Microsoft ADC Cybersecurity Skilling Program

Week 7 Lab Assignment

Student Name: Vincent Onchieku Collins

Student ID: ADC-CSS02-25052

Introduction

In this lab exercise, I was tasked with deploying and configuring Azure Firewall to control inbound and outbound network traffic in a secure and efficient manner. The goal was to implement a structured firewall setup to manage access to web applications and DNS services. This lab simulated a real-world scenario where network security is vital to organizational operations. The tasks performed included deploying infrastructure, setting up routing, configuring firewall rules, assigning DNS servers, and testing the firewall functionality. Through these steps, I gained practical experience with Azure networking and security services. Below is a breakdown of each task and what I accomplished.
It included 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.

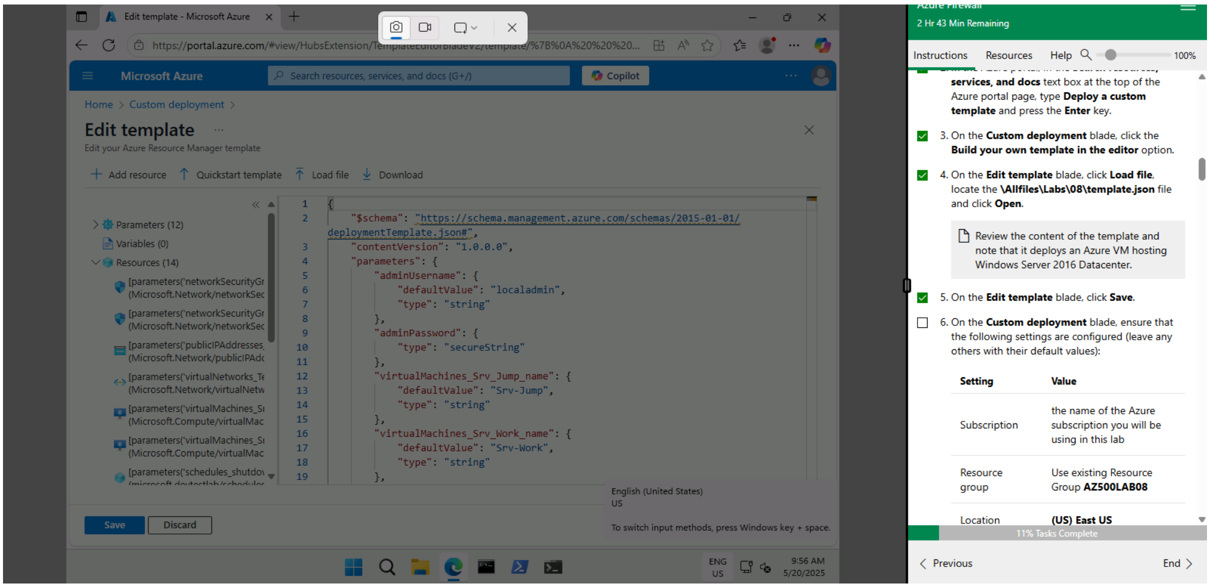
Task 6: Configure DNS servers.

Task 7: Test the firewall.

Tasks:

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

The lab began with deploying the environment using an ARM template. I signed into the Azure portal and used the “Deploy a custom template” feature to load and review the provided template.json file. This template automated the creation of a virtual network, subnets, and virtual machines. I specified parameters such as the resource group (AZ500LAB08), location (East US), and VM admin password. After validating the configuration, I deployed the resources. This task laid the foundation for the firewall setup by provisioning the core infrastructure necessary for subsequent tasks.



Edit template - Microsoft Azure

https://portal.azure.com/#view/HubsExtension/TemplateEditorBladeV2/template/%7B%0A%20%20%20...

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

Home > Custom deployment >

Edit template

Edit your Azure Resource Manager template

Add resource | Quickstart template | Load file | Download

- Parameters (12)
- Variables (0)
- Resources (14)
  - [parameters('networkSecurityGr (Microsoft.Network/networkSec
  - [parameters('networkSecurityGr (Microsoft.Network/networkSec
  - [parameters('publicIPAddresses_ (Microsoft.Network/publicIPAdc
  - [parameters('virtualNetworks_Te (Microsoft.Network/virtualNetw
  - [parameters('virtualMachines_Si (Microsoft.Compute/virtualMac
  - [parameters('virtualMachines_Si (Microsoft.Compute/virtualMac
  - [parameters('schedules_shutdo\ (microsoft.devtestlab/schedules

