

Assignment 2: Azure Firewall

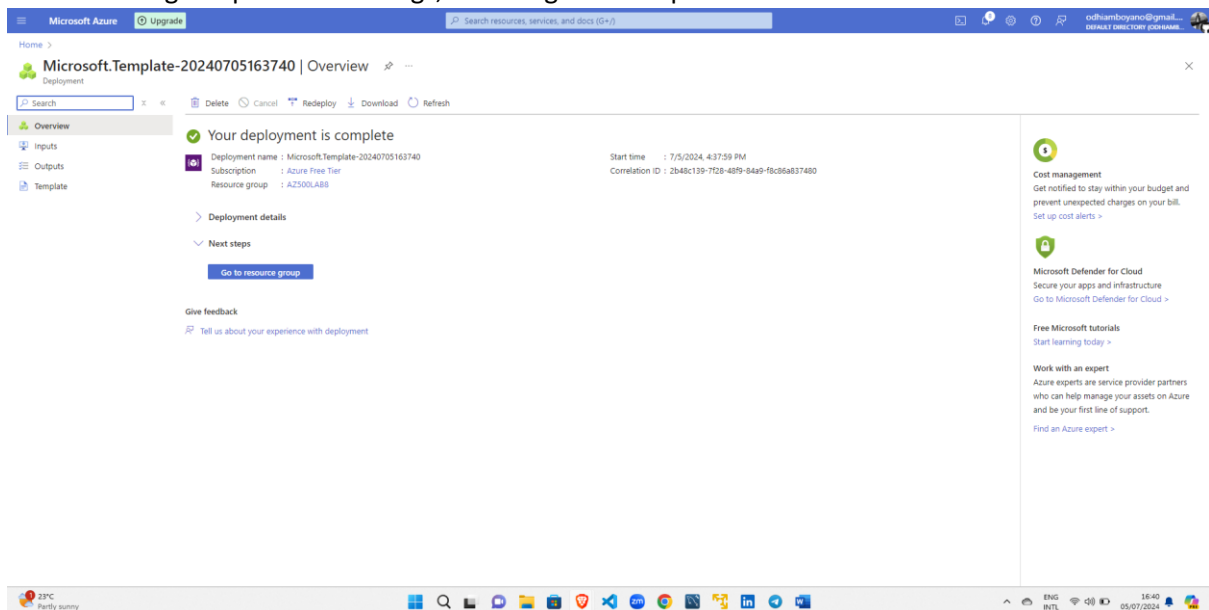
Report by: Tonny Odhiambo, CS-CNS06-24028

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.

The screenshot displays the Microsoft Azure portal interface. At the top, the header shows the Microsoft Azure logo, a search bar, and user information for 'odhiamboyano@gmail...'. The main content area is titled 'Microsoft.AzureFirewall-20240705165021 | Overview'. A sidebar on the left lists navigation options: Overview, Inputs, Outputs, and Template. The main panel features a 'Your deployment is complete' message with a green checkmark. Below this, deployment details are listed: Deployment name (Microsoft.AzureFirewall-20240705165021), Subscription (Azure Free Tier), Resource group (AZ500LAB8), Start time (7/5/2024, 4:50:55 PM), and Correlation ID (81f30edc-a172-4f3d-998e-6c9135b21923). A 'Go to resource' button is present. Further down, there are sections for 'Give feedback', 'Cost management' (with a 'Set up cost alerts' link), and 'Microsoft Defender for Cloud' (with a 'Go to Microsoft Defender for Cloud' link). The bottom of the screen shows a Windows taskbar with various application icons and system tray information including the time (16:58) and date (05/07/2024).

Home >

Microsoft Azure Search resources, services, and docs (G+)

odhiamboyano@gmail...
DEFAULT DIRECTORY (ODHIAMB...

