使用預共用金鑰在Windows 8 PC和ASA之間配置L2TP Over IPsec

目錄

簡介

本檔案介紹如何在Cisco Adaptive Security Appliance(ASA)和Windows 8本機使用者端之間使用預先共用金鑰，透過IPsec設定第2層通道通訊協定(L2TP)。

L2TP over Internet Protocol Security(IPsec)提供在單一平台中部署和管理L2TP虛擬專用網路(VPN)解決方案以及IPsec VPN和防火牆服務的功能。

必要條件

需求

思科建議您瞭解以下主題：

- 從客戶端電腦到ASA的IP連線。要測試連線，請嘗試從客戶端終端ping ASA的IP地址，反之亦然
- 確保UDP埠500和4500以及封裝安全負載(ESP)協定在連線路徑上的任何位置都不會被阻止

限制

- L2TP over IPsec僅支援IKEv1。不支援IKEv2。
- 在ASA上使用IPsec的L2TP允許LNS與整合在Windows、MAC OS X、Android和Cisco IOS等作業系統中的本地VPN客戶端進行互操作。僅支援帶有IPsec的L2TP，ASA不支援本地L2TP本身。
- Windows客戶端支援的最小IPsec安全關聯生存時間為300秒。如果ASA上的生存時間設定為少於300秒，Windows客戶端會將其忽略，並用300秒的生存時間替換。
- ASA僅支援本地資料庫上的點對點協定(PPP)身份驗證密碼身份驗證協定(PAP)和Microsoft質詢握手身份驗證協定(CHAP)版本1和2。可擴展身份驗證協定(EAP)和CHAP由代理身份驗證伺服器執行。因此，如果遠端使用者屬於使用**authentication eap-proxy**或**authentication chap**命令配置的隧道組，並且ASA配置為使用本地資料庫，則該使用者無法連線。

支援的PPP身份驗證型別

ASA上的L2TP over IPsec連線僅支援表中所示的PPP身份驗證型別

AAA伺服器支援和PPP驗證型別

AAA伺服器型別	支援的PPP身份驗證型別
本地	PAP、MSCHAPv1、MSCHAPv2
RADIUS	PAP、CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACACS+	PAP、CHAP、MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

PPP身份驗證型別特徵

關鍵字	驗證型別	
chap	CHAP	響應伺服器質詢，客戶端返回帶有明文使用者名稱的加密[質詢加密碼]。此通
eap-proxy	EAP	啟用允許安全裝置將PPP身份驗證過程代理到外部RADIUS身份驗證伺服器的
ms-chap-v1	Microsoft CHAP版本1	與CHAP類似，但更安全的是，伺服器僅儲存和比較加密密碼，而不是像CH
ms-chap-v2	Microsoft CHAP，版本，2	
pap	PAP	在身份驗證期間傳遞明文使用者名稱和密碼，並且不安全。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科5515系列ASA，運行軟體版本9.4(1)
- L2TP/IPSec客戶端(Windows 8)

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。

相關產品

此配置還可以與Cisco ASA 5500系列安全裝置8.3(1)或更高版本配合使用。

慣例

如需檔案慣例的詳細資訊，請參閱思科技術提示慣例

背景資訊

第2層通道通訊協定(L2TP)是VPN通道通訊協定，允許遠端使用者端使用公用IP網路與私人企業網路伺服器安全通訊。L2TP使用PPP over UDP（連線埠1701）來通道傳輸資料。

L2TP協定基於客戶端/伺服器模型。功能在L2TP網路伺服器(LNS)和L2TP訪問集中器(LAC)之間劃分。 LNS通常在網路網關（例如ASA）上運行，而LAC可以是撥號網路訪問伺服器(NAS)或帶有捆綁的L2TP客戶端（例如Microsoft Windows、Apple iPhone或Android）的終端裝置。

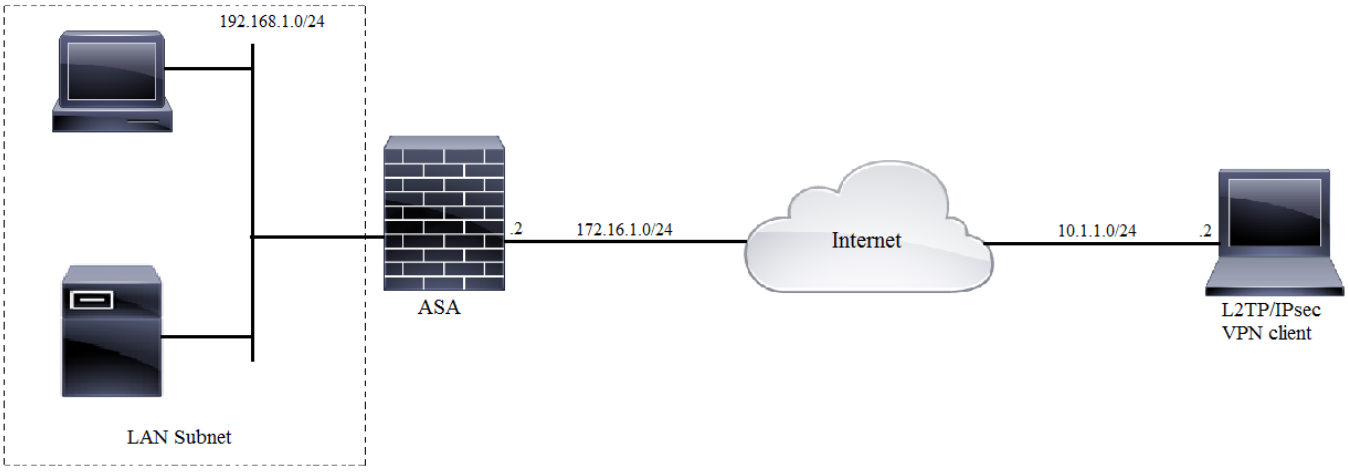
設定

本節提供用於設定本檔案中所述功能的資訊。

> **附註**：使用命令查詢工具(僅供已註冊客戶使用)可查詢有關本文檔中所用命令的更多資訊。

> **附註**：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

網路圖表

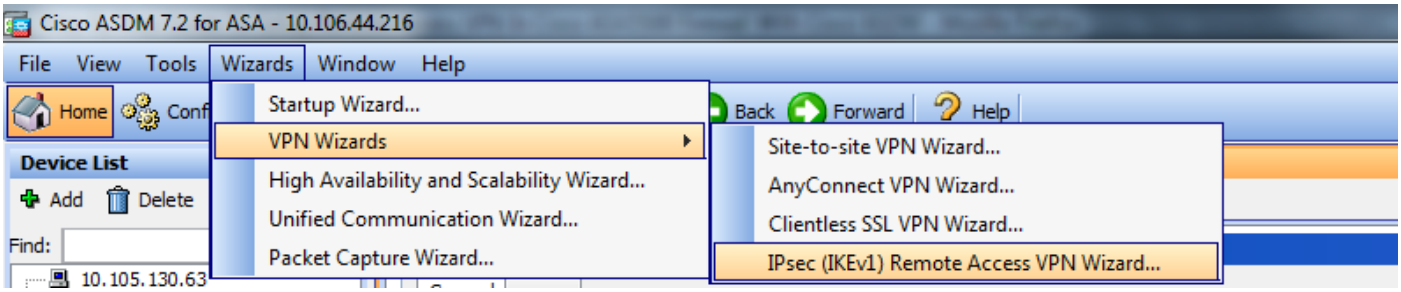


全通道組態

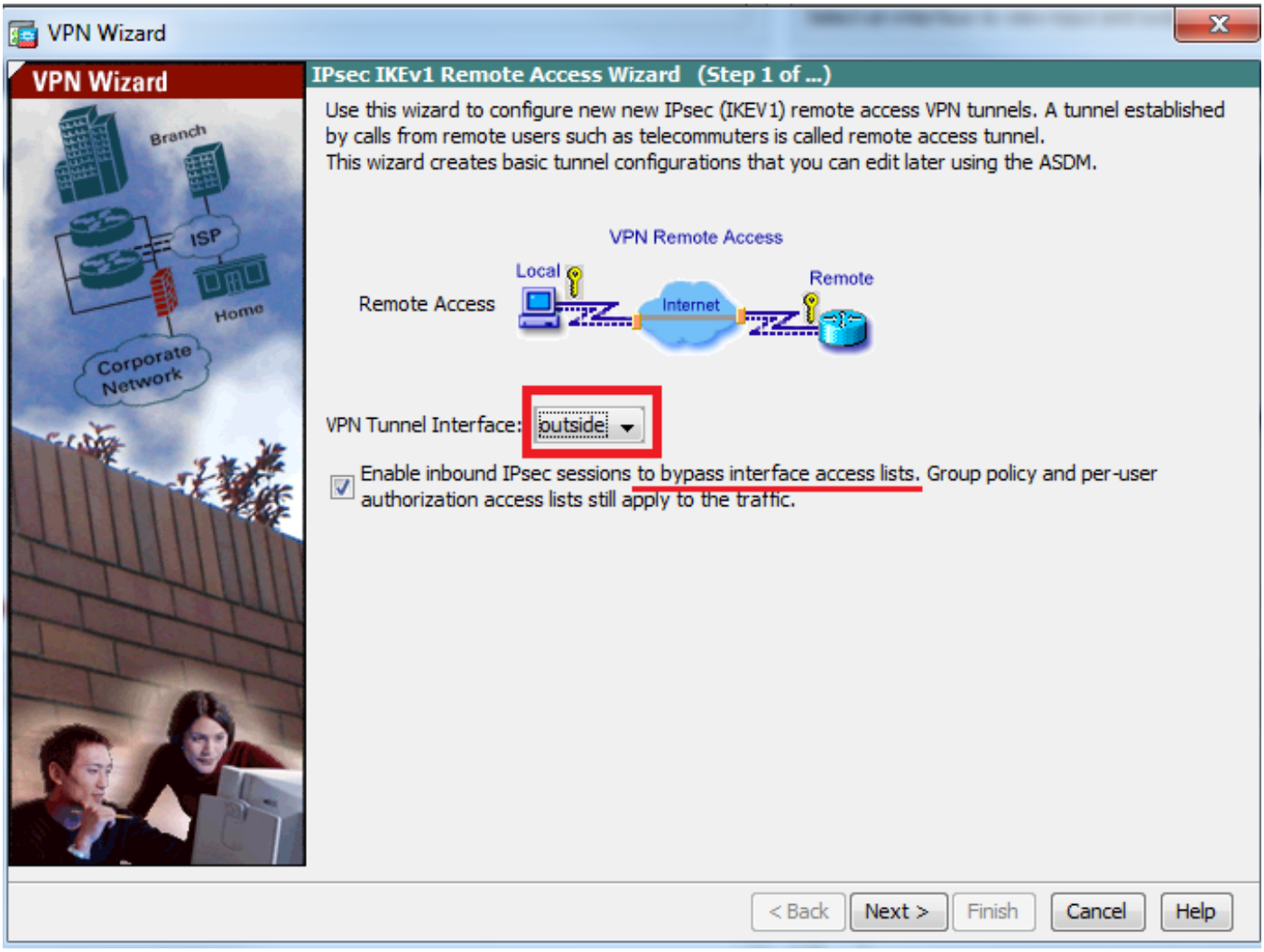
使用自適應安全裝置管理器(ASDM)的ASA配置

請完成以下步驟：

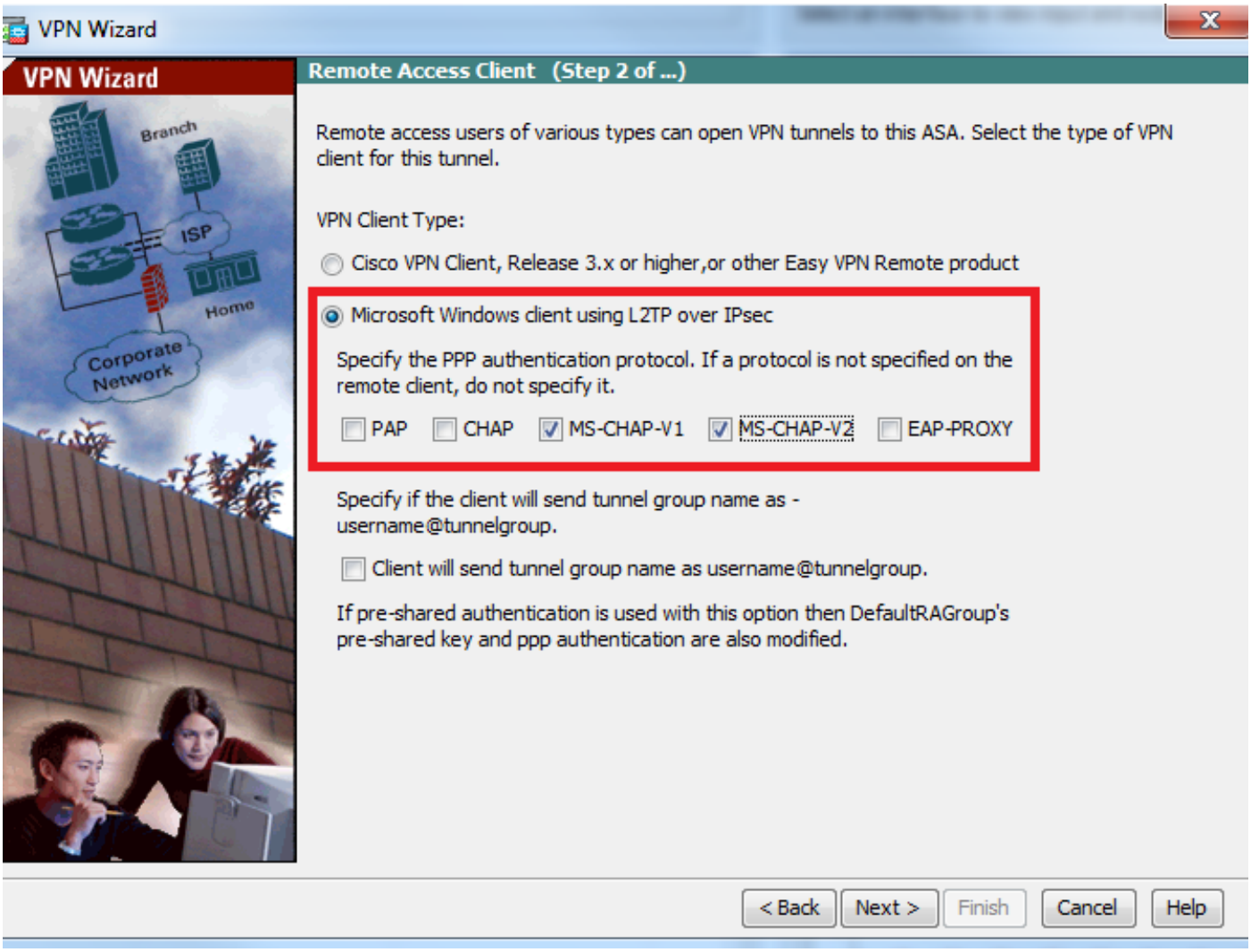
步驟1.登入到ASDM，然後導航到**Wizards > VPN Wizards > Ipsec(IKEv1)Remote Access VPN Wizard**。



