Course: Cloud and Network Security C3-2024

Student Name: Loise Murugi Murage

Student No: **CS-CNS07-24115**.

Tuesday, November 12, 2024

Week 8 Assignment 1

Class Exercise: Azure Firewall

Week 8 Assignment 1: Azure Firewall

Contents

Introduction

In this lab, we will be installing Azure Firewall a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for cloud workloads running in Azure. We have used West US as the region.

We will be creating a default route that will configure outbound traffic through the firewall. Then configure the application rule (that will allow outbound access to www.bing.com) and the Network rule that will allow outbound access to two IP addresses on port 53 (DNS). Then lastly configure DNS servers and test the firewall.

Lab 03: Azure Firewall

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.

Lab objectives

In this lab, you will complete the following exercise:

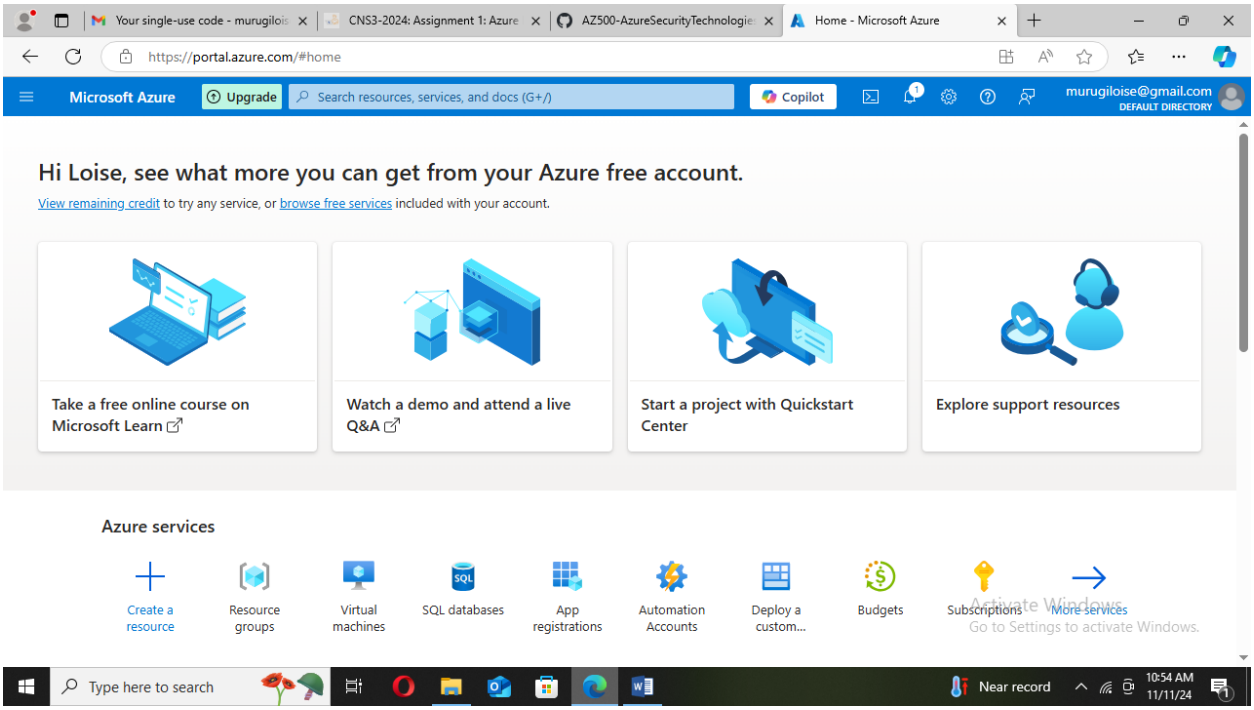
Exercise 1: Deploy and test an Azure Firewall

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

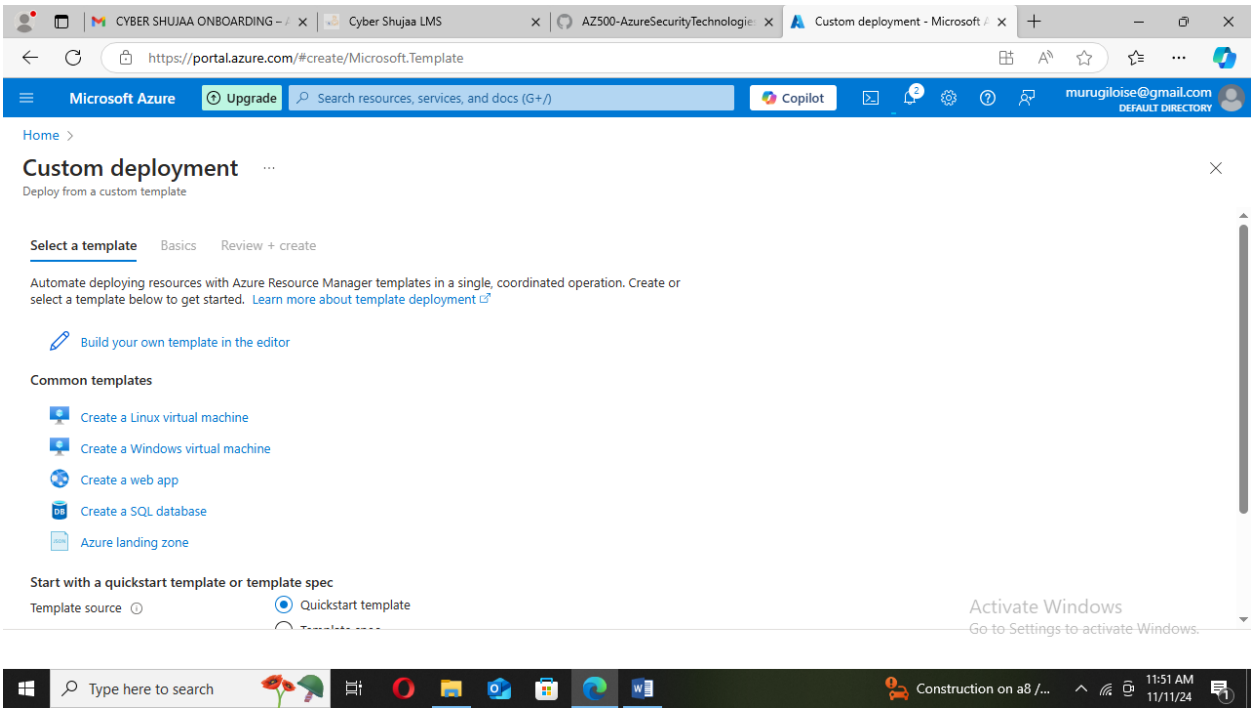
In this task, you will create a virtual machine by using an ARM template. This virtual machine will be used in the last exercise for this lab.

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

Week 8 Assignment 1: Azure Firewall

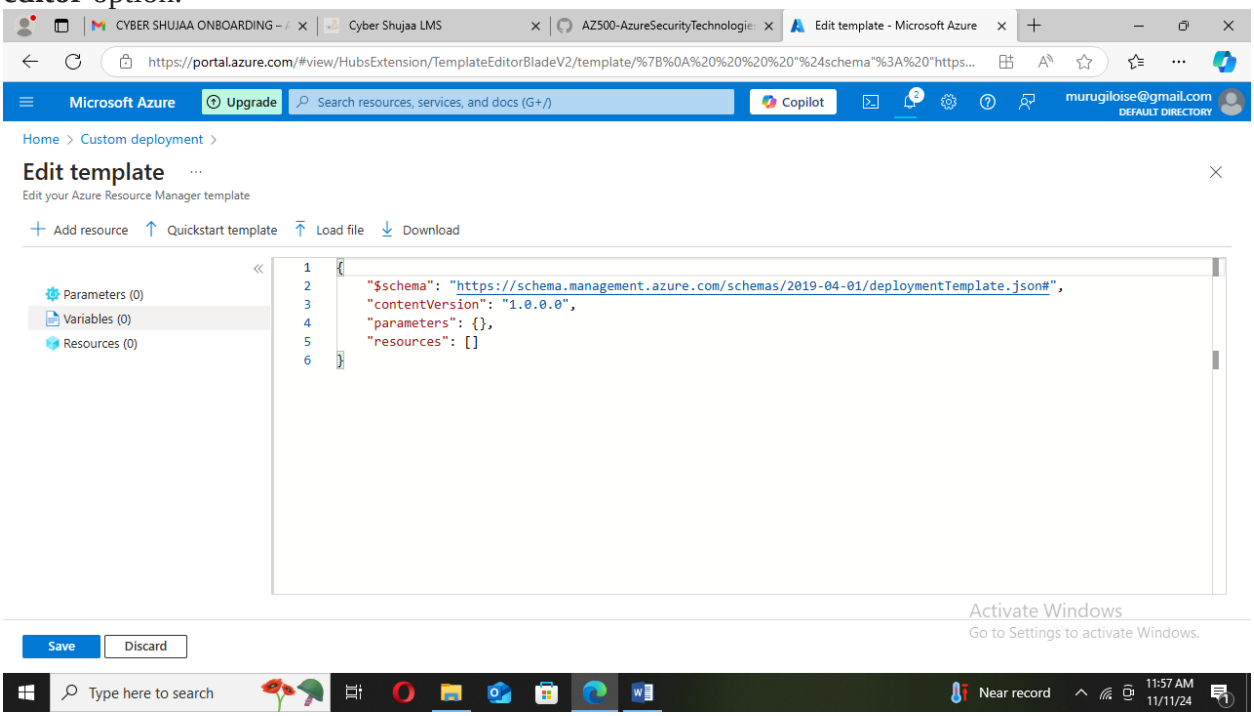


2. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Deploy a custom template** and press the **Enter** key.

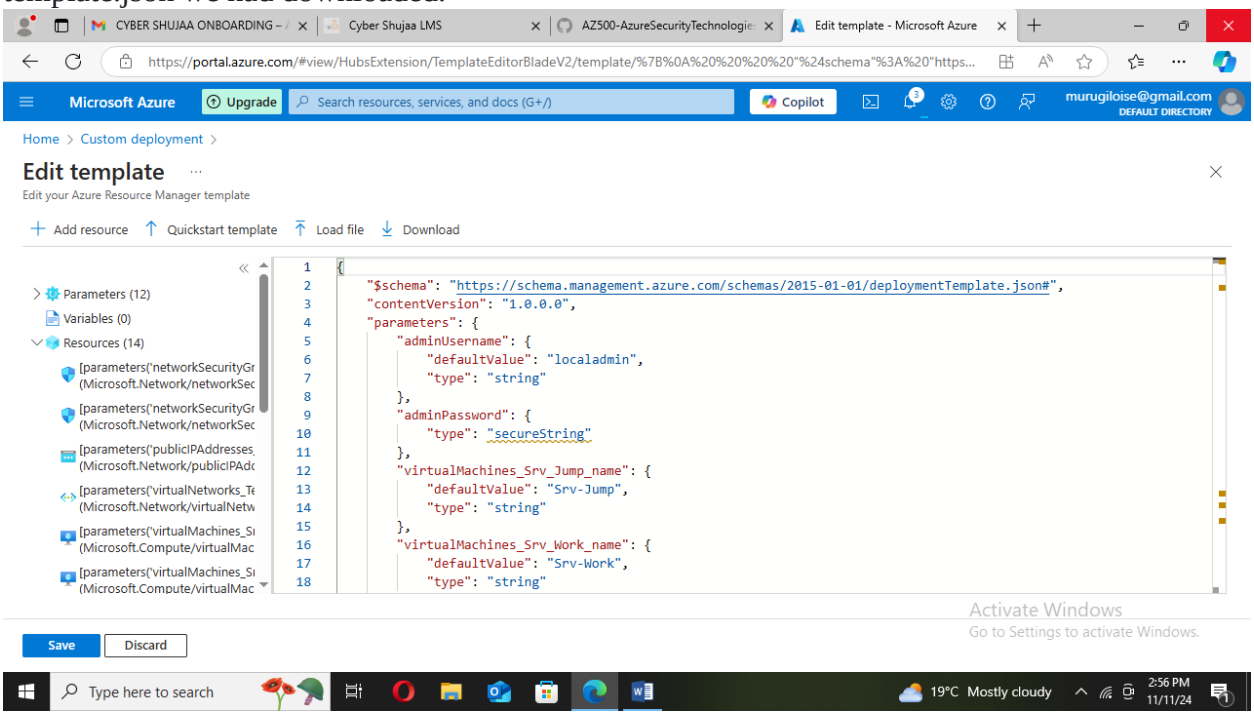


Week 8 Assignment 1: Azure Firewall

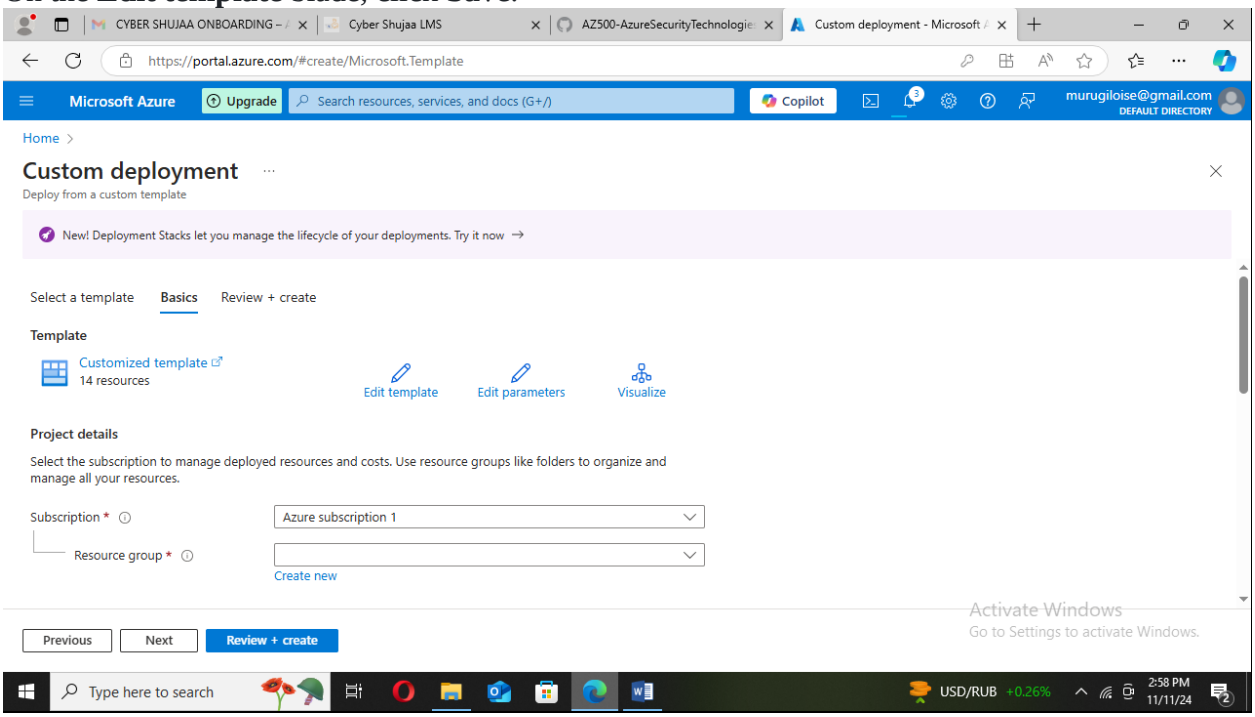
3. On the **Custom deployment** blade, click the **Build your own template in the editor** option.



4. On the **Edit template** blade, click **Load file**, locate the **\Allfiles\Labs\08\template.json** file and click **Open**. We have loaded the template.json we had downloaded.



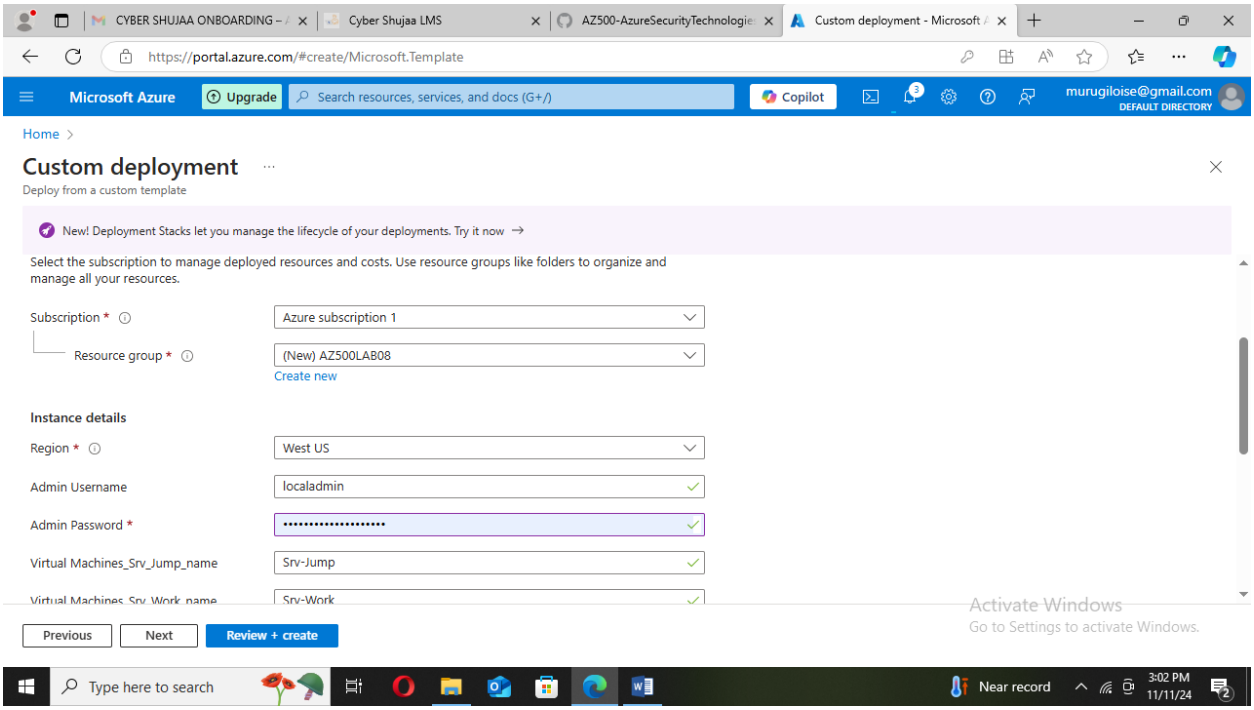
On the **Edit template** blade, click **Save**.



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	click **Create new** and type the name **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.

