

Yumaan Mustafa

2280133

BSSE 7A

Lab 6

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.

The screenshot shows the Microsoft Azure portal homepage. At the top, there's a banner with the message "Hi Yumaan, see what more you can get from your Azure free account." Below the banner are four cards: "Take a free online course on Microsoft Learn", "Watch a demo and attend a live Q&A", "Start a project with Quickstart Center", and "Explore support resources". Below these cards is a section titled "Azure services" with icons for "Create a resource", "Storage accounts", "Virtual networks", "Virtual machines", "Quickstart Center", "Azure AI Foundry", "Kubernetes services", "App Services", "SQL databases", and "More services". At the bottom of the page, there's a "Resources" section with tabs for "Recent" and "Favorite".

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

The screenshot shows the "Create a new virtual machine" wizard. It has several sections: "Subscription" (selected), "Resource group" (selected), "Instance details", "Virtual machine name" (SimpleWinVM), "Region" ((Africa) South Africa North), and "Availability options" (No infrastructure redundancy required). The "Instance details" section also includes a "Deploy to an Azure Extended Zone" link.

3. On the Basics tab, fill in the following information (leave the defaults for everything else):
- | | |
|-----------------------|--|
| Subscription | SimpleWinVM (US) |
| Resource group | East US |
| Virtual machine name | Windows Server 2019 Datacenter Gen 2 |
| Image | Standard D2s v3 |
| Administrator account | username: azureuser, password: Pa\$\$w0rd1234 |
| password | Administrator account password: Pa\$\$w0rd1234 |
| Inbound port rules | None |

Administrator account

Username *	azureuser
Password *	*****
Confirm password *	*****

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

None
 Allow selected ports

Select inbound ports

Select one or more ports

ⓘ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

4. Switch to the Networking tab, and configure the following setting:
- | | | |
|--------|----------------------------|------|
| Values | NIC network security group | None |
|--------|----------------------------|------|

Networking

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) vnet-southafricanorth (Lab6)
[Edit virtual network](#)

Subnet * ⓘ

(New) snet-southafricanorth-1
[Edit subnet](#) 172.16.0.0 - 172.16.0.255 (256 addresses)

Public IP ⓘ

[Create new](#)

NIC network security group ⓘ

None
 Basic
 Advanced

5. Switch to the Management tab, and in its Monitoring section, select the following setting:
- | | | |
|--------|------------------|---------|
| Values | Boot diagnostics | Disable |
|--------|------------------|---------|

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

Configure monitoring options for your VM.

Alerts

Enable recommended alert rules

Diagnostics

Boot diagnostics Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics

Health

Enable application health monitoring

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.

 Deployment succeeded 

Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-202-20251106181812' to resource group 'Lab6' was successful.

[Go to resource](#)

[!\[\]\(2bae76de5ebbd5c4d7d47162f1673734_img.jpg\) Pin to dashboard](#)

a few seconds ago

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.

Network interface / IP configuration
simplewinvm838 (primary) / ipconfig1 (primary)