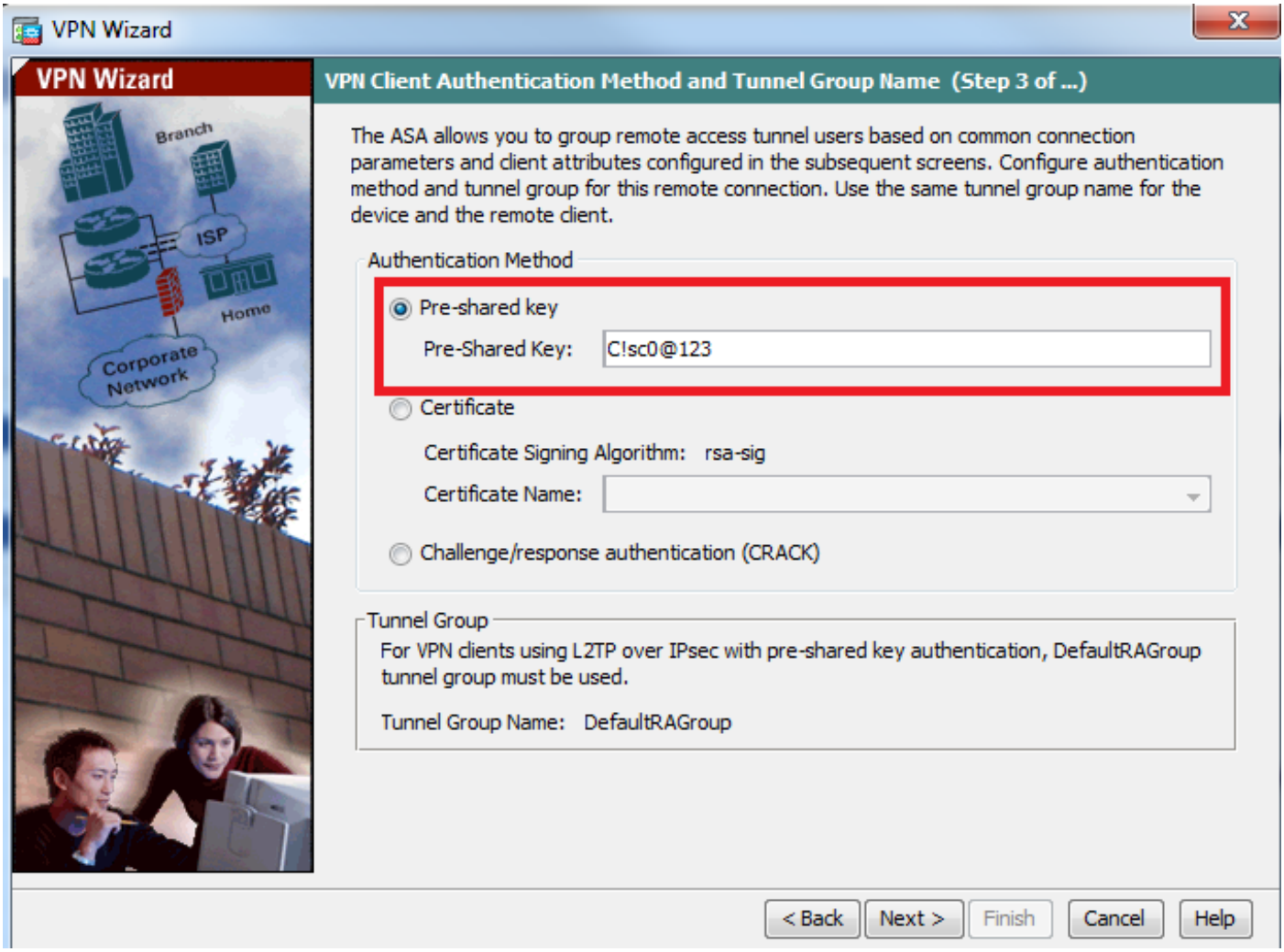
步驟2.出現Remote Access VPN設定視窗。從下拉選單中，選擇必須終止VPN隧道的介面。在此示例中，外部介面連線到WAN，因此在此介面上終止VPN隧道。保留**啟用入站IPSec會話以繞過介面訪問清單框。組策略和每使用者授權訪問清單仍然應用於檢查的流量**，因此不需要在外部介面上配置新的訪問清單來允許客戶端訪問內部資源。按「**Next**」（下一步）。



步驟3.如本圖所示，選擇客戶端型別作為**Microsoft Windows客戶端，使用L2TP over IPSec**和**MS-CHAP-V1**以及**MS-CHAP-V2**作為PPP身份驗證協定，因為PAP不安全，並且LOCAL資料庫不支援其他身份驗證型別作為身份驗證伺服器，然後按一下**下一步**。

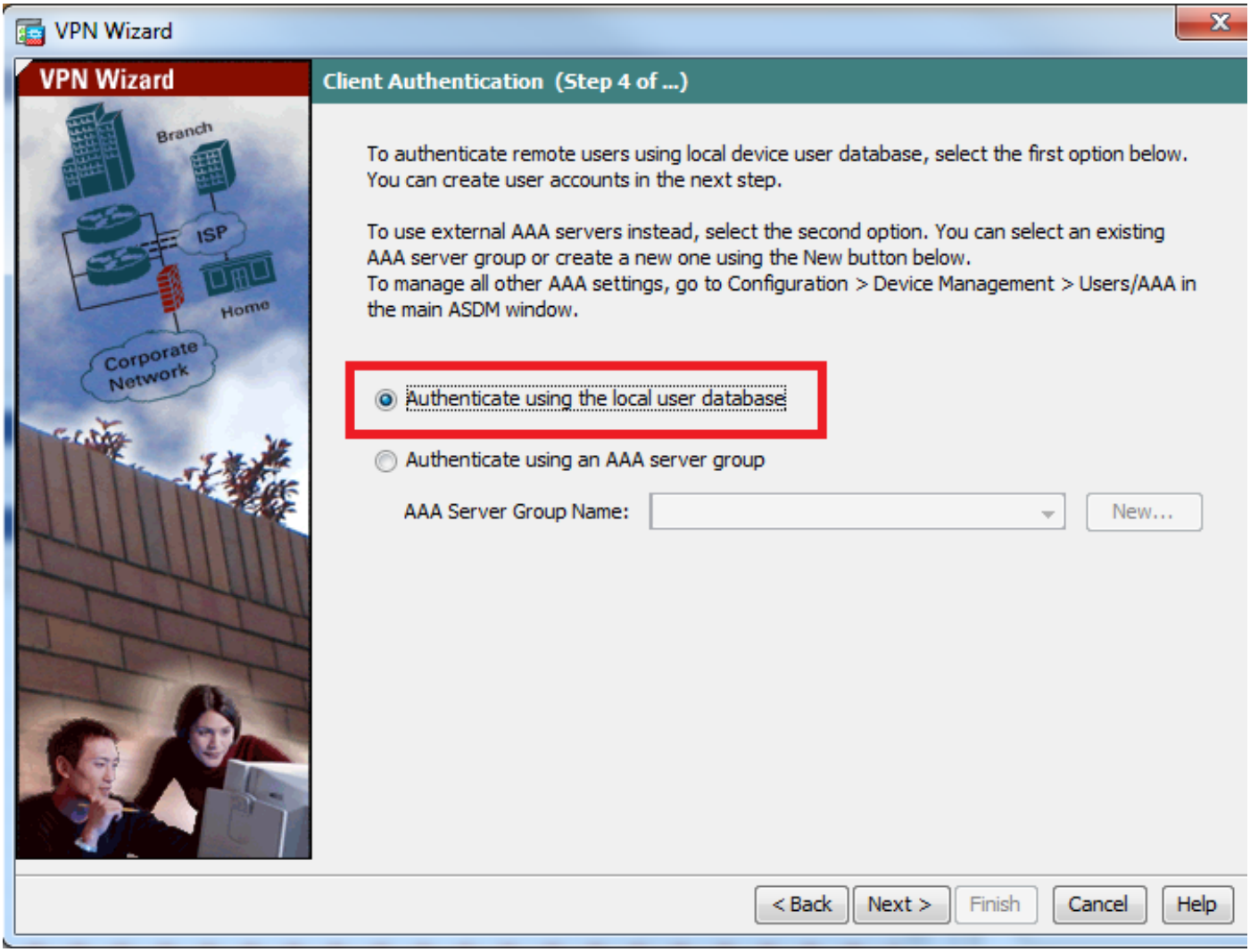


步驟4.選擇驗證方法作為**Pre-shared-key**，然後在客戶端鍵入必須相同的預共用金鑰，然後按一下**Next**，如下圖所示。

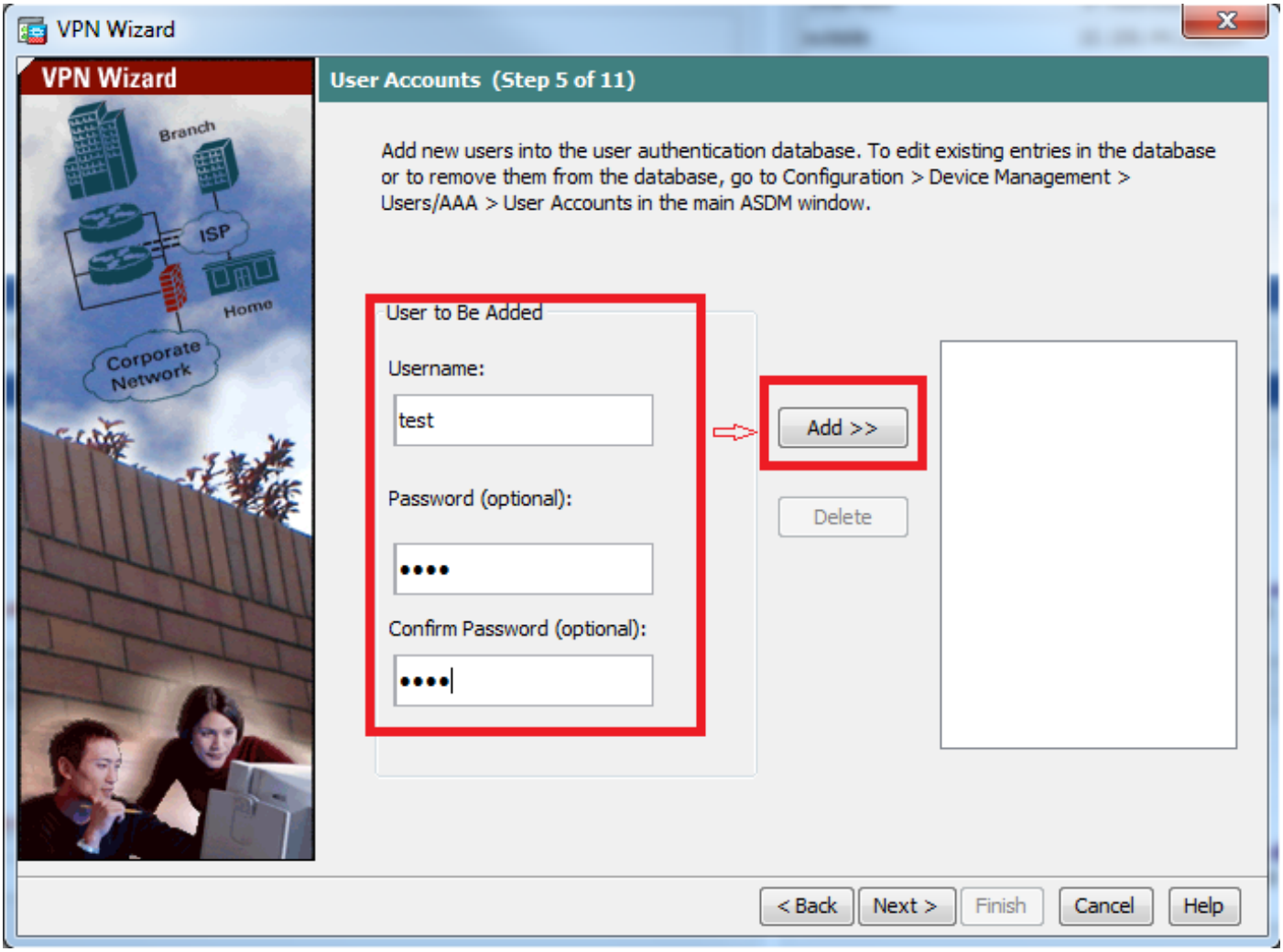


步驟5.指定對嘗試通過IPsec進行L2TP連線的使用者進行身份驗證的方法。可以使用外部AAA身份驗證伺服器或它自己的本地資料庫。如果要根據ASA的本地資料庫對客戶端進行身份驗證，請選擇**Authenticate using the local user database**，然後按一下**Next**。

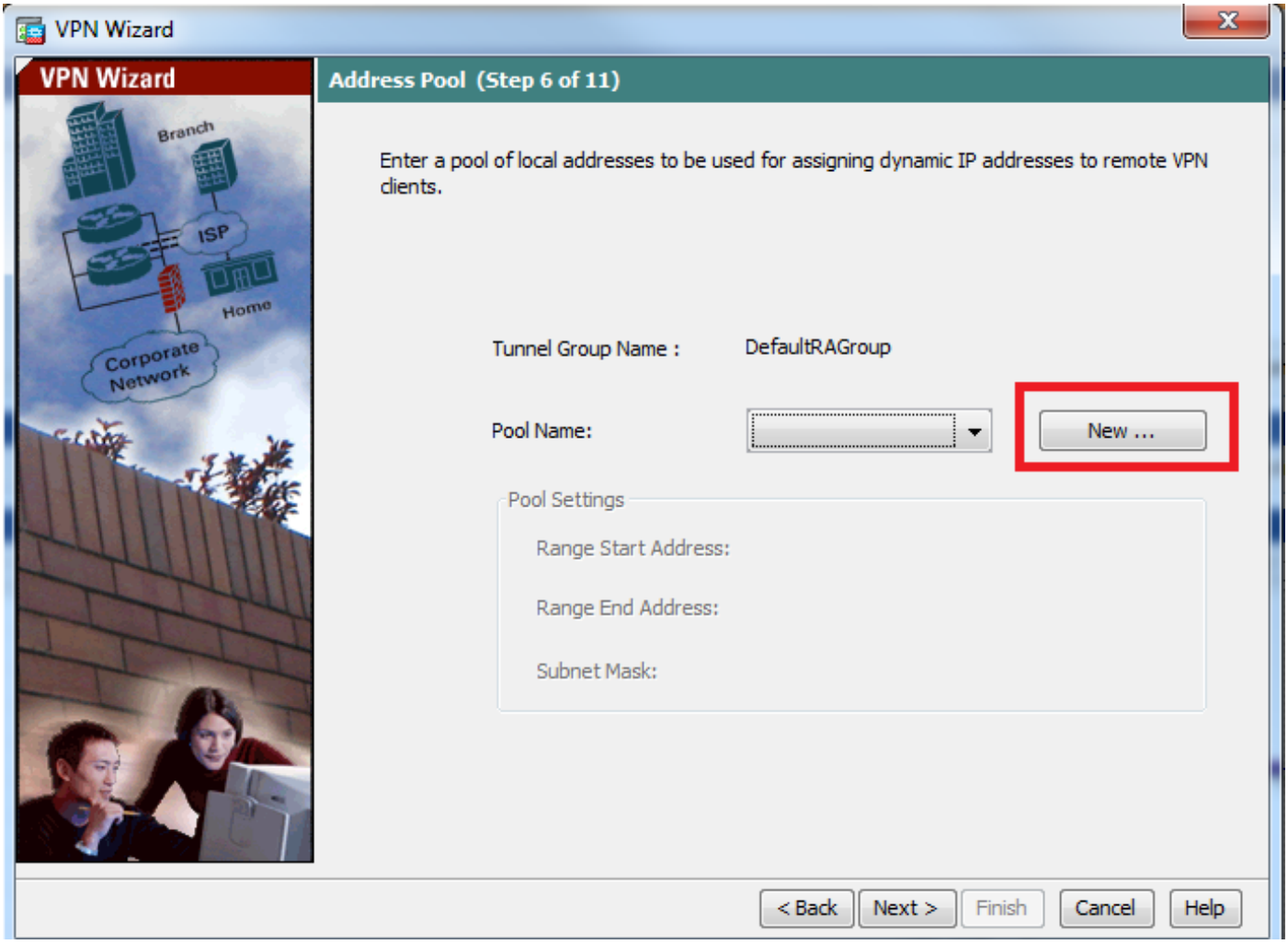
附註：請參閱為VPN使用者配置RADIUS身份驗證，以使用外部AAA伺服器對使用者進行身份驗證。