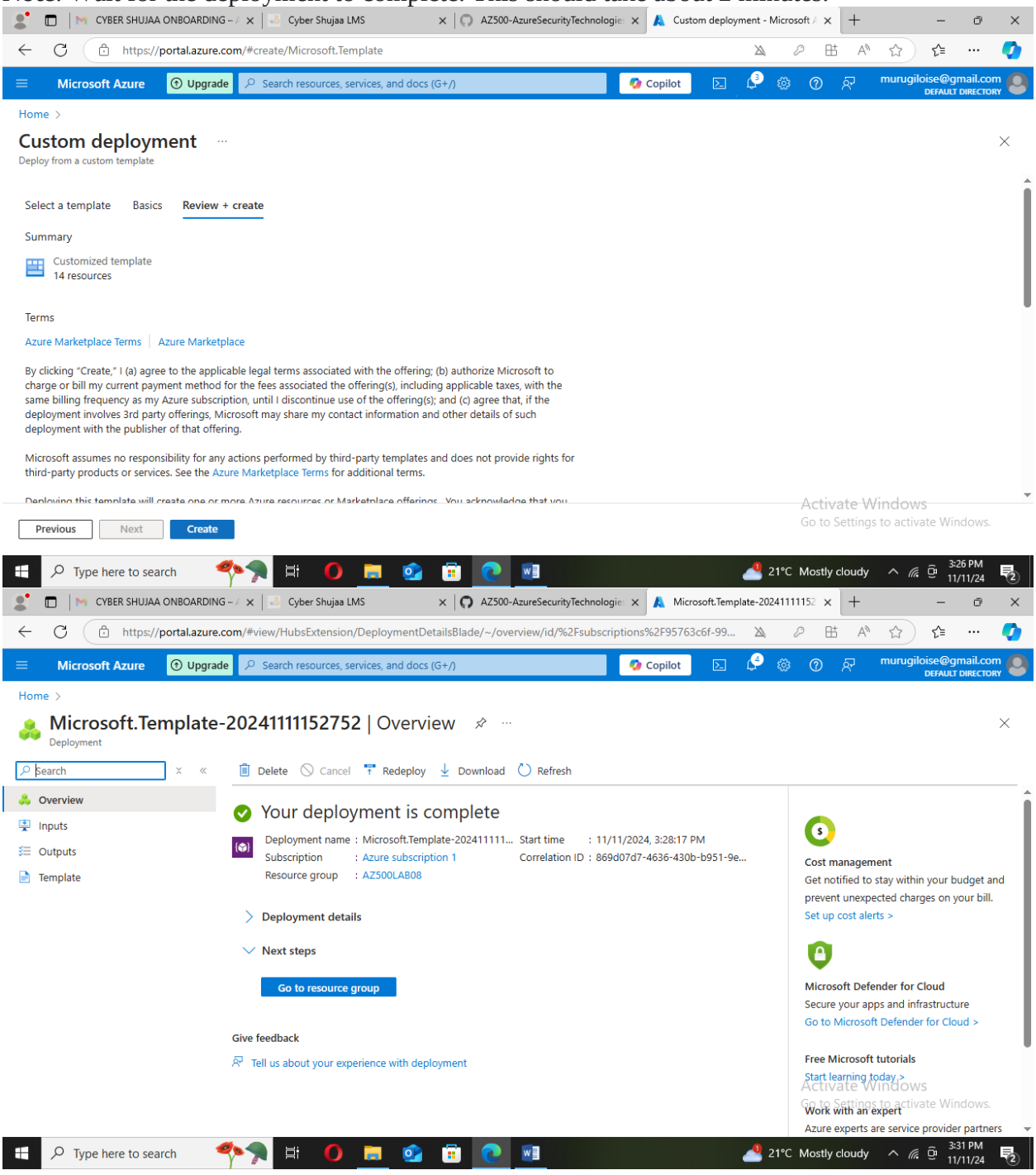
Week 8 Assignment 1: Azure Firewall



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

Week 8 Assignment 1: Azure Firewall

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

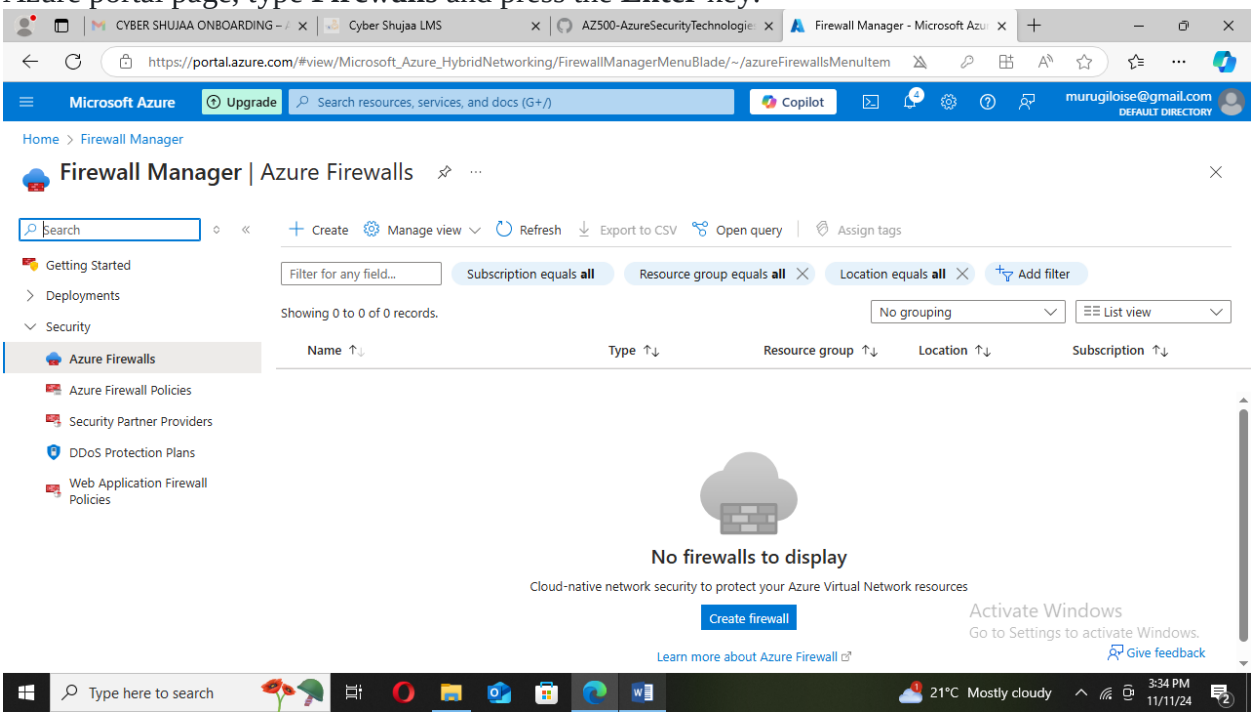


Task 2: Deploy the Azure firewall

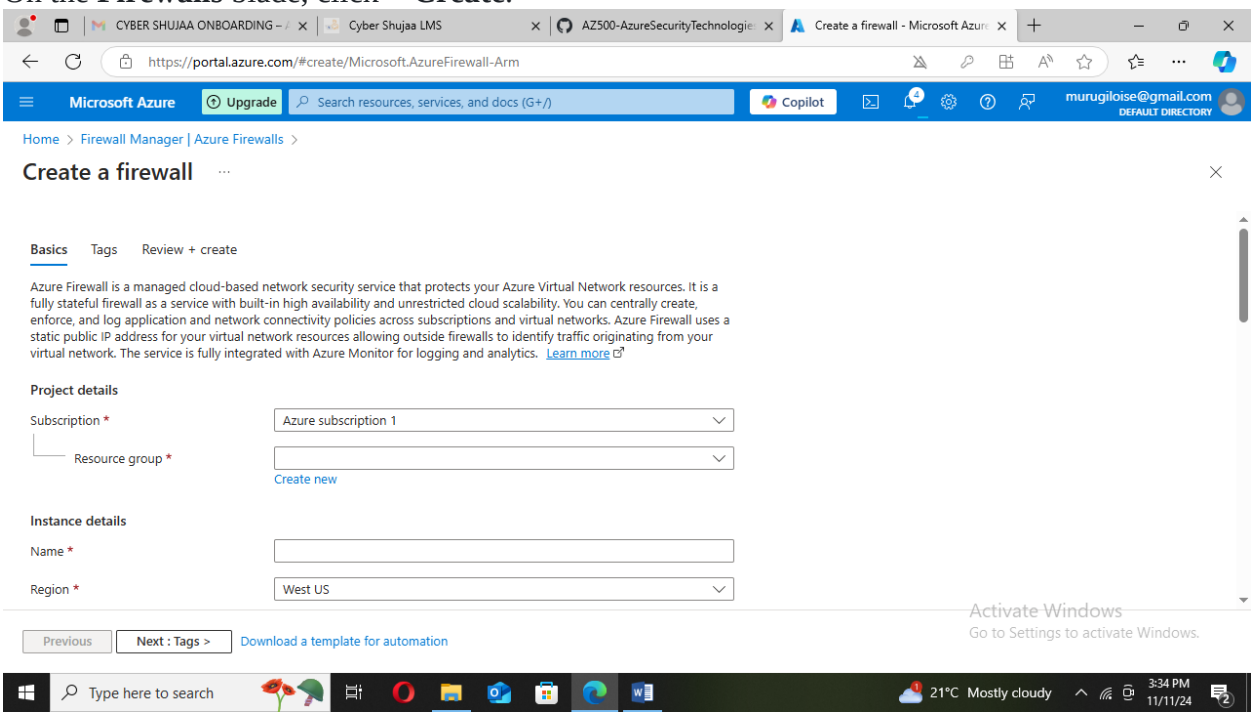
In this task you will deploy the Azure firewall into the virtual network.

Week 8 Assignment 1: 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 **Firewalls** and press the **Enter** key.



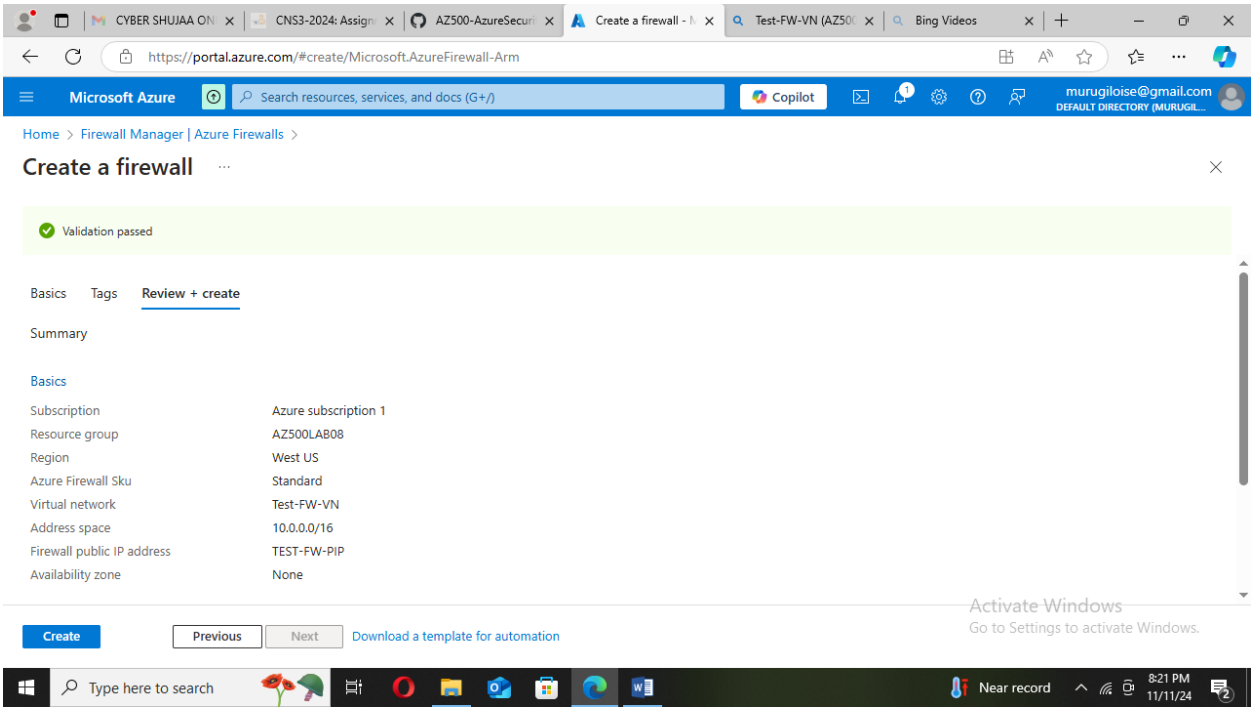
2. On the **Firewalls** blade, click **+ Create**.



3. On the **Basics** tab of the **Create a firewall** blade, specify the following settings (leave others with their default values):

Week 8 Assignment 1: Azure Firewall

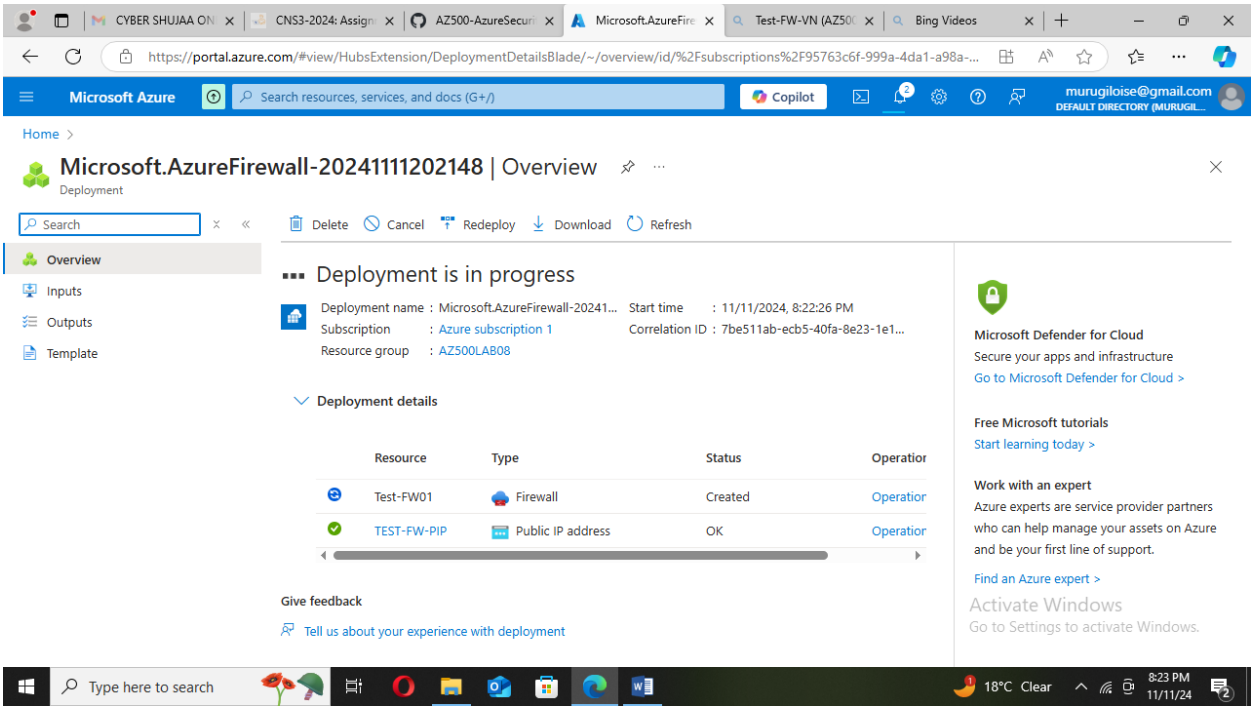
Setting	Value
Resource group	**AZ500LAB08**
Name	**Test-FW01**
Region	**(US) East US**
Firewall SKU	**Standard**
Firewall management	**Use Firewall rules (classic) to manage this firewall**
Choose a virtual network	click the **Use existing** option and, in the drop-down list, select **Test-FW-VN**
Public IP address	clck **Add new** and type the name **TEST-FW-PIP** and click **OK**



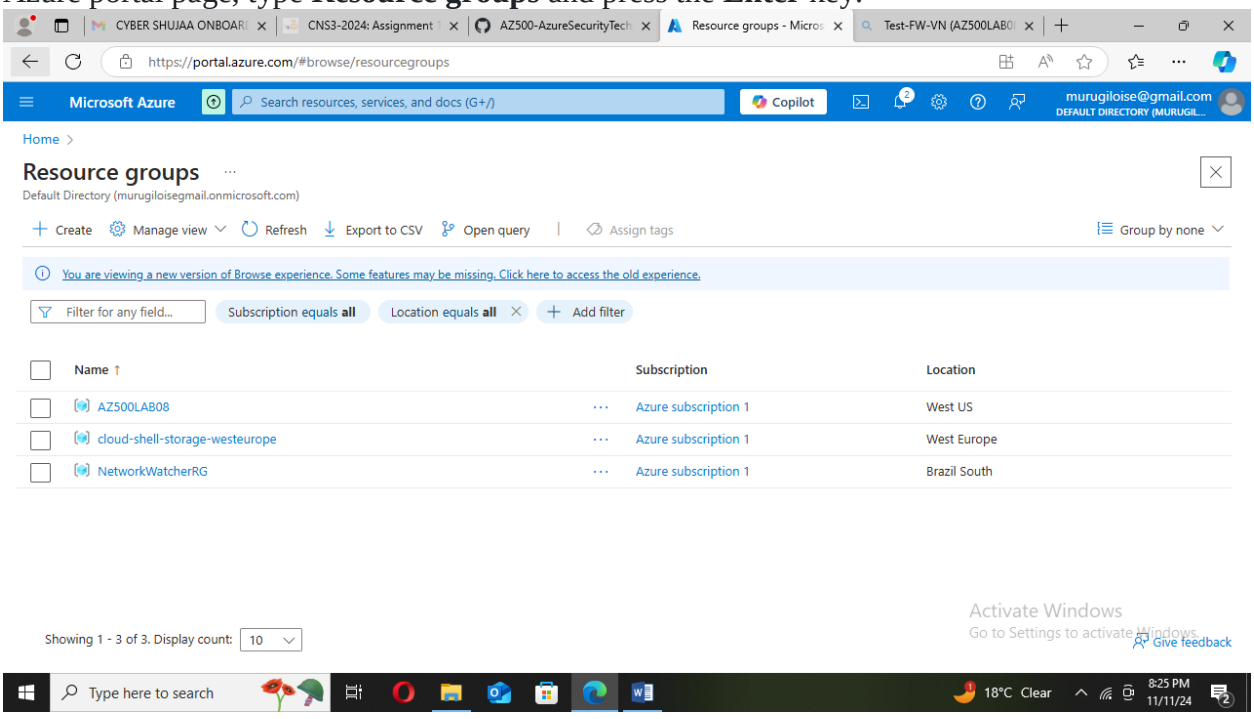
4. Click **Review + create** and then click **Create**.

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

Week 8 Assignment 1: Azure Firewall



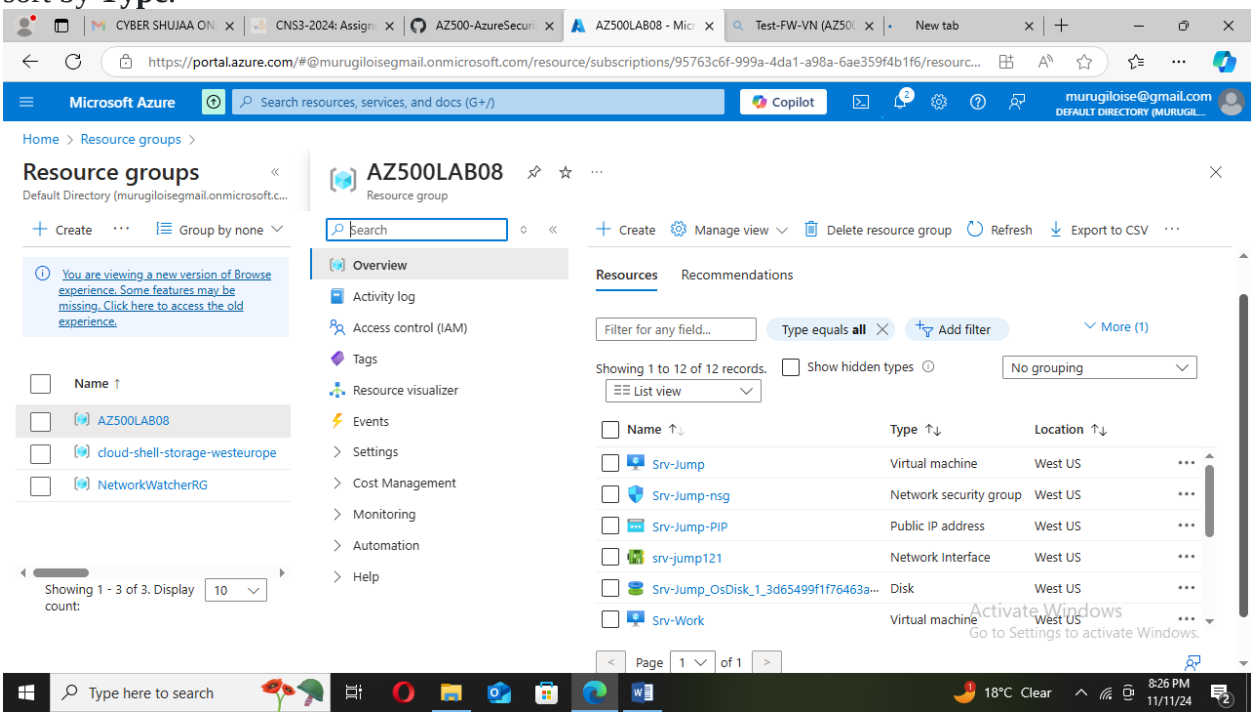
5. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Resource groups** and press the **Enter** key.



