WEEK 8: Assignment 2: Azure Firewall

Report by Hapidael Mumbi

CS-CNS06-24062

Introduction

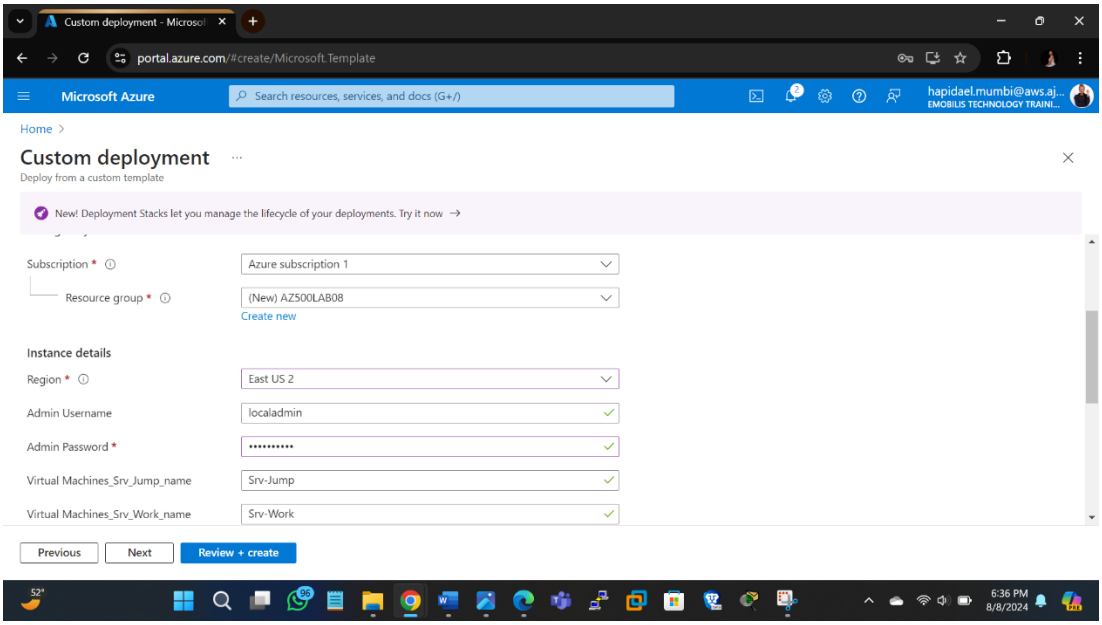
In this lab, we will explore the deployment and configuration of Azure Firewall, a critical component in enhancing network security within Azure environments. Azure Firewall is a managed, cloud-based network security service that helps protect your virtual networks by controlling both inbound and outbound traffic. By setting up a virtual network with subnets, virtual machines, and specific firewall rules, we will learn how to manage and secure traffic effectively. This lab focuses on using Azure Firewall to allow or restrict access to specific applications and services, ensuring that our network traffic is tightly controlled.

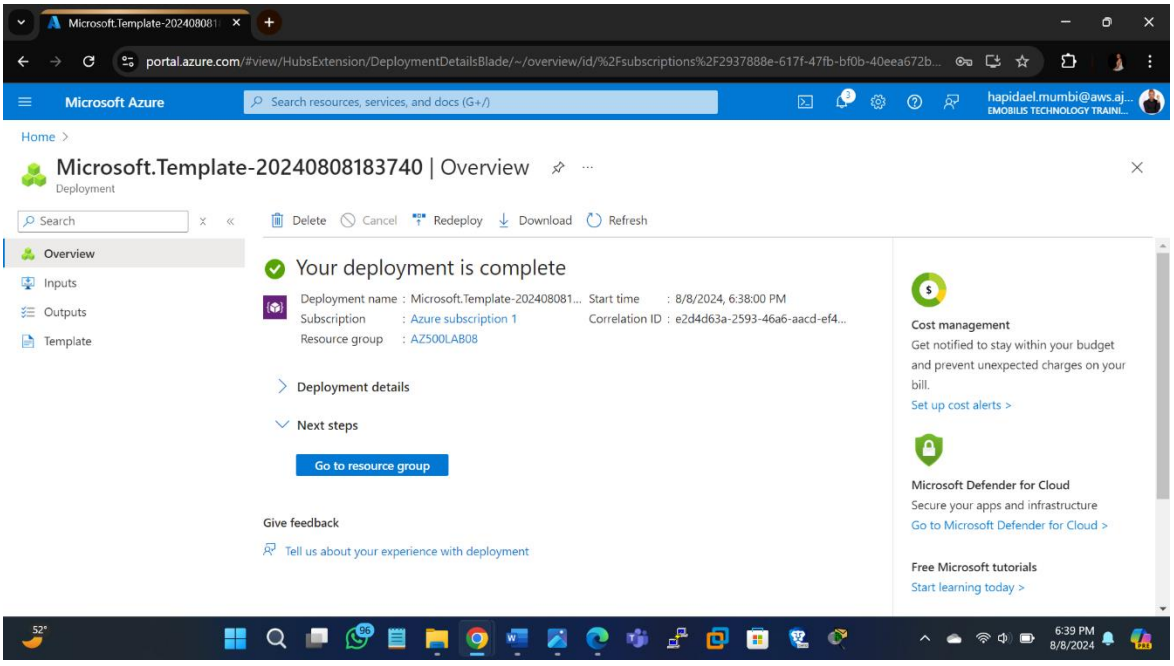
Objectives

1. Deploy a Virtual Network and Subnets: Create a virtual network with two subnets—one for the workload and one for the jump host—where we will deploy virtual machines.
2. Deploy an Azure Firewall: Install Azure Firewall into the virtual network, which will act as a security barrier for network traffic.
3. Create a Default Route: Configure a custom route that forces all outbound traffic from the workload subnet to pass through the Azure Firewall.
4. Configure Firewall Rules: Set up application and network rules in Azure Firewall to manage outbound traffic. Specifically, we will allow access to certain websites and DNS servers while blocking others.
5. Test the Firewall Configuration: Validate the configuration by testing access to allowed and blocked websites from the deployed virtual machines.

