COURSE: CLOUD AND NEWTORK SECURITY

NAME: DENISE SOPHY ONDISO MUTAYI

STUDENT NO: CS-CN09-25047

AZURE FIREWALL

Contents

INTRODUCTION ... 3

DEPLOY AND TEST AN AZURE FIREWALL ... 4

Task 1: Use a template to deploy the lab environment ... 4

Task 2: Deploy the Azure firewall ... 5

Task 3: Create a default route ... 6

Task 4: Configure an application rule ... 8

Task 5: Configure a network rule ... 9

Task 6: Configure the virtual machine DNS servers ... 9

Task 7: Test the firewall ... 10

CONCLUSION ... 14

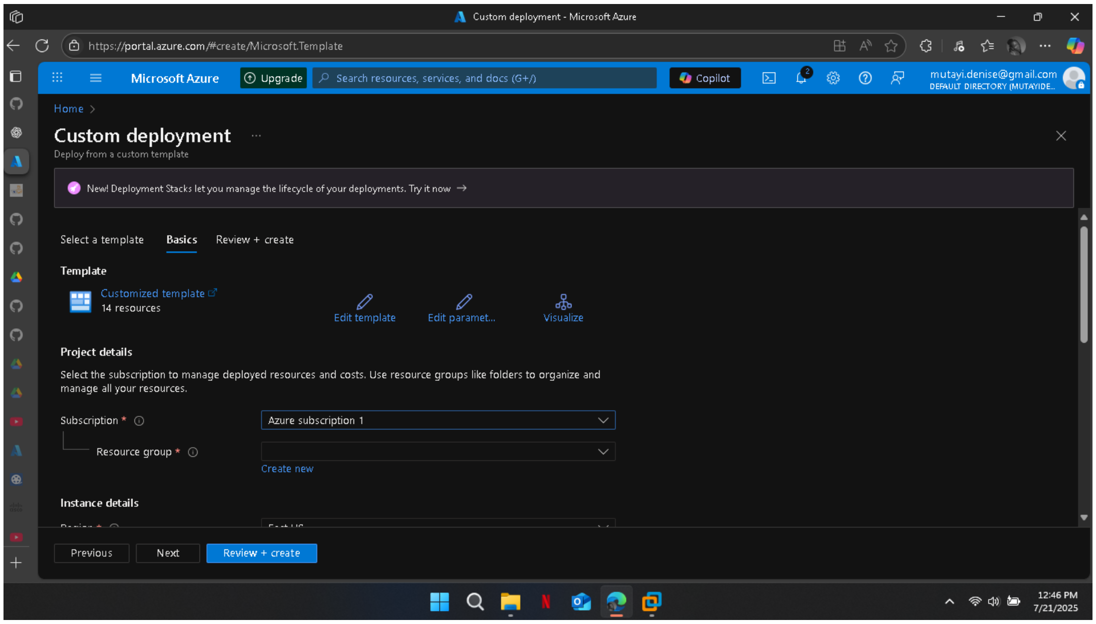
INTRODUCTION

In this lab, I set out to deploy and configure an Azure Firewall within a controlled virtual network environment. The goal was to get hands-on experience with deploying secure, scalable network perimeter protection using Azure-native tools. Starting from the creation of a dedicated resource group named AZ500LAB08, I provisioned essential components including a virtual network, a subnet for the firewall, and a public IP address. I also configured route tables and verified firewall functionality through access control. This lab was a practical dive into how Azure Firewall integrates with network security strategies and centralizes traffic governance in the cloud.

DEPLOY AND TEST AN AZURE FIREWALL

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

In this task, I deployed a Windows Server 2016 virtual machine in Azure using an ARM template. After signing into the Azure portal, I navigated to Custom deployment, selected Build your own template, and loaded the provided template.json file. I created a new resource group named AZ500LAB08, set the location to East US, and configured a secure admin password. Finally, I reviewed and initiated the deployment, which completed successfully



Custom deployment - Microsoft Azure
https://portal.azure.com/#create/Microsoft.Template
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAYIDE...
Home >

Custom deployment

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Select a template
Basics
Review + create

Template

Customized template
14 resources

Edit template
Edit paramet...
Visualize

Project details

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

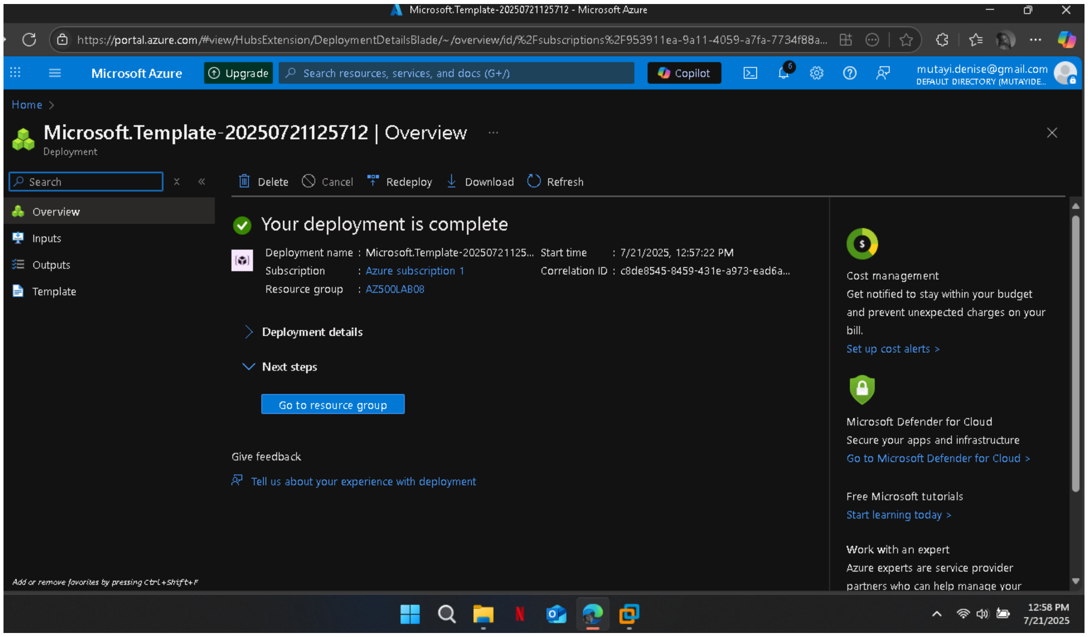
Subscription * : Azure subscription 1

Resource group * :