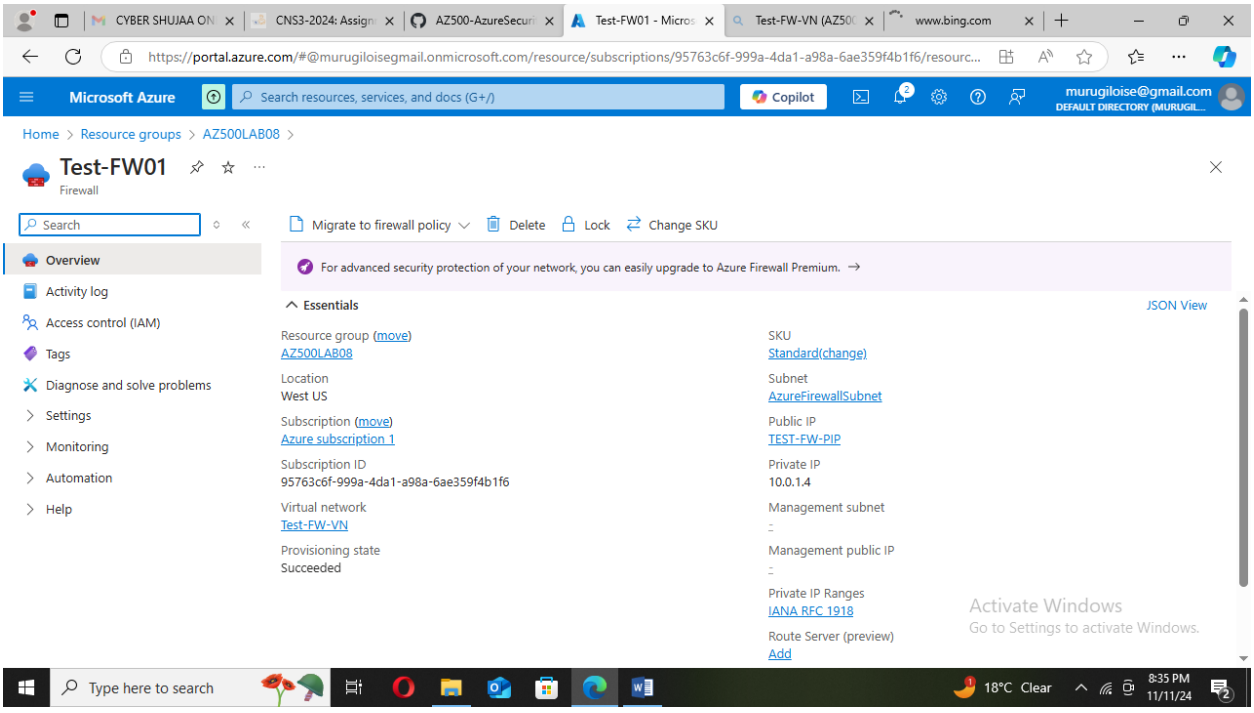
6. On the **Resource groups** blade, in the list of resource group, click the **AZ500LAB08** entry.

Week 8 Assignment 1: Azure Firewall

Note: 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.



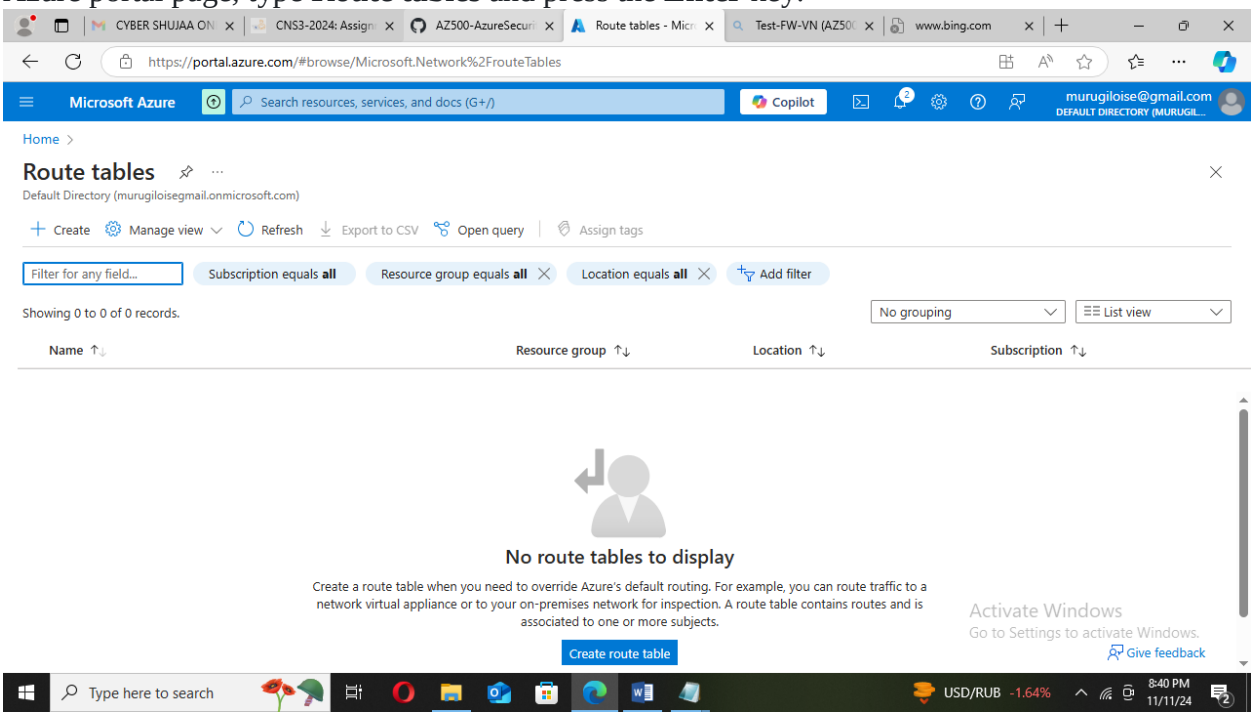
8. On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

Note: You will need this information in the next task. The private IP is 10.0.1.4

Task 3: Create a default route

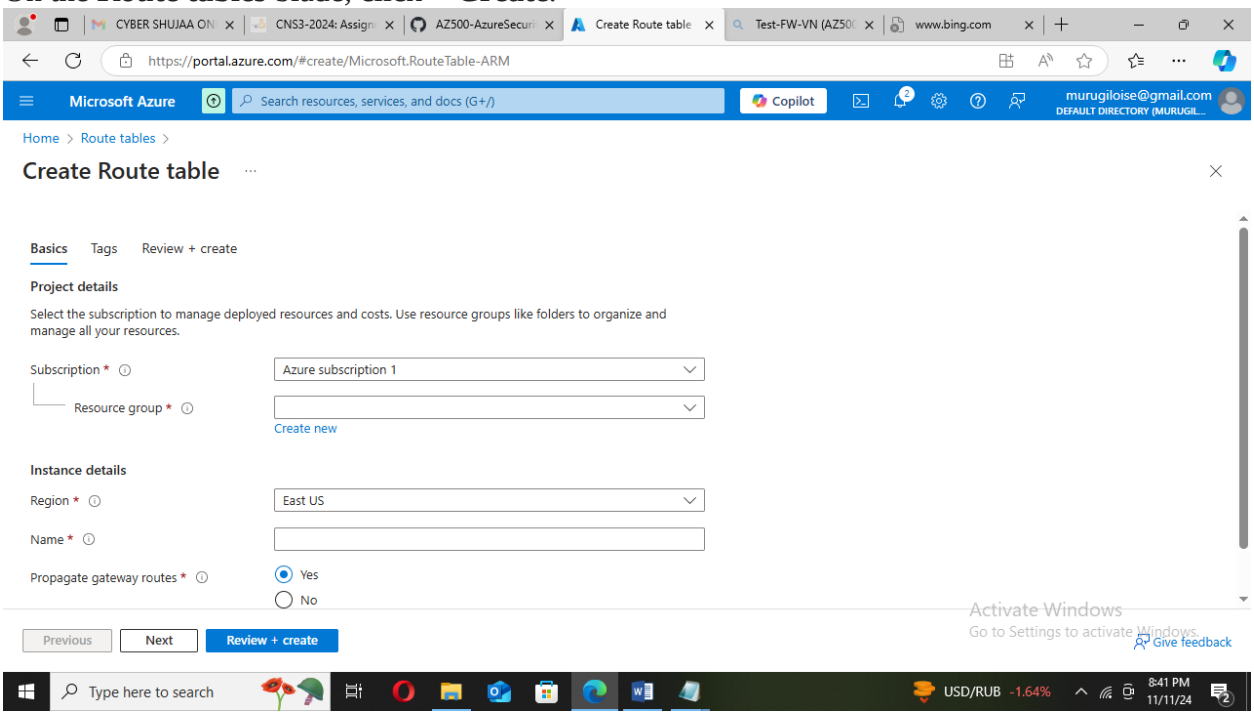
In this task, you will create a default route for the **Workload-SN** subnet. This route will configure outbound traffic through the firewall.

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.



Week 8 Assignment 1: Azure Firewall

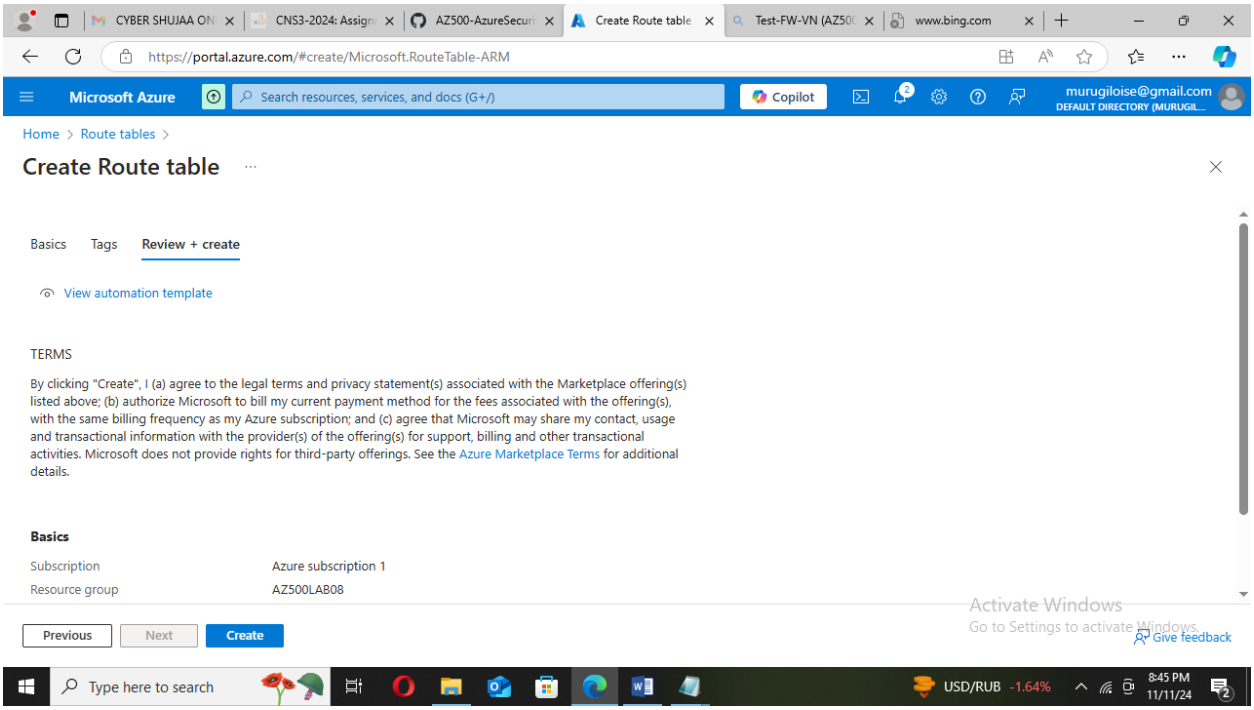
2. On the **Route tables** blade, click **+ Create**.



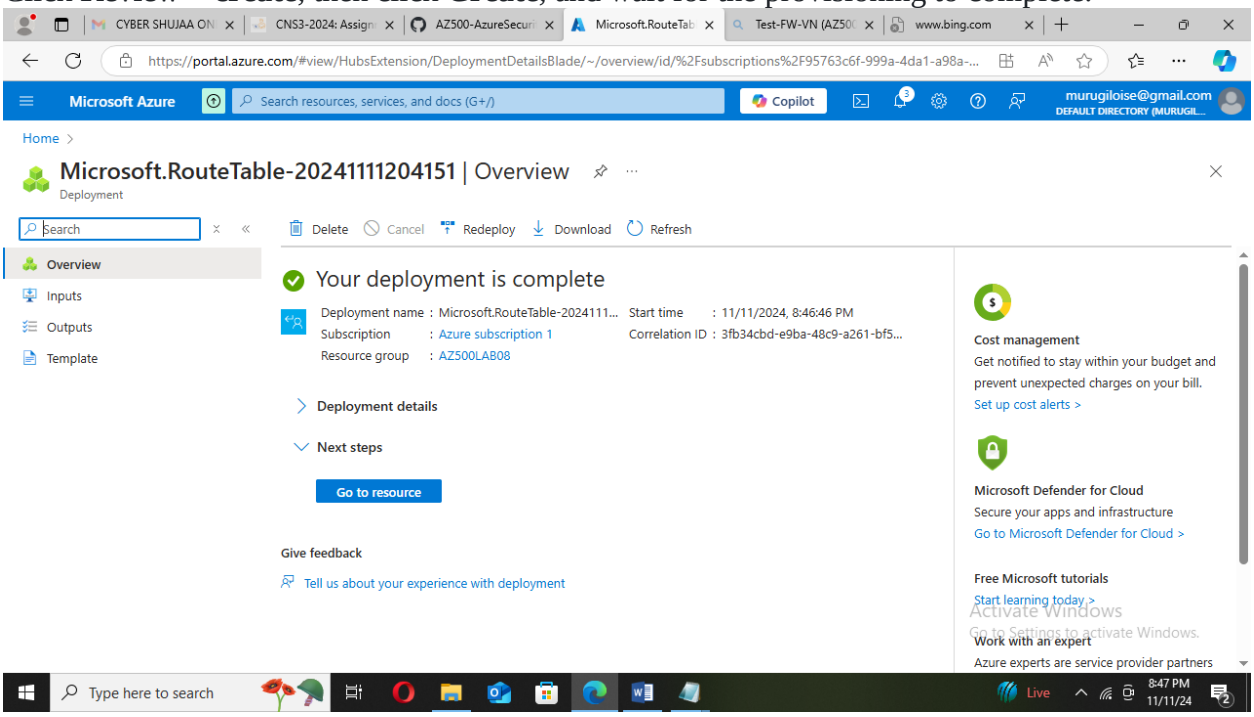
3. On the **Create route table** blade, specify the following settings:

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

Week 8 Assignment 1: Azure Firewall

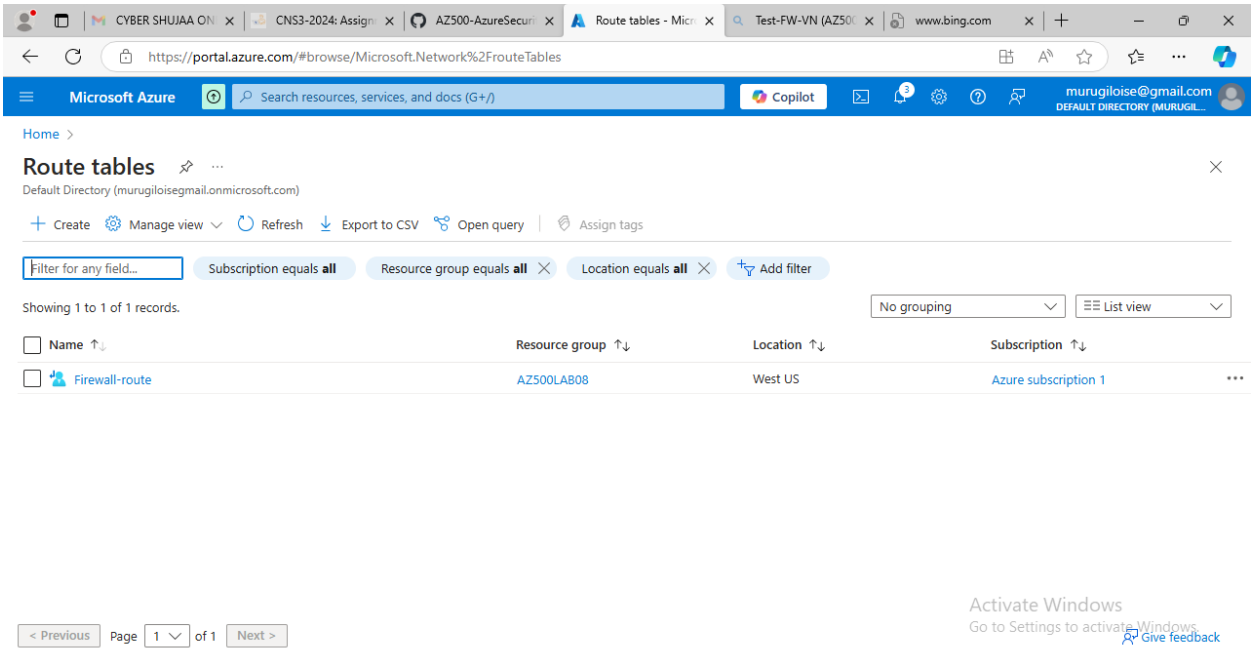


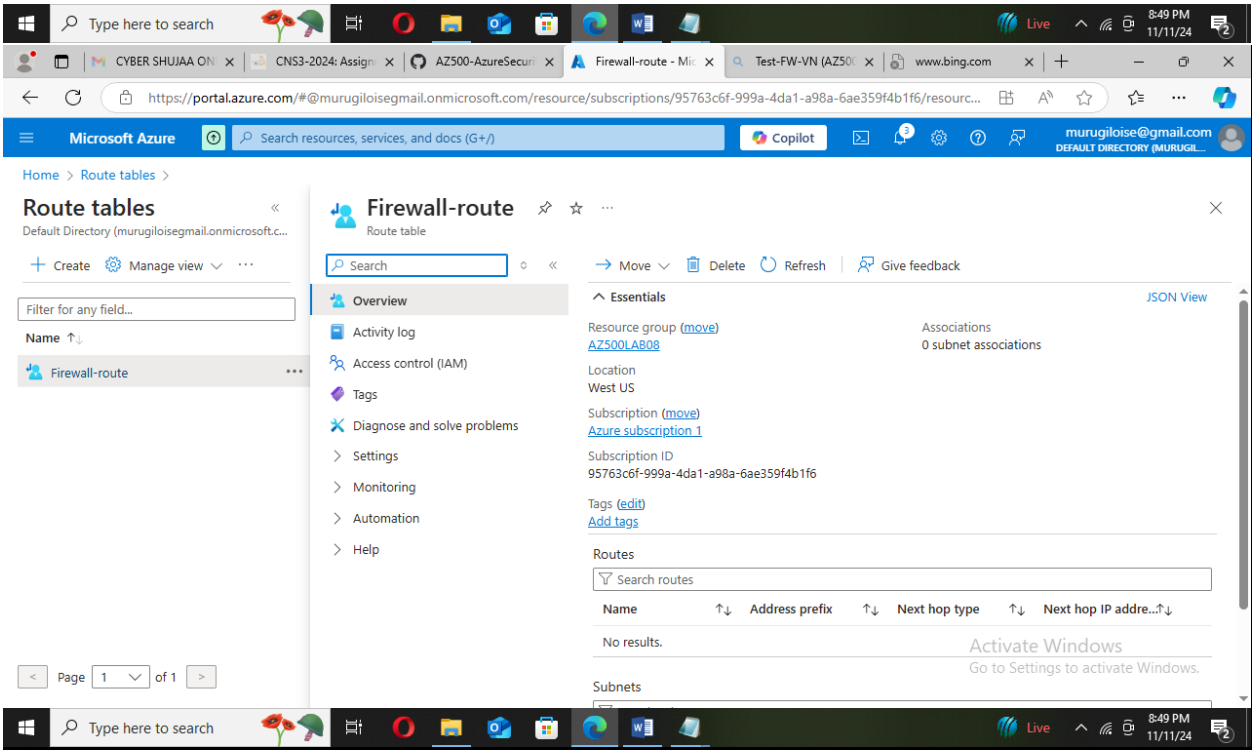
4. Click **Review + create**, then click **Create**, and wait for the provisioning to complete.



