😊 Network Security Group

A Network Security Group (NSG) in Azure is a fundamental component of network security that acts as a virtual firewall for controlling inbound and outbound traffic to Azure resources. It's a layer of security that helps protect your Azure Virtual Network (VNet) and the resources within it by allowing or denying traffic based on rules that you define.

Here are the key aspects of Network Security Groups (NSGs):

1. **Traffic Filtering:** NSGs allow you to define security rules that filter traffic based on criteria such as source and destination IP addresses, ports, and protocols. You can specify whether to allow or deny traffic that matches these criteria.
2. **Layer of Defense:** NSGs provide a layer of defense by allowing you to enforce network security policies at the subnet or individual resource level. This helps protect your Azure resources from unauthorized access, malware, and other security threats.
3. **Default and Custom Rules:** NSGs include default rules for allowing or denying traffic by default. Additionally, you can create custom rules to meet specific security requirements for your environment.
4. **Association with Resources:** NSGs can be associated with subnets, individual virtual machines (VMs), or network interfaces (NICs). When associated with a subnet, the NSG's rules apply to all resources within that subnet by default.
5. **Stateful Inspection:** NSGs perform stateful packet inspection, meaning they keep track of the state of active connections. This allows them to allow response traffic for outbound connections initiated from within the VNet without the need for explicit rules.
6. **Logging and Monitoring:** NSGs provide logging and monitoring capabilities, allowing you to track network traffic and security rule evaluations. This helps you identify and respond to security incidents and compliance requirements.

😄 Use Cases of Network Security Group:

Network Security Groups (NSGs) in Azure serve various use cases across different scenarios and industries. Here are some common ones:

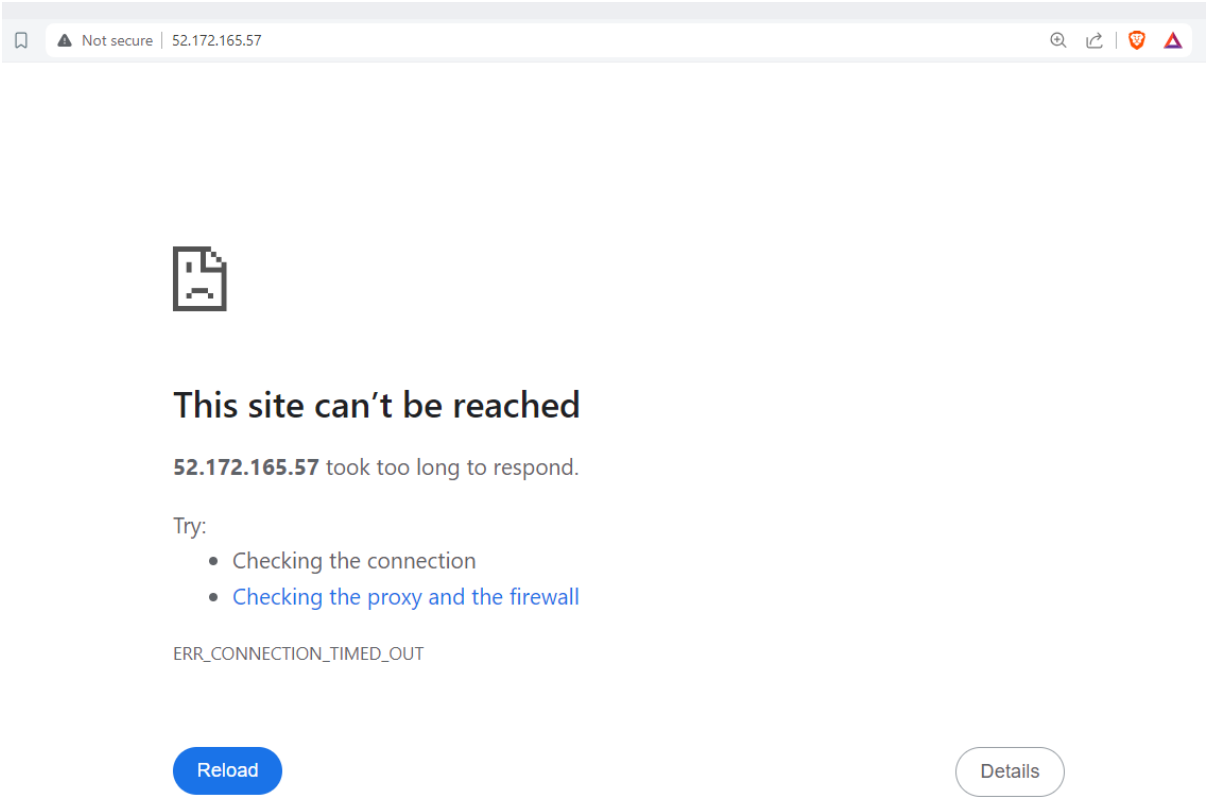
1. **Traffic Filtering and Access Control:** NSGs are commonly used to control inbound and outbound traffic to Azure resources based on specific criteria such as source and destination IP addresses, ports, and protocols. This use case is crucial for enforcing access control policies and limiting exposure to potential security threats.
2. **Segmentation and Isolation:** NSGs enable network segmentation by allowing you to define separate security rules for different subnets within a Virtual Network (VNet). This segmentation helps isolate resources and restrict communication between different tiers of applications, enhancing security and compliance.
3. **Application Security:** NSGs play a vital role in securing web applications and APIs hosted on Azure by allowing you to enforce security policies at the network level. You

can use NSGs to restrict access to sensitive endpoints, such as databases or administrative interfaces, and prevent unauthorized access or malicious attacks.

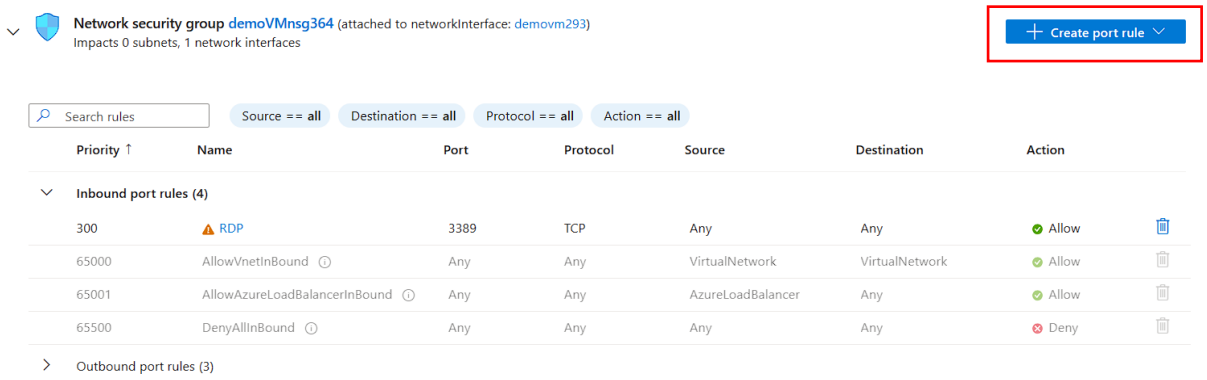
4. **Hybrid Cloud Security:** For organizations with hybrid cloud environments, NSGs help secure communication between Azure resources and on-premises networks. By defining rules that control traffic between Azure VNets and on-premises networks through VPN or ExpressRoute connections, NSGs ensure secure and compliant connectivity across hybrid deployments.
5. **Internet-Facing Applications:** NSGs are commonly used to secure internet-facing applications hosted on Azure by allowing or denying traffic from the public internet based on predefined criteria. By configuring NSG rules to permit only necessary inbound traffic and block unauthorized access attempts, organizations can protect their applications from external threats and attacks.
6. **Compliance and Regulatory Requirements:** NSGs help organizations meet compliance and regulatory requirements by enforcing network security policies that align with industry standards and best practices. By defining rules restricting access to sensitive data and resources, organizations can ensure data protection and maintain compliance with GDPR, HIPAA, and PCI DSS regulations.
7. **Monitoring and Auditing:** NSGs provide logging and monitoring capabilities that enable organizations to track network traffic and security rule evaluations. By monitoring NSG logs and analyzing network traffic patterns, organizations can identify and respond to security incidents, conduct audits, and enforce security policies effectively.

😄 To begin with the Lab:

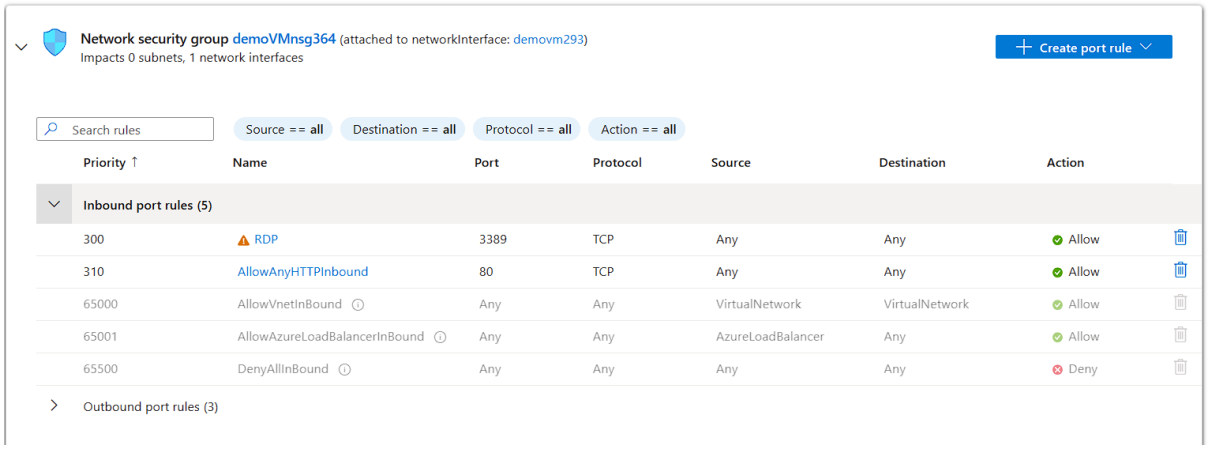
1. There are some prerequisites for this lab, and they are: You should have a virtual network in place on which your Windows virtual machine should be running.
2. Now you are going to RDP into your Virtual Machine and install IIS into your VM.
3. Once IIS is installed then you are going to copy the public IP address of your VM and paste it into a new browser or tab.
4. Immediately you will get this error that the site cannot be reached because at this moment we haven’t allowed port 80 for HTTP on our VM.



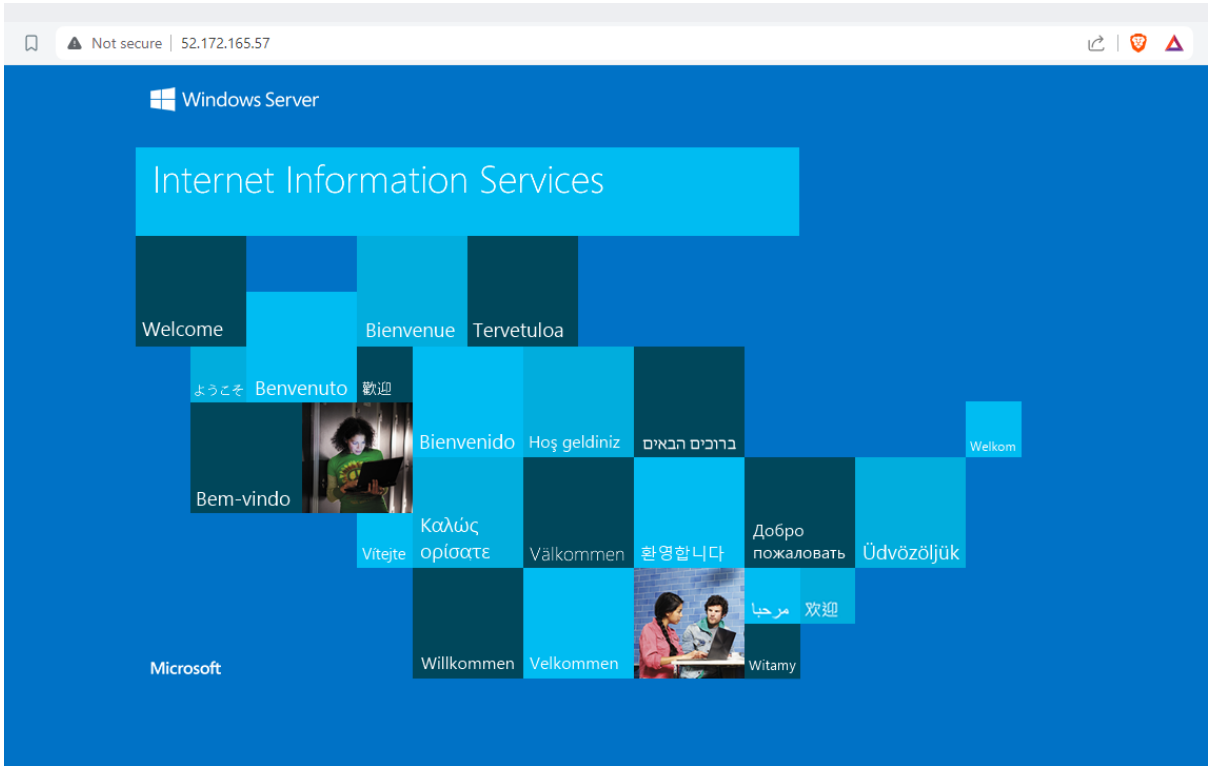
5. Now go to the networking section or say network security group then there you must click on create port rule then on the inbound rule.
6. Furthermore, you can see that port 3389 for RDP is allowed currently which let us to login to our VM and install IIS on it.



