Configuración de la tunelización dividida para los clientes VPN en ASA

Contenido

Introducción

Este documento describe el proceso para permitir el acceso de los clientes VPN a Internet mientras se tunelizan en un Cisco ASA 5500 Series Security Appliance.

Prerequisites

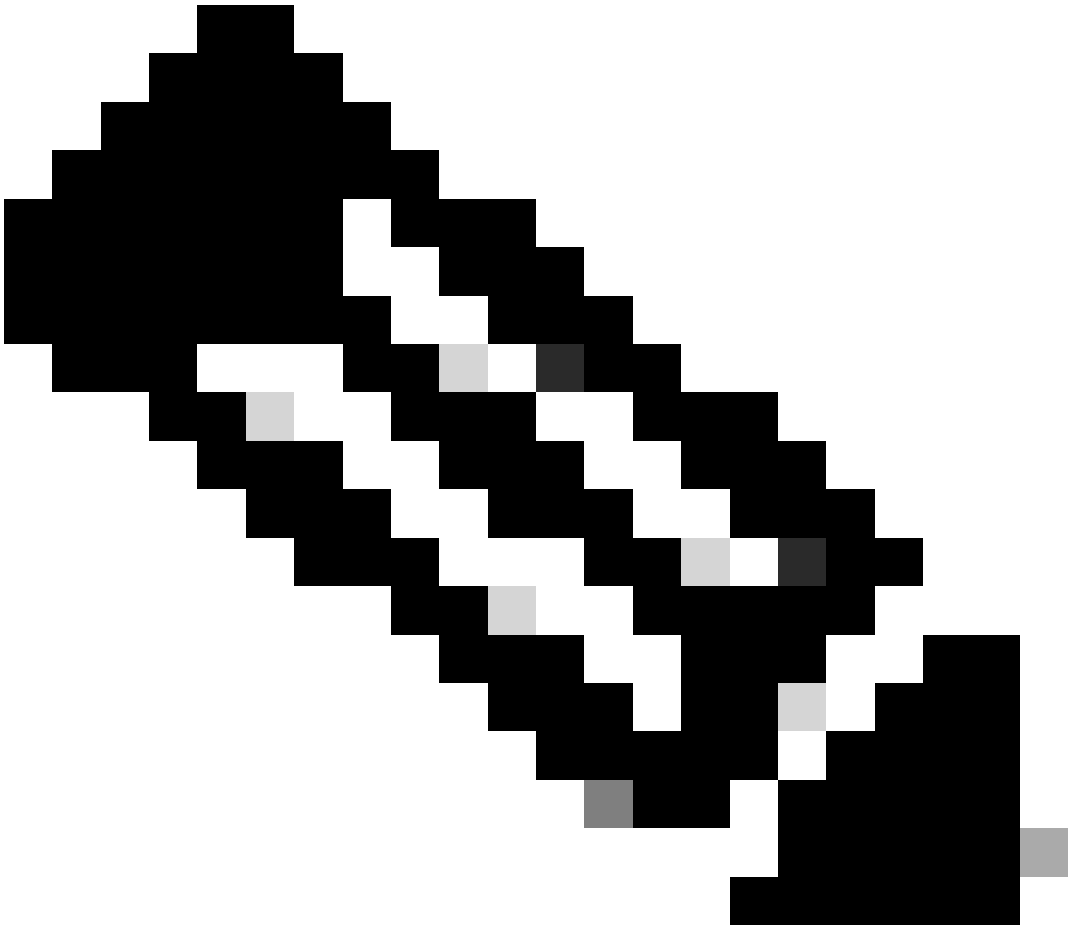
Requirements

Este documento asume que ya existe una configuración de VPN de acceso remoto en funcionamiento en ASA. Consulte Ejemplo de Configuración de PIX/ASA 7.x como Servidor VPN Remoto Usando ASDM si aún no se ha configurado uno.

Componentes Utilizados

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

- Software Cisco ASA 5500 Series Security Appliance versión 7.x y posteriores
- Cisco Systems VPN Client versión 4.0.5
- Adaptive Security Device Manager (ASDM)



Nota: Este documento también contiene la configuración de PIX 6.x CLI que es compatible con Cisco VPN Client 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Diagrama de la red

El cliente VPN se encuentra en una red SOHO típica y se conecta a través de Internet a la oficina principal.

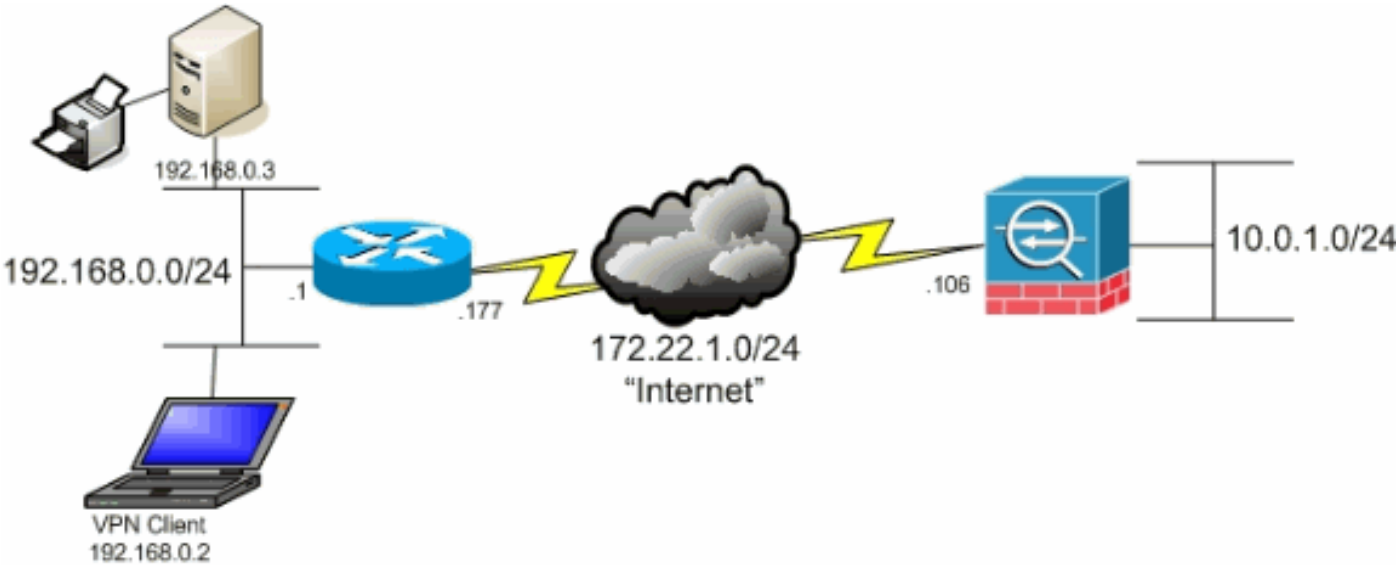


Diagrama de la red

Productos Relacionados

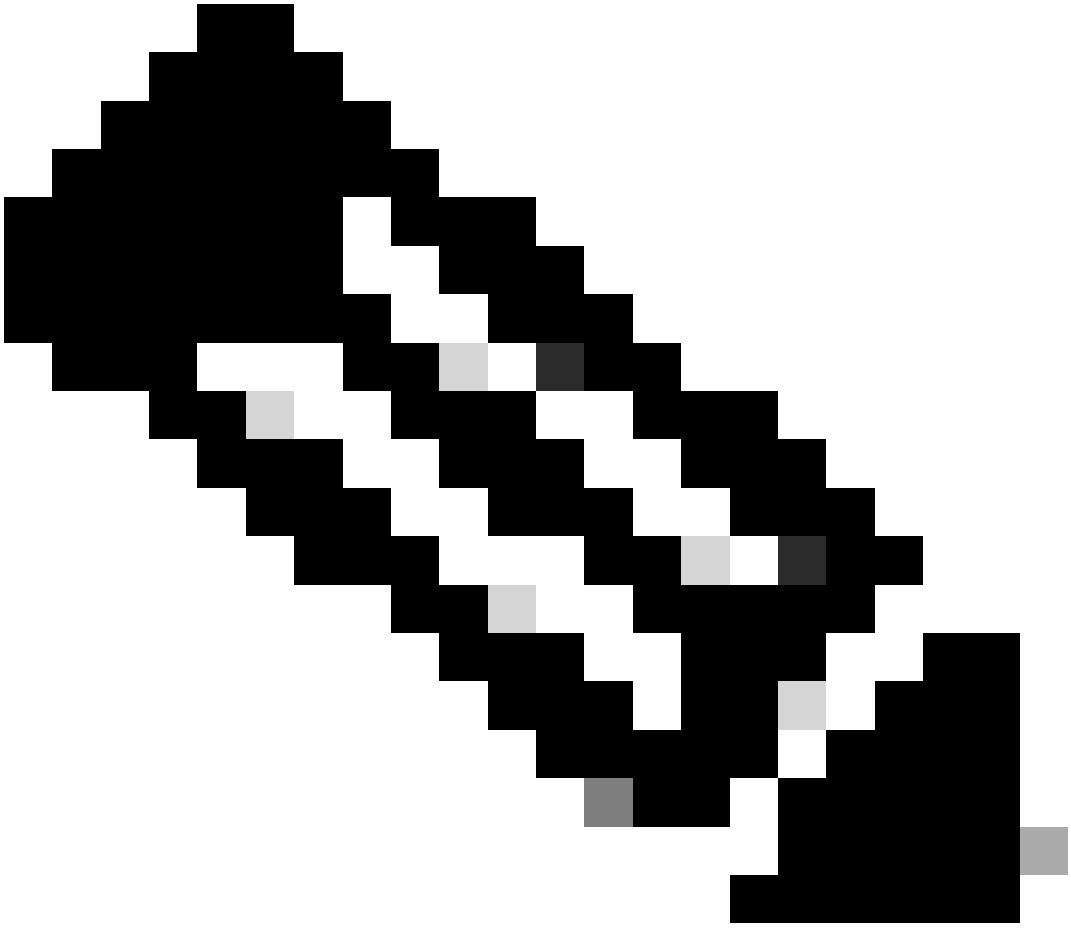
Esta configuración también se puede utilizar con la versión 7.x del Cisco PIX 500 Series Security Appliance Software.

Convenciones

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

Antecedentes

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: La tunelización completa se considera la configuración más segura porque no habilita el acceso simultáneo de dispositivos a Internet y a la LAN corporativa. Un compromiso entre la tunelización completa y la tunelización dividida permite a los clientes VPN el acceso local a la LAN solamente. Consulte Ejemplo de Configuración de PIX/ASA 7.x: Allow Local LAN Access for VPN Clients para obtener más información.

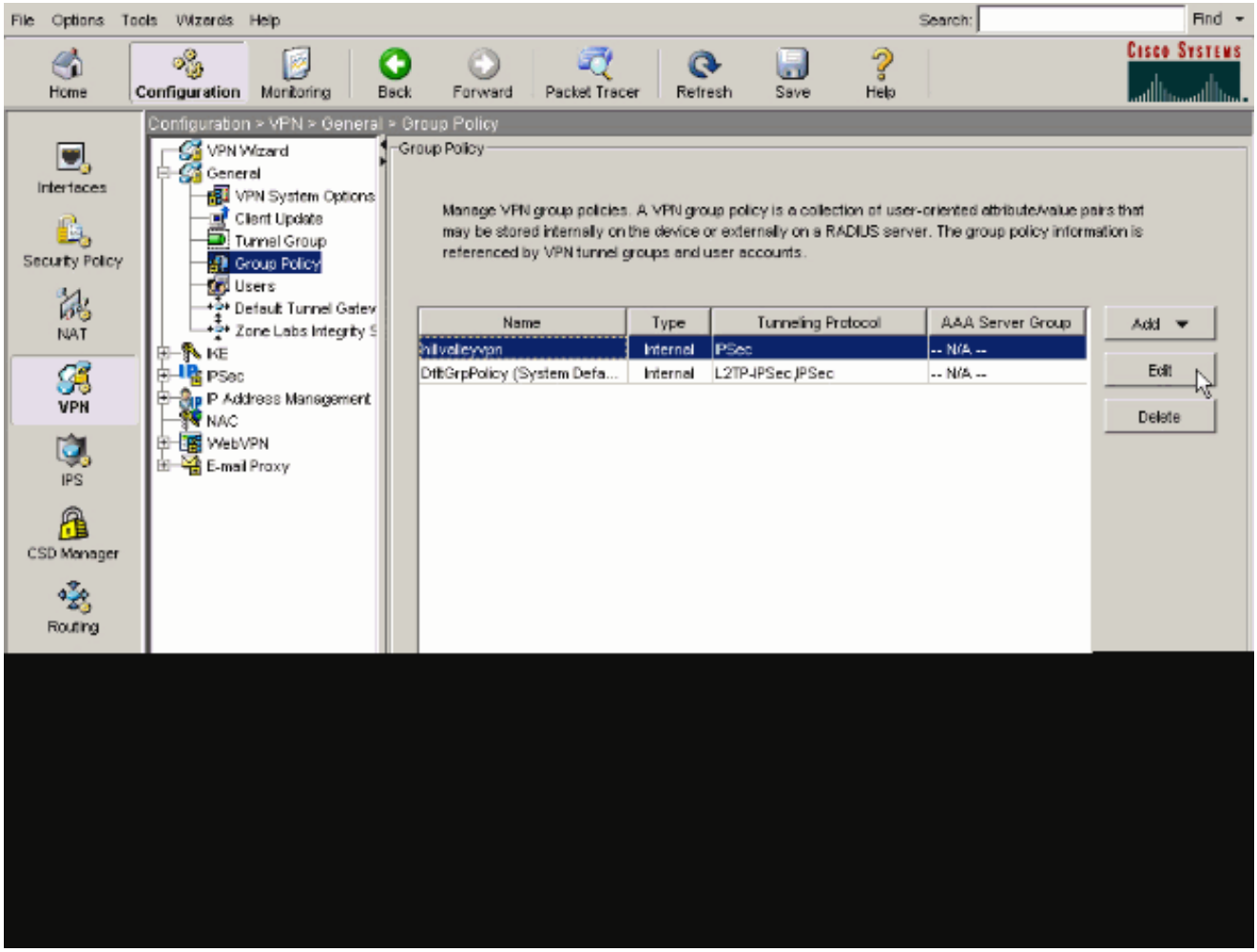
En un escenario básico de VPN Client a ASA, todo el tráfico del VPN Client se cifra y se envía al ASA sin importar cuál sea su destino. Según la configuración y el número de usuarios admitidos, esta configuración puede consumir un gran ancho de banda. La tunelización dividida puede funcionar para aliviar este problema ya que permite a los usuarios enviar solamente ese tráfico que está destinado a la red corporativa a través del túnel. El resto del tráfico, como la mensajería instantánea, el correo electrónico o la navegación casual, se envía a Internet a través de la LAN local del cliente VPN.

