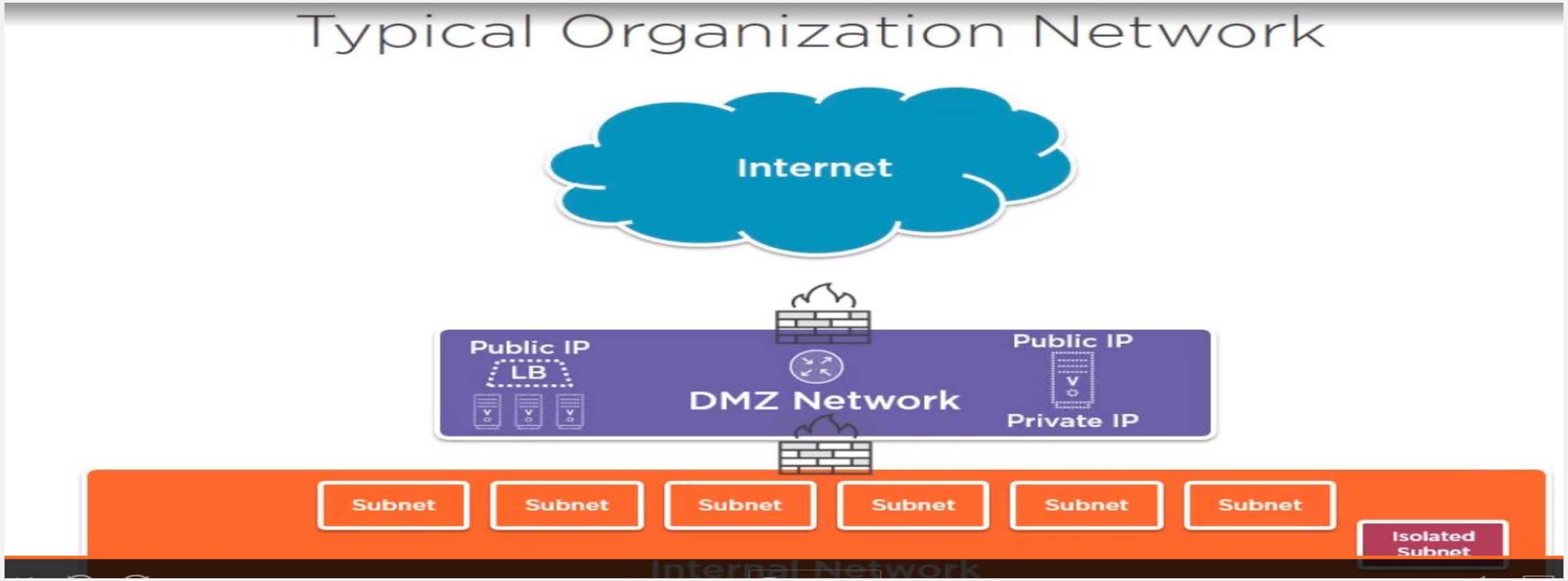
AZURE NETWORKING

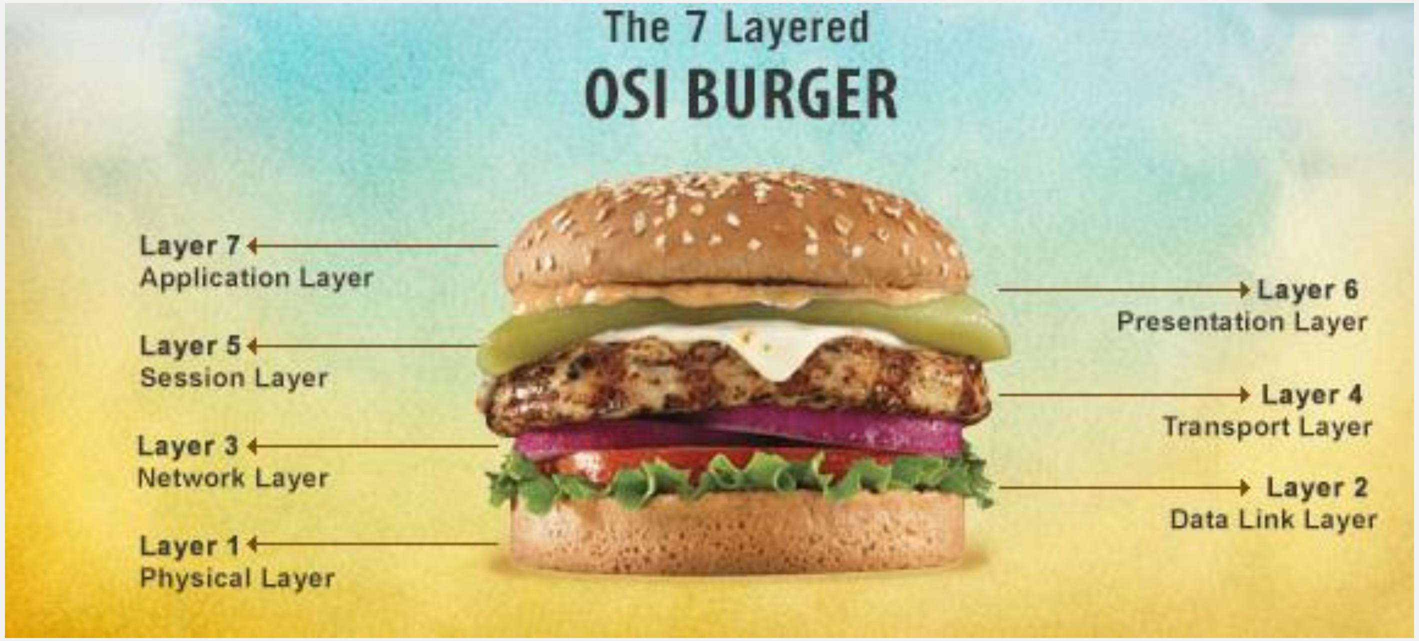
Networking Fundamentals

Networking provides communication between systems.