步驟6.若要將新使用者新增到本地資料庫以進行使用者身份驗證，請輸入使用者名稱和密碼，然後按一下**ADD**，否則可以使用資料庫中的現有使用者帳戶，如下圖所示。按「**Next**」（下一步）。

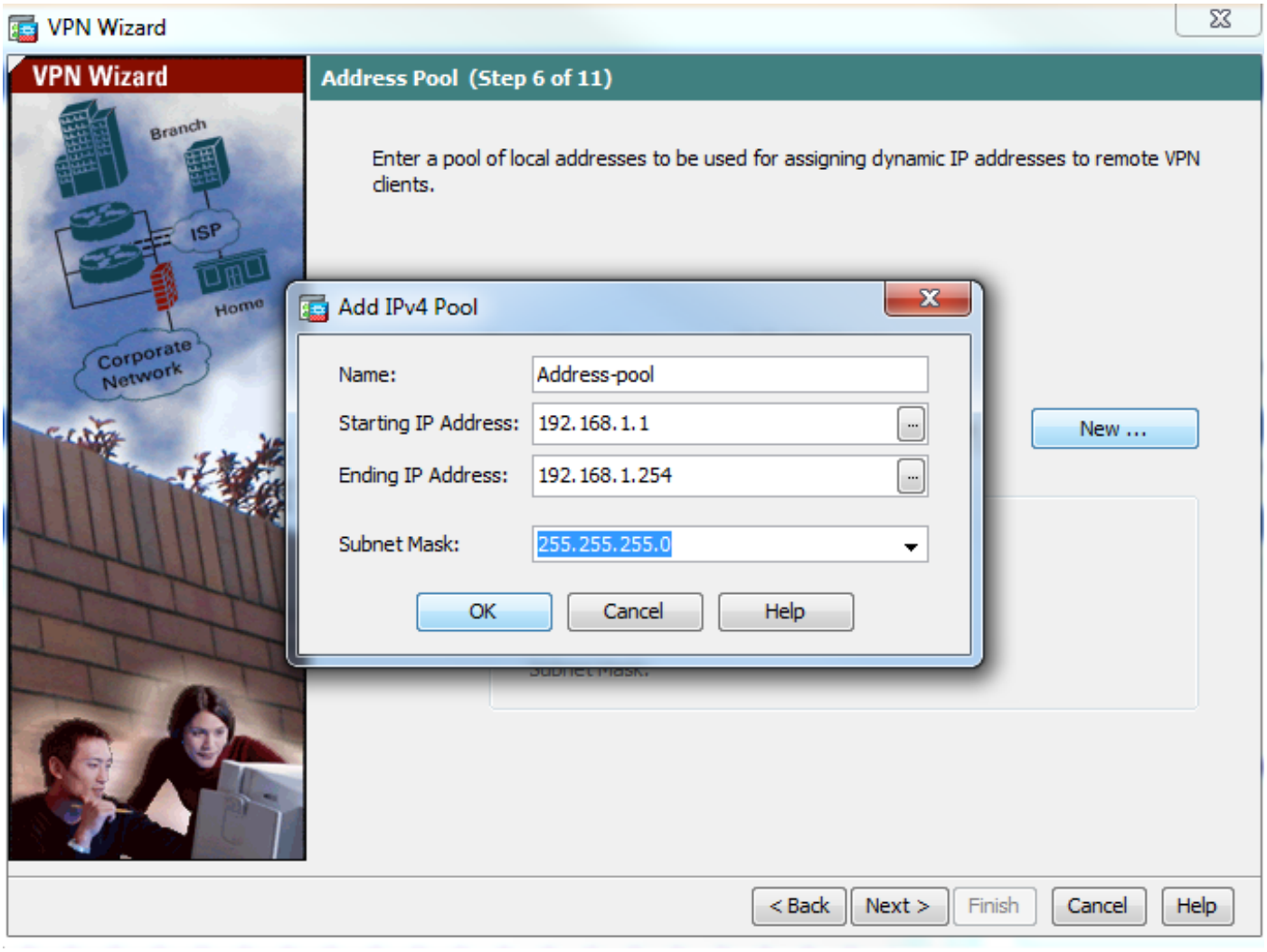


步驟7.從下拉選單中，選擇要用於為客戶端分配IP地址的地址池。若要建立新的地址池，請按一下**New**，如下圖所示。

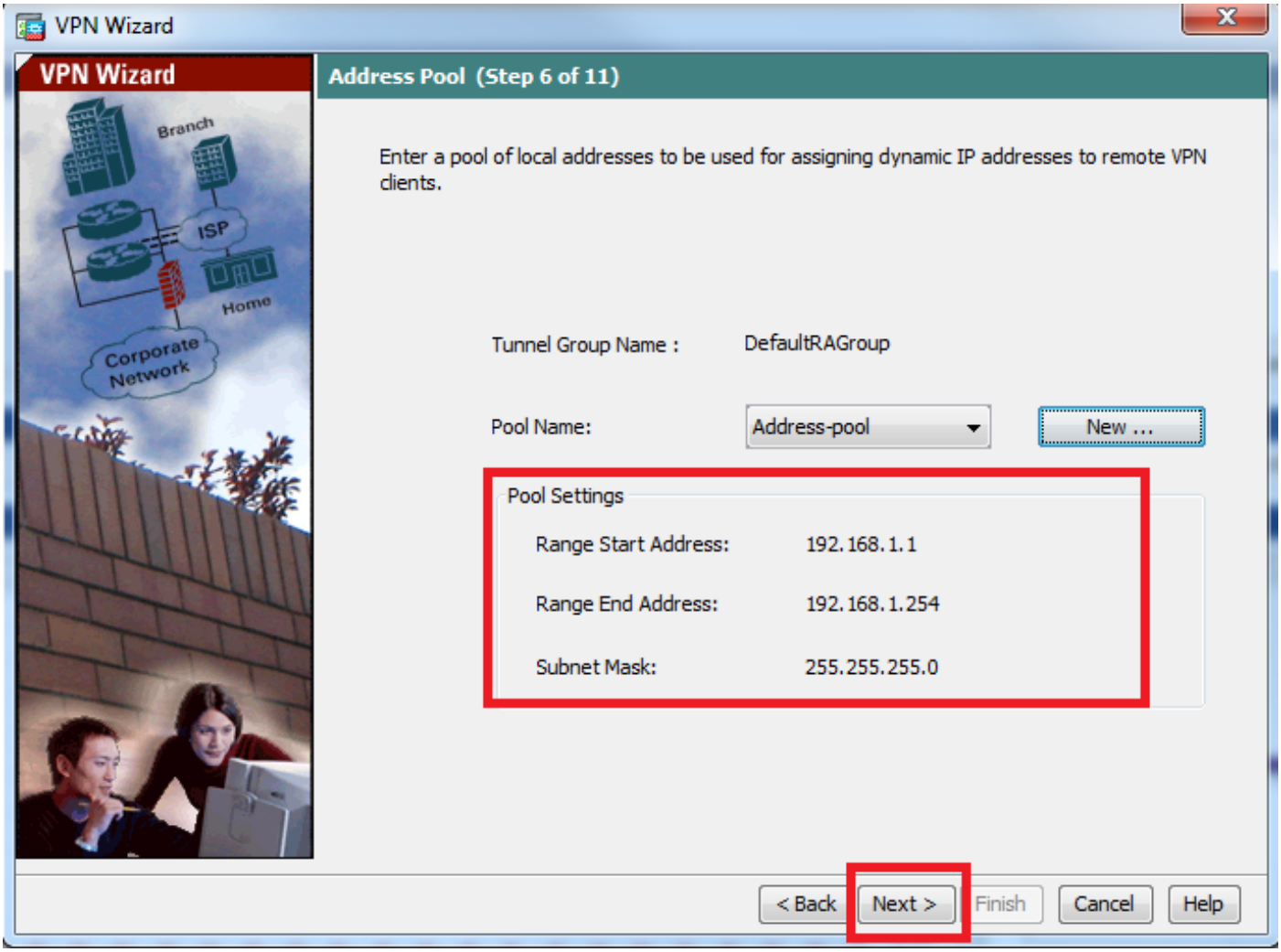


步驟8.出現Add IPv4 Pool對話方塊。

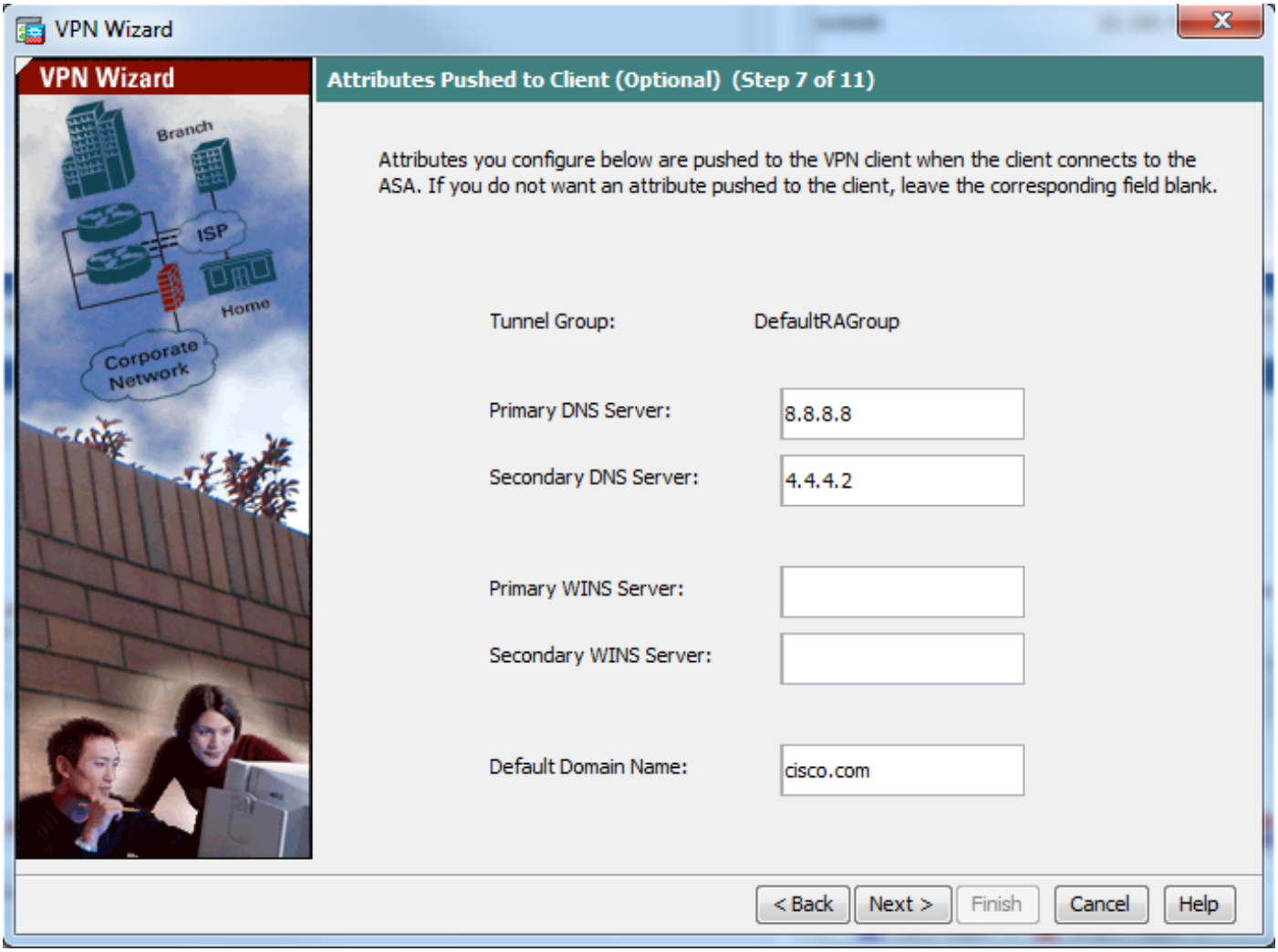
1. 輸入新IP地址池的名稱。
2. 輸入起始和結束IP地址。
3. 輸入子網掩碼並按一下 **確定**.



