Assignment 2: Azure Firewall

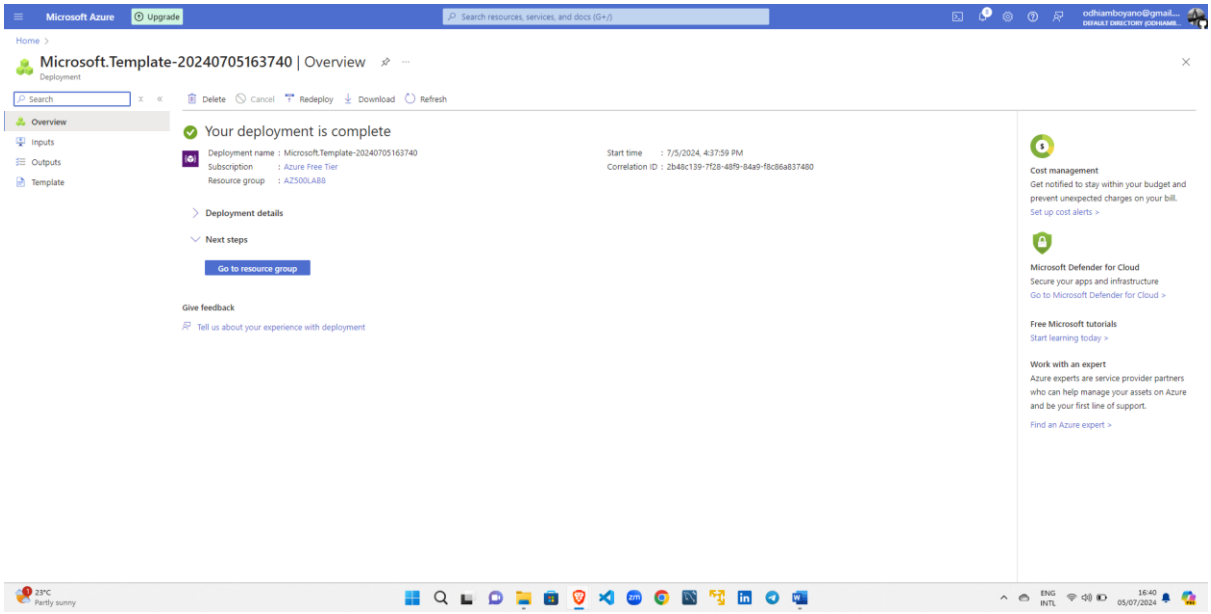
Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction

In this lab, I set out to deploy and test an Azure Firewall to enhance network security for my organization. The main goal was to establish a virtual network with a workload subnet and a jump host subnet, deploy virtual machines in each subnet, and create custom routes and firewall rules to control inbound and outbound traffic. This exercise is critical for ensuring that network security policies are enforced effectively, preventing unauthorized access and ensuring that only permitted traffic can traverse the network.

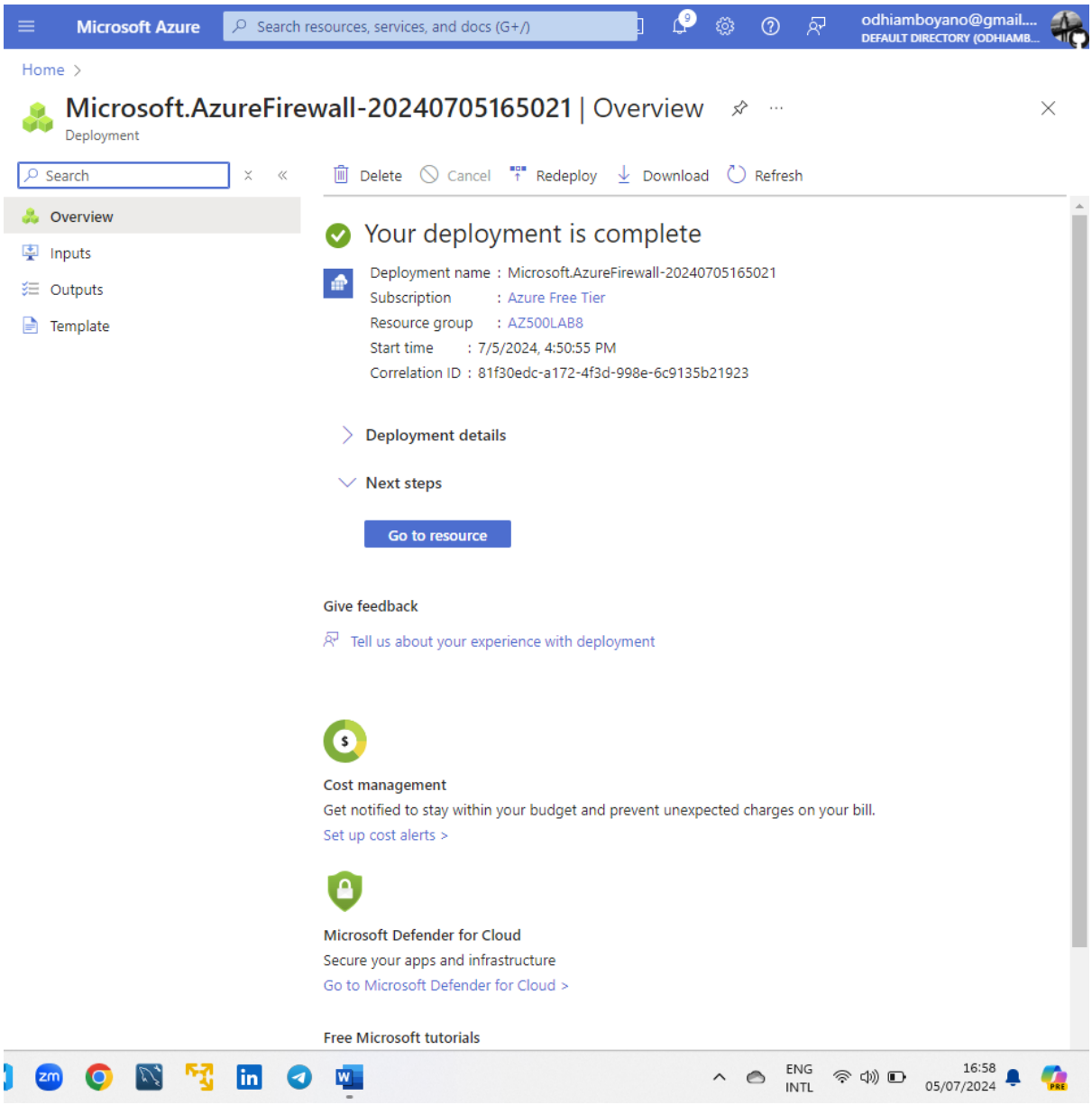
Task 1: Use a Template to Deploy the Lab Environment

