What is VPN Gateway?

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.
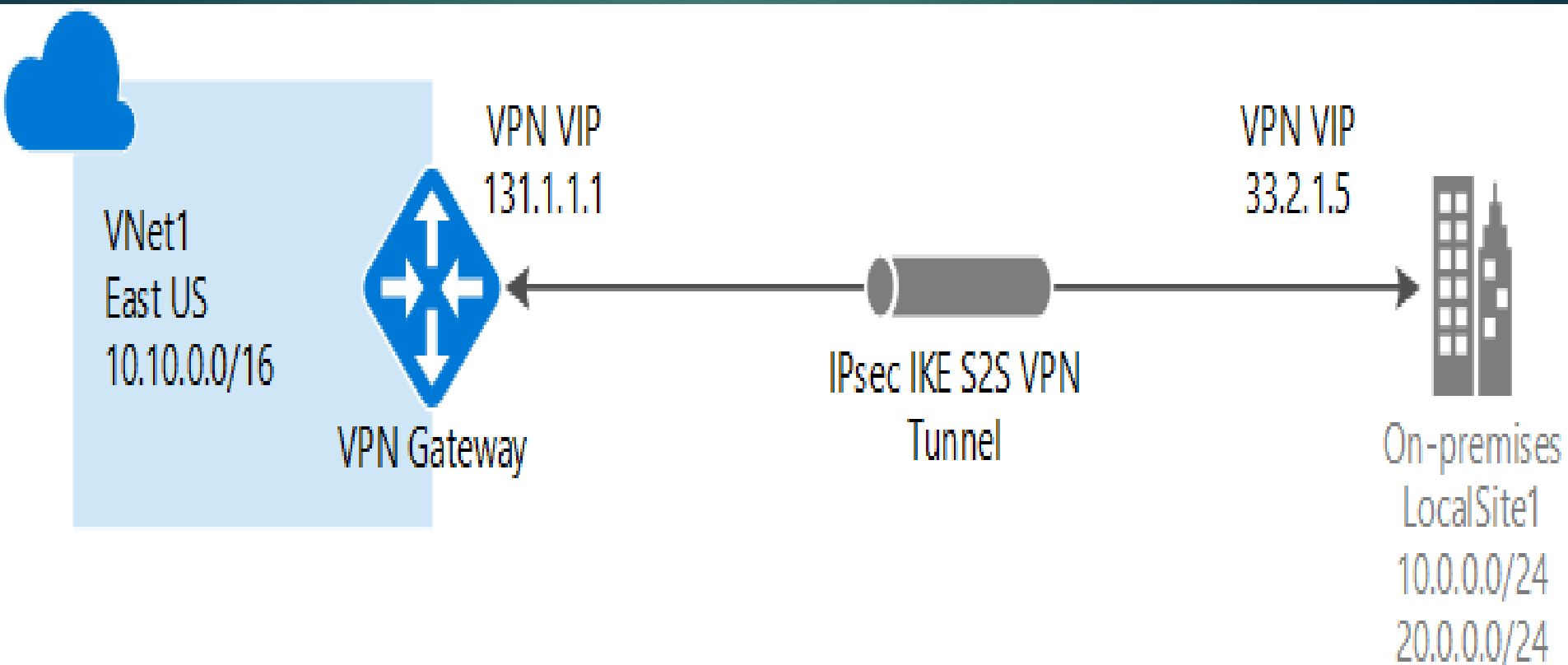
You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.

Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway.

When you create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

Site-to-Site and Multi-Site (IPsec/IKE VPN tunnel)

Site-to-Site

A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. S2S connections can be used for cross-premises and hybrid configurations. A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it and is not located behind a NAT.

VNet1
East US
10.10.0.0/16

VPN VIP
131.1.1.1

VPN Gateway

IPsec IKE S2S VPN
Tunnel

VPN VIP
33.2.1.5

On-premises
LocalSite1
10.0.0.0/24
20.0.0.0/24

Multi-Site

This type of connection is a variation of the Site-to-Site connection. You create more than one VPN connection from your virtual network gateway, typically connecting to multiple on-premises sites.

When working with multiple connections, you must use a RouteBased VPN type (known as a dynamic gateway when working with classic VNets).

