單臂公共網際網路VPN的PIX/ASA和VPN客戶端配置示例

目錄

簡介

本文檔介紹如何設定ASA安全裝置7.2及更高版本以在單臂上執行IPsec。即使 ASA 不允許分割通道，且使用者在獲准連線至網際網路之前直接與 ASA 連線，此特定情況亦適用於此設定。

注意：在PIX/ASA版本7.2及更高版本中，*intra-interface***關鍵字允許所有流量進入和退出同一介面，而不只是IPsec流量。**

請參閱單臂公共網際網路的路由器和VPN客戶端配置示例，在中心站點路由器上完成類似的配置。

請參閱使用TACACS+身份驗證的PIX/ASA 7.x增強型輻條到客戶端VPN配置示例，以瞭解有關集線器PIX將流量從VPN客戶端重定向到分支PIX的方案的詳細資訊。

注意：為了避免網路中IP地址重疊，請為VPN客戶端分配完全不同的IP地址池（例如，10.x.x.x、172.16.x.x和192.168.x.x）。 此IP編址方案有助於排除網路故障。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 中心PIX/ASA安全裝置需要運行7.2版或更高版本
- Cisco VPN使用者端版本5.x

採用元件

本文檔中的資訊基於PIX或ASA安全裝置版本8.0.2和Cisco VPN客戶端版本5.0。

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。

相關產品

此配置還可以與Cisco PIX安全裝置7.2版及更高版本配合使用。

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

髮夾或U形轉彎

對於進入介面但隨後從同一介面路由出去的VPN流量，此功能非常有用。例如，如果您有一個中心輻射型VPN網路，其中安全裝置是中心，而遠端VPN網路是輻射型，為了使一個輻射型與另一個輻射型通訊，流量必須進入安全裝置，然後再次流向另一個輻射型。

使用**same-security-traffic**命令允許流量進入和退出同一介面。

```
securityappliance(config)#same-security-traffic permit intra-interface
```

注意：迴轉或U形轉彎也適用於VPN客戶端與VPN客戶端的通訊。

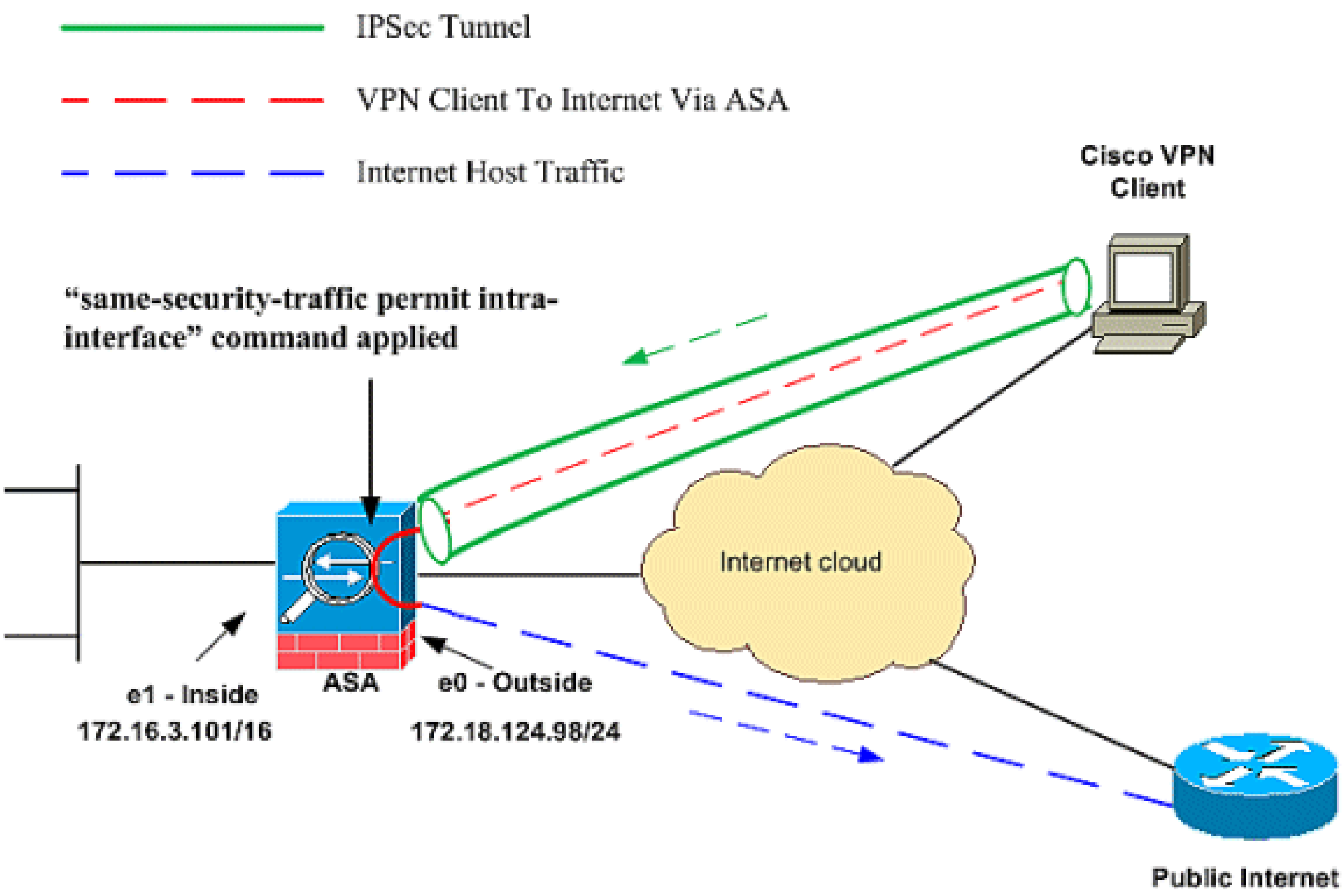
組態

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



PIX/ASA的CLI配置

- PIX/ASA

在PIX/ASA上運行配置

```

PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
```

```
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface
access-list 100 extended permit icmp any any echo-reply
pager lines 24
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500

ip local pool vpnpool
   192.168.10.1-192.168.10.254 mask 255.255.255.0

no failover
monitor-interface outside
monitor-interface inside
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control!--- The address pool for the VPN Clients. !-
-- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP.

global (outside) 1 172.18.124.166

!--- The NAT statement to define what to encrypt (the
addresses from the vpn-pool). nat (outside) 1
192.168.10.0 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 172.16.3.102 172.16.3.102
   netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.124.98 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal
group-policy clientgroup attributes
vpn-idle-timeout 20
```

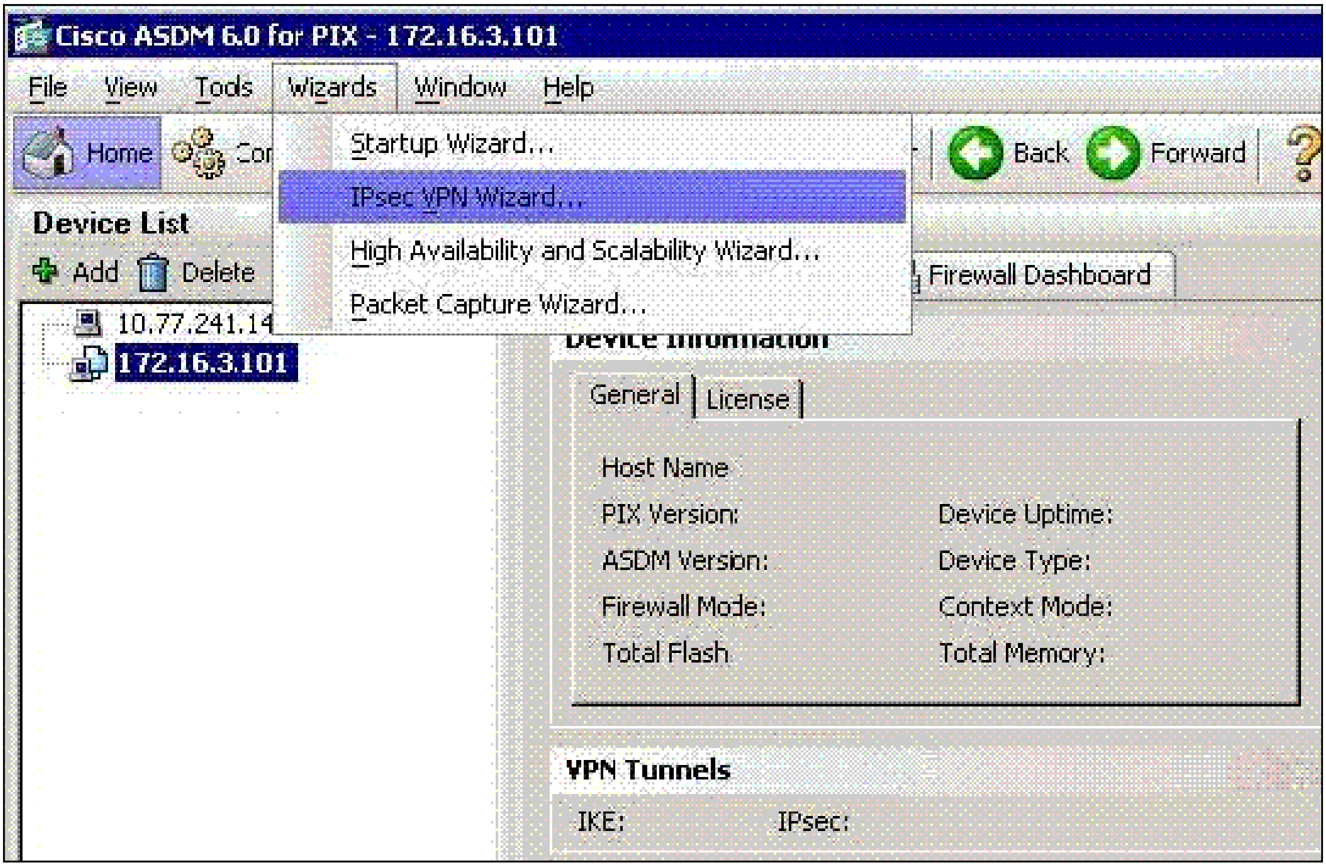
```
!--- Forces VPN Clients over the tunnel for Internet
access. split-tunnel-policy tunnelall


no snmp-server location
no snmp-server contact
snmp-server enable traps snmp

!--- Configuration of IPsec Phase 2. crypto ipsec
transform-set myset esp-3des esp-sha-hmac

!--- Crypto map configuration for VPN Clients that
connect to this PIX. crypto dynamic-map rtpdynmap 20 set
transform-set myset

!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap

!--- Crypto map applied to the outside interface. crypto
map mymap interface outside

!--- Enable ISAKMP on the outside interface. isakmp
identity address
isakmp enable outside

!--- Configuration of ISAKMP policy. isakmp policy 10
authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 65535 authentication pre-share
isakmp policy 65535 encryption 3des
isakmp policy 65535 hash sha
isakmp policy 65535 group 2
isakmp policy 65535 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Configuration of tunnel-group with group
information for VPN Clients. tunnel-group rtptacvpn type
ipsec-ra

!--- Configuration of group parameters for the VPN
Clients. tunnel-group rtptacvpn general-attributes
address-pool vpnpool

!--- Disable user authentication. authentication-server-
group none


!--- Bind group-policy parameters to the tunnel-group
for VPN Clients. default-group-policy clientgroup
tunnel-group rtptacvpn ipsec-attributes
pre-shared-key *
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map global_policy
class inspection_default
```

```
 inspect dns maximum-length 512
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0
: end
```