Microsoft.AzureFirewall-20240705165021 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name : Microsoft.AzureFirewall-20240705165021
Subscription : Azure Free Tier
Resource group : AZ500LAB8
Start time : 7/5/2024, 4:50:55 PM
Correlation ID : 81f30edc-a172-4f3d-998e-6c9135b21923

> Deployment details

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

zm Chrome Task View LinkedIn Telegram Word ENG INTL 16:58 05/07/2024

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 screenshot shows the 'Create Route table' form in the Microsoft Azure portal. The form is divided into three tabs: 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is active. Under 'Project details', the 'Subscription' is set to 'Azure Free Tier' and the 'Resource group' is 'AZ500LAB8'. Under 'Instance details', the 'Region' is 'Canada Central' and the 'Name' is 'Firewall-route'. The 'Propagate gateway routes' option is set to 'Yes'.

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

Home > Route tables >

Create Route table

Basics Tags Review + create

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 Free Tier

Resource group * AZ500LAB8 [Create new](#)

Instance details

Region * Canada Central

Name * Firewall-route

Propagate gateway routes * ☒ Yes ☐ No

The deployment completed successfully.

The screenshot shows the 'Overview' page for the deployment 'Microsoft.RouteTable-20240705170713'. The page displays a success message: 'Your deployment is complete'. It lists the deployment details: 'Deployment name : Microsoft.RouteTable-20240705170713', 'Subscription : Azure Free Tier', 'Resource group : AZ500LAB8', 'Start time : 7/5/2024, 5:10:45 PM', and 'Correlation ID : 88ae00e7-4f9a-42fa-a5eb-3583606efee4'. There are also links for 'Deployment details' and 'Next steps', and a 'Go to resource' button.

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

Home >

Microsoft.RouteTable-20240705170713 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name : Microsoft.RouteTable-20240705170713

Subscription : Azure Free Tier

Resource group : AZ500LAB8

Start time : 7/5/2024, 5:10:45 PM

Correlation ID : 88ae00e7-4f9a-42fa-a5eb-3583606efee4

> Deployment details

Next steps

[Go to resource](#)

I then associated the Firewall to the virtual network subnet

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft.RouteTable-20240705170713 | Overview > Firewall-route

Firewall-route | Subnets

Route table

Search Associate

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Configuration
 - Routes
 - Subnets**

Search subnets

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

I then added a route to the Firewall

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft.RouteTable-20240705170713 | Overview > Firewall-route

Firewall-route | Routes

Route table

Search Add Refresh Give feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Configuration
 - Routes**

Search routes

Name ↑↓	Address prefix ↑↓	Next hop type ↑↓	Next hop IP address ↑↓
FW-DG	0.0.0.0/0	VirtualAppliance	10.0.1.4

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.

The screenshot shows the 'Add application rule collection' form in the Microsoft Azure portal. The form is titled 'Add application rule collection' and has a close button (X) in the top right corner. The form fields are as follows:

- Name ***: App-Coll01 (with a green checkmark)
- Priority ***: 200 (with a green checkmark)
- Action ***: Allow (with a dropdown arrow)
- Rules**: A section for adding rules, currently empty.
- FQDN tags**: A table with columns: name, Source type, Source, and FQDN tags. The table is currently empty.
- Target FQDNs**: A table with columns: name, Source type, Source, Protocol:Port, and Target FQDNs. The table contains two rows:
 - Row 1: name: AllowGH (with a green checkmark), Source type: IP address (with a dropdown arrow), Source: 10.0.2.0/24 (with a green checkmark), Protocol:Port: http:80, https:443 (with a green checkmark), Target FQDNs: www.bing.com (with a green checkmark).
 - Row 2: name: (empty), Source type: IP address (with a dropdown arrow), Source: *, 192.168.10.1, 192.168.10.0/24... (with a green checkmark), Protocol:Port: http, http:8080, https, m... (with a green checkmark), Target FQDNs: www.microsoft.com, *... (with a green checkmark).

