ASA/PIX: Ejemplo de Configuración Cómo habilitar la Tunelización Dividida para los Clientes VPN en ASA

Contenido

Introducción

Este documento proporciona instrucciones paso a paso sobre cómo conceder a los clientes VPN acceso a Internet mientras que son tunelizados en un dispositivo de seguridad Cisco Adaptive Security Appliance (ASA) 5500 Series. Esta configuración concede a los clientes VPN acceso seguro a los recursos corporativos a través de IPsec, mientras que concede acceso no seguro a Internet.

Nota: El Tunelización lleno se considera la configuración más segura porque no habilita el acceso del dispositivo simultáneo a Internet y al LAN corporativo. Un compromiso entre el Tunelización y el Túnel dividido llenos no prohibe a clientes VPN el acceso del LAN local solamente. Consulte PIX/ASA 7.x: Permita el acceso del LAN local para el ejemplo de configuración de los clientes VPN para más información.

prerrequisitos

Requisitos

Este documento asume que una configuración de trabajo del VPN de acceso remoto existe ya en el ASA. Refiera al PIX/ASA 7.x como servidor VPN remoto que usa el ejemplo de la Configuración de ASDM si uno no se configura ya.

Componentes Utilizados

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

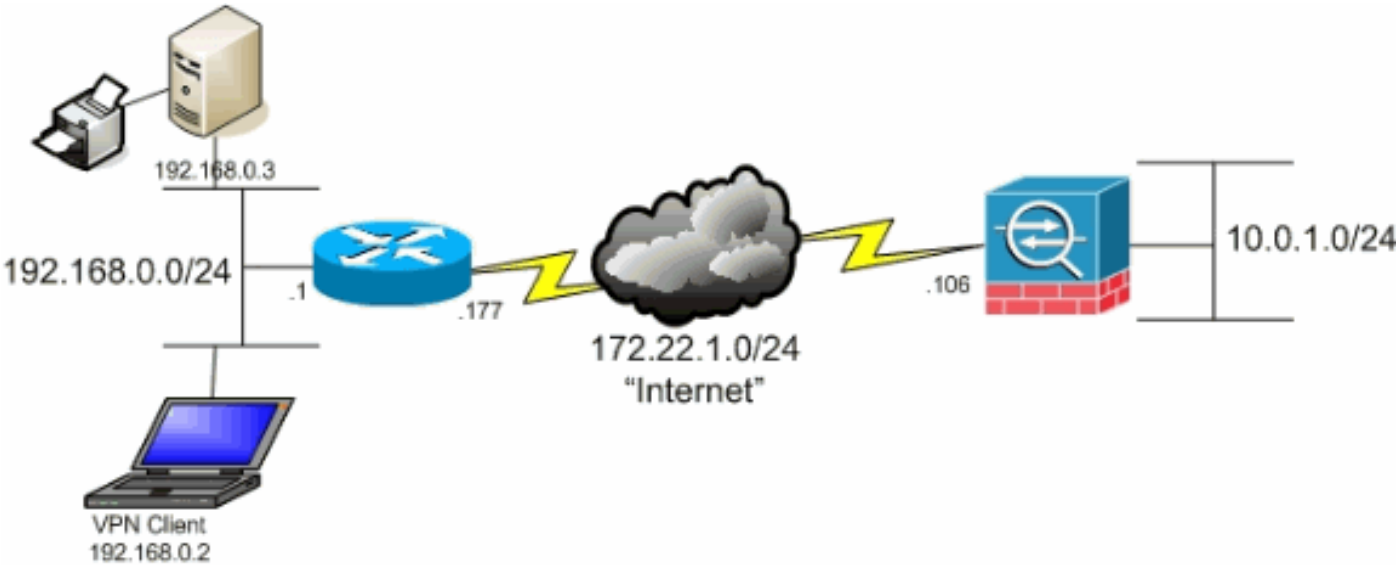
- Versión de software 7.x del dispositivo de seguridad de las 5500 Series de Cisco ASA y posterior
- Versión 4.0.5 del cliente VPN de Cisco Systems

Nota: Este documento también contiene la configuración CLI PIX 6.x que es compatible para el Cliente Cisco VPN 3.x.

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.

Diagrama de la red

El cliente VPN está situado en las redes SOHO típicas y conecta a través de Internet con la oficina principal.



Productos Relacionados

Esta configuración se puede también utilizar con la versión de software 7.x del dispositivo de seguridad de la serie del Cisco PIX 500.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

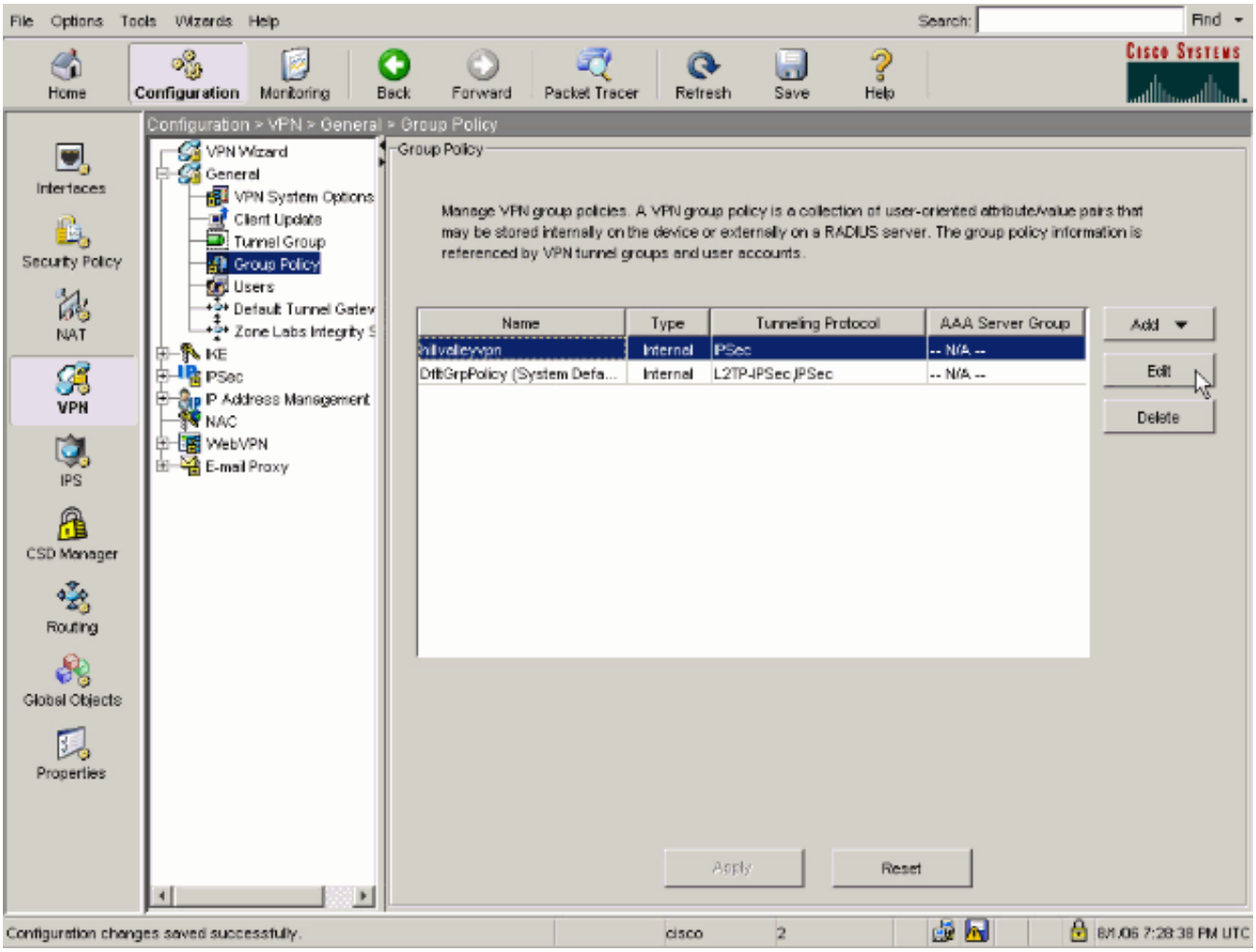
En un cliente VPN básico al escenario ASA, todo el tráfico del cliente VPN se cifra y se envía al ASA no importa qué es su destino. De acuerdo con su configuración y el número de usuarios soportados, tal configuración puede convertirse en intensidad de ancho de banda. El Túnel dividido puede trabajar para paliar este problema puesto que permite que los usuarios envíen solamente ese tráfico que sea destinado para la red corporativa a través del túnel. El resto del tráfico tal como Mensajería inmediata, correo electrónico, u ojeada casual se envía a Internet vía el LAN local del cliente VPN.

Túnel dividido de la configuración en el ASA

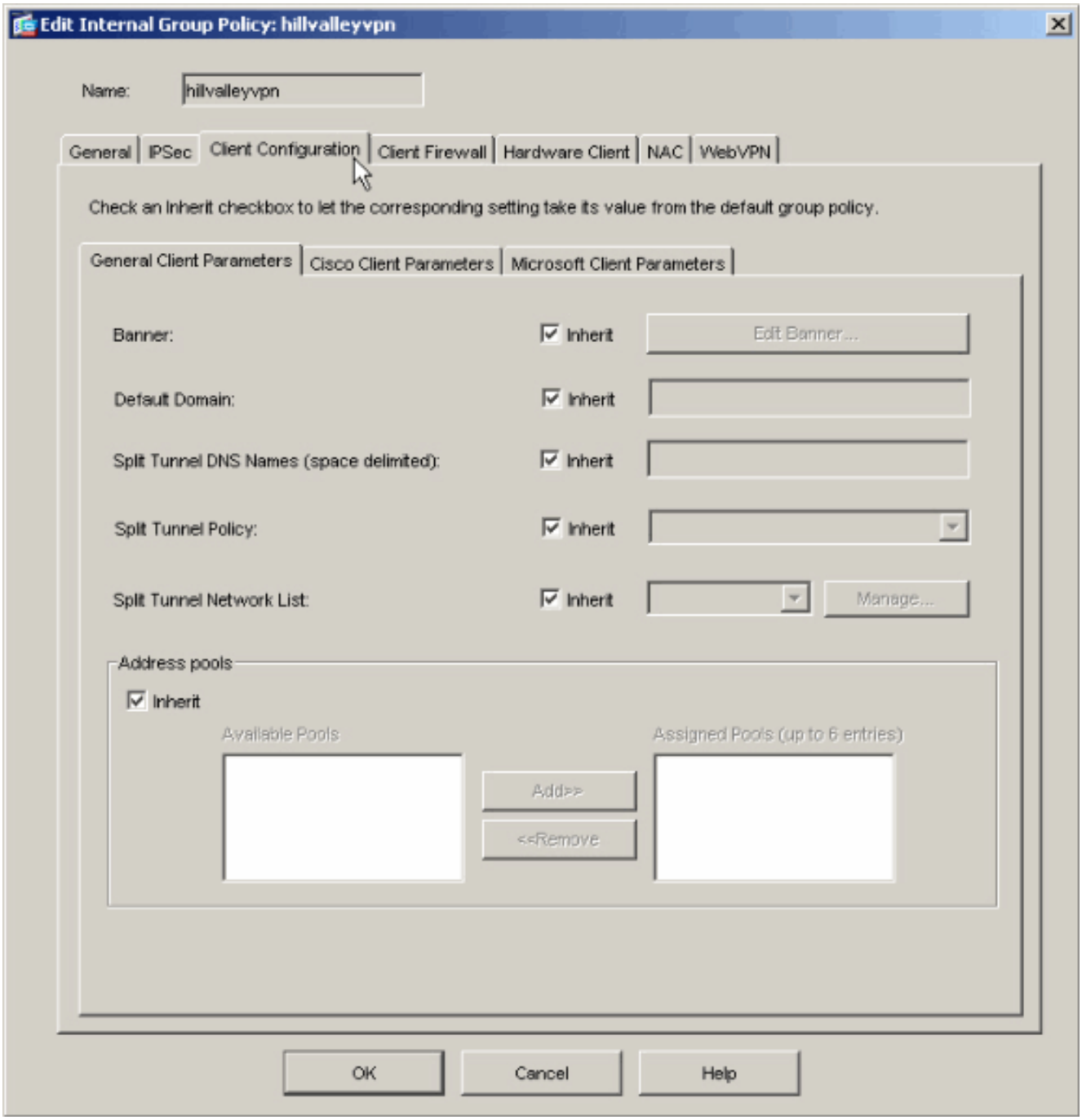
Configure el ASA 7.x con el Administrador de dispositivos de seguridad adaptante (ASDM) 5.x

Complete estos pasos para configurar a su grupo de túnel para permitir el Túnel dividido para los usuarios en el grupo.

