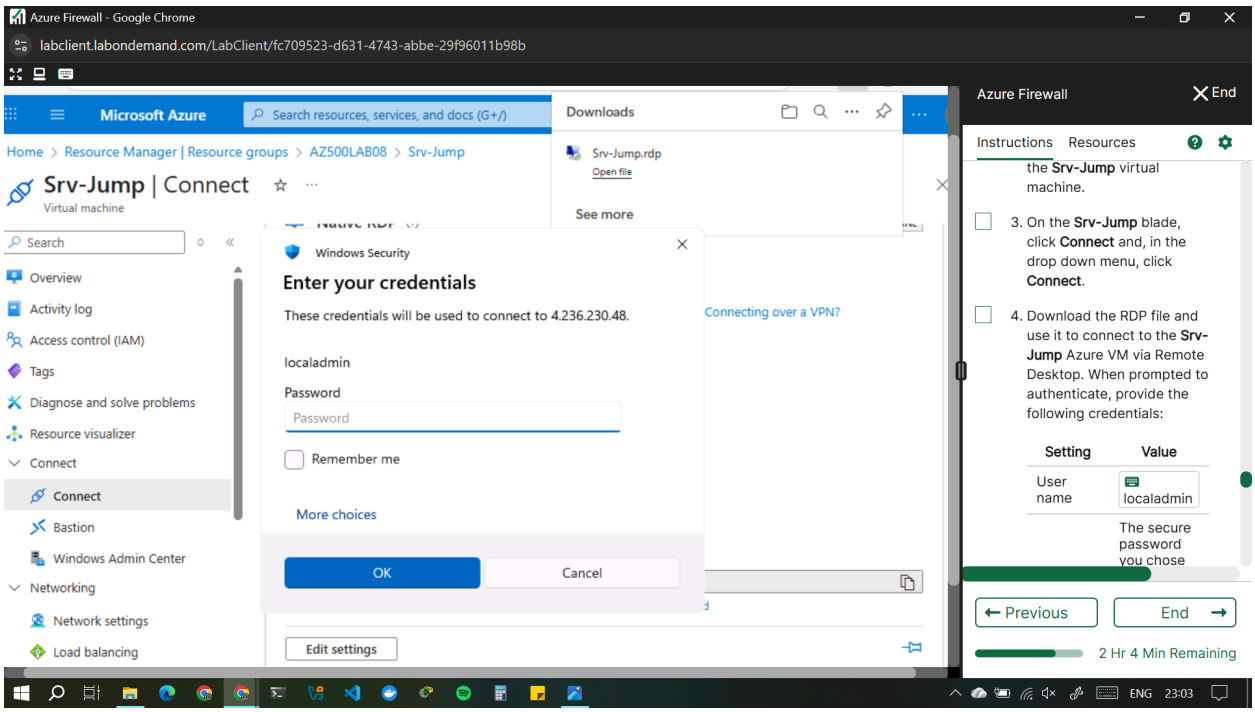
In this task, you will test the firewall to confirm that it works as expected.

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

4. Download the 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.





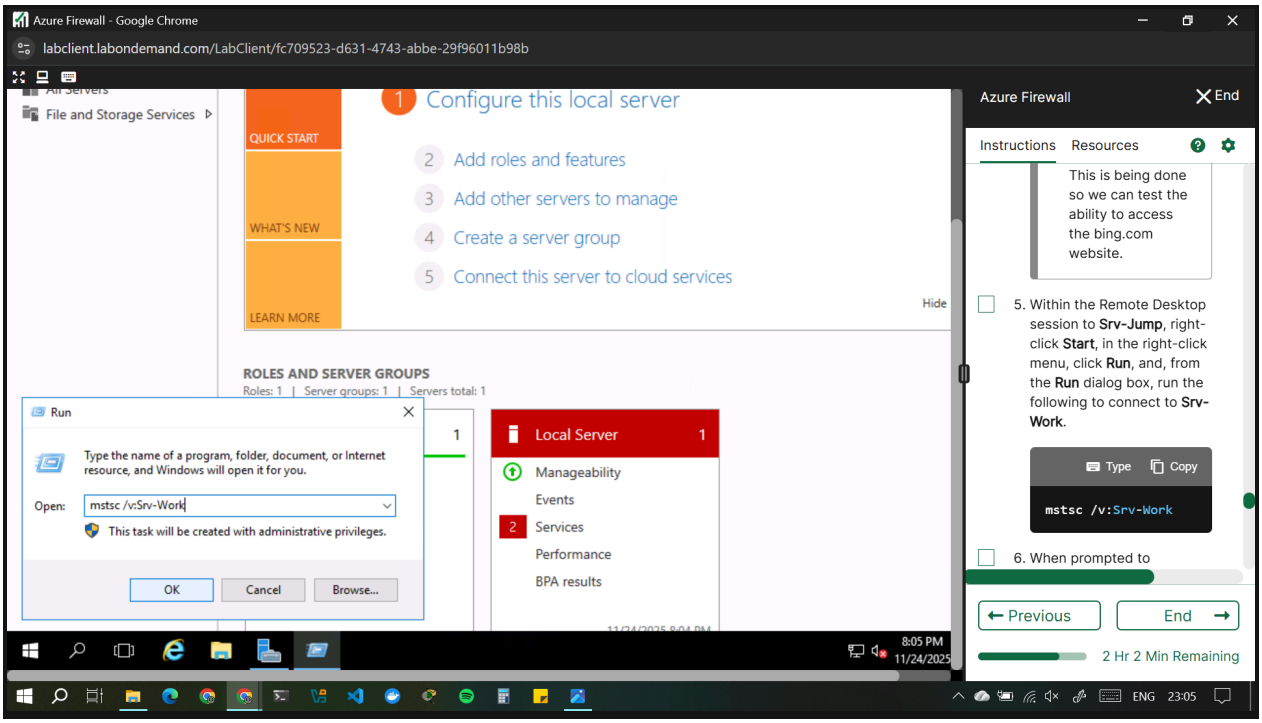
5. The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.

