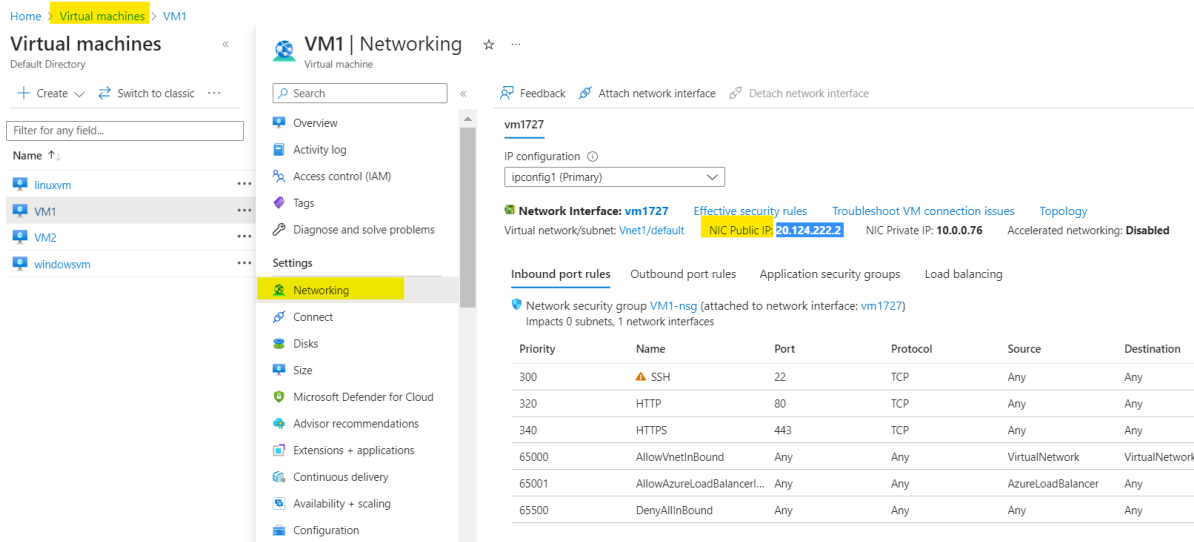




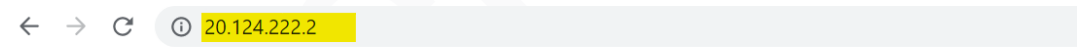
Module 6: Hands-On: Add Security Rule to NSG

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



Priority	Name	Port	Protocol	Source	Destination
300	SSH	22	TCP	Any	Any
320	HTTP	80	TCP	Any	Any
340	HTTPS	443	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Step 2: Open its public IP (NIC Public IP) in the browser (notice you can't access it)



Your connection was interrupted

A network change was detected.

ERR_NETWORK_CHANGED

Reload

Step 3: Open the Network security group and click on Inbound security rules

Home > Network security groups >

Network security g...

Default Directory

+ Create Manage view ...

Filter for any field...

Name ↑↓

- basicNsgrg-4-vnet-nic01
- linuxvm-nsg
- nwewds-nsg
- VM1-nsg**
- VM2-nsg
- windowsvm-nsg

VM1-nsg
Network security group

Search

Move Delete Refresh Give feedback

Overview

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

Settings

- Inbound security rules**
- Outbound security rules
- Network interfaces
- Subnets
- Properties
- Locks

Monitoring

- Alerts

Essentials

Resource group (move) : [Az-104](#)

Location : East US

Subscription (move) : [Azure Pass - Sponsorship](#)

Subscription ID : 4362042a-1e87-43ca-83aa-3c7ebc545a78

Tags (edit) : [Click here to add tags](#)

Filter by name Port == all

Priority ↑↓	Name ↑↓	Port ↑↓
Inbound Security Rules		
300	SSH	22
320	HTTP	80
340	HTTPS	443
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBalanc...	Any
65500	DenyAllInBound	Any

Step 4: Click on +Add

VM1-nsg | Inbound security rules

Network security group

Search

+ Add Hide default rules Refresh Delete Give feedback

Overview

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

Settings


- Inbound security rules**
- Outbound security rules
- Network interfaces
- Subnets
- Properties

Network security group security rules are evaluated by priority using the combination of source, rule can't have the same priority and direction as an existing rule. You can't delete default security rules.

Filter by name Port == all Protocol == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
<input type="checkbox"/> 300	SSH	22	TCP
<input type="checkbox"/> 320	HTTP	80	TCP
<input type="checkbox"/> 340	HTTPS	443	TCP
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	Any	Any
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any

Step 5: Enter the details and click on Add

 **Add inbound security rule** ×
VM1-nsg

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

HTTP

Destination port ranges ⓘ

80

Protocol

☐ Any

☒ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority * ⓘ


350 ✓

Name *

AllowAnyHTTPInbound ✓

Add

Cancel

 Give feedback