ASSIGNMENT TWO: AZURE FIREWALL WRITEUP

BY CS-CNS03-23082 – ABUOR ISABELLA MERCY

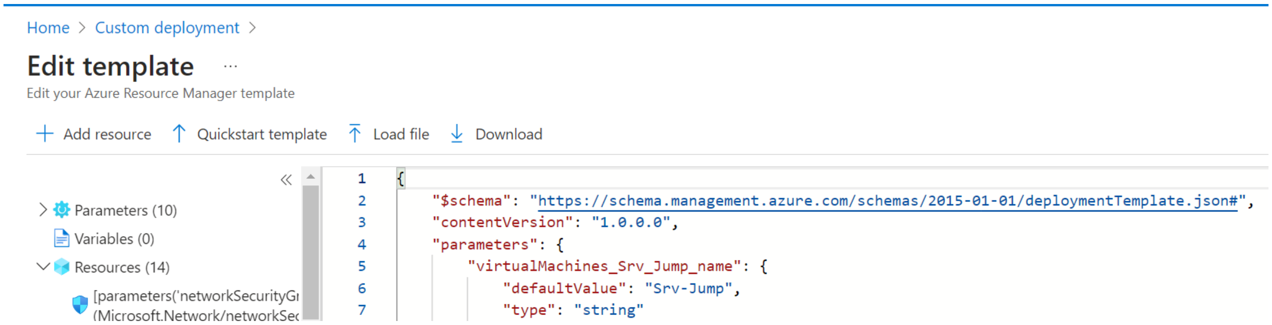
INTRODUCTION

This guided exercise embarks on a journey through seven tasks. guides the deployment and configuration of essential components. Starting with the utilization of a template for environment deployment, the tasks proceed to establish an Azure firewall, set up a default route, and configure both application and network rules. Further steps involve the configuration of DNS servers and culminate in a comprehensive firewall test to ensure its effective functionality. The following is a descriptive of a step-by-step procedure of how the tasks were achieved.

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

This task shows the steps we took to review and deploy the lab environment. We created a virtual machine by using an ARM template. We used the build your own template in the editor option on deploy a custom template page.

On the Edit template blade, Loaded the file \Allfiles\Labs\08\template.json file and clicked Open and saved.

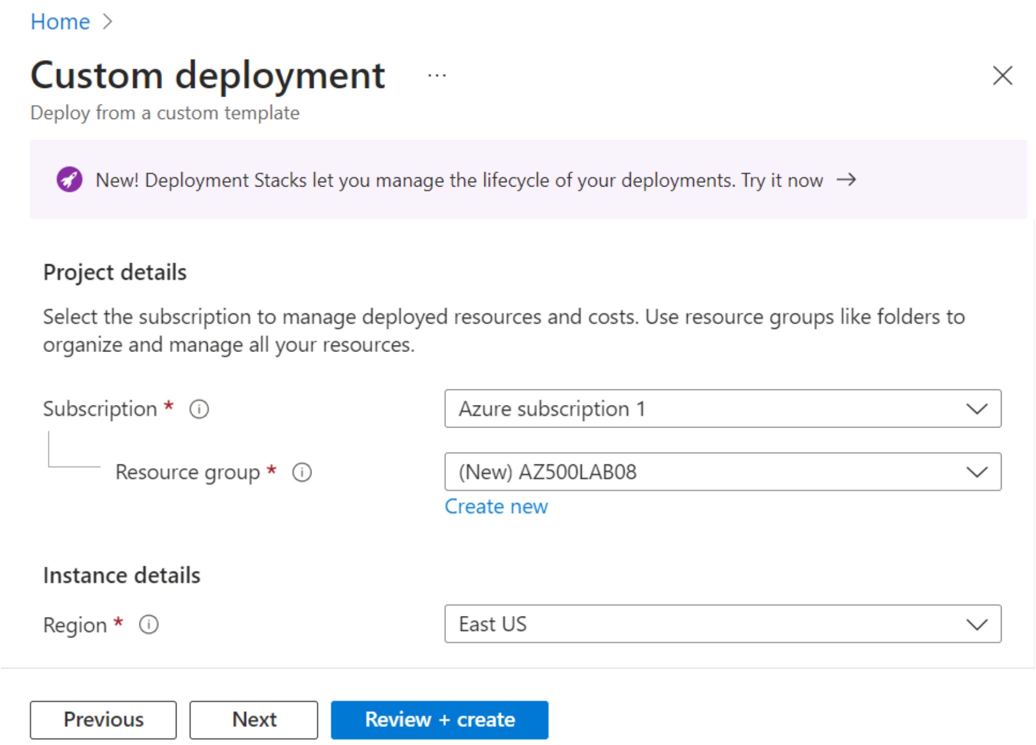


Edit template

Edit your Azure Resource Manager template

```
{
    "$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"
```

