

Describe Azure networking services

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/describe-azure-networking-services/1-introduction>

Introduction

Completed

This module introduces Azure networking services that help you connect, secure, and route traffic between resources. You explore foundational capabilities for communication within Azure, between Azure and on-premises environments, and across internet-connected clients.

Learning objectives

After completing this module, you'll be able to:

- Describe Azure virtual networking, including subnets and endpoints.
- Describe connectivity options with Azure VPN Gateway.
- Describe when to use Azure ExpressRoute.
- Describe Azure DNS capabilities.
- Configure basic network access for an Azure resource.

2. Describe Azure virtual networking

<https://learn.microsoft.com/en-us/training/modules/describe-azure-networking-services/2-virtual-network>

Describe Azure virtual networking

Completed

Azure virtual networks and virtual subnets enable Azure resources, such as VMs, web apps, and databases, to communicate with each other, with users on the internet, and with your on-premises

client computers. You can think of an Azure network as an extension of your on-premises network with resources that link other Azure resources.

Azure virtual networks provide the following key networking capabilities:

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources
- Route network traffic
- Filter network traffic
- Connect virtual networks

Azure virtual networking supports both public and private endpoints to enable communication between external or internal resources with other internal resources.

- Public endpoints have a public IP address and can be accessed from anywhere in the world.
- Private endpoints exist within a virtual network and have a private IP address from within the address space of that virtual network.

Isolation and segmentation

Azure Virtual Network lets you create multiple isolated virtual networks. When you set up a virtual network, you define a private IP address space by using either public or private IP address ranges. The IP range only exists within the virtual network and isn't internet routable. You can divide that IP address space into subnets and allocate part of the defined address space to each named subnet.

For name resolution, you can use the name resolution service built into Azure. You also can configure the virtual network to use either an internal or an external DNS server.

Internet communications

You can enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer.

Communicate between Azure resources

Azure resources can communicate securely with each other in one of two ways:

- Virtual networks can connect not only VMs but other Azure resources, such as the App Service Environment for Power Apps, Azure Kubernetes Service, and Azure virtual machine scale sets.
- Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach lets you link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

Communicate with on-premises resources

Azure virtual networks let you link resources together in your on-premises environment and within your Azure subscription. In effect, you can create a network that spans both your local and cloud environments. There are three ways to achieve this connectivity:

- Point-to-site virtual private network connections are from a computer outside your environment back into your private network. In this case, the client computer initiates an encrypted VPN connection to connect to the Azure virtual network.
- Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.
- Azure ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet. ExpressRoute is useful for environments where you need greater bandwidth and even higher levels of security.

Route network traffic

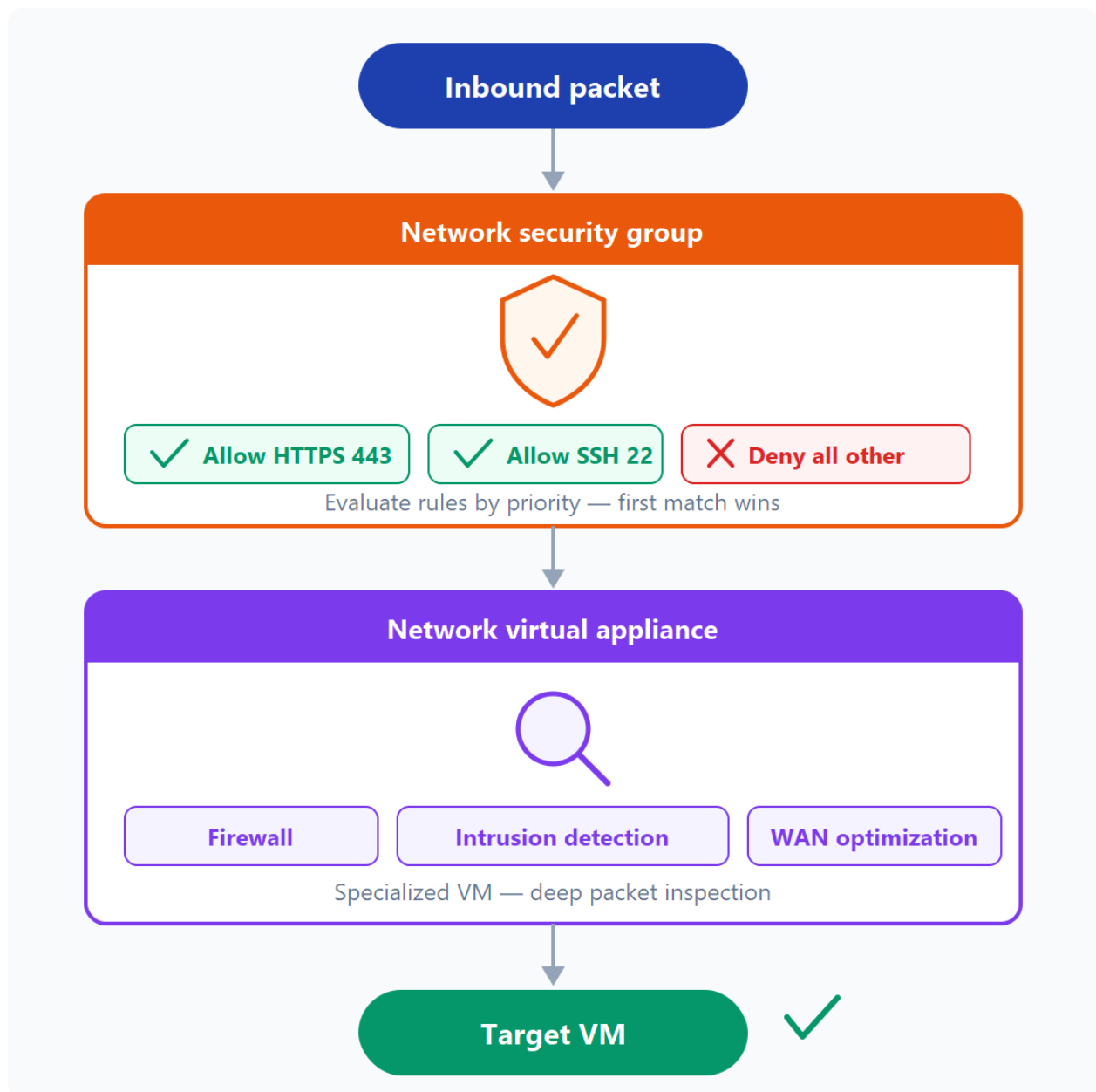
By default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows:

