Design and Implement Core Networking Infrastructure

Understanding a simple request from a home network

Mobile

Laptop

Home wireless router

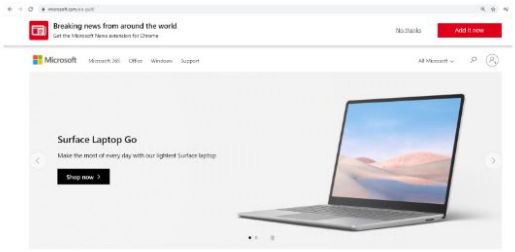
2.10.90.20

Internet

Server

www.microsoft.com

23.209.106.110



A simple network

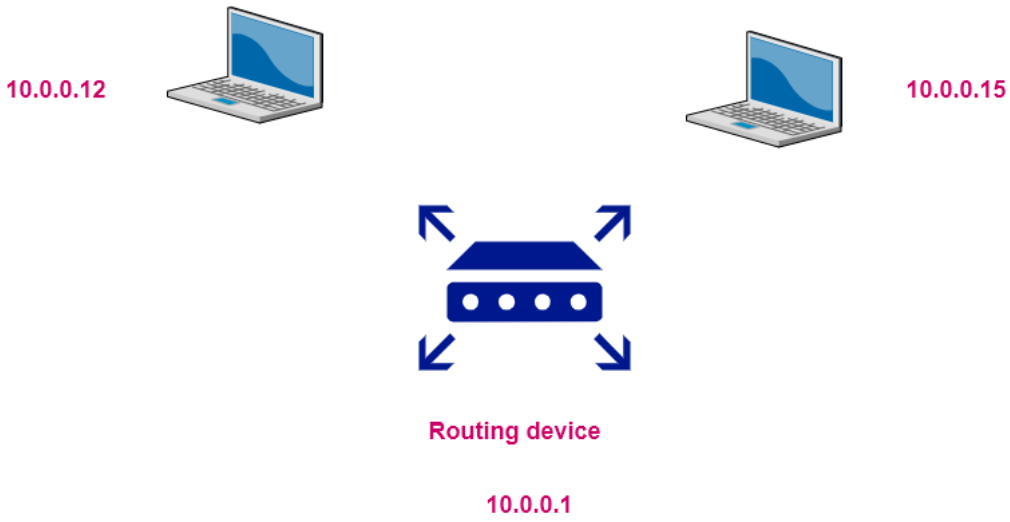
You can make two devices talk to each other

10.0.0.10

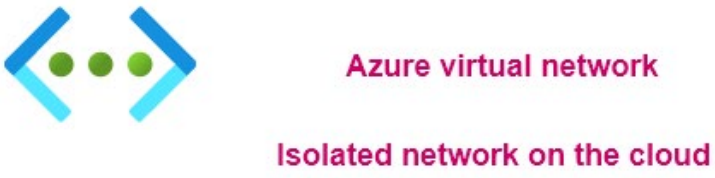
10.0.0.13

10.0.0.11

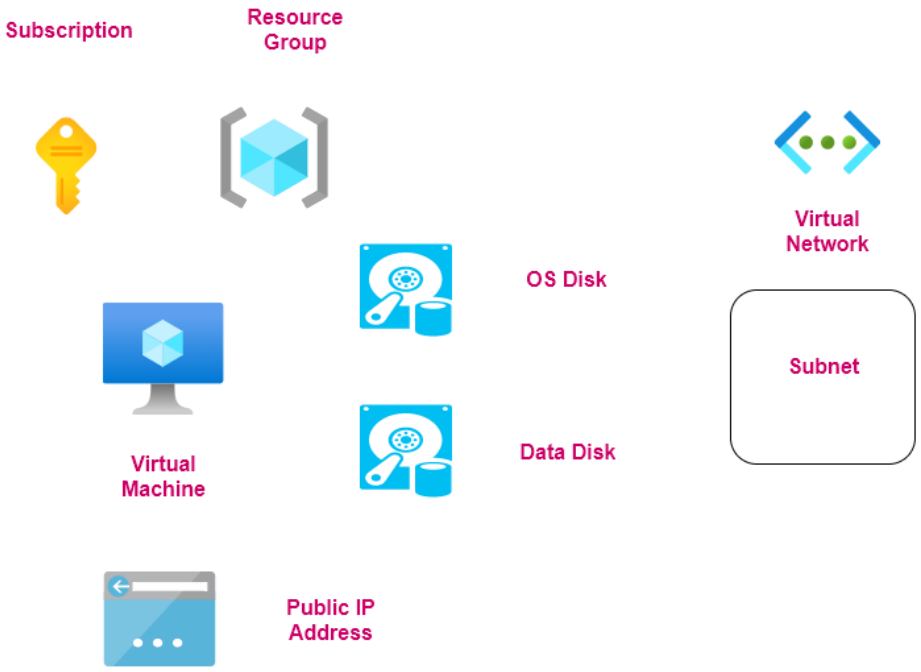
10.0.0.14



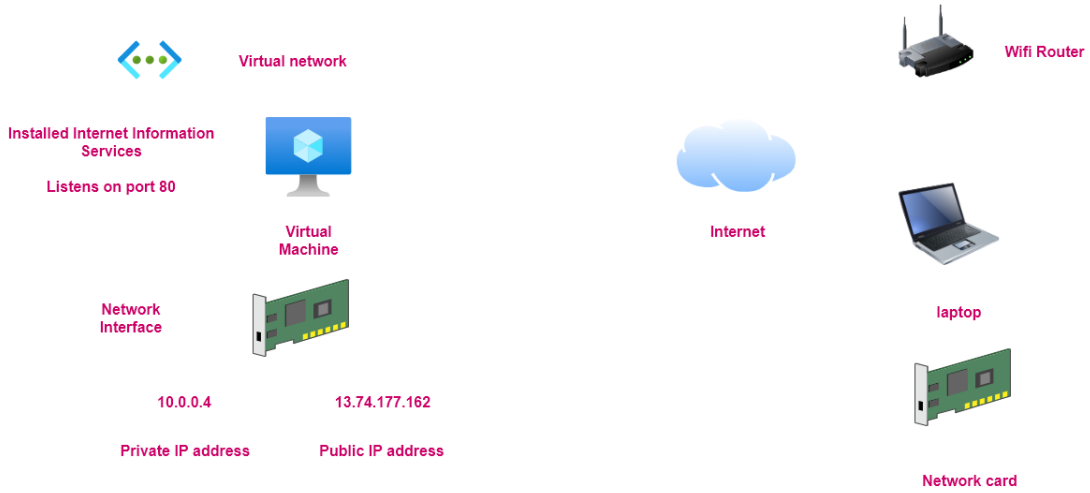
What is an Azure virtual network



What goes into the deployment of a virtual machine



Lab - Installing Internet Information Services on the machine



Understanding IP addresses

IP Address

An IP address is a 32-bit number

It is written in a human-readable format

Example - 192.0.2.1

11000000.00000000.00000010.00000001

Each part of the IP address is an octet that is seperated by a dot notation

Each octet can have a decimal value between 0 and 255

Minimum value - 0 0 0 0 0 0 0 0

Maximum value - 1 1 1 1 1 1 1 1

Number of values -	**256**	**128**	**64**	**32**	**16**	**8**	**4**	**2**
	0	0	0	0	0	0	0	0

Place value	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
	0	0	0	0	0	0	0	0

Subnet Mask and CIDR

Network and host ID

An IP address is also associated with a subnet mask

The subnet mask is used to distinguish between the network and the host id

Example - 192.0.2.0

Subnet mask - 255.255.255.0

Here 192.0.2.0 is the network id

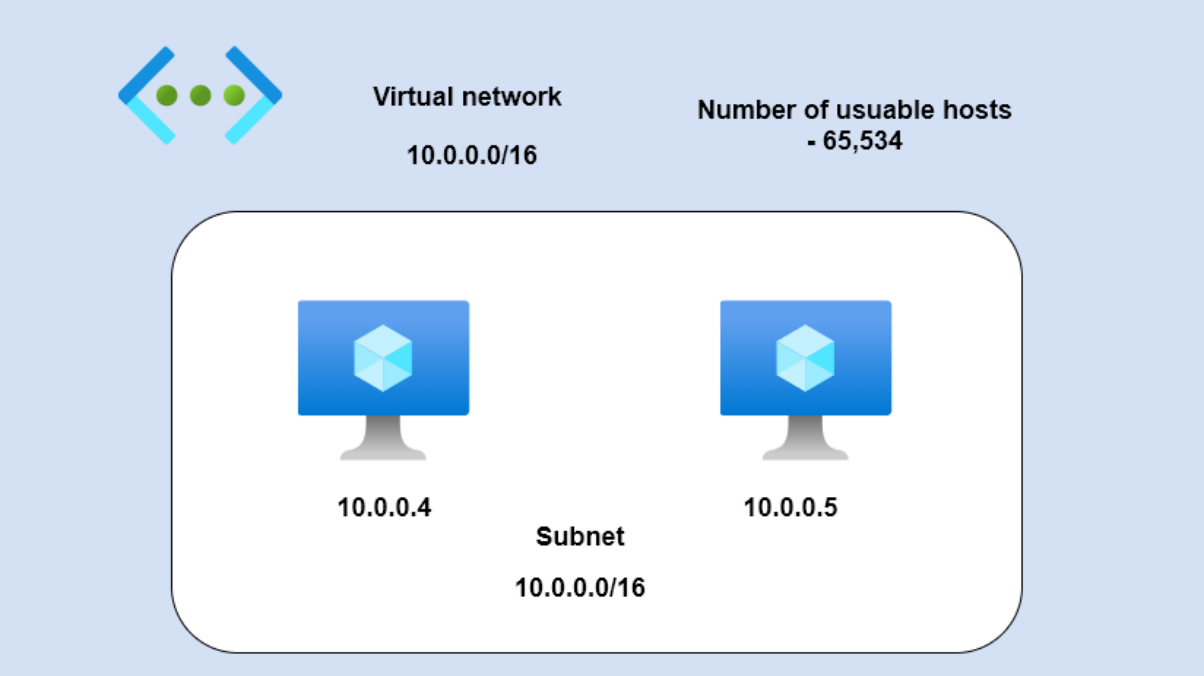
192.0.2.1 **192.0.2.2** **192.0.2.3**

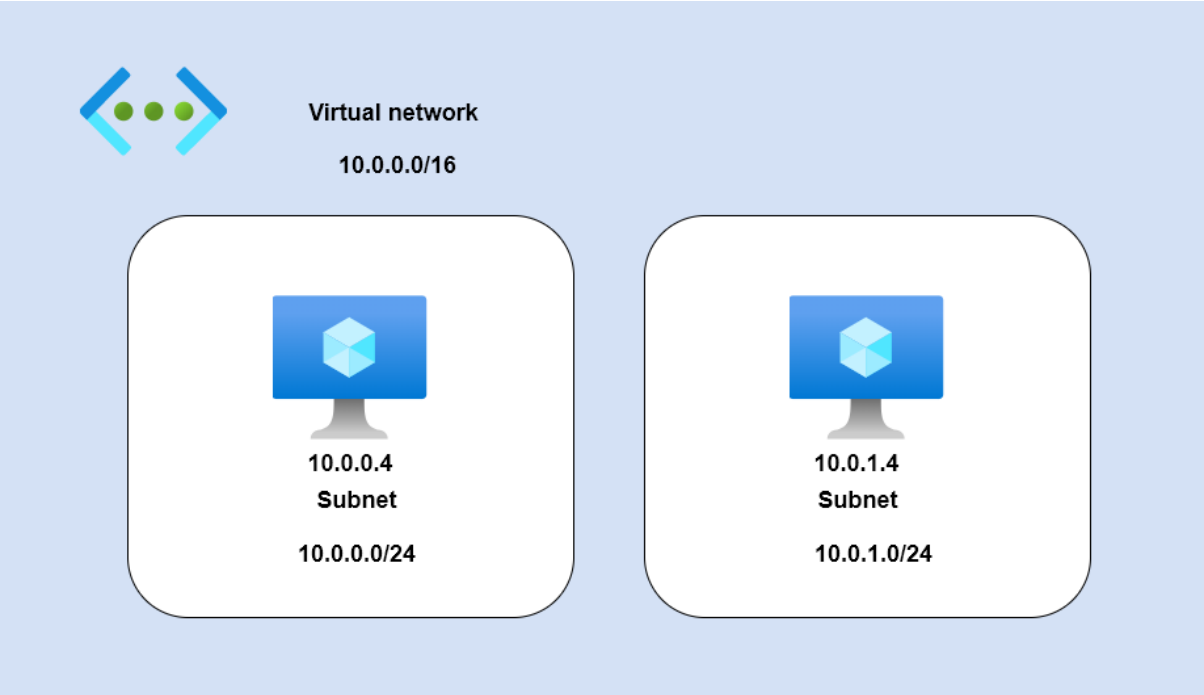
Here you get 256 total number of hosts

The number of usuable IP addresses is 254

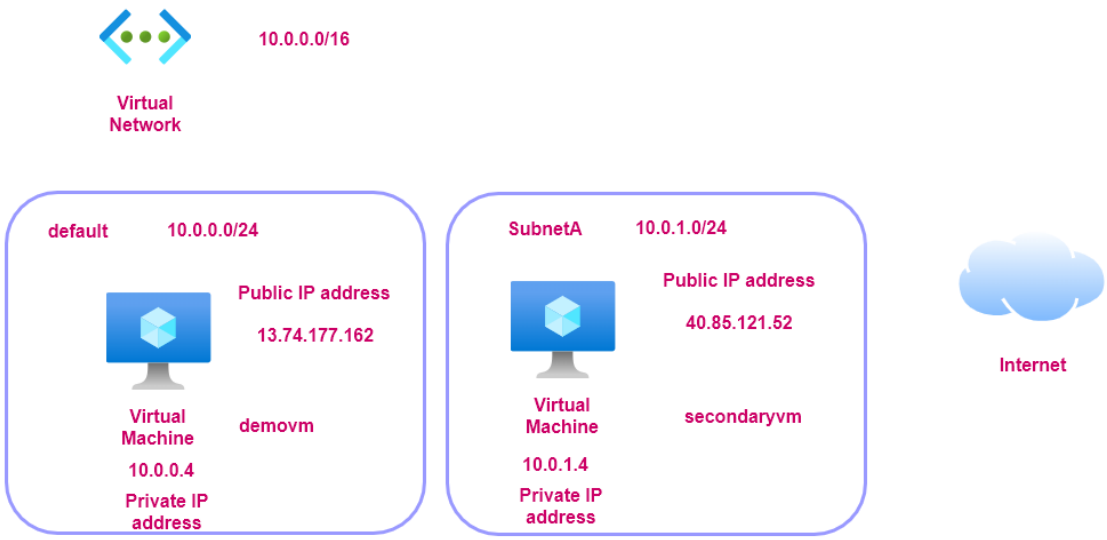
192.0.2.0 is the network id and 192.0.2.255 is the broadcast id

What are subnets

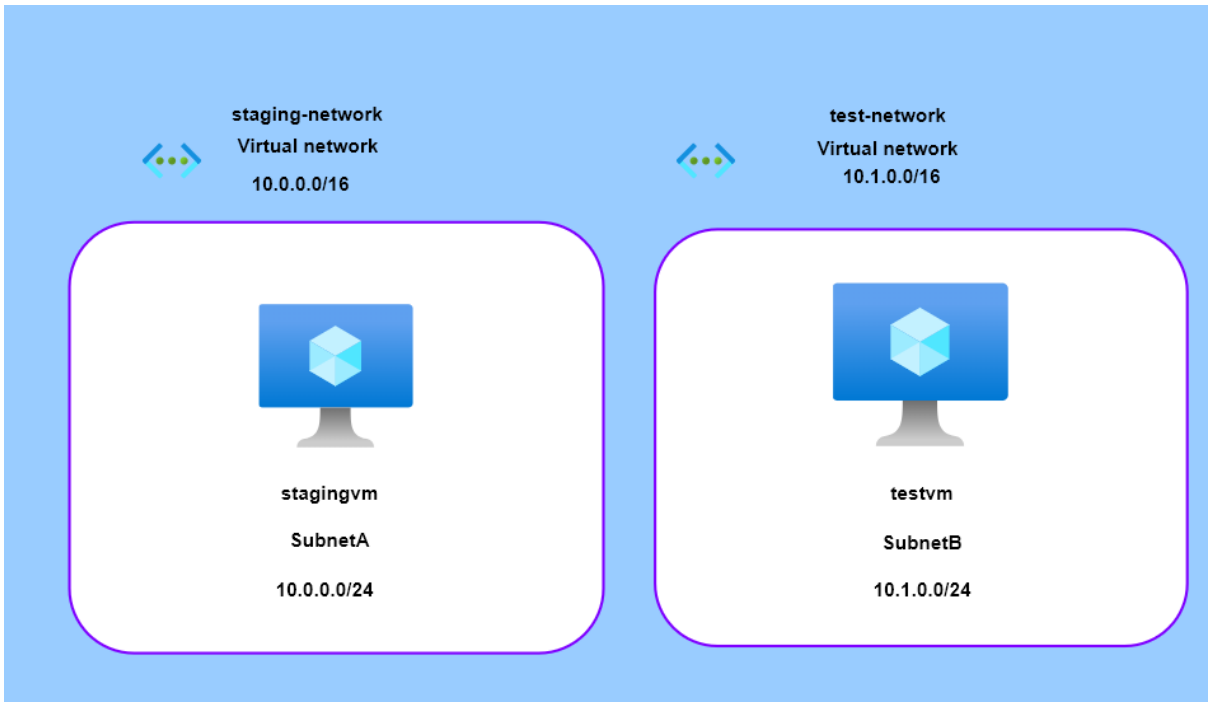




Communication between 2 machines



Virtual Network Peering



What is the domain name system

Mobile

Laptop

Home wireless router

2.10.90.20

Internet

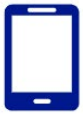
Server

www.microsoft.com

23.209.106.110

When packets of data need to be routed via the TCP protocol , a connection needs to be established between the client and the server with the use of IP addresses

So how does my client know the IP address of www.microsoft.com



Mobile

Laptop

Home wireless router

2.10.90.20

Internet

Server

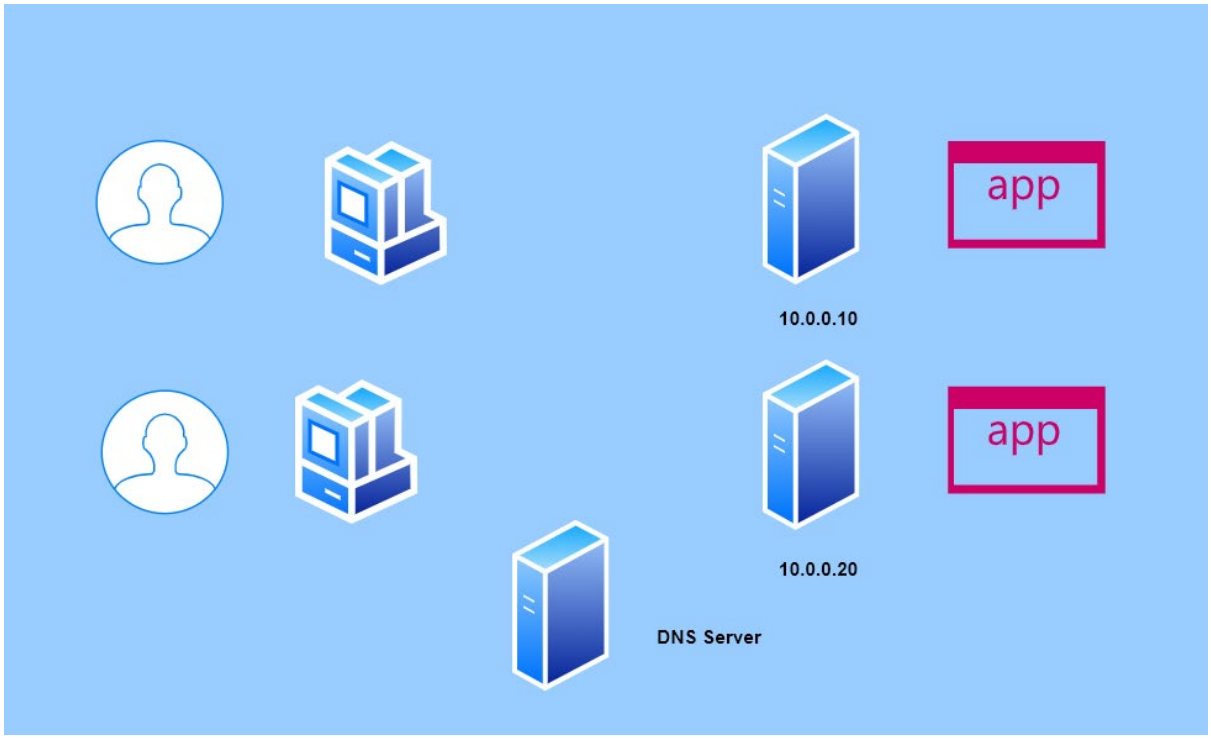
www.microsoft.com

23.209.106.110

DNS servers

Records

23.209.106.110 www.microsoft.com



Lab - Local DNS - Setting up the domain

new-network

10.2.0.0/16

SubnetA - 10.2.0.0/24

SubnetB - 10.2.1.0/24

dns-server

1. Install Active Directory Domain services

2. Promote the server to a domain controller

3. Specify a root domain name - cloud2hub.com

6. Use Azure provided DNS names web-server.internal.cloudapp.net

web-server

4. Create a new server as part of a new subnet

5. Install Internet Information Services on the server

7. Now its time to use our DNS server

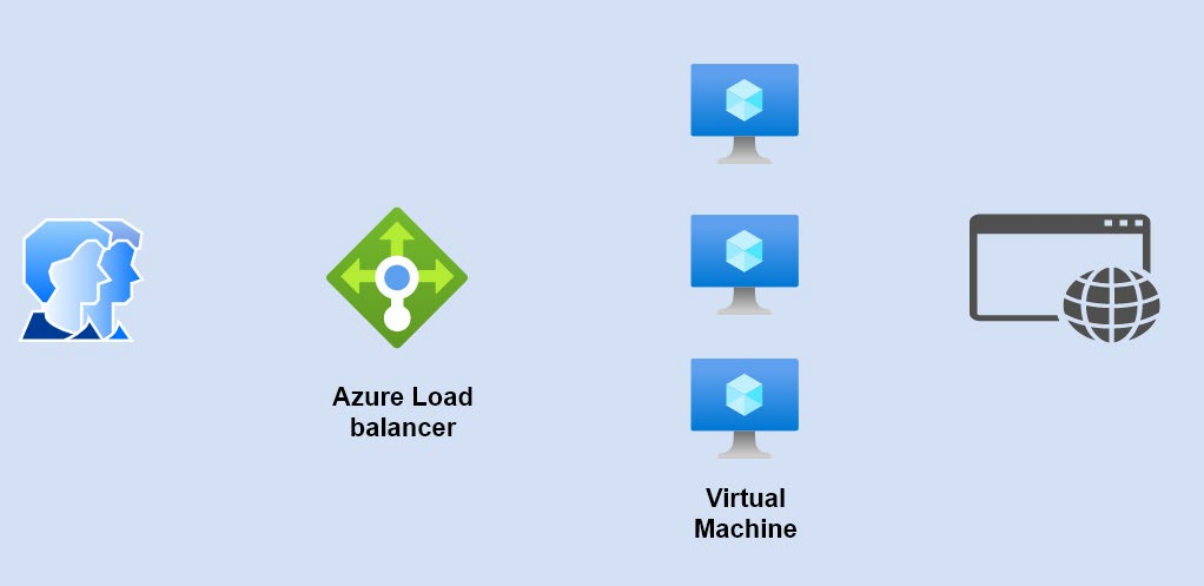
7.1 For the network , we need to mention our DNS Server

7.2 Restart our servers

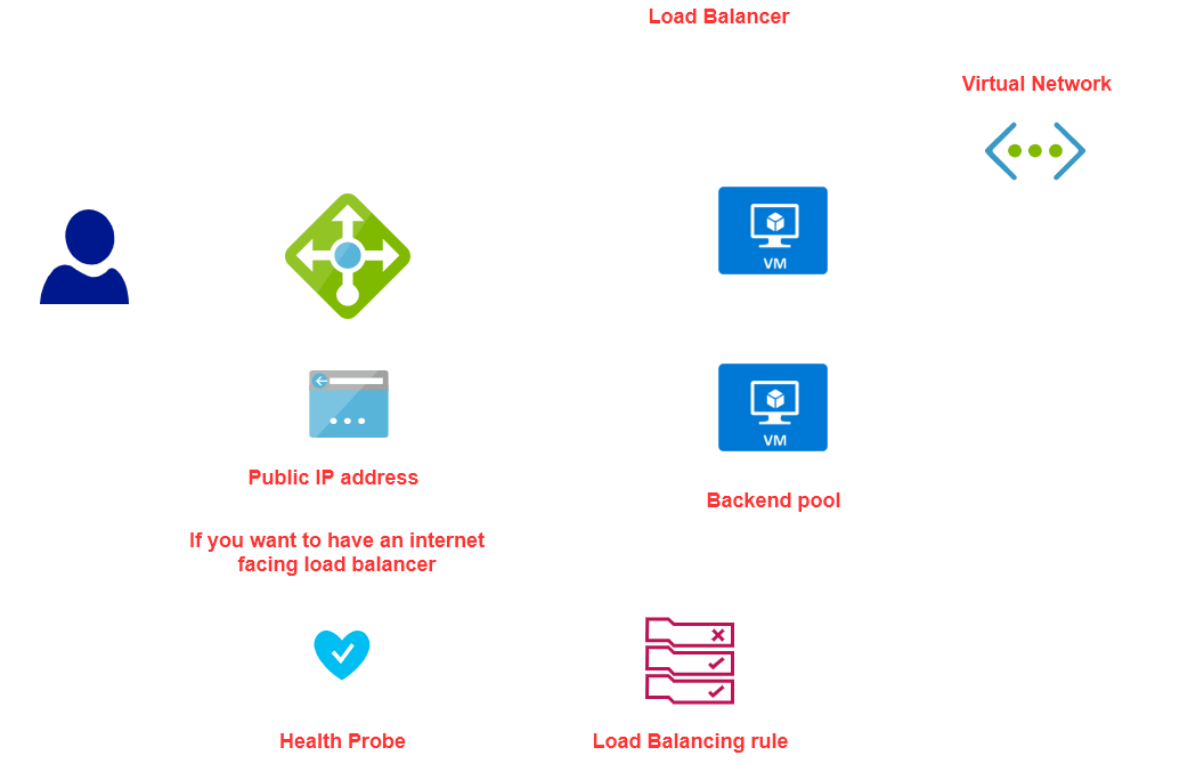
7.3 Add a record to the zone

Design and Implement Routing

What is the Azure Load balancer service

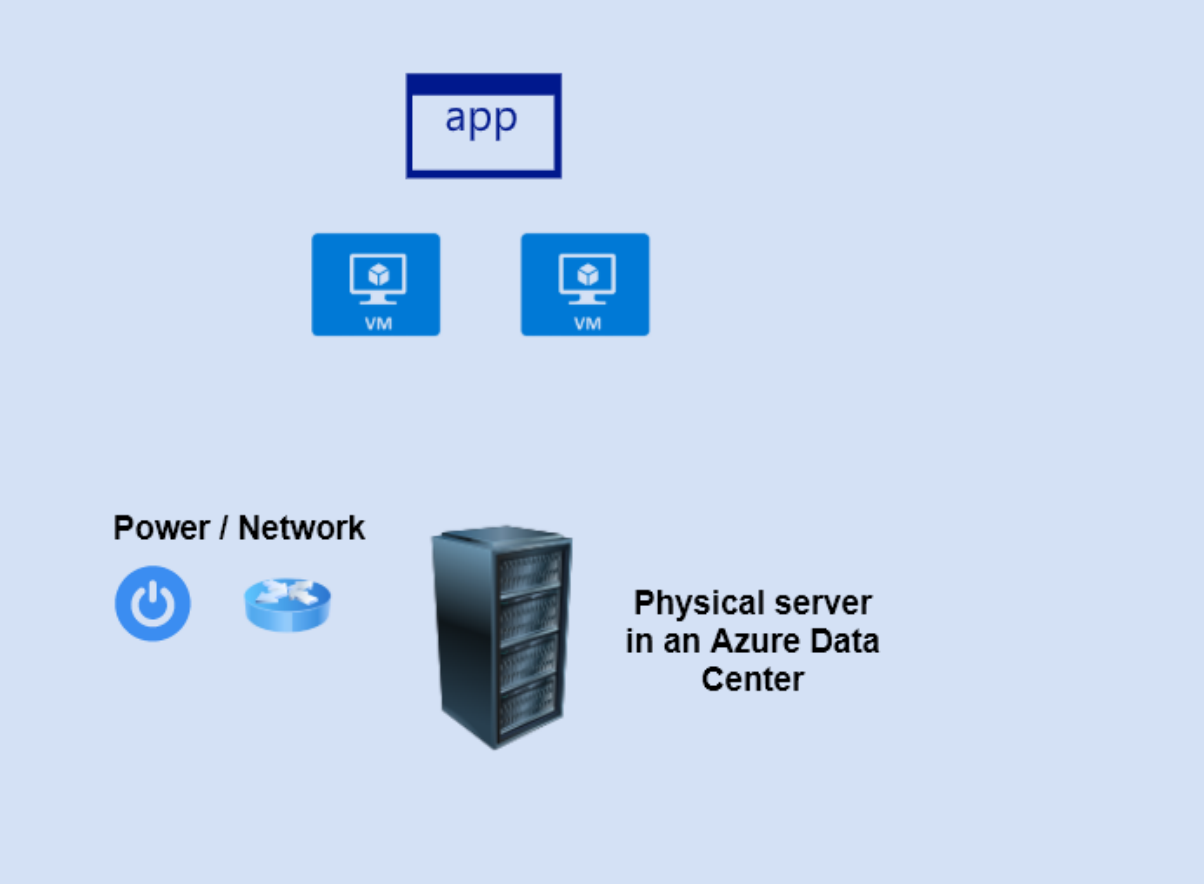


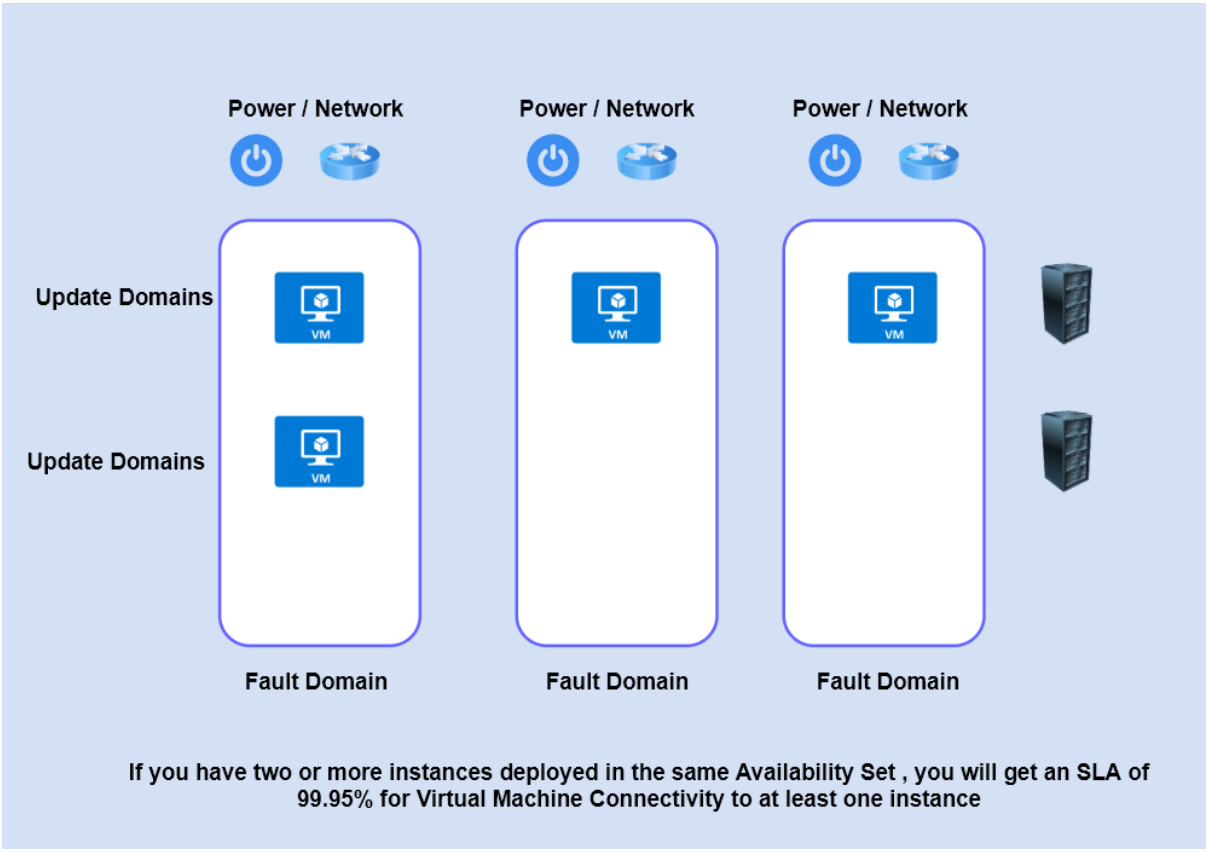
Load Balancer SKU's



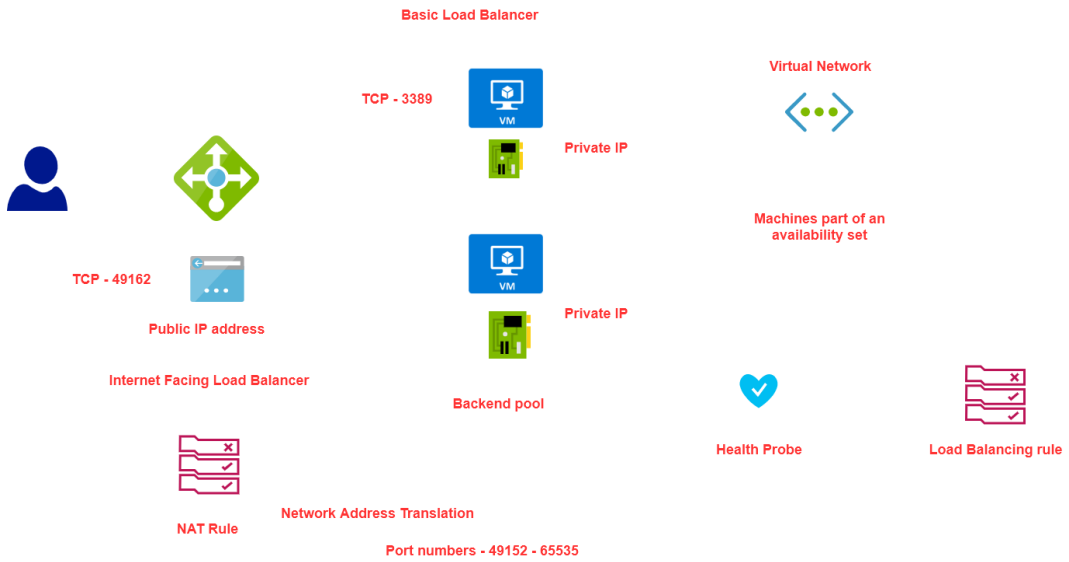
Basic Load Balancer	Standard Load Balancer
Free	Charge per hour
The machines in the backend pool need to be part of an availability set or scale set	Here the machines can also be indepedent machines that are part of a virtual network
Health probes - TCP, HTTP	Health probes - TCP, HTTP, HTTPS
No support for Availability zones	Support for Availability zones
No SLA	SLA of 99.99%

Availability Sets

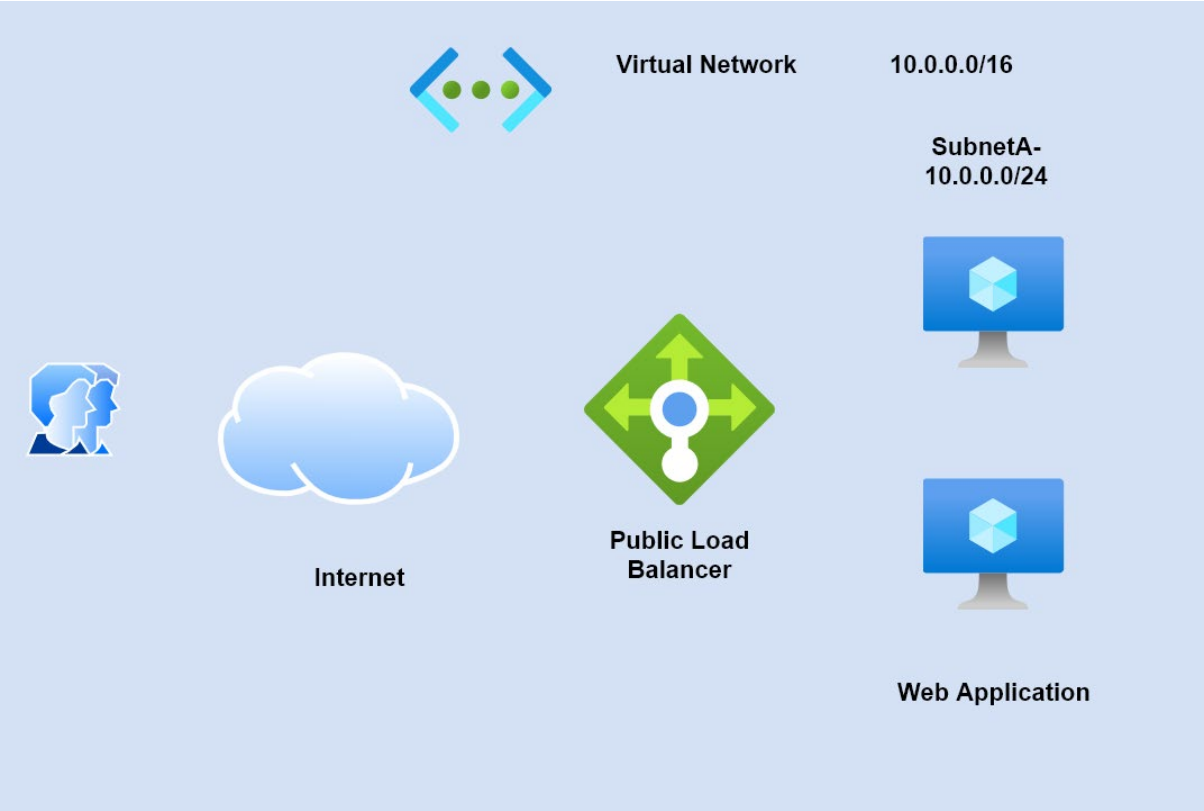




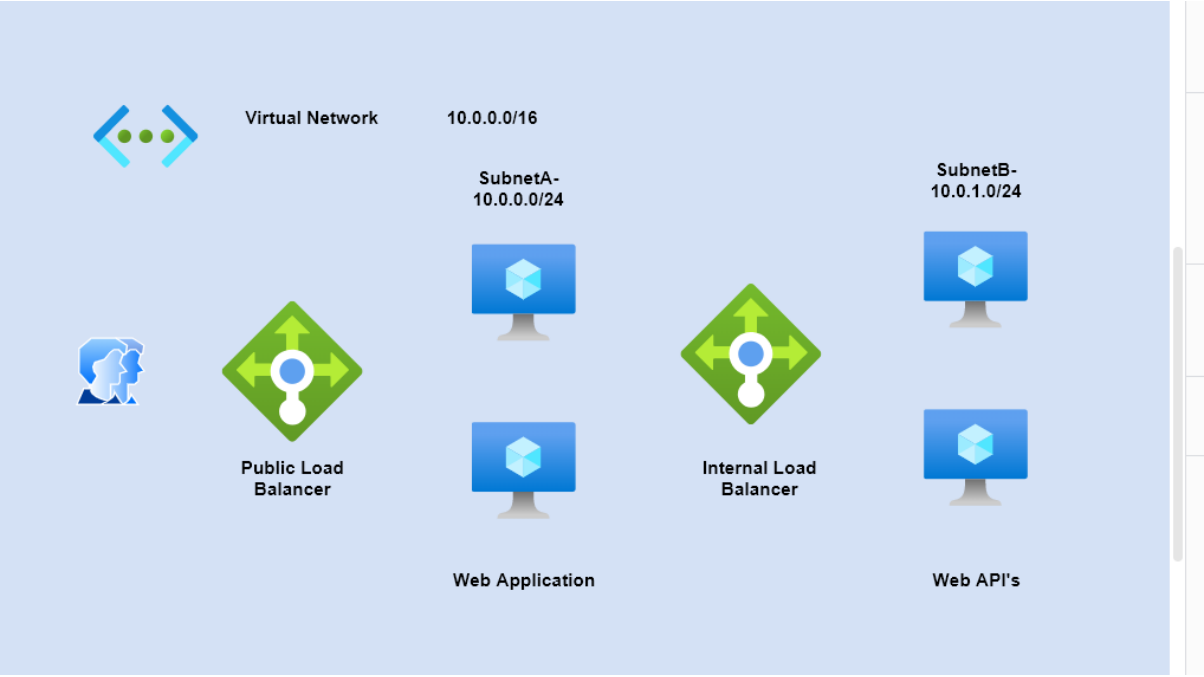
Lab - Basic Load Balancer - NAT rules



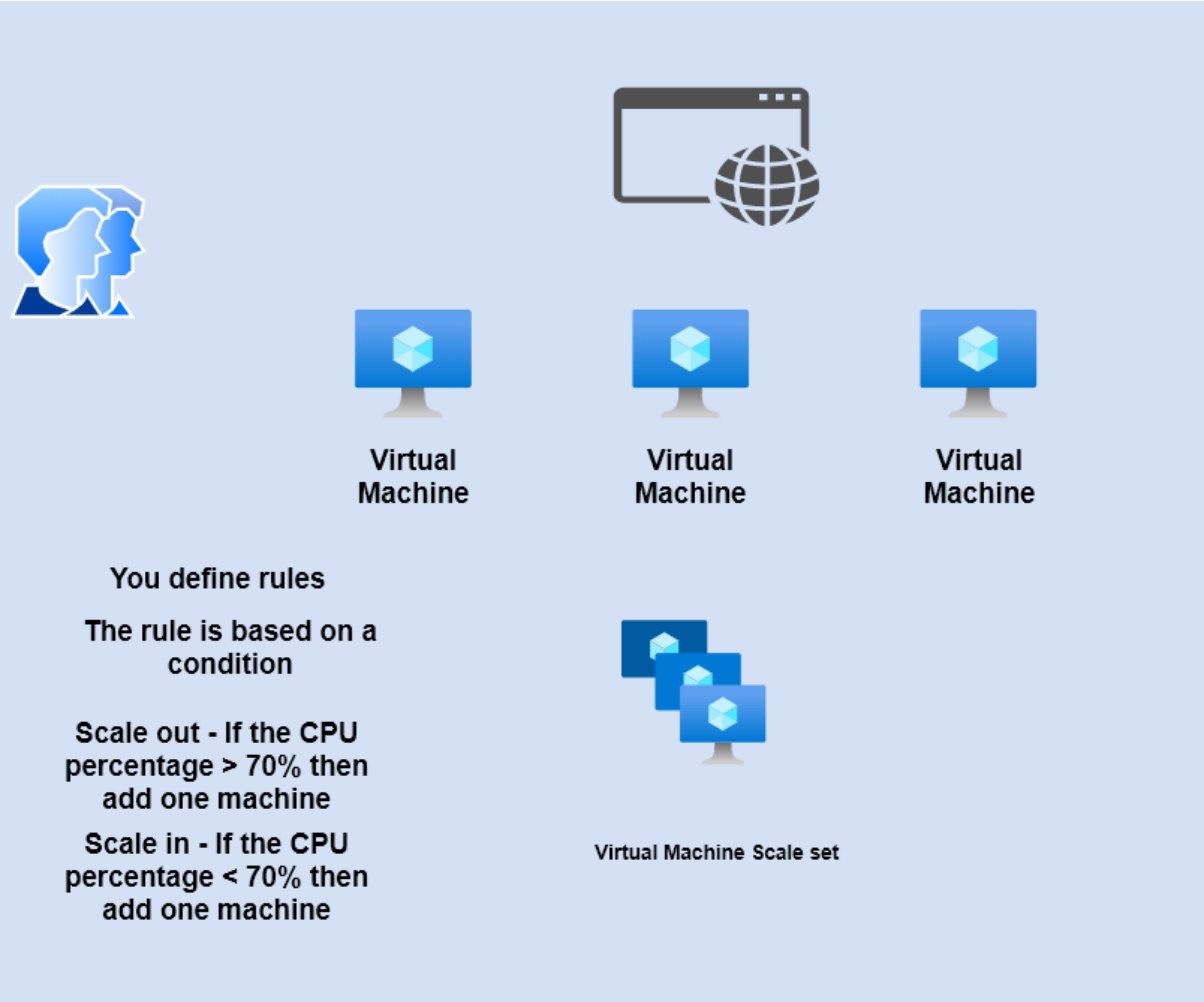
Standard Load Balancer - Outbound Rules



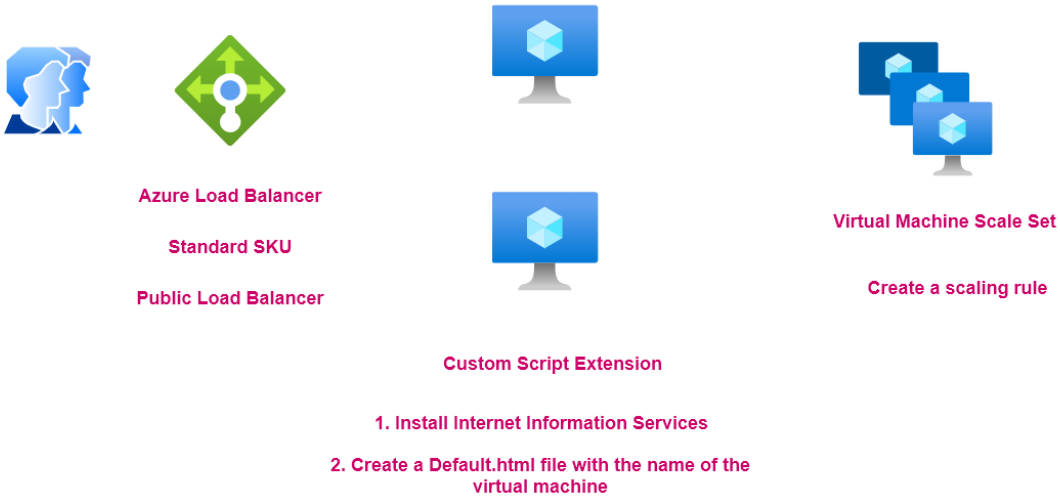
Load Balancer - Internal Load balancer



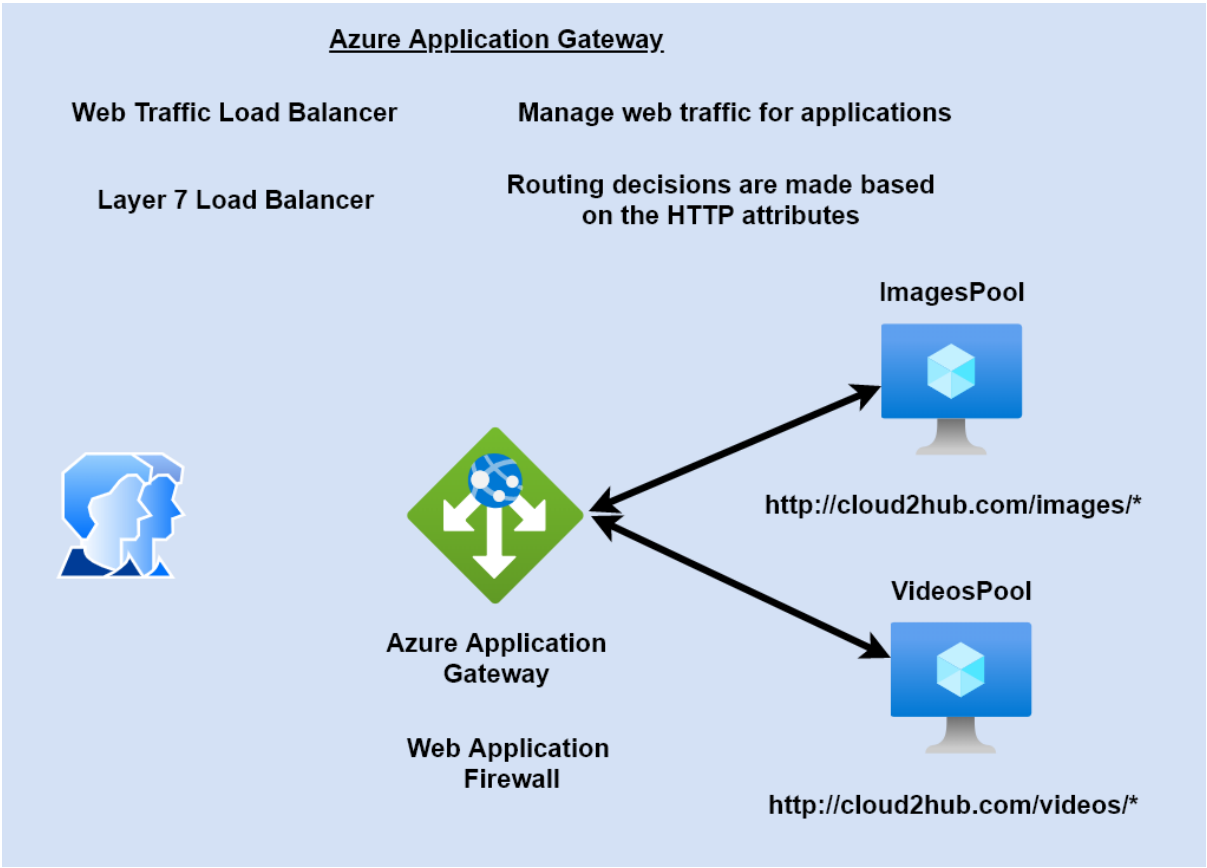
Virtual Machine Scale sets



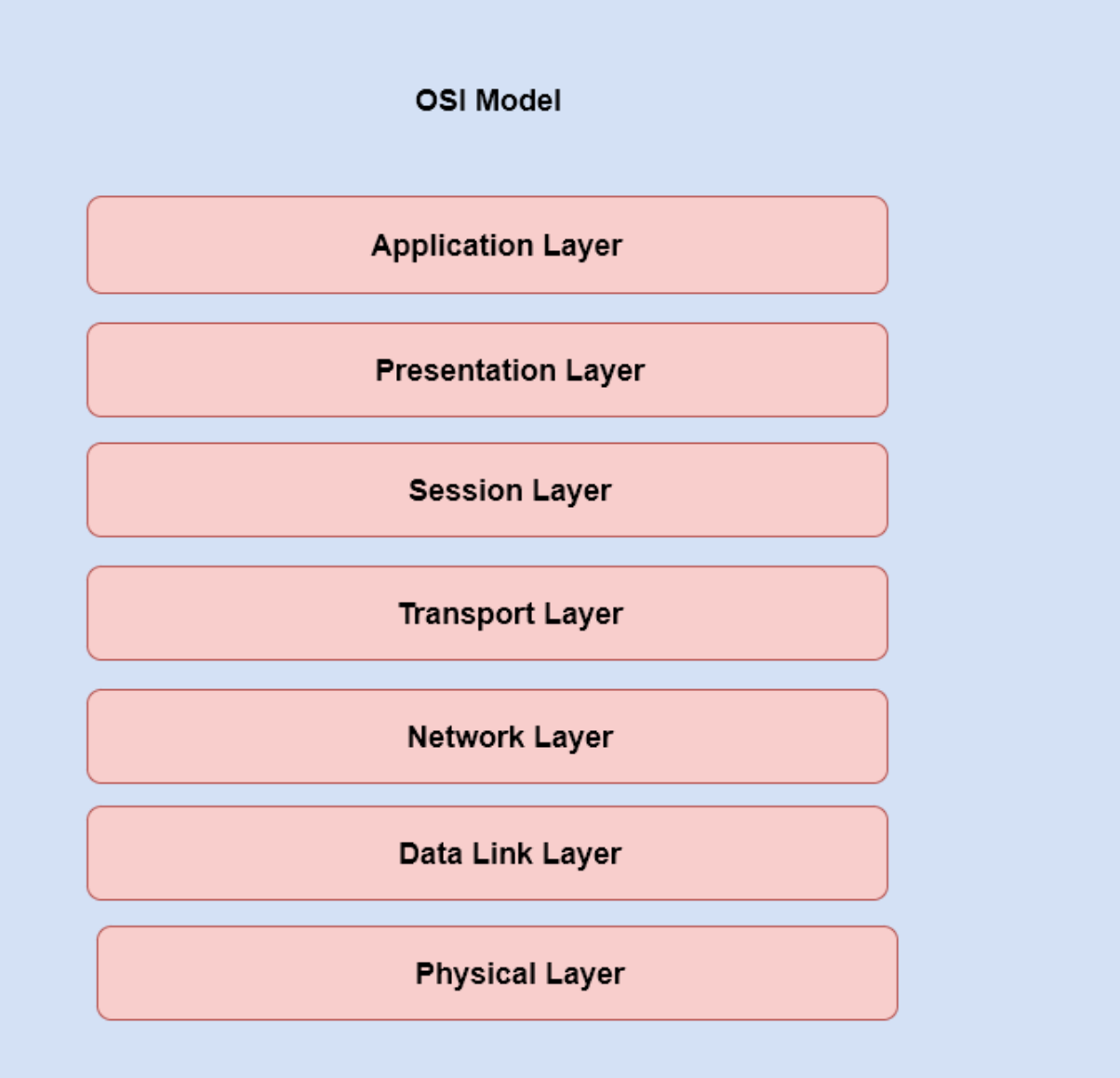
Lab - Virtual Machine Scale Set – Extensions



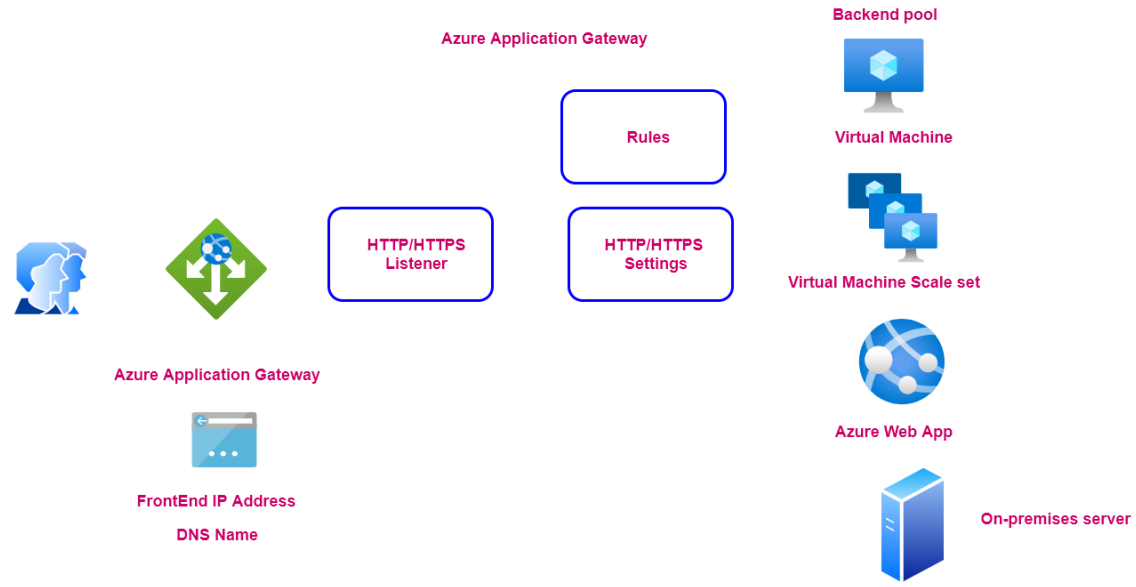
Azure Application Gateway



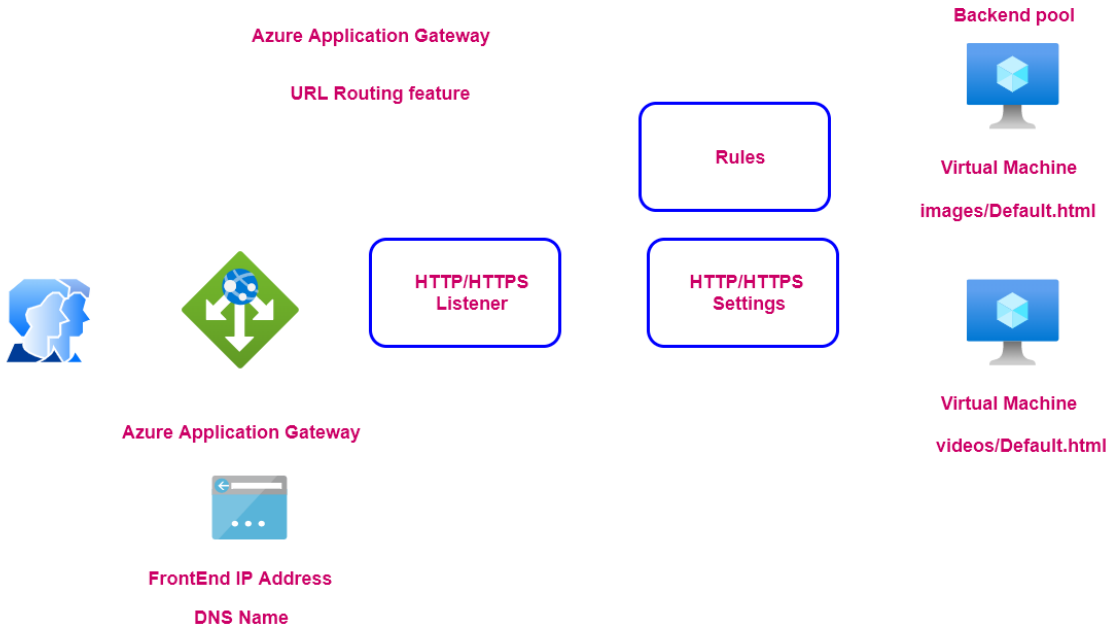
Open Systems Interconnection Model



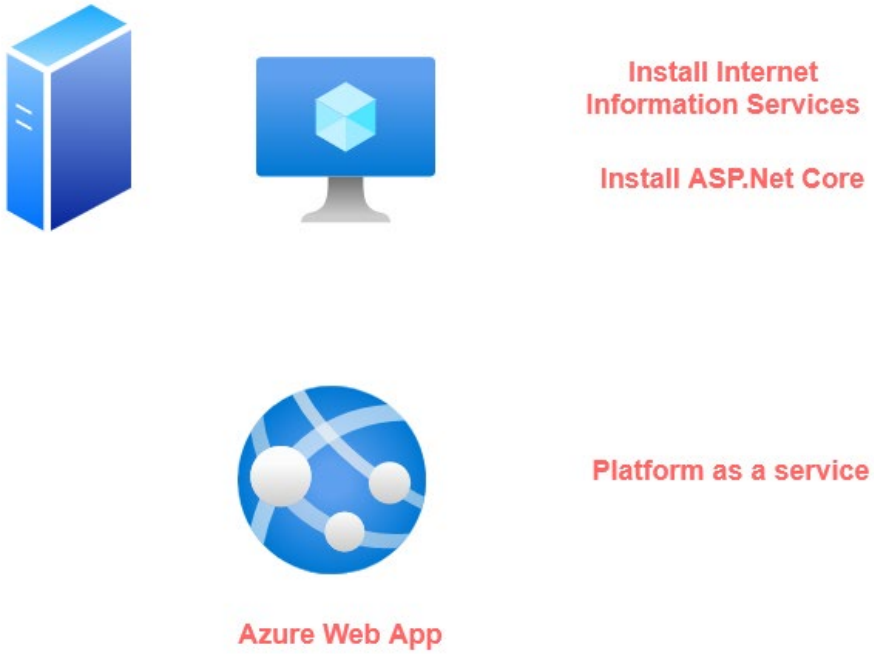
Azure Application Gateway – Components



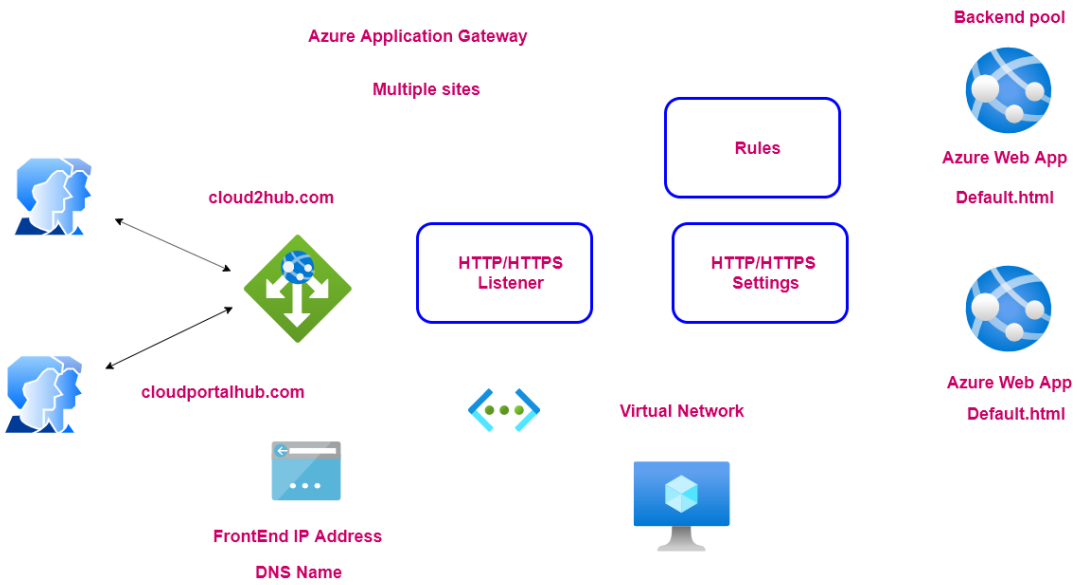
Lab - Azure Application Gateway - URL Routing – Setup



Azure Web Apps



Azure Application Gateway - Multiple Sites – Setup



Azure Traffic Manager

Azure Traffic Manager

This is a DNS-based traffic load balancer

Allows you to direct client requests to an appropriate service endpoint based on a routing method

The endpoint needs to be a public endpoint that can be hosted inside or outside of Azure

Azure Traffic Manager performs health monitoring for the endpoints

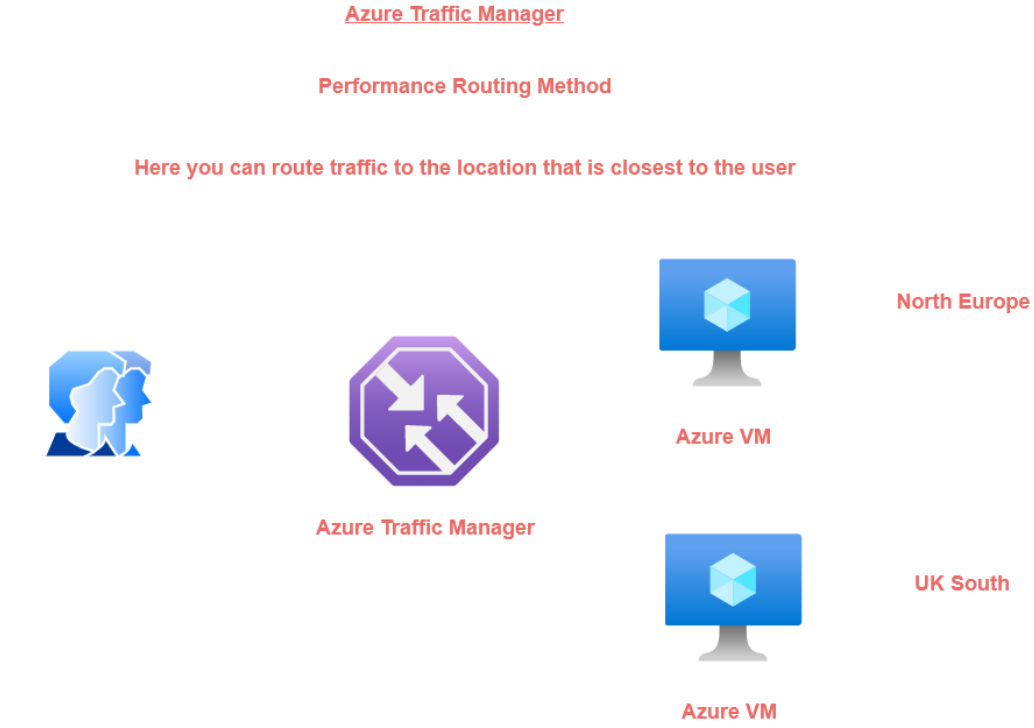
Azure Traffic Manager

Azure VM

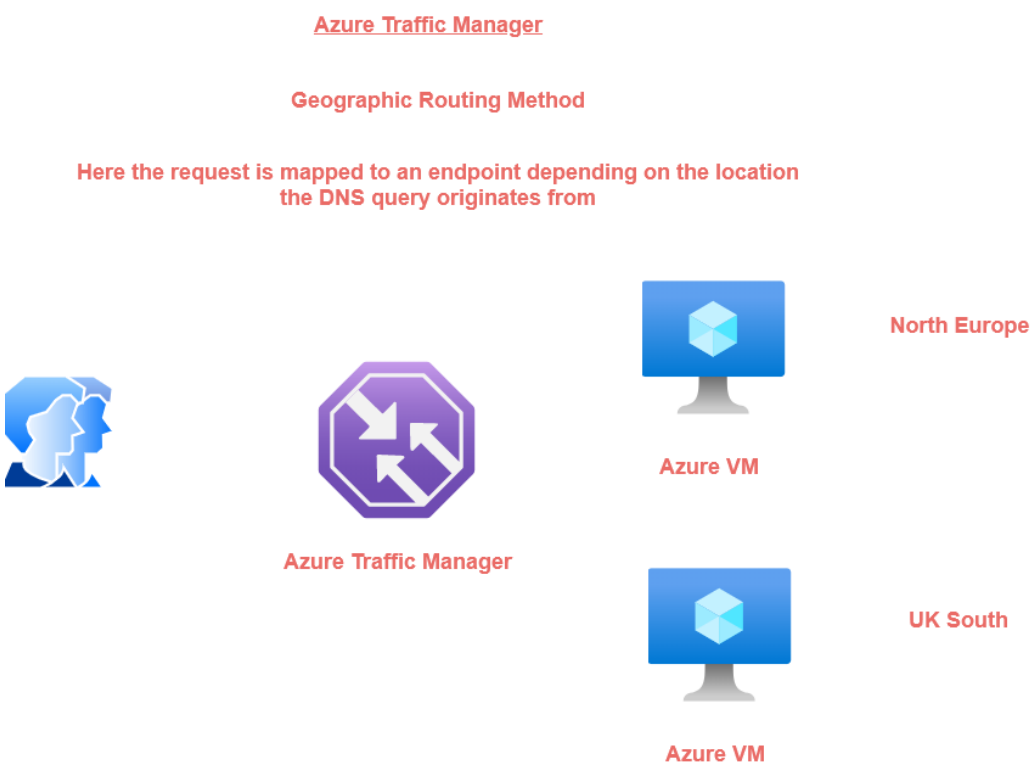
Azure Web App

Lab - Azure Traffic Manager - Priority Routing method

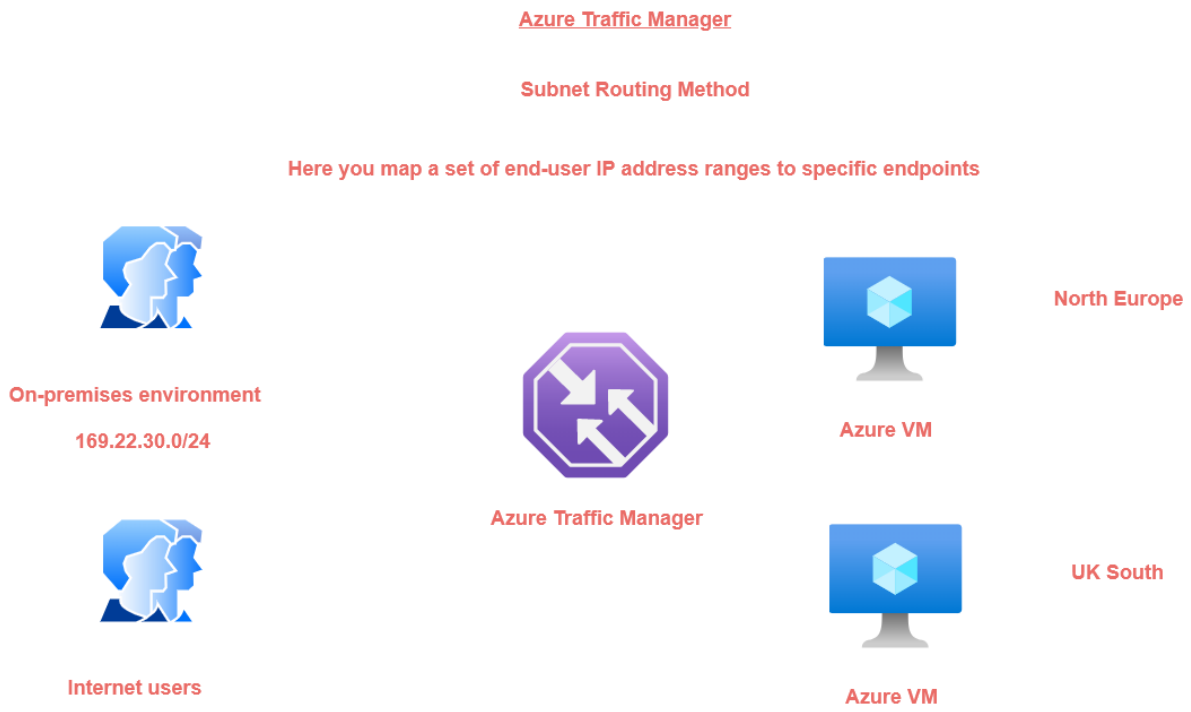
Lab - Azure Traffic Manager - Performance Routing method



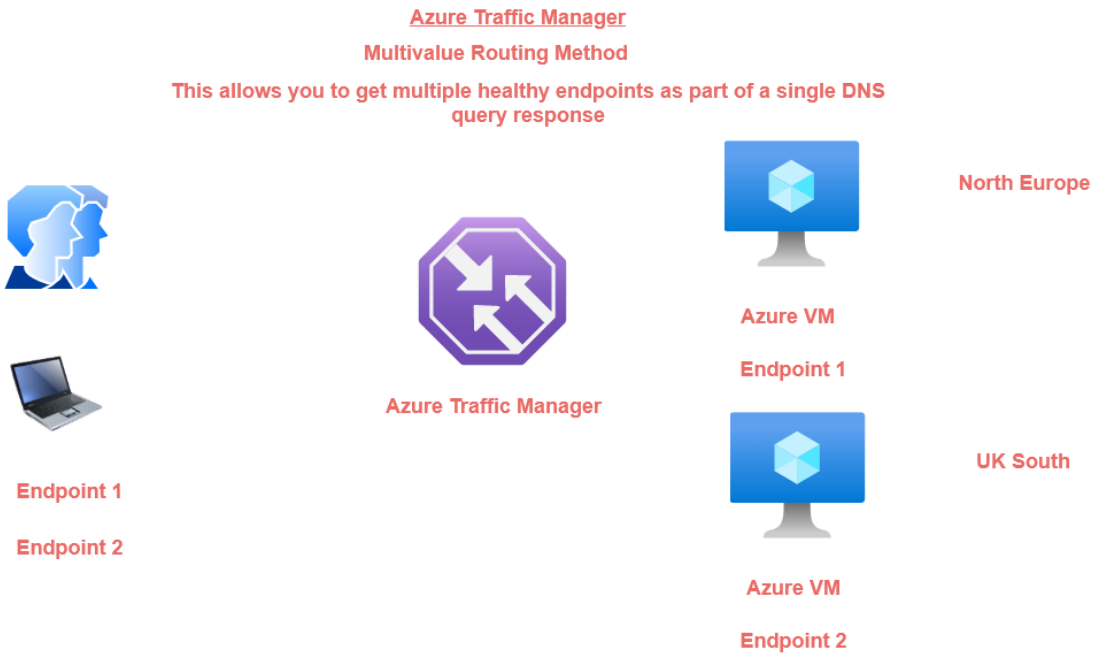
Lab - Azure Traffic Manager - Geographic Routing method



Lab - Azure Traffic Manager - Subnet Routing method



Lab - Azure Traffic Manager - Multivalue routing method



Lab - Azure Traffic Manager - Weighted Routing Method

Lab - Azure Traffic Manager - Nested Endpoints

Azure Traffic Manager

Nested Endpoints

Azure Traffic Manager

Performance Routing method

Azure Traffic Manager

Priority Routing method

Azure VM

North Europe

Azure VM

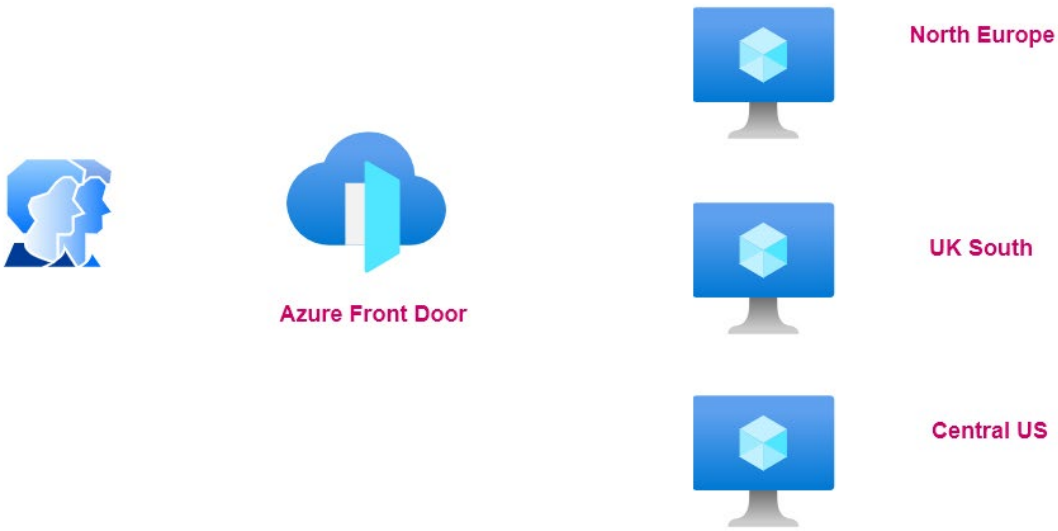
UK South

Azure VM

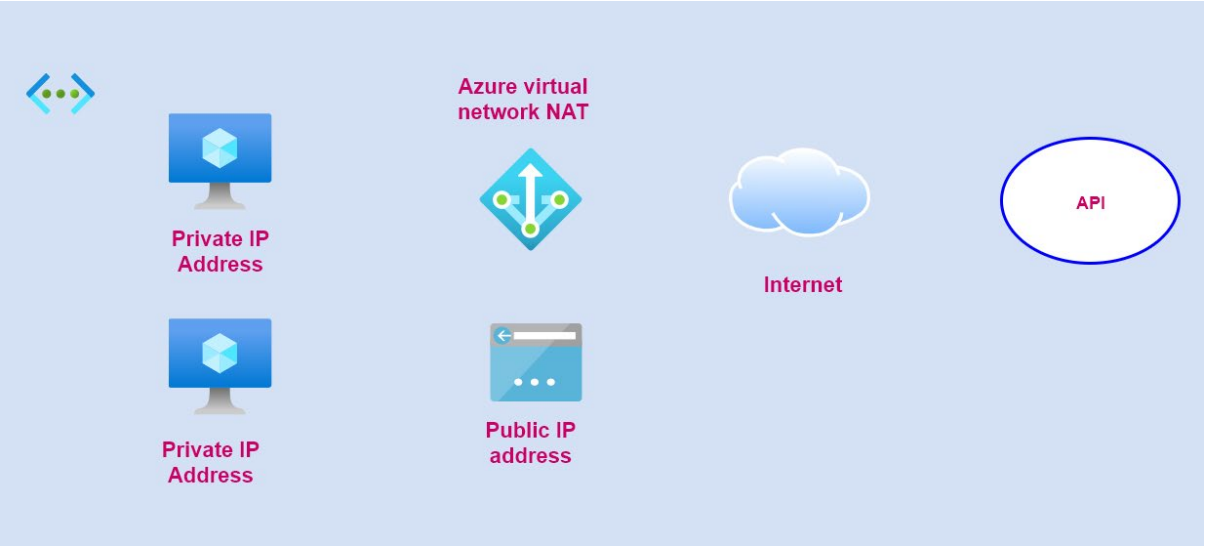
UK South

Azure Front Door

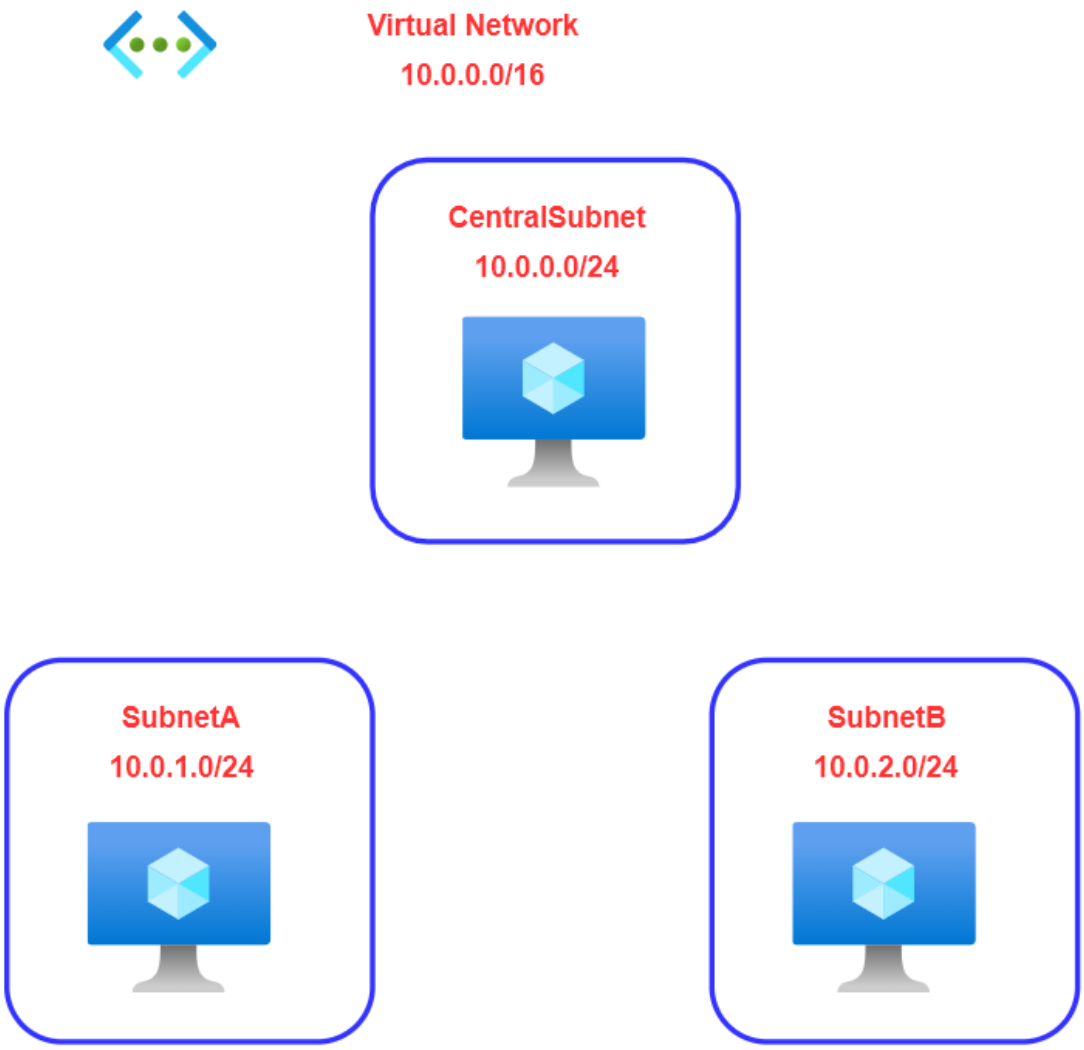
Lab - Azure Front Door – Setup



Azure Virtual Network NAT



User Defined Routes



Design, Implement, and Manage Hybrid Networking

What is a Virtual private network

VPN - Virtual Private Network

Internet

Your Internet Services provider will know all of the requests that are made from your machine onto the Internet

Sometimes privacy can always be a concern

VPN is used to create a private network

Here your public IP address is not placed in the requests that are made onto the Internet

Also VPN connections are encrypted so that the data transfer is more secure

VPN server

Internet

Azure Point-to-Site VPN

10.0.0.0/16

GatewaySubnet

10.0.1.0/24

default

10.0.0.0/24

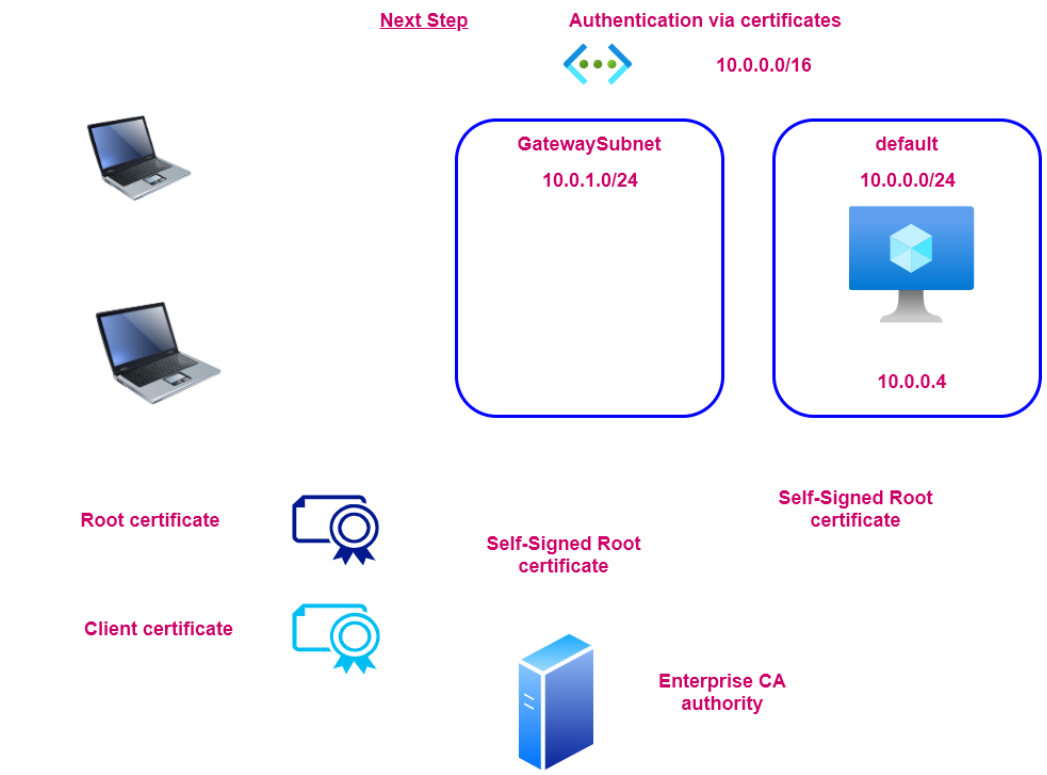
10.0.0.4

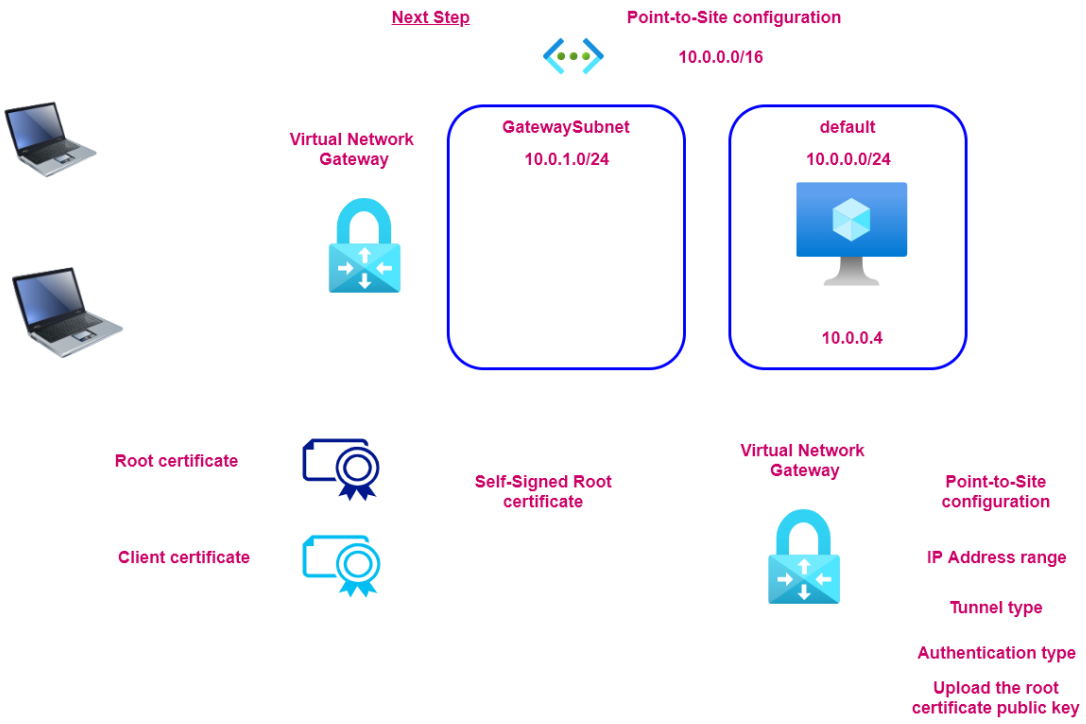
The gateway subnet is used to host gateway VM's and services

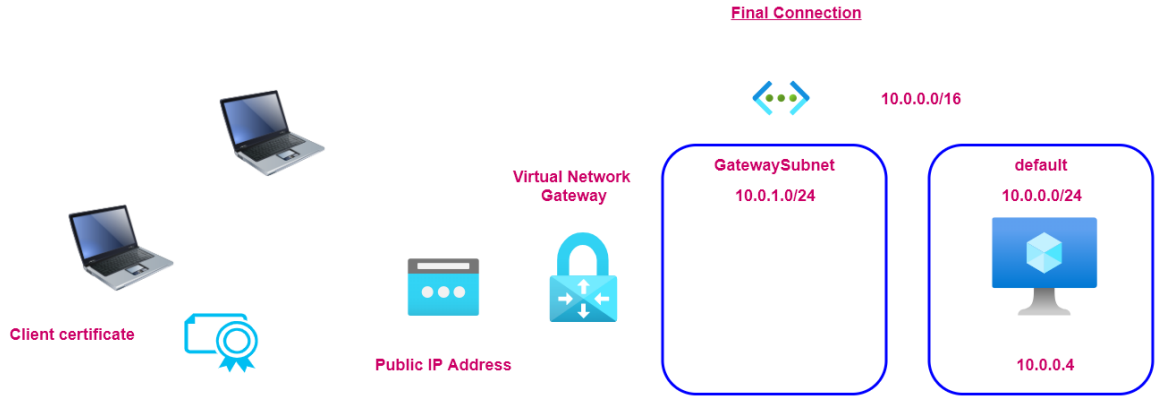
The VM's in the gateway subnet are configured with the required VPN gateway settings

No other VM's must be deployed to the gateway subnet

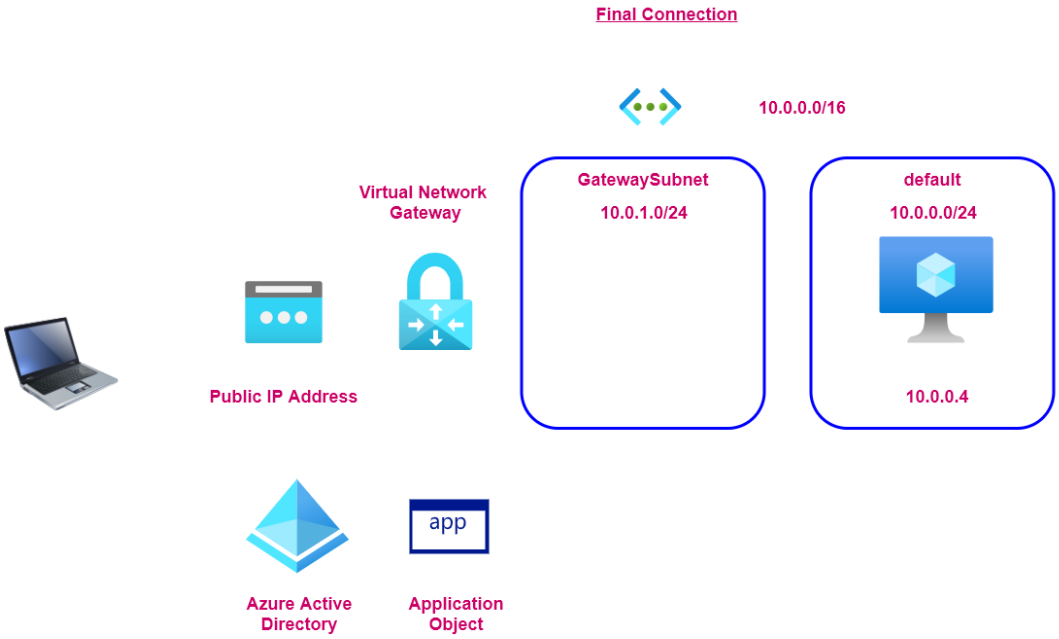
The gateway subnet can be configured as /29, but Microsoft recommends /27, /26


Next Step
Authentication via certificates
10.0.0.0/16
GatewaySubnet
10.0.1.0/24
default
10.0.0.0/24
10.0.0.4
Root certificate
Client certificate
Self-Signed Root certificate
Self-Signed Root certificate
Enterprise CA authority

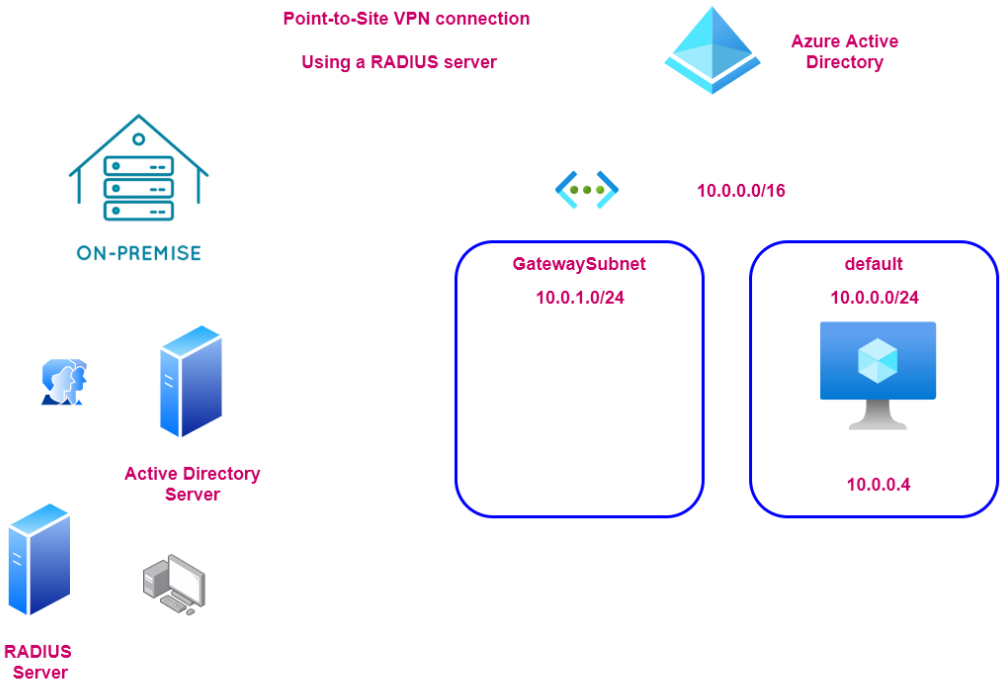

Next Step
Point-to-Site configuration
10.0.0.0/16
Virtual Network Gateway
GatewaySubnet
10.0.1.0/24
default
10.0.0.0/24
10.0.0.4
Root certificate
Client certificate
Self-Signed Root certificate
Virtual Network Gateway
Point-to-Site configuration
IP Address range
Tunnel type
Authentication type
Upload the root certificate public key



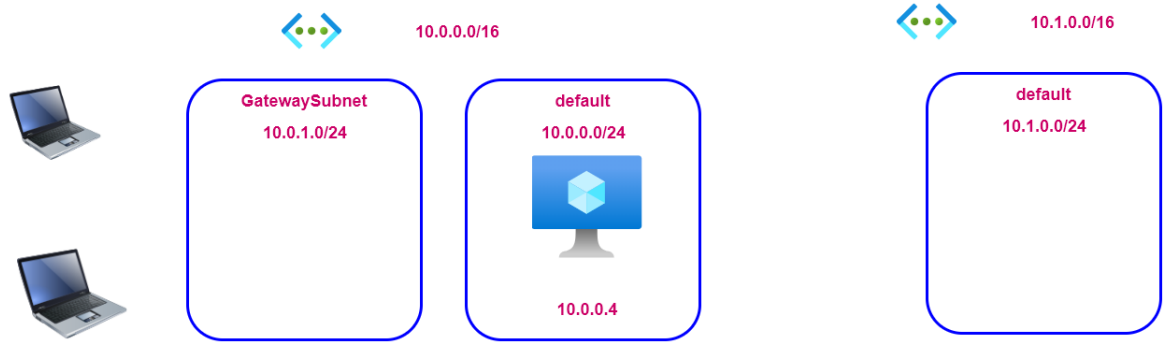
Lab - Point-to-Site VPN - Using Azure AD Authentication



Point-to-Site VPN - RADIUS Server



Point-to-Site VPN - Note on peering connections



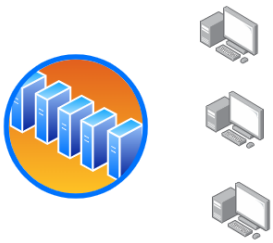
There is already a P2S connection

You then implement virtual network peering

You have to redownload the VPN client package needs to be downloaded on the client machine again.

Azure Site-to-Site VPN

Site-to-Site VPN



Router

Public IP Address

10.0.0.0/16

GatewaySubnet

10.0.1.0/24

default

10.0.0.0/24

10.0.0.4

The gateway subnet is used to host gateway VM's and services

The VM's in the gateway subnet are configured with the required VPN gateway settings

No other VM's must be deployed to the gateway subnet

The gateway subnet can be configured as /29, but Microsoft recommends /27, /26

Next Step

On-premises setup

10.1.0.0/16

default

10.1.0.0/24

10.1.0.4

Windows Server 2019

VPN/Routing server

10.0.0.0/16

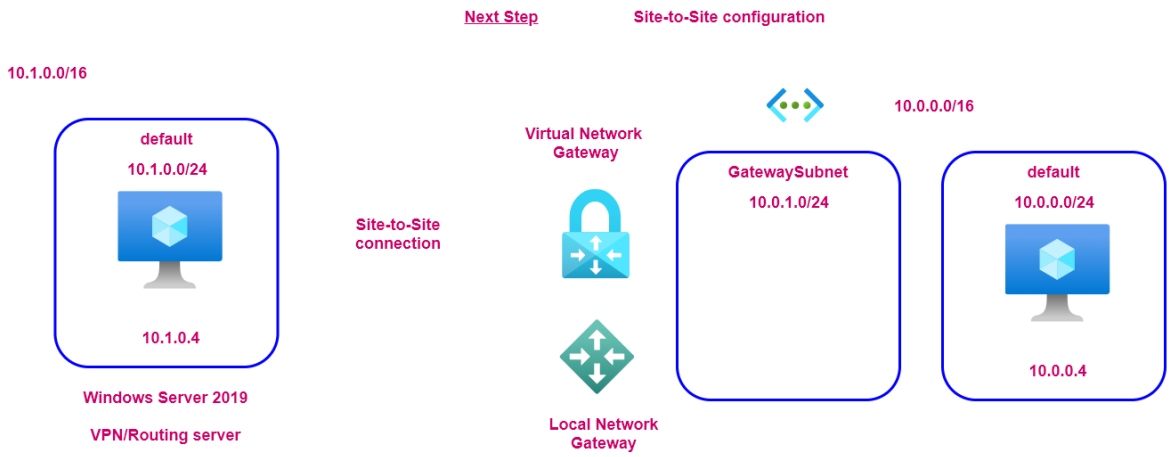
GatewaySubnet

10.0.1.0/24

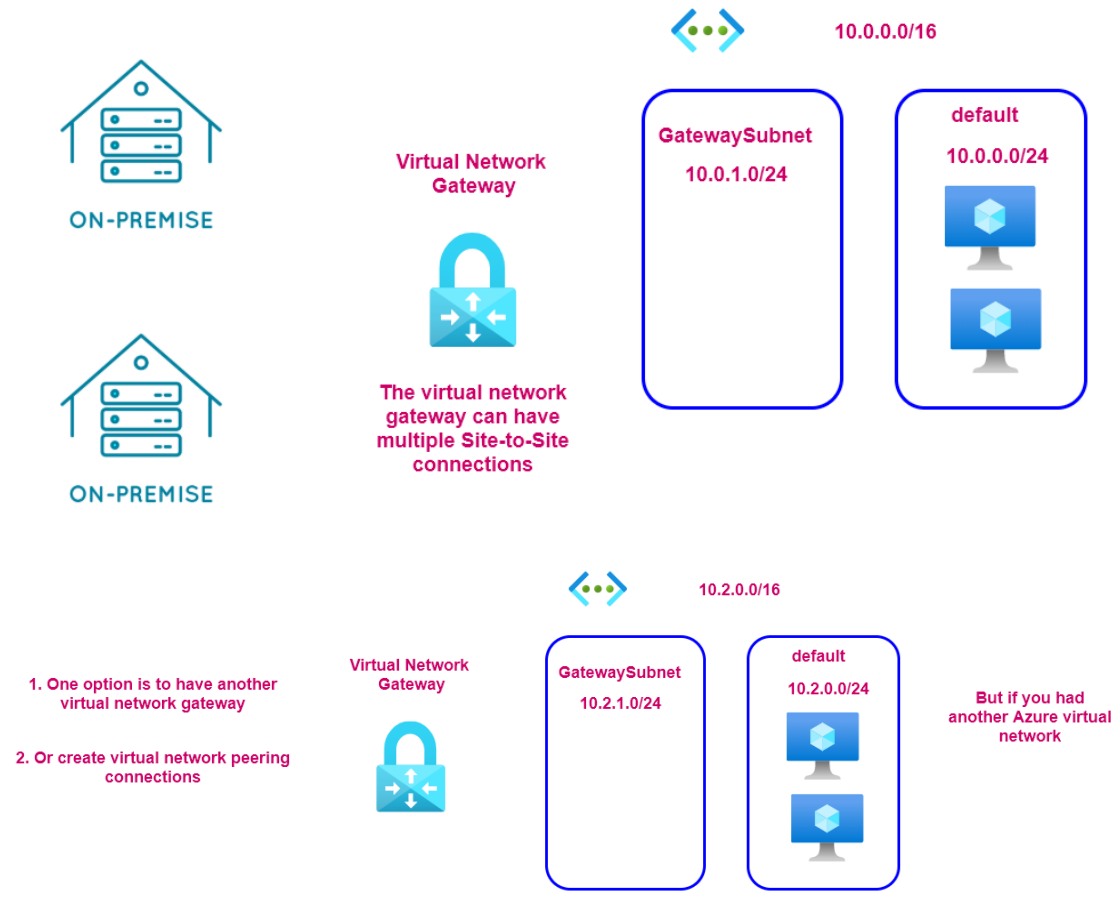
default

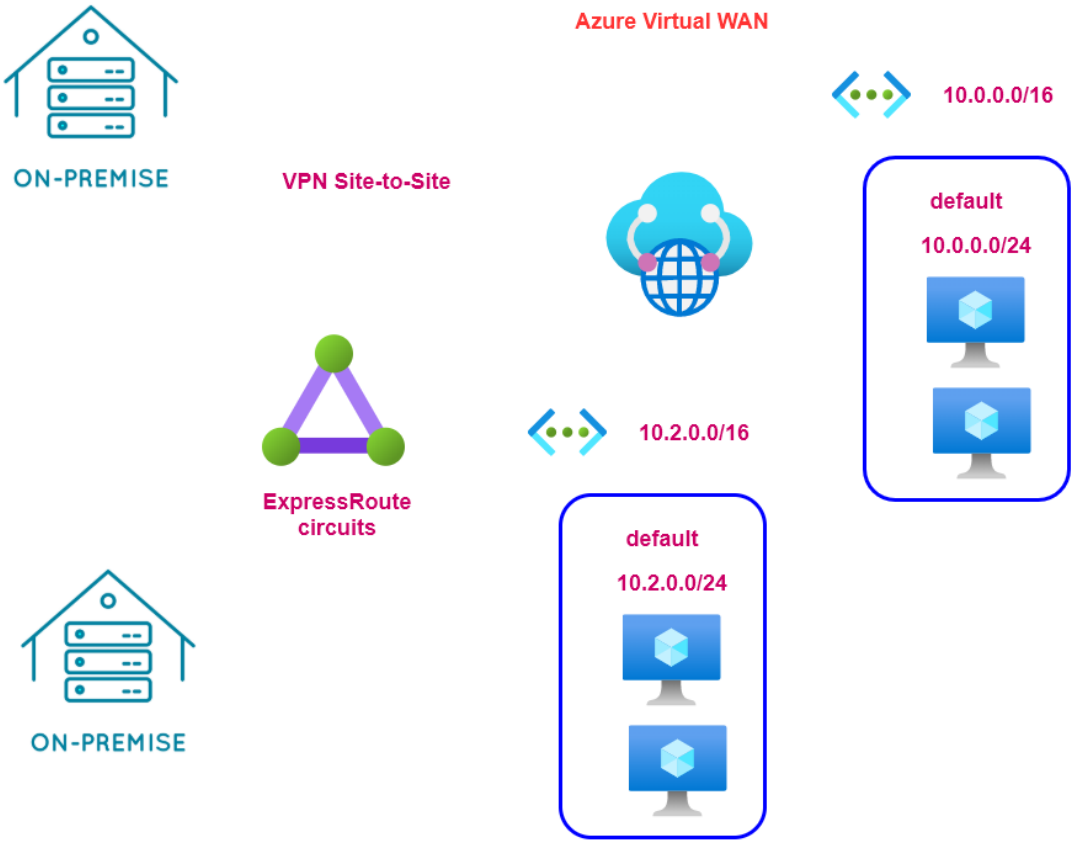
10.0.0.0/24

10.0.0.4



Azure Virtual WAN





The different resources

virtualWAN - This represents the virtual overlay of the Azure virtual network and other resources

Hub - You create a virtual hub in the virtual WAN resource. This is a Microsoft-managed virtual network

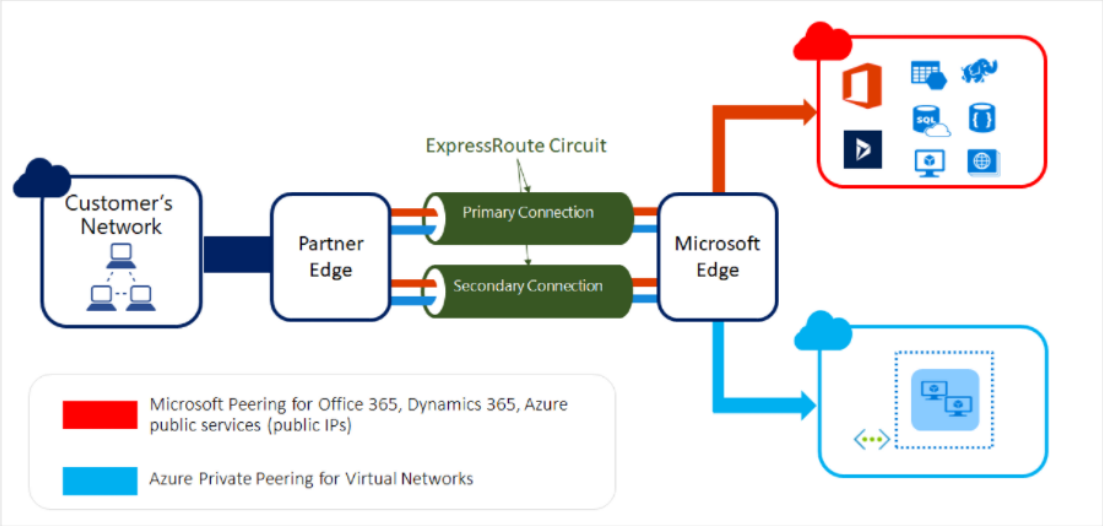
You then connect the various endpoints to the Hub - Azure virtual network, Site-to-Site

Azure ExpressRoute

Azure ExpressRoute

Allows you to connect your on-premises networks to Microsoft cloud over the private connection

Here the connection is established with the help of a connectivity provider



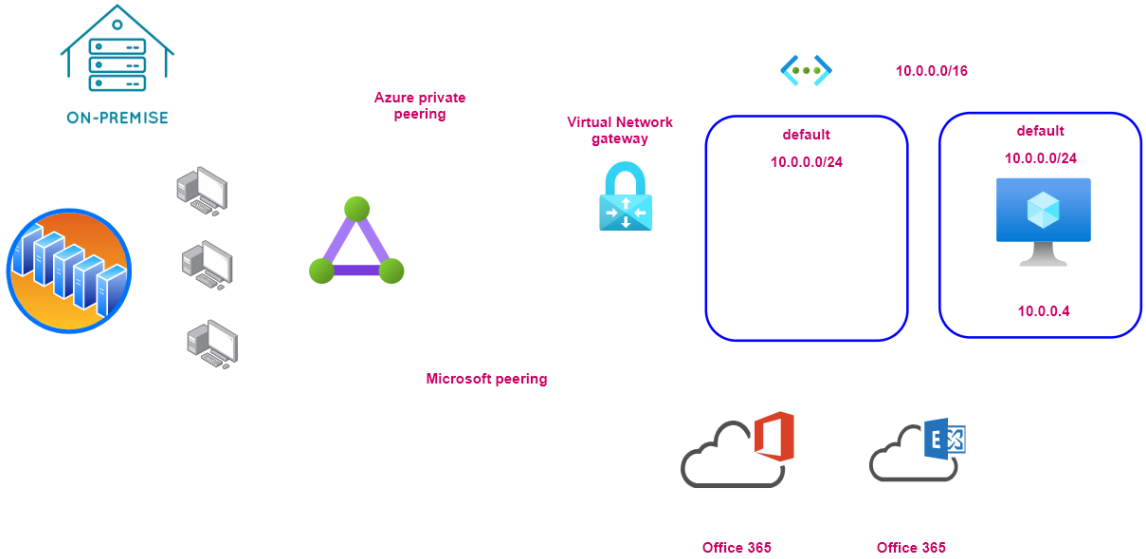
Reference - https://docs.microsoft.com/en-ca/azure/expressroute/expressroute-introduction

The ExpressRoute connection does not go over the public Internet

Your connections are more reliable, faster and you get less latency

You get two connections for each ExpressRoute circuit for redundancy

Azure ExpressRoute peering connections



Azure ExpressRoute - SKU and Subscription

ExpressRoute connectivity

Local SKU **Standard SKU** **Premium SKU**

With Local SKU , you get connectivity to one region

With Standard SKU , you get connectivity to a geopolitical region

Azure regions to ExpressRoute locations within a geopolitical region.

The following table provides a map of Azure regions to ExpressRoute locations within a geopolitical region.

Geopolitical region	Azure regions	ExpressRoute locations
Australia Government	Australia Central, Australia Central 2	Canberra, Canberra2
Europe	France Central, France South, Germany North, Germany West Central, North Europe, Norway East, Norway West, Switzerland North, Switzerland West, UK West, UK South, West Europe	Amsterdam, Amsterdam2, Berlin, Copenhagen, Dublin, Dublin2, Frankfurt, Frankfurt2, Geneva, London, London2, Madrid, Marseille, Milan, Munich, Newport(Wales), Oslo, Paris, Stavanger, Stockholm, Zurich
North America	East US, West US, East US 2, West US 2,West US 3, Central US, South Central US, North Central US, West Central US, Canada Central, Canada East	Atlanta, Chicago, Chicago2, Dallas, Denver, Las Vegas, Los Angeles, Los Angeles2, Miami, Minneapolis, Montreal, New York, Phoenix, Quebec City, Queretaro(Mexico), Quincy, San Antonio, Seattle, Silicon Valley, Silicon Valley2, Toronto, Toronto2, Vancouver, Washington DC, Washington DC2

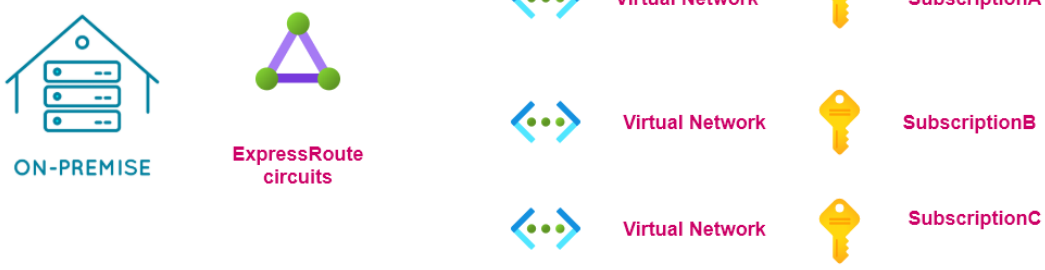
Reference - https://docs.microsoft.com/en-us/azure/expressroute/expressroute-locations#locations

Premium SKU

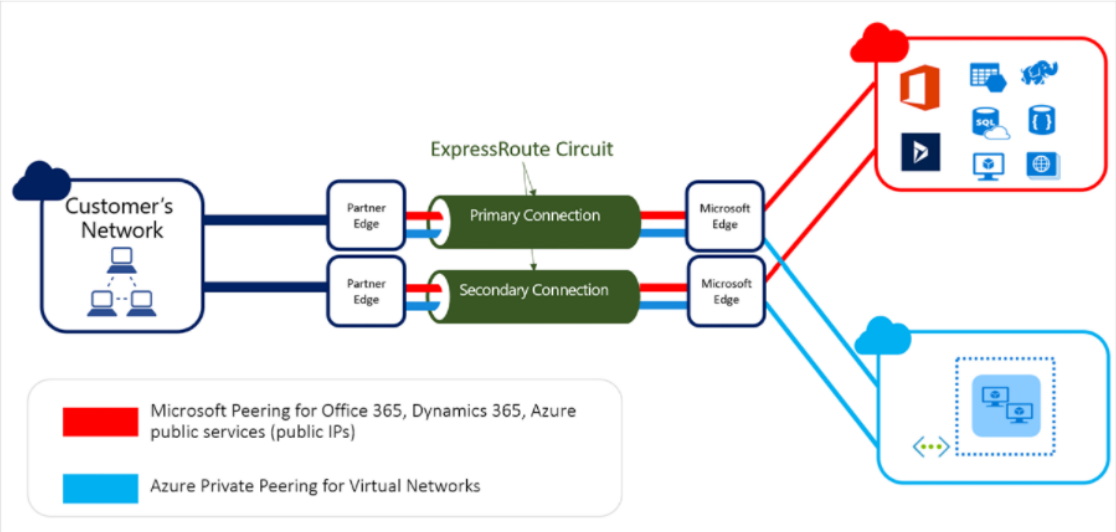
You can connect your ExpressRoute circuit to locations beyond the geo-political boundaries

ExpressRoute circuits for multiple subscriptions

You can share your ExpressRoute circuit across multiple subscriptions



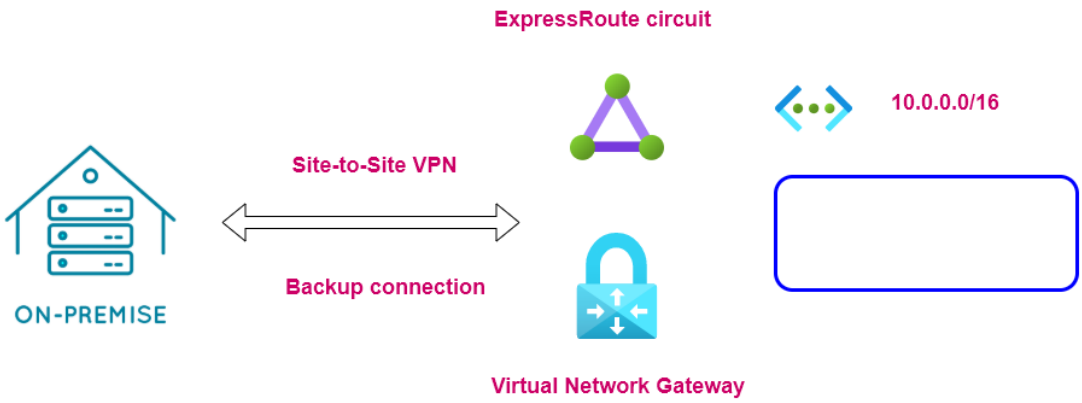
Azure ExpressRoute - High Availability



Reference - https://docs.microsoft.com/en-ca/azure/expressroute/designing-for-high-availability-with-expressroute

Each ExpressRoute circuit by default has two connections which work in active-active mode

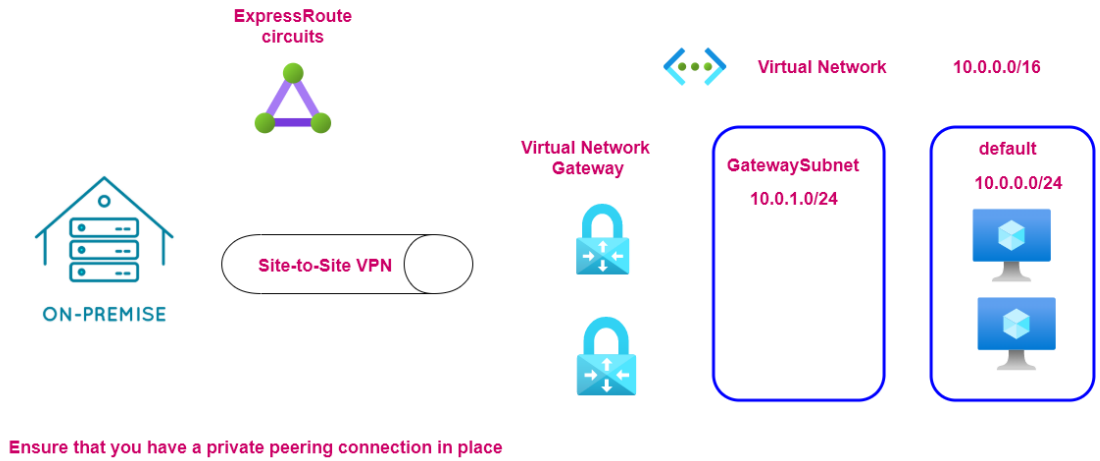
If one connection fails, all traffic can be diverted to the other connection



In this scenario only route-based VPN gateway is supported

The gateway subnet must be atleast /27

Azure ExpressRoute - Coexisting Connection – Note



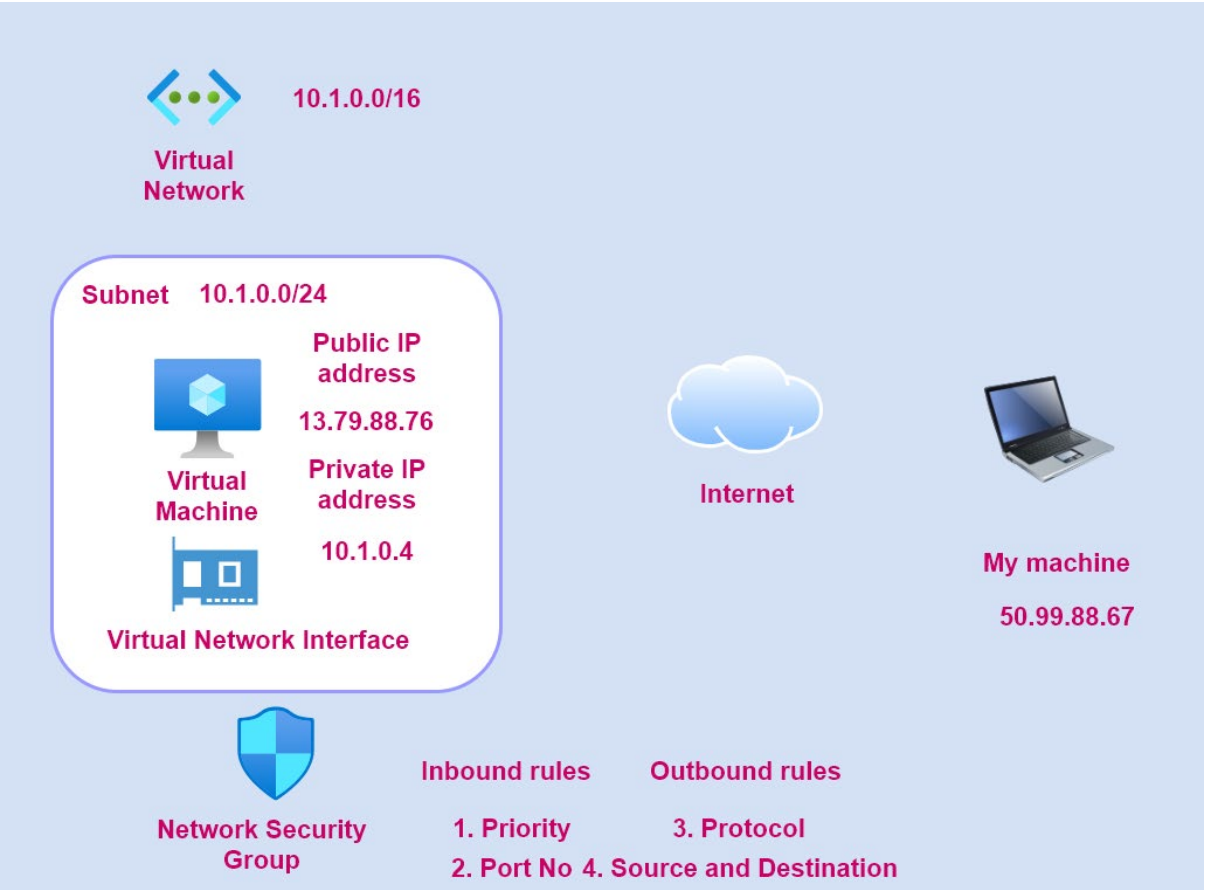
Ensure that you have a private peering connection in place

You can link upto 10 Azure virtual networks to an ExpressRoute circuit

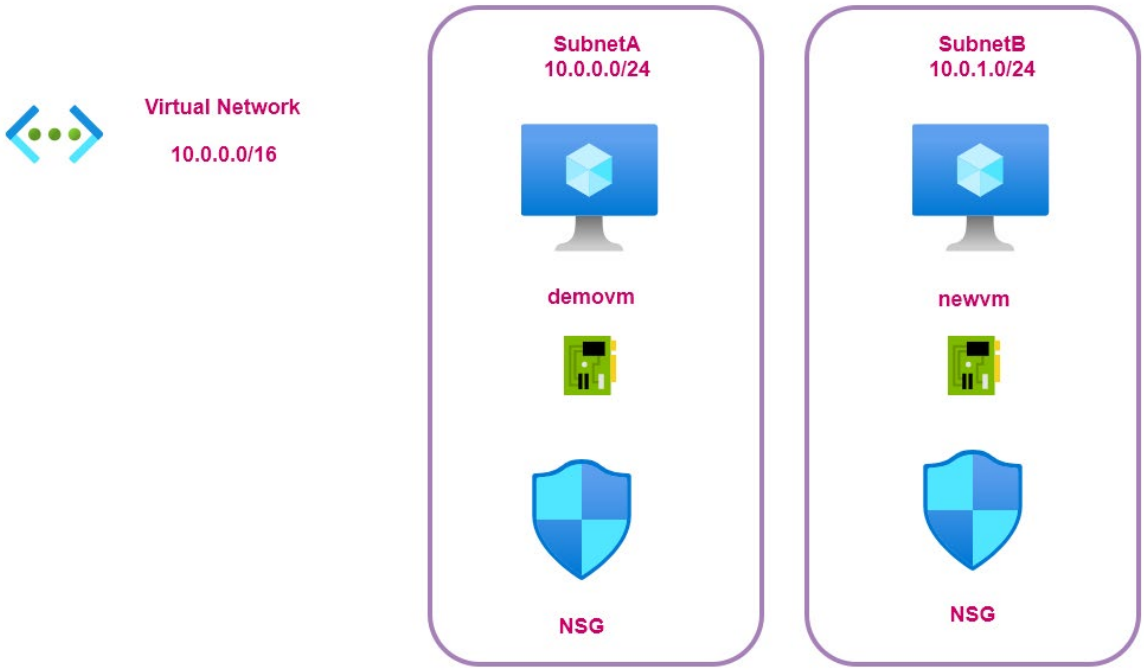
An Aure virtual network can be linked to up to 16 ExpressRoute circuits

Secure and Monitor Networks

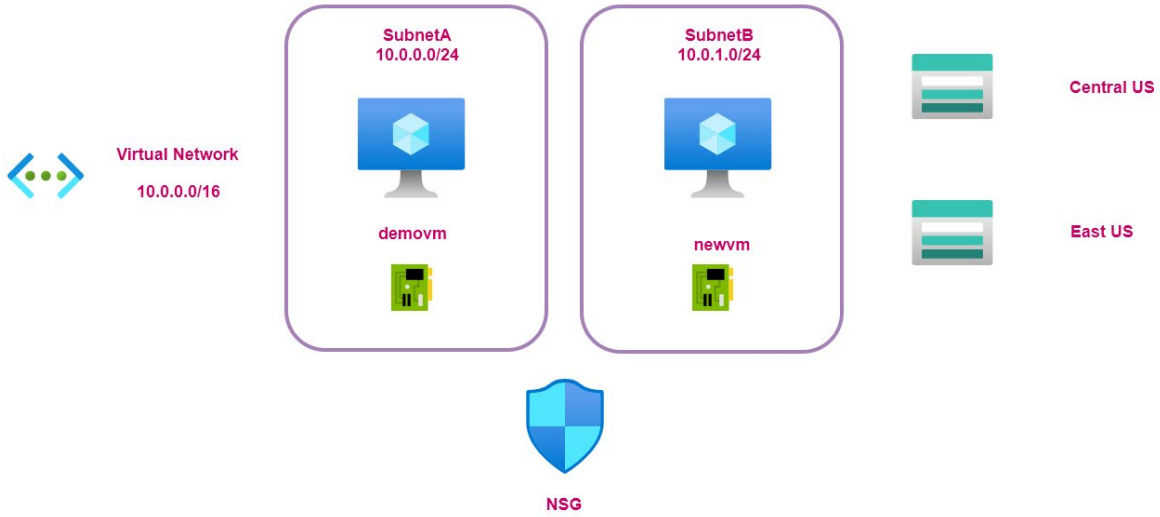
Network Security Groups



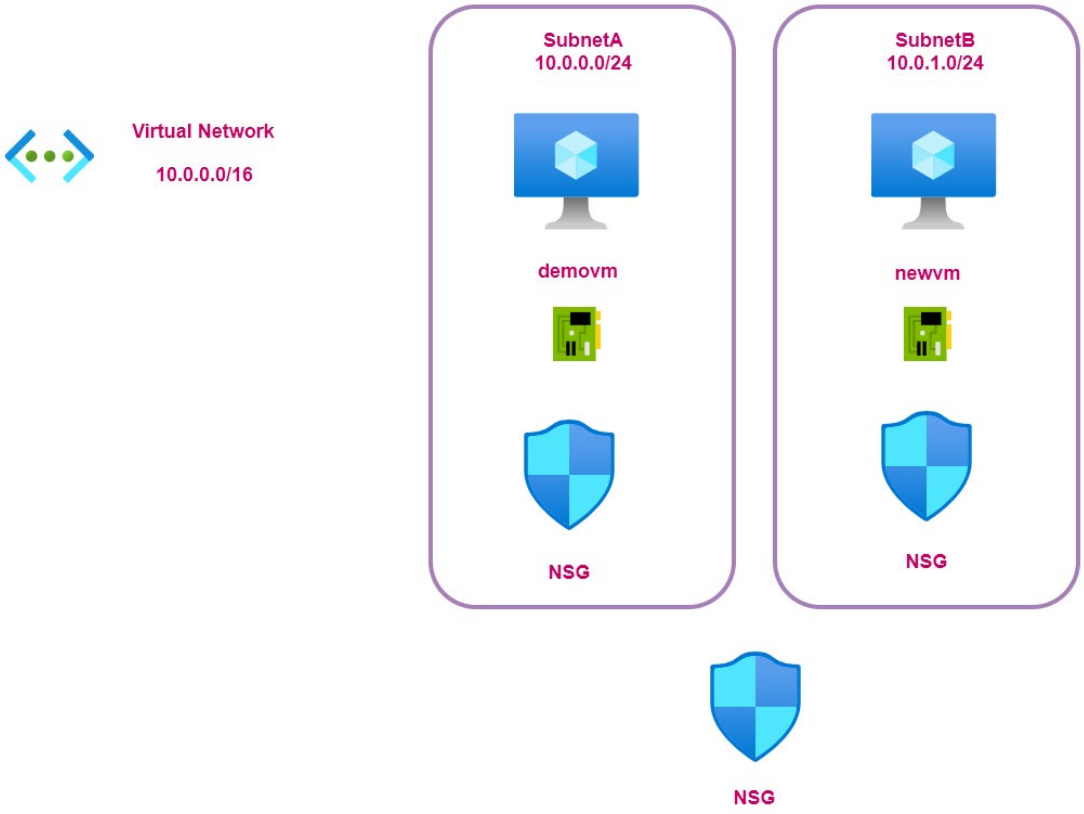
Lab - Network Security Groups - Default Rules



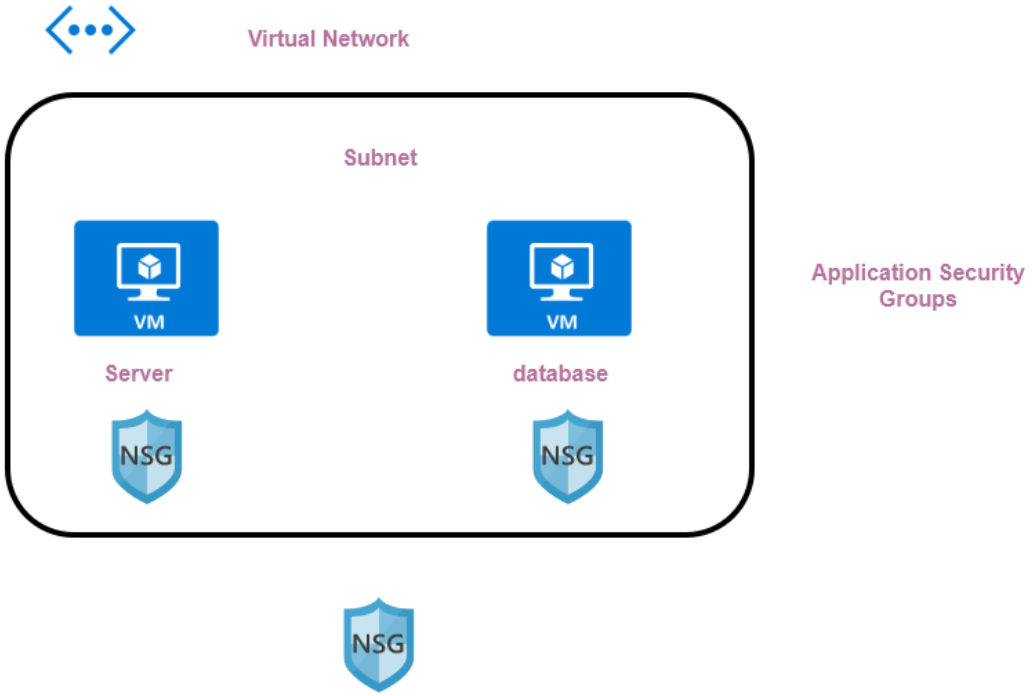
Lab - Network Security Groups - Storage accounts – Setup



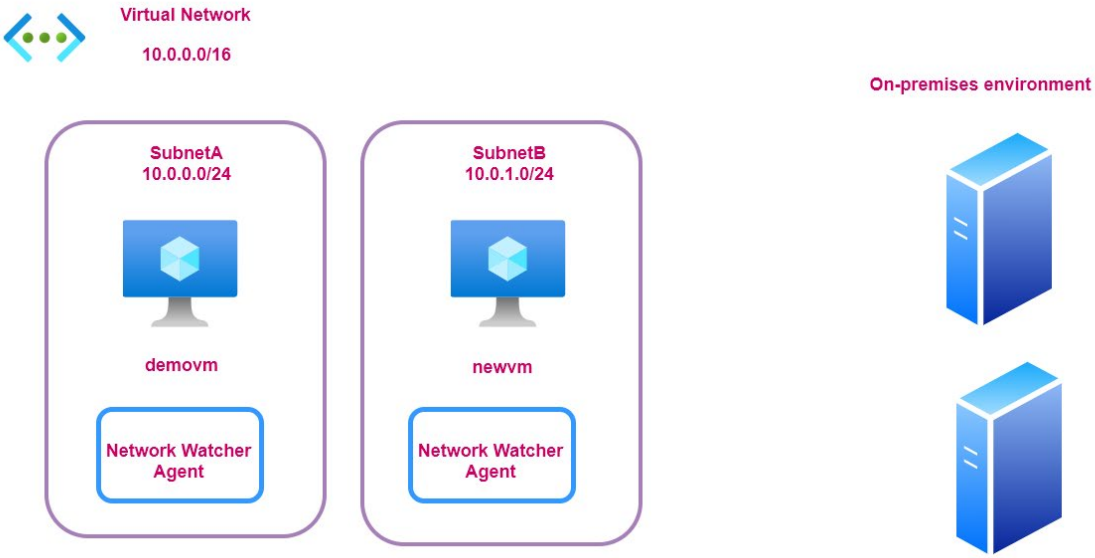
Lab - Network Security Groups - On the Network Interface and Subnet



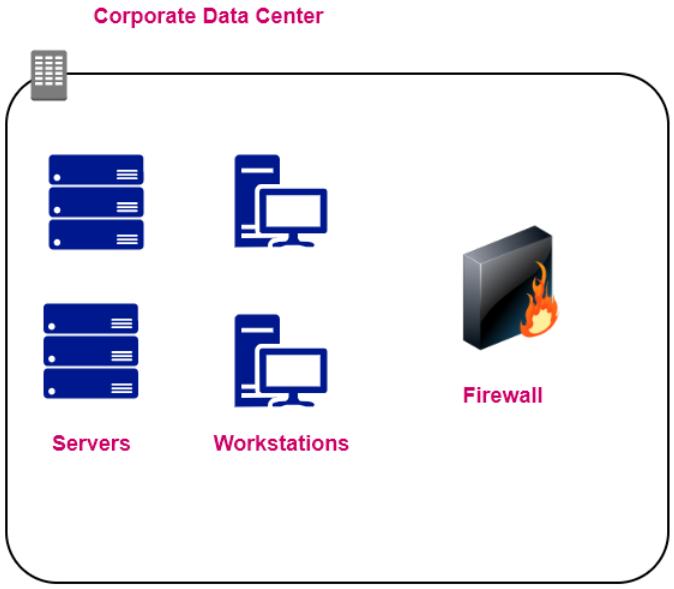
Application Security Groups

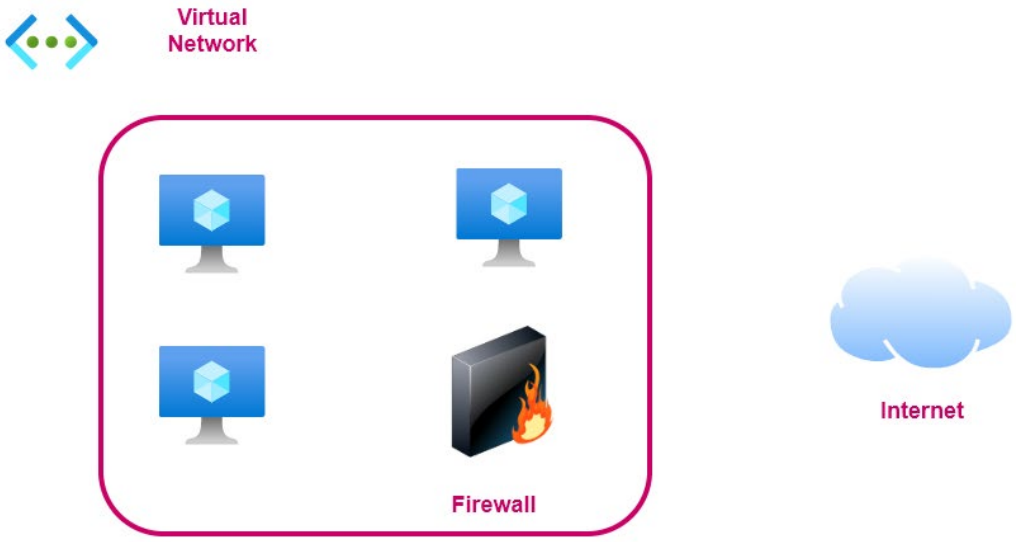


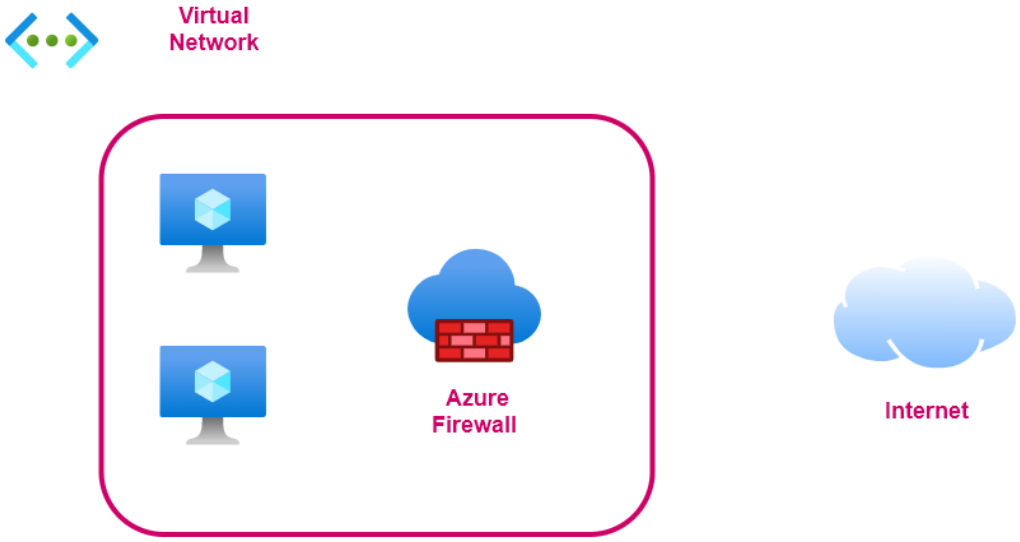
Lab - Network Watcher - Connection Monitor



Azure Firewall







1. Has built-in high availability

2. Can deploy the Azure Firewall Instance across two or more Availability zones - 99.99% SLA

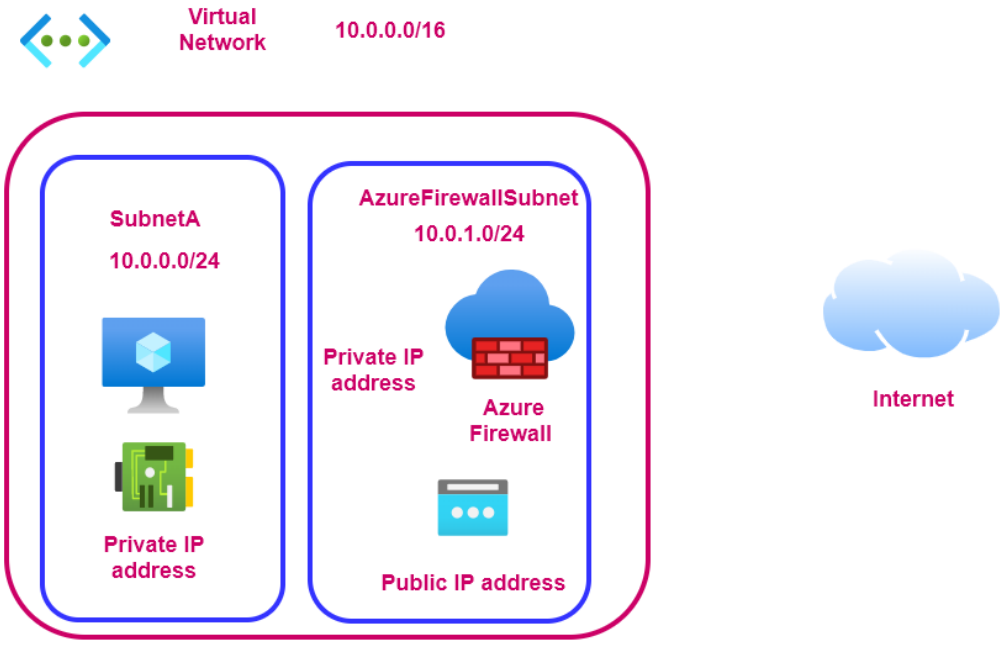
3. You can filter traffic based on fully-qualified domain names

4. You can also create network filtering rules - Based on source and destination IP address, port and protocol

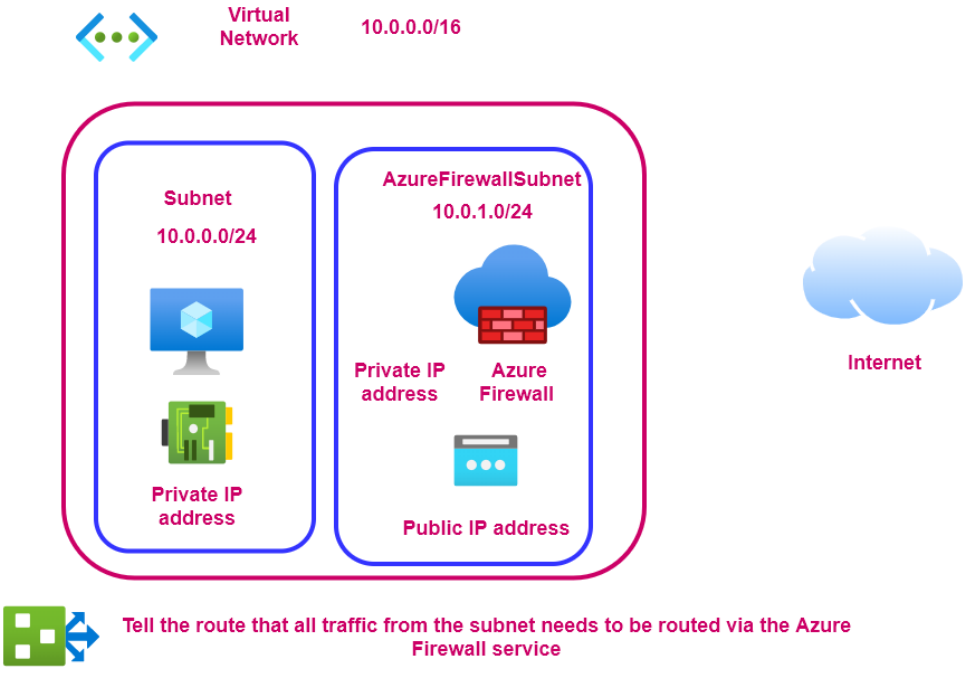
5. It is stateful in nature, so it understands what packets of data to allow

6. It has built-in Threat Intelligence - Here you can get alerts or deny traffic from/to malicious IP addresses and domains

Lab - Azure Firewall – Deployment



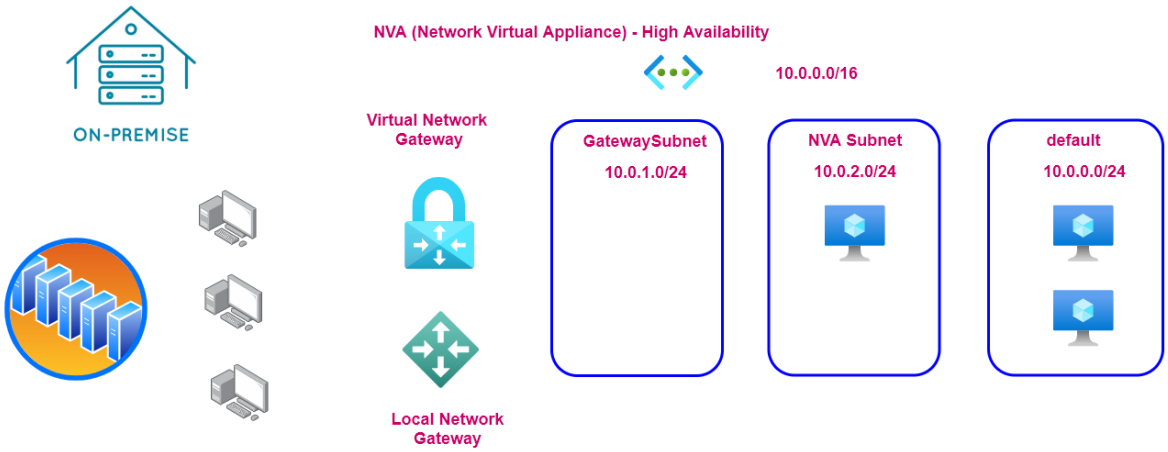
Step 1 : Create our virtual network and Azure Firewall appliance



Tell the route that all traffic from the subnet needs to be routed via the Azure Firewall service

Step 2 : Create a route table and assign it to the Subnet hosting the virtual machine

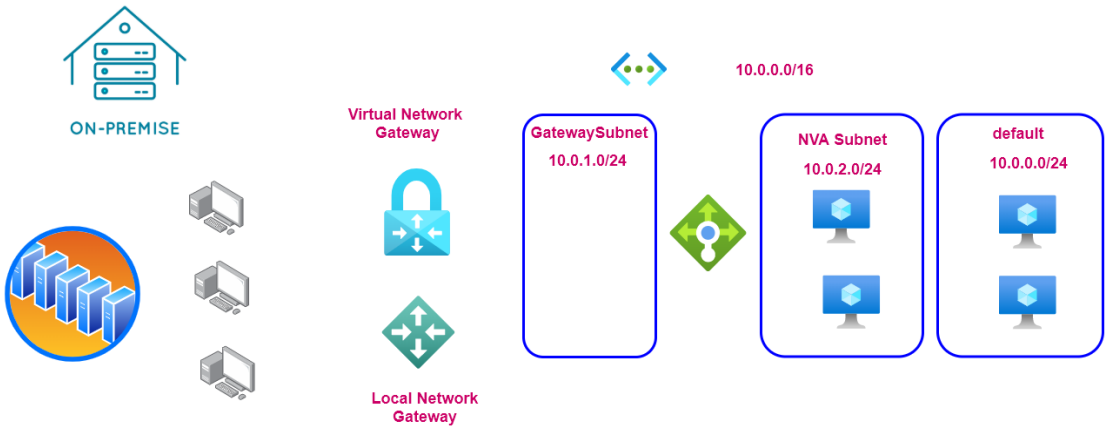
Note on Network Virtual Appliance High Availability



The Network appliance is used to filter the incoming and outgoing traffic

Here if you have just one virtual machine to support the appliance, it could be a point of failure

In such a case you should look at high availability options

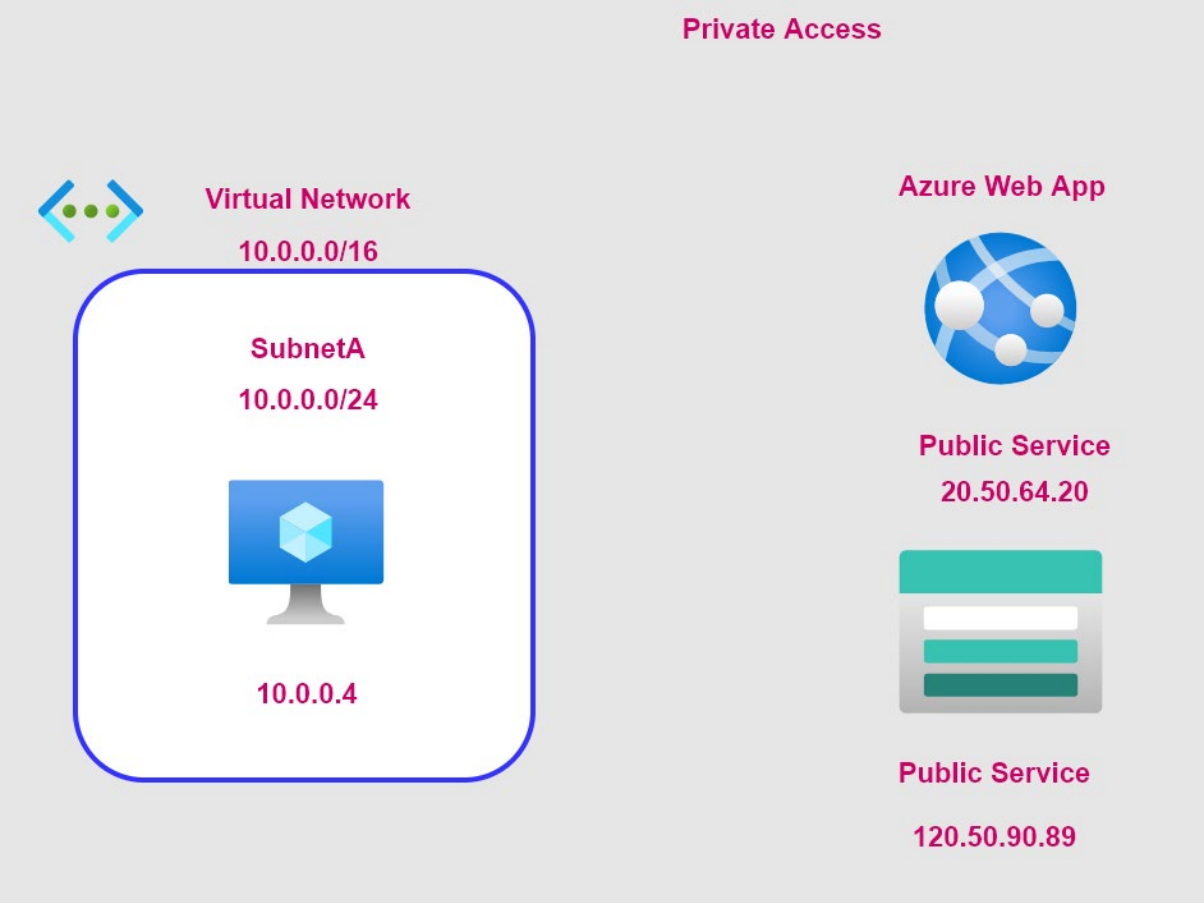


Here you can use a Standard Load Balancer with High Availability Ports to distribute traffic across the NVA's.

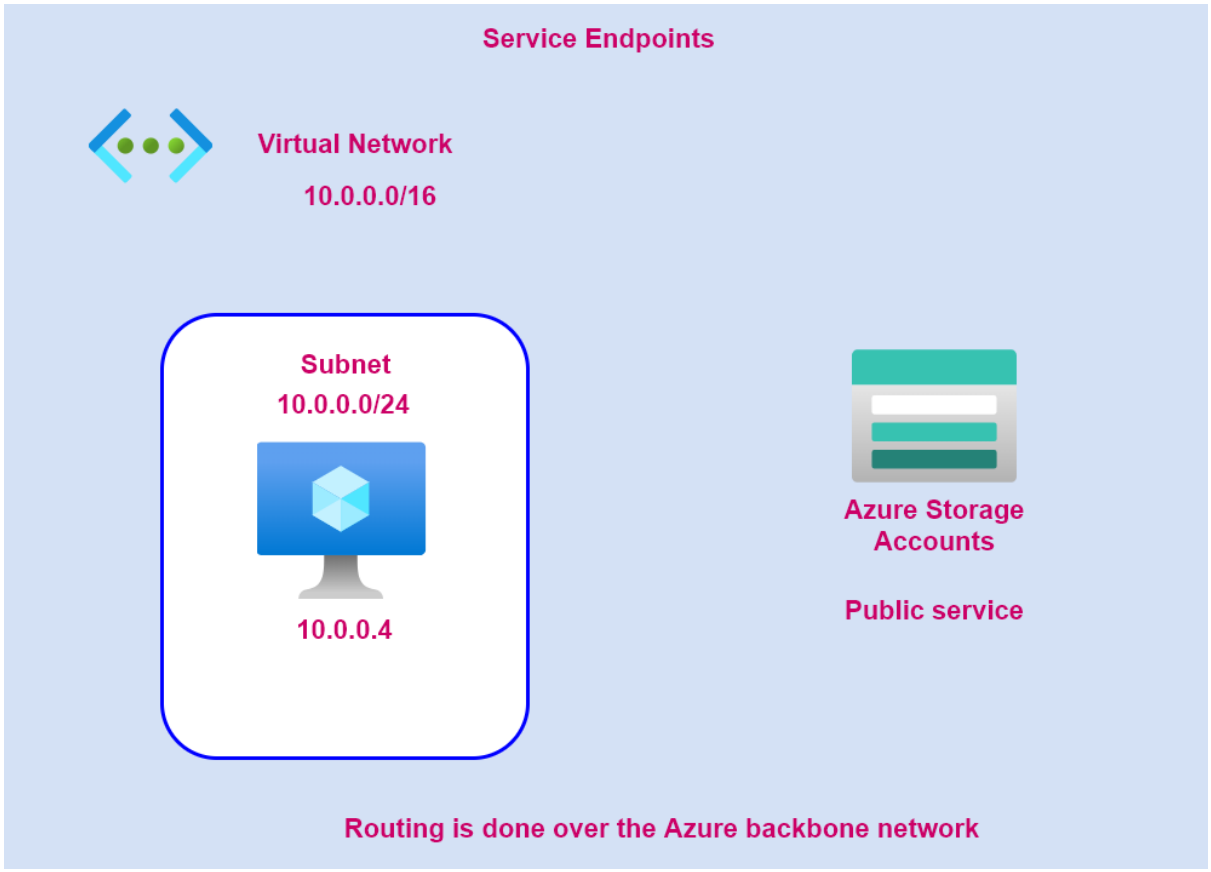
Whitelisting IP Addresses

Design and Implement Private Access to Azure Services

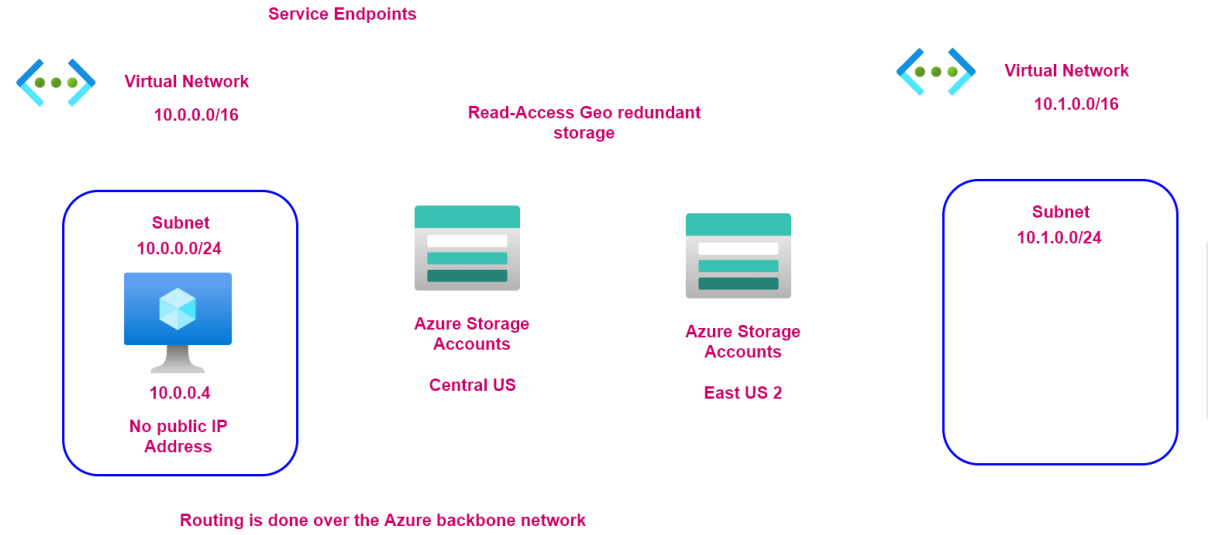
Why consider private access to resources



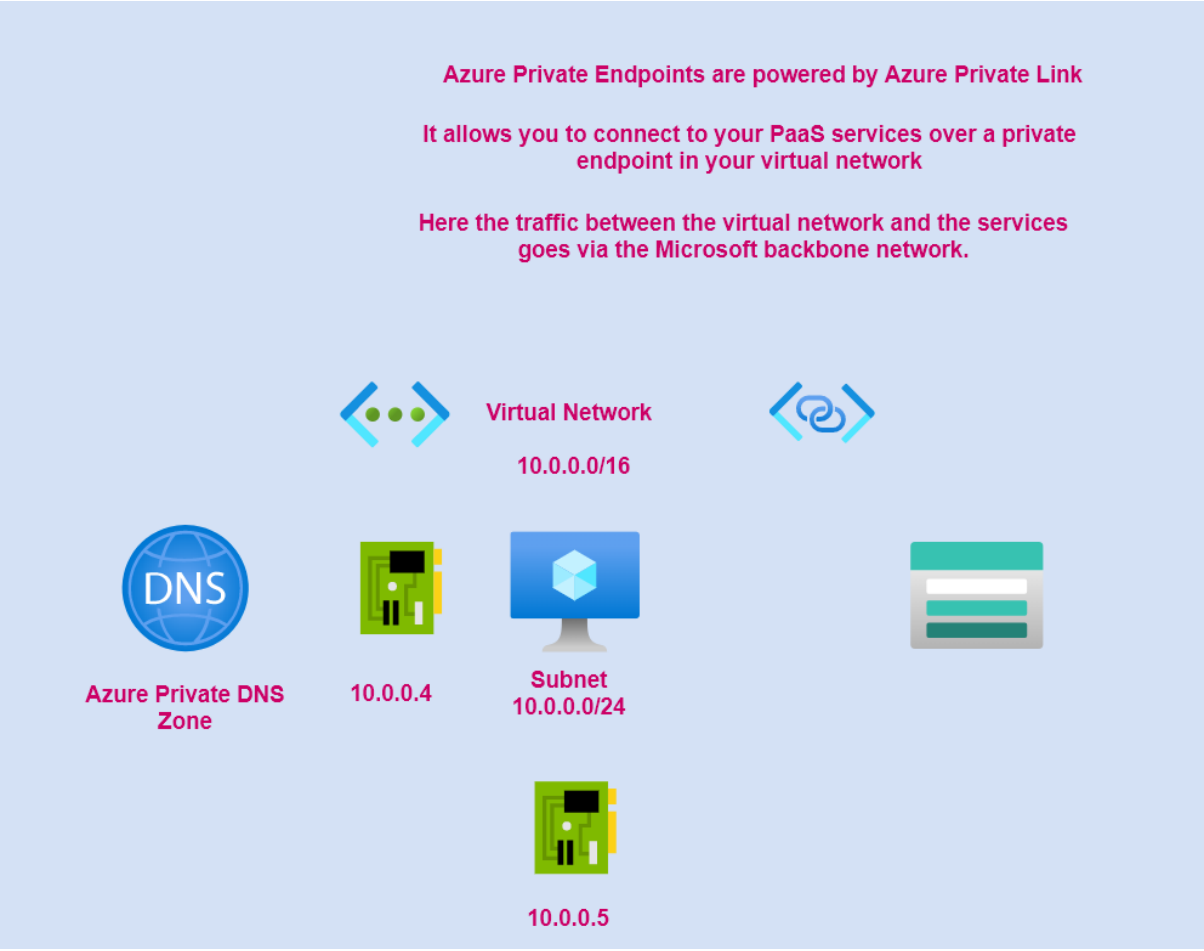
Service endpoints



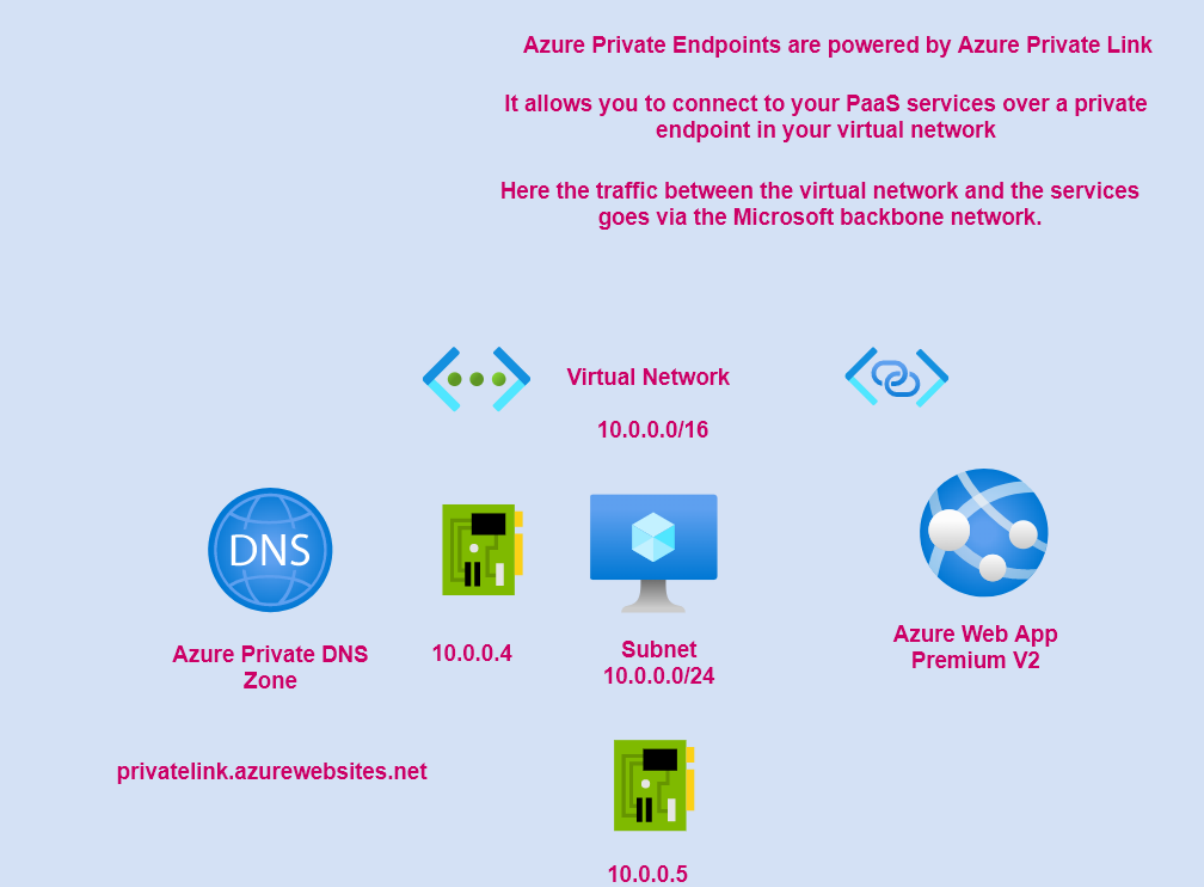
Service endpoints - Secondary location



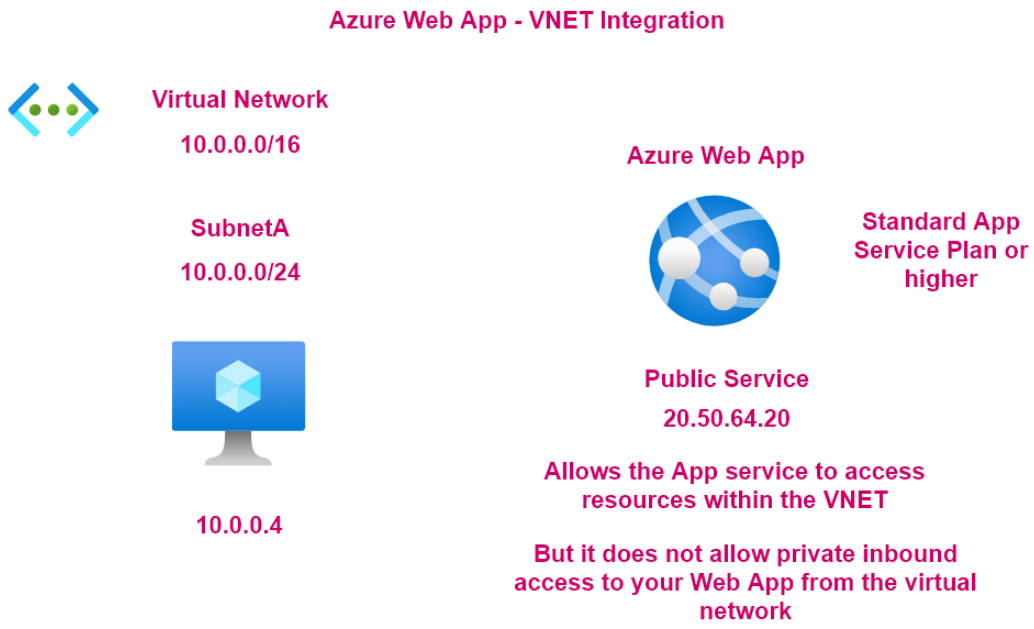
Private Endpoint



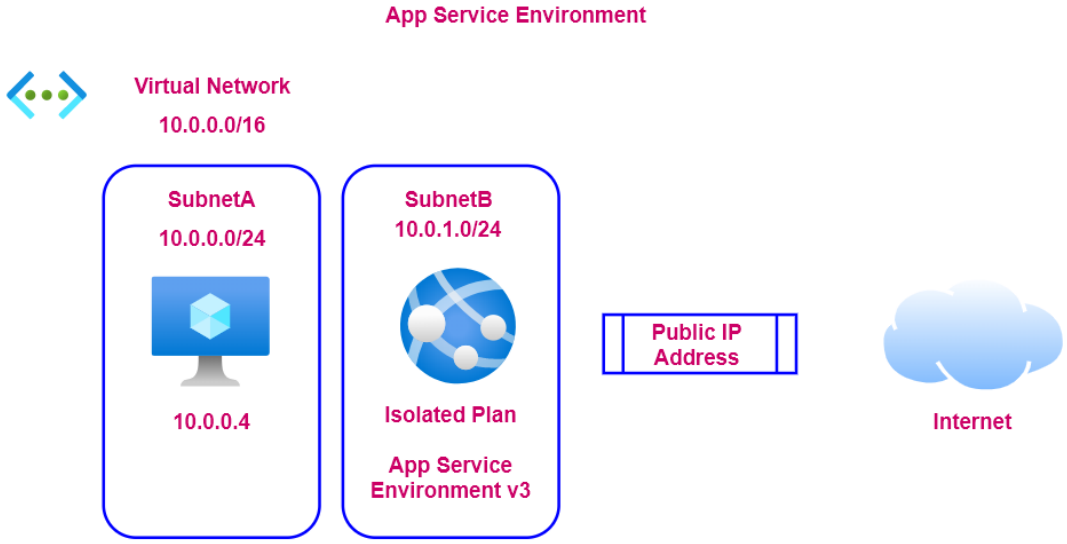
Azure Web App - Private Endpoint



Azure Web App - VNET Integration



Azure Web App - App Service Environment

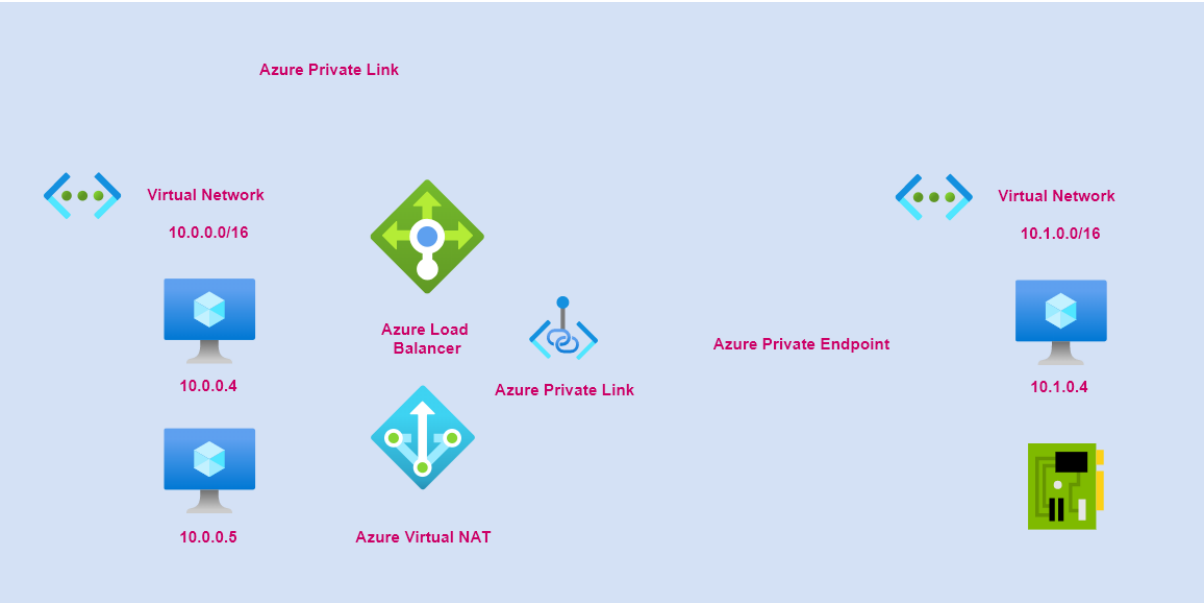


All App Service Environments have a public VIP that is used for inbound management traffic

