ASA/PIX: Exemplo de Configuração de Habilitação do Tunelamento Dividido for VPN Clients no ASA

Índice

Introdução

Este documento fornece instruções passo a passo sobre como permitir que Clientes VPN acessem a Internet enquanto são enviados pelo túnel para dentro de um Mecanismo de Segurança Cisco Adaptive Security Appliance (ASA) 5500 Series. Esta configuração fornece aos Clientes VPN acesso seguro aos recursos corporativos através do IPsec, ao passo que gera acesso não protegido à Internet.

Nota: O Tunelamento completo é considerado a configuração a mais segura porque não permite o acesso de dispositivo simultâneo ao Internet e à LAN corporativa. Um acordo entre o Tunelamento e o Split Tunneling completos permite a clientes VPN o acesso do LAN local somente. Refira ao PIX/ASA 7.x: Permita o acesso do LAN local para o exemplo de configuração dos clientes VPN para mais informação.

Pré-requisitos

Requisitos

Este documento supõe que uma configuração de trabalho do acesso remoto VPN já existe no ASA. Consulte Exemplo de Configuração do PIX/ASA 7.x como Um Servidor Remoto Usando o ASDM se uma configuração não estiver disponível.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

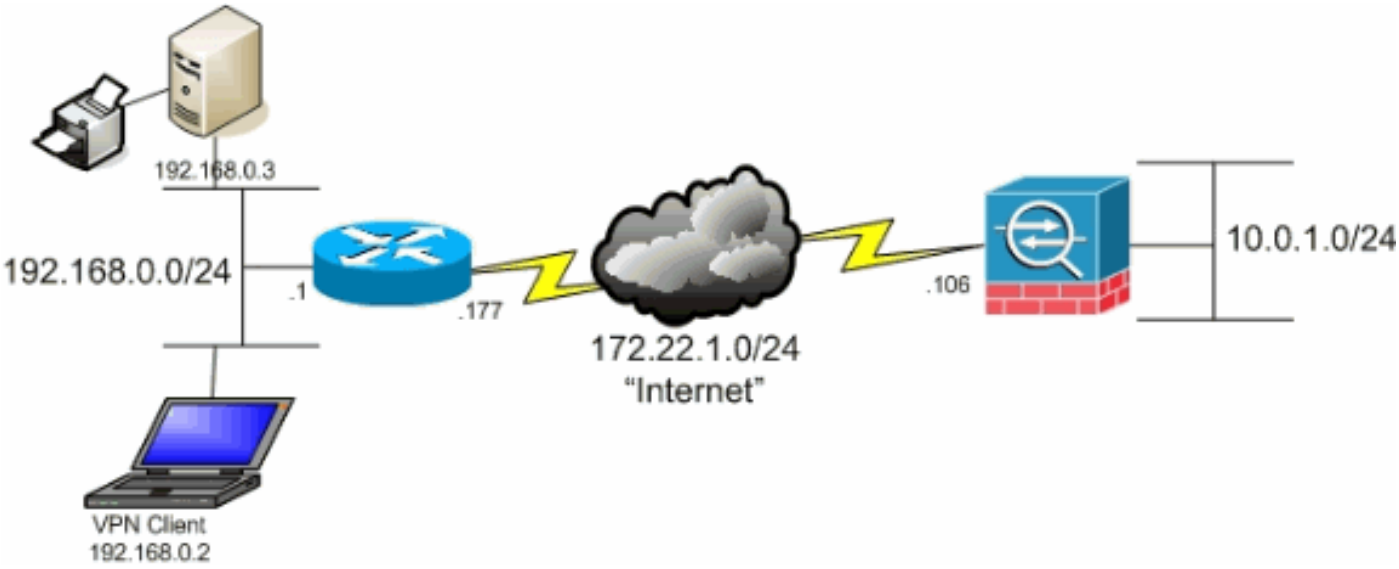
- Cisco ASA 5500 Series Security Appliance Software versão 7.x ou posterior
- Versão 4.0.5 do Cisco Systems VPN client

Nota: Este documento igualmente contém a configuração de CLI PIX 6.x que é compatível para o Cisco VPN Client 3.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede

O cliente VPN é ficado situado em uma rede SOHO típica e conecta através do Internet ao escritório principal.



Produtos Relacionados

Esta configuração pode igualmente ser usada com versão de software 7.x da ferramenta de segurança da série do Cisco PIX 500.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

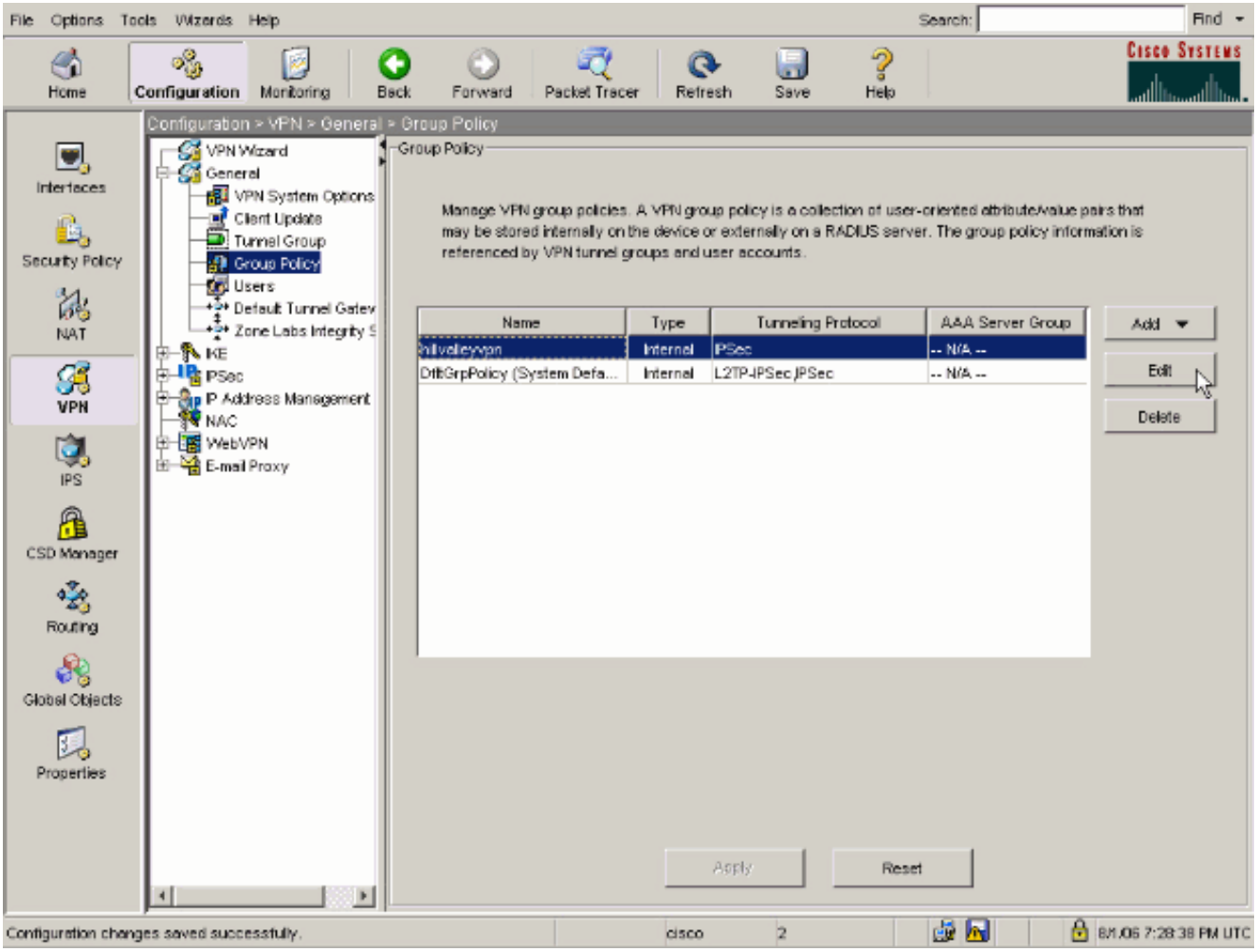
Em um cliente VPN básico à encenação ASA, todo o tráfego do cliente VPN é cifrado e enviado ao ASA não importa o que seu destino é. Baseado em sua configuração e no número de usuários apoiados, tal estabelecido pode transformar-se largura de banda intensiva. O Split Tunneling pode trabalhar para aliviar este problema desde que permite que os usuários enviem somente esse tráfego que é destinado para a rede corporativa através do túnel. Todo tráfego restante tal como mensagens instantâneas, email, ou a consultação ocasional é mandado ao Internet através do LAN local do cliente VPN.

Configuração da Separação de Túneis no ASA

Configuração do ASA 7.x com o Adaptive Security Device Manager (ASDM) 5.x

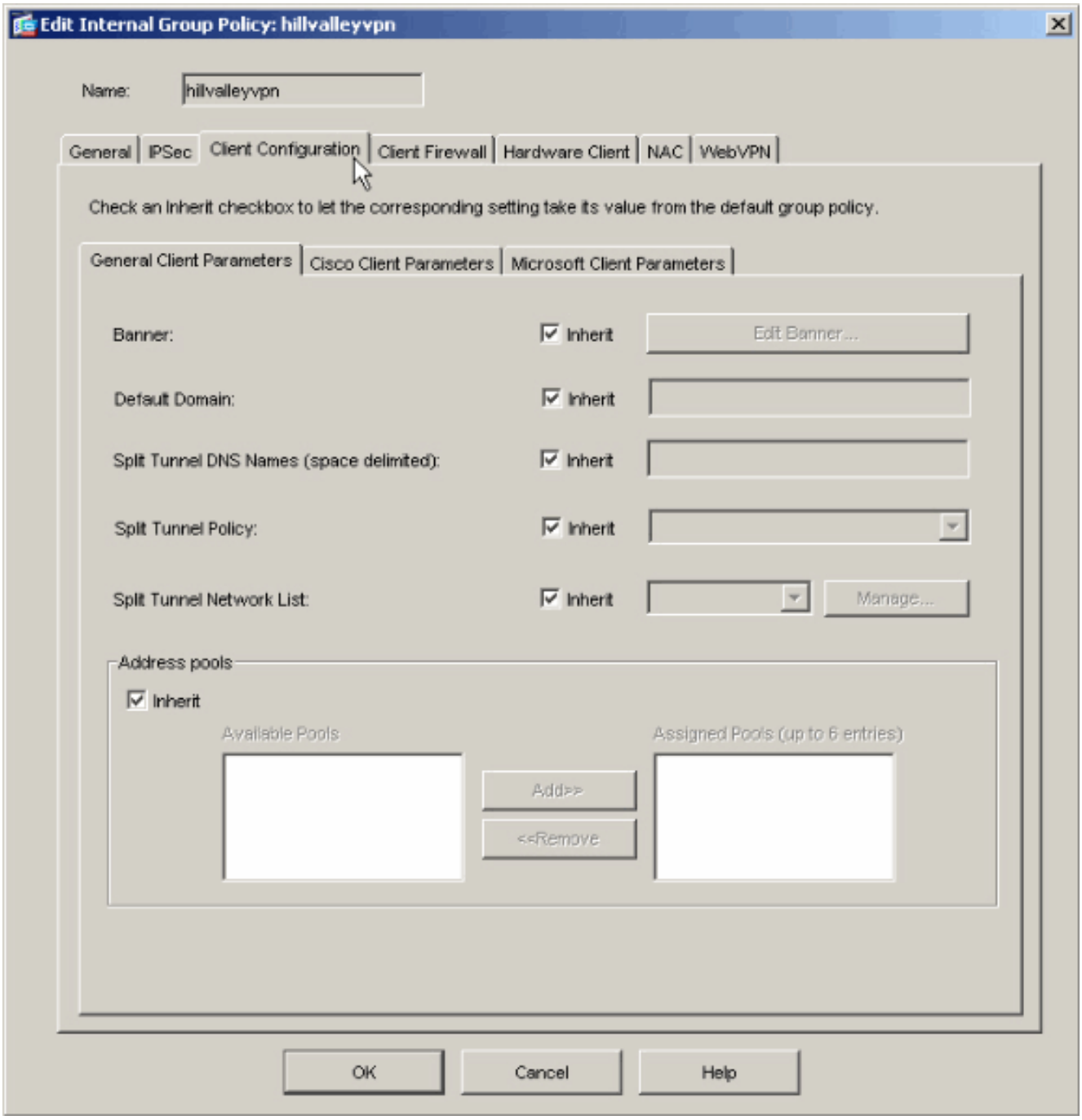
Termine estas etapas a fim configurar seu grupo de túneis para permitir o Split Tunneling para os usuários no grupo.

1. Escolha a **configuração > o VPN > a política do general > do grupo** e selecione a política do grupo que você deseja permitir dentro o acesso do LAN local. Clique então **editam**.

