**Introducción**

Azure Network Watcher es una herramienta eficaz que permite supervisar, diagnosticar y administrar recursos en una red virtual de Azure.

Imagine que es administrador de TI para una gran empresa de comercio electrónico. Su empresa se basa en gran medida en su red virtual de Azure para hospedar su sitio web y controlar las transacciones de los clientes. Un día, recibe informes de los clientes de que no pueden acceder al sitio web o completar sus compras. Debe identificar rápidamente la causa de las incidencias de conectividad y resolverlas para minimizar el impacto en su empresa.

Su organización planea usar Network Watcher. Las funcionalidades de supervisión y diagnóstico de Network Watcher permiten identificar fácilmente la causa principal del problema y realizar las acciones adecuadas. Mediante el uso de características como la comprobación del flujo de IP, el análisis del próximo salto y la solución de problemas de conexión, puede asegurarse de que la red virtual funciona de forma óptima.

En este módulo, obtendrá información sobre las distintas características y casos de uso de Azure Network Watcher. Los temas tratados incluyen la comprobación del flujo de IP, el análisis del próximo salto y la herramienta de topología. El módulo le guía sobre cómo diagnosticar incidencias de configuración de red, como reglas de seguridad interrumpidas.

El objetivo de este módulo es proporcionarle una comprensión completa de Azure Network Watcher y sus funcionalidades. Al final de este módulo, supervisará, diagnosticará y administrará eficazmente la red virtual de Azure mediante Network Watcher.

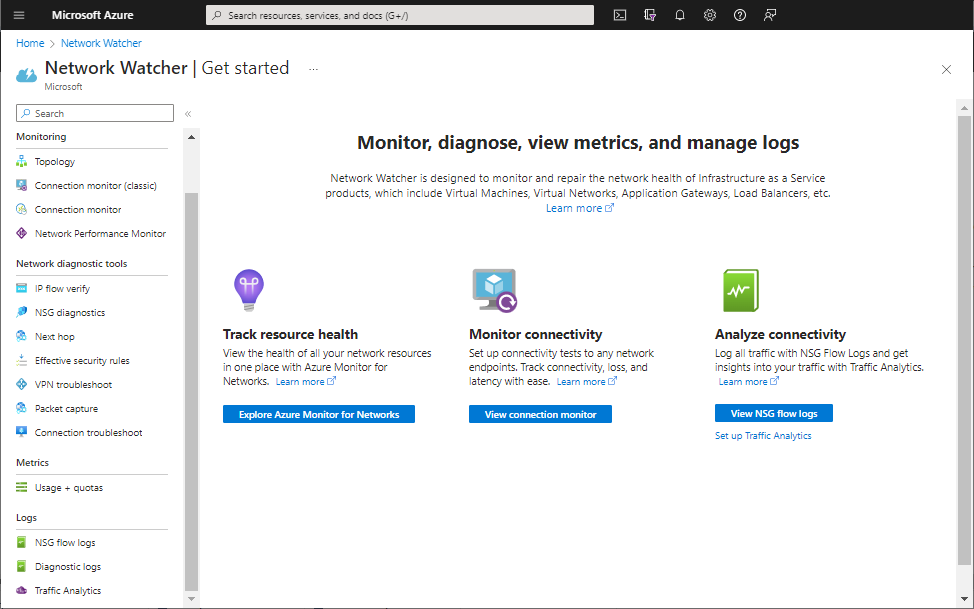
**Objetivos de aprendizaje**

En este módulo aprenderá a:

* Identificar las características y los casos de uso de Azure Network Watcher.
* Configurar las funcionalidades de diagnóstico, como la comprobación del flujo de IP, el próximo salto y la topología de red.

**Descripción de las características de Azure Network Watcher**

Azure Network Watcher proporciona herramientas para supervisar, diagnosticar, ver las métricas y habilitar o deshabilitar registros de recursos en una red virtual de Azure. Network Watcher es un servicio regional que permite supervisar y diagnosticar las condiciones en un nivel de escenario de red.



