Networking

What is Azure Virtual Network	Azure virtual network enables Azure resources to securely communicate with each other, the internet, and on-premises networks.
Communicate between Azure resources	• **Through a virtual network:** • **Through a virtual network service endpoint:** • **Through VNet Peering:**
Communicate with on-premises resources (**create point to site** or site-site VPN)	• **Point-to-site virtual private network (VPN):** Established between a virtual network and a single computer in your network. Each computer that wants to establish connectivity with a virtual network must configure its connection. • **Site-to-site VPN:** Established between your on-premises VPN device and an Azure VPN Gateway that is deployed in a virtual network. • **Azure ExpressRoute:** Established between your network and Azure, through an ExpressRoute partner. This connection is private..
Route network traffic (**Create a route table to make subnet private**)	• **Route tables:** You can create custom route tables with routes that control where traffic is routed to for each subnet. Learn more about route tables. • **Border gateway protocol (BGP) routes:** If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks. Learn more about using BGP with Azure VPN Gateway and ExpressRoute.
Create Virtual Network (**create network**)	Powershell

PowerShell

Copy Try It

```
New-AzResourceGroup -Name TestResourceGroup -Location centralus
$frontendSubnet = New-AzVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix "10.0.1.0/24"
$backendSubnet  = New-AzVirtualNetworkSubnetConfig -Name backendSubnet  -AddressPrefix "10.0.2.0/24"
New-AzVirtualNetwork -Name MyVirtualNetwork -ResourceGroupName TestResourceGroup -Location centralus -Addressf
```

Cli

Azure CLI

```
az network vnet create \
  --name myVNet \
  --resource-group CreateVNetQS-rg \
  --subnet-name default
```

Virtual network traffic routing
System routes

(Check the default routes)

(add a peering and check optional default routes)

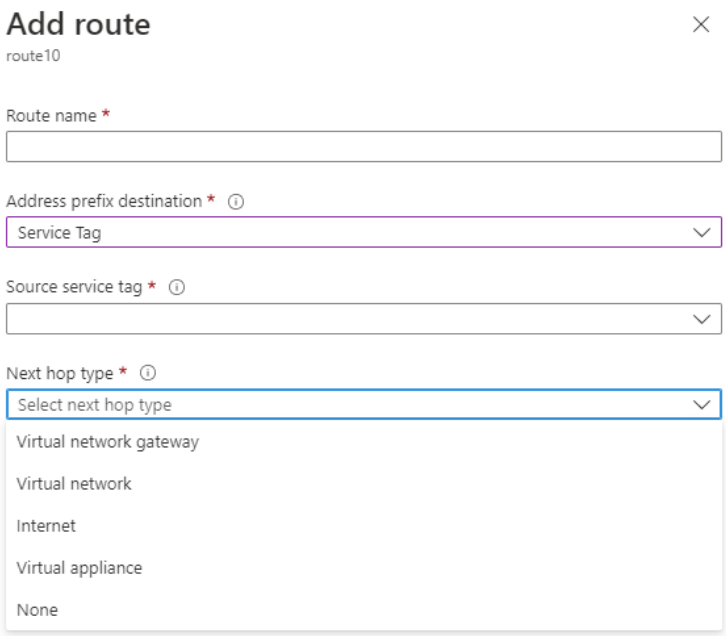
Azure automatically creates a route table for each subnet within an Azure virtual network and adds system default routes to the table.
System routes
Default

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	172.16.0.0/12	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None

Optional default routes

	<table><tr><th>Source</th><th>Address prefixes</th><th>Next hop type</th><th>Subnet within virtual network that route is added to</th></tr><tr><td>Default</td><td>Unique to the virtual network, for example: 10.1.0.0/16</td><td>VNet peering</td><td>All</td></tr><tr><td>Virtual network gateway</td><td>Prefixes advertised from on-premises via BGP, or configured in the local network gateway</td><td>Virtual network gateway</td><td>All</td></tr><tr><td>Default</td><td>Multiple</td><td>VirtualNetworkServiceEndpoint</td><td>Only the subnet a service endpoint is enabled for.</td></tr></table> • **Virtual network (VNet) peering:** • **Virtual network gateway:** • **VirtualNetworkServiceEndpoint:** The public IP addresses for certain services are added to the route table by Azure when you enable a service endpoint to the service. Service endpoints are enabled for individual subnets within a virtual network, so the route is only added to the route table of a subnet a service endpoint is enabled for. The public IP addresses of Azure services change periodically.
Virtual network traffic routing **Custom routes** **(create a route table and verify next hop types)**	You can create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to add more routes to a subnet's route table. You can specify the following **next hop types** when creating a user-defined route: **Virtual network:** Specify when you want to override the default routing within a virtual network. **Internet:** **Virtual appliance:** A virtual appliance is a virtual machine that typically runs a network application, such as a firewall. **Virtual network gateway:** Specify when you want traffic destined for specific address prefixes routed to a virtual network gateway. The virtual network gateway must be created with type VPN.

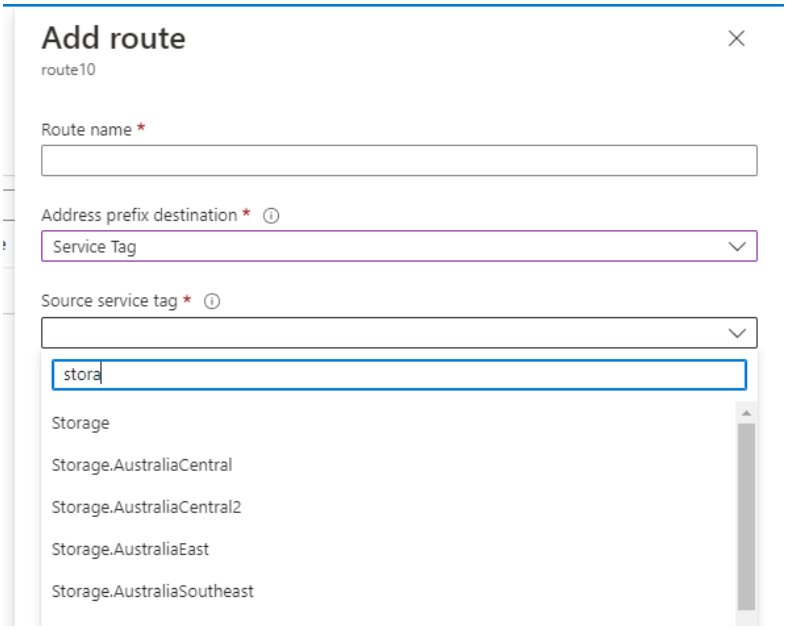
None: Specify when you want to drop traffic to an address prefix, rather than forwarding the traffic to a destination.



You can't specify VNet peering or VirtualNetworkServiceEndpoint as the next hop type in user-defined routes. Routes with the VNet peering or VirtualNetworkServiceEndpoint next hop types are only created by Azure, when you configure a virtual network peering, or a service endpoint.

Service Tags for user-defined routes

You can now specify a service tag as the address prefix for a user-defined route instead of an explicit IP range. A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change.

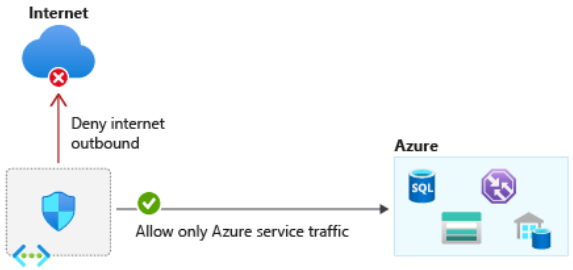
	
How Azure selects a route	When outbound traffic is sent from a subnet, Azure selects a route based on the destination IP address, using the **longest prefix match algorithm. Azure will select a more specific route.** If multiple routes contain the same address prefix, Azure selects the route type, based on the following priority: 1. User-defined route 2. BGP route 3. System route

Virtual network peering **(create peering,** **Modify address ranges)**	Azure supports the following types of peering: ● Virtual network peering: Connecting virtual networks within the same Azure region. ● Global virtual network peering: Connecting virtual networks across Azure regions. You can **resize the address space** of Azure virtual networks that are peered without incurring any downtime on the currently peered address space. After resizing the address space, all that is required is **for peers to be synced with the new address space changes**. Addresses can be resized in the following ways: ● Modifying the address range prefix of an existing address range (For example changing 10.1.0.0/16 to 10.1.0.0/18) ● Adding address ranges to a virtual network ● Deleting address ranges from a virtual network
Private Endpoints (**create private endpoint**)	Private endpoints allow ingress of traffic from your virtual network to an Azure resource securely. This private link is established **without the need of public IP addresses. A private endpoint is a special network interface for an Azure service in your virtual network.** When you create a private endpoint for your resource, it provides secure connectivity between clients on your virtual network and your Azure resource. The client application typically uses a **DNS host name to reach the target service. No changes are needed to the application. DNS resolution in the VNet must be configured** to resolve that same host name to the target resource's private IP address instead of the original public IP address. With a private path between the client and the target service, the client doesn't rely on the public IP address. When you create a private endpoint, a private DNS zone is also created.
Service endpoints **(create service endpoint)**	**Endpoints allow you to secure your Azure resources to only your virtual networks.** Service endpoints enable private IP addresses in the VNet to reach an Azure service without the need of an outbound public IP.

	Without service endpoints, restricting access to just your VNet can be challenging. **With service endpoints, DNS entries for Azure services remain as-is and continue to resolve to public IP addresses assigned to the Azure service.** **Network security groups (NSGs) with service endpoints:** ● By default, NSGs allow outbound internet traffic and also allow traffic from your VNet to Azure services. This traffic continues to work with service endpoints as is. ● **If you want to deny all outbound internet traffic and allow only traffic to specific Azure services, you can do so using service tags in your NSGs.** You can specify supported Azure services as destinations in your NSG rules and Azure also provides the maintenance of IP addresses underlying each tag. **Key Benefits:** ● **Improved security for your Azure service resources:** Service endpoints enable securing of Azure service resources to your virtual network by extending VNet identity to the service. ● **Optimal routing for Azure service traffic from your virtual network** ● **Simple to set up with less management overhead**

Private Endpoints vs Service Endpoints
(use both and compare)

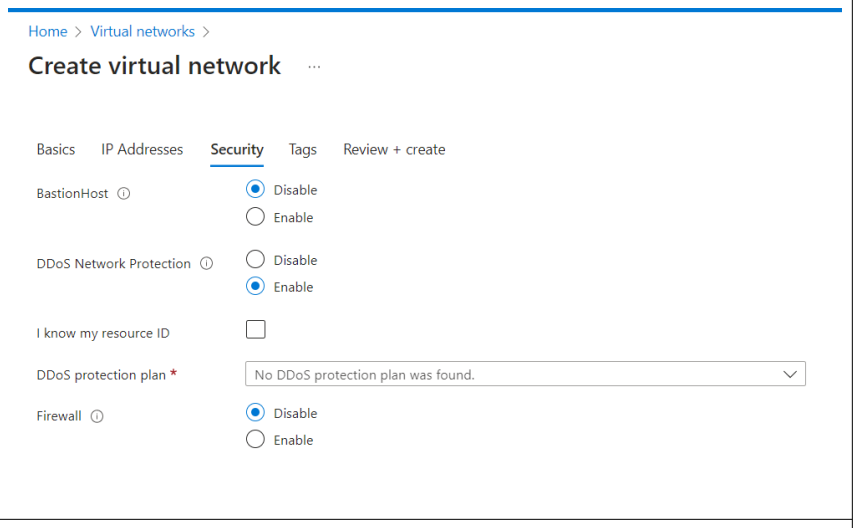
Consideration	Service Endpoints	Private Endpoints
Service scope at which level the configuration applies	Entire service (for example, *all* SQL Servers or Storage accounts of *all* customers)	Individual instance (for example, a specific SQL Server instance or Storage account *you* own)
In-Built Data Exfiltration Protection - ability to move/copy data from protected PaaS resource to other unprotected PaaS resource by malicious insider	No	Yes
Private Access to PaaS resource from On-Premises	No	Yes
NSG configuration required for Service Access	Yes (using Service Tags)	No
Service can be reached without using any public IP address	No	Yes
Azure-to-Azure traffic stays on the Azure backbone network	Yes	Yes
Service can disable its public IP address	No	Yes
You can easily restrict traffic coming from an Azure Virtual Network	Yes (allow access from specific subnets and or use NSGs)	Yes
You can easily restrict traffic coming from on-prem (VPN/ExpressRoute)	N/A**	Yes
Requires DNS changes	No	Yes (see DNS configuration)
Impacts the cost of your solution	No	Yes (see Private link pricing)
Impacts the composite SLA of your solution	No	Yes (Private link service itself has a 99.99% SLA)
Setup and maintenance	Simple to set up with less management overhead	Additional effort is required
Limits	No limit on the total number of service endpoints in a virtual network. Azure services may enforce limits on the number of subnets used for securing the resource. (see VNet FAQ)	Yes (see Private Link limits)

Virtual network service endpoint policies for Azure Storage (create service endpoint policies)	• Endpoint policies allow you to specify the Azure Storage accounts that are allowed virtual network outbound access and restrict access to all the other storage accounts. This gives much more granular security control for protecting data exfiltration from your virtual network. • By default, if no policies are attached to a subnet with endpoints, you can access all storage accounts in the service.
Service tags**(Use service tags in nsg)**	A service tag represents a group of IP address prefixes from a given Azure service. With service tags, you can define network access controls on network security groups or Azure Firewall. You can allow or deny the traffic for the service. To allow or deny the traffic, specify the service tag in the source or destination field of a rule.  **Service Tags in a network security group** Action | Name | Source | Destination | Destination service tag | Protocol **Allow** | AllowStorage | VirtualNetwork | Service Tag | **Storage** | Any **Allow** | AllowSQL | VirtualNetwork | Service Tag | **Sql.EastUS** | Any **Deny** | DenyAllOutBound | Any | Any | Any | Any Default tags are predefined identifiers that represent a category of IP addresses. The VirtualNetwork tag denotes all virtual and local network address spaces. The AzureLoadBalancer tag denotes the IP addresses from where Azure load balancer health probes will originate. The Internet tag denotes the public IP address space.

Private Link	Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network. **Traffic between your virtual network and the service travels the Microsoft backbone network.** Exposing your service to the public internet is no longer necessary. You can create your own private link service in your virtual network and deliver it to your customers. Setup and consumption using Azure Private Link is consistent across Azure PaaS, customer-owned, and shared partner services. **Key benefits:** ● **Privately access services on the Azure platform** ● **On-premises and peered networks** ● **Protection against data leakage**: A private endpoint is mapped to an instance of a PaaS resource instead of the entire service. Consumers can only connect to the specific resource. ● **Global reach** ● **Extend to your own services**
Application security groups (**create app security group, verify the constraints**)	Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. **The rules that specify an application security group as the source or destination are only applied to the network interfaces that are members of the application security group.** Application security groups have the following constraints: ● **You cannot add network interfaces from different virtual networks to the same application security group.** ● **If you specify an application security group as the source and destination in a security rule, the network interfaces in both application security groups must exist in the same virtual network.**

Azure DDoS Protection **(check how to create Ddos protection)**	## Key benefits **Always-on traffic monitoring** **Adaptive real time tuning** Intelligent traffic profiling learns your application's traffic over time, and selects and updates the profile that is the most suitable for your service. The profile adjusts as traffic changes over time. **DDoS Protection telemetry, monitoring, and alerting** Azure DDoS Protection applies three auto-tuned mitigation policies (TCP SYN, TCP, and UDP) for each public IP of the protected resource, in the virtual network that has DDoS enabled. The policy thresholds are auto-configured via machine learning-based network traffic profiling. DDoS mitigation occurs for an IP address under attack only when the policy threshold is exceeded. **Azure DDoS Rapid Response** During an active attack, Azure DDoS Protection customers have access to the DDoS Rapid Response (DRR) team, who can help with attack investigation during an attack and post-attack analysis. For more information, see Azure DDoS Rapid Response. ## SKU Azure DDoS Protection is offered in two available SKUs, **DDoS IP Protection and DDoS Network Protection**. For more information about the SKUs, see SKU comparison. **Native platform integration** Natively integrated into Azure. Includes configuration through the Azure portal. Azure DDoS Protection understands your resources and resource configuration. **Turnkey protection** Simplified configuration immediately protects all resources on a virtual network as soon as **DDoS Network Protection** is enabled. No intervention or user definition is required. Similarly, simplified configuration immediately protects a public IP resource when **DDoS IP Protection** is enabled for it.

	Multi-Layered protection When deployed with a web application firewall (WAF), Azure DDoS Protection protects both at the network layer (Layer 3 and 4, offered by Azure DDoS Protection) and at the application layer (Layer 7, offered by a WAF). WAF offerings include Azure Application Gateway WAF SKU and third-party web application firewall offerings available in the Azure Marketplace. **Extensive mitigation scale** All L3/L4 attack vectors can be mitigated, with global capacity, to protect against the largest known DDoS attacks. **Attack analytics** Get detailed reports in five-minute increments during an attack, and a complete summary after the attack ends. **Attack metrics** Summarized metrics from each attack are accessible through Azure Monitor. See View and configure DDoS protection telemetry to learn more. **Attack alerting** **Cost guarantee** Receive data-transfer and application scale-out service credit for resource costs incurred as a result of documented DDoS attacks.

Load Balancer

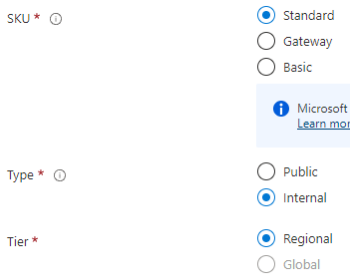
What is Azure Load Balancer?	Azure Load Balancer operates at **layer 4** of the Open Systems Interconnection (OSI) model. A public load balancer can provide outbound connections for virtual machines (VMs) inside your virtual network. An internal (or private) load balancer is used where private IPs are needed at the frontend only.

SKUs:

Standard Load Balancer:
(public or private)
(tier: regional or global)

Basic Load Balancer:
(public or private)
(tier: regional)

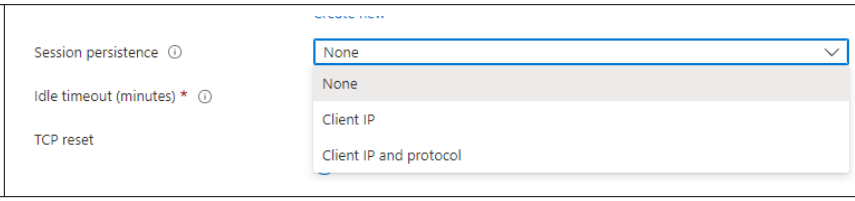
Gateway Load Balancer:
(private only)
(tier regional)



(create each of these load balancers and instances to its backend(availability sets, scale set etc))

	Standard Load Balancer	Basic Load Balancer
Scenario	Equipped for load-balancing network layer traffic when high performance and ultra-low latency is needed. Routes traffic within and across regions, and to availability zones for high resiliency.	Equipped for small-scale applications that don't need high availability or redundancy. Not compatible with availability zones.
Backend type	IP based, NIC based	NIC based
Protocol	TCP, UDP	TCP, UDP
Backend pool endpoints	Any virtual machines or virtual machine scale sets in a single virtual network	Virtual machines in a single availability set or virtual machine scale set
Health probes	TCP, HTTP, HTTPS	TCP, HTTP
Health probe down behavior	TCP connections stay alive on an instance probe down and on all probes down.	TCP connections stay alive on an instance probe down. All TCP connections end when all probes are down.
Availability Zones	Zone-redundant and zonal frontends for inbound and outbound traffic	Not available
Diagnostics	Azure Monitor multi-dimensional metrics	Not supported
HA Ports	Available for Internal Load Balancer	Not available
Secure by default	Closed to inbound flows unless allowed by a network security group. Internal traffic from the virtual network to the internal load balancer is allowed.	Open by default. Network security group optional.
Outbound Rules	Declarative outbound NAT configuration	Not available
TCP Reset on Idle	Available on any rule	Not available
Multiple front ends	Inbound and outbound	Inbound only
Management Operations	Most operations < 30 seconds	60-90+ seconds typical
SLA	99.99%	Not available
Global VNet Peering Support	Standard ILB is supported via Global VNet Peering	Not supported
NAT Gateway Support	Both Standard ILB and Standard Public LB are supported via Nat Gateway	Not supported
Private Link Support	Standard ILB is supported via Private Link	Not supported
Global tier (Preview)	Standard LB supports the Global tier for Public LBs enabling cross-region load balancing	Not supported

Azure Load Balancer components (**explore all these components and change/add few settings, use powershell to create**)	**Frontend IP configuration:** The IP address of your Azure Load Balancer. It's the point of contact for clients. These IP addresses can be either: ● Public IP Address (Public load balancer) ● Private IP Address (Internal Load Balancer) **Backend pool:** Backend pools support addition of instances via network interface or IP addresses. **Health probes :** A health probe is used to determine the health status of the instances in the backend pool. **Load Balancer rules:** A load balancer rule is used to define how incoming traffic is distributed to all the instances within the backend pool. A load-balancing rule maps a given frontend IP configuration and port to multiple backend IP addresses and ports. **Inbound NAT rules:** An inbound NAT rule forwards incoming traffic sent to frontend IP address and port combination. The traffic is sent to a specific virtual machine or instance in the backend pool. **Outbound rules:** An outbound rule configures outbound Network Address Translation (NAT) for all virtual machines or instances identified by the backend pool. This rule enables instances in the backend to communicate (outbound) to the internet or other endpoints.
High Availability Ports **(create HA port LB and check its functioning)**	A load balancer rule configured with 'protocol - all and port - 0' is known as an High Availability (HA) port rule. This rule enables a single rule to load-balance all TCP and UDP flows that arrive on all ports of an **internal Standard Load Balancer.** The HA ports load-balancing rules help you with critical scenarios, such as high availability and scale for network virtual appliances (NVAs) inside virtual networks. The feature can help when a large number of ports must be load-balanced.
Load balancing algorithm (use each of these algos and see how they behave differently)	Azure Load Balancer distribution modes: 1. Hash based 2. Session persistence a. Session Persistence: Client IP b. Session Persistence: Client IP and Protocol Under load balancing rules:



Azure Load Balancer distribution modes

Distribution mode	Hash based	Session persistence: Client IP	Session persistence: Client IP and protocol
Overview	Traffic from the same client IP routed to any healthy instance in the backend pool	Traffic from the same client IP is routed to the same backend instance	Traffic from the same client IP and protocol is routed to the same backend instance
Tuples	5 tuple	2 tuple	3 tuple
Azure portal configuration	Session persistence: **None**	Session persistence: **Client IP**	Session persistence: **Client IP and protocol**
REST API	`"loadDistribution":"Default"`	`"loadDistribution":SourceIP`	`"loadDistribution":SourceIPProtocol`

Hash based

Azure Load Balancer uses a five tuple hash based distribution mode by default.

The five tuple consists of:

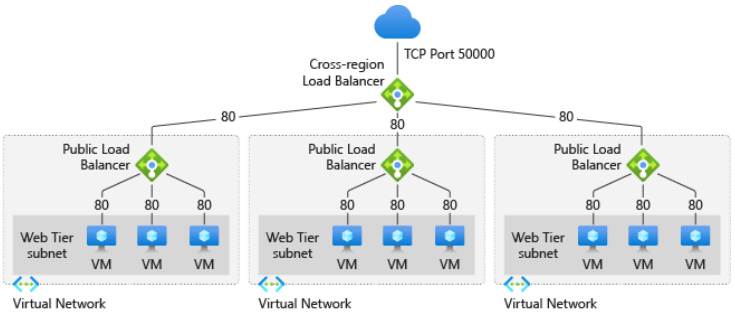
- Source IP
- Source port
- Destination IP
- Destination port
- Protocol type

Session persistence

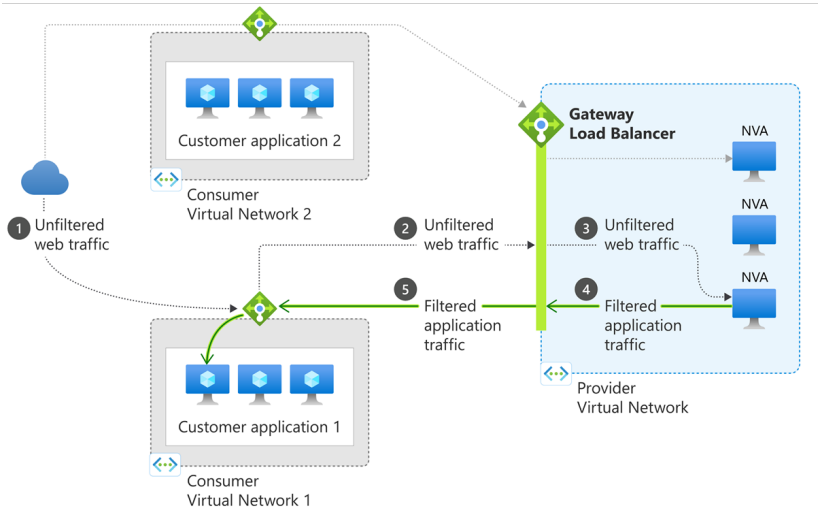
Session persistence is also known as session affinity, source IP affinity, or client IP affinity. This distribution mode uses a two-tuple (source IP and destination IP) or three-tuple (source IP, destination IP, and protocol type) hash to route to backend instances.

Session persistence mode has two configuration types:

- **Client IP (2-tuple) -** Specifies that successive requests from the same client IP address will be handled by the same backend instance.
- **Client IP and protocol (3-tuple)** - Specifies that successive requests from the same client IP address and protocol combination will be handled by the same backend instance.

Load Balancer and Availability Zones **(create LB with one of these options)**	A Load Balancer can either be **zone redundant, zonal, or non-zonal**. **zone redundant(zones= [1,2,3])** **zonal(zone=[1] or [2])** **non-zonal(zone=[ ])**
Cross-region load balancer (create cross LB)	 If one region fails, the traffic is routed to the next closest healthy regional load balancer.

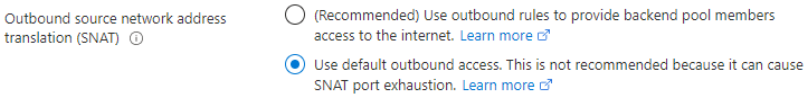
	The health probe of the cross-region load balancer gathers information about availability of each regional load balancer every 20 seconds. Azure cross-region load balancer uses a geo-proximity load-balancing algorithm for the routing decision. **Cross-region load balancer is a Layer-4 pass-through network load balancer. This pass-through preserves the original IP of the packet.** The original IP is available to the code running on the virtual machine. This preservation allows you to apply logic that is specific to an IP address. The backend pool of cross-region load balancer contains one or more regional load balancers.
Gateway Load Balancer (create gateway lb)	Gateway Load Balancer is a SKU of the Azure Load Balancer portfolio catered for high performance and high availability scenarios with third-party Network Virtual Appliances (NVAs). With the capabilities of Gateway Load Balancer, you can easily deploy, scale, and manage NVAs. Traffic moves from the consumer virtual network to the provider virtual network. The traffic then returns to the consumer virtual network. The consumer virtual network and provider virtual network can be in different subscriptions, tenants, or regions removing management overhead.

	
High availability ports overview	Azure Standard Load Balancer helps you load-balance all protocol flows on all ports simultaneously when you're using an internal load balancer via HA Ports. High availability (HA) ports are a type of load balancing rule that provides an easy way to load-balance all flows that arrive on all ports of an internal standard load balancer. The load-balancing decision is made per flow. This action is based on the following five-tuple connection: source IP address, source port, destination IP address, destination port, and protocol
Load Balancer TCP Reset and Idle Timeout (**set these options**)	Load Balancer's default behavior is to silently drop flows when the idle timeout of a flow is reached. Enabling TCP reset will cause Load Balancer to **send bidirectional TCP Resets (TCP RST packet) on idle timeout.** This will inform your application endpoints that the connection has timed out and is no longer usable. Endpoints can immediately establish a new connection if needed.

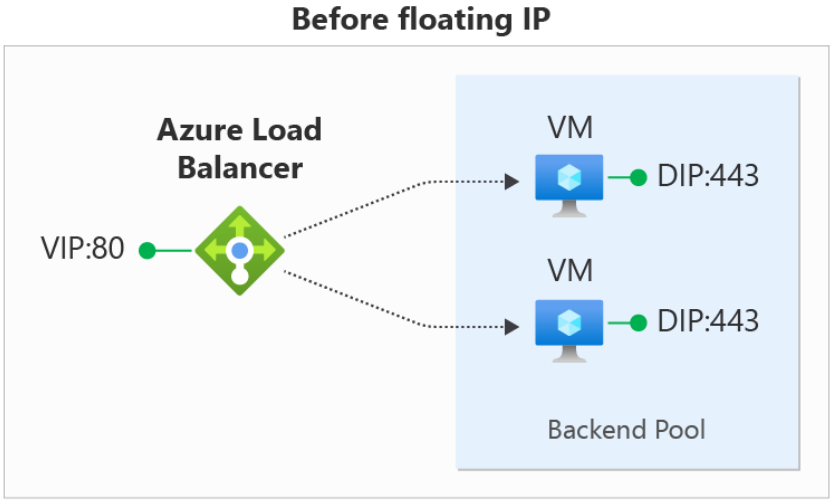
Azure's outbound connectivity methods

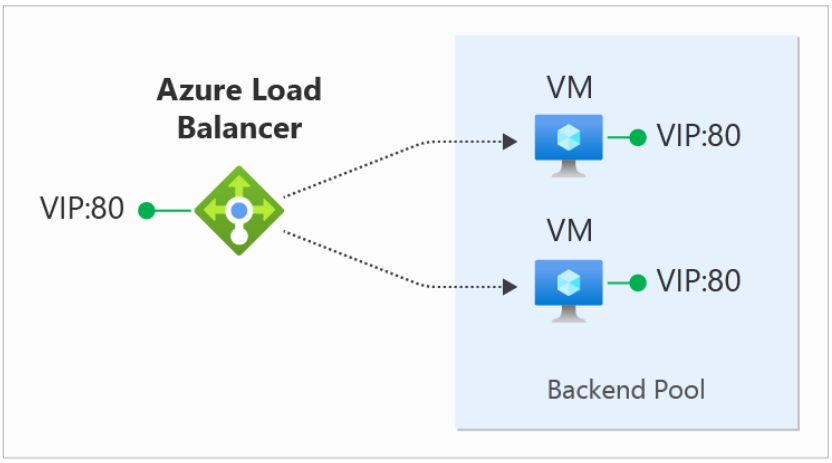
#	Method	Type of port allocation	Production-grade?	Rating
1	Use the frontend IP address(es) of a load balancer for outbound via outbound rules	Static, explicit	Yes, but not at scale	OK
2	Associate a NAT gateway to the subnet	Dynamic, explicit	Yes	Best
3	Assign a public IP to the virtual machine	Static, explicit	Yes	OK
4	Default outbound access use	Implicit	No	Worst

Create and use 1,3 and 4
4th option can be set from load balancing rules:



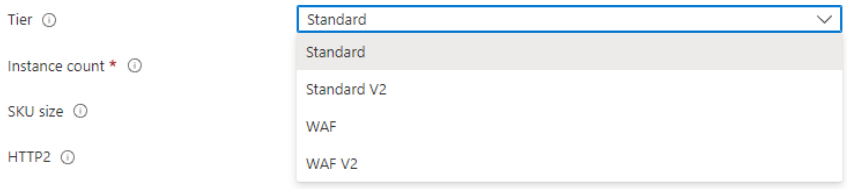
Floating IP (create floating IP config)	Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool. Common examples of port reuse include: • clustering for high availability • network virtual appliances • exposing multiple TLS endpoints without re-encryption. If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

	 Before floating IP Azure Load Balancer VIP:80 VM DIP:443 VM DIP:443 Backend Pool

	 To configure floating IP you need to add load balancer IP address in VM as a loopback IP. Need more diagrams and info

Azure Application Gateway

What is Azure Application Gateway Works at OSI layer 7 URL based / path based routing	Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

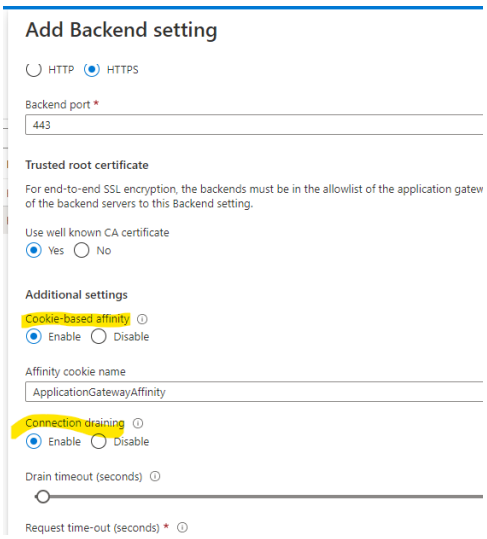
	Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. This type of routing is known as application layer (**OSI layer 7**) load balancing. Azure Application Gateway can do URL-based routing and more.
SKUs (**create standard, standard v2 and waf v2**) **Standard** **Standard V2** WAF WAF V2	Standard WAF Standard V2 WAF V2 
What is Azure Application Gateway v2? (use and compare features listed on right on standard and v2) **Auto scaling** **Zone redundancy** Static VIP mTLS Key vault integration Private link	The v2 SKU offers performance enhancements and adds support for critical new features like **autoscaling, zone redundancy, and support for static VIPs.** The new v2 SKU includes the following enhancements: • **Autoscaling:** • **Zone redundancy:** An Application Gateway or WAF deployment can span multiple Availability Zones, removing the need to provision separate Application Gateway instances in each zone with a Traffic Manager. • **Static VIP:** Application Gateway v2 SKU supports the static VIP type exclusively. This ensures that the VIP associated with the application gateway doesn't change for the lifecycle of the deployment, even after a restart. • **Header Rewrite:** Application Gateway allows you to add, remove, or update HTTP request and response headers with v2 SKU. • **Key Vault Integration for SSL:** • **Mutual Authentication (mTLS):** Application Gateway v2 supports authentication of client requests. • **Azure Kubernetes Service Ingress Controller:** • **Private link:** • **Performance enhancements:**.

	• **Faster deployment and update time**

Feature comparison between v1 SKU and v2 SKU

Feature	v1 SKU	v2 SKU
Autoscaling		✓
Zone redundancy		✓
Static VIP		✓
Azure Kubernetes Service (AKS) Ingress controller		✓
Azure Key Vault integration		✓
Rewrite HTTP(S) headers		✓
URL-based routing	✓	✓
Multiple-site hosting	✓	✓
Mutual Authentication (mTLS)		✓
Private Link support		✓
Traffic redirection	✓	✓
Web Application Firewall (WAF)	✓	✓
WAF custom rules		✓
WAF policy associations		✓
Transport Layer Security (TLS)/Secure Sockets Layer (SSL) termination	✓	✓
End-to-end TLS encryption	✓	✓
Session affinity	✓	✓
Custom error pages	✓	✓
WebSocket support	✓	✓
HTTP/2 support	✓	✓
Connection draining	✓	✓
Proxy NTLM authentication	✓	

Azure Application Gateway features (check and configure each of the options mentioned on left)	**Secure Sockets Layer (SSL/TLS) termination** **Autoscaling** **Zone redundancy:** A Standard_v2 Application Gateway can span multiple Availability Zones. Frontend IP can only be basic in standard LB. **Static VIP** **Web Application Firewall / Ingress Controller for AKS** **URL-based routing / Multiple-site hosting** **Redirection / Session affinity / Websocket and HTTP/2 traffic** **Connection draining / Custom error pages / Rewrite HTTP headers and URL**
Application gateway components (go to each of these components and play) ● **Frontend IP address** ● **Listeners (basic / multisite)** ● **HTTP settings** ● **Backend Pool** ● **Health Probes**	**Frontend IP addresses:** You can configure an application gateway to have a public IP address, a private IP address, or both. **Listeners:** There are two types of listeners: ● **Basic** ● **Multi-Site** **HTTP settings** An application gateway routes traffic to the backend servers (specified in the request routing rule that include HTTP settings) by using the port number, protocol, and other settings detailed in this component. The port and protocol used in the HTTP settings determine whether the traffic between the application gateway and backend servers is encrypted (providing end-to-end TLS) or unencrypted. This component is also used to: ● Determine whether a user session is to be kept on the same server by using the **cookie-based session affinity**. ● Gracefully remove backend pool members by using **connection draining**. ● Associate **a custom probe** to monitor the backend health, set the request timeout interval, override hostname and path in the request, and provide one-click ease to specify settings for the App Service backend.



Backend pools

A backend pool routes requests to backend servers, which serve the request. Backend pools can contain:

- NICs
- Virtual machine scale sets
- Public IP addresses
- Internal IP addresses
- FQDN
- Multitenant backends (such as App Service)

Health probes

Virtual network and dedicated subnet	An application gateway is a dedicated deployment in your virtual network. **Within your virtual network, a dedicated subnet is required** for the application gateway. You can have multiple instances of a given application gateway deployment in a subnet. You can also deploy other application gateways in the subnet. But you can't deploy any other resource in the application gateway subnet.
TLS termination PFX format End-to-end TLS encryption **(setup end-to-end TLS encryption)**	Application Gateway supports TLS termination at the gateway, after which traffic typically flows unencrypted to the backend servers. **The certificate provided to the Application Gateway must be in Personal Information Exchange (PFX) format, which contains both the private and public keys.** When configured with end-to-end TLS communication mode, Application Gateway terminates the TLS sessions at the gateway and decrypts user traffic. It then applies the configured rules to select an appropriate backend pool instance to route traffic to. Application Gateway then initiates a new TLS connection to the backend server and re-encrypts data using the backend server's public key certificate before transmitting the request to the backend. Any response from the web server goes through the same process back to the end user. End-to-end TLS is enabled by setting protocol settings in Backend HTTP Setting to HTTPS, which is then applied to a backend pool.
Diagnostic logs (enable all logs mentioned and check/simulate their entries) • **Activity Log** • **Access log** • **Performance log** • **Firewall log**	• **Activity log:** You can use Azure activity logs (formerly known as operational logs and audit logs) to view all operations that are submitted to your Azure subscription, and their status. Activity log entries are collected by default, and you can view them in the Azure portal. • **Access log:** You can use this log to view Application Gateway access patterns and analyze important information. This includes the caller's IP, requested URL, response latency, return code, and bytes in and out. • **Performance log:** You can use this log to view how Application Gateway instances are performing. This log captures performance information for each instance, including total requests served, throughput in bytes, total requests served, failed request count, and healthy and unhealthy backend instance count. A performance log is collected every 60 seconds. The Performance log is available only for the v1 SKU. For the v2 SKU, use Metrics for performance data. • **Firewall log:** You can use this log to view the requests that are logged through either detection or prevention mode of an application gateway that is configured with the web application firewall. Firewall logs are collected every 60 seconds.
Metrics for Application Gateway (check and analyze these metrics)	**Timing metrics**

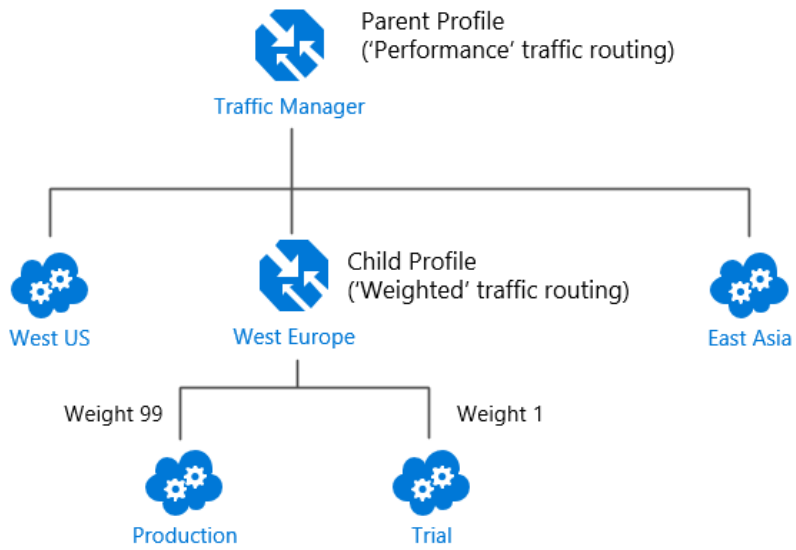
	• **Backend connect time** • **Backend first byte response time** • **Backend last byte response time** • **Application gateway total time** • **Client RTT** **Application Gateway metrics** • **Bytes received** Count of bytes received by the Application Gateway from the clients • **Bytes sent** Count of bytes sent by the Application Gateway to the clients • **Client TLS protocol** Count of TLS and non-TLS requests initiated by the client that established connection with the Application Gateway. To view TLS protocol distribution, filter by the dimension TLS Protocol. • **Current capacity units** Count of capacity units consumed to load balance the traffic. There are three determinants to capacity unit - compute unit, persistent connections and throughput. Each capacity unit is composed of at most: 1 compute unit, or 2500 persistent connections, or 2.22-Mbps throughput. • **Current compute units** Count of processor capacity consumed. Factors affecting compute unit are TLS connections/sec, URL Rewrite computations, and WAF rule processing. • **Current connections** The total number of concurrent connections active from clients to the Application Gateway • **Estimated Billed Capacity units** With the v2 SKU, the pricing model is driven by consumption. Capacity units measure consumption-based cost that is charged in addition to the fixed cost. *Estimated Billed Capacity units* indicate the number of capacity units using which the billing is estimated. This is calculated as the greater value between *Current capacity units* (capacity units required to load balance the traffic) and *Fixed billable capacity units* (minimum capacity units kept provisioned). • **Failed Requests** Number of requests that Application Gateway has served with 5xx server error codes. • **Fixed Billable Capacity Units** The minimum number of capacity units kept provisioned as per the *Minimum scale units* setting (one instance translates to 10 capacity units) in the Application Gateway configuration. • **New connections per second** The average number of new TCP connections per second established from clients to the Application Gateway and from the Application Gateway to the backend members.

	• **Response Status** HTTP response status returned by Application Gateway. The response status code distribution can be further categorized to show responses in 2xx, 3xx, 4xx, and 5xx categories. • **Throughput** Number of bytes per second the Application Gateway has served • **Total Requests** **Backend metrics** For Application Gateway, the following metrics are available: • **Backend response status** • **Healthy host count** • **Unhealthy host count** • **Requests per minute per Healthy Host**

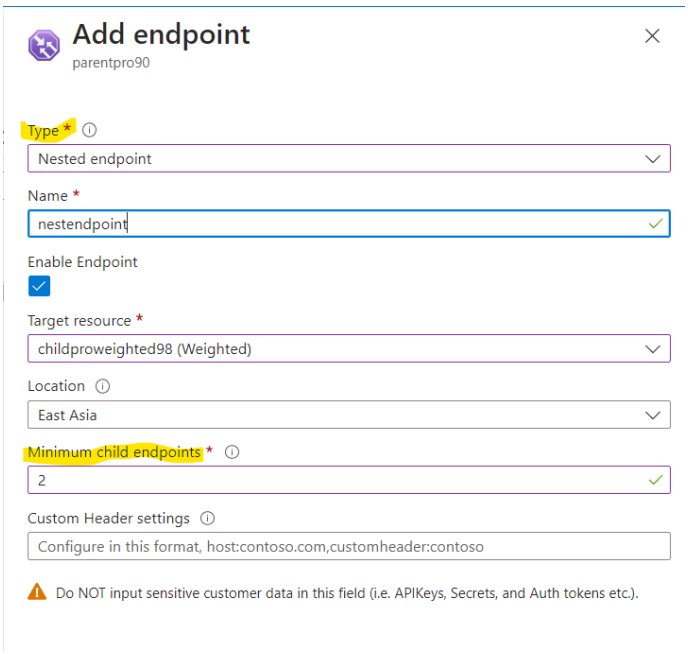
Traffic Manager

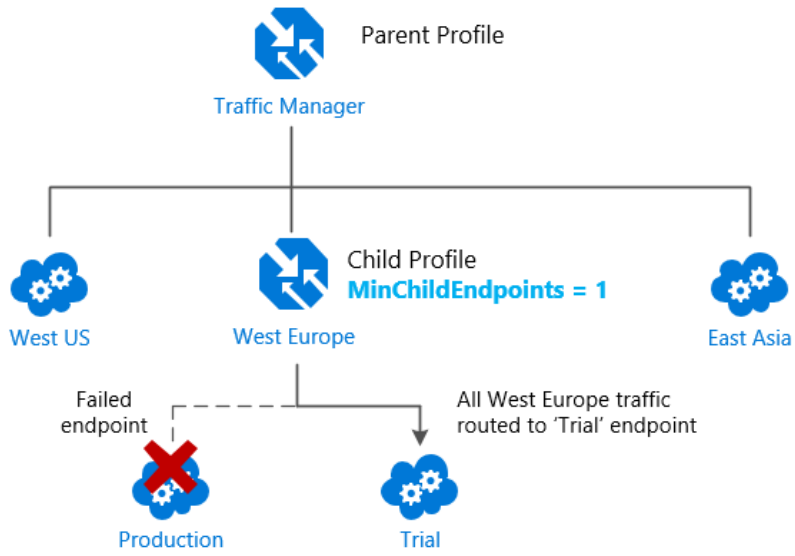
What is a Traffic Manager	Azure Traffic Manager is a **DNS-based traffic load balancer**. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.
Traffic Manager routing methods (create traffic manager profile by using one of the methods) 1. **Priority** 2. **Weighted** 3. **Performance** 4. **Geographic**	The following traffic routing methods are available in Traffic Manager: • **Priority**: Select Priority routing when you want to **have a primary service endpoint for all traffic.** You can provide multiple backup endpoints in case the primary or one of the backup endpoints is unavailable.

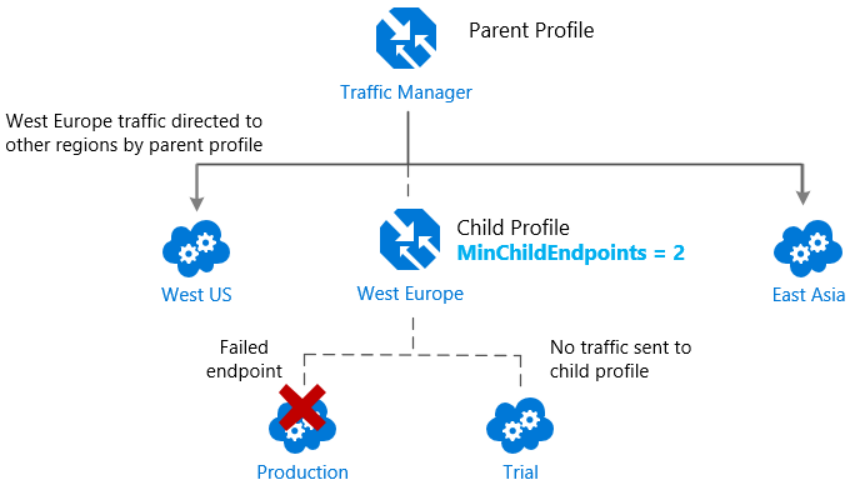
5. **Multivalue** 6. **Subnet (get more info)**	• **Weighted**: Select Weighted routing when **you want to distribute traffic across a set of endpoints** based on their weight. Set the weight the same to distribute evenly across all endpoints. • **Performance**: Select Performance routing when you have endpoints in different geographic locations and **you want end users to use the "closest" endpoint** for the lowest network latency. • **Geographic**: Select Geographic routing to direct users to specific endpoints (Azure, External, or Nested) **based on where their DNS queries originate from geographically.** With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions. • **Multivalue**: Select MultiValue for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, **all healthy endpoints are returned.** • **Subnet**: Select Subnet traffic-routing method to map sets of **end-user IP address ranges to a specific endpoint**. When a request is received, the endpoint returned will be the one mapped for that request's source IP address.
Nested Traffic Manager profiles **(create one nested traffic profile)**	Traffic Manager includes a range of traffic-routing methods that allow you to control how Traffic Manager chooses which endpoint should receive traffic from each end user. **You can nest Traffic Manager profiles to combine the benefits of more than one traffic-routing method.** ## Example 1: Combining 'Performance' and 'Weighted' traffic routing The following diagram illustrates this example:



Nested endpoint and minimum child endpoint.

	
Example 2: Endpoint monitoring in Nested Profiles **(make one of the endpoints fail)**	Traffic Manager actively monitors the health of each service endpoint. If an endpoint is unhealthy, Traffic Manager directs users to alternative endpoints to preserve the availability of your service. This endpoint monitoring and failover behavior applies to all traffic-routing methods. Endpoint monitoring works differently for nested profiles. With nested profiles, the parent profile doesn't perform health checks on the child directly. Instead, the health of the child profile's endpoints is used to calculate the overall health of the child profile. This health information is propagated up the nested profile hierarchy. The parent profile uses this aggregated health to determine whether to direct traffic to the child profile. Returning to the previous example, suppose the production deployment in West Europe fails. By default, the 'child' profile directs all traffic to the test deployment. If the test

	deployment also fails, the parent profile determines that the child profile should not receive traffic since all child endpoints are unhealthy. Then, the parent profile distributes traffic to the other regions.  You might be happy with this arrangement. Or you might be concerned that all traffic for West Europe is now going to the test deployment instead of a limited subset traffic. Regardless of the health of the test deployment, you want to fail over to the other regions when the production deployment in West Europe fails. In the scenario below, the **MinChildEndpoints value is set to 2**. Below this threshold, the parent profile considers the entire child profile to be unavailable and directs traffic to the other endpoints:

	
Traffic Manager endpoints	There are three types of endpoint supported by Traffic Manager: • **Azure endpoints** are used for services hosted in Azure. • **External endpoints** are used for IPv4/IPv6 addresses, FQDNs, or for services hosted outside Azure. Theses services can either be on-premises or with a different hosting provider. • **Nested endpoints** are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

Azure Front Door

<table>
<tr>
<td>What is Azure Front Door?</td>
<td>
A secure, modern cloud CDN provides a distributed platform of servers. This helps minimize latency when users are accessing webpages. Historically, IT staff might have used a CDN and a web-application firewall to control HTTP and HTTPS traffic flowing to and from target applications.

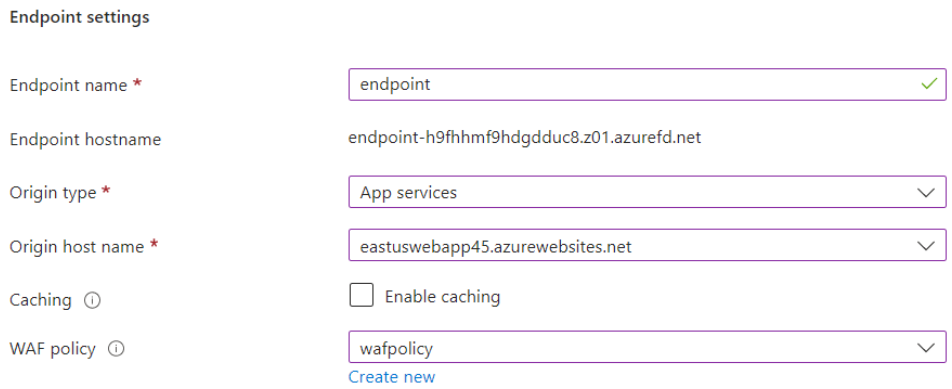
If an organization uses Azure, they might achieve these goals by implementing the products described in the following table:

<table>
<tr><th>Product</th><th>Description</th></tr>
<tr><td>Azure Front Door</td><td>Enables an entry point to your apps positioned in the Microsoft global edge network. Provides faster, more secure, and scalable access to your web applications.</td></tr>
<tr><td>Azure Content Delivery Network</td><td>Delivers high-bandwidth content to your users by caching their content at strategically placed physical nodes around the world.</td></tr>
<tr><td>Azure Web Application Firewall</td><td>Helps provide centralized, greater protection for web applications from common exploits and vulnerabilities.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Azure Front Door definition</td>
<td>
Azure Front Door Standard/Premium provides the capabilities of these three products (Azure Front Door Classic, Azure CDN). It offers a fast, reliable, and more secure modern cloud CDN by using the Microsoft global edge network to integrate with intelligent threat protection. Azure Front Door resides in the edge locations and manages user requests to your hosted applications. Users connect to your application through the Microsoft global network. Azure Front Door then routes user requests to the fastest and most available application backend.

The following Azure Front door SKUs are available:

Azure Front Door, which is the entry level. Existing Azure customers often bolster these features with Azure Content Delivery Network, and Azure Web Application Firewall.
Azure Front Door Standard, which is optimized for virtually seamless content delivery.

</td>
</tr>
</table>

	• **Azure Front Door Premium**, which is optimized for improved security.
Azure Front Door Standard **(create Azure Front Door standard)**	Azure Front Door Standard provides the capabilities of Azure Front Door (Classic), Azure Content Delivery Network, and Azure Web Application Firewall. Azure Front Door Standard includes: • Content-delivery optimization • Static and dynamic content acceleration • Global load balancing • Secure Sockets Layer (SSL) offload • Domain and certificate management • Enhanced traffic analytics • Basic security capabilities
Azure Front Door Standard **(Quick create)** Define one endpoint with one origin and one WAF policy to get your Front Door up and running quickly.	 **Route:** A route maps your domains and matching URL path patterns to a specific origin group. **Origin group:** An origin group is a set of origins to which Front Door load balances your client requests.

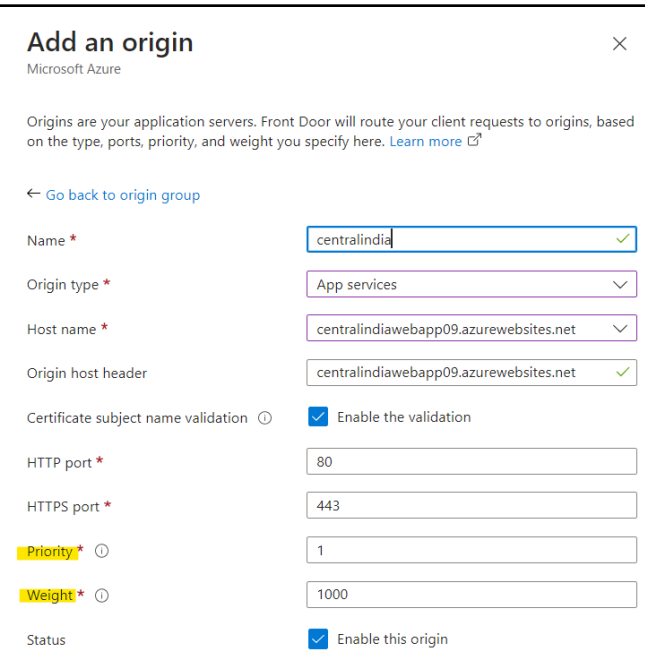
<table>
<tr>
<td>Azure Front Door Premium

(create front door premium)</td>
<td>Azure Front Door Premium provides the same capabilities as Azure Front Door Standard. However, it's security optimized and includes the following additional features:

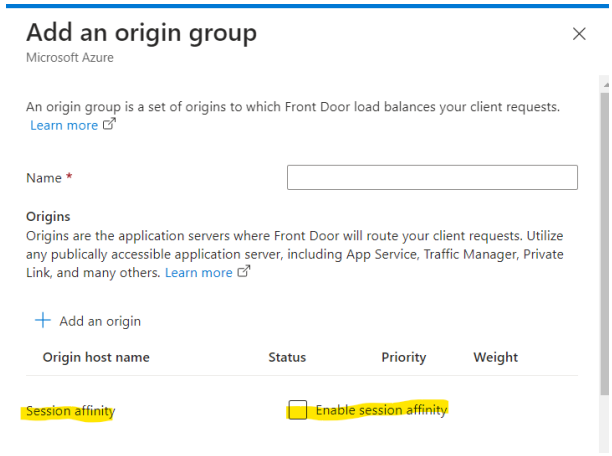
• Extensive security capabilities across Web Application Firewall
• Private link support
• Integration with Microsoft Threat Intelligence and security analytics</td>
</tr>
<tr>
<td>How Azure Front Door optimizes content delivery
(use the routing methods described)</td>
<td>Azure Front Door uses the anycast protocol with split TCP at layer 7 to route HTTP/S client requests to the most available and fastest application backend. The way Azure Front Door routes requests depends on the routing method you select, and on backend health. Azure Front Door supports four routing methods, as the following table describes:

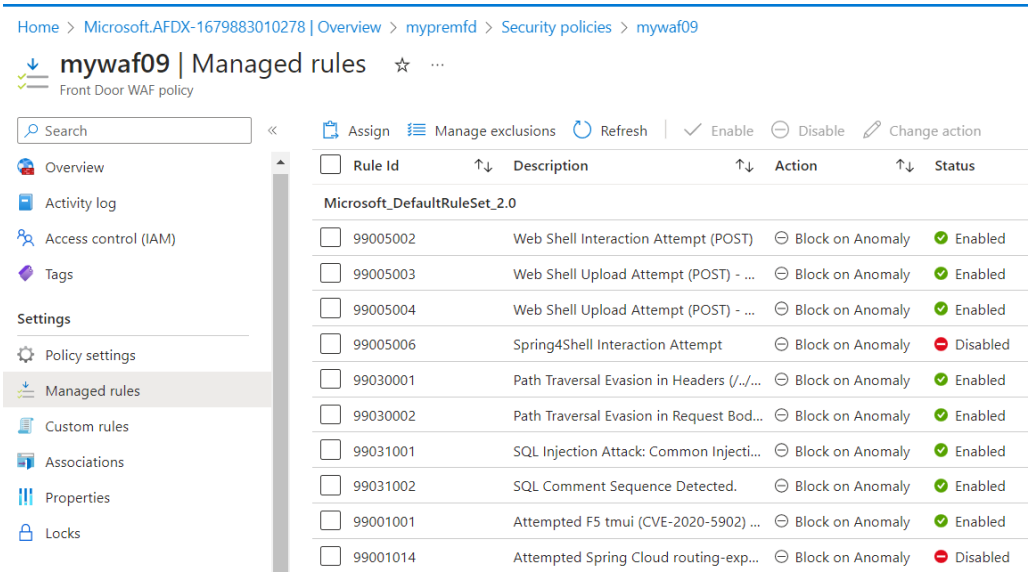
<table>
<tr><th>Routing method</th><th>Description</th></tr>
<tr><td>Latency</td><td>Helps ensure requests are sent to the lowest latency backends, within an acceptable sensitivity range.</td></tr>
<tr><td>Priority</td><td>Uses administrator-assigned priorities to your backends when you want to configure a primary backend to service all traffic.</td></tr>
<tr><td>Weighted</td><td>Uses administrator-assigned weights to your backends when you want to distribute traffic across a set of backends.</td></tr>
<tr><td>Session Affinity</td><td>Allows you to configure session affinity for your frontend hosts or domains. This helps ensure requests from the same end user are sent to the same backend.</td></tr>
</table>

Priority and Weight can be configured during creating origin:</td>
</tr>
</table>



You can enable session affinity white creating origin group:



How Azure Front Door helps secure content (**configure WAF**)	Azure Front Door provides web-application firewall capabilities to help protect your web applications from exploits and vulnerabilities. Managing security for your applications can be challenging because web applications are increasingly targeted. Azure Front Door operates at the network's edge, close to potential attacks. This helps prevent attacks before they can enter your network. Azure Front Door's web application firewall is based on policies you can associate with one or more instances of Azure Front Door. These firewall policies consist of: • *Managed rule sets*, which are a collection of preconfigured rules • Custom rules that you can configure 
When to use Azure Front Door	It's also important to consider several other Azure products you could use instead of Azure Front Door, including: • Azure Traffic Manager, which provides DNS-based global routing. However, it doesn't provide for Transport Layer Security (TLS) protocol termination, or *SSL offload*, per-HTTP/HTTPS request, or application-layer processing.

- Azure Application Gateway, which can load-balance between your servers in a region at the application layer.

The decision you make depends on whether you require the other features that Azure Front Door Standard and Azure Front Door Premium offer.

Criteria	Analysis
Scalability	Does your organization scale out content? Organizations that host scalable content will benefit more from using Azure Front Door.
Pricing	Does your organization prefer a monthly charge for each policy or hourly billing? Do you want to pay extra charges for custom rules? Review the pricing considerations in the *Pricing* section later in this unit.
Content delivery	Do you require content optimization, without extensive security capabilities? Azure Front Door Standard is a good choice in this case.
Security	Do you have enhanced security requirements? Azure Front Door Premium is your best option.

Scalability

Organizations that don't host global, scalable web applications might not benefit from implementing Azure Front Door. However, if it builds, operates, and scales out dynamic web applications and static content, it can benefit from the use of the different Azure Front Door tiers.

Consider using Azure Front Door when you want to:

- Define, manage, and monitor your web traffic's global routing.
- Optimize for top-tier, end-user performance and reliability through quick global failover.

Content delivery

Consider using Azure Front Door Standard when you want to:

- **Optimize your content delivery.**
- **Provide for both static and dynamic content acceleration.**

	• **Support global load balancing.** • **Implement SSL offload.** • **Implement domain and certificate management.** • **Benefit from enhanced traffic analytics.** • **Benefit from basic security capabilities.** **Security** Consider using Azure Front Door Premium when you need Azure Front Door Standard features and require: • Extensive security capabilities across Web Application Firewall. • BOT protection. • Private Link support. • Integration with Microsoft Threat Intelligence and security analytics.

Azure Firewall

What is Azure Firewall	Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability.

Azure Firewall Standard

(create and use azure firewall standard)

Azure Firewall Standard features:

Built-in high availability:

Availability Zones:
Azure Firewall can be configured during deployment to span multiple Availability Zones for increased availability.

Application FQDN filtering rules
You can limit outbound HTTP/S traffic or Azure SQL traffic to a specified list of fully qualified domain names (FQDN) including wild cards.

Network traffic filtering rules
You can centrally create allow or deny network filtering rules by source and destination IP address, port, and protocol. Azure Firewall is fully stateful, so it can distinguish legitimate packets for different types of connections.

FQDN tags
FQDN tags make it easy for you to allow well-known Azure service network traffic through your firewall. For example, say you want to allow Windows Update network traffic through your firewall. You create an application rule and include the Windows Update tag. Now network traffic from Windows Update can flow through your firewall.

Service tags
A service tag represents a group of IP address prefixes to help minimize complexity for security rule creation.

Threat intelligence
Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.

DNS proxy

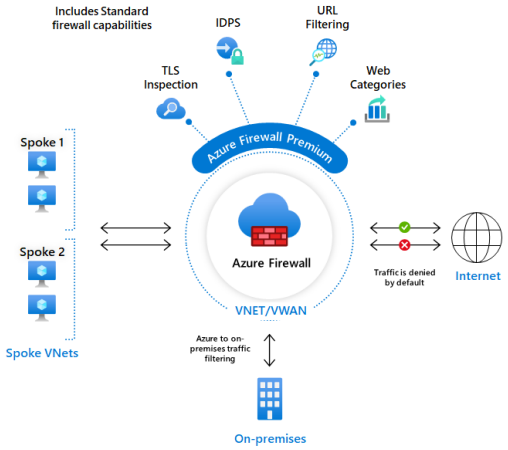
Custom DNS

Outbound SNAT support
All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP (Source Network Address Translation).

Inbound DNAT support

Multiple public IP addresses
You can associate multiple public IP addresses (up to 250) with your firewall.

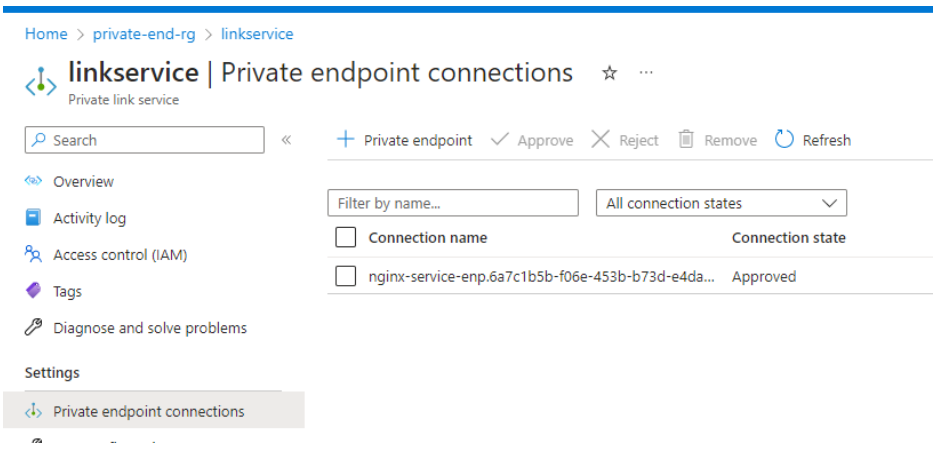
Web categories
Web categories let administrators allow or deny user access to web site categories such as gambling websites, social media websites, and others. Web categories are included in Azure Firewall Standard, but it's more fine-tuned in Azure Firewall Premium.

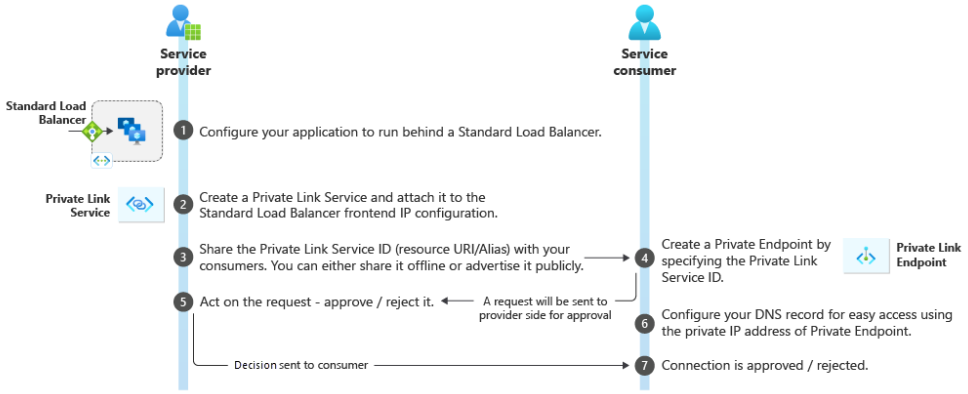
Azure Firewall Premium 	Azure Firewall Premium features Azure Firewall Premium includes the following features: • **TLS inspection** - decrypts outbound traffic, processes the data, then encrypts the data and sends it to the destination. • **IDPS - A network intrusion detection and prevention system (IDPS)** allows you to monitor network activities for malicious activity, log information about this activity, report it, and optionally attempt to block it. • URL filtering - extends Azure Firewall's FQDN filtering capability **to consider an entire URL along with any additional path.** For example, `www.contoso.com/a/c` instead of `www.contoso.com`. • **Web categories** - administrators can allow or deny user access to website categories such as gambling websites, social media websites, and others.

Private Link

Azure Private Link	Azure Private Link enables you to access Azure PaaS Services (for example, Azure Storage and SQL Database) and Azure hosted customer-owned/partner services over a private endpoint in your virtual network. **Key benefits:** • **Privately access services on the Azure platform:**

	• **On-premises and peered networks:** Access services running in Azure from on-premises over ExpressRoute private peering, VPN tunnels, and peered virtual networks using private endpoints. • **Protection against data leakage:** • **Global reach:** • **Extend to your own services:** Enable the same experience and functionality to render your service privately to consumers in Azure. By placing your service behind a standard Azure Load Balancer, you can enable it for Private Link. The consumer can then connect directly to your service using a private endpoint in their own virtual network. You can manage the connection requests using an approval call flow. Azure Private Link works for consumers and services belonging to different Azure Active Directory tenants.
Private endpoint **(check network policies and ASG with private endpoint)**	A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network. • The private endpoint must be deployed in the same region and subscription as the virtual network. • The private-link resource can be deployed in a different region than the one for the virtual network and private endpoint. **Private endpoints support network policies. Network policies enable support for Network Security Groups (NSG), User Defined Routes (UDR), and Application Security Groups (ASG).** For more information about enabling network policies for a private endpoint, see Manage network policies for private endpoints. To use an ASG with a private endpoint, see Configure an application security group (ASG) with a private endpoint.
Access to a private-link resource using approval workflow	• **Automatically approve:** • **Manually request:**

	
DNS configuration	The DNS settings that you use to connect to a private-link resource are important. Existing Azure services might already have a DNS configuration you can use when you're connecting over a public endpoint. To connect to the same service over private endpoint, separate DNS settings, often configured via private DNS zones, are required. Ensure that your DNS settings are correct when you use the fully qualified domain name (FQDN) for the connection. The settings must resolve to the private IP address of the private endpoint.
Azure Private Link service (create a private link service)	Azure Private Link service is the reference to your own service that is powered by Azure Private Link. Your service that is running behind Azure Standard Load Balancer can be enabled for Private Link access so that consumers to your service can access it privately from their own VNets. Your customers can create a private endpoint inside their virtual network and map it to this service. Workflow



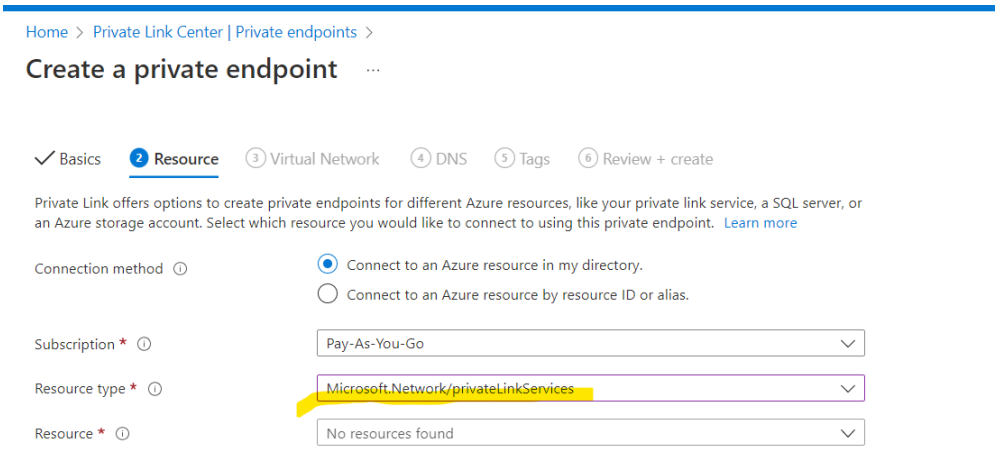
Alias

Alias is a globally unique name for your service. It helps you mask the customer data for your service and at the same time creates an easy-to-share name for your service. When you create a Private Link service, Azure generates an alias for your service that you can share with your customers. Your customers can use this alias to request a connection to your service.

Control service exposure

The Private Link service provides you with three options in the Visibility setting to control the exposure of your service. Your visibility setting determines whether a consumer can connect to your service. Here are the visibility setting options, from most restrictive to least restrictive:

- **Role-based access control only:** If your service is for private consumption from different virtual networks that you own, use role-based access control inside subscriptions that are associated with the same Active Directory tenant. Cross tenant visibility is permitted through role-based access control.

	• **Restricted by subscription:** If your service will be consumed across different tenants, you can restrict the exposure to a limited set of subscriptions that you trust. Authorizations can be pre-approved. • **Anyone with your alias:** If you want to make your service public and allow anyone with your Private Link service alias to request a connection, select this option. 
Azure services DNS zone configuration **(confirm the CNAME created)**	Azure creates a canonical name DNS record (CNAME) on the public DNS. The CNAME record redirects the resolution to the private domain name. You can override the resolution with the private IP address of your private endpoints. Your applications don't need to change the connection URL. When resolving to a public DNS service, the DNS server will resolve to your private endpoints. The process doesn't affect your existing applications.

Azure Virtual WAN

<table>
<tr><td>Azure Virtual WAN
(create virtual WAN)</td><td>Azure Virtual WAN is a hub-and-spoke architecture. The Virtual WAN is a Microsoft-managed, Azure-based networking service.

Microsoft hosts and manages all the components that make up this service. It's easy to deploy and use, while offering the following services:

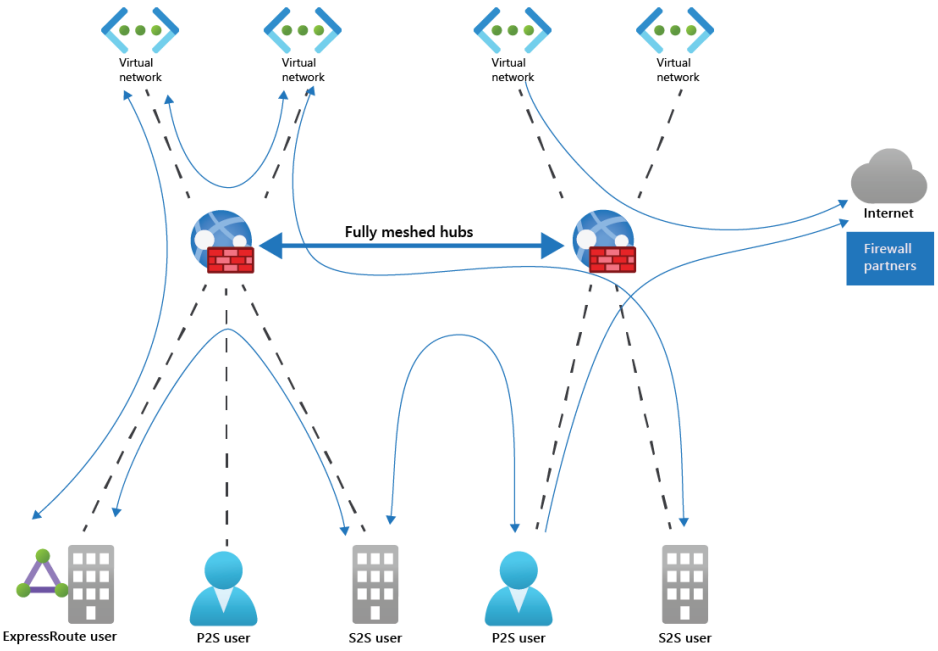
● Enables any-to-any connectivity to workloads distributed globally in virtual networks.
● Connects:
○ Working at home and mobile users using point-to-site VPN
○ Branch offices using site-to-site VPN
○ Main campuses and datacenters using ExpressRoute for private connections</td></tr>
<tr><td>Virtual WAN options</td><td><table><tr><th>Virtual WAN type</th><th>Hub type</th><th>Available configurations</th></tr><tr><td>Basic</td><td>Basic</td><td>Site-to-site VPN only</td></tr><tr><td>Standard</td><td>Standard</td><td>Full-mesh connectivity, ExpressRoute, User VPN (P2S), VPN (site-to-site), Inter-hub, Virtual Network-to-Virtual Network transiting through the virtual hub</td></tr></table></td></tr>
<tr><td>Azure Virtual WAN hubs
(create virtual WAN hub and connect two networks via same)</td><td>The classic hardware hub allows all network devices plugged into it to communicate directly with each other. A Virtual WAN hub is a sophisticated software-defined hub.

You can deploy an Azure Virtual WAN hub in any Azure region. Each hub can be connected to use standard Azure connection services.

For example, a branch office in an Azure region in the UK can connect to a region in the USA. They connect using hub-to-hub connectivity through the Azure global network.

In a single virtual WAN that spans multiple regions with multiple hubs deployed, the hubs are automatically interconnected by hub-to-hub links. These interconnections enable global connectivity to branches and virtual networks.

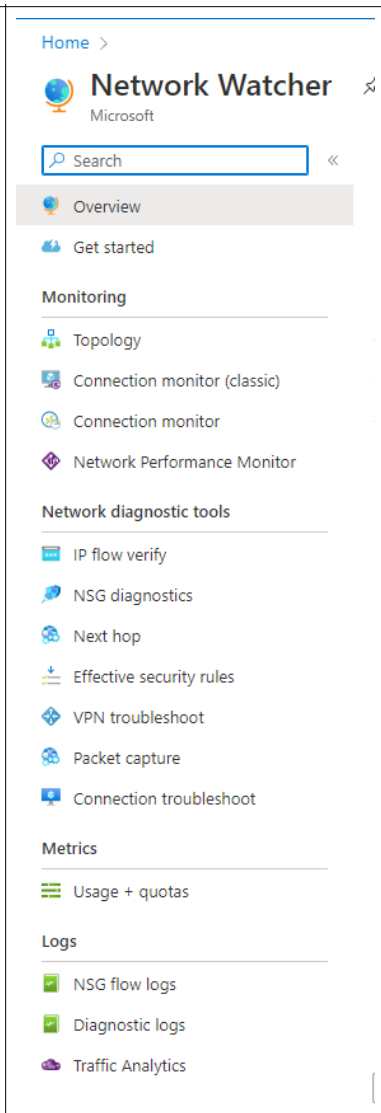
The following image depicts an Azure Virtual WAN deployment with two Virtual hubs in different Azure regions and the network traffic flow.</td></tr>
</table>

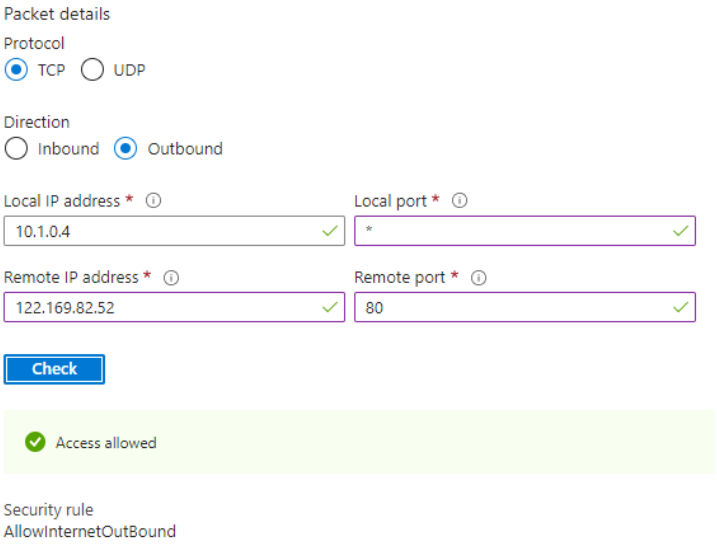
	
Secure virtual hub	To convert the virtual hub to a secure virtual hub, use Azure Firewall Manager. Firewall rules, created by the Firewall Manager, allow for the creation of security and routing policies for network traffic. Data flowing from the internet, private IP addresses, or Azure platform services can be filtered. The secure virtual hub supports the provisioning of two security providers: • Azure Firewall for private traffic • Third-party security providers that are integrated with Firewall Manager

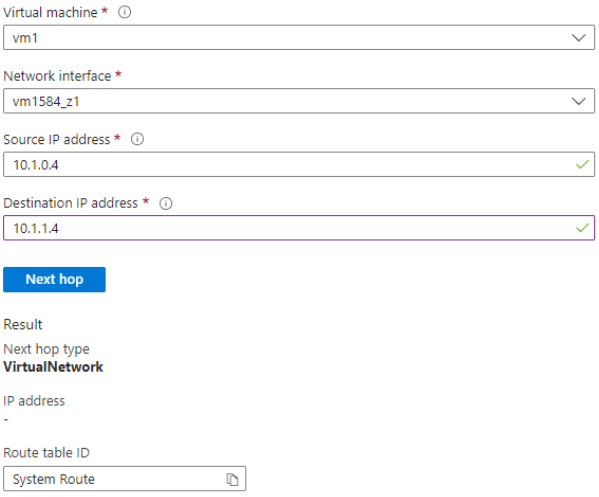
	Virtual hubs or secure virtual hubs are the regional connection points for a virtual WAN. These hubs support multiple service endpoints. The endpoints provide connectivity between networks and services. They're the core of networking for each region.
Service components of Azure Virtual WAN	- The virtual hub: All traffic flows through these fully meshed hubs. An address space and routing tables are provided at creation. - Hub-to-Hub connections: Enable cross-region connectivity between all on-premises and Azure network endpoints. - Virtual hub router: Supports custom route tables for virtual networks. Acts as default route table for branches (P2S, S2S, ER). Associates connections to route tables and propagates routes from connections to route tables. - Connection between sites: Supports: - Any-to-any branch to Azure - Branch to branch - Users to branch - Virtual network to virtual network transit - VPN to ExpressRoute transit connectivity. - Secure virtual hub: Added security with the integration of Azure Firewall Manager to: - Create policy and apply across multiple firewalls - Work across regions/subscription/deployments - Secure internet traffic (virtual network to internet and branch to internet) - Secure private traffic (virtual network to and from a branch) - Secure with Security-as-a-Service (SECaaS) partners: Supported partners that currently have integration into Azure Firewall Manager's API to set up security policies are: - zScaler - iBoss - Check Point

Azure Network Watcher

Azure Network Watcher **Verify IP Flow** **Next Hop** **Connection Troubleshoot** **Effective security rules** **NSG Flow Logs** **Connection Monitor** **Network Topology** **Packet Capture** **VPN Diagnostics**	Azure Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end-to-end network level view. Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your network in Azure. Network Watcher is enabled through the creation of a Network Watcher resource, which allows you to utilize Network Watcher capabilities.

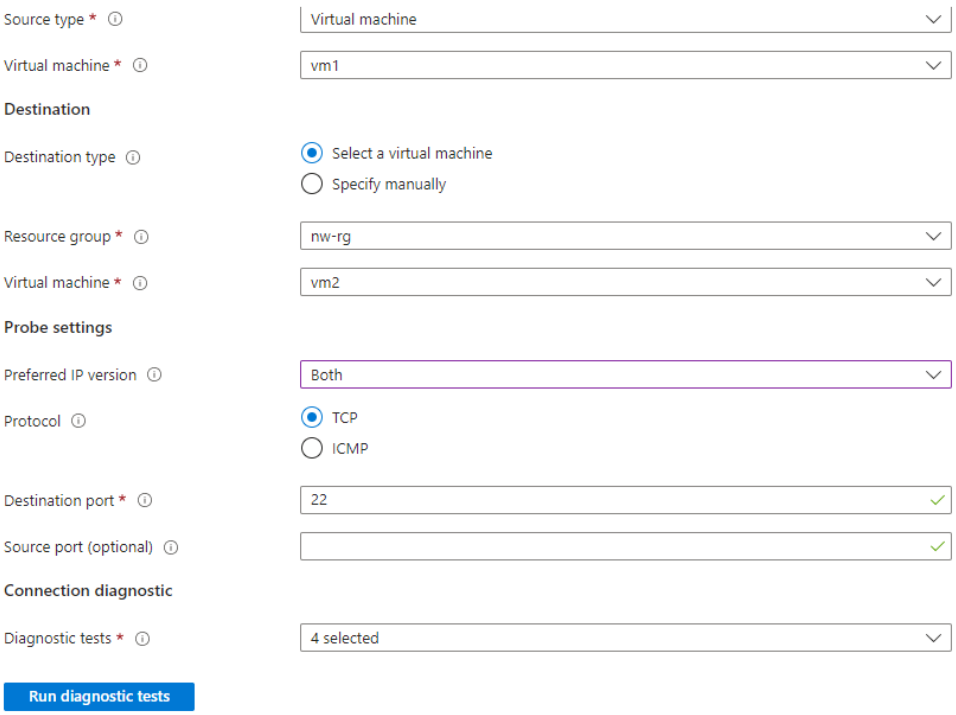

Home
Network Watcher
Microsoft
Search
Overview
Get started
Monitoring
Topology
Connection monitor (classic)
Connection monitor
Network Performance Monitor
Network diagnostic tools
IP flow verify
NSG diagnostics
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Usage + quotas
Logs
NSG flow logs
Diagnostic logs
Traffic Analytics

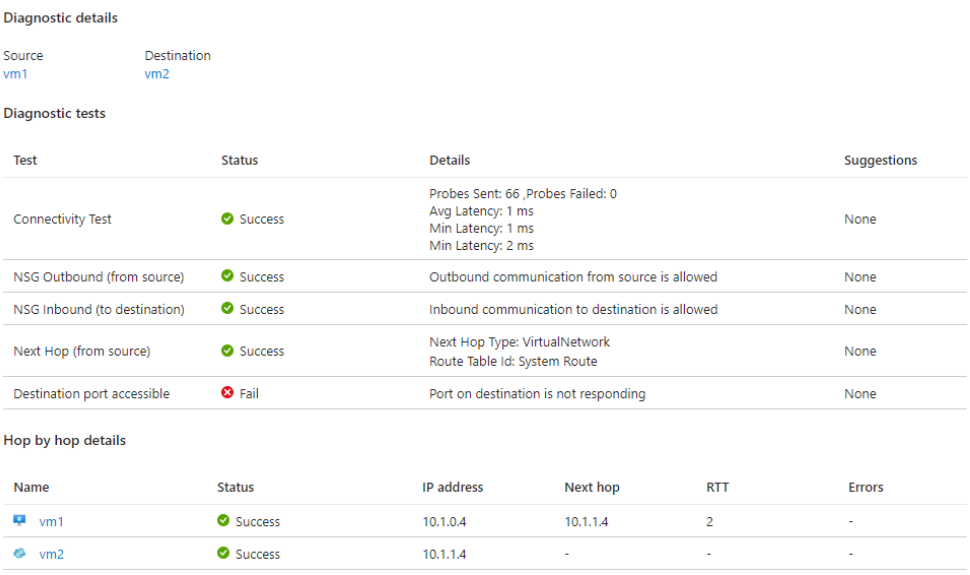
Network Topology **(use and test the feature)**	The topology capability enables you to generate a visual diagram of the resources in a virtual network, and the relationships between the resources.
Verify IP Flow **(use and test the feature)** Check NSG rule	Quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment. For example, confirming if a security rule is blocking **ingress or egress traffic to or from a virtual machine.** IP flow verify is ideal for making sure **security rules are being correctly applied.** When used for troubleshooting, if IP flow verify doesn't show a problem, you will need to explore other areas such as firewall restrictions. 
Next Hop **(use and test the feature)**	To determine if traffic is being directed to the intended destination by showing the next hop. This will help determine if networking **routing is correctly configured.** Next hop also returns the route table associated with the next hop. If the route is defined as a user-defined route, that route is returned. Otherwise, next hop returns System Route.