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/
deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "adminUsername": {
            "defaultValue": "localadmin",
            "type": "string"
        },
        "adminPassword": {
            "type": "secureString"
        },
        "virtualMachines_Srv_Jump_name": {
            "defaultValue": "Srv-Jump",
            "type": "string"
        },
        "virtualMachines_Srv_Work_name": {
            "defaultValue": "Srv-Work",
            "type": "string"
        },
```

English (United States)
US

To switch input methods, press Windows key + space.

Save | Discard

ENG US 9:56 AM 5/20/2025

Azure Firewall

2 Hr 43 Min Remaining

Instructions | Resources | Help 100%

☑ 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.

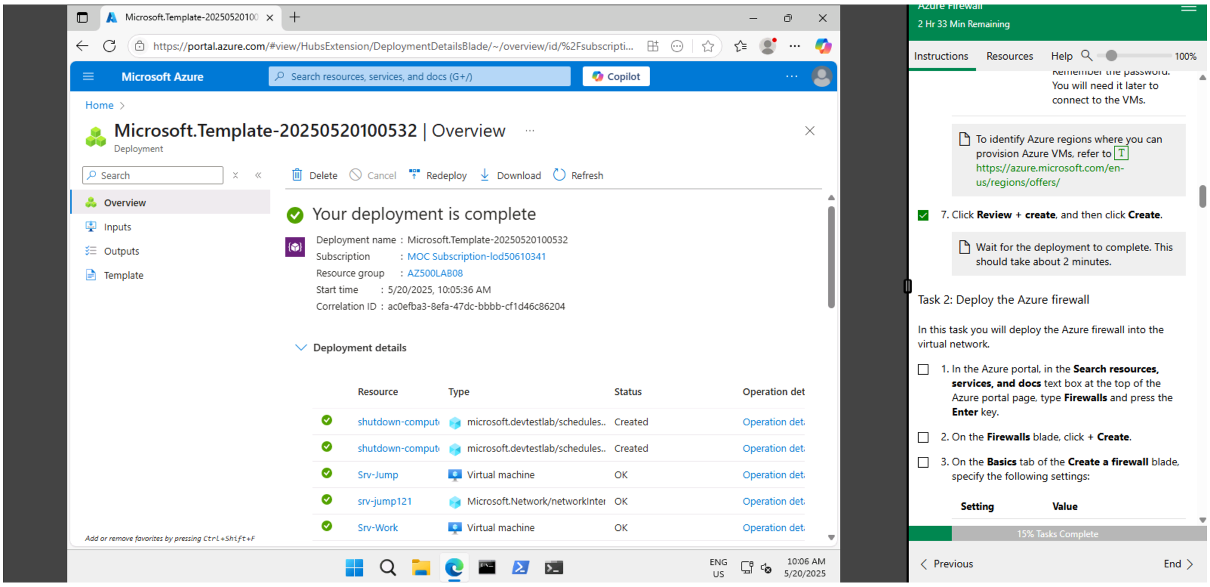
☑ 5. On the **Edit template** blade, click **Save**.

☐ 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**

11% Tasks Complete

< Previous | End >



Microsoft.Template-2025052010(

https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscripti...

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

Home >

Microsoft.Template-20250520100532 | Overview

Deployment

Search

- Overview
- Inputs
- Outputs
- Template

Delete | Cancel | Redeploy | Download | Refresh

Your deployment is complete

Deployment name : Microsoft.Template-20250520100532
Subscription : MOC Subscription-lod50610341
Resource group : AZ500LAB08
Start time : 5/20/2025, 10:05:36 AM
Correlation ID : ac0efba3-8efa-47dc-bbbb-cf1d46c86204

Deployment details

	Resource	Type	Status	Operation det
✓	shutdown-comput	microsoft.devtestlab/schedules..	Created	Operation det
✓	shutdown-comput	microsoft.devtestlab/schedules..	Created	Operation det
✓	Srv-Jump	Virtual machine	OK	Operation det
✓	srv-jump121	Microsoft.Network/networkInter	OK	Operation det
✓	Srv-Work	Virtual machine	OK	Operation det

Add or remove favorites by pressing Ctrl+Shift+F

ENG US 10:06 AM 5/20/2025

Azure Firewall

2 Hr 33 Min Remaining

Instructions | Resources | Help 100%