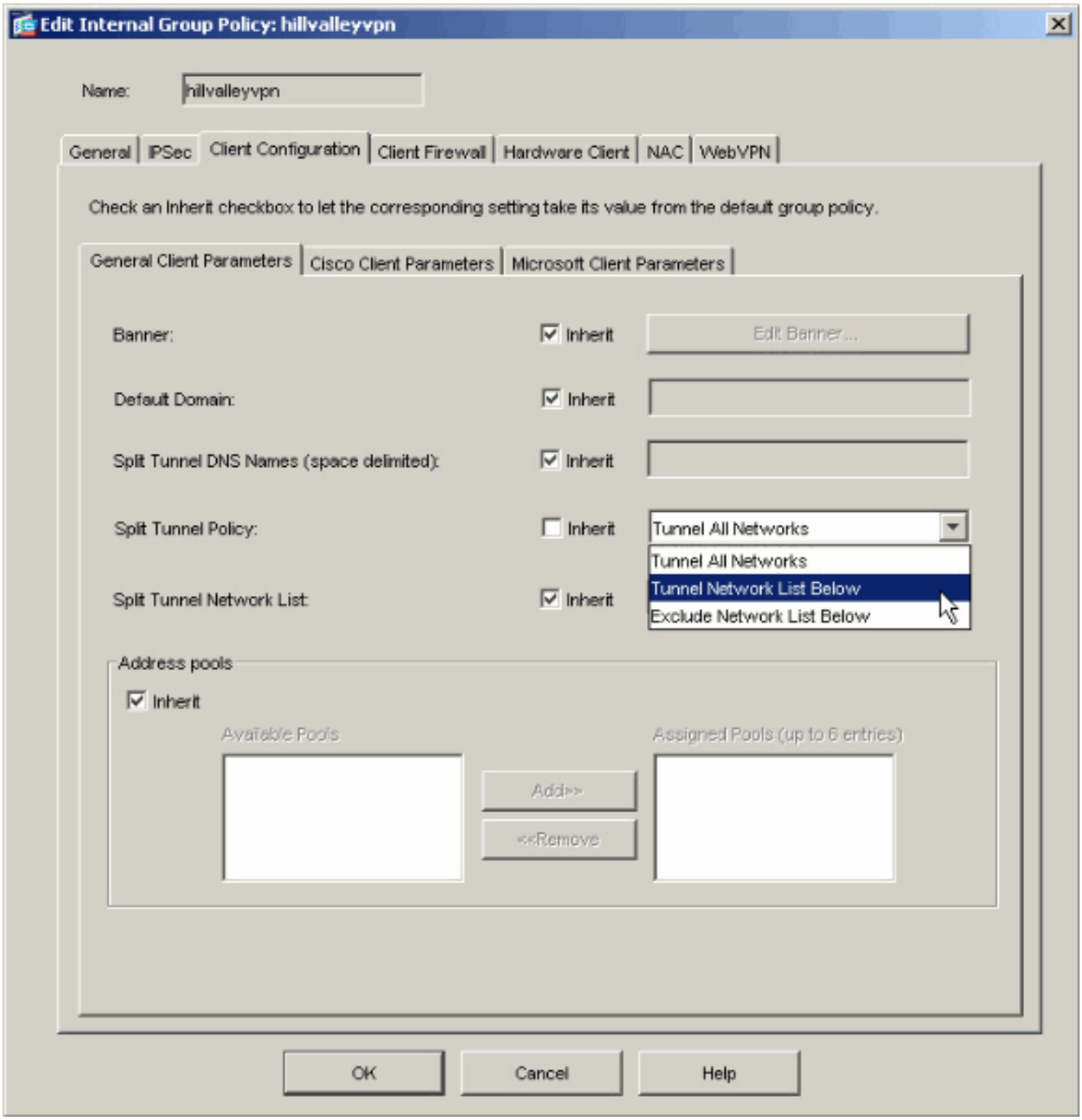
1. Elija la **configuración > el VPN > la directiva del general > del grupo** y seleccione la directiva del grupo que usted desea habilitar el acceso del LAN local adentro. Entonces haga clic **editan**.



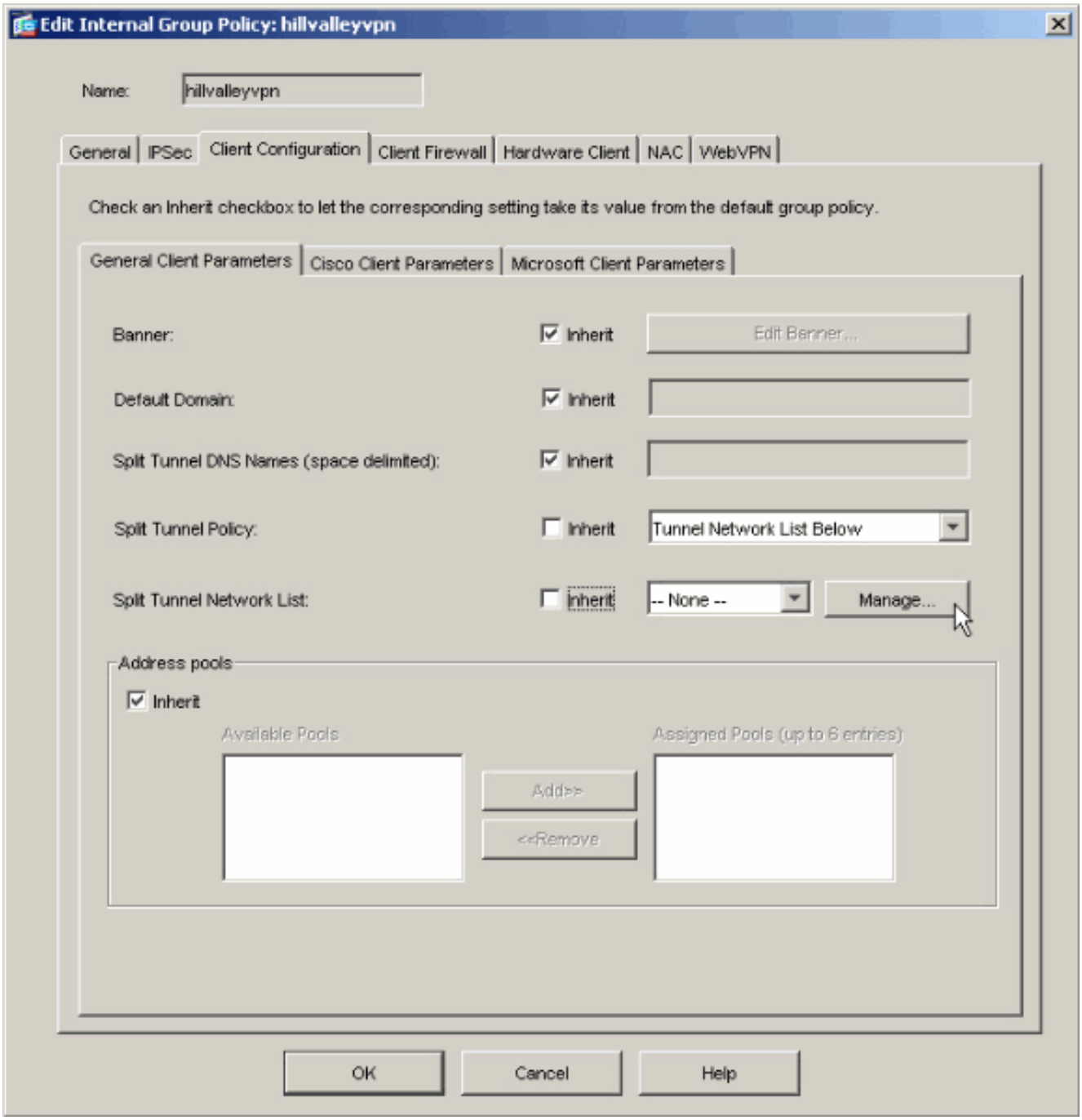
2. Vaya a la lengueta de la configuración del cliente.



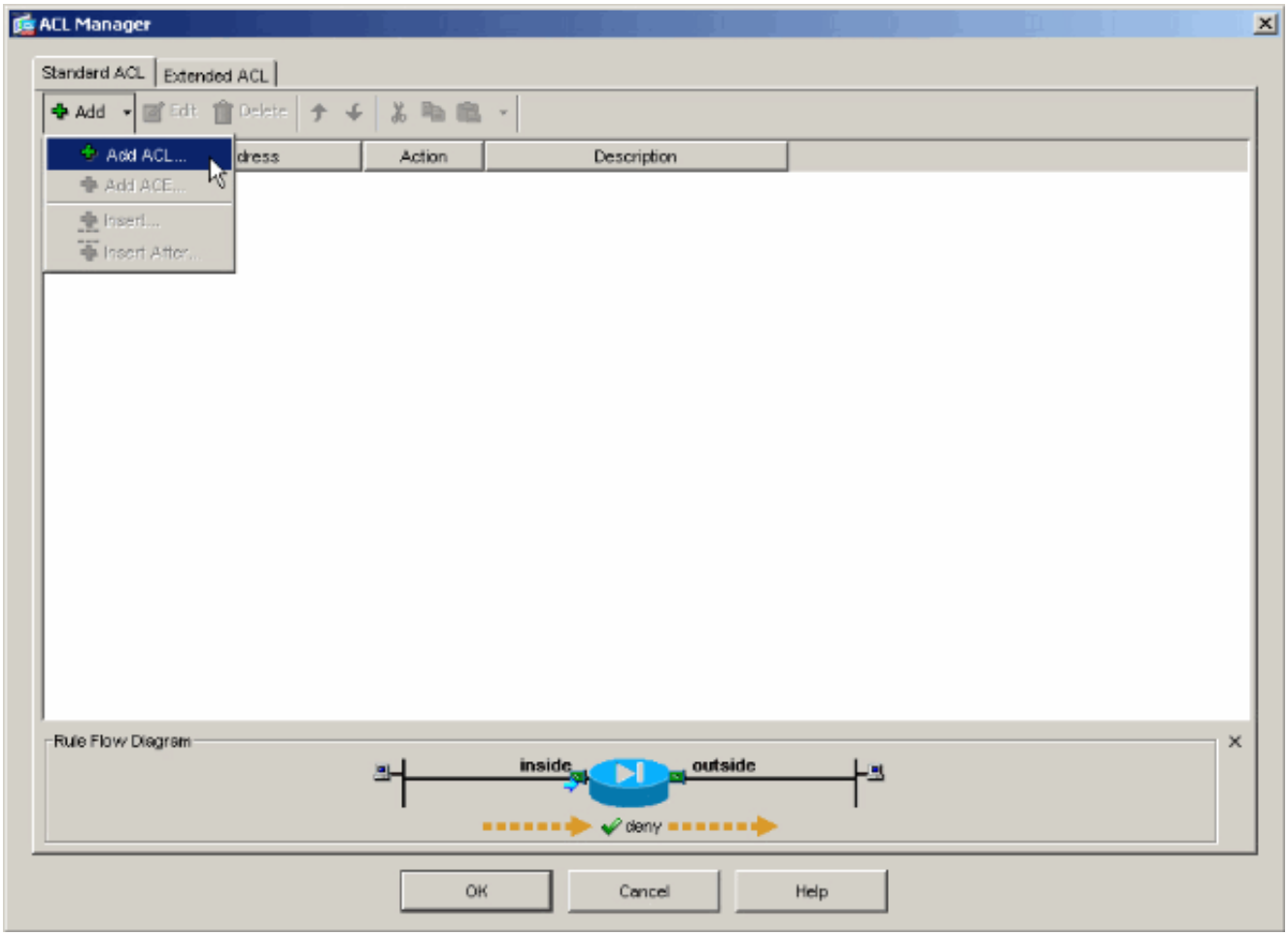
3. Desmarque el cuadro de la **herencia** para la directiva del túnel dividido y eligió la **lista de la red de túneles**
abajo.



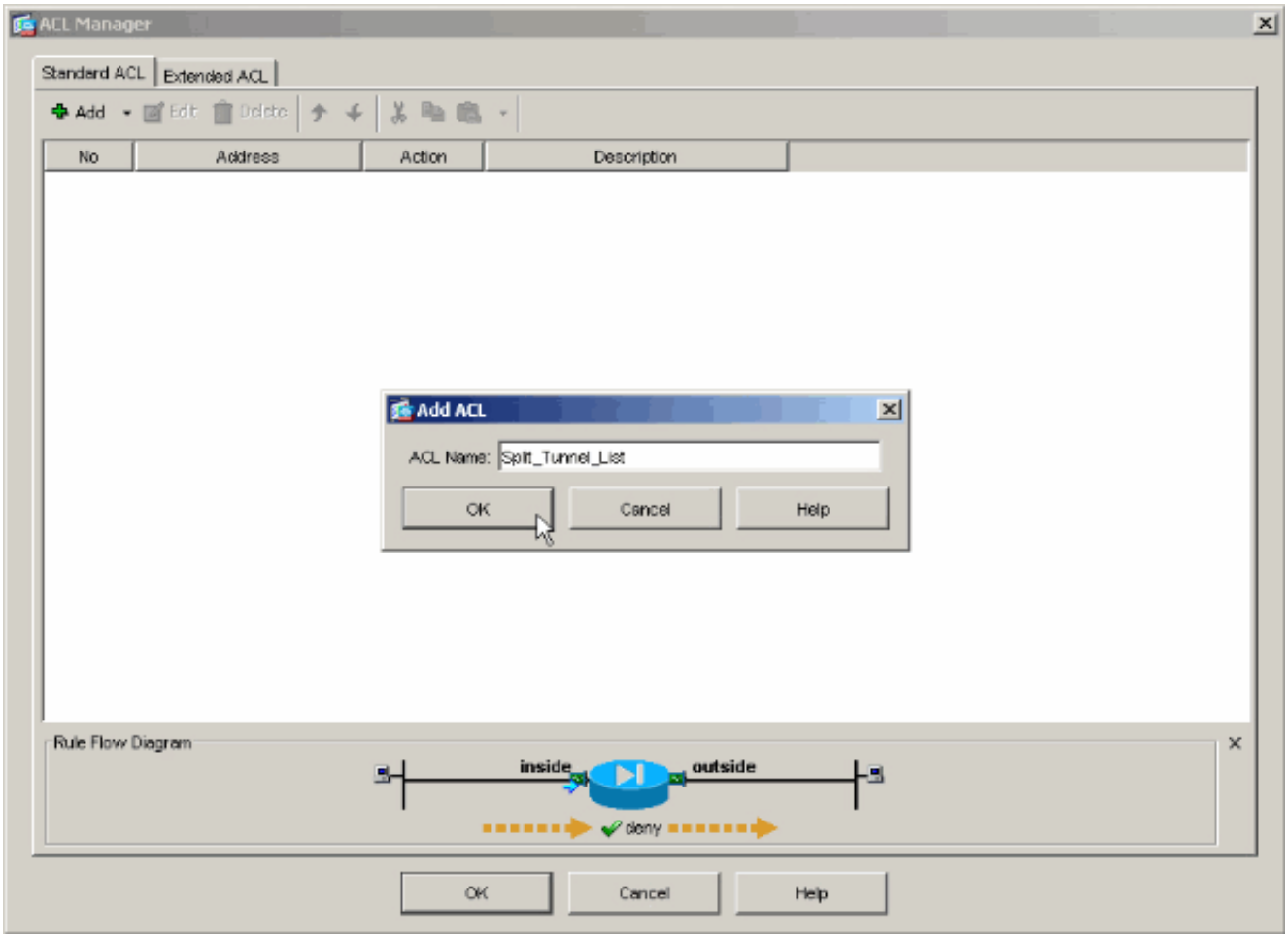
4. Desmarque el cuadro de la **herencia** para la lista de red del túnel dividido y después haga clic **manejan** para iniciar el ACL
   Manager.



5. Dentro del Administrador de ACL, elija **Add > Add ACL...** para crear una nueva lista de acceso.

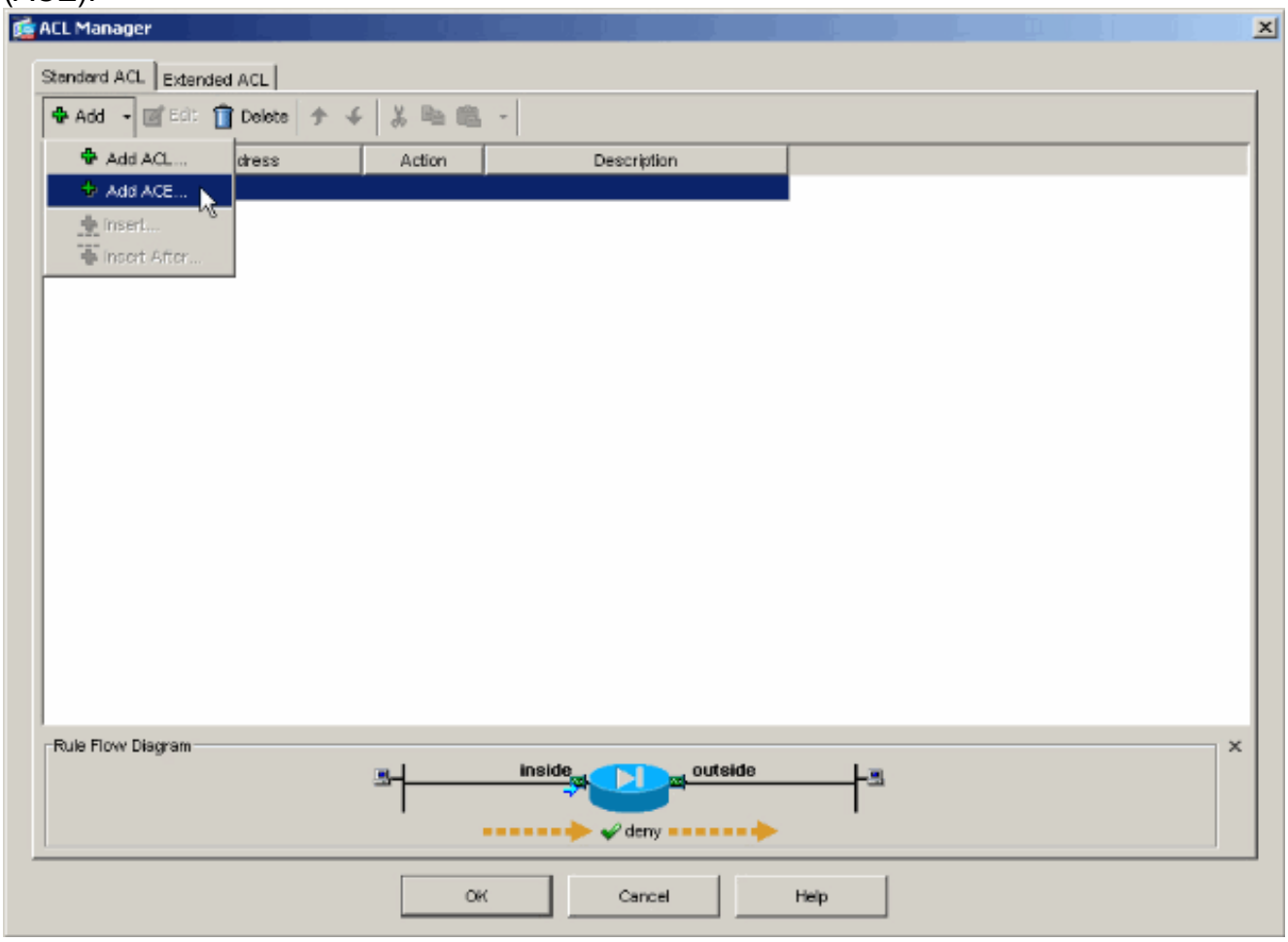


6. Asigne un nombre al ACL y haga clic en **OK**.

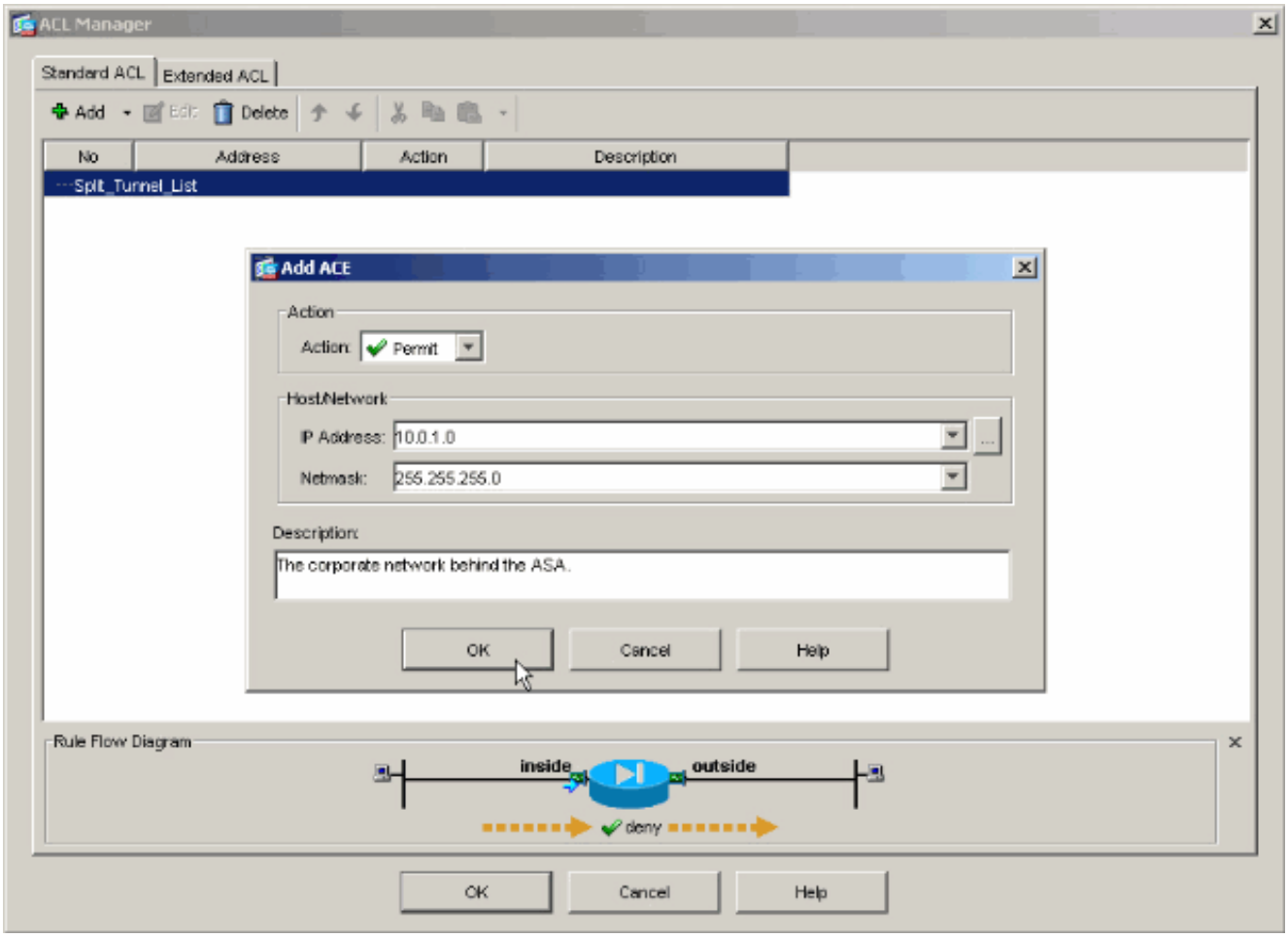


7. Una vez que se crea el ACL, elija **agregan > Add ACE...** para agregar una Entrada de

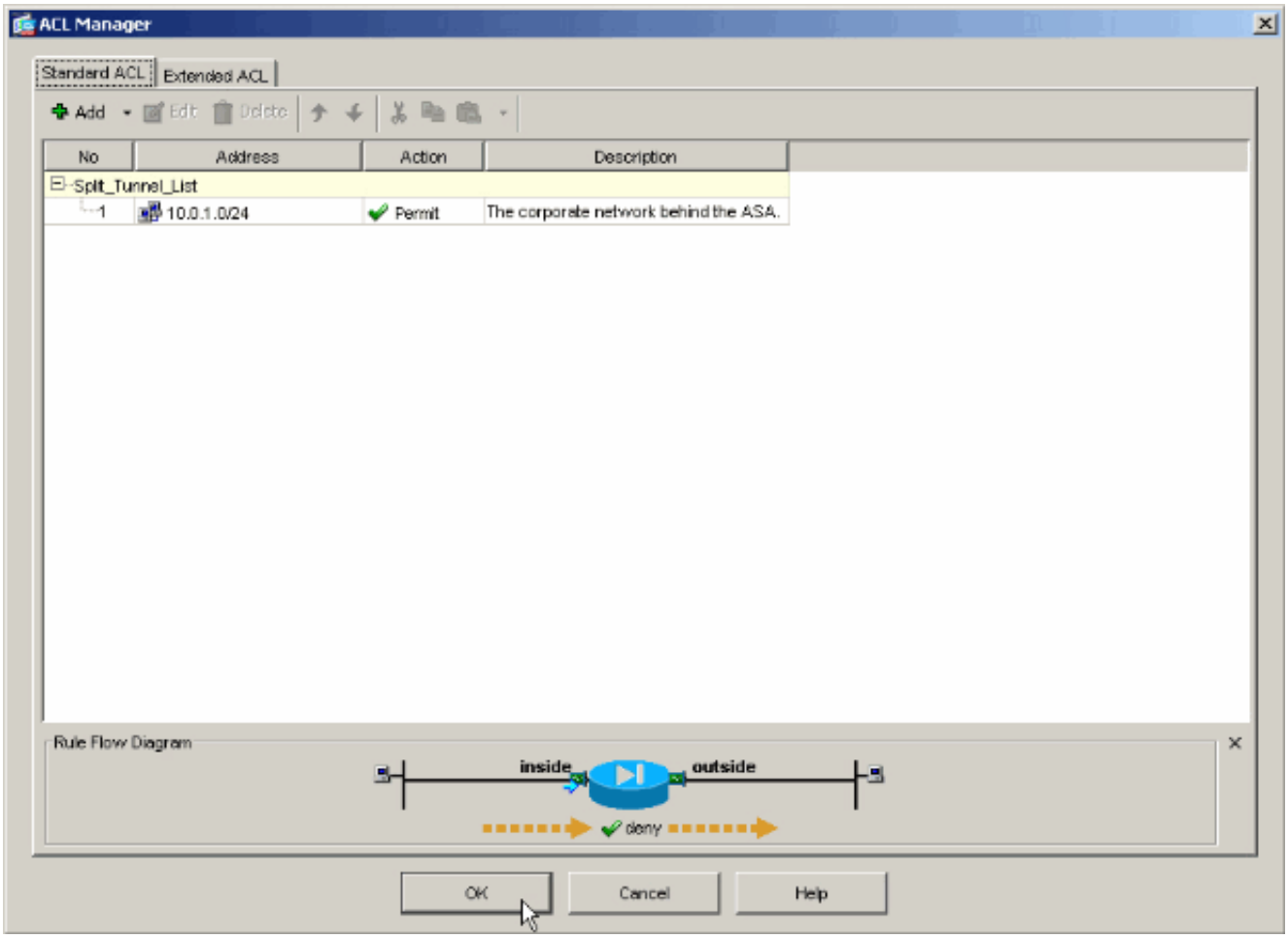
control de acceso
(ACE).



8. Defina el ACE que corresponde al LAN detrás del ASA. En este caso, la red es 10.0.1.0/24.Elija el **permiso**.Elija una dirección IP de **10.0.1.0**Elija un netmask de **255.255.255.0**.*(Opcional)* proporcione una descripción.Haga clic en OK.

