Task - 10

Azure Firewall

Prepare R & D Documentation about Azure Firewall

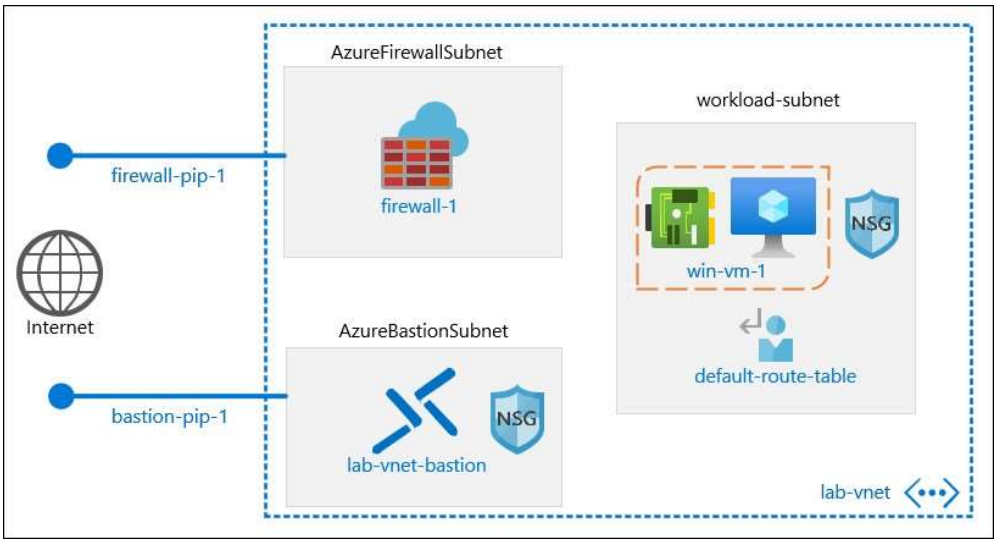
Ananya Srivastava
CLOUD INFRA

Table of Contents

1. Introduction

Azure Firewall is a managed, cloud-based network security service that protects Azure Virtual Network resources. It provides comprehensive network and application-level protection across different subscription boundaries. This documentation explores the capabilities, deployment, configuration, and management of Azure Firewall, along with practical exercises to demonstrate its functionalities.

Azure Firewall is a comprehensive, managed, cloud-based network security service designed to protect resources in Azure Virtual Networks. It acts as a central security policy enforcement point, providing robust control over inbound and outbound network traffic. With its built-in high availability and unrestricted cloud scalability, Azure Firewall ensures seamless and efficient security management across diverse and complex environments. Its key features include threat intelligence-based filtering, application FQDN filtering rules, and extensive logging and analytics. These features enable organizations to enhance visibility, detect threats, and respond promptly to security incidents. Azure Firewall supports both network and application-level filtering, allowing for granular control over traffic based on various parameters such as IP addresses, ports, protocols, and fully qualified domain names (FQDNs). Additionally, it integrates smoothly with Azure Monitor, offering comprehensive logging, monitoring, and alerting capabilities to ensure continuous security posture visibility. By leveraging Azure Firewall, businesses can centralize their network security, simplify management, and strengthen their overall security posture, thereby safeguarding their critical applications and data in the cloud.



