Configuración de Cisco Umbrella en la red mediante los routers de la serie RV34x

Introducción

A partir de la versión de firmware 1.0.0.2.16, los routers de la serie RV34x admiten ahora Cisco Umbrella. Umbrella utiliza DNS como un vector o escudo de defensa contra el malware y las intrusiones de datos.

Dispositivos aplicables

- Router de la serie RV34x

Versión del software

- 1.0.02.16

Requirements

- Una cuenta Umbrella activa (¿No tiene ninguna? Solicite un presupuesto o inicie una prueba gratuita)

Objetivo

Esta guía de uso le mostrará los pasos necesarios para integrar la plataforma de seguridad de Umbrella en su red. Antes de entrar en los detalles esenciales, responderemos a algunas preguntas que quizá se esté haciendo sobre Umbrella.

¿Qué es un paraguas?

Umbrella es una plataforma de seguridad para la nube de Cisco sencilla pero muy eficaz. Umbrella funciona en la nube y presta muchos servicios relacionados con la seguridad. De la amenaza emergente a la investigación posterior al evento. Umbrella detecta y evita ataques en todos los puertos y protocolos.

¿Cómo funciona?

Umbrella utiliza DNS como su principal vector de defensa. Cuando los usuarios introducen una URL en la barra del navegador y pulsan Intro, Umbrella participa en la transferencia. Esa URL pasa a la resolución DNS de Umbrella y, si hay una advertencia de seguridad asociada al dominio, la solicitud se bloquea. Estos datos de telemetría se transfieren y analizan en microsegundos, lo que prácticamente no añade latencia. Los datos de telemetría utilizan registros e instrumentos que rastrean miles de millones de solicitudes de DNS en todo el mundo. Cuando estos datos son omnipresentes, su correlación en todo el

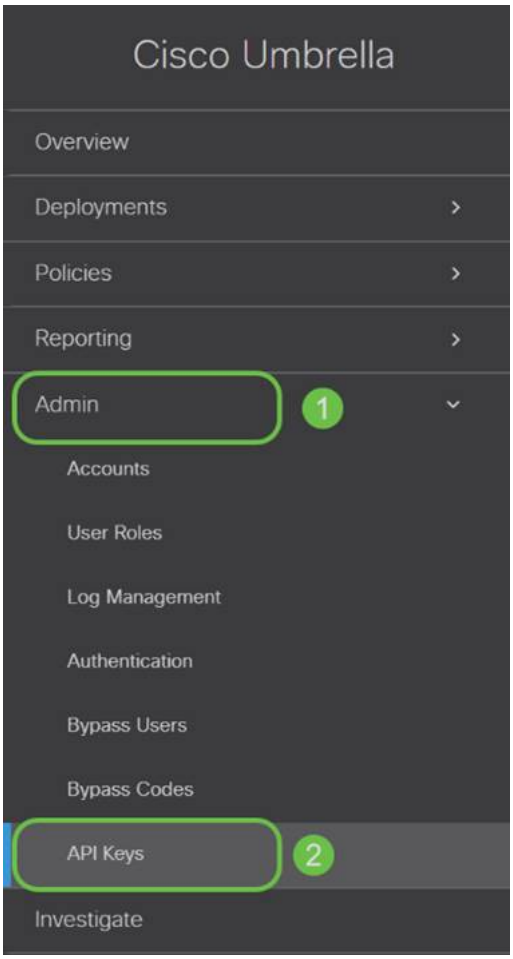
mundo permite una respuesta rápida a los ataques a medida que estos comienzan. Consulte la política de privacidad de Cisco aquí para obtener más información: política completa,versión resumida. Piense en los datos de telemetría como datos derivados de herramientas y registros.

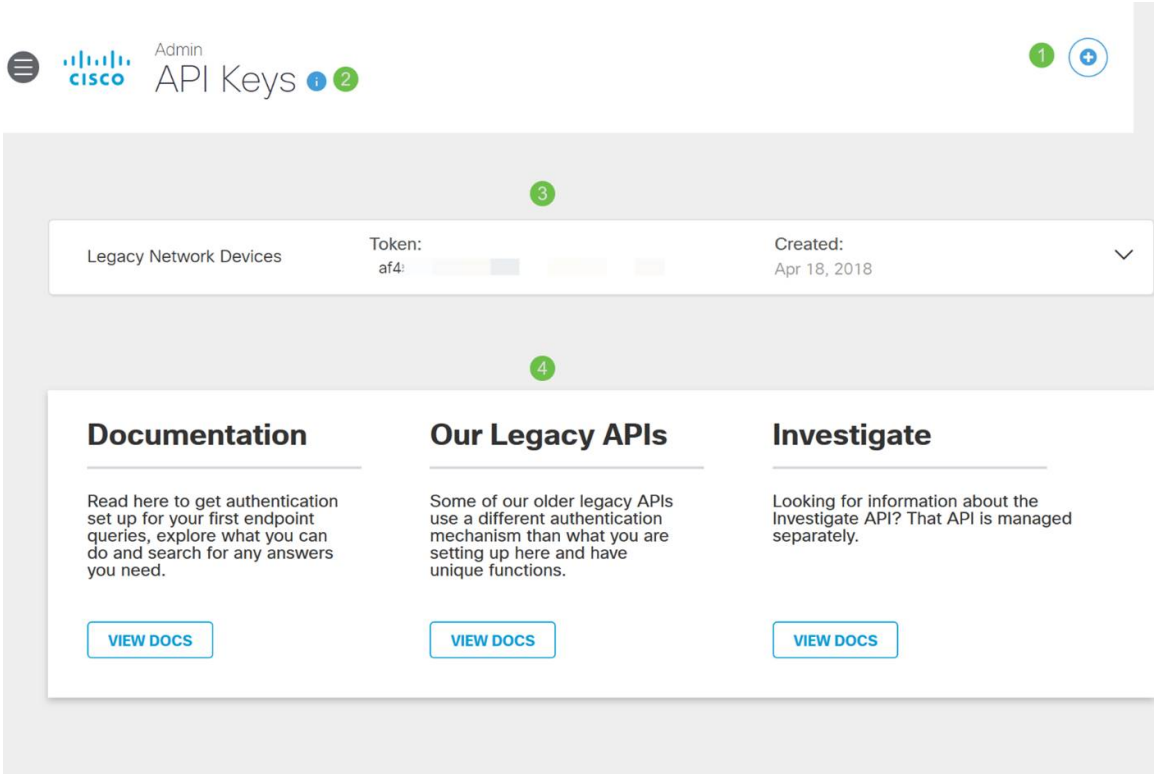
Para resumir en una metáfora, imagine que está en una fiesta. En esta fiesta todos están en su teléfono navegando por la web. El silencio del grupo se ve acentuado por los asistentes a la fiesta que golpean sus pantallas. No es una gran fiesta, pero mientras que en su propio teléfono se ve un hipervínculo a un gatito GIF que parece irresistible. Sin embargo, la URL parece cuestionable, por lo que no está seguro de si debe tocar o no. Así que antes de tocar el hipervínculo, gritas al resto de la fiesta "¿Es malo este enlace?" Si otra persona de la fiesta ha ido al enlace y ha descubierto que era una estafa, gritaría "¡Sí, lo hice y es una estafa!" Agradeces a esa persona por salvarte, continuando tu noble búsqueda de imágenes de lindos animales. Por supuesto, a escala de Cisco, este tipo de comprobaciones de seguridad de devolución de llamada y solicitud se producen millones de veces por segundo, lo que redunda en beneficio de la seguridad de su red.

Suena genial, ¿cómo empezamos esto?

En el lugar por el que se desplaza esta guía, empiece por coger la clave API y la clave secreta del panel de la cuenta de Umbrella. Después, iniciaremos sesión en el dispositivo del router para agregar la API y la clave secreta. Si tiene algún problema, consulte aquí la documentación y aquí las opciones de Umbrella Support.

Paso 1. Después de iniciar sesión en su cuenta de Umbrella, desde la pantalla *Panel*, haga clic en **Admin > API Keys**.

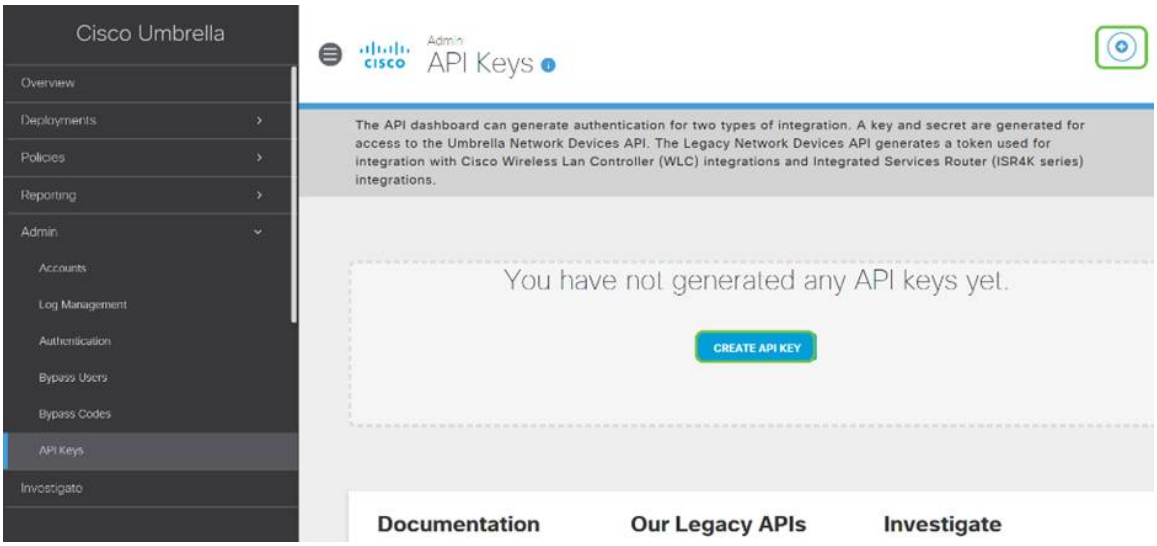




Anatomía de la pantalla API Keys (Claves de API preexistentes):

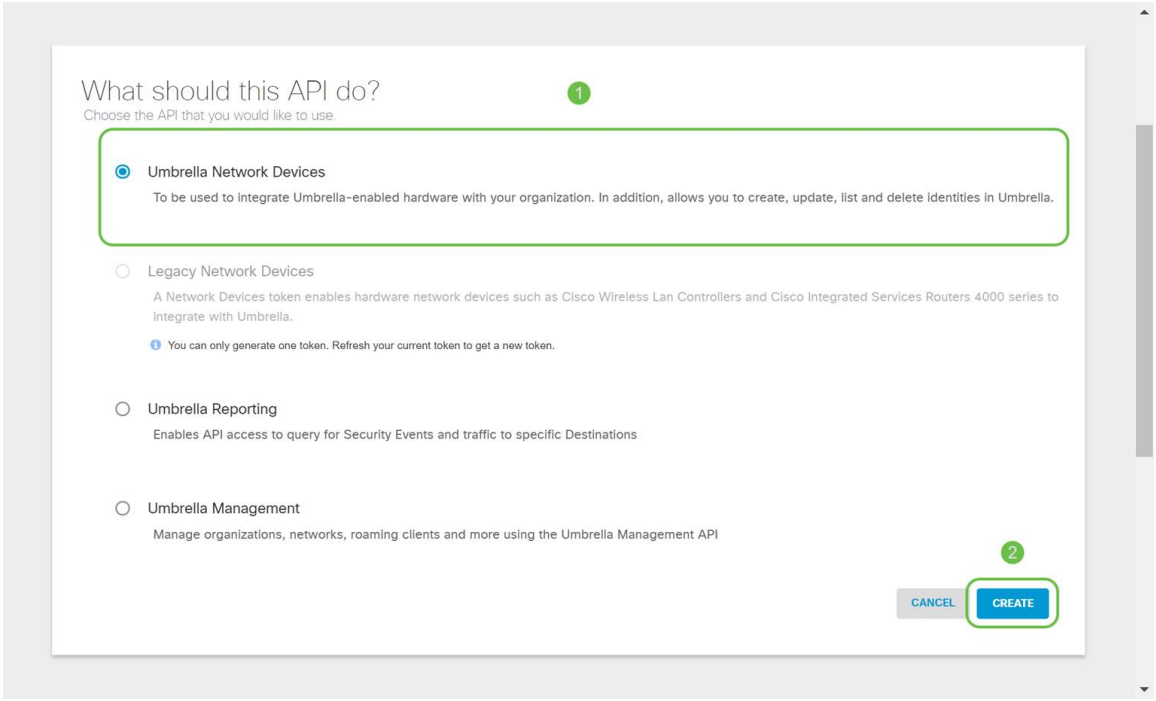
1. Add API Key (Agregar clave de API): inicia la creación de una nueva clave para utilizarla con la API Umbrella.
2. Información adicional: se desliza hacia abajo/hacia arriba con una explicación para esta pantalla.
3. Token Well - Contiene todas las claves y tokens creados por esta cuenta. (Se rellena una vez creada la clave)
4. Documentos de soporte - Enlaces a la documentación del sitio de Umbrella relativa a los temas de cada sección.

Paso 2. Haga clic en el botón **Add API Key** en la esquina superior derecha, o haga clic en el botón **Create API Key**. Ambos funcionan de la misma manera.

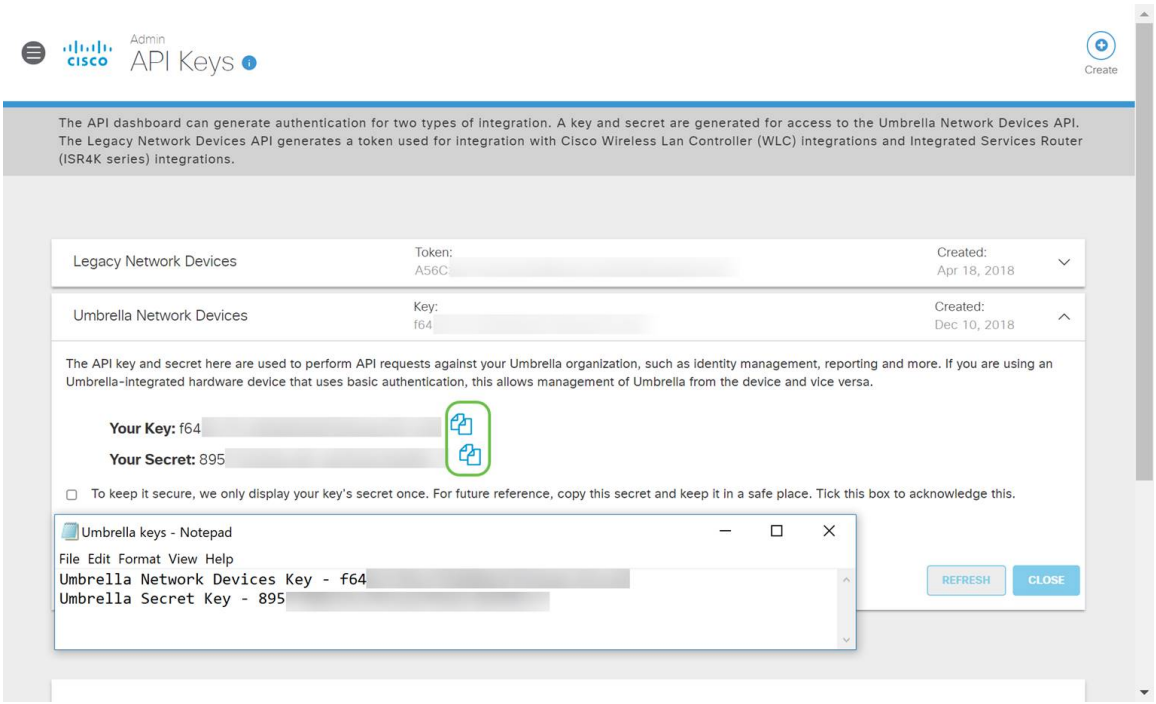


Nota: la captura de pantalla anterior sería similar a lo que vería al abrir este menú por primera vez.

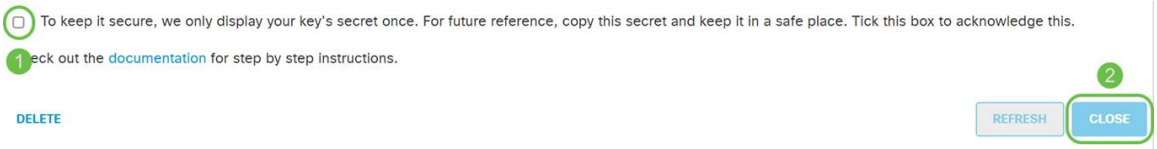
Paso 3. Seleccione **Umbrella Network Devices** y luego haga clic en el botón **Create**.



Paso 4. Abra un editor de texto como el bloc de notas y luego haga clic en el botón **Copiar** a la derecha de su API y API *Clave Secreta,* una notificación emergente confirmará que la clave se copia en el portapapeles. De uno en uno, pegue el secreto y la clave API en el documento, etiquetándolos para futuras referencias. En este caso, su etiqueta es "Umbrella network devices key". A continuación, guarde el archivo de texto en una ubicación segura a la que pueda acceder fácilmente más adelante.



Paso 5. Después de copiar la clave y la clave secreta en una ubicación segura, desde la *pantalla Umbrella API* haga clic en la **casilla de verificación** para confirmar que se ha realizado la confirmación de la visualización temporal de la clave secreta y, a continuación, haga clic en el botón **Close**.



Nota importante: Si pierde o elimina accidentalmente la clave secreta, no habrá ningún

número de función o soporte al que llamar para recuperar esta clave. Mantenlo en secreto, mantenlo a salvo. Si se pierde, tendrá que eliminar la clave y volver a autorizar la nueva clave API con cada dispositivo que desee proteger con Umbrella.

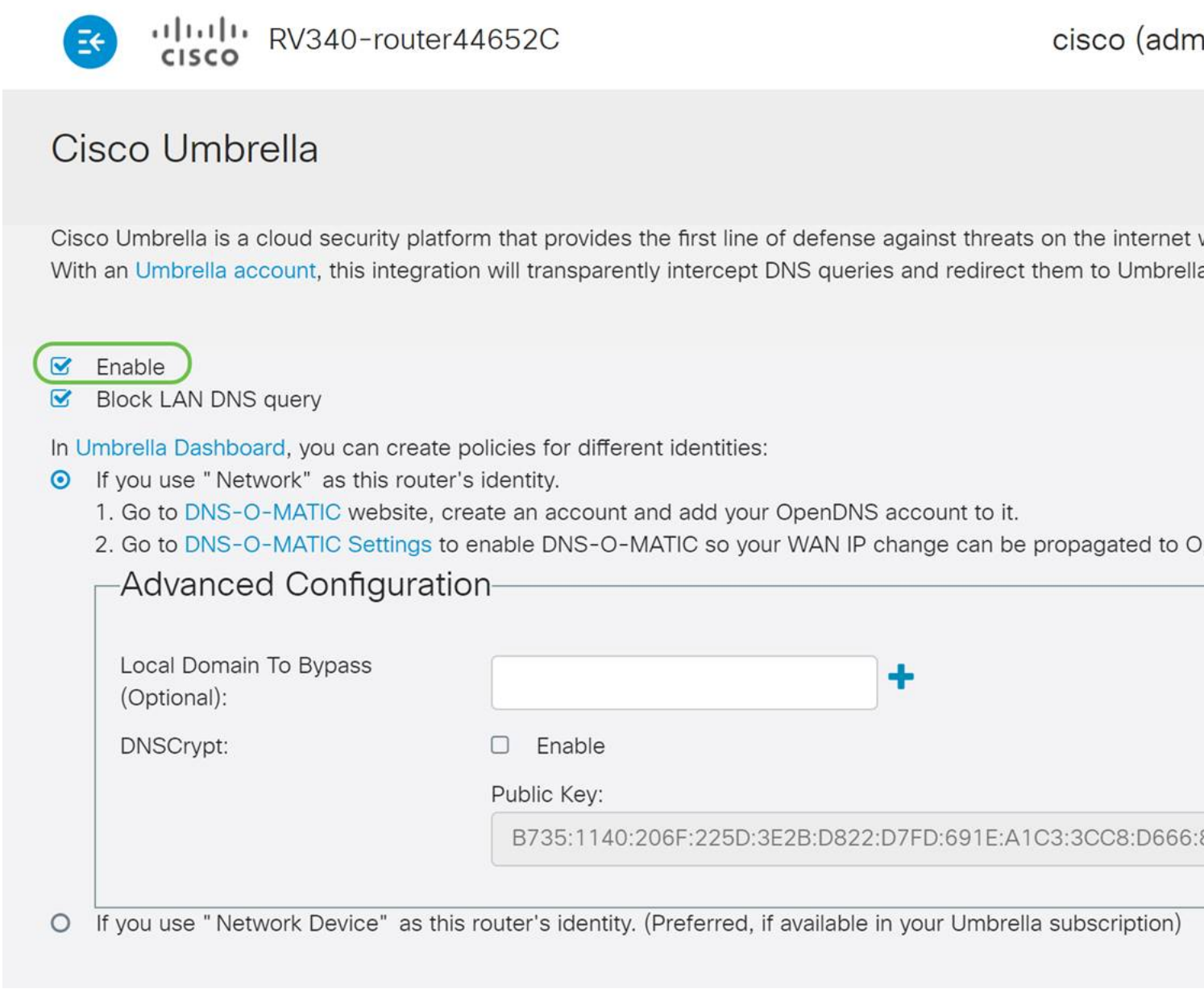
Práctica recomendada: Guarde una *sola* copia de este documento en un dispositivo, como una unidad de almacenamiento en miniatura USB, inaccesible desde cualquier red.

Configuración de Umbrella en su dispositivo RV34x

Ahora que hemos creado claves API en Umbrella, las tomaremos e las instalaremos en nuestros dispositivos RV34x. En nuestro caso estamos utilizando un RV340.

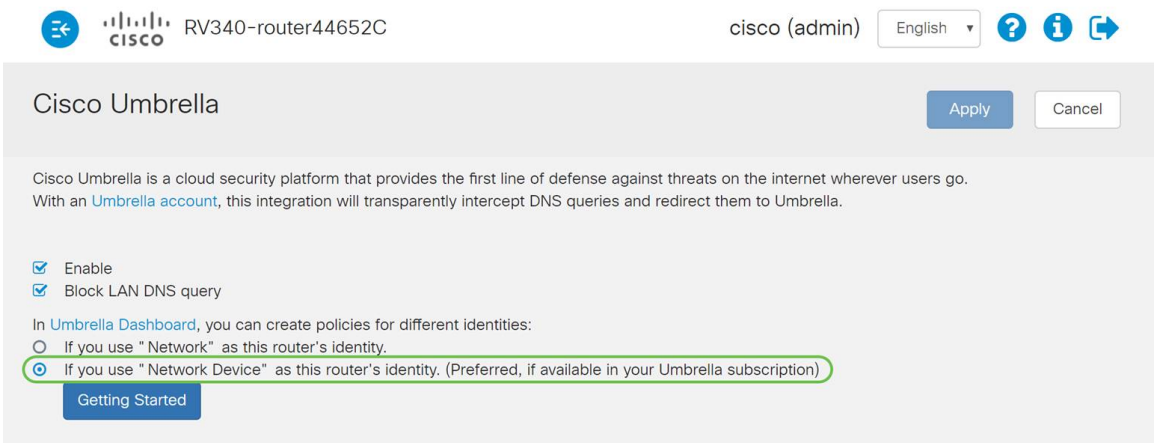
Paso 1. Después de iniciar sesión en su dispositivo RV34x, haga clic en **Seguridad > Paraguas** en el menú de la barra lateral.

Paso 2. La pantalla Umbrella API tiene un rango de opciones, comience a habilitar Umbrella haciendo clic en la casilla de verificación **Enable**.

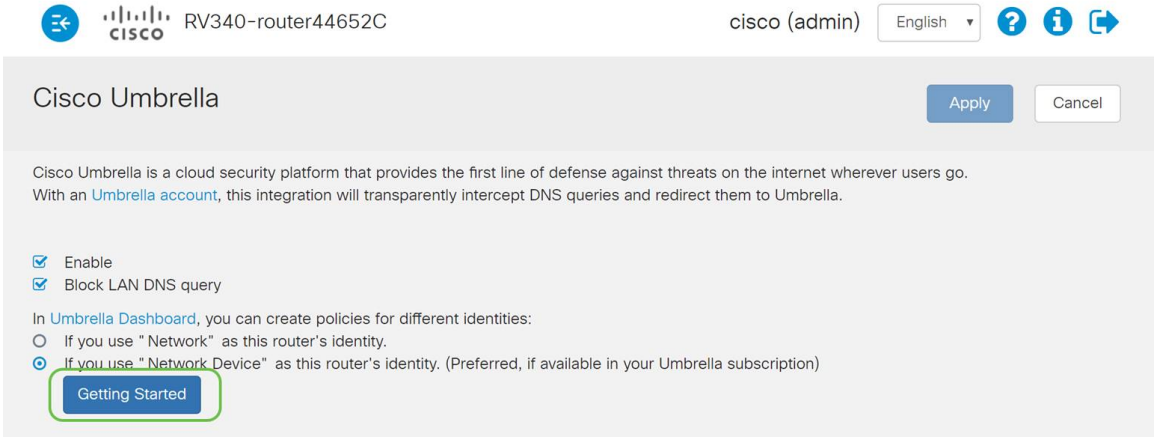


Paso 3. (Opcional) De forma predeterminada, la casilla Block LAN DNS Queries (Bloquear consultas DNS de LAN) está activada. Esta función limpia crea automáticamente listas de control de acceso en el router que evitarán que el tráfico DNS salga a Internet. Esta función obliga a que todas las solicitudes de traducción de dominios se dirijan a través del RV34x y es una buena idea para la mayoría de los usuarios.

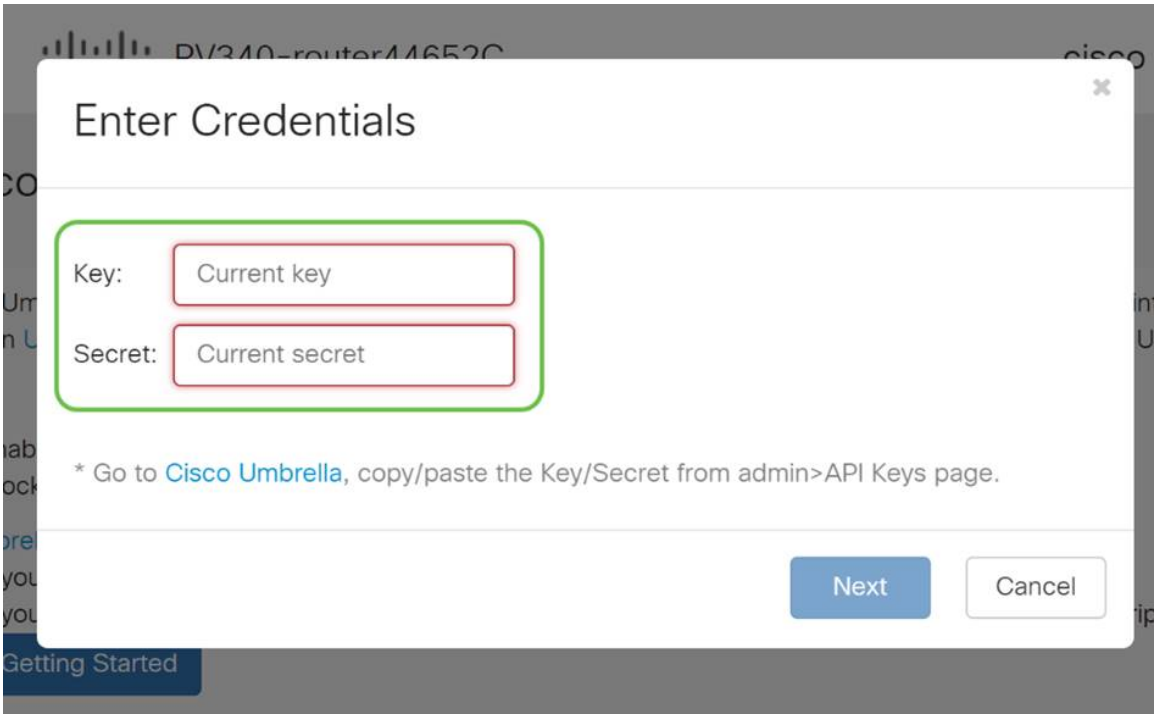
Paso 4. El siguiente paso se desarrolla de dos maneras diferentes. Ambos dependen de la configuración de la red. Si utiliza un servicio como DynDNS o NoIP, debe dejar el esquema de nombres predeterminado de "Red". A continuación, deberá iniciar sesión en esas cuentas para garantizar que Umbrella interactúa con esos servicios, ya que proporciona protección. Para nuestros fines, dependemos de "Dispositivo de red", haga clic en el botón radial inferior.



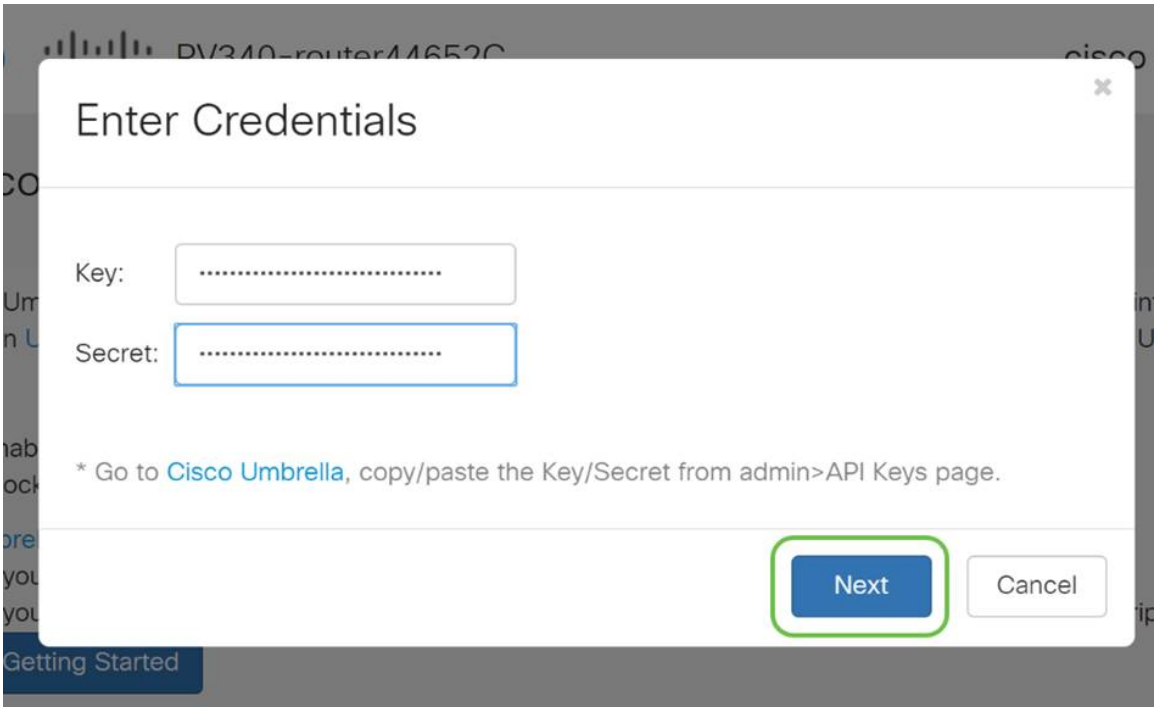
Paso 5. Ahora haga clic en **Introducción** para iniciar el miniasistente.



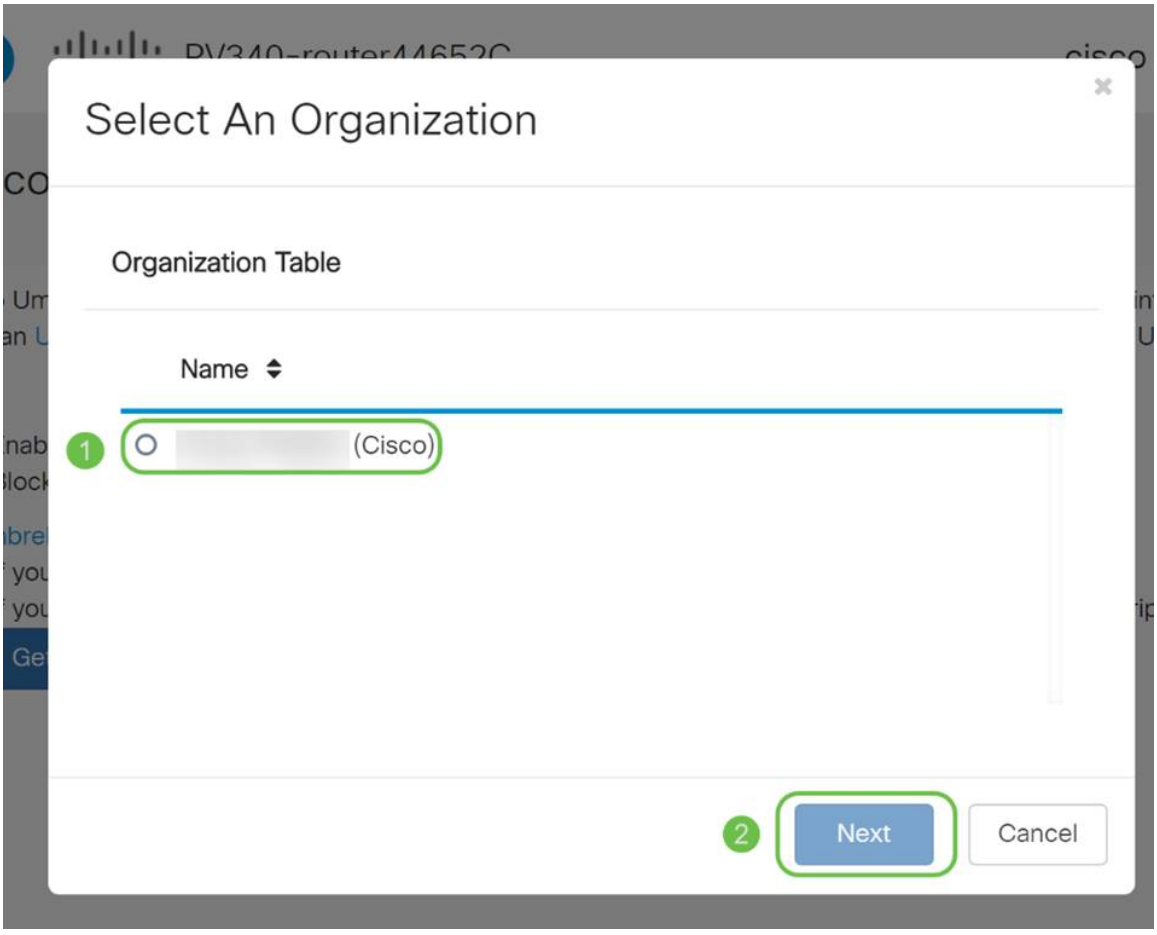
Paso 6. Ahora ingrese la **clave API** y la **clave secreta** en los cuadros de texto.



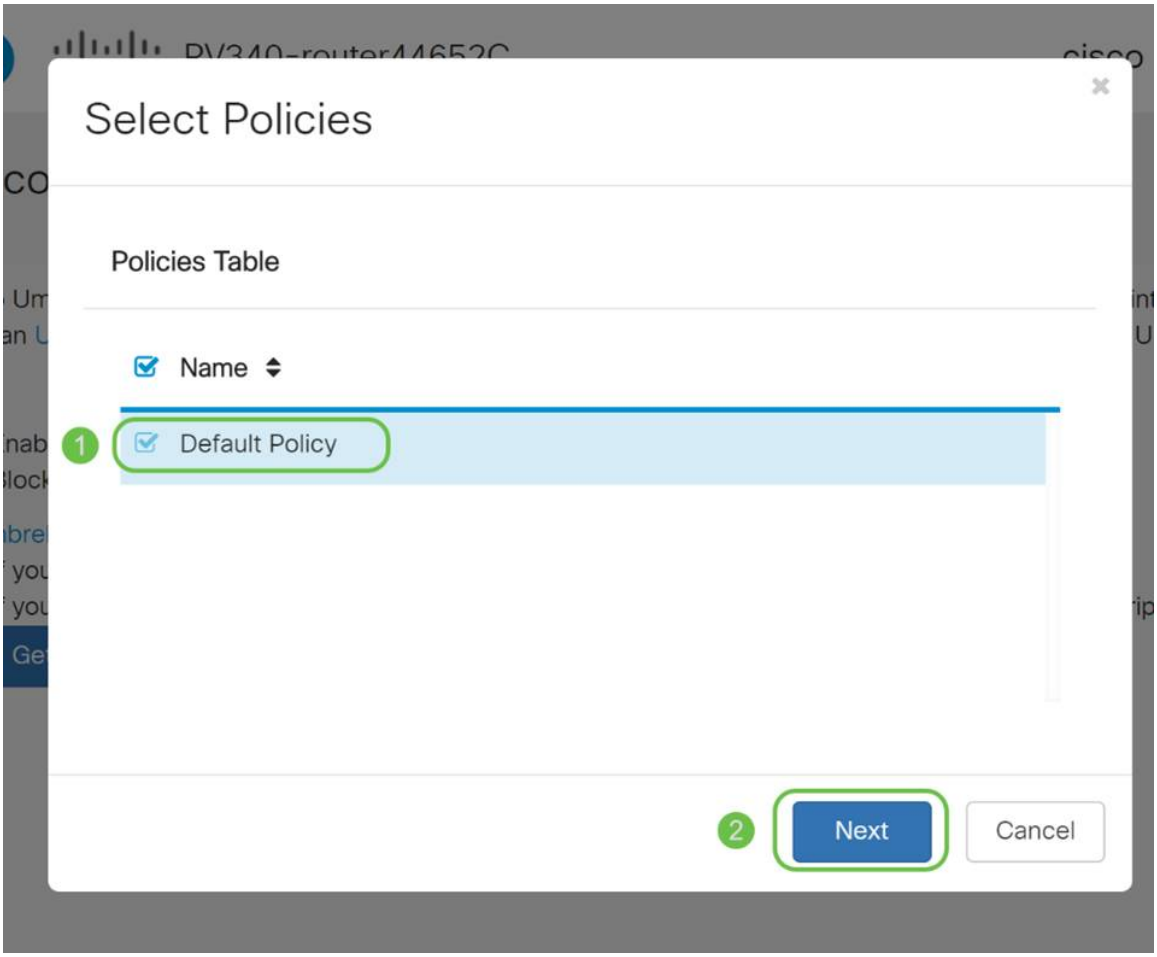
Paso 7. Después de ingresar su API y clave secreta, haga clic en el botón **Next**.



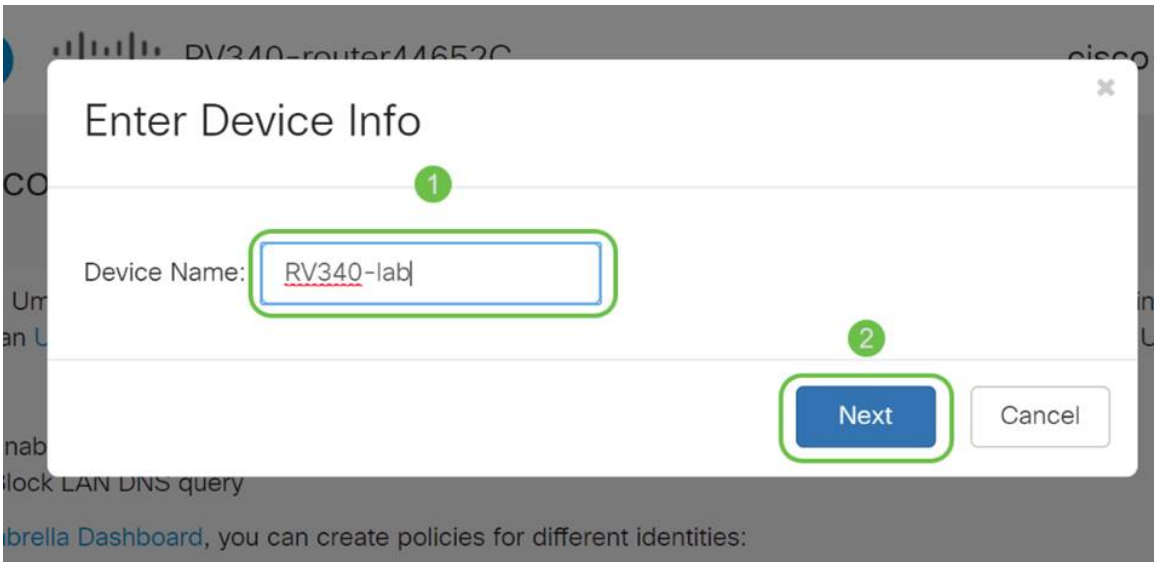
Paso 8. En la siguiente pantalla, seleccione la **organización** que desea asociar al router y, a continuación, haga clic en **Next**.



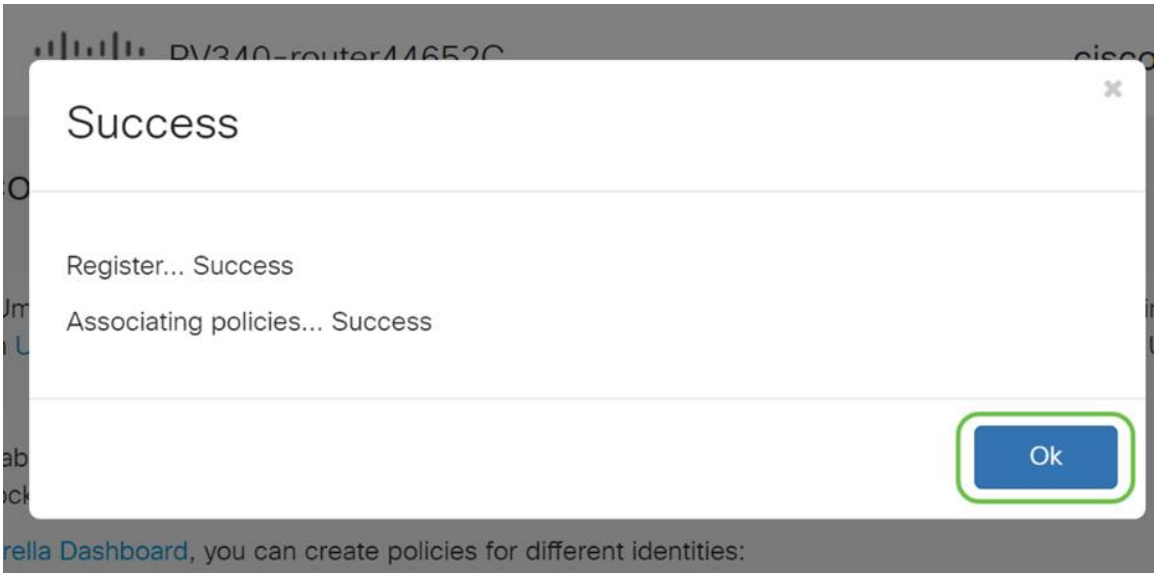
Paso 9. Ahora seleccione la política que se aplicará al tráfico enrutado por el RV34x. Para la mayoría de los usuarios, la política predeterminada proporcionará suficiente cobertura.



Paso 10. **Asigne un nombre** al dispositivo para que pueda designarse en Umbrella reporting. En nuestra configuración hemos asignado "RV340-lab".



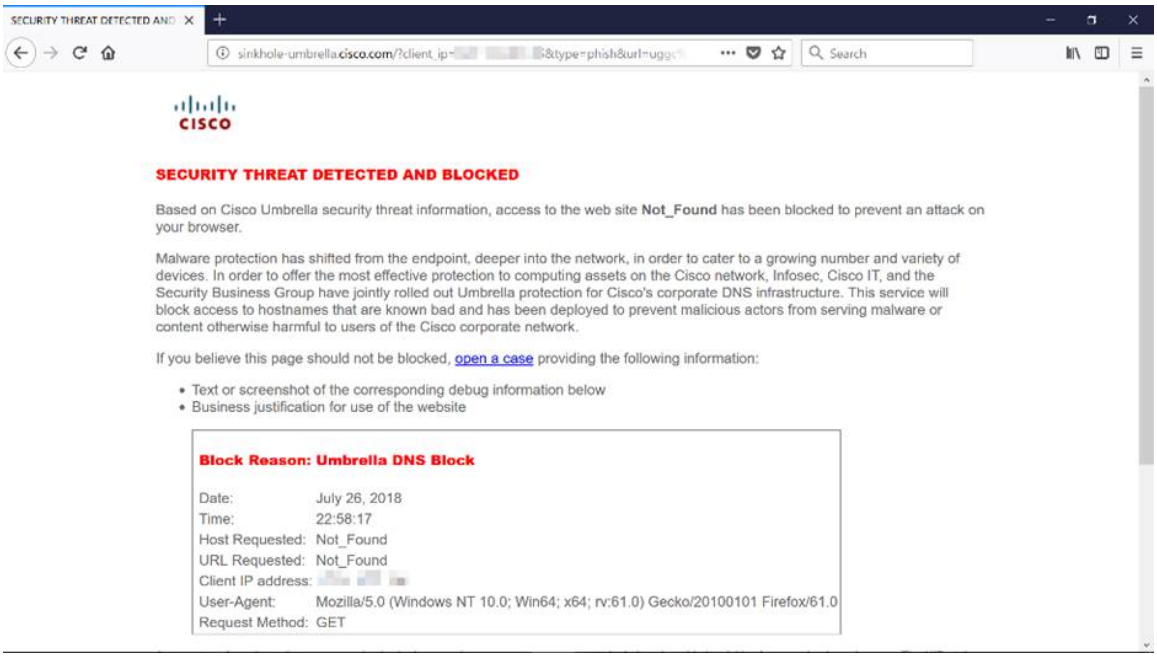
Paso 11. La siguiente pantalla validará la configuración elegida y proporcionará una actualización, cuando se asocie correctamente, haga clic en **Aceptar**.



Confirmar que todo está en su lugar correcto

Enhorabuena, ya está protegido con Cisco Umbrella. ¿O sí? No olvidemos que, al comprobar dos veces con un ejemplo en directo, Cisco ha creado un sitio web dedicado a determinar este aspecto tan rápido como se carga la página. Haga clic aquí o escriba https://InternetBadGuys.com en la barra del explorador.

Si Umbrella está configurado correctamente, será recibido por una pantalla similar a esta!



Ver un vídeo relacionado con este artículo...

Haga clic aquí para ver otras charlas tecnológicas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).