SMITKUMAR KHOKHARIYA

Project 2: Azure Virtual Machine Networking Setup

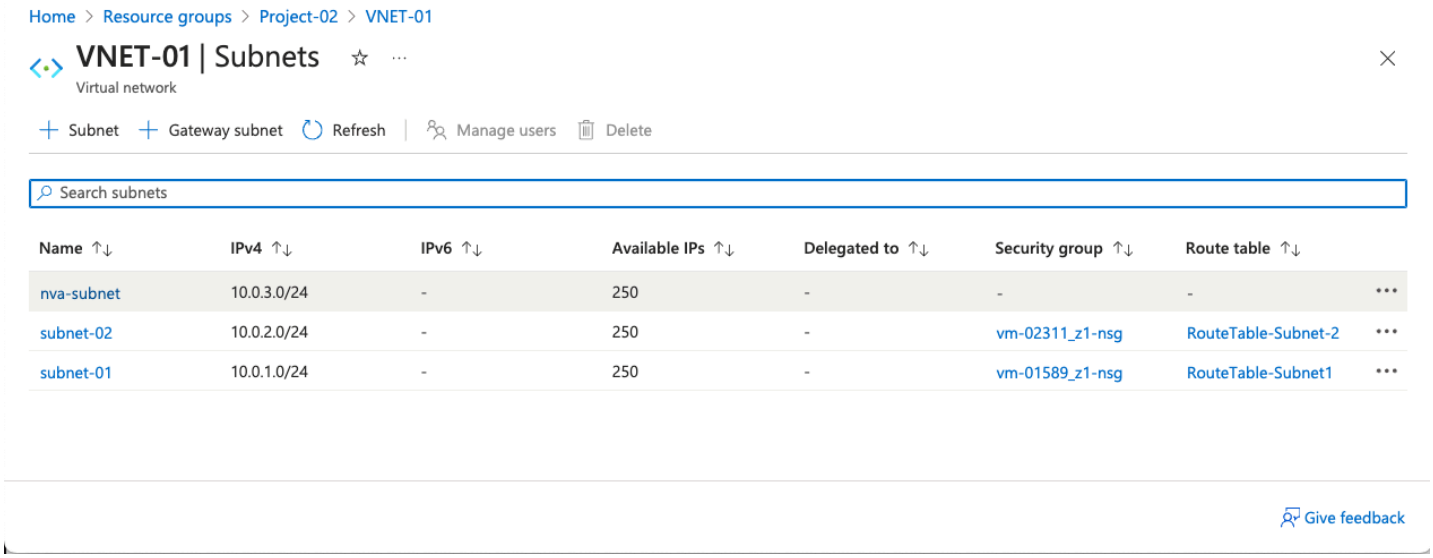
Objective: Configure networking for Azure Virtual Machines (VMs) to enable communication both within the virtual network and with external resources.

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.

