

Identity

Active Directory
LDAP, Kerberos, NTLM

Sync

→ AADDS
Azure Active Directory
HTTPS
x OU, x GPO

Azure AD Connect. (Appt.)

└ Password Hash
└ Pass Through

Azure AD

Domain Join

vs

Domain Register.

Full Control.

BYOD, Partial Control.

User

Group

└ Self Service Password Reset.

1. Request User / Group.

└ SMS

Call

Mail

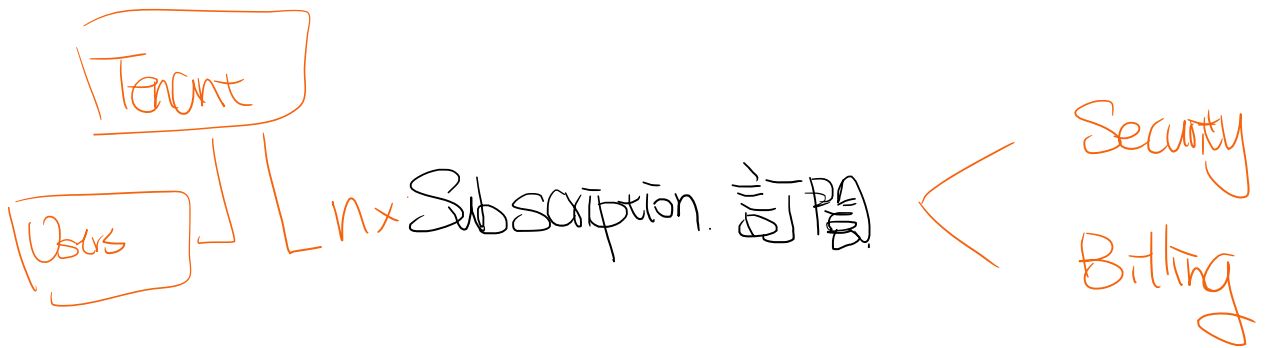
MFA.

Question.

Role

Global Admin
User Admin

Group - Manual (指派方式)
Security Group Dynamic User
M365 Group Dynamic Device



EA (Enterprise Agreement)

CSP
Day as You Go < 訂閱式

License - A費

Are Hybrid Benefits (Bfa)

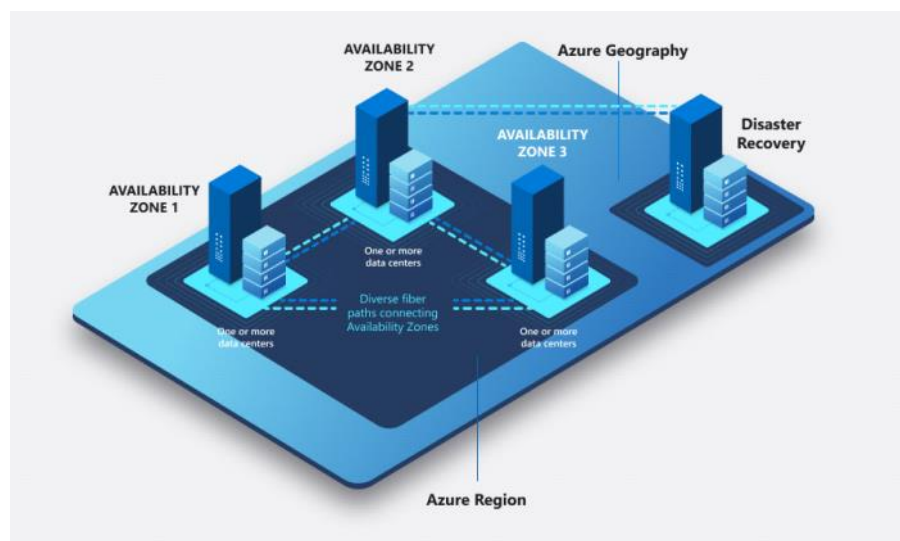
Data Center 數據中心

Availability Zone 可用區 (域)

Region 區域



Region Pair.



Azure AD can be synchronized with an on-premises AD DS environment to provide a single identity to users that works natively in the cloud. -> Azure AD Connect

Rebalance.

in the cloud. > Azure AD connect

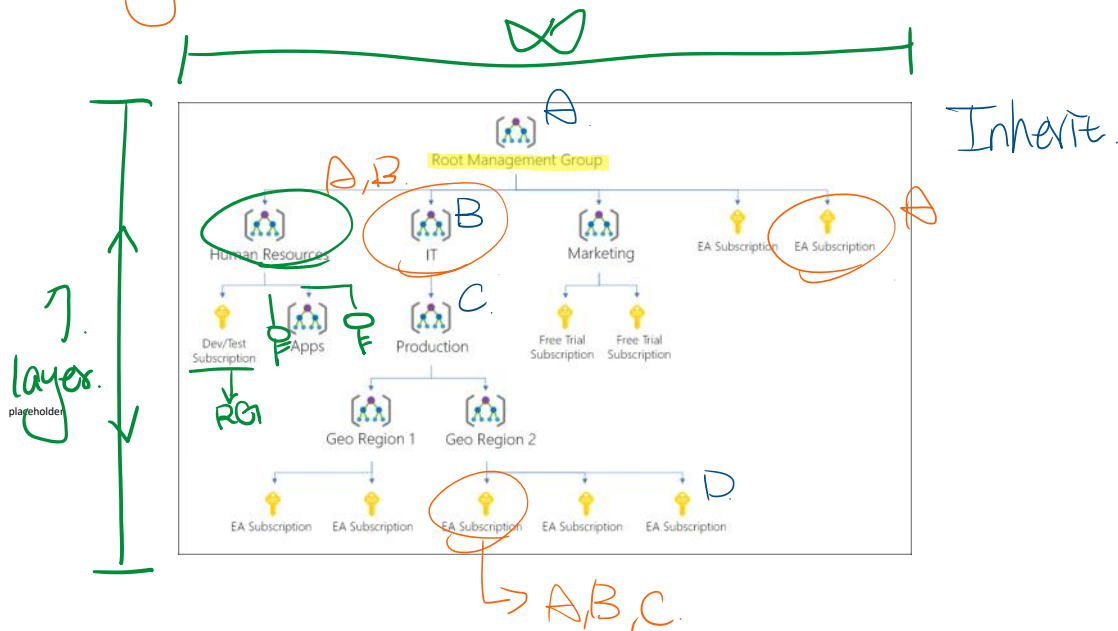
Resource.

Azure AD DS integrates with Azure AD,

which itself can synchronize with an on-premises AD DS environment.

Cost = Cost Management

Management Group



Azure Policy

Definition — Policy — Built-in.

Custom. (JSON)

Initiative — Policy's Folder

← Initiative - KSTay's folder

Assignment
(Scope) [Subscription
RGs

Check / Enforce.

Identity

User
Group

Resource
App Registration
Managed Identity

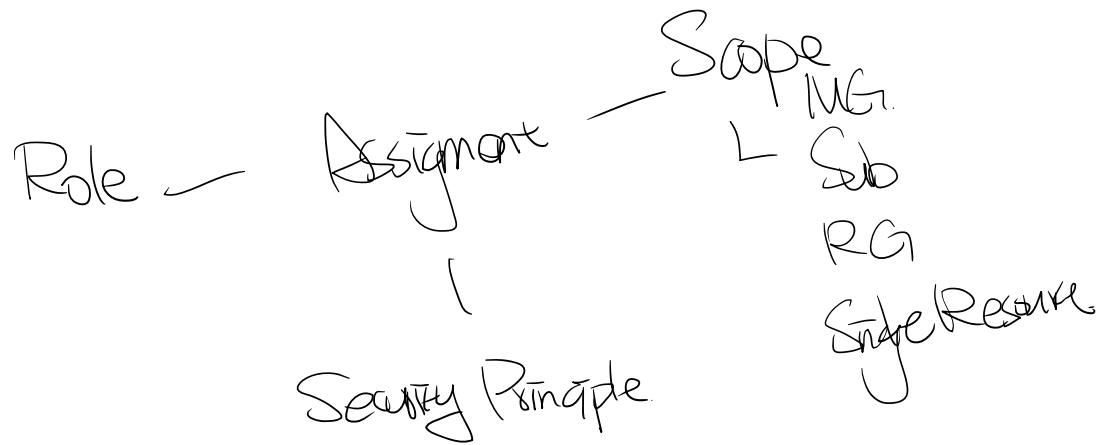
Security Principle
[User Principle
Service Principle

Role based Access Control (RBAC)

base on Azure Resource Manager (ARM)

Role = 1 or n Permission.

↳ JSON [Action / Not Action
Data Action / Not Data --
Assignable Scope.



Azure Portal.

L Cloud Shell. — Container.



New - AZVM - - - - - 声明式 - IaC

$\rightarrow$ 幂等性

ARM Template - JSON - [Parameter - Sub
 Variable

VM - Disk

Resource - DependsOn

Function - PreDefine
 - in...

Done Bicep - Bicep.

Syntax.

SDK

Done REST API.

Function
Output.

└ Krebeline
└ User --

Networking

Virtual Network (VNET) - Addr Space - CIDR.

Independent

SDN.

10.10.0.0/16

.0 ~ .255

10.10.1.0/24

.0, .255, .1, .2, .3

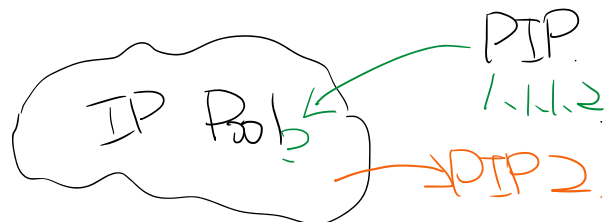
10.10.2.0/27

⇒ 27 IP

.0 ~ .31, .0, .1, .2, .3

IP - Private IP - Dynamic / Static
 (4) → Azure

Public IP - Azure Resource - Basic / Standard AZ. Dynamic / Static



NSG (Network Security Group) Layer 4 FW. (TCP/IP)

Inbound - Rule x n - Priority (int) 100 ~ 4096 越小越优先

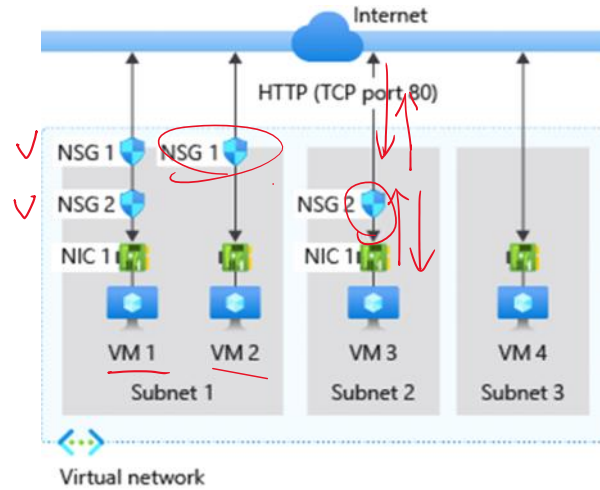
Outbound

Default Rules

Appliance (VM-NIC)

Subnet

Default Rules

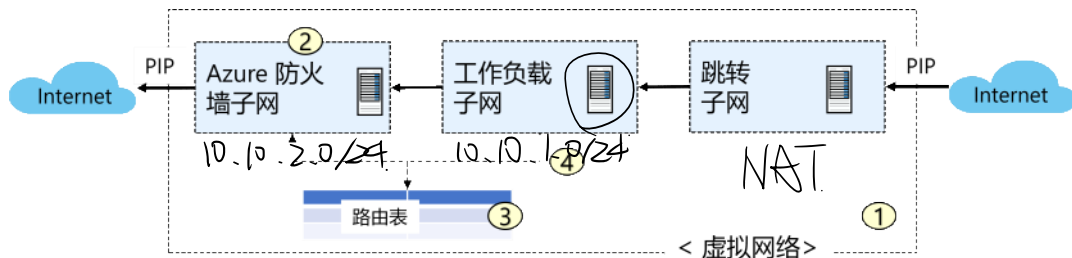


Azure Firewall (Layer 3, PaaS)

{ NAT
 { Network
 { Application

{ HA
 { Scale

(VM) → Dedicate Subnet.



Route — System Route ← Azure Managed

— User Define Route

— Route Table — Route × n.

— Associate — subnet

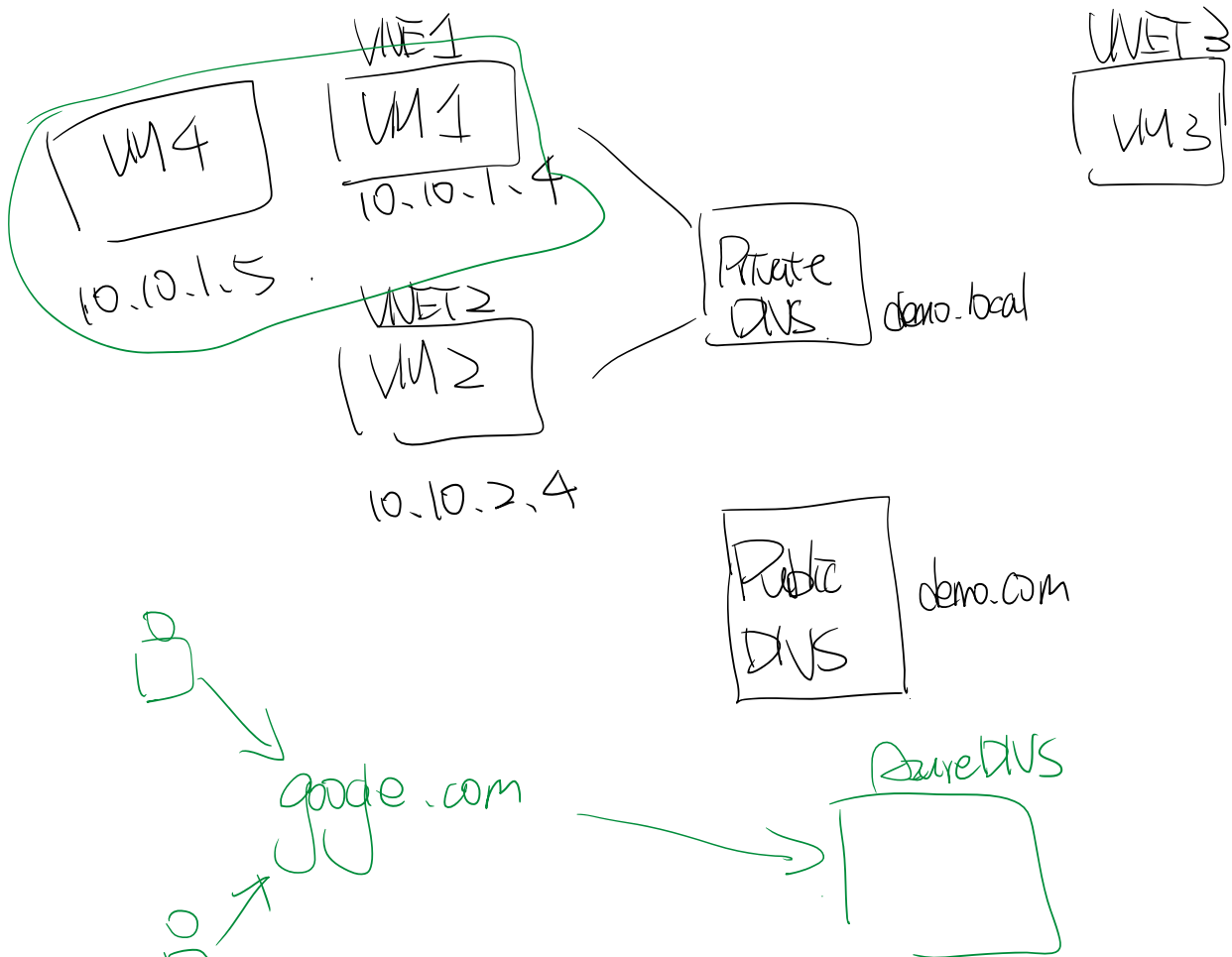
Azure DNS (PaaS)

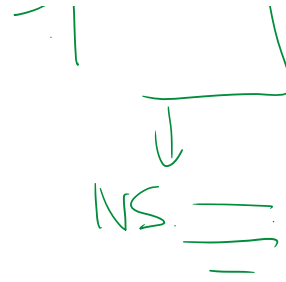
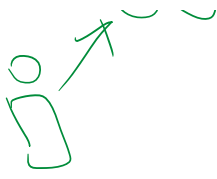
- Public DNS Zone
 - Child Zone

- Private DNS Zone = Any Name, Demo.local

- Non-Public
 - Link VNET

✓ Auto Registration (Discovery) (By VNET)



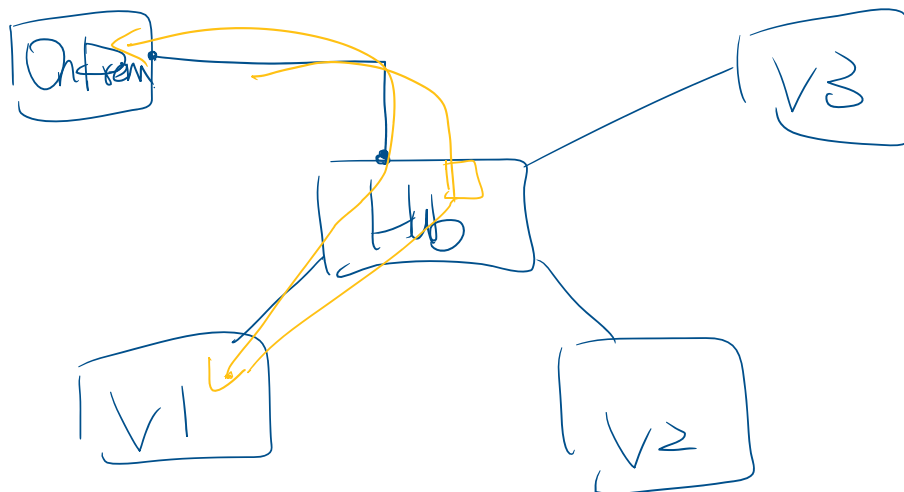


Inter Site Connectivity

Peering VNET ↔ VNET
(VPN)



Hub - Spoke Model



VNET ↔ Other

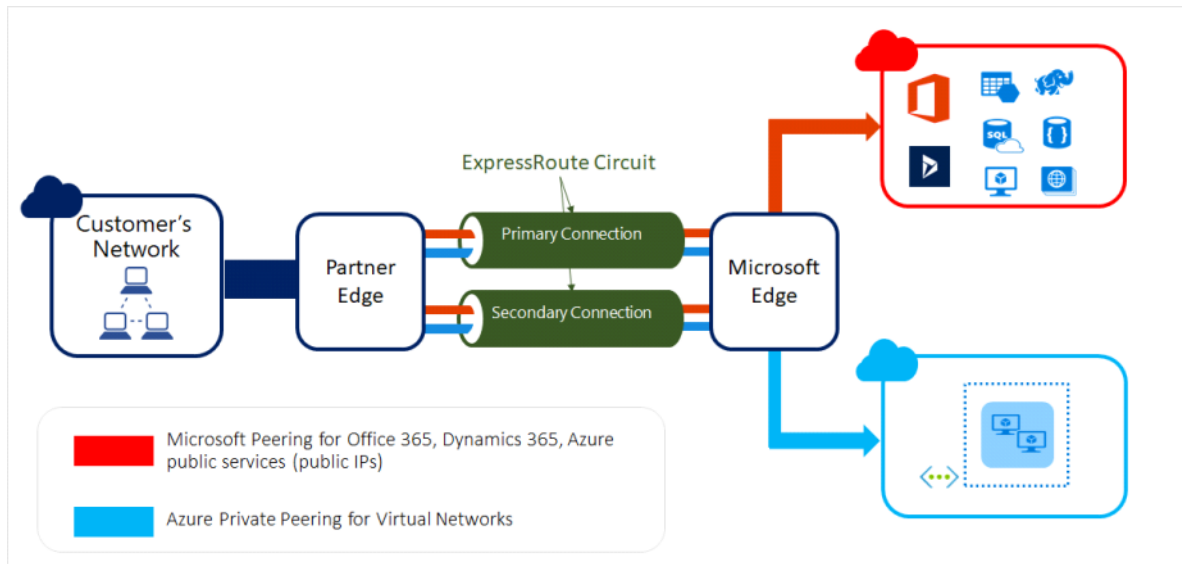
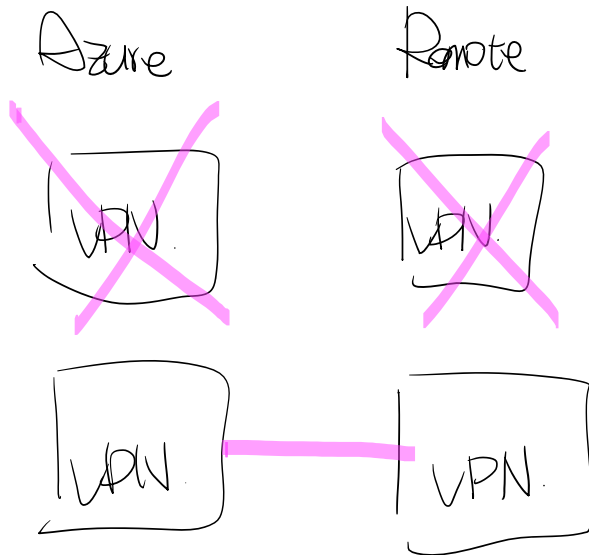
VPN Point 2 Site
Site 2 Site

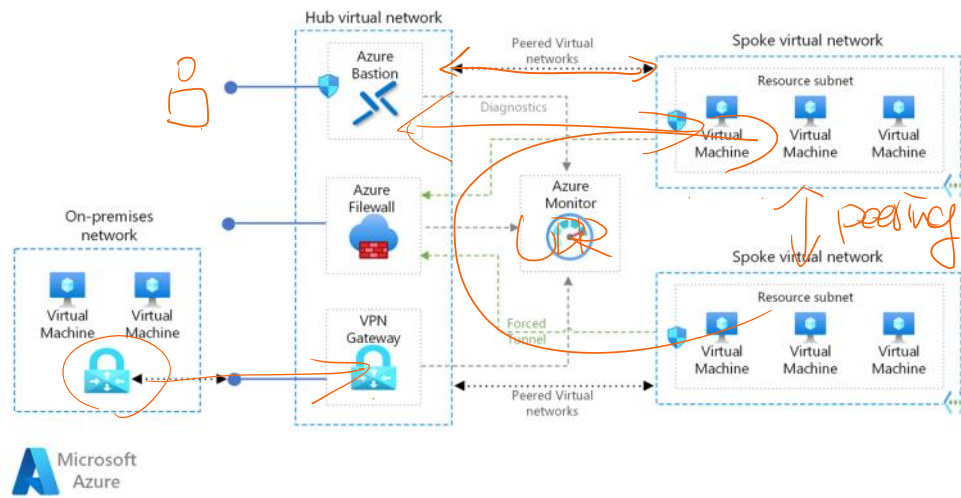
VNET Gateway
(VPN)

