What is Azure Virtual Network?

By asudbring

Archived: 2026-04-05 21:56:06 UTC

Azure Virtual Network provides the fundamental building block for your private network in Azure. This service enables Azure resources like virtual machines (VMs) to securely communicate with each other, the internet, and on-premises networks. Virtual networks deliver the scale, availability, and isolation benefits of Azure infrastructure while maintaining the familiar networking concepts you use in traditional datacenters.

Note

Azure Virtual Network is one of the services that make up the Network Foundations category in Azure. Other services in this category include Azure DNS and Azure Private Link. Each service has its own unique features and use cases. For more information on this service category, see Network Foundations.

Key scenarios that you can accomplish with a virtual network include:

- Communication of Azure resources with the internet.
- Communication between Azure resources.
- Communication with on-premises resources.
- Filtering of network traffic.
- Routing of network traffic.
- Integration with Azure services.

All resources in a virtual network can communicate outbound with the internet, by default. You can also use a public IP address, NAT gateway, or public load balancer to manage your outbound connections. You can communicate inbound with a resource by assigning a public IP address or a public load balancer.

When you're using only an internal standard load balancer, outbound connectivity isn't available until you define how you want outbound connections to work with an instance-level public IP address or a public load balancer.

Azure resources communicate securely with each other in one of the following ways:

- **Virtual network**: You can deploy VMs and other types of Azure resources in a virtual network. Examples of resources include App Service Environments, Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets. To view a complete list of Azure resources that you can deploy in a virtual network, see Deploy dedicated Azure services into virtual networks.

Note

To move a virtual machine from one virtual network to another, you must delete and recreate the virtual machine in the new virtual network. The virtual machine's disks can be retained for use in the new virtual machine.

- **Virtual network service endpoint**: You can extend your virtual network's private address space and the identity of your virtual network to Azure service resources over a direct connection. Examples of resources include Azure Storage accounts and Azure SQL Database. Service endpoints allow you to secure your critical Azure service resources to only a virtual network. To learn more, see Virtual network service endpoints.

- **Virtual network peering**: You can connect virtual networks to each other by using virtual peering. The resources in either virtual network can then communicate with each other. The virtual networks that you connect can be in the same, or different, Azure regions. To learn more, see Virtual network peering.

You can connect your on-premises computers and networks to a virtual network by using any of the following options:

- **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. This connection type is useful if you're just getting started with Azure, or for developers, because it requires few or no changes to an existing network. The communication between your computer and a virtual network is sent through an encrypted tunnel over the internet. To learn more, see About point-to-site VPN.

- **Site-to-site VPN**: Established between your on-premises VPN device and an Azure VPN gateway deployed in a virtual network. This connection type enables any on-premises resource that you authorize to access a virtual network. The communication between your on-premises VPN device and an Azure VPN gateway is sent through an encrypted tunnel over the internet. To learn more, see Site-to-site VPN.

- **Azure ExpressRoute**: Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic doesn't go over the internet. To learn more, see What is Azure ExpressRoute?

You can filter network traffic between subnets by using either or both of the following options:

- **Network security groups**: Network security groups and application security groups can contain multiple inbound and outbound security rules. These rules enable you to filter traffic to and from resources by source and destination IP address, port, and protocol. To learn more, see Network security groups and Application security groups.

- **Network virtual appliances**: A network virtual appliance is a virtual machine that performs a network function, such as a firewall or WAN optimization. To view a list of available network virtual appliances that you can deploy in a virtual network, go to Azure Marketplace.

Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the internet, by default. You can implement either or both of the following options to override the default routes that Azure creates:

- **Route tables**: You can create custom route tables that control where traffic is routed to for each subnet.
- **Border gateway protocol (BGP) routes**: If you connect your virtual network to your on-premises network by using an Azure VPN gateway or an ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks.

Integrating Azure services with an Azure virtual network enables private access to the service from virtual machines or compute resources in the virtual network. You can use the following options for this integration:

- Deploy dedicated instances of the service into a virtual network. The services can then be privately accessed within the virtual network and from on-premises networks.
- Use Azure Private Link to privately access a specific instance of the service from your virtual network and from on-premises networks.
- Access the service over public endpoints by extending a virtual network to the service, through service endpoints. Service endpoints allow service resources to be secured to the virtual network.

There are limits to the number of Azure resources that you can deploy. Most Azure networking limits are at the maximum values. However, you can increase certain networking limits. For more information, see Networking limits.

Virtual networks and subnets span all availability zones in a region. You don't need to divide them by availability zones to accommodate zonal resources. For example, if you configure a zonal VM, you don't have to take into consideration the virtual network when selecting the availability zone for the VM. The same is true for other zonal resources.

There's no charge for using Azure Virtual Network. It's free of cost. Standard charges apply for resources, such as VMs and other products. To learn more, see Virtual Network pricing and the Azure pricing calculator.

- Learn about Azure Virtual Network concepts and best practices
- Get started with using a virtual network by creating one, deploying a few VMs to it, and communicating between the VMs. To learn how, see the Use the Azure portal to create a virtual network quickstart.
- Follow a training module on designing and implementing core Azure networking infrastructure, including virtual networks: Introduction to Azure virtual networks.