Below the tables, there are two informational messages:

- FQDN tags**: FQDN tags may require additional configuration. [Learn more](#)
- mssql**: SQL should be enabled in proxy mode. This may require additional configuration. [Learn more](#)

I configured the rule and added it successfully

The screenshot shows the 'Test-FW01 | Rules (classic)' page in the Microsoft Azure portal. The page is titled 'Test-FW01 | Rules (classic)' and has a close button (X) in the top right corner. The page layout is as follows:

- Navigation pane**: A sidebar on the left with the following items: Overview, Activity log, Access control (IAM), Tags, Settings, DNS, Rules (classic) (selected), Public IP configuration, Learned SNAT IP Prefixes (preview), and Threat intelligence.
- Header**: A blue header bar with the Microsoft Azure logo, a search bar, and user information (odhiamboyano@gmail.com, DEFAULT DIRECTORY (ODHIAMB...)).
- Breadcrumbs**: Home > Firewall Manager | Azure Firewalls > Test-FW01
- Content area**: The main content area shows the 'Rules (classic)' view for 'Test-FW01'. It includes a search bar, a 'Refresh' button, and a list of rules. The 'Application rule collection' tab is selected, showing a table with columns: Priority, Name, Action, and Rules. The table contains one rule: Priority: 200, Name: App-Coll01, Action: Allow, Rules: > 1 rule. (with a green checkmark). Below the table, there is an informational message: Azure infrastructure application rule collection is enabled by default. [Learn more](#)

Task 5: Configure a Network Rule

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

The screenshot shows the 'Add network rule collection' dialog in the Microsoft Azure portal. The dialog has a blue header with the Microsoft Azure logo and a search bar. Below the header, there are fields for 'Name *' (Net-Coll01), 'Priority *' (200), and 'Action *' (Allow). Below these fields, there is a 'Rules' section with a table of IP addresses. The table has columns for 'name', 'Protocol', 'Source type', 'Source', 'Destination type', 'Destination Addr...', and 'Des'. The first row shows 'AllowDNS' (checked), 'UDP', 'IP address', '10.0.2.0/24' (checked), 'IP address', '209.244.0.3, 209.2...', and '53'. The second row shows '0 selected', '0 selected', 'IP address', '*', '192.168.10.1, 192...', 'IP address', '*', '192.168.10.1, 192...', and '808'. Below the table, there is a 'Service Tags' section.

name	Protocol	Source type	Source	Destination type	Destination Addr...	Des
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...	808

It was successfully added as shown below.

The screenshot shows the 'Test-FW01 | Rules (classic)' page in the Microsoft Azure portal. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there is a breadcrumb trail: 'Home > Firewall Manager | Azure Firewalls > Test-FW01'. The main content area shows the 'Test-FW01 | Rules (classic)' page. On the left, there is a sidebar with navigation links: 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Settings', 'DNS', and 'Rules (classic)'. The 'Rules (classic)' link is selected. The main content area shows a table of rules. The table has columns for 'Priority', 'Name', 'Action', and 'Rules'. The first row shows '200', 'Net-Coll01', 'Allow', and '> 1 rule.'. There is also a '+ Add network rule collection' link.

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

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.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information for 'odhiamboyano@gmail...'. The breadcrumb trail indicates the path: Home > Resource groups > AZ500LAB8 > Srv-Work | Network settings > srv-work267. The main heading is 'srv-work267 | DNS servers', with a subheading 'Network interface'. A search bar and 'Save'/'Discard' buttons are present. The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Settings (expanded), IP configurations, DNS servers (selected), Network security group, Properties, Locks, Monitoring, Automation, and Help. The main content area features a warning message about DNS updates, a 'DNS servers' section with 'Inherit from virtual network' and 'Custom' options (the latter is selected), a table of DNS servers (209.244.0.3 and 209.244.0.4), and an 'Applied DNS servers' section with a descriptive note and a list of the same two IP addresses.

Microsoft Azure Search resources, services, and docs (G+)