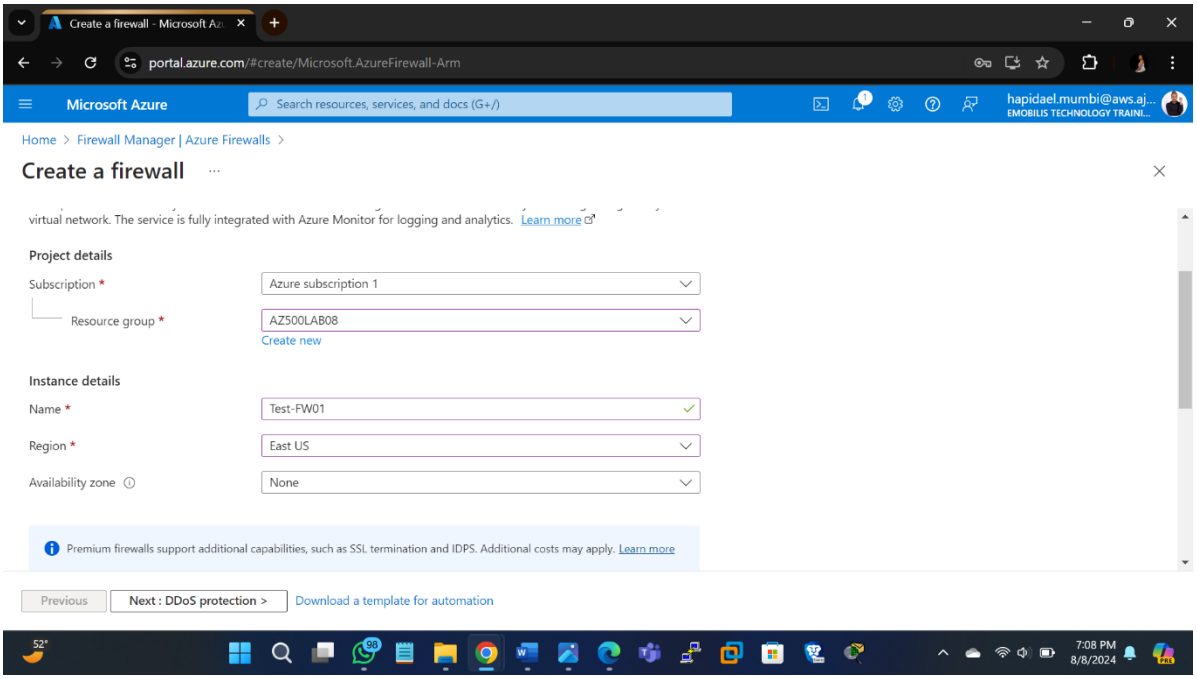
Step 1

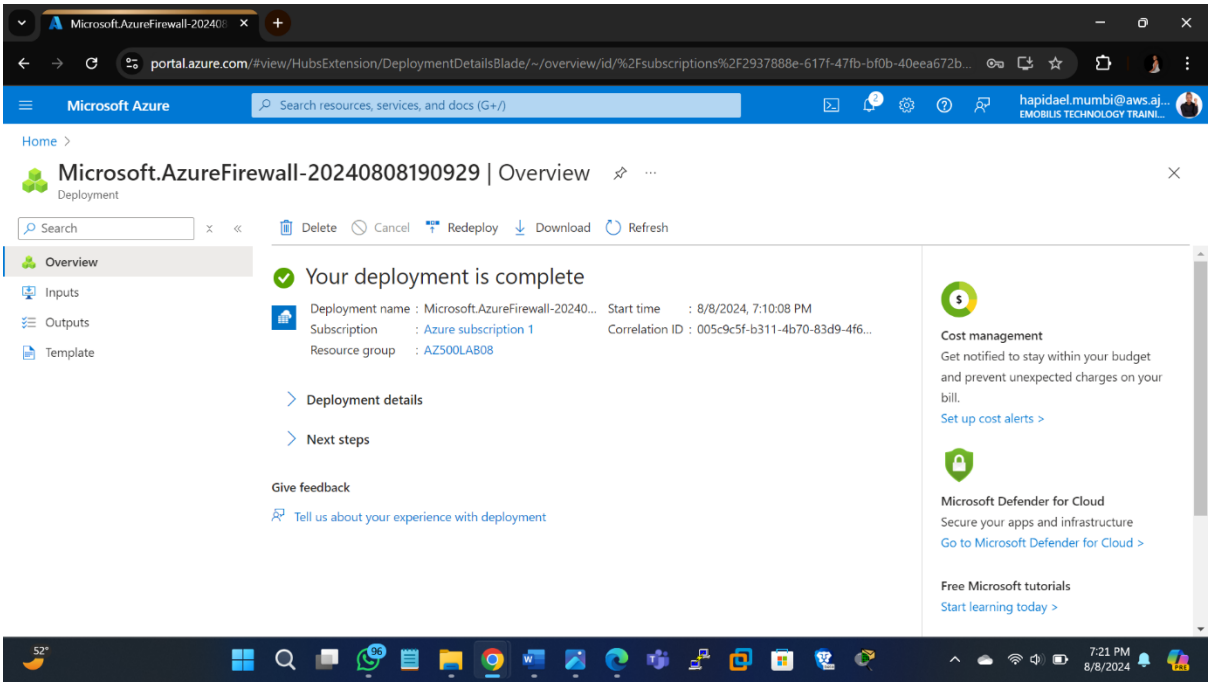
Deploy the Lab Environment: Using an ARM template, you will deploy a virtual network with two subnets and virtual machines, setting the stage for firewall configuration.



