Azure Active Directory (Azure AD) Application Proxy: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client.

IP Flow Verify: checks if a packet is allowed or denied to or from a virtual machine.

Azure Internet Analyzer: a client-side measurement platform that enables you to test how networking infrastructure changes will impact your customers’ performance.

Multiple Websites in IIS By Using VMSS: Birden fazla website’I Windows server’lara IIS ozelligi ile yuklersek www.web1.com , [www.web2.com](http://www.web2.com) seklinde. Ilgili trafigi Routing rules ve Backend listeners ile ilgili websitesine yonlendiririz.

**APP SERVICE:**

App Service’i Ayni Region’daki Vnet’e Baglama: App service’e tabi dedicated subnet olusturulur.

App Service’i Farkli Region’daki Vnet’e Baglama: VPN gateway (Azure virtual network gateway) kurulur.

App – Vnet Baglantisi: HErbir

**DOMAIN:**

Private Domain:

* Bir regionda kurulur: baska regiondaki Vnet’ler de baglanabilir.
* Domain’e Baglanti: Vnet sadece bir zone (private domain)’a baglanabilir.
* Virtual Network Link: Vnet’i Domain’e baglar.
* Auto Registration: Link kurulurken secilir.
* Manually Registration: Auto registrate olmus olan VM’i manual register edersek manual registration esas olur.
* Deletion of Registration: VM silinirse; auto registrate olan VM’nin record’u da silinir, ama record manual olusturulmussa VM ile birlikte silinmez.
* DNS Record’un Degismesi: Auto registration olan VM’in IP address’I degisirse record’u DHCP varsa otomatik degisir.
* On Prem DNS Server’in Firewall’lu Private DNS Zone’daki VM’lerin Resolve Etmesi: Firewall’da DNS proxy enable edilir. On-prem DNS server’da configure forwarders that point to frontend IP address of Firewall.

DNS Domain Olusturma:

* Create a DNS zone,
* Identify the FQDNs of the name servers.
* Modify the NS records for the domain.

DNS Proxy Configuration:

* Enable DNS proxy in Azure Firewall DNS settings.
* Optionally configure your custom DNS server or use the provided default.
* Finally, you must configure the Azure Firewall’s private IP address as a custom DNS server in your virtual network DNS server settings. This ensures DNS traffic is directed to Azure Firewall.

app1.privatelink.azurewebsites.net: the name that is registered in Azure DNS for the private endpoint for App service app1. app1 icin private endpoint olusturursak otomatik olarak Azure DNS’e register edilir yukarki isimle.

Azure Active Directory (Azure AD) Application Proxy: Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

Azure Key Vault: To enable the HTTPS protocol for securely delivering content on a Front Door custom domain, you must use a TLS/SSL certificate. You can choose to use a certificate that is managed by Azure Front Door or use your own certificate. To use your own certificate to enable the HTTPS feature is done through an integration with Azure Key Vault, which allows you to store your certificates securely. Azure Front Door uses this secure mechanism to get your certificate.

Virtual Network Link: Azure’da Private DNS Zone olusturduktan sonra on-prem/cloud’dan private DNS zone’a baglanabilmek icin bir Vnet’in Private DNS Zone’a baglanmasi gerek. Vnet baglantisi esnasinda “enable autoregistration” secenegi secilir. Bu Vnet private DNS zone icin registration Vnet olur. Her bagli/baglanacak VM icin otomatik olarak A DNS Record olusur.

DNS Server: Bir Azure VM’i DNS server olarak konfigure ederek name resolution icra edilir. Her VM’nin name resolution’u kendi Vnet’indeki DNS Server tarafindan icra edilir. DNS server’lar arasinda DNS forwarding ile veri transferi olur.

WebApp’in Privat Domain’e Baglanmasi:  Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link. When you deploy a Private Endpoint, the DNS entry to point will be updated to the canonical name webapp1.privatelink.azurewebsites.net. So you must create a CNAME that maps to the updated DNS entry.

**EXPRESSROUTE**:

ExpressRoute Local: gives you access only to one or two Azure regions in or near the same metro. The price includes data transfer fees. It is a more economical solution if you have massive amount of data to transfer.

ExpressRoute Global Reach: connects on-premises networks via the ExpressRoute service through Microsoft's global network. For example, if you have a private data center in California connected to ExpressRoute in Silicon Valley and another private data center in Texas connected to ExpressRoute in Dallas, with ExpressRoute Global Reach, you can connect your private data centers together through the two ExpressRoute connections and your cross data center traffic will traverse through Microsoft's network backbone.

ExpressRoute Direct: connect directly into Microsoft’s global network at peering locations strategically distributed across the world.