Home > Resource groups > AZ500LAB8 > Srv-Work | Network settings > srv-work267

srv-work267 | DNS servers Network interface

Search Save Discard

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

Locks

Monitoring

Automation

Help

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

Applied DNS servers ⓘ

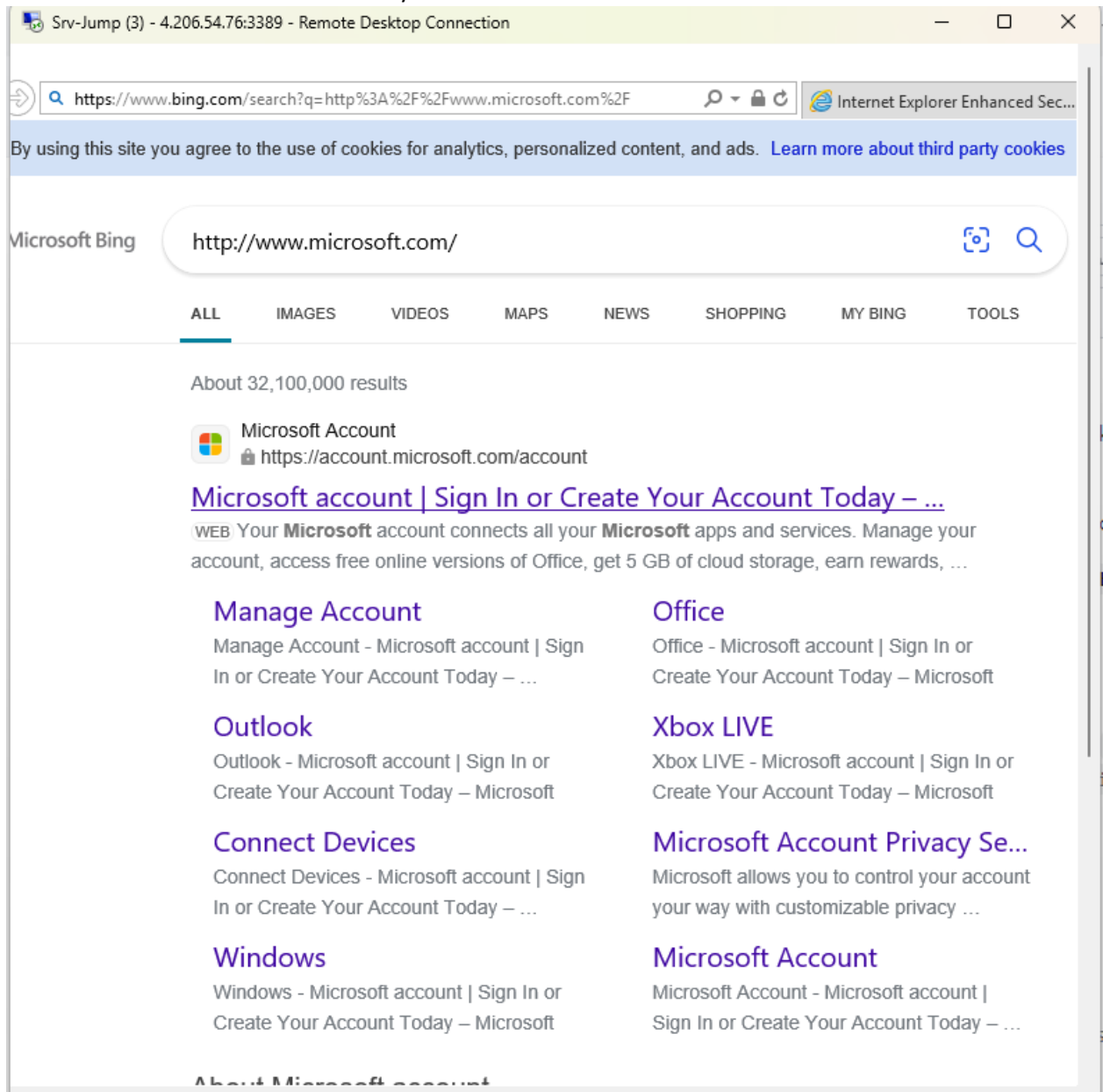
For virtual machines in an availability set, the list of applied DNS servers is the union of all DNS servers from all network interfaces that are a part of the availability set.

