Contents

[Vnet 1](#_Toc49999580)

[Deploy dedicated Azure services into virtual networks 1](#_Toc49999581)

[Subnet 1](#_Toc49999582)

[FAQs 1](#_Toc49999583)

[Virtual Network basics 1](#_Toc49999584)

[Name Resolution (DNS) 2](#_Toc49999585)

[Connecting virtual machines 3](#_Toc49999586)

[Azure services that connect to VNets 4](#_Toc49999587)

[VNet peering 4](#_Toc49999588)

[Virtual network service endpoints 6](#_Toc49999589)

[Load Balancers 6](#_Toc49999590)

[Decision tree for load balancing in Azure 6](#_Toc49999591)

[Azure Front Door 7](#_Toc49999592)

[URL-based routing 7](#_Toc49999593)

[Multiple-site hosting 8](#_Toc49999594)

[TLS termination 8](#_Toc49999595)

[Application layer security 8](#_Toc49999596)

[Traffic Manager 9](#_Toc49999597)

[Azure Application Gateway 9](#_Toc49999598)

[Application Gateway Features 10](#_Toc49999599)

[Azure Load Balancer 11](#_Toc49999600)

# Vnet

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-troubleshoot-peering-issues>

## Deploy dedicated Azure services into virtual networks

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services>

TASK:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-multiple-ip-addresses-portal#os-config>

# Subnet

# FAQs

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq>

## Virtual Network basics

1. Can I have public IP addresses in my VNets?
2. Are there any restrictions on using IP addresses within these subnets?

Azure reserves 5 IP addresses within each subnet. These are x.x.x.0-x.x.x.3 and the last address of the subnet. x.x.x.1-x.x.x.3 is reserved in each subnet for Azure services.

x.x.x.0: Network address

x.x.x.1: Reserved by Azure for the default gateway

x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space

x.x.x.255: Network broadcast address

1. 3.How small and how large can VNets and subnets be?

The smallest supported IPv4 subnet is /29, and the largest is /8 (using CIDR subnet definitions). IPv6 subnets must be exactly /64 in size.

1. Can I specify custom routing policies on my VNets and subnets?

Yes. You can create a route table and associate it to a subnet. For more information about routing in Azure, see Routing overview.

1. Do VNets support multicast or broadcast?

No. Multicast and broadcast are not supported.

1. Can I ping my default routers within a VNet?

No.

1. Can I use tracert to diagnose connectivity?

No.

1. Can I modify the size of my subnet after I create it?

Yes. You can add, remove, expand, or shrink a subnet if there are no VMs or services deployed within it.

1. Can a VNet span regions?

No. A VNet is limited to a single region. A virtual network does, however, span availability zones.

## Name Resolution (DNS)

1. Can I specify DNS servers for a VNet?

Yes. You can specify DNS server IP addresses in the VNet settings. The setting is applied as the default DNS server(s) for all VMs in the VNet.

1. Can I override my DNS settings on a per-VM or cloud service basis?

Yes. You can set DNS servers per VM or cloud service to override the default network settings. However, it's recommended that you use network-wide DNS as much as possible.

1. Can I bring my own DNS suffix?

No. You cannot specify a custom DNS suffix for your VNets.

## Connecting virtual machines

1. Can I deploy VMs to a VNet?

Yes. All network interfaces (NIC) attached to a VM deployed through the Resource Manager deployment model must be connected to a VNet. VMs deployed through the classic deployment model can optionally be connected to a VNet.

1. Can I reserve a private IP address for a VM that I will create at a later time?

No. You cannot reserve a private IP address. If a private IP address is available, it is assigned to a VM or role instance by the DHCP server. The VM may or may not be the one that you want the private IP address assigned to. You can, however, change the private IP address of an already created VM, to any available private IP address.

1. Do private IP addresses change for VMs in a VNet?

It depends. If the VM was deployed through Resource Manager, no, regardless of whether the **IP address was assigned with the static or dynamic allocation method**. If the VM was deployed through the classic deployment model, dynamic IP addresses can change when a VM is started after having been in the stopped (deallocated) state. The address is released from a VM deployed through either deployment model when the VM is deleted.

1. Can I manually assign IP addresses to NICs within the VM operating system?

Yes, but it's not recommended unless necessary, such as when assigning multiple IP addresses to a virtual machine. For details, see Adding multiple IP addresses to a virtual machine. If the IP address assigned to an Azure NIC attached to a VM changes, and the IP address within the VM operating system is different, you lose connectivity to the VM.

1. If I stop a Cloud Service deployment slot or shutdown a VM from within the operating system, what happens to my IP addresses?

Nothing. The IP addresses (public VIP, public, and private) remain assigned to the cloud service deployment slot or VM.

1. Can I configure a static MAC address for my VM?

No. A MAC address cannot be statically configured.

1. Will the MAC address remain the same for my VM once it's created?

Yes, the MAC address remains the same for a VM deployed through both the Resource Manager and classic deployment models until it's deleted. Previously, the MAC address was released if the VM was stopped (deallocated), but now the MAC address is retained even when the VM is in the deallocated state. The MAC address remains assigned to the network interface until the network interface is deleted or the private IP address assigned to the primary IP configuration of the primary network interface is changed.

1. Can I move VMs from one subnet to another subnet in a VNet without redeploying?

Yes. You can find more information in the How to move a VM or role instance to a different subnet article.

## Azure services that connect to VNets

1. Can I move my services in and out of VNets?

No. You cannot move services in and out of VNets. To move a resource to another VNet, you have to delete and redeploy the resource.

## VNet peering

1. What are the constraints related to Global VNet Peering and Load Balancers?

If the two virtual networks in two different regions are peered over Global VNet Peering, you cannot connect to resources that are behind a Basic Load Balancer through the Front End IP of the Load Balancer. This restriction does not exist for a Standard Load Balancer. The following resources can use Basic Load Balancers which means you cannot reach them through the Load Balancer's Front End IP over Global VNet Peering. You can however use Global VNet peering to reach the resources directly through their private VNet IPs, if permitted.

VMs behind Basic Load Balancers

Virtual machine scale sets with Basic Load Balancers

Redis Cache

Application Gateway (v1) SKU

Service Fabric

SQL MI

API Management

Active Directory Domain Service (ADDS)

Logic Apps

HDInsight

Azure Batch

App Service Environment

You can connect to these resources via ExpressRoute or VNet-to-VNet through VNet Gateways.

1. Can I enable VNet Peering if my virtual networks belong to subscriptions within different Azure Active Directory tenants?

Yes. It is possible to establish VNet Peering (whether local or global) if your subscriptions belong to different Azure Active Directory tenants. You can do this via PowerShell or CLI. Portal is not yet supported.

1. My VNet peering connection is in Initiated state, why can't I connect?

If your peering connection is in an Initiated state, this means you have created only one link. A bidirectional link must be created in order to establish a successful connection. For example, to peer VNet A to VNet B, a link must be created from VNetA to VNetB and from VNetB to VNetA. Creating both links will change the state to Connected.

1. My VNet peering connection is in Disconnected state, why can't I create a peering connection?

If your VNet peering connection is in a Disconnected state, it means one of the links created was deleted. In order to re-establish a peering connection, you will need to delete the link and recreate it.

1. Can I peer two VNets with matching or overlapping address ranges?

No. Address spaces must not overlap to enable VNet Peering.

1. How much do VNet peering links cost?

There is no charge for creating a VNet peering connection. Data transfer across peering connections is charged.

1. Is VNet peering traffic encrypted?

No. Traffic between resources in peered VNets is private and isolated. It remains completely on the Microsoft Backbone.

1. If I peer VNetA to VNetB and I peer VNetB to VNetC, does that mean VNetA and VNetC are peered?

No. Transitive peering is not supported. You must peer VNetA and VNetC for this to take place.

1. Are there any bandwidth limitations for peering connections?

No. VNet peering, whether local or global, does not impose any bandwidth restrictions. Bandwidth is only limited by the VM or the compute resource.

## Virtual network service endpoints

Todo

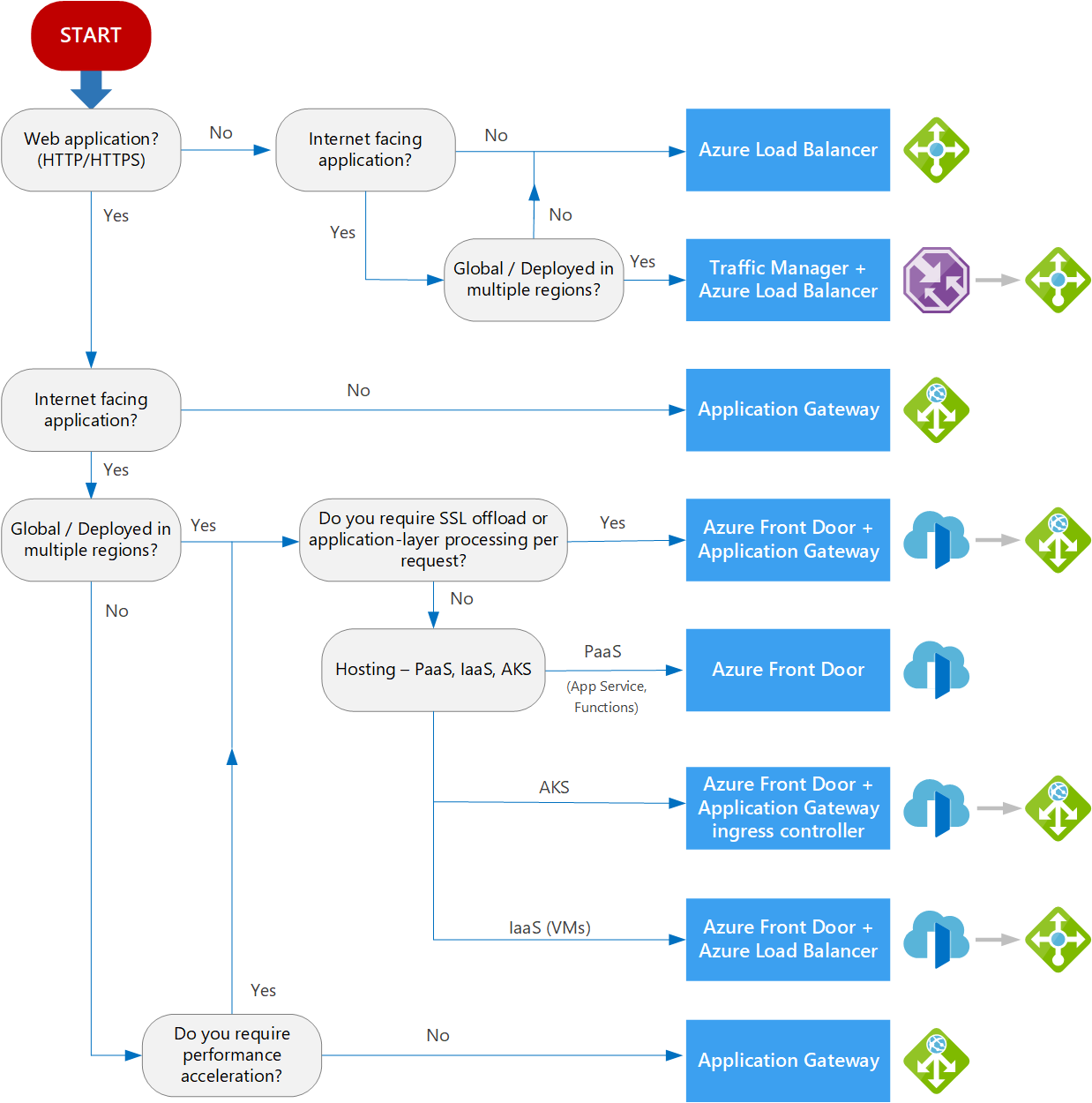
# Load Balancers

<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview>

## Decision tree for load balancing in Azure

When selecting the load-balancing options, here are some factors to consider:

* **Traffic type**. Is it a web (HTTP/HTTPS) application? Is it public facing or a private application?
* **Global versus. regional**. Do you need to load balance VMs or containers within a virtual network, or load balance scale unit/deployments across regions, or both?
* **Availability**. What is the service [SLA](https://azure.microsoft.com/support/legal/sla/)?
* **Cost**. See [Azure pricing](https://azure.microsoft.com/pricing/). In addition to the cost of the service itself, consider the operations cost for managing a solution built on that service.
* **Features and limits**. What are the overall limitations of each service?



## Azure Front Door

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview>

[Front Door](https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview) 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.

### URL-based routing

For example, requests for http://www.contoso.com/users/\* are routed to UserProfilePool, and http://www.contoso.com/products/\* are routed to ProductInventoryPool.

### Multiple-site hosting

For example, Front Door can serve traffic for images.contoso.com and videos.contoso.com from two backend pools called ImagePool and VideoPool.

Similarly, you can have two different domains www.contoso.com and www.fabrikam.com configured on the same Front Door.

### TLS termination

Front Door supports TLS termination at the edge that is, individual users can set up a TLS connection with Front Door environments instead of establishing it over long haul connections with the application backend.

### Application layer security

Azure Front Door allows you to author custom Web Application Firewall (WAF) rules for access control to protect your HTTP/HTTPS workload from exploitation based on client IP addresses, country code, and http parameters.

FAQ Front Door

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq>

1. What is the difference between Azure Front Door and Azure Application Gateway?

While both Front Door and Application Gateway are layer 7 (HTTP/HTTPS) load balancers, the primary difference is that Front Door is a global service whereas Application Gateway is a regional service. While Front Door can load balance between your different scale units/clusters/stamp units across regions, Application Gateway allows you to load balance between your VMs/containers etc. that is within the scale unit.

1. When should we deploy an Application Gateway behind Front Door?

The key scenarios why one should use Application Gateway behind Front Door are:

Front Door can perform path-based load balancing only at the global level but if one wants to load balance traffic even further within their virtual network (VNET) then they should use Application Gateway.

Since Front Door doesn't work at a VM/container level, so it cannot do Connection Draining. However, Application Gateway allows you to do Connection Draining.

With an Application Gateway behind Front Door, one can achieve 100% TLS/SSL offload and route only HTTP requests within their virtual network (VNET).

Front Door and Application Gateway both support session affinity. While Front Door can direct subsequent traffic from a user session to the same cluster or backend in a given region, Application Gateway can direct affinitize the traffic to the same server within the cluster.

1. Can we deploy Azure Load Balancer behind Front Door?

Yes

## Traffic Manager

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>

[Traffic Manager](https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview) 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. Because Traffic Manager is a **DNS-based(Level 3-4 and higher as well as it communicates directly )** load-balancing service, it load balances only at the domain level. For that reason, it can't fail over as quickly as Front Door, because of common challenges around DNS caching and systems not honoring DNS TTLs.

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works>

FAQs Traffic Manager:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-faqs>

1. What types of traffic can be routed using Traffic Manager?

Traffic Manager can route traffic that originates from the public internet to a set of endpoints that are also internet facing. If you have endpoints that are inside a private network (for example, an internal version of [Azure Load Balancer](https://docs.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations)) or have users making DNS requests from such internal networks, then you cannot use Traffic Manager to route this traffic.

1. What application protocols can I use with Traffic Manager?

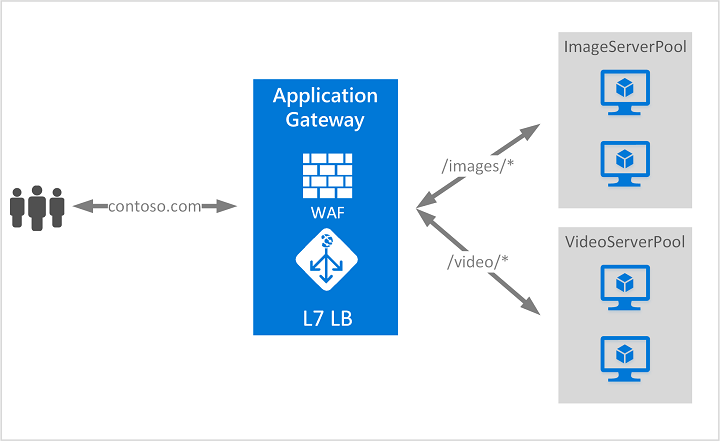
Traffic Manager works at the DNS level. Once the DNS lookup is complete, clients connect to the application endpoint directly, not through Traffic Manager. Therefore, the connection can use any application protocol.

## Azure Application Gateway

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

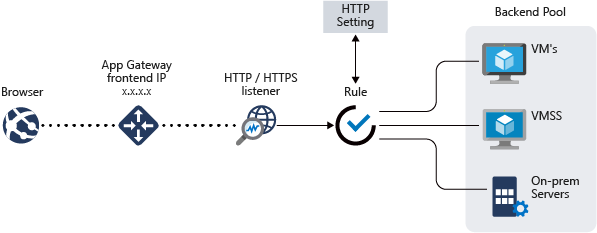
[Application Gateway](https://docs.microsoft.com/en-us/azure/application-gateway/overview) provides application delivery controller (ADC) as a service, offering various Layer 7 load-balancing capabilities. Use it to optimize web farm productivity by offloading CPU-intensive SSL termination to the gateway.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if /images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.



### Application Gateway Features

<https://docs.microsoft.com/en-us/azure/application-gateway/features>



* [Secure Sockets Layer (SSL/TLS) termination](https://docs.microsoft.com/en-us/azure/application-gateway/features#secure-sockets-layer-ssltls-termination)
* [Autoscaling](https://docs.microsoft.com/en-us/azure/application-gateway/features#autoscaling)
* [Zone redundancy](https://docs.microsoft.com/en-us/azure/application-gateway/features#zone-redundancy)
* [Static VIP](https://docs.microsoft.com/en-us/azure/application-gateway/features#static-vip)
* [Web Application Firewall](https://docs.microsoft.com/en-us/azure/application-gateway/features#web-application-firewall)
* [Ingress Controller for AKS](https://docs.microsoft.com/en-us/azure/application-gateway/features#ingress-controller-for-aks)
* [URL-based routing](https://docs.microsoft.com/en-us/azure/application-gateway/features#url-based-routing)
* [Multiple-site hosting](https://docs.microsoft.com/en-us/azure/application-gateway/features#multiple-site-hosting)
* [Redirection](https://docs.microsoft.com/en-us/azure/application-gateway/features#redirection)
* [Session affinity](https://docs.microsoft.com/en-us/azure/application-gateway/features#session-affinity)
* [Websocket and HTTP/2 traffic](https://docs.microsoft.com/en-us/azure/application-gateway/features#websocket-and-http2-traffic)
* [Connection draining](https://docs.microsoft.com/en-us/azure/application-gateway/features#connection-draining)
* [Custom error pages](https://docs.microsoft.com/en-us/azure/application-gateway/features#custom-error-pages)
* [Rewrite HTTP headers and URL](https://docs.microsoft.com/en-us/azure/application-gateway/features#rewrite-http-headers-and-url)
* [Sizing](https://docs.microsoft.com/en-us/azure/application-gateway/features#sizing)

## Azure Load Balancer

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

[Azure Load Balancer](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview) is a high-performance, low-latency Layer 4 load-balancing service (inbound and outbound) for all UDP and TCP protocols. It is built to handle millions of requests per second while ensuring your solution is highly available. Azure Load Balancer is **zone-redundant**, ensuring high availability across Availability Zones.

A [**public load balancer**](https://docs.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

An [**internal (or private) load balancer**](https://docs.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.