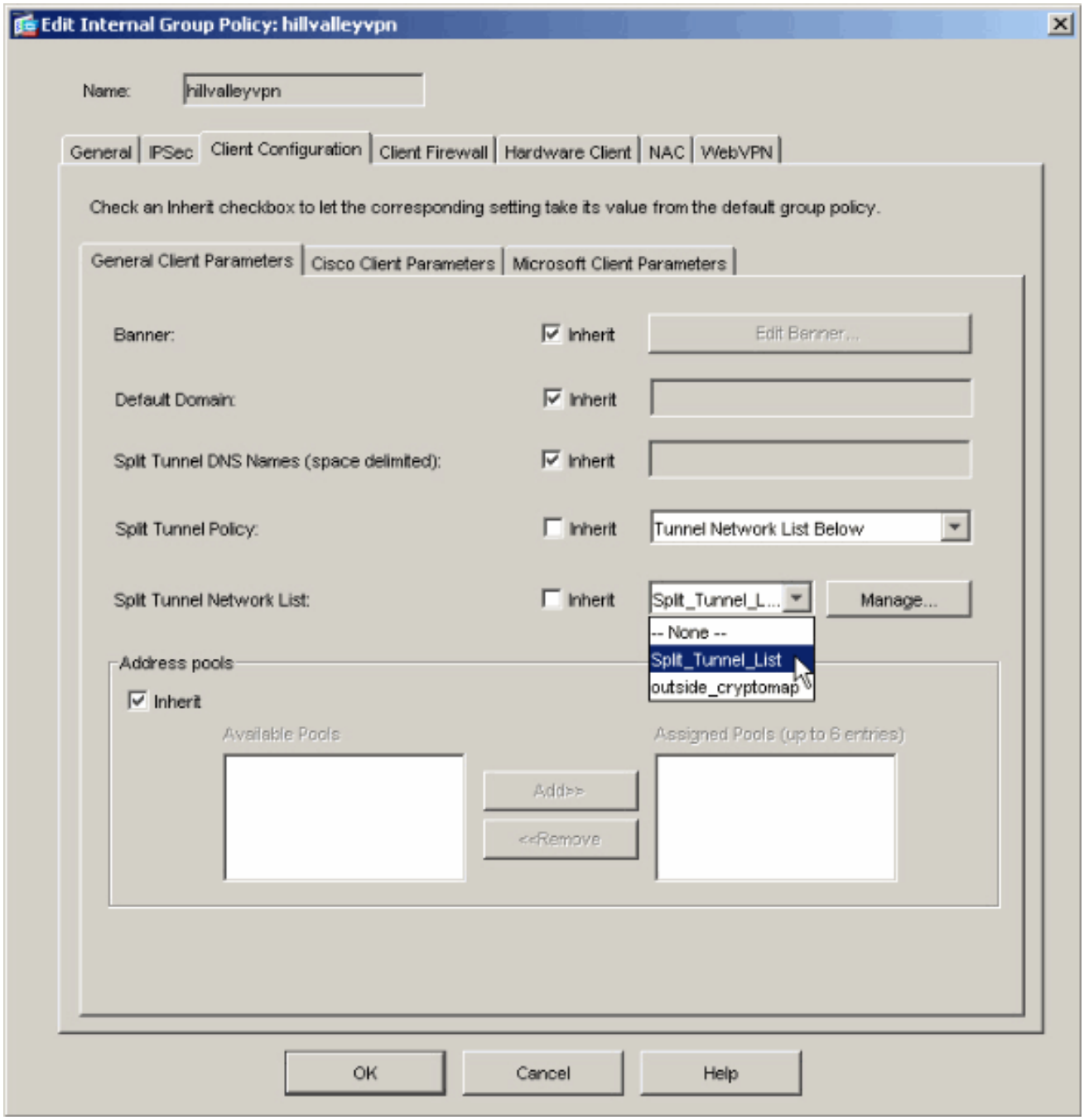


9. Haga clic en OK para salir del Administrador de ACL.

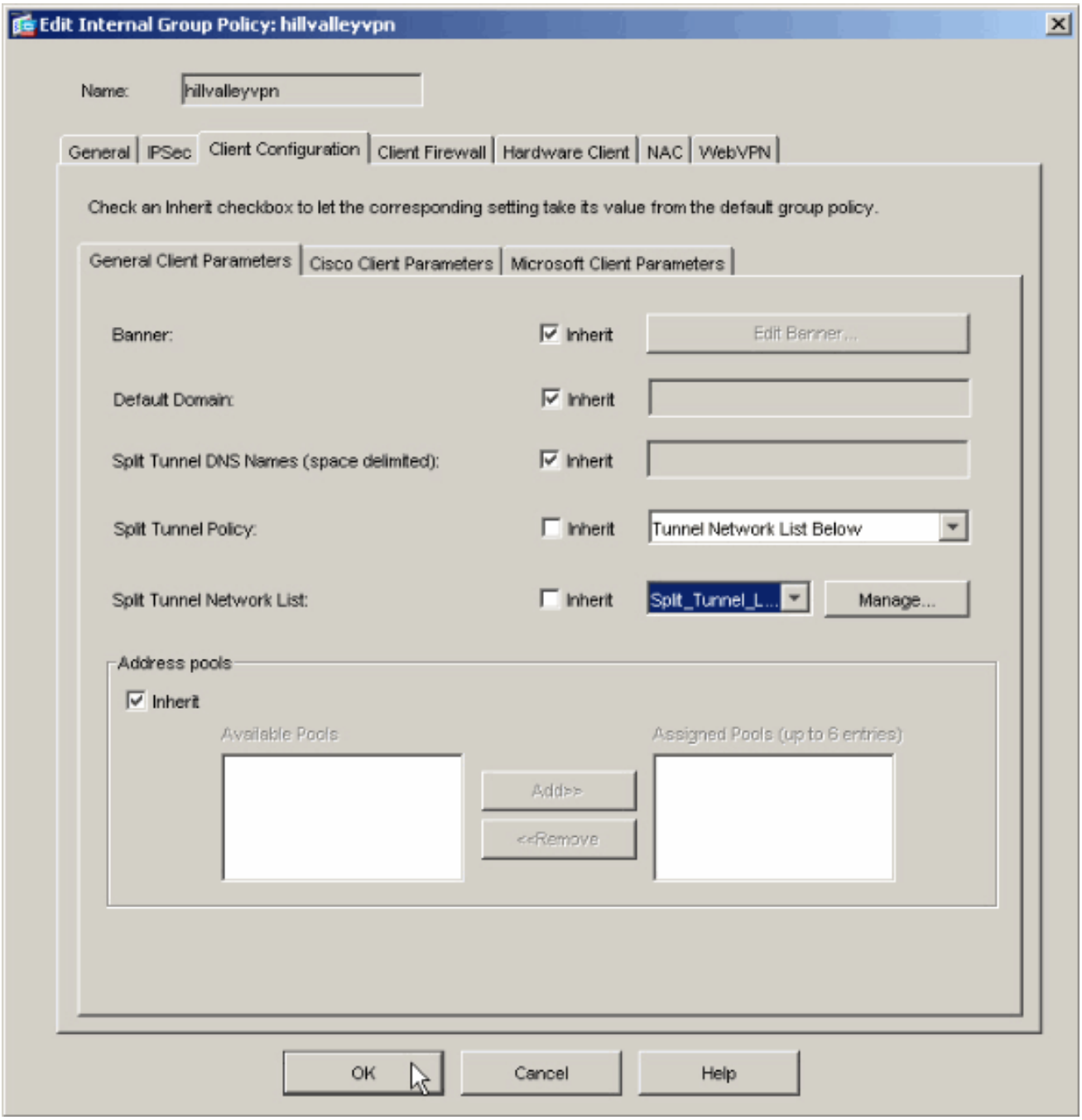


10. Esté seguro que el ACL que usted acaba de crear está seleccionado para la lista de red del

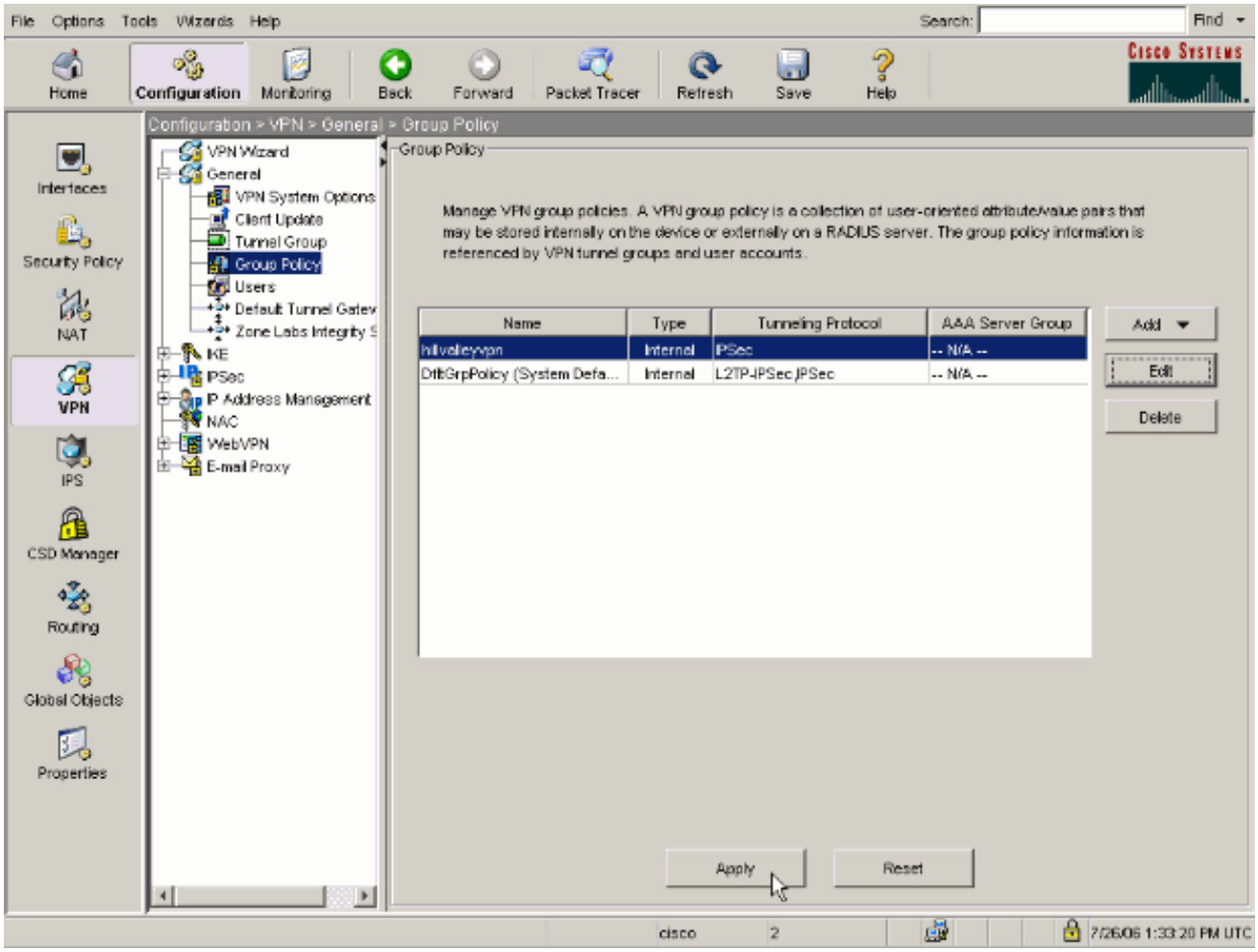
túnel
dividido.



11. Haga clic en OK para volver a la configuración de la Política de Grupo.



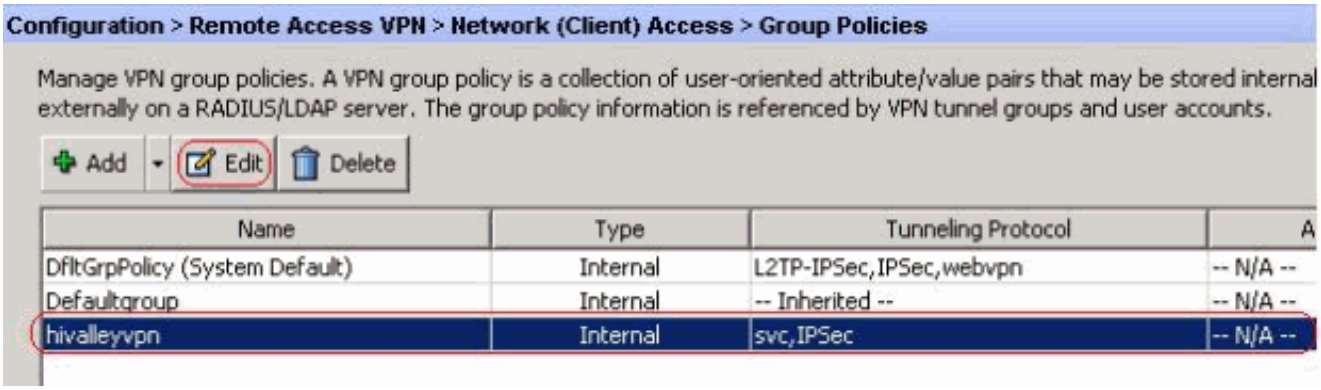
12. Haga clic **se aplican** y después **envían** (si procede) para enviar los comandos al ASA.



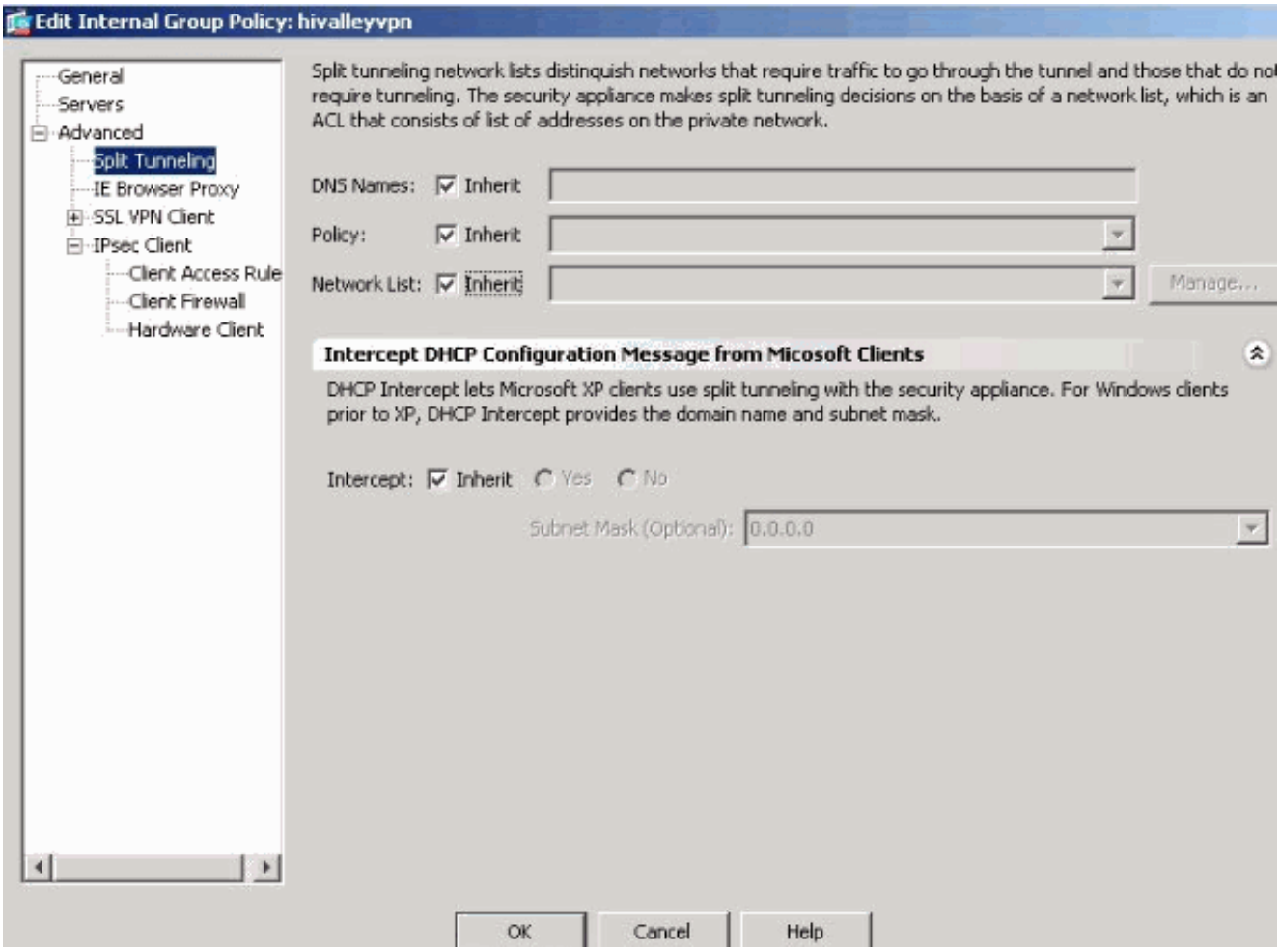
Configure el ASA 8.x con el Administrador de dispositivos de seguridad adaptante (ASDM) 6.x

Complete estos pasos para configurar a su grupo de túnel para permitir el Túnel dividido para los usuarios en el grupo.

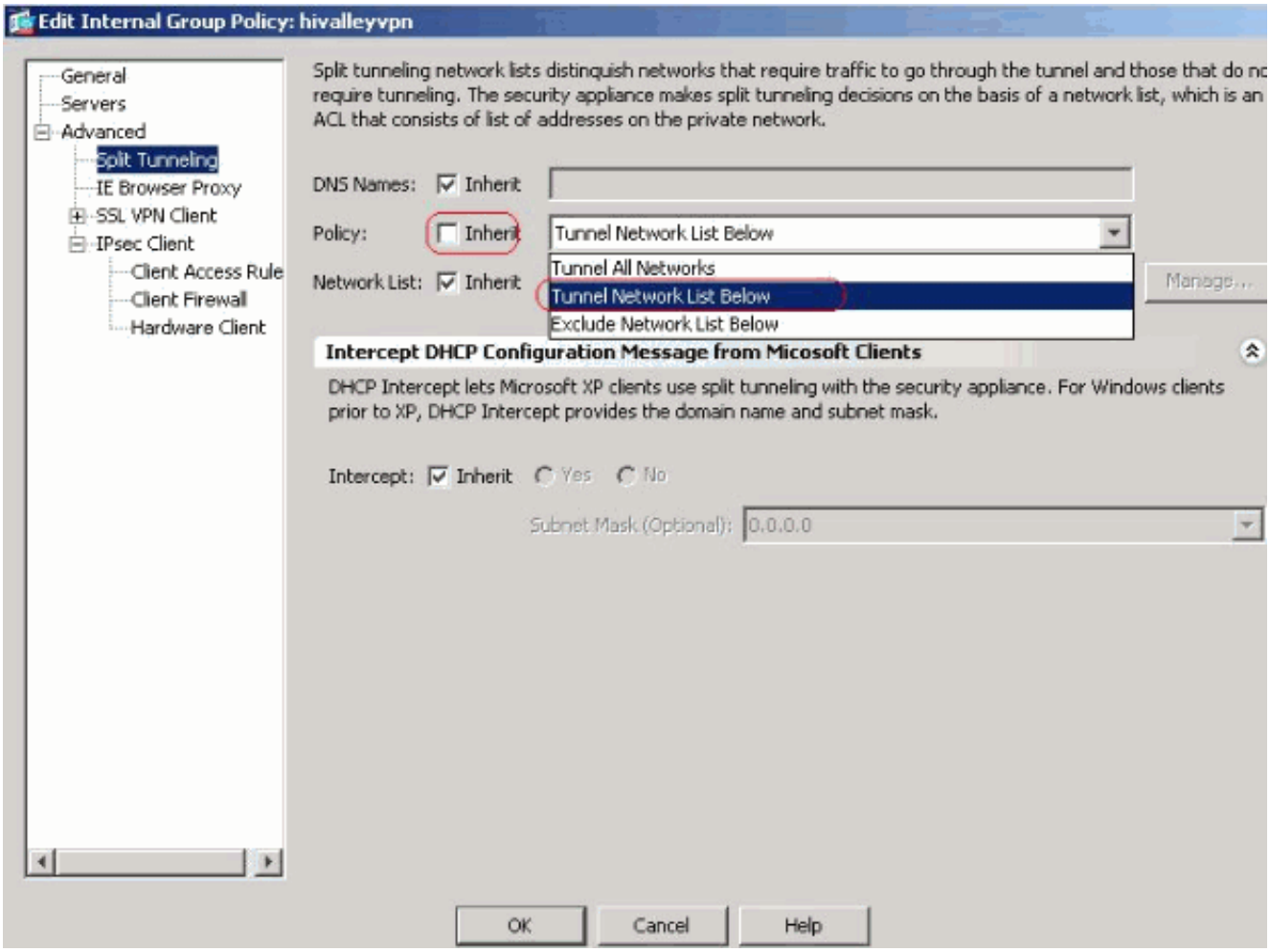
1. Elija la **configuración > el VPN de acceso remoto > las directivas del acceso > del grupo de la red (cliente)**, y elija la directiva del grupo en la cual usted quiere habilitar el acceso del LAN local. Entonces haga clic
editan.



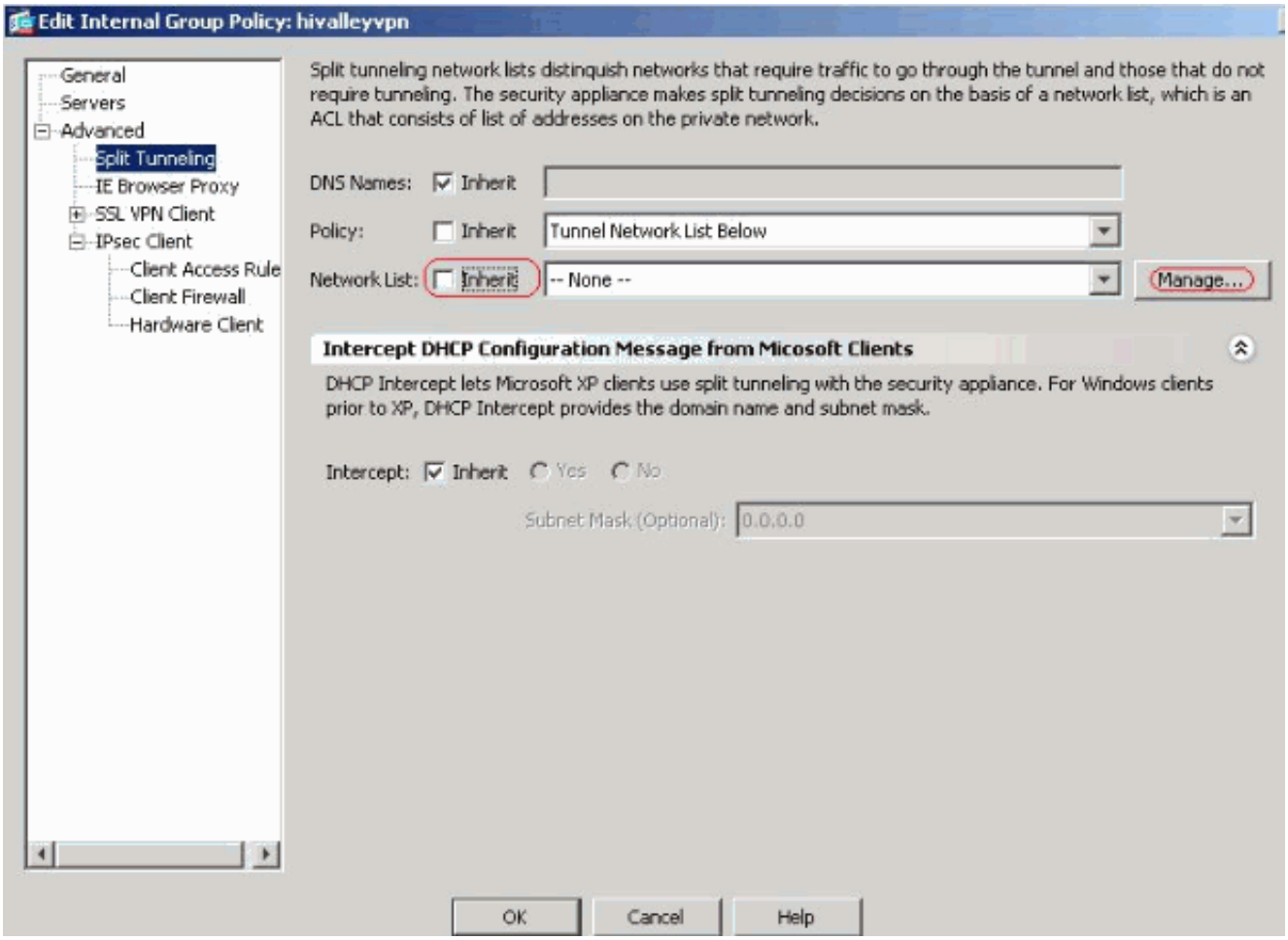
2. Haga clic el **Túnel
dividido**.



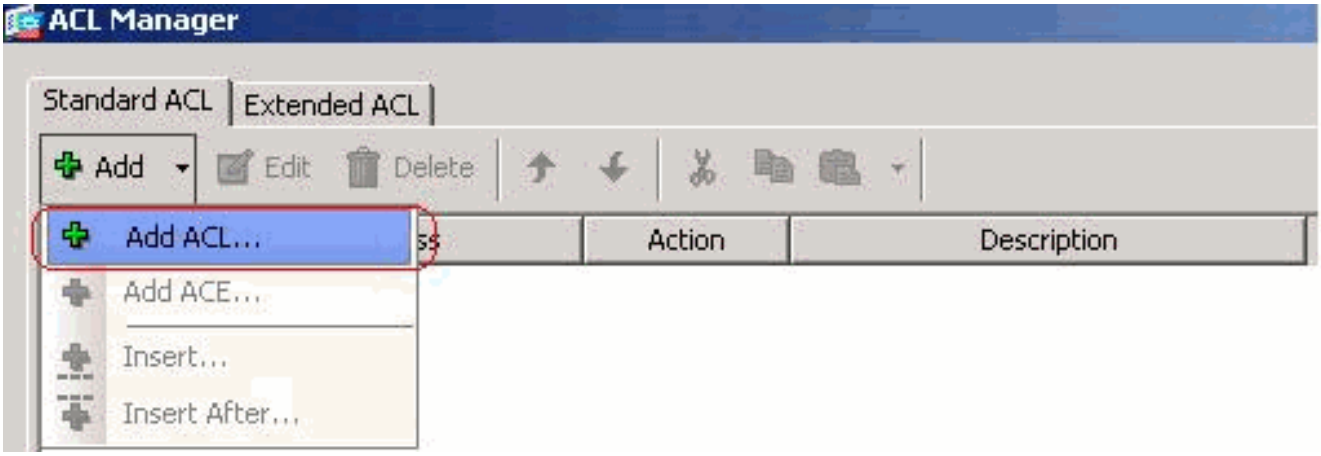
3. Desmarque el cuadro de la **herencia** para la directiva del túnel dividido, y eligió la **lista de la red de túneles**
abajo.