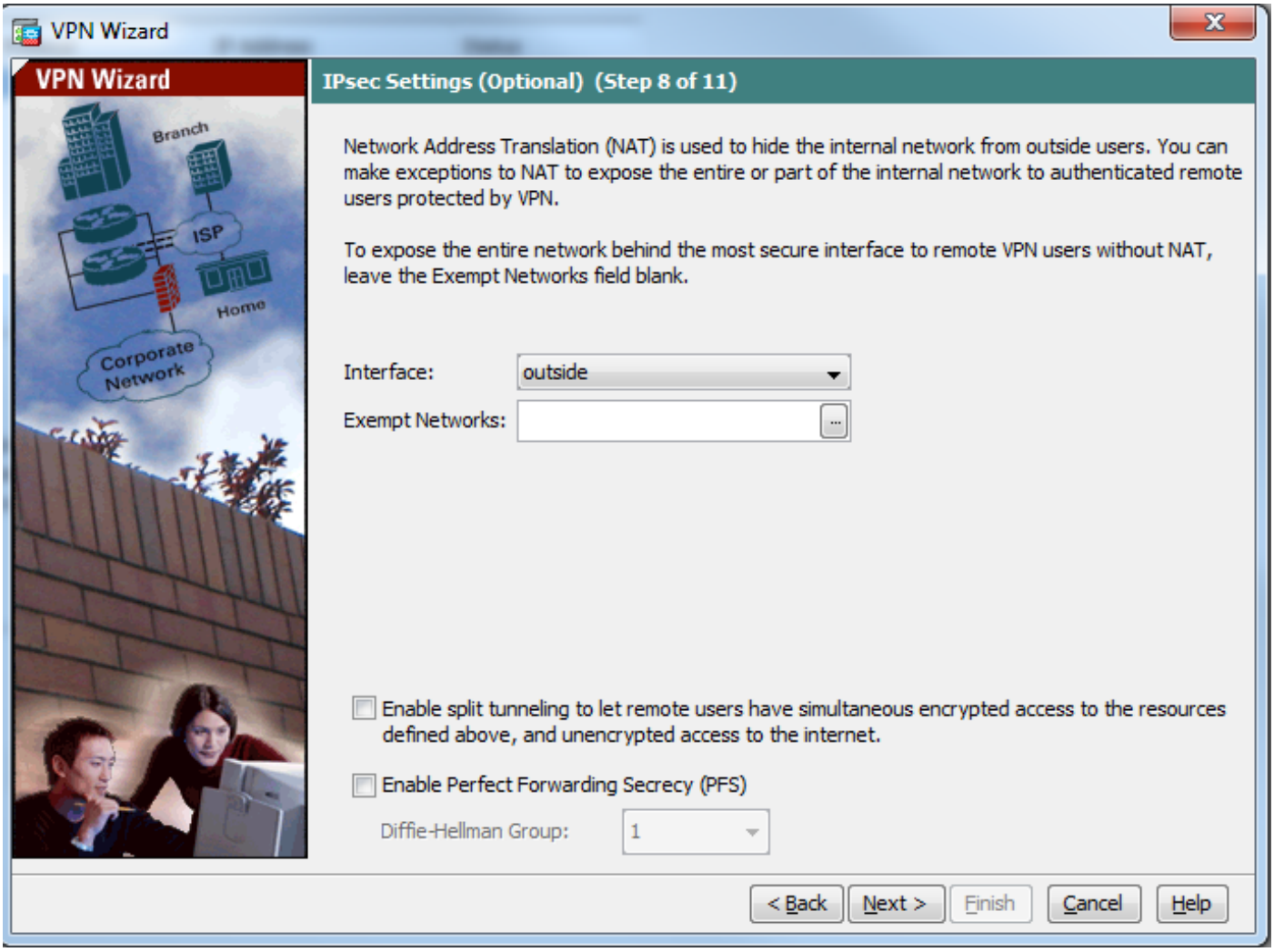
步驟9.驗證池設定並按一下**下一步。**



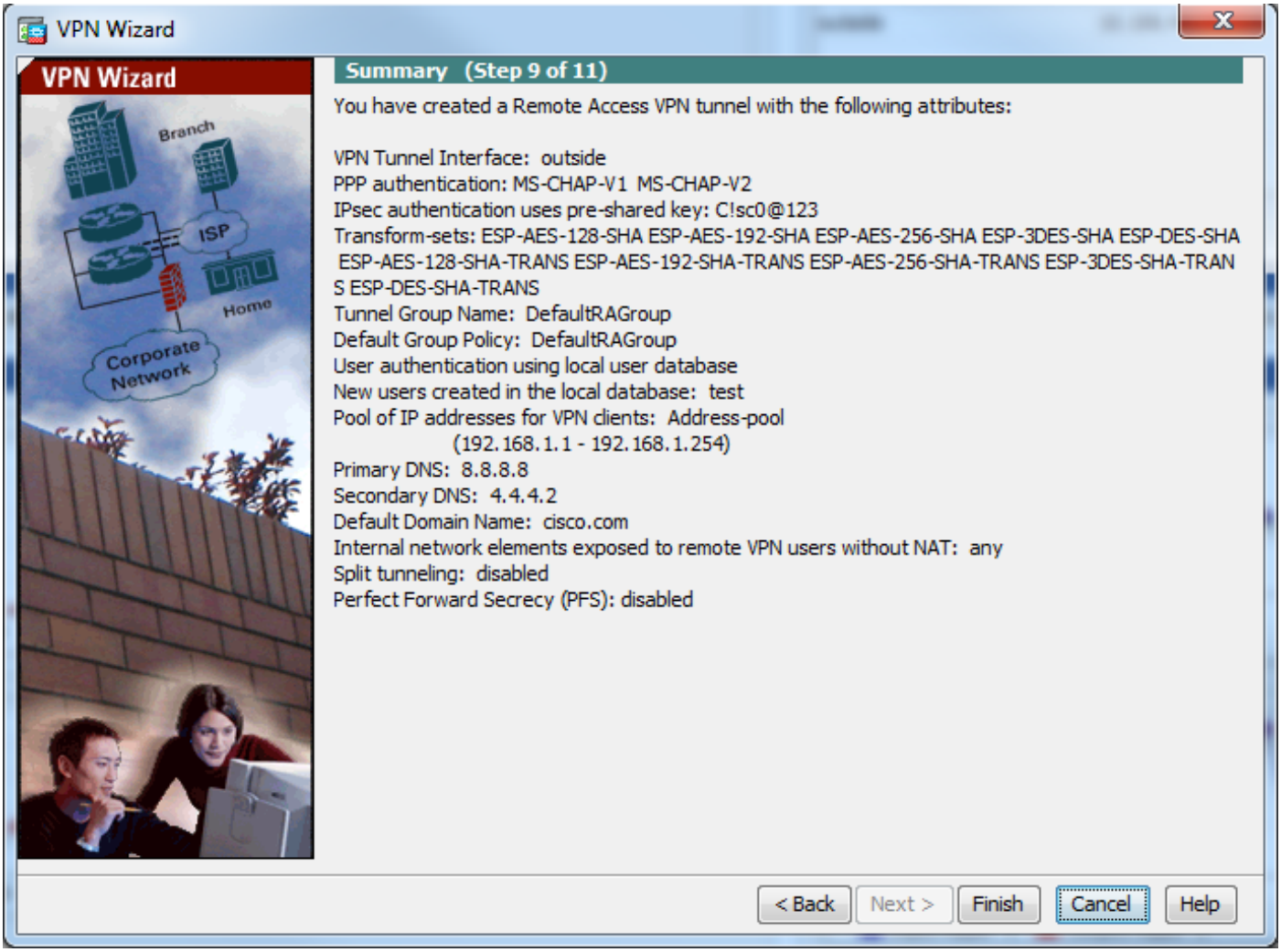
步驟10.配置要推送到客戶端的屬性，或將其留空，然後按一下**下一步**。



步驟11:確保未選中**啟用完全轉發保密(PFS)**框，因為某些客戶端平台不支援此功能。**啟用分割隧道使遠端使用者能夠同時加密訪問上述定義的資源，並且未選中對網際網路盒的未加密訪**問，這意味著啟用完整隧道，其中來自客戶端的所有流量（包括網際網路流量）將通過VPN隧道傳送到ASA。按「**Next**」（下一步）。



步驟12.檢視摘要資訊，然後按一下**完成。**



使用CLI配置ASA

步驟1.配置IKE階段1策略引數。

此策略用於保護對等體之間的控制流量（即，它保護預共用金鑰和階段2協商）

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

步驟2.配置轉換集。

它包含用於保護資料流量的IKE第2階段策略引數。由於Windows L2TP/IPsec客戶端使用IPsec傳輸模式，請將模式設定為傳輸。預設為通道模式

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

步驟3.配置動態對映。

由於Windows客戶端從ISP或本地DHCP伺服器（示例數據機）獲取動態IP地址，因此ASA不知道對等IP地址，這會導致ASA端上的靜態對等配置出現問題。因此，必須接近動態加密配置，其中不必定義所有引數，而丟失的引數稍後動態獲知，這是來自客戶端的IPSec協商的結果。

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-
SHA
```

步驟4.將動態對映繫結到靜態加密對映，應用加密對映並在外部介面上啟用IKEv1

無法在介面上應用動態加密對映，因此將其繫結到靜態加密對映。動態加密集應該是加密對映集中優先順序最低的加密對映（即，它們應該具有最高的序列號），以便ASA首先評估其他加密對映。僅當其他（靜態）對映條目不匹配時，才會檢查動態加密對映集。

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

步驟5.建立IP地址池

建立一個地址池，從該地址池將IP地址動態分配給遠端VPN客戶端。忽略此步驟以使用ASA上的現有池。

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

步驟6.配置組策略

將組策略標識為內部，這意味著從本地資料庫中提取屬性。

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

> **附註**：可以使用預設組策略(DfltGrpPolicy)或使用者定義的組策略配置L2TP/IPsec連線。無論哪種情況，必須將組策略配置為使用L2TP/IPsec隧道協定。在預設組策略的VPN協定屬性上配置l2tp-ipsec，如果未在預設組策略上配置vpn協定屬性，則該預設組策略將繼承給使用者定義的組策略。

配置vpn隧道協定（在本例中為l2tp-ipsec）、域名、DNS和WINS伺服器IP地址以及新使用者帳戶等屬性

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

除了使用AAA之外，還可在裝置上配置使用者名稱和密碼。如果使用者是使用Microsoft CHAP版本1或版本2的L2TP客戶端，並且ASA配置為根據本地資料庫進行身份驗證，則必須包含mschap關鍵字。例如，使用者名稱<username> password <password> mschap。

```
ciscoasa(config-group-policy)# username test password test mschap
```

步驟7.配置隧道組

使用tunnel-group命令建立隧道組，並指定用於向客戶端分配IP地址的本地地址池名稱。如果身份驗證方法是預共用金鑰，則隧道組名稱必須是DefaultRAGroup，因為客戶端上沒有任何選項來指定隧道組，因此它僅停留在預設隧道組。使用default-group-policy命令將組策略繫結到隧道組

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

附註：如果執行基於預共用金鑰的身份驗證，則必須配置預設連線配置檔案（隧道組）DefaultRAGroup。如果執行基於證書的身份驗證，可以根據證書識別符號選擇使用者定義的連線配置檔案

使用**tunnel-group ipsec-attributes**命令進入ipsec-attribute配置模式以設定預共用金鑰。

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)#  ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

在隧道組ppp-attributes模式下使用**authentication type**命令配置PPP身份驗證協定。禁用CHAP，如果AAA伺服器配置為本地資料庫，則預設啟用該CHAP，因為不支援該CHAP。

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

步驟8.配置NAT免除

配置NAT-Exemption，以便客戶端可以訪問連線到內部介面的內部資源（在本示例中，內部資源連線到內部介面）。

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
```

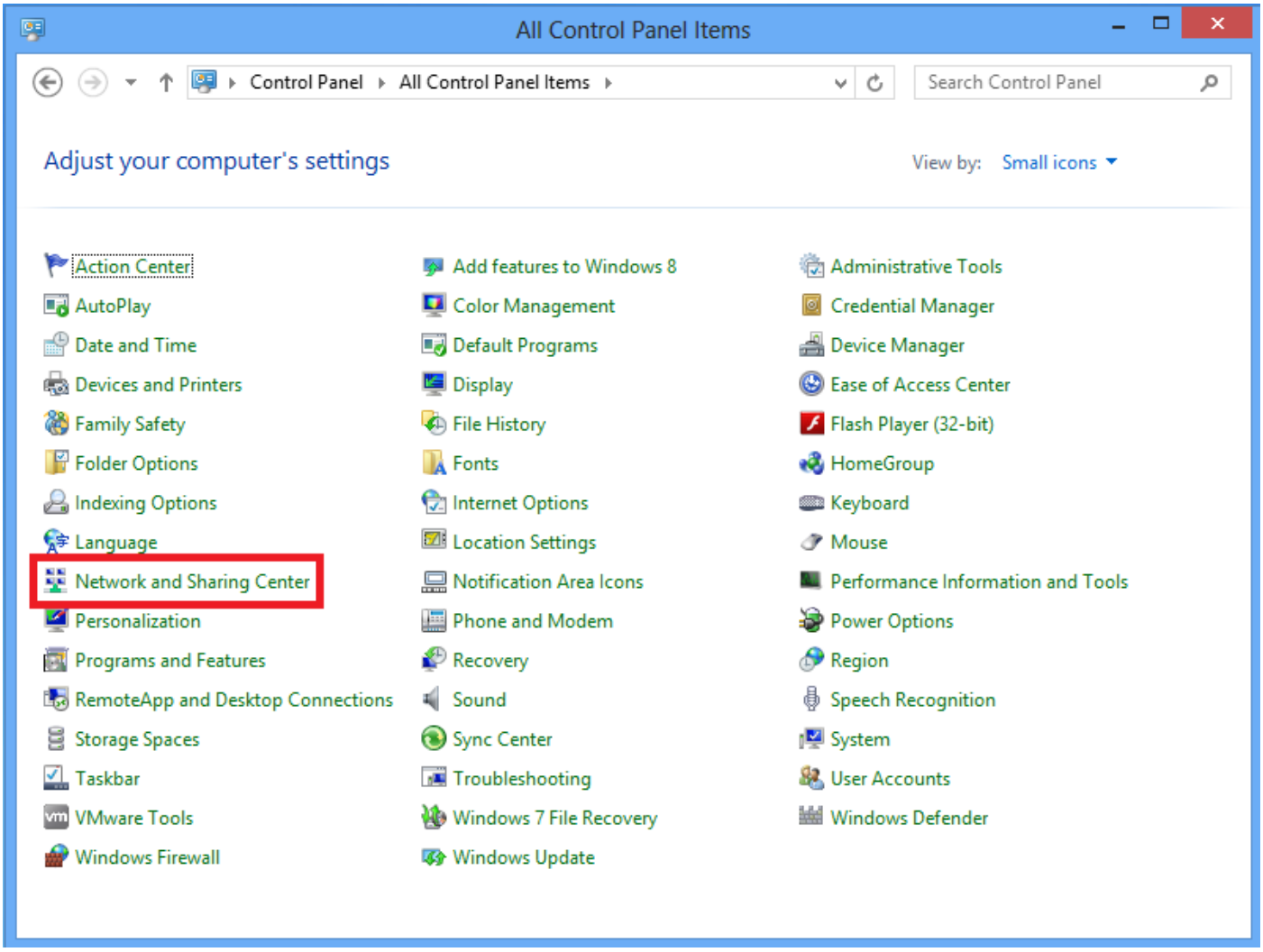
完成示例配置

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit

crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
```

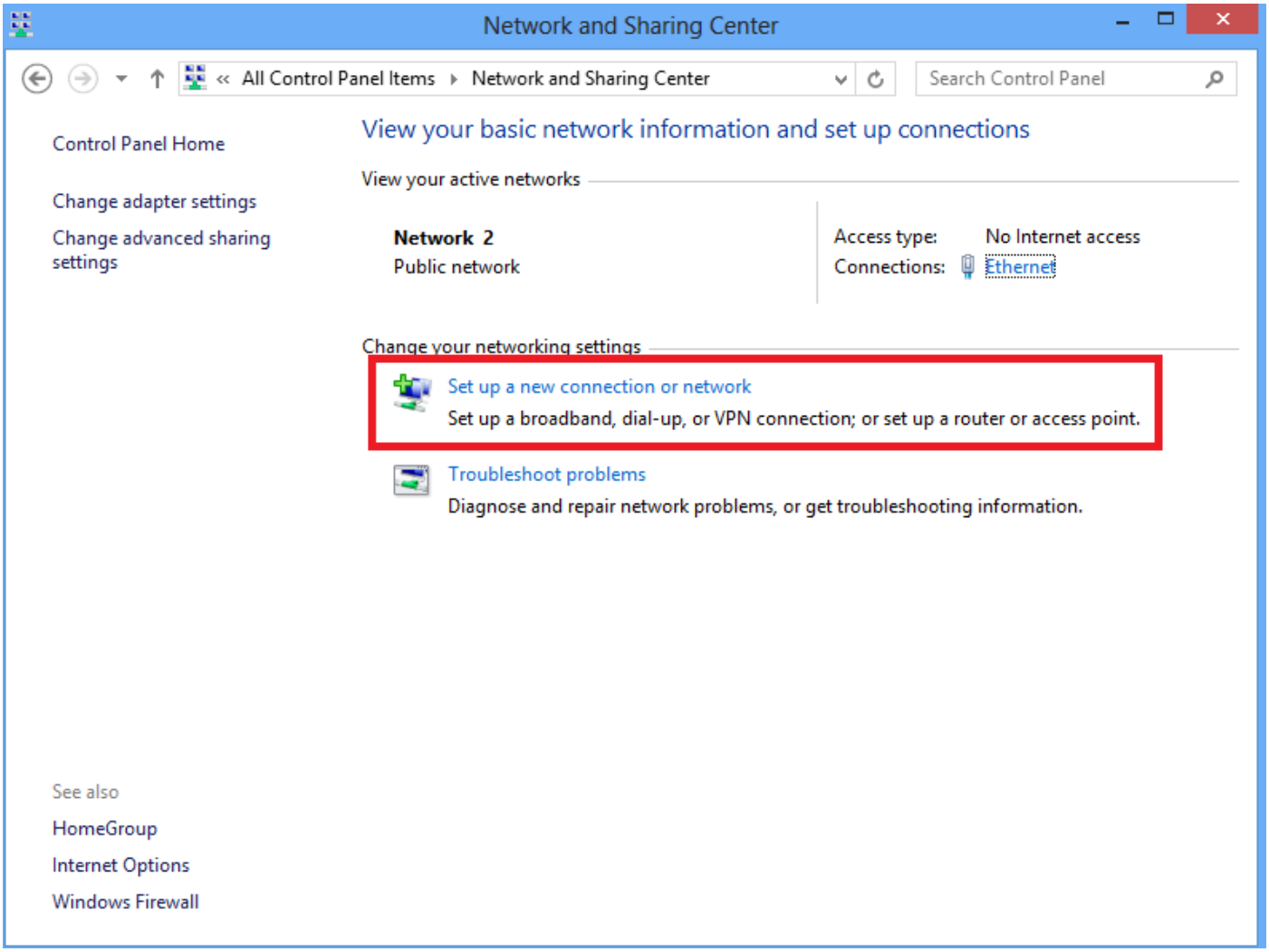
```
default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

