Lab 08: Azure Firewall Report

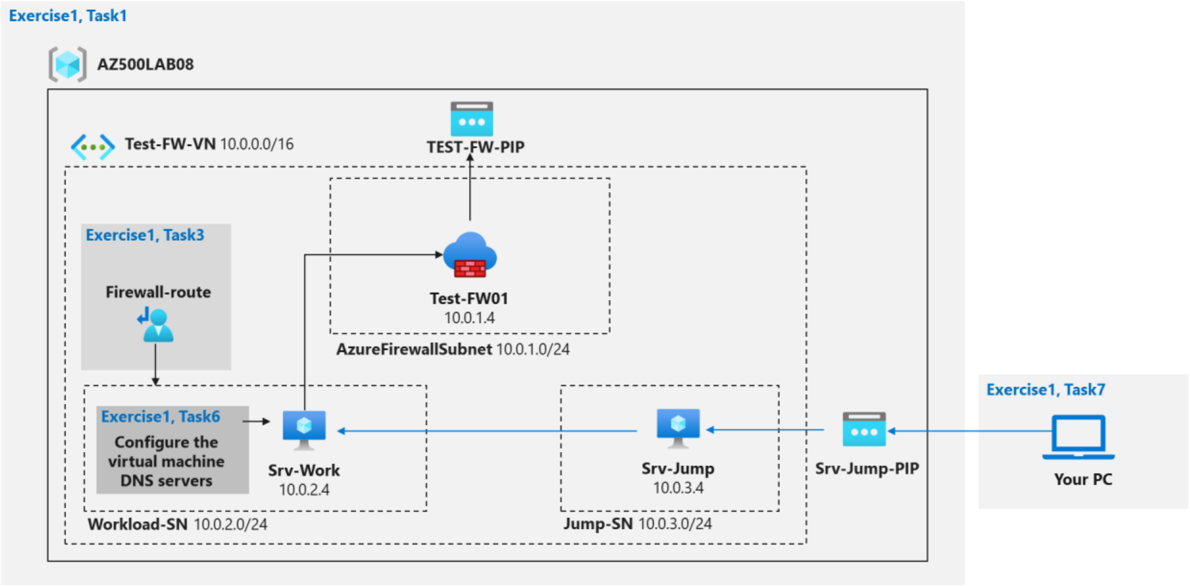
Yunis Mohamed

MICROSOFT AZURE LAB 08

Introduction

The Lab 08: Azure Firewall, provides an environment to learn and implement the powerful features of Azure Firewall and delve into implementing robust network security measures within the environment. The lab scenario consists of a virtual network with two subnets: a workload subnet and a jump host subnet, each containing virtual machines. My primary focus will be on ensuring secure outbound traffic from the workload subnet by configuring a custom route that directs all outbound traffic through Azure Firewall. Additionally, I will establish Firewall Application rules to limit outbound access exclusively to www.bing.com. To facilitate external DNS server lookups, I will set up Firewall Network rules. Throughout this hands-on lab, I will aim to gain practical experience in deploying, configuring, and managing Azure Firewall, empowering me to enhance cloud and network security.

Azure Firewall diagram

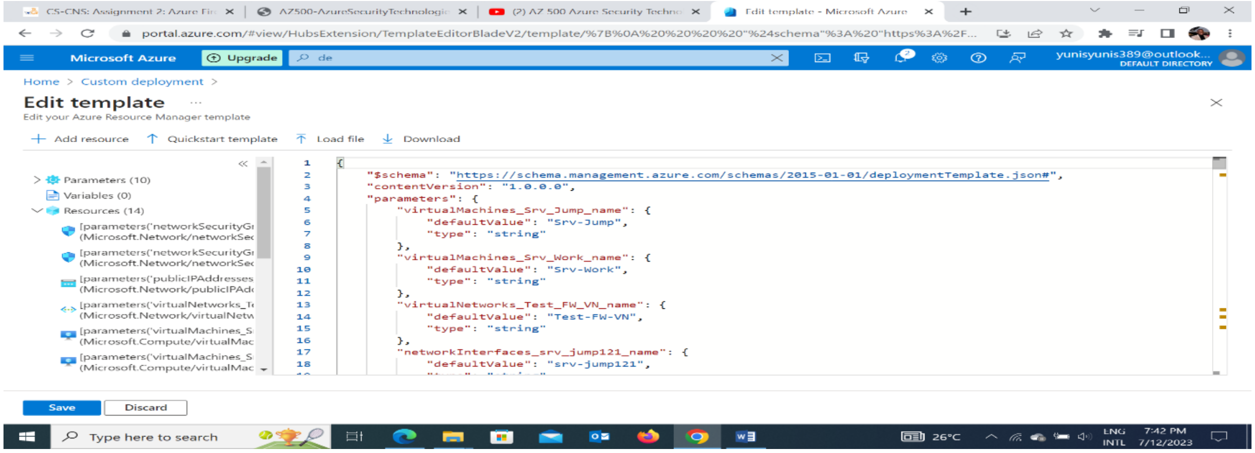


Exercise 1: Deploy and test an Azure Firewall

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

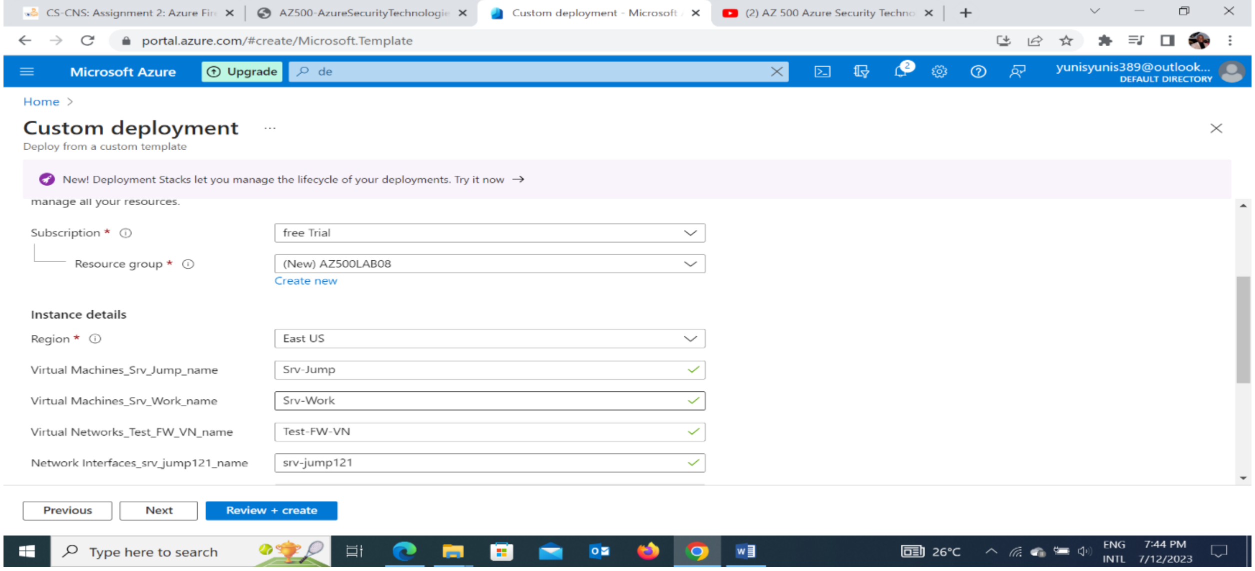
In this task, I will review and deploy the lab environment and create a virtual machine by using an ARM template.

