Azure Virtual Networks

(IAAS)

Hosting isolated network on the cloud.

Network interface is a hardware device in each machine, all your data will go through the network interface.

Network interface gets an IP address.

* Each virtual machine will have 1 virtual Network interface.

Private IP address :- Internal communication within the network

Public IP address :- External communication (Internet) with the network.

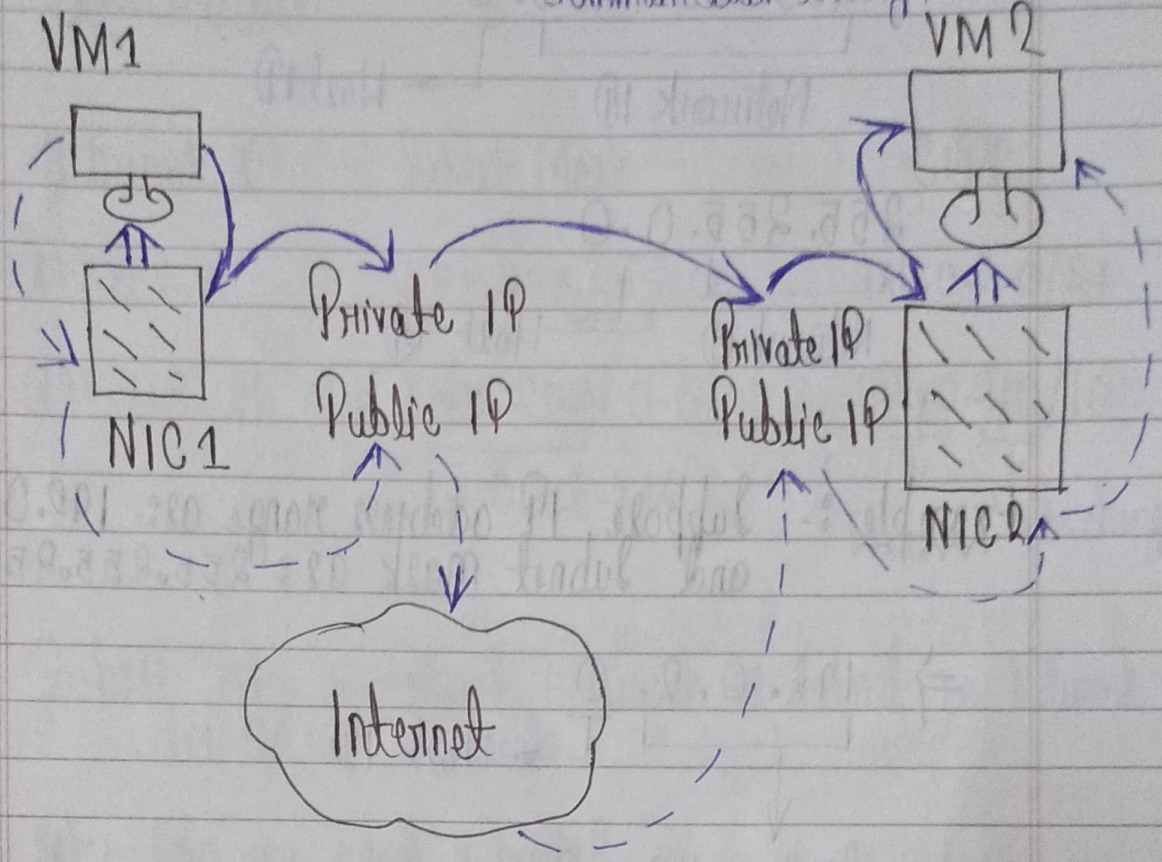
Private IP address number will depend upon subnet but public IP address is independent of subnet.

Que:- You dont want internet exposure for the VM.
Disable the public IP address

Teacher's Signature .....

——— Communication within Same Network

- - - - Communication through internet



Address Space

192.0.2.1 → Human Readable IP address

11000000.00000000.00000010.00000001 32 bit formal

* Subnet mask indicate what portion of an IP address represent network ID and what portion can represent host (device) ID.

