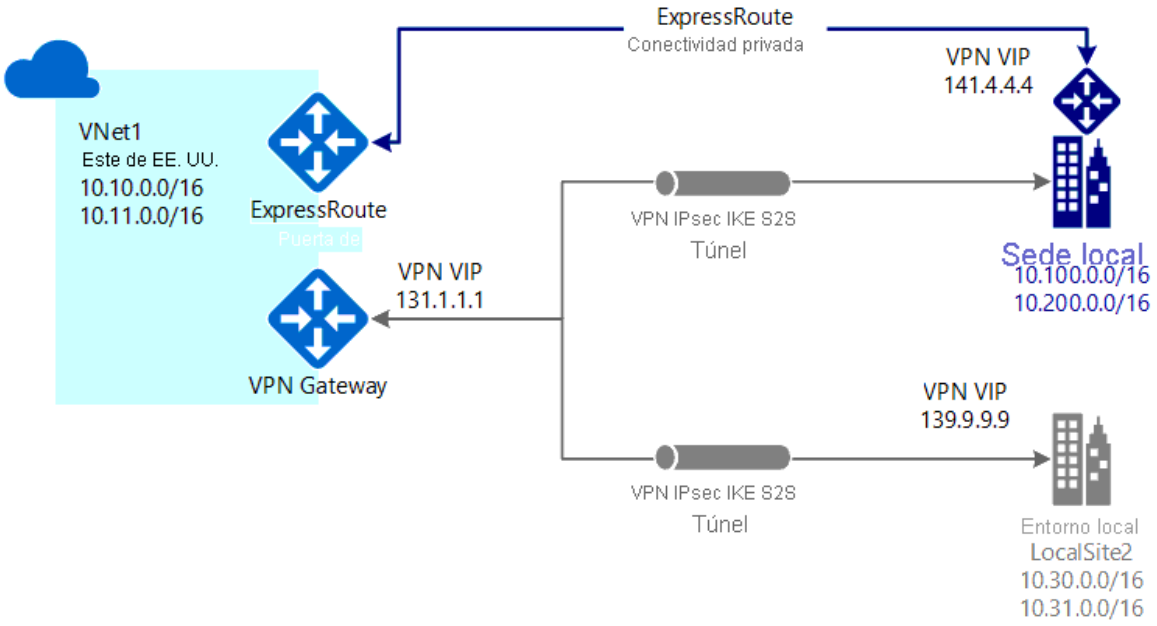
Revisión de ExpressRoute

ExpressRoute es una conexión directa y privada desde su WAN (no a través de la red Internet pública) a los servicios Microsoft, incluido Azure. El tráfico VPN de sitio a sitio viaja cifrado a través de la red pública de Internet. Poder configurar las conexiones VPN de sitio a sitio y ExpressRoute para la misma red virtual tiene varias ventajas.

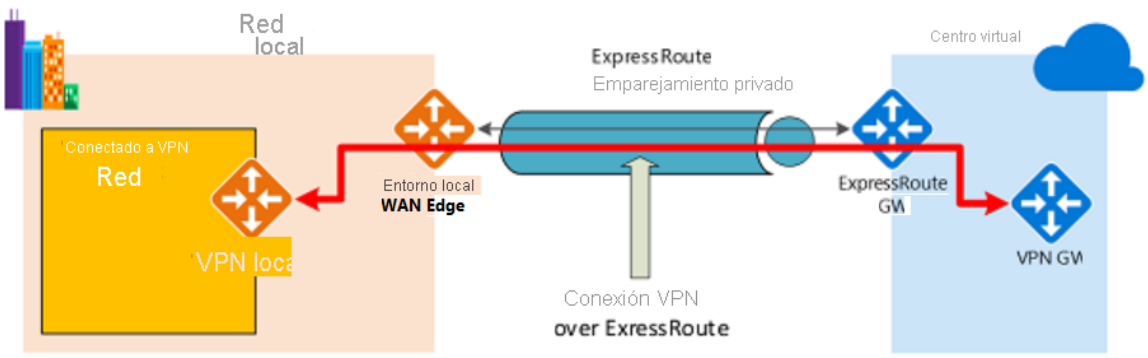
Puede configurar una VPN de sitio a sitio como una ruta de acceso seguro de conmutación por error para ExpressRoute, o bien usar la VPN de sitio a sitio para conectarse a sitios que no forman parte de su red, pero que están conectados a través de ExpressRoute. Tenga en cuenta que esta configuración requiere dos puertas de enlace de red virtual en la misma red virtual, una con el tipo de puerta de enlace "Vpn" y otra con -el tipo de puerta de enlace "ExpressRoute".