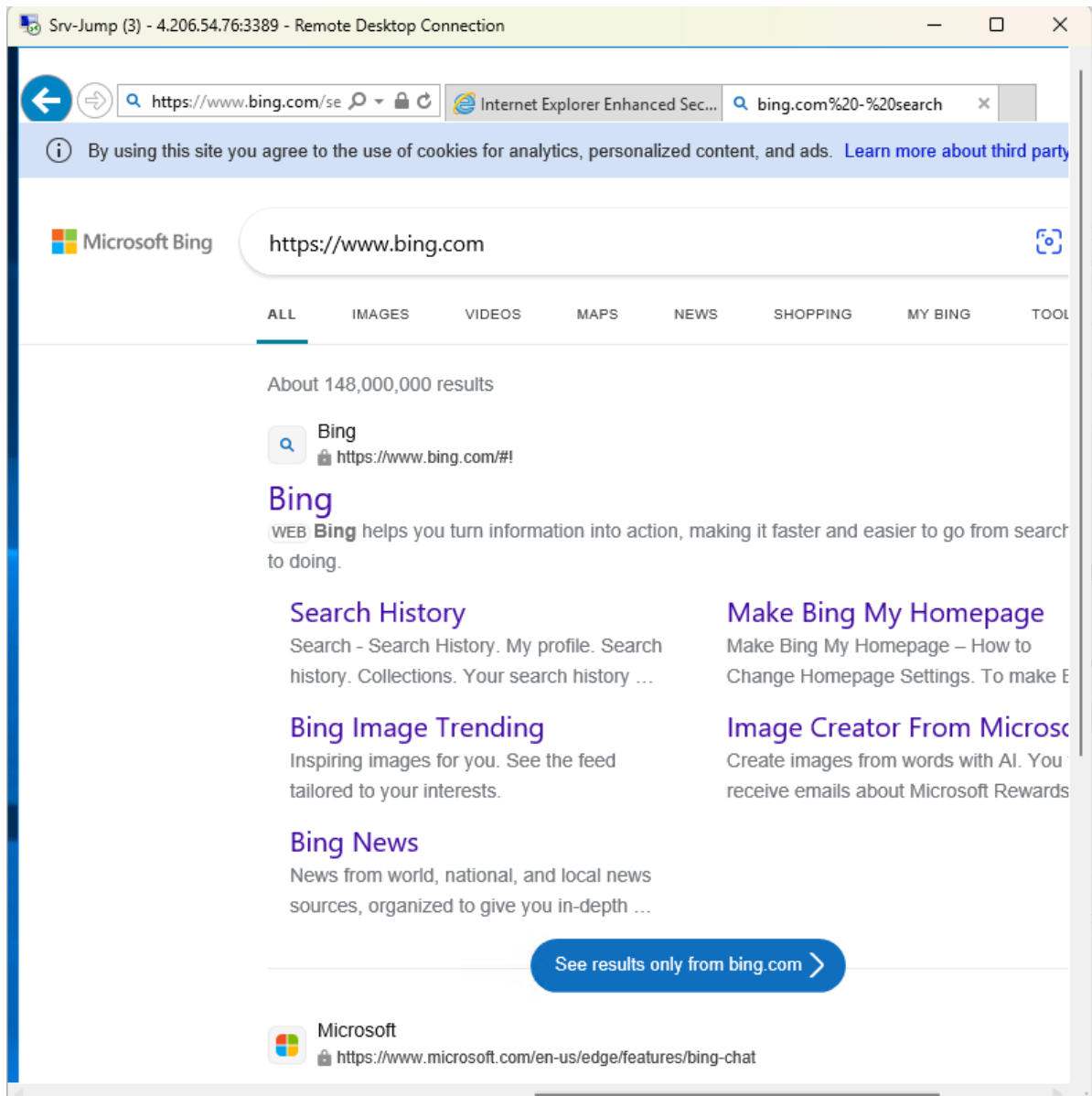
Applied DNS servers

209.244.0.3
209.244.0.4

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.



odhiamboyano@gmail...
DEFAULT DIRECTORY (ODHIAMB...



Notifications

[More events in the activity log →](#)[Dismiss all](#) 



Deleted resource group NetworkWatcherRG
Deleted resource group NetworkWatcherRG



6 minutes ago



Deleted resource group NetworkWatcherRG
Deleted resource group NetworkWatcherRG



6 minutes ago



Deleted resource group AZ500LAB08
Deleted resource group AZ500LAB08



8 minutes ago



Deleted resource group AZ500LAB8
Deleted resource group AZ500LAB8



an hour ago

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.