

SMITKUMAR KHOKHARIYA

Project 2: Azure Virtual Machine Networking Setup

Objective: Configure networking for Azure Virtual Machines (VMs) to enable communication both within the virtual network and with external resources.


Solution Steps:

1) Create Virtual Networks (VNETs) and Subnets: Set up one or more virtual networks in Azure, dividing them into subnets based on the network segmentation requirements of your application.

-> Here, I have created on Virtual Network named **VNET-01** with three subnet; **subnet-01** (10.0.1.0/24), **subnet-02**(10.0.2.0/24), **subnet-nva**(10.0.3.0/24)

in a “**Project-02**” resource group.

[Home](#) > [Resource groups](#) > [Project-02](#) > [VNET-01](#)

 **VNET-01 | Subnets** ☆ ...

Virtual network

[+ Subnet](#) [+ Gateway subnet](#) [Refresh](#) | [Manage users](#) [Delete](#)

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓	
nva-subnet	10.0.3.0/24	-	250	-	-	-	...
subnet-02	10.0.2.0/24	-	250	-	vm-02311_z1-nsg	RouteTable-Subnet-2	...
subnet-01	10.0.1.0/24	-	250	-	vm-01589_z1-nsg	RouteTable-Subnet1	...

[Give feedback](#)

2) Deploy Linux and Windows VMs: Create Linux and Windows VM instances within the configured subnets. Ensure that each VM is assigned appropriate network interfaces and private IP addresses.

-> For these steps, I have created Three Virtual machines; **VM-01**, **VM-02** and **NVA-VM**.

Home >

Virtual machines

Default Directory (smitkhokhariyaoutlook.onmicrosoft.com)

+ Create ▾ ↻ Switch to classic ⌚ Reservations ▾ ⚙ Manage view ▾ ↻ Refresh ⬇ Export to CSV 🔍 Open query | 🏷 Assign tags ▶ Start ⏮ Restart ☐ Stop 🗑 Delete

Filter for any field... Subscription equals all Type equals all Resource group equals all Location equals all Add filter

Showing 1 to 3 of 3 records. No grouping

<input type="checkbox"/> Name ↑↓	Subscription ↑↓	Resource group ↑↓	Location ↑↓	Status ↑↓	Operating system ↑↓	Size ↑↓	Public IP address
<input type="checkbox"/> NVA-VM	Azure subscription 1	PROJECT-02	Canada Central	Running	Linux	Standard_B1s	52.138.38.100
<input type="checkbox"/> VM-01	Azure subscription 1	PROJECT-02	Canada Central	Running	Linux	Standard_B1s	4.206.135.224
<input type="checkbox"/> VM-02	Azure subscription 1	Project-02	Canada Central	Running	Linux	Standard_B1s	4.206.0.144

3) Configure Network Security Groups (NSGs): Define NSGs to control inbound and outbound traffic to the VMs. Specify firewall rules to allow or deny traffic based on protocol, port, and source/destination IP addresses.

-> configured and associated NSG to the respective VMs. applied rule to allow internal communication and make SSH possible.

-> configured rule to allow traffic coming from NVA and reach successfully to destination vm.

vm-01589_z1-nsg

Network security group

 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
 - Diagnostic settings
 - Logs
 - NSG flow logs
- Automation
 - CLI / PS

Essentials

Resource group (move) : [Project-02](#)

Location : Canada Central

Subscription (move) : [Azure subscription 1](#)

Subscription ID : 7640872c-7cea-48ed-bc85-f6c700d4265a

Tags (edit) : [Add tags](#)

Custom security rules : 2 inbound, 1 outbound

Associated with : 1 subnets, 1 network interfaces

[JSON View](#)

Port == all

Protocol == all

Source == all

Destination == all

Action == all

Priority	Name	Port	Protocol	Source	Destination	Action	
Inbound Security Rules							
120	AllowAnySSHInbound	22	TCP	Any	VirtualNetwork	Allow	
130	AllowWebRoute	Any	Any	10.0.3.0/24	10.0.1.4	Allow	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
65001	AllowAzureLoadBalance...	Any	Any	AzureLoadBalancer	Any	Allow	
65500	DenyAllInBound	Any	Any	Any	Any	Deny	
Outbound Security Rules							
110	AllowAnyCustom80443...	Any	Any	10.0.1.4	10.0.3.0/24	Allow	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	

