Contents

[Vnet 2](#_Toc50858371)

[Deploy dedicated Azure services into virtual networks 2](#_Toc50858372)

[Subnet 2](#_Toc50858373)

[Route Table 2](#_Toc50858374)

[Network Security Group 2](#_Toc50858375)

[Application Security Group 3](#_Toc50858376)

[NAT 3](#_Toc50858377)

[VNET Peering 3](#_Toc50858378)

[Virtual Network Gateway 3](#_Toc50858379)

[Gateway types 3](#_Toc50858380)

[VPN 5](#_Toc50858381)

[VPN Types based on Connectivity: 5](#_Toc50858382)

[Point to Site(P2S) : 5](#_Toc50858383)

[Site to Site (S2S) : 5](#_Toc50858384)

[VNet-to-VNet (VNet2VNet) 6](#_Toc50858385)

[Virtual Network Gateway SKUs by feature set 6](#_Toc50858386)

[VPN types based on network routing 7](#_Toc50858387)

[PolicyBased: 7](#_Toc50858388)

[RouteBased: 8](#_Toc50858389)

[Express Route 8](#_Toc50858390)

[Key benefits 8](#_Toc50858391)

[Gateway subnet 9](#_Toc50858392)

[Express Route Direct 9](#_Toc50858393)

[Express Route FastPath 10](#_Toc50858394)

[Express Route Global Reach 10](#_Toc50858395)

[Virtual WAN 11](#_Toc50858396)

[FAQs 12](#_Toc50858397)

[Virtual Network basics 12](#_Toc50858398)

[Name Resolution (DNS) 13](#_Toc50858399)

[Connecting virtual machines 13](#_Toc50858400)

[Azure services that connect to VNets 14](#_Toc50858401)

[VNet peering 14](#_Toc50858402)

[Virtual network service endpoints 16](#_Toc50858403)

[Load Balancers 16](#_Toc50858404)

[Decision tree for load balancing in Azure 16](#_Toc50858405)

[Azure Front Door 17](#_Toc50858406)

[URL-based routing 17](#_Toc50858407)

[Multiple-site hosting 18](#_Toc50858408)

[TLS termination 18](#_Toc50858409)

[Application layer security 18](#_Toc50858410)

[Traffic Manager 19](#_Toc50858411)

[Azure Application Gateway 19](#_Toc50858412)

[Application Gateway Features 20](#_Toc50858413)

[Azure Load Balancer 21](#_Toc50858414)

# 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>

## Virtual network service endpoints

Todo

## Subnet

## Route Table

## Network Security Group

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

## Application Security Group

## NAT

<https://docs.microsoft.com/en-us/azure/virtual-network/nat-overview>

Virtual Network NAT (network address translation) simplifies **outbound-only Internet connectivity for virtual networks.** When configured on a subnet, all outbound connectivity uses your specified static public IP addresses. Outbound connectivity is possible without load balancer or public IP addresses directly attached to virtual machines. NAT is fully managed and highly resilient.

# VNET Peering

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

## Global Peering

# Virtual Network Gateway

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between **an Azure virtual network and an on-premises location** over the public Internet. You can also use a VPN gateway to send encrypted traffic between **Azure virtual networks over the Microsoft network**. **Each virtual network can have only one VPN gateway (of one type each i.e VPN and Express route).** However, you can create multiple connections to the same VPN gateway. When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

### Gateway types

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings>

**Each virtual network can only have one virtual network gateway of each type**. The available values for -GatewayType are:

* **Vpn :** To send encrypted traffic across the public Internet, you use the gateway type 'Vpn'. This is also referred to as a VPN gateway. **Site-to-Site, Point-to-Site, and VNet-to-VNet connections** all use a VPN gateway.
* **ExpressRoute :** To send network traffic on a private connection, you use the gateway type 'ExpressRoute'. This is also referred to as an ExpressRoute gateway and is the type of gateway used when configuring ExpressRoute.

**Note :**

1. **In general whenever Virtual Network Gateway is mentioned it means VPN unless Express Route is mentioned.**
2. **There is a cost associated with Virtual Network Gateway device, which doesn’t exist in VNet Peering.**