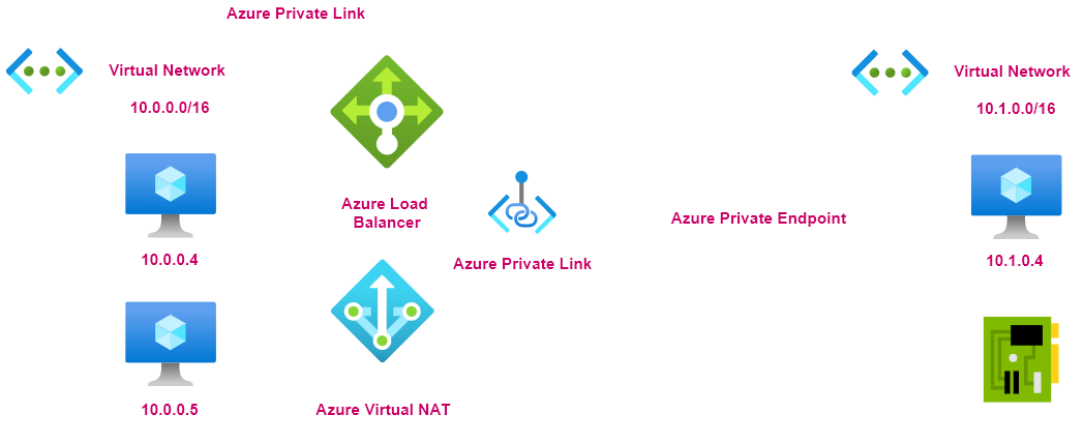
With App Service Environment v2, you can deploy an internal load balanced App Service Environment or an External ASE

With the External ASE, you can use the public IP address as the endpoint to resolve HTTP/HTTPS , FTP/FTPS, Web deployment, Remote debugging

Private Link

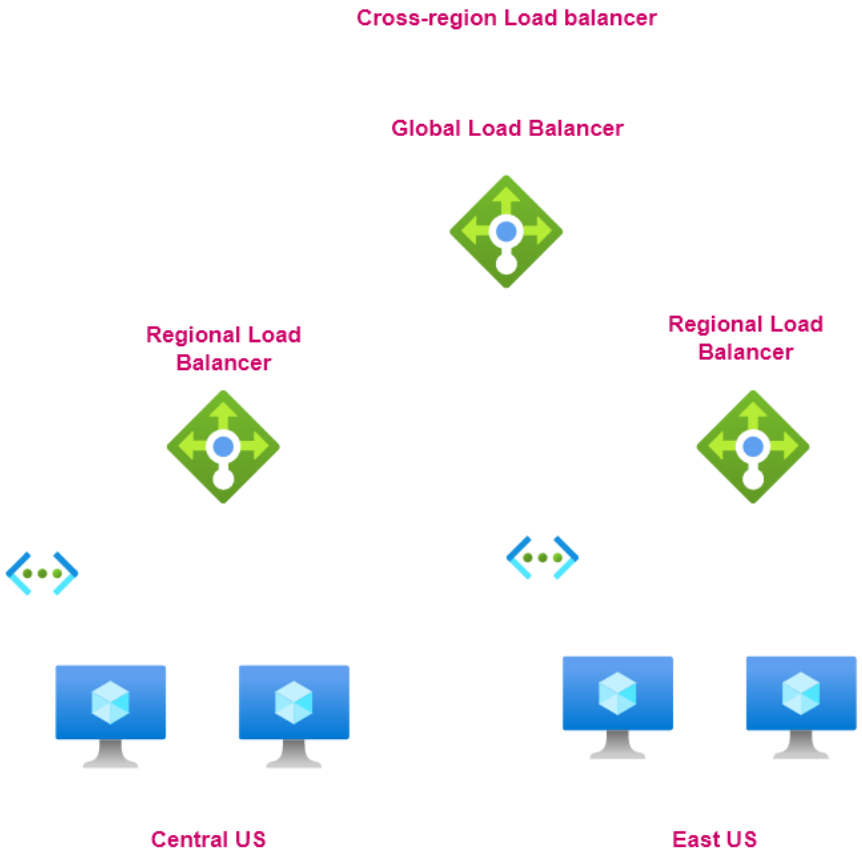


Lab - Azure Private Link

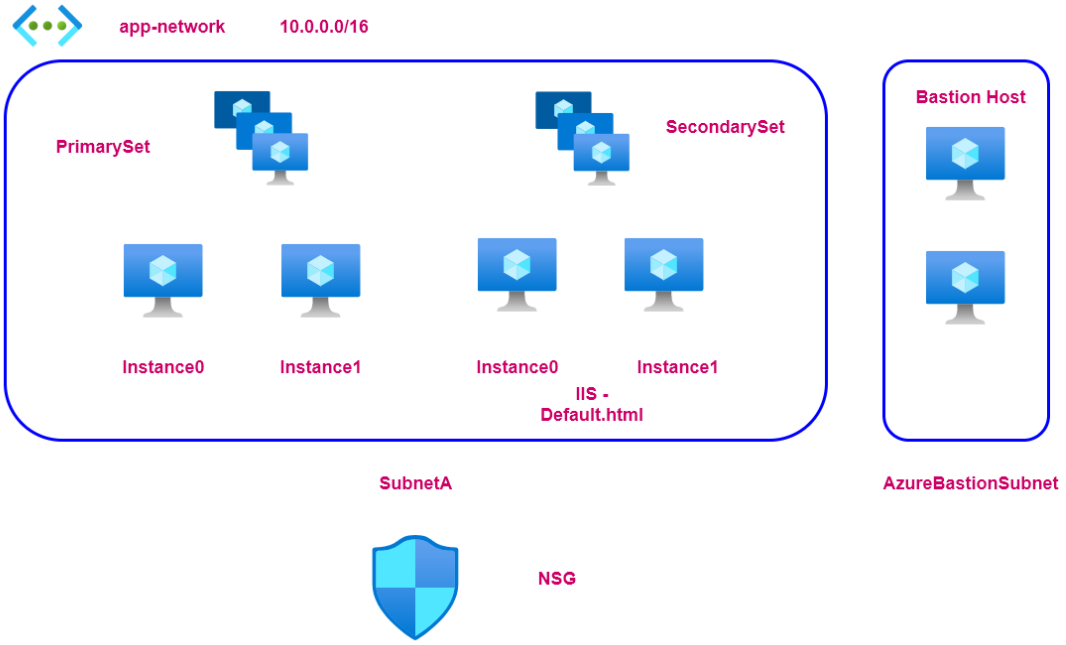


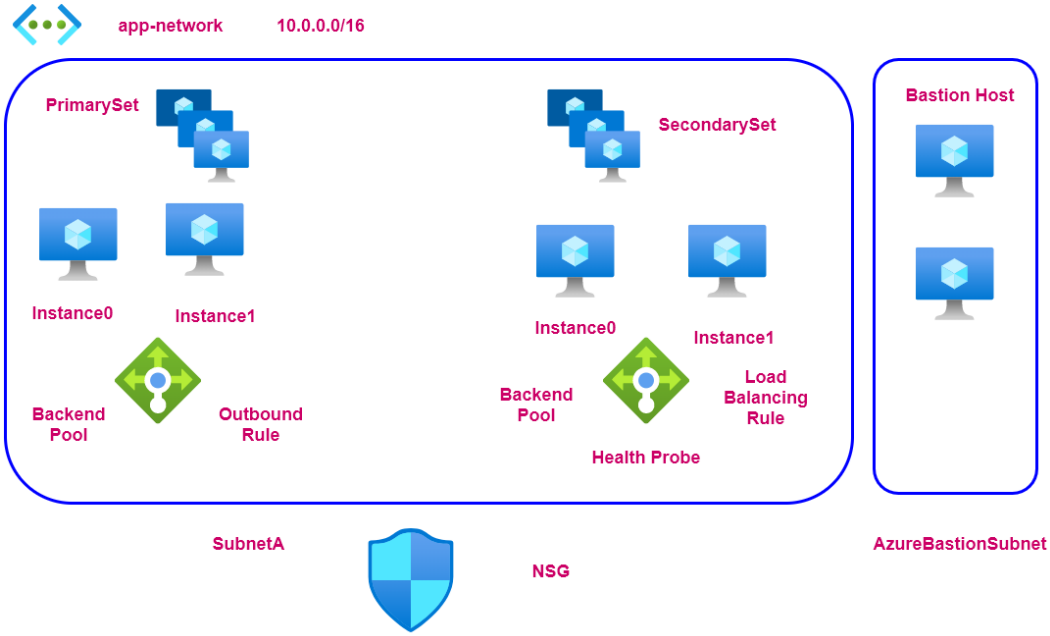
Further Learning

Cross-Region Load Balancer

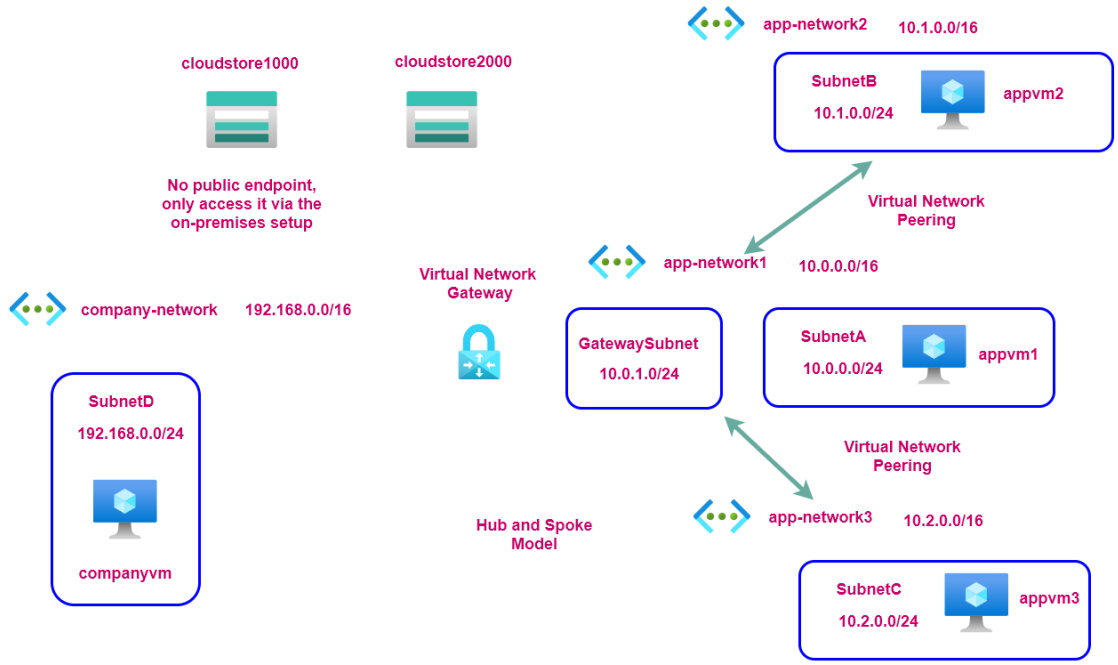


Lab - Virtual Machine Scale Sets in a virtual network

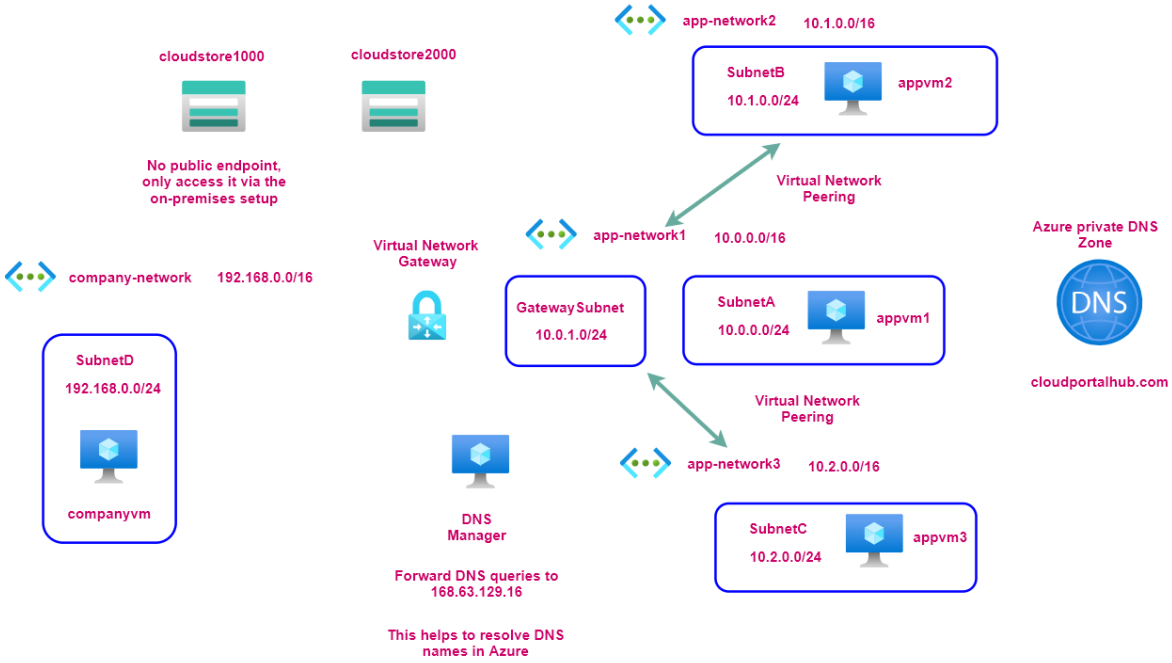




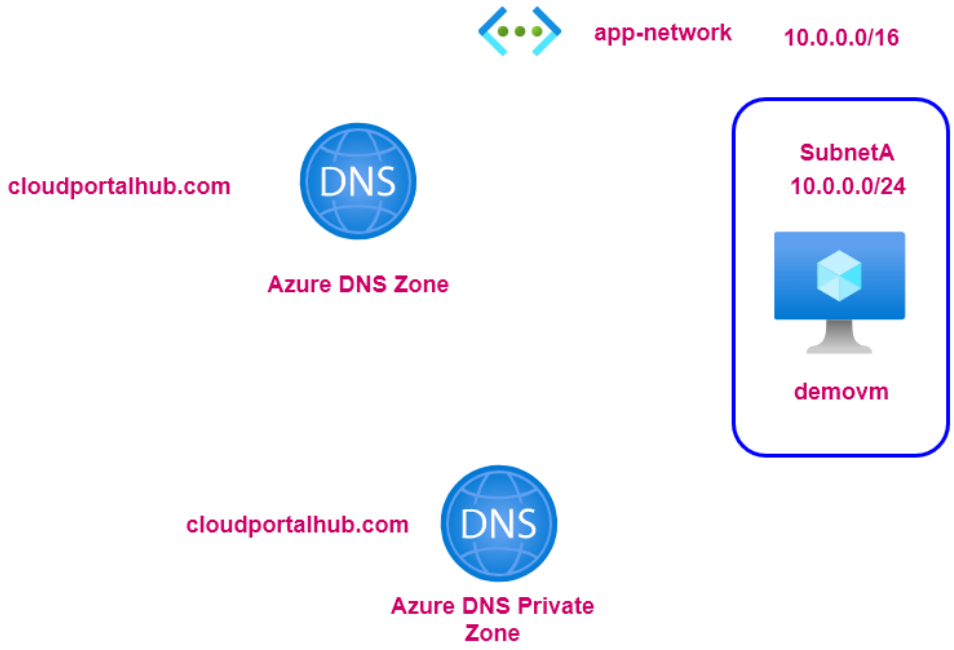
Reference Architecture Overview



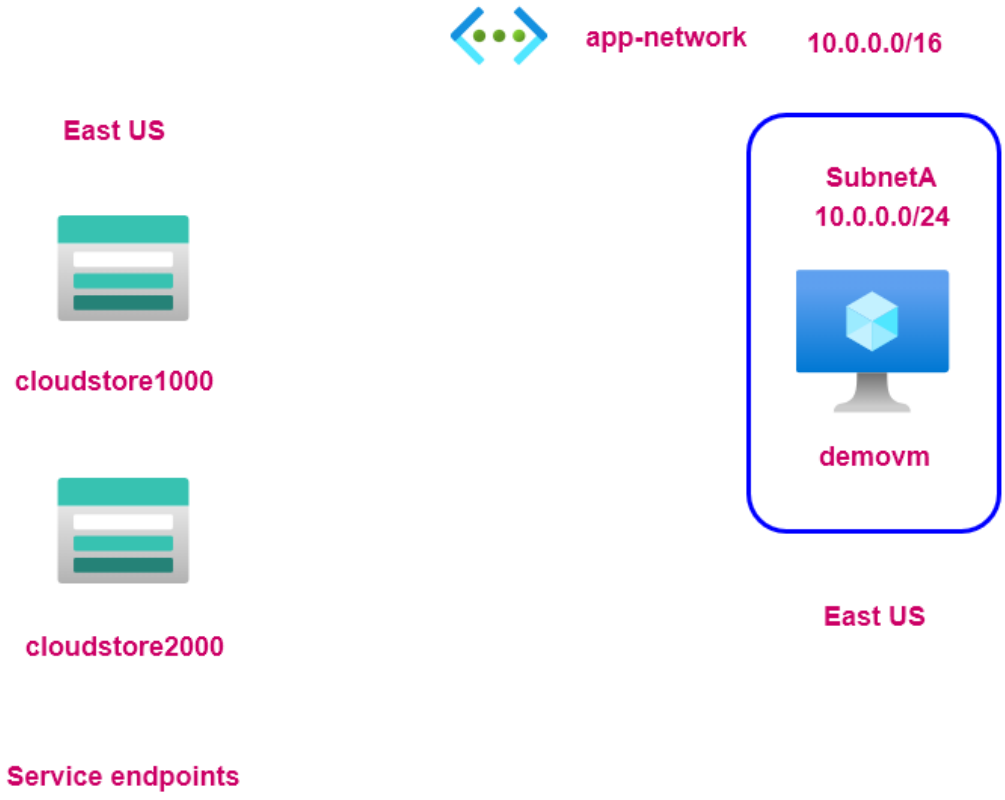
Reference Architecture - Azure Private DNS Zone



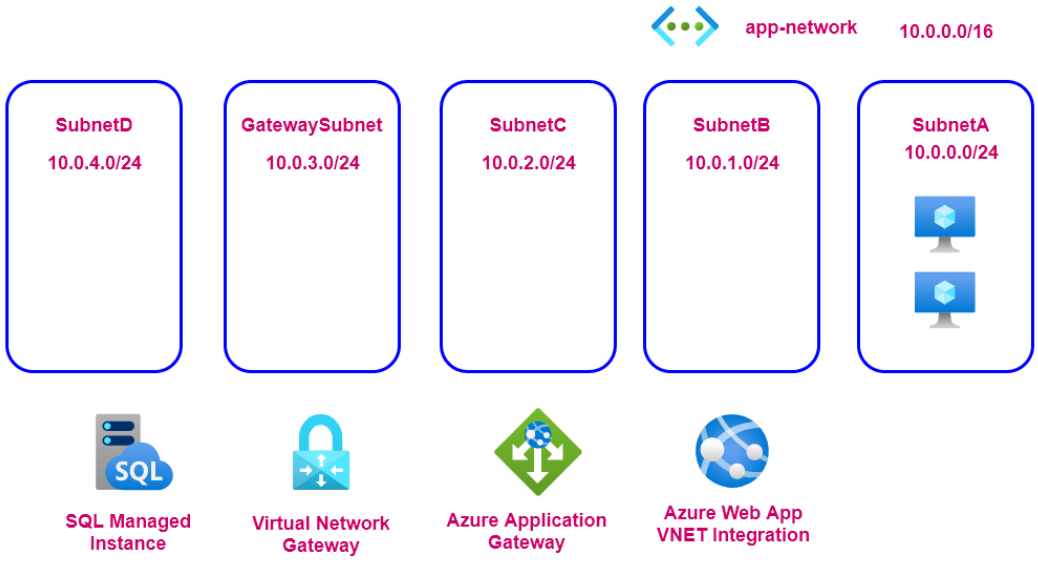
Having the same Azure DNS and Azure Private DNS Zone



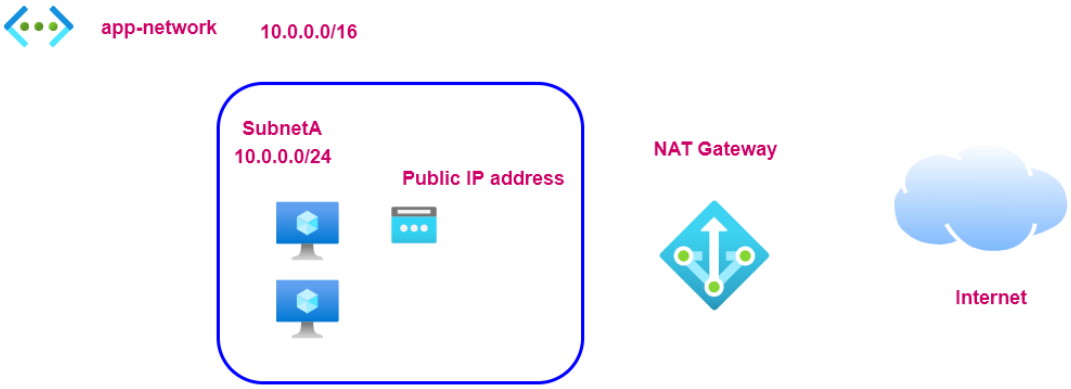
Limiting access to storage accounts from a virtual machine



Subnet Requirements



NAT Gateway - Important points



All machines in the subnet will use the NAT gateway for outbound connectivity

You can assign the NAT gateway to multiple subnets. But the NAT gateway can't be assigned across virtual networks

Reference Architecture - Azure Firewall