在ASA上為VPN客戶端配置分割隧道

目錄

簡介

必要條件

- 需求
- 採用元件
- 網路圖表
- 相關產品
- 慣例

背景資訊

在ASA上配置分割隧道

- 使用自適應安全裝置管理器(ASDM) 5.x配置ASA 7.x
- 使用ASDM6.x配置ASA 8.x
- 透過CLI配置ASA 7.x及更高版本
- 透過CLI配置PIX 6.x

驗證

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

疑難排解

- 分割通道ACL中的專案數限制

相關資訊

簡介

本文檔介紹在將VPN客戶端透過隧道連線到Cisco ASA 5500系列安全裝置時允許VPN客戶端訪問網際網路的過程。

必要條件

需求

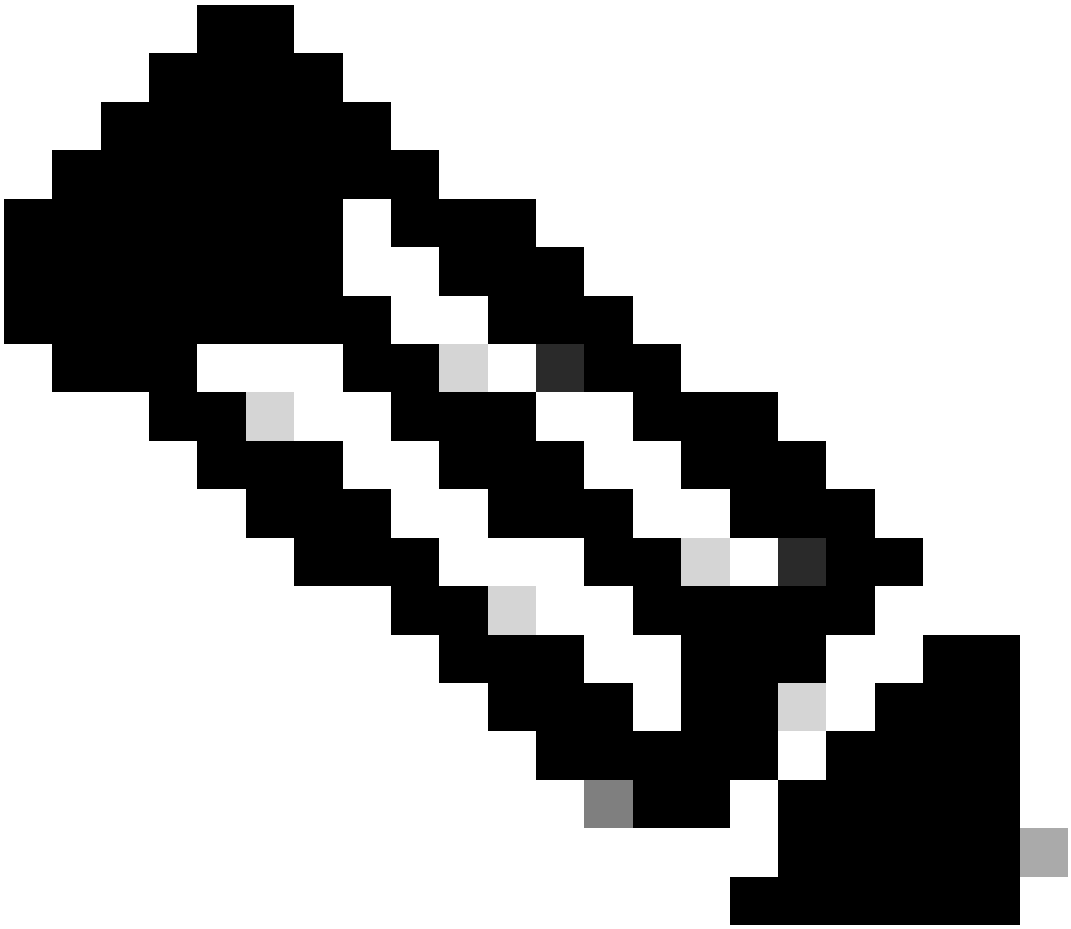
本文檔假設ASA上已存在有效的遠端訪問VPN配置。如果尚未配置PIX/ASA 7.x，請參閱使用ASDM將其配置為遠端VPN伺服器的配置示例。

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4.0.5版
- 調適型安全裝置管理員(ASDM)

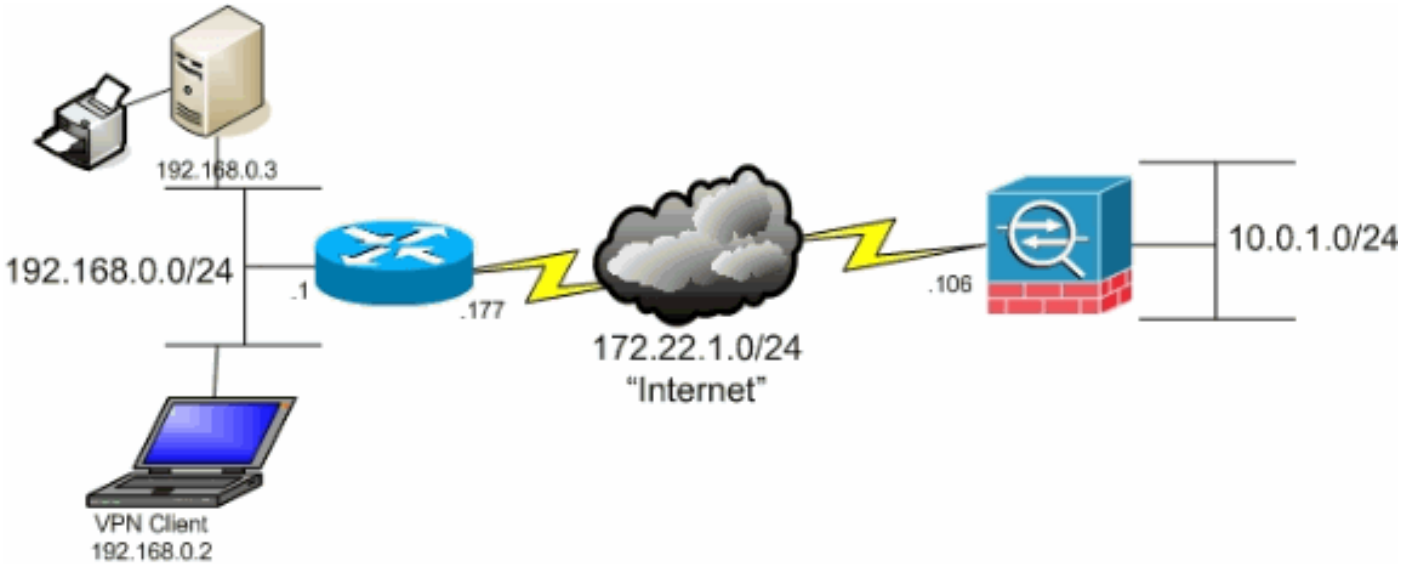


注意：本文檔還包含與Cisco VPN Client 3.x相容的PIX 6.x CLI配置。

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。如果您的網路運作中，請確保您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網路中，透過Internet連線到總部。



網路圖表

相關產品

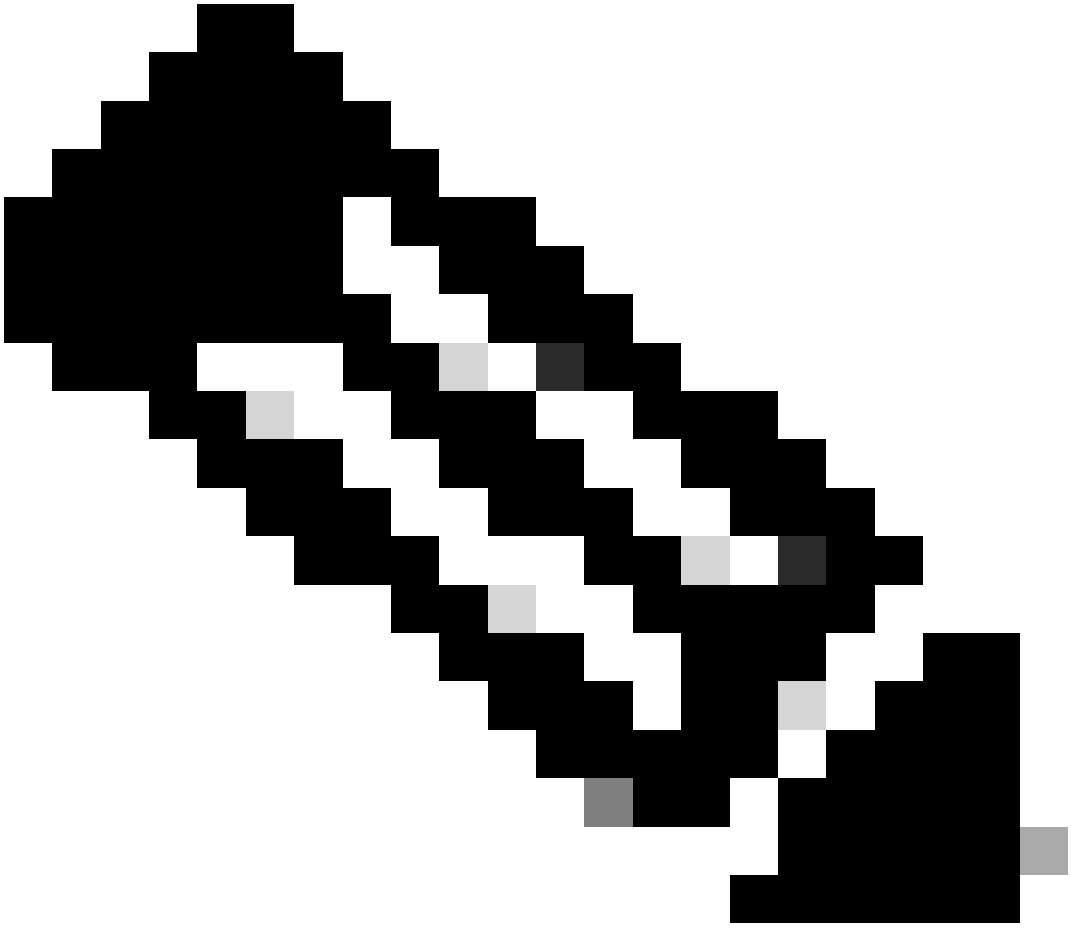
此配置還可用於Cisco PIX 500系列安全裝置軟體版本7.x。

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

本文檔提供有關如何允許VPN客戶端在透過隧道連線到Cisco自適應安全裝置(ASA) 5500系列安全裝置時訪問網際網路的分步說明。此配置允許VPN Client透過IPsec安全地訪問公司資源，同時提供對Internet的不安全訪問。



注意：完全隧道配置被視為最安全的配置，因為它不支援同時裝置訪問Internet和公司LAN。全隧道和分割隧道之間的折衷方案僅允許VPN客戶端訪問本地LAN。有關詳細資訊，請參閱PIX/ASA 7.x：允許VPN Client訪問本地LAN的配置示例。

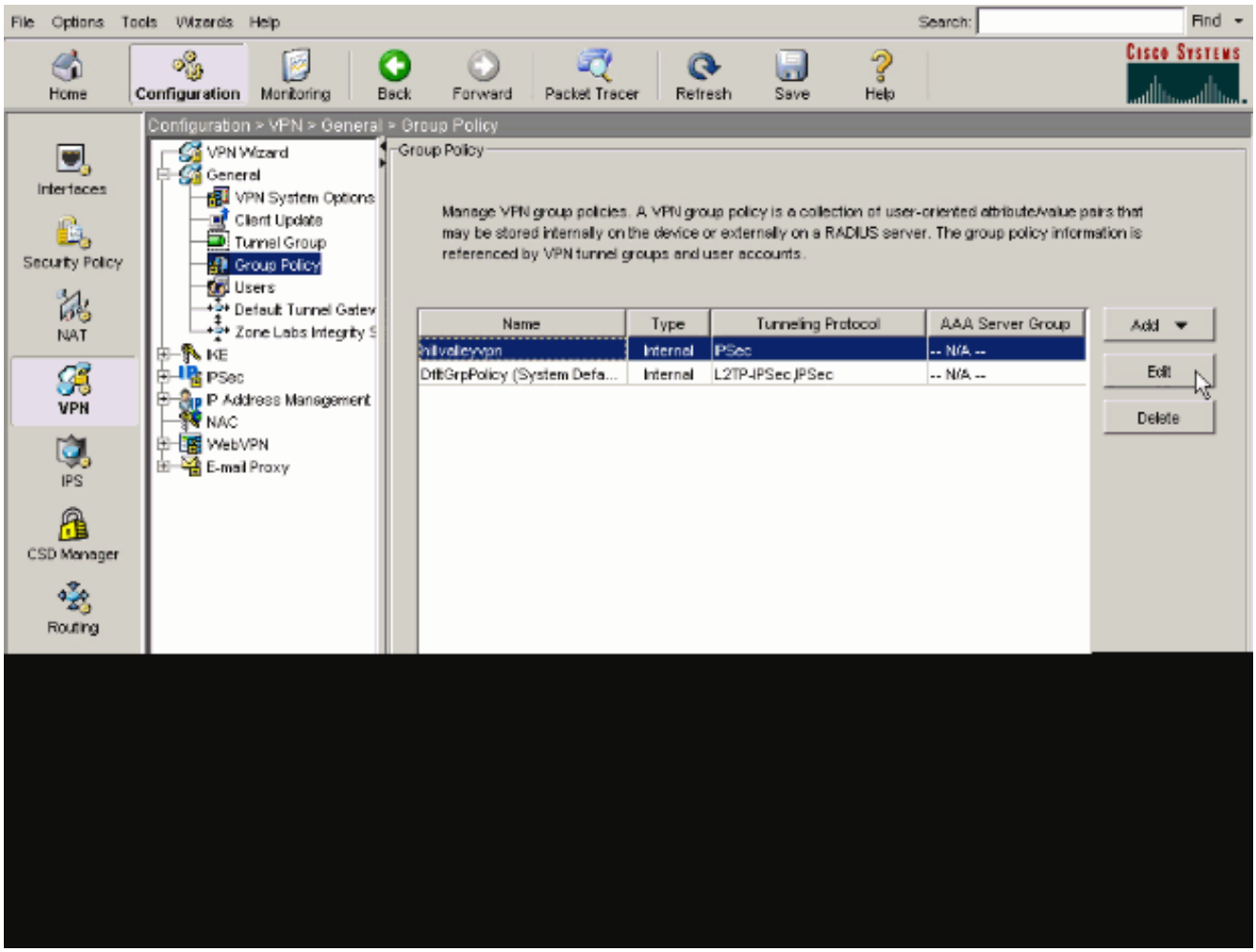
在從VPN客戶端到ASA的基本場景中，來自VPN客戶端的所有流量都會被加密並傳送到ASA，無論其目標是什麼。根據您的配置和支援的使用者數量，此類設定會成為頻寬密集型設定。分割隧道可以緩解此問題，因為它允許使用者透過隧道僅傳送發往企業網路的流量。所有其他流量（如即時消息、電子郵件或臨時瀏覽）透過VPN客戶端的本地LAN傳送到網際網路。

