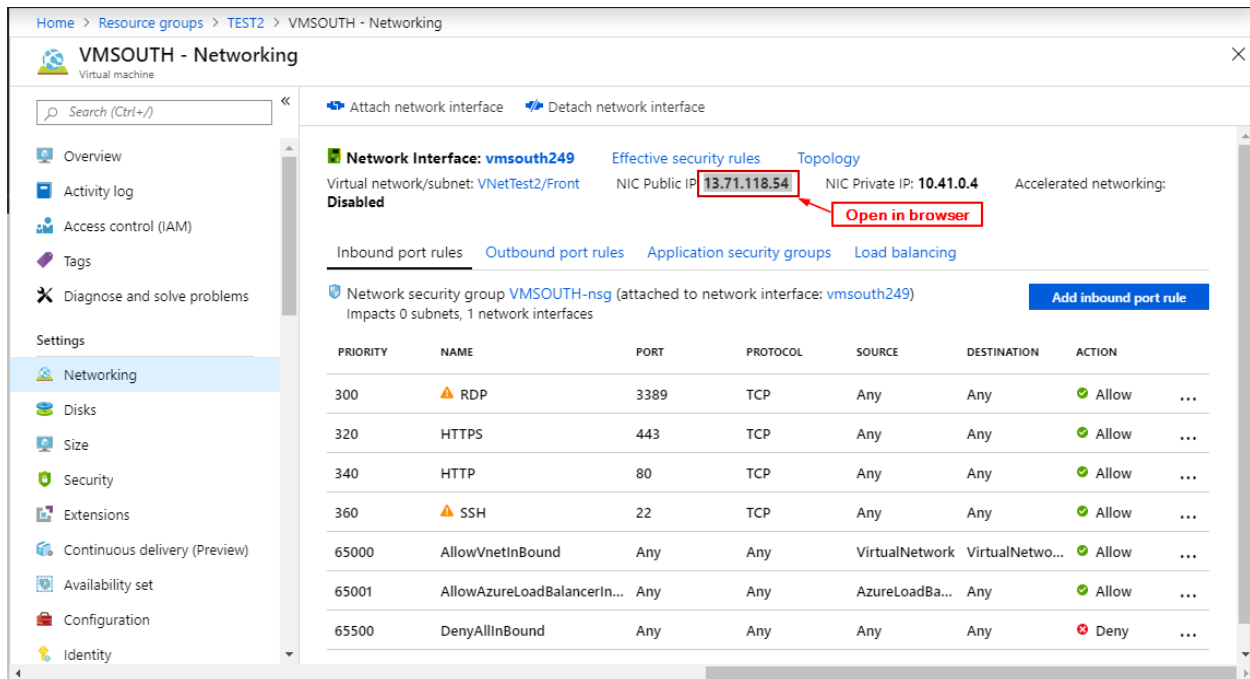


Azure 104 Module 6, Hands On – 11

Add Security rule to NSG

Step 1: Open the VM Attached with the subnet on which security group will be applied.



Home > Resource groups > TEST2 > VMSOUTH - Networking

VMSOUTH - Networking

Virtual machine

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Networking
Disks
Size
Security
Extensions
Continuous delivery (Preview)
Availability set
Configuration
Identity

Attach network interface Detach network interface

Network Interface: vmsouth249 Effective security rules Topology

Virtual network/subnet: VNetTest2/Front Disabled

NIC Public IP: 13.71.118.54 NIC Private IP: 10.41.0.4 Accelerated networking:

Open in browser

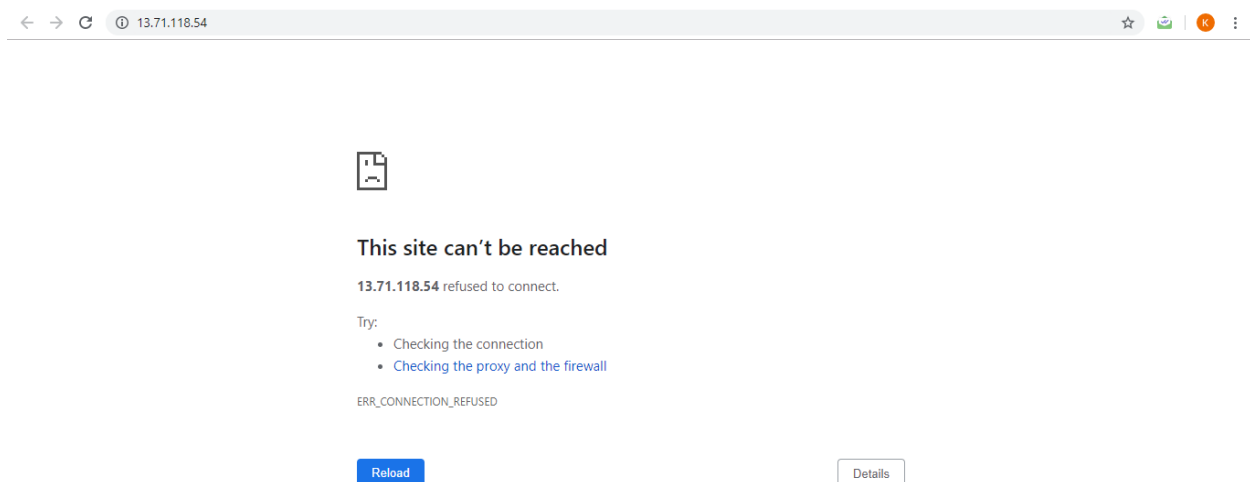
Inbound port rules Outbound port rules Application security groups Load balancing

