Vnet Peering vs VNet Gateway Differences

A virtual network is a virtual, isolated portion of the Azure public network. By default, traffic cannot be routed between two virtual networks. However, it's possible to connect virtual networks, either within a single region or across two regions, so that traffic can be routed between them.

**Virtual network connection types**

**Virtual network peering**. Virtual network peering connects two Azure virtual networks. Once peered, the virtual networks appear as one for connectivity purposes. Traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, through private IP addresses only. No public internet is involved. You can also peer virtual networks across Azure regions (global peering).

**VPN gateways**. A VPN gateway is a specific type of virtual network gateway that is used to send traffic between an Azure virtual network and an on-premises location over the public internet. You can also use a VPN gateway to send traffic between Azure virtual networks. Each virtual network can have at most one VPN gateway. You should enable [Azure DDOS Protection](https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview) on any perimeter virtual network.

Virtual network peering provides a low-latency, high-bandwidth connection. There is no gateway in the path, so there are no extra hops, ensuring low latency connections. It's useful in scenarios such as cross-region data replication and database failover. Because traffic is private and remains on the Microsoft backbone, also consider virtual network peering if you have strict data policies and want to avoid sending any traffic over the internet.

VPN gateways provide a limited bandwidth connection and are useful in scenarios where you need encryption but can tolerate bandwidth restrictions. In these scenarios, customers are also not as latency-sensitive.

**Gateway transit**

Virtual network peering and VPN Gateways can also coexist via gateway transit

Gateway transit enables you to use a peered virtual network's gateway for connecting to on-premises, instead of creating a new gateway for connectivity. As you increase your workloads in Azure, you need to scale your networks across regions and virtual networks to keep up with the growth. Gateway transit allows you to share an ExpressRoute or VPN gateway with all peered virtual networks and lets you manage the connectivity in one place. Sharing enables cost-savings and reduction in management overhead.

With gateway transit enabled on virtual network peering, you can create a transit virtual network that contains your VPN gateway, Network Virtual Appliance, and other shared services. As your organization grows with new applications or business units and as you spin up new virtual networks, you can connect to your transit virtual network using peering. This prevents adding complexity to your network and reduces management overhead of managing multiple gateways and other appliances.

**Comparison of virtual network peering and VPN Gateway**

Expand table

| **Item** | **Virtual network peering** | **VPN Gateway** |
| --- | --- | --- |
| Limits | Up to 500 virtual network peerings per virtual network (see [Networking limits](https://learn.microsoft.com/en-us/azure/azure-subscription-service-limits#networking-limits)). | One VPN gateway per virtual network. The maximum number of tunnels per gateway depends on the [gateway SKU](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku). |
| Pricing model | [Ingress/Egress](https://azure.microsoft.com/pricing/details/virtual-network/) | [Hourly + Egress](https://azure.microsoft.com/pricing/details/vpn-gateway/) |
| Encryption | [Azure Virtual Network Encryption](https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-encryption-overview) can be leveraged. | Custom IPsec/IKE policy can be applied to new or existing connections. See [About cryptographic requirements and Azure VPN gateways](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-compliance-crypto). |
| Bandwidth limitations | No bandwidth limitations. | Varies based on SKU. See [Gateway SKUs by tunnel, connection, and throughput](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#benchmark). |
| Private? | Yes. Routed through Microsoft backbone and private. No public internet involved. | Public IP involved, but routed through Microsoft backbone if [Microsoft global network](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/routing-preference-overview) is enabled. |
| Transitive relationship | Peering connections are non-transitive. Transitive networking can be achieved using NVAs or gateways in the hub virtual network. See [Hub-spoke network topology](https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/hub-spoke) for an example. | If virtual networks are connected via VPN gateways and BGP is enabled in the virtual network connections, transitivity works. |
| Initial setup time | Fast | ~30 minutes |
| Typical scenarios | Data replication, database failover, and other scenarios needing frequent backups of large data. | Encryption-specific scenarios that are not latency sensitive and do not need high throughout. |