Ejemplo de Configuración del Cliente VPN sobre LAN Inalámbrica con WLC

Contenido

Introducción

Este documento presenta el concepto de red privada virtual (VPN) en un entorno inalámbrico. El documento explica las configuraciones involucradas en la implementación de un túnel VPN entre un cliente inalámbrico y un servidor VPN a través de un Controlador de LAN Inalámbrica (WLC).

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de WLCs y cómo configurar los parámetros básicos del WLC
- Conocimiento de los conceptos de acceso Wi-Fi protegido (WPA)
- Conocimiento básico de VPN y sus tipos
- Conocimiento de IPsec

- Conocimiento básico de los algoritmos de cifrado, autenticación y hash disponibles

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco 2006 que ejecuta la versión 4.0.179.8
- Punto de acceso ligero (LAP) Cisco serie 1000
- Cisco 3640 que ejecuta Cisco IOS® Software Release 12.4(8)
- Cliente Cisco VPN versión 4.8

Nota: Este documento utiliza un router 3640 como servidor VPN. Para admitir funciones de seguridad más avanzadas, también puede utilizar un servidor VPN dedicado.

Nota: Para que un router actúe como servidor VPN, necesita ejecutar un conjunto de funciones que admita IPSec básico.

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Una VPN es una red de datos privada que se utiliza para transmitir de forma segura los datos dentro de una red privada a través de la infraestructura pública de telecomunicaciones, como Internet. Esta VPN mantiene la privacidad de los datos a través del uso de un protocolo de tunelización y procedimientos de seguridad.

VPN de acceso remoto

Una configuración VPN de acceso remoto se utiliza para permitir que los clientes de software VPN, como los usuarios móviles, accedan de forma segura a los recursos de red centralizados que residen detrás de un servidor VPN. En la terminología de Cisco, estos clientes y servidores VPN también se denominan servidor Easy VPN de Cisco y dispositivo remoto Easy VPN de Cisco.

Un dispositivo remoto Cisco Easy VPN puede ser routers Cisco IOS, dispositivos de seguridad Cisco PIX, clientes de hardware Cisco VPN 3002 y Cisco VPN Client. Se utilizan para recibir

políticas de seguridad en una conexión de túnel VPN desde un servidor Cisco Easy VPN. Esto minimiza los requisitos de configuración en la ubicación remota. Cisco VPN Client es un cliente de software que se puede instalar en PC, portátiles, etc.

Un servidor Cisco Easy VPN puede ser routers Cisco IOS, dispositivos de seguridad Cisco PIX y concentradores Cisco VPN 3000.

Este documento utiliza el software Cisco VPN Client que se ejecuta en un equipo portátil como VPN Client y Cisco 3640 IOS Router como el servidor VPN. El documento utiliza el estándar IPsec para establecer un túnel VPN entre un cliente y un servidor.

IPsec

IPSec es un marco de estándares abiertos desarrollado por el Grupo de trabajo de ingeniería de Internet (IETF). IPSec proporciona seguridad para la transmisión de información confidencial a través de redes no protegidas como Internet.

IPSec proporciona cifrado de datos de red en el nivel de paquete IP, lo que ofrece una solución de seguridad sólida basada en estándares. La tarea principal de IPSec es permitir el intercambio de información privada a través de una conexión insegura. IPSec utiliza el cifrado para proteger la información de la interceptación o la intercepción. Sin embargo, para utilizar el cifrado de forma eficaz, ambas partes deben compartir un secreto que se utilice tanto para el cifrado como para el descifrado de la información.

IPSec funciona en dos fases para permitir el intercambio confidencial de un secreto compartido:

- Fase 1: controla la negociación de los parámetros de seguridad necesarios para establecer un canal seguro entre dos pares IPsec. La fase 1 se suele implementar a través del protocolo de intercambio de claves de Internet (IKE). Si el peer IPSec remoto no puede realizar IKE, puede utilizar la configuración manual con claves previamente compartidas para completar la Fase 1.
- Fase 2: utiliza el túnel seguro establecido en la Fase 1 para intercambiar los parámetros de seguridad necesarios para transmitir realmente los datos del usuario. Los túneles seguros utilizados en ambas fases de IPsec se basan en asociaciones de seguridad (SA) utilizadas en cada punto final de IPsec. Las SA describen los parámetros de seguridad, como el tipo de autenticación y cifrado que ambos extremos aceptan utilizar.

Los parámetros de seguridad intercambiados en la fase 2 se utilizan para crear un túnel IPsec que, a su vez, se utiliza para la transferencia de datos entre el cliente VPN y el servidor.

Consulte Configuración de IPSec para obtener más información sobre IPSec y su configuración.

Una vez que se establece un túnel VPN entre el cliente VPN y el servidor, las políticas de seguridad definidas en el servidor VPN se envían al cliente. Esto minimiza los requisitos de configuración del cliente.

Nota: Utilice la herramienta de búsqueda de comandos (solo para clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utilizan estas configuraciones:

- Dirección IP de la interfaz de administración del WLC-172.16.1.10/16
- Dirección IP de la interfaz del administrador de AP del WLC-172.16.1.11/16
- Gateway predeterminado: 172.16.1.20/16

  Nota: En una red activa, este gateway predeterminado debe apuntar a la interfaz entrante del router inmediato que conecta el WLC al resto de la red y/o a Internet.

- Dirección IP del servidor VPN s3/0-192.168.1.11/24

  Nota: Esta dirección IP debe señalar a la interfaz que termina el túnel VPN en el lado del servidor VPN. En este ejemplo, s3/0 es la interfaz que termina el túnel VPN en el servidor VPN.

- El segmento LAN en el servidor VPN utiliza el rango de direcciones IP de 10.0.0.0/8.

Configurar

En una arquitectura centralizada WLAN, para permitir que un cliente VPN inalámbrico como un portátil establezca un túnel VPN con un servidor VPN, es necesario que el cliente se asocie con un Lightweight Access Point (LAP) que a su vez necesita ser registrado con un WLC. Este documento tiene el LAP como ya está registrado con el WLC usando el proceso de detección de broadcast de subred local explicado en Registro ligero del AP (LAP) a un controlador de LAN inalámbrico (WLC).

El siguiente paso es configurar el WLC para VPN.

Terminación y paso a través de VPN

Con los WLC de Cisco serie 4000 anteriores a la versión 4, se admite una función llamada terminación de VPN IPsec (compatibilidad con IPsec). Esta función permite que estos controladores finalicen las sesiones de VPN Client directamente en el controlador. En resumen, esta función permite que el propio controlador actúe como un servidor VPN. Pero esto requiere que se instale un módulo de hardware de terminación de VPN independiente en el controlador.

Esta compatibilidad con VPN IPsec no está disponible en:

- WLC de las Cisco 2000 Series
- Cualquier WLC que ejecute la versión 4.0 o posterior

Por lo tanto, la única función de VPN compatible con las versiones posteriores a la 4.0 es el paso a través de VPN. Esta función también se soporta en el WLC de la serie 2000 de Cisco.

El paso a través de VPN es una función que permite a un cliente establecer un túnel sólo con un servidor VPN específico. Por lo tanto, si necesita acceder de forma segura al servidor VPN configurado, así como a otro servidor VPN o a Internet, esto no es posible con el paso a través de VPN habilitado en el controlador. Bajo tales requisitos, debe inhabilitar el paso a través de VPN. Sin embargo, el WLC se puede configurar para actuar como passthrough para alcanzar los gateways múltiples de VPN cuando se crea una ACL apropiada y se aplica a la WLAN correspondiente. Por lo tanto, en estos casos en los que desee alcanzar varios gateways VPN para obtener redundancia, desactive el paso a través de VPN y cree una ACL que permita el acceso a los gateways VPN y aplique la ACL a la WLAN.

Configuración del WLC para el paso a través de VPN

Complete estos pasos para configurar el paso a través de VPN.

1. Desde el WLC GUI, haga clic en WLAN para ir a la página WLANs.
2. Haga clic en Nuevo para crear un nuevo WLAN.
3. En este ejemplo, el SSID de WLAN se denomina vpnclient. Haga clic en Apply (Aplicar).
4. Configure el SSID de vpnclient con seguridad de Capa 2. Esta opción es opcional.

   Este ejemplo utiliza WPA1+WPA2 como tipo de seguridad.
5. Configure el tipo de administración de la política WPA y la clave de autenticación que se va a utilizar.

   Este ejemplo utiliza Pre-Shared Key (PSK) para la administración de claves de autenticación. Una vez seleccionada PSK, seleccione ASCII como formato PSK y escriba el valor PSK. Este valor debe ser el mismo en la configuración SSID del cliente inalámbrico para que los clientes que pertenecen a este SSID se asocien con esta WLAN.
6. Seleccione VPN Pass-through como Layer 3 Security (Seguridad de capa 3). Este es el ejemplo.
7. Una vez seleccionado el paso a través de VPN como seguridad de capa 3, agregue la dirección de la puerta de enlace VPN como se muestra en este ejemplo.

   Esta dirección de gateway debe ser la dirección IP de la interfaz que termina el túnel VPN en el lado del servidor. En este ejemplo, la dirección IP de la interfaz s3/0 (192.168.1.11/24) en el servidor VPN es la dirección de gateway que se va a configurar.
8. Haga clic en Apply (Aplicar). La WLAN llamada vpnclient ahora está configurada para el paso a través de VPN.

Configuración del servidor VPN

Esta configuración muestra el router Cisco 3640 como el servidor VPN.

Nota: Para mayor simplicidad, esta configuración utiliza routing estático para mantener la disponibilidad de IP entre los terminales. Puede utilizar cualquier protocolo de enrutamiento dinámico, como el Protocolo de información de enrutamiento (RIP), Abrir primero la ruta de acceso más corta (OSPF), etc., para mantener la accesibilidad.

Nota: El túnel no se establece si no hay disponibilidad de IP entre el cliente y el servidor.

Nota: Este documento asume que el usuario es consciente de cómo habilitar el ruteo dinámico en la red.

```
<#root>

vpnrouter#

show running-config


Building configuration...

Current configuration : 1623 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!

aaa new-model

!
!

aaa authorization network employee local

!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1

!--- Create an Internet Security Association and Key Management !--- Protocol (ISAKMP) policy for Phas

hash md5

!--- Choose the hash algorithm to be md5.

authentication pre-share

!--- The authentication method selected is pre-shared.

group 2

!--- With the
group
 command, you can declare what size modulus to !--- use for Diffie-Hellman calculation. Group 1 is 768



crypto isakmp client configuration group employee
 key cisco123
 pool mypool
!

!--- Create the Phase 2 policy for actual data encryption.

crypto ipsec transform-set myset esp-3des esp-md5-hmac

!--- Create a dynamic map and apply the transform set that was created. !--- Set reverse-route for the

crypto dynamic-map mymap 10
 set transform-set myset
 reverse-route
!

crypto map clientmap isakmp authorization list employee

!--- Create the crypto map.
```

```
crypto map clientmap client configuration address
crypto map clientmap 10 ipsec-isakmp dynamic mymap

!

!--- Apply the

employee

 group list that was created earlier.



!
!
!
!
interface Ethernet0/0
 ip address 10.0.0.20 255.0.0.0
 half-duplex
!

interface Serial3/0
 ip address 192.168.1.11 255.255.255.0
 clock rate 64000
 no fair-queue
 crypto map clientmap


!--- Apply the crypto map to the interface.

!
interface Serial3/1
 no ip address
 shutdown
!
interface Serial3/2
 no ip address
 shutdown
!
interface Serial3/3
 no ip address
 shutdown
!
interface Serial3/4
 no ip address
 shutdown
!
interface Serial3/5
 no ip address
 shutdown
!
interface Serial3/6
 no ip address
 shutdown
!
interface Serial3/7
 no ip address
 shutdown

ip local pool mypool 10.0.0.50 10.0.0.60
```

```
!--- Configure the Dynamic Host Configuration Protocol !--- (DHCP) pool which assigns the tunnel !--- 


ip http server
no ip http secure-server
!
ip route 172.16.0.0 255.255.0.0 192.168.1.10
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end


ip subnet-zero . . .
!
end
```

Nota: Este ejemplo utiliza solamente la autenticación de grupo. No utiliza autenticación de usuario individual.

Configuración de cliente VPN

Se puede descargar un software VPN Client desde el Cisco.com Software Center.

Nota: Algunos programas de Cisco requieren que inicie sesión con un nombre de usuario y una contraseña de CCO.

Complete estos pasos para configurar el VPN Client.

1. Desde su cliente inalámbrico (laptop), elija Inicio > Programas > Cisco Systems VPN Client > VPN Client para acceder a VPN Client. Esta es la ubicación predeterminada donde se instala VPN Client.

2. Haga clic en New para iniciar la ventana Create New VPN Connection Entry.

3. Introduzca el nombre de la entrada de conexión junto con una descripción. Este ejemplo

utiliza vpn.

El campo Descripción es opcional. Introduzca la dirección IP del servidor VPN en el cuadro Host. A continuación, introduzca el nombre del grupo VPN y la contraseña y haga clic en Save.

Nota: El nombre de grupo y la contraseña configurados aquí deben ser los mismos que los configurados en el servidor VPN. En este ejemplo se utilizan los campos Name employee y Password cisco123.

Verificación

Para verificar esta configuración, configure el SSID vpnclient en el cliente inalámbrico con los mismos parámetros de seguridad configurados en el WLC y asocie el cliente a esta WLAN. Hay varios documentos que explican cómo configurar un cliente inalámbrico con un nuevo perfil.

Una vez que el cliente inalámbrico esté asociado, vaya a VPN Client (Cliente VPN) y haga clic en la conexión que ha configurado. A continuación, haga clic en Connect en la ventana principal de VPN Client.

Puede ver los parámetros de seguridad de fase 1 y fase 2 negociados entre el cliente y el servidor.

Nota: Para establecer este túnel VPN, el cliente VPN y el servidor deben tener alcance IP entre ellos. Si el cliente VPN no puede ponerse en contacto con el gateway de seguridad (servidor VPN), el túnel no se establece y se muestra un cuadro de alerta en el lado del cliente con este mensaje:

```
Reason 412: The remote peer is no longer responding
```

Para asegurarse de que un túnel VPN esté establecido correctamente entre el cliente y el servidor, puede encontrar un icono de candado que se crea junto al cliente VPN establecido. La barra de estado también indica Conectado a "vpn". Aquí está un ejemplo.

Además, asegúrese de que puede transmitir con éxito datos al segmento LAN en el lado del servidor desde el cliente VPN y viceversa. En el menú principal de VPN Client, elija Status > Statistics. Allí puede encontrar las estadísticas de los paquetes cifrados y descifrados que pasan a través del túnel.

En esta captura de pantalla, puede ver la dirección del cliente como 10.0.0.57. Esta es la dirección que el servidor VPN asigna al cliente desde su conjunto configurado localmente después de una negociación exitosa de la Fase 1. Una vez establecido el túnel, el servidor VPN agrega automáticamente una ruta a esta dirección IP DHCP asignada en su tabla de rutas.

También puede ver el aumento del número de paquetes cifrados mientras se transfieren los datos

del cliente al servidor y el aumento del número de paquetes descifrados durante una transferencia de datos inversa.

Nota: Dado que el WLC se configura para el paso a través de VPN, permite que el cliente acceda solamente al segmento conectado con el gateway VPN (aquí, es el servidor VPN 192.168.1.11) configurado para el paso a través. Esto filtra el resto del tráfico.

Puede verificar esto configurando otro servidor VPN con la misma configuración y configurando una nueva entrada de conexión para este servidor VPN en VPN Client. Ahora, cuando intenta establecer un túnel con este servidor VPN, no tiene éxito. Esto se debe a que el WLC filtra este tráfico y permite un túnel solamente a la dirección del gateway VPN configurada para el paso a través de VPN.

También puede verificar la configuración desde la CLI del servidor VPN.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Estos comandos show utilizados en el servidor VPN también pueden ser útiles para ayudarlo a verificar el estado del túnel.

- El comando show crypto session se utiliza para verificar el estado del túnel. A continuación se muestra un ejemplo de salida de este comando.

```
<#root>

Crypto session current status

Interface: Serial3/0

Session status: UP-ACTIVE

Peer: 172.16.1.20 port 500
  IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58


Active SAs: 2, origin: dynamic crypto map
```

- La política show crypto isakmp se utiliza para ver los parámetros de la fase 1 configurada.

Troubleshoot

Los comandos debug y show explicados en la sección Verify también se pueden utilizar para

resolver problemas.

- debug crypto isakmp
- debug crypto ipsec
- show crypto session
- El comando debug crypto isakmp en el servidor VPN muestra todo el proceso de negociación de la Fase 1 entre el cliente y el servidor. Este es un ejemplo de una negociación exitosa de la Fase 1.

<#root>

```
------------------------------------------------------------------
 ----------------------------------------------------------
------------------------------------------------------------------
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):

Checking ISAKMP transform 14
   against priority 1 policy

*Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC
*Aug 28 10:37:29.515: ISAKMP:      hash MD5
*Aug 28 10:37:29.515: ISAKMP:      default group 2
*Aug 28 10:37:29.515: ISAKMP:      auth pre-share
*Aug 28 10:37:29.515: ISAKMP:      life type in seconds
*Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):

atts are acceptable. Next payload is 0

*Aug 28
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):

SA authentication status:
    authenticated

*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact,
  bring down existing phase 1 and 2 SA's with local 192.168.1.11
  remote 172.16.1.20 remote port 500
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
  the address pool: 10.0.0.57
*Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade
  1583442981 to QM_IDLE
*Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY
  RESPONDER_LIFETIME protocol 1
    spi 1689265296, message ID = 1583442981
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to
  172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981
*Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400

*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Aug 28 10:37:29.967:

ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2
  New State = IKE_P1_COMPLETE
```

- El comando debug crypto ipsec en el servidor VPN muestra la negociación IPSec de fase 1 y la creación exitosas del túnel VPN. Aquí tiene un ejemplo:

```
<#root>

----------------------------------------------------------------------
 ----------------------------------------------------------------
----------------------------------------------------------------------
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
    from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA

*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for
  peer or rekeying for peer 172.16.1.20

*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0

*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added
  10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0

*Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F
*Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58,
  dest_port 0

*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.11, sa_proto= 50,
    sa_spi= 0x8538A817(2235082775),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
*

Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.20, sa_proto= 50,
    sa_spi= 0xFFC80936(4291299638),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

Información Relacionada

- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Página de Soporte del Protocolo IKE/la Negociación de IPSec

- Configuración de seguridad de red IPSec
- Preguntas y respuestas sobre Cisco Easy VPN
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Ejemplo de configuración de ACL en controladores de LAN inalámbricas
- Preguntas frecuentes sobre el controlador LAN inalámbrico (WLC)
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems

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).