Ejemplo de Configuración de Filtros VPN en Cisco ASA

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Ejemplo 1. vpn-filter with AnyConnect or VPN Client](#)
[Ejemplo 2. vpn-filter with L2L VPN Connection](#)
[Filtros VPN y grupos de acceso de anulación por usuario](#)
[Verificación](#)
[Troubleshoot](#)

Introducción

Este documento describe los filtros VPN en detalle y se aplica a LAN a LAN (L2L), Cisco VPN Client y Cisco AnyConnect Secure Mobility Client.

Los filtros constan de reglas que determinan si se deben permitir o rechazar los paquetes de datos tunelizados que pasan a través del dispositivo de seguridad, basándose en criterios como la dirección de origen, la dirección de destino y el protocolo. Las listas de control de acceso (ACL) se configuran para permitir o denegar varios tipos de tráfico. El filtro se puede configurar en la directiva de grupo, los atributos de nombre de usuario o la directiva de acceso dinámico (DAP).

DAP reemplaza el valor configurado bajo los atributos de nombre de usuario y la política de grupo. El valor del atributo username reemplaza el valor de la política de grupo en caso de que DAP no asigne ningún filtro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de túneles L2L VPN
- Configuración de acceso remoto de cliente VPN (RA)
- Configuración de AnyConnect RA

Componentes Utilizados

La información de este documento se basa en la versión 9.1(2) del dispositivo de seguridad

adaptable (ASA) de la serie 5500-X de Cisco.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

El comando **sysopt connection permit-vpn** permite que todo el tráfico que ingresa al dispositivo de seguridad a través de un túnel VPN omita las listas de acceso a la interfaz. La política de grupo y las listas de acceso de autorización por usuario siguen aplicándose al tráfico.

Un filtro vpn se aplica al tráfico postdescifrado después de salir de un túnel y al tráfico precifrado antes de entrar en un túnel. Una ACL que se utiliza para un filtro vpn NO se debe utilizar también para un grupo de acceso de interfaz.

Cuando se aplica un filtro vpn a una política de grupo que controla las conexiones del cliente VPN de acceso remoto, la ACL debe configurarse con las direcciones IP asignadas al cliente en la posición src_ip de la ACL y la red local en la posición dest_ip de la ACL. Cuando se aplica un filtro vpn a una política de grupo que gobierna una conexión VPN L2L, la ACL debe configurarse con la red remota en la posición src_ip de la ACL y la red local en la posición dest_ip de la ACL.

Configurar

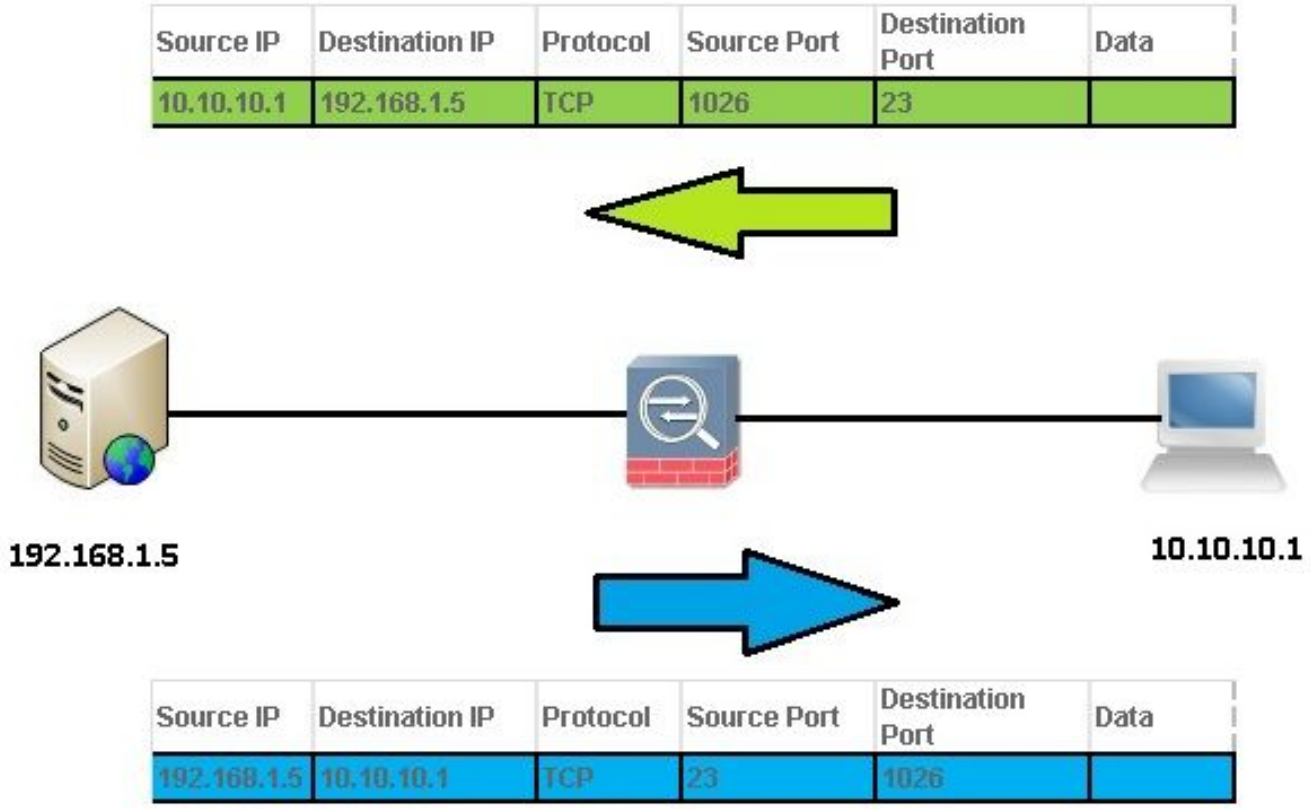
Los filtros VPN deben configurarse en dirección entrante, aunque las reglas se siguen aplicando bidireccionalmente. La mejora CSCsf99428 se ha abierto para admitir reglas unidireccionales, pero aún no se ha programado ni comprometido su implementación.

