Microsoft AZ-700

Azure Network Engineer Associate

Candidates for this exam should have subject matter expertise in planning, implementing, and maintaining Azure networking solutions, including hybrid networking, connectivity, routing, security, and private access to Azure services.

Candidates for this exam should also have expert Azure administration skills, in addition to extensive experience and knowledge of networking, hybrid connections, and network security.

Skills measured

- **Design, implement, and manage hybrid networking (10—15%)**
- **Design and implement core networking infrastructure (20—25%)**
- **Design and implement routing (25—30%)**
- **Secure and monitor networks (15—20%)**
- **Design and implement Private access to Azure Services (10—15%)**

Prepared By: Arup jyoti Hui

Difference between Inbound and Outbound Traffic: Inbound traffic originates from outside the network, while outbound traffic originates inside the network.

Static IP: Address does not change after assigned
Dynamic IP: Address Changes over time

Policy Based Routing: Works on the principle of static Routing
Route Based Routing : Works on the principle of Dynamic Routing

Regional V-net peering: Connect Azure Vnet in same region
Global V-net Peering: Connect Azure Vnet in different region

Virtual Network NAT:

- Azure NAT is a fully managed resilient Network address translation (NAT) Services.
- Provides outbound internet connectivity for one or more subnets of a virtual network.
- Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet.
- Static IP addresses come from public IP addresses, Public IP prefixes (Set of IP's) or from both.
- If a Public IP prefix is used, all IP addresses of the entire Public IP prefixes are consumed by a NAT gateway.
- Each NAT gateway can provide up to 50 Gbps of throughput
- Each NAT gateway can support 64000 flows each for TCP and UDP per assigned outbound IP addresses & 16 such public Ips can be used.
- After NAT is configured all UDP and TCP outbound flows from any virtual machine instance will use NAT for internet connectivity.
- NAT takes precedence over other outbound scenarios and replaces the default internet destinations of a subnet.
-

Limitations Of NAT:

- NAT is compatible with standard SKU public IP, Public IP prefix and load balancer resources.
- Therefore Basic resources must be placed on a subnet not configured with NAT.
- NAT only supports IPv4 address. No support for IPv6 address family.
- Therefore NAT can't be deployed on a subnet with an IPv6 prefix.

System routes:

Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create or remove system routes, but you can override some system routes with custom routes. Azure creates default system routes for each subnet, and adds additional optional default routes to specific subnets, or every subnet, when you use specific Azure capabilities. Some defaults rules are:

- Communication from within the same subnet
- From a subnet to another within a Vnet.
- From Vnet to Internet
- From a Vnet to another Vnet through VPN gateway.
- From Vnet to your on-prem network through a VPN gateway.

Custom routes:

To control the way network traffic is routed more precisely, you can override the default routes that Azure creates by using your own user-defined routes (UDR). This technique can be useful when you want to ensure that traffic between two subnets passes through a firewall appliance, or if you want to ensure that no traffic from a VNet could be routed to the internet

Services That can be deployed into a V-Net:

Category	Service	Dedicated Subnet
Compute	Virtual machines: Linux or Windows	No
	Virtual machine scale sets	No
	Cloud Service: Virtual network (classic) only	No
	Azure Batch	No
Network	Application Gateway - WAF	Yes
	VPN Gateway	Yes
	Azure Firewall	Yes
	Azure Bastion	Yes
	Network Virtual Appliances	No
Data	RedisCache	Yes
	Azure SQL Managed Instance	Yes
Analytics	Azure HDInsight	No
	Azure Databricks	No
Identity	Azure Active Directory Domain Services	No

Containers	Azure Kubernetes Service (AKS)	No
	Azure Container Instance (ACI)	Yes
	Azure Container Service Engine with Azure Virtual Network CNI plug-in	No
	Azure Functions	Yes
Web	API Management	Yes
	Web Apps	Yes
	App Service Environment	Yes
	Azure Logic Apps	Yes
Hosted	Azure Dedicated HSM	Yes
	Azure NetApp Files	Yes
Azure Spring Apps	Deploy in Azure virtual network (VNet injection)	Yes
Virtual desktop infrastructure	Azure Lab Services	Yes

Gateway Subnet:

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. We recommend that you create a gateway subnet that uses a /27 or /28.

BGP:

What is BGP? Border Gateway Protocol (BGP) refers to a gateway protocol that enables the internet to exchange routing information between autonomous systems (AS). As networks interact with each other, they need a way to communicate. This is accomplished through peering. BGP makes peering possible. Without it, networks would not be able to send and receive information with each other.

Creation Of Site to site connection: *(Connection between On-prem and Azure)*

1. Create a V-net
2. Create a Virtual network gateway (VPN)
3. Create a local network gateway (Which will work as ON-prem network)
4. Create a connection in virtual network gateway which will add the local network gateway.

High availability options for VPN connections:

To provide better availability for your VPN connections, there are a few options available:

- VPN Gateway redundancy (Active-standby)
- Multiple on-premises VPN devices (Two local network gateway as on prem which will work as Active & passive and One Vnet in Azure)
- Active-active Azure VPN gateway (One on-prem network with Two Azure vnet but not as Active and passive)
- Combination of both (Two On-prem network and two Azure Vnet)

Troubleshoot Azure VPN Gateway using diagnostic logs:

Using diagnostic logs, you can troubleshoot multiple VPN gateway related events including configuration activity, VPN Tunnel connectivity, IPsec logging, BGP route exchanges, Point to Site advanced logging.

There are several diagnostic logs you can use to help troubleshoot a problem with your VPN Gateway.

- **GatewayDiagnosticLog** - Contains diagnostic logs for gateway configuration events, primary changes, and maintenance events.
- **TunnelDiagnosticLog** - Contains tunnel state change events. Tunnel connect/disconnect events have a summarized reason for the state change if applicable.
- **RouteDiagnosticLog** - Logs changes to static routes and BGP events that occur on the gateway.
- **IKEDiagnosticLog** - Logs IKE control messages and events on the gateway.
- **P2SDiagnosticLog** - Logs point-to-site control messages and events on the gateway.

Creation of Point to Site Connection: *(Connection between Azure and Client system/Remote User)*

1. Create a V-net
2. Create a Virtual Network gateway
3. Add Point to site connection in Virtual network gateway (give a IP which will not override V-net)
4. Add root certificate and finish configuration of Point to site connection
5. Download the VPN client

Authentication methods of P-to-S:

- Authenticate using native Azure certificate authentication
- Authenticate using native Azure Active Directory authentication
- Authenticate using Active Directory (AD) Domain Server

WAN:

An organization might have a large user center at headquarters, multiple branch offices, and multiple remote users. All these sites need to connect to resources throughout the organization. Historically, organizations used a combination of VPNs to provide site-to-site connections for branch offices, point-to-site connections for individual remote users, and connections to Cloud services. Traditional Software Defined Wide Area Network (SD WAN) technologies combine and manage the connections, requiring connectivity appliances such as gateways at each site, and connecting them through internet tunnels.

Azure Virtual WAN combines all these methods of connectivity to enable the organization to leverage the Microsoft backbone network, which connects Microsoft data centers across Azure regions and a large mesh of edge-nodes around the world. By connecting to the backbone network, organizations can leverage its reliability, capacity, and flexibility to connect their regional Azure VNets, network edge locations like ExpressRoute, and carrier neutral connections.

A Virtual WAN is a security delineation; each instance of a Virtual WAN is self-contained in terms of connectivity and hence also provides security isolation.