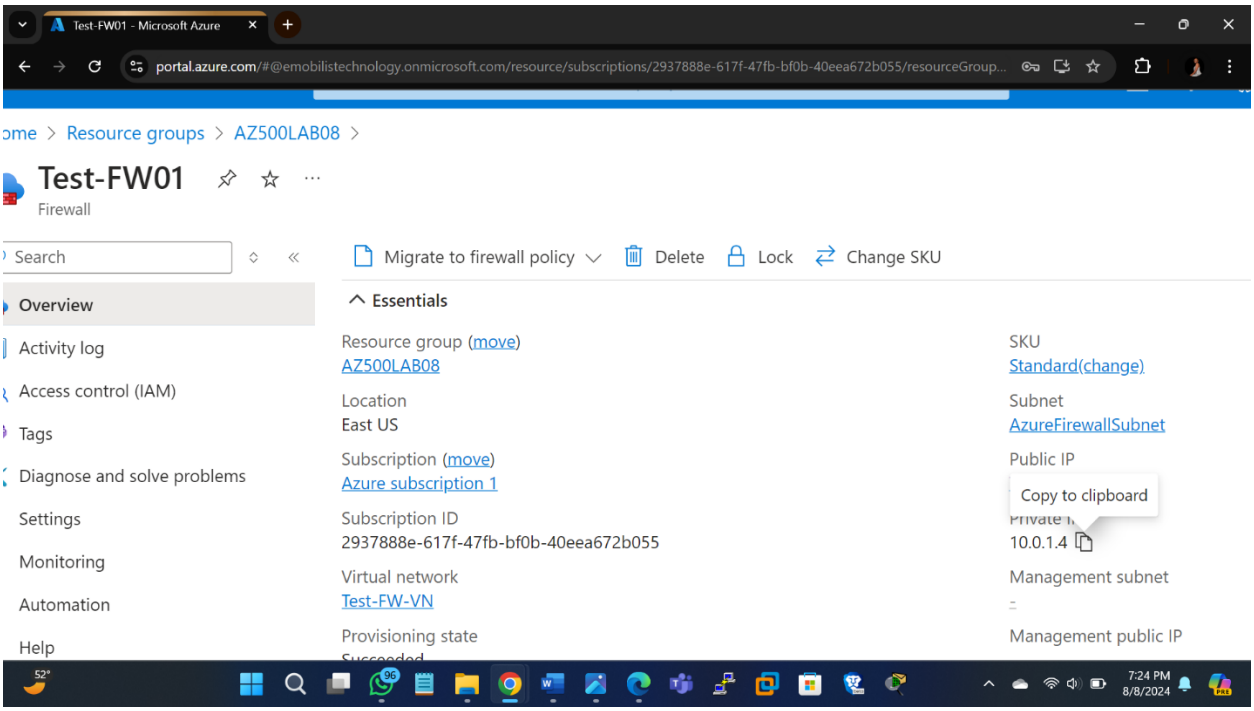


The next step is creating a firewall

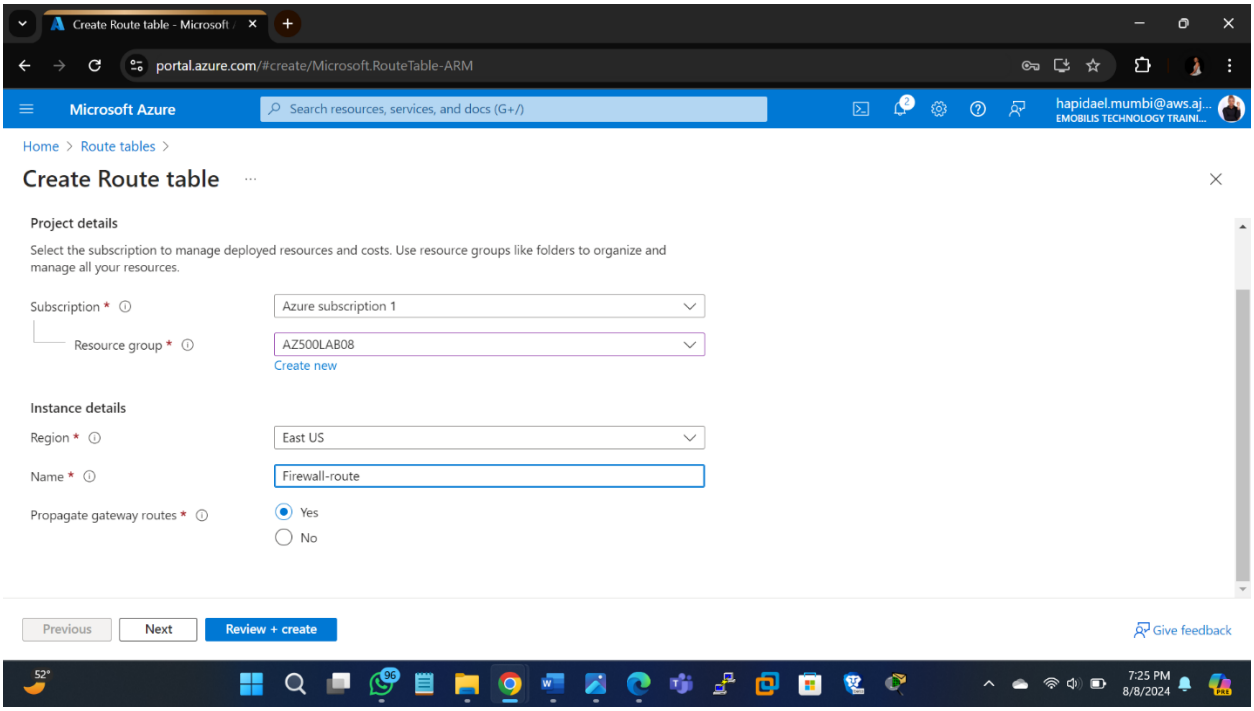


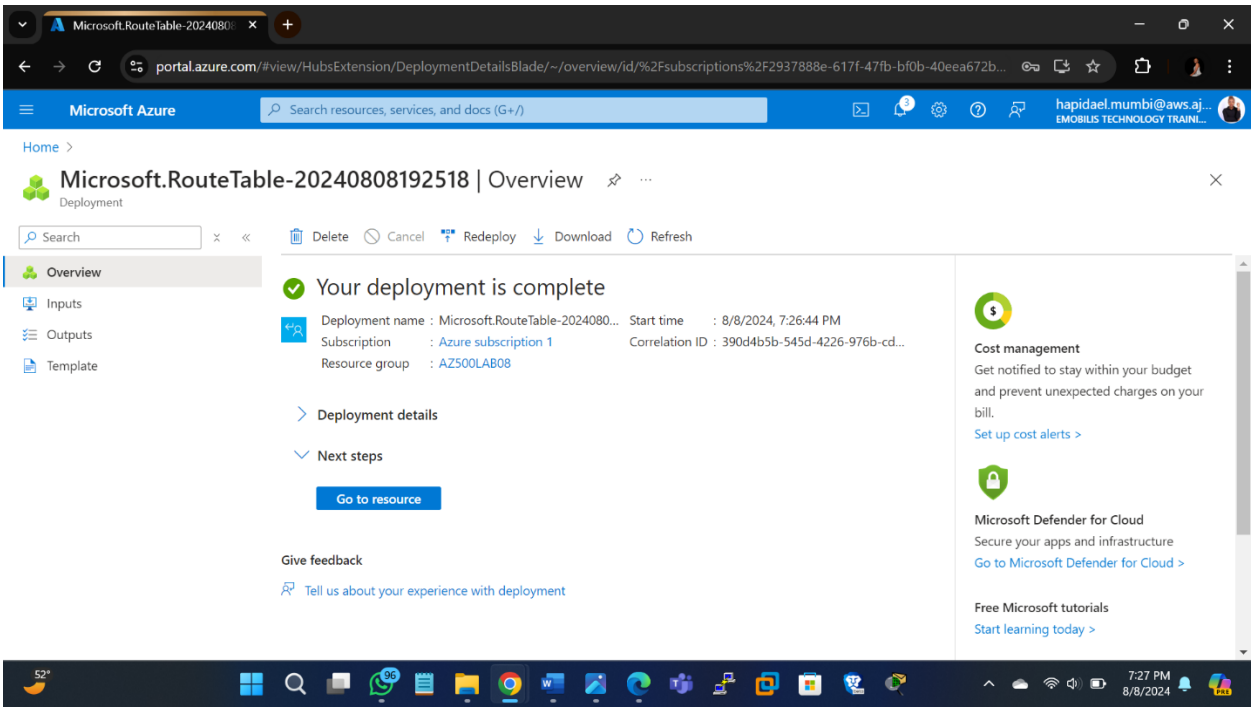


Below you can see the private ip address that was assigned to the firewall

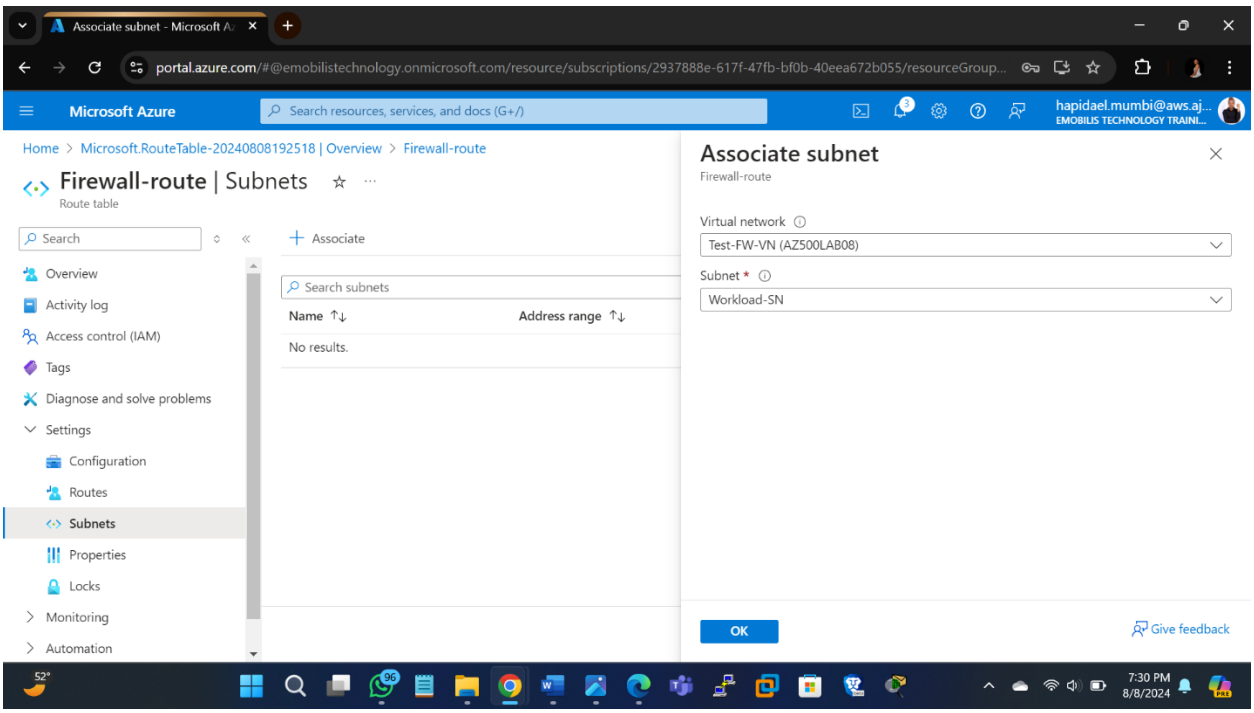