Configuración de la tunelización dividida en el ASA

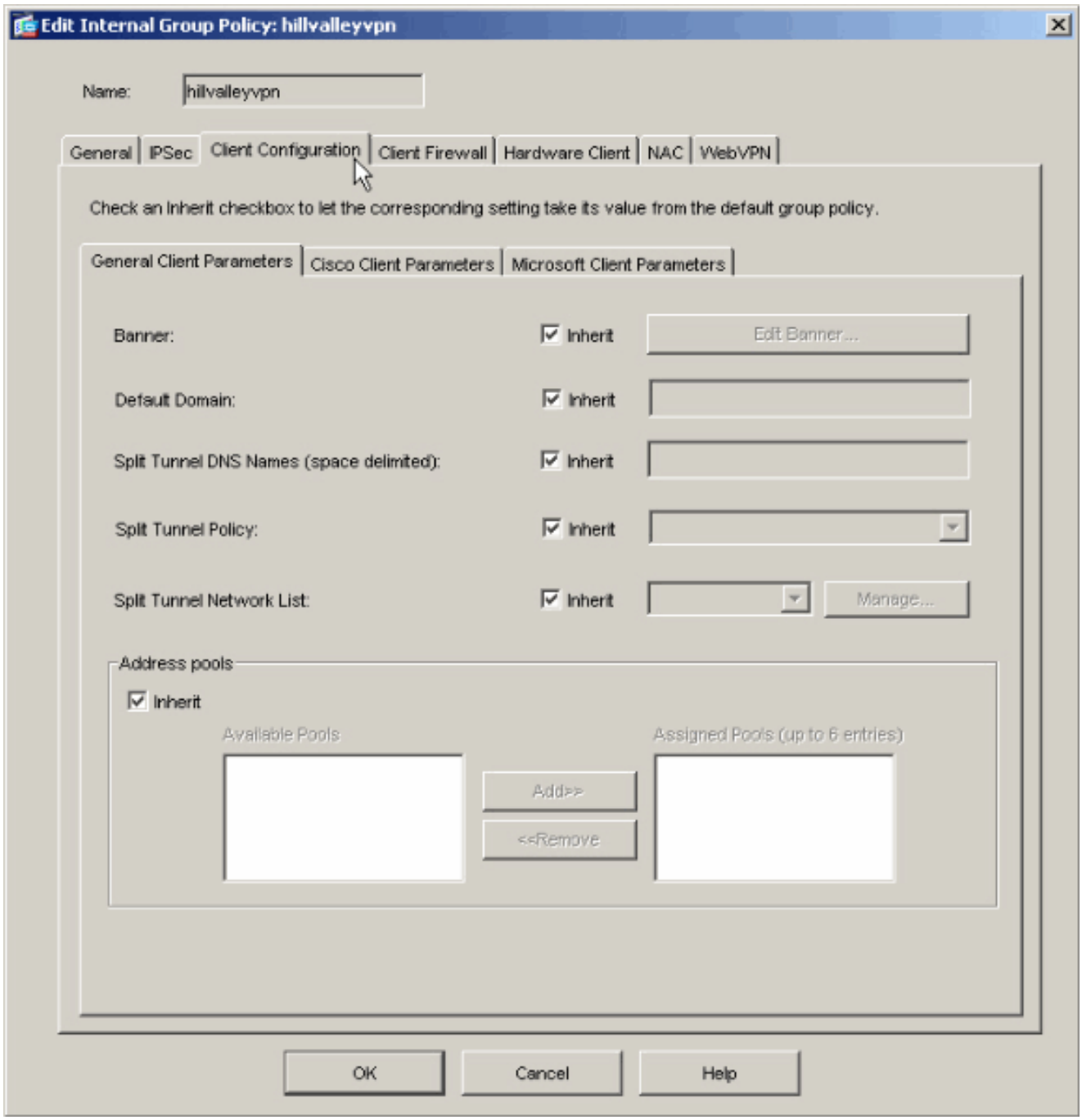
Configuración de ASA 7.x con Adaptive Security Device Manager (ASDM) 5.x

Complete estos pasos para configurar su grupo de túnel para permitir la tunelización dividida para los usuarios en el grupo.

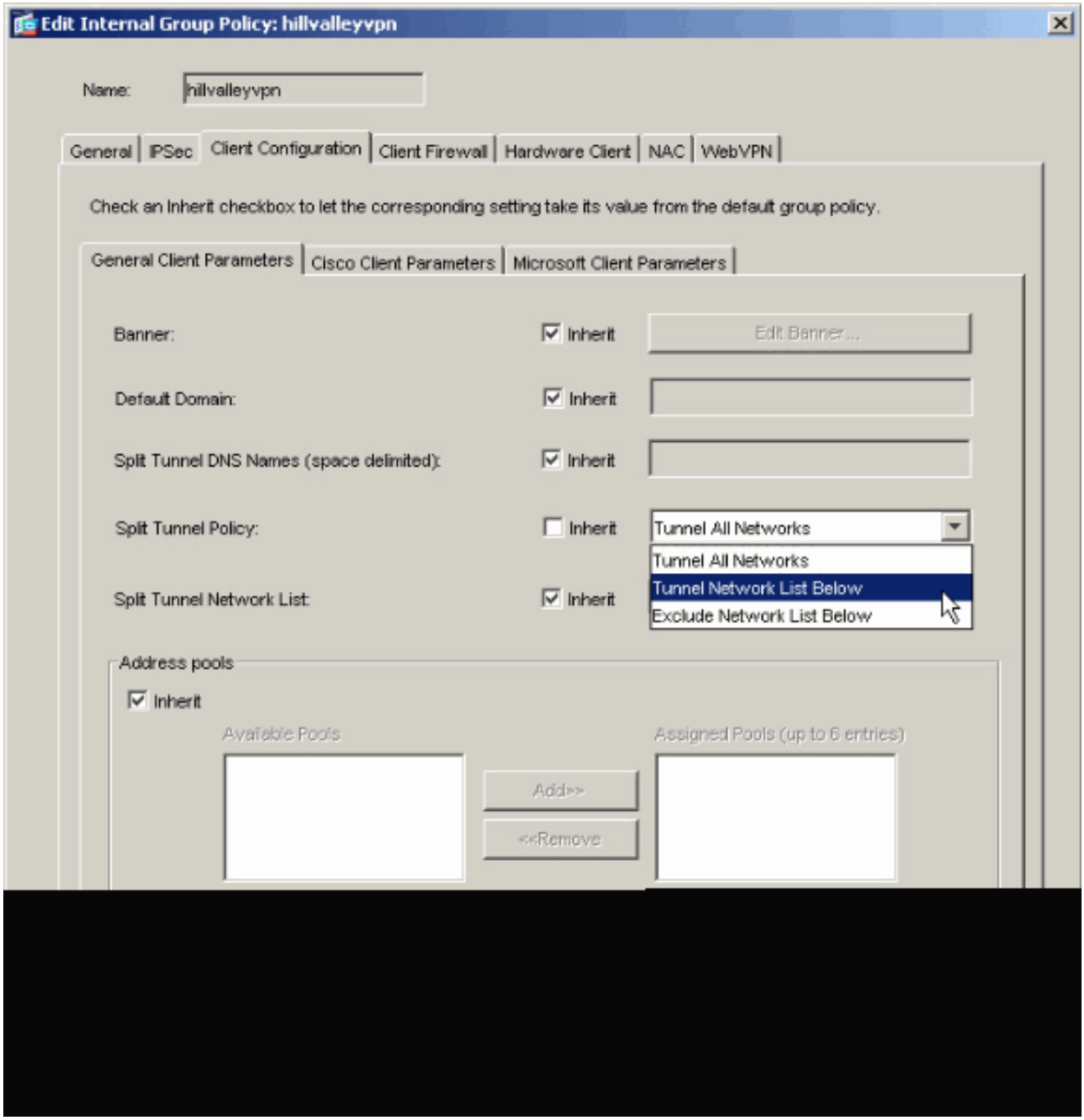
1. Elija Configuration > VPN > General > Group Policy y seleccione la política de grupo en la que desea habilitar el acceso LAN local. Luego, haga clic en Edit (Editar).



2. Vaya a la ficha Configuración del cliente.

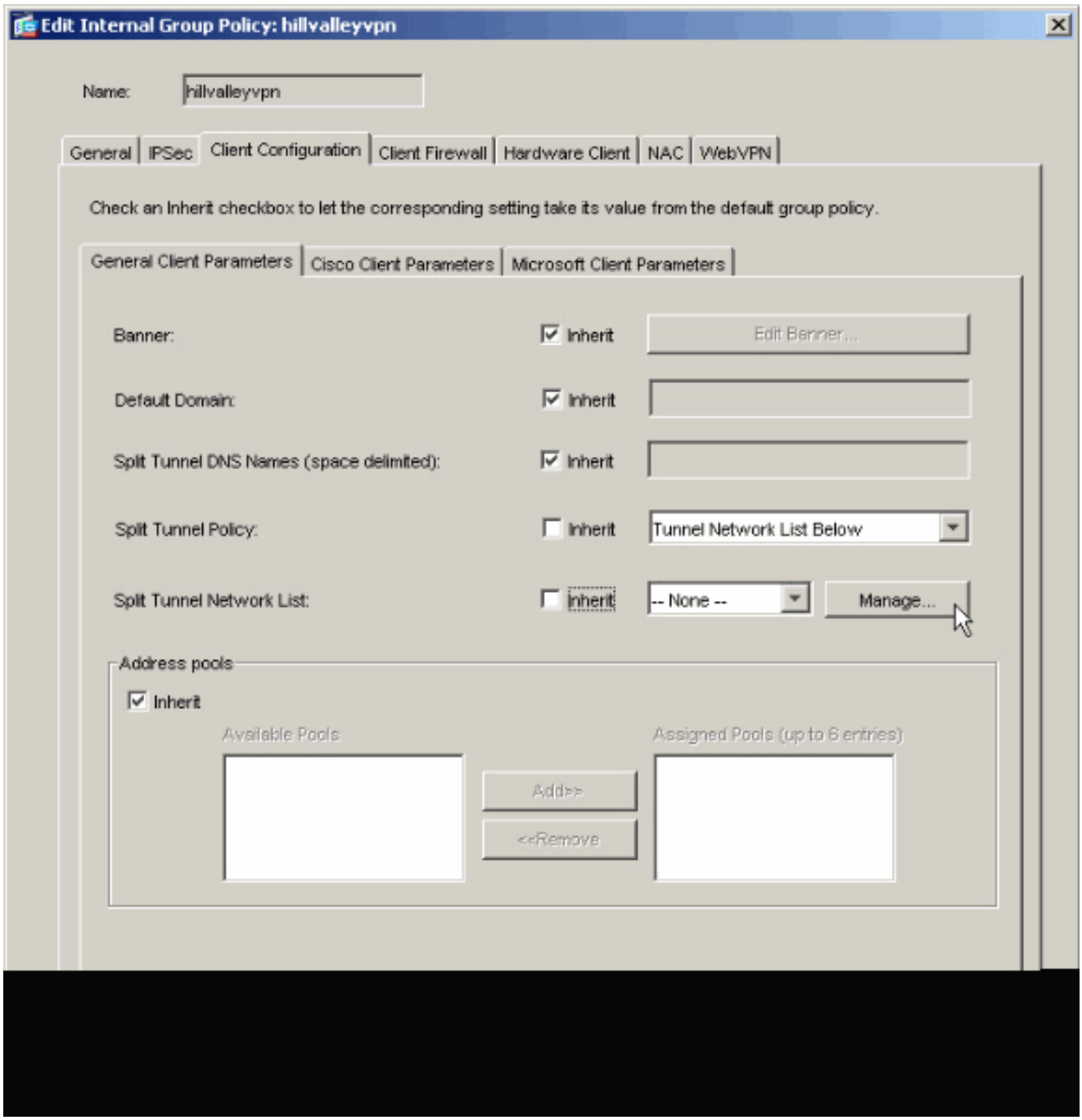


3. Desmarque la casilla Heredar para la política de túnel dividido y elija Tunnel Network List Below ..



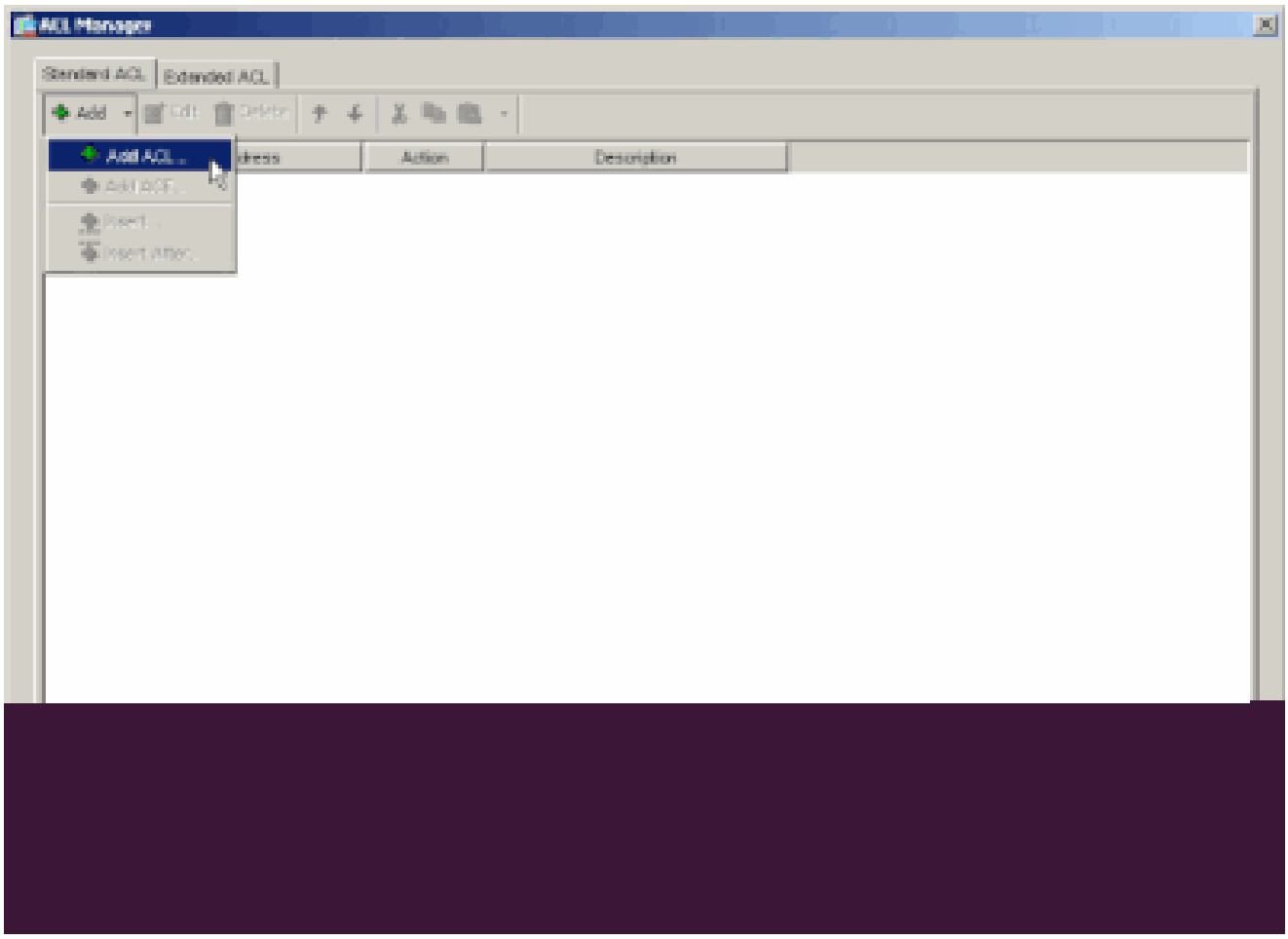
•

Desmarque la casilla **Inherit** para la Lista de Red de Túnel Dividido y luego haga clic en **Manage** para iniciar el Administrador ACL.



