**Introducción**

Este módulo está diseñado para proporcionar a los administradores los conocimientos y aptitudes necesarios para planear e implementar medidas de seguridad sólidas para redes virtuales de Azure, garantizando la confidencialidad, integridad y disponibilidad de los recursos de red.

**Escenario**

Imagine que es un especialista en seguridad de red de Azure responsable de proteger las redes virtuales en el entorno en la nube de su organización. Su organización se basa en los servicios de Azure y necesita un conocimiento exhaustivo de la seguridad de red, desde los grupos de seguridad de red (NSG) hasta el cifrado a través de ExpressRoute.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Planee e implemente medidas de seguridad para redes virtuales en Azure para proteger los datos y los recursos.
* Use eficazmente grupos de seguridad de red (NSG) y grupos de seguridad de aplicaciones (ASG) para proteger el tráfico de red.
* Cree y administre rutas definidas por el usuario (UDR) para optimizar el enrutamiento del tráfico de red.
* Establezca el emparejamiento de red virtual o las puertas de enlace de VPN para la conectividad de red segura.
* Planee e implemente Virtual WAN, incluidos los centros virtuales protegidos, para la administración de red optimizada.
* Proteja la conectividad VPN, incluidas las configuraciones de punto a sitio y de sitio a sitio, para el acceso remoto y la conectividad de rama.
* Implemente el cifrado a través de ExpressRoute para garantizar la privacidad y la integridad de los datos.
* Configure las opciones de firewall en los recursos de plataforma como servicio (PaaS) para controlar el tráfico entrante y saliente.
* Supervise la seguridad de red de forma eficaz mediante Network Watcher, incluido el registro de flujo de NSG para la detección y el análisis de amenazas.

**Objetivos**

El módulo tiene como objetivo dotar a los participantes con los conocimientos y la experiencia necesarios para diseñar, implementar y mantener un entorno de red virtual altamente seguro en Azure. Los participantes podrán proteger los datos confidenciales, las aplicaciones y los recursos frente a posibles amenazas y vulnerabilidades, a la vez que mantienen la integridad y disponibilidad de la red.

**Planificación e implementación de grupos de seguridad de red (NSG) y grupos de seguridad de aplicaciones (ASG)**

Puede usar el grupo de seguridad de red de Azure para filtrar el tráfico de red entre los recursos de Azure de una red virtual de Azure. Un grupo de seguridad de red contiene reglas de seguridad que permiten o deniegan el tráfico de red entrante o el tráfico de red saliente de varios tipos de recursos de Azure. En todas las reglas, puede **especificar un origen y destino**, un **puerto** y un **protocolo**.

**Grupos de seguridad de red**

**Reglas de seguridad**

Un grupo de seguridad de red contiene tantas reglas como desee, siempre que esté dentro de los límites de la suscripción de Azure. Cada regla especifica las siguientes propiedades:

| **Propiedad** | **Explicación** |
| --- | --- |
| Nombre | Un nombre único dentro del grupo de seguridad de red. El nombre puede tener hasta 80 caracteres. Debe comenzar con un carácter de palabra y debe terminar con un carácter de palabra o con "\_". El nombre puede contener caracteres de palabra o ".", "-", "\_". |
| Priority | Un número entre 100 y 4096. Las reglas se procesan en orden de prioridad. Se procesan primero las reglas con los números más bajos ya que estos tienen más prioridad. Si el tráfico coincide con una regla, se detiene el procesamiento. Como resultado, las reglas con menor prioridad (números más altos) que tengan los mismos atributos que las reglas con una prioridad mayor no se procesarán. Las reglas de seguridad predeterminadas de Azure reciben el número más alto con la prioridad más baja para asegurarse de que las reglas personalizadas siempre se procesan primero. |
| Origen o destino | Cualquiera, una dirección IP individual, un bloque CIDR de enrutamiento entre dominios sin clases (10.0.0.0/24, por ejemplo), una etiqueta de servicio o un grupo de seguridad de aplicaciones. Si especifica una dirección para un recurso de Azure, especifique la dirección IP privada asignada al recurso. Las grupos de seguridad de red se procesan después de que Azure traduzca una dirección IP pública a una dirección IP privada para el tráfico de entrada y antes de que Azure traduzca una dirección IP privada a una dirección IP pública para el tráfico de salida. Se necesitan menos reglas de seguridad cuando se especifica un intervalo, una etiqueta de servicio o un grupo de seguridad de aplicaciones. La posibilidad de especificar varias direcciones IP individuales e intervalos (no puede especificar varias etiquetas de servicio ni grupos de aplicaciones) en una regla se conoce como reglas de seguridad aumentada. Las reglas de seguridad aumentada solo se pueden generar en los grupos de seguridad de red creados mediante el modelo de implementación de Resource Manager. No puede especificar varias direcciones IP ni intervalos de ellas en grupos de seguridad de red creados mediante el modelo de implementación clásica. |
| Protocolo | TCP, UDP, ICMP, ESP, AH o cualquiera. Los protocolos ESP y AH no están disponibles actualmente a través de Azure Portal, pero se pueden usar a través de plantillas de Azure Resource Manager. |
| Dirección | Si la regla se aplica al tráfico entrante o al saliente. |
| Intervalo de puertos | Puede especificar un puerto individual o un intervalo de puertos. Por ejemplo, puede especificar 80 o 10000-10005. La especificación de intervalos le permite crear menos reglas de seguridad. Las reglas de seguridad aumentada solo se pueden generar en los grupos de seguridad de red creados mediante el modelo de implementación de Resource Manager. No puede especificar varios puertos ni intervalos de ellos en la misma regla de seguridad de los grupos de seguridad de red creados mediante el modelo de implementación clásica. |
| Acción | Permitir o denegar |

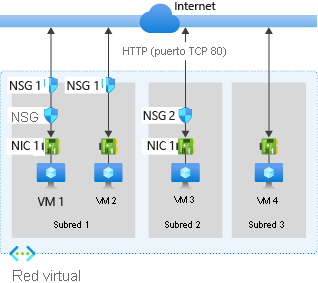
Las reglas de seguridad se evalúan y aplican en función de la información de cinco tuplas (**1. origen, 2. puerto de origen, 3. destino, 4. puerto de destino y 5. protocolo**). No puede crear dos reglas de seguridad con la misma prioridad y dirección. Se crea un registro de flujo para las conexiones existentes. Se permite o deniega la comunicación en función del estado de conexión del registro de flujo. El registro de flujo permite que un grupo de seguridad de red sea con estado. Por ejemplo, si especifica una regla de seguridad de salida para cualquier dirección a través del puerto 80, no será necesario especificar una regla de seguridad de entrada para la respuesta al tráfico saliente. Solo debe especificar una regla de seguridad de entrada si la comunicación se inicia de forma externa. Lo contrario también es cierto. Si se permite el tráfico entrante a través de un puerto, no es necesario especificar una regla de seguridad de salida para responder al tráfico a través del puerto.

No es posible interrumpir las conexiones existentes cuando se elimina una regla de seguridad que permitió la conexión. Al modificar las reglas de grupo de seguridad de red, solo se verán afectadas las nuevas conexiones. Cuando se crea una nueva regla o se actualiza una regla ya existente en un grupo de seguridad de red, solo se aplicará a las nuevas conexiones. Las conexiones ya existentes no se reevalúan con las nuevas reglas.

No es posible interrumpir las conexiones existentes cuando se elimina una regla de seguridad que permitió la conexión. Al modificar las reglas de grupo de seguridad de red, solo se verán afectadas las nuevas conexiones. Cuando se crea una nueva regla o se actualiza una regla ya existente en un grupo de seguridad de red, solo se aplicará a las nuevas conexiones. Las conexiones ya existentes no se reevalúan con las nuevas reglas.

**Cómo filtran el tráfico de red los grupos de seguridad de red**

Puede implementar recursos de varios servicios de Azure en una red virtual de Azure. Puede asociar cero o un grupo de seguridad de red a cada subred e interfaz de red de la red virtual en una máquina virtual. El mismo grupo de seguridad de red se puede asociar a tantas interfaces de red y subredes como se desee. La siguiente imagen ilustra los diferentes escenarios de cómo se podrían implementar grupos de seguridad de red para **permitir el tráfico de red hacia y desde Internet a través del puerto TCP 80**:



Consulte la imagen, junto con el texto siguiente, para conocer la forma Azure procesa las reglas de entrada y salida para los grupos de seguridad de red:

**Tráfico entrante**

Para el tráfico entrante, Azure procesa las reglas de un grupo de seguridad de red asociadas a una subred en primer lugar, si hay alguna y, a continuación, las reglas de un grupo de seguridad de red asociadas a la interfaz de red, si hay alguna. Este proceso incluye también el tráfico dentro de la subred.

* VM1: las reglas de seguridad de *NSG1* se procesan, ya que está asociado a *Subnet 1* y *VM1* está en *Subnet 1*. A menos que haya creado una regla que permita el puerto 80 entrante, la regla de seguridad predeterminada **DenyAllInbound** deniega el tráfico. El tráfico no se evalúa mediante NSG2 porque está asociado a la interfaz de red. Si *NSG1* permite el puerto 80 en su regla de seguridad, *NSG2* procesa el tráfico. Para permitir el puerto 80 para la máquina virtual, tanto *NSG1* como *NSG2* deben tener una regla que permita el puerto 80 desde Internet.
* VM2: las reglas de *NSG1* se procesan porque *VM2* también está en *Subnet 1*. Puesto que *VM2* no tiene un grupo de seguridad de red asociado a su interfaz de red, recibe todo el tráfico permitido por *NSG1* o se deniega todo el tráfico denegado por *NSG1*. El tráfico se permite o deniega a todos los recursos de la misma subred cuando un grupo de seguridad de red está asociado a una subred.
* VM3: al no haber ningún grupo de seguridad de red asociado a *Subnet 2*, se permite el tráfico en la subred y *NSG2* lo procesa, ya que *NSG2* está asociado a la interfaz de red conectada a *VM3*.
* VM4: se permite el tráfico a *VM4,* ya que un grupo de seguridad de red no está asociado a *Subnet 3* ni a la interfaz de red de la máquina virtual. Si no tienen un grupo de seguridad de red asociado, se permite todo el tráfico de red a través de una subred y una interfaz de red.

**Tráfico saliente**

Para el tráfico saliente, Azure procesa las reglas de un grupo de seguridad de red asociadas a una interfaz de red en primer lugar, si hay alguna y, a continuación, las reglas de un grupo de seguridad de red asociadas a la subred, si hay alguna. Este proceso incluye también el tráfico dentro de la subred.

* VM1: se procesan las reglas de seguridad de *NSG2*. La regla de seguridad predeterminada **AllowInternetOutbound** permite el tráfico de *NSG1* y *NSG2*, a menos que cree una regla de seguridad que deniegue el puerto 80 de salida a Internet. Si *NSG2* deniega el puerto 80 en su regla de seguridad, deniega el tráfico y *NSG1* nunca lo evalúa. Para denegar el puerto 80 desde la máquina virtual, uno o ambos de los grupos de seguridad de red deben tener una regla que deniegue el puerto 80 a Internet.
* VM2: todo el tráfico se envía a través de la interfaz de red a la subred, ya que la interfaz de red conectada a *VM2* no tiene un grupo de seguridad de red asociado. Se procesan las reglas de *NSG1*.
* VM3: si *NSG2* deniega el puerto 80 en su regla de seguridad, deniega el tráfico. Si *NSG2* no deniega el puerto 80, la regla de seguridad predeterminada **AllowInternetOutbound** de *NSG2* permite el tráfico, ya que no hay ningún grupo de seguridad de red asociado a *Subnet2*.
* VM4: se permite todo el tráfico desde *VM4*, porque un grupo de seguridad de red no está asociado a la interfaz de red conectada a la máquina virtual, ni a *Subnet3*.

**Tráfico dentro de la subred**

Es importante tener en cuenta que las reglas de seguridad de un NSG asociado a una subred pueden afectar la conectividad entre las máquinas virtuales dentro de ella. De manera predeterminada, las máquinas virtuales de la misma subred pueden comunicarse en función de una regla de NSG predeterminada que permita el tráfico dentro de la subred. Si agrega una regla a *NSG1* que deniega todo el tráfico entrante y saliente, *VM1* y *VM2* no podrán comunicarse entre sí.

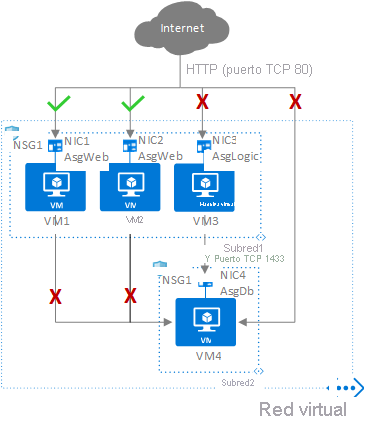
Puede ver fácilmente las reglas agregadas que se aplican a una interfaz de red mediante la visualización de las **reglas de seguridad vigentes** de una interfaz de red. También puede usar la funcionalidad **Comprobación del flujo de IP** de Azure Network Watcher para determinar si se permite la comunicación hacia una interfaz de red o desde esta. Puede usar la comprobación del flujo de IP para determinar si se permite o se deniega una comunicación. Además, use la comprobación del flujo de IP para exponer la identidad de la regla de seguridad de red responsable de permitir o denegar el tráfico.

