4. Azure Virtual Networks(VNET)

Chapter 1 Azure virtual networks
↓
Chapter 2 Azure Application Gateway
↓
Chapter 3 Azure VPN gateway
↓
Chapter 4 Azure Load Balancer
↓
Chapter 5 Azure Firewall
↓
Chapter 6 Azure DNS
↓
Chapter 7 Azure Traffic Manager
↓
Chapter 8 Azure Front Door
↓
Chapter 9 Azure Bastion
↓
Chapter 10 Azure Private Link

References

An ***Azure Virtual Network*** (**VNet**) is a network or environment that can be used to run VMs and applications in the cloud.

Azure Virtual Network (**VNet**) is a representation of your own network in the cloud. It is a logical isolation of the **Azure** cloud dedicated to your subscription.

Key components of Azure VNets

- [ ] **Subnets :**

  Each Virtual Network can be divided into sub parts, these sub parts are called subnets.

  You can create any number of Subnets within a VNet. All the subnets must be fully contained in the virtual network address space and should not overlap with one another.

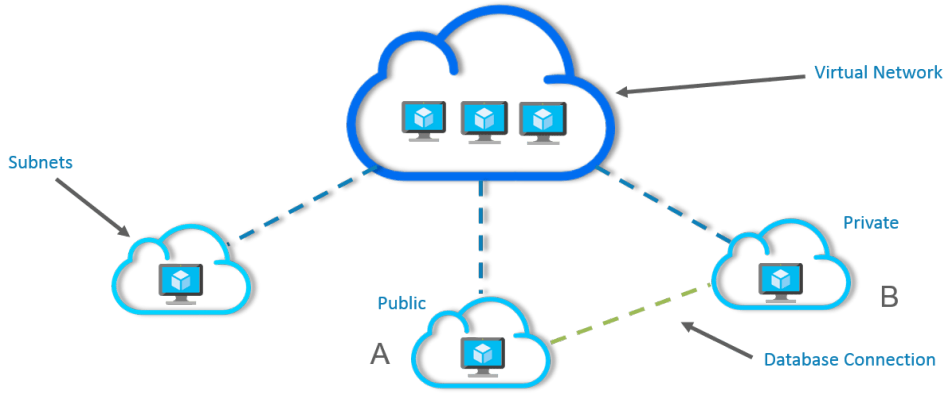
  A subnet can further be divided into:

  Private Subnet – A network in which there is no internet access.

  Public Subnet – A network in which there is internet access.

By default, when you create a VNet, it's also mandatory that you create a Subnet. You can also create multiple Subnets after you create a VNet.

The smallest subnet that Azure supports is a /29 and the largest is a /8 (using CIDR subnet definitions).



In the above image, a single virtual network has been divided into subnets and each subnet contains a server.

- **Subnet A** is a webserver and hence it is a public subnet because your website will be accessible over the internet.
- **Subnet B** is a database server and since a database should just be able to connect to the webserver, there is no need of an internet connection, hence it is a private subnet.

You might be wondering, where to do all these settings, which connections to allow and which not to, right?

*Well, that is where the second component comes into the picture i.e the **Network Security Groups**.*

Network Security Groups

This is where you do all your connection settings, like which ports to open, by default all are closed.

Network security group (NSG) contains a list of Access Control List (ACL) rules that allow or deny network traffic to your VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet. When a NSG is associated with a subnet, the ACL rules apply to all the VM instances in that subnet. In addition, traffic to an individual VM

can be restricted further by associating a NSG directly to that VM.

NSGs can have two type of rules

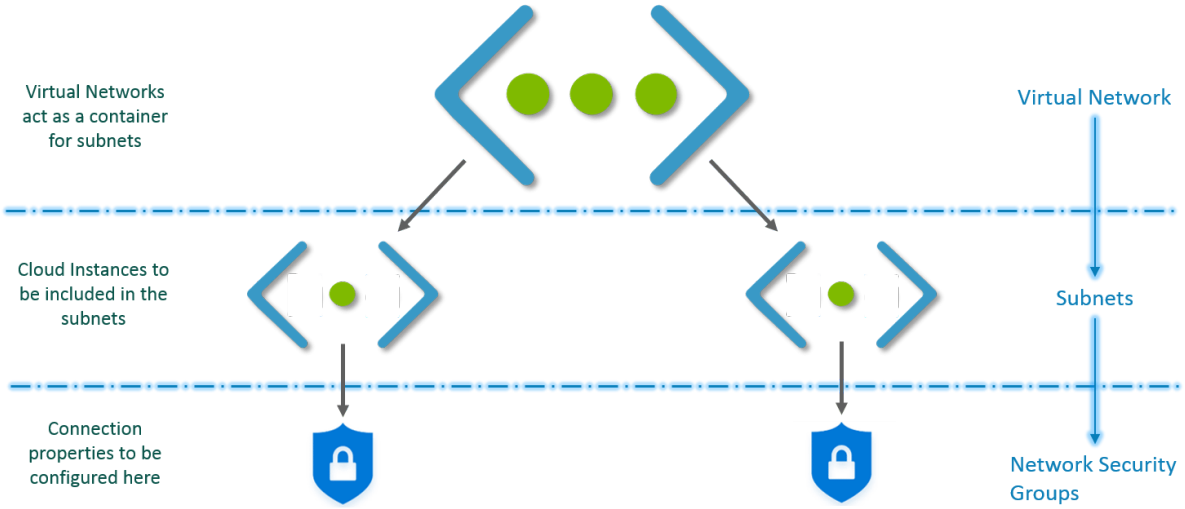
- *Inbound Rule*

  You can control all the Ingress using these Inbound rules

- *Outbound Rule*

  You can control all the Egress using these Outbound rules.

But first, let me show you how the final architecture for a Virtual Network looks like:



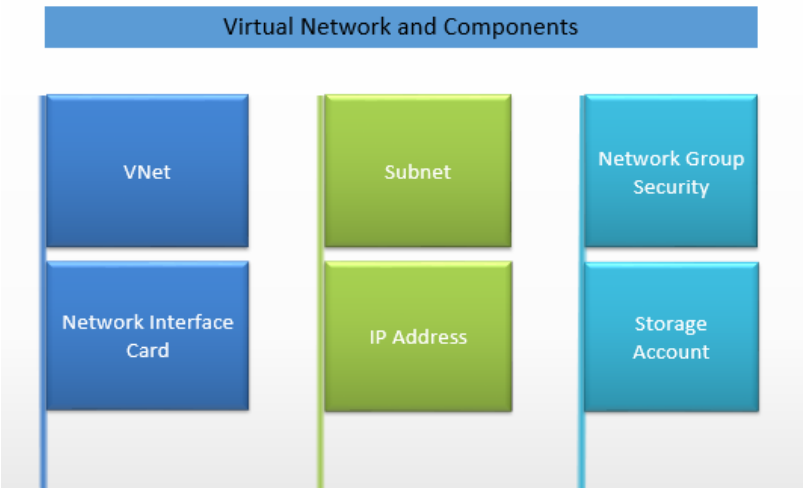
This is how Virtual Network works:

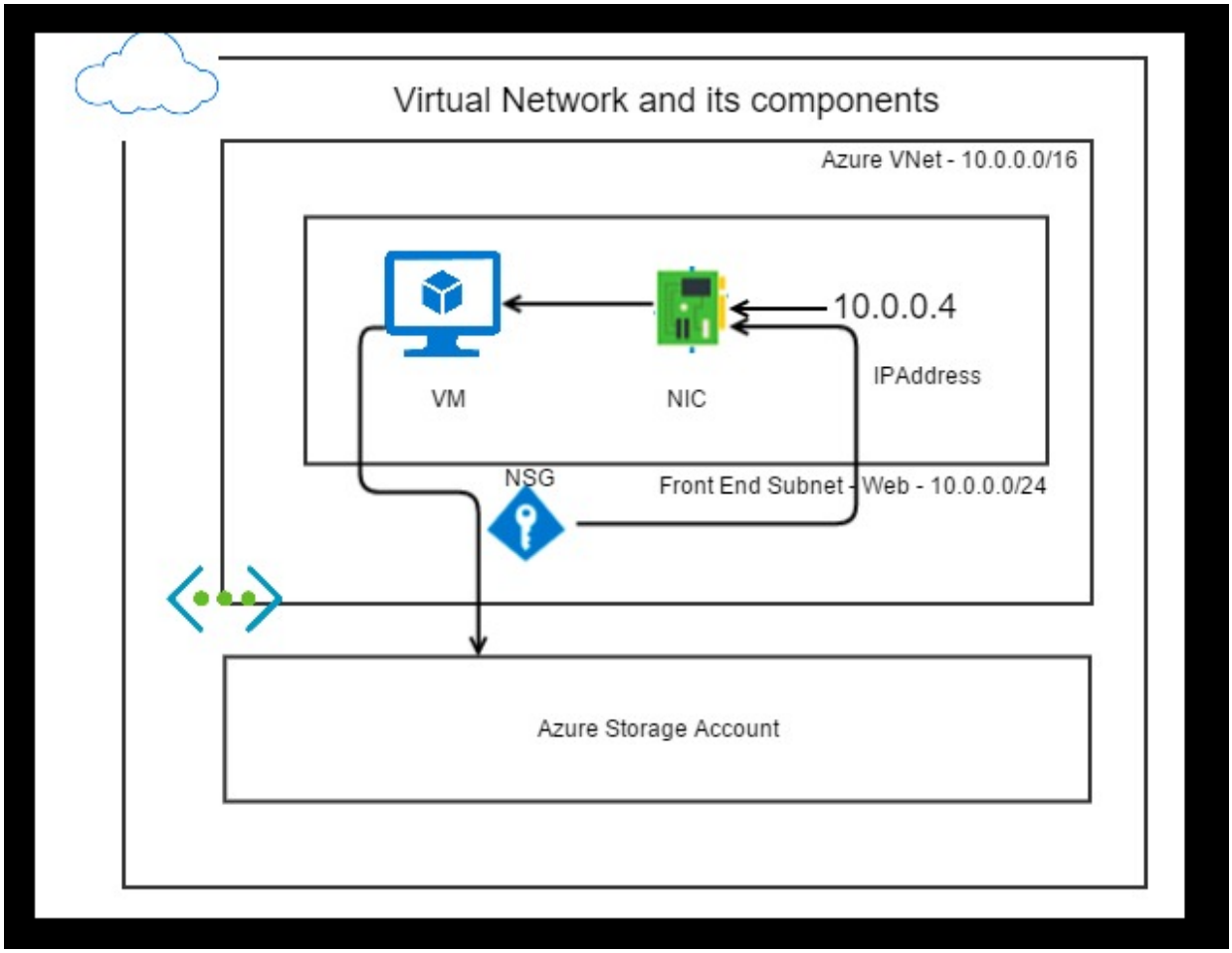
1. First you create a virtual network.
2. Then, in this virtual network you create subnets.
3. You associate each subnet with the respective Virtual Machines or Cloud Instances.
4. Attach the relevant Network Security Group to each subnet.
5. Configure the properties in the NSGs and you are set!