To deploy a custom template in the Azure Portal, I first signed in with an account that has the Owner or Contributor role. Then, I searched for "Deploy a custom template" in the portal. I loaded the provided template.json file, reviewed its contents, and deployed the template to create a virtual machine using the provided settings, including a secure password for later use.



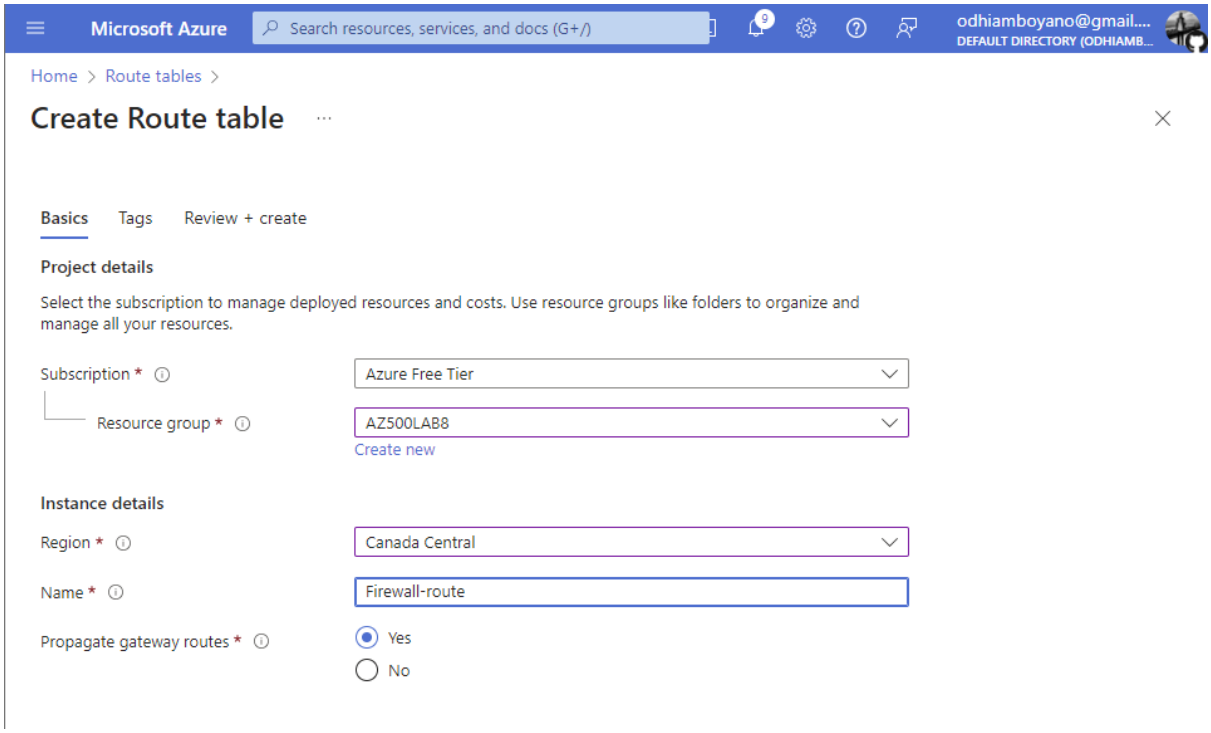
Task 2: Deploy the Azure Firewall

In the Azure portal, I navigated to "Firewalls," created a new firewall using the existing resource group and virtual network, configured the firewall settings, and deployed it, noting the private IP address assigned to the firewall.

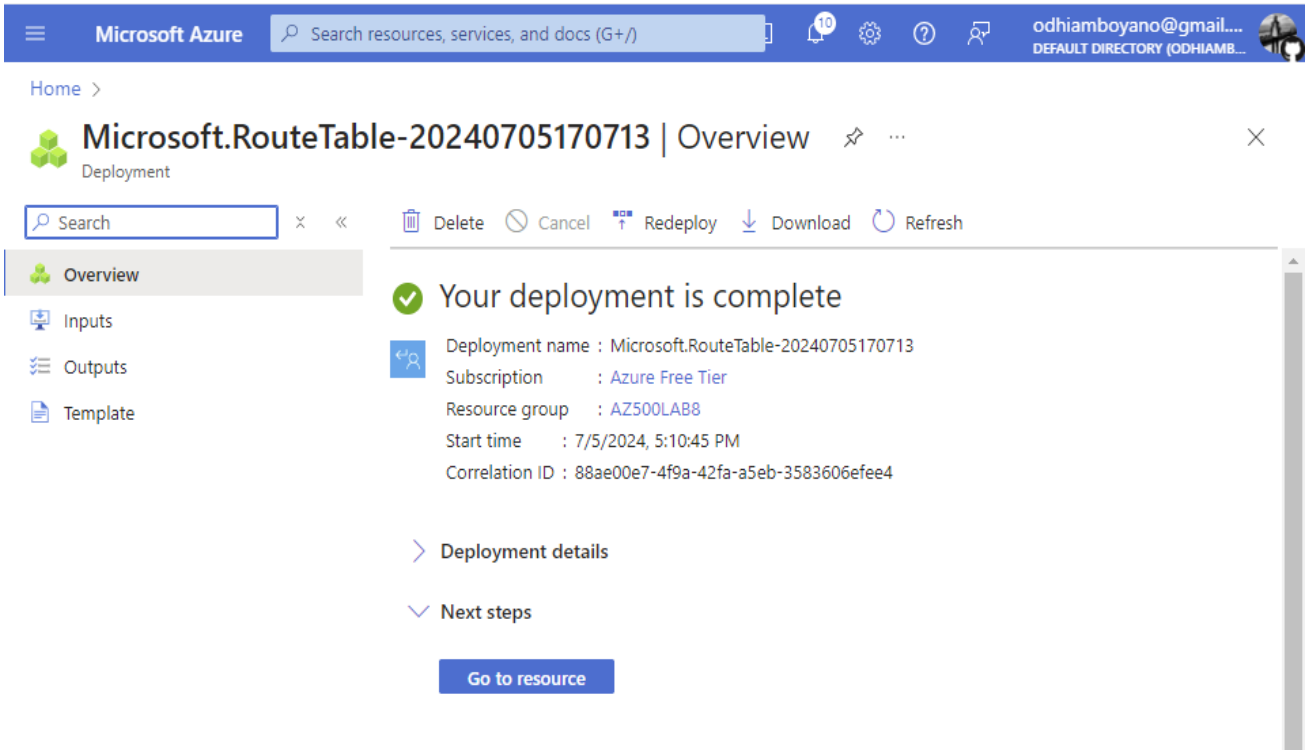


Task 3: Create a Default Route

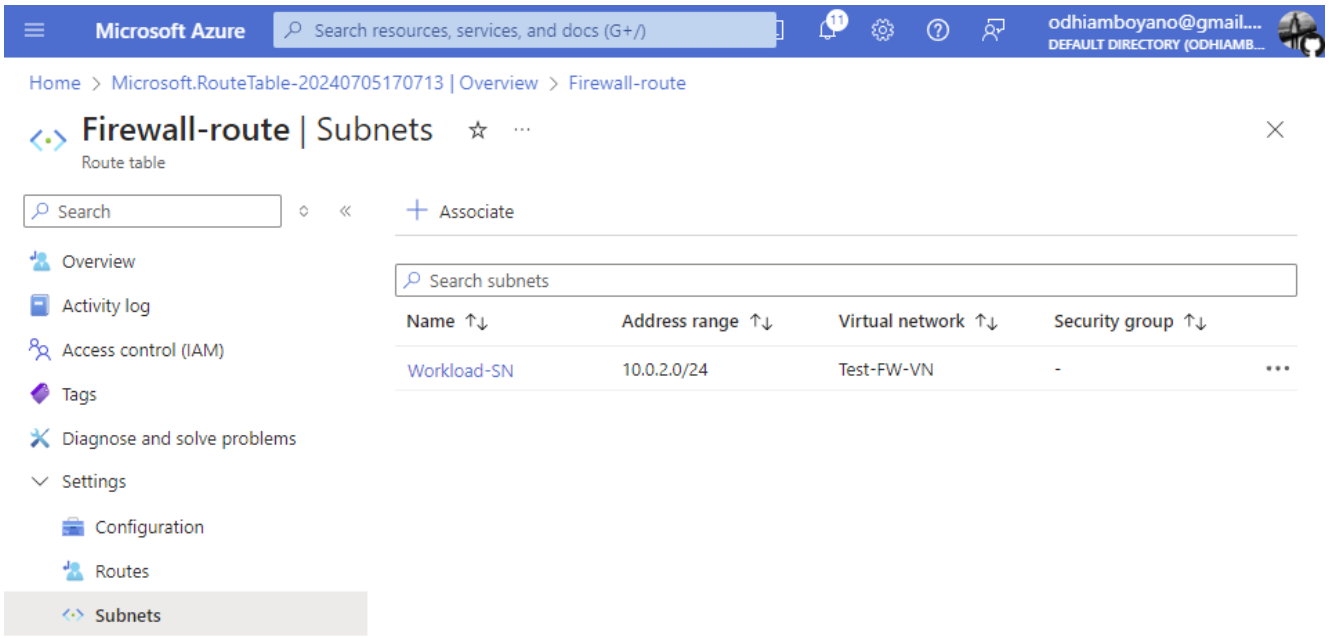
I created a new route table in the Canada Central region, associated it with the Workload-SN subnet, and added a route that directs all outbound traffic from this subnet through the firewall.