7. Now below you can see that port 80 has been allowed.
8. Go back to where you must try to open the web server and try to access it again.



9. Now you can see that it is working as expected.



😁 Step 1: Priority Setting

In Azure Network Security Groups (NSGs), priority settings determine the order in which security rules are evaluated. Each rule in an NSG has an associated priority value, ranging from 100 to 4096, where lower numbers indicate higher priority. When multiple rules match traffic, Azure applies the rule with the lowest priority value that matches the traffic, effectively giving it precedence.

Here's how priority settings work in NSGs:

1. **Evaluation Order:** NSG rules are evaluated in priority order, starting from the lowest priority value (e.g., 100) to the highest priority value (e.g., 4096). Azure evaluates traffic against each rule sequentially until it finds a match.

2. **Matching Traffic:** When traffic matches the criteria specified in a rule (e.g., source IP address, destination port), Azure applies the corresponding action defined in that rule (e.g., allow, deny).
3. **Rule Conflicts:** If multiple rules match the same traffic, Azure applies the rule with the lowest priority value. Therefore, it's essential to set the priority values appropriately to ensure that the desired rules take precedence.
4. **Default Rules:** NSGs include default rules for inbound and outbound traffic with priority values of 65000 and 65500, respectively. These rules allow all traffic by default unless overridden by specific rules with lower priority values.
5. **Custom Rules:** You can create custom rules with priority values based on your requirements. Lower priority values indicate higher precedence, so rules with lower priority values are evaluated before rules with higher priority values.
6. **Rule Modification:** You can modify the priority of existing rules to change their evaluation order. Adjusting the priority values allows you to fine-tune the behavior of NSGs and ensure that traffic is handled according to your security requirements.

😄 Use cases of Priority setting:

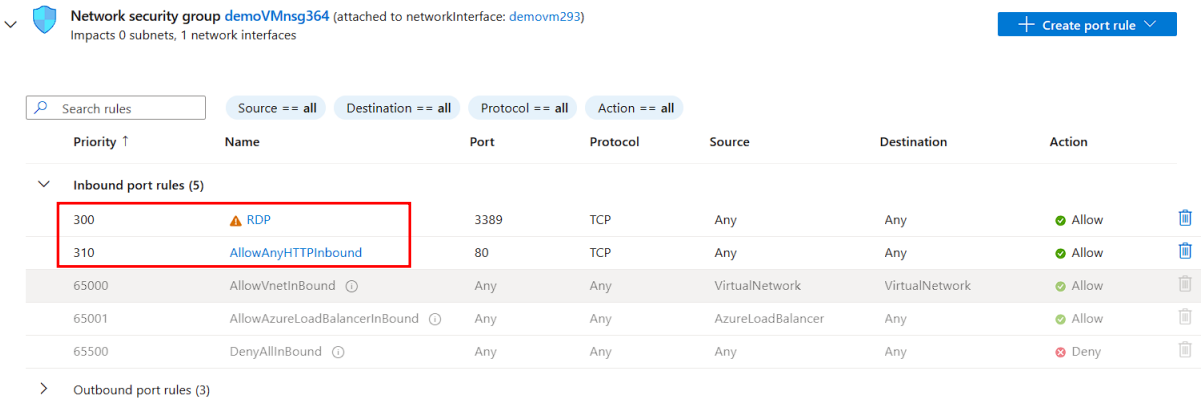
The priority setting in Azure Network Security Groups (NSGs) is crucial for controlling the order in which security rules are evaluated. Here are some common use cases for prioritizing NSG rules:

1. **Traffic Prioritization:** By assigning lower priority values to specific rules, you can ensure that critical traffic is processed before less important traffic. For example, you may prioritize rules that allow access to essential services or applications over rules that allow less critical traffic.
2. **Overriding Default Rules:** Azure NSGs include default rules that allow or deny traffic by default. However, you may need to override these default rules with custom rules that have lower priority values. This allows you to define more specific security policies tailored to your organization's requirements.
3. **Enforcing Security Policies:** Priority settings enable you to enforce security policies effectively by ensuring that security rules are applied in the correct order. For example, you can prioritize rules that block traffic from known malicious IP addresses or restrict access to sensitive resources to prevent unauthorized access attempts.
4. **Network Segmentation:** When implementing network segmentation, you can use priority settings to control the flow of traffic between different segments of your network. By assigning lower priority values to rules that allow traffic within the same segment and higher priority values to rules that allow traffic between segments, you can enforce strict segmentation policies.
5. **Load Balancing and Redundancy:** If you're using Azure Load Balancer or implementing redundant network configurations, you can prioritize rules to ensure that traffic is distributed evenly across multiple endpoints. By assigning lower priority values to rules associated with active endpoints and higher priority values to rules associated with standby endpoints, you can achieve load balancing and failover capabilities.

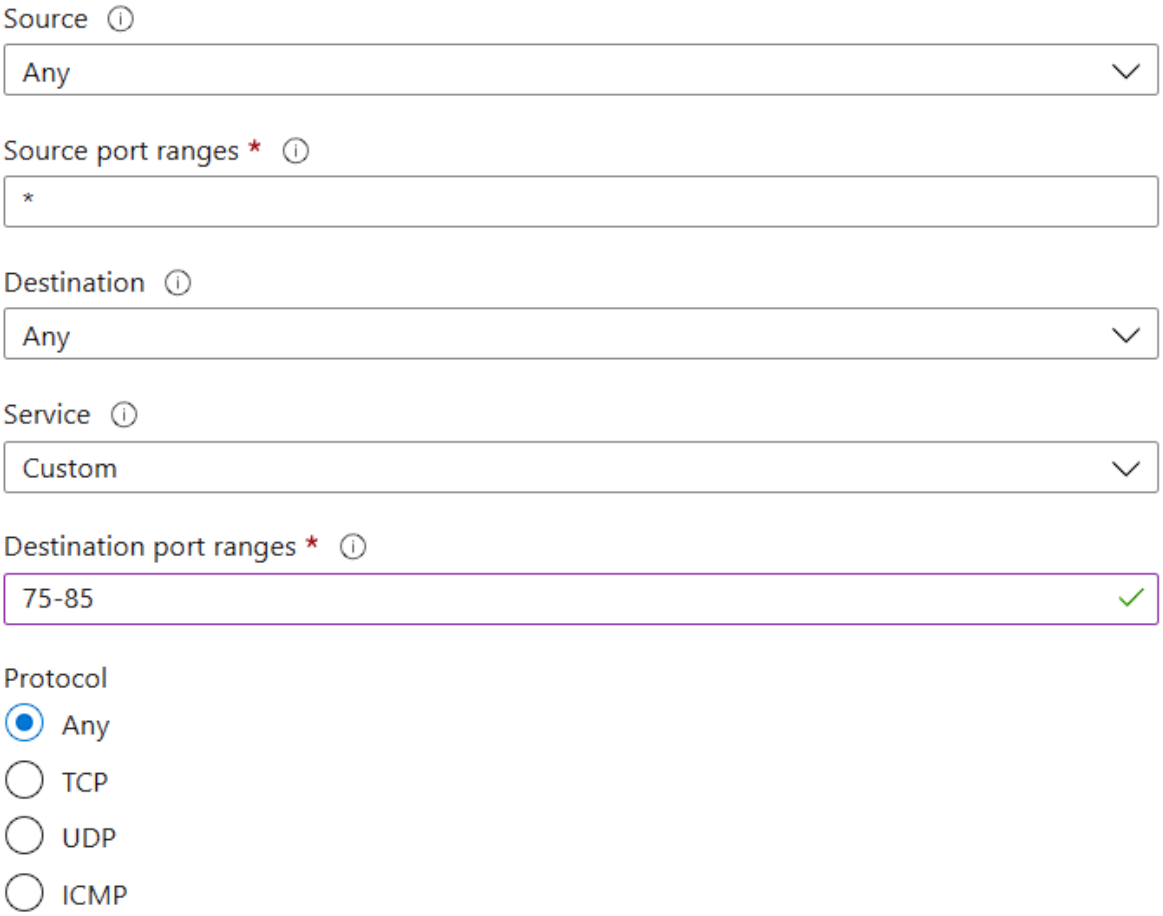
6. **Compliance Requirements:** Priority settings allow you to meet compliance requirements by ensuring that security rules are evaluated in the correct sequence. For example, you can prioritize rules that enforce compliance with industry regulations or internal security policies to ensure that they are applied consistently across your Azure environment.

Now in your Azure Portal in the Network security group.

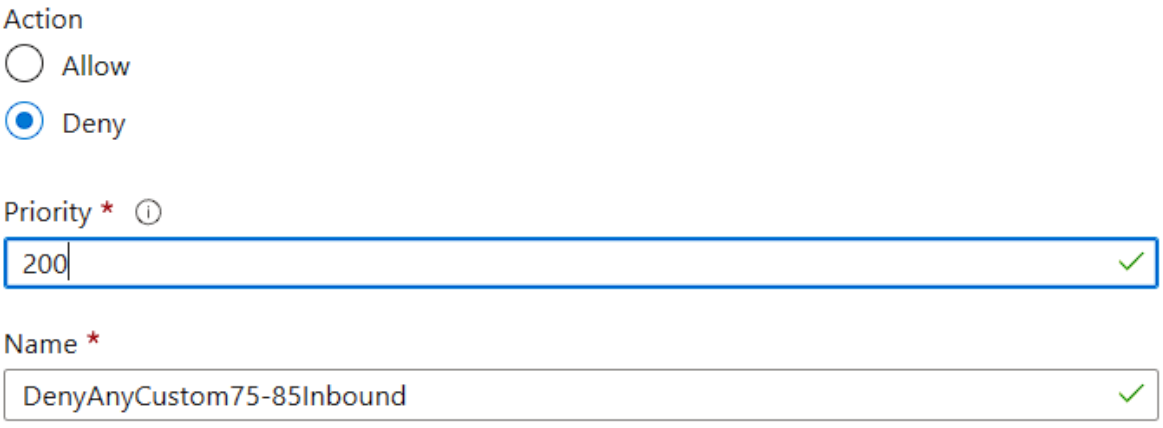
1. Now from the above you know that we created a port rule for port 80.
2. And below you can see that currently, we have two inbound port rules allowed one for RDP (3389) and the other for HTTP (80).
3. If you look carefully they both have a priority set, RDP has a priority of 300 and HTTP has priority of 310.