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

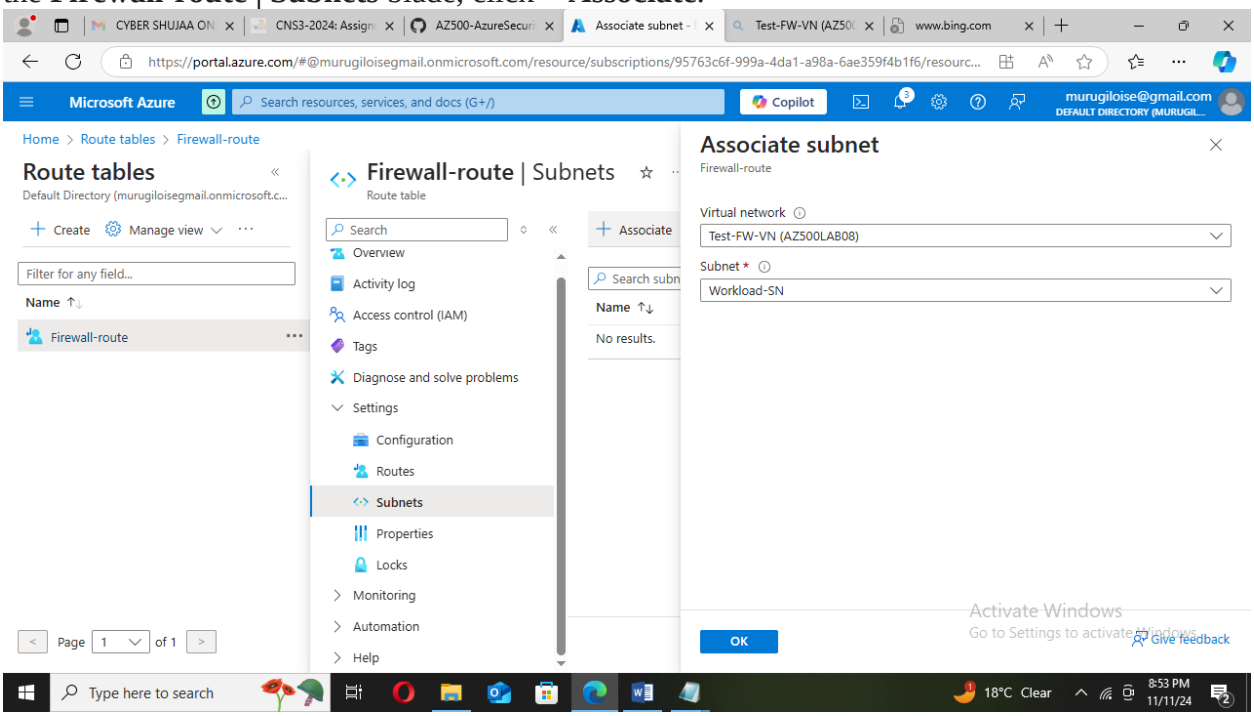
Week 8 Assignment 1: Azure Firewall





Week 8 Assignment 1: Azure Firewall

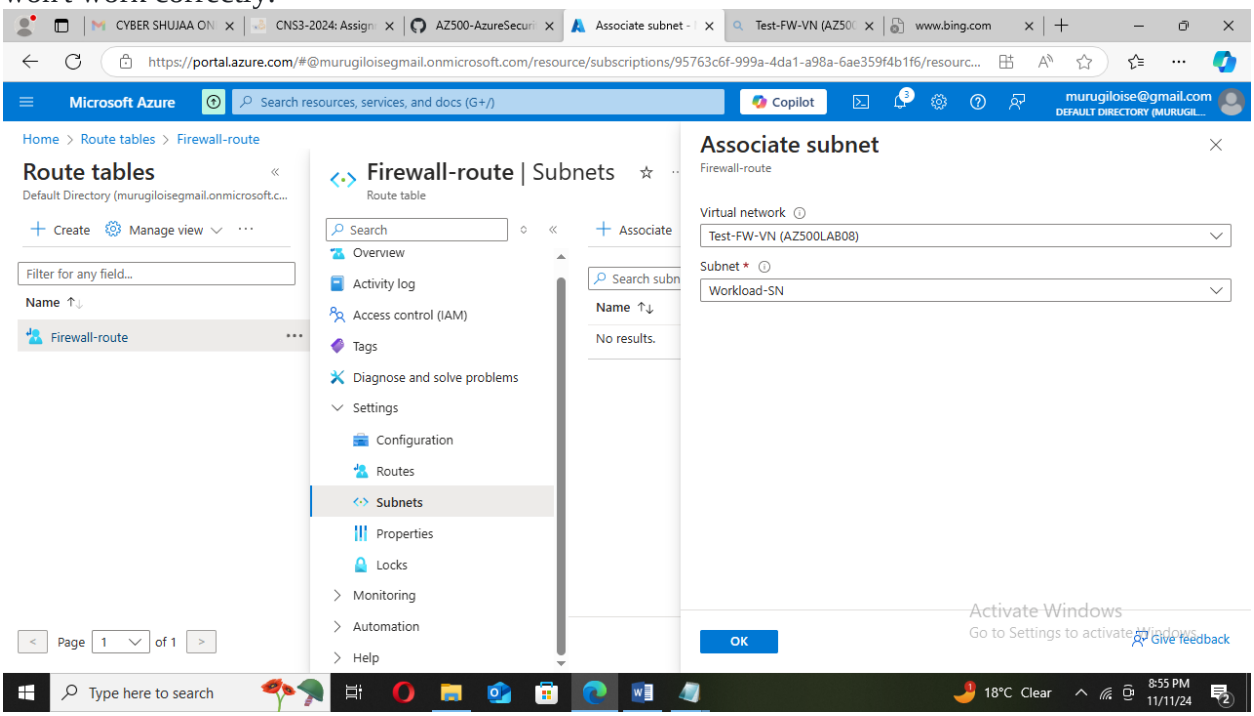
6. On the **Firewall-route** blade, in the **Settings** section, click **Subnets** and then, on the **Firewall-route | Subnets** blade, click **+ Associate**.



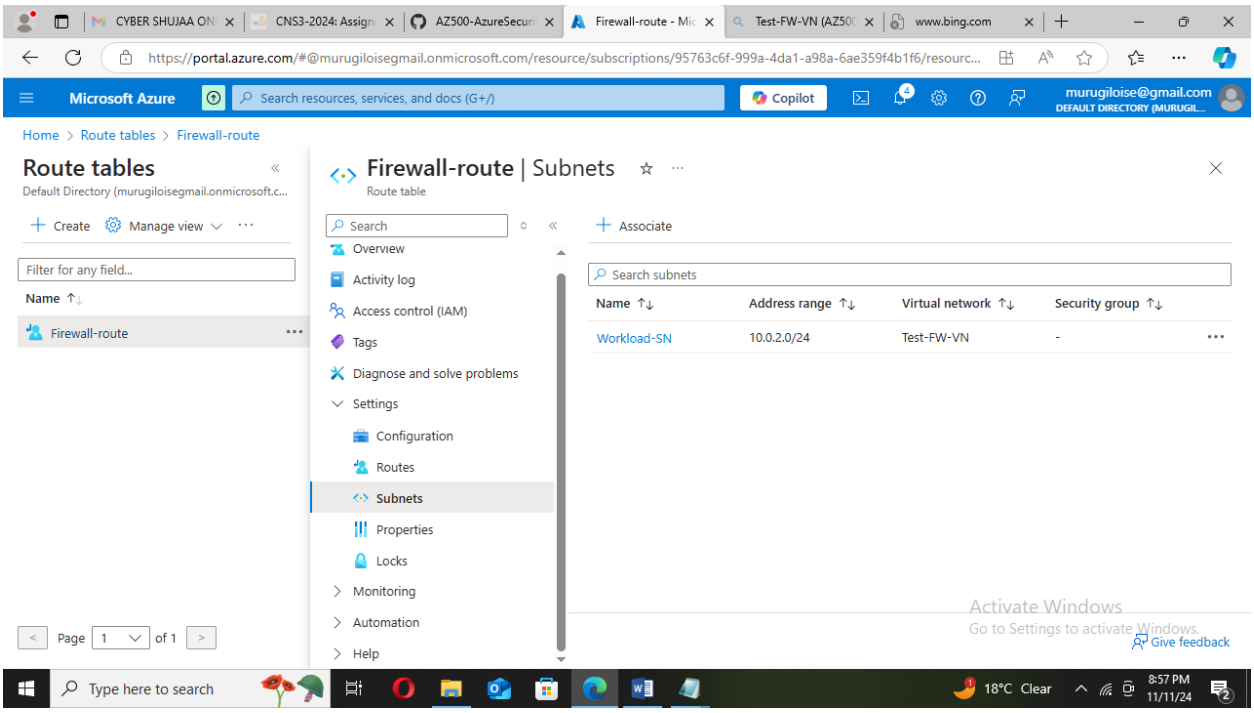
7. On the **Associate subnet** blade, specify the following settings:

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

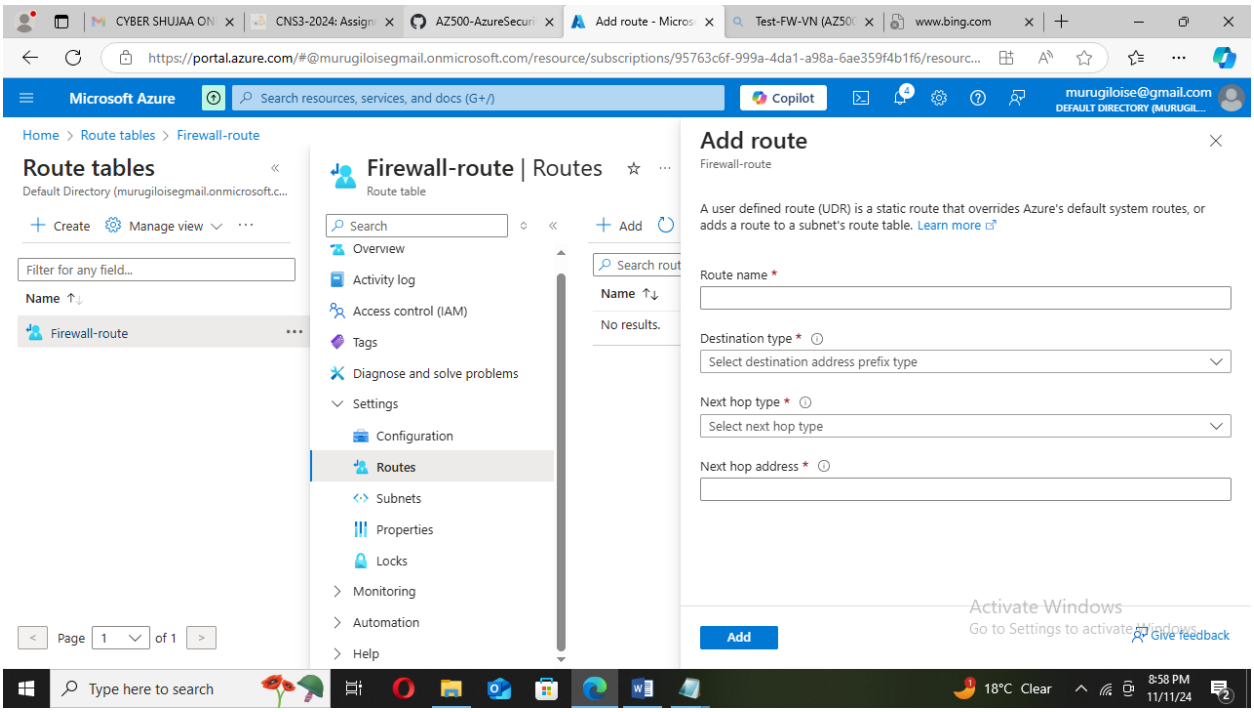
Note: Ensure the **Workload-SN** subnet is selected for this route, otherwise the firewall won't work correctly.



8. Click **OK** to associate the firewall to the virtual network subnet. The subnet has been associated to the virtual network **Test-FW-VN.**



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

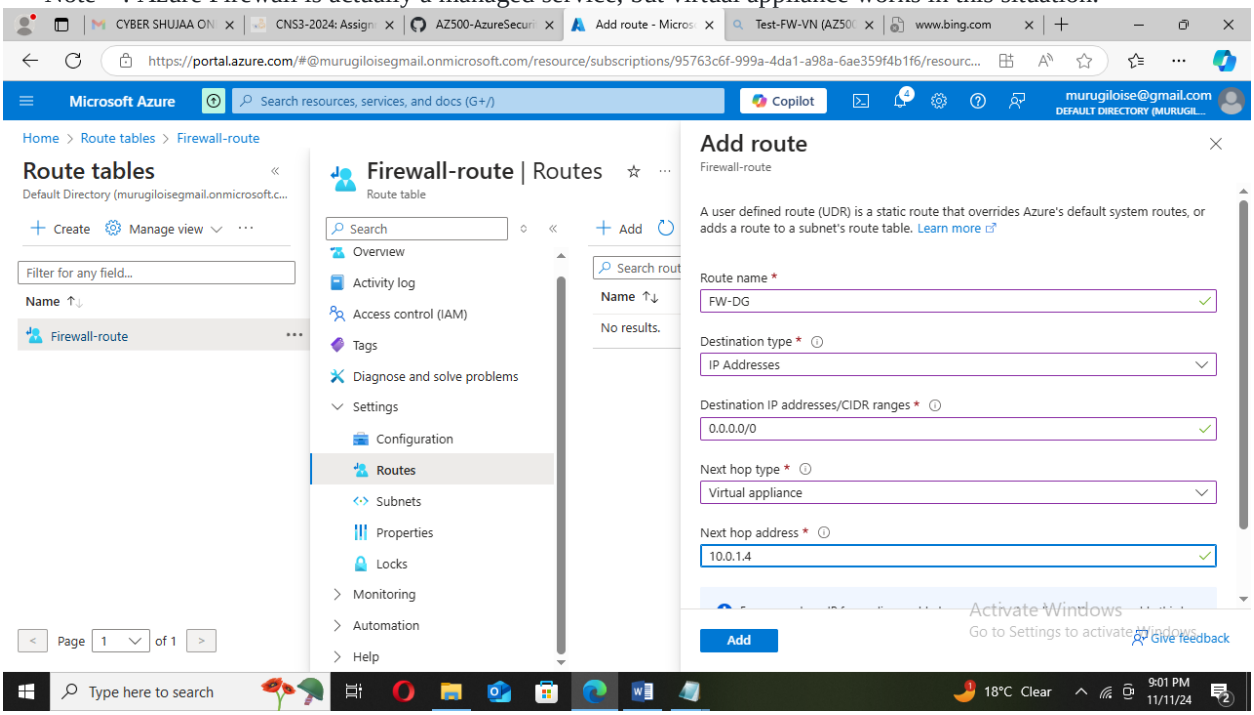


10. On the **Add route** blade, specify the following settings:

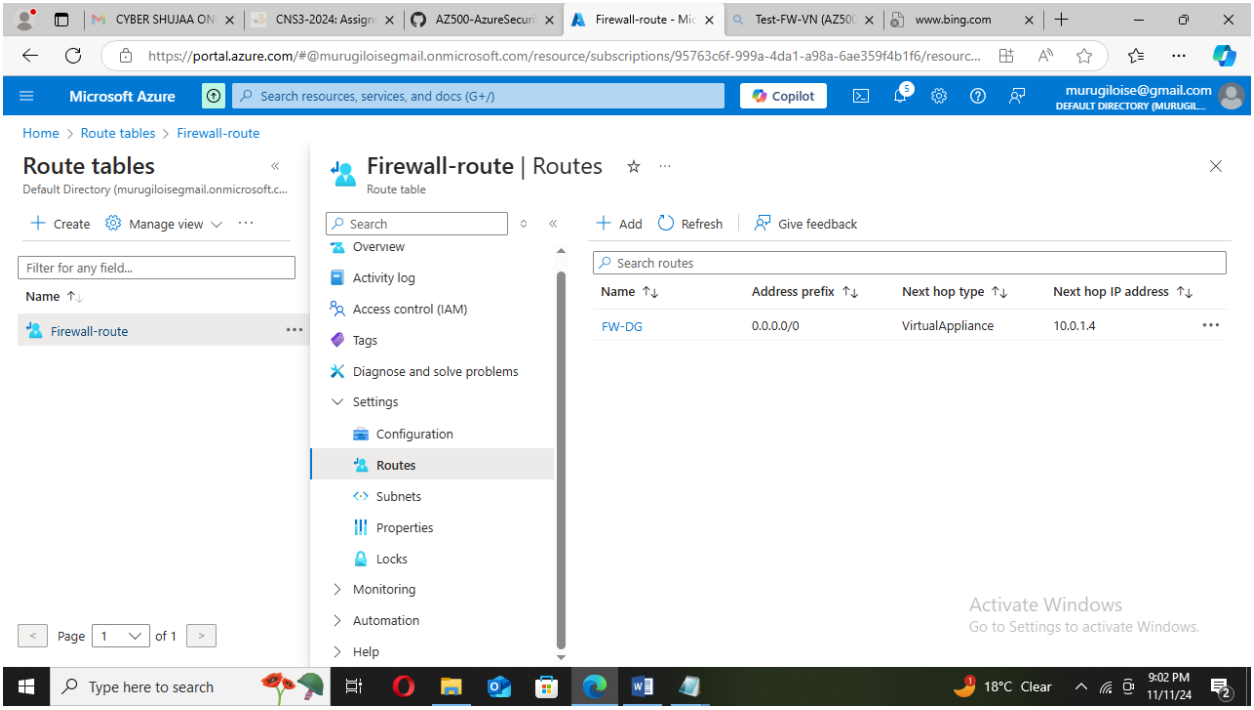
Setting	Value
Route name	**FW-DG**
Address prefix destination	**IP Address**
Destination IP addresses/CIDR ranges	**0.0.0.0/0**
Next hop type	**Virtual appliance**
Next hop address	the private IP address of the firewall that you identified in the previous task

Week 8 Assignment 1: Azure Firewall

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



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

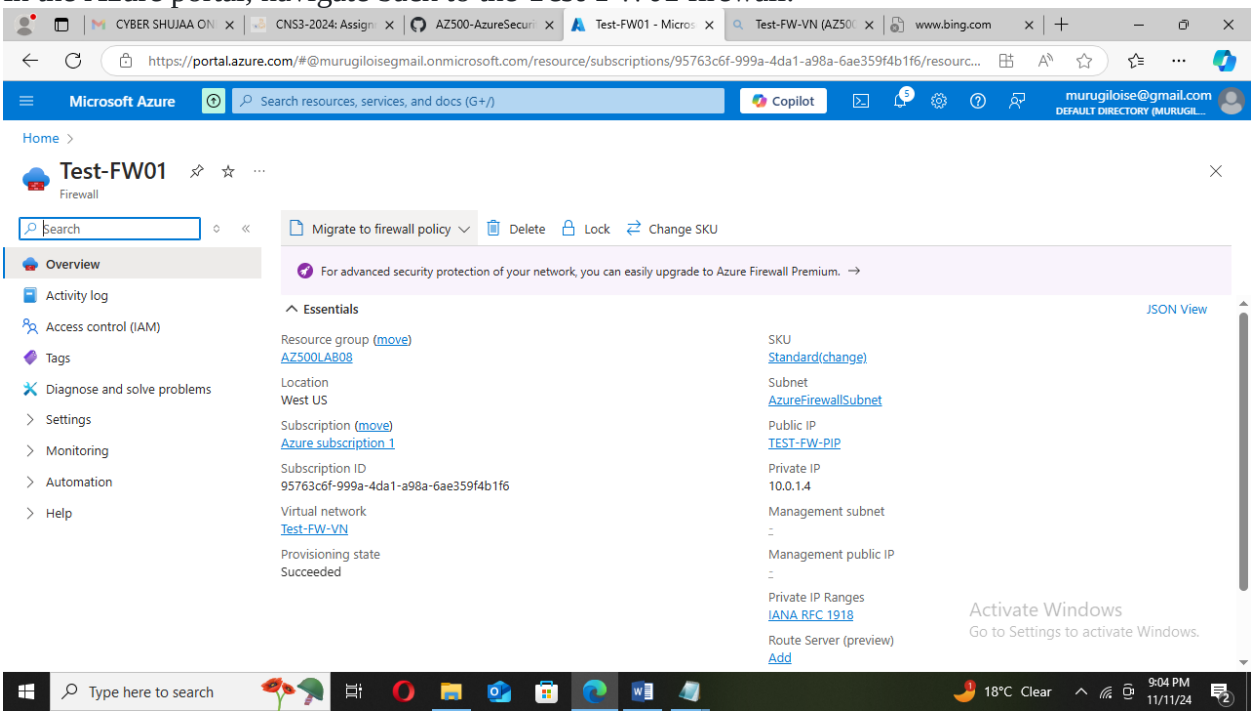


Task 4: Configure an application rule

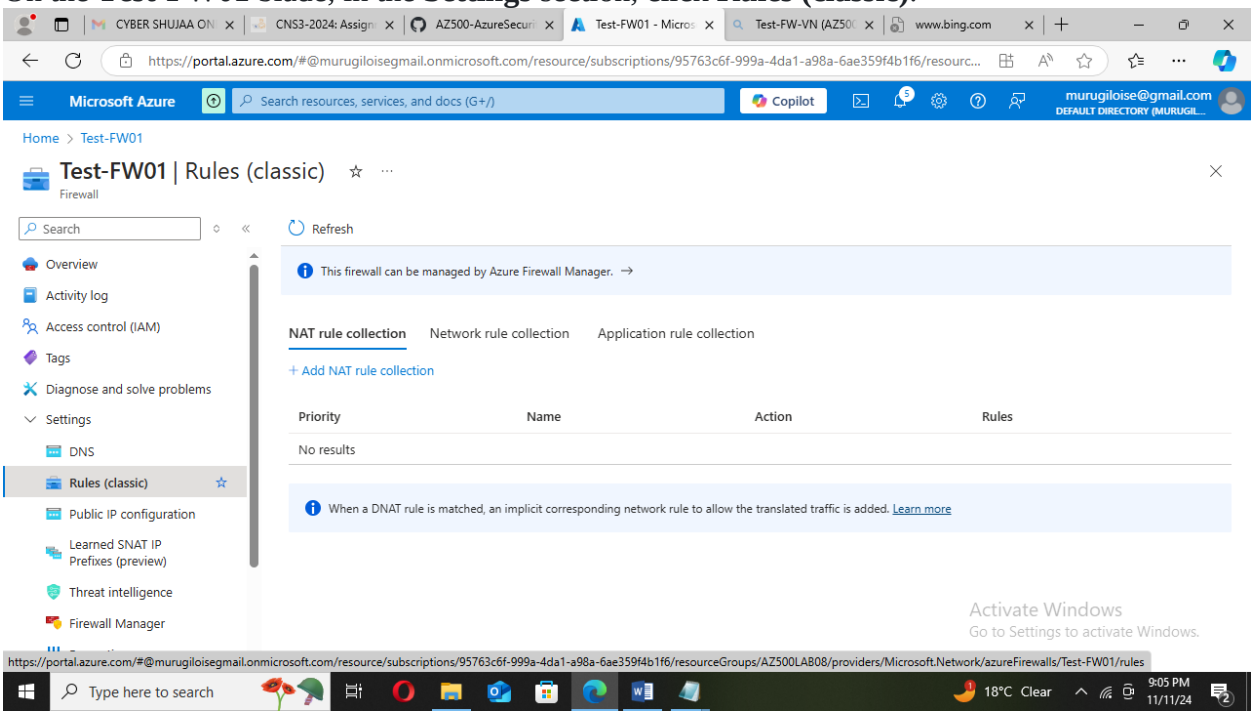
In this task you will create an application rule that allows outbound access to www.bing.com.