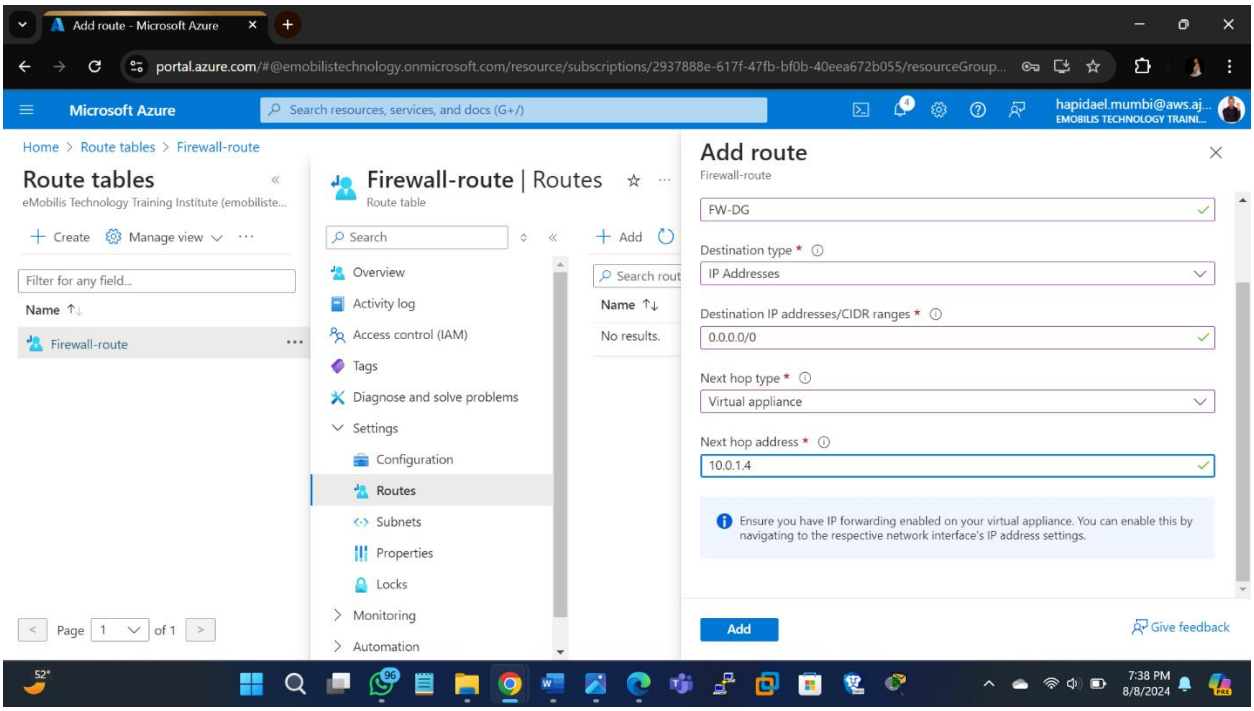
Here I will create a default route for the **Workload-SN** subnet. This route will configure outbound traffic through the firewall.





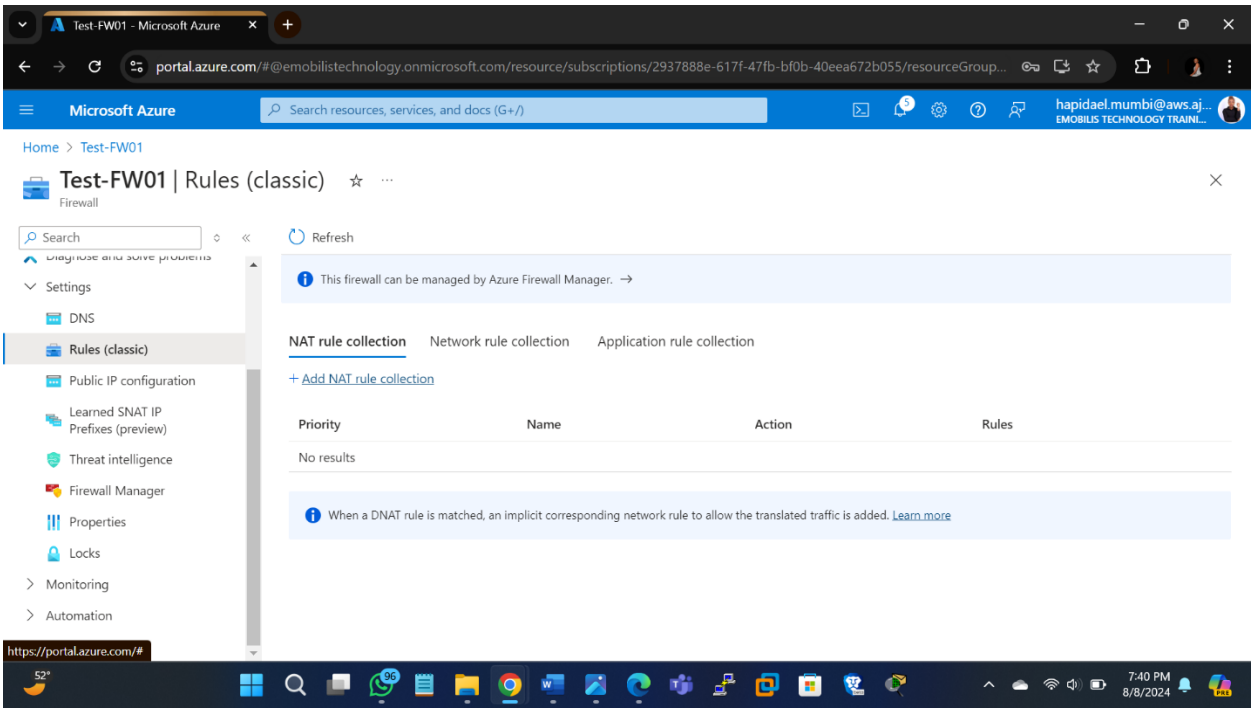
Associating the firewall to the virtual network subnet



