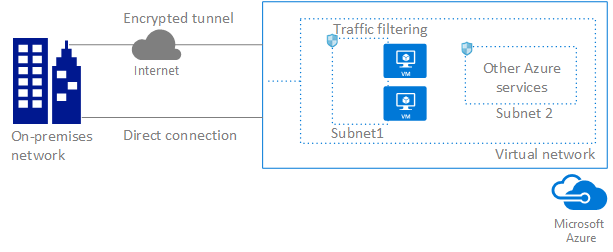
Azure Virtual Network

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with other in a virtual network. A virtual network is a representation of your own network in the cloud. A virtual network is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or to your on-premises network. The following picture shows some of the capabilities of the Azure Virtual Network service:3



To learn more about the following Azure Virtual Network capabilities, click the capability:

* [**Isolation:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#isolation) Virtual networks are isolated from one another. You can create separate virtual networks for development, testing, and production that use the same CIDR (10.0.0.0/0, for example) address blocks. Conversely, you can create multiple virtual networks that use different CIDR address blocks and connect the networks together. You can segment a virtual network into multiple subnets. Azure provides internal name resolution for resources deployed in a virtual network. If necessary, you can configure a virtual network to use your own DNS servers, instead of using Azure internal name resolution.
* [**Internet communication:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#internet) Resources, such as virtual machines deployed in a virtual network, have access to the Internet, by default. You can also enable inbound access to specific resources, as needed.
* [**Azure resource communication:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#within-vnet) Azure resources deployed in a virtual network can communicate with each other using private IP addresses, even if the resources are deployed in different subnets. Azure provides default routing between subnets, connected virtual networks, and on-premises networks, so you don't have to configure and manage routes. If desired, you can customize Azure's routing.
* [**Virtual network connectivity:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#connect-vnets) Virtual networks can be connected to each other, enabling resources in any virtual network to communicate with resources in any other virtual network.
* [**On-premises connectivity:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#connect-on-premises) A virtual network can be connected to an on-premises network, enabling resources to communicate between each other.
* [**Traffic filtering:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#filtering) You can filter network traffic to and from resources in a virtual network by source IP address and port, destination IP address and port, and protocol.
* [**Routing:**](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview#routing) You can optionally override Azure's default routing by configuring your own routes, or by propagating BGP routes through a network gateway.

Network isolation and segmentation

You can implement multiple virtual networks within each Azure [subscription](https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#subscription) and Azure [region](https://docs.microsoft.com/en-us/azure/azure-glossary-cloud-terminology?toc=%2fazure%2fvirtual-network%2ftoc.json#region). Each virtual network is isolated from other virtual networks. For each virtual network you can:

* Specify a custom private IP address space using public and private (RFC 1918) addresses. Azure assigns resources in a virtual network a private IP address from the address space you assign.
* Segment the virtual network into one or more subnets and allocate a portion of the virtual network's address space to each subnet.
* Use Azure-provided name resolution, or specify your own DNS server, for use by resources in a virtual network. To learn more about name resolution in virtual networks, see [Name resolution for resources in virtual networks](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-name-resolution-for-vms-and-role-instances) article.

1

Internet communication

All resources in a virtual network can communicate outbound to the Internet. By default, the private IP address of the resource is source network address translated (SNAT) to a public IP address selected by the Azure infrastructure. To learn more about outbound Internet connectivity, read the [Understanding outbound connections in Azure](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections?toc=%2fazure%2fvirtual-network%2ftoc.json#standalone-vm-with-no-instance-level-public-ip-address) article. To prevent outbound Internet connectivity, you can implement custom routes or traffic filtering.1

To communicate inbound to Azure resources from the Internet, or to communicate outbound to the Internet without SNAT, a resource must be assigned a public IP address. To learn more about public IP addresses, read the [Public IP addresses](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address) article.

Secure communication between Azure resources

You can deploy virtual machines within a virtual network. Virtual machines communicate with other resources in a virtual network through a network interface. To learn more about network interfaces, see [Network interfaces](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface).

You can also deploy several other types of Azure resources to a virtual network, such as Azure App Service Environments and Azure Virtual Machine Scale Sets. For a complete list of Azure resources you can deploy into a virtual network, see [Virtual network service integration for Azure services](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-for-azure-services).3

Some resources can't be deployed into a virtual network, but enable you to limit communication to resources within a virtual network only. To learn more about how to limit access to resources, see [Virtual network service endpoints](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview).

Connect virtual networks

You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other using virtual network peering. The bandwidth and latency of communication between resources in different virtual networks is the same as if the resources were in the same virtual network. To learn more about peering, read the [Virtual network peering](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview)article.

Connect to an on-premises network

You can connect your on-premises network to a virtual network using any combination of the following options:

* **Point-to-site virtual private network (VPN):** Established between a virtual network and a single PC in your network. Each PC that wants to establish connectivity with a virtual network must configure its connection independently. This connection type is great if you're just getting started with Azure, or for developers, because it requires little or no changes to your existing network. The connection uses the SSTP protocol to provide encrypted communication over the Internet between the PC and a virtual network. The latency for a point-to-site VPN is unpredictable, since the traffic traverses the Internet.
* **Site-to-site VPN:** Established between your VPN device and an Azure VPN Gateway deployed in a virtual network. This connection type enables any on-premises resource you authorize to access a virtual network. The connection is an IPSec/IKE VPN that provides encrypted communication over the Internet between your on-premises device and the Azure VPN gateway. The latency for a site-to-site connection is unpredictable, since the traffic traverses the Internet.
* **Azure ExpressRoute:** Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not traverse the Internet. The latency for an ExpressRoute connection is predictable, since traffic doesn't traverse the Internet.

1

To learn more about all the previous connection options, see [Connection topology diagrams](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways?toc=%2fazure%2fvirtual-network%2ftoc.json#diagrams).

Filter network traffic

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

* **Network security groups:** A network security group can contain multiple inbound and outbound security rules that enable you to filter traffic by source and destination IP address, port, and protocol. You can apply a network security group to each network interface in a virtual machine. You can also apply a network security group to the subnet a network interface, or other Azure resource, is in. To learn more about network security groups, see [Network security groups](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups).
* **Network virtual appliances:** A network virtual appliance is a virtual machine running software that performs a network function, such as a firewall. View a list of available network virtual appliances in the [Azure Marketplace](https://azuremarketplace.microsoft.com/marketplace/apps/category/networking?page=1&subcategories=appliances). Network virtual appliances are also available that provide WAN optimization and other network traffic functions. Network virtual appliances are typically used with user-defined or BGP routes. You can also use a network virtual appliance to filter traffic between virtual networks.

Route network traffic

Azure creates route tables that enable resources connected to any subnet in any virtual network to communicate with each other, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

* **User-defined routes:** You can create custom route tables with routes that control where traffic is routed to for each subnet. To learn more about user-defined routes, see [User-defined routes](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview#user-defined).
* **BGP routes:** If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate BGP routes to your virtual networks.