

## Azure Firewall

Azure Firewall is a managed, cloud-based network security service provided by Microsoft Azure. It acts as a barrier between your Azure Virtual Network resources and the internet, controlling and monitoring inbound and outbound traffic based on rules and policies that you define.

Key features of Azure Firewall include:

1. **Application FQDN filtering:** Allows you to create rules based on fully qualified domain names (FQDNs), enabling more granular control over allowed or denied traffic.
2. **Network traffic filtering:** Enables you to define rules based on IP addresses, ports, and protocols to control traffic flow to and from Azure resources.
3. **Network Address Translation (NAT):** Supports source NAT for outbound traffic and destination NAT for inbound traffic, allowing you to hide the internal IP addresses of your resources.
4. **Threat intelligence-based filtering:** Integrates with Microsoft's threat intelligence feeds to provide protection against known malicious IP addresses and domains.
5. **Logging and analytics:** Provides detailed logs for all traffic passing through the firewall, allowing you to monitor and analyze network activity.
6. **High availability:** Supports availability zones for increased resiliency and fault tolerance.

Azure Firewall can be deployed and managed using the Azure Portal, Azure PowerShell, Azure CLI, or ARM templates. It integrates seamlessly with other Azure services and can be used to secure traffic between virtual networks, on-premises networks, and the internet.

## Use cases of firewall:

Azure Firewall is a cloud-based network security service provided by Microsoft Azure. It offers many use cases for securing your cloud resources and applications. Here are some common scenarios where Azure Firewall can be beneficial:

1. **Network Segmentation:** Azure Firewall allows you to create multiple application and network tiers within your Azure Virtual Network (VNet). You can enforce different security policies for each tier, restricting or allowing traffic based on your organizational needs.
2. **Centralized Network Security Management:** With Azure Firewall, you can centrally manage and monitor your network security policies across multiple VNets and Azure subscriptions. This simplifies security management, especially in large-scale environments.
3. **Internet Access Control:** Azure Firewall can be used to control outbound internet traffic from your Azure resources. You can define rules to allow or deny access to

specific websites or categories of websites, protecting your resources from accessing malicious or unauthorized content.

4. **Application Security:** Azure Firewall supports application-level filtering, allowing you to inspect and filter traffic based on specific application protocols and ports. This helps in securing your applications by blocking unauthorized access and preventing attacks targeting application vulnerabilities.
5. **Threat Intelligence Integration:** Azure Firewall integrates with Azure Security Center and Azure Sentinel to provide advanced threat detection and response capabilities. It leverages threat intelligence feeds to identify and block malicious traffic, enhancing your network security posture.
6. **Hybrid Cloud Security:** Azure Firewall can be deployed in hybrid cloud environments, allowing you to extend your network security policies to on-premises resources connected to Azure using VPN or ExpressRoute. This ensures consistent security enforcement across your entire infrastructure.
7. **Secure Remote Access:** Azure Firewall can be used to secure remote access to Azure Virtual Machines (VMs) using Azure Bastion. It acts as a secure gateway, allowing authorized users to connect to VMs over Remote Desktop Protocol (RDP) or Secure Shell (SSH) while protecting against unauthorized access attempts.
8. **DDoS Protection:** Azure Firewall provides built-in DDoS protection to safeguard your Azure resources against distributed denial-of-service (DDoS) attacks. It automatically detects and mitigates volumetric attacks, ensuring the availability of your applications and services.
9. **Logging and Monitoring:** Azure Firewall logs all network traffic and security events, which can be integrated with Azure Monitor and Azure Log Analytics for centralized logging and monitoring. This allows you to gain insights into your network traffic patterns and security incidents.
10. **Compliance Requirements:** Azure Firewall helps you meet various compliance requirements such as PCI DSS, HIPAA, and GDPR by providing features like network segmentation, access control, and logging, which are essential for maintaining regulatory compliance.

**The end goal is to enhance the security of the VM by using Azure Firewall to manage and filter network traffic, thereby protecting the VM and the overall network environment from unauthorized access and threats.**

### **To begin with the Lab:**

1. First, we are going to create a virtual machine based on Windows Server 2022, but we will make sure that this does not have a Public IP address.

