使用CLI和ASDM進行擴展身份驗證的PIX/ASA作為遠端VPN伺服器的配置示例

目錄

簡介

本文檔介紹如何使用Adaptive Security Device Manager(ASDM)或CLI將Cisco 5500系列自適應安全裝置(ASA)配置為遠端VPN伺服器。ASDM通過直觀易用的基於Web的管理介面提供世界一流的安全管理和監控。Cisco ASA配置完成後，可以使用Cisco VPN客戶端進行驗證。

請參閱使用Windows 2003 IAS RADIUS（針對Active Directory）的PIX/ASA 7.x和Cisco VPN客戶端4.x身份驗證配置示例，以在Cisco VPN客戶端(4.x for Windows)和PIX 500系列安全裝置7.x之間設定遠端訪問VPN連線。遠端VPN客戶端使用者使用Microsoft Windows 2003 Internet身份驗證服務(IAS)RADIUS伺服器對Active Directory進行身份驗證。

請參閱適用於Cisco安全ACS的PIX/ASA 7.x和Cisco VPN客戶端4.x身份驗證配置示例，以使用思科安全訪問控制伺服器（ACS版本3.2）進行擴展身份驗證(Xauth)，在Cisco VPN客戶端（適用於Windows的4.x）和PIX 500系列安全裝置7.x之間建立遠端訪問VPN連線。

必要條件

需求

本文檔假定ASA已完全正常運行並配置為允許Cisco ASDM或CLI進行配置更改。

註：請參閱允許ASDM或PIX/ASA 7.x的HTTPS訪問:內部和外部介面上的SSH配置示例，允許通過ASDM或安全外殼(SSH)遠端配置裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科自適應安全裝置軟體版本7.x及更高版本
- 自適應安全裝置管理器5.x版及更高版本
- Cisco VPN客戶端4.x版及更高版本

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.x版及更高版本配合使用。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

遠端訪問配置為Cisco VPN客戶端（例如移動使用者）提供安全的遠端訪問。遠端訪問VPN使遠端使用者能夠安全地訪問集中式網路資源。Cisco VPN Client符合IPSec協定，專門設計用於與安全裝置配合使用。但是，安全裝置可以與許多符合協定的客戶端建立IPSec連線。有關IPSec的詳細資訊，請參閱ASA配置指南。

組和使用者是VPN安全管理和安全裝置配置中的核心概念。它們指定用於確定使用者對VPN的訪問許可權和使用的屬性。組是被視為單個實體的使用者集合。使用者從組策略獲取其屬性。隧道組標識特定連線的組策略。如果未向使用者分配特定組策略，則應用連線的預設組策略。

隧道組由確定隧道連線策略的一組記錄組成。這些記錄標識了通道使用者向其進行身份驗證的伺服器，以及連線資訊傳送到其的記帳伺服器（如果有）。它們還標識連線的預設組策略，並且它們包含特定於協定的連線引數。隧道組包含與建立隧道本身相關的少量屬性。隧道組包括指向定義面向使用者的屬性的組策略的指標。

注意：在本文檔的示例配置中，本地使用者帳戶用於身份驗證。如果要使用其他服務（例如LDAP和RADIUS），請參閱配置外部RADIUS伺服器以進行授權和身份驗證。

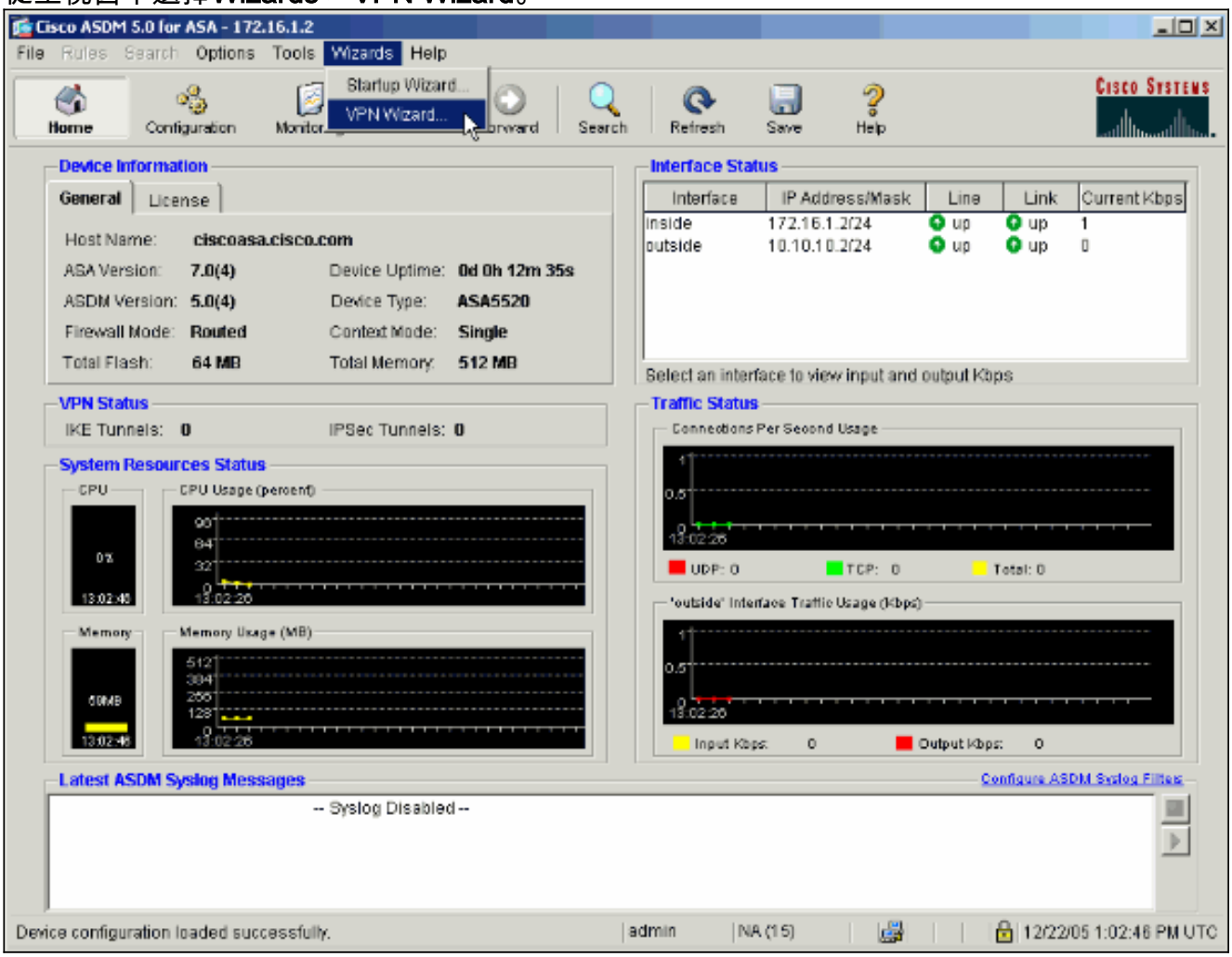
Internet安全關聯和金鑰管理協定(ISAKMP)（也稱為IKE）是主機就如何建立IPSec安全關聯達成協定的協商協定。每個ISAKMP協商分為兩個部分，第1階段和第2階段。第1階段建立第一個隧道以保護後來的ISAKMP協商消息。Phase2建立隧道，以保護通過安全連線傳輸的資料。有關ISAKMP的詳細資訊，請參閱適用於CLI命令的ISAKMP策略關鍵字。

組態

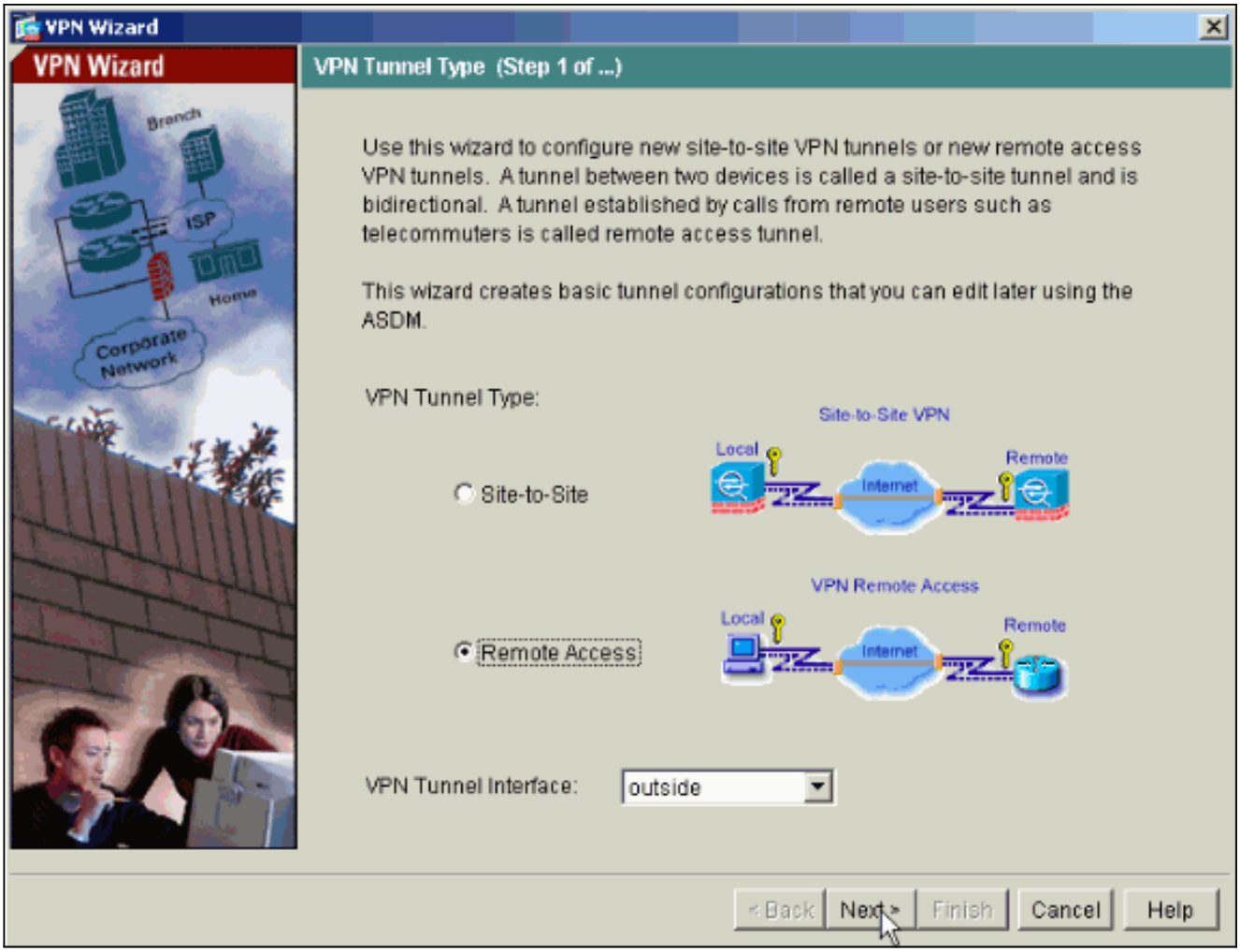
使用ASDM將ASA/PIX配置為遠端VPN伺服器

完成以下步驟，以便使用ASDM將Cisco ASA配置為遠端VPN伺服器：

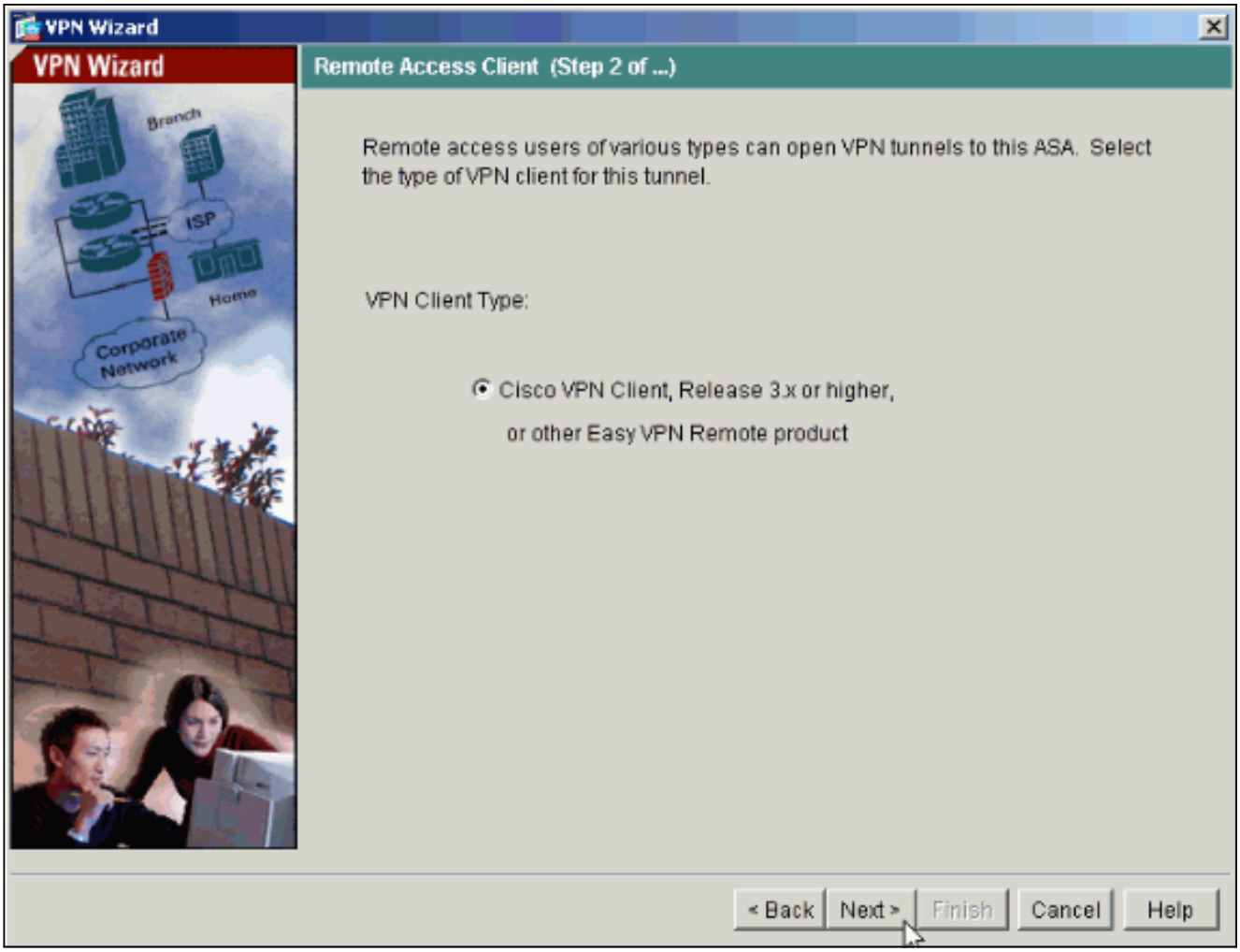
1. 從主視窗中選擇**Wizards > VPN Wizard**。



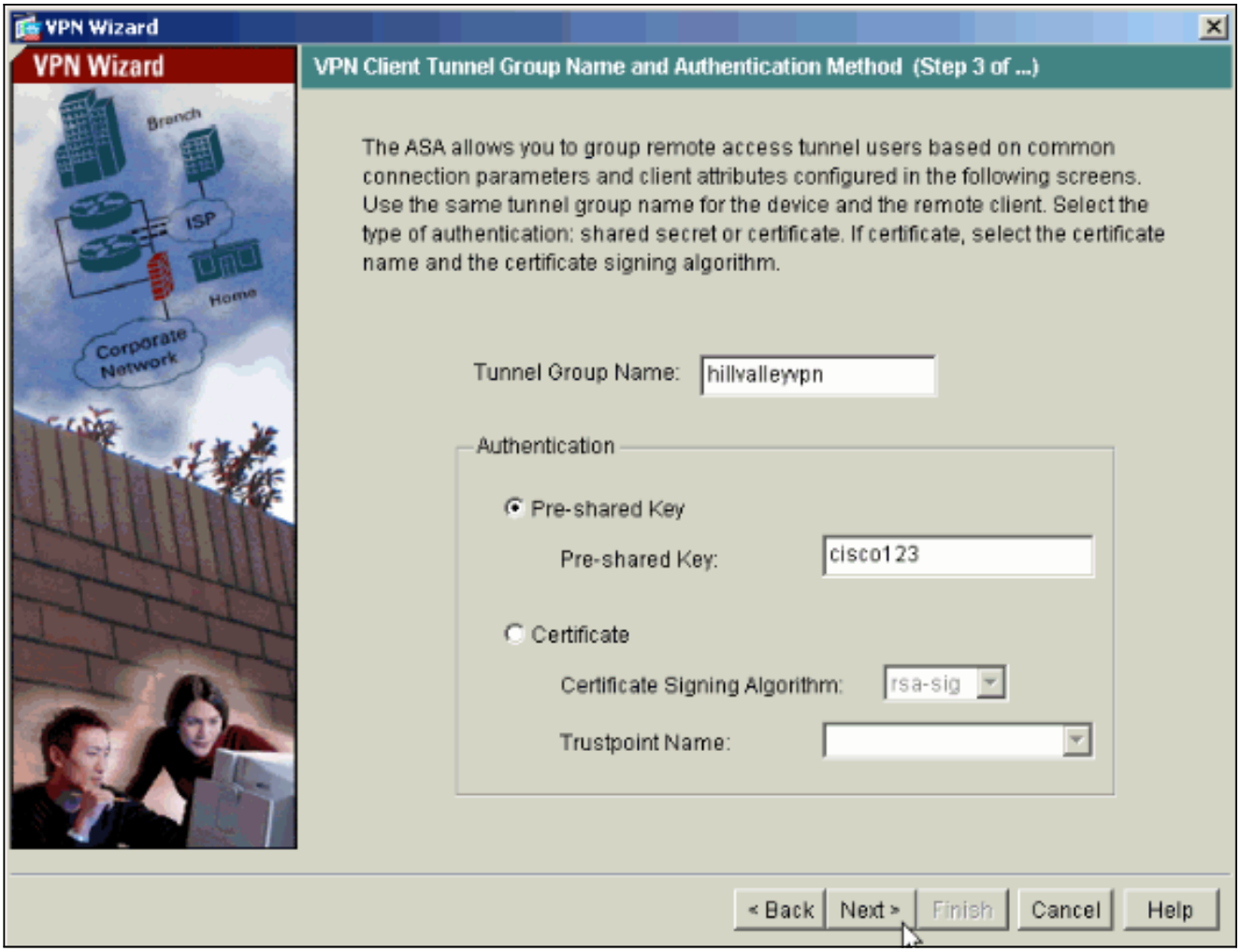
2. 選擇**Remote Access** VPN隧道型別，並確保已根據需要設定VPN隧道介面。



