

Task - 10

Azure Firewall

Prepare R & D Documentation about Azure Firewall

Ananya Srivastava
CLOUD INFRA

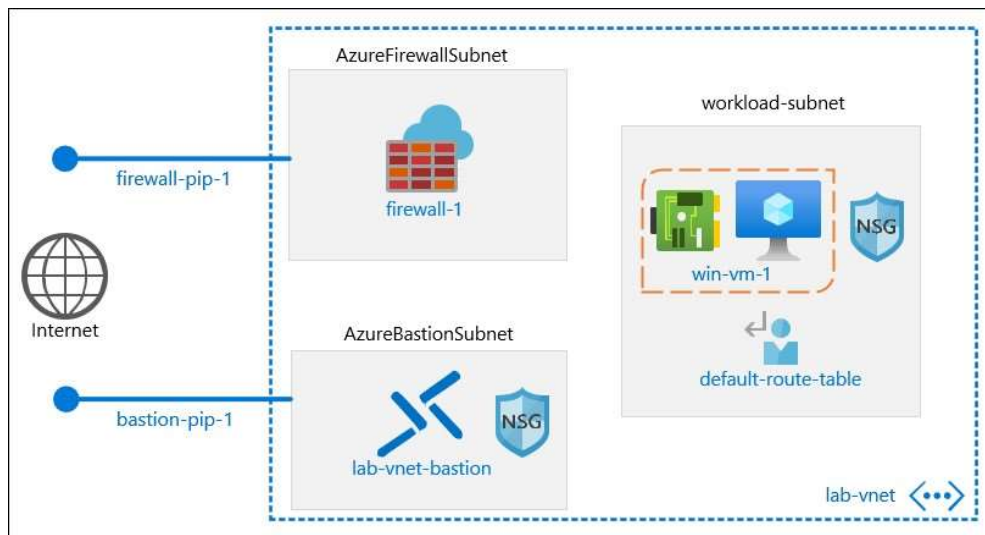
Table of Contents

1. Introduction
2. Overview of Azure Firewall
 - Key Features
 - Benefits
3. Azure Firewall Deployment
 - Prerequisites
 - Step-by-Step Deployment Guide
4. Configuring Azure Firewall
 - Network Rules
 - Application Rules
 - NAT Rules
5. Managing and Monitoring Azure Firewall
 - Logging and Analytics
 - Alerts and Notifications
6. Practical Exercise
 - Setting Up Azure Firewall in Azure Portal
 - Creating and Testing Rules
7. References

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

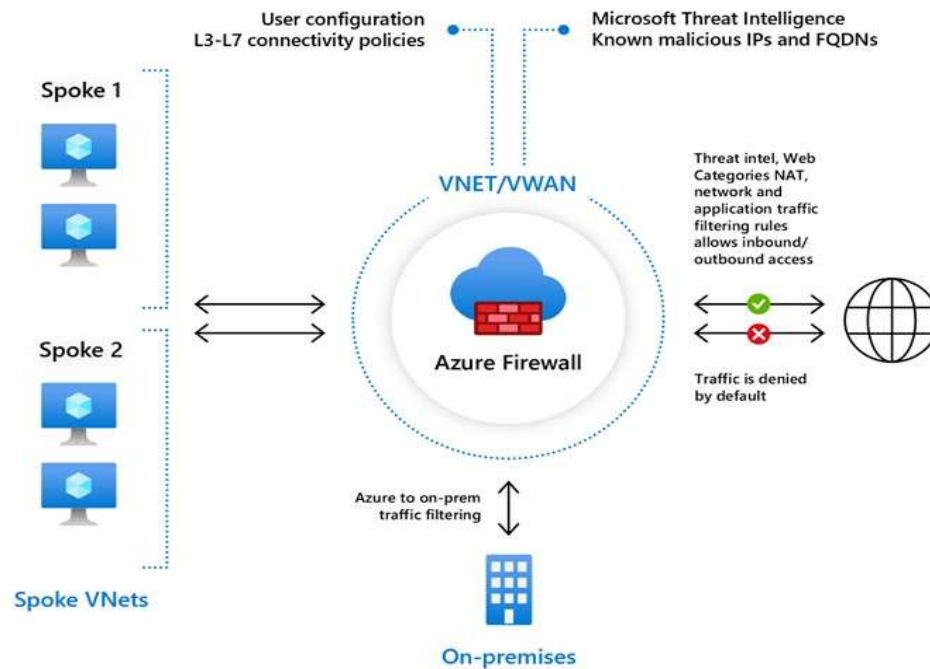
Key Features

- **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'.