1. Sign-in to the Azure portal **https://portal.azure.com/**.
2. In the Azure portal, in the Search resources, services, and docs text box at the top of the Azure portal page, type Deploy a custom template and press the Enter key.
3. On the Custom deployment blade, click the Build your own template in the editor option.
4. On the Edit template blade, click Load file, locate the \Allfiles\Labs\08\template.json file and click Open.
5. On the Edit template blade, click Save.



```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "virtualMachines_Srv_Jump_name": {
            "defaultValue": "Srv-Jump",
            "type": "string"
        },
        "virtualMachines_Srv_Work_name": {
            "defaultValue": "Srv-Work",
            "type": "string"
        },
        "virtualNetworks_Test_FW_VN_name": {
            "defaultValue": "Test-FW-VN",
            "type": "string"
        },
        "networkInterfaces_srv_jump121_name": {
            "defaultValue": "srv-jump121",
```

6. On the Custom deployment blade, ensure that the following settings are configured (leave any others with their default values):



Custom deployment

Deploy from a custom template

Subscription *	free Trial
Resource group *	(New) AZ500LAB08
Instance details	
Region *	East US
Virtual Machines_Srv_Jump_name	Srv-Jump
Virtual Machines_Srv_Work_name	Srv-Work
Virtual Networks_Test_FW_VN_name	Test-FW-VN
Network Interfaces_srv_jump121_name	srv-jump121

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

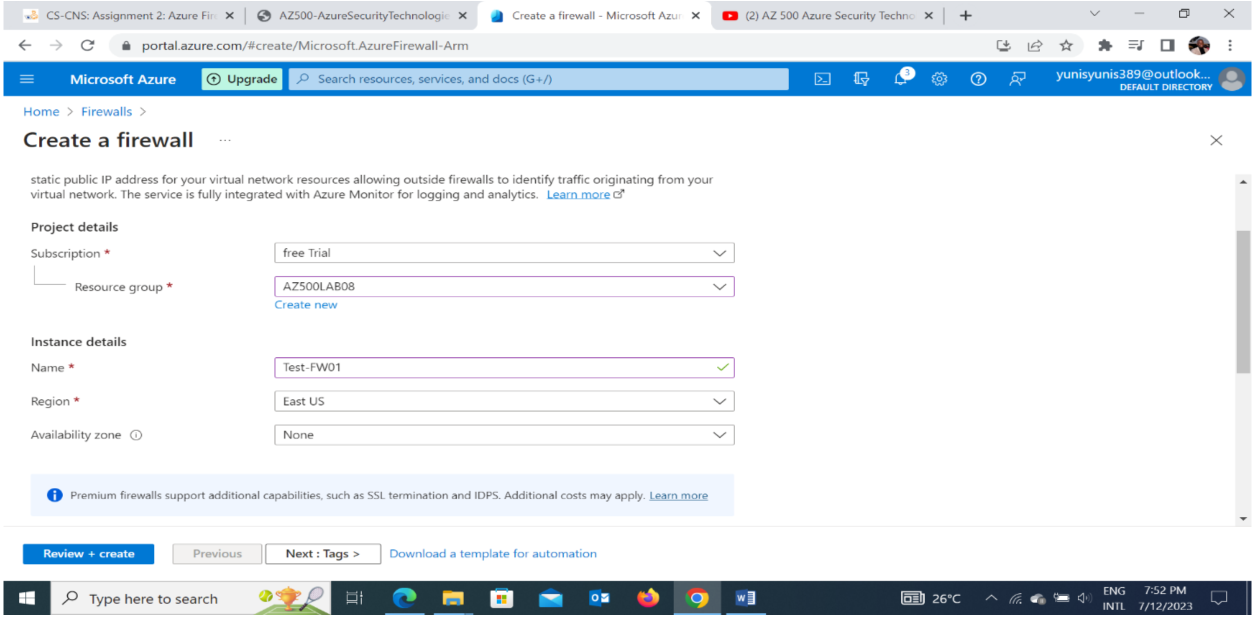
Task 2: Deploy the Azure firewall

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

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

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

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


CS-CNS: Assignment 2: Azure Fir
AZ500-AzureSecurityTechnologie
Create a firewall - Microsoft Azur
(2) AZ 500 Azure Security Techno
portal.azure.com/#create/Microsoft.AzureFirewall-Arm
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
yunisyunis389@outlook...
DEFAULT DIRECTORY
Home > Firewalls >