Windows 8 L2TP/IPsec客戶端配置

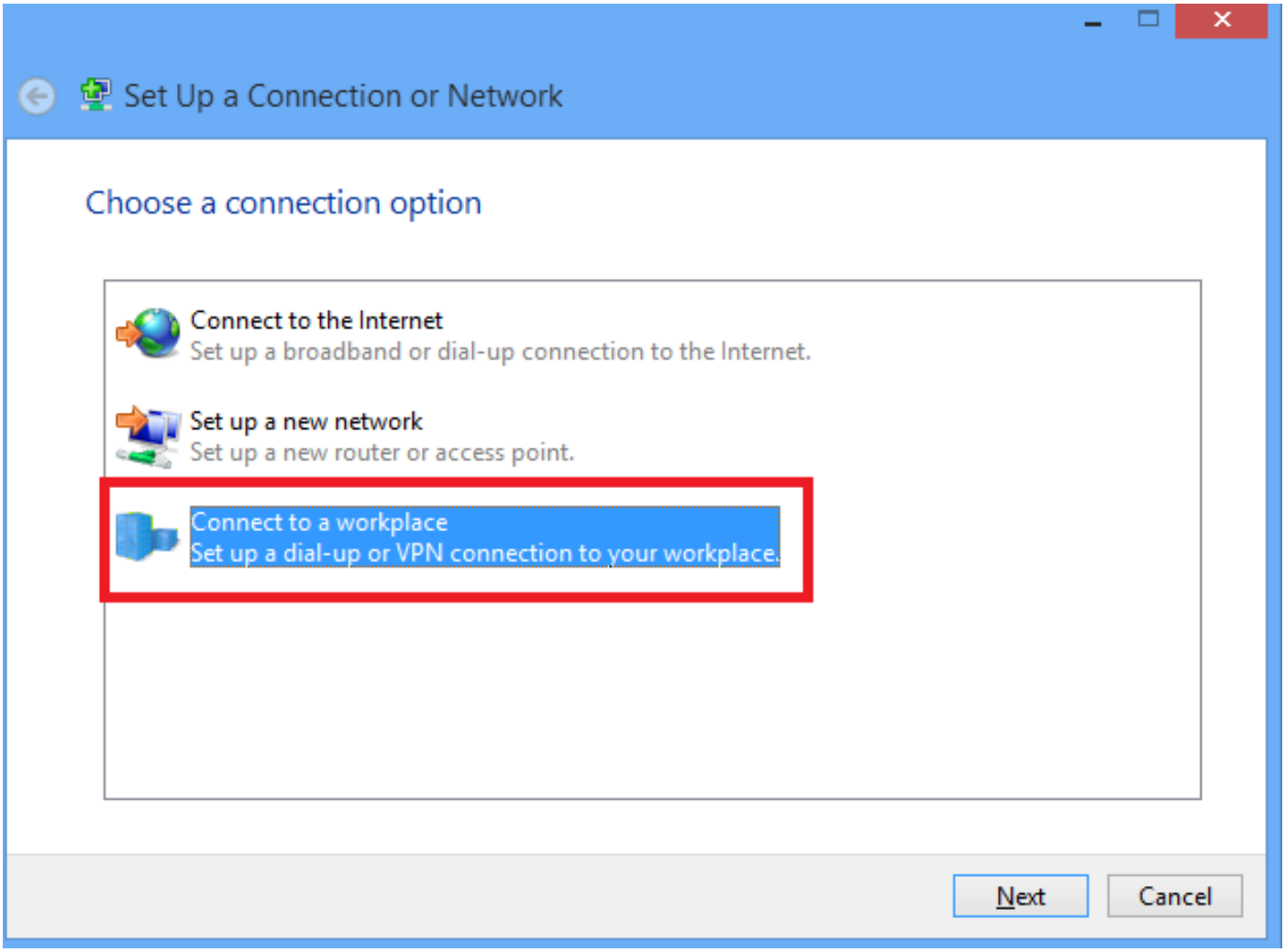
1.開啟「控制面板」並選擇「網路和共用中心」。



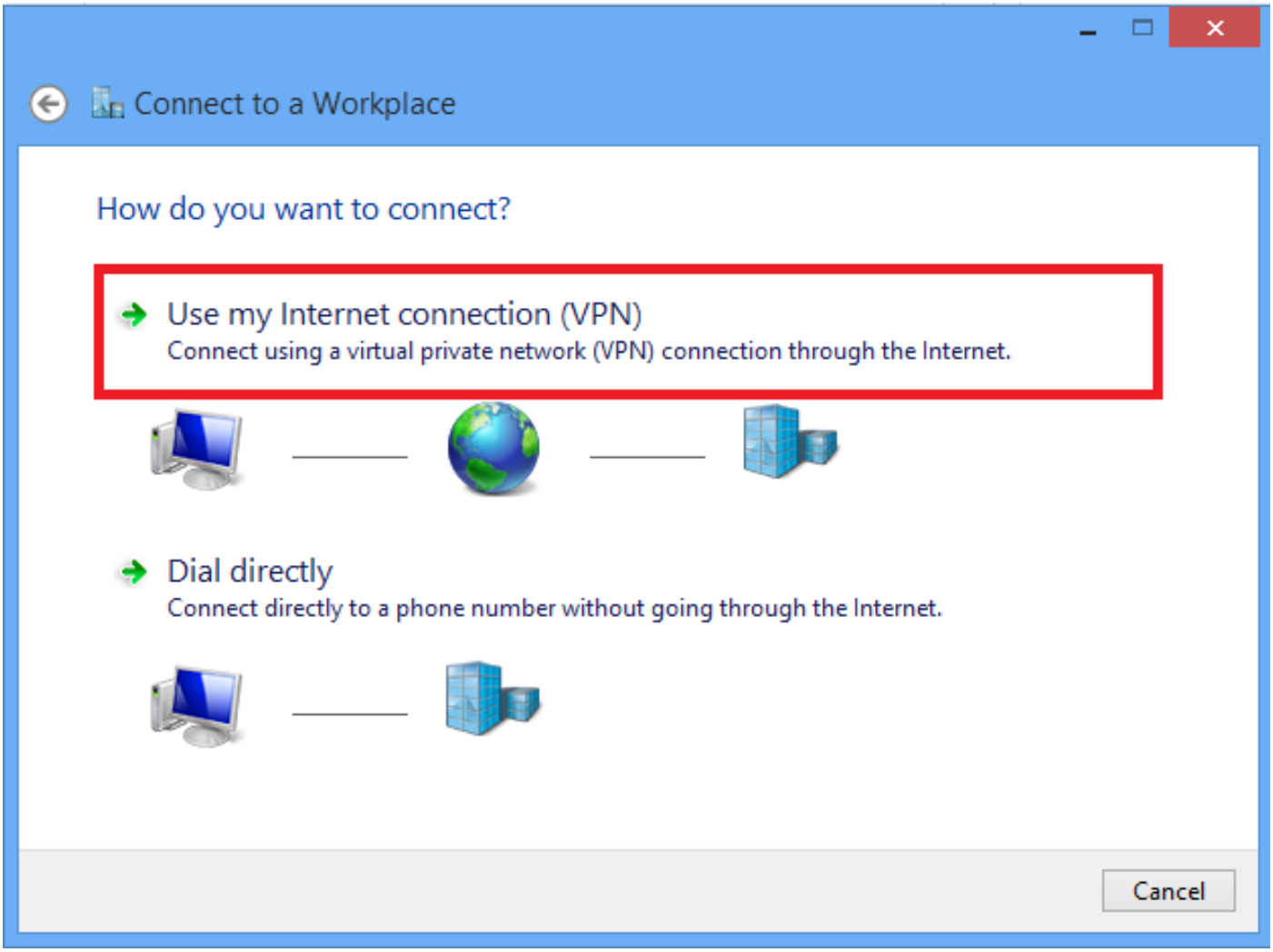
2.選擇**設定新連線或網路**選項。



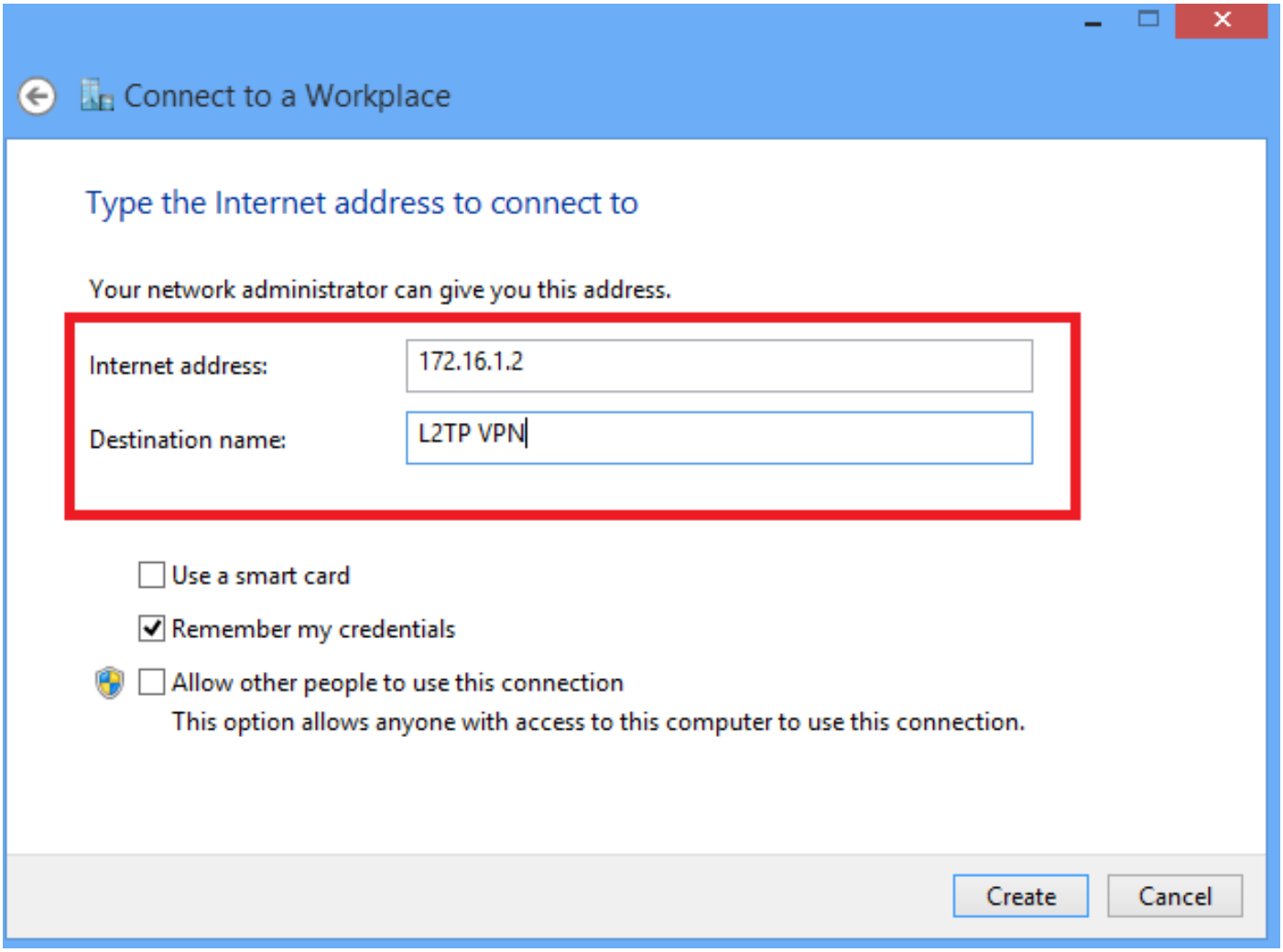
3.選擇「連**接到工作場所」選**項並按一下「下一**步」。**



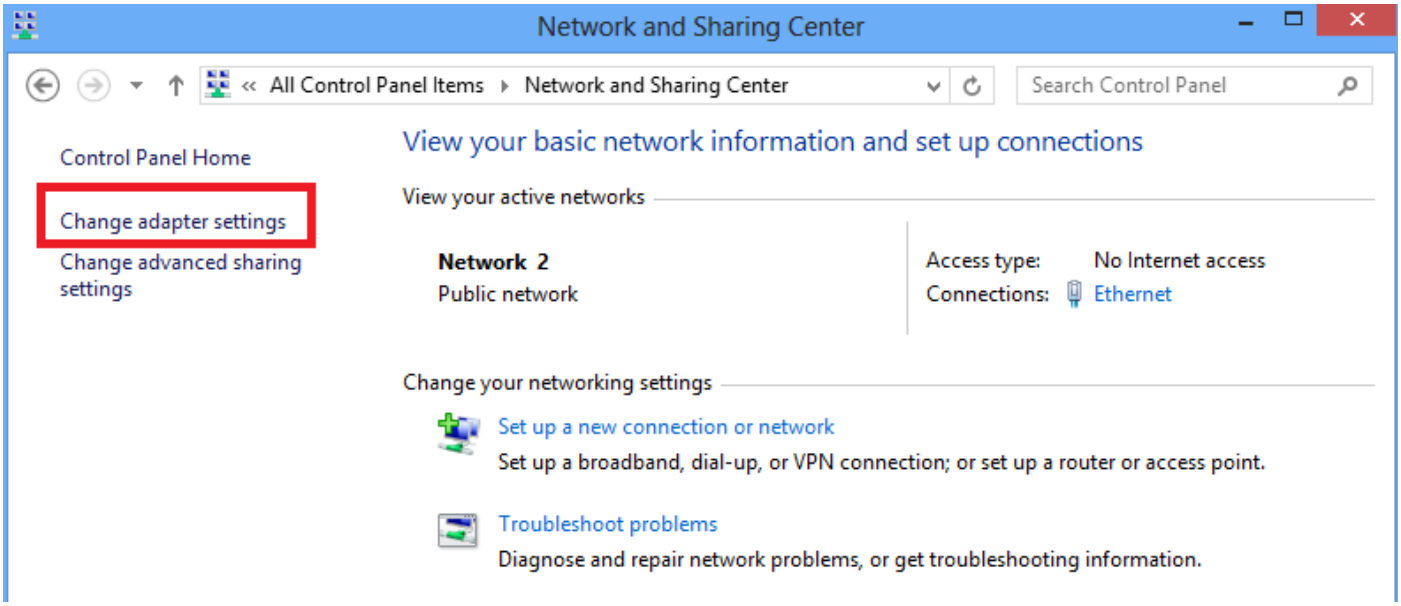
4.按一下**Use my Internet connection(VPN)選項**。



