Filtros VPN en el ejemplo de la configuración de ASA de Cisco

Contenido

Introducción

Este documento describe los filtros VPN detalladamente y se aplica al LAN a LAN (L2L), al Cliente Cisco VPN, y al Cliente de movilidad Cisco AnyConnect Secure.

Los filtros consisten en las reglas que determinan si permitir o rechazar los paquetes de datos tunneled que vienen a través del dispositivo de seguridad, sobre la base de los criterios tales como dirección de origen, dirección destino, y protocolo. Usted configura tipos de tráfico del permit or deny del Listas de control de acceso (ACL) para los diversos. El filtro se puede configurar en la directiva del grupo, los atributos del nombre de usuario, o la directiva del acceso dinámico (DAP).

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

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- El L2L VPN hace un túnel la configuración
- Configuración del Acceso Remoto del cliente VPN (RA)
- Configuración de AnyConnect RA

Componentes Utilizados

La información en este documento se basa en la versión 9.1(2) adaptante del dispositivo de seguridad de las Cisco 5500-X Series (ASA).

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El comando de permiso-**VPN de la conexión del sysopt** permite todo el tráfico que ingresa el dispositivo de seguridad a través de un túnel VPN para desviar las Listas de acceso de la interfaz. La directiva del grupo y por usuario las Listas de acceso de la autorización todavía se aplica al tráfico.

Un vpn-filtro se aplica al tráfico postdecrypted después de que salga un túnel y al tráfico preencrypted antes de que ingrese un túnel. Un ACL que isused para un VPN-filtro no se debe también utilizar para un acceso-grupo de la interfaz.

Cuando un VPN-filtro se aplica a una grupo-directiva que gobierne las conexiones del cliente VPN de acceso remoto, el ACL se debe configurar con los IP Address asignados del cliente en la posición del src_ip del ACL y la red local en la posición del dest_ip del ACL. Cuando un VPN-filtro se aplica a una grupo-directiva que gobierne una conexión VPN L2L, el ACL se debe configurar con la red remota en la posición del src_ip del ACL y la red local en la posición del dest_ip del ACL.

Configurar

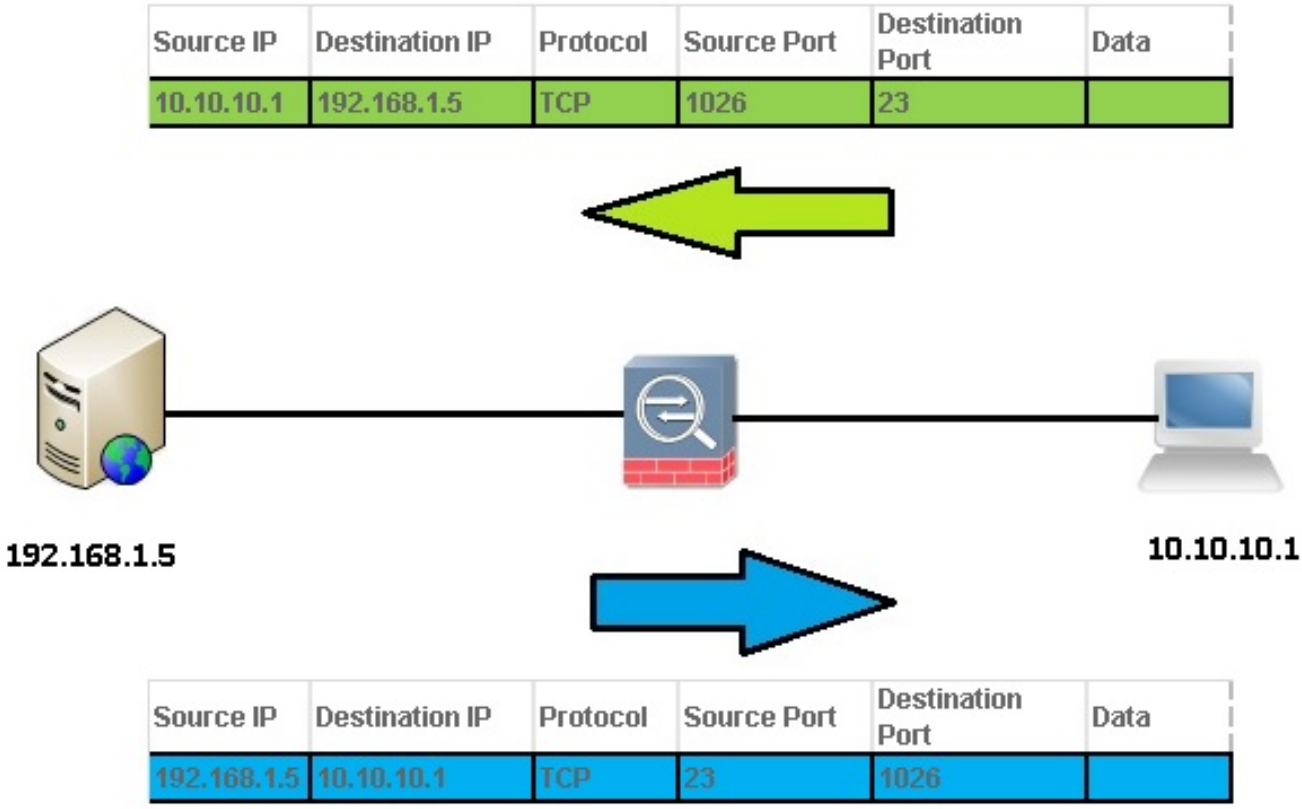
Los filtros VPN se deben configurar en la dirección entrante aunque las reglas todavía se apliquen bidireccional. La mejora CSCsf99428 se ha abierto para soportar las reglas unidireccionales, pero todavía no se ha programado/ha estado confiada para la implementación.

VPN-filtro del ejemplo 1. con AnyConnect o el cliente VPN

Asuma que la dirección IP asignada al 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 de AnyConnect a Telnet a la red local:

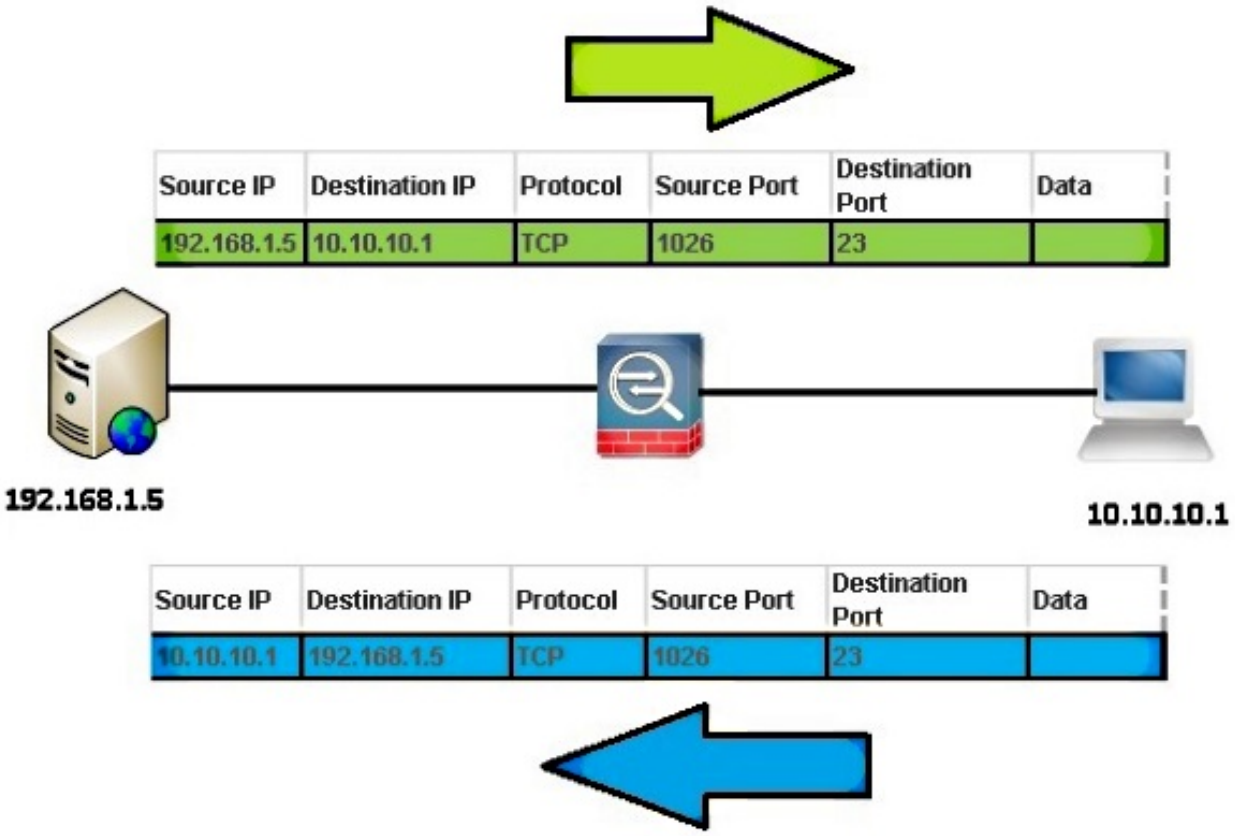
```
access-list vpnfilt-ra permit tcp
10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```



Nota: El eq 23 tcp 10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 del permiso del vpnfilt-ra de la lista de acceso de ACE también permite que la red local inicie una conexión al cliente RA en cualquier puerto TCP si utiliza un puerto de origen de 23.

Este ACE permite la red local a Telnet al cliente de 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: El eq 23 192.168.1.0 255.255.255.0 tcp 10.10.10.1 255.255.255.255 del permiso del vpnfilt-ra de la lista de acceso de ACE también permite que el cliente RA inicie una conexión a la red local en cualquier puerto TCP si utiliza un puerto de origen de 23.

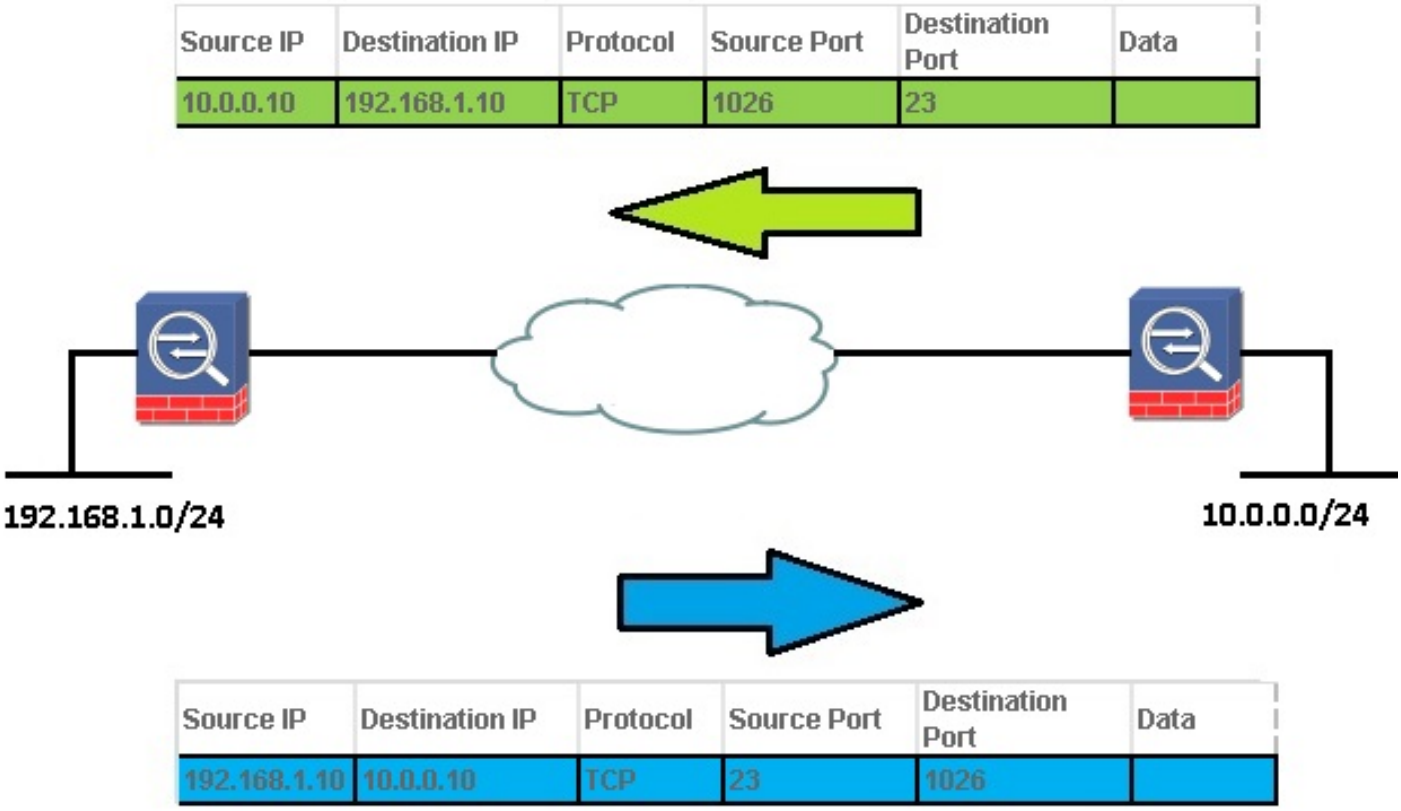
Precaución: La característica del VPN-filtro permite para que el tráfico sea filtrado en la dirección entrante solamente y la regla saliente se compila automáticamente. Por lo tanto, cuando usted crea una lista de acceso del Internet Control Message Protocol (ICMP), no especifique el ICMP teclean adentro el formato de la lista de acceso si usted quiere los filtros direccionales.

VPN-filtro del ejemplo 2. con la conexión VPN L2L

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

Este ACE permite la red remota a Telnet a la red local:

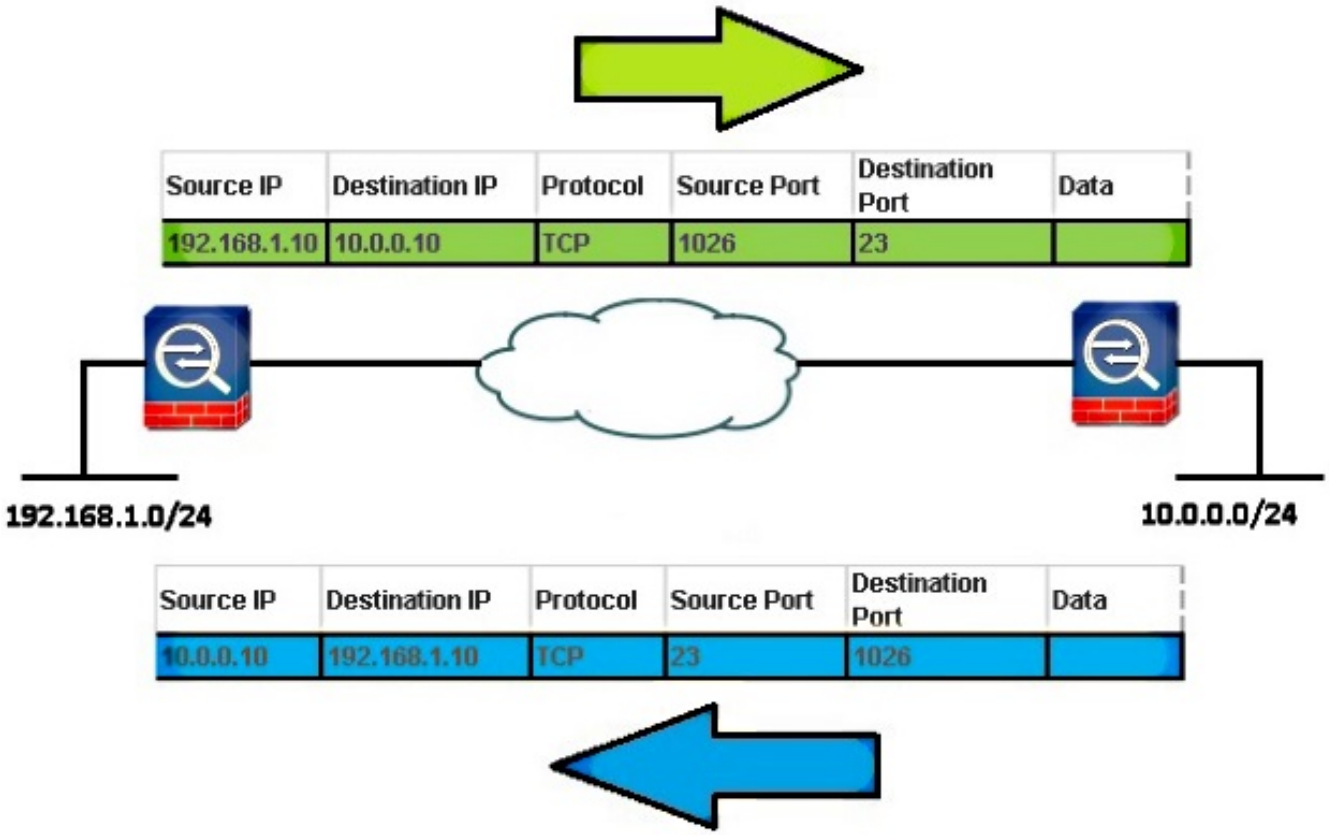
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



Nota: El eq 23 tcp 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 del permiso de la lista de acceso vpnfilt-l2l de ACE 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.

Este ACE permite la red local a Telnet a 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: El eq 23 192.168.1.0 255.255.255.0 tcp 10.0.0.0 255.255.255.0 del permiso de la lista de acceso vpnfilt-l2l de ACE 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 característica del VPN-filtro permite para que el tráfico sea filtrado en la dirección entrante solamente y la regla saliente se compila automáticamente. Por lo tanto, cuando usted crea una lista de acceso ICMP, no especifique el ICMP teclean adentro el formato de la lista de acceso si usted quiere los filtros direccionales.

Filtros VPN y grupos de acceso de la por-usuario-invalidación

El tráfico VPN no es filtrado por la interfaz ACL. El comando **ninguna conexión permiso-VPN del sysopt** se puede utilizar para cambiar el comportamiento predeterminado. En este caso, dos ACL se pueden aplicar al tráfico de usuarios: la interfaz ACL primero y después se marca el VPN-filtro.

La palabra clave de la por-usuario-**invalidación** (para ACL entrantes solamente) permite al usuario dinámico ACL que se descarga para la autorización de usuario para reemplazar el ACL asignado a la interfaz. Por ejemplo, si la interfaz ACL niega todo el tráfico de 10.0.0.0, solamente el ACL dinámico permite todo el tráfico de 10.0.0.0, después el ACL dinámico reemplaza la interfaz ACL para ese usuario y se permite el tráfico.

Ejemplos (cuando no se configura **ninguna conexión permiso-VPN del sysopt**):

- ninguna por-usuario-invalidación, ningún VPN-filtro - el tráfico se corresponde con contra la interfaz ACL

- ninguna por-usuario-invalidación, VPN-filtro - el tráfico se corresponde con primero contra la

interfaz ACL, entonces contra el VPN-filtro

- por-usuario-invalidación, VPN-filtro - el tráfico se corresponde con contra el VPN-filtro solamente

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.

- **muestre el [hits] del [access-list <acl-name>] del filtro de la tabla ASP**

  Para hacer el debug de las tablas aceleradas del filtro de la trayectoria de la Seguridad, utilice el comando del **filtro de la tabla de la demostración ASP** en el modo EXEC privilegiado. Cuando un filtro se ha aplicado a un túnel VPN, las reglas para filtros están instaladas en la tabla del filtro. Si el túnel tiene un filtro especificado, después la tabla del filtro se marca antes del cifrado y después de que desciframiento para determinar si el paquete interno debe ser permitido o ser negado.

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

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

- **borre el [access-list <acl-name>] del filtro de la tabla ASP**

  Este comando borra a los contadores de aciertos para las entradas de tabla del filtro ASP.

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

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

Troubleshooting

Esta sección brinda información que puede utilizar para la solución de 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**.

- **haga el debug del filtro acl**

  Este comando habilita el debugging del filtro VPN. Puede ser utilizado para ayudar a resolver problemas las instalaciones/retiro de los filtros VPN en la tabla del filtro ASP. Para el VPN-filtro del ejemplo 1. con AnyConnect o el cliente VPN.

  Salida de los debugs cuando el user1 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 los debugs cuando user2 conecta (después del user1 y del 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 los debugs cuando user2 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
```

  Salida de los debugs cuando el user1 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.
```

- **muestre la tabla ASP**

  Aquí está la salida del **filtro de la tabla de la demostración ASP** antes de cuando el user1 conecta. Solamente el implícitos niegan las reglas están instalados para el IPv4 y el IPv6 en ambos en y hacia fuera las direcciones.

```
 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
```