

NSG in Subnet Level

→Creating a virtual machine

Home > Compute infrastructure | Virtual machines

Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group *
[Create new](#)

Instance details

Virtual machine name *

Region *
[Deploy to an Azure Extended Zone](#)

Availability options

Security type
[Configure security features](#)

Image *
[See all images](#) | [Configure VM generation](#)

VM architecture ☐ ☒

< Previous Next: Disks > **Review + create**

[Give feedback](#)

→Creation of Virtual machine

Home > Compute infrastructure | Virtual machines

Create a virtual machine

Validation passed

Basics

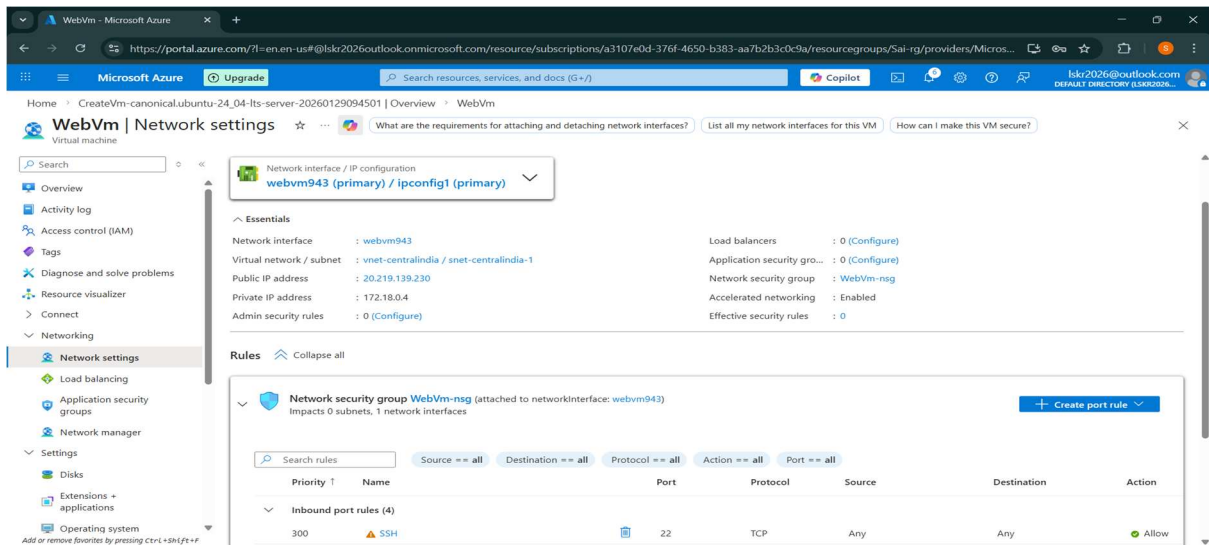
Subscription	Azure subscription 1
Resource group	Sai-rg
Virtual machine name	WebVm
Region	Central India
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Ubuntu Server 24.04 LTS - Gen2
VM architecture	x64
Size	Standard D2ls v5 (2 vcpus, 4 GiB memory)
Enable Hibernation	No
Authentication type	Password
Username	azadmin
Public inbound ports	SSH
Azure Spot	No

