Cyber Shujaa

Cloud Security Specialist

Assignment 13: Lab 3 - Azure Firewall

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

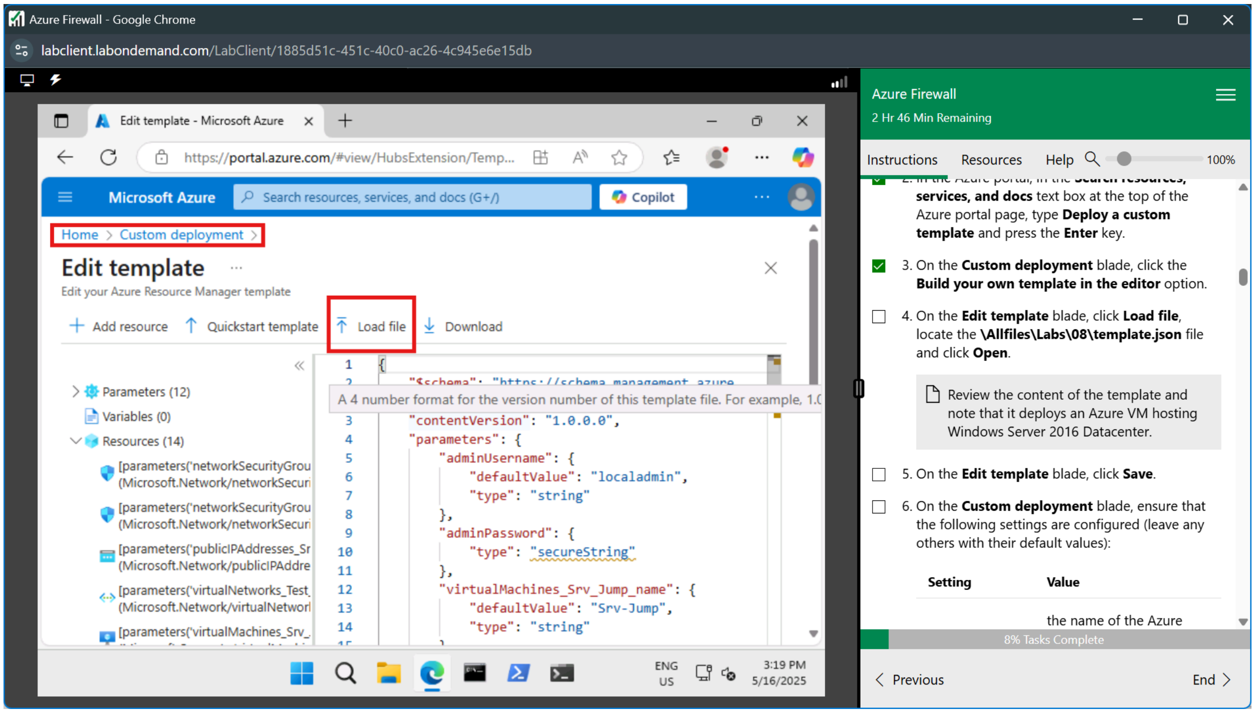
Introduction

In this lab scenario, we will install Azure Firewall. This will help control inbound and outbound network access which is an important part of an overall network security plan. We will specifically walk through creating and testing a virtual network with hosts, custom routes and firewall rules fro both network and application that safeguards our overall network.

Deploy and test an Azure Firewall

In this task, we will use a template to deploy our environment then, deploy an Azure Firewall, create a default rule, deploy a network rule and an application rule, configure a DNS server and test the firewall.

In custom deployment page, we provision our own template through the following steps.


Azure Firewall - Google Chrome
labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db
Edit template - Microsoft Azure
https://portal.azure.com/#view/HubsExtension/Temp...
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('networkSecurityGrou (Microsoft.Network/networkSecuri
[parameters('networkSecurityGrou (Microsoft.Network/networkSecuri
[parameters('publicIPAddresses_Sr (Microsoft.Network/publicIPAddre
[parameters('virtualNetworks_Test_ (Microsoft.Network/virtualNetwor
[parameters('virtualMachines_Srv_
ENG
US
3:19 PM
5/16/2025
Azure Firewall
2 Hr 46 Min Remaining
Instructions
Resources
Help
100%
8% Tasks Complete
Previous
End

A 4 number format for the version number of this template file. For example, 1.(

```
{
    "$schema": "https://schema.management.azure
    "contentVersion": "1.0.0.0",
    "parameters": {
        "adminUsername": {
            "defaultValue": "localadmin",
            "type": "string"
        },
        "adminPassword": {
            "type": "secureString"
        },
        "virtualMachines_Srv_Jump_name": {
            "defaultValue": "Srv-Jump",
            "type": "string"
```

☑ **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**.

