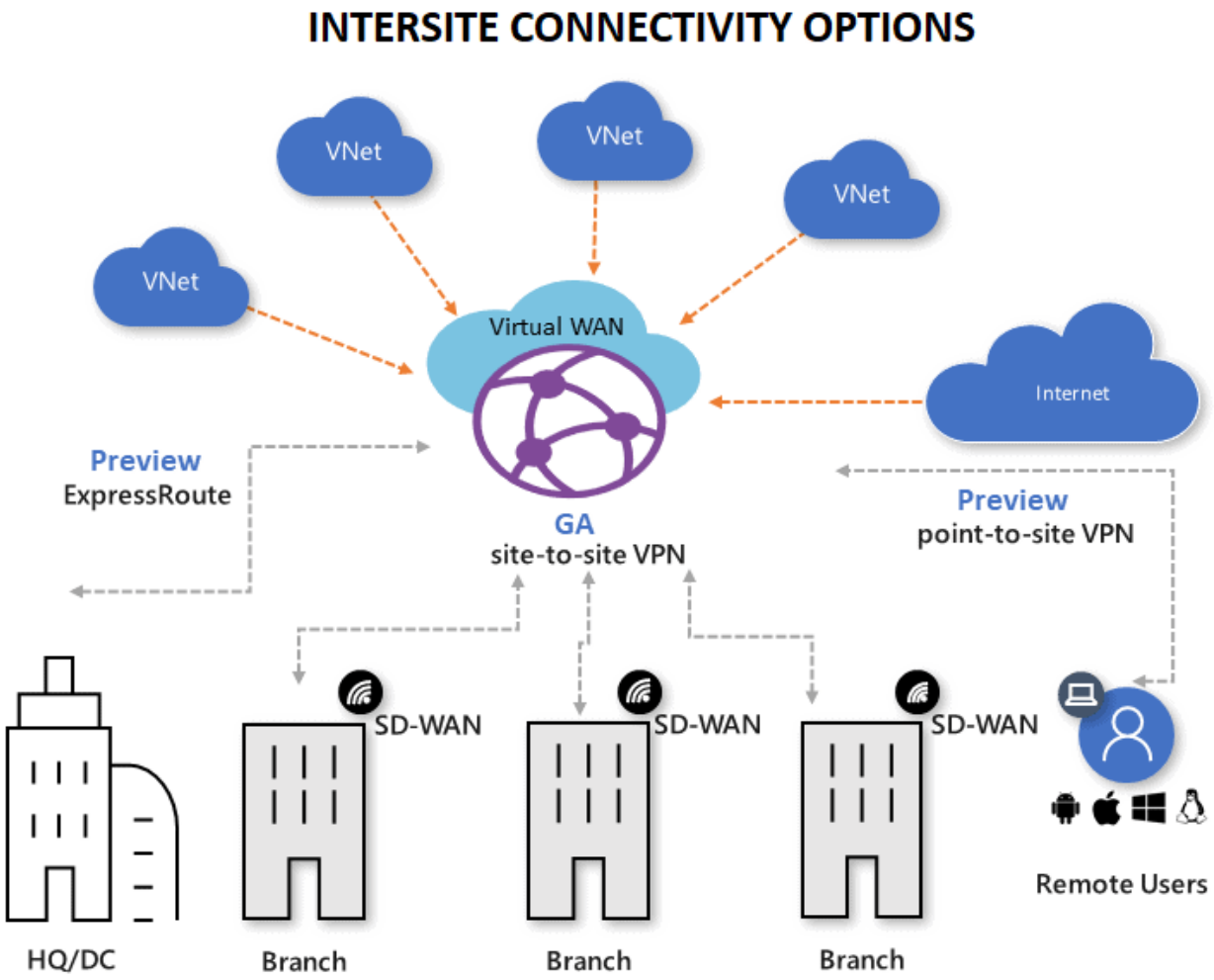
# Azure Intersite Connectivity

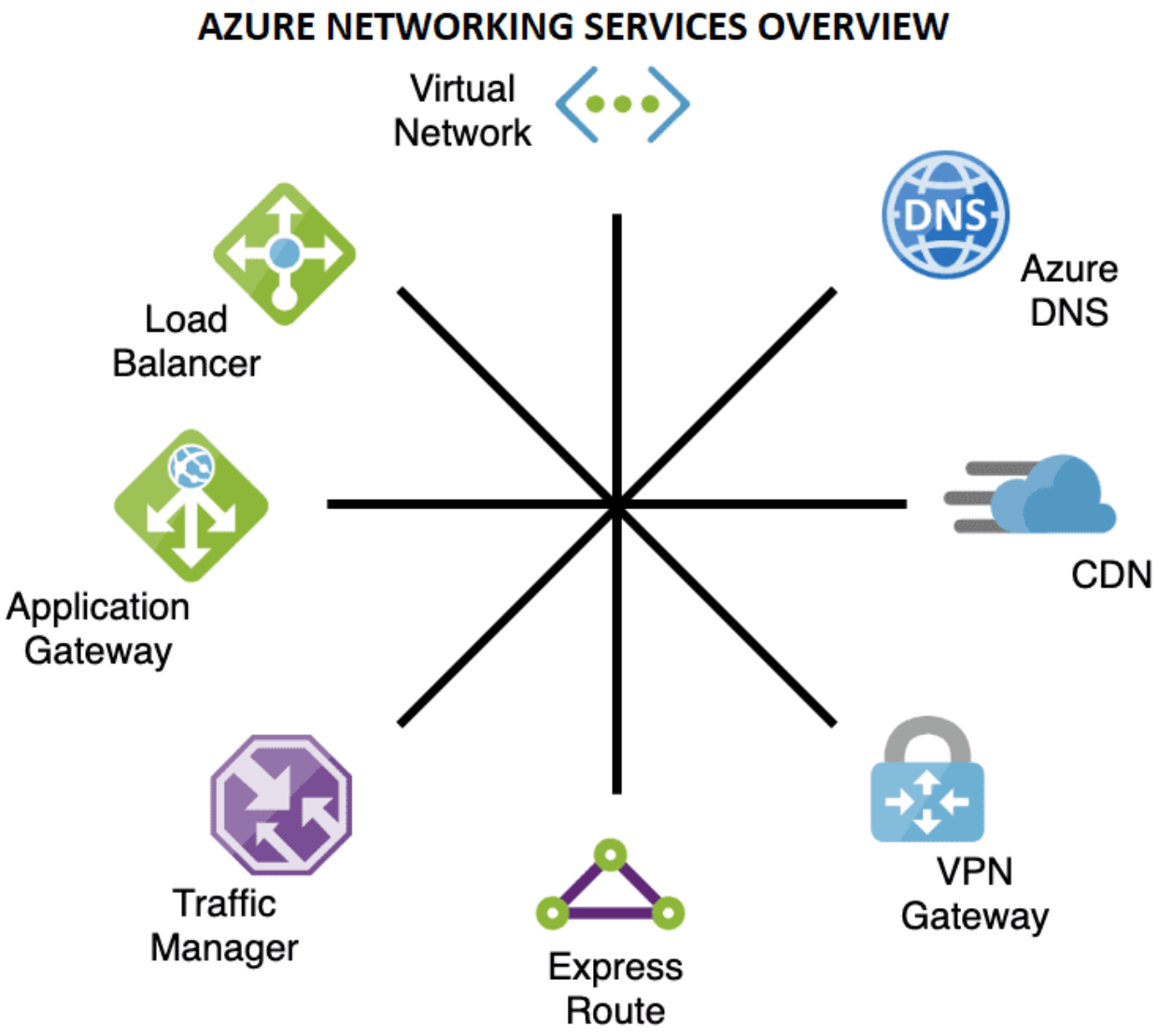
An Azure provides the ability to communicate with different virtual networks and the ability to transfer data across Azure subscriptions, deployment models, and Azure regions.




## Azure Networking Services Overview

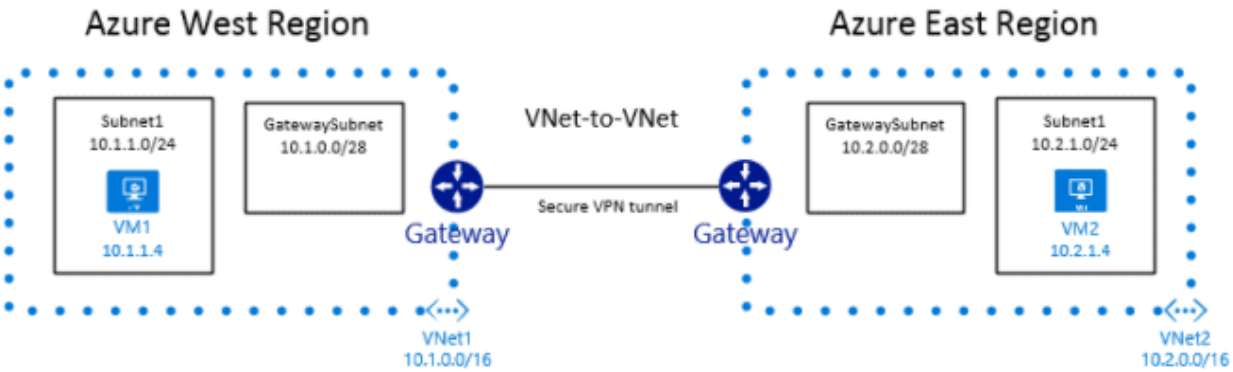
The networking services in Azure provide a variety of networking capabilities that can be used together or separately.

- **Connectivity Services:** Connect Azure resources and on-premises resources using any or a combination of these networking services in Azure – ExpressRoute, Peering service, virtual WAN, etc.,
- **Application Protection Services:** Protect your applications using any or a combination of these networking services in Azure – Load Balancer, Firewall, Network Security Groups, etc.,
- **Application Delivery Services:** Deliver applications in the Azure network using any or a combination of these networking services in Azure – Traffic Manager, Application Gateway, Load Balancer, etc.,
- **Network monitoring:** Monitor your network resources using any or a combination of these networking services in Azure – Network Watcher, ExpressRoute Monitor, etc.




## VNet-TO-VNet Connection

VNet-to-VNet connection is a simple way to connect two Virtual Networks. When you connect a virtual network to another virtual network with a VNet-to-VNet connection type (VNet2VNet), it's **similar** to creating a Site-to-Site IPsec connection to an on-premises location.