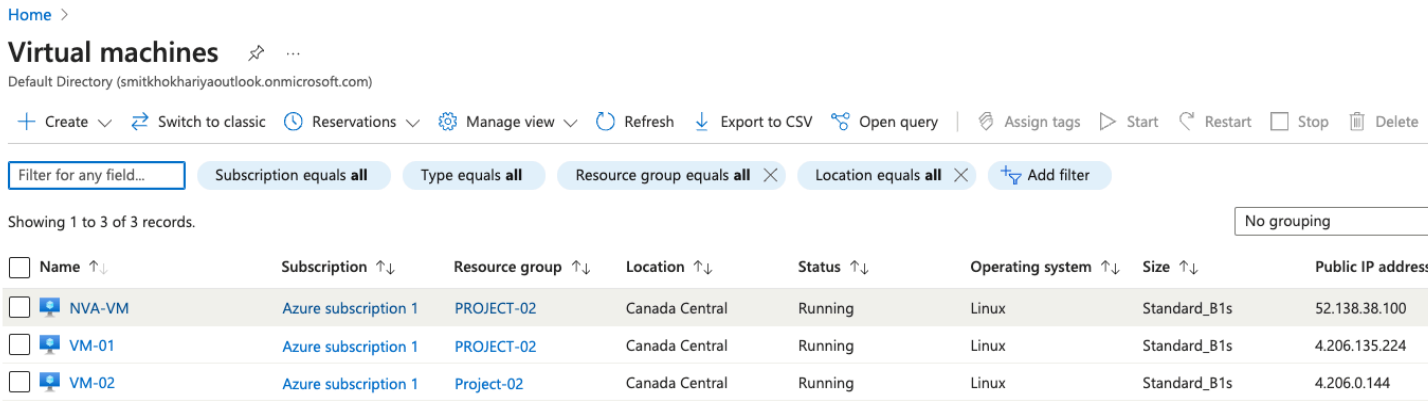
-> Here, I have created on Virtual Network named **VNET-01** with three subnet; **subnet-01** (10.0.1.0/24),
subnet-02(10.0.2.0/24),
subnet-nva(10.0.3.0/24)

in a **"Project-02"** resource group.



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**.



Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address
NVA-VM	Azure subscription 1	PROJECT-02	Canada Central	Running	Linux	Standard_B1s	52.138.38.100
VM-01	Azure subscription 1	PROJECT-02	Canada Central	Running	Linux	Standard_B1s	4.206.135.224
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.

Home > Virtual machines > VM-01 | Network settings >

vm-01589_z1-nsg

Network security group

Search

- 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

Move | Delete | Refresh | Give feedback

Essentials JSON View

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

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

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
120	AllowAnySSHInbou...	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