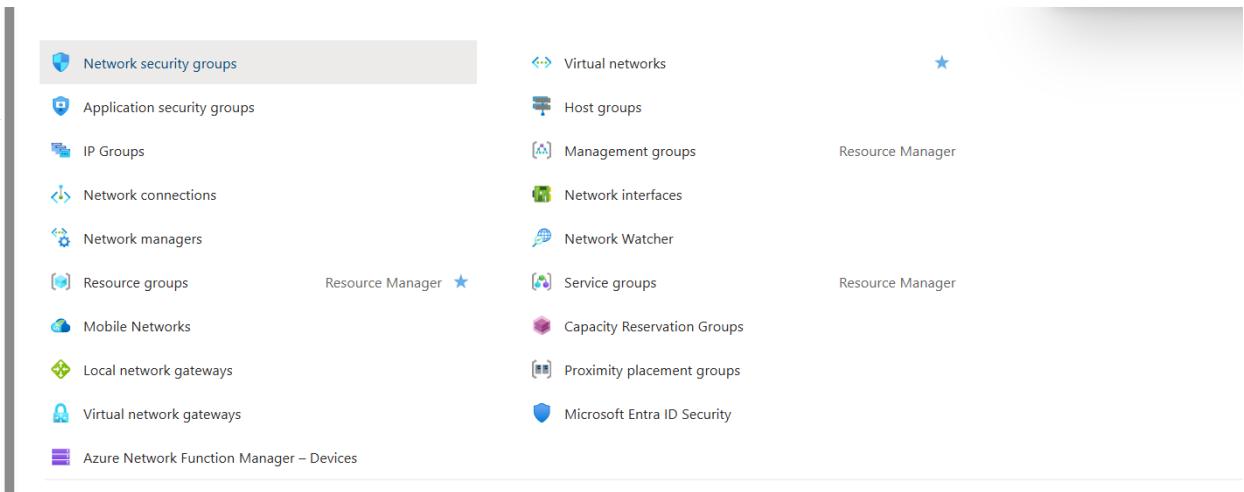
Essentials

Setting	Value	Actions
Network interface	: simplewinvm838	Edit
Virtual network / subnet	: vnet-southafricanorth / snet-southafricanorth-1	
Public IP address	: 4.221.56.26	
Private IP address	: 172.16.0.4	
Admin security rules	: 0 (Configure)	
Load balancers	: 0 (Configure)	
Application security gro...	: 0 (Configure)	
Network security group	: -	
Accelerated networking	: Enabled	
Effective security rules	: 0	

Task 2: Create a network security group

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

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

All services > Network security group >
Create network security group ...

Basics Tags Review + create

Project details

Subscription * Azure subscription 1
Resource group * NetworkWatcherRG
Create new

Instance details

Name * myNSGSecure
Region * South Africa North

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.

All services > CreateNetworkSecurityGroupBladeV2-20251106183141 | Overview > myNSGSecure

myNSGSecure | Network interfaces ⚡ ...

Network security group

Search Associate Refresh Dissociate

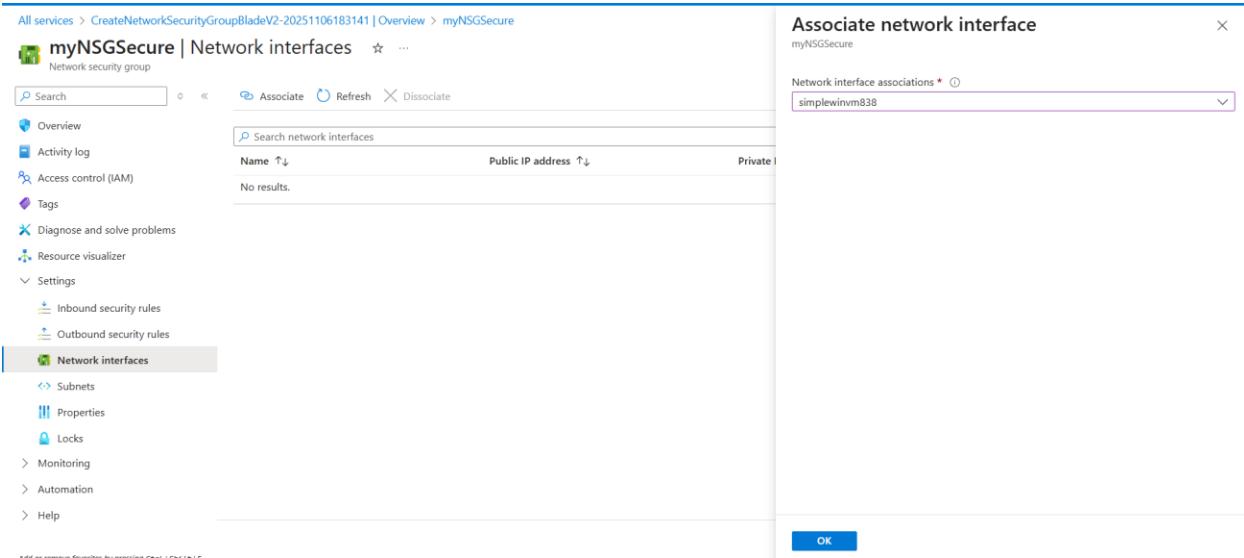
Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings Inbound security rules Outbound security rules Network interfaces Subnets Properties Locks Monitoring Automation Help

Associate network interface

myNSGSecure

Network interface associations * simplewinvm838

OK



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.

