😊 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

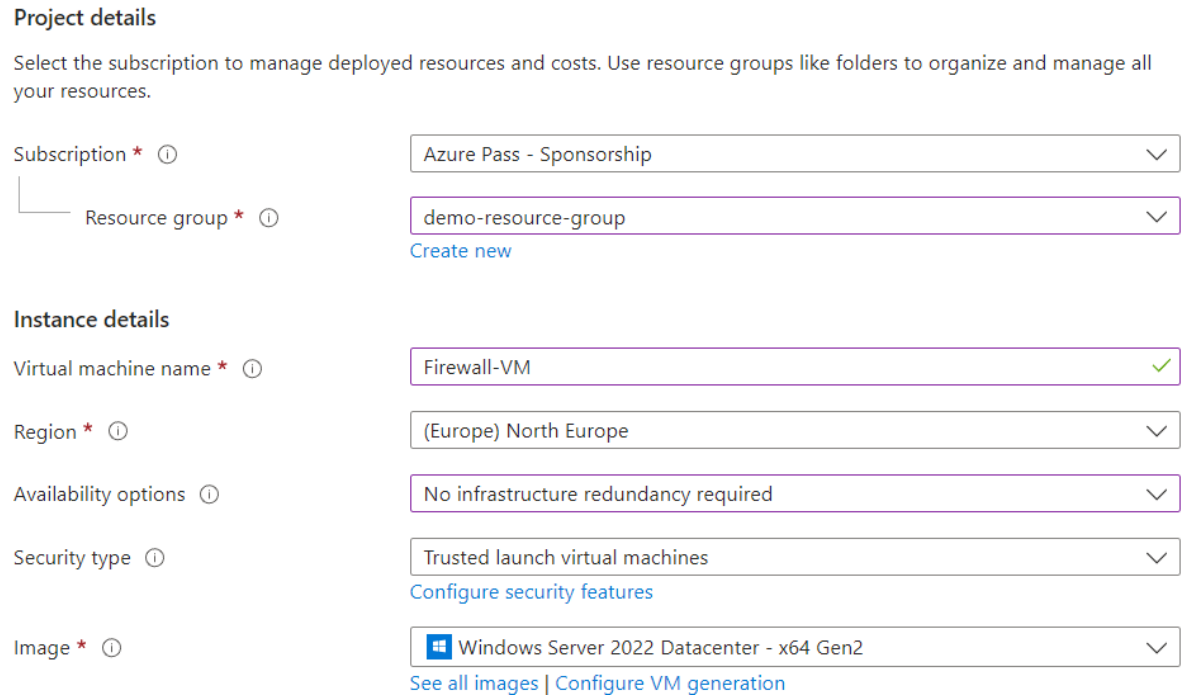
specific websites or categories of websites, protecting your resources from accessing malicious or unauthorized content.

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.

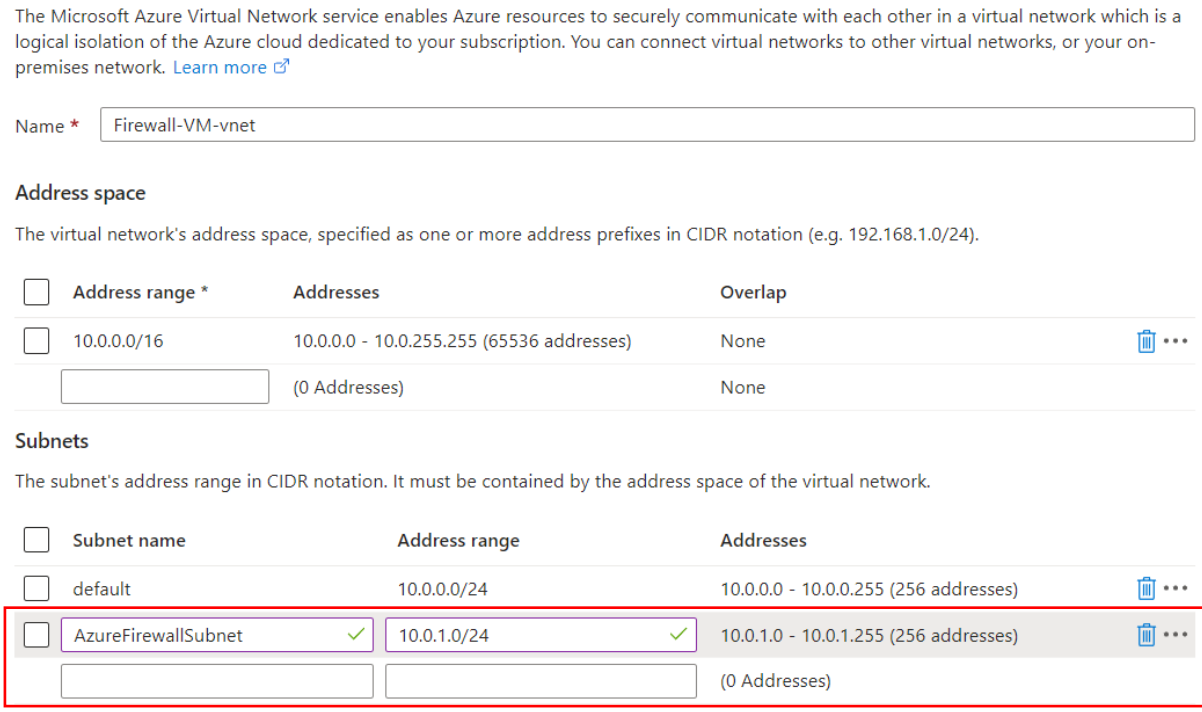
The end goal is to enhance the security of the VM by using Azure Firewall to manage and filter network traffic, thereby protecting the VM and the overall network environment from unauthorized access and threats.

