

NAME: Zohaib Hassan
ID: 2280168
Section – 7B
LAB:06

06 - Secure network traffic (10 min)

In this walk-through, we will configure a network security group.

Task 1: Create a virtual machine

In this task, we will create a Windows Server 2019 Datacenter virtual machine.

1. Sign in to the [Azure portal](#).
2. From the **All services** blade, search for and select **Virtual machines**, and then click **+ Add**, **+ Create**, **+ New Virtual Machine**.
3. On the **Basics** tab, fill in the following information (leave the defaults for everything else):

Settings	Values
Subscription	Use default provided
Resource group	Create new resource group
Virtual machine name	SimpleWinVM
Region	(US) East US
Image	Windows Server 2019 Datacenter Gen 2
Size	Standard D2s v3
Administrator account username	azureuser
Administrator account password	Pa\$\$w0rd1234
Inbound port rules	None

4. Switch to the **Networking** tab, and configure the following setting:

Settings	Values
NIC network security group	None

5. Switch to the **Management** tab, and in its **Monitoring** section, select the following setting:

Settings	Values
Boot diagnostics	Disable

6. Leave the remaining defaults and then click the **Review + create** button at the bottom of the page.
7. Once Validation is passed click the **Create** button. It can take about five minutes to deploy the virtual machine.
8. Monitor the deployment. It may take a few minutes for the resource group and virtual machine to be created.
9. From the deployment blade or from the Notification area, click **Go to resource**.

10. On the **SimpleWinVM** virtual machine blade, click **Networking**, review the **Inbound port rules** tab, and note that there is no network security group associated with the network interface of the virtual machine or the subnet to which the network interface is attached.

Note: Identify the name of the network interface. You will need it in the next task.

Task 2: Create a network security group

In this task, we will create a network security group and associate it with the network interface.

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

2. On the **Basics** tab of the **Create network security group** blade, specify the following settings.

Setting	Value
Subscription	Use default subscription
Resource group	Select default from drop down
Name	myNSGSecure
Region	(US) East US

3. Click **Review + create** and then after the validation click **Create**.
4. After the NSG is created, click **Go to resource**.
5. Under **Settings** click **Network interfaces** and then **Associate**.
6. Select the network interface you identified in the previous task.

7.

The screenshot shows the Microsoft Azure portal. The URL is [CreateNetworkSecurityGroupBladeV2-20251107061715 | Overview](#). The deployment name is "CreateNetworkSecurityGroupBladeV2-20251107061715". Deployment status: Your deployment is complete. Deployment details: Deployment name: CreateNetworkSecurityGroupBladeV2..., Start time: 11/7/2025, 5:17:58 AM, Subscription: Azure for Students, Correlation ID: fffffb988-4332-41ea-bfa3-22a7f6808da7, Resource group: CloudComputing. Next steps: Go to resource. The user is signed in as bsse2280168@szabist.pk.

8.

The screenshot shows the Microsoft Azure portal. The URL is [Home > CreateNetworkSecurityGroupBladeV2-20251107061715 | Overview > myNSGSecure](#). The network security group is "myNSGSecure". The user is performing an action to "Associate network interface". A modal dialog is open with the title "Associate network interface". It shows the network interface "simplewinvm765" selected under "Network interface associations". The status message says "Saving network interface 'simplewinvm765'". The user is signed in as bsse2280168@szabist.pk.

9.

10.

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

In this task, we will allow RDP traffic to the virtual machine by configuring an inbound security port rule.

1. In the Azure portal, navigate to the blade of the **SimpleWinVM** virtual machine.
2. On the **Overview** pane, click **Connect**.
3. Attempt to connect to the virtual machine by selecting RDP and downloading an running the RDP file. By default the network security group does not allow RDP. Close the error window.

4.

5. On the virtual machine blade, scroll down to the **Settings** section, click on **Networking**, and notice the inbound rules for the **myNSGSecure (attached to network interface: myVMNic)** network security group denies all inbound traffic except traffic within the virtual network and load balancer probes.
6. On the **Inbound port rules** tab, click **Add inbound port rule**. Click **Add** when you are done.

Setting	Value
Source	Any
Source port ranges	*
Destination	Any

Destination port ranges **3389**

Setting	Value
Protocol	TCP
Action	Allow
Priority	300
Name	AllowRDP

7. Select **Add** and wait for the rule to be provisioned and then try again to RDP into the virtual machine by going back to **Connect**. This time you should be successful. Remember the user is **azureuser** and the password is **Pa\$\$w0rd1234**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and a sign-in dropdown for 'bsse2280168@szabist.pk'. The main content area is titled 'SimpleWinVM | Network settings' under 'Virtual machine'. On the left, a sidebar lists options like 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Connect', 'Networking' (selected), 'Network settings' (selected), 'Load balancing', 'Application security groups', 'Network manager', 'Settings', and 'Availability + scale'. The right pane displays network interface details for 'simplewinvm765 (primary) / ipconfig1 (primary)'. Under 'Essentials', it shows the network interface, virtual network, public IP address (4.213.100.230), private IP address (172.16.0.4), and admin security rules (0). Under 'Rules', a new rule is listed: 'Network security group myNSGSecure (attached to networkInterface: simplewinvm765)'. The rule table shows the following data:

Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowRDP	3389	TCP	Any	Any	Allow

8.

