**Aspectos básicos de Azure Virtual Network**

Completado100 XP

* 8 minutos

Tailwind Traders tiene un centro de datos local que va a mantener, pero quiere usar Azure para descargar los picos de tráfico mediante máquinas virtuales (VM) hospedadas en Azure. Quiere mantener el esquema de direcciones IP y los dispositivos de red existentes, y asegurarse de que todas las transferencias de datos sean seguras.

El uso de Azure Virtual Network para las redes virtuales puede ayudarle a conseguir sus objetivos.

**¿Qué son las redes virtuales de Azure?**

Las *redes virtuales de Azure* permiten a los recursos de Azure, como las máquinas virtuales, las aplicaciones web y las bases de datos, comunicarse entre sí, con los usuarios de Internet y con los equipos cliente en el entorno local. Se puede pensar en una red de Azure como en un conjunto de recursos que se vincula a otros recursos de Azure.

Las redes virtuales de Azure proporcionan las importantes funcionalidades de red siguientes:

* Aislamiento y segmentación
* Comunicación con Internet
* Comunicación entre recursos de Azure
* Comunicación con los recursos locales
* Enrutamiento del tráfico de red
* Filtrado del tráfico de red
* Conexión de redes virtuales

**Configuración de red para las máquinas virtuales**

**Aislamiento y segmentación**

Virtual Network permite crear varias redes virtuales aisladas. Al configurar una red virtual, se define un espacio de direcciones IP privadas con intervalos de direcciones IP públicas o privadas. Después, puede dividir ese espacio de direcciones IP en subredes y asignar parte del espacio de direcciones definido a cada subred con nombre.

En la resolución de nombres, puede usar el servicio de resolución de nombres integrado en Azure. También puede configurar la red virtual para que use un servidor DNS interno o externo.

**Comunicación con Internet**

Una máquina virtual en Azure se puede conectar a Internet de forma predeterminada. Puede habilitar las comunicaciones entrantes desde Internet si define una dirección IP pública o un equilibrador de carga público. Para la administración de la máquina virtual, puede conectarse a través de la CLI de Azure, el Protocolo de escritorio remoto o Secure Shell.

**Comunicación entre los recursos de Azure**

Le interesará habilitar los recursos de Azure para que se comuniquen entre sí de forma segura. Puede hacerlo de dos maneras:

* **Redes virtuales** Las redes virtuales no solo pueden conectar máquinas virtuales, sino también otros recursos de Azure, como App Service Environment para Power Apps, Azure Kubernetes Service y conjuntos de escalado de máquinas virtuales de Azure.
* **Puntos de conexión de servicio** Puede usar los puntos de conexión de servicio para conectarse a otros tipos de recursos de Azure, como cuentas de almacenamiento y bases de datos SQL de Azure. Este enfoque permite vincular varios recursos de Azure con las redes virtuales para mejorar la seguridad y proporcionar un enrutamiento óptimo entre los recursos.

**Comunicación con recursos locales**

Las redes virtuales de Azure permiten vincular entre sí los recursos del entorno local y dentro de la suscripción de Azure. De hecho, puede crear una red que abarque tanto el entorno local como el entorno en la nube. Existen tres mecanismos para lograr esta conectividad:

* **Redes privadas virtuales de punto a sitio** El enfoque habitual para una conexión de red privada virtual (VPN) consiste en establecer la conexión con la red corporativa desde un equipo ajeno a la organización. En este caso, el equipo cliente inicia una conexión VPN cifrada para conectar ese equipo a la red virtual de Azure.
* **Redes virtuales privadas de sitio a sitio** Una VPN de sitio a sitio vincula un dispositivo o puerta de enlace de VPN local con la puerta de enlace de VPN de Azure en una red virtual. De hecho, puede parecer que los dispositivos de Azure están en la red local. La conexión se cifra y funciona a través de Internet.
* **Azure ExpressRoute** Para los entornos donde se necesita más ancho de banda e incluso mayores niveles de seguridad, Azure ExpressRoute es el mejor sistema. ExpressRoute proporciona una conectividad privada dedicada a Azure que no viaja a través de Internet. (Obtendrá más información sobre ExpressRoute en una unidad independiente más adelante en este módulo.)

**Enrutamiento del tráfico de red**

De forma predeterminada, Azure enruta el tráfico entre las subredes de todas las redes virtuales conectadas, las redes locales e Internet. También puede controlar el enrutamiento e invalidar esa configuración del siguiente modo:

* **Tablas de rutas** Una tabla de rutas permite definir reglas para dirigir el tráfico. Puede crear tablas de rutas personalizadas que controlen cómo se enrutan los paquetes entre las subredes.
* **Protocolo de puerta de enlace de borde** El Protocolo de puerta de enlace de borde (BGP) funciona con puertas de enlace de VPN de Azure o con ExpressRoute para propagar las rutas BGP locales a las redes virtuales de Azure.

**Filtrado del tráfico de red**

Las redes virtuales de Azure permiten filtrar el tráfico entre las subredes mediante los métodos siguientes:

* **Grupos de seguridad de red** Un grupo de seguridad de red es un recurso de Azure que puede contener varias reglas de seguridad de entrada y salida. Estas reglas se pueden definir para permitir o bloquear el tráfico en función de factores como el protocolo, el puerto y las direcciones IP de destino y origen.
* **Aplicaciones virtuales de red** Una aplicación virtual de red es una máquina virtual especializada que se puede comparar con un dispositivo de red protegido. Una aplicación virtual de red ejerce una función de red determinada, como ejecutar un firewall o realizar la optimización de la red de área extensa (WAN).

**Conexión de redes virtuales**

Puede vincular redes virtuales entre sí mediante el *emparejamiento* de red virtual. El emparejamiento permite que los recursos de cada red virtual se comuniquen entre sí. Estas redes virtuales pueden estar en regiones distintas, lo que permite crear una red global interconectada con Azure.

UDR es enrutamiento definido por el usuario. Se trata de una actualización importante de las redes virtuales de Azure, ya que permite a los administradores de red controlar las tablas de enrutamiento entre las subredes de una red virtual, así como entre redes virtuales, lo que permite un mayor control sobre el flujo de tráfico de red.