Disks

< Previous Next > **Create**

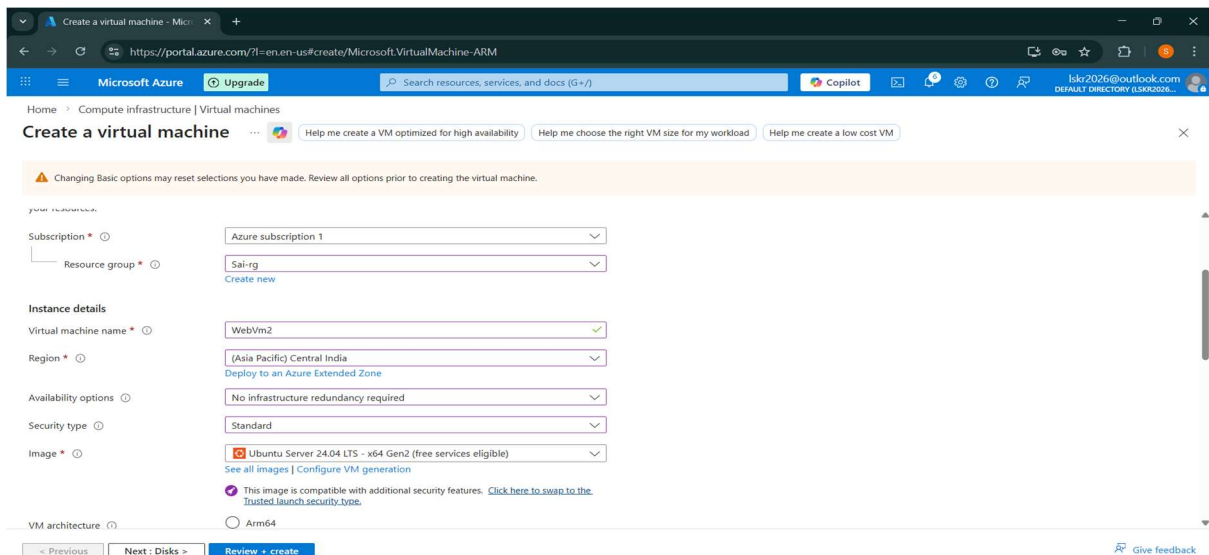
[Download a template for automation](#) [Give feedback](#)

→Nsg while creating the Virtual machine

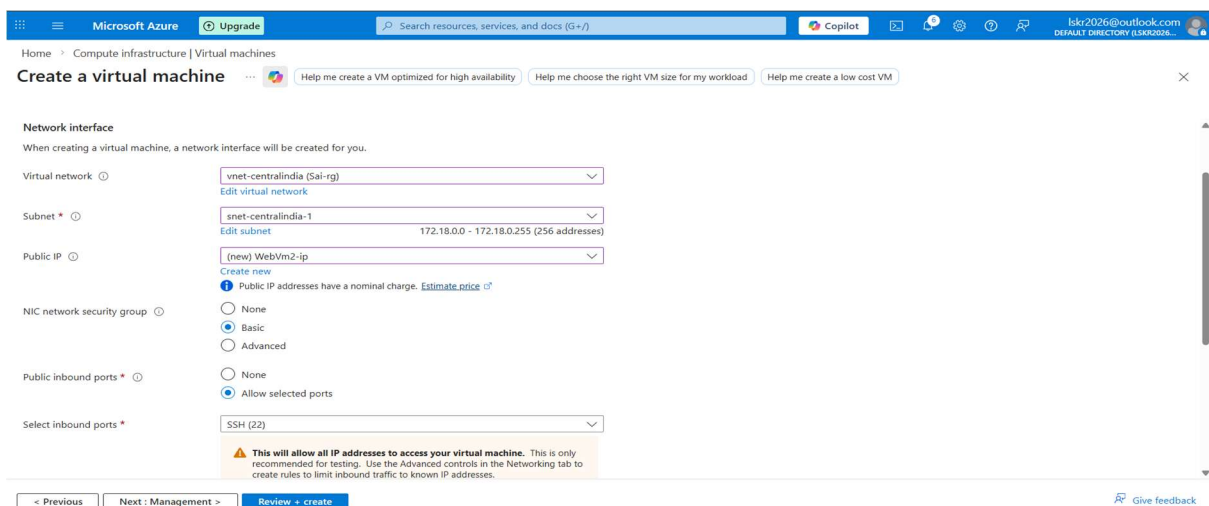


→ It has only one rule allow ssh from any source

→ Creating Web Vm2 with in the same region



→ With in the Same Vnet and subnet



→ Network Security group for WebVm2

Microsoft Azure | Upgrade | Search resources, services, and docs (G+)

Home > CreateVm-canonical.ubuntu-24.04-lts-server-20260129095708 | Overview > WebVm2

WebVm2 | Network settings | Virtual machine

What are the requirements for attaching and detaching network interfaces? | List all my network interfaces for this VM | How can I make this VM secure?

