Shaheed Zulfikar Ali Bhutto Institute of Science and Technology

Department of Software Engineering

Bisma Saeed – 2280108

BSSE – 7A

Lab: 06

Task 1: Create a 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.

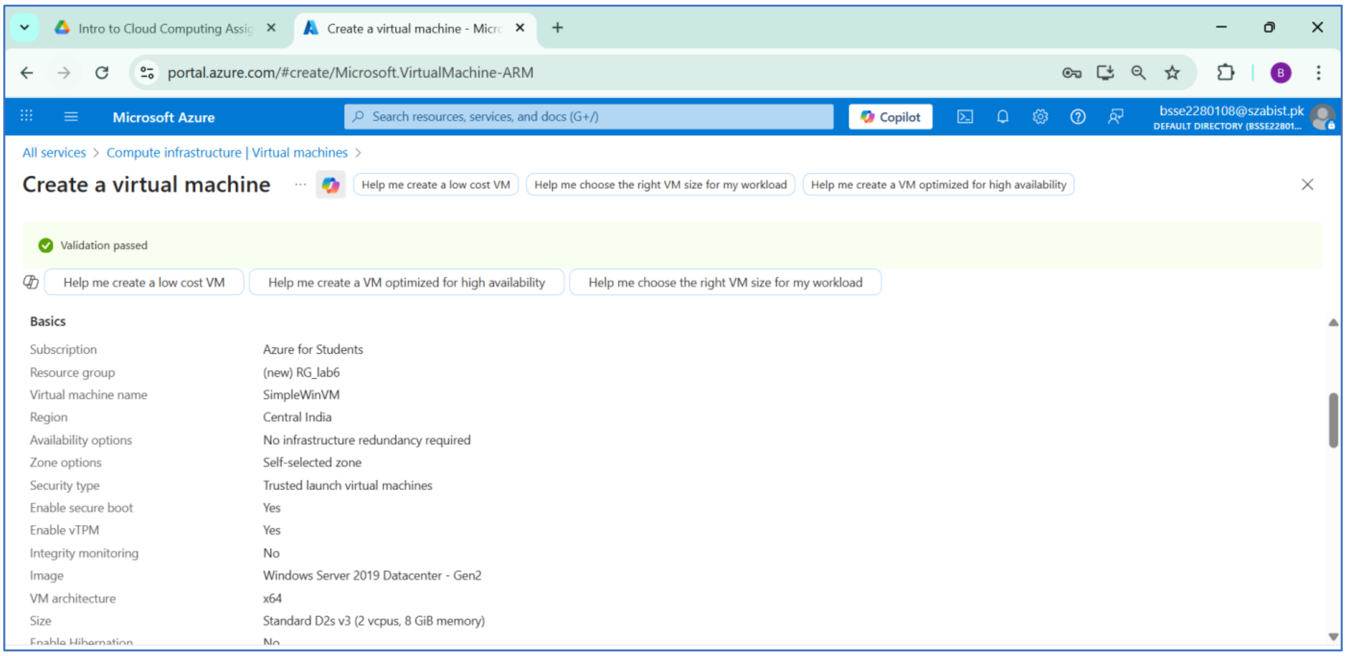
3. On the Basics tab, fill in the following information (leave the defaults for everything else):

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

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

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.



Intro to Cloud Computing Assig
Create a virtual machine - Micr
portal.azure.com/#create/Microsoft.VirtualMachine-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
bsse2280108@szabist.pk
DEFAULT DIRECTORY (BSSE22801...
All services > Compute infrastructure | Virtual machines >
Help me create a low cost VM
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability

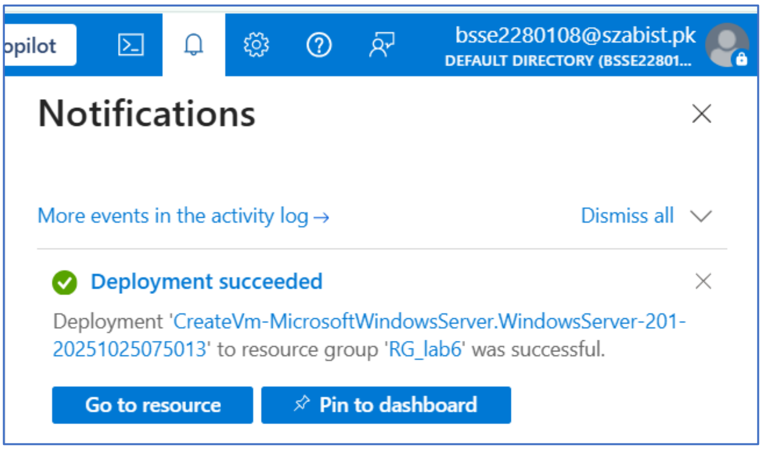
Create a virtual machine

Validation passed

Basics

Subscription	Azure for Students
Resource group	(new) RG_lab6
Virtual machine name	SimpleWinVM
Region	Central India
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No