- Route tables let you define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
- Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or Azure ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.
- User-defined routes (UDR) let you control the routing tables between subnets within a virtual network or between virtual networks, giving you greater control over network traffic flow.

Filter network traffic

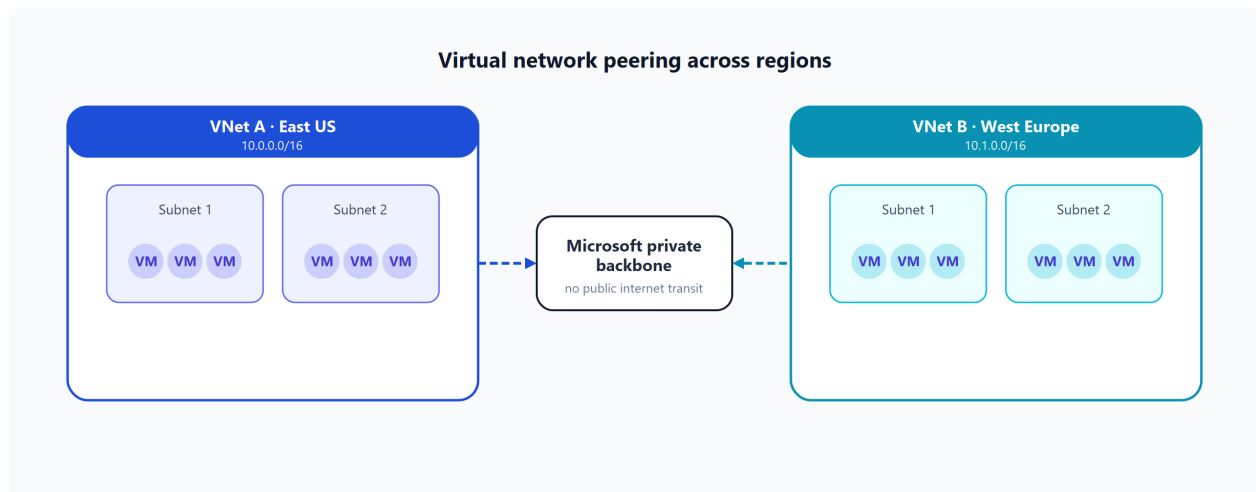
Azure virtual networks let you filter traffic between subnets by using the following approaches:

- Network security groups are Azure resources that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
- Network virtual appliances are specialized VMs that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.



Connect virtual networks

You can link virtual networks together by using virtual network peering. Peering allows two virtual networks to connect directly to each other. Network traffic between peered networks is private, and travels on the Microsoft backbone network, never entering the public internet. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which lets you create a global interconnected network through Azure.