- [ ] **Routing**

- It delivers the data by choosing a suitable path from source to destination.
- For each subnet, the virtual network automatically routes traffic and creates a routing table.

Below are the components that are required for a VM to be provisioned in the Azure Cloud.





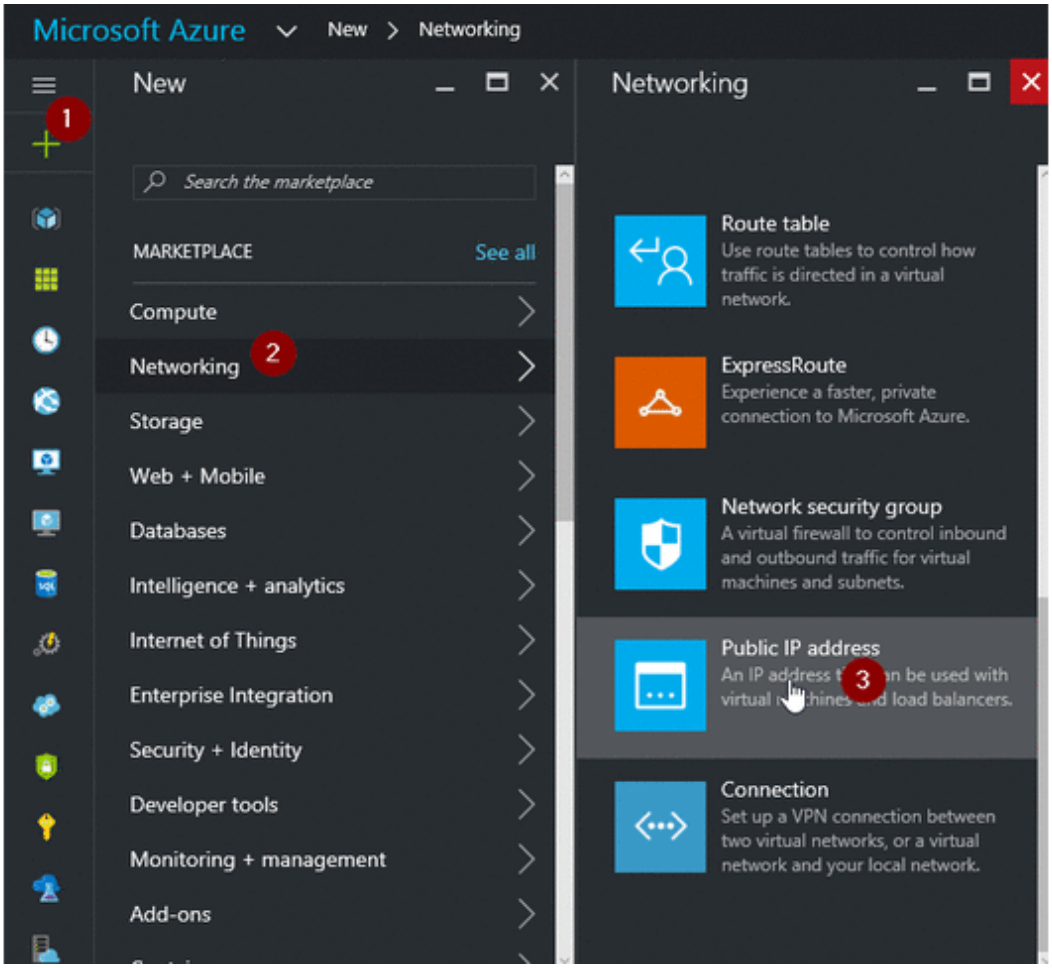
- [ ] Network Interface Card

A Virtual Machine could only be associated with a Virtual Network with the help of a Network Interface Card (NIC). You can think of NIC as a connection between a VM and VNet.
A NIC can be associated with both Private IP Address as well as a Public IP Address.
You can also associate a NSG to a NIC to allow or deny the traffic from and to the Virtual Machine that you attach to the NIC.

- [ ] **IP Address**

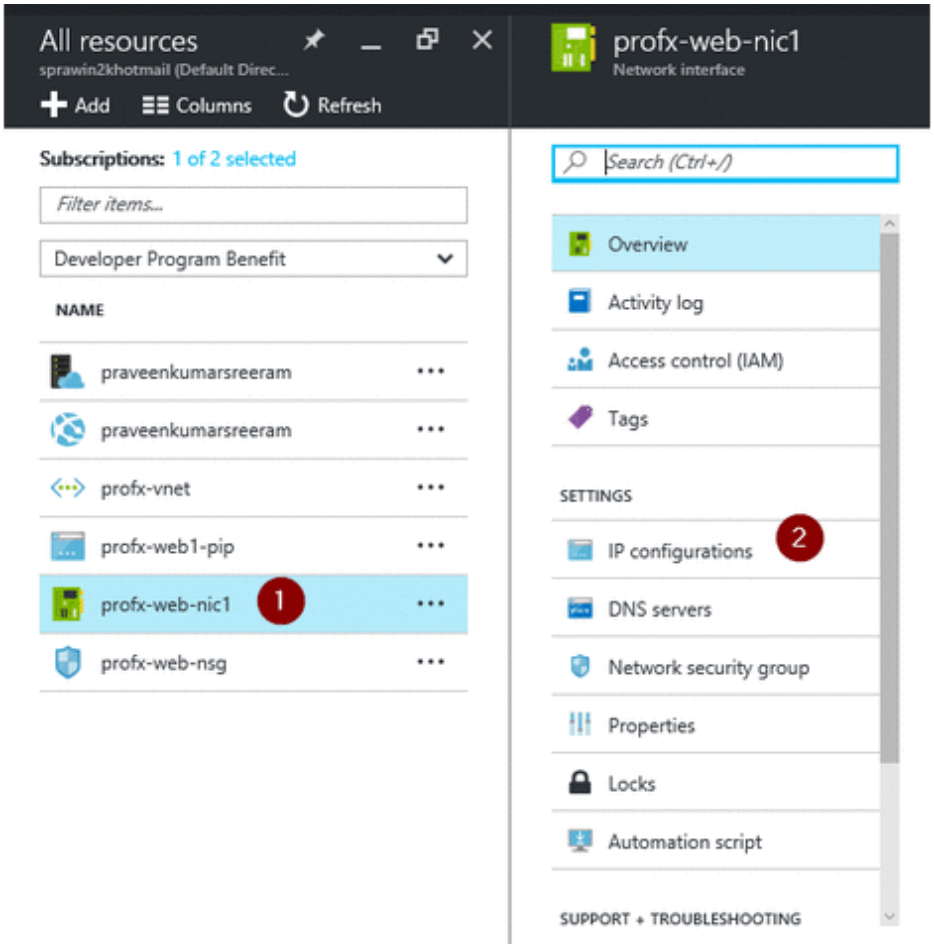
Each device within a network could be addressed using an IP Address. IP addresses allow all the network resources to be reached via a Network Interface.

- *Private IP Address*
  These type of addresses allows the resources to communicate between then within the Network.
- *Public IP Address*
  These are used to communicate with the resources across the internet.



How to associate NIC with an IP Address?

Once you create both the NIC (Network Interface Card) and IP Address, you need to associate both of them. Please find the following animated image for the steps to associate a NIC to an IP Address.



VNet Use Case

- VNet with a single public subnet.
- VNet with public and private subnets (NAT).

- [ ] **NAT Gateway**
  - Allows your virtual network resources to have an outbound-only connection.
  - A NAT gateway resource can use up to 16 static IP addresses.
  - You can use multiple subnets in a NAT gateway.
- [ ] **Application Security Group (ASG):**

  ASGs enable source/destination definition based on a label, rather than IP/network address. An ASG in and of itself is not actually a policy group, but rather an arbitrary definition that can be applied to resources, such as "AppServer",

"DataBase", "myApp", etc. This definition can later be used in rule inside an NSG. This is useful when a rule needs to be applied to resources based on their purpose, rather than their IP CIDR, which offers greater flexibility in policy application.

- [ ] **Virtual Network Gateway**: Virtual Network Gateway sits on the boundary of a VNet's subnet and enables connectivity between that subnet and other networks or VPNs. This is where most of the VPN configuration resides.
- [ ] **Local Network Gateway**: Local Network Gateway is a representation of customers gateway on the other end of the tunnel. This simply holds configuration that tunnel needs to know about to build a VPN tunnel to the other end
- [ ] **Border Gateway Protocol (BGP)**: When setting up a hybrid cloud, we need to ensure that both ends of connection know about networks that reside on the other end. While static routing is an option, it normally isn't the most suitable approach for a production network. In order to learn on-prem routes efficiently, there is a need for a routing protocol to communicate routes dynamically. BGP is the defacto choice of today, and Azure supports BGP over IPSec with route-based VPN options. With BGP running on top of you Azure VPN Gateway or ExpressRoute connection, you can propagate local BGP routes across your cloud and on-prem routers without the need for manual admin intervention. More information about the use of BGP with Azure VPN Gateway and ExpressRoute.

What should we do to communicate between two different VNet's inside azure?

- [ ] **VNet Peering**

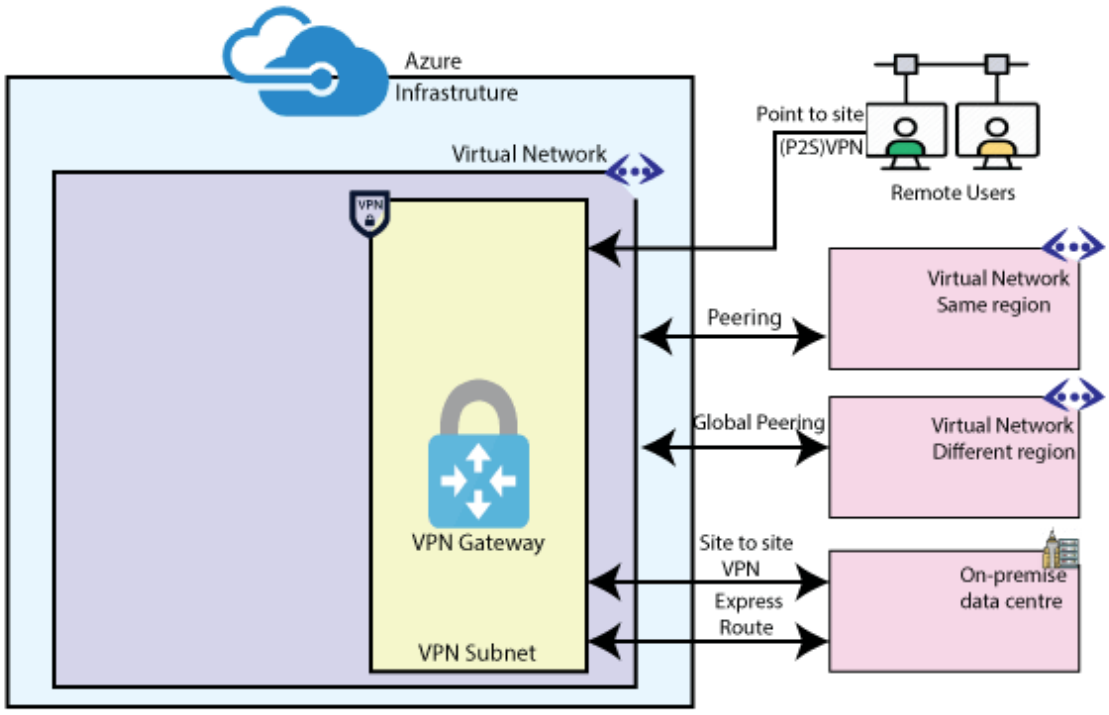
  With the help of VNet Peering, our azure resources can communicate with the private IP address.