- Communication can be broken down into 3 broad types
  - In one location probably one subnet
  - Between location probably by using a Secured tunnel
  - Over internet



The OSI Model



All People Seem To Need Data Processing

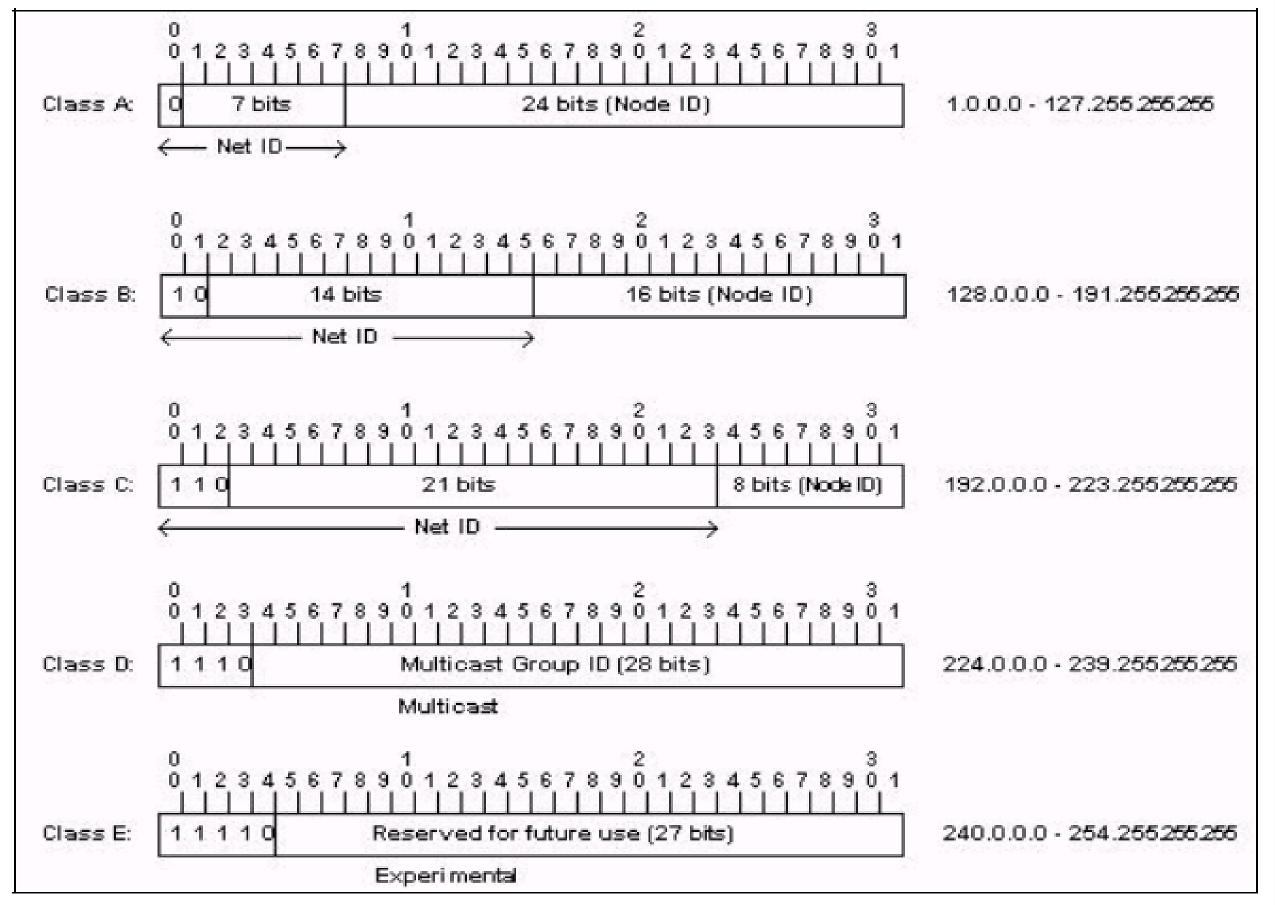
1. Layer 7 - Application Layer – Application and User Communication happens
2. Layer 6 - Presentation Layer – The Data is changed into an acceptable format ,Encrypt Decrypt also happens at this layer.
3. Layer 5 - Session Layer - Session layer is responsible for creating and maintaining sessions between OS.
4. Layer 4 - Transport Layer - TCP UDP protocols run here ,responsible for transfer of data between end systems.
5. Layer 3 - Network Layer - Routers operate on this layer ,routers forward packets of information between computers, this is where IP address comes in.
6. Layer 2 - Data link layer - this is where switches operate and provide a reliable link between two directly connected nodes. (MAC Address and Switches)
7. Layer 1 - Physical hardware that makes up the network
   - Define physical specs
   - Define protocols
   - Define transmission mode
   - Define network topology

IP V4 Addressing

- Network communication for a computer is directed to the IPv4 address of that computer, hence each networked computer should have a unique IPv4 address.