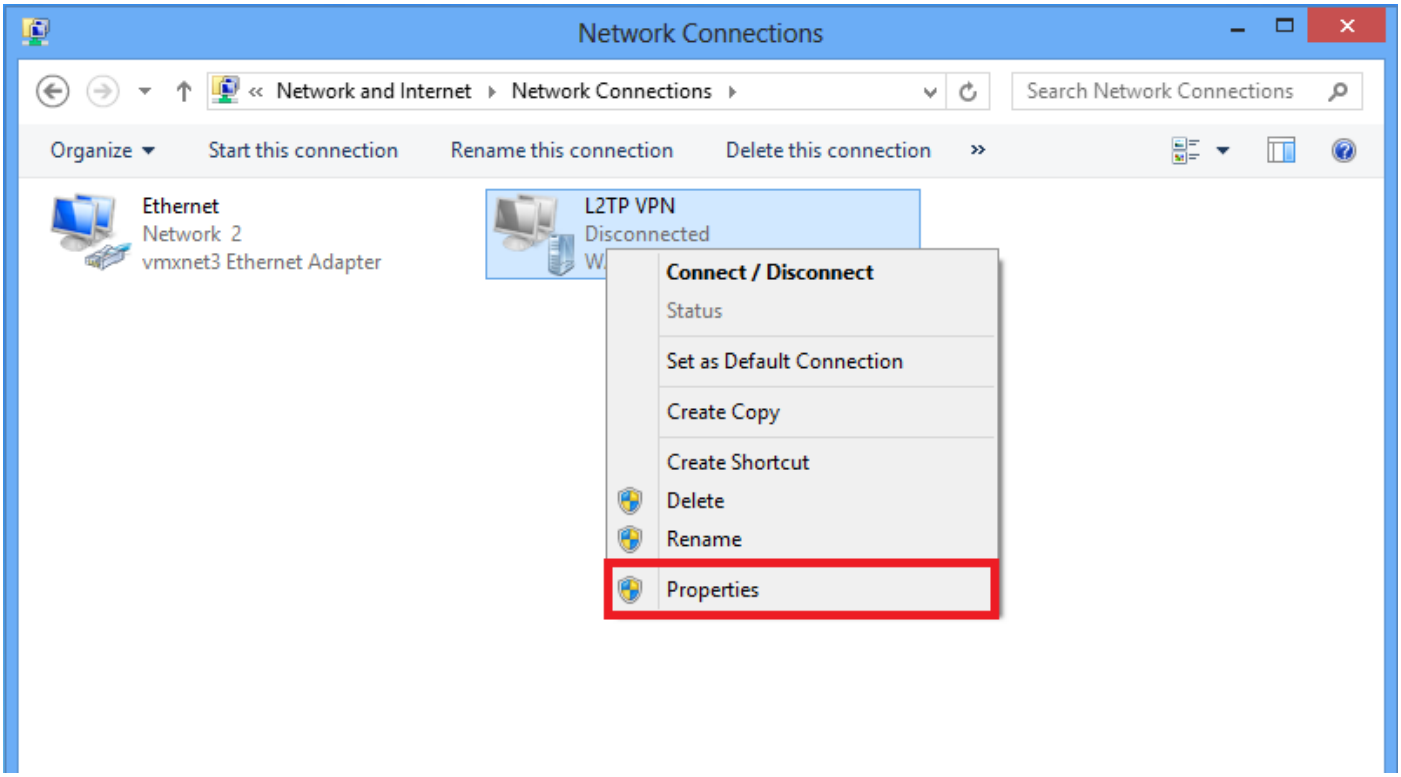
5.輸入ASA的WAN介面或FQDN的IP地址以及VPN介面卡的任何本地名稱，然後按一下**Create**。



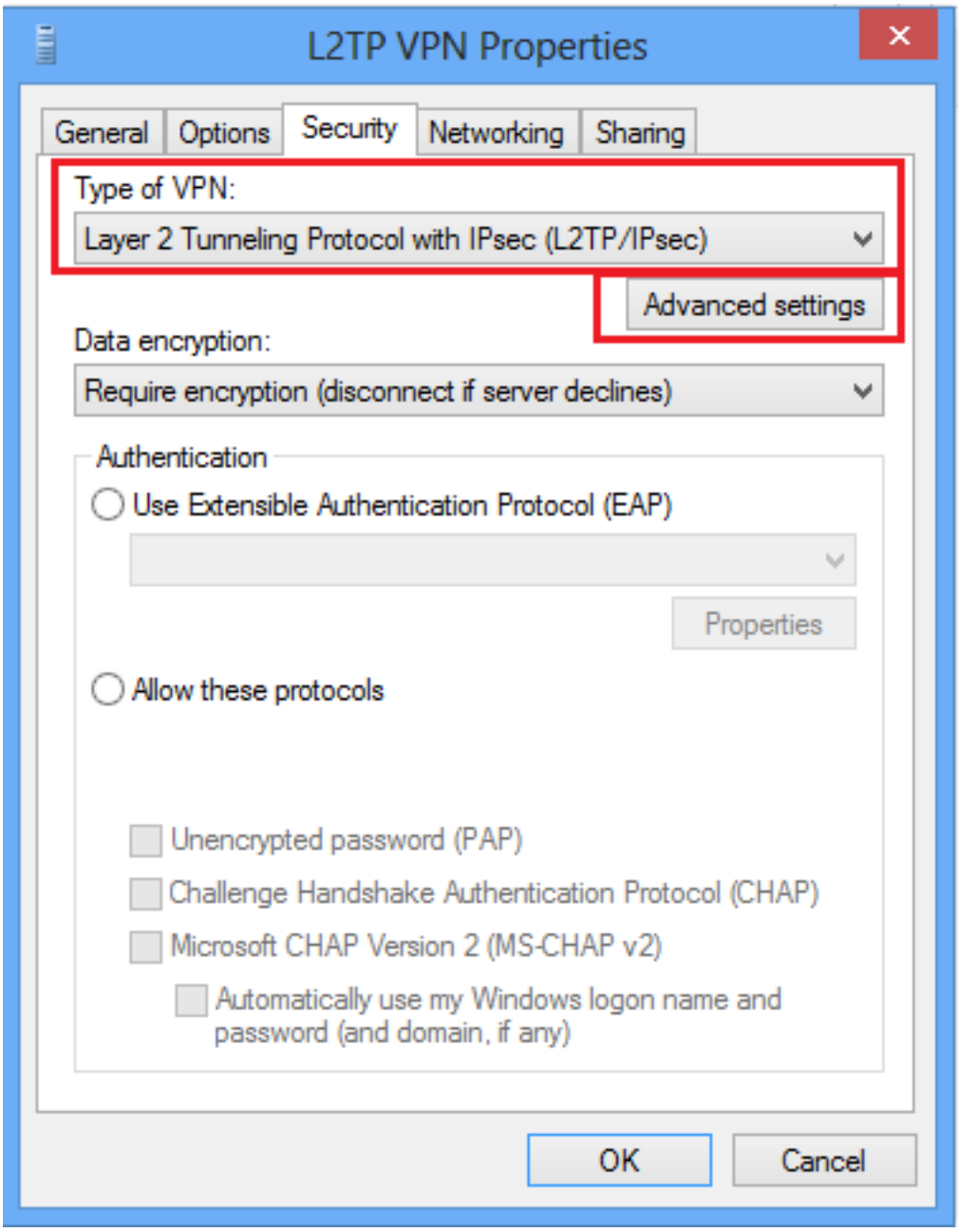
6.在「網路和共用中心」上，選擇視窗左側窗格中的**更改介面卡設定**選項。



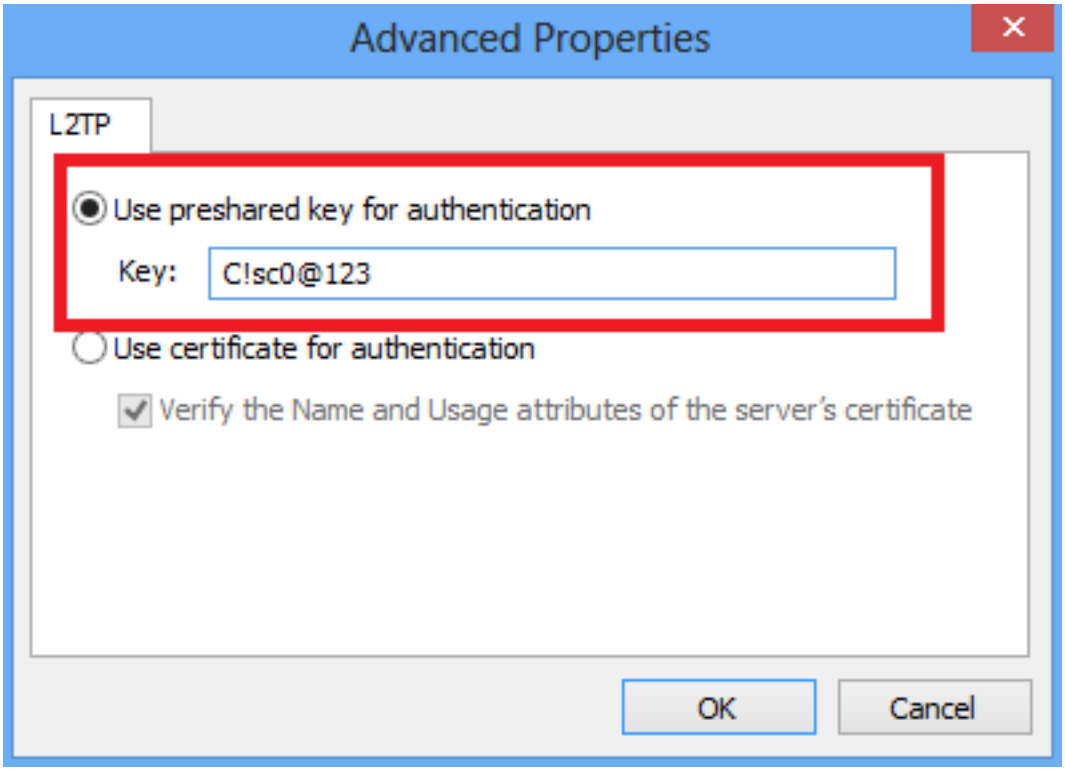
7.按一下右鍵最近為L2TP VPN建立的介面卡，然後選擇**屬性。**



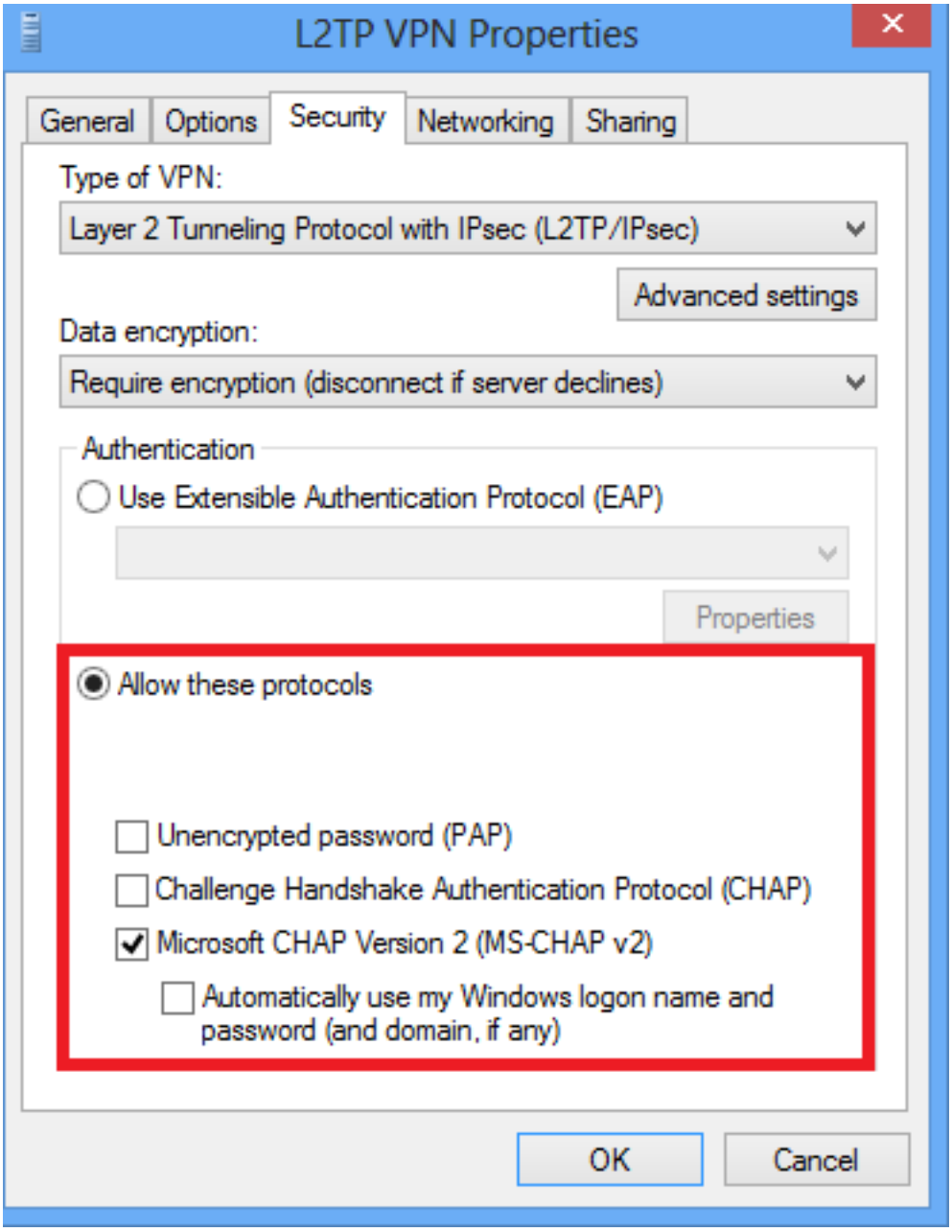
8.導航到**Security**頁籤，選擇Type of VPN as **Layer 2 Tunneling Protocol with IPsec(L2TP/IPsec)**，然後按一下**Advanced settings**。



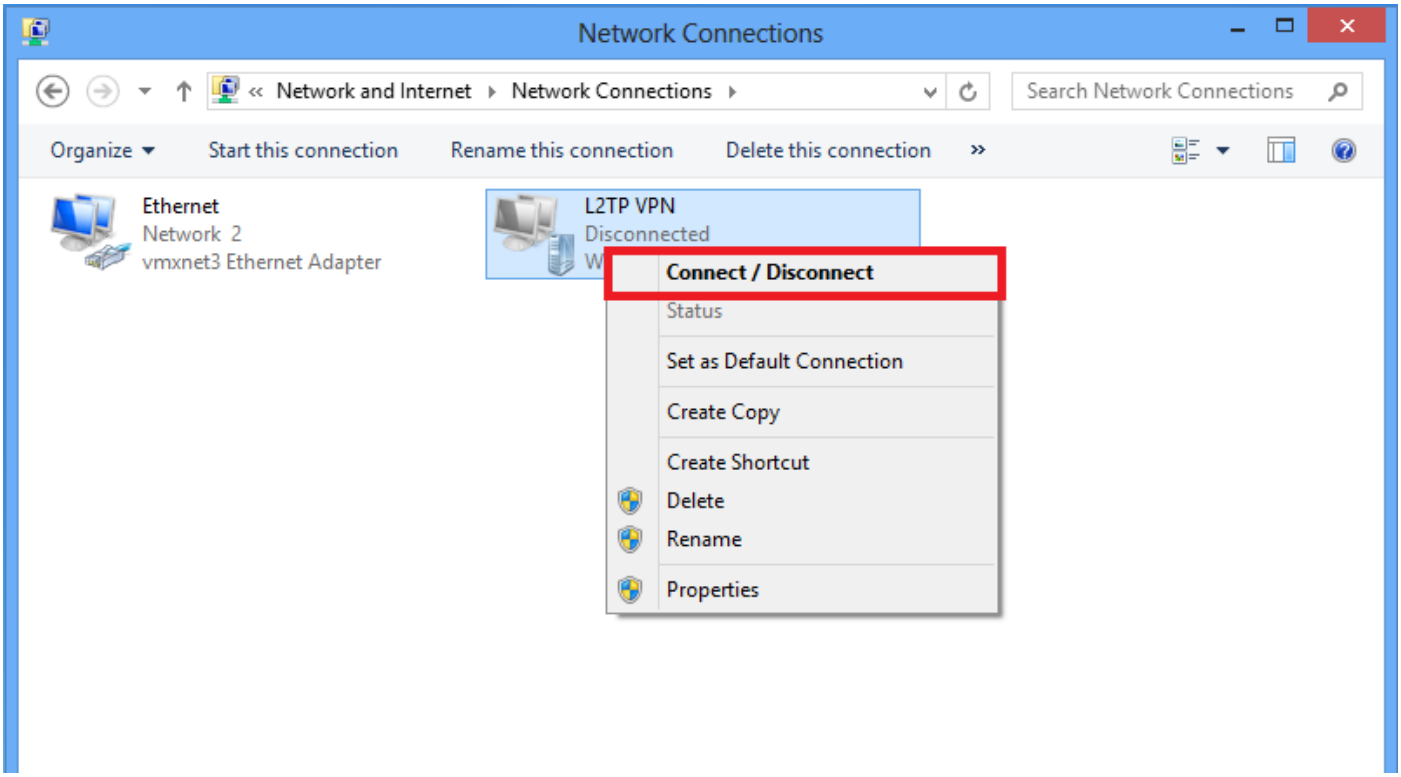
9.輸入與隧道組**DefaultRAGroup**中提到的相同預共用金鑰，然後按一下**OK**。在本示例中，C!sc0@123用作預共用金鑰。



