Configurar o tunelamento dividido para clientes VPN no ASA

Contents

Introdução

Este documento descreve o processo para permitir que clientes VPN acessem a Internet enquanto fazem o tunelamento em um Cisco ASA 5500 Series Security Appliance.

Pré-requisitos

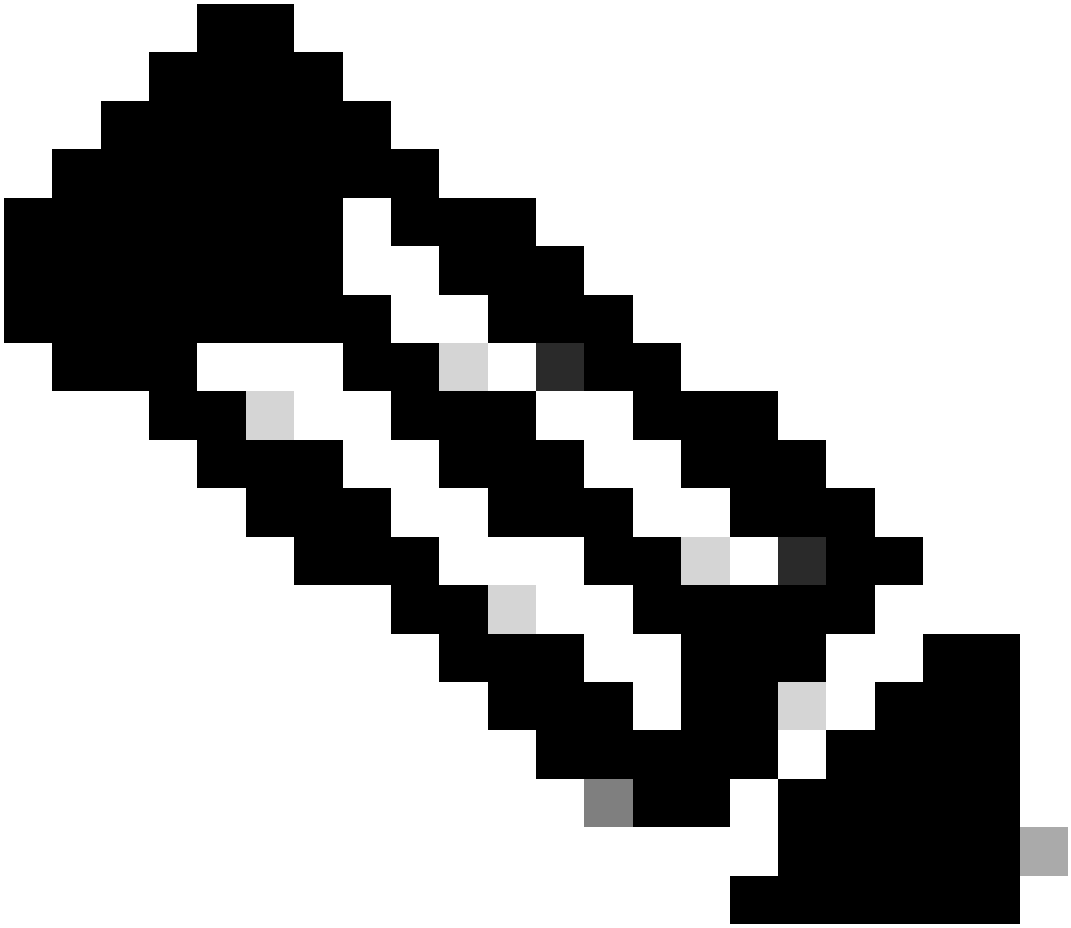
Requisitos

Este documento supõe que já existe uma configuração de VPN de acesso remoto em funcionamento 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
- Cisco Systems VPN Client versão 4.0.5
- Adaptive Security Device Manager (ASDM)



Observação: este documento também contém a configuração CLI do PIX 6.x que é compatível com 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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Diagrama de Rede

O VPN Client está localizado em uma rede SOHO típica e se conecta pela Internet ao escritório principal.

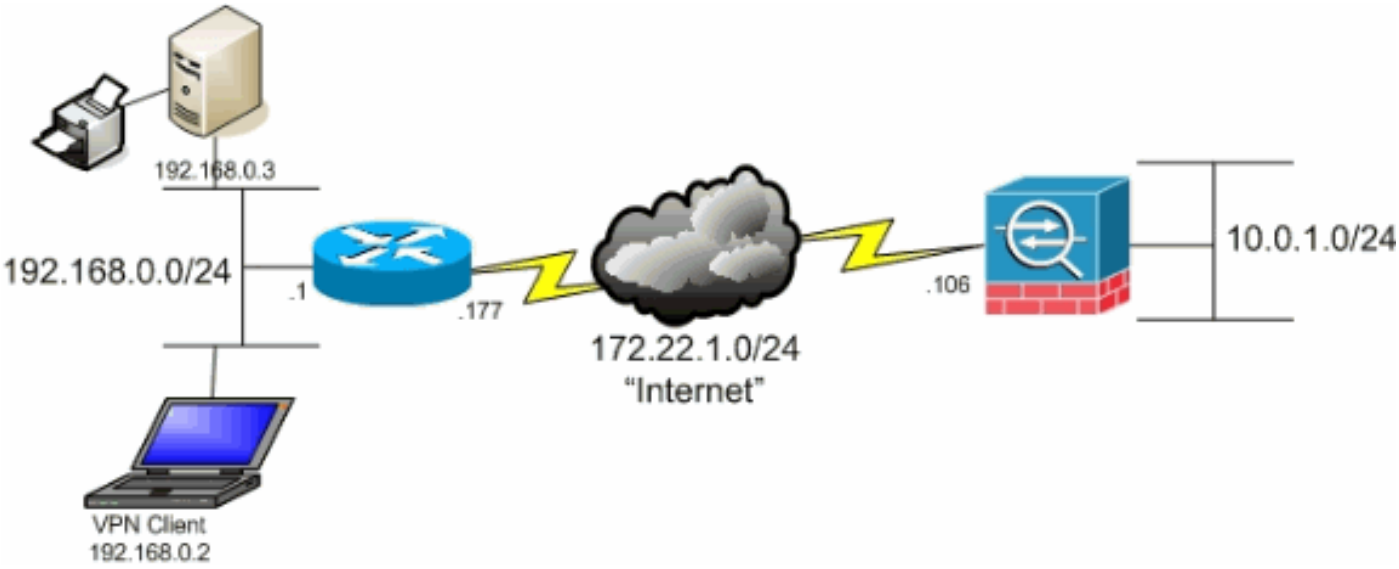


Diagrama de Rede

Produtos Relacionados

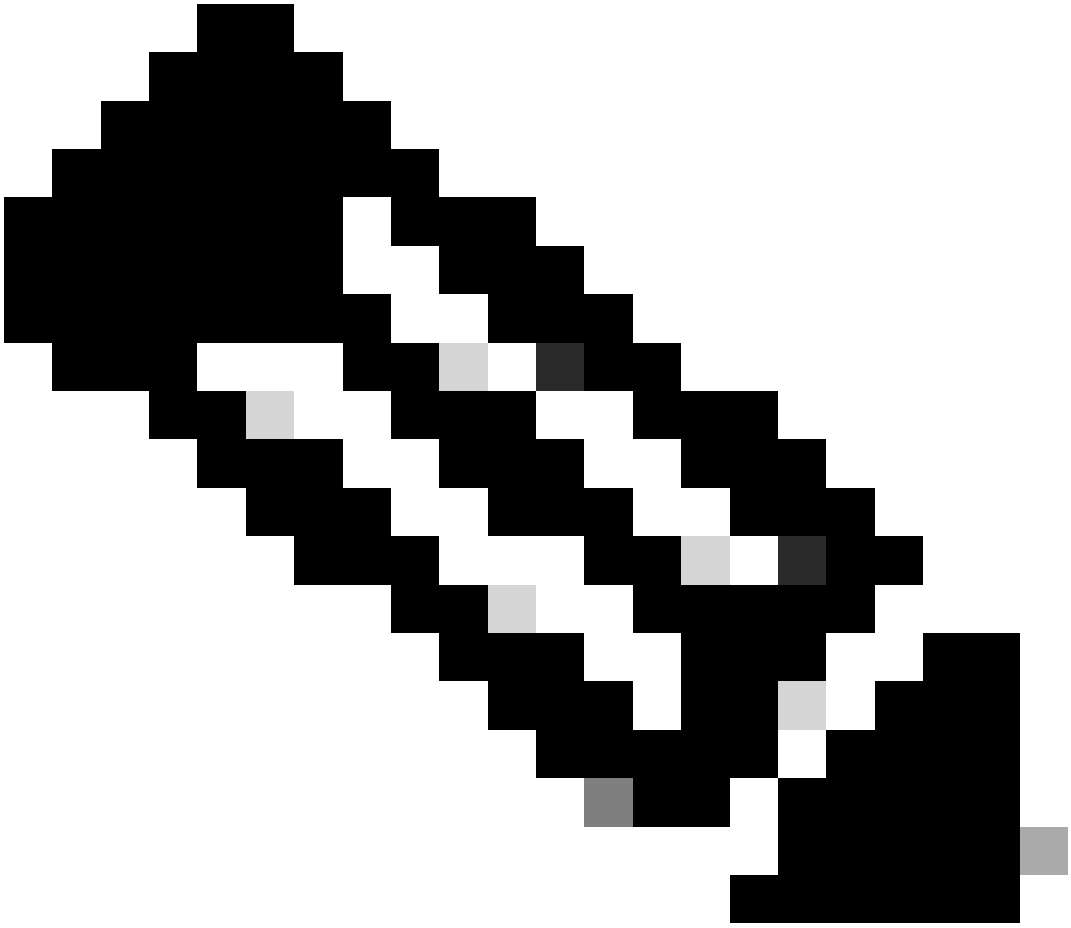
Essa configuração também pode ser usada com o Cisco PIX 500 Series Security Appliance Software versão 7.x.

Conventions

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

Informações de Apoio

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.



Observação: o tunelamento completo é considerado a configuração mais segura porque não permite o acesso simultâneo do dispositivo à Internet e à LAN corporativa. Um comprometimento entre o tunelamento completo e o tunelamento dividido permite que os clientes VPN acessem apenas a LAN local. Consulte PIX/ASA 7.x: Exemplo de Configuração de Permissão de Acesso à LAN Local para Clientes VPN para obter mais informações.

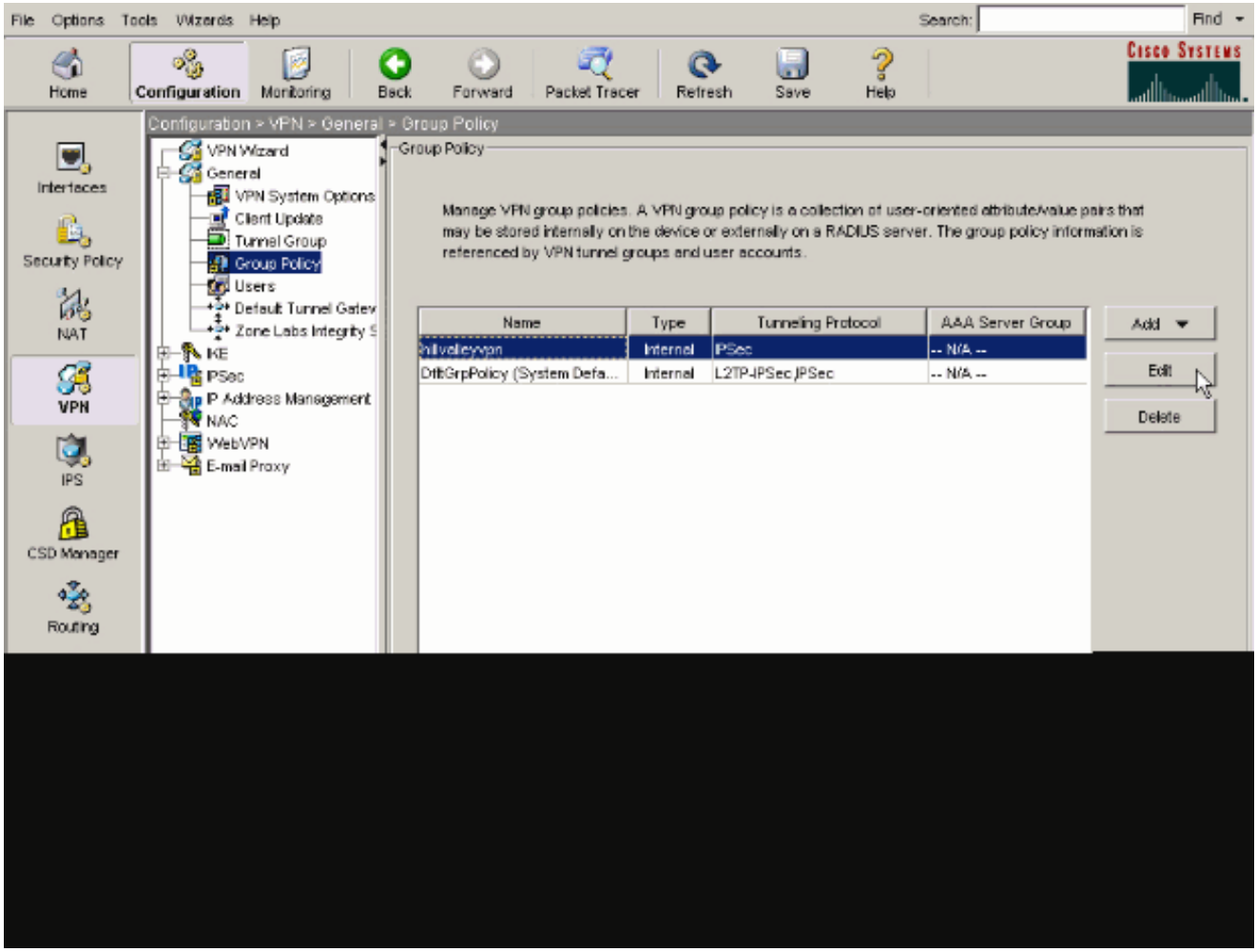
Em um cenário básico de VPN Client para ASA, todo o tráfego do VPN Client é criptografado e enviado para o ASA, independentemente de seu destino. Com base na sua configuração e no número de usuários suportados, essa configuração pode consumir muita largura de banda. O tunelamento dividido pode funcionar para aliviar esse problema, pois permite que os usuários enviem apenas o tráfego destinado à rede corporativa pelo túnel. Todo o tráfego restante, como mensagens instantâneas, e-mail ou navegação ocasional, é enviado para a Internet através da LAN local do VPN Client.