- VNet Peering is one best option when compared to VPN Gateway.
- VNet Peering is a seamless connection between two different VNet's it works on the Azure Backbone network which means no need for public internet. In the case of VPN Gateway, we need the internet.
- If we want to communicate between two different VNet's in Different Region or Different Subscription we also have an option Azure that's called Azure Global VNet Peering, this also runs on azure backbone network no need public network and also a gateway.
- Now Global VNet is generally available.

How to communicate Azure resources with On-Premises

- [ ] **VPN Gateway**
    - We can communicate with Azure to On-Premises by the help of VPN Gateway.
    - VPN Gateway is like normal VPN, it is used to communicate with Azure resources.
- [ ] **Express Route**
    - We can use the express route to communicate between Azure and On-Premises.
    - It was huge cost when compare with VPN Gateway.
    - Because, it was dedicated route between Azure and on-premises, for the express route configuration we support from our On-Premises Internet Service Provider.
    - My suggestion if we have large number of resources then we can go for Express Route otherwise VPN Gateway.

Azure VNet Connectivity

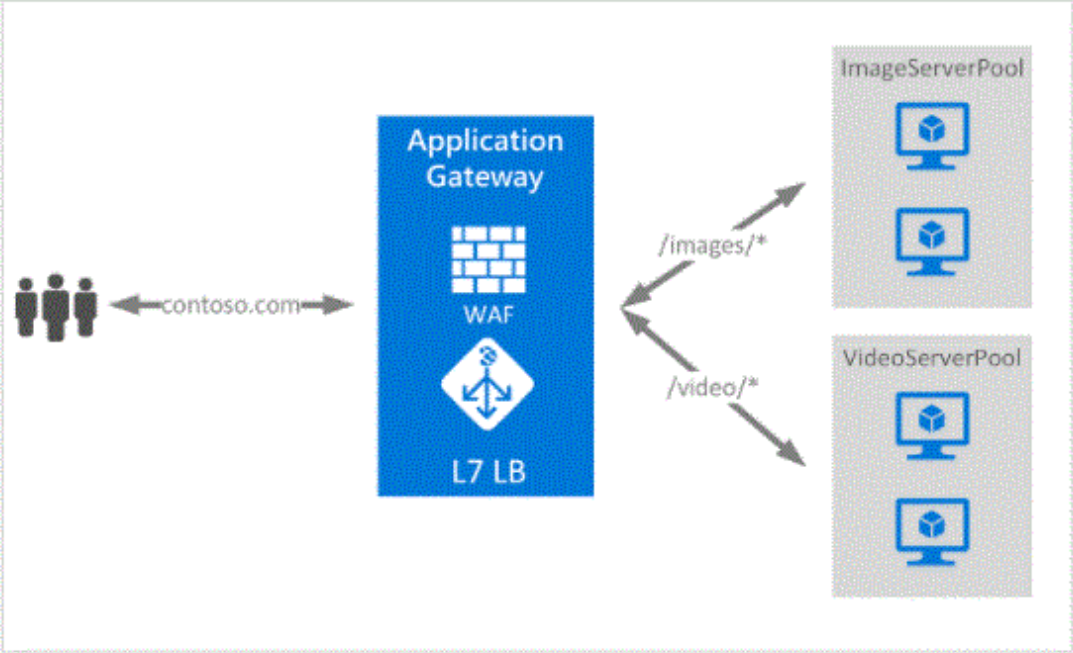


Azure Application Gateway

What is Azure Application Gateway?

- Azure Application Gateway is a web traffic load balancer that enables you to manage traffic on your web applications. Traditional load balancers operate at the transport layer (OSI Layer 4 – TCP and UDP) and route traffic to the destination IP address and port based on the source IP address and port.
- The application gateway can make routing decisions based on additional characteristics of the HTTP request, for example the URI path or the host header. For example, you can route traffic based on an incoming URL. So if /images is in the incoming URL, you can route the traffic to a specific set of servers (known as a pool) configured for the images. If /video is in the URL, that traffic is routed to another pool optimised for the video.Azure provides a suite of fully managed load-balancing solutions for your scenarios.
- If you want to perform DNS-based global routing and do not have Transport Layer Security (TLS) protocol termination ("SSL offload"), per-HTTP/HTTPS requests, or application-layer processing requirements, review Traffic Manager.

- If you need to optimise the global routing of your web traffic and optimise top-level end-user performance and reliability through accelerated global failover, check out Front Door.
- To perform network layer load balancing, review the load balancer. Your entire scenario can benefit from combining these solutions as needed. For a comparison of Azure load-balancing options, see Overview of load-balancing options in Azure.



- [ ] **Azure Application Gateway features:**

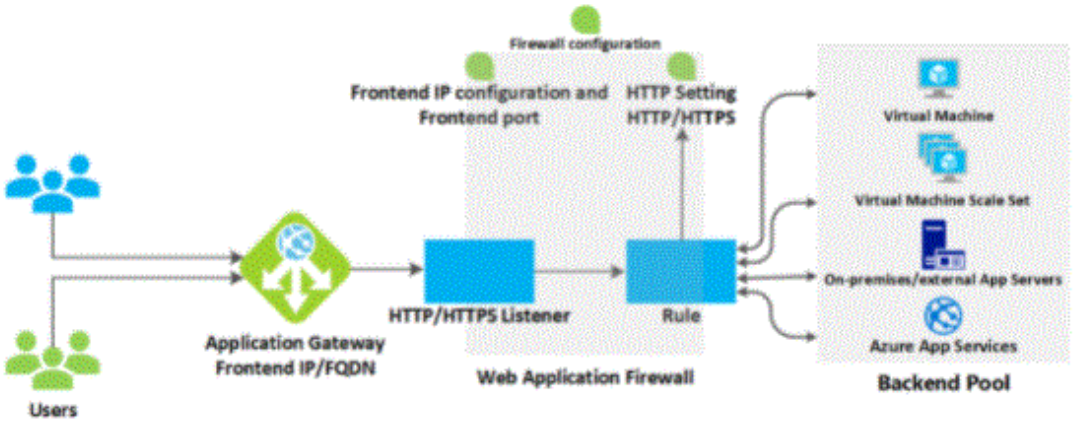
  Azure Application Gateway is a web traffic load balancer that enables you to manage traffic on your web applications.

- [ ] **Application gateway conceptual:**

  Application Gateway includes the following features:

  - Secure Sockets Layer (SSL/TLS) termination
  - Auto scaling
  - Field redundancy
  - Static VIP
  - Web application firewall
  - Access Controller for AKS
  - URL-Based Routing
  - Multi-site hosting

- Redirection
- Session affinity
- Websockets and HTTP/2 traffic
- Connection drainage
- Custom error page
- Rewrite HTTP Headers and URLs
- Shape



- **How an application gateway accepts a request:**
  - Before a client sends a request to an application gateway, it resolves the application gateway's domain name using a domain name system (DNS) server. Azure controls DNS entry because all application gateways are in the azure.com domain.

  - Azure DNS returns the IP address to the client, which is the frontend IP address of the application gateway. The application gateway intercepts incoming traffic on one or more listeners. A listener is a logical entity that examines connection requests. It is configured with the frontend IP address, protocol and port number for the connection from the client to the application gateway.

- If a Web Application Firewall (WAF) is in use, the Application Gateway checks the request header and body, if present, against the WAF rules. This action determines whether the request is a valid request or a security threat. If the request is valid, it is forwarded to the backend. If the request is not valid and the WAF is in containment mode, it is blocked as a security threat. If it is in detection mode, the request is evaluated and logged, but still forwarded to the backend server.

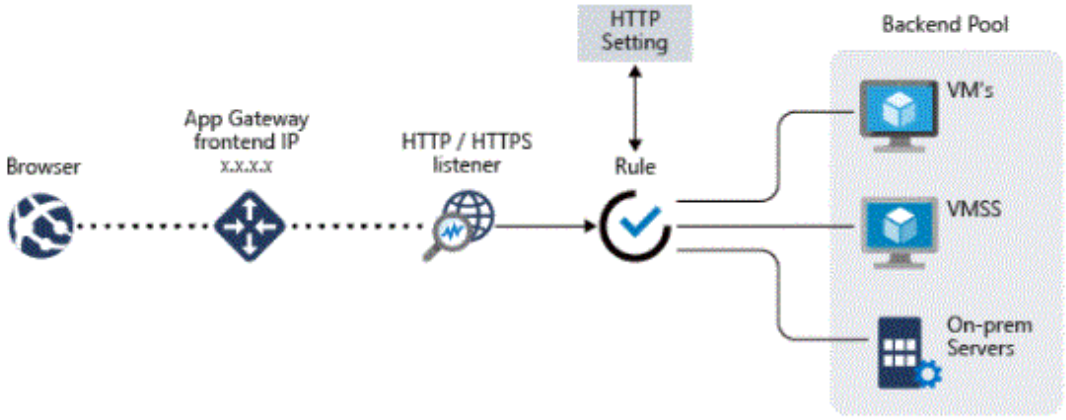
- Azure Application Gateway can be used as an internal application load balancer or as an Internet-facing application load balancer. An Internet-facing application gateway uses a public IP address. The DNS name of an Internet-facing application gateway is publicly resolvable to its public IP address. As a result, Internet-facing application gateways can route client requests to and from the Internet.

- Internal application gateways only use private IP addresses. If you are using a custom or private DNS zone, the domain name must be internally resolvable to the application gateway's private IP address. Therefore, internal load-balancers can only route requests from clients with access to the virtual network to the application gateway.

☐ **How an application gateway routes a request:**

- If a request is valid and is not blocked by the WAF, the application gateway evaluates the request routing rule that is attached to the listener. This action determines which backend pool to route the request to.
- Based on the request routing rule, the application gateway determines whether to route all requests on the listener to a specific backend pool, to make requests to different backend pools based on the URL path, or to another port or external site Redirect requests.