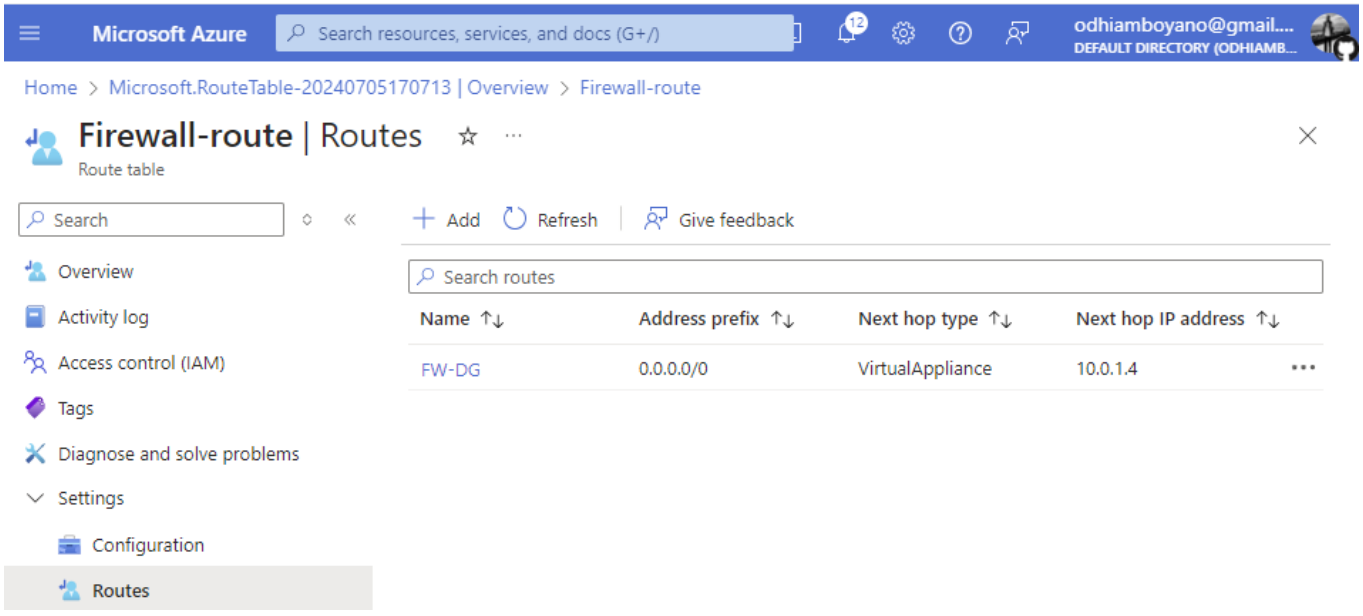
The deployment completed successfully.