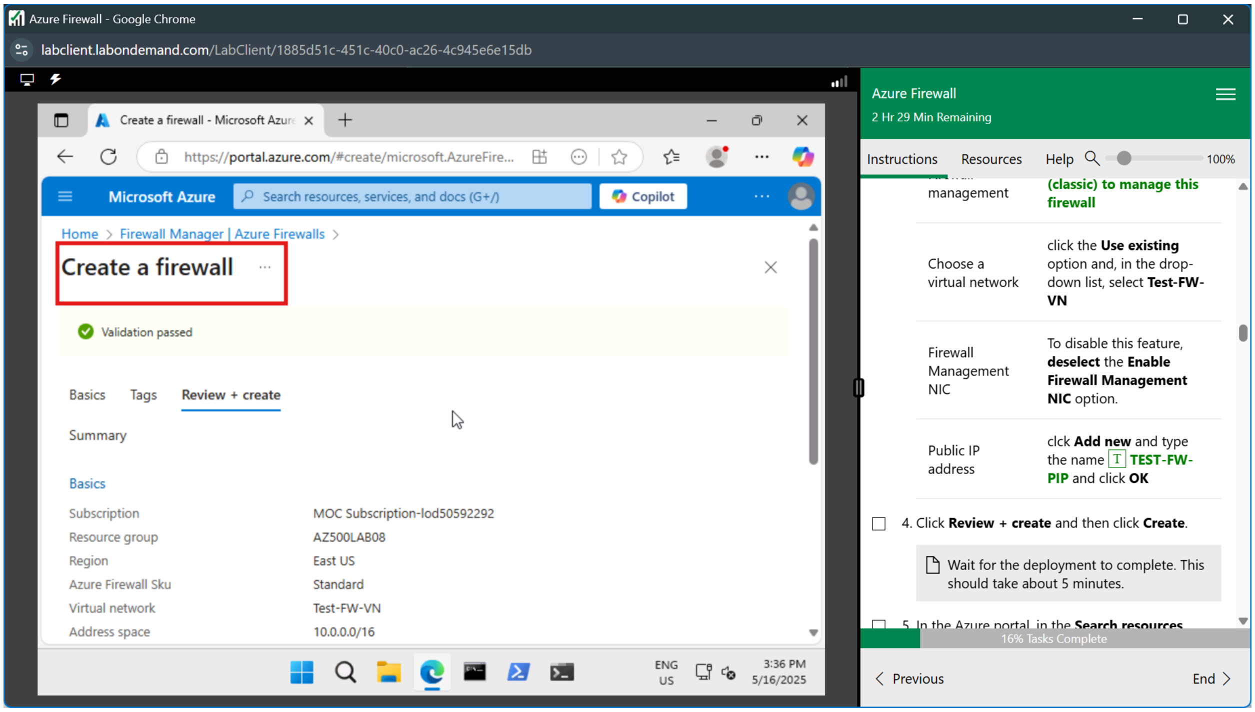
> Review the content of the template and note that it deploys an Azure VM hosting Windows Server 2016 Datacenter.

□ 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
	the name of the Azure

Here we load an existing template to provision our resources as defined in the template. With a successful deployment we can now deploy our firewall as shown below



Azure Firewall - Google Chrome
labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db
Create a firewall - Microsoft Azure
https://portal.azure.com/#create/microsoft.AzureFire...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Firewall Manager | Azure Firewalls >
ENG US
3:36 PM 5/16/2025

Create a firewall

Validation passed

Basics | Tags | Review + create

Summary

Basics

Subscription	MOC Subscription-lod50592292
Resource group	AZ500LAB08
Region	East US
Azure Firewall Sku	Standard
Virtual network	Test-FW-VN
Address space	10.0.0.0/16

Azure Firewall

2 Hr 29 Min Remaining

Instructions
Resources
Help
100%

management	(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**

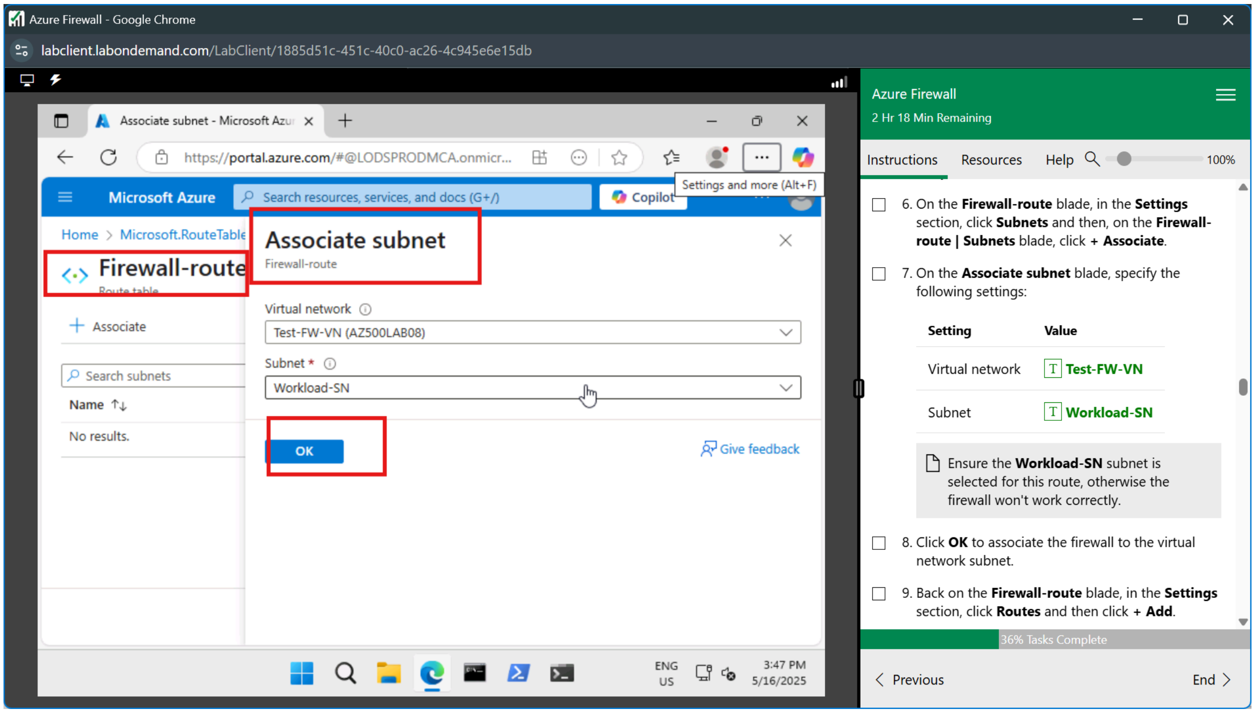
☐ 4. Click **Review + create** and then click **Create**.