ExpressRoute Standard: access to all Azure regions in a geopolitical area.

Ultra-Performance ExpressRoute: On-prem datacenter ile Vnet’ler arasinda FastPath saglar.

ExpressRoute FastPath: improves the data path performance between your on-premises network and your virtual network. When enabled, FastPath sends network traffic directly to virtual machines in the virtual network, bypassing the gateway.

Gateway Transit: allows to share an ExpressRoute or VPN gateway with all peered VNets and lets you manage the connectivity in one place. Sharing enables cost-savings and reduction in management overhead.

BGP Route Exchange: It directs the default route of 0.0.0.0/0 on Vnet2 and Vnet3 to the Boston datacenter over an ExpressRoute circuit. Vnet1 will get the default from BGP and propagate it to Vnet2 and Vnet3

Service Key: identifies an ExpressRoute circuit. If you need assistance/yardim from Microsoft or from an ExpressRoute partner to troubleshoot an ExpressRoute issue, provide the service key to readily identify the circuit.

ExpressRout’e Bagli Vnet’e Baska Vnet’ler Peering Yapilirsa: Connect all the virtual networks to the ExpressRoute FastPath circuit directly. To avoid traffic being routed through the VNet gateways, connect all the VNets to ExpressRoute FastPath circuit directly.

ExpressRoute Gateway: ExpressRoute kurulacak Vnet’lere kurulur.

**FIREWALL:**

Firewall: Statefull; FQDN filtering; FQDN tags; Network traffic filtering rules; Outbound SNAT support; Inbound DNAT support; Centrally create, enforce, and log application and network connectivity policies across Azure subscriptions and VNETs; Fully integrated with Azure Monitor for logging and analytics.

Application Rule: defines fully qualified domain names (FQDNs) that can be accessed from a subnet.

Network Rules: defines source address, protocol, destination port, and destination address.

DNAT Rule: Inbound Internet connectivity can be enabled by configuring Destination Network Address Translation (DNAT). Gelen trafigi configure ederiz.

Forced Tunneling: You can configure Forced Tunneling during Firewall creation by enabling Forced Tunnel mode. You cannot enable it once Firewall is created.

Azure Custom Route: The Azure Windows VMs need to connect to the Azure KMS server for Windows activation. The activation requires that the activation request come from an Azure public IP address. To resolve the problem, use the Azure custom route to route activation traffic to the Azure KMS server. Onceden A rule routing of 0.0.0.0/0 to FW1 in RT1 which is associated Subnet1 var.

Resource Group: The firewall, VNet, and the public IP address all must be in the same resource group.

Forced Tunneling: Management Subnet and Management Public IP is empty; it means NO FORCE TUNNELING. Force tunnelling can only be enabled during FW creation.

**Load Balancer:**

Front Door Service: is an application delivery network that provides global load balancing and site acceleration service for web applications. It offers Layer 7 capabilities for your application like SSL offload, path-based routing, fast failover, caching, etc. to improve performance and high-availability of your applications.

Front Door: requires a public IP or publicly resolvable DNS name to route traffic. So, AFD directly cannot route within a virtual network, but using an Application Gateway or Azure Load Balancer in between will solve this scenario. Farkli regionlardaki Vnet’lerdeki VM’lere ulasabilmek icin arada an Application Gateway or Azure Load Balancer gerekli.

Front Door Configure Routing Rules: HTTP protocols (HTTP/HTTPS), Hosts, and Paths configure edilir.

Custom Rule That Uses a Match Rule: Custom rules allow you to create tailored rules to suit the exact needs of your applications and security policies. Now, you can restrict access to your web applications by country/region. As with all custom rules, this logic can be compounded with other rules to suit the needs of your application. To create a geo-filtering custom rule in the Azure portal, simply select Geo location as the Match Type, and then select the country/region or countries/regions you want to allow/block from your application.

Traffic Manager: DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. It improves application responsiveness by directing traffic to the endpoint with the lowest network latency for the client. It doesn’t support URL routing.

* Degraded: Ilgili endpoint zayif calismiyor.
* Once child profile’a sevkeder.
* Child Profile: Ena z bir calisan endpoint olmali yoksa calismaz.
* Ilgili region calismiyorsa en yakin regiona sevkeder.
* Farkli routing methodlarini destekler: weigted, … Boylece Active/Standby seklinde iki web app kurulabilir.
  + Performance: when you have endpoints in different geographic locations, and you want end users to use the "closest" endpoint for the lowest network latency.
  + Geographic: direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically.
  + Priority: When you have a primary service endpoint for all traffic. You can provide multiple backup endpoints in case the primary or one of the backup endpoints is unavailable. (failower durumuna karsin alternatif)
* **Multivalue** traffic routing: method allows you to return multiple healthy endpoints and helps increase the reliability of your application since clients have more options to retry without having to do another DNS lookup. External endpoint’leri destekler.
* CheckingEndpoint: Degragaded degildir. Bu endpoint’e gelen request’leri cavaplar.
* CNAME records: Sadece bu record ile calisir.