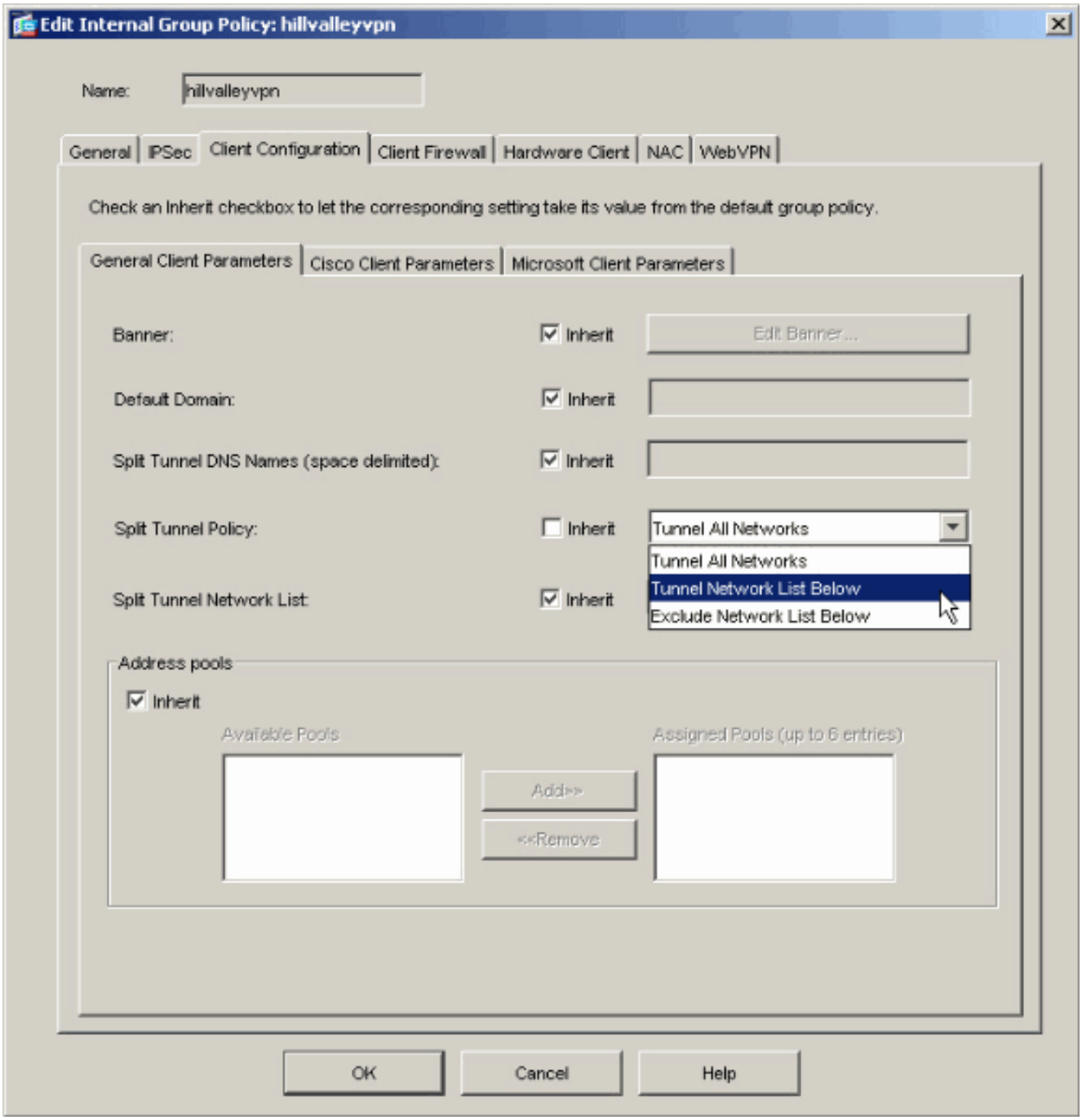


2. Vá à aba da configuração de

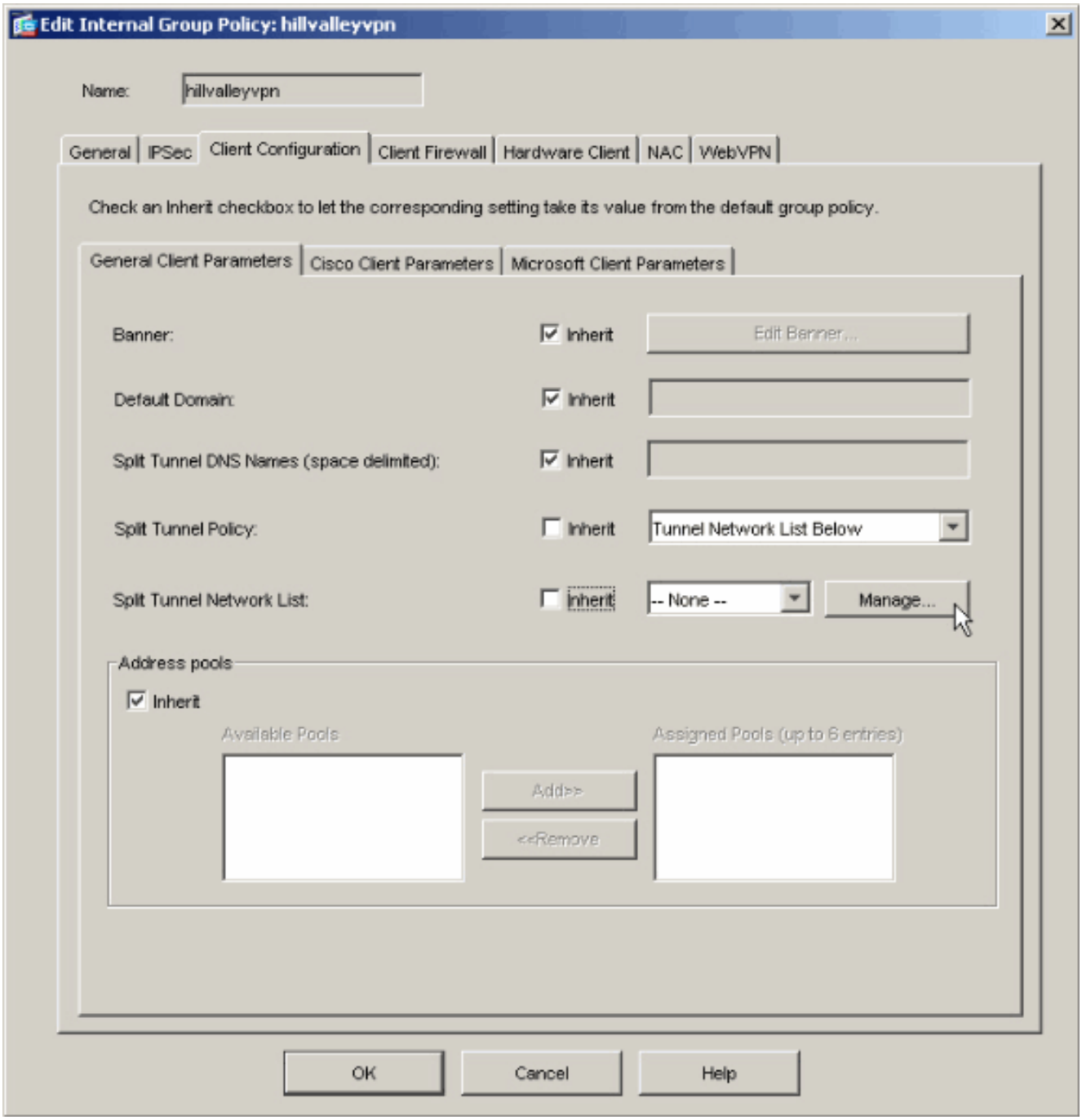
cliente.



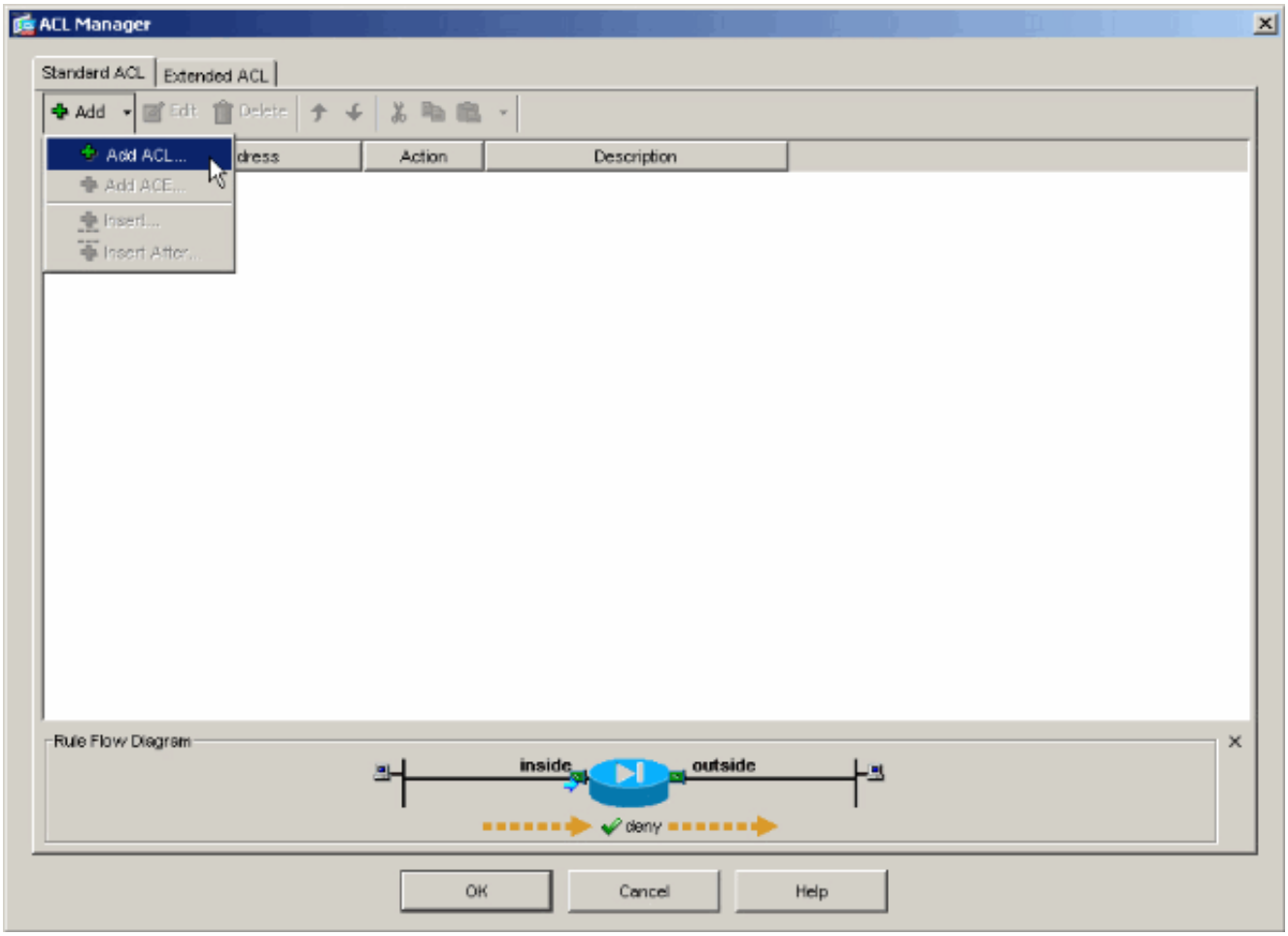
3. Desmarcar a caixa **herdar** para a política do túnel em divisão e escolheu a **lista da rede de túnel**
abaixo.



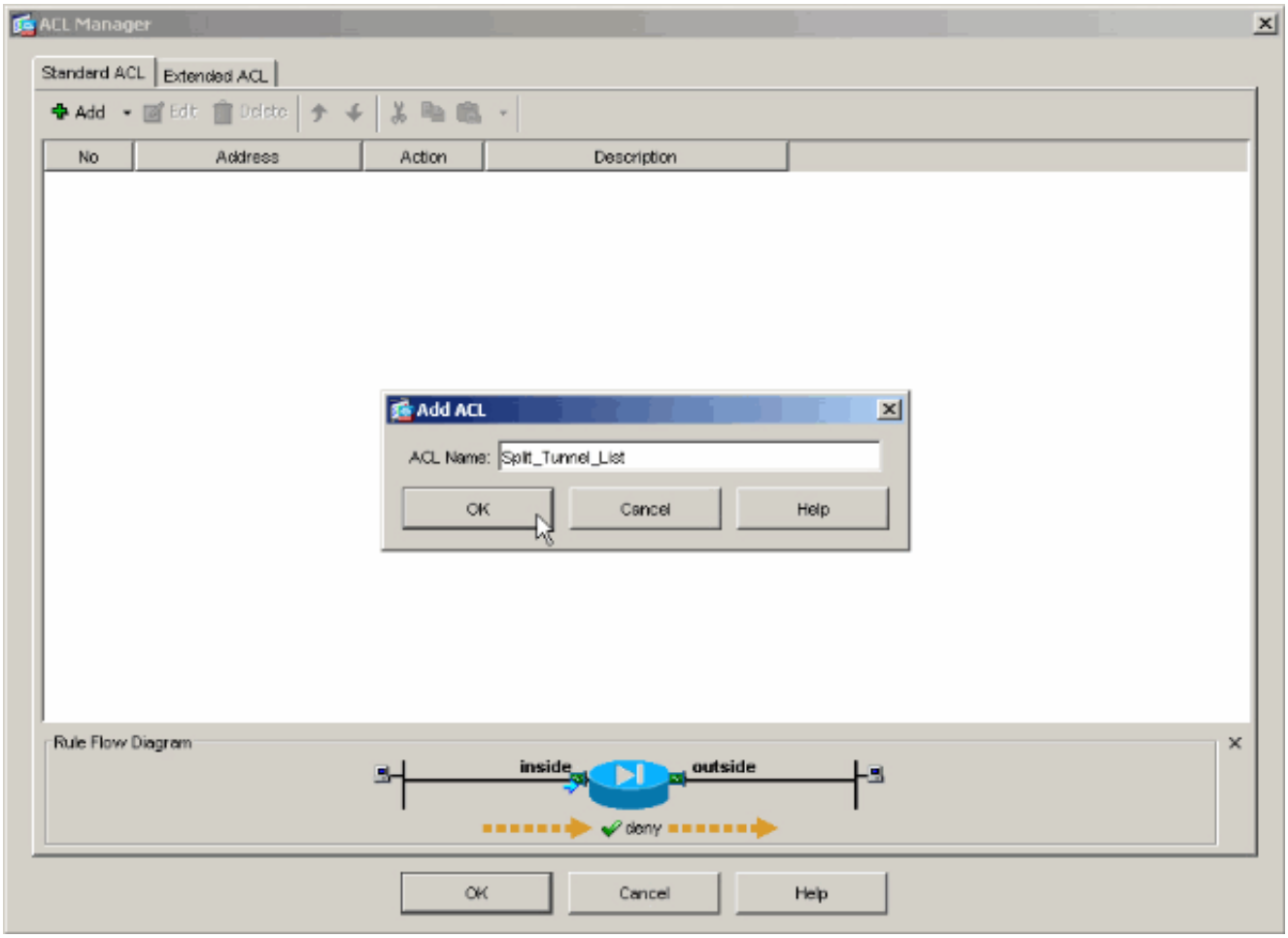
4. Desmarcar a caixa **herdar** para o liste de redes do túnel em divisão e clique-a então **controlam** a fim lançar o gerente
   ACL.