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, 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:

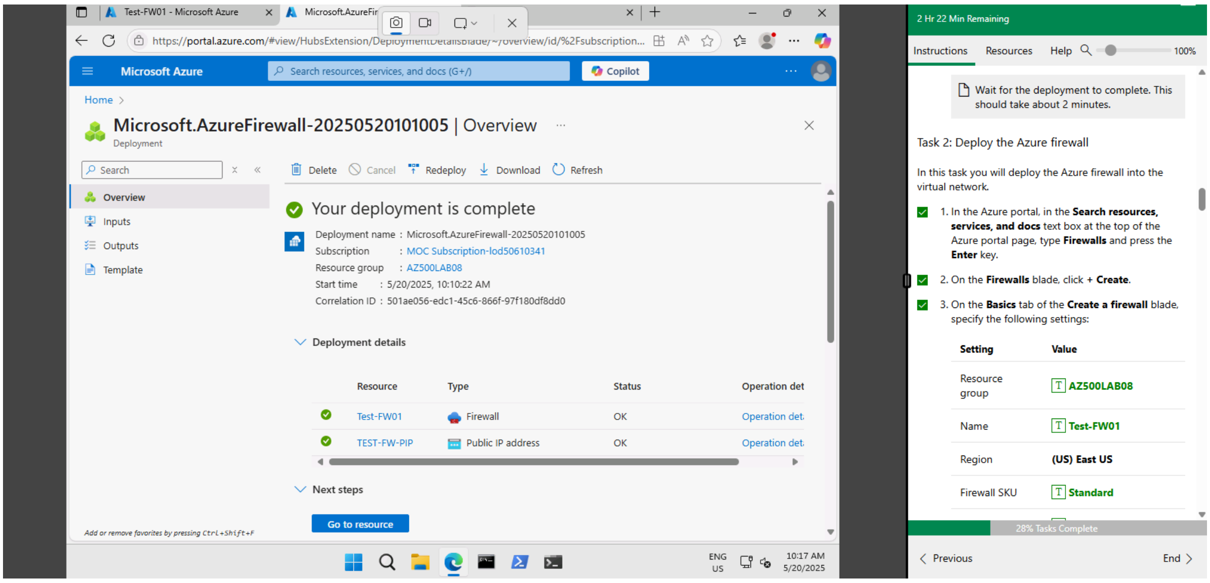
Setting	Value

15% Tasks Complete

< Previous | End >

Task 2: Deploy the Azure Firewall

Next, I deployed the Azure Firewall to the virtual network. I navigated to the “Firewalls” section in the Azure portal and created a new firewall named Test-FW01. I selected the standard SKU and disabled the management NIC. I also created a new public IP address (TEST-FW-PIP) for the firewall. After deployment, I reviewed the firewall resource and noted its private IP address, which was needed in later steps. This task introduced me to Azure Firewall as a cloud-native, stateful network security service designed to protect Azure Virtual Network resources.


Test-FW01 - Microsoft Azure
Microsoft.AzureFir
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscription...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Go to resource
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
10:17 AM
5/20/2025

Microsoft.AzureFirewall-20250520101005 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.AzureFirewall-20250520101005
Subscription : MOC Subscription-lod50610341
Resource group : AZ500LAB08
Start time : 5/20/2025, 10:10:22 AM
Correlation ID : 501ae056-edc1-45c6-866f-97f180df8dd0

Deployment details

	Resource	Type	Status	Operation det
✓	Test-FW01	Firewall	OK	Operation det:
✓	TEST-FW-PIP	Public IP address	OK	Operation det:

Next steps

2 Hr 22 Min Remaining

Instructions Resources Help 100%

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.

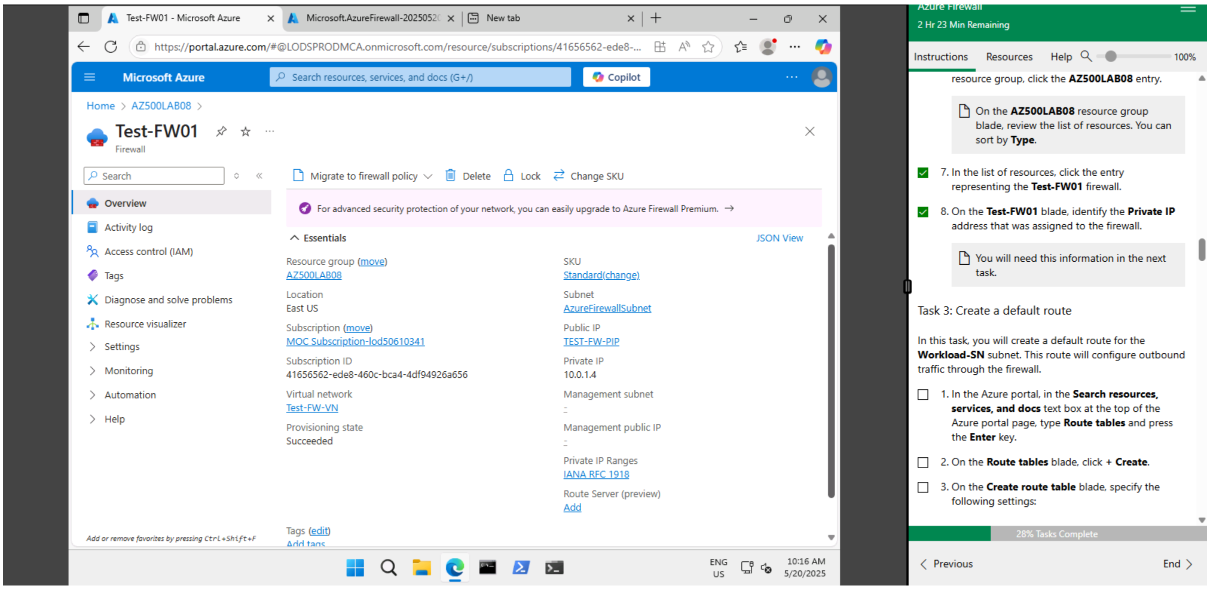
☑ 2. On the **Firewalls** blade, click + **Create**.

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

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

28% Tasks Complete

Previous End


Test-FW01 - Microsoft Azure
Microsoft.AzureFirewall-2025052
New tab
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/41656562-ede8-...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
AZ500LAB08
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Monitoring