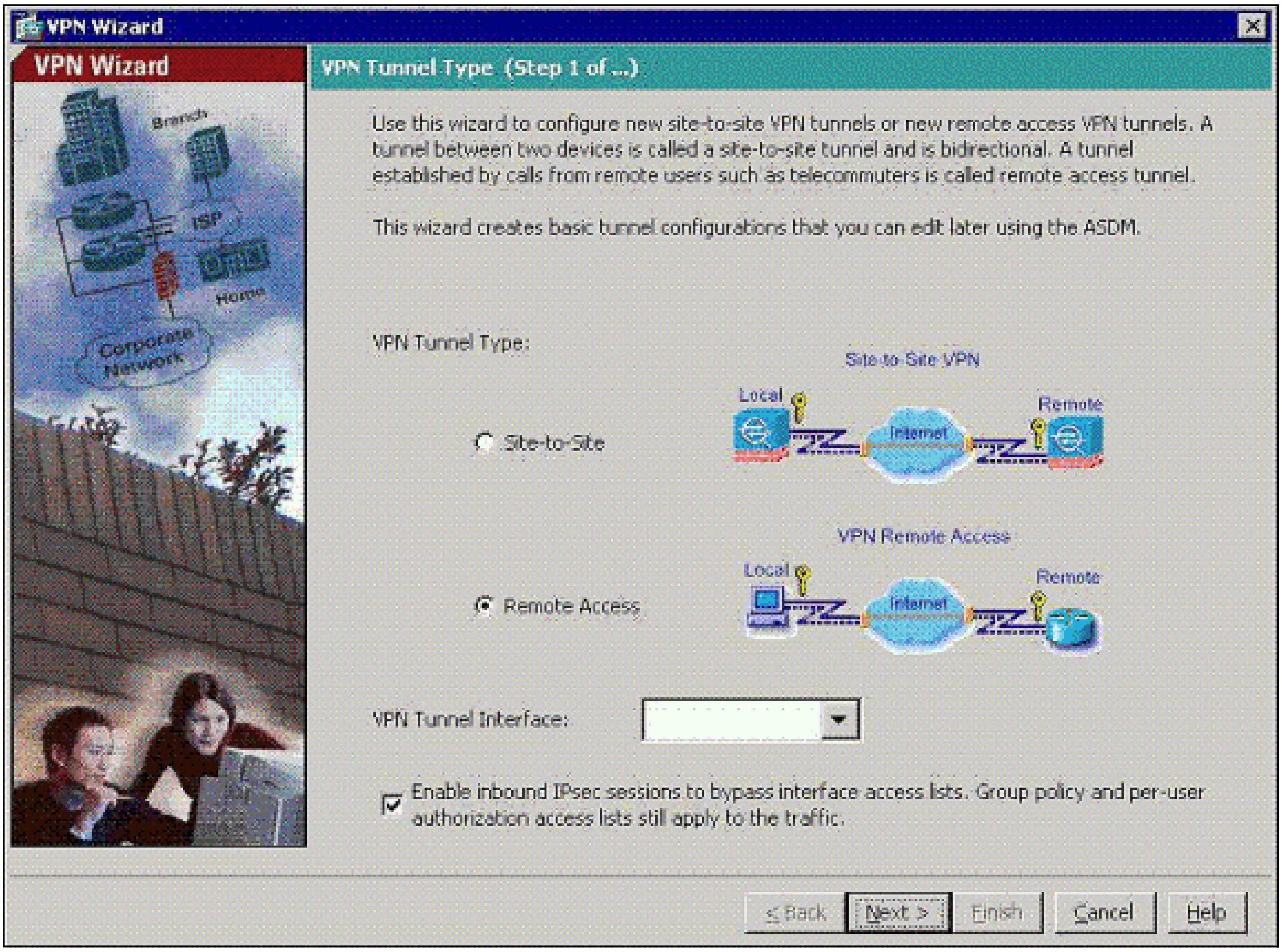
使用ASDM配置ASA/PIX

完成以下步驟，以便使用ASDM將Cisco ASA配置為遠端VPN伺服器：

1. 從主視窗中選擇**Wizards > IPsec VPN Wizard**。



2. 選擇**Remote Access** VPN隧道型別，並確保已根據需要設定VPN隧道介面。



VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

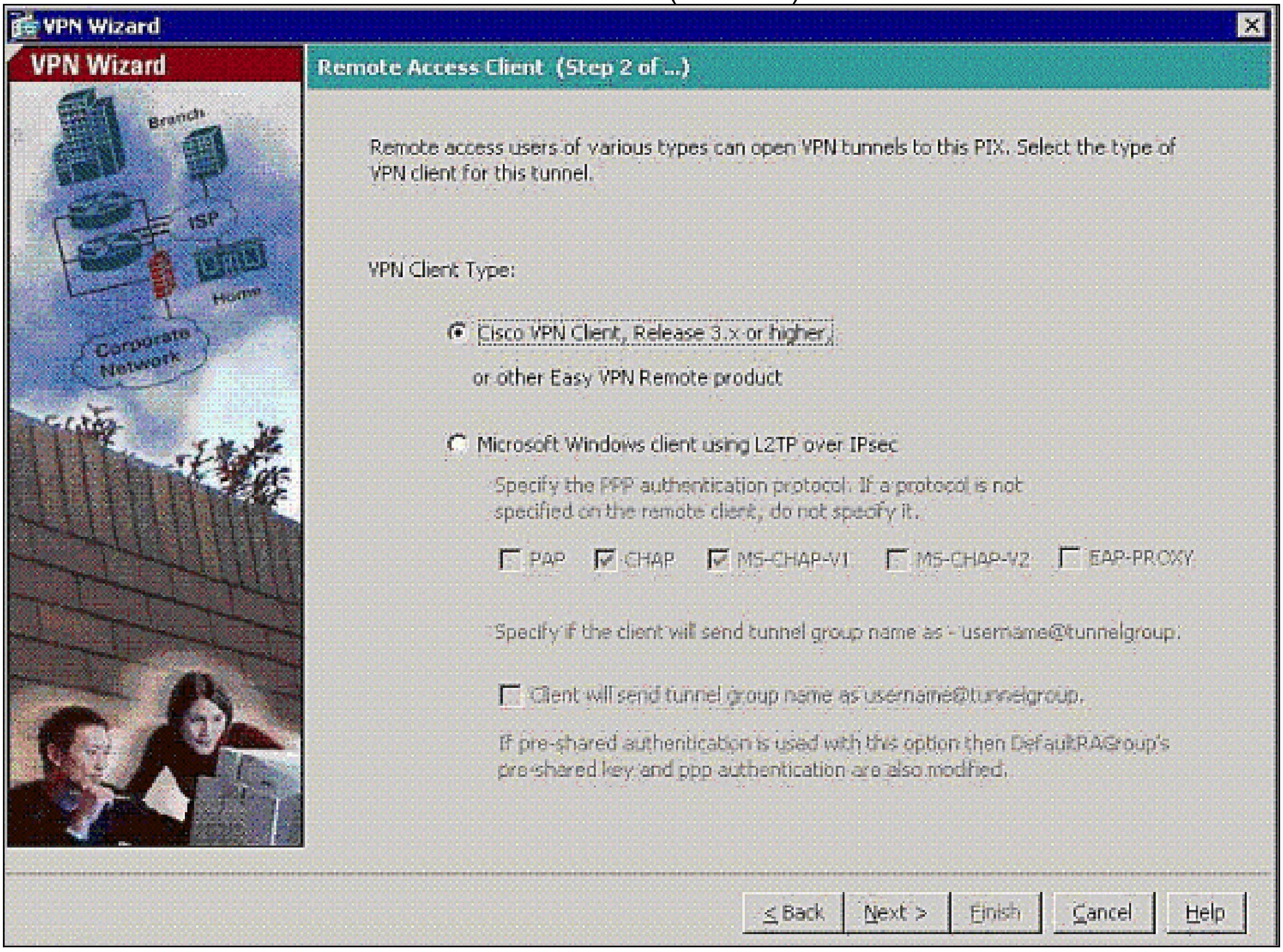
○ Site-to-Site

● Remote Access

VPN Tunnel Interface:

☑ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

3. 已選擇唯一可用的VPN客戶端型別。按「**Next**」（下一步）。



Remote Access Client (Step 2 of ...)

Remote access users of various types can open VPN tunnels to this PIX. Select the type of VPN client for this tunnel.

VPN Client Type:

● Cisco VPN Client, Release 3.x or higher,

or other Easy VPN Remote product

○ Microsoft Windows client using L2TP over IPsec

Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.

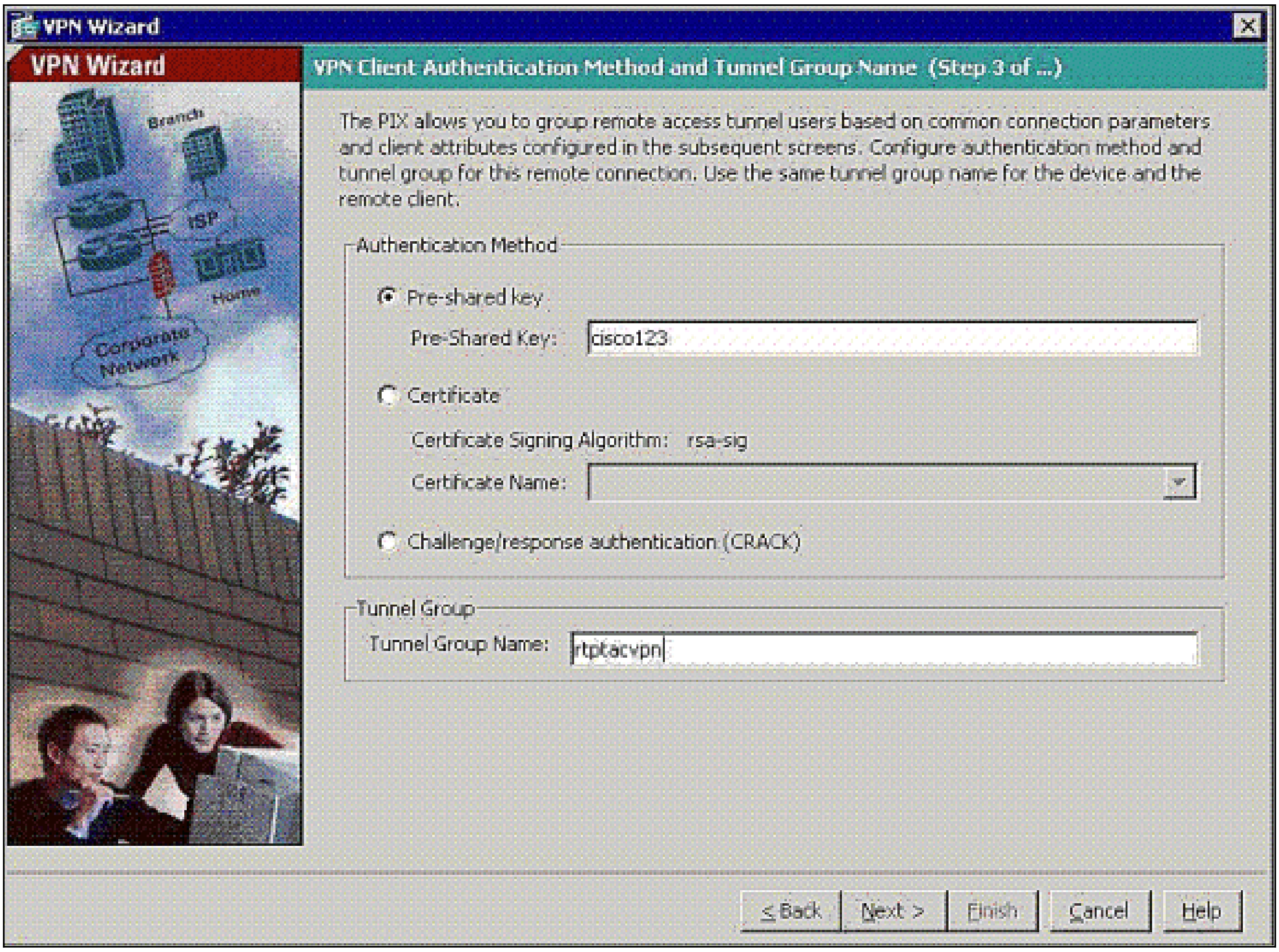
□ PAP ☑ CHAP ☑ MS-CHAP-V1 □ MS-CHAP-V2 □ EAP-PROXY

Specify if the client will send tunnel group name as - username@tunnelgroup.

□ Client will send tunnel group name as username@tunnelgroup.

If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.

4. 輸入隧道組名稱的名稱。提供要使用的身份驗證資訊。**本範例中選**擇預先共用金鑰。



VPN Client Authentication Method and Tunnel Group Name (Step 3 of ...)

The PIX allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client.

Authentication Method

● Pre-shared key

Pre-Shared Key: cisco123

○ Certificate

Certificate Signing Algorithm: rsa-sig

Certificate Name:

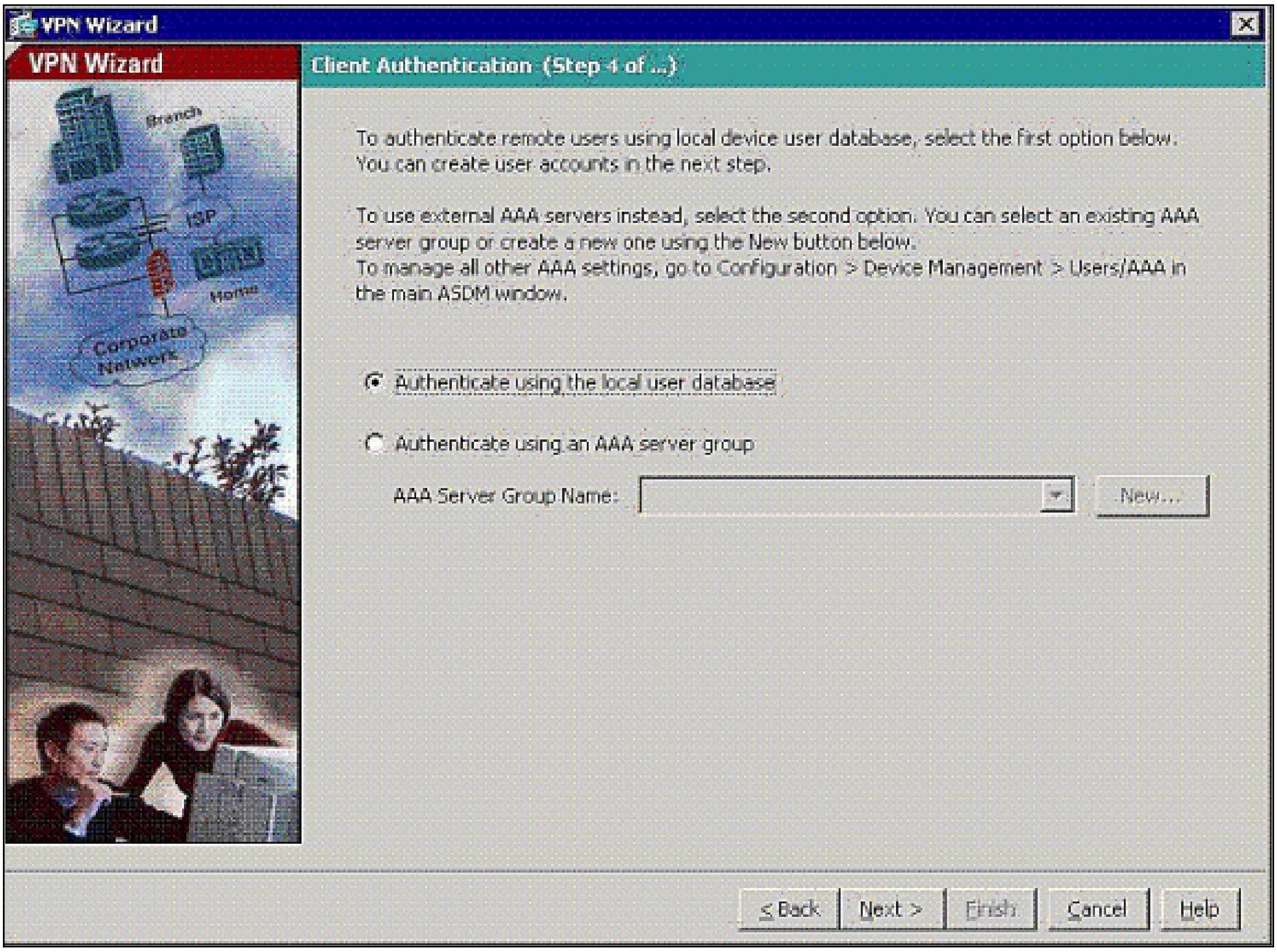
○ Challenge/response authentication (CRACK)

Tunnel Group

Tunnel Group Name: rtptacvpn

注意：無法隱藏/加密ASDM上的預共用金鑰。原因是ASDM只能由配置ASA的人員或協助客戶進行此配置的人員使用。

5. 選擇是要對本地使用者資料庫還是外部AAA伺服器組驗證遠端使用者。**註：您可**以在步驟6中將使用者新增到本地使用者資料庫。**注意**：有關如何通過ASDM配置外部AAA伺服器組的資訊，請參閱通過ASDM為VPN使用者配置PIX/ASA 7.x身份驗證和授權伺服器組配置示例。



To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step.

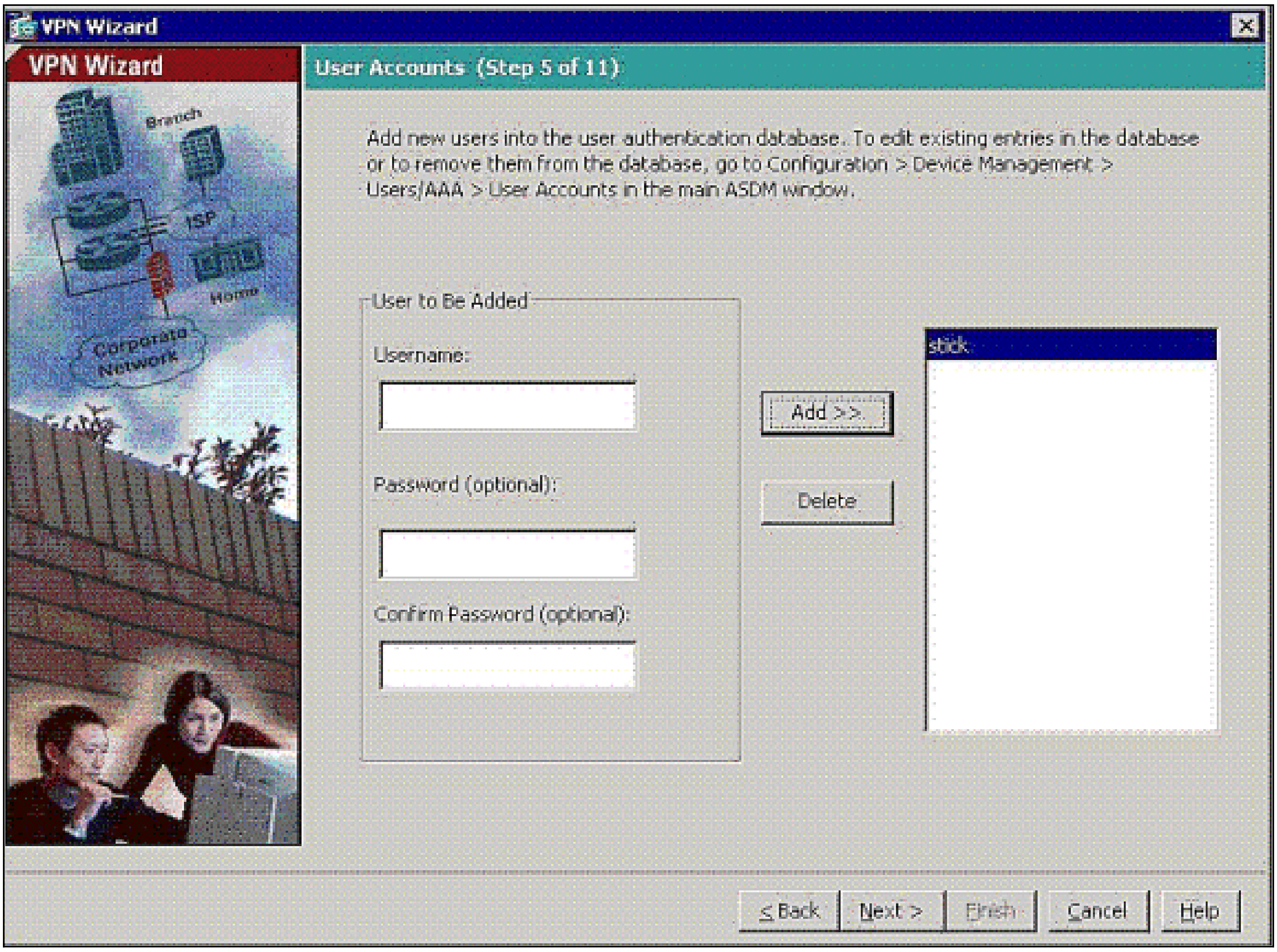
To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below.
To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.

● Authenticate using the local user database

○ Authenticate using an AAA server group

AAA Server Group Name:

6. 如有必要，將使用者新增到本地資料庫。**注意：**不要從此視窗中刪除當前使用者。在ASDM主視窗中選擇**Configuration > Device Administration > Administration > User Accounts**，以編輯資料庫中的現有條目或從資料庫中刪除這些條目。



User Accounts (Step 5 of 11)

Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.