2. Overview of Azure Firewall

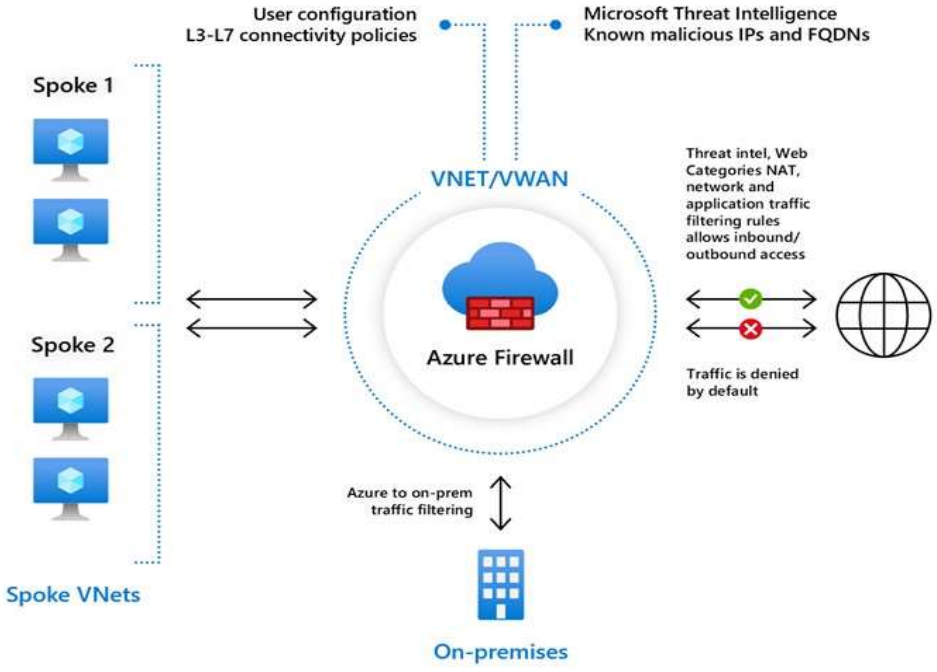
Key Features

- **High Availability**: Azure Firewall is built-in high availability and requires no additional load balancer.
- **Unrestricted Cloud Scalability**: The firewall can scale up as per the requirements.
- **Application FQDN Filtering Rules**: Allows users to restrict outbound HTTP/S traffic based on the fully qualified domain names (FQDN).

- **Threat Intelligence**: Leverages Microsoft threat intelligence to alert or block known malicious IP addresses and domains.

Benefits

- **Centralized Network Security**: Provides centralized security policy management.
- **Enhanced Visibility**: Offers extensive logging and analytics for better monitoring and threat detection.
- **Simplified Management**: Managed service that eliminates the need for complex setup and maintenance.