Teacher's Signature

→ First 3 Octet will represent network and will be fixed

255. 255. 255. 0
Network ID | Host ID

255. 255. 0. 0
Network ID | Host ID

Example :- Suppose, IP address range as:- 192.0.2.0
and Subnet mask as: 255.255.255.0

⇒ 192. 0. 2. 0
Network ID | Host ID

⇒ Allowed device = 256 but usable IP = 254
because

⇒ IP address of one device connected to network can be:

192.0.2.0 → Network ID
192.0.2.1
192.0.2.2
192.0.2.3
:
192.0.2.255 → Broadcast ID

Teacher's Signature

CIDR Notation

Network ID	Subnet Mask	CIDR
192.0.2.0	255.255.255.0	192.0.2.0/24
192.0.2.0	255.255.0.0 (2 Octet ⇒ 16)	192.0.2.0/16 ⇒ (192.0 ↓ Fixed; 2.0 ↓ Can be changed.)

* Subset of a virtual network is subnet i.e Network is divided in subnets

Q:- Why do we need subnets?

You can create multiple subnets in a network and can use these subnets as group.

Ex:- 1 subnet for web servers
1 subnet for Database
1 subnet for Users VM

and it also allow you to apply policy at these subnets (Security)

Teacher's Signature .....

Enroll
Page No:
Date: / /

Create Virtual Network

All Resources → Virtual Network → Create

* If you wish to deploy a VM to a VN, ~~it nee~~ they both need to be part of same location. i.e Region

Static and Dynamic IP

Dynamic IP ⇒ Will change after restart of VM

Static IP ⇒ Will remains same even after VM.

* You can attach static IP to BOTH private and public IP

★ You can also attach secondary Network interface to virtual Machines. → Enhance security

Network Interface 1 ⇒ Private / Public IP

Network interface 2 ⇒ Private IP → Internal Communication

Teacher's Signature .....

Enroll

Page No:

Date: / /

Network Security Group

- Provide basic firewall feature to Azure VM
- Filter Traffic

Inbound Traffic ⇒ Traffic coming to Virtual Machine

Outbound Traffic ⇒ Traffic going out from V.M

* NSG can be applied to Network interface, or Subnet : you can't apply NSG to ~~Virtual~~ entire Virtual Network.

Q:- How to get public IP assigned to my PC/VM?
↳ Search What is MY IP in Google

- Source :- From where you want traffic
  Use "IP Addresses". If want to restrict traffic from your ~~VM~~ Laptop only.
- Destination :- Where you want to send traffic, use private IP address of VM.

Q:- A NSG is attached to 3 subnet and 2 NIC, You want to send all request coming from internet to a specific NIC.