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

☐ 5. In the Azure portal, in the **Search resources**

16% Tasks Complete

We then create a default route for the Workload-SN subnet. This route will configure outbound traffic through the firewall. We will also associate our route with the workload subnet as shown.



Azure Firewall - Google Chrome
labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db
Associate subnet - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicr...
Settings and more (Alt+F)
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Microsoft.RouteTable
Firewall-route
Route table
Associate
Search subnets
Name
No results.
Give feedback
ENG US
3:47 PM 5/16/2025

Associate subnet

Firewall-route

Virtual network: Test-FW-VN (AZ500LAB08)

Subnet *: Workload-SN

OK

Azure Firewall

2 Hr 18 Min Remaining

Instructions
Resources
Help
100%

☐ 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**

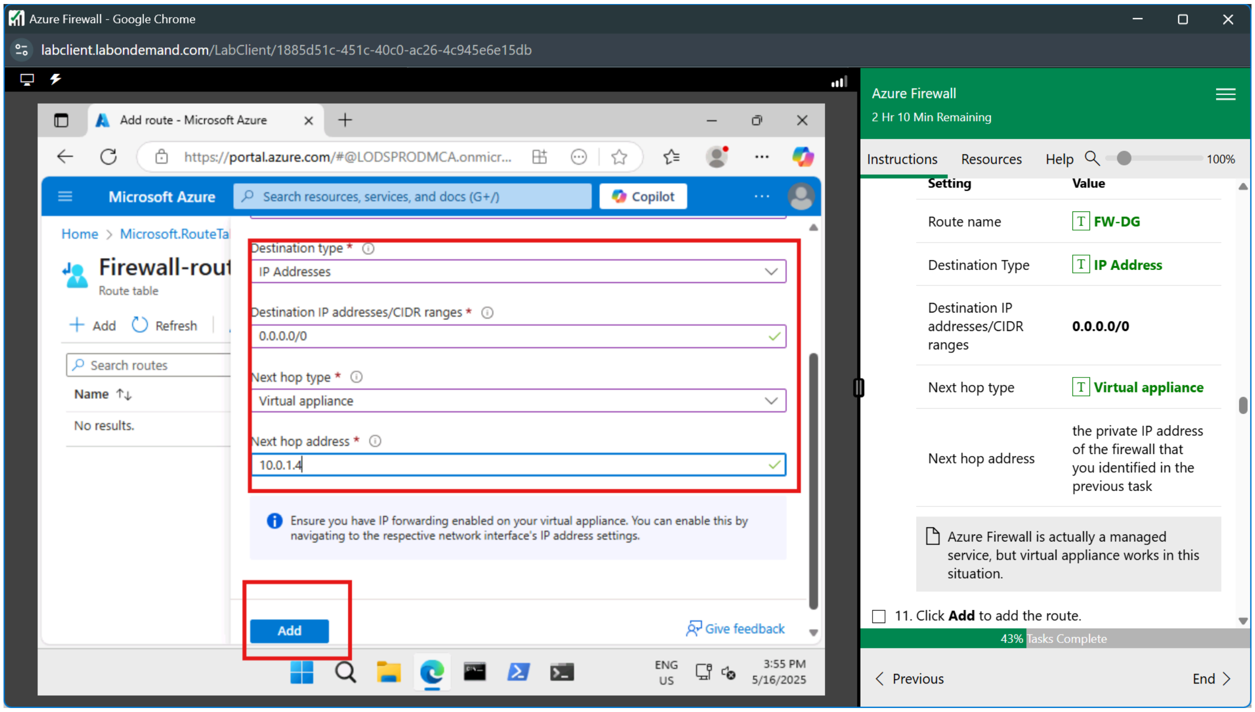
Ensure the **Workload-SN** subnet is selected for this route, otherwise the firewall won't work correctly.