3. Describe Azure virtual private networks

<https://learn.microsoft.com/en-us/training/modules/describe-azure-networking-services/3-virtual-private-networks>

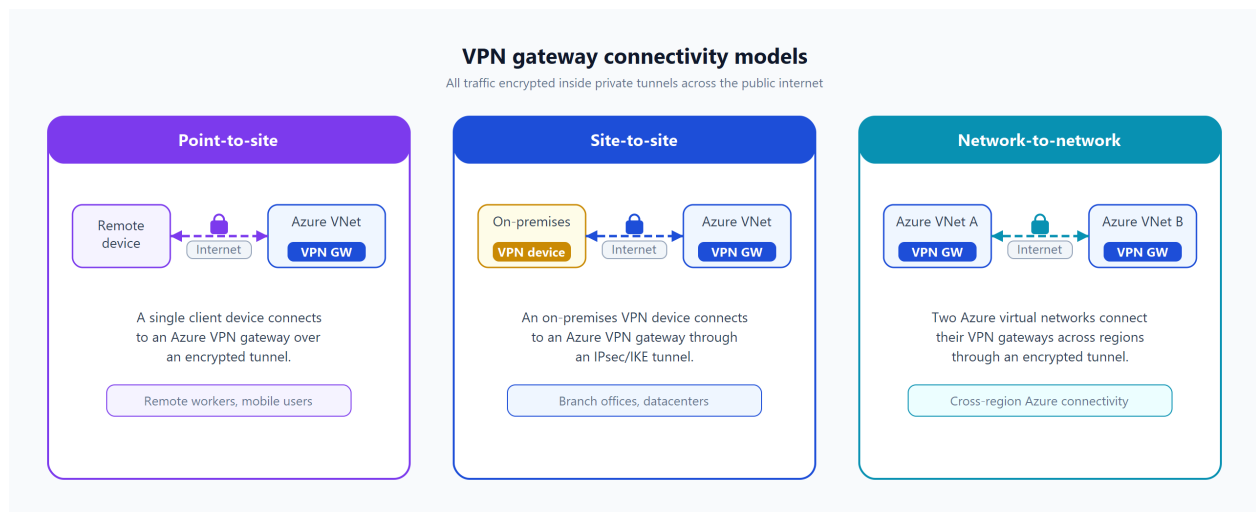
Describe Azure virtual private networks

Completed

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks. VPNs can enable networks to safely and securely share sensitive information.

VPN gateways

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in a dedicated subnet of the virtual network and enable the following connectivity:



- Connect on-premises datacenters to virtual networks through a site-to-site connection.
- Connect individual devices to virtual networks through a point-to-site connection.
- Connect virtual networks to other virtual networks through a network-to-network connection.

All data transfer is encrypted inside a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network. However, you can use one gateway to connect to multiple locations, which includes other virtual networks or on-premises datacenters.

When setting up a VPN gateway, you must specify the type of VPN - either policy-based or route-based. The primary distinction between these two types is how they determine which traffic needs encryption. In Azure, regardless of the VPN type, the method of authentication employed is a preshared key.

- Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel through which that packet is sent.
- In route-based gateways, IPsec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.

Use a route-based VPN gateway if you need any of the following types of connectivity:

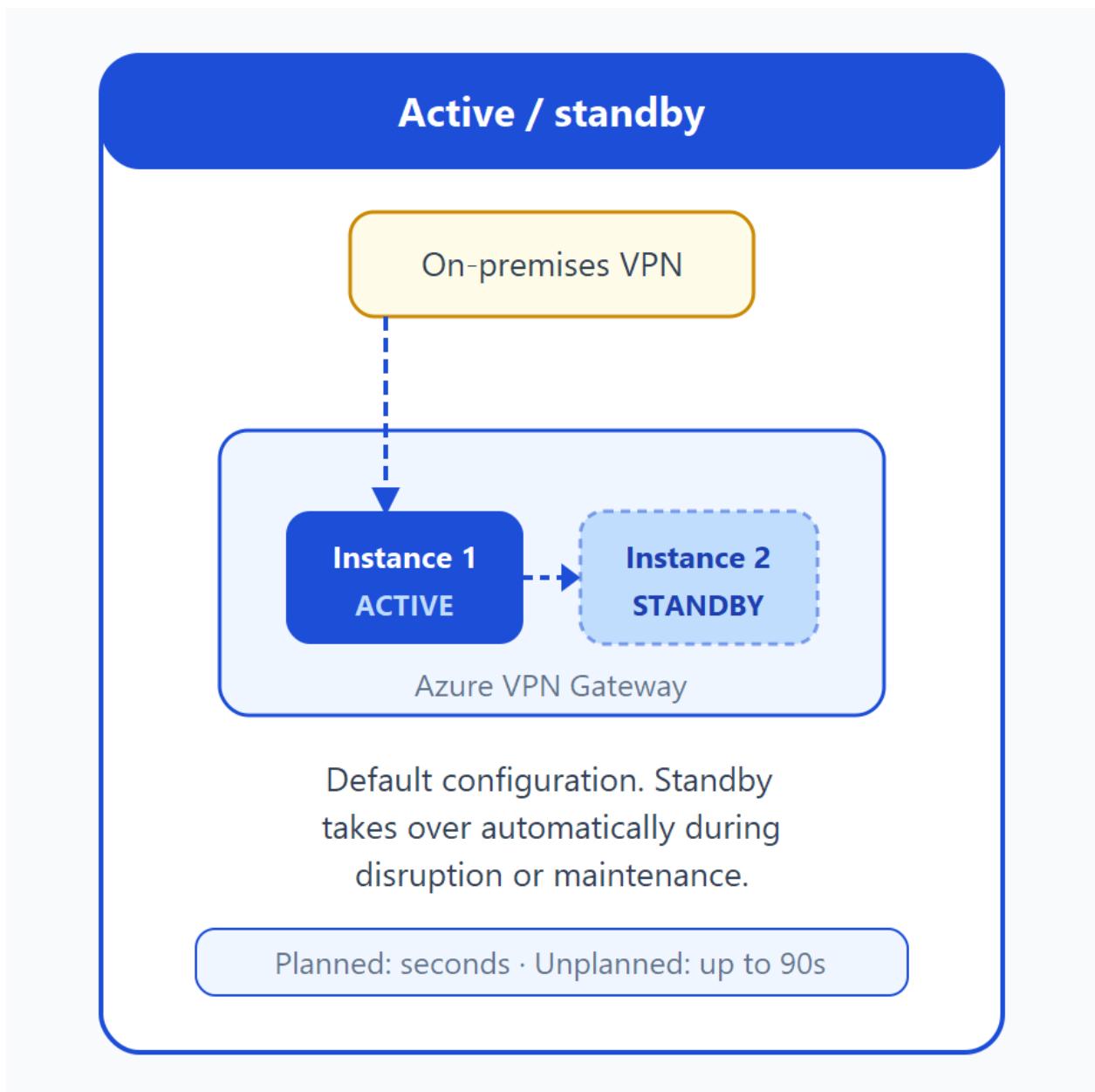
- Connections between virtual networks
- Point-to-site connections
- Multisite connections
- Coexistence with an Azure ExpressRoute gateway