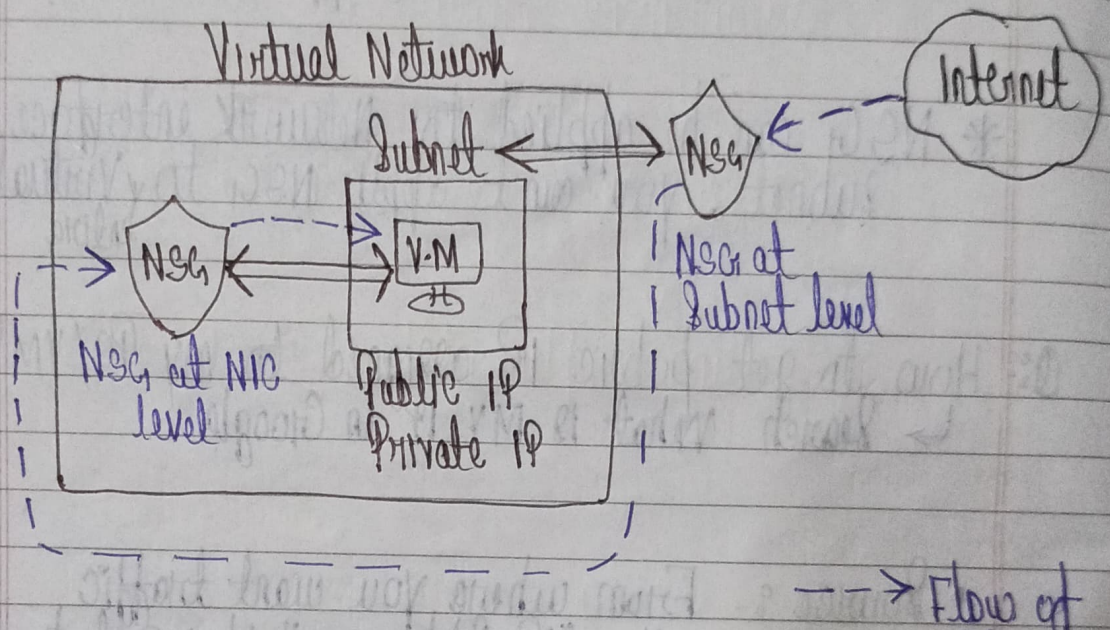
⇒ Create ~~one~~ NSG rules for port 443 and 80 with destination as NIC, where you wish to send.

Teacher's Signature .....

Que:- Configure a NSG rule which allow all VM, whose IP address is in form of 192.168.1.....

Que:- Can You have multiple NSG for 1 VM?

For 1 VM, NSG can exist at 2 levels i.e Subnet level and VM level.



- Incoming/Outgoing traffic will be first validated at Subnet NSG and then at NIC NSG in AND gate format
- Can a VM exist without a NSG?
  Yes.

Teacher's Signature

Enroll

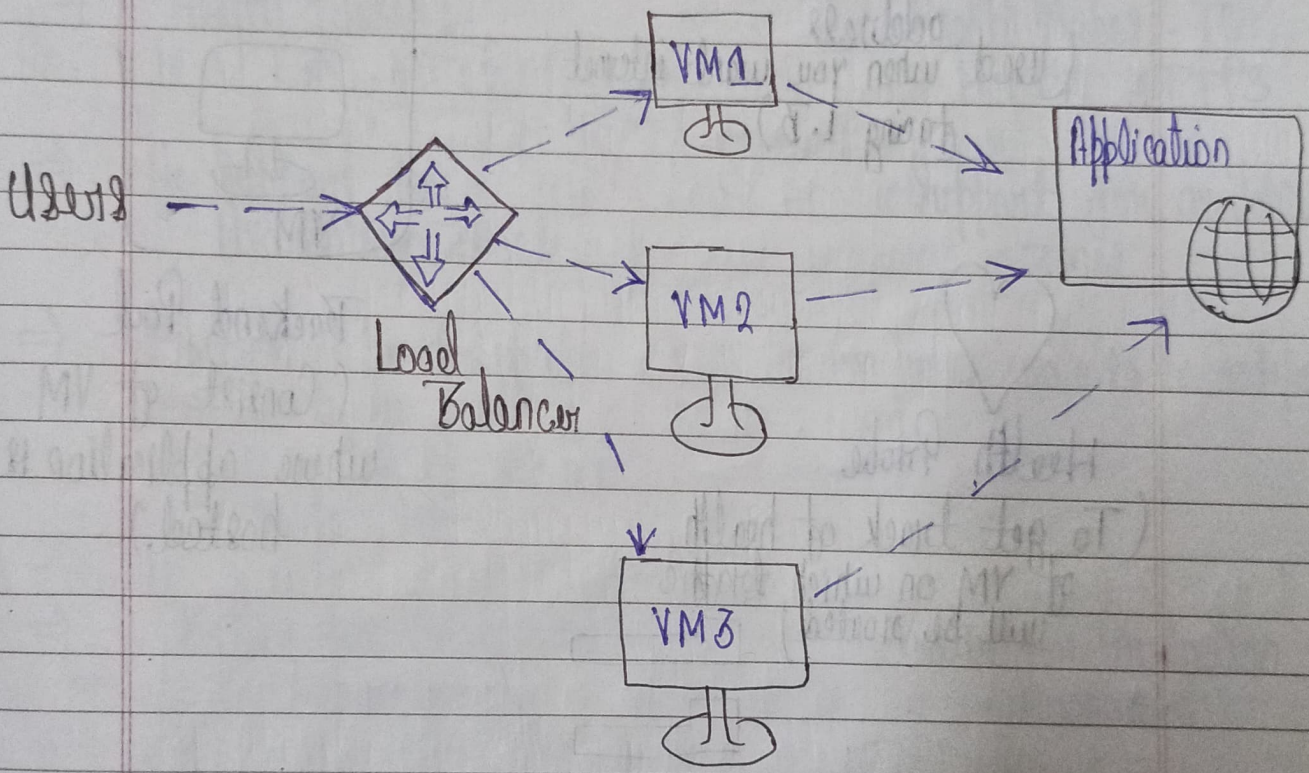
Page No:

Date: / /

Azure Load Balancer

- Traffic distribution Model

Generally, any real world application is hosted on multiple servers, to ensure better performance and high availability. Now, to distribute incoming traffic evenly on these servers, we use load balancer.

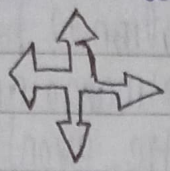


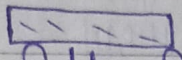
Q:- Difference in Internet facing Load Balancer and Non-Internet facing Load Balancer.

Teacher's Signature .....

Components of Load balancer

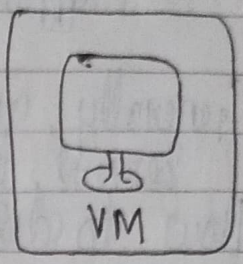
Load Balancer

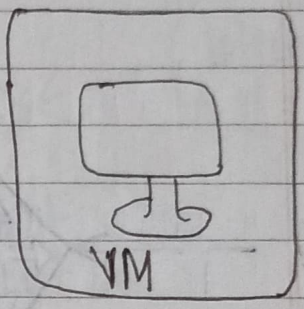




Public IP address

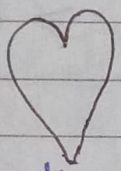
(used when you want internet facing L.B)





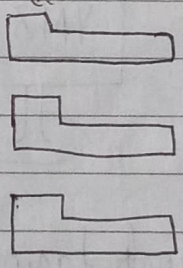
Backend Pool

(Consist of VM where application is hosted.)



Health Probe

(To get track of health of VM on which traffic will be routed)



Load Balancing Rule

(How to distribute traffic)

Enroll

Page No:

Date: / /

Basic Load Balancer	Standard Load Balancer
⇒ Free	Charge per hour
⇒ No SLA	99.99% SLA
⇒ Health Probes:- TCP, HTTP	Health Probes:- TCP, HTTP, HTTPS
⇒ No support for Availability Zones	Support for availability Zones
⇒ Machine in backend pool need to be part of an availability set or scale set	Machines can also be independent.
⇒ Better for Development environment	Better for Production environment

* Virtual machines in load balancer must be part of same virtual network.

Teacher's Signature .....

Basic Load Balancer

* Machines in backend pool must be part of either an availability set or scale set.

* For a basic load Balancer → You can use basic Public IP address.
  For a standard load balancer → You need standard public IP address

* If you are using internet facing Load balancer, all your incoming traffic will pass through load balancer; Load balancer can internally distribute traffic using private IP of VMs in backend pool.
  So, you don't need public IP of VM's in backend pool, unless you don't want to login there.