Configuração da Separação de Túneis no ASA

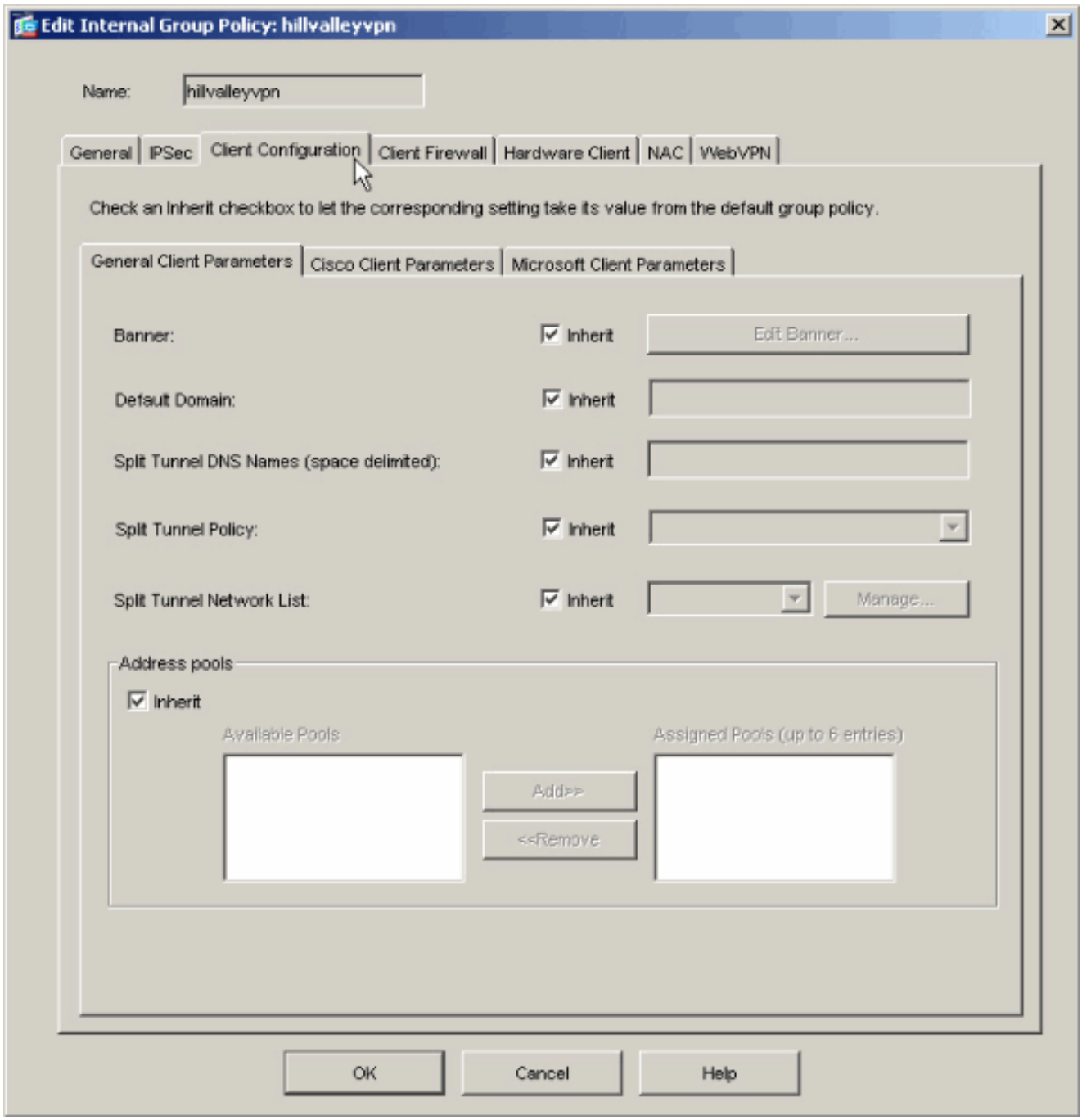
Configuração do ASA 7.x com o Adaptive Security Device Manager (ASDM) 5.x

Conclua estes passos para configurar seu grupo de túneis para permitir o tunelamento dividido para os usuários no grupo.

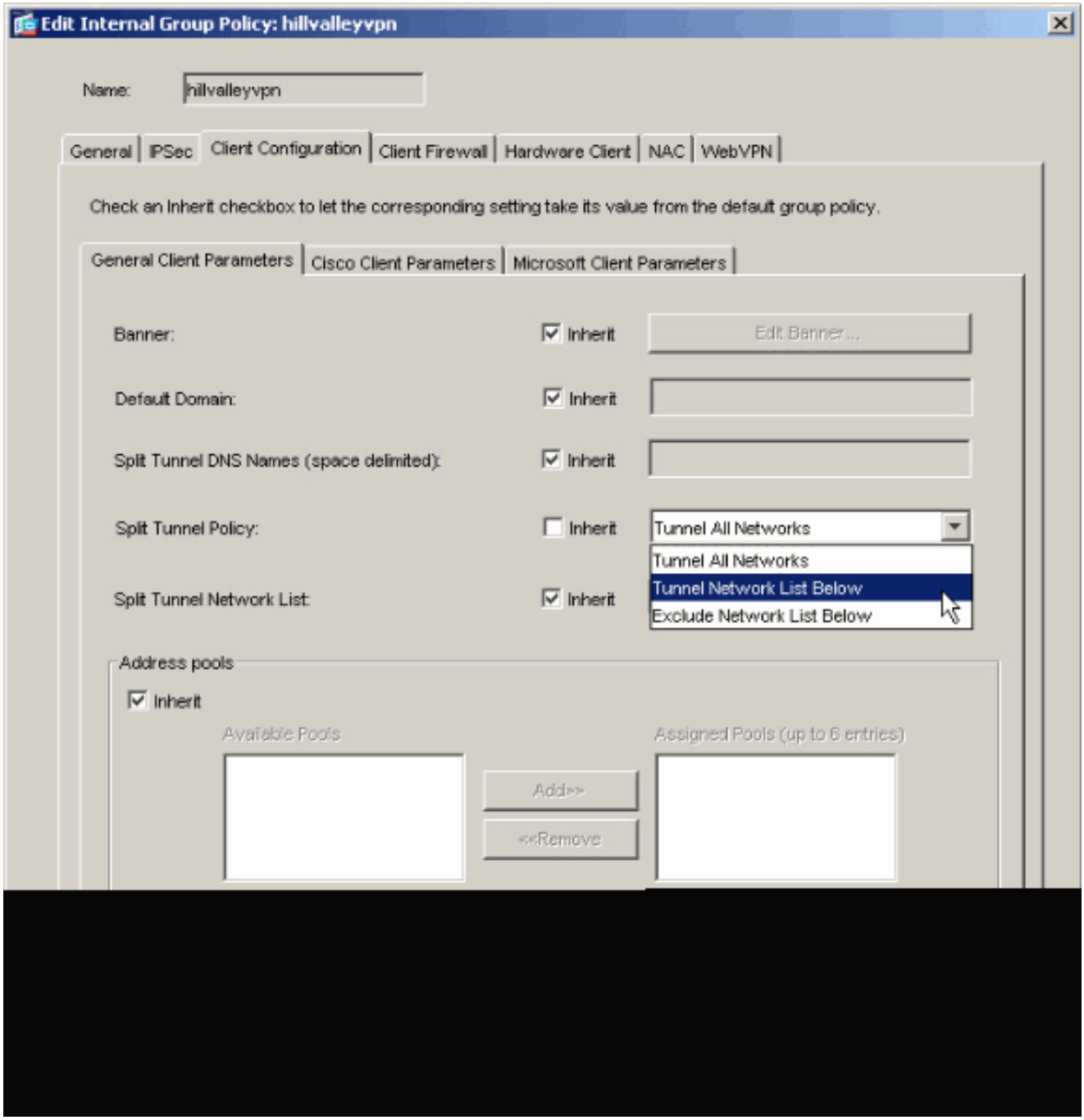
1. Escolha Configuration > VPN > General > Group Policy e selecione a Group Policy na qual você deseja habilitar o acesso à LAN local. Em seguida, clique em Editar.



2. Vá até a guia Client Configuration (Configuração do cliente).

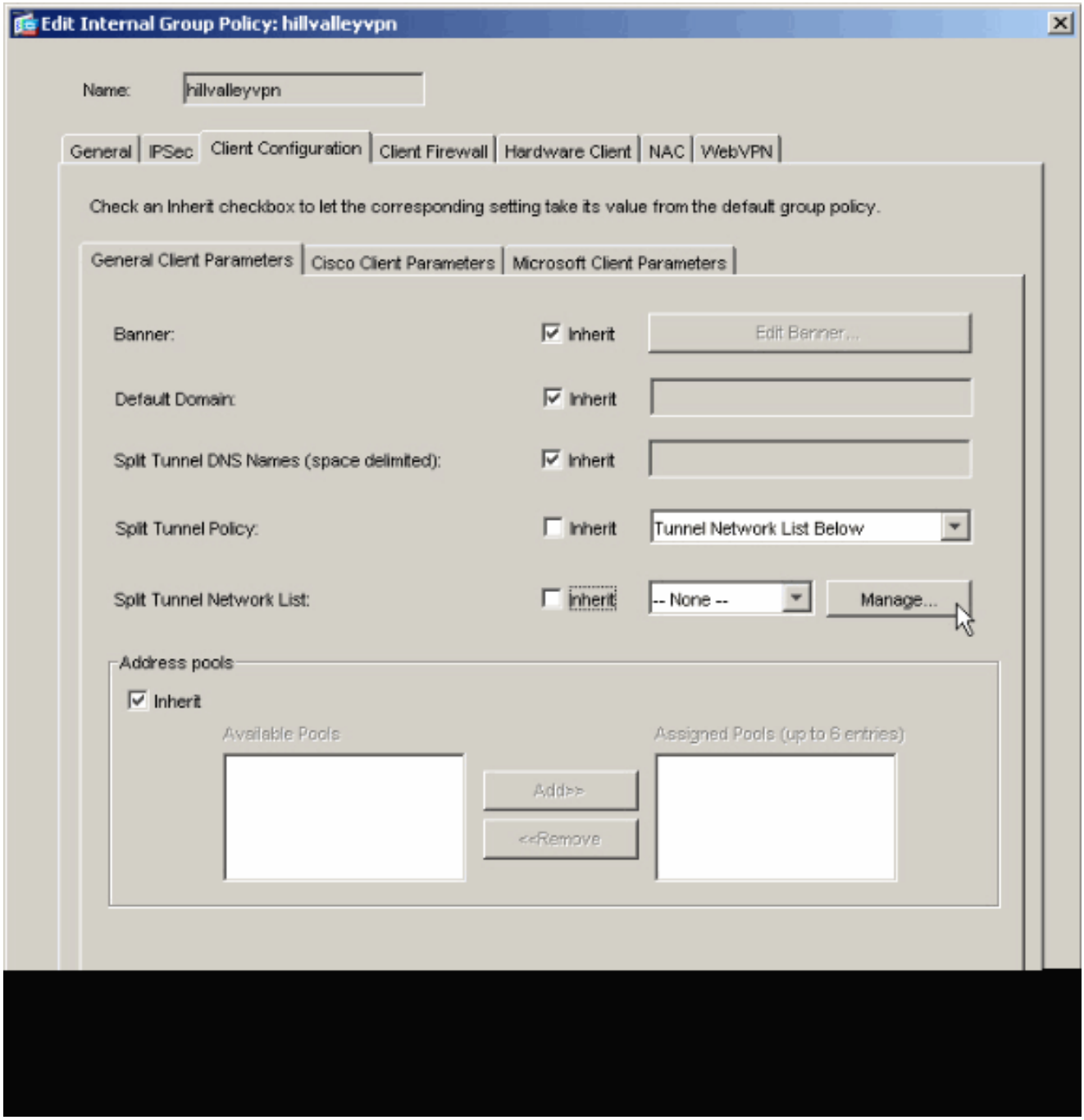


3. Desmarque a caixa Inherit para Split Tunnel Policy e selecione Tunnel Network List Below ..



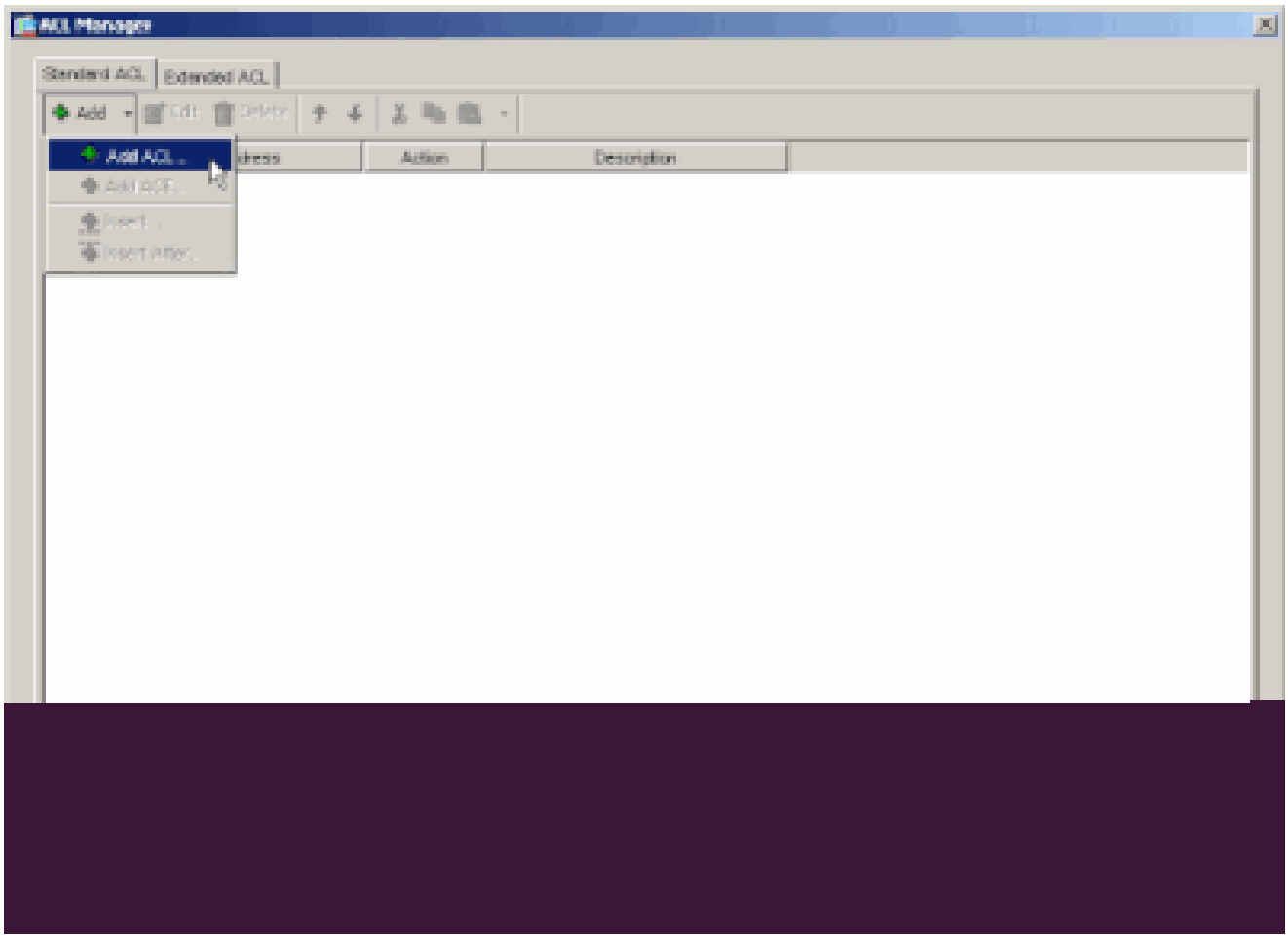
•

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



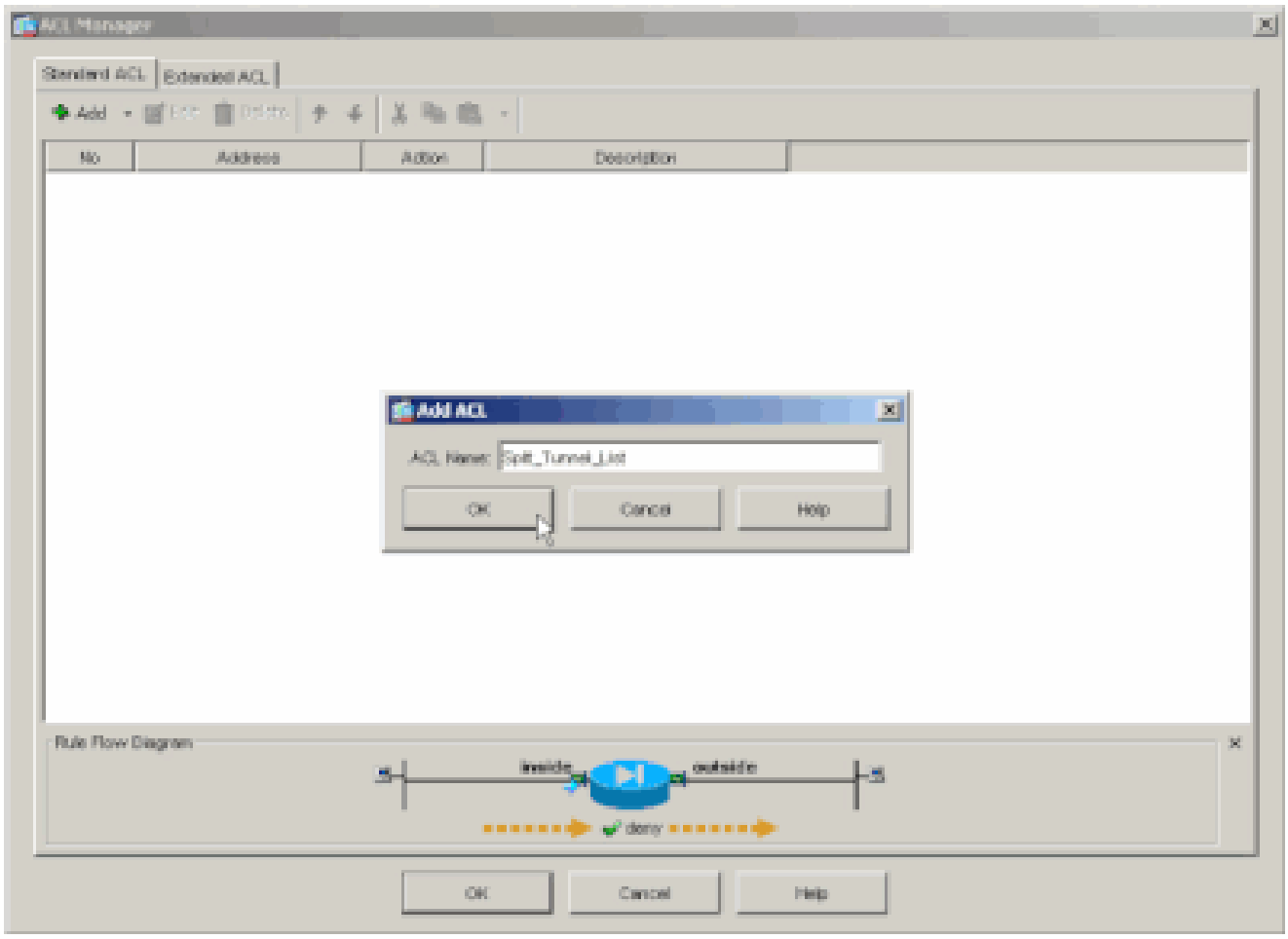
•

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



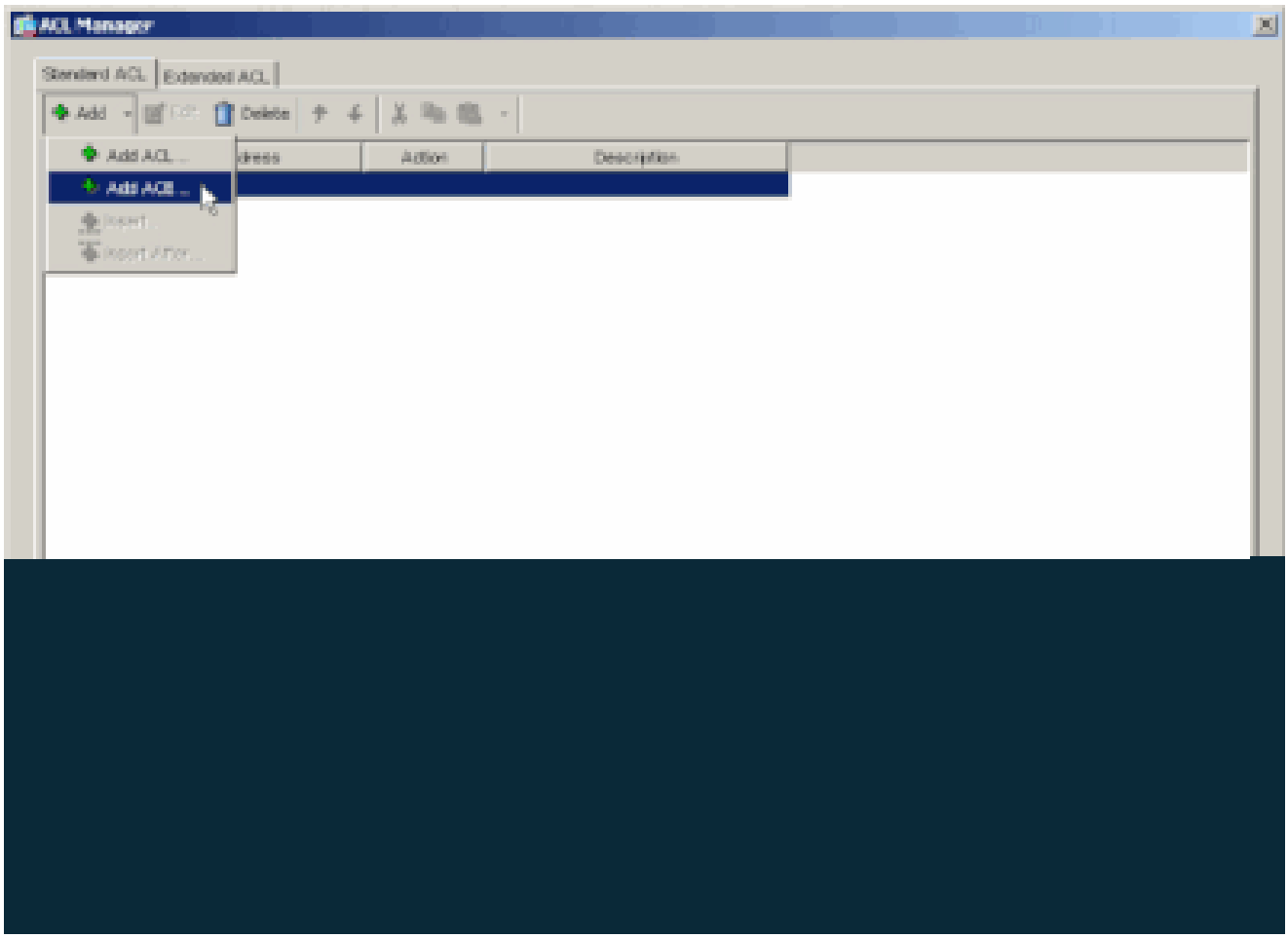
•

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



•

Depois que a ACL for criada, escolha **Add > Add ACE. .**para adicionar uma entrada de controle de acesso (ACE).



•

Defina a ACE que corresponde à LAN por trás do ASA. Nesse caso, a rede é 10.0.1.0/24.

a.

Escolha Permitir.

b.

Escolha o endereço IP 10.0.1.0

c.

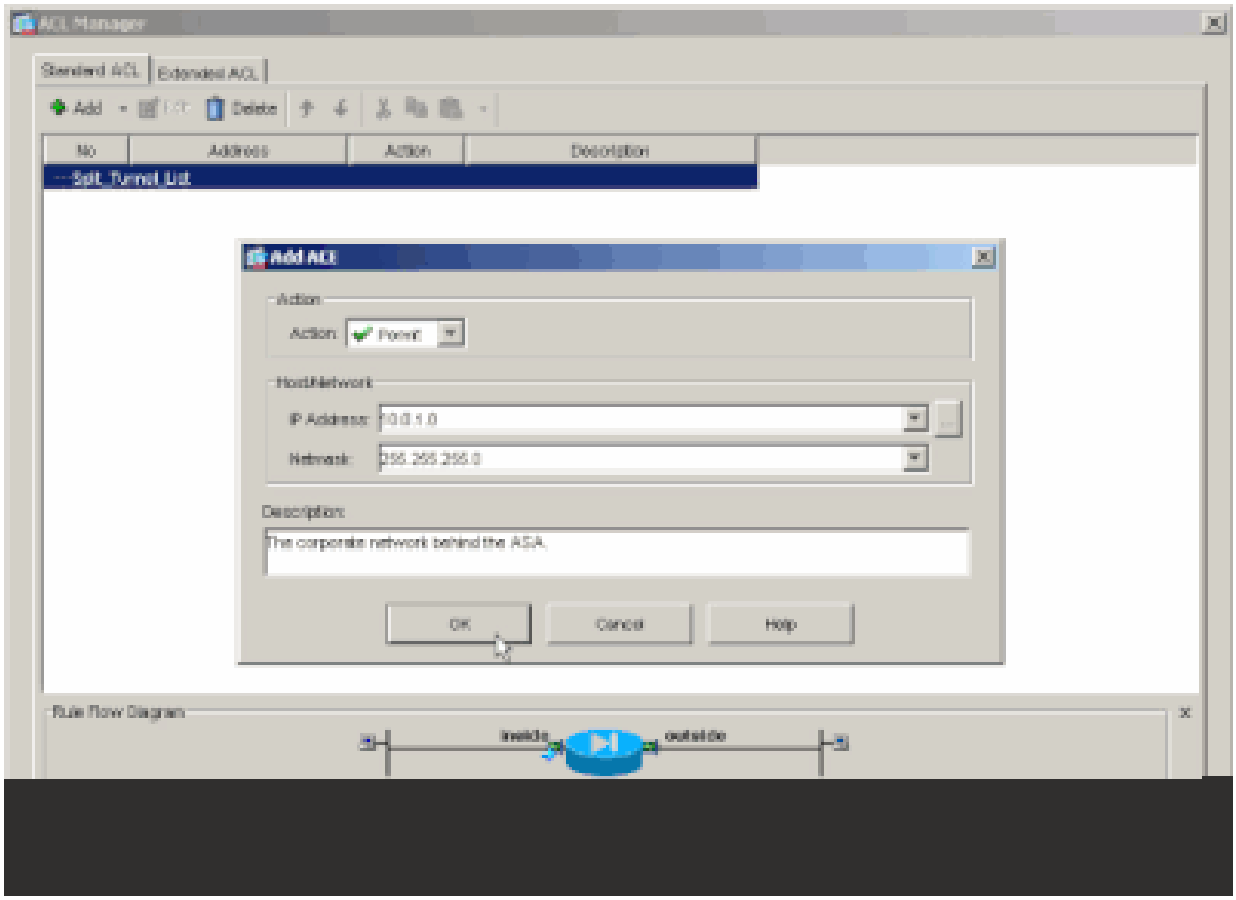
Escolha a máscara de rede **255.255.255.0.**

d.

*(Opcional)*Forneça uma descrição.

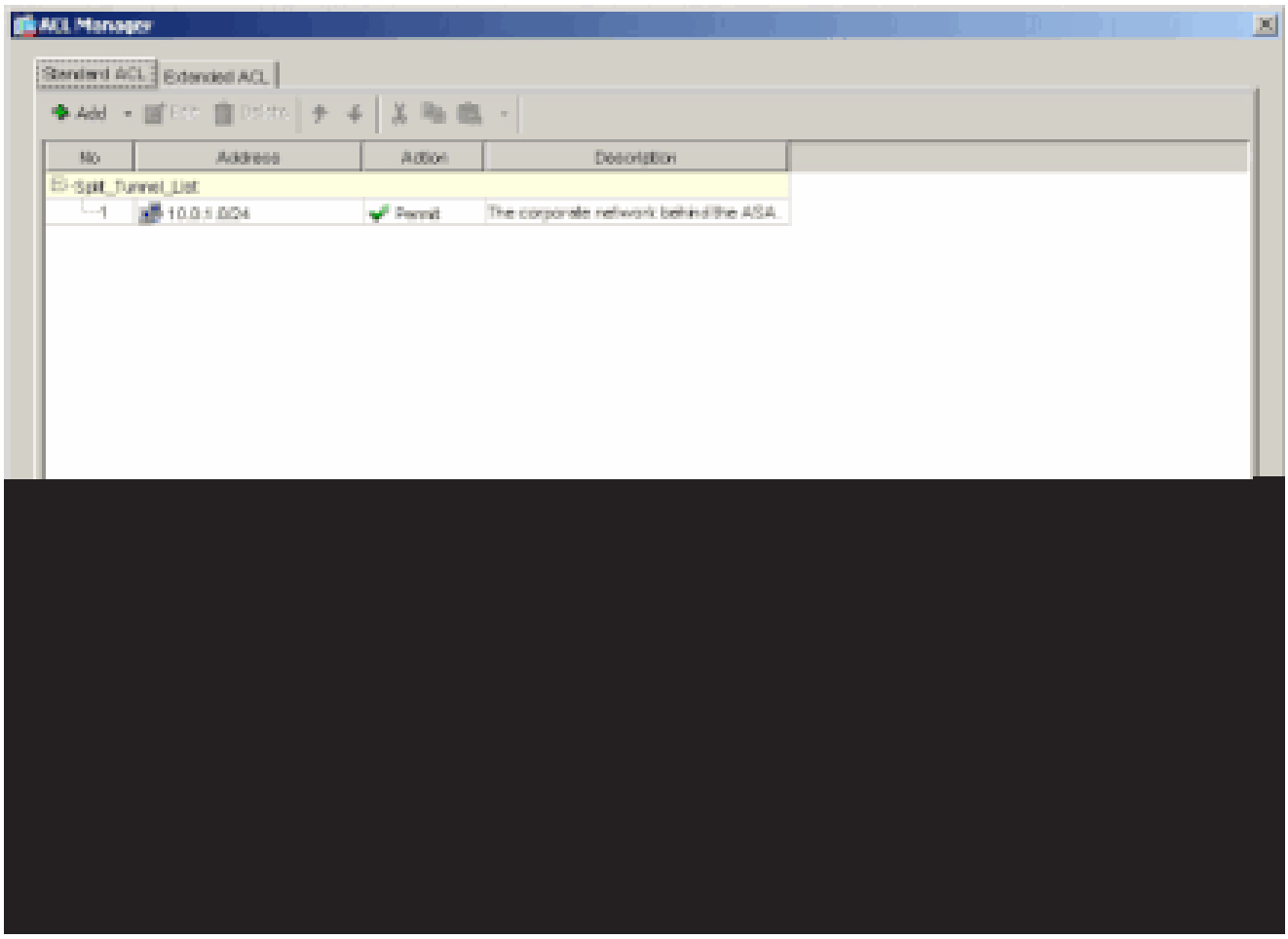
e.

Clique em > **OK**.



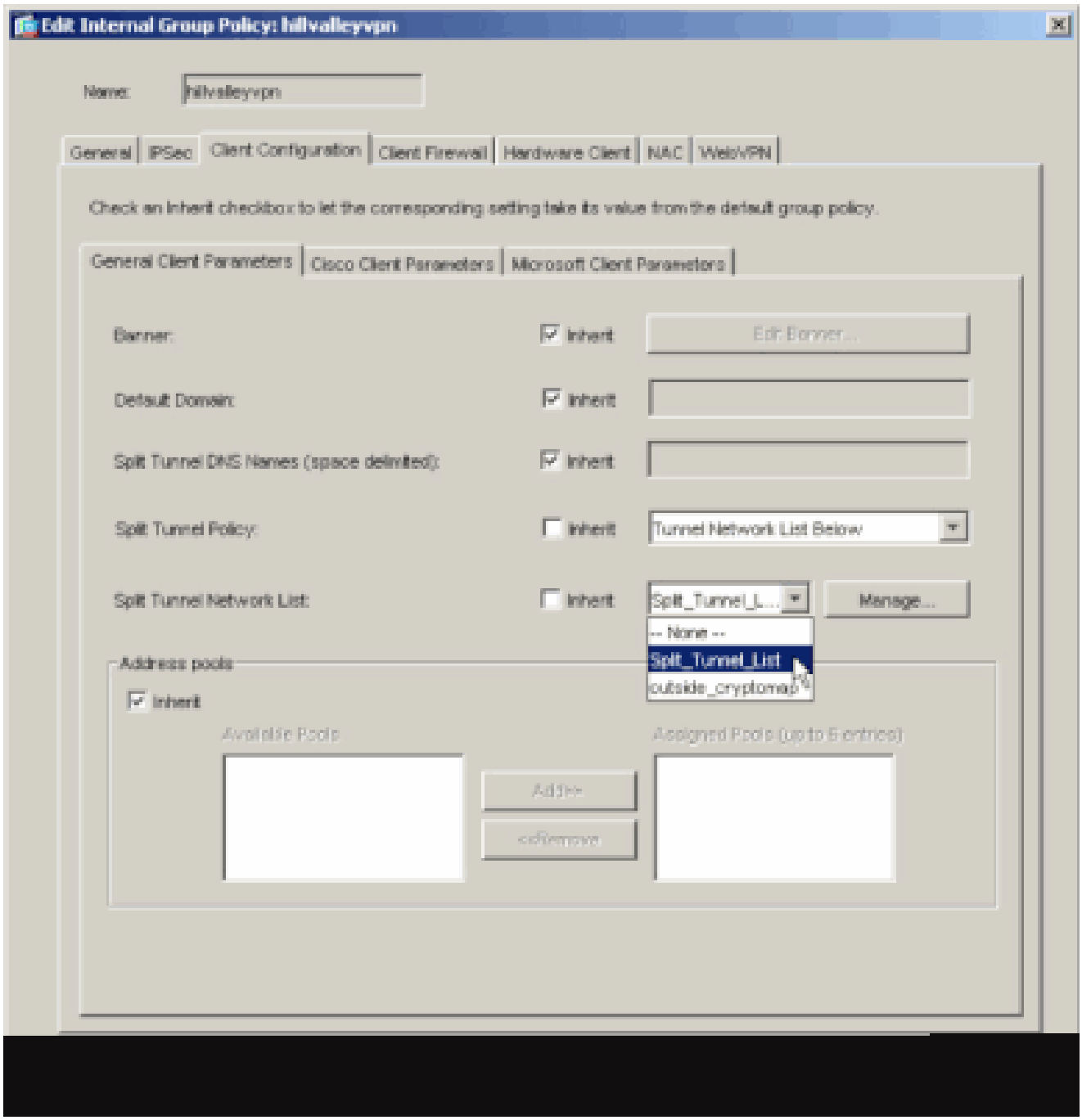
•

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



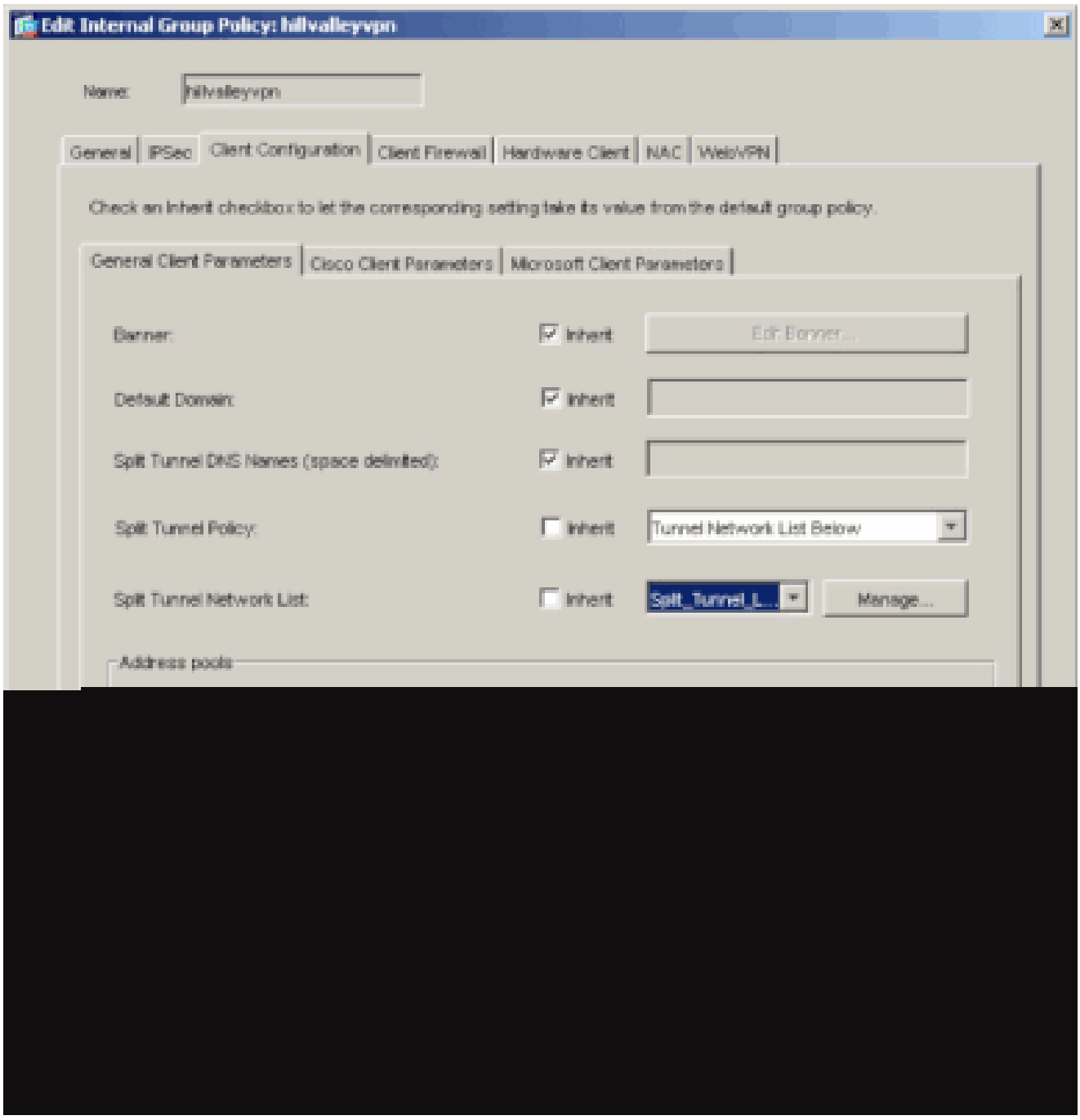
•

Certifique-se de que a ACL que você acabou de criar esteja selecionada para Split Tunnel Network List.



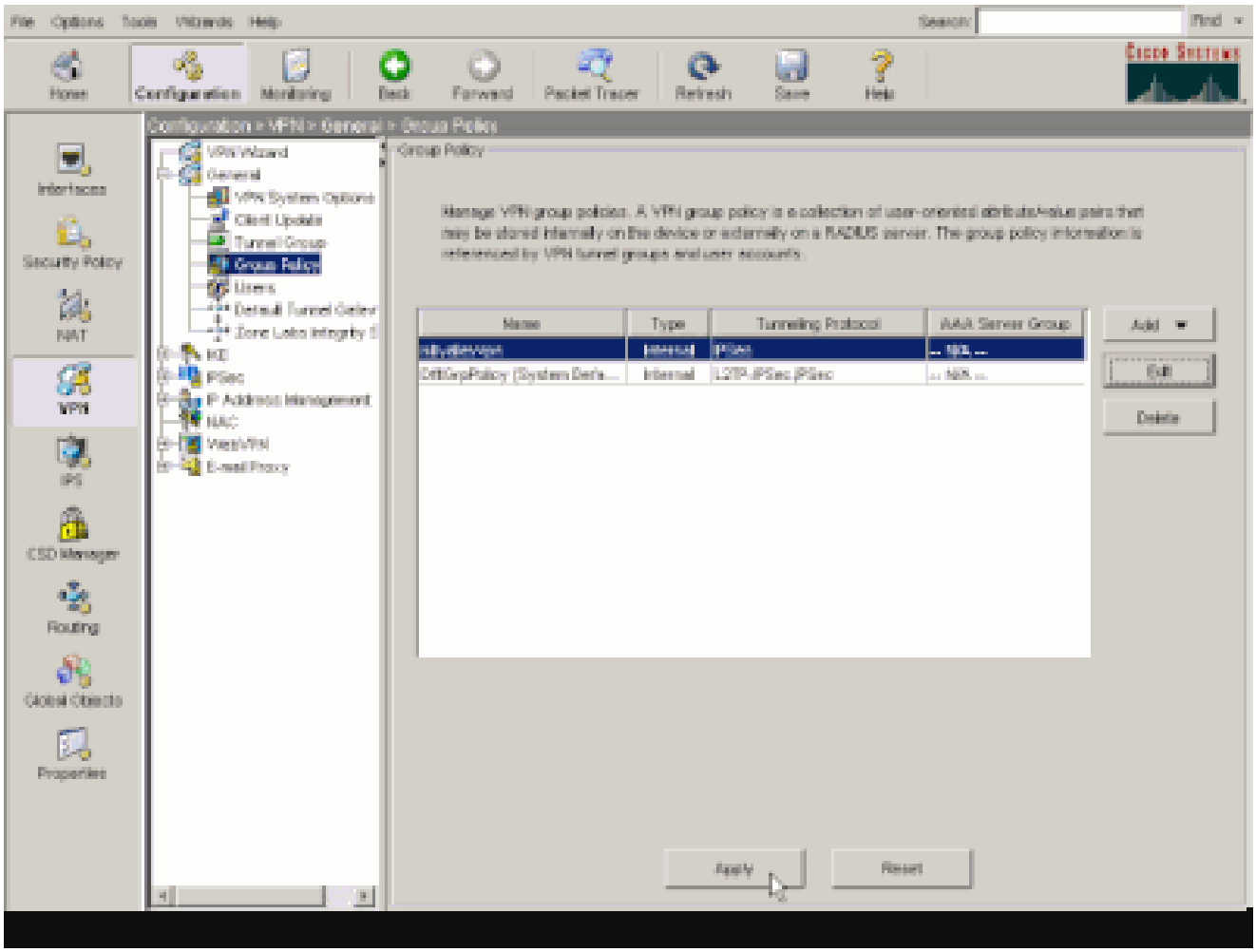
•

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



•

Clique em Aplicar e depois em Enviar (se necessário) para enviar os comandos para o ASA.

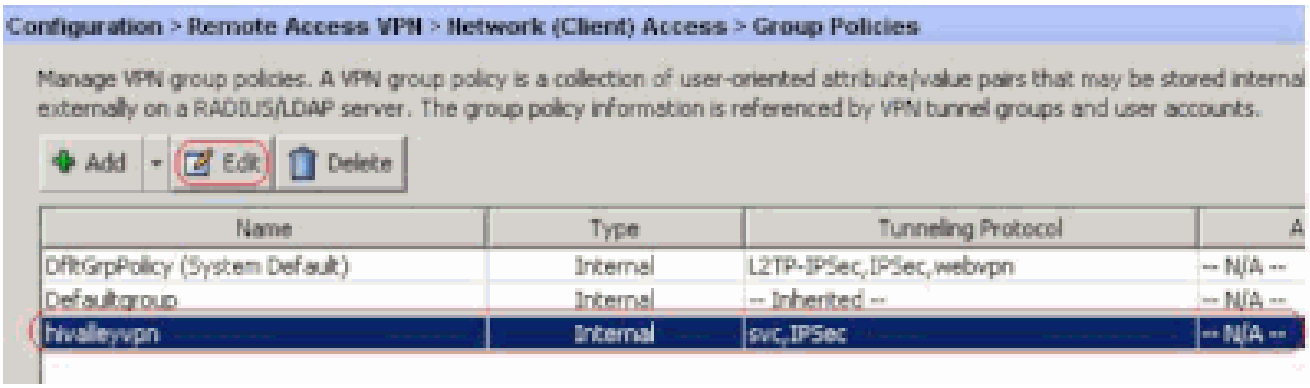


Configurar o ASA 8.x com o ASDM 6.x

Conclua estes passos para configurar seu grupo de túneis para permitir o tunelamento dividido para os usuários no grupo.

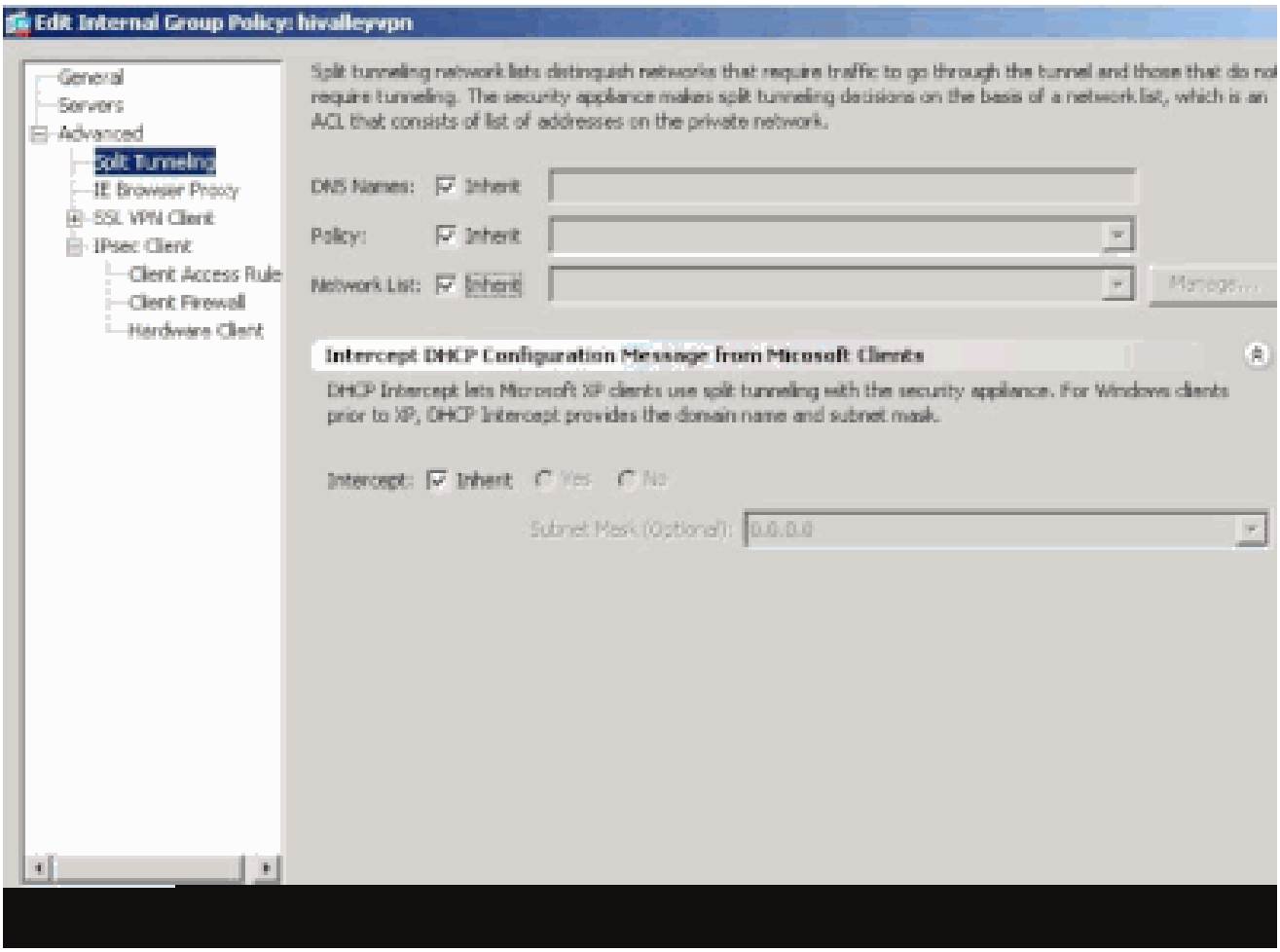
-

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. Em seguida, clique em Editar.



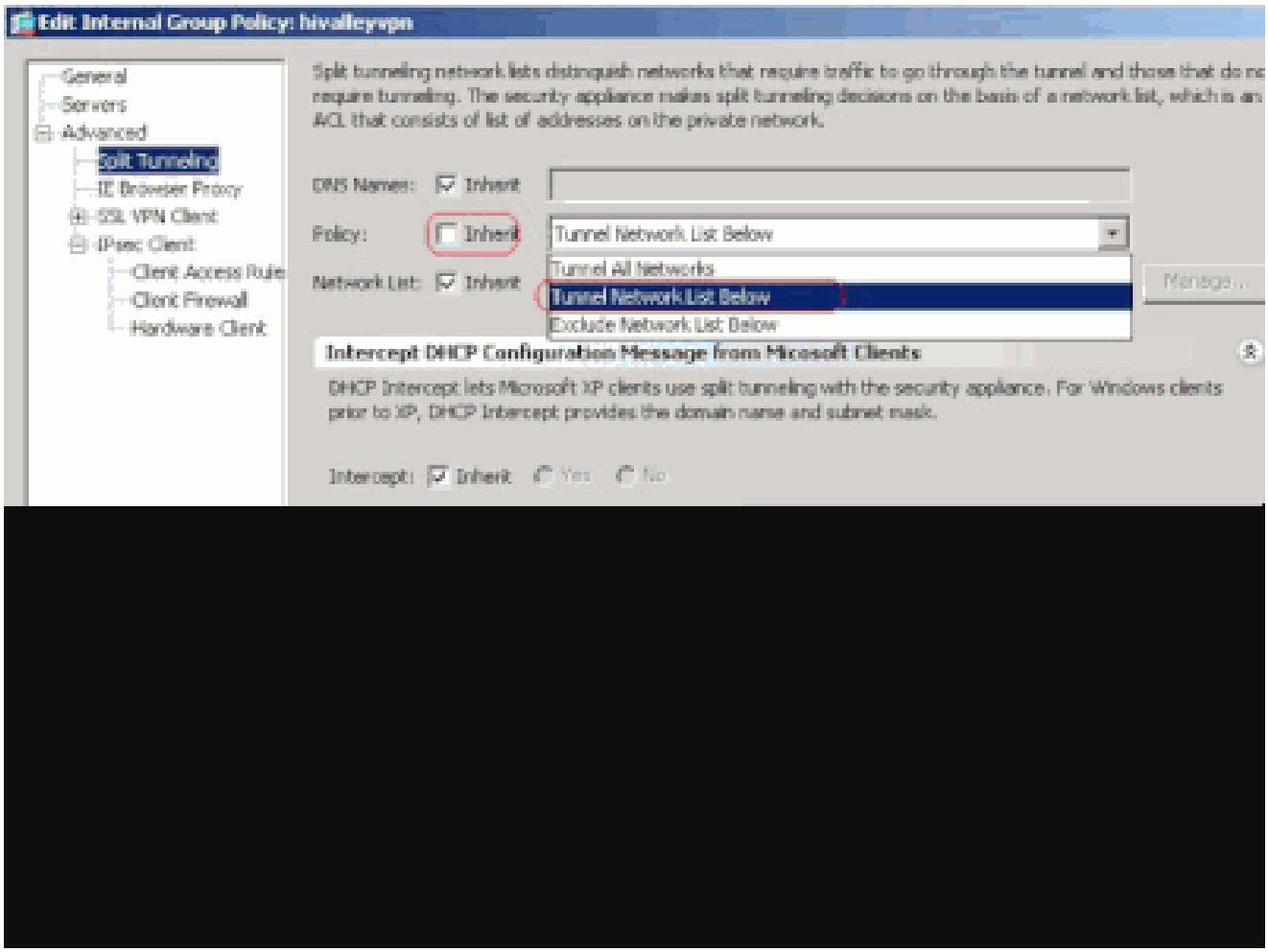
-

Clique em Split Tunneling.



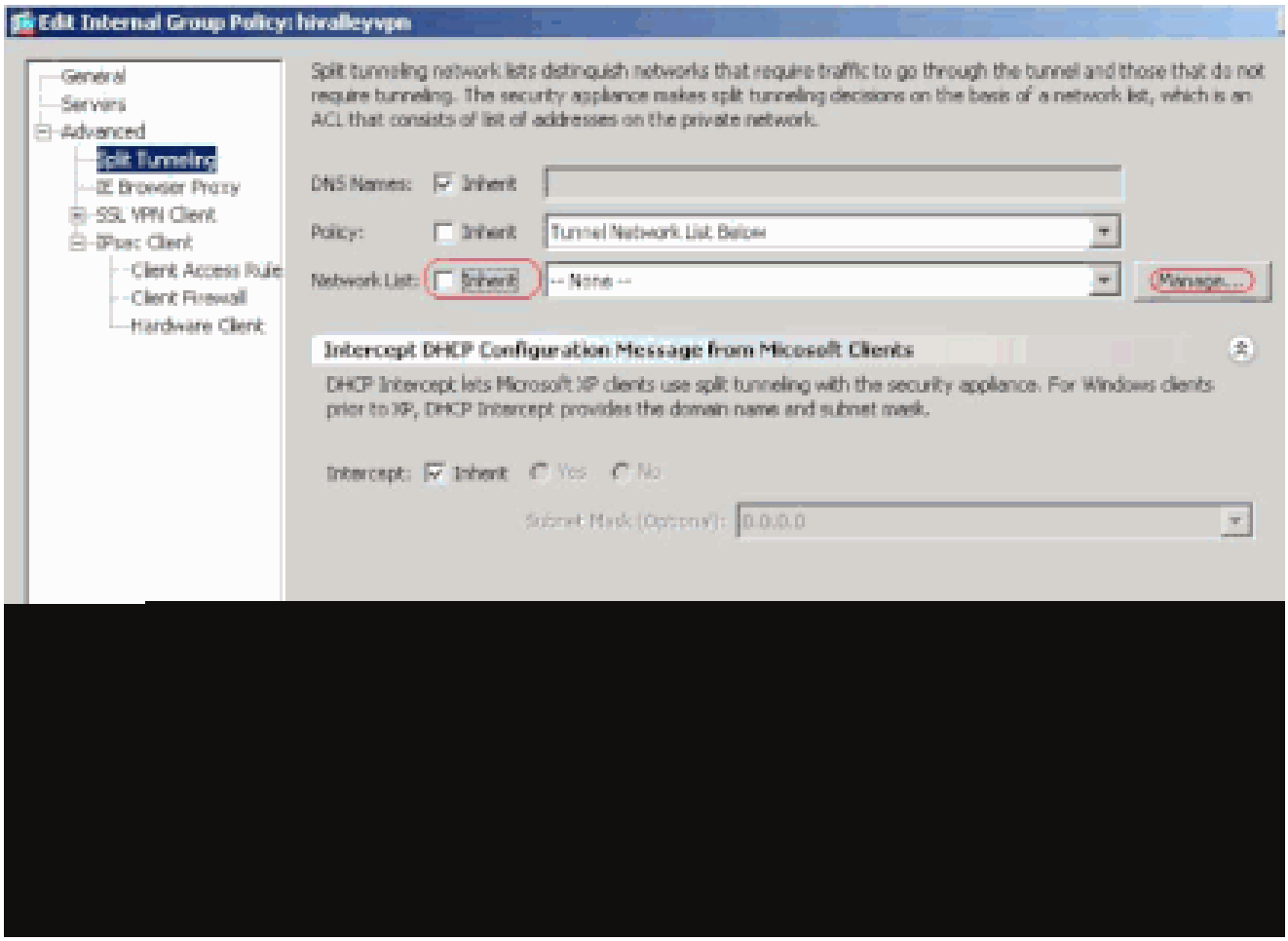
•

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



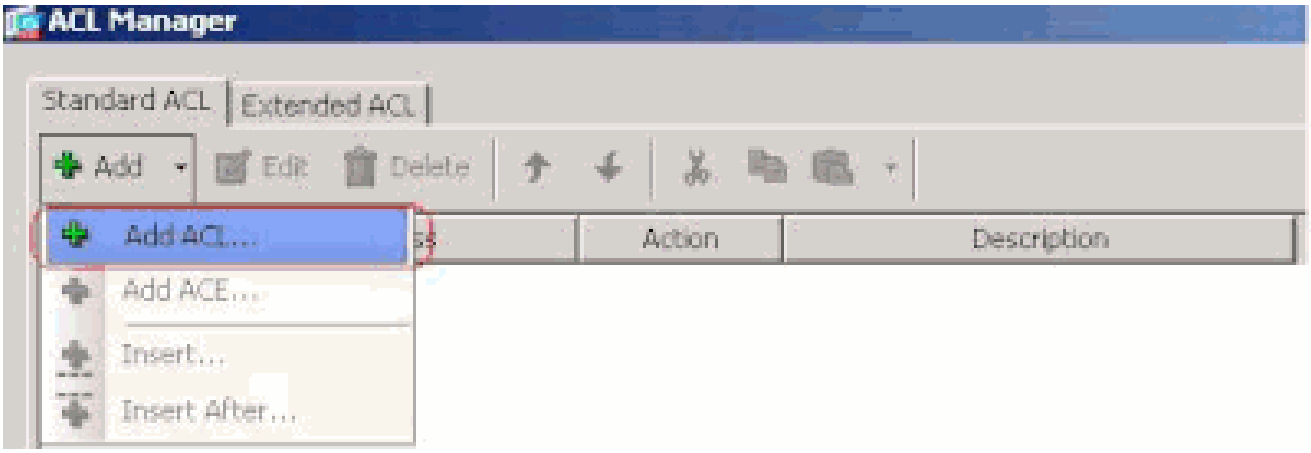
•

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



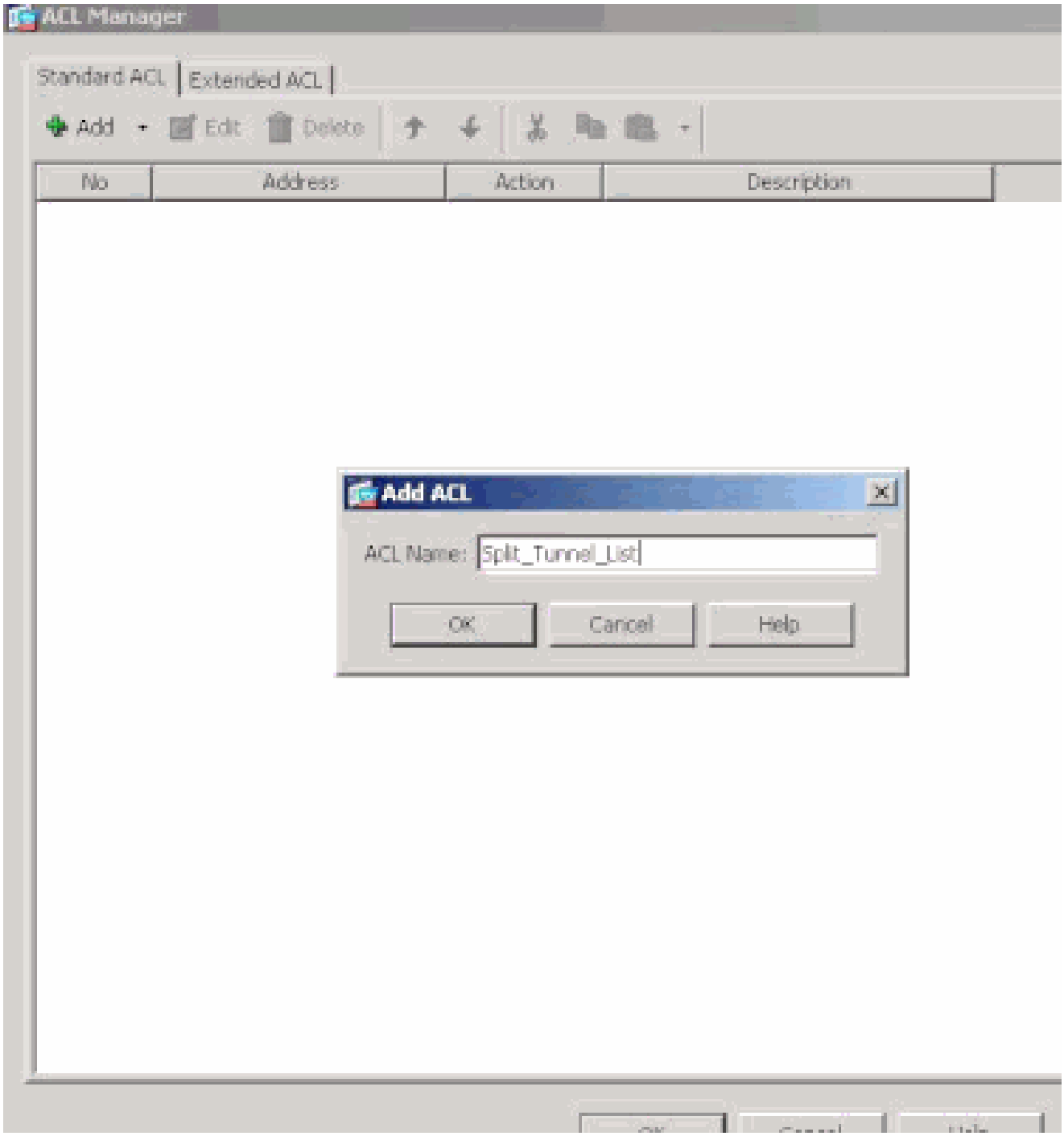
•

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



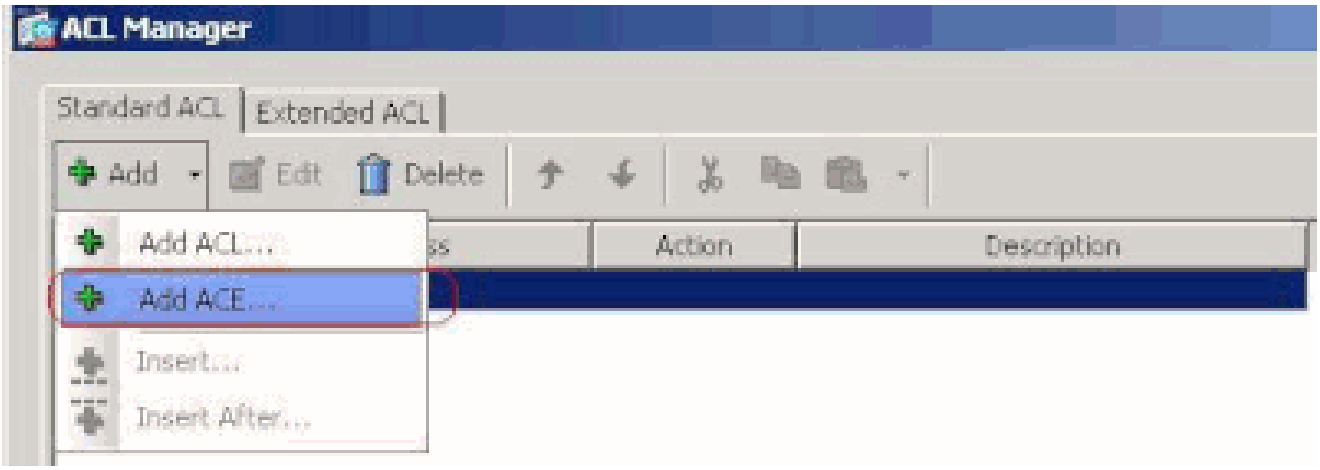
•

Forneça um nome para a ACL e clique em OK.



•

Após criar a ACL, selecione Adicionar > Adicionar ACE... para adicionar uma entrada de controle de acesso (ACE).



-

Defina a ACE que corresponde à LAN por trás do ASA. Nesse caso, a rede é 10.0.1.0/24.

a.

Clique no botão de opção Permit.

b.

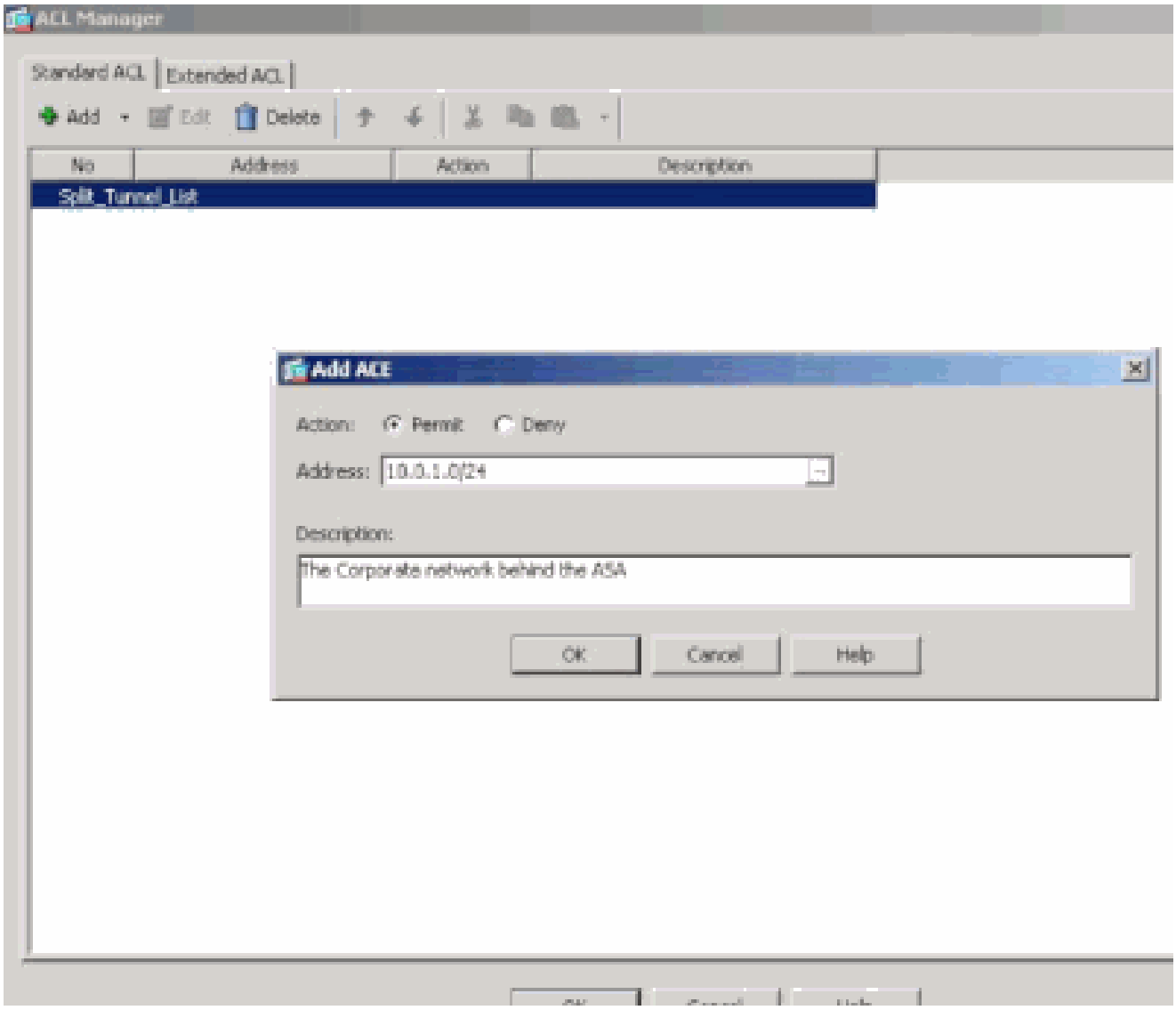
Selecione o endereço de rede com a máscara 10.0.1.0/24 .

c.

(Opcional) Forneça uma descrição.

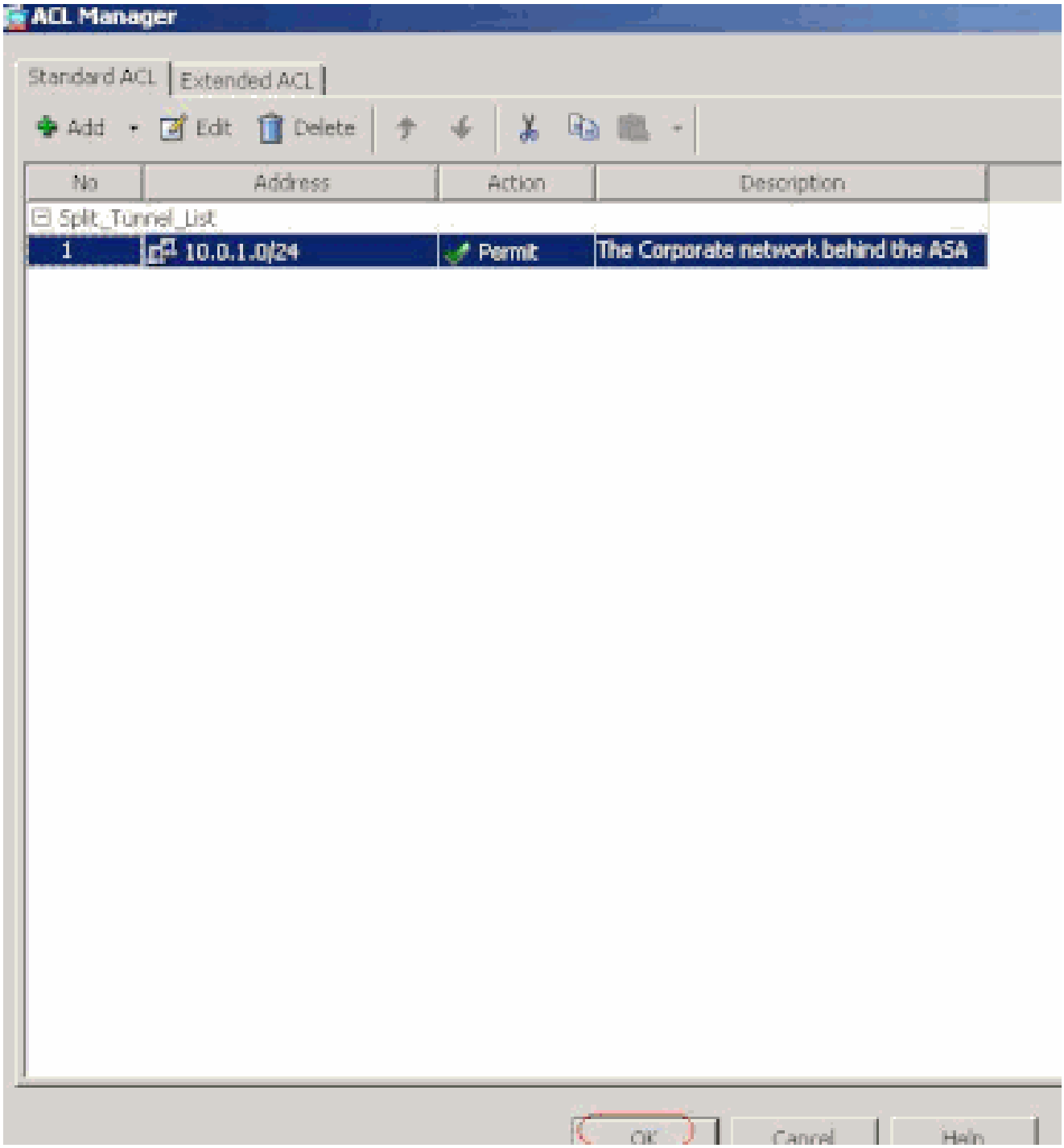
d.

Click OK.



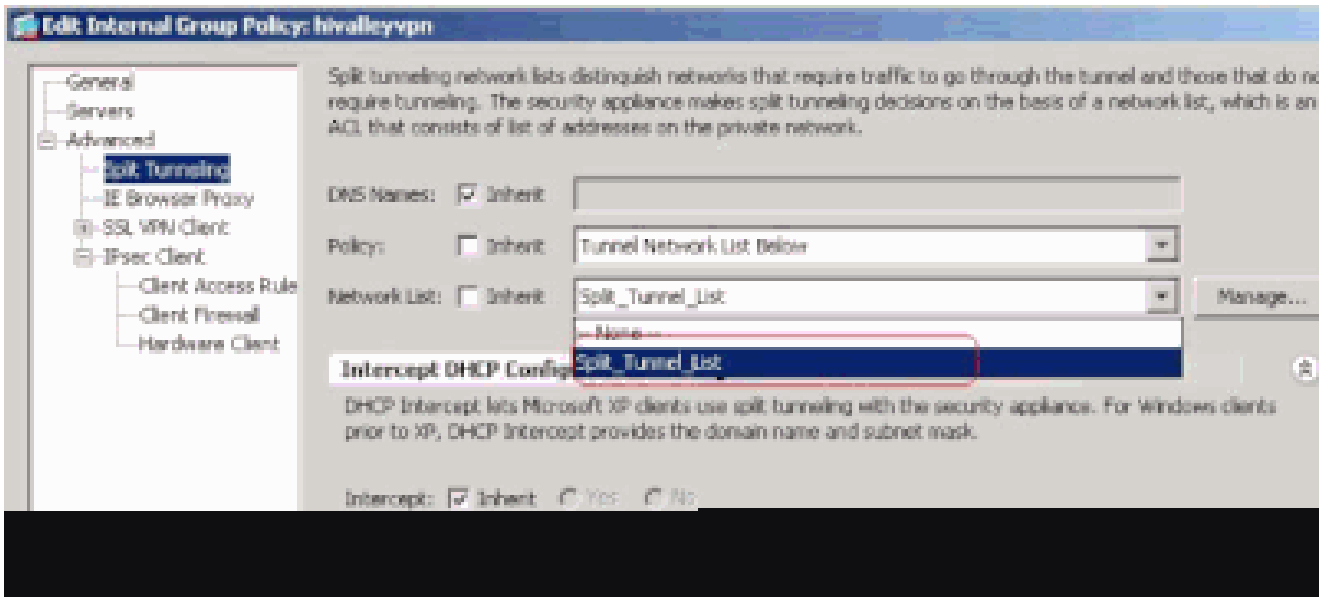
•

Clique em OK para sair do ACL Manager.



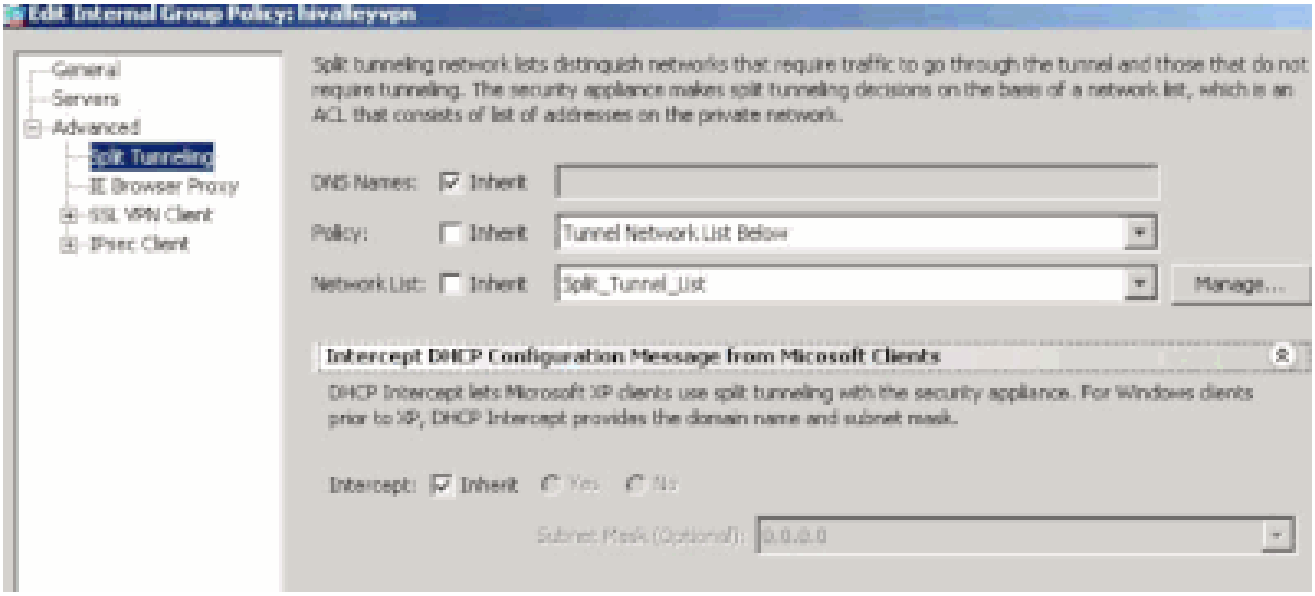
•

Certifique-se de que a ACL que você acabou de criar esteja selecionada para Split Tunnel Network List.



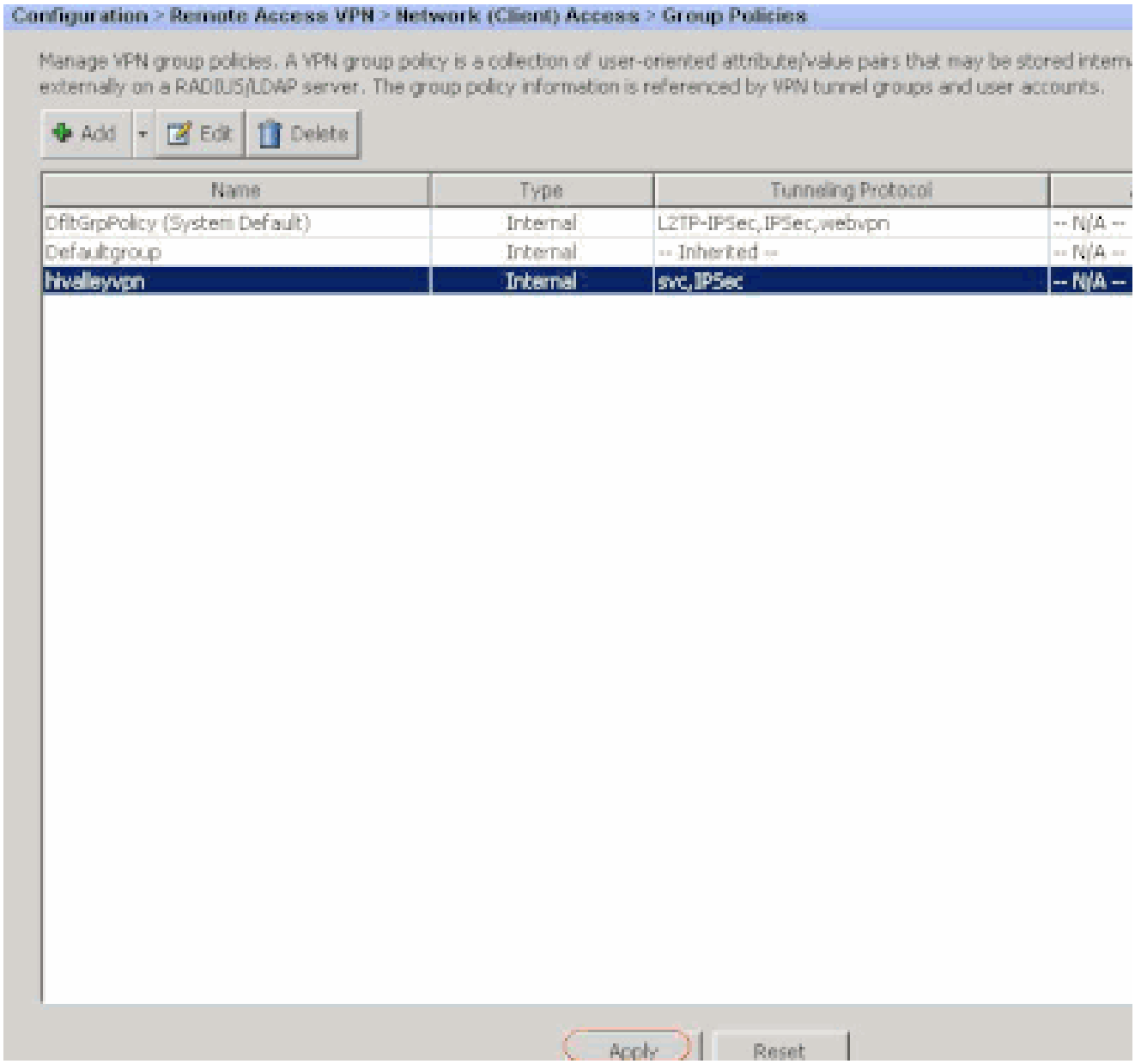
•

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



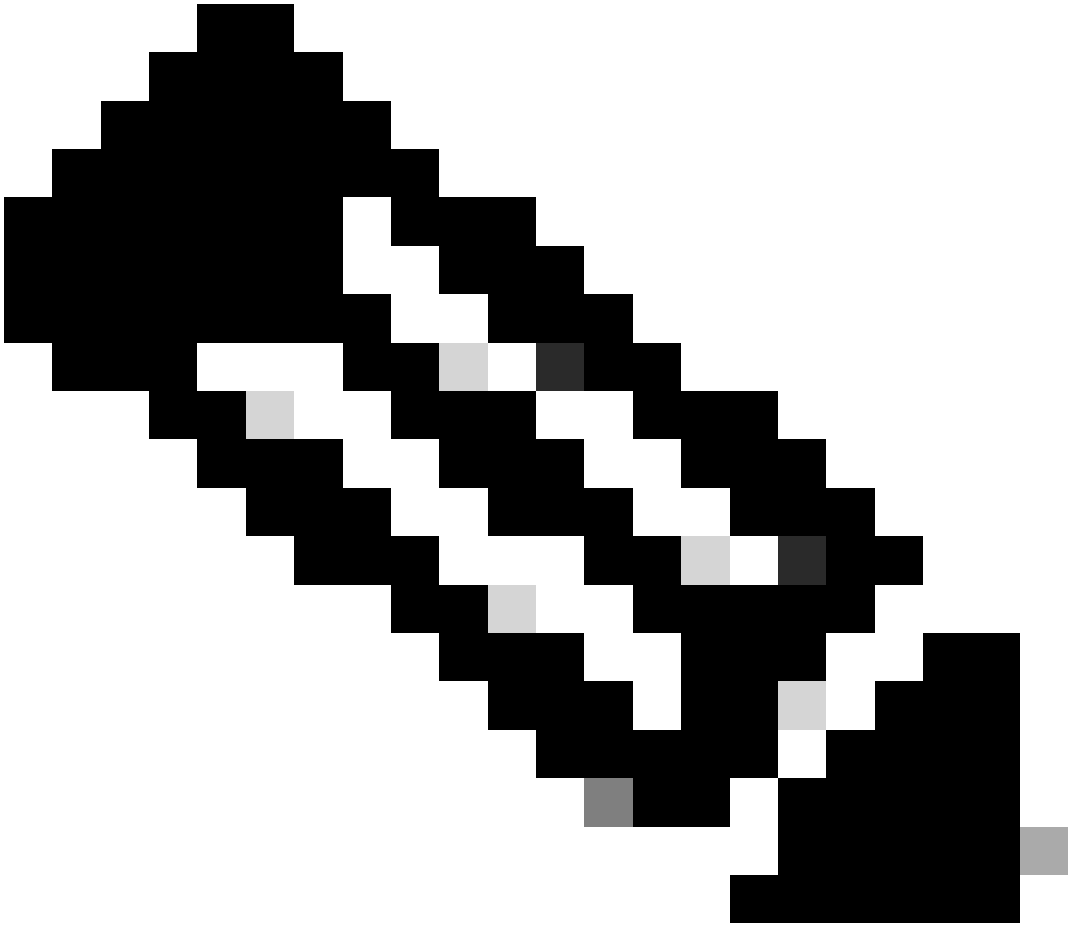
•

Clique em Aplicar e depois em Enviar (se necessário) para enviar os comandos para o ASA.



Configurar o ASA 7.x ou posterior via CLI

Em vez de usar o ASDM, você pode concluir estas etapas na CLI do ASA para permitir o tunelamento dividido no ASA:



Nota:A configuração da separação de túneis na CLI é a mesma para o ASA 7.x e 8.x.

-

Entre no modo de configuração.

```
<#root>

ciscoasa>
```

```
enable
```

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

```
configure terminal
```

```
ciscoasa(config)#
```

-

Crie a lista de acesso que define a rede por trás do 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
```

-

Entre no modo de configuração de Política de Grupo para a política que você deseja modificar.

```
    <#root>

ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

-

Especifique a política de túnel dividido. Neste caso, a política é tunnelspecified.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

-

Especifique a lista de acesso de túnel dividido. Neste caso, a lista é Split_Tunnel_List.

```
    <#root>

ciscoasa(config-group-policy)#

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

-

Emita este comando:

```
    <#root>

ciscoasa(config)#

 tunnel-group hillvalleyvpn general-attributes
```

-

Associe a política do grupo ao grupo do túnel.

```
    <#root>

ciscoasa(config-tunnel-ipsec)#

 default-group-policy hillvalleyvpn
```

-

Saia dos dois modos de configuração.

```
    <#root>

ciscoasa(config-group-policy)#

 exit

ciscoasa(config)#

 exit
```

```
ciscoasa#
```

- Salve a configuração na RAM não volátil (NVRAM) e pressione Enter quando avisado para especificar o nome de arquivo de origem.

```
<#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#
```

Configurar o PIX 6.x através do CLI

Conclua estes passos:

- Crie a lista de acesso que define a rede atrás do PIX.

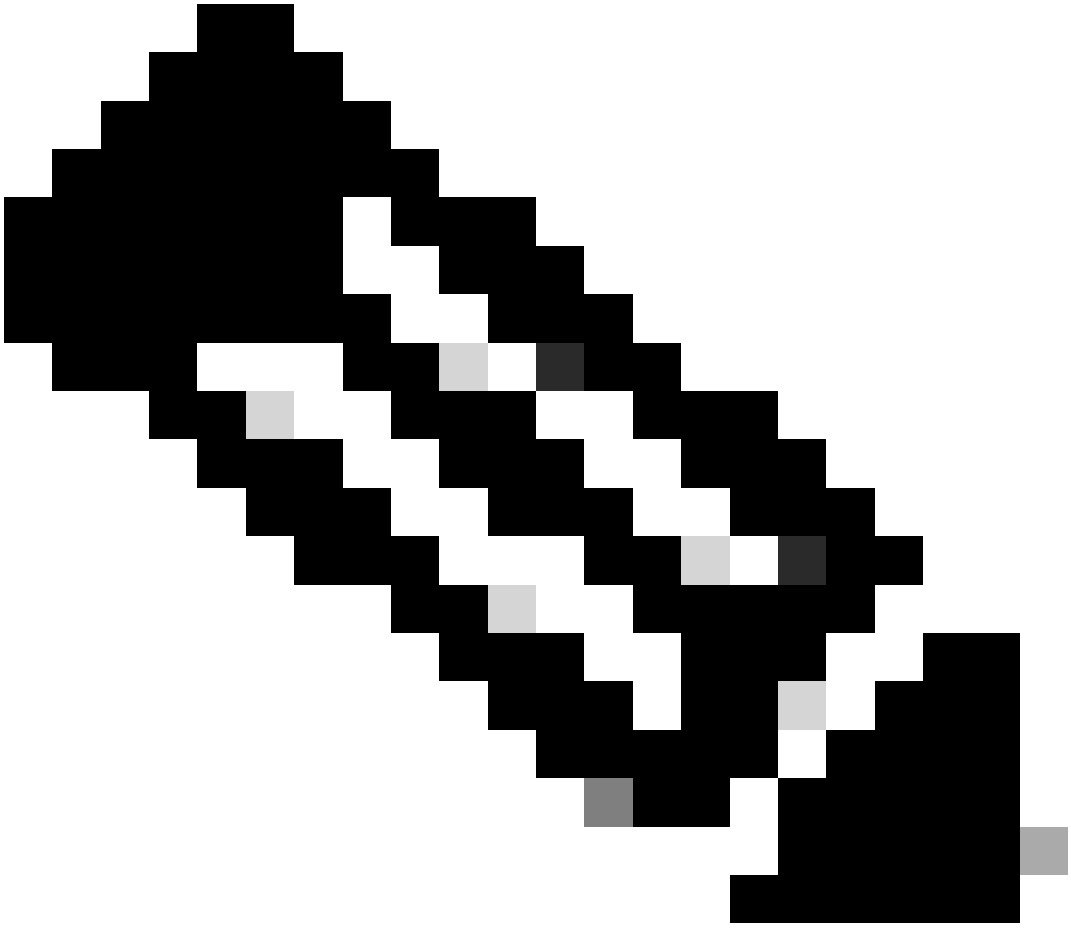
```
<#root>

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

- Crie um vpn group **vpn3000** e especifique a ACL do túnel dividido para ele como mostrado:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



Observação: consulte o Cisco Secure PIX Firewall 6.x e o Cisco VPN Client 3.5 para Windows com Autenticação IAS RADIUS do Microsoft Windows 2000 e 2003 para obter mais informações sobre a configuração de VPN de acesso remoto para o PIX 6.x.

Verificar

Conclua as etapas nessas seções para verificar a configuração.

- Conexão com o Cliente VPN

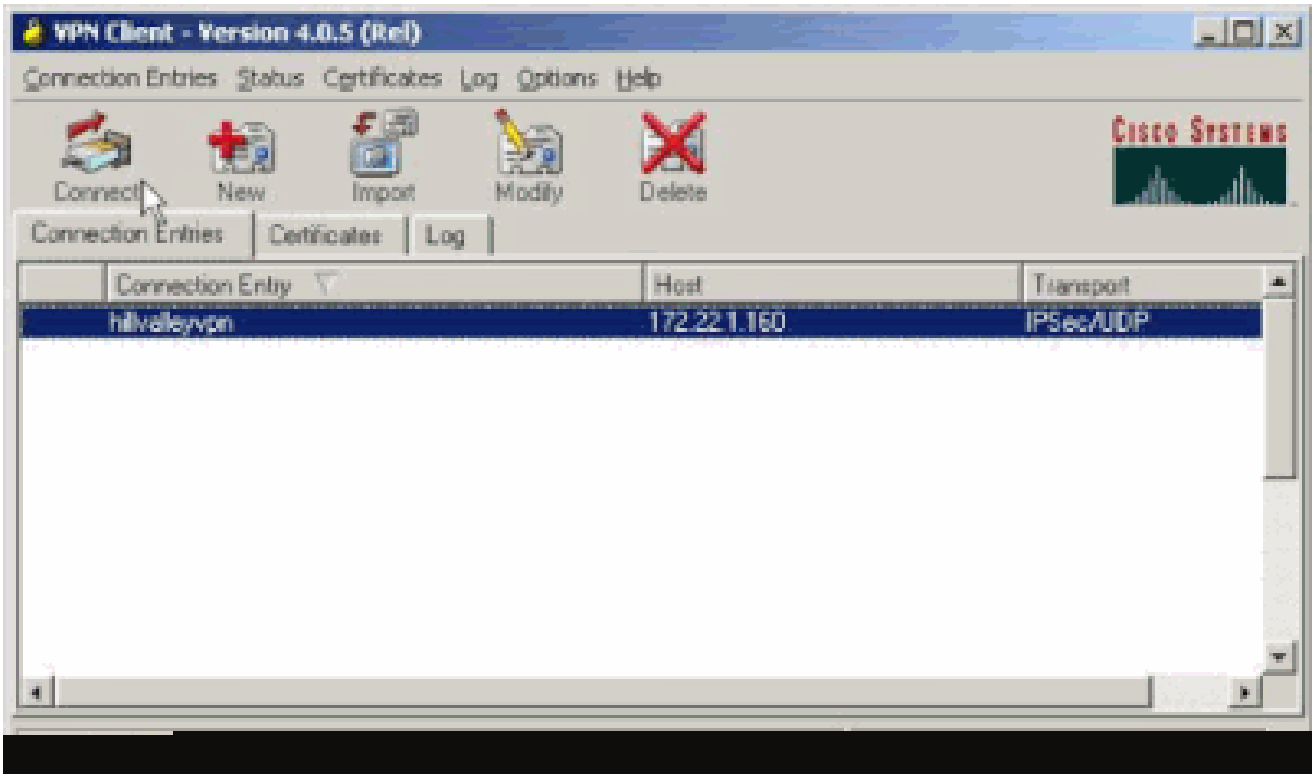
- Exibir o registro do cliente VPN

- Teste o acesso à LAN local com ping

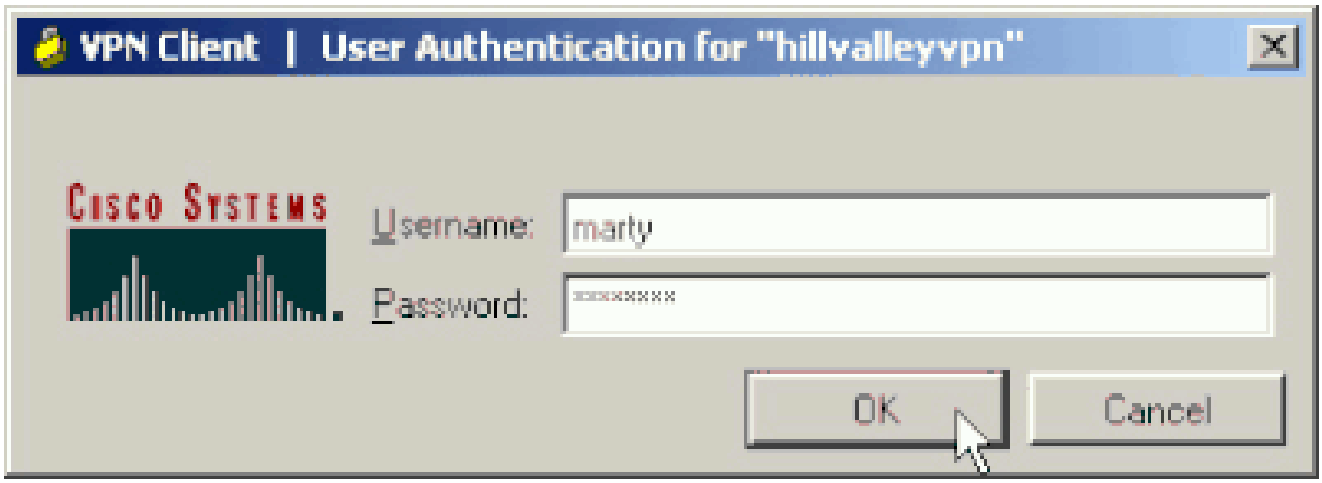
Conexão com o Cliente VPN

Conecte seu VPN Client ao VPN Concentrator para verificar sua configuração.

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

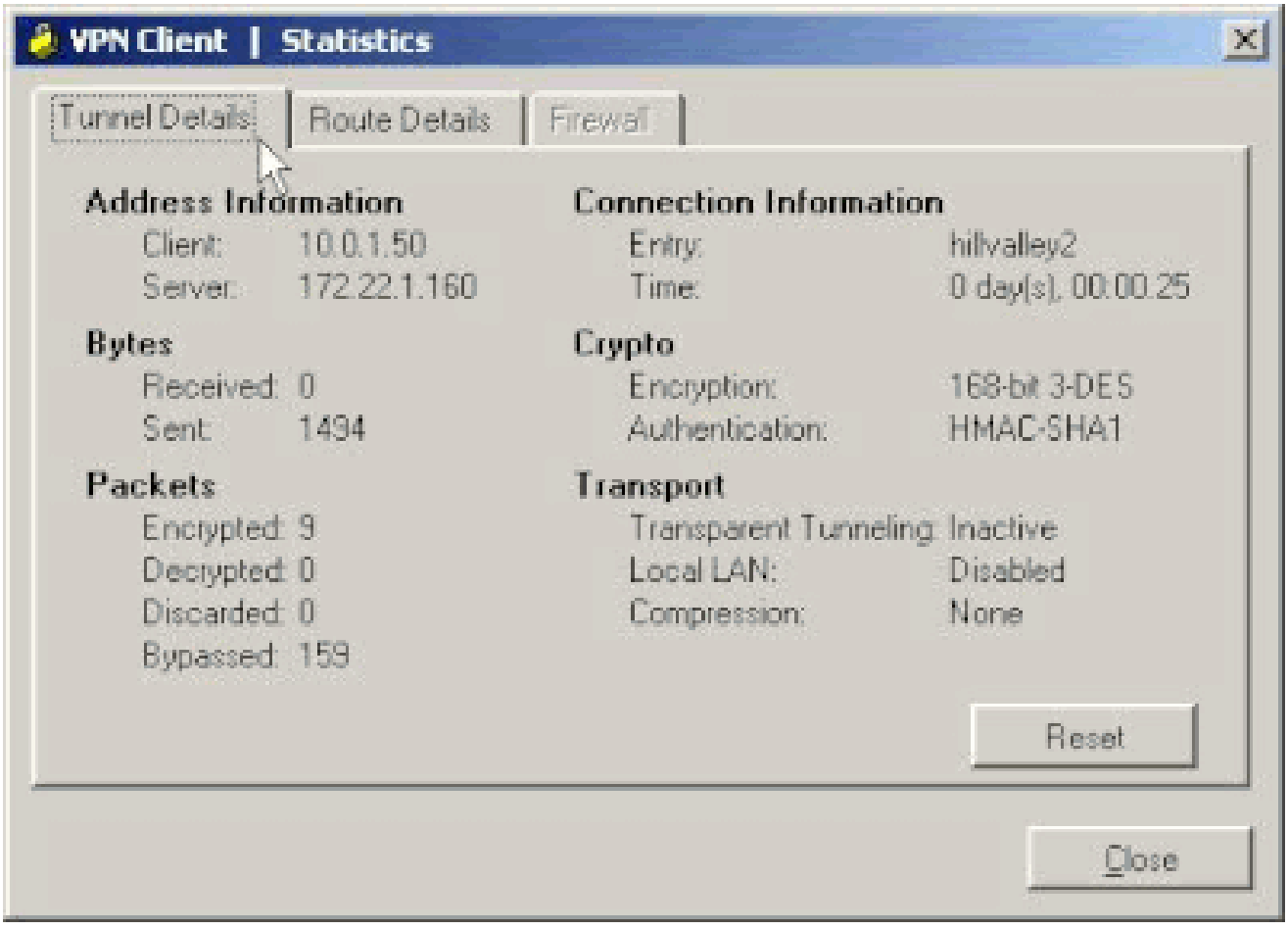


- Digite suas credenciais.



•

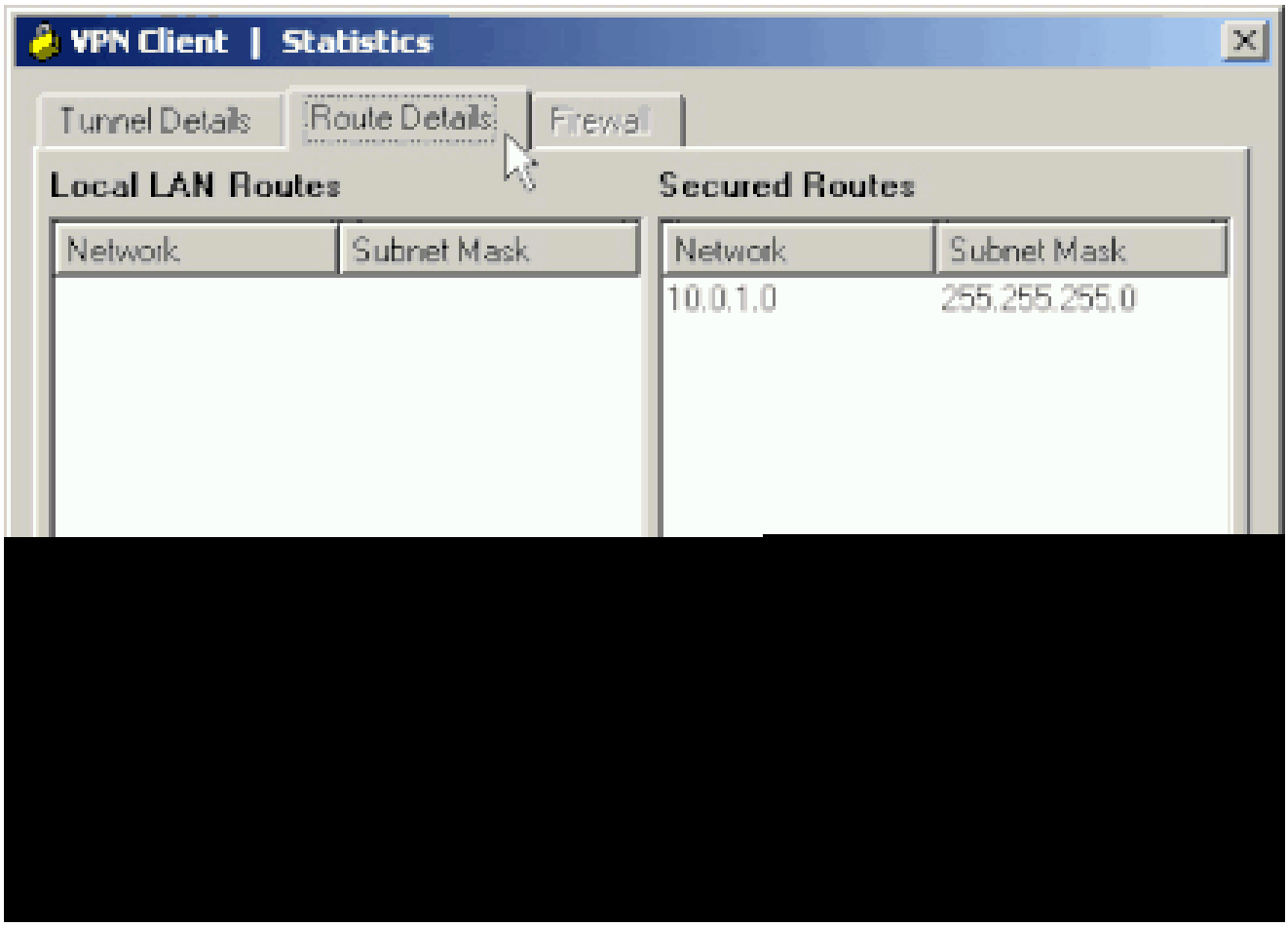
Escolha **Status > Statistics...** para exibir a janela Tunnel Details onde você pode inspecionar os detalhes do túnel e ver o tráfego fluindo.



•

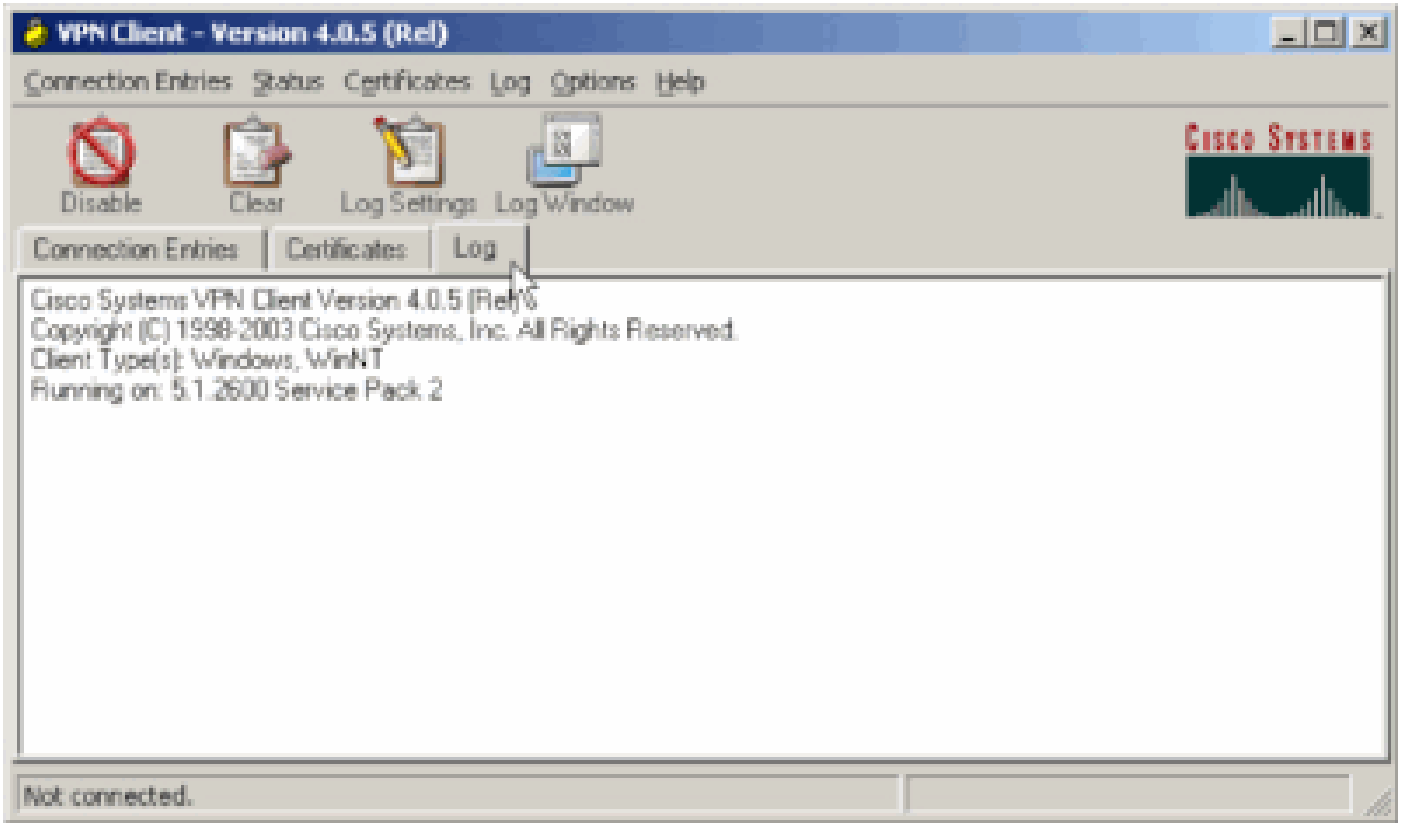
Acesse a guia Route Details para ver as rotas que o VPN Client está protegendo para o ASA.

Neste exemplo, o VPN Client está protegendo o acesso a 10.0.1.0/24 enquanto todo o tráfego restante não é criptografado e não é enviado pelo túnel.



Exibir o registro do cliente VPN

Ao examinar o log do VPN Client, você pode determinar se o parâmetro que especifica o tunelamento dividido está ou não definido. Para visualizar o registro, vá para a guia Log no VPN Client. Em seguida, clique em **Log Settings** para ajustar o que está 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/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.
```

Teste o acesso à LAN local com ping

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. A LAN local do VPN Client é 192.168.0.0/24 e outro host está presente na rede com um endereço IP 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
```

Troubleshooting

Limitação com número de entradas em uma ACL de túnel dividido

Há uma restrição com o número de entradas em uma ACL usada para o túnel dividido. Recomenda-se não usar mais de 50 a 60 entradas ACE para uma funcionalidade satisfatória. Você é recomendado implementar o recurso de sub-rede para cobrir um intervalo de endereços IP.

Informações Relacionadas

- **PIX/ASA 7.x como servidor VPN remoto, usando o exemplo de configuração do ASDM**
- **Dispositivos de segurança adaptáveis Cisco ASA 5500 Series**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.