VM-02 | Network settings

Virtual machine

 This is a new experience. [Please provide feedback](#)Rules Collapse all

Network security group **vm-02311_z1-nsg** (attached to subnet: [subnet-02](#))
Impacts 1 subnets, 1 network interfaces

[+ Create port rule](#)

Source == all

Destination == all

Protocol == all

Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
120	AllowAnySSHInbound	22	TCP	Any	VirtualNetwork	Allow
130	AllowWebRoute	Any	Any	10.0.3.0/24	10.0.2.4	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (4)						
110	AllowAnyCustom80443Outbound	Any	Any	10.0.2.4	10.0.3.0/24	Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

4) Implement Azure Firewall or Network Virtual Appliances (NVAs): Optionally, deploy Azure Firewall or third-party Network Virtual Appliances (NVAs) to add an additional layer of security and advanced traffic filtering capabilities to your virtual network.

-> Deployed a NVA-VM as a **Network Virtual Appliances (NVAs)**, configured to make it act as a NVM. Enable IP forwarding to forward incoming traffic to respective VM.

Virtual machine

NVA-VM | Network settings

☆ ...

×

Search

⌕

⌕ This is a new experience. [Please provide feedback](#)

×

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Connect

Bastion

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Operating system

Configuration

Advisor recommendations

Properties

Locks

Availability + scale

Size

Availability + scaling

Security

Identity

Virtual network / subnet : VNET-01 / nva-subnet

Public IP address : 52.138.38.100

Private IP address : 10.0.3.4

Admin security rules : 0 (Configure)

Application security grou... : 0 (Configure)

Network security group : nva-vm440_z1-nsg

Accelerated networking : Disabled

Effective security rules : 0

Rules

⌵ Collapse all

Network security group nva-vm440_z1-nsg (attached to networkInterface: nva-vm440_z1)

Impacts 0 subnets, 1 network interfaces

+ Create port rule

Search rules

Source == all

Destination == all

Protocol == all

Action == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action	
Inbound port rules (6)							
100	AllowAnySSHInbound	22	TCP	Any	Any	Allow	
110	AllowCidrBlockCustom8080Inbound	Any	Any	10.0.1.0/24	10.0.3.4	Allow	
122	AllowCidrBlockCustom8080Inbound01	Any	Any	10.0.2.0/24	10.0.3.4	Allow	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	
65500	DenyAllInBound	Any	Any	Any	Any	Deny	
Outbound port rules (5)							
130	AllowCidrBlockCustom8080Outbound	Any	Any	10.0.3.4	10.0.1.0/24	Allow	
142	AllowCidrBlockCustom8080Outbound	Any	Any	10.0.3.4	10.0.2.0/24	Allow	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	

Home > Virtual machines > NVA-VM | Network settings > nva-vm440_z1

nva-vm440_z1 | IP configurations

☆ ...

Network interface

Search

⌕

Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

Locks

Monitoring

Insights

Alerts

Metrics

Diagnostic settings

IP Settings

Enable IP forwarding

Virtual network

Gateway load balancer

Subnet

250 free IP addresses

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. [Learn more](#)

+ Add ⚙ Make primary 🗑 Delete

Name	IP Version	Type	Private IP Address	Public IP Address
<input type="checkbox"/> ipconfig1	IPv4	Primary	10.0.3.4 (Dynamic)	52.138.38.100 (pip-vnet-01-canadacentral-nva-subnet)

5) Set Up Network Address Translation (NAT) Gateway: Configure NAT Gateway to allow VMs within a private subnet to initiate outbound connections to the internet while keeping their private IP addresses hidden.

-> Set up NAT Gateway to not expose private IP of Subnet-1 and Subnet-2 to the internet.

NAT-Gateway | Subnets

NAT gateway

Search [] x << Save Discard Disassociate Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Outbound IP
 - Subnets**
 - Configuration
 - Properties
 - Locks
- Monitoring
 - Insights

To use the NAT gateway, at least one subnet must be selected. You can add and remove subnets after creating the NAT gateway.