**Aspectos que se deben conocer sobre Network Watcher**

Veamos algunas de las características destacadas de Network Watcher.

| **Característica** | **Descripción** | **Escenarios** |
| --- | --- | --- |
| **Comprobación de flujo de IP** | Diagnostique rápidamente problemas de conectividad desde o hacia Internet, y desde o hacia el entorno local. | *Identificar si una regla de seguridad bloquea el tráfico de entrada o de salida hacia una máquina virtual o desde ella*  *Solucionar problemas para determinar si se requiere otra exploración* |
| **Próximo salto** | Vea el siguiente punto de conexión (o *próximo salto*) en la ruta de red y analice la configuración de enrutamiento de red. | *Determinar si hay un próximo salto y ver su destino, tipo y tabla de rutas*  *Confirmar que el tráfico llega a un destino previsto* |
| **Solución de problemas de VPN** | Diagnostique y solucione el estado de la puerta de enlace de red virtual o la conexión con datos recopilados. Vea estadísticas de conexión, información de CPU y memoria, errores de seguridad de IKE, eliminaciones de paquetes, búferes y eventos. | *Visualizar diagnósticos de resumen en Azure Portal*  *Revisar diagnósticos detallados en los archivos de registro generados que se almacenan en la cuenta de almacenamiento de Azure*  *Solucionar problemas de varias puertas de enlace o conexiones simultáneamente* |
| **Diagnósticos del grupo de seguridad de red** | Use registros de flujo para asignar el tráfico IP a través de un grupo de seguridad de red (NSG). Es habitual implementar los registros de flujo de NSG para satisfacer las normativas de cumplimiento de seguridad y los requisitos de auditoría. | *Definir reglas de NSG prescriptivas para la organización y realizar auditorías de cumplimiento periódicas*  *Comparar las reglas de NSG prescriptivas con las reglas vigentes para cada máquina virtual de la red* |
| **Solucionar problemas de conexión** | Solución de problemas de conexión de Network Watcher es una adición reciente al conjunto de herramientas y funcionalidades de red de Network Watcher. Compruebe una conexión TCP o ICMP directa desde una máquina virtual, una puerta de enlace de aplicaciones o un host de Azure Bastion a una máquina virtual. | *Solucionar problemas de conectividad y rendimiento de la red en Azure*  *Solucionar problemas de conexión de una máquina virtual, una puerta de enlace de aplicación o un host de Azure Bastion* |

**Nota**

Para usar Network Watcher, debe ser propietario, colaborador o colaborador de red. Si crea un rol personalizado, el rol debe ser capaz de leer, escribir y eliminar el servicio Network Watcher.

