

Yumaan Mustafa

2280133

BSSE 7A

Lab 6

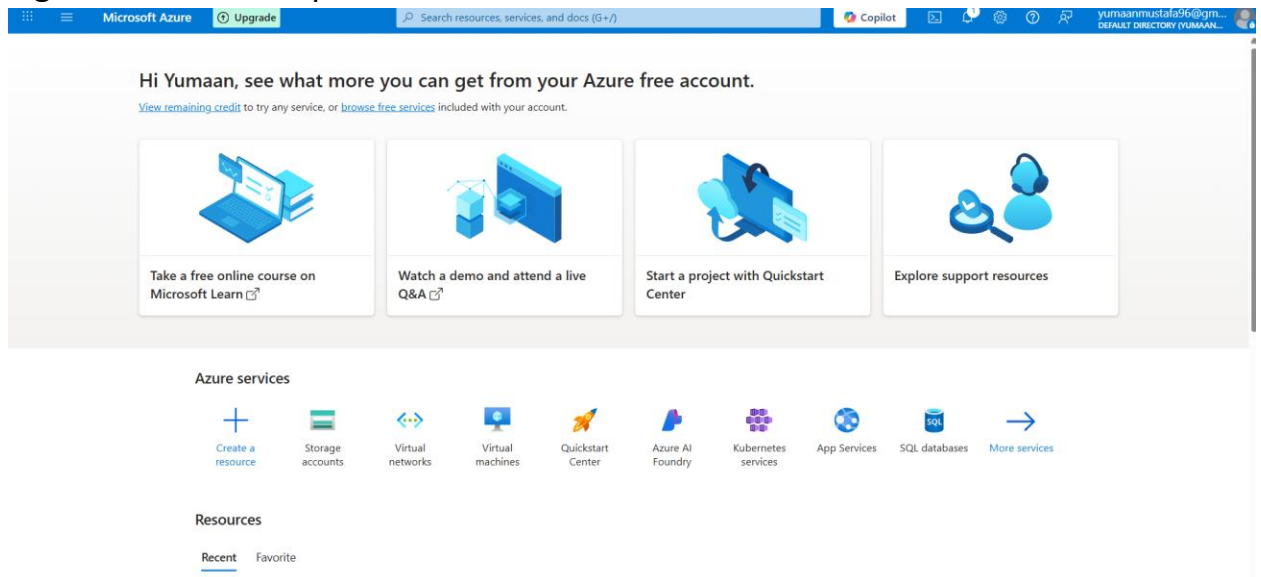
06 - Secure network traffic (10 min)

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.



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

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ (New) Lab6
[Create new](#)

Instance details

Virtual machine name * ⓘ SimpleWinVM ✓

Region * ⓘ (Africa) South Africa North
[Deploy to an Azure Extended Zone](#)

Availability options ⓘ No infrastructure redundancy required ✓

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

Administrator account

Username * ⓘ ✓

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 ▼

i 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: Settings Values NIC network security group None

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 ⓘ ▼ [Edit virtual network](#)

Subnet * ⓘ ▼ [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: Settings 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](#) [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) ▼