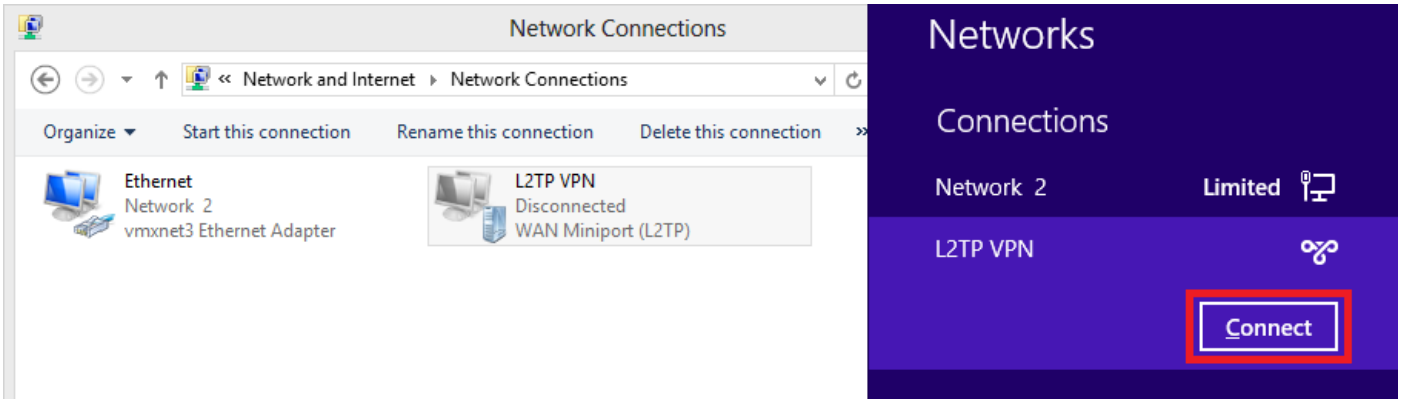
10.將身份驗證方法選擇為允許這些協定，並確保僅選中「**Microsoft CHAP Version 2(MS-CHAP v2)**」覈取方塊，然後按一下**確定**。



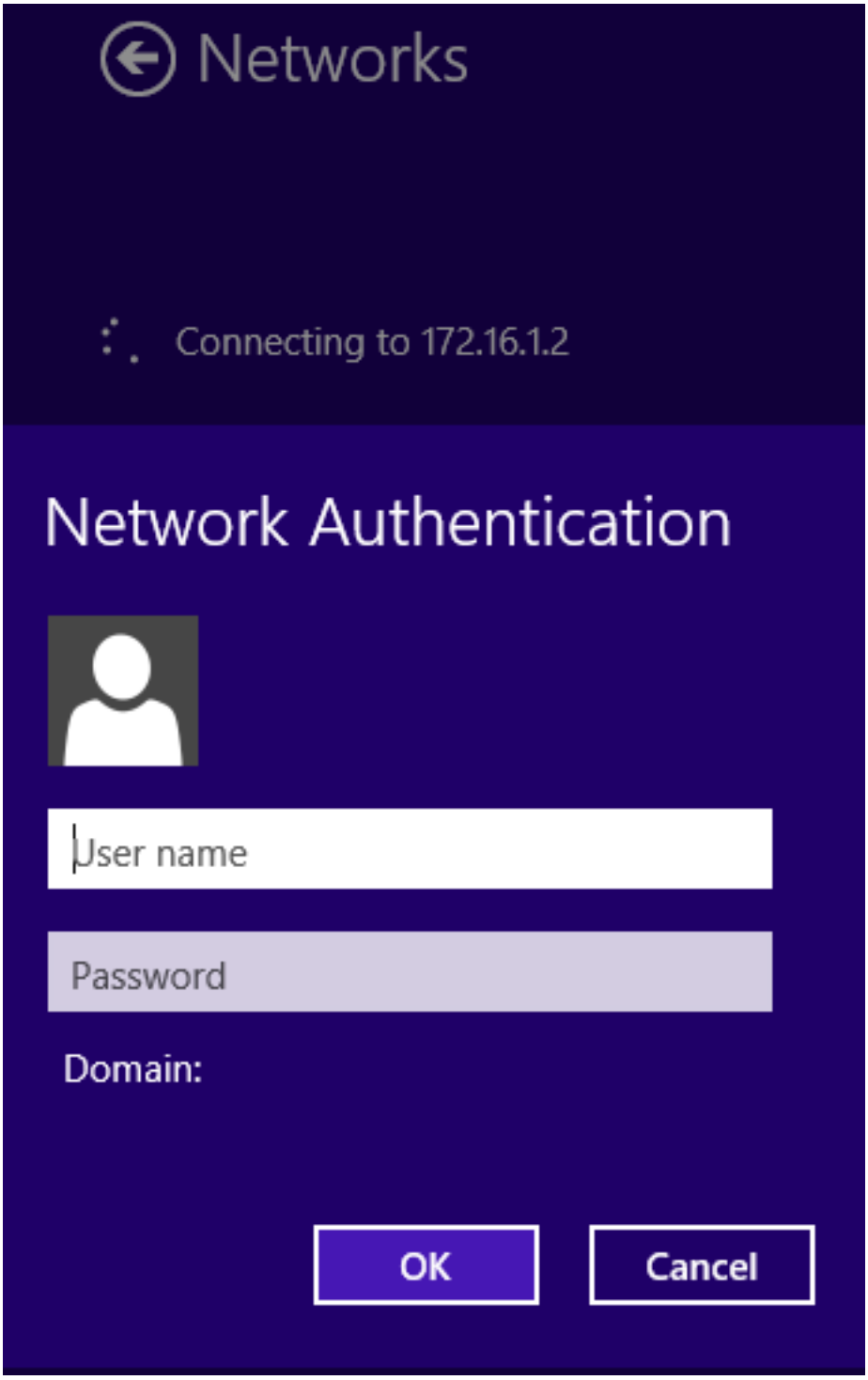
11.在「網路連線」下，按一下右鍵L2TP VPN介面卡，然後選擇**「連線/斷開」。**



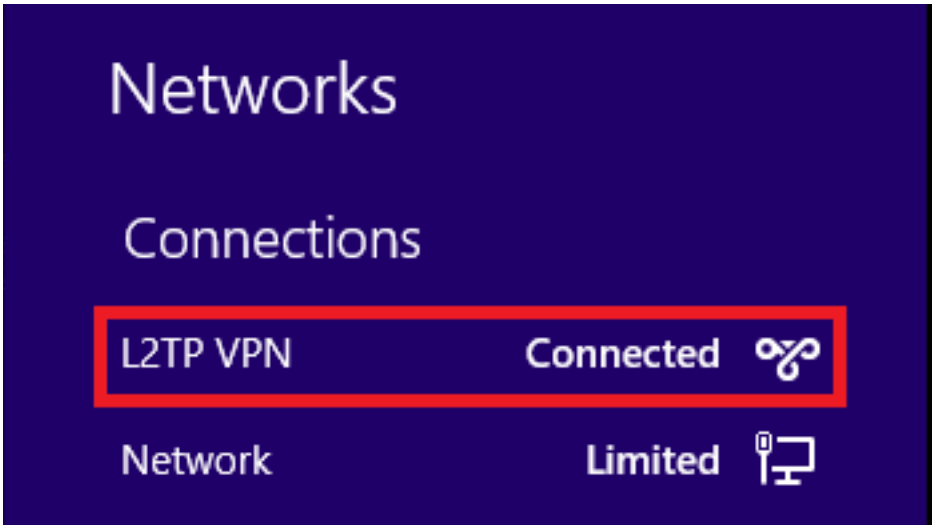
12.將彈出網路圖示，然後按一下**Connect** on L2TP VPN connection。



13.輸入使用者憑證，然後按一下**確定**。



如果兩端都匹配了所需的引數，則將建立L2TP/IPsec連線。



分割隧道配置

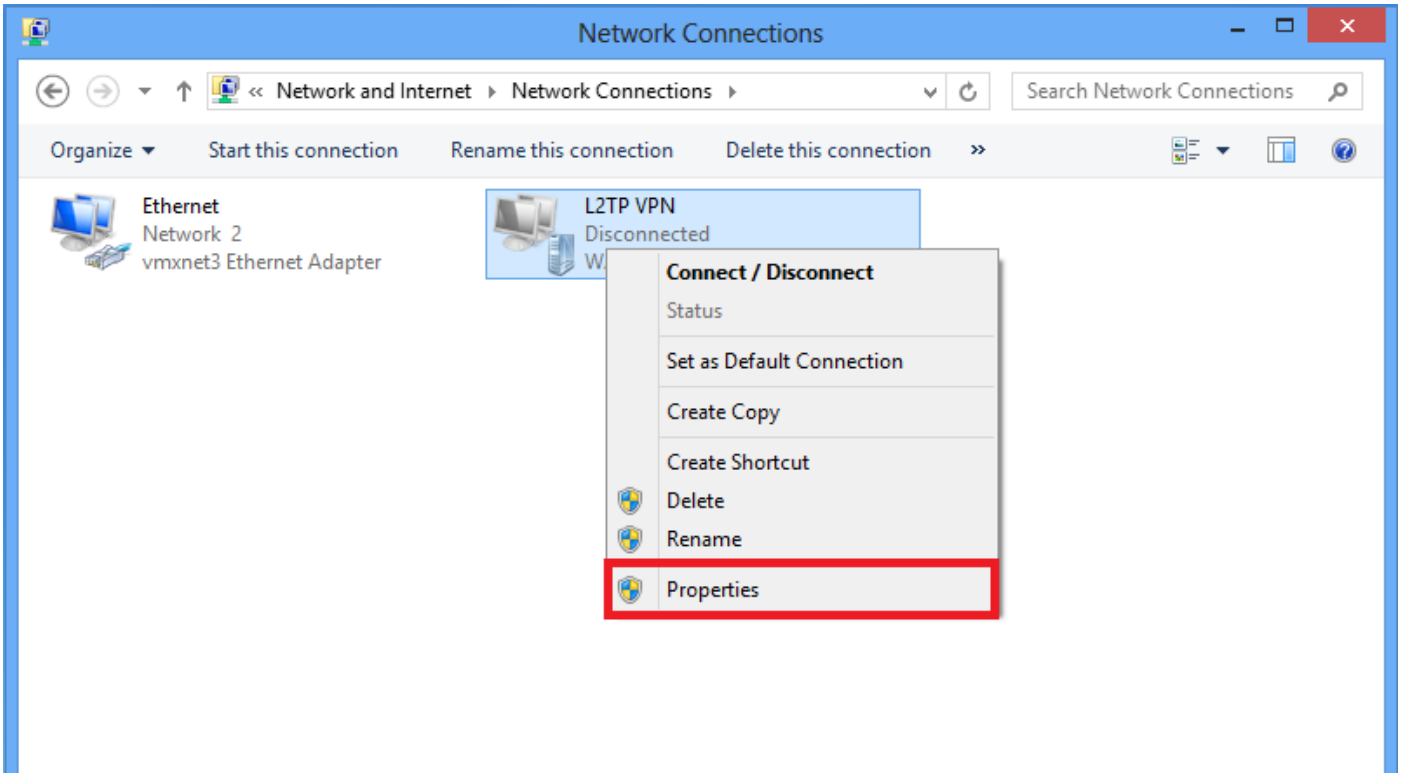
分割隧道是一種功能，可用於定義必須加密的子網或主機的流量。其中涉及與此功能相關聯的存取控制清單(ACL)的組態。此ACL上定義的子網或主機的流量通過隧道從客戶端進行加密，這些子網的路由安裝在PC路由表中。ASA會攔截來自客戶端的DHCPINFORM消息，並使用子網掩碼、域名和無類靜態路由做出響應。