## 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 Pass - Sponsorship
Resource group *	demo-resource-group
	<a href="#">Create new</a>

## Instance details

Virtual machine name *	Firewall-VM
Region *	(Europe) North Europe
Availability options	No infrastructure redundancy required
Security type	Trusted launch virtual machines
Image *	Windows Server 2022 Datacenter - x64 Gen2
	<a href="#">See all images</a>   <a href="#">Configure VM generation</a>

- Below you can see that in the networking section in network interface we are adding a new subnet for firewall. Then the name should be the same as shown below.

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. [Learn more](#)

Name \* Firewall-VM-vnet

### Address space

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

<input type="checkbox"/> Address range *	Addresses	Overlap		...
<input type="checkbox"/> 10.0.0.0/16	10.0.0.0 - 10.0.255.255 (65536 addresses)	None		
	(0 Addresses)	None		

### Subnets

The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

<input type="checkbox"/> Subnet name	Address range	Addresses		...
<input type="checkbox"/> default	10.0.0.0/24	10.0.0.0 - 10.0.0.255 (256 addresses)		
<input type="checkbox"/> AzureFirewallSubnet	10.0.1.0/24	10.0.1.0 - 10.0.1.255 (256 addresses)		

- Also, you need to make sure that the subnet should be default while launching the VM and the Public IP should be set to none.

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more](#)

#### Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	(new) Firewall-VM-vnet	▼
	<a href="#">Create new</a>	
Subnet *	(new) default (10.0.0.0/24)	▼
Public IP	None	▼
	<a href="#">Create new</a>	

4. After that just go ahead and launch your Virtual Machine.
5. Once your machine is deployed now, we are going to create a firewall for it. For that, in the marketplace, you need to search the firewall and choose this server accordingly.

The screenshot shows the Azure Marketplace search results for 'Firewall'. The top result is 'Firewall' from Microsoft, described as an Azure Service. It has a 3.4 rating based on 12 reviews. Below the search bar, there's a 'Plan' dropdown set to 'Firewall' and a large blue 'Create' button.

6. Now you need to choose your resource group then give it a name then choose your region and scroll down.

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, 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 Pass - Sponsorship

Resource group \*

demo-resource-group

Create new

#### Instance details

Name \*

firewall

Region \*

North Europe

Availability zone ⓘ

None

7. Now in the firewall SKU you need to choose standard then for firewall management, you need to choose to use a firewall policy to manage this firewall.
8. Then you need to click on add new and create a new firewall policy. Then you need to choose your virtual network and for the public IP address click on add new.
9. After that just move to the review page and create your firewall.

Firewall SKU

Basic  
 Standard  
 Premium

Firewall management

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

Firewall policy \*

(New) firewall-policy

Add new

Choose a virtual network

Create new  
 Use existing

Virtual network

Firewall-VM-vnet (demo-resource-group)

Public IP address \*

(New) firewall-ip

Add new

Forced tunneling ⓘ

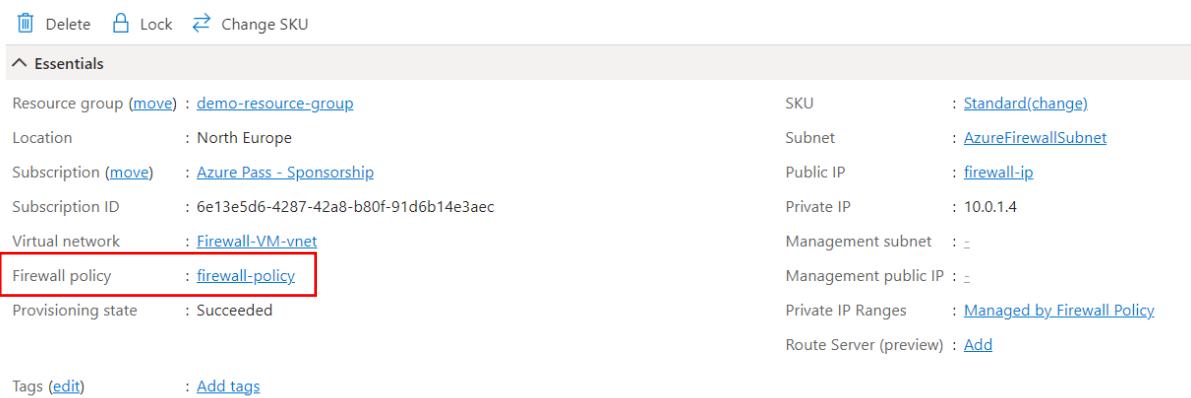
Disabled

10. See, the entire purpose of a firewall system is to look at the traffic which is flowing from your internal network onto the internet. At the same time, it is also used to look at traffic that is coming on from the internet onto your internal network. So

definitely you need to add a public IP address assigned to the Azure Firewall. That exposes its interface to the internet itself.

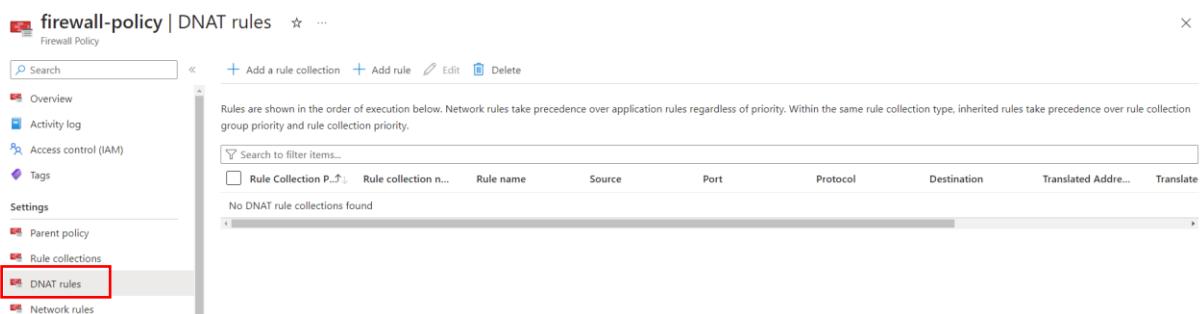
## Nat Rule Collection

- Once your deployment is complete then go to the firewall. So, from the dashboard of the firewall, you will see the private IP address of the firewall and if you have a Public IP configuration then you can see the public IP address of the firewall.
- Now we are going to add a rule which will allow us to log in to our VM.
- For that from the overview of the firewall we need to go to a firewall policy. For that click on the highlighted place as shown below.



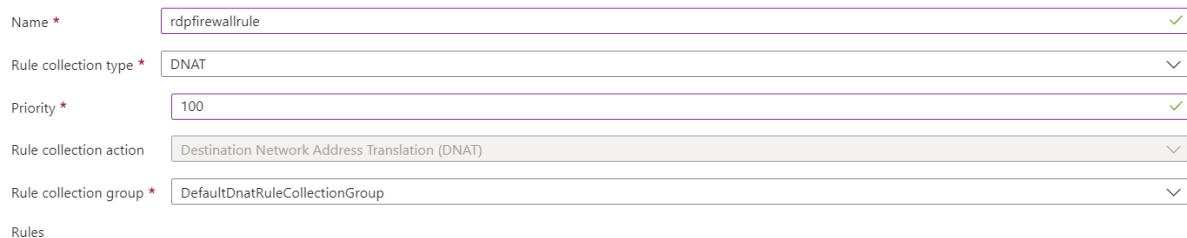
The screenshot shows the 'Essentials' tab of an Azure Firewall's overview page. A red box highlights the 'Firewall policy' field, which is set to 'firewall-policy'. Other visible details include the resource group ('demo-resource-group'), location ('North Europe'), subscription ('Azure Pass - Sponsorship'), and various network configurations like Virtual network ('Firewall-VM-vnet') and Subnet ('AzureFirewallSubnet').

- Here you need to go to DNAT rules and click on add a rule collection.



