**Introducción**

Los administradores usan rutas de red para controlar el flujo de tráfico a través de una red. Las redes virtuales de Azure proporcionan funcionalidades que le ayudarán a personalizar las rutas de red, establecer puntos de conexión de servicio y acceder a vínculos privados.

En este módulo, supondremos que su empresa ha sufrido recientemente un incidente de seguridad que ha expuesto la información personal de los clientes. Como consecuencia de este incidente de seguridad, no solo perdió los datos confidenciales de los clientes, sino su confianza. Para abordar este escenario, el equipo de TI ha recomendado implementar aplicaciones virtuales de red (NVA). Debe asegurarse de que el tráfico se enrute correctamente mediante las aplicaciones virtuales. Explorará otras opciones de seguridad, como puntos de conexión de servicio y vínculos privados.

**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Implementar rutas del sistema y rutas definidas por el usuario
* Configurar una ruta personalizada
* Implementar puntos de conexión de servicio
* Identificar las características y los casos de uso de vínculos privados y servicios de punto de conexión.

**Aptitudes evaluadas**

El contenido del módulo le ayuda a prepararse para el [examen AZ-104: Administrador de Microsoft Azure](https://learn.microsoft.com/es-es/certifications/exams/az-104). Los conceptos del módulo tratan los siguientes aspectos:

Configuración y administración de redes virtuales (25-30 %)

* Implementación y administración de redes virtuales.
  + Configuración de rutas de red definidas por el usuario
  + Configuración de puntos de conexión en subredes
  + Configuración de puntos de conexión privados

**Revisión de las rutas del sistema**

Azure usa *rutas del sistema* para dirigir el tráfico de red entre máquinas virtuales, redes locales e Internet. La información sobre las rutas del sistema se registra en una *tabla de rutas*.

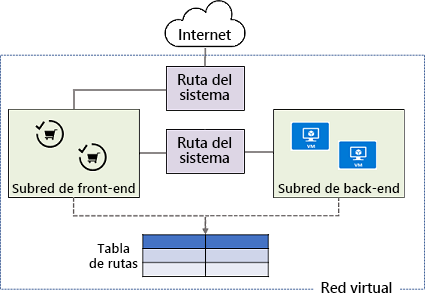
**Aspectos que saber sobre las rutas del sistema**

Echemos un vistazo más detallado a la forma en que Azure implementa las rutas del sistema.

* Azure usa rutas del sistema para controlar el tráfico de las máquinas virtuales en varios escenarios:
  + Tráfico entre máquinas virtuales en la misma subred
  + Tráfico entre máquinas virtuales en subredes diferentes de la misma red virtual
  + Tráfico de máquinas virtuales a Internet
* Una tabla de enrutamiento contiene un conjunto de reglas, denominadas *rutas*, que especifica cómo se deben enrutar los paquetes en una red virtual.
* Las tablas de enrutamiento registran información sobre las rutas del sistema, donde las tablas están asociadas a subredes.
* Cada paquete que sale de una subred se controla en función de la tabla de redirección asociada.
* Los paquetes se hacen coincidir con las rutas mediante el uso del destino. El destino puede ser una dirección IP, una puerta de enlace de red virtual, una aplicación virtual o Internet.
* Si no se encuentra una ruta que coincida, se descarta el paquete.

**Escenario empresarial**

Supongamos que tiene una red virtual con dos subredes. En esta configuración, puede usar rutas del sistema de Azure para controlar la comunicación entre las subredes y entre subredes e Internet. Una subred de front-end puede usar una ruta del sistema para acceder a Internet. Una subred de back-end puede usar una ruta del sistema para acceder a la subred de front-end. Ambas subredes acceden a una tabla de rutas. En la ilustración siguiente se destaca este escenario:



**Identificación de las rutas definidas por el usuario**

Azure controla automáticamente todo el enrutamiento del tráfico de red, pero en algunos casos, es preferible una configuración personalizada. En estas situaciones, puede configurar *rutas definidas por el usuario* (UDR) y destinos de *próximo salto*.

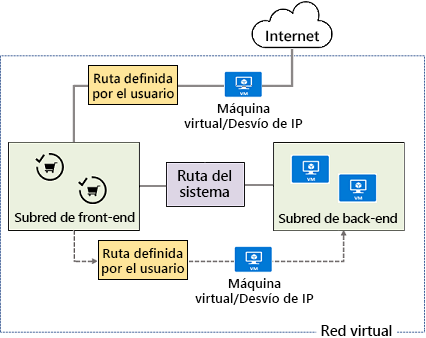
**Aspectos que se deben conocer sobre las rutas definidas por el usuario**

Examinemos las características de las rutas definidas por el usuario.