Create new

Instance details

Previous
Next
Review + create
12:46 PM
7/21/2025



Microsoft.Template-20250721125712 - Microsoft Azure
https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F953911ea-9a11-4059-a7fa-7734f88a...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAYIDE...
Home >

Microsoft.Template-20250721125712 | Overview

Deployment

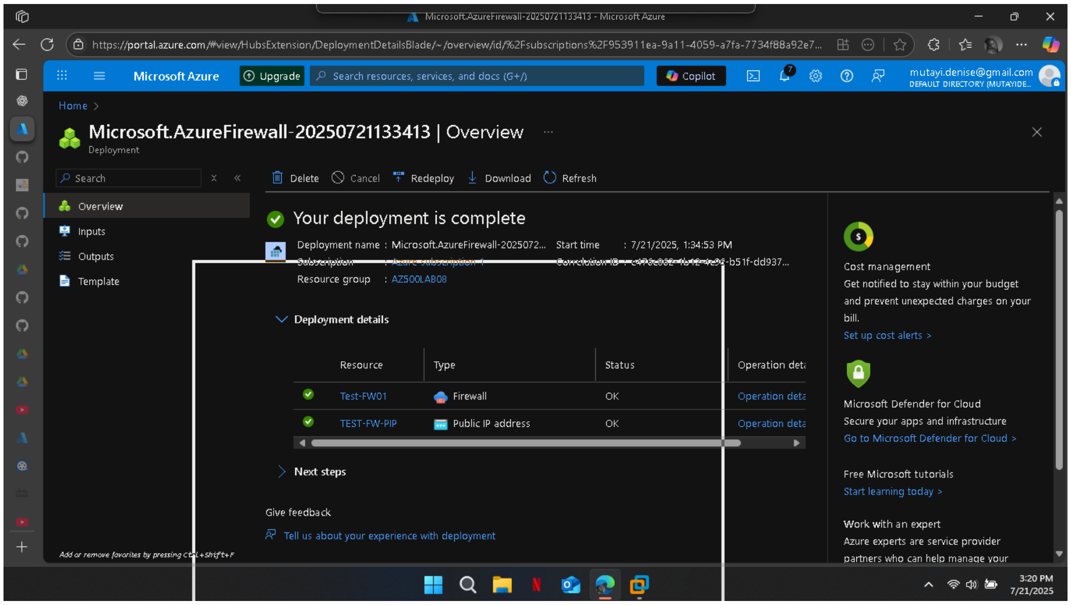
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

Your deployment is complete

Deployment name : Microsoft.Template-20250721125...
Subscription : Azure subscription 1
Resource group : AZ500LAB08
Start time : 7/21/2025, 12:57:22 PM
Correlation ID : c8de8545-8459-431e-a973-ead6a...

Deployment details
Next steps
Go to resource group
Give feedback
Tell us about your experience with deployment
Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your
Add or remove favorites by pressing Ctrl+Shift+F
12:58 PM
7/21/2025

Task 2: Deploy the Azure firewall



Microsoft.AzureFirewall-20250721133413 - Microsoft Azure

https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F953911ea-9a11-4059-a7fa-7734f88a92e7...

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYIDE...

Home >

Microsoft.AzureFirewall-20250721133413 | Overview

Deployment

Delete | Cancel | Redeploy | Download | Refresh

Overview
Inputs
Outputs
Template

Your deployment is complete

Deployment name : Microsoft.AzureFirewall-2025072... Start time : 7/21/2025, 1:34:53 PM

Subscription : Azure subscription 1 Correlation ID : c476c862-1b12-4c96-b51f-dd937...

Resource group : AZ500LAB08

Deployment details

	Resource	Type	Status	Operation deta
✓	Test-FW01	Firewall	OK	Operation deta
✓	TEST-FW-PIP	Public IP address	OK	Operation deta

Next steps

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

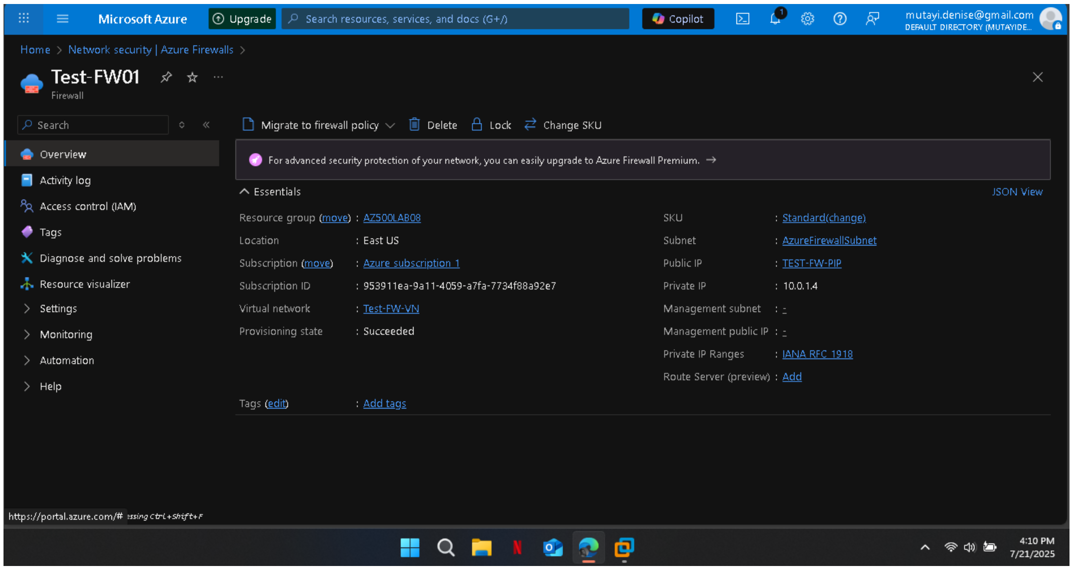
Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your