☐ 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**.

36% Tasks Complete

We can then add a route to our firewall with the following configurations.


Azure Firewall - Google Chrome

labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db

Add route - Microsoft Azure

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

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

Home > Microsoft.RouteTa

Firewall-rout
Route table

+ Add | Refresh

Search routes

Name ↑↓

No results.

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.

Add

Give feedback

ENG US 3:55 PM 5/16/2025

Azure Firewall
2 Hr 10 Min Remaining

Instructions | Resources | Help | 100%

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

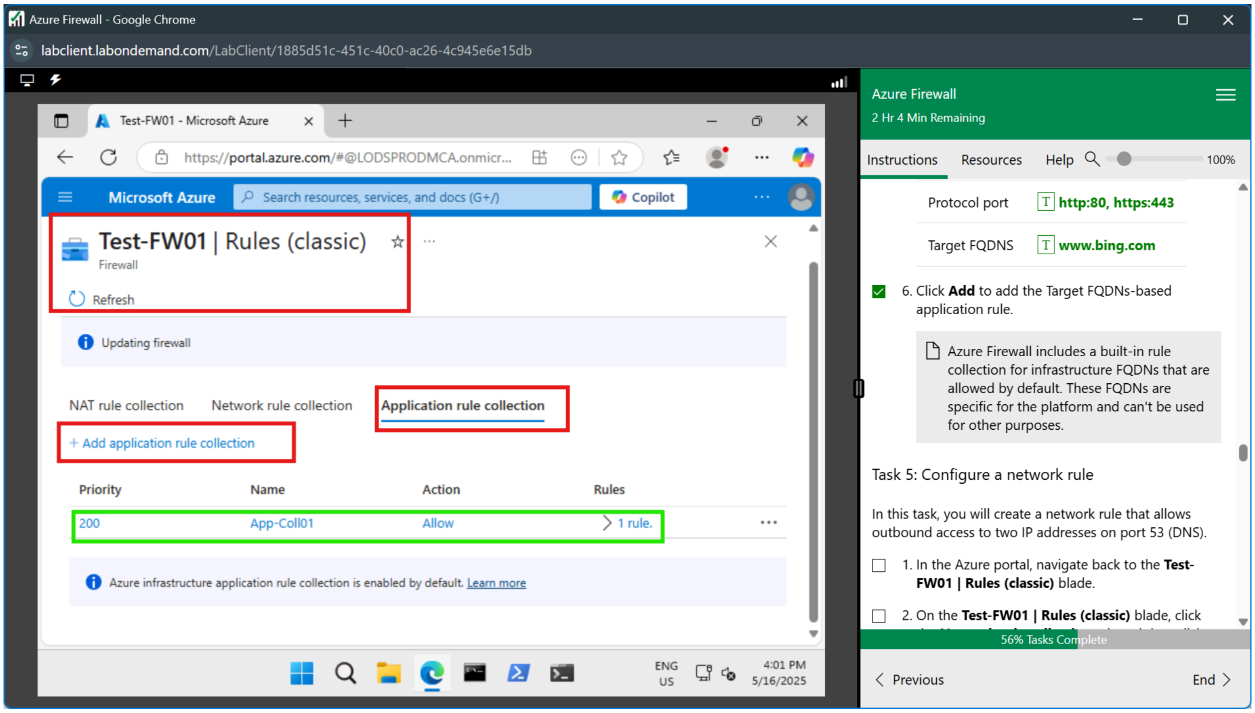
Azure Firewall is actually a managed service, but virtual appliance works in this situation.

□ 11. Click **Add** to add the route.

43% Tasks Complete

Previous | End

In this step, we will create an application rule on our Firewall to allow only outbound traffic to Bing.com


Azure Firewall - Google Chrome

labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db

Test-FW01 - Microsoft Azure

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

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

Test-FW01 | Rules (classic)
Firewall

Refresh

Updating firewall

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

ENG US 4:01 PM 5/16/2025

Azure Firewall
2 Hr 4 Min Remaining

Instructions | Resources | Help | 100%

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).

