

Week 8 Assignment 1: Azure Firewall

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

Class Exercise: Azure Firewall	1
Introduction.....	3
Lab 03: Azure Firewall	3
Lab scenario	3
Lab objectives	3
Exercise 1: Deploy and test an Azure Firewall	3
Task 1: Use a template to deploy the lab environment.....	3
Task 2: Deploy the Azure firewall	8
Task 3: Create a default route.....	13
Task 4: Configure an application rule	20
Task 5: Configure a network rule	25
Task 6: Configure the virtual machine DNS servers	28
Task 7: Test the firewall	30
Clean up resources	37
Conclusion	39

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 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

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

The screenshot shows the Microsoft Azure portal homepage. At the top, there are several tabs: 'Your single-use code - murugiloise' (active), 'CNS3-2024: Assignment 1: Azure', 'AZ500-AzureSecurityTechnologie', and 'Home - Microsoft Azure'. The main header bar includes 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+)'), and icons for Copilot, Mail, Notifications, Settings, and Help. The email 'murugiloise@gmail.com' and 'DEFAULT DIRECTORY' are also visible.

The main content area features a message: 'Hi Loise, see what more you can get from your Azure free account.' Below this are four cards:

- 'Take a free online course on Microsoft Learn' (with a laptop icon)
- 'Watch a demo and attend a live Q&A' (with a video camera icon)
- 'Start a project with Quickstart Center' (with a cloud icon)
- 'Explore support resources' (with a magnifying glass and person icon)

Below these cards is a section titled 'Azure services' with various icons and links:

- Create a resource
- Resource groups
- Virtual machines
- SQL databases
- App registrations
- Automation Accounts
- Deploy a custom...
- Budgets
- Subscriptions
- Activate Windows

The taskbar at the bottom includes the Windows logo, a search bar ('Type here to search'), pinned icons for File Explorer, Edge, and File Hub, and system status indicators ('Near record', '10:54 AM', '11/11/24').

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.

The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal. The URL in the address bar is <https://portal.azure.com/#create/Microsoft.Template>. The page has a header with 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+)'), and icons for Copilot, Mail, Notifications, Settings, and Help. The email 'murugiloise@gmail.com' and 'DEFAULT DIRECTORY' are also visible.

The main content area is titled 'Custom deployment' with the sub-instruction 'Deploy from a custom template'. It includes a 'Select a template' section with tabs for 'Select a template' (selected), 'Basics', and 'Review + create'. A note says: 'Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Create or select a template below to get started.' Below this is a link to 'Learn more about template deployment'.

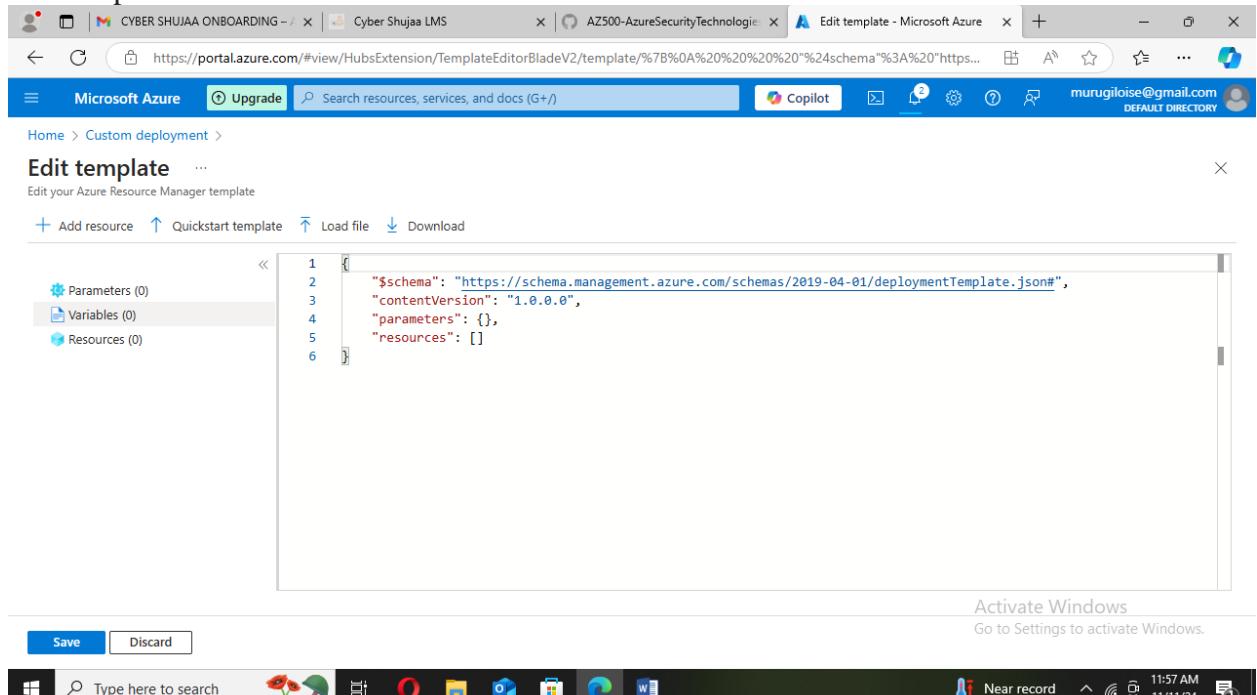
Under 'Common templates', there are links to:

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

At the bottom, there's a section titled 'Start with a quickstart template or template spec' with a 'Template source' dropdown set to 'Quickstart template'. To the right, there's an 'Activate Windows' link with the sub-instruction 'Go to Settings to activate Windows.' The taskbar at the bottom includes the Windows logo, a search bar ('Type here to search'), pinned icons for File Explorer, Edge, and File Hub, and system status indicators ('Construction on a8 /...', '11:51 AM', '11/11/24').

Week 8 Assignment 1: Azure Firewall

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

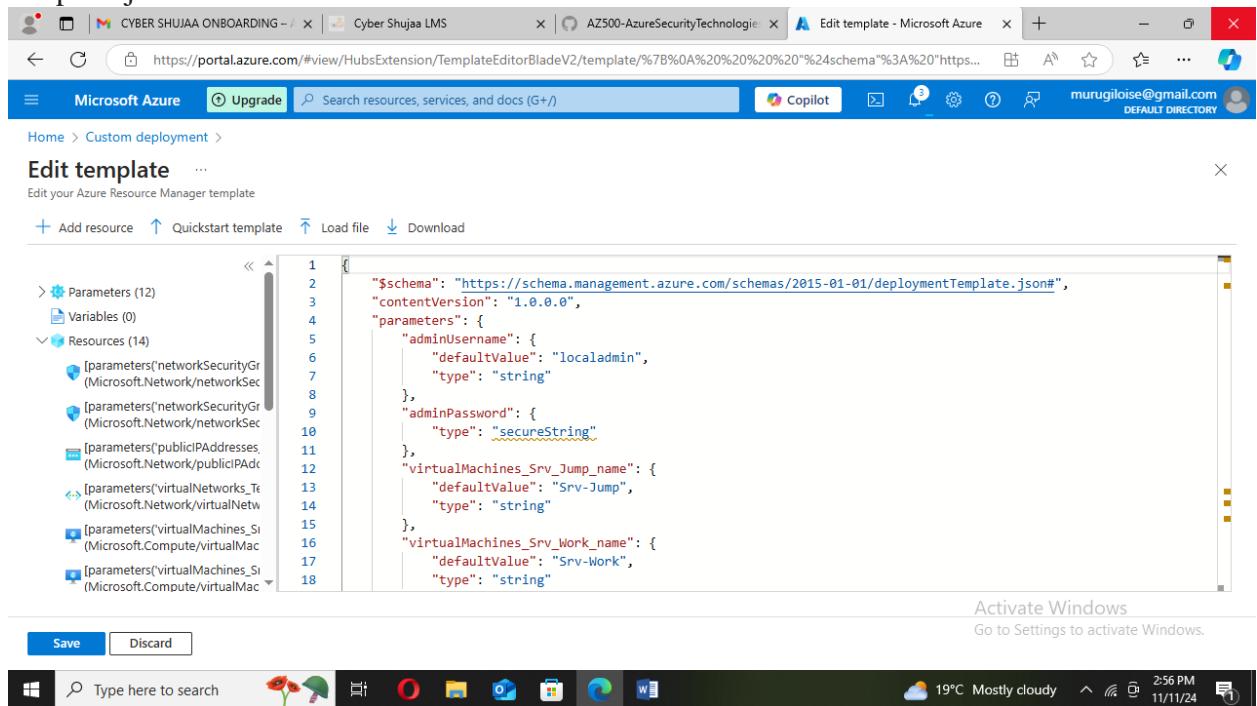


The screenshot shows the 'Edit template' blade in the Azure portal. The URL in the address bar is <https://portal.azure.com/#view/HubsExtension/TemplateEditorBladeV2/template/%7B%0A%20%20%20%24schema%3A%20%22https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json%22%0A%7D>. The left sidebar shows 'Parameters (0)', 'Variables (0)', and 'Resources (0)'. The main area contains the following JSON code:

```
$schema: "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
contentVersion: "1.0.0.0",  
parameters: {},  
resources: []
```

At the bottom, there are 'Save' and 'Discard' buttons. A Windows taskbar at the bottom shows the date and time as 11/11/24 11:57 AM.

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.



The screenshot shows the 'Edit template' blade in the Azure portal after loading a local template. The URL in the address bar is <https://portal.azure.com/#view/HubsExtension/TemplateEditorBladeV2/template/%7B%0A%20%20%20%24schema%3A%20%22https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json%22%0A%7D>. The left sidebar shows expanded sections for 'Parameters (12)', 'Variables (0)', and 'Resources (14)'. The main area contains a large JSON object with many nested properties. At the bottom, there are 'Save' and 'Discard' buttons. A Windows taskbar at the bottom shows the date and time as 11/11/24 2:56 PM.

```
$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"  
    }},  
    ... (many more parameters and resources defined)
```

Week 8 Assignment 1: Azure Firewall

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

The screenshot shows the Microsoft Azure portal interface. The browser tabs include CYBER SHUJAA ONBOARDING, Cyber Shujaa LMS, AZ500-AzureSecurityTechnologies, and Custom deployment - Microsoft. The main content area is titled "Custom deployment" and shows a "Customized template" with 14 resources. The "Basics" tab is selected. Under "Project details", there is a "Subscription" dropdown set to "Azure subscription 1" and a "Resource group" dropdown with "Create new" selected. At the bottom, there are "Previous", "Next", and "Review + create" buttons, with "Review + create" being the active button. A status bar at the bottom shows "Activate Windows", "Go to Settings to activate Windows", and system icons.

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

The screenshot shows the Microsoft Azure portal interface for creating a custom deployment from a template. The top navigation bar includes tabs for CYBER SHUJAA ONBOARDING, Cyber Shujaa LMS, AZ500-AzureSecurityTechnology, and Custom deployment - Microsoft. The main content area is titled "Custom deployment" and shows the following configuration:

- Subscription:** Azure subscription 1
- Resource group:** (New) AZ500LAB08
- Instance details:**
 - Region:** West US
 - Admin Username:** localadmin
 - Admin Password:** (masked)
 - Virtual Machines_Srv_Jump_name:** Srv-Jump
 - Virtual Machines_Srv_Work_name:** Srv-Work

At the bottom of the form, there are "Previous" and "Next" buttons, and a prominent blue "Review + create" button. To the right of the "Review + create" button, there is a message: "Activate Windows" and "Go to Settings to activate Windows." The bottom of the screen shows the Windows taskbar with various pinned icons.

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.

The screenshot shows two windows of the Microsoft Azure portal. The top window is titled 'Custom deployment' and shows a progress bar indicating 'Review + create' is selected. It displays a summary of a 'Customized template' with 14 resources. The bottom window shows the 'Microsoft.Template-2024111152752 | Overview' page, which states 'Your deployment is complete'. Deployment details include a name, start time (11/11/2024, 3:28:17 PM), subscription, correlation ID, and resource group. A 'Deployment details' section is expanded, and a 'Next steps' section is collapsed. The status bar at the bottom of both windows shows the date (11/11/24) and time (3:26 PM).

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.

The screenshot shows the 'Firewall Manager | Azure Firewalls' blade in the Azure portal. The left sidebar has 'Getting Started', 'Deployments', and 'Security' sections, with 'Azure Firewalls' selected. The main area displays a table header with columns: Name, Type, Resource group, Location, and Subscription. Below the table, a large cloud icon is centered with the text 'No firewalls to display'. At the bottom, there's a 'Create firewall' button and a link to 'Learn more about Azure Firewall'.

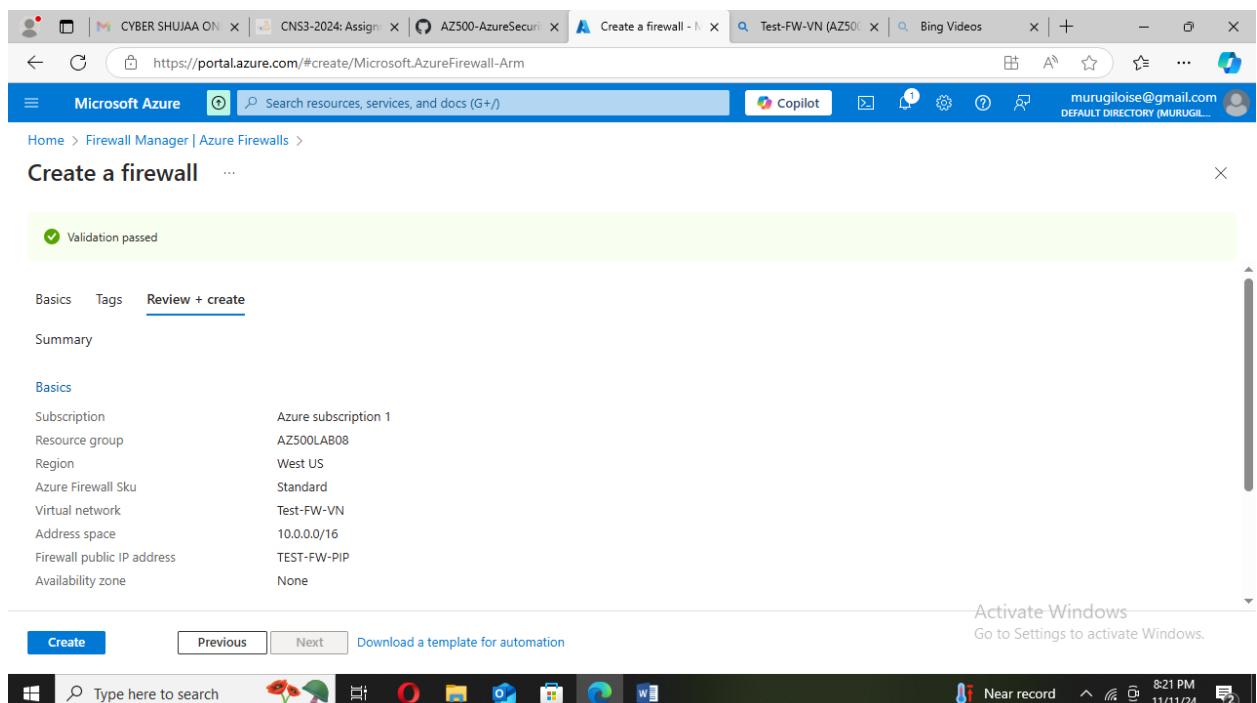
2. On the **Firewalls** blade, click **+ Create**.

The screenshot shows the 'Create a firewall - Microsoft Azure' blade. The top navigation bar includes 'Basics', 'Tags', and 'Review + create'. The main content area describes Azure Firewall as a managed cloud-based network security service. Under 'Project details', 'Subscription' is set to 'Azure subscription 1' and 'Resource group' is set to 'Create new'. Under 'Instance details', 'Name' is empty and 'Region' is set to 'West US'. At the bottom, there are 'Previous' and 'Next : Tags >' buttons, along with a link to 'Download a template for automation'. A status bar at the bottom indicates 'Activate Windows'.

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	click Add new and type the name TEST-FW-PIP and click OK



The screenshot shows the Microsoft Azure portal interface for creating a new Azure Firewall. The page title is "Create a firewall". A green banner at the top indicates "Validation passed". Below it, there are tabs for "Basics", "Tags", and "Review + create", with "Review + create" being the active tab. The "Summary" section displays the following configuration details:

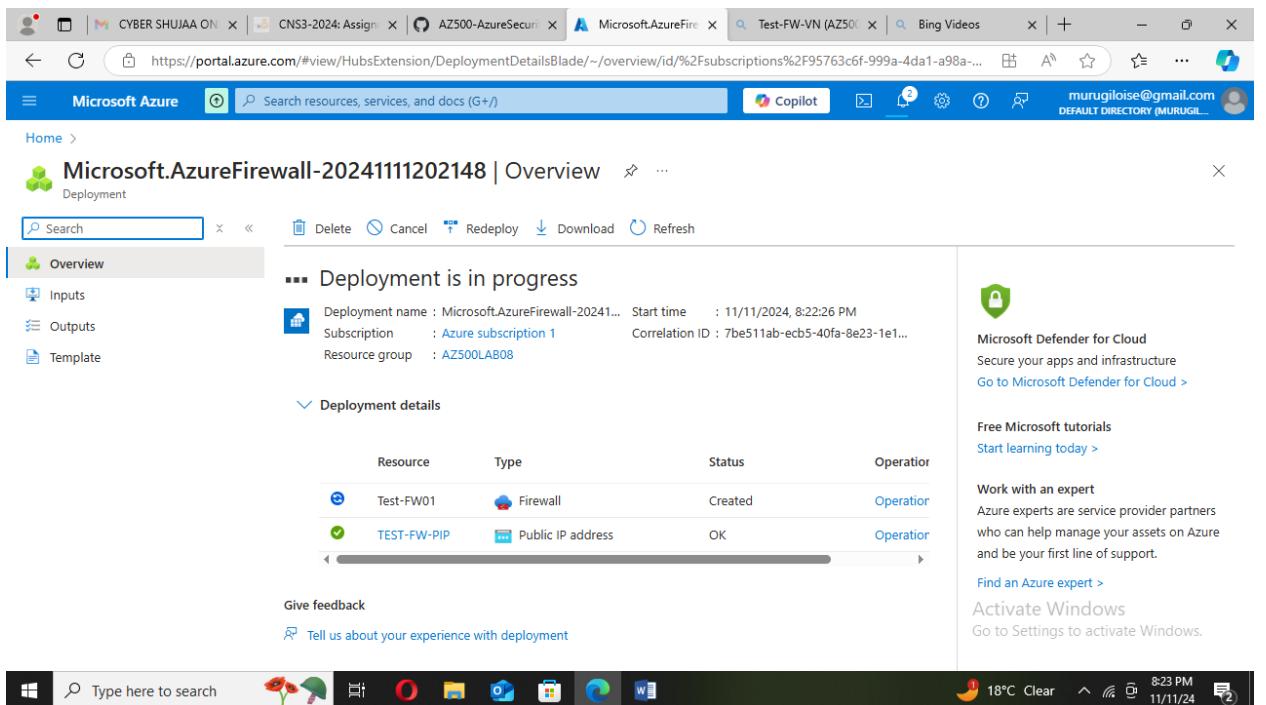
Setting	Value
Subscription	Azure subscription 1
Resource group	AZ500LAB08
Region	West US
Azure Firewall Sku	Standard
Virtual network	Test-FW-VN
Address space	10.0.0.0/16
Firewall public IP address	TEST-FW-PIP
Availability zone	None

At the bottom of the screen, the Windows taskbar is visible with various pinned icons and the system tray showing the date and time.

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



Microsoft.AzureFirewall-2024111202148 | Overview

Deployment

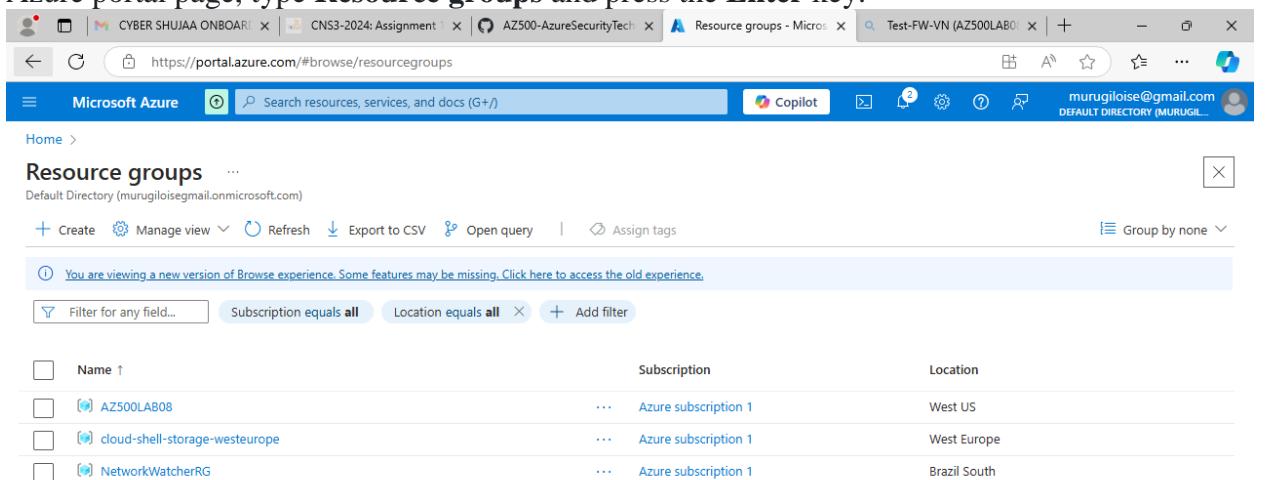
Deployment is in progress

Resource	Type	Status	Operator
Test-FW01	Firewall	Created	Operator
TEST-FW-PIP	Public IP address	OK	Operator

Give feedback

Tell us about your experience with deployment

- 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.



Resource groups

Name	Subscription	Location
AZ500LAB08	Azure subscription 1	West US
cloud-shell-storage-westeurope	Azure subscription 1	West Europe
NetworkWatcherRG	Azure subscription 1	Brazil South

- 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.

Week 8 Assignment 1: Azure 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.

The screenshot shows the Azure portal interface. At the top, there are several tabs: CYBER SHUJAA ON, CNS3-2024: Assign, AZ500-AzureSecuri, Route tables - Micro, Test-FW-VN (AZ500), www.bing.com. Below the tabs is a search bar with the placeholder 'Search resources, services, and docs (G+/)'. The main content area is titled 'Route tables' and shows a message: 'No route tables to display'. Below this message is a blue button labeled 'Create route table'. The page also features standard Azure navigation elements like 'Home >', 'Copilot', and a user profile icon. At the bottom, there's a taskbar with icons for various Windows applications like File Explorer, Edge, and Task View, along with system status indicators for battery, signal, and time.

Week 8 Assignment 1: Azure Firewall

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

The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#create/Microsoft.RouteTable-ARM>. The page title is "Create Route table". The "Basics" tab is selected. Under "Project details", it shows "Subscription" set to "Azure subscription 1" and "Resource group" set to "Create new". Under "Instance details", it shows "Region" set to "East US" and "Name" as an empty field. The "Propagate gateway routes" option is set to "Yes". At the bottom, there are "Previous", "Next", and "Review + create" buttons. The status bar at the bottom right shows "Activate Windows", "Go to Settings to activate Windows.", "Give feedback", "USD/RUB -1.64%", "8:41 PM", and "11/11/24".

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

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#create/Microsoft.RouteTable-ARM>. The page is titled 'Create Route table'. At the top, there are tabs for 'Basics', 'Tags', and 'Review + create'. The 'Review + create' tab is selected. Below it, there is a 'View automation template' link. A 'TERMS' section contains legal text about agreeing to Microsoft's terms and privacy statement. Under the 'Basics' section, 'Subscription' is set to 'Azure subscription 1' and 'Resource group' is set to 'AZ500LAB08'. At the bottom of the wizard, there are 'Previous', 'Next', and 'Create' buttons. The status bar at the bottom right shows 'Activate Windows', 'USD/RUB -1.64%', '8:45 PM 11/11/24', and a notification icon.

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

The screenshot shows the Microsoft Azure portal with the URL <https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F95763c6f-999a-4da1-a98a-...>. The page is titled 'Microsoft.RouteTable-2024111204151 | Overview'. The left sidebar has 'Overview' selected, along with 'Inputs', 'Outputs', and 'Template'. The main area displays deployment details: Deployment name: Microsoft.RouteTable-2024111..., Start time: 11/11/2024, 8:46:46 PM, Subscription: Azure subscription 1, Correlation ID: 3fb34cbd-e9ba-48c9-a261-bf5..., Resource group: AZ500LAB08. Below this, there are sections for 'Deployment details' and 'Next steps'. At the bottom, there is a 'Go to resource' button and a 'Give feedback' link. The status bar at the bottom right shows '8:47 PM 11/11/24' and a notification icon.

- 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

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes tabs for CYBER SHUJAA ON, CNS3-2024: Assign..., AZ500-AzureSecurity, Route tables - Mic..., Test-FW-VN (AZ500...), www.bing.com, and Copilot. The main title is "Route tables". Below the title, it says "Default Directory (murugiloisegmail.onmicrosoft.com)". There are buttons for "+ Create", "Manage view", "Refresh", "Export to CSV", "Open query", and "Assign tags". A search bar says "Search resources, services, and docs (G+/)". The user's email, "murugiloise@gmail.com", is shown in the top right.

Showing 1 to 1 of 1 records.

Name	Resource group	Location	Subscription
Firewall-route	AZ500LAB08	West US	Azure subscription 1

The screenshot shows the Microsoft Azure portal interface, similar to the previous one but with a different URL: https://portal.azure.com/#/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Network/routeTables/1. The title is "Firewall-route". The left sidebar shows "Route tables" and "Default Directory (murugiloisegmail.onmicrosoft.com)". The main content area shows the "Overview" tab selected. It displays the following details:

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Monitoring
- Automation
- Help

Essentials:

- Resource group ([move](#)) **AZ500LAB08**
- Location **West US**
- Subscription ([move](#)) **Azure subscription 1**
- Subscription ID **95763c6f-999a-4da1-a98a-6ae359f4b1f6**
- Tags ([edit](#)) [Add tags](#)

Routes:

Name	Address prefix	Next hop type	Next hop IP address
No results.			

Subnets:

Name	Address range
No subnets found.	

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**.

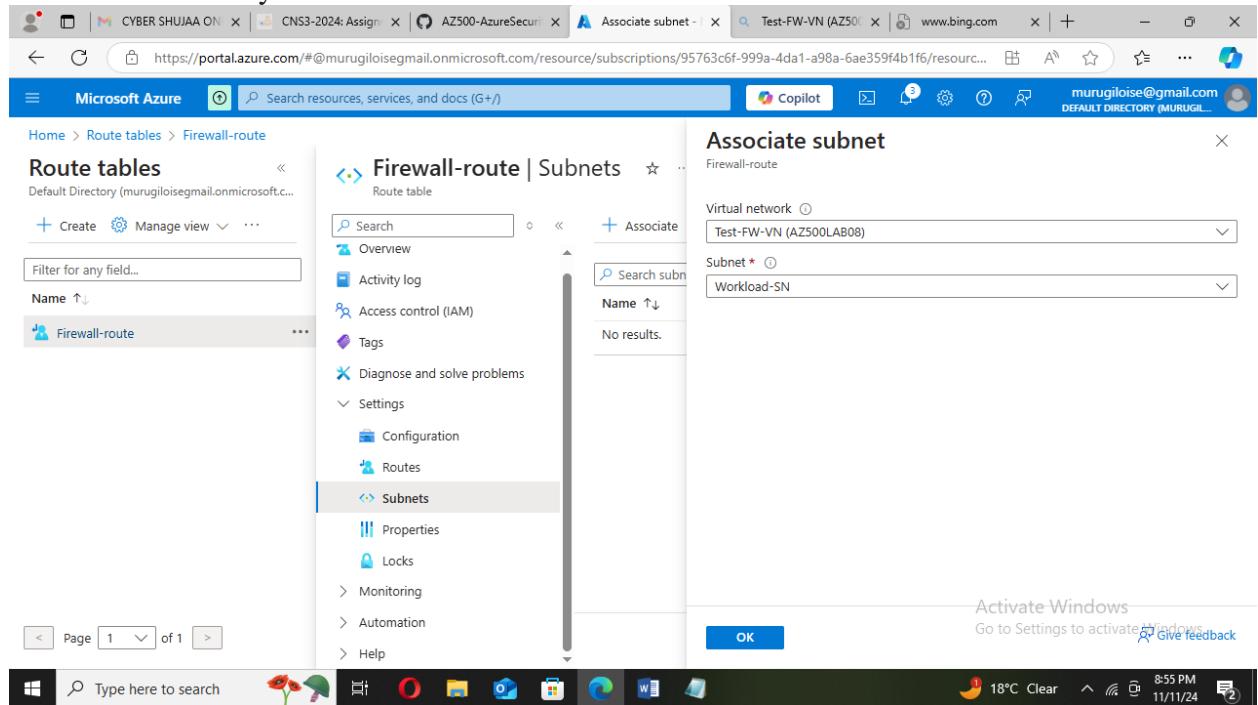
The screenshot shows the Microsoft Azure portal interface. The left sidebar has 'Route tables' selected, and 'Firewall-route' is highlighted. In the main area, a 'Firewall-route | Subnets' blade is open. On the right, a 'Associate subnet' dialog box is displayed over the main blade. The dialog has 'Virtual network' set to 'Test-FW-VN (AZ500LAB08)' and 'Subnet' set to 'Workload-SN'. At the bottom right of the dialog is a blue 'OK' button.

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

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

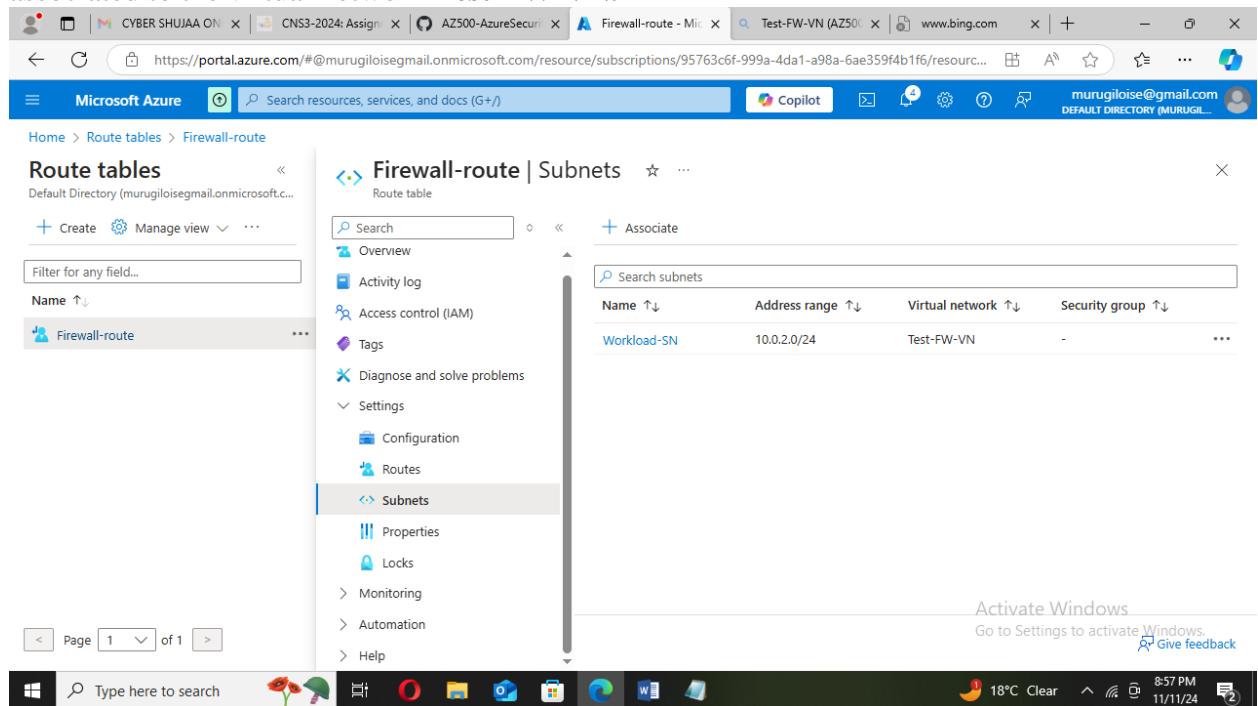
Week 8 Assignment 1: Azure Firewall

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



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar has 'Route tables' selected under 'Firewall-route'. The main content area displays the 'Associate subnet' dialog for a 'Firewall-route' named 'Subnets'. The dialog includes fields for 'Virtual network' (set to 'Test-FW-VN (AZ500LAB08)') and 'Subnet' (set to 'Workload-SN'). A large blue 'OK' button is visible at the bottom right of the dialog. The status bar at the bottom right shows the date and time as '11/11/24 8:55 PM'.

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



The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar has 'Route tables' selected under 'Firewall-route'. The main content area displays the 'Firewall-route | Subnets' page for the 'Firewall-route' named 'Subnets'. The table lists one subnet: 'Workload-SN' with 'Address range' '10.0.2.0/24' and 'Virtual network' 'Test-FW-VN'. The status bar at the bottom right shows the date and time as '11/11/24 8:57 PM'.

Week 8 Assignment 1: Azure Firewall

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

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is [https://portal.azure.com/#/murmurloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/Test-FW-VN\(AZ500\)/providers/Microsoft.Network/fwRules?api-version=2024-01-01&subscriptionId=95763c6f-999a-4da1-a98a-6ae359f4b1f6](https://portal.azure.com/#/murmurloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/Test-FW-VN(AZ500)/providers/Microsoft.Network/fwRules?api-version=2024-01-01&subscriptionId=95763c6f-999a-4da1-a98a-6ae359f4b1f6). The page title is "Add route - Microsoft Azure". The left sidebar shows "Route tables" and "Firewall-route" is selected. The main content area is titled "Firewall-route | Routes" and contains a "Search" bar and a "No results." message. On the right, there is a "Add route" form with fields for "Route name" (with a placeholder "Name"), "Destination type" (with a dropdown "Select destination address prefix type"), "Next hop type" (with a dropdown "Select next hop type"), and "Next hop address" (with a placeholder "Address"). A blue "Add" button is at the bottom right of the form. The status bar at the bottom shows "Activate Windows" and the date/time "8:58 PM 11/11/24".

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.

The screenshot shows the Microsoft Azure portal interface. The user is in the 'Route tables' section under 'Firewall-route'. A modal window titled 'Add route' is open, prompting for route configuration. The 'Route name' field contains 'FW-DG'. The 'Destination type' dropdown is set to 'IP Addresses'. The 'Destination IP addresses/CIDR ranges' field contains '0.0.0.0/0'. The 'Next hop type' dropdown is set to 'Virtual appliance'. The 'Next hop address' field contains '10.0.1.4'. The bottom right of the modal has an 'Add' button and a note about activating Windows.

11. Click Add to add the route.

The screenshot shows the 'Firewall-route | Routes' page in the Azure portal. The left sidebar shows the 'Routes' section is selected. A table lists the added route: FW-DG, with an address prefix of 0.0.0.0/0, a next hop type of VirtualAppliance, and a next hop IP address of 10.0.1.4. The bottom right of the page has an 'Activate Windows' note.

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.

The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Network/azureFirewalls/Test-FW01>. The page title is "Test-FW01 - Microsoft Azure". The main content area displays the "Overview" section for the Test-FW01 firewall. Key details shown include:

- Resource group: AZ500LAB08
- Location: West US
- Subscription: Azure subscription 1
- Subscription ID: 95763c6f-999a-4da1-a98a-6ae359f4b1f6
- 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: (dropdown menu)
- Management public IP: (dropdown menu)
- Private IP Ranges: IANA RFC 1918
- Route Server (preview): Add

The status bar at the bottom shows the date and time as 11/11/24 9:04 PM.

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

The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Network/azureFirewalls/Test-FW01/rules>. The page title is "Test-FW01 | Rules (classic) - Microsoft Azure". The main content area displays the "NAT rule collection" tab. Key details shown include:

- Priority
- Name
- Action
- Rules

The status bar at the bottom shows the date and time as 11/11/24 9:05 PM.

Week 8 Assignment 1: Azure Firewall

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

The screenshot shows the Microsoft Azure portal interface. The left sidebar is for the 'Test-FW01 Firewall' resource, with 'Rules (classic)' selected. The main content area is titled 'Add application rule collection'. It has fields for 'Name' (empty), 'Priority' (set to 'allowed numeric values between 100-65000'), and 'Action' (set to 'Allow'). Below these are sections for 'Rules' and 'FQDN tags'. Under 'Rules', there's a table with columns 'name', 'Source type', 'Source', and 'FQDN tags'. The 'Source type' dropdown is set to 'IP address', and the 'Source' dropdown contains multiple IP addresses. Under 'FQDN tags', it says '0 selected'. A note below the table says 'FQDN tags may require additional configuration.' Under 'Target FQDNs', there's another table with columns 'name', 'Source type', 'Source', 'Protocol:Port', and 'Target FQDNs'. The 'Source type' dropdown is set to 'IP address', and the 'Source' dropdown contains multiple IP addresses. The 'Protocol:Port' dropdown contains 'http, http:8080, https, mssql:...'. The 'Target FQDNs' dropdown contains 'www.microsoft.com, *.micros...'. An 'Add' button is at the bottom of this section. At the bottom of the page, there's a Windows taskbar with a search bar, weather information (18°C Clear), and system status.

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

The screenshot shows the 'Add application rule collection' blade in the Microsoft Azure portal. The left sidebar shows the 'Test-FW01' firewall resource. The main form has the following settings:

- Name:** App-Coll01
- Priority:** 200
- Action:** Allow
- Rules:** FQDN tags
- FQDN tags:** A table with one row: name: AllowGH, Source type: IP address, Source: 10.0.2.0/24, Protocol:Port: http:80, https:443, Target FQDNs: www.bing.com
- Target FQDNs:** A table with one row: name: AllowGH, Source type: IP address, Source: 10.0.2.0/24, Protocol:Port: http:80, https:443, Target FQDNs: www.bing.com

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

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

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

Week 8 Assignment 1: Azure Firewall

The screenshot shows the 'Add application rule collection' page in the Microsoft Azure portal. The rule is named 'AllowGH' and is configured to allow traffic from IP address 10.0.2.0/24 on port http:80, https:443 to the FQDN www.bing.com.

name	Source type	Source	FQDN tags
AllowGH	IP address	10.0.2.0/24	www.bing.com

The 'Target FQDNs' section also lists the FQDN www.microsoft.com and port mssql:1433.

- 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.

The screenshot shows the 'Test-FW01 | Rules (classic)' page in the Microsoft Azure portal. A success message indicates that the firewall was updated successfully.

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

The 'Application rule collection' tab is selected, and the rule 'App-Coll01' is listed with priority 200, action Allow, and one rule.

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.

The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Network/azureFirewalls/Test-FW01/rules>. The page title is "Test-FW01 | Rules (classic)". The left sidebar shows "Rules (classic)" is selected. The main content area has tabs for "NAT rule collection", "Network rule collection", and "Application rule collection", with "Application rule collection" being the active tab. A table lists one rule: "Priority": 200, "Name": App-Coll01, "Action": Allow, and "Rules": > 1 rule. A note at the bottom states: "Azure infrastructure application rule collection is enabled by default. [Learn more](#)". The status bar at the bottom right shows "Activate Windows Go to Settings to activate Windows".

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

The screenshot shows the "Add network rule collection" dialog box. The "Name" field is empty. The "Priority" field is set to "allowed numeric values between 100-65000". The "Action" field is set to "Allow". The "IP Addresses" section contains a table with columns: name, Protocol, Source type, Source, Destination type, Destination Addr..., and Destination Ports. It shows two entries: "*, 192.168.10.1, 192..." and "*, 192.168.10.1, 192..." with destination ports "8080, 8080-8090, *". The "Service Tags" section contains a table with columns: name, Protocol, Source type, Source, Service Tags, and Destination Ports. It shows one entry with "0 selected" under Service Tags and destination ports "8080, 8080-8090, *". The "FQDNs" section contains a table with columns: name, Protocol, Source type, Source, Destination FQDNs, and Destination Ports. It shows one entry with "0 selected" under Destination FQDNs and destination ports "8080, 8080-8090, *". The status bar at the bottom right shows "Activate Windows Go to Settings to activate Windows".

Week 8 Assignment 1: Azure Firewall

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
--------	--------------

The screenshot shows the 'Add network rule collection' blade in the Azure portal. The 'Name' field is set to 'Net-Coll01', 'Priority' is 200, and 'Action' is 'Allow'. The 'IP Addresses' section contains one entry: Source IP address range is '*', Destination IP address range is '192.168.10.1, 192.168.10.2', and Destination Ports are '8080, 8080-8090'. Below this, there are sections for 'Service Tags', 'FQDNs', and an 'Add' button. The left sidebar shows the 'Test-FW01' resource group and its sub-components like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve, Settings, DNS, Rules (classic), Public IP config, Learned SNAT IP Prefixes (preview), Threat intelligence, Firewall Manager, and Properties.

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
-------------	-------------------

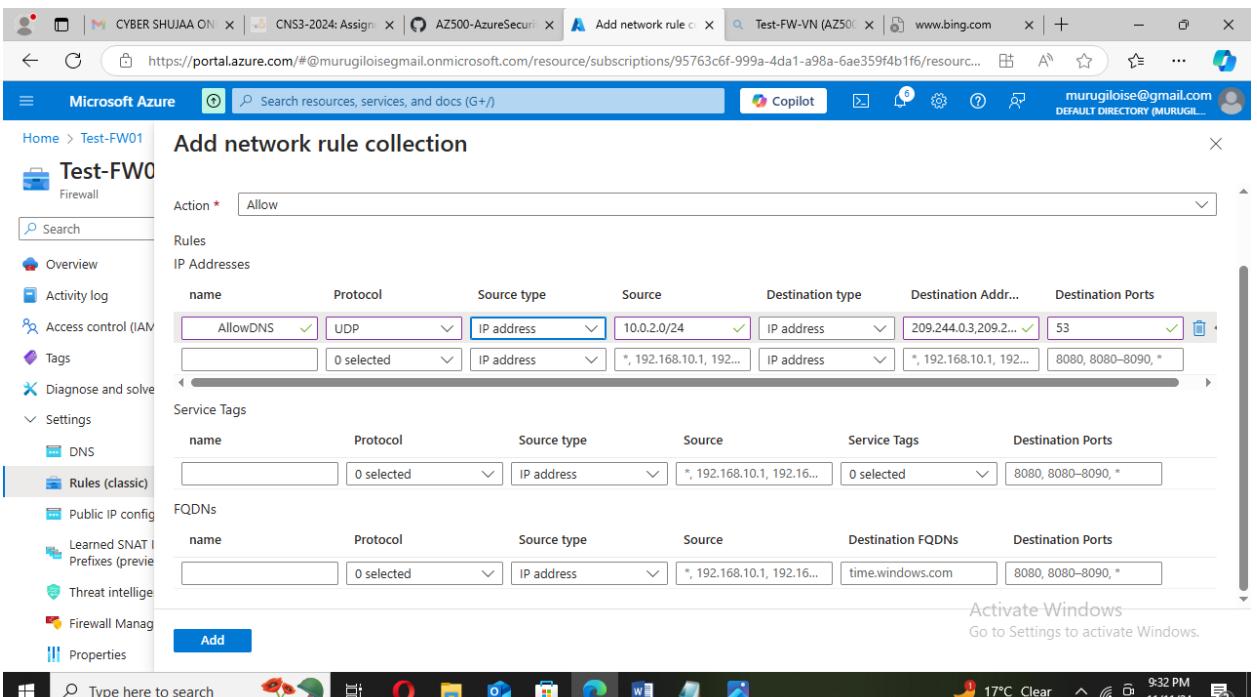
Source Addresses	10.0.2.0/24
------------------	--------------------

Destination type	IP address
------------------	-------------------

Destination Address	209.244.0.3,209.244.0.4
---------------------	--------------------------------

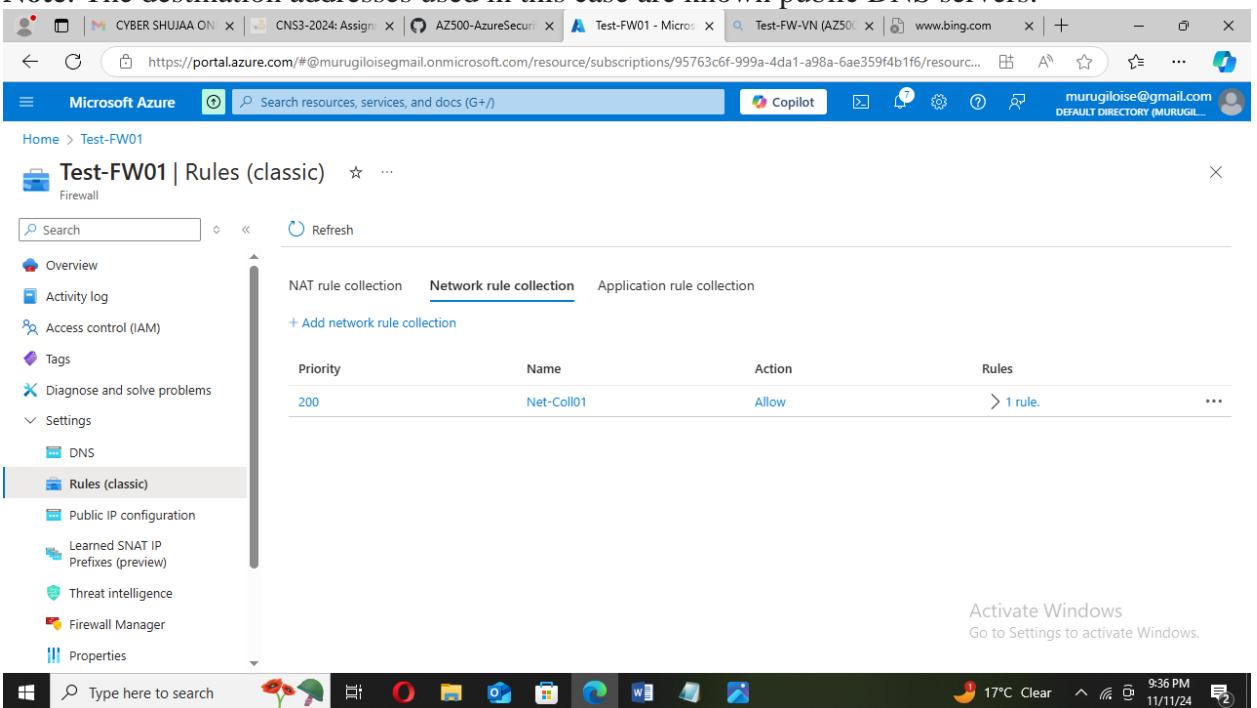
Week 8 Assignment 1: Azure Firewall

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.

The screenshot shows the Microsoft Azure portal interface. The left sidebar shows the navigation path: Home > AZ500LAB08 > Srv-Work. The main content area displays the 'Overview' tab for the 'Srv-Work' virtual machine. Key details include:

- Resource group: AZ500LAB08
- Status: Running
- Location: West US
- Subscription: Azure subscription 1
- Subscription ID: 95763c6f-999a-4da1-a98a-6ae359f4b1f6
- Operating system: Windows (Windows Server 2016 Datacenter)
- Size: Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
- Public IP address: (not explicitly shown)
- Virtual network/subnet: Test-FW-VN/Workload-SN
- DNS name: (not explicitly shown)
- Health state: (not explicitly shown)
- Time created: 11/11/2024, 12:28 PM UTC

The 'Networking' section is visible in the sidebar under the 'Essentials' heading. The status bar at the bottom shows the date and time as 11/11/24 and 9:40 PM.

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

The screenshot shows the Microsoft Azure portal interface, specifically the 'Network settings' blade for the 'Srv-Work' virtual machine. The left sidebar shows the navigation path: Home > AZ500LAB08 > Srv-Work. The main content area displays the 'Network settings' tab. Key details include:

- Network interface: srv-work267 (primary) / ipconfig1 (primary)
- Virtual network / subnet: Test-FW-VN / Workload-SN
- Public IP address: (Configure)
- Private IP address: 10.0.2.4
- Load balancers: 0 (Configure)
- Application security groups: 0 (Configure)
- Network security group: Srv-Work-nsg
- Accelerated networking: Disabled

The 'Networking' section is visible in the sidebar under the 'Network settings' heading. The status bar at the bottom shows the date and time as 11/11/24 and 9:42 PM.

Week 8 Assignment 1: Azure Firewall

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

srv-work267 | IP configurations

IP Settings

Subnet: Workload-SN (10.0.2.0/24) 250 free IP addresses

DNS servers

Applied DNS servers: 209.244.0.3, 209.244.0.4

Activate Windows
Go to Settings to activate [Give feedback](#)

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.

srv-work267 | DNS servers

DNS servers

Inherit from virtual network (radio button)

Custom (radio button)

DNS server: 209.244.0.3, 209.244.0.4

Applied DNS servers: 209.244.0.3, 209.244.0.4

Activate Windows
Go to Settings to activate [Give feedback](#)

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.

The screenshot shows the Microsoft Azure portal interface. At the top, there are several browser tabs open, including 'CYBER SHUJAA ON', 'CNS3-2024: Assign', 'AZ500-AzureSecuri...', 'Srv-Work - Microsoft Edge', 'Test-FW-VN (AZ500...', and 'www.bing.com'. The main navigation bar shows 'Microsoft Azure' and the user's email 'murugiloise@gmail.com'. Below the navigation bar, the breadcrumb path 'Home > AZ500LAB08 > Srv-Work' is visible. On the left, a sidebar menu is open under 'Srv-Work', showing options like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Connect', 'Networking', 'Settings', 'Availability + scale', 'Security', 'Backup + disaster recovery', 'Operations', 'Monitoring', and 'Automation'. The 'Overview' tab is selected. The main content area displays the 'Essentials' section for the VM. Key details include:

Resource group	Operating system
AZ500LAB08	Windows (Windows Server 2016 Datacenter)
Status	Size
Running	Standard DS1 v2 (1 vcpu, 3.5 GiB memory)
Location	Public IP address
West US	[redacted]
Subscription	Virtual network/subnet
Azure subscription 1	Test-FW-VN/Workload-SN
Subscription ID	DNS name
95763c6f-999a-4da1-a98a-6ae359f4b1f6	[redacted]
	Health state
	-
	Time created
	11/11/2024, 12:28 PM UTC

At the bottom of the screen, there is a taskbar with various icons and a weather widget indicating '17°C Clear' at 9:52 PM on 11/11/24.