User to Be Added

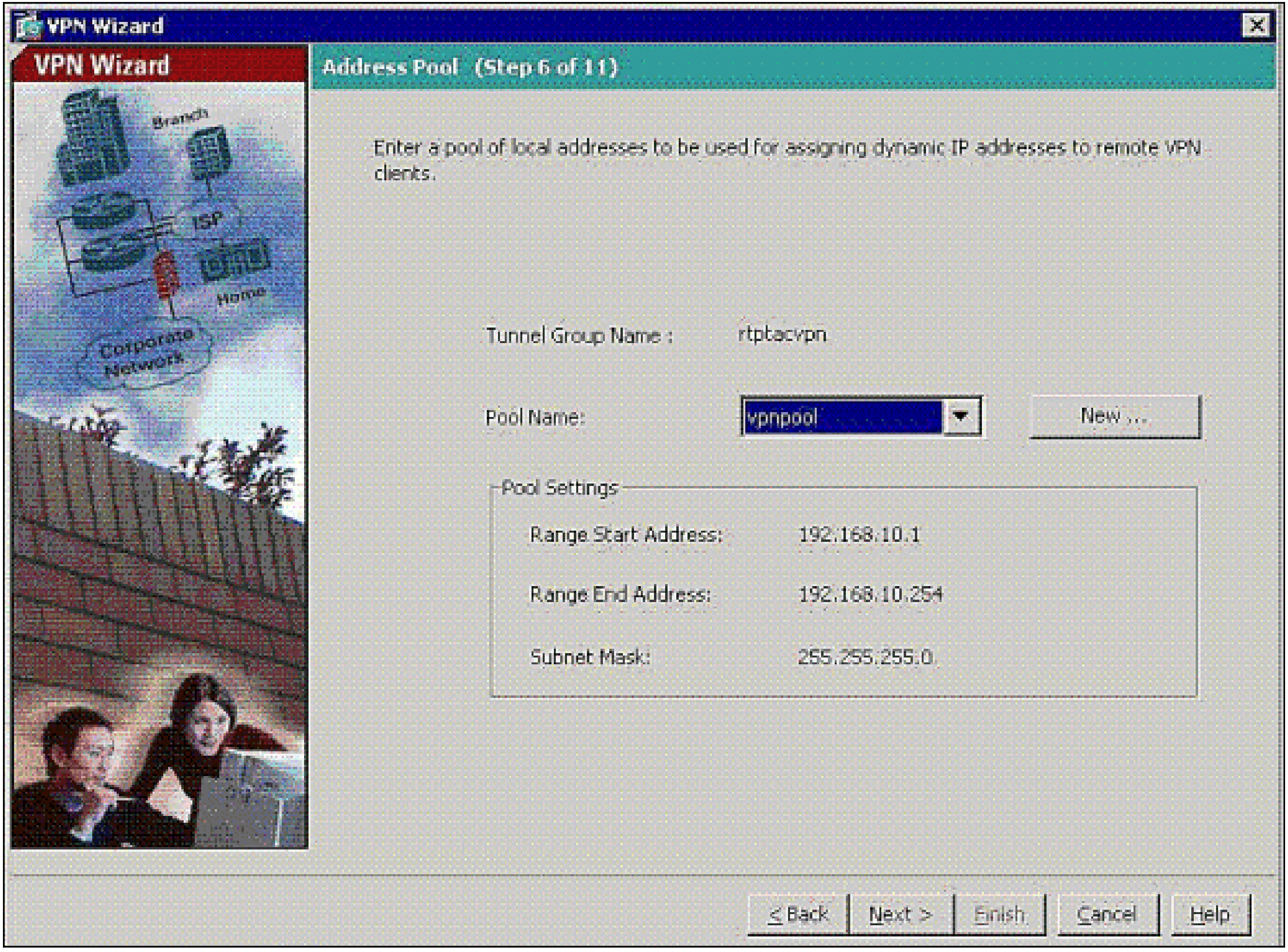
Username:

Password (optional):

Confirm Password (optional):

stick

7. 定義一個本地地址池，在遠端VPN客戶端連線時將其動態分配給它們。



Address Pool (Step 6 of 11)

Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.

Tunnel Group Name : rtptacvpn

Pool Name: vpnpool

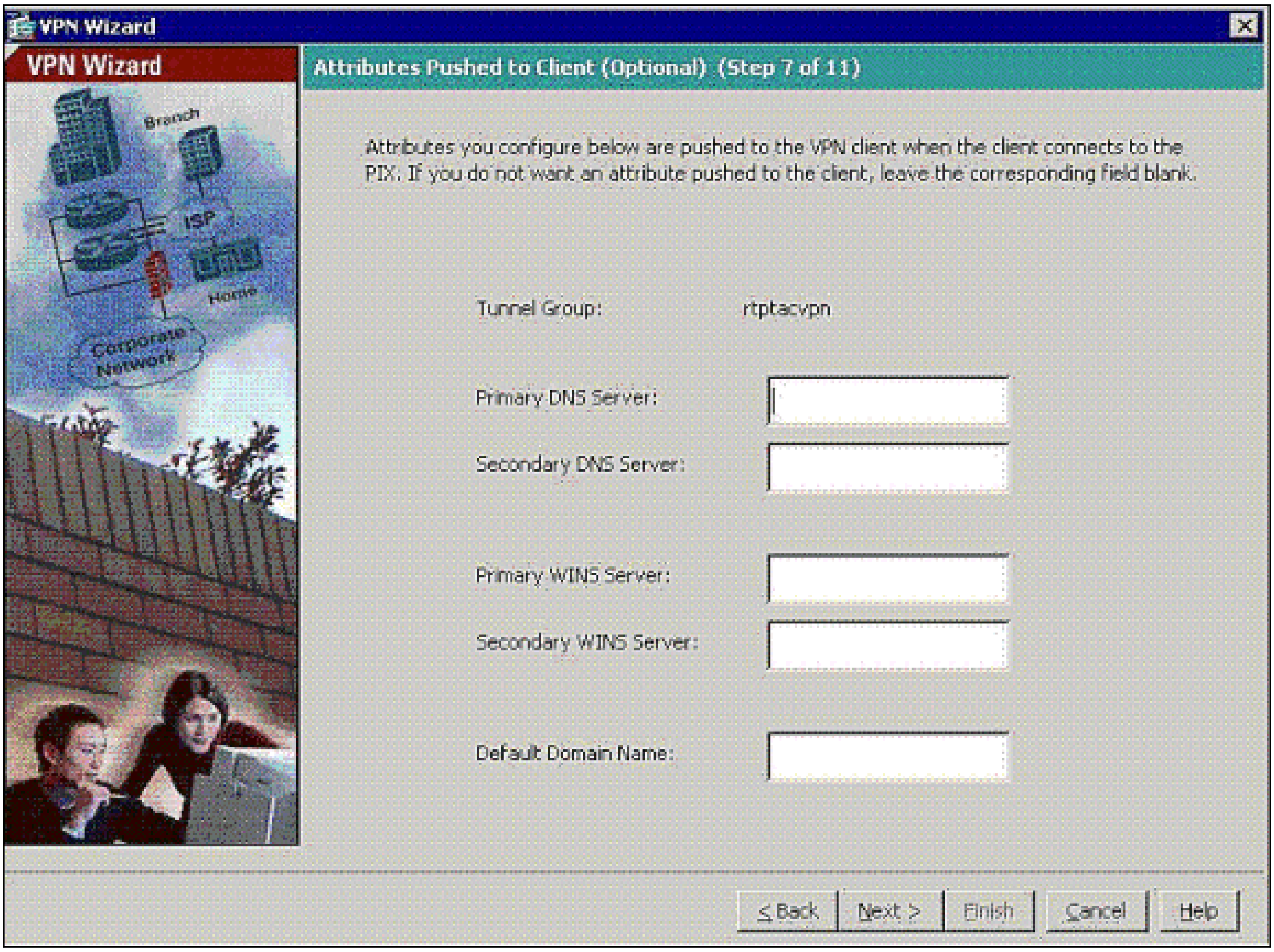
Pool Settings

Range Start Address: 192.168.10.1

Range End Address: 192.168.10.254

Subnet Mask: 255.255.255.0

8. *可選：*指定要推送到遠端VPN客戶端的DNS和WINS伺服器資訊以及預設域名。



Attributes Pushed to Client (Optional) (Step 7 of 11)

Attributes you configure below are pushed to the VPN client when the client connects to the PIX. If you do not want an attribute pushed to the client, leave the corresponding field blank.

Tunnel Group: rtptacvpn

Primary DNS Server:

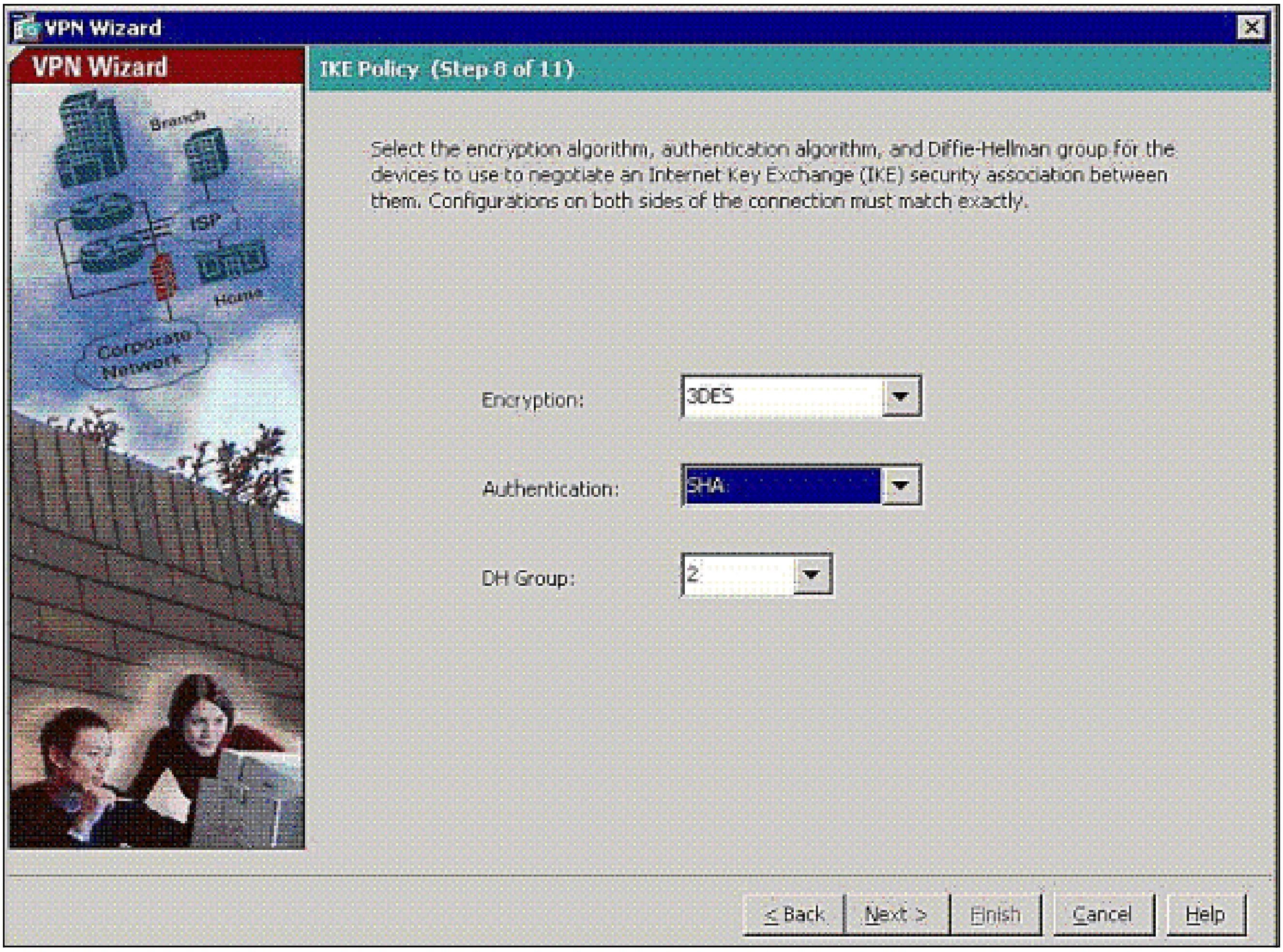
Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain Name:

9. 指定IKE的引數，也稱為IKE階段1。隧道兩端的配置必須完全匹配，但Cisco VPN客戶端會自動為自己選擇正確的配置。客戶端PC上無需配置IKE。



IKE Policy (Step 8 of 11)