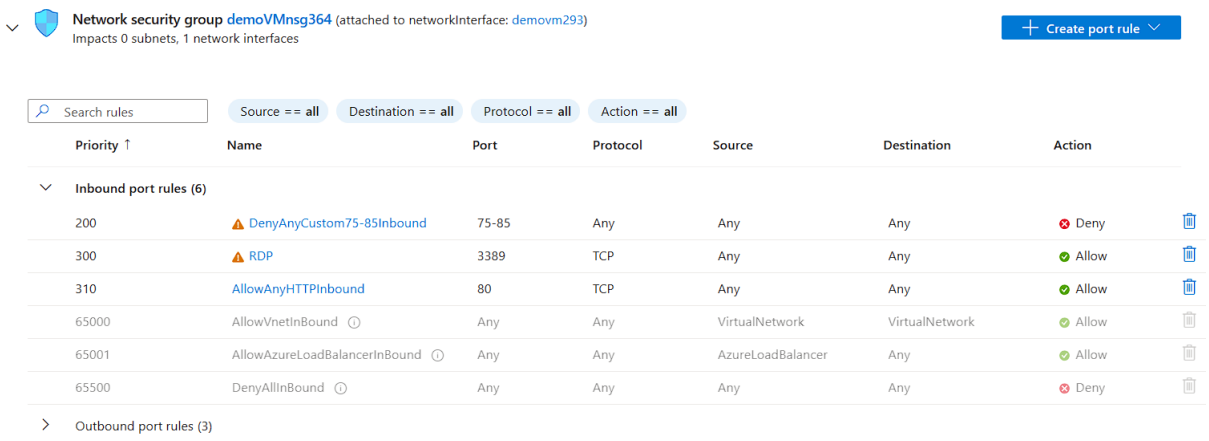
4. Now we are going to create another inbound port rule to allow traffic.
5. Below you can see that we have defined service as custom and the destination port ranges between port 75 to 85.



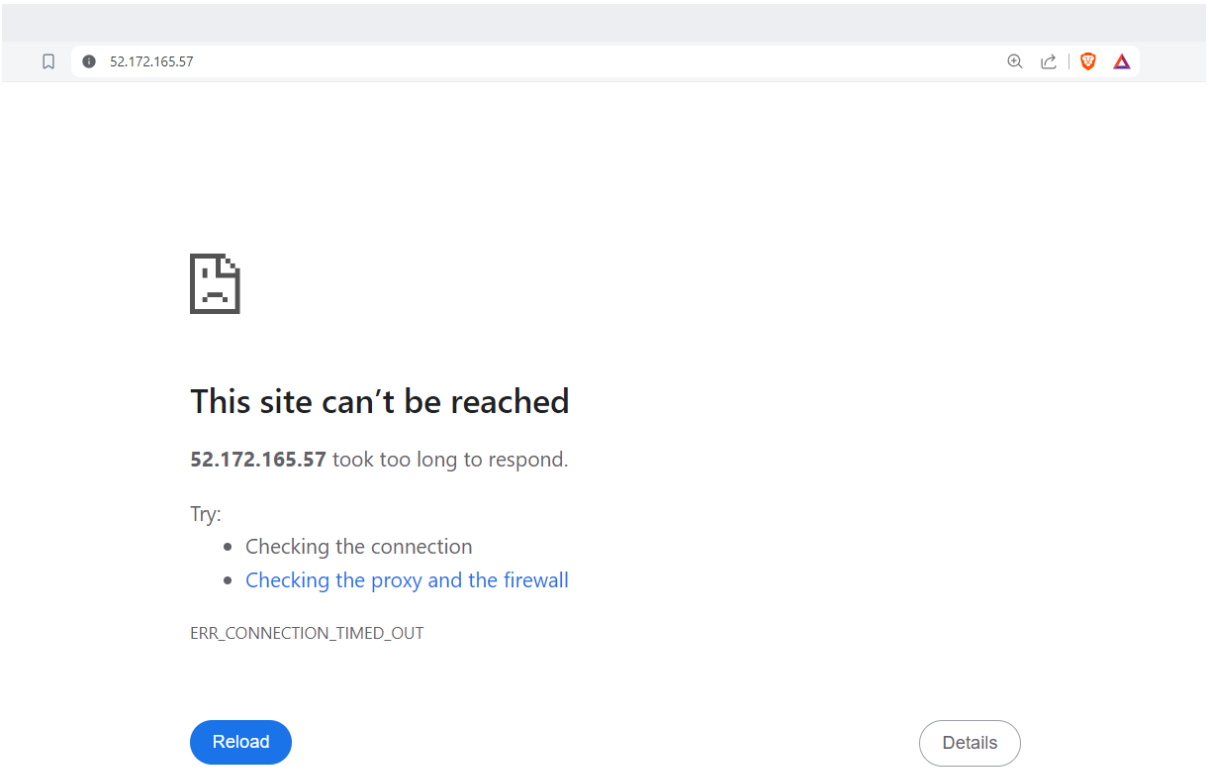
7. And you can see that the action we selected is deny and we this time we have set the priority to 200. And just create our inbound port rule.



8. Below you can see that we now have a new inbound port rule.

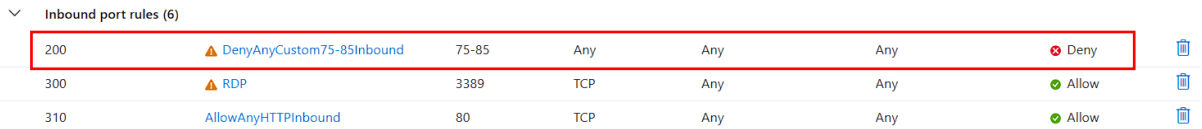


9. Now again we will copy the public IP address of the VM and paste it in a new browser to check whether our web server is running or not.
10. You will notice that you are getting an error.

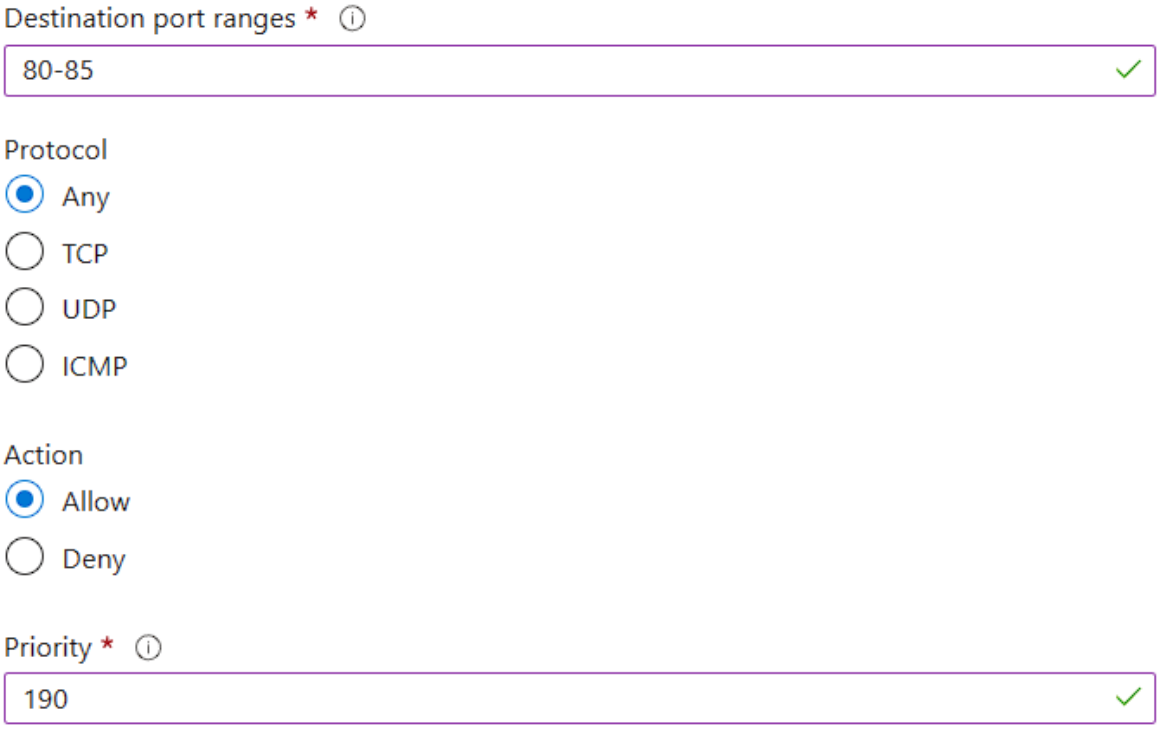


11. So, we added a deny rule but then we also have this allow rule as well to allow traffic on Port 80. How does the NSG know or how does the NSG evaluate whether to allow or deny a request? What happens is that we said, let's say that the request is coming in right on the VM on Port 80.
12. First, it's going to go in the order of priority. It's going to check each rule. It will check the first rule with a priority of 200 here the request matches this rule because we are making a request onto Port 80 for the VM. It's coming in from any source. It's going on to any destination. Hence, it's going to deny the request. It is not going to proceed on

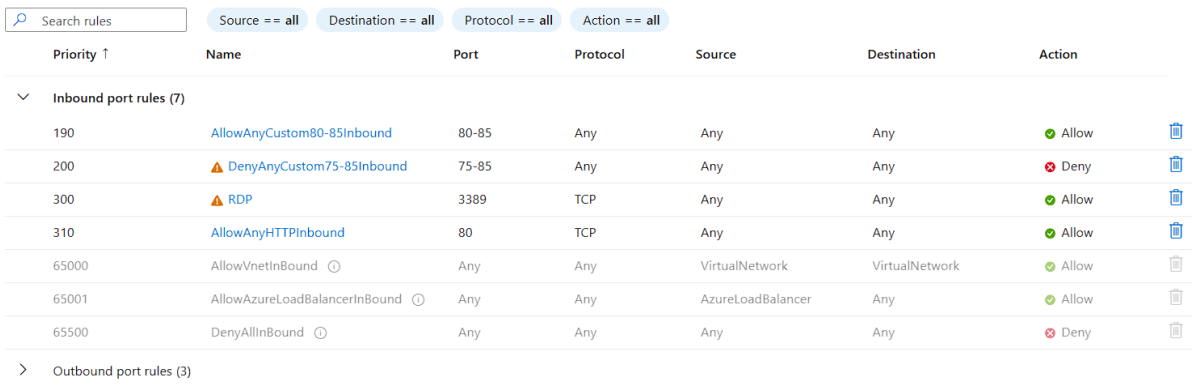
to the other rules. Once it finds a matching rule, whether it be allowed or denied, it's going to evaluate that rule and not evaluate the rules thereafter. That is why it is not even considering this rule of allow HTTP inbound traffic.



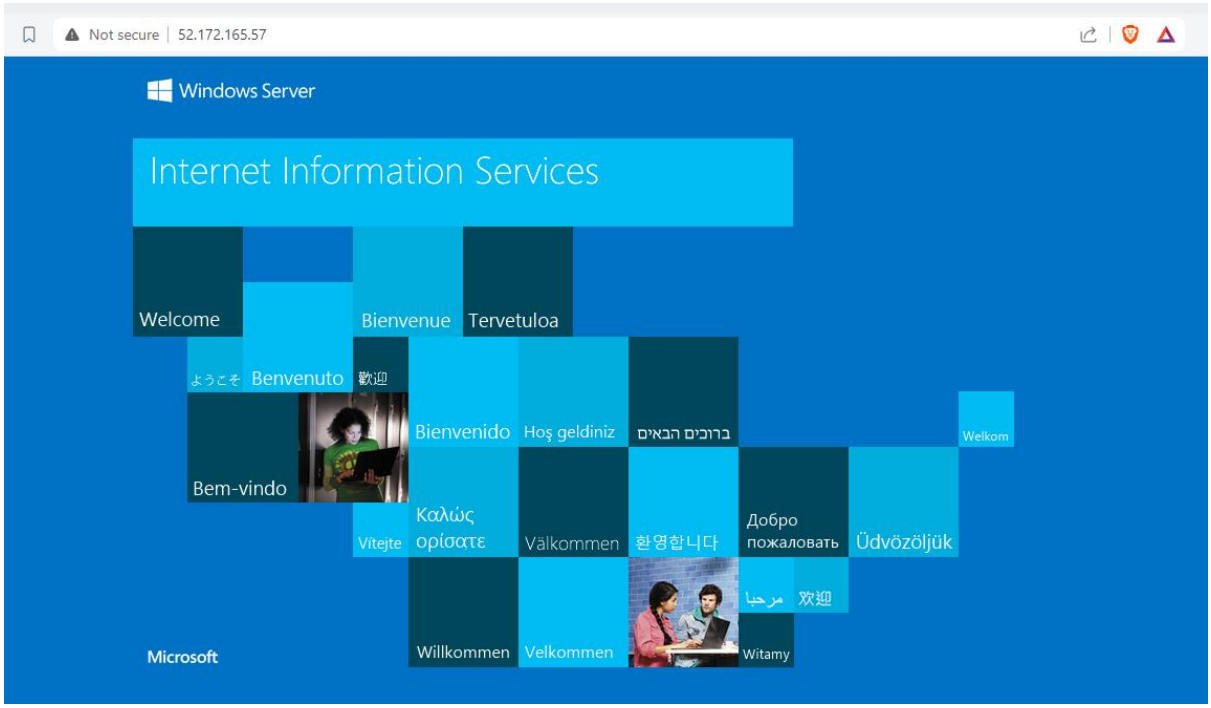
13. So, when it comes to network security groups, it does not try to add the conditions of all the rules together and then do the evaluation. No, it goes step by step, rule by rule. And if a rule is being matched, it will go ahead and proceed with that rule.
14. Now again we are going to create a new inbound rule to allow port range between 80-85 and we have the set the priority to 190.