Los grupos de seguridad de red se asocian a las subredes o a las máquinas virtuales y a los servicios en la nube que se implementan en el modelo de implementación clásica, y en las subredes o interfaces de red del modelo de implementación de Resource Manager.

A menos que tenga un motivo concreto, se recomienda que asocie un grupo de seguridad de red a una subred o a una interfaz de red, pero no a ambas. Puesto que las reglas de un grupo de seguridad de red asociado a una subred pueden entrar en conflicto con las reglas de un grupo de seguridad de red asociado a una interfaz de red, puede tener problemas de comunicación inesperados que necesiten solución.

**Grupos de seguridad de aplicaciones (ASG)**

Los grupos de seguridad de aplicaciones le permiten configurar la seguridad de red como una extensión natural de la estructura de una aplicación, lo que le permite agrupar máquinas virtuales y directivas de seguridad de red basadas en esos grupos. Puede reutilizar la directiva de seguridad a escala sin mantenimiento manual de direcciones IP explícitas. La plataforma controla la complejidad de las direcciones IP explícitas y de varios conjuntos de reglas, lo que le permite centrarse en su lógica de negocios. Para entender mejor los grupos de seguridad de aplicaciones, considere el ejemplo siguiente:



En la imagen anterior, *NIC1* y *NIC2* son miembros del grupo de seguridad de aplicaciones *AsgWeb*. *NIC3* es miembro del grupo de seguridad de aplicaciones *AsgLogic*. *NIC4* es miembro del grupo de seguridad de aplicaciones *AsgDb*. Aunque cada interfaz de red (NIC) de este ejemplo solo es miembro de un grupo de seguridad de aplicaciones, una interfaz de red puede ser miembro de varios grupos de seguridad de aplicaciones, hasta los límites de Azure. Ninguna de las interfaces de red tiene un grupo de seguridad de red asociado. *NSG1* está asociado a ambas subredes y contiene las siguientes reglas:

**Allow-HTTP-Inbound-Internet**

Esta regla es necesaria para permitir el tráfico de Internet a los servidores web. Dado que la regla de seguridad predeterminada DenyAllInbound deniega el tráfico entrante desde Internet, no es necesaria ninguna regla extra para los grupos de seguridad de aplicaciones *AsgLogic* y *AsgDb*.

| **Prioridad** | **Origen** | **Puertos de origen** | **Destino** | **Puertos de destino** | **Protocolo** | **Acceder** |
| --- | --- | --- | --- | --- | --- | --- |
| 100 | Internet | \* | AsgWeb | 80 | TCP | Allow |

**Deny-Database-All**

Dado que la regla de seguridad predeterminada AllowVNetInBound permite todas las comunicaciones entre los recursos de la misma red virtual, se necesita esta regla para denegar el tráfico desde todos los recursos.

| **Prioridad** | **Origen** | **Puertos de origen** | **Destino** | **Puertos de destino** | **Protocolo** | **Acceder** |
| --- | --- | --- | --- | --- | --- | --- |
| 120 | \* | \* | AsgDb | 1433 | Any | Denegar |

**Allow-Database-BusinessLogic**

Esta regla permite el tráfico desde el grupo de seguridad de aplicaciones *AsgLogic* al grupo de seguridad de aplicaciones *AsgDb*. La prioridad de esta regla es mayor que la prioridad de la regla *Deny-Database-All*. Como resultado, esta regla se procesa antes que la regla *Deny-Database-All*, por lo que se permite el tráfico del grupo de seguridad de aplicaciones *AsgLogic*, mientras que el resto del tráfico es bloqueado.

| **Prioridad** | **Origen** | **Puertos de origen** | **Destino** | **Puertos de destino** | **Protocolo** | **Acceder** |
| --- | --- | --- | --- | --- | --- | --- |
| 110 | AsgLogic | \* | AsgDb | 1433 | TCP | Allow |

Las interfaces de red que son miembros del grupo de seguridad de aplicaciones aplican las reglas que la especifican como origen o destino. Las reglas no afectan a otras interfaces de red. Si la interfaz de red no es miembro de un grupo de seguridad de aplicaciones, la regla no se aplica a la interfaz de red aunque el grupo de seguridad de red esté asociado a la subred.

Los grupos de seguridad de aplicaciones presentan las siguientes restricciones:

* Hay límites en el número de grupos de seguridad de aplicaciones que puede tener en una suscripción y otros límites relacionados con los grupos de seguridad de aplicaciones.
* Todas las interfaces de red asignadas a un grupo de seguridad de aplicaciones deben existir en la misma red virtual en la que se encuentra la primera interfaz de red asignada a dicho grupo. Por ejemplo, si la primera interfaz de red asignada a un grupo de seguridad de aplicaciones llamado *AsgWeb* está en la red virtual llamada *VNet1*, todas las sucesivas interfaces de red asignadas a *ASGWeb* deben existir en *VNet1*. No se pueden agregar interfaces de red de distintas redes virtuales al mismo grupo de seguridad de aplicaciones.
* Si especifica grupos de seguridad de aplicaciones como origen y destino de una regla de seguridad, las interfaces de red de ambos grupos de seguridad de aplicaciones deben existir en la misma red virtual.
  + Un ejemplo sería si *AsgLogic* tuviera interfaces de red de *VNet1* y *AsgDb* tuviera interfaces de red de *VNet2*. En este caso, sería imposible asignar *AsgLogic* como origen y *AsgDb* como destino en una regla. Todas las interfaces de red para los grupos de seguridad de aplicaciones de origen y de destino deben existir en la misma red virtual.

Para minimizar el número de reglas de seguridad que necesita y la necesidad de cambiar las reglas, planee los grupos de seguridad de aplicaciones que necesita y cree reglas mediante etiquetas de servicio o grupos de seguridad de aplicaciones en lugar de direcciones IP individuales o intervalos de direcciones IP siempre que sea posible.

**Planeamiento e implementación de las rutas definidas por el usuario (UDR)**

En Azure se pueden crear rutas **personalizadas** o **definidas por el usuario (estáticas)** para reemplazar las rutas del sistema predeterminadas o para agregar más rutas a una tabla de rutas de una subred. En Azure, cree una tabla de rutas y asóciela a cero o más subredes de red virtual. Cada subred puede tener cero o una ruta de tablas de ruta asociada. Para obtener información acerca del número máximo de rutas que puede agregar a una tabla de rutas y del número máximo de tablas de rutas definidas por el usuario que se pueden crear por suscripción de Azure, consulte el artículo acerca de los límites de Azure. Si crea una tabla de rutas y la asocia a una subred, las rutas de la tabla se combinan con las rutas predeterminadas de la subred. Si hay asignaciones de rutas en conflicto, las rutas definidas por el usuario invalidarán las rutas predeterminadas.

Puede especificar los siguientes tipos de próximo salto al crear una ruta definida por el usuario:

* Aplicación virtual: una aplicación virtual es una máquina virtual que ejecuta normalmente una aplicación de red como, por ejemplo, un firewall. Para más información sobre las aplicaciones virtuales de red preconfiguradas que se pueden implementar en una red virtual, visite Azure Marketplace. Al crear una ruta con el tipo de salto de aplicación virtual, especifique también una dirección IP del próximo salto. La dirección IP puede ser:  
  + La dirección IP privada de una interfaz de red conectada a una máquina virtual. Cualquier interfaz de red conectada a una máquina virtual que reenvíe el tráfico de red a una dirección que no sea la suya propia debe tener la opción Habilitar reenvío de IP habilitada. El valor deshabilita la comprobación que realiza Azure del origen y destino en una interfaz de red. Obtenga más información acerca de cómo habilitar el reenvío IP en una interfaz de red. Aunque Habilitar reenvío de IP es un valor de Azure, es posible que también necesite habilitar el reenvío IP en el sistema operativo de la máquina virtual para que el dispositivo desvíe el tráfico entre las direcciones IP privadas asignadas a interfaces de red de Azure. Si el dispositivo necesita enrutar el tráfico a una dirección IP pública, debe redirigir mediante proxy el tráfico o realizar la traducción de direcciones de red (NAT) desde la dirección IP privada del origen hasta su propia dirección IP privada. Después, Azure realiza la NAT en una dirección IP pública antes de enviar el tráfico a Internet. Para determinar la configuración necesaria en la máquina virtual, consulte la documentación del sistema operativo o la aplicación de red.
  + La dirección IP privada de un equilibrador de carga interno de Azure. A menudo se usa un equilibrador de carga como parte de una estrategia de alta disponibilidad para aplicaciones virtuales de red.

Puede definir una ruta usando 0.0.0.0/0 como prefijo de la dirección y un tipo de próximo salto de aplicación virtual. Esta configuración permite al dispositivo inspeccionar el tráfico y determinar si se reenvía o se anula el tráfico. Si tiene intención de crear una definida por el usuario que contenga el prefijo de dirección 0.0.0.0/0, consulte antes el apartado 0.0.0.0/0 address prefix (Prefijo de dirección 0.0.0.0/0).

* **Puerta de enlace de red virtual**: se especifica cuando se desea que el tráfico destinado a prefijos de dirección específicos se enrute a una puerta de enlace de red virtual. La puerta de enlace de red virtual debe crearse con el tipo VPN. No se puede especificar una puerta de enlace de red virtual creada con el tipo ExpressRoute en una ruta definida por el usuario, ya que con ExpressRoute es preciso usar BGP para las rutas personalizadas. Tampoco puede especificar puertas de red virtuales si tiene conexiones VPN y ExpressRoute coexistentes. Puede definir una ruta que dirige el tráfico destinado al prefijo de dirección 0.0.0.0/0 a una puerta de enlace de red virtual basada en ruta. En un entorno local, puede tener un dispositivo que compruebe el tráfico y determine si se reenvía o se elimina. Si tiene intención de crear una definida por el usuario para el prefijo de dirección 0.0.0.0/0, consulte antes el apartado 0.0.0.0/0 address prefix (Prefijo de dirección 0.0.0.0/0). En lugar de configurar una ruta definida por el usuario para el prefijo de dirección 0.0.0.0/0, es posible anunciar una ruta con el prefijo 0.0.0.0/0 a través de BGP, si ha habilitado BGP para una puerta de enlace de red virtual de VPN.
* **Ninguna**: se especifica cuando se desea colocar tráfico en un prefijo de dirección, en lugar de reenviar el tráfico a un destino. Si no ha configurado completamente una funcionalidad, Azure puede enumerar No para algunas de las rutas de opcional del sistema. Por ejemplo, si ve No en Dirección IP del próximo salto con un Tipo de próximo salto de Puerta de enlace de red virtual o Aplicación virtual, puede deberse a que el dispositivo no funciona o no está completamente configurado. Azure crea rutas predeterminadas del sistema para los prefijos de direcciones reservados con No como tipo de próximo salto.
* **Red virtual**: Especifique la opción Red virtual cuando desee invalidar el enrutamiento predeterminado dentro de una red virtual.
* **Internet**: Especifique la opción Internet cuando desee enrutar explícitamente el tráfico destinado a un prefijo de dirección a Internet, o si desea que el tráfico destinado a los servicios de Azure con direcciones IP públicas se mantenga dentro de la red troncal de Azure.

En las rutas definidas por el usuario, no se puede especificar emparejamiento de red virtual o VirtualNetworkServiceEndpoint como tipo de próximo salto. Las rutas con los tipos de próximo salto emparejamiento de red virtual o VirtualNetworkServiceEndpoint solo las crea Azure al configurar un emparejamiento de red virtual o un punto de conexión de servicio.

**Etiquetas de servicio para rutas definidas por el usuario**

Ahora puede especificar una etiqueta de servicio como prefijo de dirección de una ruta definida por el usuario en lugar de un intervalo IP explícito. Una etiqueta de servicio representa un grupo de prefijos de direcciones IP de un servicio de Azure determinado. Microsoft administra los prefijos de direcciones que la etiqueta de servicio incluye y actualiza automáticamente dicha etiqueta a medida que las direcciones cambian. Así se minimiza la complejidad de las actualizaciones frecuentes de las rutas definidas por el usuario y se reduce el número de rutas que hay que crear. Actualmente, puede crear hasta 25 rutas con etiquetas de servicio en cada tabla de rutas. Con esta versión, también se admite el uso de etiquetas de servicio en escenarios de enrutamiento para contenedores.