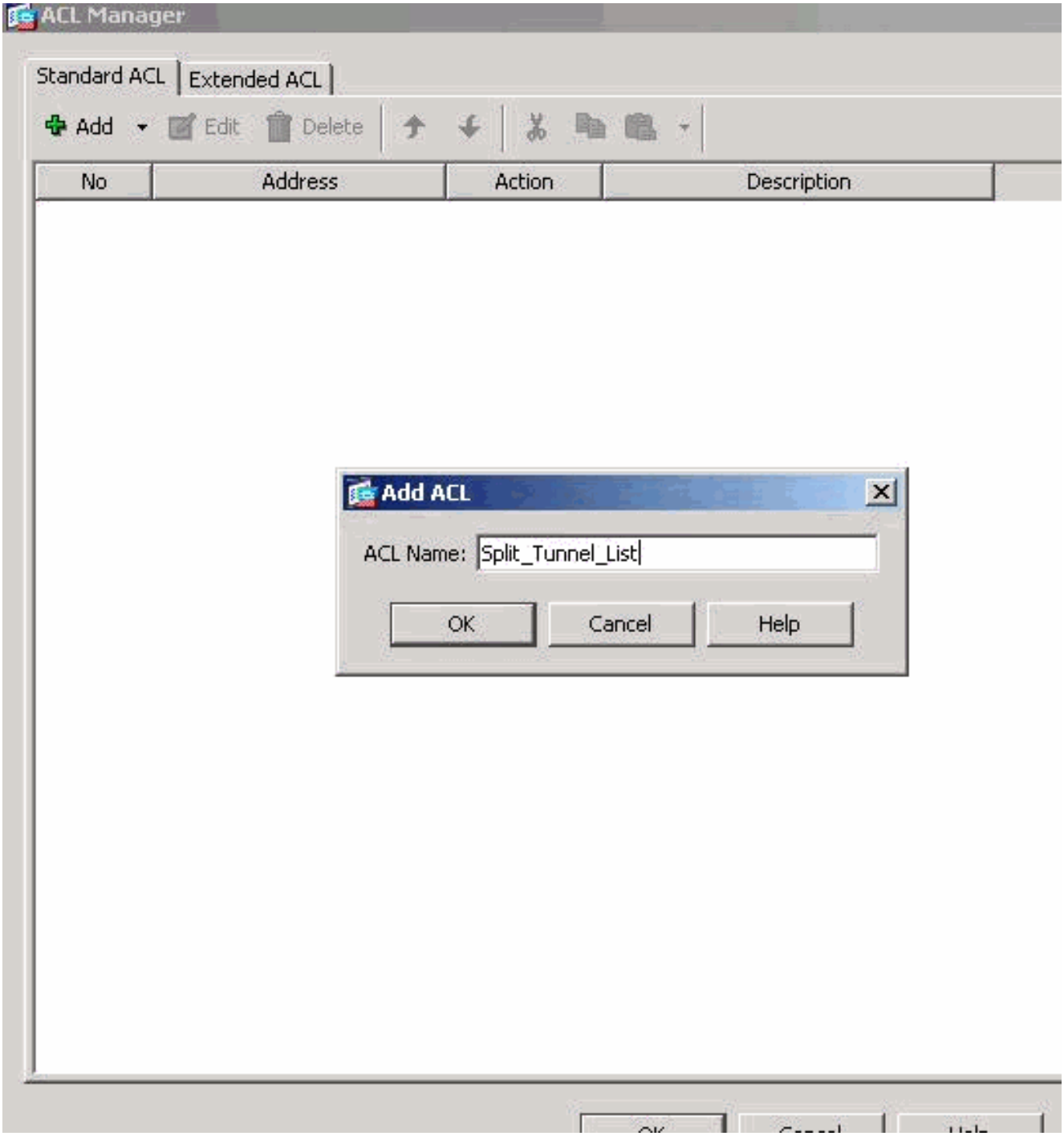
4. Desmarque el cuadro de la **herencia** para la lista de red del túnel dividido, y después haga clic **manejan** para iniciar el ACL
   Manager.



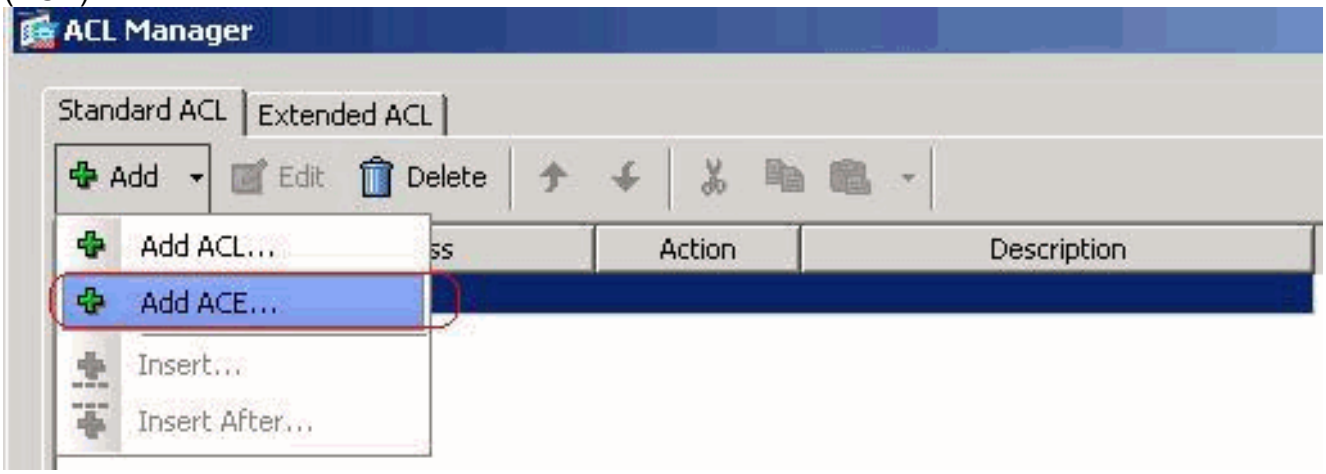
5. Dentro del Administrador de ACL, elija **Add > Add ACL...** para crear una nueva lista de acceso.



6. Proporcione un nombre para el ACL, y haga clic la **AUTORIZACIÓN**.

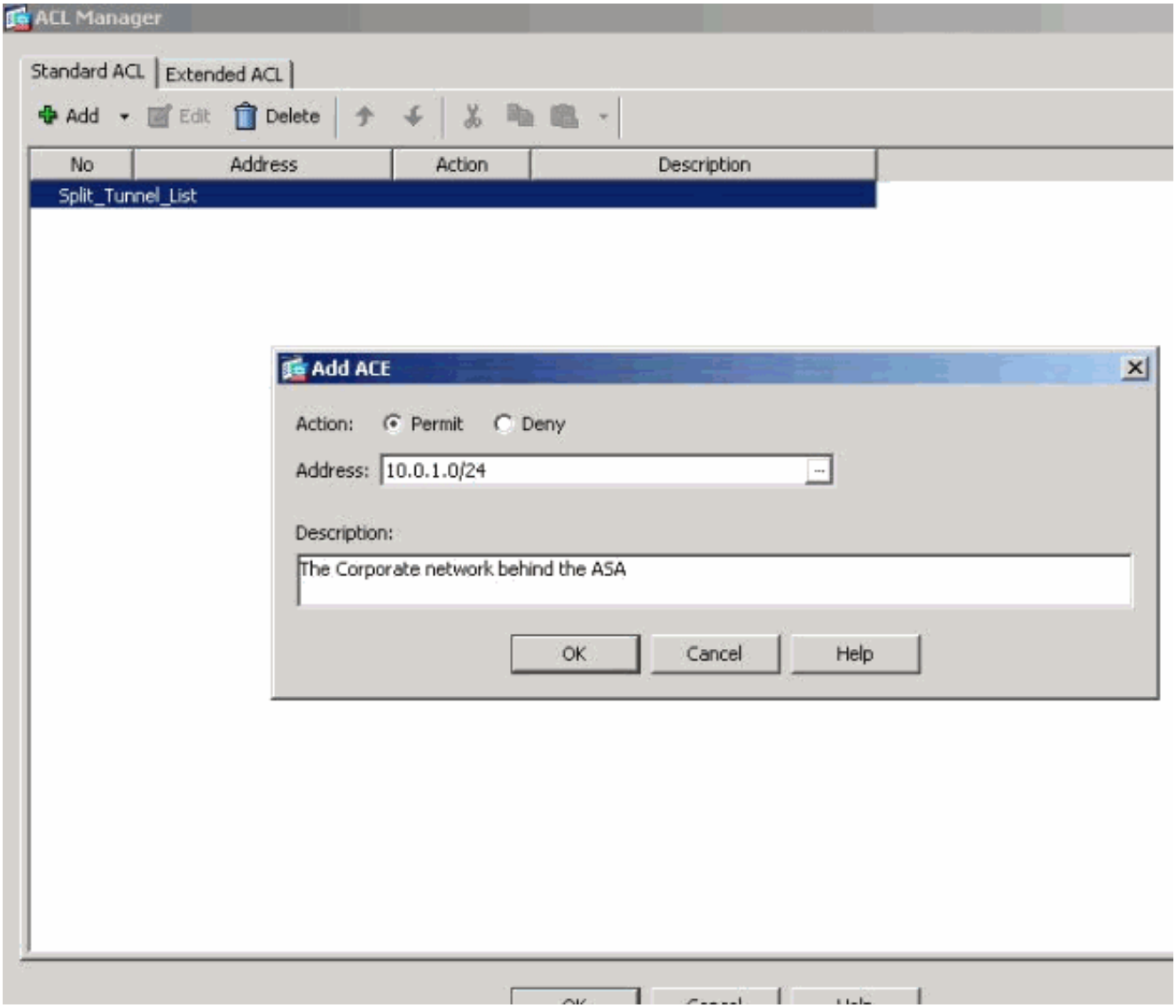


7. Una vez que se crea el ACL, elija **agregan > Add ACE...** para agregar una Entrada de control de acceso
(ACE).

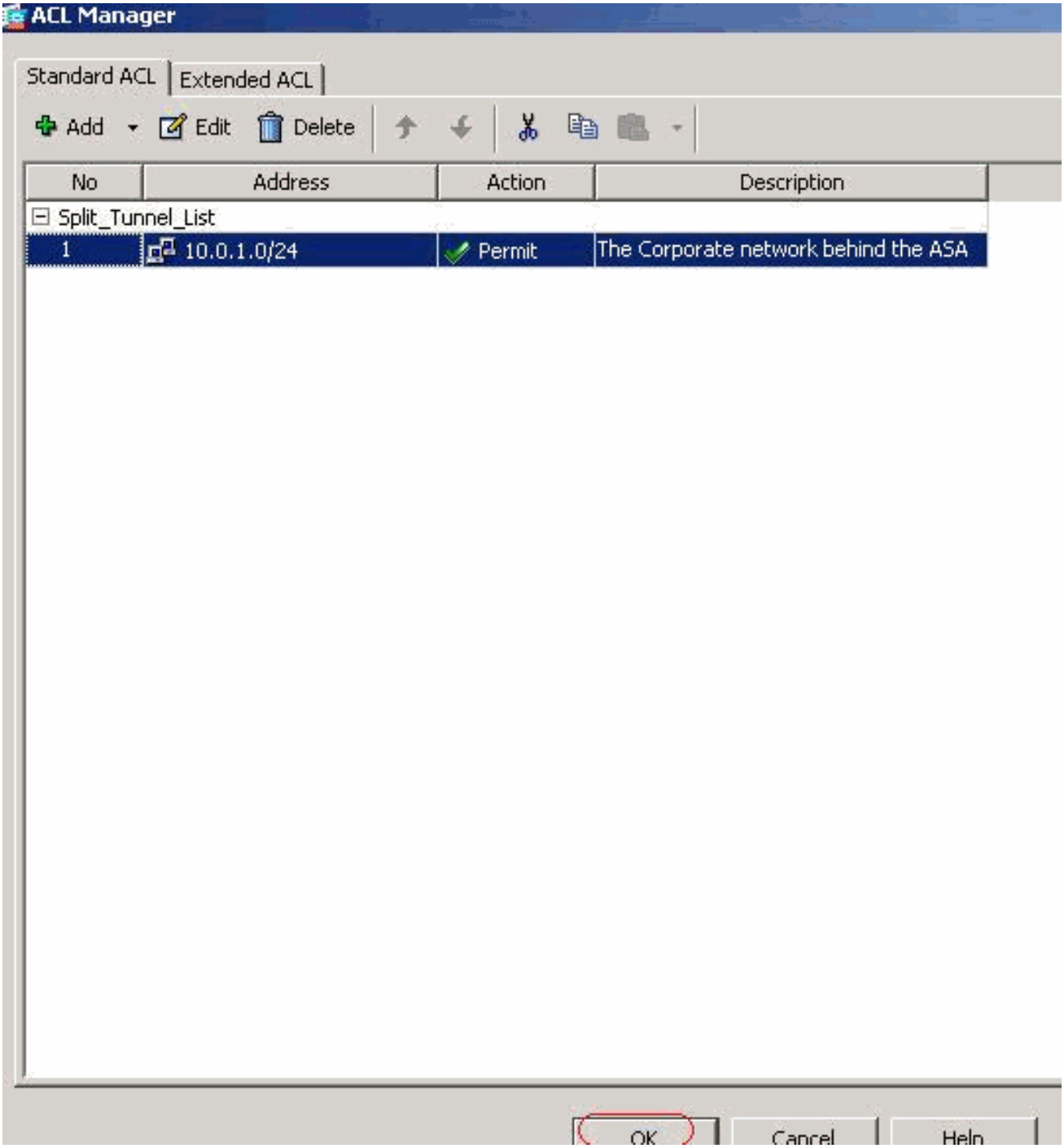


8. Defina el ACE que corresponde al LAN detrás del ASA. En este caso, la red es

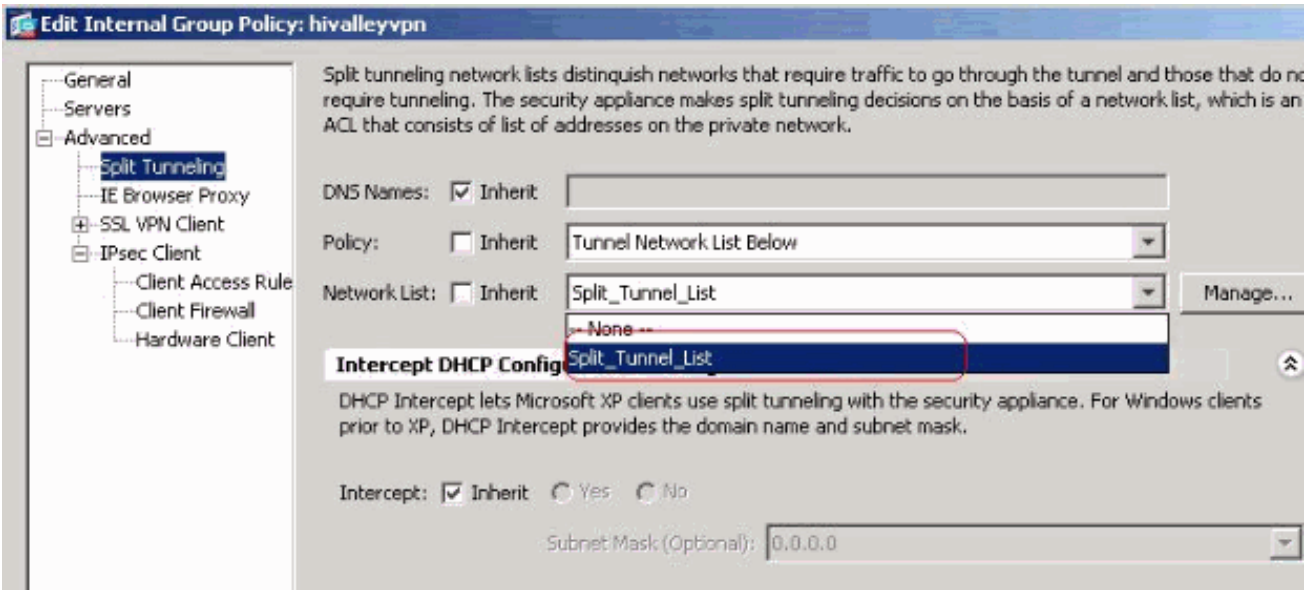
10.0.1.0/24.Haga clic el botón de radio del **permiso**.Elija a la dirección de red con la máscara **10.0.1.0/24**.(Opcional) proporcione una descripción.Haga clic en OK.