**Configuración de Azure Virtual Network**

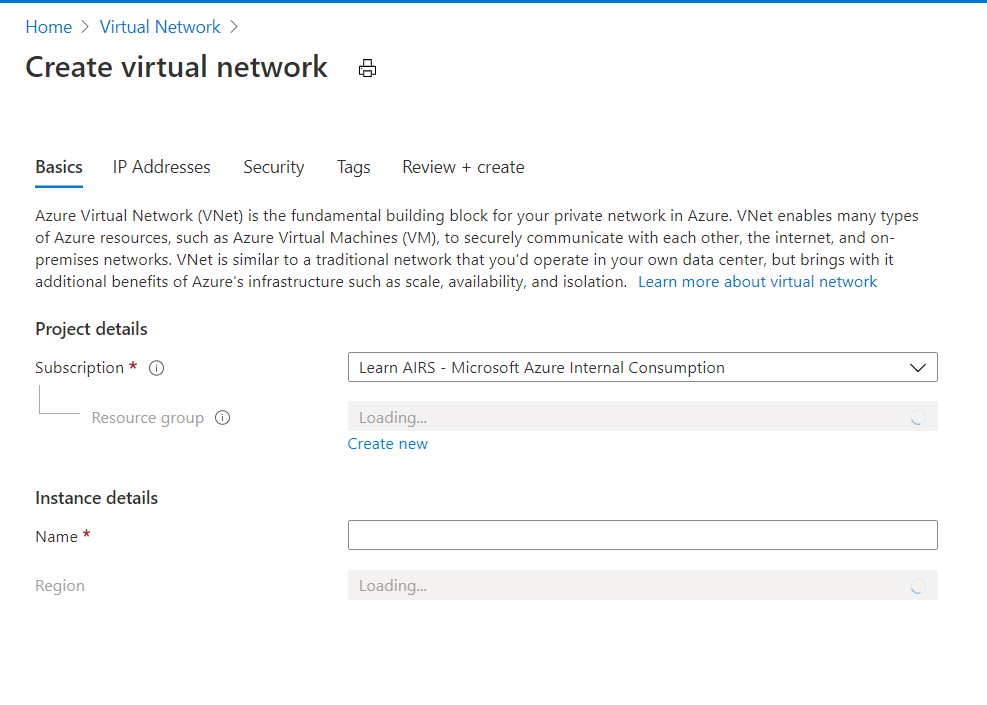
Completado100 XP

* 7 minutos

Puede crear y configurar instancias de Azure Virtual Network desde Azure Portal, Azure PowerShell en el equipo local o Azure Cloud Shell.

**Creación de una red virtual**

Cuando se crea una red virtual de Azure, se configuran algunas opciones básicas. Tendrá la posibilidad de configurar opciones avanzadas, como varias subredes, protección contra denegación de servicio distribuido (DDoS) y puntos de conexión de servicio.



Configurará las opciones siguientes para una red virtual básica:

* **Nombre de red** El nombre de red debe ser único en la suscripción, pero no es necesario que lo sea globalmente. Elija un nombre descriptivo que sea fácil de recordar e identificar con respecto a otras redes virtuales.
* **Espacio de direcciones** Al configurar una red virtual, se define el espacio de direcciones internas con el formato de Enrutamiento de interdominios sin clases (CIDR). Este espacio de direcciones debe ser único dentro de la suscripción y de cualquier otra red a la que se conecte. Supongamos que elige un espacio de direcciones de 10.0.0.0/24 para la primera red virtual. Las direcciones definidas en este intervalo del espacio de direcciones van de 10.0.0.1 a 10.0.0.254. Luego cree una segunda red virtual y elija un espacio de direcciones de 10.0.0.0/8. Las direcciones de este intervalo del espacio de direcciones van de 10.0.0.1 a 10.255.255.254. Algunas de las direcciones se superponen y no se pueden usar para las dos redes virtuales. Pero puede usar 10.0.0.0/16, con direcciones que van desde 10.0.0.1 hasta 10.0.255.254 y 10.1.0.0/16, con direcciones que van desde 10.1.0.1 hasta 10.1.255.254. Puede asignar estos espacios de direcciones a las redes virtuales porque ninguna dirección se superpone.

**Nota**

Podrá agregar espacios de direcciones después de crear la red virtual.

* **Suscripción** Esta opción solo se aplica si tiene varias suscripciones para elegir.
* **Grupo de recursos** Como cualquier otro recurso de Azure, una red virtual debe existir en un grupo de recursos. Puede seleccionar un grupo de recursos existente o crear uno.
* **Ubicación** Seleccione la ubicación donde desea que resida la red virtual.
* **Subred** Dentro de cada intervalo de direcciones de red virtual, puede crear una o varias subredes que dividirán el espacio de direcciones de la red virtual. El enrutamiento entre las subredes dependerá de las rutas de tráfico predeterminadas. También puede definir rutas personalizadas. Como alternativa, puede definir una subred que abarque todo el intervalo de direcciones de la red virtual.

**Nota**

Los nombres de las subredes deben comenzar con una letra o un número y terminar con una letra, un número o un guión bajo. Solo pueden contener letras, números, guiones bajos, puntos o guiones.

* **Protección contra DDoS** Puede seleccionar la protección DDoS básica o estándar. La protección contra DDoS estándar es un servicio Prémium. Para más información sobre la protección contra DDoS estándar, vea [Introducción a Protección contra DDoS de Azure estándar](https://docs.microsoft.com/es-es/azure/virtual-network/ddos-protection-overview).
* **Puntos de conexión de servicio** Aquí se habilitan los puntos de conexión de servicio. Después, se seleccionan en la lista los puntos de conexión de servicio de Azure que se quieren habilitar. Las opciones incluyen Azure Cosmos DB, Azure Service Bus, Azure Key Vault, etc.

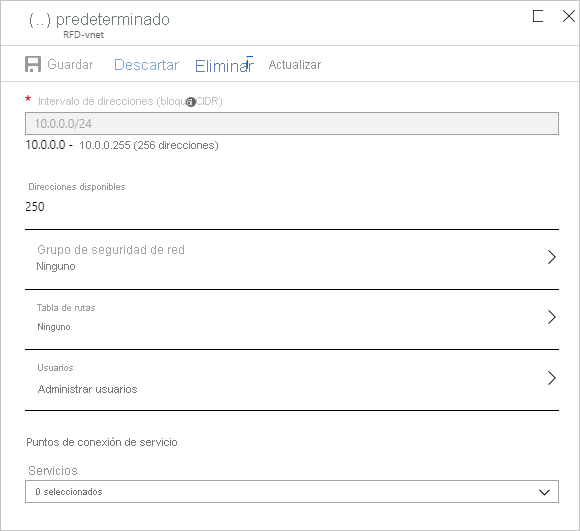
Después de configurar estas opciones, seleccione **Crear**.