3. Azure Firewall Deployment

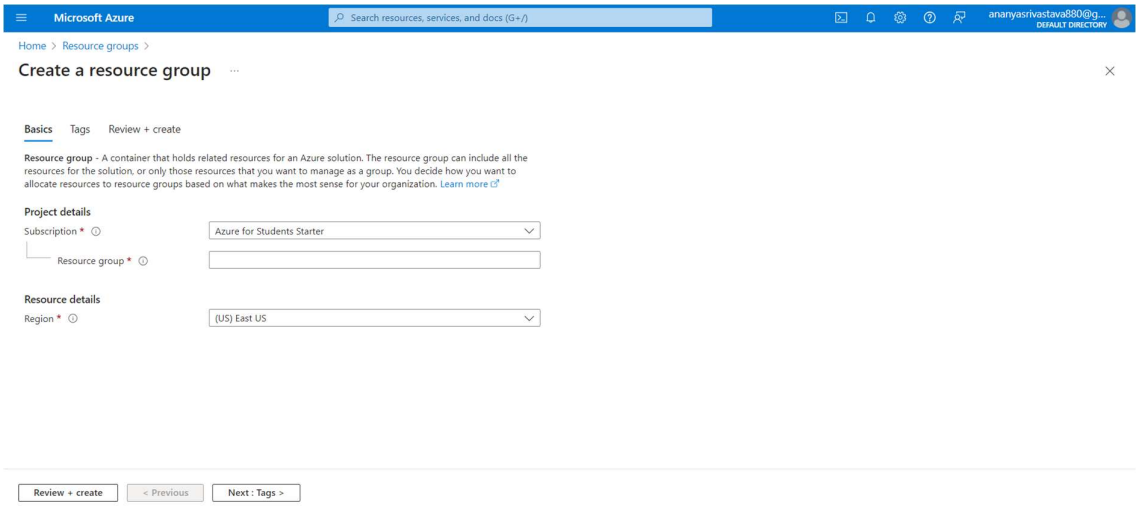
Prerequisites

- Azure subscription
- Virtual Network (VNet) set up
- Subnet for Azure Firewall

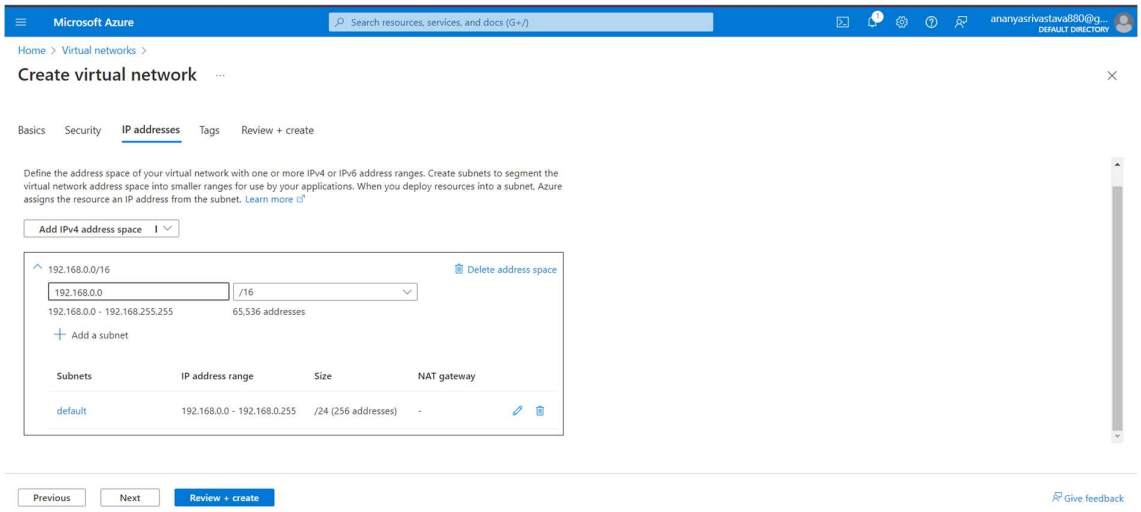
Step-by-Step Deployment Guide

1. **Create a Virtual Network (VNet)**

- Go to the Azure portal, navigate to 'Create a resource' > 'Networking' > 'Virtual Network'.

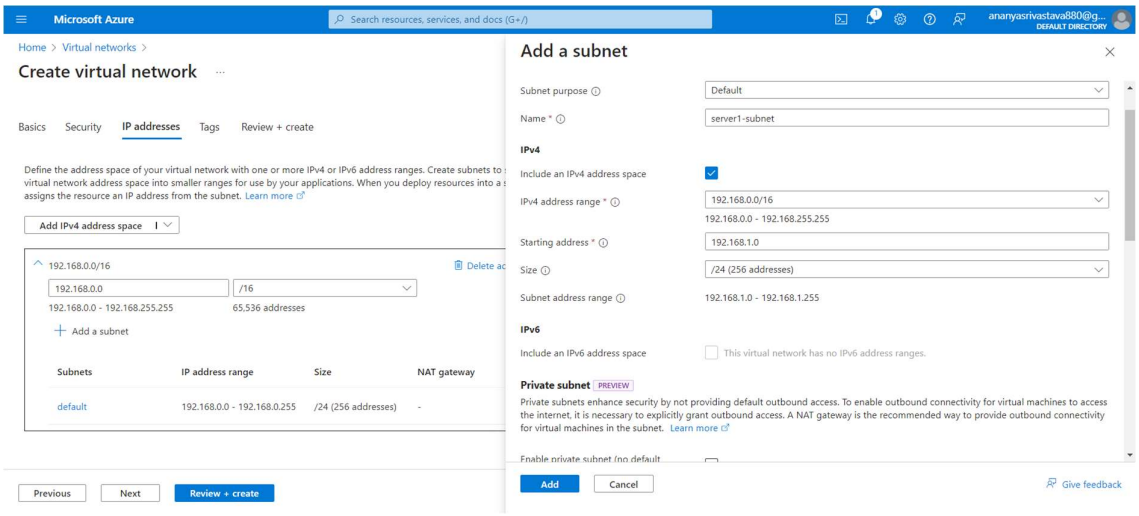


- Fill in the required fields and create a VNet.