	
Effective security rules: **(use and test the feature)**	Network Security groups are associated at a subnet level or at a NIC level. When associated at a subnet level, it applies to all the VM instances in the subnet. Effective security rules view returns all the configured NSGs and rules that are associated at a NIC and subnet level for a virtual machine providing insight into the configuration. In addition, the effective security rules are returned for each of the NICs in a VM. Using Effective security rules view, you can assess a VM for network vulnerabilities such as open ports.
VPN Diagnostics (use and test the feature)	Troubleshoot gateways and connections. VPN Diagnostics returns a wealth of information. Summary information is available in the portal and more detailed information is provided in log files. The log files are stored in a storage account and include things like connection statistics, CPU and memory information, IKE security errors, packet drops, and buffers and events.
Packet Capture **(use and test the feature)**	Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactively. Other uses include gathering network statistics, gaining information on network intrusions, to debug client-server communications and much more.

Connection Troubleshoot
(use and test the feature)
Combines IP flow verify and next hop

Azure Network Watcher Connection Troubleshoot is a more recent addition to the Network Watcher suite of networking tools and capabilities. Connection Troubleshoot enables you to troubleshoot network performance and connectivity issues in Azure.





NSG Flow Logs
(use and test the feature)

NSG Flow Logs maps IP traffic through a network security group. These capabilities can be used in security compliance and auditing. You can define a prescriptive set of security rules as a model for security governance in your organization. A periodic compliance audit can be implemented in a programmatic way by comparing the prescriptive rules with the effective rules for each of the VMs in your network.

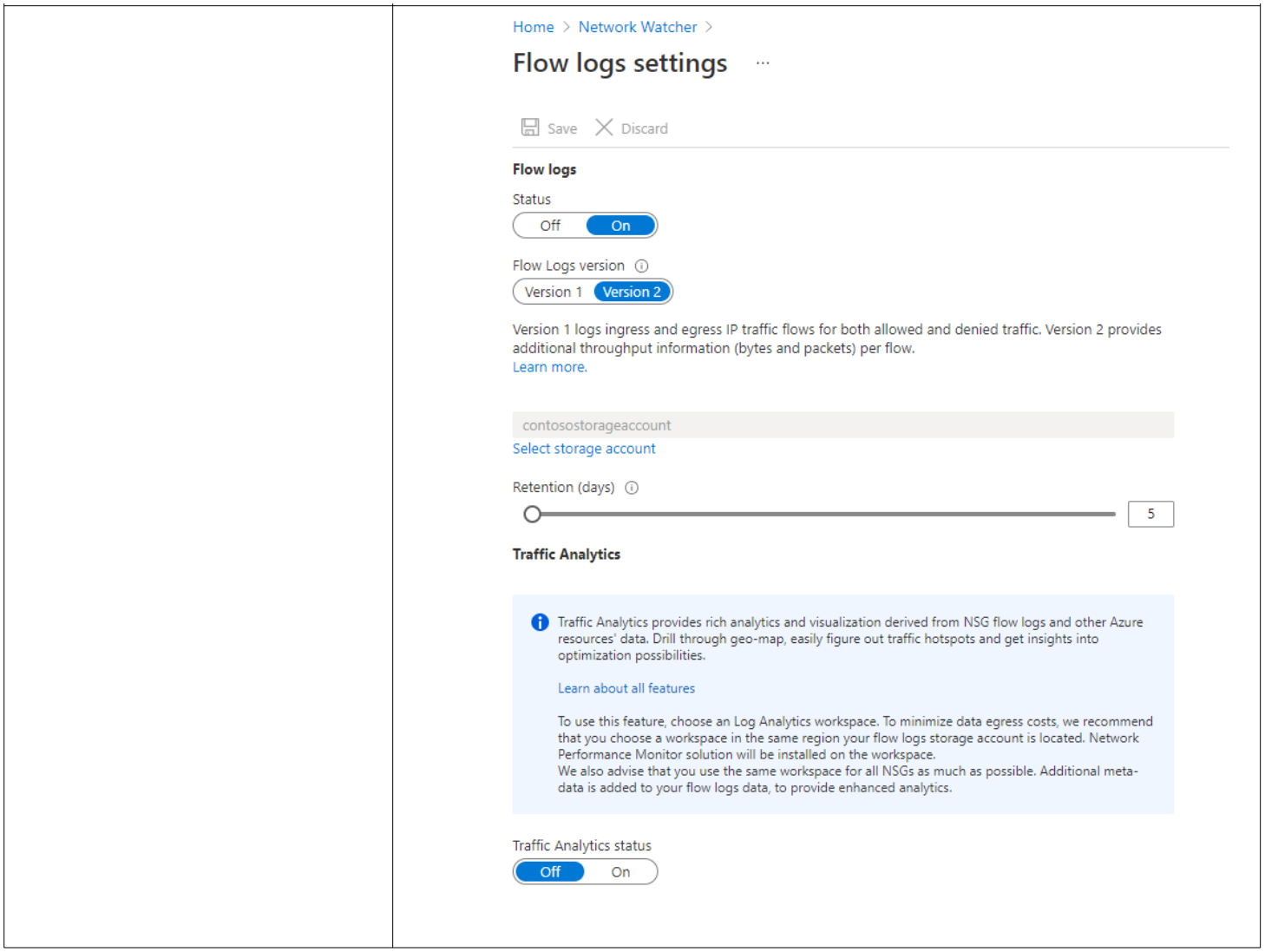
Configure NSG Flow Logs

Network security groups (NSG) allow or deny inbound or outbound traffic to a network interface in a VM.

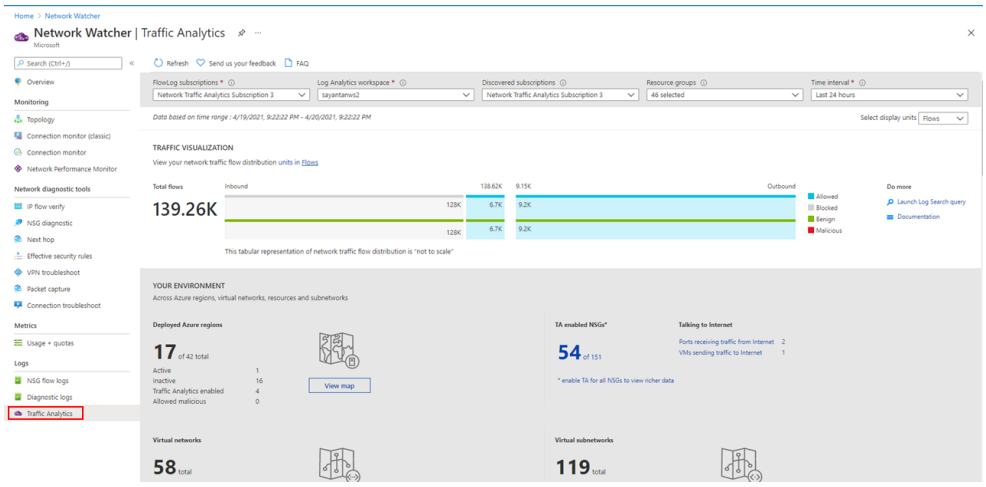
NSG flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG. The NSG flow log capability allows you to log the source and destination IP address, port, protocol, and whether traffic was allowed or denied by an NSG.

	1. To configure the parameters of NSG flow logs in the Azure portal, navigate to the NSG Flow Logs section in Network Watcher.

	2. Click the name of the NSG to bring up the Settings pane for the Flow log.


Home > Network Watcher >
Flow logs settings
Save
Discard
Flow logs
Status
Off
On
Flow Logs version
Version 1
Version 2
Version 1 logs ingress and egress IP traffic flows for both allowed and denied traffic. Version 2 provides additional throughput information (bytes and packets) per flow.
Learn more.
contosostorageaccount
Select storage account
Retention (days)
5
Traffic Analytics
Traffic Analytics provides rich analytics and visualization derived from NSG flow logs and other Azure resources' data. Drill through geo-map, easily figure out traffic hotspots and get insights into optimization possibilities.
Learn about all features
To use this feature, choose an Log Analytics workspace. To minimize data egress costs, we recommend that you choose a workspace in the same region your flow logs storage account is located. Network Performance Monitor solution will be installed on the workspace.
We also advise that you use the same workspace for all NSGs as much as possible. Additional meta-data is added to your flow logs data, to provide enhanced analytics.
Traffic Analytics status
Off
On

Connection Monitor **(use and test the feature)**	Connection Monitor provides unified end-to-end connection monitoring in Azure Network Watcher. The Connection Monitor feature supports hybrid and Azure cloud deployments. Network Watcher provides tools to monitor, diagnose, and view connectivity-related metrics for your Azure deployments. Here are some benefits of Connection Monitor: ● Unified, intuitive experience for Azure and hybrid monitoring needs ● Cross-region, cross-workspace connectivity monitoring ● Higher probing frequencies and better visibility into network performance ● Faster alerting for your hybrid deployments ● Support for connectivity checks that are based on HTTP, TCP, and ICMP ● Metrics and Log Analytics support for both Azure and non-Azure test setups
Traffic Analytics **(use and test the feature)**	Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic Analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud and provide rich visualizations of data written to NSG flow logs. With Traffic Analytics, you can: ● Visualize network activity across your Azure subscriptions and identify hot spots. ● Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks. ● Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity. ● Pinpoint network misconfigurations leading to failed connections in your network. The example screenshot below shows the Traffic Analytics dashboard.


Home > Network Watcher
Network Watcher | Traffic Analytics
Microsoft
Search (Ctrl+/)
Overview
Monitoring
Topology
Connection monitor (classic)
Connection monitor
Network Performance Monitor
Network diagnostic tools
IP flow verify
NSG diagnostic
Next hop
Effective security rules
VPN troubleshoot
Packet capture
Connection troubleshoot
Metrics
Usage + quotas
Logs
NSG flow logs
Diagnostic logs
Traffic Analytics
Refresh
Send us your feedback
FAQ
FlowLog subscriptions *
Network Traffic Analytics Subscription 3
Log Analytics workspace *
sayantanws2
Discovered subscriptions
Network Traffic Analytics Subscription 3
Resource groups
46 selected
Time interval *
Last 24 hours
Data based on time range : 4/19/2021, 9:22:22 PM - 4/20/2021, 9:22:22 PM
Select display units
Flows
TRAFFIC VISUALIZATION
View your network traffic flow distribution units in Flows
Total flows
139.26K
Inbound
Outbound
128K
6.7K
138.62K
9.15K
9.2K
128K
6.7K
9.2K
Allowed
Blocked
Benign
Malicious
Do more
Launch Log Search query
Documentation
This tabular representation of network traffic flow distribution is 'not to scale'
YOUR ENVIRONMENT
Across Azure regions, virtual networks, resources and subnetworks
Deployed Azure regions
17 of 42 total
Active 1
Inactive 16
Traffic Analytics enabled 4
Allowed malicious 0
View map
TA enabled NSGs*
54 of 151
* enable TA for all NSGs to view richer data
Talking to Internet
Ports receiving traffic from Internet 2
VMs sending traffic to Internet 1
Virtual networks
58 total
Virtual subnetworks
119 total