**Definición de opciones de configuración adicionales**

Después de crear una red virtual, puede definir más opciones. Entre ellas se incluyen las siguientes:

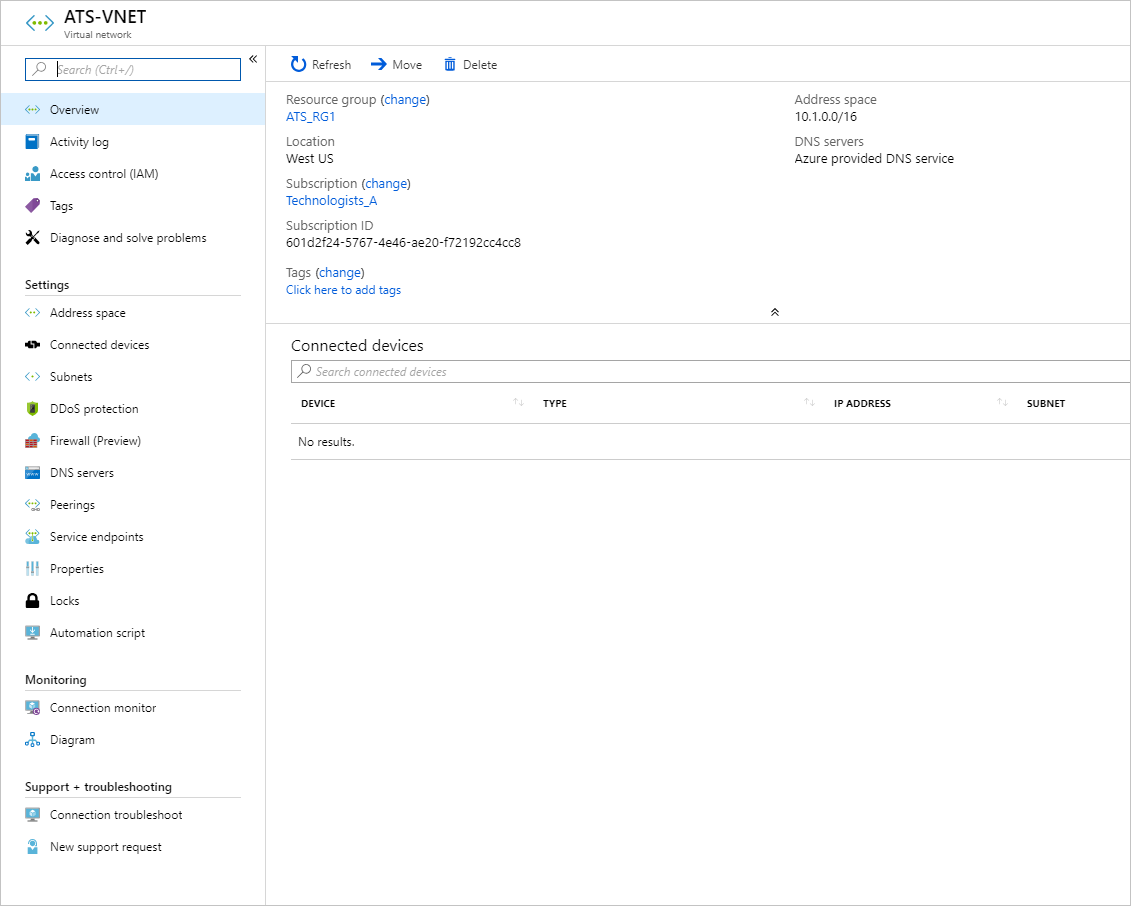
* **Grupo de seguridad de red** Los grupos de seguridad de red tienen reglas de seguridad que permiten filtrar el tipo de tráfico de red que puede entrar o salir de las interfaces de red y las subredes de red virtual. Cree el grupo de seguridad de red por separado. Después, asócielo con la red virtual.
* **Tabla de rutas** Azure crea automáticamente una tabla de rutas para cada subred de una red virtual de Azure y agrega las rutas predeterminadas del sistema a la tabla. Puede agregar tablas de rutas personalizadas para modificar el tráfico entre las redes virtuales.

También se pueden modificar los puntos de conexión de servicio.



**Configuración de redes virtuales**

Una vez creada una red virtual, puede cambiar la configuración adicional desde el panel **Redes virtuales** de Azure Portal. Como alternativa, puede usar comandos de PowerShell o Cloud Shell para realizar los cambios.



Después, puede revisar y cambiar la configuración en paneles secundarios adicionales. Esta configuración incluye:

* **Espacios de direcciones**: puede agregar espacios de direcciones adicionales a la definición inicial.
* **Dispositivos conectados**: use la red virtual para conectar las máquinas.
* **Subredes**: puede agregar subredes adicionales.
* **Emparejamientos**: vincule las redes virtuales mediante organizaciones de emparejamiento.

También puede supervisar las redes virtuales y solucionar sus problemas. O bien, puede crear un script de automatización para generar la red virtual actual.

Las redes virtuales son mecanismos eficaces y muy configurables para conectar las entidades de Azure. Puede conectar los recursos de Azure entre sí o a los recursos del entorno local. Puede aislar, filtrar y enrutar el tráfico de red. Azure le permite aumentar la seguridad donde considere que es necesario.

**Aspectos básicos de Azure VPN Gateway**

Completado100 XP

* 10 minutos

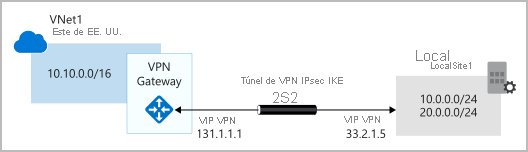
Las redes privadas virtuales usan un túnel cifrado en otra red. Normalmente, se implementan para conectar entre sí dos o más redes privadas de confianza a través de una red que no es de confianza (normalmente, la red pública de Internet). El tráfico se cifra mientras viaja por la red que no es de confianza para evitar ataques de interceptación o de otro tipo.

En el caso de nuestro escenario de Tailwind Traders, las VPN pueden permitir a las sucursales compartir información confidencial entre ubicaciones. Por ejemplo, supongamos que las oficinas en la región de la costa este de Estados Unidos necesitan acceder a los datos privados de clientes de la empresa, que se almacenan en servidores que están ubicados físicamente en una región de la costa oeste. Una VPN que conecta las oficinas de la costa este a los servidores de la costa oeste permite que su empresa acceda de forma segura a los datos privados de sus clientes.

**Puertas de enlace de VPN**

Una puerta de enlace de VPN es un tipo de puerta de enlace de red virtual. Las instancias de Azure VPN Gateway se implementan en instancias de Azure Virtual Network y habilitan la conectividad siguiente:

* Conectar los centros de datos locales a redes virtuales a través de una conexión de *sitio a sitio*.
* Conectar los dispositivos individuales a redes virtuales a través de una conexión de *punto a sitio*.
* Conectar las redes virtuales a otras redes virtuales a través de una conexión *entre redes*.