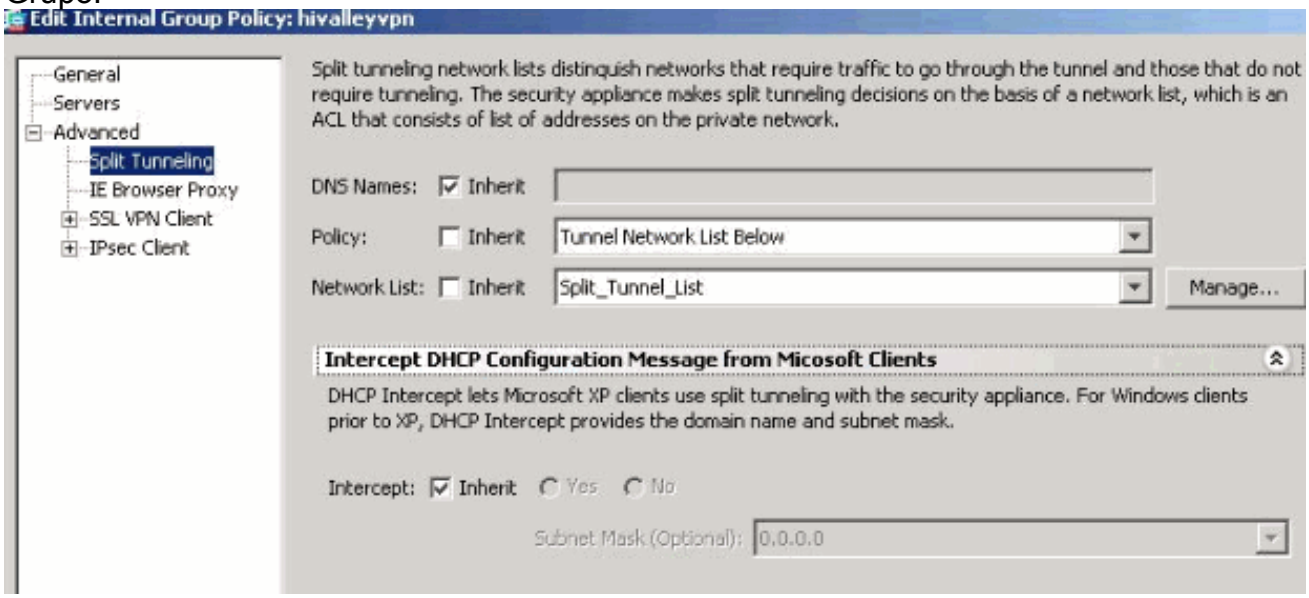
9. Haga clic en OK para salir del Administrador de ACL.



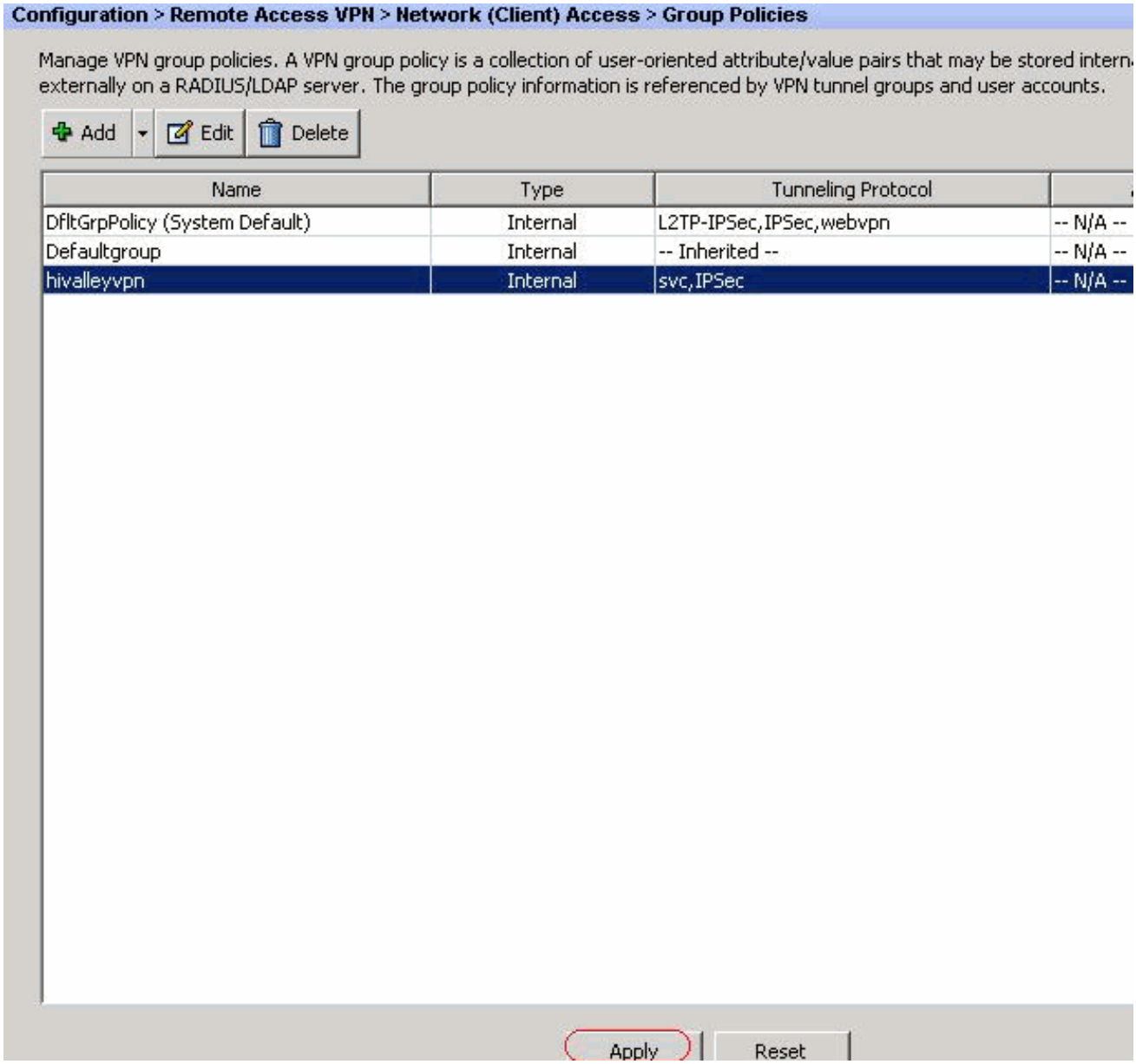
10. Esté seguro que el ACL que usted acaba de crear está seleccionado para la lista de red del túnel
dividido.



11. Haga clic en OK para volver a la configuración de la Política de Grupo.



12. Haga clic **se aplican** y después **envían** (si procede) para enviar los comandos al ASA.



Configure el ASA 7.x y posterior vía el CLI

Bastante que el ASDM, usted puede completar estos pasos en el ASA CLI para permitir el Túnel dividido en el ASA:

Nota: La configuración del Túnel dividido CLI es lo mismo para ASA 7.x y 8.x.

1. Ingrese al modo de configuración.`ciscoasa>`**`enable`** `Password: ******** ciscoasa#`**`configure terminal`** `ciscoasa(config)#`
2. Cree la lista de acceso que define la red detrás del ASA.`ciscoasa(config)#`**`access-list Split_Tunnel_List remark The corporate network behind the ASA.`** `ciscoasa(config)#`**`access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0`**
3. Ingrese el modo de la configuración de la política del grupo para la directiva que usted desea modificar.`ciscoasa(config)#`**`group-policy hillvalleyvpn attributes`** `ciscoasa(config-group-policy)#`
4. Especifique la directiva del túnel dividido. En este caso la directiva **tunnelspecified**.`ciscoasa(config-group-policy)#`**`split-tunnel-policy tunnelspecified`**
5. Especifique la lista de acceso del túnel dividido. En este caso, la lista es **Split_Tunnel_List**.`ciscoasa(config-group-policy)#`**`split-tunnel-network-list value Split_Tunnel_List`**

6. Ejecutar este comando:`ciscoasa(config)#`**`tunnel-group hillvalleyvpn general-attributes`**
7. Asocie la política del grupo al grupo de túnel`ciscoasa(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
8. Dé salida a los dos modos de configuración.`ciscoasa(config-group-policy)#`**`exit`**
`ciscoasa(config)#`**`exit`** `ciscoasa#`
9. Salve la configuración al RAM no volátil (NVRAM) y al Presione ENTER cuando está indicado para especificar el nombre de archivo de origen.`ciscoasa#`**`copy running-config startup-config`** `Source filename [running-config]? Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a 3847 bytes copied in 3.470 secs (1282 bytes/sec) ciscoasa#`

Configure PIX 6.x con el CLI

Complete estos pasos:

1. Cree la lista de acceso que define la red detrás del PIX.
`PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0`
2. Cree un grupo *VPN3000 del* vpn y especifique el túnel dividido ACL a él como se muestra:`PIX(config)#`**`vpngroup vpn3000 split-tunnel Split_Tunnel_List`** **Nota:** Refiera al Cisco Secure PIX Firewall 6.x y al Cliente Cisco VPN 3.5 para Windows con el Microsoft Windows 2000 y la autenticación de RADIUS de 2003 IAS para más información sobre la configuración del VPN de acceso remoto para PIX 6.x.

Verificación

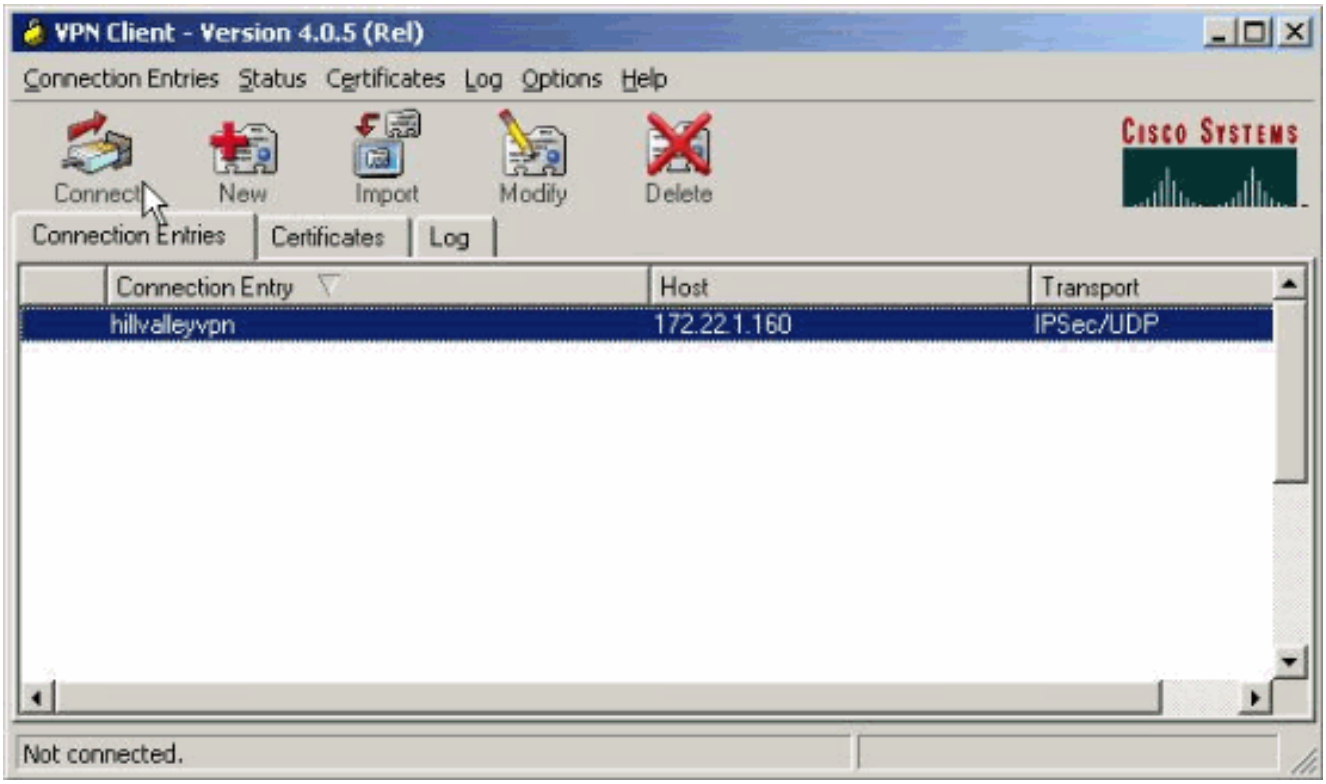
Siga los pasos en estas secciones para verificar su configuración.