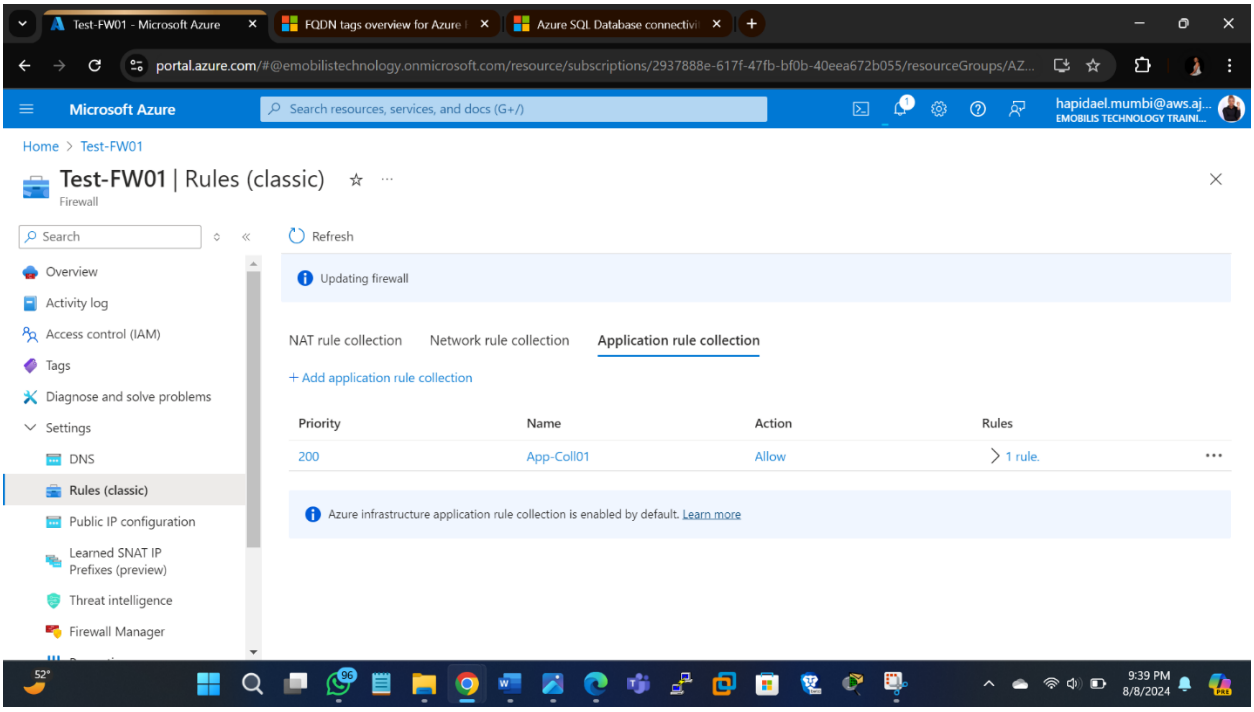


Task 4: Configure an application rule

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



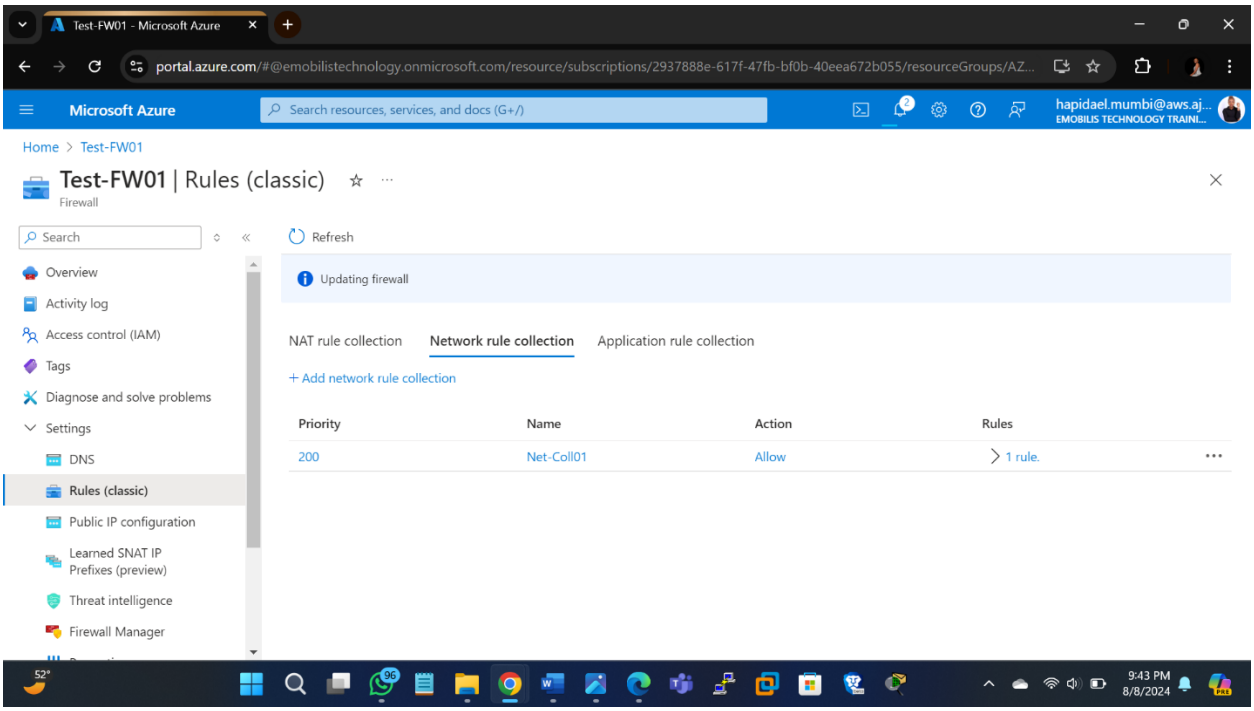
Adding an application rule



Task 5: Configure a network rule

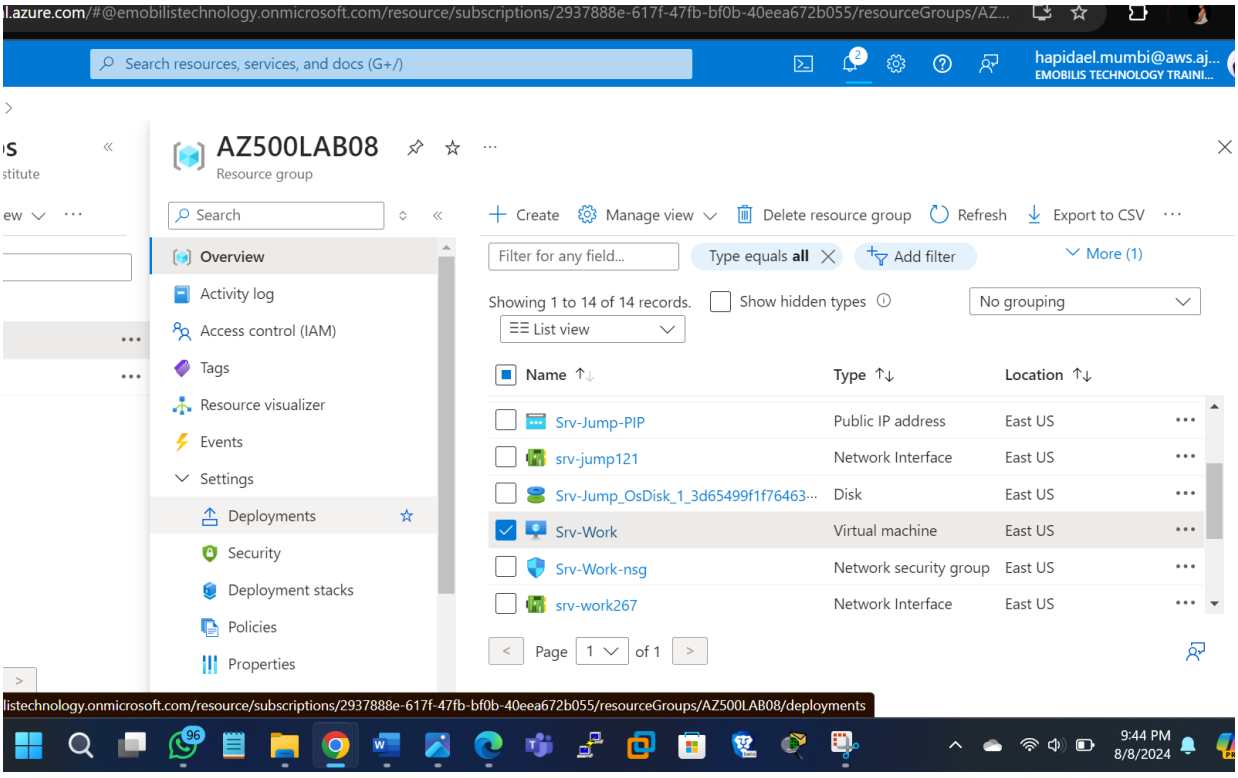
In this task, I will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