15. Below you can see that the rule has been created.



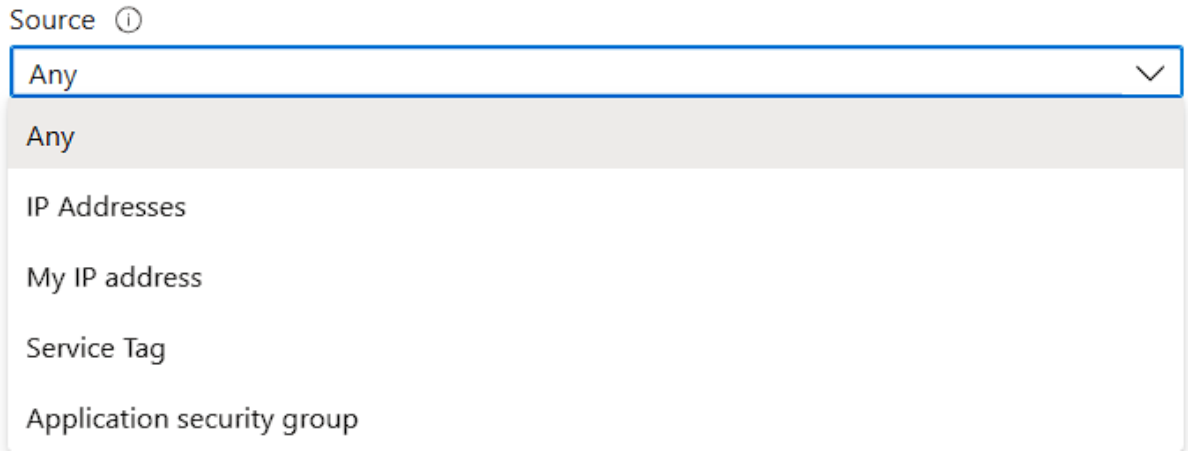
16. Now if you go back again and refresh the page where you have tried to access the web server. You will see that everything is working as expected.

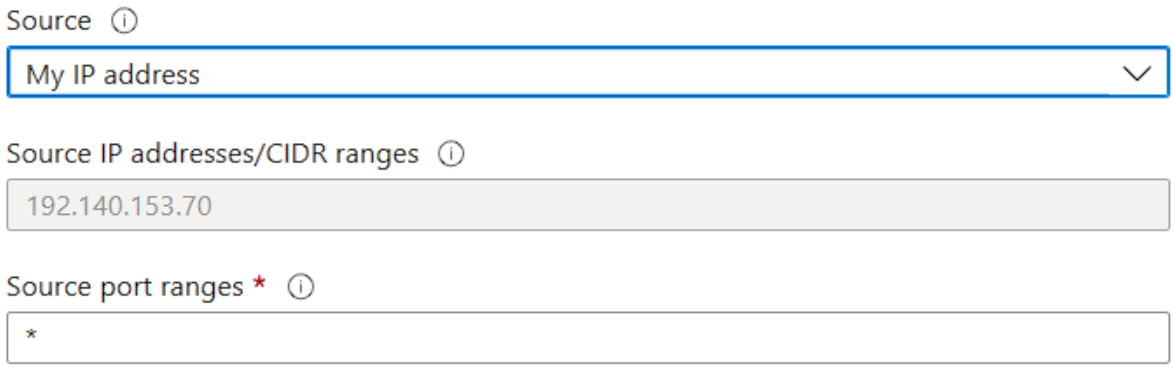


17. Once you are done just delete the inbound rules that you have created.

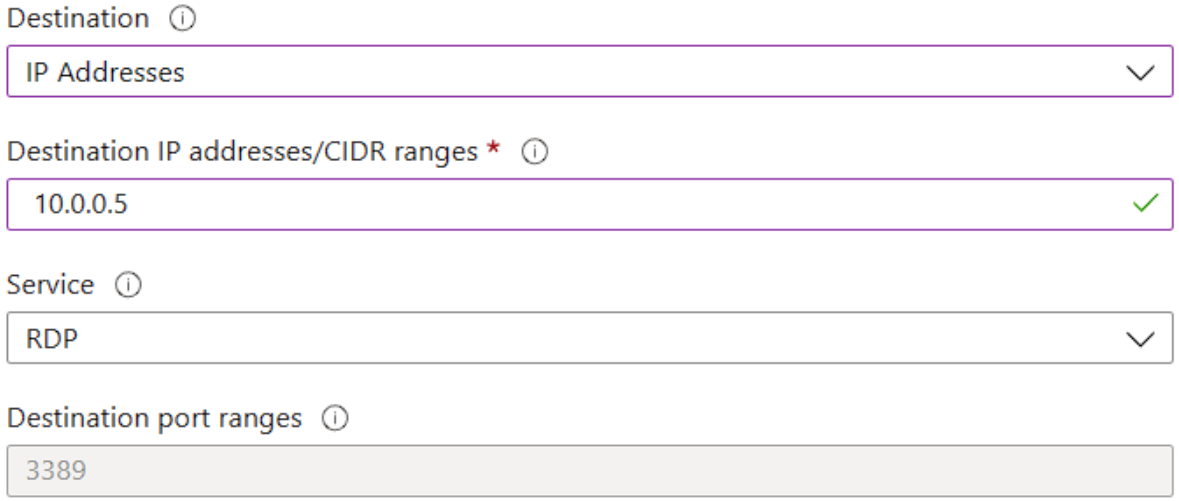
😁 Step 2: IP Address

1. Now here we are going to allow only the VM's private IP address for RDP.
2. In your network security group if you click on RDP inbound rule you will see that you can make changes to it.
3. Here in sources, you have so many options to choose from but for now we will choose My IP address.
4. Now here I want to say that only connections from only my laptop should be accepted by the virtual machine.

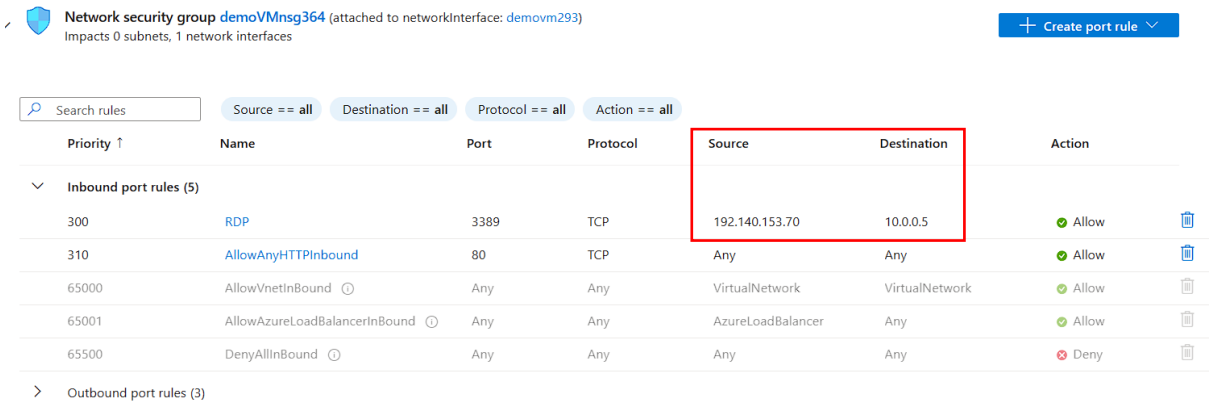




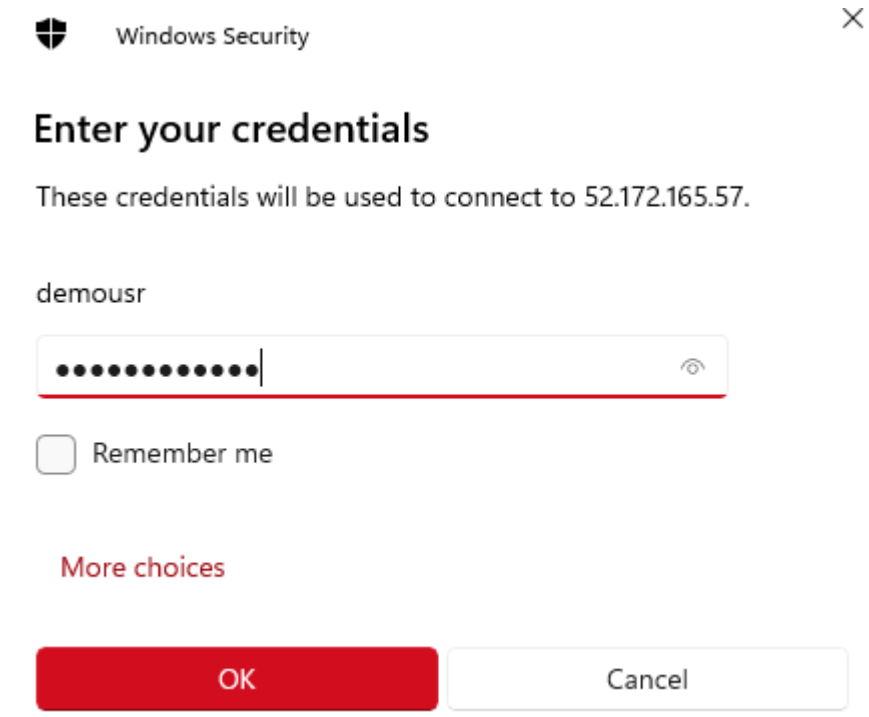
5. You want to be very specific. You want to say that you only want to connect to the app because see here the destination is VM and the source is our laptop. We want to connect onto the destination. That's the virtual machine here. Also, we can specify the Private IP address.
6. Then just click on save.

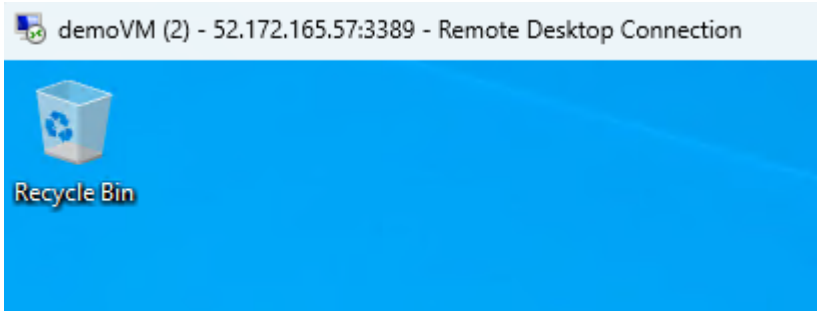


7. Now you can see the source and destination in your inbound rule.



8. Now you are going to make a connection. Below you can see that it is asking you for the password which means that the connection was successful.