Search

Overview | Activity log | Access control (IAM) | Tags | Diagnose and solve problems | Resource visualizer | Connect | Networking | Network settings | Load balancing | Application security groups | Network manager | Settings | Disks | Extensions + applications | Operating system

Network interface / IP configuration
webvm2800 (primary) / ipconfig1 (primary)

Essentials

Network interface : webvm2800
Virtual network / subnet : vnet-centralindia / snet-centralindia-1
Public IP address : 20.204.16.190
Private IP address : 172.18.0.5
Admin security rules : 0 (Configure)

Load balancers : 0 (Configure)
Application security gro... : 0 (Configure)
Network security group : WebVm2-nsg
Accelerated networking : Enabled
Effective security rules : 0

Rules Collapse all

Network security group WebVm2-nsg (attached to networkInterface: webvm2800)
Impacts 0 subnets, 1 network interfaces

Create port rule

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

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

→ In the both Nsg doesn't have the inbound http rule

→ Here I can create a Network Security group and add it to the subnet level

→ Install Nginx on two Vms

→ WebVm

```
root@WebVm:/home/azadmin# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-01-29 04:42:40 UTC; 46s ago
     Docs: man:nginx(8)
  Process: 2688 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Process: 2689 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 2720 (nginx)
    Tasks: 3 (limit: 4662)
   Memory: 2.4M (peak: 5.3M)
      CPU: 19ms
   CGroup: /system.slice/nginx.service
           └─2720 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─2722 "nginx: worker process"
               └─2723 "nginx: worker process"

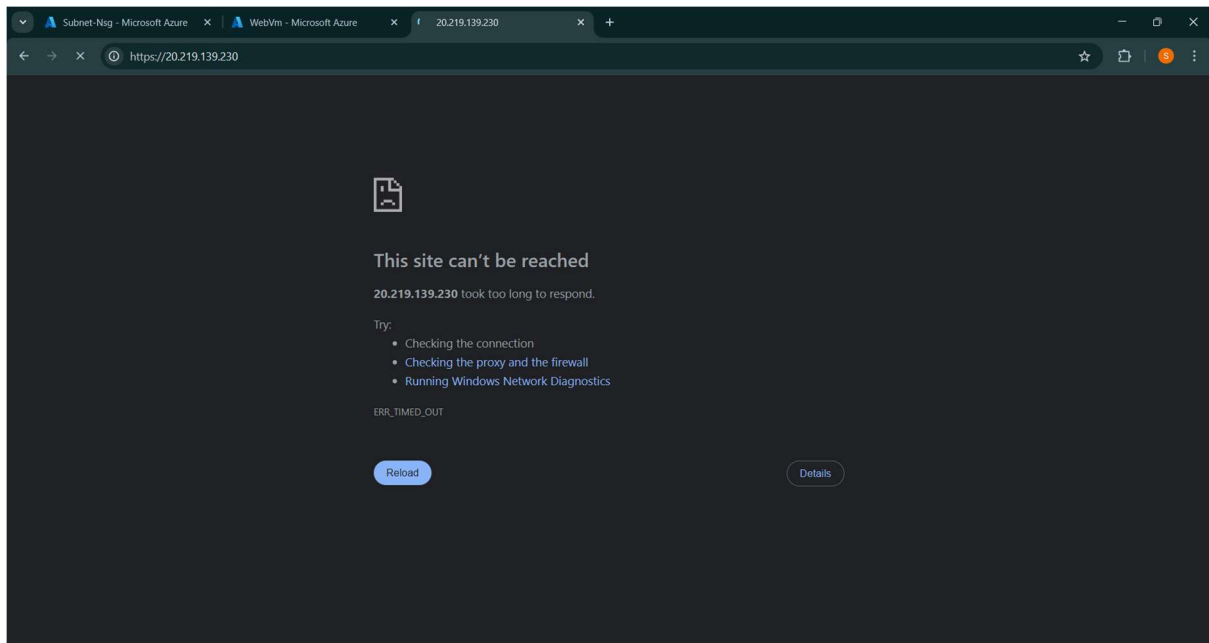
Jan 29 04:42:40 WebVm systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Jan 29 04:42:40 WebVm systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@WebVm:/home/azadmin#
```