Organizations will generally only require one instance of a Virtual WAN. Each Virtual WAN is implemented as a hub-and-spoke topology, and can have one or more hubs, which support connectivity between different types of endpoints including connectivity vendors like AT&T, Verizon, and T-Mobile. All hubs are connected in a full mesh topology in a Standard Virtual WAN making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) transitive connectivity.

ExpressRoute:

Some key benefits of ExpressRoute are:

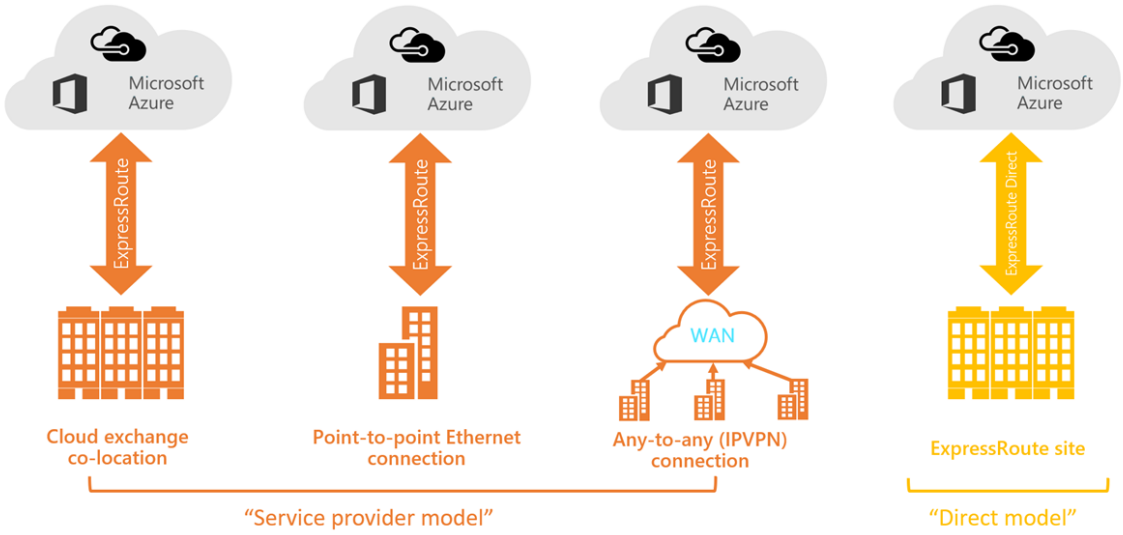
- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider
- Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange
- Connectivity to Microsoft cloud services across all regions in the geopolitical region
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on
- Built-in redundancy in every peering location for higher reliability

ExpressRoute Global Reach is the service where if you have two datacenters, which are located at different geo-locations and both are connected to Microsoft Azure via Express Route then these two datacenters can also connect to each other securely via Microsoft's backbone.

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.

ExpressRoute connectivity models

You can create a connection between your on-premises network and the Microsoft cloud in four different ways, CloudExchange Co-location, Point-to-point Ethernet Connection, Any-to-any (IPVPN) Connection, and ExpressRoute Direct. Connectivity providers may offer one or more connectivity models.



Co-located at a cloud exchange

If you are co-located in a facility with a cloud exchange, you can order virtual cross-connections to the Microsoft cloud through the co-location provider's Ethernet exchange. Co-location providers can offer either Layer 2 cross-connections, or managed Layer 3 cross-connections between your infrastructure in the co-location facility and the Microsoft cloud.

Point-to-point Ethernet connections

You can connect your on-premises datacenters/offices to the Microsoft cloud through point-to-point Ethernet links. Point-to-point Ethernet providers can offer Layer 2 connections, or managed Layer 3 connections between your site and the Microsoft cloud.

Any-to-any (IPVPN) networks

You can integrate your WAN with the Microsoft cloud. IPVPN providers (typically MPLS VPN) offer any-to-any connectivity between your branch offices and datacenters. The Microsoft cloud can be interconnected to your WAN to make it look just like any other branch office. WAN providers typically offer managed Layer 3 connectivity.

Direct from ExpressRoute sites

You can connect directly into the Microsoft's global network at a peering location strategically distributed across the world. ExpressRoute Direct provides dual 100 Gbps or 10-Gbps connectivity, which supports Active/Active connectivity at scale.

Using ExpressRoute direct vs using a Service Provider

ExpressRoute using a Service Provider	ExpressRoute Direct
Uses 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

Design redundancy for an ExpressRoute deployment

There are 2 ways in which redundancy can be planned for an ExpressRoute deployment.

- Configure ExpressRoute and site to site coexisting connections
- Create a zone redundant VNET gateway in Azure Availability zones

Configure ExpressRoute and site to site coexisting connections

This section helps you configure ExpressRoute and Site-to-Site VPN connections that coexist. Having the ability to configure Site-to-Site VPN and ExpressRoute has several advantages. You can configure Site-to-Site VPN as a

secure failover path for ExpressRoute or use Site-to-Site VPNs to connect to sites that are not connected through ExpressRoute.

Configuring Site-to-Site VPN and ExpressRoute coexisting connections has several advantages:

- You can configure a Site-to-Site VPN as a secure failover path for ExpressRoute.
- Alternatively, you can use Site-to-Site VPNs to connect to sites that are not connected through ExpressRoute.

You can configure either gateway first. Typically, you will incur no downtime when adding a new gateway or gateway connection.

- Only route-based VPN gateway is supported
- The ASN of Azure VPN Gateway must be set to 65515
- The gateway subnet must be /27 or a shorter prefix
- Coexistence in a dual stack VNet is not supported

Create a zone redundant VNet gateway in Azure availability zones

You can deploy VPN and ExpressRoute gateways in Azure Availability Zones. This brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure Availability Zones physically and logically separates gateways within a region, while protecting your on-premises network connectivity to Azure from zone-level failures.

Zone-redundant gateways

To automatically deploy your virtual network gateways across availability zones, you can use zone-redundant virtual network gateways. With zone-redundant gateways, you can benefit from zone-resiliency to access your mission-critical, scalable services on Azure.

Zonal gateways

To deploy gateways in a specific zone, you can use zonal gateways. When you deploy a zonal gateway, all instances of the gateway are deployed in the same Availability Zone.

Gateway SKUs

Zone-redundant and zonal gateways are available as gateway SKUs. There is a new virtual network gateway SKUs in Azure AZ regions. These SKUs are like the corresponding existing SKUs for ExpressRoute and VPN Gateway, except that they are specific to zone-redundant and zonal gateways. You can identify these SKUs by the "AZ" in the SKU name.

Public IP SKUs

Zone-redundant gateways and zonal gateways both rely on the Azure public IP resource Standard SKU. The configuration of the Azure public IP resource determines whether the gateway that you deploy is zone-redundant, or zonal. If you create a public IP resource with a Basic SKU, the gateway will not have any zone redundancy, and the gateway resources will be regional.

- Zone-redundant gateways
    - When you create a public IP address using the **Standard** public IP SKU without specifying a zone, the behavior differs depending on whether the gateway is a VPN gateway, or an ExpressRoute gateway.
    - For a VPN gateway, the two gateway instances will be deployed in any 2 out of these three zones to provide zone-redundancy.
    - For an ExpressRoute gateway, since there can be more than two instances, the gateway can span across all the three zones.

- Zonal gateways
    - When you create a public IP address using the **Standard** public IP SKU and specify the Zone (1, 2, or 3), all the gateway instances will be deployed in the same zone.
- Regional gateways
    - When you create a public IP address using the **Basic** public IP SKU, the gateway is deployed as a regional gateway and does not have any zone-redundancy built into the gateway.
    -

Load Balancing Solutions:

1. Load balancer
2. Traffic manager
3. Application gateway
4. Azure Front door
5.

1.Load Balancer:

- Load balancer operates at the layer-4 of the OSI model (transport layer)
- Does not understand HTTP(s) because that;s layer-7 (application layer)
- Only supporting balancing traffic inside a single virtual network

1. Basic Load Balancer:

- Backend pool- Up to 300 instances
- Backend pool- Virtual machines in a single availability set or a VMSS
- Health probes- TCP,HTTP only
- Availability zone- Does not support
- High Availability- Does not support
- Security- NSG optional
- NO SLA

2. Standard Load Balancer:

- Backend pool- Up to 1000 instances
- Backend pool- Any VM and VMSS in a single V-Net
- Health probes- TCP,HTTP,HTTPS
- Availability zones- Yes
- High Availability- Internal load balancer
- Security- NSG required
- 99.99% SLA

3. Public Load Balancer : Which facing to external

4. Internal Load Balancer: Which facing inside internal resources

2.Traffic Manager features

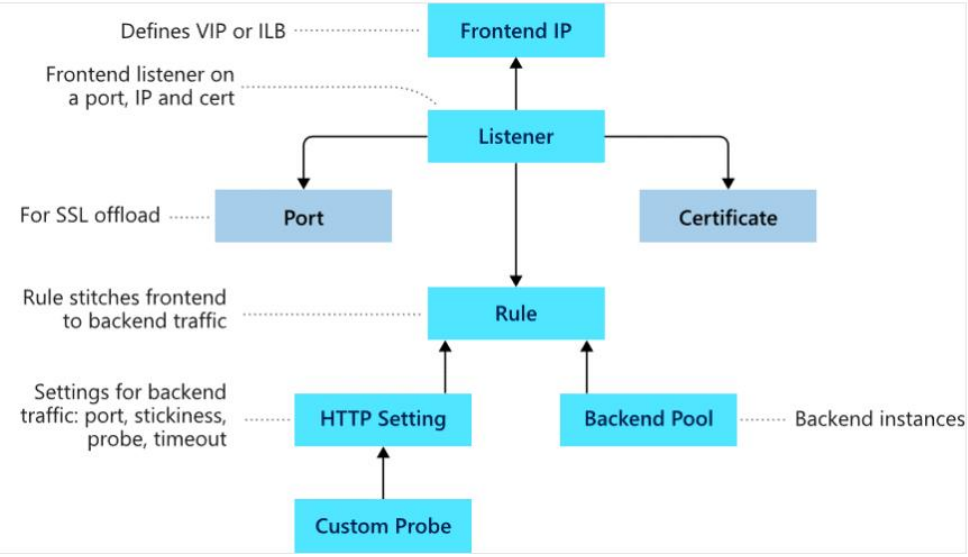
- DNS based global routing between regions.
- Intercepts the request to translate a domain-name into an IP address.
- Sends the traffic to the best region around the world for that client.
- Automatic failover when one region goes down.
- Not limited to only HTTP(s)/Web traffic.

Routing method	When to use
Priority	Select this routing method 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.
Weighted	Select this routing method 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 the routing method 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 this routing method 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 compliant with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.
MultiValue	Select this routing method 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 this 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.

3.Application Gateway:

- Support for the HTTP, HTTPS, HTTP/2 and WebSocket protocols.
- It's operates on Layer-7(Application layer) and can understand URLs, paths etc.
- Limited to HTTP/web traffic.
- Supports load balancing across regions.
- A web application firewall to protect against web application vulnerabilities.
- End-to-end request encryption.
- Autoscaling, to dynamically adjust capacity as your web traffic load change.

- **Redirection**: Redirection can be used to another site, or from HTTP to HTTPS.
- **Rewrite HTTP headers**: HTTP headers allow the client and server to pass parameter information with the request or the response.
- **Custom error pages:** Application Gateway allows you to create custom error pages instead of displaying default error pages. You can use your own branding and layout using a custom error page.



1. Path-based routing

- Path-based routing sends requests with different URL paths different pools of back-end servers. For example, you could direct requests with the path /video/* to a back-end pool containing servers that are optimized to handle video streaming, and direct /images/* requests to a pool of servers that handle image retrieval.

2. Multiple site routing

- Multiple site routing configures more than one web application on the same application gateway instance. In a multi-site configuration, you register multiple DNS names (CNAMEs) for the IP address of the Application Gateway, specifying the name of each site. Application Gateway uses separate listeners to wait for requests for each site. Each listener passes the request to a different rule, which can route the requests to servers in a different back-end pool.

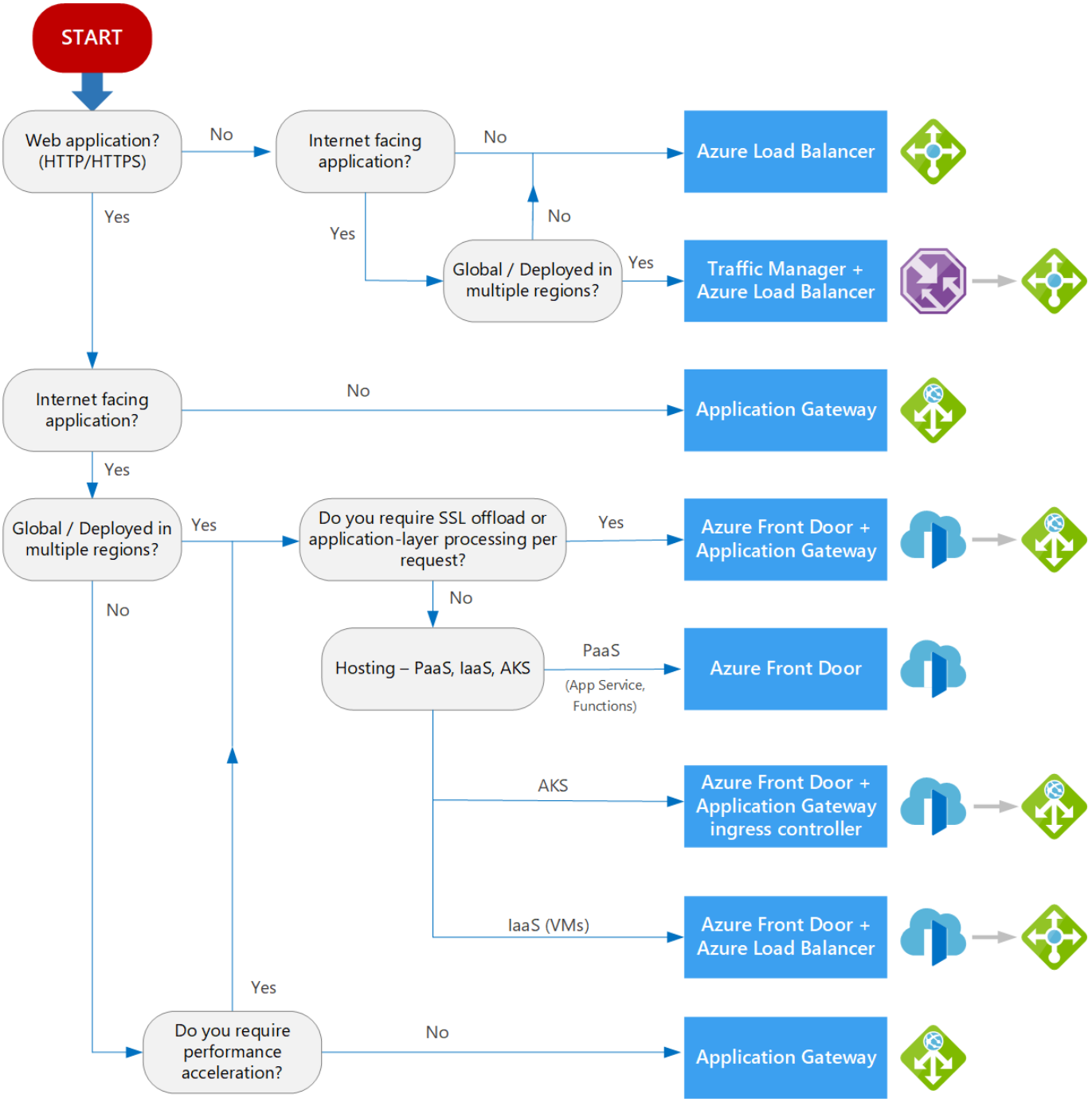
4.Azure Front door service:

Front Door works at Layer 7 (HTTP/HTTPS layer) using anycast protocol with split TCP and Microsoft's global network to improve global connectivity. Based on your routing method you can ensure that Front Door will route your client requests to the fastest and most available application backend. An application backend is any Internet-facing service hosted inside or outside of Azure. Front Door provides a range of traffic-routing methods and backend health monitoring options to suit different application needs and automatic failover scenarios. Like Traffic Manager, Front Door is resilient to failures, including failures to an entire Azure region.

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.

- The most recent innovation in load balancing and supports Global load balancing between regions
- Operates at layer-7(Application layer)
- Can understand URLs and paths.
- Combined load balancing, WAF, Caching, app acceleration features into one
- Serves as the public endpoint for your app/websites
- Supports SSL offloading.

Load Balancing Options:



What is Azure Private Endpoint?

By-default all PaaS service are publicly accessible. To make it secure private endpoint are used to access the PaaS resources privately. Private Endpoint is the key technology behind Private Link. Private Endpoint is a network interface that enables a private and secure

connection between your virtual network and an Azure service. In other words, Private Endpoint is the network interface that replaces the resource's public endpoint.

Distributed Denial of Service (DDoS)

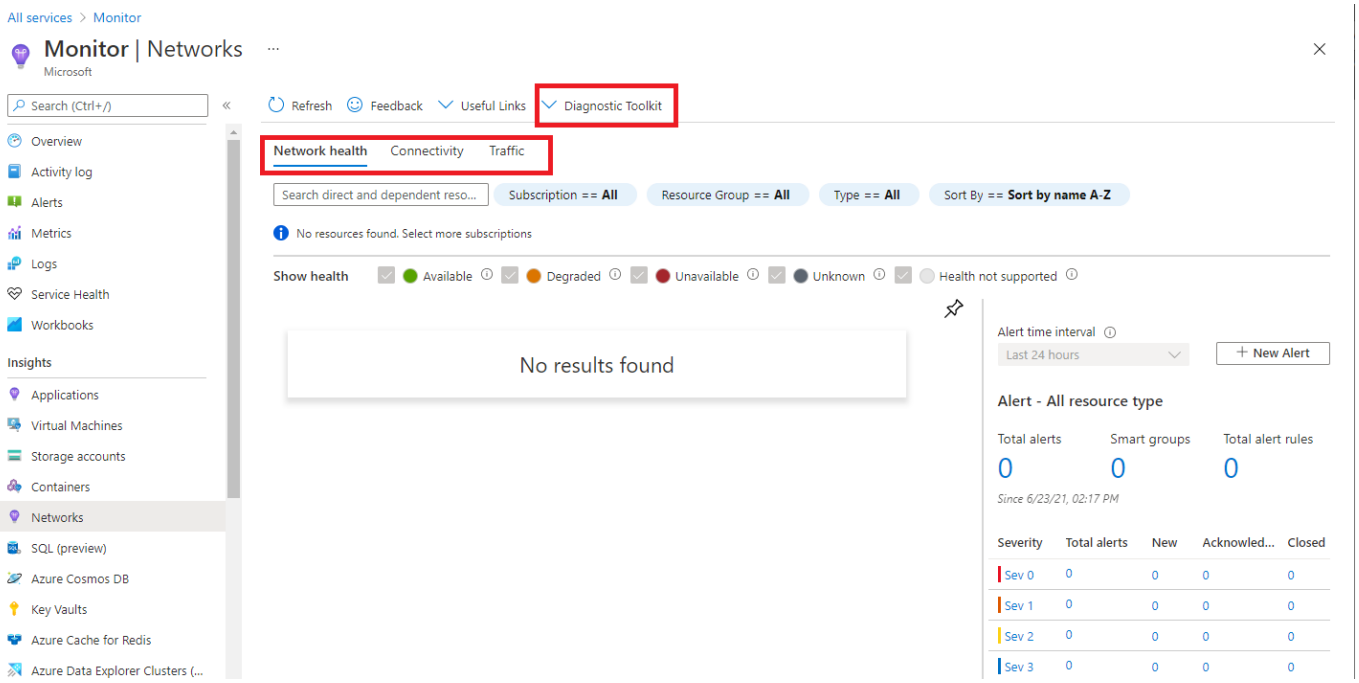
A denial of service attack (DoS) is an attack that has the goal of preventing access to services or systems. If the attack originates from one location, it is called a DoS. If the attack originates from multiple networks and systems, it is called distributed denial of service (DDoS).

Monitor network resources with Azure Monitor Network Insights

You can use the **Insights>Networks** section in **Azure Monitor** to obtain a broad view of health and metrics for all your deployed network resources, without requiring any configuration. It also provides access to network monitoring features such as Connection Monitor, flow logging for network security groups (NSG) flow logs, and Traffic Analytics, and it provides other network diagnostic features.

Azure Monitor Network Insights is structured around these key components of monitoring:

- Network health and metrics
- Connectivity
- Traffic
- Diagnostic Toolkit



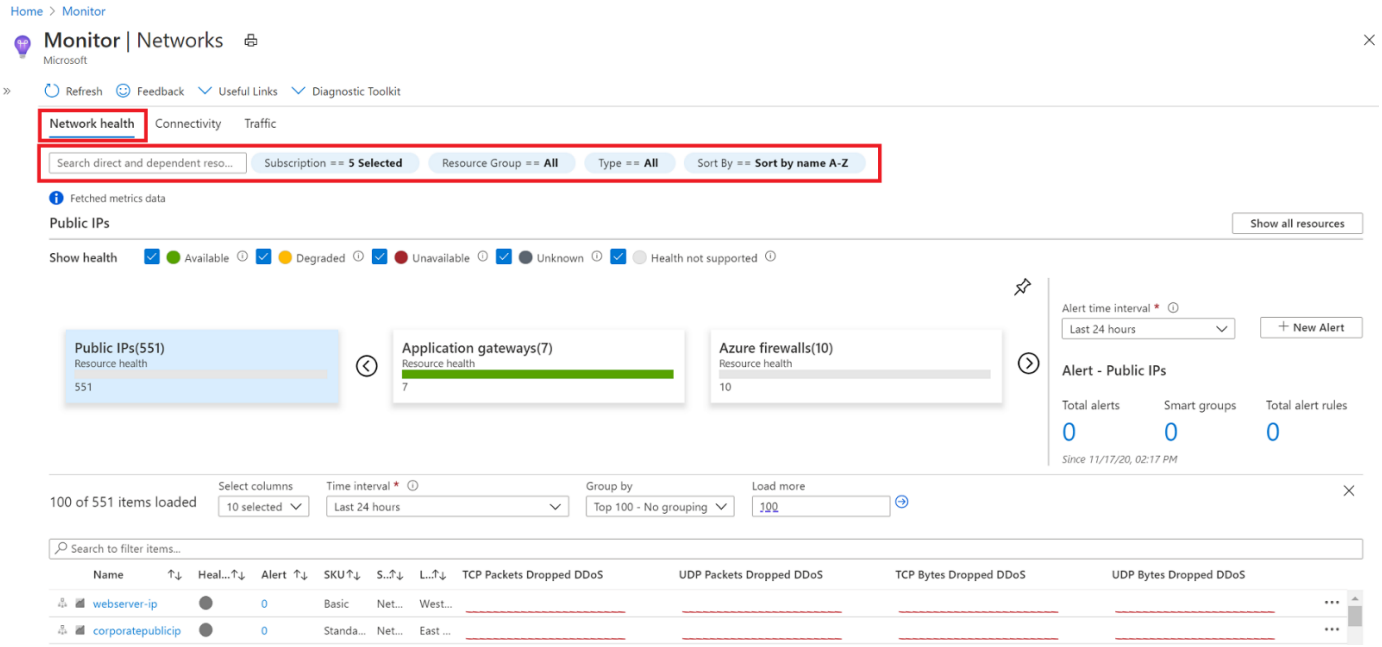
Network health and metrics

The **Network health** tab of Azure Monitor Network Insights offers a simple method for visualizing an inventory of your networking resources, together with resource health and alerts. It is divided into four key functionality areas: search and filtering, resource health and metrics, alerts, and dependency view.

Search and filtering

You can customize the resource health and alerts view by using filters such as **Subscription**, **Resource Group**, and **Type**.

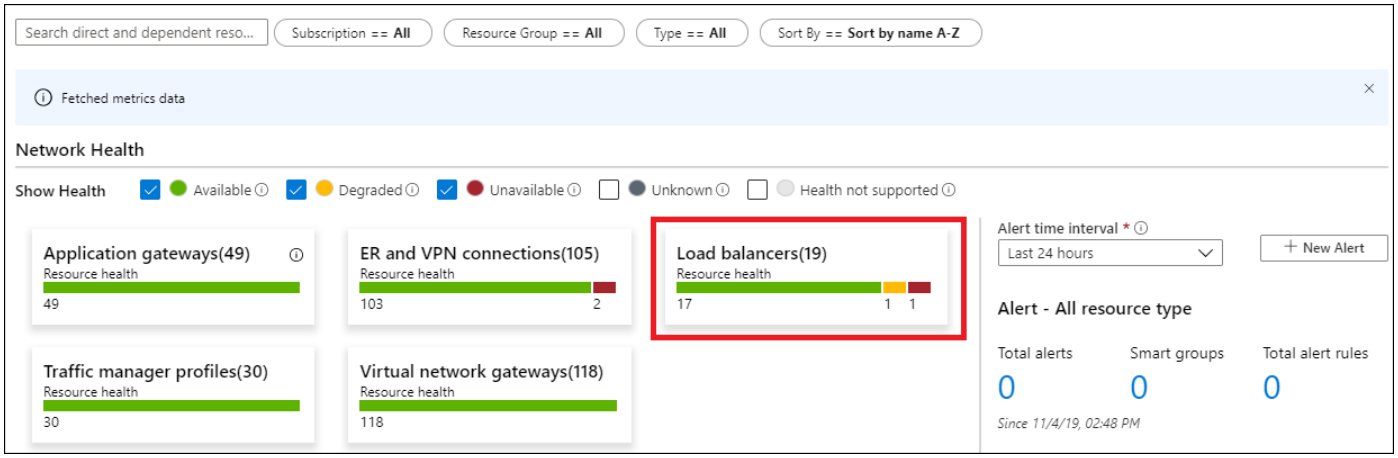
You can use the search box to search for network resources and their associated resources. For example, a public IP is associated with an application gateway, so a search for the public IP's DNS name would return both the public IP and the associated application gateway.



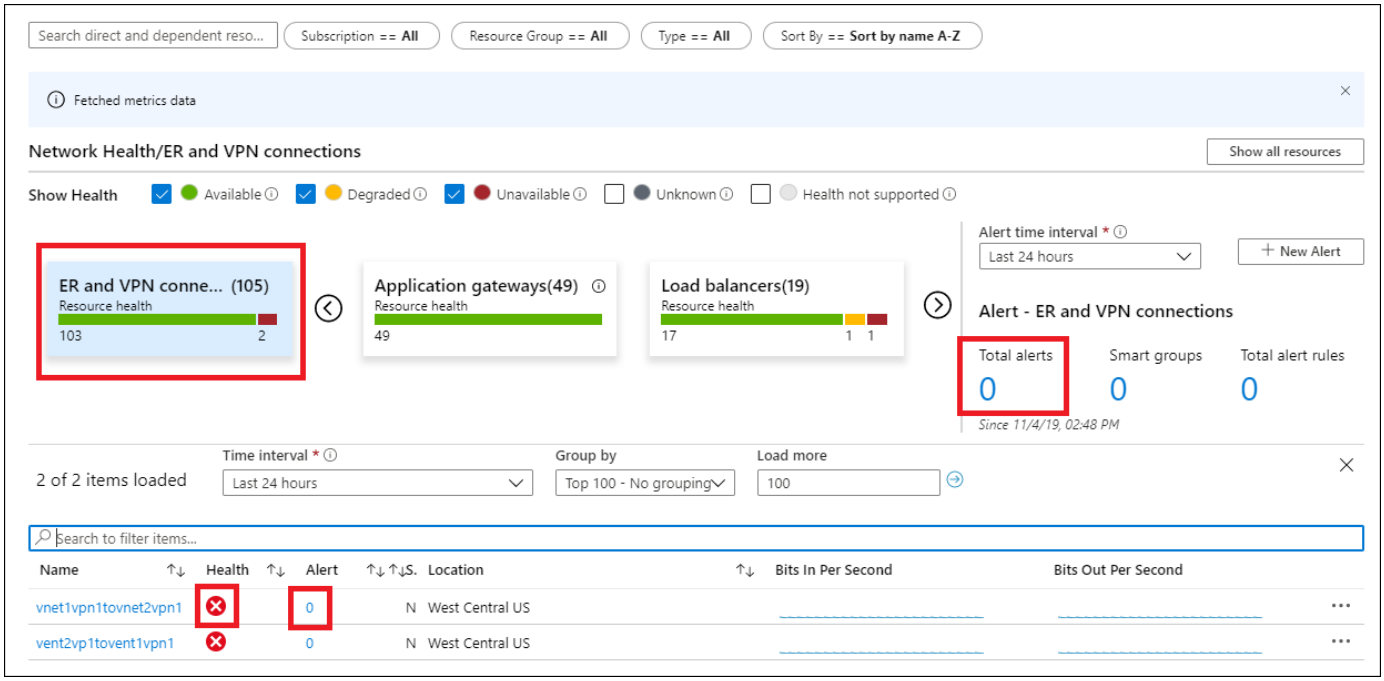
Network resource health and metrics

You can use the health and metrics information to get an overview of the health status of your various network resources.

In the example screenshot below, each tile represents a particular type of network resource. The tile displays the number of instances of that resource type that are deployed across all your selected subscriptions. It also displays the health status of the resource. Here you can see that there are 19 **Load balancers** deployed, 17 of which are healthy, 1 is degraded, and 1 is unavailable.



If you select one of the tiles, you get a view of the metrics for that network resource. In the example screenshot below, you can see the metrics for the **ER and VPN connections** resource.