|  | **Point-to-Site** | **Site-to-Site** | **ExpressRoute** |
| --- | --- | --- | --- |
| **Azure Supported Services** | Cloud Services and Virtual Machines | Cloud Services and Virtual Machines | [Services list](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs#supported-services) |
| **Typical Bandwidths** | Based on the gateway SKU | Typically < 1 Gbps aggregate | 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps |
| **Protocols Supported** | Secure Sockets Tunneling Protocol (SSTP), OpenVPN and IPsec | IPsec | Direct connection over VLANs, NSP's VPN technologies (MPLS, VPLS,...) |
| **Routing** | RouteBased (dynamic) | We support PolicyBased (static routing) and RouteBased (dynamic routing VPN) | BGP |
| **Connection resiliency** | active-passive | active-passive or active-active | active-active |
| **Typical use case** | Prototyping, dev / test / lab scenarios for cloud services and virtual machines | Dev / test / lab scenarios and small scale production workloads for cloud services and virtual machines | Access to all Azure services (validated list), Enterprise-class and mission critical workloads, Backup, Big Data, Azure as a DR site |
| **SLA** | [SLA](https://azure.microsoft.com/support/legal/sla/) | [SLA](https://azure.microsoft.com/support/legal/sla/) | [SLA](https://azure.microsoft.com/support/legal/sla/) |
| **Pricing** | [Pricing](https://azure.microsoft.com/pricing/details/vpn-gateway/) | [Pricing](https://azure.microsoft.com/pricing/details/vpn-gateway/) | [Pricing](https://azure.microsoft.com/pricing/details/expressroute/) |
| **Technical Documentation** | [VPN Gateway Documentation](https://azure.microsoft.com/documentation/services/vpn-gateway/) | [VPN Gateway Documentation](https://azure.microsoft.com/documentation/services/vpn-gateway/) | [ExpressRoute Documentation](https://azure.microsoft.com/documentation/services/expressroute/) |
| **FAQ** | [VPN Gateway FAQ](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq) | [VPN Gateway FAQ](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vpn-faq) | [ExpressRoute FAQ](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs) |

## VPN

### Gateway subnet

Before you create a VPN gateway, you must create a **gateway subnet**. The gateway subnet contains the IP addresses that the virtual network gateway VMs and services use. When you create your virtual network gateway, gateway VMs are deployed to the gateway subnet and configured with the required VPN gateway settings. Never deploy anything else (for example, additional VMs) to the gateway subnet. The gateway subnet must be named **'GatewaySubnet'** to work properly. Naming the gateway subnet '**GatewaySubnet'** lets Azure know that this is the subnet to deploy the virtual network gateway VMs and services to.

### VPN Types based on Connectivity:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/design>

### Point to Site(P2S) :

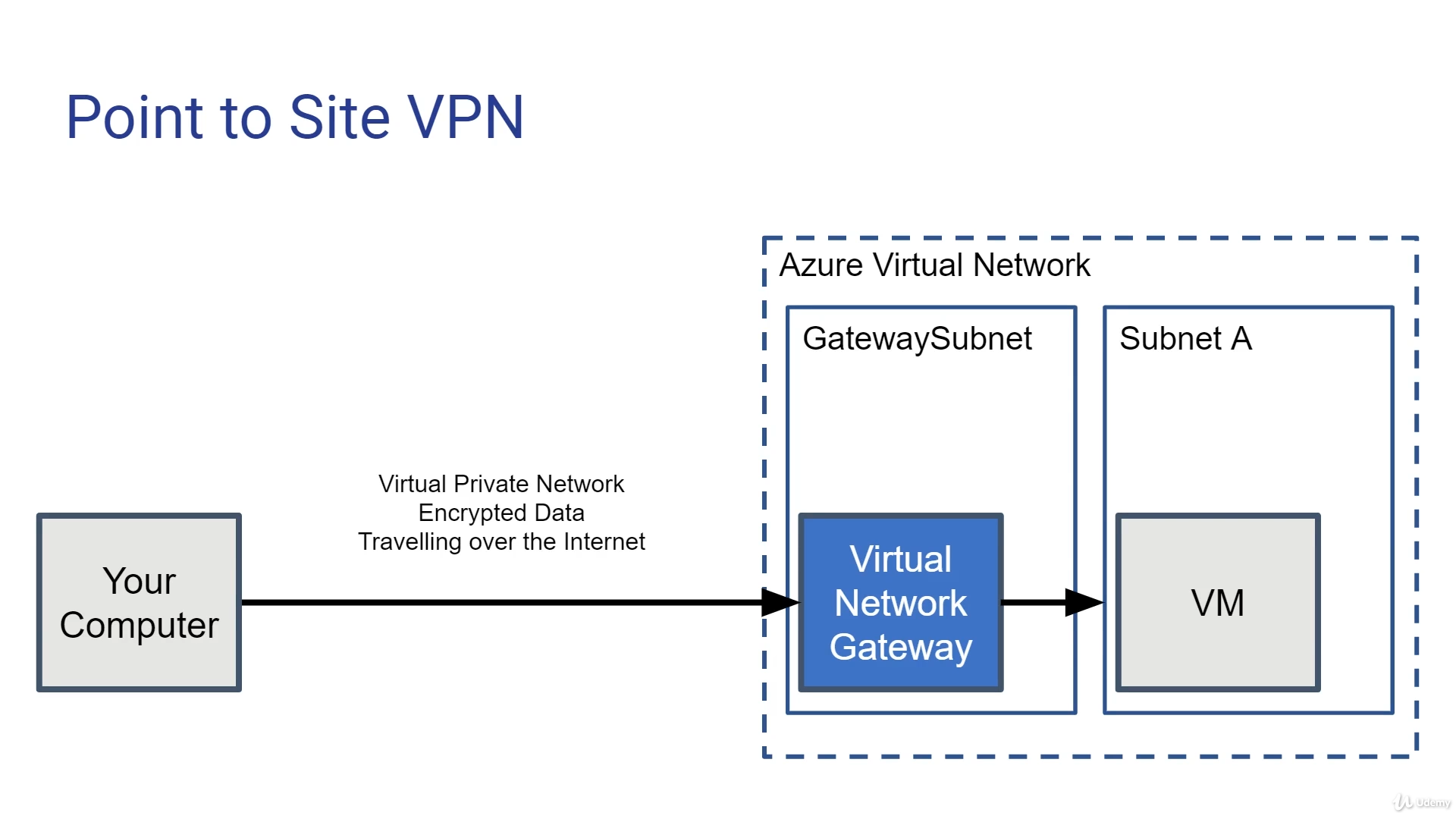
<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer.

