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.

**DOMAIN:**

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.

**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 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.

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

Connection Monitor: provides end-to-end connection monitoring in Azure Network Watcher. You can use connection monitor to check the connectivity between your on-premises setups and the Azure VMs that host your cloud application.

**FIREWALL:**

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).

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.

**Load Balancer:**

Azure 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.

Azure 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.

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

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.

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.

**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.

**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.

**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**, 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.

**PRIVATE ENDPOINT**:

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

**TRAFFIC ANALYTICS**:

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.

**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

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.

**WAF:**

Rule: Ne kadar kisitlama tanimlanacaksa o kadar rule tanimlanir.