😄 To begin with the Lab:

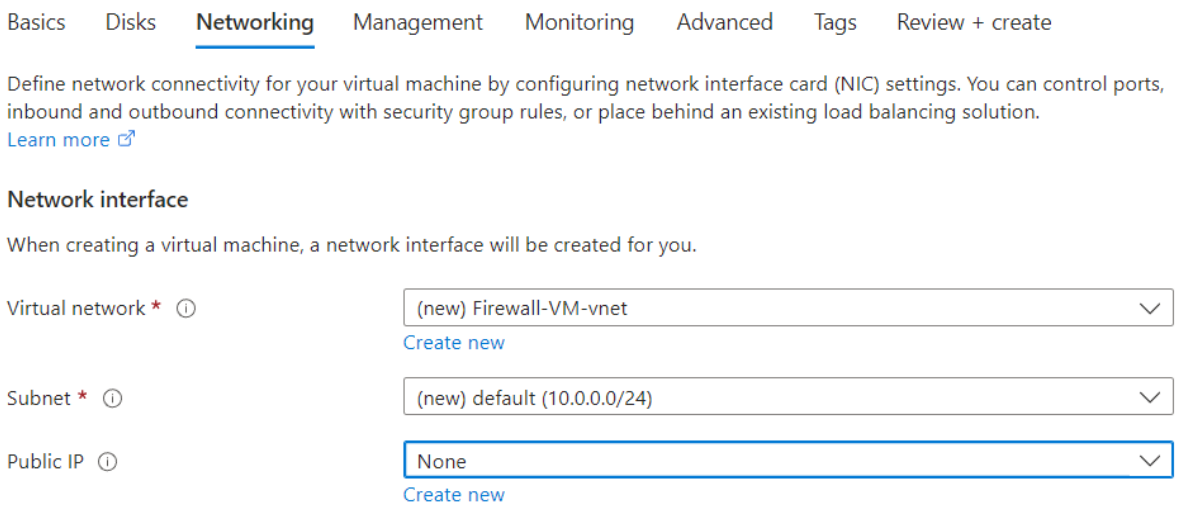
1. First, we are going to create a virtual machine based on Windows Server 2022, but we will make sure that this does not have a Public IP address.



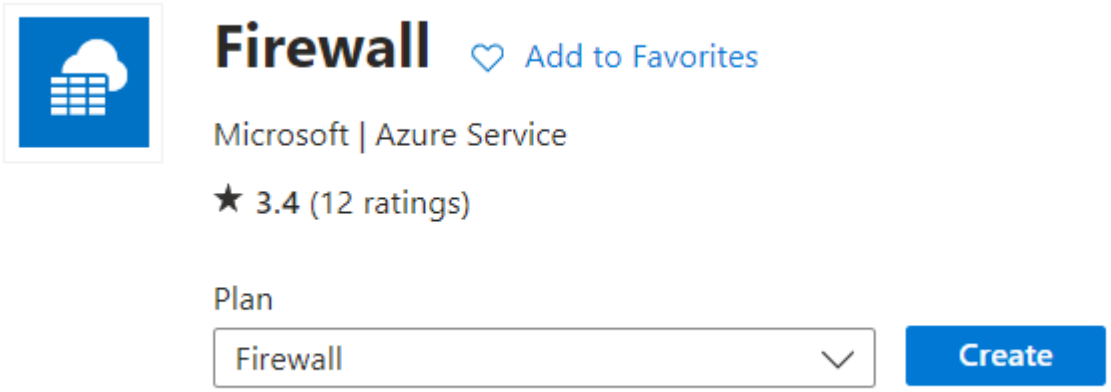
2. Below you can see that in the networking section in network interface we are adding a new subnet for firewall. Then the name should be the same as shown below.



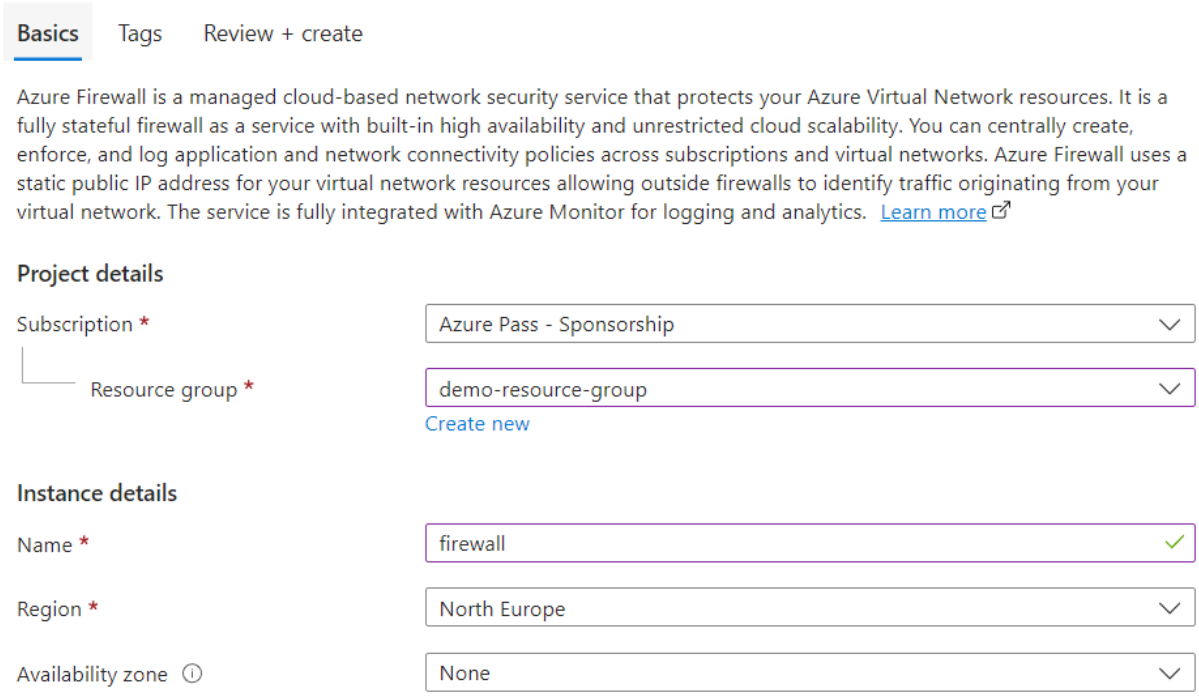
3. Also, you need to make sure that the subnet should be default while launching the VM and the Public IP should be set to none.