## VNet Peering

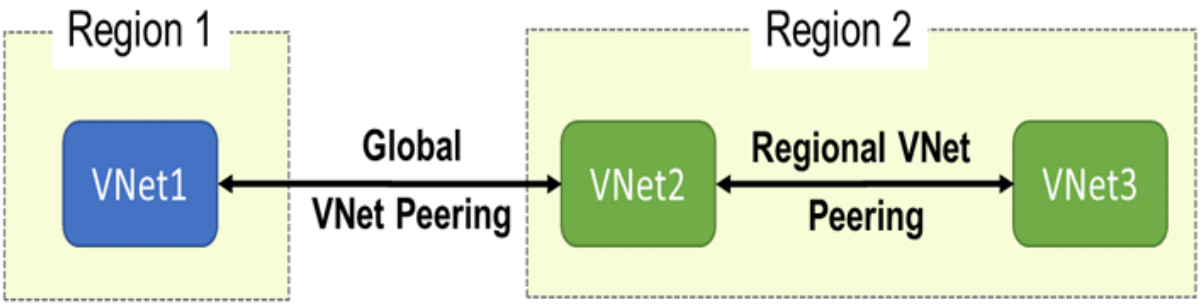
Virtual network peering enables us to connect two VNet in the same or across regions. If both of the virtual networks are in Azure and also within the same region, then you can use **peering.** Due to this, the workload in those virtual machines can communicate with each other.

- Once peered, the virtual networks appear as one, for connectivity purposes.
- Traffic remains private between VNet, it's kept on Microsoft's **backbone** network.

**Two types of Vnet Peering:**

- **Regional Vnet peering** connects Azure virtual networks in the same region.
- **Global Vnet peering** connects Azure virtual networks in different regions.


**Q1: Can we peer the VNet with a VNet in a different subscription?**
Ans. Yes. You can peer virtual networks (VNets) across subscriptions and across regions.
**Q2: Can we peer two VNets with matching or overlapping address ranges?**
Ans. No. Address spaces must not overlap to enable VNet Peering.
**Q3: Can we create a peering connection to a VNet in a different region?**
Ans. Yes. **Global VNet peering** enables you to peer VNet in different regions. Global VNet peering is available in all Azure public regions, China cloud regions, and Government cloud regions. You cannot globally peer from Azure public regions to national cloud regions.

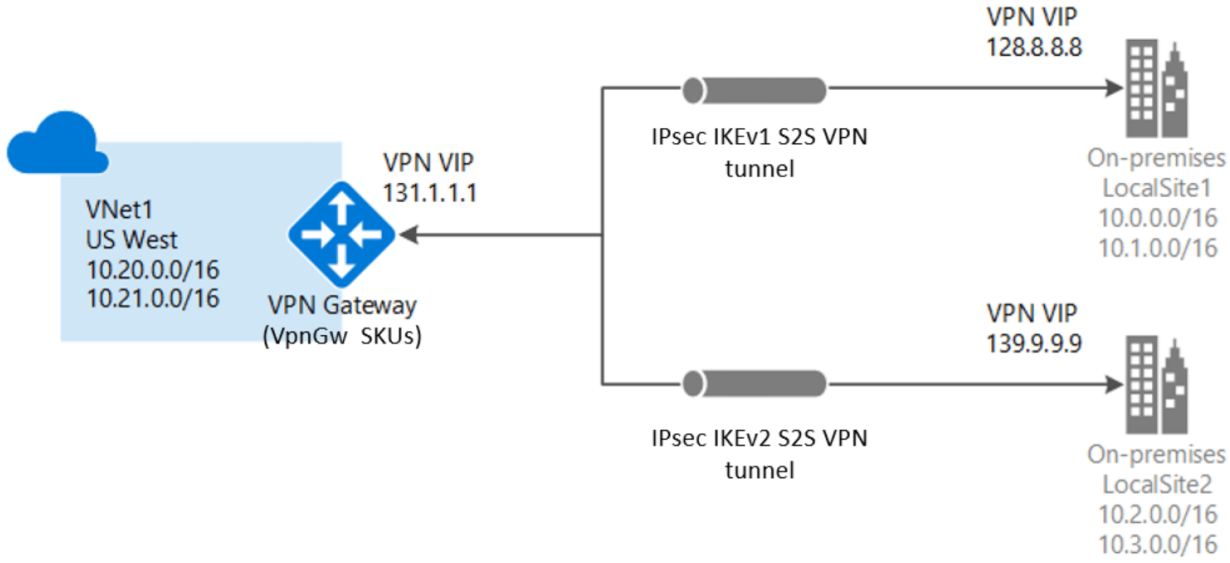



**Q4: Does peering will be a good option for end-users?**
Ans. Peering typically produces a more **direct path** between two networks, thereby reducing the distance that data have to travel. The result is **lower latency** and improved user experience.
**Q5: If we peer VNetA to VNetB and I peer VNetB to VNetC, does that mean VNetA and VNetC are peered?**
Ans. No. **Transitive** peering is not supported. You must peer VNetA and VNetC for this to take place.
If we have 3 VNets peered with each other; example A <> B <> C. We want Azure VM in A Vnet to talk to Azure VM in C Vnet then it won't work; because A and C VNet have not peered directly to each other; but through B Vnet.Fact that VM in A VNet not able to reach VM in C Vnet is called as **"Transitive Routing Problem".**

**Q6: Are there any bandwidth limitations for peering connections?**
Ans. No. VNet peering, whether local or global, does not impose any bandwidth restrictions. Bandwidth is **only** limited by the VM or the compute resource.