Week 8 Assignment 1: Azure Firewall

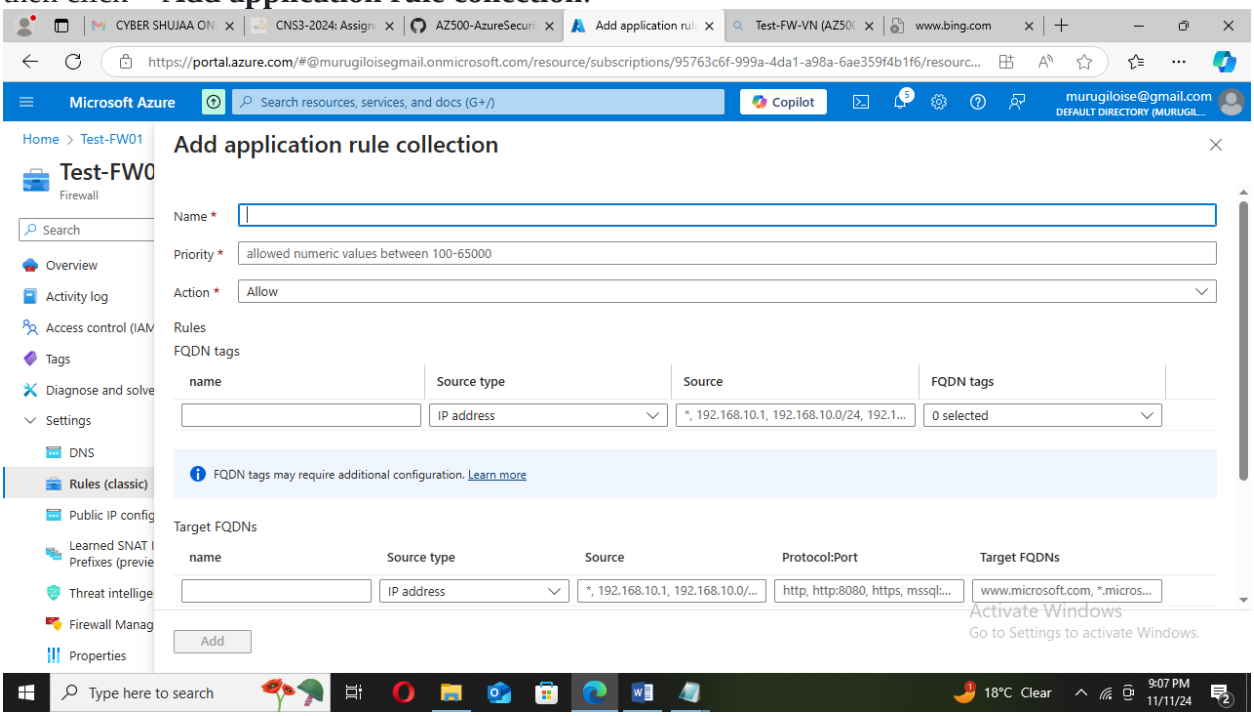
1. In the Azure portal, navigate back to the **Test-FW01** firewall.



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



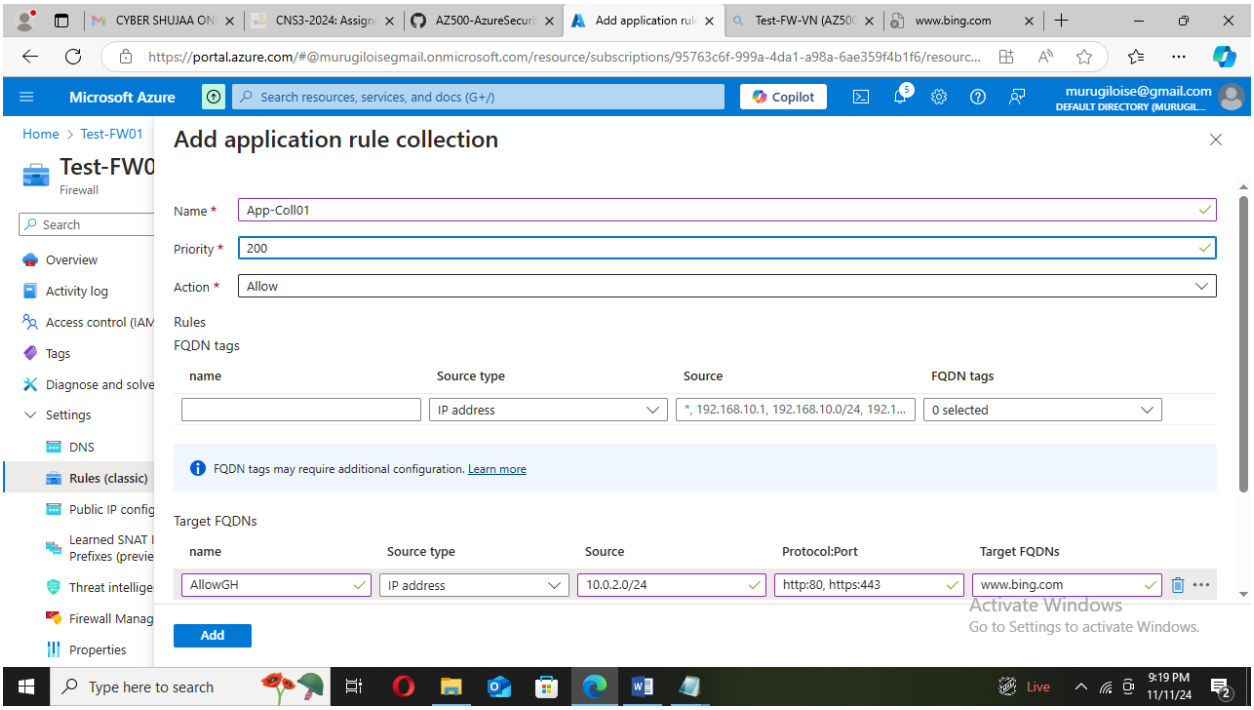
3. On the **Test-FW01 | Rules (classic)** blade, click the **Application rule collection** tab, and then click **+ Add application rule collection**.



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**

Week 8 Assignment 1: Azure Firewall

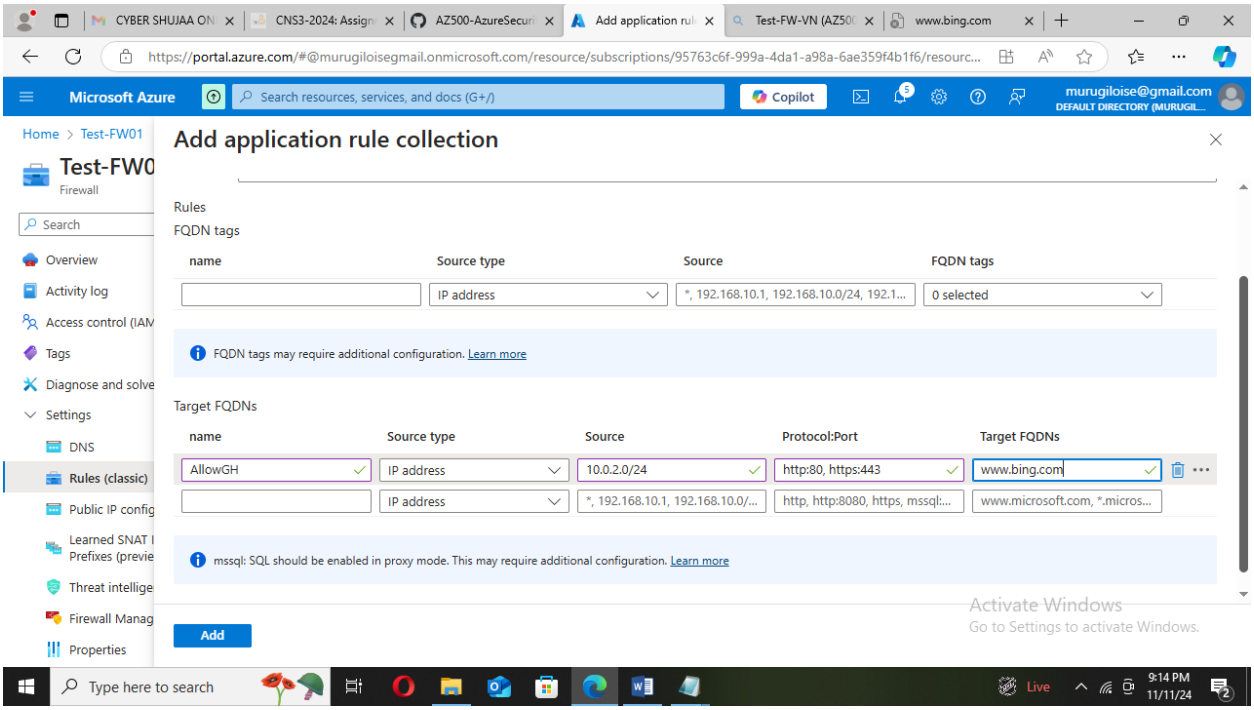


5. On the **Add application rule collection** blade, create a new entry in the **Target FQDNs** section with the following settings (leave others with their default values):

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**

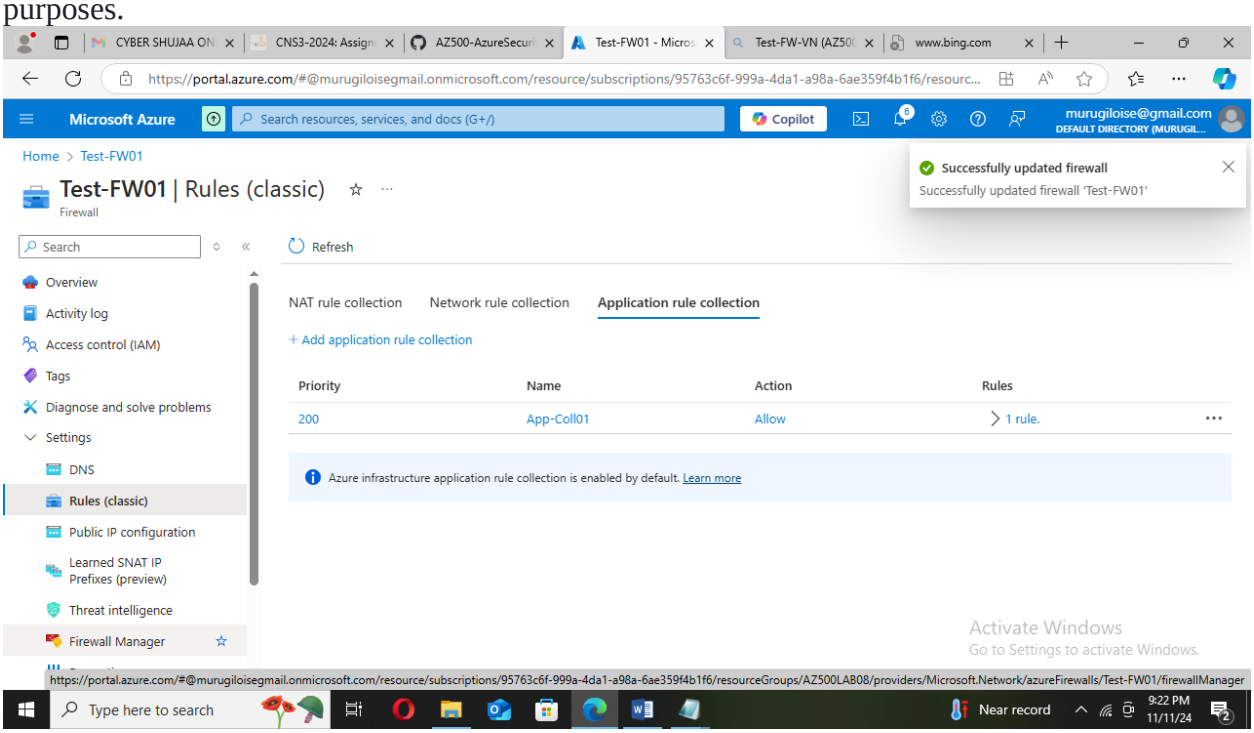
We have created a new entry in the **Target FQDNs** as seen below.

Week 8 Assignment 1: Azure Firewall



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

Note: 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.

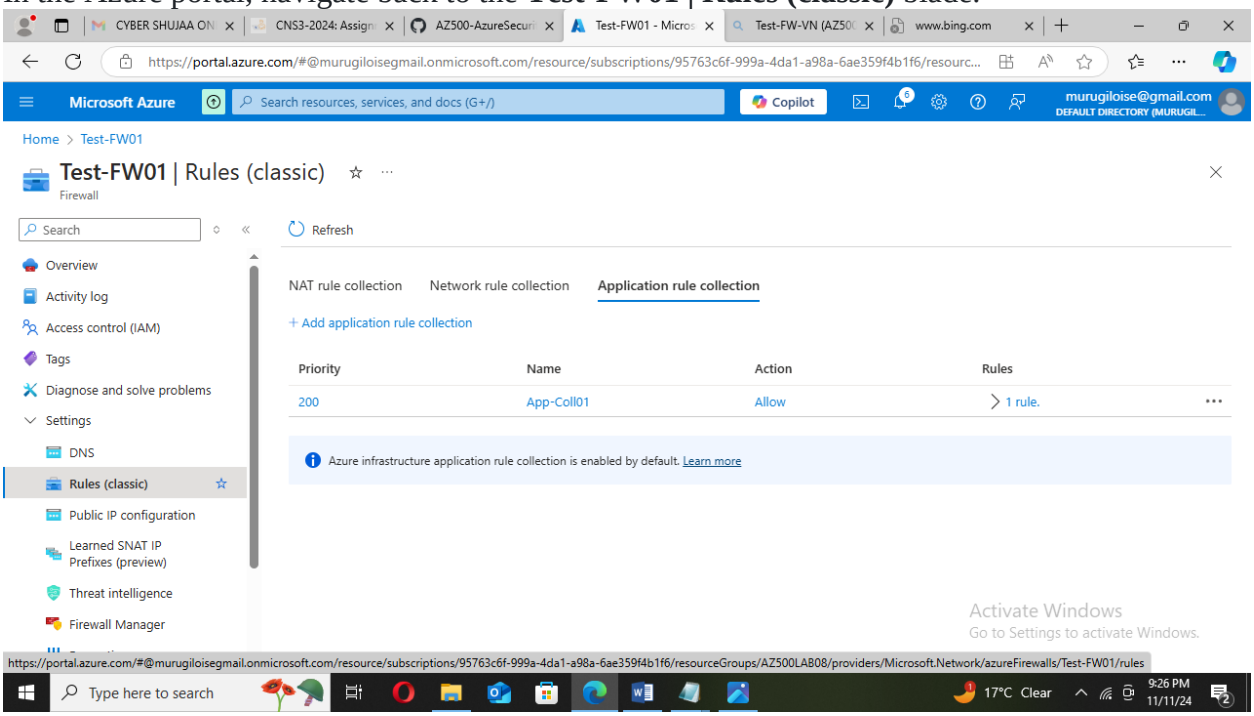


Week 8 Assignment 1: Azure Firewall

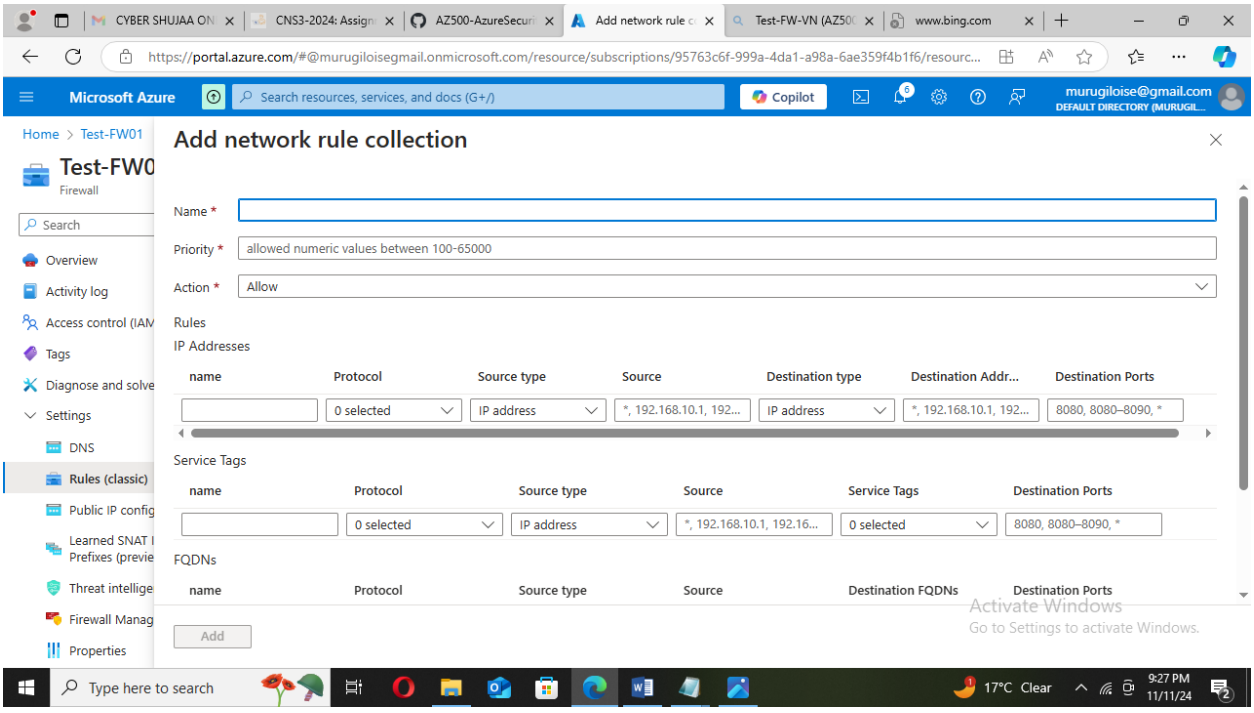
Task 5: Configure a network rule

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.

