ASA/PIX:允許在ASA上為VPN客戶端分割隧道的配置示例

目錄

簡介

本文檔提供了有關如何允許VPN客戶端在通過隧道連線到思科自適應安全裝置(ASA)5500系列安全裝置時訪問網際網路的逐步說明。此配置允許VPN客戶端通過IPsec安全地訪問公司資源，同時提供對Internet的不安全訪問。

註：全通道配置被認為是最安全的配置，因為它不支援同時訪問網際網路和公司LAN的裝置。全通道和分割通道之間的危害僅允許VPN客戶端本地LAN存取。請參閱PIX/ASA 7.x:Allow Local LAN Access for VPN Clients配置示例了解詳細資訊。

必要條件

需求

本文檔假定ASA上已存在有效的遠端訪問VPN配置。如果尚未配置PIX/ASA 7.x作為使用ASDM的遠

端VPN伺服器配置示例。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

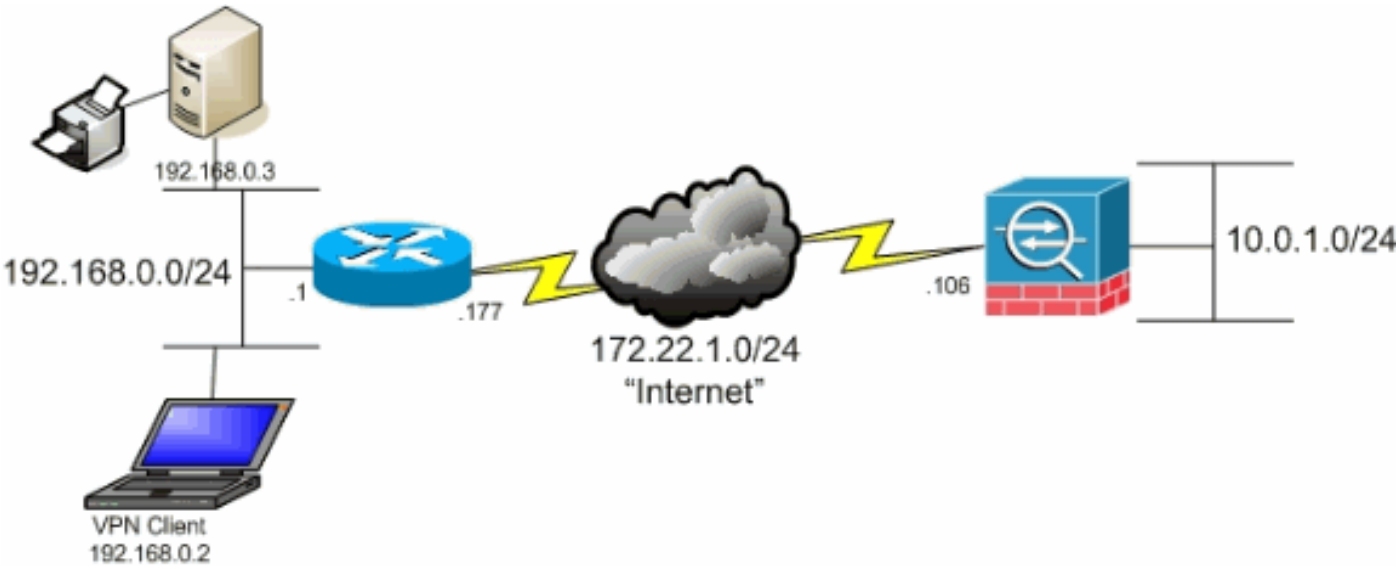
- Cisco ASA 5500系列安全裝置軟體版本7.x及更高版本
- Cisco系統VPN使用者端版本4.0.5

注意：本文檔還包含與Cisco VPN客戶端3.x相容的PIX 6.x CLI配置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

VPN客戶端位於典型的SOHO網路上，通過Internet連線到總部。



相關產品

此配置還可以與Cisco PIX 500系列安全裝置軟體版本7.x一起使用。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

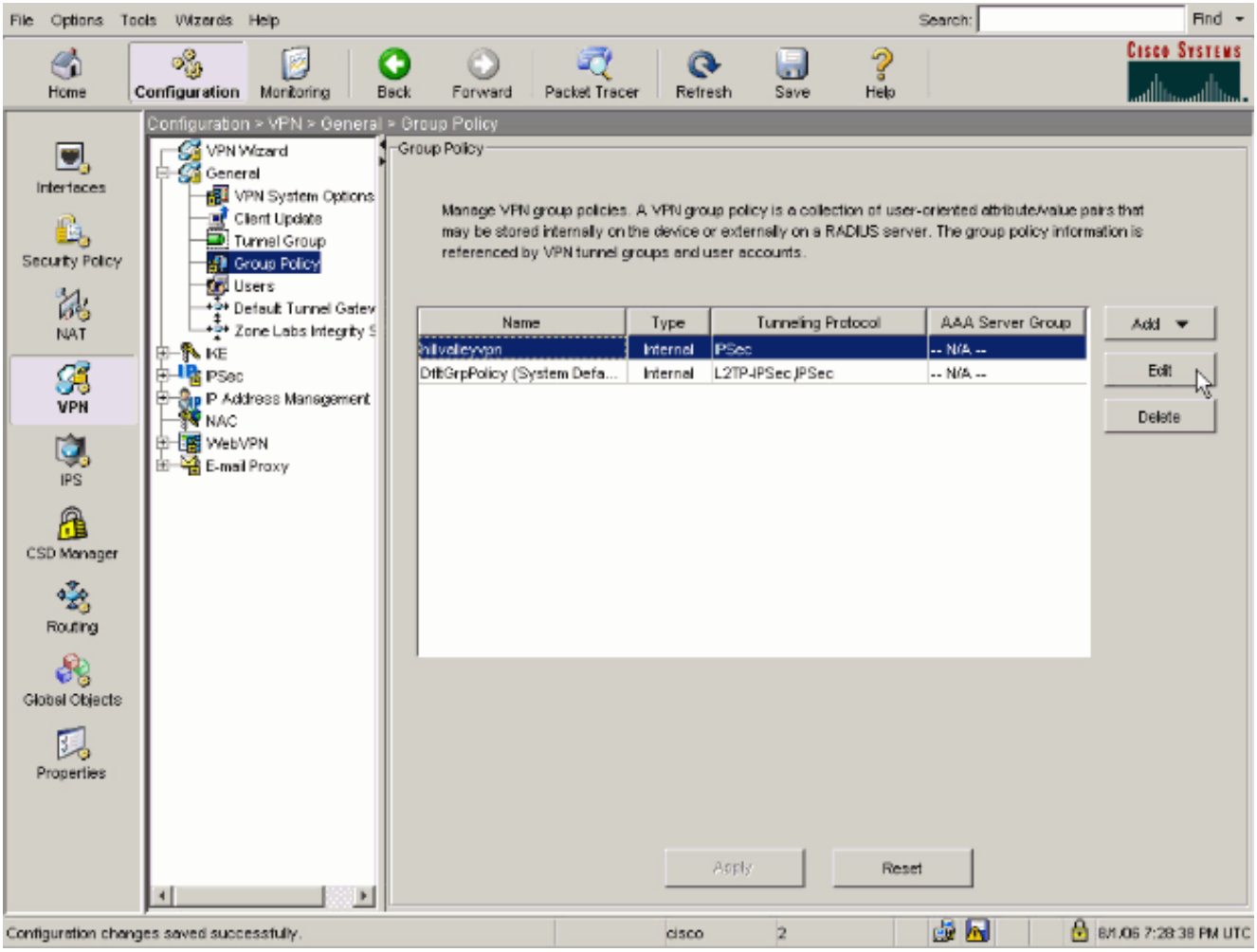
在基本的VPN客戶端到ASA場景中，來自VPN客戶端的所有流量都會被加密並傳送到ASA，而不管其目標是什麼。根據您的配置和支援的使用者數量，此類設定可能會佔用大量頻寬。分割通道可以緩解此問題，因為它允許使用者僅傳送通過通道傳送到公司網路的流量。所有其他流量（如即時消息、電子郵件或隨意瀏覽）均通過VPN客戶端的本地LAN傳送到網際網路。