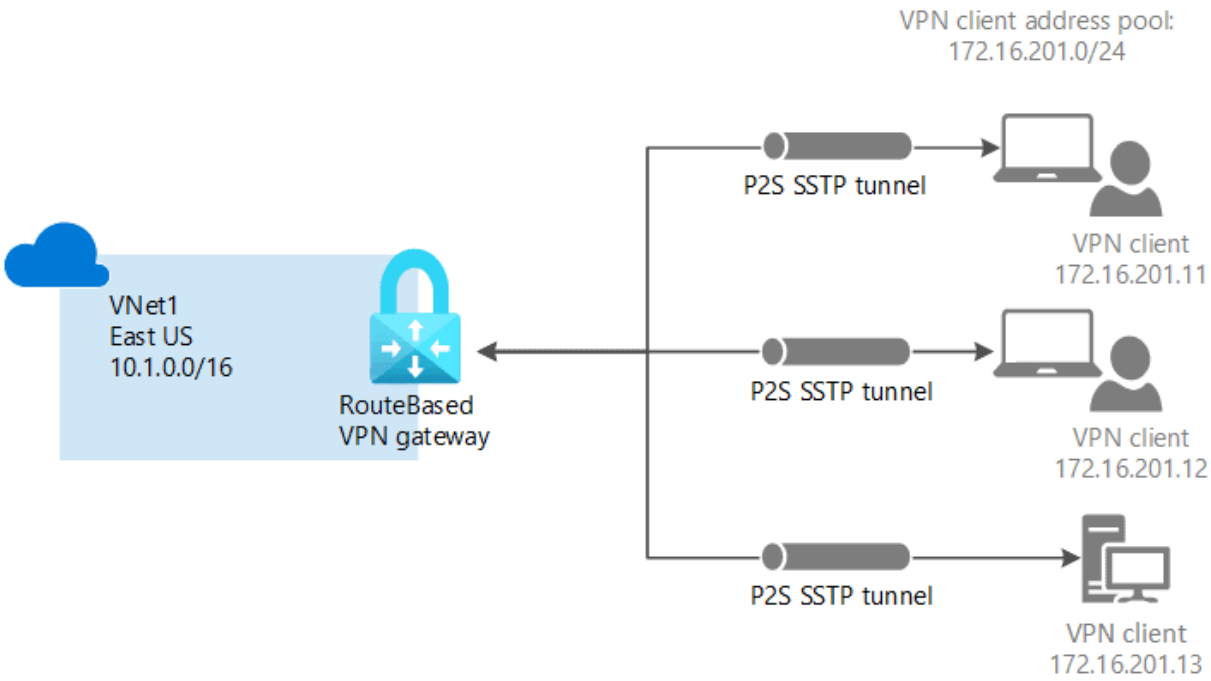
## Azure Network Gateways

A **VPN gateway** is a specific type of virtual network gateway, which is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet. VPN gateway act as a **middle man** on both sides of the virtual networks. And if the workloads in those virtual networks need to communicate with each other, they will communicate via this encrypted channel of communication between the VPN gateways of both virtual networks.



## Point-to-Site Connection

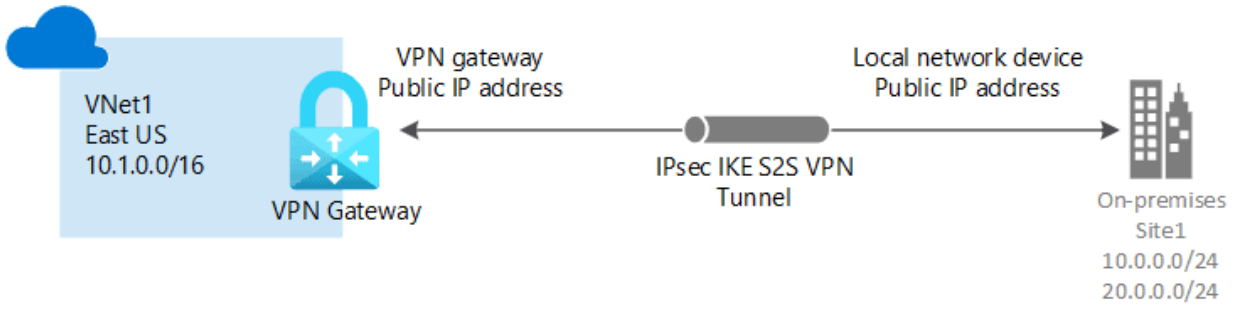
A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an **individual** client computer. A P2S connection is established by starting it from the client's computer.