The screenshot shows the 'Rule collections' section of the DNAT rules blade. A red box highlights the 'DNAT rules' link under the 'Rule collections' heading. The main area displays a table with columns for Rule Collection P., Rule collection n., Rule name, Source, Port, Protocol, Destination, Translated Address, and Translate. The message 'No DNAT rule collections found' is displayed.

- First you need to give it a name and then give the priority, after that you need to scroll down.



The screenshot shows the 'Add DNAT rule collection' form. The fields filled in are:

- Name \*: rdpfirewallrule
- Rule collection type \*: DNAT
- Priority \*: 100
- Rule collection action: Destination Network Address Translation (DNAT)
- Rule collection group \*: DefaultDnatRuleCollectionGroup

- Then you need to give a name and choose the IP address as your source type, and you need to give the IP address of your laptop here and then choose the protocol as TCP.

7. After that give any random eligible destination port and in the destination, you need to put the public IP address of the firewall.

Name *	Source type	Source	Protocol *	Destination Ports *	Destination (Firewall IP)
virtualmachine ✓	IP Address ✓	192.140.153.5 ✓	TCP ✓	5000 ✓	40.113.11.26
The value cannot have trailing commas, trailing spaces or empty spaces. Invalid IP address					
	IP Address ✓	* , 192.168.10.1, 192...	0 selected ✓	8080	192.168.10.1

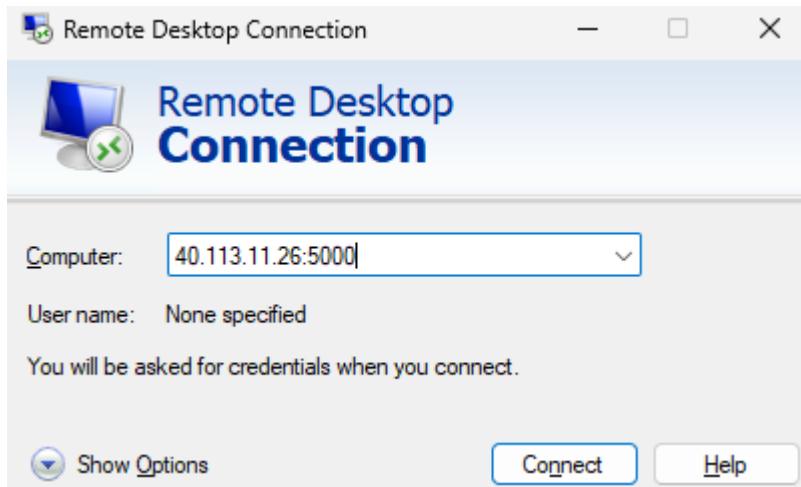
8. Then again in the translated type choose the IP address and in the translated address you need to put the Private IP address of your virtual machine and the translated port is 3389.

Translated type *	Translated address or	Translated port *
IP Address ✓	10.0.0.4	3389 ✓
IP Address ✓	192.168.10.0	8080