* Las UDR controlan el tráfico de red mediante la definición de rutas que especifican el *próximo salto* del flujo de tráfico.
* El próximo salto puede ser uno de los siguientes destinos:
  + Puerta de enlace de red virtual
  + Virtual network
  + Internet
  + Aplicación virtual de red (NVA)
* De forma similar a las rutas del sistema, las UDR también acceden a las tablas de rutas.
* Una tabla de rutas se puede asociar a varias subredes.
* Cada subred solo se puede asociar a una tabla de rutas.
* No se aplica ningún cargo por crear tablas de rutas en Microsoft Azure.

**Escenario empresarial**

Supongamos que tiene una máquina virtual que realiza una función de red, como el enrutamiento, la tarea de firewall o la optimización de WAN. Quiere dirigir cierto tráfico de subred a la NVA. Para realizar esta configuración, puede colocar una NVA entre subredes o entre una subred e Internet. La subred puede usar una UDR para acceder a la NVA y, a continuación, a Internet. La subred puede usar otra UDR y NVA para acceder a la subred de backend. En la ilustración siguiente se destaca este escenario:



**Determinación de los usos del punto de conexión de servicio**

Un *punto de conexión de servicio* de red virtual proporciona la identidad de la red virtual al servicio de Azure. Una vez que los puntos de conexión de servicio se habilitan en la red virtual, puede proteger los recursos de servicio de Azure en la red virtual mediante la incorporación de una *regla de red virtual* a los recursos.

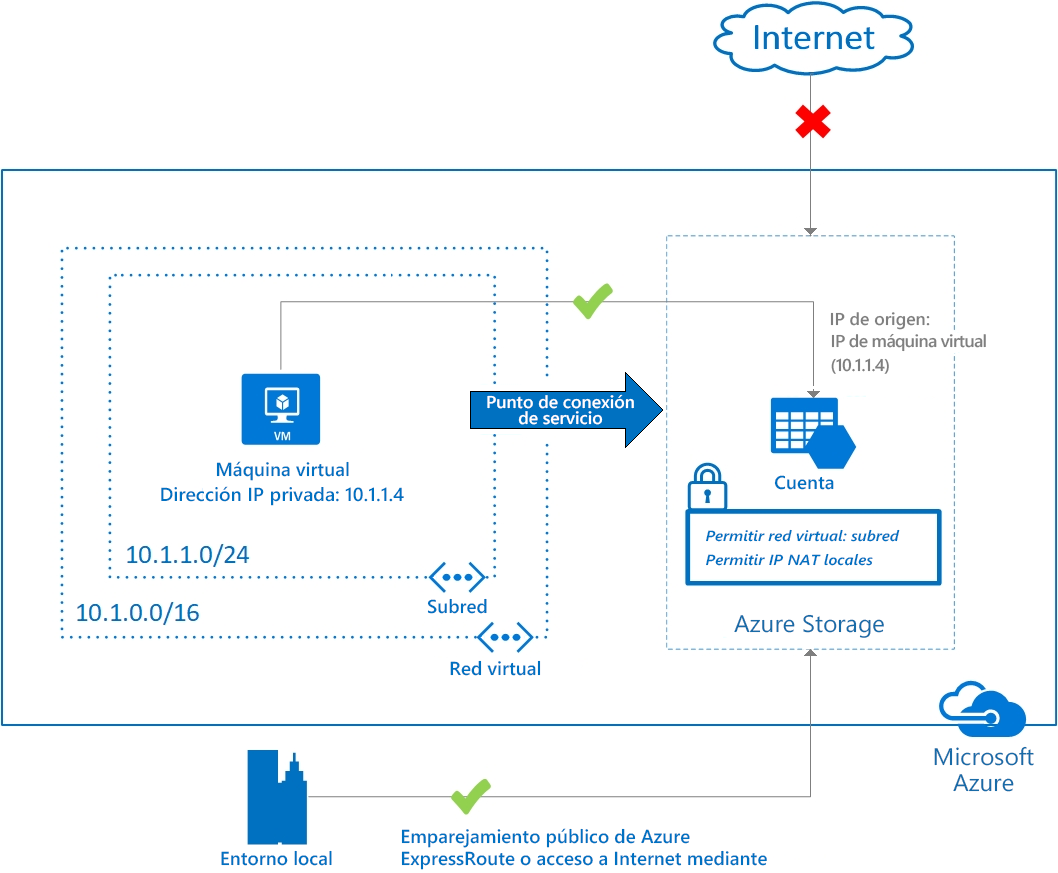
Actualmente, el tráfico del servicio de Azure desde una red virtual usa direcciones IP públicas como direcciones IP de origen. Con los puntos de conexión de servicio, el tráfico del servicio cambia para usar direcciones privadas de red virtual como la direcciones IP de origen al acceder al servicio de Azure desde una red virtual. Este modificador permite acceder a los servicios sin necesidad de direcciones IP públicas y reservadas utilizadas normalmente en los firewalls IP.