I then associated the Firewall to the virtual network subnet

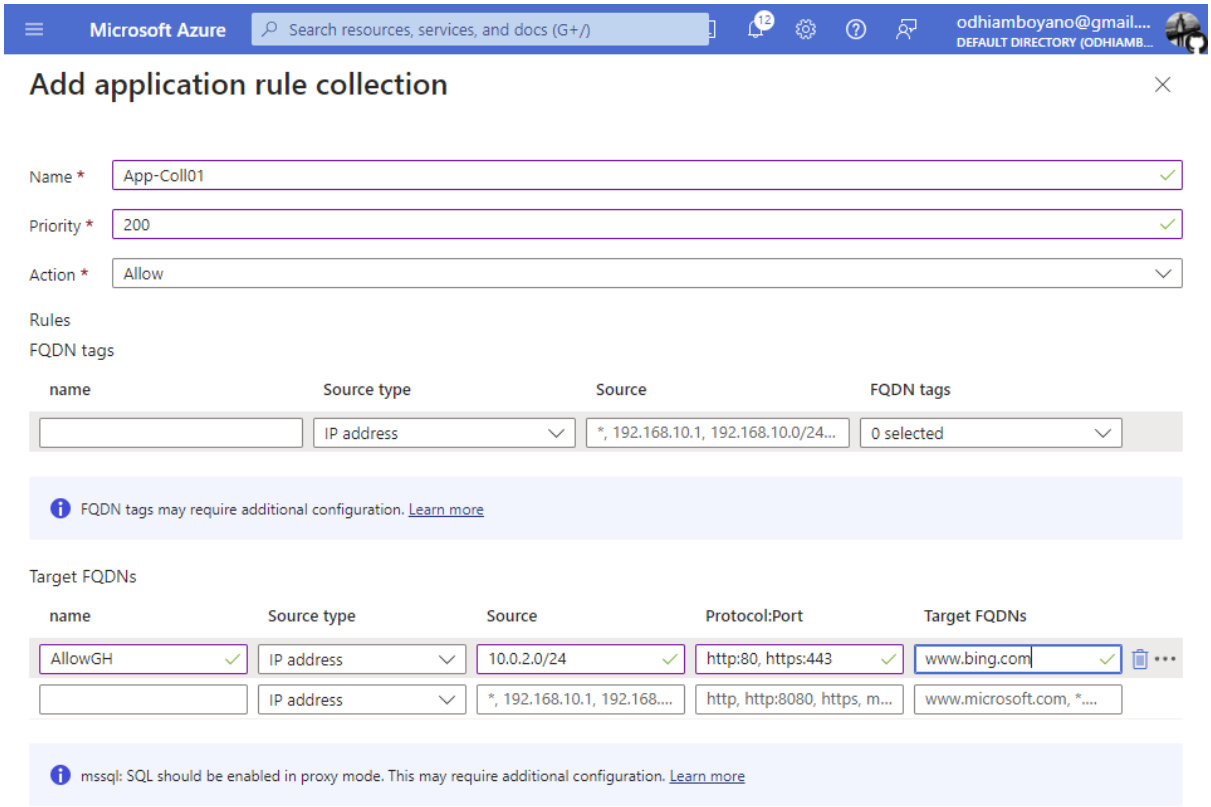


I then added a route to the Firewall

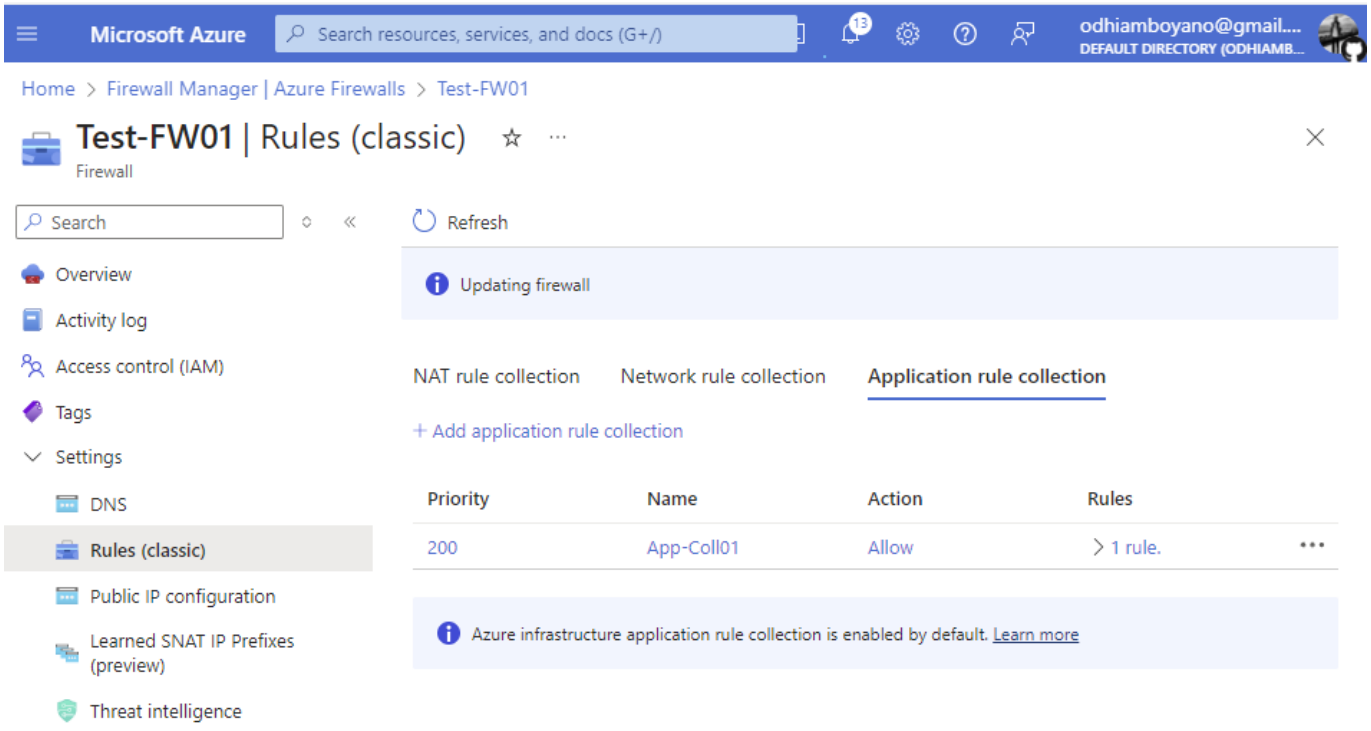


Task 4: Configure an Application Rule

I navigated to the firewall, created an application rule collection, and allowed outbound traffic to www.bing.com from the workload subnet.