Que: Create a basic and standard load balancer with 3 VM

* Based on health Probe configuration, Load balancer will initiate a handshake with VMs periodically to ensure VMs are in good state

Que: You have a load balancer and 3 VMs in its pool. those VMs have no public IP associated with it. How you will do RDP or access other services such as MSSQL on those VMs?

Teacher's Signature

NAT ⇒ Network Address Translation

Enroll

Page No:

Date: / /

Generally VM in load balancer pools doesn't have public IP. To use services on those VM, we can use two ways:-

I ⇒ Associate a public IP and use it for services such as RDP ⟶ Will expose the VM to internet.

II ⇒ Use a NAT rule in Load balancer to allow specific service or port.

Load Balancer ⟶ Select Load Balancer

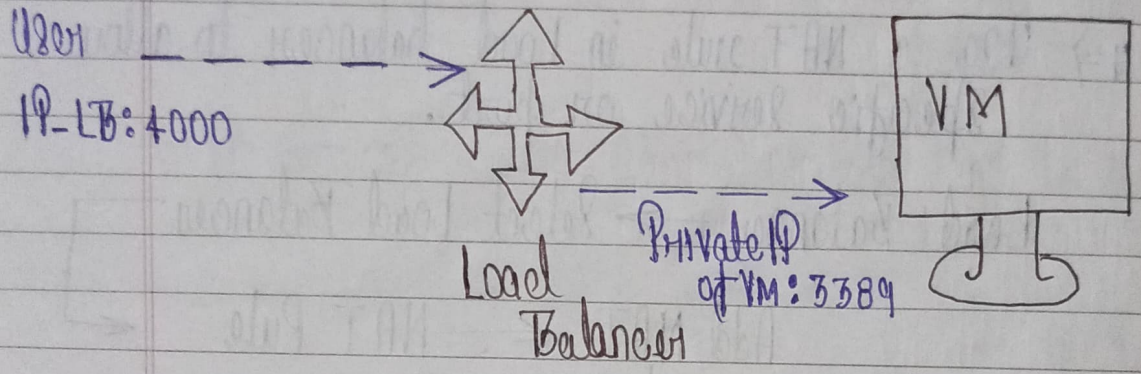
Add NAT rule ⟵ NAT Rule

- Port ⟶ Port of Load balancer, traffic coming to this port will be forwarded to VM configured service.
- Target VM
- Port Mapping
- Target Port ⟶ Port of VM

Teacher's Signature .....

Ex:- NAT rule with below config:-

Port = 4000
Target VM = load VM1
Port Mapping = Custom
Target Port = 3389



How to connect using rule:-

Open RDP → Provide ~~NS~~ LB public IP:port number

- You can create multiple NAT for multiple VM, multiple services
- You can also add VM scale set to a load balancer by using "Add backend Pool" option
- Even if you are using load balancer, you will need rules to allow/deny traffic in NSG.
- If an instance is added to scale set, it will be automatically added to backend pool of Load Balancer automatically

Teacher's Signature

Enroll

Page No:

Date: / /

To dissociate an Public IP

VM → Select VM → Networking → Network Interface → IP Configuration → Dissociate

Que:- You have a secure server using HTTPS method, which load balancer is well suited?

Since standard load balancer support HTTPS health probe, you should use standard load balancer in above case.

Using standard load balancer skill, if your VMs are serving different purposes, you can create multiple backend pool in one load balancer.

You have 4 VM, serving some purpose in load balancer, How will you login to machine using RDP.

1⇒ Add NAT rule with different port but same target port (3389) and connect to RDP using PIP of LB : Port

eg:- 192.168.32.5 : 4000
192.168.32.5 : 4001
:
192.168.32.5 : 4003

Difficult to maintain and remember port number to different VM

Teacher's Signature .....

Better Solution

Use different frontend IP address while designing different NAT and keep the ports as same.

* By default, Load balancer blocks all outbound ports (Traffic coming out of VM), as a result; you won't be able to access internet.
  To access internet or allow outbound traffic, you have to add outbound rule in Load balancer.