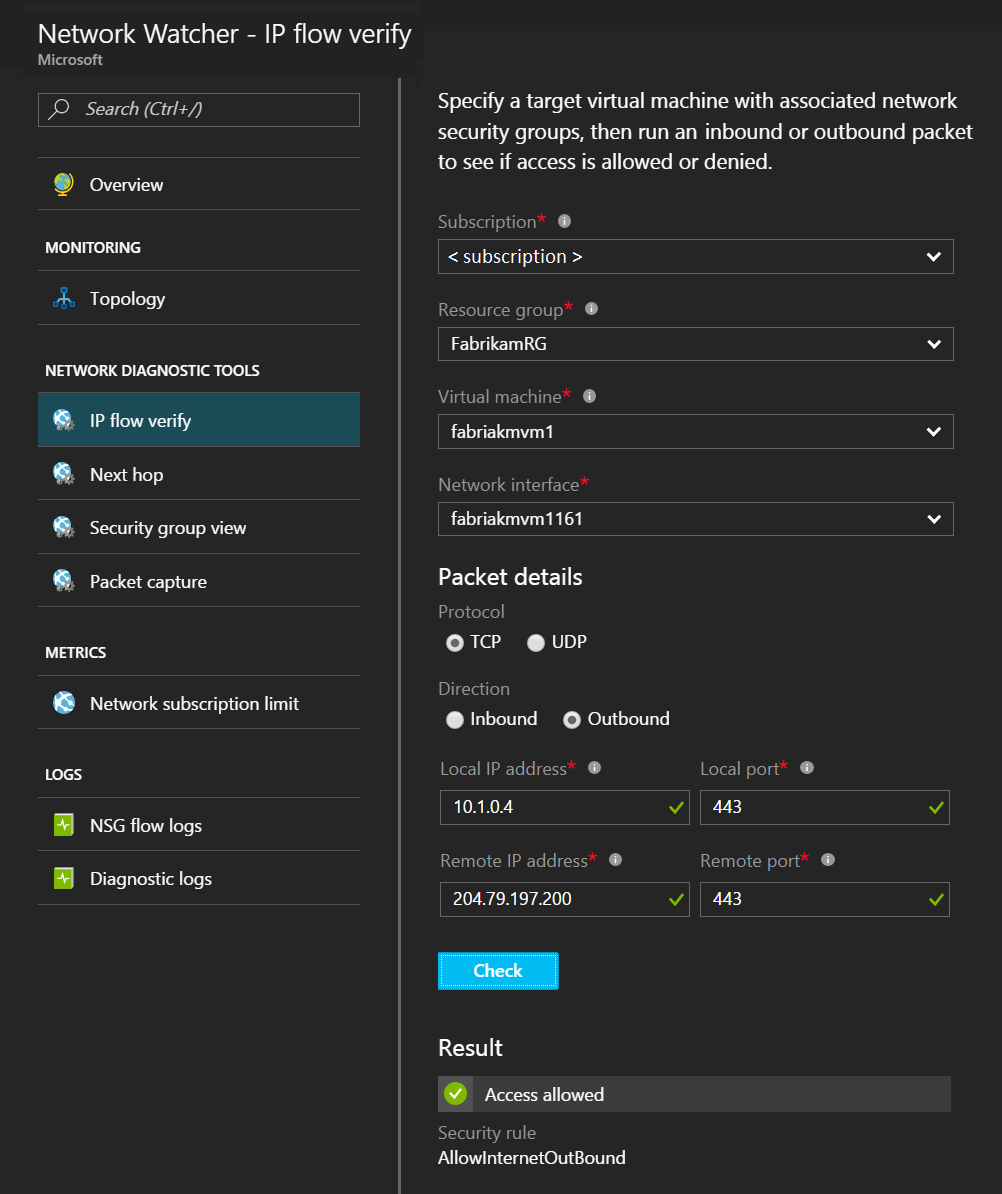
**Aspectos que se deben tener en cuenta al usar Network Watcher**

Azure Network Watcher admite muchas tareas y escenarios de supervisión de Azure. A medida que revise estas características, piense de qué manera puede ayudarle Network Watcher a admitir los requisitos de supervisión de Azure.

* **Considere la posibilidad de realizar la supervisión remota**. Automatización de la supervisión de la red remota con captura de paquetes. Puede supervisar y diagnosticar problemas de red sin iniciar sesión en las máquinas virtuales.
* **Tenga en cuenta las notificaciones de alerta**. Establezca alertas para desencadenar la captura de paquetes y acceder a información de rendimiento en tiempo real en el ámbito de paquete. Cuando observe un problema, puede investigar en detalle para obtener mejores diagnósticos.
* **Tenga en cuenta el diagnóstico del registro de flujo de NSG**. Use registros de flujo de NSG para obtener información sobre el tráfico de la red. Conozca al detalle el patrón de tráfico de red mediante los registros de flujo de NSG. La información que proporcionan los registros de flujo le ayuda a recopilar datos para el cumplimiento, la auditoría y la supervisión de su perfil de seguridad de red.
* **Considere la posibilidad de analizar los registros**. Diagnostique los problemas más comunes de las conexiones y de Azure VPN Gateway. Puede identificar los problemas y usar los registros detallados generados para ayudar al análisis.

**Revisión de los diagnósticos de comprobación del flujo de IP**

La característica de **comprobación del flujo de IP** en Azure Network Watcher comprueba la conectividad desde o hacia Internet, y desde o hacia el entorno local. Esta característica le ayuda a identificar si una regla de seguridad bloquea el tráfico hacia o desde la máquina virtual o Internet.



**Aspectos que se deben conocer sobre la comprobación del flujo de IP**

Vamos a examinar los detalles de configuración y la funcionalidad de la característica de comprobación de flujo de IP en Azure Network Watcher.