8. Monitor the deployment. It may take a few minutes for the resource group and virtual machine to be created.



Notifications

More events in the activity log →

Dismiss all

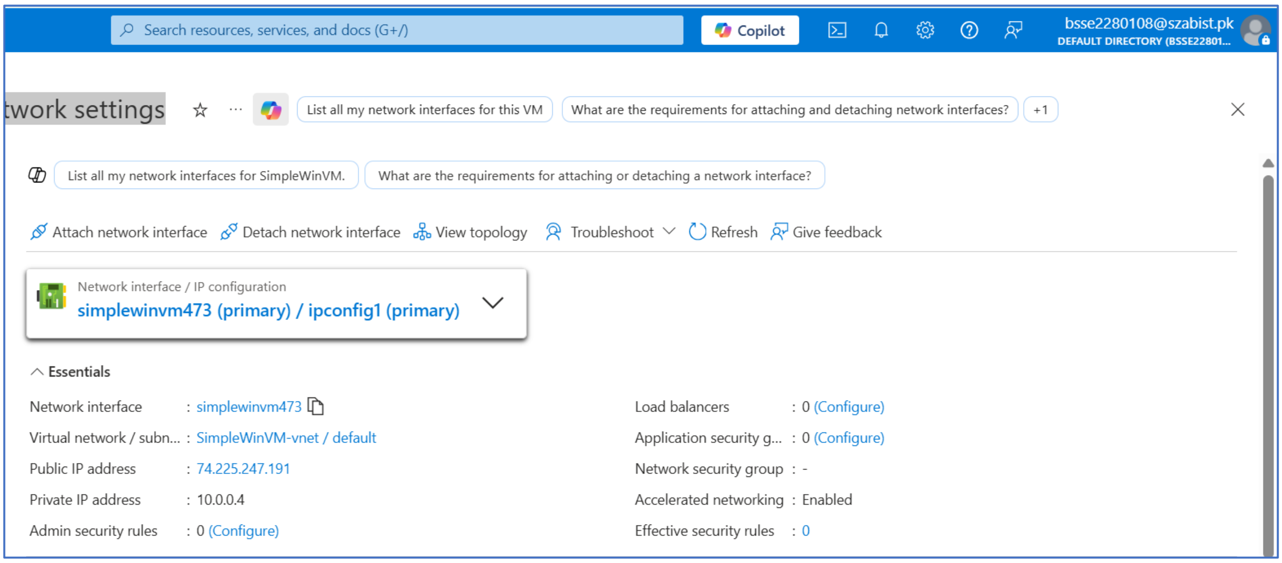
Deployment succeeded

Deployment 'CreateVm-MicrosoftWindowsServer.WindowsServer-201-20251025075013' to resource group 'RG_lab6' was successful.

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.



Search resources, services, and docs (G+/)
Copilot
bsse2280108@szabist.pk
DEFAULT DIRECTORY (BSSE22801...
twork settings
List all my network interfaces for this VM
What are the requirements for attaching and detaching network interfaces?
+1
List all my network interfaces for SimpleWinVM.
What are the requirements for attaching or detaching a network interface?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback

Network interface / IP configuration

simplewinvm473 (primary) / ipconfig1 (primary)

Essentials

Network interface	: simplewinvm473	Load balancers	: 0 (Configure)
Virtual network / subn...	: SimpleWinVM-vnet / default	Application security g...	: 0 (Configure)
Public IP address	: 74.225.247.191	Network security group	: -
Private IP address	: 10.0.0.4	Accelerated networking	: Enabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