High-availability scenarios

If you're configuring a VPN to keep your information safe, you also want to make sure it's a highly available and fault-tolerant VPN configuration. There are a few ways to maximize the resiliency of

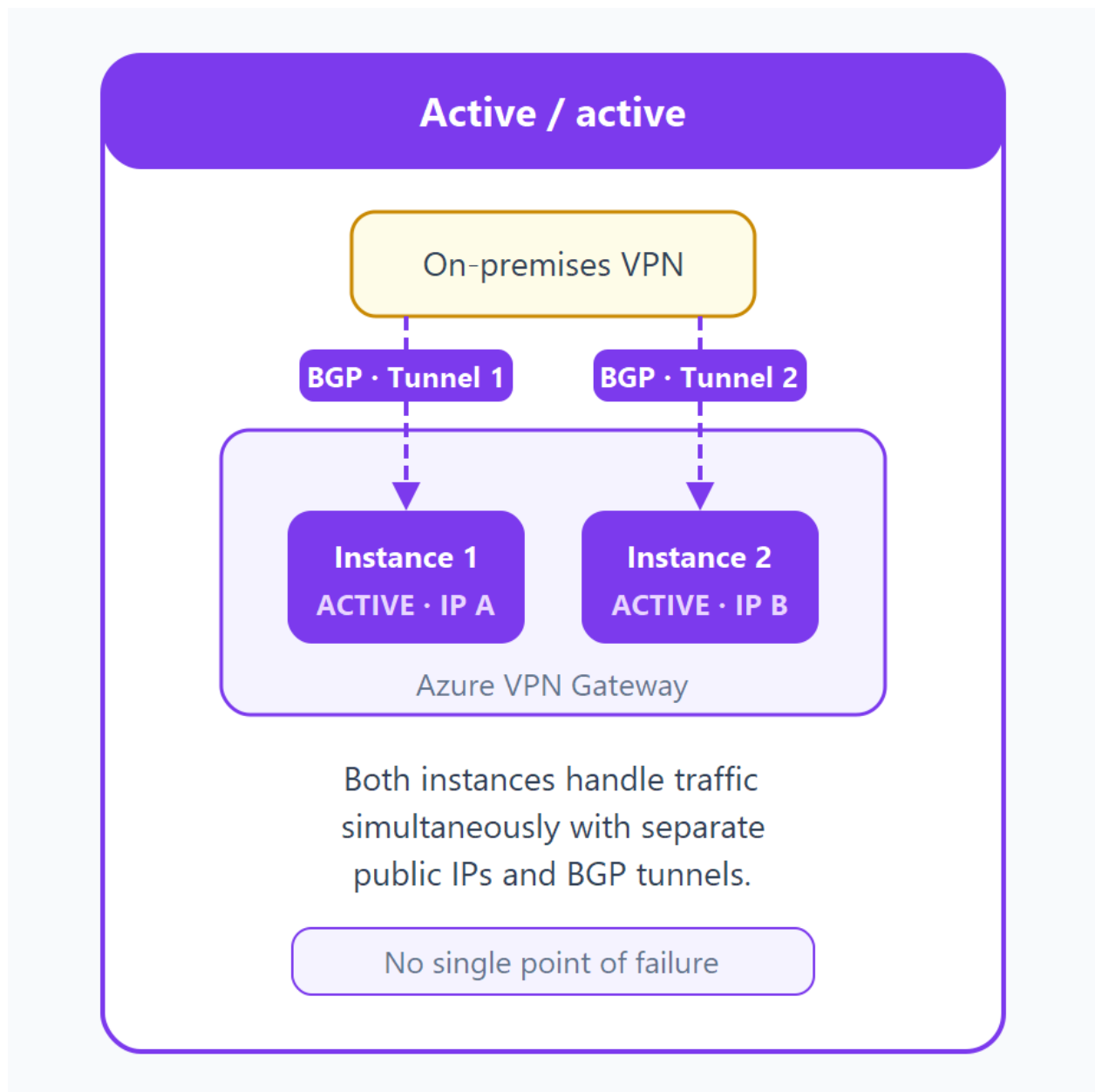
your VPN gateway.