The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Resource groups >'. The page title is 'Create a resource group'. There are tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is active. A description of a resource group is provided. Under 'Project details', the 'Subscription' is set to 'Azure for Students Starter' and the 'Resource group' is a new, empty field. Under 'Resource details', the 'Region' is set to '(US) East US'. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next: Tags >'.

- Fill in the required fields and create a VNet.

The screenshot shows the 'Create virtual network' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Virtual networks >'. The page title is 'Create virtual network'. There are tabs for 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create'. The 'IP addresses' tab is active. A description of defining the address space is provided. There is a section to 'Add IPv4 address space' with a dropdown showing '192.168.0.0/16'. Below this, a table lists subnets. The table has columns for 'Subnets', 'IP address range', 'Size', and 'NAT gateway'. One subnet named 'default' is listed with the IP range '192.168.0.0 - 192.168.0.255', size '/24 (256 addresses)', and no NAT gateway. At the bottom, there are buttons for 'Previous', 'Next', and 'Review + create'. A 'Give feedback' link is in the bottom right corner.

Subnets	IP address range	Size	NAT gateway
default	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	-

2. Create a Subnet for Azure Firewall

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

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security **IP addresses** Tags Review + create

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to divide your virtual network address space into smaller ranges for use by your applications. When you deploy resources into a virtual network, they are assigned an IP address from the subnet. [Learn more](#)

Add IPv4 address space

192.168.0.0/16

192.168.0.0 /16 65,536 addresses

Subnets

Subnets	IP address range	Size	NAT gateway
default	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	-

Add a subnet

Add a subnet

Subnet purpose: Default

Name: server1-subnet

IPv4

Include an IPv4 address space: ☒

IPv4 address range: 192.168.0.0/16

Starting address: 192.168.1.0

Size: /24 (256 addresses)

Subnet address range: 192.168.1.0 - 192.168.1.255

IPv6

Include an IPv6 address space: ☐ This virtual network has no IPv6 address ranges.

Private subnet PREVIEW

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the Internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default): ☐

Add **Cancel**

[Give feedback](#)

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

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security **IP addresses** Tags Review + create

assigns the resource an IP address from the subnet. [Learn more](#)

Add IPv4 address space

192.168.0.0/16

192.168.0.0 /16 65,536 addresses

Subnets

Subnets	IP address range	Size	NAT gateway
default	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	-
server1-subnet	192.168.1.0 - 192.168.1.255	/24 (256 addresses)	-

Add a subnet

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose: Default

Name: server2-subnet

IPv4

Include an IPv4 address space: ☒

IPv4 address range: 192.168.0.0/16

Starting address: 192.168.2.0

Size: /24 (256 addresses)

Subnet address range: 192.168.2.0 - 192.168.2.255

IPv6

Include an IPv6 address space: ☐ This virtual network has no IPv6 address ranges.

Private subnet PREVIEW

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the Internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default): ☐

Add **Cancel**

[Give feedback](#)

3. Deploy Virtual Machine

Home >

CreateVm-MicrosoftWindowsServer.WindowsServer-202-20220816120917 | Overview

Deployment

Search (Ctrl+F)

Delete Cancel Redeploy Download Refresh

We'd love your feedback! →

Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsServer-202-20220816120917 Start time: 8/16/2022, 12:14:21 PM
Subscription: Merchenlab99 Correlation ID: 19ec6978-18f6-4a41-ae42-f336e3de32c5
Resource group: Firewall-demo

Deployment details

Next steps

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

Go to resource **Create another VM**

Deployment succeeded

Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-202-20220816120917' to resource group 'Firewall-demo' was successful.