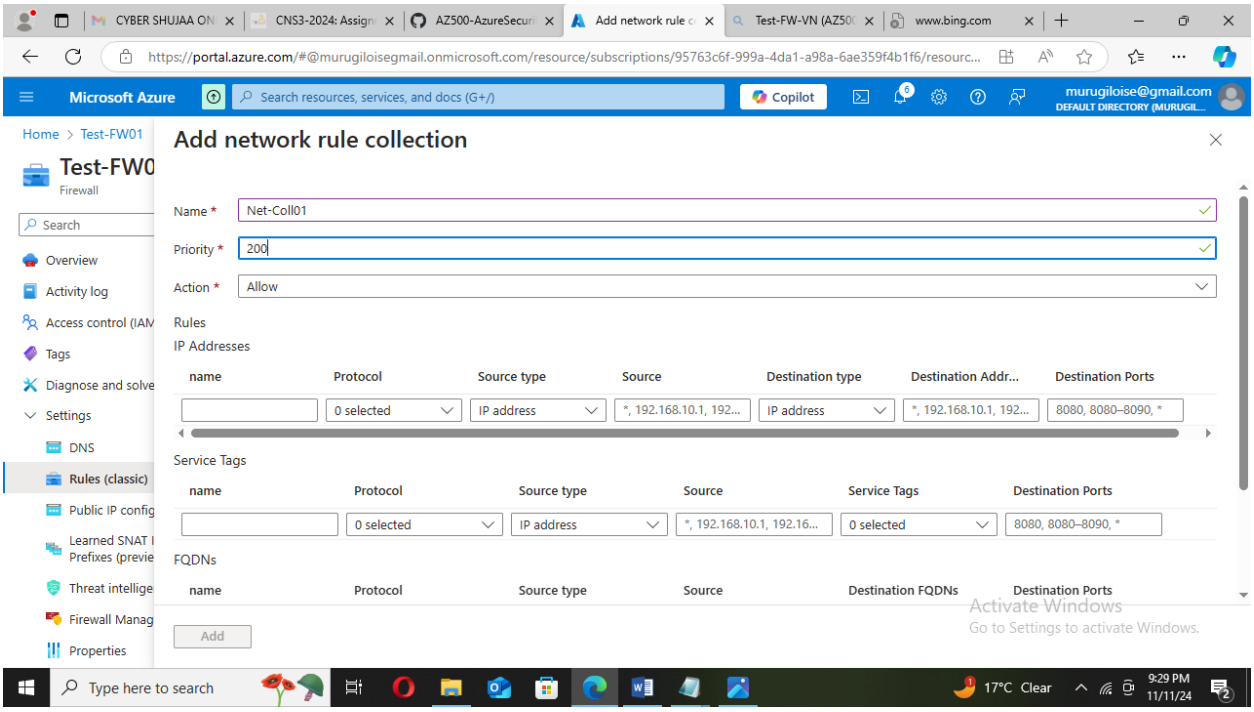


2. On the **Test-FW01 | Rules (classic)** blade, click the **Network rule collection** tab and then click **+ Add network rule collection**.



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

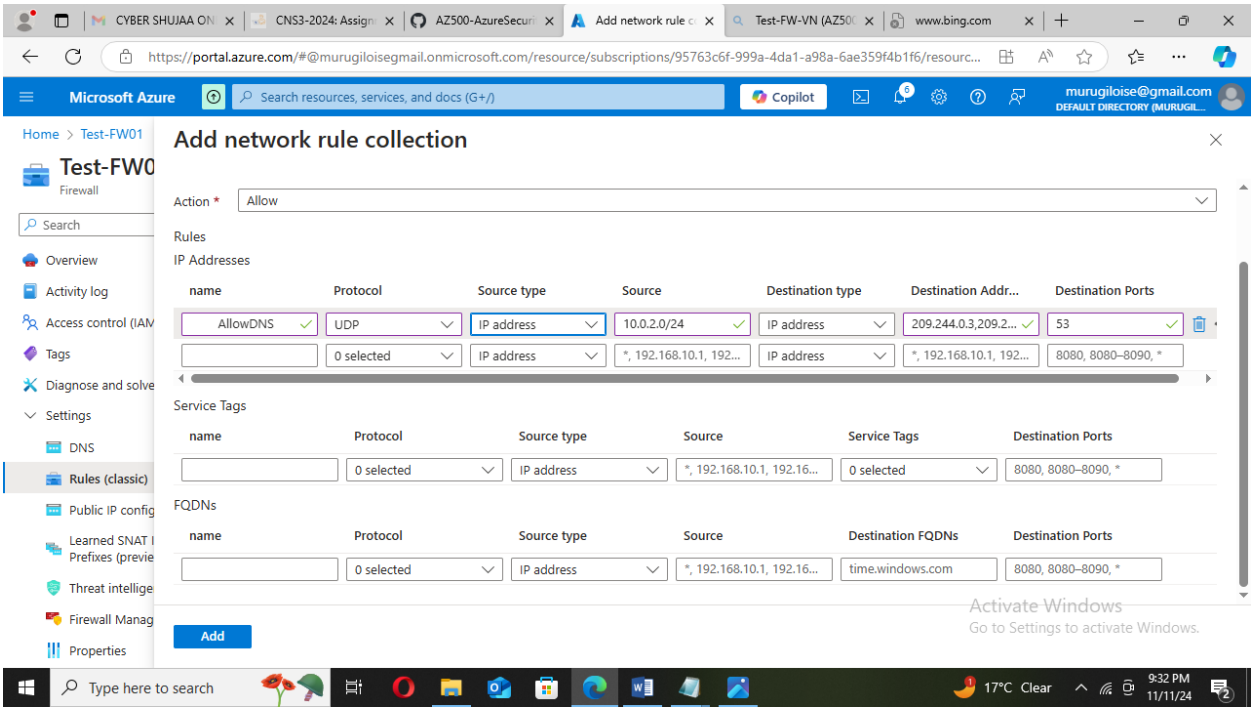
Setting	Value
Name	**Net-Coll01**
Priority	**200**
Action	**Allow**



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):

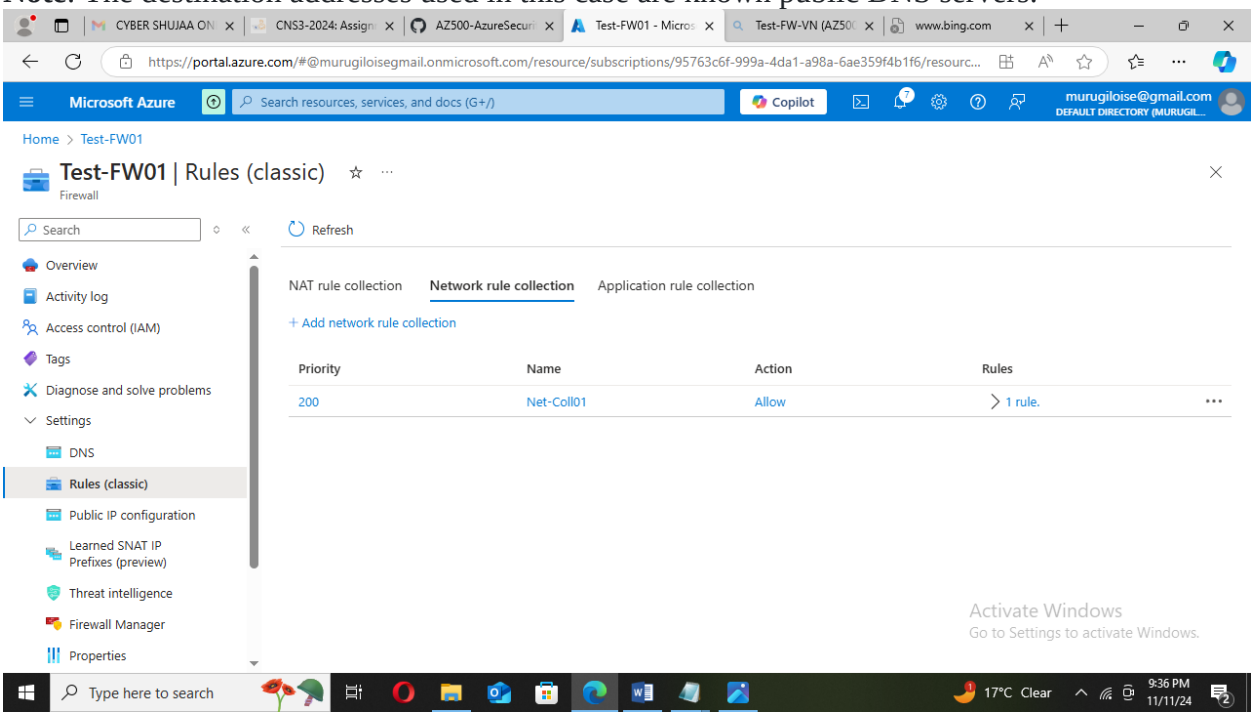
Setting	Value
Name	**AllowDNS**
Protocol	**UDP**
Source type	**IP address**
Source Addresses	**10.0.2.0/24**
Destination type	**IP address**
Destination Address	**209.244.0.3,209.244.0.4**

Setting	Value
Destination Ports	**53**



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

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

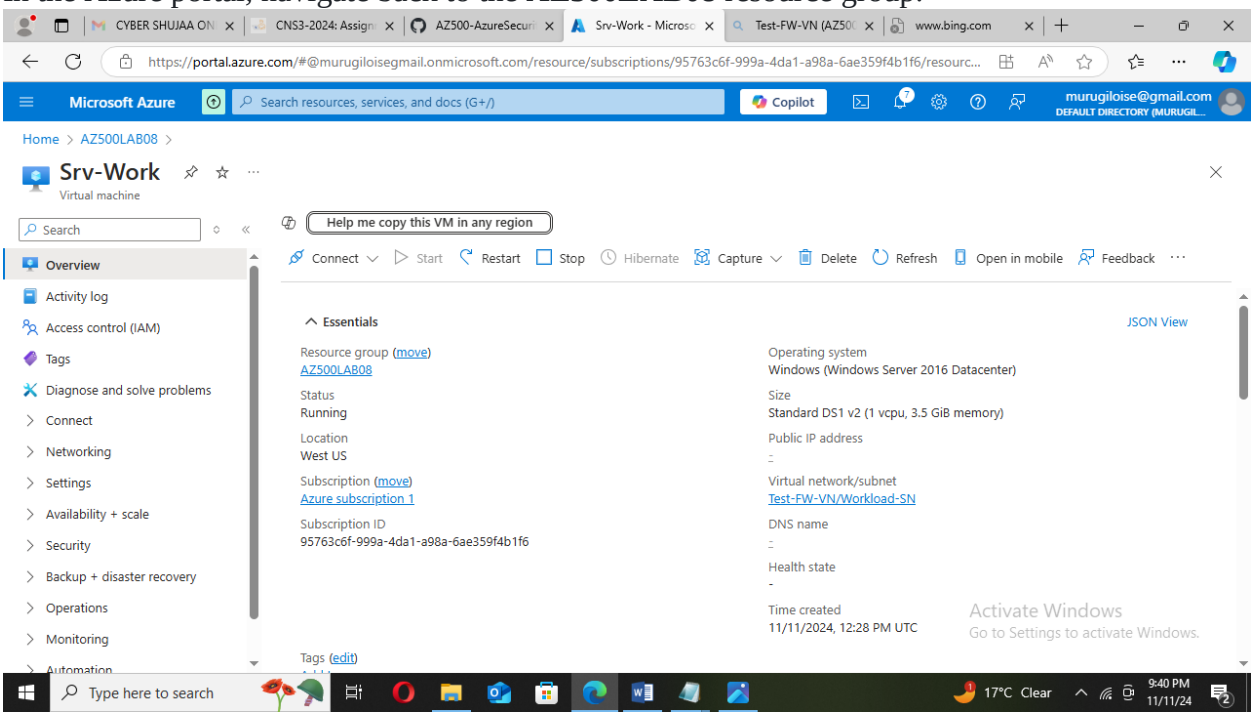


Week 8 Assignment 1: Azure Firewall

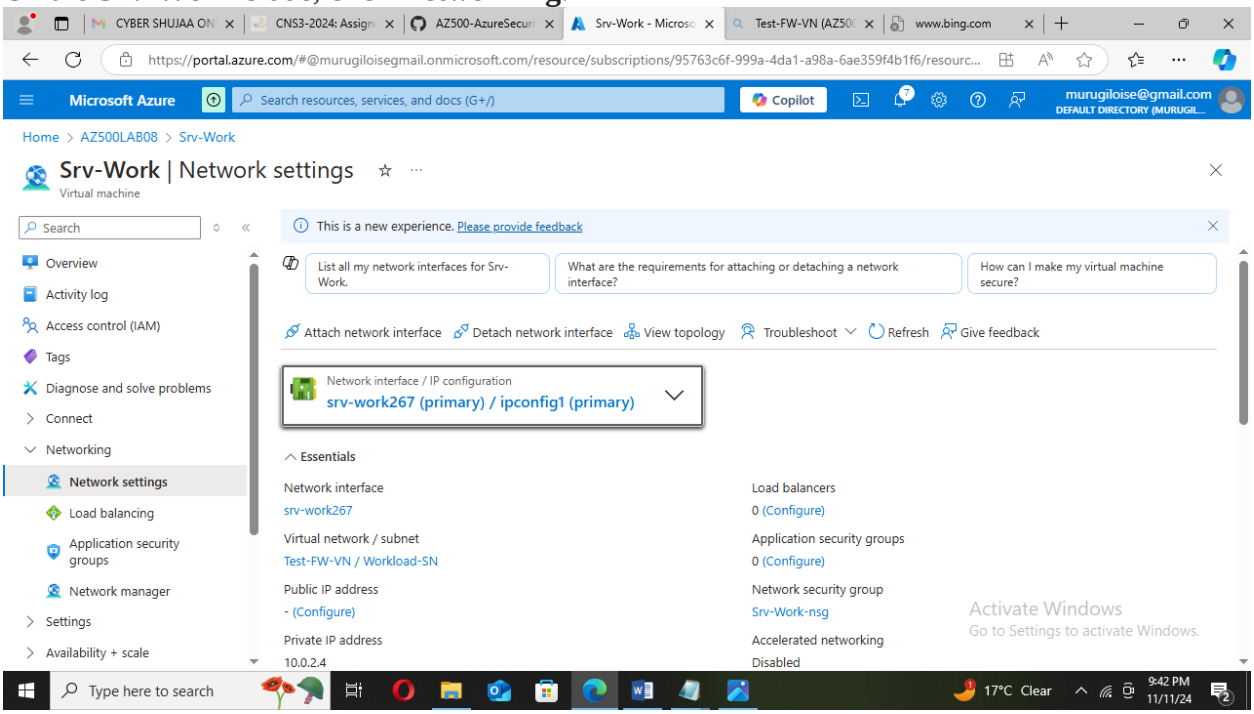
Task 6: Configure the virtual machine DNS servers

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

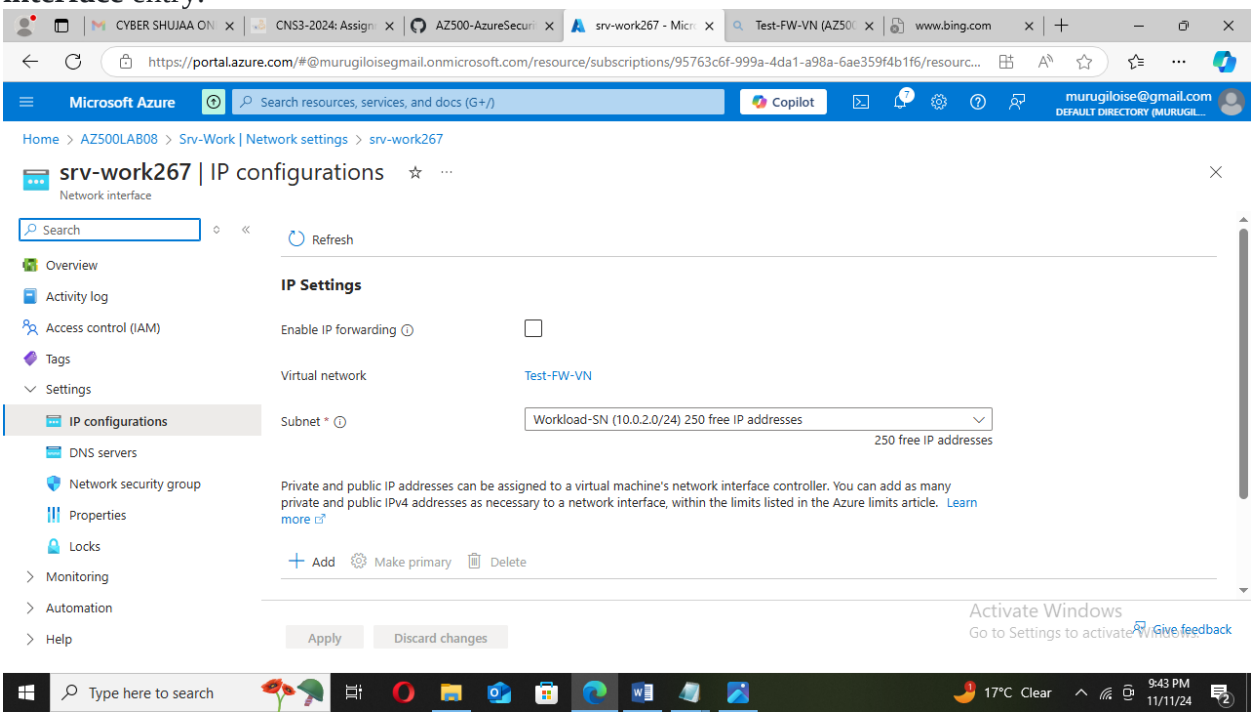


3. On the **Srv-Work** blade, click **Networking**.

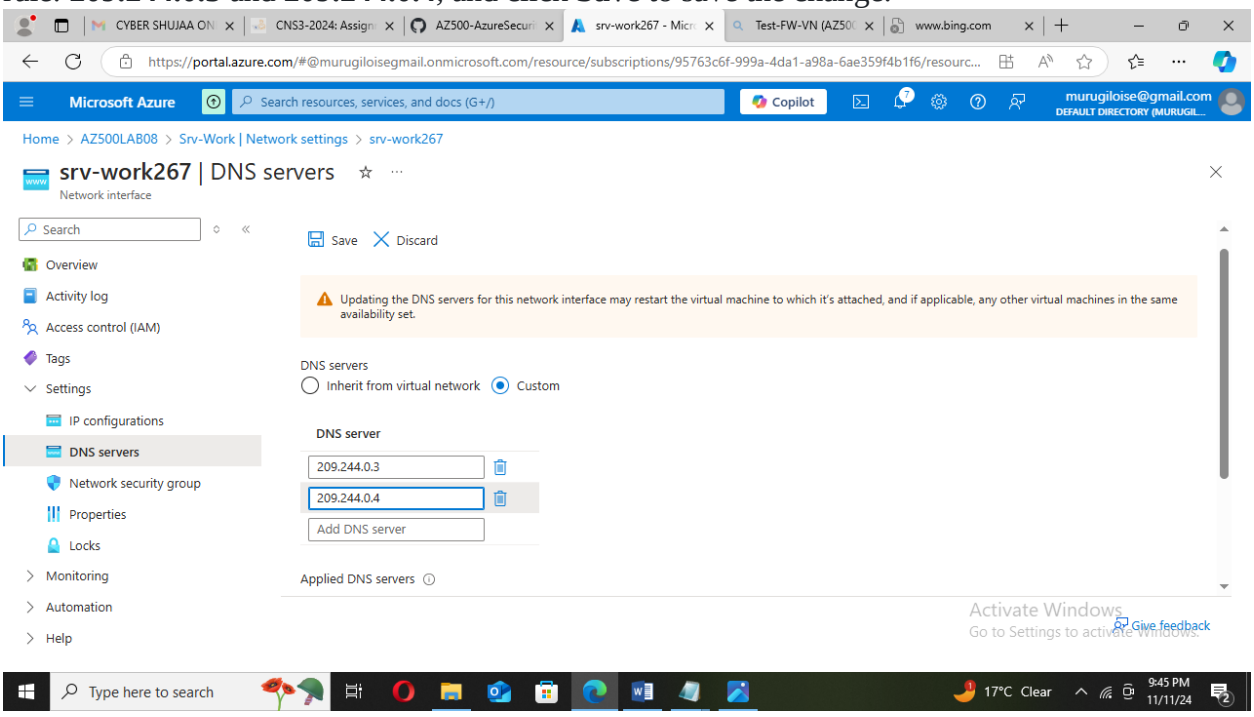


Week 8 Assignment 1: Azure Firewall

4. On the **Srv-Work | Networking** 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.

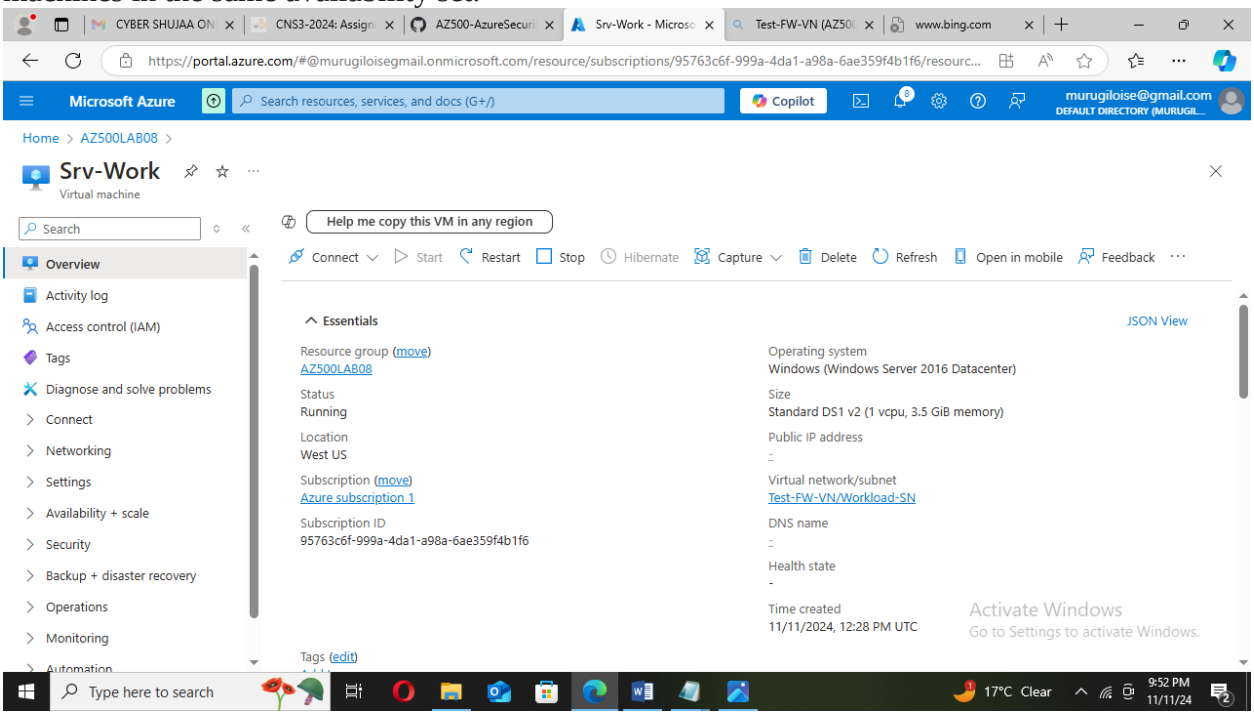


6. Return to the **Srv-Work** virtual machine page.

Note: Wait for the update to complete.