Virtual network ⓘ
VNET-01
[Create new](#)

Subnets that have any of the following resources are not shown because they are not compatible:

- A load balancer with a Basic SKU
- A public IP address with a Basic SKU
- An existing NAT gateway
- A virtual network gateway

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> nva-subnet	10.0.3.0/24
<input checked="" type="checkbox"/> subnet-02	10.0.2.0/24
<input checked="" type="checkbox"/> subnet-01	10.0.1.0/24

[Manage subnets >](#)

NAT-Gateway | Outbound IP

NAT gateway

Search [] x << Edit Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Outbound IP** ☆
 - Subnets
 - Configuration
 - Properties

View and configure which public IP addresses and public IP prefixes will be used for outbound connectivity. At l

Public IP addresses

Name ↓	IP address ↑↓	DNS name ↑↓	Remove
nat-pip	4.206.1.194		×

Public IP prefixes

Name ↓	IP prefix ↑↓	Remove
--------	--------------	--------

6) Establish External Communication: Configure public IP addresses and associate them with the appropriate VMs to enable external access. Implement port forwarding rules in NSGs or Azure Firewall to allow inbound traffic to reach specific VMs and services.

- attached NSG screenshot in a NSG section **3)**

7) Enable Internal Communication Between VMs: Ensure that VMs within the same virtual network can communicate with each other using private IP addresses. Adjust NSG rules as needed to allow required traffic between VMs.

-> Configure route table rule to pass traffic through NVA-VM and reach the destination.

RouteTable-Subnet-2

Route table

Search

MoveDeleteRefreshGive feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Properties

Locks

Monitoring

Alerts

Automation

CLI / PS

Essentials

Associations : 1 subnet associations

Resource group (move) : Project-02

Location : Canada Central

Subscription (move) : Azure subscription 1

Subscription ID : 7640872c-7cea-48ed-bc85-f6c700d4265a

Tags (edit) : Add tags

Routes

Search routes

Name	Address prefix	Next hop type	Next hop IP address	
RT-Subnet-2	10.0.1.0/24	Virtual appliance	10.0.3.4	...

Subnets

Search subnets

Name	Address range	Virtual network	Security group	
subnet-02	10.0.2.0/24	VNET-01	vm-02311_z1-nsg	...

RouteTable-Subnet1

Route table

Search

MoveDeleteRefreshGive feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Properties

Locks

Monitoring

Alerts

Automation

CLI / PS

Essentials

Associations : 1 subnet associations

Resource group (move) : Project-02

Location : Canada Central

Subscription (move) : Azure subscription 1

Subscription ID : 7640872c-7cea-48ed-bc85-f6c700d4265a

Tags (edit) : Add tags

Routes

Search routes

Name	Address prefix	Next hop type	Next hop IP address	
Route-to-NVA	10.0.2.0/24	Virtual appliance	10.0.3.4	...

Subnets

Search subnets

Name	Address range	Virtual network	Security group	
subnet-01	10.0.1.0/24	VNET-01	vm-01589_z1-nsg	...

```
Downloads — azureuser@VM-02: ~ — ssh -i key2.pem azureuser@4.206.0.144 — 71x13
[azureuser@VM-02:~$ ping 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp_seq=1 ttl=63 time=3.61 ms
64 bytes from 10.0.1.4: icmp_seq=2 ttl=63 time=2.41 ms
64 bytes from 10.0.1.4: icmp_seq=3 ttl=63 time=2.50 ms
64 bytes from 10.0.1.4: icmp_seq=4 ttl=63 time=1.80 ms
64 bytes from 10.0.1.4: icmp_seq=5 ttl=63 time=3.40 ms
64 bytes from 10.0.1.4: icmp_seq=6 ttl=63 time=2.28 ms
64 bytes from 10.0.1.4: icmp_seq=7 ttl=63 time=2.75 ms
█
```

```
Downloads — azureuser@VM-01: ~ — ssh -i key2.pem azureuser@4.206.135.224 — ...
[azureuser@VM-01:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=63 time=2.09 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=63 time=2.33 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=63 time=2.31 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=63 time=3.11 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=63 time=2.25 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=63 time=2.51 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=63 time=3.41 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=63 time=1.94 ms
```

8) Test Communication From Inside and Outside: Verify that VMs can communicate with each other within the virtual network and with external resources such as internet services or on-premises networks. Perform network connectivity tests and troubleshoot any issues that arise.