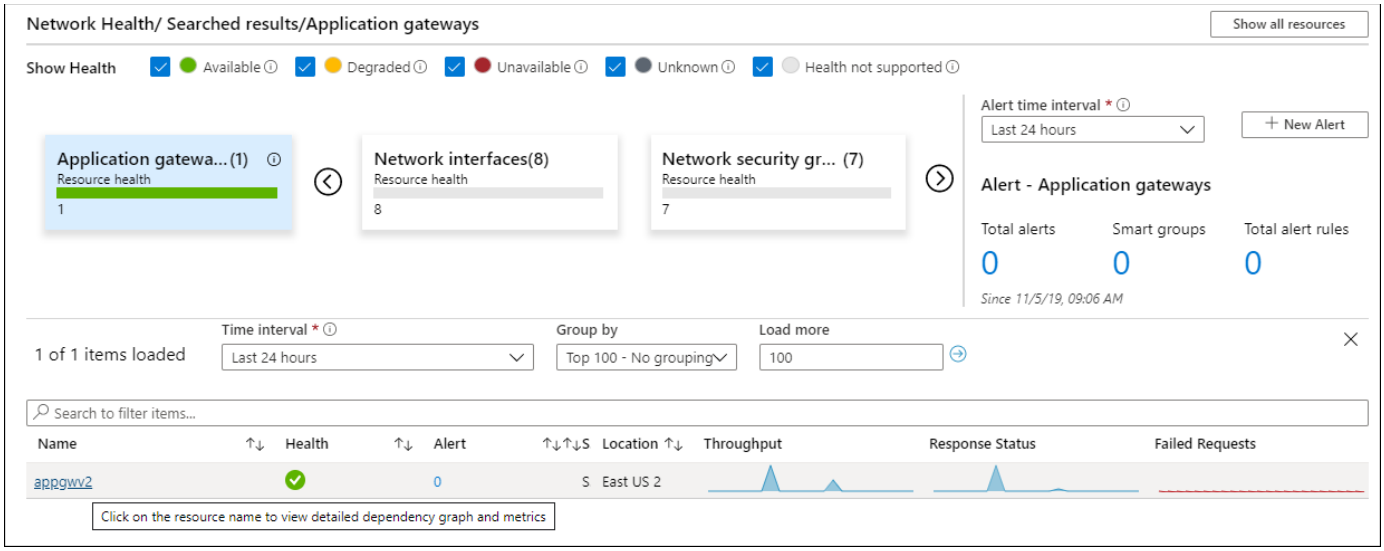
You can select any item in this grid view. For example, you could select the icon in the **Health** column to get resource health for that connection, or select the value in the **Alert** column to go to the alerts and metrics page for the connection.

Alerts

The **Alert** box on the right side of the page provides a view of all alerts generated for the selected resources across all your subscriptions. If there is a value for the alerts on an item, simply select the alert count for that item to go to a detailed alerts page for it.

Dependency view

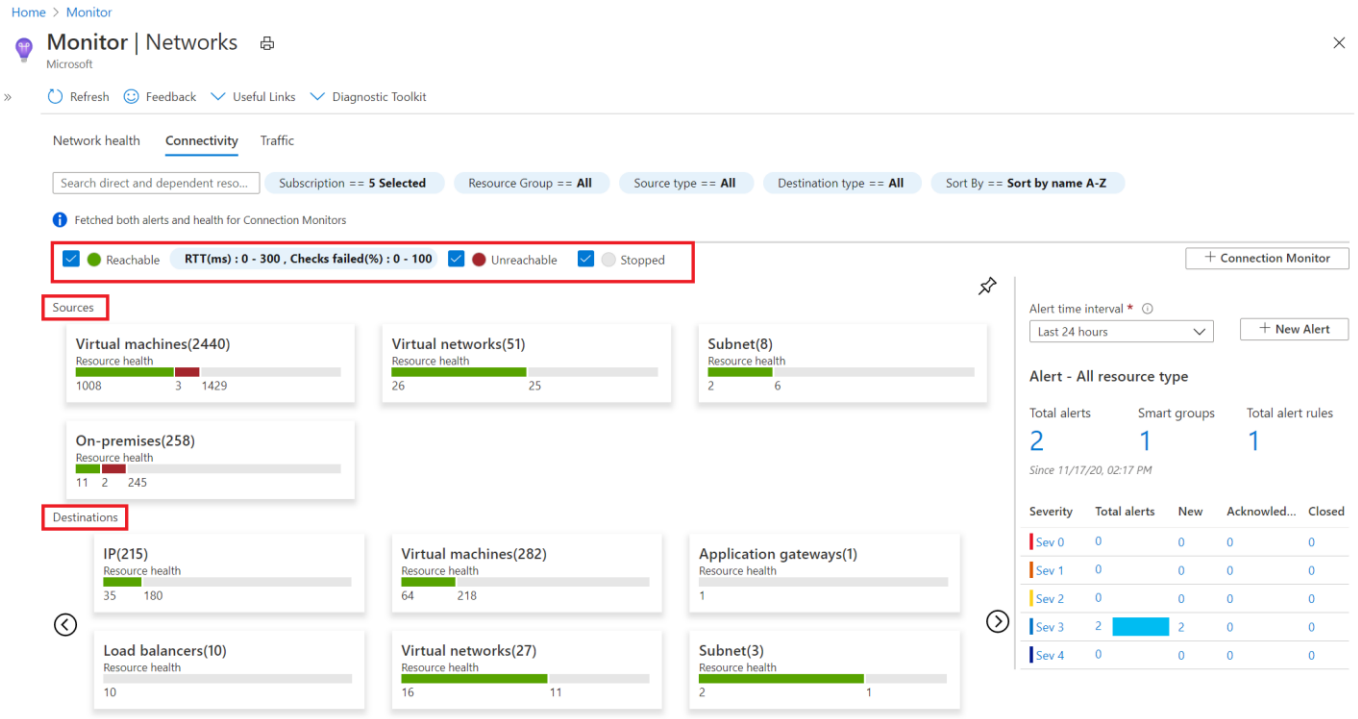
Dependency view helps you visualize how a resource is configured. Dependency view is currently available for **Azure Application Gateway**, **Azure Virtual WAN**, and **Azure Load Balancer**. For example, for Application Gateway, you can access dependency view by selecting the Application Gateway resource name in the metrics grid view. You can do the same thing for Virtual WAN and Load Balancer.