On the Custom deployment blade, the following settings were configured as follows:



Home >

Custom deployment

Deploy from a custom template

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

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 *	(New) AZ500LAB08

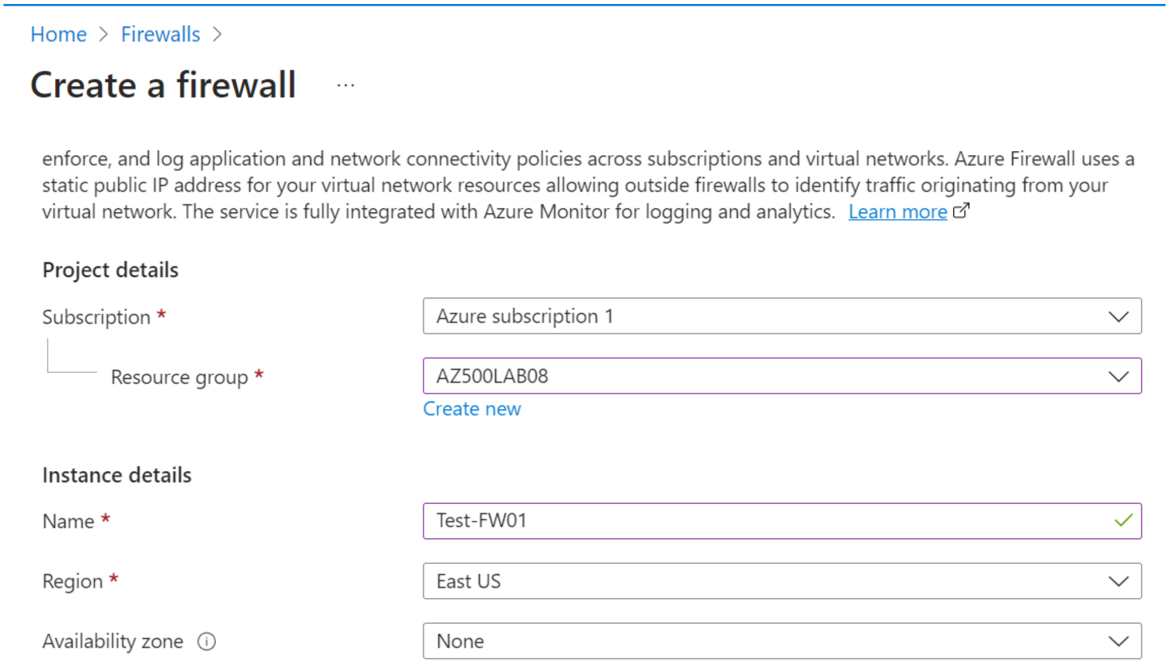
Create new

Instance details

Region *	East US

Task 2: Deploy the Azure firewall

This task describes a step-by-step process of deploying the Azure firewall into the virtual network. On the Firewalls page, created a new firewall and specified the following settings:



Home > Firewalls >

Create a firewall

enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a 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