Add or remove favorites by pressing Ctrl+Shift+F

3:20 PM 7/21/2025



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | mutayi.denise@gmail.com DEFAULT DIRECTORY (MUTAYIDE...

Home > Network security | Azure Firewalls >

Test-FW01

Firewall

Migrate to firewall policy | Delete | Lock | Change SKU

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

For advanced security protection of your network, you can easily upgrade to Azure Firewall Premium. →

Essentials JSON View

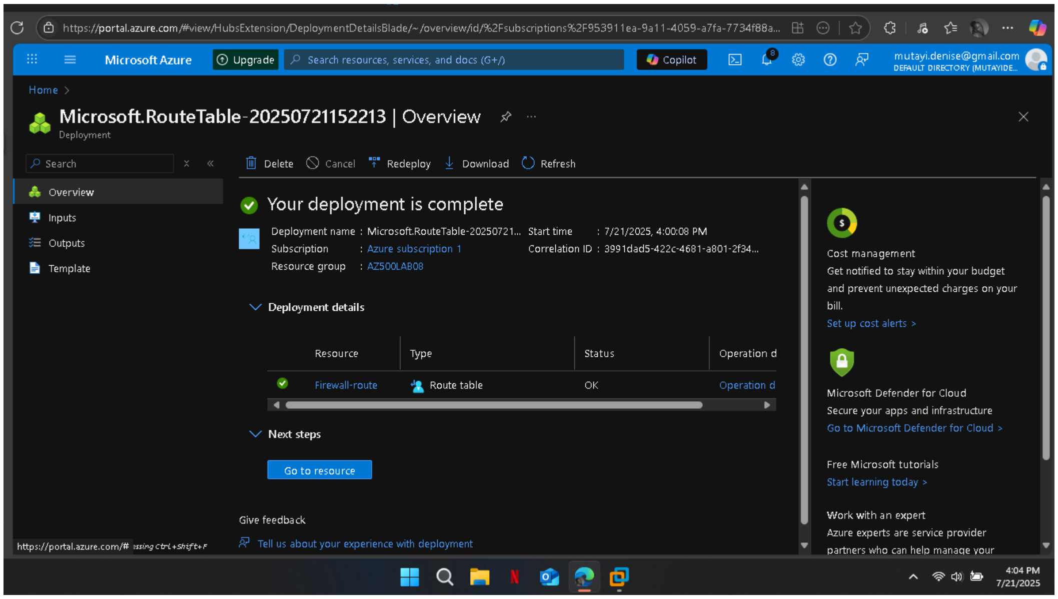
Resource group (move)	: AZ500LAB08	SKU	: Standard(change)
Location	: East US	Subnet	: AzureFirewallSubnet
Subscription (move)	: Azure subscription 1	Public IP	: TEST-FW-PIP
Subscription ID	: 953911ea-9a11-4059-a7fa-7734f88a92e7	Private IP	: 10.0.1.4
Virtual network	: Test-FW-VN	Management subnet	: -
Provisioning state	: Succeeded	Management public IP	: -
		Private IP Ranges	: IANA RFC 1918
		Route Server (preview)	: Add
Tags (edit)	: Add tags		

https://portal.azure.com/#

4:10 PM 7/21/2025

In this task, I deployed an Azure Firewall into an existing virtual network using the Azure portal. I navigated to the *Firewalls* section, created a new firewall named Test-FW01 in the AZ500LAB08 resource group, and selected the East US region. I chose the Standard SKU, opted for classic firewall rules, and linked it to the existing virtual network Test-FW-VN. I disabled the Firewall Management NIC and created a new public IP named TEST-FW-PIP. After deployment, I accessed the AZ500LAB08 resource group to review resources and noted the private IP address assigned to the firewall for use in upcoming configurations.

Task 3: Create a default route



https://portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F953911ea-9a11-4059-a7fa-7734f88a...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
mutayi.denise@gmail.com
DEFAULT DIRECTORY (MUTAYIDE...
Home
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

Microsoft.RouteTable-20250721152213 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.RouteTable-20250721... Start time : 7/21/2025, 4:00:08 PM
Subscription : Azure subscription 1 Correlation ID : 3991dad5-422c-4681-a801-2f34...
Resource group : AZ500LAB08