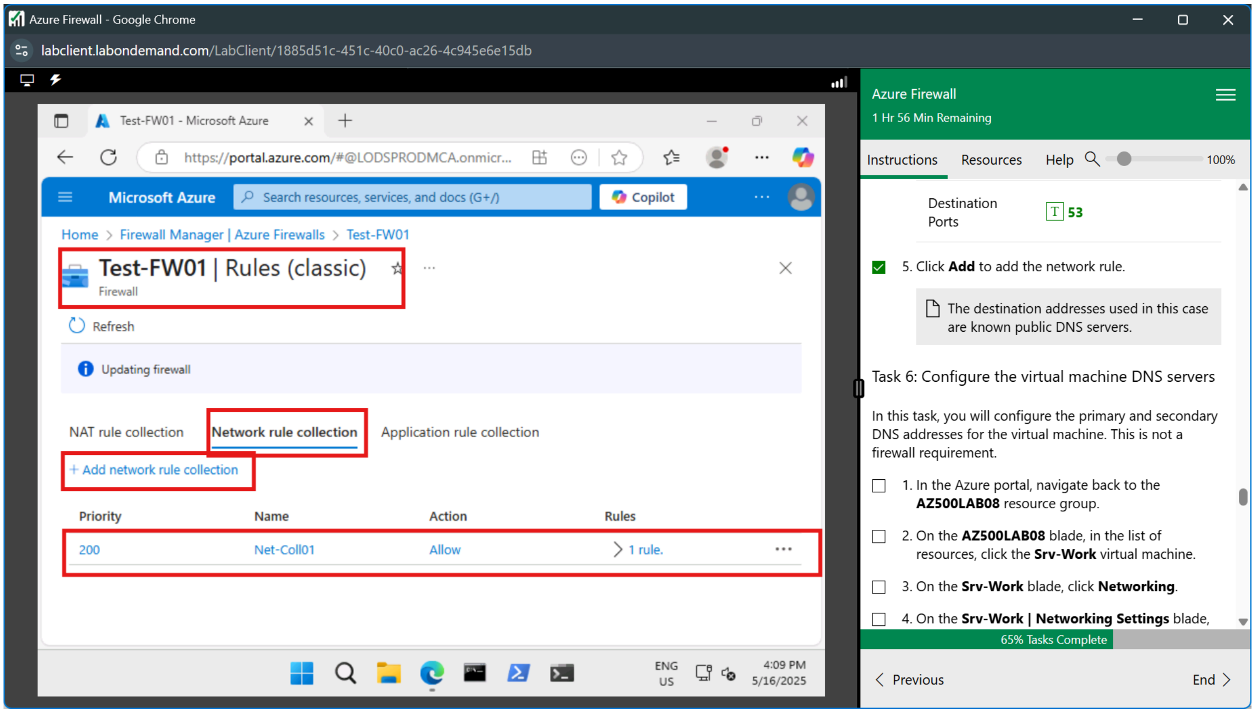
□ 1. In the Azure portal, navigate back to the **Test-FW01 | Rules (classic)** blade.

□ 2. On the **Test-FW01 | Rules (classic)** blade, click

56% Tasks Complete

Previous | End

After the application rule, we then configure a network rule that allows outbound access to two IP addresses on port 53 (DNS).


Azure Firewall - Google Chrome
labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db
Test-FW01 - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicr...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Firewall Manager | Azure Firewalls > Test-FW01
Refresh
NAT rule collection
Network rule collection
Application rule collection
+ Add network rule collection
ENG US
4:09 PM 5/16/2025
Azure Firewall
1 Hr 56 Min Remaining
Instructions
Resources
Help
100%
65% Tasks Complete
Previous
End

Test-FW01 | Rules (classic)
Firewall

Updating firewall

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

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.

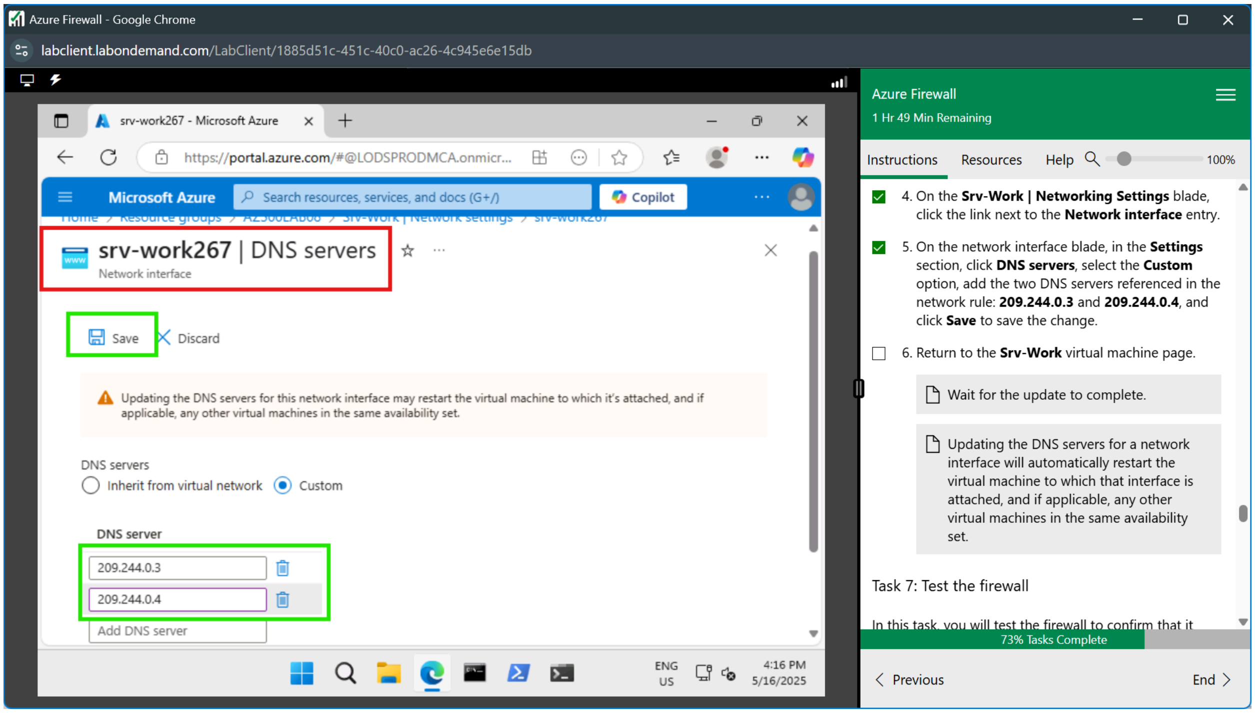
☐ 1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