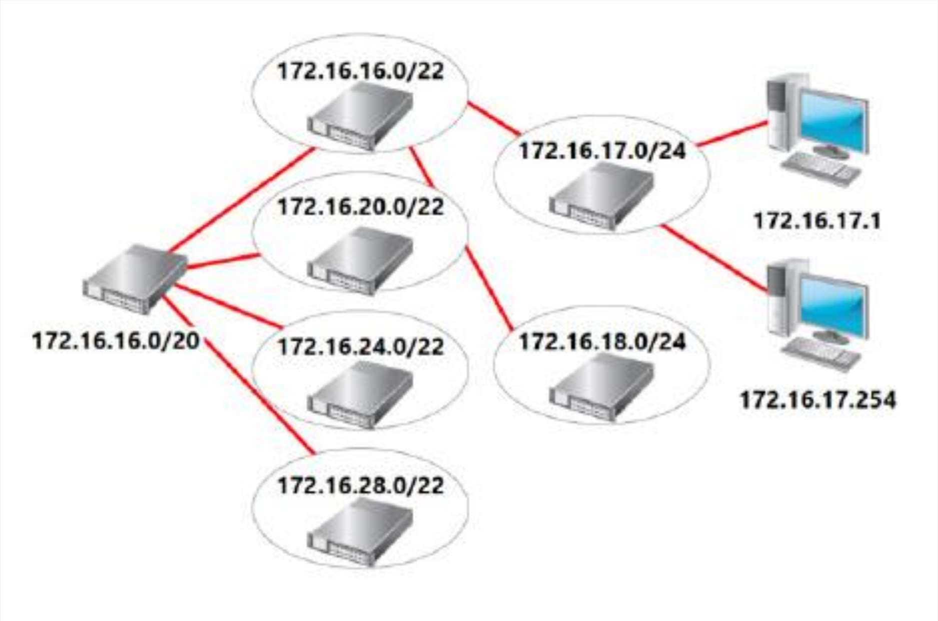
IP Address	172	16	0	10

- The address is made up of 32 binary bits which can be divisible into a network portion and host portion with the help of a subnet mask.
- 32 binary bits are broken into four octets (1 octet = 8 bits)
- IP Address Classes



- The IP Addresses understood by the computer are in Binary format.

IP V4 Addressing contd



- This is called CIDR(Classless Interdomain Routing) e.g.172.16.0.0/20 =

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

11111111	.11111111.	11110000.	00000000
255	255	240	0

LAB – Private range IP address 172.10.60.16/29 Find usable address range.

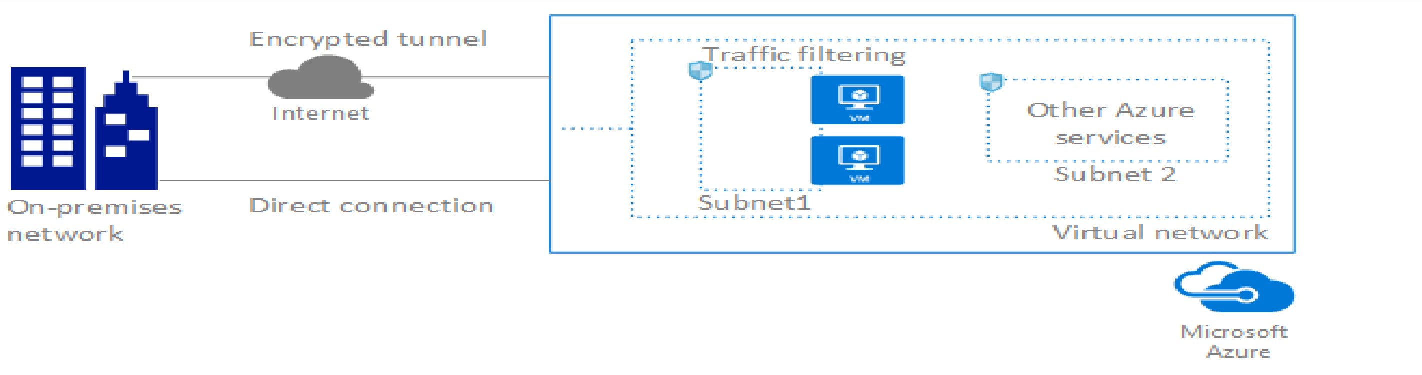
Azure Networking

- Azure provides a variety of networking capabilities which enable it to be used together or separately.
- Each Vnet is isolated from each other ,in each Vnet one can assign.
  - Peering Allows resources from different Vnets to connect to each other ,the bandwidth and latency of peering is same as if they were in the same vnet.
  - Enables resources connected to different Azure Vnets within different regions to communicate with each other. Traffic between the Vnets flows through the VPN gateway.
- Azure Virtual Data center - The vDC concept was born out of a necessity to support large scale cloud applications
- Consideration on implementing a Virtual Data center
  - Identity and Directory services
  - Connectivity with the local data center
  - Connectivity within the cloud
  - Security infrastructure

Azure Virtual Networks

A *virtual network* is a logically isolated network on Azure.
A virtual network is scoped to a single region; however, multiple virtual networks from different regions can be connected together using virtual network peering.