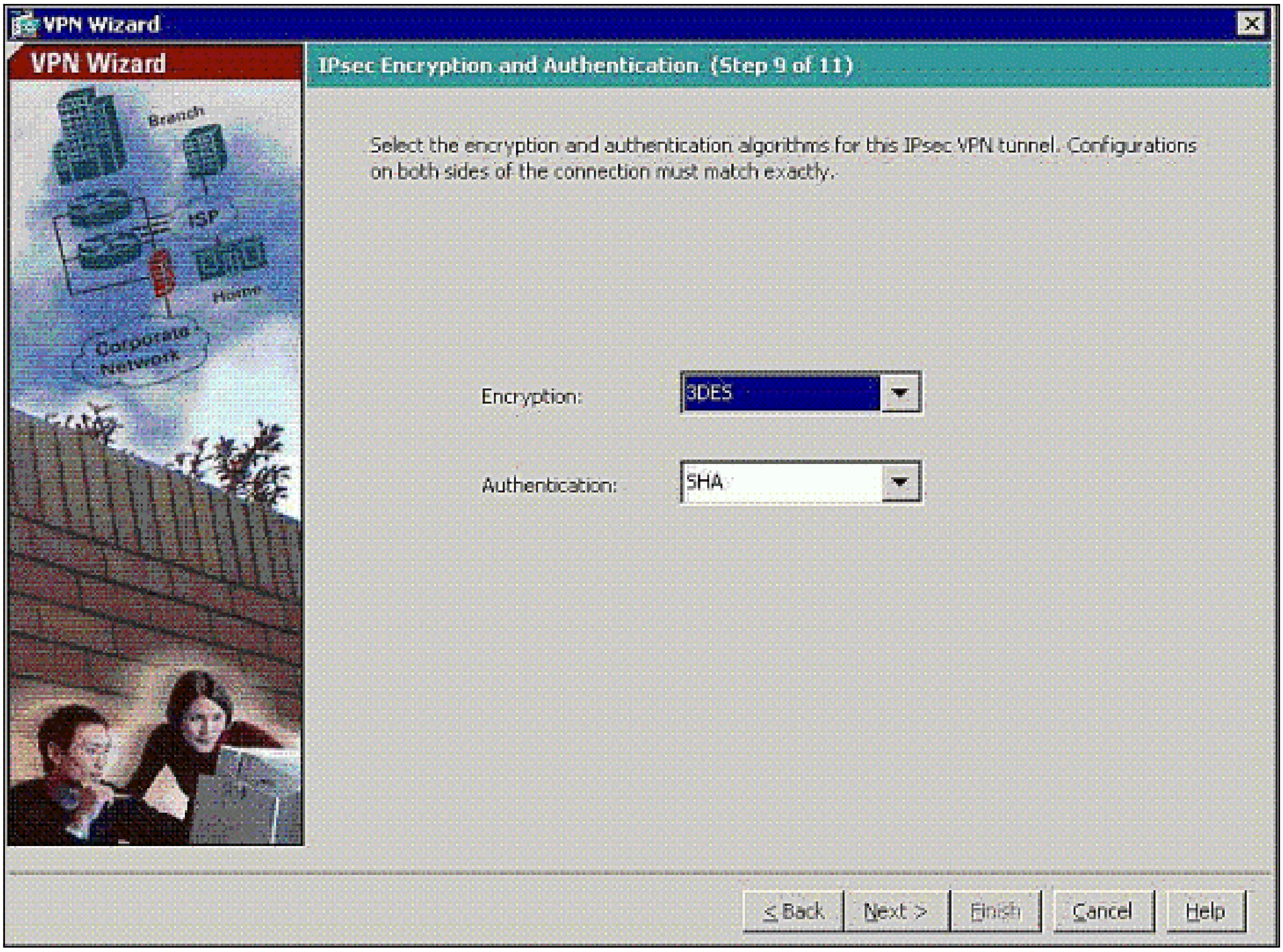
Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

DH Group: 2

10. 指定IPSec（也稱為IKE階段2）的引數。隧道兩端的配置必須完全匹配，但Cisco VPN客戶端會自動為自己選擇正確的配置。客戶端PC上無需配置IKE。

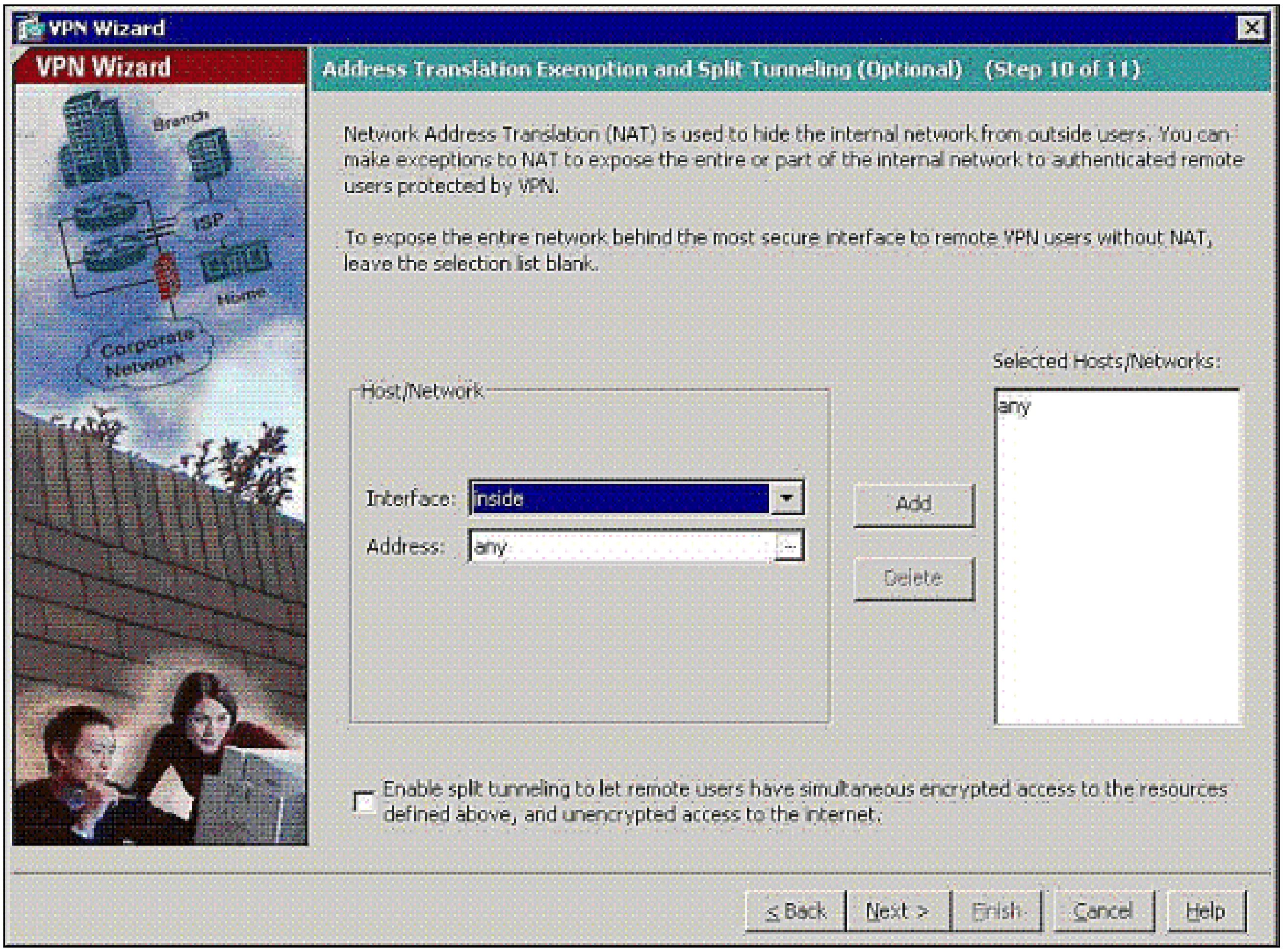


Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

11. 指定可以向遠端VPN使用者公開哪些內部主機或網路（如果有）。如果將此清單留空，則遠端VPN使用者可訪問ASA的整個內部網路。您還可以在此視窗中啟用分割隧道。分割隧道可加密流向此過程前面定義的資源的流量，並通過不對該流量進行隧道傳輸來提供對一般網際網路的未加密訪問。如果未啟用*拆分隧道*，則所有來自遠端VPN使用者的流量都會通過隧道連線到ASA。根據您的配置，這會佔用大量頻寬和處理器。



Address Translation Exemption and Split Tunneling (Optional) (Step 10 of 11)

Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.

To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.

Host/Network

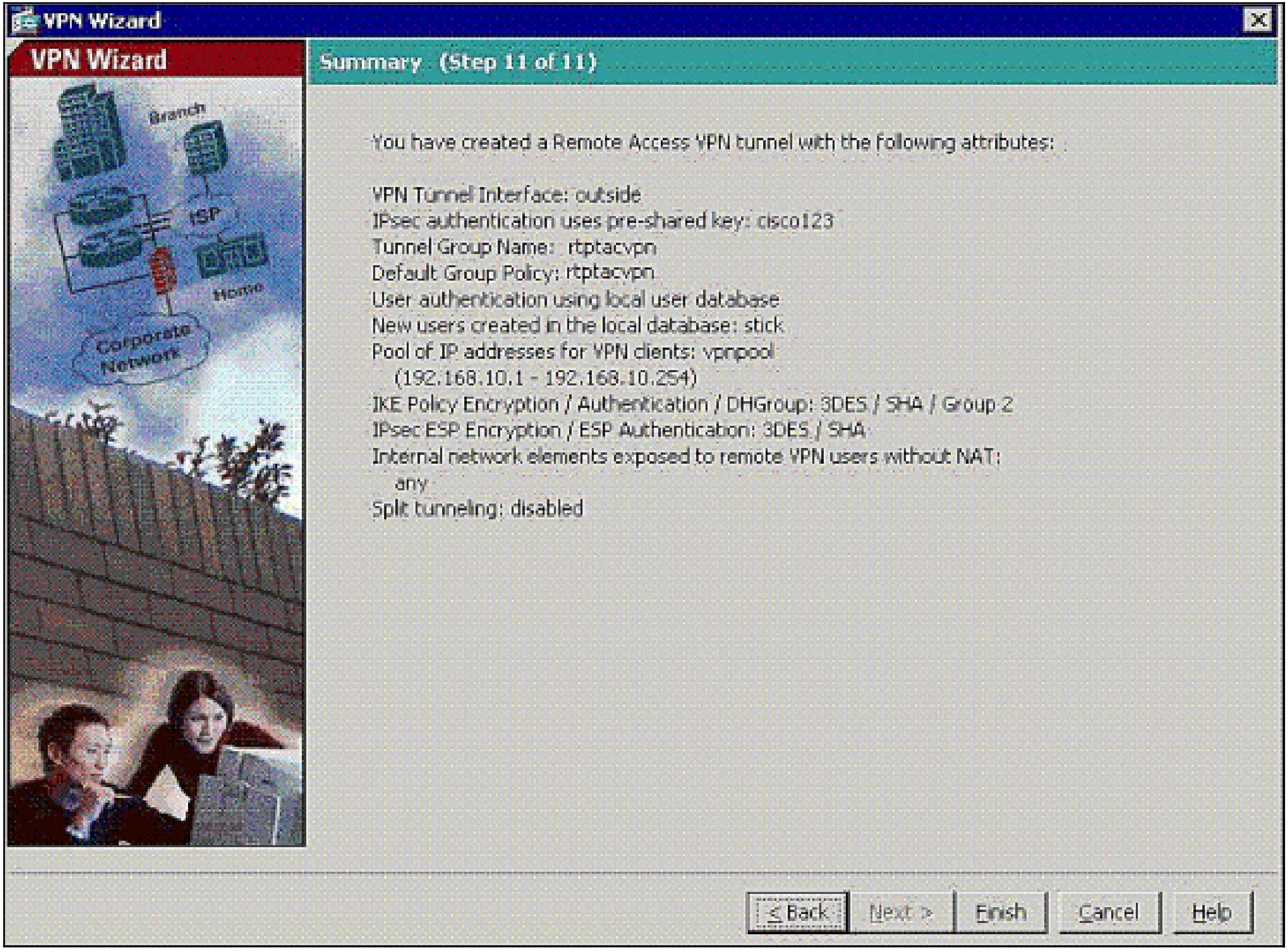
Interface: inside

Address: any

Selected Hosts/Networks: any

□ Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.