Network security group VMSOUTH-nsg (attached to network interface: vmsouth249)
Impacts 0 subnets, 1 network interfaces


Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
300	RDP	3389	TCP	Any	Any	Allow
320	HTTPS	443	TCP	Any	Any	Allow
340	HTTP	80	TCP	Any	Any	Allow
360	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwo...	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Step 2: Try to open its public IP ('NIC Public IP') in browser (Notice you can't access it yet).



← → ↻ ⓘ 13.71.118.54 ☆ | K



This site can't be reached

13.71.118.54 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

Reload Details

Step 3: Open the Network Security Group.

Network security groups

Default Directory

+ Add Edit columns Refresh Assign tags

Subscriptions: Free Trial

Filter by name... All resource groups All locations All tags No grouping

14 items

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
<input type="checkbox"/> AllowIIS	TEST2	South India	Free Trial
<input type="checkbox"/> FirstScaleSetnsg	Scaling	South India	Free Trial
<input type="checkbox"/> linuxvm-nsg	demo1	West US	Free Trial
<input type="checkbox"/> VM1-nsg	VNETDEMO	South India	Free Trial
<input type="checkbox"/> VM1nsg143	VNETDEMO	South India	Free Trial
<input type="checkbox"/> VM1nsg696	VNETDEMO	South India	Free Trial
<input type="checkbox"/> VM2-nsg	VNETDEMO	South India	Free Trial
<input type="checkbox"/> VM2nsg479	VNETDEMO	South India	Free Trial
<input type="checkbox"/> VM2nsg598	VNETDEMO	South India	Free Trial
<input type="checkbox"/> VM3TEST-nsg	TEST3	West India	Free Trial
<input type="checkbox"/> VMSOUTH-nsg	TEST2	South India	Free Trial

Click here

Step 4: Click on 'Inbound security rules'.

Home > Network security groups > AllowIIS

AllowIIS
Network security group

Search (Ctrl+/) Move Delete Refresh

Resource group (change)
TEST2

Location
South India

Subscription (change)
Free Trial

Subscription ID
b9be3eac-a886-420f-88c4-c8a6156af111

Tags (change)
[Click here to add tags](#)