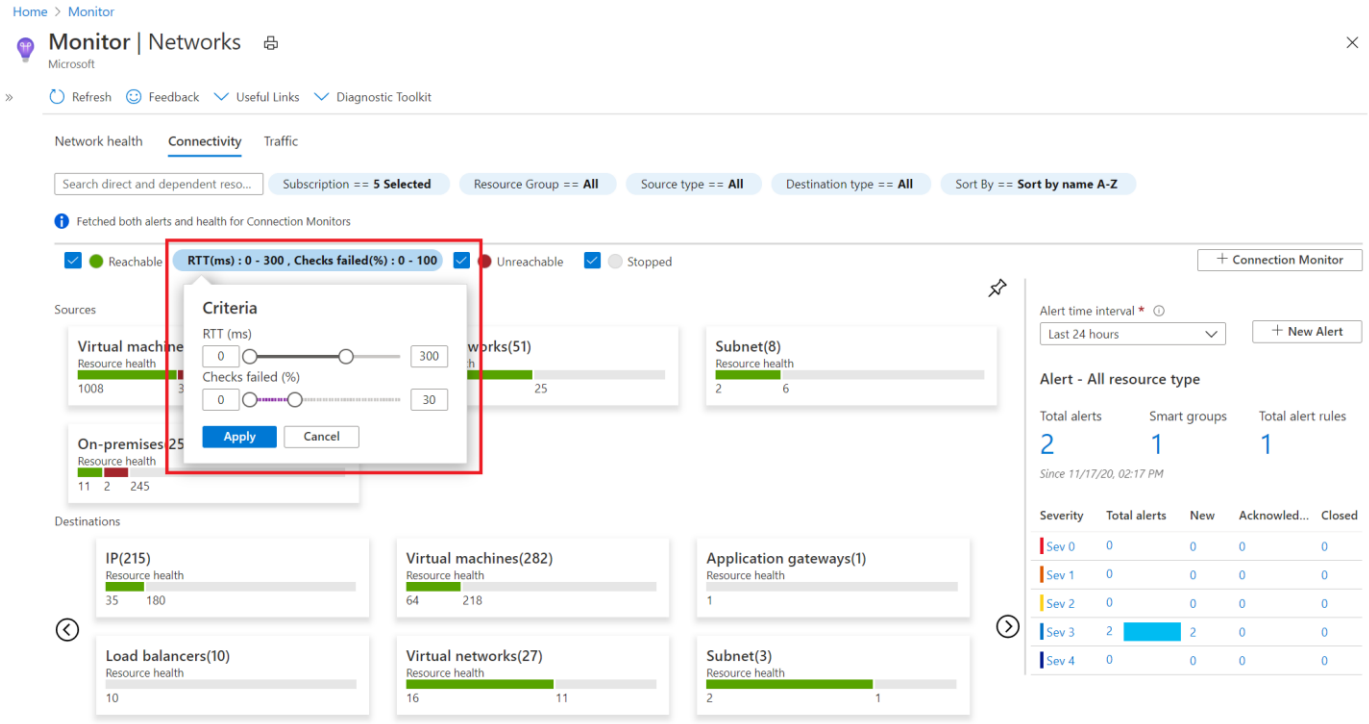
Connectivity

The **Connectivity** tab of Azure Monitor Network Insights provides an easy way to visualize all tests configured via Connection Monitor and Connection Monitor (classic) for the selected set of subscriptions.

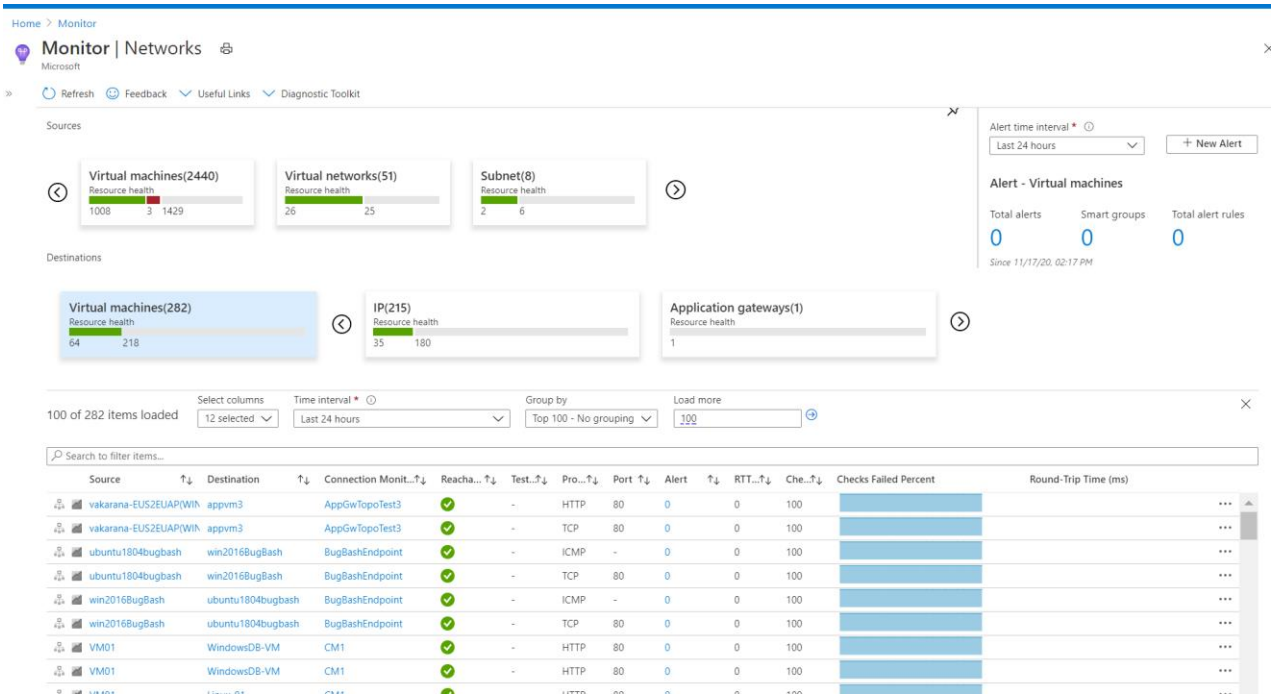
Tests are grouped by **Sources** and **Destinations** tiles and display the reachability status for each test. Reachable settings provide easy access to configurations for your reachability criteria, based on **Checks failed(%)** and **RTT(ms)**.



After you set the values, the status for each test updates based on the selection criteria.

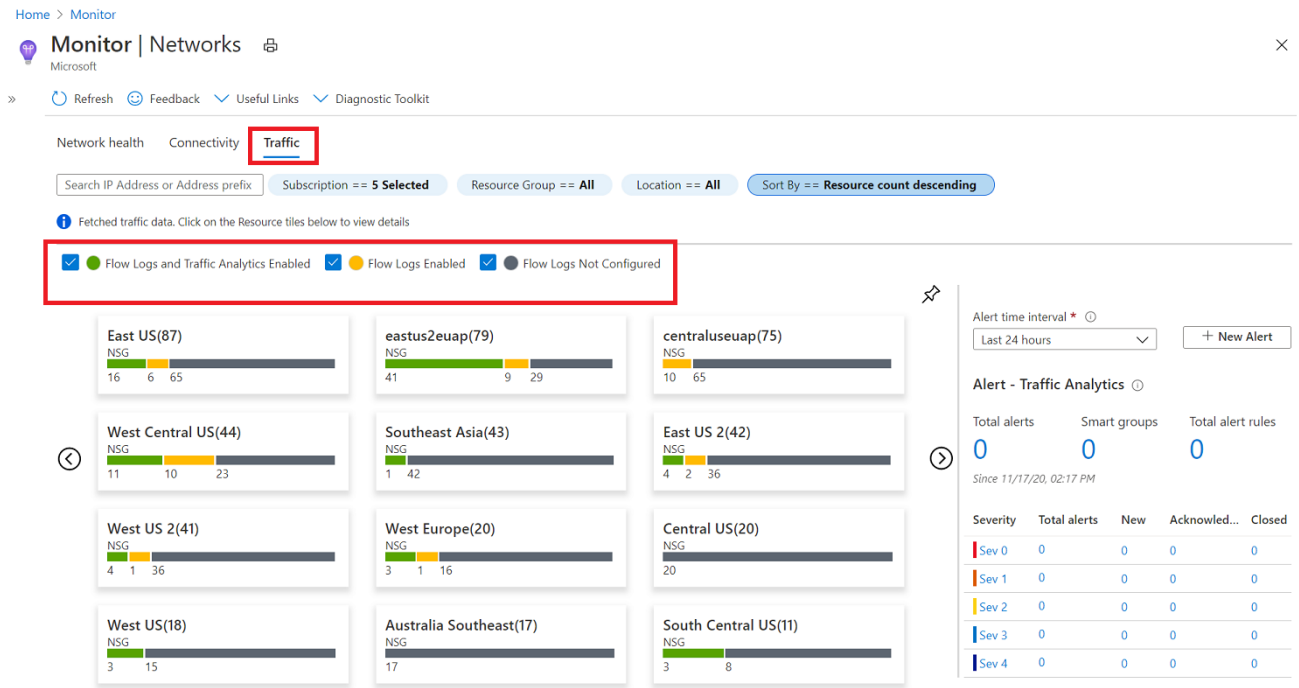


From here, you can then select any source or destination tile to open it up in metric view. In the example screenshot below, the metrics for the **Destinations>Virtual machines** tile are being displayed.

