1. Azure Front Door

Azur service designed to implement scalable and secure entry points for fast delivery of your global applications

Network Connections

1. Virtual Network
2. Virtual WAN
3. ExpressRoute
4. VPN
5. DNS

Network Monitoring

1. Network Watcher
2. ExpressRoute Monitor
3. Azure Monitor
4. Virtual Network TAP

Network Protection

1. DDoS Protection
2. Firewall
3. NSG
4. Web Application Firewall
5. Virtual Network Endpoints

Network Deliver

1. CDN - Content Delivery Network Ex- You tube Service
2. Front Door

* Global POP, HTTP(s) traffic, Layer 7 traffic

1. Traffic Manager - Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

* Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.
* Traffic routing methods: Priority, Weighted, Performance, Geographic. Multivalue, Subnet.
* Global POP, Non HTTP(s) traffic, Layer 4 traffic
* Delivers exceptionally high availability of applications through endpoint monitoring
* automatic failover
* Enhances responsiveness for applications that need high-performance.

The Azure Traffic Manager service is a DNS-based traffic load balancer that distributes traffic across services that are distributed across different Azure regions.

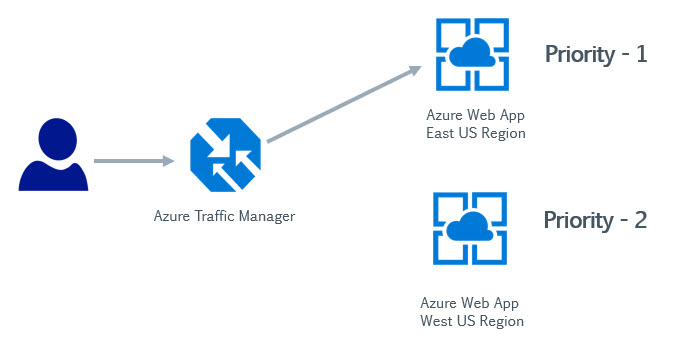
The Traffic Manager service is used to direct client requests to the most appropriate service endpoint that is based on a traffic-routing method and the health of the endpoints.

The different traffic routing methods available for the Azure Traffic Manager are

* Priority – Route traffic to another endpoint in case the primary fails.
* Weighted – Route traffic to different endpoints based on weight.
* Performance - you want end users to use the "closest" endpoint in terms of the lowest network latency.
* Geographic - geographic location their DNS query originates from.
* Multivalue – Here different endpoints are sent to the client. The client then selects the endpoint to send the request to.
* Subnet – This maps a set of end-user IP address ranges to a specific endpoint within a Traffic Manager profile.

Below is an example of the Priority routing method that can be used with the Azure Traffic Manager service

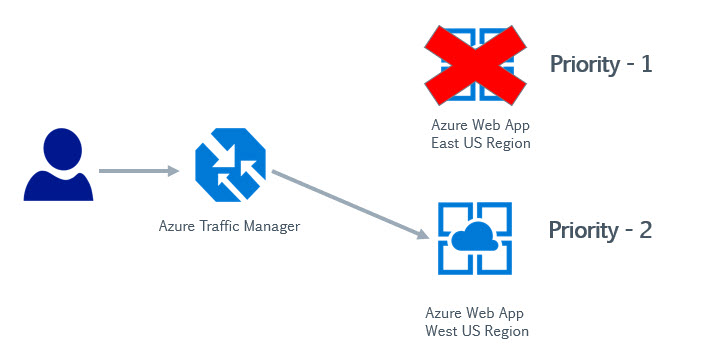
Here we are assuming that a company has similar web applications , both are running using the Azure Web App service. One web application is running in the East US Region and the other is running in the West US Region.



1. Here we create a Traffic Manager profile and create two endpoints. Each endpoint points to each Azure Web app respectively. We assign a priority of 1 to the service endpoint attached to the Azure Web App running in the East US region and  a priority of 2 to the other service endpoint.

1. Here users would make requests to the Traffic Manager service.

2. The requests could be initially be directed to an Azure Web App located in the East US region , since there is a priority of 1 to the service endpoint attached to this endpoint.

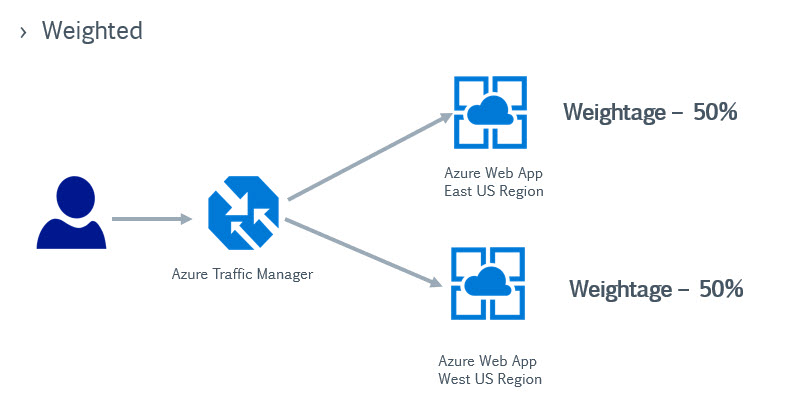


3. Now let's say there is an issue with the web application running in the East US region, Azure Traffic Manager would then understand that there is an issue with the web application running in this region.