Automation
Help
Migrate to firewall policy
Delete
Lock
Change SKU
JSON View
Add or remove favorites by pressing Ctrl+Shift+F
ENG
US
10:16 AM
5/20/2025

Test-FW01

Firewall

For advanced security protection of your network, you can easily upgrade to Azure Firewall Premium. →

Essentials

Resource group (move)
AZ500LAB08

Location
East US

Subscription (move)
MOC Subscription-lod50610341

Subscription ID
41656562-ede8-460c-bca4-4df94926a656

Virtual network
Test-FW-VN

Provisioning state
Succeeded

SKU
Standard(change)

Subnet
AzureFirewallSubnet

Public IP
TEST-FW-PIP

Private IP
10.0.1.4

Management subnet
-

Management public IP
-

Private IP Ranges
IANA RFC 1918

Route Server (preview)
Add

Tags (edit)
Add tags

Azure Firewall

2 Hr 23 Min Remaining

Instructions Resources Help 100%

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**.

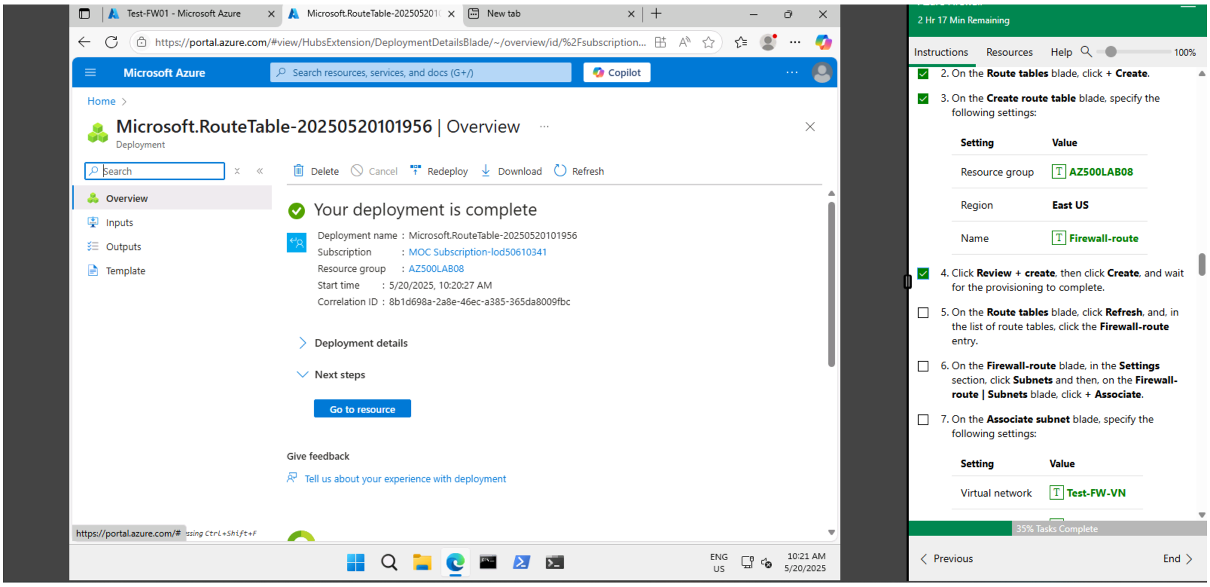
☐ 3. On the **Create route table** blade, specify the following settings:

28% Tasks Complete

Previous End

Task 3: Create a Default Route

In this task, I configured routing to force all outbound traffic from the Workload-SN subnet through the firewall. I created a new route table called Firewall-route and associated it with the workload subnet. Then, I added a default route (FW-DG) with destination 0.0.0.0/0 and next hop set as a virtual appliance using the private IP of the firewall. This ensured all internet-bound traffic from the workload subnet was inspected and filtered by the firewall. This task helped me understand how custom routing is used in Azure to direct traffic through security appliances.



Microsoft.RouteTable-20250520101956 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.RouteTable-20250520101956
Subscription : MOC Subscription-lod50610341
Resource group : AZ500LAB08
Start time : 5/20/2025, 10:20:27 AM
Correlation ID : 8b1d698a-2a8e-46ec-a385-365da8009fbc

2 Hr 17 Min Remaining

☑ 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.

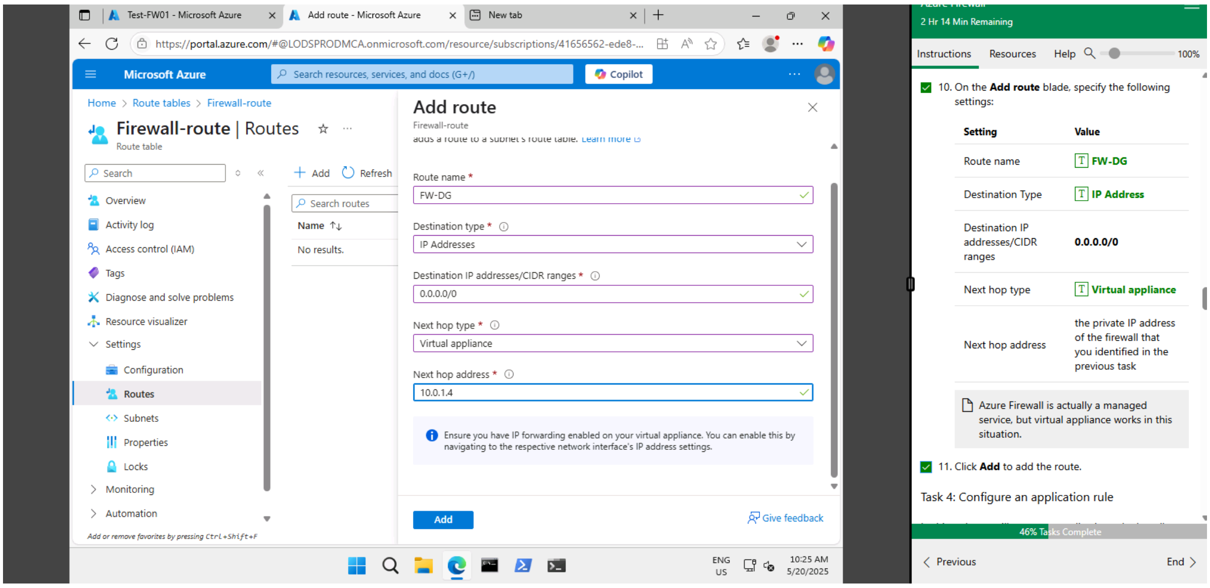
☐ 6. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click + **Associate**.