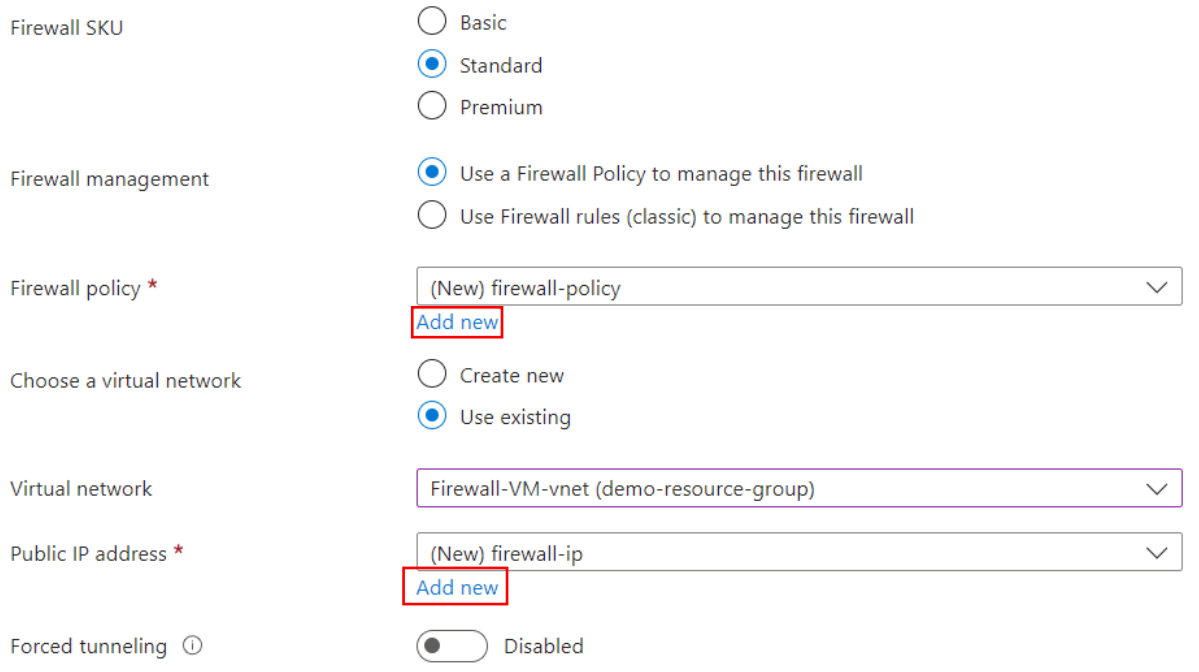
4. After that just go ahead and launch your Virtual Machine.
5. Once your machine is deployed now, we are going to create a firewall for it. For that, in the marketplace, you need to search the firewall and choose this server accordingly.



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



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.

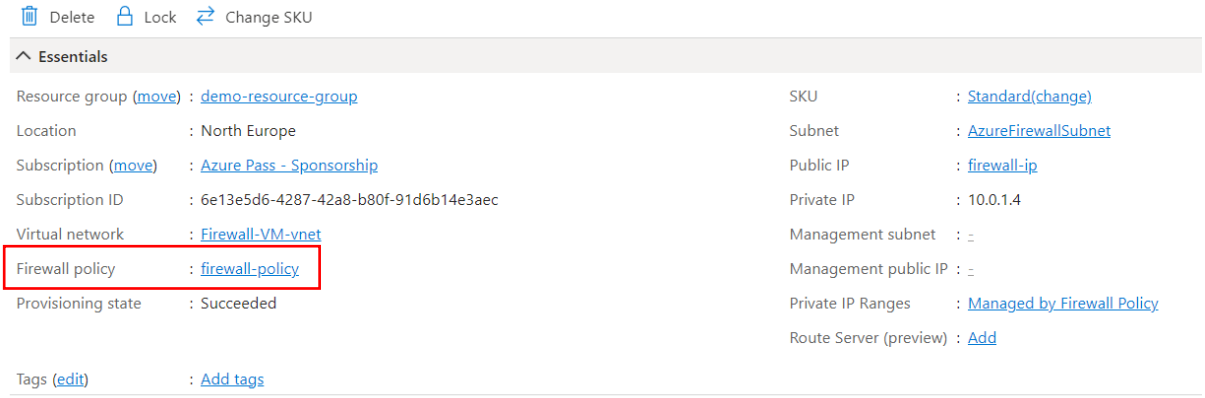


10. See, the entire purpose of a firewall system is to look at the traffic which is flowing from your internal network onto the internet. At the same time, it is also used to look at traffic that is coming on from the internet onto your internal network. So

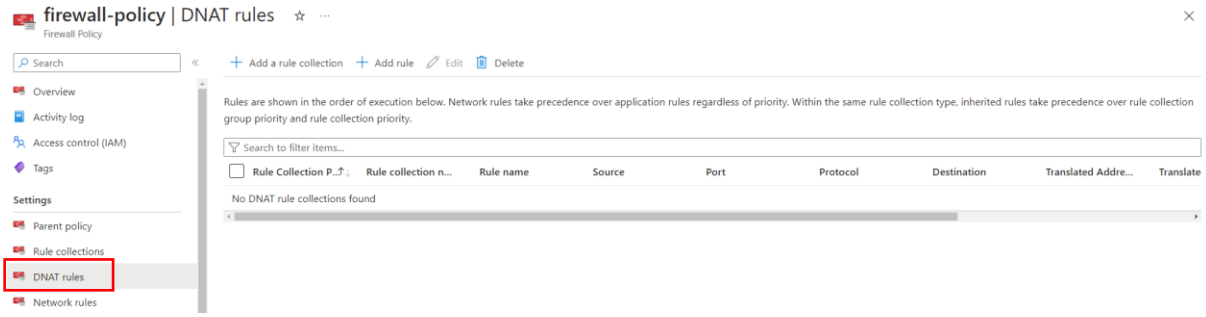
definitely you need to add a public IP address assigned to the Azure Firewall. That exposes its interface to the internet itself.