The screenshot shows the 'Native RDP' blade in the Azure portal. On the left, a sidebar lists various connectivity options like Tags, Diagnose and solve problems, Resource visualizer, Connect, and Connect (which is currently selected). The main area displays connection details: Source machine (Windows, Local IP | 182.190.128.160), Destination VM (Public IP | 4.221.56.26, VM port 3389), Connection prerequisites (VM access stopped), and a 'Validate' button. It also includes a 'Connect using RDP file' section with a 'Download RDP file' button and a 'Username' field set to 'azureuser'. A note at the bottom says 'Forgot password? Reset password'.

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.

The screenshot shows a 'Remote Desktop Connection' error dialog box. It displays a red 'X' icon and the message: 'Remote Desktop can't connect to the remote computer for one of these reasons: 1) Remote access to the server is not enabled 2) The remote computer is turned off 3) The remote computer is not available on the network'. Below the message, it says 'Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.' At the bottom, there is a 'See details' link, a '3389' port number, and an 'OK' button.

4. 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.
5. On the Inbound port rules tab, click Add inbound port rule . Click Add when you are done. Setting Source Source port ranges Destination Value Any * Any Destination port ranges 3389 Setting Protocol Action Priority Name Value TCP Allow 300 AllowRDP

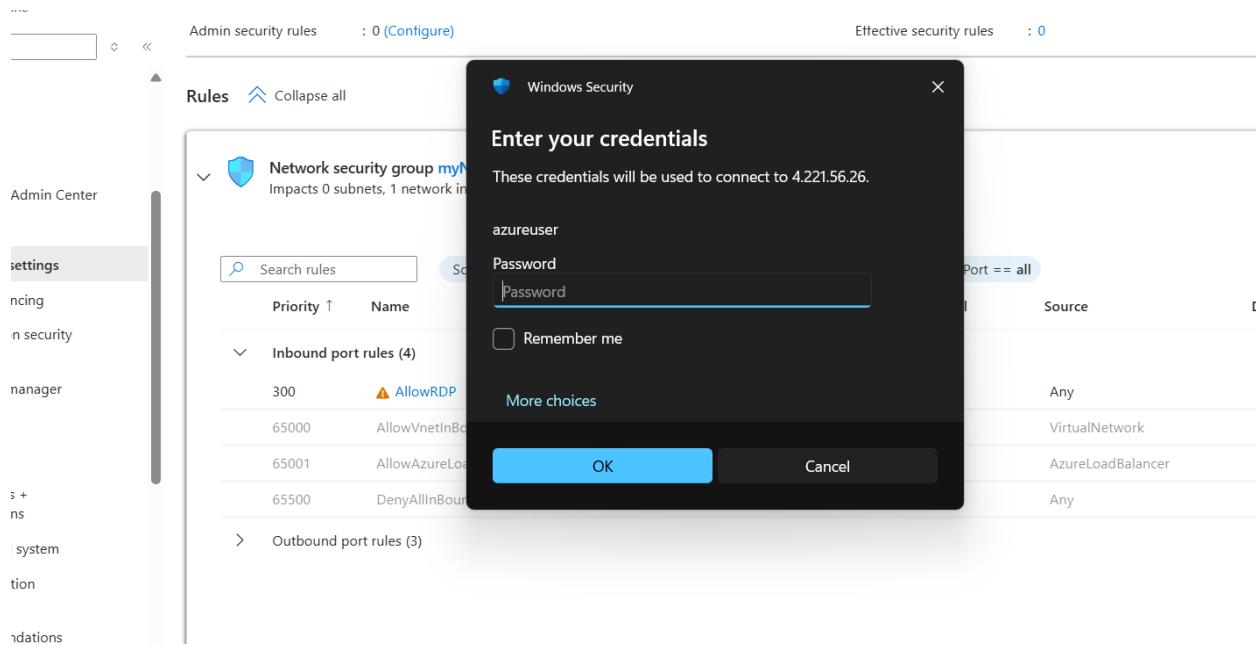
The screenshot shows the Azure portal interface for a virtual machine named 'SimpleWinVM'. The left sidebar is open to 'Network settings'. In the main pane, under 'Rules', a new security rule is being created. The rule is named 'AllowRDP' and is associated with the network security group 'myNSGSecure'. The configuration includes:

- Protocol:** TCP
- Port:** 3389
- Action:** Allow
- Priority:** 300
- Name:** AllowRDP

The screenshot shows the Azure portal interface for the same virtual machine 'SimpleWinVM'. The left sidebar is open to 'Network settings'. In the main pane, under 'Rules', the list of security rules is displayed. The newly created rule 'AllowRDP' is now listed along with others:

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

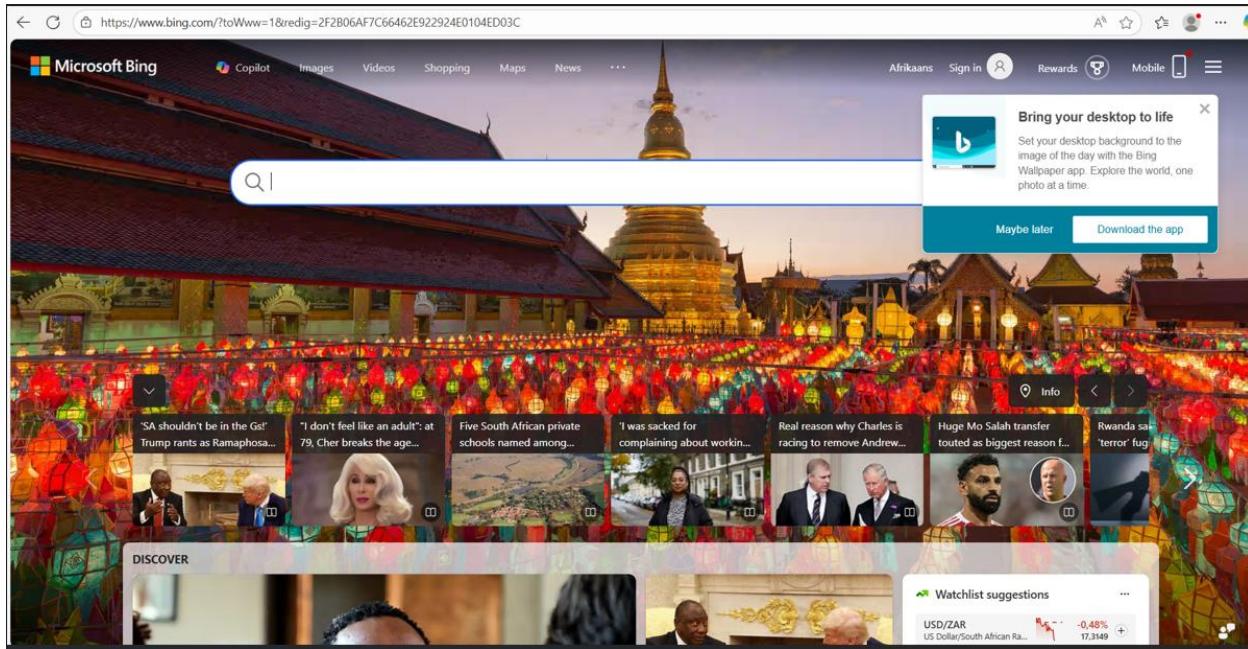
6. Select Add and wait for the rule to be provisioned and then try again to RDP into the virtual machine by going back to Connect This time you should be successful. Remember the user is azureuser and the password is Pa\$\$w0rd1234.



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

The screenshot shows two main windows from the Azure portal:

- SimpleWinVM | Network settings**: This window displays the network interface for the VM, showing Public IP address (4.221.56.26), Private IP address (172.16.0.4), and Admin security rules (0). It also lists the NSG attached to the interface.
- Add outbound security rule**: A modal dialog for creating a new NSG rule. It shows the NSG name (myNSGSecure), destination port range (0), protocol (Any), and action (Deny). The priority is set to 4000, and the name is "DenyInternet".
- myNSGSecure**: The overview of the NSG, showing its resource group (NetworkWatcherRG), location (South Africa North), and inbound/outbound rules.

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.

