200 XP

Identify routing capabilities of an Azure virtual network

10 minutes

To control traffic flow within your virtual network, you must learn the purpose and benefits of custom routes. You must also learn how to configure the routes to direct traffic flow through a network virtual appliance (NVA).

Azure routing

Network traffic in Azure is automatically routed across Azure subnets, virtual networks, and on-premises networks. This routing is controlled by system routes, which are assigned by default to each subnet in a virtual network. With these system routes, any Azure virtual machine that is deployed to a virtual network can communicate with all other Azure virtual machines in subnets in that network. These virtual machines are also potentially accessible from on-premises through a hybrid network or the internet.

You can't create or delete system routes. But you can override the system routes by adding custom routes to control traffic flow to the next hop.

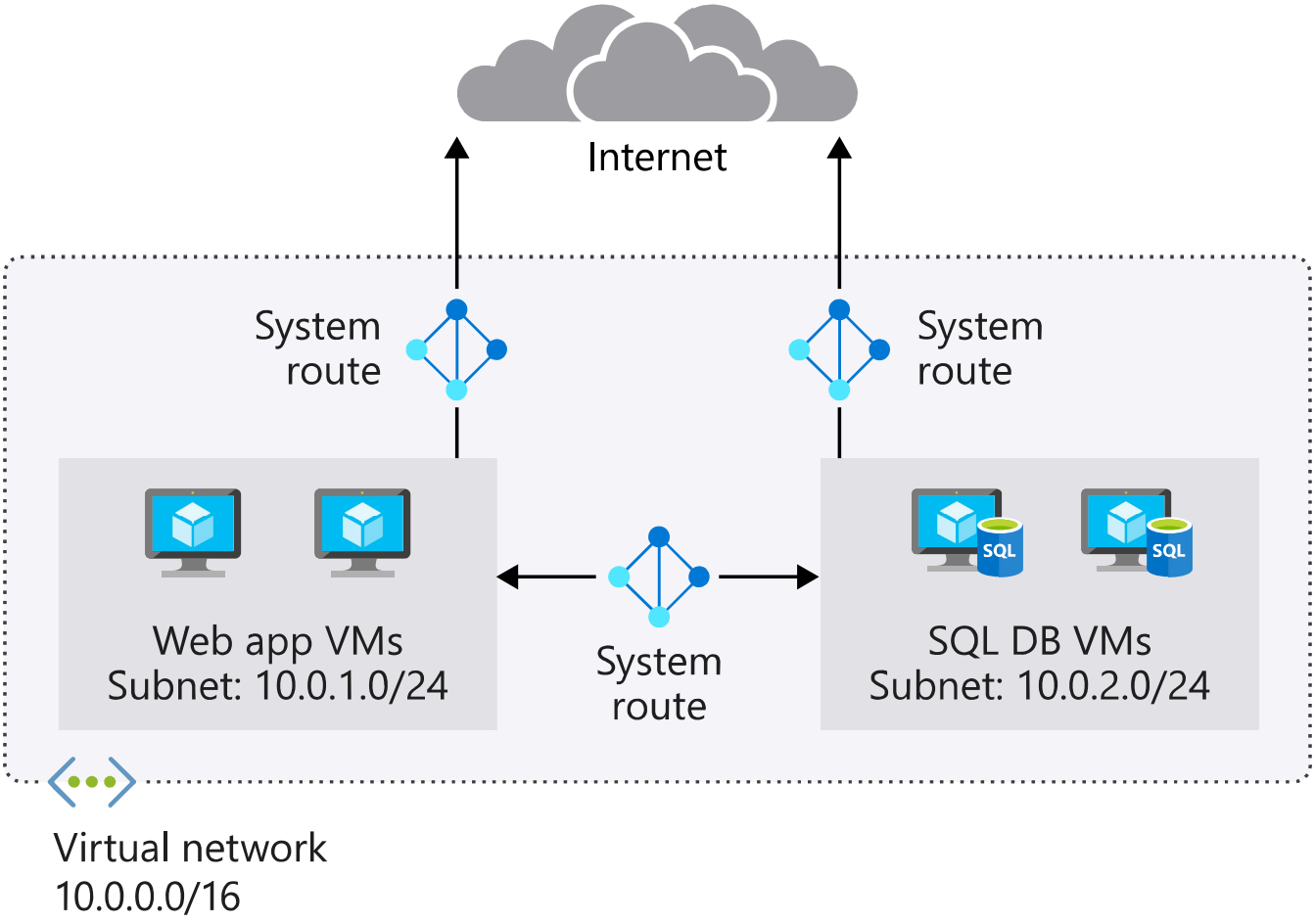
Every subnet has the following default system routes:

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

The **Next hop type** column shows the network path taken by traffic sent to each address prefix. The path can be one of the following hop types:

- **Virtual network**: A route is created in the address prefix. The prefix represents each address range created at the virtual-network level. If multiple address ranges are specified, multiple routes are created for each address range.
- **Internet**: The default system route 0.0.0.0/0 routes any address range to the internet, unless you override Azure's default route with a custom route.
- **None**: Any traffic routed to this hop type is dropped and doesn't get routed outside the subnet. By default, the following IPv4 private-address prefixes are created: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The prefix 100.64.0.0/10 for a shared address space is also added. None of these address ranges are globally routable.