Reference: Application Gateway



- [ ] **Modifications to the request:**

- The Application Gateway inserts five additional headers into all requests before forwarding the requests to the backend. These headers are **X-Forwarded-For, X-Forwarded-Proto, X-Forwarded-Port, X-Origin-Host and X-APGW-Trace-ID**. The format of the x-forwarded-for header is a comma-separated list of IP: ports.
- Valid values for x-forwarded-proto are HTTP or HTTPS. X-Forwarded-Port Specifies the port where the request arrived at the application gateway. The X-Origin-Host header contains the original host header the request came with. This header is useful in Azure website integration, where the incoming host header is modified before traffic is routed to the backend. If session affinity is enabled as an option, it adds a gateway-managed affinity cookie.

- x-appgw-trace-id is a unique guid generated by the Application Gateway for each client request and presented in the request forwarded to the backend pool member. The guide consists of 32 alphanumeric characters without dashes (for example: ac882cd65a2712a0fe1289ec2bb6aee7). This guide can be used to correlate the request received by the application gateway and initiated to the backend pool member via the TransactionID property in the diagnostic log.

- You can configure Application Gateway to modify request and response headers and URLs to rewrite HTTP headers and URLs, or to modify the URI path by using the path-override setting. However, unless configured to do so, all incoming requests are proxied to the backend.

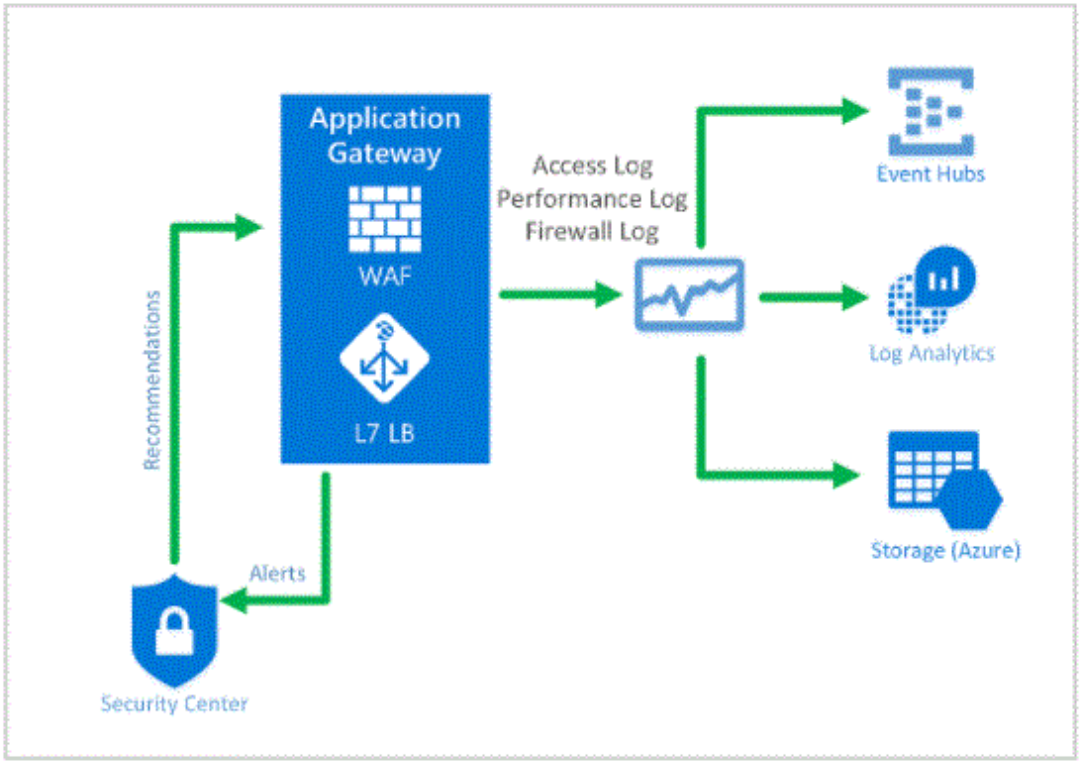
- [ ] **What types of logs does Application Gateway provide?**

  Application Gateway provides three logs:

  ApplicationGatewayAccessLog: The access log contains each request submitted to the Application Gateway frontend. Data includes the caller's IP, requested URL, response latency, return code, and bytes in and out. It has one record per application gateway.

  Application gateway performance log: The performance log captures the performance information for each application gateway. Information includes throughput in bytes, total requests served, failed request numbers, and healthy and unhealthy backend instance counts.

  Application gateway firewall log: For the application gateway you have configured with WAF, the firewall log contains requests that are logged either through detection mode or prevention mode.All logs are collected every 60 seconds. For more information, see Backend health, diagnostics logs and metrics for Application Gateway.



- **How is Azure Application Gateway used?**

  It primarily provides a complete, cloud based, secure and scalable load balancing solution for web applications and services. Some of the ways to use it include:
- Deliver and manage load balancing solutions for websites, web applications or Internet based services.
- Provide load balancing for internal web enabled/powered services.
- Provide cookie based session affinity service.
- Enable SSL Offloading service which removes the encryption/decryption burden from the primary web server.

	Load Balancer	Application Gateway	Traffic Manager	Front Door
Service	Network load balancer.	Web traffic load balancer.	DNS-based traffic load balancer.	Global application delivery
Network Protocols	Layer 4 (TCP or UDP)	Layer 7 (HTTP/HTTPS)	Layer 7 (DNS)	Layer 7 (HTTP/HTTPS)
Type	Internal and Public	Standard and WAF	–	Standard and Premium
Routing	Hash-based,Source IP affinity	Path-based	Performance, Weighted, Priority, Geographic, Multi Value, Subnet	Latency, Priority, Weighted, Session Affinity
Global/Regional Service	Global	Regional	Global	Global
Recommended Traffic	Non-HTTP(S)	HTTP(S)	Non-HTTP(S)	HTTP(S)
Endpoints	NIC (VM/VMSS), IP address	IP address/FQDN, Virtual machine/VMSS, App services	Cloud service, App service/slot, Public IP address	App service, Cloud service, Storage, Application Gateway, API Management, Public IP address, Traffic Manager, Custom Host

Endpoint Monitoring	Health probes	Health probes	HTTP/HTTPS GET requests	Health probes
Redundancy	Zone redundant and Zonal	Zone redundant	Resilient to regional failures	Resilient to regional failures
SSL/TLS Termination	–	Supported	–	Supported
Web Application Firewall	–	Supported	–	Supported
Sticky Sessions	Supported	Supported	–	Supported
VNet Peering	Supported	Supported	–	–
SKU	Basic and Standard	Standard and WAF (v1 & v2)	–	Standard and Premium
Pricing	Standard Load Balancer – charged based on the number of rules and processed data.	Charged based on Application Gateway type, processed data, outbound data transfers, and SKU.	Charged per DNS queries, health checks, measurements, and processed data points.	Charged based on outbound/inbound data transfers, and incoming requests from client to Front Door POPs.

AZURE VPN GATEWAY

- A secured hybrid cloud architecture.

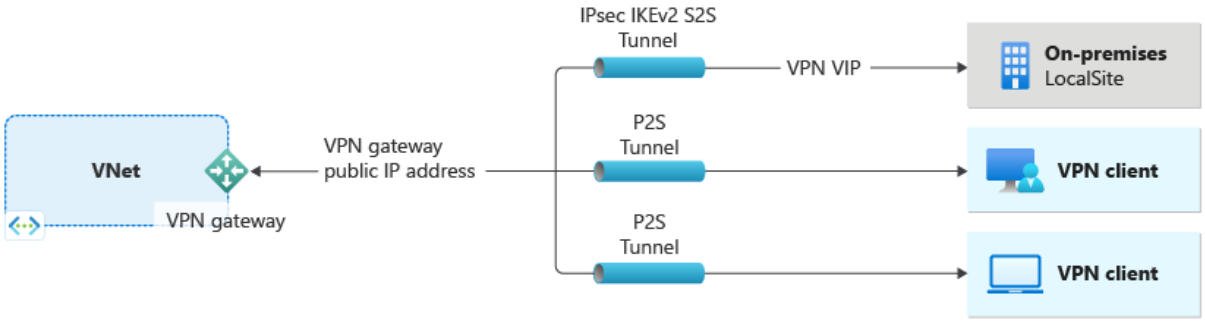
- It is composed of gateway subnet, tunnel, and on-premises gateway.
- Protocols: Internet Protocol Security (IPsec) and Internet Key Exchange (IKE)
- VPN gateway connections: **VNet-to-VNet**, **Site-to-Site**, and **Point-to-Site**
    - Create a secure connection from your on-premises network to an Azure virtual network with a site-to-site VPN.
    - VNet-to-VNet connection automatically routes to the updated address space, if you updated the address space on the other VNet.
    - If you need to establish a connection to your virtual network from a remote location, you can use a point-to-site (P2S) VPN.
- You can also have one VPN gateway with more than one on-premises network using a Multi-Site connection.

Routing

- **Policy-based gateway**
    - Implements a policy-based VPN.
    - Policy-based VPNs are used to encrypt and direct packets to IPsec tunnels.
    - The policy or traffic selector is defined as an access list in the VPN configuration.
    - You cannot change a policy-based VPN to a route-based VPN, and vice versa.
- **Route-based gateway**
    - Implements a route-based VPN.
    - Route-based VPNs use routes in the routing table to direct packets to tunnel interfaces.
    - Tunnel interfaces can encrypt and decrypt packets.
    - The policy or traffic selector are configured as wild cards (any-to-any).

Connection Resiliency

Details	Site-to-Site	Point-to-Site
Supported Services	Cloud Services and Virtual Machines	Cloud Services and Virtual Machines
Bandwidths	Typically < 1 Gbps aggregate	Based on the gateway SKU
Protocols	IPsec	Secure Sockets Tunneling Protocol (SSTP), OpenVPN and IPsec
Routing	We support PolicyBased (static routing) and RouteBased (dynamic routing VPN)	RouteBased (dynamic)
Connection resiliency	active-passive or active-active	active-passive
Use case	Dev / test / lab scenarios and small scale production workloads for cloud services and virtual machines	Prototyping, dev / test / lab scenarios for cloud services and virtual machines



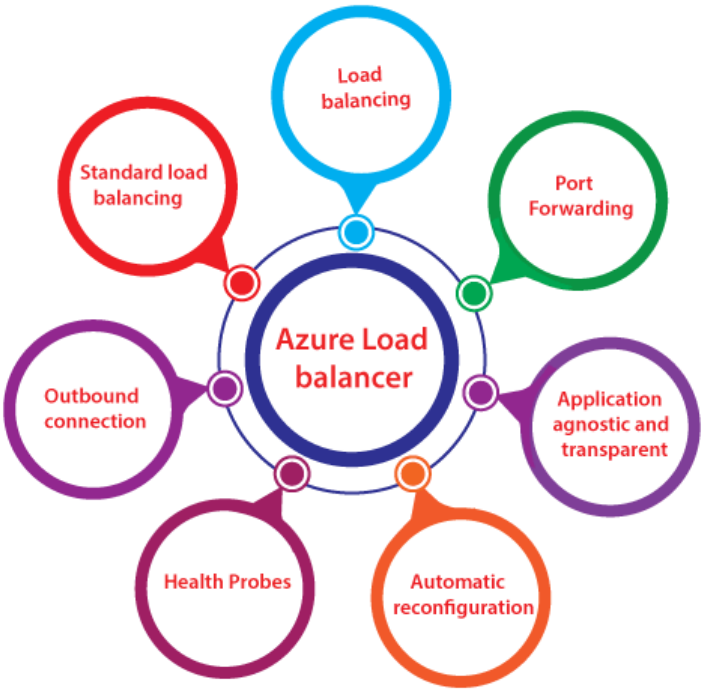
When we are planning to deploy a VPN gateway into Azure, we can configure the number of setting related to it:

- **Gateway SKUs:** We need to select the SKU that satisfies our requirements based on the types of workloads, throughputs, features, and SLAs.
- **Zone-redundant gateways:** We can get benefits from zone-resiliency to access your mission-critical, scalable service on Azure when we use zone-redundant gateways.
- **Connection types:** Connection type can be IPsec, Vnet2Vnet, ExpressRoute, VPNClient.
- **VPN types:** The VPN type that we choose depends on the connection topology that we want to create and the VPN device. It can be a policy-based VPN or Route-based VPN.
- **Gateway subnet:** Before you create a VPN gateway, you must create a gateway subnet with the name 'GatewaySubnet' and do not deploy anything else into that subnet.
- **Local network gateway:** Local network gateway usually represents your on-premises location, i.e., VPN devices, and address prefixes.
- **Connection topologies:** Site to site, Multi-site, point-to-site, Vnet-to-Vnet, and express route.
- **Monitoring and Alerts:** Monitors the key metrics and configure alerts

---

- [ ] **AZURE LOAD BALANCER**
  - **load balancer** is used to distribute the incoming traffic to the pool of virtual machines.
  - It stops routing the traffic to a failed virtual machine in the pool.

- In this way, we can make our application resilient to any software or hardware failures in that pool of virtual machines.



Features of Azure load balancer

- **Load Balancing:** Azure load balancer uses a 5-tuple hash composed of source IP, source port, destination IP, destination port, and protocol. We can configure a load balancing role within the load balancer in such a way based on the source port and source IP address from where the traffic is originating.
- **Port forwarding:** Load balancer also has port forwarding capability if we have a pool of web servers, and we don't want to associate public IP address for each web server in that pool. If we're going to carry out any maintenance activities, you need to RDP into those Web servers having a public IP address on that web servers.
- **Application agnostic and transparent:** Load balancer doesn't directly interact with TCP or UDP or the application layer. We can route the traffic based on URL or multi-site hosting, and then we can go for the application gateway.
- **Automatic reconfiguration:** Load balancer can reconfigure itself when we scale up or down instances. So, if we are adding more virtual machines into the backend pool, automatically load balancer will reconfigure.

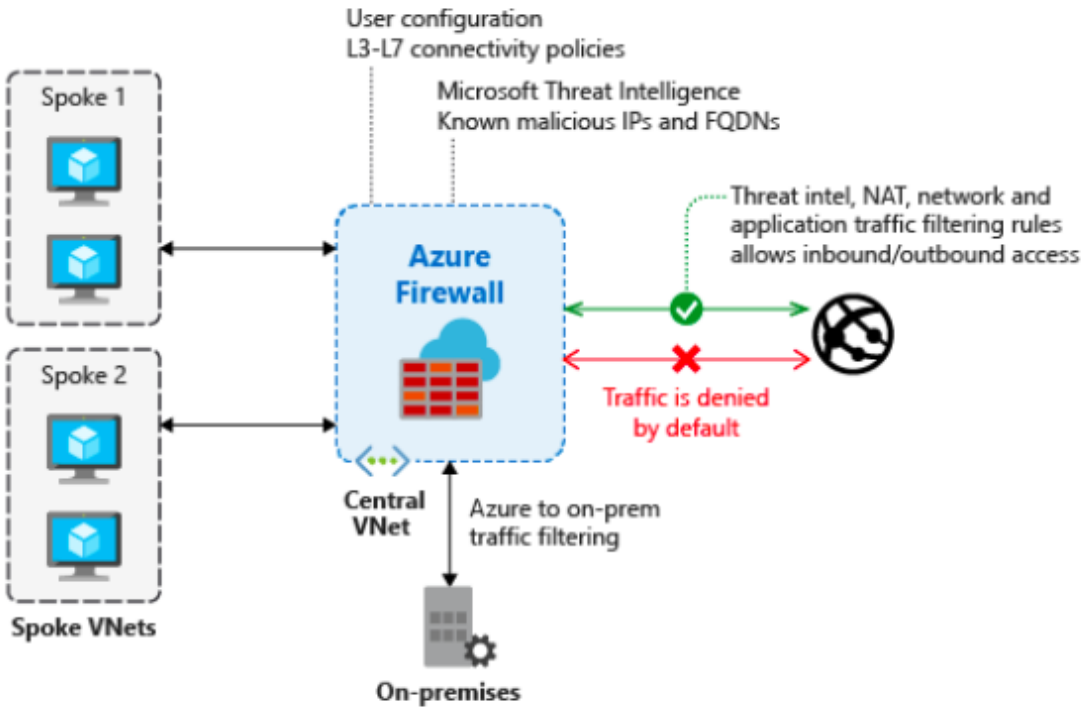
- **Health probes:** As we discussed earlier, the load balancer can recognize any failed virtual machines in the backend pool and stop routing the traffic to that particular failed virtual machine. It will recognize using health probes we can configure a health probe to determine the health of the instances in the backend pool.
- **Outbound connection:** All the outbound flows from a private IP address inside our virtual network to public IP addresses on the Internet can be translated to a frontend IP of the load balancer.

Configuration elements of Load Balancer

- **Front-end IP configuration:** It is the IP address to which the incoming traffic will initially come to, and Azure load balancer can have one or more front end IP addresses. They are sometimes also called as virtual IPs.
- **Back-end address pool:** These are the pool of virtual machines to which the traffic will eventually go to.
- **Load balancing rules:** A load balancing rule is simply a mapping between the front end IP configuration and back-end address pool.
- **Probes:** Probes enable us to keep track of the health of VM instances. If a health probe files, the VM instance will be taken out of rotation automatically.
- **Inbound & Outbound NAT rules:** NAT rules defining the inbound traffic flowing through the front end IP and distributes to the backend IP. Outbound rules will transmit VM private IP to load balancer public IP.

- [ ] **AZURE FIREWALL**
- [ ] **Reference:**
  - A service that uses a static public IP address to protect your VNet resources.
  - Azure Firewall is PCI, SOC, ISO, ICSA Labs, and HITRUST compliant.
  - Azure Firewall is stateful firewall as a Service with high availability integrated and unrestricted cloud scalability that protects Azure virtual network resources.
  - You can deploy Azure Firewall on any virtual network, but customers typically deploy it on a central virtual network and peer other virtual networks to it in a **hub-and-spoke model.**

- Azure Firewall supports inbound and outbound filtering. Inbound protection is for non-HTTP/S protocols. For example, **RDP, SSH, and FTP** protocols.
- Azure Firewall needs a dedicated subnet "**AzureFirewallSubnet"**
- Azure Firewall is integrated with **Azure Monitor** for viewing and analyzing firewall logs.
- Azure Firewall supports rules and rule collections.
  - A rule collection is a set of rules that share the same order and priority.
  - Rule collections are executed in order of their priority.
  - Network rule collections are higher priority than application rule collections, and all rules are terminating.
- Azure Firewall cost:
  - Fixed fee: $1.25/firewall/hour,
  - Data Processing fee: $0.016 per GB processed by the firewall (ingress or egress)
  - A fixed hourly fee will be charged per a firewall deployment regardless of scale. In addition, data processing fee is billed per deployment for any date processed by your firewall.



Features

- A stateful firewall service.
- You can enable **forced tunneling** to route Internet-bound traffic to an additional firewall or virtual network appliance.
- Limit outbound traffic to a given **FQDN** list, including wild cards.
    - Filter any TCP/UDP protocol outbound traffic.
    - To use FQDNs in your rules, you must enable DNS proxy.
- Deny the traffic of a malicious IP address with **threat intelligence-based filtering**.
    - It has the highest priority rules and will always be processed first.
    - Threat intelligence modes: Off, Alert only, Alert and deny
- With a DNS proxy, a firewall listens to port 53 and forwards the DNS requests to a DNS server.You can minimize the complexity of creating a security rule using a **service tag**.
- Associate up to 250 public IP addresses in your firewall.
- It supports SNAT and DNAT translation.
    - SNAT – Source NAT for outbound VNet traffic.
    - DNAT – Destination NAT for inbound network traffic.
- Azure Firewall diagnostic logs (JSON format):
    - Application rule log
    - Network rule log
- You can store all your logs in a storage account, event hubs, and Azure monitor logs.
- Azure Firewall metrics:
    - Application/Network rules hit count
    - Data processed
    - Throughput
    - Firewall health state
    - SNAT port utilization
- To manage multiple firewalls, you can use **Azure Firewall Manager**.
- Protect your VDI deployments using Azure firewall DNAT rules and threat Intelligence filtering.

Azure Firewall and NSG seem pretty similar ; so, let us compare them side by side.

Features	Azure Firewall	NSG
Rule-based filtering	Firewall supports rule-based filtering	NSG also supports rule-based filtering
FQDN tags	Firewall supports FQDN tags	NSG does not support FQDN tags
Service tags	Firewall supports service tags	NSG also supports service tags
Threat-intelligence-based filtering	Firewall supports threat-intelligence-based filtering	NSG does not support threat-intelligence-based filtering
Destination and source network address translation (DNAT and SNAT)	Firewall supports DNAT and SNAT	NSG does not support DNAT and SNAT
Azure Monitor integration	The firewall is well-integrated with Azure Monitor	NSG also has Azure Monitor integration

AZURE DNS

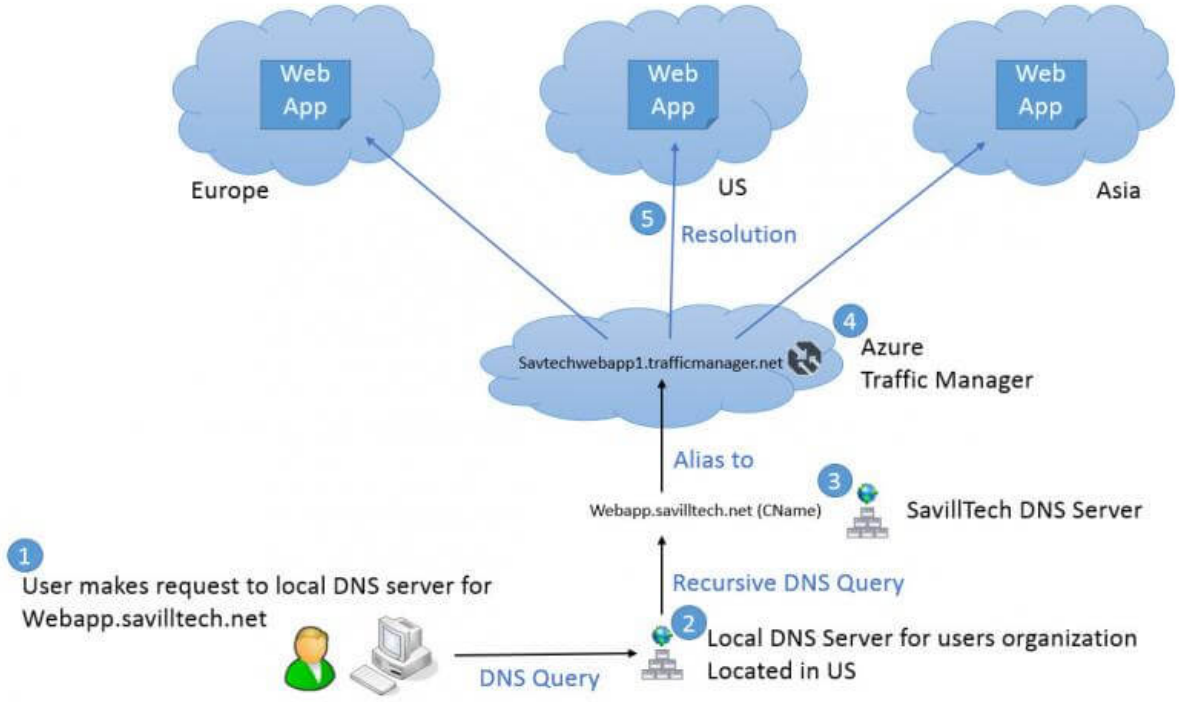
- Enables you to host your DNS zone and manage your DNS records.
- DNS zone allows you to configure a private and public DNS zone.
- Alias recordsets:
  - A – maps the host to IPv4.
  - AAAA – maps the host to IPv6.
  - CNAME – create a record to point to another domain.
- A limit of 20 alias record sets per resource.
- Uses Anycast networking to route users to the closest name servers.
- You can monitor your DNS zone metrics using Azure Monitor.
  - **QueryVolume** – query traffic received.
  - **RecordSetCount** – the number of recordsets in your DNS.
  - **RecordSetCapacityUtilization** – percentage of utilization of your recordset capacity.
- **Azure Private DNS** allows you to use your custom domain name in your private VNet.
- Alias record allows you to point your naked domain or apex to a traffic manager or CDN endpoint.

Private DNS

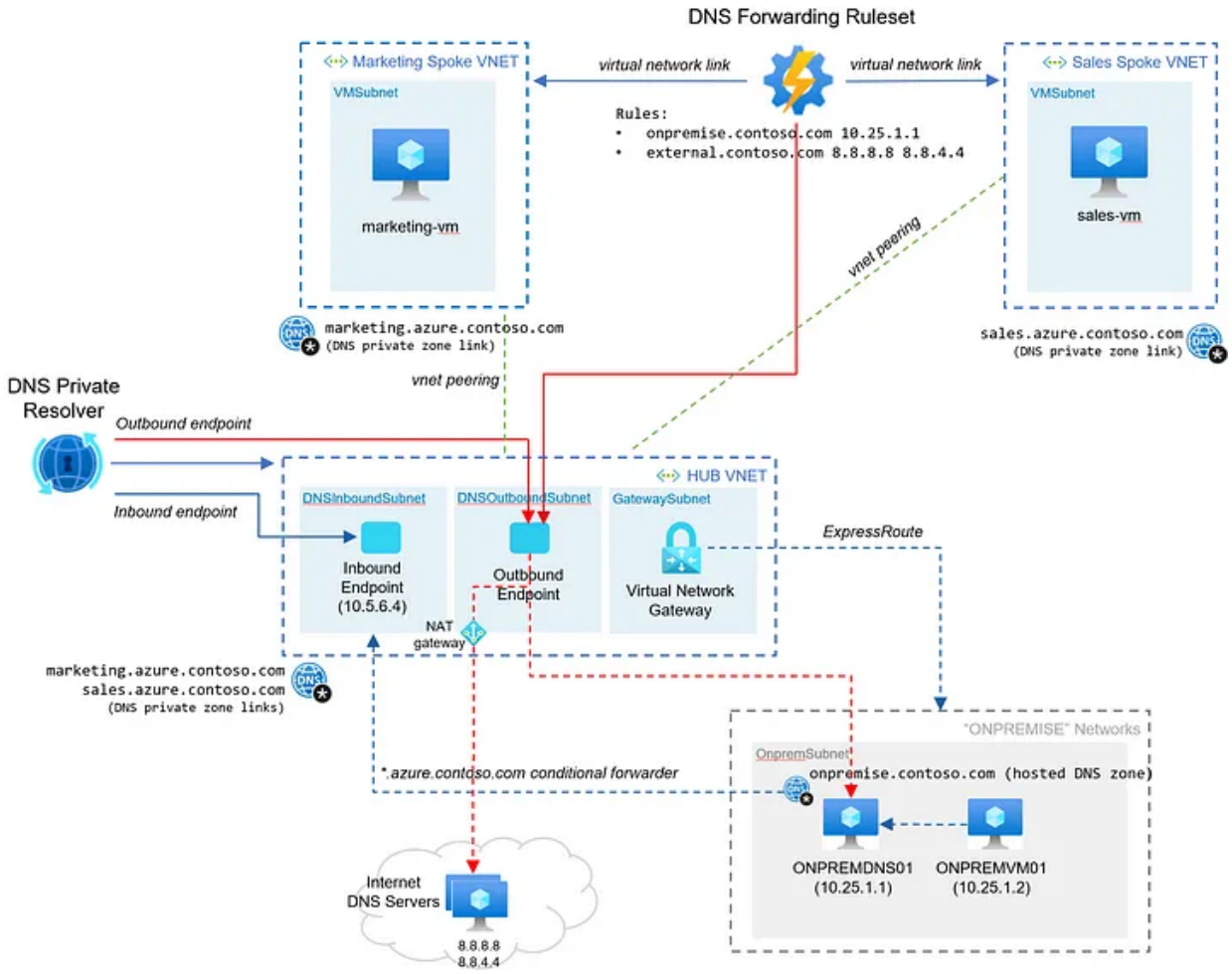
- Allows you to manage and resolve domain names in a virtual network.
- Configure a split-horizon DNS to create zones with the same name.
- It also supports all types of DNS records types: A, AAAA, CNAME, MX, PTR, SOA, SRV, and TXT.
- A virtual network can be linked to only one private zone. But you can link multiple virtual networks to a single DNS zone.
- Private IP space in the linked virtual network allows reverse DNS.

Azure DNS Security

- To prevent accidental zone deletion, you can apply a 'CanNotDelete' lock.
- Create a custom role to ensure it doesn't have a zone delete permission.
- You can deploy a DNS firewall to mitigate DNS-related security issues.



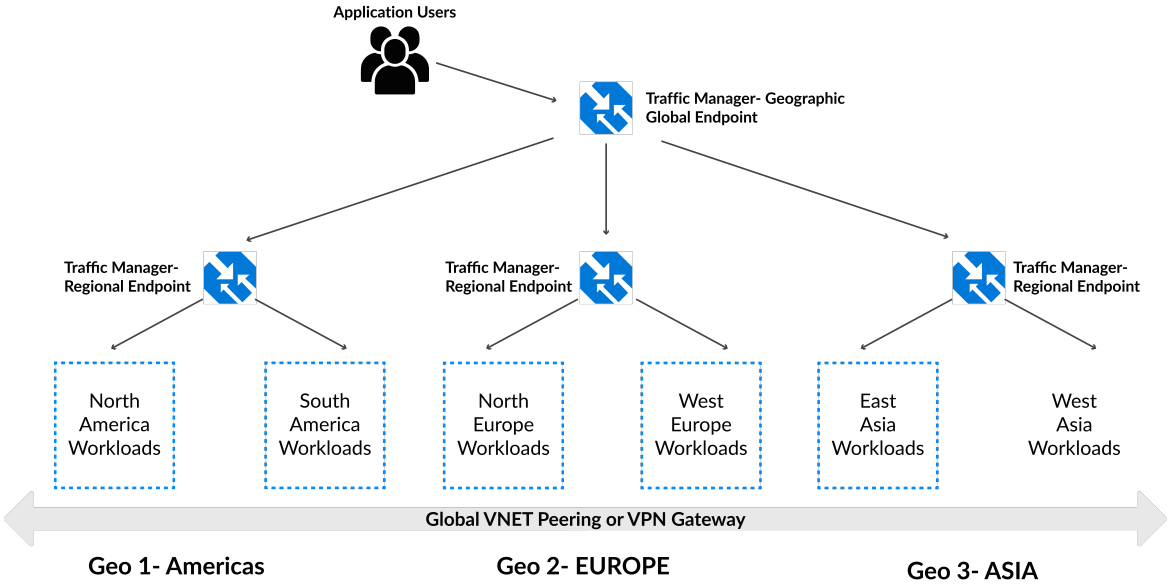
Key components



☐ AZURE TRAFFIC MANAGER

- A DNS-based traffic load balancer.
- Improves the responsiveness of your applications by sending the request to the closest endpoint.

- It offers a range of **traffic-routing methods** and **endpoint monitoring options**.



Why Do We Use Traffic Manager?

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.
An endpoint is any Internet-facing service hosted inside or outside of Azure.
It provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. It is resilient to failure, including the failure of an entire Azure region.

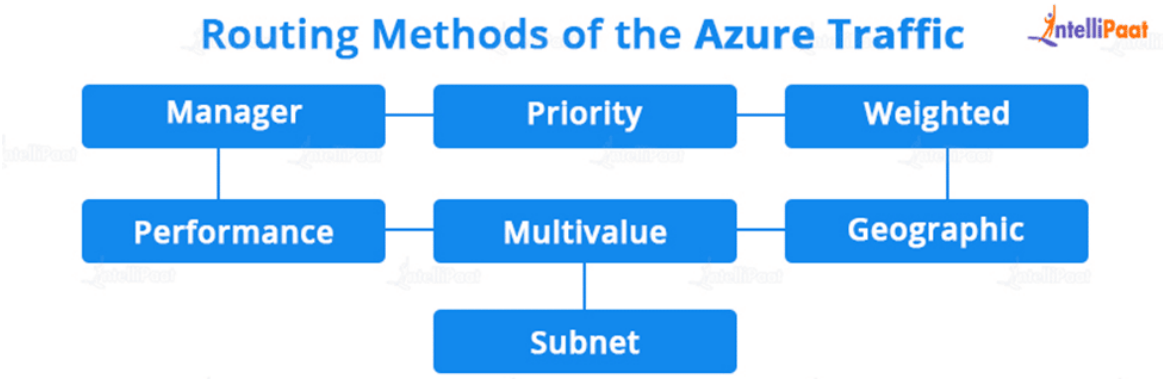
Features

- It is resilient to failure.
- You can obtain actionable insights about your users using a **traffic view.**
- Improve the availability of your applications by using traffic manager health checks.
- Offers automatic failover when an endpoint goes down.
- Traffic Manager endpoints: **Azure**, **External**, and **Nested**
- Combine multiple traffic-routing methods using **nested traffic manager profiles**.

Routing Methods

- Priority – allows you to set a primary endpoint for all traffic.
- Weighted – distribute traffic according to weights.
- Performance – routes users to the closest endpoint.
- Geographic – direct users to a specific endpoint.

- Multivalue – endpoints for IPv4/IPv6 addresses.
- Subnet – map a group of end-user IP address range to a specific endpoint.

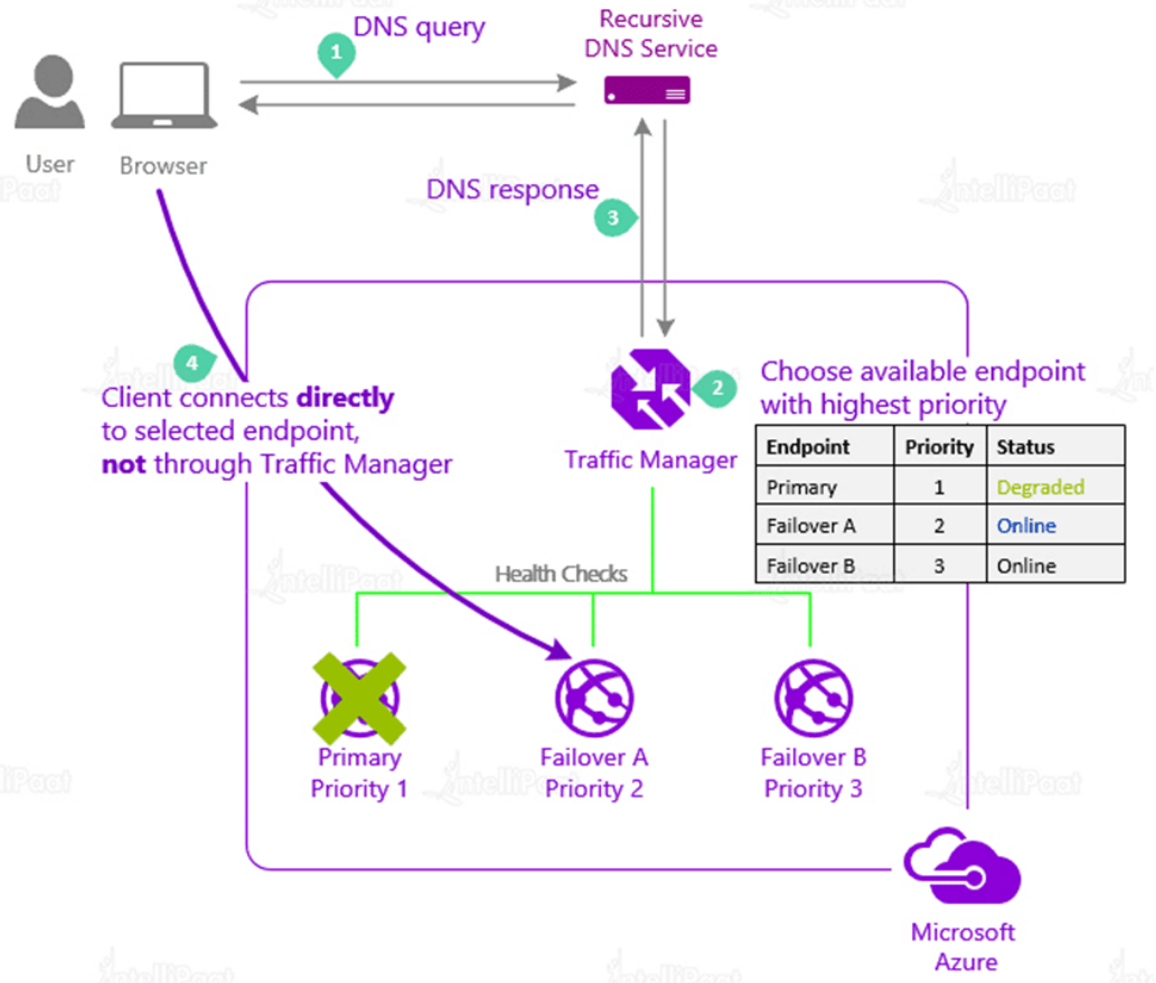


There are the following traffic routing strategies available:

Priority

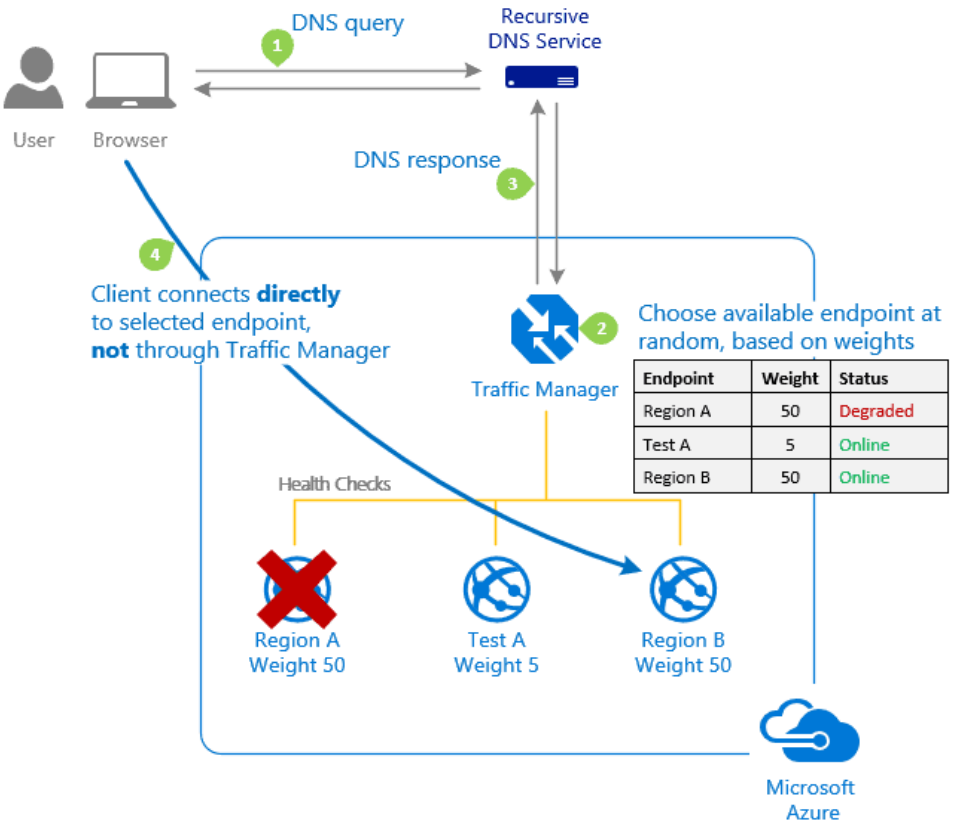
- The primary service endpoint has the top priority with all traffic when you select the priority routing strategy, which displays a prioritized list of service endpoints.

- Traffic is forwarded to the endpoint with the next greatest priority if the primary service endpoint is unavailable.



Weighted

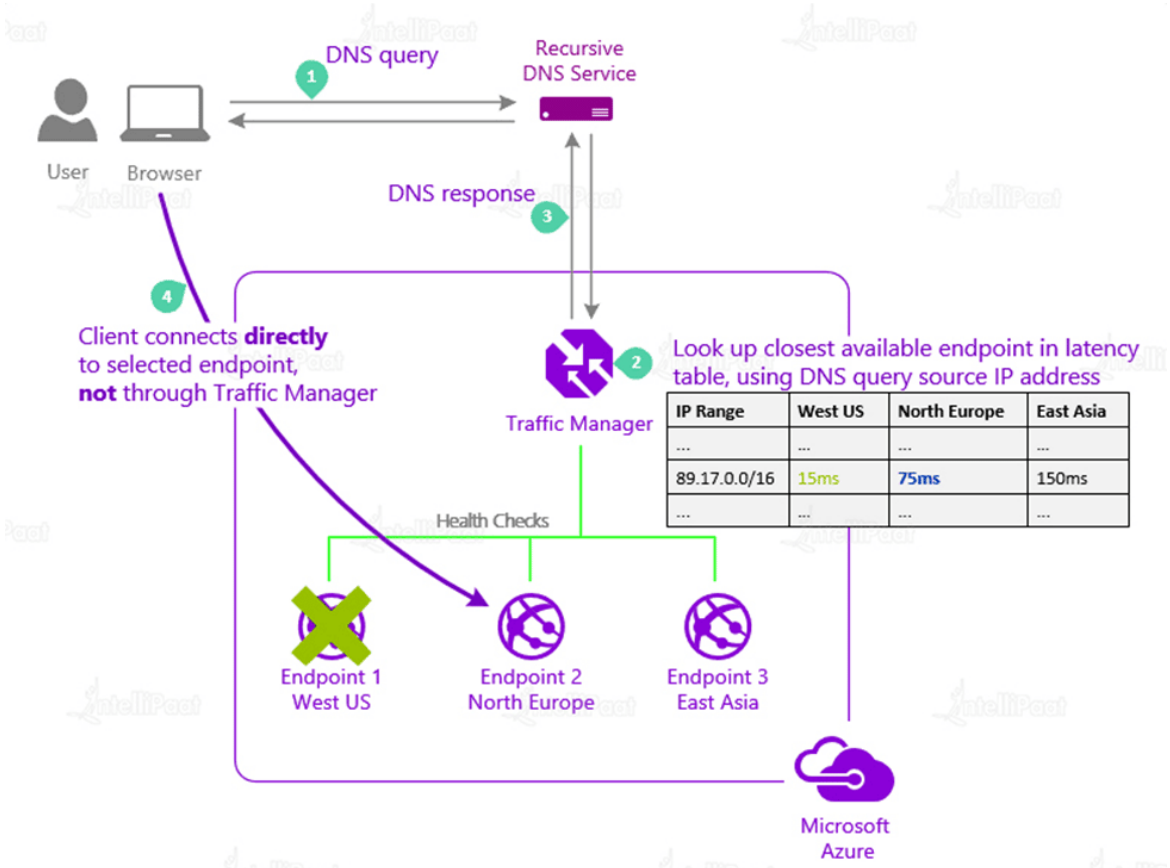
- Weighted routing is used when you want to evenly distribute traffic or apply pre-determined weights to a group of destinations.
- This traffic-routing method involves giving each endpoint a weight, which is a number between 200 and 2000, in the Microsoft Azure Traffic Manager profile option.



Performance

- By sending traffic to the location closest to the user, this traffic routing technology helps various apps respond more quickly.
- The 'nearest' endpoint isn't usually the one that is physically closest.

- On the other hand, the "Performance" traffic-routing strategy chooses the nearest destination by analyzing network latency.