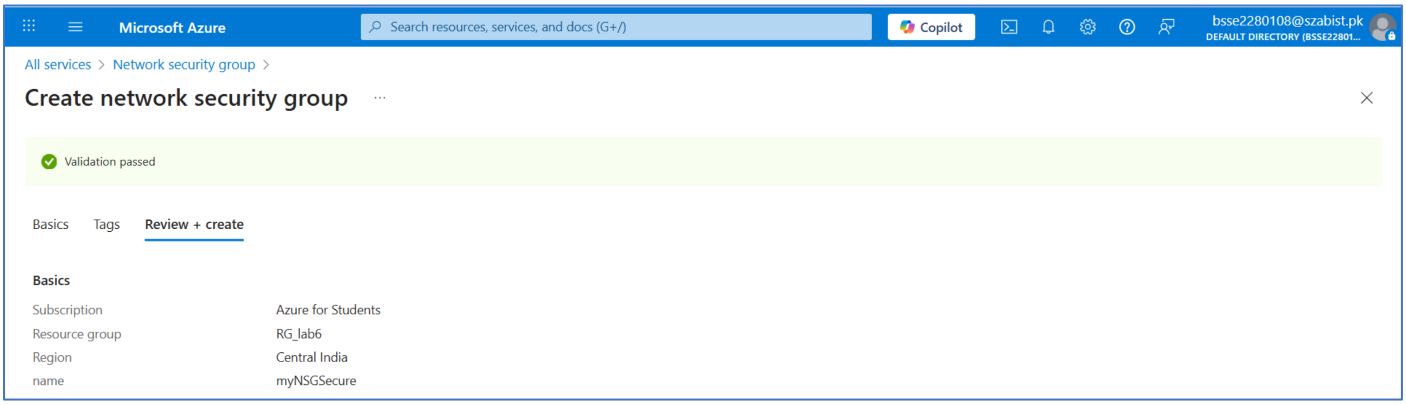
Task 2: Create a network security group

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.

3. Click Review + create and then after the validation click Create.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
bsse2280108@szabist.pk
DEFAULT DIRECTORY (BSSE22801...
All services > Network security group >

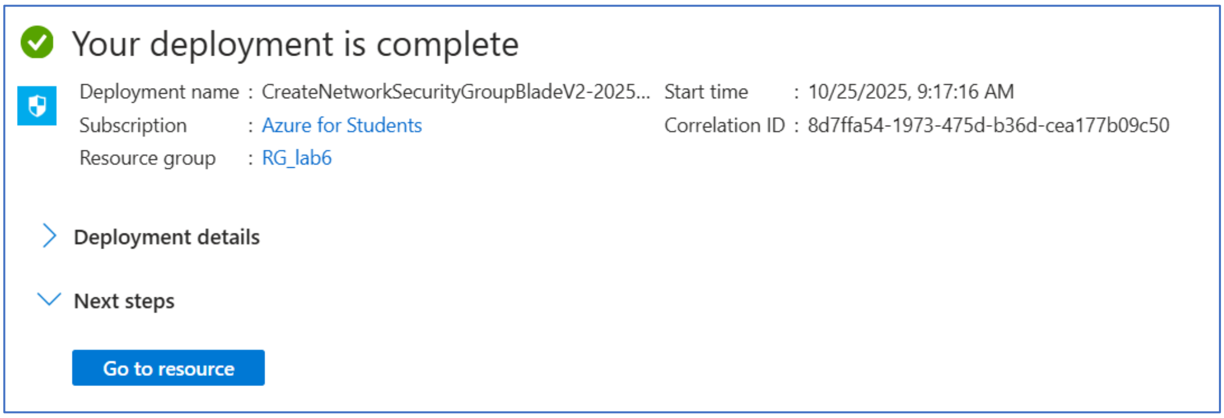
Create network security group

Validation passed

Basics
Tags
Review + create

Basics

Subscription	Azure for Students
Resource group	RG_lab6
Region	Central India
name	myNSGSecure



Your deployment is complete

Deployment name : CreateNetworkSecurityGroupBladeV2-2025...

Start time : 10/25/2025, 9:17:16 AM

Subscription : Azure for Students

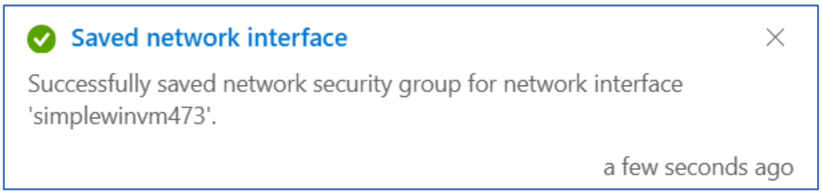
Correlation ID : 8d7ffa54-1973-475d-b36d-cea177b09c50

Resource group : RG_lab6

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.