Endpoint Monitor Settings in Traffic Manager: You need to configure endpoint monitoring settings – Tolerated number of failures - This value specifies how many failures a Traffic Manager probing agent tolerates before marking that endpoint as unhealthy. Its value can range between 0 and 9. A value of 0 means a single monitoring failure can cause that endpoint to be marked as unhealthy. If no value is specified, it uses the default value of 3.

Upload the public key certificate to the HTTP settings: You configure the listener for HTTPS by uploading an enterprise-signed certificate. And to be sure that the application gateway can provide end-to-end encryption for App1.

Rules: You need to configure rules to route traffic. URL Path Based Routing allows you to route traffic to back-end server pools based on URL Paths of the request.

CNAME record that maps www.healthengine.com to TMprofile1.trafficmanager.net: as1.healthengine.com ve as2.healthengine.com apps’larina Traffic Manager’in trafigi route etmesi icin kullanilir. Traffic Manager only supports custom domain mapping with CNAME records, and because DNS standards don't support CNAME records for mapping root domains (for example, **contoso.com**), Traffic Manager doesn't support mapping to root domains. To work around this issue, use a URL redirect from at the app level.

Public IP Address SKU: Load balancer and the public IP address SKU must match when you use them with public IP addresses.

High Availability for the NVAs: The NVAs will be used to inspect all the traffic within the virtual network. Azure Standard Load Balancer with HA ports for appliances, high availibility saglar.

Standard Load Balancer: It supports outbound connections.

Azure Load Balancer: It is a regional load balancing solution.

Floating IP Enabled: Standard Load balancer provides several capabilities for both UDP and TCP applications. If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

Application Load Balancer ile Iki Backend Pool’a Routing: [www.site1.com](http://www.site1.com) ve [www.site2.com](http://www.site2.com) adreslerini iki ayri backend pool’daki VMSS-VM-IP address/FQDN-App Service’lere yonlendirmek icin:

* Add two backend pool: Her iki VMSS icin backend pool’lar olusturulur.
* Add two listener: Her iki pool icin ayri olusturulur.
* Add two rules: Listenerlerdeki request’leri ilgili rule’a sevkedecek rule’lar olusturulur.

Listener Policy & Global Policy to Azure Application Gateway: Herhangi bir Listener’a associate edilmeyen policy global policy olur. Her Listener kendine associate edilen policy’i dikkate alir. Eger Listener’a policy associate edilmemisse o zaman global policy calisir.

Azure Application Gateway: Azure Application Gateway supports end-to-end encryption of traffic. It terminates the SSL connection at the application gateway. The gateway then applies the routing rules to the traffic, re-encrypts the packet, and forwards the packet to the appropriate back-end server based on the routing rules defined. Secure all communications by using Secured Socket layer (SSL). SSL encryption and decryption is processed efficiently to support high traffic load on the web application.

Rewrites: Application Gateway allows you to rewrite/modify selected content of requests and responses. Application Gateway allows you to add, remove, or update HTTP request and response headers while the request and response packets move between the client and back-end pools.

Port Forwarding: Load balancer’a gelen bir RDP baglantisini yalniz VM1’e sevketmek icin inbound NAT port-forwarding rule olusturulur. Inbound NAT rule olarak gecer.

**NAT GATEWAY**:

NAT gateway: Any outbound configuration from a load-balancing rule or outbound rules is superseded by NAT gateway. The VM will use NAT gateway for outbound connections.

SNAT Ports: A single NAT gateway resource supports from 64,000 up to 1 million concurrent flows. Each IP address provides 64,000 SNAT ports to the available inventory. You can use up to 16 IP addresses per NAT gateway resource. If some users report that they cannot access internet resources during peak hours and in Azure Monitor, you discover many failed SNAT connections so add public IP address.

Public IP Address: NAT Gateway yalniz Standard SKU Public IPv4 IP addresi ile calisir.

**NETWORK:**

Azure App Service: is delegate to create resources in the virtual network. So you need configure vNet integration for Azure app service. An integration subnet is required to integrate Azure App service with virtual network.

GatewaySubnet: Virtual network gateway icin deidicated subnet gerekli.

SQL Managed Instance: is placed inside the Azure virtual network and the subnet that's dedicated to managed instances.

Provision Virtual Network Gateways: Virtual network gateway allows to establish connectivity between two virtual networks. Virtual networks can be in different regions and from different subscriptions. When you connect VNets from different subscriptions, the subscriptions don't need to be associated with the same Active Directory tenant. Baglanti icin VPN kurulur.

Regional Virtual Network Integration: The Azure App Service and a Vnet are in the same region. When you connect to virtual networks in the same region, you must have a dedicated subnet in the virtual network you're integrating with.

Azure Private Link: enables you to access Azure PaaS Services over a private endpoint in your virtual network. Azure Storage, Azure SQL Database ve Azure Cosmos DB icin olusturulabilir. Private bir IP adresi ile endpoint olusturulur. Boylece diger resource’lar public ip addresi gerekmeden bunlara ulasabilir. Private endpoint bir subnet’e uygulanmissa diger subnetteki resource’larda onu kullanabilir.

Service Endpoints: provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. It does not restrict traffic. Public IP’ri expose eder.

Virtual Hub: Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity. From your on-premises network (vpnsite), you can connect to a VPN Gateway inside the virtual hub, connect ExpressRoute circuits to a virtual hub, or even connect mobile users to a Point-to-site gateway in the virtual hub. The hub is the core of your network in a region. Multiple virtual hubs can be created in the same region.

Network Virtual Appliance (NVA): Azure Virtual WAN supports connections from networking partners, such as VMware SD-WAN. These types of devices are known as network virtual appliances (NVAs).

Iki Ayri Peering’li Vnet’I Ortadaki Vnet’in Route Etmesi:

* On the peering from Vnet1, select Allow Gateway Transit.
* On the peerings from Vnet2 and Vnet3 to Vnet1, select Use Remote Gateways.

**NSG**:

Service Tag: represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules. You can use service tags to define network access controls on network security groups or Azure Firewall. Use service tags in place of specific IP addresses when you create security rules. By specifying the service tag name, such as **AzureCosmosDB, Storages**, in the apropriate source or destination field of a rule, you can allow or deny the traffic for the corresponding service.

Application Security Group: allows you to group virtual machines and define network security policies based on those groups.

Default Rules:

* Internetten gelen trafige kapalidir.
* Subnet to subnet is allowed.

**PRIVATE ENDPOINT**:

Private Endpoint: Subnet’te olusturulur ve ilgili storage account/blob’a izin verir. Baska Subnet’ler de bu private endpoint’i kullanabilir.

**TROUBLESHHOTING**:

Traffic Analytics: cloud-based solution that provides visibility into user and application activity in cloud networks. You must create a log analytics workspace and a storage account. VM’ni analiz edeceksek once NSG flow logs kurulur.

IP flow verify: enables to specify a source and destination IPv4 address, port, protocol (TCP or UDP), and traffic direction (inbound or outbound). IP flow verify then tests the communication and informs you if the connection succeeds or fails.

Connection Troubleshoot: enables to test a connection between a VM and another VM, an FQDN, a URI, or an IPv4 address. The test returns similar information returned when using the connection monitor capability, but tests the connection at a point in time, rather than monitoring it over time, as connection monitor does.

Connection Monitor: provides end-to-end connection monitoring in Azure Network Watcher. You can check the connectivity between your on-premises setups and the Azure VMs that host your cloud application. It provides you average round-trip time (RTT) values on a per-minute granularity. Region bazinda kurulur.

Network Watcher: we can capture all the network traffic of VM1 by using Azure Network Watcher and save to Azure storage account or a local path on VM1.

Network Performance Monitor: a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.  
You can monitor network connectivity across cloud deployments and on-premises locations. So, you can detect network issues before users complain.

NSG flow logs: allows you to log information about IP traffic flowing through an NSG.

**VIRTUAL NETWORK GATEWAY:**

/\*: Ozellikle /videos, /photos/cats vb rule’lara uymayan tum request’ler yonlendirilir bu rule’a. Azure front door rule’udur.

/videos/11/\*: /videos/11/deneme request’i gelirse rule’ler arasinda /videos/11, /\* olsa da bu rule uygulanir.

400: Bad Request Error HTTP Response: Herhangi bir rule ile match etmediginde gonderilir.

**VPN:**

Radius Server:  to create an Azure Point-to-Site (P2S) VPN connection that will use OpenVPN. On-premise Active Directory domain will be used for authentication. You need to deploy Radius server to support the VPN authentication. The authentication methods:

* RADIUS server
* VPN Gateway native certificate authentication
* Native Azure Active Directory authentication (Windows 10 only)

BGP for a Site-to-Site VPN connection between the datacenter and Azure:

* Virtual network gateway
* Local network gateway

Border Gateway Protocol (BGP): You must use BGP to advertise on-premises routes to the Microsoft Edge router. You cannot create user-defined routes to force traffic to the ExpressRoute virtual network gateway if you deploy a virtual network gateway deployed as type: ExpressRoute’lu iki ayri region’daki Vnet’lerin en yakinlarinda bulunan on-prem service’lere gitmesini, on premlerin hata vermesi durumunda diger on-prem server’a gitmelerini saglar.

Route Based: VPN devices use any-to-any (wildcard) traffic selectors, and let routing/forwarding tables direct traffic to different IPsec tunnels. It is typically built on router platforms where each IPsec tunnel is modeled as a network interface or VTI (virtual tunnel interface). It is critical if you want to set up a VPN-based mesh topology in Azure or to/from multiple on-premise sites. ExpressRoute fail olursa Site-to-Site VPN’e gecebilir.

Policy Based & Static Routing: Policy-based (sometimes called as static routing) VPN devices use the combinations of prefixes from both networks to define how traffic is encrypted/decrypted through IPsec tunnels. It is typically built on firewall devices that perform packet filtering. IPsec tunnel encryption and decryption are added to the packet filtering and processing engine. Active-Active VPN not possible.

tablo içeren bir resim

Açıklama otomatik olarak oluşturuldu

VPN Gateway: Virtual Network Gateway olarak da tanimlanabilir ve VPN kurulan Vnet’e kurulur.

Virtual Network Gateway: A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

Hub-Spoke Peering VPN: To allow gateway traffic to flow from spoke to hub and connect to remote networks. Eger peering veya network topologs’sinde degisiklik yapilirsa on-prem’deki Windows client’a Vpn client package for Windows clients yeniden download/reinstall edilmeli.

* Configure the peering connection in the hub to **allow gateway transit**.
* Configure the peering connection in each spoke to **use remote gateways**.
* Configure all peering connections to **allow forwarded traffic**.
* RemoteVirtualNetworkId $spoke.id AllowGatewayTransit
* RemoteVirtualNetworkId $hub.id UseRemoteGateways

Route Table: Route table ile yonlendirilen trafik VPN’i kullanmak yerine burayi kullaniyor demektir.

Peering: VPN ile peered Vnet’lere ulasilabilir ama VPN client’e reinstall edilmeli.

IKEDiagnosticLog: The IKEDiagnosticLog table offers verbose debug logging for IKE/IPsec. This is useful to review troubleshooting disconnections, or failure to connect VPN scenarios.

Virtual WAN: architecture is a hub and spoke architecture for branches and users. It enables global transit network architecture, where the cloud-hosted network 'hub' enables transitive connectivity between endpoints that may be distributed across different types of 'spokes'. All hubs are connected in full mesh in a Standard Virtual WAN making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity. This satisfies the requirement to provide the quickest set up at the lowest cost. On-prem ile Vnet arasindaki Expressroute’a baska on-premier ve several remote employees eklemek icin kullanilir.

Virtual WAN: There are two types of virtual WAN types – Basic & Standard.

* Virtual WAN Basic: Sadece S2S VPN’I destekler.
* Virtual WAN Standard: P2S VPN, S2S VPN and ExpressRout’u destekler.

metin içeren bir resim

Açıklama otomatik olarak oluşturuldu

Basic SKU: does not support outbound rules. Internetten veri gelecekse LA’ya Basic SKU kullanilmaz. Point-to-Site (P2S) VPN’i de desteklemez.

Scale Unit:

* 1 scale unit of VPN = 500 Mbps.
* 1 scale unit of ExpressRoute = 2 Gbps

Point-To-Site VPN: can use one of the following protocols:

* OpenVPN:  Configure Azure Active Directory (Azure AD) authentication. It’s 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). Sonra deneme.com tenant’inda Grant consent to an Azure AD application.
* **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), Windows.

**WAF:**

Rule: Ne kadar kisitlama tanimlanacaksa o kadar rule tanimlanir.

Rule Modify: AFD onunde ve tek lokasyona tanimli rule 3 farkli lokasyona tanimlanacaksa sadece mevcut rule’a diger iki lokasyonun IP adres’leri eklenir.

Rule Tanimlama: Herbir policy icin yeni rule olusturduk.

* Create a custom rule
* Create a policy: gelen requestin header’i ”video” iceriyorsa <https://www.deneme.com/videos> ’a yonlendirir.
* Create an association