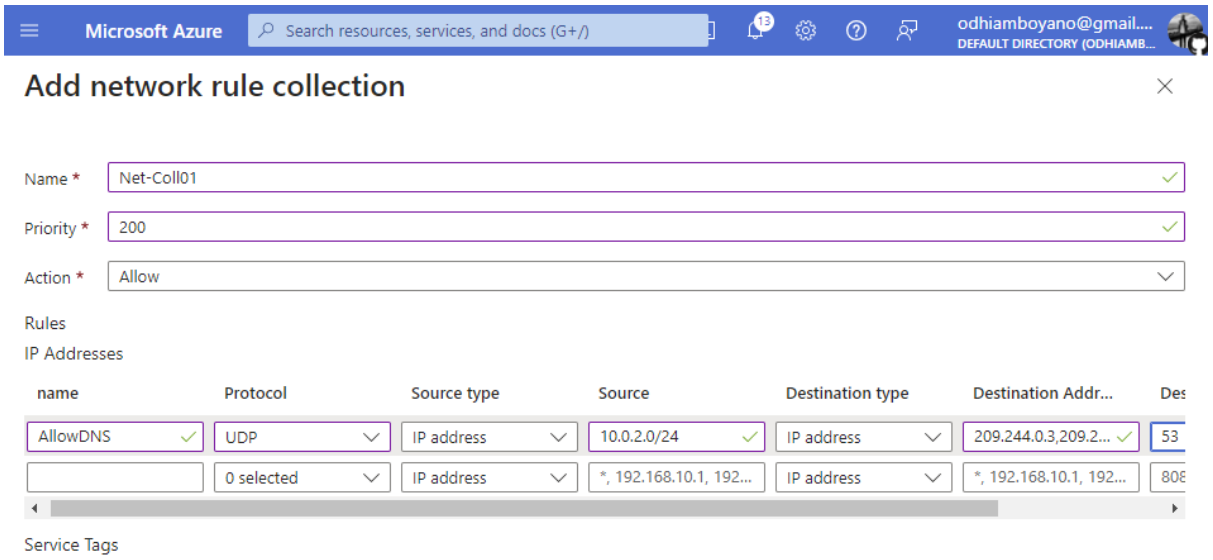


I configured the rule and added it successfully

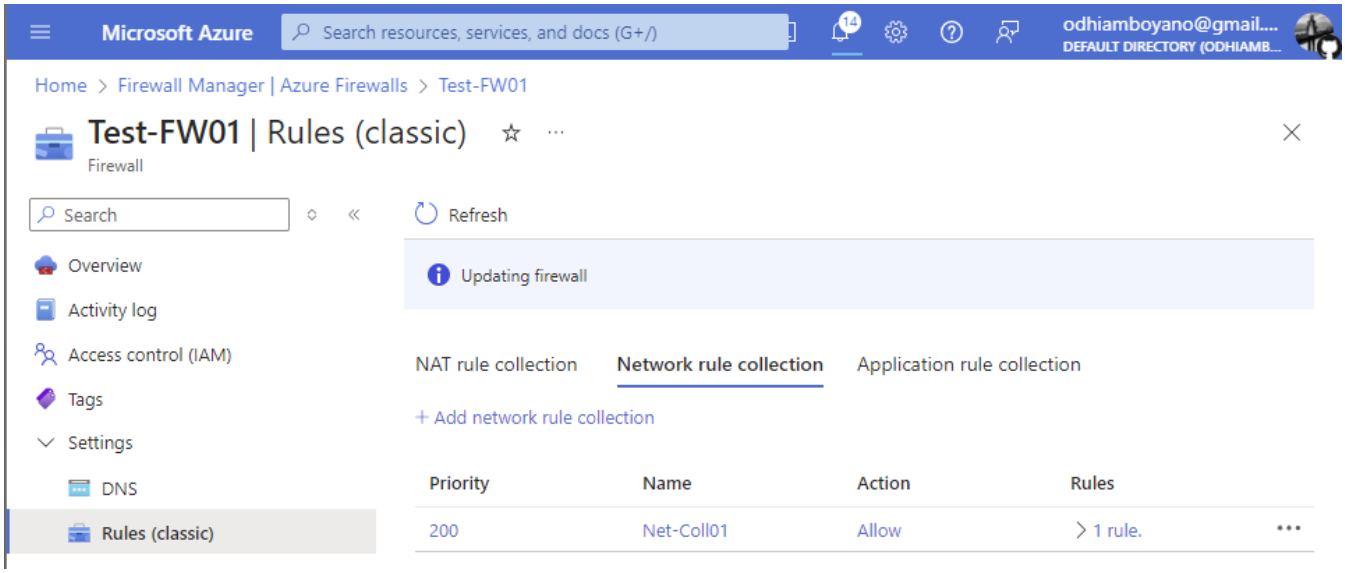


Task 5: Configure a Network Rule

I created a network rule that allows outbound DNS queries to specific public DNS servers.