Active/standby



By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure. When planned maintenance or unplanned disruption affects the active instance, the standby instance automatically assumes responsibility for connections without any user intervention. Connections are interrupted during this failover, but they're typically restored within a few seconds for planned maintenance and within 90 seconds for unplanned disruptions.

Active/active

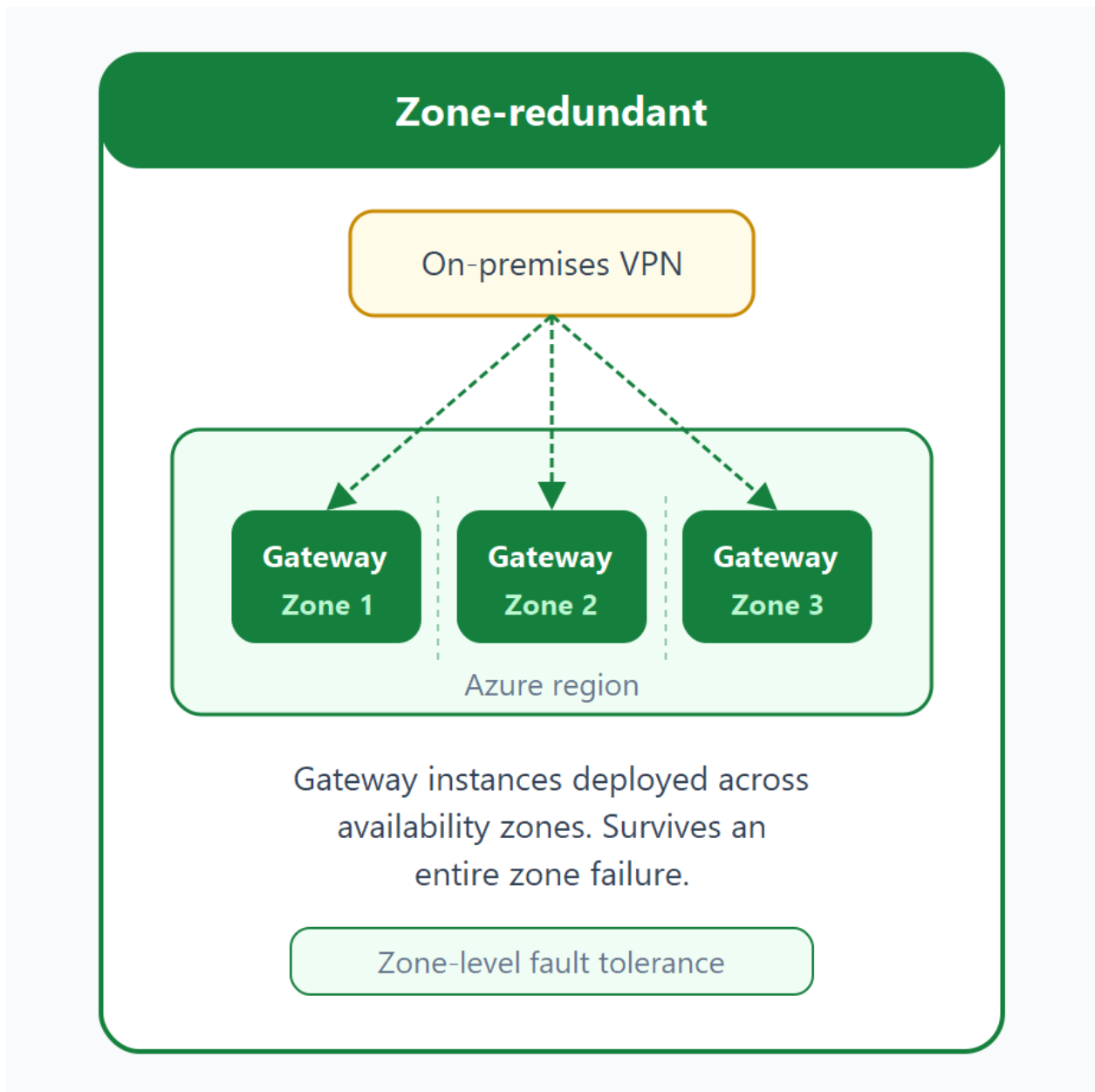


With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an active/active configuration. In this configuration, you assign a unique public IP address to each instance. You then create separate tunnels from the on-premises device to each IP address. You can extend the high availability by deploying an additional VPN device on-premises.

ExpressRoute failover

Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections. ExpressRoute circuits have resiliency built in. However, they aren't immune to physical problems that affect the cables delivering connectivity or outages that affect the complete ExpressRoute location. In high-availability scenarios, where there's risk associated with an outage of an ExpressRoute circuit, you can also provision a VPN gateway that uses the internet as an alternative method of connectivity. In this way, you can ensure there's always a connection to the virtual networks.

Zone-redundant gateways



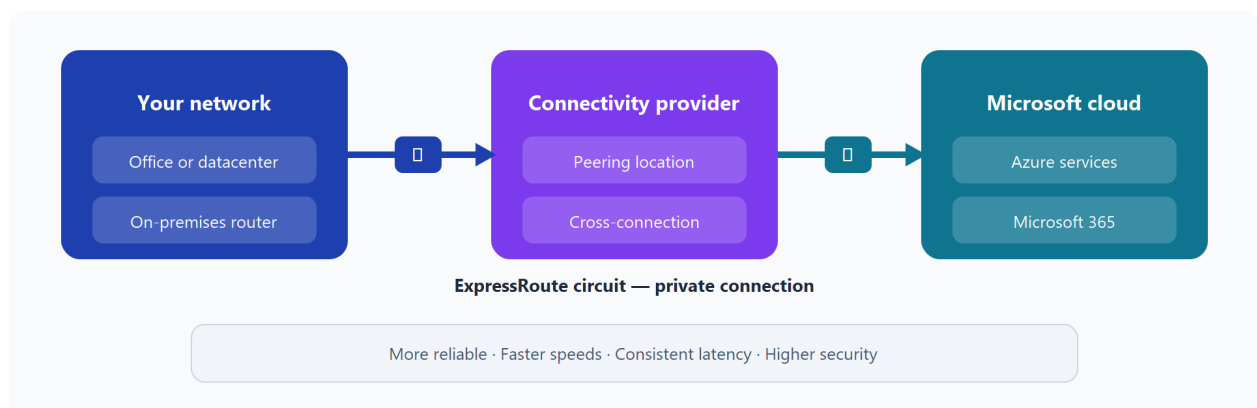
In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration. This configuration brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure availability zones physically and logically separates gateways within a region while protecting your on-premises network connectivity to Azure from zone-level failures. These gateways require different gateway stock keeping units (SKUs) and use Standard public IP addresses instead of Basic public IP addresses.

4. Describe Azure ExpressRoute

Describe Azure ExpressRoute

Completed

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider. This connection is called an ExpressRoute Circuit. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365. ExpressRoute lets you connect offices, datacenters, or other facilities to the Microsoft cloud. Each location would have its own ExpressRoute circuit.



Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public internet. Because they bypass the public internet, ExpressRoute connections offer more reliability, faster speeds, consistent latencies, and higher security than typical internet connections.

Features and benefits of ExpressRoute

There are several benefits to using ExpressRoute as the connection service between Azure and on-premises networks.

- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute Global Reach.
- Dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP).
- Built-in redundancy in every peering location for higher reliability.

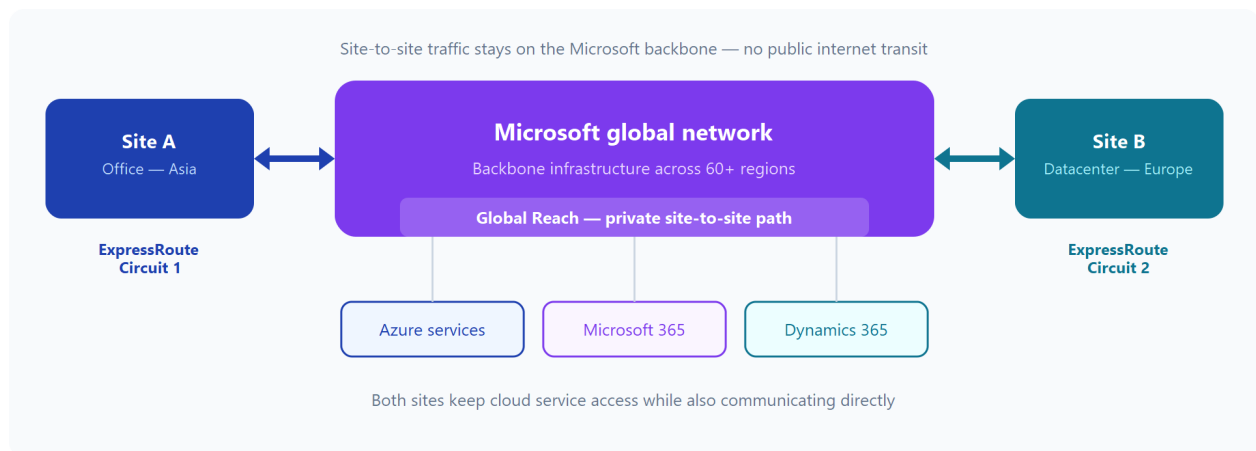
Connectivity to Microsoft cloud services

ExpressRoute enables direct access to the following services in all regions:

- Microsoft Office 365
- Microsoft Dynamics 365
- Azure compute services, such as Azure Virtual Machines
- Azure cloud services, such as Azure Cosmos DB and Azure Storage

Global connectivity

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, suppose you have an office in Asia and a datacenter in Europe, both with ExpressRoute circuits connecting them to the Microsoft network. You can use ExpressRoute Global Reach to connect those two facilities, allowing them to communicate without transferring data over the public internet.



Dynamic routing

ExpressRoute uses BGP to exchange routes between on-premises networks and resources running in Azure. This protocol enables dynamic routing between your on-premises network and services running in the Microsoft cloud.

Built-in redundancy

Each connectivity provider uses redundant devices to ensure that connections established with Microsoft are highly available. You can configure multiple circuits to complement this feature.

Connectivity model options

ExpressRoute supports several connectivity options depending on your provider and network design, including provider-based connectivity, point-to-point Ethernet, and direct connectivity at ExpressRoute locations. At this level, focus on when to use ExpressRoute rather than detailed implementation models.

At a high level, choose ExpressRoute when:

- You need private, consistent connectivity between on-premises networks and Azure.

- Your team has strict compliance or data-transfer requirements.
- You need predictable latency and high-throughput network performance.
- You want to avoid sending critical traffic over the public internet.

Security considerations

With ExpressRoute, your data doesn't travel over the public internet, reducing the risks associated with internet communications. ExpressRoute is a private connection from your on-premises infrastructure to your Azure infrastructure. Even if you have an ExpressRoute connection, DNS queries, certificate revocation list checking, and Azure Content Delivery Network requests are still sent over the public internet.

5. Describe Azure DNS

<https://learn.microsoft.com/en-us/training/modules/describe-azure-networking-services/5-domain-name-system>

Describe Azure DNS

Completed

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

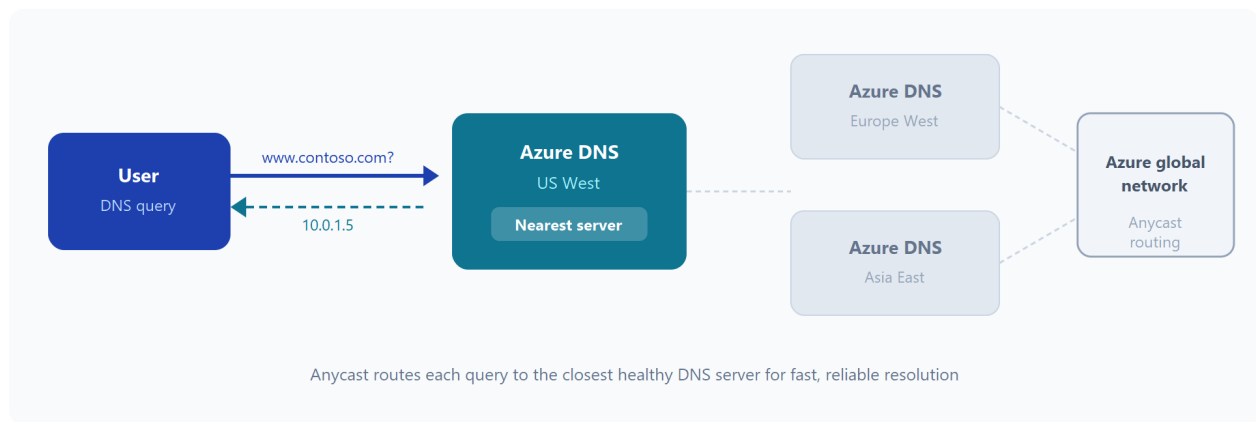
Benefits of Azure DNS

Azure DNS uses the scope and scale of Microsoft Azure to provide numerous benefits, including:

- Reliability and performance
- Security
- Ease of use
- Customizable virtual networks
- Alias records

Reliability and performance

DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers, providing resiliency and high availability. Azure DNS uses anycast networking, so the closest available DNS server answers each DNS query, providing fast performance and high availability for your domain.