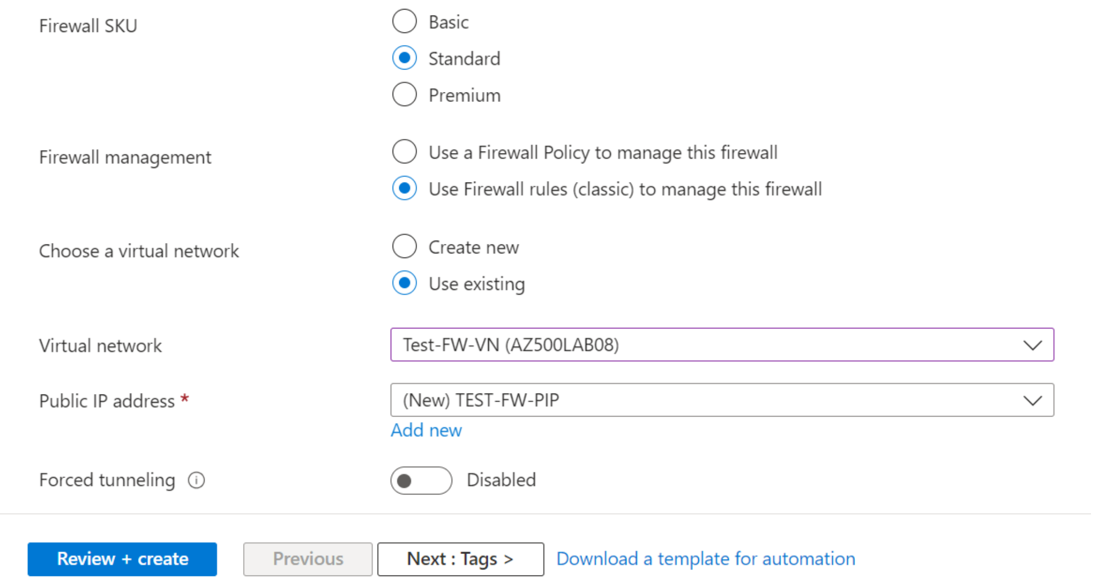
Project details

Subscription *	Azure subscription 1
Resource group *	AZ500LAB08

Create new

Instance details

Name *	Test-FW01
Region *	East US
Availability zone	None



Firewall SKU
○ Basic
● Standard
○ Premium

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

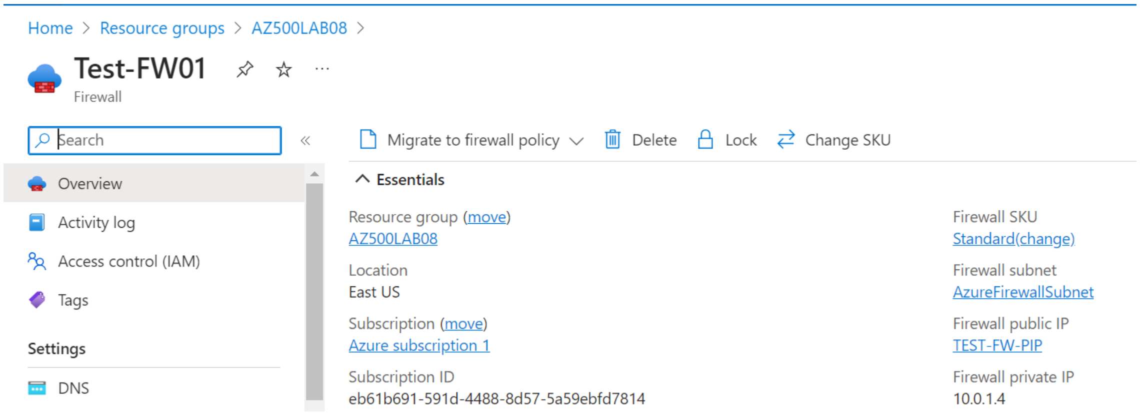
Choose a virtual network
○ Create new
● Use existing

Virtual network: Test-FW-VN (AZ500LAB08)

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

Forced tunneling: Disabled

On the Resource groups blade, in the list of resource group, clicked the AZ500LAB08 entry clicked the entry representing the Test-FW01 firewall on the list of resources. On the Test-FW01 blade, identify the Private IP address that was assigned to the firewall.