Saved network interface

Successfully saved network security group for network interface 'simplewinvm473'.

a few seconds ago

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.

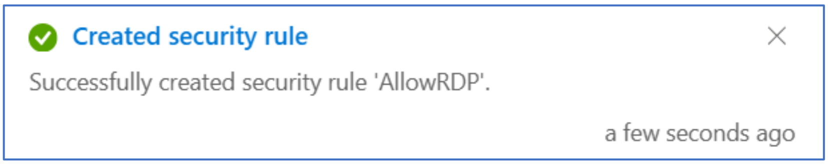
2. On the Overview pane, click Connect.

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. 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.

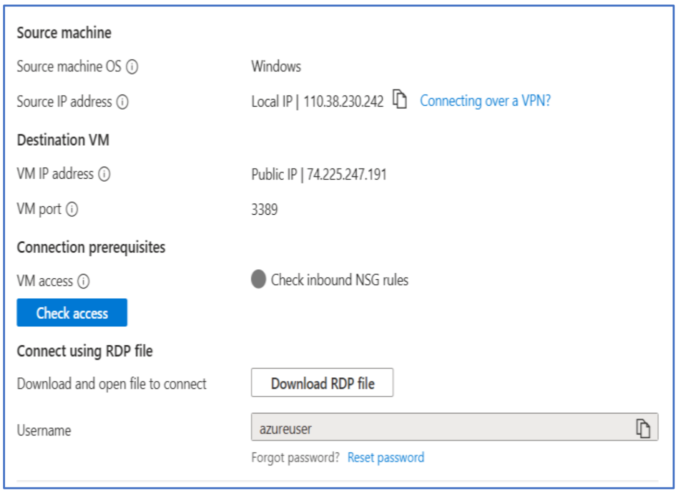
6. Select Add and wait for the rule to be provisioned and then try again to RDP into the virtual machine by going back to Connect This time you should be successful. Remember the user is azureuser and the password is Pa$$w0rd1234.



Created security rule

Successfully created security rule 'AllowRDP'.

a few seconds ago



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 | 74.225.247.191

VM port: 3389

Connection prerequisites

VM access: ● Check inbound NSG rules

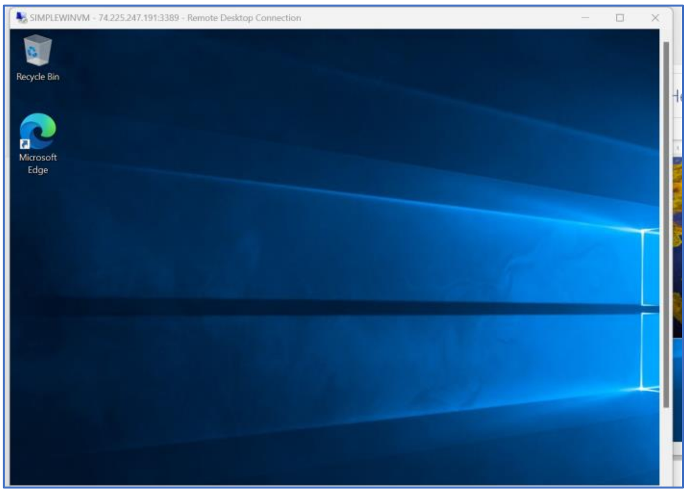
Check access

Connect using RDP file

Download and open file to connect: Download RDP file

Username: azureuser

Forgot password? Reset password



SIMPLEWINVM - 74.225.247.191:3389 - Remote Desktop Connection
Recycle Bin
Microsoft Edge

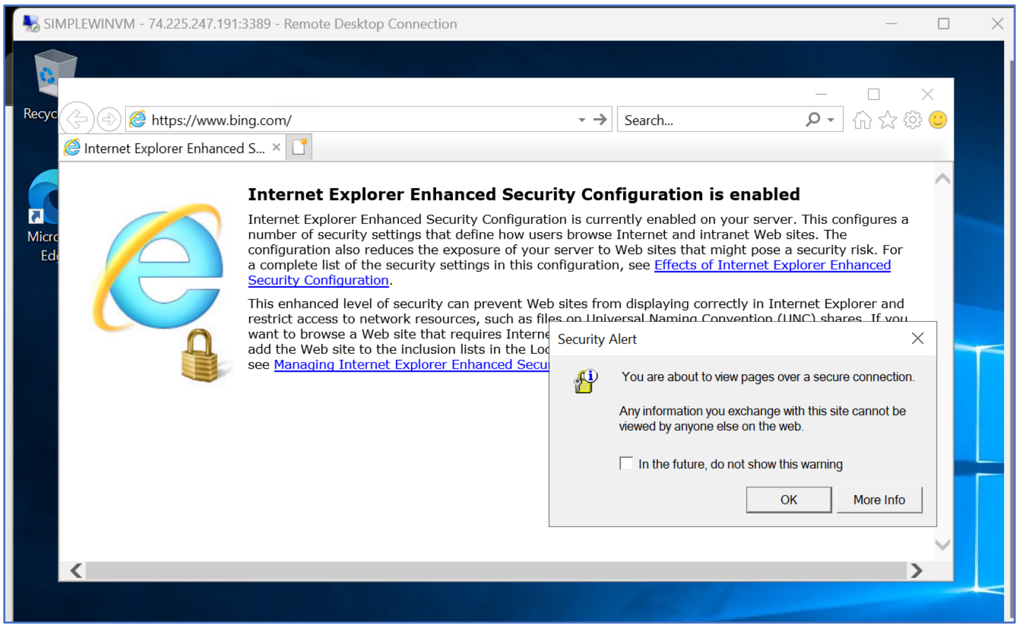
Task 4: Configure an outbound security port rule to deny Internet access

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.


SIMPLEWINVM - 74.225.247.191:3389 - Remote Desktop Connection
https://www.bing.com/
Search...
Internet Explorer Enhanced S...
Recyc
Micro
Ed

Internet Explorer Enhanced Security Configuration is enabled

Internet Explorer Enhanced Security Configuration is currently enabled on your server. This configures a number of security settings that define how users browse Internet and intranet Web sites. The configuration also reduces the exposure of your server to Web sites that might pose a security risk. For a complete list of the security settings in this configuration, see Effects of Internet Explorer Enhanced Security Configuration.

This enhanced level of security can prevent Web sites from displaying correctly in Internet Explorer and restrict access to network resources, such as files on Universal Naming Convention (UNC) shares. If you want to browse a Web site that requires Interne add the Web site to the inclusion lists in the Loc see Managing Internet Explorer Enhanced Secu

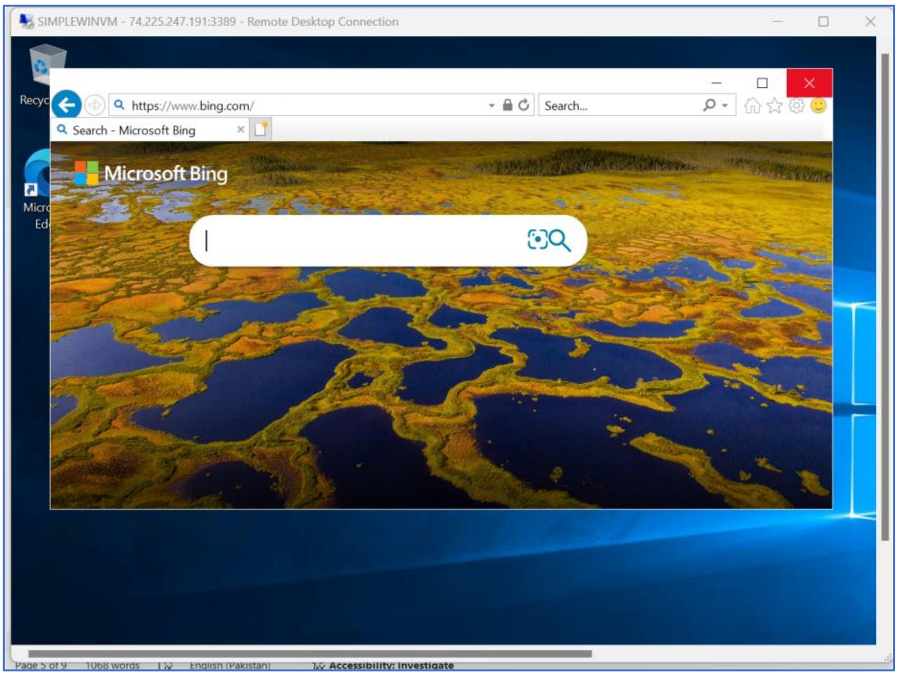
Security Alert

You are about to view pages over a secure connection.

Any information you exchange with this site cannot be viewed by anyone else on the web.

□ In the future, do not show this warning

OK | More Info



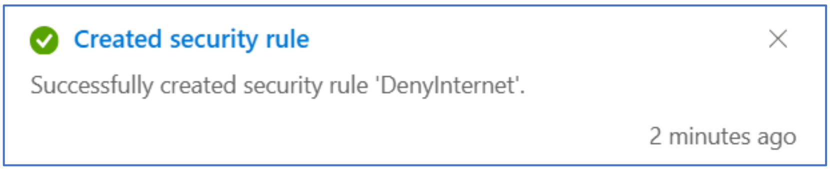
Note: We will now configure a rule to deny outbound internet access.

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.



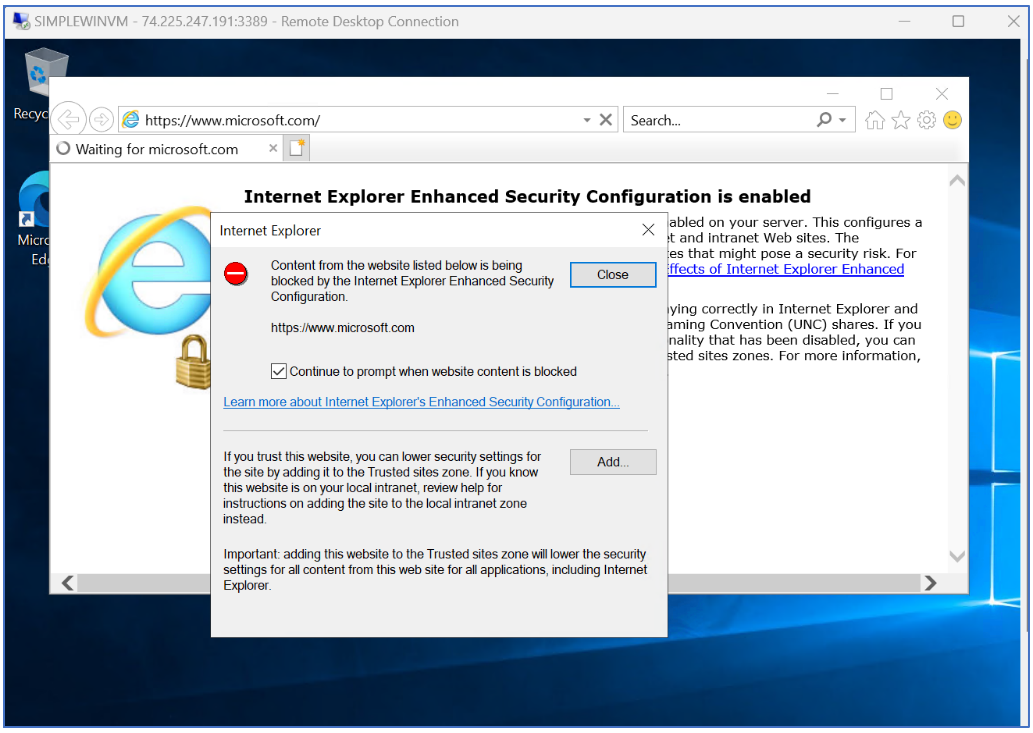
Created security rule

Successfully created security rule 'DenyInternet'.

2 minutes ago

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.



SIMPLEWINVM - 74.225.247.191:3389 - Remote Desktop Connection
Recyc
Micro
Ed
https://www.microsoft.com/
Search...
Waiting for microsoft.com

Internet Explorer Enhanced Security Configuration is enabled

abled on your server. This configures a t and intranet Web sites. The es that might pose a security risk. For ffects of Internet Explorer Enhanced

ying correctly in Internet Explorer and aming Convention (UNC) shares. If you nality that has been disabled, you can sted sites zones. For more information,

Internet Explorer

Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.

https://www.microsoft.com

☑ Continue to prompt when website content is blocked

Learn more about Internet Explorer's Enhanced Security Configuration...

If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.

Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.