在ASA上配置分割隧道

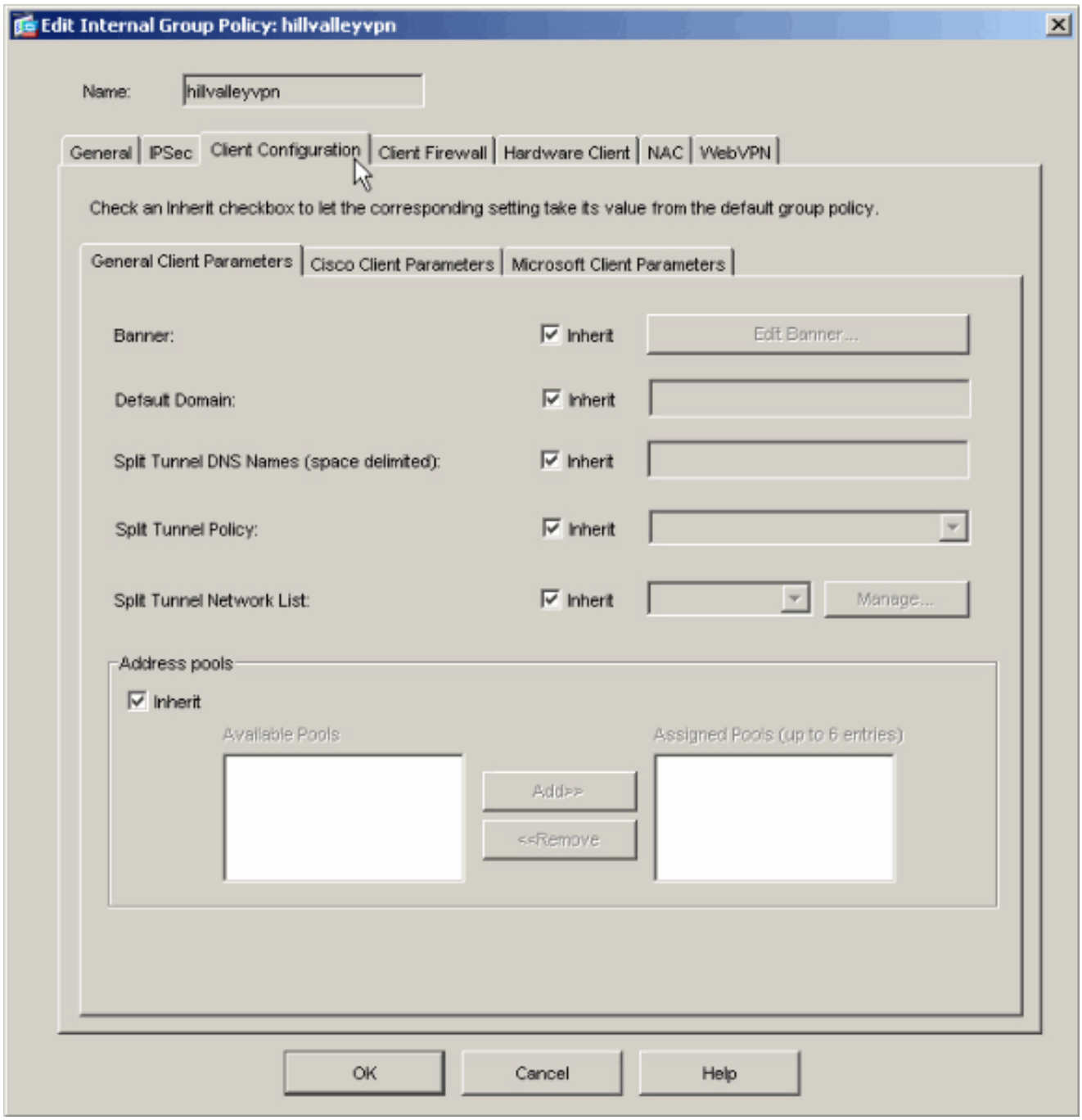
使用自適應安全裝置管理器(ASDM) 5.x配置ASA 7.x

完成以下步驟以配置您的隧道組，以允許對該組中的使用者使用分割隧道。

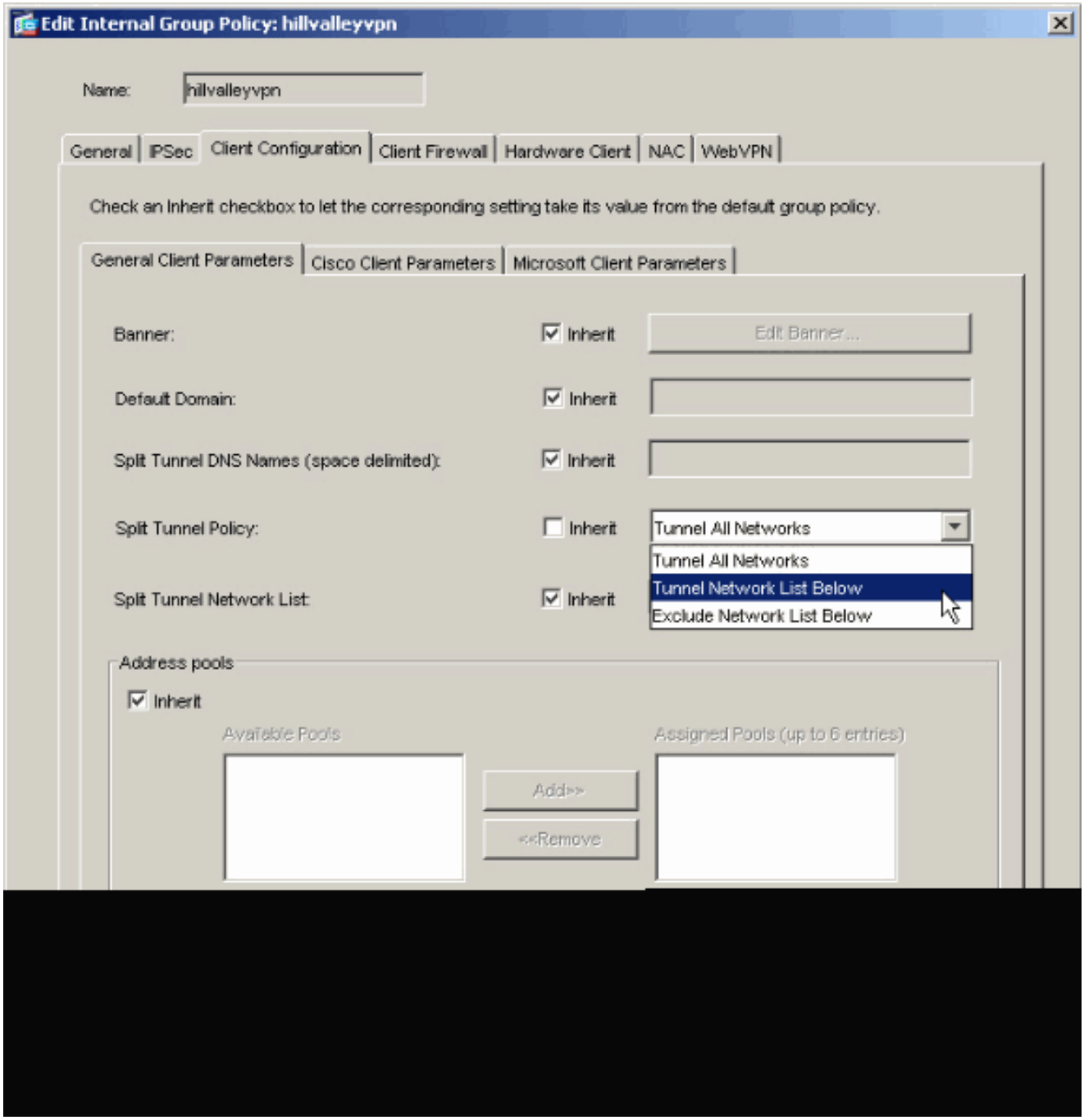
1. 選擇Configuration > VPN > General > Group Policy，並選擇您希望在其中啟用本地LAN訪問的組策略。然後按一下Edit。



2. 轉到Client Configuration頁籤。

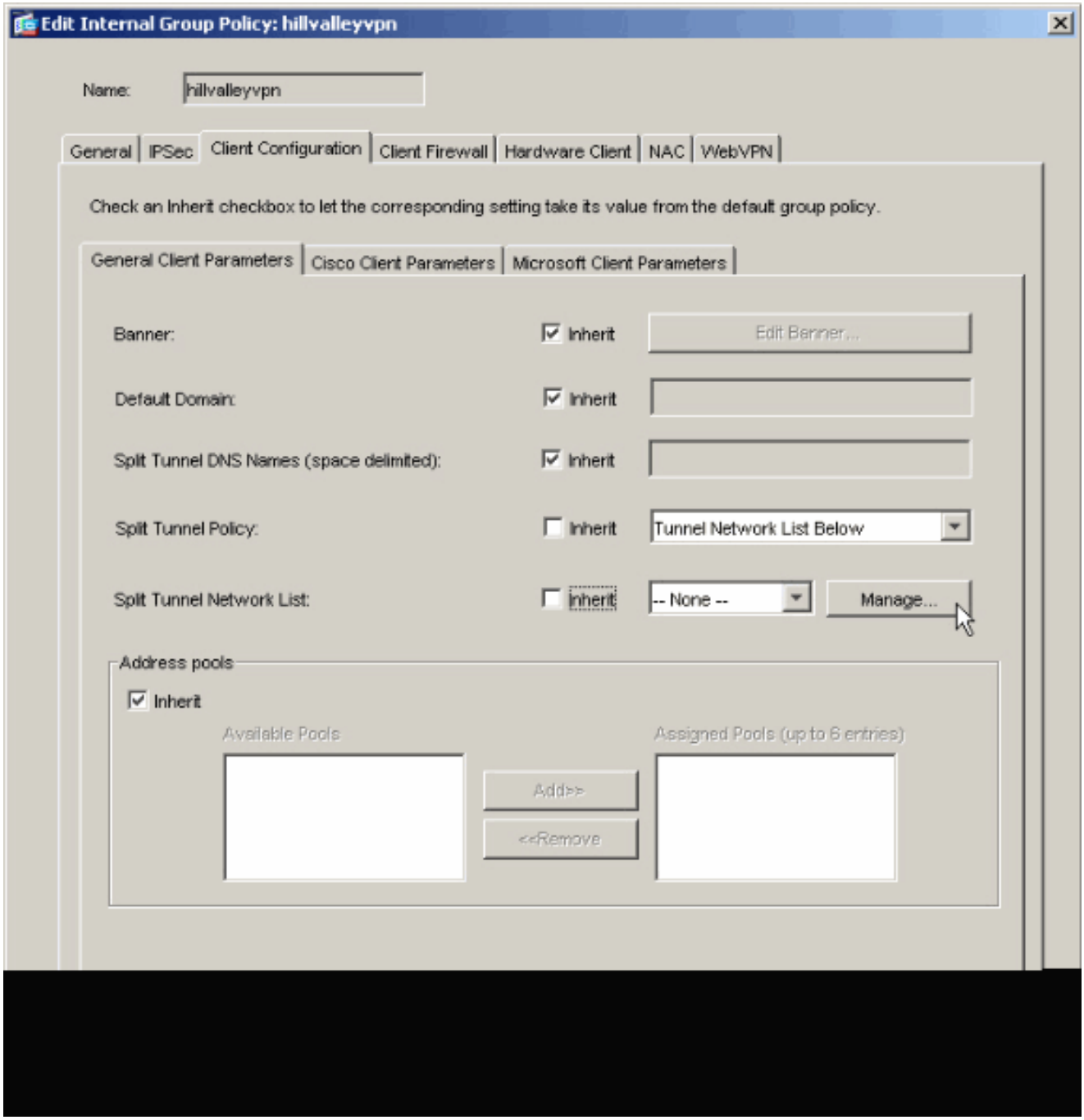


3. 取消選中分割隧道策略的Inherit框，然後選擇Tunnel Network List Below...



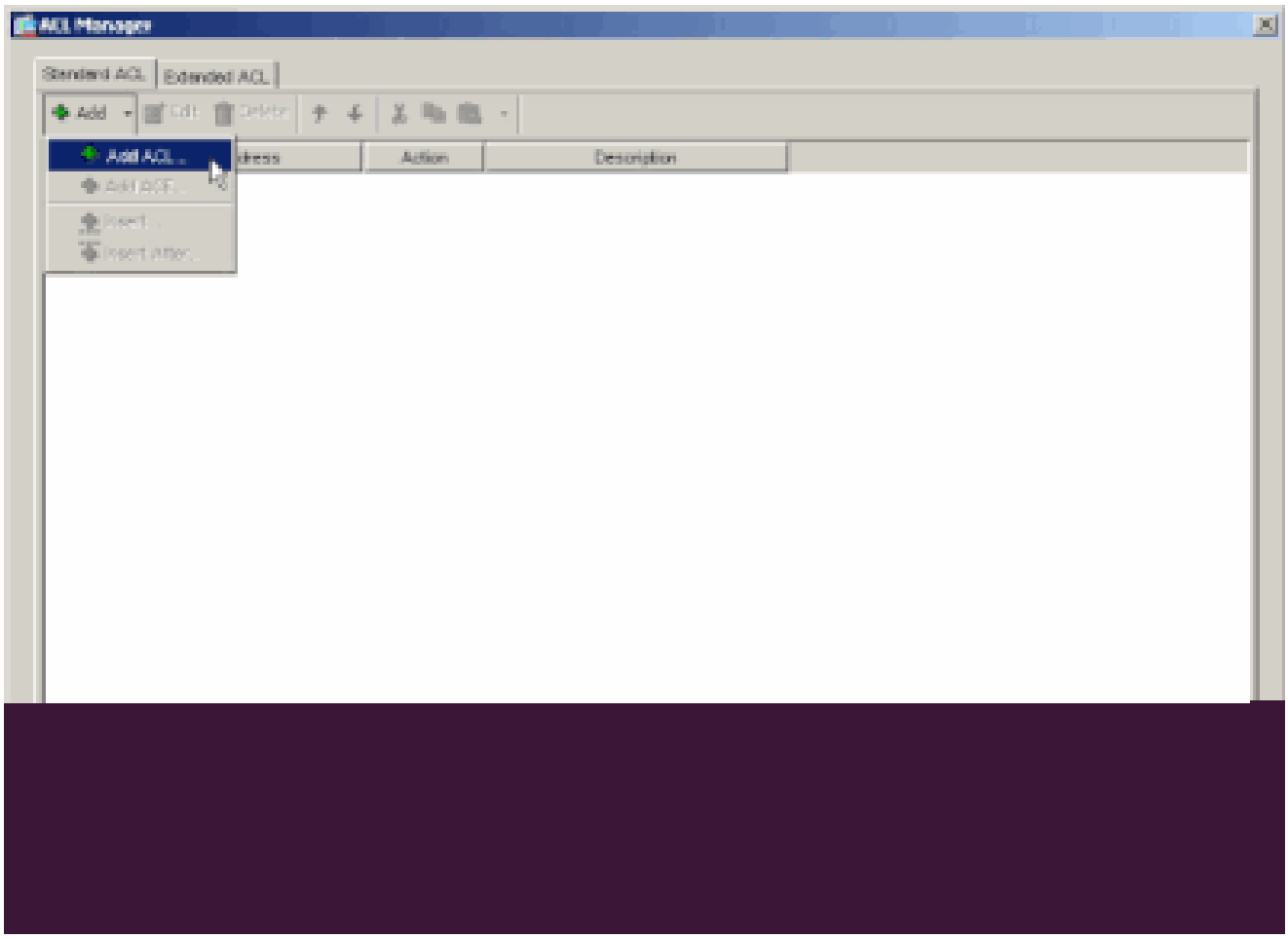
•

取消選中Split Tunnel Network List所對應的**Inherit**框，然後按一下**Manage**啟動ACL Manager。



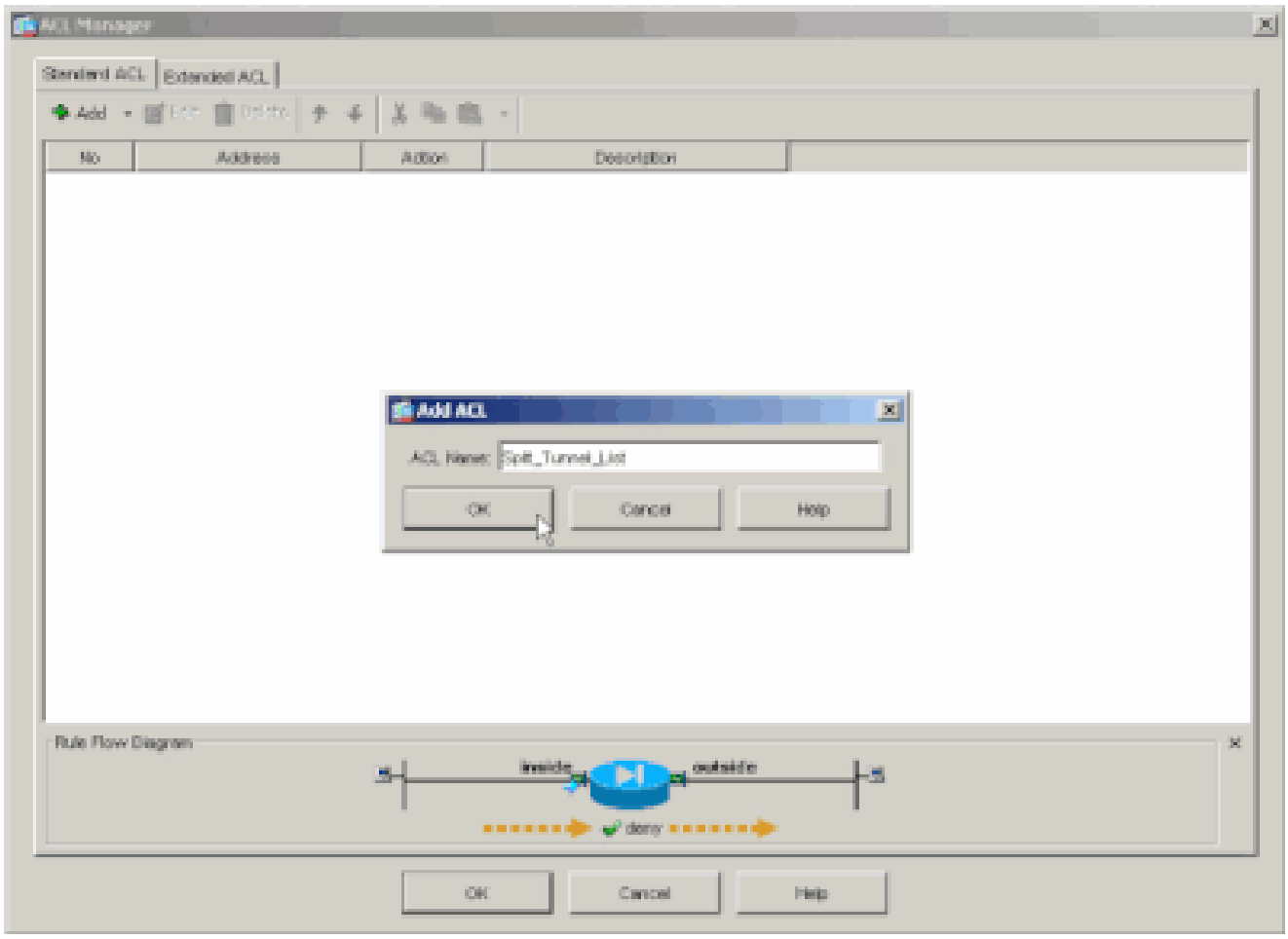
•

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



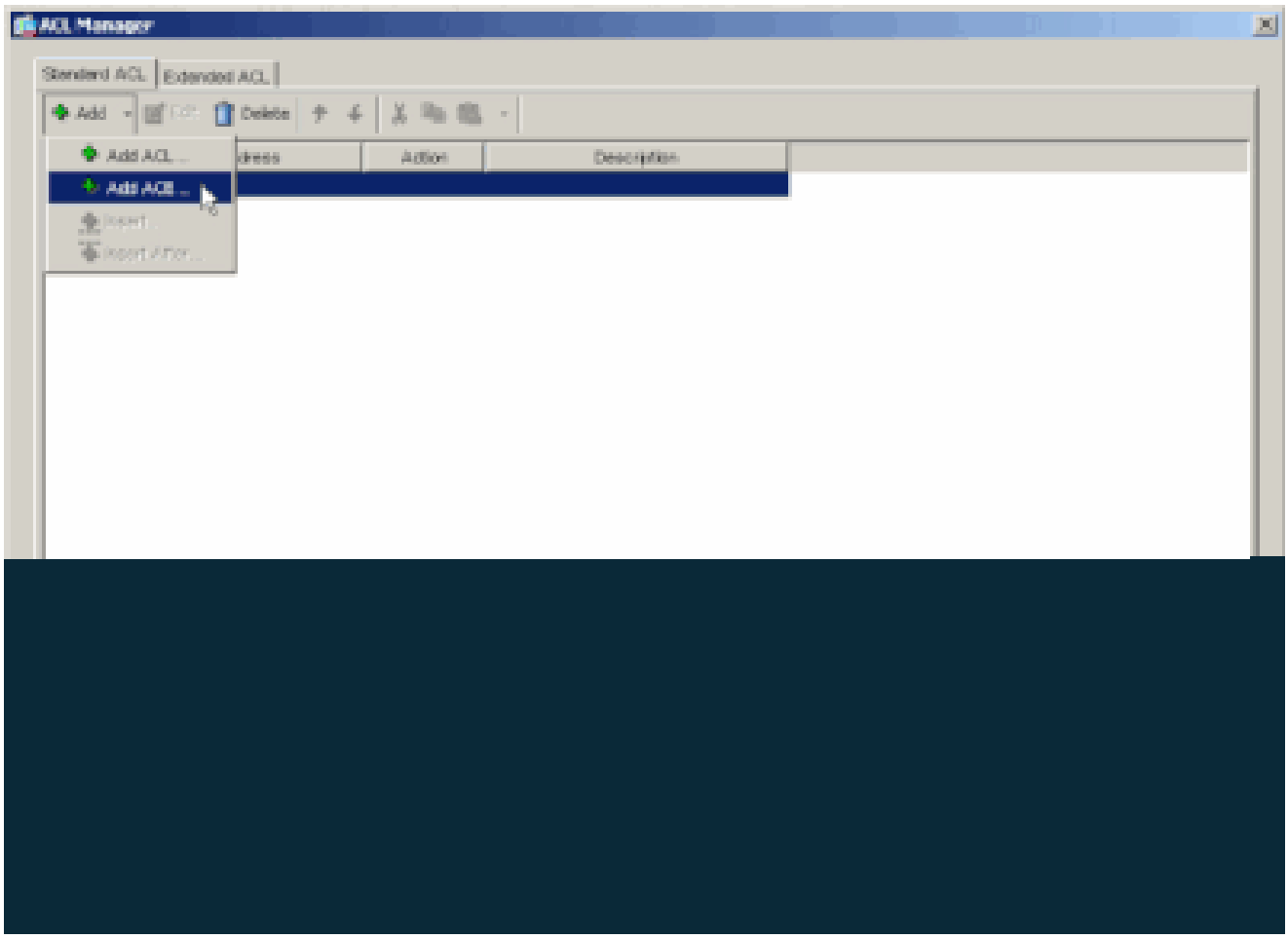
-

為此ACL提供一個名稱，然後按一下**OK**。



•

建立ACL後，選擇**Add > Add ACE**。.以便增加訪問控制條目(ACE)。



-

定義與ASA後面的LAN對應的ACE。在本例中，網路是10.0.1.0/24。

a.

選擇Permit。

b.

選擇IP地址10.0.1.0

c.

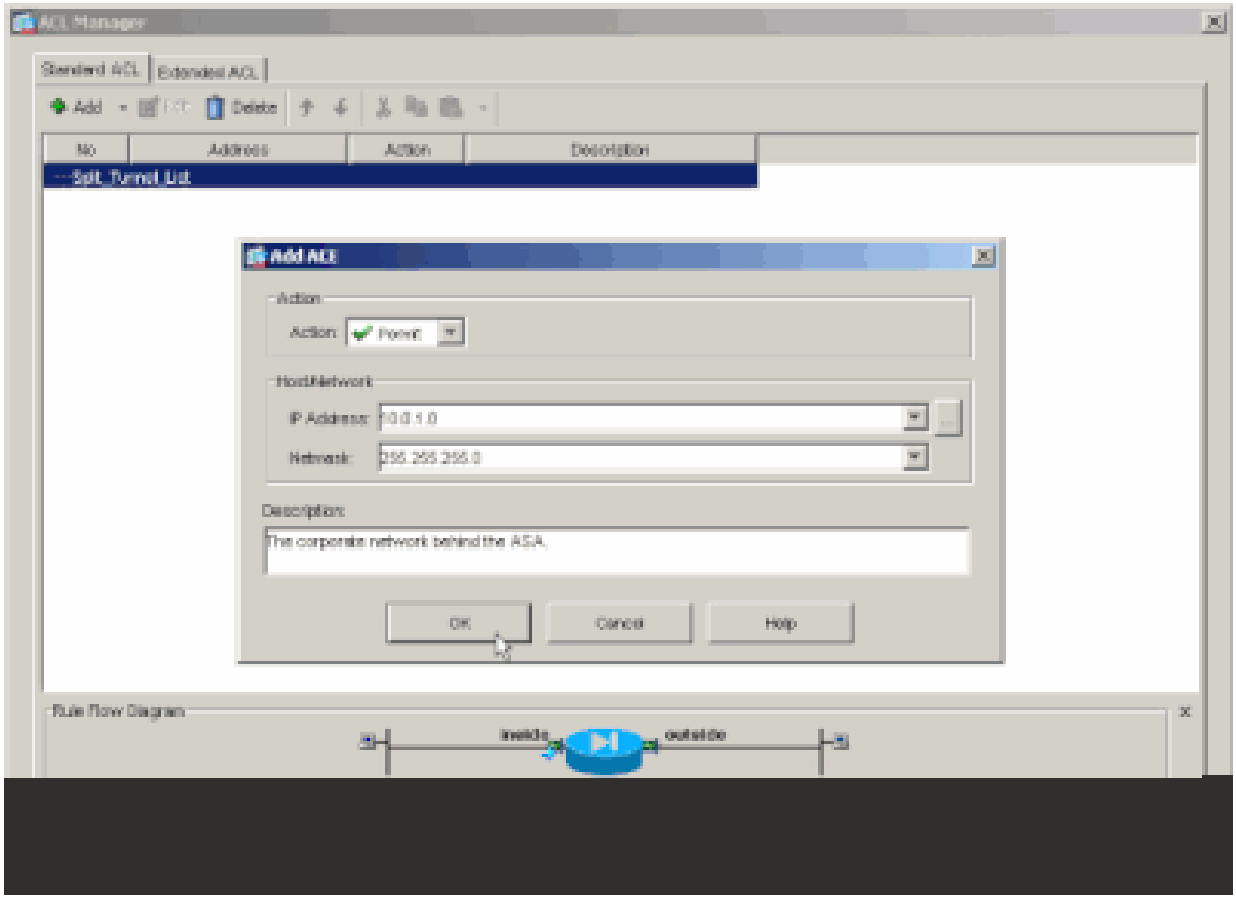
選擇網路掩碼255.255.255.0。

d.

（可選）提供說明。

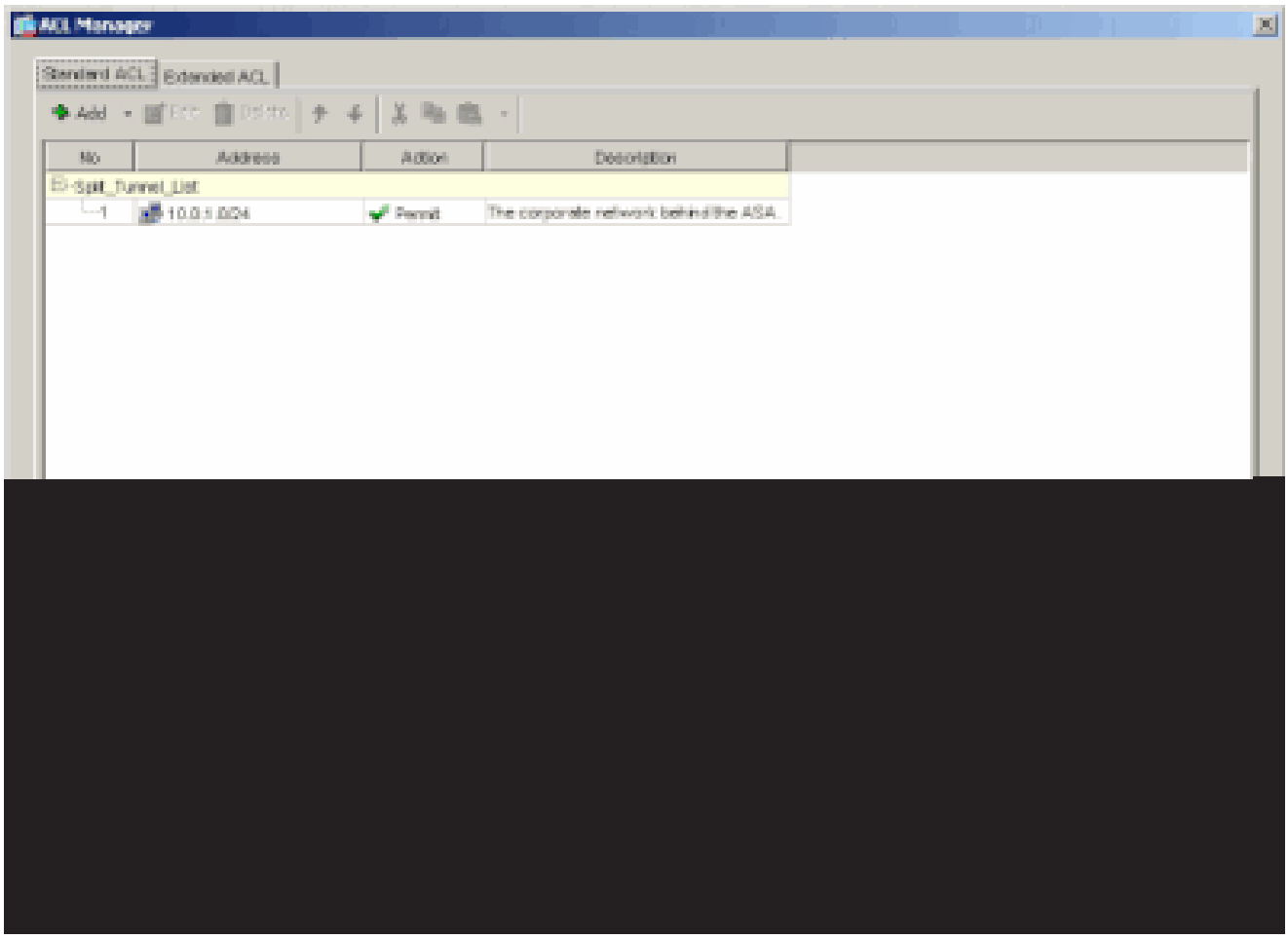
e.

按一下>「確定」。



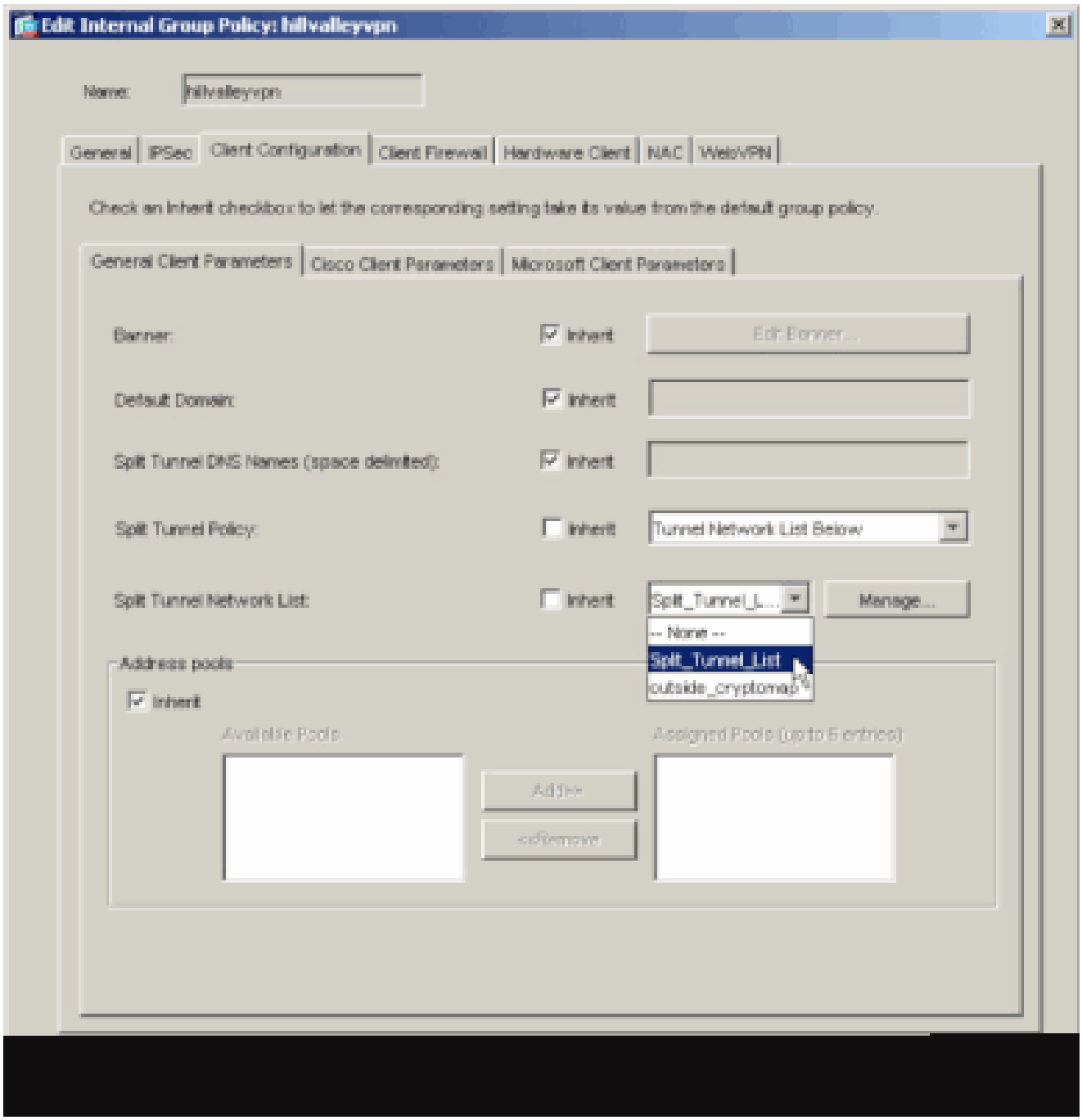
•

按一下**OK** 以退出ACL Manager。



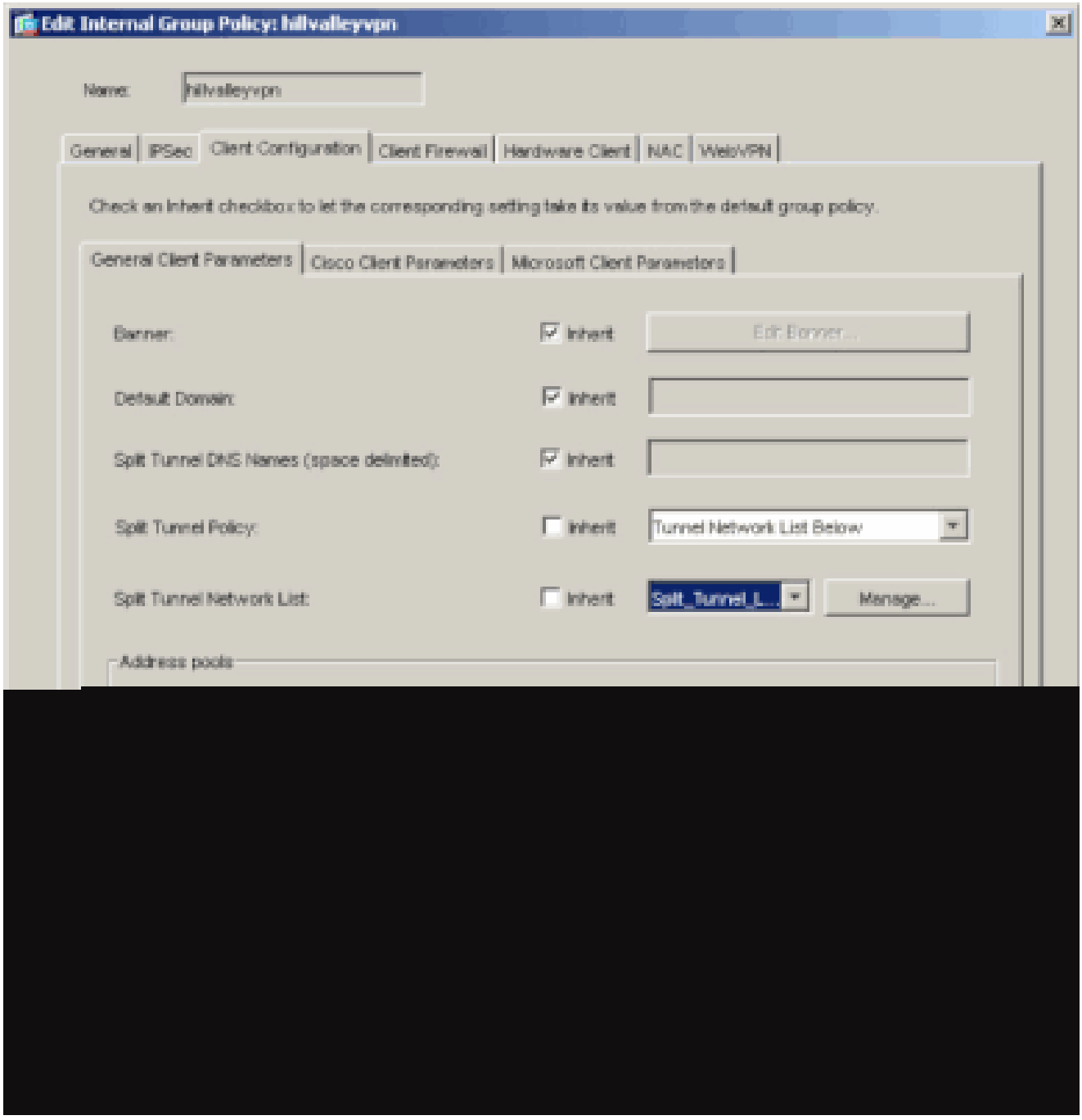
•

確保您剛剛建立的ACL已為Split Tunnel Network List選中。



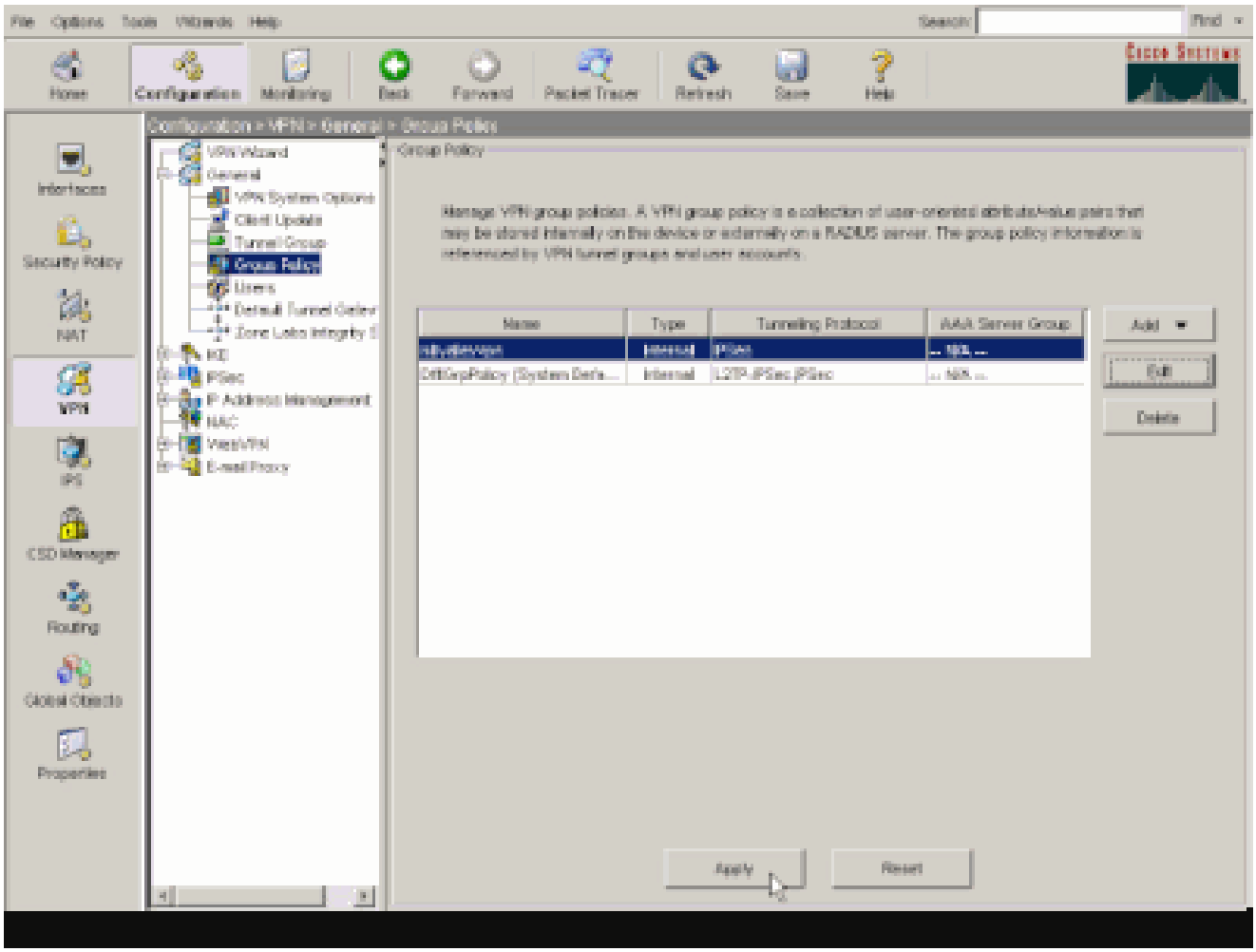
•

按一下**OK** 以返回組策略配置。



•

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

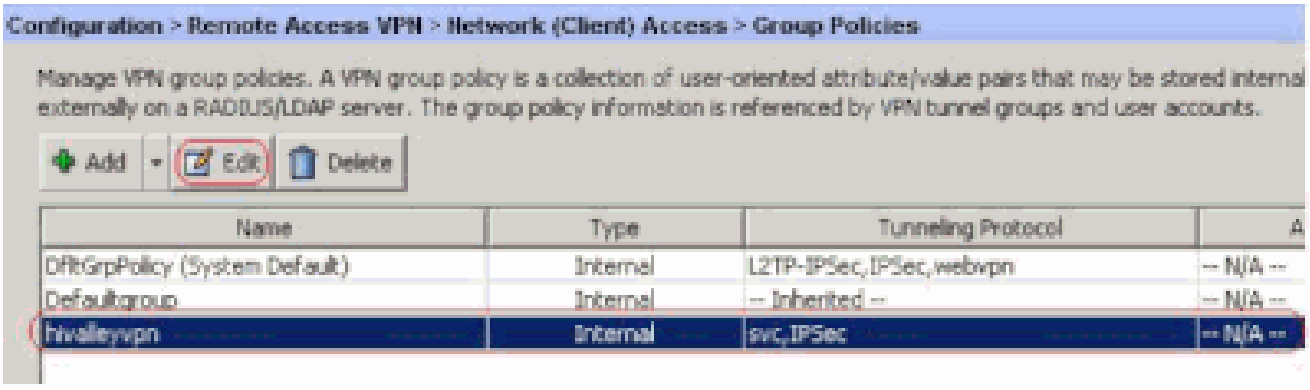


使用ASDM 6.x配置ASA 8.x

完成以下步驟以配置您的隧道組，以允許對該組中的使用者使用分割隧道。

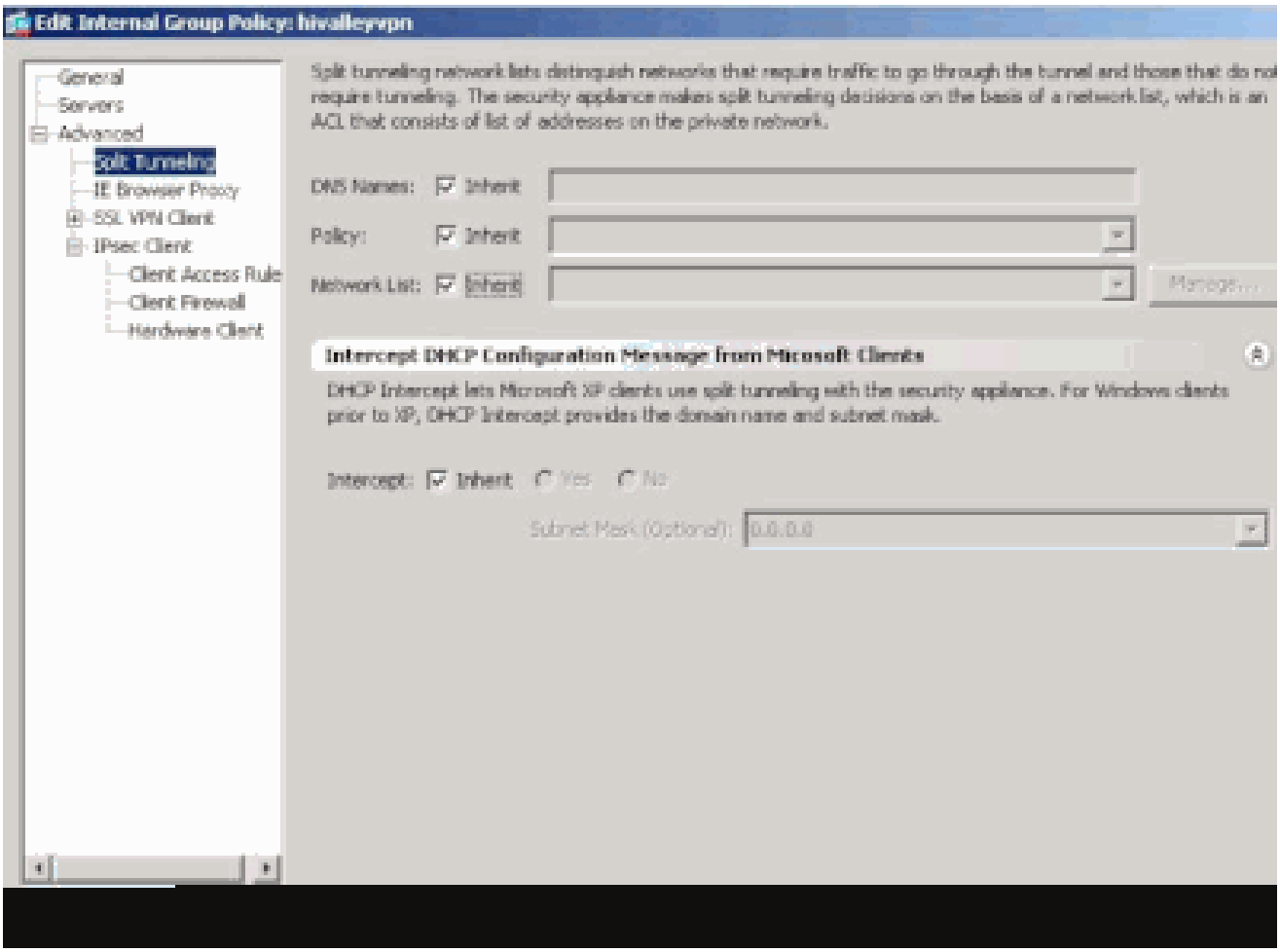
-

選擇**Configuration > Remote Access VPN > Network (Client) Access > Group Policies**，並選擇您希望在其中啟用本地LAN訪問的組策略。然後按一下**Edit**。



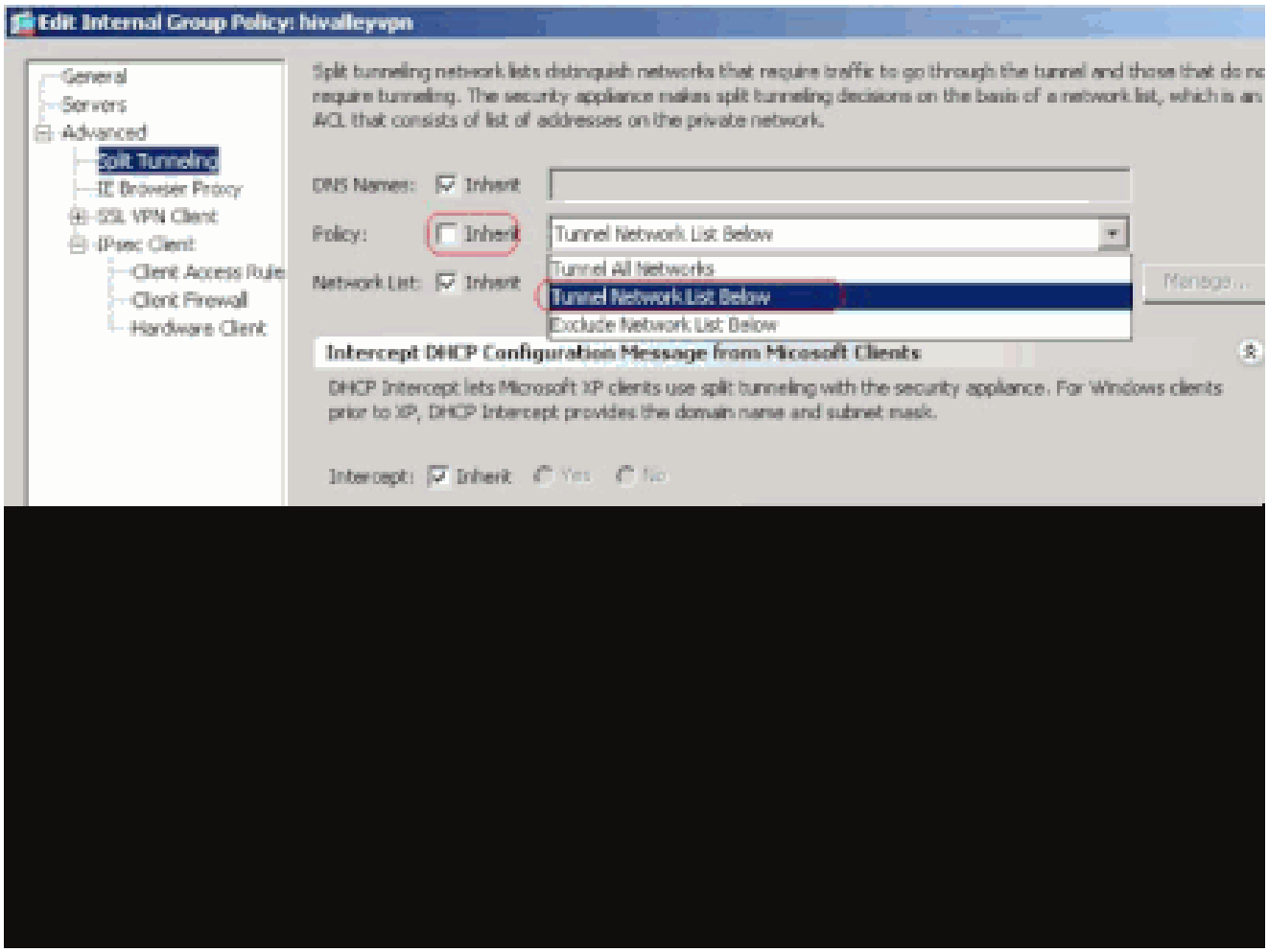
-

按一下**Split Tunneling**。



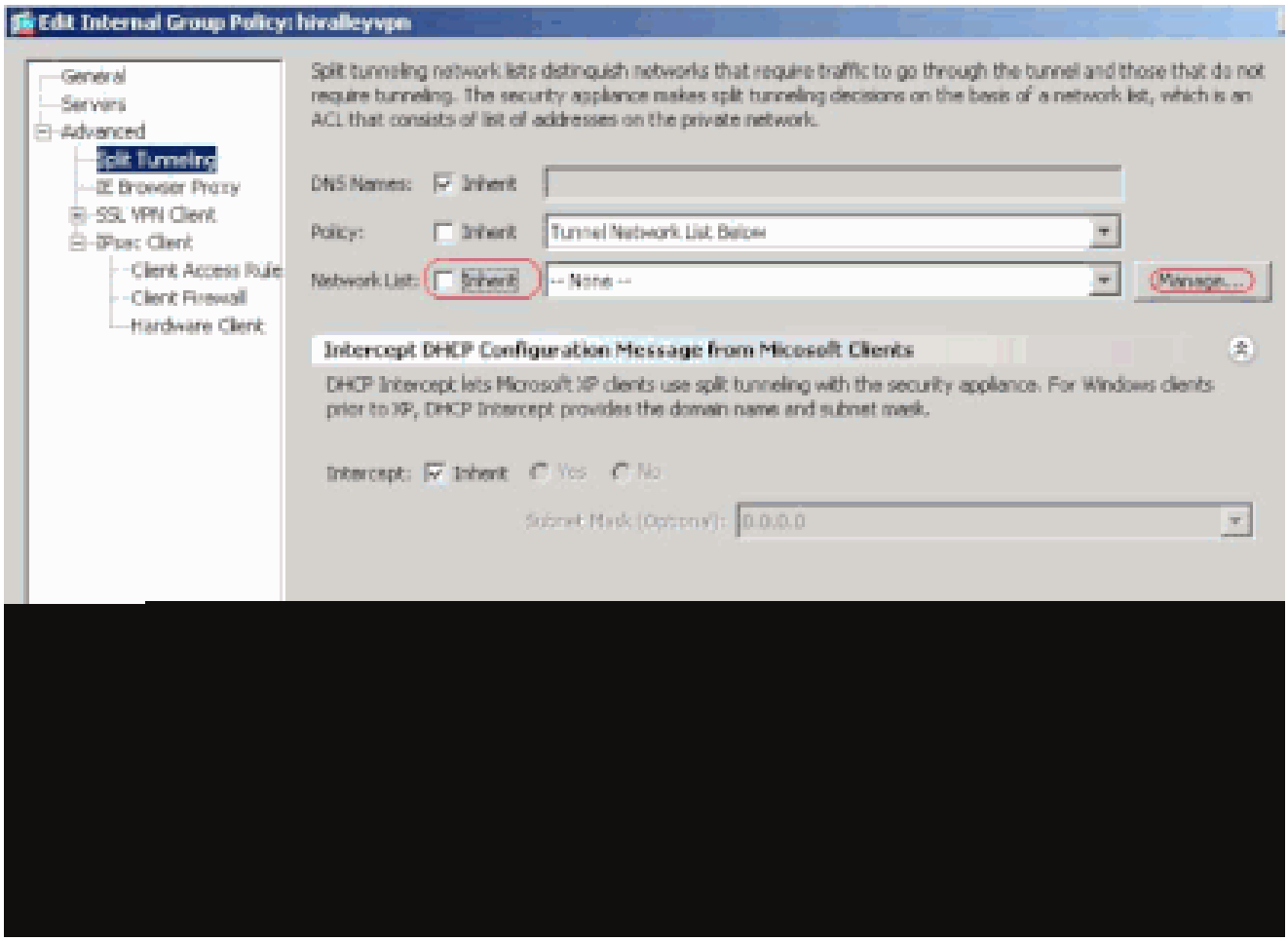
-

取消選中Split Tunnel Policy所對應的**Inherit**框，然後選擇**Tunnel Network List Below**。



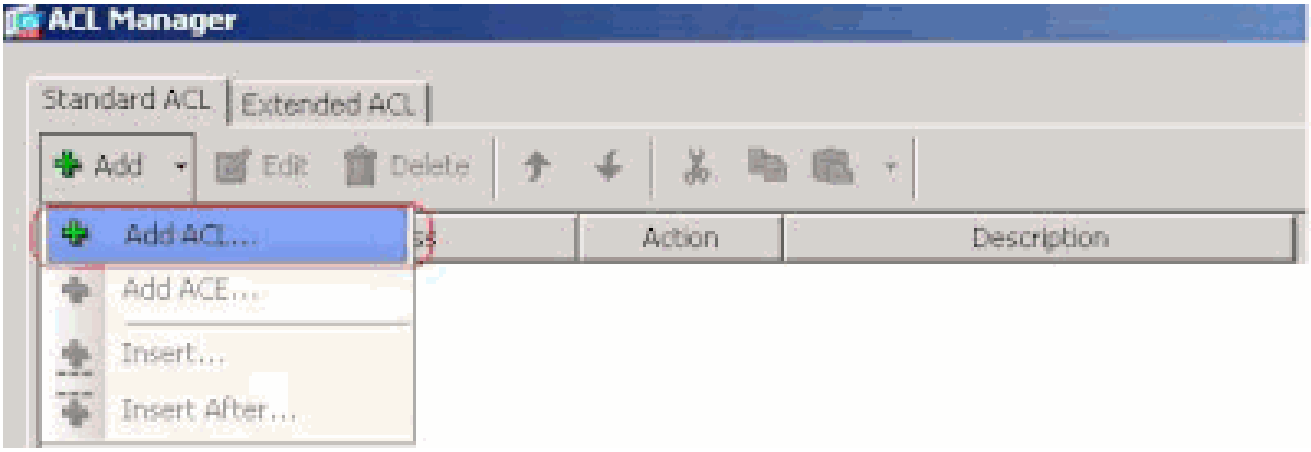
•

取消選中Split Tunnel Network List所對應的**Inherit**框，然後按一下**Manage**啟動ACL Manager。



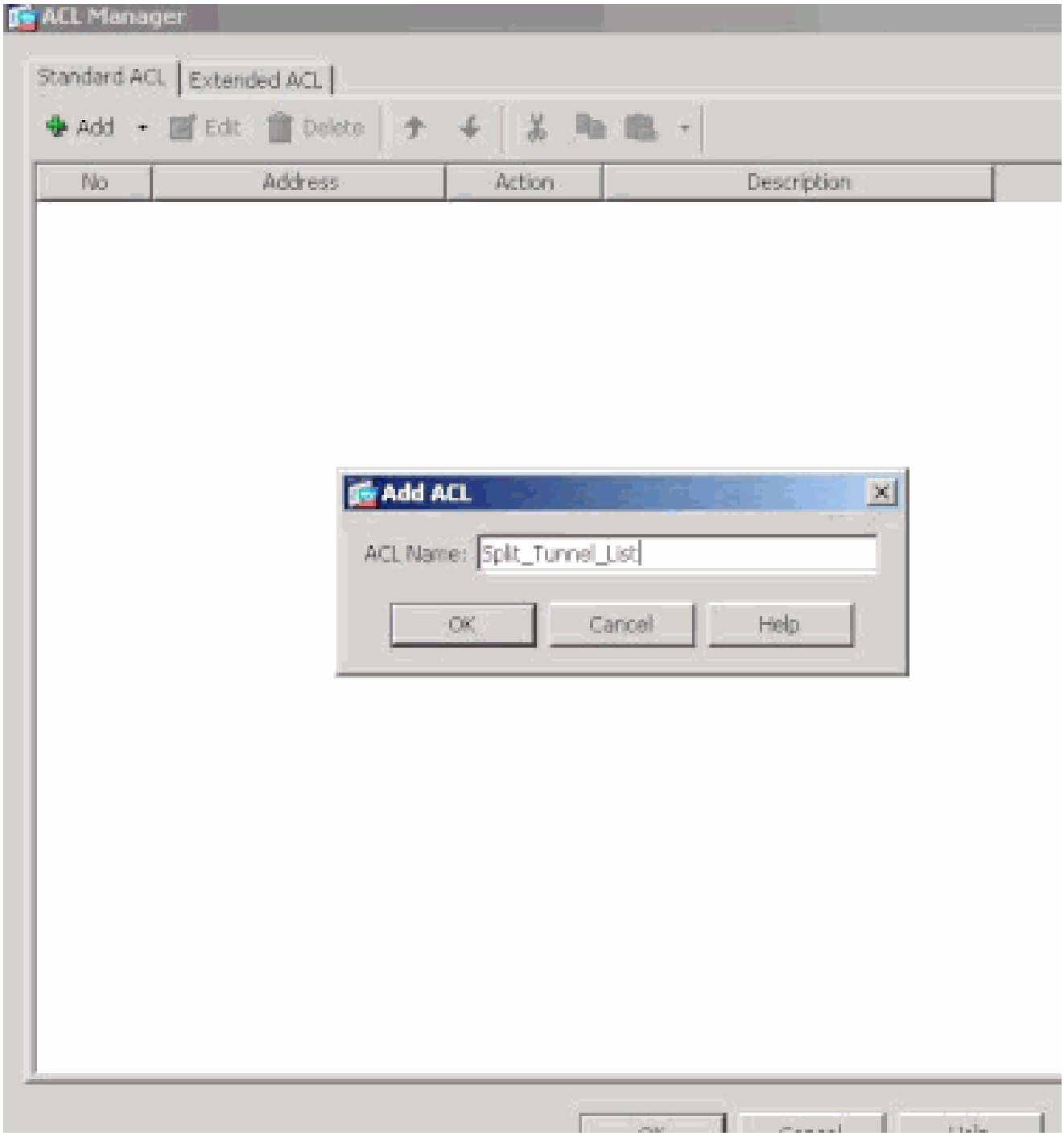
-

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



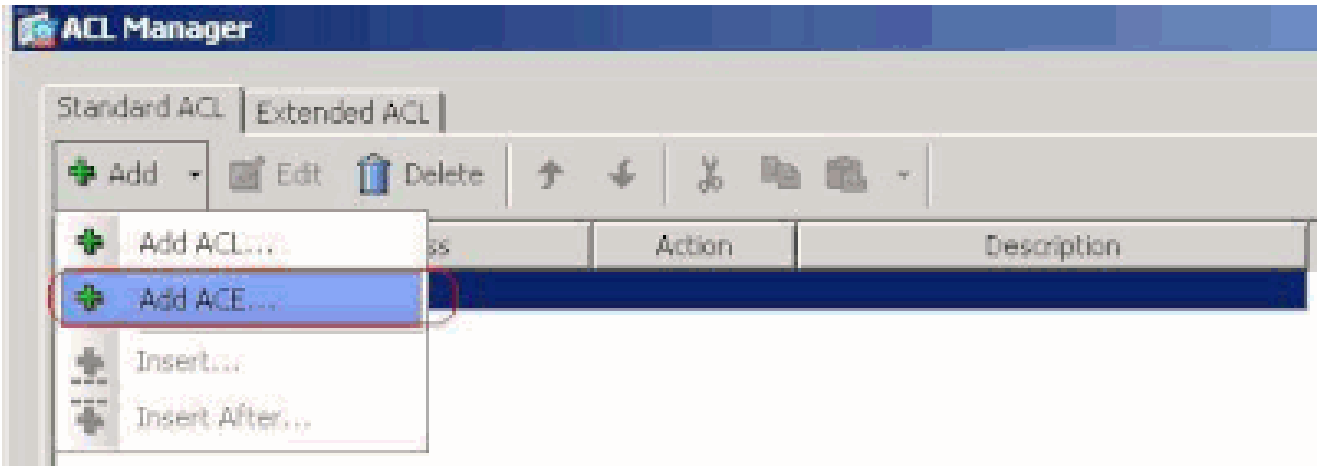
-

為ACL提供一個名稱，然後按一下**OK**。



-

建立ACL後，選擇**Add > Add ACE...**以增加訪問控制項(ACE)。



-

定義與ASA後面的LAN對應的ACE。在本例中，網路是10.0.1.0/24。

a.

按一下**Permit**單選按鈕。

b.

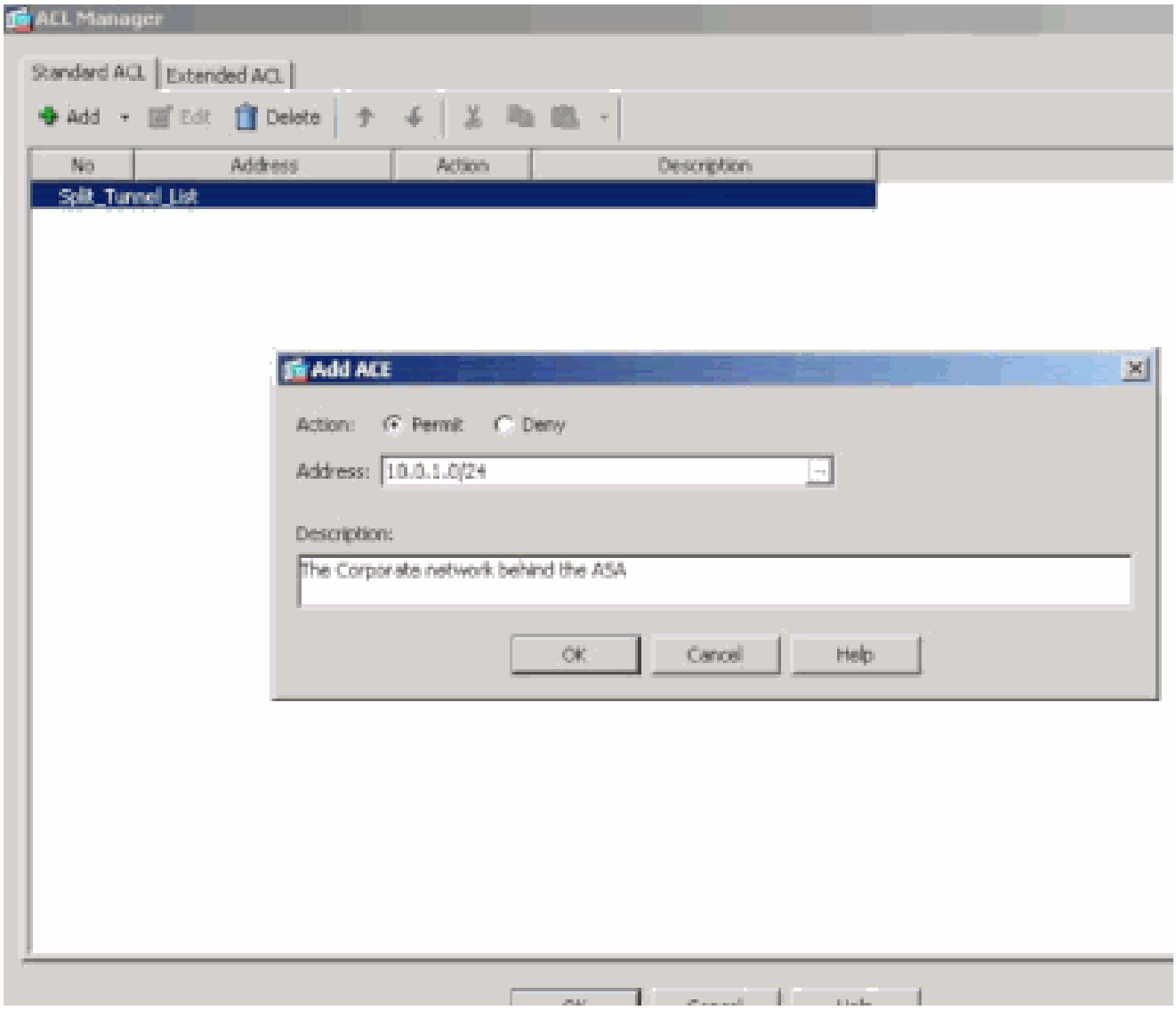
選擇掩碼為**10.0.1.0/24**的網路地址。

c.

（可選）提供說明。

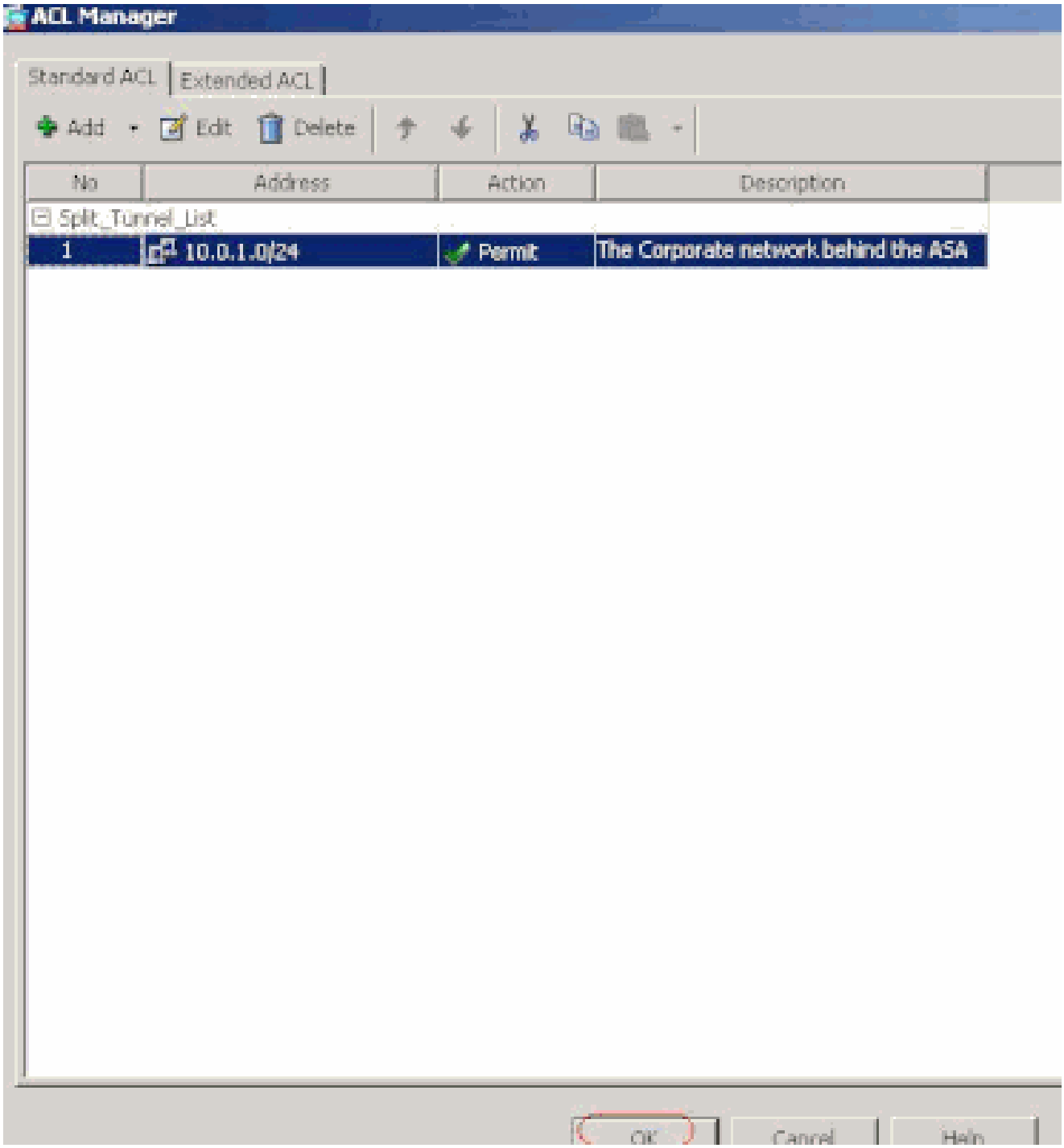
d.

按一下「OK」（確定）。



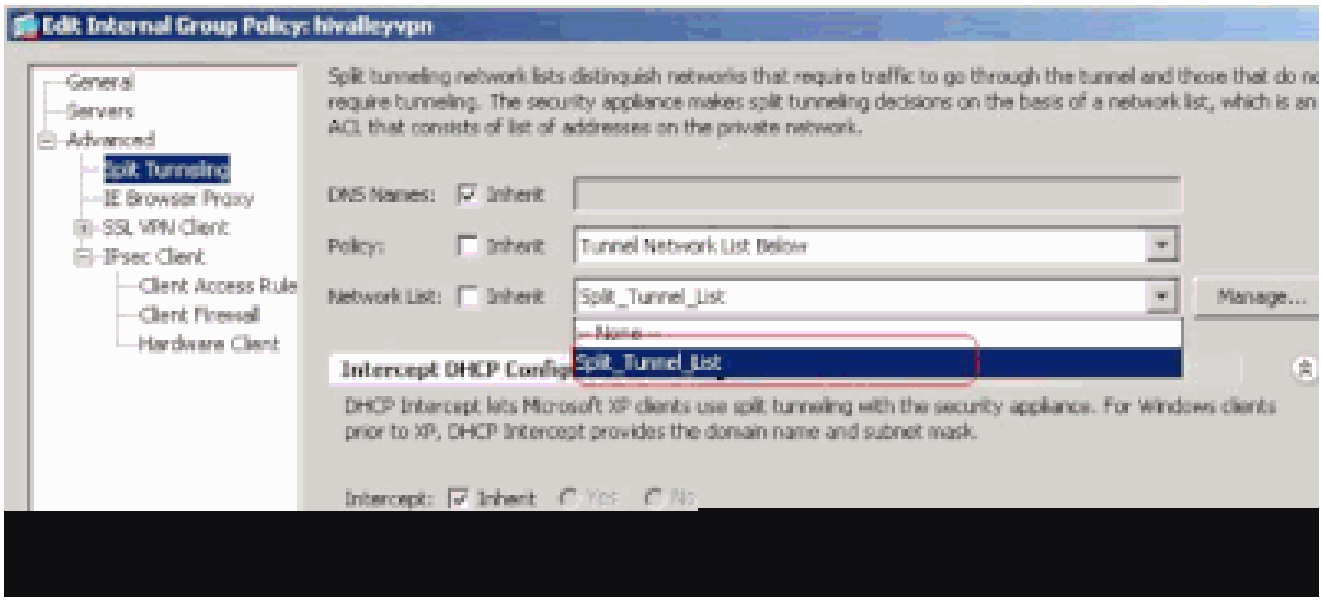
•

按一下**OK** 以退出ACL Manager。



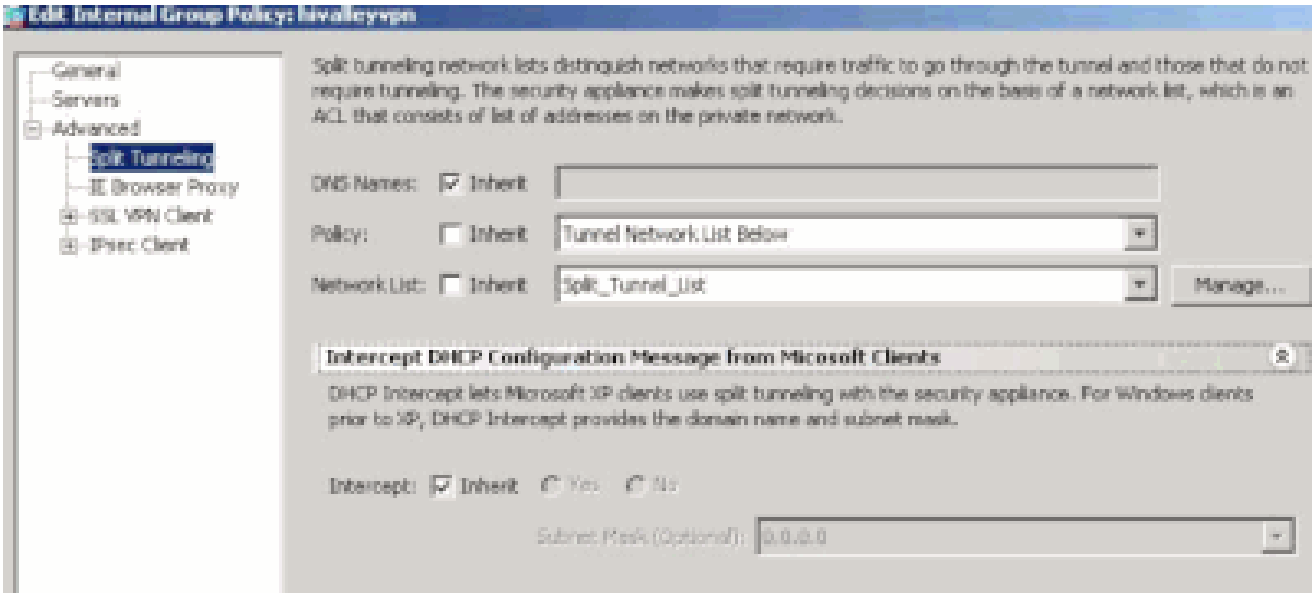
•

確保您剛剛建立的ACL已為Split Tunnel Network List選中。



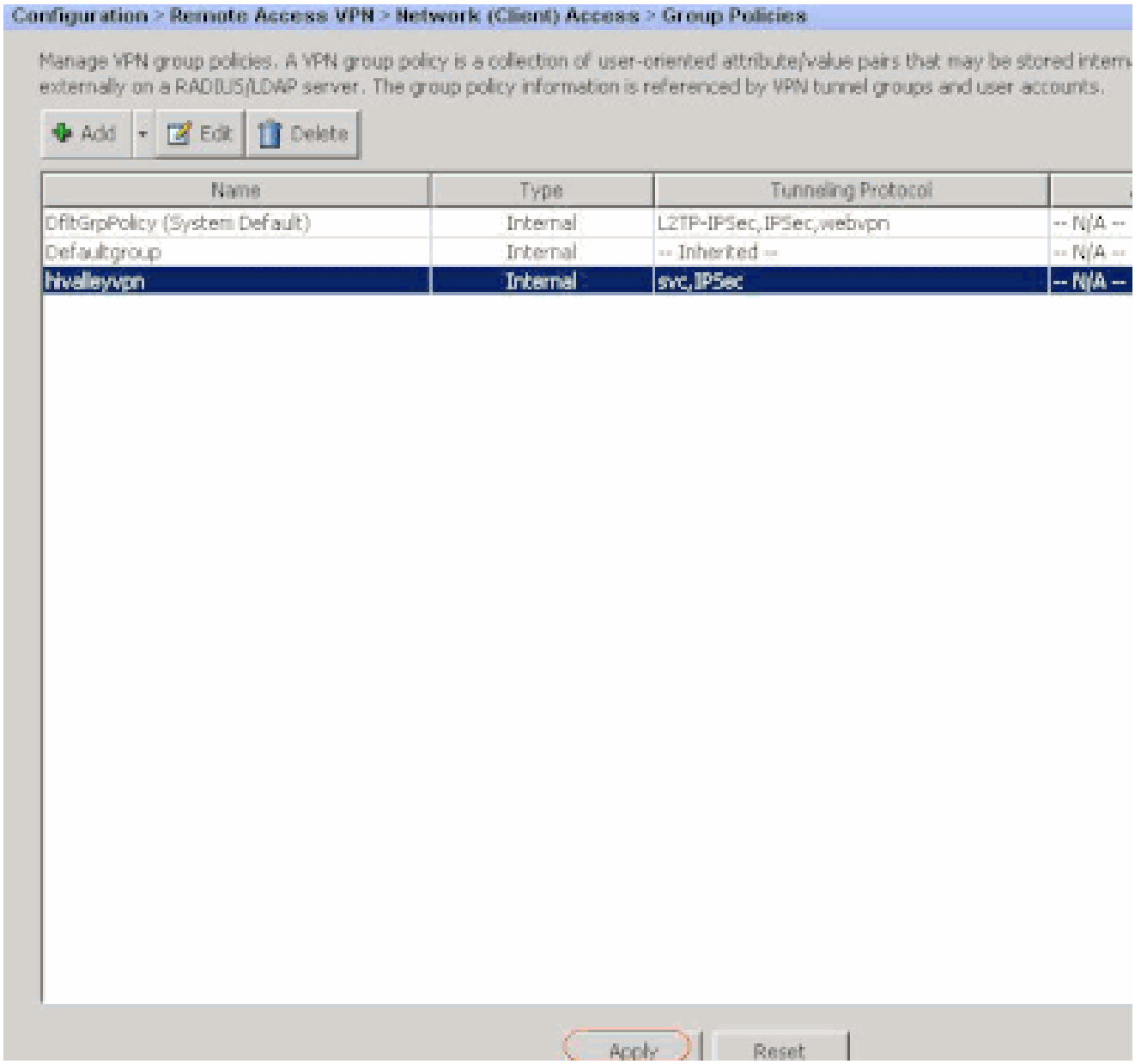
•

按一下**OK** 以返回組策略配置。



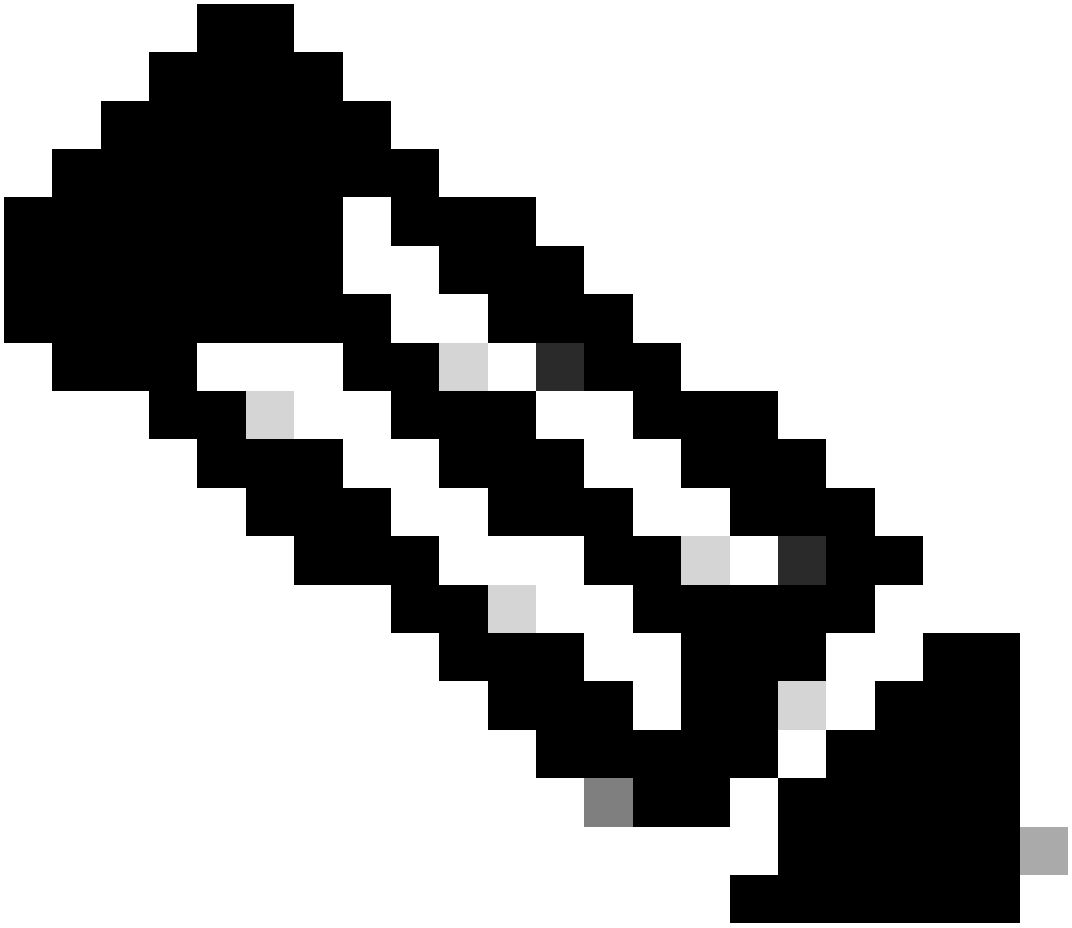
•

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



透過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上允許分割隧道，而不是使用ASDM：



注意：CLI分割隧道配置對於ASA 7.x和8.x均相同。

-

進入配置模式。

```
<#root>

ciscoasa>
```

enable

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

configure terminal

ciscoasa(config)#

- 建立定義ASA後方的網路的訪問清單。

<#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

- 進入要修改的策略的組策略配置模式。

<#root>

```
ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

- 指定拆分隧道策略。在本示例中，此策略為**tunnelspecified**。

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

- 指定拆分隧道訪問清單。在本示例中，此清單為**Split_Tunnel_List**。

```
    <#root>

ciscoasa(config-group-policy)#

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

- 發出以下命令：

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

- 將組策略與隧道組關聯

<#root>

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

- 退出兩種配置模式。

<#root>

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

```
 exit


ciscoasa#
```

- 將配置儲存到非易失性RAM (NVRAM)，並在系統提示指定源檔名時按**Enter**。

```
    <#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#
```

透過CLI配置PIX 6.x

請完成以下步驟：

- 建立定義PIX後方的網路的訪問清單。

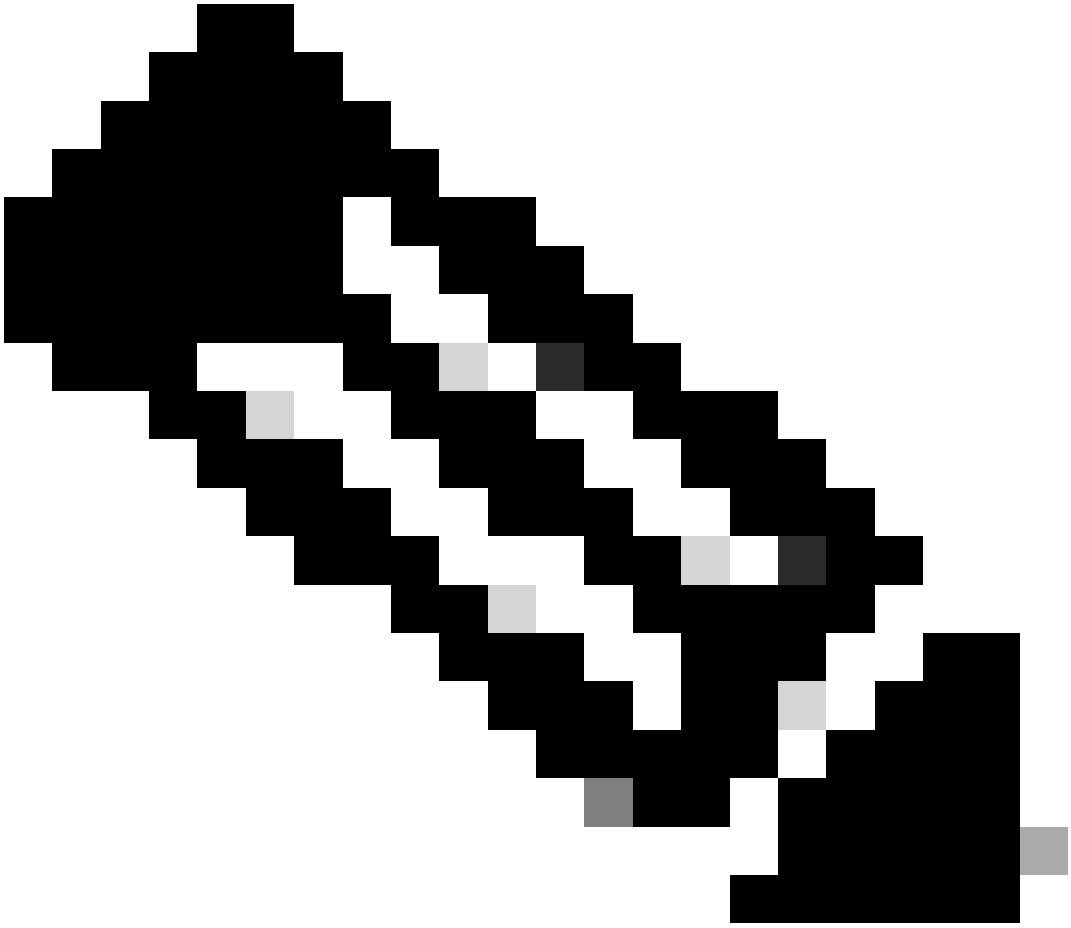
```
    <#root>


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

- 建立一個vpn組**vpn3000**，並向其指定分割隧道ACL，如下所示：

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



注意：有關PIX 6.x的遠端訪問VPN配置的詳細資訊，請參閱使用Microsoft Windows 2000和2003 IAS RADIUS身份驗證配置適用於Windows的Cisco Secure PIX Firewall 6.x和Cisco VPN客戶端3.5。

驗證

完成以下部分中的步驟以驗證您的配置。

- 連線VPN客戶端

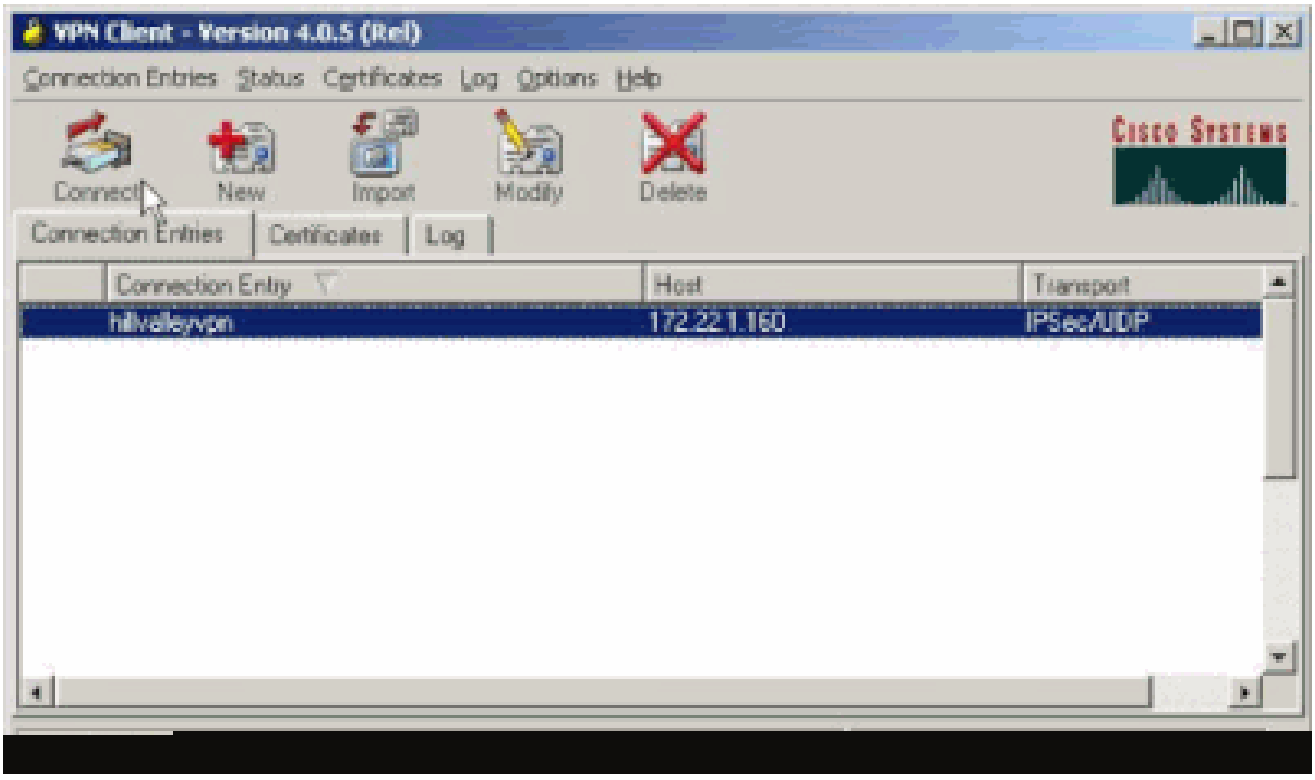
- 檢視VPN客戶端日誌

- 使用Ping測試本地LAN訪問

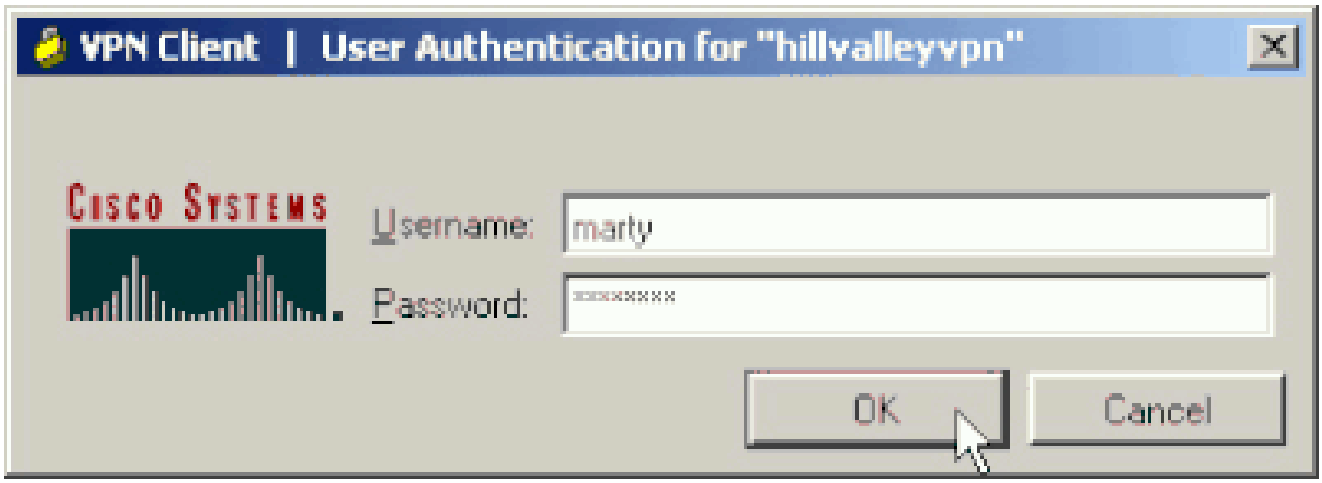
連線VPN客戶端

將您的VPN客戶端連線到VPN集中器以驗證您的配置。

- 從清單中選擇連線條目，並按一下**Connect**。

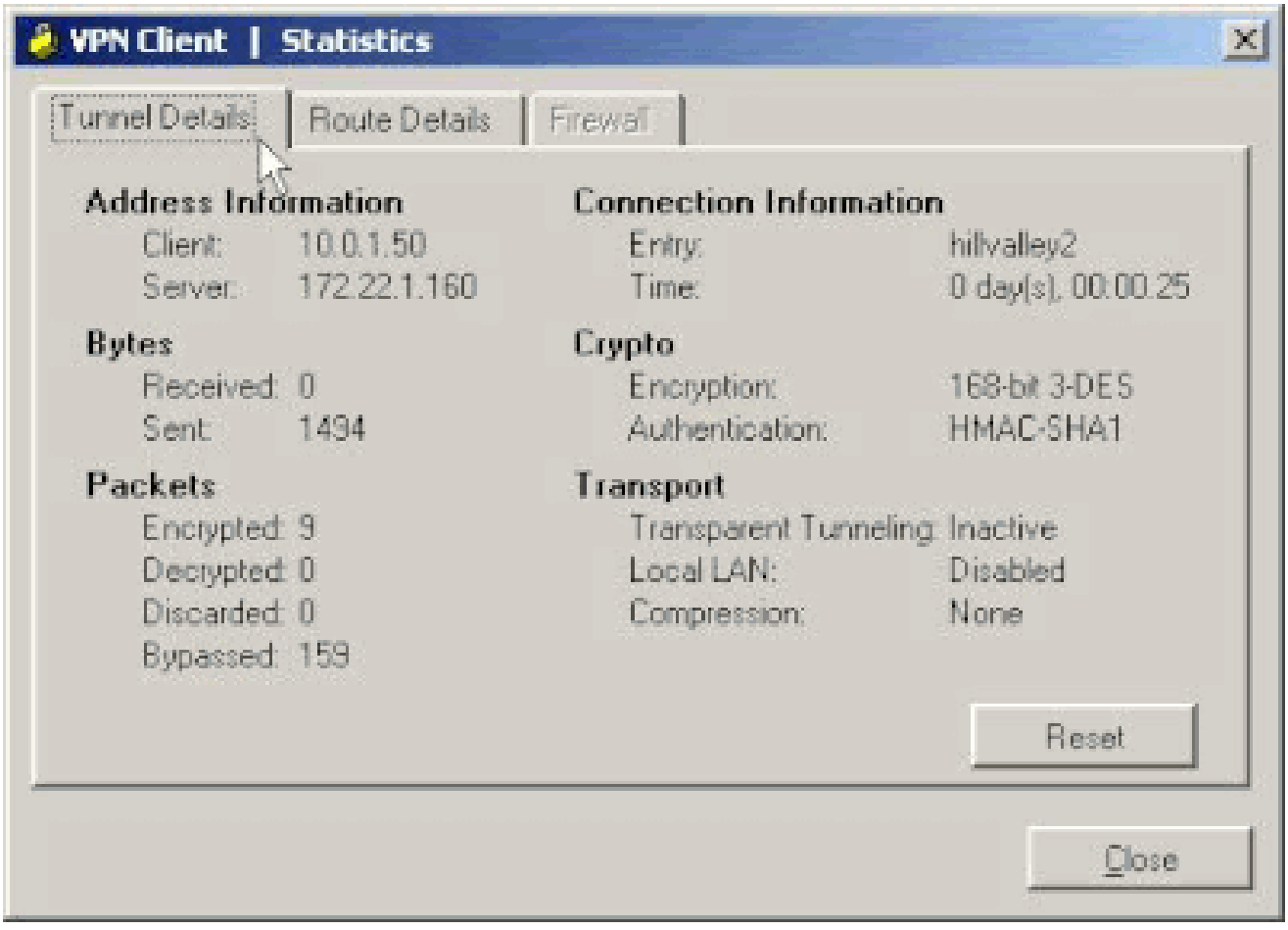


- 輸入您的認證。



•

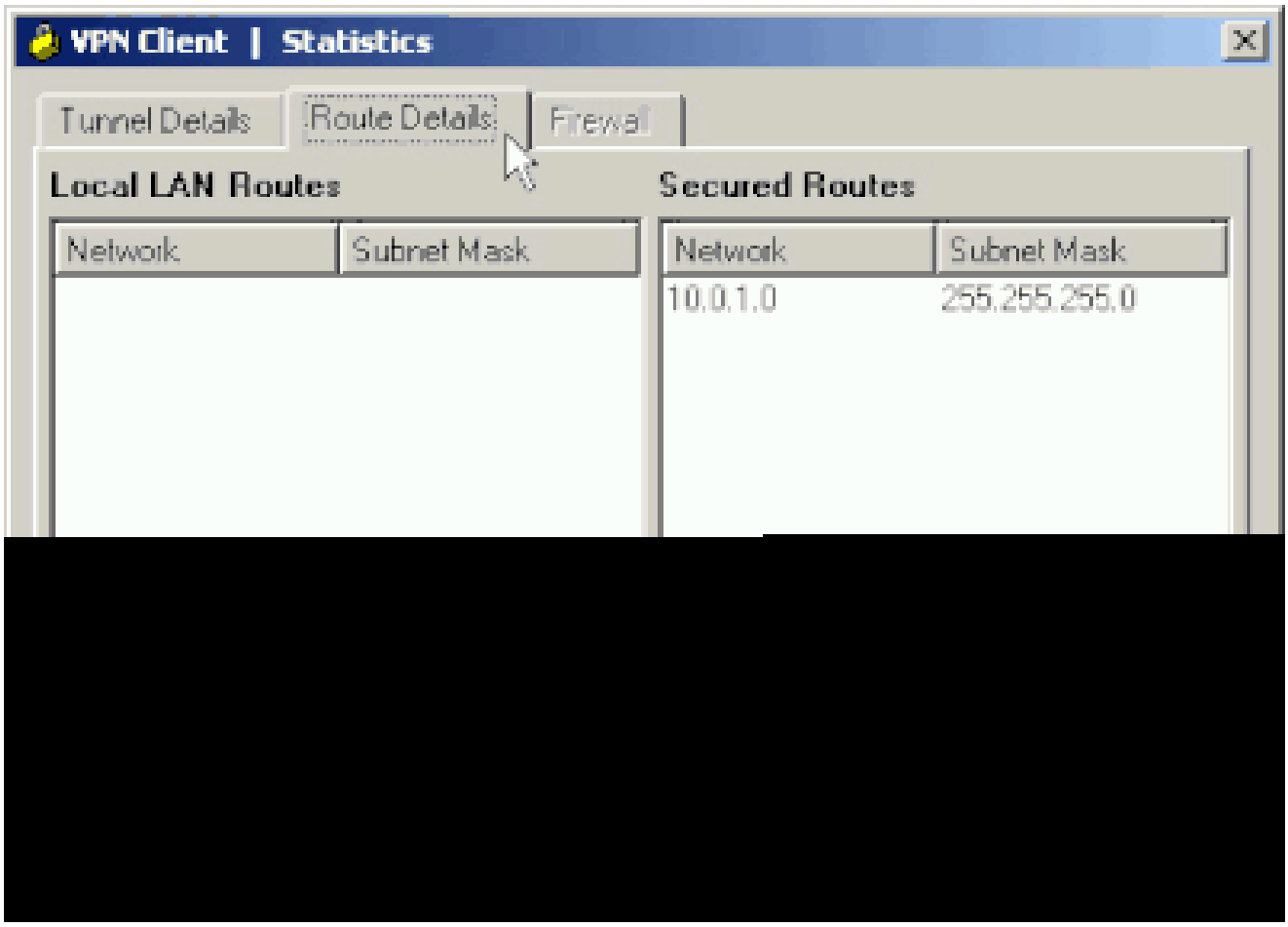
選擇**Status** > **Statistics...**以便顯示Tunnel Details窗口，您可以在此窗口中檢查隧道特定資訊並檢視資料流。



•

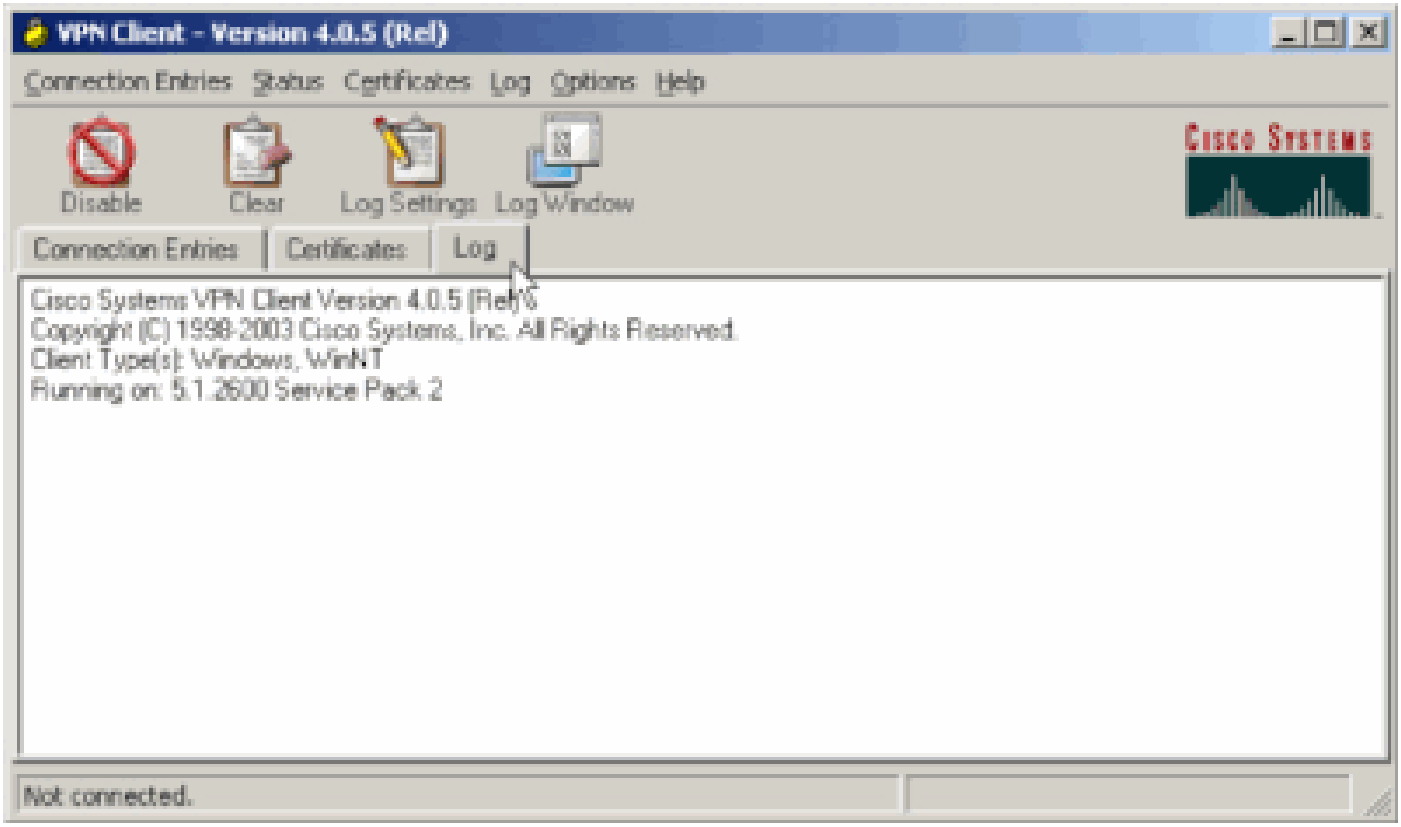
轉至Route Details頁籤，檢視VPN客戶端保護到ASA的路由。

在本示例中，VPN客戶端保護對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，您可以確定是否設定了指定分割隧道的引數。要檢視日誌，請轉到VPN Client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設定為**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/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.
```

使用Ping測試本地LAN訪問

測試VPN客戶端在透過隧道連線到ASA時是否配置了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。

```
   <#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
```

疑難排解

分割通道ACL中的專案數限制

ACL中用於分割隧道的條目數量存在限制。建議不要使用50到60個以上的ACE條目以獲得滿意的功能。建議您實施子網劃分功能以覆蓋一系列IP地址。

相關資訊

- **使用ASDM將PIX/ASA 7.x配置為遠端VPN伺服器的配置示例**
- **Cisco ASA 5500系列調適型安全裝置**
- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。