Home > Resource groups > AZ500LAB08 >

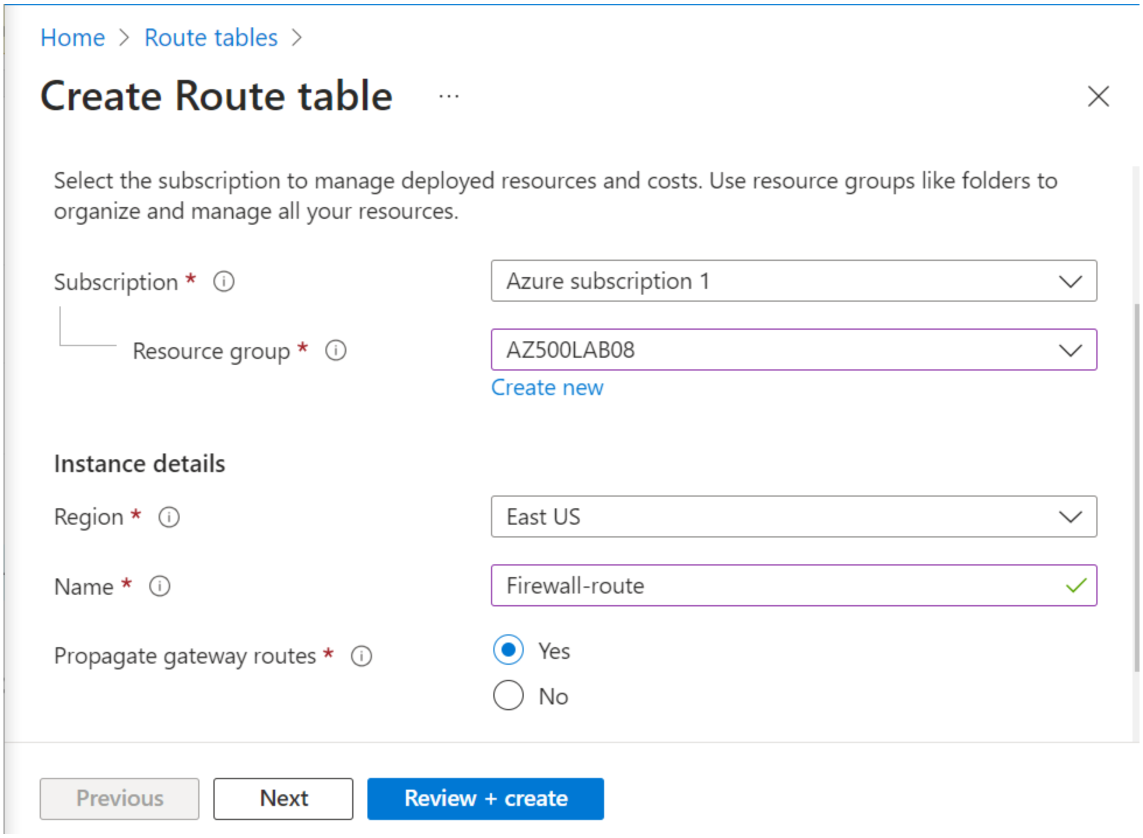
Test-FW01
Firewall

Essentials

Resource group (move) AZ500LAB08	Firewall SKU Standard(change)
Location East US	Firewall subnet AzureFirewallSubnet
Subscription (move) Azure subscription 1	Firewall public IP TEST-FW-PIP
Subscription ID eb61b691-591d-4488-8d57-5a59ebfd7814	Firewall private IP 10.0.1.4

Task 3: Create a default route

In this task, we created a default route for the Workload-SN subnet. This route will configure outbound traffic through the firewall. On the Route tables blade, we created a route table blade with the specific settings:



Home > Route tables >

Create Route table

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 * : AZ500LAB08

Create new

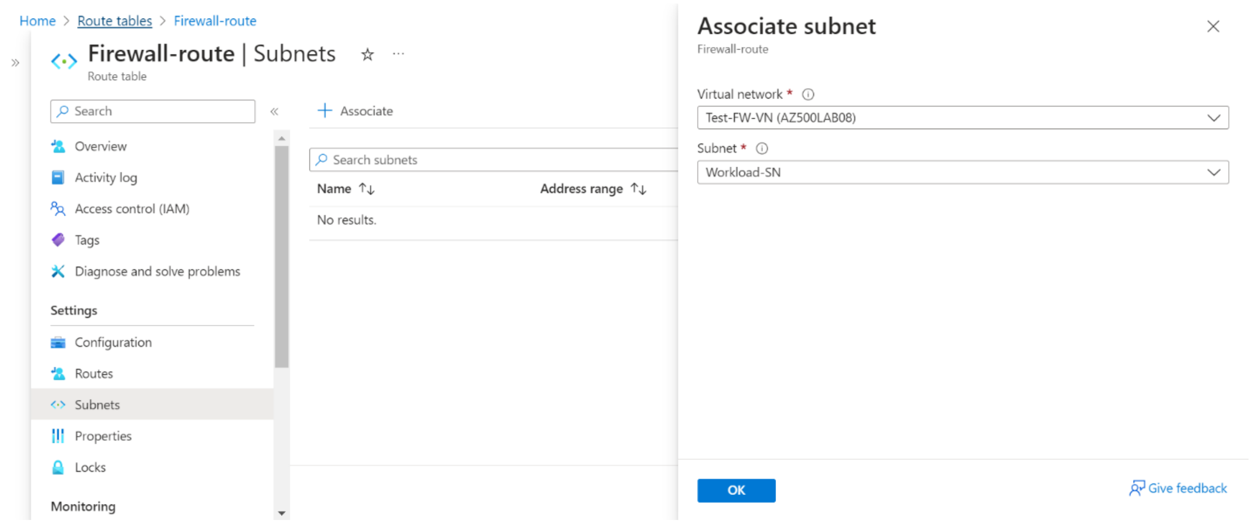
Instance details

Region * : East US

Name * : Firewall-route

Propagate gateway routes * : ● Yes ○ No

On the Route tables blade, click Refresh, and, in the list of route tables, click the Firewall-route entry. On the Firewall-route blade, in the Settings section, clicked on Subnets and then, on the Firewall-route | Subnets blade, click + Associate and specify the following settings:



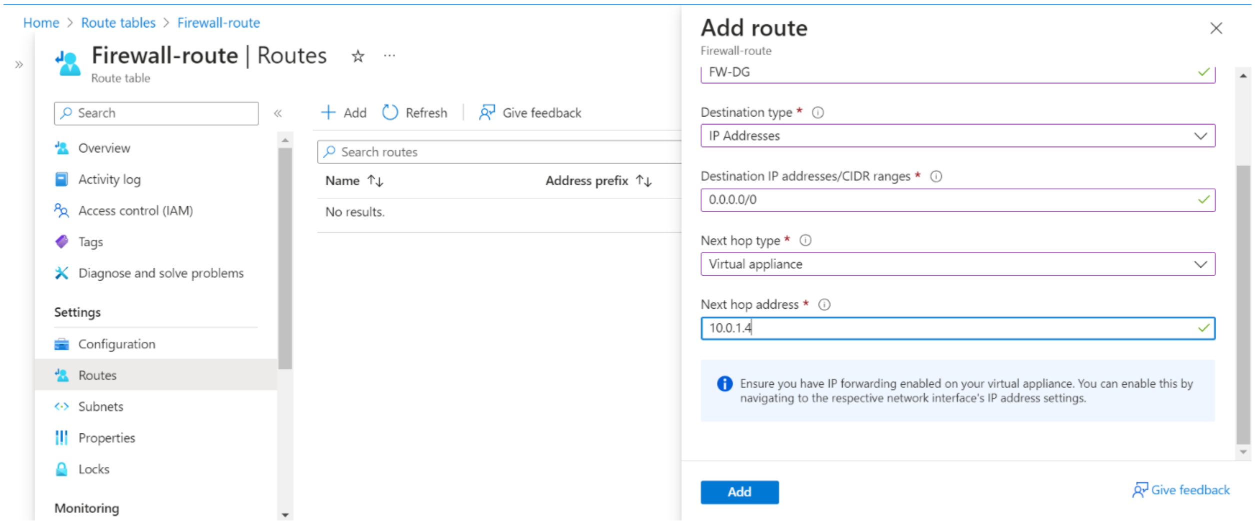
Associate subnet

Firewall-route

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

Subnet * : Workload-SN

Back on the Firewall-route blade, in the Settings section, click Routes and then click + Add and specify the following settings:



Add route

Firewall-route

FW-DG

Destination type * : IP Addresses

Destination IP addresses/CIDR ranges * : 0.0.0.0/0

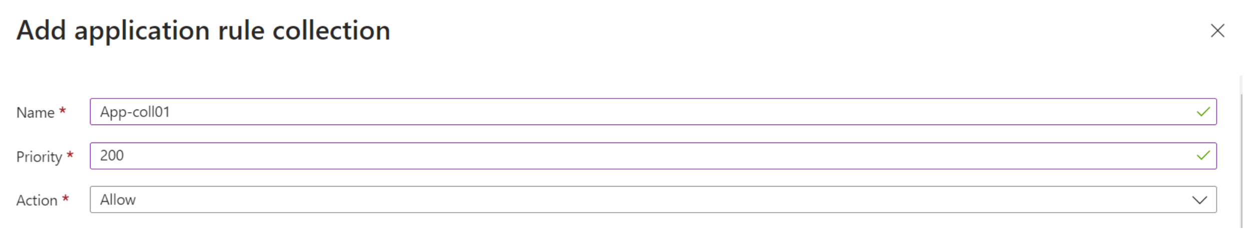
Next hop type * : Virtual appliance

Next hop address * : 10.0.1.4

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Task 4: Configure an application rule