12. 此視窗顯示您已採取的操作的摘要。如果對配置滿意，請按一下**Finish**。



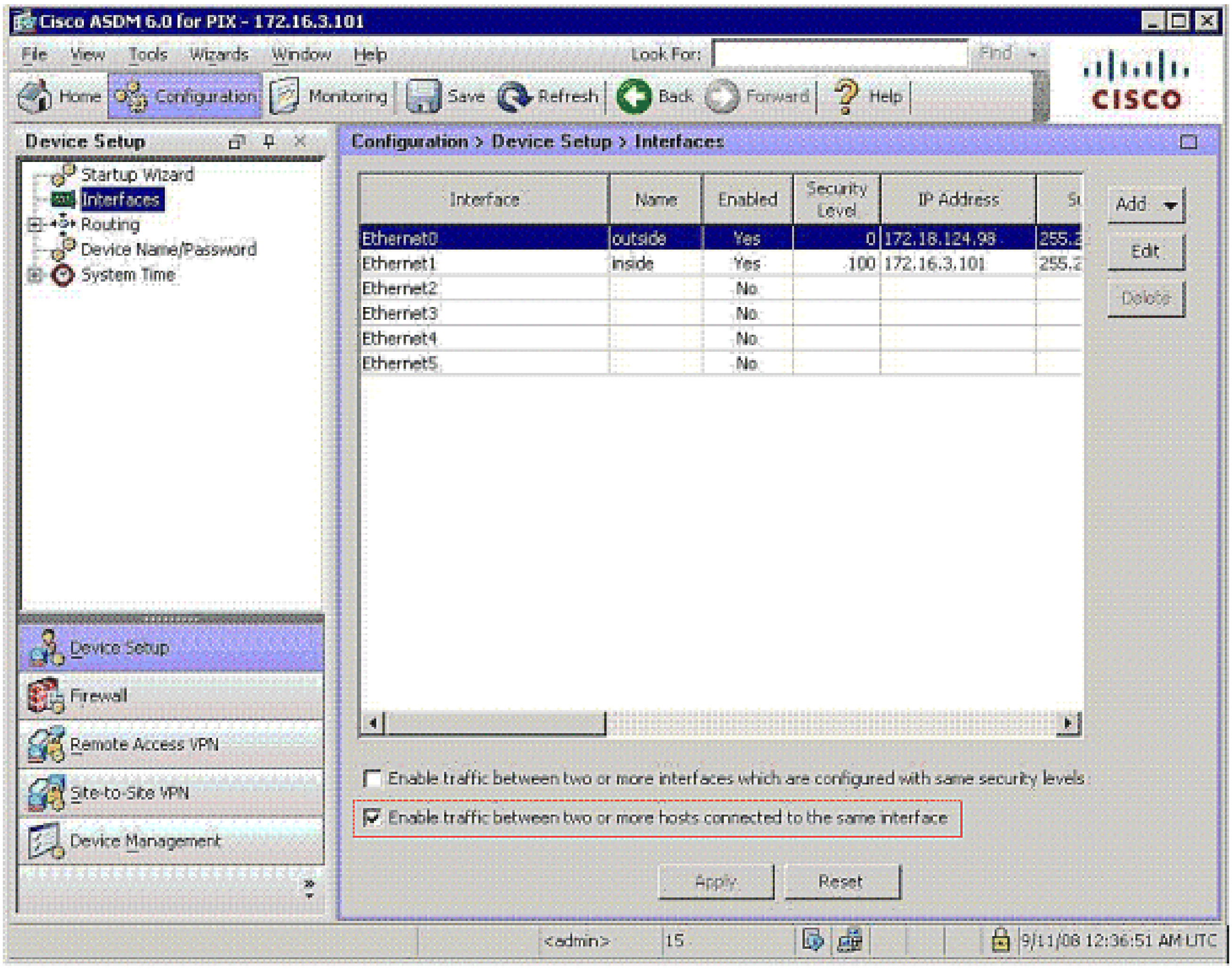
Summary (Step 11 of 11)

You have created a Remote Access VPN tunnel with the following attributes:

VPN Tunnel Interface: outside
IPsec authentication uses pre-shared key: cisco123
Tunnel Group Name: rtptacvpn
Default Group Policy: rtptacvpn
User authentication using local user database
New users created in the local database: stick
Pool of IP addresses for VPN clients: vpnpool
(192.168.10.1 - 192.168.10.254)
IKE Policy Encryption / Authentication / DHGroup: 3DES / SHA / Group 2
IPsec ESP Encryption / ESP Authentication: 3DES / SHA
Internal network elements exposed to remote VPN users without NAT:
any
Split tunneling: disabled

13. 按一下覈取方塊時，配置命令**same-security-traffic**，以在連線到同一介面的兩個或多個主機

之間啟用流量，如下所示
：



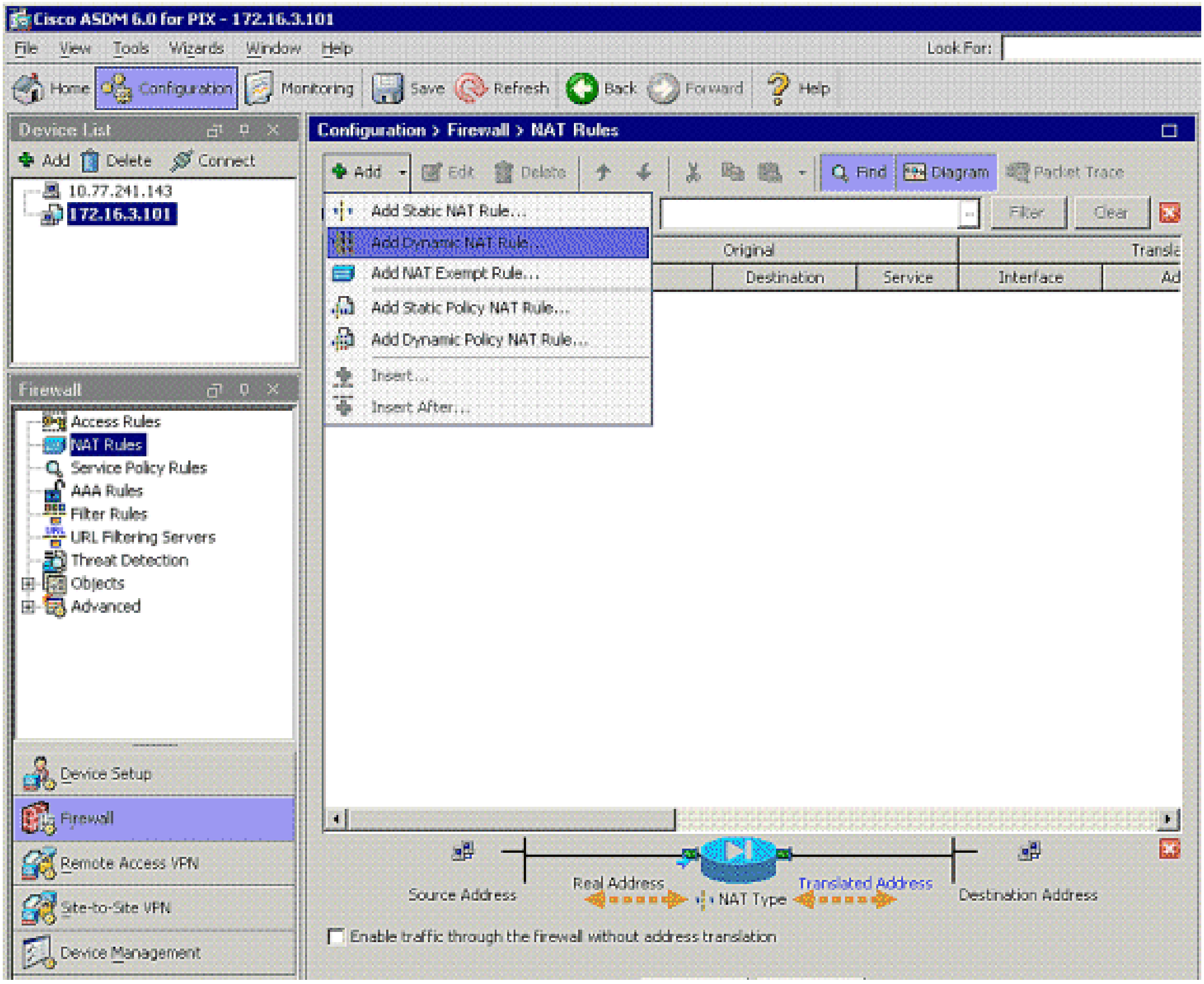
Configuration > Device Setup > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Su
Ethernet0	outside	Yes	0	172.18.124.98	255.2
Ethernet1	inside	Yes	100	172.16.3.101	255.2
Ethernet2		No			
Ethernet3		No			
Ethernet4		No			
Ethernet5		No			

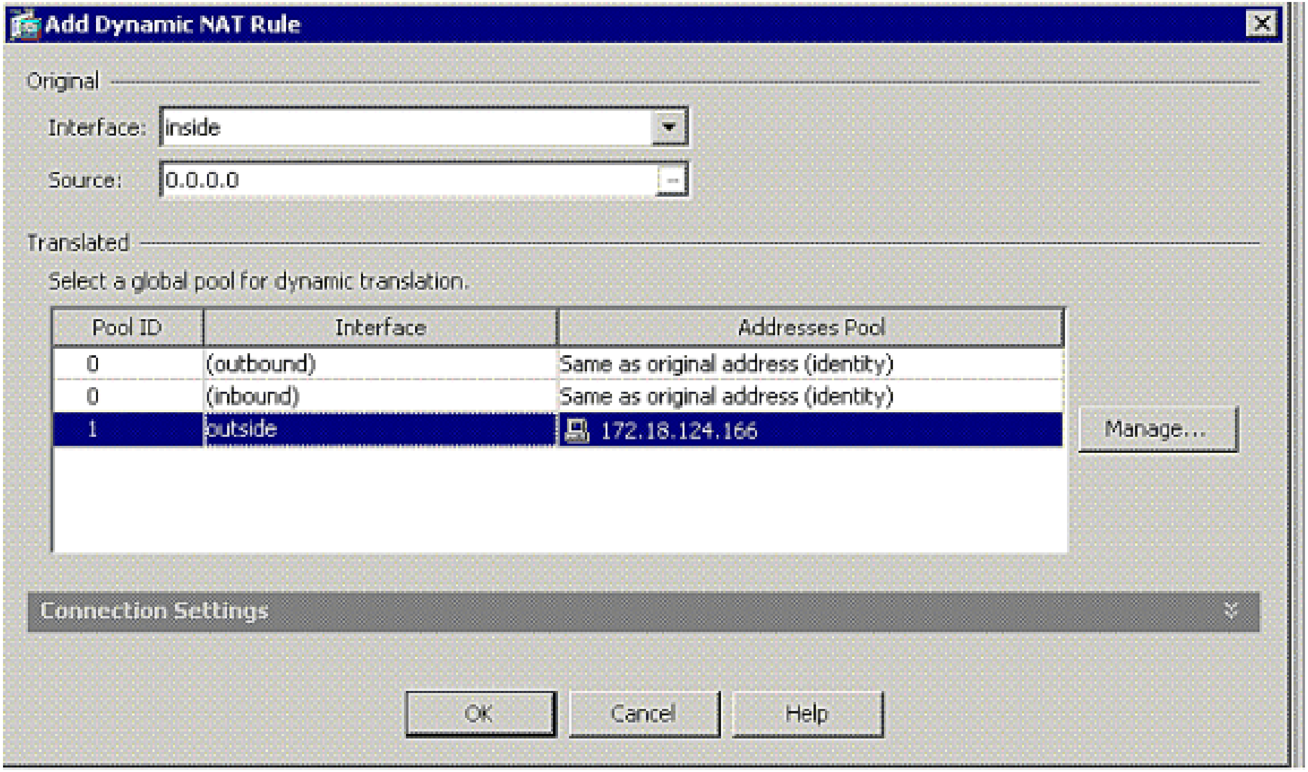
☐ Enable traffic between two or more interfaces which are configured with same security levels