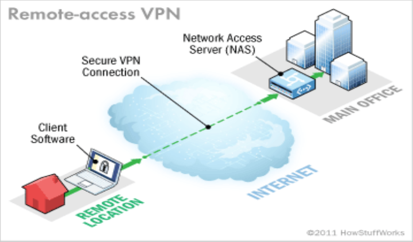
•Azure Virtual Network Service allows to securely connect Azure Resources to each other.
•A Vnet is a logical isolation of Azure cloud dedicated to own subscription.



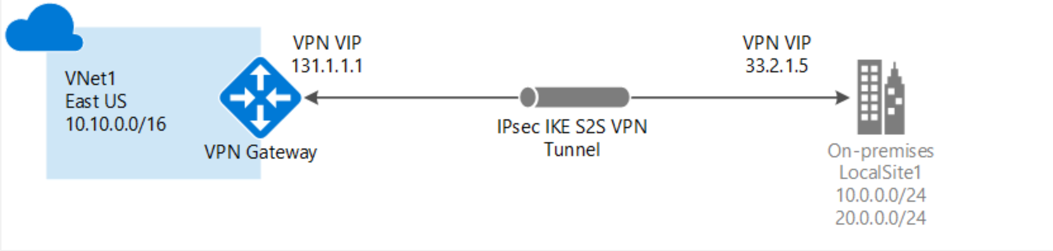
Some of the capabilities of Azure Vnets
•Isolation
•Hybrid Cloud Networking Architecture
•Internet Connectivity
•Azure resource connectivity
•Vnet Connectivity

Azure Virtual Networks contd..