**P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.**

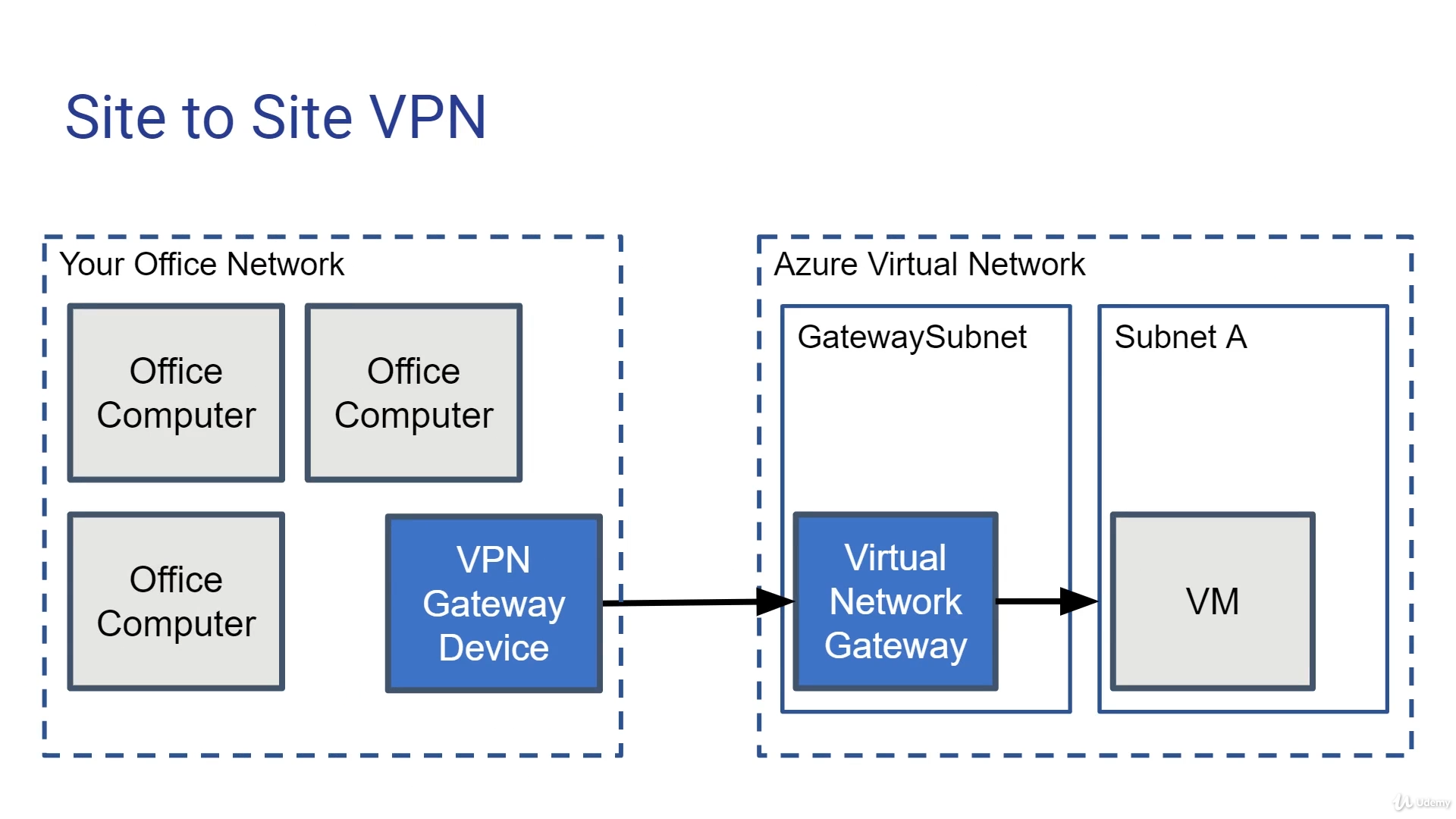
Point-to-site VPN can use one of the following protocols:

* **OpenVPN® Protocol**, an SSL/TLS based VPN protocol.
* Secure Socket Tunneling Protocol (SSTP), a proprietary TLS-based VPN protocol.
* IKEv2 VPN, a standards-based IPsec VPN solution.



### Site to Site (S2S) :

Unlike a software in P2S in case of S2S a VPN gateway device is required at the site from where we need to create the connection. However it has advantages like redundancy, active-active etc



### VNet-to-VNet (VNet2VNet)

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>

When you connect a virtual network to another virtual network with a VNet-to-VNet connection type (VNet2VNet), it's similar to creating a Site-to-Site IPsec connection to an on-premises location. Both connection types use a VPN gateway to provide a secure tunnel with IPsec/IKE and function the same way when communicating. However, they differ in the way the local network gateway is configured.

You can also connect your VNets by using VNet peering. VNet peering doesn't use a VPN gateway and has different constraints.

You may want to connect virtual networks by using a VNet-to-VNet connection for the following reasons:

* You can set up your own geo-replication or synchronization with secure connectivity without going over internet-facing endpoints.
* With Azure Traffic Manager and Azure Load Balancer, you can set up highly available workload with geo-redundancy across multiple Azure regions. For example, you can set up SQL Server Always On availability groups across multiple Azure regions.
* Within the same region, you can set up multi-tier applications with multiple virtual networks that are connected together because of isolation or administrative requirements.

### Virtual Network Gateway SKUs by feature set

The new VPN gateway SKUs streamline the feature sets offered on the gateways:

| Gateway SKUs by feature set | |
| --- | --- |
| **SKU** | **Features** |
| **Basic** (\*\*) | **Route-based VPN**: 10 tunnels for S2S/connections; no RADIUS authentication for P2S; no IKEv2 for P2S **Policy-based VPN**: (IKEv1): 1 S2S/connection tunnel; no P2S |
| **All Generation1 and Generation2 SKUs except Basic** | **Route-based VPN**: up to 30 tunnels (\*), P2S, BGP, active-active, custom IPsec/IKE policy, ExpressRoute/VPN coexistence |

Due to the differences in SLAs and feature sets, we recommend the following SKUs for production vs. dev-test:

| Gateway SKUs - Production vs. Dev-Test Workloads | |
| --- | --- |
| **Workload** | **SKUs** |
| **Production, critical workloads** | **All Generation1 and Generation2 SKUs except Basic** |
| **Dev-test or proof of concept** | Basic (\*\*) |

## VPN types based on network routing

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#vpntype>

When you create the virtual network gateway for a VPN gateway configuration, you must specify a VPN type. The VPN type that you choose depends on the connection topology that you want to create.

Once a virtual network gateway has been created, you can't change the VPN type. You have to delete the virtual network gateway and create a new one. There are two VPN types:

### PolicyBased:

PolicyBased VPNs were previously called static routing gateways in the classic deployment model. When using a PolicyBased VPN, keep in mind the following limitations:

* **PolicyBased VPNs can only be used on the Basic gateway SKU**. This VPN type is not compatible with other gateway SKUs.
* You can have only 1 tunnel when using a PolicyBased VPN.
* You can only use PolicyBased VPNs for S2S connections, and only for certain configurations. **Most VPN Gateway configurations require a RouteBased VPN**.

### **RouteBased**:

RouteBased VPNs were previously called dynamic routing gateways in the classic deployment model. RouteBased VPNs use "routes" in the IP forwarding or routing table to direct packets into their corresponding tunnel interfaces. The tunnel interfaces then encrypt or decrypt the packets in and out of the tunnels. The policy (or traffic selector) for RouteBased VPNs are configured as any-to-any (or wild cards). The value for a RouteBased VPN type is RouteBased.