5. No ACL Manager, selecione **Add > Add ACL...** para criar uma nova lista de acesso.

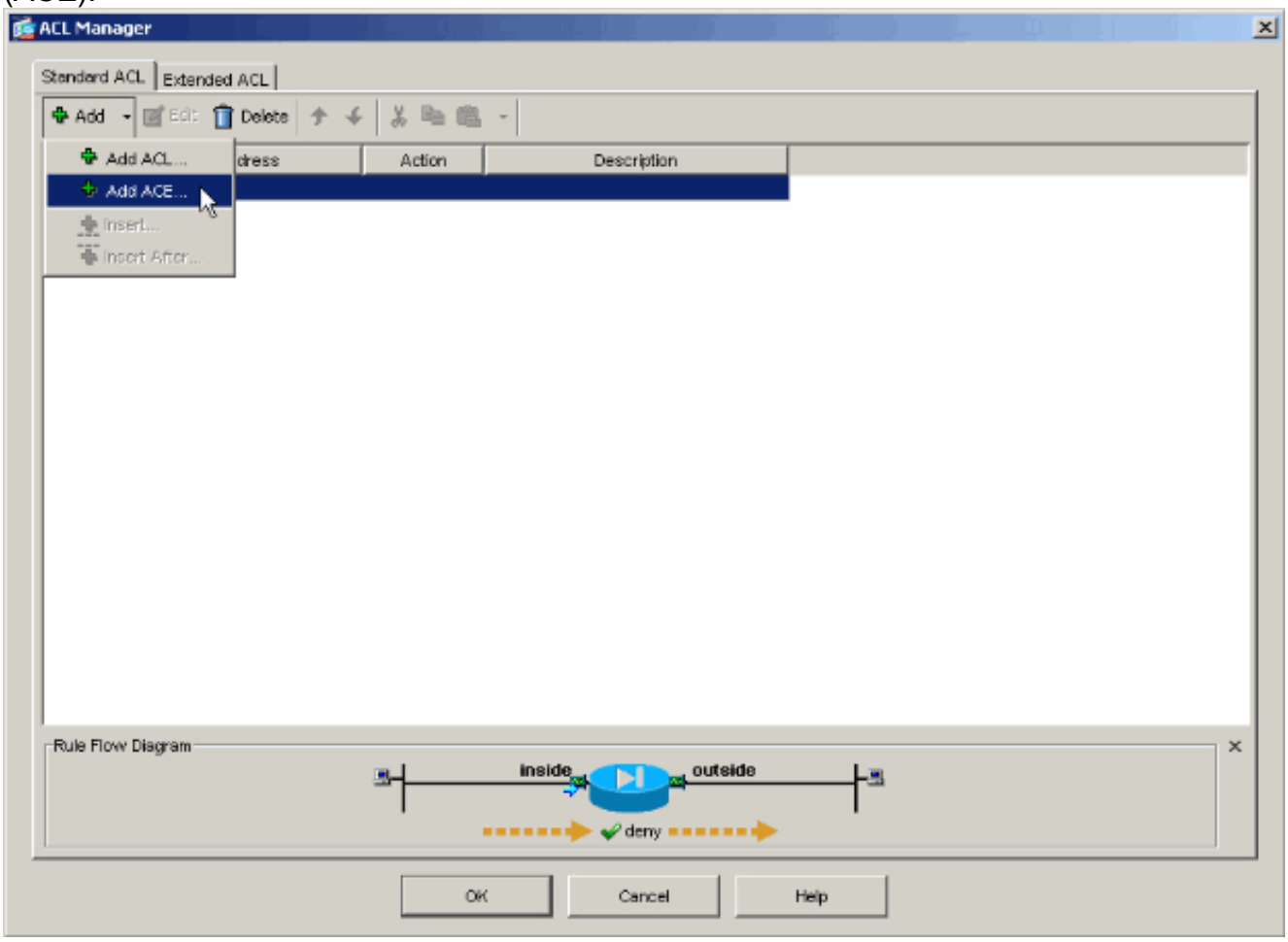


6. Forneça um nome para a ACL e clique em **OK**.

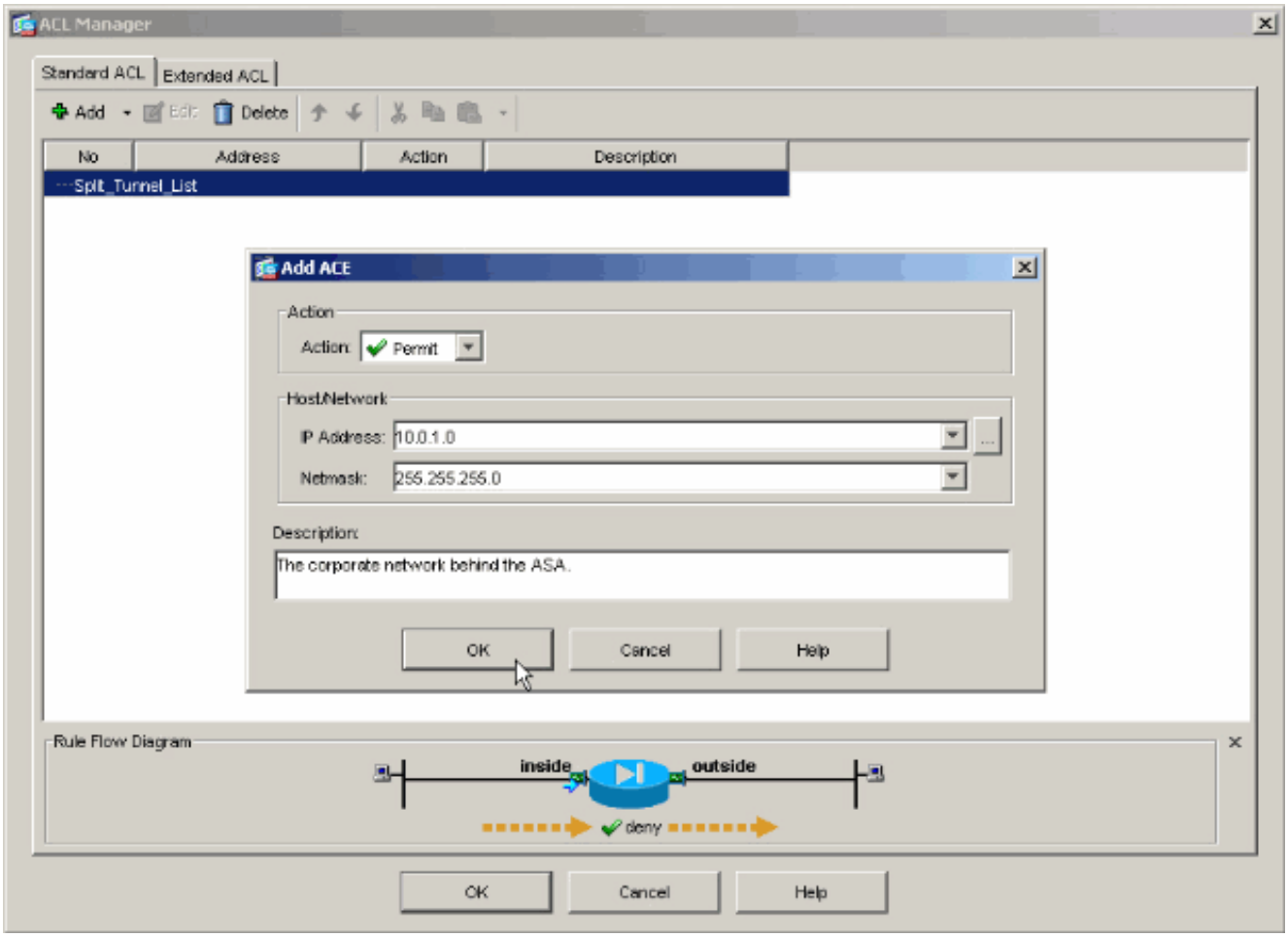


7. Uma vez que o ACL é criado, escolha **adicionam o > Add ACE...** a fim adicionar uma

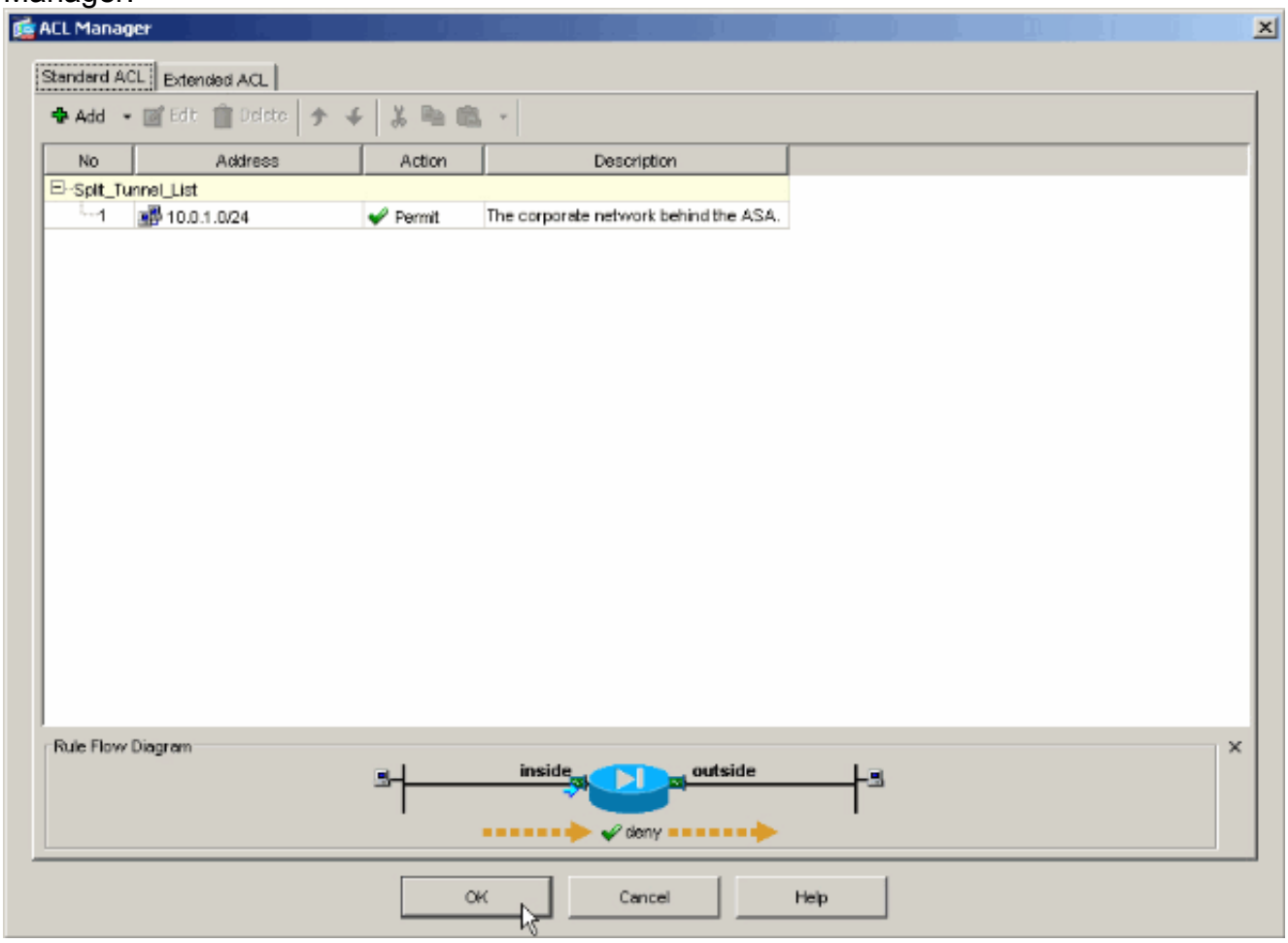
entrada de controle de acesso
(ACE).



8. Defina a ACE que corresponde à LAN por trás do ASA. Neste caso, a rede é 10.0.1.0/24.Escolha a **licença**.Escolha o endereço IP **10.0.1.0**Escolha a máscara de rede **255.255.255.0**.*(Opcional)* forneça uma descrição.Clique em **OK**.