**Coincidencia exacta**

El sistema da preferencia a la ruta con el prefijo explícito cuando hay una coincidencia exacta de prefijo entre una ruta con un prefijo de IP explícito y una ruta con una etiqueta de servicio. Cuando varias rutas con etiquetas de servicio tienen prefijos de IP que coinciden, las rutas se evalúan en el orden siguiente:

1. Etiquetas regionales (por ejemplo, Storage.EastUS, AppService.AustraliaCentral)
2. Etiquetas de nivel superior (por ejemplo, Storage, AppService)
3. Etiquetas regionales de AzureCloud (por ejemplo, AzureCloud.canadacentral, AzureCloud.eastasia)
4. La etiqueta de AzureCloud

Para usar esta característica, especifique un nombre de etiqueta de servicio para el parámetro de prefijo de dirección en los comandos de la tabla de rutas. Por ejemplo, en PowerShell puede crear una nueva ruta para dirigir el tráfico enviado a un prefijo IP de Azure Storage a una aplicación virtual mediante:

Azure PowerShellCopy

$param = @{

Name = 'StorageRoute' AddressPrefix = 'Storage' NextHopType = 'VirtualAppliance' NextHopIpAddress = '10.0.100.4' } New-AzRouteConfig @param

El mismo comando para la CLI es el siguiente:

Azure CLI

az network route-table route create \

--resource-group MyResourceGroup \ --route-table-name MyRouteTable \ --name StorageRoute \ --address-prefix Storage \ --next-hop-type VirtualAppliance \ --next-hop-ip-address 10.0.100.4

**Planee e implemente el emparejamiento de red virtual o puerta de enlace**

Una red virtual es una parte virtual y aislada de la red pública de Azure. De manera predeterminada, no se puede enrutar el tráfico entre dos redes virtuales. Sin embargo, es posible conectar redes virtuales, ya sea dentro de una sola región o en dos regiones, de modo que se pueda enrutar el tráfico entre ellas.

**Tipos de conexiones de Virtual Network**

Emparejamiento de red virtual. El emparejamiento de red virtual conecta dos redes virtuales de Azure. Una vez emparejadas, las redes virtuales aparecen como una sola a efectos de conectividad. El tráfico entre las máquinas virtuales en las redes virtuales emparejadas se enruta a través de la infraestructura de red troncal de Microsoft, únicamente a través de direcciones IP privadas. No implica la red pública de Internet. También puede emparejar redes virtuales entre regiones de Azure (emparejamiento global).

Instancias de VPN Gateway. VPN Gateway es un tipo específico de puerta de enlace de red virtual que se usa para enviar tráfico entre una red virtual de Azure y una ubicación local a través de la red pública de Internet. También puede utilizar una instancia de VPN Gateway para enviar tráfico entre redes virtuales de Azure. Cada red virtual puede tener una instancia de VPN Gateway como máximo. Debe habilitar Azure DDOS Protection Standard en cualquier red virtual perimetral.

El emparejamiento de red virtual proporciona una conexión de baja latencia y ancho de banda alto. No hay ninguna puerta de enlace en la ruta de acceso, por lo que no hay saltos adicionales, lo que garantiza conexiones de latencia baja. Es útil en escenarios como la replicación de datos entre regiones y la conmutación por error de base de datos. Dado que el tráfico es privado y permanece en la red troncal de Microsoft, considere también el emparejamiento de red virtual si tiene directivas de datos estrictas y quiere evitar el envío de tráfico a través de Internet.

Las instancias de VPN Gateway proporcionan una conexión de ancho de banda limitado y son útiles en escenarios donde se necesita cifrado, pero pueden tolerar restricciones de ancho de banda. En estos casos, los clientes tampoco son tan susceptibles a la latencia.

**Tránsito de puerta de enlace**

El emparejamiento de red virtual y las instancias de VPN Gateway también pueden coexistir a través del tránsito de puerta de enlace.

El tránsito de puerta de enlace le permite usar la puerta de enlace de una red virtual emparejada para conectarse en el entorno local, en lugar de crear una nueva puerta de enlace para la conectividad. A medida que aumente las cargas de trabajo en Azure, deberá escalar las redes entre regiones y redes virtuales para mantener el crecimiento. El tránsito de puerta de enlace le permite compartir una puerta de enlace de ExpressRoute o una instancia de VPN Gateway con todas las redes virtuales emparejadas, así como administrar la conectividad en un solo lugar. El uso compartido permite ahorrar costos y reducir la sobrecarga de administración.

Con el tránsito de puerta de enlace habilitado en el emparejamiento de red virtual, puede crear una red virtual de tránsito que contenga la instancia de VPN Gateway, el dispositivo de red virtual y otros servicios compartidos. A medida que la organización crece con nuevas aplicaciones o unidades de negocio y pone en marcha nuevas redes virtuales, puede conectarse a la red virtual de tránsito mediante el emparejamiento. Esto evita agregar complejidad a la red y reduce la sobrecarga de administración que supone administrar varias puertas de enlace y otros dispositivos.

**Configuración de conexiones**

El emparejamiento de red virtual y las instancias de VPN Gateway admiten los siguientes tipos de conexión:

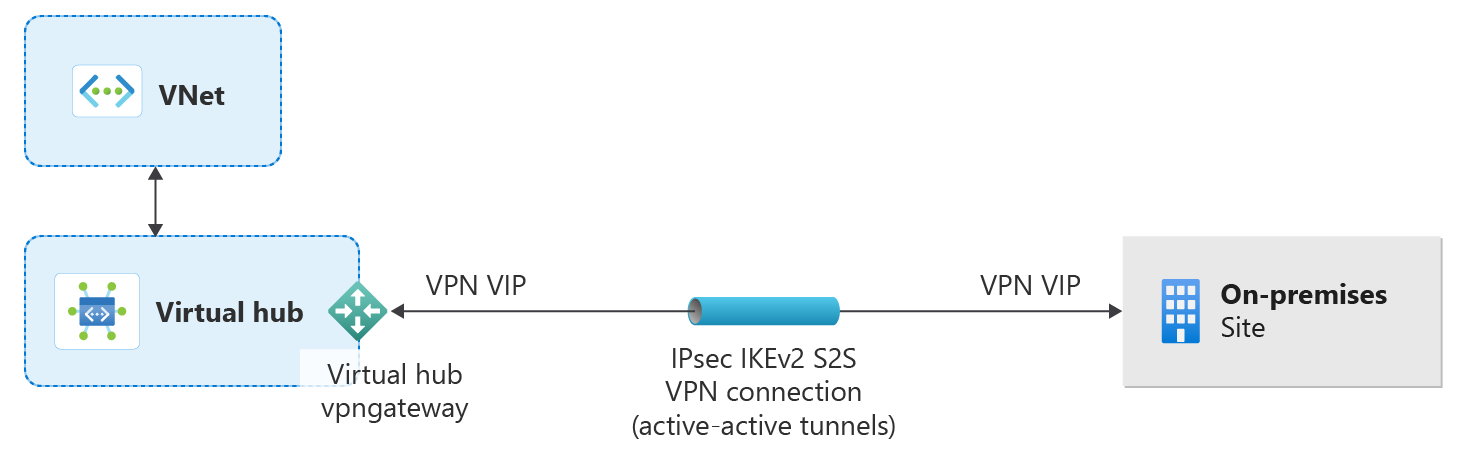
* Redes virtuales en regiones diferentes.
* Redes virtuales en distintos inquilinos de Microsoft Entra.
* Redes virtuales en diferentes suscripciones de Azure.
* Redes virtuales que usan una combinación de modelos de implementación de Azure (clásico y de Resource Manager).

**Comparación del emparejamiento de red virtual y VPN Gateway**

| **Elemento** | **Interconexión de red virtual** | **VPN Gateway** |
| --- | --- | --- |
| Límites | Hasta 500 emparejamientos de red virtual por red virtual | Una instancia de VPN Gateway por cada red virtual. El número máximo de túneles por puerta de enlace depende del SKU de puerta de enlace. |
| Modelo de precios | Entrada/salida | Cada hora y salida |
| Cifrado | Se recomienda el cifrado de nivel de software. | La directiva de IPsec o IKE personalizada se puede aplicar a las conexiones nuevas o existentes. |
| Limitaciones de ancho de banda | Sin limitaciones de ancho de banda. | Varía en función del SKU. |
| ¿Es privado? | Sí. Se enruta a través de la red troncal de Microsoft y de forma privada. No implica la red pública de Internet. | IP pública implicada, pero enrutada a través de la red troncal de Microsoft si está habilitada la red global de Microsoft. |
| Relación transitiva | Las conexiones de emparejamiento no son transitivas. Las redes transitivas se pueden lograr mediante NVA o puertas de enlace en la red virtual del centro de conectividad. | Si las redes virtuales están conectadas a través de instancias de VPN Gateway y BGP está habilitado en las conexiones de red virtual, la transitividad funciona. |
| Tiempo de instalación inicial | Fast (rápido) | 30 minutos aproximadamente |
| Escenarios típicos | La replicación de datos, la conmutación por error de base de datos y otros escenarios necesitan copias de seguridad frecuentes de datos de gran tamaño. | Escenarios específicos de cifrado que no son susceptibles a la latencia y no necesitan un rendimiento alto. |

**Planee e implemente Virtual Wide Area Network, incluyendo el centro virtual protegido**

Usar Virtual WAN para conectarse a los recursos de Azure a través de una conexión VPN de IPsec/IKE (IKEv1 e IKEv2). Este tipo de conexión requiere un dispositivo VPN local que tenga una dirección IP pública asignada.



**Requisitos previos**

* Compruebe que tiene una suscripción a Azure. Si todavía no la tiene, puede activar sus ventajas como suscriptor de MSDN o registrarse para obtener una cuenta gratuita.
* Decida el intervalo de direcciones IP que desea usar para el espacio de direcciones privadas del centro virtual. Esta información se usa al configurar el centro virtual. Un centro de conectividad virtual es una red virtual que Virtual WAN crea y usa. Es el núcleo de la red Virtual WAN en una región. El intervalo del espacio de direcciones debe cumplir determinadas reglas.  
  + El intervalo de direcciones que especifique para el centro no se puede superponer con ninguna de las redes virtuales existentes a las que se conecta.
  + El intervalo de direcciones no se puede superponer con los intervalos de direcciones locales a las que se conecta.
  + Si no está familiarizado con los intervalos de direcciones IP ubicados en la configuración de red local, consulte a alguien que pueda proporcionarle estos detalles.

**Azure Portal o Azure PowerShell**

Puede usar los cmdlets de Azure Portal o Azure PowerShell para crear una conexión de sitio a sitio para Azure Virtual WAN. Cloud Shell es un shell interactivo gratis que tiene herramientas comunes de Azure preinstaladas y configuradas para usar con la cuenta.

Para abrir Cloud Shell, seleccione **Abrir Cloud Shell** en la esquina superior derecha de un bloque de código. También puede abrir Cloud Shell en una pestaña independiente desde [**https://shell.azure.com/powershell**](https://shell.azure.com/powershell). Seleccione **Copiar** para copiar los bloques de código, péguelos en Cloud Shell y, a continuación, seleccione la tecla Entrar para ejecutarlos.

También puede instalar y ejecutar los cmdlets de Azure PowerShell localmente en el equipo. Los cmdlets de PowerShell se actualizan con frecuencia. Si no ha instalado la última versión, los valores especificados en las instrucciones pueden dar lugar a errores. Para buscar las versiones de Azure PowerShell instaladas en el equipo, use el Get-Module -ListAvailable Az cmdlet.

**Iniciar sesión**

Si usa **Azure Cloud Shell**, se le dirigirá automáticamente para iniciar sesión en su cuenta después de abrir Cloud Shell. No es necesario ejecutar Connect-AzAccount. Una vez que haya iniciado sesión, podrá cambiar las suscripciones si fuera necesario mediante Get-AzSubscription y Select-AzSubscription.

Si PowerShell se ejecuta localmente, abra la consola de PowerShell con privilegios elevados y conéctese a su cuenta de Azure. El cmdlet Connect-AzAccount le pide las credenciales. Después de la autenticación, descarga la configuración de la cuenta para que esté disponible en Azure PowerShell. Puede cambiar la suscripción mediante Get-AzSubscription y Select-AzSubscription -SubscriptionName "Name of subscription".

**Creación de una instancia de Virtual WAN**

Para poder crear una WAN virtual, debe crear un grupo de recursos para hospedarla o usar un grupo de recursos existente. Use uno de los ejemplos que se muestran a continuación.

En este ejemplo se crea un grupo de recursos denominado **TestRG** en la ubicación **Este de EE. UU.** Si quiere usar un grupo de recursos existente en su lugar, podría modificar el comando $resourceGroup = Get-AzResourceGroup -ResourceGroupName "NameofResourceGroup" y, a continuación, completar los pasos de este ejercicio con sus propios valores.

1. Cree un grupo de recursos.

**Azure PowerShell**

New-AzResourceGroup -Location "East US" -Name "TestRG"

1. Cree la WAN virtual mediante el cmdlet New-AzVirtualWan.

**Azure PowerShell**

$virtualWan = New-AzVirtualWan -ResourceGroupName TestRG -Name TestVWAN1 -Location "East US"

**Creación del centro y configuración de valores del centro**

Un centro de conectividad es una red virtual que puede contener puertas de enlace para las funcionalidades de sitio a sitio, ExpressRoute o de punto a sitio. Cree una ruta de centro virtual con New-AzVirtualHub. En este ejemplo, se creará un centro virtual predeterminado denominado Hub1 con el prefijo de dirección especificado y una ubicación para el centro.