在ASA上配置拆分隧道

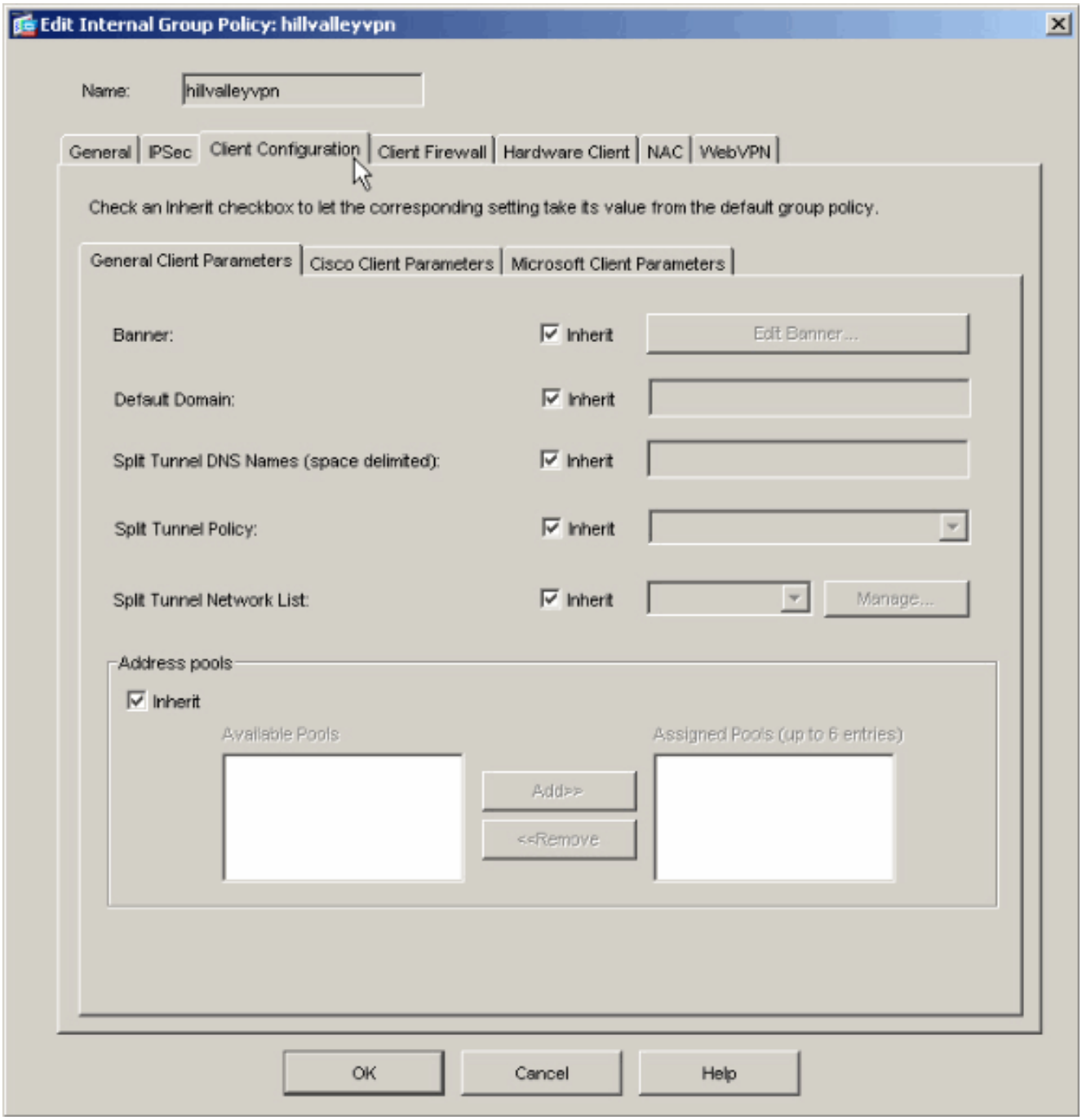
使用自適應安全裝置管理器(ASDM)5.x配置ASA 7.x

完成這些步驟，將通道組配置為允許組內使用者的拆分通道。

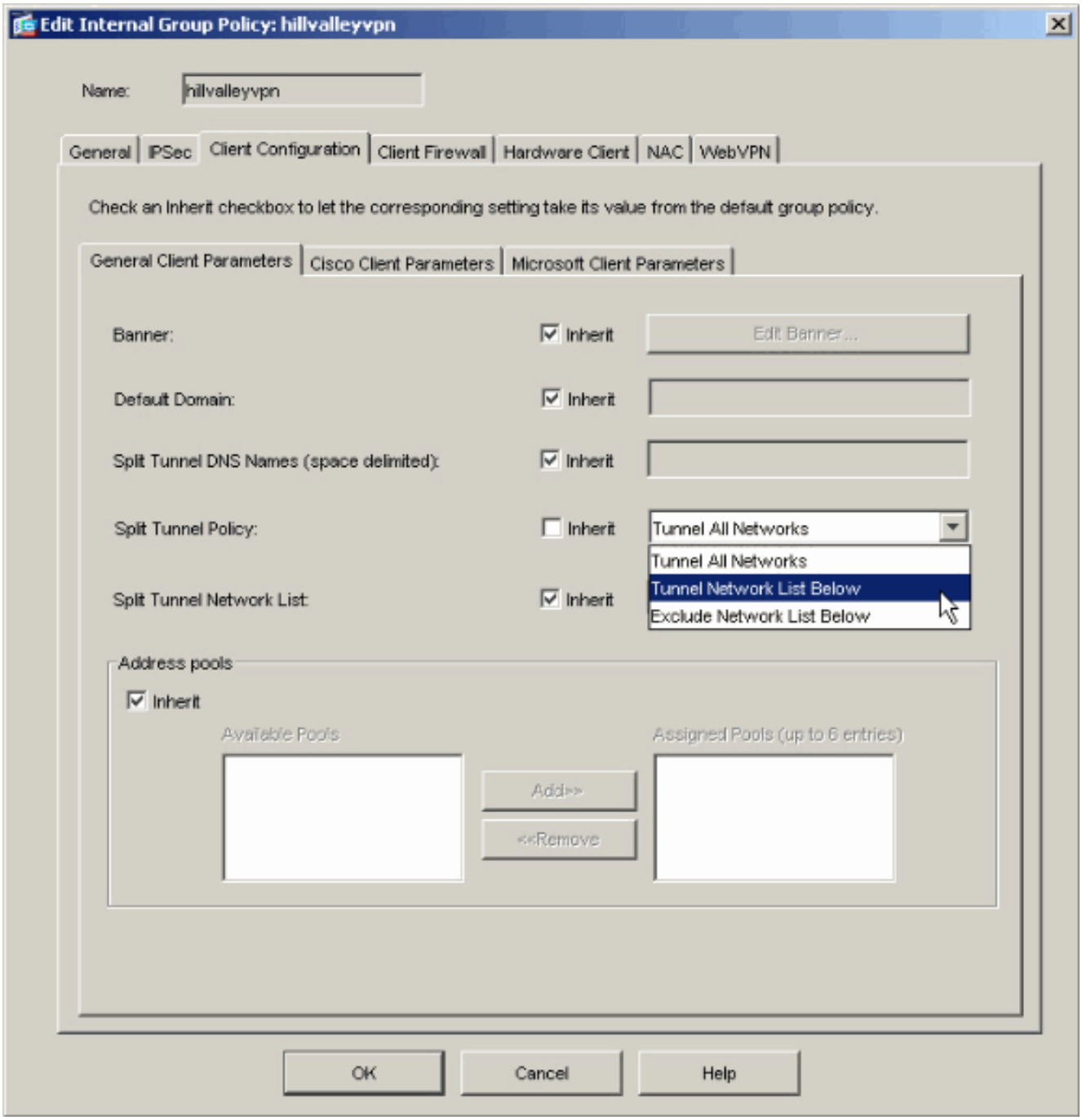
1. 選擇**Configuration > VPN > General > Group Policy**，然後選擇要啟用本地LAN訪問的組策略。然後按一下**Edit**。



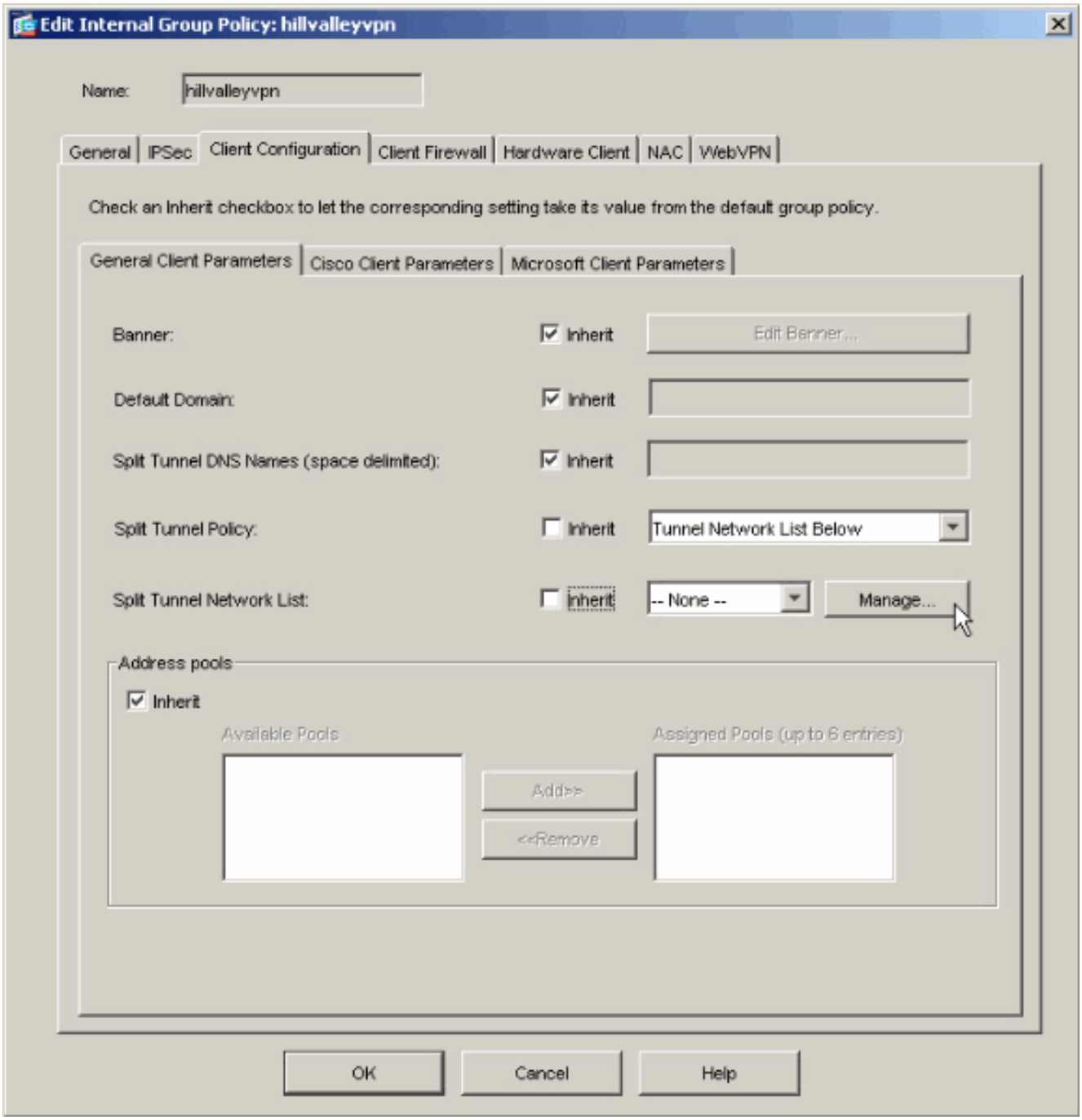
2. 轉到「客戶端配置」頁籤。



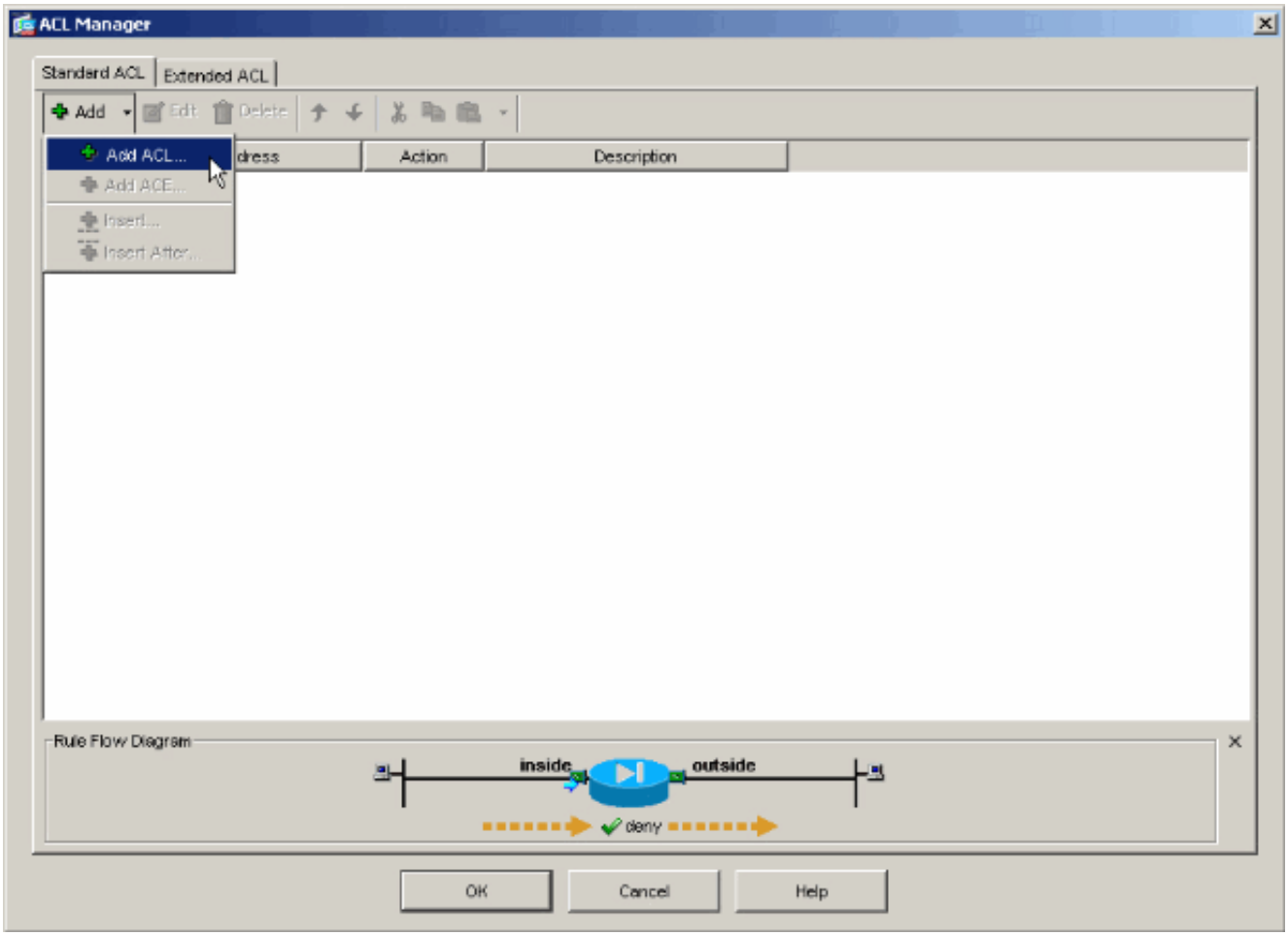
3. 取消選中Split Tunnel Policy的**Inherit**框，然後選擇**Tunnel Network List Below**。



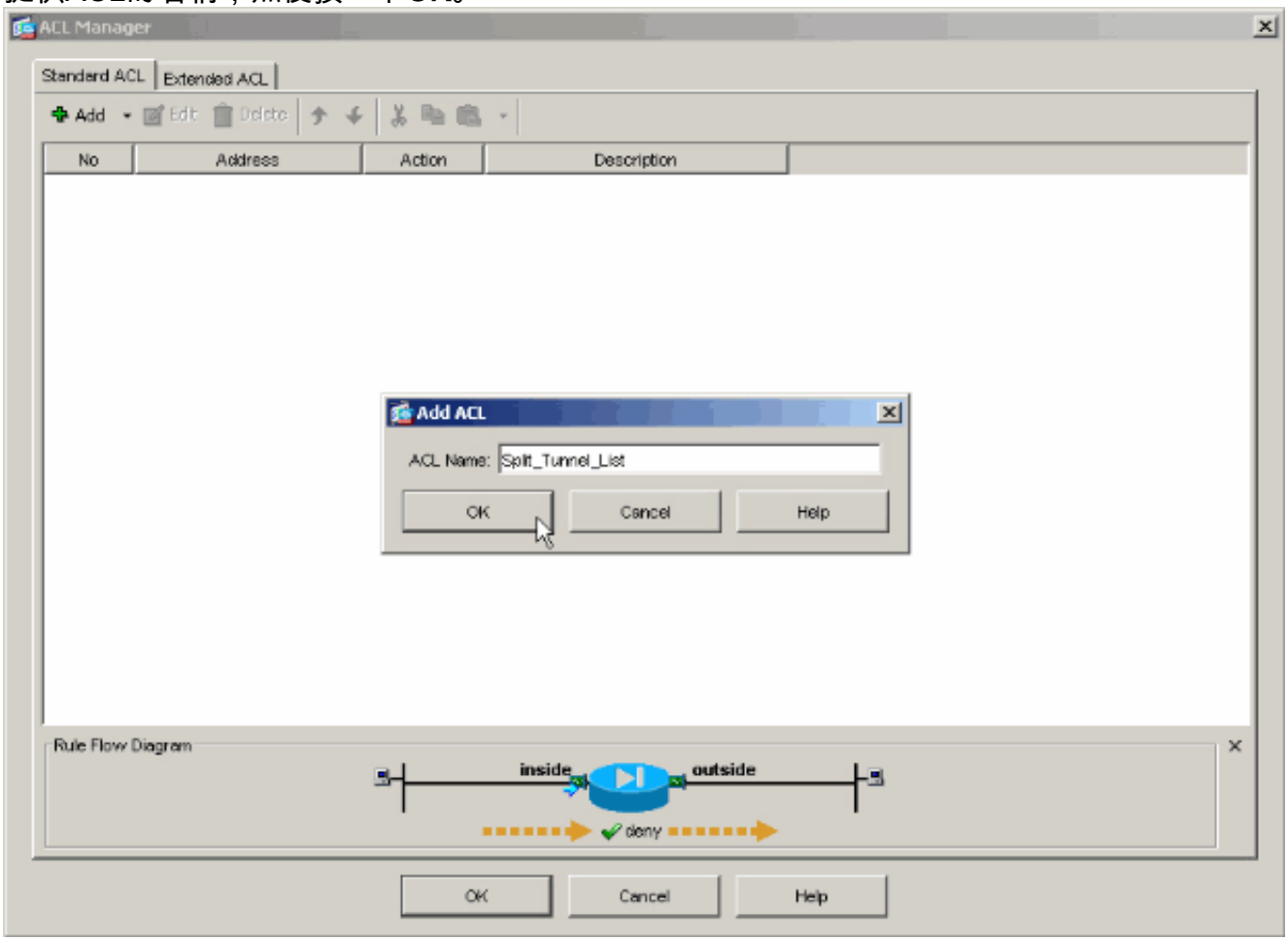
4. 取消選中Split Tunnel Network List的**Inherit**框，然後按一下**Manage**以啟動ACL Manager。