Deployment details

	Resource	Type	Status	Operation d
✓	Firewall-route	Route table	OK	Operation d

Next steps

Go to resource

Give feedback

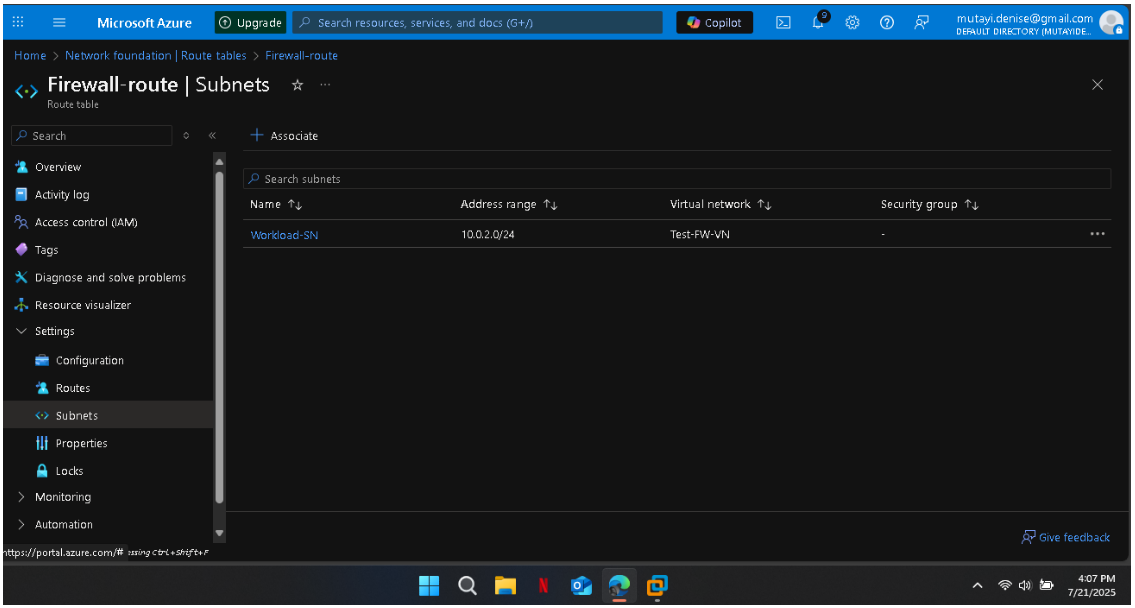
Tell us about your experience with deployment

Cost management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >

Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >

Free Microsoft tutorials
Start learning today >

Work with an expert
Azure experts are service provider partners who can help manage your

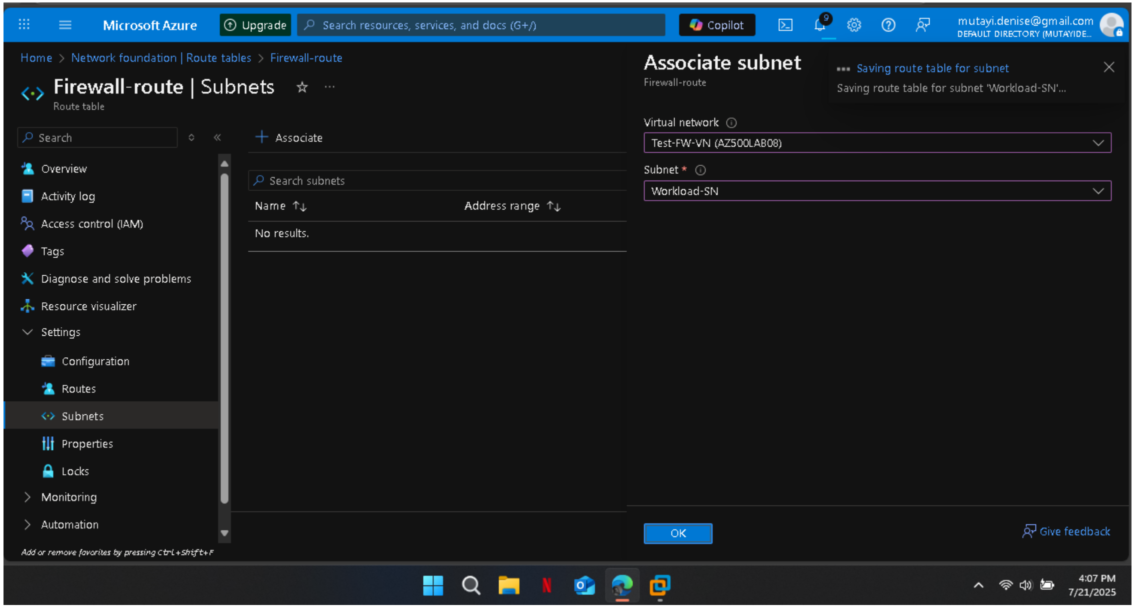


Home > Network foundation | Route tables > Firewall-route

Firewall-route | Subnets

Route table

Name	Address range	Virtual network	Security group
Workload-SN	10.0.2.0/24	Test-FW-VN	-



Home > Network foundation | Route tables > Firewall-route

Firewall-route | Subnets

Route table

Name	Address range
No results.	

Associate subnet

Firewall-route

Virtual network: Test-FW-VN (AZ500LAB08)