😁 Step 3: Outbound rules

Outbound port rules in Azure Network Security Groups (NSGs) define the allowed or denied outbound traffic from Azure resources based on destination port numbers. These rules are applied to control the traffic leaving the Azure Virtual Network (VNet) and are commonly used for various purposes, such as:

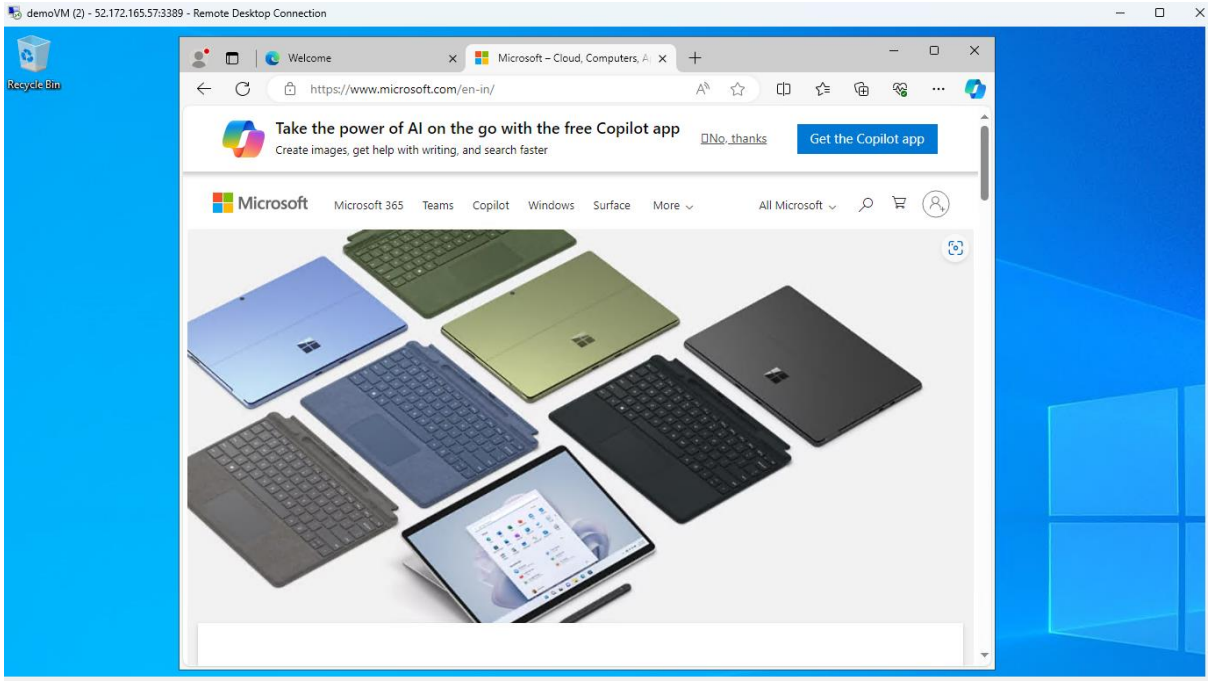
1. **Restricting Outbound Access:** Outbound port rules can be used to restrict outbound access from Azure resources to specific destination ports or port ranges. This helps enforce security policies and prevent unauthorized communication with certain external services or destinations.
2. **Enforcing Compliance:** Outbound port rules can help organizations enforce compliance requirements by blocking outbound traffic to ports associated with non-compliant or restricted services. For example, organizations may block outbound traffic to ports commonly used for peer-to-peer file sharing or communication protocols that are not compliant with industry regulations.
3. **Limiting Outbound Communication:** Outbound port rules can be used to limit outbound communication to only essential ports required for legitimate business

purposes. By restricting outbound traffic to specific ports, organizations can minimize the risk of data exfiltration, malware propagation, or other malicious activities that may exploit unnecessary outbound communication channels.

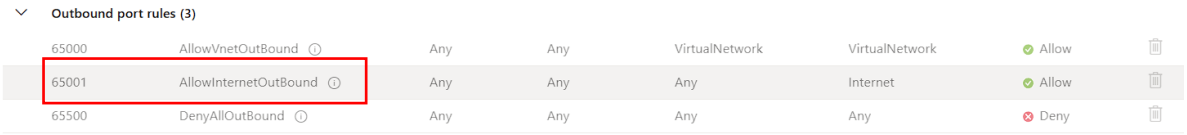
4. **Preventing Data Leakage:** Outbound port rules can help prevent data leakage by blocking outbound traffic to ports commonly associated with data exfiltration techniques or unauthorized data transfer methods. By blocking outbound access to these ports, organizations can mitigate the risk of sensitive data leaving the Azure environment without authorization.
5. **Protecting Against Threats:** Outbound port rules can be used as part of a defense-in-depth strategy to protect Azure resources against outbound threats, such as malware or command-and-control communication. By blocking outbound access to ports commonly used by malware or malicious actors, organizations can reduce the risk of compromise and unauthorized access to external resources.
6. **Auditing and Monitoring:** Outbound port rules can also be used for auditing and monitoring purposes to track outbound traffic patterns and detect anomalous or suspicious activities. By logging outbound traffic allowed or denied by specific port rules, organizations can gain visibility into potential security incidents and proactively respond to threats or policy violations.

Now to begin Outbound Port Rules:

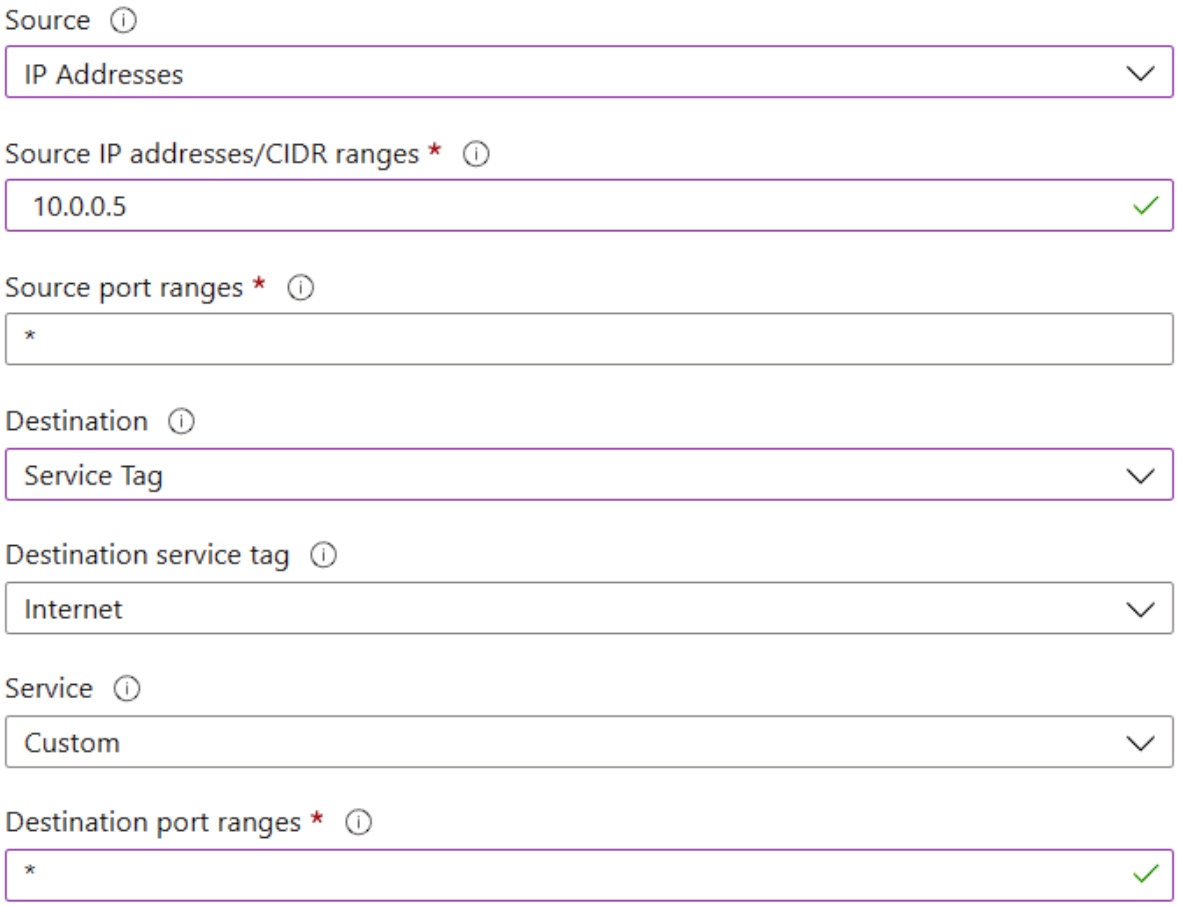
1. Now in this part we are going to discuss about outbound port rules.
2. First you are going to login to your VM then you are going to open edge browser in your VM and open Microsoft.com in it.
3. You will see that you were able to reach the website easily.



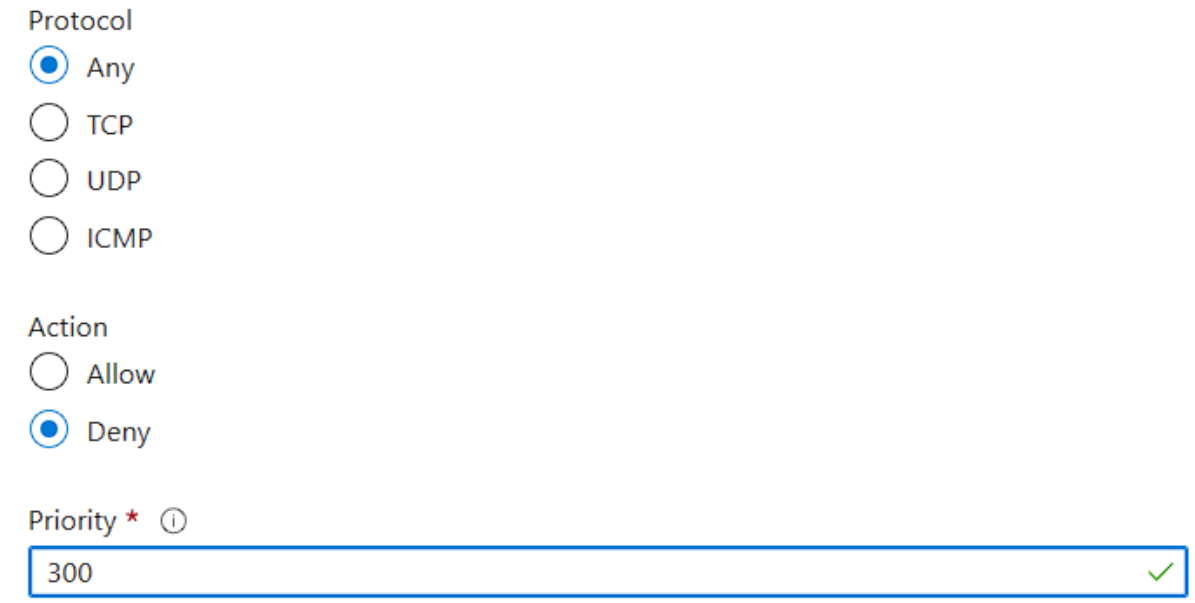
4. This is because in your outbound port rules you can see that by default port number 65001 with the name Allow internet outbound is allowed.



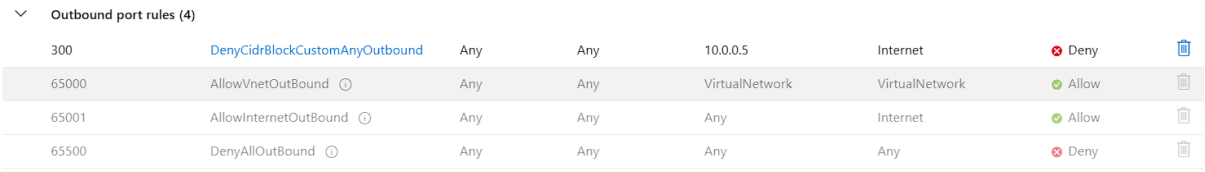
5. Now you are going to create an outbound port rule.
6. The source is the IP address of the virtual machine itself because this is now traffic that is being initiated. This is an outbound port rule traffic that has been initiated from the VM onto the outside world.
7. Put the private IP address of your VM then the destination is Service tag of Internet. Then in destination port ranges put a star (*) basically it means any port range on the internet.