I added a network rule collection

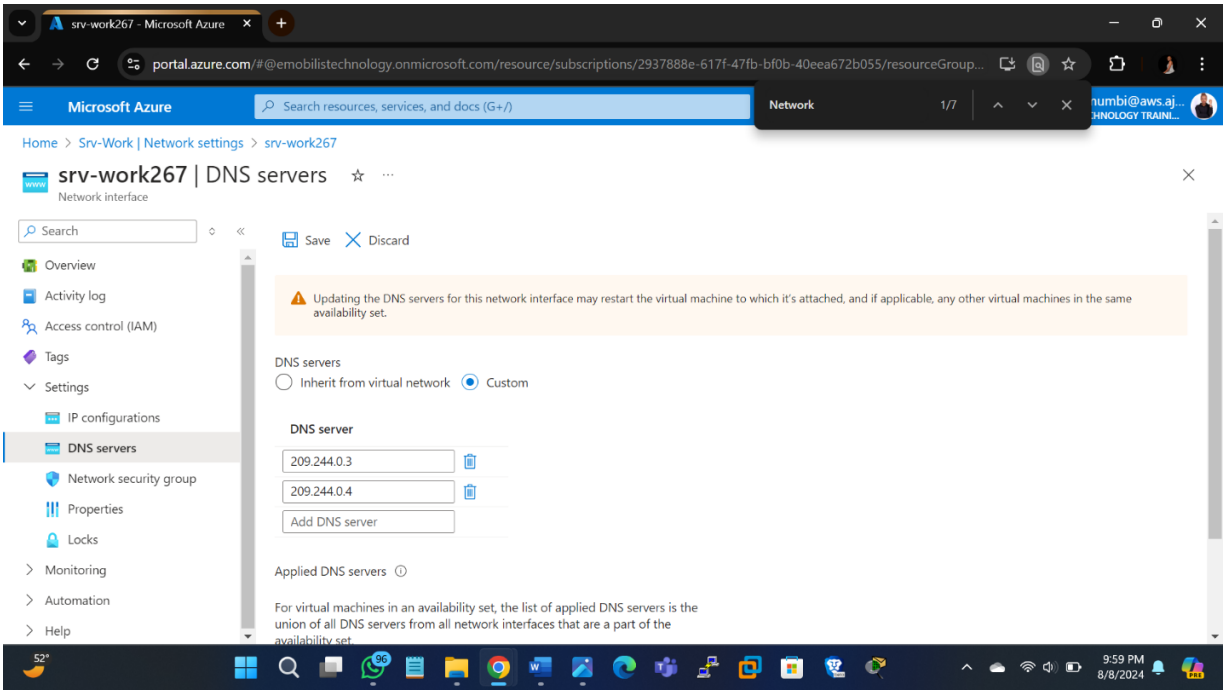


Task 6: Configure the virtual machine DNS servers

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

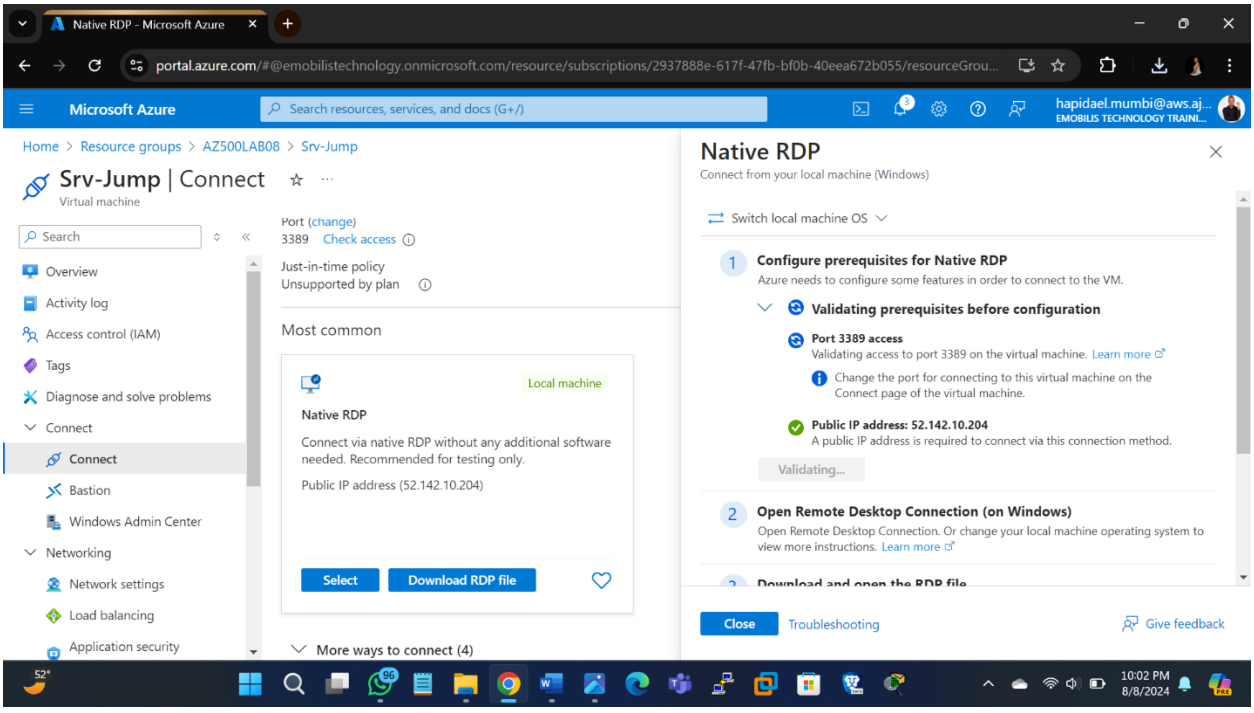


Adding the DNS servers **209.244.0.3** and **209.244.0.4**,

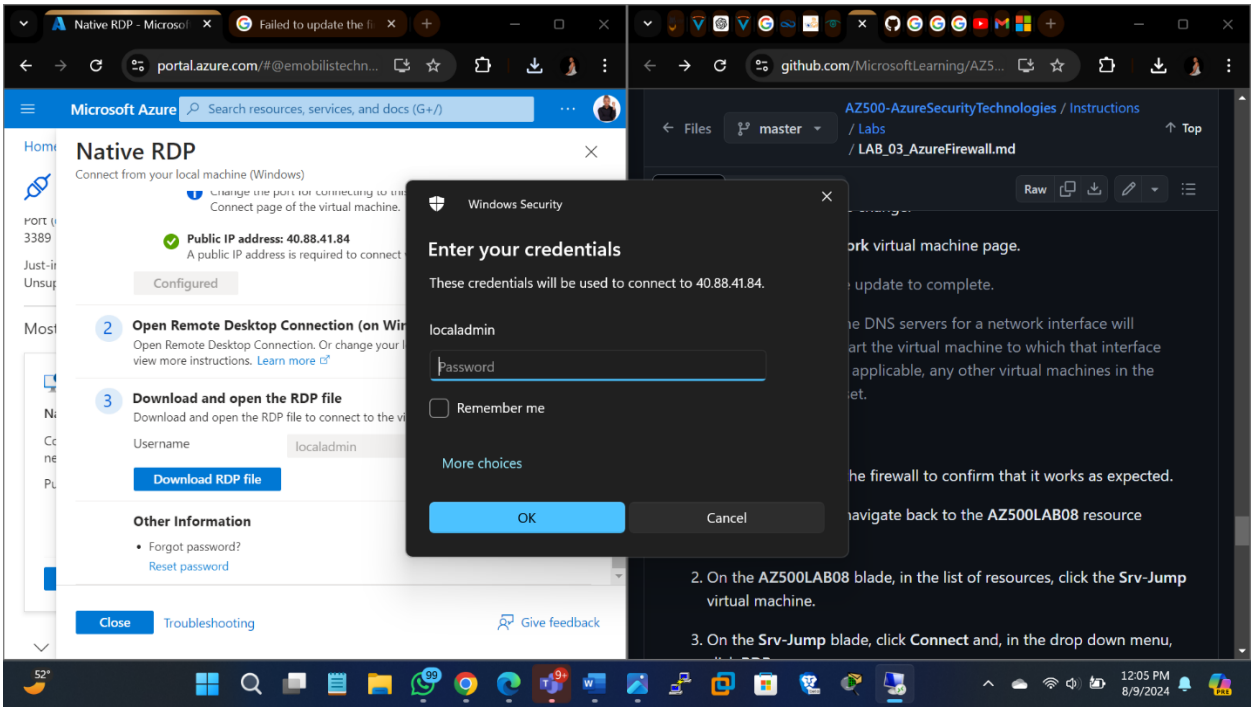


Task 7: Test the firewall

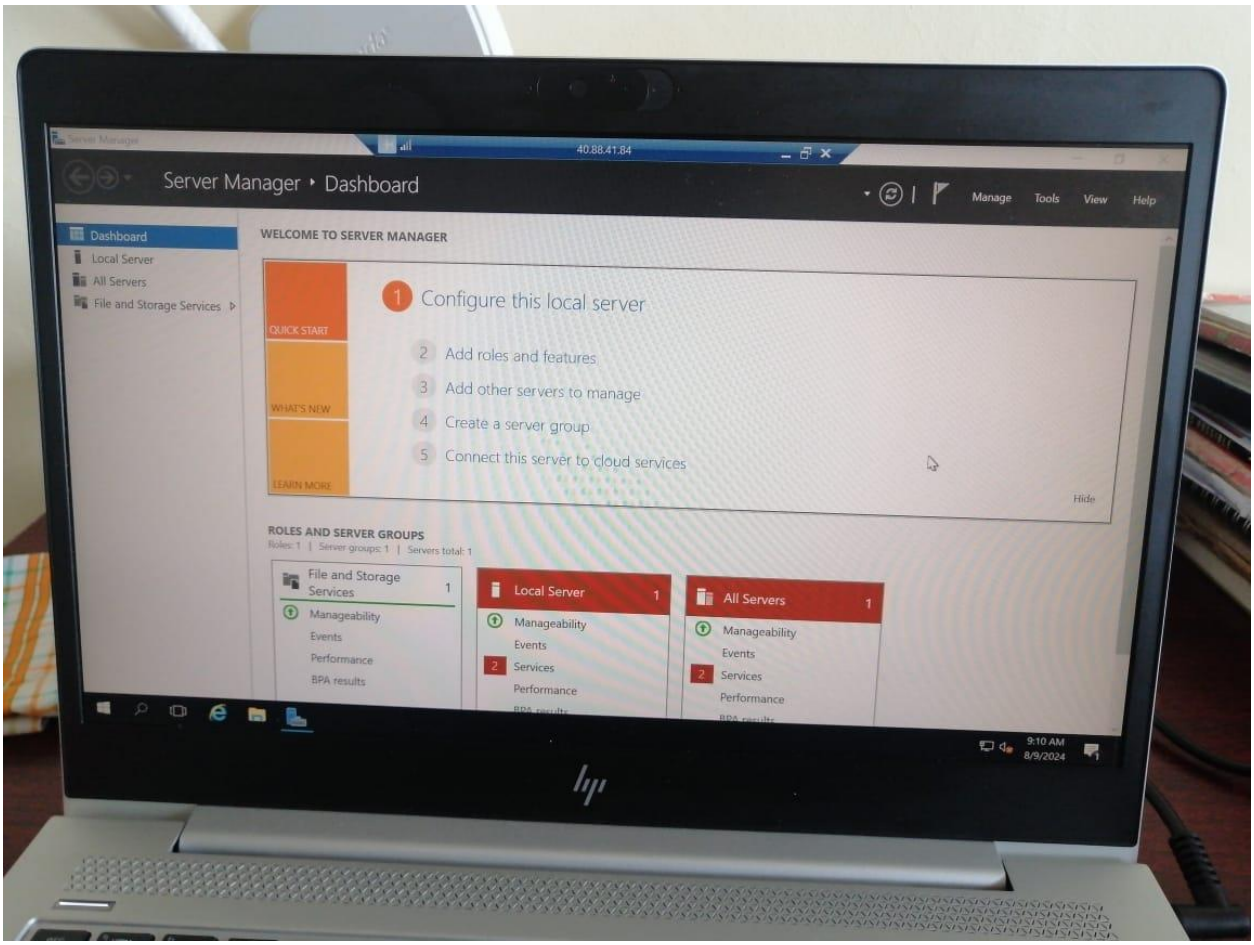
In this task, I will test the firewall to confirm that it works as expected.

