

# Respuesta a preguntas frecuentes sobre AnyConnect: túneles, DPD y temporizador de inactividad

## Contenido

---

### [Introducción](#)

### [Antecedentes](#)

[Tipos de túneles](#)

[Salida de muestra de ASA](#)

### [DPD y temporizadores de inactividad](#)

[¿Cuándo se considera una sesión inactiva?](#)

[¿Cuándo el ASA descarta el SSL-Tunnel?](#)

[¿Por qué deben activarse los keepalives si los DPD ya están activados?](#)

### [Comportamiento del cliente AnyConnect en caso de reconexiones](#)

[El proceso real](#)

### [Comportamiento del cliente de AnyConnect en caso de suspensión del sistema](#)

### [Preguntas Frecuentes](#)

[Q1. Anyconnect DPD tiene un intervalo pero no reintentos - ¿cuántos paquetes tiene que perder antes de que marque el extremo remoto como muerto?](#)

[Q2. ¿El procesamiento de DPD es diferente para AnyConnect con IKEv2?](#)

[Q3. ¿Existe otro propósito para el túnel principal de AnyConnect?](#)

[Q4. ¿Puede filtrar y cerrar la sesión solo de las sesiones inactivas?](#)

[P5. ¿Qué sucede con el túnel principal cuando vence el tiempo de espera inactivo de los túneles DTLS o TLS?](#)

[P6. ¿Por qué mantener la sesión una vez que los temporizadores DPD han desconectado la sesión y por qué ASA no libera la dirección IP?](#)

[P7. ¿Cuál es el comportamiento si ASA falla de Activo a En espera?](#)

[P8. ¿Por qué hay dos tiempos de espera diferentes, el tiempo de espera inactivo y el tiempo de espera desconectado, si ambos tienen el mismo valor?](#)

[P9. ¿Qué ocurre cuando se suspende el equipo cliente?](#)

[P10. Cuando se produce una reconexión, ¿el adaptador virtual de AnyConnect se inestabiliza o la tabla de routing cambia?](#)

[P11. ¿Proporciona la reconexión automática persistencia de sesiones? En caso afirmativo, ¿se ha añadido alguna funcionalidad adicional en el cliente AnyConnect?](#)

[P12. Esta función funciona en todas las variantes de Microsoft Windows \(Vista de 32 y 64 bits, XP\). ¿Qué tal el Macintosh? ¿Funciona en OS X 10.4?](#)

[P13. ¿Existe alguna limitación en cuanto a la conectividad \(por cable, Wi-Fi, 3G, etc.\)? ¿Admite la transición de un modo a otro \(de Wi-Fi a 3G, 3G a redes por cable, etc.\)?](#)

[P14. ¿Cómo se autentica la operación de reanudación?](#)

[P15. ¿Se realiza también la autorización LDAP al volver a conectar o solo la autenticación?](#)

[P16. ¿Se puede ejecutar antes del inicio de sesión y/o el host tras la reanudación?](#)

[P17. Con respecto al balance de carga de VPN \(LB\) y la reanudación de la conexión, ¿el cliente se conecta de nuevo directamente al miembro del clúster al que estaba conectado antes?](#)

### [Información Relacionada](#)

---

# Introducción

Este documento describe los túneles de Cisco AnyConnect Secure Mobility Client, el comportamiento de reconexión, la detección de puntos inactivos (DPD) y el temporizador de inactividad.

## Antecedentes

### Tipos de túneles

Hay dos métodos utilizados para conectar una sesión de AnyConnect:

- A través del portal (sin cliente)
- A través de la aplicación independiente

Según la forma en la que se conecte, puede crear tres túneles (sesiones) diferentes en el dispositivo de seguridad adaptable de Cisco (ASA), cada uno con un objetivo específico:

1. Clientless o Parent-Tunnel: Esta es la sesión principal que se crea en la negociación para configurar el token de sesión que es necesario en caso de que se necesite una reconexión debido a problemas de conectividad de red o hibernación. En función del mecanismo de conexión, ASA muestra la sesión como sin cliente (Webaunch a través del portal) o principal (AnyConnect independiente).



**Nota:** AnyConnect-Parent representa la sesión cuando el cliente no está conectado activamente. Efectivamente, funciona de manera similar a una cookie, en el sentido de que es una entrada de base de datos en el ASA que se asigna a la conexión desde un cliente en particular. Si el cliente duerme o hibernar, los túneles (IPsec/Intercambio de claves de Internet (IKE)/Seguridad de la capa de transporte (TLS)/Seguridad de la capa de transporte del datagrama (DTLS)) se desactivan, pero el principal permanece hasta que se aplica el temporizador de inactividad o el tiempo máximo de conexión. Esto permite al usuario volver a conectarse sin volver a autenticarse.

---

2. Túnel de capa de conexión segura (SSL): la conexión SSL se establece en primer lugar y los datos se transfieren a través de esta conexión mientras se intenta establecer una conexión DTLS. Una vez establecida la conexión DTLS, el cliente envía los paquetes a través de la conexión DTLS en lugar de a través de la conexión SSL. Los paquetes de control, por otro lado, siempre pasan por la conexión SSL.
3. Túnel DTLS: cuando el túnel DTLS está completamente establecido, todos los datos se mueven al túnel DTLS y el túnel SSL sólo se utiliza para el tráfico ocasional del canal de control. Si le ocurre algo al Protocolo de datagramas de usuario (UDP), el túnel DTLS se desactiva y todos los datos pasan de nuevo a través del túnel SSL.

## Salida de muestra de ASA

A continuación se muestra un ejemplo de salida de los dos métodos de conexión.

AnyConnect conectado mediante inicio web:

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username      : walter                      Index       : 1435
Assigned IP   : 192.168.1.4                 Public IP   : 172.16.250.17
Protocol      : Clientless SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : Clientless: (1)RC4  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing       : Clientless: (1)SHA1  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx      : 335765                     Bytes Rx    : 31508
Pkts Tx       : 214                       Pkts Rx     : 18
Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
Group Policy  : My-Network                 Tunnel Group : My-Network
Login Time    : 22:13:37 UTC Fri Nov 30 2012
Duration      : 0h:00m:34s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                       VLAN        : none
```

```
Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

Clientless:

```
Tunnel ID     : 1435.1
Public IP     : 172.16.250.17
Encryption    : RC4                       Hashing      : SHA1
Encapsulation: TLSv1.0                   TCP Dst Port : 443
Auth Mode     : userPassword
Idle Time Out: 2 Minutes                 Idle TO Left : 1 Minutes
Client Type   : Web Browser
Client Ver    : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx      : 329671                     Bytes Rx     : 31508
```

SSL-Tunnel:

```
Tunnel ID     : 1435.2
Assigned IP   : 192.168.1.4                 Public IP   : 172.16.250.17
Encryption    : RC4                       Hashing      : SHA1
Encapsulation: TLSv1.0                   TCP Src Port : 1241
TCP Dst Port  : 443                       Auth Mode    : userPassword
Idle Time Out: 2 Minutes                 Idle TO Left : 1 Minutes
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx      : 6094                       Bytes Rx     : 0
Pkts Tx       : 4                         Pkts Rx     : 0
Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
```

DTLS-Tunnel:

```
Tunnel ID     : 1435.3
Assigned IP   : 192.168.1.4                 Public IP   : 172.16.250.17
Encryption    : AES128                    Hashing      : SHA1
```

Encapsulation: DTLSv1.0                      Compression : LZS  
UDP Src Port : 1250                          UDP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 2 Minutes                    Idle TO Left : 1 Minutes  
Client Type : DTLS VPN Client  
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0  
Bytes Tx : 0                                  Bytes Rx : 0  
Pkts Tx : 0                                  Pkts Rx : 0  
Pkts Tx Drop : 0                            Pkts Rx Drop : 0

AnyConnect conectado a través de la aplicación independiente:

<#root>

ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter                            Index : 1436  
Assigned IP : 192.168.1.4                    Public IP : 172.16.250.17  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 12244                            Bytes Rx : 777  
Pkts Tx : 8                                  Pkts Rx : 1  
Pkts Tx Drop : 0                            Pkts Rx Drop : 0  
Group Policy : My-Network                   Tunnel Group : My-Network  
Login Time : 22:15:24 UTC Fri Nov 30 2012  
Duration : 0h:00m:11s  
Inactivity : 0h:00m:00s  
NAC Result : Unknown  
VLAN Mapping : N/A                          VLAN : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 1436.1  
Public IP : 172.16.250.17  
Encryption : none                            Hashing : none  
TCP Src Port : 1269                          TCP Dst Port : 443  
Auth Mode : userPassword  
Idle Time Out: 2 Minutes                    Idle TO Left : 1 Minutes  
Client Type : AnyConnect  
Client Ver : 3.1.01065  
Bytes Tx : 6122                              Bytes Rx : 777  
Pkts Tx : 4                                  Pkts Rx : 1  
Pkts Tx Drop : 0                            Pkts Rx Drop : 0

SSL-Tunnel

:  
Tunnel ID : 1436.2  
Assigned IP : 192.168.1.4                    Public IP : 172.16.250.17  
Encryption : RC4                            Hashing : SHA1  
Encapsulation: TLSv1.0                      TCP Src Port : 1272

```
TCP Dst Port : 443                Auth Mode    : userPassword
Idle Time Out: 2 Minutes          Idle TO Left : 1 Minutes
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx      : 6122              Bytes Rx     : 0
Pkts Tx       : 4                 Pkts Rx     : 0
Pkts Tx Drop  : 0                Pkts Rx Drop : 0
```

#### DTLS-Tunnel

```
:
Tunnel ID      : 1436.3
Assigned IP    : 192.168.1.4      Public IP     : 172.16.250.17
Encryption     : AES128          Hashing       : SHA1
Encapsulation  : DTLSv1.0        Compression   : LZS
UDP Src Port   : 1280            UDP Dst Port  : 443
Auth Mode      : userPassword
Idle Time Out: 2 Minutes          Idle TO Left  : 1 Minutes
Client Type    : DTLS VPN Client
Client Ver     : 3.1.01065
Bytes Tx       : 0                Bytes Rx      : 0
Pkts Tx        : 0                Pkts Rx      : 0
Pkts Tx Drop   : 0                Pkts Rx Drop : 0
```

## DPD y temporizadores de inactividad

### ¿Cuándo se considera una sesión inactiva?

La sesión se considera Inactiva (y el temporizador comienza a aumentar) sólo cuando el SSL-Tunnel ya no existe en la sesión. Por lo tanto, cada sesión tiene una marca de tiempo con el tiempo de caída del Túnel SSL.

```
ASA5520-C# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username       : walter                Index        : 1336
Public IP      : 172.16.250.17
Protocol       : AnyConnect-Parent    <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License        : AnyConnect Premium
Encryption     : AnyConnect-Parent: (1)none
Hashing        : AnyConnect-Parent: (1)none
Bytes Tx       : 12917                  Bytes Rx     : 1187
Pkts Tx        : 14                     Pkts Rx     : 7
Pkts Tx Drop   : 0                       Pkts Rx Drop : 0
Group Policy   : My-Network              Tunnel Group : My-Network
Login Time     : 17:42:56 UTC Sat Nov 17 2012
Duration       : 0h:09m:14s
Inactivity     : 0h:01m:06s             <- So the session is considered Inactive
NAC Result     : Unknown
VLAN Mapping   : N/A                    VLAN         : none
```

## ¿Cuándo el ASA descarta el SSL-Tunnel?

Hay dos maneras de desconectar un SSL-Tunnel:

1. DPD: El cliente utiliza las DPD para detectar un fallo en las comunicaciones entre el cliente AnyConnect y el centro distribuidor ASA. Los DPD también se utilizan para limpiar los recursos en el ASA. Esto garantiza que el centro distribuidor no mantenga conexiones en la base de datos si el punto final no responde a los pings DPD. Si ASA envía un DPD al terminal y responde, no se realiza ninguna acción. Si el terminal no responde, después del número máximo de retransmisión (depende de si se utiliza IKEv1 o IKEv2) el ASA desmonta el túnel en la base de datos de sesión y mueve la sesión a un modo de espera para reanudación. Esto significa que se ha iniciado DPD desde el centro distribuidor y que el centro distribuidor ya no se comunica con el cliente. En tales situaciones, el ASA mantiene el Túnel Principal activo para permitir al usuario vagar por las redes, ir a dormir y recuperar la sesión. Estas sesiones cuentan para las sesiones conectadas activamente y se borran en estas condiciones:
  - User Idle-Timeout
  - El cliente reanuda la sesión original y cierra la sesión correctamente.

Para configurar DPDs, utilice el `anyconnect dpd-interval` comando debajo de los atributos WebVPN en las configuraciones de la política de grupo. De forma predeterminada, el DPD está activado y configurado en 30 segundos tanto para el ASA (gateway) como para el cliente.



Precaución: tenga en cuenta el Id. de error de Cisco [CSCts6926](#): DPD no puede terminar el túnel DTLS después de perder la conexión del cliente.

---

2. Idle-Timeout (Tiempo de espera inactivo): La segunda forma en que se desconecta el túnel SSL es cuando expira el tiempo de espera inactivo para este túnel. Sin embargo, recuerde que no es sólo el SSL-Tunnel el que debe estar inactivo, sino también el túnel DTLS. A menos que se agote el tiempo de espera de la sesión DTLS, el túnel SSL se conserva en la base de datos.

## ¿Por qué deben activarse los keepalives si los DPD ya están activados?

Como se explicó anteriormente, el DPD no elimina la sesión de AnyConnect en sí. Simplemente mata el túnel dentro de esa sesión para que el cliente pueda restablecer el túnel. Si el cliente no puede restablecer el túnel, la sesión permanece hasta que el temporizador de inactividad caduca en el ASA. Dado que los DPD están habilitados de forma predeterminada, los clientes a menudo pueden desconectarse debido a que los flujos se cierran en una dirección con la traducción de direcciones de red (NAT), el firewall y los dispositivos proxy. La activación de señales de mantenimiento a intervalos bajos, como 20 segundos, ayuda a evitar esto.

Las señales de mantenimiento se habilitan bajo los atributos WebVPN de una política de grupo

determinada con el `anyconnect ssl keepalive` comando. De forma predeterminada, los temporizadores se establecen en 20 segundos.

## Comportamiento del cliente AnyConnect en caso de reconexiones

AnyConnect intenta volver a conectarse si se interrumpe la conexión. Esto no se puede configurar automáticamente. Mientras la sesión VPN en ASA siga siendo válida y AnyConnect pueda restablecer la conexión física, se reanuda la sesión VPN.

La función de reconexión continúa hasta que caduca el tiempo de espera de la sesión o el tiempo de espera de desconexión, que en realidad es el tiempo de espera inactivo (o 30 minutos si no se ha configurado ningún tiempo de espera). Una vez que caducan, el cliente no puede continuar porque las sesiones VPN ya se han eliminado en el ASA. El cliente continúa mientras piense que el ASA aún tiene la sesión VPN.

AnyConnect se vuelve a conectar independientemente de cómo cambie la interfaz de red. No importa si la dirección IP de la tarjeta de interfaz de red (NIC) cambia o si la conectividad cambia de una NIC a otra (de inalámbrica a con cables o viceversa).

Al considerar el proceso de reconexión para AnyConnect, hay tres niveles de sesiones que debe recordar. Además, el comportamiento de reconexión de cada una de estas sesiones se asocia libremente, en el sentido de que cualquiera de ellas se puede restablecer sin una dependencia de los elementos de sesión de la capa anterior:

1. Reconexiones TCP o UDP [capa OSI 3]
2. TLS, DTLS o IPSec (IKE+ESP) [Capa OSI 4]: no se admite la reanudación de TLS.
3. VPN [capa OSI 7]: el token de sesión VPN se utiliza como un token de autenticación para restablecer la sesión VPN en un canal seguro cuando hay una interrupción. Es un mecanismo propietario muy similar, conceptualmente, a cómo se utiliza un token Kerberos o un certificado de cliente para la autenticación. El token es único y está generado criptográficamente por el centro distribuidor, que contiene el ID de sesión más una carga aleatoria generada criptográficamente. Se pasa al cliente como parte del establecimiento VPN inicial después de que se establece un canal seguro al centro distribuidor. Sigue siendo válido durante toda la duración de la sesión en el centro distribuidor y se almacena en la memoria del cliente, que es un proceso privilegiado.



Sugerencia: estas versiones de ASA y posteriores contienen un token de sesión criptográfica más fiable: 9.1(3) y 8.4(7.1)

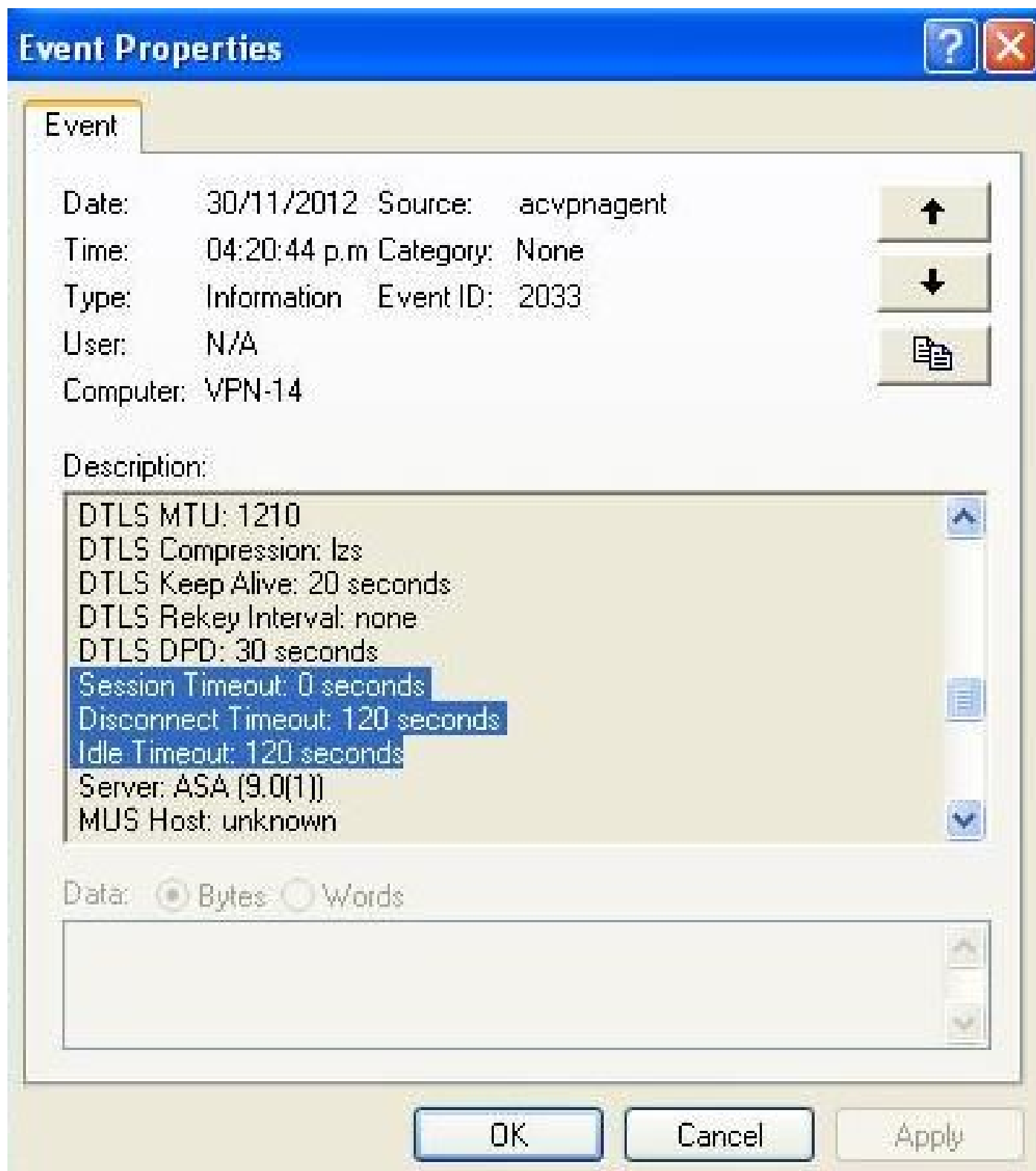
---

### El proceso real

Se inicia un temporizador de tiempo de espera de desconexión tan pronto como se interrumpe la

conexión de red. El cliente AnyConnect continúa intentando volver a conectarse mientras este temporizador no caduque. El tiempo de espera de desconexión se establece en el valor más bajo de Tiempo de espera de inactividad de la directiva de grupo o Tiempo máximo de conexión.


El valor de este temporizador se ve en el Visor de eventos para la sesión de AnyConnect en la negociación:



En este ejemplo, la sesión se desconecta después de dos minutos (120 segundos), que se pueden comprobar en el Historial de mensajes de AnyConnect:




```
[30/11/2012 04:30:02 p.m.] Checking for product updates...
[30/11/2012 04:30:02 p.m.] Checking for customization updates...
[30/11/2012 04:30:02 p.m.] Performing any required updates...
[30/11/2012 04:30:02 p.m.] Establishing VPN session...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Initiating connection...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Examining system...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Activating VPN adapter...
[30/11/2012 04:30:05 p.m.] Establishing VPN - Configuring system...
[30/11/2012 04:30:05 p.m.] Establishing VPN...
[30/11/2012 04:30:05 p.m.] Connected to 10.198.16.140.
[30/11/2012 04:30:06 p.m.] Connected to 10.198.16.140.
[30/11/2012 04:33:28 p.m.] Reconnecting to 10.198.16.140...
[30/11/2012 04:33:28 p.m.] Reconnecting, waiting for network connectivity...
[30/11/2012 04:35:28 p.m.] Reconnecting to 10.198.16.140...
[30/11/2012 04:35:28 p.m.] Disconnect in progress, please wait...
[30/11/2012 04:35:28 p.m.] Disconnect in progress, please wait...
[30/11/2012 04:35:34 p.m.] Verify your network connection.
```

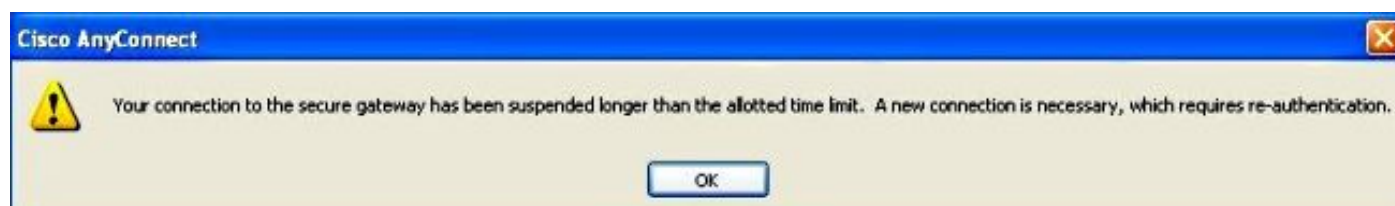
 Sugerencia: Para que ASA responda a un cliente que intenta reconectarse, la sesión de túnel principal debe seguir existiendo en la base de datos ASA. En caso de fallo, los DPD también deben activarse para que funcione el comportamiento de reconexión.

Como se puede ver en los mensajes anteriores, la reconexión falló. Sin embargo, si la reconexión es exitosa, esto es lo que sucede:


1. El túnel principal sigue siendo el mismo. Esto no se renegocia porque este túnel mantiene el token de sesión que se requiere para que la sesión se vuelva a conectar.
2. Se generan nuevas sesiones SSL y DTLS, y se utilizan diferentes puertos de origen en la reconexión.
3. Se restauran todos los valores de Idle-Timeout.
4. Se restaura el tiempo de espera de inactividad.

 Precaución: tenga en cuenta el Id. de error de Cisco [CSCtg3110](#). La base de datos de sesión VPN no actualiza la dirección IP pública en la base de datos de sesión ASA cuando AnyConnect se vuelve a conectar.

En esta situación en la que fallan los intentos de reconexión, aparece este mensaje:



---


 Nota: Esta solicitud de mejora se ha presentado para hacer esto más granular: ID de bug de Cisco [CSCsl52873](#) - ASA no tiene un tiempo de espera desconectado configurable para AnyConnect.

---

## Comportamiento del cliente de AnyConnect en caso de suspensión del sistema

Existe una función de itinerancia que permite que AnyConnect se vuelva a conectar después de la suspensión del PC. El cliente continúa intentando hasta que caducan los tiempos de espera de inactividad o de sesión y el cliente no cierra inmediatamente el túnel cuando el sistema entra en hibernación/espera. Para los usuarios que no deseen esta función, establezca el tiempo de espera de la sesión en un valor bajo para evitar reconexiones de suspensión/reanudación.

---

 Nota: Después de la corrección del Id. de error de Cisco [CSCso17627](#) (Versión 2.3(111)+), se introdujo un botón de control para inhabilitar esta función de reconexión al reanudar.

---

El comportamiento de la Reconexión automática para AnyConnect se puede controlar a través del perfil XML de AnyConnect con esta configuración:

```
<AutoReconnect UserControllable="true">true
  <AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

Con este cambio, AnyConnect intenta volver a conectarse cuando el equipo vuelve de la suspensión. El valor predeterminado de la preferencia AutoReconnectBehavior es DisconnectOnSuspend. Este comportamiento es diferente al de AnyConnect Client Release 2.2. Para la reconexión después de la reanudación, el administrador de red debe establecer ReconnectAfterResume en el perfil o hacer que las preferencias AutoReconnect y AutoReconnectBehavior sean controlables por el usuario en el perfil para permitir que los usuarios lo establezcan.

## Preguntas Frecuentes

Q1. Anyconnect DPD tiene un intervalo pero no reintentos - ¿cuántos paquetes tiene que perder antes de que marque el extremo remoto como muerto?

R. Desde la perspectiva del cliente, los DPD solo derriban un túnel durante la etapa de establecimiento del túnel. Si el cliente encuentra tres reintentos (envía cuatro paquetes) durante la etapa de establecimiento del túnel y no recibe una respuesta del servidor VPN primario, vuelve a utilizar uno de los servidores de respaldo si uno está configurado. Sin embargo, una vez que se ha establecido el túnel, los DPD perdidos no tienen ningún impacto en el túnel desde la

perspectiva del cliente. El impacto real de las DPD se produce en el servidor VPN, como se explica en la sección [DPDs y temporizadores de inactividad](#).

Q2. ¿El procesamiento de DPD es diferente para AnyConnect con IKEv2?

R. Sí, IKEv2 tiene un número fijo de reintentos: seis reintentos/siete paquetes.

Q3. ¿Existe otro propósito para el túnel principal de AnyConnect?

R. Además de ser un mapping en el ASA, el túnel principal se utiliza para enviar las actualizaciones de imagen de AnyConnect del ASA al cliente, porque el cliente no está conectado activamente durante el proceso de upgrade.

Q4. ¿Puede filtrar y cerrar la sesión solo de las sesiones inactivas?

R. Puede filtrar las sesiones inactivas con el comando `show vpn-sessiondb anyconnect filter inactive`. Sin embargo, no hay ningún comando para cerrar la sesión solo en las sesiones inactivas. En su lugar, debe cerrar sesiones específicas o cerrar todas las sesiones por usuario (índice - nombre), protocolo o grupo de túnel. Una solicitud de mejora, ID de bug de Cisco [CSCuh5707](#), ha sido archivada para agregar la opción de cerrar solamente las sesiones inactivas.

P5. ¿Qué sucede con el túnel principal cuando vence el tiempo de espera inactivo de los túneles DTLS o TLS?

A. El temporizador Idle TO Left de la sesión principal de AnyConnect se restablece después de que se desactive el túnel SSL o el túnel DTLS. Esto permite que idle-timeout actúe como un tiempo de espera desconectado. Este efectivamente se convierte en el tiempo permitido para que el cliente se vuelva a conectar. Si el cliente no se vuelve a conectar dentro del temporizador, el túnel principal se termina.

P6. ¿Por qué mantener la sesión una vez que los temporizadores DPD han desconectado la sesión y por qué ASA no libera la dirección IP?

R. El centro distribuidor no tiene conocimiento del estado del cliente. En este caso, ASA espera a que el cliente se vuelva a conectar con suerte hasta que la sesión agote el tiempo de espera del temporizador de inactividad. DPD no mata una sesión de AnyConnect; simplemente mata el túnel (dentro de esa sesión) para que el cliente pueda restablecer el túnel. Si el cliente no restablece un túnel, la sesión permanece hasta que caduca el temporizador de inactividad.


Si la preocupación es acerca de las sesiones que se están agotando, establezca los inicios de sesión simultáneos en un valor bajo como uno. Con esta configuración, los usuarios que tienen una sesión en la base de datos de sesión eliminan su sesión anterior cuando vuelven a iniciar sesión.

P7. ¿Cuál es el comportamiento si ASA falla de Activo a En espera?

R. Inicialmente, cuando se establece la sesión, los tres túneles (Parent, SSL y DTLS) se replican en la unidad en espera. Una vez que el ASA falla, las sesiones DTLS y TLS se restablecen ya que no se sincronizan con la unidad standby, pero cualquier dato que fluya a través de los túneles debe funcionar sin interrupción después de que se restablezca la sesión de AnyConnect.

Las sesiones SSL/DTLS no son stateful, por lo que el estado SSL y el número de secuencia no se mantienen y pueden ser bastante gravosos. Por lo tanto, esas sesiones deben restablecerse desde cero, lo que se hace con la sesión principal y el token de sesión.

---

 Consejo: En caso de falla, las sesiones del cliente SSL VPN no se traspasan al dispositivo en espera si las señales de mantenimiento están inhabilitadas.

---

P8. ¿Por qué hay dos tiempos de espera diferentes, el tiempo de espera inactivo y el tiempo de espera desconectado, si ambos tienen el mismo valor?

R. Cuando se desarrollaron los protocolos, se proporcionaron dos tiempos de espera diferentes para:

- Tiempo de espera inactivo: el tiempo de espera inactivo es para cuando no se transfieren datos a través de una conexión.
- Tiempo de espera desconectado: El tiempo de espera desconectado es para cuando abandona la sesión VPN porque se ha perdido la conexión y no se puede restablecer.

El tiempo de espera desconectado nunca se implementó en el ASA. En su lugar, ASA envía el valor de tiempo de espera inactivo para los tiempos de espera inactivos y desconectados al cliente.

El cliente no utiliza el tiempo de espera inactivo, porque ASA maneja el tiempo de espera inactivo. El cliente utiliza el valor de tiempo de espera desconectado, que es el mismo que el valor de tiempo de espera inactivo, para saber cuándo abandonar los intentos de reconexión ya que ASA ha interrumpido la sesión.

Aunque no está conectado activamente con el cliente, ASA agota el tiempo de espera de la sesión a través del tiempo de espera inactivo. La razón principal para no implementar el tiempo de espera desconectado en el ASA fue evitar la adición de otro temporizador para cada sesión VPN y el aumento en la sobrecarga en el ASA (aunque el mismo temporizador se podría utilizar en ambos casos, solo con diferentes valores de tiempo de espera, ya que los dos casos son mutuamente excluyentes).

El único valor agregado con el tiempo de espera desconectado es permitir que un administrador especifique un tiempo de espera diferente para cuando el cliente no está conectado activamente frente a inactivo. Como se mencionó anteriormente, el ID de bug de Cisco [CSCsl52873](#) se ha registrado para esto.

P9. ¿Qué ocurre cuando se suspende el equipo cliente?

R. De forma predeterminada, AnyConnect intenta restablecer una conexión VPN cuando se

pierde la conectividad. No intenta restablecer una conexión VPN después de que el sistema se reanude de forma predeterminada. Consulte [Comportamiento del Cliente de AnyConnect en Caso de Suspensión del Sistema](#) para obtener detalles.

P10. Cuando se produce una reconexión, ¿el adaptador virtual de AnyConnect se inestabiliza o la tabla de routing cambia?

R. Una reconexión a nivel de túnel tampoco funciona. Esta es una reconexión en SSL o DTLS solamente. Estos van unos 30 segundos antes de que se den por vencidos. Si DTLS falla, simplemente se descarta. Si SSL falla, provoca una reconexión en el nivel de sesión. Una reconexión a nivel de sesión rehace completamente el ruteo. Si la dirección de cliente asignada en la reconexión, o cualquier otro parámetro de configuración que afecte al adaptador virtual (VA), no ha cambiado, el VA no se desactivará. Aunque es poco probable que se produzca algún cambio en los parámetros de configuración recibidos del ASA, es posible que un cambio en la interfaz física utilizada para la conexión VPN (por ejemplo, si desacopla y pasa de una conexión con cables a una Wi-Fi) pueda dar lugar a un valor de unidad de transmisión máxima (MTU) diferente para la conexión VPN. El valor de MTU afecta al VA, y un cambio en él hace que el VA se inhabilite y luego se vuelva a habilitar.

P11. ¿La Reconexión automática proporciona persistencia de sesión? En caso afirmativo, ¿se ha añadido alguna funcionalidad adicional en el cliente AnyConnect?

R. AnyConnect no proporciona ninguna magia adicional para admitir la persistencia de sesiones en las aplicaciones. Sin embargo, la conectividad VPN se restaura automáticamente poco después de que se reanude la conectividad de red con el gateway seguro, siempre que los tiempos de espera de sesión y de inactividad configurados en el ASA no hayan caducado. Y a diferencia del cliente IPSec, la reconexión automática da como resultado la misma dirección IP del cliente. Mientras AnyConnect intenta volver a conectarse, el adaptador virtual de AnyConnect permanece activado y en el estado conectado, de modo que la dirección IP del cliente permanece presente y activada en el PC cliente todo el tiempo, lo que proporciona persistencia en la dirección IP del cliente. Sin embargo, las aplicaciones de PC cliente todavía perciben la pérdida de conectividad con sus servidores en la red de la empresa si se tarda demasiado en restaurar la conectividad VPN.

P12. Esta función funciona en todas las variantes de Microsoft Windows (Vista de 32 bits y 64 bits, XP). ¿Qué tal el Macintosh? ¿Funciona en OS X 10.4?

R. Esta función funciona en Mac y Linux. Ha habido problemas con Mac y Linux, pero se han hecho mejoras recientes, especialmente para Mac. Linux aún requiere soporte adicional (ID de bug de Cisco [CSCsr16670](#), ID de bug de Cisco [CSCsm69213](#)), pero la funcionalidad básica está ahí también. Con respecto a Linux, AnyConnect no reconoce que se ha producido una suspensión/reanudación (suspensión/activación). Esto tiene básicamente dos impactos:

- La configuración de perfil/preferencia de AutoReconnectBehavior no se puede soportar en Linux sin soporte de suspensión/reanudación, por lo que una reconexión siempre ocurre

después de suspender/reanudar.

- En Microsoft Windows y Macintosh, las reconexiones se realizan inmediatamente en el nivel de sesión después de la reanudación, lo que permite un cambio más rápido a una interfaz física diferente. En Linux, debido a que AnyConnect no es consciente de la suspensión/reanudación, las reconexiones se realizan primero en el nivel del túnel (SSL y DTLS) y esto puede significar que las reconexiones tardan un poco más. Pero las reconexiones aún ocurren en Linux.

P13. ¿Existe alguna limitación en cuanto a la conectividad (por cable, Wi-Fi, 3G, etc.)? ¿Admite la transición de un modo a otro (de Wi-Fi a 3G, 3G a redes por cable, etc.)?

R. AnyConnect no está vinculado a una interfaz física determinada durante la vida útil de la conexión VPN. Si se pierde la interfaz física utilizada para la conexión VPN o si los intentos de reconexión superan un umbral de error determinado, AnyConnect ya no utiliza esa interfaz e intenta alcanzar el gateway seguro con las interfaces disponibles hasta que caduquen los temporizadores de sesión o de inactividad. Tenga en cuenta que un cambio en la interfaz física podría resultar en un valor de MTU diferente para el VA, lo que hace que el VA tenga que ser inhabilitado y habilitado de nuevo, pero aún con la misma dirección IP del cliente.

Si se produce alguna interrupción en la red (interfaz inactiva, redes modificadas o interfaces modificadas), AnyConnect intenta volver a conectarse; no es necesario volver a autenticar la conexión al volver a conectarse. Esto incluso se aplica a un switch de interfaces físicas:

Ejemplo:

1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in 30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs

P14. ¿Cómo se autentica la operación de reanudación?

R. En un currículum, se vuelve a enviar el token autenticado que permanece durante la duración de la sesión y, a continuación, se restablece la sesión.

P15. ¿Se realiza también la autorización LDAP tras la reconexión o solo la autenticación?

R. Esto solo se realiza en la conexión inicial.

P16. ¿Se ejecuta el inicio de sesión previo y/o el hostscan al reanudar?

R. No, se ejecutan sólo en la conexión inicial. Algo como esto estaría programado para la función

de evaluación periódica de postura futura.

P17. Con respecto al Balanceo de Carga de VPN (LB) y la reanudación de la conexión, ¿el cliente se conecta directamente con el miembro del clúster al que estaba conectado antes?

R: Sí, esto es correcto ya que no vuelve a resolver el nombre de host a través de DNS para el restablecimiento de una sesión actual.

## Información Relacionada

- Referencia de DPD de ASA: ID de error de Cisco [CSCsr63074](#): DPD no se envía cuando el par está muerto y el túnel no está inactivo en s2s con 7.2.4
- [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).