Subnet *: Workload-SN

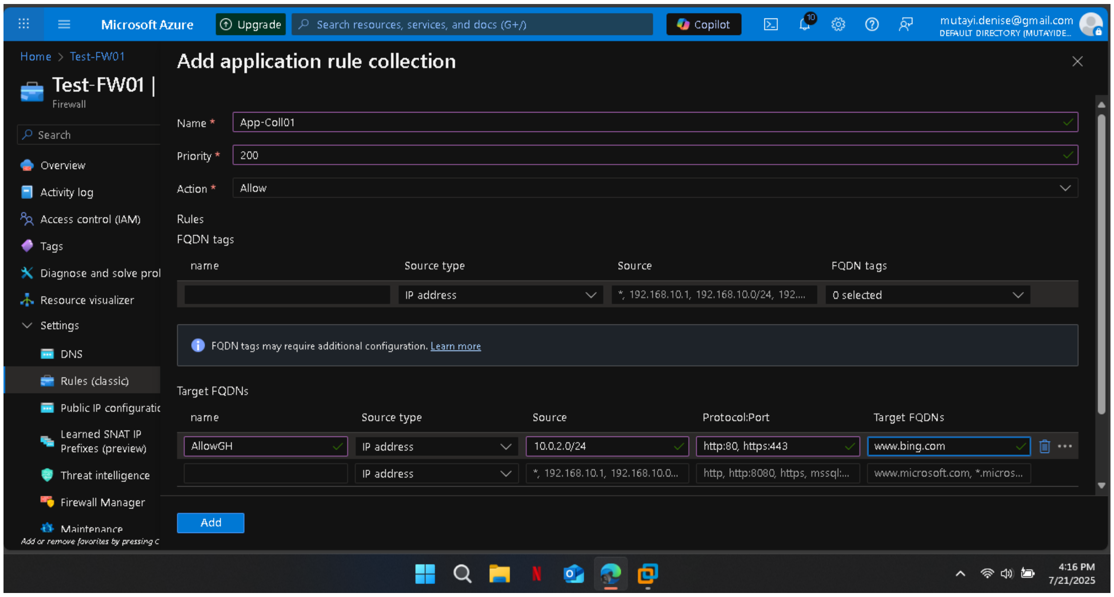
Saving route table for subnet

Saving route table for subnet 'Workload-SN'...

In this task, I created a custom route to ensure that all outbound traffic from the Workload-SN subnet is directed through the Azure Firewall. I began by creating a route table named Firewall-route in the AZ500LAB08 resource group and East US region. After the route table was successfully deployed, I associated it with the Workload-SN subnet within the Test-FW-VN virtual network.

Next, I added a new route to this table. I named the route FW-DG, set the destination to 0.0.0.0/0 to match all outbound traffic, and selected Virtual appliance as the next hop type. I then used the private IP address of the firewall that I had previously deployed (Test-FW01) as the next hop address. This effectively redirected all outbound traffic from the subnet through the Azure Firewall, strengthening the network's security posture.

Task 4: Configure an application rule



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....	0 selected

FQDN tags may require additional configuration. Learn more

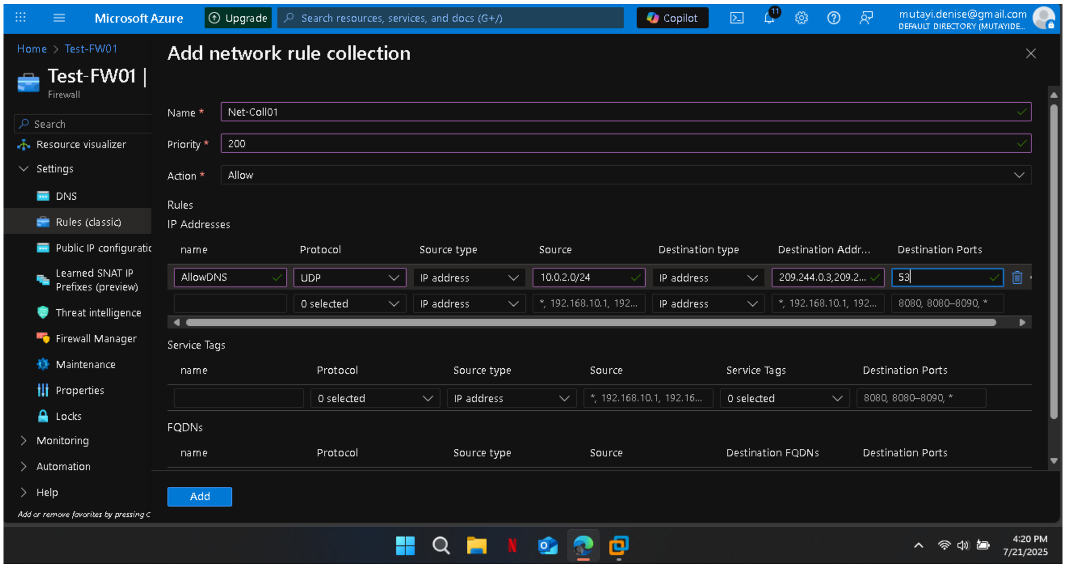
Target FQDNs

name	Source type	Source	Protocol:Port	Target FQDNs
AllowGH	IP address	10.0.2.0/24	http:80, https:443	www.bing.com
	IP address	*, 192.168.10.1, 192.168.10.0...	http, http:8080, https, mssql:...	www.microsoft.com, *.micros...

Add

In this task, I created an application rule within the Azure Firewall (Test-FW01) to allow outbound access to www.bing.com. This was done by navigating to the Rules (classic) section and adding a new Application rule collection named App-Coll01, with a priority of 200 and action set to Allow. Under this collection, I configured a rule named AllowGH to permit HTTP and HTTPS traffic (ports 80 and 443) from the source IP range 10.0.2.0/24 specifically targeting the FQDN www.bing.com. This setup ensures controlled access while respecting Azure's default infrastructure FQDN permissions.