Todos los datos transferidos se cifran en un túnel privado mientras atraviesa Internet. Solo se puede implementar una instancia de VPN Gateway en cada red virtual, pero se puede usar una puerta de enlace para conectarse a varias ubicaciones, que incluye otras redes virtuales o centros de datos locales.

Al implementar una instancia de VPN Gateway, especifique el tipo de red privada virtual, es decir, *basada en directivas* o *basada en rutas*. La principal diferencia entre estos dos tipos de VPN es cómo se especifica el tráfico que se va a cifrar. En Azure, ambos tipos de puertas de enlace de VPN usan una clave previamente compartida como único método de autenticación. Ambos tipos también se basan en el intercambio de claves por red (IKE) en las versiones 1 o 2 y en el protocolo de seguridad de Internet (IPsec). El IKE se usa para establecer una asociación de seguridad (un contrato del cifrado) entre dos puntos de conexión. Esta asociación, después, se pasa al conjunto de IPsec, que cifra y descifra los paquetes de datos encapsulados en el túnel VPN.

**Redes privadas virtuales basadas en directivas**

Las instancias de VPN Gateway basadas en directivas especifican de forma estática la dirección IP de los paquetes que se deben cifrar a través de cada túnel. Este tipo de dispositivo evalúa cada paquete de datos en función de los conjuntos de direcciones IP para elegir el túnel a través del cual se va a enviar el paquete.

Entre las características clave de las instancias de VPN Gateway basadas en directivas en Azure se incluyen:

* Compatibilidad solo con IKEv1.
* Uso del *enrutamiento estático*, en el que las combinaciones de prefijos de dirección de ambas redes controlan cómo se cifra y descifra el tráfico a través del túnel VPN. El origen y destino de las redes de túnel se declaran en la directiva y no necesitan declararse en las tablas de enrutamiento.
* Las redes privadas virtuales basadas en directivas se deben usar en escenarios específicos que las necesiten, por ejemplo, para ofrecer compatibilidad con dispositivos de red privada virtual locales heredados.

**Redes privadas virtuales basadas en rutas**

Si la definición de las direcciones IP que están detrás de cada túnel es demasiado compleja, se pueden usar puertas de enlace basadas en rutas. Con las puertas de enlace basadas en rutas, los túneles IPSec se modelan como una interfaz de red o una interfaz de túnel virtual. El enrutamiento IP (ya sean rutas estáticas o protocolos de enrutamiento dinámico) decide cuál de estas interfaces de túnel se va a usar al enviar cada paquete. Las redes privadas virtuales basadas en rutas son el método preferido para conectar dispositivos locales. Son más resistentes a los cambios de la topología, como la creación de subredes.

Si necesita alguno de los siguientes tipos de conectividad, use una instancia de VPN Gateway basada en rutas:

* Conexiones entre redes virtuales
* Conexiones de punto a sitio
* Conexiones de varios sitios
* Coexistencia con una puerta de enlace de Azure ExpressRoute

Entre las características clave de las instancias de VPN Gateway basadas en rutas en Azure se incluyen:

* Compatibilidad con IKEv2
* Uso de selectores de tráfico universales (comodín)
* Puede usar *protocolos de enrutamiento dinámico*, donde las tablas de enrutamiento y reenvío dirigen el tráfico a diferentes túneles IPSec. En este caso, las redes de origen y destino no se definen estáticamente como en las VPN basadas en directivas o incluso en las VPN basadas en rutas con enrutamiento estático. En su lugar, los paquetes de datos se cifran en función de las tablas de enrutamiento de red que se crean de forma dinámica mediante protocolos de enrutamiento, como el Protocolo de puerta de enlace de borde (BGP).

**Tamaños de las instancias de VPN Gateway**

La SKU o el tamaño que implemente determinarán las funcionalidades de la instancia de VPN Gateway. En la tabla siguiente se muestran las funcionalidades principales de cada SKU disponible.

**SKU**

**Túneles de sitio a sitio o de red a red**

**Pruebas comparativas de rendimiento agregado**

**Compatibilidad con el Protocolo de puerta de enlace de borde**

Básico [Vea la nota]

Máximo: 10

100 Mbps

No compatible

VpnGw1/Az

Máximo: 30

650 Mbps

Compatible

VpnGw2/Az

Máximo: 30

1 Gbps

Compatible

VpnGw3/Az

Máximo: 30

1,25 Gbps

Compatible

**Nota**

La instancia básica de VPN Gateway solo debe usarse en cargas de trabajo de desarrollo/pruebas. Además, el SKU básico no se puede migrar más adelante a los SKU VpnGW1/2/3/Az sin quitar la puerta de enlace y volver a implementarla.

**Implementación de instancias de VPN Gateway**

Antes de implementar una instancia de VPN Gateway, necesitará algunos recursos de Azure y locales.

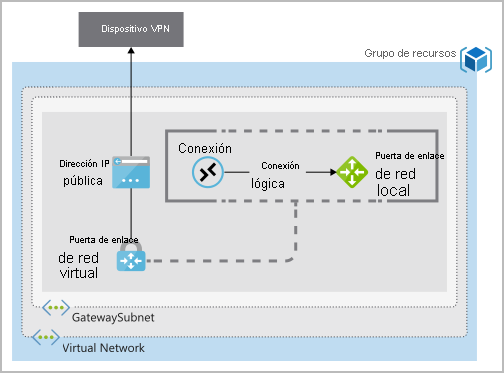
**Recursos de Azure necesarios**

Se necesitarán estos recursos de Azure para poder implementar una instancia de VPN Gateway operativa:

* **Red virtual**. Implemente una red virtual que tenga suficiente espacio de direcciones para la subred adicional que necesitará para la instancia de VPN Gateway. El espacio de direcciones para esta red virtual no se debe superponer con la red local que se va a conectar. Solo se puede implementar una única instancia de VPN Gateway en una red virtual.
* **GatewaySubnet**. Implemente una subred llamada GatewaySubnet para la instancia de VPN Gateway. Use al menos una máscara de dirección **/27** con el fin de asegurarse de que proporciona suficientes direcciones IP en la subred para un crecimiento futuro. Esta subred no se puede usar para otros servicios.
* **Dirección IP pública**. Cree una dirección IP pública dinámica de SKU básico si usa una puerta de enlace que no tenga en cuenta la zona. Esta dirección proporciona una dirección IP pública enrutable como destino para el dispositivo VPN local. Aunque esta dirección IP es dinámica, no se cambiará, a menos que elimine y vuelva a crear la instancia de VPN Gateway.
* **Puerta de enlace de red local**. Cree una puerta de enlace de red local para definir la configuración de la red local; por ejemplo, dónde y a qué se conectará la instancia de VPN Gateway. Esta configuración incluye la dirección IPv4 pública del dispositivo VPN local y las redes de enrutamiento locales. Esta información la usa la instancia de VPN Gateway con el fin de enrutar paquetes destinados para las redes locales a través del túnel IPSec.
* **Puerta de enlace de red virtual**. Cree la puerta de enlace de red virtual para enrutar el tráfico entre la red virtual y el centro de datos local u otras redes virtuales. La puerta de enlace de red virtual puede ser una puerta de enlace de VPN o ExpressRoute, pero en esta unidad solo se trata el tipo de puerta de enlace de red virtual de VPN. (Obtendrá más información sobre ExpressRoute en una unidad independiente más adelante en este módulo.)
* **Conexión**. Cree un recurso de conexión para crear una conexión lógica entre la instancia de VPN Gateway y la puerta de enlace de red local.
  + La conexión se realiza a las direcciones IPv4 del dispositivo VPN local, tal como define la puerta de enlace de red local.
  + La conexión se realiza desde la puerta de enlace de red virtual y la dirección IP pública asociada.

Se pueden crear varias conexiones.

En el diagrama siguiente se muestra esta combinación de recursos y sus relaciones para que le resulte más fácil entender los requisitos necesarios para implementar una instancia de VPN Gateway.



**Recursos locales necesarios**

Para conectar el centro de datos a una instancia de VPN Gateway, se necesitarán los siguientes recursos locales:

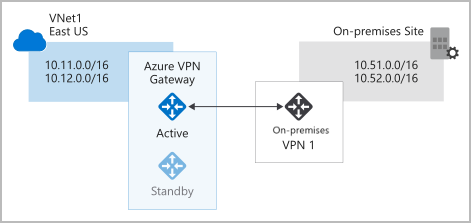
* Un dispositivo VPN que admita instancias de VPN Gateway basadas en directivas o en rutas.
* Una dirección IPv4 de acceso público (enrutable por Internet).

**Escenarios de alta disponibilidad**

Hay varias opciones para asegurarse de que se tiene una configuración de tolerancia a errores.

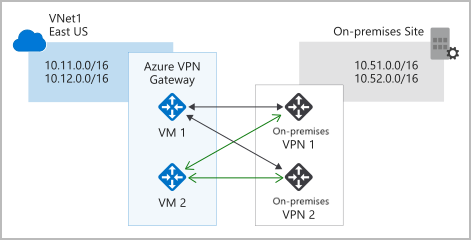
**Configuración de activo-en espera**

De forma predeterminada, las instancias de VPN Gateway se implementan como dos instancias en una configuración de activo-en espera, incluso si solo ve un recurso de VPN Gateway en Azure. Cuando el mantenimiento planeado o la interrupción imprevista afectan a la instancia activa, la instancia en espera asume de forma automática la responsabilidad de las conexiones sin ninguna intervención del usuario. Durante esta conmutación por error, las conexiones se interrumpen, pero por lo general se restauran en cuestión de segundos si se trata del mantenimiento planeado y en un plazo de 90 segundos en el caso de las interrupciones imprevistas.



**Activo/activo**

Al incorporar compatibilidad con el protocolo de enrutamiento de BGP, también puede implementar puertas de enlace VPN en una configuración del tipo activo/activo. En esta configuración, se asigna una IP pública única a cada instancia. Después, se crean túneles independientes desde el dispositivo local a cada dirección IP. Se puede ampliar la alta disponibilidad mediante la implementación de un dispositivo VPN local adicional.



**Conmutación por error de ExpressRoute**

Otra opción de alta disponibilidad consiste en configurar una instancia de VPN Gateway como una ruta segura de conmutación por error para las conexiones ExpressRoute. Los circuitos ExpressRoute tienen resistencia integrada. Sin embargo, no son inmunes a los problemas físicos que afectan a los cables que entregan conectividad ni a las interrupciones que afectan a la ubicación completa de ExpressRoute. En escenarios de alta disponibilidad, en los que existe un riesgo asociado a una interrupción de un circuito ExpressRoute, también puede aprovisionar una instancia de VPN Gateway que usa Internet como un método alternativo de conectividad. De este modo, puede garantizar que siempre haya una conexión a las redes virtuales.

**Puertas de enlace con redundancia de zona**

En las regiones que admiten zonas de disponibilidad, se pueden implementar puertas de enlace VPN y ExpressRoute en una configuración con redundancia de zona. Esta configuración aporta una mayor disponibilidad, escalabilidad y resistencia a las puertas de enlace de red virtual. Implementar puertas de enlace en Azure Availability Zones separa de forma física y lógica las puertas de enlace dentro de una región, al mismo tiempo que protege la conectividad de red local en Azure de errores de nivel de zona. Estas puertas de enlace requieren diferentes SKU de puerta de enlace y usan direcciones IP públicas estándar en lugar de direcciones IP públicas básicas.

**Aspectos básicos de Azure VPN Gateway**

Completado100 XP

* 10 minutos

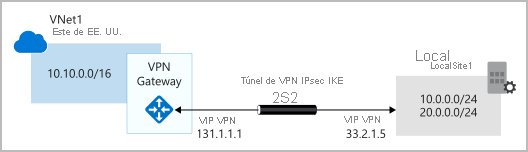
Las redes privadas virtuales usan un túnel cifrado en otra red. Normalmente, se implementan para conectar entre sí dos o más redes privadas de confianza a través de una red que no es de confianza (normalmente, la red pública de Internet). El tráfico se cifra mientras viaja por la red que no es de confianza para evitar ataques de interceptación o de otro tipo.

En el caso de nuestro escenario de Tailwind Traders, las VPN pueden permitir a las sucursales compartir información confidencial entre ubicaciones. Por ejemplo, supongamos que las oficinas en la región de la costa este de Estados Unidos necesitan acceder a los datos privados de clientes de la empresa, que se almacenan en servidores que están ubicados físicamente en una región de la costa oeste. Una VPN que conecta las oficinas de la costa este a los servidores de la costa oeste permite que su empresa acceda de forma segura a los datos privados de sus clientes.

**Puertas de enlace de VPN**

Una puerta de enlace de VPN es un tipo de puerta de enlace de red virtual. Las instancias de Azure VPN Gateway se implementan en instancias de Azure Virtual Network y habilitan la conectividad siguiente:

* Conectar los centros de datos locales a redes virtuales a través de una conexión de *sitio a sitio*.
* Conectar los dispositivos individuales a redes virtuales a través de una conexión de *punto a sitio*.
* Conectar las redes virtuales a otras redes virtuales a través de una conexión *entre redes*.