* Configure la característica de comprobación del flujo de IP con las siguientes propiedades en Azure Portal:
  + La suscripción y el grupo de recursos
  + La dirección IP local (origen) y el número de puerto local
  + La dirección IP remota (destino) y el número de puerto remoto
  + El protocolo de comunicación (TCP o UDP)
  + La dirección del tráfico (entrante o saliente)
* La característica prueba la comunicación de una máquina virtual de destino con las reglas del grupo de seguridad de red (NSG) asociadas. Para ello, ejecuta paquetes entrantes y salientes hacia y desde la máquina.
* Una vez completada la prueba, la característica le informa de si la comunicación con la máquina se realiza correctamente (permite el acceso) o produce un error (deniega el acceso).
* Si la máquina de destino deniega el paquete debido a un grupo de seguridad de red, la característica devuelve el nombre de la regla de seguridad de control.

**Aspectos que se deben tener en cuenta al usar la comprobación del flujo de IP**

La característica de comprobación del flujo de IP es ideal para ayudar a garantizar la aplicación de correcciones de las reglas de seguridad.

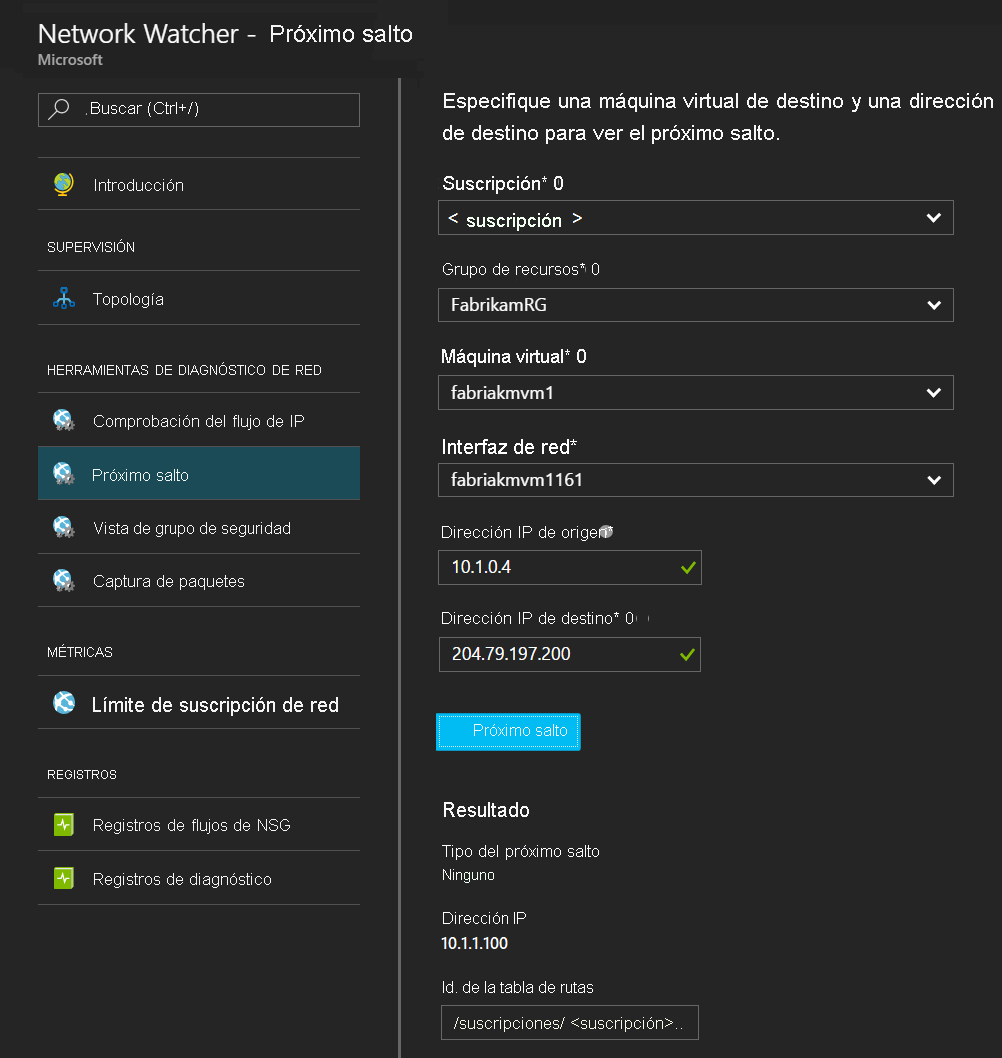
Cuando se implementa una máquina virtual, Azure aplica varias reglas de seguridad predeterminadas a la máquina virtual. Las reglas de seguridad permiten o deniegan el tráfico hacia o desde la máquina virtual. Puede invalidar las reglas predeterminadas de Azure o crear otras reglas.

