ASA/PIX：在 ASA 上允许 VPN Client 使用分割隧道的配置示例

目录

简介

本文档提供在 VPN 客户端通过隧道连接到 Cisco 自适应安全设备 (ASA) 5500 系列安全设备时如何允许 VPN 客户端访问 Internet 的分步说明。此配置允许 VPN 客户端在无法安全访问 Internet 时通过 IPsec 安全地访问公司资源。

注意： 因为不启用对互联网和公司LAN的同时设备访问全双工隧道认为多数安全的配置。在全双工隧道和分割隧道之间的一妥协允许VPN客户端仅本地LAN访问。请参阅 PIX/ASA 7.x：允许 VPN 客户端访问本地 LAN 的配置示例。

先决条件

要求

本文档假定 ASA 上已存在有效的远程访问 VPN 配置。如果尚未配置此配置，请参阅使用 ASDM

将 PIX/ASA 7.x 配置为远程 VPN 服务器的配置示例。

使用的组件

本文档中的信息基于以下软件和硬件版本：

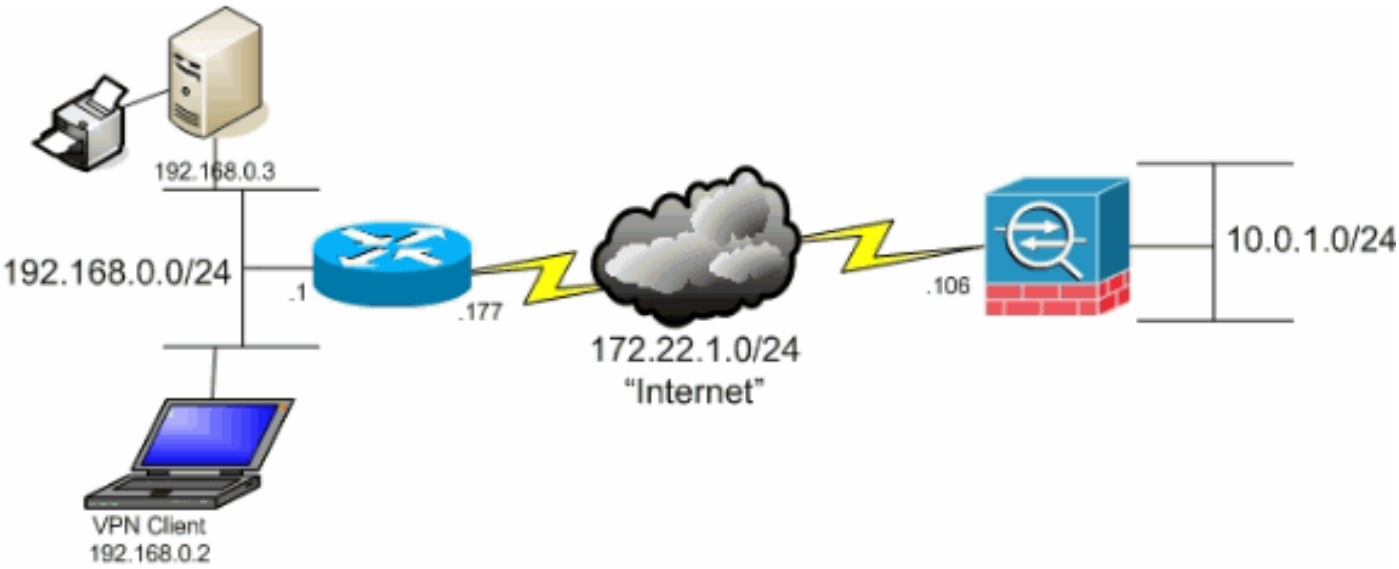
- Cisco ASA 5500 系列安全设备软件版本 7.x 及更高版本
- Cisco Systems VPN 客户端 4.0.5 版

注意： 本文档还包含与 Cisco VPN 客户端 3.x 兼容的 PIX 6.x CLI 配置。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

VPN 客户端位于典型的 SOHO 网络中，并通过 Internet 连接到总部。



相关产品

此配置还可用于 Cisco PIX 500 系列安全设备软件版本 7.x。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

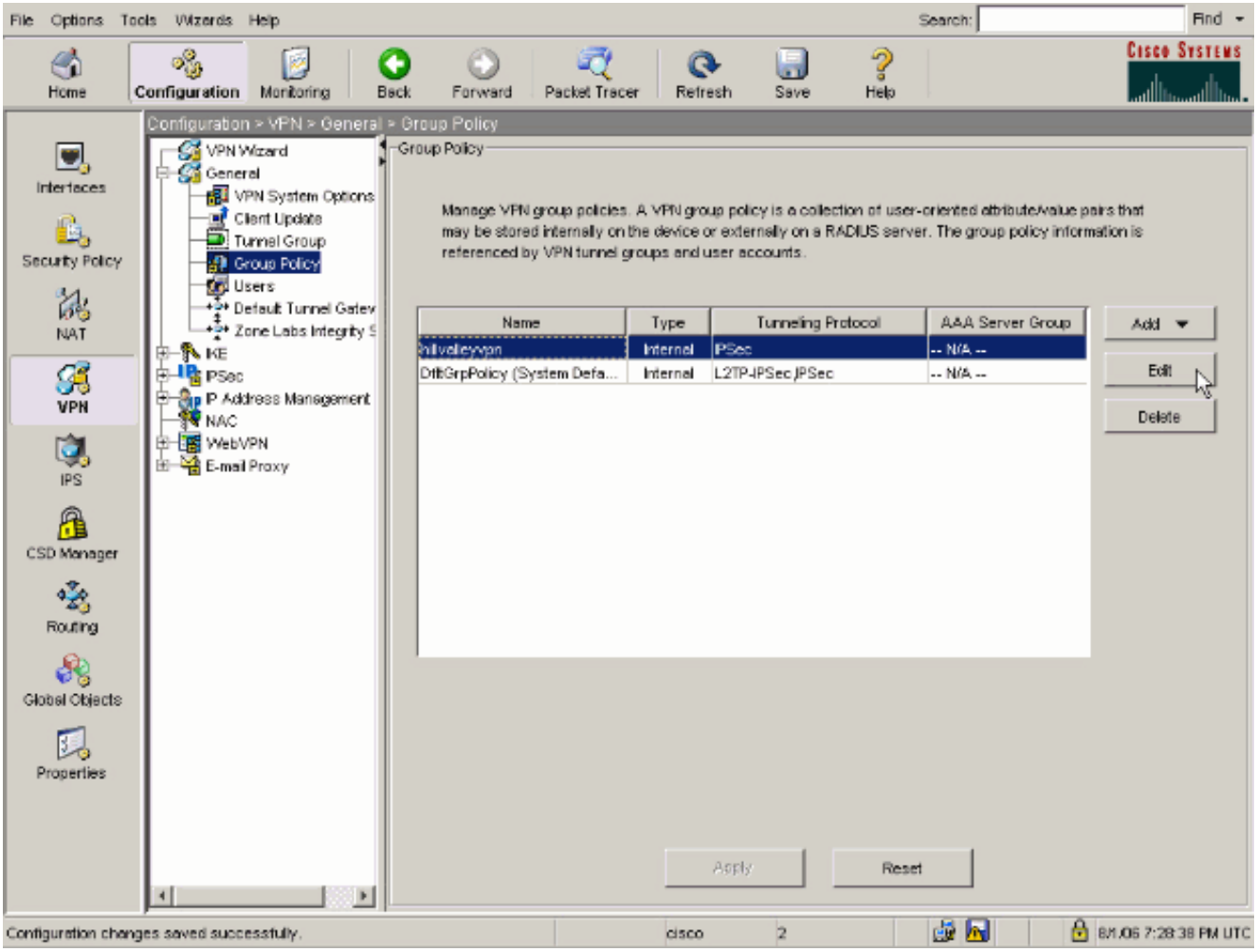
在 VPN 客户端到 ASA 的基本方案中，不管流量目标如何，将对来自 VPN 客户端的所有流量进行加密并将其发送到 ASA。根据您的配置和支持的用户数量，此设置可变为带宽密集型设置。运行分割隧道可以缓解此问题，这是因为它允许用户通过隧道只发送要发送到公司网络的流量。即时消息、电子邮件或临时浏览等所有其他流量将通过 VPN 客户端的本地 LAN 向外发送到 Internet。