[Go to resource](#) [Pin to dashboard](#)

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 assets on Azure and be your first line of support.

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

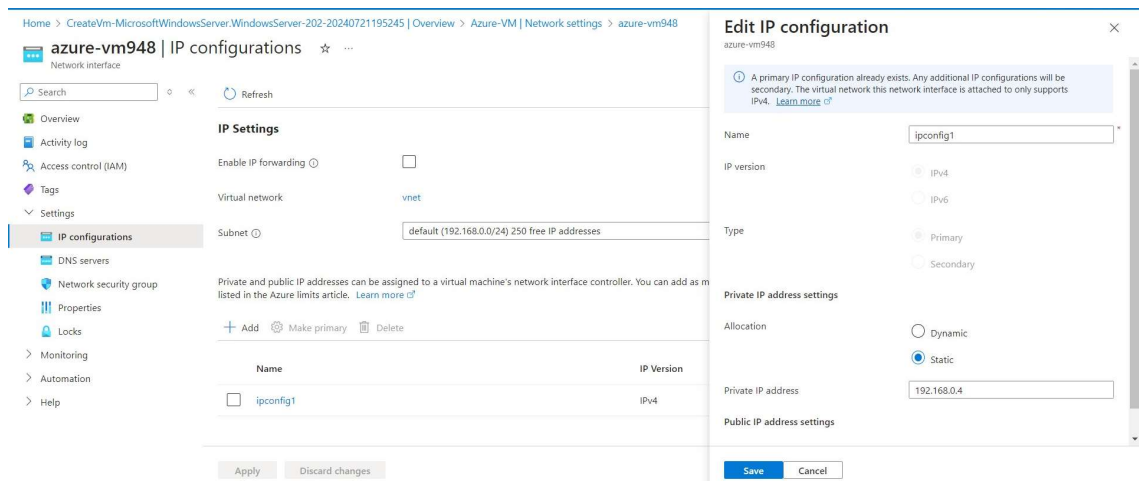
- **Create network rules** to allow or deny traffic based on source and destination IP addresses, ports, and protocols.