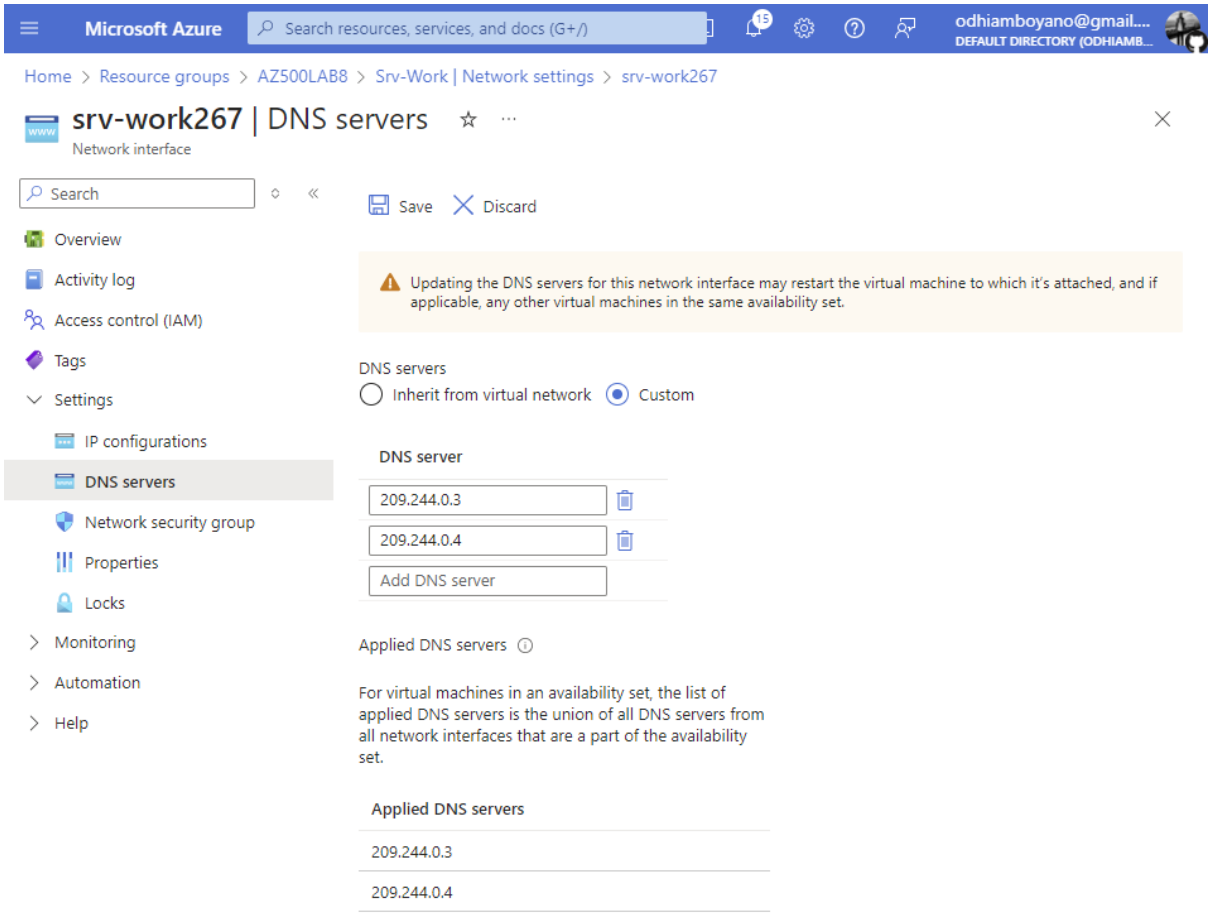


It was successfully added as shown below.