😊 Nat Rule Collection

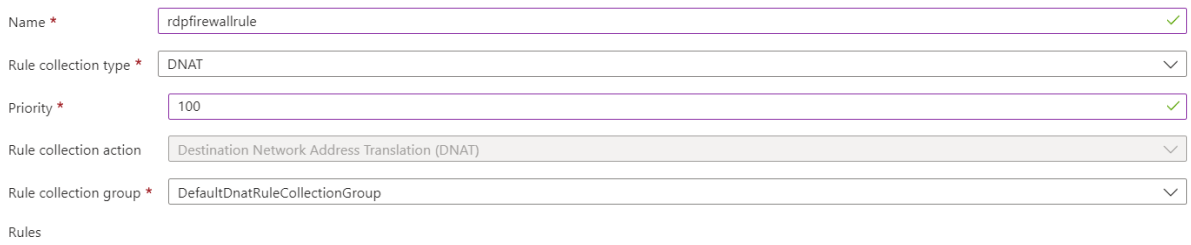
1. Once your deployment is complete then go to the firewall. So, from the dashboard of the firewall, you will see the private IP address of the firewall and if you have a Public IP configuration then you can see the public IP address of the firewall.
2. Now we are going to add a rule which will allow us to log in to our VM.
3. 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.



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

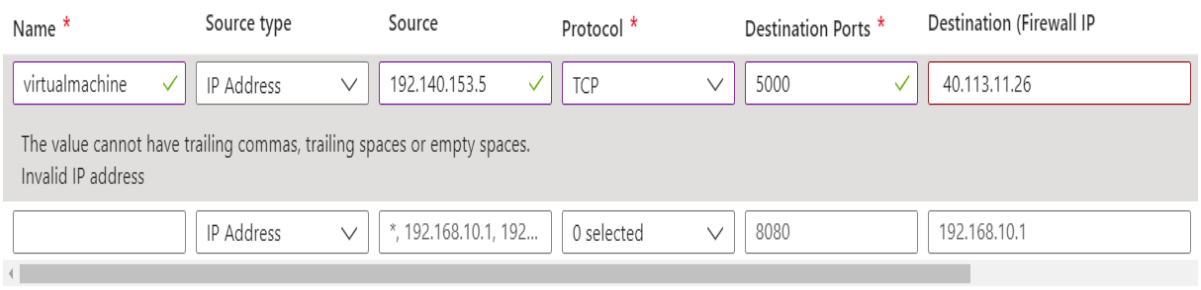


5. First you need to give it a name and then give the priority, after that you need to scroll down.

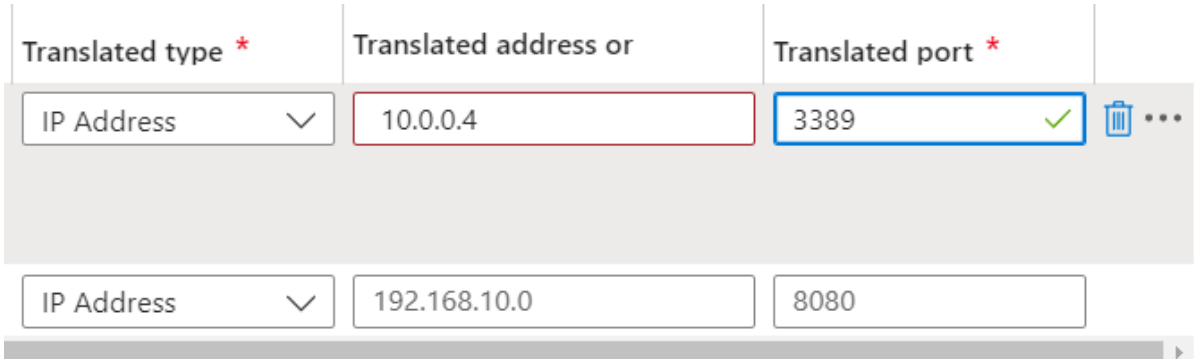


6. Then you need to give a name and choose the IP address as your source type, and you need to give the IP address of your laptop here and then choose the protocol as TCP.

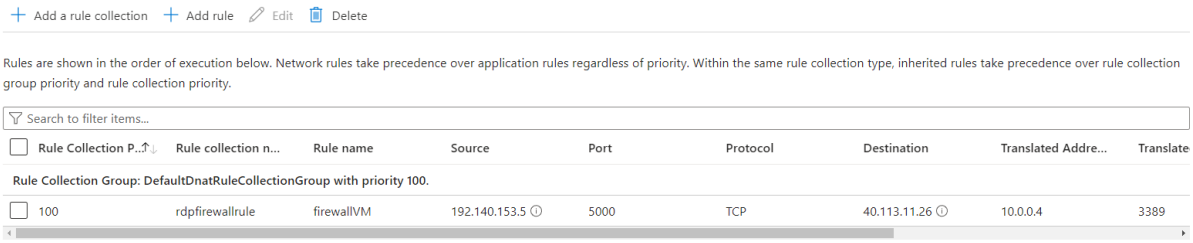
7. After that give any random eligible destination port and in the destination, you need to put the public IP address of the firewall.



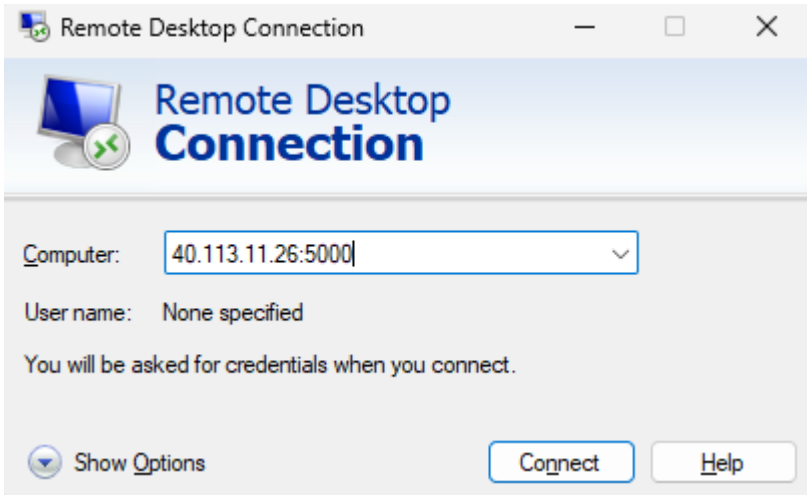
8. Then again in the translated type choose the IP address and in the translated address you need to put the Private IP address of your virtual machine and the translated port is 3389.