-> Internal Traffic is successfully passing through **NVA-VM**

```
Downloads — azureuser@VM-02: ~ — ssh -i key2.pem azureuser@4.206.0.144 — 80x13
[azureuser@VM-02:~$ traceroute 10.0.1.4
traceroute to 10.0.1.4 (10.0.1.4), 30 hops max, 60 byte packets
 1 nva-vm.internal.cloudapp.net (10.0.3.4) 1.639 ms 1.885 ms 1.555 ms
 2 * vm-01.internal.cloudapp.net (10.0.1.4) 2.431 ms *
azureuser@VM-02:~$ █

Downloads — azureuser@VM-01: ~ — ssh -i key2.pem azureuser@4.206.135.224 — 79x13
[azureuser@VM-01:~$ traceroute 10.0.2.4
traceroute to 10.0.2.4 (10.0.2.4), 30 hops max, 60 byte packets
 1 nva-vm.internal.cloudapp.net (10.0.3.4) 1.537 ms 1.492 ms 1.468 ms
 2 vm-02.internal.cloudapp.net (10.0.2.4) 2.974 ms 2.825 ms 2.793 ms
azureuser@VM-01:~$ █
```


For external traffic:

It is not exposing the private ip of the VM when it reaches the internet. It is exposing NAT public ip.

```
Downloads — azureuser@VM-02: ~ — ssh -i key2.pem azureuser@4.206.0.144 — 92x23
azureuser@VM-02:~$ curl ifconfig.me
azureuser@VM-02:~$ curl ifconfig.me
4.206.1.194azureuser@VM-02:~$ █

Downloads — azureuser@VM-01: ~ — ssh -i key2.pem azureuser@4.206.135.224 — 85x13
azureuser@VM-01:~$ curl ifconfig.me
azureuser@VM-01:~$ curl ifconfig.me
4.206.1.194azureuser@VM-01:~$ █

Downloads — azureuser@VM-02: ~ — ssh -i key2.pem azureuser@4.206.0.144 — 80x26
azureuser@VM-02:~$ traceroute 10.0.1.4
traceroute to 10.0.1.4 (10.0.1.4), 30 hops max, 60 byte packets
 1 nva-vm.internal.cloudapp.net (10.0.3.4)  1.639 ms  1.885 ms  1.555 ms
 2 * vm-01.internal.cloudapp.net (10.0.1.4)  2.431 ms *
azureuser@VM-02:~$ curl http://www.google.com
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-
CA"><head><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><me
ta content="/images/branding/googleg/1x/googleg_standard_color_128dp.png" itempr
op="image"><title>Google</title><script nonce="iSKutfX6k42XgNnTWGVmiw">(functior
){var __g={kEI:'JoQFZ-D0M6-m2roPLOSu-Qo',kEXPI:'0,3700278,1106,448528,90133,2872
,2891,89155,18161,60057,102380,23024,6700,106646,19673,8155,8860,14490,7451,1498
5,9779,62658,76208,15816,1804,7734,28495,10853,340,1292,13496,15783,27083,521267
6,1020,115,5991295,2841102,881,3,1,36,35,19,50,14,3,3,5,1,9,69,2,12,3,7440096,
20539788,14297,2375,43887,3,1603,3,2124363,23029351,8163,4636,16436,12024,72021,
22622,15165,8181,33256,16174,21672,6752,155,2,2482,13503,7737,7041,2097,4600,328
,3217,4,1238,1766,1116,1831,3807,832,5,2827,10183,5684,1705,5633,688,2730,3,777,
4285,3,3015,5452,3068,546,6427,3548,965,171,210,13648,54,50,2163,2,9,4770,2110,1
,2,1632,12,4881,2381,1484,978,525,4,2767,692,5692,1109,1941,241,6850,1539,4176,7
97,377,5407,2434,4,455,1,4646,1449,2,4,1520,4,567,7114,3066,487,1836,2595,2,3,50
98,3006,251,594,1805,915,398,2016,2,531,484,1515,1481,1753,45,248,856,1500,3,128
9,2,2,3,273,2,353,435,388,41,228,1,1,1700,2,3,1409,2199,2719,5,249,2837,529,1155
,123,75,400,1,130,514,2,1107,202,194,488,18,608,1697,724,724,601,1097,1,32,1348,
102,156,1101,86,473,3,1,59,147,986,443,1,80,342,471,247,705,274,1609,563,805,317
,42,4,1,6,682,343,2,2442,29,122,159,1436,126,563,826,131,181,216,110,645,51,131,
2677,287,478,241,484,154,4,161,1308,8,1,1,4,1,4,678,3,570,959,752,468,596,84,44,
46,344,6,243,525,891,86,284,192,23,494,258,2,43,75,3,7,61,337,677,51,28,5,80,141
}

Downloads — azureuser@VM-01: ~ — ssh -i key2.pem azureuser@4.206.135.224 — 79x13
azureuser@VM-01:~$ curl http://apple.ca
<HTML>
<HEAD>
<TITLE>Document Has Moved</TITLE>
</HEAD>


<BODY BGCOLOR="white" FGCOLOR="black">
<H1>Document Has Moved</H1>
<HR>

<FONT FACE="Helvetica,Arial"><B>
Description: The document you requested has moved to a new location. The new l
ocation is "https://www.apple.com/ca/".
```