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.

The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Compute/virtualMachines/Srv-Jump>. The page displays the 'Overview' section for the AZ500LAB08 resource group. On the left, there's a sidebar with options like Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, Automation, and Help. The main area shows a table of resources with columns for Name, Type, and Location. The resources listed are:

Name	Type	Location
Firewall-route	Route table	West US
Srv-Jump	Virtual machine	West US
Srv-Jump-nsg	Network security group	West US
Srv-Jump-PIP	Public IP address	West US
srv-jump121	Network Interface	West US
Srv-Jump_OsDisk_1_3d65499f1f76463ab31b970d6a05091f	Disk	West US
Srv-Work	Virtual machine	West US

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

The screenshot shows the Azure portal interface with the URL <https://portal.azure.com/#@murugiloisegmail.onmicrosoft.com/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Compute/virtualMachines/Srv-Jump>. The page displays the 'Overview' section for the Srv-Jump virtual machine. On the left, there's a sidebar with options like Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Networking, Settings, Availability + scale, Security, Backup + disaster recovery, Operations, Monitoring, and Automation. The main area shows the VM details. The 'Essentials' section includes information such as Resource group (move) to AZ500LAB08, Status (Running), Location (West US), Subscription (move) to Azure subscription 1, Subscription ID 95763c6f-999a-4da1-a98a-6ae359f4b1f6, Operating system (Windows Server 2016 Datacenter), Size (Standard DS1 v2), Public IP address (13.88.62.95), Virtual network/subnet (Test-FW-VN/Jump-SN), DNS name (Not configured), and Health state (Unknown). The time created is 11/11/2024, 12:28 PM UTC.

Week 8 Assignment 1: Azure Firewall

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

The screenshot shows the Microsoft Azure portal interface. The URL in the address bar is <https://portal.azure.com/#/resource/subscriptions/95763c6f-999a-4da1-a98a-6ae359f4b1f6/resourceGroups/AZ500LAB08/providers/Microsoft.Compute/virtualMachines/Srv-Jump>. The page title is "Srv-Jump | Connect". The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Connect. Under Connect, "Native RDP" is selected. The main content area displays "Admin username: localadmin", "Port (change): 3389", and "Just-in-time policy: Unsupported by plan". Below this, a "Most common" section shows "Native RDP" with a description: "Connect via native RDP without any additional software needed. Recommended for testing only." It also shows the "Public IP address (13.88.62.95)". At the bottom, there are "Select" and "Download RDP file" buttons. The taskbar at the bottom right shows the date and time as 10:03 PM, 11/11/24.

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

Setting	Value
---------	-------

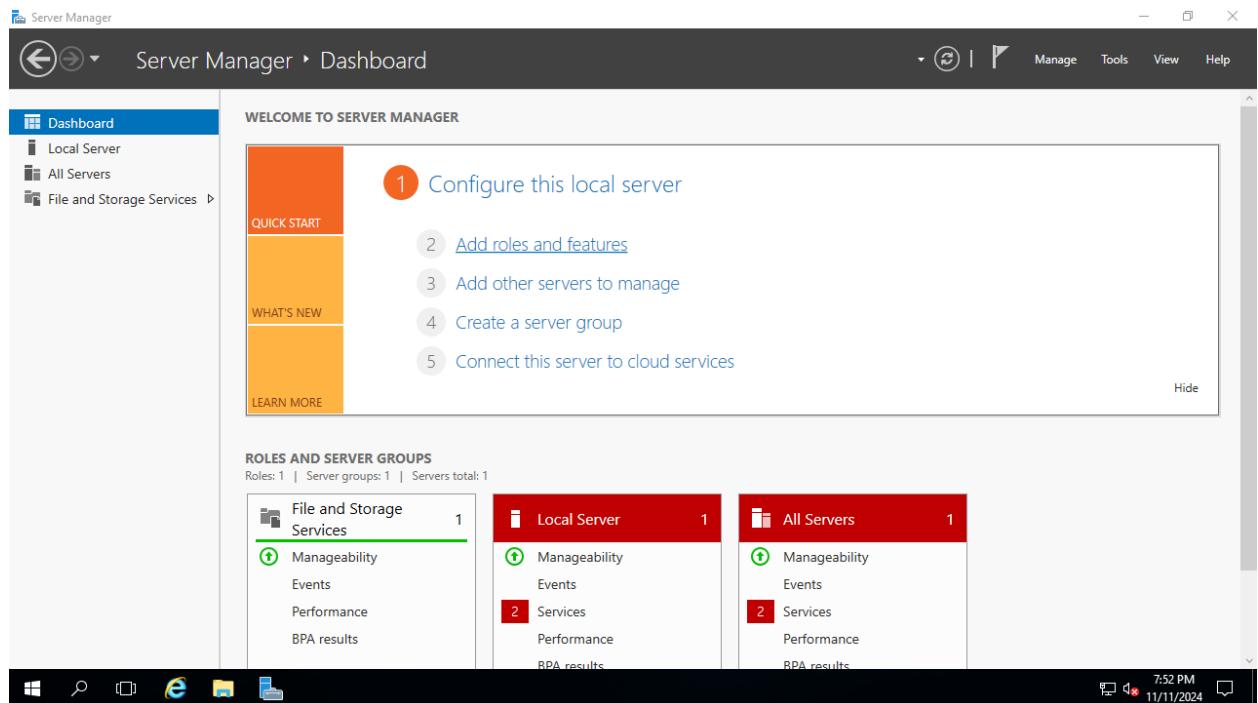
User name	localadmin
-----------	-------------------

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

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

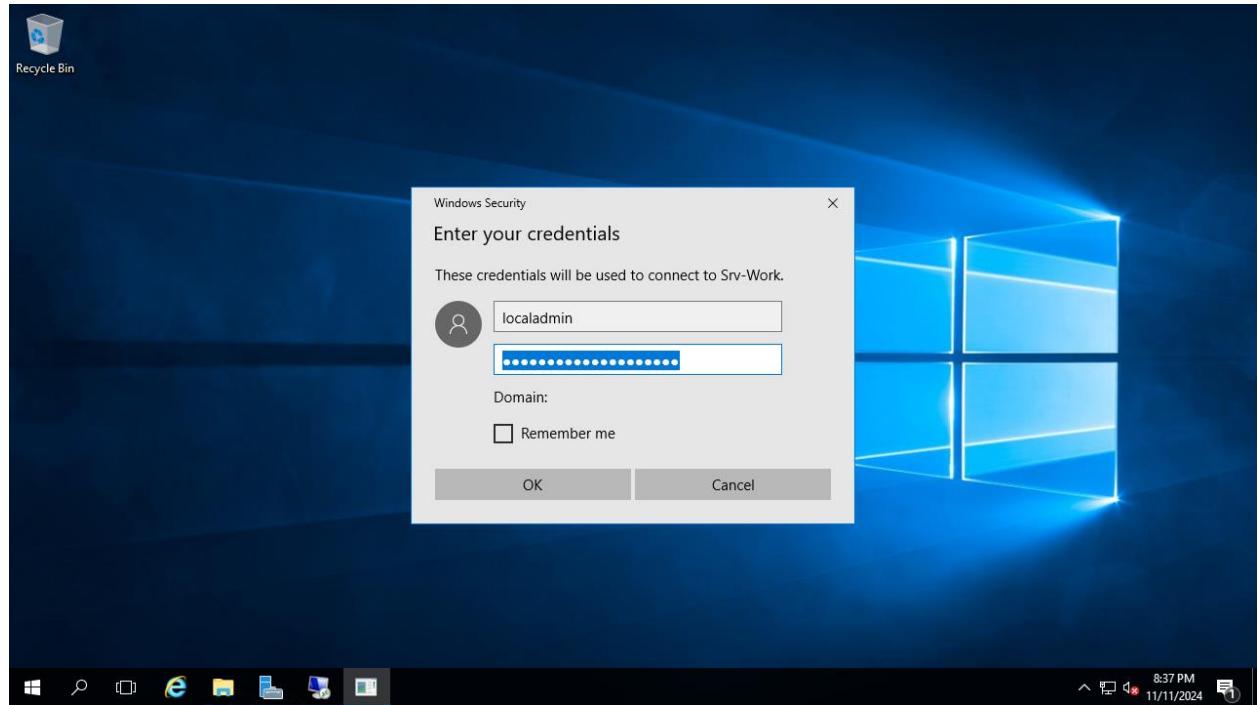
Note: You will connect to the **Srv-Work** virtual machine. This is being done so we can test the ability to access the [bing.com](http://www.bing.com) website. We were able to successfully connect to the **Srv-Work** virtual machine as seen below.

Week 8 Assignment 1: Azure Firewall



- 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**.