It would then start redirecting user requests to the second endpoint which has the Priority of 2.

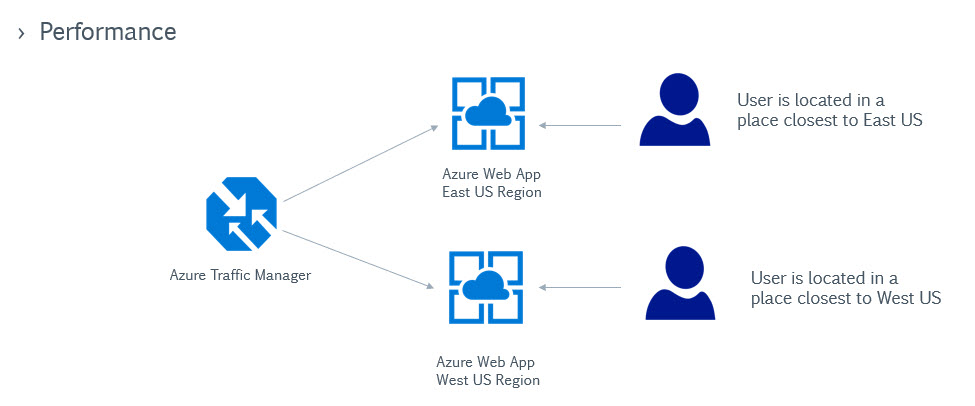
Hence over here you are adding a higher availability to your architecture by ensuring that user requests are always adhered to by redirecting requests if the primary service fails for any reason.

If you use the Weighted Routing method , you can actually load balance requests across multiple service endpoints

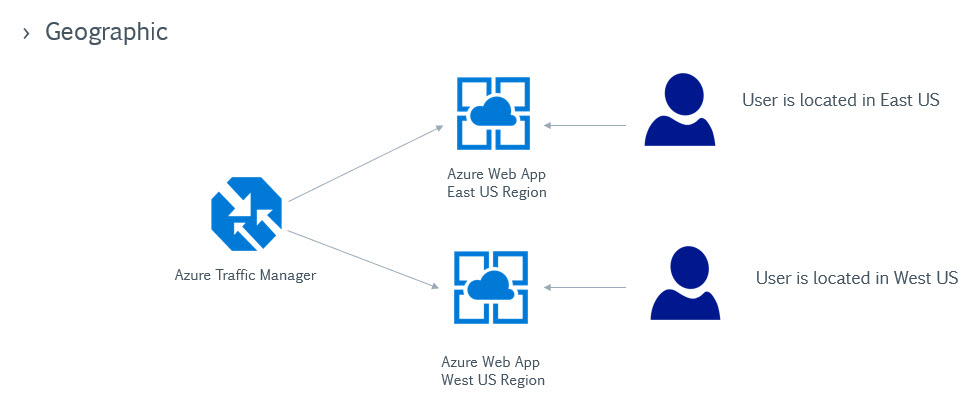


Over here , users requests would be directed or load balanced across both web applications running in different regions.

In the Performance routing method as shown below, users will be directed based on the least latency of an endpoint.



And then we have the Geographic routing method wherein users would be directed to an endpoint based on their geographic location



1. Application Gateway - Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers.

* Regional POP, HTTP(s) traffic, Layer 7 traffic
* This type of routing is known as application layer (OSI layer 7) load balancing.
* This service is a web traffic load balancer that is used to distribute traffic to web applications.
* The web applications can reside on Virtual Machines, Virtual Machine Scale sets or even on on-premise servers.
* The Application gateway is an OSI Layer 7 load balancer.

Some of the features of the Azure Application Gateway Service

**Secure Sockets Layer (SSL/TLS) termination**

* Here requests to the Application Gateway can be secure.
* And then the requests to the backend pool resources can go unencrypted.
* This can lift the burden of the backend pool for decrypting requests.
* The decryption of requests can be left to the Application gateway resource.

**Autoscaling**

* Here the Application Gateway can scale based on demand.
* You can also distribute the deployment of the Application Gateway across multiple zones to ensure better availability of the Azure Application Gateway service

**Web Application Firewall**

* This feature provides protection of your web applications against common exploits and attacks from the Internet
* Here your application could be protected against SQL injection and cross-site scripting attacks
* The Web Application Firewall uses a set of rules to protect your web applications. These rules are based on the Open Web Application  Security Project. These rules are automatically updated to ensure all the latest threats are included in the rules.
* You can also create your own custom policies for your Web Application Firewall

**Components of the Azure Application Gateway**

**Frontend IP address**– Users will hit the Application Gateway via the Frontend IP address.

**Listener** – This is a logical entity that checks for incoming connection requests. There can be multiple listeners attached to an application gateway.