Because each virtual network can only have one VPN gateway, all connections through the gateway share the available bandwidth.
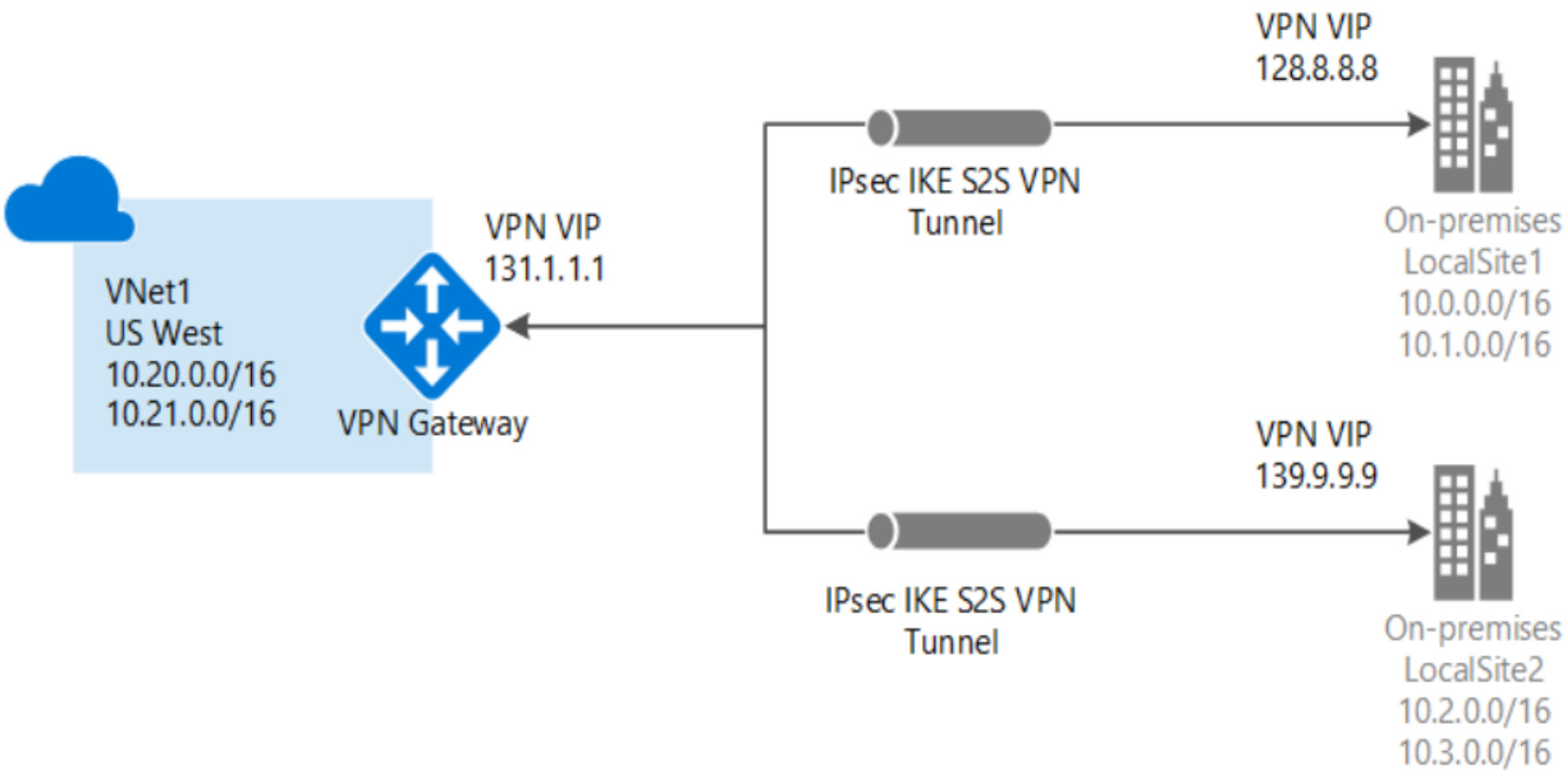
Point-to-Site VPN

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 computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference.