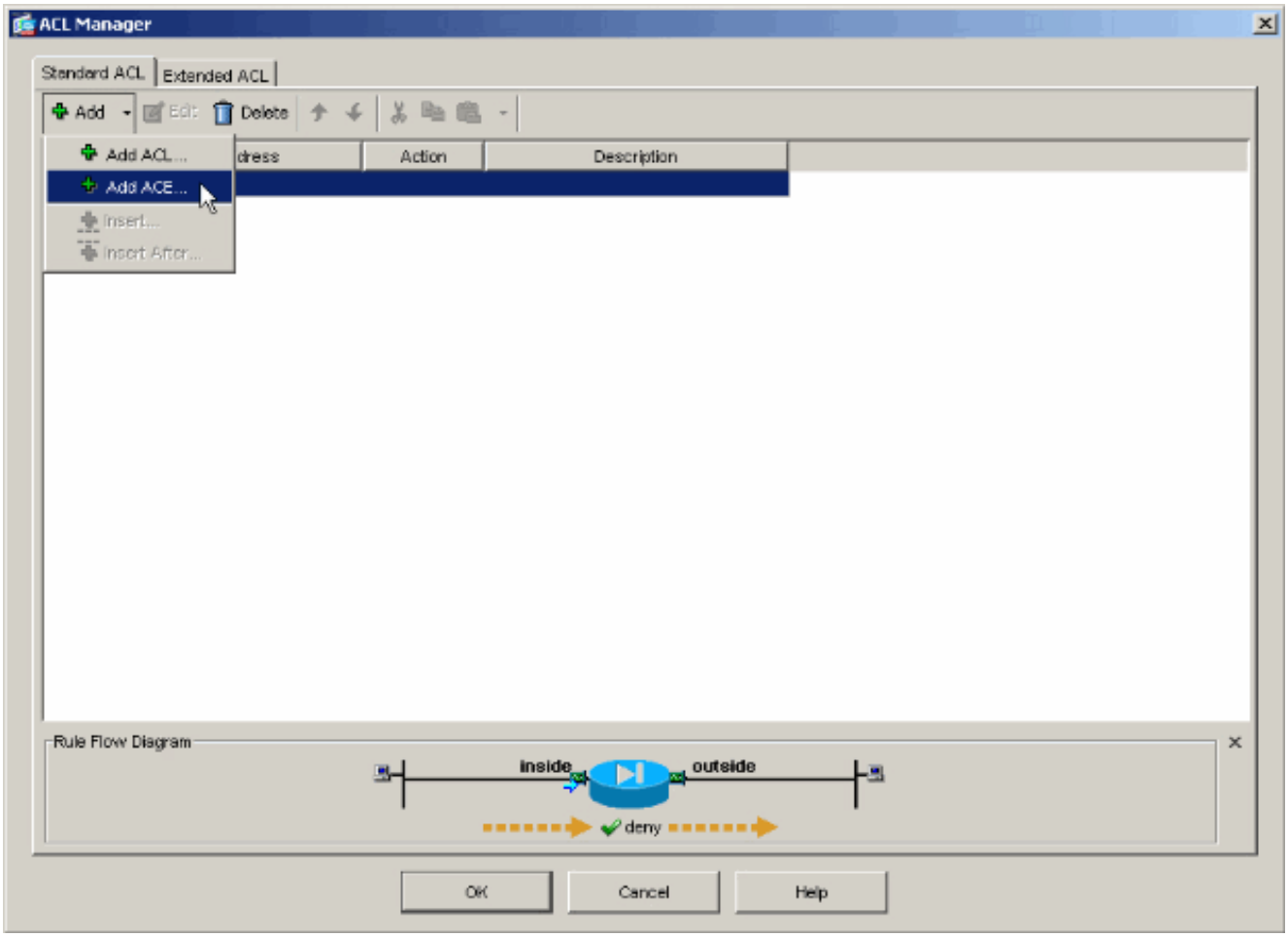
5. 在ACL Manager中，選擇**Add > Add ACL...**以建立新的訪問清單。



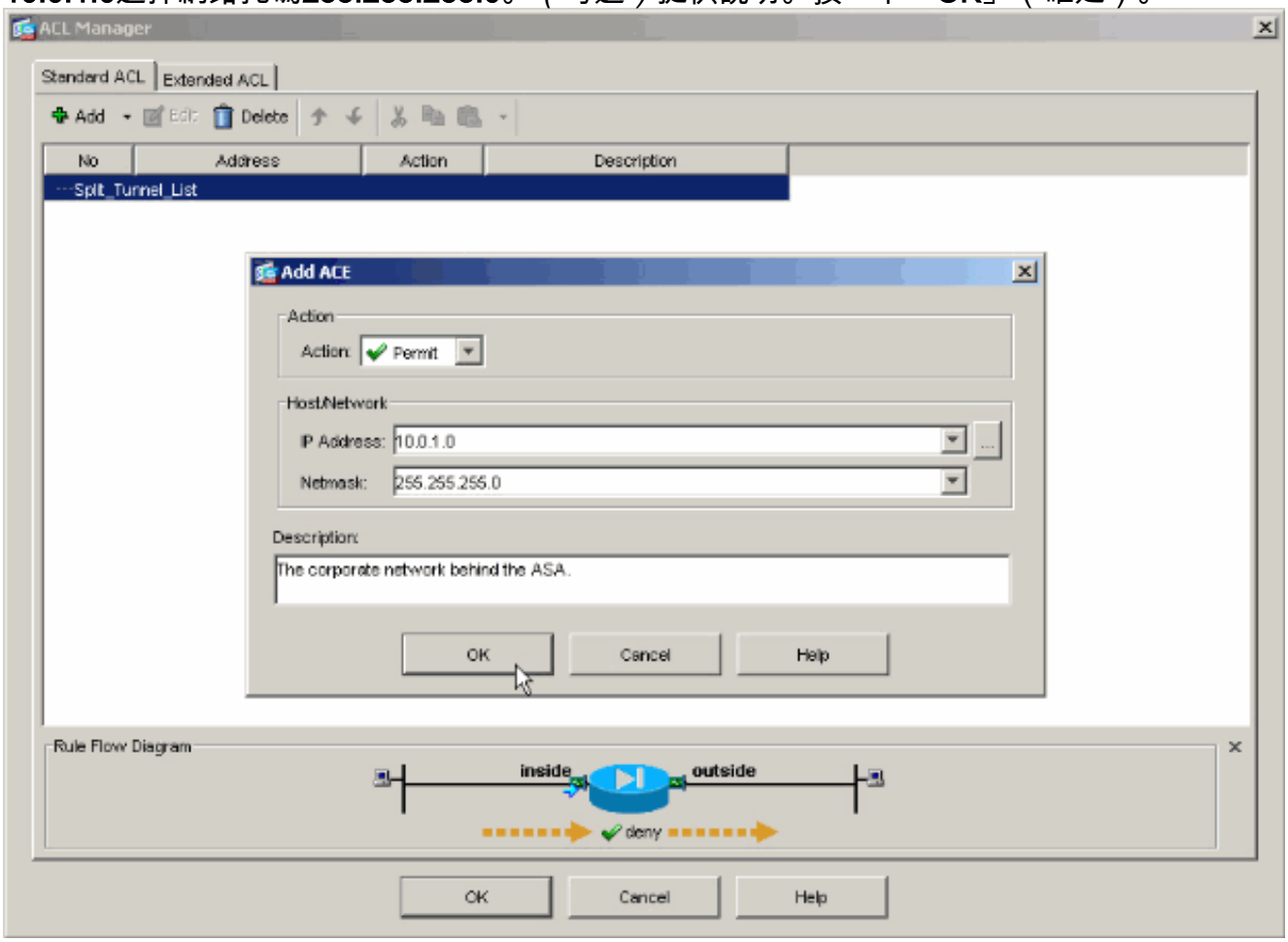
6. 提供ACL的名稱，然後按一下**OK**。



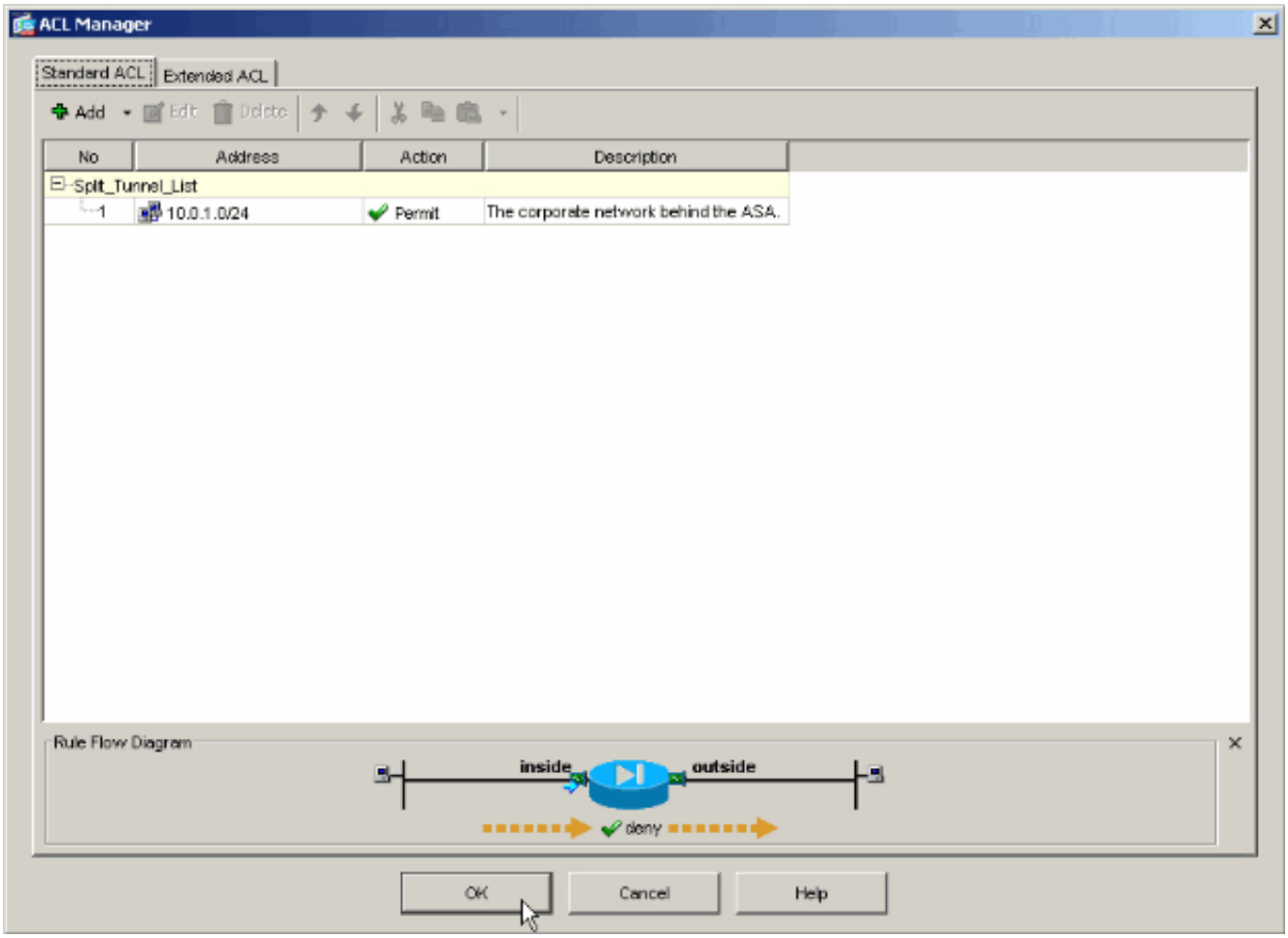
7. 建立ACL後，選擇**Add > Add ACE...**以新增訪問控制條目(ACE)。