**Aspectos que debe conocer sobre los puntos de conexión de servicio**

Revise las siguientes características de los puntos de conexión de servicio.

* Los puntos de conexión de servicio pueden ampliar la identidad de red virtual a los servicios de Azure para proteger los recursos de servicio.
* Los recursos de servicio de Azure se protegen en la red virtual mediante reglas de red virtual.
* Las reglas de red virtual pueden quitar el acceso público a Internet a los recursos y permitir el tráfico solo desde la red virtual.
* Los puntos de conexión de servicio siempre toman el tráfico del servicio directamente de la red virtual al servicio en la red troncal de Microsoft Azure.
* Los puntos de conexión de servicio se configuran mediante la subred. No se requiere ninguna sobrecarga adicional para mantener los puntos de conexión.

En la siguiente ilustración se muestra una máquina virtual que se conecta al servicio de Azure a través de un punto de conexión de servicio. Una máquina virtual de una subred accede a una cuenta de Azure Storage a través de un punto de conexión de servicio. Las reglas de red virtual permiten que la máquina virtual acceda al recurso de servicio de Azure sin comunicarse con Internet.



**Aspectos que se deben tener en cuenta al usar puntos de conexión de servicio**

Hay varios escenarios en los que el uso de puntos de conexión de servicio puede ser ventajoso. Revise los puntos siguientes y piense en cómo puede implementar puntos de conexión de servicio en la configuración.

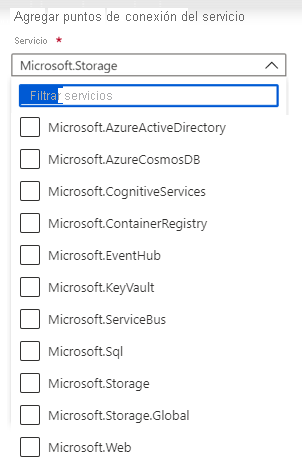
* **Considere la posibilidad de mejorar la seguridad de los recursos**. Implemente puntos de conexión de servicio para mejorar la seguridad de los recursos de servicio de Azure. Cuando los puntos de conexión de servicio están habilitados en la red virtual, los recursos de los servicios de Azure se protegen en la red virtual con reglas de red virtual. Esta regla mejora la seguridad, ya que elimina totalmente el acceso público de Internet a los recursos y solo permite el tráfico que procede de la red virtual.
* **Considere el enrutamiento óptimo para el tráfico de servicio**. Las rutas de la red virtual que fuerzan el tráfico de Internet a las aplicaciones virtuales o locales también suelen forzar al tráfico del servicio de Azure a que realice la misma ruta que el tráfico de Internet. Este proceso de control de tráfico se conoce como *tunelización forzada*. Los puntos de conexión de servicio proporcionan un enrutamiento óptimo para el tráfico de servicio de Azure para que pueda eludir la tunelización forzada.
* **Considere la posibilidad de dirigir el tráfico a la red de Microsoft**. Use puntos de conexión de servicio para mantener el tráfico en la red troncal de Azure. Este enfoque te permite seguir auditando y supervisando el tráfico saliente de Internet desde las redes virtuales, a través de la tunelización forzada, sin que afecte al tráfico del servicio. Obtenga más información sobre las [rutas definidas por el usuario y la tunelización forzada](https://learn.microsoft.com/es-es/azure/firewall/forced-tunneling).
* **Considere la posibilidad de facilitar la configuración y el mantenimiento**. Configure los puntos de conexión de servicio en las subredes para una configuración sencilla y un bajo mantenimiento. Ya no necesita direcciones IP públicas y reservadas en sus redes virtuales para proteger los recursos de Azure a través de una dirección IP del firewall. No hay ningún dispositivo NAT o de puerta de enlace necesario para configurar los puntos de conexión de servicio.

