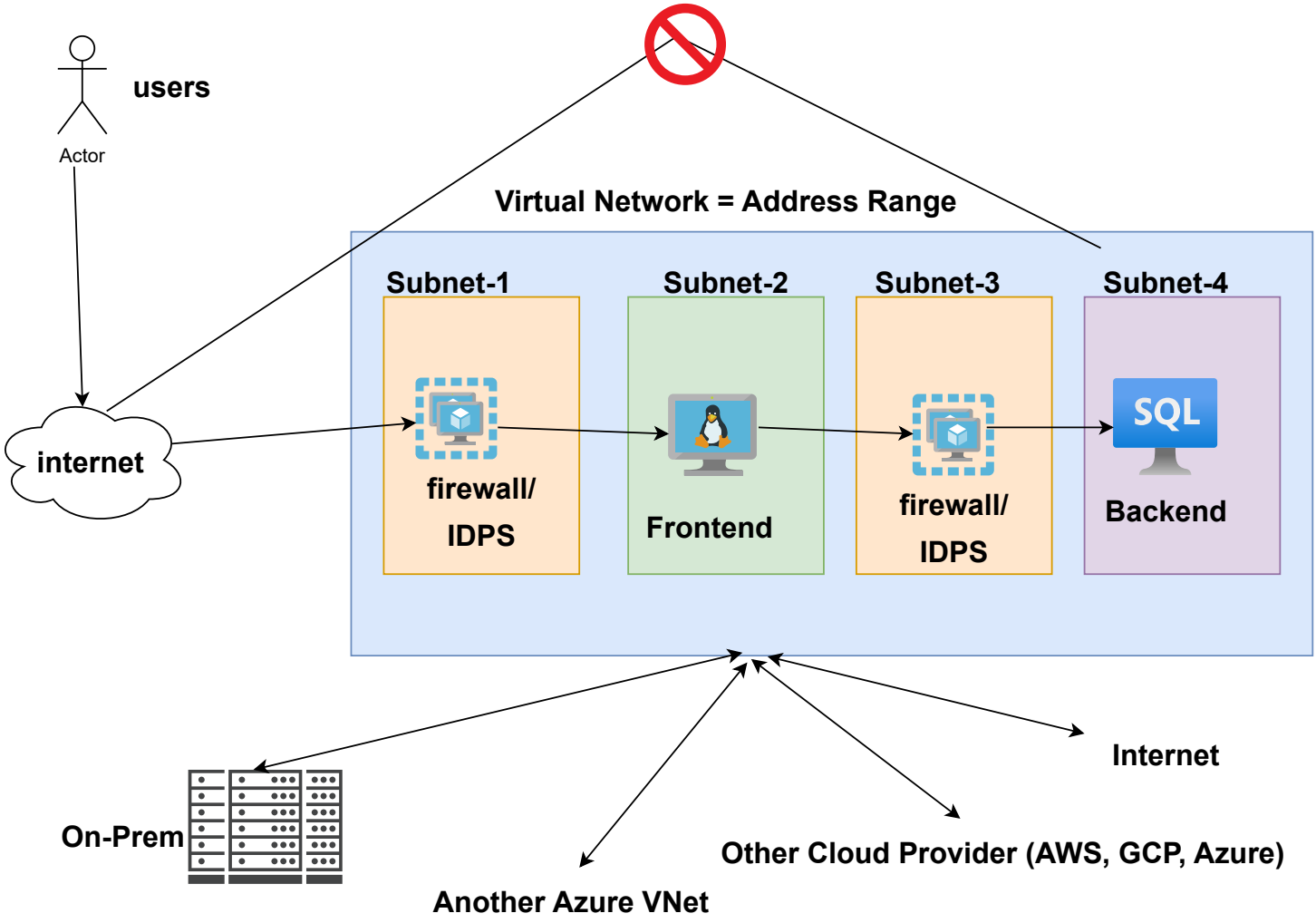


IP traffic stays entirely within our global network and never enters the public Internet

What is Subnet

- Part of a network having unique address range within network
- Firewall rules, Routing, etc Network config at subnet
- Every Machines within subnet gets effected
- "Seperation of concern"
- 1 subnet = 1 functional Requirement

example: Seperate subnets for Firewall, VPN

- components of app

+61 Mobile Number => Australia ==> Address Range ==> Network

NSW

Best Practice :

- Think of future (same address range as on-prem 🚫)

- CHeck MS FAQ address Range

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

Address resrved in subnet

Yes. Azure reserves the first four addresses and the last address, for a total of five IP addresses within each subnet.

Address Range = CIDR Notation

Public = Internet

IP address: Unique Number to Identiy a machine within local network OR Internet

Private IP
- Mandatory
- from your subnet
- Helps in Local Private communication

Public IP
- optional
- helps in connecting internet
- charged $$

https://azure.microsoft.com/en-in/explore/global-infrastructure/global-network

Public IP addresses allow internet resources to communicate inbound to your Azure resources. You can also associate public IP addresses to Azure resources, like virtual machines, to communicate to the internet and public facing Azure services.

NIC Card = gives connectivity to vm

A public IP address prefix is a reserved range of public IP addresses in Azure.
Public IP prefixes are assigned from a pool of addresses in each Azure region.

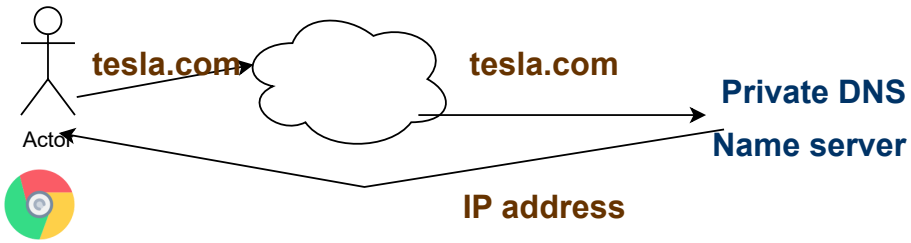
Azure DNS:

Phonebook - Domain Names (tesla.com) => 14.8.9.7

Azure DNS supports both internet-facing
DNS domains and private DNS zones, and provides the following services:

- Private DNS
- Public DNS

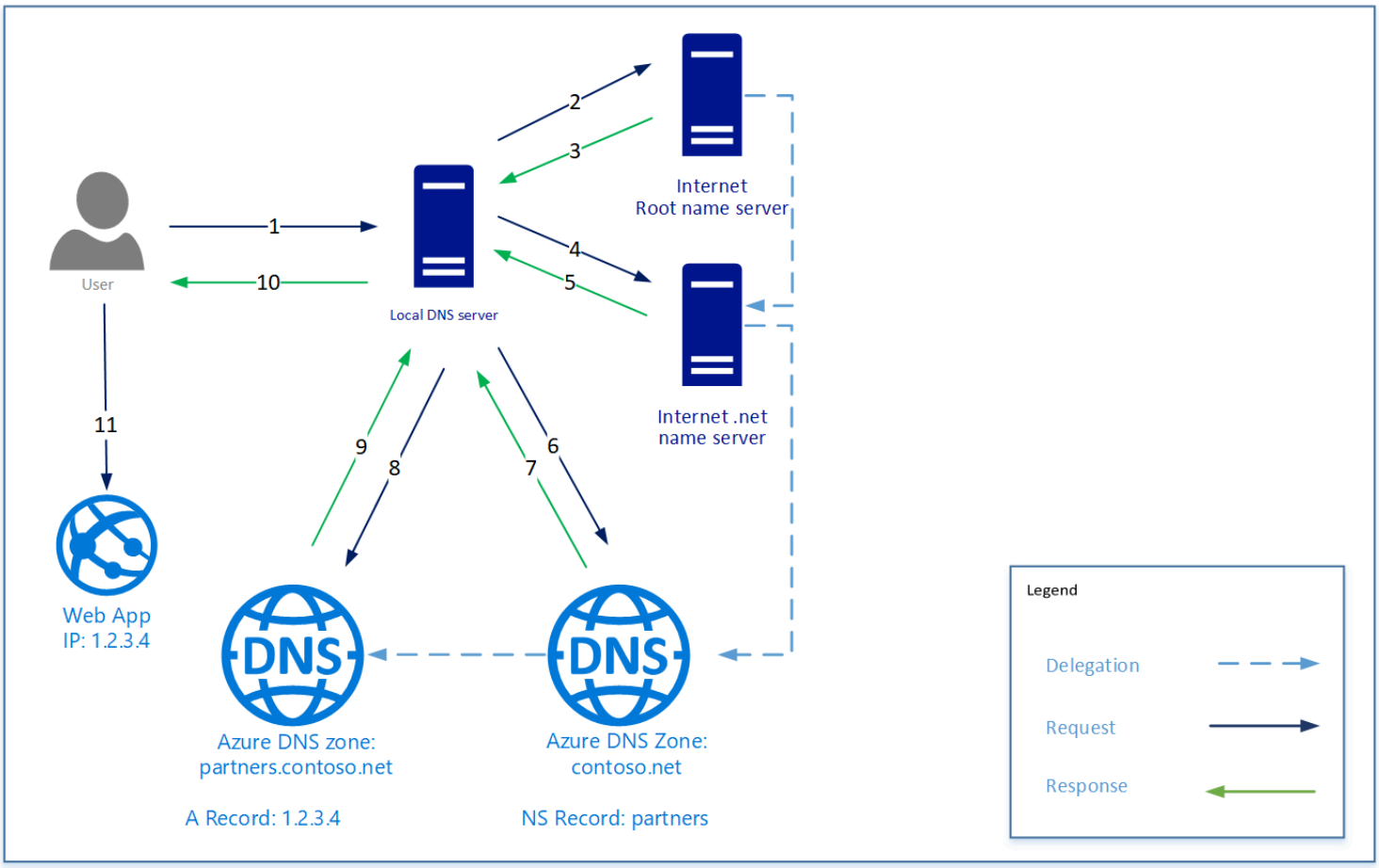
Azure Private DNS is a DNS service
for your virtual networks. Azure Private DNS manages and
resolves domain names in the
virtual network without the need to configure a custom DNS solution.



Public DNS: If you need MS Infra for supporting Name Resolution

Delegate DNS : Purchased DNS

- You Wish MS to handle it



1 vnet = 1 region

For what use cases you would connect two networks together?

1. B2B

2. Merger

3. Hub and Spoke

4. DR

vnet Peering = Connects two Azure Networks

- within same / different subscription, tenant, region

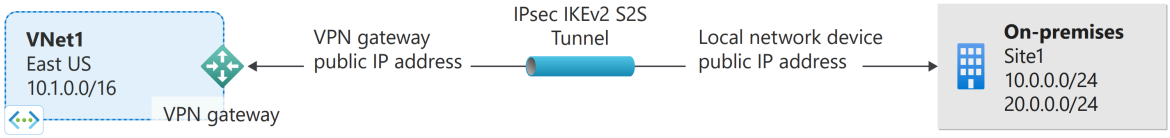
We use route table to route traffic through firewall in hub and spoke

Default Gateway:

Machine that Forwards packet from source to Other Network

to reach other L3 networks, it's routed via default gateway

VPN : encrypting private traffic over public networks



IPsec Tunnel => Sender Encrypt => Reciever Dencrypt => IKEv2

Use Cases:

P2S VPN for WFH

remote office to Cloud

connecting to another site

Cloud to Cloud

Site-site VPN : Network 2 Network

Point to Site VPN: Device to Network

virtual network gateway: Require isolated subnet

Scaling, Bandwidth => Gateway subnet

gateway is used to send encrypted traffic between

your Azure virtual networks or between Azure and your on-premises network.

VPN Connection → **WhatsApp Call**

P2S VPN Protocols:

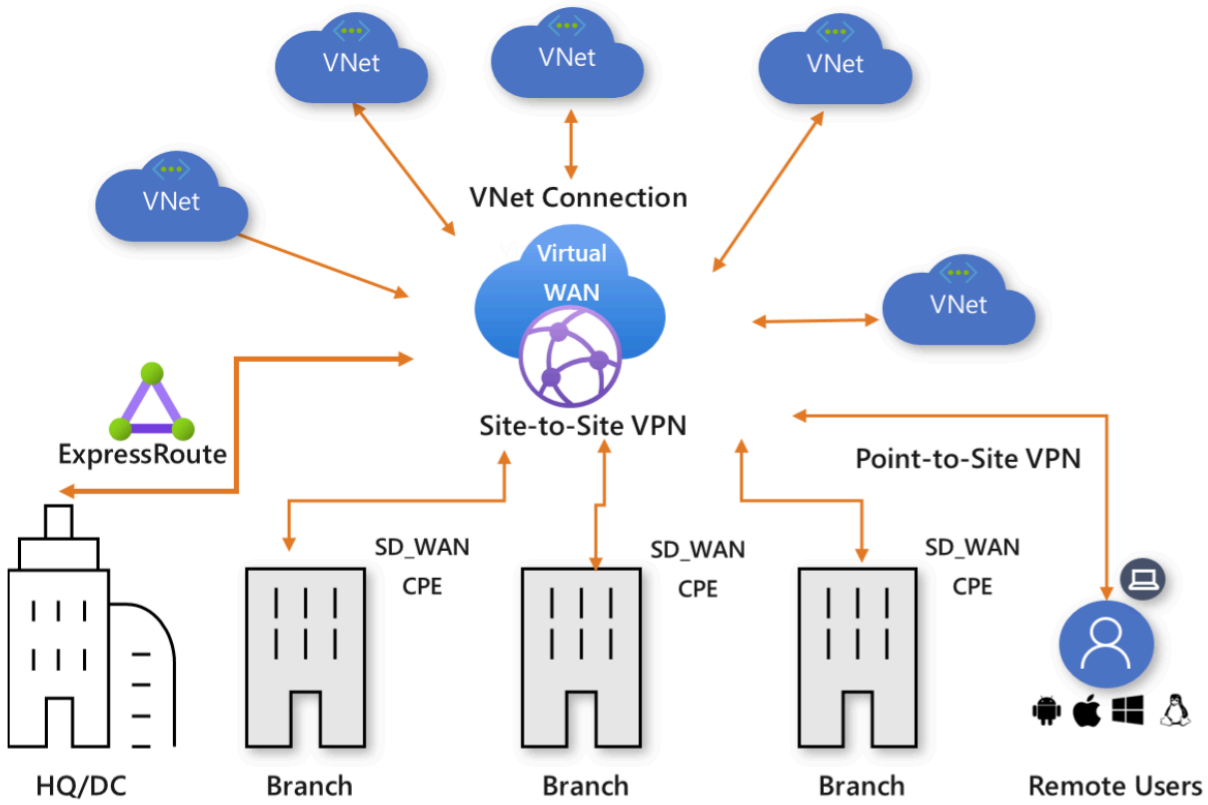
OpenVPN® Protocol, an SSL/TLS based VPN protocol.
A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. OpenVPN
can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux, and Mac devices (macOS versions 10.13 and above).

Secure Socket Tunneling Protocol (SSTP), a proprietary TLS-based VPN protocol.
A TLS VPN solution can penetrate firewalls,
since most firewalls open TCP port 443 outbound, which TLS uses.
SSTP is only supported on Windows devices.
Azure supports all versions of Windows that have
SSTP and support TLS 1.2 (Windows 8.1 and later).

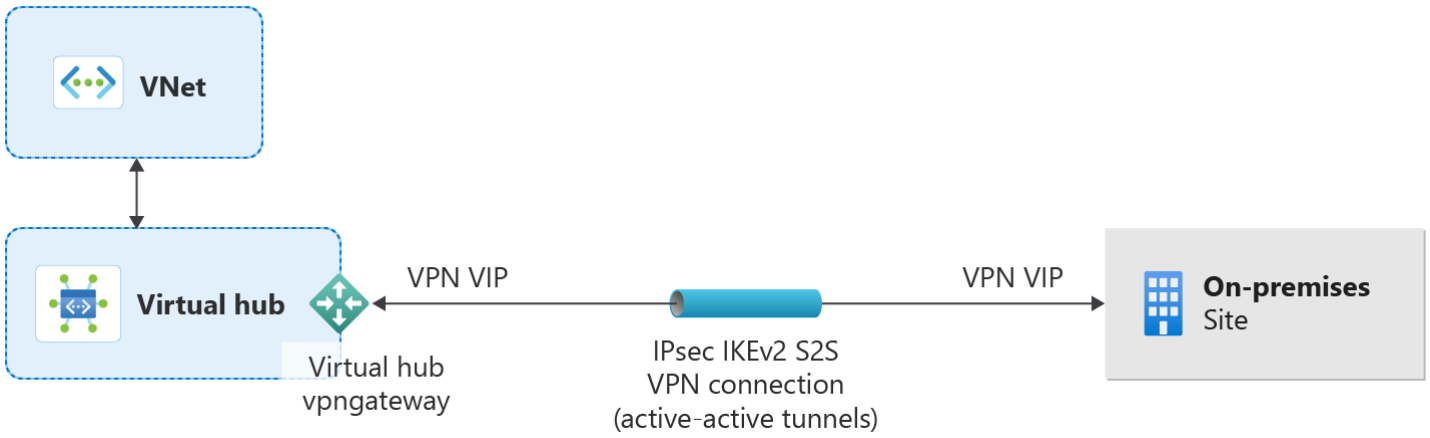
IKEv2 VPN, a standards-based IPsec VPN solution.
IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above).

Tunnel Type	Authentication Mechanism
OpenVPN	Any subset of Microsoft Entra ID, Radius Auth and Azure Certificate
SSTP	Radius Auth/ Azure Certificate
IKEv2	Radius Auth/ Azure Certificate
IKEv2 and OpenVPN	Radius Auth/ Azure Certificate/ Microsoft Entra ID and Radius Auth/ Microsoft Entra ID and Azure Certificate
IKEv2 and SSTP	Radius Auth/ Azure Certificate

The Virtual WAN architecture is a hub and spoke architecture
with scale and performance built in for branches (VPN/SD-WAN devices),
users (Azure VPN/OpenVPN/IKEv2 clients),
ExpressRoute circuits, and virtual networks.



Virtual WAN type	Hub type	Available configurations
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute User VPN (P2S) VPN (site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub Azure Firewall NVA in a virtual WAN



Site in Vwan = Physical Location

these on-prem vpn device endpoint

PSK in VPN:

mixture of letters and numbers, used to establish encryption for the connection.

The same shared key must be used in both the virtual network and local network gateways.

The local network gateway is a

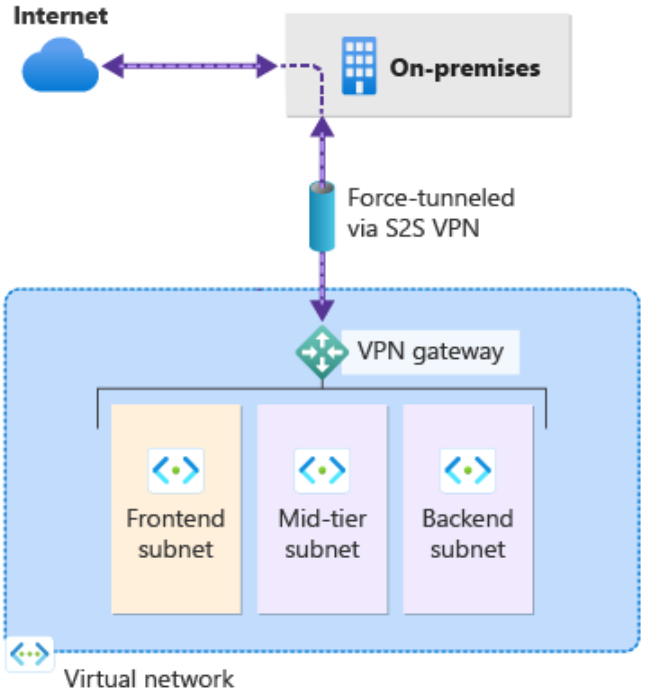
specific object deployed to Azure that

represents your on-premises location (the site) for routing purposes

Forced tunneling lets you redirect or "force" all

Internet-bound traffic back

to your on-premises location via S2S VPN tunnel for inspection and auditin



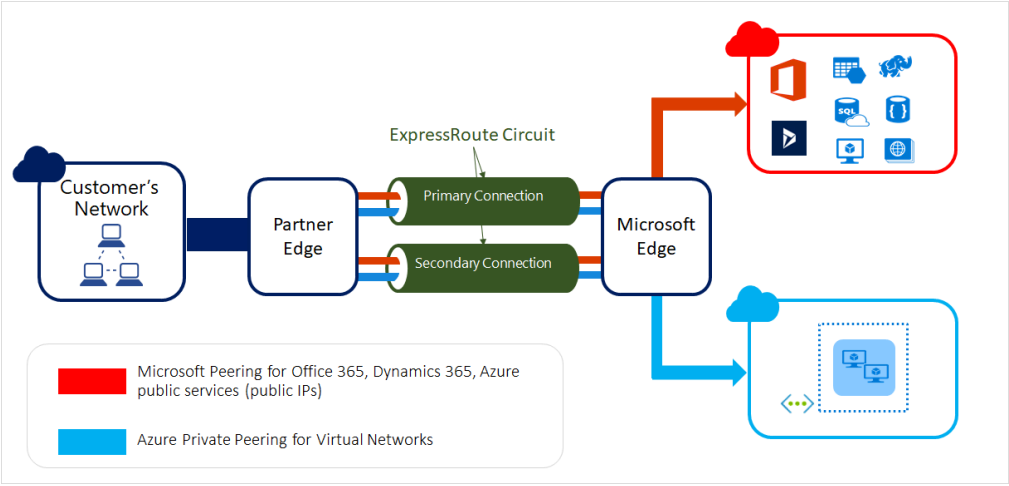
Broadband Internet = ExpressRoute = Physical Cable connectivity

1. Speed - 100 GBPS

2. Security -

3. Cost - Unlimited Data Transfer (opt for it)

For Hybrid Cloud

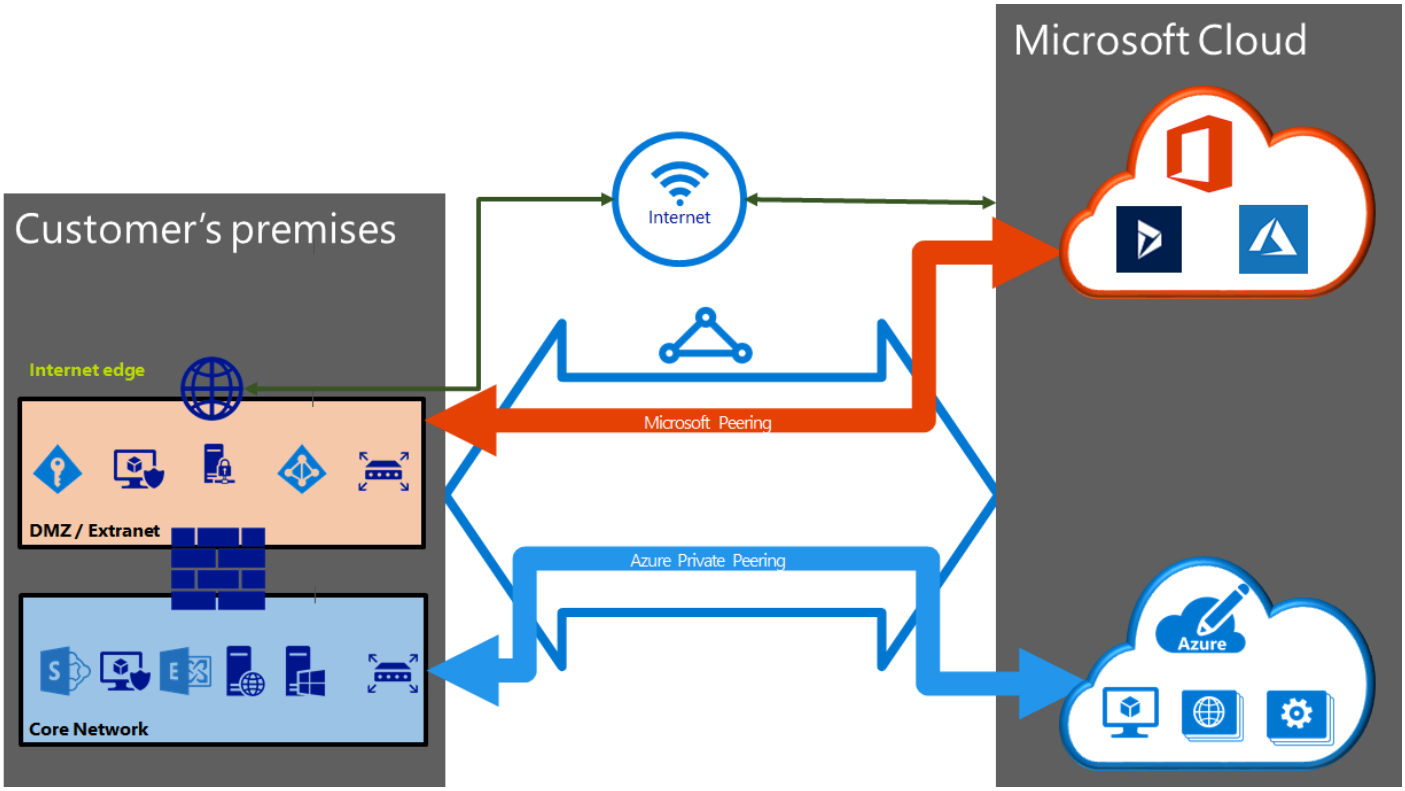


Downgrade from Unlimited to Metered is not allowed after circuit creation.

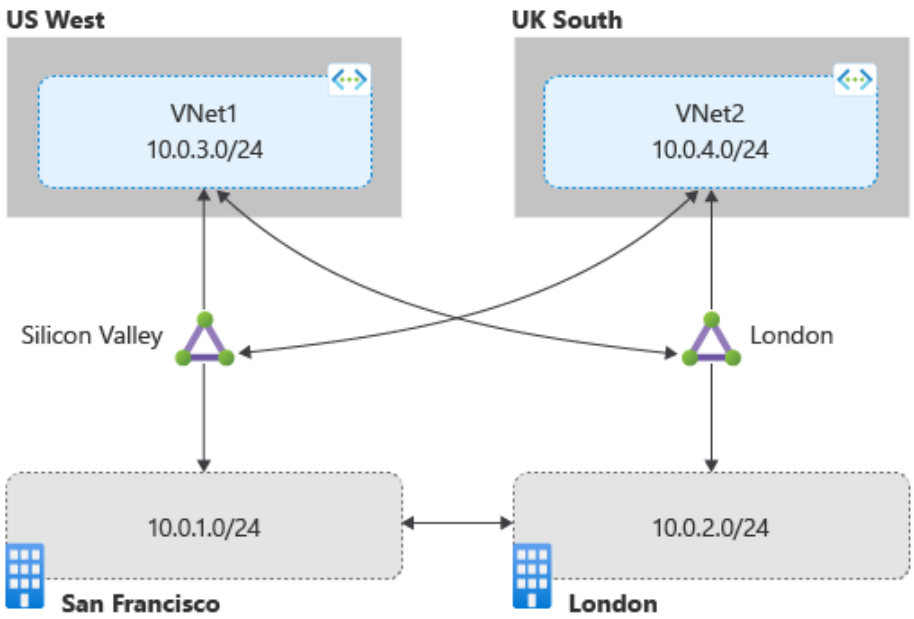
ExpressRoute connections enable access to the following services:

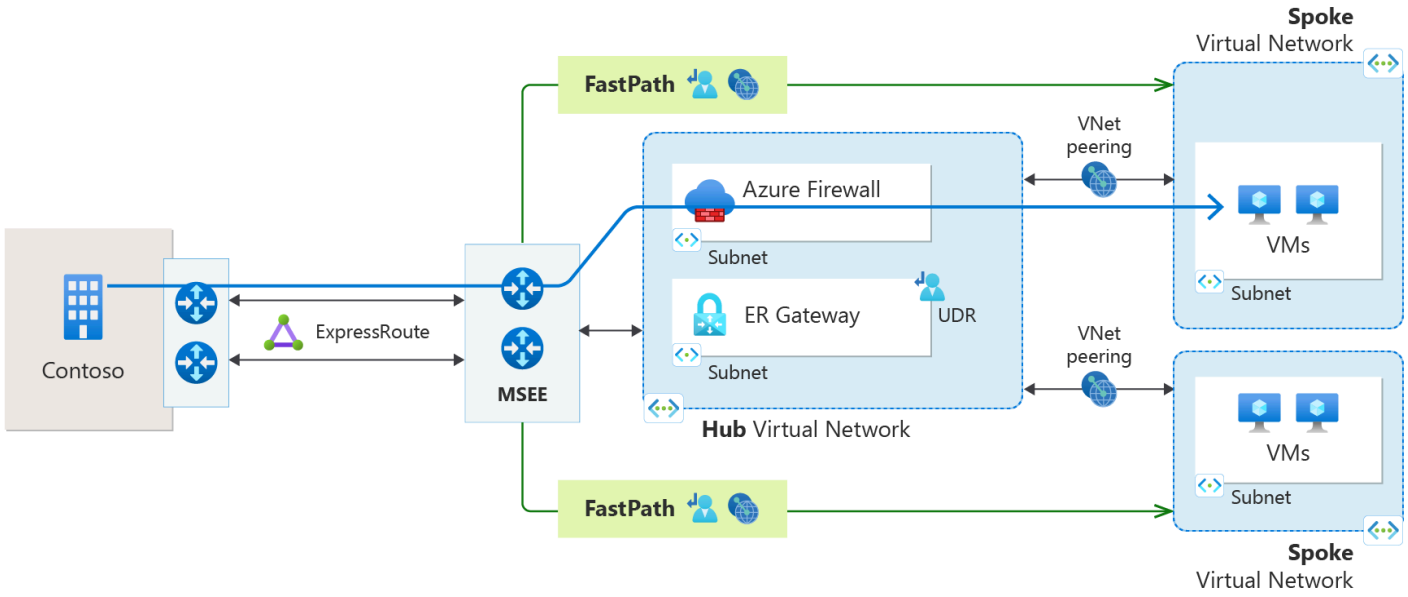
Microsoft Azure services

Microsoft 365 services



https://learn.microsoft.com/en-us/answers/questions/1531211/peering-location-in-azure