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.

6. 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**.

```
TypeCopy

mstsc /v:Srv-Work
```

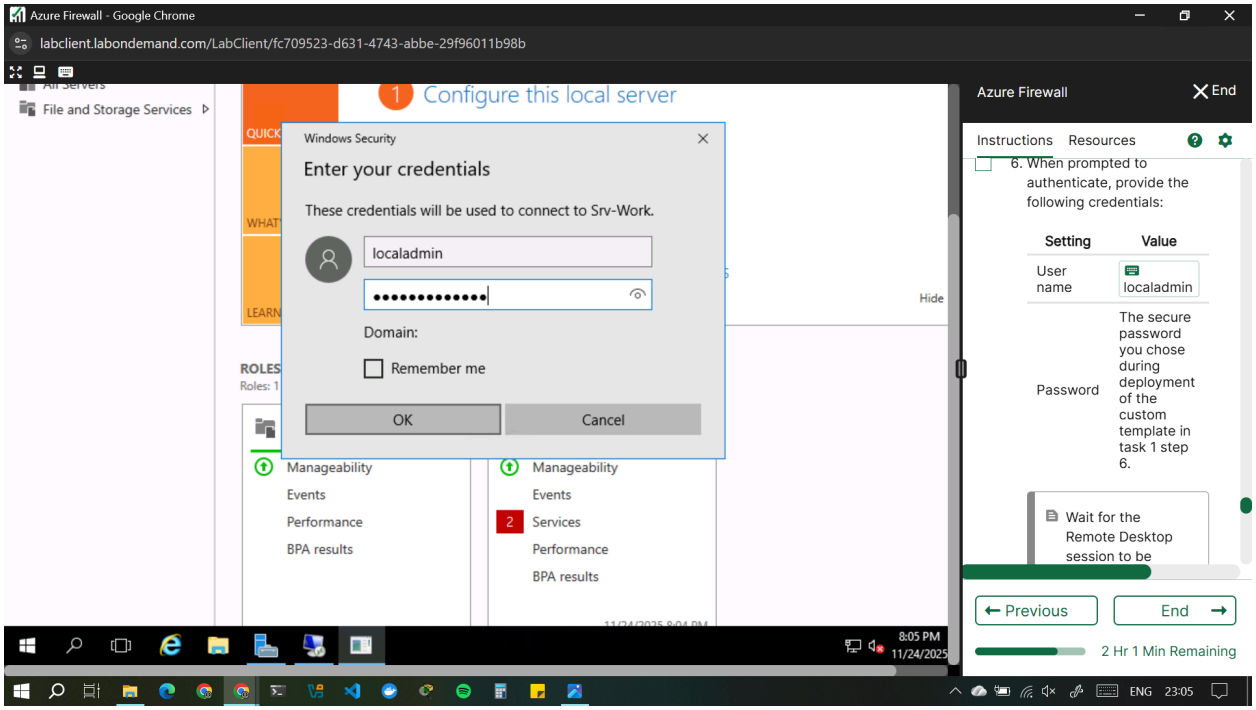


7. When prompted to authenticate, provide the following credentials:

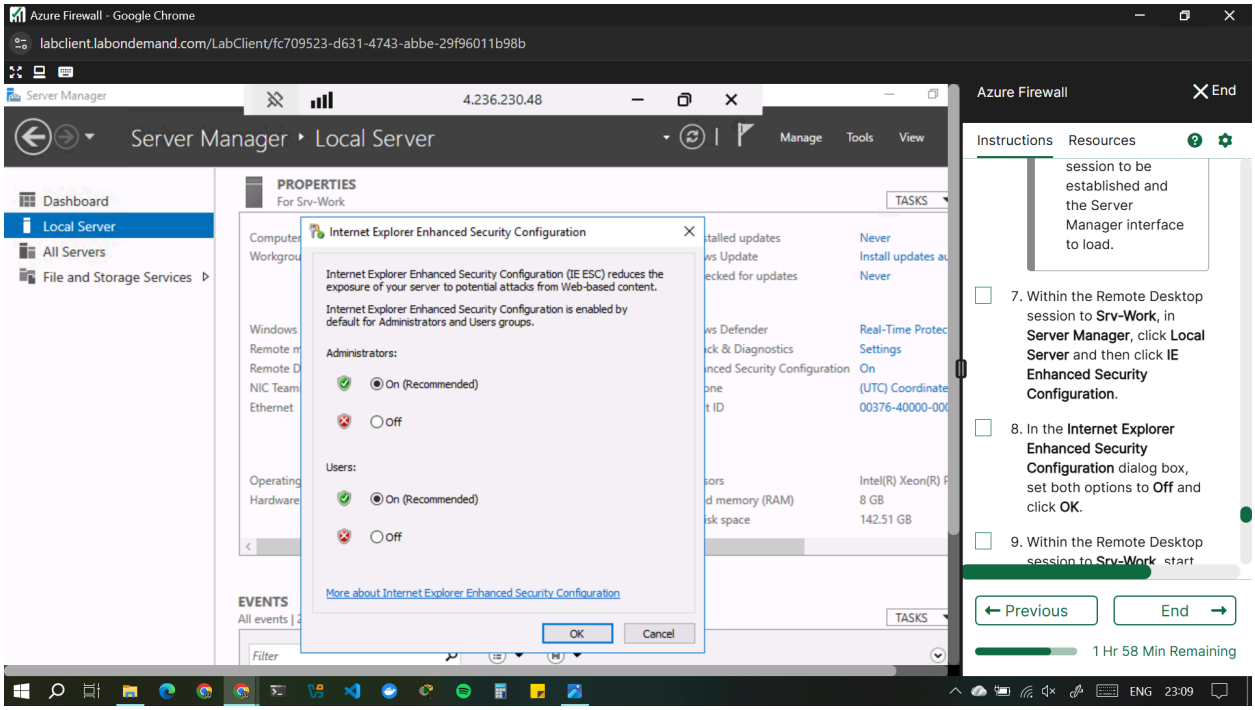
Setting	Value
User name	localadmin

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.