P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.
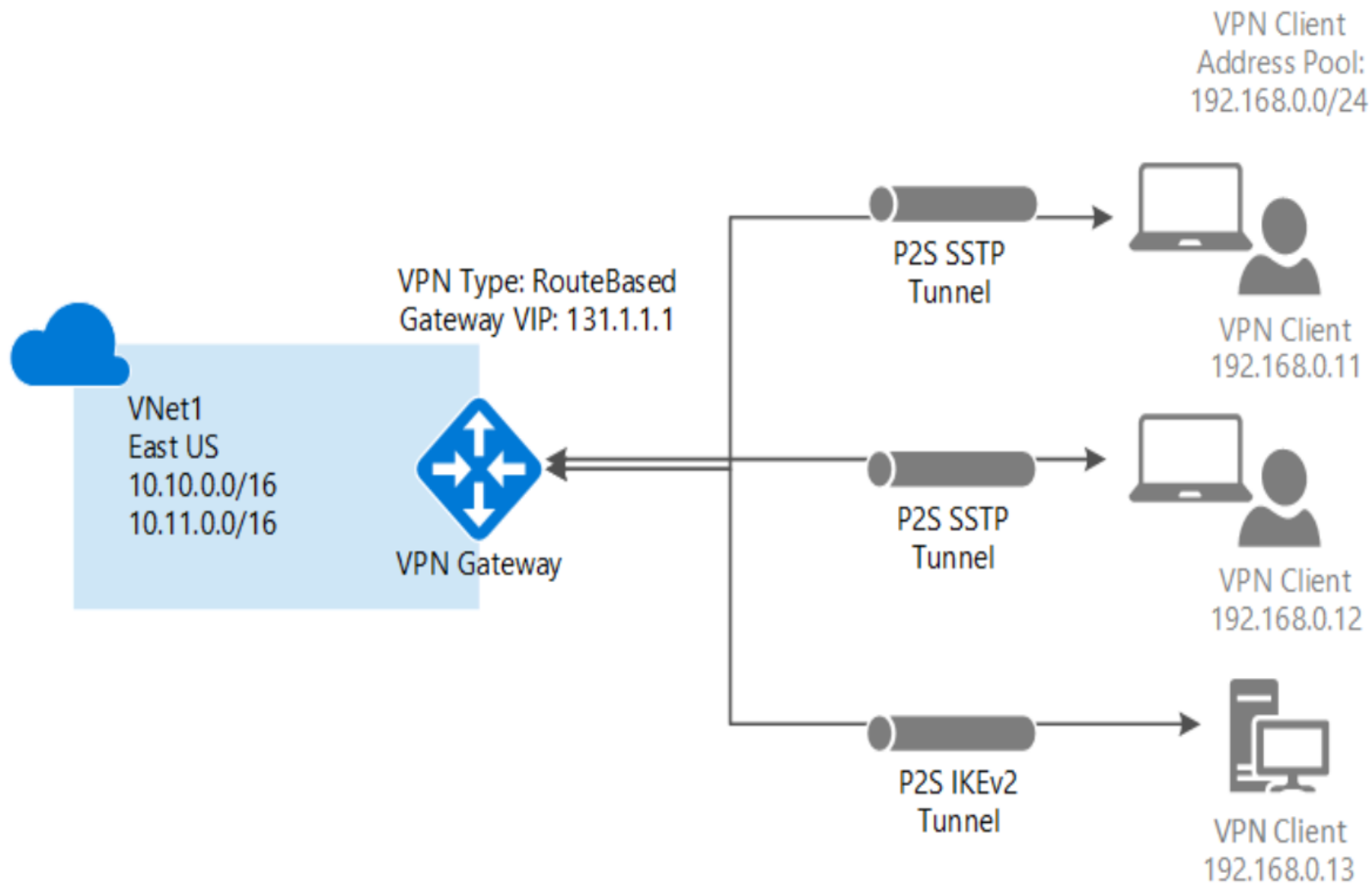
VNet-to-VNet connections (IPsec/IKE VPN tunnel)

Connecting a virtual network to another virtual network (VNet-to-VNet) is similar to connecting a VNet to an on-premises site location.

Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE.

You can even combine VNet-to-VNet communication with multi-site connection configurations.

This lets you establish network topologies that combine cross-premises connectivity with inter-virtual network connectivity.