**Nota**

Con los puntos de conexión de servicio, las direcciones IP de las máquinas virtuales cambian de direcciones IPv4 públicas a privadas. Las reglas existentes de firewall de servicio de Azure que utilizan direcciones IP públicas de Azure dejarán de funcionar con este cambio. Asegúrese de que las reglas de firewall de los servicios de Azure permitan este cambio antes de configurar los puntos de conexión de servicio. También es posible que experimente una interrupción temporal del tráfico de servicio desde esta subred mientras configura los puntos de conexión de servicio.

**Determinación de los servicios del punto de conexión de servicio**

Es fácil agregar un punto de conexión de servicio a la red virtual. En Azure Portal, seleccione el servicio de Azure para el que se vaya a crear el punto de conexión. En esta unidad, examinamos varios servicios, como Azure Cosmos DB, Event Hubs, Key Vault y SQL Database.



**Nota**

Se pueden tardar hasta 15 minutos en agregar los puntos de conexión de servicio. Cada integración de punto de conexión de servicio tiene su propia página de documentación de Azure.

| **Servicio** | **Disponibilidad** | **Descripción** |
| --- | --- | --- |
| **Almacenamiento de Azure** | Disponibilidad general en todas las regiones de Azure | Este punto de conexión proporciona al tráfico una ruta óptima hasta el servicio de Azure Storage. Cada cuenta de almacenamiento admite hasta 100 reglas de red virtual. |
| **Azure SQL Database y Azure SQL Data Warehouse** | Disponibilidad general en todas las regiones de Azure | Una característica de seguridad de firewall controla si la base de datos acepta la comunicación de subredes concretas en redes virtuales. Esta característica se aplica al servidor de bases de datos para las bases de datos únicas y el grupo elástico en SQL Database o en las bases de datos de SQL Data Warehouse. |
| **Azure Database for PostgreSQL y Azure Database for MySQL** | Disponibilidad general en las regiones de Azure en las que el servicio de base de datos esté disponible | Las reglas y los puntos de conexión de servicios de red virtual amplían el espacio de direcciones privadas de una red virtual al servidor de Azure Database for PostgreSQL y de Azure Database for MySQL. |
| **Azure Cosmos DB** | Disponibilidad general en todas las regiones de Azure | Puede configurar la cuenta de Azure Cosmos DB para permitir el acceso solo desde una subred específica de una red virtual. Habilite los puntos de conexión de servicio para acceder a Azure Cosmos DB en la subred dentro de una red virtual. El tráfico de la subred se envía a Azure Cosmos DB con la identidad de la subred y la red virtual. Una vez habilitado el punto de conexión de servicio de Azure Cosmos DB, puede limitar el acceso a la subred agregándola a la cuenta de Azure Cosmos DB. |
| **Azure Key Vault** | Disponibilidad general en todas las regiones de Azure | Los puntos de conexión de servicio de red virtual para Key Vault permiten restringir el acceso a una red virtual especificada. También permiten restringir el acceso a una lista de intervalos de direcciones IPv4 (protocolo de Internet, versión 4). A todos los usuarios que se conecten a su almacén de claves desde fuera de esos orígenes se les negará el acceso. |
| **Azure Service Bus y Azure Event Hubs** | Disponibilidad general en todas las regiones de Azure | La integración de Service Bus con los puntos de conexión de servicio de una red virtual permite el acceso seguro a las funcionalidades de mensajería de cargas de trabajo como las de máquinas virtuales que están enlazadas a redes virtuales. La ruta de acceso del tráfico de red está protegida en ambos extremos. |

**Identificación de los usos de Private Link**

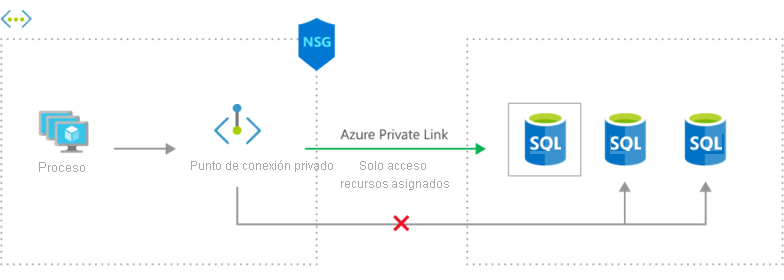
Azure Private Link proporciona conectividad privada desde una red virtual a la plataforma como servicio (PaaS) de Azure, propiedad del cliente o servicios de asociados de Microsoft. Simplifica la arquitectura de red y protege la conexión entre los puntos de conexión de Azure mediante la eliminación de la exposición de los datos a la red pública de Internet.

**Aspectos que se deben conocer sobre Azure Private Link**

Vamos a examinar las características de las configuraciones de enrutamiento de red y Azure Private Link.