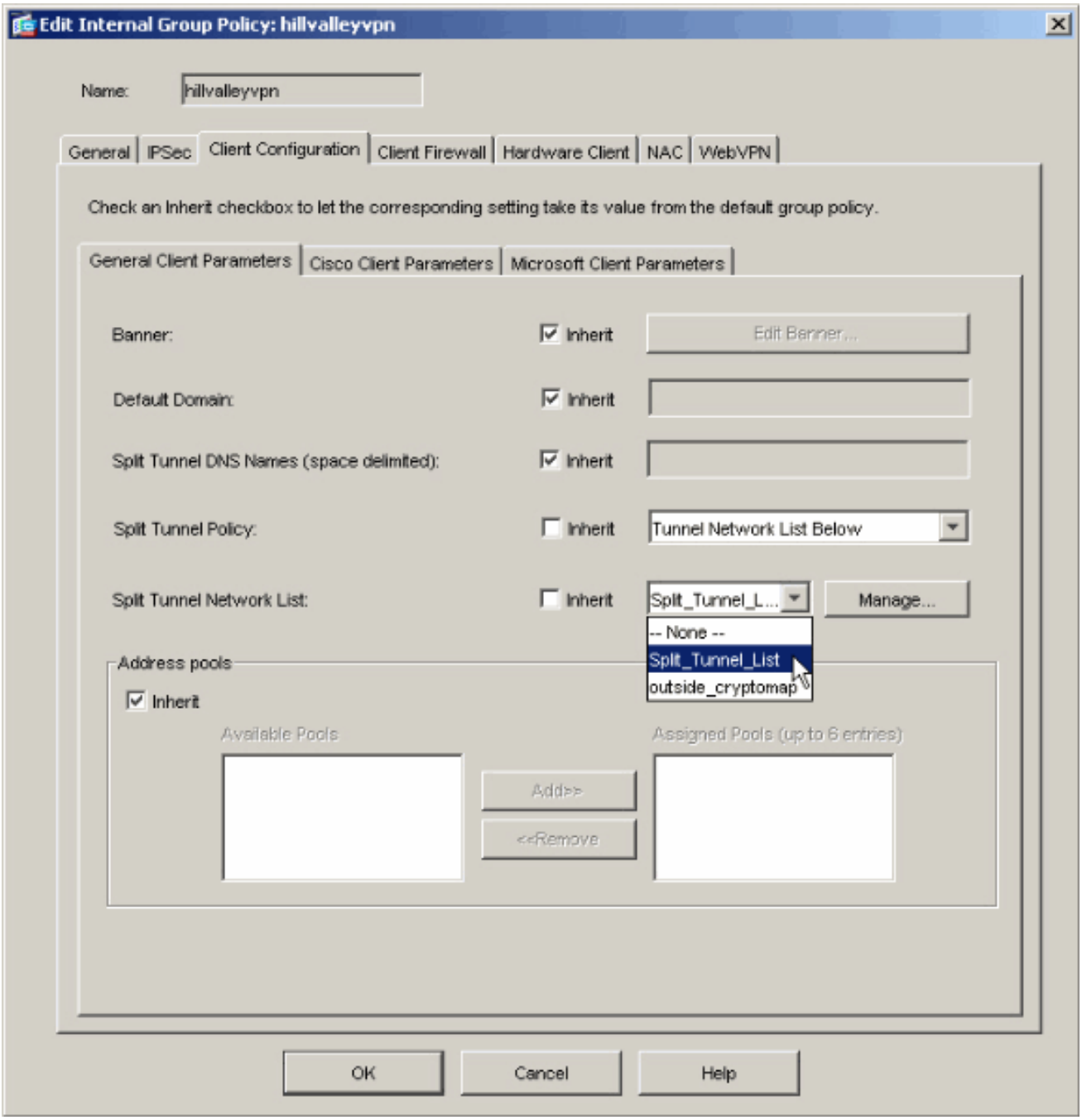
8. 定義與ASA後面的LAN對應的ACE。在本例中，網路是10.0.1.0/24。選擇**Permit**。選擇IP地址**10.0.1.0**選擇網路掩碼**255.255.255.0**。*（可選）*提供說明。按一下「**OK**」（確定）。



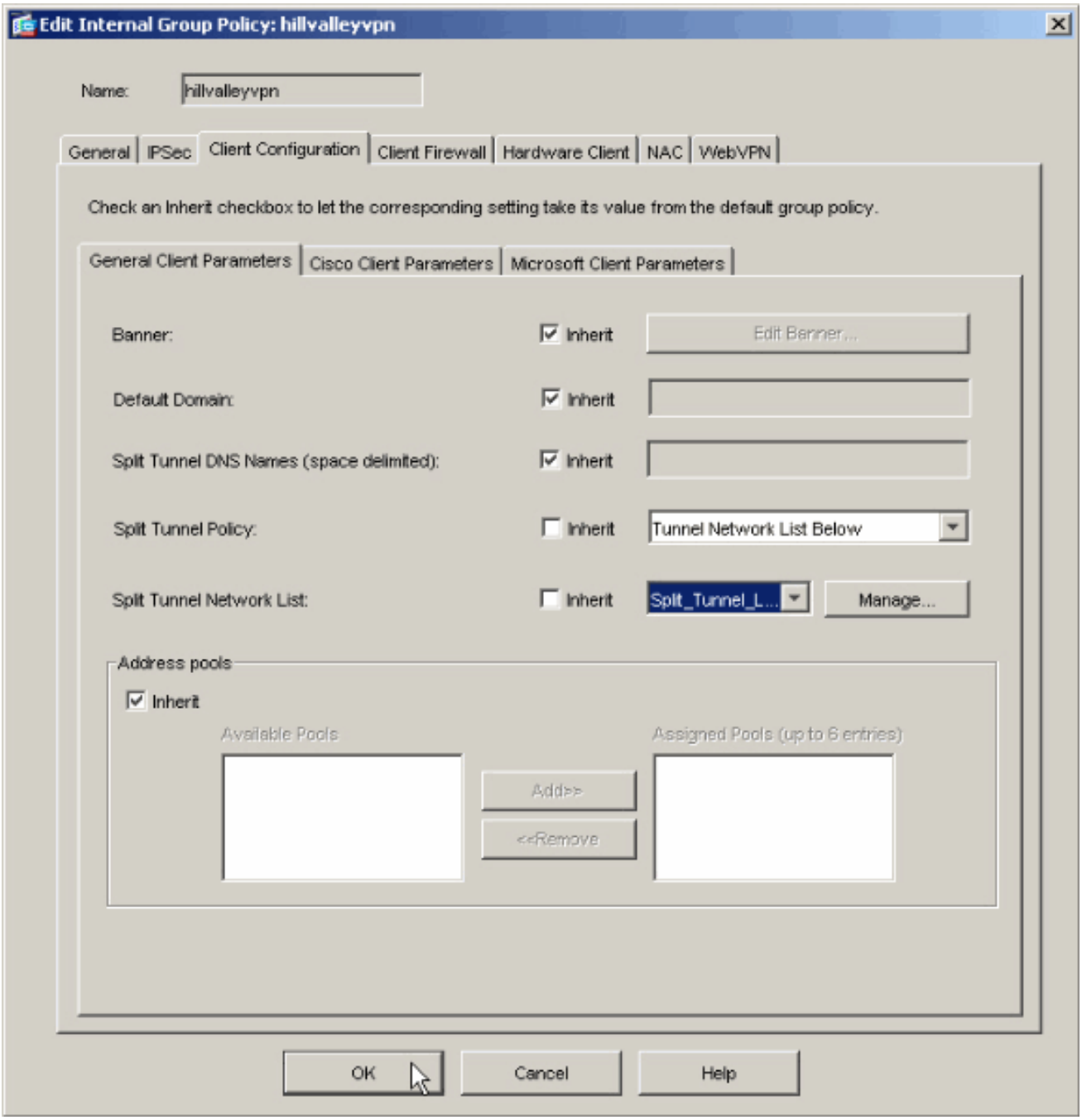
9. 按一下「**OK**」以退出ACL Manager。



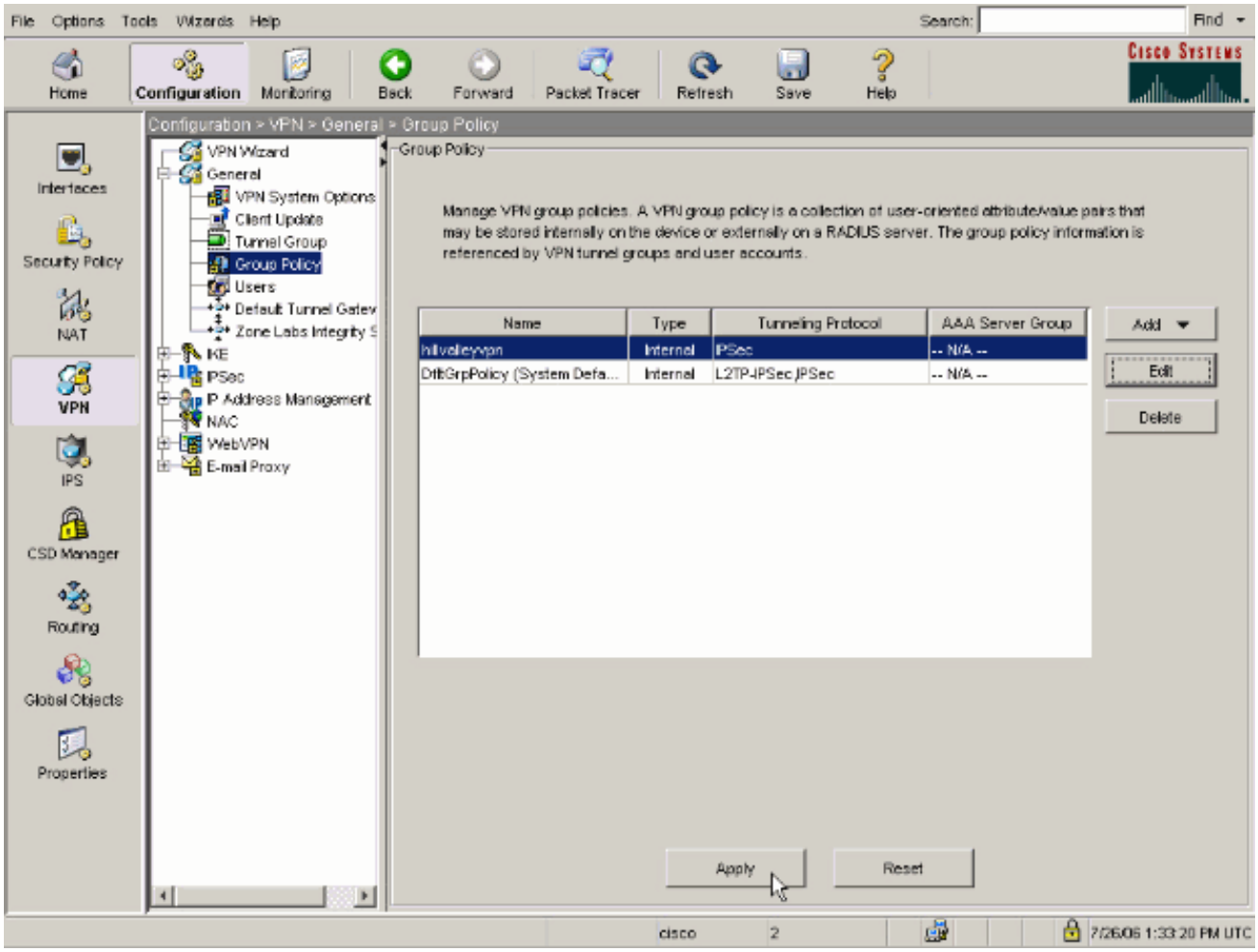
10. 請確保為分割隧道網路清單選擇了您剛剛建立的ACL。



11. 按一下**OK**以返回組策略配置。



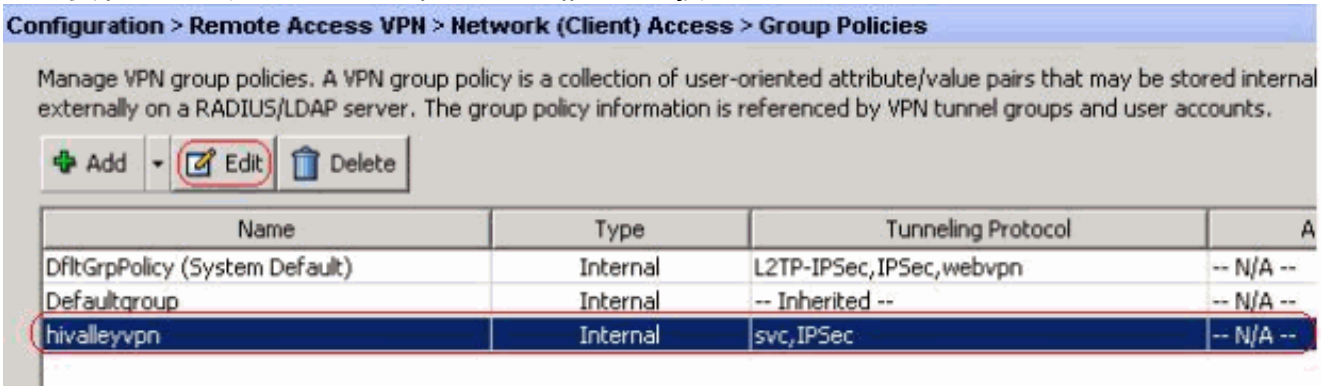
12. 按一下**Apply**，然後按一下**Send**（如果需要），以將命令傳送到ASA。



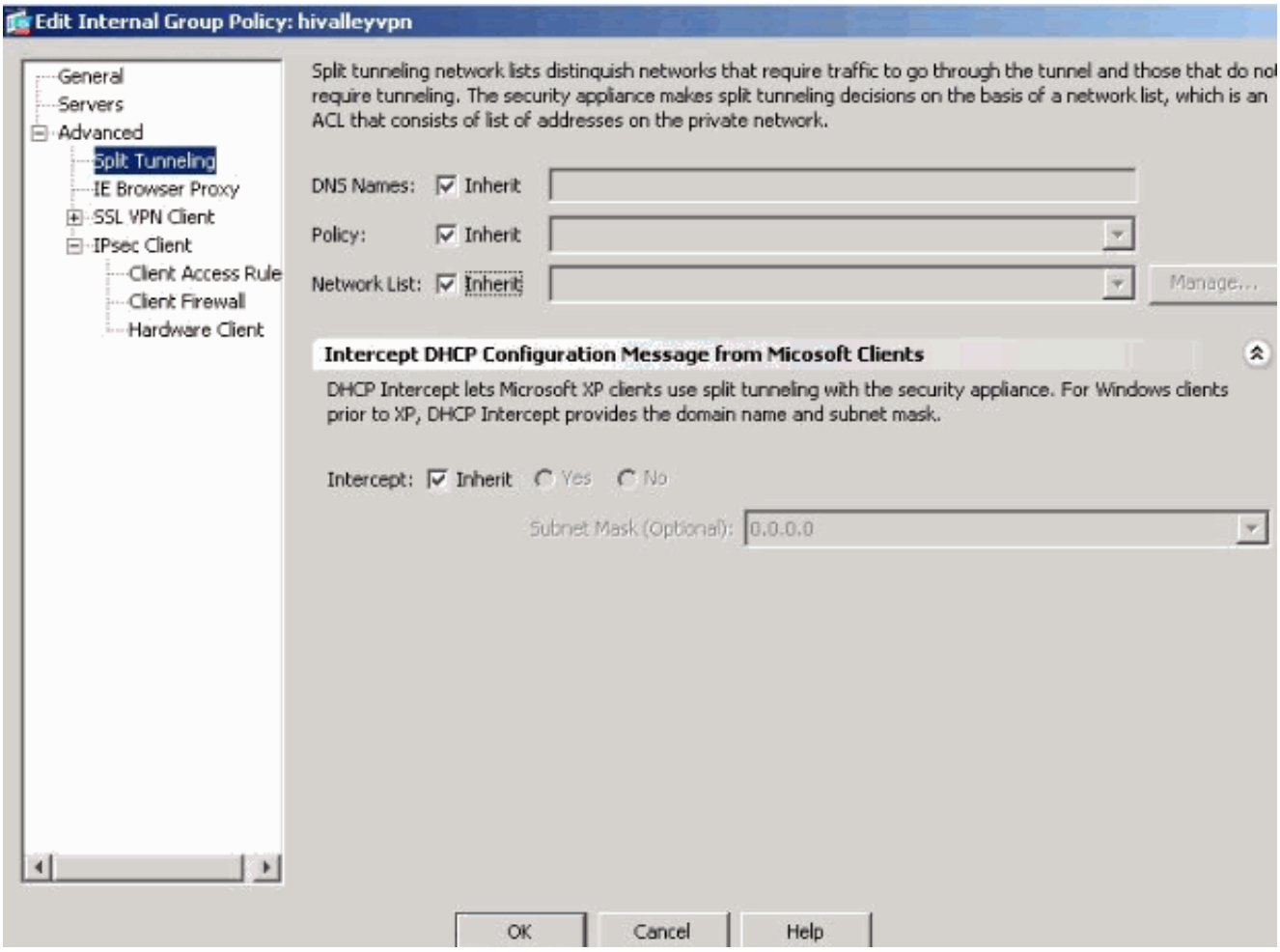
使用自適應安全裝置管理器(ASDM)6.x配置ASA 8.x

完成這些步驟，將通道組配置為允許組內使用者的拆分通道。

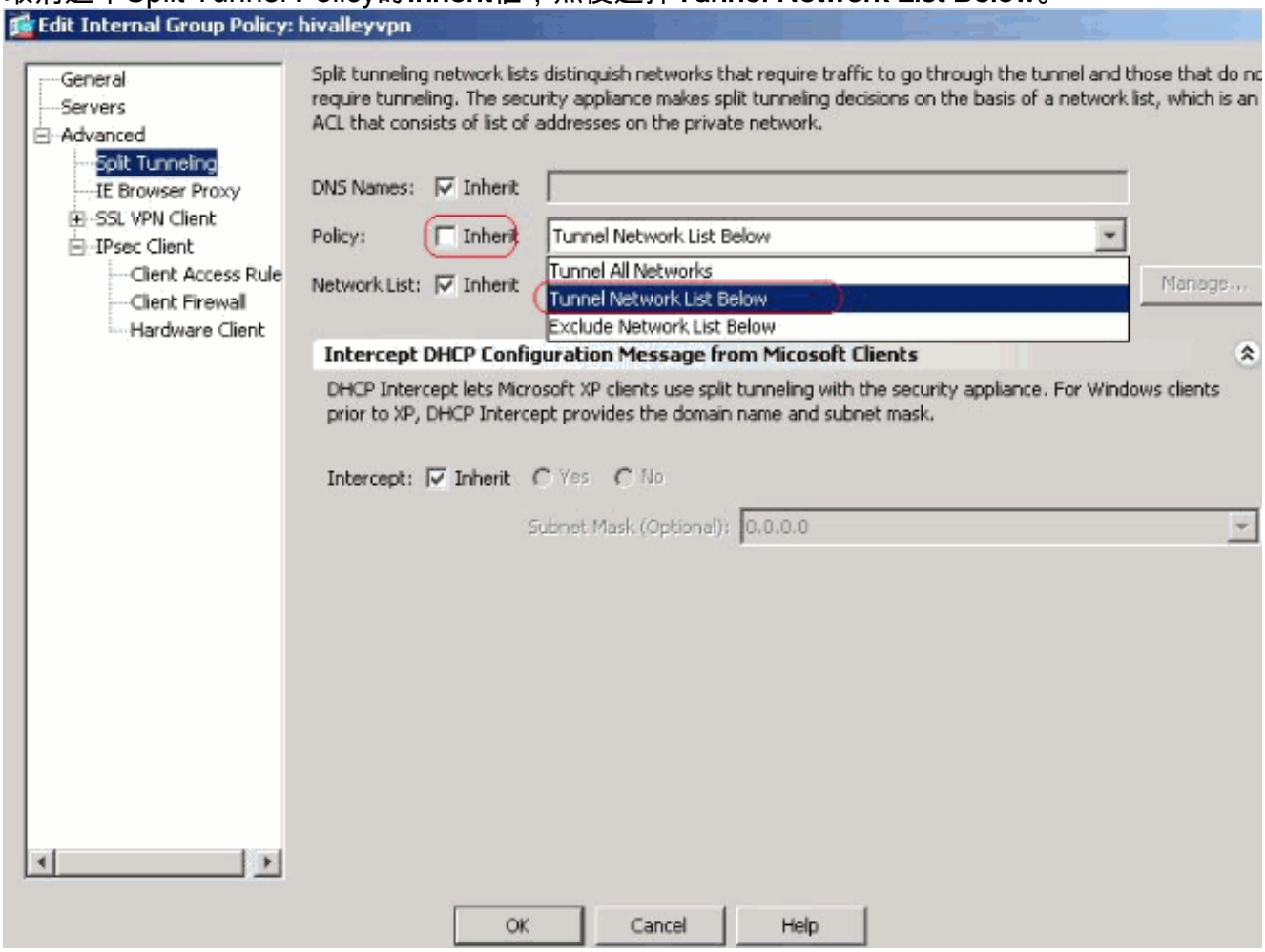
1. 選擇**Configuration > Remote Access VPN > Network(Client)Access > Group Policies**，然後選擇要在其中啟用本地LAN訪問的組策略。然後按一下**Edit**。



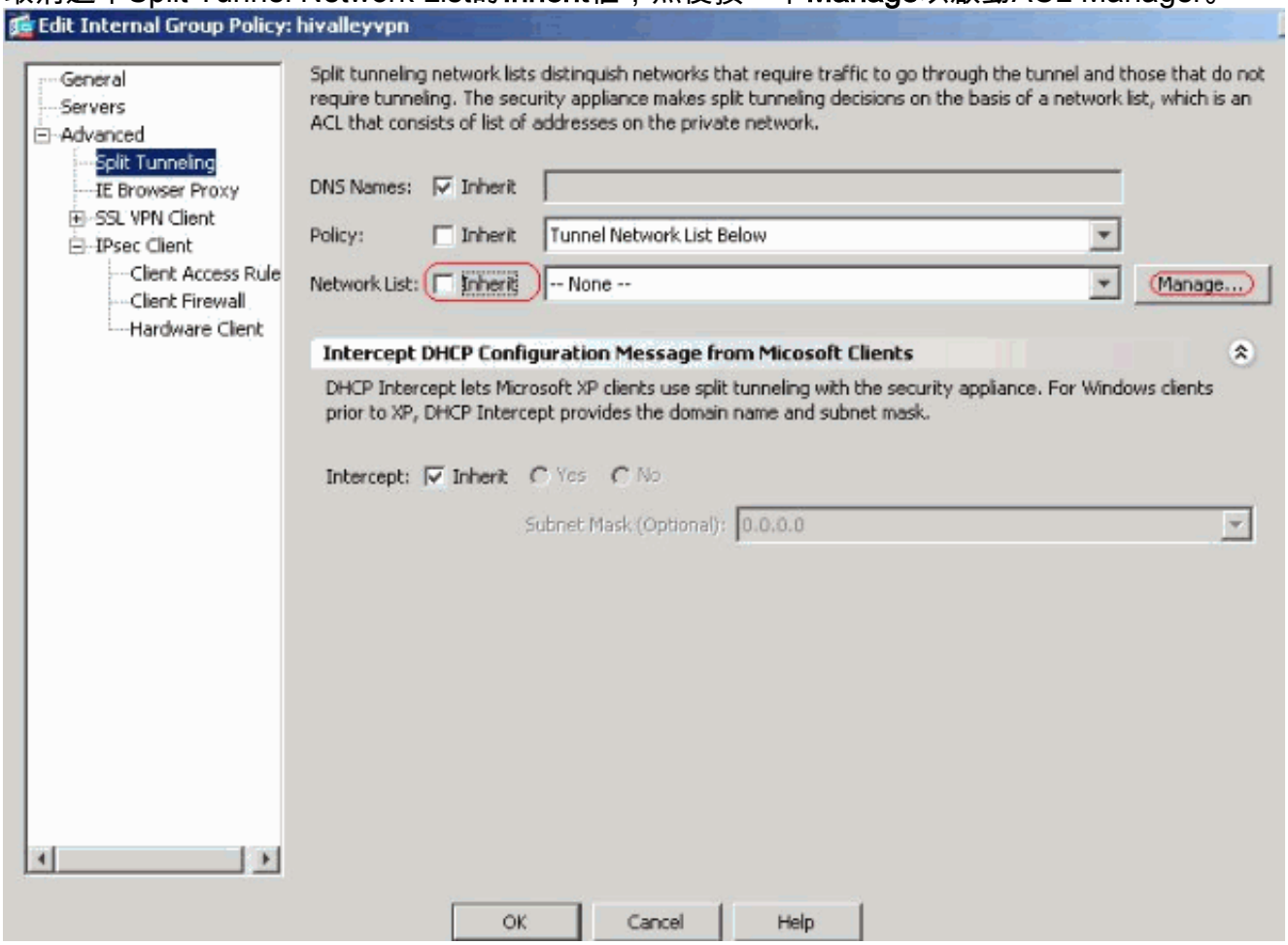
2. 按一下**Split Tunneling**。



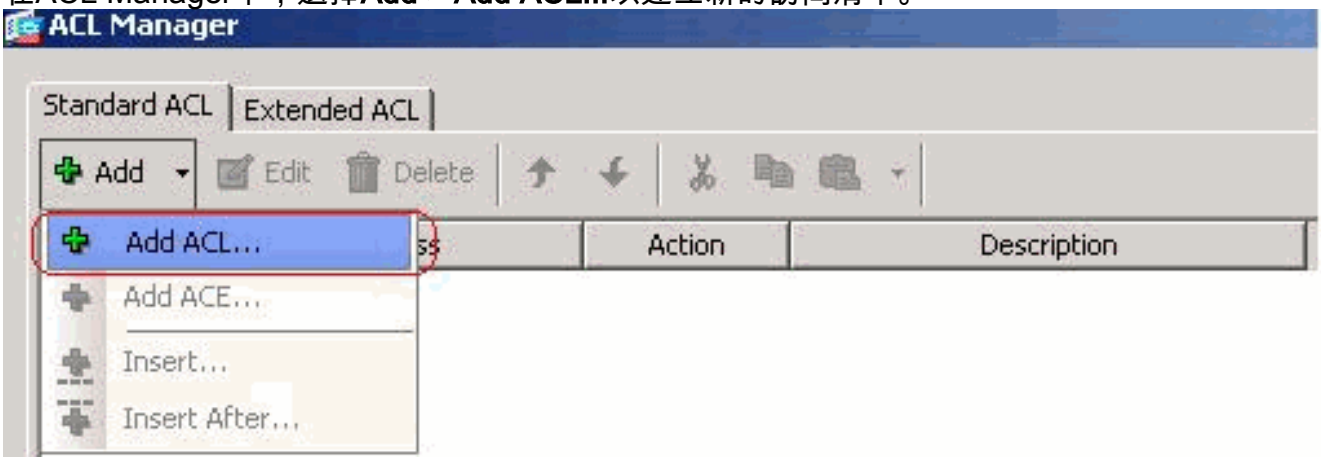
3. 取消選中Split Tunnel Policy的**Inherit**框，然後選擇**Tunnel Network List Below**。



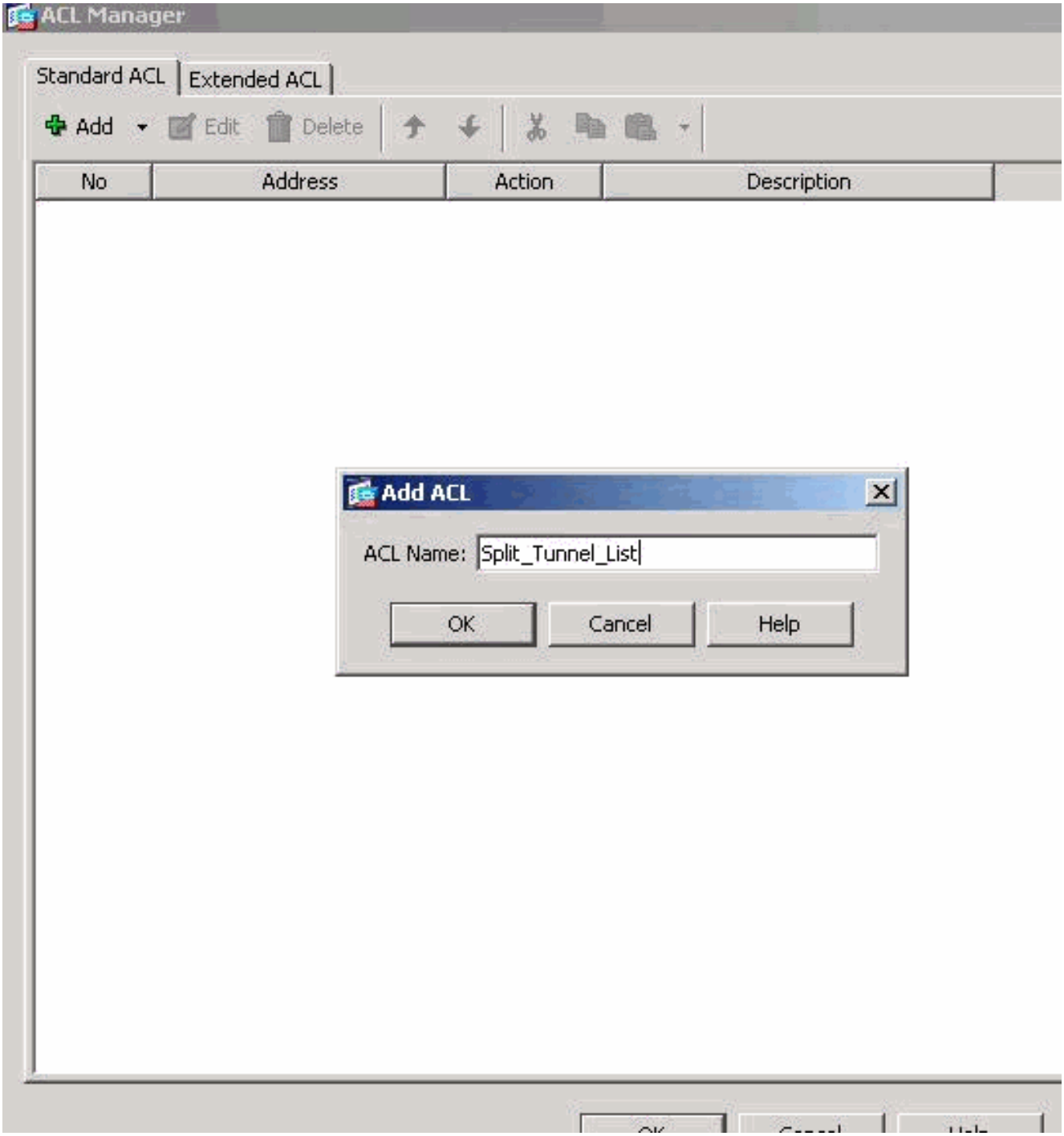
4. 取消選中Split Tunnel Network List的**Inherit**框，然後按一下**Manage**以啟動ACL Manager。



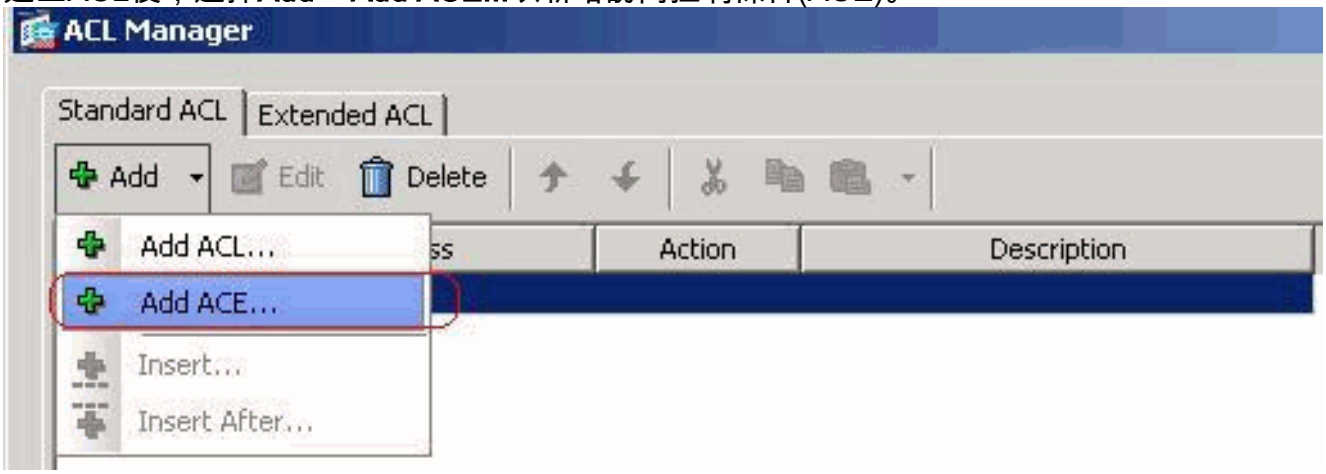
5. 在ACL Manager中，選擇**Add > Add ACL...**以建立新的訪問清單。



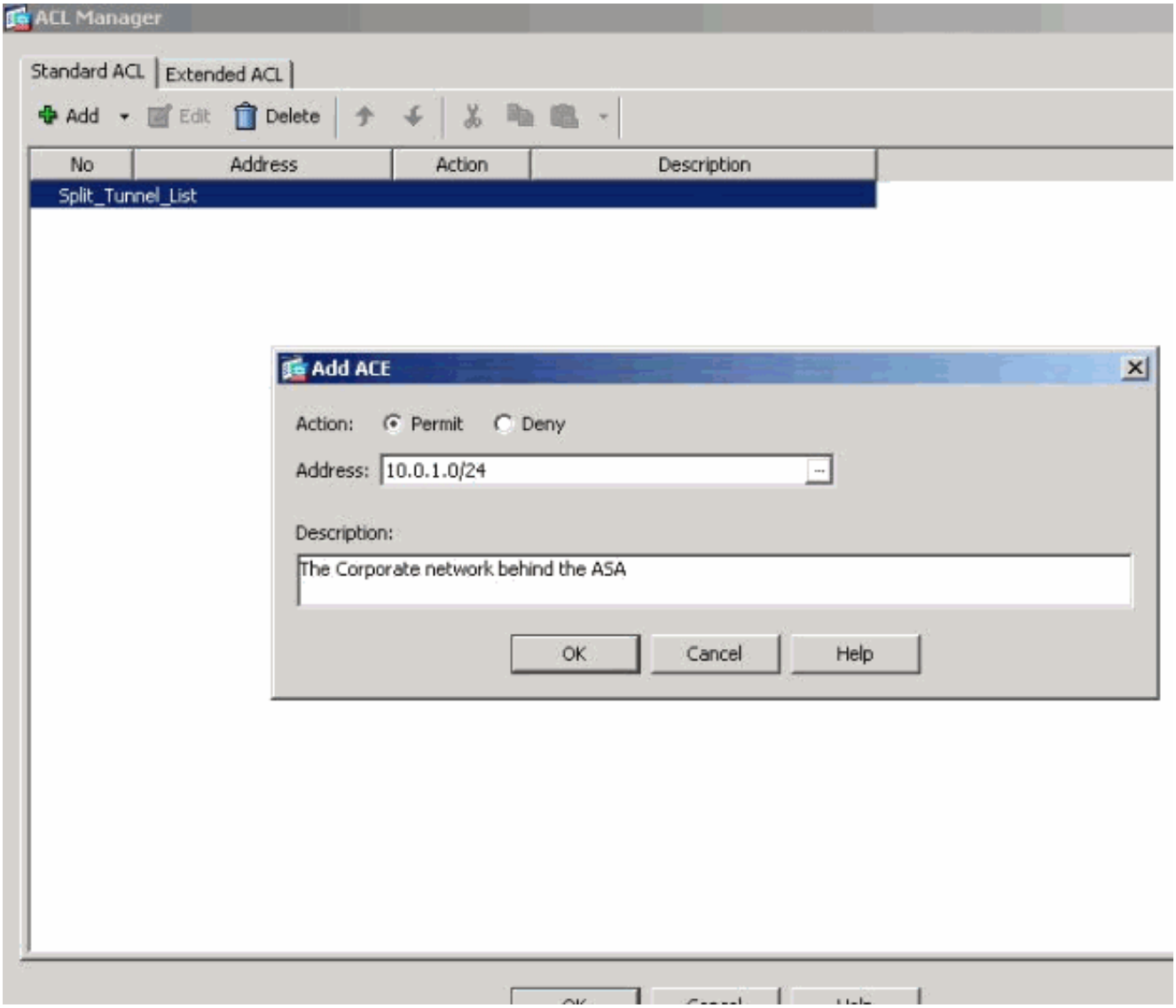
6. 提供ACL的名稱，然後按一下**OK**。



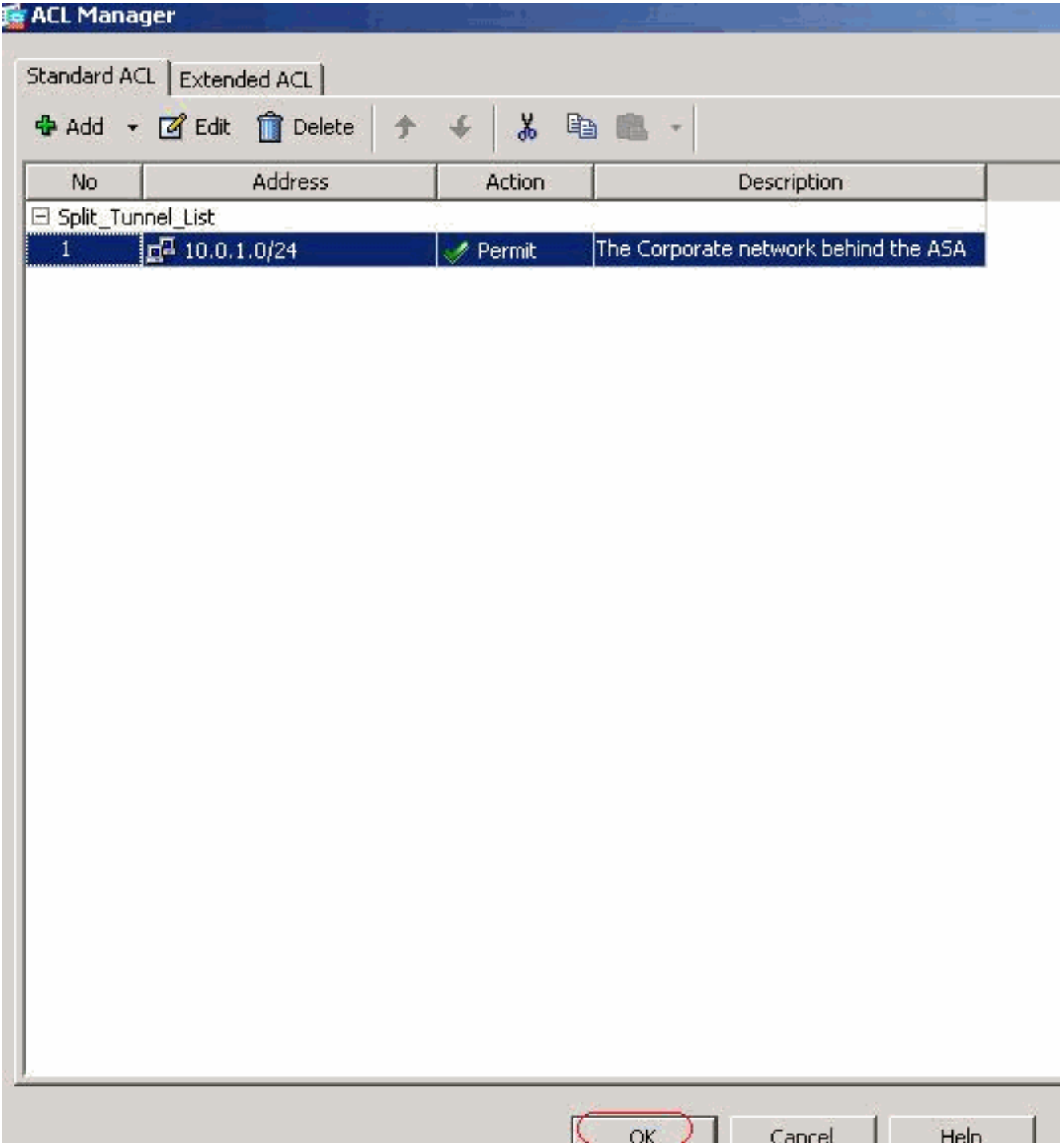
7. 建立ACL後，選擇**Add > Add ACE...**以新增訪問控制條目(ACE)。



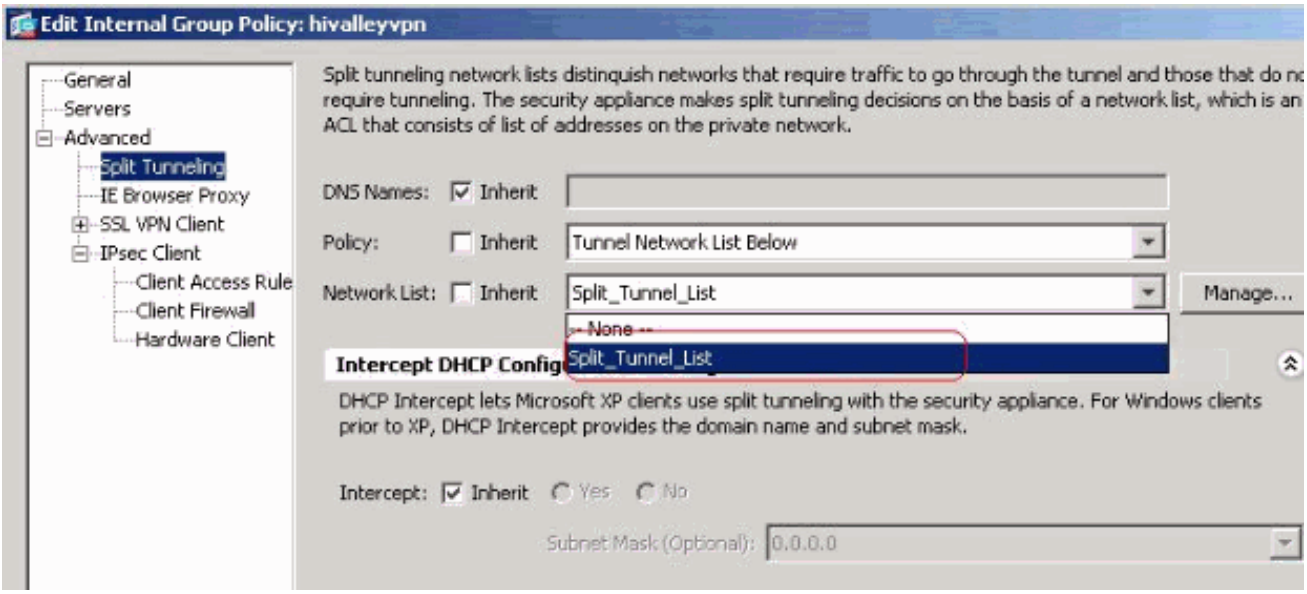
8. 定義與ASA後面的LAN對應的ACE。在本例中，網路是10.0.1.0/24。按一下**Permit**單選按鈕。選擇掩碼為**10.0.1.0/24**的網路地址。（可選）提供說明。按一下「**OK**」（確定）。



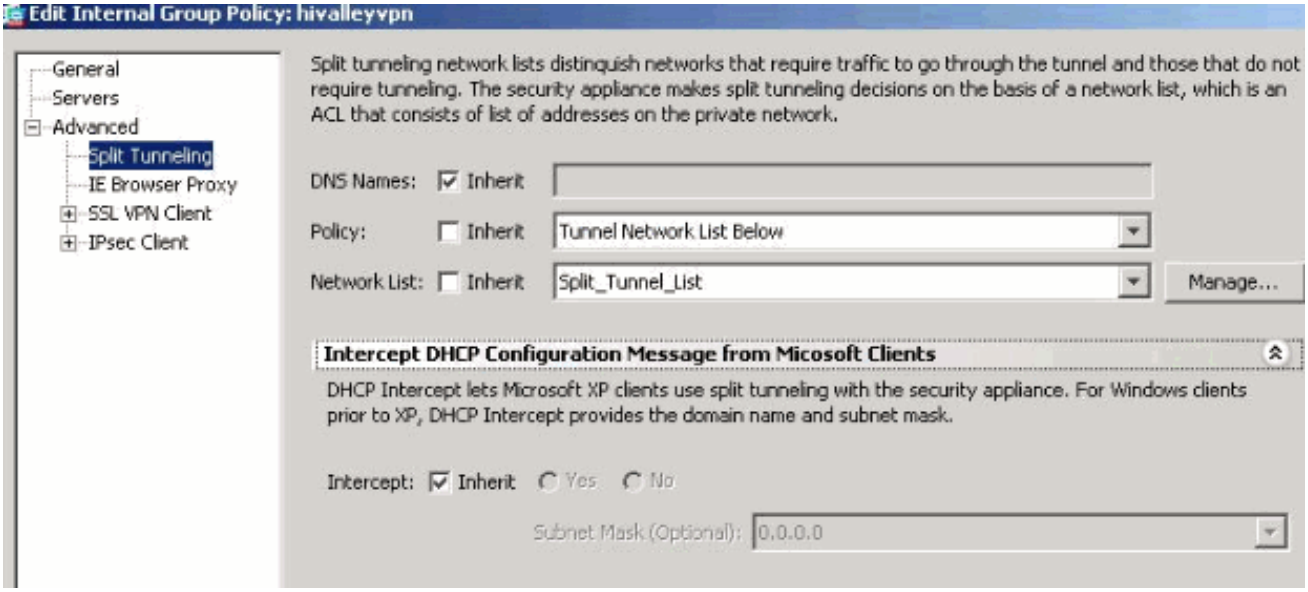
9. 按一下「**OK**」以退出ACL Manager。



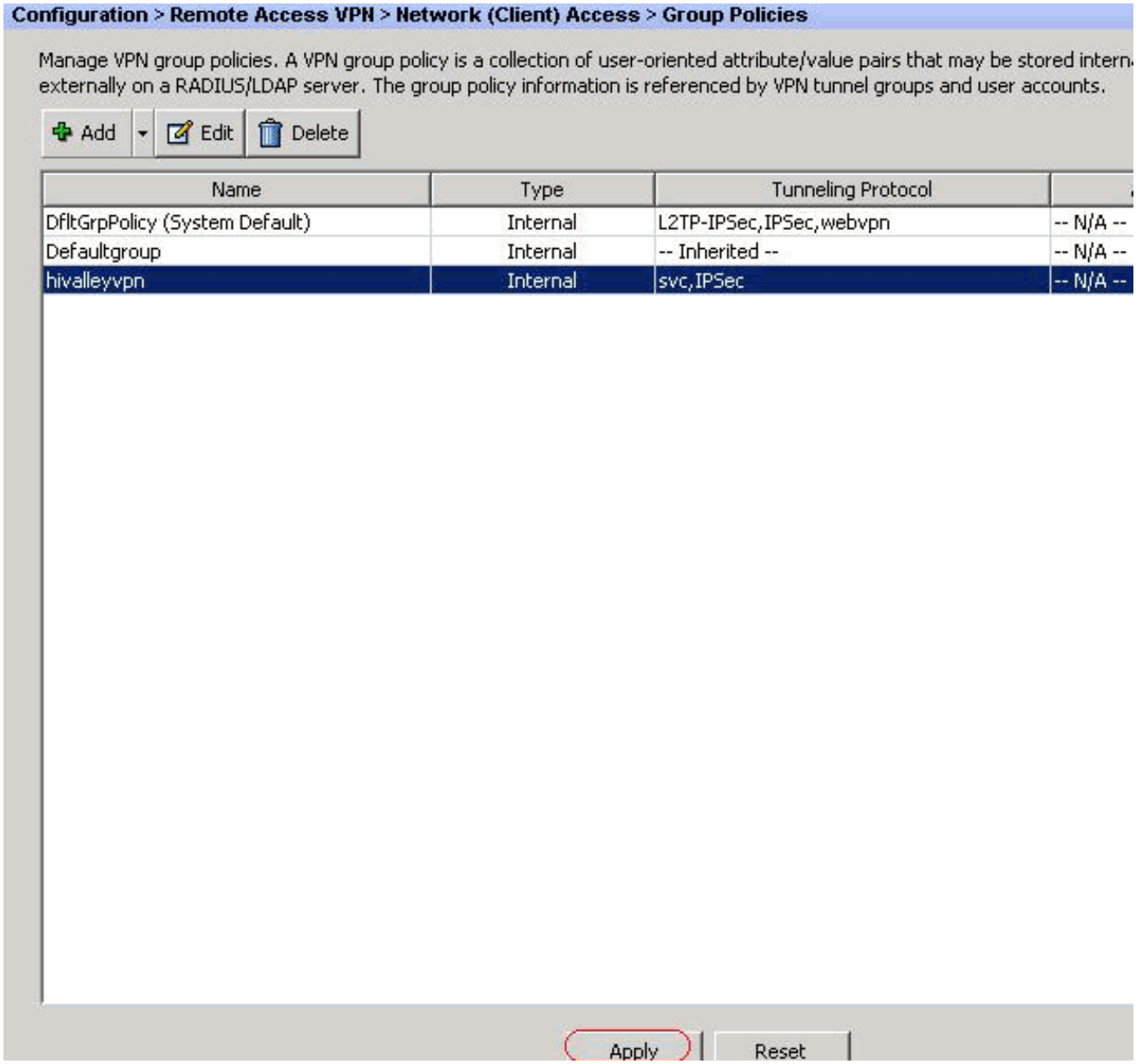
10. 請確保為分割隧道網路清單選擇了您剛剛建立的ACL。



11. 按一下**OK**以返回組策略配置。



12. 按一下**Apply**，然後按一下**Send**（如果需要），以將命令傳送到ASA。



通過CLI配置ASA 7.x及更高版本

您可以在ASA CLI中完成以下步驟，以便在ASA上允許拆分隧道，而不是使用ASDM:

註：ASA 7.x和8.x的CLI拆分隧道配置相同。

1. 進入配置模式。
```
ciscoasa>enable
Password: ********
ciscoasa#configure terminal
ciscoasa(config)#
```
2. 建立定義ASA後網路的訪問清單。
```
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. 進入要修改的策略的組策略配置模式。
```
ciscoasa(config)#group-policy hillvalleyvpn attributes
ciscoasa(config-group-policy)#
```
4. 指定拆分隧道策略。在這種情況下，策略為tunnelspecified。
```
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified
```

5. 指定拆分隧道訪問清單。在這種情況下，該清單為Split_Tunnel_List。
   ```
   ciscoasa(config-group-policy)#split-tunnel-network-list value Split_Tunnel_List
   ```

6. 發出以下命令：
   ```
   ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes
   ```

7. 將組策略與隧道組關聯
   ```
   ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
   ```

8. 退出兩種配置模式。
   ```
   ciscoasa(config-group-policy)#exit
   ciscoasa(config)#exit
   ciscoasa#
   ```
9. 將組態儲存到非易失性RAM(NVRAM)中，並在系統提示時按下Enter以指定來源檔案名稱。
   ```
   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#
   ```

通過CLI配置PIX 6.x

請完成以下步驟：

1. 建立定義PIX後網路的訪問清單。

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

2. 建立vpn組*vpn3000*並指定其拆分隧道ACL，如下所示：
   ```
   PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List
   ```

   註：有關PIX 6.x遠端訪問VPN配置的詳細資訊，請參閱 Cisco Secure PIX Firewall 6.x和Cisco VPN Client 3.5 for Windows with Microsoft Windows 2000和2003 IAS RADIUS Authentication。

驗證

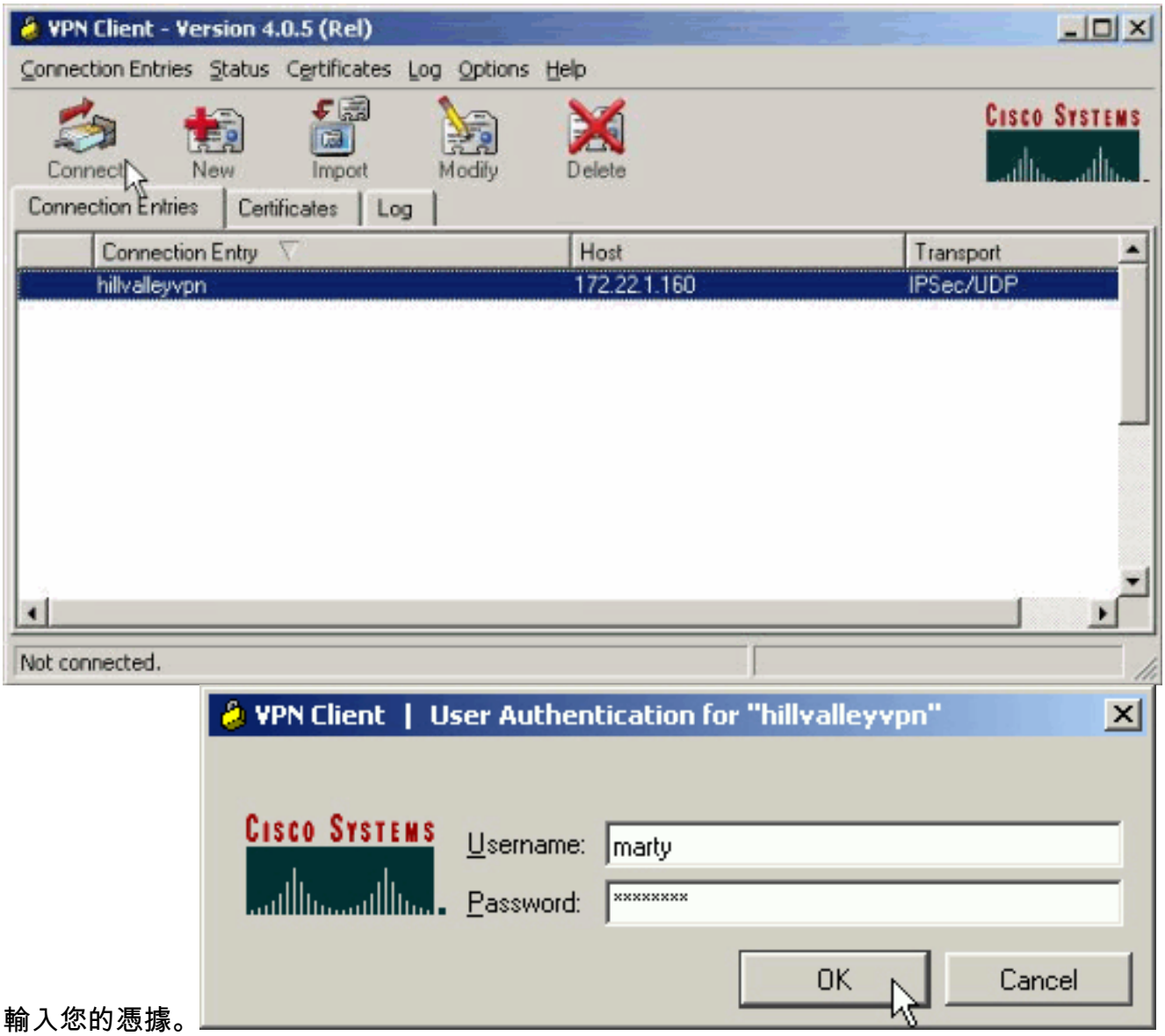
請依照以下各節中的步驟操作，以驗證您的設定。

- 連線VPN客戶端
- 檢視VPN客戶端日誌
- 使用Ping測試本地LAN訪問

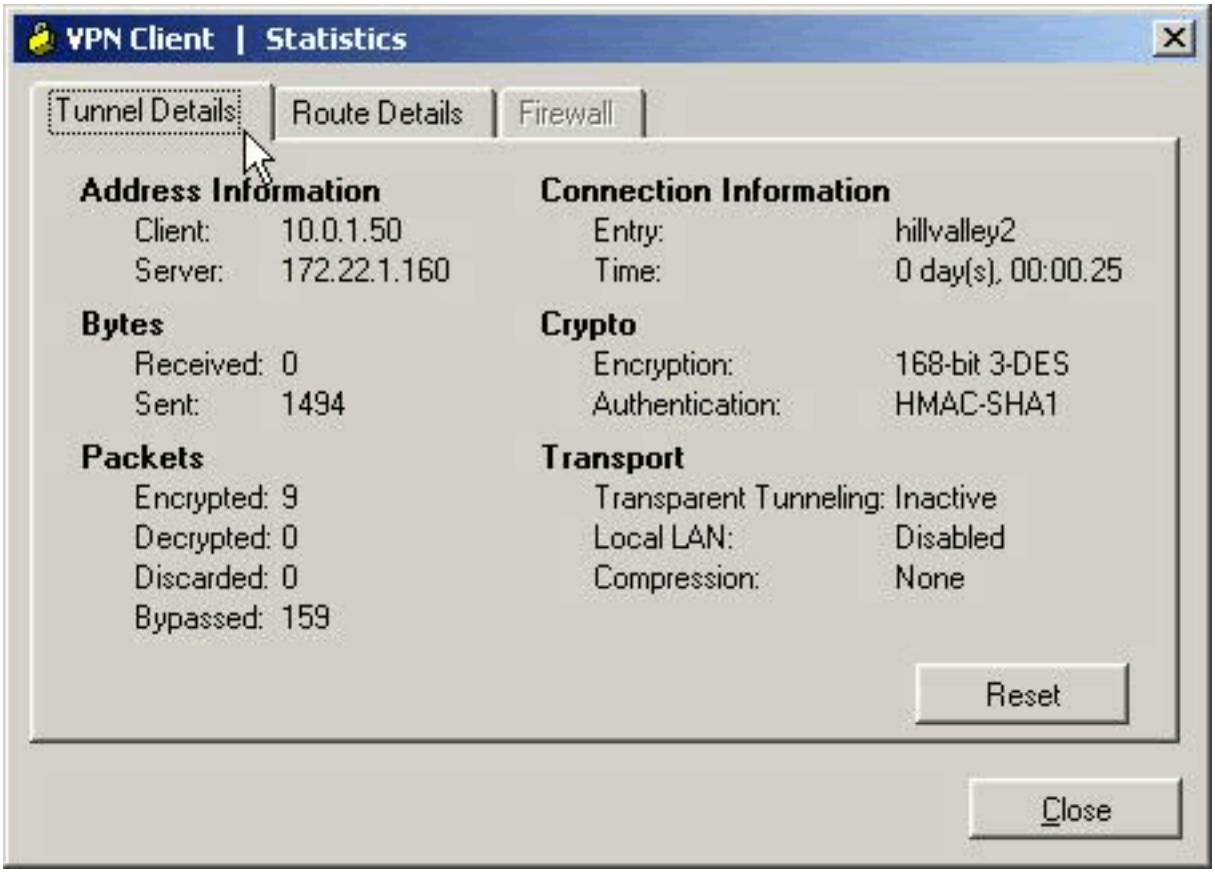
連線VPN客戶端

將VPN客戶端連線到VPN集中器以驗證您的配置。

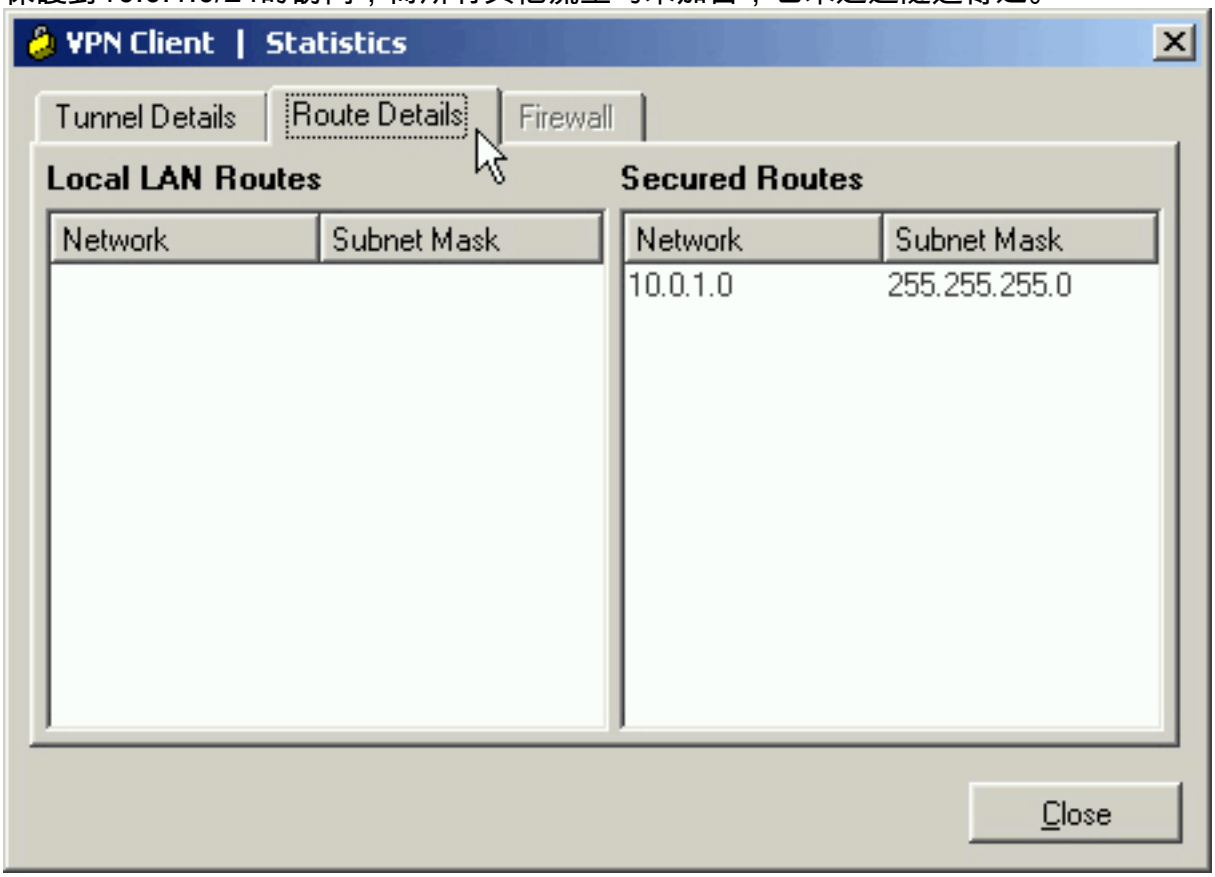
1. 從清單中選擇連線條目，然後按一下Connect。



2. 輸入您的憑據。
3. 選擇**Status > Statistics...**以顯示「Tunnel Details」視窗，您可以在此視窗中檢查隧道的詳細資訊並檢視流量流。



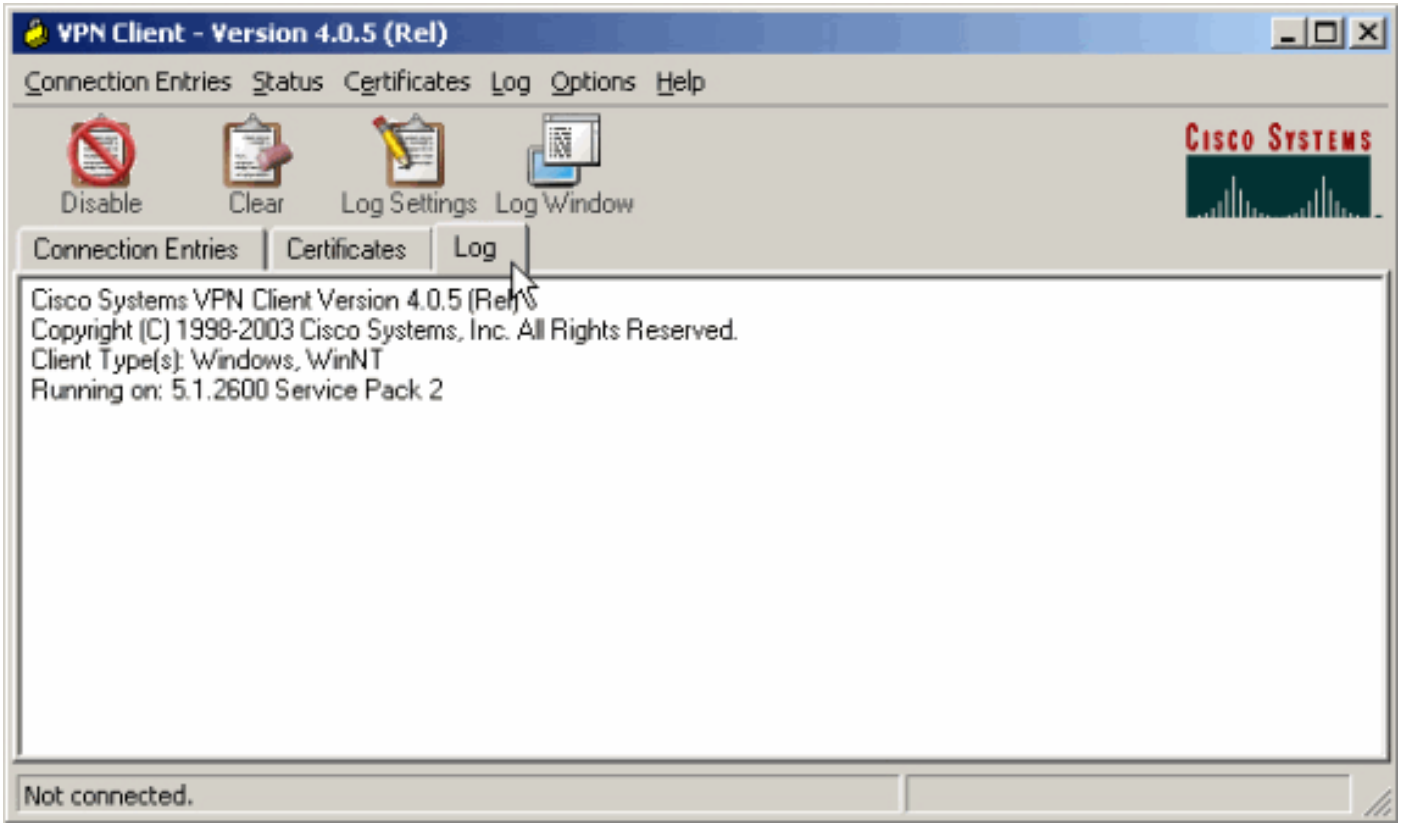
4. 轉至Route Details頁籤，以檢視VPN客戶端保護到ASA的路由。在本示例中，VPN客戶端正在保護對10.0.1.0/24的訪問，而所有其他流量均未加密，也未通過隧道傳送。



檢視VPN客戶端日誌

檢查VPN客戶端日誌時，可以確定是否設定了指定拆分隧道的引數。要檢視日誌，請轉到VPN客戶端中的Log頁籤。然後按一下**Log Settings**以調整記錄的內容。在本示例中，IKE設定為**3 - High**，而

所有其他日誌元素都設**置為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.
```

使用Ping測試本地LAN訪問

測試VPN客戶端在隧道連線到ASA時是否配置為分割隧道的另一種方法是在Windows命令列中使用**ping**命令。VPN客戶端的本地LAN是192.168.0.0/24，而網路中存在IP地址為192.168.0.3的另一台

主機。

```
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
```

疑難排解

分割通道ACL中的專案數限制

用於分割通道的ACL中的專案數量有限制。建議不要使用超過50-60個ACE條目以獲得滿意功能。建議您實作子網劃分功能，以涵蓋一系列IP位址。

相關資訊

- 使用ASDM將PIX/ASA 7.x用作遠端VPN伺服器配置示例
- Cisco ASA 5500系列調適型安全裝置
- 技術支援與文件 - Cisco Systems