

Introduction to Cloud Computing

LAB 06

Name: Muhammad Yahya

ID: 2280155

BS-SE 7B

Task 1: Create a virtual machine

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The current step is 'Review + create'. At the top, there's a green validation message: 'Validation passed'. Below it are three help links: 'Help me create a low cost VM', 'Help me create a VM optimized for high availability', and 'Help me choose the right VM size for my workload'. The navigation bar includes 'Basics', 'Disks', 'Networking', 'Management', 'Monitoring', 'Advanced', 'Tags', and 'Review + create'. The 'Review + create' tab is selected. Under 'Price', it shows '1 X Standard D2s v3 by Microsoft' at a cost of '0.1970 USD/hr'. There are links for 'Subscription credits apply', 'Terms of use', and 'Privacy policy'. Under 'Pricing for other VM sizes', there's a link to 'Pricing for other VM sizes'. The 'TERMS' section contains legal text about agreeing to terms and conditions. The 'Basics' section shows 'Subscription' as 'Azure for Students'. At the bottom, there are buttons for '< Previous', 'Next >', and 'Create', along with links for 'Download a template for automation' and 'Give feedback'.

- From the All services blade, search for and select Virtual machines, and then click + Add, + Create, + New Virtual Machine.

The screenshot shows the 'testVM' Overview page in Microsoft Azure. The left sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Windows Admin Center, Networking, and Settings. The main content area displays the 'Essentials' section with details like Resource group (move) : rg1, Status : Creating, Location : Central India, Subscription (move) : Azure for Students, Subscription ID : db878fcc-8781-42d0-a61d-55de3d976446, Operating system : Windows, Size : Standard D2s v3 (2 vcpus, 8 GiB memory), Primary NIC public IP : 74.225.153.68 (1 associated public IPs), Virtual network/subnet : snet-centralindia/snet-centralindia-1, DNS name : Not configured, Health state : -, and Time created : 11/4/2025, 5:13 PM UTC. Below this, there are sections for 'Properties' (Computer name: testVM, Operating system: Windows, VM generation: V2, VM architecture: x64) and 'Networking' (Public IP address: 74.225.153.68 (Network interface testvm556), Public IP address (IPv6): -, Private IP address: 172.16.0.4). A 'Tags (edit)' button is also present.

Task 2: Create a network security group

- From the All services blade, search for and select Network security groups and then click + Add, + Create, + New

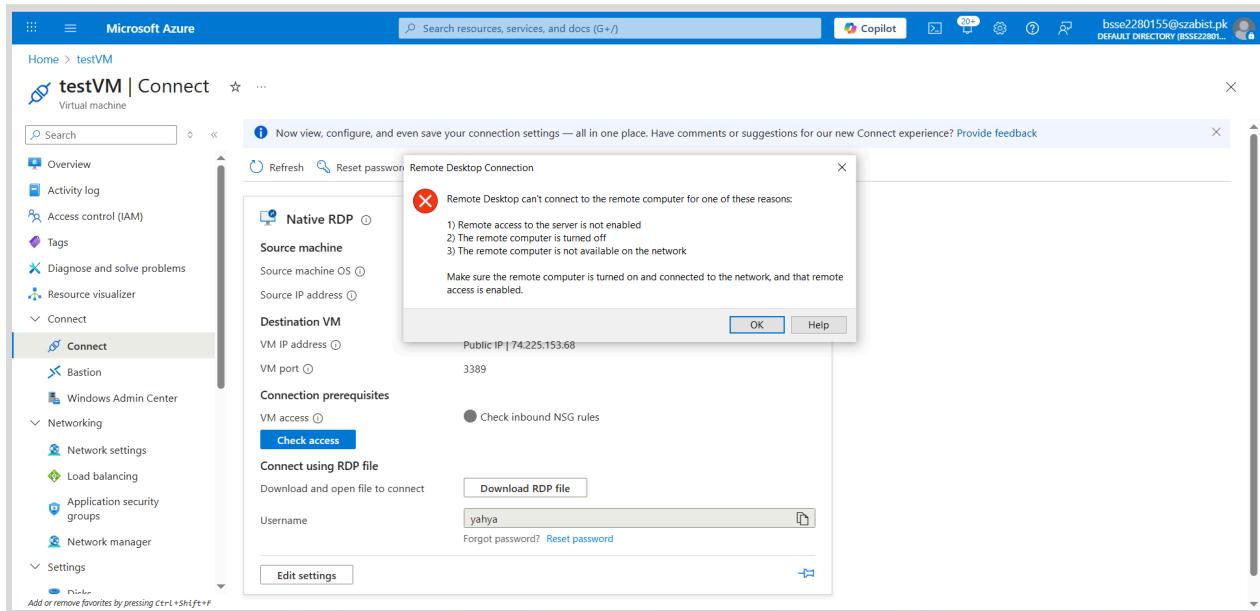
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. The main content area is titled "Network foundation | Network security groups". On the left, a sidebar lists several network-related services: Overview, Virtual network (selected), NAT gateways, Public IP addresses, Network interfaces, Network security groups (selected), Application security groups, Bastions, Route tables, Route servers, Private Link, DNS, and Monitoring and management. A message at the top states, "You are viewing a new version of Browse experience. Click here to access the old experience." Below the sidebar, there is a filter bar with dropdowns for Subscription equals all, Resource Group equals all, and Location equals all, along with an "Add filter" button. In the center, a large shield icon is displayed with the text "No network security groups to display". Below the icon, a descriptive message reads, "Create a network security group with rules to filter inbound traffic to, and outbound traffic from, virtual machines and subnets." A prominent blue "Create" button is located at the bottom of this section. At the very bottom of the page, there is a note about adding favorites and a "Give feedback" link.