The VNets you connect can be:

- In the same or different regions
- In the same or different subscriptions
- In the same or different deployment models
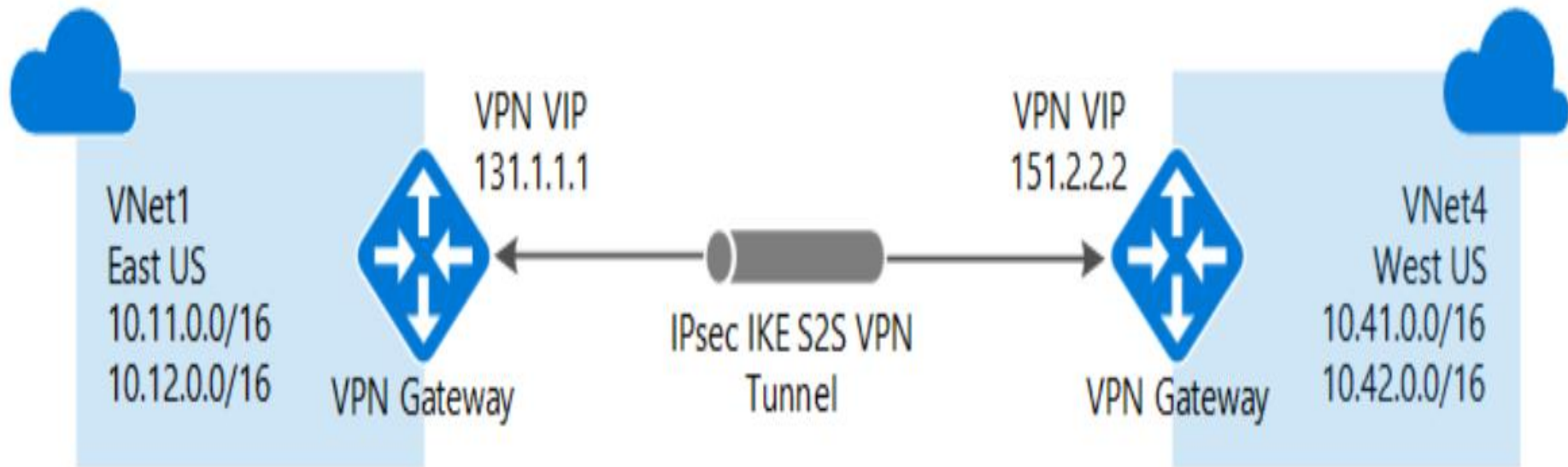
Connections between deployment models :

Azure currently has two deployment models: classic and Resource Manager. If you have been using Azure for some time, you probably have Azure VMs and instance roles running in a classic VNet. Your newer VMs and role instances may be running in a VNet created in Resource Manager. You can create a connection between the VNets to allow the resources in one VNet to communicate directly with resources in another.

Gateway SKUs by tunnel, connection, and throughput

| VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported
Generation1	VpnGw1	Max. 30*	Max. 128	Max. 250	650 Mbps	Supported
Generation1	VpnGw2	Max. 30*	Max. 128	Max. 500	1 Gbps	Supported
Generation1	VpnGw3	Max. 30*	Max. 128	Max. 1000	1.25 Gbps	Supported
Generation1	VpnGw1AZ	Max. 30*	Max. 128	Max. 250	650 Mbps	Supported
Generation1	VpnGw2AZ	Max. 30*	Max. 128	Max. 500	1 Gbps	Supported
Generation1	VpnGw3AZ	Max. 30*	Max. 128	Max. 1000	1.25 Gbps	Supported
Generation2	VpnGw2	Max. 30*	Max. 128	Max. 500	1.25 Gbps	Supported
Generation2	VpnGw3	Max. 30*	Max. 128	Max. 1000	2.5 Gbps	Supported
Generation2	VpnGw4	Max. 30*	Max. 128	Max. 1000	5 Gbps	Supported
Generation2	VpnGw5	Max. 30*	Max. 128	Max. 1000	10 Gbps	Supported

ExpressRoute :

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Office 365.

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 co-location facility.

Express Route connections do not go over the public Internet.