## Express Route

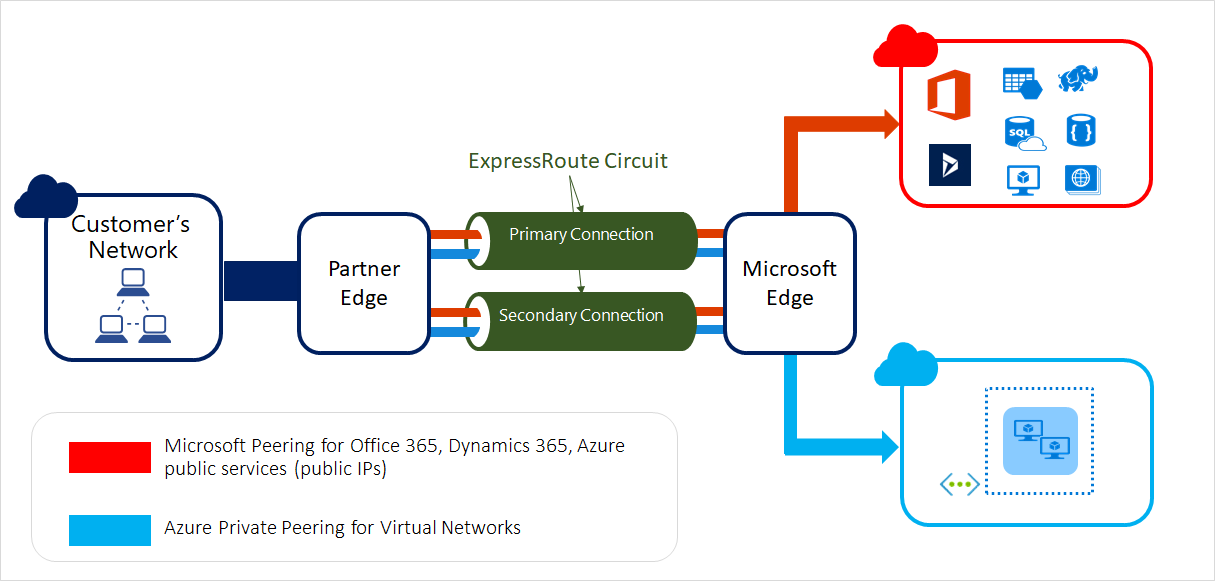
<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction>

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider.

## Key benefits

* Layer 3 connectivity **between your on-premises network and the Microsoft Cloud through a connectivity provider**. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
* Connectivity to **Microsoft cloud services across all regions in the geopolitical region**.
* Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
* Dynamic routing between your network and Microsoft via BGP.
* Built-in redundancy in every peering location for higher reliability.
* Connection uptime [SLA](https://azure.microsoft.com/support/legal/sla/).
* QoS support for Skype for Business.

Each ExpressRoute circuit consists of two connections to two Microsoft Enterprise edge routers (MSEEs) at an ExpressRoute Location from the connectivity provider/your network edge. Microsoft requires dual BGP connection from the connectivity provider/your network edge – one to each MSEE. You may choose not to deploy redundant devices/Ethernet circuits at your end. However, connectivity providers use redundant devices to ensure that your connections are handed off to Microsoft in a redundant manner. A redundant Layer 3 connectivity configuration is a requirement for our SLA to be valid.



<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-about-virtual-network-gateways>

ExpressRoute virtual network gateways can use the following SKUs:

* Standard
* HighPerformance
* UltraPerformance

### Gateway subnet

Before you create an ExpressRoute gateway, you must create a gateway subnet. The gateway subnet contains the IP addresses that the virtual network gateway VMs and services use. When you create your virtual network gateway, gateway VMs are deployed to the gateway subnet and configured with the required ExpressRoute gateway settings. Never deploy anything else (for example, additional VMs) to the gateway subnet. The gateway subnet must be named 'GatewaySubnet' to work properly. Naming the gateway subnet 'GatewaySubnet' lets Azure know that this is the subnet to deploy the virtual network gateway VMs and services to.

### Express Route Direct

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-erdirect-about>

ExpressRoute Direct provides dual 100 Gbps or 10 Gbps connectivity, which supports Active/Active connectivity at scale.