☐ 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,

Next, we will configure the virtual machine's primary and secondary DNS addresses, although this is not a firewall requirement.


Azure Firewall - Google Chrome
labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db
srv-work267 - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicr...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Resource groups > AZ500LAB08 > Srv-Work | Network settings > srv-work267
Save
Discard
ENG US
4:16 PM 5/16/2025
Azure Firewall
1 Hr 49 Min Remaining
Instructions
Resources
Help
100%
73% Tasks Complete
Previous
End

srv-work267 | DNS servers
Network interface

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

☑ 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.

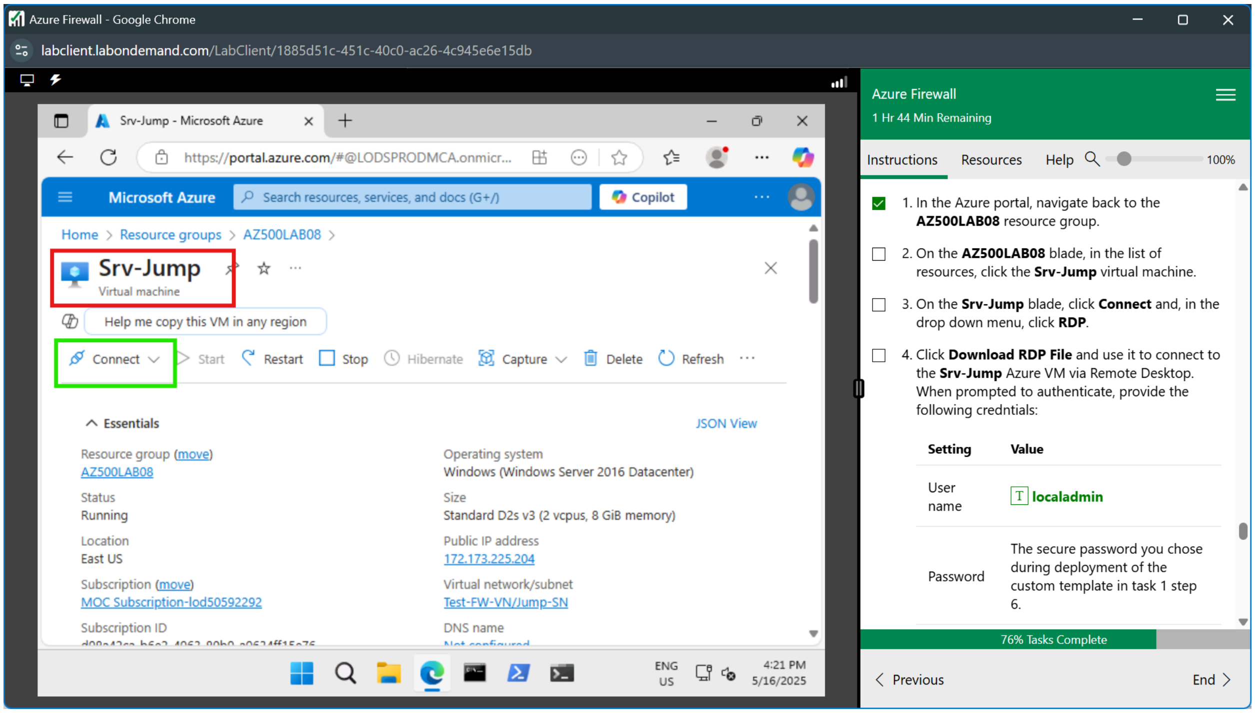
Wait for the update to complete.

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

Now we can test our Firewall to confirm that it works as expected. We will use the jump host provisioned in the subnets to achieve this.



Azure Firewall - Google Chrome

labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db

Srv-Jump - Microsoft Azure

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

Microsoft Azure

Home > Resource groups > AZ500LAB08 >

Srv-Jump
Virtual machine

Help me copy this VM in any region

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh

Essentials | JSON View

Resource group (move) AZ500LAB08	Operating system Windows (Windows Server 2016 Datacenter)
Status Running	Size Standard D2s v3 (2 vcpus, 8 GiB memory)
Location East US	Public IP address 172.173.225.204
Subscription (move) MOC Subscription-lod50592292	Virtual network/subnet Test-FW-VN/Jump-SN
Subscription ID	DNS name

4:21 PM 5/16/2025

Azure Firewall
1 Hr 44 Min Remaining

Instructions | Resources | Help | 100%

☑ 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**.