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

Setting	Value
Virtual network	Test-FW-VN

35% Tasks Complete

Test-FW01 - Microsoft Azure
Microsoft.RouteTable-2025052010
New tab
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscription...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Search
Delete
Cancel
Redeploy
Download
Refresh
Overview
Inputs
Outputs
Template
Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
https://portal.azure.com/#
ENG
US
10:21 AM
5/20/2025
Instructions
Resources
Help
100%
Previous
End



Add route

Firewall-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.

2 Hr 14 Min Remaining

☑ 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
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.

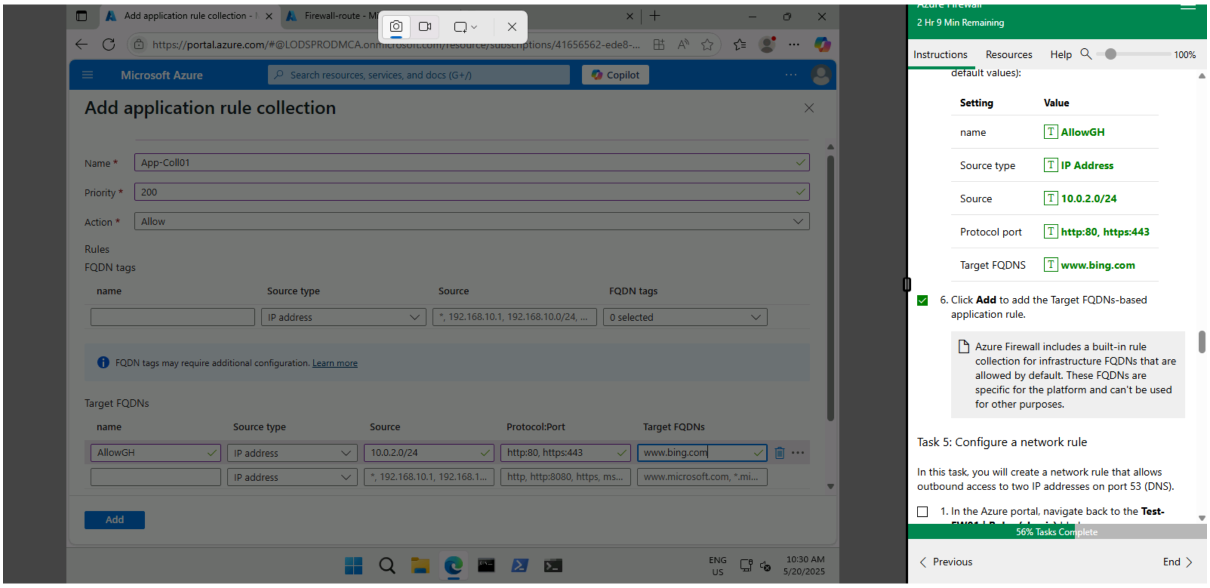
☑ 11. Click **Add** to add the route.

Task 4: Configure an application rule

46% Tasks Complete

Task 4: Configure an Application Rule

I then created an application rule within the firewall to allow access to a specific FQDN—www.bing.com. Under the firewall's "Rules (classic)" section, I added an application rule collection named App-Coll01 with priority 200 and action set to allow. I specified the source IP range as 10.0.2.0/24 and added a rule named AllowGH to permit traffic to www.bing.com on HTTP and HTTPS ports. This rule helped enforce strict control over web traffic by allowing access only to permitted applications or URLs.


Add application rule collection - M
Firewall-route - Mi
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/41656562-ede8-...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
ENG
US
10:30 AM
5/20/2025
Instructions
Resources
Help
100%
Previous
End

Add application rule collection

Name * App-Coll01

Priority * 200

Action * Allow

Rules

FQDN tags

name	Source type	Source	FQDN tags
	IP address	*, 192.168.10.1, 192.168.10.0/24, ...	0 selected

FQDN tags may require additional configuration. Learn more

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
	IP address	*, 192.168.10.1, 192.168.1...	http, http:8080, https, ms...	www.microsoft.com, *.mi...