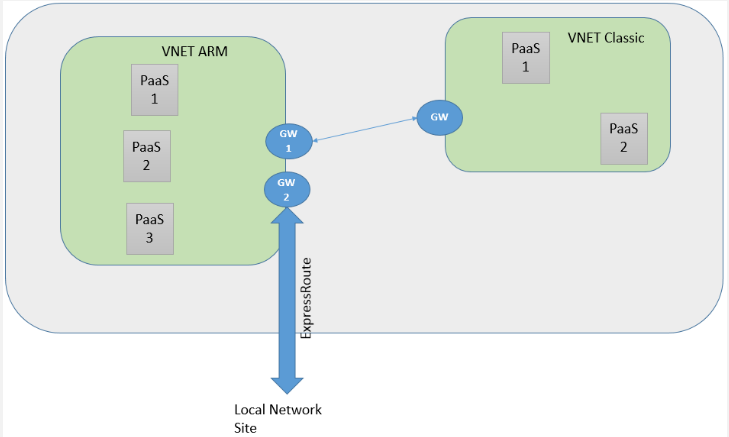
- Point to site VPN



- Site to Site VPN

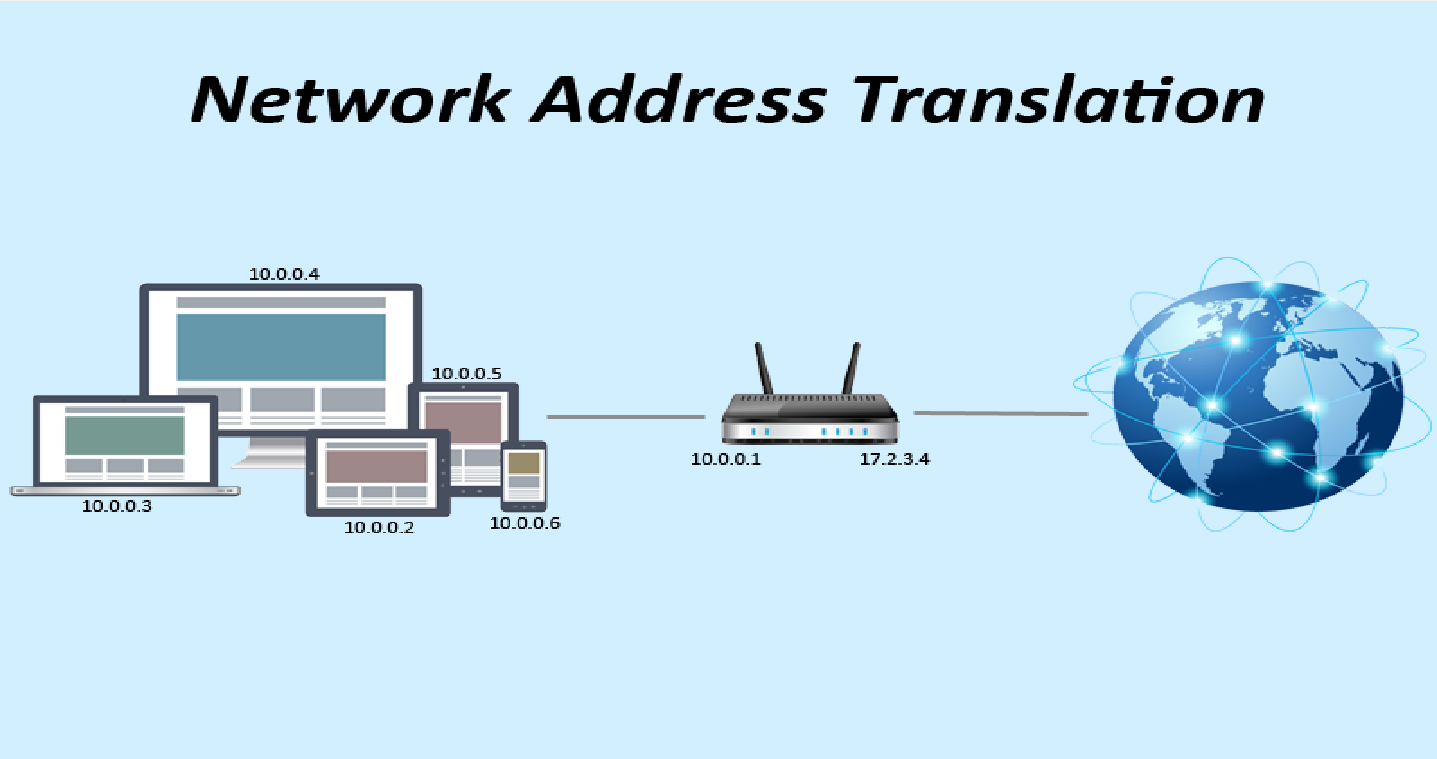


- EXPRESSROUTE



PUBLIC IP and NATTING

- Public IP addresses allow Internet resources to communicate inbound to Azure resources.
- Also enable Azure resources to communicate outbound to Internet and public-facing Azure services with an IP address assigned to the resource.
- In Azure Resource Manager, a public IP address is a resource that has its own properties.
- *Network Address Translation* (NAT) is the process where a network device, assigns a public address to a computer (or group of computers) inside a private network



Virtual Network Gateway

- A VPN gateway is a virtual network gateway which sends encrypted traffic across a public connection to an prem location.
- This may also be used to send traffic between Vnets in Azure over Microsoft network.
- A virtual network gateway is composed of two or more virtual machines which are setup when the Virtual network is created.
- When a Virtual network gateway is created it creates a VPN gateway ,this gateway encrypts traffic and can take upto 45 mins to create.
- The Gateway SKU determines how powerful the VM are.

SKU	S2S/Vnet to Vnet Tunnel	P2S Connection	Aggregate Throughput Benchmark
VpnGw1	Max 30	128	650 Mbps
VpnGw2	30	128	1 GBPS
VpnGw3	30	128	1.25 GBPS
Basic	10	128	100 Mbps
Generation2	VpnGw5AZ	Max. 128	10 Gbps

- Route Based and Policy Based VPN

Vnet Security

NSG

- Network traffic can be limited by using Network security groups.
- NSG contains a set of rules which allow or deny inbound or outbound traffic based on source or destination IP address
- NSG rules are applied in the following way
  - ✓ Inbound Traffic - By Default all traffic is blocked if an NSG is enabled.NSG at subnet level is evaluated first and then the nsg on network interface.
  - ✓ Outbound traffic - Vice versa the traffic is evaluated by NSG attached to the network interface and then by the NSG attached to the subnet.

Name	A unique name within the network security group
Priority	A number between 100 and 4096.Lower number have higher priority
Source or destination	The IP adress range or single ip address.
Protocol	TCP,UDP or any(ANY = TCP,UDP and ICMP)
Direction	Inbound outbound
Port Range	Specify numbers between 80 to 10000
Action	Allow or deny

Application Security Groups

- Application security group allows to create a set of rules which can then be applied to a group of virtual machines.
- This feature allows to reuse security policy at scale without need to maintain explicit IP addresses.