Week 8 Assignment 1: Azure Firewall

Note: 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.

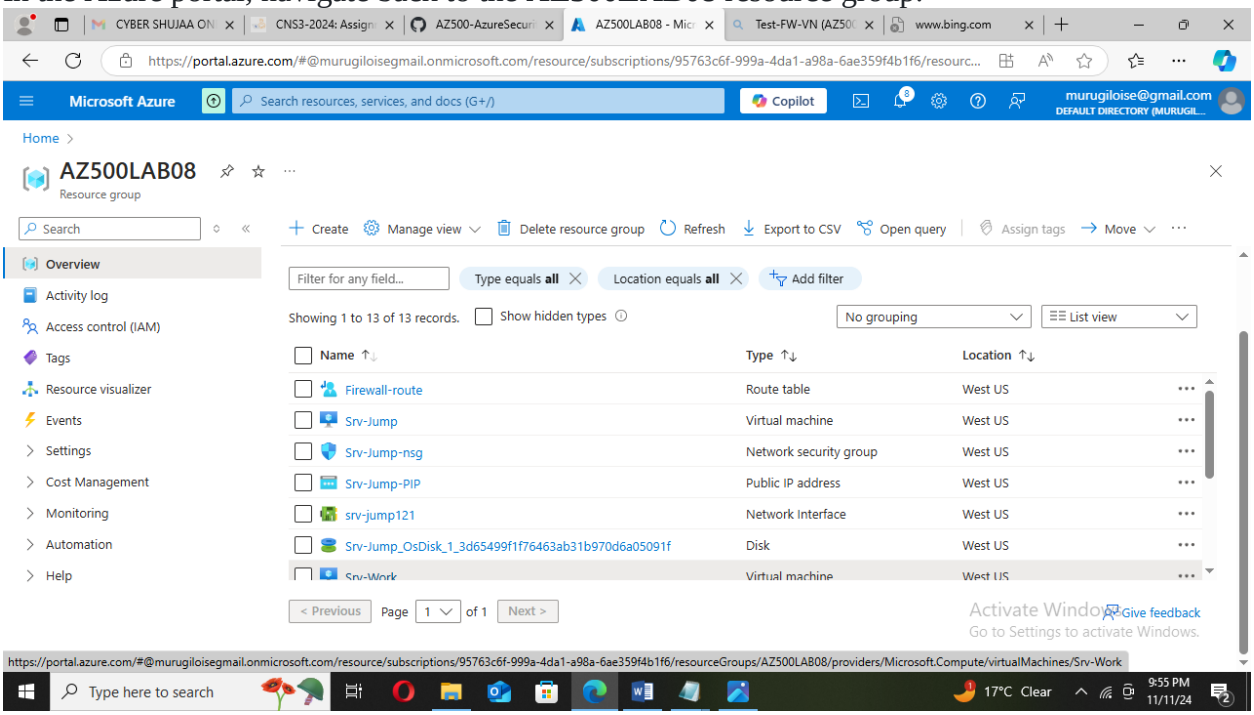


Task 7: Test the firewall

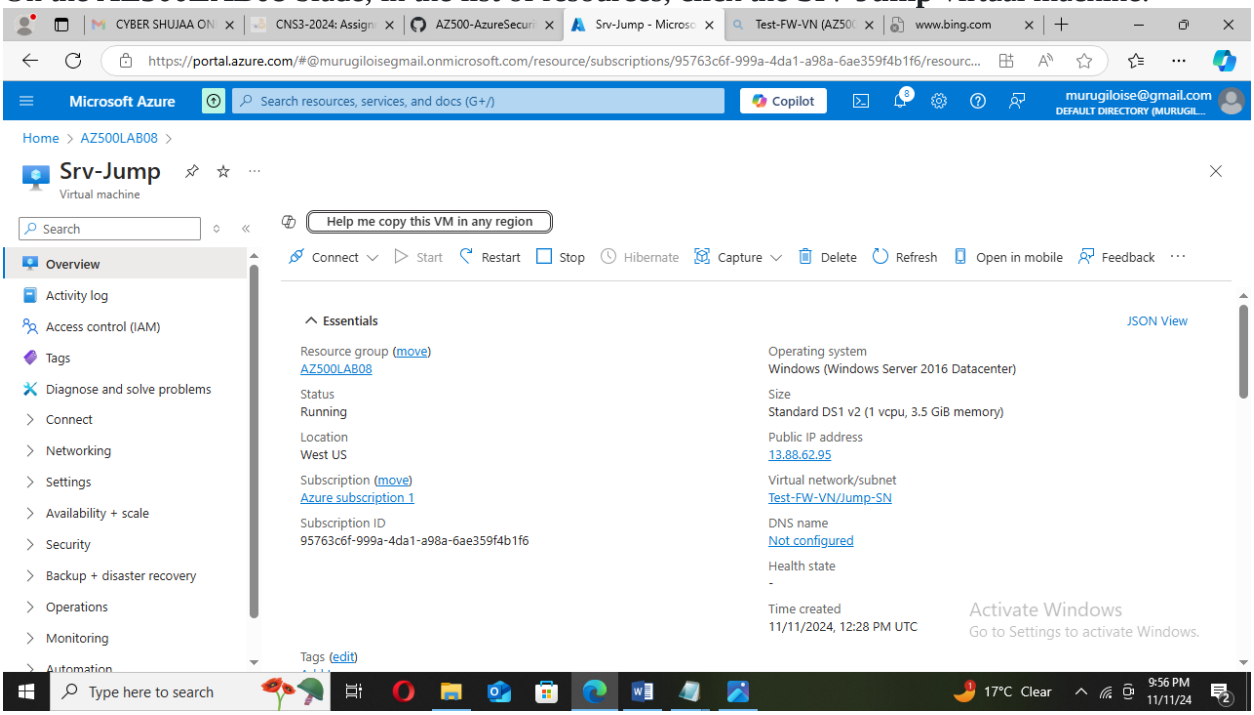
In this task, you will test the firewall to confirm that it works as expected.

Week 8 Assignment 1: Azure Firewall

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

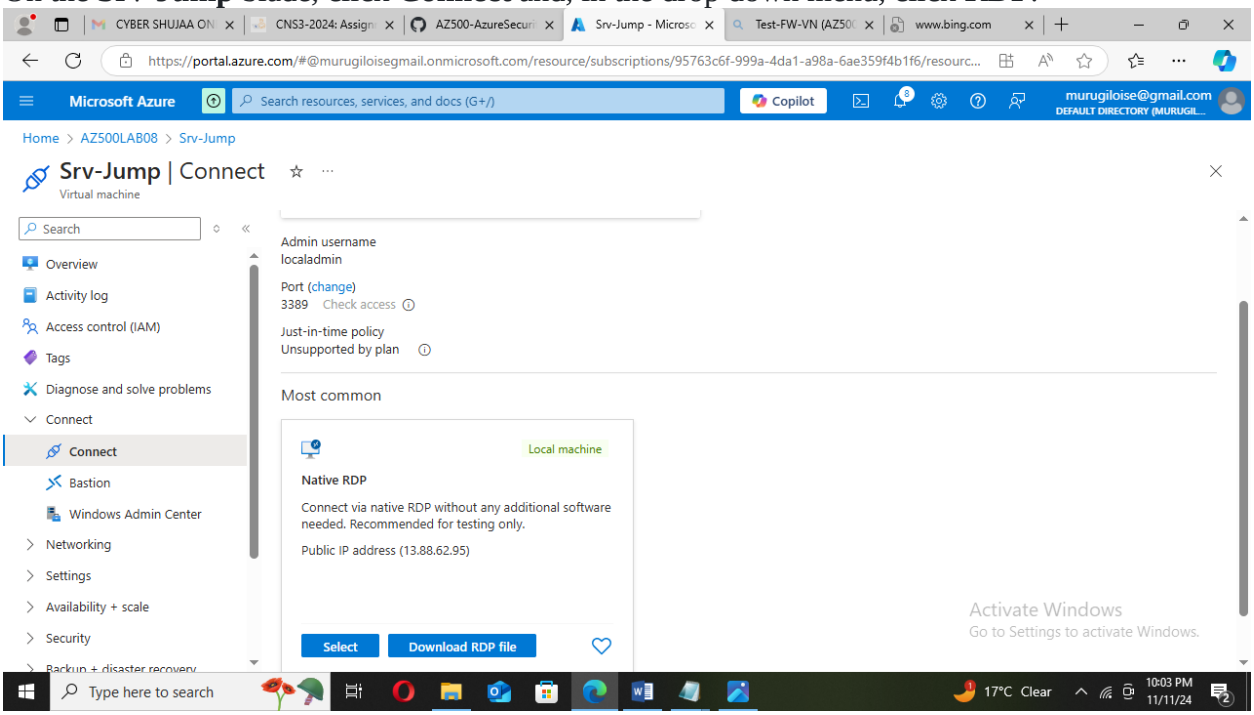


2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.



Week 8 Assignment 1: Azure Firewall

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

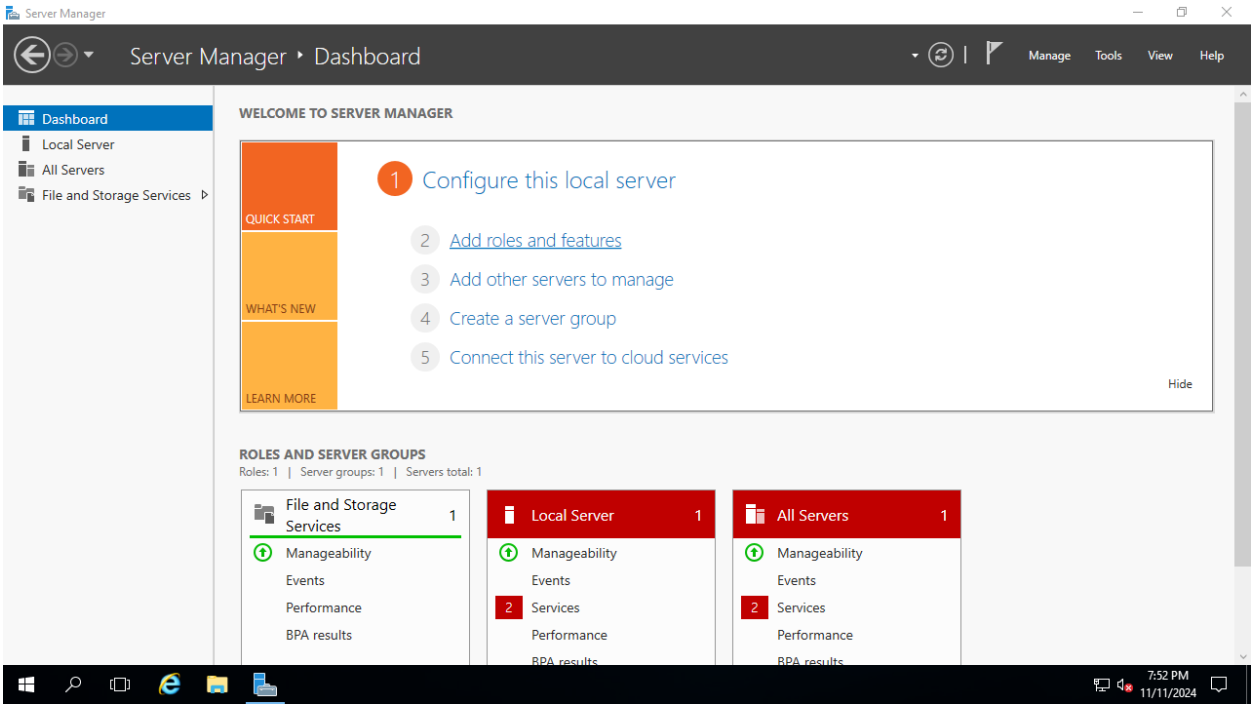


4. Click **Download RDP File** and use it to connect to the **Srv-Jump** Azure VM via Remote Desktop. When prompted to authenticate, provide the following credntials:

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

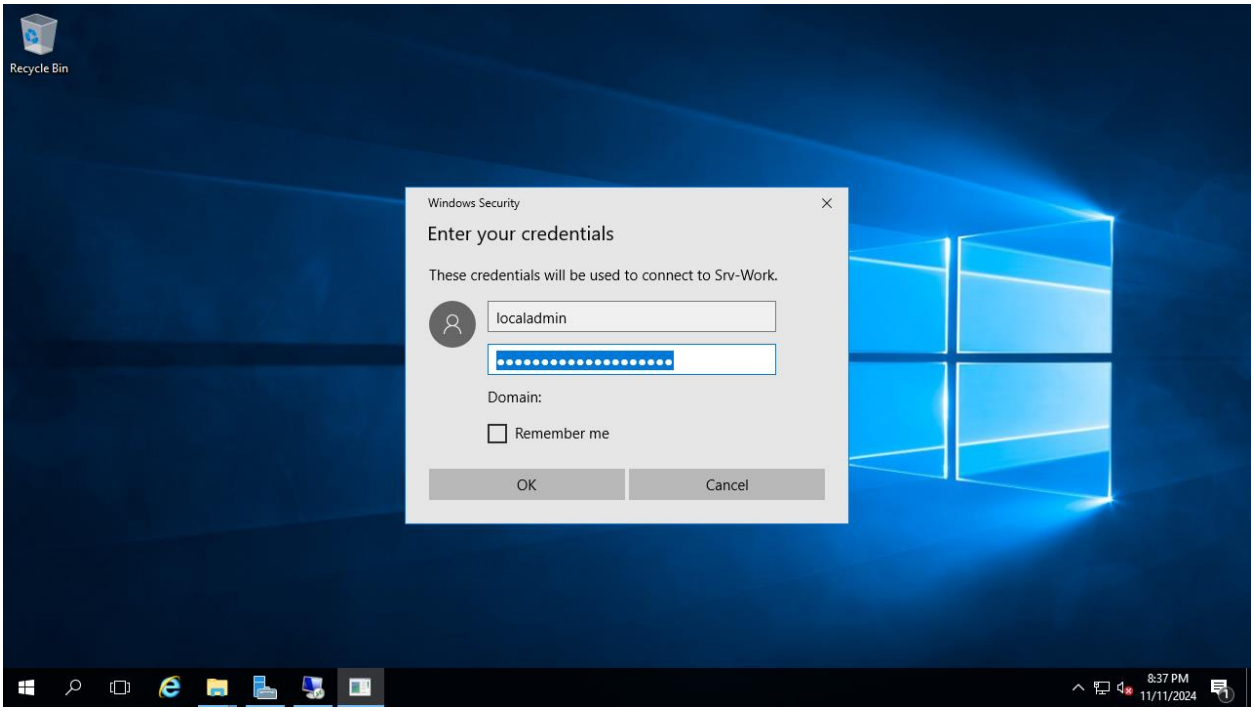
Note: The following steps are performed in the Remote Desktop session to the **Srv-Jump** Azure VM.

Note: 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. We were able to successfully connect to the Srv-Work virtual machine as seen below.



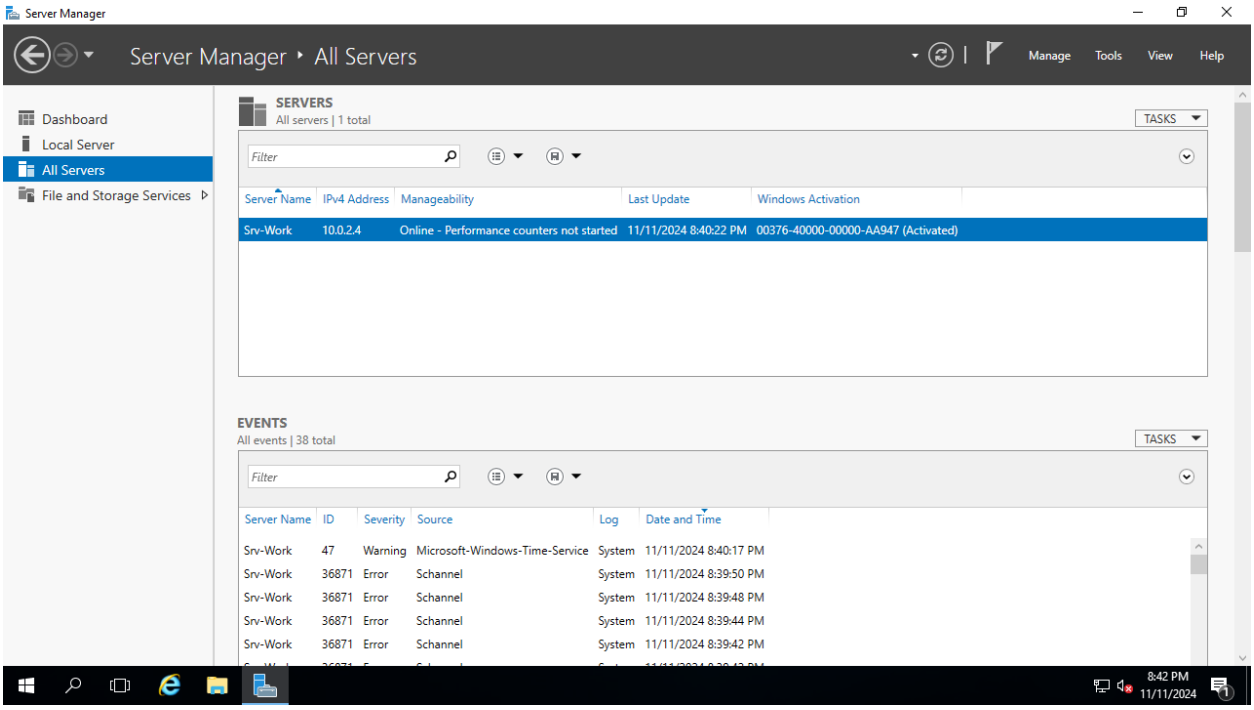
5. Within the Remote Desktop session to **Srv-Jump**, right-click **Start**, in the right-click menu, click **Run**, and, from the **Run** dialog box, run the following to connect to **Srv-Work**.