* Private Link mantiene el tráfico en la red global de Microsoft. No hay acceso a la red pública de Internet.
* Private Link es global y no hay restricciones regionales. Puede conectarse de forma privada a los servicios que se ejecutan en otras regiones de Azure.
* Puede llevar los servicios entregados en Azure a la red virtual privada mediante la asignación de su red a un punto de conexión privado.
* Private Link puede ofrecer sus propios servicios de forma privada en las redes virtuales de los clientes.
* Todo el tráfico al servicio se puede enrutar a través del punto de conexión privado. No se requieren puertas de enlace, dispositivos NAT, conexiones VPN o Azure ExpressRoute, ni direcciones IP públicas.

En la ilustración siguiente, se muestra una configuración de enrutamiento de red con Azure Private Link. El servicio se conecta a un punto de conexión privado de un grupo de seguridad de red (NSG) mediante Azure SQL Database. Esta configuración impide una conexión directa.



**Aspectos que se deben tener en cuenta al usar Azure Private Link**

Hay muchas ventajas para trabajar con Azure Private Link. Revise los puntos siguientes y tenga en cuenta cómo puede implementar el servicio para sus escenarios.

* **Considere usar la conectividad privada a los servicios de Azure**. Conéctese de forma privada a los servicios que se ejecutan en otras regiones de Azure. El tráfico permanece en la red de Microsoft, sin acceso a la red pública de Internet.
* **Considere usar la integración con redes locales y emparejadas**. Acceda a puntos de conexión privados mediante el emparejamiento privado o túneles VPN desde redes virtuales locales o emparejadas. Microsoft hospeda el tráfico, por lo que no es necesario configurar el emparejamiento público ni usar Internet para migrar las cargas de trabajo a la nube.
* **Considere usar la protección contra la filtración de datos de recursos de Azure**. Asigne puntos de conexión privados a recursos de PaaS de Azure. Durante un incidente de seguridad dentro de la red, solo se podrá acceder a los recursos asignados. Esta implementación elimina la amenaza de la filtración de datos.
* **Considere usar los servicios entregados directamente a las redes virtuales de los clientes**. Consuma de forma privada servicios de PaaS de Azure, de asociados de Microsoft y los suyos propios en sus redes virtuales en Azure. Private Link funciona en los inquilinos de Microsoft Entra para ayudar a unificar su experiencia entre servicios. Envíe, apruebe o rechace solicitudes directamente sin permisos ni controles de acceso basados en roles.

**Prueba de conocimientos**

Su empresa está implementando aplicaciones virtuales de red y está desarrollando el plan para asegurarse de que el tráfico se enruta correctamente al dispositivo adecuado. Está trabajando para implementar rutas de red personalizadas, puntos de conexión de servicio y vínculos privados para garantizar la seguridad de los datos del cliente. Algunos equipos han enviado sus requisitos de configuración y sus preguntas para que los evalúe:

* Su empresa debe ampliar su espacio de direcciones privadas en Azure proporcionando una conexión directa a los recursos de Azure.
* El equipo de TI necesita una lista de los tipos de próximo salto válidos.
* El equipo de infraestructura ha solicitado información general sobre las funcionalidades y requisitos de enrutamiento de Azure.

**Responda a las siguientes preguntas**

Elija la respuesta más adecuada para cada una de las siguientes preguntas. Después, seleccione **Comprobar las respuestas**.

Principio del formulario

**1. ¿Qué afirmación describe mejor el enrutamiento de Azure?**

1. Los administradores pueden crear rutas del sistema.
2. Cuando el tipo del próximo salto es *Ninguno*, se anula el tráfico.
3. Se necesitan puertas de enlace de Azure para enrutar el tráfico entre subredes.

**2. ¿Qué es un tipo de próximo salto válido?**

1. Load Balancer
2. ExpressRoute
3. Internet

**3. ¿Cómo puede ampliar el espacio de direcciones privadas de la empresa con conexiones directas a recursos de Azure?**

1. Puntos de conexión de Virtual Network
2. Rutas definidas por el usuario
3. Dispositivos virtuales
4. B
5. C
6. A

Final del formulario

**Resumen y recursos**

Las rutas de red controlan el flujo de tráfico por la red. Puede personalizar estas rutas e implementar puntos de conexión de servicio, y trabajar con vínculos privados.

En este módulo, ha aprendido a implementar rutas del sistema y rutas definidas por el usuario. Ha identificado las características y los casos de uso de Azure Private Link y los servicios de punto de conexión. Ha explorado cómo configurar una ruta personalizada y ha descubierto cómo trabajar con puntos de conexión de servicio.