**Azure PowerShell**

$virtualHub = New-AzVirtualHub -VirtualWan $virtualWan -ResourceGroupName "TestRG" -Name "Hub1" -AddressPrefix "10.1.0.0/16" -Location "westus"

**Crear una puerta de enlace de VPN de sitio a sitio**

En esta sección, creará una puerta de enlace de VPN de sitio a sitio en la misma ubicación del centro virtual al que se hace referencia. Al crear la puerta de enlace de VPN, especifique las unidades de escalado que desee. La creación de la puerta de enlace suele tardar unos 30 minutos.

1. Si cerró Azure Cloud Shell o agotó el tiempo de espera de la conexión, es posible que tenga que volver a declarar la variable para $virtualHub.

**Azure PowerShell**

$virtualHub = Get-AzVirtualHub -ResourceGroupName "TestRG" -Name "Hub1"

1. Cree una puerta de enlace de VPN mediante el cmdlet New-AzVpnGateway.

**Azure PowerShell**

New-AzVpnGateway -ResourceGroupName "TestRG" -Name "vpngw1" -VirtualHubId $virtualHub.Id -VpnGatewayScaleUnit 2

1. Una vez que se cree la puerta de enlace de VPN, puede verla mediante el ejemplo siguiente.

**Azure PowerShell**

Get-AzVpnGateway -ResourceGroupName "TestRG" -Name "vpngw1"

**Creación de un sitio y de las conexiones**

En esta sección, creará sitios que se correspondan con las ubicaciones físicas y las conexiones. Estos sitios contienen los puntos de conexión de dispositivo VPN locales; puede crear hasta 1000 sitios por centro virtual en una WAN virtual. Si tiene varios centros, puede crear 1000 sitios en cada uno de ellos.

1. Establezca la variable para la puerta de enlace de VPN y para el espacio de direcciones IP que se encuentra en el sitio local. El tráfico destinado a este espacio de direcciones se enruta al sitio local. Esto es necesario cuando no se habilita BGP para el sitio.

**Azure PowerShell**

$vpnGateway = Get-AzVpnGateway -ResourceGroupName "TestRG" -Name "vpngw1"

$vpnSiteAddressSpaces = New-Object string[] 2

$vpnSiteAddressSpaces[0] = "192.168.2.0/24"

$vpnSiteAddressSpaces[1] = "192.168.3.0/24"

1. Cree vínculos para agregar información sobre los vínculos físicos en la rama, incluidos los metadatos sobre la velocidad del vínculo, el nombre del proveedor de vínculos y la dirección IP pública del dispositivo local.

**Azure PowerShell**

$vpnSiteLink1 = New-AzVpnSiteLink -Name "TestSite1Link1" -IpAddress "15.25.35.45" -LinkProviderName "SomeTelecomProvider" -LinkSpeedInMbps "10"

$vpnSiteLink2 = New-AzVpnSiteLink -Name "TestSite1Link2" -IpAddress "15.25.35.55" -LinkProviderName "SomeTelecomProvider2" -LinkSpeedInMbps "100"

1. Cree el sitio VPN y haga referencia a las variables de los vínculos del sitio VPN que acaba de crear.

Si cerró Azure Cloud Shell o agotó el tiempo de espera de la conexión, vuelva a declarar la variable virtual WAN:

**Azure PowerShell**

$virtualWan = Get-AzVirtualWAN -ResourceGroupName "TestRG" -Name "TestVWAN1"

1. Cree el sitio VPN mediante el cmdlet New-AzVpnSite.
2. Cree la conexión de los vínculos del sitio. La conexión está compuesta por dos túneles activo-activo desde una rama o sitio a la puerta de enlace escalable.

**Azure PowerShell**

$vpnSiteLinkConnection1 = New-AzVpnSiteLinkConnection -Name "TestLinkConnection1" -VpnSiteLink $vpnSite.VpnSiteLinks[0] -ConnectionBandwidth 100

$vpnSiteLinkConnection2 = New-AzVpnSiteLinkConnection -Name "testLinkConnection2" -VpnSiteLink $vpnSite.VpnSiteLinks[1] -ConnectionBandwidth 10

**Conexión del sitio de VPN con el centro de conectividad**

Conecte el sitio VPN a la puerta de enlace del centro de VPN de sitio a sitio mediante el cmdlet New-AzVpnConnection.

1. Antes de ejecutar el comando, es posible que tenga que volver a declarar las siguientes variables:

**Azure PowerShell**

$virtualWan = Get-AzVirtualWAN -ResourceGroupName "TestRG" -Name "TestVWAN1"

$vpnGateway = Get-AzVpnGateway -ResourceGroupName "TestRG" -Name "vpngw1"

$vpnSite = Get-AzVpnSite -ResourceGroupName "TestRG" -Name "TestSite1"

1. Conexión del sitio de VPN con el centro de conectividad.

**Azure PowerShell**

New-AzVpnConnection -ResourceGroupName $vpnGateway.ResourceGroupName -ParentResourceName $vpnGateway.Name -Name "testConnection" -VpnSite $vpnSite -VpnSiteLinkConnection @($vpnSiteLinkConnection1, $vpnSiteLinkConnection2)

**Conexión de una red virtual al centro**

El siguiente paso será conectar el centro a la red virtual. Si creó un nuevo grupo de recursos para este ejercicio, normalmente no tendrá una red virtual (VNet) en el grupo de recursos. Los pasos siguientes le ayudarán a crear una red virtual si aún no tuviera una. Entonces, puede crear una conexión entre el centro de conectividad y la red virtual.

**Creación de una red virtual**

Puede usar los siguientes valores de ejemplo para crear una red virtual. Asegúrese de sustituir los valores de los ejemplos por los valores que usó para su entorno.

1. Crear una red virtual

**Azure PowerShell**

$vnet = @{

Name = 'VNet1'

ResourceGroupName = 'TestRG'

Location = 'eastus'

AddressPrefix = '10.21.0.0/16'

}

$virtualNetwork = New-AzVirtualNetwork @vnet

1. Especifique la configuración de subred.

**Azure PowerShell**

$subnet = @{

Name = 'Subnet-1'

VirtualNetwork = $virtualNetwork

AddressPrefix = '10.21.0.0/24'

}

$subnetConfig = Add-AzVirtualNetworkSubnetConfig @subnet

1. Establezca la red virtual.

**Azure PowerShell**

$virtualNetwork | Set-AzVirtualNetwork

**Conectar una red virtual a un concentrador**

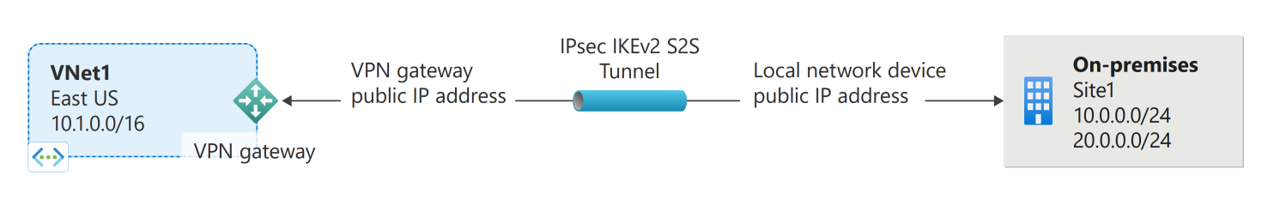
**Configurar dispositivo VPN**

**Proteger la conectividad de las VPN, incluida la de punto a sitio y la de sitio a sitio**

Es importante saber que hay distintas configuraciones disponibles para las conexiones de VPN Gateway. Es preciso determinar qué configuración es la que mejor se adapta a sus necesidades. En las secciones siguientes, puede ver diagramas de topología e información de diseño sobre las siguientes conexiones de VPN Gateway. Use los gráficos y las descripciones como ayuda para seleccionar la topología de conexión que mejor se ajuste a sus requisitos. Los diagramas muestran las principales topologías de referencia, pero también se pueden crear configuraciones más complejas con los diagramas como guía.

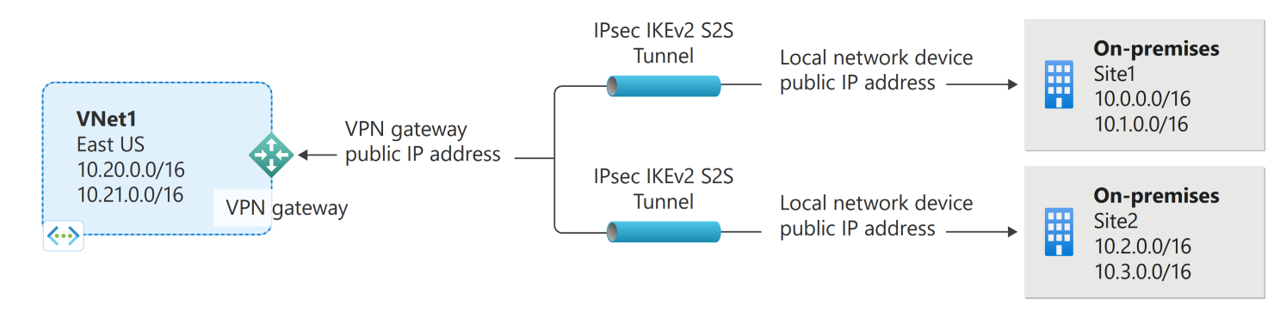
**VPN de sitio a sitio**

Una conexión de puerta de enlace de VPN de sitio a sitio (S2S) es una conexión a través de un túnel VPN IPsec/IKE (IKEv1 o IKEv2). Se pueden usar conexiones S2S para las configuraciones híbridas y entre locales. Una conexión S2S requiere un dispositivo VPN local que tenga una dirección IP pública asignada.



VPN Gateway se puede configurar en modo activo-espera mediante una dirección IP pública o en modo activo-activo con dos direcciones IP públicas. En modo activo-espera, hay un túnel IPsec activo y el otro túnel está en espera. En esta configuración, el tráfico fluye a través del túnel activo y, si se produce algún problema con este túnel, el tráfico cambia al túnel en espera. Se recomienda la configuración de VPN Gateway en modo activo-activo, porque ambos túneles de IPsec están activos simultáneamente, con datos que fluyen a través de los dos al mismo tiempo. Una ventaja adicional del modo activo-activo es que los clientes experimentan un mayor rendimiento.

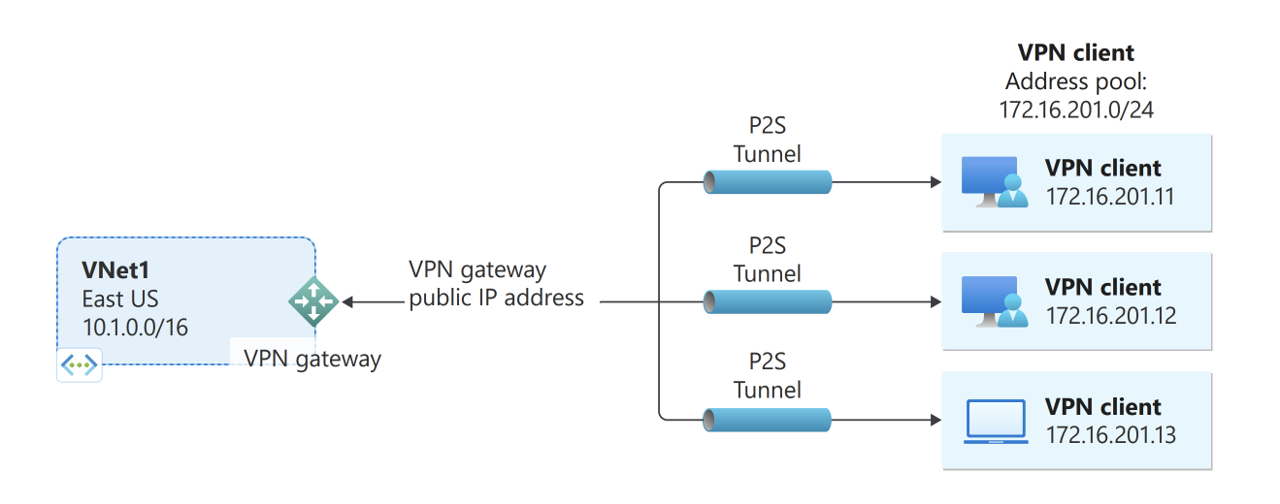
Puede crear más de una conexión VPN desde la puerta de enlace de red virtual, normalmente conectándose a varios sitios locales. Cuando trabaje con varias conexiones, debe usar una VPN de tipo RouteBased (conocida como puerta de enlace dinámica al trabajar con redes virtuales clásicas). Como cada red virtual solo puede tener una puerta de enlace de red virtual, todas las conexiones a través de la puerta de enlace comparten el ancho de banda disponible. Este tipo de conexión se denomina con frecuencia "conexión multisitio".