Add

2 Hr 9 Min Remaining

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.

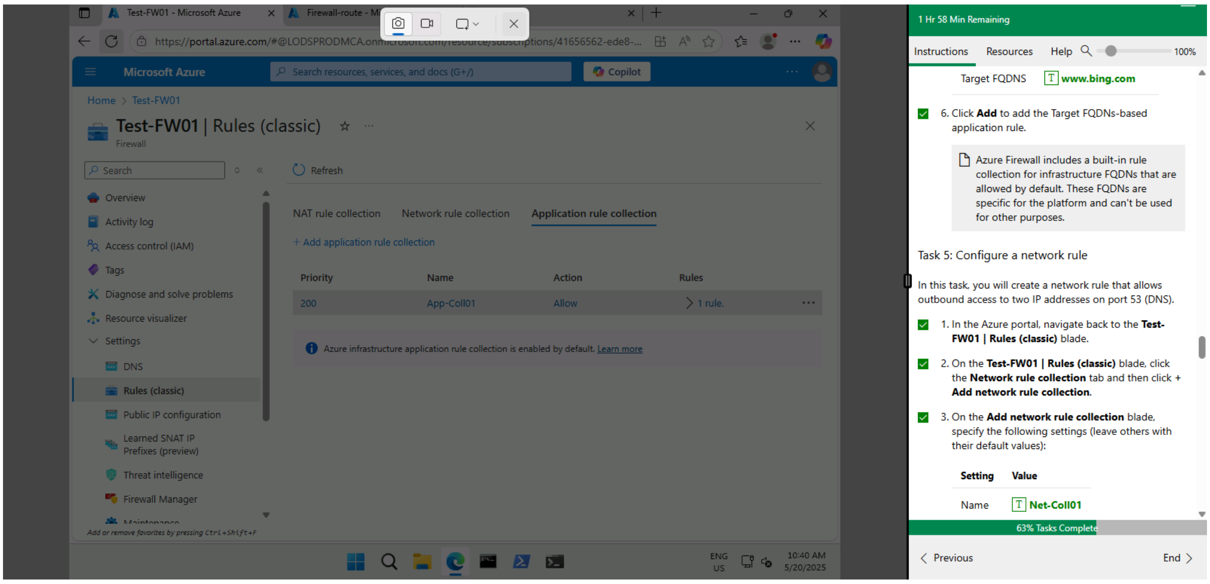
Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes.

Task 5: Configure a network rule

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-**

56% Tasks Complete



Test-FW01 | Rules (classic)

NAT rule collection | Network rule collection | Application rule collection

+ Add application rule collection

Priority	Name	Action	Rules
200	App-Coll01	Allow	1 rule.

Azure infrastructure application rule collection is enabled by default. Learn more

1 Hr 58 Min Remaining

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**.

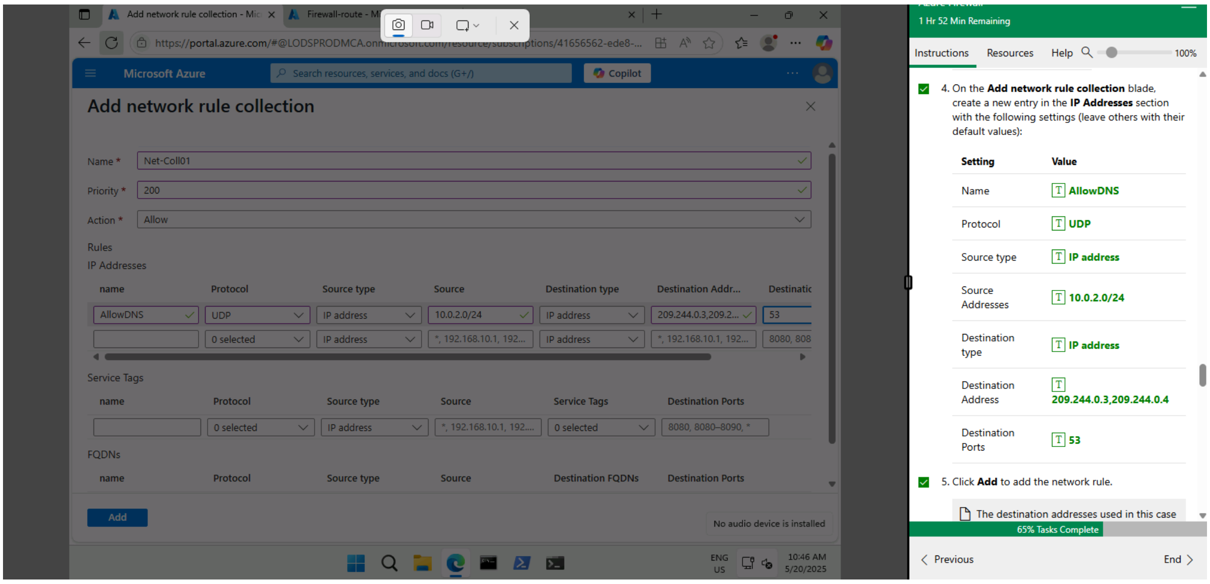
☑ 3. On the **Add network rule collection** blade, specify the following settings (leave others with their default values):

Setting	Value
Name	Net-Coll01

63% Tasks Complete

Task 5: Configure a Network Rule

In this task, I created a network rule to allow DNS resolution. Under the firewall's network rule collection, I added a new rule collection named Net-Coll01 with action set to allow. I created a rule called AllowDNS that permitted UDP traffic from 10.0.2.0/24 to destination IPs 209.244.0.3 and 209.244.0.4 on port 53. These public IPs are external DNS servers. This step demonstrated how Azure Firewall can allow or block traffic at the protocol and port level, ensuring only necessary network traffic is permitted.



Add network rule collection - Mic
Firewall-route - M
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/41656562-ede8-...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot

Add network rule collection

Name * Net-Coll01

Priority * 200

Action * Allow

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addr...	Destinatic
AllowDNS	UDP	IP address	10.0.2.0/24	IP address	209.244.0.3,209.2...	53
	0 selected	IP address	*, 192.168.10.1, 192...	IP address	*, 192.168.10.1, 192...	8080, 808

Service Tags

name	Protocol	Source type	Source	Service Tags	Destination Ports