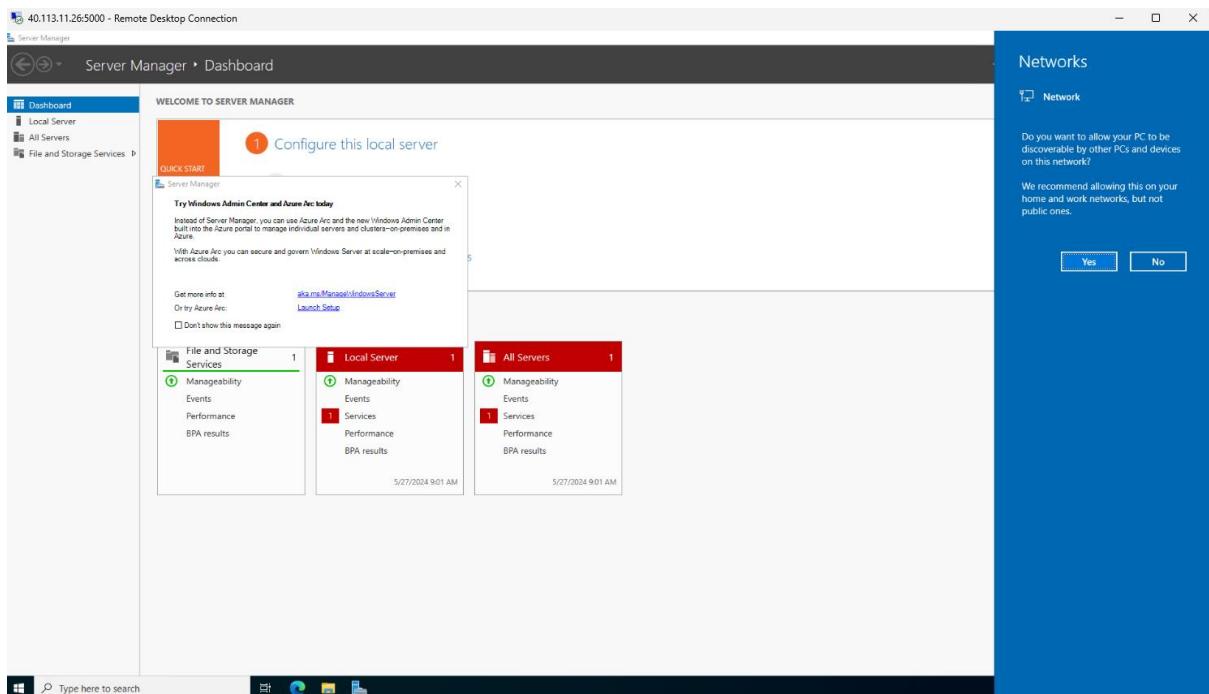
9. After that just click on add. After some time, you can see your rule in place.

Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.								
<input type="checkbox"/> Search to filter items... <input type="checkbox"/> Rule Collection P.. ↑ <input type="checkbox"/> Rule collection n... <input type="checkbox"/> Rule name <input type="checkbox"/> Source <input type="checkbox"/> Port <input type="checkbox"/> Protocol <input type="checkbox"/> Destination <input type="checkbox"/> Translated Addre... <input type="checkbox"/> Translate								
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.								
<input type="checkbox"/> 100	rdpfirewallrule	firewallVM	192.140.153.5 ⓘ	5000	TCP	40.113.11.26 ⓘ	10.0.0.4	3389

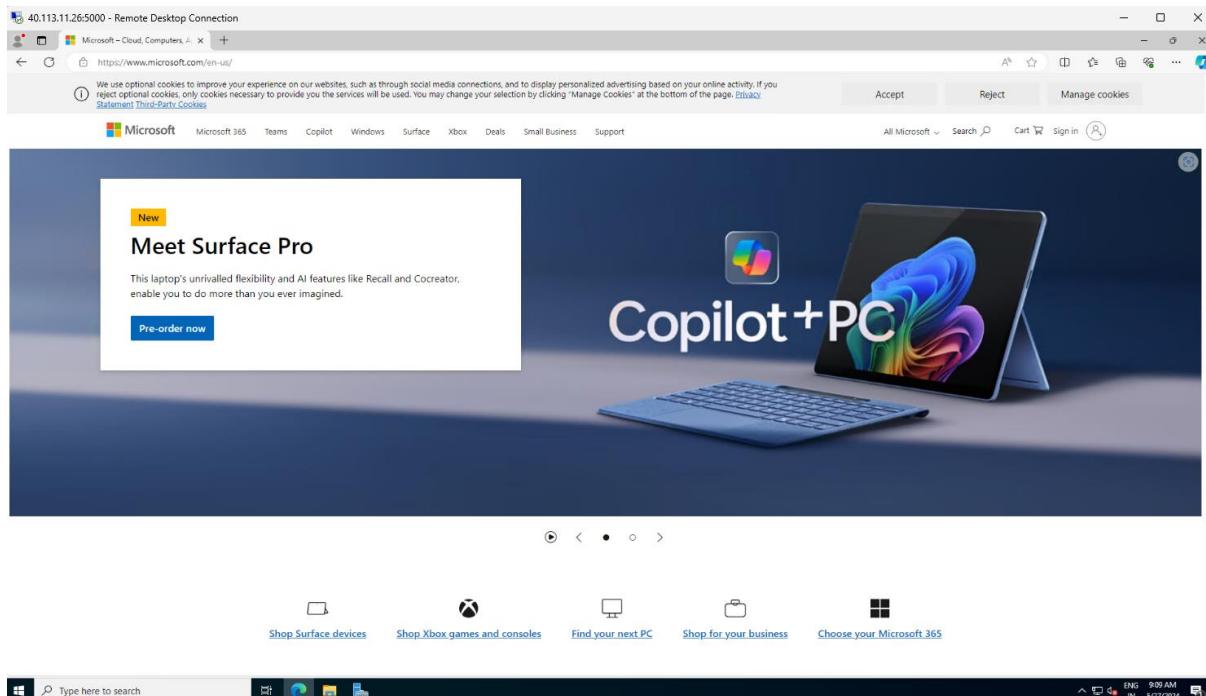
10. Now copy the Public IP address of the Firewall and open RDP on your laptop. Then paste the IP address with the destination port appended.