Create a firewall

static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. Learn more

Project details

Subscription * free Trial

Resource group * AZ500LAB08

Create new

Instance details

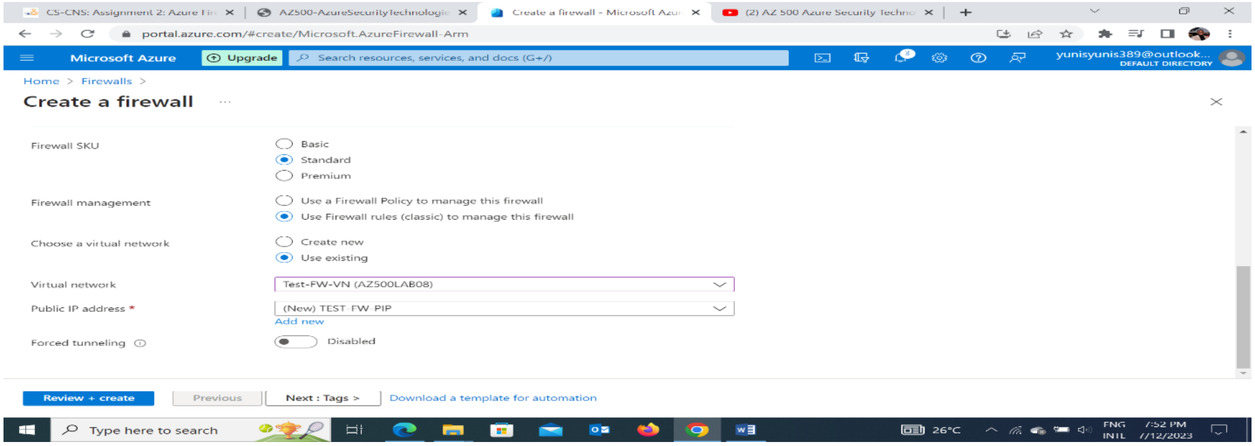
Name * Test-FW01

Region * East US

Availability zone None

Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. Learn more

Review + create
Previous
Next : Tags >
Download a template for automation
Type here to search
26°C
ENG INTL
7:52 PM
7/12/2023


CS-CNS: Assignment 2: Azure Fir
AZ500-AzureSecurityTechnologie
Create a firewall - Microsoft Azur
(2) AZ 500 Azure Security Techno
portal.azure.com/#create/Microsoft.AzureFirewall-Arm
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
yunisyunis389@outlook...
DEFAULT DIRECTORY
Home > Firewalls >

Create a firewall

Firewall SKU ○ Basic ● Standard ○ Premium

Firewall management ○ Use a Firewall Policy to manage this firewall ● Use Firewall rules (classic) to manage this firewall

Choose a virtual network ○ Create new ● Use existing

Virtual network Test-FW-VN (AZ500LAB08)

Public IP address * (New) TEST-FW-PIP

Add new

Forced tunneling Disabled

Review + create
Previous
Next : Tags >
Download a template for automation
Type here to search
26°C
ENG INTL
7:52 PM
7/12/2023

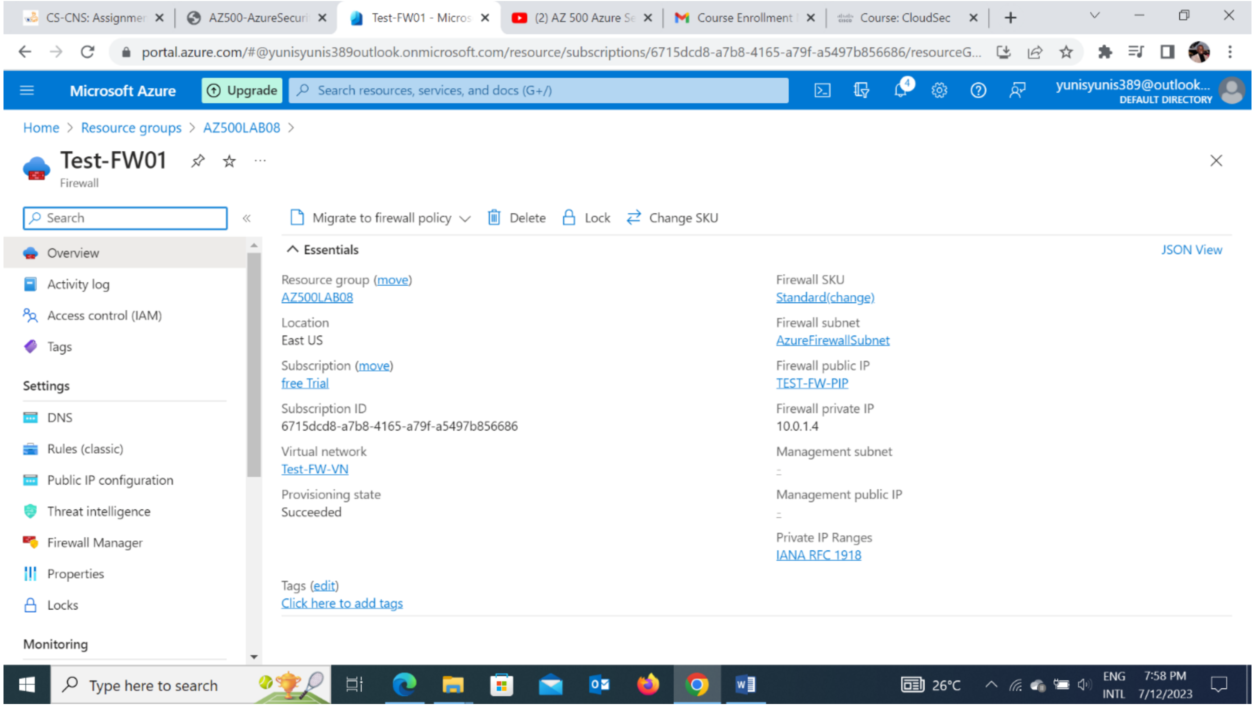
4. Click **Review + create** and then click **Create**.

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.

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.



Test-FW01

Firewall

Essentials

Resource group (move)
AZ500LAB08

Location
East US

Subscription (move)
free Trial

Subscription ID
6715dcd8-a7b8-4165-a79f-a5497b856686

Virtual network
Test-FW-VN

Provisioning state
Succeeded

Tags (edit)
Click here to add tags

Firewall SKU
Standard(change)

Firewall subnet
AzureFirewallSubnet

Firewall public IP
TEST-FW-PIP

Firewall private IP
10.0.1.4

Management subnet
-

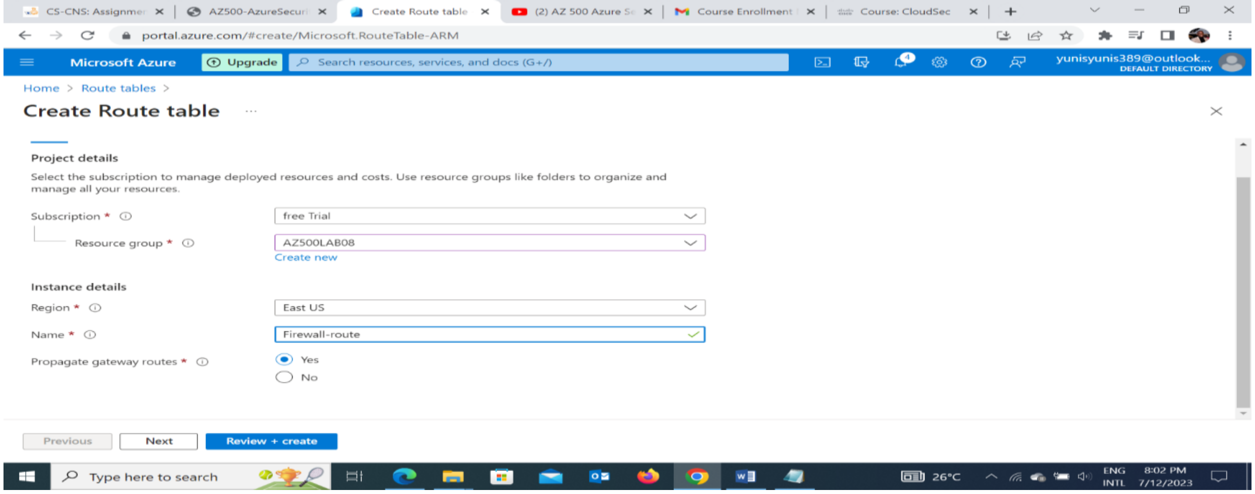
Management public IP
-

Private IP Ranges
IANA RFC 1918

Task 3: Create a default route

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

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



Create Route table

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * free Trial

Resource group * AZ500LAB08

Create new

Instance details

Region * East US

Name * Firewall-route

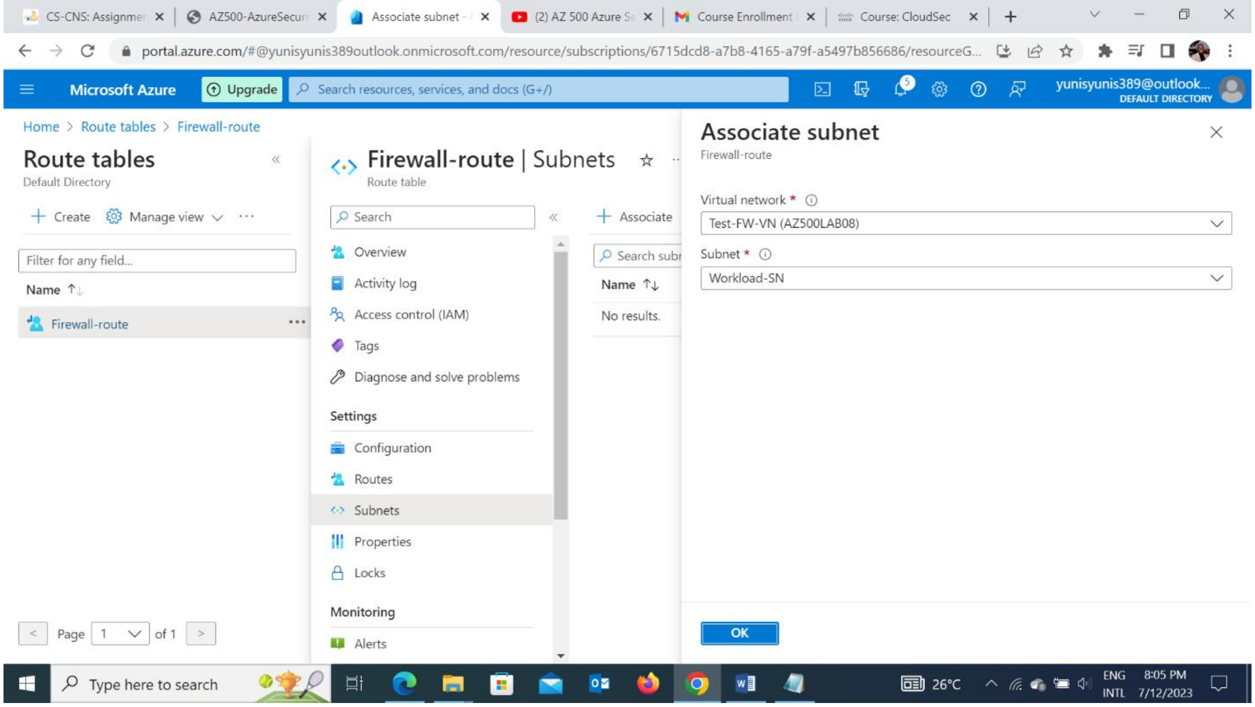
Propagate gateway routes * ● Yes ○ No

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

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

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

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



Associate subnet

Firewall-route

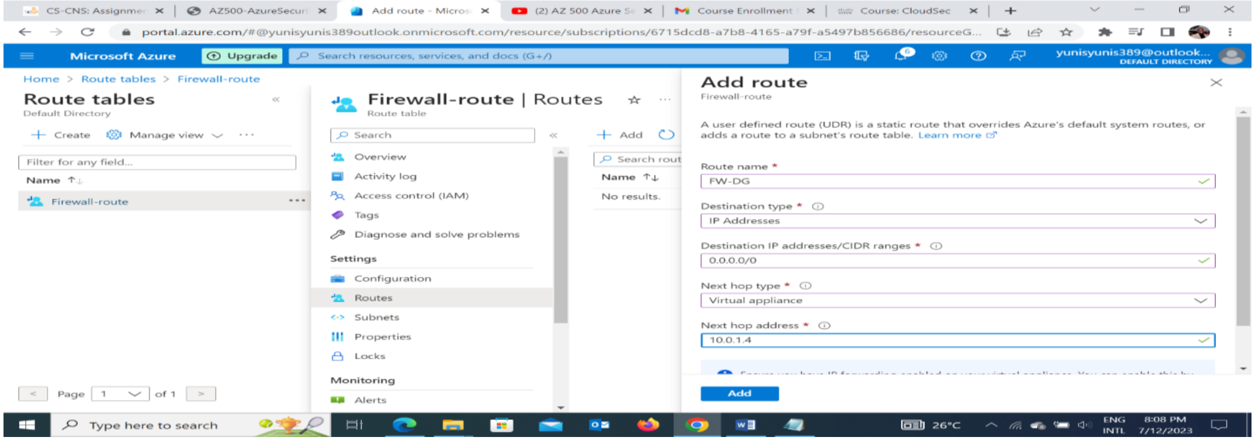
Virtual network * : Test-FW-VN (AZ500LAB08)

Subnet * : Workload-SN

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.

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



Add route

Firewall-route

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. Learn more

Route name * : FW-DG

Destination type * : IP Addresses

Destination IP addresses/CIDR ranges * : 0.0.0.0/0

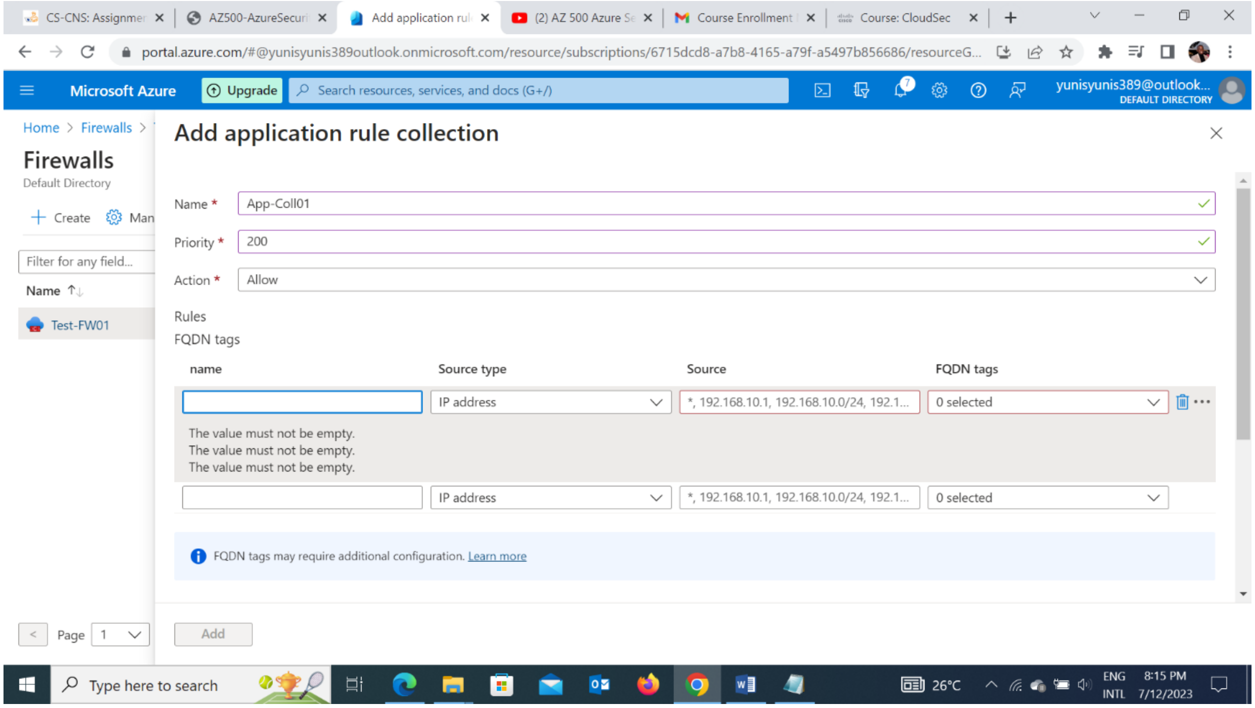
Next hop type * : Virtual appliance

Next hop address * : 10.0.1.4

Task 4: Configure an application rule

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

1. In the Azure portal, navigate back to the **Test-FW01** firewall.
2. On the **Test-FW01** blade, in the **Settings** section, click **Rules (classic)**.
3. On the **Test-FW01 | Rules (classic)** blade, click the **Application rule collection** tab, and then click **+ Add application rule collection**.
4. On the **Add application rule collection** blade, specify the following settings (leave others with their default values):



Add application rule collection

Name * App-Coll01

Priority * 200

Action * Allow

Rules

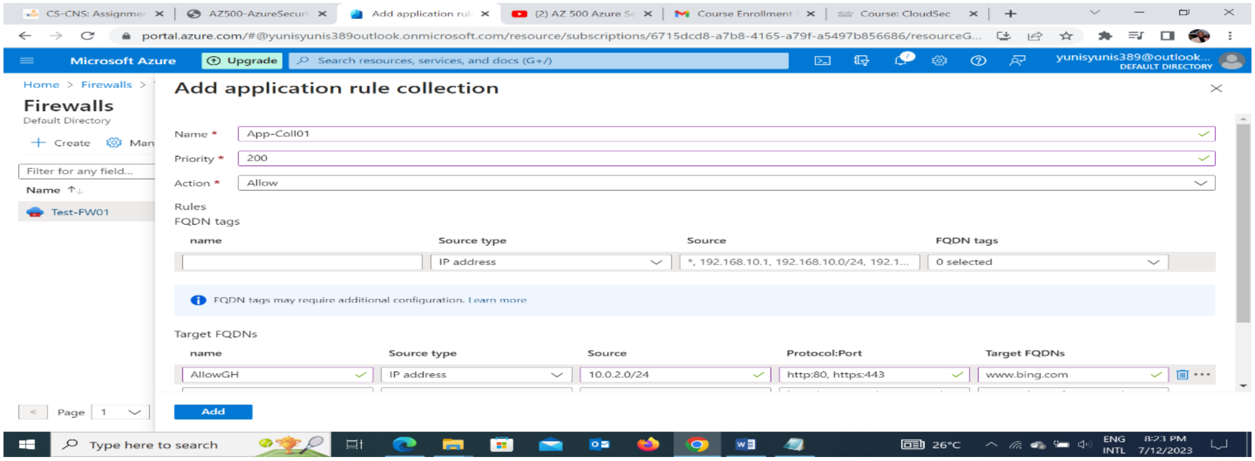
FQDN tags

name	Source type	Source	FQDN tags
	IP address	*, 192.168.10.1, 192.168.10.0/24, 192.1...	0 selected
	IP address	*, 192.168.10.1, 192.168.10.0/24, 192.1...	0 selected

The value must not be empty.
The value must not be empty.
The value must not be empty.