Ejemplo 1. vpn-filter with AnyConnect or VPN Client

Suponga que la dirección IP asignada por el cliente es 10.10.10.1/24 y la red local es 192.168.1.0/24.

Esta entrada de control de acceso (ACE) permite al cliente AnyConnect establecer una conexión Telnet con la red local:

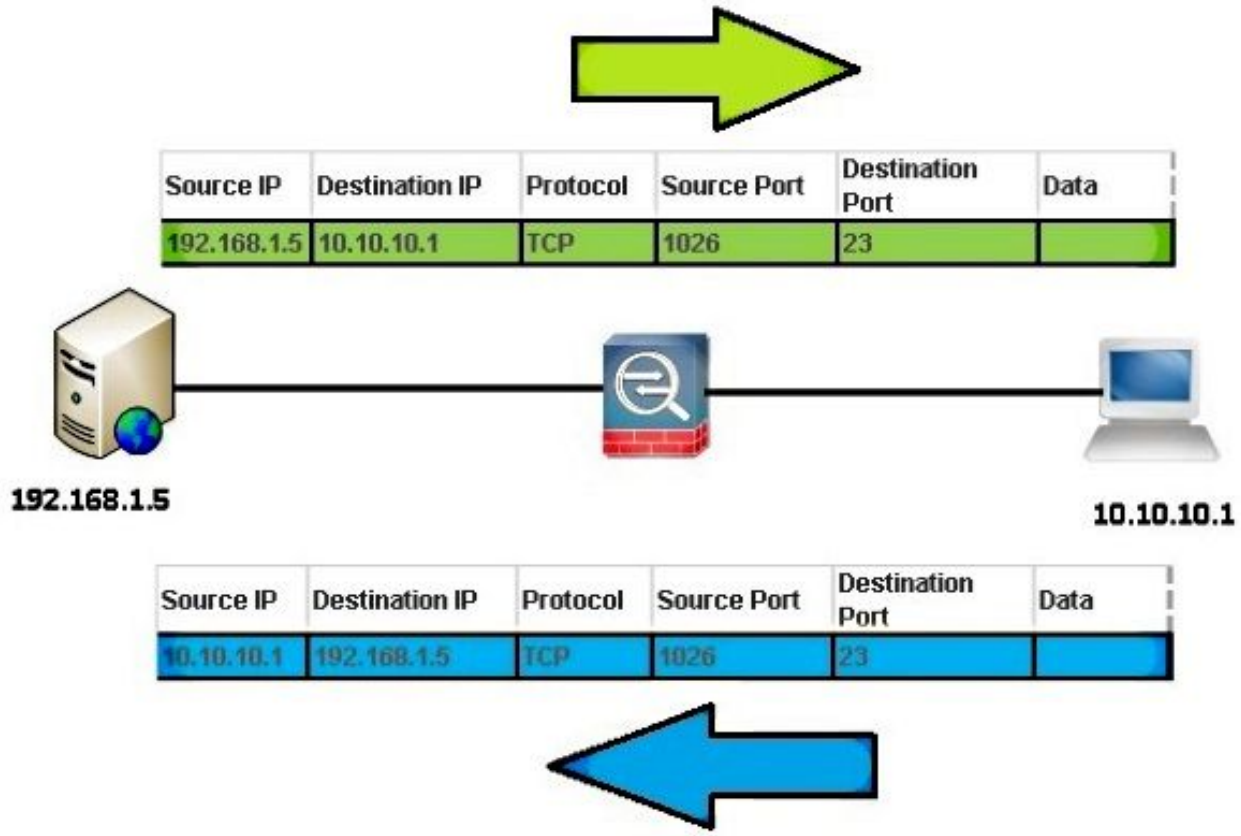
```
access-list vpnfilt-ra permit tcp
10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```



Nota: La ACE access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23 también permite que la red local inicie una conexión con el cliente RA en cualquier puerto TCP si utiliza un puerto de origen de 23.

Esta ACE permite que la red local establezca una conexión Telnet con el cliente AnyConnect:

```
access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255
eq 23 192.168.1.0 255.255.255.0
```



Nota: La ACE access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0 también permite al cliente RA iniciar una conexión a la red local en cualquier puerto TCP si utiliza un puerto de origen de 23.

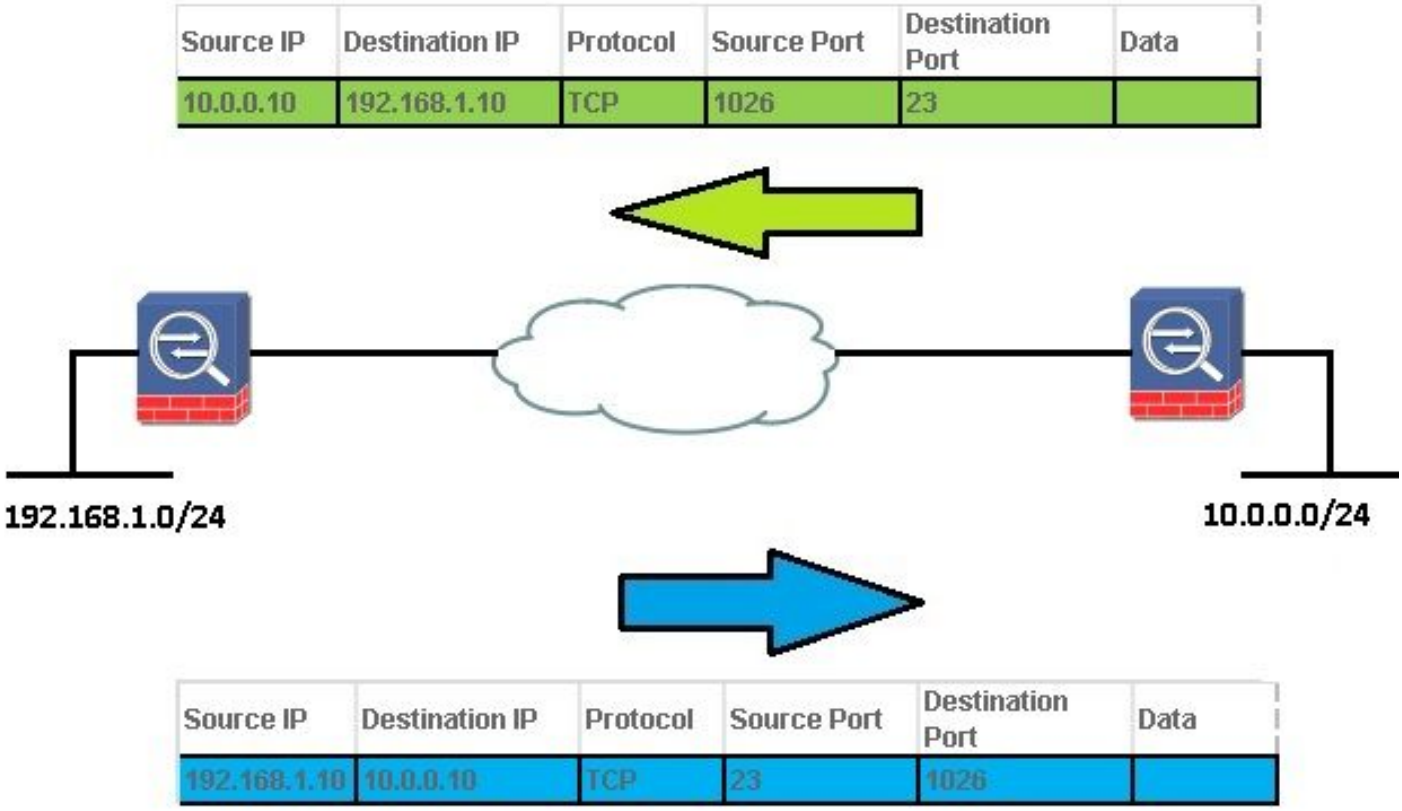
Precaución: La función vpn-filter permite que el tráfico se filtre sólo en la dirección entrante y la regla saliente se compila automáticamente. Por lo tanto, cuando cree una lista de acceso ICMP (Internet Control Message Protocol), no especifique el tipo de ICMP en el formato de la lista de acceso si desea filtros direccionales.

Ejemplo 2. vpn-filter with L2L VPN Connection

Suponga que la red remota es 10.0.0.0/24 y la red local es 192.168.1.0/24.

Esta ACE permite que la red remota establezca Telnet a la red local:

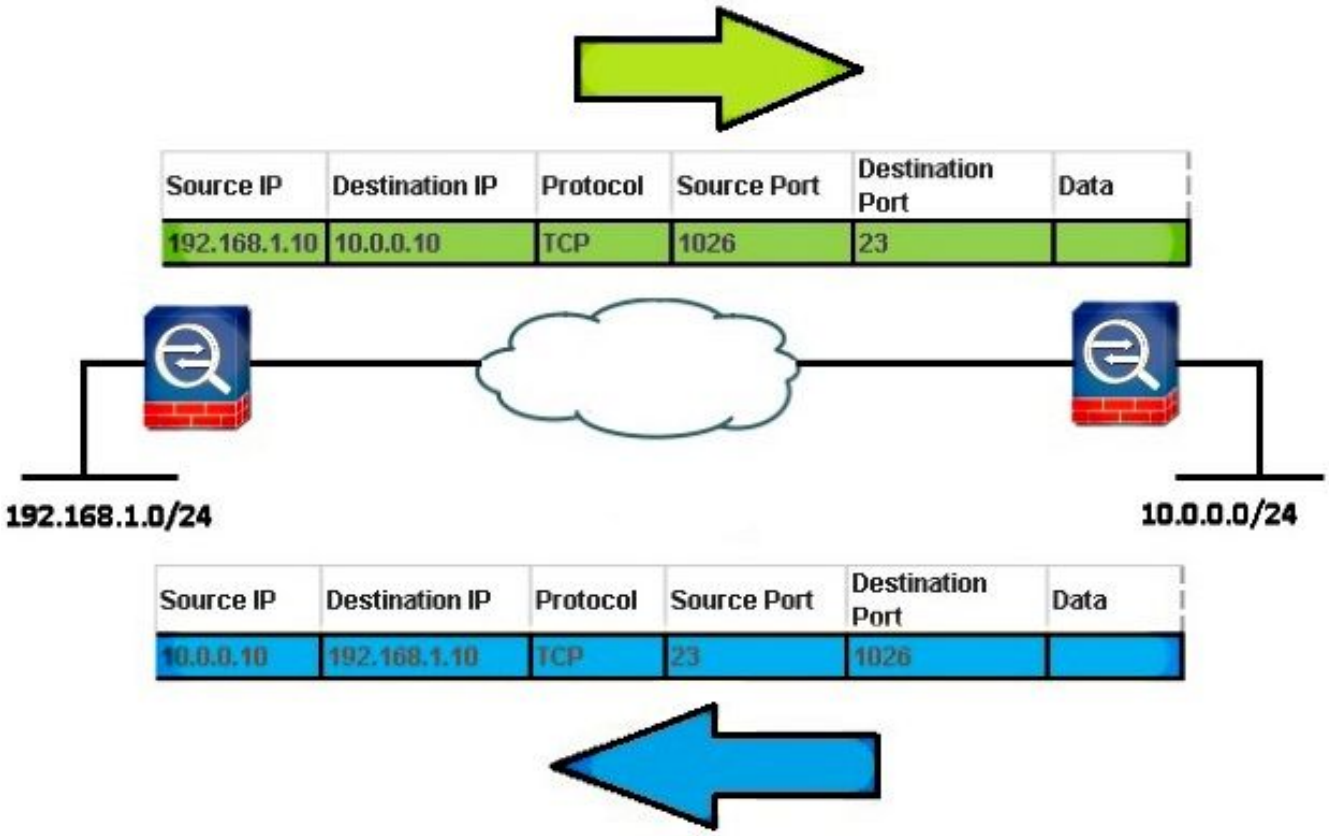
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



Nota: La ACE access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23 también permite que la red local inicie una conexión a la red remota en cualquier puerto TCP si utiliza un puerto de origen de 23.

Esta ACE permite a la red local establecer una conexión Telnet con la red remota:

```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```



Nota: La ACE access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0 también permite que la red remota inicie una conexión a la red local en cualquier puerto TCP si utiliza un puerto de origen de 23.

Precaución: La función vpn-filter permite que el tráfico se filtre sólo en la dirección entrante y la regla saliente se compila automáticamente. Por lo tanto, cuando cree una lista de acceso ICMP, no especifique el tipo ICMP en el formato de la lista de acceso si desea filtros direccionales.

Filtros VPN y grupos de acceso de anulación por usuario

El tráfico VPN no se filtra por las ACL de interfaz. El comando **no sysopt connection permit-vpn** se puede utilizar para cambiar el comportamiento predeterminado. En este caso, se pueden aplicar dos ACL al tráfico del usuario: la interfaz ACL se verifica primero y luego el filtro vpn.

La palabra clave **per-user-override** (sólo para ACL entrantes) permite ACL de usuario dinámicas que se descargan para autorización de usuario para anular la ACL asignada a la interfaz. Por ejemplo, si la ACL de interfaz niega todo el tráfico de 10.0.0.0, pero la ACL dinámica permite todo el tráfico de 10.0.0.0, entonces la ACL dinámica invalida la ACL de interfaz para ese usuario y se permite el tráfico.

Ejemplos (cuando **no** se configura **sysopt connection permit-vpn**):

- no per-user-override, no vpn-filter - el tráfico se compara con la interfaz ACL
- no per-user-override, vpn-filter: el tráfico se compara primero con la ACL de la interfaz y, a continuación, con el filtro vpn

- per-user-override, vpn-filter: el tráfico solo se compara con el filtro vpn

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show. Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

- **show asp table filter [access-list <*acl-name*>] [hits]**

  Para depurar las tablas de filtro de trayectoria de seguridad acelerada, utilice el comando **show asp table filter** en el modo EXEC privilegiado. Cuando se ha aplicado un filtro a un túnel VPN, las reglas de filtro se instalan en la tabla de filtros. Si el túnel tiene un filtro especificado, la tabla de filtros se verifica antes del cifrado y después del descifrado para determinar si se debe permitir o denegar el paquete interno.

```
 USAGE
 show asp table filter [access-list
```

```
 SYNTAX <acl-name>      Show installed filter for access-list <acl-name>
hits Show filter rules which have non-zero hits values
```

- **clear asp table filter [access-list <*acl-name*>]**

  Este comando borra los contadores de visitas para las entradas de la tabla de filtros ASP.

```
 USAGE
clear asp table filter [access-list
```

```
 SYNTAX
<acl-name> Clear hit counters only for specified access-list <acl-name>
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show. Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

> **Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

- **debug acl filter**

  Este comando habilita la depuración de filtros VPN. Se puede utilizar para ayudar a solucionar problemas de instalación o eliminación de los filtros VPN en la tabla de filtros ASP. Para el ejemplo 1. vpn-filter con AnyConnect o VPN Client.

  Salida de depuración cuando el usuario 1 se conecta:

```
 ACL FILTER INFO: first reference to inbound filter vpnfilt-ra(2): Installing
rule into NP.
ACL FILTER INFO: first reference to outbound filter vpnfilt-ra(2): Installing
rule into NP.
```

  Salida de depuración cuando el usuario 2 se conecta (después del usuario 1 y el mismo filtro):

```
 ACL FILTER INFO: adding another reference to outbound filter vpnfilt-ra(2): refCnt=2
ACL FILTER INFO: adding another reference to inbound filter vpnfilt-ra(2): refCnt=2
```

  Salida de depuración cuando el usuario 2 se desconecta:

```
 ACL FILTER INFO: removing a reference from inbound filter vpnfilt-ra(2): remaining
refCnt=1
ACL FILTER INFO: removing a reference from outbound filter vpnfilt-ra(2): remaining
refCnt=1
```

  Resultado de depuración cuando user1 se desconecta:

```
 ACL FILTER INFO: releasing last reference from inbound filter vpnfilt-ra(2): Removing
rule into NP.
ACL FILTER INFO: releasing last reference from outbound filter vpnfilt-ra(2): Removing
rule into NP.
```

- **show asp table**

  Este es el resultado de **show asp table filter** antes de cuando el usuario 1 se conecta. Sólo las reglas de denegación implícitas se instalan para IPv4 e IPv6 en las direcciones de entrada y salida.

```
 Global Filter Table:
in id=0xd616ef20, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0
in id=0xd616f420, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
src ip=::/0, port=0
dst ip=::/0, port=0
out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
src ip=::/0, port=0
dst ip=::/0, port=0
```

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).