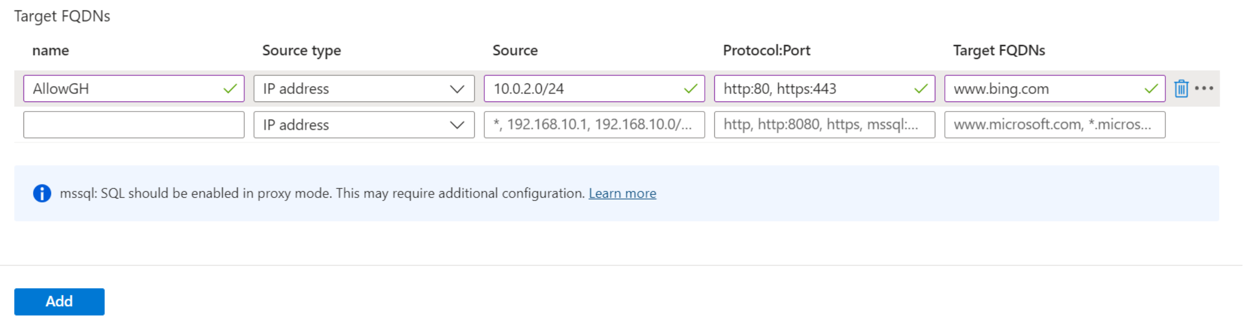
In this task we created an application rule that allows outbound access to www.bing.com. On the Test-FW01 blade, in the Settings section, click Rules (classic) and clicked the Application rule collection tab, and then click + Add application rule collection and specify the following settings:



Add application rule collection

Name *	App-coll01
Priority *	200
Action *	Allow

On the Add application rule collection blade, create a new entry in the Target FQDNs section with the following settings:



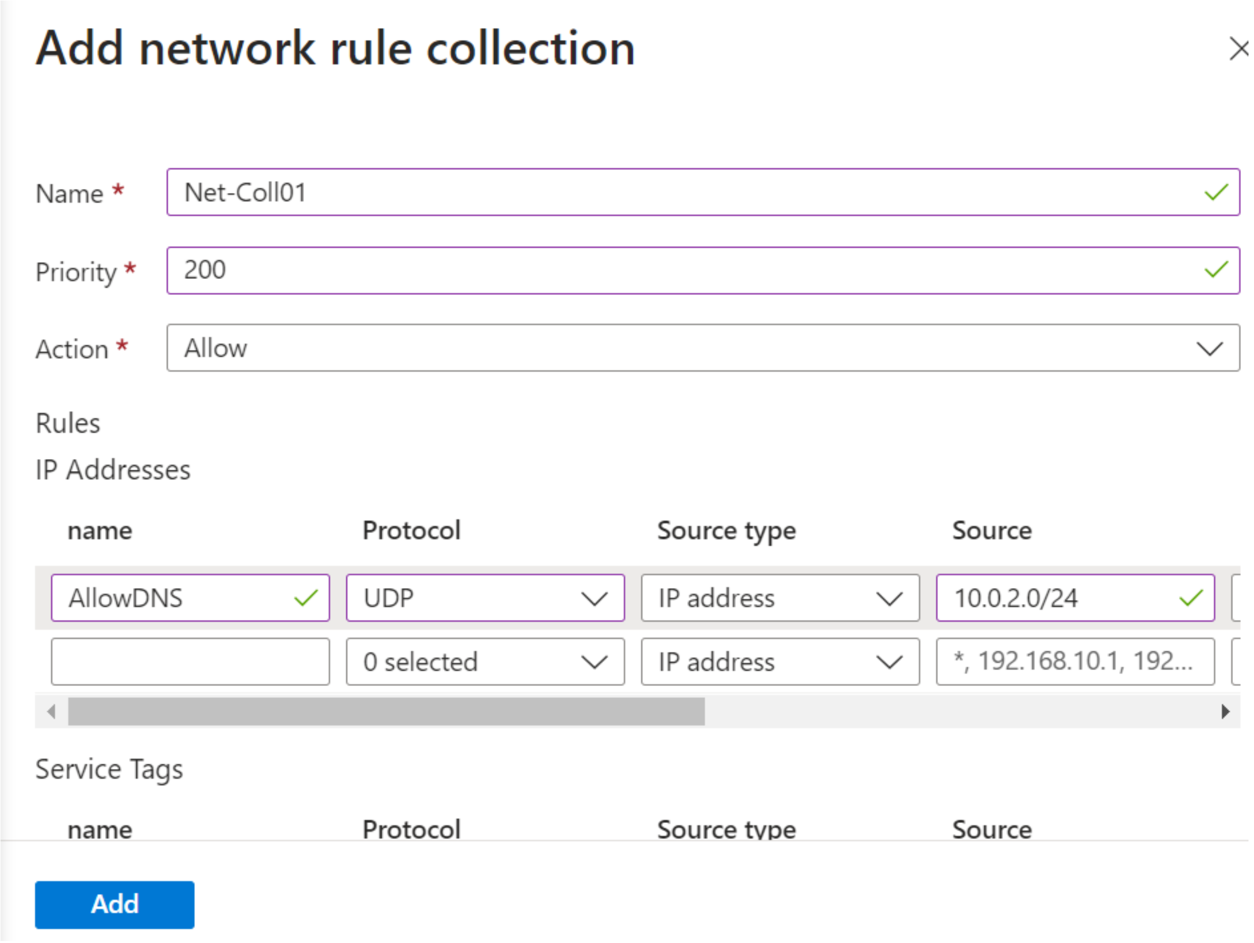
Target FQDNs

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...