11. Below you can see that you are logged in to your VM using the Public IP address of firewall.



12. Now if you open up the Microsoft Edge browser you can reach the Microsoft.com easily.



13. So, here you can see that we can reach the homepage of [microsoft.com](https://microsoft.com). So, remember the purpose of a firewall is to ensure that it restricts the traffic that is flowing out of your Azure virtual network.
14. So even though we have deployed the Azure Firewall onto our Azure virtual network, we don't see any such restrictions in place. We can still browse for websites on the internet. Now, the reason for this is we have to route all the traffic from the Subnet via the Azure Firewall resource, and for that, we need to create a route table.
15. So we've already seen the use case of using route tables, in this case also, we need to create a route table, attach that table onto the subnet, and then create a route saying that for any traffic that is destined for the internet needs to flow via the Azure Firewall resource.
16. Now from the marketplace we will search for a route table and create it. For that, you just need to choose your resource group, and your region and give it a name then move to review page and create your 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 Pass - Sponsorship

Resource group \* ⓘ

demo-resource-group

[Create new](#)

### Instance details

Region \* ⓘ

North Europe

Name \* ⓘ

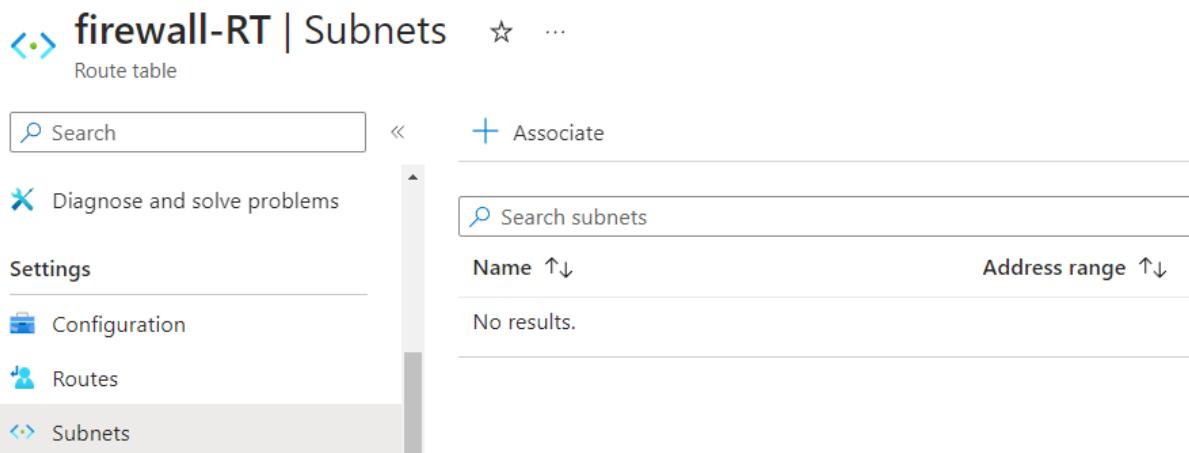
firewall-RT

Propagate gateway routes \* ⓘ

Yes

No

17. Once your route table has deployed go towards it. Then go to subnets and associate it with the default subnet that your VM has.

firewall-RT | Subnets ⚡ ...  
Route table

Search

+ Associate

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Name ↑↓	Address range ↑↓
No results.	