Todos los datos transferidos se cifran en un túnel privado mientras atraviesa Internet. Solo se puede implementar una instancia de VPN Gateway en cada red virtual, pero se puede usar una puerta de enlace para conectarse a varias ubicaciones, que incluye otras redes virtuales o centros de datos locales.

Al implementar una instancia de VPN Gateway, especifique el tipo de red privada virtual, es decir, *basada en directivas* o *basada en rutas*. La principal diferencia entre estos dos tipos de VPN es cómo se especifica el tráfico que se va a cifrar. En Azure, ambos tipos de puertas de enlace de VPN usan una clave previamente compartida como único método de autenticación. Ambos tipos también se basan en el intercambio de claves por red (IKE) en las versiones 1 o 2 y en el protocolo de seguridad de Internet (IPsec). El IKE se usa para establecer una asociación de seguridad (un contrato del cifrado) entre dos puntos de conexión. Esta asociación, después, se pasa al conjunto de IPsec, que cifra y descifra los paquetes de datos encapsulados en el túnel VPN.

**Redes privadas virtuales basadas en directivas**

Las instancias de VPN Gateway basadas en directivas especifican de forma estática la dirección IP de los paquetes que se deben cifrar a través de cada túnel. Este tipo de dispositivo evalúa cada paquete de datos en función de los conjuntos de direcciones IP para elegir el túnel a través del cual se va a enviar el paquete.

Entre las características clave de las instancias de VPN Gateway basadas en directivas en Azure se incluyen:

* Compatibilidad solo con IKEv1.
* Uso del *enrutamiento estático*, en el que las combinaciones de prefijos de dirección de ambas redes controlan cómo se cifra y descifra el tráfico a través del túnel VPN. El origen y destino de las redes de túnel se declaran en la directiva y no necesitan declararse en las tablas de enrutamiento.
* Las redes privadas virtuales basadas en directivas se deben usar en escenarios específicos que las necesiten, por ejemplo, para ofrecer compatibilidad con dispositivos de red privada virtual locales heredados.

**Redes privadas virtuales basadas en rutas**

Si la definición de las direcciones IP que están detrás de cada túnel es demasiado compleja, se pueden usar puertas de enlace basadas en rutas. Con las puertas de enlace basadas en rutas, los túneles IPSec se modelan como una interfaz de red o una interfaz de túnel virtual. El enrutamiento IP (ya sean rutas estáticas o protocolos de enrutamiento dinámico) decide cuál de estas interfaces de túnel se va a usar al enviar cada paquete. Las redes privadas virtuales basadas en rutas son el método preferido para conectar dispositivos locales. Son más resistentes a los cambios de la topología, como la creación de subredes.

Si necesita alguno de los siguientes tipos de conectividad, use una instancia de VPN Gateway basada en rutas:

* Conexiones entre redes virtuales
* Conexiones de punto a sitio
* Conexiones de varios sitios
* Coexistencia con una puerta de enlace de Azure ExpressRoute

Entre las características clave de las instancias de VPN Gateway basadas en rutas en Azure se incluyen:

* Compatibilidad con IKEv2
* Uso de selectores de tráfico universales (comodín)
* Puede usar *protocolos de enrutamiento dinámico*, donde las tablas de enrutamiento y reenvío dirigen el tráfico a diferentes túneles IPSec. En este caso, las redes de origen y destino no se definen estáticamente como en las VPN basadas en directivas o incluso en las VPN basadas en rutas con enrutamiento estático. En su lugar, los paquetes de datos se cifran en función de las tablas de enrutamiento de red que se crean de forma dinámica mediante protocolos de enrutamiento, como el Protocolo de puerta de enlace de borde (BGP).

**Tamaños de las instancias de VPN Gateway**

La SKU o el tamaño que implemente determinarán las funcionalidades de la instancia de VPN Gateway. En la tabla siguiente se muestran las funcionalidades principales de cada SKU disponible.

**SKU**

**Túneles de sitio a sitio o de red a red**

**Pruebas comparativas de rendimiento agregado**

**Compatibilidad con el Protocolo de puerta de enlace de borde**

Básico [Vea la nota]

Máximo: 10

100 Mbps

No compatible

VpnGw1/Az

Máximo: 30

650 Mbps

Compatible

VpnGw2/Az

Máximo: 30

1 Gbps

Compatible

VpnGw3/Az

Máximo: 30

1,25 Gbps

Compatible

**Nota**

La instancia básica de VPN Gateway solo debe usarse en cargas de trabajo de desarrollo/pruebas. Además, el SKU básico no se puede migrar más adelante a los SKU VpnGW1/2/3/Az sin quitar la puerta de enlace y volver a implementarla.

**Implementación de instancias de VPN Gateway**

Antes de implementar una instancia de VPN Gateway, necesitará algunos recursos de Azure y locales.

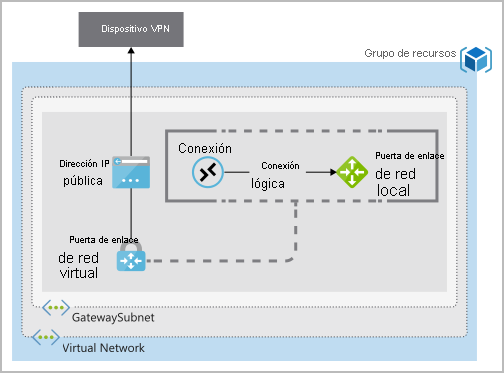
**Recursos de Azure necesarios**

Se necesitarán estos recursos de Azure para poder implementar una instancia de VPN Gateway operativa:

* **Red virtual**. Implemente una red virtual que tenga suficiente espacio de direcciones para la subred adicional que necesitará para la instancia de VPN Gateway. El espacio de direcciones para esta red virtual no se debe superponer con la red local que se va a conectar. Solo se puede implementar una única instancia de VPN Gateway en una red virtual.
* **GatewaySubnet**. Implemente una subred llamada GatewaySubnet para la instancia de VPN Gateway. Use al menos una máscara de dirección **/27** con el fin de asegurarse de que proporciona suficientes direcciones IP en la subred para un crecimiento futuro. Esta subred no se puede usar para otros servicios.
* **Dirección IP pública**. Cree una dirección IP pública dinámica de SKU básico si usa una puerta de enlace que no tenga en cuenta la zona. Esta dirección proporciona una dirección IP pública enrutable como destino para el dispositivo VPN local. Aunque esta dirección IP es dinámica, no se cambiará, a menos que elimine y vuelva a crear la instancia de VPN Gateway.
* **Puerta de enlace de red local**. Cree una puerta de enlace de red local para definir la configuración de la red local; por ejemplo, dónde y a qué se conectará la instancia de VPN Gateway. Esta configuración incluye la dirección IPv4 pública del dispositivo VPN local y las redes de enrutamiento locales. Esta información la usa la instancia de VPN Gateway con el fin de enrutar paquetes destinados para las redes locales a través del túnel IPSec.
* **Puerta de enlace de red virtual**. Cree la puerta de enlace de red virtual para enrutar el tráfico entre la red virtual y el centro de datos local u otras redes virtuales. La puerta de enlace de red virtual puede ser una puerta de enlace de VPN o ExpressRoute, pero en esta unidad solo se trata el tipo de puerta de enlace de red virtual de VPN. (Obtendrá más información sobre ExpressRoute en una unidad independiente más adelante en este módulo.)
* **Conexión**. Cree un recurso de conexión para crear una conexión lógica entre la instancia de VPN Gateway y la puerta de enlace de red local.
  + La conexión se realiza a las direcciones IPv4 del dispositivo VPN local, tal como define la puerta de enlace de red local.
  + La conexión se realiza desde la puerta de enlace de red virtual y la dirección IP pública asociada.

Se pueden crear varias conexiones.

En el diagrama siguiente se muestra esta combinación de recursos y sus relaciones para que le resulte más fácil entender los requisitos necesarios para implementar una instancia de VPN Gateway.



**Recursos locales necesarios**

Para conectar el centro de datos a una instancia de VPN Gateway, se necesitarán los siguientes recursos locales:

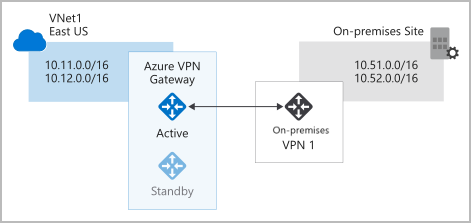
* Un dispositivo VPN que admita instancias de VPN Gateway basadas en directivas o en rutas.
* Una dirección IPv4 de acceso público (enrutable por Internet).

**Escenarios de alta disponibilidad**

Hay varias opciones para asegurarse de que se tiene una configuración de tolerancia a errores.

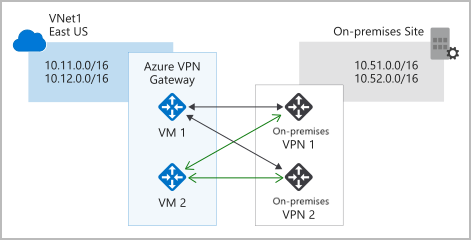
**Configuración de activo-en espera**

De forma predeterminada, las instancias de VPN Gateway se implementan como dos instancias en una configuración de activo-en espera, incluso si solo ve un recurso de VPN Gateway en Azure. Cuando el mantenimiento planeado o la interrupción imprevista afectan a la instancia activa, la instancia en espera asume de forma automática la responsabilidad de las conexiones sin ninguna intervención del usuario. Durante esta conmutación por error, las conexiones se interrumpen, pero por lo general se restauran en cuestión de segundos si se trata del mantenimiento planeado y en un plazo de 90 segundos en el caso de las interrupciones imprevistas.



**Activo/activo**

Al incorporar compatibilidad con el protocolo de enrutamiento de BGP, también puede implementar puertas de enlace VPN en una configuración del tipo activo/activo. En esta configuración, se asigna una IP pública única a cada instancia. Después, se crean túneles independientes desde el dispositivo local a cada dirección IP. Se puede ampliar la alta disponibilidad mediante la implementación de un dispositivo VPN local adicional.



**Conmutación por error de ExpressRoute**

Otra opción de alta disponibilidad consiste en configurar una instancia de VPN Gateway como una ruta segura de conmutación por error para las conexiones ExpressRoute. Los circuitos ExpressRoute tienen resistencia integrada. Sin embargo, no son inmunes a los problemas físicos que afectan a los cables que entregan conectividad ni a las interrupciones que afectan a la ubicación completa de ExpressRoute. En escenarios de alta disponibilidad, en los que existe un riesgo asociado a una interrupción de un circuito ExpressRoute, también puede aprovisionar una instancia de VPN Gateway que usa Internet como un método alternativo de conectividad. De este modo, puede garantizar que siempre haya una conexión a las redes virtuales.

**Puertas de enlace con redundancia de zona**

En las regiones que admiten zonas de disponibilidad, se pueden implementar puertas de enlace VPN y ExpressRoute en una configuración con redundancia de zona. Esta configuración aporta una mayor disponibilidad, escalabilidad y resistencia a las puertas de enlace de red virtual. Implementar puertas de enlace en Azure Availability Zones separa de forma física y lógica las puertas de enlace dentro de una región, al mismo tiempo que protege la conectividad de red local en Azure de errores de nivel de zona. Estas puertas de enlace requieren diferentes SKU de puerta de enlace y usan direcciones IP públicas estándar en lugar de direcciones IP públicas básicas.

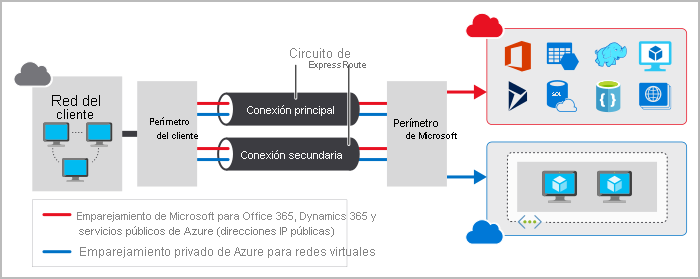
**Aspectos básicos de Azure ExpressRoute**

Completado100 XP

* 5 minutos

ExpressRoute le permite ampliar las redes locales a la nube de Microsoft mediante una conexión privada con la ayuda de un proveedor de conectividad. Con ExpressRoute, puede establecer conexiones con servicios en la nube de Microsoft, como Microsoft Azure y Microsoft 365.

La conectividad puede ser desde una red de conectividad universal (IP VPN), una red Ethernet de punto a punto o una conexión cruzada virtual a través de un proveedor de conectividad en una instalación de ubicación compartida. Las conexiones de ExpressRoute no pasan por la red pública de Internet. Esto permite a las conexiones de ExpressRoute ofrecer más confiabilidad, más velocidad, latencia coherentes y mayor seguridad que las conexiones normales a través de Internet. Para información sobre cómo conectar la red a Microsoft mediante ExpressRoute, consulte ExpressRoute connectivity models (Modelos de conectividad de ExpressRoute).