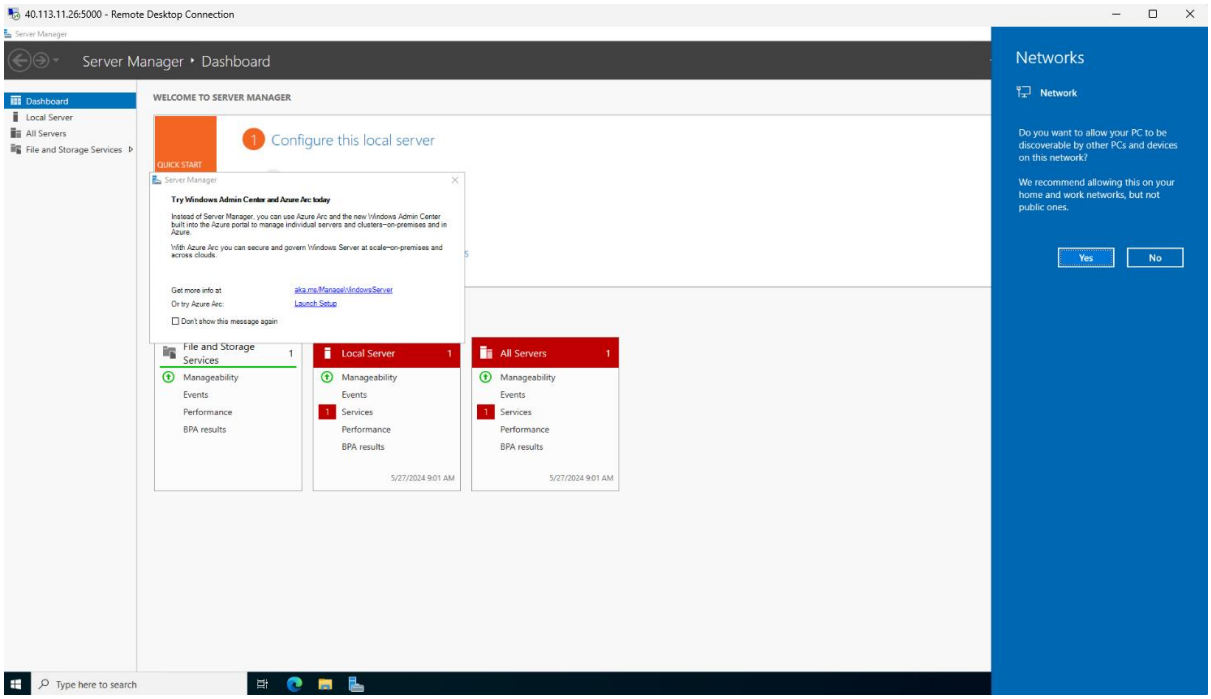
9. After that just click on add. After some time, you can see your rule in place.



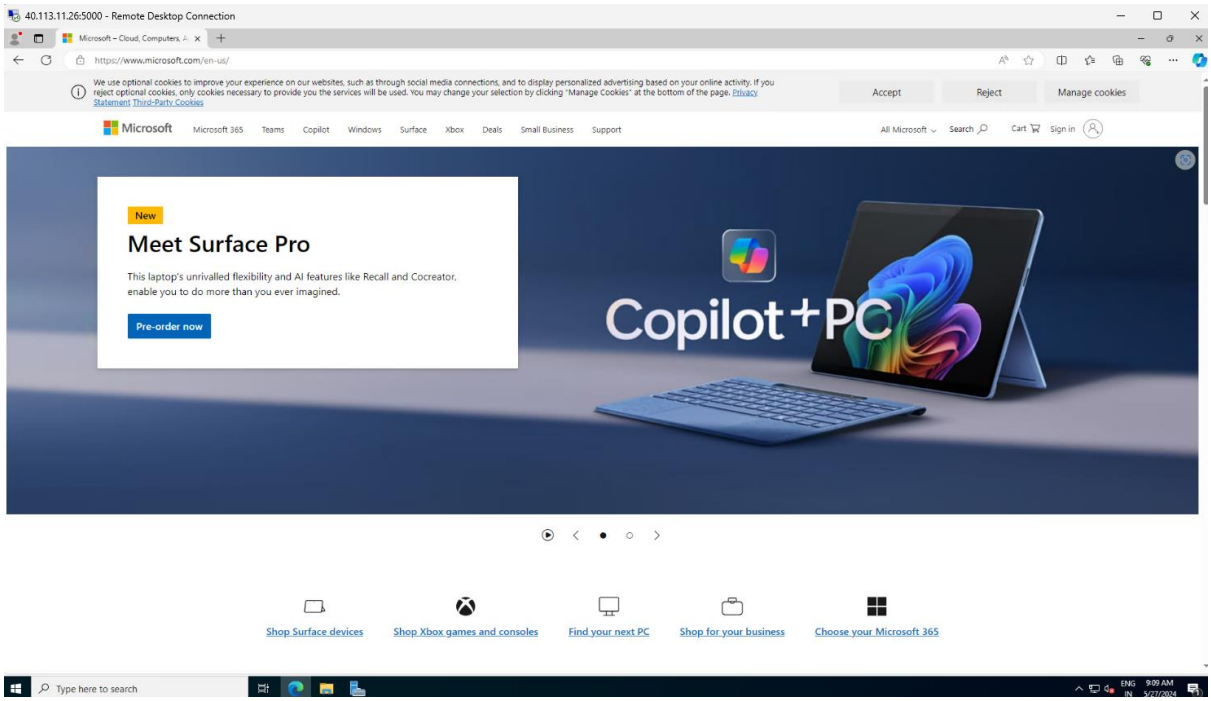
10. Now copy the Public IP address of the Firewall and open RDP on your laptop. Then paste the IP address with the destination port appended.