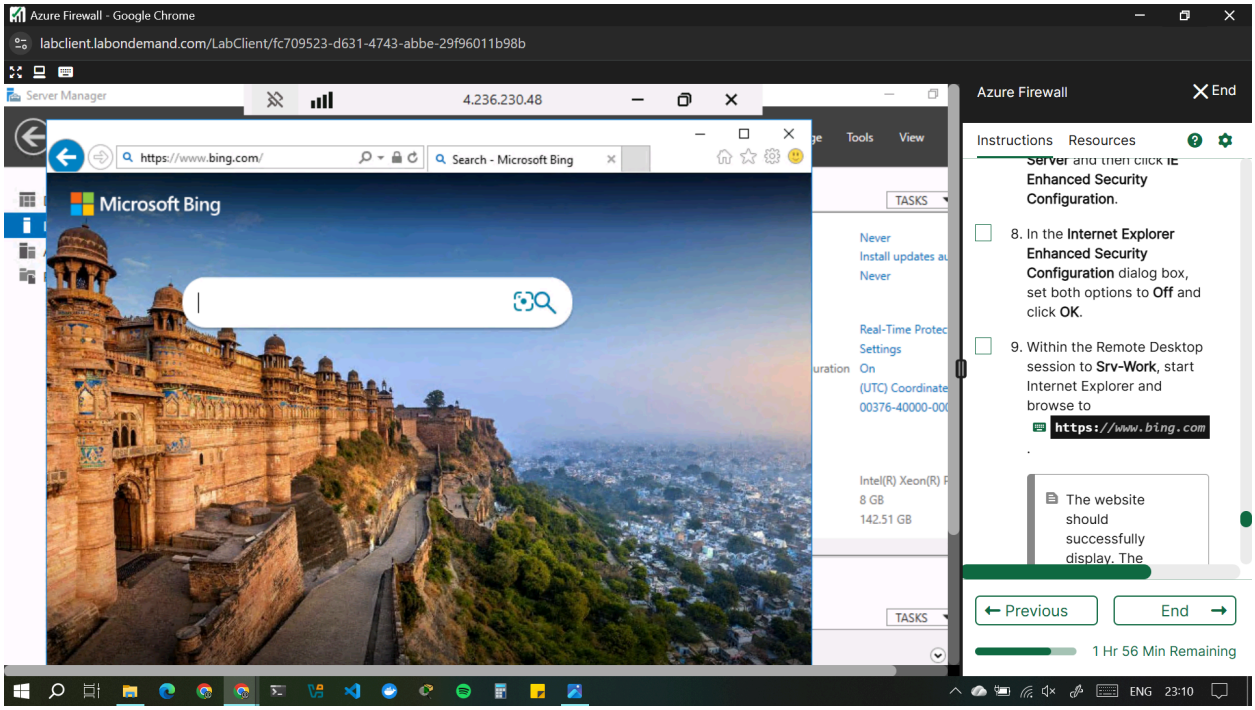


8. Within the Remote Desktop session to **Srv-Work**, in **Server Manager**, click **Local Server** and then click **IE Enhanced Security Configuration**.
9. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.



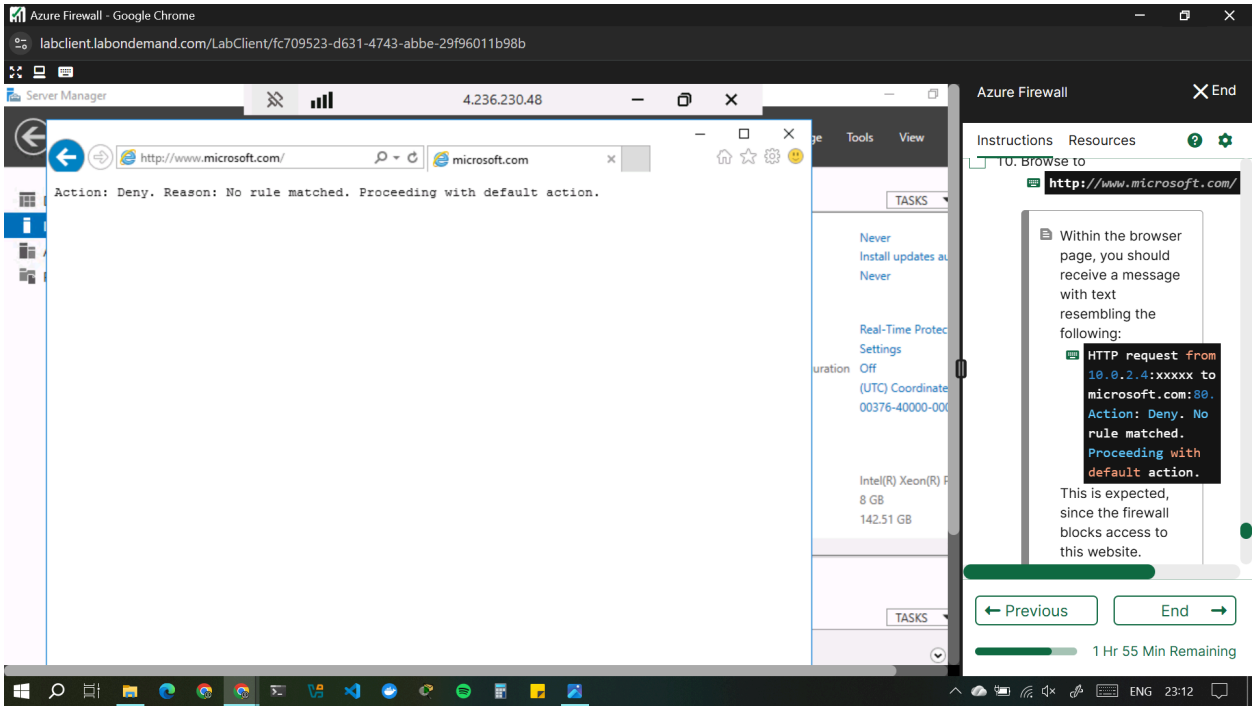
10. Within the Remote Desktop session to **Srv-Work**, start Internet Explorer and browse to `https://www.bing.com`.

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



11. 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.



12. Terminate both Remote Desktop sessions.

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

Conclusion

In this lab, I successfully deployed and tested Azure Firewall as part of a secure network architecture. By using an ARM template, I provisioned the foundational environment, including virtual networks, subnets, and virtual machines. I then deployed Azure Firewall, configured custom routing to enforce outbound traffic inspection, and created both application and network rule collections to tightly control allowed traffic flows. After configuring DNS settings and validating the setup through controlled testing, I confirmed that only authorized outbound traffic—such as access to www.bing.com was permitted, while unauthorized requests were correctly denied.

This hands-on exercise demonstrated how Azure Firewall provides centralized, scalable, and stateful network security in Azure. It reinforced key concepts such as route table configuration, rule-based traffic filtering, and secure access through jump hosts. Overall,

the lab provided practical experience in implementing a robust cloud firewall solution, strengthening my understanding of Azure network security best practices.