LAB – Create a Vnet and enable NSG

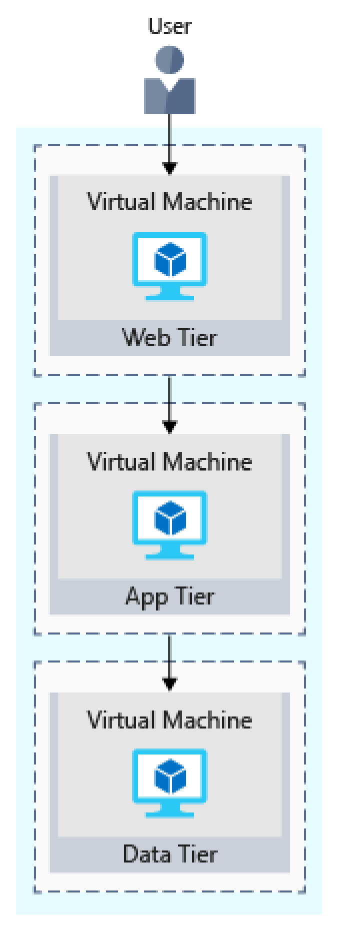
Study the default NSG

Enable port 80 from All

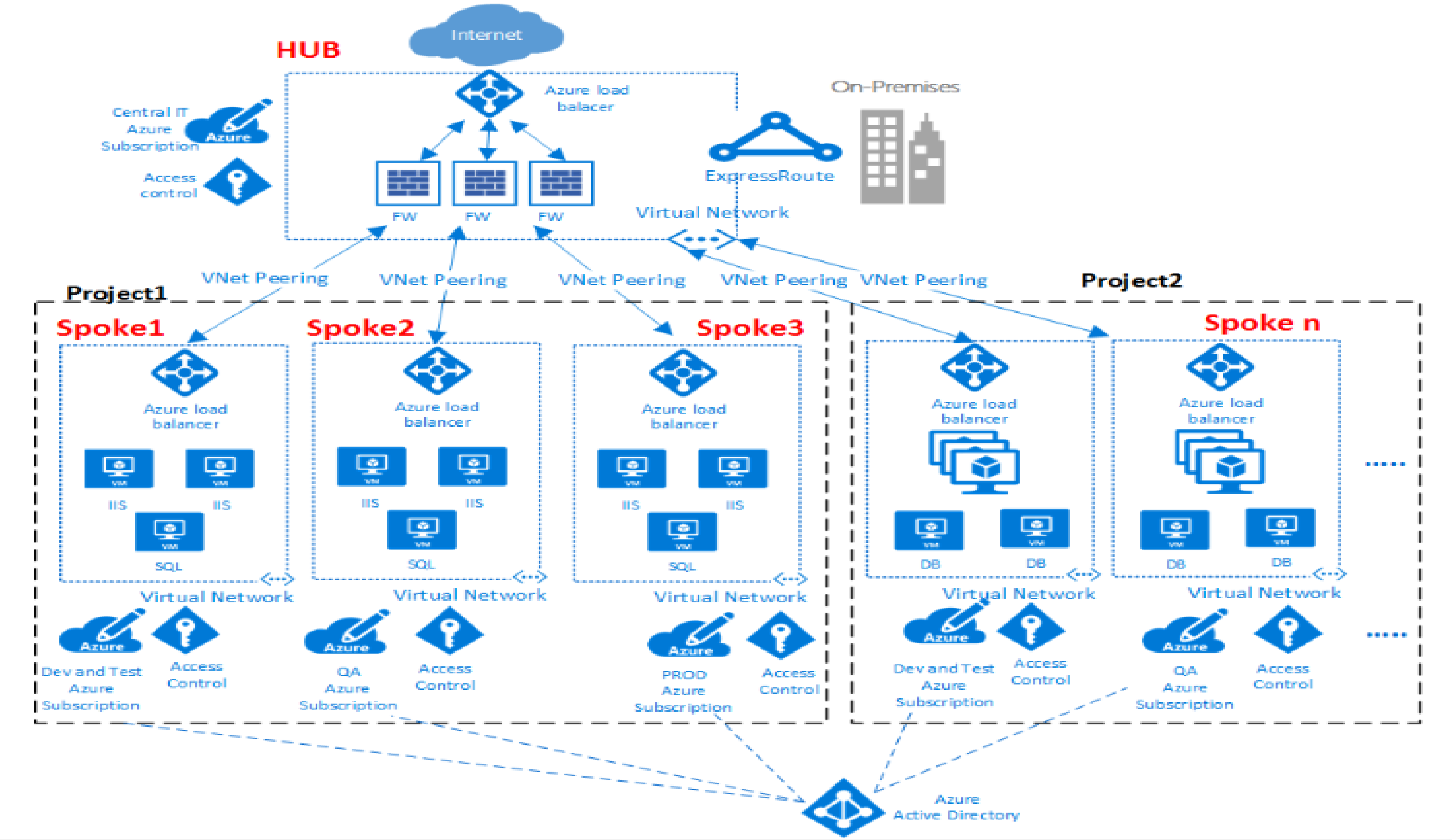
Using an N-tier architecture

An architectural pattern that can be used to build loosely coupled systems is *N-tier*.

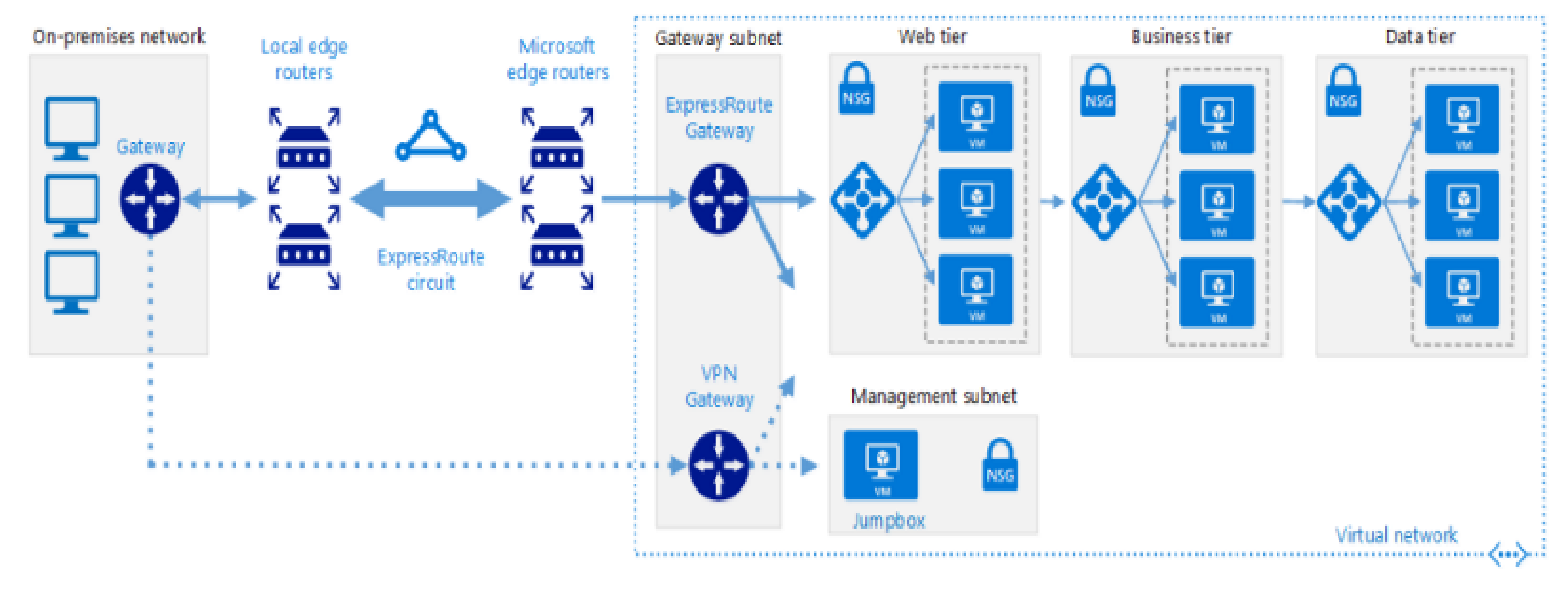
An N-tier architecture divides an application into two or more logical tiers. Architecturally, a higher tier can access services from a lower tier, but a lower tier should never access a higher tier.