FQDN tags may require additional configuration. Learn more

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):



Add application rule collection

Name * App-Coll01

Priority * 200

Action * Allow

Rules

FQDN tags

name	Source type	Source	FQDN tags
	IP address	*, 192.168.10.1, 192.168.10.0/24, 192.1...	0 selected

FQDN tags may require additional configuration. Learn more

Target FQDNs

name	Source type	Source	Protocol:Port	Target FQDNs
AllowGH	IP address	10.0.2.0/24	http:80, https:443	www.bing.com

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

Task 5: Configure a network rule

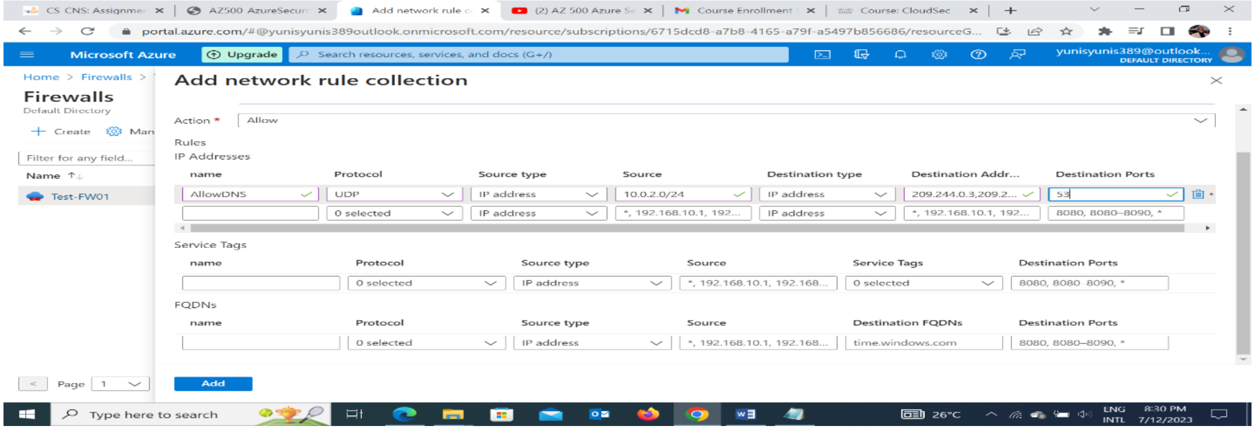
In this task, I will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

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):

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):



Add network rule collection

Action * Allow

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addr...	Destination Ports
AllowDNS	UDP	IP address	10.0.2.0/24	IP address	209.244.0.3,209.2...	53
	0 selected	IP address	*, 192.168.10.1, 192...	IP address	*, 192.168.10.1, 192...	8080, 8080–8090, *

Service Tags

name	Protocol	Source type	Source	Service Tags	Destination Ports
	0 selected	IP address	*, 192.168.10.1, 192.168...	0 selected	8080, 8080 8090, *

FQDNs

name	Protocol	Source type	Source	Destination FQDNs	Destination Ports
	0 selected	IP address	*, 192.168.10.1, 192.168...	time.windows.com	8080, 8080–8090, *

Add

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

Task 6: Configure the virtual machine DNS servers

In this task, I will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

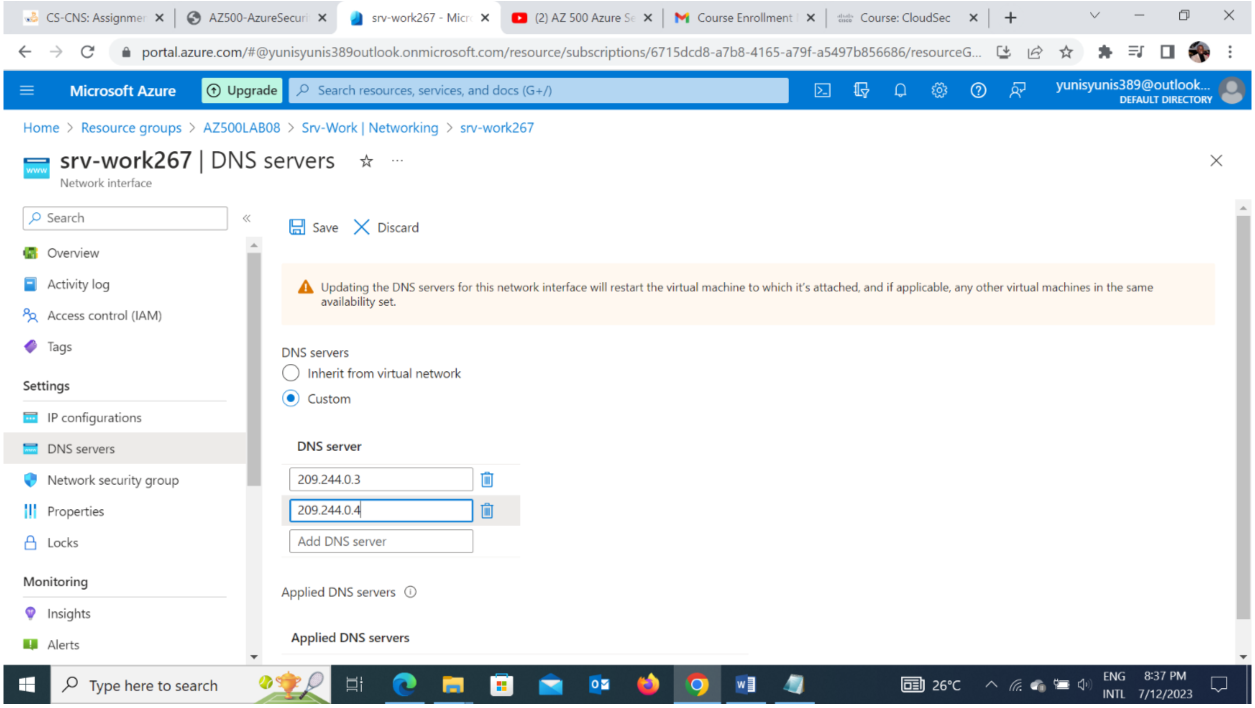
1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

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

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

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.



srv-work267 | DNS servers
Network interface

⚠ Updating the DNS servers for this network interface will 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