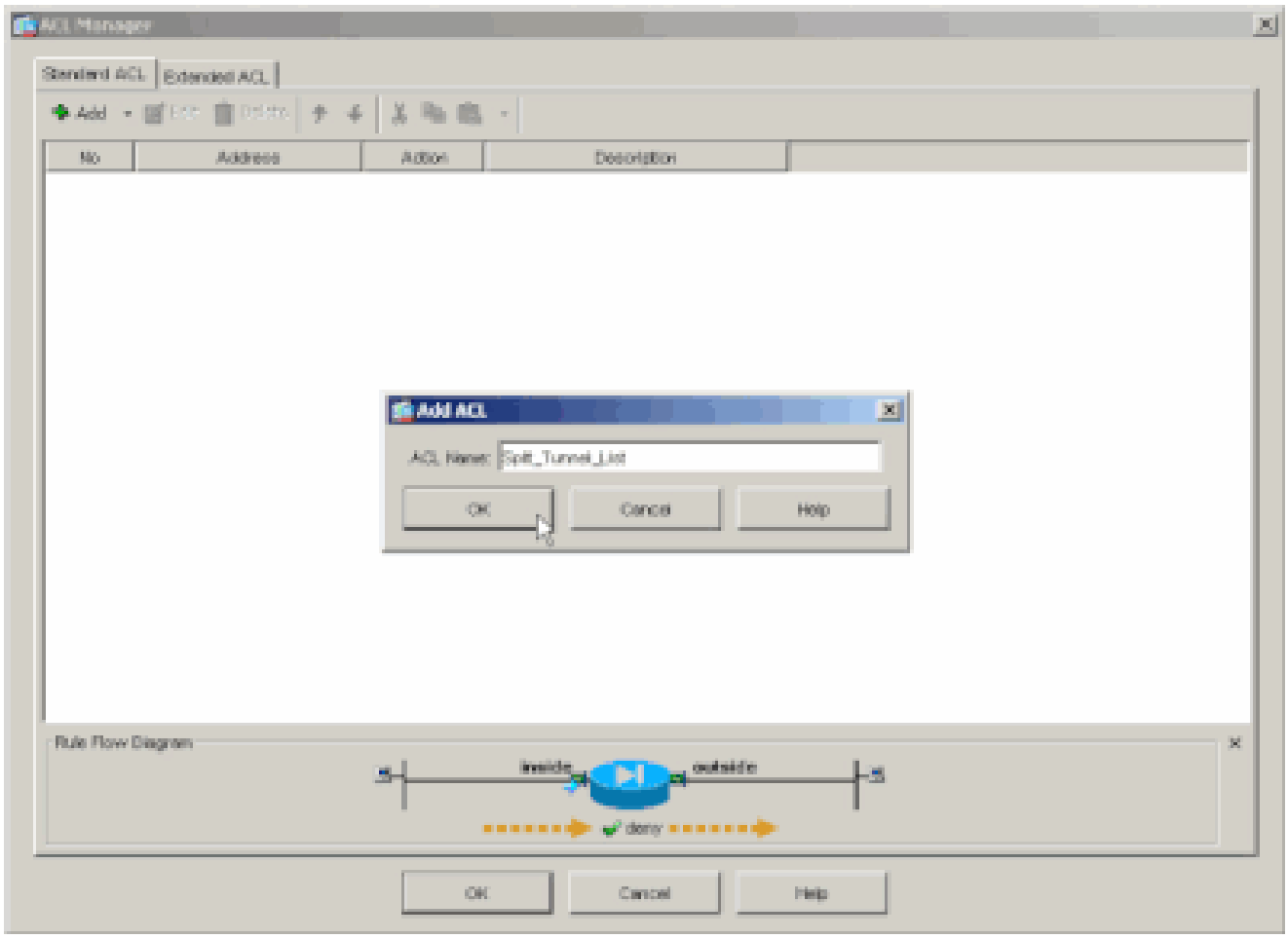
•

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



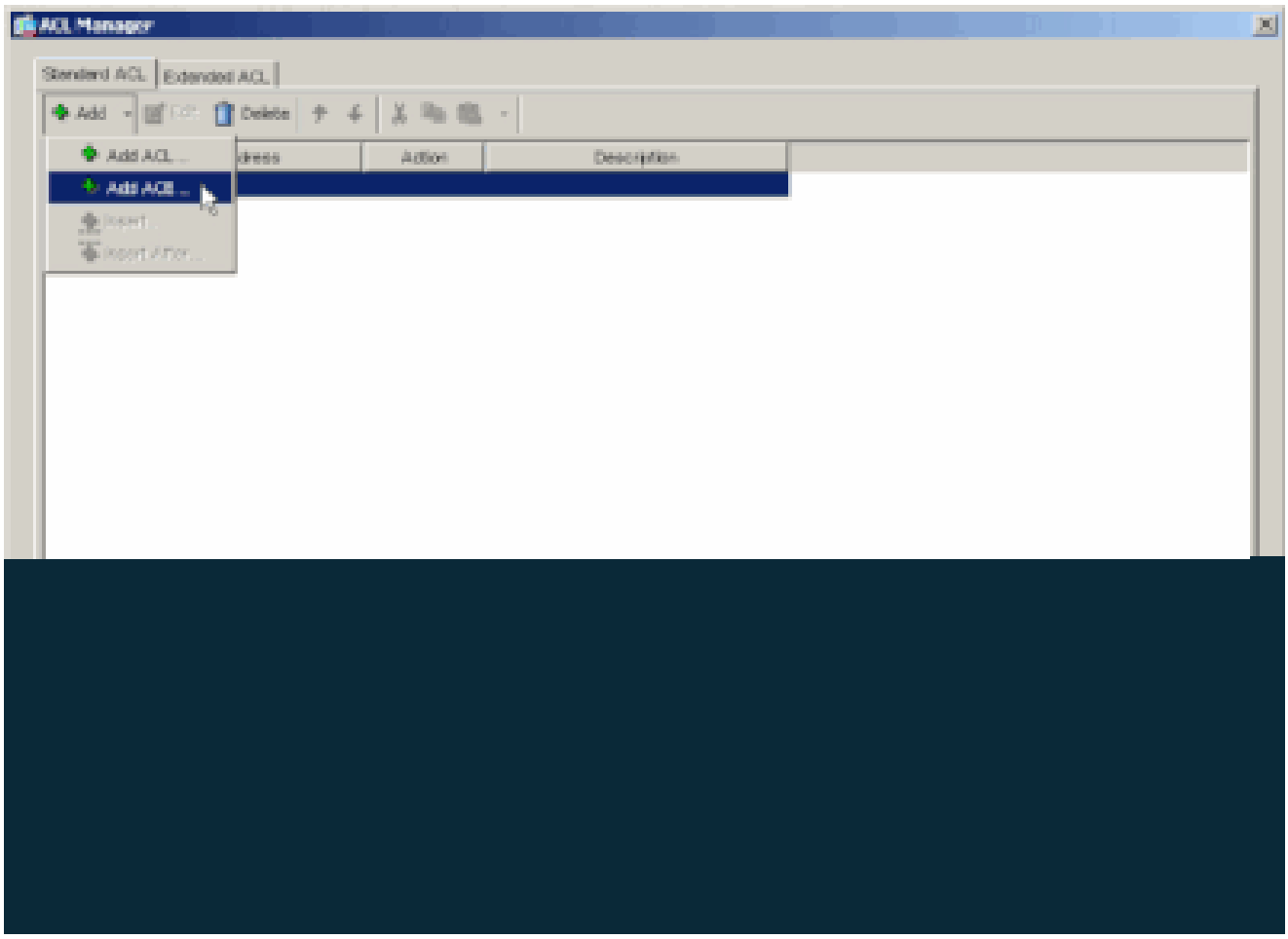
•

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



•

Una vez creada la ACL, elija **Add > Add ACE. .**para agregar una entrada de control de acceso (ACE).



•

Defina el ACE que corresponde al LAN detrás del ASA. En este caso, la red es 10.0.1.0/24.

a.

Seleccione Permit (Permitir).

b.

Elija una dirección IP de 10.0.1.0.

c.

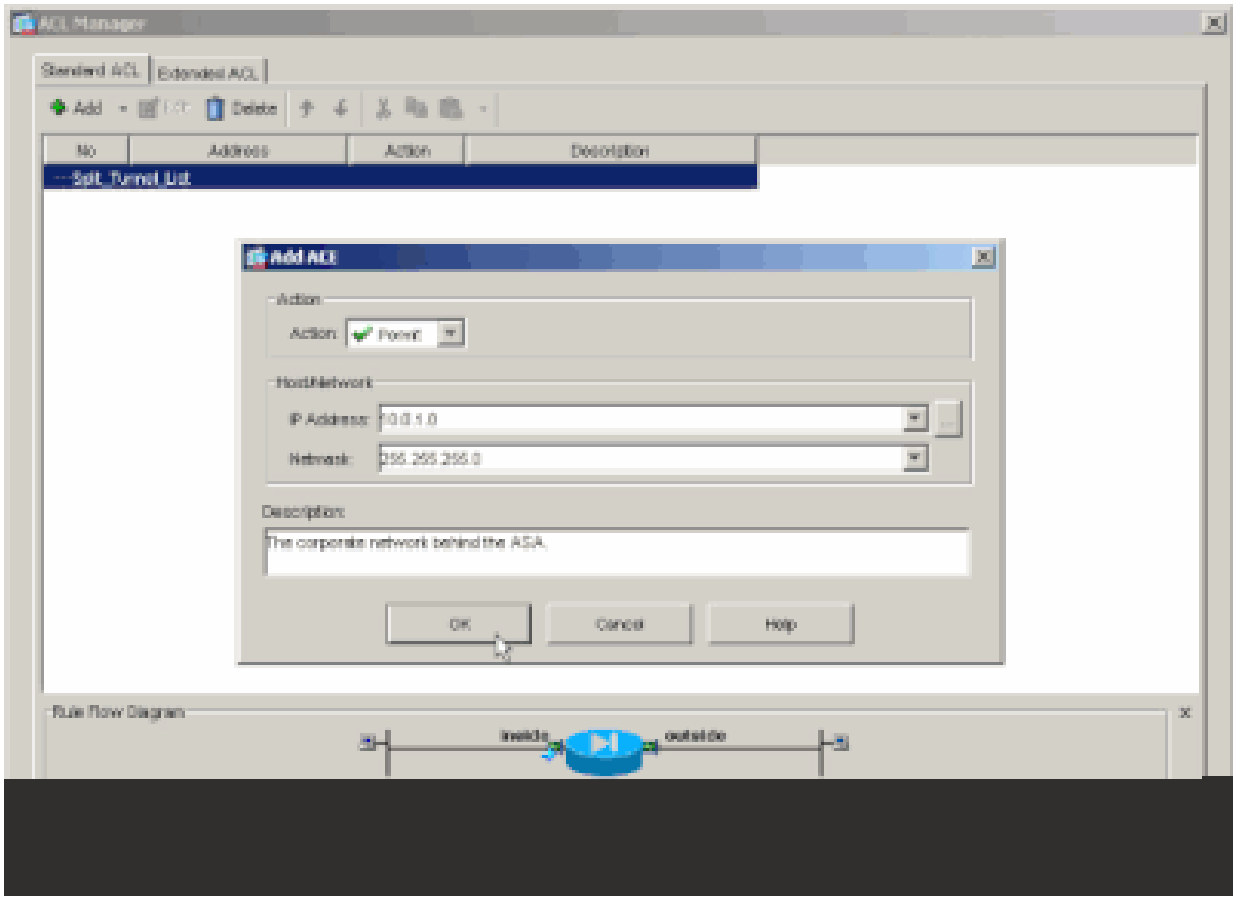
Elija una máscara de red de **255.255.255.0**.

d.

*(Opcional)*Proporcione una descripción.

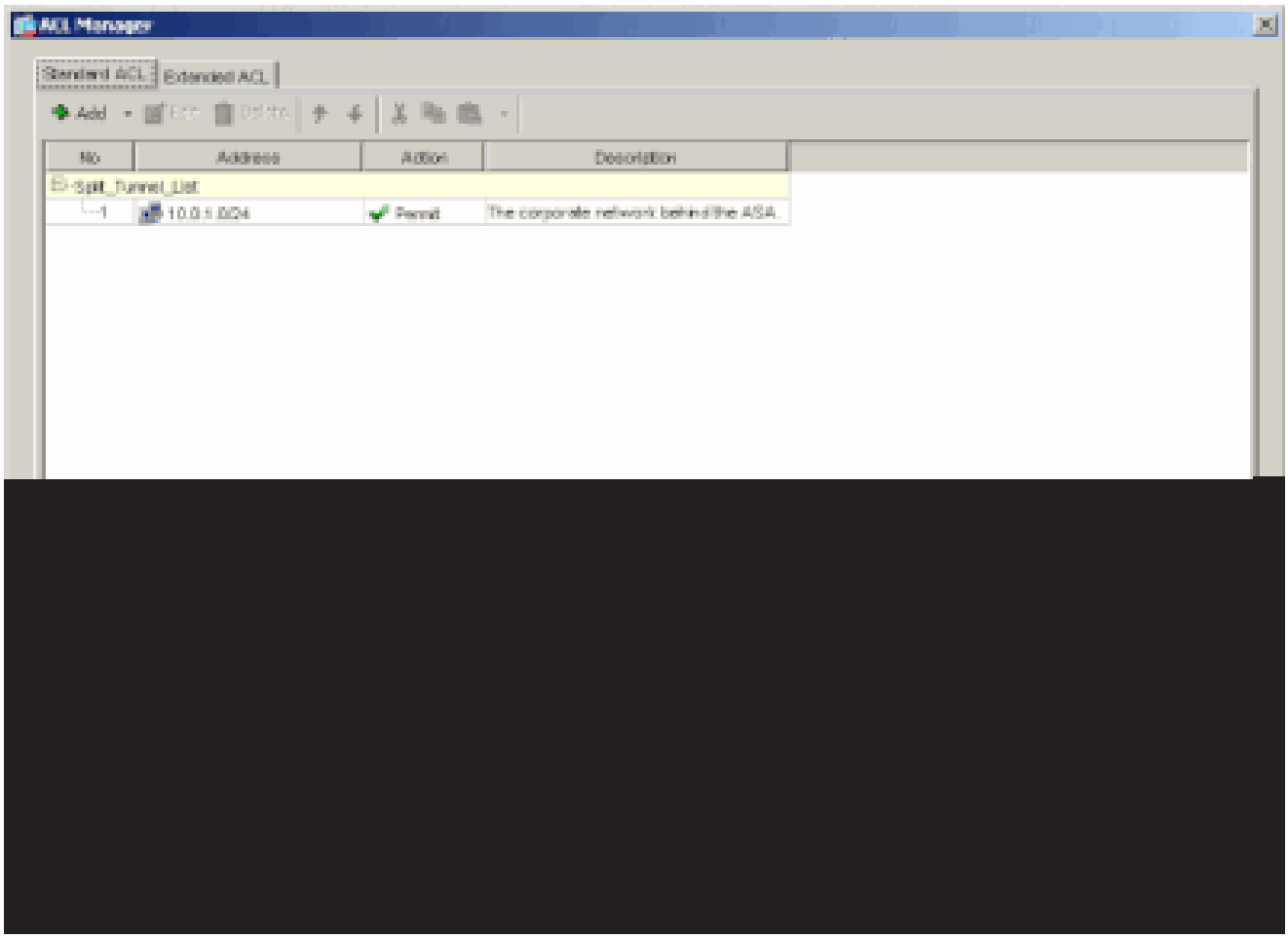
e.

Haga clic en > **Aceptar**.



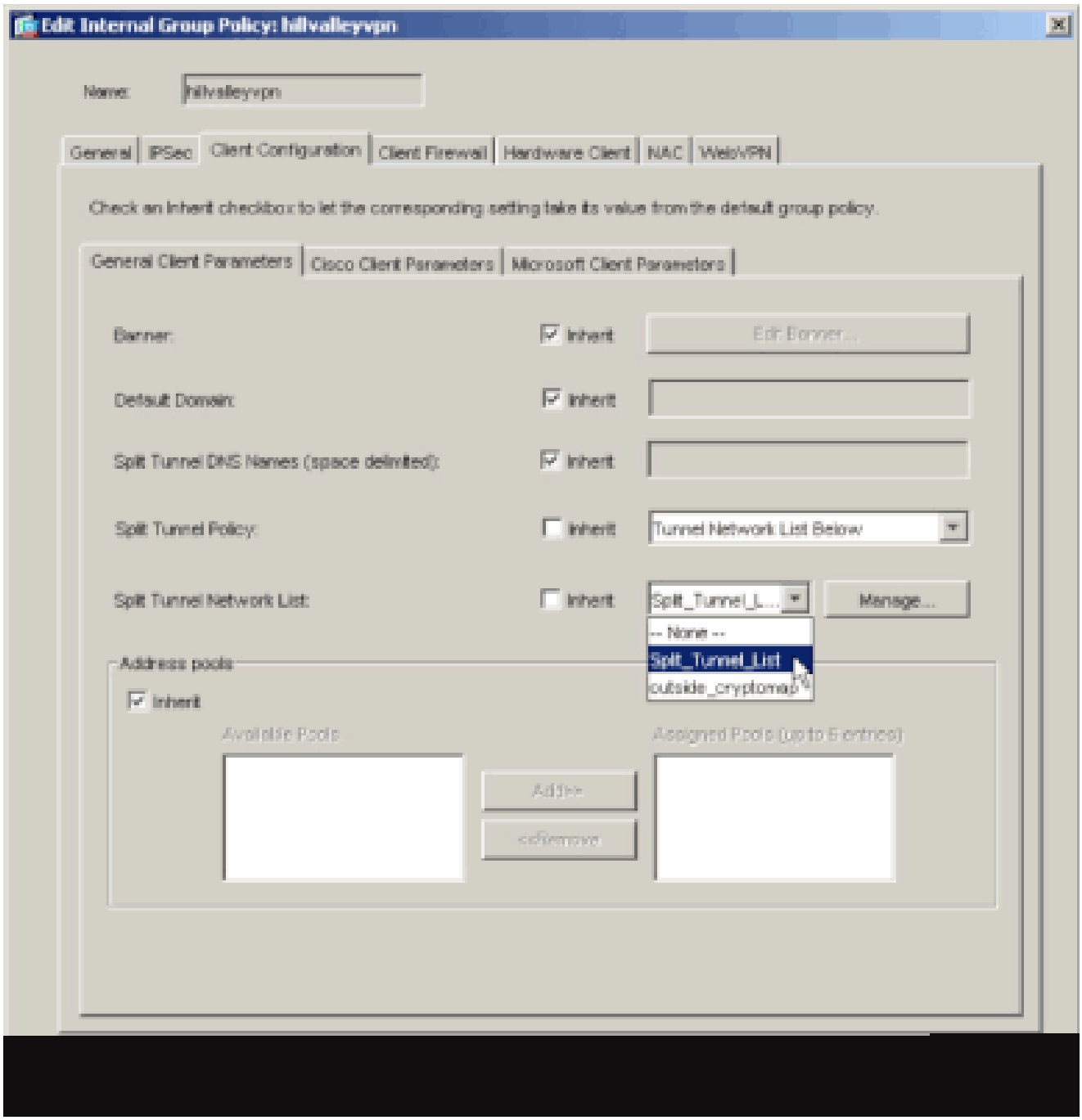
•

Haga clic en OK para salir del Administrador de ACL.



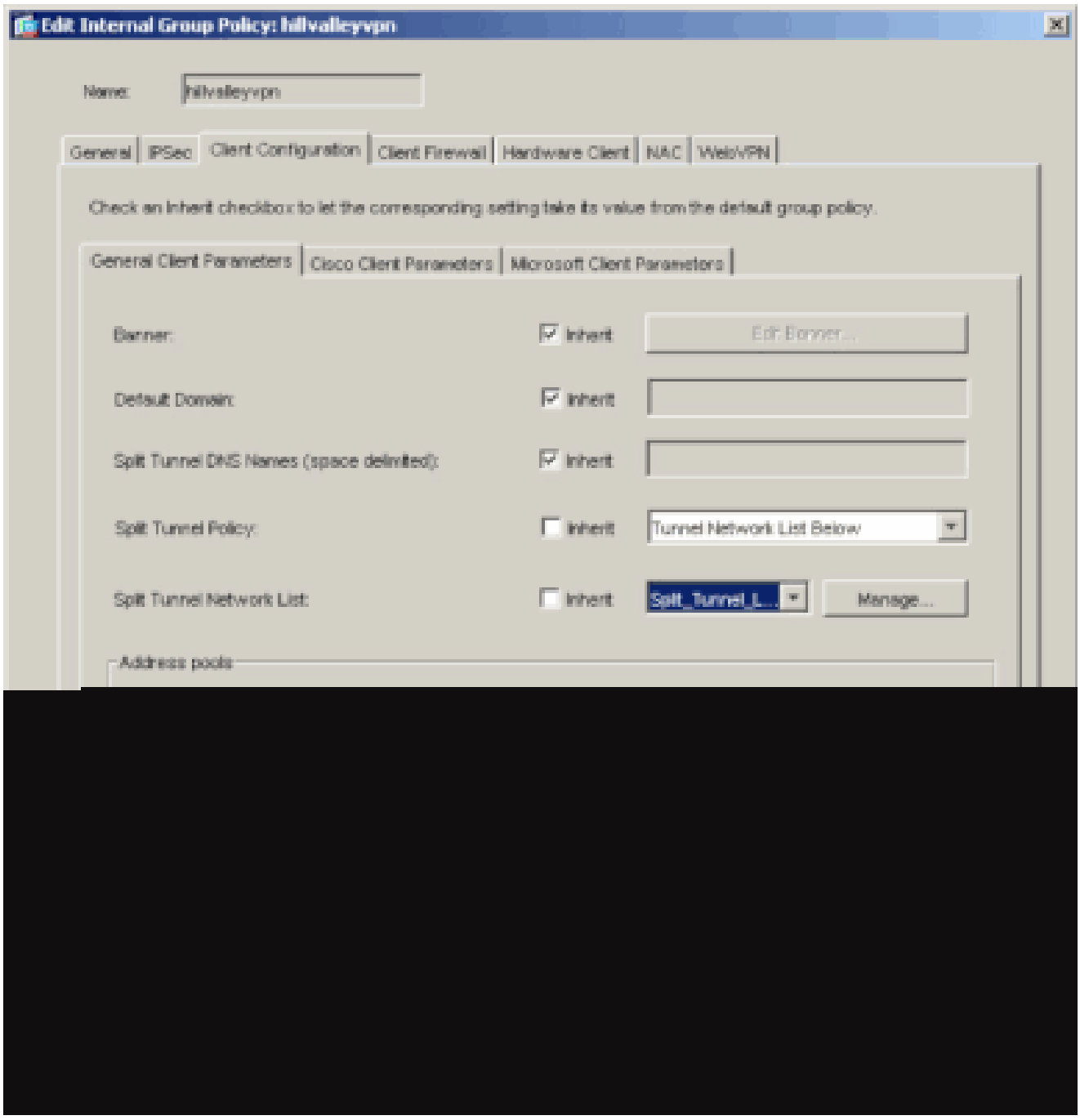
•

Asegúrese de que la ACL que acaba de crear esté seleccionada para la Lista de Red de Túnel Dividido.



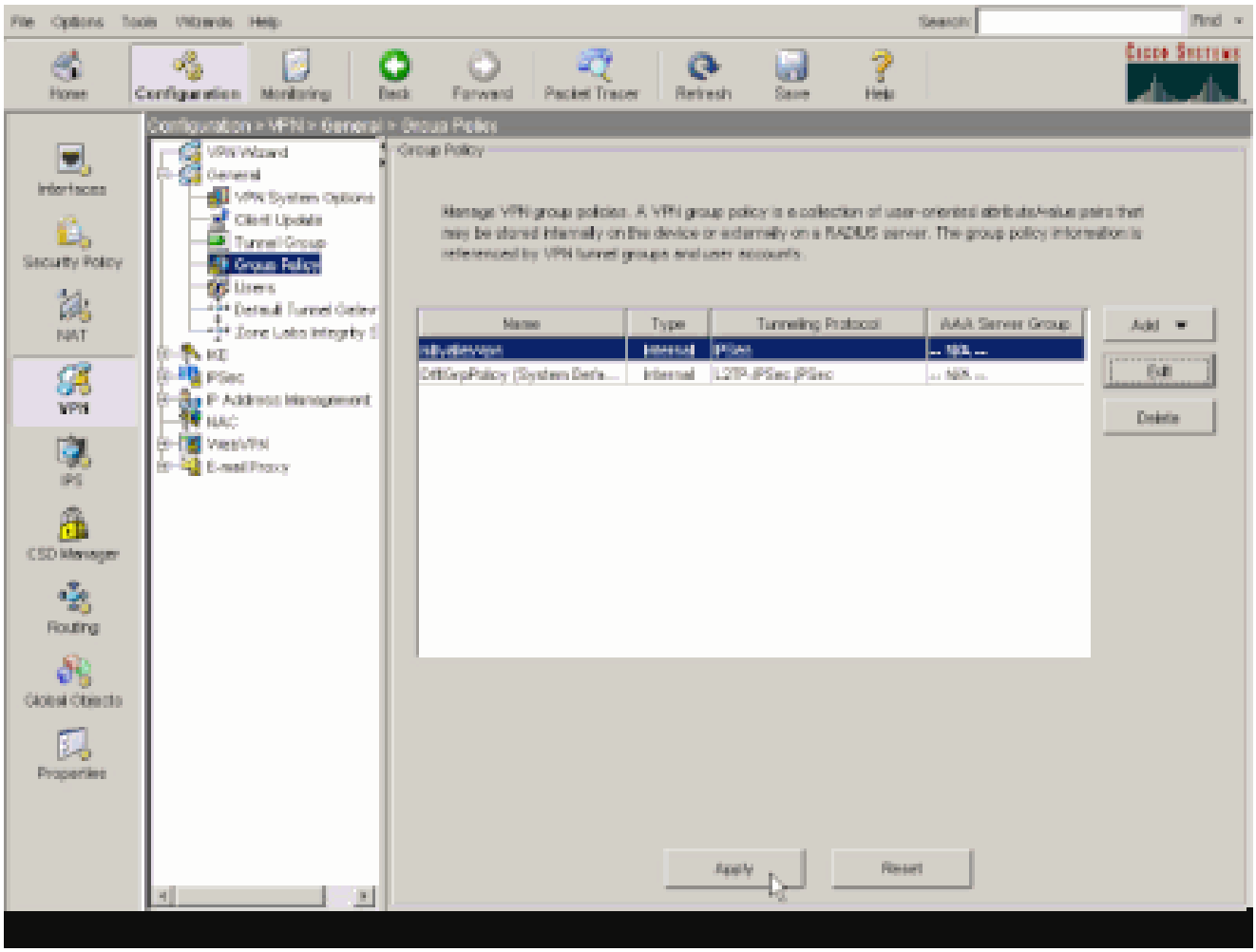
•

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



•

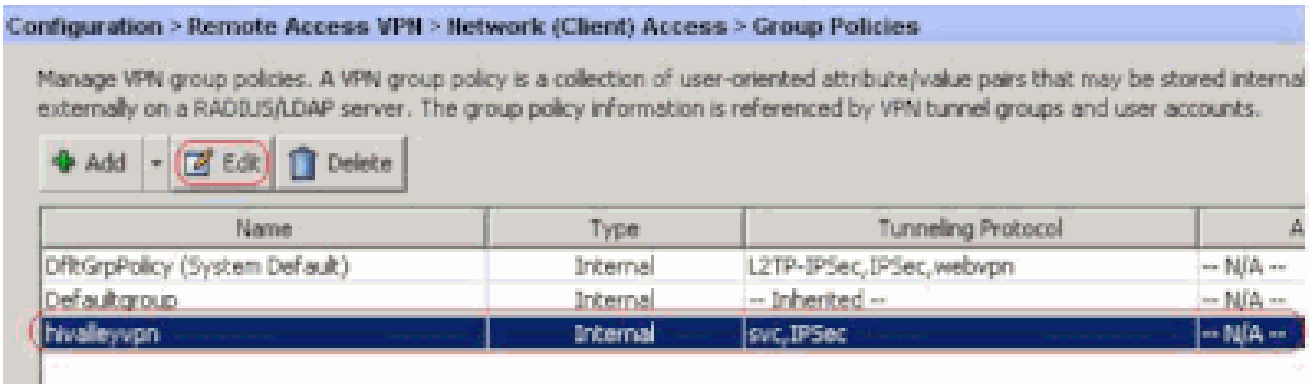
Haga clic en Apply (Aplicar) y, luego, en Send (Enviar) (si es necesario) para enviar comandos al ASA.



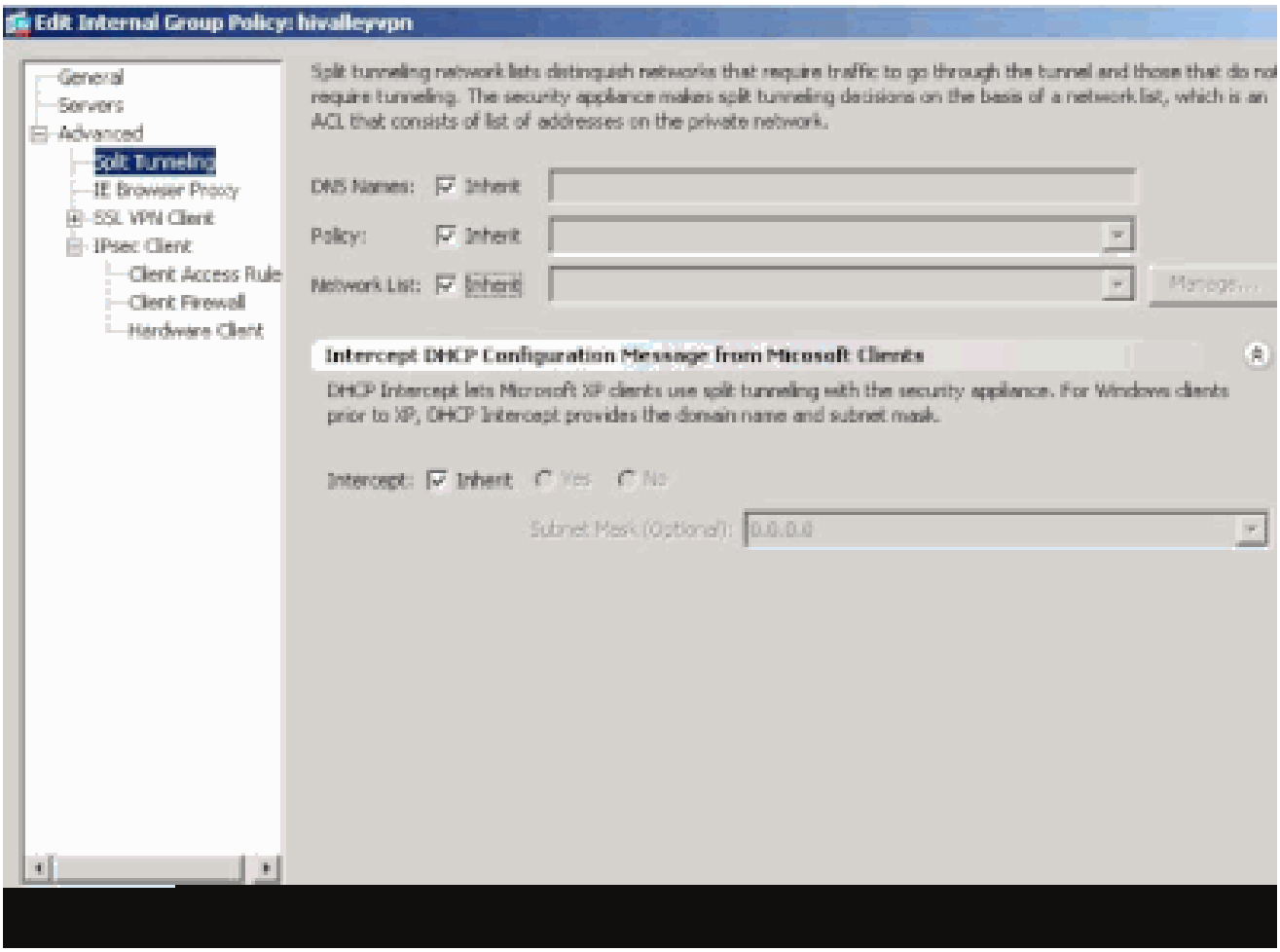
Configuración de ASA 8.x con ASDM 6.x

Complete estos pasos para configurar su grupo de túnel para permitir la tunelización dividida para los usuarios en el grupo.