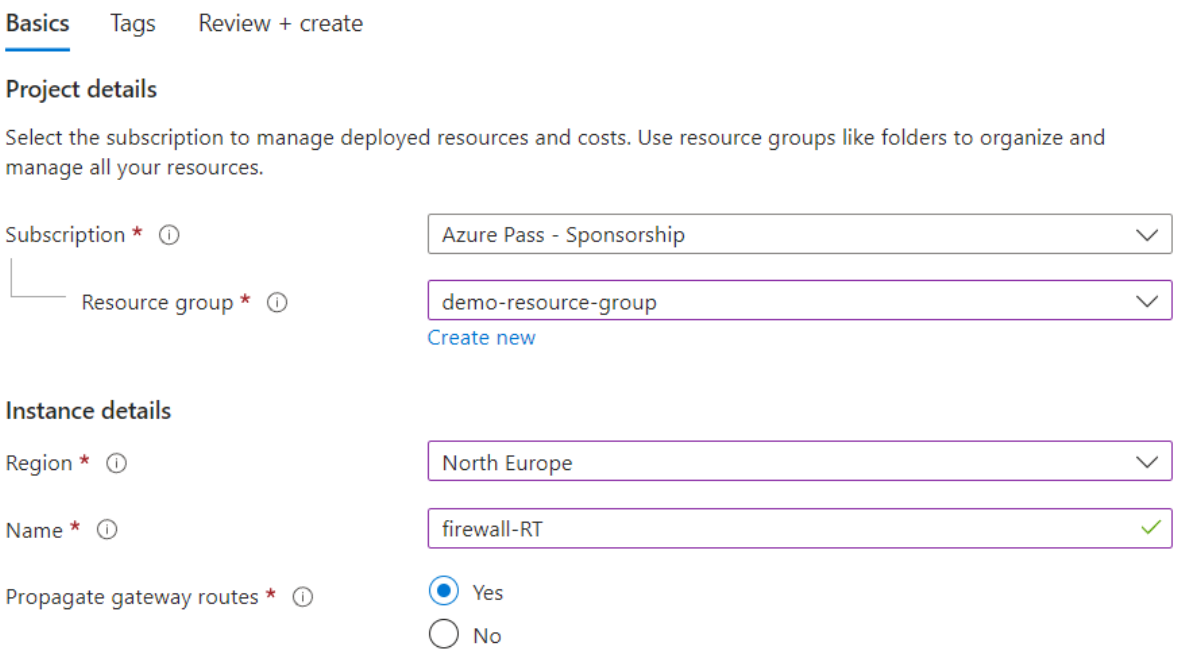
11. Below you can see that you are logged in to your VM using the Public IP address of firewall.



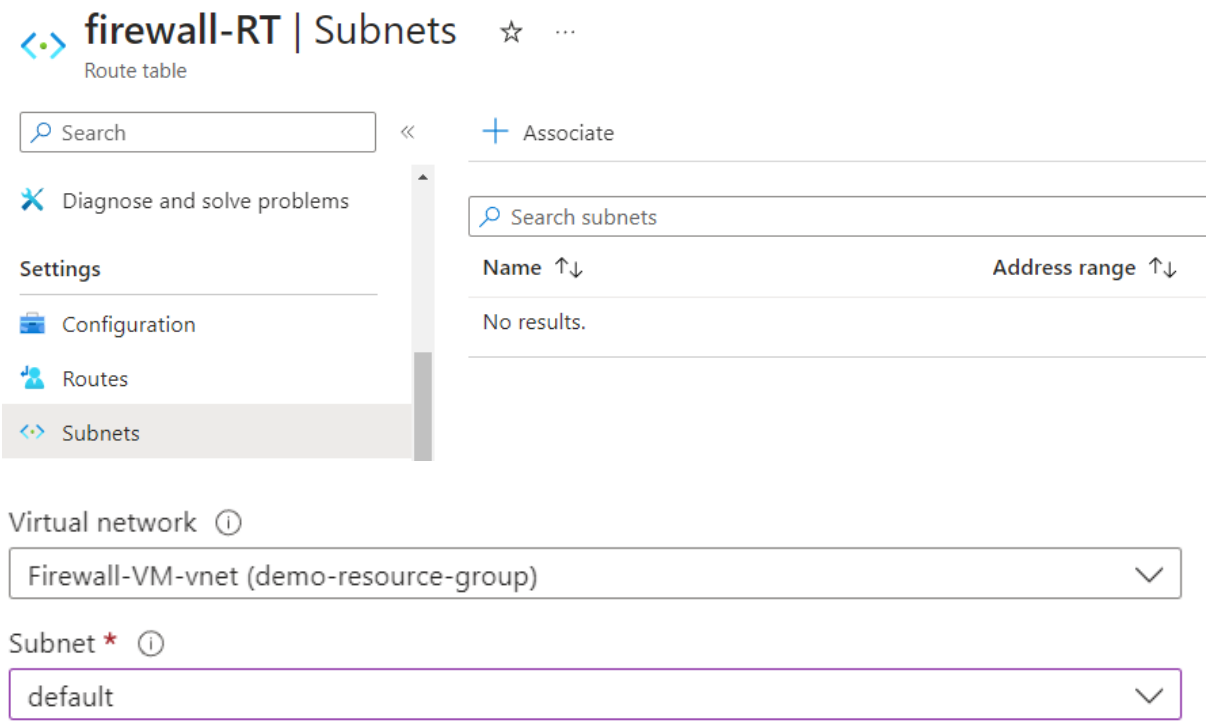
12. Now if you open up the Microsoft Edge browser you can reach the Microsoft.com easily.



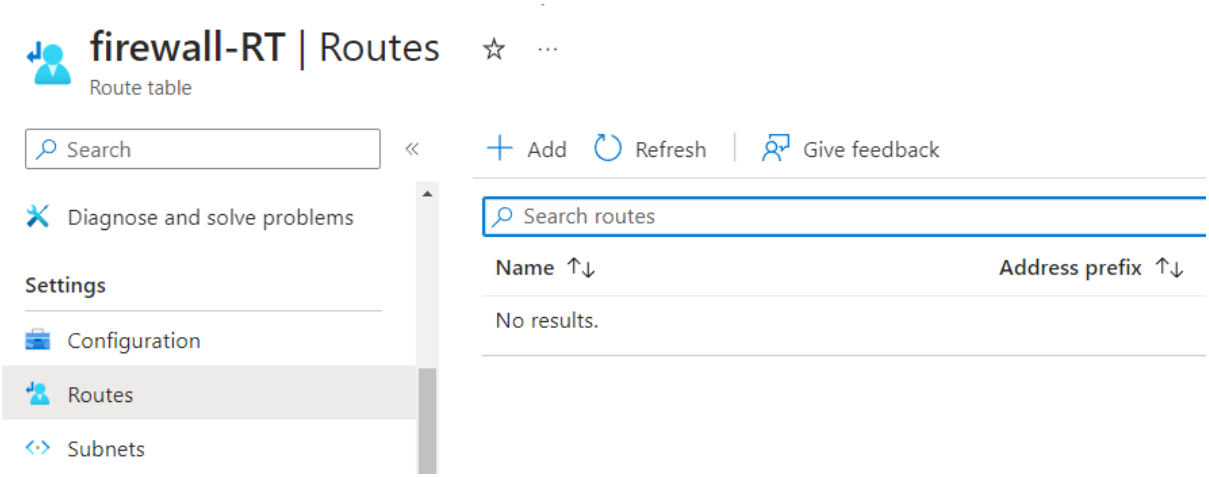
13. So, here you can see that we can reach the homepage of microsoft.com. So, remember the purpose of a firewall is to ensure that it restricts the traffic that is flowing out of your Azure virtual network.
14. So even though we have deployed the Azure Firewall onto our Azure virtual network, we don't 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.



