

# Configuración de la propagación de TrustSec SGT SXP en SD-WAN

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Integración de Cisco TrustSec](#)

[Métodos de propagación de SGT](#)

[Propagación de SGT con SXP](#)

[Habilitar la propagación de SGT SXP y descargar políticas SGACL](#)

[Paso 1. Configure los Parámetros de Radius](#)

[Paso 2. Configure los Parámetros SXP](#)

[Verificación](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe la configuración del método de propagación del protocolo de intercambio de etiquetas de grupos de seguridad (SXP) en redes de área extensa definidas por software (SD-WAN).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) Cisco Catalyst
- Fabric de acceso definido por software (SD-Access)
- Cisco Identity Service Engine (ISE)

### Componentes Utilizados

La información de este documento se basa en:

- Cisco IOS® XE Catalyst SD-WAN Edges versión 17.9.5a
- Cisco Catalyst SD-WAN Manager versión 20.12.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

### Integración de Cisco TrustSec

La propagación de SGT con la integración de Cisco TrustSec es compatible con Cisco IOS® XE Catalyst SD-WAN versión 17.3.1a y posteriores. Esta función permite que los dispositivos periféricos SD-WAN Catalyst de Cisco IOS® XE propaguen etiquetas en línea de Security Group Tag (SGT) generadas por switches habilitados para Cisco TrustSec en las sucursales a otros dispositivos periféricos de la red SD-WAN de Cisco Catalyst.

Conceptos básicos de Cisco TrustSec:

- Enlaces SGT: Asociación entre IP y SGT, todos los enlaces tienen la configuración más común y aprenden directamente de Cisco ISE.
- Propagación de SGT: Los métodos de propagación se utilizan para propagar estas SGT entre saltos de red.
- Políticas SGTACLs: Conjunto de reglas que especifican los privilegios de un origen de tráfico dentro de una red de confianza.
- Aplicación de SGT: Dónde se aplican las políticas, en función de la política de SGT.

### Métodos de propagación de SGT

Los métodos de propagación de SGT son:

- Etiquetado en línea de propagación de SGT
- Propagación de SGT SXP

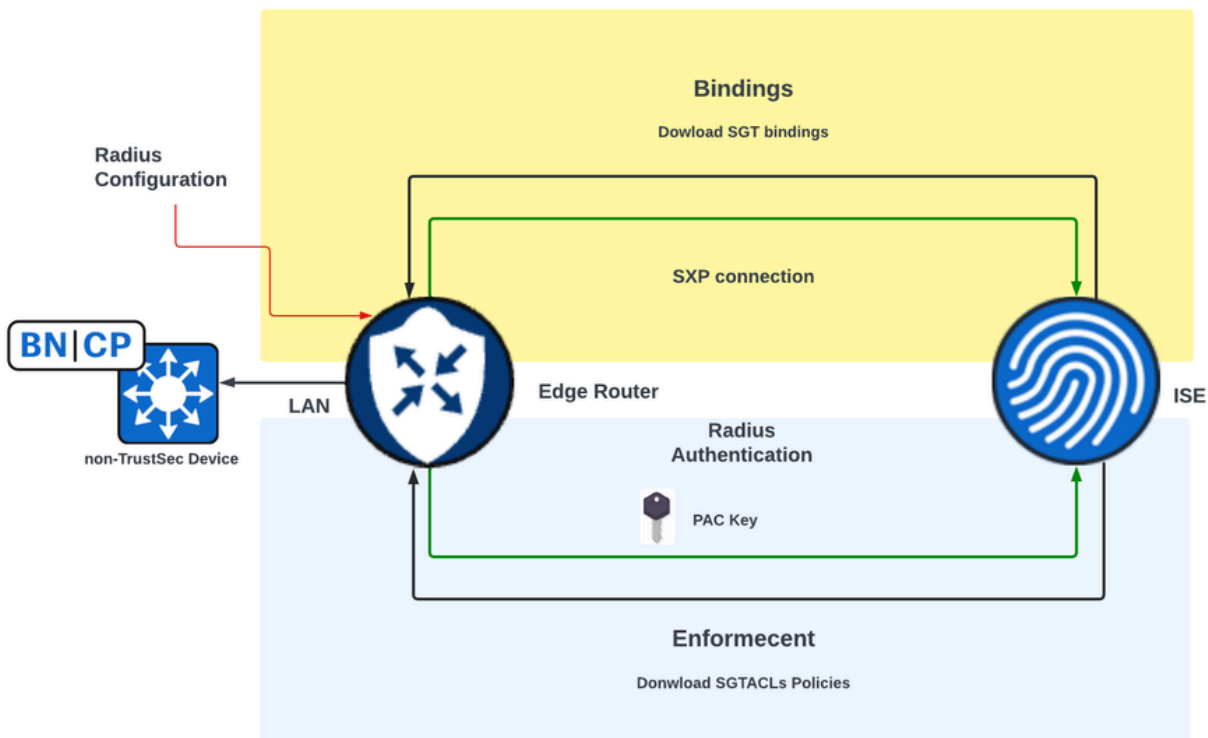
### Propagación de SGT con SXP

Para la propagación del etiquetado en línea, las sucursales deben estar equipadas con switches habilitados para Cisco TrustSec que puedan gestionar el etiquetado en línea de SGT (dispositivos Cisco TrustSec). Si el hardware no admite el etiquetado en línea, la propagación de SGT utiliza el protocolo de intercambio de etiquetas de grupos de seguridad (SXP) para propagar SGT por los dispositivos de red.


Cisco ISE permite crear un enlace de IP a SGT (IP-SGT dinámico) y, a continuación, descarga el enlace de IP a SGT mediante SXP en un dispositivo Catalyst SD-WAN de Cisco IOS® XE para la propagación de SGT a través de la red Cisco Catalyst SD-WAN. Además, las políticas para el tráfico SGT en la salida SD-WAN se aplican descargando políticas SGACL desde ISE.


Ejemplo:

- El switch de Cisco (nodo de borde) no admite el etiquetado en línea (dispositivo que no es TrustSec).
- Cisco ISE permite descargar enlaces IP-SGT a través de una conexión SXP a un dispositivo Catalyst SD-WAN Cisco IOS® XE (router de extremo).
- Cisco ISE permite descargar políticas SGACL a través de la integración Radius y la clave PAC en un Dispositivo Cisco IOS® XE Catalyst SD-WAN (router de extremo).



Requisitos para habilitar la propagación de SXP y descargar políticas SGACL en dispositivos periféricos SD-WAN

 Nota: Las políticas SGACL no se aplican en el tráfico de entrada, solo en el tráfico de salida en una red Cisco Catalyst SD-WAN.

 Nota: La función Cisco TrustSec no es compatible con más de 24 000 políticas SGT en modo de controlador.

## Habilitar la propagación de SGT SXP y descargar políticas SGACL

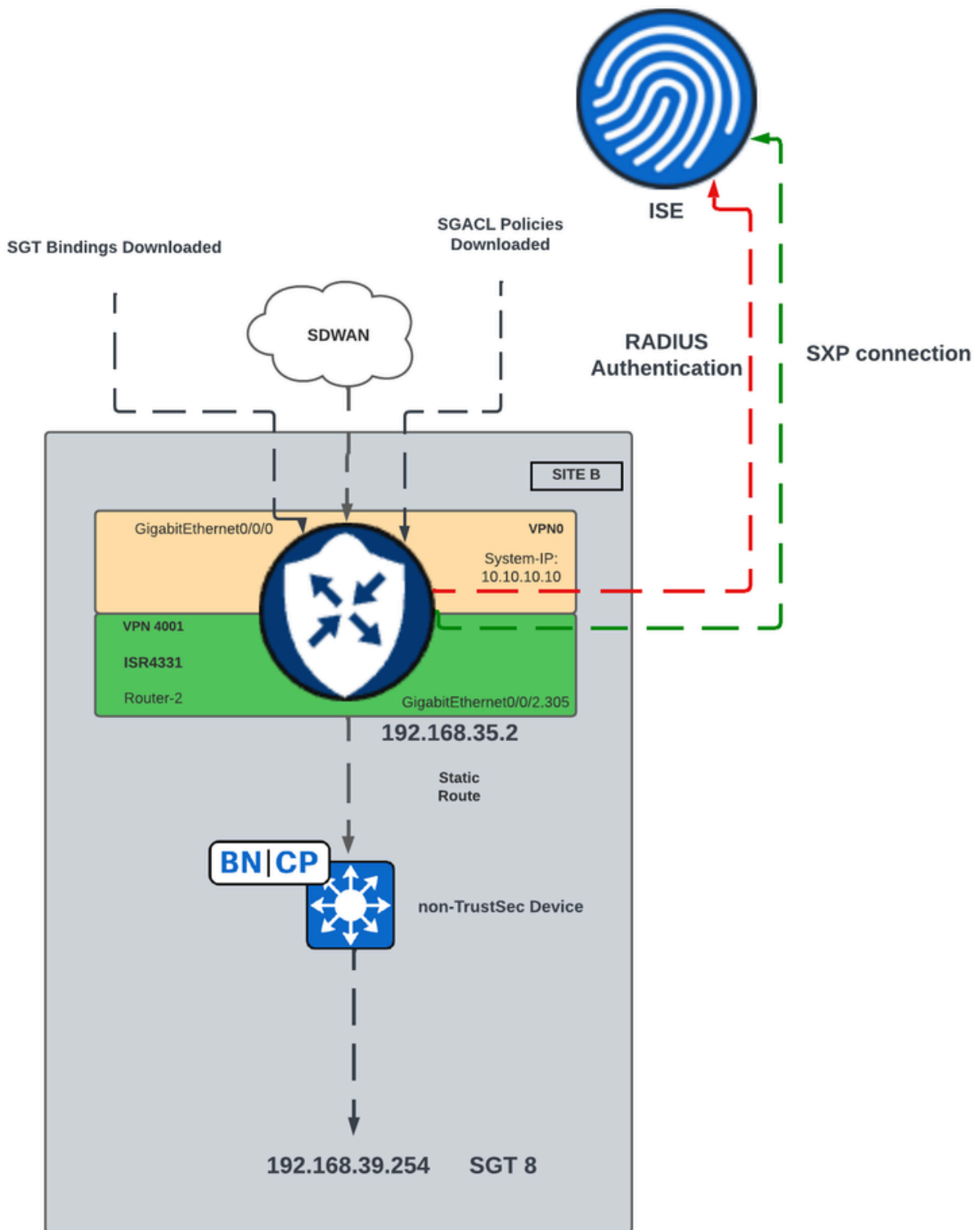


Diagrama de red para la propagación de SGT SXP en SD-WAN

## Paso 1. Configure los Parámetros de Radius

- Inicie sesión en la GUI de Cisco Catalyst SD-WAN Manager.
- Vaya a Configuration > Templates > Feature Template > Cisco AAA. Haga clic en RADIUS

SERVER.

- Configure los parámetros RADIUS SERVER y Key.

Feature Template > Cisco AAA > AAARadius

New RADIUS Server

Address



10.4.113.0

Authentication Port



1812

Accounting Port



1813

Timeout



5

Retransmit Count



3

Key Type



Key

PAC Key

Key



\*\*\*\*\*

Configuración del servidor de RADIUS

- Ingrese los valores para configurar los parámetros del Grupo Radius.

▼ RADIUS

RADIUS SERVER   **RADIUS GROUP**   RADIUS COA   TRUSTSEC

[New RADIUS Group](#)

VPN ID

Source Interface

Radius Server

Configuración de Grupo RADIUS

- Ingrese los valores para configurar los parámetros de Radius COA.

▼ RADIUS

RADIUS SERVER   RADIUS GROUP   **RADIUS COA**   TRUSTSEC

Domain Stripping  Yes  No  Right to Left

Authentication Type  Yes  All  Session Key

Port


Server Key Password

[New RADIUS CoA](#)

Client IP

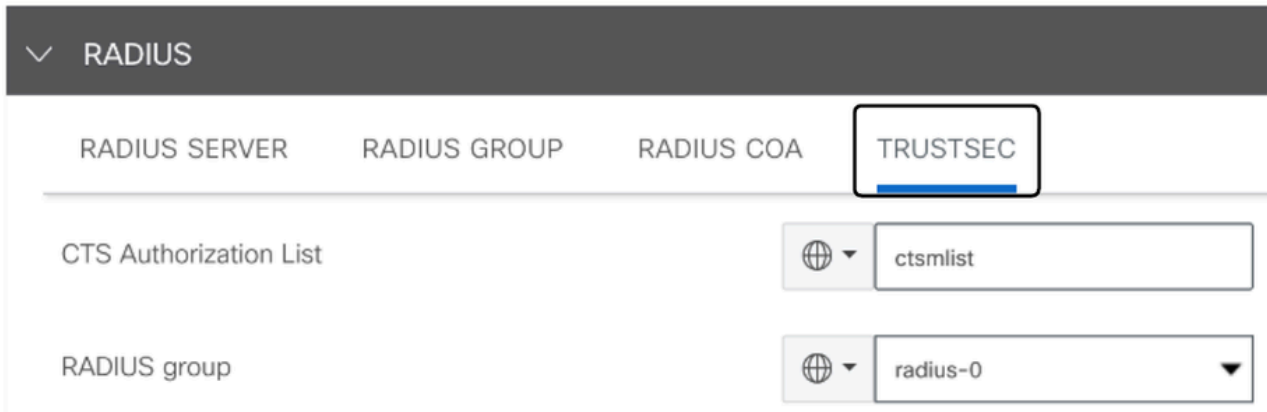
VPN ID

Server Key Password

 Nota: Si Radius COA no está configurado, el router SD-WAN no puede descargar las políticas SGACL automáticamente. Después de crear o modificar una política SGACL desde ISE, se utiliza el comando `cts refresh policy` para descargar las políticas.

- Navegue hasta la sección TRUSTSEC e ingrese los valores.


[Feature Template](#) > [Cisco AAA](#) > [AAARadius](#)




Feature Template > Cisco AAA > AAARadius

▼ RADIUS

RADIUS SERVER    RADIUS GROUP    RADIUS COA    **TRUSTSEC**

CTS Authorization List     ▼    ctsmlist

RADIUS group     ▼    radius-0 ▼

Configuración de TRUSTSEC

- Adjunte la plantilla de función Cisco AAA a la plantilla de dispositivo.

## Paso 2. Configure los Parámetros SXP

- Vaya a Configuration > Templates > Feature Template > TrustSec.
- Configure las credenciales CTS y asigne un enlace SGT a las interfaces de dispositivo.

GLOBAL

Device SGT	<input type="text" value="2"/>
Credentials ID	<input type="text" value="FLM2206W092"/> ⓘ
Credentials Password	<input type="password" value="....."/>
Enable Enforcement	<input checked="" type="radio"/> On <input type="radio"/> Off

Plantilla de función TrustSec

- Navegue hasta la sección SXP Default e ingrese los valores para configurar los parámetros SXP Default.

SXP DEFAULT

Enable SXP	<input checked="" type="radio"/> On <input type="radio"/> Off
Source IP	<input type="text" value="192.168.35.2"/>
Password	<input type="password" value="....."/>

Configuración predeterminada de SXP

- Navegue hasta SXP Connection y configure los parámetros de SXP Connection, luego haga clic en Save.





## ✓ SXP CONNECTION

New Connection

Peer IP	Source IP	Preshared Key	Mode	Mode Type	Minimum Hold Time	Action
10.88.244.146	192.168.35.2	Password	Local	Listener	0	 

Configuración de la conexión SXP

 Nota: Cisco ISE tiene un límite en el número de sesiones SXP que puede gestionar. Por lo tanto, como alternativa, se podría utilizar un reflector SXP para escalar horizontalmente la red.

 Nota: Se recomienda utilizar un reflector SXP para establecer un par SXP con los dispositivos Catalyst SD-WAN de Cisco IOS® XE.

- Vaya a Configuration > Templates > Device Template > Additional Templates > TrustSec.
- Seleccione la plantilla de la función TrustSec creada anteriormente y haga clic en Guardar.

### Additional Templates

AppQoE	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ...
Cisco Banner	Choose...
Cisco SNMP	Choose...
ThousandEyes Agent	Choose...
<b>TrustSec</b>	ISR433_SXPTrustSec

Sección Plantillas adicionales

## Verificación

Ejecute el comando `show cts sxp connections vrf (service vrf)` para mostrar la información de conexiones de Cisco TrustSec SXP.

```
<#root>
```

```
#show
```

```
cts
```

```
sxp
```

```
connections
```

```
vrf
```

```
4001
```

```
SXP : Enabled
```

```
Highest Version Supported: 5
```

```
Default Password : Set
```

```
Default Key-Chain: Not Set
```

```
Default Key-Chain Name: Not Applicable
```

```
Default Source IP: 192.168.35.2
```

```
Connection retry open period: 120 secs
```

```
Reconcile period: 120 secs
```

```
Retry open timer is not running
```

```
Peer-Sequence traverse limit for export: Not Set
```

```
Peer-Sequence traverse limit for import: Not Set
```

```
-----
```

```
Peer IP : 10.88.244.146
```

```
Source IP : 192.168.35.2
```

```
Conn status : On
```

```
Conn version : 4
```

```
Conn capability : IPv4-IPv6-Subnet
```

```
Conn hold time : 120 seconds
```

```
Local mode : SXP Listener
```

```
Connection inst# : 1
```

```
TCP conn fd : 1
```

```
TCP conn password: default SXP password
```

```
Hold timer is running
```

```
Total num of SXP Connections = 1
```

Ejecute el comando `show cts role-based sgt-map` para mostrar el mapa SGT global de Cisco TrustSec entre los enlaces de dirección IP y SGT.

```
<#root>
```

```
#
```

```
show
```

```
cts
```

```
  role-based
```

```
sgt
```

```
-map
```

```
vrf
```

```
  4001 all
```

#### Active IPv4-SGT Bindings Information

IP Address	SGT	Source
------------	-----	--------

=====

192.168.1.2	2	INTERNAL
-------------	---	----------

192.168.35.2	2	INTERNAL
--------------	---	----------

192.168.39.254	8	SXP	<<< Bindings learned through SXP for the host connected in the
----------------	---	-----	--

#### IP-SGT Active Bindings Summary

=====

Total number of CLI bindings = 0

Total number of SXP bindings = 1

Total number of INTERNAL bindings = 2

Total number of active bindings = 3

Ejecute el comando `show cts environment-data` para mostrar los datos globales del entorno Cisco TrustSec.

```
<#root>
```

```
#show
```

```
cts
```

```
  environment-data
```

#### CTS Environment Data

=====

Current state = COMPLETE

Last status = Successful

Service Info Table:

Local Device SGT:

SGT tag = 2-01:TrustSec\_Devices

Server List Info:

Installed list: CTSServerList1-0002, 1 server(s):

Server: 10.88.244.146, port 1812, A-ID B546BF54CA5778A0734C8925EECE2215

Status = ALIVE

auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

Security Group Name Table:

0-00:Unknown

2-01:TrustSec\_Devices

3-00:Network\_Services

4-00:Employees

5-00:Contractors

6-00:Guests

7-00:Production\_Users

8-02:Developers

<<<<< Security Group assigned to the host connected in the LAN side (SGT 8)

9-00:Auditors

10-00:Point\_of\_Sale\_Systems

11-00:Production\_Servers

12-00:Development\_Servers

13-00:Test\_Servers

14-00:PCI\_Servers

15-01:BYOD

Environment Data Lifetime = 86400 secs

Ejecute el comando `show cts pacs` para mostrar la PAC de Cisco TrustSec suministrada.

```
<#root>
```

```
#show cts pacs
```

```
AID: B546BF54CA5778A0734C8925EECE2215
```

```
PAC-Info:
```

```
PAC-type = Cisco Trustsec
```

```
AID: B546BF54CA5778A0734C8925EECE2215
```

```
I-ID: FLM2206W092
```

```
A-ID-Info: Identity Services Engine
```

```
Credential Lifetime: 22:24:54 UTC Tue Dec 17 2024
```

```
PAC-Opaque: 000200B80003000100040010B546BF54CA5778A0734C8925EECE22150006009C00030100BE30CE655A7649A5CED8
```

Ejecute el comando `show cts role-based permissions` para mostrar las políticas SGACL.

```
<#root>
```

```
#show
```

```
cts
```

```
role-based permissions
```

```
IPv4 Role-based permissions default:
```

```
Permit IP-00
```

```
IPv4 Role-based permissions from group 5:Contractors to group 2:TrustSec_Devices:
```

```
Deny IP-00
```

```
IPv4 Role-based permissions from group 5:Contractors to group 8:Developers:
```

```
DNATELNET-00
```

```
IPv4 Role-based permissions from group 5:Contractors to group 15:BYOD:
```

```
Deny IP-00
```

Ejecute el comando `show cts rbacl (SGACLName)` para mostrar la configuración de la lista de control de acceso (SGACL).

```
<#root>
```

```
#show
```

```
cts
```

```
rbacl
```

```
DNATELNET
```

```
CTS RBACL Policy
```

```
=====
```

```
RBACL IP Version Supported: IPv4 & IPv6
```

```
name =
```

```
DNATELNET-00
```

```
IP protocol version = IPV4, IPV6
```

```
refcnt = 2
```

```
flag = 0xC1000000
```

```
stale = FALSE
```

```
RBACL ACEs:
```

```
deny
```

```
tcp
```

```
dst
```

```
eq 23 log
```

```
<<<<< SGACL action
```

```
permit
```

```
ip
```

## Información Relacionada

- [Guía de configuración de seguridad de Cisco Catalyst SD-WAN](#)
- [Guía de configuración de Cisco TrustSec](#)

## 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).