	0 selected	IP address	*, 192.168.10.1, 192....	0 selected	8080, 8080–8090, *

FQDNs

name	Protocol	Source type	Source	Destination FQDNs	Destination Ports

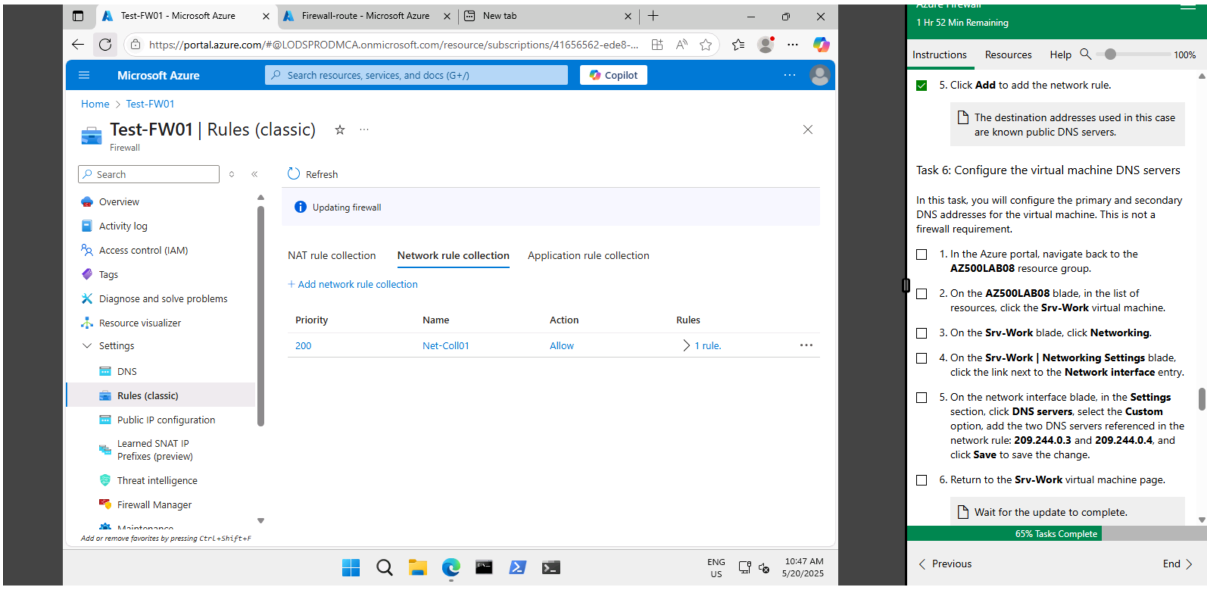
☑ 4. On the **Add network rule collection** blade, create a new entry in the **IP Addresses** section with the following settings (leave others with their default values):

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

65% Tasks Complete
Previous
End



Test-FW01 - Microsoft Azure
Firewall-route - Microsoft Azure
New tab
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/41656562-ede8-...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Test-FW01

Test-FW01 | Rules (classic)

Firewall

Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
DNS
Rules (classic)
Public IP configuration
Learned SNAT IP Prefixes (preview)
Threat intelligence
Firewall Manager
Maintenance
Add or remove favorites by pressing Ctrl+Shift+F
Refresh

Updating firewall

NAT rule collection
Network rule collection
Application rule collection
+ Add network rule collection

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

ENG US
10:47 AM 5/20/2025
1 Hr 52 Min Remaining
Instructions
Resources
Help
100%

☑ 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.

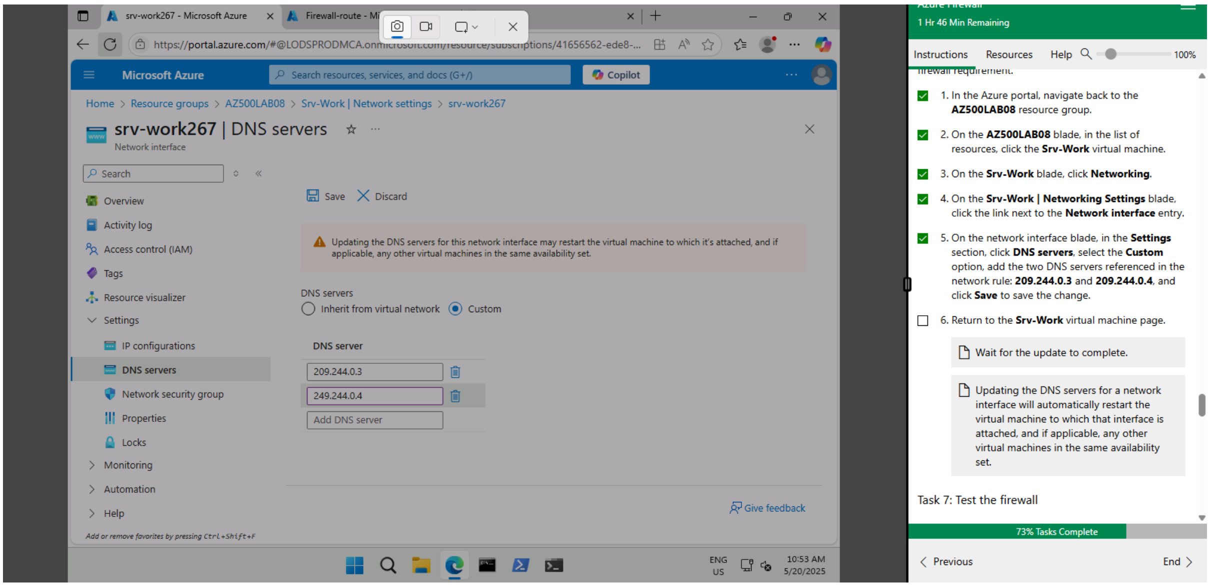
☐ 5. On the network interface blade, in the **Settings** section, click **DNS servers**, select the **Custom** option, add the two DNS servers referenced in the network rule: **209.244.0.3** and **209.244.0.4**, and click **Save** to save the change.

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

Wait for the update to complete.

Task 6: Configure DNS Servers

With the network rule in place, I updated the virtual machine's DNS settings. I navigated to the network interface of the Srv-Work VM and set its DNS servers to the same public IP addresses allowed in the previous task: 209.244.0.3 and 209.244.0.4. Saving this change caused the virtual machine to reboot automatically. This step was critical to ensure the VM could resolve domain names using the external DNS servers allowed by the firewall, thus enabling proper internet functionality within the security constraints.