Security

Azure DNS is based on Azure Resource Manager, which provides features such as Azure role-based access control (Azure RBAC), activity logs, and resource locks to help protect DNS resources and records.

Ease of use

Azure DNS can manage DNS records for your Azure services and provide DNS for your external resources as well. Azure DNS is integrated in the Azure portal and uses the same credentials, support contract, and billing as your other Azure services.

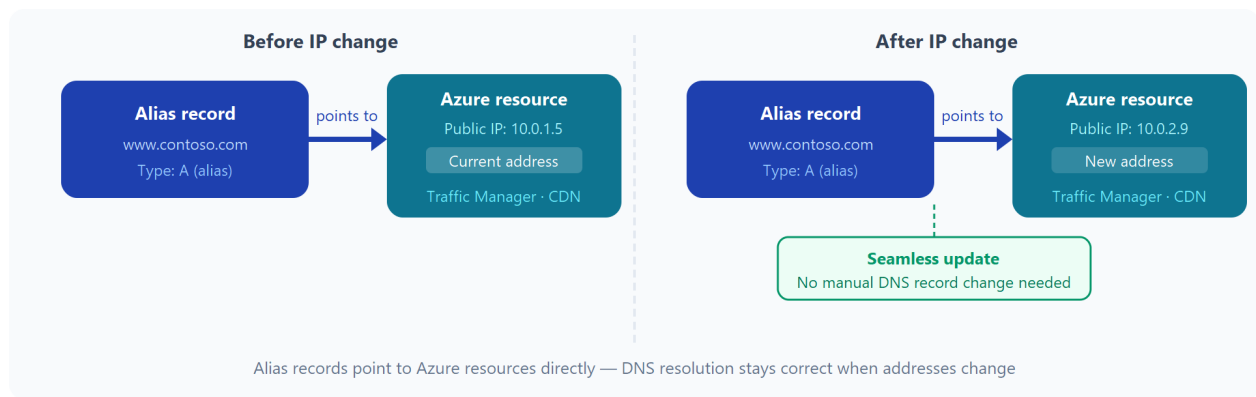
Because Azure DNS runs on Azure, you can manage your domains and records with the Azure portal, Azure PowerShell cmdlets, and the cross-platform Azure CLI. Applications that require automated DNS management can integrate with the service by using the REST API and SDKs.

Customizable virtual networks with private domains

Azure DNS also supports private DNS domains. This feature lets you use your own custom domain names in your private virtual networks instead of the Azure-provided names.

Alias records

Azure DNS also supports alias record sets. You can use an alias record set to refer to an Azure resource, such as an Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network (CDN) endpoint. If the IP address of the underlying resource changes, the alias record set seamlessly updates itself during DNS resolution. The alias record set points to the service instance, and the service instance is associated with an IP address.



Important

You can't use Azure DNS to buy a domain name. For an annual fee, you can buy a domain name by using App Service domains or a third-party domain name registrar. Once purchased, your domains can be hosted in Azure DNS for record management.

6. Module assessment

<https://learn.microsoft.com/en-us/training/modules/describe-azure-networking-services/6-knowledge-check>

Module assessment

Completed

7. Summary

<https://learn.microsoft.com/en-us/training/modules/describe-azure-networking-services/7-summary>

Summary

Completed

In this module, you learned how Azure networking services support secure and reliable connectivity. You reviewed virtual networking fundamentals, including segmentation with subnets and communication options through public and private endpoints.

You also explored VPN Gateway, ExpressRoute, and Azure DNS, and when each service is most appropriate. With these fundamentals, you can make better decisions about connectivity options for cloud-only and hybrid scenarios.

Learning objectives

You should now be able to:

- Describe Azure virtual networking, including subnets and endpoints.
- Describe connectivity options with Azure VPN Gateway.
- Describe when to use Azure ExpressRoute.
- Describe Azure DNS capabilities.
- Configure basic network access for an Azure resource.

Additional resources

- [Introduction to Azure network foundation services](#) is a Microsoft Learn course that provides deeper networking guidance in Azure.

Explore with Copilot

Tip

Try one of these prompts in Copilot Chat:

- "Design a secure hybrid connectivity plan that chooses between VPN Gateway and ExpressRoute, and explain the tradeoffs in cost, latency, and reliability."
- "Walk me through a DNS strategy for an app that has both internet-facing endpoints and private internal services in Azure."
- "Create a troubleshooting flowchart for a connectivity issue from on-premises users to an Azure workload, including likely root causes and checks."