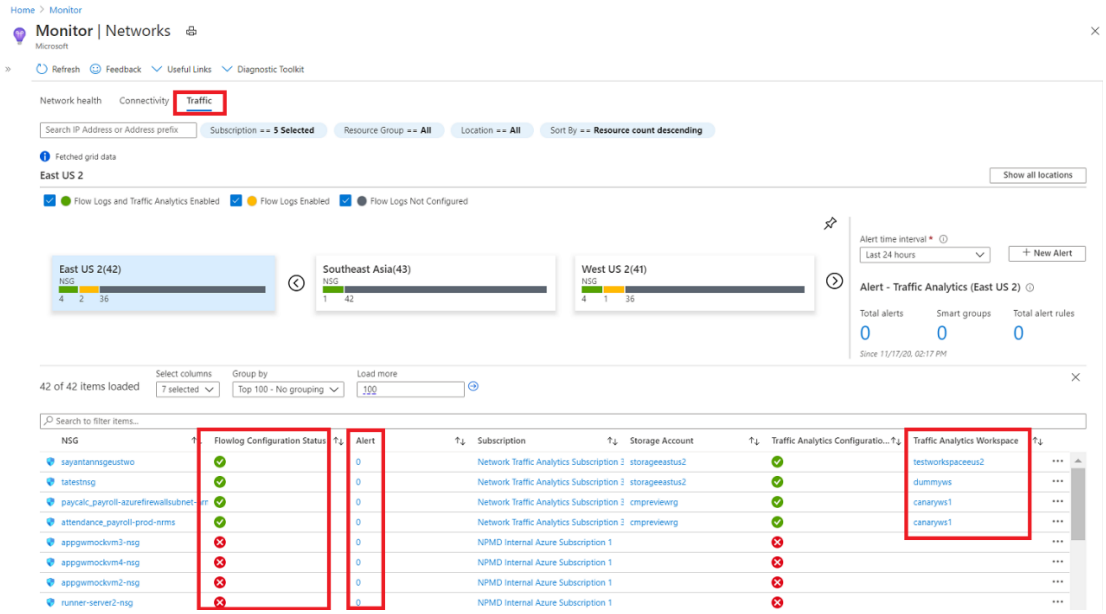


Traffic

The **Traffic** tab of Azure Monitor Network Insights provides access to all NSGs configured for **NSG flow logs** and **Traffic Analytics** for the selected set of subscriptions, grouped by location. The search functionality provided on this tab enables you to identify the NSGs configured for the searched IP address. You can search for any IP address in your environment. The tiled regional view will display all NSGs along with the NSG flow logs and Traffic Analytics configuration status.



If you select any region tile, a grid view will appear which shows NSG flow logs and Traffic Analytics in a view that is simple to interpret and configure.



In this grid view you can select an icon in the **Flow log Configuration Status** column to edit the NSG flow log and Traffic Analytics configuration. Or you can select a value in the **Alert** column to go to the traffic alerts configured for that NSG, and you can navigate to the Traffic Analytics view by selecting the **Traffic Analytics Workspace**.

Diagnostic Toolkit

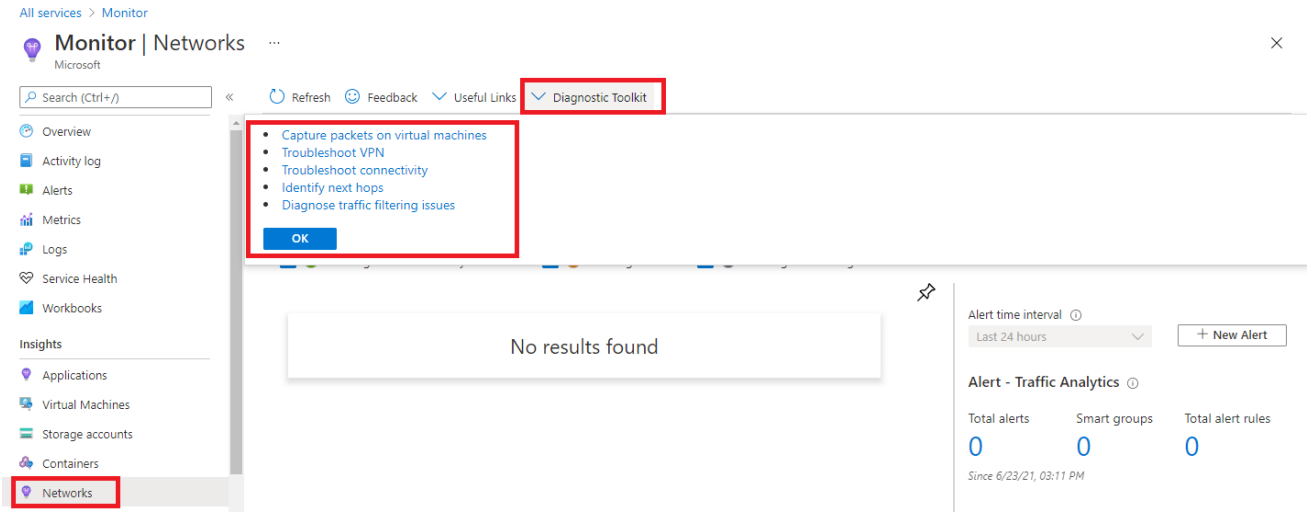
The Diagnostic Toolkit feature in Azure Monitor Network Insights provides access to all the diagnostic features available for troubleshooting your networks and their components.

The **Diagnostic Toolkit** drop-down list provides to access to the following network monitoring features:

- Capture packets on virtual machines - opens the **Network Watcher packet capture** network diagnostic tool to enable you create capture sessions to track traffic to and from a virtual machine. Filters are provided for the capture session to ensure you capture only the traffic you want. Packet capture helps to diagnose network anomalies, both reactively, and proactively. Packet capture is a virtual machine extension that is remotely started through Network Watcher.
- Troubleshoot VPN - opens the **Network Watcher VPN Troubleshoot** tool to diagnose the health of a virtual network gateway or connection.
- Troubleshoot connectivity - opens the **Network Watcher Connection Troubleshoot** tool to check a direct TCP connection from a virtual machine (VM) to a VM, fully qualified domain name (FQDN), URI, or IPv4 address.
- Identify next hops - opens the **Network Watcher Next hop** network diagnostic tool to obtain the next hop type and IP address of a packet from a specific VM

and NIC. Knowing the next hop can help you establish if traffic is being directed to the expected destination, or whether the traffic is being sent nowhere.

- Diagnose traffic filtering issues - opens the **Network Watcher IP flow verify** network diagnostic tool to verify if a packet is allowed or denied, to or from a virtual machine, based on 5-tuple information. The security group decision and the name of the rule that denied the packet is returned.



Network Watcher:

Network Topology: 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: 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: 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. Depending on your situation the next hop could be Internet, Virtual Appliance, Virtual Network Gateway, VNet Local, VNet Peering, or None. None lets you know that while there may be a valid system route to the destination, there is no next hop to route the traffic to the destination. When you create a virtual network, Azure creates several default outbound routes for network traffic. The outbound traffic from all resources, such as VMs, deployed in a virtual network, are routed based on Azure's default routes. You might override Azure's default routes or create additional routes.

Effective security rules: 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: 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: 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: 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: 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.