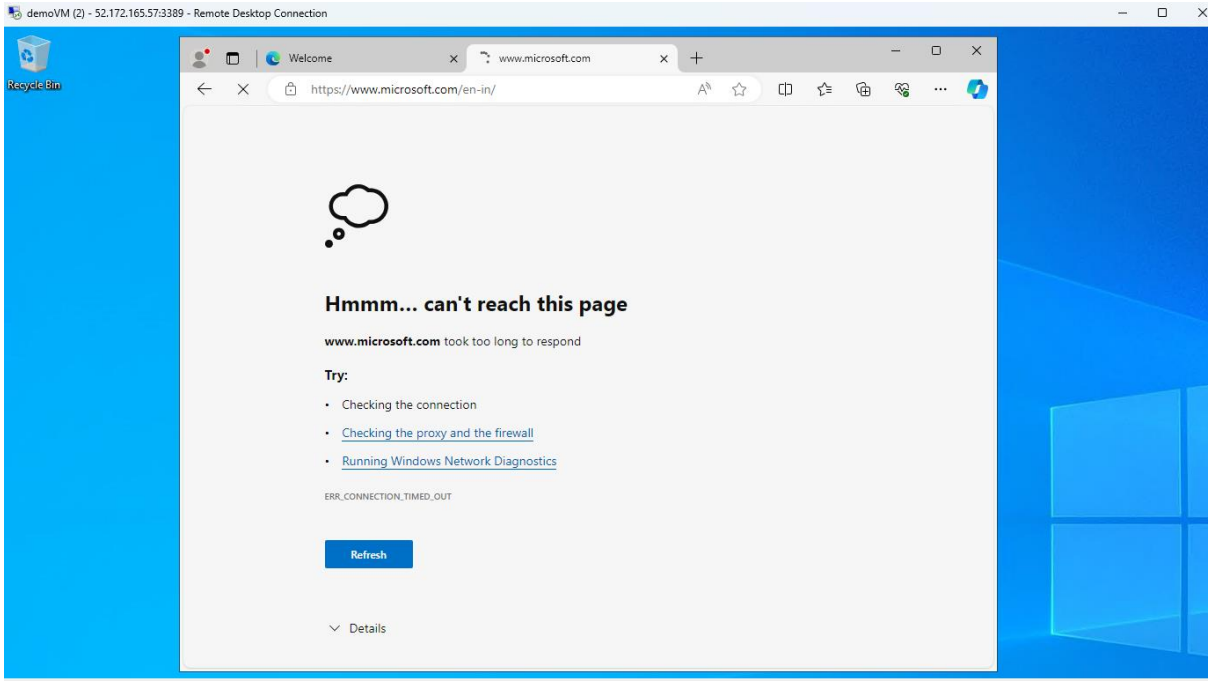
8. Then the protocol type is Any and the action here is deny. Set the priority to 300.



9. Below you can see the outbound port accordingly.



10. Now if you back to your virtual machine and refresh the Microsoft.com page then you will see that it is not able to reach the page.



11. Now if you will delete the outbound port rule you will see that the Microsoft.com is reachable now.

😁 Step 4: Allow ICMP

ICMP (Internet Control Message Protocol) is a protocol used for diagnostic and control purposes within IP networks, including the internet. It's primarily used for sending error messages, network status updates, and troubleshooting information between devices on a network. ICMP messages are typically encapsulated within IP packets and are an integral part of the Internet Protocol suite.

Here are some key aspects of ICMP:

1. **Error Reporting:** ICMP is commonly used to report errors encountered during the transmission of IP packets. For example, when a packet cannot reach its destination due to network congestion or an unreachable host, ICMP error messages are sent back to the source to inform it of the issue.
2. **Network Status Updates:** ICMP messages are used to provide status updates about network conditions, such as notifying routers about changes in network topology or informing hosts about changes in routing tables.
3. **Ping and Echo Requests:** One of the most well-known uses of ICMP is for the "ping" command, which sends ICMP Echo Request messages to a destination host and waits for ICMP Echo Reply messages in response. This is commonly used to test network connectivity and measure round-trip latency.
4. **Traceroute:** ICMP is also used in the "traceroute" command, which sends a series of ICMP Time Exceeded messages with increasing Time-to-Live (TTL) values to determine the path that packets take to reach a destination.
5. **Path MTU Discovery:** ICMP is used for Path MTU Discovery, a process to determine the maximum transmission unit (MTU) size along a path between two hosts. This helps prevent fragmentation of packets and improves network performance.
6. **Security Implications:** While ICMP is essential for network troubleshooting and diagnostics, it can also be exploited for malicious purposes, such as ICMP-based denial-of-service (DoS) attacks or network reconnaissance. As a result, network administrators may choose to control ICMP traffic using firewalls or network security policies.

😁 Use cases of ICMP:

ICMP (Internet Control Message Protocol) serves various use cases in network communication and diagnostics. Here are some common scenarios where ICMP is utilized:

1. **Network Connectivity Testing:** ICMP is widely used for testing network connectivity between devices. The "ping" command sends ICMP Echo Request messages to a target host, and if the host is reachable, it responds with ICMP Echo Reply messages. This use case helps diagnose network connectivity issues and measure round-trip latency.
2. **Network Troubleshooting:** ICMP provides valuable diagnostic information for troubleshooting network problems. ICMP error messages, such as Destination Unreachable and Time Exceeded, help identify issues like unreachable hosts, network

congestion, or routing problems. This information assists network administrators in resolving connectivity issues efficiently.

3. **Network Path Analysis:** Traceroute, a tool based on ICMP, traces the path that packets take from the source to the destination. By sending ICMP Echo Request messages with varying Time-to-Live (TTL) values, Traceroute elicits ICMP Time Exceeded messages from intermediate routers, revealing the path and network latency between two hosts.
4. **MTU Discovery:** ICMP Path MTU Discovery is used to determine the Maximum Transmission Unit (MTU) along a network path. By sending ICMP messages with varying packet sizes, hosts can identify the largest packet size that can traverse the network without fragmentation. This helps optimize network performance and prevent packet loss due to fragmentation.
5. **Router Configuration and Management:** ICMP is essential for router configuration and management tasks. Network administrators use ICMP Echo Request and Reply messages to verify connectivity to routers and other network devices. ICMP is also used for remotely accessing routers through protocols like SNMP (Simple Network Management Protocol).
6. **Network Monitoring and Diagnostics:** ICMP messages are valuable for network monitoring and diagnostics. By monitoring ICMP traffic, network administrators can detect and respond to network anomalies, such as high latency, packet loss, or network congestion. ICMP-based monitoring tools provide insights into network performance and reliability.
7. **Security and Firewall Configuration:** ICMP can be used for security-related purposes, such as implementing firewall rules to allow or block ICMP traffic. Network administrators can configure firewalls to permit specific ICMP message types while blocking others to enhance network security and prevent ICMP-based attacks, such as Ping Flood attacks.

Now in this part we are going to allow ICMP.

1. Now if you try to ping the public IP address of your VM from your laptop.
2. You will see that the request has been timed out.