## Site-to-Site Connection

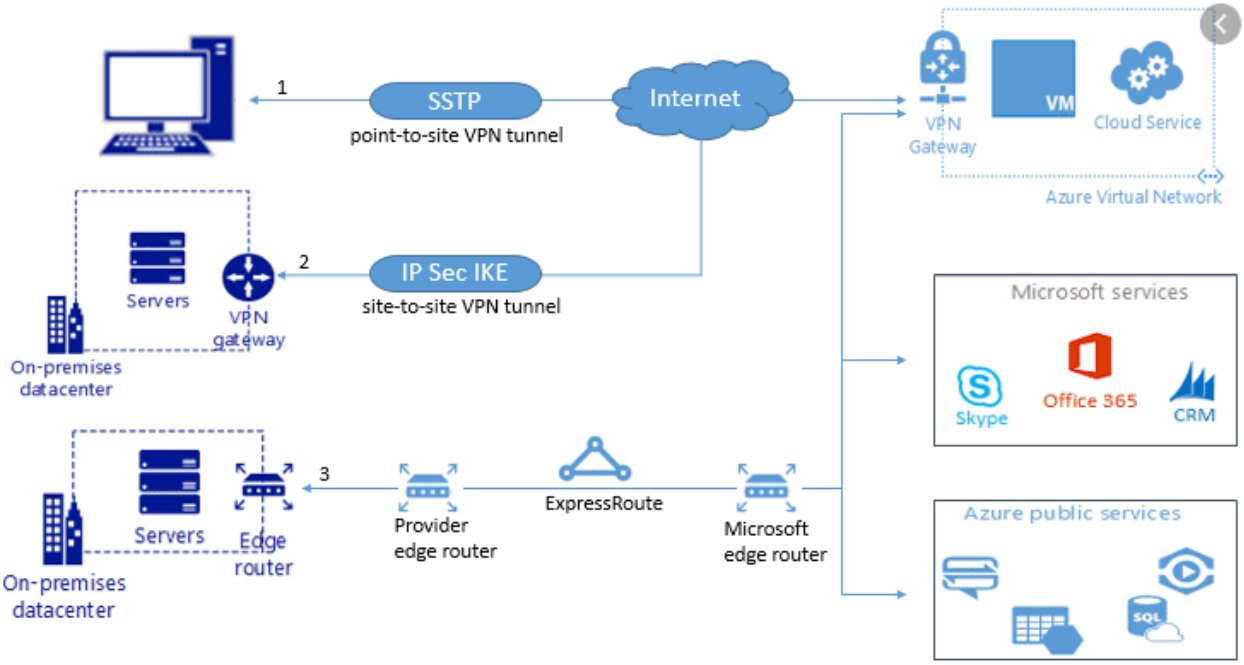
If we have an on-premises virtual network, and we may have other virtual networks existing in other cloud providers. To **connect** to our virtual network in Azure with the network that is an on-premises data center, we can use a Site-to-site VPN.

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an **externally** facing public IP address assigned to it.




**Q7: Does site to site is mostly on-premise to Azure?**

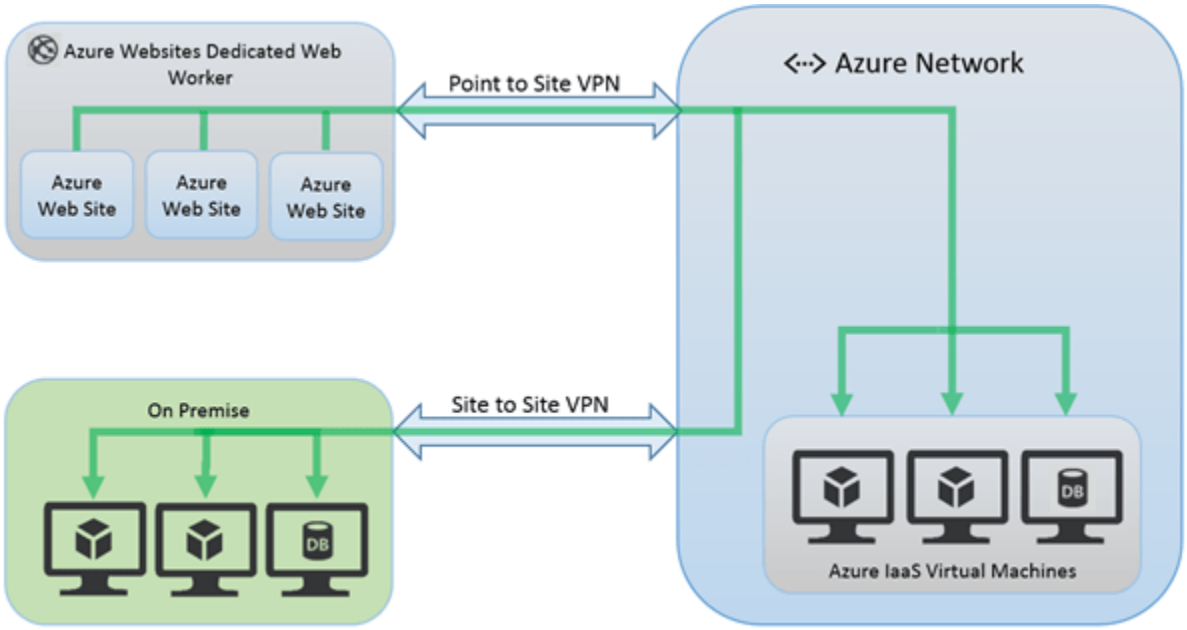
Ans. **Yes,** a Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.