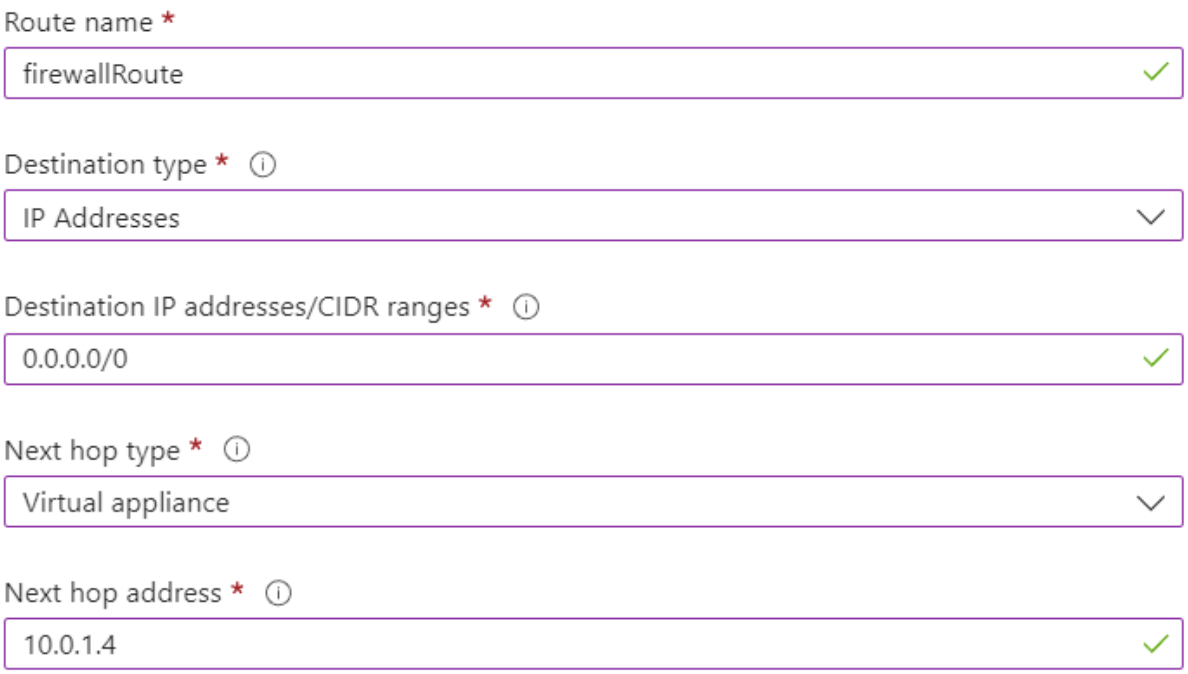
17. Once your route table has deployed go towards it. Then go to subnets and associate it with the default subnet that your VM has.



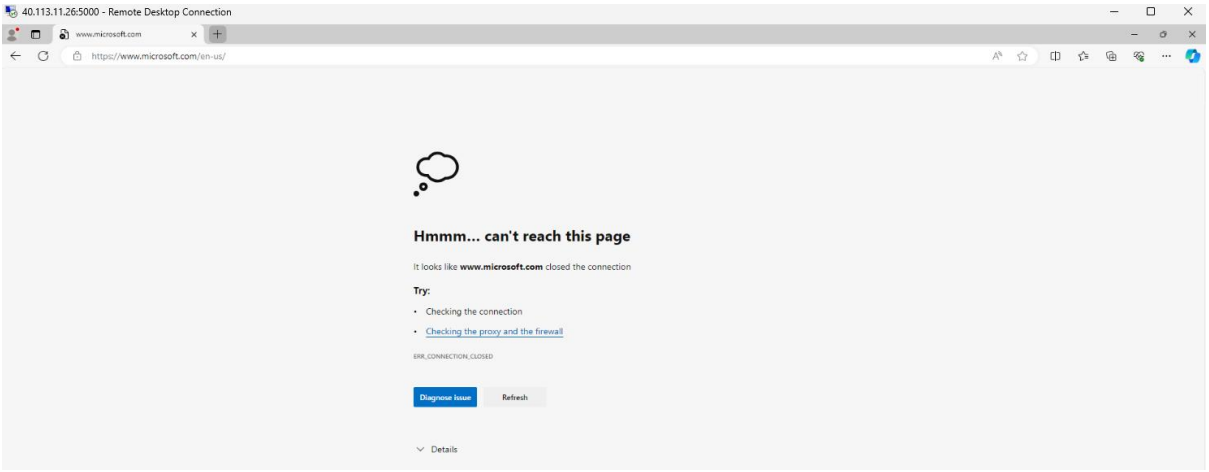
18. Then go to routes and add a route.