3. 已選擇唯一可用的VPN客戶端型別。按「**Next**」（下一步）。

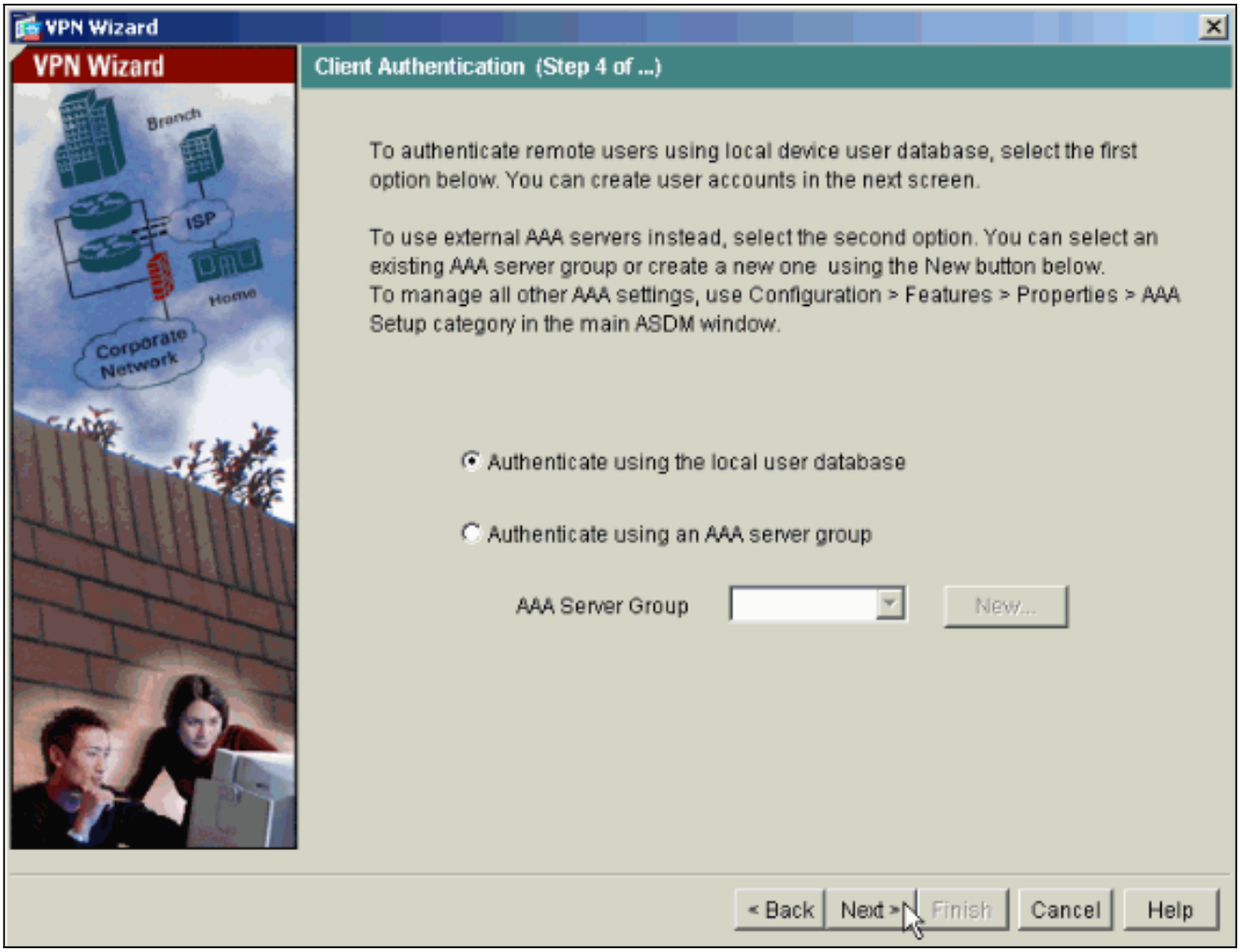


4. 輸入隧道組名稱的名稱。提供要使用的身份驗證資訊。**在此示例中**選擇了預共用金鑰。

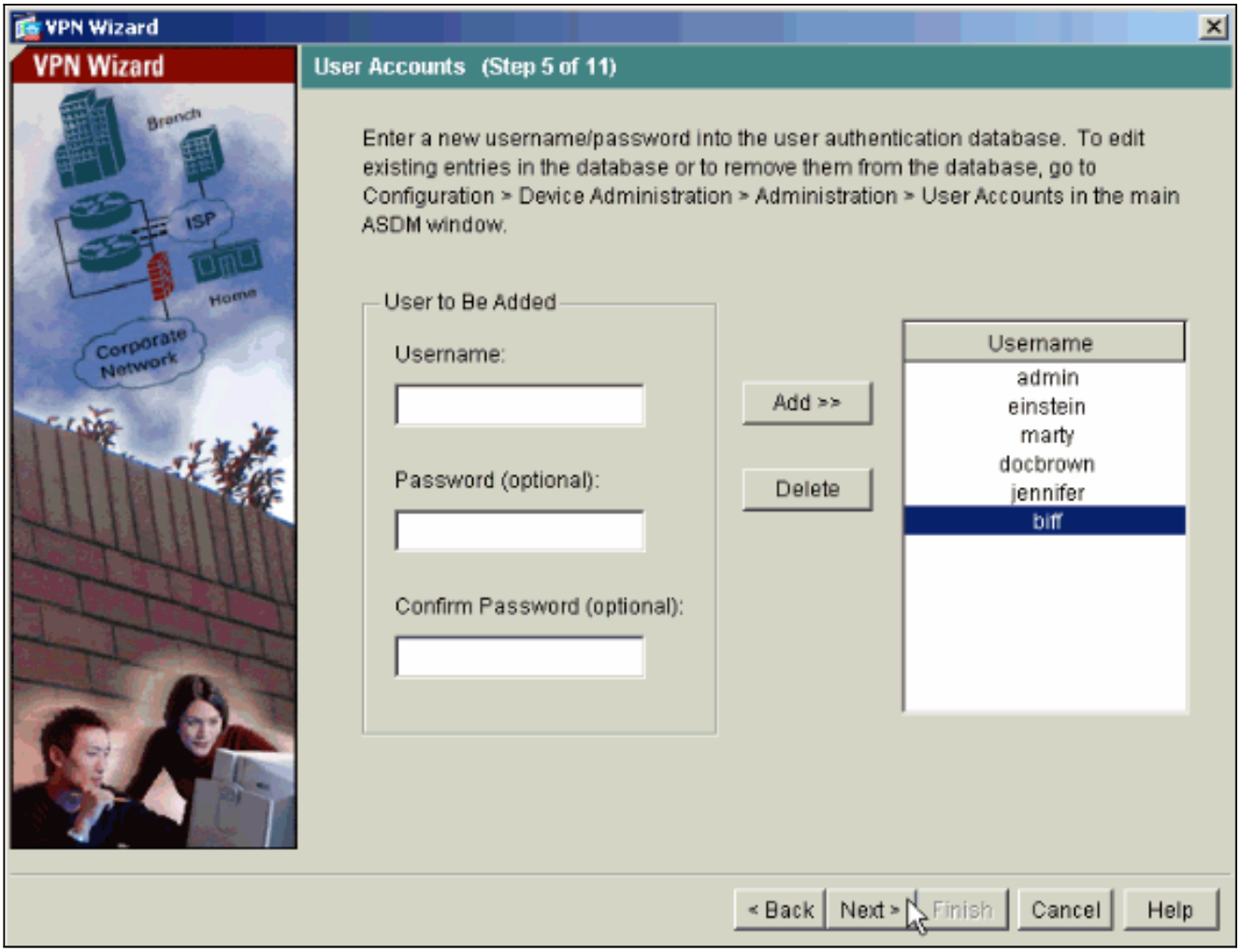


注意：無法隱藏/加密ASDM上的預共用金鑰。原因是ASDM只能由配置ASA的人員或協助客戶進行此配置的人員使用。

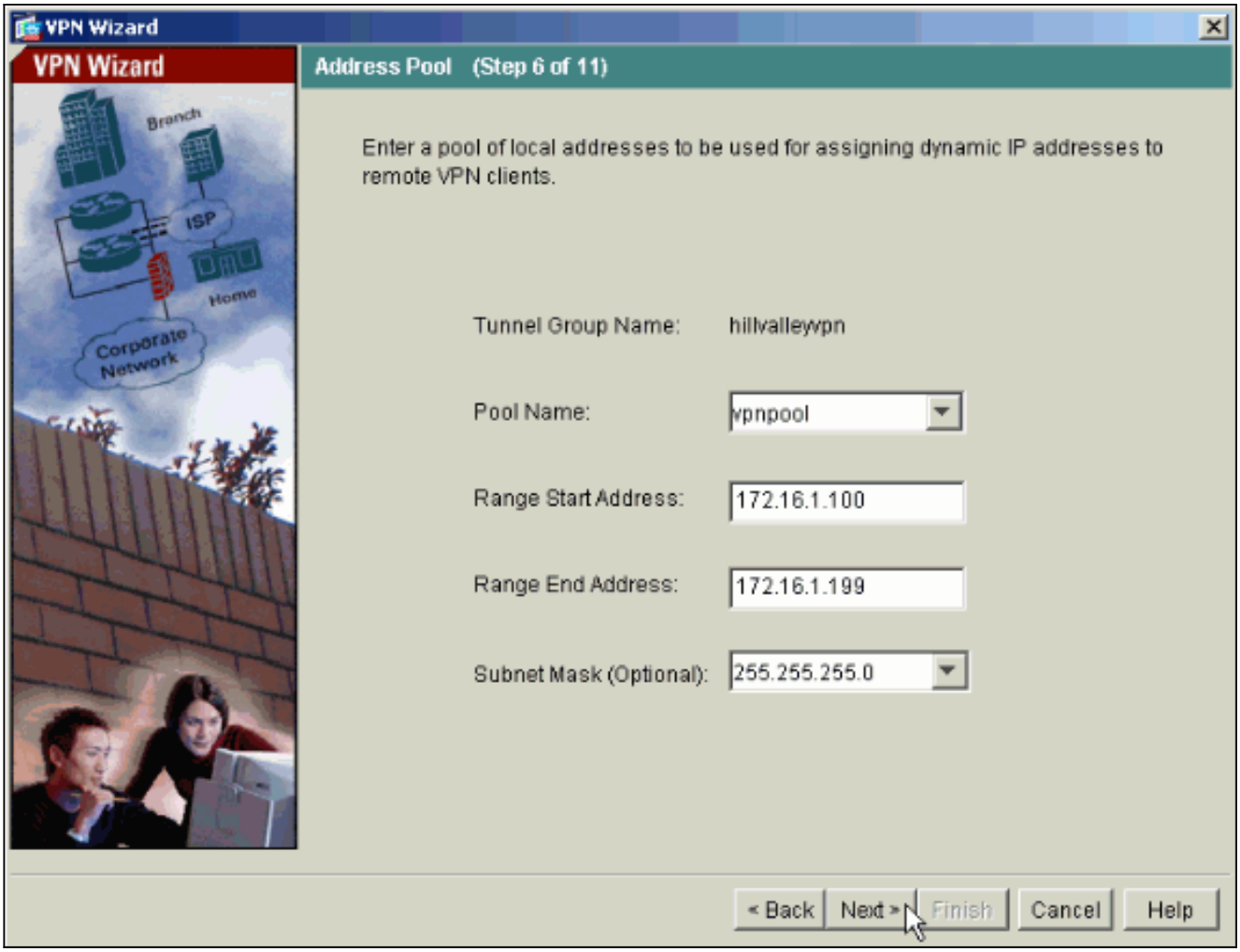
5. 選擇是要對本地使用者資料庫還是外部AAA伺服器組驗證遠端使用者。**註：您可**以在步驟6中將使用者新增到本地使用者資料庫。**注意**：有關如何通過ASDM配置外部AAA伺服器組的資訊，請參閱通過ASDM為VPN使用者配置PIX/ASA 7.x身份驗證和授權伺服器組配置示例。



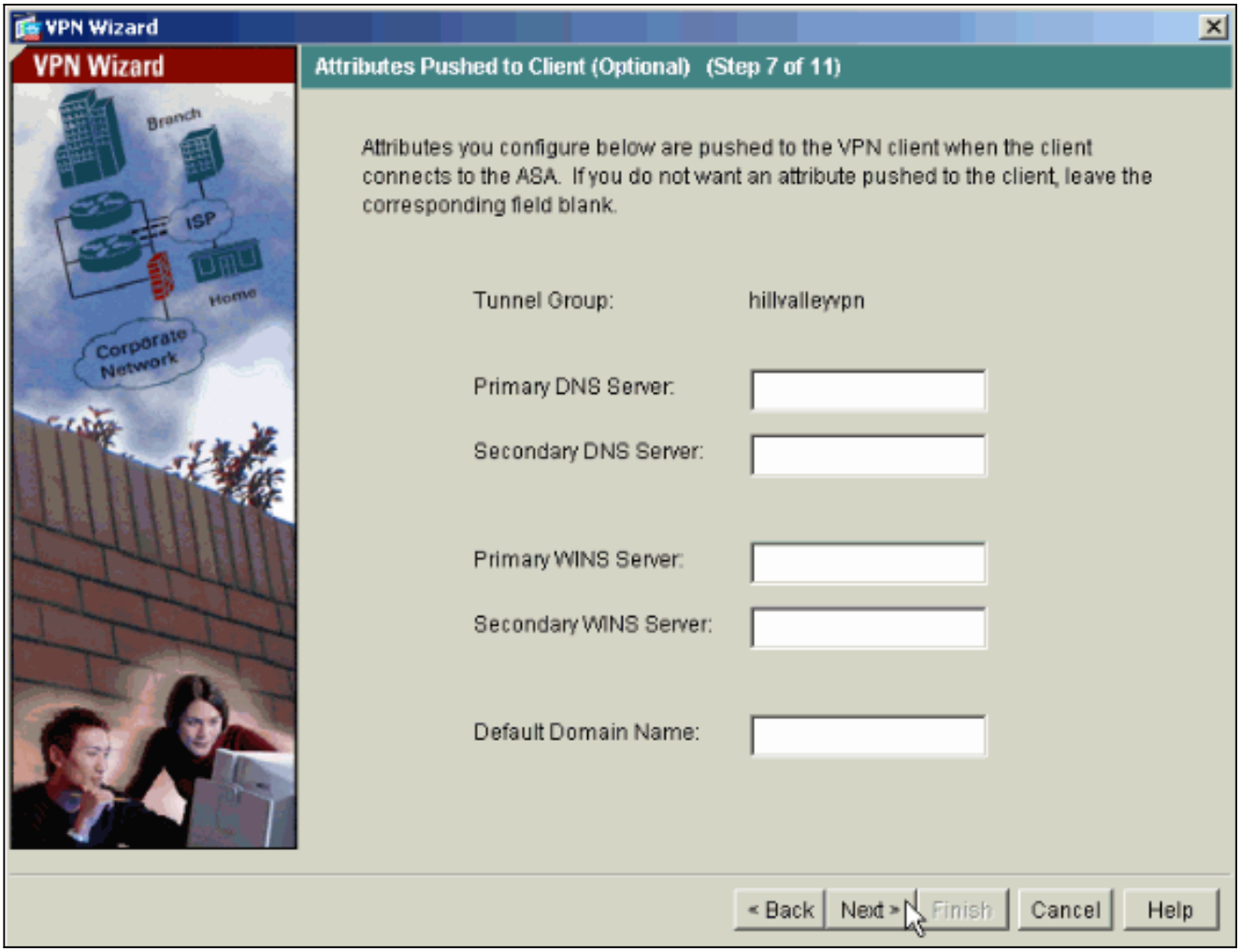
6. 如有必要，將使用者新增到本地資料庫。**注意**：不要從此視窗中刪除現有使用者。在ASDM主視窗中選擇**Configuration > Device Administration > Administration > User Accounts**，以編輯資料庫中的現有條目或從資料庫中刪除這些條目。



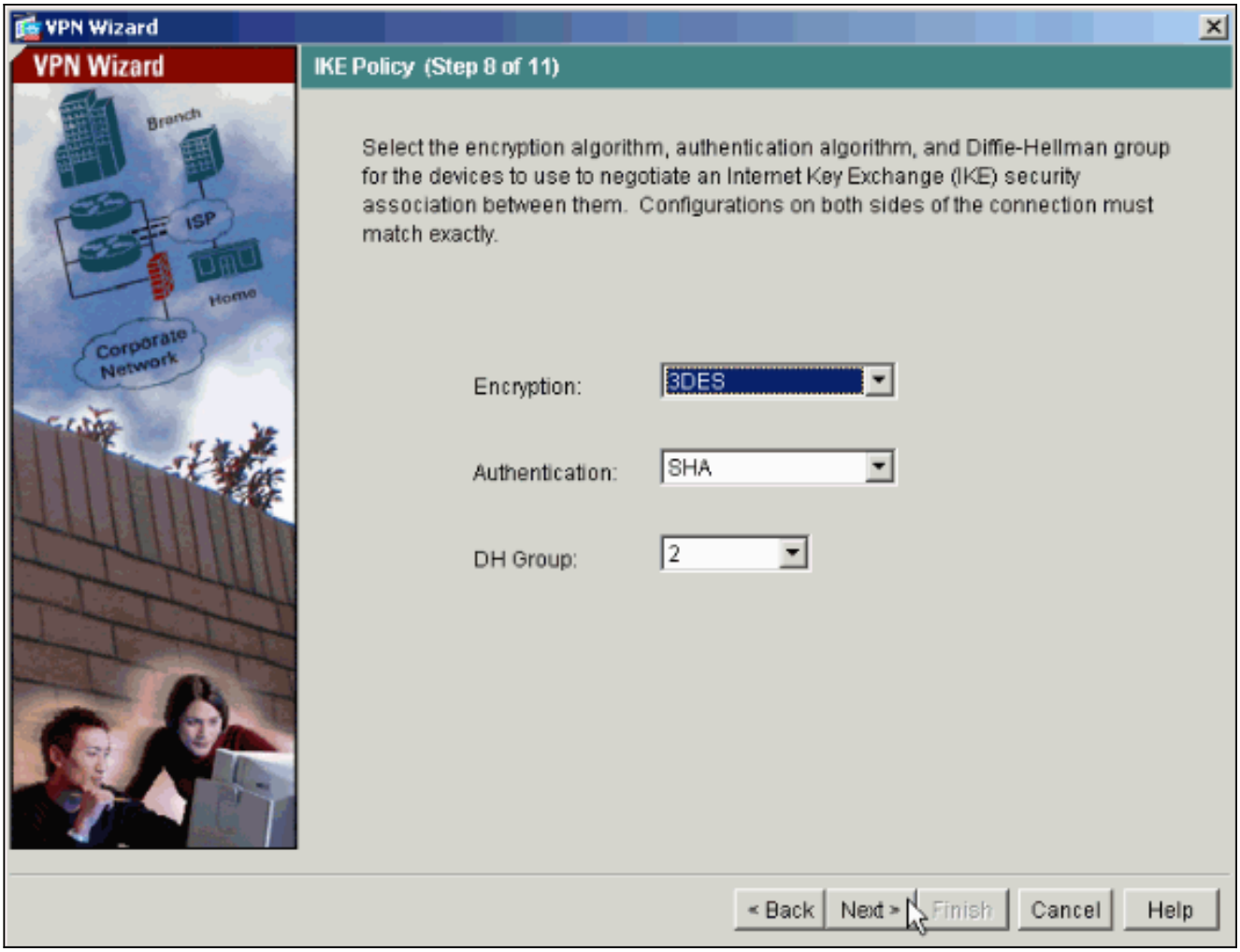
7. 定義一個本地地址池，在遠端VPN客戶端連線時將其動態分配給它們。



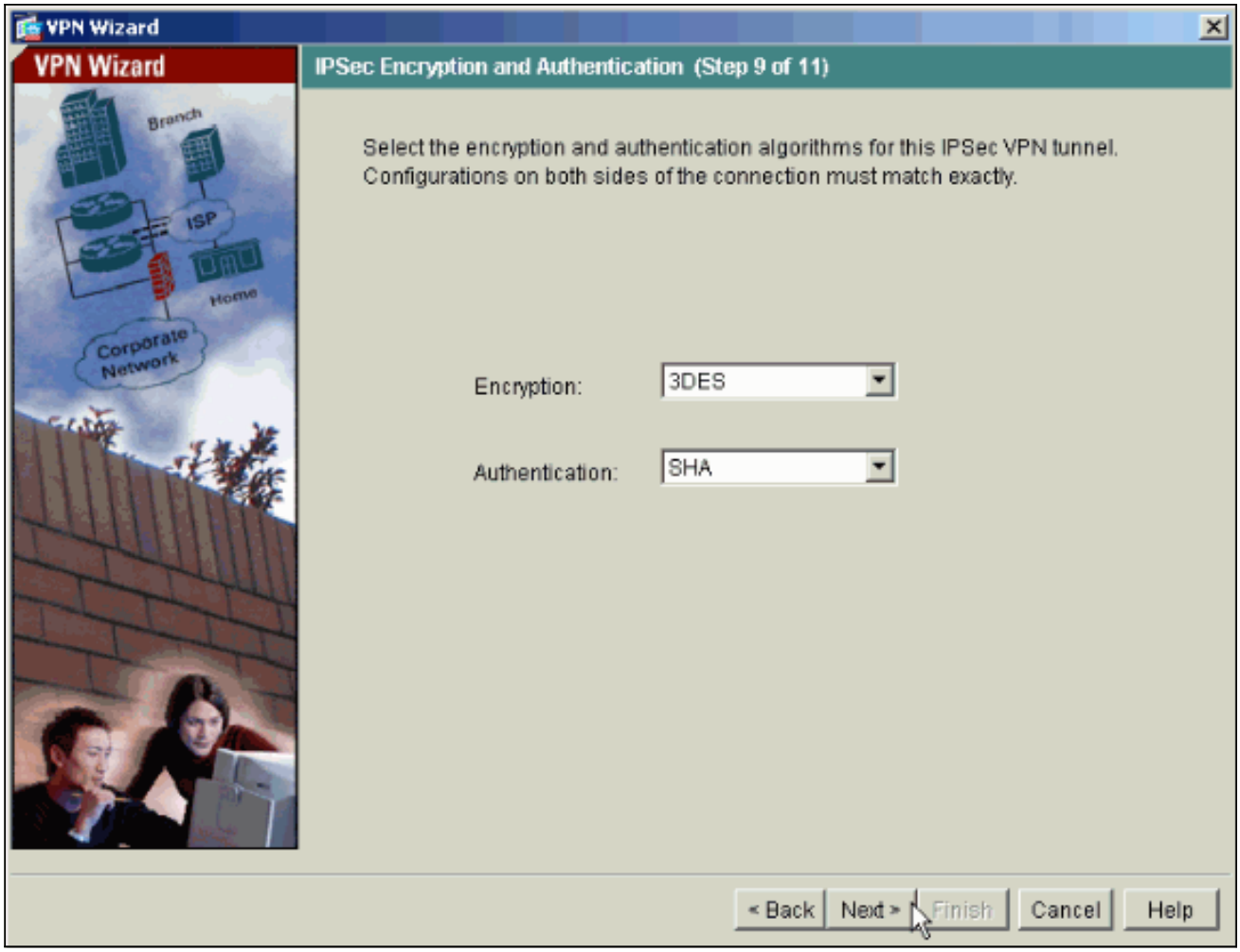
8. *可選：*指定要推送到遠端VPN客戶端的DNS和WINS伺服器資訊以及預設域名。



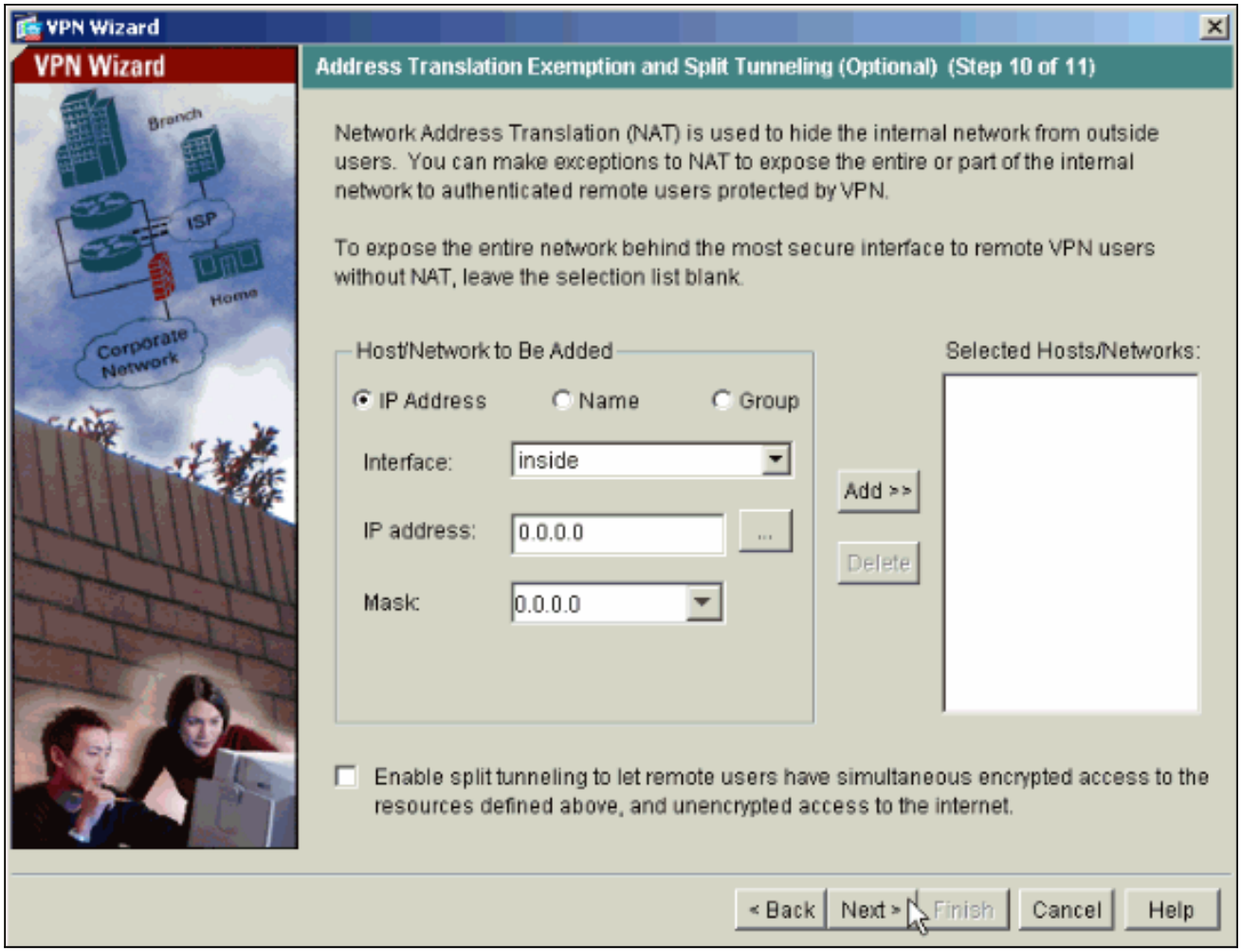
9. 指定IKE的引數，也稱為IKE階段1。通道兩端的設定必須完全相符。但是，Cisco VPN客戶端會自動為自己選擇正確的配置。因此，客戶端PC上無需進行IKE配置。