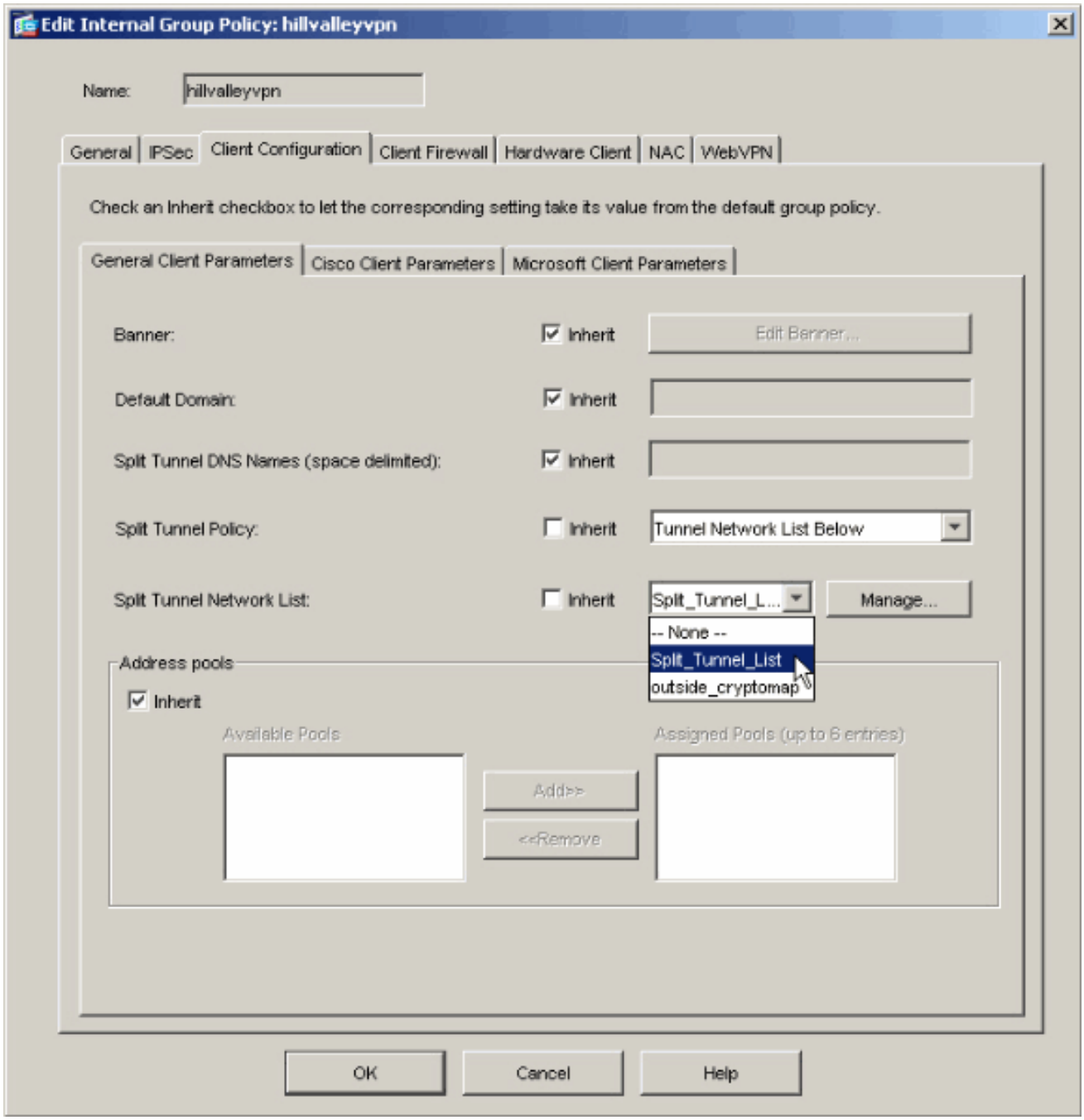


9. Clique em **OK** para sair do ACL Manager.

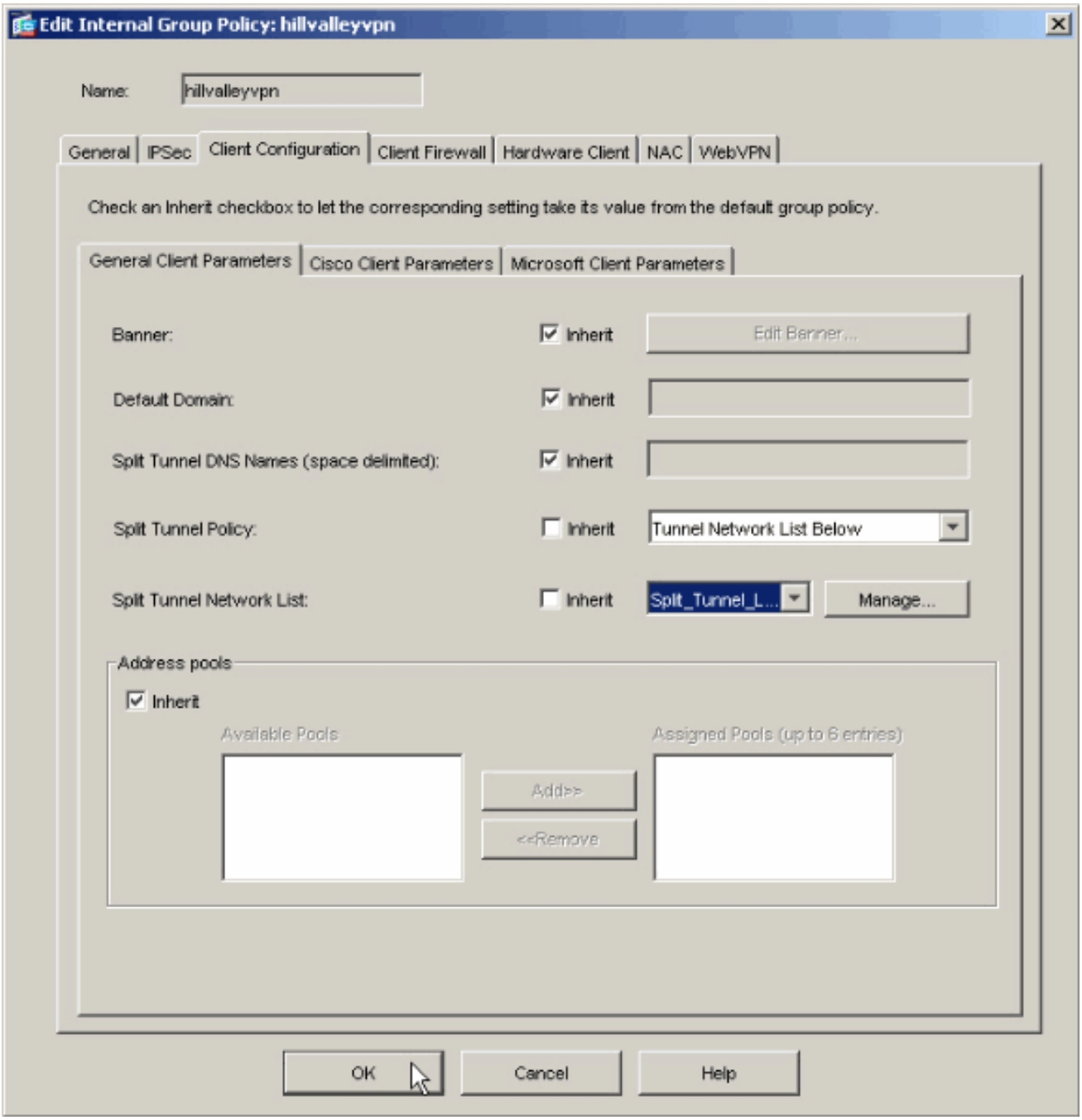


10. Seja certo que o ACL que você apenas criou está selecionado para o liste de redes do

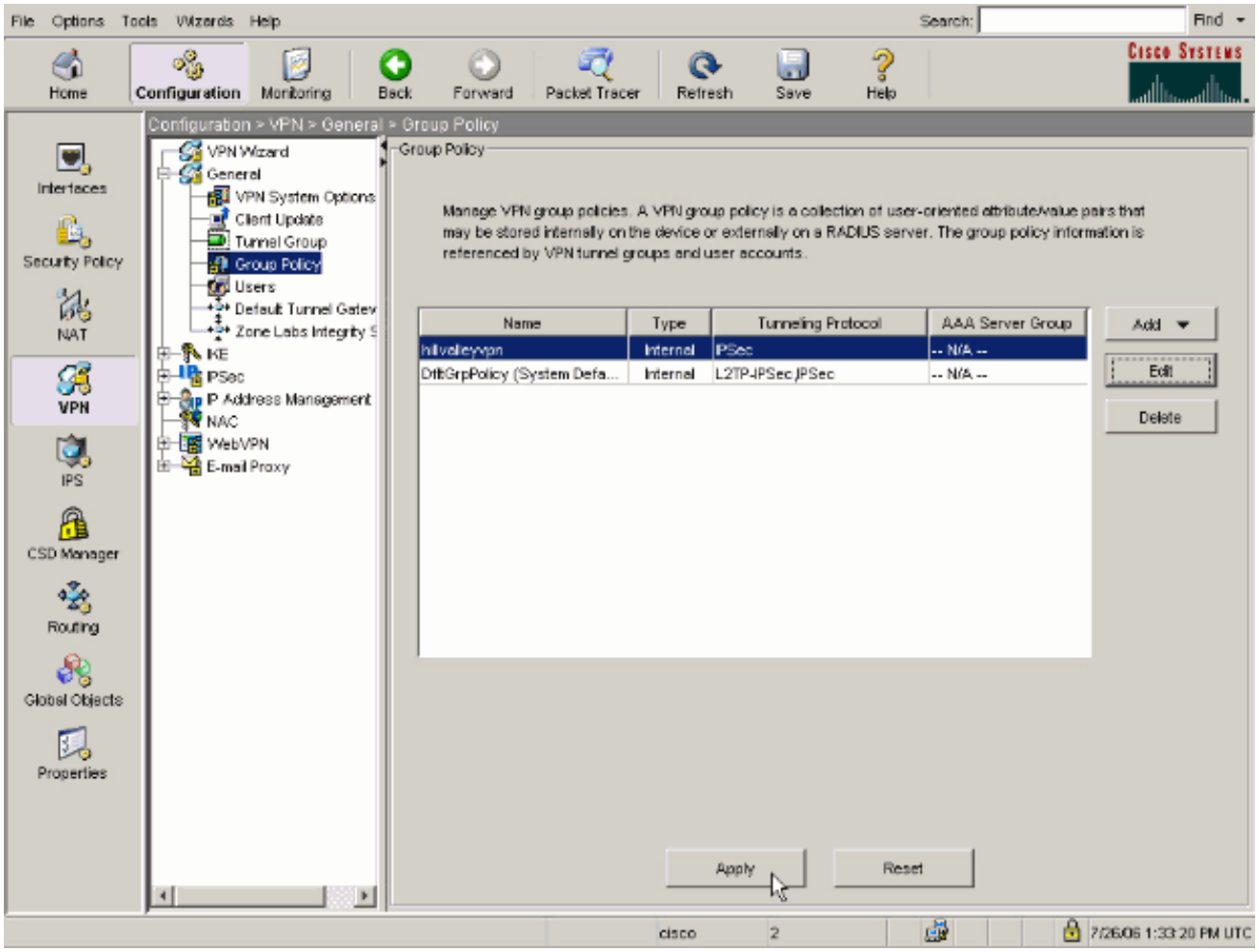
túnel em
divisão.



11. Clique em **OK** para retornar à configuração da Política de Grupo.



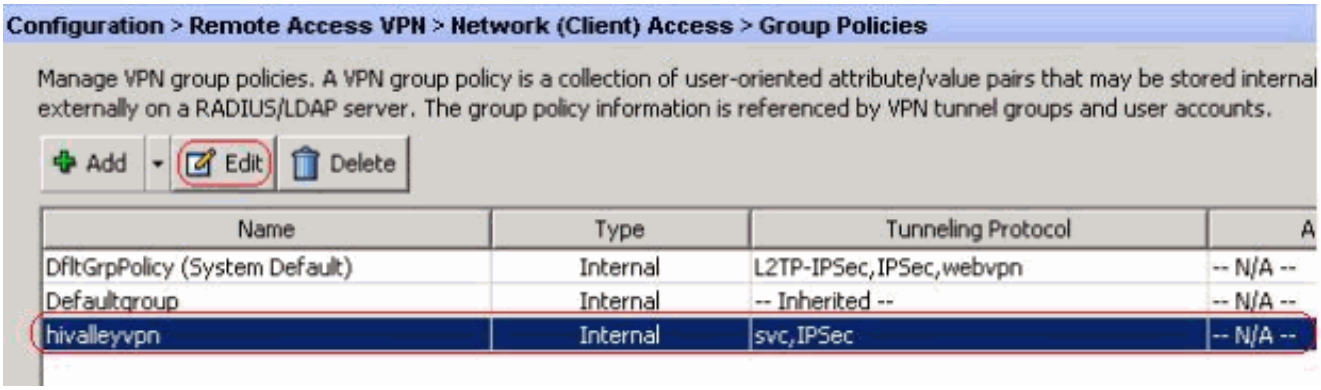
12. O clique **aplica-se** e **envia-se** então (se for necessário) a fim enviar os comandos ao ASA.



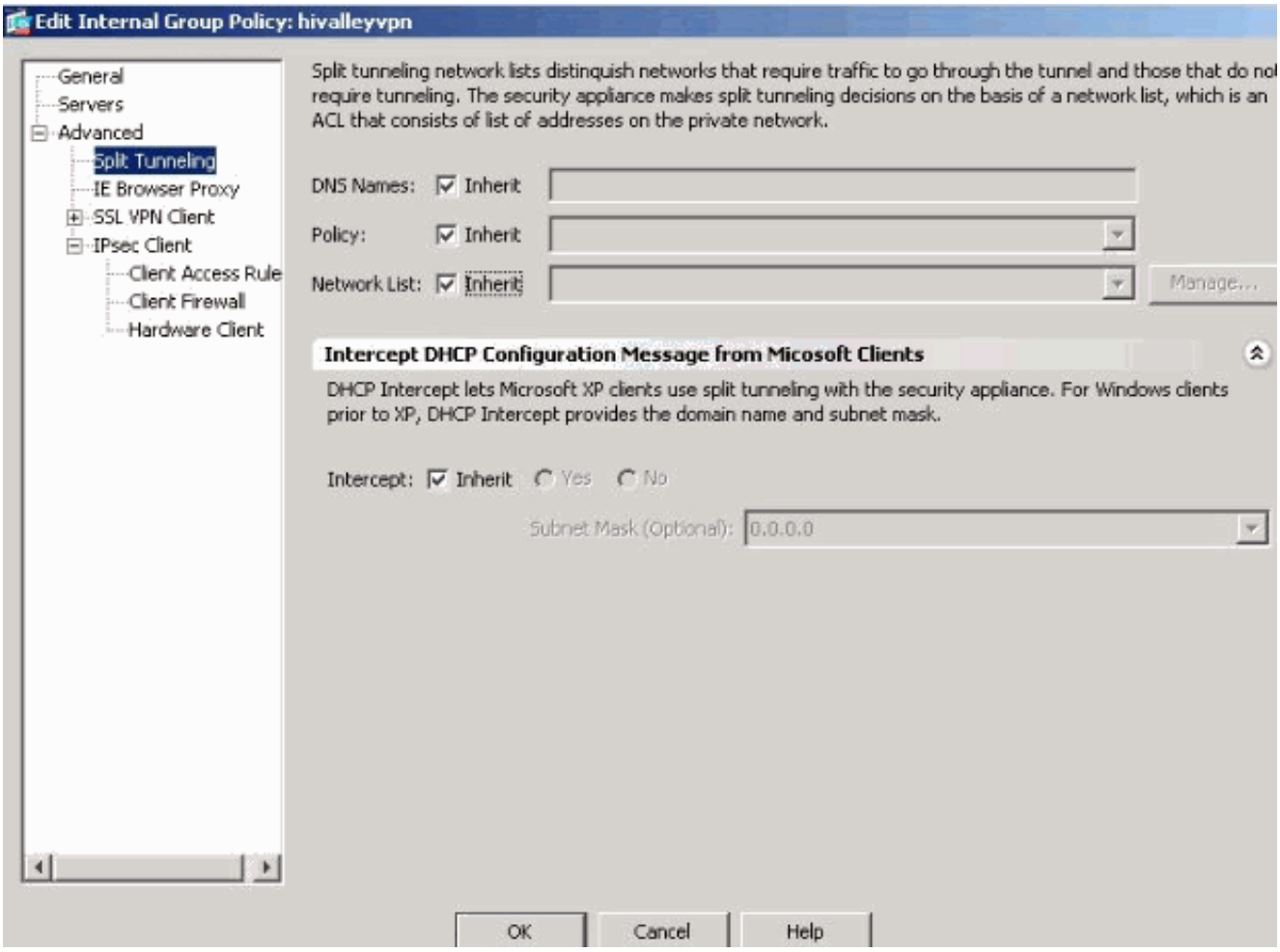
Configurar o ASA 8.x com Security Device Manager adaptável (ASDM) 6.x

Termine estas etapas a fim configurar seu grupo de túneis para permitir o Split Tunneling para os usuários no grupo.

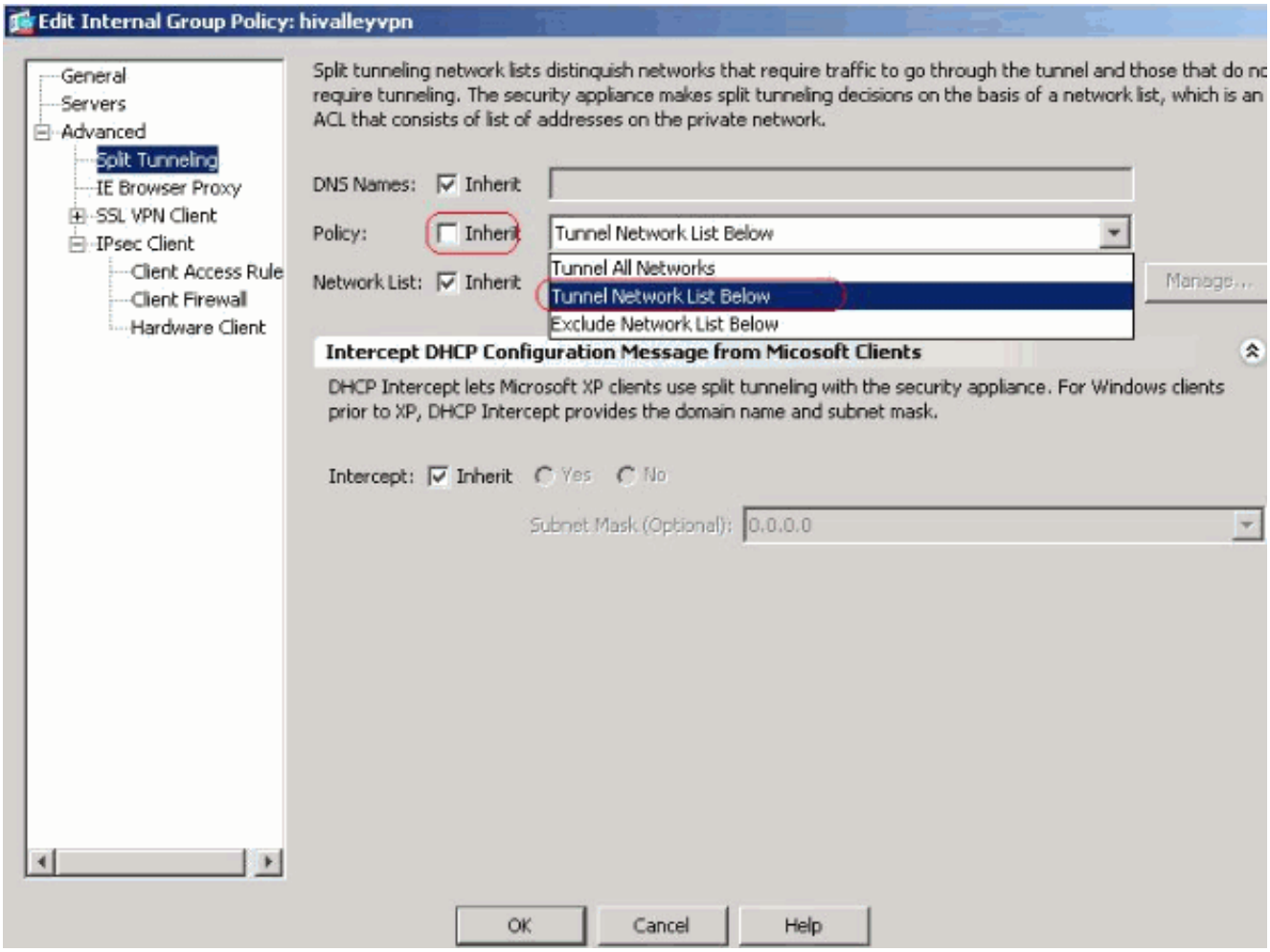
1. Selecione **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** e escolha a Política de Grupo na qual deseja habilitar o acesso à LAN local. Clique então **editam**.



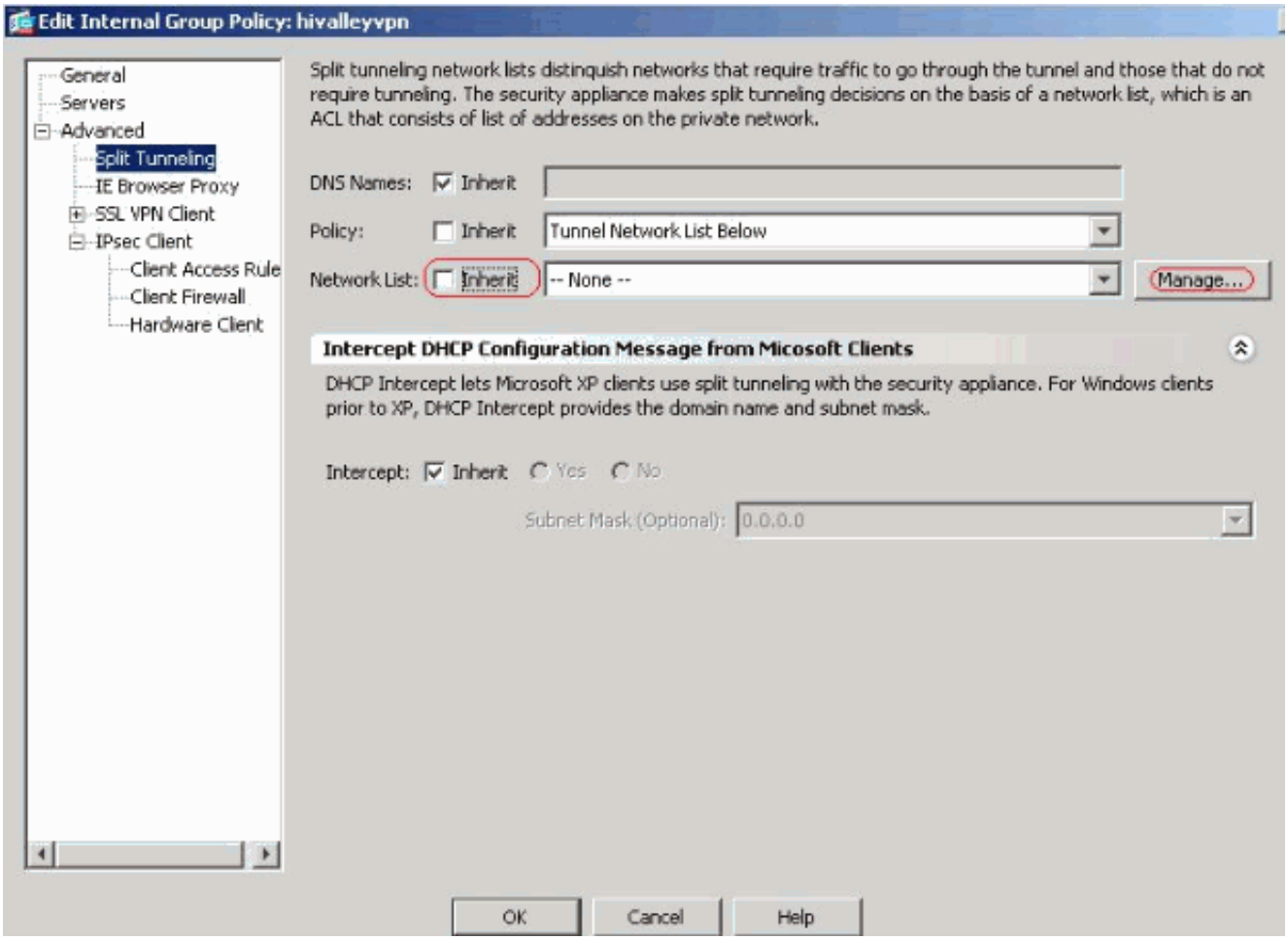
2. Clique em **Split Tunneling**.



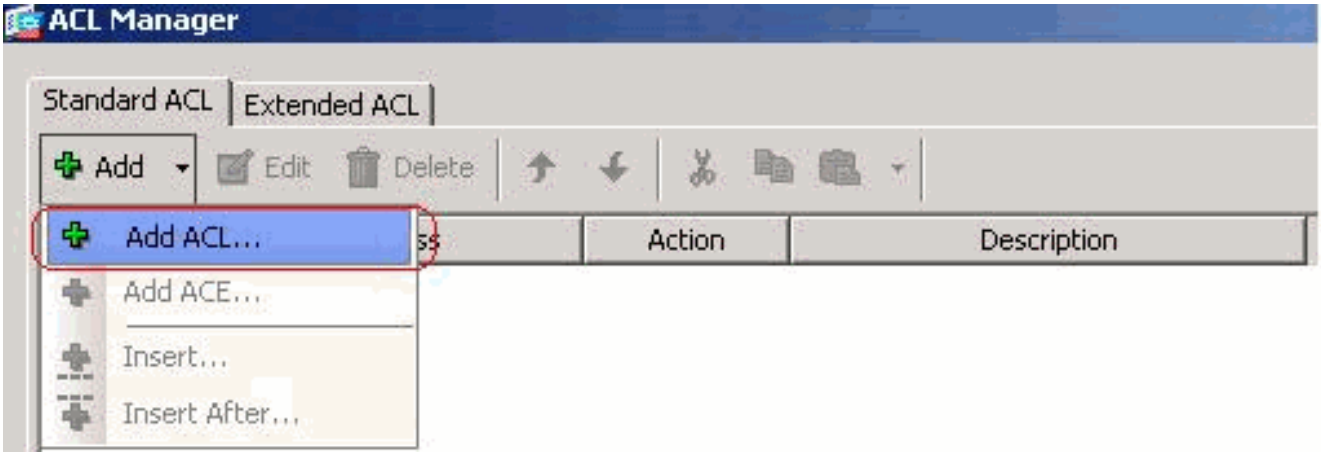
3. Desmarque a caixa **Inherit** da Split Tunnel Policy e selecione **Tunnel Network List Below**.



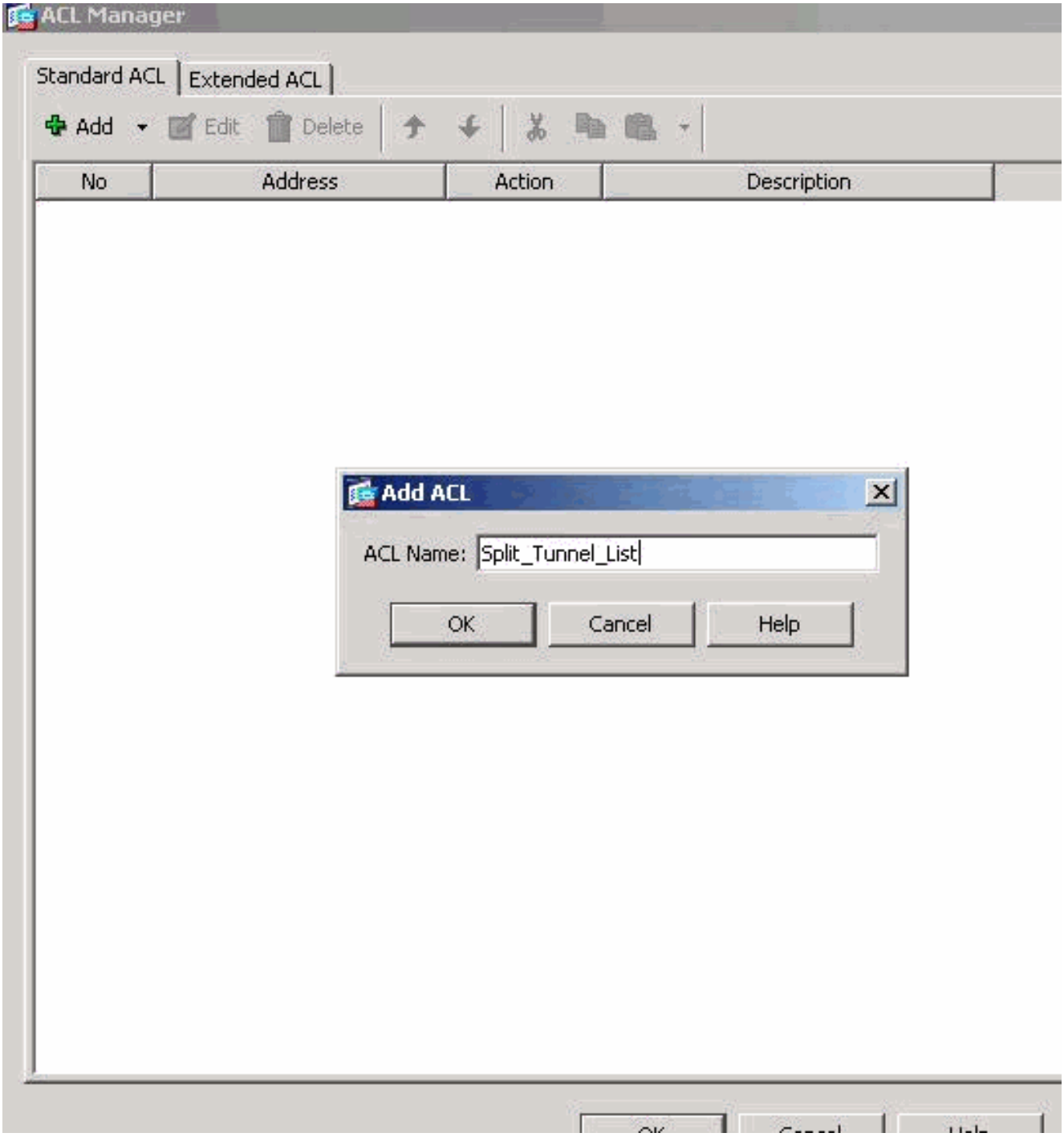
4. Desmarque a caixa **Inherit** da Split Tunnel Network List e clique em **Manage** para iniciar o ACL
   Manager.



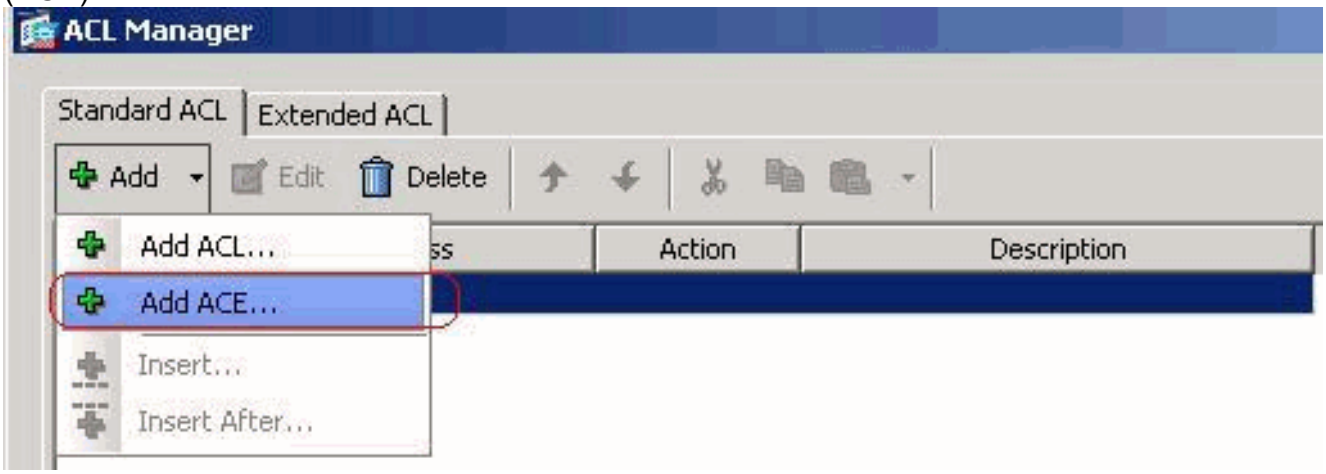
5. No ACL Manager, selecione **Add > Add ACL...** para criar uma nova lista de acesso.



6. Forneça um nome para a ACL e clique em **OK**.

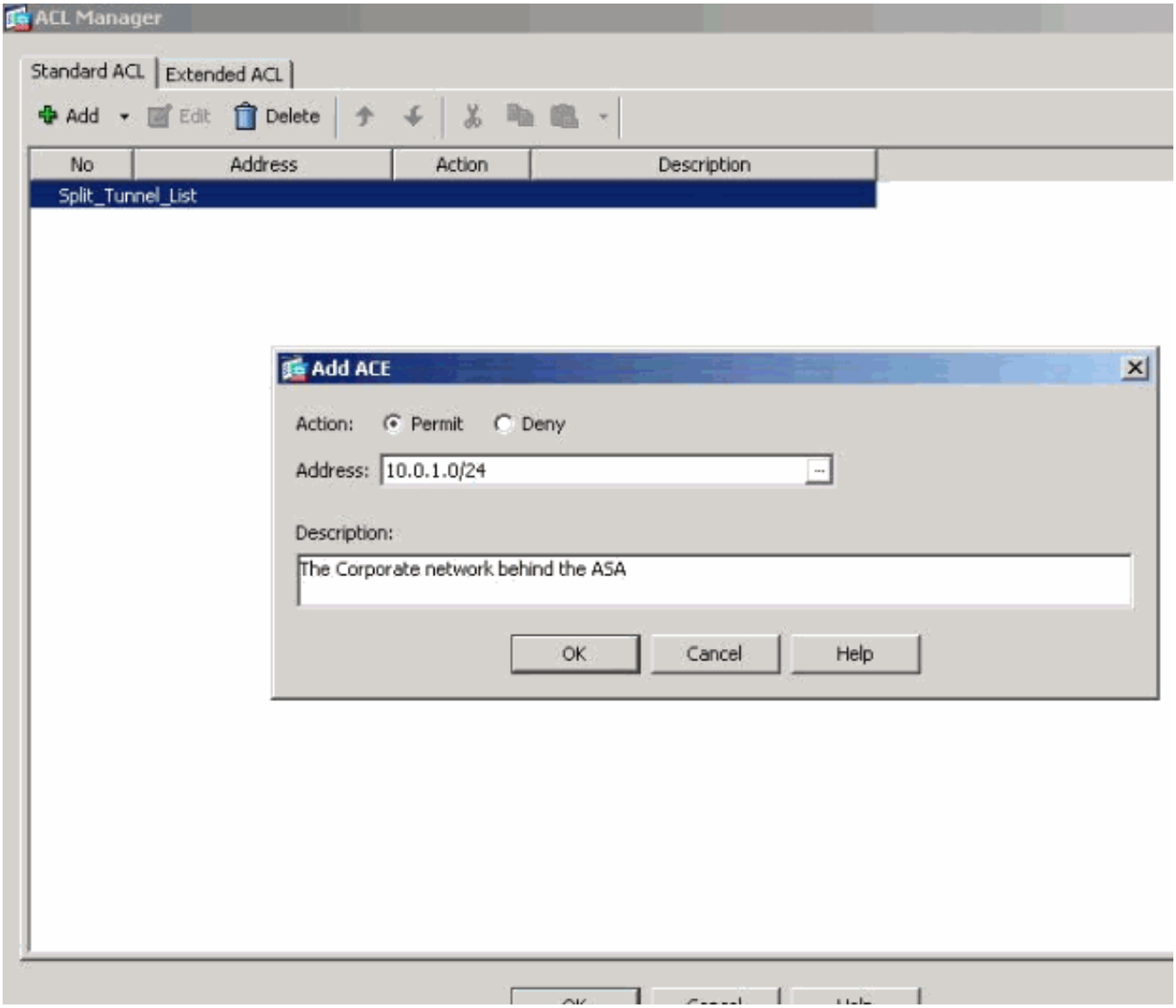


7. Uma vez que o ACL é criado, escolha **adicionam o > Add ACE...** a fim adicionar uma entrada de controle de acesso
(ACE).

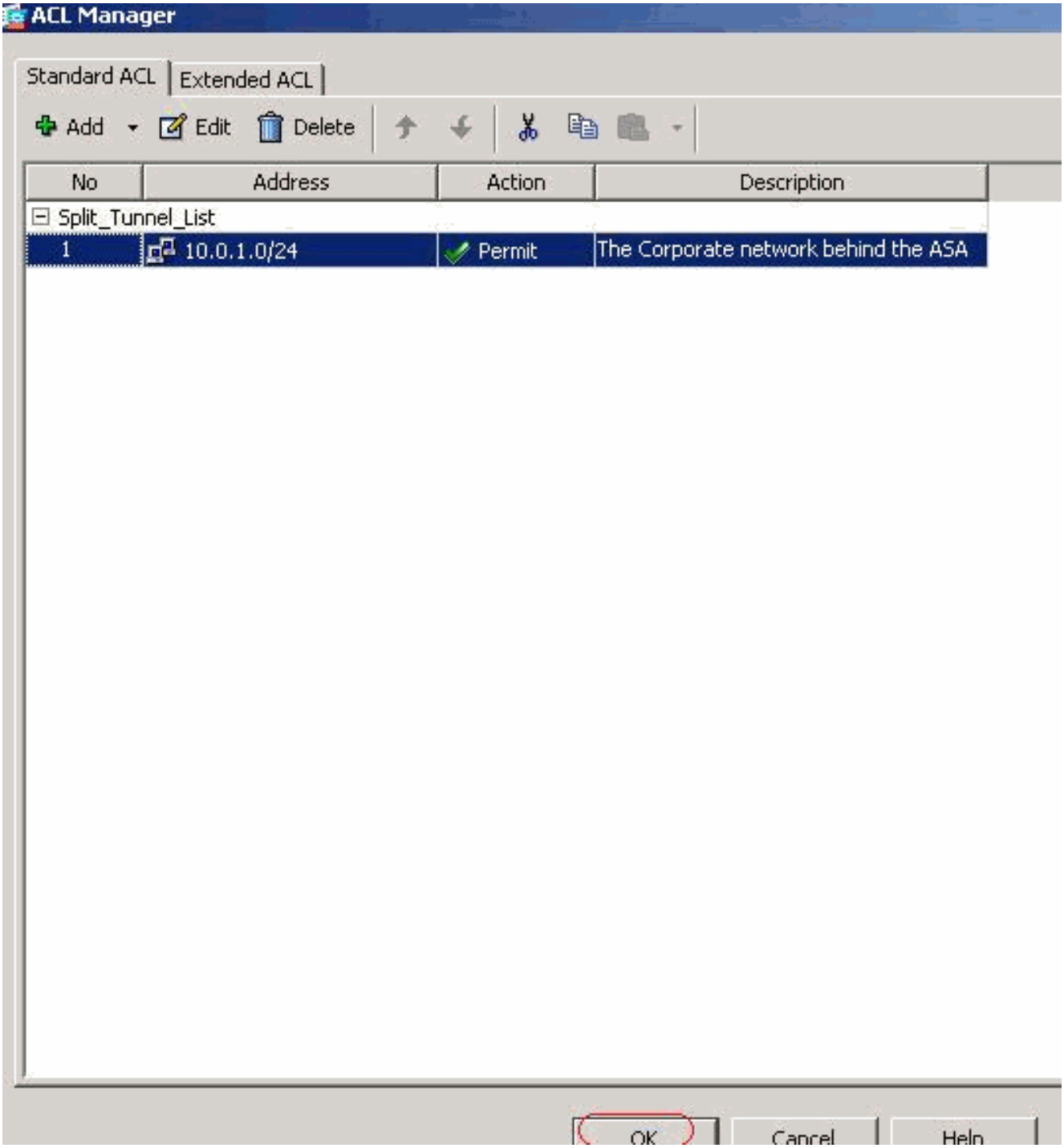


8. Defina a ACE que corresponde à LAN por trás do ASA. Neste caso, a rede é

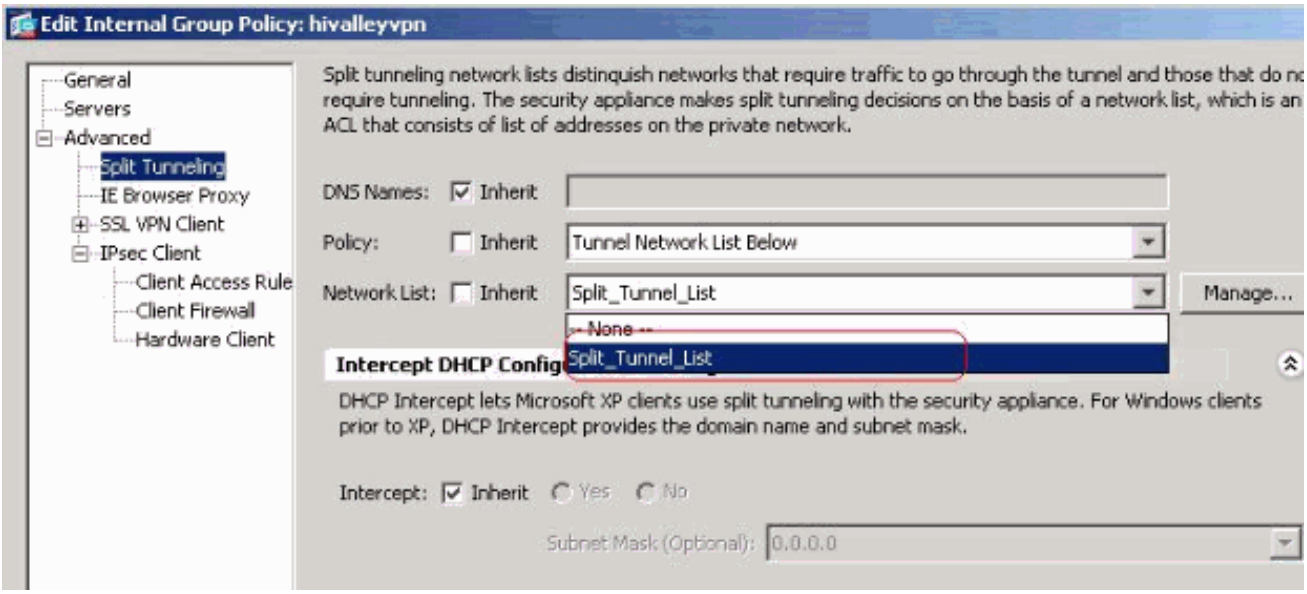
10.0.1.0/24.Clique no botão de opção **Permit**.Selecione o endereço de rede com a máscara **10.0.1.0/24** .(Opcional) forneça uma descrição.Clique em **OK**.



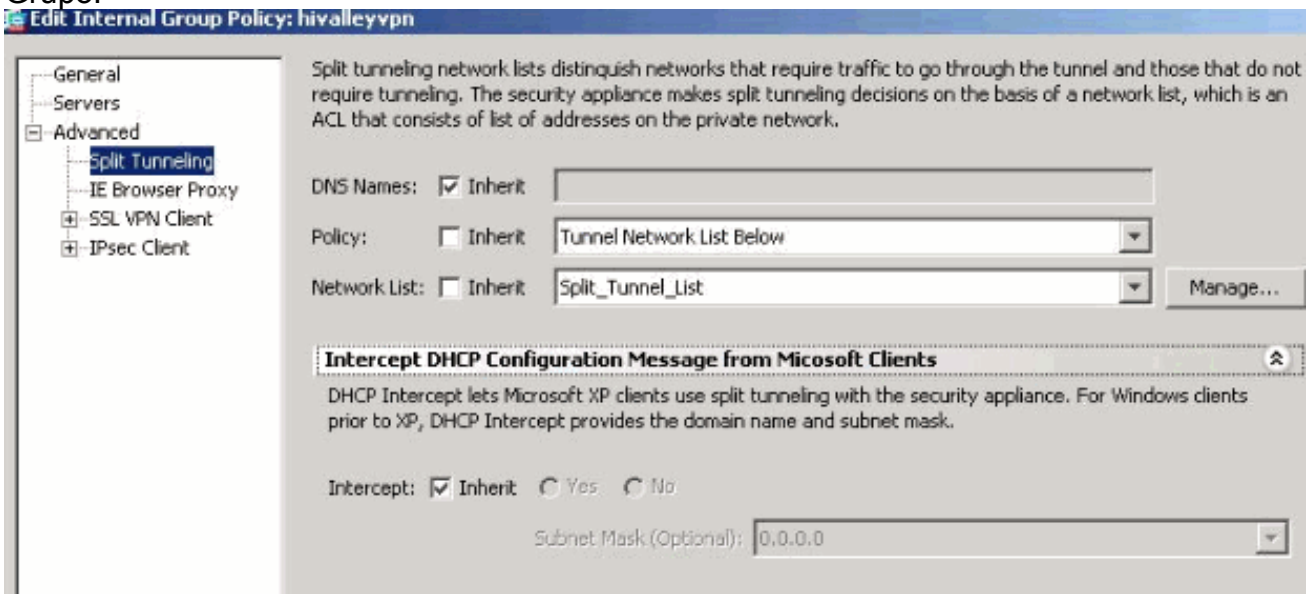
9. Clique em **OK** para sair do ACL Manager.



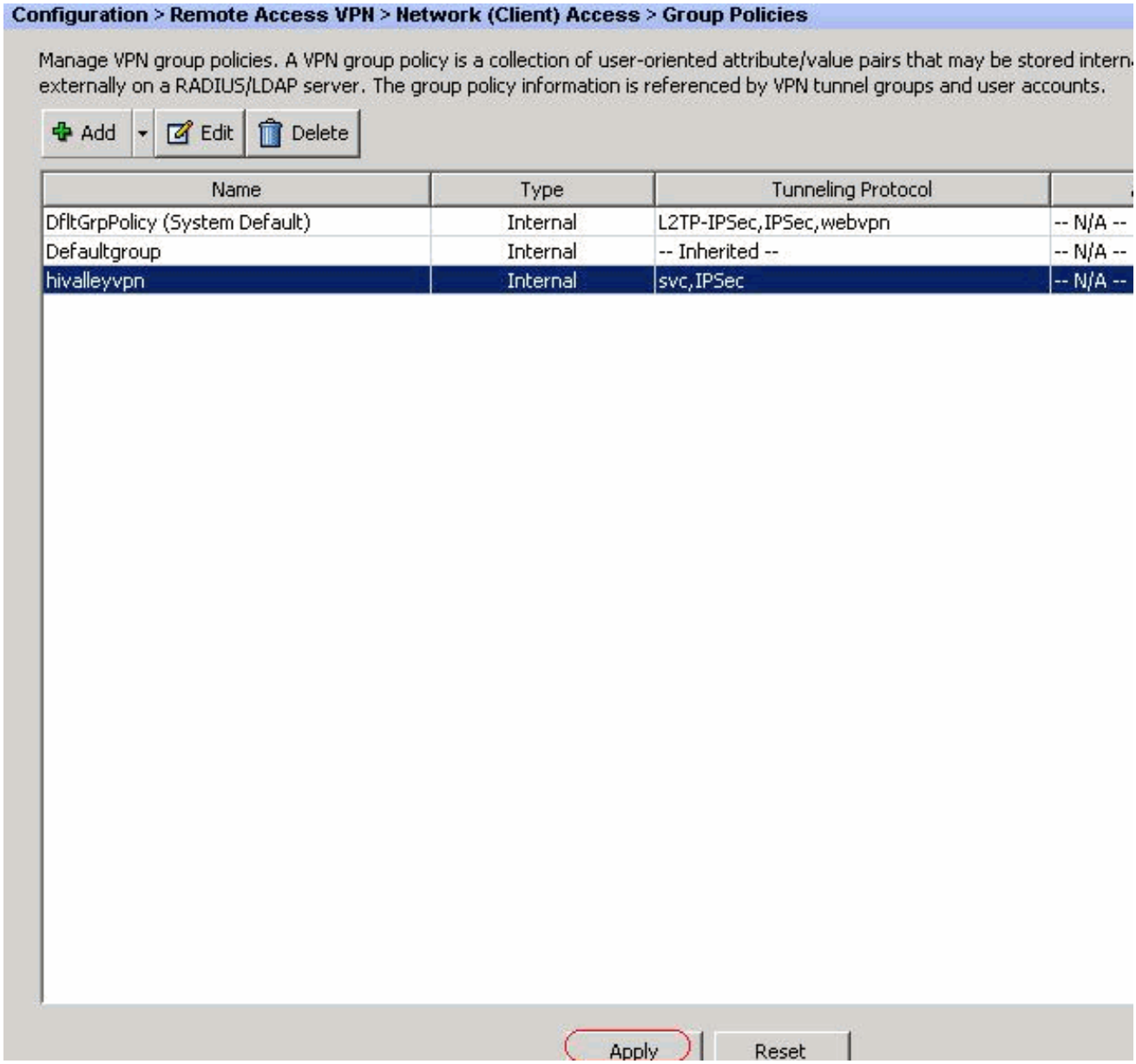
10. Seja certo que o ACL que você apenas criou está selecionado para o liste de redes do túnel em
divisão.



11. Clique em **OK** para retornar à configuração da Política de Grupo.



12. O clique **aplica-se** e **envia-se** então (se for necessário) a fim enviar os comandos ao ASA.



Configurar o ASA 7.x e mais tarde através do CLI

Um pouco do que usa o ASDM, você pode terminar estas etapas no ASA CLI a fim permitir o Split Tunneling no ASA:

Nota: A configuração do Split Tunneling CLI é a mesma para ASA 7.x e 8.x.

1. Incorpore o modo de configuração.`ciscoasa>`**`enable`** `Password: ******** ciscoasa#`**`configure terminal`** `ciscoasa(config)#`
2. Crie a lista de acessos que define a rede atrás do 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. Entre no modo da configuração das normas do grupo para a política que você deseja alterar.`ciscoasa(config)#`**`group-policy hillvalleyvpn attributes`** `ciscoasa(config-group-policy)#`
4. Especifique a política do túnel em divisão. Neste caso, a política é **tunnelspecified**.`ciscoasa(config-group-policy)#`**`split-tunnel-policy tunnelspecified`**
5. Especifique a lista de acessos do túnel em divisão. Neste caso, a lista é **Split_Tunnel_List**.`ciscoasa(config-group-policy)#`**`split-tunnel-network-list value Split_Tunnel_List`**

6. Emita este comando:`ciscoasa(config)#`**`tunnel-group hillvalleyvpn general-attributes`**
7. Associe a política do grupo ao grupo do túnel.`ciscoasa(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
8. Retire os dois modos de configuração.`ciscoasa(config-group-policy)#`**`exit`**
`ciscoasa(config)#`**`exit`** `ciscoasa#`
9. Salve a configuração na RAM não volátil (NVRAM) e pressione **Enter** quando avisado para especificar o nome de arquivo de origem.`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#`

Configurar PIX 6.x com o CLI

Conclua estes passos:

1. Crie a lista de acessos que define a rede atrás do PIX.
`PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0`
2. Crie um *VPN3000 do* grupo do vpn e especifique-lhe o túnel em divisão ACL como mostrado:`PIX(config)#`**`vpngroup vpn3000 split-tunnel Split_Tunnel_List`** **Nota:** Refira o firewall PIX segura Cisco 6.x e o Cisco VPN Client 3.5 para Windows com Microsoft Windows 2000 e a autenticação RADIUS de 2003 IAS para obter mais informações sobre da configuração do acesso remoto VPN para PIX 6.x.

Verificar

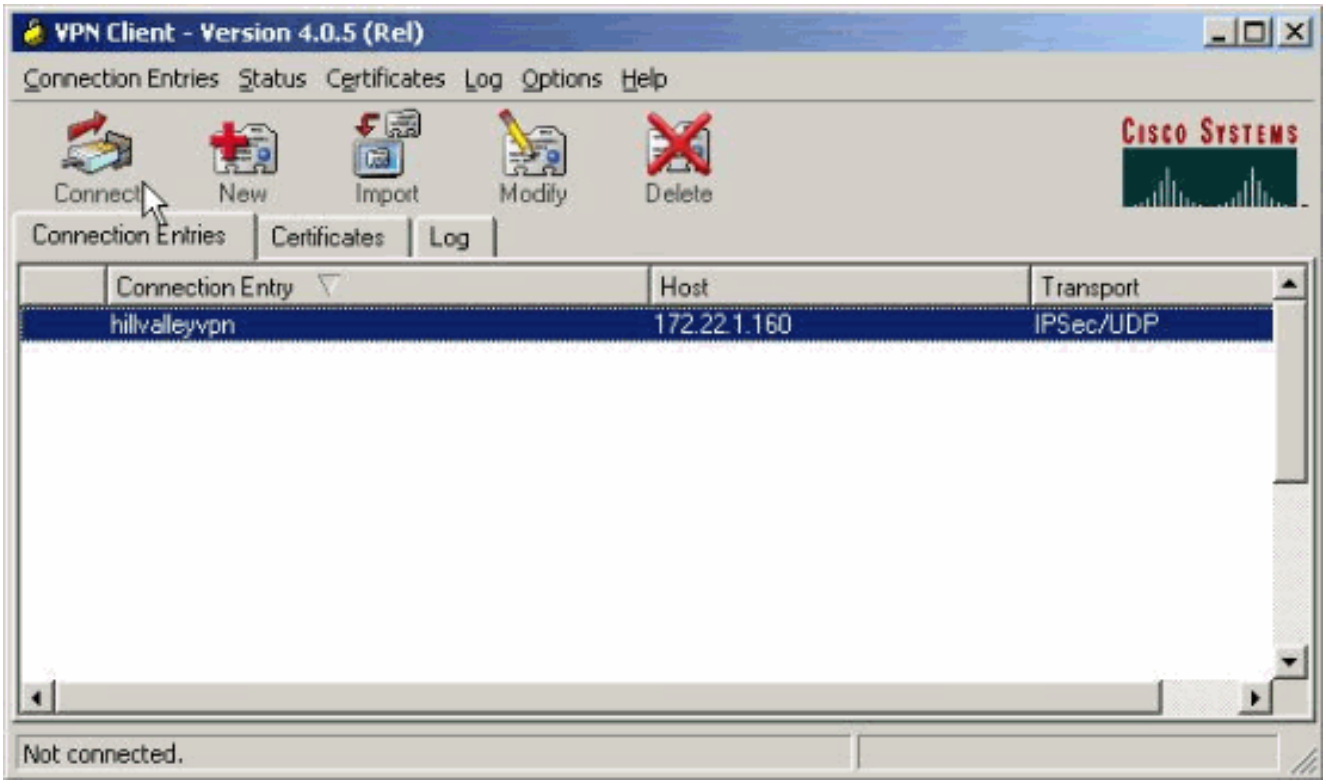
Siga as etapas nestas seções a fim verificar sua configuração.

- Conexão com o Cliente VPN
- Veja o log de cliente VPN
- Teste o acesso do LAN local com sibilo

Conexão com o Cliente VPN

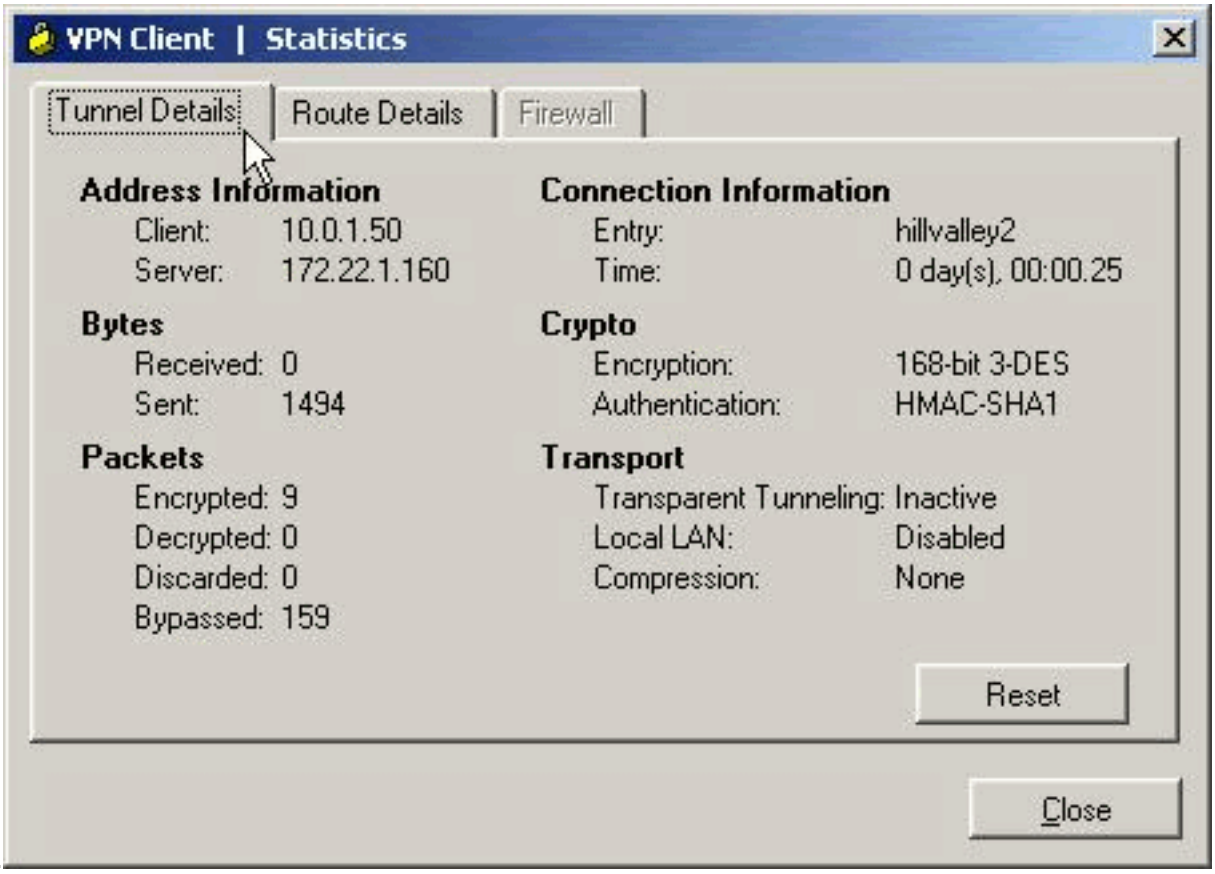
Conecte seu cliente VPN ao concentrador VPN a fim verificar sua configuração.

1. Selecione sua entrada de conexão da lista e clique em
Connect.



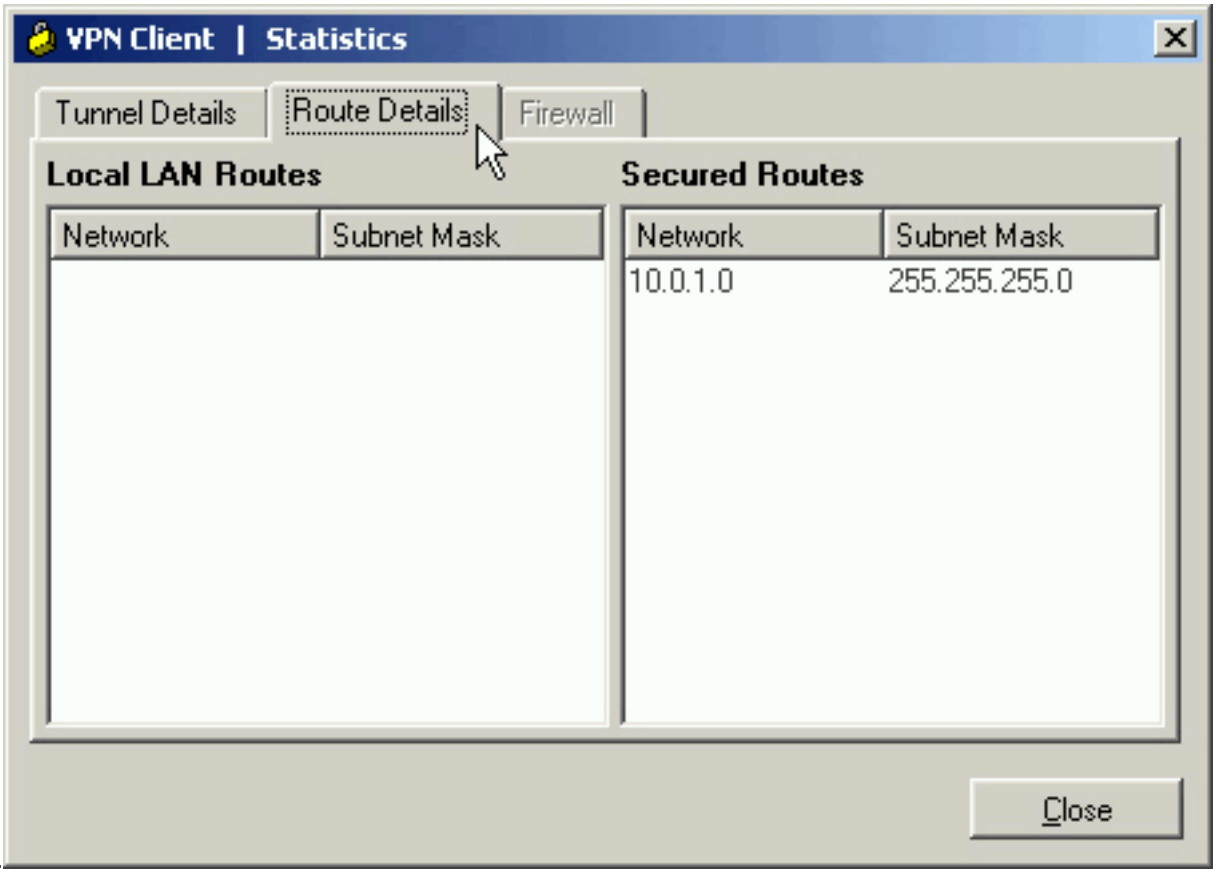
2. Incorpore suas credenciais.

3. Escolha o **estado > as estatísticas…** a fim indicar o indicador dos detalhes do túnel onde você pode inspecionar os detalhes do túnel e ver o fluxo de



tráfego.

4. Vá à aba dos detalhes da rota a fim ver as rotas que o cliente VPN está fixando ao ASA.Neste exemplo, o cliente VPN está fixando o acesso a 10.0.1.0/24 quando todo tráfego restante não for cifrado e não é enviado através do

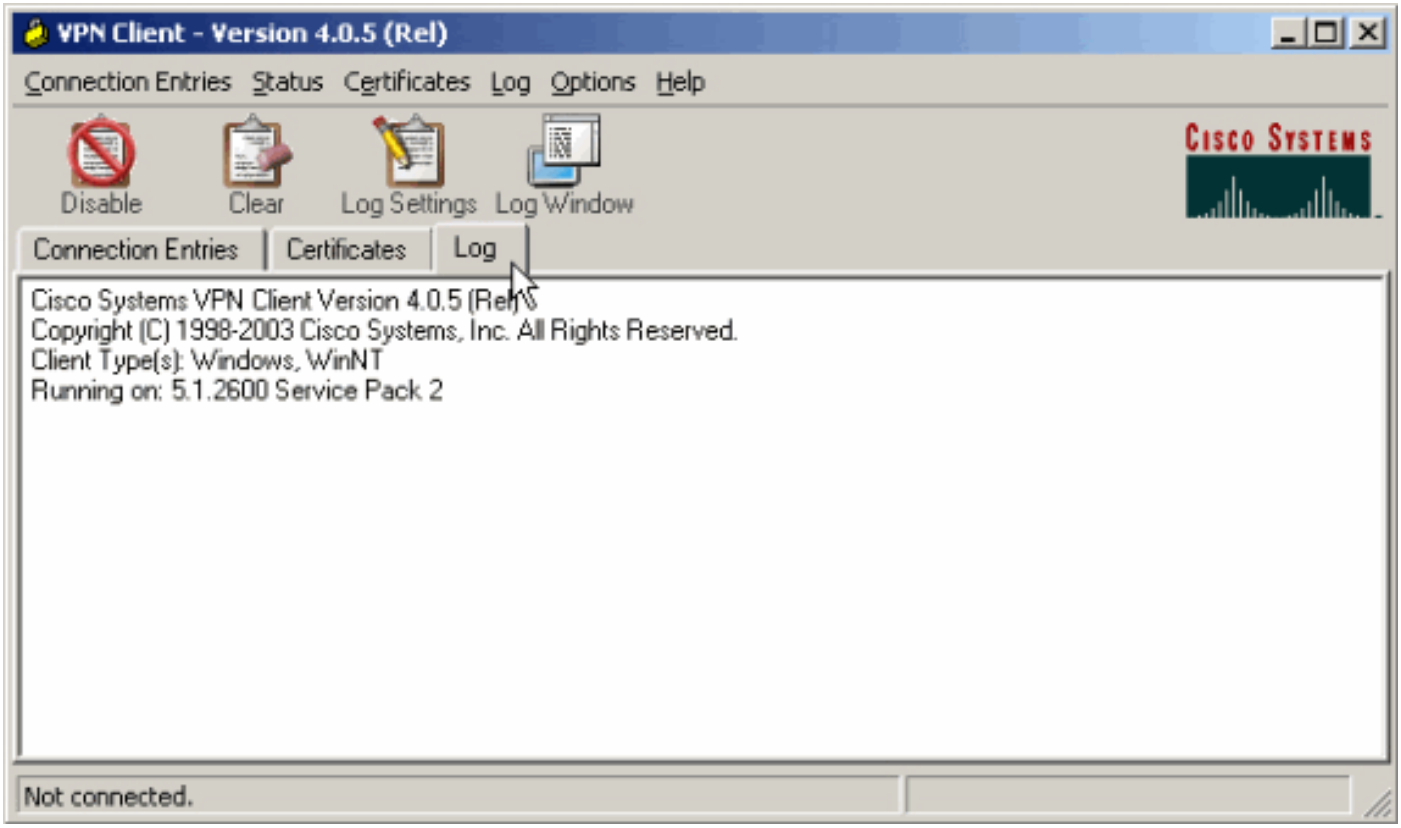


túnel.

Veja o log de cliente VPN

Quando você examina o log de cliente VPN, você pode determinar mesmo se o parâmetro que

especifica o Split Tunneling está ajustado. A fim ver o log, vá à aba do log no cliente VPN. Clique então sobre **configurações de registro** a fim ajustar o que é registrado. Neste exemplo, o IKE é definido como **3 - High**, enquanto que todos os demais elementos são definidos como **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/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.
```

Teste o acesso do LAN local com sibilo

Uma maneira adicional de testar se o cliente VPN está configurado para a separação de túneis

enquanto permanece encapsulado no ASA é usar o comando **ping** na linha de comando do Windows. O LAN local do cliente VPN é 192.168.0.0/24 e um outro host esta presente na rede com um endereço IP de Um ou Mais Servidores Cisco ICM NT 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

Limitação com o número das entradas em um túnel em divisão ACL

Há uma limitação com o número de entradas em um ACL usado para o túnel em divisão. Recomenda-se não usar mais de 50-60 entradas ACE para a funcionalidade satisfatória. Você é recomendado executar a característica do sub-rede para cobrir uma escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT.

Informações Relacionadas

- PIX/ASA 7.x como um servidor de VPN remoto usando o exemplo da configuração ASDM
- Cisco ASA 5500 Series Adaptive Security Appliances
- Suporte Técnico e Documentação - Cisco Systems