Home > Virtual machines > VM-02

VM-02 | Network settings

Virtual machine

Search

- 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

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

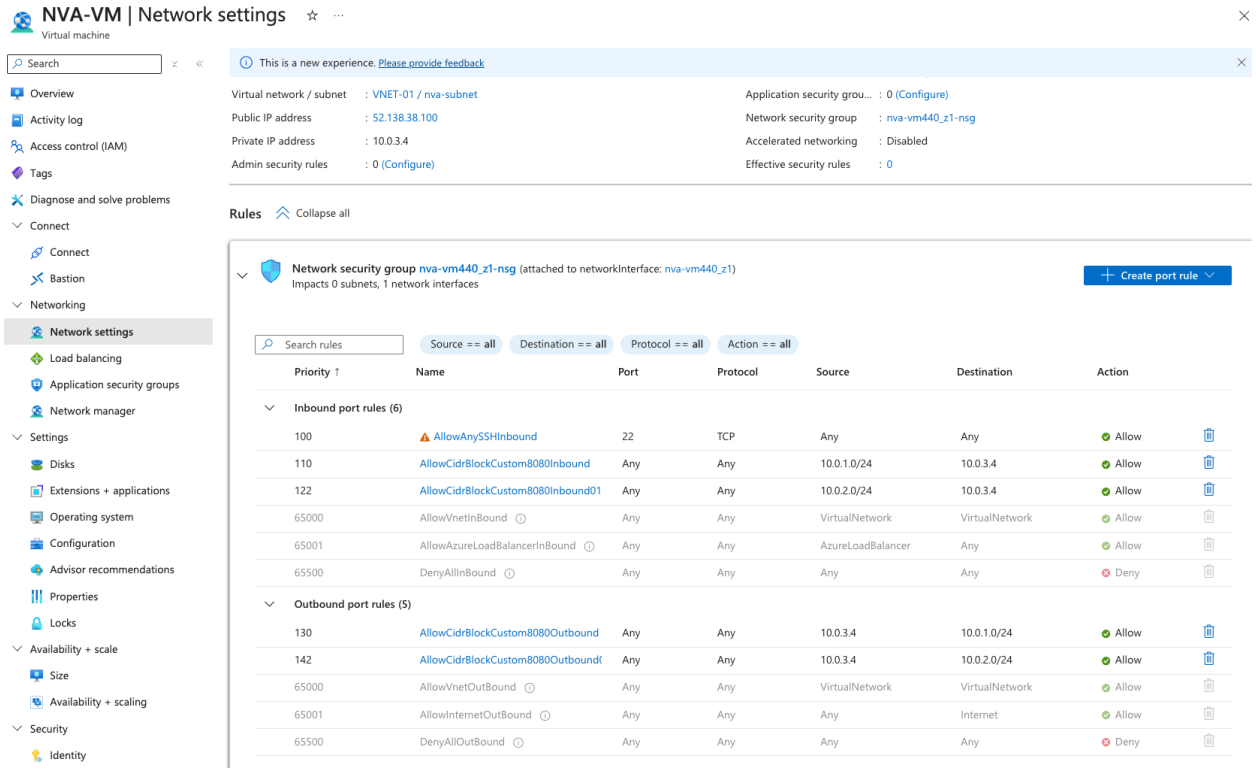
Create port rul

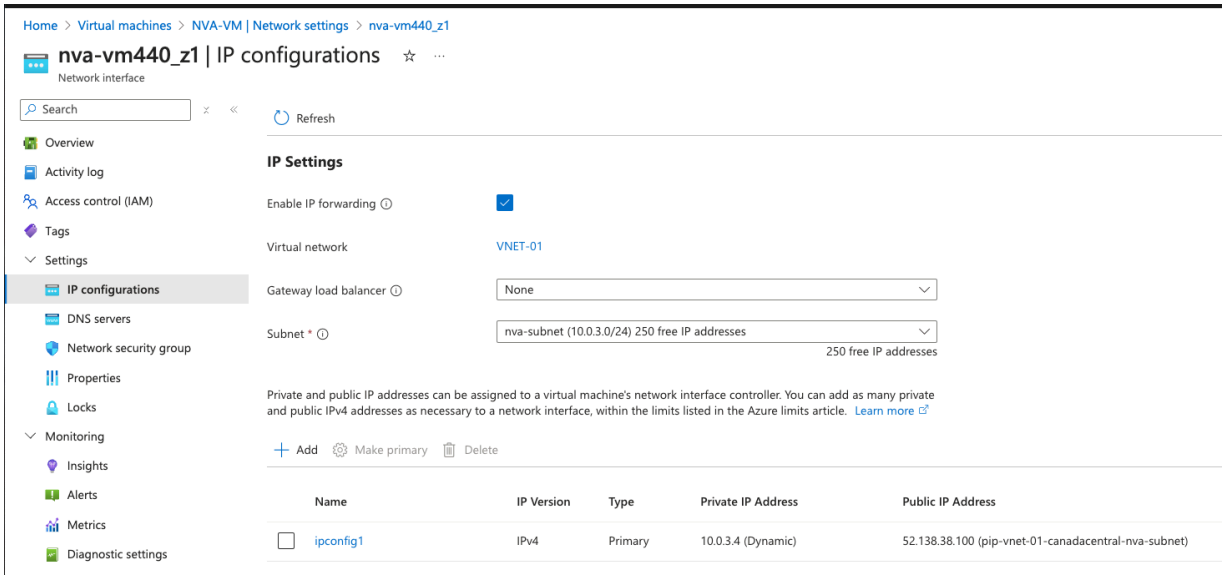
Search rules | Source == all | Destination == all | Protocol == all | Action == all

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.