Virtual network ⓘ

Firewall-VM-vnet (demo-resource-group)

Subnet \* ⓘ

default

18. Then go to routes and add a route.

The screenshot shows the 'firewall-RT | Routes' interface. At the top, there's a search bar with a magnifying glass icon, followed by 'Add', 'Refresh', and 'Give feedback' buttons. Below the search bar is a sidebar with 'Diagnose and solve problems', 'Settings', 'Configuration', and 'Routes' (which is selected and highlighted in grey). To the right of the sidebar is a table header with 'Name ↑↓' and 'Address prefix ↑↓'. A message 'No results.' is displayed below the header.

19. Now you need to give it a name then in the destination type choose the IP address and, in the destination, IP put the same address as shown below. After that, you need to choose a virtual appliance in the next hop type and the next hop address is the private IP address of your Firewall.

Route name \*

 ✓

Destination type \* ⓘ

 ▼

Destination IP addresses/CIDR ranges \* ⓘ

 ✓

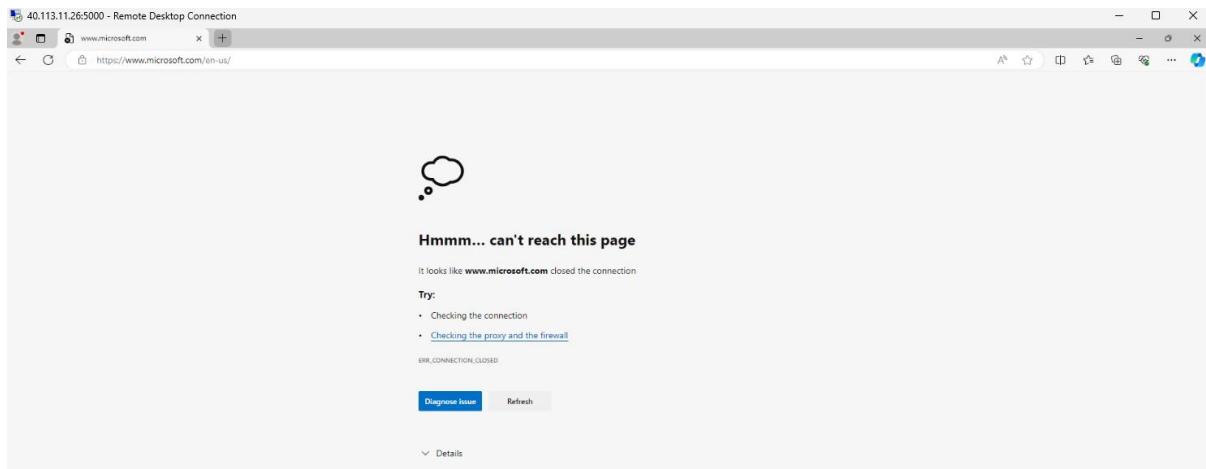
Next hop type \* ⓘ

 ▼

Next hop address \* ⓘ

 ✓

20. Once your route is in place then go to your VM and refresh the page then you will see that you are getting an error.



21. Now we are going to all the rules so that our VM can reach the internet. For that in firewall policy, you need to go to application rules and click on add a rule collection.

22. So, you need to give it a name and then give the priority after that in the IP address you need to give the Private IP of your VM then in the protocol we will allow both HTTP and HTTPS then in the destination we will allow www.Microsoft.com.

Name *	allowinternet
Rule collection type *	Application
Priority *	100
Rule collection action	Allow
Rule collection group *	DefaultApplicationRuleCollectionGroup

Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
allowMicrosoft	IP Address	10.0.0.4	http,https	<input type="checkbox"/> TLS inspection	FQDN	microsoft.com
	IP Address	*, 192.168.10.1, 192...	http:80,https,mssql:...	<input type="checkbox"/> TLS inspection	FQDN	*.microsoft.com,*...

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

23. Then go back to your VM and refresh the page you will be able to reach Microsoft.com.