The following diagram shows an overview of system routes and shows how traffic flows among subnets and the internet by default. You can see from the diagram that traffic flows freely among the two subnets and the internet.



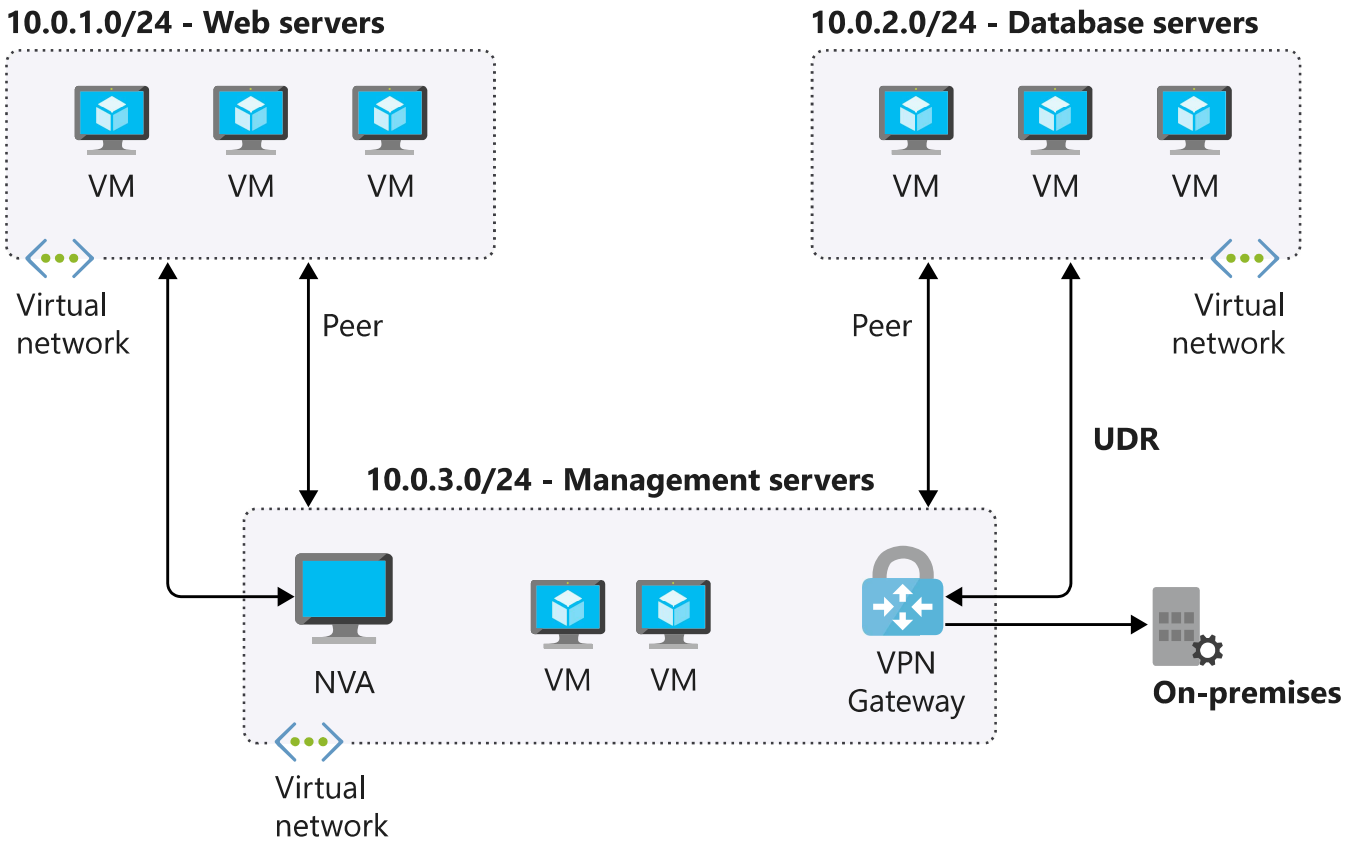
Within Azure, there are additional system routes. Azure will create these routes if the following capabilities are enabled:

- Virtual network peering
- Service chaining
- Virtual network gateway
- Virtual network service endpoint