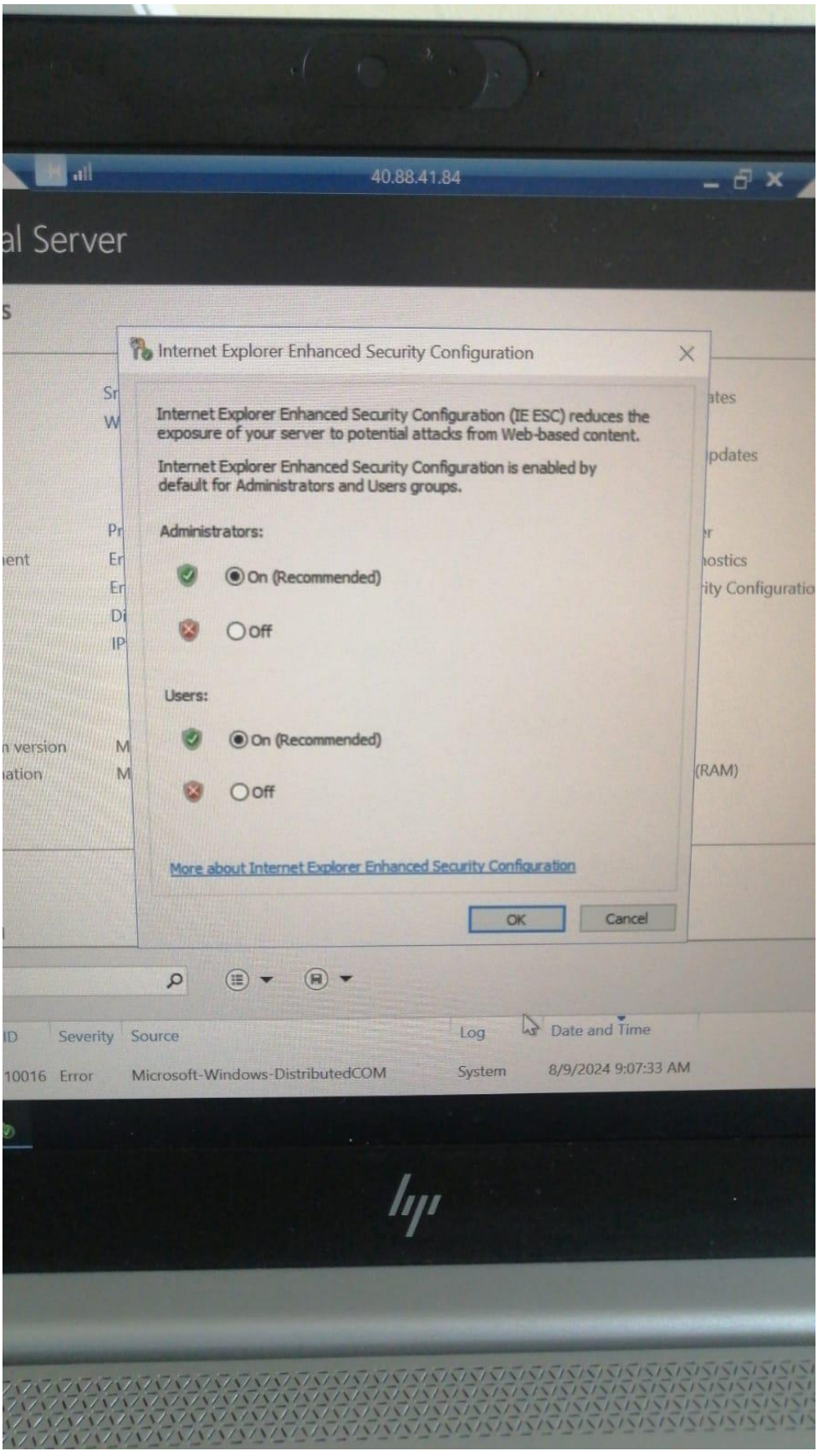


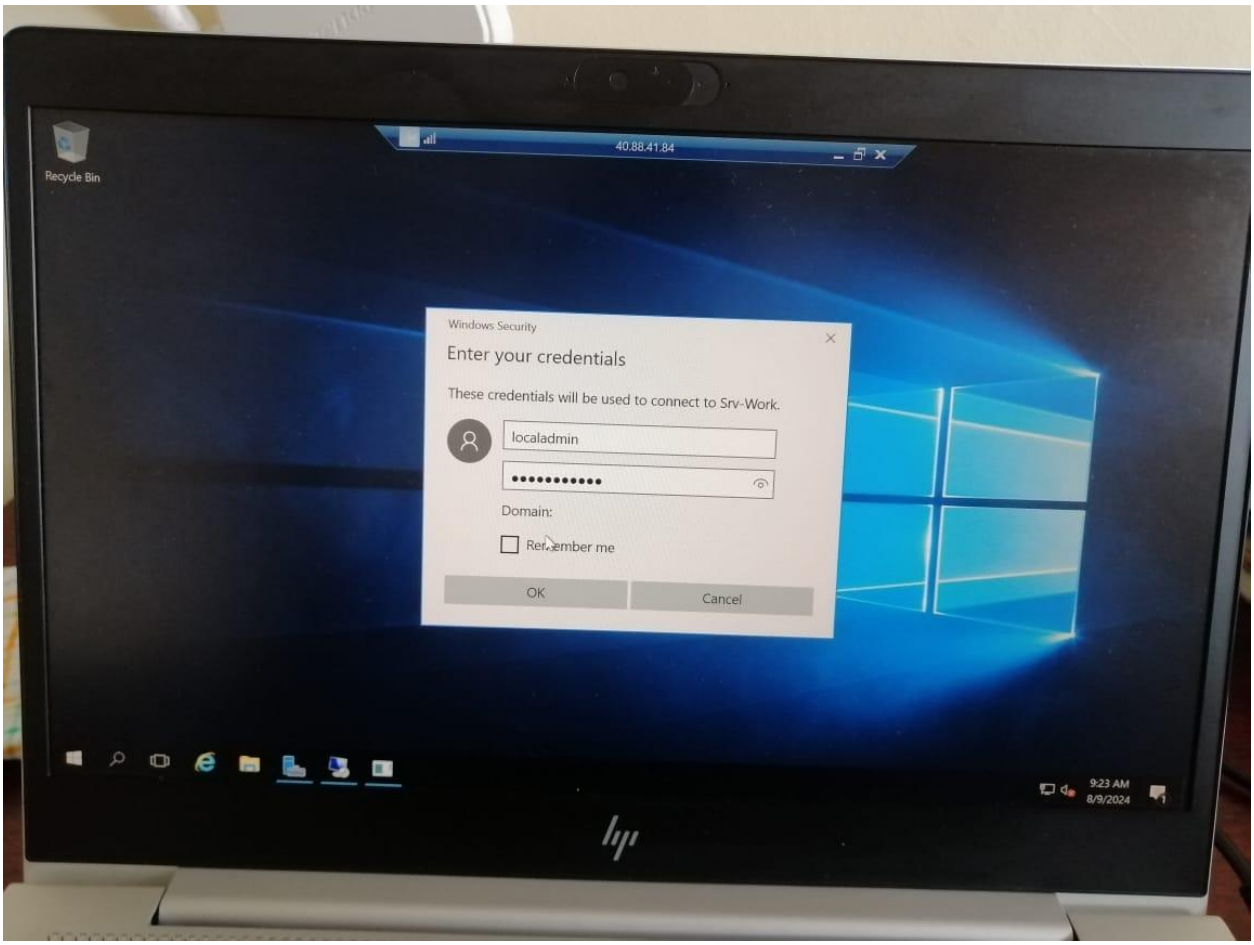
After downloading the RDP file I'll use it to connect srv-jump azure vm via Remote desktop



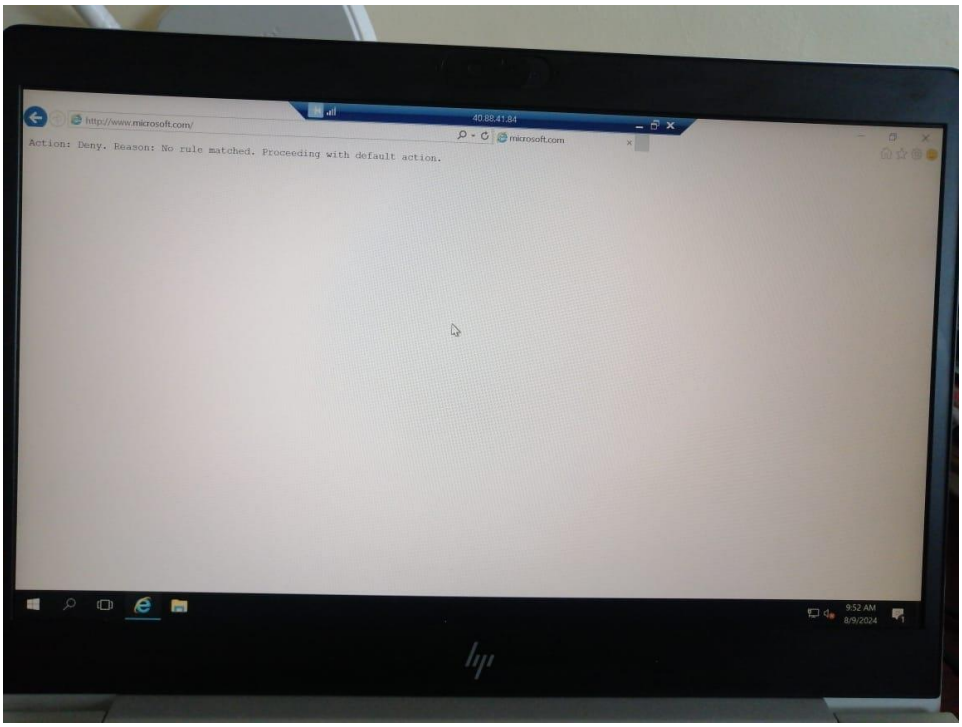
Within the Remote Desktop session to Srv-Work, in Server Manager, I'll click Local Server and then click IE Enhanced Security Configuration as show in the figures below

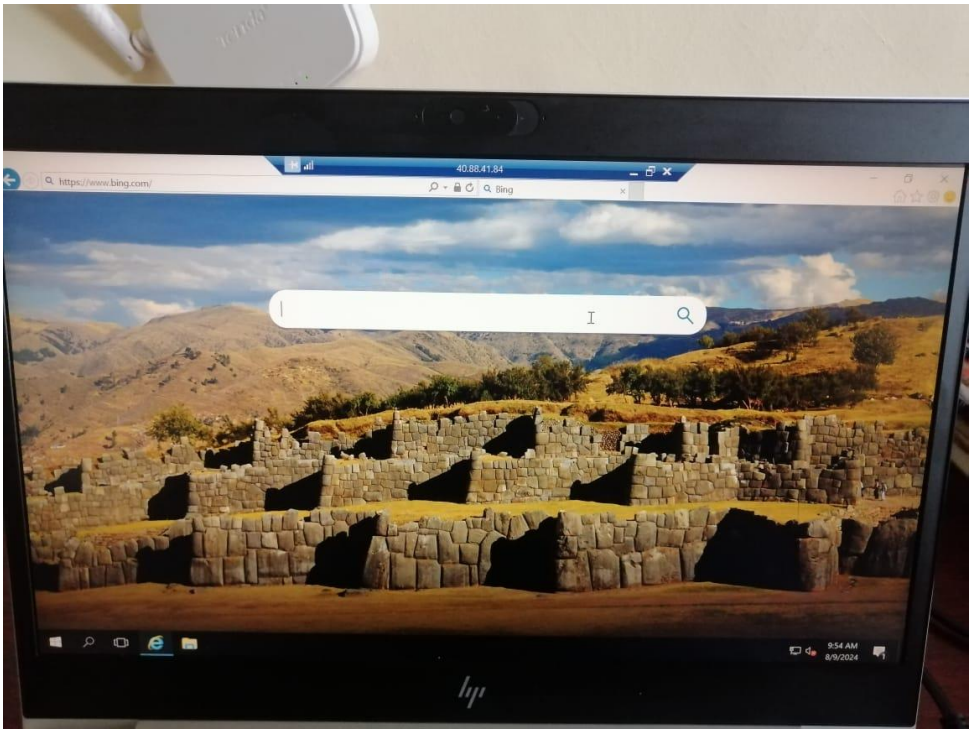

40.88.41.84
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
2 Services
Performance
All Servers 1
Manageability
Events
2 Services
Performance
9:10 AM
8/9/2024


40.88.41.84
al Server
Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
More about Internet Explorer Enhanced Security Configuration
OK
Cancel
ID
Severity
Source
Log
Date and Time
10016
Error
Microsoft-Windows-DistributedCOM
System
8/9/2024 9:07:33 AM


Recycle Bin
40.88.41.84
Windows Security
Enter your credentials
These credentials will be used to connect to Srv-Work.
localadmin
Domain:
Remember me
OK
Cancel
9:23 AM
8/9/2024

From the explore I'll Browse to **http://www.microsoft.com/** and **http://www.microsoft.com/** as shown in the diagrams below.





Conclusion

By practicing this lab, I have gained hands-on experience with deploying and configuring Azure Firewall to manage network traffic within an Azure environment.

Also understood how to set up a secure virtual network, create custom routes, and implement firewall rules to control outbound and inbound traffic.

Additionally, I have learnt how to validate the firewall's effectiveness through practical testing