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
249.244.0.4
Add DNS server

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.

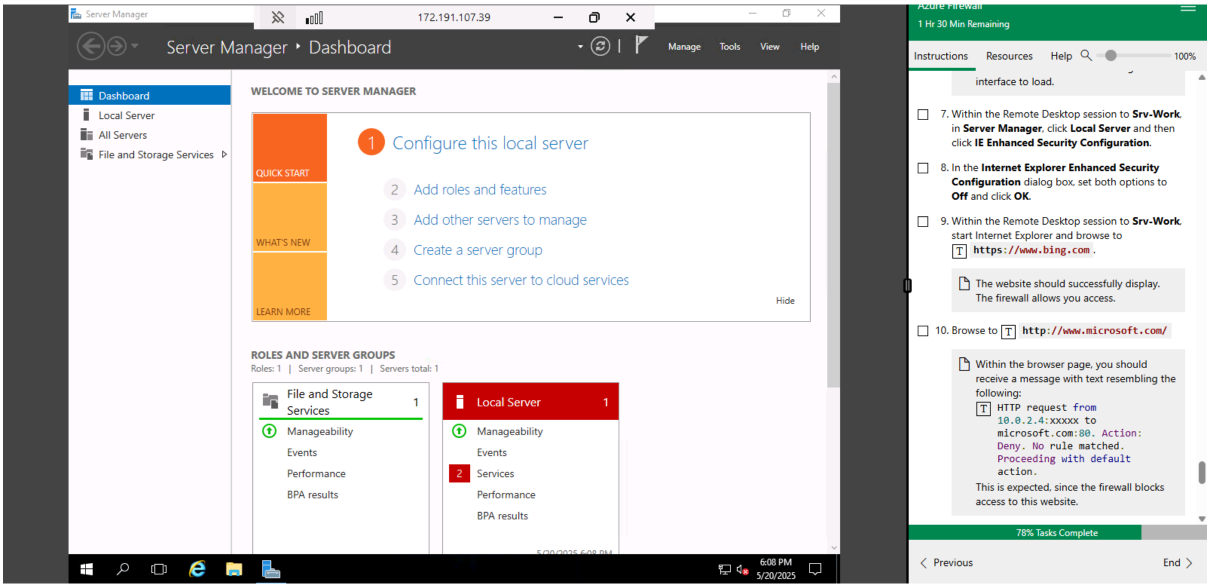
Wait for the update to complete.

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

Task 7: Test the Firewall

Finally, I tested the firewall setup. I connected to the Srv-Jump VM using Remote Desktop and, from there, connected to the Srv-Work VM. Once logged in, I attempted to browse to www.bing.com and verified that the request succeeded, confirming that the application rule was functioning. I also tested DNS resolution to ensure the firewall network rule was allowing DNS traffic as configured. This final task validated that the Azure Firewall was correctly filtering and allowing traffic based on the defined security policies.



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.

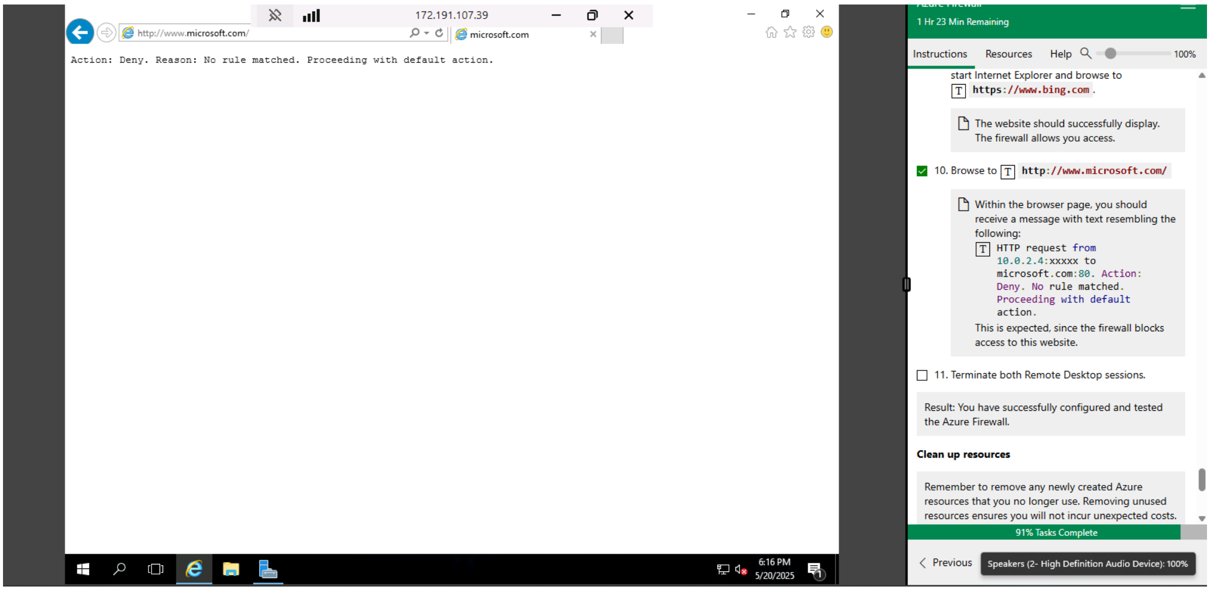
□ 10. Browse to `http://www.microsoft.com/`

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

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

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

78% Tasks Complete



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

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.

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.

91% Tasks Complete

Conclusion

Completing this lab provided hands-on experience in deploying and configuring Azure Firewall to secure virtual network traffic. Each task progressively built on the previous one to create a functional and secure network environment. I learned how to route traffic through the firewall, apply granular access control via application and network rules, and ensure DNS functionality through explicit permissions. This lab emphasized the importance of proper firewall configuration as a cornerstone of cloud network security. The practical skills acquired are directly applicable in real-world scenarios where protecting cloud resources is a top priority.