Configuración de la protección contra ataques en el router VPN RV132W o RV134W

Objetivo

La protección frente a ataques permite proteger la red frente a tipos habituales de ataques, como la detección, las inundaciones y las tormentas de eco. Mientras que el router tiene activada la protección contra ataques de forma predeterminada, puede ajustar los parámetros para que la red sea más sensible y más receptiva a los ataques que pueda detectar.

En este artículo se explica cómo configurar la protección frente a ataques en el RV132W y el router VPN RV134W.

Dispositivos aplicables

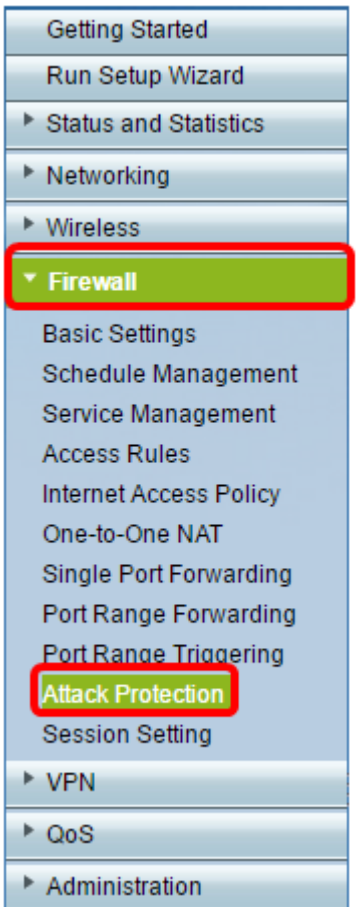
- RV 132W
- RV134W

Versión del software

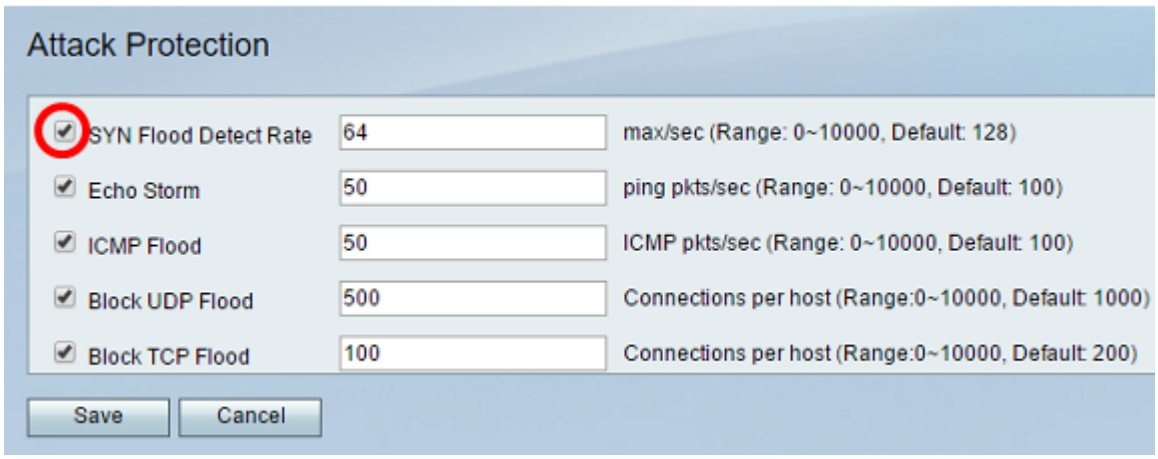
- 1.0.0.17 — RV132W
- 1.0.0.24 — RV134W

Configurar protección frente a ataques

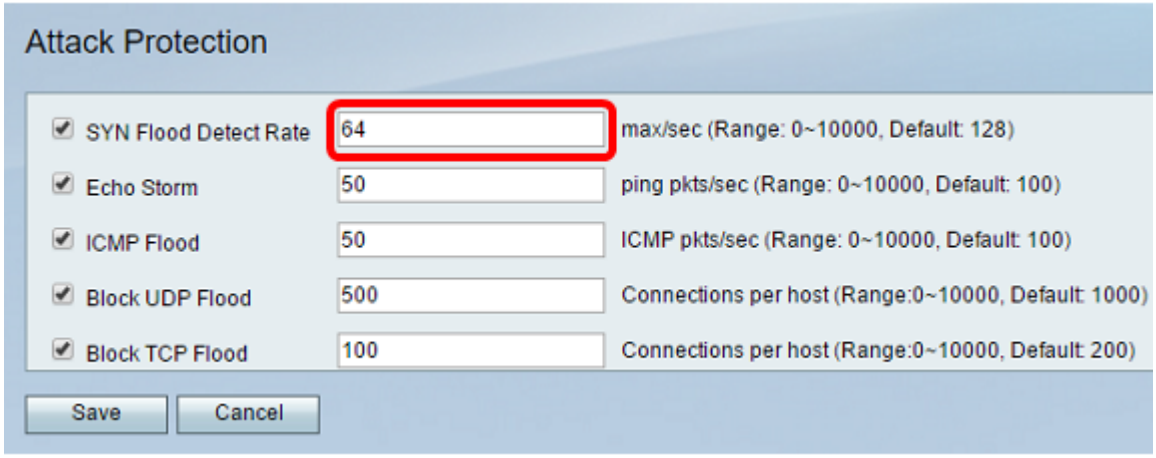
Paso 1. Inicie sesión en la utilidad basada en Web y seleccione **Firewall > Attack Protection**.



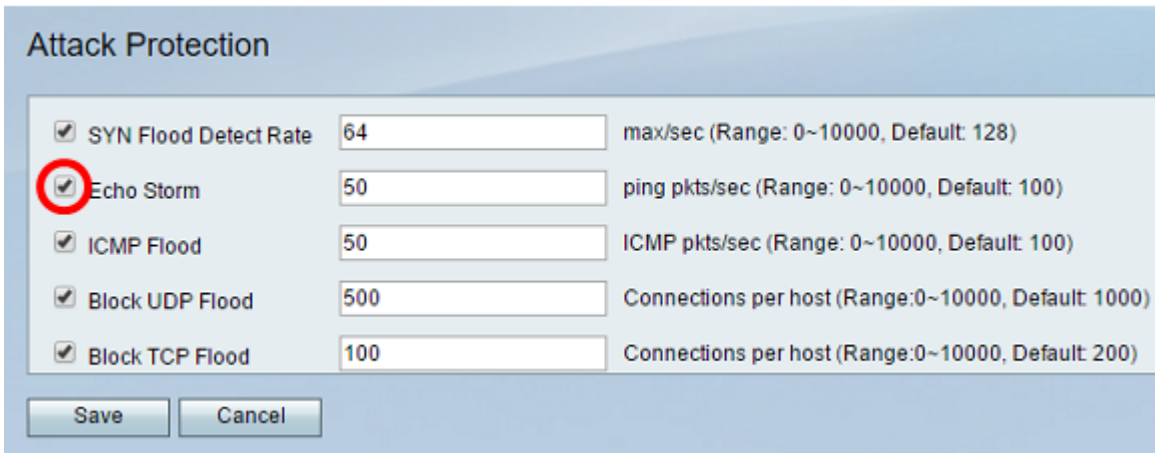
Paso 2. Verifique que la casilla de verificación SYN Flood Detect Rate (Velocidad de detección de inundación SYN) esté marcada para asegurarse de que la función está activa. Esta opción está activada de forma predeterminada.



Paso 3. Introduzca un valor en el campo *SYN Flood Detect Rate*. El valor predeterminado es 128 paquetes SYN por segundo. Puede introducir un valor entre 0 y 10000. Será el número de paquetes SYN por segundo lo que hará que el dispositivo de seguridad determine que se está produciendo una intrusión de inundación SYN. Un valor de cero indicará que la función SYN Flood Detection está inhabilitada. En este ejemplo, el valor introducido es 64. Esto significa que el dispositivo detectaría una intrusión de inundación SYN a solo 64 paquetes SYN por segundo, lo que lo hace más sensible que la configuración predeterminada.

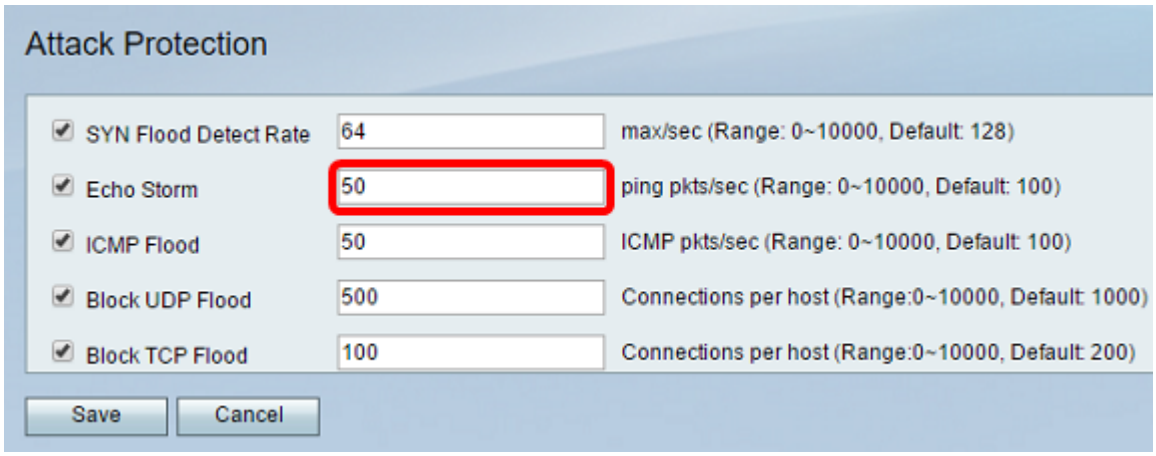


Paso 4. Compruebe que la casilla de verificación Tormenta de eco está activada para asegurarse de que la función está activa. Esta opción está activada de forma predeterminada.

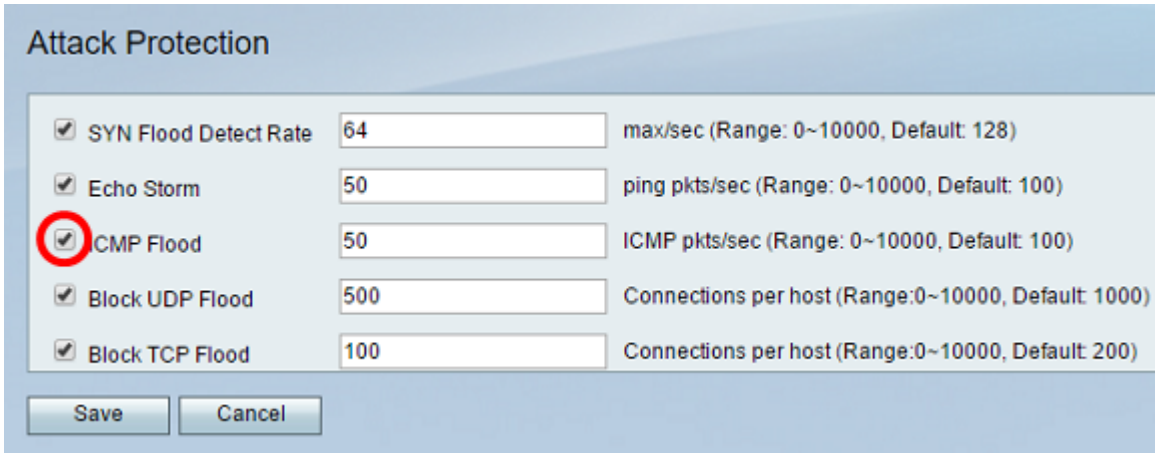


Paso 5. Introduzca un valor en el campo *Tormenta de eco*. El valor predeterminado es 100 pings por segundo. Puede introducir un valor entre 0 y 10000. Será el número de pings por segundo que hará que el dispositivo de seguridad determine que se está produciendo un evento de intrusión de tormenta de eco. Un valor de cero indicará que la función Tormenta de eco está desactivada.

Nota: en este ejemplo, el dispositivo detectaría un evento de tormenta de eco a solo 50 pings por segundo.

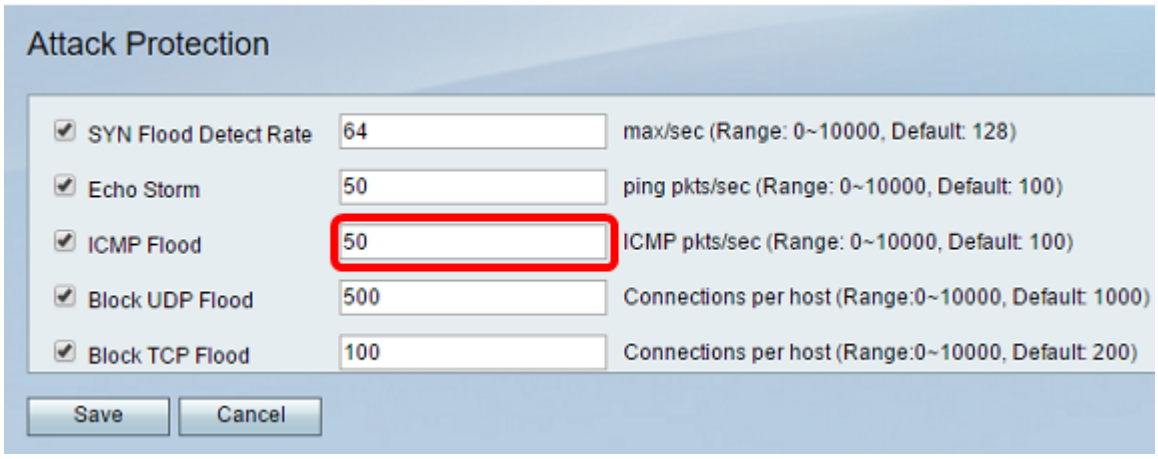


Paso 6. Compruebe que la casilla de verificación Inundación del protocolo de mensajes de control de Internet (ICMP) está activada para asegurarse de que la función está activa. Esta función está activada de forma predeterminada.

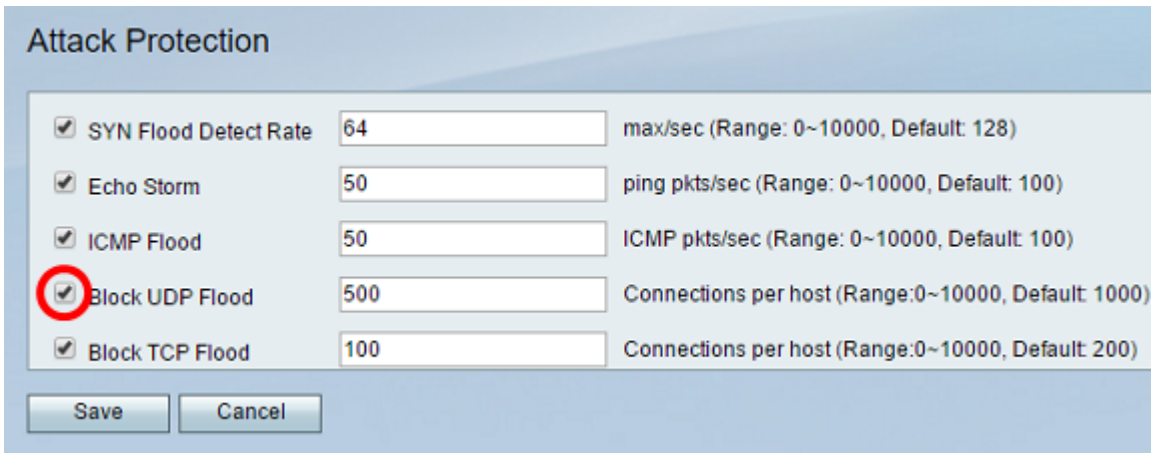


Paso 7. Introduzca un valor numérico en el campo *ICMP Flood*. El valor predeterminado es 100 paquetes ICMP por segundo. Puede introducir un valor entre 0 y 10000. Será el número de paquetes ICMP por segundo lo que hará que el dispositivo de seguridad determine que se está produciendo un evento de intrusión de inundación ICMP. Un valor de cero indicará que la función ICMP Flood está inhabilitada.

Nota: En este ejemplo, el valor ingresado es 50, lo que lo hace más sensible a la inundación ICMP que su configuración predeterminada.

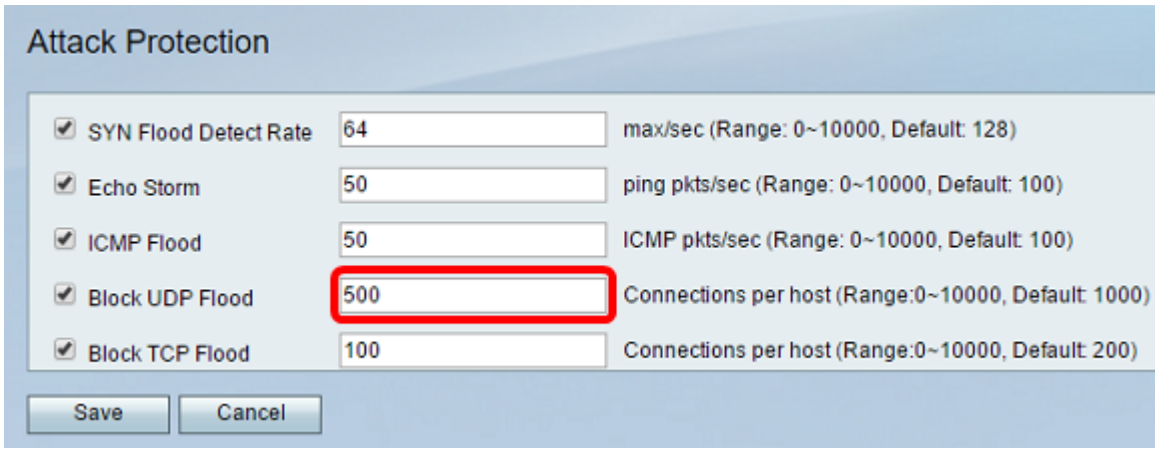


Paso 8. Compruebe que la casilla de verificación Block UDP Flood (Bloquear inundación UDP) está activada para asegurarse de que la función está activa e impedir que el dispositivo de seguridad acepte más de 150 conexiones activas simultáneas de protocolo de datagramas de usuario (UDP) por segundo desde un único ordenador de la red de área local (LAN). Esta opción está activada de forma predeterminada.

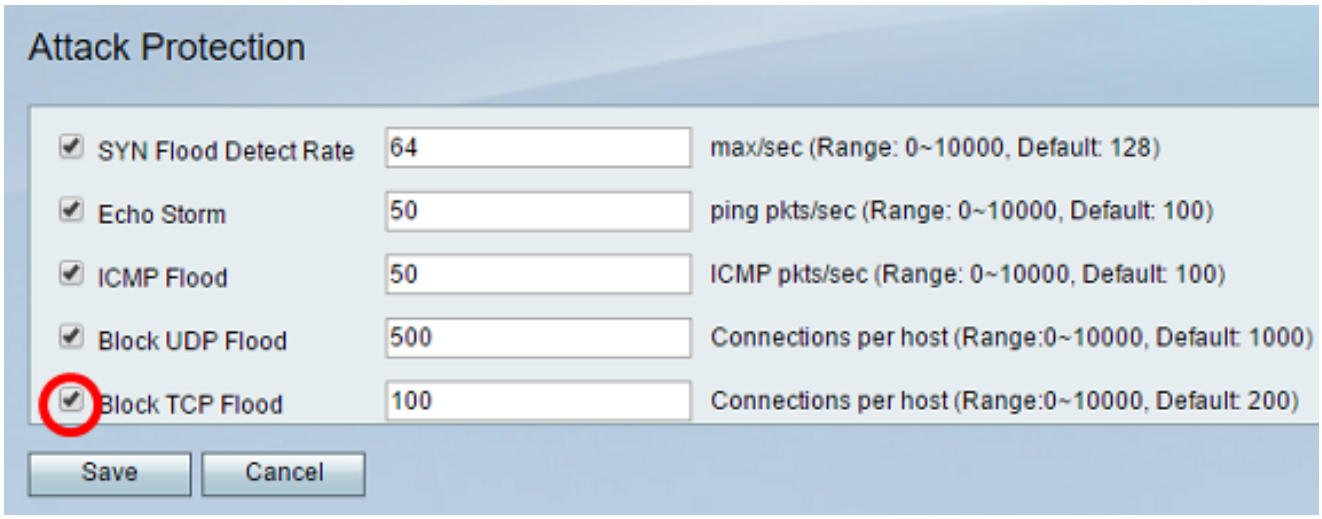


Paso 9. Introduzca un valor entre 0 y 10000 en el campo *Block UDP Flood*. El valor

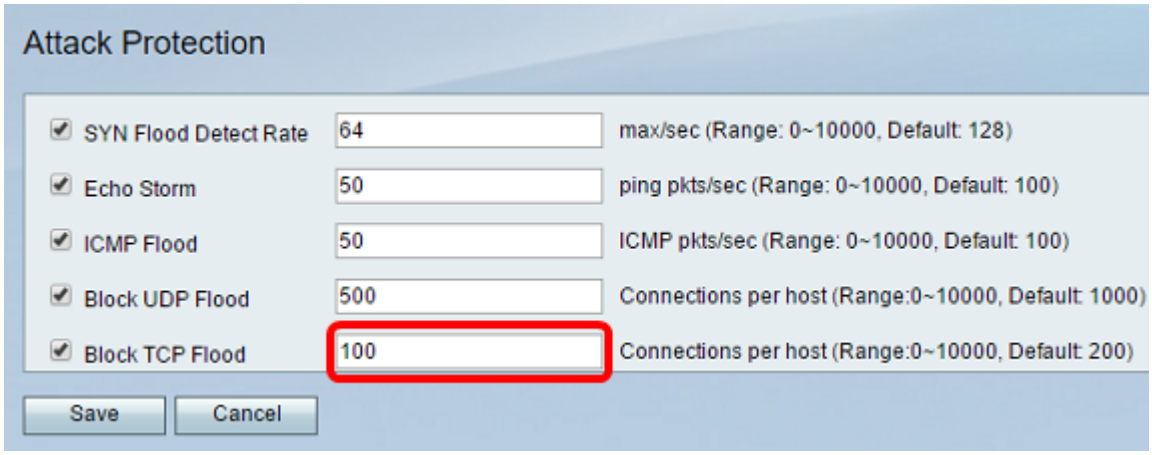
predeterminado es 1000. En este ejemplo, el valor introducido es 500, lo que lo hace más sensible.



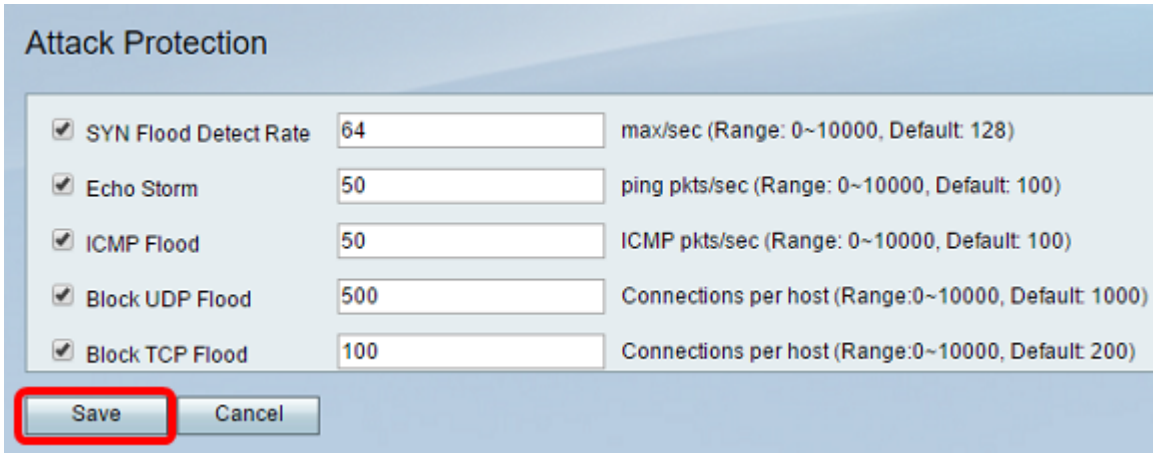
Paso 10. Verifique que la casilla de verificación Block TCP Flood (Bloquear inundación de TCP) esté marcada para descartar todos los paquetes de Protocolo de control de transmisión (TCP) no válidos. Esta opción está activada de forma predeterminada.



Paso 11. Introduzca un valor entre 0 y 10000 en el campo *Block TCP Flood* para proteger la red de un ataque de saturación SYN. El valor predeterminado es 200. En este ejemplo, se introduce 100, lo que hace que sea más sensible.



Paso 12. Click **Save**.



Ahora debería haber configurado correctamente la protección frente a ataques en el router RV132W o RV134W.

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).