Como parte de su trabajo para Tailwind Traders, debe comprender qué es Azure ExpressRoute y cómo se integra con las redes locales y de Azure. En esta unidad, conocerá las ventajas que proporciona ExpressRoute en comparación con otras opciones de conectividad de sitio a sitio. Como resultado, observará si ExpressRoute puede proporcionar a la empresa el mejor rendimiento de red posible.

A lo largo de esta unidad, nos centraremos en dos niveles diferentes del modelo de interconexión de sistemas abiertos (OSI):

* **Nivel 2 (L2)**: se trata del nivel de vínculo de datos, que proporciona una comunicación de nodo a nodo entre dos nodos de la misma red.
* **Nivel 3 (L3)**: se trata del nivel de red, que proporciona el direccionamiento y enrutamiento entre los nodos de una red de varios nodos.

**Características y ventajas de ExpressRoute**

El uso de ExpressRoute como servicio de conexión entre Azure y las redes locales tiene varias ventajas.

* Conectividad de nivel 3 entre su red local y Microsoft Cloud a través de un proveedor de conectividad. La conectividad puede ser desde una red de conectividad universal (IP VPN), una red Ethernet de punto a punto, o una conexión cruzada virtual a través de un intercambio de Ethernet.
* Conectividad de servicios en la nube de Microsoft en todas las regiones dentro de la región geopolítica.
* Conectividad global a los servicios de Microsoft en todas las regiones con el complemento ExpressRoute Premium.
* Enrutamiento dinámico entre la red y Microsoft a través de BGP.
* Redundancia integrada en todas las ubicaciones de configuración entre pares para una mayor confiabilidad.
* El tiempo de actividad de conexión SLA.
* Compatibilidad con QoS de Skype para la empresa.

**Conectividad de nivel 3**

ExpressRoute proporciona conectividad de nivel 3 (nivel de dirección) entre la red local y la nube de Microsoft a través de asociados de conectividad. Estas conexiones pueden ser de una red punto a punto o universal. También puede tratarse de conexiones cruzadas virtuales a través de un intercambio.

**Redundancia integrada**

Cada proveedor de conectividad usa dispositivos redundantes para garantizar que las conexiones establecidas con Microsoft tengan alta disponibilidad. Puede configurar varios circuitos para complementar esta característica. Todas las conexiones redundantes se configuran con conectividad de nivel 3 para cumplir los Acuerdos de Nivel de Servicio.

**Conectividad con los Servicios en la nube de Microsoft**

ExpressRoute permite el acceso directo a los siguientes servicios en todas las regiones:

* Microsoft Office 365
* Microsoft Dynamics 365
* Servicios de proceso de Azure, como Azure Virtual Machines
* Servicios en la nube de Azure, como Azure Cosmos DB y Azure Storage

Office 365 se creó para tener acceso a él de forma segura y fiable a través de Internet. Por este motivo, se recomienda utilizar ExpressRoute en escenarios concretos. La sección "Más información" al final de este módulo incluye un vínculo sobre el uso de ExpressRoute para acceder a Office 365.

**Conectividad local con Global Reach de ExpressRoute**

Puede permitir que Global Reach de ExpressRoute intercambie datos entre los sitios locales si conecta los diferentes circuitos ExpressRoute. Por ejemplo, supongamos que tiene un centro de datos privado en California conectado a ExpressRoute en Silicon Valley. Tiene otro centro de centros privado en Texas conectado a ExpressRoute en Dallas. Con Global Reach de ExpressRoute, puede conectar sus centros de recursos privados a través de dos circuitos ExpressRoute. El tráfico de los centros de datos viajará a través de la red de Microsoft.

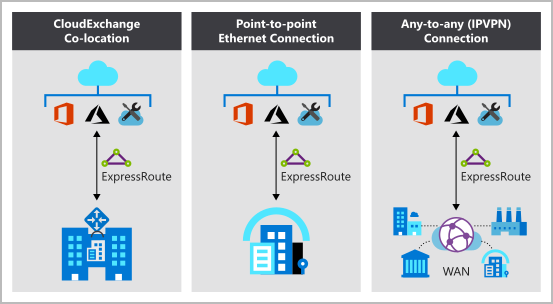
**Enrutamiento dinámico**

ExpressRoute usa el protocolo de enrutamiento Protocolo de puerta de enlace de borde (BGP). BGP se usa para intercambiar rutas entre las redes locales y los recursos que se ejecutan en Azure. Este protocolo permite el enrutamiento dinámico entre la red local y los servicios que se ejecutan en la nube de Microsoft.

**Modelos de conectividad de ExpressRoute**

ExpressRoute admite tres modelos que puede usar para conectar la red local con la nube de Microsoft:

* Ubicación de CloudExchange
* Conexión Ethernet de punto a punto
* Conexión universal



**Coubicación en un intercambio en la nube**

Normalmente, los proveedores de coubicación pueden ofrecer conexiones de nivel 2 y nivel 3 entre la infraestructura, que puede encontrarse en las instalación de la coubicación, y la nube de Microsoft. Por ejemplo, si el centro de datos tiene la ubicación compartida en un intercambio en la nube, como un ISP, puede solicitar una conexión cruzada virtual a la nube de Microsoft.

**Conexión Ethernet de punto a punto**

Las conexiones de punto a punto proporcionan conectividad de nivel 2 y nivel 3 entre el sitio local y Azure. Puede conectar sus oficinas o centros de datos a Azure mediante vínculos de punto a punto. Por ejemplo, si tiene un centro de datos local, puede usar un vínculo de Ethernet de punto a punto para conectarse a Microsoft.

**Redes universales**

Con la conectividad universal, puede integrar la red de área extensa (WAN) con Azure si proporciona conexiones a las oficinas y los centros de datos. Azure se integra con la conexión WAN para proporcionarle una conexión, como la que tendría entre el centro de datos y las sucursales.

Con las conexiones universales, todos los proveedores de WAN ofrecen conectividad de nivel 3. Por ejemplo, si ya usa la conmutación de etiquetas de multiprotocolo para conectarse a las sucursales o a otros sitios de la organización, una conexión ExpressRoute a Microsoft se comporta como cualquier otra ubicación en la WAN privada.

**Consideraciones sobre la seguridad**

Con ExpressRoute los datos no viajan a través de la red pública de Internet y, por tanto, no se exponen a los posibles riesgos asociados a las comunicaciones de Internet. ExpressRoute es una conexión privada de la infraestructura local a la infraestructura de Azure. Incluso si tiene una conexión ExpressRoute, las consultas de DNS, la comprobación de la lista de revocación de certificados y las solicitudes de Azure Content Delivery Network se siguen enviando a través de la red pública de Internet.