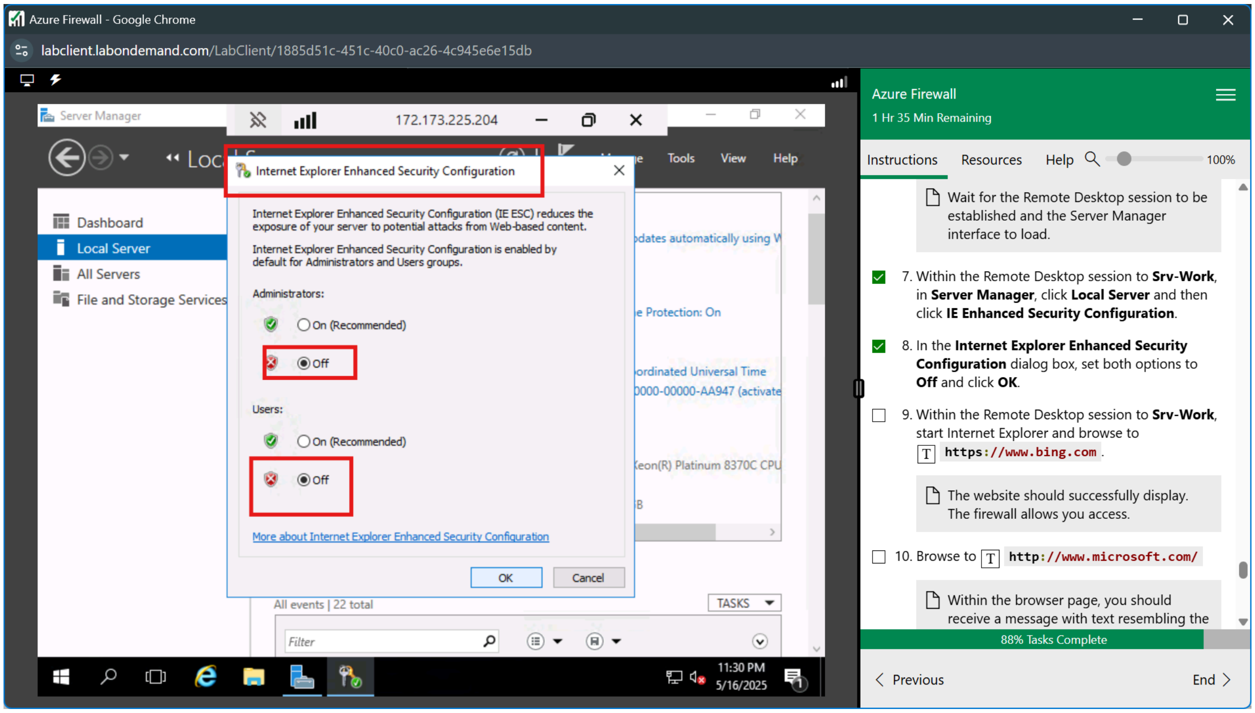
□ 4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

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

76% Tasks Complete

Previous | End

After connecting to our work server we configure the IE enhanced security configurations to allow us to use the server for web content.