En algún momento, es posible que la máquina virtual no pueda comunicarse con otros recursos debido a una regla de seguridad. Puede usar la característica de comprobación del flujo de IP para solucionar problemas relacionados con las reglas de NSG.

Si se produce un error en una serie de pruebas, pero la característica de comprobación del flujo de IP no indica que el problema está relacionado con las reglas de NSG, debe explorar otras áreas, como las restricciones de firewall.

**Revisión de los diagnósticos del próximo salto**

La característica de **próximo salto** de Azure Network Watcher comprueba si el tráfico se dirige al destino previsto. Esta característica le permite ver el siguiente punto de conexión (o *próximo salto*) en la ruta de red y le ayuda a comprobar si la configuración de red es correcta.



**Aspectos que se deben conocer sobre la característica próximo salto**

Veamos las propiedades de configuración y el resumen de la característica de próximo salto en Azure Network Watcher.

* Configure la característica de próximo salto con las siguientes propiedades en Azure Portal:
  + La suscripción y el grupo de recursos
  + La máquina virtual y la interfaz de red
  + Dirección IP de origen
  + La dirección IP de destino (si quiere confirmar que se puede acceder a un destino específico)
* La característica prueba el siguiente punto de conexión de la configuración de la ruta de red.
* La prueba del próximo salto devuelve tres elementos:
  + Tipo de próximo salto
  + La dirección IP del próximo salto (si está disponible)
  + La tabla de rutas para el próximo salto (si está disponible)
* Algunos ejemplos de un próximo salto son *Internet*, *Red virtual* y *Punto de conexión de servicio de red virtual*.
* Si el próximo salto es una ruta definida por el usuario (UDR), el proceso devuelve la ruta UDR. De lo contrario, el próximo salto devuelve la ruta del sistema.
* Si el próximo salto es de tipo *None*, podría haber una ruta del sistema válida a la dirección IP de destino, pero no existe ningún próximo salto para enrutar el tráfico al destino.

**Aspectos que se deben tener en cuenta al usar la característica de próximo salto**

La característica de próximo salto es ideal para identificar máquinas virtuales que no responden o rutas rotas de la red.

Cuando se crea una red virtual, Azure crea varias rutas de salida predeterminadas para el tráfico de red. El tráfico saliente de todos los recursos (como máquinas virtuales) implementados en la red virtual se enruta en función de las rutas predeterminadas de Azure. Puede invalidar las rutas predeterminadas de Azure o crear otras rutas.

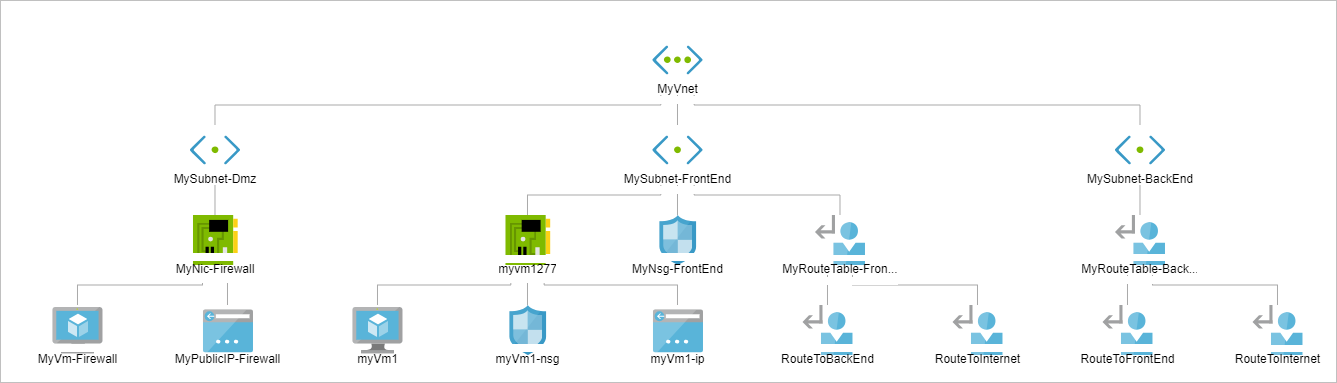
Es posible que una máquina virtual ya no pueda comunicarse con otros recursos conectados mediante una ruta específica. Puede usar la característica de próximo salto para examinar una dirección IP de origen y destino específica de la configuración.