mssql: SQL should be enabled in proxy mode. This may require additional configuration. Learn more

Task 5: Configure a network rule

In this task, we created a network rule that allows outbound access to two IP addresses on port 53 (DNS). On the Test-FW01 | Rules (classic) blade, click the Network rule collection tab and then click + Add network rule collection and specify the following settings:



Add network rule collection

Name * Net-Coll01

Priority * 200

Action * Allow

Rules

IP Addresses

name	Protocol	Source type	Source
AllowDNS	UDP	IP address	10.0.2.0/24
	0 selected	IP address	*, 192.168.10.1, 192...

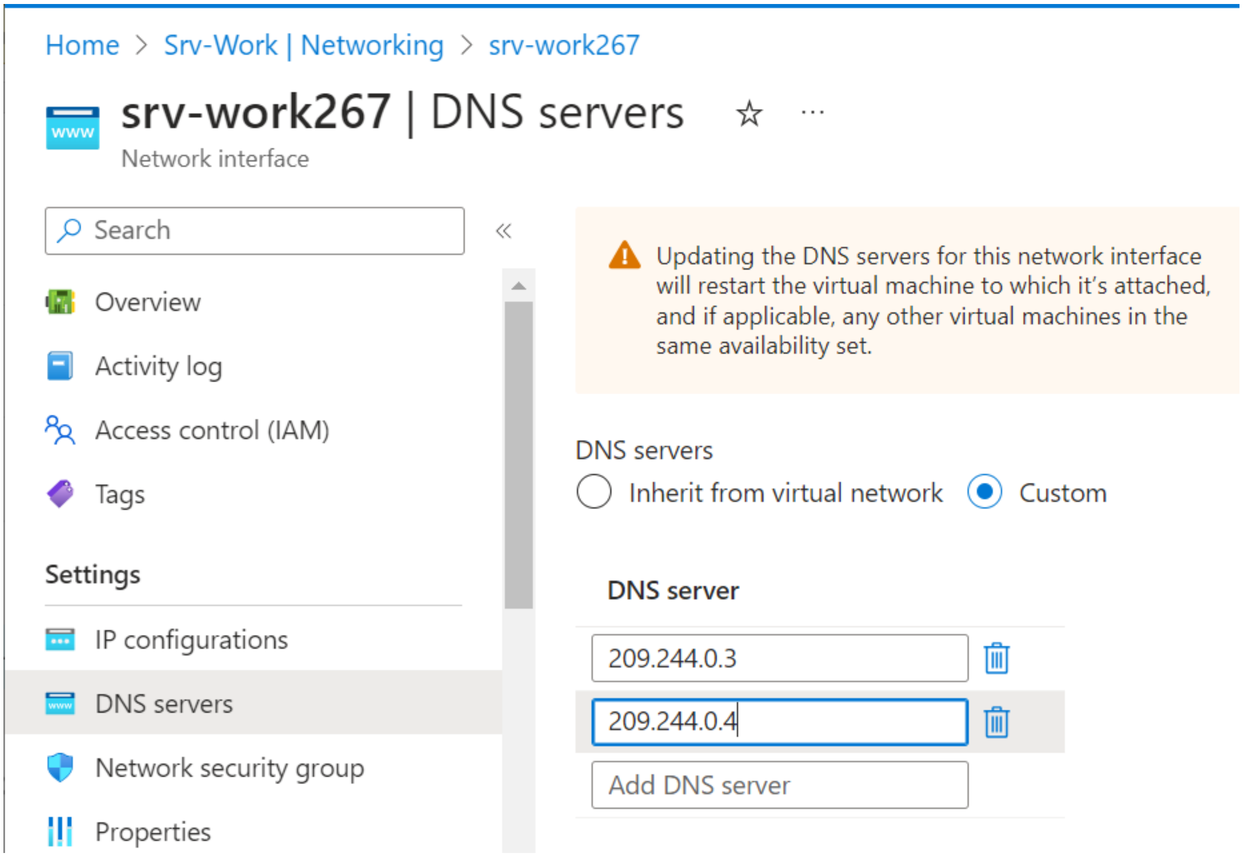
Service Tags

name	Protocol	Source type	Source

Task 6: Configure the virtual machine DNS servers

In this task, we configured the primary and secondary DNS addresses for the virtual machine. On the AZ500LAB08 blade, in the list of resources, clicked the Srv-Work virtual machine, in the Settings section, click Networking. Clicked the link next to the Network interface entry.