**Q8: What is the difference between point-to-site and site-to-site?**

Ans. In point-to-site, you have to connect to the network you want to access **manually.** Usually, if you log off or restart the workstation it loses connection, and you have to reconnect every time. It's common to use this type of VPN when we are working remotely, and we need to access our company assets. The channel is bi-directional, but it's **1-to-many.**

Site-to-site is used when you want to connect two networks and keep the communication up all the time. It's also bi-directional, but it's **many-to-many** and stays up no matter if your server/workstation is running or not because the connection is established through a network gateway and not from the computer operating system.

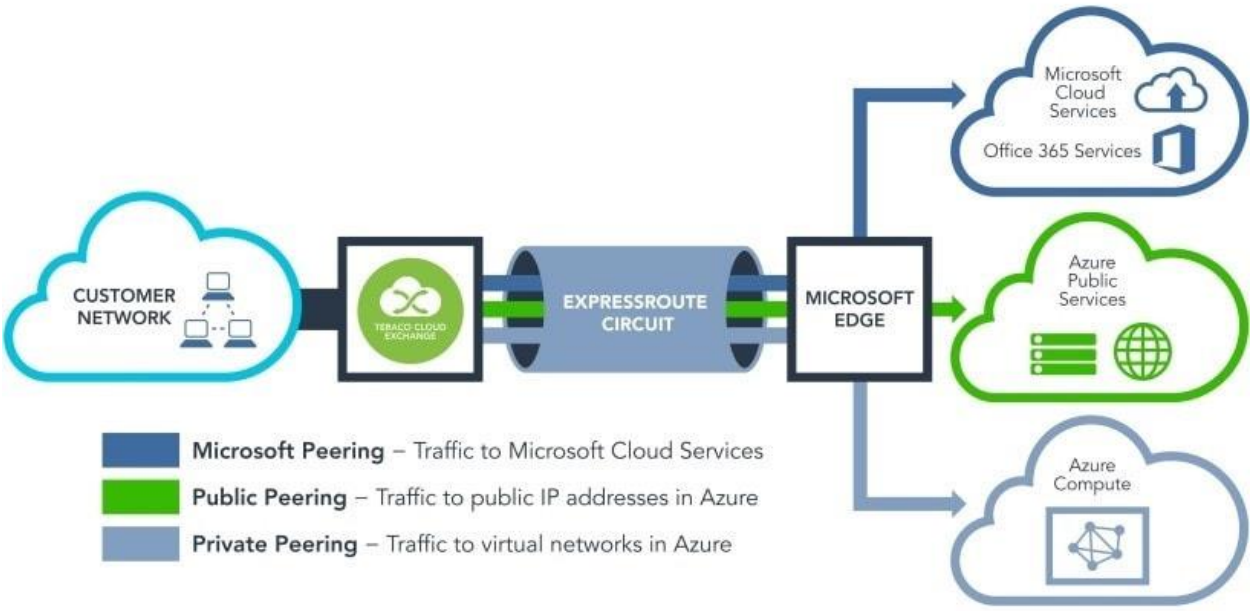


## ExpressRoute

ExpressRoute is an Azure service that lets you create **private** connections between Microsoft datacenters and infrastructure that's on your premises or in a colocation facility.
ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the **help** of a connectivity provider. With ExpressRoute, you can **establish** connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.
There are **similar services** with different **terms** as Azure ExpressRoutes provided by other **Cloud providers:**
**Amazon Web Services –** AWS **Direct Connect** is a cloud service solution that makes it easy to establish a dedicated network connection from your premise to AWS.

**Google Cloud Platform –** GCP **Dedicated Interconnect** provides direct physical connections between your on-premises network and Google's network.

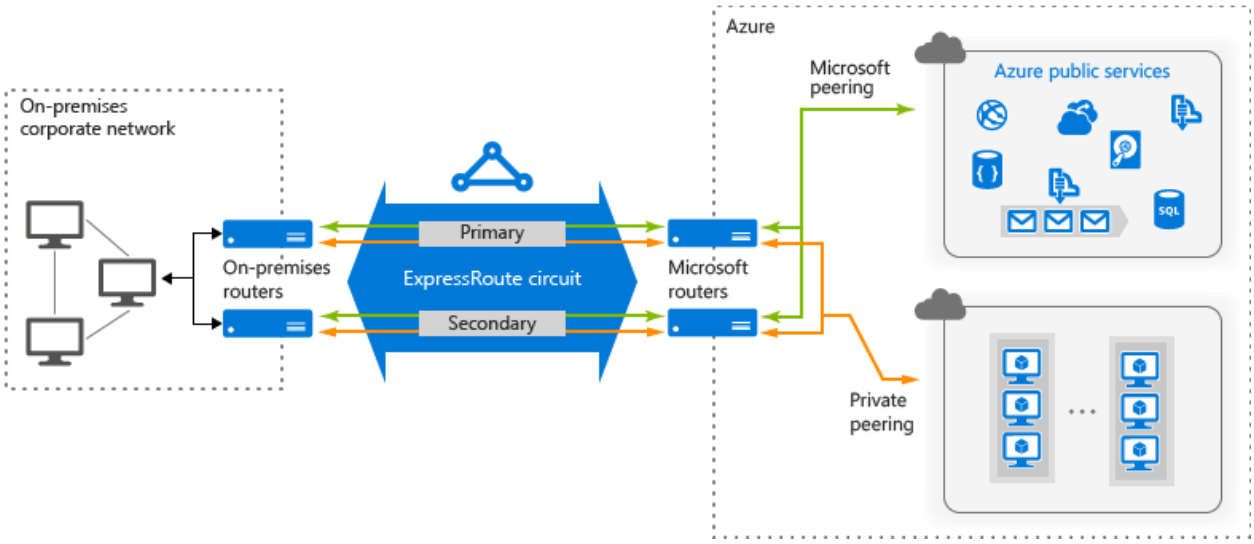
**Oracle Cloud Infrastructure –** Oracle Cloud Infrastructure **FastConnect** provides an easy way to create a dedicated, private connection between your data center and Oracle Cloud Infrastructure. FastConnect provides higher-bandwidth options, and a more reliable and consistent networking experience compared to internet-based connections.