Applied DNS servers ⓘ

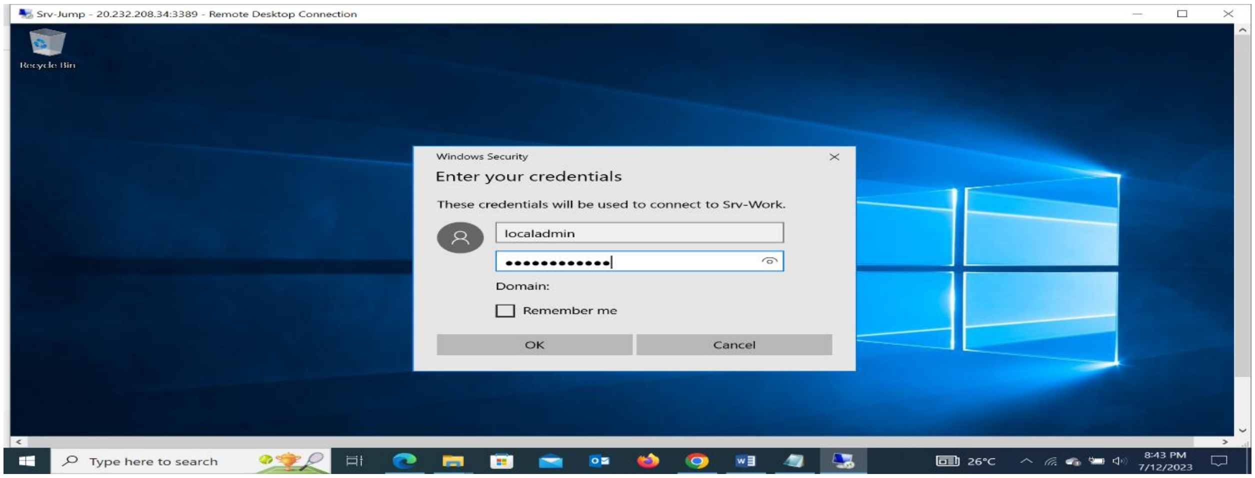
Applied DNS servers

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

Task 7: Test the firewall

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

1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.
2. On the **AZ500LAB08** blade, in the list of resources, click the **Srv-Jump** virtual machine.
3. On the **Srv-Jump** blade, click **Connect** and, in the drop down menu, click **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:
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**.
6. When prompted to authenticate, provide the following credentials:



Srv-Jump - 20.232.208.34:3389 - Remote Desktop Connection

Windows Security

Enter your credentials

These credentials will be used to connect to Srv-Work.

localadmin

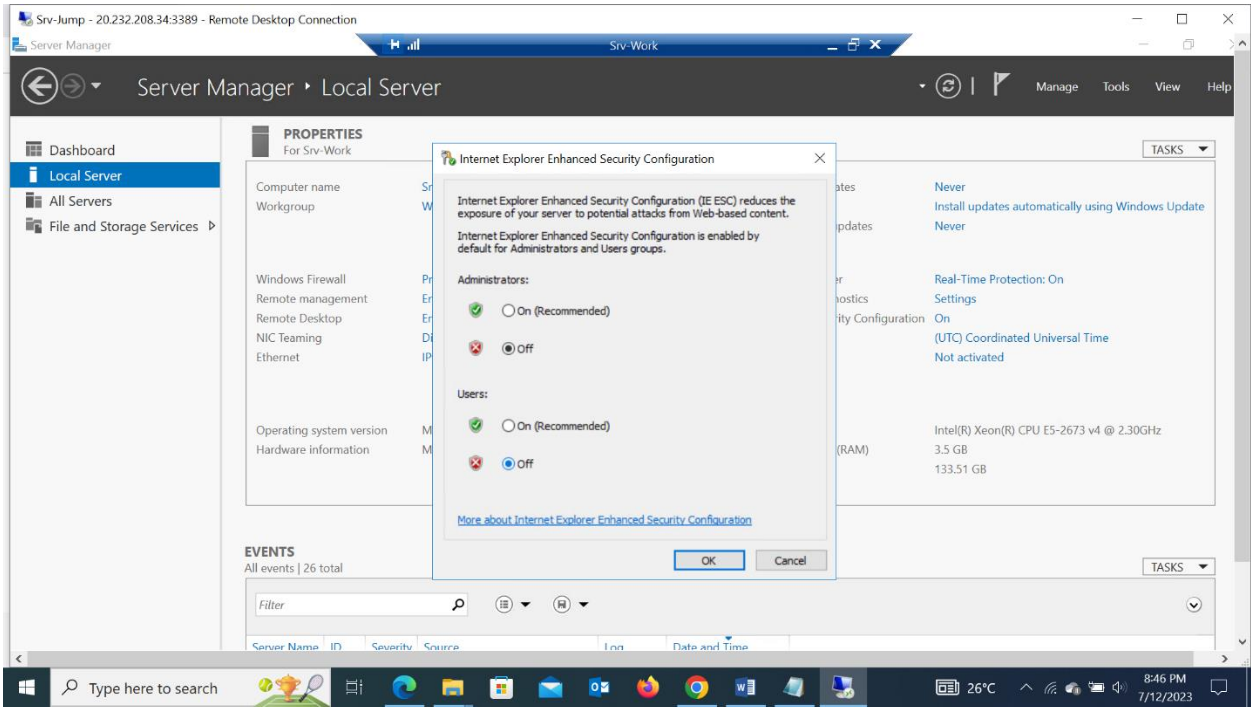
•••••••••••••

Domain:

□ Remember me

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.