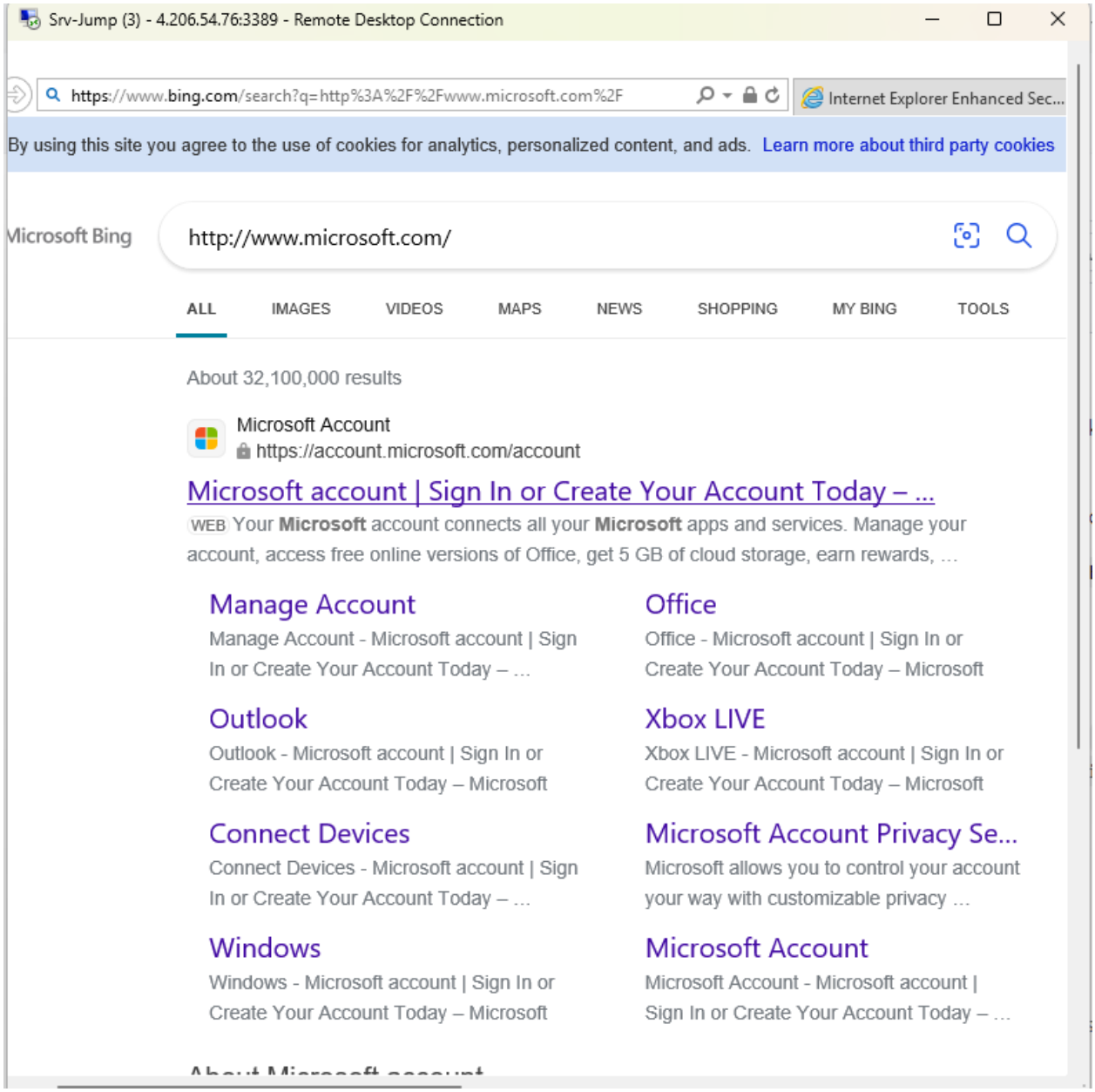
Task 6: Configure DNS Servers

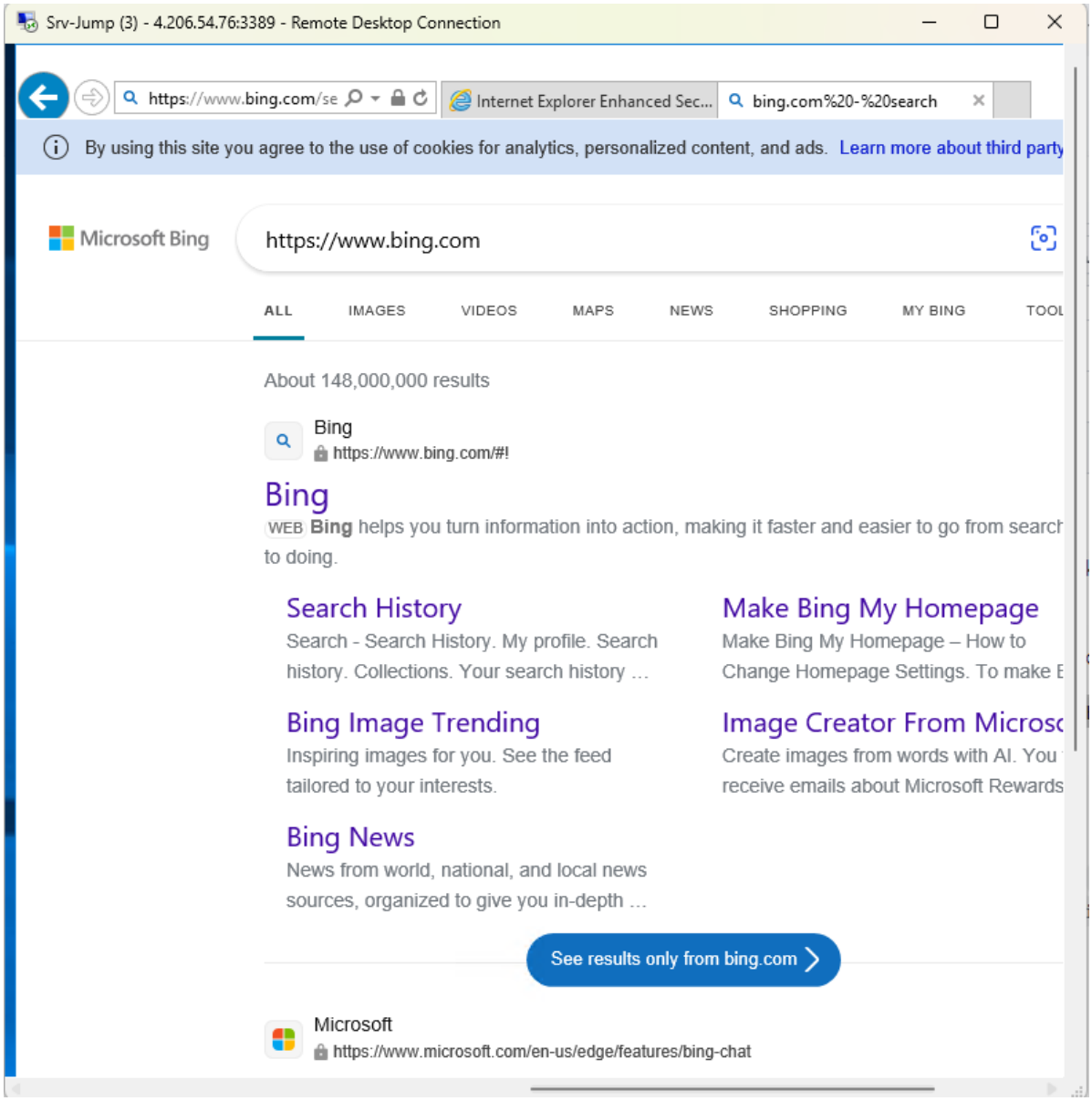
I updated the DNS settings for the network interface of the workload virtual machine to use the specified DNS servers.



Task 7: Test the Firewall

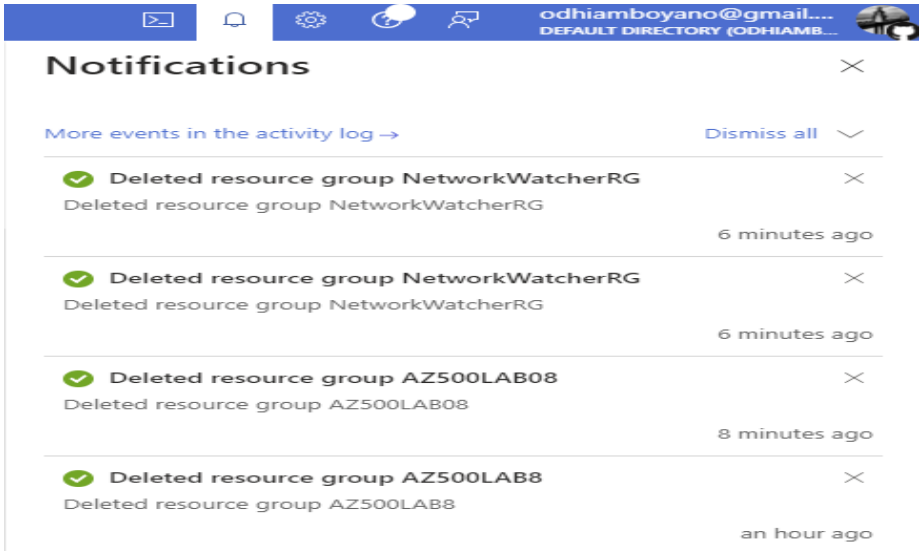
I used RDP to connect to the jump host and then to the workload VM, testing outbound access to allowed and blocked websites to verify the firewall rules.





Cleanup

All resources created during the lab were removed to avoid unnecessary costs.



Conclusion

Completing this lab provided me with hands-on experience in deploying and configuring an Azure Firewall. I successfully set up a secure network environment by directing traffic through the firewall and enforcing specific rules for outbound traffic.

This exercise highlighted the importance of network security and the capabilities of Azure Firewall in managing and controlling access to resources. By configuring application and network rules, I ensured that only authorized traffic could flow through the network, thereby enhancing the overall security posture of the organization. This practical experience will be invaluable in future network security planning and implementation tasks.