**Red privada virtual de punto a sitio**

Una conexión de puerta de enlace VPN de punto a sitio (P2S) le permite crear una conexión segura con la red virtual desde un equipo cliente individual. Se establece una conexión de punto a sitio al iniciarla desde el equipo cliente. Esta solución resulta útil para los teletrabajadores que deseen conectarse a redes virtuales de Azure desde una ubicación remota, por ejemplo, desde casa o un congreso. La conexión VPN de punto a sitio también es una solución útil en comparación con la conexión VPN de sitio a sitio cuando solo necesitan conectarse a la red virtual algunos clientes.

A diferencia de las conexiones S2S, las conexiones P2S no necesitan una dirección IP pública local ni dispositivos VPN. Se pueden usar conexiones P2S con conexiones S2S a través de la misma instancia de VPN Gateway, siempre que todos los requisitos de configuración para ambas conexiones sean compatibles.

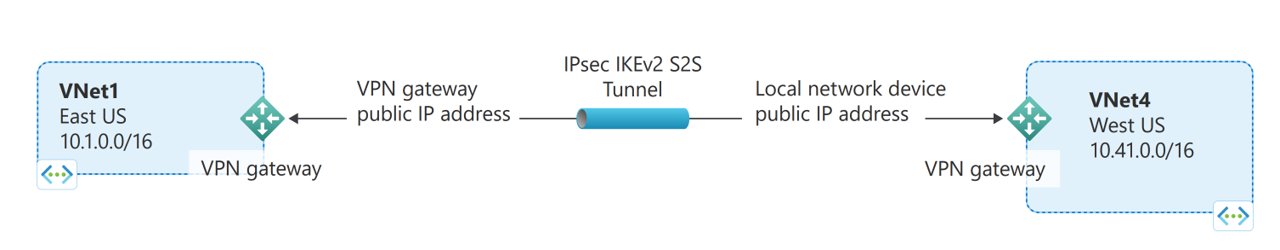


**Conexiones de red virtual a red virtual (protocolo de Internet seguro/túnel de red privada virtual de Intercambio de claves por red)**

La conexión de una red virtual a otra es muy parecida a la conexión de una red virtual a una ubicación de un sitio local. Ambos tipos de conectividad usan una puerta de enlace de VPN para proporcionar un túnel seguro con IPsec/IKE. Incluso puede combinar la comunicación de red virtual a red virtual con configuraciones de conexión multisitio. Esto permite establecer topologías de red que combinen la conectividad entre entornos con la conectividad entre redes virtuales.

Las redes virtuales que conecta pueden:

* estar en la misma región o en distintas;
* pertenecer a la misma suscripción o a distintas;
* usar el mismo modelo de implementación o diferentes.



**Conexiones entre modelos de implementación**

Actualmente, Azure tiene dos modelos de implementación: el clásico y el de Resource Manager. Si lleva un tiempo usando Azure, es probable que tenga máquinas virtuales de Azure y roles de instancia que se ejecuten en una red virtual clásica. Es posible que sus máquinas virtuales e instancias de roles más recientes se estén ejecutando en una red virtual creada en Resource Manager. Puede crear una conexión entre las redes virtuales para permitir que los recursos de una red virtual se comuniquen directamente con los recursos de otra.

**Emparejamiento de VNET**

Es posible que pueda usar el emparejamiento de VNET para crear la conexión, siempre que la red virtual cumpla determinados requisitos. El emparejamiento de VNET no utiliza una puerta de enlace de red virtual.

**Conexiones de sitio a sitio y de ExpressRoute coexistentes**

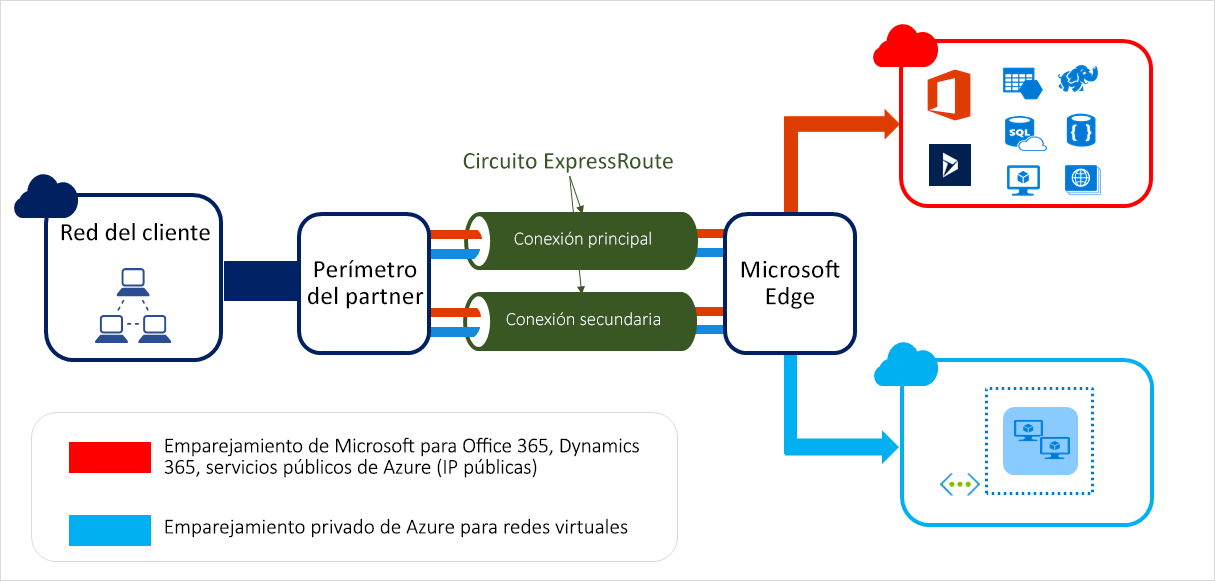
ExpressRoute es una conexión directa y privada desde su WAN (no a través de la red Internet pública) a los servicios Microsoft, incluido Azure. El tráfico VPN de sitio a sitio viaja cifrado a través de la red pública de Internet. Poder configurar las conexiones VPN de sitio a sitio y ExpressRoute para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

**Azure ExpressRoute**

ExpressRoute le permite ampliar sus redes locales en la nube de Microsoft a través de 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 ofrecen más fiabilidad, más velocidad, latencia más coherente y mayor seguridad que las conexiones a Internet normales porque no se realizan a través de una conexión a Internet pública.



**Ventajas principales**

* 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 del Protocolo de puerta de enlace de borde (BGP).
* Redundancia integrada en todas las ubicaciones de configuración entre pares para una mayor confiabilidad.
* Acuerdo de Nivel de Servicio (SLA) del tiempo de actividad de conexión.
* Compatibilidad con Calidad de servicio (QoS) para Skype Empresarial.

**Características**

**Conectividad de nivel 3**

Microsoft usa BGP, un protocolo de enrutamiento dinámico estándar del sector, para intercambiar las rutas entre su red local, las instancias de Azure y las direcciones públicas de Microsoft. Establecemos varias sesiones BGP con su red para perfiles de tráfico diferentes.

**Redundancia**

Cada circuito ExpressRoute consta de dos conexiones a dos enrutadores perimetrales de Microsoft Enterprise (MSEE) de una ubicación de ExpressRoute desde el proveedor de conectividad o el perímetro de la red. Microsoft requiere una conexión BGP dual desde el proveedor de conectividad o el perímetro de la red, uno a cada MSEE. Si lo desea, tiene la opción de no implementar dispositivos redundantes o circuitos Ethernet en el extremo. Sin embargo, los proveedores de conectividad usan dispositivos redundantes para garantizar que las conexiones se entregan a Microsoft de forma redundante.

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

Las conexiones ExpressRoute habilitan el acceso a los servicios siguientes:

* Servicios de Microsoft Azure
* Servicios de Microsoft 365

**Conectividad a todas las regiones dentro de una región geopolítica**

Puede conectarse a Microsoft desde una de nuestras ubicaciones de emparejamiento y acceder a las regiones con la misma región geopolítica.

Por ejemplo, si se conecta a Microsoft en Ámsterdam a través de ExpressRoute, Tiene acceso a todos los servicios en la nube de Microsoft hospedados en las regiones Norte de Europa y Oeste de Europa.

**Conectividad global con ExpressRoute Premium**

Puede habilitar ExpressRoute Premium para extender la conectividad a través de límites geopolíticos. Si se conecta a Microsoft en Ámsterdam mediante ExpressRoute, tiene acceso a todos los servicios en la nube de Microsoft hospedados en todas las regiones del mundo. Por ejemplo, tiene acceso a los servicios implementados en Oeste de EE. UU. o Este de Australia de la misma manera que accede a las regiones Norte y Oeste de Europa. Se excluyen las nubes nacionales.

**Conectividad local con ExpressRoute Local**

Puede transferir datos de forma rentable habilitando las referencias de almacén (SKU) locales. Con la SKU local, puede traer los datos a una ubicación de ExpressRoute cerca de la región de Azure que desee. Con Local, la transferencia de datos se incluye en la carga del puerto de ExpressRoute.

**Conectividad local con Global Reach de ExpressRoute**

Si habilita Global Reach de ExpressRoute, puede intercambiar datos entre los sitios locales a través de los diferentes circuitos ExpressRoute. Por ejemplo, supongamos que tiene dos centros de datos privados, uno en California y otro en Texas, cada uno conectado a un circuito ExpressRoute en sus respectivas regiones. Puede usar Global Reach de ExpressRoute para vincular los centros de datos con estos circuitos y el tráfico entre centros de datos usa la red de Microsoft.

**Ecosistema de socios de conectividad enriquecida**

ExpressRoute tiene un ecosistema de proveedores de conectividad y asociados integradores de sistemas en constante crecimiento.

**Conectividad con nubes nacionales**

Microsoft administra entornos de nube aislados para regiones geopolíticas y segmentos de clientes especiales.

**ExpressRoute Direct**

ExpressRoute Direct ofrece a los clientes la oportunidad de 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, que es compatible con la conectividad activa/activa a escala.

Algunas de las características clave que ofrece ExpressRoute Direct incluyen:

* Ingesta de datos masivos en servicios como Azure Storage y Azure Cosmos DB.
* Aislamiento físico para sectores regulados y que necesitan una conectividad dedicada y aislada. Por ejemplo: bancos, gobiernos y minoristas.
* Control granular del circuito de distribución en función de la unidad de negocio.

**Opciones de ancho de banda**

Puede comprar los circuitos ExpressRoute para una amplia gama de anchos de banda. A continuación se enumera la lista de anchos de banda admitidos. Asegúrese de consultar a su proveedor de conectividad para determinar la lista de anchos de banda admitidos que proporcionan.

* 50 megabits por segundo (Mbps)
* 100 Mbps
* 200 Mbps
* 500 Mbps
* 1 gigabit por segundo (Gbps)
* 2 Gbps
* 5 Gbps
* 10 Gbps

La redundancia integrada del circuito se configura mediante conexiones principales y secundarias, cada una de ellas del ancho de banda adquirido, a dos enrutadores perimetrales de Microsoft Enterprise (los MSEE). El ancho de banda disponible mediante la conexión secundaria se puede usar para permitir más tráfico, si fuera necesario. Dado que la conexión secundaria está pensada para la redundancia, no está garantizada y no debe utilizarse para tráfico adicional durante un periodo de tiempo prolongado. Si planea usar solo la conexión principal para transmitir el tráfico, el ancho de banda de la conexión es fijo y al intentar saturarlo se produce un aumento en los descartes de paquetes.

**Escalado dinámico del ancho de banda**

Puede aumentar el ancho de banda del circuito ExpressRoute sin necesidad de eliminar sus conexiones.

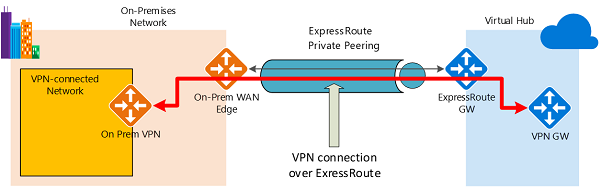
**Modelos flexibles de facturación**

* Puede elegir el modelo de facturación que más le convenga:
* Datos ilimitados. La facturación se basa en unos honorarios mensuales y todas las transferencias de datos de entrada y de salida están incluidas de forma gratuita.
* Datos medidos. La facturación se basa en unos honorarios mensuales y todas las transferencias de datos de entrada están incluidas de forma gratuita. Las transferencias de datos de salida se cobran de acuerdo a un precio por GB de transferencia de datos. Las tasas de transferencia de datos varían según la región.
* Complemento ExpressRoute Premium. ExpressRoute Premium es un complemento que se agrega a un circuito ExpressRoute. El complemento ExpressRoute Premium ofrece las siguientes capacidades:
  + Límites de ruta ampliados para las configuraciones entre pares públicos y privados de Azure, de 4.000 rutas a 10.000 rutas.
  + Conectividad global para los servicios. Un circuito ExpressRoute creado en cualquier región (excepto las nubes nacionales) tiene acceso a los recurso de cualquier otra región del mundo. Por ejemplo, un circuito ExpressRoute aprovisionado en Silicon Valley puede acceder a una red virtual creada en Oeste de Europa .
  + Número de vínculos de red virtual por circuito ExpressRoute ampliado de 10 a un límite superior, que depende del ancho de banda del circuito.