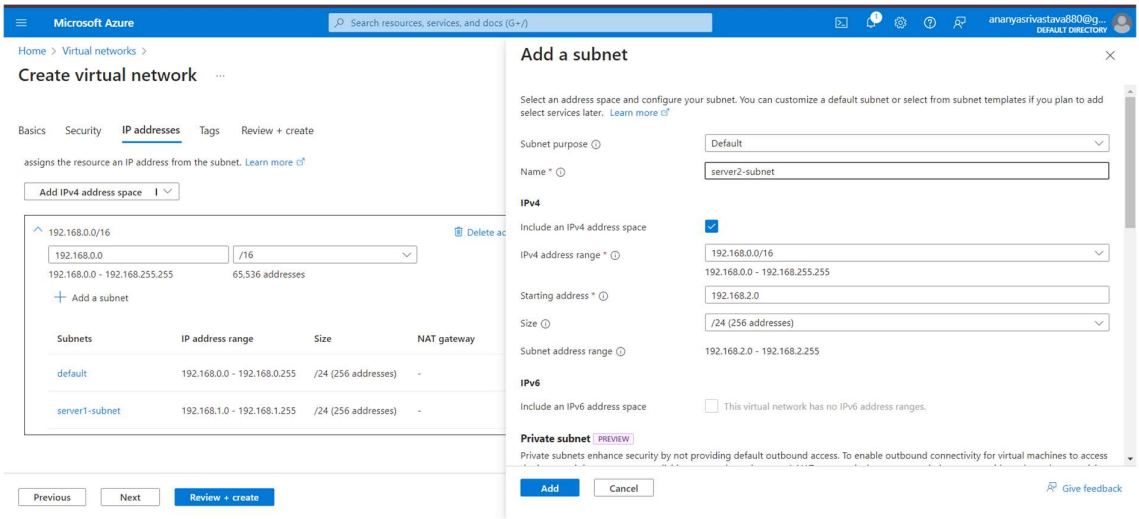


2. Create a Subnet for Azure Firewall

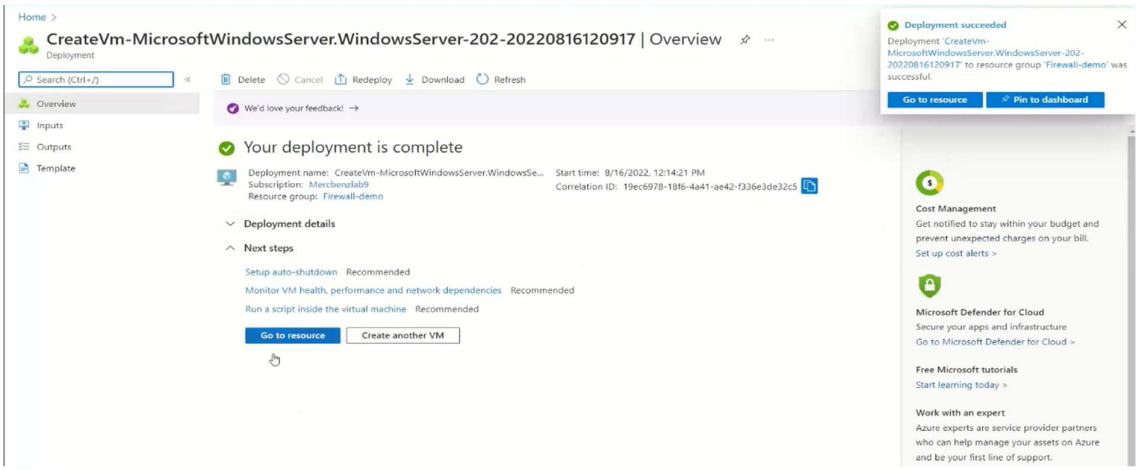
- Within the created VNet, add a first-subnet named 'server1-subnet'.



- Add a second-subnet named 'server2-subnet'.



3. Deploy Virtual Machine



4. **Deploy Azure Firewall**
    - Go to 'Create a resource' > 'Networking' > 'Azure Firewall'.
    - Fill in the necessary details, select the previously created VNet and subnet, and create the firewall.