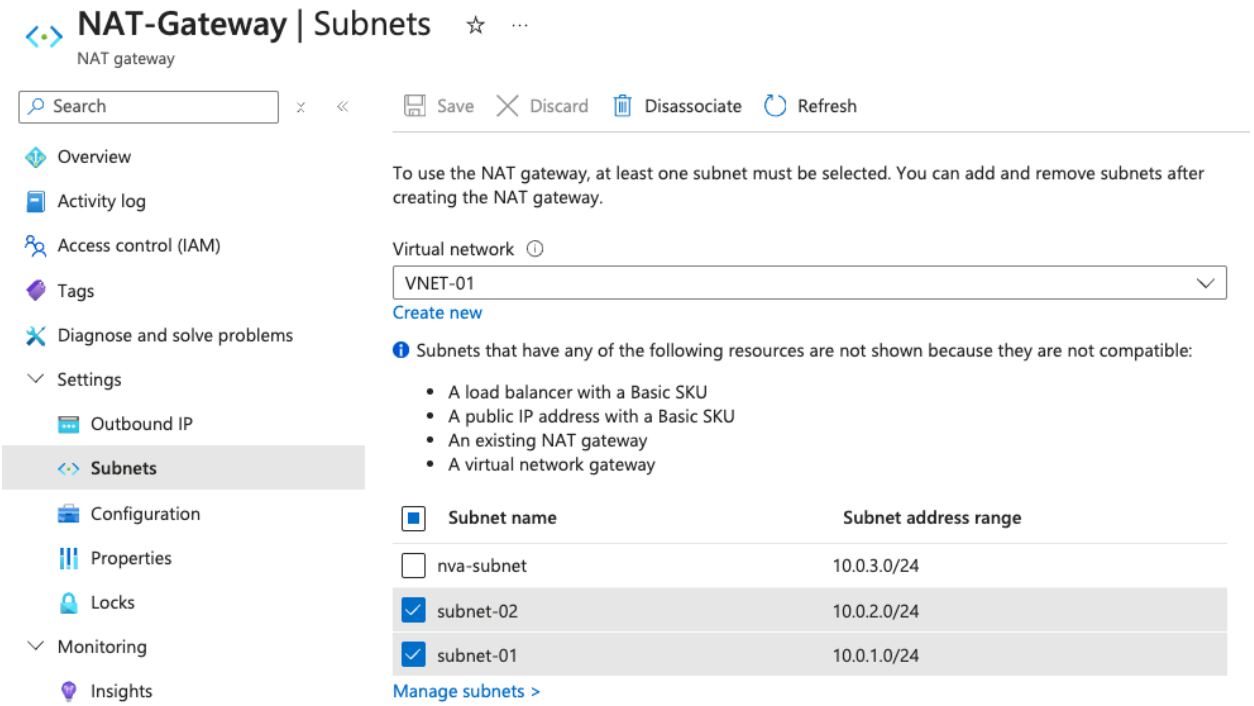
-> Deployed a NVA-VM as a **Network Virtual Appliances (NVAs),** configured to make it act as a NVM. Enable IP forwarding to forward incoming traffic to respective VM.

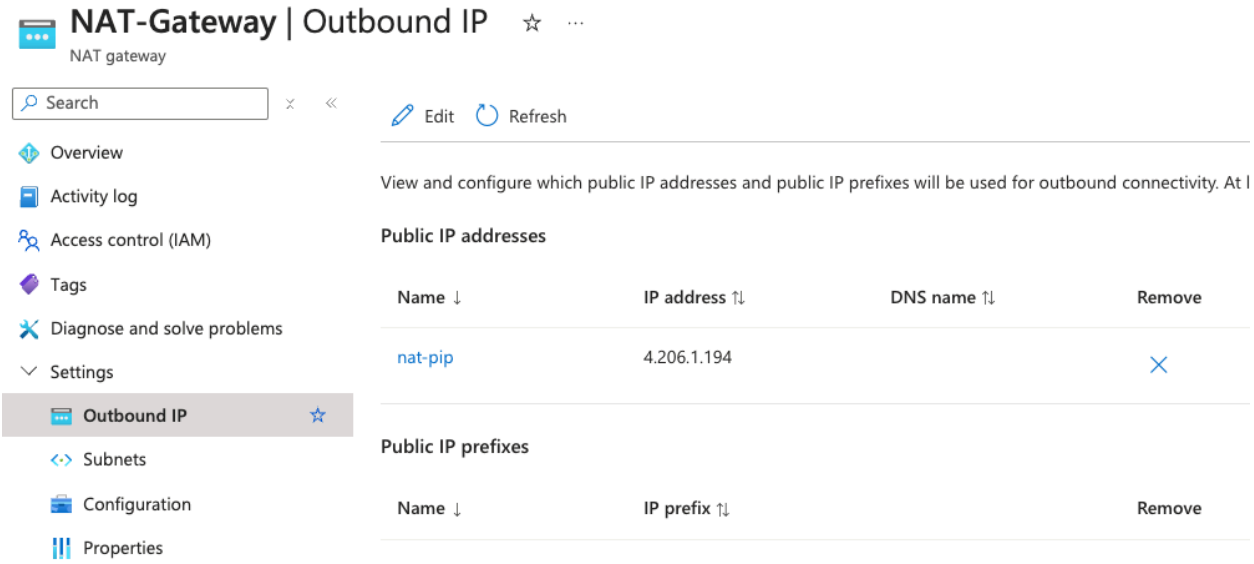




5) Set Up Network Address Translation (NAT) Gateway: Configure NAT Gateway to allow VMs within a private subnet to initiate outbound connections to the internet while keeping their private IP addresses hidden.

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





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

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Configuration
  - Routes
  - Subnets
  - Properties
  - Locks
- Monitoring
  - Alerts
- Automation
  - CLI / PS

Move | Delete | Refresh | Give feedback

Essentials JSON View

Resource group (move) : Project-02
Location : Canada Central
Subscription (move) : Azure subscription 1
Subscription ID : 7640872c-7cea-48ed-bc85-f6c700d4265a
Tags (edit) : Add tags

Associations : 1 subnet associations

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

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Configuration
  - Routes
  - Subnets
  - Properties
  - Locks
- Monitoring
  - Alerts
- Automation
  - CLI / PS

Move | Delete | Refresh | Give feedback

Essentials JSON View

Resource group (move) : Project-02
Location : Canada Central
Subscription (move) : Azure subscription 1
Subscription ID : 7640872c-7cea-48ed-bc85-f6c700d4265a
Tags (edit) : Add tags