→ WebVm2

```
root@WebVm2:/home/azadmin# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-01-29 04:47:09 UTC; 1min 27s ago
     Docs: man:nginx(8)
  Process: 2301 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Process: 2303 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 2333 (nginx)
    Tasks: 3 (limit: 4662)
   Memory: 2.4M (peak: 5.3M)
      CPU: 19ms
   CGroup: /system.slice/nginx.service
           └─2333 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─2335 "nginx: worker process"
               └─2336 "nginx: worker process"

Jan 29 04:47:09 WebVm2 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Jan 29 04:47:09 WebVm2 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@WebVm2:/home/azadmin#
```

→Browsing WebVm public IP



→Creating a new Security Group

Home > Network foundation | Network security groups

Create network security group ...

✓ Validation passed

Basics Tags Review + create

Basics

Subscription	Azure subscription 1
Resource group	Sai-rg
Region	Central India
name	Subnet-Nsg

Tags

None

Create

< Previous

Next >

[Download a template for automation](#)

→Nsg with default rules

Home > CreateNetworkSecurityGroupBladeV2-20260129101959 | Overview

Subnet-Nsg
Network security group

Diagnose connectivity issues related to this security group | Retrieve detailed information for troubleshooting security rules | Analyze security rules for this network security group

Search resources, services, and docs (G+/)

Move | Delete | Refresh | Give feedback

Overview

Activity log | Access control (IAM) | Tags | Diagnose and solve problems | Resource visualizer | Settings | Monitoring | Automation | Help

Essentials

Resource group (move): Sai-rg | Custom security rules: 0 inbound, 0 outbound
Location: Central India | Associated with: 0 subnets, 0 network interfaces
Subscription (move): Azure subscription 1
Subscription ID: a3107e0d-376f-4650-b383-aa7b2b3c0c9a
Tags (edit): Add tags

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

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Add or remove favorites by pressing Ctrl+Shift+F

→Click on Settings

→Then click on Inbound Security rules

→Click on add

→Enter the rule allowing http

Home > Network foundation | Network security groups > Subnet-Nsg

Subnet-Nsg | Inbound security rules
Network security group

Search resources, services, and docs (G+/)

Add | Hide default rules | Refresh | Delete | Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, protocol, and action. Rules with the same priority and direction as an existing rule can be overridden, but you can't delete default security rules.

Filter by name | Port == all | Protocol == all | Source == all

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule
Subnet-Nsg

Source: Any

Source port ranges: *

Destination: Any

Service: HTTP

Destination port ranges: 80

Protocol: TCP

Action: Allow

Add | Cancel | Give feedback

Add or remove favorites by pressing Ctrl+Shift+F

→ Rule Created allowing http to any

Home > Network foundation > Network security groups > Subnet-Nsg

Subnet-Nsg | Inbound security rules

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

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

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowingWebServices	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

→ Select Subnets and click on Associate

Home > Subnet-Nsg

Subnet-Nsg | Subnets

Associate

Search subnets

Name	Address range	Virtual network
No results.		

→ Select Vnet and Subnet

Home > Subnet-Nsg

Subnet-Nsg | Subnets

Associate

Search subnets

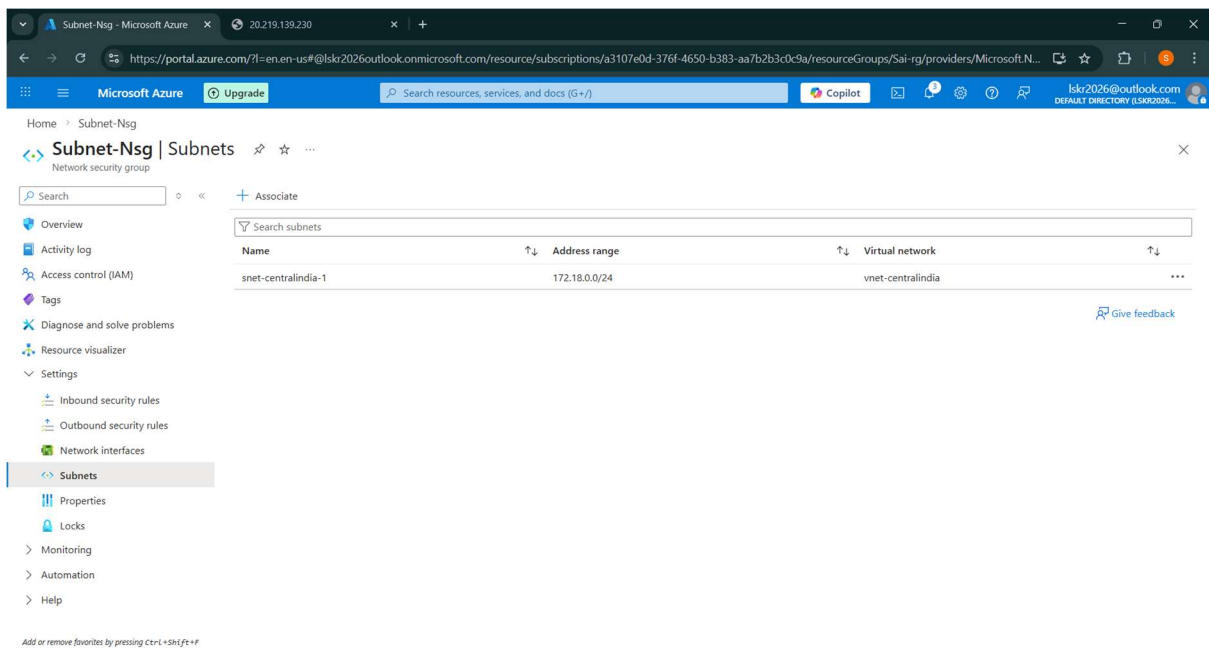
No results.