El próximo salto prueba la comunicación entre el origen y el destino e informa del tipo de próximo salto en la ruta de tráfico. Después, puede quitar, cambiar o agregar una ruta para resolver los problemas de enrutamiento.

**Visualización de la topología de red**

A veces, los administradores deben solucionar problemas de redes virtuales que no ayudaron a crear. Es posible que no sean totalmente conscientes de todos los aspectos de la infraestructura y la configuración.

Azure Network Watcher proporciona una herramienta de **topología** de supervisión de red para ayudar a los administradores a visualizar y comprender la infraestructura. En la imagen siguiente se muestra un diagrama de topología de ejemplo de una red virtual en Network Watcher.



**Aspectos que se deben conocer sobre la herramienta de topología**

Revise las siguientes características de la funcionalidad de topología de red en Azure Network Watcher.

* La herramienta de topología de Network Watcher genera un diagrama visual de los recursos de una red virtual.
* En la representación gráfica se muestran los recursos de la red, sus interconexiones y las relaciones entre sí.
* Puede ver subredes, máquinas virtuales, interfaces de red, direcciones IP públicas, grupos de seguridad de red, tablas de rutas, etc.
* Para generar una topología, necesita una instancia de Azure Network Watcher en la misma región que la red virtual.

**Cómo solucionar los problemas más comunes con recursos de Azure**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

<https://youtu.be/FgfcSdHErus>

**Prueba de conocimientos**

Su empresa implementa máquinas virtuales en Azure. Como administrador, es responsable de ayudar a garantizar la conectividad de red de todos los recursos y solucionar los problemas que surjan. Usa Azure Network Watcher como ayuda en sus tareas. Se necesita ayuda en varias áreas.

* El equipo de infraestructura considera que sería útil obtener una representación visual de los elementos de red de la empresa.
* Los usuarios informan de errores de conectividad y tiempos de espera agotados. El departamento de soporte técnico cree que una regla de seguridad podría estar bloqueando el tráfico hacia o desde una de las máquinas virtuales.
* Debe identificar qué escenarios empresariales se van a admitir mediante Network Watcher.

**Responda a las siguientes preguntas**

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

Principio del formulario

**1. ¿Cómo admite Azure Network Watcher las visualizaciones gráficas de las redes?**

1. Próximo salto
2. Vistas
3. Herramienta de topología

**2. ¿Qué característica de Azure Network Watcher puede ayudarle a solucionar rápidamente el problema que ha notificado el departamento de soporte técnico?**

1. Comprobación del flujo de IP
2. Solución de problemas de conexión
3. Captura de paquetes

**3. ¿Qué escenario es un buen caso de uso para Azure Network Watcher?**

1. Registro de eventos de actividad
2. Diagnóstico de problemas de filtrado del tráfico de red hacia o desde una máquina virtual
3. Supervisión de PaaS y análisis web

1. CFinal del formulario

2. A

3. B

**Resumen y recursos**

Azure Network Watcher proporciona las herramientas que necesita para supervisar, solucionar problemas y optimizar su infraestructura de red.

En este módulo, ha identificado las características y los casos de uso de Azure Network Watcher. Ha revisado cómo configurar y trabajar con varias características de Network Watcher, incluida la comprobación del flujo de IP, el próximo salto y la herramienta de topología. Ha descubierto cómo diagnosticar la configuración de red en lo relativo a varios problemas, como el incumplimiento de reglas de seguridad.

Las principales conclusiones de este módulo son:

* Network Watcher es una herramienta eficaz para supervisar y solucionar problemas de infraestructura de red en Azure.
* Network Watcher tiene muchas características, como la comprobación del flujo de IP, el análisis del próximo salto y una herramienta de visualización de topología de red.
* La característica de comprobación del flujo de IP comprueba las reglas de seguridad y administración para el enrutamiento de paquetes a una máquina virtual de Azure.
* La característica de próximo salto le ayuda a determinar si el tráfico se dirige al destino previsto.
* La característica de topología de red le permite visualizar y comprender la infraestructura de las redes virtuales.