Task 5: Configure a network rule



Add network rule collection

Name * Net-Coll01

Priority * 200

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, 192.16...	0 selected	8080, 8080–8090, *

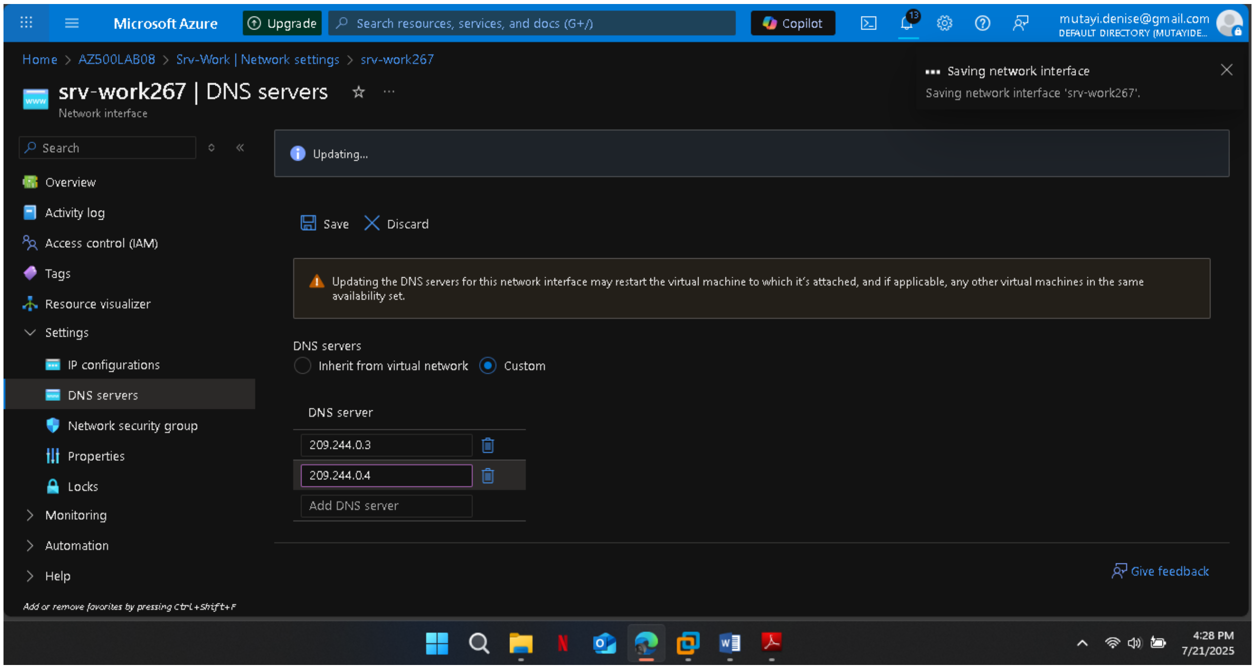
FQDNs

name	Protocol	Source type	Source	Destination FQDNs	Destination Ports

Add

In this task, I configured a network rule in the Azure Firewall (Test-FW01) to permit outbound DNS traffic. I accessed the Network rule collection tab and added a new rule collection named Net-Coll01, set with a priority of 200 and action set to Allow. Within this collection, I created a rule named AllowDNS to allow UDP traffic on port 53 (used for DNS) from the source IP range 10.0.2.0/24 to two specific public DNS server IPs: 209.244.0.3 and 209.244.0.4. This setup ensures that DNS queries can reach external resolvers securely and efficiently.

Task 6: Configure the virtual machine DNS servers



Saving network interface

Saving network interface 'srv-work267'.

Updating...

Save Discard

Updating the DNS servers for this network interface may restart the virtual machine to which it's attached, and if applicable, any other virtual machines in the same availability set.