mstsc /v:Srv-Work



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

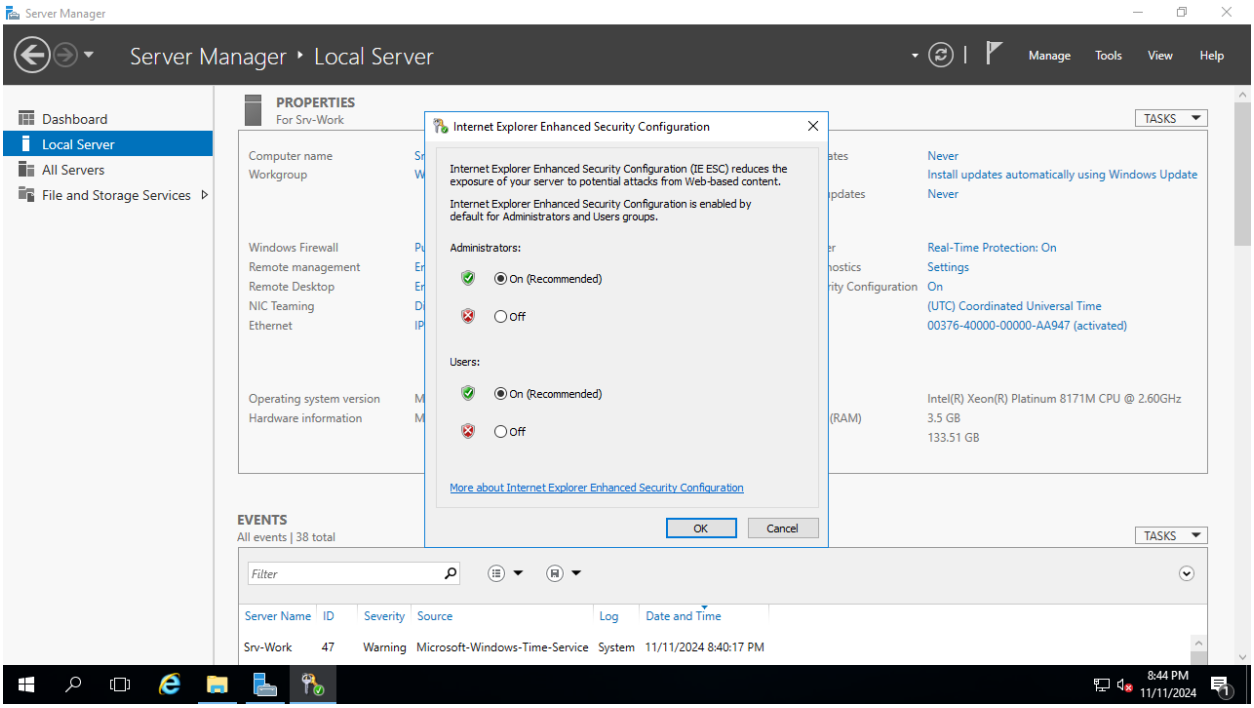
Setting	Value
User name	**localadmin**
Password	The secure password you chose during deployment of the custom template in task 1 step 6. We were able to connect to Srv-W



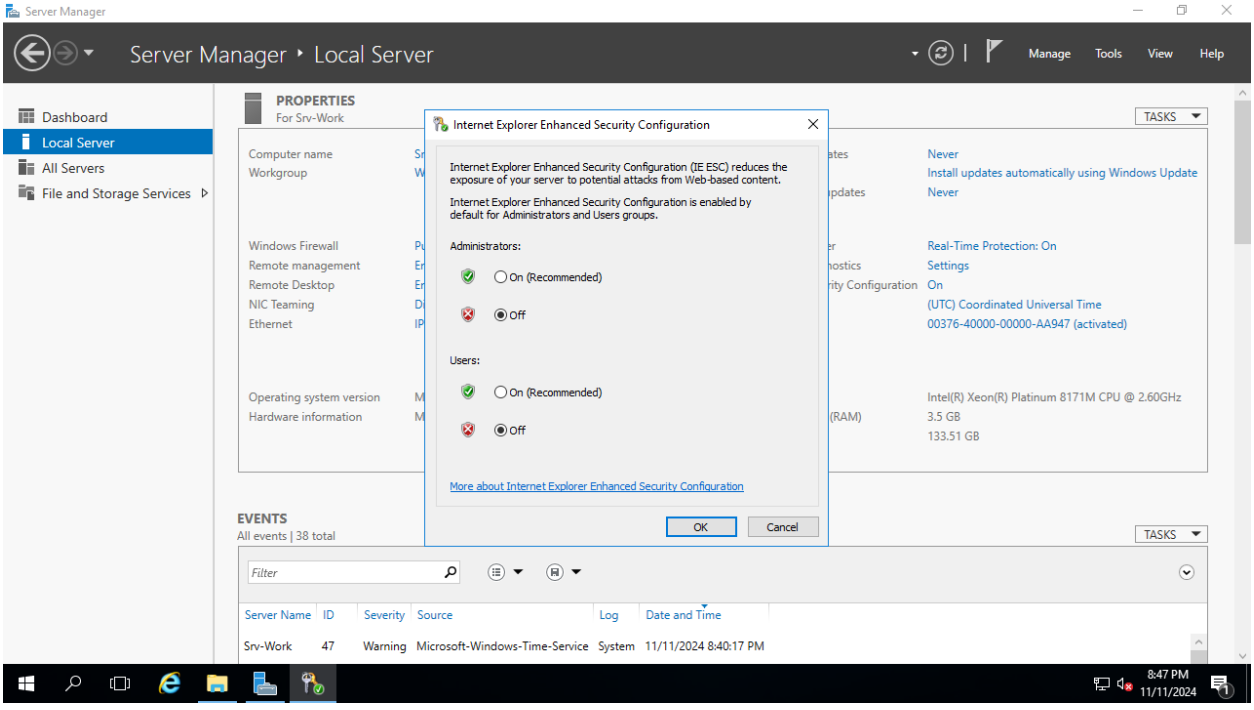
Note: Wait for the Remote Desktop session to be established and the Server Manager interface to load.

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

Week 8 Assignment 1: Azure Firewall

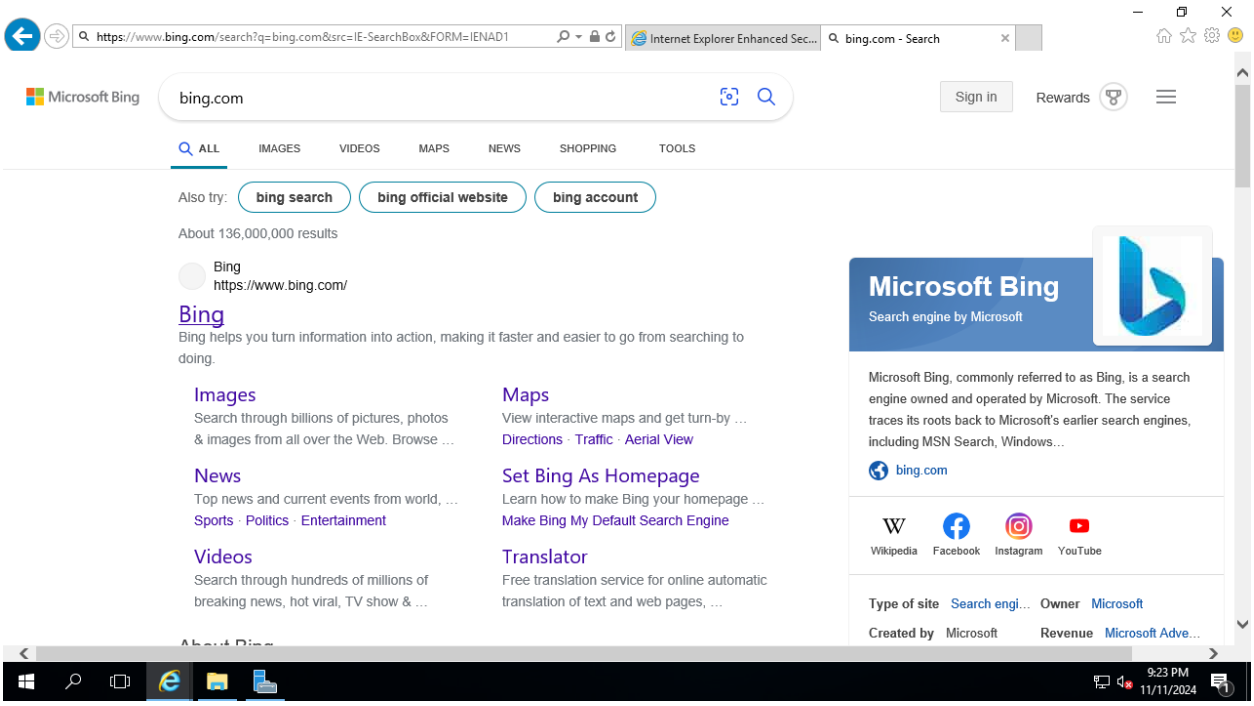


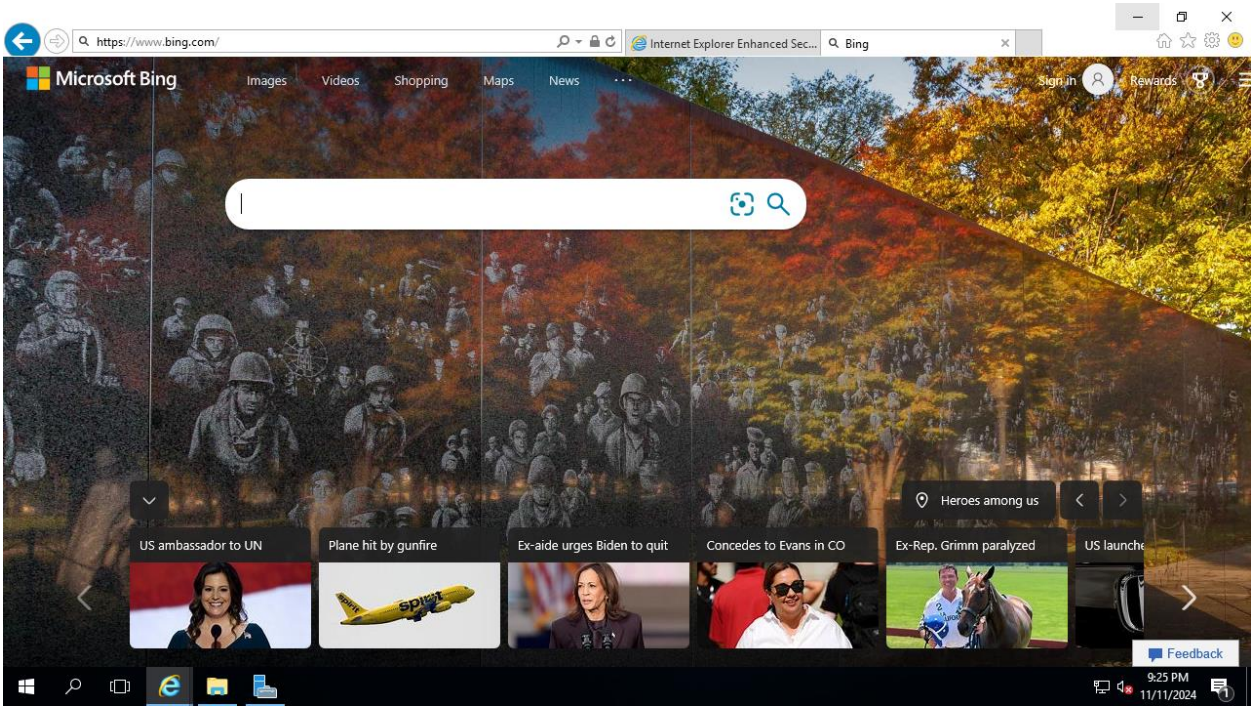
8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.



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

Note: The website should successfully display. The firewall allows you access. We were able to access the website



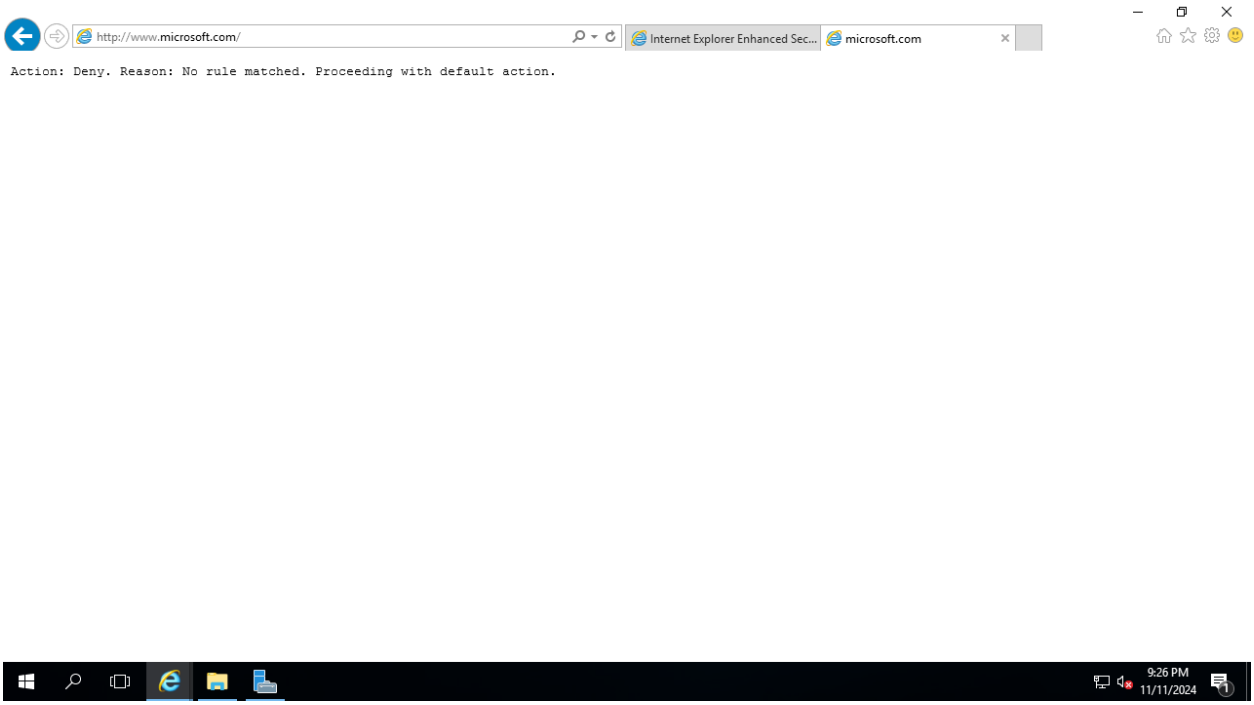


10. Browse to **http://www.microsoft.com/**

Note: 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.

We have been denied access to the //www.microsoft.com/ as seen below.



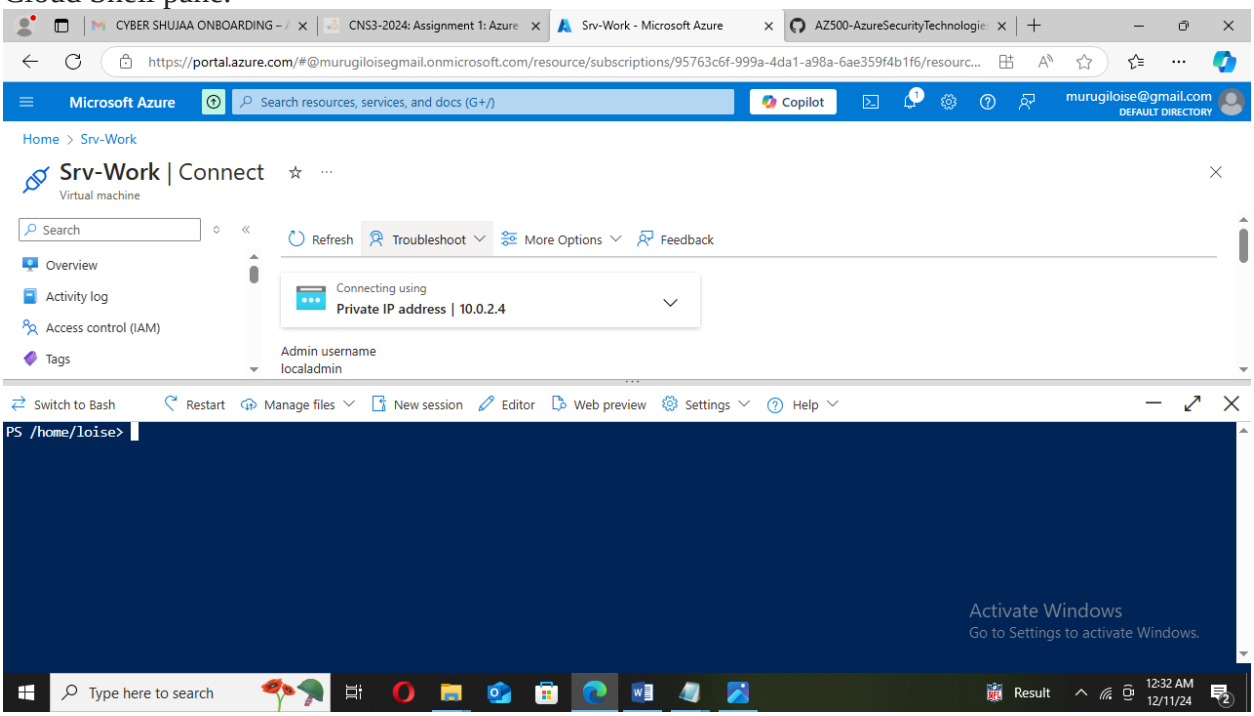
11. Terminate both Remote Desktop sessions.
    We have successfully configured and tested the Azure Firewall.

Clean up resources

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**.

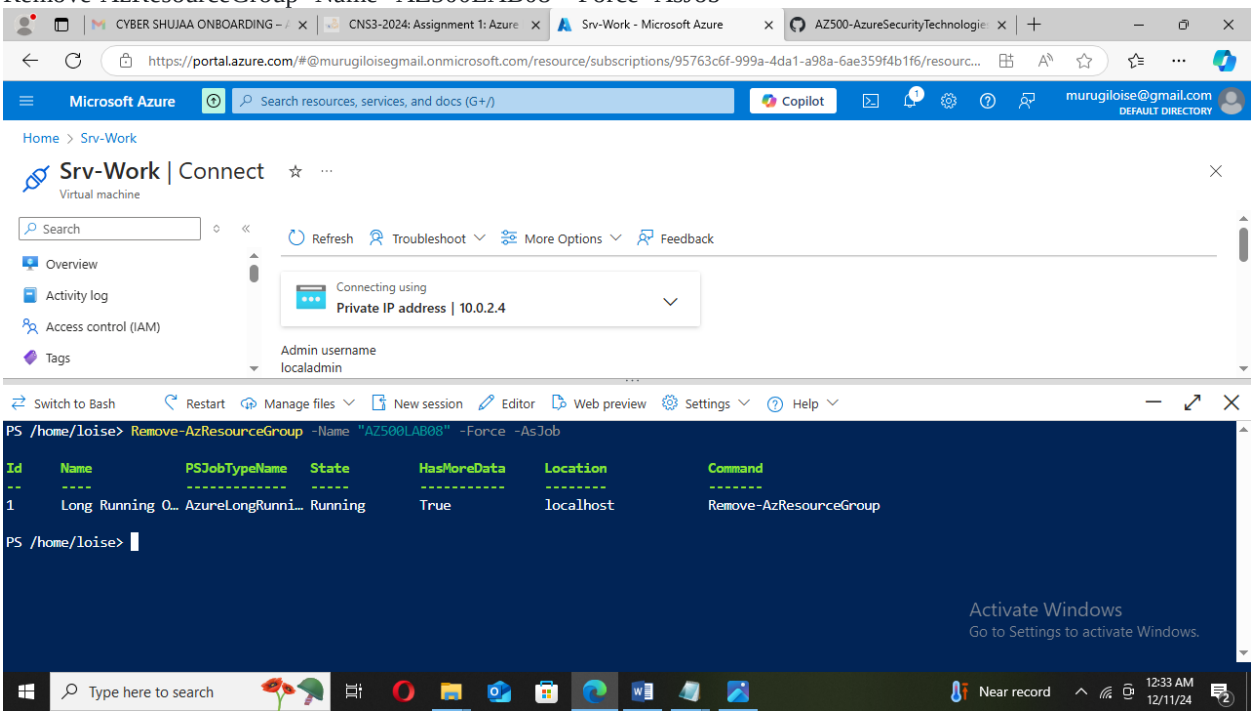
Week 8 Assignment 1: Azure Firewall

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 "AZ500LAB08" -Force -AsJob
```



Conclusion

In this lab activity, we have deployed and tested the azure firewall by first deploying a template that was provided for this lab. Then deploy the azure firewall by using the settings provided then create a resource group AZ500LAB08. We then created a default route that will configure outbound traffic through the firewall. Then configured an application rule that allowed outbound access to www.bing.com.

We then configured a network rule that allowed outbound access to two IP addresses (209.244.0.3 and 209.244.0.4) on port 53 (DNS). Then configured the virtual machine DNS server. We then restarted the virtual machine to be able to login to the virtual machine. Finally, we tested the firewall to confirm its working as expected, we first connected to the Srv-Jump virtual machine via RDP (Remote desktop). Then connected to the Srv-Work virtual machine to test if the firewall allows us to access https://www.bing.com which we were able to access, but denied access to http://www.microsoft.com/ where the firewall blocks access to the website.