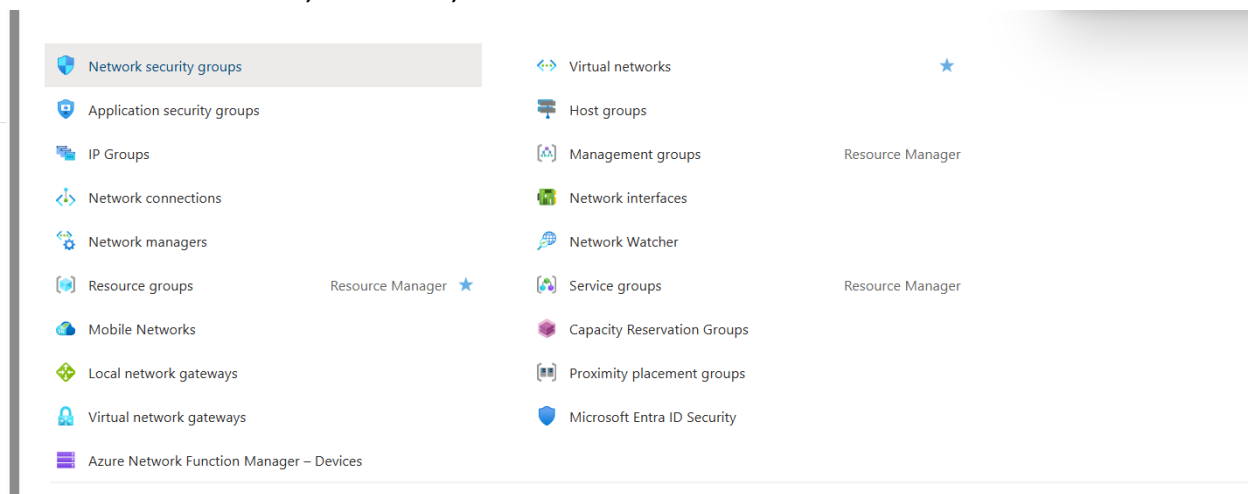
^ Essentials

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

Resource group *
[Create new](#)

Instance details

Name * ✓

Region *

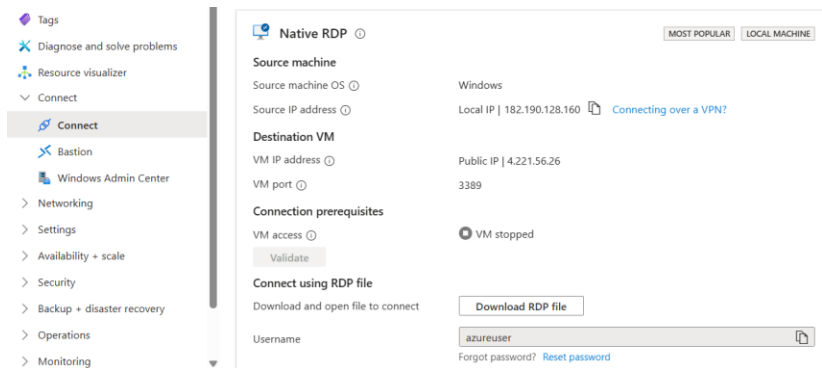
3. Click Review + create and then after the validation click Create.
4. After the NSG is created, click Go to resource.
5. Under Settings click Network interfaces and then ** Associate**.
6. Select the network interface you identified in the previous task.

The screenshot shows the Azure portal interface. On the left, the navigation pane is open, showing the 'Settings' section with 'Network interfaces' selected. The main area displays the 'myNSGSecure' Network security group page. The 'Network interfaces' tab is active, showing a table with columns 'Name', 'Public IP address', and 'Private IP address'. The table is empty, displaying 'No results.' Below the table, there are buttons for 'Associate', 'Refresh', and 'Dissociate'. On the right, a modal dialog titled 'Associate network interface' is open. It shows a dropdown menu for 'Network interface associations' with the value 'simplewinvm838' selected. At the bottom of the dialog is an 'OK' button.

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

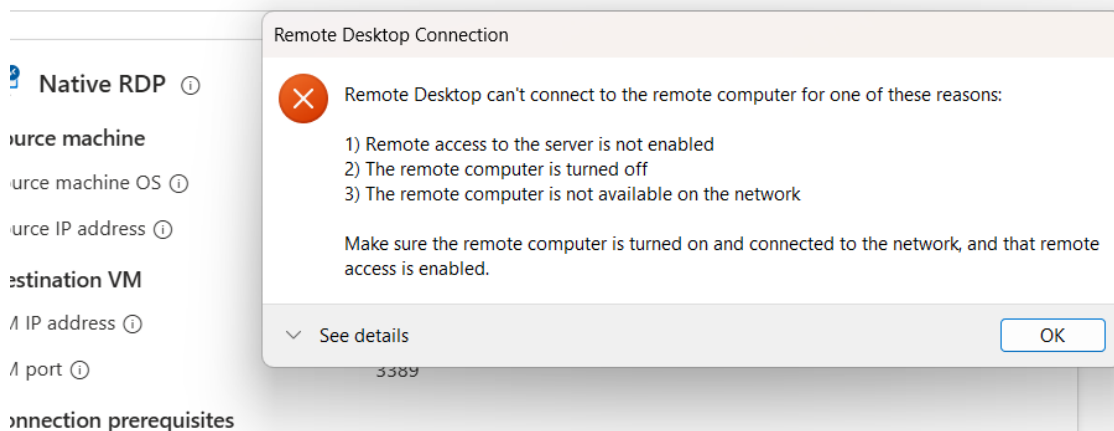
In this task, we will allow RDP traffic to the virtual machine by configuring an inbound security port rule.