在 ASA 上配置分割隧道

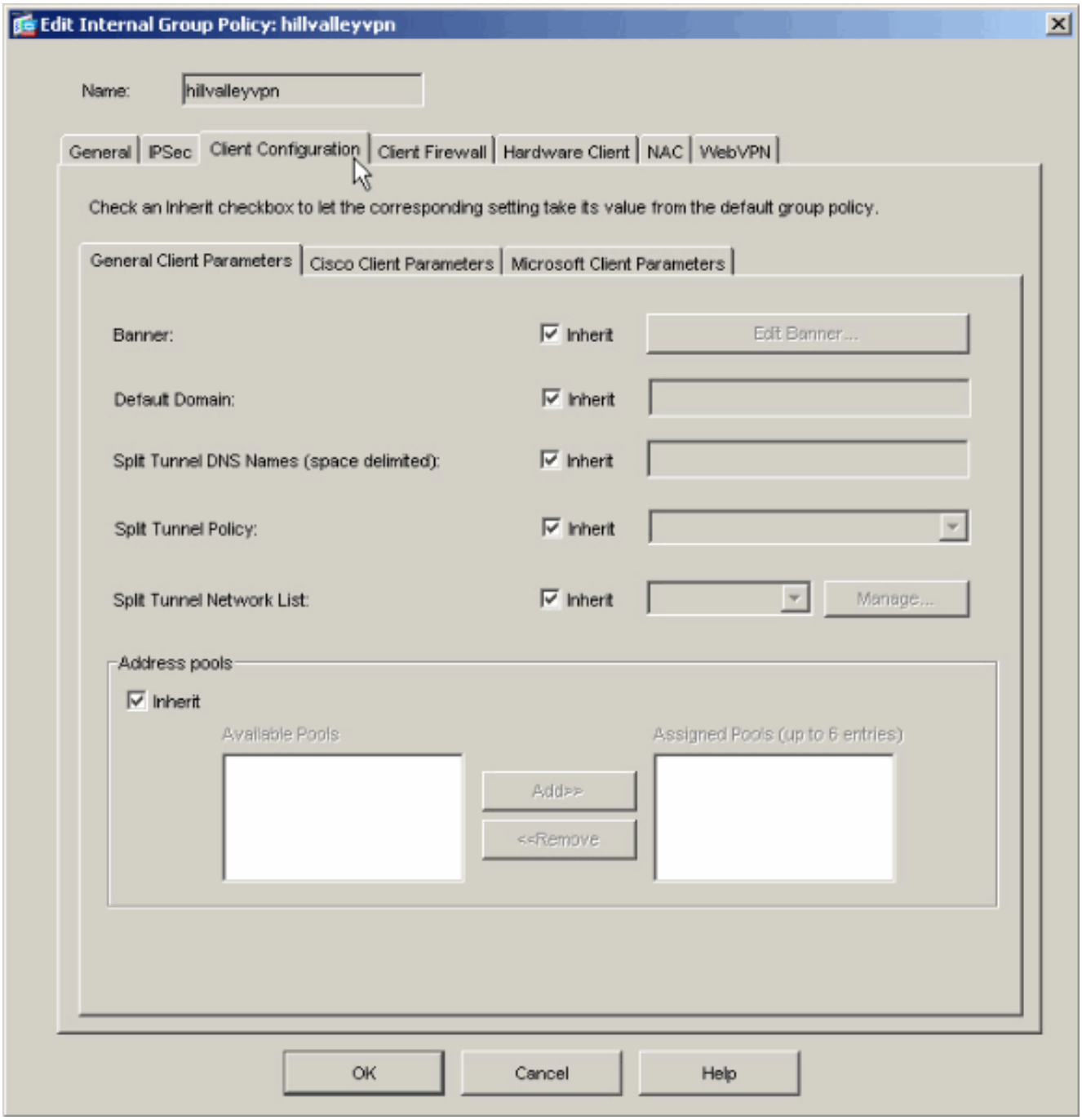
使用自适应安全设备管理器 (ASDM) 5.x 配置 ASA 7.x

完成以下步骤以便将隧道组配置为允许该组中的用户使用分割隧道。

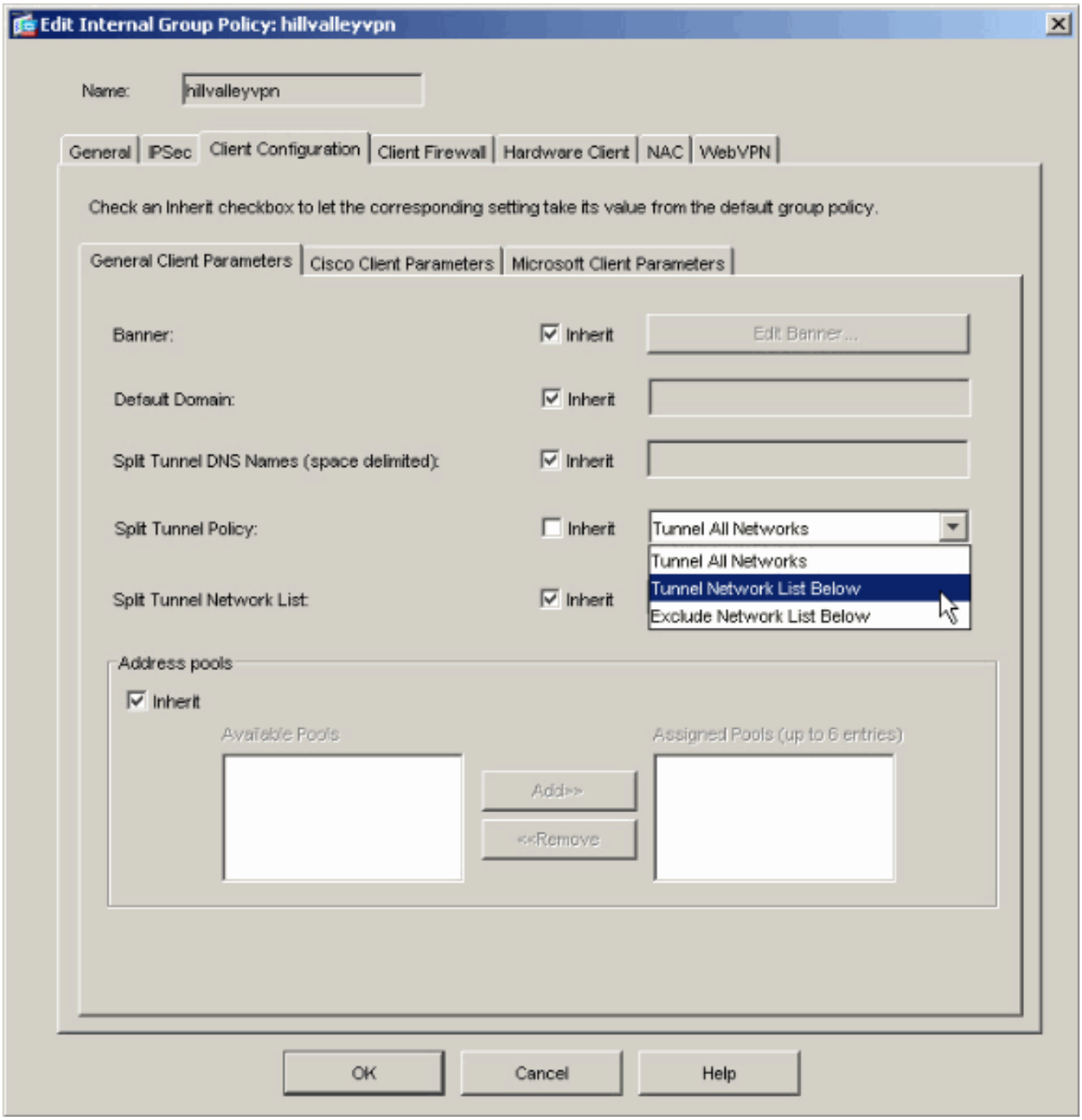
1. 依次选择 **Configuration > VPN > General > Group Policy**，并选择您希望在其中启用本地 LAN 访问的组策略。然后单击 **Edit**。



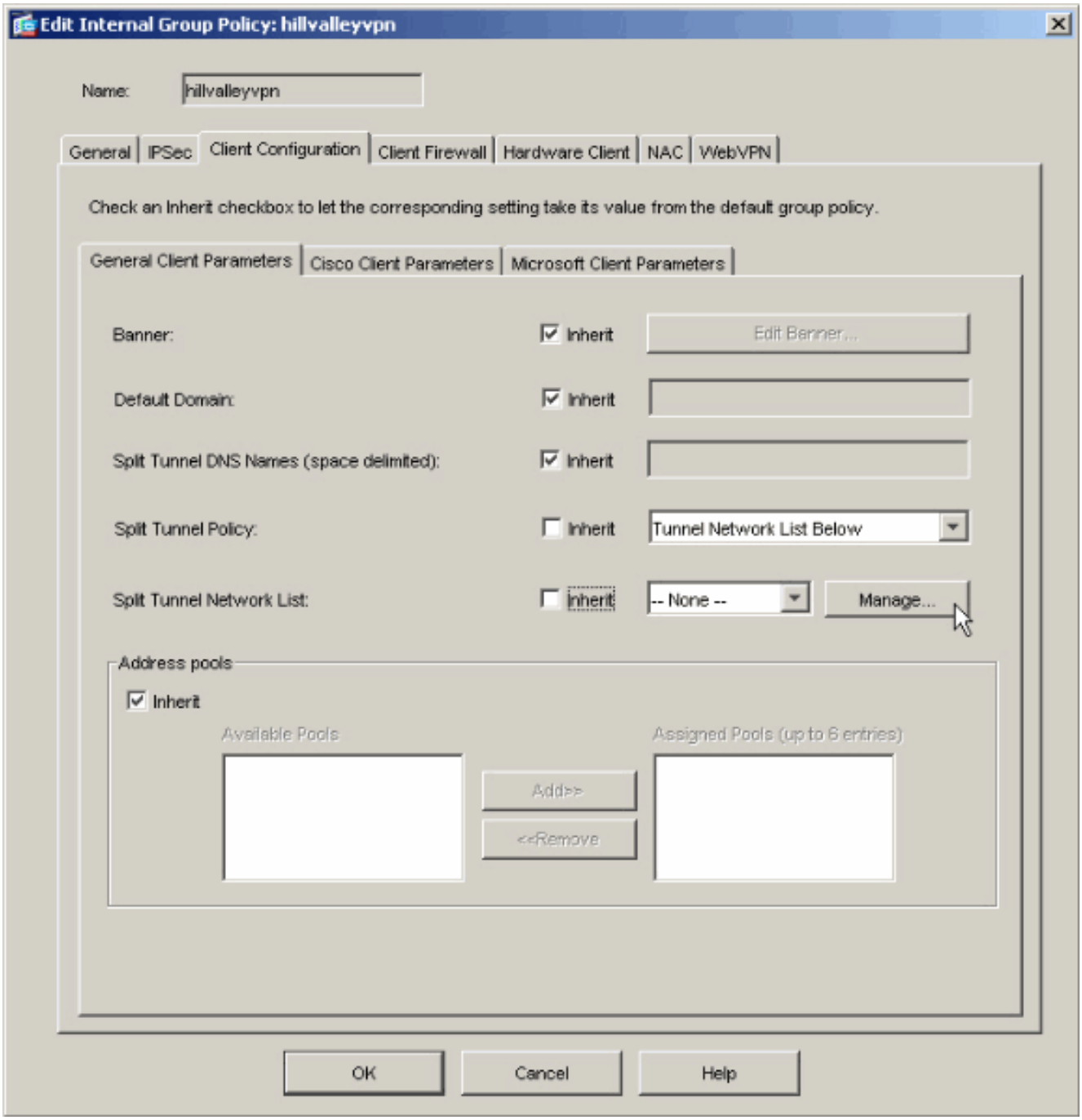
2. 转至 Client Configuration 选项卡。



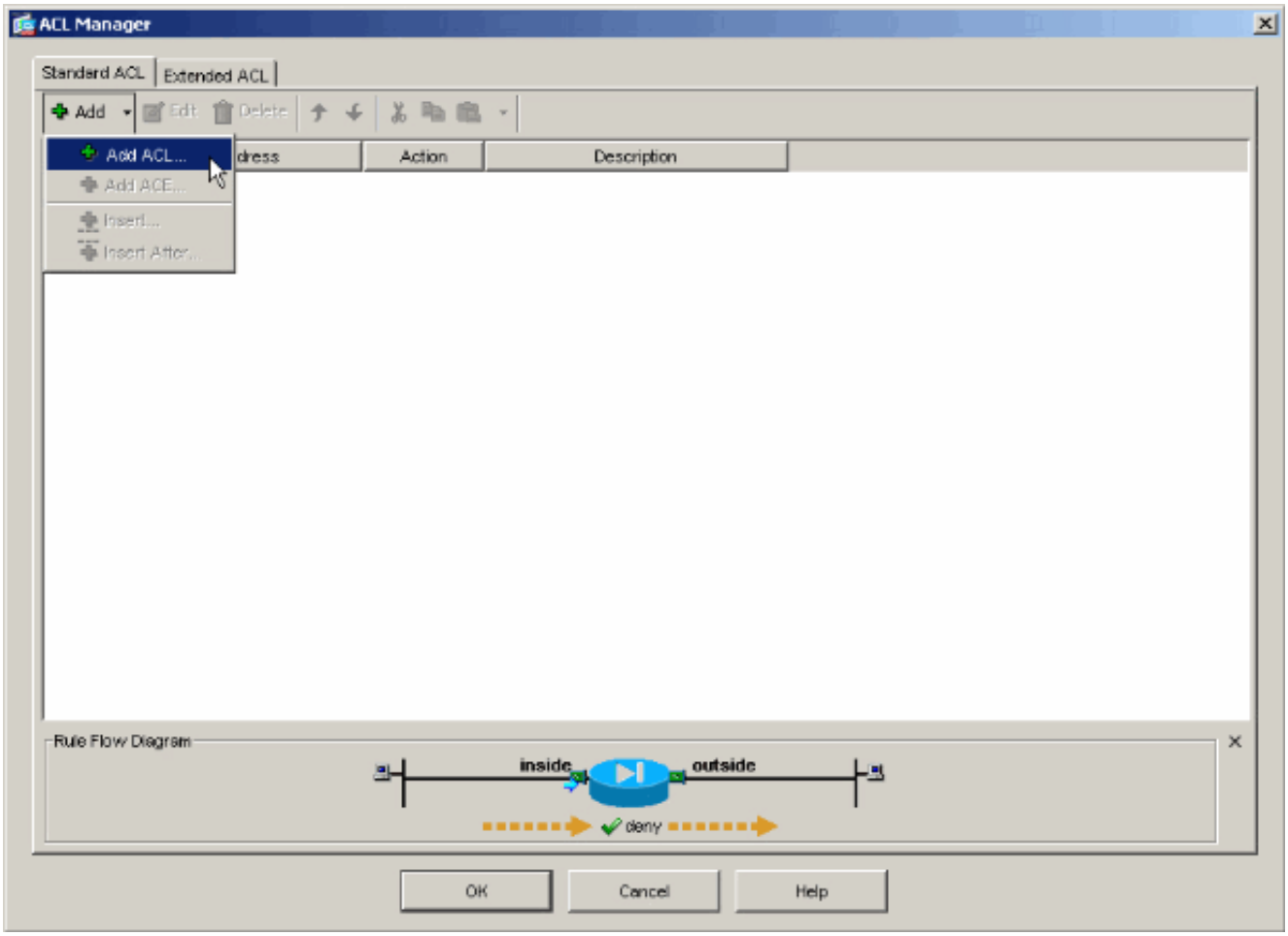
3. 取消选中 Split Tunnel Policy 所对应的 **Inherit** 框，然后选择 Tunnel Network List Below。



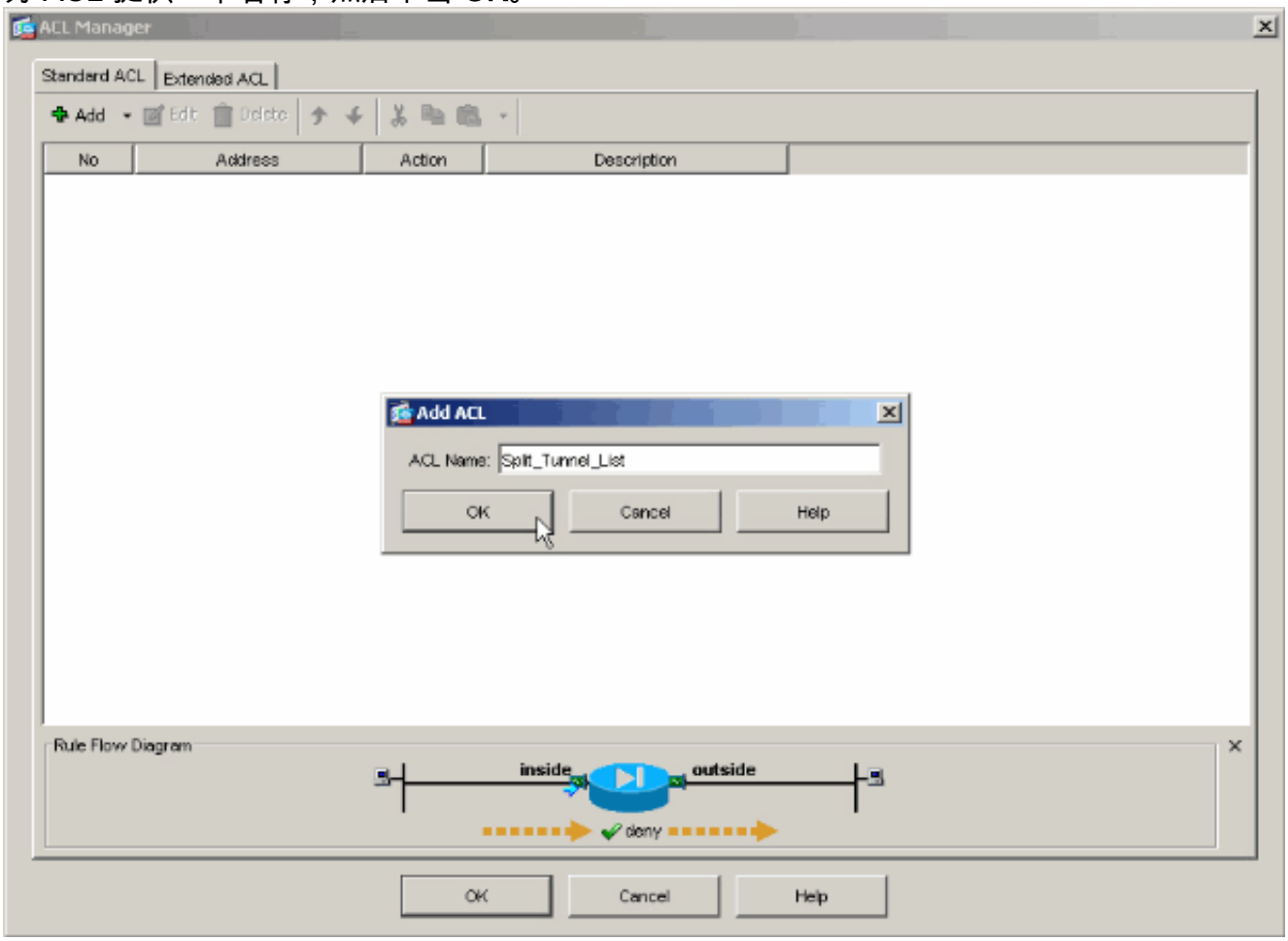
4. 取消选中 Split Tunnel Network List 所对应的 **Inherit** 框，然后单击 Manage 启动 ACL Manager。



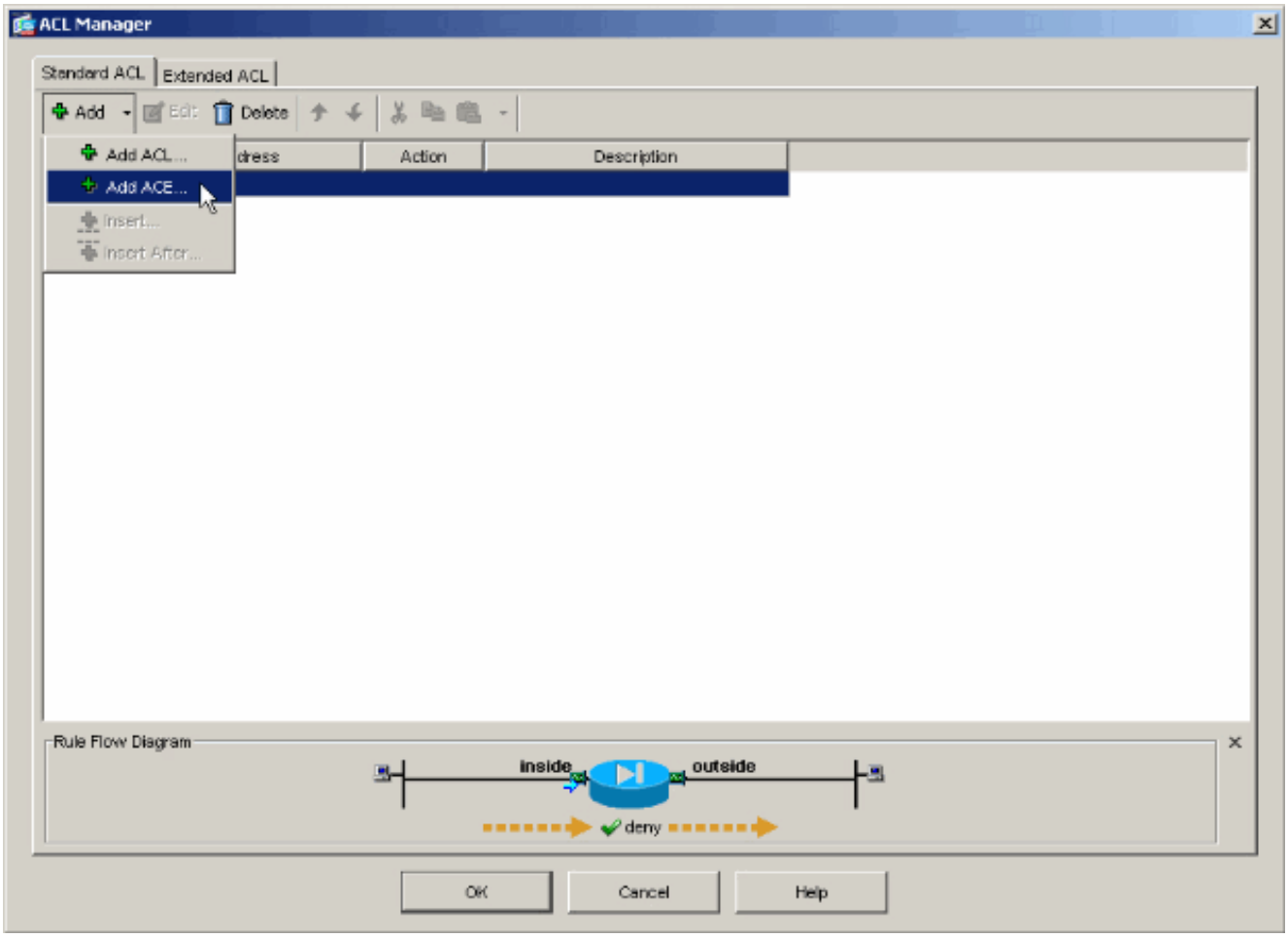
5. 在 ACL Manager 中，选择 **Add > Add ACL...** 以创建新的访问列表。



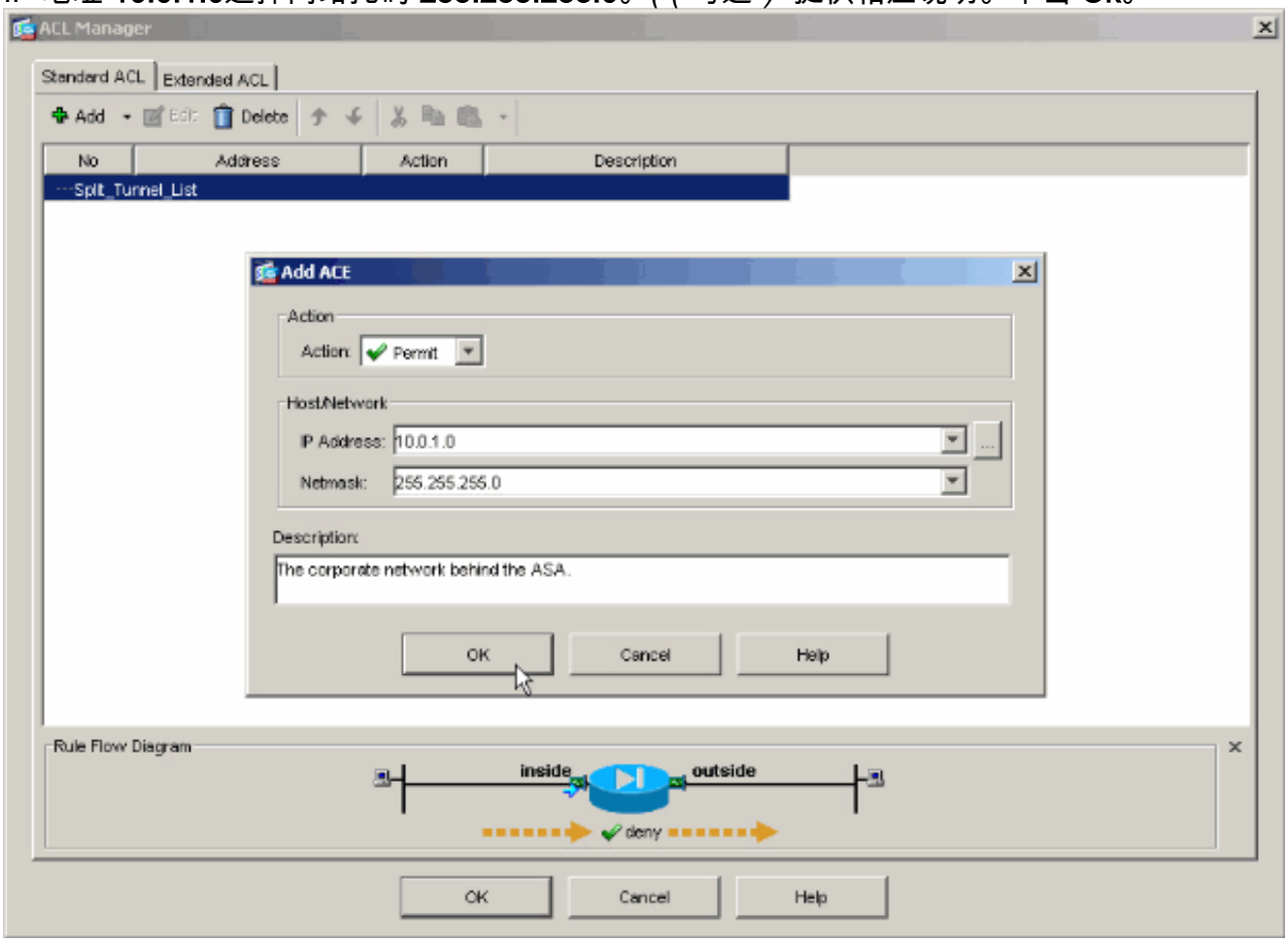
6. 为 ACL 提供一个名称，然后单击 **OK**。



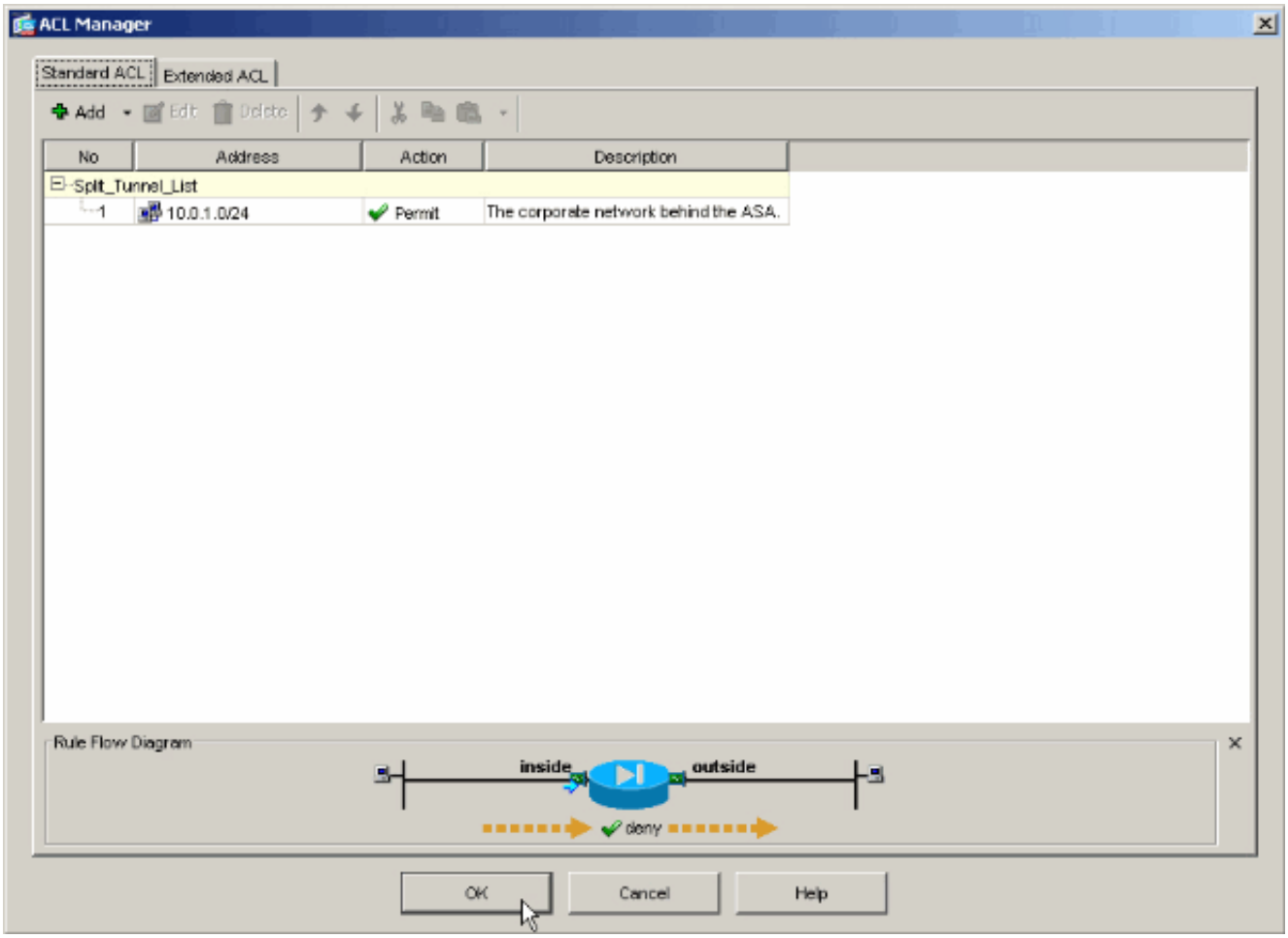
7. 创建 ACL 之后，依次选择 **Add > Add ACE...** 以添加访问控制条目 (ACE)。



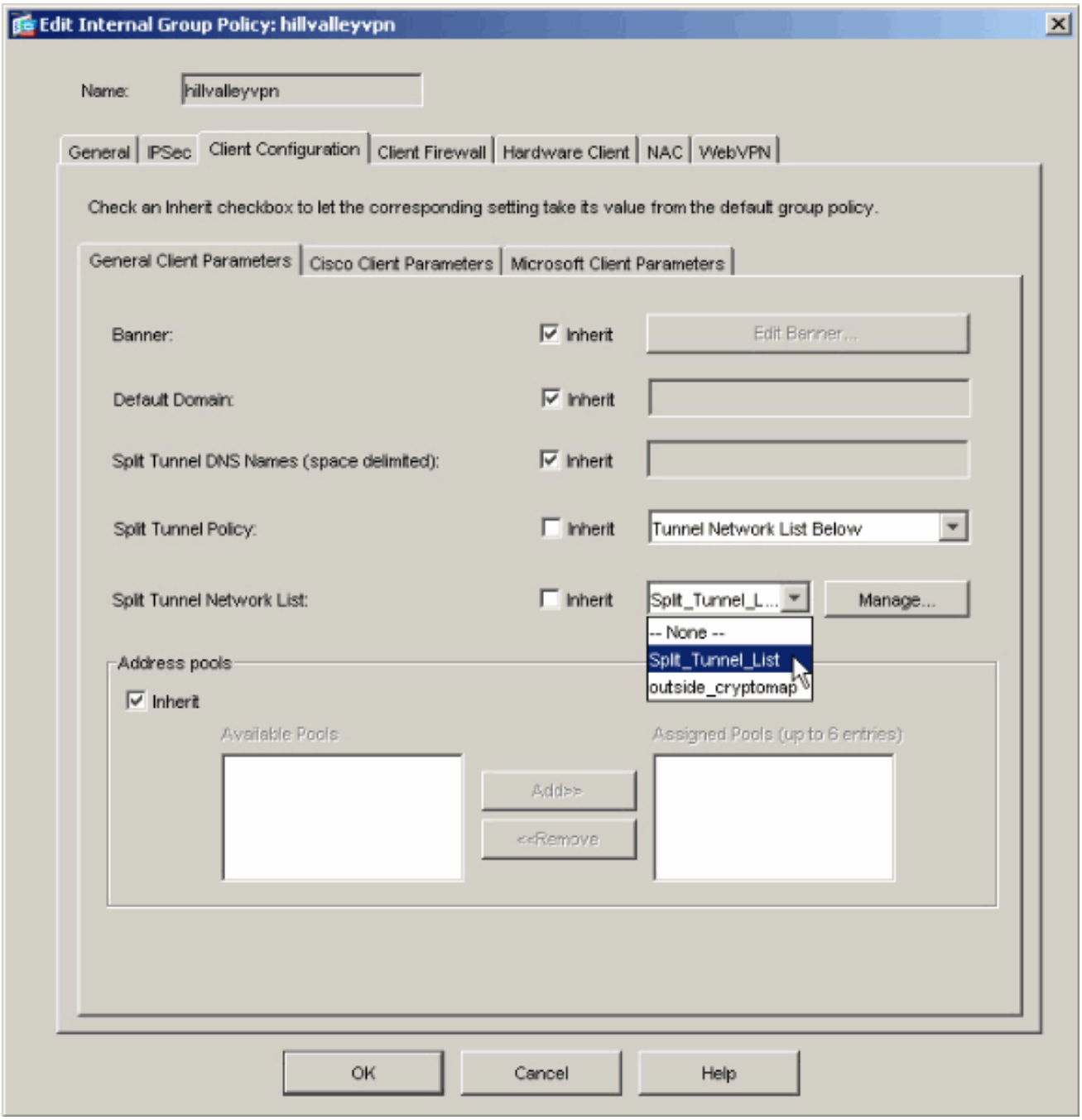
8. 定义与 ASA 后的 LAN 对应的 ACE。在本示例中，该网络为 10.0.1.0/24。选择 **Permit**。选择 IP 地址 **10.0.1.0**选择网络掩码 **255.255.255.0**。*（可选）*提供相应说明。单击 **Ok**。



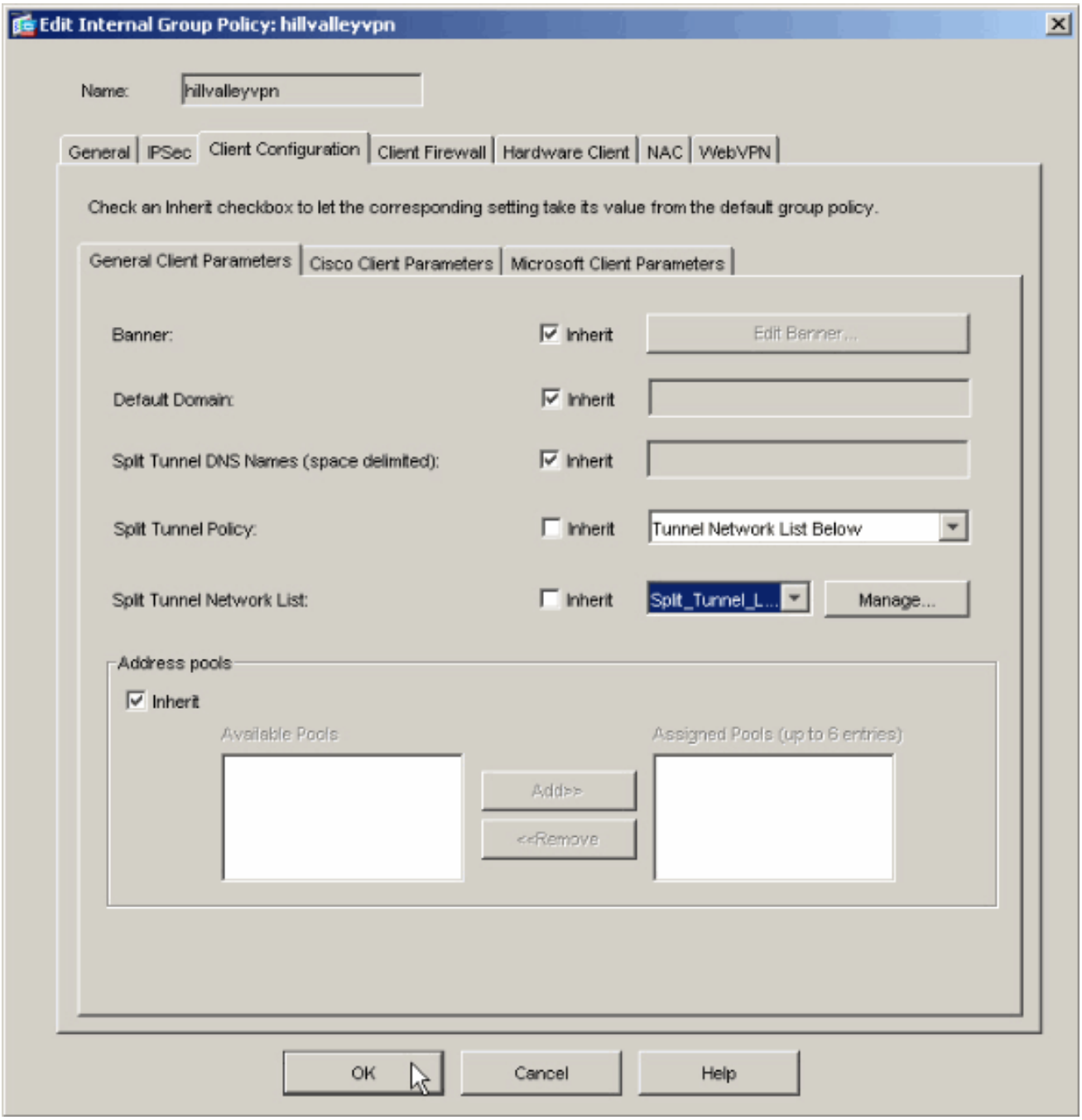
9. 单击 **OK** 以退出 ACL Manager。



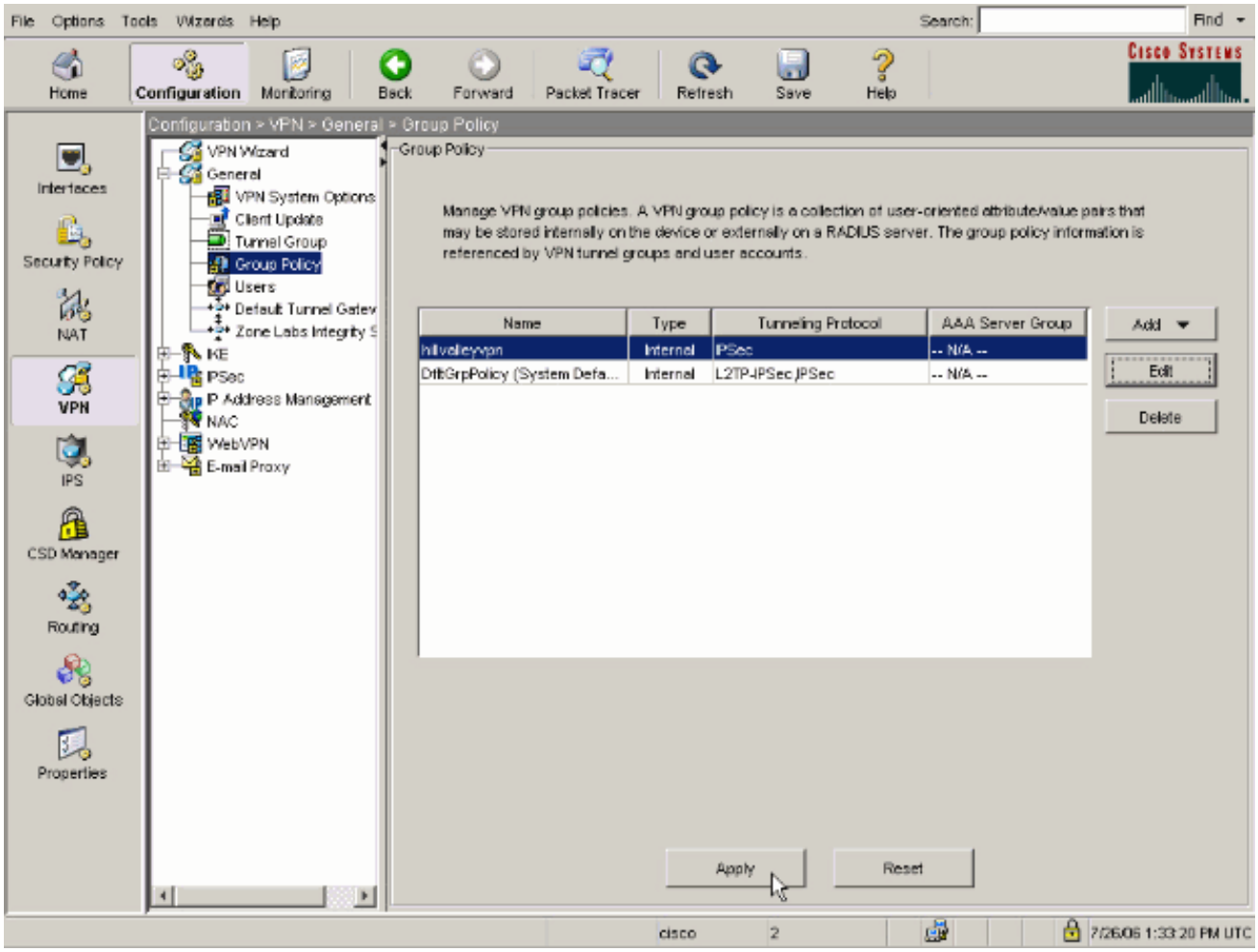
10. 确保在 Split Tunnel Network List 中选择刚刚创建的 ACL。



11. 单击 **OK** 以返回组策略配置。



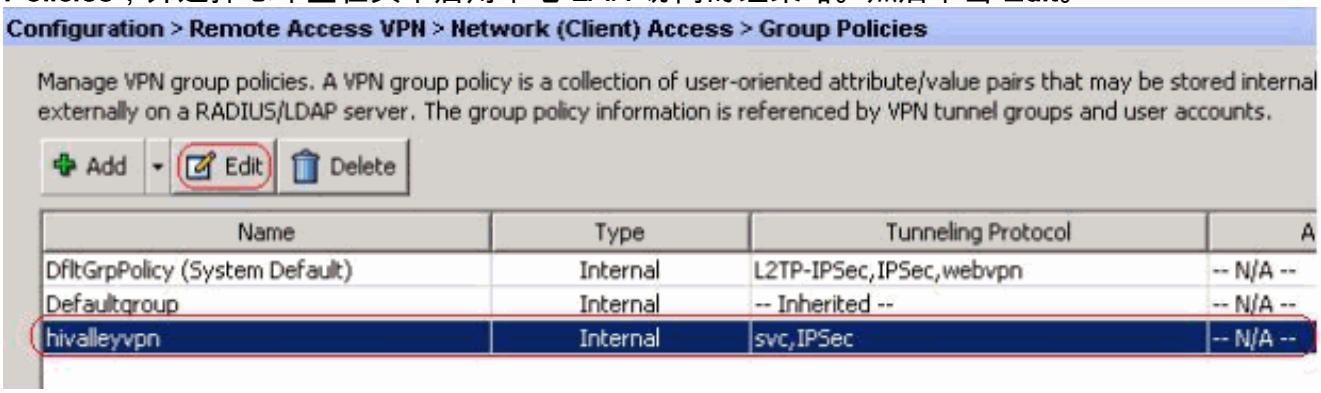
12. 单击 **Apply**，然后单击 Send（如果需要），以将命令发送到 ASA。



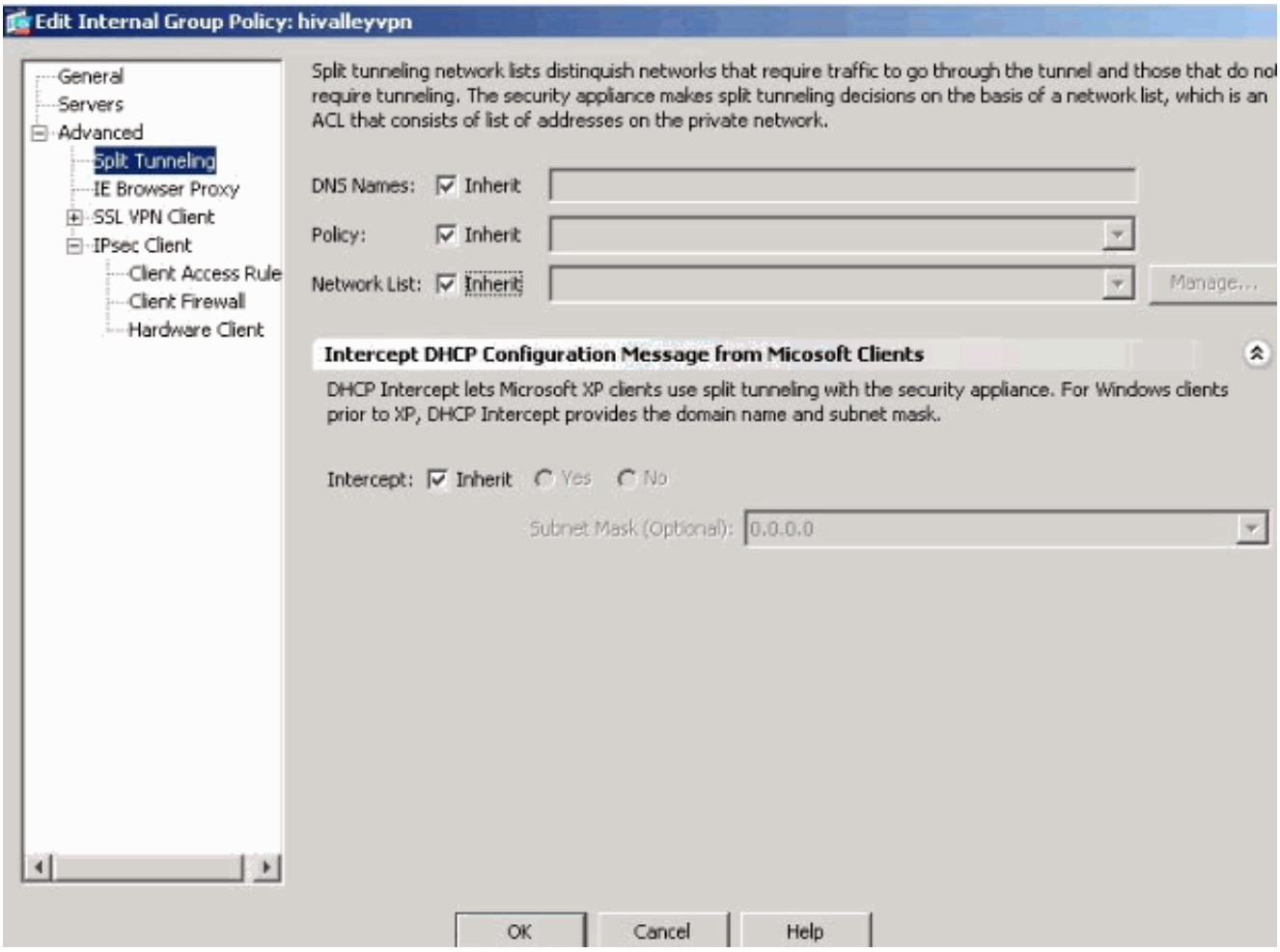
使用自适应安全设备管理器 (ASDM) 6.x 配置 ASA 8.x

完成以下步骤以便将隧道组配置为允许该组中的用户使用分割隧道。

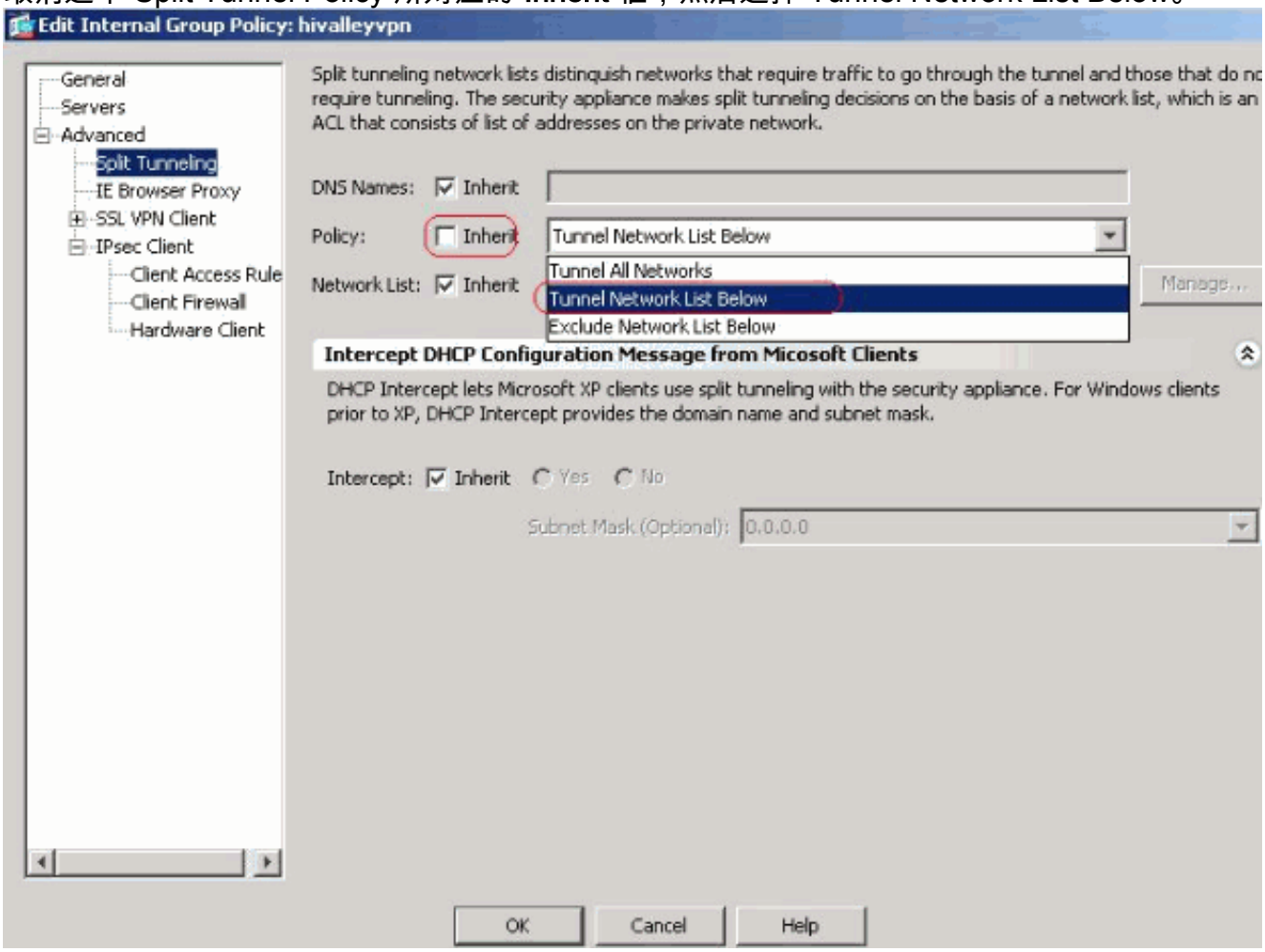
1. 依次选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**，并选择您希望在其中启用本地 LAN 访问的组策略。然后单击 **Edit**。



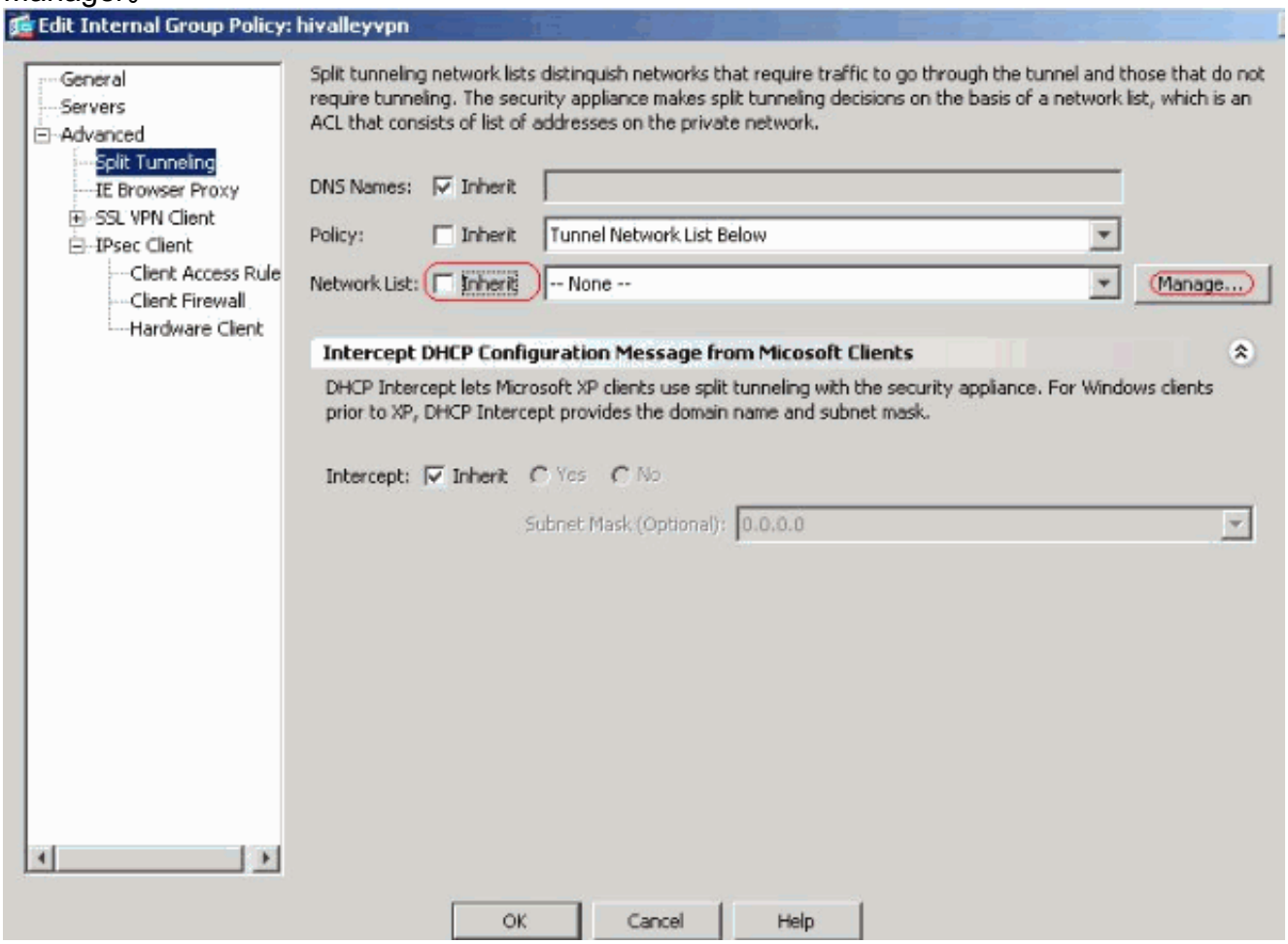
2. 单击 **Split Tunneling**。



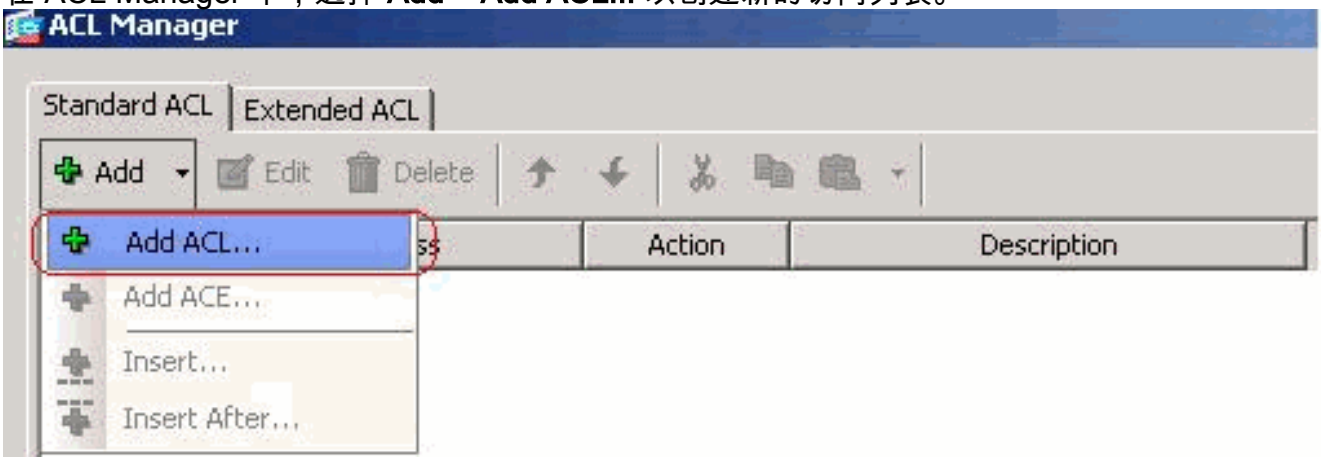
3. 取消选中 Split Tunnel Policy 所对应的 **Inherit** 框，然后选择 Tunnel Network List Below。



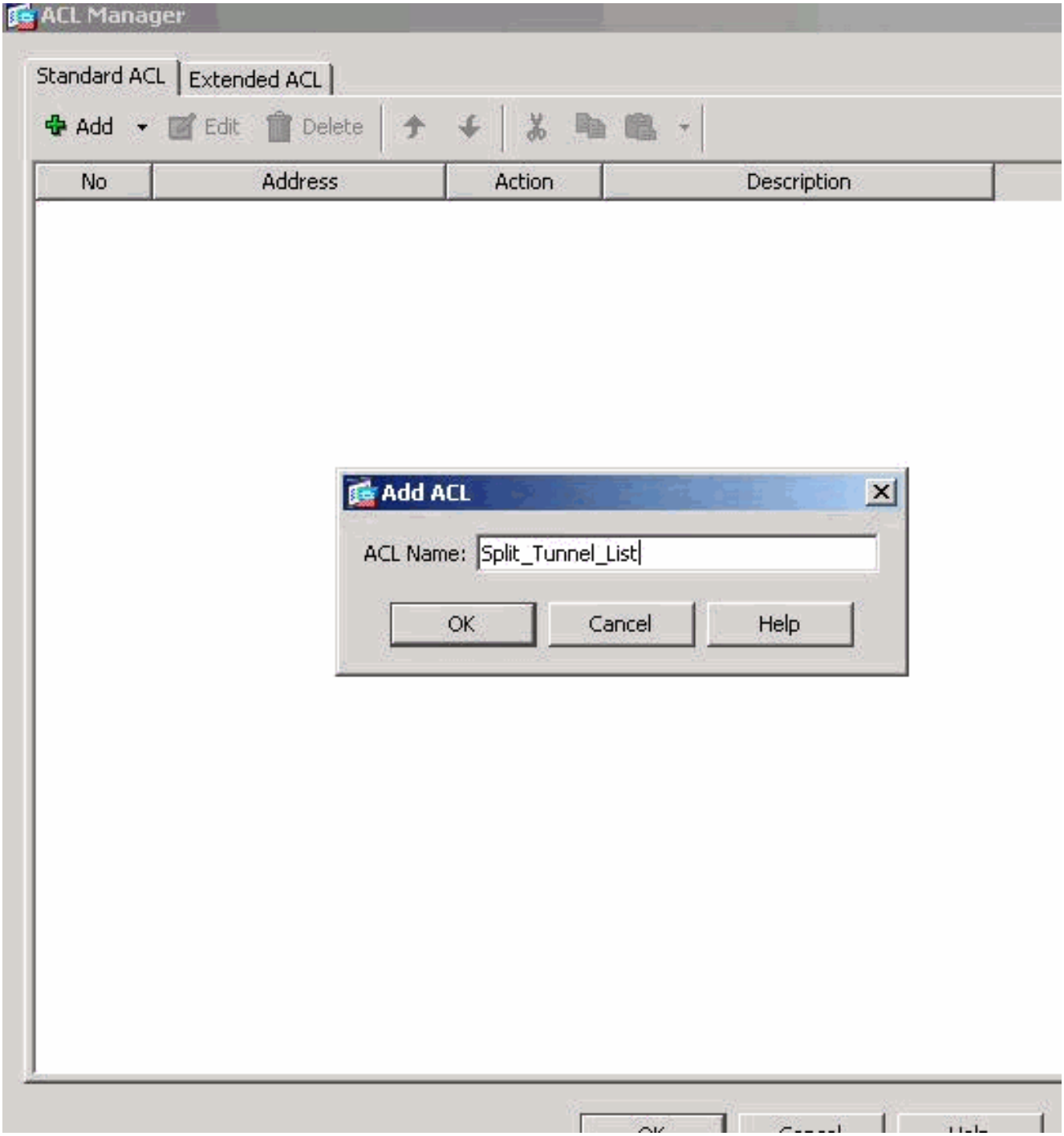
4. 取消选中 Split Tunnel Network List 所对应的 **Inherit** 框，然后单击 Manage 启动 ACL Manager。



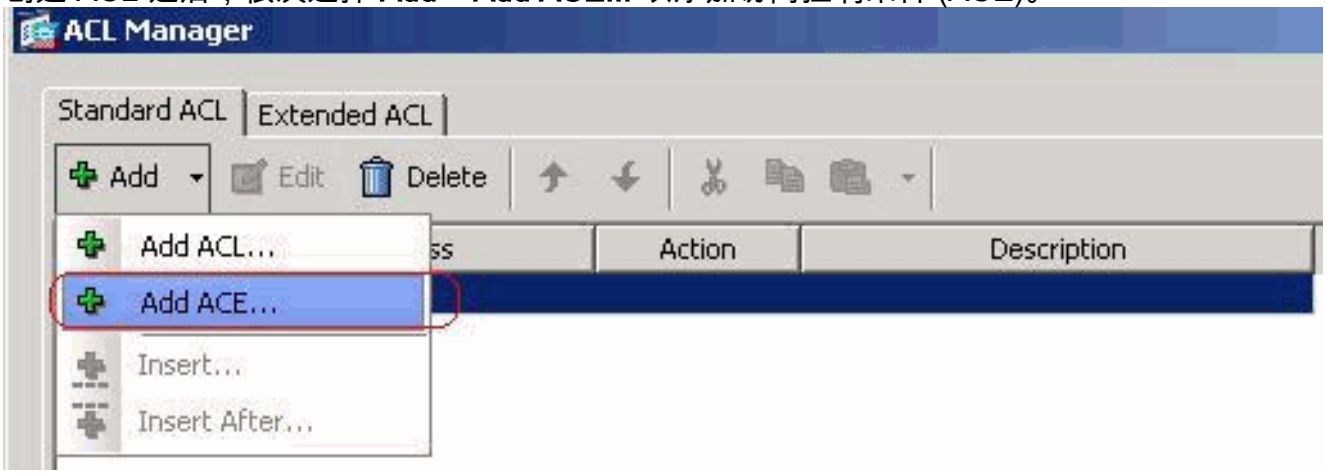
5. 在 ACL Manager 中，选择 **Add > Add ACL...** 以创建新的访问列表。



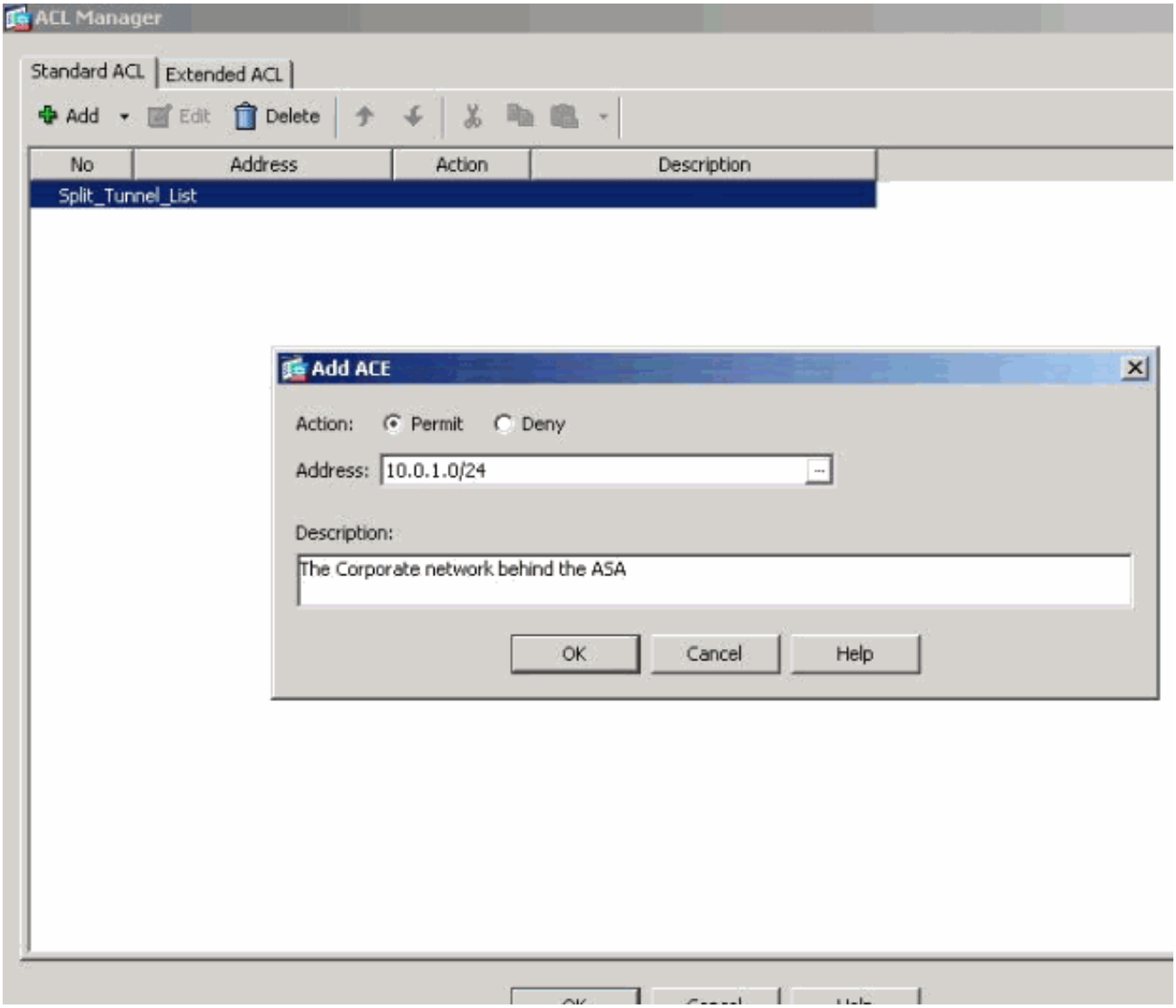
6. 为此 ACL 提供一个名称，然后单击 **OK**。



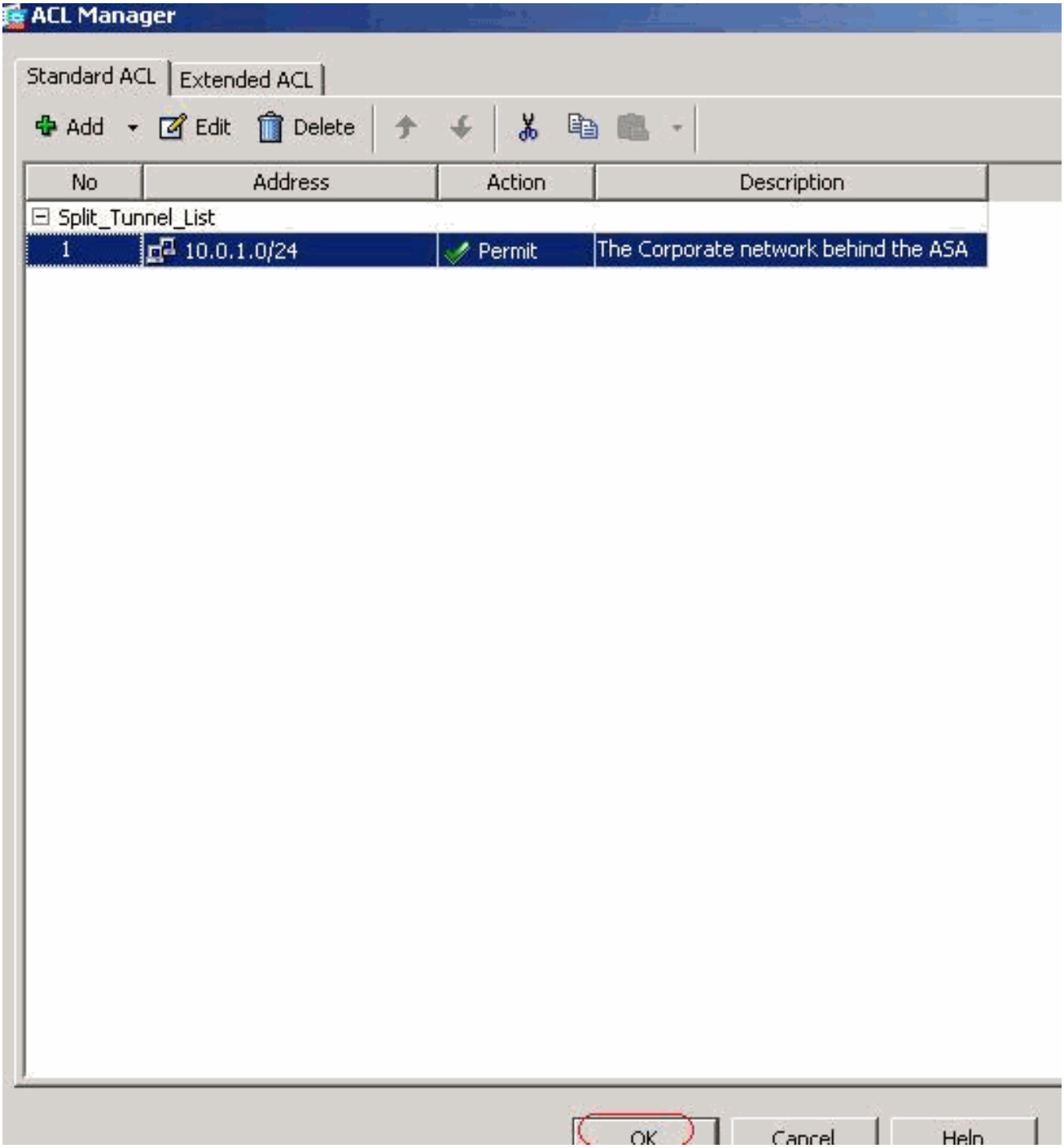
7. 创建 ACL 之后，依次选择 **Add > Add ACE...** 以添加访问控制条目 (ACE)。



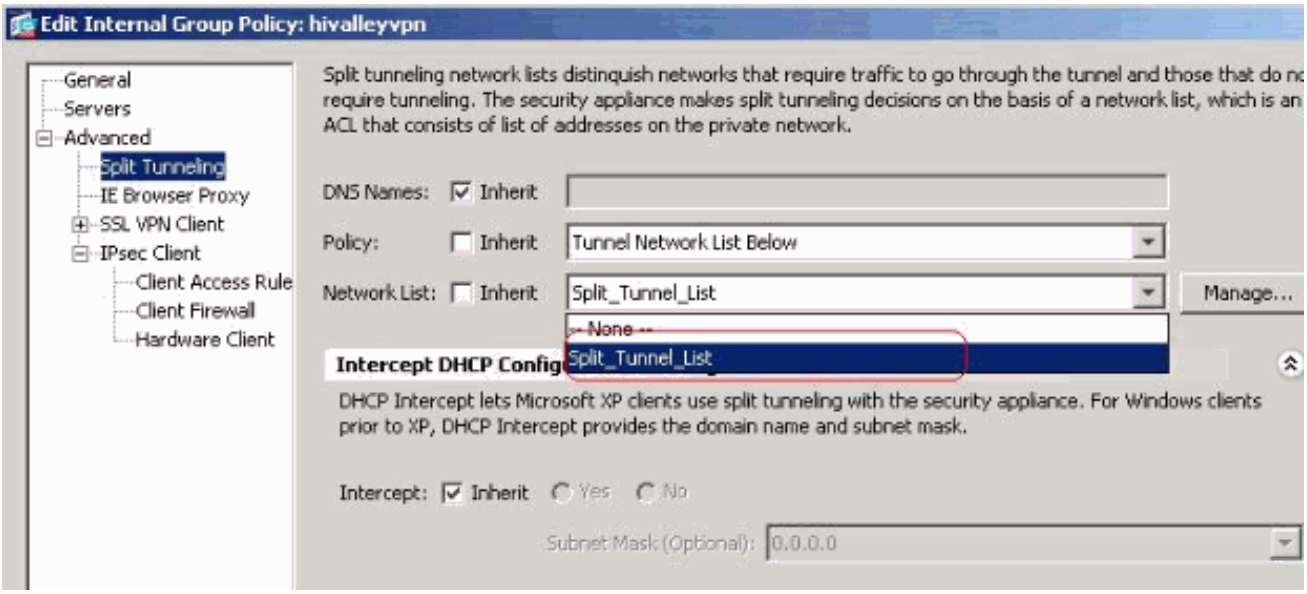
8. 定义与 ASA 后的 LAN 对应的 ACE。在本示例中，该网络为 10.0.1.0/24。单击 **Permit** 单选按钮。选择掩码为 **10.0.1.0/24** 的网络地址。*（可选）*提供相应说明。单击 **Ok**。



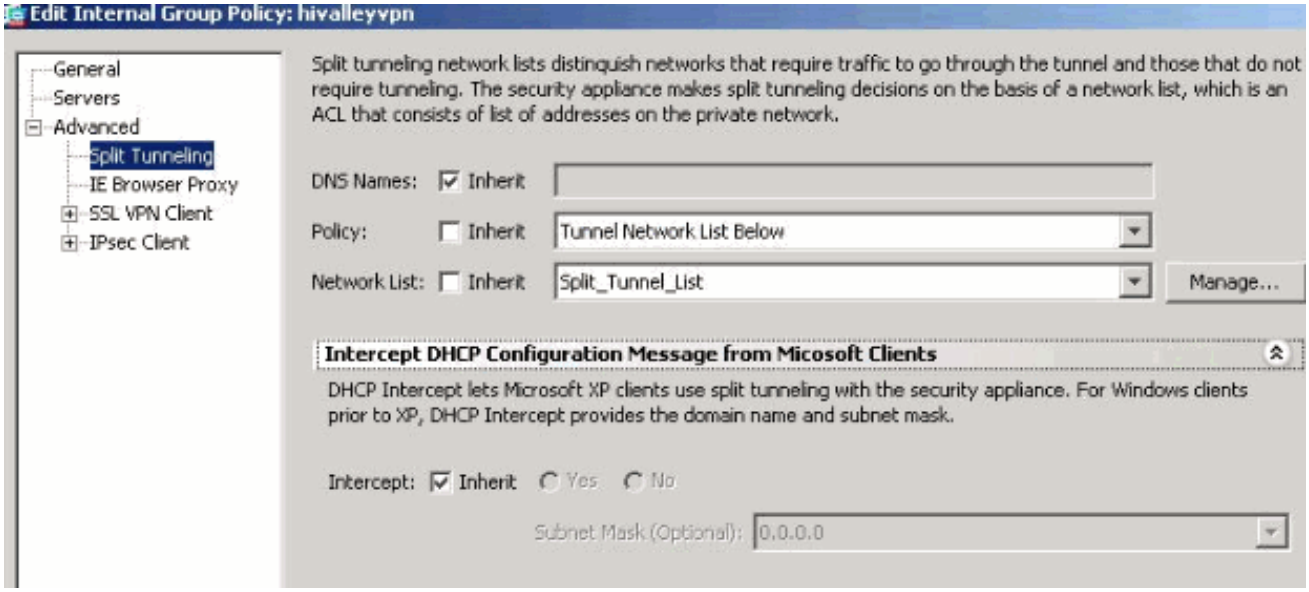
9. 单击 **OK** 以退出 ACL Manager。



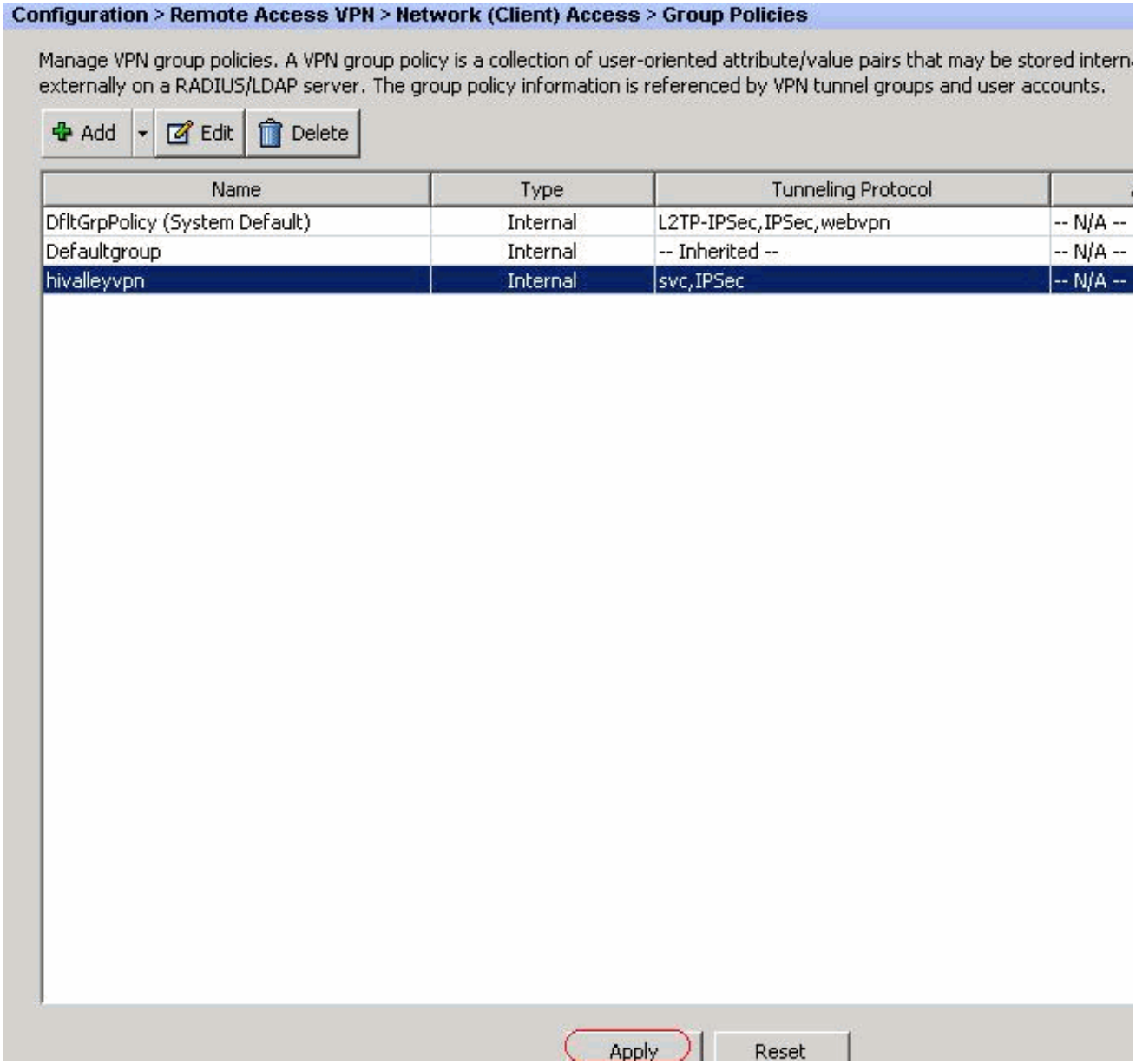
10. 确保在 Split Tunnel Network List 中选择刚刚创建的 ACL。



11. 单击 **OK** 以返回组策略配置。



12. 单击 **Apply**，然后单击 Send（如果需要），以将命令发送到 ASA。



通过 CLI 配置 ASA 7.x 及更高版本

您可以在 ASA CLI 中完成以下步骤（而不是使用 ASDM），以便允许在 ASA 上使用分割隧道：

注意： 在 ASA 7.x 和 8.x 中，CLI 分割隧道配置都是相同的。

1. 进入配置模式。`ciscoasa>`**`enable`** `Password: ********* ciscoasa#`**`configure terminal`** `ciscoasa(config)#`
2. 创建定义 ASA 后台网络的访问列表。`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. 进入您希望对其进行修改的策略的组策略配置模式。`ciscoasa(config)#`**`group-policy hillvalleyvpn attributes`** `ciscoasa(config-group-policy)#`
4. 指定分割隧道策略。在本示例中，此策略为 **tunnelspecified**。`ciscoasa(config-group-policy)#`**`split-tunnel-policy tunnelspecified`**
5. 指定分割隧道访问列表。在本示例中，此列表为 **Split_Tunnel_List**。`ciscoasa(config-group-policy)#`**`split-tunnel-network-list value Split_Tunnel_List`**
6. 发出以下命令：`ciscoasa(config)#`**`tunnel-group hillvalleyvpn general-attributes`**
7. 将组策略与隧道组关联`ciscoasa(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
8. 退出上述两种配置模式。`ciscoasa(config-group-policy)#`**`exit`** `ciscoasa(config)#`**`exit`** `ciscoasa#`

9. 将配置保存到非易失性 RAM (NVRAM)，并在系统提示指定源文件名时按 **Enter**。
```
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#
```

通过 CLI 配置 PIX 6.x

完成这些步骤：

1. 创建定义 PIX 后台网络的访问列表。
   PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
2. 创建一个 VPN 组 *vpn3000*，并向其指定分割隧道 ACL，如下所示：`PIX(config)#`**vpngroup vpn3000 split-tunnel Split_Tunnel_List** **注意：** 有关适用于 PIX 6.x 的远程访问 VPN 配置的详细信息，请参阅使用 Microsoft Windows 2000 和 2003 IAS RADIUS 身份验证配置适用于 Windows 的 Cisco Secure PIX Firewall 6.x 和 Cisco VPN 客户端 3.5。

验证

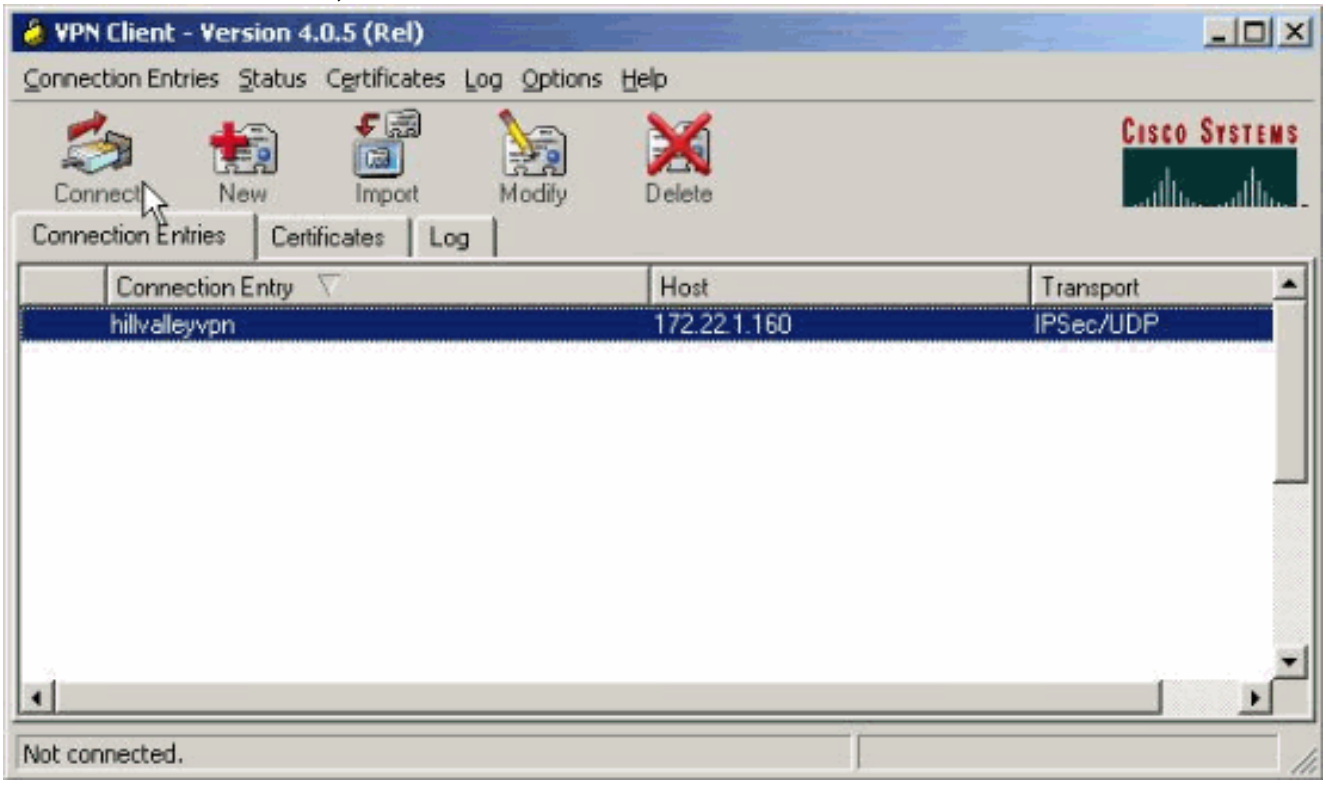
请完成以下部分中的步骤，以便验证配置。

- 连接 VPN 客户端
- 查看 VPN 客户端日志
- 通过 Ping 测试本地 LAN 访问

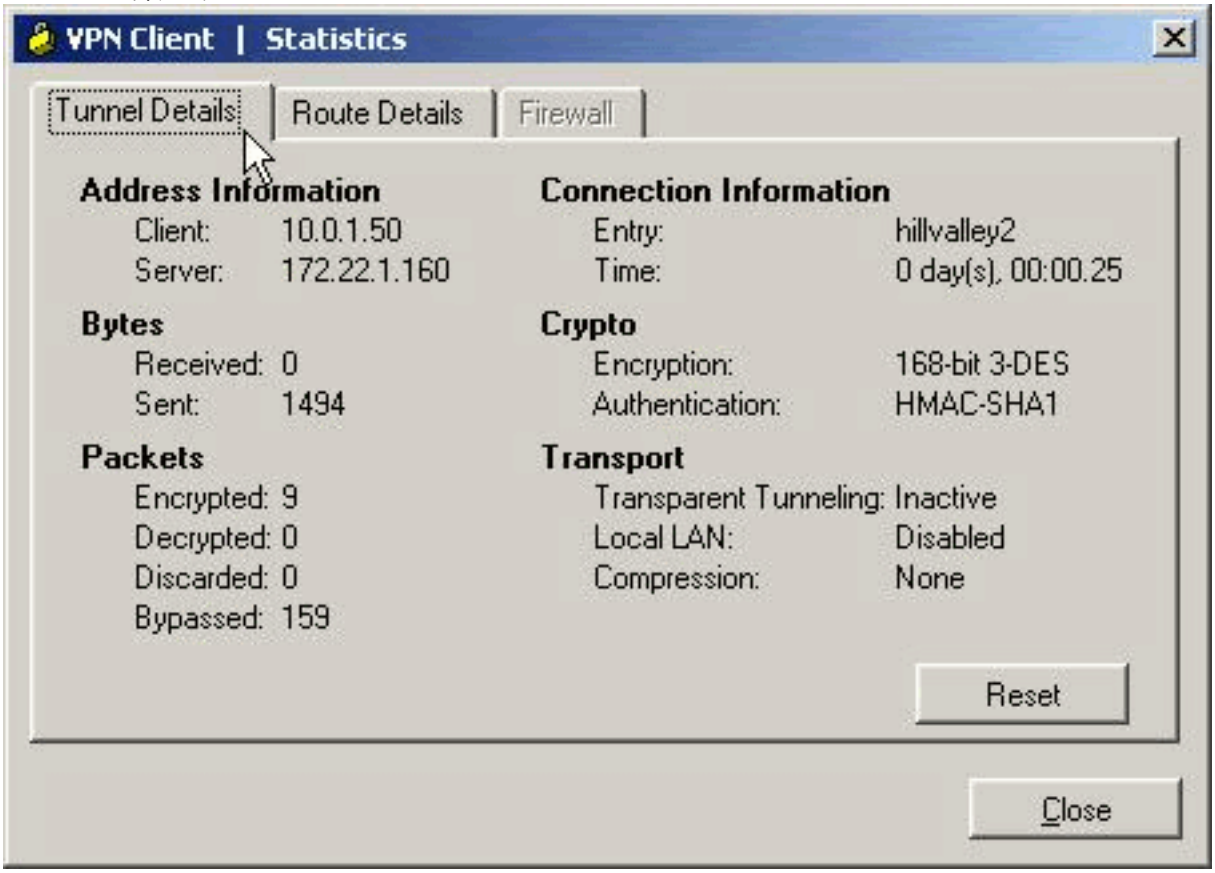
连接 VPN 客户端

将 VPN 客户端连接到 VPN 集中器，以便验证配置。

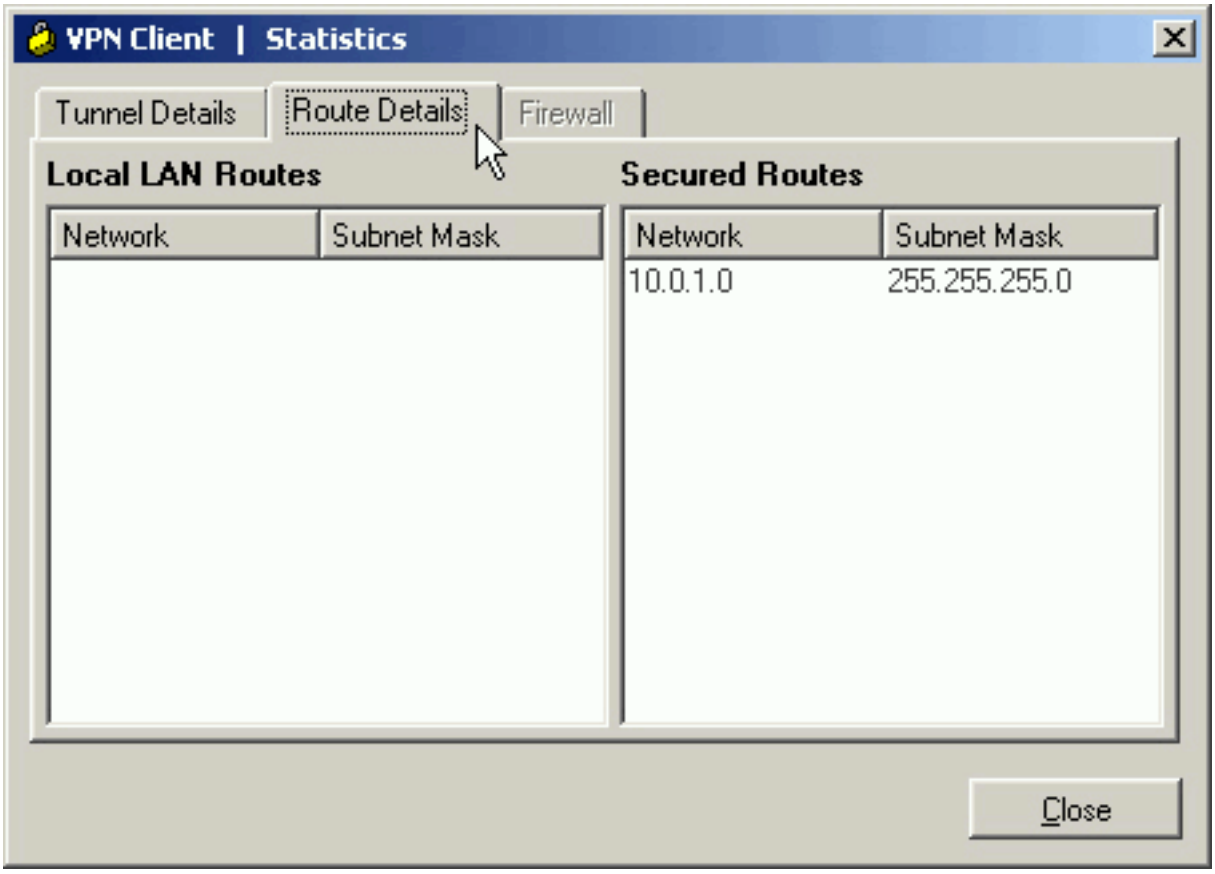
1. 从列表中选择连接条目，并单击 **Connect**。



2. 输入您的凭证。
3. 选择 **Status > Statistics...** 以便显示 Tunnel Details 窗口，您可以在此窗口中检查隧道特定信息并查看数据流。

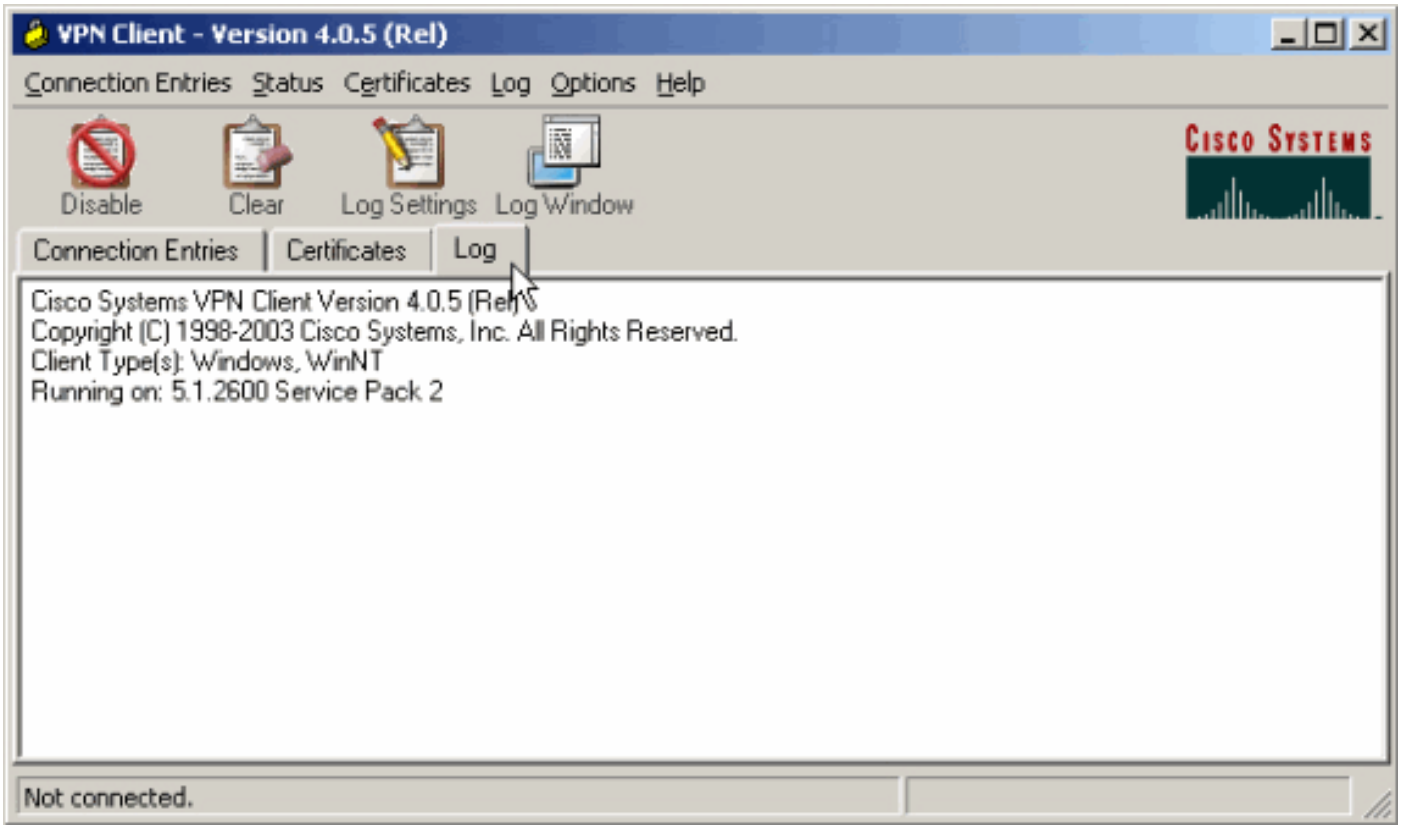


4. 转至 Route Details 选项卡，以便查看 VPN 客户端已安全连接到 ASA 的路由。在本示例中，VPN 客户端可以安全地访问 10.0.1.0/24，而所有其他流量将被加密并通过隧道发送。



查看 VPN 客户端日志

当检查 VPN 客户端日志时，您可以确定是否已设置指定分割隧道的参数。要查看日志，请在 VPN 客户端中转至 Log 选项卡。然后单击 **Log Settings** 以调整所记录的内容。在本示例中，IKE 设置为 **3 - High**，而所有其他日志元素设置为 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.
```

通过 Ping 测试本地 LAN 访问

测试 VPN 客户端在通过隧道连接到 ASA 时是否配置了分割隧道的另一种方法是：在 Windows 命令行中使用 **ping** 命令。VPN 客户端的本地 LAN 为 192.168.0.0/24，并且网络中存在另一台 IP 地址为 192.168.0.3 的主机。

```
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
```

故障排除

以条目的数量限制在分割隧道ACL

有一限制用条目数量在用于分割隧道的ACL的。推荐不使用超过50-60个ACE条目令人满意的功能。您建议实现子网划分功能覆盖IP地址范围。

相关信息

- 使用 ASDM 将 PIX/ASA 7.x 配置为远程 VPN 服务器的配置示例
- Cisco ASA 5500 系列自适应安全设备
- 技术支持和文档 - Cisco Systems