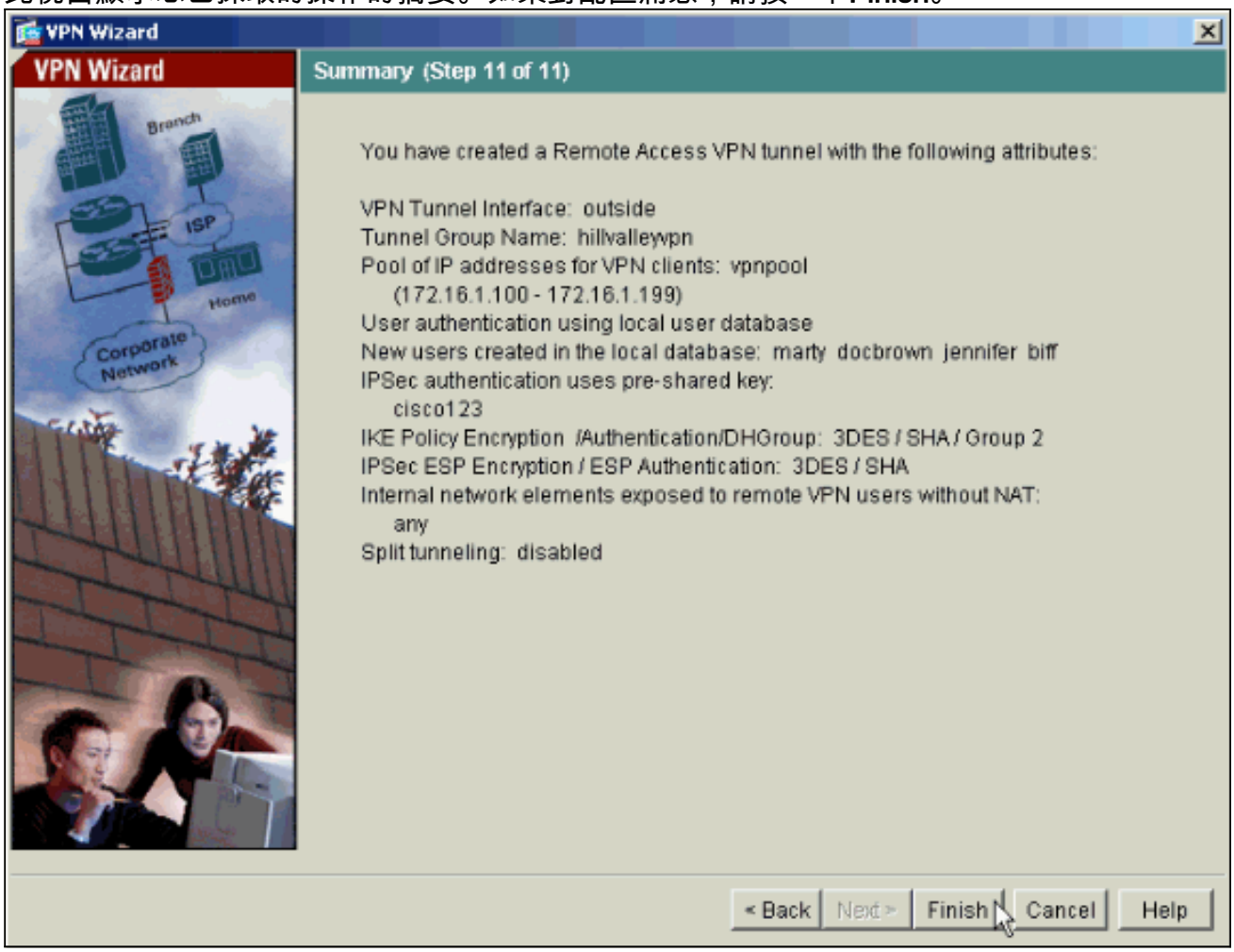
10. 指定IPSec（也稱為IKE階段2）的引數。通道兩端的設定必須完全相符。但是，Cisco VPN客戶端會自動為自己選擇正確的配置。因此，客戶端PC上無需進行IKE配置。



11. 指定應向遠端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。



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**。



使用CLI將ASA/PIX配置為遠端VPN伺服器

完成以下步驟，以便從命令列配置遠端VPN訪問伺服器。有關所使用的每個命令的詳細資訊，請參閱配置遠端訪問VPN或Cisco ASA 5500系列自適應安全裝置 — 命令參考。

1. 在全域性配置模式下輸入**ip local pool**命令，以配置用於VPN遠端訪問隧道的IP地址池。要刪除地址池，請輸入此命令的no形式。安全裝置使用基於連線隧道組的地址池。如果為隧道組配置多個地址池，安全裝置將按配置順序使用它們。發出此命令，以建立可用於向遠端訪問VPN客戶端分配動態地址的本地地址池：
   ```
   ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
     255.255.255.0
   ```

2. 發出以下命令：
   ```
   ASA-AIP-CLI(config)#username marty password 12345678
   ```

3. 發出此組命令以設定特定通道：ASA-AIP-CLI(config)#isakmp策**略1身份驗證預共用**ASA-AIP-CLI(config)#isakmp **policy 1 encryption 3des**ASA-AIP-CLI(config)#isakmp策**略1雜湊sha**ASA-AIP-CLI(config)#isakmp**策略1組2**ASA-AIP-CLI(config)#isakmp策**略1生存期43200**ASA-AIP-CLI(config)#isakmp enable **outside**ASA-AIP-CLI(config)**#crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI(config)**#crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA-AIP-CLI(config)**#crypto dynamic-map outside_dyn_map 10 set reverse-route**ASA-AIP-CLI(config)**#crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000**ASA-AIP-CLI(config)**#crypto map outside_map 10 ipsec-isakmp dynamic outside_dyn_map**ASA-AIP-CLI(config)**#crypto map outside_map interface outside**ASA-AIP-CLI(config)**#crypto isakmp nat-traversal**
4. *可選：*如果您希望連線繞過應用於介面的存取清單，請發出以下命令：
   ```
   ASA-AIP-CLI(config)#sysopt connection permit-ipsec
   ```

   注意：此命令適用於7.2(2)之前的7.x映像。 如果您使用映像7.2(2)，請發出`ASA-AIP-CLI(config)#sysopt connection permit-vpn`命令。
5. 發出以下命令：
   ```
   ASA-AIP-CLI(config)#group-policy hillvalleyvpn internal
   ```

6. 發出以下命令以配置客戶端連線設定：ASA-AIP-CLI(config)**#group-policy hillvalleyvpn屬性**ASA-AIP-CLI(config)#(config-group-policy)**#dns-server value 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)**#vpn-tunnel-protocol IPSec**ASA-AIP-CLI(config)#(config-group-policy)**#default-domain value test.com**
7. 發出以下命令：
   ```
   ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-ra
   ```

8. 發出以下命令：
   ```
   ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-attributes
   ```

9. 發出以下命令：
   ```
   ASA-AIP-CLI(config-tunnel-ipsec)#pre-shared-key cisco123
   ```

10. 發出以下命令：
    ```
    ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn general-attributes
    ```

11. 發出此命令，以引用本地使用者資料庫進行身份驗證。
    ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**

12. 將組策略與隧道組關聯
    ASA-AIP-CLI(config-tunnel-ipsec)# **default-group-policy hillvalleyvpn**

13. 在hillvalleyvpn tunnel-group的general-attributes模式下發出此命令，以便將步驟1中建立的vpnpool分配給hillvalleyvpn組。
    ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

在ASA裝置上運行配置

```
ASA-AIP-CLI(config)#show running-config
ASA Version 7.2(2)
!
hostname ASAwAIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
```

```
arp timeout 14400
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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
 dns-server value 172.16.1.11
 vpn-tunnel-protocol IPSec
 default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map outside_map 10 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
 address-pool vpnpool
 default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Cisco VPN客戶端密碼儲存配置

如果您有多個Cisco VPN客戶端，則很難記住所有VPN客戶端使用者名稱和密碼。要在VPN客戶端電腦中儲存密碼，請按照本節所述配置ASA/PIX和VPN客戶端。

ASA/PIX

在全域性配置模式下使用**group-policy attributes**命令：

```
group-policy VPNusers attributes
  password-storage enable
```

Cisco VPN使用者端

編輯**.pcf檔案**並修改以下引數：

```
SaveUserPassword=1
UserPassword=
```

禁用擴展身份驗證

在隧道組模式下，輸入以下命令以禁用PIX/ASA 7.x上的擴展身份驗證（預設情況下啟用）：

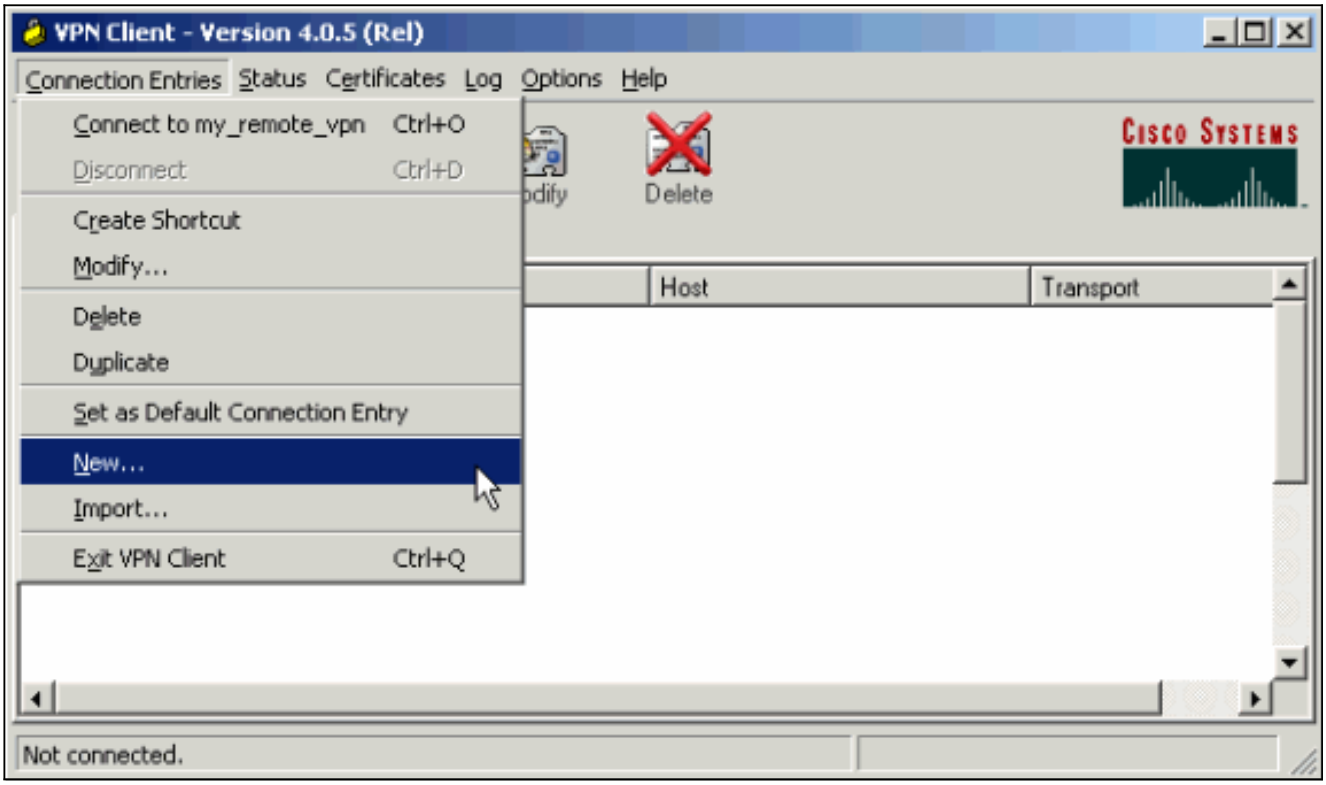
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

禁用擴展身份驗證後，VPN客戶端不會彈出用於身份驗證(Xauth)的使用者名稱/密碼。 因此，ASA/PIX不需要使用者名稱和密碼配置來驗證VPN客戶端。

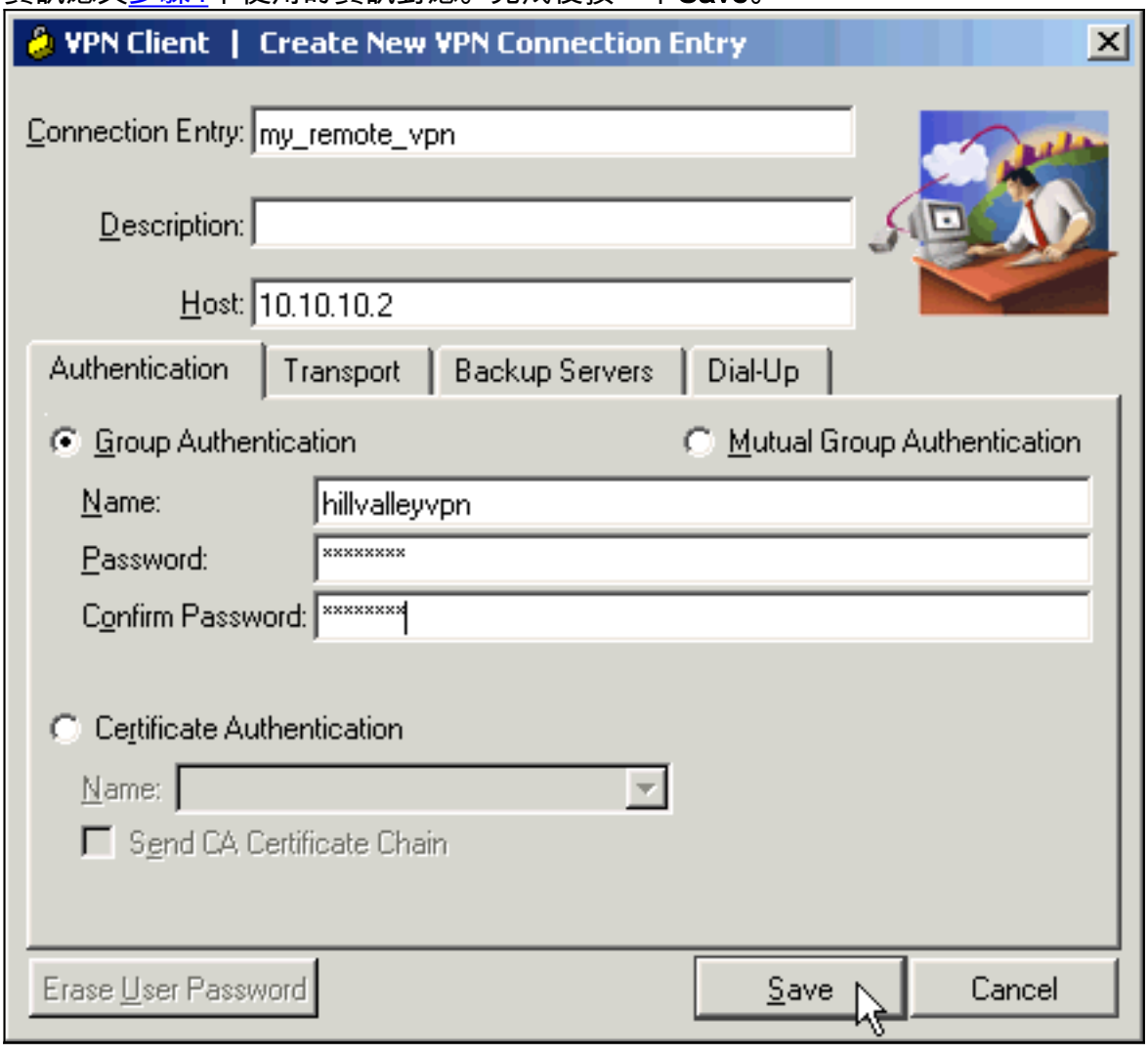
驗證

嘗試使用Cisco VPN客戶端連線到Cisco ASA，以驗證ASA配置是否成功。

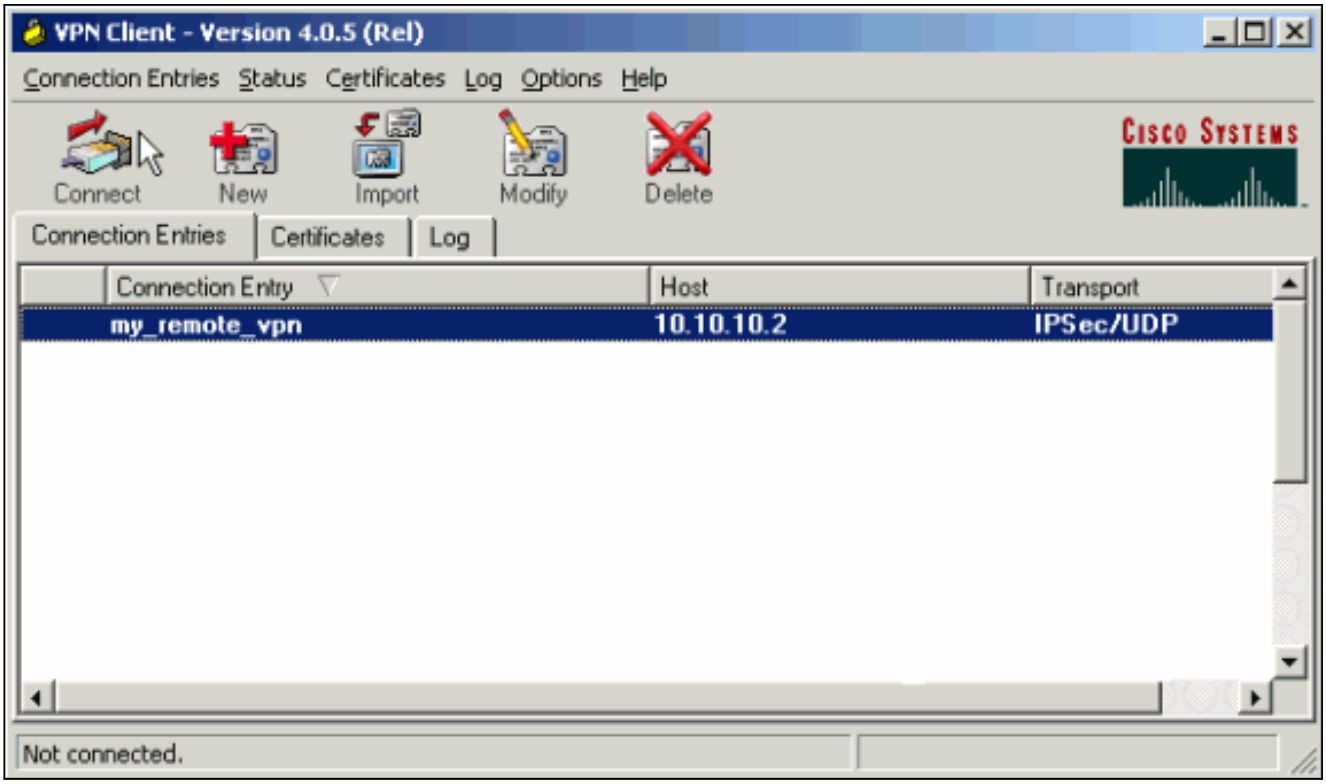
1. 選擇Connection Entries > New。



2. 填寫新連線的詳細資訊。Host欄位應包含先前配置的Cisco ASA的IP地址或主機名。群組驗證資訊應與步驟4中使用的資訊對應。完成後按一下Save。