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.

Refresh Reset password or keys Manage JIT Troubleshoot Feedback



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

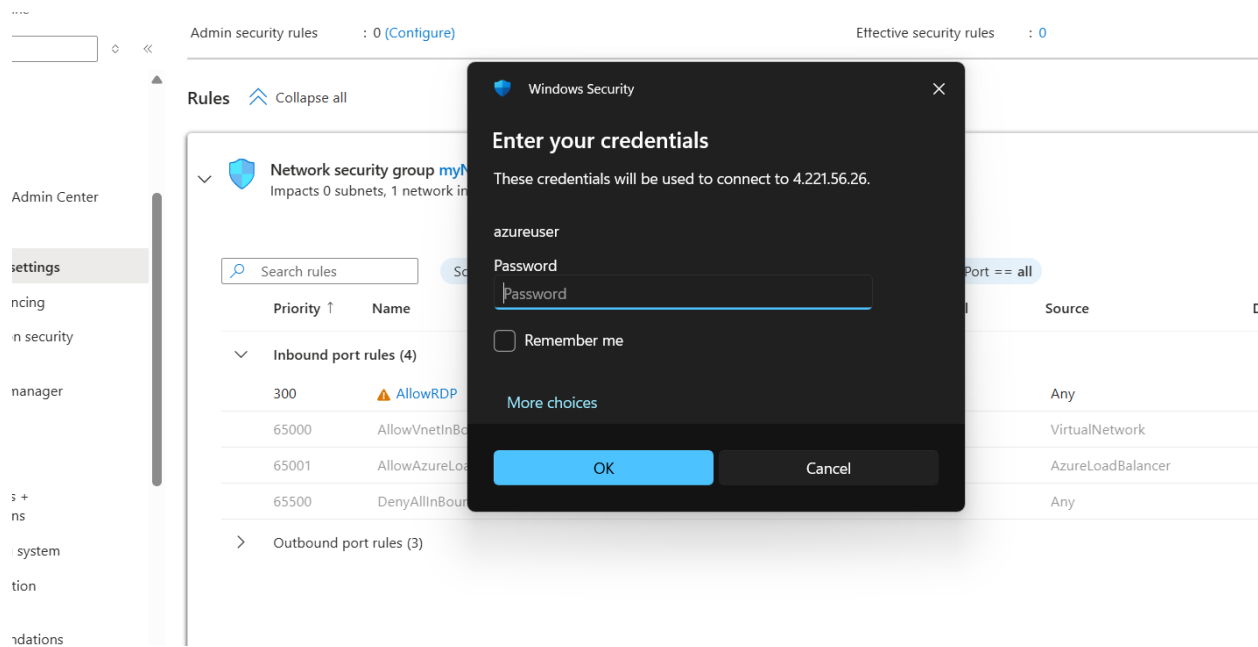
The top screenshot shows the 'SimpleWinVM | Network settings' page. The 'Rules' section for the network security group 'myNSGSecure' is expanded, showing 'Inbound port rules (3)'. A dialog box titled 'Creating security rule' is open, showing the configuration for a new rule named 'AllowRDP'. The rule is configured with the following settings:

- Protocol: TCP
- Action: Allow
- Priority: 300
- Name: AllowRDP
- Description: (empty)

The bottom screenshot shows the same 'SimpleWinVM | Network settings' page, but the 'Rules' section now shows 'Inbound port rules (4)'. The 'AllowRDP' rule has been added to the list of inbound port rules. The table of rules is as follows:

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

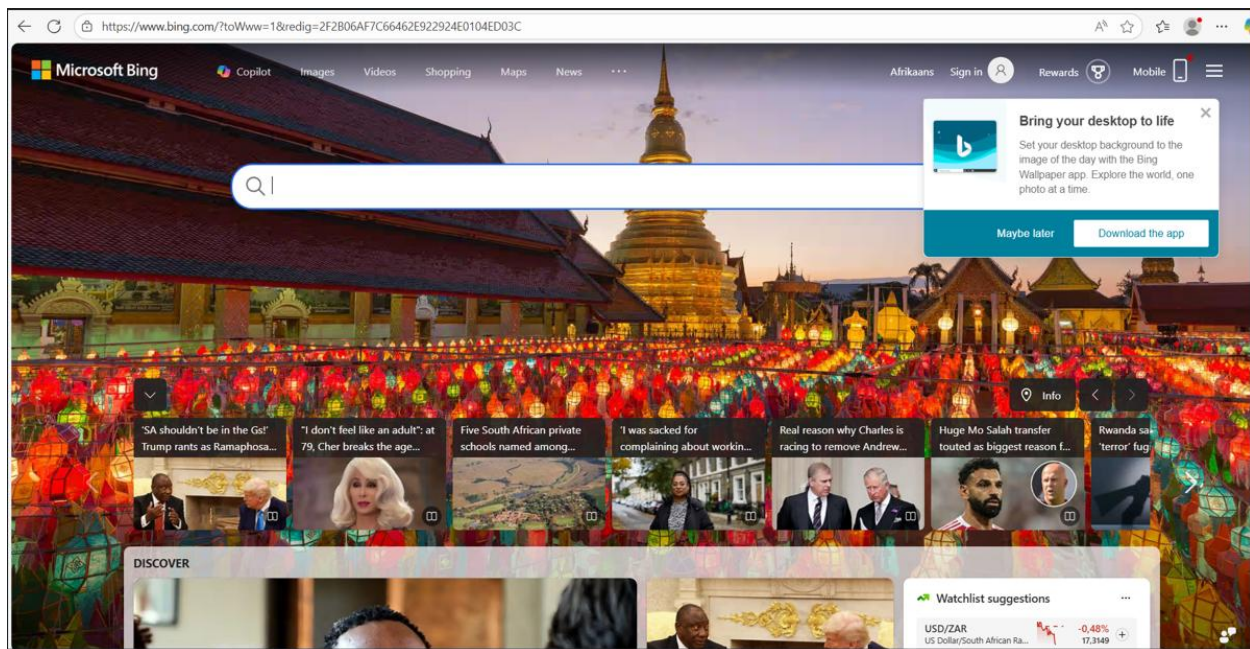
6. Select Add and wait for the rule to be provisioned and then try again to RDP into the virtual machine by going back to Connect This time you should be successful. Remember the user is azureuser and the password is Pa\$\$w0rd1234.



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 is 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

Home > SimpleWinVM

SimpleWinVM | Network settings

Virtual machine

Public IP address : 4.221.56.26
Private IP address : 172.16.0.4
Admin security rules : 0 (Configure)

Rules Collapse all

Network security group **myNSGSecure** (attached to networkInterface: simplewinvm838)
Impacts 0 subnets, 1 network interfaces

Search rules Source == all Destination == all Protocol == all Action ==

Priority	Name	Port
Inbound port rules (4)		
300	AllowRDP	3389
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBalancerInBound	Any
65500	DenyAllInBound	Any

Add outbound security rule

myNSGSecure

Service: Custom

Destination port ranges: *

Protocol: ☒ Any ☐ TCP ☐ UDP ☐ ICMPv4 ☐ ICMPv6

Action: ☐ Allow ☒ Deny

Priority: 4000

Name: DenyInternet

Description:

myNSGSecure

Network security group

Diagnose connectivity issues related to this security group Retrieve detailed information for troubleshooting security rules How do I create an alert to track firewall metric failures

Move Delete Refresh Give feedback

Resource group (move): NetworkWatcherRG
Location: South Africa North
Subscription (move): Azure subscription 1
Subscription ID: a3e17407-645b-4443-990f-e8d6df69025c
Tags (edit): Add tags

Custom security rules: 1 inbound, 1 outbound
Associated with: 0 subnets, 1 network interfaces

Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
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 Security Rules						
4000	DenyInternet	Any	Any	Any	Internet	Deny

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.