Associations : 1 subnet associations

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 — 71×13
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 — 80×13
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 — 79×13
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 — 92×23
azureuser@VM-02:~$ curl ifconfig.me
azureuser@VM-02:~$ curl ifconfig.me
4.206.1.194azureuser@VM-02:~$
```

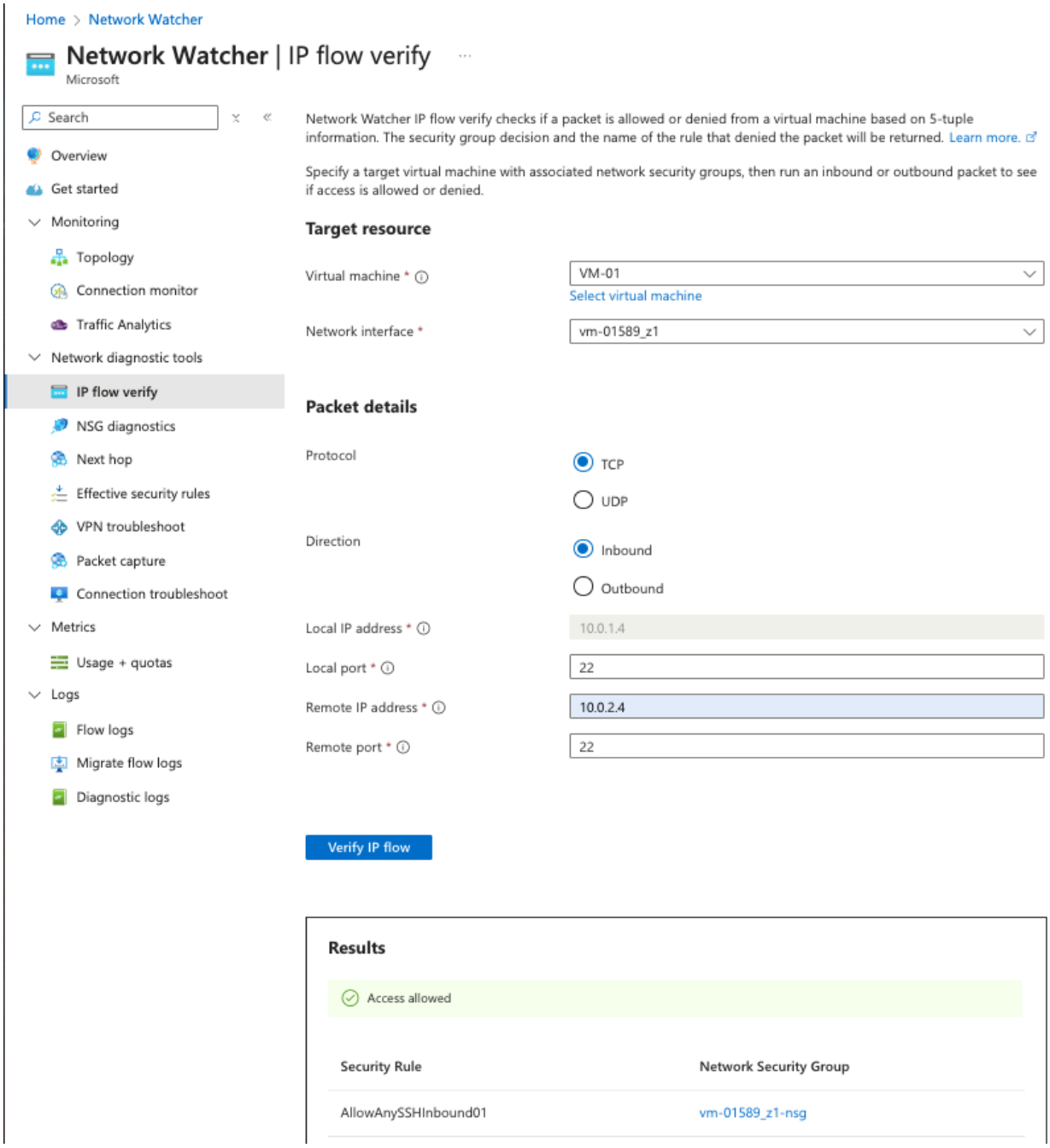
```
Downloads — azureuser@VM-01: ~ — ssh -i key2.pem azureuser@4.206.135.224 — 85×13
azureuser@VM-01:~$ curl ifconfig.me
azureuser@VM-01:~$ curl ifconfig.me
4.206.1.194azureuser@VM-01:~$
```