- Elija **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** , y elija la política de grupo en la que desea habilitar el acceso LAN local. Luego, haga clic en Edit (Editar).

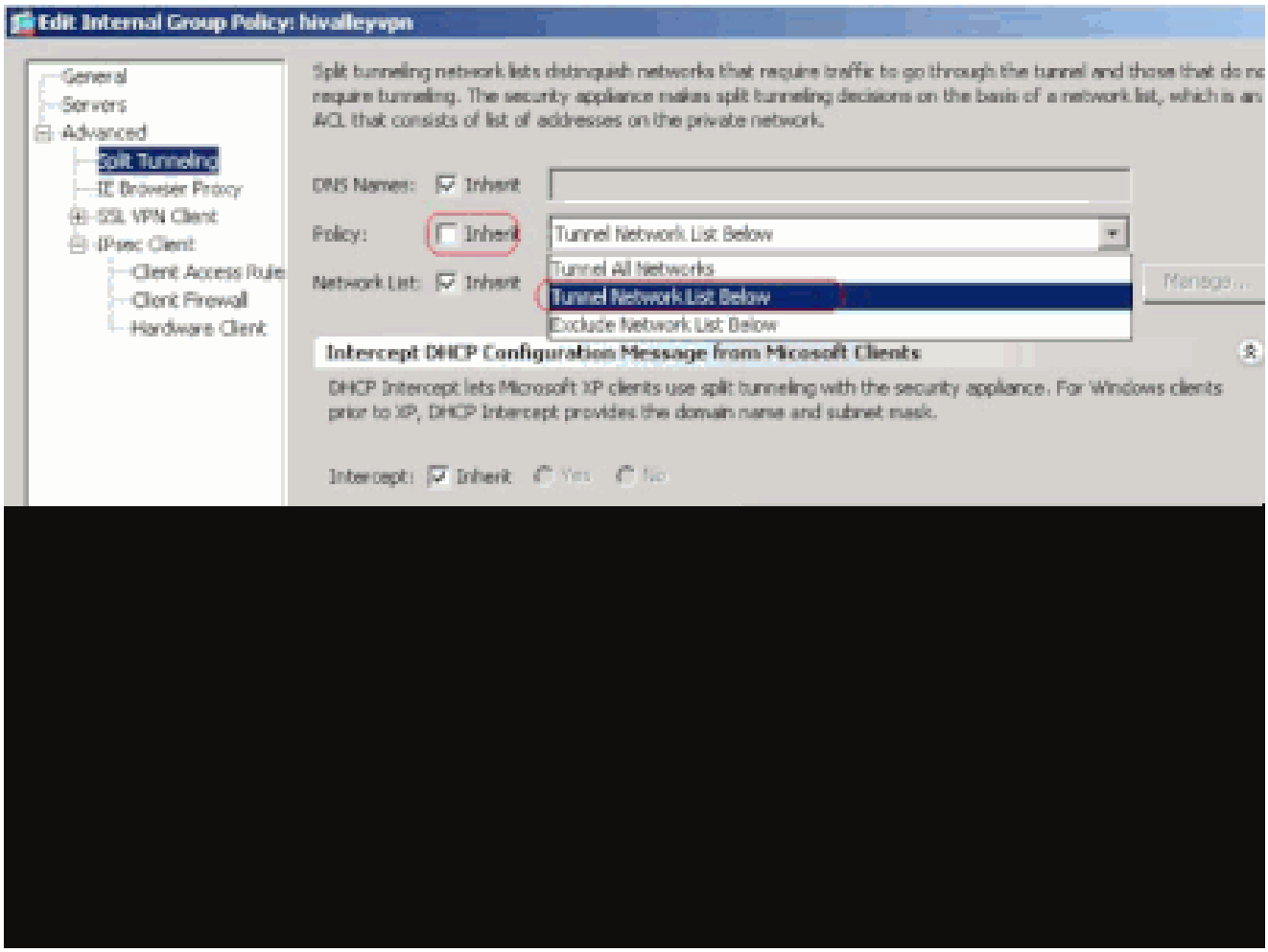


- Haga clic en **Split Tunneling**.



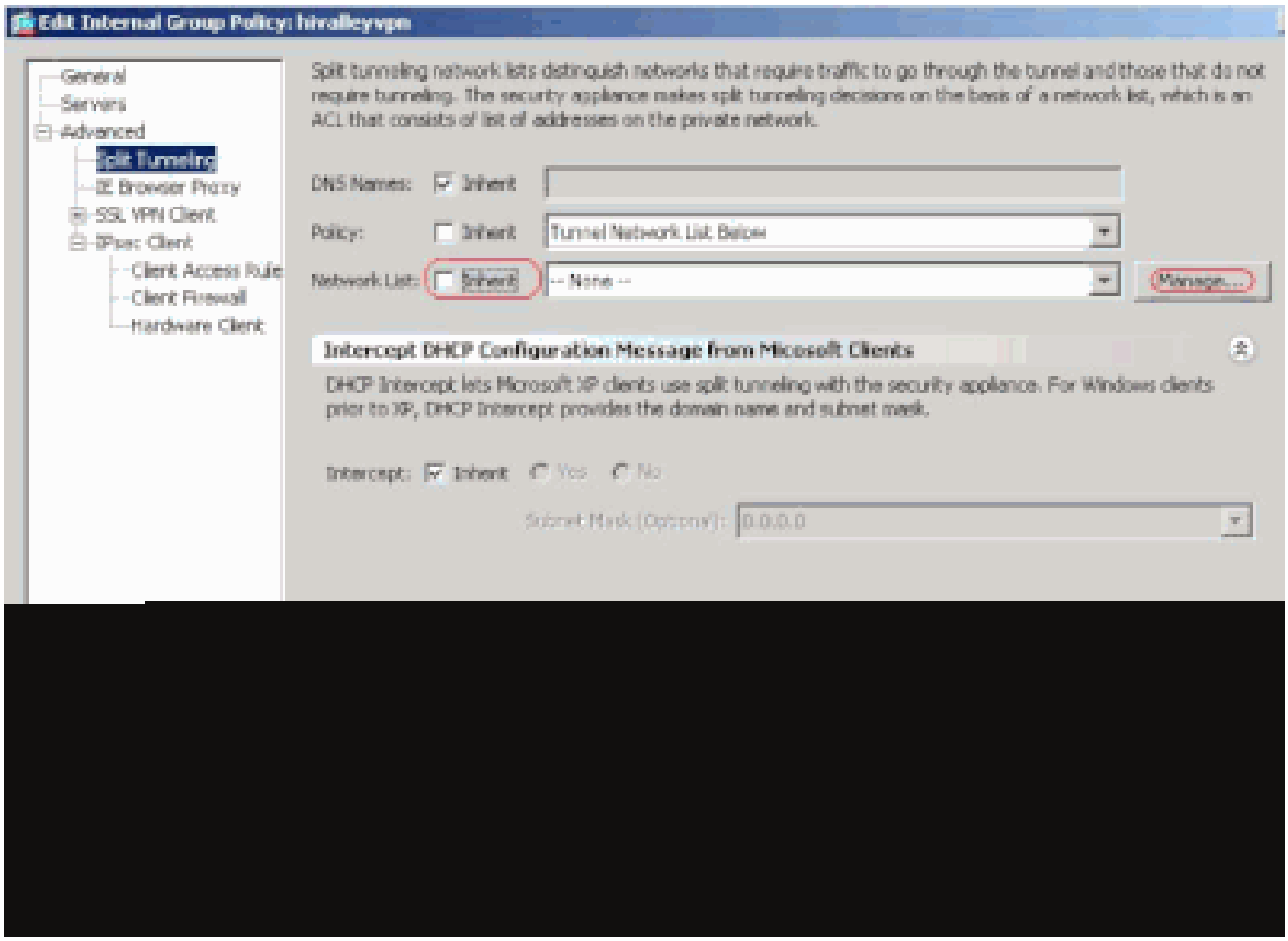
•

Desmarque la casilla **Inherit** para la política de túnel dividido y elija la **Lista de redes de túnel a continuación**.



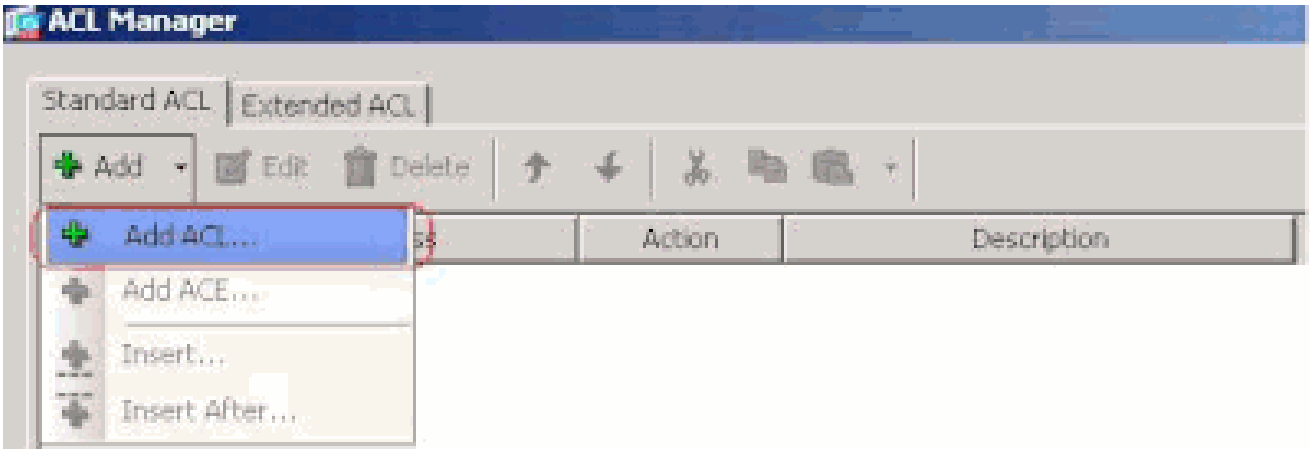
•

Desmarque la casilla **Inherit** para la Lista de Red de Túnel Dividido y luego haga clic en **Manage** para iniciar el Administrador ACL.



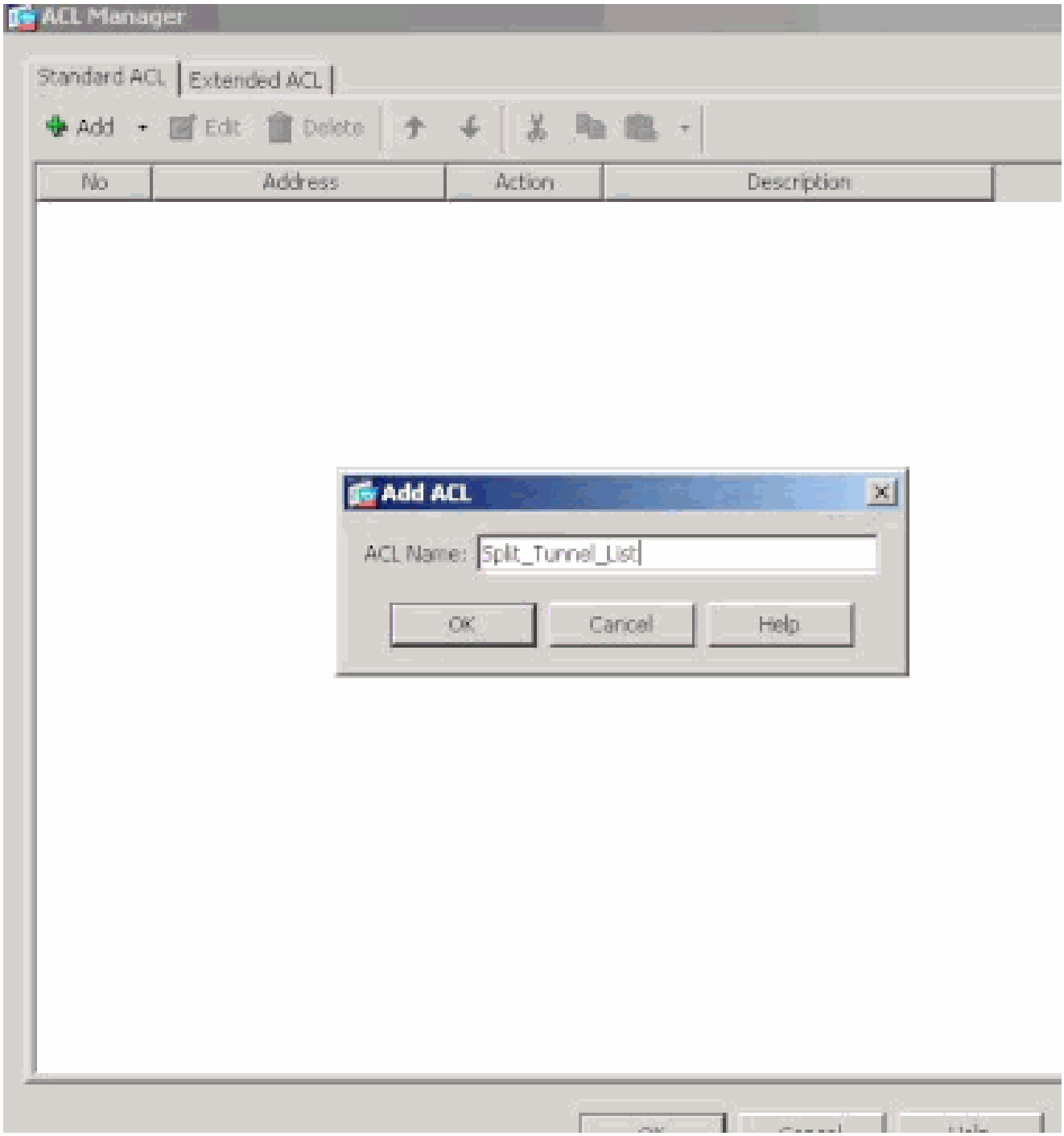
•

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



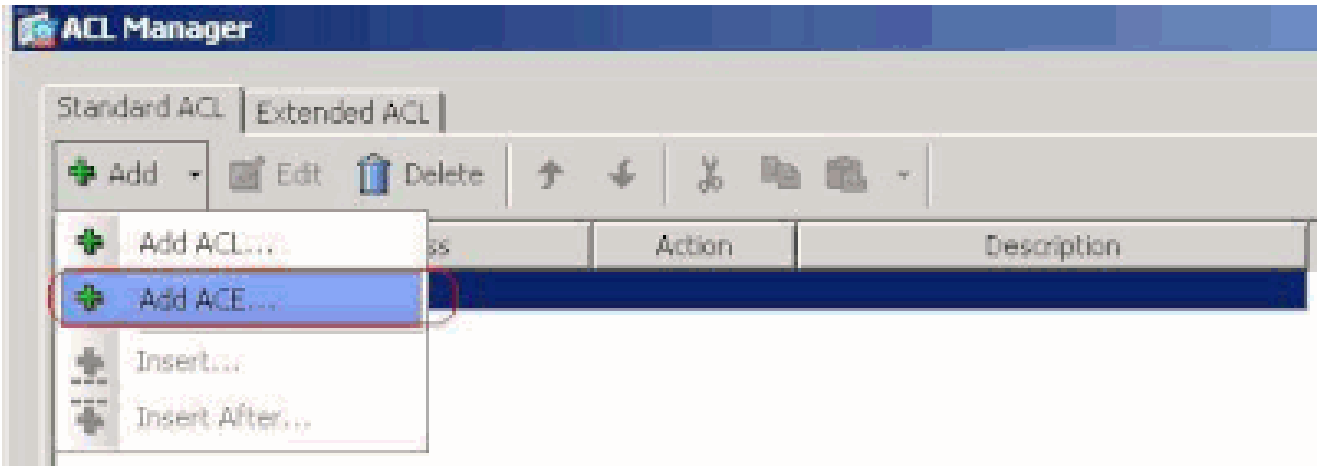
•

Proporcione un nombre para la ACL y haga clic en **OK**.



•

Una vez creada la ACL, seleccione Add > Add ACE... (Agregar > Agregar ACE...) para agregar una entrada de control de acceso (ACE).



-

Defina el ACE que corresponde al LAN detrás del ASA. En este caso, la red es 10.0.1.0/24.

a.

Haga clic en el botón de opción **Permitir**.

b.

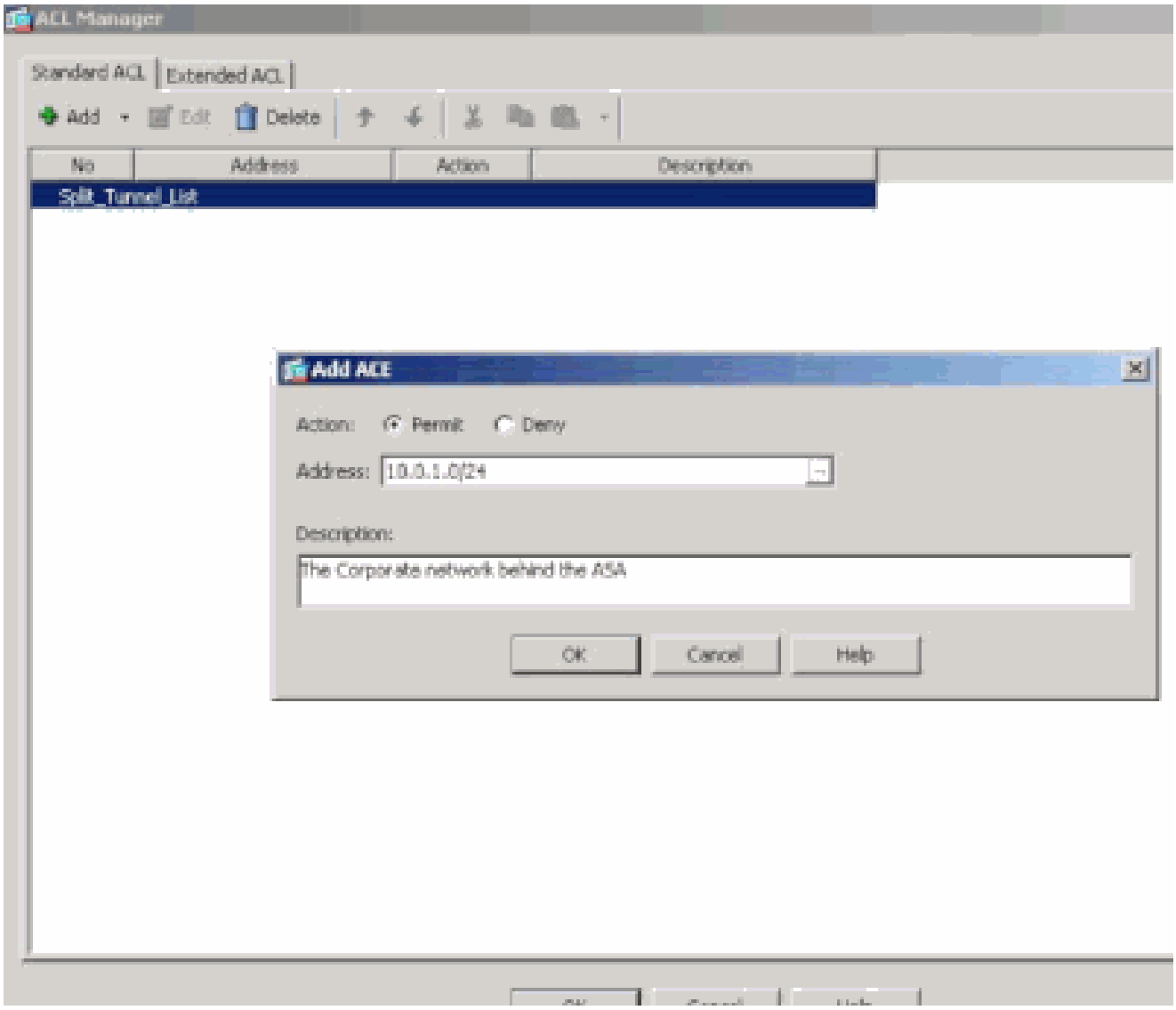
Elija la dirección de red con la máscara **10.0.1.0/24**.

c.

(Opcional) Proporcione una descripción.

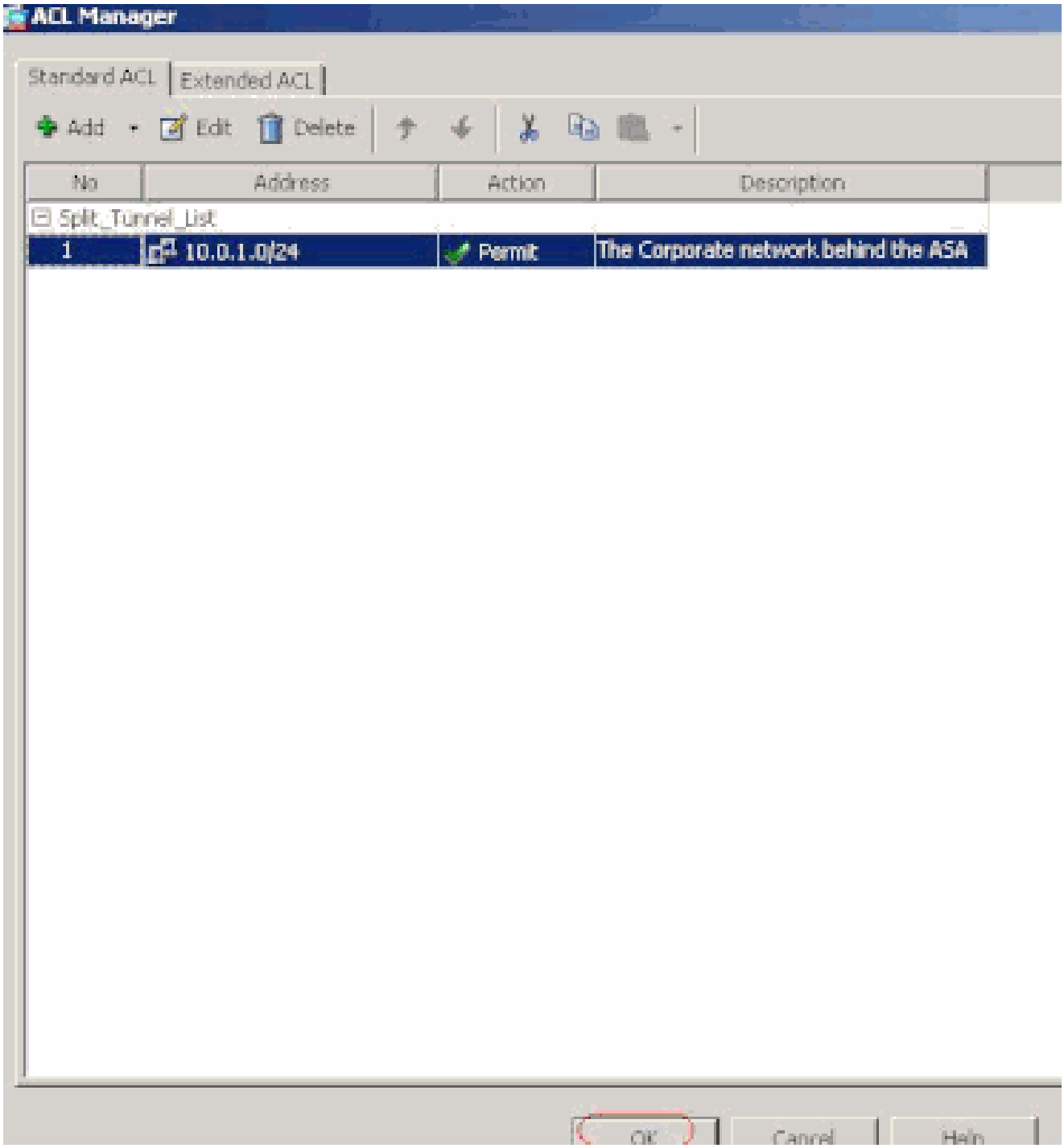
d.

Click OK.



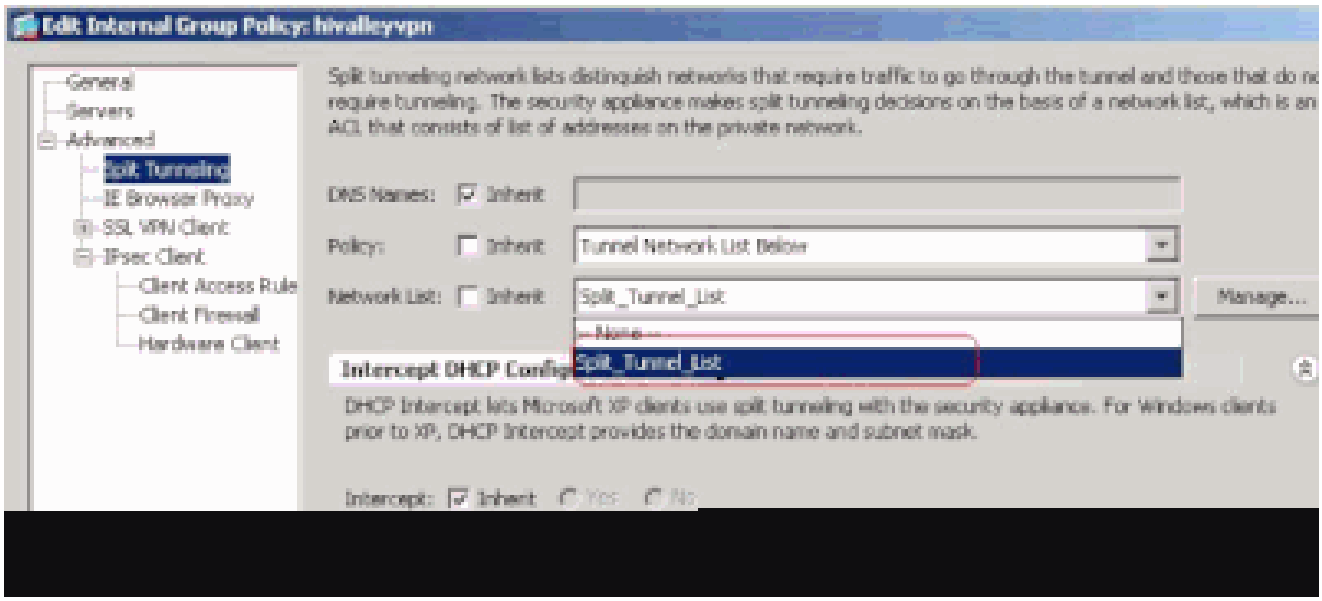
•

Haga clic en OK para salir del Administrador de ACL.



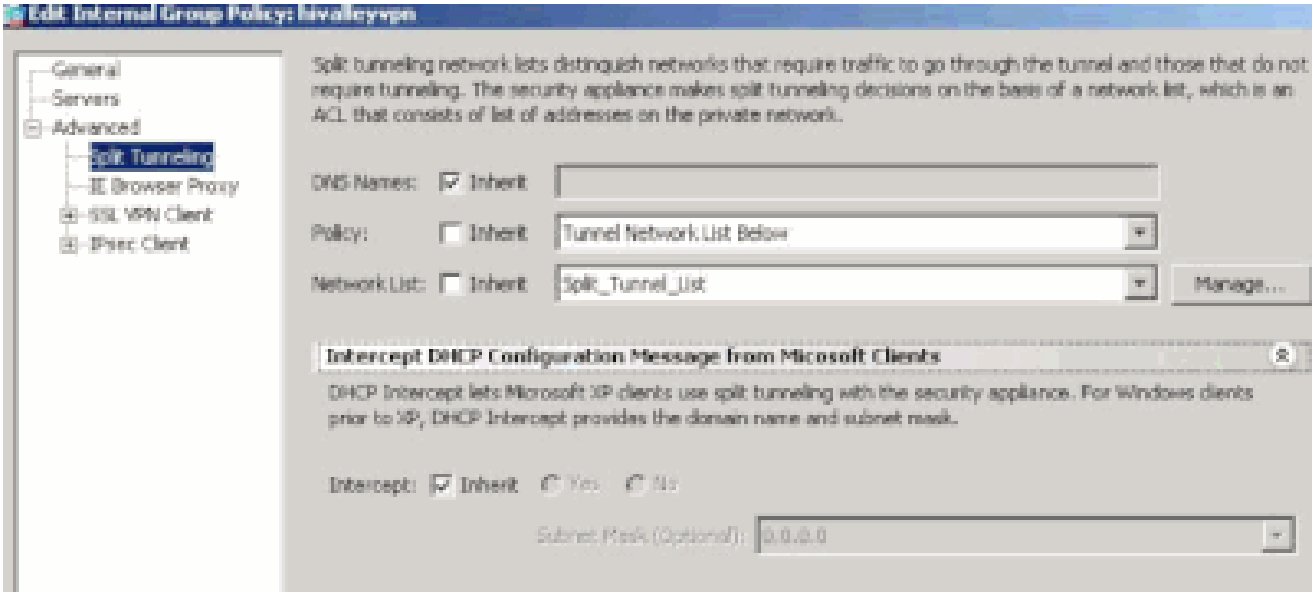
•

Asegúrese de que la ACL que acaba de crear esté seleccionada para la Lista de Red de Túnel Dividido.



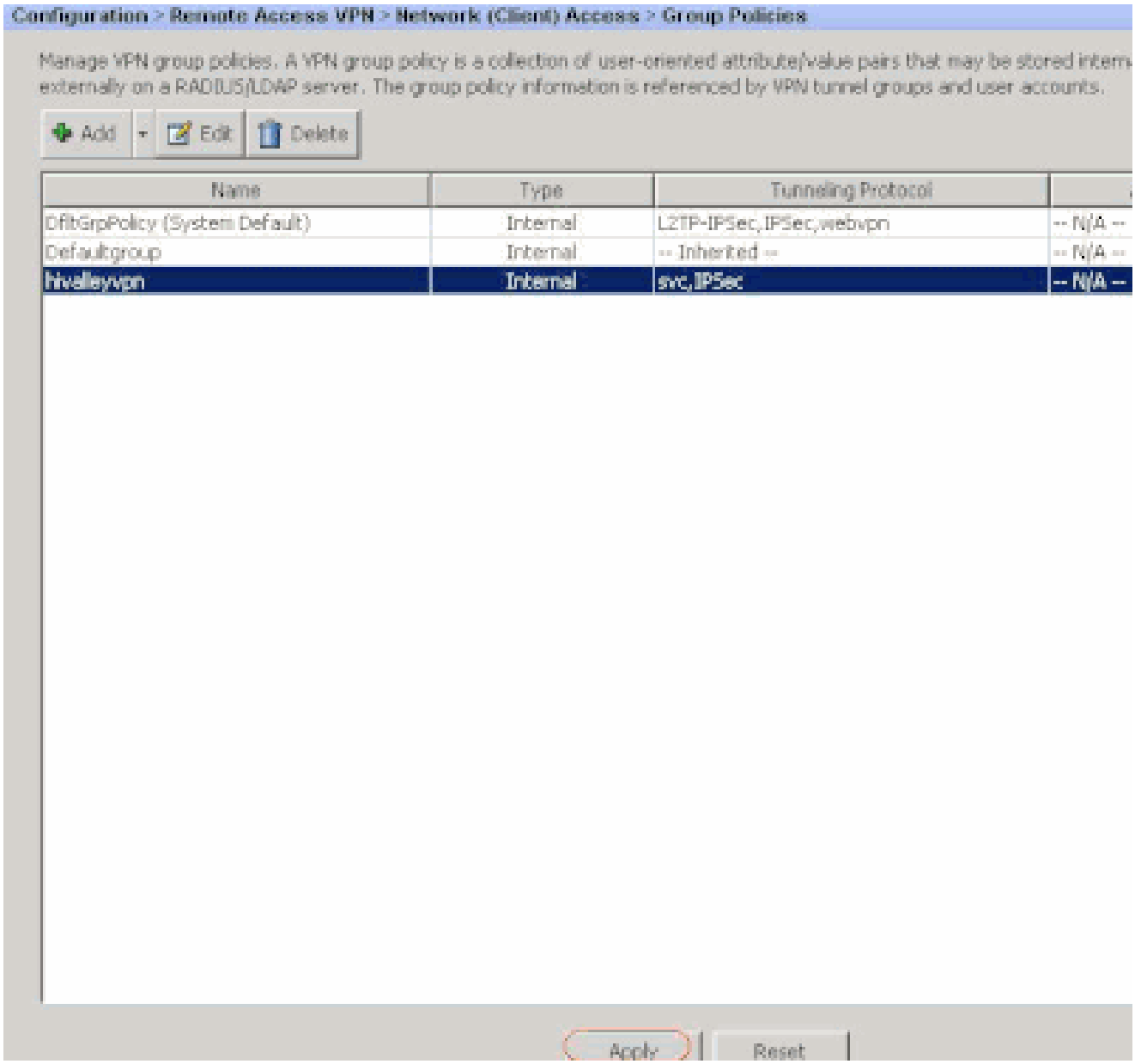
•

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



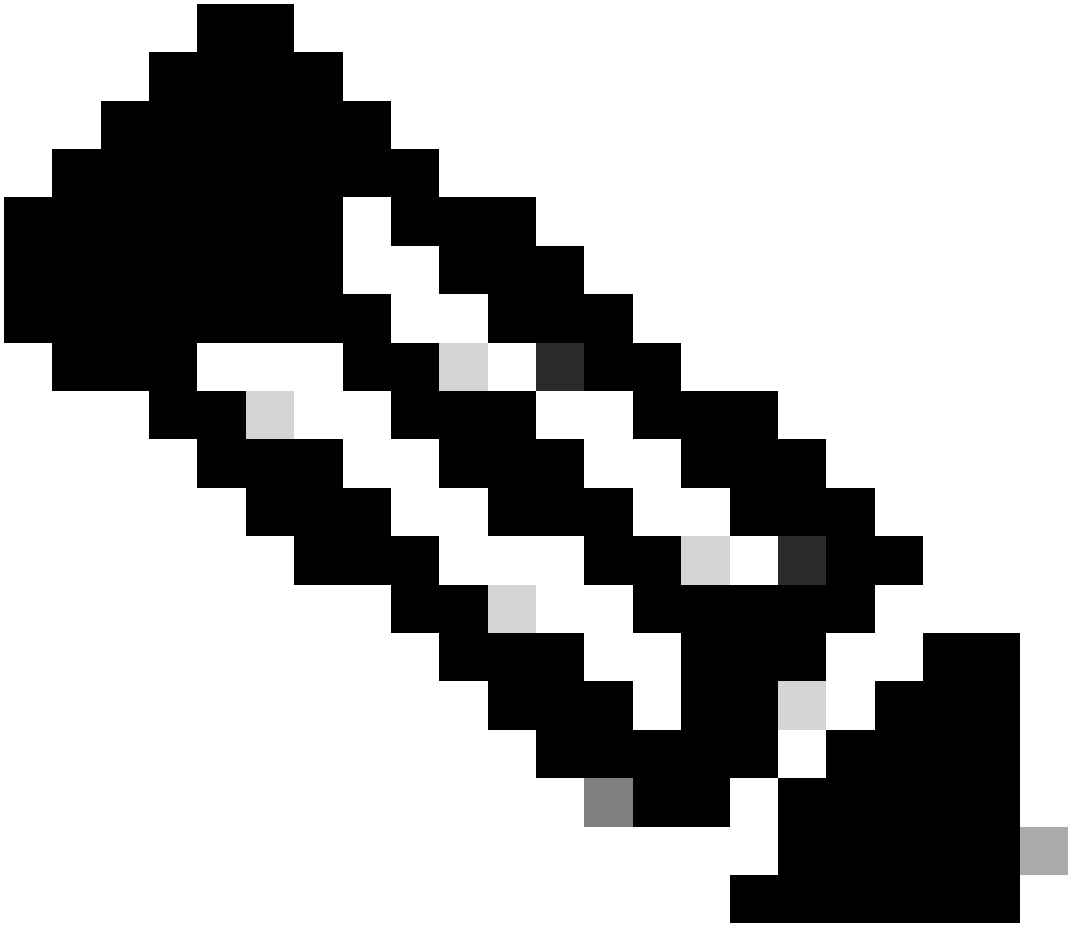
•

Haga clic en Apply (Aplicar) y, luego, en Send (Enviar) (si es necesario) para enviar comandos al ASA.



Configuración de ASA 7.x y posterior mediante CLI

En lugar de utilizar el ASDM, puede completar estos pasos en la CLI de ASA para permitir la tunelización dividida en el ASA:



Nota: La configuración de la tunelización dividida CLI es la misma para ASA 7.x y 8.x.

- Ingrese al modo de configuración.

```
<#root>

ciscoasa>
```

```
enable
```

```
Password: ********
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

-

Cree la lista de acceso que define la red detrás del ASA.

```
    <#root>

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
```

-

Introduzca el modo de configuración de directiva de grupo para la directiva que desea modificar.

```
    <#root>

ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

```
ciscoasa(config-group-policy)#
```

-

Especifique la política de tunel dividido. En este caso, la política se especifica **tunnelspecified**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

-

Especifique la lista de acceso de tunel dividido. En este caso, la lista es **Split_Tunnel_List**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-network-list value Split_Tunnel_List
```

-

Ejecutar este comando:

```
    <#root>

ciscoasa(config)#

 tunnel-group hillvalleyvpn general-attributes
```

-

Asocie la política del grupo al grupo de túnel

```
    <#root>

ciscoasa(config-tunnel-ipsec)#

 default-group-policy hillvalleyvpn
```

-

Salga de los dos modos de configuración.

```
    <#root>

ciscoasa(config-group-policy)#

 exit

ciscoasa(config)#

 exit
```

```
ciscoasa#
```

- Guarde la configuración en la RAM no volátil (NVRAM) y presione Enter (Entrar) cuando se le solicite especificar el nombre de archivo de origen.

```
    <#root>

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#
```

Configuración de PIX 6.x a través de la CLI

Complete estos pasos:

- Cree la lista de acceso que define la red detrás del PIX.

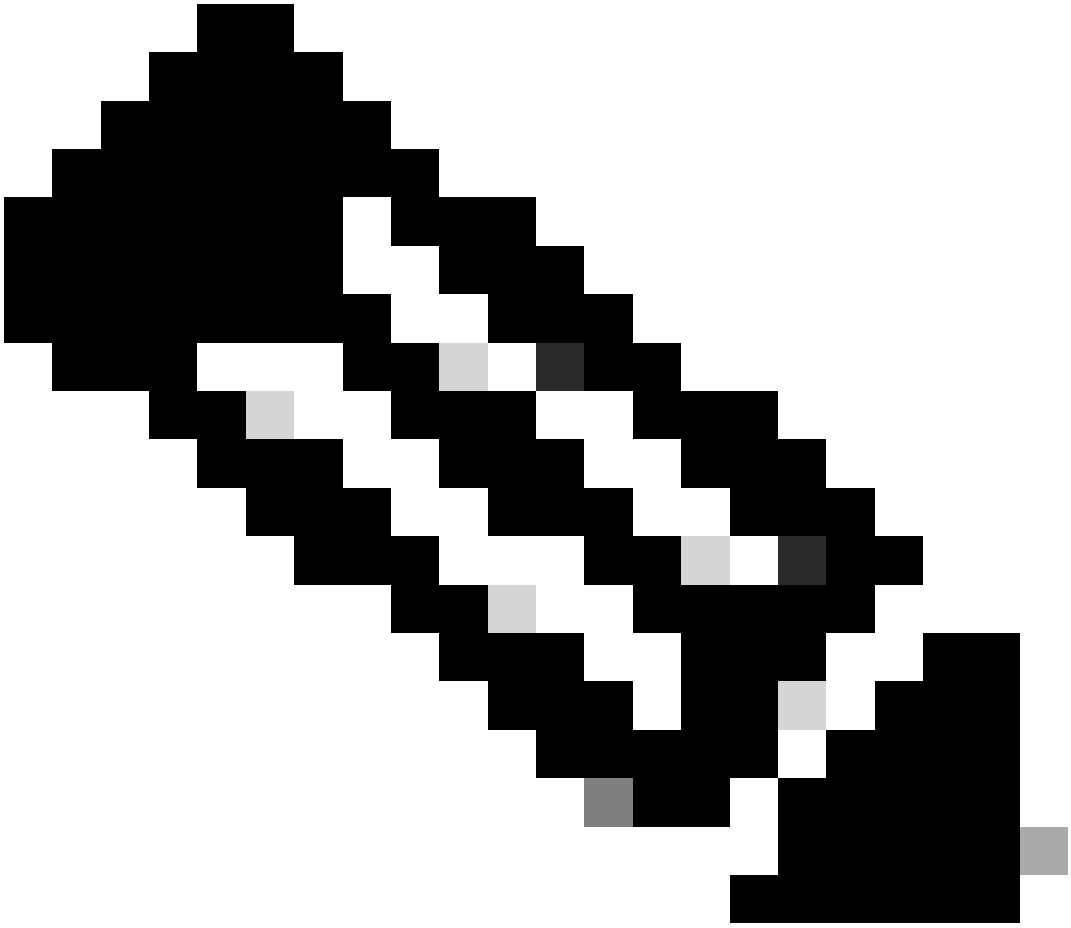
```
    <#root>

 PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- Cree un vpn group **vpn3000** y especifique la ACL de túnel dividido a él como se muestra:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



Nota: Refiérase a Cisco Secure PIX Firewall 6.x y Cisco VPN Client 3.5 para Windows con la Autenticación RADIUS de Microsoft Windows 2000 y 2003 IAS para obtener más información sobre la configuración VPN de acceso remoto para PIX 6.x.

Verificación

Siga los pasos de estas secciones para verificar la configuración.

- Conexión con el cliente VPN

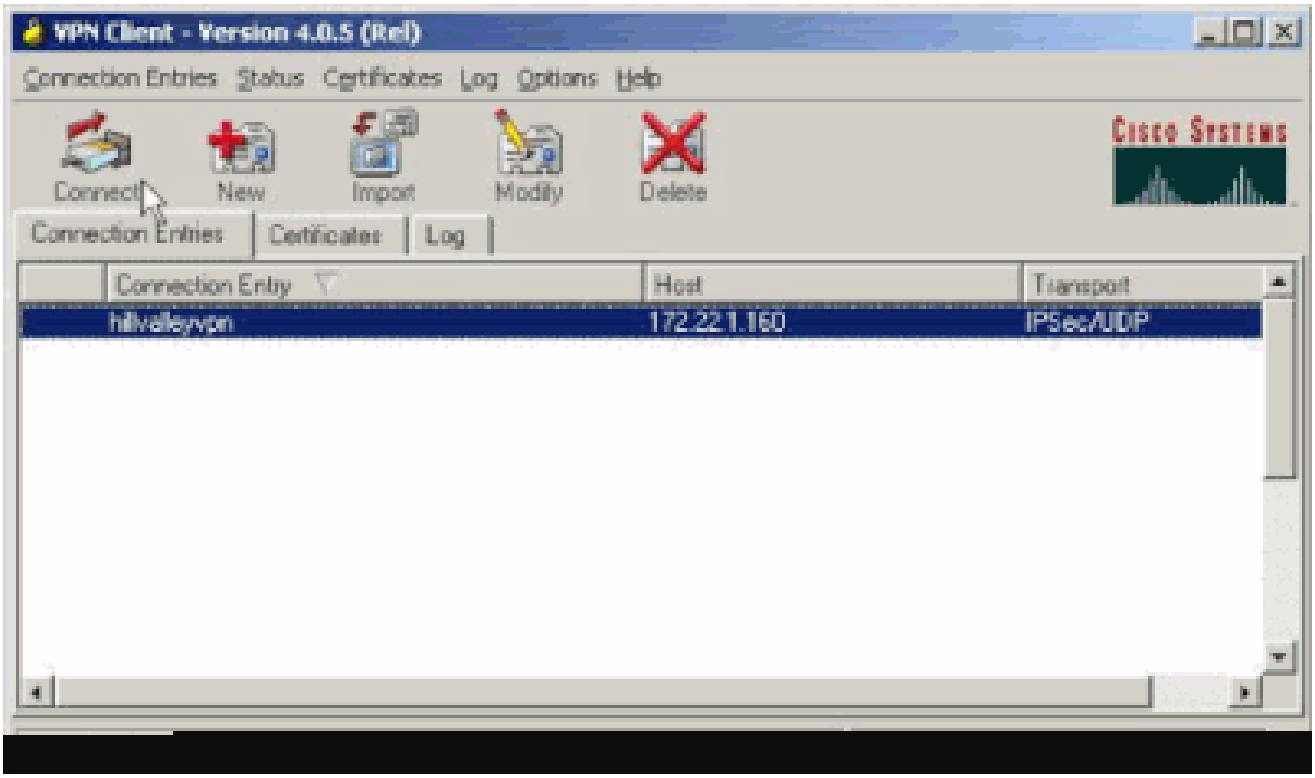
- Ver el registro del cliente VPN

- Probar el acceso LAN local con ping

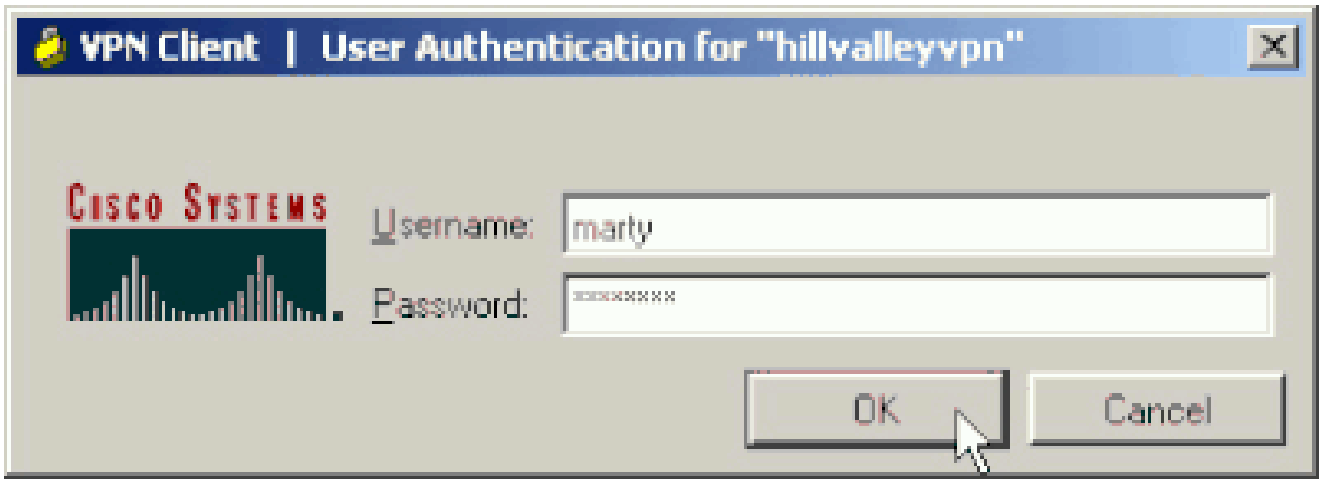
Conexión con el cliente VPN

Conecte su VPN Client al VPN Concentrator para verificar su configuración.

- Elija la entrada de conexión de la lista y haga clic en **Connect**.

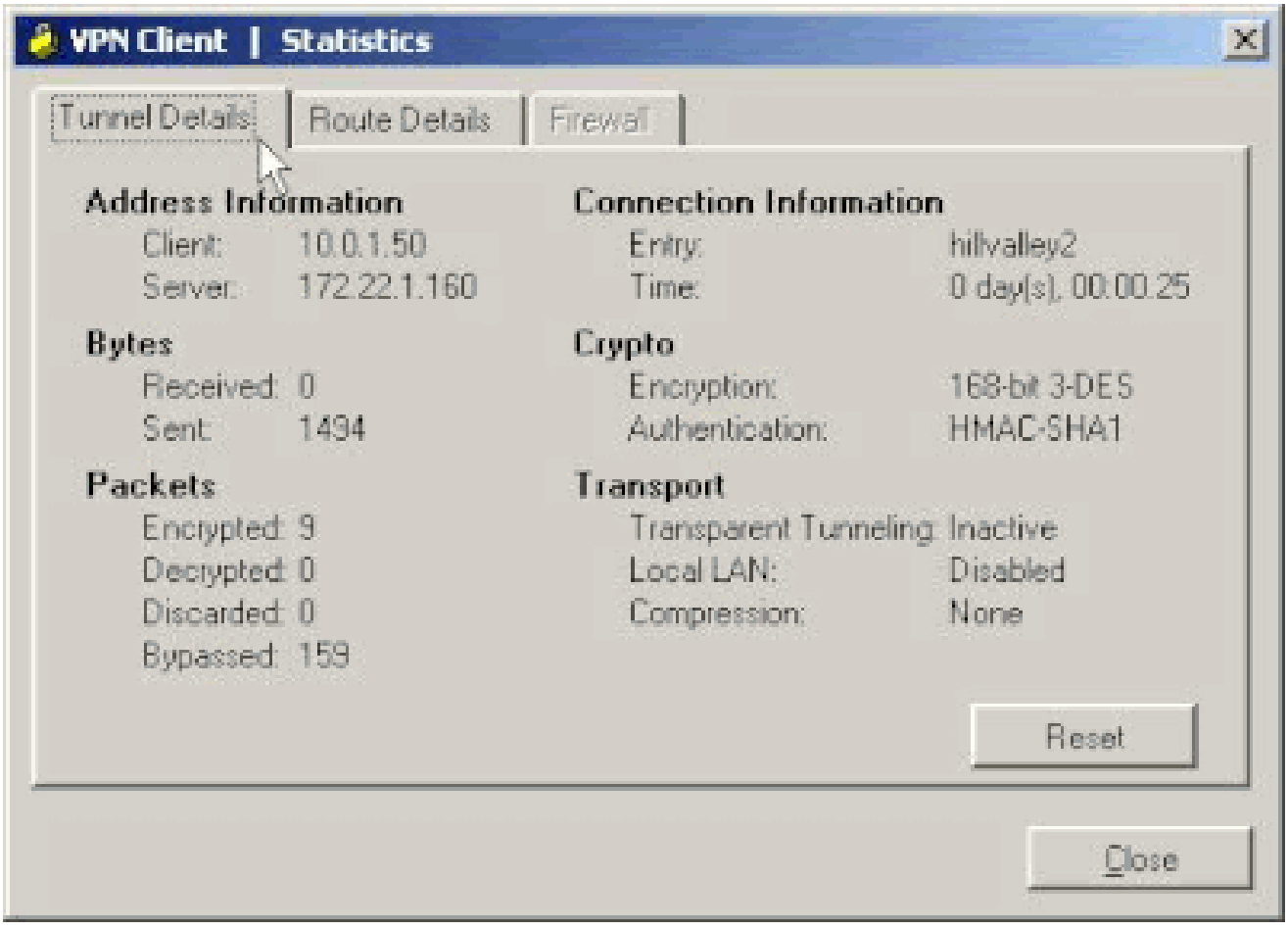


- Introduzca sus credenciales.



-

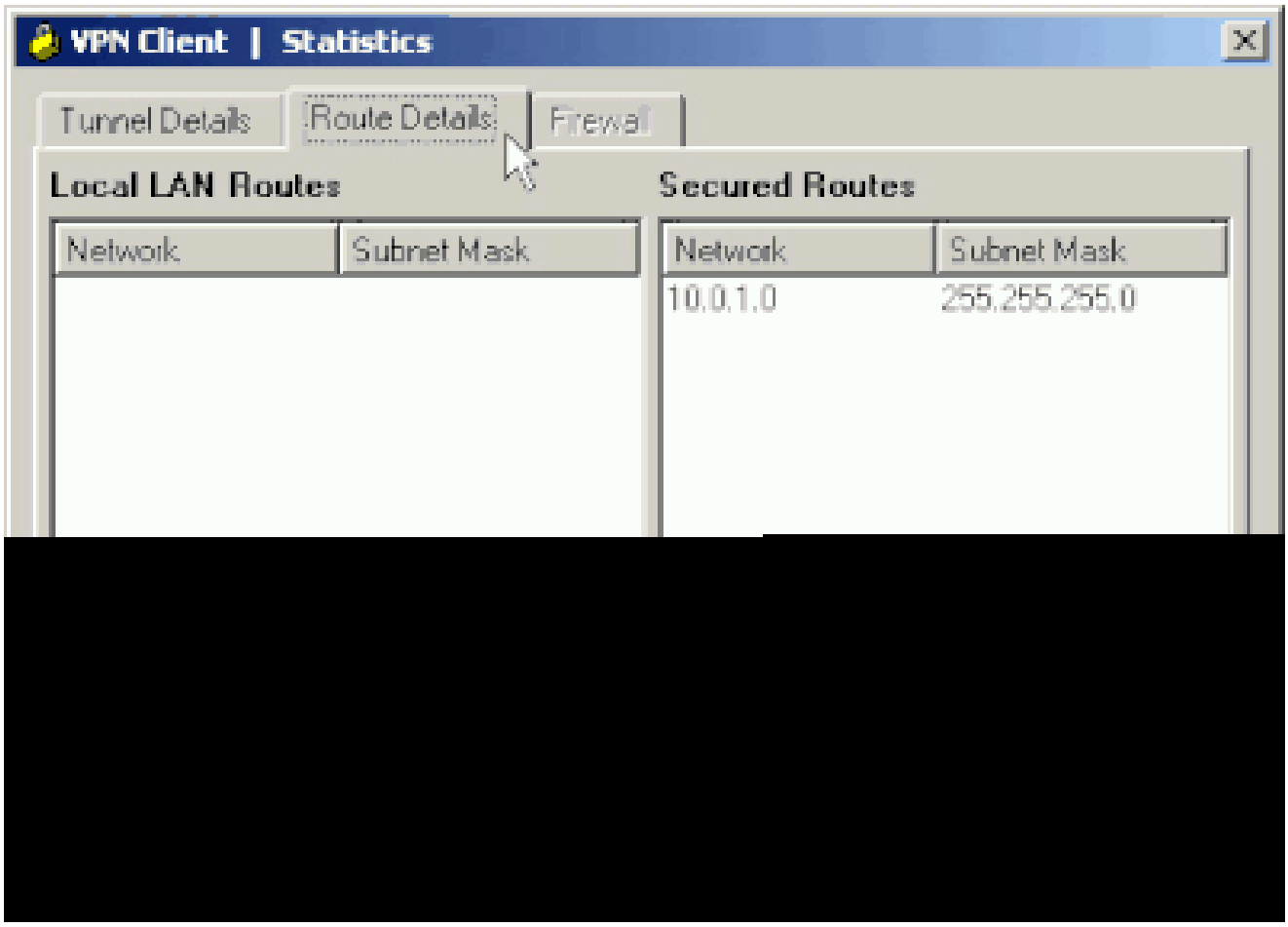
Elija **Status > Statistics...** para visualizar la ventana Detalles del Túnel donde puede inspeccionar los detalles del túnel y ver el tráfico que fluye.



-

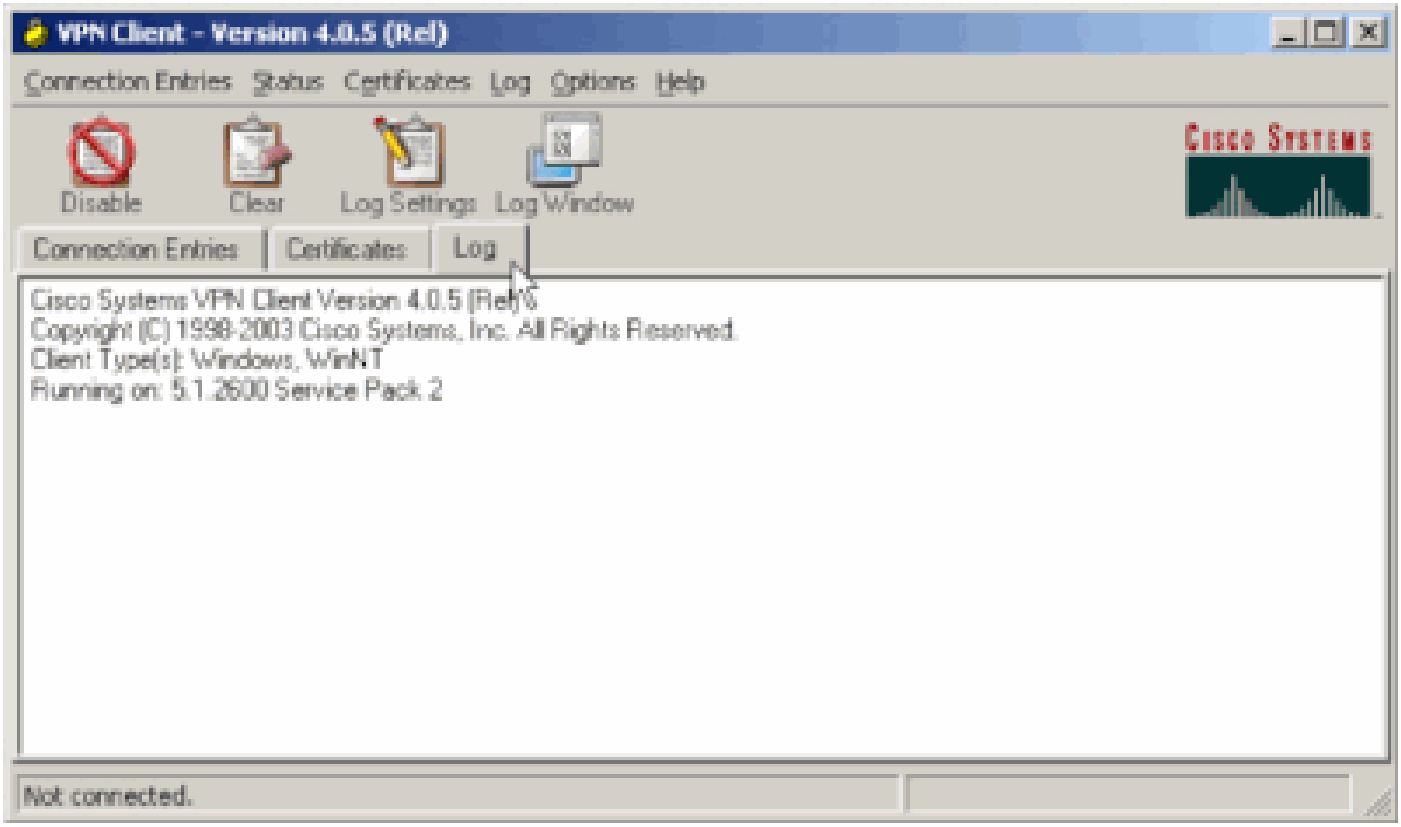
Vaya a la ficha Route Details para ver las rutas que el cliente VPN está asegurando al ASA.

En este ejemplo, el cliente VPN protege 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.



Ver el registro del cliente VPN

Cuando examina el registro de VPN Client, puede determinar si el parámetro que especifica la tunelización dividida está establecido o no. Para ver el registro, vaya a la ficha Log (Registro) en VPN Client. Luego haga clic en **Log Settings** para ajustar lo que se registra. En este ejemplo, IKE se establece en **3 - High** mientras que todos los demás elementos de registro se establecen en **1 - Low**.




```
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/6    IKE/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.
```

Probar el acceso LAN local con ping

Una manera adicional de probar que el cliente VPN está configurado para la tunelización dividida mientras está tunelizado al ASA es utilizar el comando **ping** en la línea de comandos de Windows. La 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.

```
   <#root>

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
```

Troubleshoot

Limitación con Número de Entradas en una ACL de Túnel Dividido

Hay una restricción con el número de entradas en una ACL utilizada para el túnel dividido. Se recomienda no utilizar más de 50-60 entradas ACE para obtener una funcionalidad satisfactoria. Se recomienda implementar la función de subredes para cubrir un rango de direcciones IP.

Información Relacionada

- **Ejemplo de configuración de PIX/ASA 7.x como servidor VPN remoto mediante ASDM**
- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Soporte técnico y descargas de Cisco**

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).