Key features that ExpressRoute Direct provides include, but aren't limited to:

* Massive Data Ingestion into services like Storage and Cosmos DB
* Physical isolation for industries that are regulated and require dedicated and isolated connectivity like: Banking, Government, and Retail
* Granular control of circuit distribution based on business unit

| **ExpressRoute using a service provider** | **ExpressRoute Direct** |
| --- | --- |
| Utilizes service providers to enable fast onboarding and connectivity into existing infrastructure | Requires 100 Gbps/10 Gbps infrastructure and full management of all layers |
| Integrates with hundreds of providers including Ethernet and MPLS | Direct/Dedicated capacity for regulated industries and massive data ingestion |
| Circuits SKUs from 50 Mbps to 10 Gbps | Customer may select a combination of the following circuit SKUs on 100 Gbps ExpressRoute Direct:   * 5 Gbps * 10 Gbps * 40 Gbps * 100 Gbps   Customer may select a combination of the following circuit SKUs on 10 Gbps ExpressRoute Direct:   * 1 Gbps * 2 Gbps * 5 Gbps * 10 Gbps |
| Optimized for single tenant | **Optimized for single tenant with multiple business units and multiple work environments** |

### Express Route FastPath

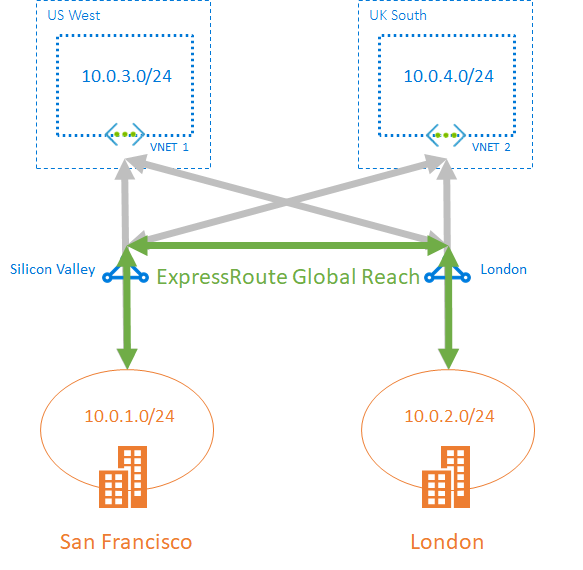
<https://docs.microsoft.com/en-us/azure/expressroute/about-fastpath>

ExpressRoute virtual network gateway is designed to exchange network routes and route network traffic. FastPath is designed to improve 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.

### Express Route Global Reach

<https://docs.microsoft.com/en-us/azure/expressroute/expressroute-global-reach>

ExpressRoute Global Reach is designed to complement your service provider’s WAN implementation and connect your branch offices across the world. For example, if your service provider primarily operates in the United States and has linked all of your branches in the U.S., but the service provider doesn’t operate in Japan and Hong Kong, with ExpressRoute Global Reach you can work with a local service provider and Microsoft will connect your branches there to the ones in the U.S. using ExpressRoute and our global network.



# Azure Relay

<https://docs.microsoft.com/en-us/azure/azure-relay/relay-what-is-it>

The Azure Relay service enables you to securely expose services that run in your corporate network to the public cloud. You can do so without opening a port on your firewall, or making intrusive changes to your corporate network infrastructure.

The relay service supports the following scenarios between on-premises services and applications running in the cloud or in another on-premises environment.

* Traditional one-way, request/response, and peer-to-peer communication
* Event distribution at internet-scope to enable publish/subscribe scenarios
* Bi-directional and unbuffered socket communication across network boundaries.