```
Downloads — azureuser@VM-02: ~ — ssh -i key2.pem azureuser@4.206.0.144 — 80×26
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
6,1020,115,5991295,2841102,881,3,1,36,35,19,50,14,3,3,3,5,1,9,69,2,12,3,7440096,
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
9,2,2,3,273,2,353,435,388,41,228,1,1,1700,2,3,1409,2199,2719,5,249,2837,529,1159
,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
```

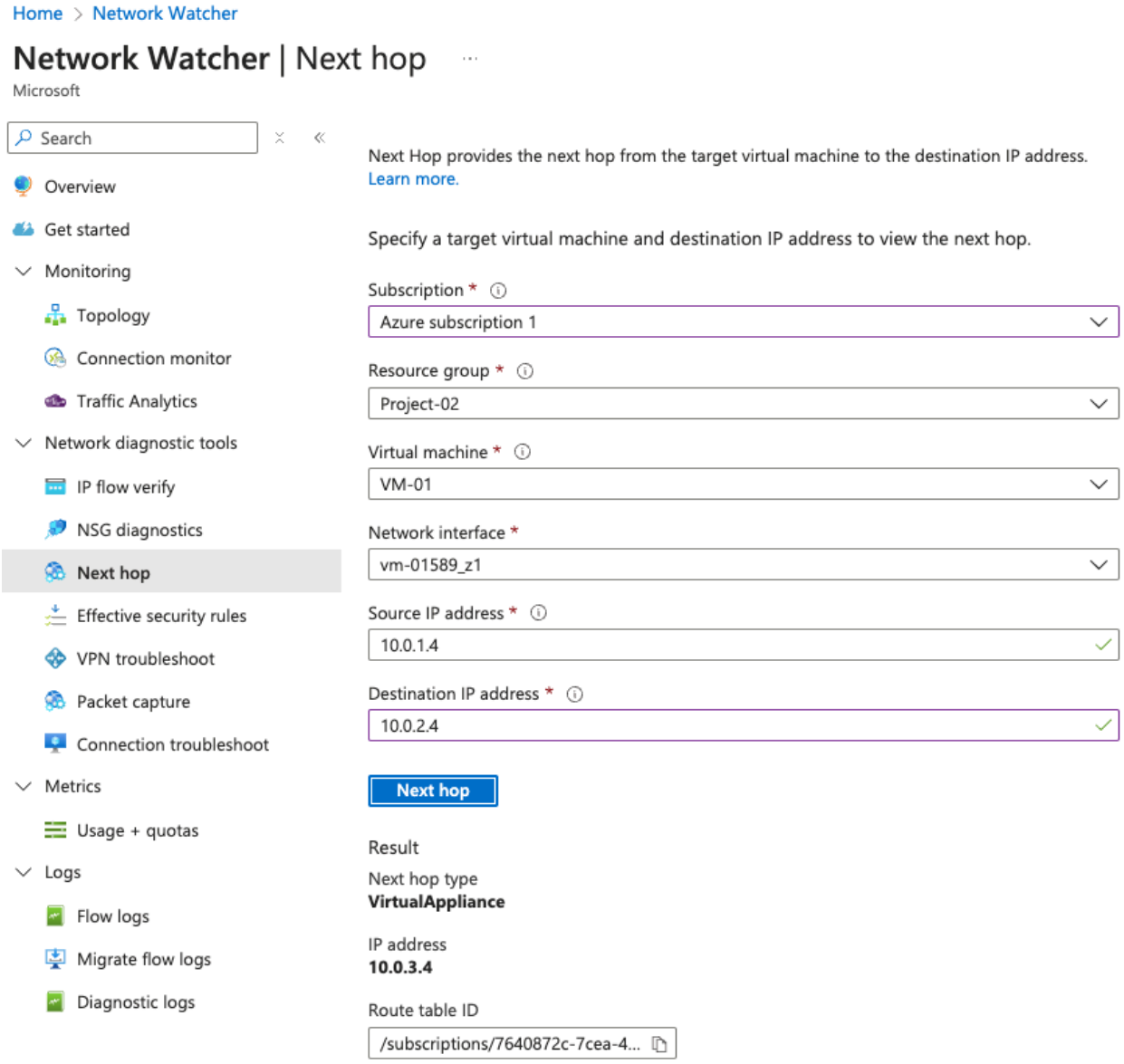
```
Downloads — azureuser@VM-01: ~ — ssh -i key2.pem azureuser@4.206.135.224 — 79×13
azureuser@VM-01:~$ curl http://apple.ca
<HTML>
<HEAD>
<TITLE>Document Has Moved</TITLE>
</HEAD>

<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



ii) monitored that traffic is passing though NVA



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.