Azure Firewall - Google Chrome

labclient.labondemand.com/LabClient/1885d51c-451c-40c0-ac26-4c945e6e15db

Server Manager

172.173.225.204

Dashboard
Local Server
All Servers
File and Storage Services

Tools | View | Help

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

More about Internet Explorer Enhanced Security Configuration

OK | Cancel

All events | 22 total

TASKS

11:30 PM 5/16/2025

Azure Firewall
1 Hr 35 Min Remaining

Instructions | Resources | Help | 100%

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

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

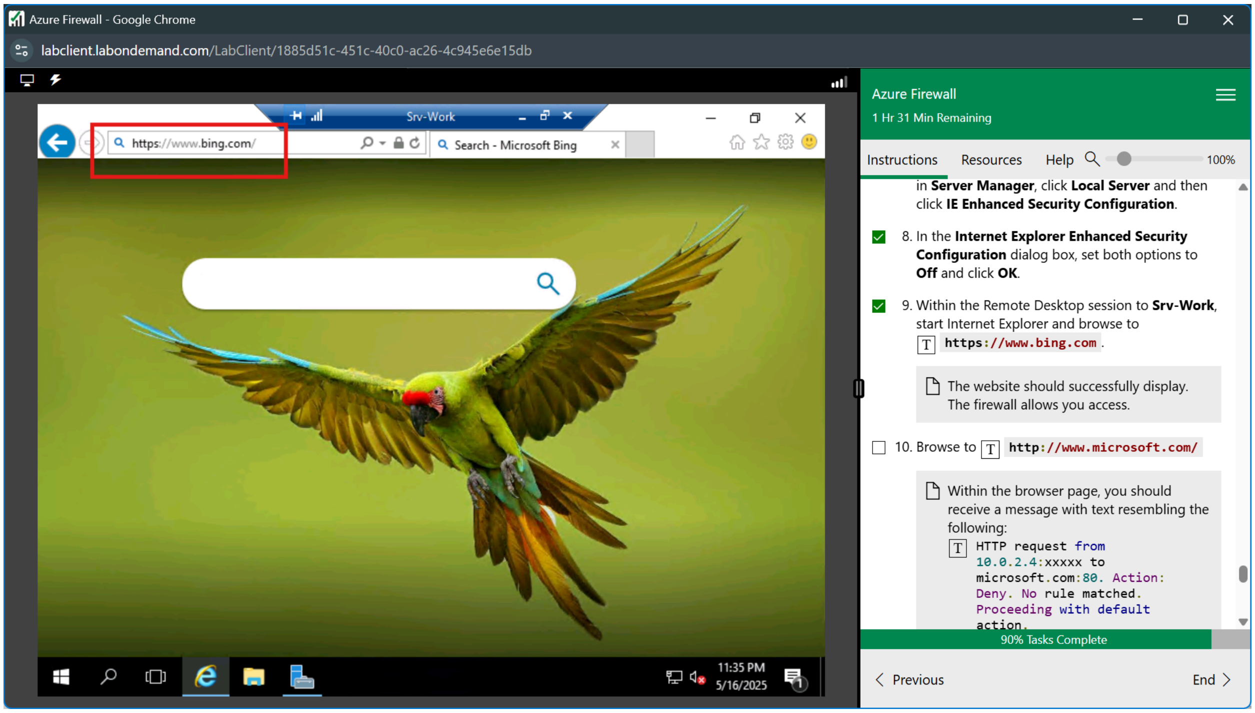
□ 10. Browse to T `http://www.microsoft.com/`

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

88% Tasks Complete

Previous | End

We then visited www.bing.com to confirm successful browsing as per our application rule on the firewall.



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`.

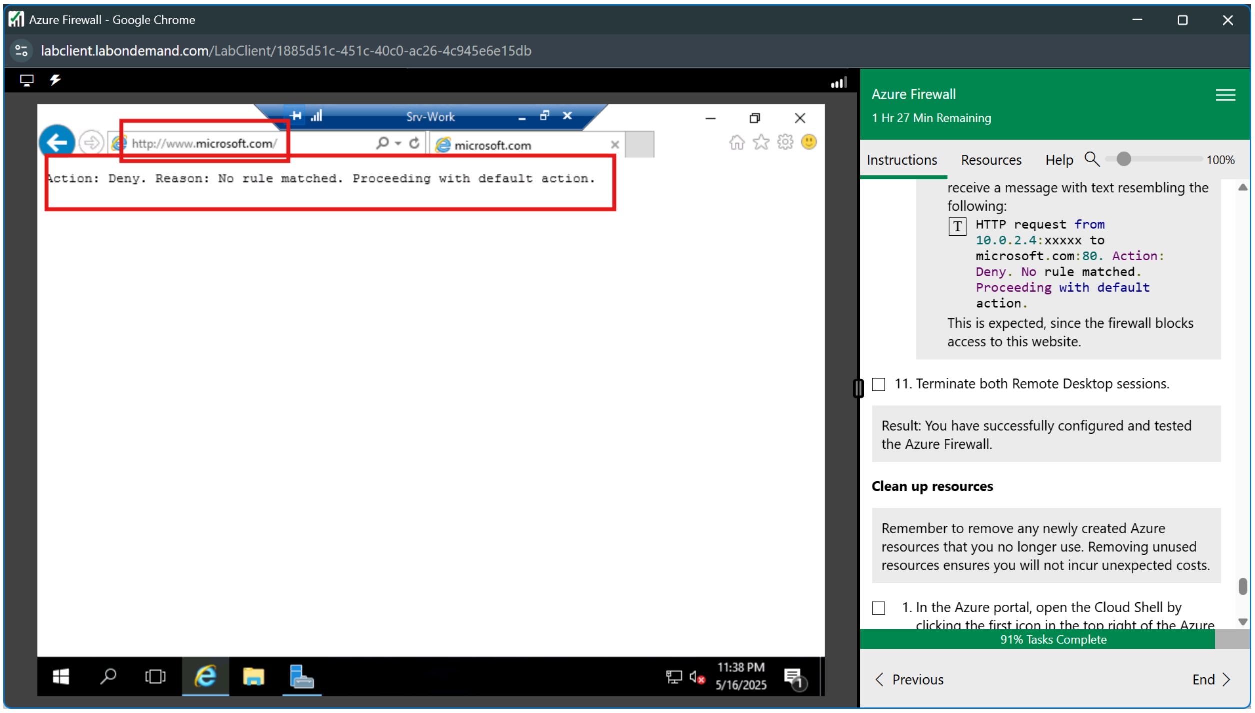
The website should successfully display. The firewall allows you access.

□ 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.
```

Navigating to microsoft.com gave us an error as shown below.



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

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 clicking the first icon in the top right of the Azure

Conclusion

In conclusion, we have learnt how to provision an Azure environment using a JSON template. The environment had a virtual network, a subnet and two VMs in the subnet. We then deployed a firewall to secure our network environment using application rules and network rules. We were also able to route traffic through our firewall using UDR.