**Implementar el cifrado en ExpressRoute**

Implemente Azure Virtual WAN para establecer una conexión VPN de IPsec/IKE desde la red local a Azure por medio del emparejamiento privado de un circuito 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.

**Topología y enrutamiento**



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. Establezca la conectividad VPN como se describe en este artículo.

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.

**Tráfico desde redes locales a Azure**

En el caso del tráfico entre las redes locales y Azure, los prefijos de Azure (lo que incluye el centro de conectividad virtual y todas las redes virtuales de radio conectadas a ese centro) se anuncian a través de los protocolos de puerta de enlace de borde del emparejamiento privado de ExpressRoute y de la red privada virtual. El resultado son dos rutas de red (rutas de acceso) hacia Azure desde las redes locales:

* Una sobre la ruta de acceso protegida mediante IPsec
* Otra directamente sobre ExpressRoute, sin protección de IPsec

Para aplicar el cifrado a la comunicación, debe asegurarse de que para la red conectada a VPN del diagrama, se prefieren las rutas de Azure a través de la puerta de enlace de VPN local a la ruta de acceso directa de ExpressRoute.

**Tráfico desde Azure a las redes locales**

El mismo requisito se aplica al tráfico de Azure a las redes locales. Para asegurarse de que la ruta de acceso de IPsec se elige antes que la ruta de acceso directa de ExpressRoute (sin IPsec), tiene dos opciones:

Anuncie prefijos más específicos en la sesión BGP de VPN para la red conectada a VPN. Puede anunciar un rango mayor que abarque la red conectada a VPN a través del emparejamiento privado de ExpressRoute y, después, rangos más específicos en la sesión del protocolo de puerta de enlace de borde de VPN. Por ejemplo, anuncie 10.0.0.0/16 a través de ExpressRoute y 10.0.1.0/24 a través de VPN.

Anuncie prefijos disjuntos para VPN y ExpressRoute. Si los rangos de redes conectadas a VPN no están unidos a otras redes conectadas de ExpressRoute, puede anunciar los prefijos en las sesiones de los protocolos de puerta de enlace de borde de ExpressRoute y VPN, respectivamente. Por ejemplo, anuncie 10.0.0.0/24 a través de ExpressRoute y 10.0.1.0/24 a través de VPN.

En ambos ejemplos, Azure enviará tráfico a 10.0.1.0/24 a través de la conexión VPN en lugar de hacerlo directamente a través de ExpressRoute sin protección VPN.

**Antes de empezar**

Antes de iniciar la configuración, compruebe que cumple los siguientes criterios:

* Si ya tiene una red virtual a la que quiere conectarse, compruebe que ninguna de las subredes de la red local se superponga con ella. La red virtual no requiere una subred de puerta de enlace y no puede tener ninguna puerta de enlace de red virtual. Si no tiene una red virtual, siga los pasos de este artículo para crear una.
* Obtenga un intervalo de direcciones IP para la región del concentrador. El centro de conectividad es una red virtual, y el intervalo de direcciones que especifique para la región del concentrador no se puede superponer con ninguna de las redes virtuales existentes a las que esté conectado. Tampoco se puede superponer con los intervalos de direcciones a los que se conecte en el entorno local. Si no está familiarizado con los intervalos de direcciones IP ubicados en la configuración de red local, consulte a alguien que pueda proporcionarle estos detalles.
* Si no tiene una suscripción a Azure, cree una cuenta gratuita antes de empezar.

**Creación de una red virtual WAN y un concentrador con puertas de enlace**

Antes de continuar deben estar en vigor los siguientes recursos de Azure y las configuraciones locales correspondientes:

* Una Azure Virtual WAN.
* Un centro de Virtual WAN con ExpressRoute y una puerta de enlace de red privada virtual.

**Creación de un sitio para la red local**

El recurso del sitio es el mismo que el de los sitios VPN que no son de ExpressRoute para una red de área extensa virtual. La dirección IP del dispositivo VPN local ahora puede ser una dirección IP privada o una dirección IP pública en la red local accesible a través de la configuración de emparejamiento privado de ExpressRoute creada anteriormente.

1. Vaya a la **red de Virtual WAN**, a los sitios **VPN** y cree un sitio para la red local. Tenga en cuenta los siguientes valores de configuración:

* **Protocolo de puerta de enlace de borde**: seleccione "Habilitar" si la red local usa el protocolo de puerta de enlace de borde.
* **Espacio de direcciones privadas**: escriba el espacio de direcciones IP que se encuentra en el sitio local. El tráfico destinado a este espacio de direcciones se enruta a la red local a través de la puerta de enlace de VPN.

1. Seleccione Vínculos para agregar información sobre los vínculos físicos. Tenga en cuenta la siguiente infomoración de configuración:

* **Nombre de proveedor**: el nombre del proveedor de acceso a Internet de este sitio. En el caso de la red local de ExpressRoute, es el nombre del proveedor de servicios de ExpressRoute.
* **Velocidad**: la velocidad del vínculo de servicio de Internet o del circuito de ExpressRoute.
* **Dirección IP**: la dirección IP pública del dispositivo VPN que reside en el sitio local. O bien, en el entorno local de ExpressRoute, es la dirección IP privada del dispositivo VPN a través de ExpressRoute.
* Si BGP está habilitado, se aplica a todas las conexiones creadas para este sitio en Azure. La configuración del protocolo de puerta de enlace de borde en Virtual WAN es igual a su configuración en Azure VPN Gateway.
* La dirección de su par BGP local *no debe* ser la misma que la dirección IP de la VPN al dispositivo o al espacio de direcciones de la red virtual del sitio VPN. Use otra dirección IP en el dispositivo VPN para la dirección IP del par BGP. Puede ser una dirección asignada a la interfaz de bucle invertido en el dispositivo. Sin embargo, *no puede* ser una dirección IP privada automática (169.254.*x*.*x*). Especifique esta dirección en el sitio VPN correspondiente que representa la ubicación.

1. Seleccione **Siguiente: Revisar y Crear**para comprobar los valores de configuración y crear el sitio VPN y, a continuación **Crear** el sitio.
2. A continuación, conecte el sitio al centro. La actualización de la puerta de enlace puede tardar hasta 30 minutos.

**Actualización de la configuración de conexión VPN para usar ExpressRoute**

Después de crear el sitio VPN y conectarlo al centro de conectividad, use estos pasos para configurar la conexión para que use el emparejamiento privado de ExpressRoute:

1. Vaya al centro de conectividad virtual. Para ello, vaya a Virtual WAN y seleccione el centro para abrir la página del centro, o bien puede ir al centro virtual conectado desde el sitio VPN.
2. En **Conectividad**, seleccione **VPN (de sitio a sitio)**.
3. Seleccione los puntos suspensivos (**...**) o haga clic con el botón derecho en el sitio VPN sobre ExpressRoute y seleccione **Editar la conexión de VPN a este concentrador**.
4. En la página **Aspectos básicos**, deje los valores predeterminados.
5. En la página **Vincular conexión 1**, configure las siguientes opciones:
   * En **Usar dirección IP privada de Azure**, seleccione **Sí**. El ajuste configura la puerta de enlace de VPN de concentrador para que use direcciones IP privadas dentro del intervalo de direcciones del concentrador en la puerta de enlace para esta conexión, en lugar de las direcciones IP públicas. Esto garantiza que el tráfico de la red local atraviesa las rutas de acceso del emparejamiento privado de ExpressRoute, en lugar de usar la red pública de Internet para esta conexión VPN.
6. Haga clic en **Crear** para actualizar la configuración. Una vez creada la configuración, la puerta de enlace de VPN de concentrador usará las direcciones IP privadas en la puerta de enlace de VPN para establecer las conexiones de IPsec/IKE con el dispositivo VPN local a través de ExpressRoute.

**Obtención de las direcciones IP privadas de puerta de enlace de VPN del centro de conectividad**

Descargue la configuración del dispositivo VPN para obtener las direcciones IP privadas de la puerta de enlace de VPN del centro de conectividad. Estas direcciones son necesarias para configurar el dispositivo VPN local.

1. En la página del centro de conectividad, seleccione **VPN (sitio a sitio)** en **Conectividad**.
2. En la parte superior de la página **Información general**, seleccione **Descargar configuración de VPN**. Azure crea una cuenta de almacenamiento en el grupo de recursos "microsoft-network-[location]", donde *location* es la ubicación de la red WAN. Después de aplicar la configuración a los dispositivos VPN, puede eliminar esta cuenta de almacenamiento.
3. Después de que se cree el archivo, seleccione el vínculo para descargarlo.
4. Aplique la configuración al dispositivo VPN.

**Archivo de configuración del dispositivo VPN**

El archivo de configuración del dispositivo contiene la configuración que se debe usar al configurar el dispositivo VPN local. Cuando visualice este archivo, tenga en cuenta la siguiente información:

* vpnSiteConfiguration: en esta sección se indica la configuración de los detalles del dispositivo como un sitio que se conecta a la WAN virtual. Incluye el nombre y la dirección IP pública del dispositivo de rama.
* vpnSiteConnections: en esta sección se proporciona información sobre la siguiente configuración:
  + Espacio de direcciones de la red virtual del centro de conectividad virtual.  
    Ejemplo: "AddressSpace":"10.51.230.0/24"
  + Espacio de direcciones de las redes virtuales que están conectadas al centro de conectividad.  
    Ejemplo: "ConnectedSubnets":["10.51.231.0/24"]
  + Direcciones IP de la puerta de enlace de VPN del centro de conectividad virtual. Dado que cada conexión de la puerta de enlace de VPN consta de dos túneles en una configuración activo-activo, verá ambas direcciones IP en este archivo. En este ejemplo, verá Instance0 e Instance1 para cada sitio, son direcciones IP privadas en lugar de direcciones IP públicas.  
    Ejemplo: "Instance0":"10.51.230.4" "Instance1":"10.51.230.5"
  + Detalles de la configuración de la conexión de la puerta de enlace de VPN, como BGP y clave precompartida. La clave precompartida se genera automáticamente. La conexión se puede modificar en cualquier momento en la página **Información general** de una clave precompartida personalizada.

**Archivo de configuración de dispositivo de ejemplo**

[{

"configurationVersion":{

"LastUpdatedTime":"2019-10-11T05:57:35.1803187Z",

"Version":"5b096293-edc3-42f1-8f73-68c14a7c4db3"

},

"vpnSiteConfiguration":{

"Name":"VPN-over-ER-site",

"IPAddress":"172.24.127.211",

"LinkName":"VPN-over-ER"

},

"vpnSiteConnections":[{

"hubConfiguration":{

"AddressSpace":"10.51.230.0/24",

"Region":"West US 2",

"ConnectedSubnets":["10.51.231.0/24"]

},

"gatewayConfiguration":{

"IpAddresses":{

"Instance0":"10.51.230.4",

"Instance1":"10.51.230.5"

}

},

"connectionConfiguration":{

"IsBgpEnabled":false,

"PSK":"abc123",

"IPsecParameters":{"SADataSizeInKilobytes":102400000,"SALifeTimeInSeconds":3600}

}

}]

},

{

"configurationVersion":{

"LastUpdatedTime":"2019-10-11T05:57:35.1803187Z",

"Version":"fbdb34ea-45f8-425b-9bc2-4751c2c4fee0"

},

"vpnSiteConfiguration":{

"Name":"VPN-over-INet-site",

"IPAddress":"13.75.195.234",

"LinkName":"VPN-over-INet"

},

"vpnSiteConnections":[{

"hubConfiguration":{

"AddressSpace":"10.51.230.0/24",

"Region":"West US 2",

"ConnectedSubnets":["10.51.231.0/24"]

},

"gatewayConfiguration":{

"IpAddresses":{

"Instance0":"51.143.63.104",

"Instance1":"52.137.90.89"

}

},

"connectionConfiguration":{

"IsBgpEnabled":false,

"PSK":"abc123",

"IPsecParameters":{"SADataSizeInKilobytes":102400000,"SALifeTimeInSeconds":3600}

}

}]

}]

**Configuración del firewall en recursos de PaaS**

**Modernización de la mentalidad de Defender for Cloud**

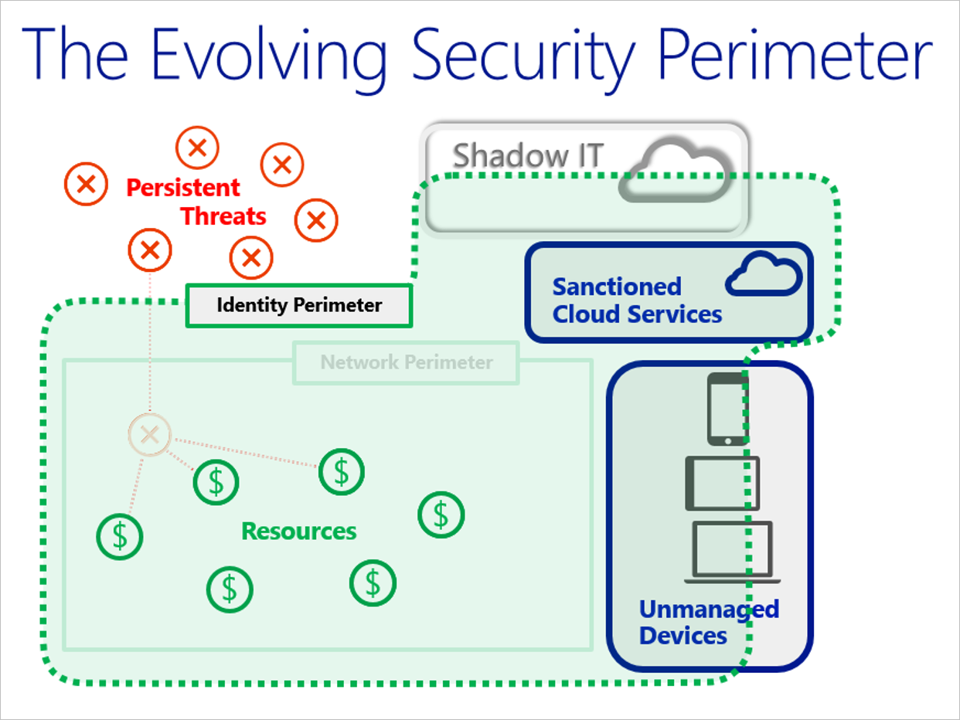
Las implementaciones de PaaS conllevan un cambio del enfoque general en relación con la seguridad. Se pasa de la necesidad de controlar todo por uno mismo a compartir la responsabilidad con Microsoft.

