

NSG in Subnet Level

→Creating 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 *

Virtual machine name *

Region *

Availability options

Security type

Image *

VM architecture

< Previous Give feedback

→Creation of 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 Create Give feedback

→Nsg while creating the Virtual machine

Network interface / IP configuration
webvm943 (primary) / ipconfig1 (primary)

Essentials

- Network interface: webvm943
- Virtual network / subnet: vnet-centralindia / snet-centralindia-1
- Public IP address: 20.219.139.230
- Private IP address: 172.18.0.4
- Admin security rules: 0 (Configure)
- Load balancers: 0 (Configure)
- Application security groups: 0 (Configure)
- Network security group: WebVm-nsg
- Accelerated networking: Enabled
- Effective security rules: 0

Rules

Network security group WebVm-nsg (attached to networkInterface: webvm943)
Impacts 0 subnets, 1 network interfaces

Priority ↑	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow

→ It has only one rule allow ssh from any source

→ Creating Web Vm2 with in the same region

Subscription: Azure subscription 1
Resource group: Sai-rg

Virtual machine name: WebVm2
Region: (Asia Pacific) Central India
Availability options: No infrastructure redundancy required
Security type: Standard
Image: Ubuntu Server 24.04 LTS - x64 Gen2 (free services eligible)
VM architecture: Arm64

Help me create a VM optimized for high availability | Help me choose the right VM size for my workload | Help me create a low cost VM

→ With in the Same Vnet and subnet

Virtual network: vnet-centralindia (Sai-rg)
Subnet: snet-centralindia-1
Public IP: (new) WebVm2-ip
NIC network security group: Basic
Public inbound ports: SSH (22)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network: vnet-centralindia (Sai-rg)
Subnet: snet-centralindia-1
Public IP: (new) WebVm2-ip
NIC network security group: Basic
Public inbound ports: SSH (22)

Select inbound ports: This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

→ Network Security group for WebVm2

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'CreateVm-canonical.ubuntu-24_04-lts-server-20260129095708'. The 'Network settings' section is selected. It displays the 'webvm2800 (primary) / ipconfig1 (primary)' configuration. Under 'Essentials', details like Network interface (webvm2800), Virtual network / subnet (vnet-centralindia / snet-centralindia-1), and Public IP address (20.204.16.190) are shown. Under 'Rules', a Network security group 'WebVm2-nsg' is listed, which impacts 0 subnets and 1 network interface. A table shows an inbound port rule for SSH (port 22, TCP, Any, Any, 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;"

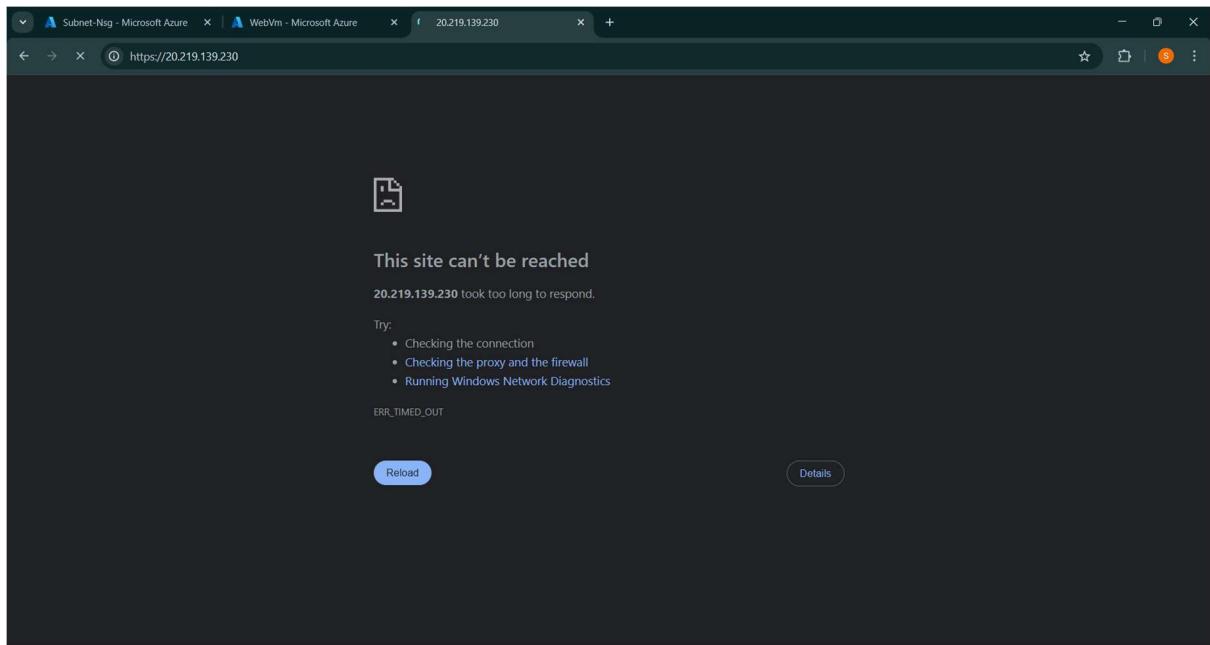
Jan 29 04:42:40 WebVm systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy server...
Jan 29 04:42:40 WebVm systemd[1]: Started nginx.service - A high performance web server and a reverse proxy server.
root@WebVm:/home/azadmin#
```

→ 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.
```

→ 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

Subnet-Nsg - Microsoft Azure

Overview

Resource group (move) : Sai-rg

Location : Central India

Subscription (move) : Azure subscription 1

Subscription ID : a3107e0d-376f-4650-b383-aa7b2b3c0c9a

Tags (edit) : Add tags

Inbound Security Rules

Priority ↑	Name ↑	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerIn	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↑	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

→ Click on Settings

→ Then click on Inbound Security rules

→ Click on add

→ Enter the rule allowing http

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

→ Rule Created allowing http to any

The screenshot shows the Microsoft Azure portal interface for managing Network Security Groups (NSGs). The user is navigating through the 'Subnet-Nsg | Inbound security rules' section. A success message in the top right corner states 'Created security rule' and 'Successfully created security rule 'AllowingWebServices''. The main table lists five security rules:

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

The screenshot shows the 'Subnet-Nsg | Subnets' page. The 'Associate' button is highlighted. The search bar shows 'Search subnets'. The table below shows no results.

Name	Address range	Virtual network
No results.		

→ Select Vnet and Subnet

The screenshot shows the 'Associate subnet' dialog box. It has two dropdown menus: 'Virtual network' set to 'vnet-centralindia (Sai-rg)' and 'Subnet' set to 'snet-centralindia-1'.

Subnet-Nsg | Subnets

Name	Address range	Virtual network
snet-centralindia-1	172.18.0.0/24	vnet-centralindia

→ Here the Subnet Nsg is attached with WebVm

Priority ↑	Name	Port	Protocol	Source	Destination	Action
100	AllowingWebServices	80	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

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

→ WebVm's

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.

Commercial support is available at nginx.com.

Thank you for using nginx.

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

→ 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 has a 'Network settings' section selected. The main area displays two tables of network rules:

- VM port rules:** This table lists rules for the VM's network interface. It includes rules for port 22 (allow-ssh), port 80 (http), and other ports like 65000 (AllowVnetInbound) and 65001 (AllowAzureLoadBalancerInbound).
- Network security group (NSG) port rules:** This table lists rules for the NSG attached to the VM. It includes rules for port 80 (http) and port 65000 (AllowVnetInbound).

The rules are organized by priority and name. The NSG table also includes columns for Source, Destination, Protocol, and Action.