ASA上的配置

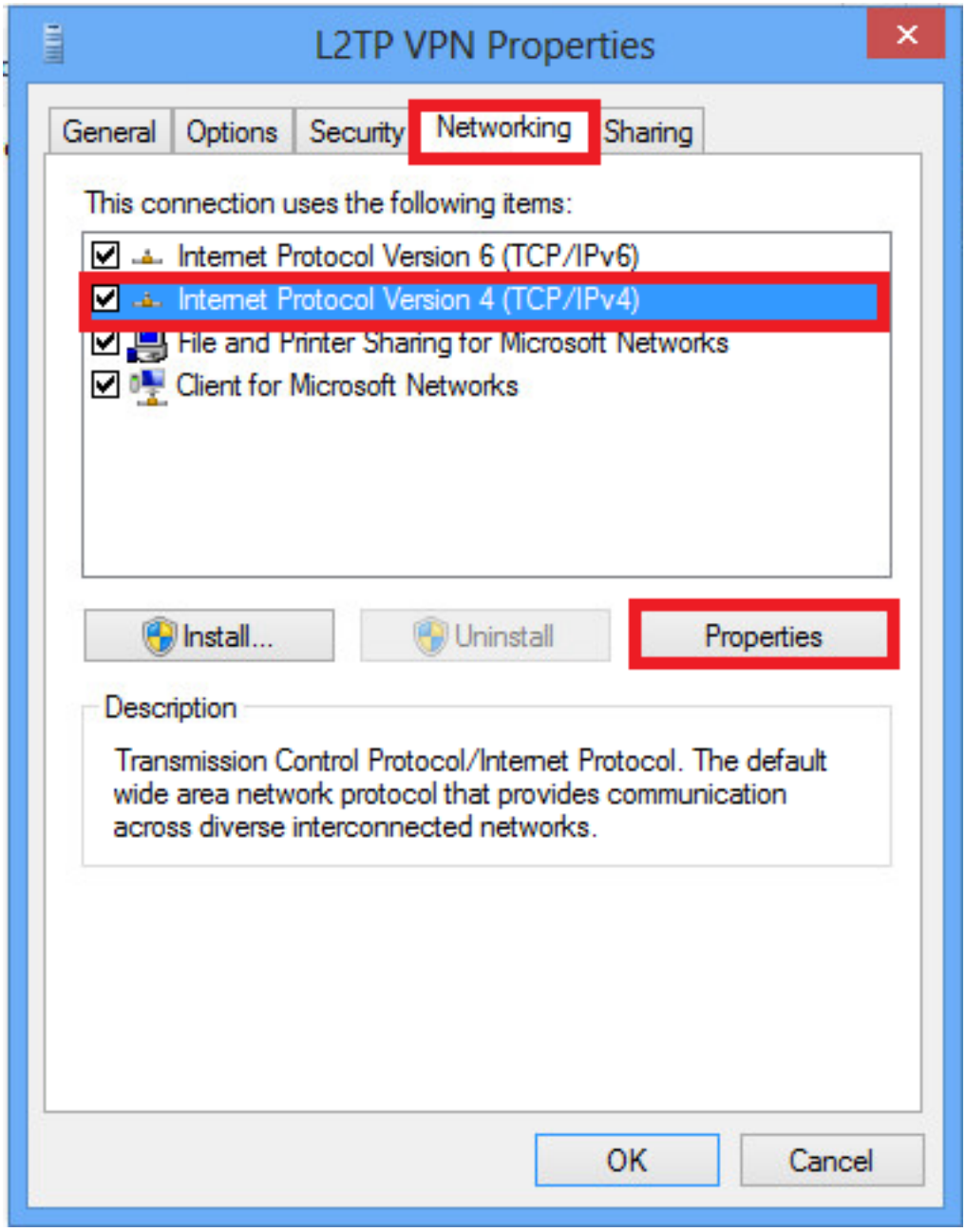
```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0

ciscoasa(config)# group-policy DefaultRAGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

L2TP/IPsec客戶端上的配置

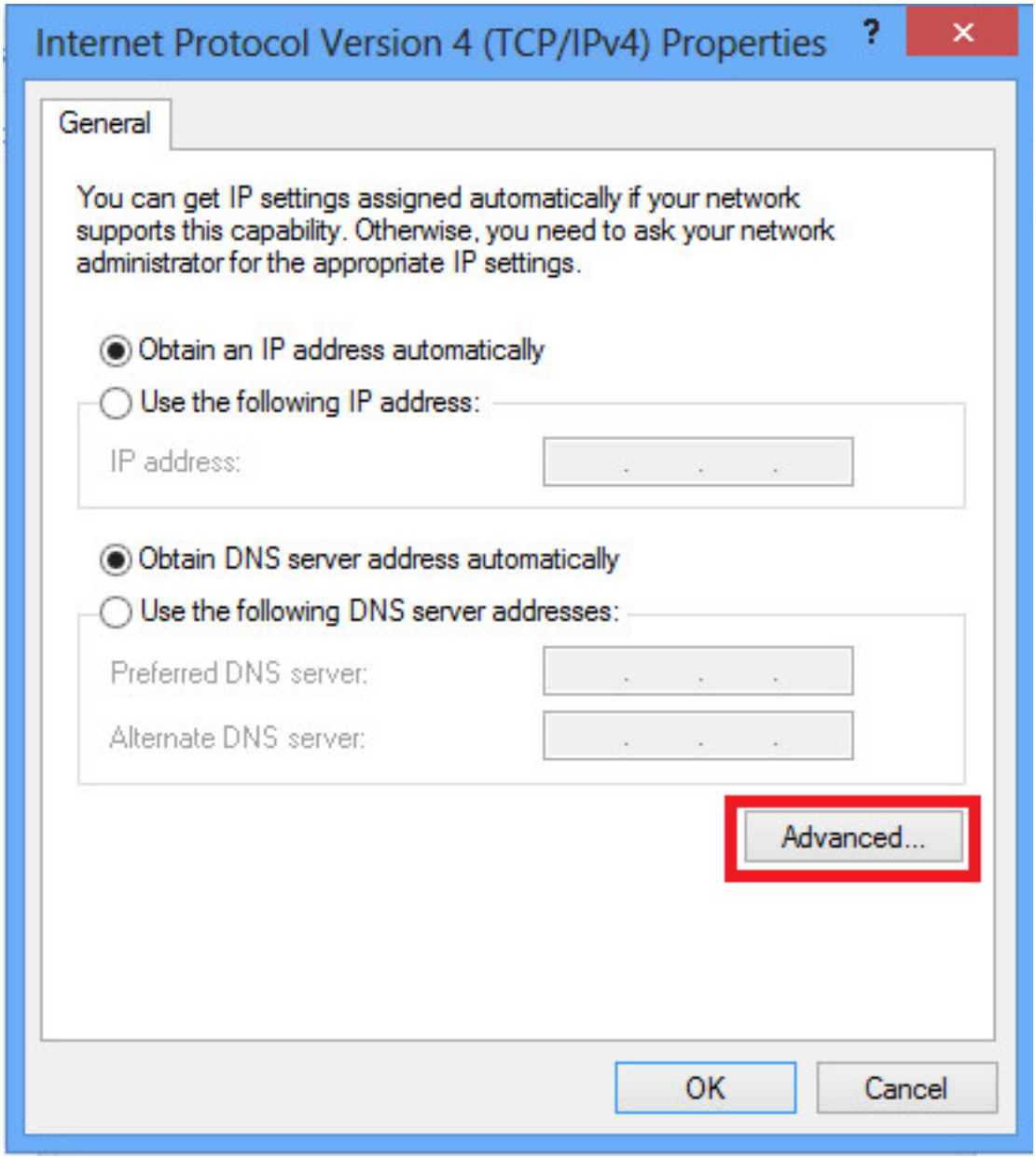
1.按一下右鍵L2TP VPN介面卡，然後選擇**屬性。**



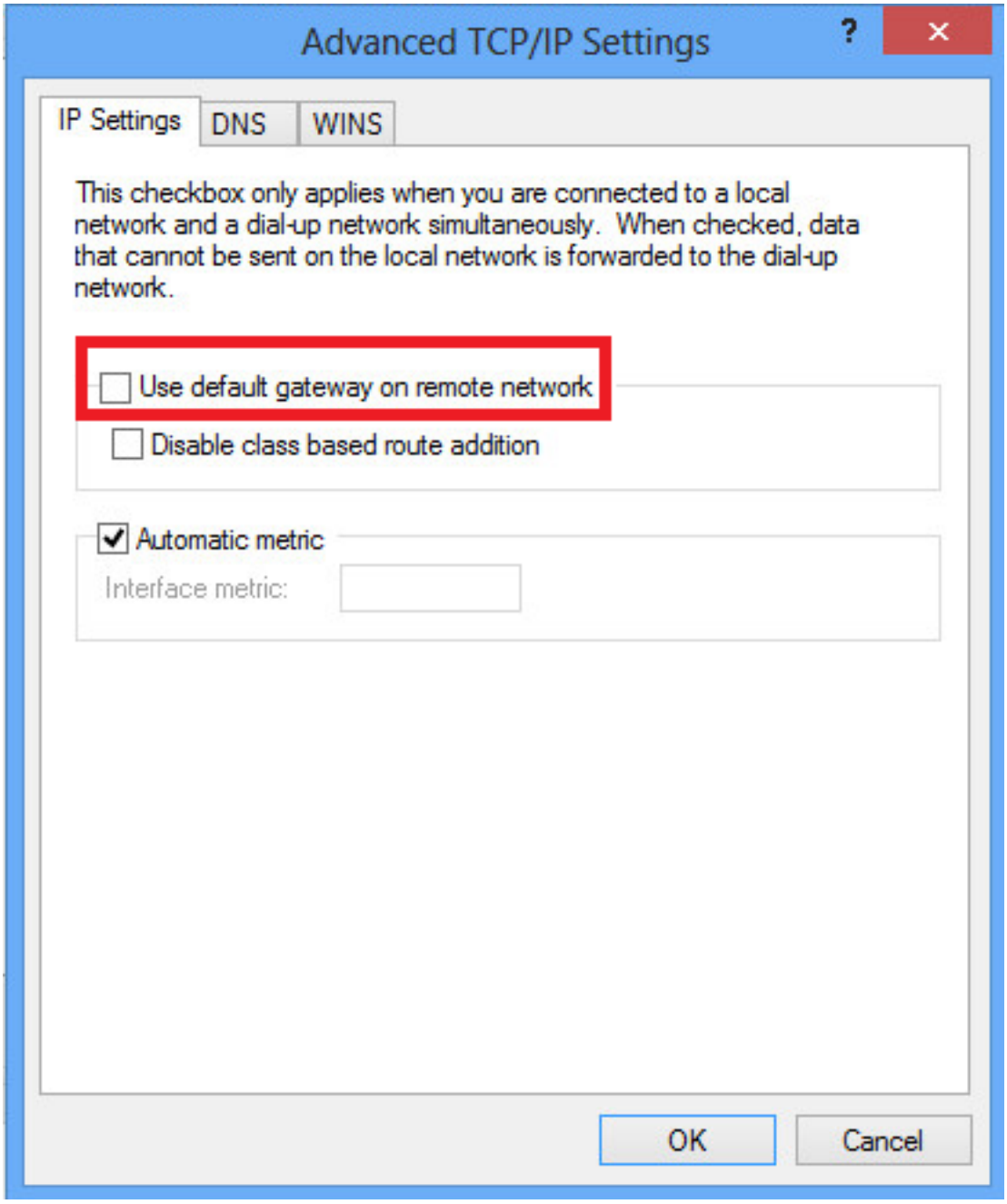
2.導航到「網路」頁籤，選擇「Internet協定版本4(TCP/IPv4)」 ，然後按一下「**屬性**」。



3.按一下**Advanced**選項。



4.取消選中**Use default gateway on remote network**選項，然後按一下**OK**。



驗證

使用本節內容，確認您的組態是否正常運作。

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

- **show crypto ikev1 sa** — 顯示對等體上的所有當前IKE SA。

```
ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1   IKE Peer:
```

10.1.1.2

```
   Type    : user            Role    : responder
   Rekey   : no
```

State   : MM_ACTIVE

- show crypto ipsec sa — 顯示對等體上的所有當前IPsec SA。

```
ciscoasa# show crypto ipsec sa
interface: outside
   Crypto map tag:
```

outside_dyn_map

```
, seq num: 10, local addr: 172.16.1.2

     local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/
```

17/1701

```
)
     remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/
```

17/1701

```
)
```

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

```
     dynamic allocated peer ip(ipv6): 0.0.0.0
```

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

```
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
     #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #TFC rcvd: 0, #TFC sent: 0
     #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
     #send errors: 0, #recv errors: 0

     local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
     path mtu 1500, ipsec overhead 58(36), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: E8AF927A
     current inbound spi : 71F346AB

   inbound esp sas:
     spi: 0x71F346AB (1911768747)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000003
   outbound esp sas:
     spi: 0xE8AF927A (3903820410)
        transform: esp-3des esp-sha-hmac no compression
        in use settings ={RA, Transport, IKEv1, }
        slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (237303/3541)
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

- **show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec - 顯示有關L2TP over IPsec連線的詳細資訊。**

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed



Username     : test

                  Index        : 1


Assigned IP  : 192.168.1.1           Public IP    : 10.1.1.2


Protocol     : IKEv1 IPsec L2TPOverIPsec
License      : Other VPN
Encryption   : IKEv1: (1)3DES  IPsec: (1)3DES  L2TPOverIPsec: (1)none
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1  L2TPOverIPsec: (1)none
Bytes Tx     : 1574                  Bytes Rx     : 12752
Pkts Tx      : 29                    Pkts Rx      : 118
Pkts Tx Drop : 0                     Pkts Rx Drop : 0


Group Policy : L2TP-VPN              Tunnel Group : DefaultRAGroup


Login Time   : 23:32:48 UTC Sat May 16 2015
Duration     : 0h:04m:05s
Inactivity   : 0h:00m:00s
```

```
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1
```

IKEv1:

```
 Tunnel ID    : 1.1
 UDP Src Port : 500                    UDP Dst Port : 500
 IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
 Encryption   : 3DES                   Hashing      : SHA1
 Rekey Int (T): 28800 Seconds          Rekey Left(T): 28555 Seconds
 D/H Group    : 2
 Filter Name  :
```

IPsec:

```
 Tunnel ID    : 1.2
 Local Addr   : 172.16.1.2/255.255.255.255/17/1701
 Remote Addr  : 10.1.1.2/255.255.255.255/17/1701
 Encryption   : 3DES                   Hashing      : SHA1
 Encapsulation: Transport
 Rekey Int (T): 3600 Seconds           Rekey Left(T): 3576 Seconds
 Rekey Int (D): 250000 K-Bytes         Rekey Left(D): 250000 K-Bytes
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Bytes Tx     : 1574                   Bytes Rx     : 12752
 Pkts Tx      : 29                     Pkts Rx      : 118
```

L2TPOverIPsec:

```
 Tunnel ID    : 1.3
```

Username : test

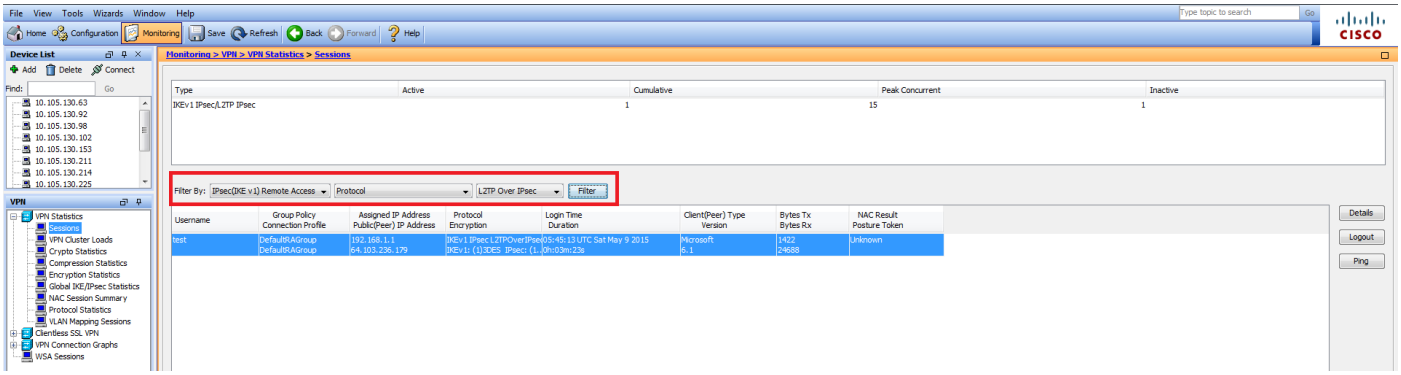
Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

```
 Encryption   : none                   Hashing      : none
```

```
Auth Mode     : msCHAPV2

Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
Client OS     : Microsoft
Client OS Ver: 6.2
Bytes Tx      : 475                  Bytes Rx     : 9093
Pkts Tx       : 18                   Pkts Rx      : 105
```

在ASDM上，在**Monitoring > VPN > VPN Statistics > Sessions**下可以看到有關VPN會話的一般資訊。L2TP over IPsec會話可以通過**IPsec(IKEv1)Remote Access > Protocol > L2TP Over IPsec**過濾。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

> **附註**：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

> **注意**：在ASA上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的詳細程度可能會增加。請謹慎執行此操作，尤其是在生產環境中！

請謹慎使用以下**debug命令**，以排除VPN隧道的問題

- **debug crypto ikev1** — 顯示有關IKE的調試資訊
- **debug crypto ipsec** — 顯示有關IPsec的調試資訊

以下是成功的L2TP over IPSec連線的調試輸出：

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
```

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended
capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,
```

Connection landed on tunnel_group DefaultRAGroup

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for
Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D
(20) + NONE (0) total length : 304
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
```

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

PSec SA Proposal # 2, Transform # 1 acceptable

  Matches global IPSec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI   : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine:
SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick
mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce
payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd
QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007fffe1c75c00,
   SCB: 0xE13ABD20,
   Direction: outbound
   SPI   : 0x8C14FD70
   Session ID: 0x00001000
   VPIF num : 0x00000002

```
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x8C14FD70
IPSEC: Creating outbound VPN context, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00000000
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: New outbound encrypt rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
```

Src ports

Upper: 1701

Lower: 1701

```
     Op   : equal
```

Dst ports

Upper: 1701

Lower: 1701

```
     Op   : equal
```

Protocol: 17

```
   Use protocol: true
   SPI: 0x00000000
   Use SPI: false
```

```
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User ()  Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x00000206
   SA   : 0x00007fffe13ab260
   SPI  : 0x7AD72E0D
   MTU  : 0 bytes
   VCID : 0x00000000
   Peer : 0x000028D4
   SCB  : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00004174
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
```

```
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 1701
     Lower: 1701
     Op   : equal
   Dst ports
     Upper: 1701
     Lower: 1701
     Op   : equal
   Protocol: 17
   Use protocol: true
   SPI: 0x00000000
   Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   Dst mask: 255.255.255.255
   Src ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Dst ports
     Upper: 0
     Lower: 0
     Op   : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

PHASE 2 COMPLETED

```
 (msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1

下表顯示了Windows客戶端上出現的一些常見的VPN相關錯誤

錯誤代碼	可能的解決方案
691	確保輸入的使用者名稱和密碼正確
789,835	確保客戶端電腦上配置的預共用金鑰與ASA上配置的預共用金鑰相同
800	1.確保VPN型別設定為「第2層隧道協定(L2TP)」 2.確保預共用金鑰配置正確
809	確保UDP埠500和4500（如果客戶端或伺服器位於NAT裝置之後）且ESP流量未被阻止

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
- 技術支援與文件 - Cisco Systems