[VPN. | route 2 site
 | Site 2 Site
 Express Route

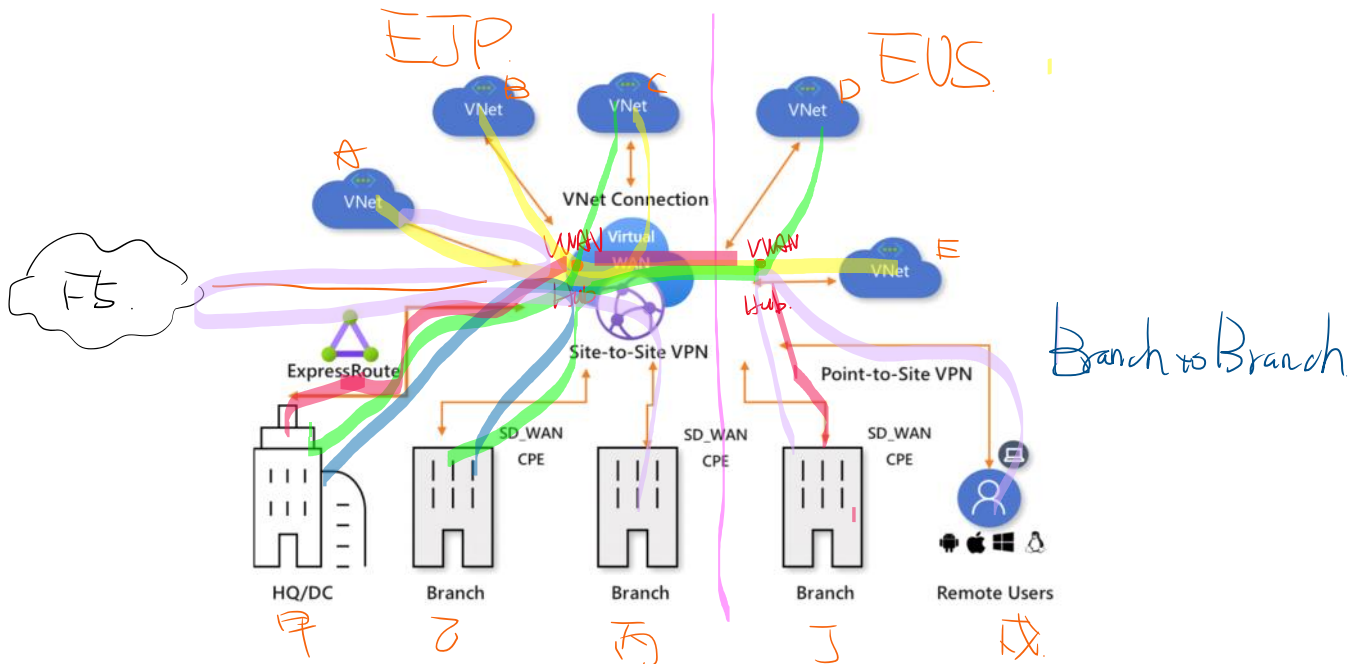
VNET Peering
 (VPN)

Active - Standby
 Active - Active



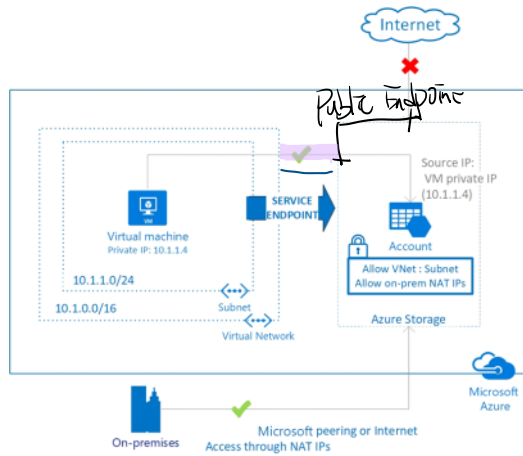


Virtual - Wan

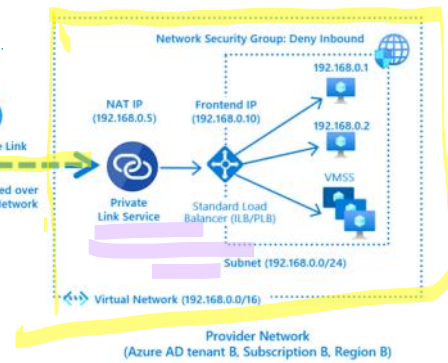
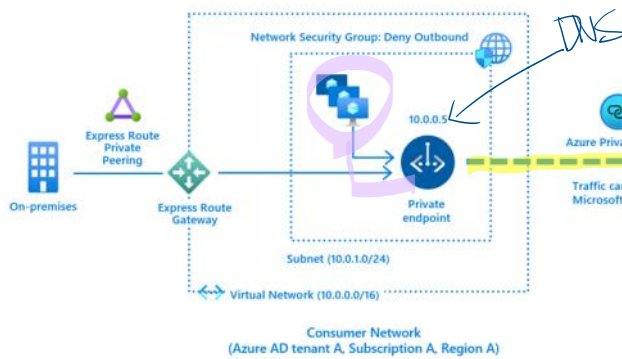


Private Endpoint / Link

Service Endpoint



PaaS - Storage

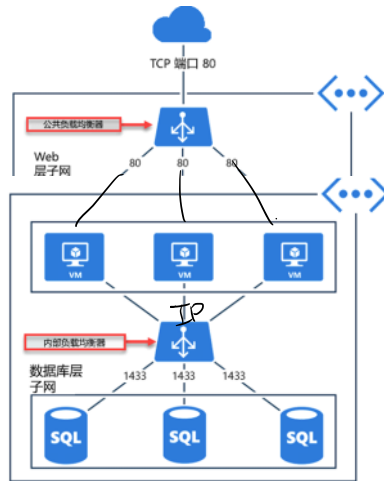


功能	应用程序网关	Front Door	负载均衡器	流量管理器
使用情况	使用 Web 应用程序防火墙增强应用程序安全性时，优化来自应用程序服务器场的交付。 <i>Layer 7</i>	可缩放的安全增强型交付点，适用于基于微服务的全局 Web 应用程序。	均衡入站和出站连接以及对应用程序或服务终结点的请求。 <i>Layer 4</i>	在全球 Azure 区域内以最佳方式向服务分发流量，同时提供高可用性和响应性。 <i>DNS</i>
协议	HTTP、HTTPS、HTTP2	HTTP、HTTPS、HTTP2	TCP、UDP	Any
专用	是	是	是	是
全球	是	是	是	是
Env	Azure、非 Azure 云、本地	Azure、非 Azure 云、本地	Azure	Azure、非 Azure 云、本地
安全性	WAF	WAF、NSG	NSG	

LB - Public
Internal

LB

- Public IP
- Private IP



Frontend IP. $\times n$

Backend Pool.

- VM
- Container.
- IP/FQDN.

Rule.