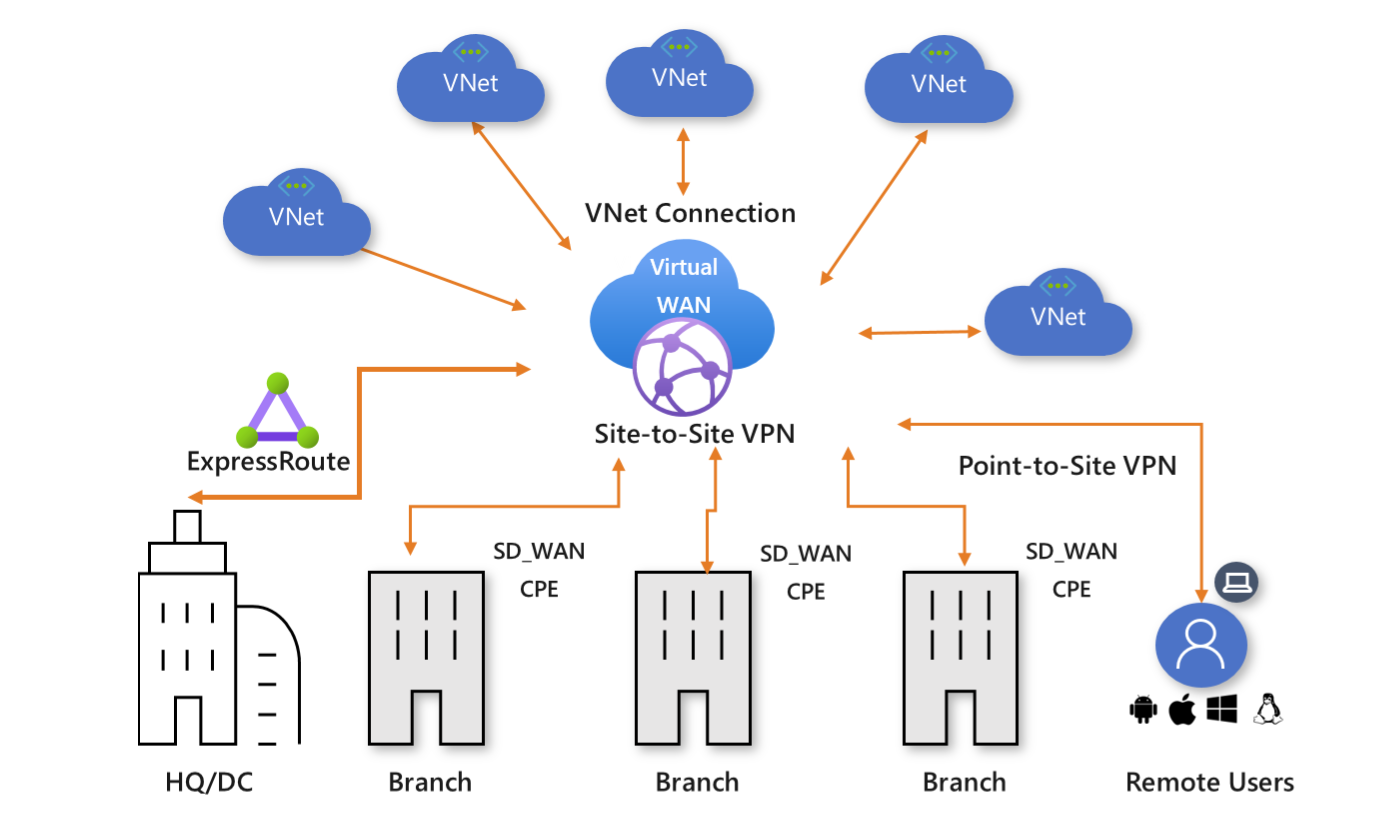
Azure Relay differs from network-level integration technologies such as VPN. An Azure relay can be scoped to a single application endpoint on a single machine. The VPN technology is far more intrusive, as it relies on altering the network environment.

# Virtual WAN

<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. These functionalities include

* branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE),
* Site-to-site VPN connectivity,
* remote user VPN (Point-to-site) connectivity,
* private (ExpressRoute) connectivity,
* intra-cloud connectivity (transitive connectivity for virtual networks),
* VPN ExpressRoute inter-connectivity,
* routing,
* Azure Firewall, and
* encryption for private connectivity.



| **Virtual WAN type** | **Hub type** | **Available configurations** |
| --- | --- | --- |
| Basic | Basic | Site-to-site VPN only |
| Standard | Standard | ExpressRoute User VPN (P2S) VPN (site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub |

TASK:

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

# 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.

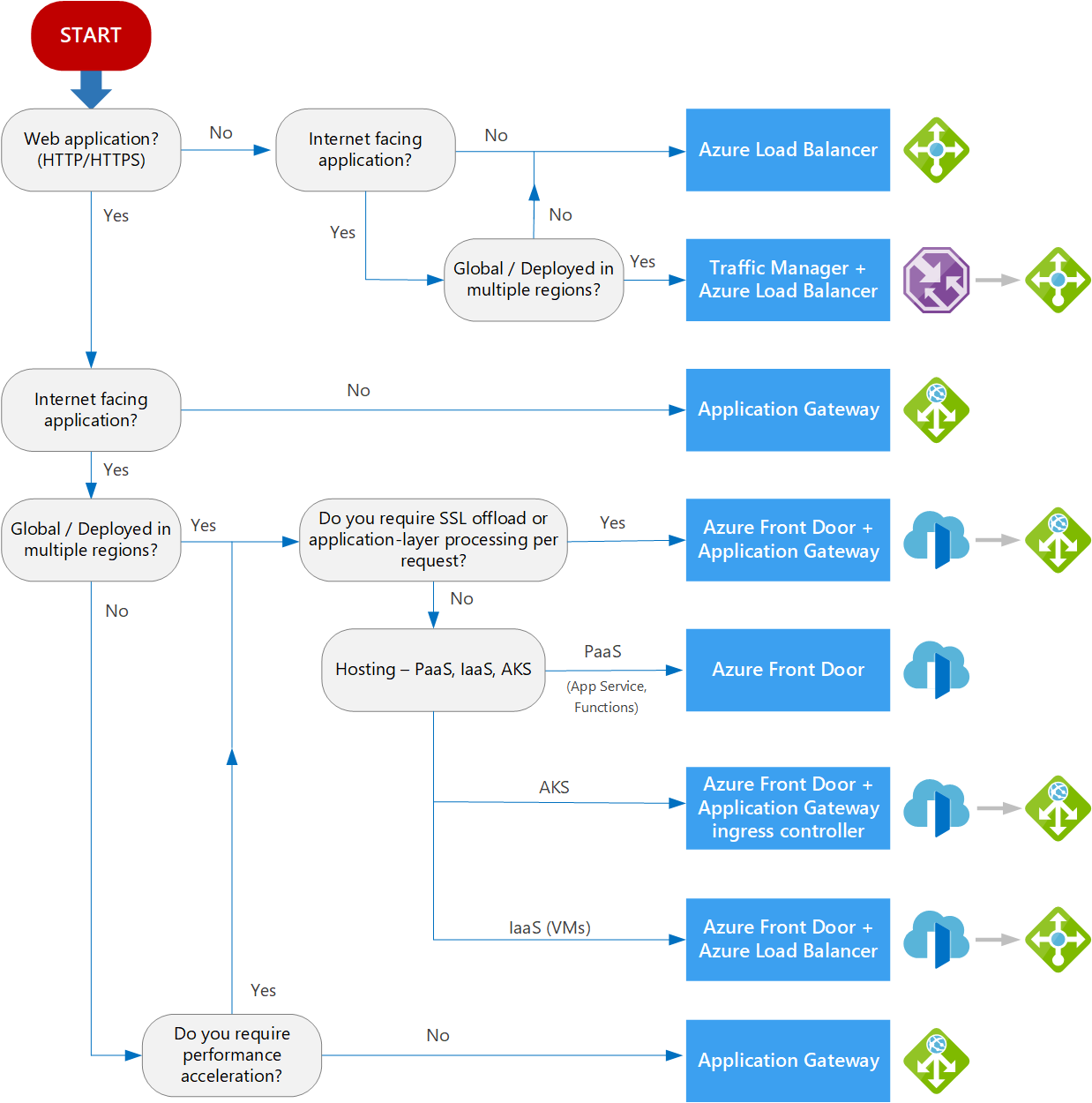
# Load Balancers

<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?

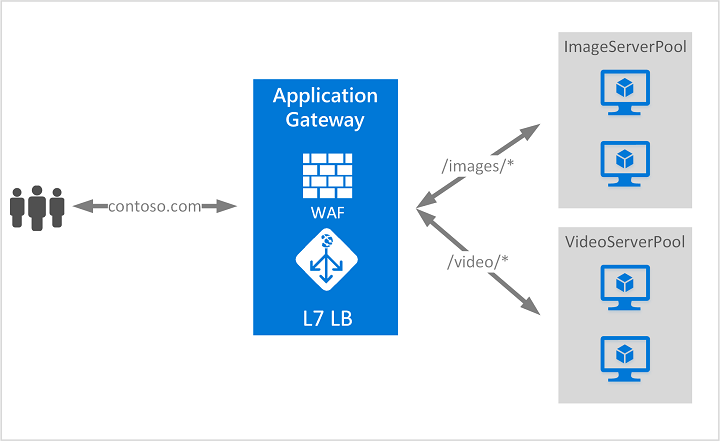
Traffic Manager works at the DNS level. Once the DNS lookup is complete, clients connect to the application endpoint directly, not through Traffic Manager. Therefore, the connection can use any application protocol.

## Azure Application Gateway

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

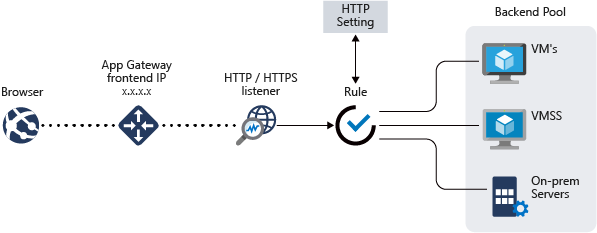
[Application Gateway](https://docs.microsoft.com/en-us/azure/application-gateway/overview) provides application delivery controller (ADC) as a service, offering various Layer 7 load-balancing capabilities. Use it to optimize web farm productivity by offloading CPU-intensive SSL termination to the gateway.

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.