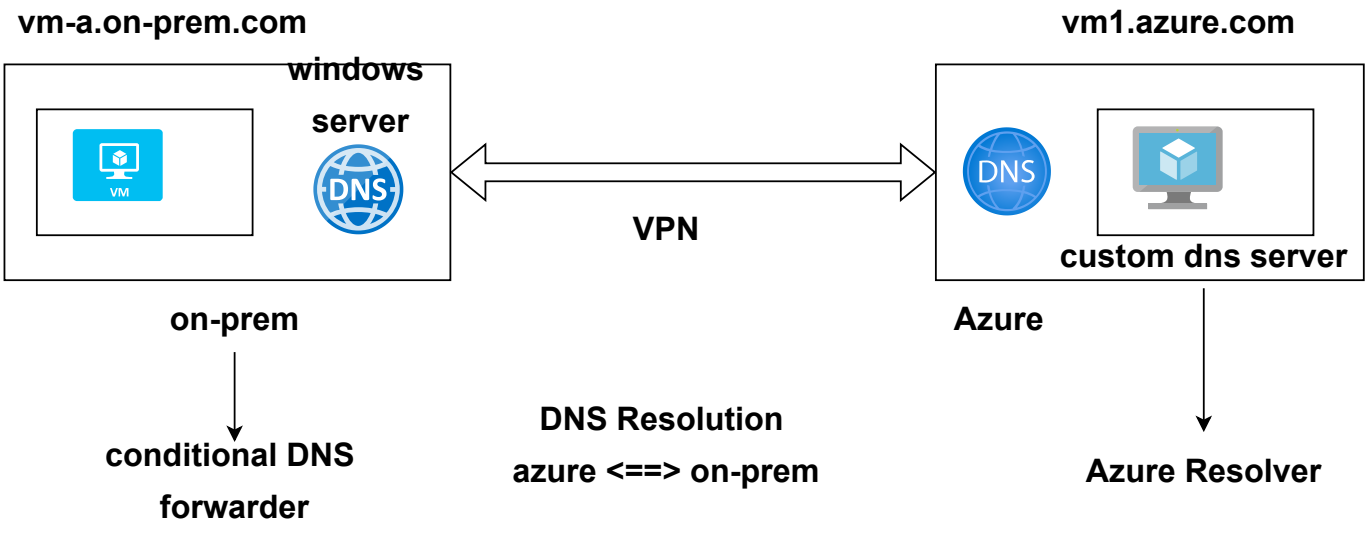
Extra Knowledge -

upto 5 CIDR to vnet

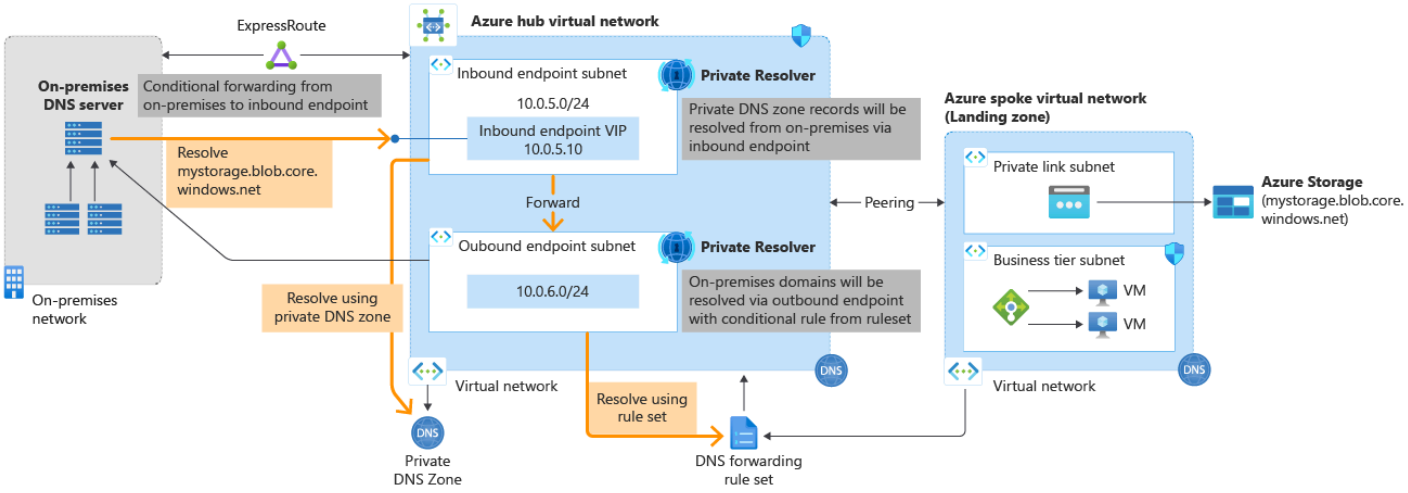
can delete a CIDR if remove all Depndency

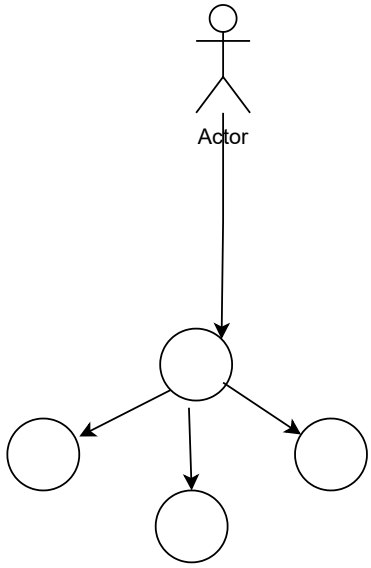
NIC Card => IP config => chnage subnet => this chnages associated Pvt IP

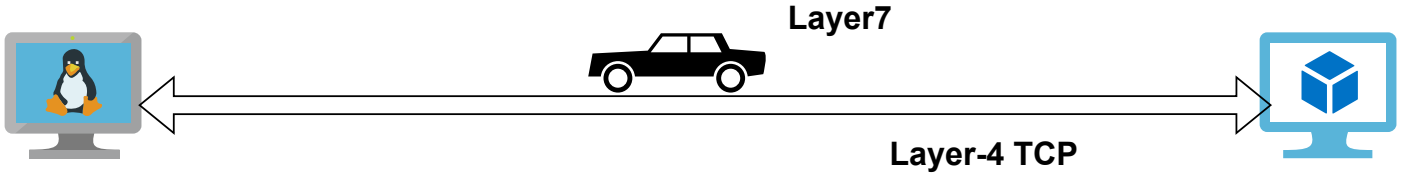
expand the existing address space like /16 to /12 ? ==> yes



IP address 168.63.129.16 is a virtual public IP address that is used to facilitate a communication channel to Azure platform resources.







1. IP, Port, Protocol => Layer4

2. HTTP Header

https://www.ionos.com/digitalguide/hosting/technical-matters/http-header/

Layer-4 Load Balancer:

- setup connection faster

- simpler and cheaper

- source / destination port

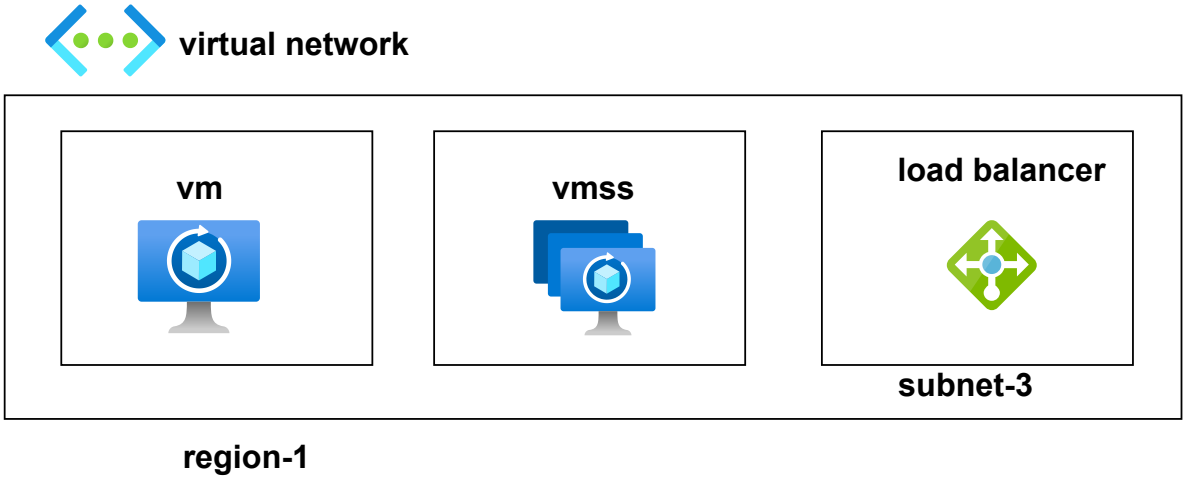
Layer-7: URL, requests, HTTP

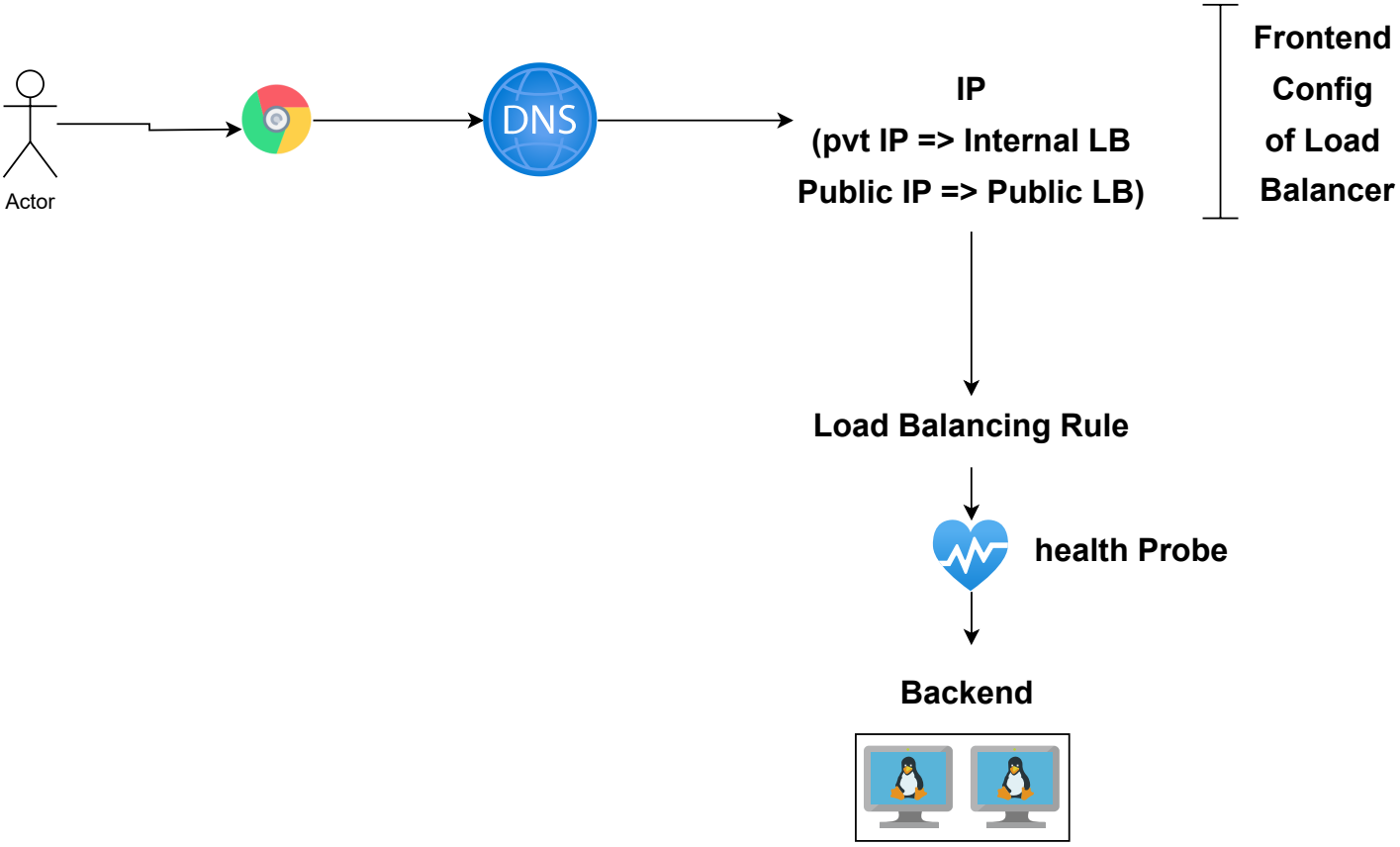
- URL Path

- /home: backend-1

/payment: backend-2

re-write http header, redirect url





Layer 4 : UDP/TCP : DNS

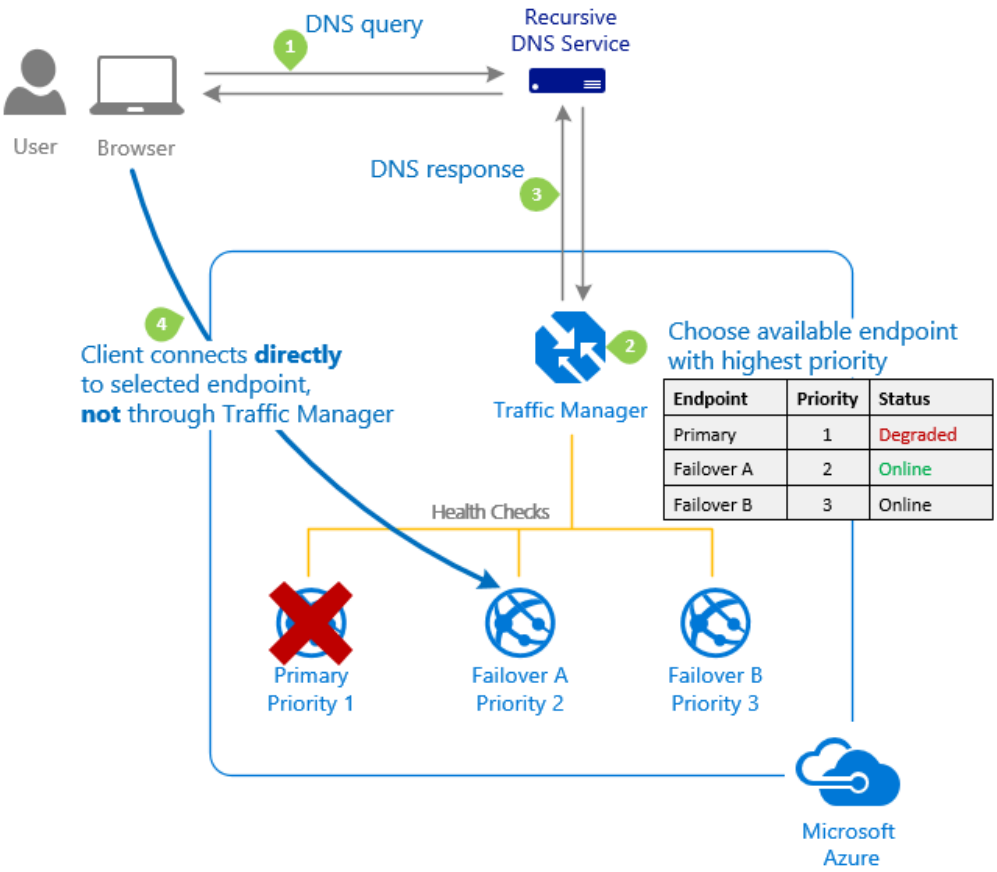
DNS is an application service,

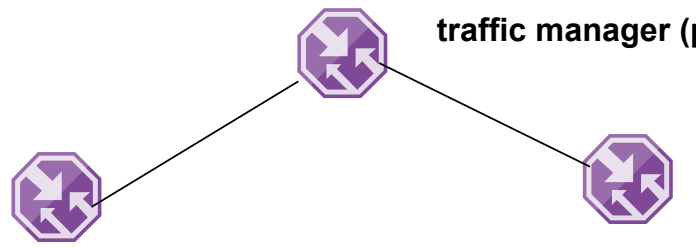
so it should be layer 7.. however it's service is listened on layer 4

Traffic Manager: Azure Traffic Manager is a DNS-based traffic load balancer.

- public facing applications across the global Azure regions

- Traffic Manager also provides your public endpoints with high availability





traffic manager (priority routing)

traffic manager (performance routing) **traffic manager (performance routing)**

Azure endpoint

External endpoint

Nested endpoint

nslookup demo8786.trafficmanager.net

Server: reliance.reliance

Address: 2405:201:6011:90d1::c0a8:1d01

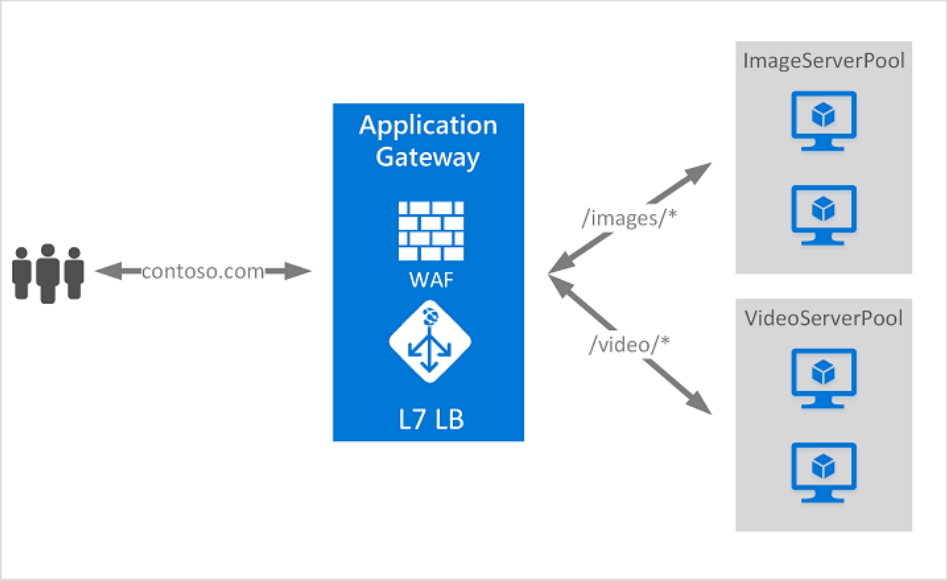
Non-authoritative answer:

Name: load-balalncer-898.centralindia.cloudapp.azure.com

Address: 4.224.68.118

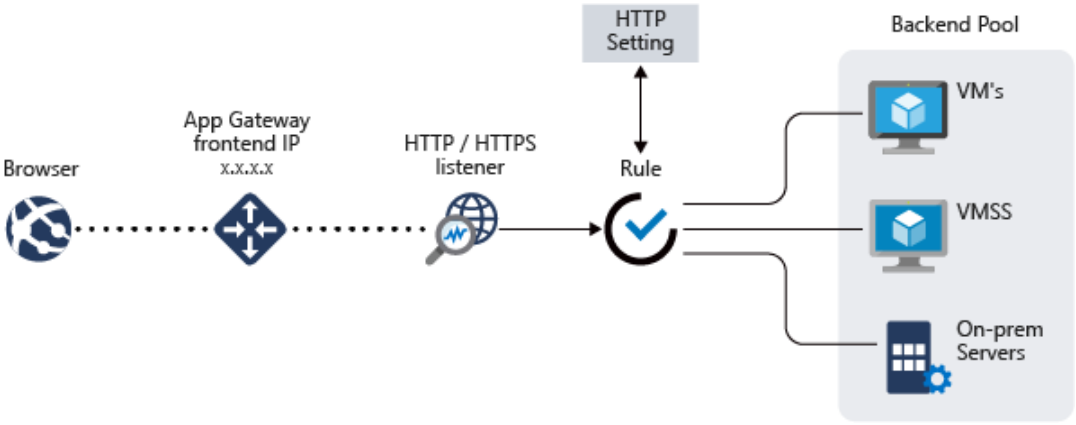
Aliases: demo8786.trafficmanager.net

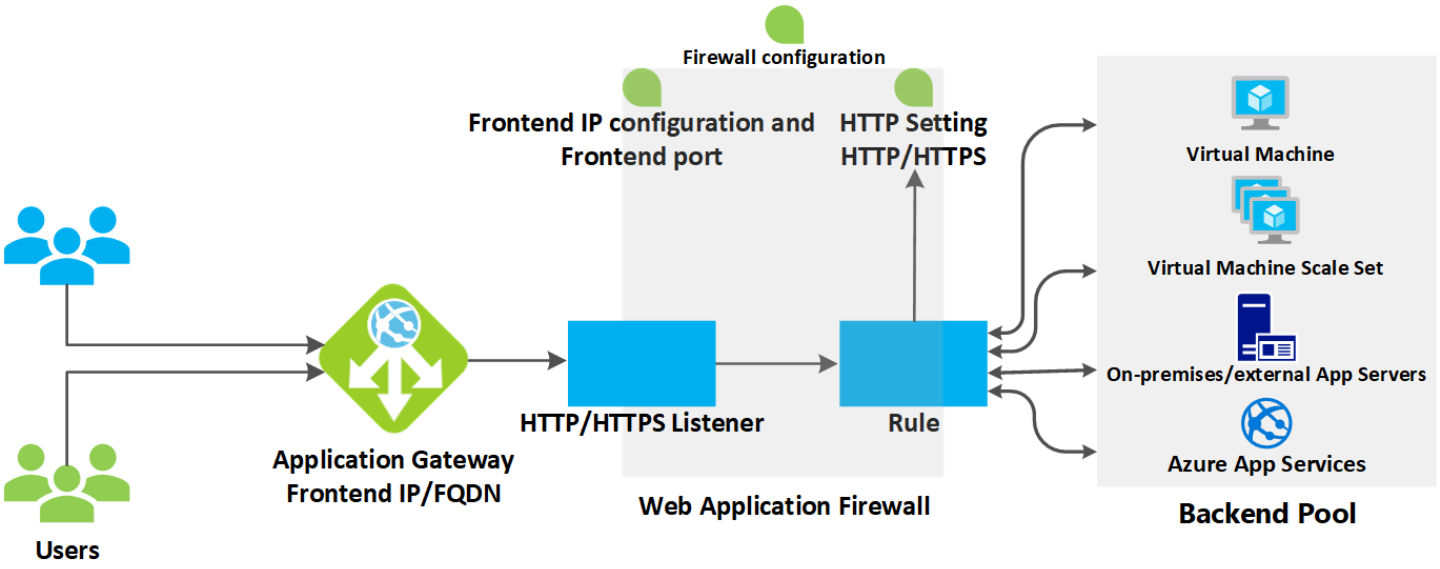
Azure Application Gateway is a web traffic (OSI layer 7) load balancer that enables you to manage traffic to your web applications



Application gateway supports SSL/TLS termination at the gateway, after which traffic typically flows unencrypted to the backend servers. This feature allows web servers to be unburdened from costly encryption and decryption overhead.

A Standard_v2 Application Gateway can span multiple Availability Zones, offering better fault resiliency and removing the need to provision separate Application Gateways in each zone.





IP of App GW

↓

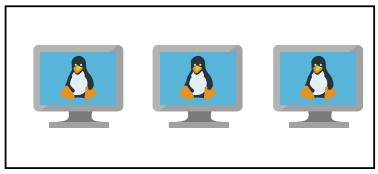
A listener is a logical entity that checks for connection request inspects URL, Header etc

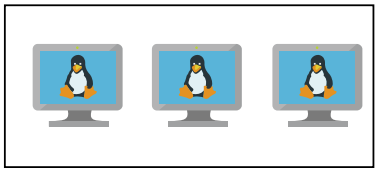
↓

if a web application firewall (WAF) is in use, the application gateway checks the request headers and the body, if present, against WAF rules

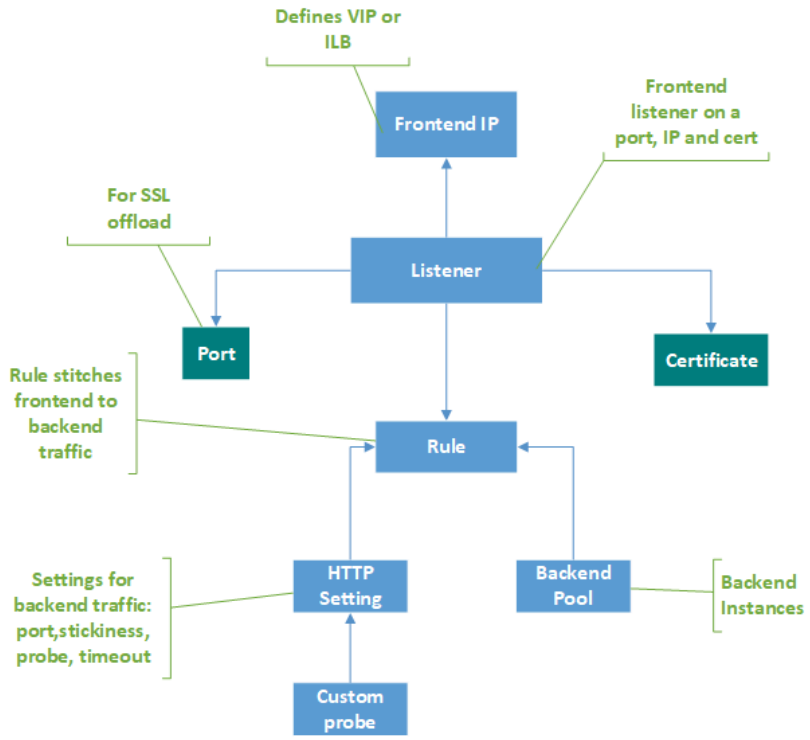
If a request is valid and not blocked by WAF, the application gateway evaluates the request routing rule that's associated with the listener. This action determines which backend pool to route the request to.

Routing Rule





backend pool contains multiple servers, the application gateway uses a round-robin algorithm



In Traffic Manager / Front Door => Endpoints Requires DNS Name (Public IP)

Azure Load balancer / App Gw ==> Endpoints DO NOT Require

LISTENER TYPES:

Basic: This type of listener listens to a single domain site, where it has a single DNS mapping to the IP address of the application gateway. This listener configuration is required when you host a single site behind an application gateway.

Multi- Site:

BACKEND TYPES:

NICs

Virtual machine scale sets

Public IP addresses

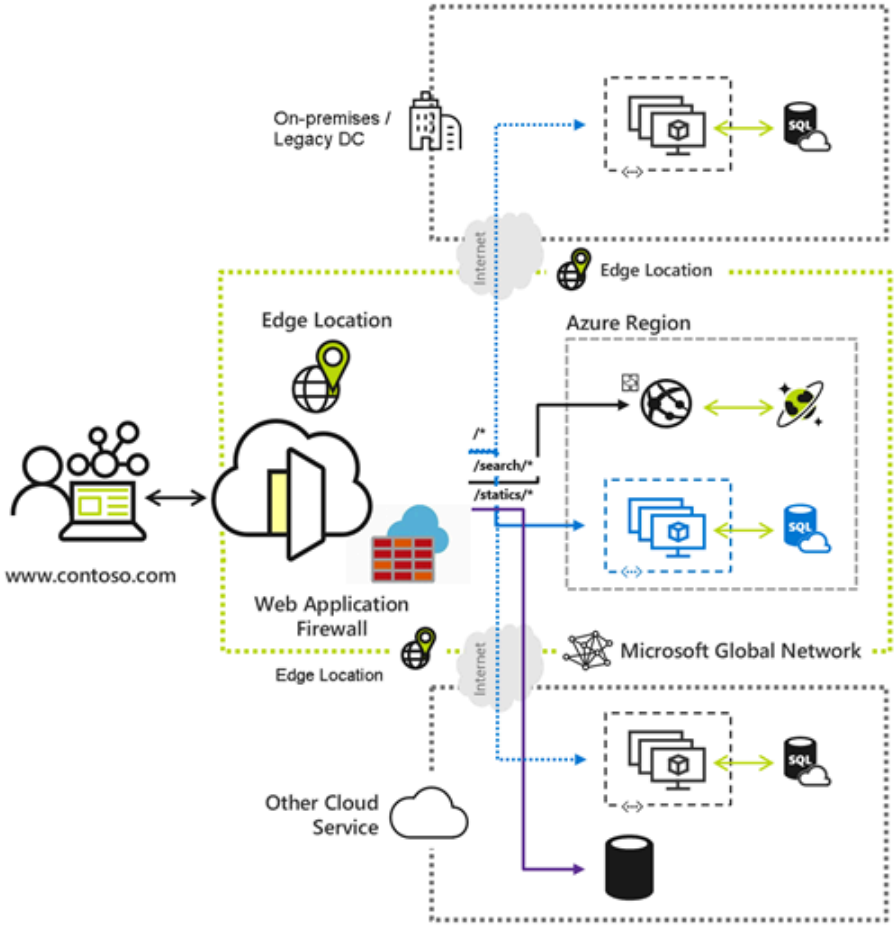
Internal IP addresses

FQDN

Multitenant backends (such as App Service)

CDN: A content delivery network (CDN) is a network of interconnected servers that speeds up webpage loading for data-heavy applications.

Frontdoor:



1. Terminate SSL offload at the edge

2. Accelerate application performance by using

Front Door's anycast network and split TCP connections.

3. Unified static and dynamic delivery offered in a single tier to accelerate

and scale your application through caching, SSL offload, and layer 3-4 DDoS prot

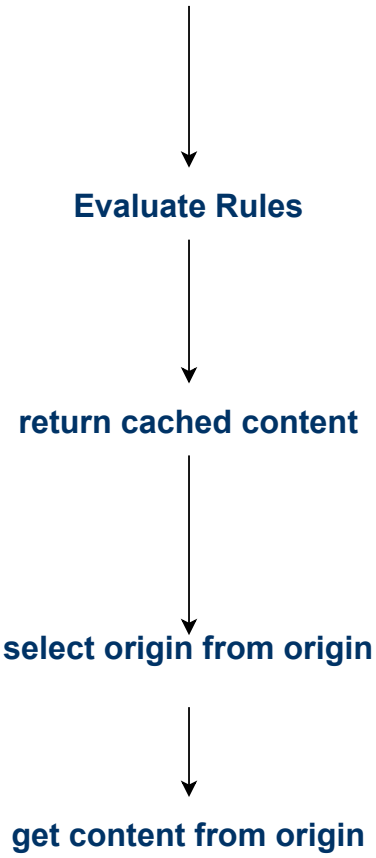
Frontdoor Domain

↓

TLS

↓

WAF



https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security

https://learn.microsoft.com/en-us/azure/security/fundamentals/network-overview

Defender for cloud: CSPM +CWP tool
Protection + recommendation

can provide time bound
access to users to login to vm

DDoS: means to degrade your service
1. Monitor
2. DDoS - at network level

But in real life,

Region is same then VM's from peered vnet-2 can be added but in a New backend where you add via IP not NIC

NSG : filters traffic in / out

a. NIC

b. Subnet

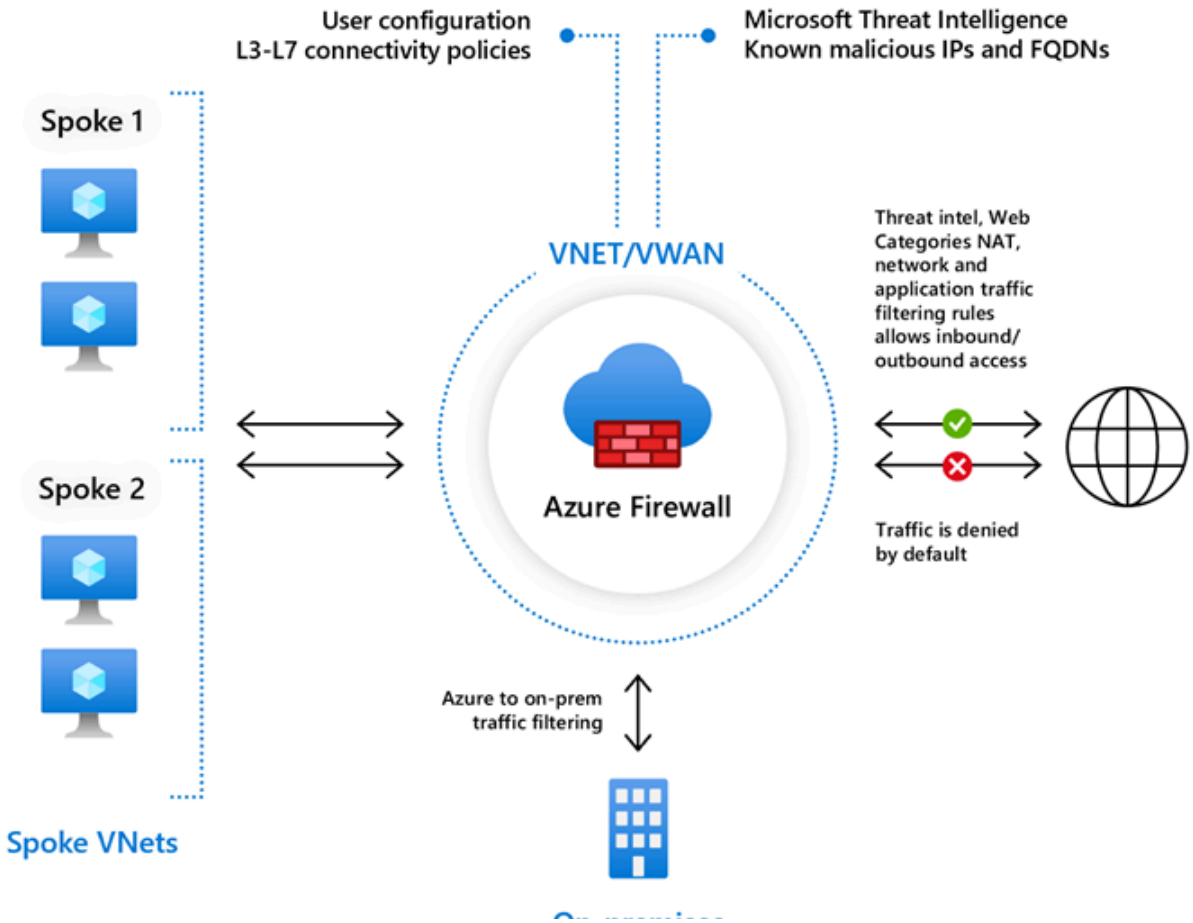
IDPS =>

inbound connectivity from internet to hosted public services

NAT = hides internal network str

masks your ip

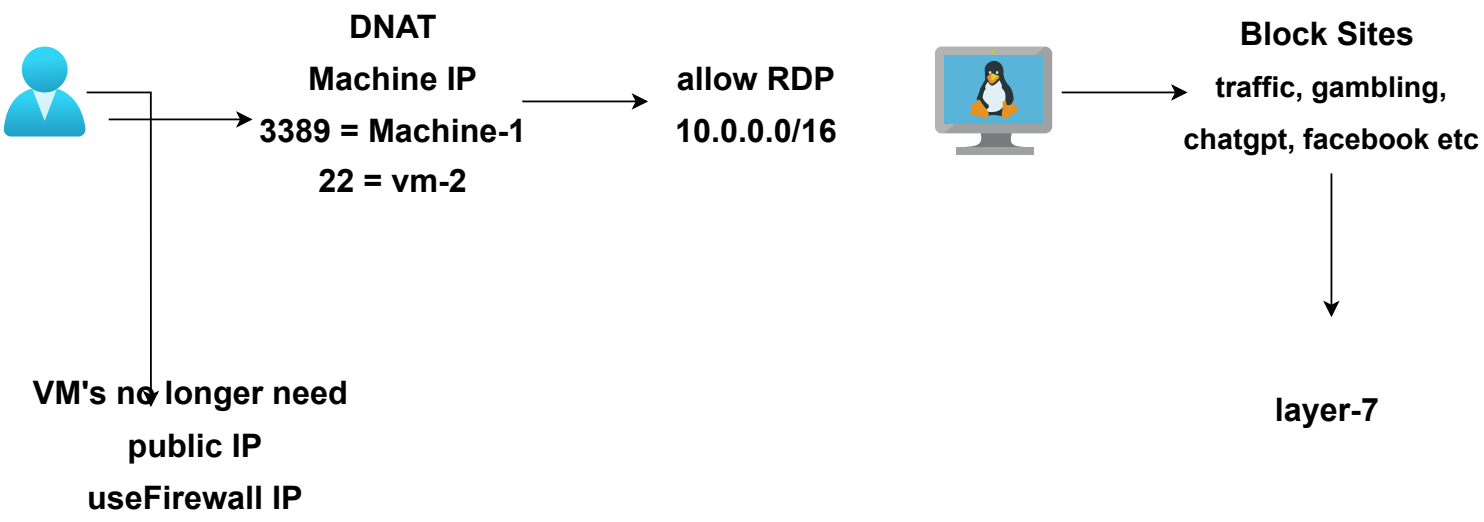
Azure Firewall = IDPS + NAT + NSG



On-premises

for azure firewall This virtual network must have a subnet named AzureFirewallSubnet.

Forced tunneling: to send Internet traffic to another resource/NVA



azure firewall blocks everything by default

Action: Deny. Reason: Policy: rules. Rule Collection Group: DefaultApplicationRuleCollectionGroup. Rule Collection: block-urls. Rule: 2. Web Category: Travel.

Azure Firewall Manager - manages multiple firewall

firewall + third Party (Zscalar, checkpoint, lboss)

1. Secured Vwan Hub

2. Hub virtual network

1. Vwan Hub with Vnet Connection

2. during or after attach firewall manager

3. FW + Partner Portal to manage ZIA, Checkpoint

4. Configure route settings

You don't create Firewall Manager

connectivity to Zscaler via vWAN is a bad idea, as it only create tunnel to a single Zscaler PoP.. no redundancy

hub | Security configuration

The Azure Web Application Firewall (WAF) on Azure Application Gateway actively safeguards your web applications against common exploits and vulnerabilities. As web applications become more frequent targets for malicious attacks, these attacks often exploit well-known vulnerabilities such as SQL injection and cross-site scripting.

WAF policy - set of rules

1. PaaS :

- can't control networking fully

Benefits of using MS Backbone

1. optimized path

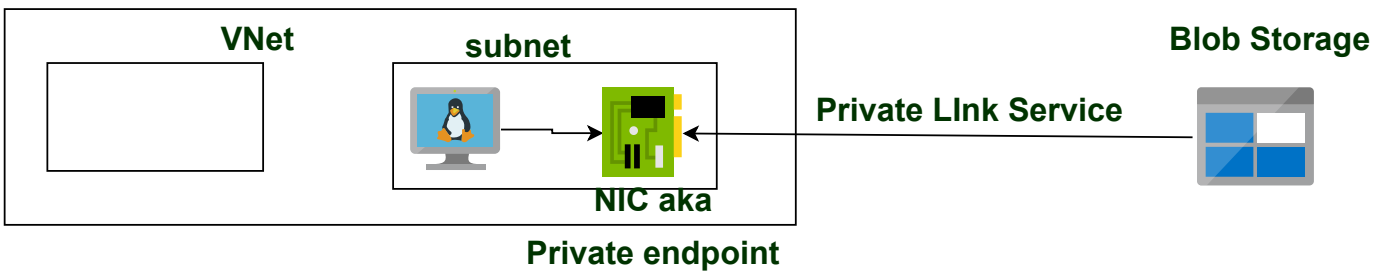
2. Don't Use internet

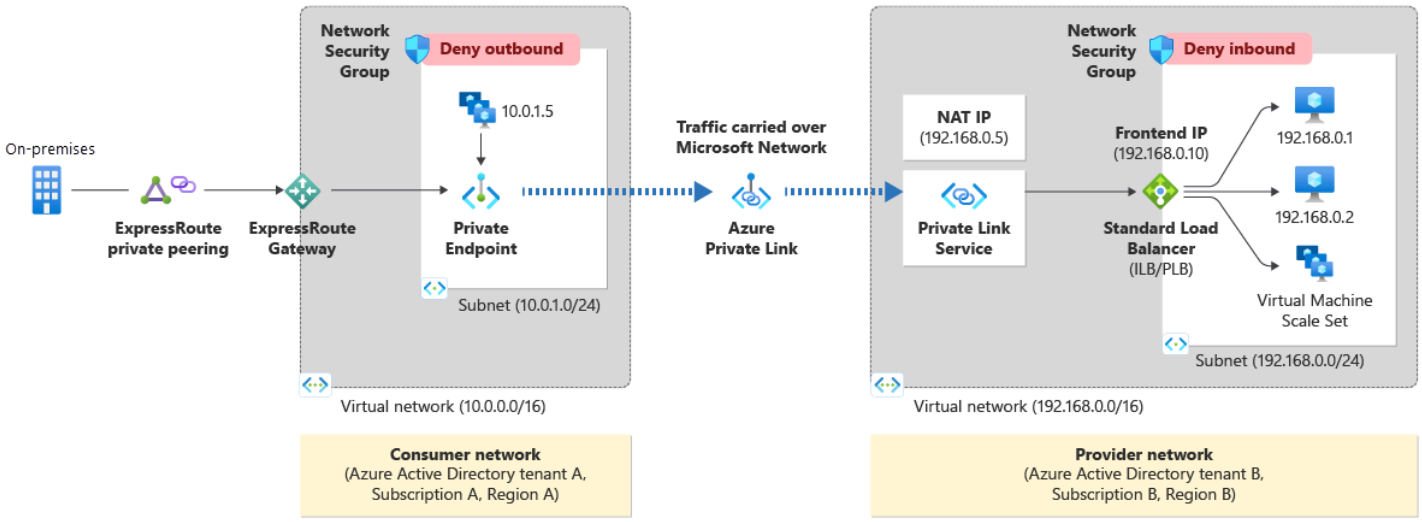
Service Endpoint

- Subnet Level

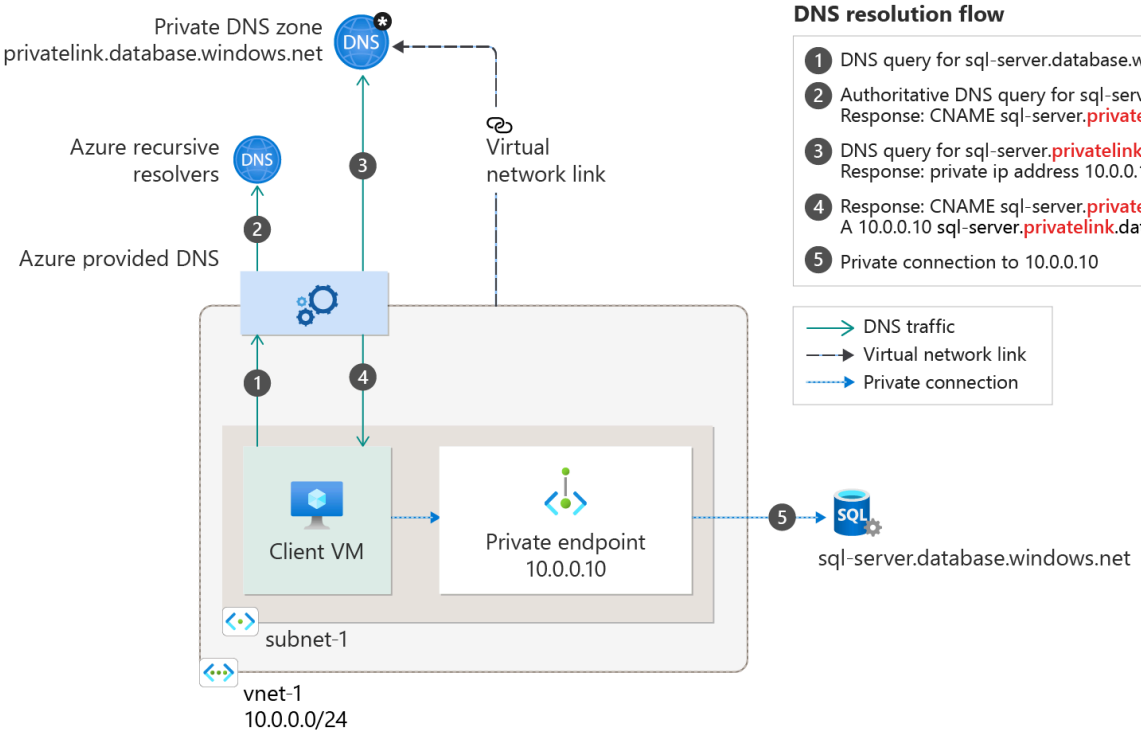
- Without Public IP connect to PaaS

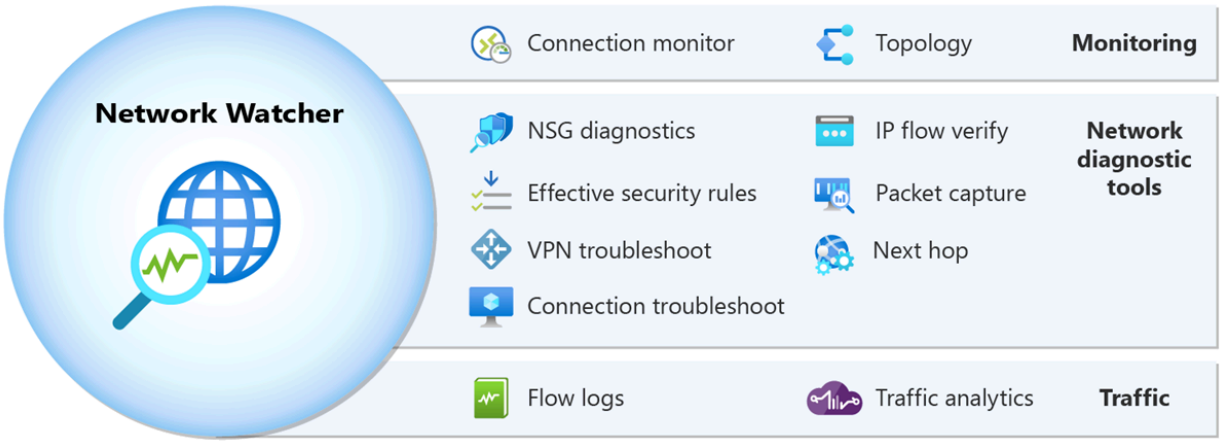
Private LInk Service





private endpoint can help on-prem to connect privately





Topology provides a visualization of the entire network for understanding network configuration

Connection Monitor enables you to monitor connectivity in your Azure and hybrid network

Layer4 - ip flow verify

Effective security rules allows you to view the effective security rules applied to a network interface. It shows you all security rules applied to the network interface, the subnet the network interface is in, and the aggregate of both.

WHihc NSG are applying

NSG FLow Logs : log information about IP traffic flowing through a network security group.
Flow data is sent to Azure Storage from where
you can access it and export it to any visualization tool,
security information and event management
(SIEM) solution, or intrusion detection system (IDS) of your choice

Azure Monitor Network Insights provides a comprehensive
and visual representation through topology, health and metrics
for all deployed network resources, without requiring
any configuration. It also provides access to network
monitoring capabilities like Connection monitor,
NSG flow logs, VNet flow logs, and Traffic analytics.
Additionally, it provides access to Network Watcher diagnostic tools.

Network insight auto enabled

Alert Rule => Do something

action group = works when alert fired ....
collection of actions