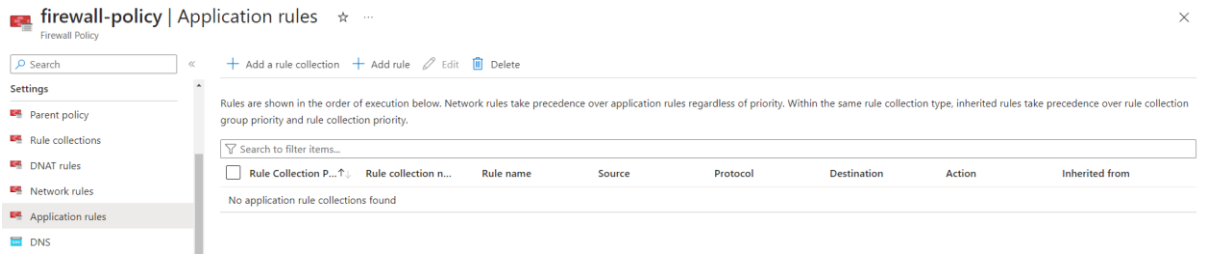
19. Now you need to give it a name then in the destination type choose the IP address and, in the destination, IP put the same address as shown below. After that, you need to choose a virtual appliance in the next hop type and the next hop address is the private IP address of your Firewall.



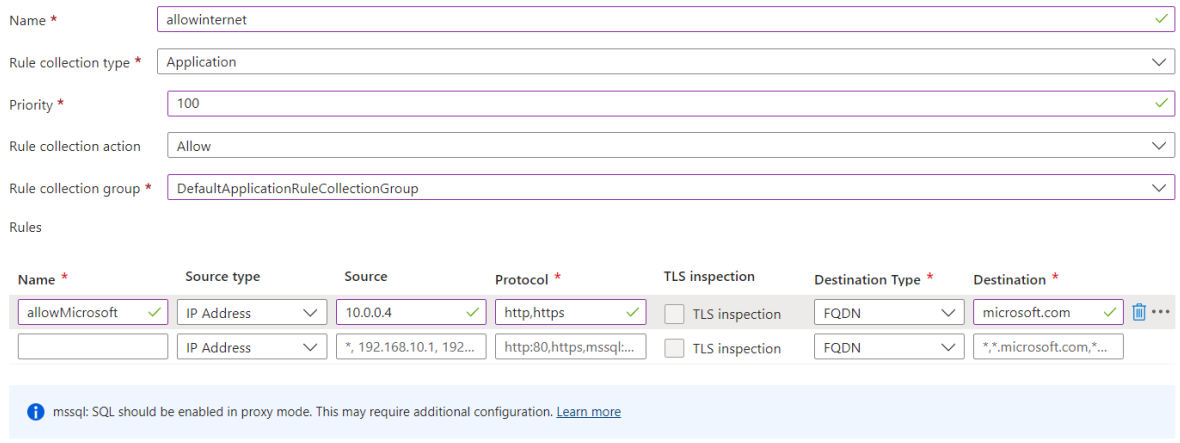
20. Once your route is in place then go to your VM and refresh the page then you will see that you are getting an error.



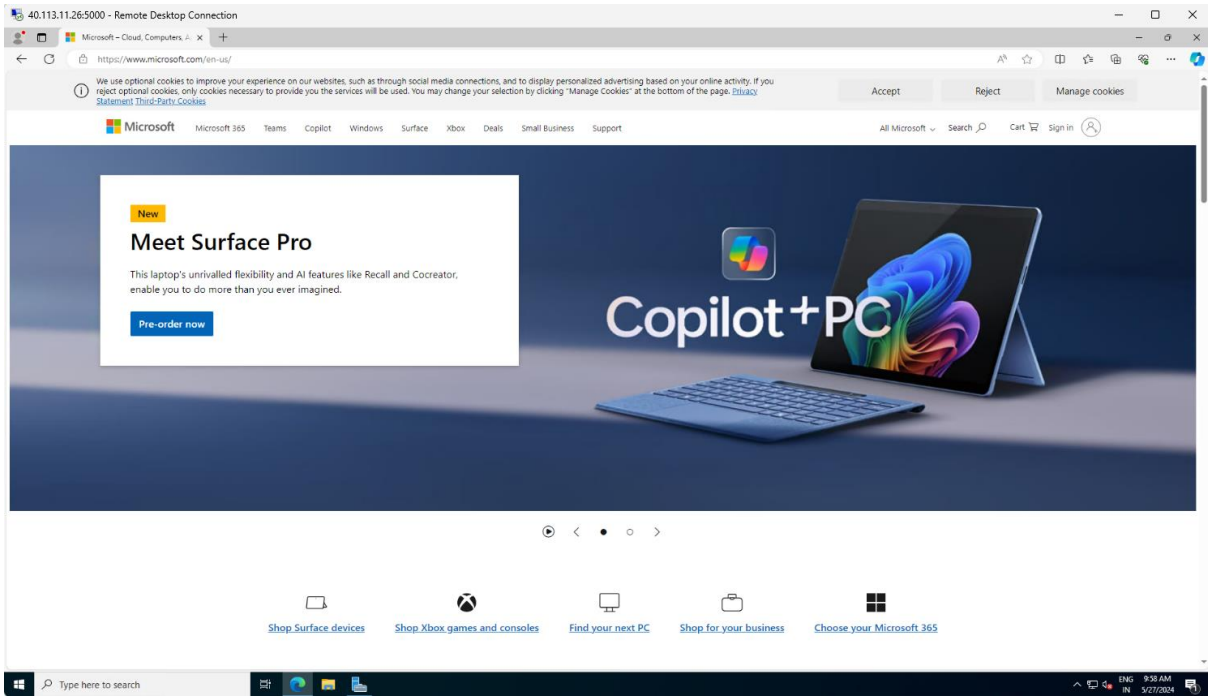
21. Now we are going to all the rules so that our VM can reach the internet. For that in firewall policy, you need to go to application rules and click on add a rule collection.



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.



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


40.113.11.26:5000 - Remote Desktop Connection
Microsoft – Cloud, Computers, A
https://www.microsoft.com/en-us/
We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. Privacy Statement Third-Party Cookies
Accept
Reject
Manage cookies
Microsoft
Microsoft 365
Teams
Copilot
Windows
Surface
Xbox
Deals
Small Business
Support
All Microsoft
Search
Cart
Sign in
New
Meet Surface Pro
This laptop's unrivalled flexibility and AI features like Recall and Cocreator, enable you to do more than you ever imagined.
Pre-order now
Copilot+PC
Shop Surface devices
Shop Xbox games and consoles
Find your next PC
Shop for your business
Choose your Microsoft 365
Type here to search
ENG
IN
9:58 AM
5/27/2024