- Conecte con el cliente VPN
- Vea el registro de cliente de VPN
- Pruebe el acceso del LAN local con el ping

Conecte con el cliente VPN

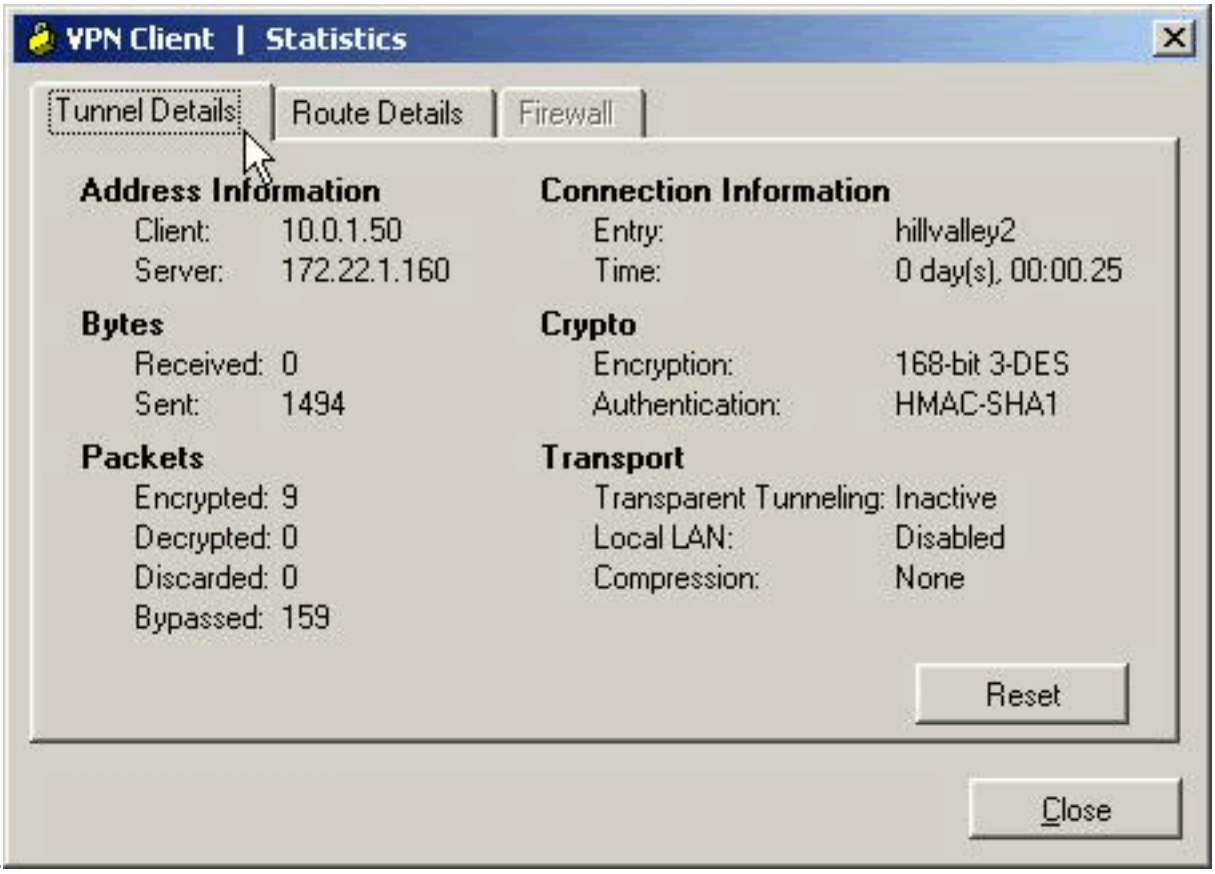
Conecte a su cliente VPN con el concentrador VPN para verificar su configuración.

1. Elija su Entrada de conexión de la lista y el tecleo
conecta.



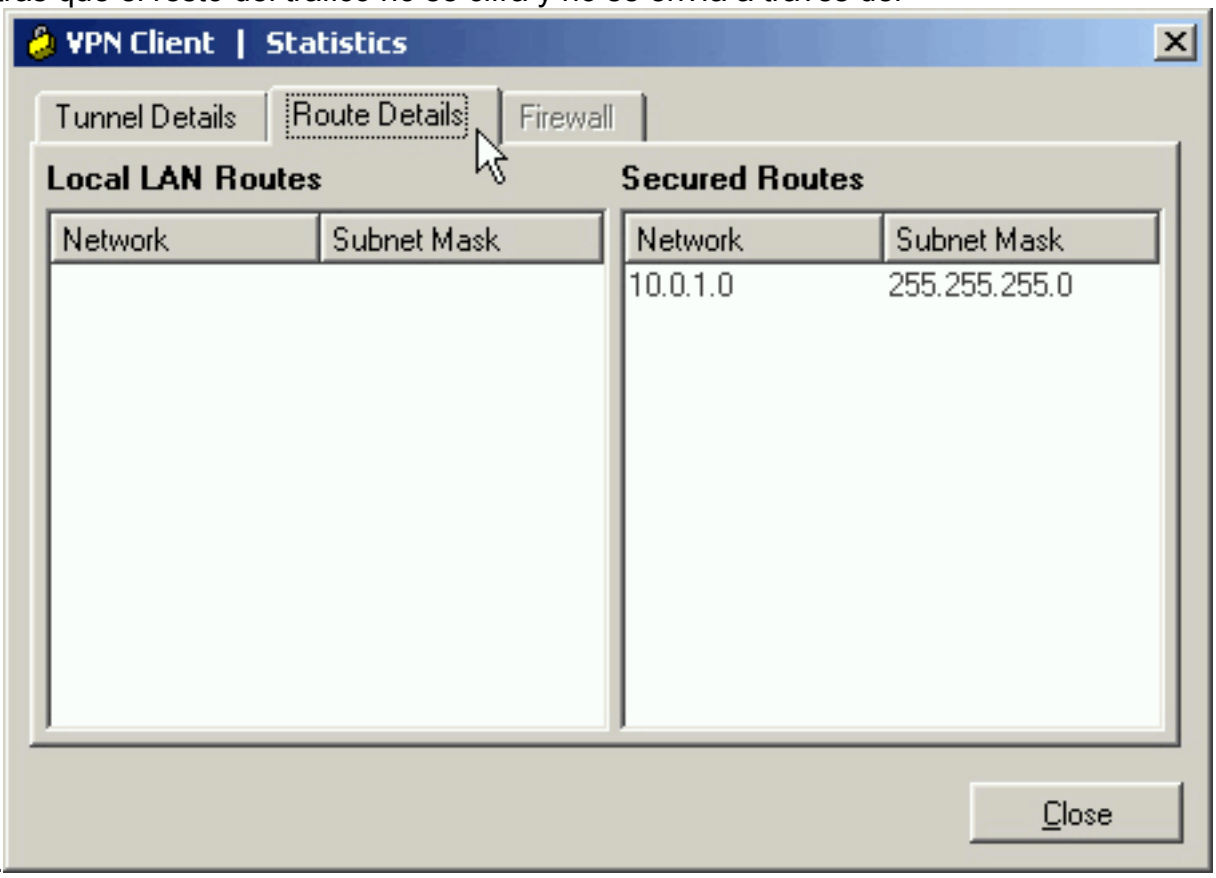
2. Ingrese sus credenciales.

3. Elija el **estatus > las estadísticas…** para visualizar la ventana de los detalles del túnel donde usted puede examinar los detalles del túnel y ver el flujo de



tráfico.

4. Vaya a la lengueta de los detalles de la ruta para ver las rutas que el cliente VPN está asegurando al ASA.En este ejemplo, el cliente VPN está asegurando el acceso a 10.0.1.0/24 mientras que el resto del tráfico no se cifra y no se envía a través del

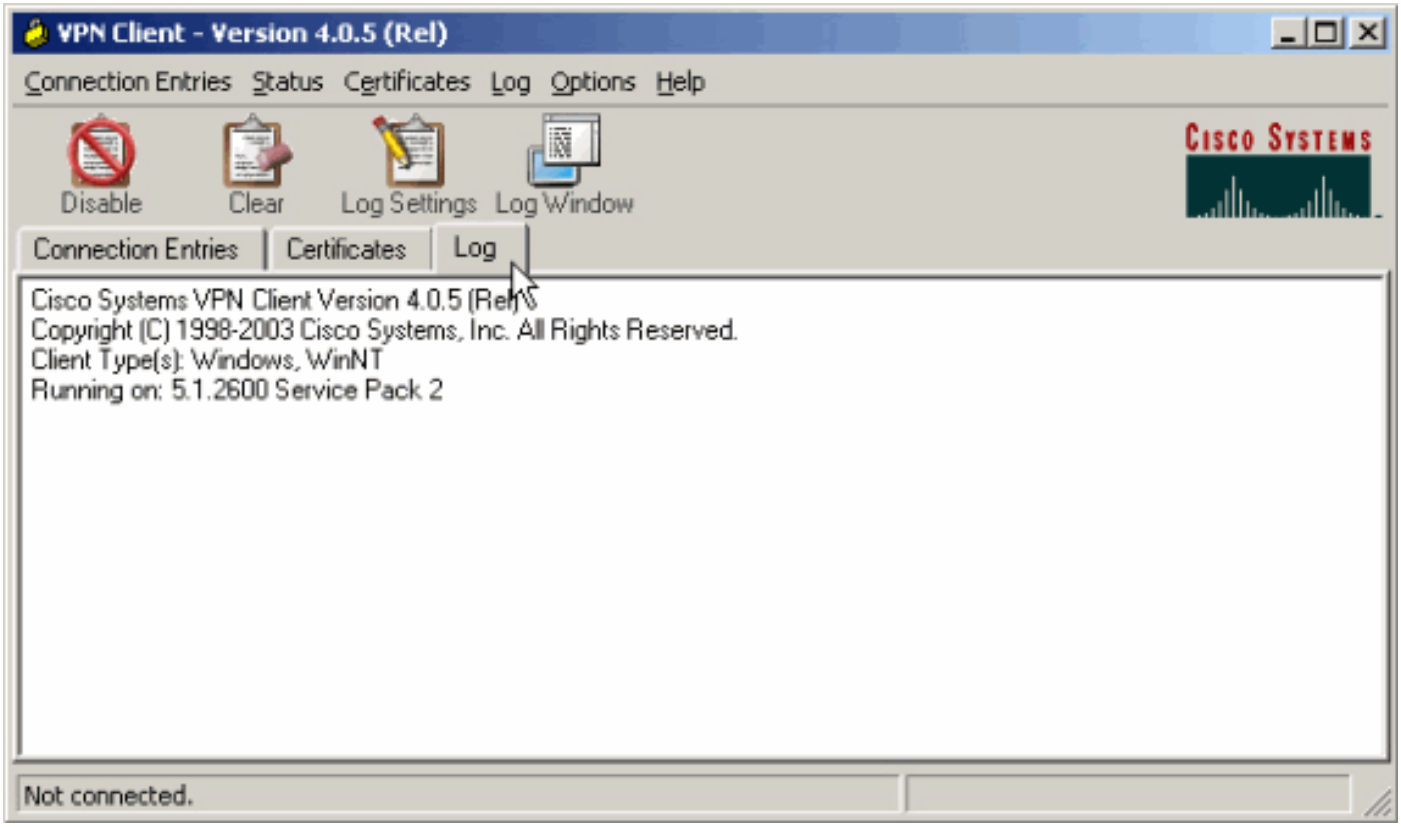


túnel.

Vea el registro de cliente de VPN

Cuando usted examina el registro de cliente de VPN, usted puede determinar

independientemente de si el parámetro que especifica el Túnel dividido está fijado. Para ver el registro, vaya a la lengueta del registro en el cliente VPN. Entonces haga clic en las **configuraciones de registro** para ajustar se registra qué. En este ejemplo, el IKE se fija a **3 - alto** mientras que el resto de los elementos del registro se fijan a **1 - puntos bajos**.




```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:20:09.532  07/27/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.160.

!--- Output is supressed 18 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 19 14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 20
14:20:14.188 07/27/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 21 14:20:14.208 07/27/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160 22 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.160 23 14:20:14.208
07/27/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.160 24 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 25 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 26 14:20:14.208
07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 27 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_PFS: , value = 0x00000000 28 14:20:14.208 07/27/06 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc ASA5510 Version
7.2(1) built by root on Wed 31-May-06 14:45 !--- Split tunneling is permitted and the remote LAN
is defined. 29 14:20:14.238 07/27/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value = 0x00000001 30 14:20:14.238 07/27/06
Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0 mask = 255.255.255.0 protocol = 0 src
port = 0 dest port=0 !--- Output is supressed.
```

Pruebe el acceso del LAN local con el ping

Una manera adicional de probar que configuran al cliente VPN para el Túnel dividido mientras que es tunneled al ASA debe utilizar el **comando ping** en la línea de comando de Windows. El LAN local del cliente VPN es 192.168.0.0/24 y otro host está presente en la red con una dirección IP de 192.168.0.3.

```
C:\>ping 192.168.0.3 Pinging 192.168.0.3 with 32 bytes of data: Reply from 192.168.0.3: bytes=32
time<1ms TTL=255 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 Reply from 192.168.0.3:
bytes=32 time<1ms TTL=255 Reply from 192.168.0.3: bytes=32 time<1ms TTL=255 Ping statistics for
192.168.0.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times
in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Troubleshooting

Limitación con el número de las entradas en un túnel dividido ACL

Hay una restricción con el número de entradas en un ACL usado para el túnel dividido. Se recomienda para no utilizar más de 50-60 entradas de ACE para las funciones satisfactorias. Le aconsejan implementar subnetting la característica para cubrir un rango de los IP Addresses.

Información Relacionada

- PIX/ASA 7.x como servidor VPN remoto que usa el ejemplo de la Configuración de ASDM
- Cisco ASA 5500 Series Adaptive Security Appliances
- Soporte Técnico y Documentación - Cisco Systems