Associate subnet

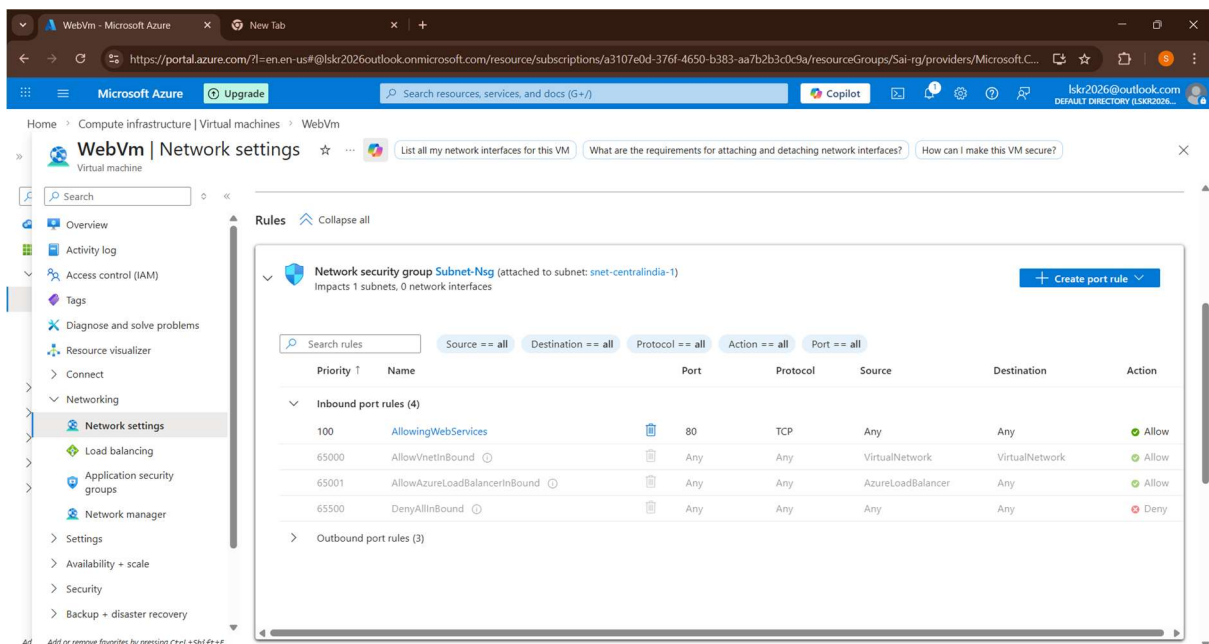
Subnet-Nsg

Virtual network: vnet-centralindia (Sai-rg)

Subnet: snet-centralindia-1

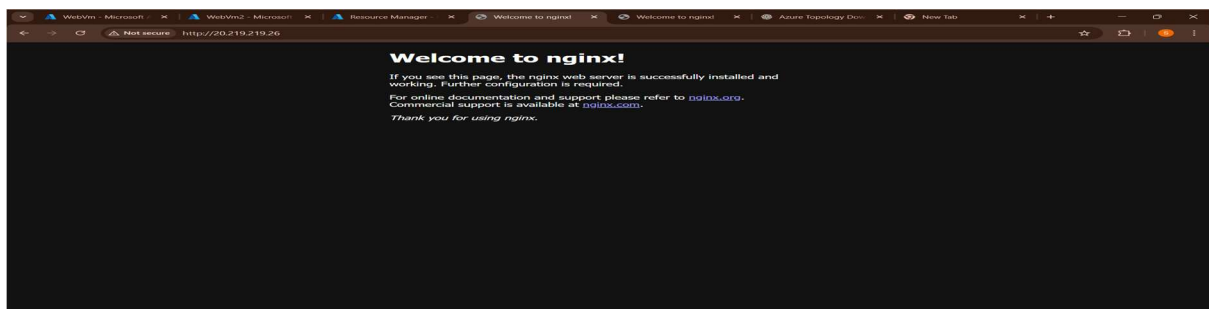


→ Here the Subnet Nsg is attached with WebVm



→ Now we can browse the public ip of two WebVm's it will work

→ WebVm's



Note: If we want to enable two security groups the rules must be in the both nic level nsrg and Subnet level nsrg

→ Here in the Network Settings there two Nsg's one is Nic level and another one is subnet level.

→ In Subnet level ssh will allow it works for both nic level and subnet level

→ In the nic level http works only for this machine.

Is there any rules in nic level it must be in subnet level

→ First it checks in nic level if it is available then check in subnet level and it works. There is no rule in subnet it will not connect

→ Main purpose

Use Subnet NSG for common rules

Use NIC NSG only for special cases

The screenshot shows the Azure portal interface for a virtual machine named 'WebVm2'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Network settings (selected), Load balancing, Application security groups, Network manager, Settings, Disks, Extensions + applications, and Operating system.

The main content area is titled 'WebVm2 | Network settings'. It includes a search bar and several tabs: 'How can I make this VM secure?', 'What are the requirements for attaching and detaching network interfaces?', and 'List all my network interfaces for this VM'. Below these tabs, there is a table of network rules.

Priority	Name	Port	Protocol	Source	Destination	Action
100	allow-ssh	22	Any	Any	Any	Allow
110	http	80	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Below the table, there is a section for 'Outbound port rules (3)'. The 'Network security group WebVm2' is shown as attached to the network interface 'webvm2174'. It impacts 0 subnets and 1 network interface. A '+ Create port rule' button is visible.

The 'Network security group WebVm2' section includes a search bar and filters: Source == all, Destination == all, Protocol == all, Action == all, Port == all. Below these filters, there is a table of inbound port rules.

Priority	Name	Port	Protocol	Source	Destination	Action
100	http	80	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow