

Preguntas frecuentes técnicas del TAC de Cisco sobre la vulnerabilidad de ampliación de privilegios de interfaz de usuario web del software Cisco IOS XE - CVE-2023-20198

Contenido

[Introducción](#)

[Overview](#)

[1. ¿Se ve afectado mi producto?](#)

[2. ¿Cómo puedo determinar si mi producto ejecuta Cisco IOS XE?](#)

[3. Estoy utilizando casos de uso de redirección de Identity Services Engine \(ISE\) y no puedo desactivar los servidores http/https. ¿Qué puedo hacer?](#)

[4. Utilizo el controlador de LAN inalámbrica \(WLC\) C9800 y no puedo desactivar los servidores http/http. ¿Qué puedo hacer?](#)

[5. En el aviso de seguridad se menciona que existen reglas de snort para detectar y bloquear esta vulnerabilidad. ¿Cómo confirmo que estas reglas están instaladas y funcionan en mi FTD?](#)

[6. Tengo un Cisco Unified Border Element \(CUBE\) que ejecuta Cisco IOS XE. ¿Puedo inhabilitar el servidor http/https?](#)

[7. Tengo un Cisco Unified Communications Manager Express \(CME\) que ejecuta Cisco IOS XE. ¿Puedo inhabilitar el servidor http/https?](#)

[8. Si inhabilito el servidor http/https. ¿afectará esto a mi capacidad para administrar mis dispositivos con Cisco DNA Center?](#)

[9. ¿Habrá un impacto en Smart Licensing si desactivamos el servidor HTTP/HTTPS en el dispositivo?](#)

[10. ¿Puede un agente de amenazas explotar la vulnerabilidad y crear un usuario local incluso si AAA está en su lugar?](#)

[11. ¿Cuál debería ser la respuesta "curl" si estoy usando mi router como servidor de la CA y la ACL HTTP/S ya está configurada para bloquear la IP de la máquina?](#)

[12. ¿Dónde puedo encontrar la información sobre la corrección de software o la disponibilidad de las unidades de mantenimiento de software \(SMU\)?](#)

Introducción

Este documento representa las Preguntas Frecuentes Técnicas de Cisco Technical Assistance Center para la Vulnerabilidad de Escalación de Privilegios de Interfaz de Usuario Web del Software Cisco IOS XE. Encontrará más información en el [aviso de seguridad](#) de la vulnerabilidad y en el [blog Talos de](#) Cisco.

Overview

Este documento describe las implicaciones de inhabilitar los comandos ip http server o ip http secure-server y qué otras funcionalidades se ven afectadas al hacerlo. Además, proporciona

ejemplos sobre cómo configurar las listas de acceso descritas en el aviso para limitar el acceso al WebBui en caso de que no pueda desactivar completamente las funciones.

1. ¿Se ve afectado mi producto?

Solo se ven afectados los productos que ejecutan el software Cisco IOS XE con las versiones 16.x y posteriores. Los productos Nexus, ACI, dispositivos IOS tradicionales, IOS XR, firewalls (ASA/FTD) e ISE no se ven afectados. En el caso de Identity Services Engine, puede haber otras implicaciones al deshabilitar el servidor http/https. Consulte la sección ISE.

2. ¿Cómo puedo determinar si mi producto ejecuta Cisco IOS XE?

Ejecute el comando show version desde la interfaz de línea de comandos (CLI) y verá el tipo de software como este:

```
switch#show version
```

Software Cisco IOS XE, versión 17.09.03

Cisco IOS Software [Cupertino], C9800-CL Software (C9800-CL-K9_IOSXE), versión 17.9.3, RELEASE SOFTWARE (fc6)

Asistencia técnica: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2023 by Cisco Systems, Inc.

Compilado Mar 14-Mar-23 18:12 por mcpre

Software Cisco IOS-XE, Copyright (c) 2005-2023 de Cisco Systems, Inc.

Todos los derechos reservados. Determinados componentes del software Cisco IOS-XE están bajo la licencia GNU General Public License ("GPL") versión 2.0. El código de software bajo licencia GPL Versión 2.0 es software libre que viene con ABSOLUTAMENTE NINGUNA GARANTÍA. Puede redistribuir y/o modificar dicho código GPL bajo los términos de la versión 2.0 de la GPL. Para obtener más información, consulte la documentación o el archivo "License Notice" (Aviso de licencia) que acompaña al software IOS-XE, o la URL correspondiente proporcionada en el folleto que acompaña al software IOS-XE.

Solo las versiones de software 16.x y superiores se ven afectadas por esta vulnerabilidad. Las versiones de software de ejemplo que se ven afectadas son:

16.3.5

16.12.4

17.3.5

17.6.1

17.9.4

Ejemplos de versiones de IOS XE que NO se ven afectadas:

3.17.4S

3.11.7E

15.6-1.S4

15.2-7.E7

3. Utilizo casos prácticos de redirección de Identity Services Engine (ISE) y no puedo desactivar los servidores http/https. ¿Qué puedo hacer?

Si se inhabilita el servidor ip http y el servidor ip http secure-server, se evitará que funcionen casos prácticos como los siguientes:

- Perfiles basados en el sensor de dispositivos
- Detección y redirección de estado
- Redireccionamiento de invitados
- Incorporación de BYOD
- Incorporación de MDM

En los dispositivos IOS-XE que no requieren acceso a la WebBui, se recomienda utilizar los siguientes comandos para evitar el acceso a la WebBui y, al mismo tiempo, permitir los casos de uso de redirección de ISE:

- ip http active-session-modules none
- ip http secure-active-session-modules none

Si es necesario el acceso a la WebBui, como en el caso de los controladores Catalyst 9800, el acceso a la WebBui se puede restringir mediante el uso de ACL de clase de acceso http:

<https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destin...>

Las ACL de clase de acceso http siguen permitiendo que funcionen los casos prácticos de redirección de ISE.

4. Utilizo el controlador de LAN inalámbrica (WLC) C9800 y no puedo desactivar los servidores http/http. ¿Qué puedo hacer?

A4. Al desactivar el servidor ip http y el servidor ip http secure-server se interrumpirán los siguientes casos prácticos:

- Acceso a la interfaz de usuario web del WLC. Esto es así tanto si se utiliza la interfaz de administración inalámbrica (WMI), el puerto de servicio o cualquier otra SVI para acceder a la interfaz de usuario de WebAdmin.
- El asistente de configuración de día 0 fallará.
- Autenticación Web - Acceso de Invitado si la página interna del WLC, la página de autenticación Web personalizada, la autenticación Web local, la autenticación Web central dejará de ser redirigida
- En un C9800-CL, la generación de certificados autofirmados fallará
- Acceso RESTCONF
- S3 y Cloudwatch
- Alojamiento de aplicaciones IOX en puntos de acceso inalámbricos

Para continuar utilizando estos servicios, deberá realizar los siguientes pasos:

(1) Mantenga HTTP/HTTPS habilitado

(2) Utilice una ACL para limitar el acceso al servidor web del WLC C9800, solo a las subredes/direcciones de confianza.

Se pueden encontrar detalles sobre la configuración de la lista de acceso:

<https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-17/221107-filter-traffic-destined-to-cisco-ios-xe.html>.



Nota:

1. Los WLC de AireOS no son vulnerables
2. Todos los formatos del C9800 (C9800-80, C9800-40, C9800-L, C9800-CL), incluidos Embedded Wireless on AP (EWC-AP) e Embedded Wireless on Switch (EWC-SW) son vulnerables
3. La ACL HTTP bloqueará solamente el acceso al servidor HTTP en el WLC C9800. No afectará al acceso de invitado de WebAuth si se utiliza la página interna de WLC, la página de autenticación Web personalizada, la autenticación Web local o la autenticación Web central
4. La ACL HTTP tampoco tiene impacto en el control CAPWAP ni en el tráfico de datos.
5. Asegúrese de que las redes no confiables como guest no estén permitidas en la ACL HTTP.

De manera opcional, si desea bloquear por completo el acceso de los clientes inalámbricos a la GUI de WebAdmin, asegúrese de que la opción "Gestión mediante conexión inalámbrica" está desactivada.

GUI:

Configuration > Wireless > Wireless Global

Default Mobility Domain *

mob-179mr

RF Group Name*

rfgp

Maximum Login Sessions Per User*

0

Management Via Wireless

Device Classification

AP LAG Mode

Dot15 Radio

Wireless Password Policy

None



CLI:

```
C9800(config)#no wireless mgmt-via-wireless  
C9800(config)#exit
```

5. En el aviso de seguridad se menciona que existen reglas de snort para detectar y bloquear esta vulnerabilidad. ¿Cómo confirmo que estas reglas están instaladas y funcionan en mi FTD?

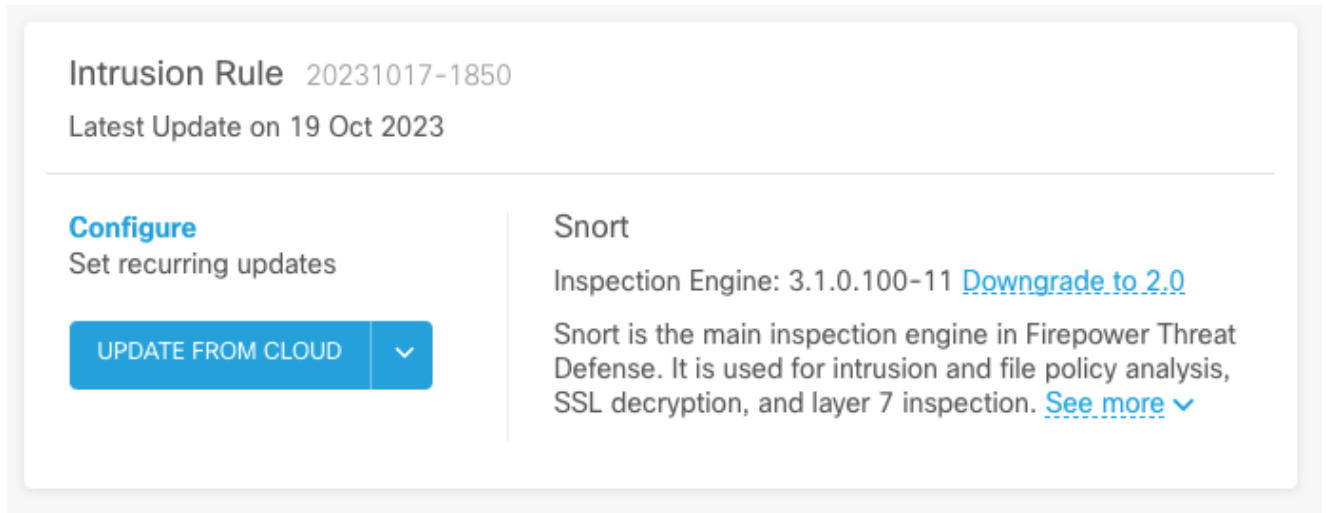
Para asegurarse de que las reglas de Snort están instaladas en su dispositivo, asegúrese de que tiene LSP 20231014-1509 o SRU-2023-10-14-001. Comprobando si esta instalación es diferente en los dispositivos gestionados por FDM y FMC:

a. Asegúrese de que las reglas estén instaladas:

FDM

1. Vaya a Dispositivo > Actualizaciones (Ver configuración)

2. Verifique la regla de intrusión y asegúrese de que sea 20231014-1509 o posterior



Intrusion Rule 20231017-1850
Latest Update on 19 Oct 2023

Configure
Set recurring updates

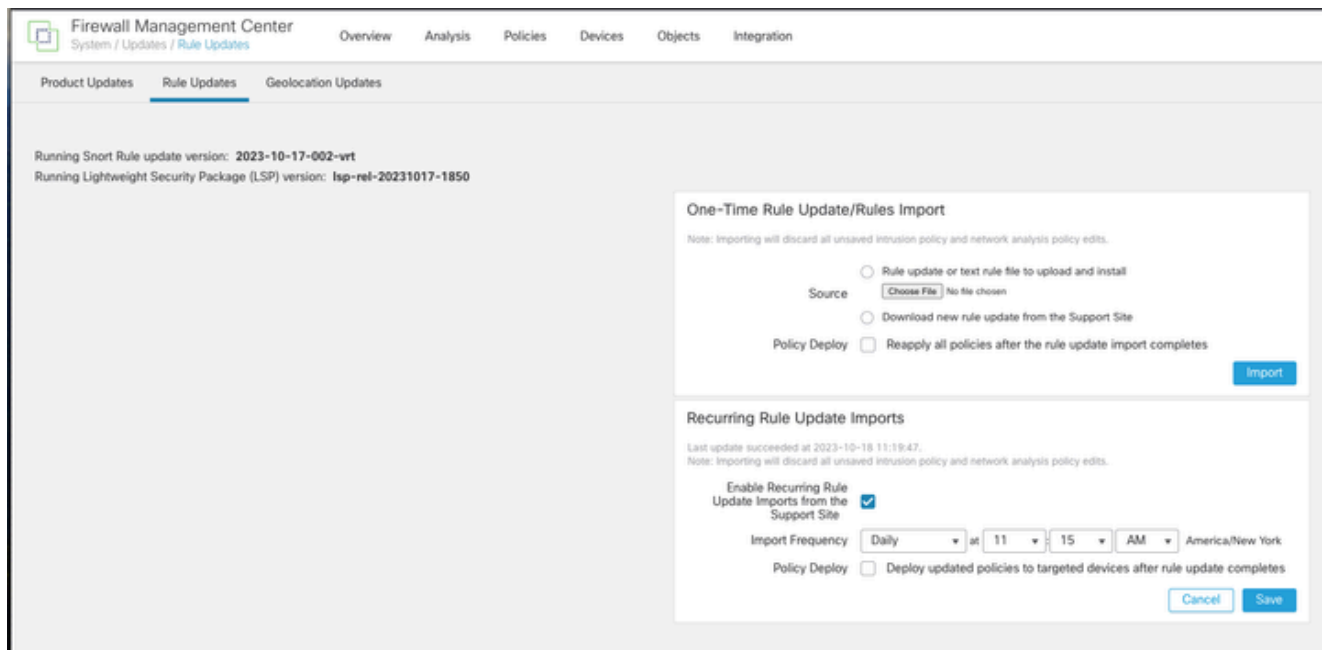
UPDATE FROM CLOUD ▼

Snort
Inspection Engine: 3.1.0.100-11 [Downgrade to 2.0](#)

Snort is the main inspection engine in Firepower Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection. [See more](#) ▼

FMC

1. Vaya a Sistema > Actualizaciones > Actualizaciones de reglas
2. Compruebe la actualización de la regla de Snort en ejecución y el paquete ligero de seguridad (LSP) y asegúrese de que ejecutan LSP 20231014-1509 o SRU-2023-10-14-001 o superior.



Firewall Management Center
System / Updates / Rule Updates

Overview Analysis Policies Devices Objects Integration

Product Updates **Rule Updates** Geolocation Updates

Running Snort Rule update version: 2023-10-17-002-vrt
Running Lightweight Security Package (LSP) version: lsp-rel-20231017-1850

One-Time Rule Update/Rules Import
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Source Rule update or text rule file to upload and install
 Choose File | No file chosen

Download new rule update from the Support Site

Policy Deploy Reapply all policies after the rule update import completes **Import**

Recurring Rule Update Imports
Last update succeeded at 2023-10-18 11:19:47.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site

Import Frequency: at :

Policy Deploy Deploy updated policies to targeted devices after rule update completes **Cancel** **Save**

b. Asegúrese de que las reglas estén habilitadas en su política de intrusiones

Si sus políticas de intrusión se basan en las políticas integradas de Talos (conectividad sobre seguridad, seguridad sobre conectividad, seguridad equilibrada y conectividad), estas reglas se activarán y se establecerán para descartarse de forma predeterminada.

Si no basa su política en una de las políticas integradas de Talos. Tendrá que activar la configuración manual de las acciones de regla para estas reglas en la directiva de intrusiones. Para ello, revise la siguiente documentación:

Snort 3: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/snort/720/snort3-configuration-guide-v72/tuning-intrusion-policies.html#ID-2237-00000683> snort3

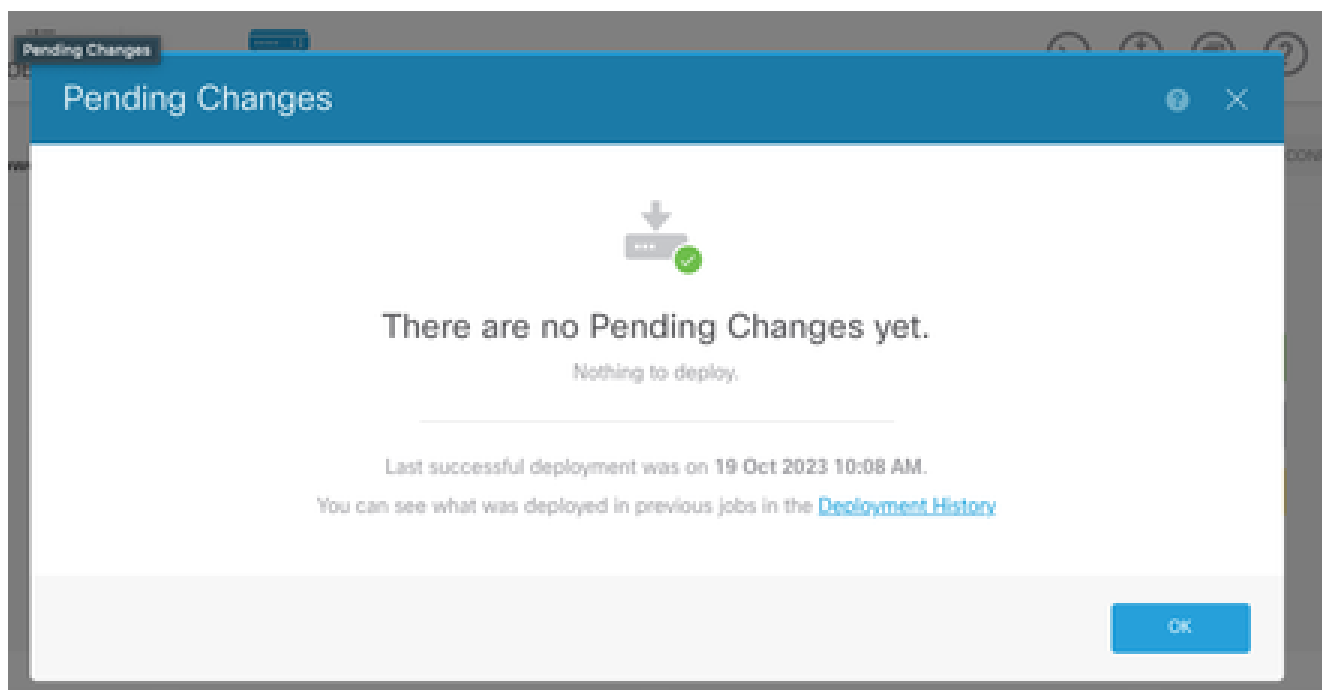
Snort 2: <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/intrusion-tuning-rules.html#ID-2237-00000683>

c. Asegúrese de que sus políticas IPS se han implementado en sus dispositivos FTD:

FDM

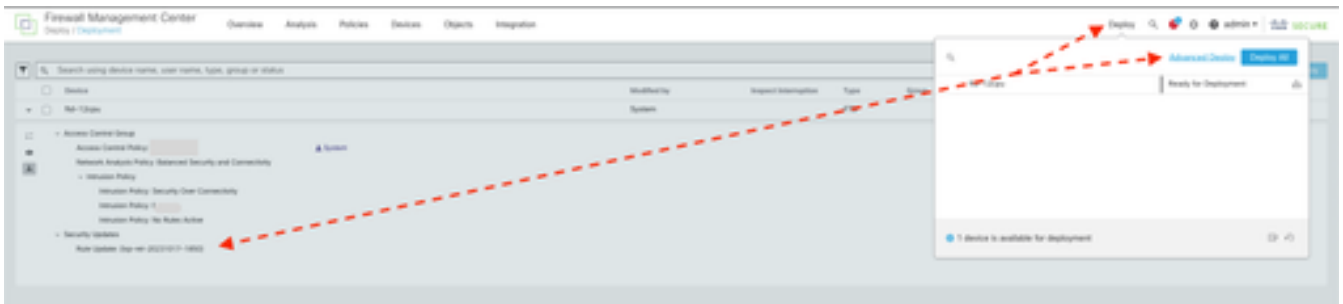


1. Haga clic en el icono de despliegue
2. Asegúrese de que no haya cambios pendientes relacionados con la SRU/LSP



FMC

1. Haga clic en Deploy > Advanced Deploy
2. Asegúrese de que no haya implementaciones pendientes relacionadas con SRU/LSP



6. Tengo un Cisco Unified Border Element (CUBE) que ejecuta Cisco IOS XE. ¿Puedo inhabilitar el servidor http/https?

La mayoría de las implementaciones de CUBE no utilizan el servicio HTTP/HTTPS incluido con IOS XE y su desactivación no afectará a la funcionalidad. Si utiliza la función de [bifurcación de medios basada en XMF](#), deberá configurar una lista de acceso y restringir el acceso al servicio HTTP para incluir únicamente hosts de confianza (CUCM/clientes de terceros). Puede ver un ejemplo de configuración [aquí](#).

7. Tengo un Cisco Unified Communications Manager Express (CME) que ejecuta Cisco IOS XE. ¿Puedo inhabilitar el servidor http/https?

La solución CME utiliza servicios HTTP para el directorio de usuarios y servicios adicionales para los teléfonos IP registrados. Si se desactiva el servicio, esta funcionalidad fallará. Deberá configurar una lista de acceso y restringir el acceso al servicio HTTP para incluir solamente la subred de la red del teléfono IP. Puede ver un ejemplo de configuración [aquí](#).

8. Si inhabilito el servidor http/https, ¿afectará esto a mi capacidad para administrar mis dispositivos con Cisco DNA Center?

La desactivación del servidor HTTP/HTTPS no afectará a las funciones de gestión de dispositivos ni a la disponibilidad de los dispositivos gestionados con Cisco DNA Center, incluidos los de los entornos SDA (acceso definido por software). La desactivación del servidor HTTP/HTTPS tendrá un impacto en la función de alojamiento de aplicaciones y en cualquier aplicación de terceros que se utilice en el entorno de alojamiento de aplicaciones de Cisco DNA Center. Estas aplicaciones de terceros pueden depender del servidor HTTP/HTTPS para la comunicación y la funcionalidad.

9. ¿Tendrá algún impacto Smart Licensing si desactivamos el

servidor HTTP/HTTPS en el dispositivo?

En general, Smart Licensing utiliza la funcionalidad de cliente HTTPS, por lo que la desactivación de la función de servidor HTTP(S) no afecta a las operaciones de Smart Licensing. La única situación en la que la comunicación de licencias inteligentes se vería afectada es cuando la aplicación externa CSLU o SSM en las instalaciones se está utilizando y configurando con RESTCONF para recuperar informes RUM de los dispositivos.

10. ¿Puede un agente de amenazas aprovechar la vulnerabilidad y crear un usuario local incluso si AAA ya existe?

Sí, creemos que un agente de amenazas puede aprovechar esta vulnerabilidad para crear un usuario local independientemente del método de autenticación que utilice. Tenga en cuenta que las credenciales serán locales para el dispositivo explotado y no para el sistema AAA.

11. ¿Cuál debería ser la respuesta "curl" si estoy usando mi router como servidor de la CA y la ACL HTTP/S ya está configurada para bloquear la IP de la máquina?

La respuesta 'curl' está prohibida en 403 como se muestra a continuación:

```
(base) desktop ~ % curl http://<device ip>
<html>
<head><title>403 Prohibido</title></head>
<body bgcolor="white">
<center><h1>403 Prohibido</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

12. ¿Dónde puedo encontrar la información sobre la corrección de software o la disponibilidad de las unidades de mantenimiento de software (SMU)?

Para obtener más información, visite la página [Disponibilidad de corrección de software para la vulnerabilidad de escalación de privilegios de interfaz de usuario web del software Cisco IOS XE.](#)

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).