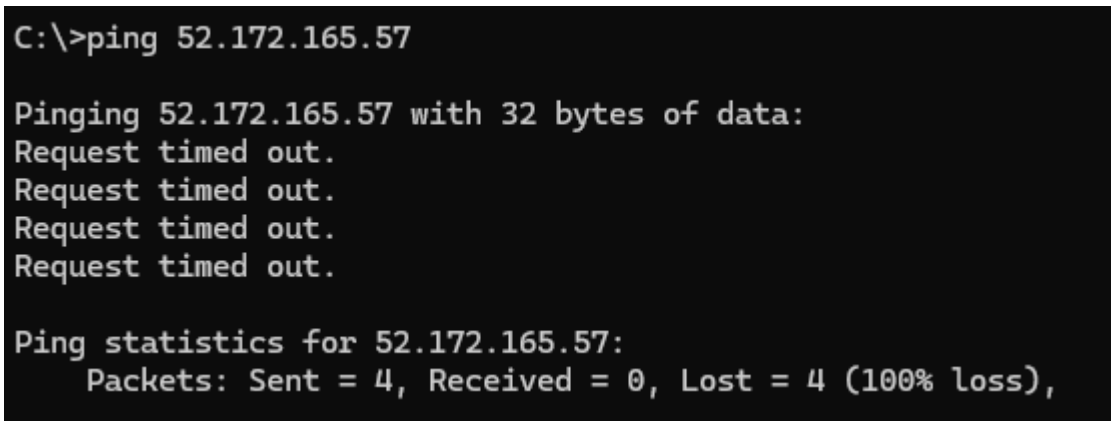
```
C:\>ping 52.172.165.57

Pinging 52.172.165.57 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 52.172.165.57:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

3. So, to allow this particular request we are going to add an inbound port rule for ICMP.
4. Now click on create inbound port rule and keep everything to default just in the protocol type choose ICMP and create inbound port rule.

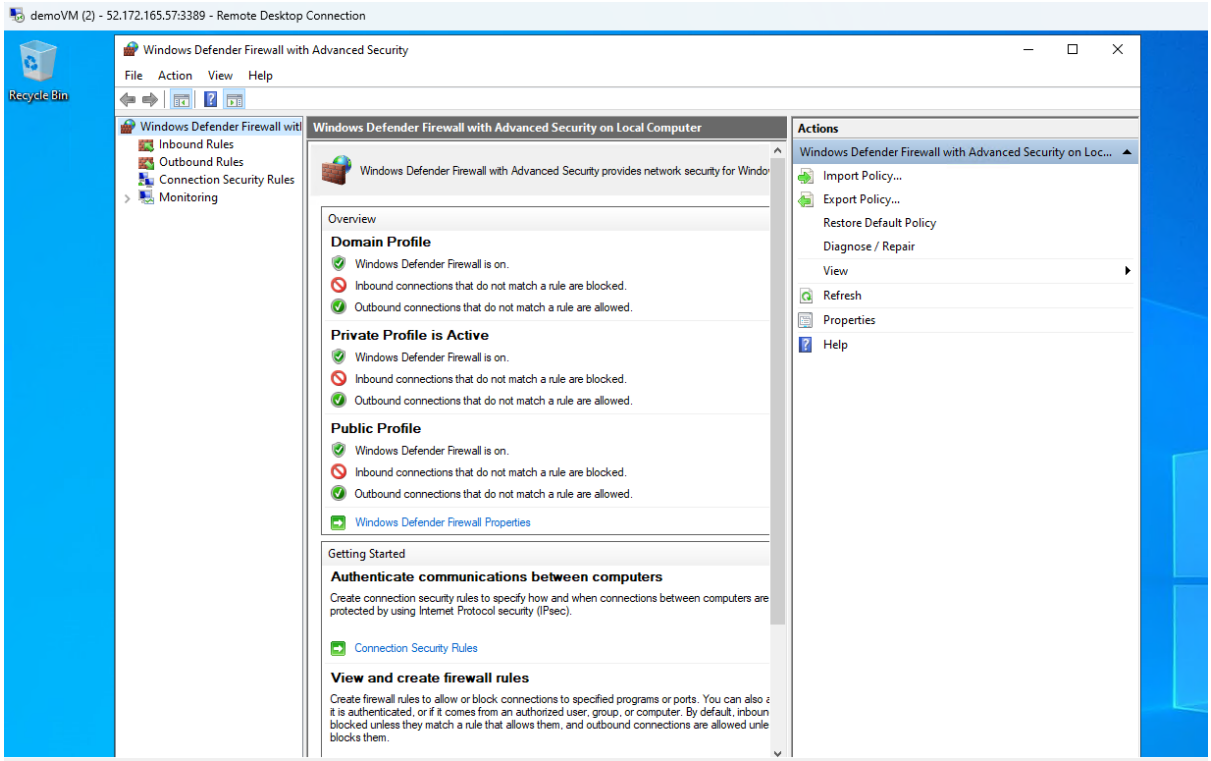
Protocol

- (•) Any
- ( ) TCP
- ( ) UDP
- (•) ICMP

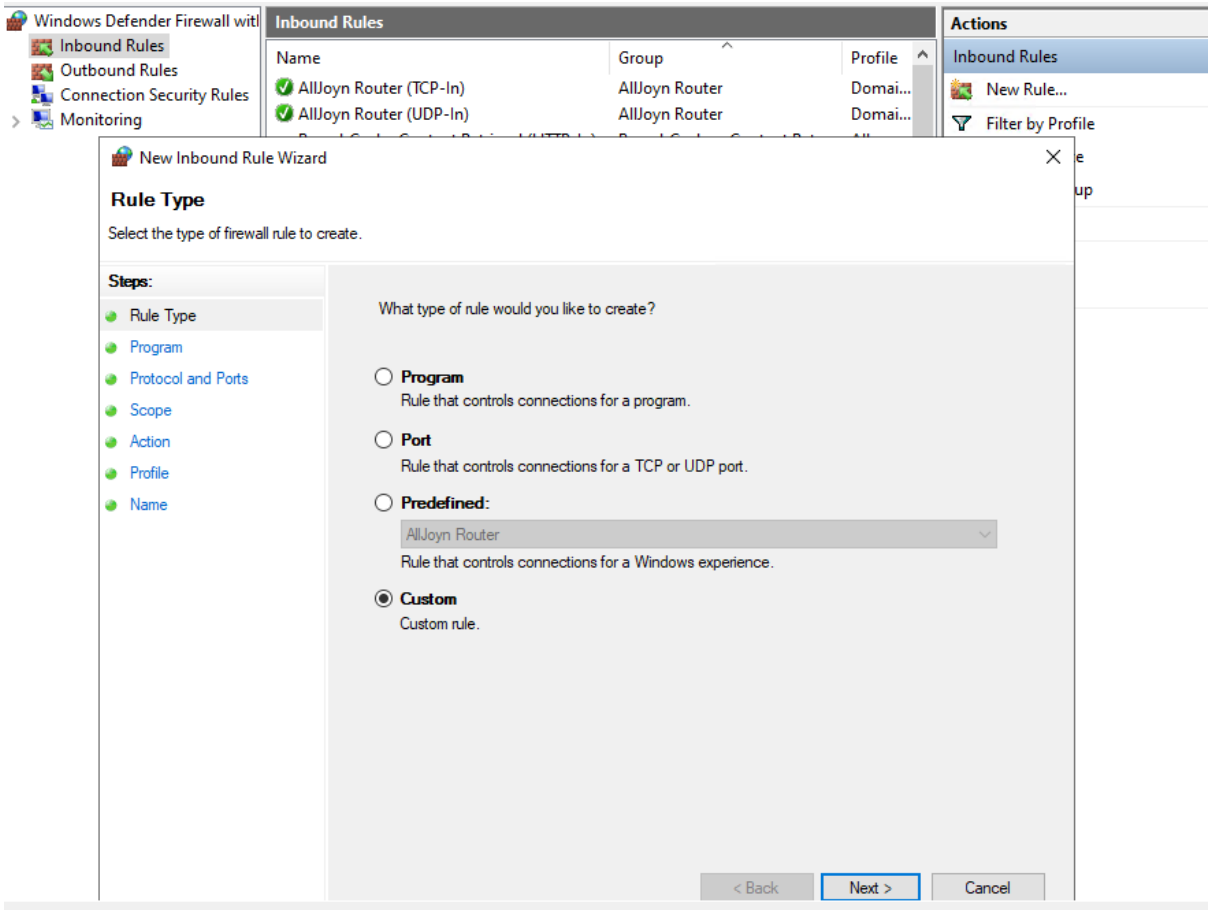
5. Now go back to command prompt and run the request again. You will see that the request has been timed out again.



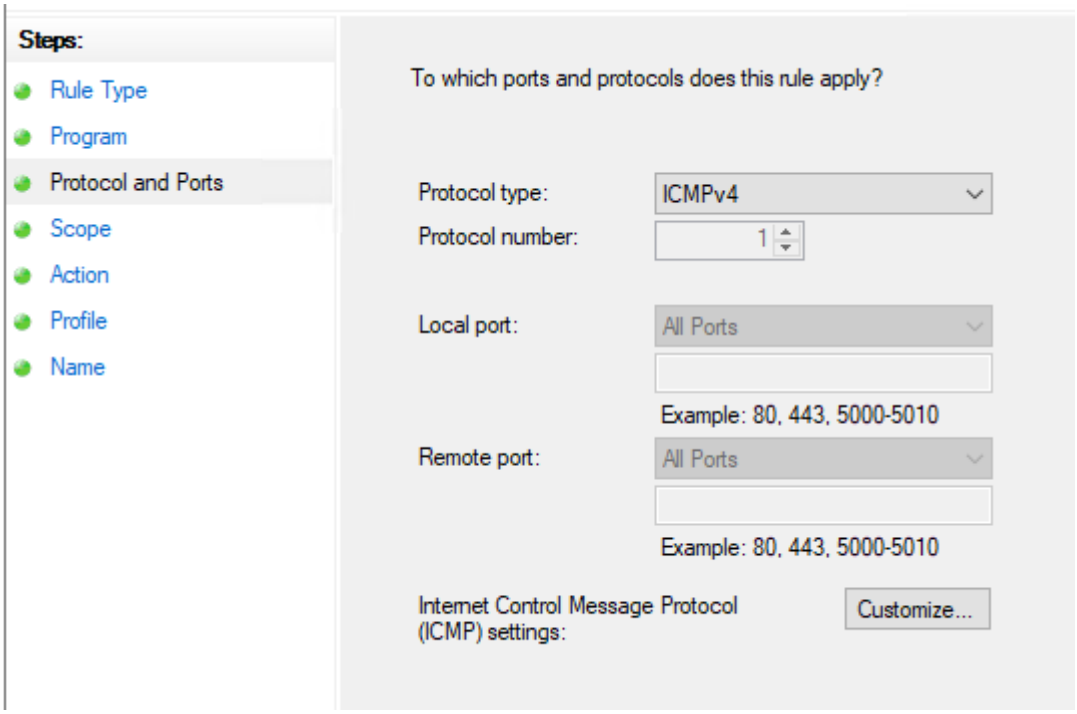
6. This is because the request is not being accepted by the VM. Now here the problem is, even though we have allowed that particular request in the network security group, remember that your machine as well could be having a firewall in place.
7. So, the first line of defense is the NSG. In this case, the NSG based on that allow rule is allowing the request. But your virtual machine, whether it be Windows or Linux, might have its own sort of rules, firewall rules at the OS level. You must understand that at the OS level also there could be rules that are not allowing the request to come in or even go out for that matter. So even at the OS level, you must be wary about these particular rules when it comes on to the common protocols like RDP port 3389 http traffic port 80. Normally these are the common ports that will be automatically allowed at the OS level.
8. But this kind of protocol of ICMP when it comes on to ping is not secure in nature.
9. Now in your virtual machine you have to open **windows defender firewall with advanced security.**
10. Here you need to go into the inbound rules and create a new rule.



11. Right click on inbound rules and then click on create new.
12. Then in the rule type choose custom.



13. Now in the protocols and ports choose ICMPv4. Then click on next to the Name section and give it a name then just click on save.



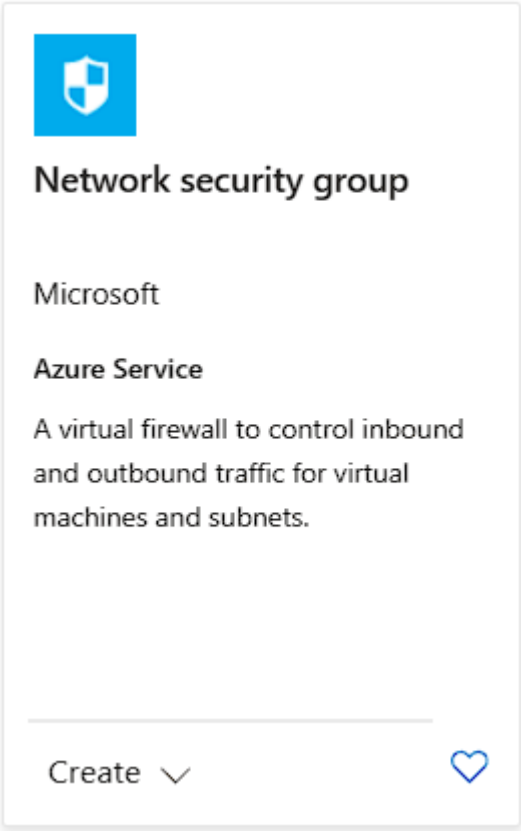
14. Once your rule is created then try to ping again you will see that it was successful.

```
C:\>ping 52.172.165.57

Pinging 52.172.165.57 with 32 bytes of data:
Reply from 52.172.165.57: bytes=32 time=28ms TTL=114
Reply from 52.172.165.57: bytes=32 time=27ms TTL=114
Reply from 52.172.165.57: bytes=32 time=27ms TTL=114
Reply from 52.172.165.57: bytes=32 time=28ms TTL=114