☑ Enable traffic between two or more hosts connected to the same interface

14. 選擇**Configuration > Firewall > NAT Rules**，然後按一下**Add Dynamic NAT Rule**，以便使用ASDM建立此動態轉換。



15. 選擇**inside**作為源介面，然後輸入要進行NAT的地址。對於Translate Address on Interface，選擇**outside**，然後按一下**OK**。



Add Dynamic NAT Rule

Original

Interface: inside

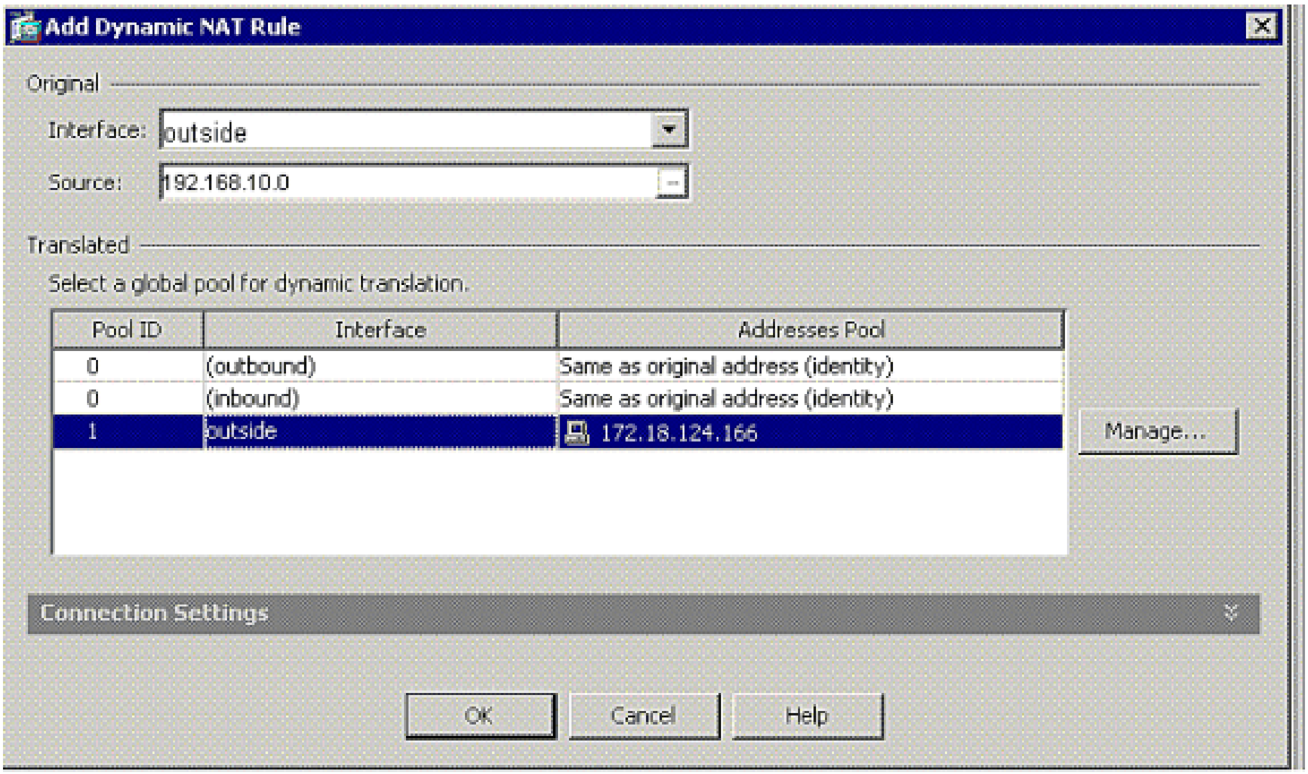
Source: 0.0.0.0

Translated

Select a global pool for dynamic translation.

Pool ID	Interface	Addresses Pool
0	(outbound)	Same as original address (identity)
0	(inbound)	Same as original address (identity)
1	outside	172.18.124.166

16. 選擇**outside**作為源介面，然後輸入您要進行NAT的地址。對於Translate Address on Interface，選擇**outside**，然後按一下**OK**。



Add Dynamic NAT Rule

Original

Interface: outside

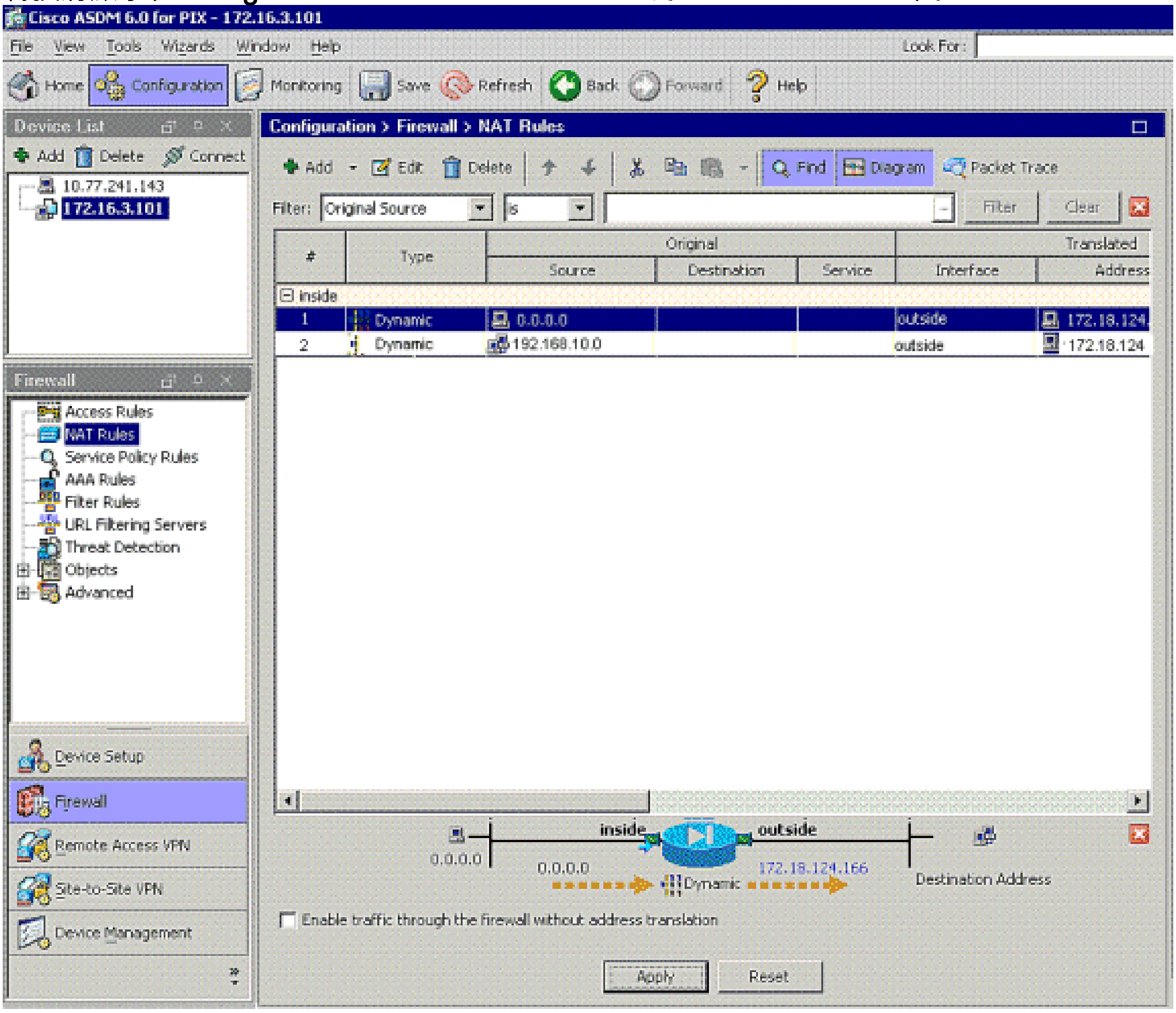
Source: 192.168.10.0

Translated

Select a global pool for dynamic translation.

Pool ID	Interface	Addresses Pool
0	(outbound)	Same as original address (identity)
0	(inbound)	Same as original address (identity)
1	outside	172.18.124.166

17. 轉換將顯示在**Configuration > Firewall > NAT Rules**的Translation Rules中。



Cisco ASDM 6.0 for PIX - 172.16.3.101

Filter: Original Source is

#	Type	Original			Translated	
		Source	Destination	Service	Interface	Address
⊟ inside						
1	Dynamic	0.0.0.0			outside	172.18.124.
2	Dynamic	192.168.10.0			outside	172.18.124

□ Enable traffic through the firewall without address translation

附註1:需要配置sysopt connection permit-vpn 命令。show running-config sysopt命令會驗證它是否已配置。

附註2:為可選的UDP傳輸新增以下輸出：

```
group-policy clientgroup attributes vpn-idle-timeout 20
ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

附註3:在PIX裝置的全域性配置中配置此命令，以便通過IPsec over TCP連線VPN客戶端：

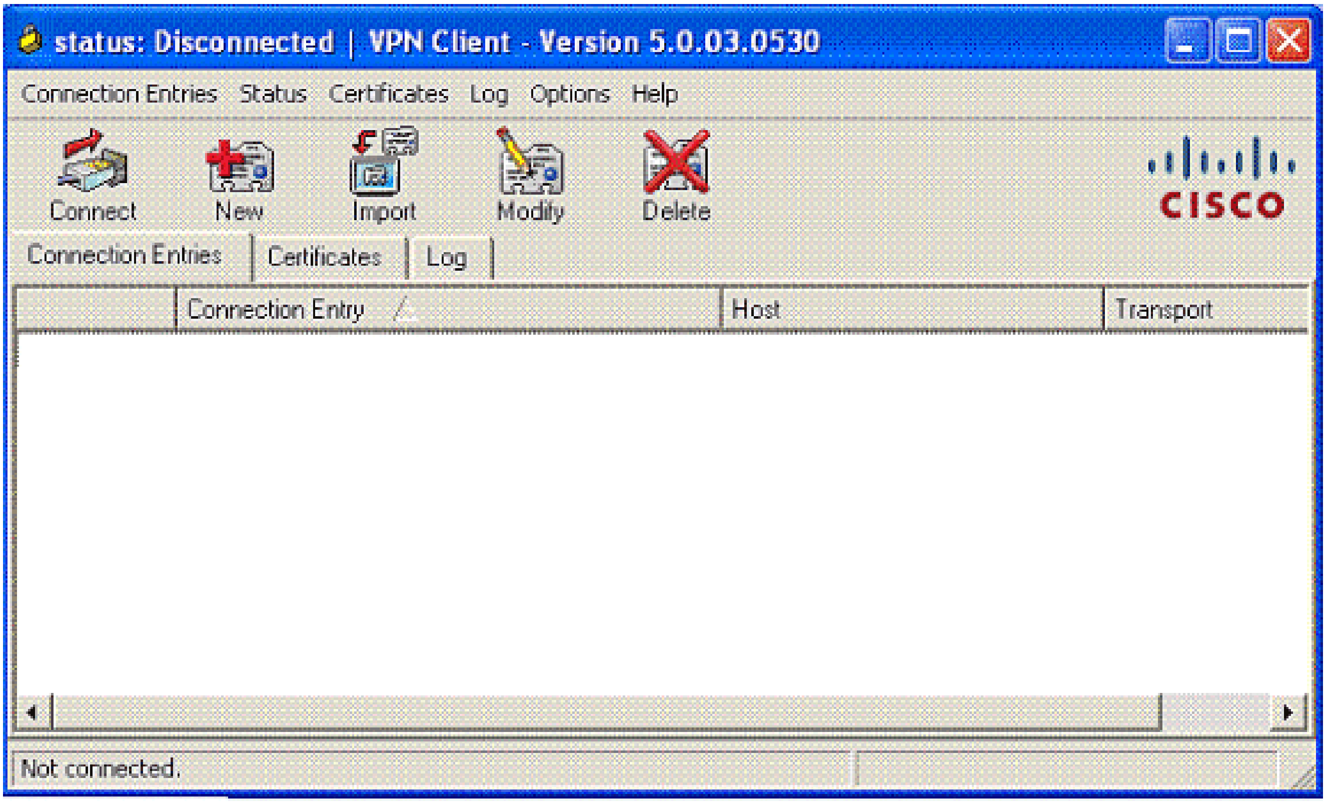
```
isakmp ipsec-over-tcp port 10000
```

注意：請參閱Cisco ASA上的髮夾影片，瞭解有關可以使用髮夾的不同方案的詳細資訊。

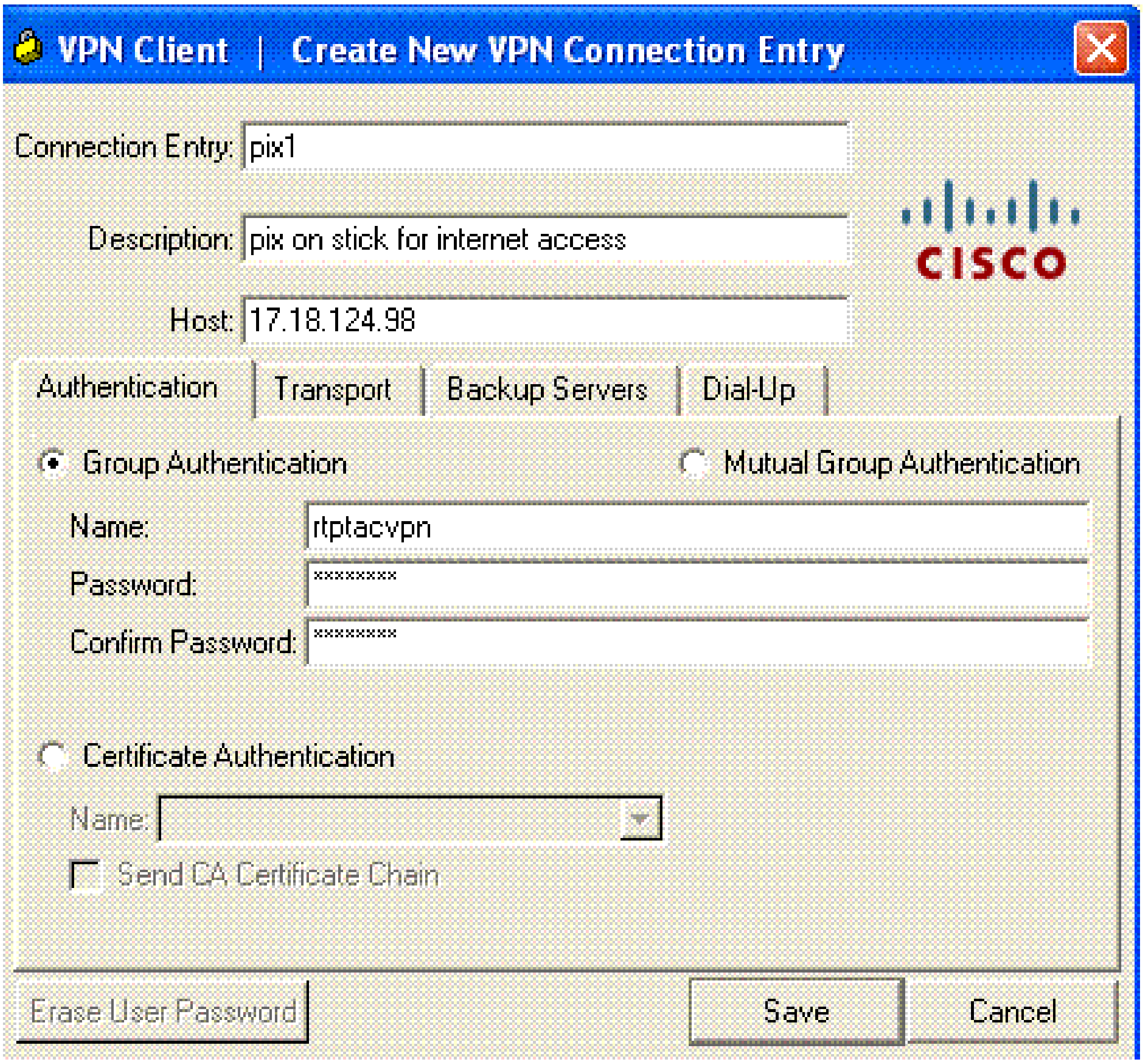
VPN客戶端配置

完成以下步驟以配置VPN客戶端：

1. 選擇**New**。



2. 輸入PIX外部介面ip地址、隧道組名稱以及用於身份驗證的密碼。



VPN Client | Create New VPN Connection Entry

Connection Entry: pix1

Description: pix on stick for internet access

Host: 17.18.124.98

● Group Authentication ○ Mutual Group Authentication

Name: rtptacvpn

Password: ********

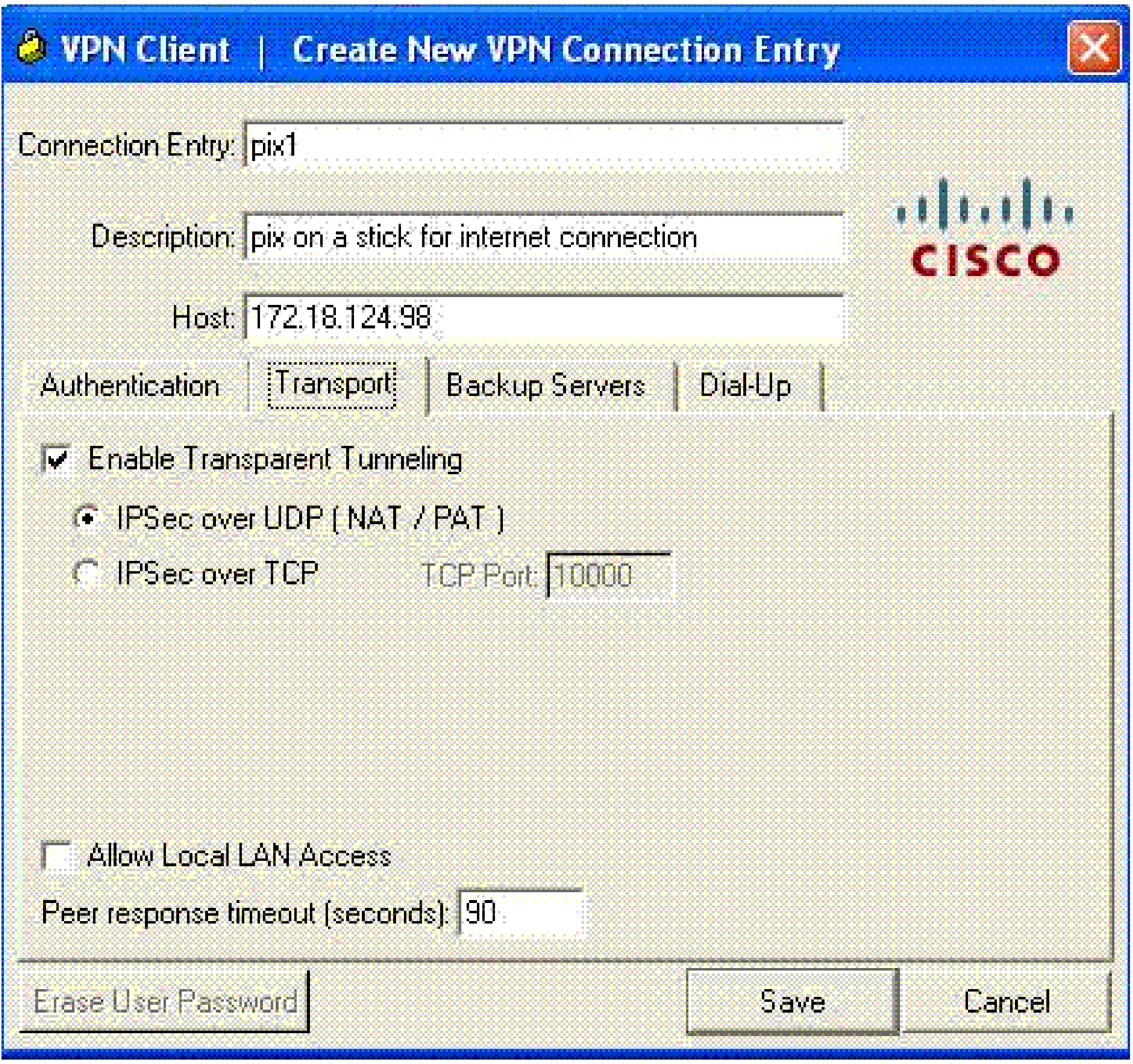
Confirm Password: ********

○ Certificate Authentication

Name:

□ Send CA Certificate Chain

3. (*可選)按一下***Transport**頁籤下的**Enable Transparent Tunneling**。(這是可選的，需要附註2中提到的額外PIX/ASA配置。



VPN Client | Create New VPN Connection Entry

Connection Entry: pix1

Description: pix on a stick for internet connection

Host: 172.18.124.98

☑ Enable Transparent Tunneling

● IPSec over UDP (NAT / PAT)

○ IPSec over TCP TCP Port: 10000

□ Allow Local LAN Access

Peer response timeout (seconds): 90

)

4. 儲存配置檔案。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- show crypto isakmp sa — 顯示對等體上的所有當前IKE安全關聯(SA)。
- show crypto ipsec sa — 顯示所有當前SA。在定義VPN客戶端流量的SA上查詢加密和解密資料包。

嘗試從客戶端(例如www.cisco.com)ping或瀏覽到公有IP地址。

注意：除非在全域性配置模式下配置了management-access命令，否則無法ping通PIX的內部介面以形成隧道。

```
PIX1(config)#management-access inside
PIX1(config)#show management-access

management-access inside
```

VPN使用者端驗證

完成以下步驟以驗證VPN客戶端。

1. 連線成功後，按一下右鍵系統托盤上出現的VPN客戶端鎖定圖示，然後選擇**statistics**選項檢視加密和解密。
2. 點選Route Details頁籤以驗證從裝置向下傳遞的no split-tunnel清單。

疑難排解

注意：有關如何排除VPN問題的詳細資訊，請參閱**VPN故障排除解決方案。**

相關資訊

- **PIX安全裝置版本7.0的增強型分支到客戶端VPN配置示例**
- **Cisco VPN使用者端**
- **IPSec 協商/IKE 通訊協定**
- **Cisco PIX防火牆軟體**
- **Cisco Secure PIX防火牆命令參考**
- **安全產品現場通知（包括PIX）**
- **Cisco ASA上的髮夾控制**
- **要求建議 (RFC)**
- **技術支援與文件 - Cisco Systems**