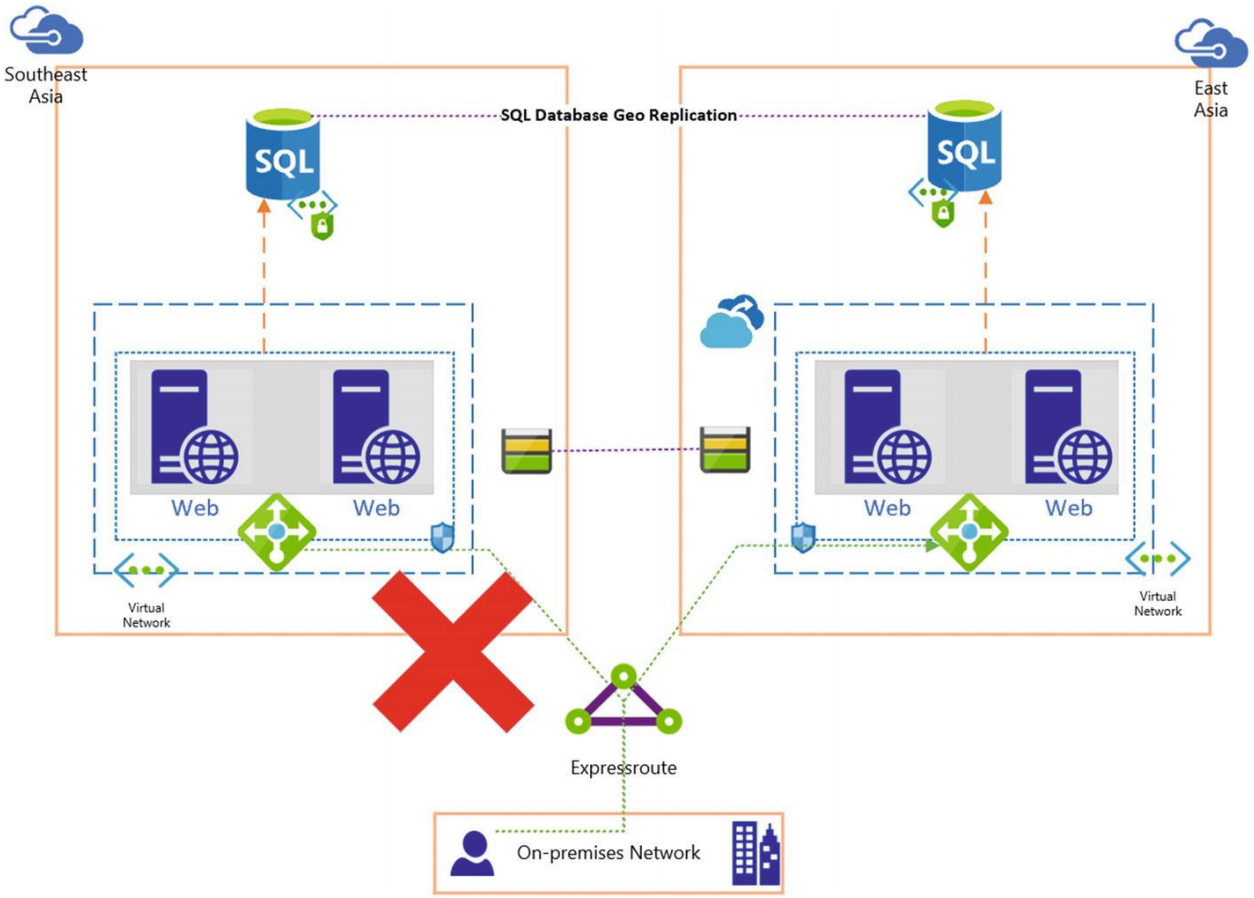

## Interconnect Microsoft Azure ExpressRoute With Oracle Cloud FastConnect

In June 2019, Microsoft announced a cloud interoperability collaboration with Oracle that will enable its customers to migrate and run enterprise workloads across Microsoft Azure and Oracle Cloud.