Cifrado de ExpressRoute

IPsec a través de ExpressRoute para Virtual WAN

Azure Virtual WAN usa una conexión VPN de intercambio de claves por red (IKE) del protocolo de seguridad de Internet (IPsec) desde la red local a Azure a través del emparejamiento privado de un circuito de Azure ExpressRoute. Esta técnica puede proporcionar un tránsito cifrado entre las redes locales y las redes virtuales de Azure a través de ExpressRoute sin necesidad de pasar por la red pública de Internet ni utilizar direcciones IP públicas. En el diagrama siguiente se muestra un ejemplo de conectividad VPN a través del emparejamiento privado de ExpressRoute.



El diagrama muestra una red dentro de la red local conectada a la puerta de enlace de VPN del centro de conectividad de Azure a través del emparejamiento privado de ExpressRoute. El establecimiento de la conectividad es sencillo:

1. Establezca la conectividad de ExpressRoute con un circuito ExpressRoute y emparejamiento privado.
2. Establecimiento de la conectividad VPN.

Un aspecto importante de esta configuración es el enrutamiento entre las redes locales y Azure a través de las rutas de acceso de ExpressRoute y VPN.

ExpressRoute admite un par de tecnologías de cifrado para garantizar la confidencialidad y la integridad de los datos que atraviesan su red y la red de Microsoft.

Cifrado de punto a punto mediante MACsec

MACsec es un estándar IEEE. Cifra los datos en el nivel de Media Access Control (MAC) o Network Layer 2. Puede usar MACsec para cifrar los vínculos físicos entre los dispositivos de red y los dispositivos de red de Microsoft cuando se conecte a Microsoft a través de ExpressRoute Direct. De forma predeterminada, MACsec está deshabilitado en los puertos de ExpressRoute Direct. Traiga su propia clave de MACsec para el cifrado y almacénela en Azure Key Vault. Decida cuándo desea rotar la clave.

Cifrado de un extremo a otro mediante IPsec y MACsec

IPsec es un estándar de IETF. Cifra los datos en el nivel Protocolo de Internet (IP) o Capa 3 de red. Puede usar IPsec para cifrar una conexión de un extremo a otro entre la red local y la red virtual (VNET) en Azure.

MACsec protege las conexiones físicas entre el usuario y Microsoft. IPsec protege la conexión de un extremo a otro entre el usuario y las redes virtuales en Azure. Puede habilitarlos de forma independiente.

ExpressRoute Direct

ExpressRoute Direct le ofrece la capacidad para conectarse directamente a la red global de Microsoft en ubicaciones de emparejamiento distribuidas estratégicamente por todo el mundo.

ExpressRoute Direct proporciona conectividad dual de 100 Gbps o 10 Gbps, que admite la conectividad activa/activa a escala.

Algunas de las características clave que ofrece ExpressRoute Direct incluyen:

- Ingesta de datos masivos en servicios como Storage y Cosmos DB
- Aislamiento físico para sectores regulados y que necesitan una conectividad dedicada y aislada, como: banca, gubernamentales y venta al por menor
- Control granular del circuito de distribución en función de la unidad de negocio

ExpressRoute Direct admite escenarios de ingesta de datos masivos en Azure Storage y otros servicios de macrodatos. Ahora, los circuitos ExpressRoute de ExpressRoute Direct 100 Gbps también admiten SKU de circuito de 40 Gbps y 100 Gbps. Los pares de puertos físicos solamente son de 100 o 10 Gbps y pueden tener varios circuitos virtuales.

ExpressRoute Direct admite los etiquetados QinQ y Dot1Q de VLAN.

- El **etiquetado QinQ de VLAN** se permite para los dominios de enrutamiento aislados por circuito ExpressRoute. Durante la creación del circuito, Azure asigna de forma dinámica una etiqueta S que no se puede cambiar. Cada emparejamiento del circuito (privado y de Microsoft) utilizará una etiqueta C única como VLAN. No es necesario que la etiqueta C sea única en los circuitos de los puertos de ExpressRoute Direct.
- El **etiquetado Dot1Q de VLAN** se permite para una única VLAN etiquetada por puerto de ExpressRoute Direct. Una etiqueta C que se use en un emparejamiento debe ser única en todos los circuitos y emparejamientos del par de puertos de ExpressRoute Direct.

ExpressRoute Direct proporciona el mismo acuerdo de nivel de servicio de nivel empresarial con conexiones redundantes activa-activa a la red global de Microsoft. La infraestructura de ExpressRoute es redundante, así como la conectividad a la red global de Microsoft es redundante y diversa y se escala conforme a los requisitos del cliente.