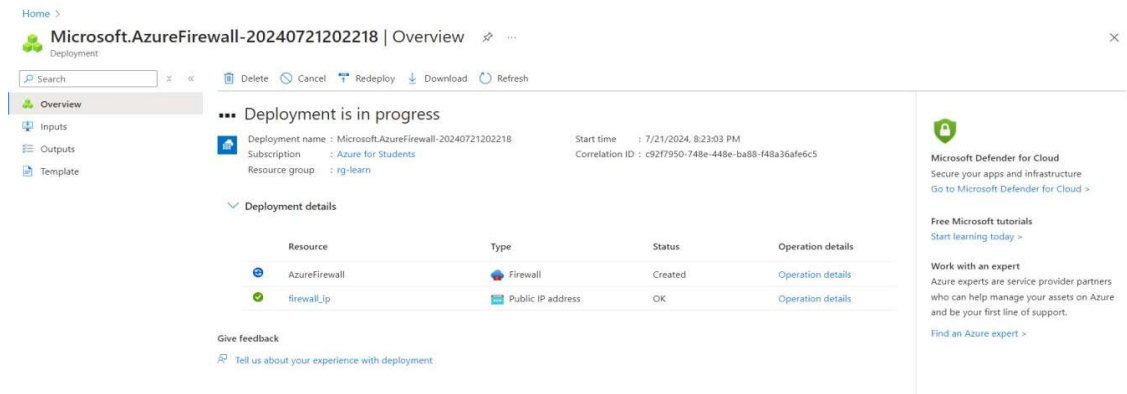
Application Rules

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

NAT Rules

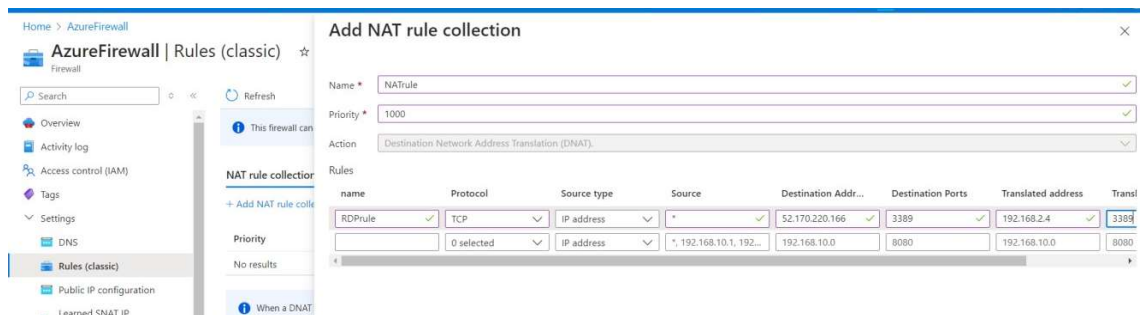
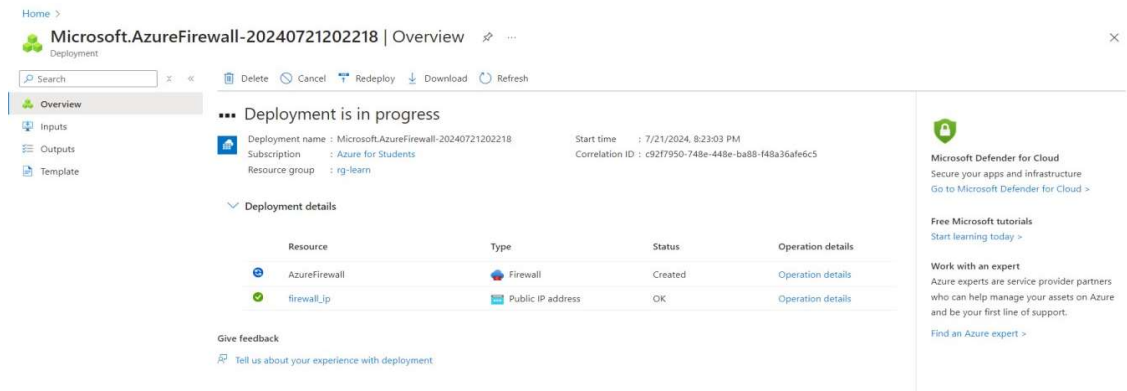
- **NAT rules** define how to translate traffic to the internal network.





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

Home > Microsoft.RouteTable-20240721203741 | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

Inputs

Outputs

Template

Your deployment is complete

Deployment name : Microsoft.RouteTable-20240721203741
Subscription : Azure for Students
Resource group : rg-learn

Start time : 7/21/2024, 8:38:34 PM
Correlation ID : 9a03c792-fc17-4e75-9b68-ba9bec30f74

Deployment details

Next steps

Go to resource

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

Home > Microsoft.RouteTable-20240721203741 | Overview > Rt

Rt | Routes

Route table

Search routes

Name	Address prefix	Next hop
No results.		

Add route

Rt

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more](#)

Route name *
myroute

Destination type *
IP Addresses

Destination IP addresses/CIDR ranges *
0.0.0.0/0

Next hop type *
Virtual appliance

Next hop address *
192.168.1.4

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.

Add

Give feedback

Home > Rt

Rt | Subnets

Route table

Search subnets

Name	Address range	Virtual ne
No results.		

Associate subnet

Rt

Virtual network
vnet (rg-learn)

Subnet *
subnet-1

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) - <https://learn.microsoft.com/en-us/azure/firewall/overview>
- [Azure Networking Documentation](https://learn.microsoft.com/en-us/azure/firewall/) - <https://learn.microsoft.com/en-us/azure/firewall/>
- [Azure Firewall Pricing](https://www.youtube.com/watch?v=-SRk0hHa-S0/) - <https://www.youtube.com/watch?v=-SRk0hHa-S0/>