This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet.
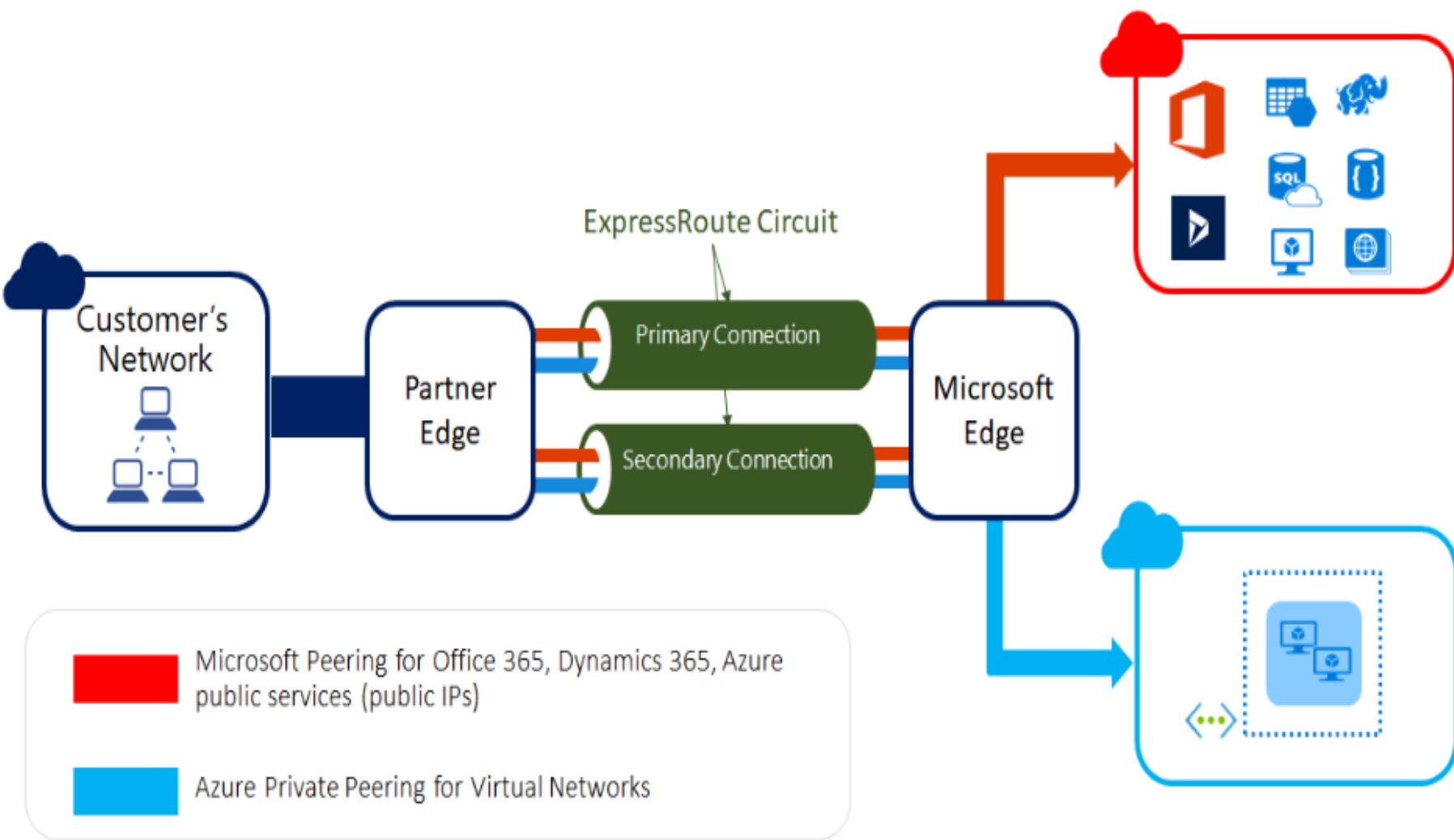
Key benefits :

•Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.

•Connectivity to Microsoft cloud services across all regions in the geopolitical region.

•Built-in redundancy in every peering location for higher reliability.

Features

Layer 3 connectivity

Microsoft uses BGP, an industry standard dynamic routing protocol, to exchange routes between your on-premises network, your instances in Azure, and Microsoft public addresses. We establish multiple BGP sessions with your network for different traffic profiles.

Redundancy :

Each ExpressRoute circuit consists of two connections to two Microsoft Enterprise edge routers (MSEEs) from the connectivity provider/your network edge.

Microsoft requires dual BGP connection from the connectivity provider/your network edge – one to each MSEE. You may choose not to deploy redundant devices/Ethernet circuits at your end.

However, connectivity providers use redundant devices to ensure that your connections are handed off to Microsoft in a redundant manner.

Connectivity to Microsoft cloud services

ExpressRoute connections enable access to the following services:

• Microsoft Azure services

• Microsoft Office 365 services

Bandwidth options :

You can purchase ExpressRoute circuits for a wide range of bandwidths. The supported bandwidths are listed below. Be sure to check with your connectivity provider to determine the bandwidths they support.

- 50 Mbps
- 100 Mbps
- 200 Mbps
- 500 Mbps
- 1 Gbps
- 2 Gbps
- 5 Gbps
- 10 Gbps