Srv-Jump - 20.232.208.34:3389 - Remote Desktop Connection

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

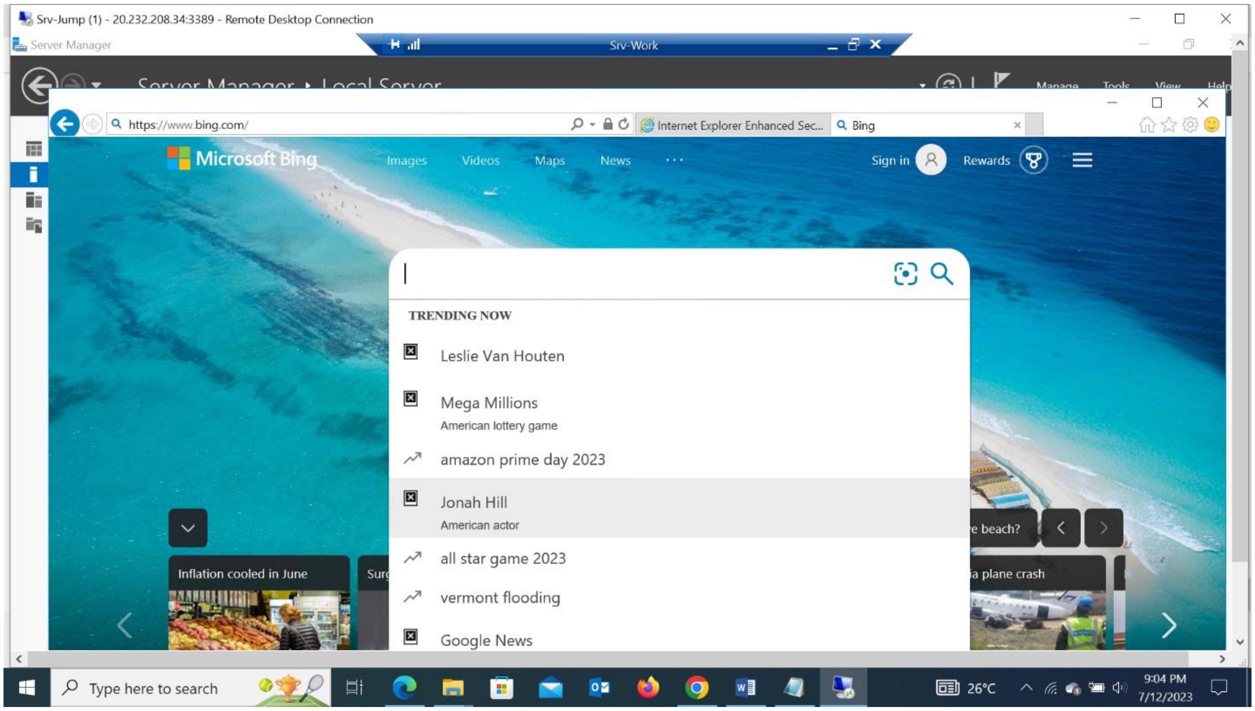
Users:

○ On (Recommended)

● Off

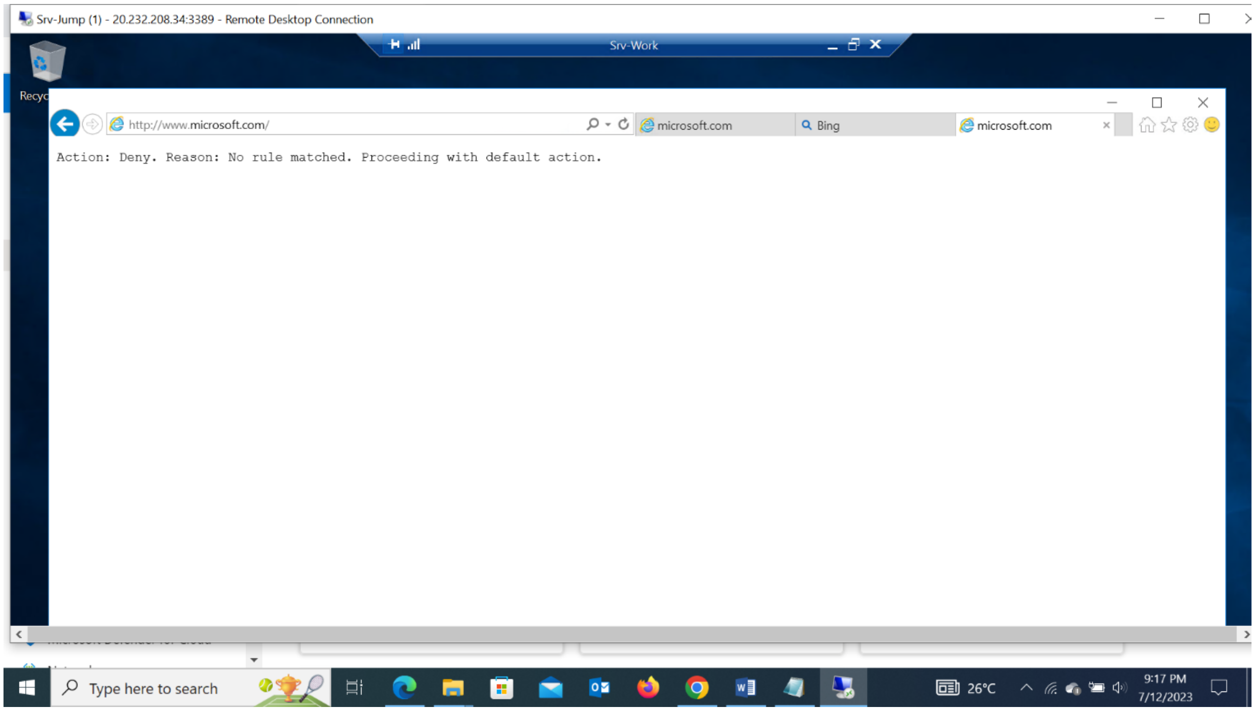
More about Internet Explorer Enhanced Security Configuration

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 access.

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


Srv-Jump (1) - 20.232.208.34:3389 - Remote Desktop Connection
Srv-Work
Recyc
http://www.microsoft.com/
microsoft.com
Bing
microsoft.com
Type here to search
26°C
9:17 PM
7/12/2023

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

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

11. Terminate both Remote Desktop sessions.

Conclusion

In conclusion, Lab 08: Azure Firewall has provided me with a deep understanding of the power and importance of implementing robust network security measures within our Azure environment. Throughout this lab, I explored the functionalities and capabilities of Azure Firewall, focusing on securing outbound traffic from a workload subnet. By configuring custom routes, Firewall Application rules, and Firewall Network rules, I have gained practical experience in directing and filtering network traffic to ensure secure and controlled access. This lab has highlighted the significance of Azure Firewall in protecting our resources against unauthorized access and potential threats. By deploying, configuring, and managing Azure Firewall, I have acquired the skills and knowledge necessary to strengthen our network security posture and safeguard cloud environment. This lab has empowered me to take control of our network security and implement effective measures to ensure the confidentiality, integrity, and availability of our resources.