9) Monitor Network Traffic and Performance: Set up Azure Network Watcher to monitor network traffic, diagnose connectivity issues, and analyze network performance metrics. Use Azure Monitor to track network-related metrics and alerts.

i) monitored VM-01 to VM-02

[Home](#) > [Network Watcher](#)

 **Network Watcher | IP flow verify** ...

Microsoft

Search

Overview

Get started

Monitoring

- Topology
- Connection monitor
- Traffic Analytics

Network diagnostic tools

- IP flow verify**
- NSG diagnostics
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Logs

- Flow logs
- Migrate flow logs
- Diagnostic logs

Network Watcher IP flow verify checks if a packet is allowed or denied from a virtual machine based on 5-tuple information. The security group decision and the name of the rule that denied the packet will be returned. [Learn more.](#)

Specify a target virtual machine with associated network security groups, then run an inbound or outbound packet to see if access is allowed or denied.

Target resource

Virtual machine * ?

VM-01

Select virtual machine

Network interface *

vm-01589_z1

Packet details

Protocol

☒ TCP

☐ UDP

Direction

☒ Inbound

☐ Outbound

Local IP address * ?

10.0.1.4

Local port * ?

22

Remote IP address * ?


10.0.2.4

Remote port * ?

22

Verify IP flow

Results

 Access allowed

Security Rule	Network Security Group
AllowAnySSHInbound01	vm-01589_z1-nsg

ii) monitored that traffic is passing though NVA

[Home](#) > [Network Watcher](#)

Network Watcher | Next hop

Microsoft

× «

- Overview
- Get started
- Monitoring
 - Topology
 - Connection monitor
 - Traffic Analytics
- Network diagnostic tools
 - IP flow verify
 - NSG diagnostics
 - Next hop**
 - Effective security rules
 - VPN troubleshoot
 - Packet capture
 - Connection troubleshoot
- Metrics
 - Usage + quotas
- Logs
 - Flow logs
 - Migrate flow logs
 - Diagnostic logs

Next Hop provides the next hop from the target virtual machine to the destination IP address. [Learn more.](#)

Specify a target virtual machine and destination IP address to view the next hop.

Subscription * ⓘ

Azure subscription 1

Resource group * ⓘ

Project-02

Virtual machine * ⓘ

VM-01

Network interface *

vm-01589_z1

Source IP address * ⓘ

10.0.1.4 ✓

Destination IP address * ⓘ

10.0.2.4 ✓

Next hop

Result

Next hop type

VirtualAppliance

IP address

10.0.3.4

Route table ID

/subscriptions/7640872c-7cea-4...

10) Documentation and Reporting: Document the networking setup, including VNet configuration, subnet definitions, NSG rules, and external/internal communication paths. Prepare a report summarizing the network architecture, security measures implemented, and performance considerations.