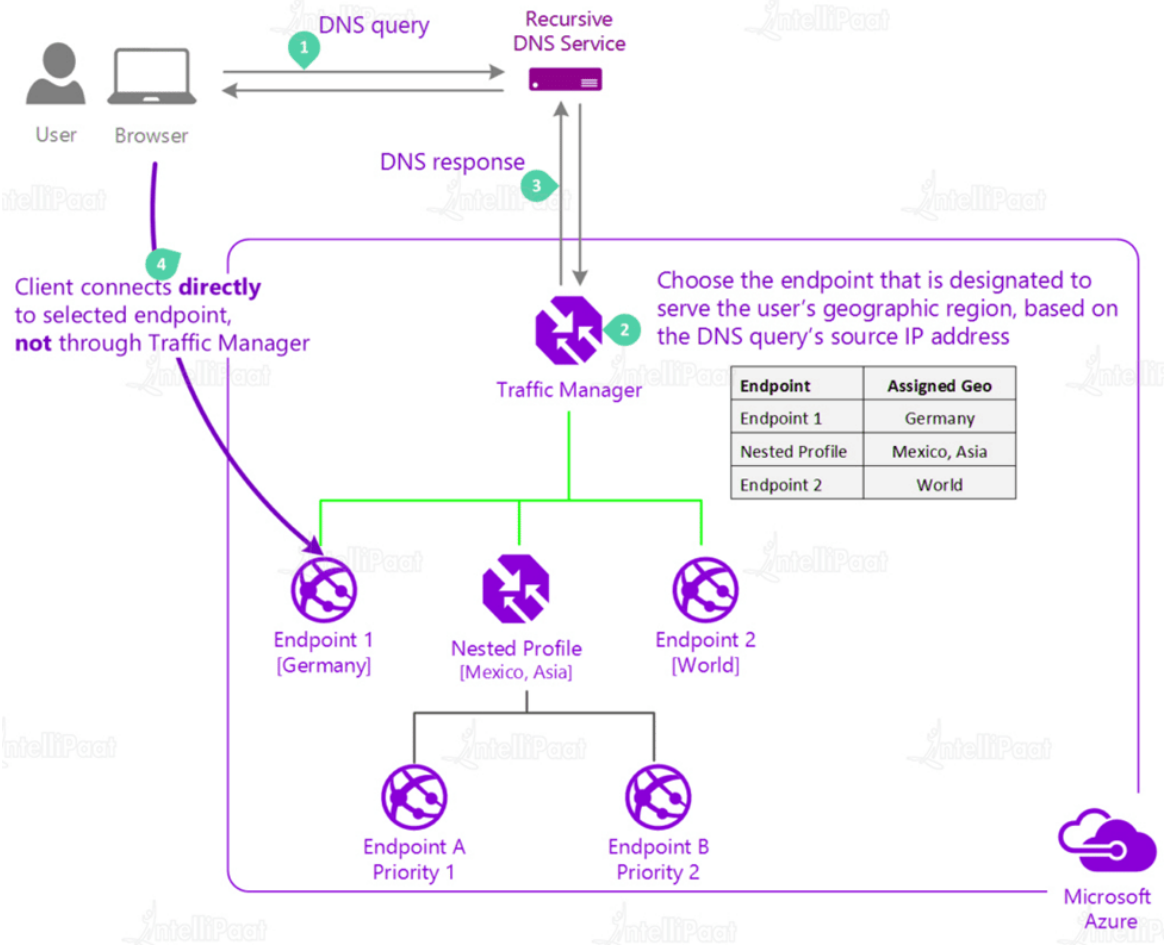
Multivalue

- You can select MultiValue if your Azure Traffic Manager profiles only include IPv2 or IPv4 addresses as destinations.
- All appropriate endpoints are retrieved when a request for this profile is made.

Geographic

- In geographic routing, a set of geographic areas must be assigned to each endpoint associated with that profile.

- Any requests from such locations are only directed to that endpoint when a region or group of regions is assigned to it.



Subnet

- Use the Subnet traffic-routing method to associate groups of end-user IP address ranges with a particular endpoint inside an Azure Traffic Manager profile.
- A request is received, and the endpoint that responds is the one that corresponds to the request's originating IP address.

☐ AZURE BASTION

What is Azure Bastion?

Azure Bastion is a PaaS service that provides a secure RDP/SSH connection to Azure VMs without exposing them over the public internet. Azure Bastion is deployed to a vNet and supports virtual network peering. Specifically, Azure Bastion manages **RDP/SSH connectivity** to VMs created in the local or peered vNet.

Why we use Azure Bastion?

In general practice there is two way we leverage for connecting Azure VMs which is listed below:

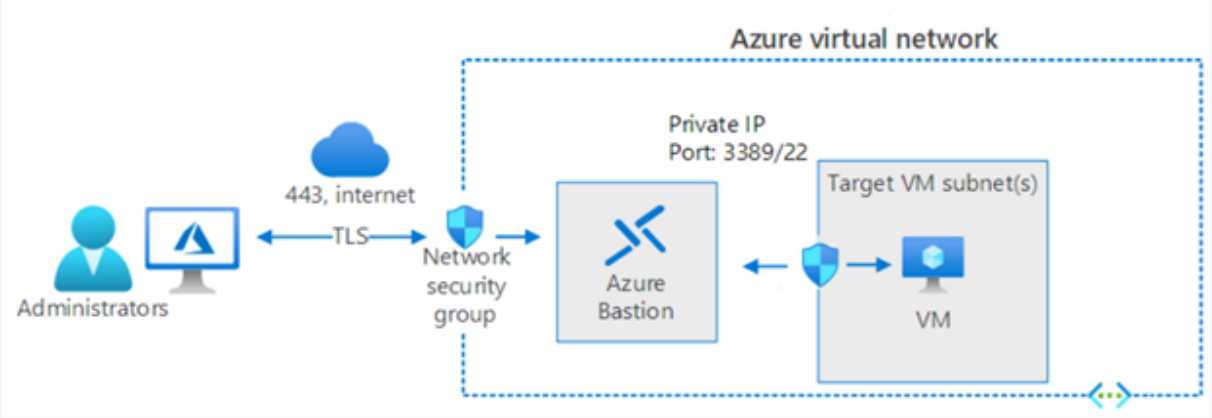
- Connect using Public IP
- Connect using Jump Box

In both modes, we have to do some network hardening and enable Just In time access which involves extra cost. To eliminate all these efforts, we use Azure Bastion, which helps us connect all the Azure VMs without exposing them over the internet.

Traffic workflow when we connect Azure VMs

#Scenario 1 – Below is the traffic workflow when we use the public Internet to access VMs –

#Scenario 2 – Below is the traffic workflow when we use Azure Bastion to access VMs –

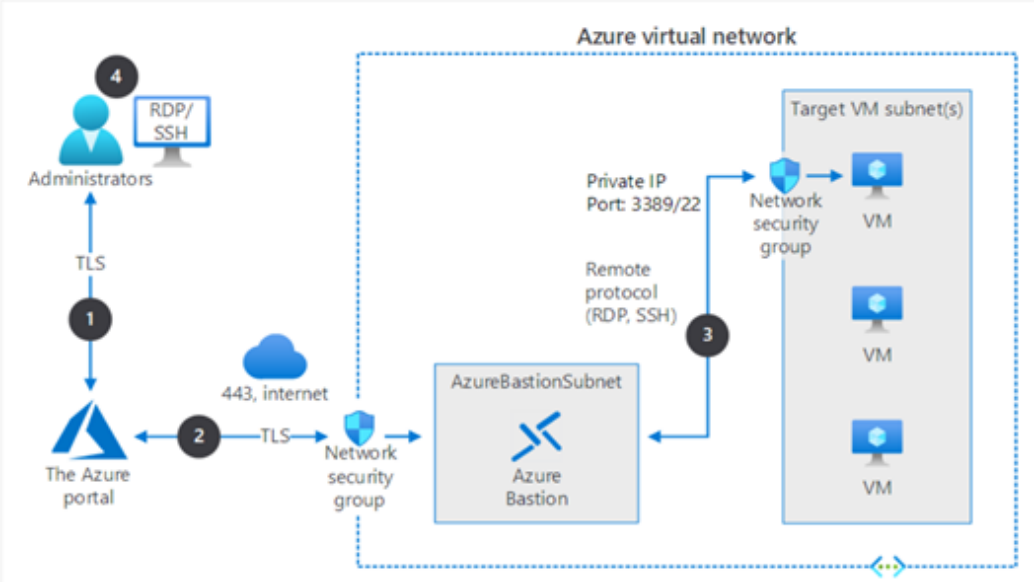


How Azure Bastion work?

Azure Bastion is configured under the same virtual network where all Azure VMs resides. Still, it has its own NSG protected subnet with the unique name “AzureBastionSubnet,”

with a minimum /27 prefix. Bastion subnet only supports communication through TCP post 443 from Azure Portal.

Azure Bastion Architecture Diagram



Prerequisites

Here are the required NSG rules that need to be taken care of for proper traffic flow from the internet to bastion subnet and bastion subnet to VMs subnet –

- **Inbound –**
  - RDP and SSH connections from the Azure Bastion subnet to the target VM subnet
  - TCP port **443** access from the internet to the Azure Bastion public IP
  - TCP access from Azure Gateway Manager on ports **443** or **4443**
- **Outbound –**
  - TCP access from the Azure platform on port **443** to support diagnostic logging.

Minimum access required for the user to leverage bastion for VMs connection –

User required **Reader access** on below Azure resources:

- The target VM.

- The network interface with private IP on the target VM.
- The Azure Bastion resource.

Azure Bastion requires a Public IP address which must have the following configuration –

- The Public IP address SKU must be **Standard**.
- The Public IP address assignment/allocation method must be **Static**.
- The Public IP address name is the resource name by which you want to refer to this public IP address.
- You can choose to use a public IP address that you already created, as long as it meets the criteria required by Azure Bastion and is not already in use.

Azure Bastion Use Cases

Now let's list some possible use-cases. Azure Bastion can be very useful (but not limited) to these scenarios:

1. Your Azure-based VMs are running in a subscription where you're unable to connect via VPN, and for security reasons, you cannot set up a dedicated Jump-host within that VNet.
2. You want to give developers access to a single VM without giving them access to additional services like a VPN or other things running within the VNet.
3. You want to implement Just in Time (JIT) Administration in Azure. You can deploy and enable Bastion Host on the fly and as you need it.

Does Azure Bastion require a VPN?

No, Azure Bastion does not require a VPN.

Can Azure Bastion be used to connect to virtual machines from anywhere with an internet connection?

Yes, Azure Bastion can be used to connect to virtual machines from anywhere with an internet connection.

What is the benefit of using Azure Bastion for remote access instead of a VPN?

Azure Bastion provides a simpler, more cost-effective, and more secure solution for remote access compared to a VPN.

Is Azure Bastion suitable for small businesses?

Yes, Azure Bastion is suitable for businesses of any size.

Can Azure Bastion be used for both RDP and SSH connectivity?

Yes, Azure Bastion can be used for both RDP and SSH connectivity.