The screenshot shows the Microsoft Azure portal interface, identical to the previous one but with the list of rules populated. The 'Rules' section now shows four entries: 'AllowRDP' (Priority 300, Port 3389, TCP, Any, Any, Allow), 'AllowVnetInBound' (Priority 65000, Port Any, TCP, Any, VirtualNetwork, VirtualNetwork, Allow), 'AllowAzureLoadBalancerInBo...' (Priority 65001, Port Any, TCP, Any, AzureLoadBalancer, Any, Allow), and 'DenyAllInBound' (Priority 65500, Port Any, TCP, Any, Any, Any, Deny). The table structure is the same as in the previous screenshot.

9.

Microsoft Azure Search resources, services, and docs (G+) Copilot

Home > SimpleWinVM

SimpleWinVM | Connect

Native RDP

Source machine

- Source machine OS: Windows
- Source IP address: Local IP | 110.38.230.242 Connecting over a VPN?

Destination VM

- VM IP address: Public IP | 4.213.100.230
- VM port: 3389

Connection prerequisites

- VM access: Port 3389 is accessible from source IP(s) [View applied NSG rules](#)
- Check access**

Connect using RDP file

- Download and open file to connect [Download RDP file](#)
- Username: azureuser
- Forgot password? [Reset password](#)

Add or remove favorites by pressing **Ctrl+Shift+F**

10.

https://www.bing.com

Microsoft Bing Copilot Images Videos Shopping Maps News ... Sign in Rewards Mobile

Languages: हिंदी चाला गुरा फैजाली मराठी तेलुगु தமிழ் கன்னட ஜாபானி மலயாளம் தெவா

The patience of a polar bear

If it wasn't for Sulakshana Pandit, Shabana Azmi woul... Zarine Khan Dies: Zayed Khan's Mother Passes Awa... Bihar Boy Asks Rahul Gandhi About His Marriage Plans;... Glenn Maxwell shakes in his boots': Former India captai... 'Nasty reporting only to blame India': Supreme Cou... Woman says she rejected Zohran Mamdani on Hinge... Please For Gujarat Dh

DISCOVER

11.

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

In this task, we will create a NSG outbound port rule that will deny Internet access and then test to ensure the rule is working.

1. Continue in your virtual machine RDP session.
2. After the machine starts, open an **Internet Explorer** browser.

3. Verify that you can access <https://www.bing.com> and then close Internet Explorer. You will need to work through the IE enhanced security pop-ups.

Note: We will now configure a rule to deny outbound internet access.

4. Back in the Azure portal, navigate back to the blade of the **SimpleWinVM** virtual machine.
 5. Under **Settings**, click **Networking**, and then **Outbound port rules**.
 6. Notice there is a rule, **AllowInternetOutbound**. This a default rule and cannot be removed.
 7. Click **Add outbound port rule** to the right of the **myNSGSecure (attached to network interface: myVMNic)** network security group and configure a new outbound security rule with a higher priority that will deny internet traffic. Click **Add** when you are finished.

Setting	Value
Source	Any
Source port ranges	*
Destination	Service Tag
Destination service tag	Internet
Destination port ranges	*
Protocol	TCP
Action	Deny
Priority	4000
Name	DenyInternet

8. Click **Add** Return to the VM you RDP's.
 9. Browse to <https://www.microsoft.com>. The page should not display. You may need to work through additional IE enhanced security pop-ups.

Note: To avoid additional costs, you can optionally remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named "SimpleWinVM". The left sidebar has a "Network settings" section selected. The main content area displays "Network settings" for "SimpleWinVM". At the top, there are search, Copilot, and notification icons. Below the title, there are two cards: "How can I make this VM secure?" and "What are the requirements for attaching and detaching network interfaces?". A "+1" button is also present.

Inbound port rules (4)

Prio...	Name	Port	Protocol	Source	Destination	Action
300	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound port rules (3)

Port	Protocol	Source	Destination	Action		
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

bsse2280168@szabist.pk DEFAULT DIRECTORY

Home > SimpleWinVM

SimpleWinVM | Network settings

Virtual machine

Created security rule
Successfully created security rule 'DenyInternet'.

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Network settings

Load balancing

Application security groups

Priority	Name	Port	Protocol	Source	Description	Action
300	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
4000	DenyInternet	8080	TCP	Any	Internet	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