Virtual network peering and service chaining

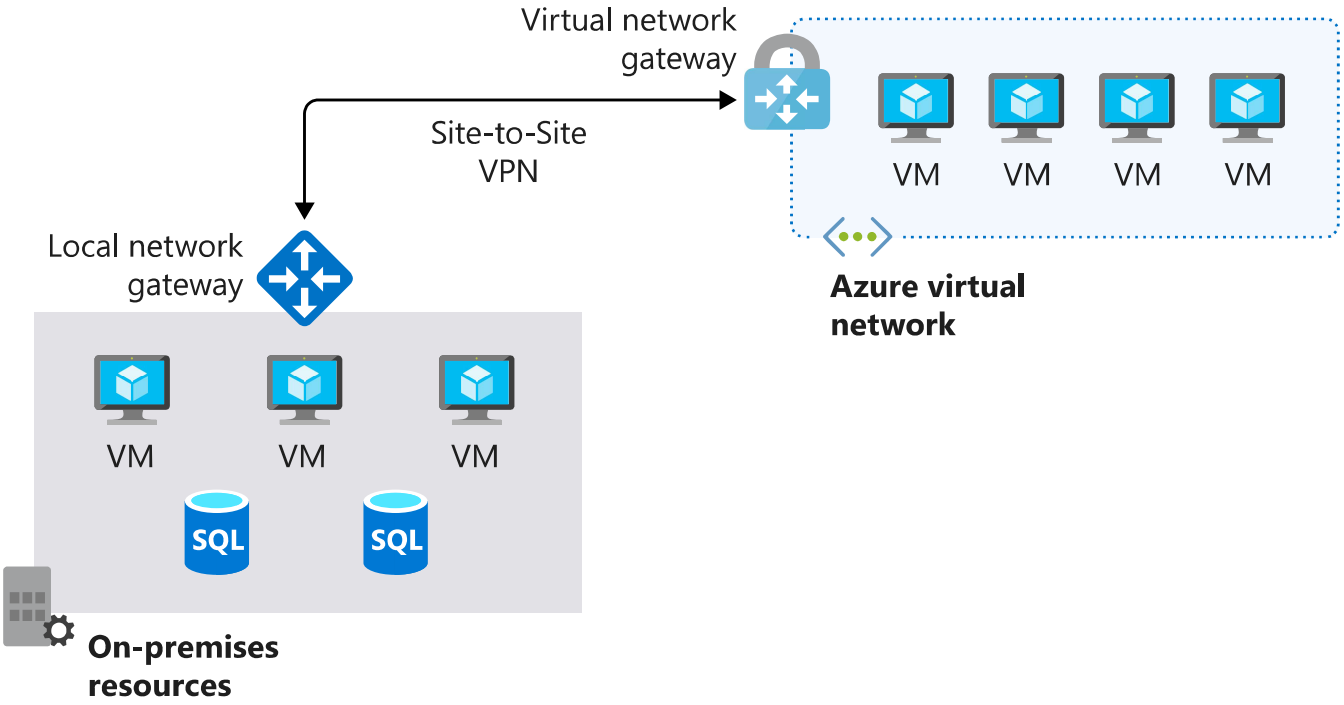
Virtual network peering and service chaining let virtual networks within Azure be connected to one another. With this connection, virtual machines can communicate with each other within the same region or across regions. This communication in turn creates additional routes within the default route table. Service chaining lets you override these routes by creating user-defined routes between peered networks.

The following diagram shows two virtual networks with peering configured. The user-defined routes are configured to route traffic through an NVA or an Azure VPN gateway.



Virtual network gateway

Use a virtual network gateway to send encrypted traffic between Azure and on-premises over the internet and to send encrypted traffic between Azure networks. A virtual network gateway contains routing tables and gateway services.



Virtual network service endpoint

Virtual network endpoints extend your private address space in Azure by providing a direct connection to your Azure resources. This connection restricts the flow of traffic: your Azure virtual machines can access your storage account directly from the private address space and deny access from a public virtual machine. As you enable service endpoints, Azure creates routes in the route table to direct this traffic.

Custom routes

System routes might make it easy for you to quickly get your environment up and running. But there are many scenarios in which you'll want to more closely control the traffic flow within your network. For example, you might want to route traffic through an NVA or through a firewall from partners and others. This control is possible with custom routes.

You have two options for implementing custom routes: create a user-defined route or use Border Gateway Protocol (BGP) to exchange routes between Azure and on-premises networks.

User-defined routes

You use a user-defined route to override the default system routes so that traffic can be routed through firewalls or NVAs.

For example, you might have a network with two subnets and want to add a virtual machine in the perimeter network to be used as a firewall. You create a user-defined route so that traffic passes through the firewall and doesn't go directly between the subnets.