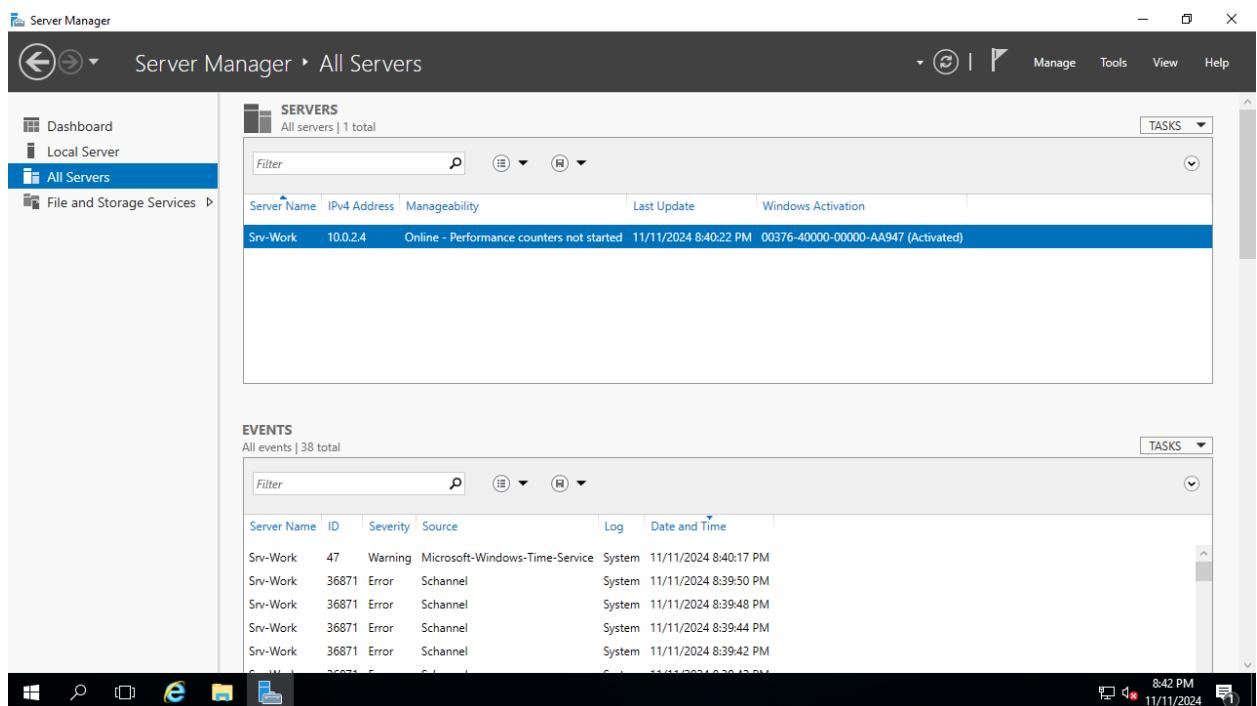
```
mstsc /v:Srv-Work
```



- When prompted to authenticate, provide the following credentials:

Week 8 Assignment 1: Azure Firewall

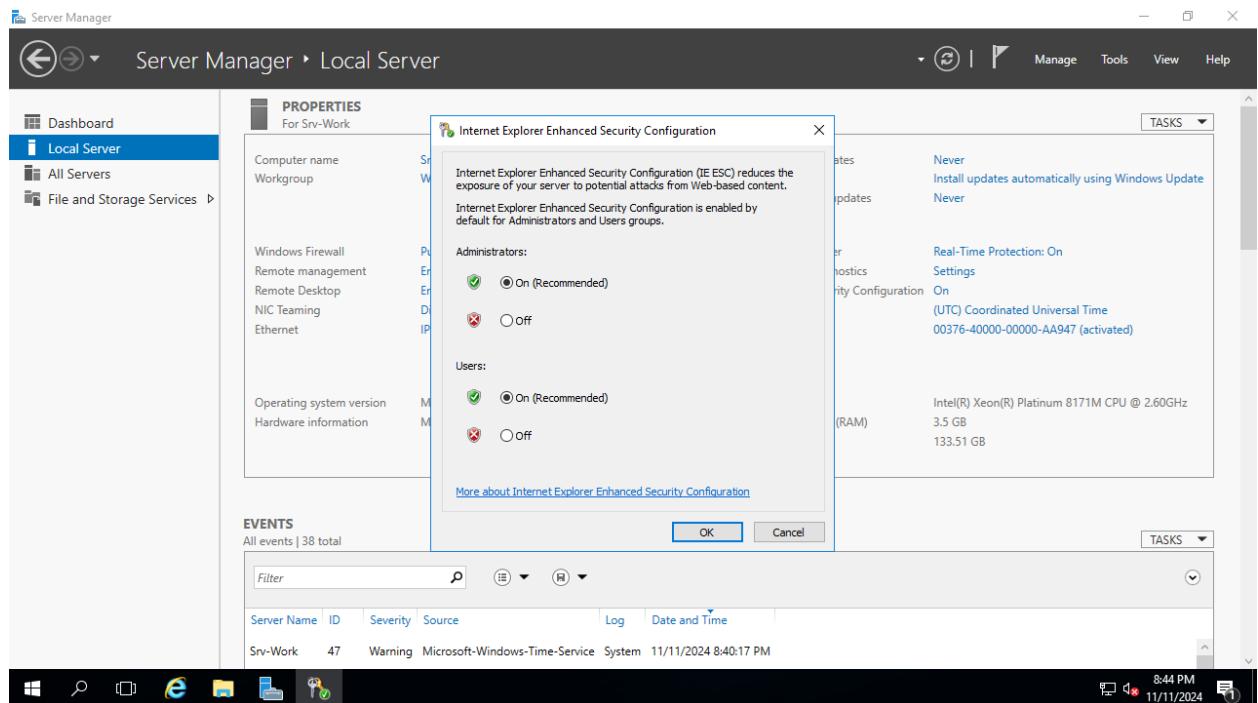
Setting	Value
User name	localadmin
Password	The secure password you chose during deployment of the custom template in task 1 step 6. We were able to connect to Srv-W



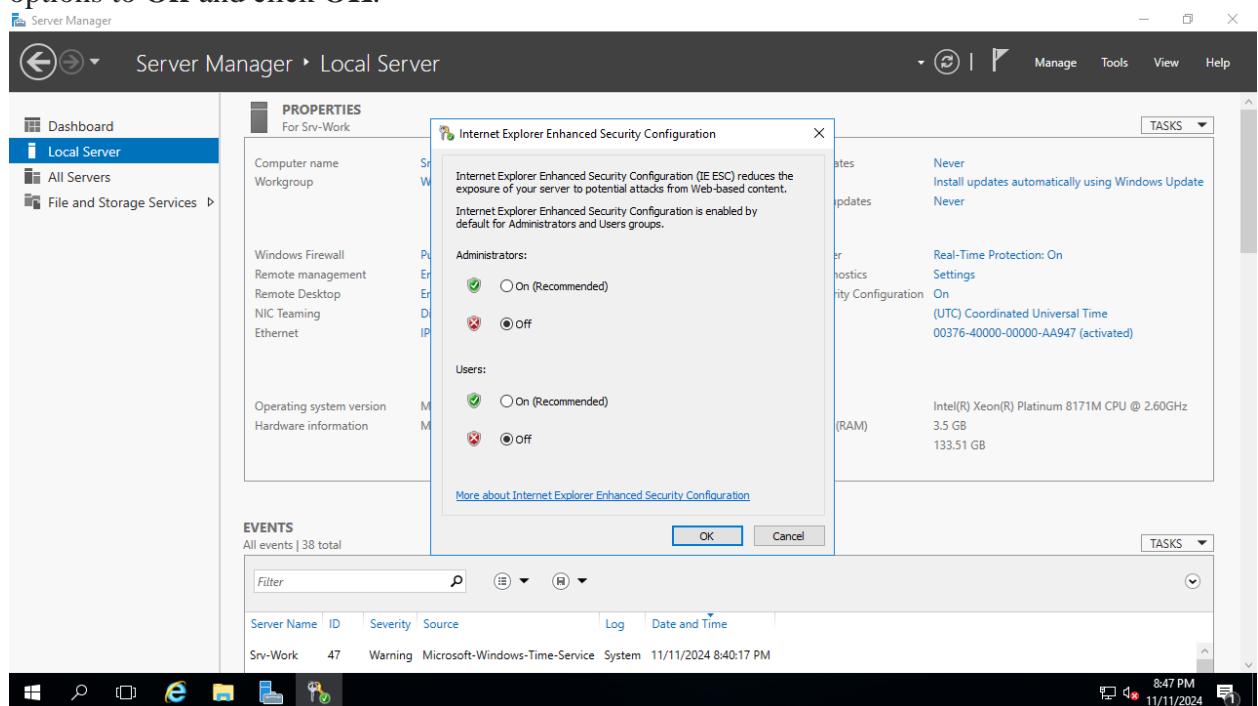
Note: Wait for the Remote Desktop session to be established and the Server Manager interface to load.

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



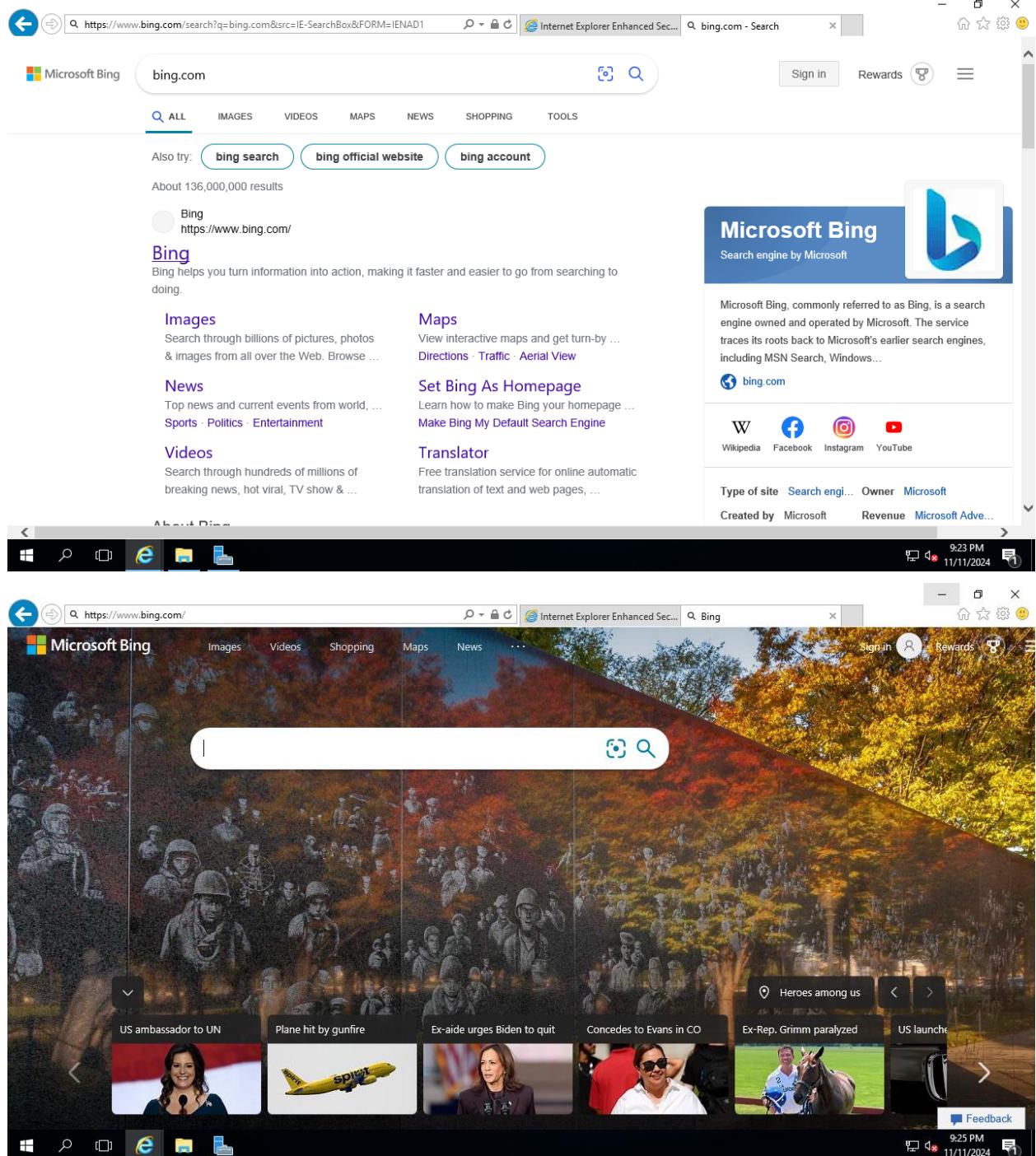
8. In the **Internet Explorer Enhanced Security Configuration** dialog box, set both options to **Off** and click **OK**.



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

Week 8 Assignment 1: Azure Firewall

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



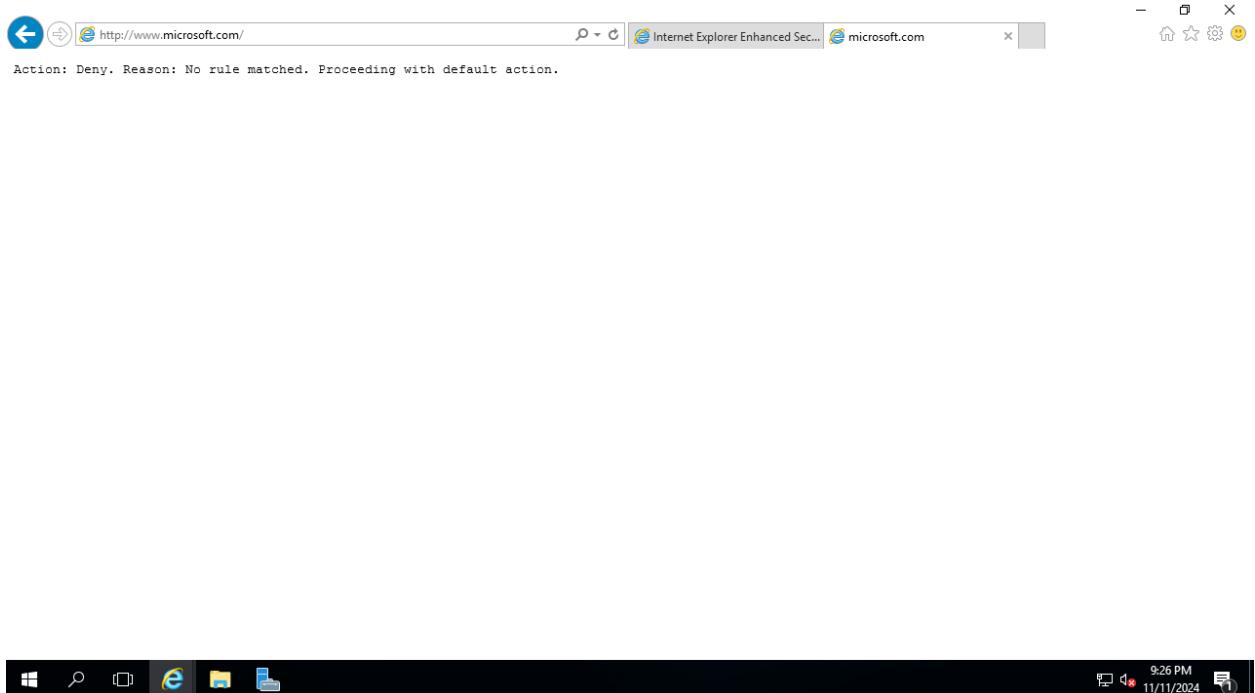
10. Browse to <http://www.microsoft.com/>

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.

Week 8 Assignment 1: Azure Firewall

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.

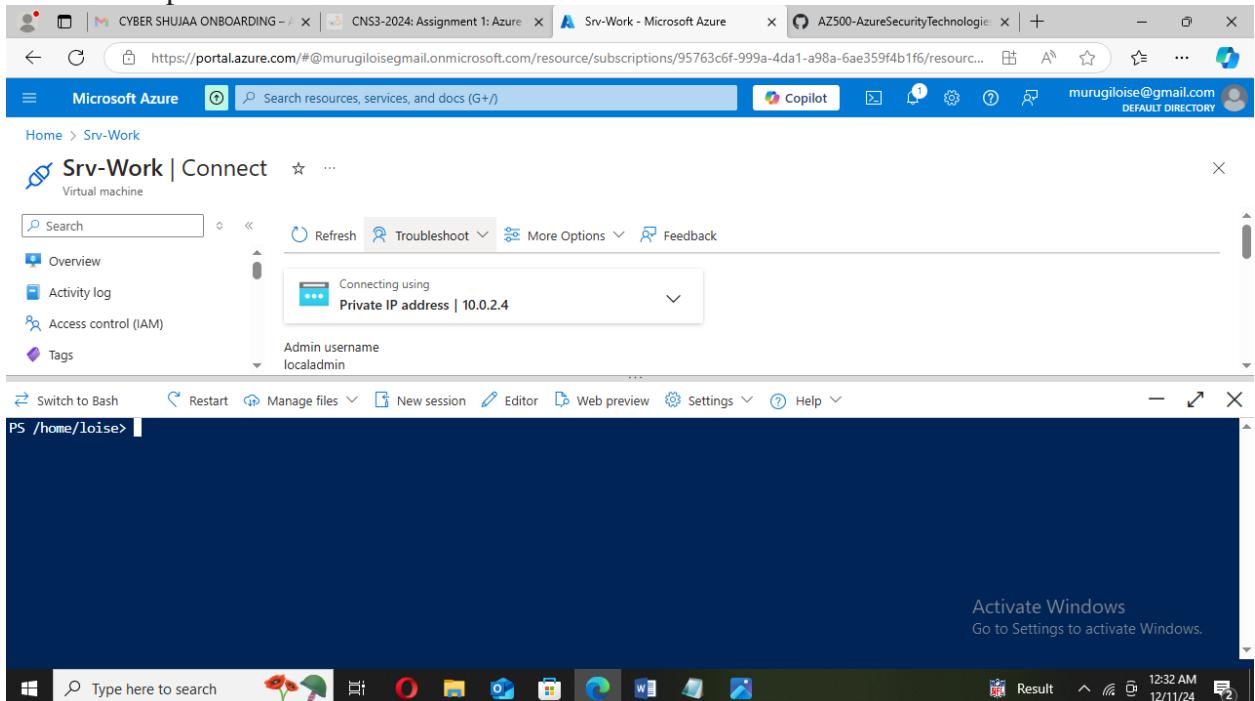
We have successfully configured and tested the Azure Firewall.

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**.

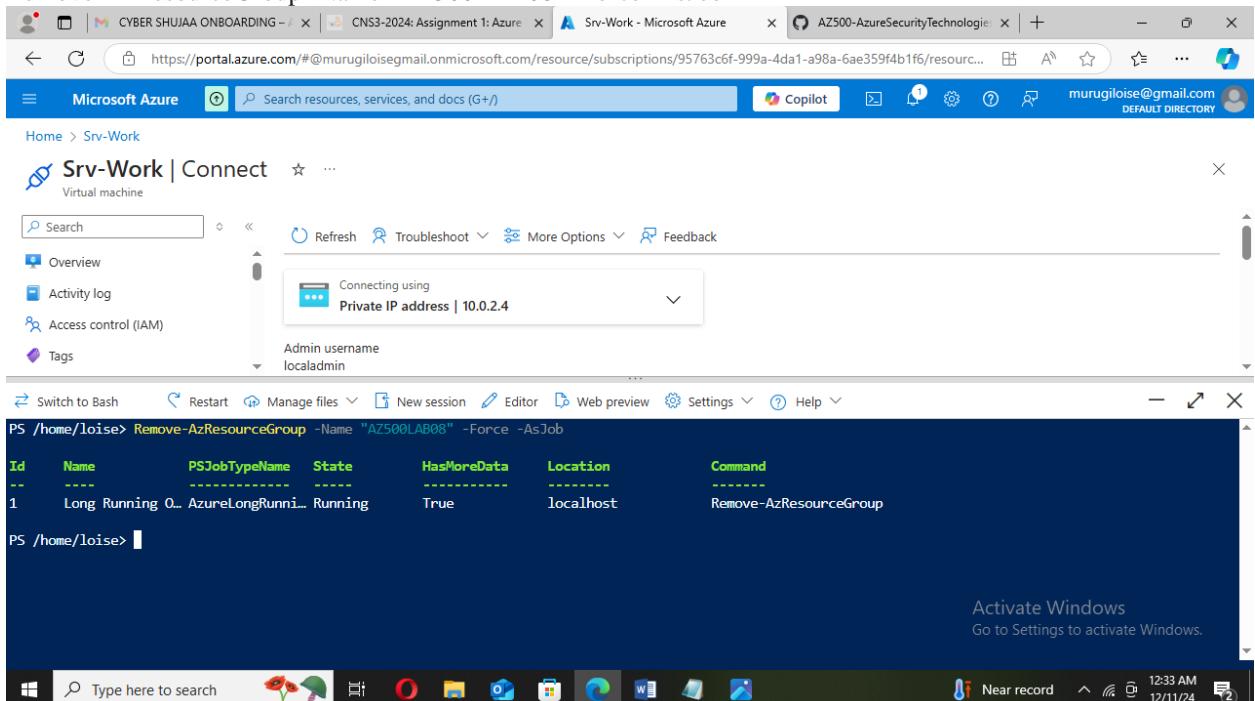
Week 8 Assignment 1: Azure Firewall

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.