Otra diferencia importante entre las implementaciones de PaaS y las implementaciones locales tradicionales es una nueva visión de lo que define el perímetro de seguridad principal. Históricamente, el perímetro de seguridad local principal era la red, y la mayoría de los diseños de seguridad locales utilizan la red como la dinámica de seguridad principal. Para las implementaciones de PaaS, se recomienda considerar la identidad como el perímetro de seguridad principal.

**Adoptar una directiva de identidad como perímetro de seguridad principal**

Una de las cinco características fundamentales de la informática en la nube es el acceso amplio a la red, lo que hace que el concepto basado en la red resulte menos relevante. El objetivo de gran parte de la informática en la nube es permitir a los usuarios acceder a los recursos con independencia de su ubicación. Para la mayoría de los usuarios, su ubicación estará en alguna parte de Internet.

En la figura siguiente se muestra cómo el perímetro de seguridad ha evolucionado de un perímetro de red a un perímetro de identidad. La seguridad se centra menos en proteger la red y más en proteger los datos, así como en administrar la seguridad de las aplicaciones y los usuarios. La diferencia principal es que la intención es basar más la seguridad en lo que resulta importante para su empresa.



Inicialmente, los servicios PaaS en Azure (por ejemplo, los roles web y Azure SQL) ofrecían poca o ninguna defensa para el perímetro de red tradicional. Se entiende que el propósito del elemento era exponerse a Internet (rol web) y que la autenticación ofrece el nuevo perímetro (por ejemplo, BLOB o Azure SQL).

Las prácticas de seguridad modernas asumen que el adversario ha infringido el perímetro de red. Por lo tanto, las prácticas de defensa modernas se han pasado al perímetro de identidad. Las organizaciones deben establecer un perímetro de seguridad basado en identidades con autenticación sólida e higiene de autorización (procedimientos recomendados).

Durante décadas, se han encontrado disponibles principios y patrones para el perímetro de red. En cambio, el sector tiene relativamente poca experiencia con el uso de la identidad como el perímetro de seguridad principal. Dicho esto, se ha adquirido suficiente experiencia para ofrecer algunas recomendaciones generales que se han probado sobre el terreno y que se han aplicado a casi todos los servicios PaaS.

Aquí tiene unas recomendaciones para administrar el perímetro de identidad.

**Procedimiento recomendado**: proteger las claves y las credenciales para proteger la implementación de PaaS. Detalles: La pérdida de claves y credenciales es un problema común. Puede usar una solución centralizada que permita almacenar claves y secretos en módulos de seguridad de hardware (HSM). Azure Key Vault guarda claves y secretos mediante el cifrado de claves de autenticación, claves de cuenta de almacenamiento, claves de cifrado de datos, archivos .pfx y contraseñas a través del uso de claves protegidas por HSM.

**Procedimiento recomendado**: no incluya credenciales y otros secretos en el código fuente o en GitHub. Detalles: mucho peor que perder las claves y las credenciales es que otra persona no autorizada acceda a ellas. Los atacantes pueden aprovechar las tecnologías de bots para encontrar claves y secretos almacenados en repositorios de código, como GitHub. No guarde claves ni secretos en estos repositorios públicos de código.

**Procedimiento recomendado**: proteja las interfaces de administración de las máquinas virtuales en servicios híbridos PaaS e IaaS. Para ello, use una interfaz de administración que permita administrar de manera remota estas máquinas virtuales directamente. Detalles: se pueden usar protocolos de administración remota como SSH, RDP y de comunicación remota de PowerShell. En general, se recomienda no habilitar el acceso remoto directo a máquinas virtuales desde Internet.

Si es posible, siga otros enfoques, como usar redes privadas virtuales en una red virtual de Azure. Si no hay otros métodos disponibles, asegúrese de usar frases de contraseña complejas y la autenticación en dos fases (como la autenticación multifactor de Microsoft Entra).

**Procedimiento recomendado**: use plataformas sólidas de autenticación y autorización. Detalle: use identidades federadas en Microsoft Entra ID en lugar de almacenes de usuarios personalizados. Cuando se usan identidades federadas, se puede beneficiar de un enfoque basado en plataformas y delegar la administración de identidades autorizadas en sus asociados. Un enfoque federado resulta especialmente importante cuando los empleados terminan los contratos y dicha información necesita reflejarse a través de varios sistemas de identidad y autorización.

Use los mecanismos de autenticación y autorización proporcionados en la plataforma en lugar del código personalizado. La razón es que desarrollar código de autenticación personalizado puede resultar un método propenso a errores. La mayoría de los desarrolladores no son expertos en seguridad y es poco probable que conozcan los detalles y los últimos desarrollos en términos de autenticación y autorización. El código comercial (por ejemplo, de Microsoft) suele revisarse de manera amplia a efectos de seguridad.

Use la autenticación en dos fases. La autenticación en dos fases es el estándar actual para la autenticación y autorización porque evita las vulnerabilidades de seguridad inherentes a tipos de nombres de usuario y contraseñas de autenticación. El acceso a las interfaces de administración de Azure (portal/PowerShell remoto) y a los servicios orientados al cliente debe diseñarse y configurarse para que use la autenticación multifactor de Microsoft Entra.

Use los protocolos de autenticación estándar, como OAuth2 y Kerberos. Estos protocolos se han sometido a revisiones exhaustivas del mismo nivel y posiblemente se implementen como parte de las bibliotecas de la plataforma a efectos de autenticación y autorización.

**Usar el modelado de amenazas durante el diseño de la aplicación**

El ciclo de vida de desarrollo de seguridad de Microsoft especifica que los equipos deben llevar a cabo un proceso denominado modelado de amenazas durante la fase de diseño. Para que este proceso sea más sencillo, Microsoft ha creado SDL Threat Modeling Tool. Al modelar el diseño de la aplicación y enumerar las amenazas de STRIDE en todos los límites de confianza, pueden detectarse errores de diseño desde el principio.

En esta tabla se enumeran las amenazas STRIDE y se incluyen algunos ejemplos de mitigación donde se usan características de Azure. Estas mitigaciones no funcionarán en todas las situaciones.

| **Amenaza** | **Propiedad de seguridad** | **Posibles mitigaciones de la plataforma Azure** |
| --- | --- | --- |
| Suplantación de identidad | Authentication | Necesita conexiones HTTPS. |
| Alteración de datos | Integridad | Valida certificados TLS/SSL. |
| Rechazo | No rechazo | Habilita opciones de supervisión y diagnóstico de Azure. |
| Divulgación de información | Confidencialidad | Cifra datos confidenciales en reposo mediante certificados de servicio. |
| Denegación de servicio | Disponibilidad | Supervisa las métricas de rendimiento de las posibles condiciones de denegación de servicio. Implementa filtros de conexión. |
| Elevación de privilegios | Authorization | Usa Privileged Identity Management. |

**Desarrollar en Azure App Service**

Azure App Service es una oferta PaaS que permite crear aplicaciones web y móviles para cualquier plataforma o dispositivo y conectarse a datos en cualquier lugar, en la nube o en un entorno local. App Service incluye las funcionalidades web y móviles que anteriormente se ofrecían por separado como Azure Websites y Azure Mobile Services. También incluye nuevas funcionalidades para automatizar procesos empresariales y hospedar las API en la nube. Como único servicio integrado, App Service ofrece un amplio conjunto de funcionalidades para escenarios web, móviles y de integración.

Estas son algunos procedimientos recomendados para usar App Service.

**Procedimiento recomendado**: Autentíquese a través de Microsoft Entra ID. Detalles: App Service proporciona un servicio OAuth 2.0 para el proveedor de identidades. OAuth 2.0 se centra en la sencillez del desarrollador del cliente y ofrece flujos de autorización específicos de aplicaciones web, aplicaciones de escritorio y teléfonos móviles. Microsoft Entra ID usa OAuth 2.0 para permitirle autorizar el acceso a las aplicaciones móviles y a las aplicaciones web.

**Procedimiento recomendado**: Restricción del acceso siguiendo los principios de seguridad de limitar el acceso a lo que se necesita saber y a los principios de seguridad con privilegios mínimos. Detalles: La restricción del acceso es fundamental para las organizaciones que deseen aplicar directivas de seguridad para el acceso a los datos. Puede usar Azure RBAC para asignar permisos a los usuarios, los grupos y las aplicaciones en un ámbito determinado. Vea Introducción a la administración de acceso para aprender más sobre cómo conceder acceso a los usuarios a las aplicaciones.

**Procedimiento recomendado**: Protección de las claves. Detalles: Azure Key Vault ayuda a proteger las claves criptográficas y los secretos que usan los servicios y aplicaciones en la nube. Con Key Vault, puede cifrar claves y secretos (por ejemplo claves de autenticación, claves de cuenta de almacenamiento, claves de cifrado de datos, archivos .PFX y contraseñas) a través del uso de claves que están protegidas por módulos de seguridad de hardware (HSM). Para tener mayor seguridad, puede importar o generar las claves en HSM. Vea Azure Key Vault para más información. También puede utilizar Key Vault para administrar los certificados TLS con renovación automática.

**Procedimiento recomendado**: Restricción de las direcciones IP de origen entrantes. Detalles: App Service Environment tiene una característica de integración de la red virtual que ayuda a restringir las direcciones IP de origen entrantes mediante grupos de seguridad de red. Las redes virtuales permiten colocar recursos de Azure en una red que se pueda enrutar distinta de Internet y a la que se controla el acceso. Vea Integración de su aplicación con una instancia de Azure Virtual Network para más información.

**Procedimiento recomendado**: supervise el estado de seguridad de los entornos de App Service. Detalle: use Microsoft Defender for Cloud para supervisar los entornos de App Service. Cuando Defender for Cloud identifica posibles vulnerabilidades de seguridad, crea recomendaciones que lo guiarán por el proceso de configuración de los controles necesarios.

**Azure Cloud Services**

Azure Cloud Services es un ejemplo de PaaS. Al igual que Azure App Service, esta tecnología está diseñada para ser compatible con aplicaciones escalables, confiables y de funcionamiento asequible. En la misma manera que App Service se hospeda en máquinas virtuales (VM), así ocurre también con Azure Cloud Services. Sin embargo, tiene más control sobre las máquinas virtuales. Puede instalar su propio software en las máquinas virtuales que usan Azure Cloud Services y puede tener acceso a ellas remotamente.

**Protección frente a DDOS**

Azure DDoS Protection, combinado con los procedimientos recomendados de diseño de aplicaciones, proporciona características mejoradas de mitigación de DDoS para ofrecer una mejor defensa frente a los ataques DDoS. Debe habilitar Azure DDOS Protection en cualquier red virtual perimetral.

**Supervisar el rendimiento de las aplicaciones**

La supervisión es el acto de recopilar y analizar datos para determinar el rendimiento, el mantenimiento y la disponibilidad de su aplicación. Una estrategia de supervisión eficaz le ayuda a comprender el funcionamiento detallado de los componentes de la aplicación. También sirve para aumentar el tiempo de actividad, ya que le notifica de cuestiones críticas para que pueda resolverlas antes de que se conviertan en problemas. También permite detectar anomalías que podrían estar relacionados con la seguridad.

Use Azure Application Insights para supervisar la disponibilidad, el rendimiento y el uso de la aplicación, tanto si se hospeda en la nube como en un entorno local. Con Application Insights, podrá identificar y diagnosticar rápidamente errores en la aplicación sin tener que esperar a que un usuario informe de ellos. Con la información que recopile, puede tomar decisiones informadas sobre el mantenimiento y las mejoras de la aplicación.

Application Insights tiene numerosas herramientas para interactuar con los datos que recopila. Application Insights almacena sus datos en un repositorio común. Puede sacar partido a las funciones compartidas, como alertas, paneles y análisis detallados con el lenguaje de consulta de Kusto.

**Supervisar el rendimiento de las aplicaciones**

La supervisión es el acto de recopilar y analizar datos para determinar el rendimiento, el mantenimiento y la disponibilidad de su aplicación. Una estrategia de supervisión eficaz le ayuda a comprender el funcionamiento detallado de los componentes de la aplicación. También sirve para aumentar el tiempo de actividad, ya que le notifica de cuestiones críticas para que pueda resolverlas antes de que se conviertan en problemas. También permite detectar anomalías que podrían estar relacionados con la seguridad.

Use Azure Application Insights para supervisar la disponibilidad, el rendimiento y el uso de la aplicación, tanto si se hospeda en la nube como en un entorno local. Con Application Insights, podrá identificar y diagnosticar rápidamente errores en la aplicación sin tener que esperar a que un usuario informe de ellos. Con la información que recopile, puede tomar decisiones informadas sobre el mantenimiento y las mejoras de la aplicación.

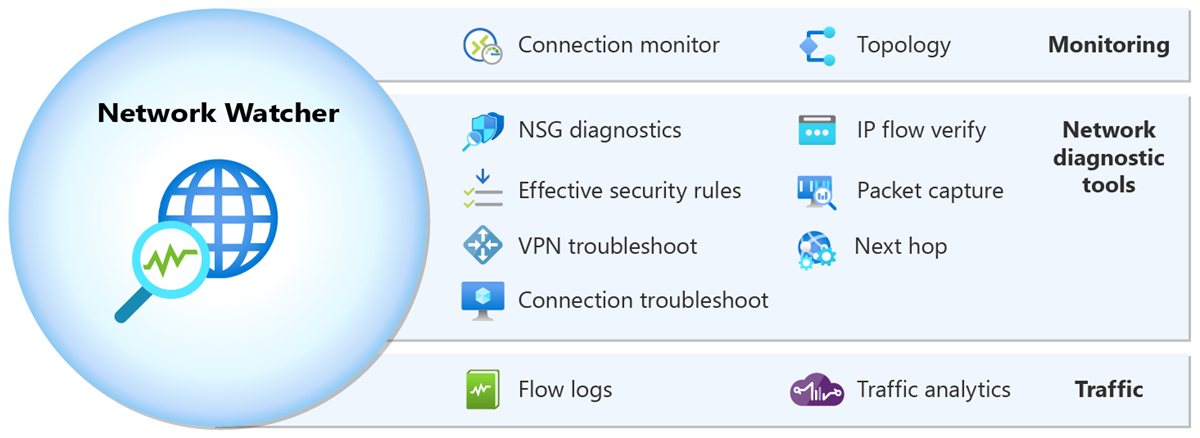
Application Insights tiene numerosas herramientas para interactuar con los datos que recopila. Application Insights almacena sus datos en un repositorio común. Puede sacar partido a las funciones compartidas, como alertas, paneles y análisis detallados con el lenguaje de consulta de Kusto.

**Supervisión de la seguridad de red con Network Watcher, incluido el registro de flujos de NSG**

Azure Network Watcher proporciona un conjunto de herramientas para monitorear, diagnosticar, ver métricas y habilitar o deshabilitar registros de recursos de IaaS (infraestructura como servicio) de Azure. Network Watcher le permite supervisar y reparar el estado de red de productos IaaS, como máquinas virtuales (VM), redes virtuales (VNet), puertas de enlace de aplicaciones, equilibradores de carga, etc. Network Watcher no está diseñado ni destinado para la supervisión de PaaS ni para el análisis web.

Network Watcher consta de tres conjuntos principales de herramientas y funcionalidades:

* Supervisión
* Herramientas de diagnóstico de red
* Tráfico



**Nota**

Cuando crea o actualiza una red virtual en la suscripción, Network Watcher se habilita automáticamente en la región de la red virtual. El hecho de habilitar Network Watcher de manera automática no afecta a los recursos ni supone un cargo adicional.

**Supervisión**

Network Watcher ofrece dos herramientas de supervisión que le ayudan a ver y supervisar los recursos:

* Topología
* Monitor de conexión

**Topología**

La topología proporciona una visualización de toda la red para comprender la configuración de red. Proporciona una interfaz interactiva para ver los recursos y sus relaciones en Azure que abarcan varias suscripciones, grupos de recursos y ubicaciones.

**Monitor de conexión**

El monitor de conexión proporciona supervisión de conexión de un extremo a otro para los puntos de conexión híbridos y de Azure. Le ayudará a comprender el rendimiento de red entre varios puntos de conexión de la infraestructura de red.

**Herramientas de diagnóstico de red**

Network Watcher ofrece siete herramientas de diagnóstico de red que ayudan a solucionar y diagnosticar problemas de red:

* Comprobación del flujo de IP
* Diagnósticos del grupo de seguridad de red
* Próximo salto
* Reglas de seguridad vigentes
* Solucionar problemas de conexión
* Captura de paquetes
* Solución de problemas de VPN

**Comprobación del flujo de IP**

Comprobación del flujo de IP permite detectar incidencias en el filtrado del tráfico a nivel de máquina virtual. Comprueba si se permite o deniega un paquete hacia o desde una dirección IP (dirección IPv4 o IPv6). También indica qué regla de seguridad permitió o denegó el tráfico.

**Diagnósticos del grupo de seguridad de red (NSG)**

Diagnóstico de NSG le permite detectar incidencias en el filtrado de tráfico a nivel de máquina virtual, conjunto de escalado de máquinas virtuales o puerta de enlace de aplicación. Comprueba si se permite o deniega un paquete hacia o desde una dirección IP, un prefijo IP o una etiqueta de servicio. Indica qué regla de seguridad permitió o denegó el tráfico. También permite agregar una nueva regla de seguridad con una prioridad más alta para permitir o denegar el tráfico.

**Próximo salto**

El próximo salto le permite detectar problemas de enrutamiento. Comprueba si el tráfico se enruta correctamente al destino previsto. Proporciona información sobre el tipo de próximo salto, la dirección IP y el identificador de la tabla de rutas para una dirección IP de destino específica.

**Reglas de seguridad vigentes**

Las reglas de seguridad eficaces permiten ver las reglas de seguridad vigentes aplicadas a una interfaz de red. Muestra todas las reglas de seguridad aplicadas a la interfaz de red, la subred en que se encuentra la interfaz de red y el agregado de ambas.

**Solucionar problemas de conexión**

La solución de problemas de conexión permite probar una conexión entre una máquina virtual, un conjunto de escalado de máquinas virtuales, una puerta de enlace de aplicaciones o un host bastión y una máquina virtual, un FQDN, un URI o una dirección IPv4. La prueba devuelve información similar a la que se devuelve al usar la funcionalidad monitor de conexión, pero prueba la conexión en un momento dado, en lugar de supervisarla con el tiempo, como bien hace la funcionalidad de supervisión de conexión.

**Captura de paquetes**

La captura de paquetes permite crear sesiones de captura de paquetes de forma remota para realizar el seguimiento del tráfico hacia y desde una máquina virtual o un conjunto de escalado de máquinas virtuales.

**Solución de problemas de VPN**

La solución de problemas de VPN le permite solucionar problemas de puertas de enlace de red virtual y sus conexiones.

**Tráfico**

Network Watcher ofrece dos herramientas de tráfico que le ayudan a registrar y visualizar el tráfico de red:

* Registros de flujos
* Análisis de tráfico

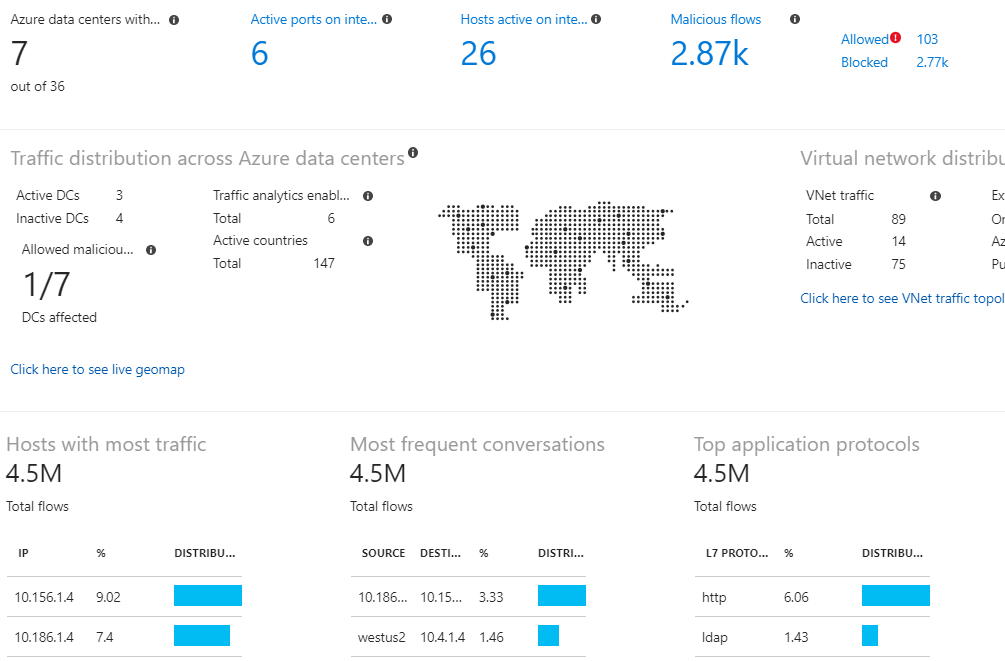
**Registros de flujos**

Los registros de flujo permiten registrar información sobre el tráfico IP de Azure y almacenar los datos en Azure Storage.

Los registros de flujo de los grupos de seguridad de red son una característica de Azure Network Watcher que permite registrar información sobre el tráfico de IP que pasa por un grupo de seguridad de red. Los datos de flujo se envían a Azure Storage y desde allí se puede acceder a ellos y exportarlos a cualquier herramienta que se quiera de visualización, solución de administración de eventos e información de seguridad (SIEM) o sistema de detección de intrusiones (IDS).

**Análisis de tráfico**

El análisis del tráfico proporciona visualizaciones enriquecidas de los datos de los registros de flujo.



**Prueba de conocimientos**

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

**Comprobación de conocimientos**

Principio del formulario

**1. Una empresa está migrando sus aplicaciones a un entorno de PaaS. Quieren asegurarse de que su perímetro de seguridad sea sólido y seguro. ¿Cuál de los siguientes es un procedimiento recomendado para administrar el perímetro de identidad?**

1. Almacene credenciales y secretos en código fuente o GitHub.
2. Use el pensamiento centrado en la red para definir el perímetro de seguridad principal.
3. Proteja claves y credenciales mediante una solución centralizada, como Azure Key Vault.

**2. Una empresa desea configurar la seguridad de la red como una extensión natural de la estructura de una aplicación. Desean agrupar máquinas virtuales y definir directivas de seguridad de red basadas en esos grupos. ¿Qué característica de Azure deberían usar?**

1. Grupo de seguridad de red (NSG)
2. Puntos de conexión de servicio de red virtual
3. Grupos de seguridad de aplicaciones (ASG)

**3. Una empresa debe conectar dos redes virtuales en Azure para que el tráfico se pueda enrutar entre ellas. ¿Qué tipo de conexión de red virtual se debería usar?**

1. Emparejamiento global
2. VPN Gateway
3. Emparejamiento de redes virtuales de Azure

**4. Un grupo de seguridad de red está asociado a la interfaz de red de una máquina virtual. Las reglas de seguridad del grupo de seguridad de red se procesan para el tráfico entrante. Si el grupo de seguridad de red permite la entrada por el puerto 80, ¿cuál de los siguientes procesará el tráfico?**

1. Las reglas de seguridad del grupo de seguridad de red asociado a la subred y a la interfaz de red
2. Las reglas de seguridad del grupo de seguridad de red asociado a la subred
3. Las reglas de seguridad del grupo de seguridad de red asociado a la interfaz de red

**5. Una empresa desea establecer topologías de red que combinen la conectividad entre entornos con la conectividad entre redes virtuales. ¿Qué característica de Azure le permite hacerlo?**

1. Puerta de enlace de red virtual de Azure
2. Azure Resource Manager
3. Emparejamiento de VNET
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, aprendió a planear e implementar medidas de seguridad completas para redes virtuales de Azure, incluyendo el uso de grupos de seguridad de red (NSG), grupos de seguridad de aplicaciones (ASG), rutas definidas por el usuario (UDR), el emparejamiento de redes virtuales, puertas de enlace de VPN, virtual WAN, conectividad VPN, el cifrado de ExpressRoute, la configuración de firewall para recursos de PaaS y la supervisión de seguridad de red con Network Watcher.