4. Configuring Azure Firewall

Network Rules

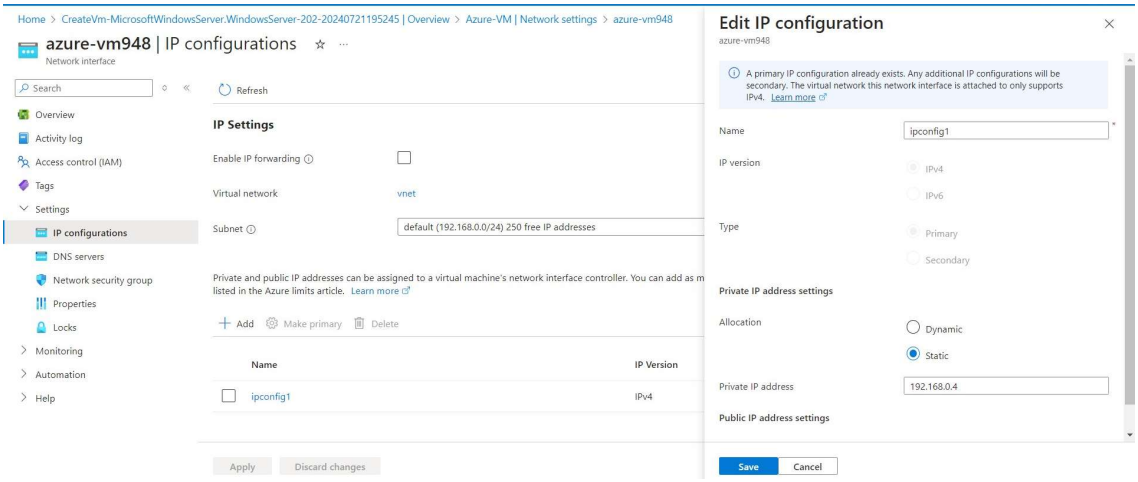
- **Create network rules** to allow or deny traffic based on source and destination IP addresses, ports, and protocols.

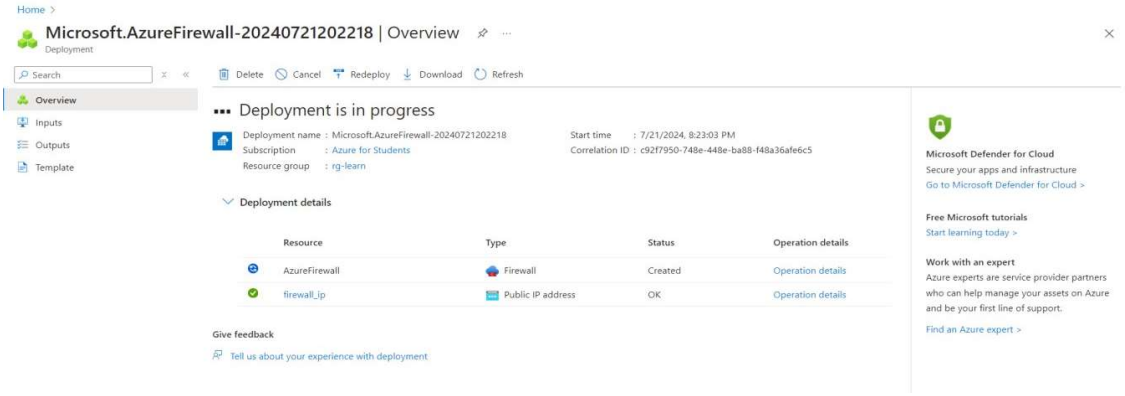
Application Rules

- **Application rules** enable the firewall to filter outbound HTTP/S traffic by FQDN.

NAT Rules

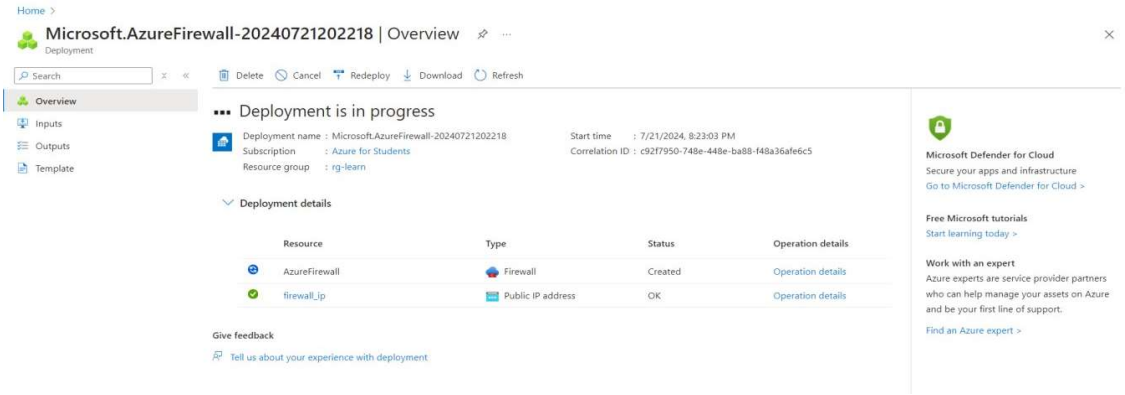
- **NAT rules** define how to translate traffic to the internal network.

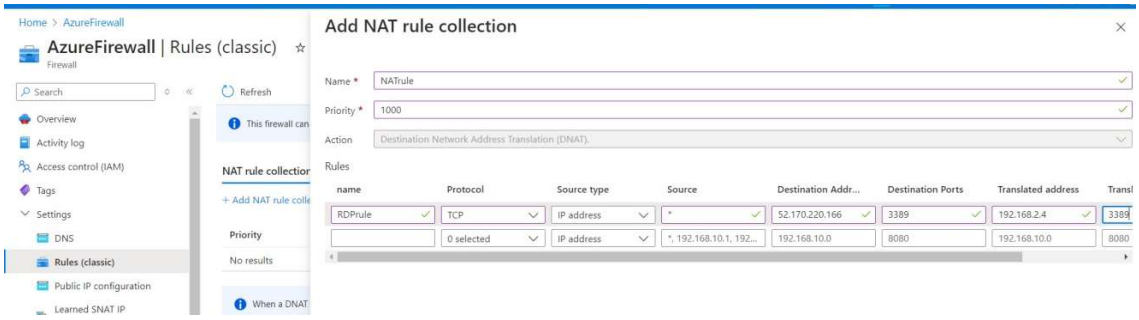




5. Create Azure Firewall Resource:

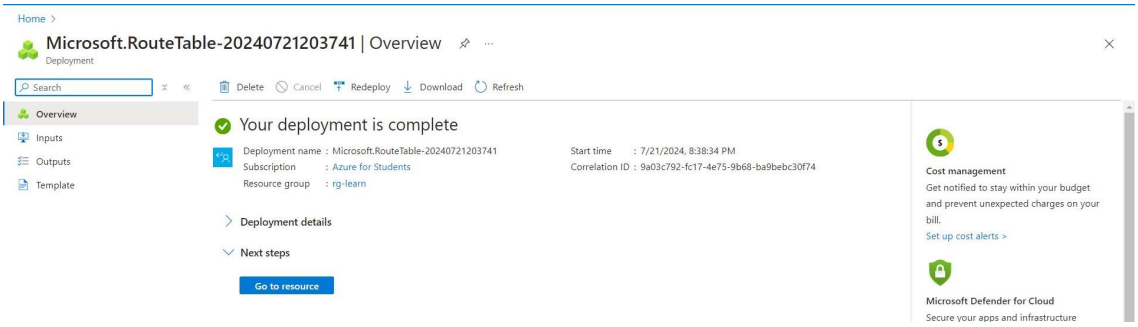
Navigate to the Azure Portal and create a new Azure Firewall instance. Specify the resource group, name, and region. Add NAT rules