**Q9: What are the benefits of using ExpressRoute and private network connections?**
Ans. ExpressRoute connections don't go over the public Internet. They offer **higher security, reliability,** and **speeds,** with lower and consistent latencies than typical connections over the Internet. In some cases, using ExpressRoute connections to transfer data between on-premises devices and Azure can yield significant cost benefits.




**Q10: Will we lose connectivity if one of our ExpressRoute links fails?**
Ans. You will not lose connectivity if one of the cross-connections fails. A redundant connection is available to **support** the load of your network and provide high availability of your ExpressRoute circuit. You can additionally **create** a circuit in a different peering location to achieve circuit-level resilience.



## Availability Set

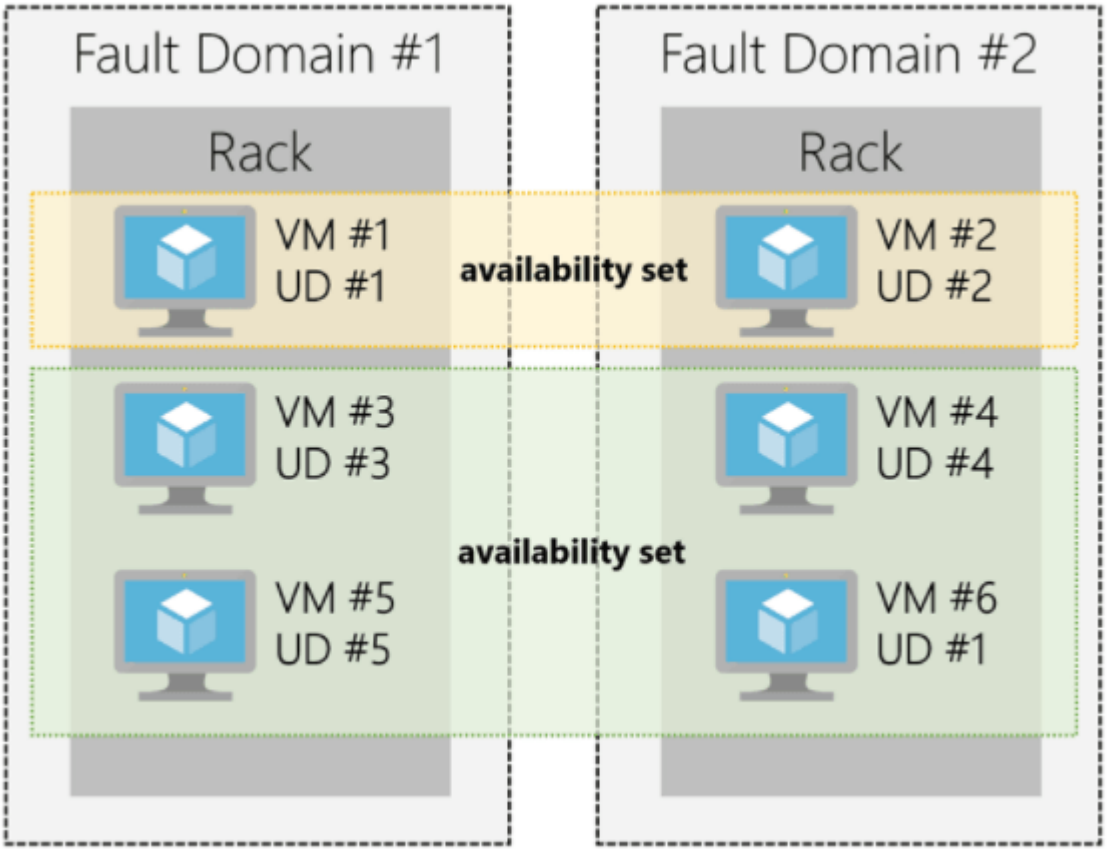
**Availability Set** is a logical grouping capability for isolating VM resources from each other when they're deployed. By deploying your VMs across multiple hardware **nodes** Azure ensures that if hardware or software **failure** happens within Azure, only a sub-set of your virtual machines is impacted and your overall solution is safe and in working condition.
It provides redundancy for your virtual machines. An Availability set **spreads** your virtual machines across multiple **fault domains** and **update domains.**

**Fault Domain**

- Azure Fault domains define the group of virtual machines that share a common power source and network switch.
- Each and every fault domain contains some racks and each rack contains a virtual machine.
- All the resources in the fault domain become unavailable when there is a failure in the fault domain.

**Update Domain**

- Virtual machines get update domains automatically once they are put inside the availability set.
- All virtual machines within that update domain will reboot together.
- They are used for the patching of virtual machines.
- Only one update domain can be updated at a time.




**Q11: What is the main advantage of an availability set?**
Ans. Availability set provides redundancy for your virtual machines. Availability set spreads your virtual machines across multiple fault domains and update domains. If you want to leverage Microsoft's **99.95%** SLA from Microsoft you must place your VMs inside the availability set except your VMs are having **premium** storage.

**Q12: What is the maximum number of virtual machines we can have in an Azure Availability Set?**

Ans. The max is **200** virtual machines per availability set, which is the same number of virtual machines that can be in a single cloud service. However, note that all virtual machines must **reside** in the same cloud service and therefore the same Azure scale unit (cluster).