DNS servers

○ Inherit from virtual network ● Custom

DNS server

209.244.0.3

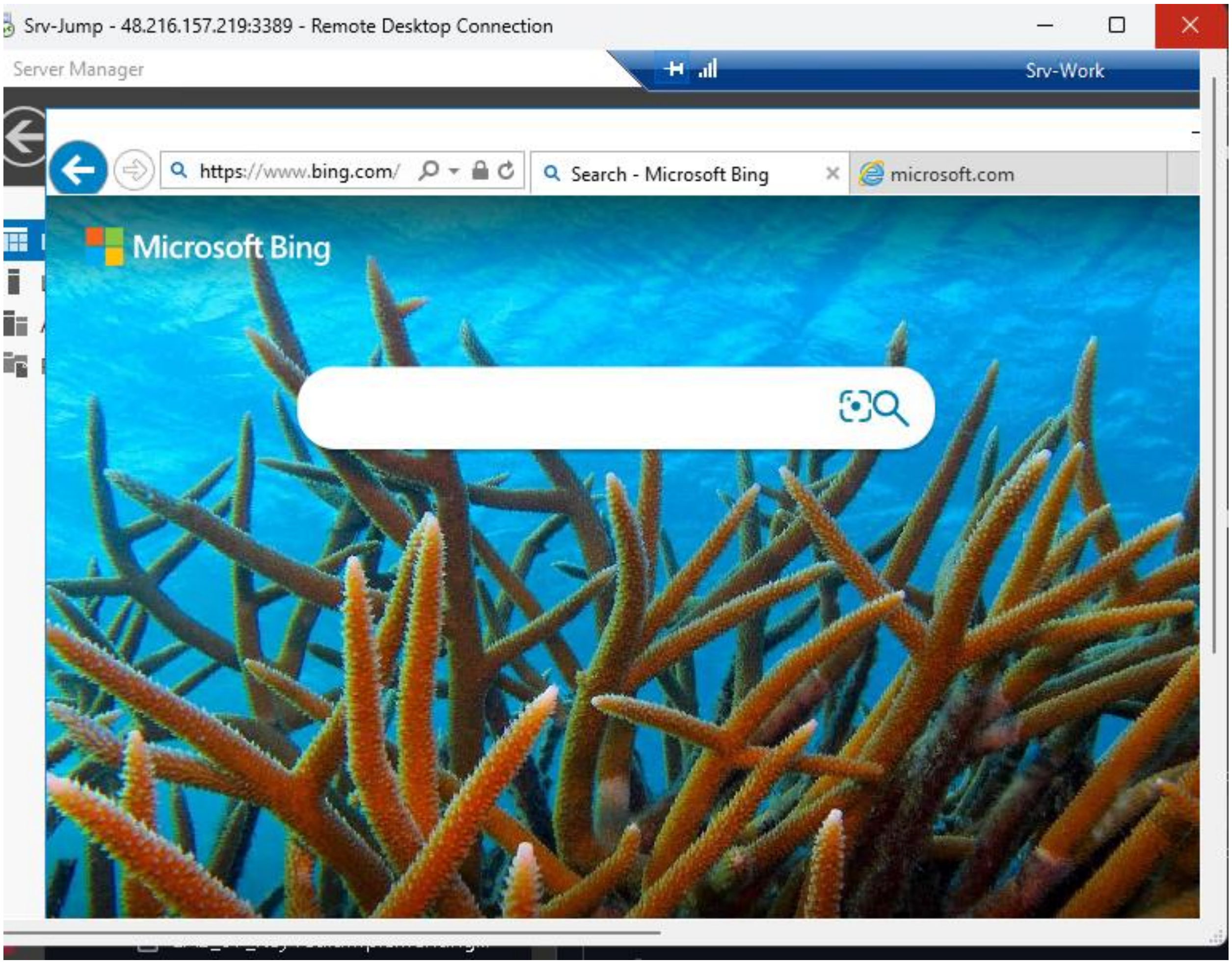
209.244.0.4

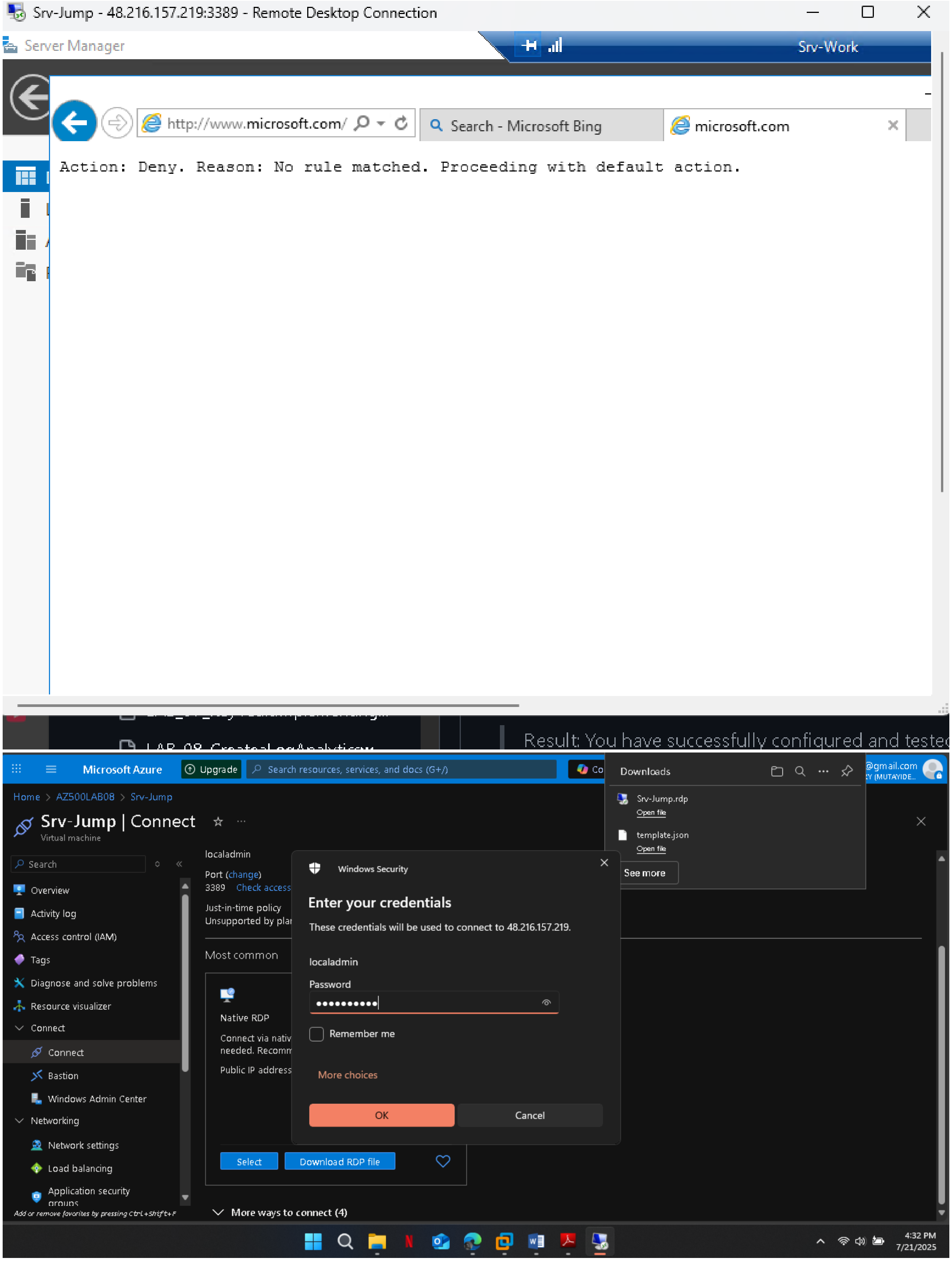
Add DNS server

In this task, I configured custom DNS servers for the Srv-Work virtual machine. Within the Azure portal, I navigated to the network interface associated with Srv-Work, accessed the DNS servers settings, and selected the Custom option. I then added the two DNS IPs (209.244.0.3 and 209.244.0.4) that were previously allowed in the firewall rule. After saving the configuration, the virtual machine restarted automatically to apply the DNS changes. This ensures Srv-Work resolves DNS queries using the specified external resolvers.