Ping statistics for 52.172.165.57:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 28ms, Average = 27ms
```

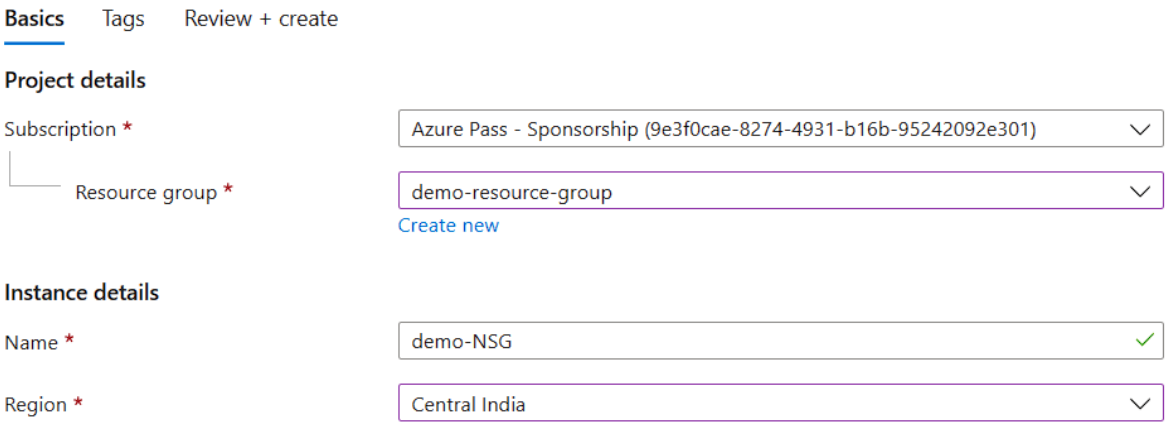
15. Once you are done kindly delete the ICMP rule from your VM.

😄 Step 5: Subnets

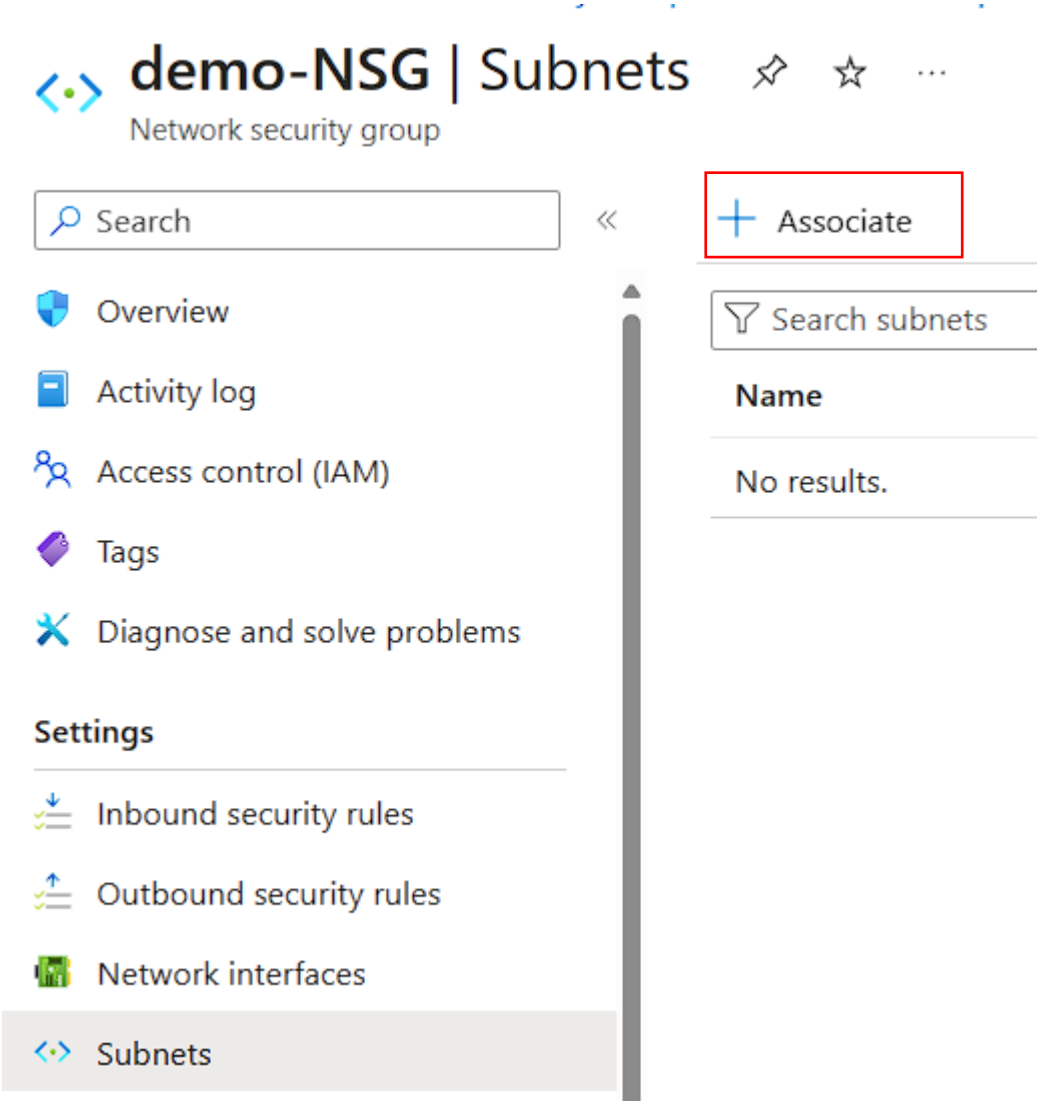
1. In this part we are going to create a network security group at subnet level.
2. For that go to create resources and search for network security groups. Choose the below service accordingly and click on create.



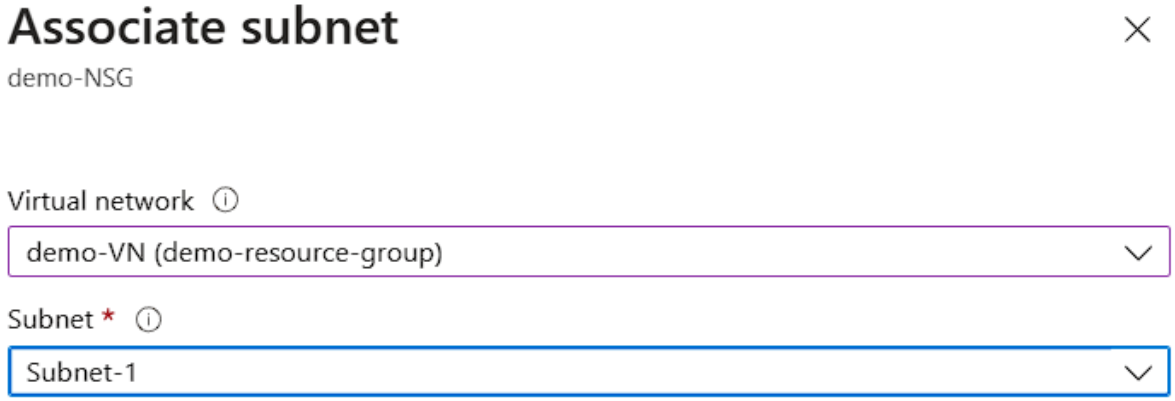
3. Here you just need to select your resource group and your region in which your other resources have been created. Then give it a name and go to review page and create your NSG.



4. Once it is created go to resources and then navigate to subnets from left pane.
5. Here you are going to associate subnets with your network security group.
6. For that click on associate.

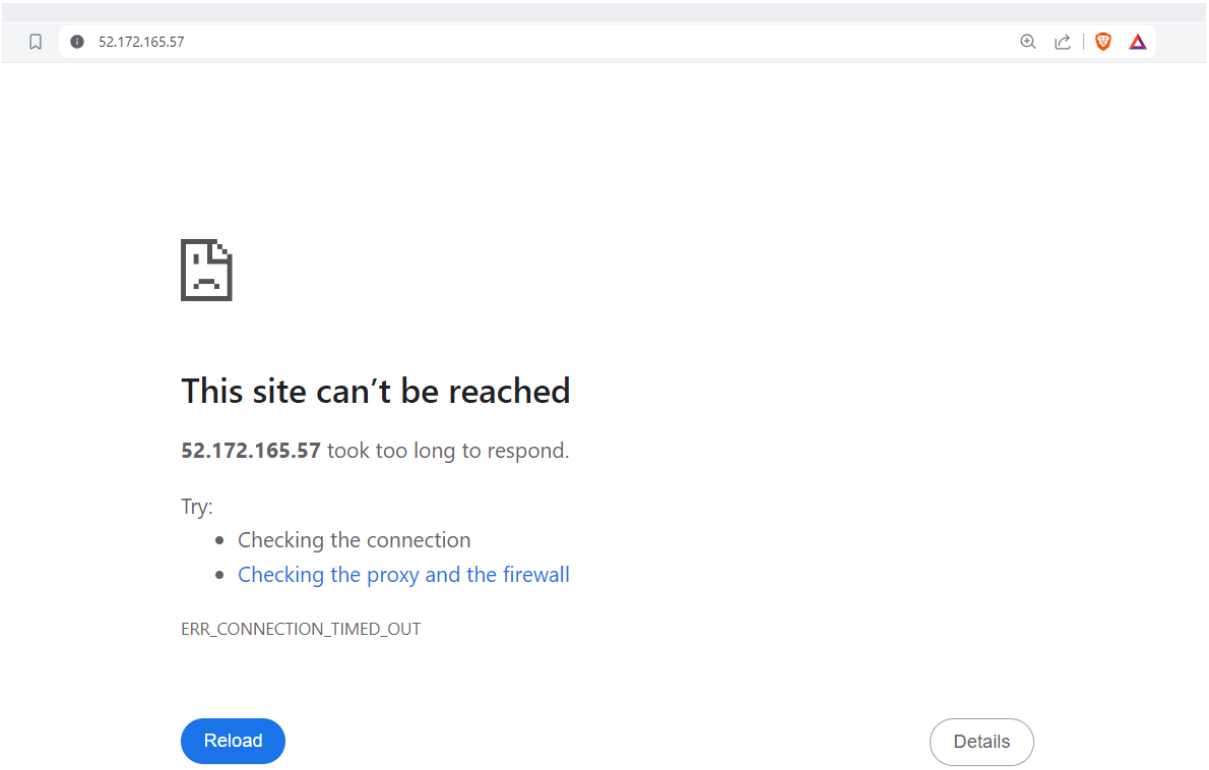


7. Now you have to select your virtual network and the subnet you want to associate.



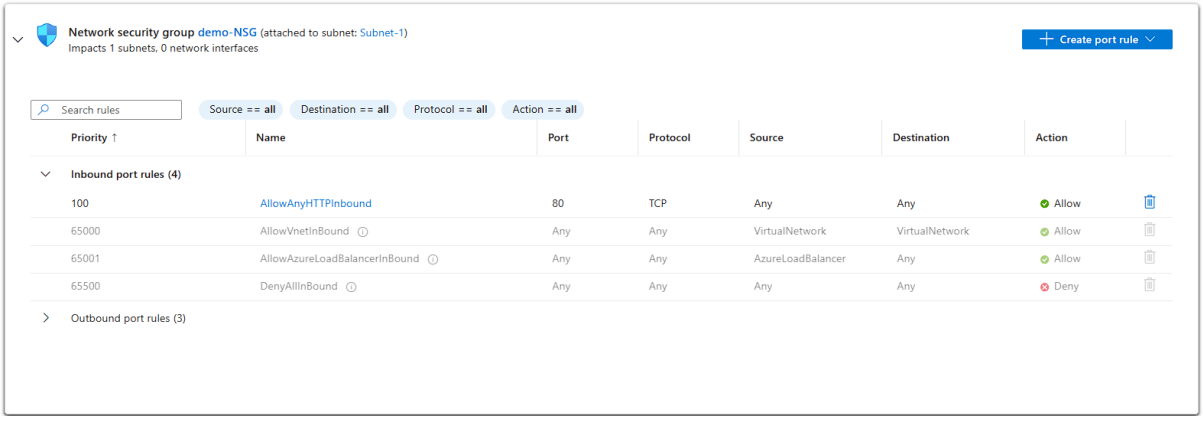
8. Below you can see your subnet attached.

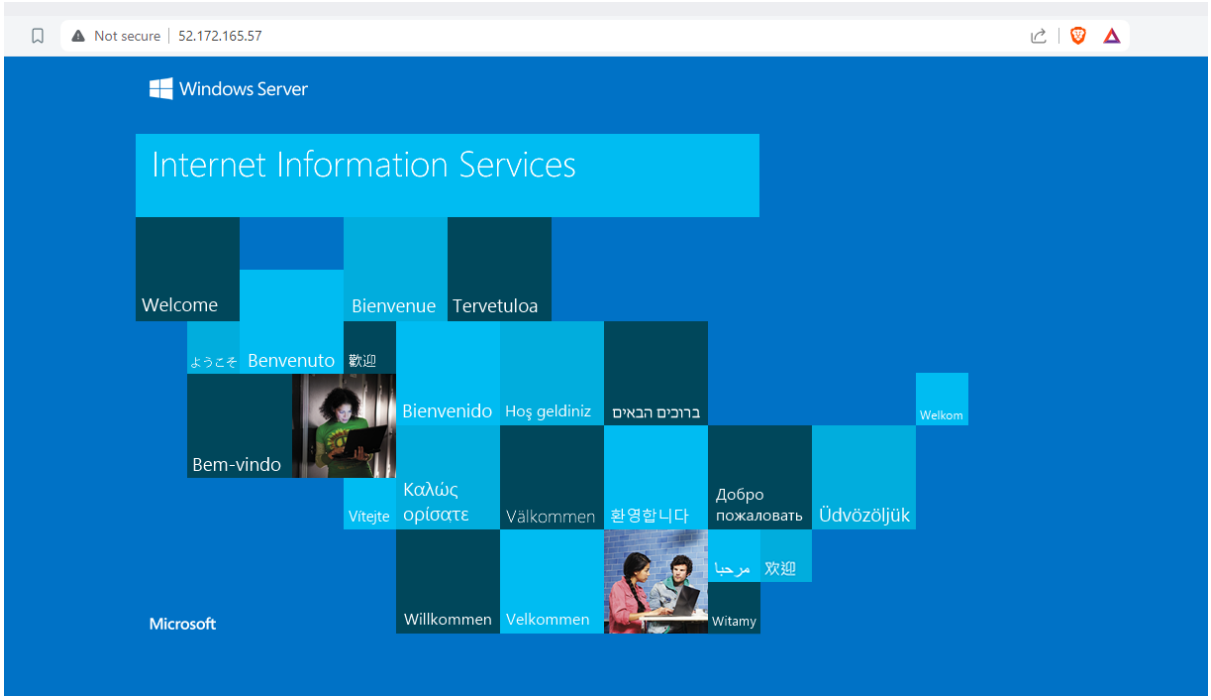
9. Now you are going to copy the public IP address of your VM and paste it in a new browser. There you will see that it cannot be reached.
10. Even though we have the rule for port 80 attached, still we are not able to reach it.



11. Now come back to the networking section of your VM.
12. There you will see that now you have two network security groups. One is directly attached to your VM.
13. Now if you look at the order of NSGs you will observe demo-NSG is coming in first which means that inbound port rules will prioritize it first.
14. That is why we were getting the error for us that the site is unreachable.

15. Now you need to allow port 80 from your new NSG and then go back to your web server. You will see that it is working now.





16. Once you are done just delete all of your resources.