- After the NSG is created, click Go to resource.
- Under Settings click Network interfaces and then Associate.
- Select the network interface you identified in the previous task (testvm556).

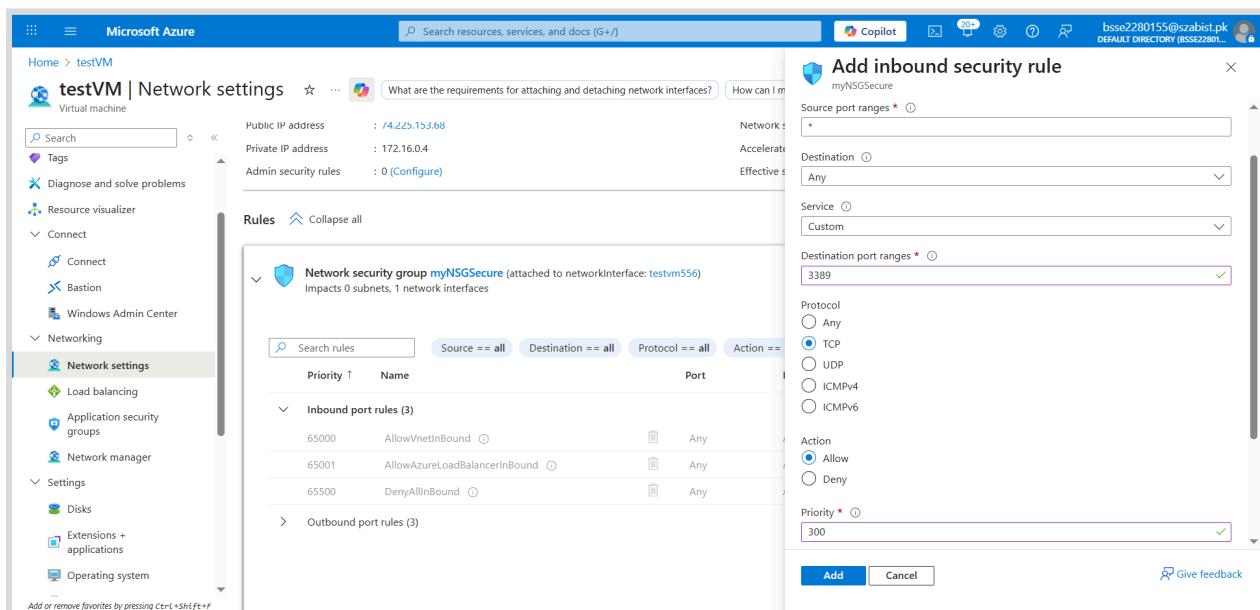
The screenshot shows the Microsoft Azure portal interface for a specific Network Security Group named "myNSGSecure". The top navigation bar includes the Microsoft Azure logo, a search bar, and various icons. The main content area is titled "myNSGSecure | Network interfaces". On the left, a sidebar lists several settings: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (selected), Inbound security rules, Outbound security rules, Network interfaces (selected), Subnets, Properties, Locks, Monitoring, Automation, and Help. A message at the top states, "All services > CreateNetworkSecurityGroupBladeV2-20251104221809 | Overview > myNSGSecure". Below the sidebar, there is a search bar labeled "Search network interfaces" and a table with four columns: Name, Public IP address, Private IP address, and Virtual machine. The table contains one row for "testvm556" with the corresponding values. At the bottom of the page, there is a note about adding favorites and a "Give feedback" link.

Task 3: Configure an inbound security port rule to allow RDP

- Attempt to connect to the virtual machine



- On the virtual machine blade, scroll down to the Settings section, click on Networking.
- On the Inbound port rules tab, click Add inbound port rule . Click Add when you are done.



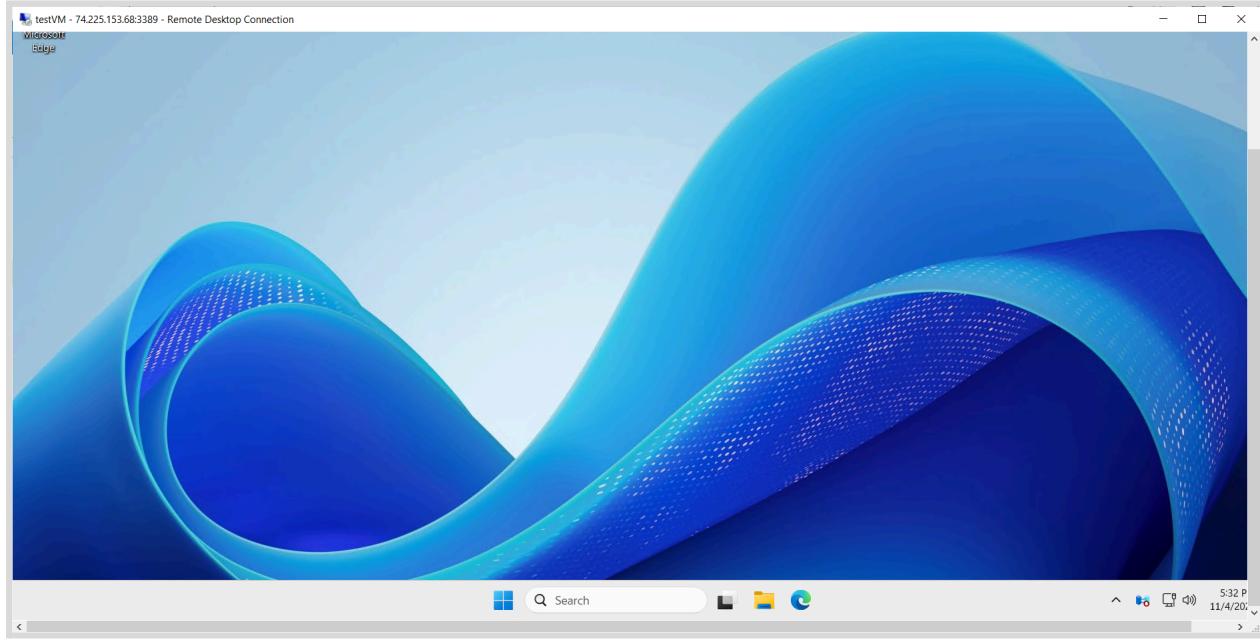
- Select Add and wait for the rule to be provisioned.

Network security group **myNSGSecure** (attached to networkInterface: **testvm556**)
 Impacts 0 subnets, 1 network interfaces

+ Create port rule ▾

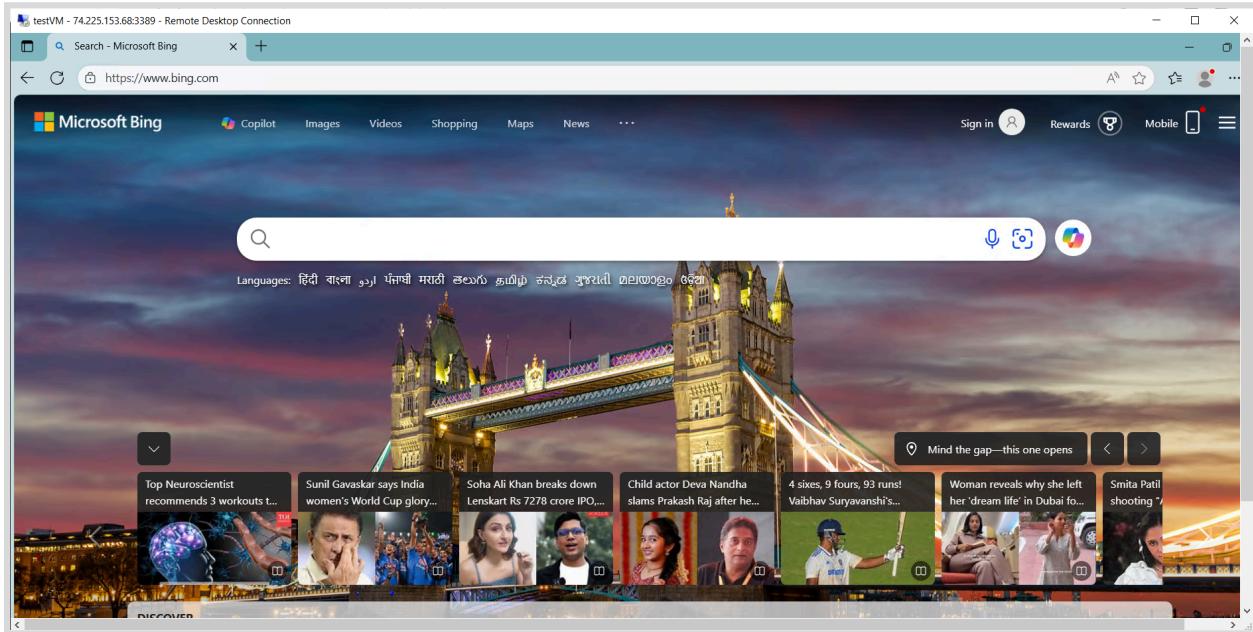
Priority ↑	Name	Port	Protocol	Source	Destination	Action
300	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound ⓘ	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound ⓘ	Any	Any	Any	Any	Deny
> Outbound port rules (3)						

- Then try again to RDP into the virtual machine by going back to Connect This time you should be successful.



Task 4: Configure an outbound security port rule to deny Internet access

- After the machine starts, open an Internet Explorer browser.
- Verify that you can access <https://www.bing.com>



- Back in the Azure portal, navigate back to the blade of the SimpleWinVM virtual machine.
- Under Settings, click **Networking**, and then Outbound port rules.
- Click **Add outbound port rule** and configure a new outbound security rule with a higher priority that will deny internet traffic. Click **Add** when you are finished.

A screenshot of the Microsoft Azure portal showing the network settings for a virtual machine named "testVM". The left sidebar shows various management options like Connect, Resource visualizer, and Network settings, which is currently selected. In the main pane, it displays basic network information such as Public IP address (4.225.153.68), Private IP address (172.16.0.4), and Admin security rules (0). It also shows a "Network security group" named "myNSGSecure" attached to the VM. The "Rules" section is expanded, showing an "Inbound port rules (4)" section and an "Outbound port rules (3)" section. The "Outbound port rules" table lists three rules:

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowNetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

- Return to the VM.
- Browse to <https://www.microsoft.com>. The page should not display.