- The **web tier** provides the web interface to your users through a browser.
- The **application tier** runs business logic.
- The **data tier** includes databases and other storage that hold product information and customer orders.


HUB
Internet
Azure load balacer
Central IT Azure Subscription
Azure
Access control
FW
FW
FW
On-Premises
ExpressRoute
Virtual Network
VNet Peering
VNet Peering
VNet Peering
VNet Peering
VNet Peering
Project1
Project2
Spoke1
Spoke2
Spoke3
Spoke n
Azure load balancer
Azure load balancer
Azure load balancer
Azure load balancer
Azure load balancer
VM
IIS
IIS
SQL
IIS
IIS
SQL
IIS
IIS
SQL
DB
DB
DB
DB
......
Virtual Network
Virtual Network
Virtual Network
Virtual Network
Virtual Network
Azure
Dev and Test Azure Subscription
Access Control
Azure
QA Azure Subscription
Access Control
Azure
PROD Azure Subscription
Access Control
Azure
Dev and Test Azure Subscription
Access Control
Azure
QA Azure Subscription
Access Control
......
Azure Active Directory

Highly Available Hybrid Architecture



Load Balancer

Uses of Load balancer

- Load balance incoming traffic to VM's called public load balancer
- Load balancer internal traffic across VM in a Vnet.
- Port forward traffic to specific ports on specific VM with inbound NAT.
- Provide outbound connectivity to VM inside Vnet by using public Load balancer.

Load balancer resources

- Front end IP configuration
- Backend IP address
- Load Balancing Rules
- Probes
- Inbound NAT rules.

Load Balancer Features

Load Balancing

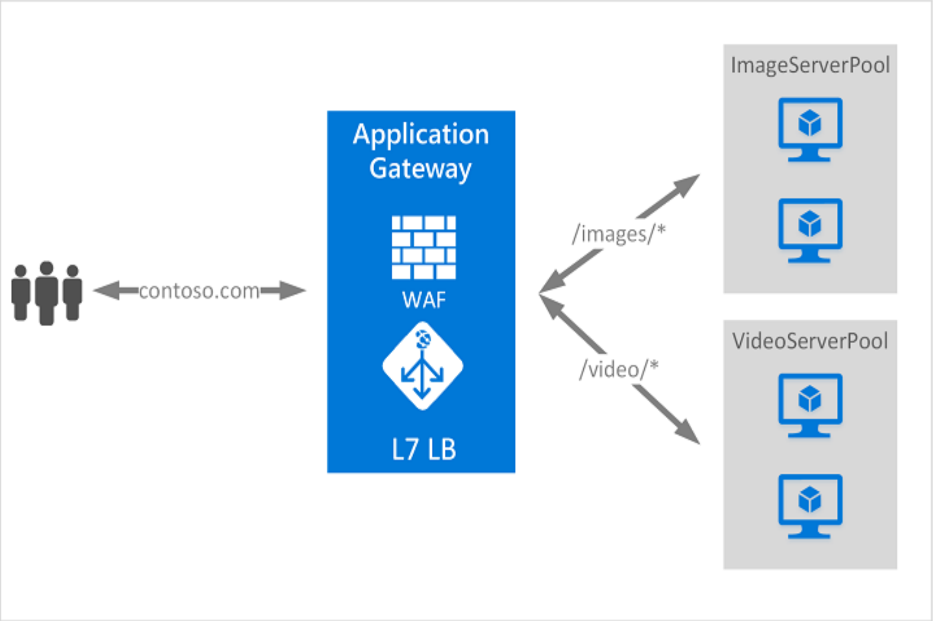
- With Azure load balancer uses a hash based algorithm for distribution of inbound flows and writes the headers of the of flows to backend pool.
- A server is available to receive a flow when the health probe indicates the endpoint is healthy.
- By default the LB uses 5 tuple hash rule to determine where it needs to send the traffic

  - ✓ Source IP
  - ✓ Source port
  - ✓ Destination IP
  - ✓ Destination Port
  - ✓ Protocol

Azure Application Gateway

If all your traffic is HTTP, a potentially better option is to use Azure Application Gateway. Application Gateway is a load balancer designed for web applications.

It uses Azure Load Balancer at the transport level (TCP) and applies sophisticated URL-based routing rules to support several advanced scenarios



This type of routing is known as application layer (OSI layer 7) load balancing since it understands the structure of the HTTP message.