On the network interface blade, in the Settings section, clicked on DNS servers, selected the Custom option and added 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.



Home > Srv-Work | Networking > srv-work267

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

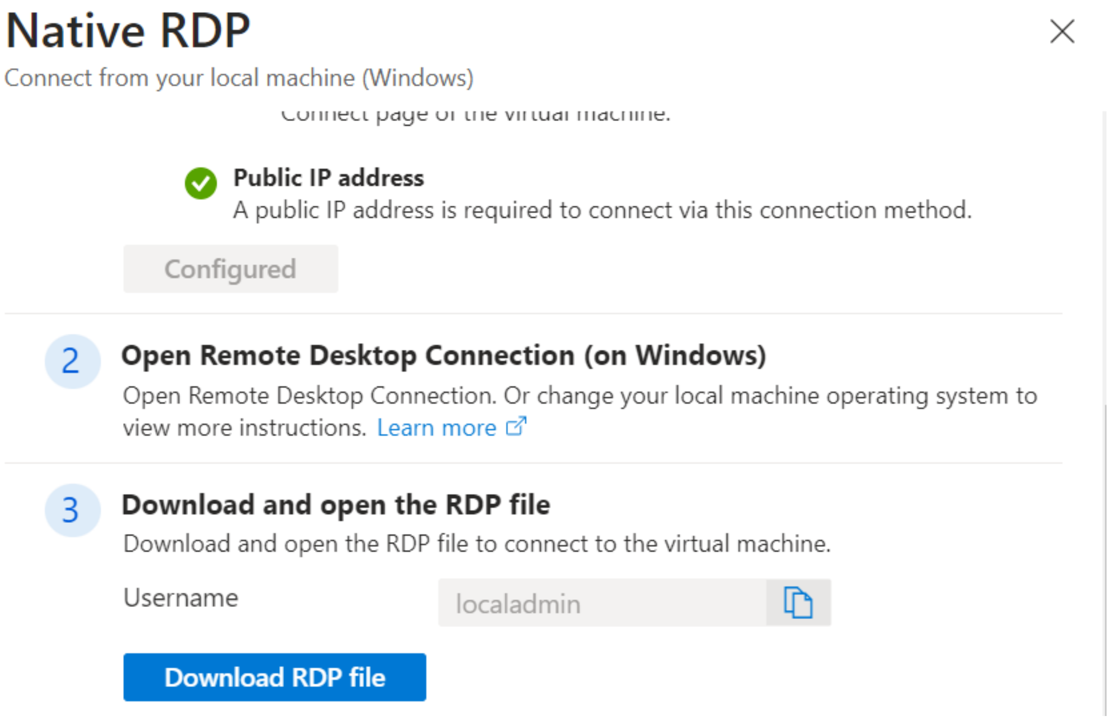
209.244.0.3

209.244.0.4

Add DNS server

Task 7: Test the firewall

In this task, we test the firewall to confirm that it works as expected. On the AZ500LAB08 blade, in the list of resources, clicked the Srv-Jump virtual machine and on the Srv-Jump blade, connected it and, clicked RDP to download the RDP file to share with the remote desktop to connect to the Srv-Jump.



Native RDP

Connect from your local machine (Windows)

Connect page of the virtual machine.

✓ **Public IP address**

A public IP address is required to connect via this connection method.

2 **Open Remote Desktop Connection (on Windows)**

Open Remote Desktop Connection. Or change your local machine operating system to view more instructions. Learn more

3 **Download and open the RDP file**

Download and open the RDP file to connect to the virtual machine.

Username: localadmin

CONCLUSION

In conclusion, learning how to set up and build a strong Azure firewall was a seamless process and I was surprised as how configuring firewalls were simple. The lab assignment also come with its challenges especially in task 7 where we were testing the firewall, since I personally lacked a second desktop hence testing was incomplete but overall, the assignment was a success. Additionally, I was ale to see the theory brought into practice when we were setting up two DNS for redundancy and resilience.