Custom security rules
0 inbound, 0 outbound

Associated with
0 subnets, 0 network interfaces

Click Here

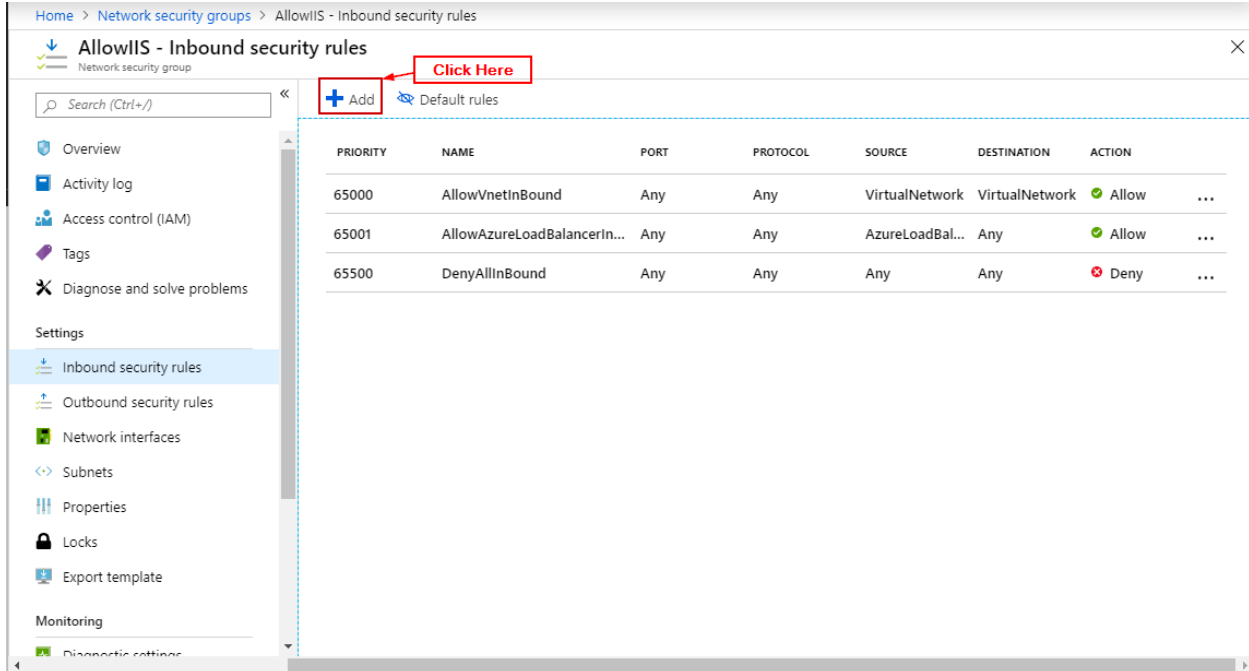
Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwo...	Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
----------	------	------	----------	--------	-------------	--------

Step 5: Click on '+ Add'.



Home > Network security groups > AllowIIS - Inbound security rules

AllowIIS - Inbound security rules

Search (Ctrl+ /)

+ Add Default rules

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

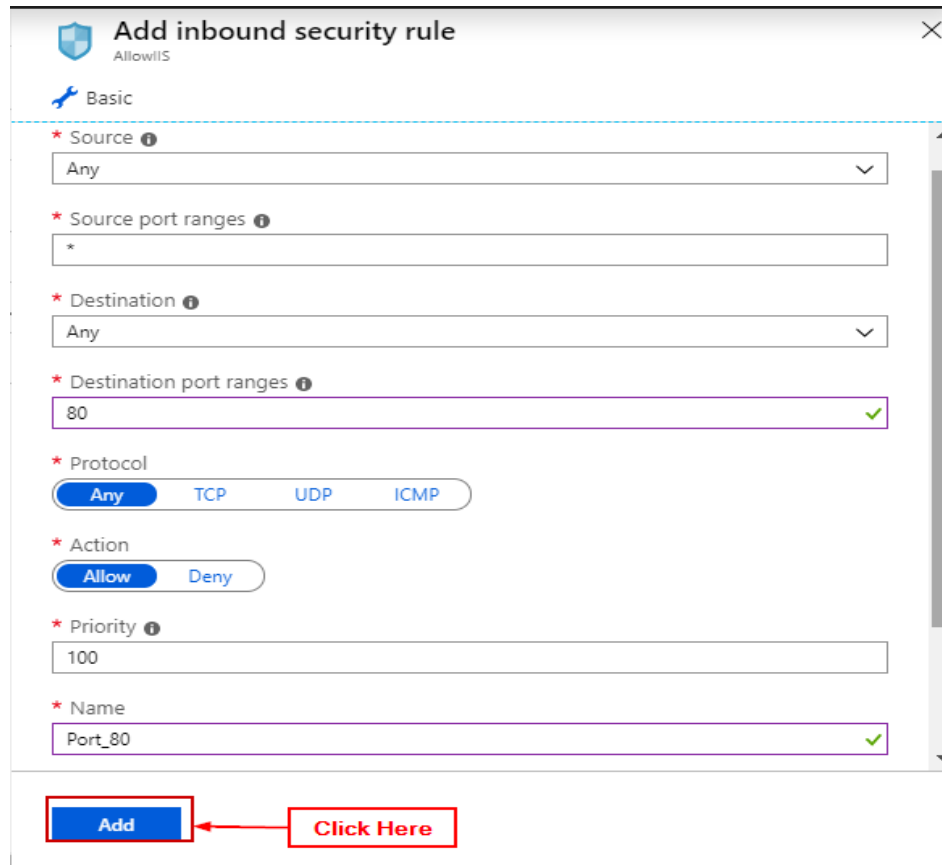
Export template

Monitoring

Diagnostic settings

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBal...	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

Step 6: Enter Details and click "Add".



Add inbound security rule

AllowIIS

Basic

* Source

Any

* Source port ranges

*

* Destination

Any

* Destination port ranges

80

* Protocol

Any TCP UDP ICMP

* Action

Allow Deny

* Priority

100

* Name

Port_80

Add