Azure Traffic Manager

Azure traffic manager allows distribution of traffic for service endpoints in different datacenters.

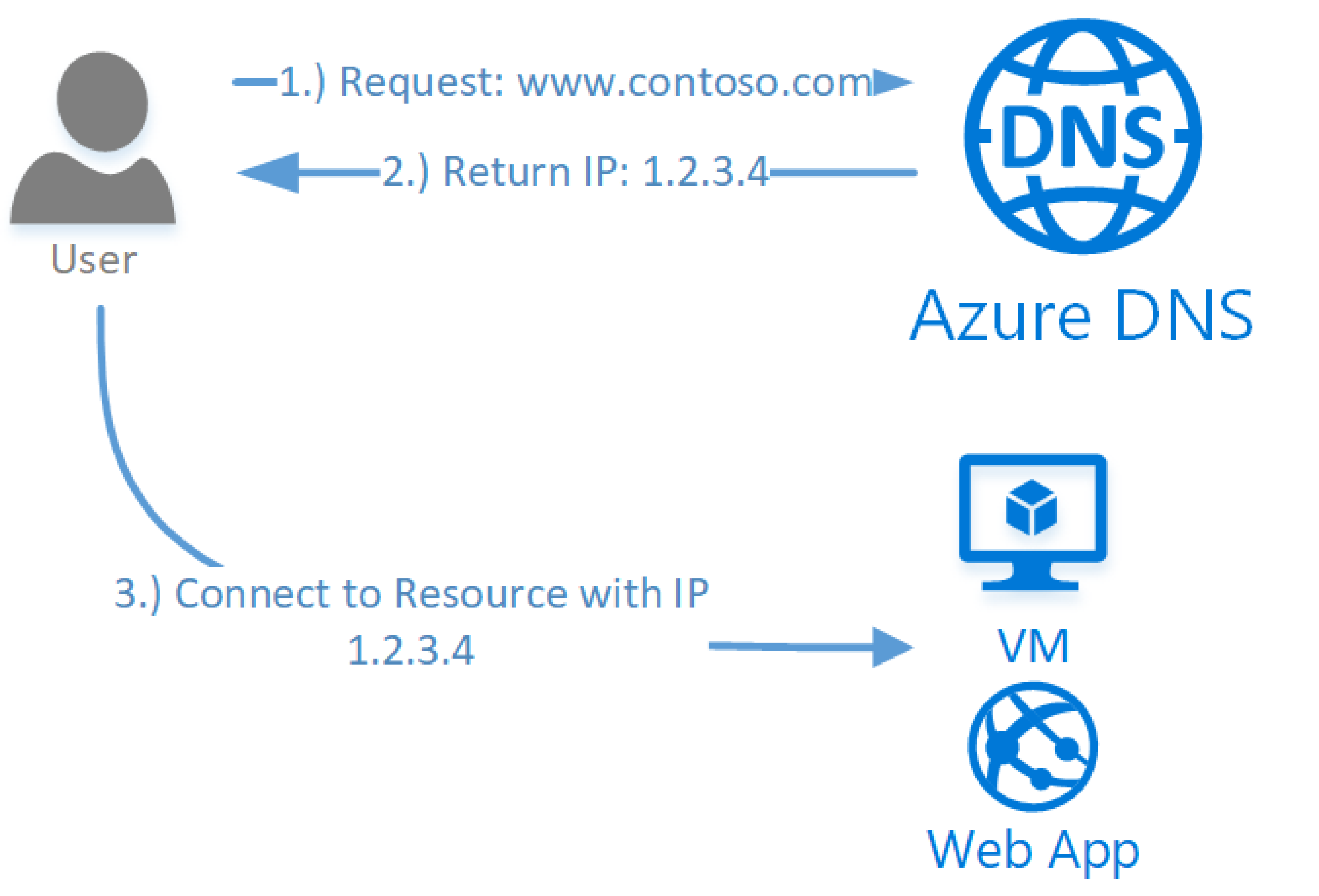
- Benefits of traffic manager.

✓ Improve availability of critical application by monitoring the endpoints and providing automatic failover.
✓ Improve responsiveness of high performance applications by directing the traffic to the endpoint with lowest network latency for the client.
✓ Perform service maintenance without downtime, perform planned maintenance on your application without a downtime, traffic manager directs traffic to alternative endpoints while maintenance is in progress.
✓ Combine on premises and cloud based applications traffic manager supports external non azure endpoints enabling it to be used with hybrid cloud and on prem deployments.
✓ Distribute traffic to large complex deployments using nested traffic manager profiles.

- The traffic manager works at a DNS level.
- It directs the client to the service endpoints based on the rules of the traffic routing method.
- Clients connect to the selected endpoints directly.
- Traffic manager is not a proxy or a gateway hence it does not see the traffic passing between the client and the service.

Azure DNS

- DNS is responsible for resolving a website or a service name to its IP address.
- Azure DNS is the hosting service for DNS domains, providing name resolution using Microsoft Azure infra.
- By hosting domains in Azure it is possible to use the same credentials to manage DNS as API billing etc.


1.) Request: www.contoso.com
2.) Return IP: 1.2.3.4
User
DNS
Azure DNS
3.) Connect to Resource with IP 1.2.3.4
VM
Web App

LAB

- Create a Address range and assign to Vnet
- Create a Vnet and deploy a Vnet Gateway.
- Create a VM inside the Vnet and access using PublicP