When creating user-defined routes, you can specify these next hop types:

- **Virtual appliance**: A virtual appliance is typically a firewall device used to analyze or filter traffic that is entering or leaving your network. You can specify the private IP address of a NIC attached to a virtual machine so that IP forwarding can be enabled. Or you can provide the private IP address of an internal load balancer.
- **Virtual network gateway**: Use to indicate when you want routes for a specific address to be routed to a virtual network gateway. The virtual network gateway is specified as a VPN for the next hop type.
- **Virtual network**: Use to override the default system route within a virtual network.
- **Internet**: Use to route traffic to a specified address prefix that is routed to the internet.
- **None**: Use to drop traffic sent to a specified address prefix.

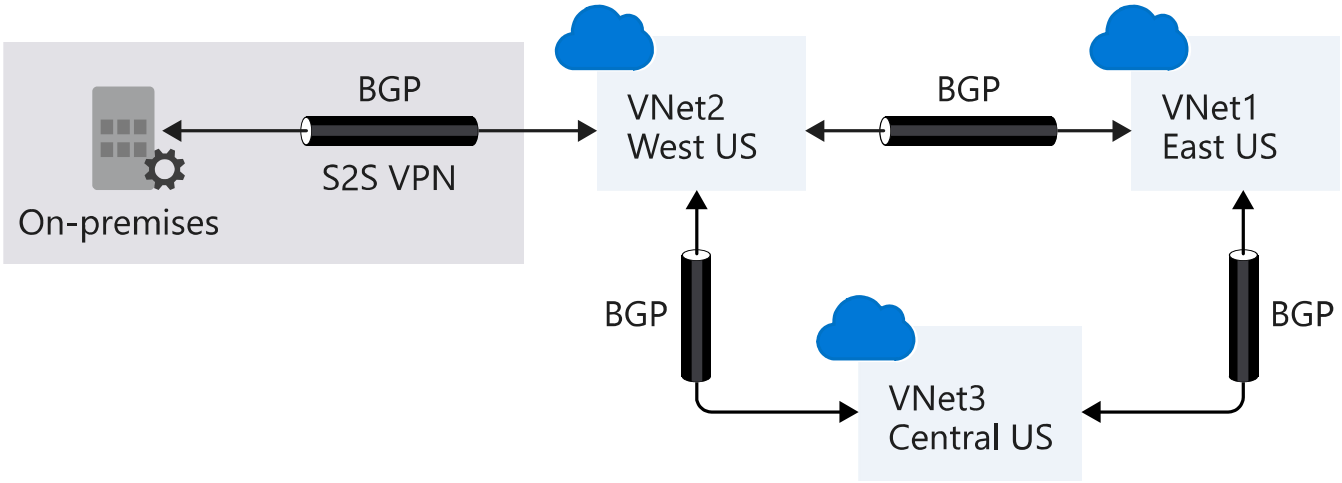
With user-defined routes, you can't specify the next hop type **VirtualNetworkServiceEndpoint**, which indicates virtual network peering.

Border gateway protocol

A network gateway in your on-premises network can exchange routes with a virtual network gateway in Azure by using BGP. BGP is the standard routing protocol that is normally used to exchange routing and information among two or more networks. BGP is used to transfer data and information between different host gateways like on the internet or between autonomous systems.

You typically use BGP to advertise on-premises routes to Azure when you're connected to an Azure datacenter through Azure ExpressRoute. You can also configure BGP if you connect to an Azure virtual network by using a VPN site-to-site connection.

The following diagram shows a topology with paths that can pass data between Azure VPN Gateway and on-premises networks:



BGP offers network stability because routers can quickly change connections to send packets if a connection path goes down.

Route selection and priority

If multiple routes are available in a route table, Azure uses the route with the longest prefix match. For example, if a message is sent to the IP address 10.0.0.2, but two routes are available with the 10.0.0.0/16 and 10.0.0.0/24 prefixes, Azure selects the route with the 10.0.0.0/24 prefix because it's more specific.

The longer the route prefix, the shorter the list of IP addresses available through that prefix. By using longer prefixes, the routing algorithm can select the intended address more quickly.

You can't configure multiple user-defined routes with the same address prefix.

If multiple routes share the same address prefix, Azure selects the route based on its type in the following order of priority:

1. User-defined routes
2. BGP routes
3. System routes

Check your knowledge

1. Why would you use a custom route in a virtual network?

- ○ To load balance the traffic in your virtual network.
- ○ To connect to your Azure virtual machines using RDP or SSH.
- ○ To control the flow of traffic in your Azure virtual network.
- ○ To connect to resources in another virtual network hosted in Azure.

2. Why might you use virtual network peering?

- ○ To connect virtual networks together in the same region or across regions.
- ○ To assign public IP addresses to all of your resources across multiple virtual networks.
- ○ So that load balancers can control traffic flow across your virtual networks.
- ○ To run custom reports that scan and identify what resources are running across all of your virtual networks, as opposed to running

reports on each virtual network.

Check your answers