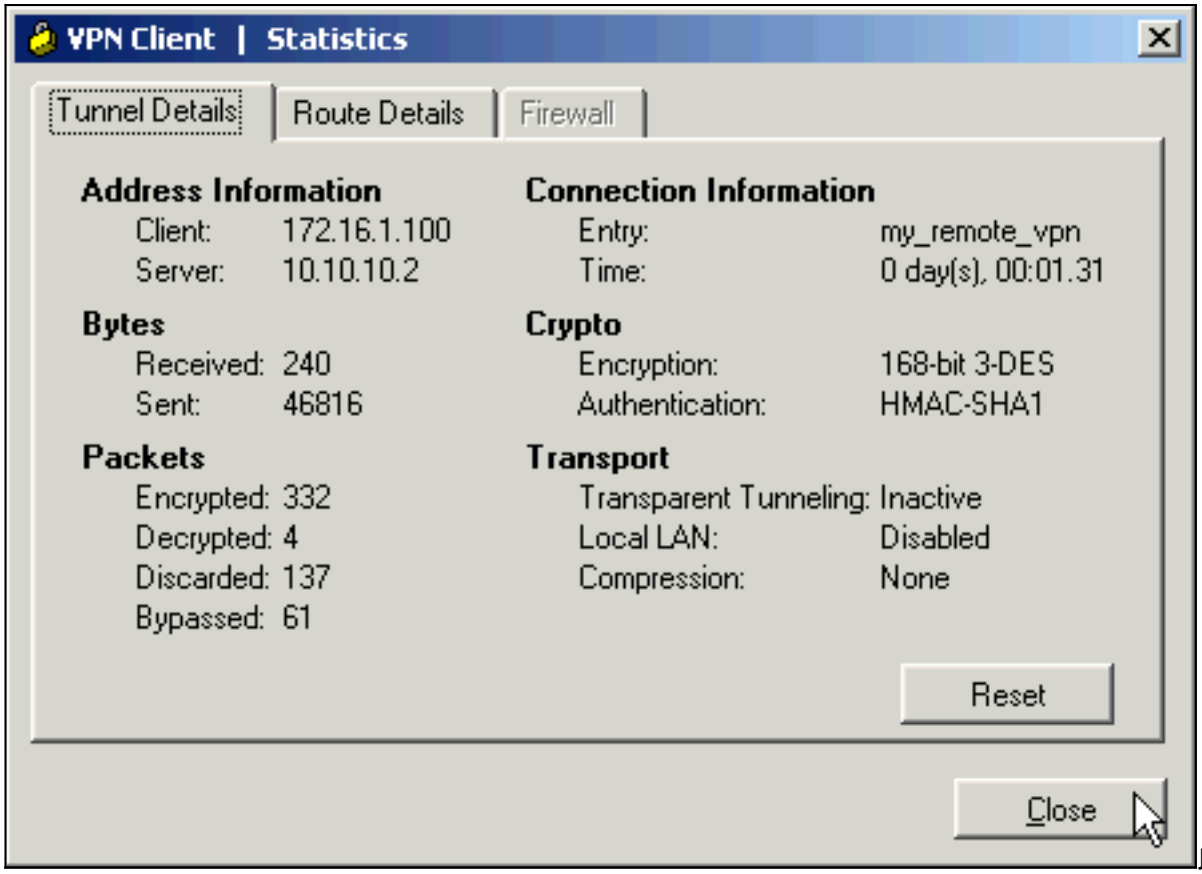


3. 選擇新建立的連線，然後按一下Connect。

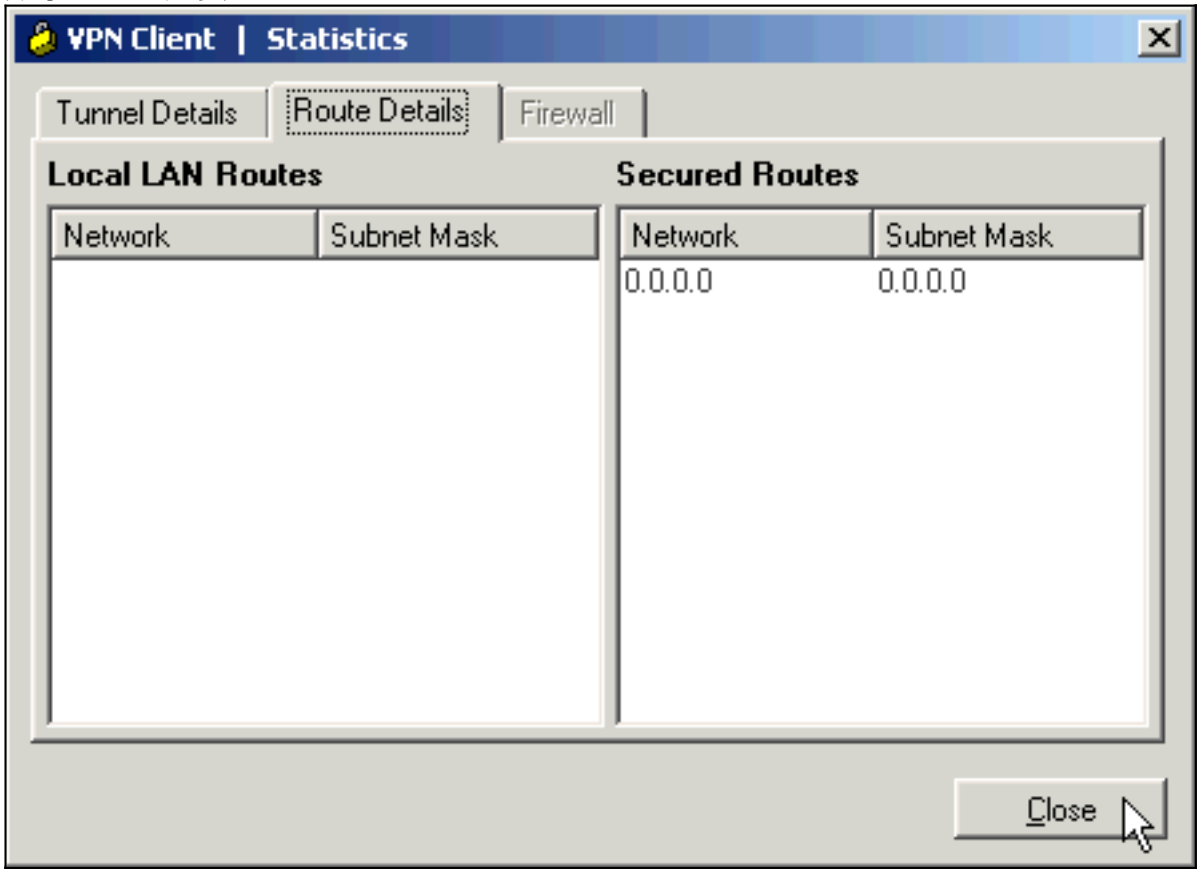


4. 輸入用於擴展身份驗證的使用者名稱和密碼。此資訊應與步驟5和6中指定的資訊相符。

5. 成功建立連線後，從Status選單中選擇**Statistics**以驗證隧道的詳細資訊。此視窗顯示流量和加密資訊

: 

此視窗顯示分割隧道資訊

: 

疑難排解

使用本節內容，對組態進行疑難排解。

加密ACL不正確

眾所周知，ASDM 5.0(2)會建立和應用加密訪問控制清單(ACL)，這可能會給使用分割隧道的VPN客戶端以及在網路擴展模式下的硬體客戶端造成問題。使用ASDM 5.0(4.3)或更高版本可避免此問題。如需更多詳細資訊，請參閱Cisco錯誤ID CSCsc10806(僅限註冊客戶)。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 最常見的L2L和遠端訪問IPsec VPN故障排除解決方案
- Cisco ASA 5500系列自適應安全裝置故障排除和警報
- 技術支援與文件 - Cisco Systems