Task 7: Test the firewall

In this lab, I worked hands-on with Azure Firewall to understand how to implement and test network security controls within an Azure environment. My goal was to simulate a secure infrastructure by deploying a firewall, configuring its network rules, and validating their effects through real-time testing using virtual machines. From setting up DNS servers to inspecting traffic behavior, I got to experience the process of establishing controlled access to internet resources and applying best practices for firewall management in a cloud setting


Srv-Jump - 48.216.157.219:3389 - Remote Desktop Connection
Server Manager
Srv-Work
https://www.bing.com/
Search - Microsoft Bing
microsoft.com
Microsoft Bing



Srv-Jump - 48.216.157.219:3389 - Remote Desktop Connection

Server Manager

Srv-Work

http://www.microsoft.com/

Search - Microsoft Bing

microsoft.com

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

Result: You have successfully configured and testec

Microsoft Azure

Upgrade

Search resources, services, and docs (G+/)

Home > AZ500LAB08 > Srv-Jump

Srv-Jump | Connect

Virtual machine

localadmin

Port (change)
3389 Check access

Just-in-time policy
Unsupported by plar

Most common

Native RDP

Connect via nativ
needed. Recomm

Public IP address

Downloads

Srv-Jump.rdp
Open file

template.json
Open file

See more

@gmail.com

Windows Security

Enter your credentials

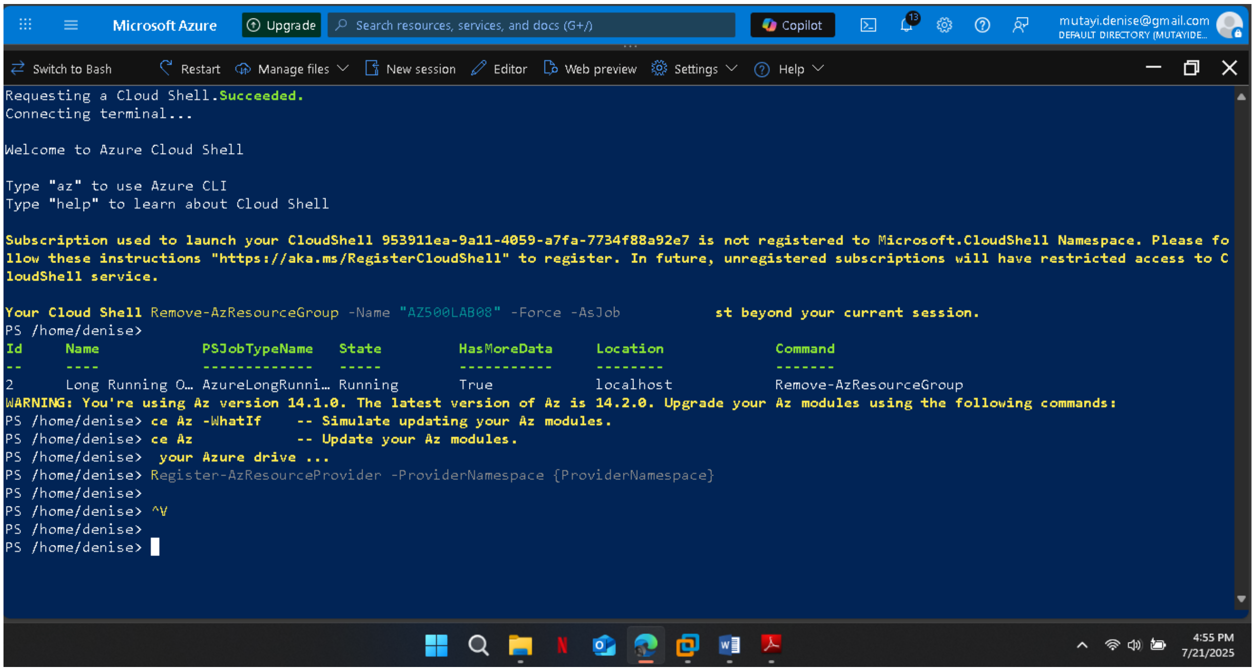
These credentials will be used to connect to 48.216.157.219.

localadmin

Password: ••••••••••

□ Remember me

4:32 PM
7/21/2025



```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

Subscription used to launch your CloudShell 953911ea-9a11-4059-a7fa-7734f88a92e7 is not registered to Microsoft.CloudShell Namespace. Please fo
llow these instructions "https://aka.ms/RegisterCloudShell" to register. In future, unregistered subscriptions will have restricted access to C
loudShell service.

Your Cloud Shell Remove-AzResourceGroup -Name "AZ500LAB08" -Force -AsJob           st beyond your current session.
PS /home/denise>
Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
2      Long Running O… AzureLongRunni… Running       True            localhost            Remove-AzResourceGroup
WARNING: You're using Az version 14.1.0. The latest version of Az is 14.2.0. Upgrade your Az modules using the following commands:
PS /home/denise> ce Az -WhatIf    -- Simulate updating your Az modules.
PS /home/denise> ce Az            -- Update your Az modules.
PS /home/denise>  your Azure drive ...
PS /home/denise> Register-AzResourceProvider -ProviderNamespace {ProviderNamespace}
PS /home/denise>
PS /home/denise> ^V
PS /home/denise>
PS /home/denise> 
```

CONCLUSION

By the end of the lab, I successfully deployed and tested Azure Firewall, confirming that it could effectively control and filter outbound network traffic. I also practiced good cloud hygiene by cleaning up the resources I had provisioned — removing the entire AZ500LAB08 resource group using PowerShell in Azure Cloud Shell. This lab not only strengthened my understanding of firewall concepts in a cloud context but also gave me confidence in managing Azure resources securely and efficiently. It was a valuable step toward becoming more fluent in Azure-based network security operations.