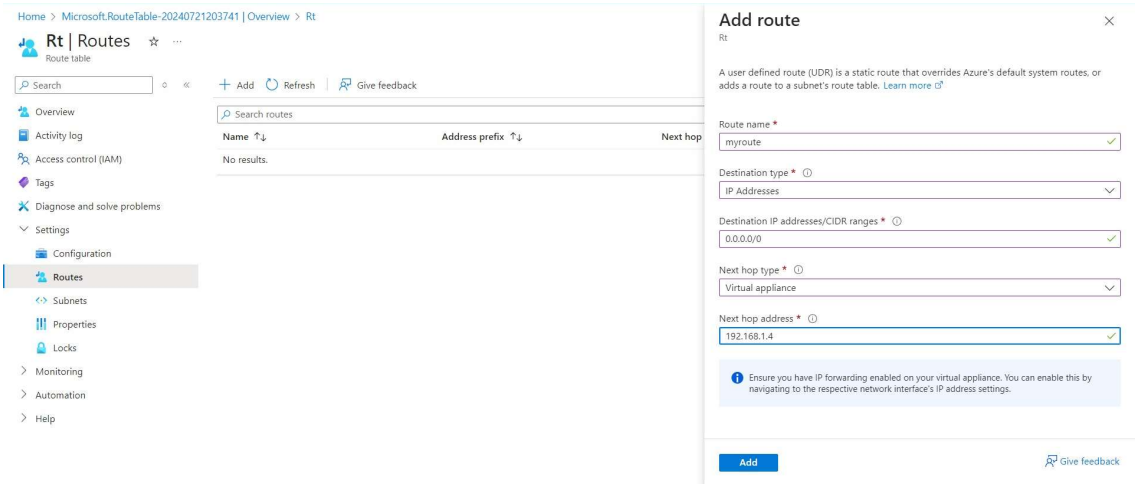


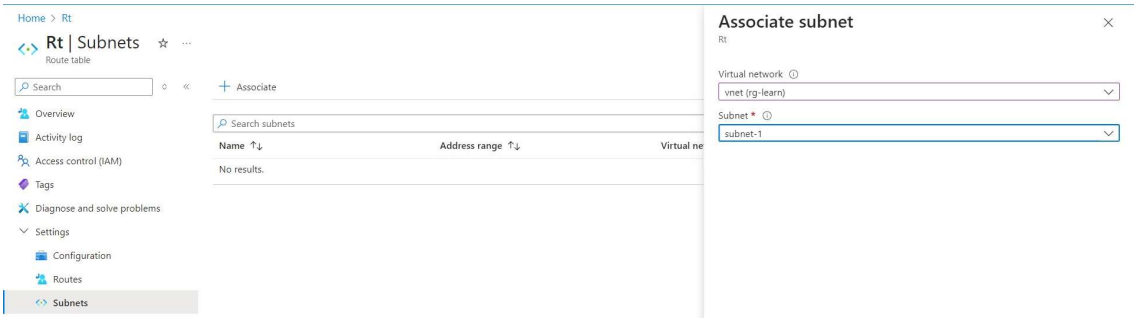


6. Create Route Table

Add routes and Associate Firewall Sub net







5. Managing and Monitoring Azure Firewall

Logging and Analytics

- Azure Firewall integrates with Azure Monitor, enabling extensive logging and analytics capabilities.

Alerts and Notifications

- Set up alerts and notifications for specific network events and threats using Azure Monitor.

6. Practical Exercise

Setting Up Azure Firewall in Azure Portal

1. **Deploy Azure Firewall** following the step-by-step guide in Section 3.
2. **Configure Firewall Rules**:
    - Navigate to the Azure Firewall resource.
    - Add network, application, and NAT rules as per the requirements.

Creating and Testing Rules

1. **Network Rule**:
    - Add a network rule to allow traffic from a specific source IP to a destination IP and port.
    - Test the rule by sending traffic from a VM within the VNet.
2. **Application Rule**:
    - Add an application rule to allow outbound traffic to a specific FQDN.
    - Test the rule by accessing the FQDN from a VM within the VNet.
3. **NAT Rule**:
    - Add a NAT rule to translate inbound traffic to an internal IP.
    - Test the rule by sending traffic to the public IP of the firewall.

7. References

- Microsoft Azure Firewall Documentation - https://learn.microsoft.com/en-us/azure/firewall/overview
- Azure Networking Documentation -https://learn.microsoft.com/en-us/azure/firewall/
- Azure Firewall Pricing - https://www.youtube.com/watch?v=-SRk0hHa-S0/