There are 2 types of Listener configurations

**Basic** – Here the listener listens to a single domain site

**Multi-site** – Here the listeners maps to multiple domain sites.

**Routing Rules**– This is used to route the traffic from the listener to the backend pool.

There are 2 types of routing rules

**Basic** – Here all requests are routed to backend pool directly.

**Path-based**– Here requests are routed to the backend pool based on the URL in the request.

**Backend pools** – These can be Network Interface cards , Virtual Machine scale sets , Public or Internal IP addresses , FQDN or backends such as App Service.

**Health Probes** – This defines how the application gateway will monitor the health of the resources in the backend pool.

1. Load Balancer

* Regional POP, Non HTTP(s) traffic, Layer 4 traffic

#### ****Availability Sets****

When you host your virtual machines in Azure, you sometimes need to cater to the following

1. An unplanned event wherein the underlying infrastructure fails unexpectedly. The failures could be attributed to network failures , local disk failures or even rack failures.
2. Planned maintenance events , wherein Microsoft needs to make planned updates to the underlying physical environment. In such cases , a reboot might be required on your virtual machine.

You can increase the availability of your application by making use of availability sets. Each virtual machine that is assigned to the availability set is assigned a separate fault and update domain.

**Fault domains** are used to define the group of virtual machines that share a common source and network switch. You can have up to 3 fault domains.

**Update domains** are used to group virtual machines and physical hardware that can be rebooted at the same time. You can have up to 20 update domains.

#### ****Availability Zones****

* This features help provides better availability for your application by protecting them from datacenter failures.
* Each Availability zone is a unique physical location in an Azure region.
* Each zone comprises of one or more data centers that has independent power, cooling, and networking
* Hence the physical separation of the Availability Zones helps protect applications against data center failures
* Using Availability Zones, you can be guaranteed an availability of 99.99% for your virtual machines. You need to ensure that you have 2 or more virtual machines running across multiple availability zones

**Notes on Point-to-Site VPN Connection**

A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines an an Azure virtual network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

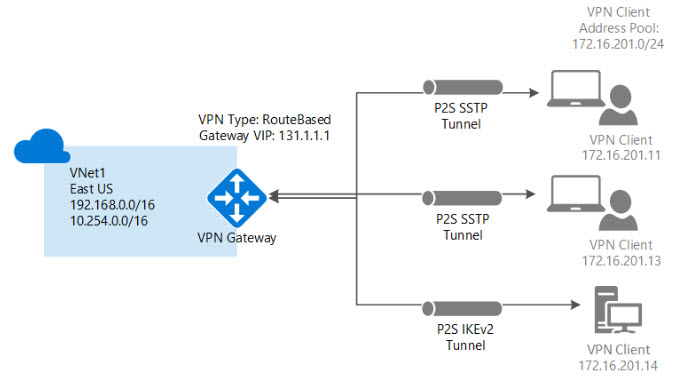


Image reference -<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

* This sort of connection is based off certificates for authentication.
* You need to have a root certificate in place that needs to be uploaded to Azure for the point-to-site connection.
* A client certificate needs to be generated from the root certificate. This client certificate needs to be on each client computer that needs to connect to the Azure virtual network via the Point-to-Site connection.
* To generate the certificates, you can use a Certificate authority or generate a self-signed certificate using PowerShell. Some commands are given below

**// To generate the root certificate**

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

-Subject "CN=RootCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

**// To generate the client certificate**

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `

-Subject "CN=ClientCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

**Notes on Site-to-Site VPN Connection**

A Site-to-Site VPN connection is used to establish a secure connection between an on-premise network and an Azure network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

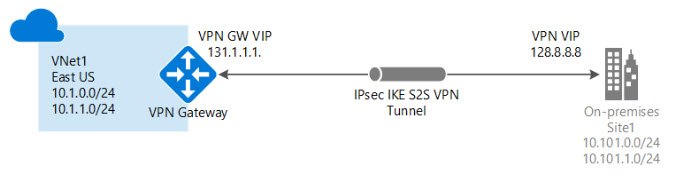


Image reference - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

* On the on-premise side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure. The VPN device can be a hardware device like a Cisco router or a software device ( e.g Windows Server 2016 running Routing and Remote services). The VPN device needs to have a publically routable IP address.
* The subnets in your on-premise network must not overlap with the subnets in your Azure virtual network
* The Site-to-Site VPN connection uses an IPSec tunnel to encrypt the traffic.
* The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premise data center and your Azure virtual network.
* There are different SKU's for the Azure VPN gateway service. Each SKU has a different pricing and attributes associated with it - Reference - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings>