

採用Microsoft Windows 2000和2003 IAS RADIUS驗證的Cisco Secure PIX防火牆6.x和 Cisco VPN客戶端3.5 for Windows

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[調試輸出示例](#)

[相關資訊](#)

簡介

此示例配置顯示如何配置用於Windows的Cisco VPN客戶端3.5版和用於Microsoft Windows 2000和2003 Internet身份驗證服務(IAS)RADIUS伺服器的Cisco Secure PIX防火牆。請參閱[Microsoft — 清單：配置IAS以進行撥號和VPN訪問](#)，以瞭解有關IAS的更多資訊。

請參閱[PIX/ASA 7.x和Cisco VPN Client 4.x for Windows with Microsoft Windows 2003 IAS RADIUS身份驗證配置示例](#)，以瞭解有關使用Cisco VPN Client 4.x的PIX/ASA 7.0中相同方案的詳細資訊。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- Cisco Secure PIX防火牆軟體版本6.0支援來自Cisco VPN Client 3.5 for Windows的VPN連線。
- 此示例配置假設PIX已經使用適當的靜態、管道或訪問清單運行。當前文檔無意說明這些基本概念，而是顯示從Cisco VPN客戶端到PIX的連線。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX防火牆軟體版本6.1.1**注意**：這已在PIX軟體版本6.1.1上進行了測試，但應該適用於所有6.x版本。
- 適用於Windows的Cisco VPN使用者端版本3.5
- 採用IAS的Windows 2000和2003 Server

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。

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。

設定

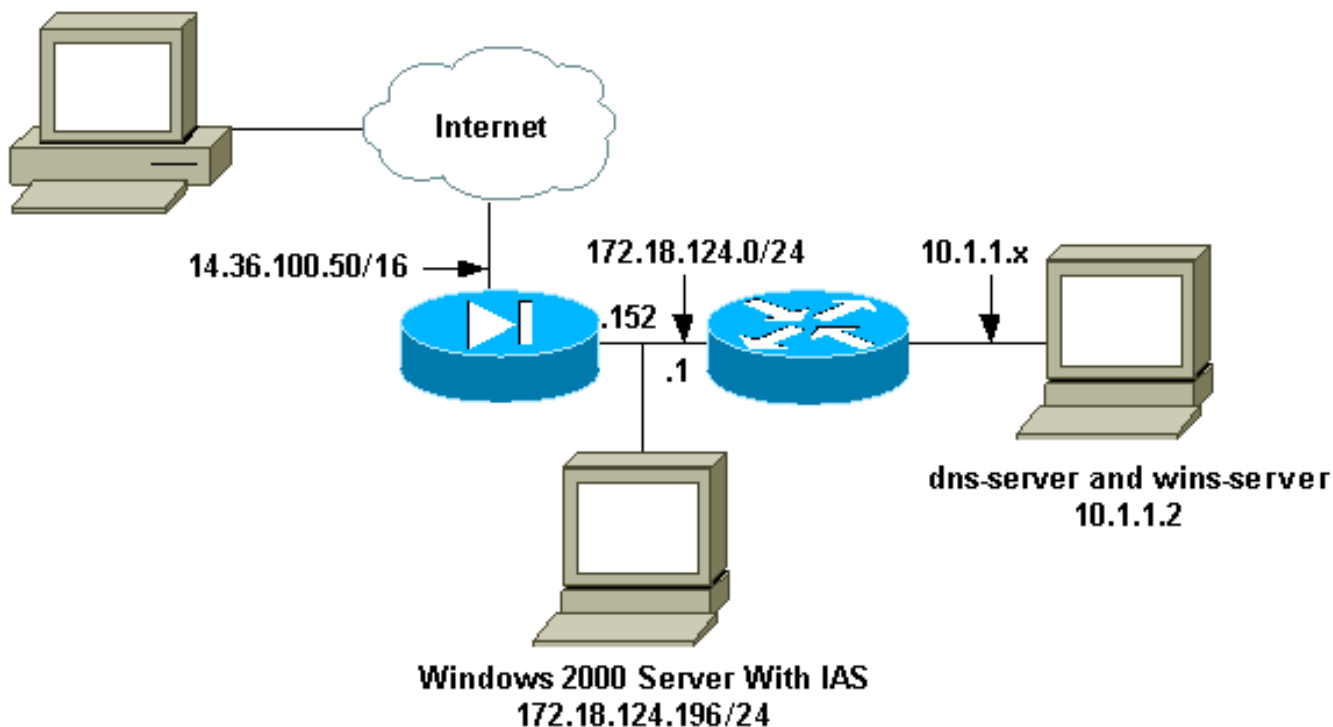
本節提供用於設定本文件中所述功能的資訊。

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：

PC With VPN Client 3.5
14.36.100.55



組態

本檔案會使用這些設定。

- [PIX防火牆](#)
- [適用於Windows的Cisco VPN使用者端3.5](#)
- [採用IAS的Microsoft Windows 2000 Server](#)
- [採用IAS的Microsoft Windows 2003 Server](#)

PIX防火牆

PIX防火牆

```

pixfirewall(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Issue the access-list command to avoid !--- Network
Address Translation (NAT) on the IPsec packets.

access-list 101 permit ip 10.1.1.0 255.255.255.0
10.1.2.0
255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 14.36.100.50 255.255.0.0
ip address inside 172.18.124.152 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
pdm history enable
arp timeout 14400
global (outside) 1 14.36.100.51
!--- Binding access list 101 to the NAT statement to
avoid !--- NAT on the IPsec packets. nat (inside) 0
access-list 101
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
route inside 10.1.1.0 255.255.255.0 172.18.124.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
!--- Enable access to the RADIUS protocol.

```

```

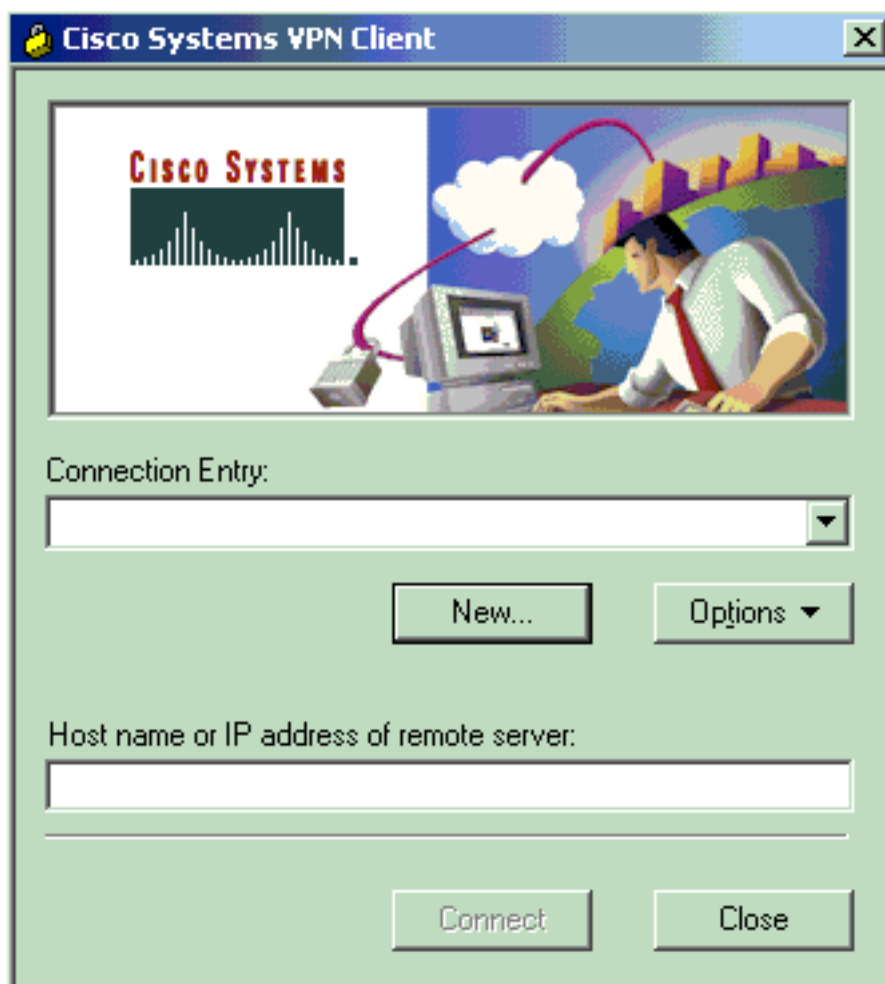
aaa-server RADIUS protocol radius
!--- Associate the partnerauth protocol to RADIUS. aaa-
server partnerauth protocol radius
aaa-server partnerauth (inside) host 172.18.124.196
cisco123
    timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Tell PIX to implicitly permit IPsec traffic. sysopt
connection permit-ipsec
no sysopt route dnat
!--- Configure a transform set that defines how the
traffic is protected. crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- Create a dynamic crypto map and specify which !---
transform sets are allowed for this dynamic crypto map
entry. crypto dynamic-map dynmap 10 set transform-set
myset
!--- Add the dynamic crypto map set into a static crypto
map set. crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- Enable the PIX to launch the Xauth application on
the VPN Client. crypto map mymap client authentication
partnerauth
!--- Apply the crypto map to the outside interface.
crypto map mymap interface outside
!--- IKE Policy Configuration. isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password *****
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:3f9e31533911b8a6bb5c0f06900c2dbc
: end
[OK]
pixfirewall(config)#

```

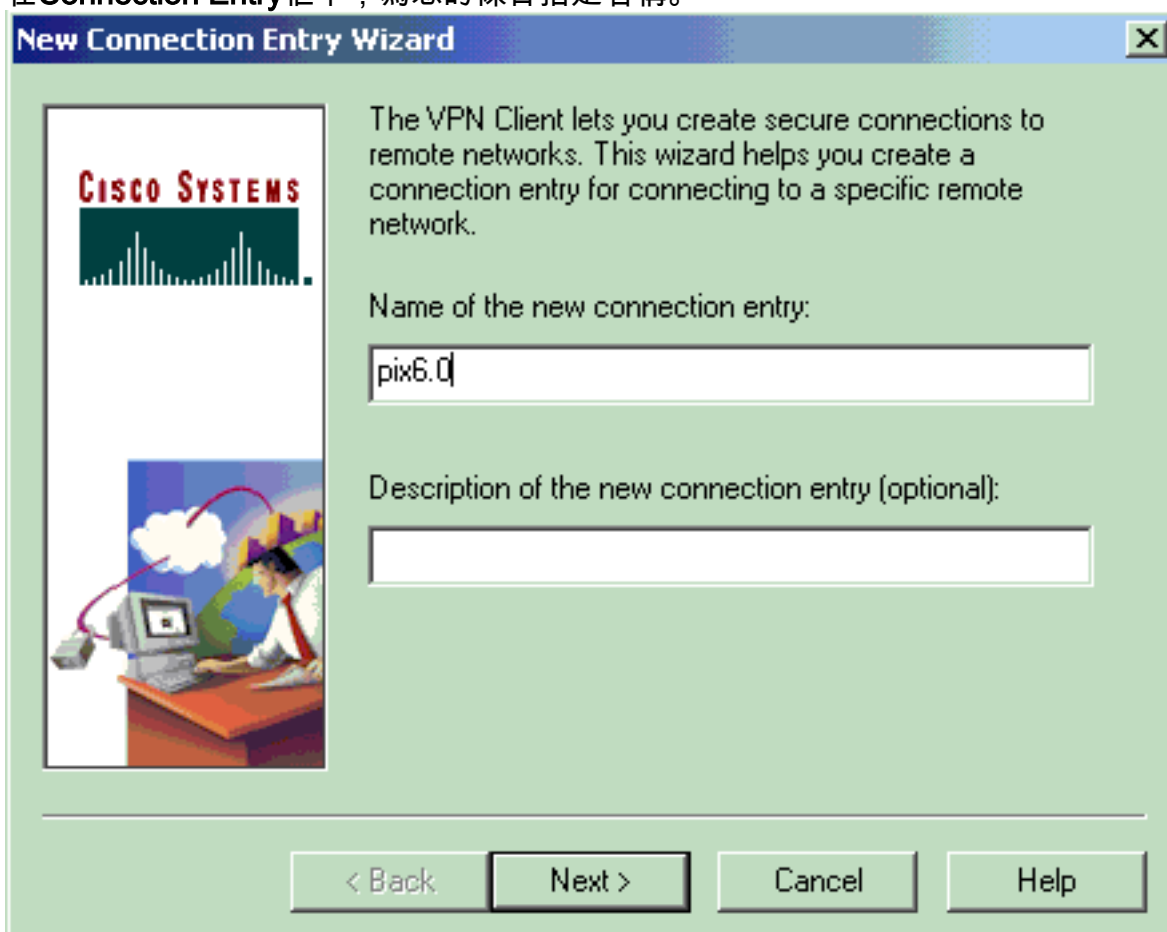
[適用於Windows的Cisco VPN使用者端3.5](#)

本節介紹如何配置Cisco VPN Client 3.5 for Windows。

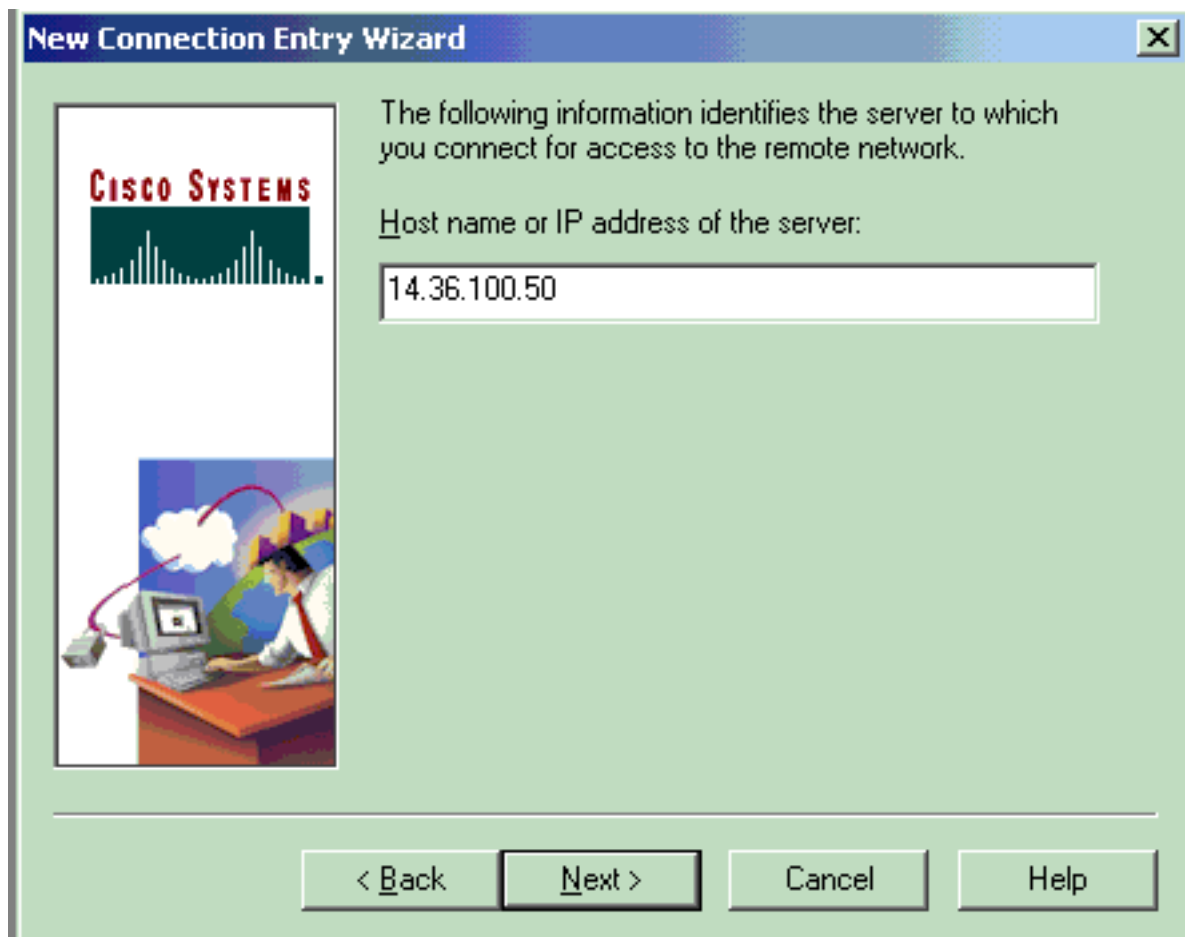
1. 啟動VPN客戶端，然後按一下**New**建立新連線。



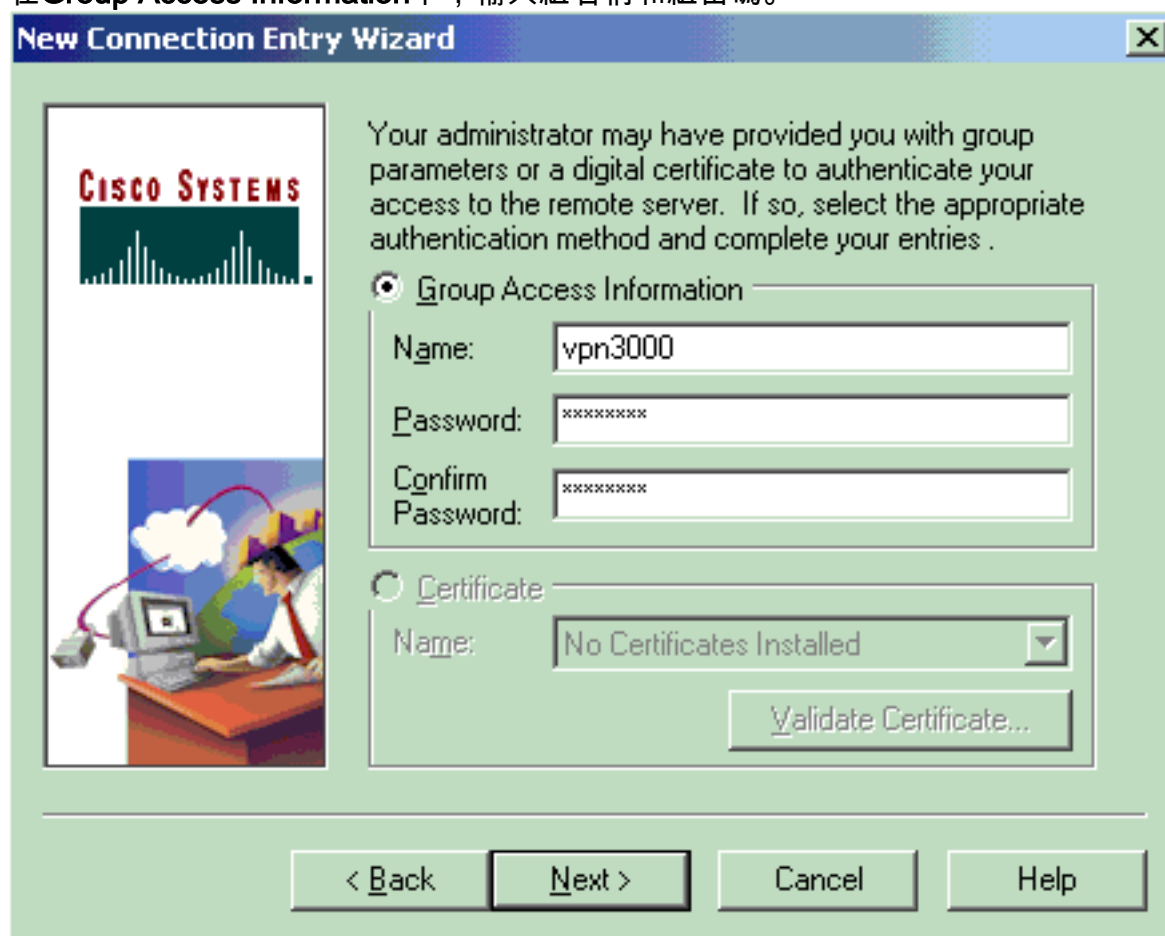
2. 在Connection Entry框中，為您的條目指定名稱。



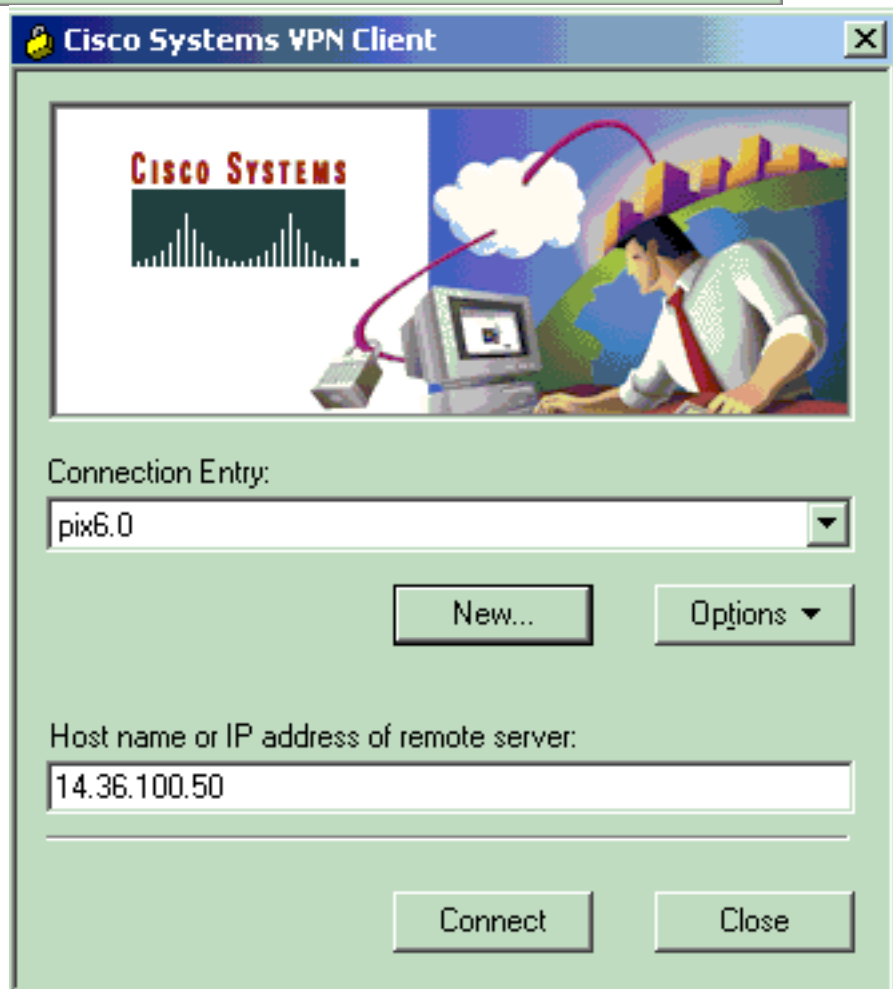
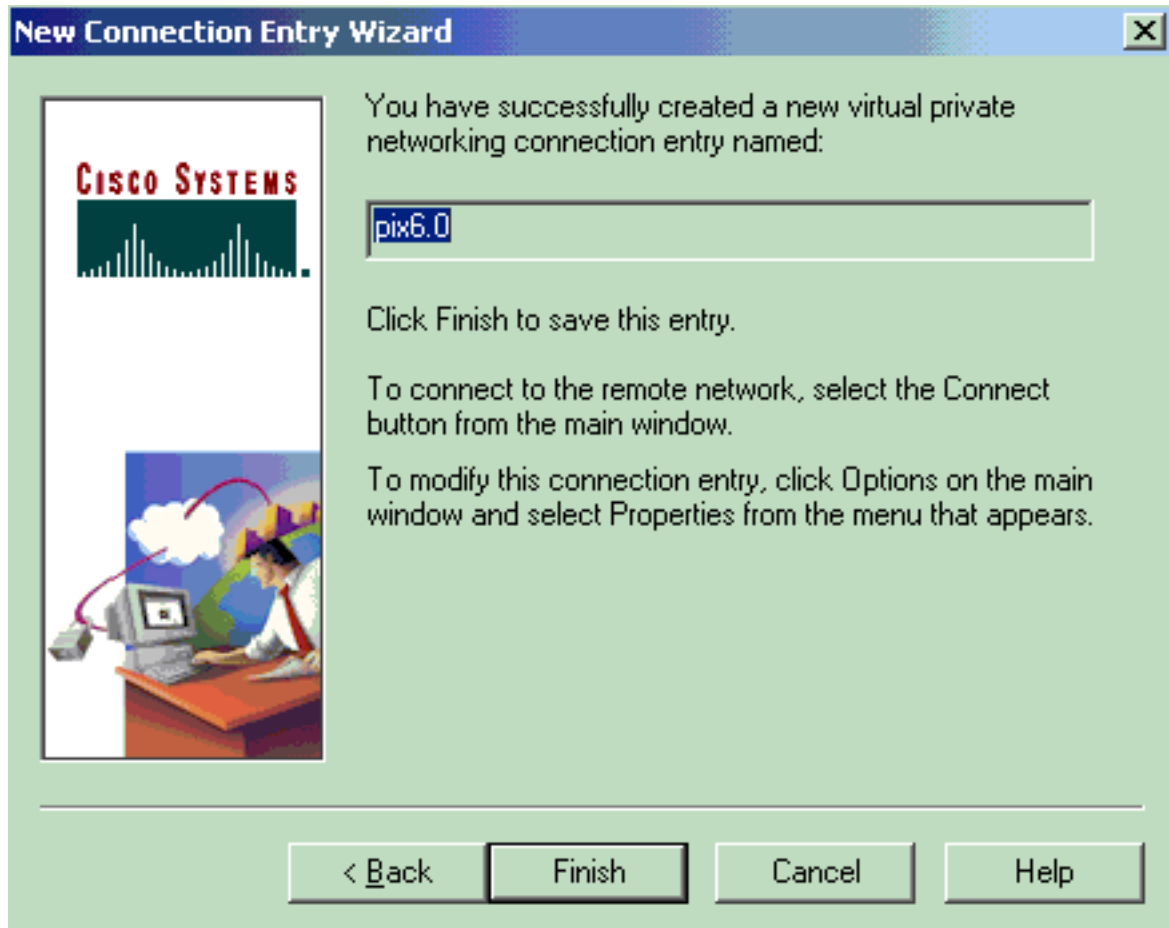
3. 輸入PIX公共介面的IP地址。



4. 在Group Access Information下，輸入組名稱和組密碼。



5. 按一下Finish將配置檔案儲存在登錄檔中。

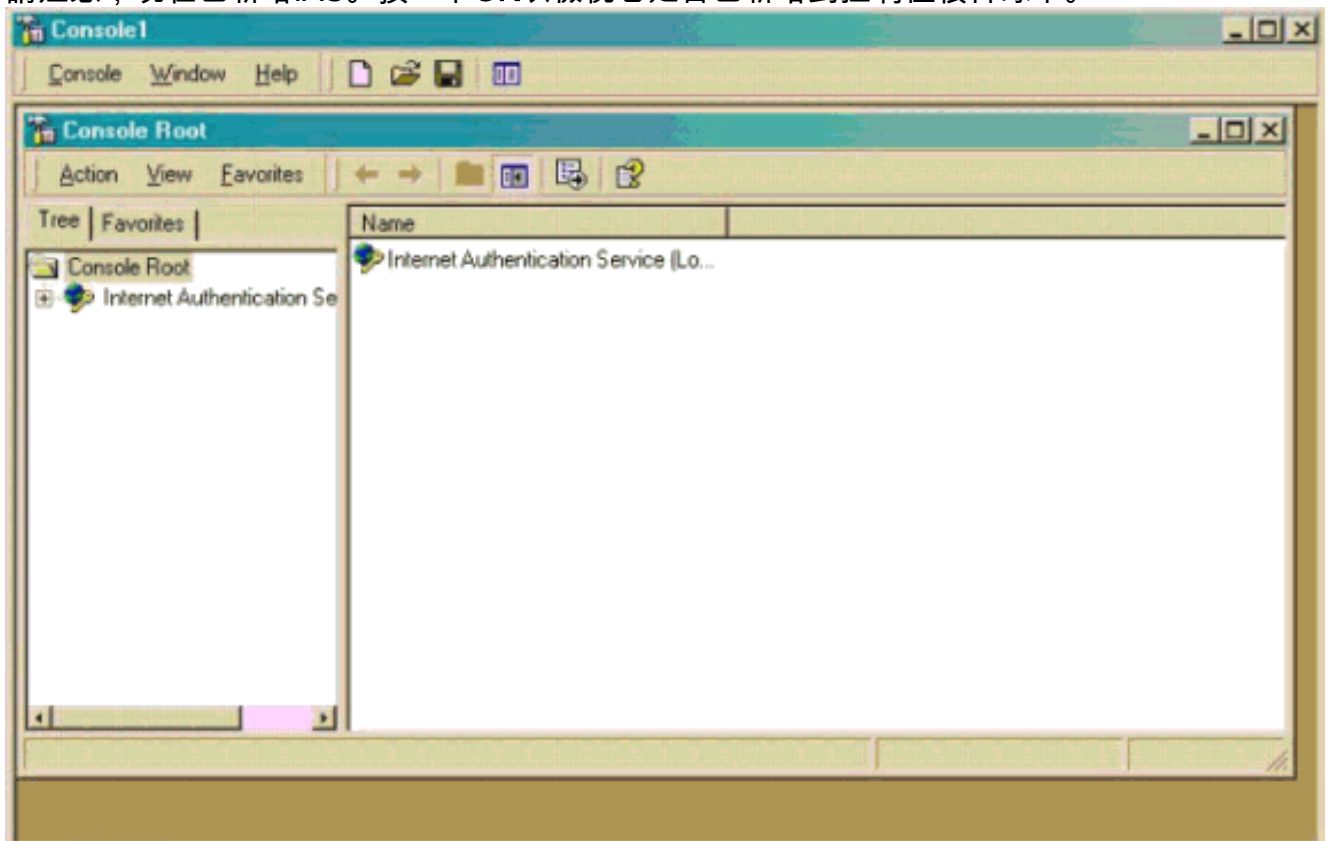


6. 按一下**Connect**連線到PIX。

完成以下步驟，使用IAS配置Microsoft Windows 2000伺服器。這是使用Windows 2000 IAS伺服器進行VPN使用者的RADIUS身份驗證的非常基本的設定。如果需要更複雜的設計，請與Microsoft聯絡以獲得幫助。

注意：這些步驟假定已在本地電腦上安裝了IAS。如果不是，請通過控制面板>新增/刪除程式新增此項。

1. 啟動Microsoft管理控制檯。選擇「Start > Run」，然後鍵入mmc。然後按一下OK。
2. 選擇Console > Add Remove Snap-In....以便將IAS服務新增到此控制檯。
3. 按一下Add以啟動包含所有可用獨立管理單元的新視窗。按一下Internet Authentication Service(IAS)，然後按一下Add。
4. 確保選中Local Computer，然後按一下Finish。然後按一下「Close」。
5. 請注意，現在已新增IAS。按一下OK以檢視它是否已新增到控制檯根目錄中。



6. 展開Internet Authentication Service，然後按一下右鍵Clients。按一下New Client並輸入名稱。名字的選擇其實並不重要；它將是您在此檢視中看到的內容。確保選擇RADIUS並按一下下一步。
7. 使用IAS伺服器所連線的PIX介面地址填寫Client address。確保選擇RADIUS Standard並新增共用金鑰，以匹配在PIX上輸入的命令：

```
aaa-server partnerauth (inside) host 172.18.124.196 cisco123 timeout 5
```

注意：在本示例中，「cisco123」是共用金鑰。

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
172.18.124.152 Verify...

Client-Vendor:
RADIUS Standard

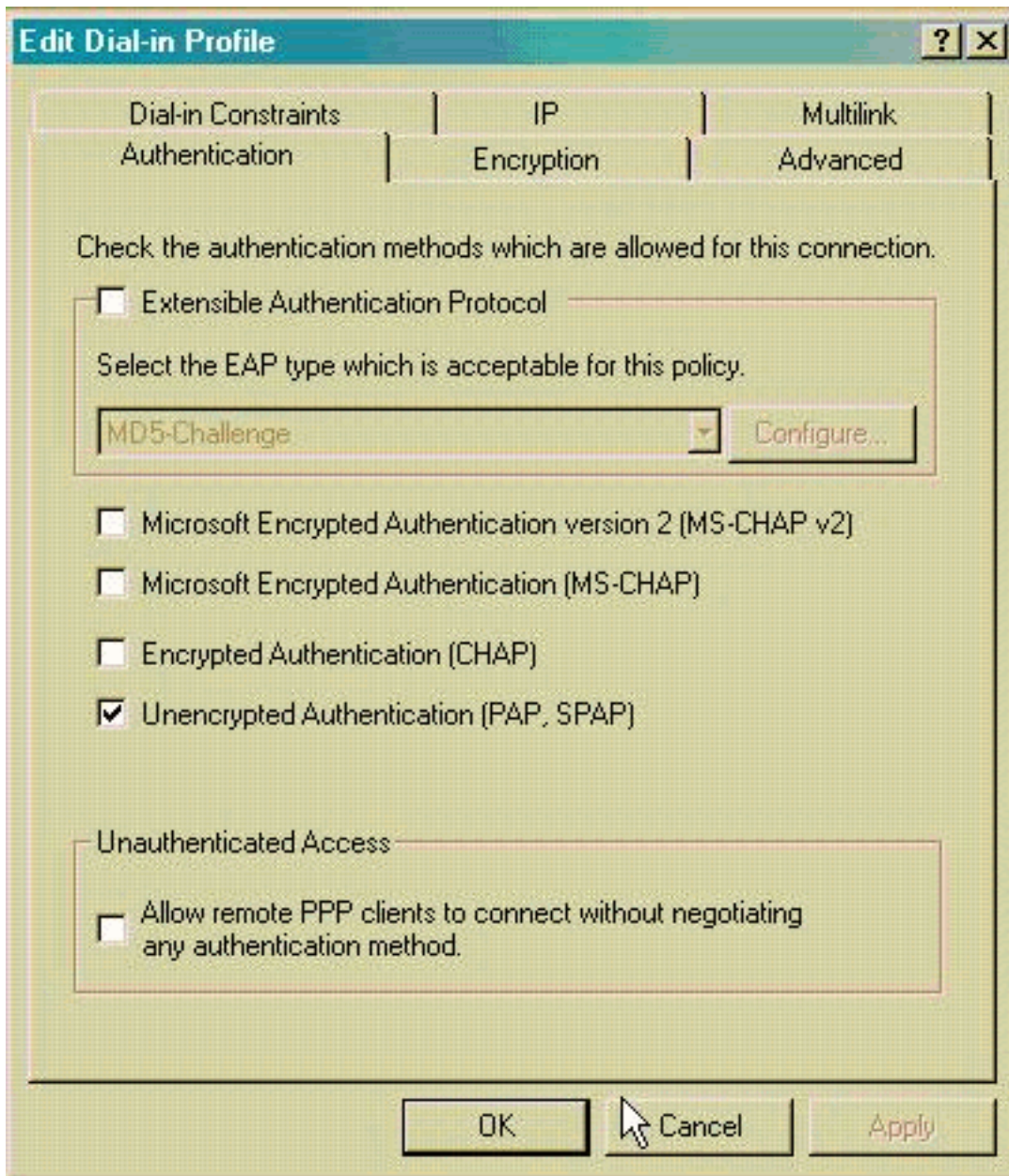
Client must always send the signature attribute in the request

Shared secret: xxxxxxxx

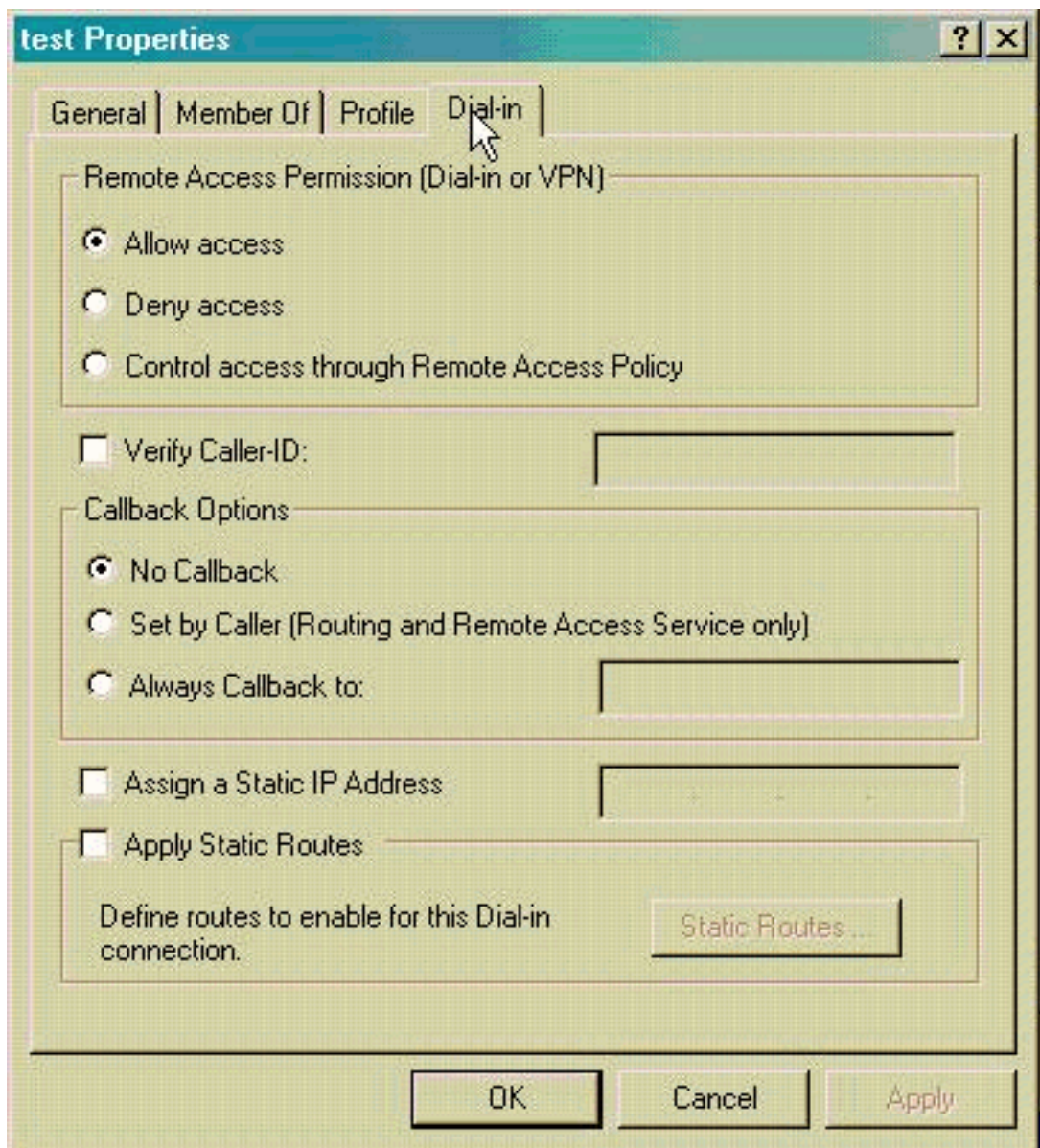
Confirm shared secret: xxxxxxxx

< Back Finish Cancel

8. 按一下**Finish**以返回控制檯根目錄。
9. 在左窗格中按一下**Remote Access Policies**，然後按兩下標籤為**Allow access if dial-in permission is enabled**的策略。
10. 按一下**Edit Profile**，然後轉到Authentication頁籤。在**Authentication Methods**下，確保僅選中**Unencrypted Authentication(PAP, SPAP)**。注意：VPN客戶端只能將此方法用於身份驗證



11. 按一下「Apply」，然後「OK」兩次。
12. 若要將使用者修改為允許連線，請選擇**Console > Add/Remove Snap-in**。按一下Add，然後選擇**Local Users and Groups**管理單元。按一下「Add」。確保選擇**Local Computer**，然後按一下Finish。按一下「OK」（確定）。
13. 展開**Local User and Groups**，然後按一下左窗格中的**Users**資料夾。在右窗格中，按兩下要允許訪問的使用者。
14. 按一下Dial-in（撥入）頁籤，然後在**Remote Access Permission(Dial-in or VPN)**下選擇**Allow**



Access。

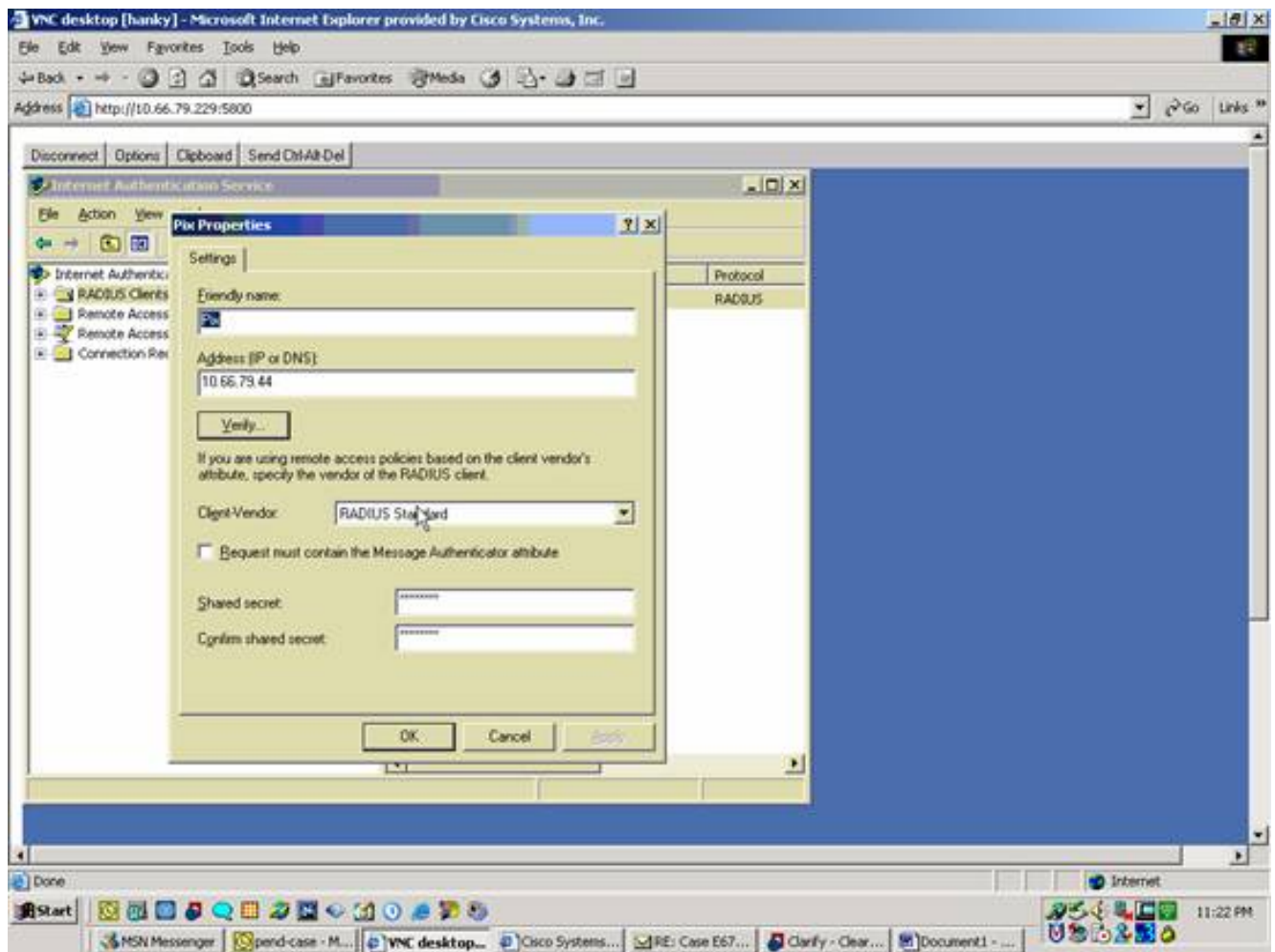
15. 按一下「Apply」和「OK」完成動作。如果需要，可以關閉Console Management螢幕並儲存會話。
16. 您修改的使用者現在應該能夠使用VPN客戶端3.5訪問PIX。請記住，IAS伺服器只對使用者資訊進行身份驗證。PIX仍然執行組身份驗證。

[採用IAS的Microsoft Windows 2003 Server](#)

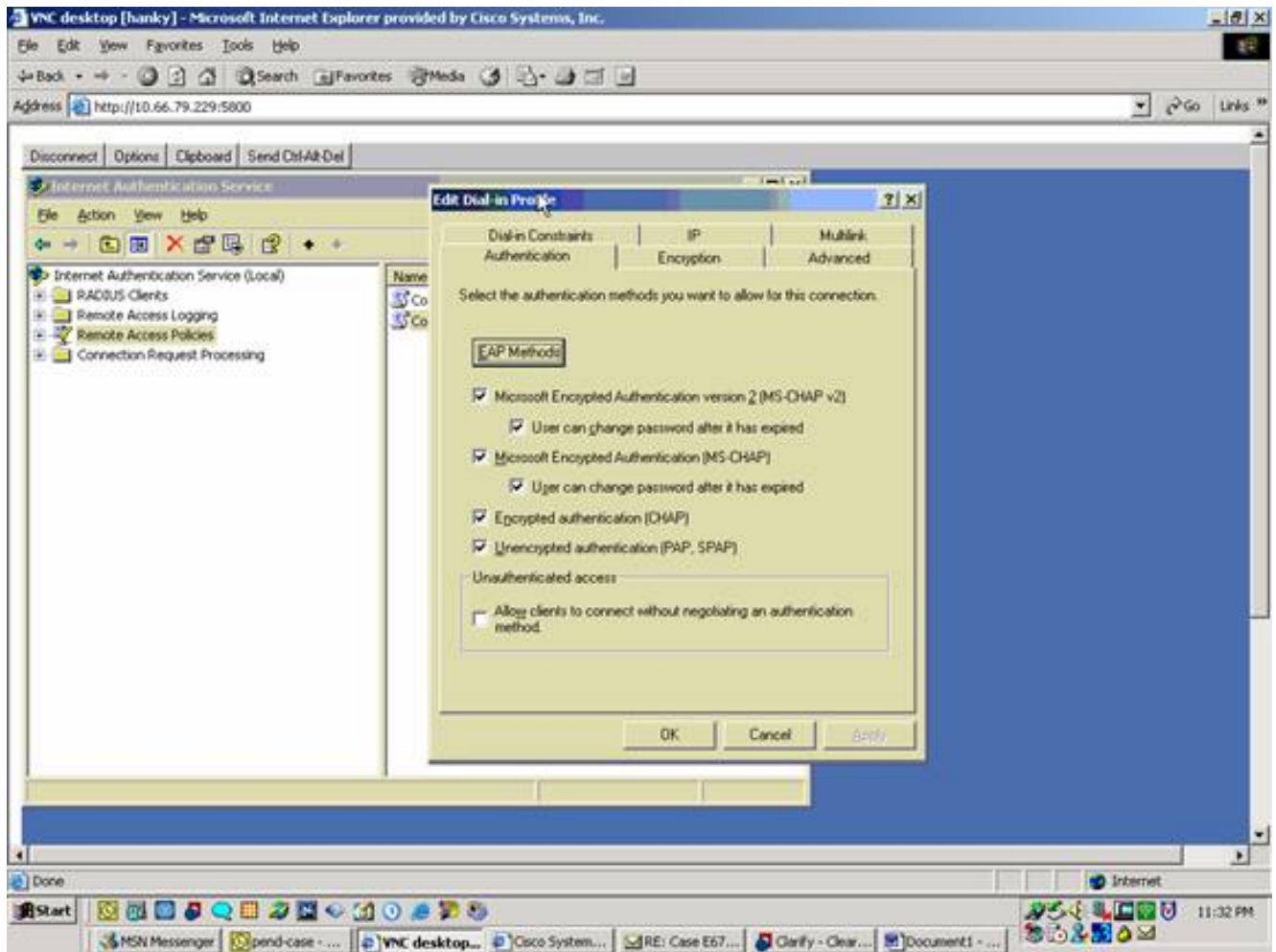
完成以下步驟，使用IAS配置Microsoft Windows 2003伺服器。

注意：這些步驟假定已在本地電腦上安裝了IAS。如果不是，請通過控制面板>新增/刪除程式新增此項。

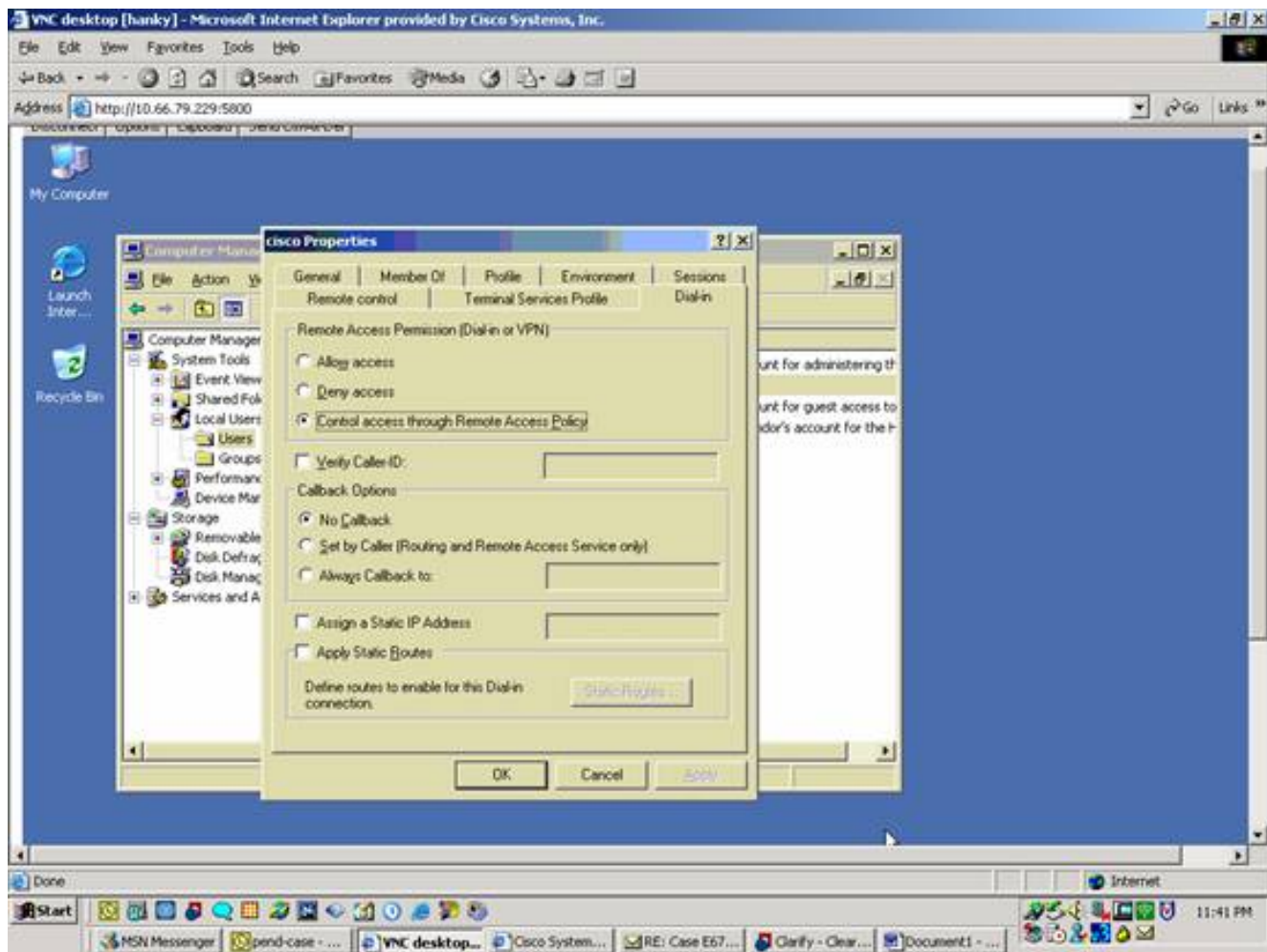
1. 選擇Administrative Tools > Internet Authentication Service，然後按一下右鍵RADIUS Client以新增新的RADIUS客戶端。鍵入客戶端資訊後，按一下OK。此範例顯示IP位址為10.66.79.44且名為「Pix」的使用者端。使用者端 — 廠商設定為RADIUS標準，而共用金鑰為「cisco123」。



2. 轉到遠端訪問策略，按一下右鍵與其他訪問伺服器的連線，然後選擇屬性。
3. 確保選中授予遠端訪問許可權的選項。
4. 按一下Edit Profile並檢查這些設定。在Authentication頁籤上，選中Unencrypted authentication(PAP，SPAP)。在「加密」頁籤上，確保選中「無加密」選項。完成後按一下OK。



5. 將使用者新增到本地電腦帳戶。為此，請選擇**管理工具>電腦管理>系統工具>本地使用者和組**。按一下右鍵**Users**並選擇**New Users**。
6. 使用思科密碼「cisco123」新增使用者並檢查此配置檔案資訊。在「General (常規)」頁籤上，確保選中**Password Never Expired**選項，而不是「User Must Change Password (使用者必須更改密碼)」選項。在「撥入」頁籤上，選擇**允許訪問** (或保留「通過遠端訪問策略控制訪問」的預設設定) 的選項。完成後按一下**OK**。



驗證

使用本節內容，確認您的組態是否正常運作。

[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** — 顯示當前安全關聯使用的設定。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。有關其他資訊，請參閱 [排除 PIX 故障以在已建立的 IPsec 隧道上傳遞資料流量](#)。

疑難排解指令

[輸出直譯器工具](#) (僅供註冊客戶使用) 支援特定命令，此工具允許您檢視 **show** 命令輸出的分析。

注意：使用 **debug** 命令之前，請先參閱 [有關 Debug 命令的重要資訊](#)，並參閱 [IP 安全故障排除 — 瞭解和使用 debug 命令](#)。

- **debug crypto ipsec** — 檢視階段 2 的 IPsec 協商。

- `debug crypto isakmp` — 檢視階段1的ISAKMP協商。
- `debug crypto engine` — 檢視已加密的流量。

調試輸出示例

- [PIX防火牆](#)
- [適用於Windows的VPN使用者端3.5](#)

PIX防火牆

```

pixfirewall(config)#
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
VPN Peer: ISAKMP: Added new peer: ip:14.36.100.55 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:14.36.100.55 Ref cnt incremented to:1
  Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy

```

ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP: Created a peer node for 14.36.100.55
ISAKMP (0): ID payload
 next-payload : 10
 type : 1
 protocol : 17
 port : 500
 length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
 spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got
 a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 14.36.100.55

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3870616596
 (0xe6b4ec14)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
 message ID = 84
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3612718114
 (0xd755b422)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
 message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange


```
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
  message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_ADDRESS (1)
ISAKMP: attribute    IP4_NETMASK (2)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ADDRESS_EXPIRY (5)
  Unsupported Attr: 5
ISAKMP: attribute    APPLICATION_VERSION (7)
  Unsupported Attr: 7
ISAKMP: attribute    UNKNOWN (28672)
  Unsupported Attr: 28672
ISAKMP: attribute    UNKNOWN (28673)
  Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28674)
ISAKMP: attribute    UNKNOWN (28676)
ISAKMP: attribute    UNKNOWN (28679)
  Unsupported Attr: 28679
ISAKMP: attribute    UNKNOWN (28680)
  Unsupported Attr: 28680
ISAKMP: attribute    UNKNOWN (28677)
  Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 14.36.100.55.
  ID = 3979868003
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1527320241

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
  IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (1)
ISAKMP : Checking IPsec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-SHA
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
  IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (2)
ISAKMP : Checking IPsec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
```

ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPsec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 2, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (6)
ISAKMP : Checking IPsec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
dest_proxy= 14.36.100.50/255.255.255.255/0/0 (type=1),
src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1527320241

ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1527320241

```
ISAKMP (0): ID_IPV4_ADDR dst 14.36.100.50 prot 0 port
  0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf39c2217(4087095831) for SA
  from 14.36.100.55 to 14.36.100.50 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3487980779

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
  inbound SA from 14.36.100.55 to 14.36.100.50
    (proxy 10.1.2.1 to 14.36.100.50)
  has spi 4087095831 and conn_id 1 and flags 4
  lifetime of 2147483 seconds
  outbound SA from 14.36.100.50 to 14.36.100.55
    (proxy 14.36.100.50 to 10.1.2.1)
  has spi 1929305241 and conn_id 2 and flags 4
  lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
  dest_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
  src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0xf39c2217(4087095831), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
  src_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
  dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0x72fedc99(1929305241), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:2
  Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:3
  Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
  inbound SA from 14.36.100.55 to 14.36.100.50
    (proxy 10.1.2.1 to 0.0.0.0)
  has spi 1791135440 and conn_id 3 and flags 4
  lifetime of 2147483 seconds
  outbound SA from 14.36.100.50 to 14.36.100.55
    (proxy 0.0.0.0 to 10.1.2.1)
  has spi 173725574 and conn_id 4 and flags 4
  lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
```

```
(key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
  dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
  src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0x6ac28ed0(1791135440), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
  src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
  dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0xa5ad786(173725574), conn_id= 4, keysize= 0, flags= 0x4
```

```
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:4
Total VPN Peers:1
```

```
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:5
Total VPN Peers:1
```

```
return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
```

```
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
```

```
spi 0, message ID = 3443334051
```

```
ISAKMP (0): received DPD_R_U_THERE from peer 14.36.100.55
```

```
ISAKMP (0): sending NOTIFY message 36137 protocol 1
```

```
return status is IKMP_NO_ERR_NO_TRANS
```

[適用於Windows的VPN使用者端3.5](#)

```
193 19:00:56.073 01/24/02 Sev=Info/6 DIALER/0x63300002
Initiating connection.
```

```
194 19:00:56.073 01/24/02 Sev=Info/4 CM/0x63100002
Begin connection process
```

```
195 19:00:56.083 01/24/02 Sev=Info/4 CM/0x63100004
Establish secure connection using Ethernet
```

```
196 19:00:56.083 01/24/02 Sev=Info/4 CM/0x63100026
Attempt connection with server "14.36.100.50"
```

```
197 19:00:56.083 01/24/02 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 14.36.100.50.
```

```
198 19:00:56.124 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
to 14.36.100.50
```

```
199 19:00:56.774 01/24/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys
```

```
200 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50
```

```
201 19:00:59.539 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH)
from 14.36.100.50
```

```
202 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100
```

```
203 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000001
Peer is a Cisco-Unity compliant peer
```

204 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

205 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000001
Peer supports DPD

206 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 6D761DDC26ACECA1B0ED11FABBB860C4

207 19:00:59.569 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 14.36.100.50

208 19:00:59.569 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

209 19:00:59.569 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

210 19:00:59.569 01/24/02 Sev=Info/4 CM/0x63100015
Launch xAuth application

211 19:01:04.236 01/24/02 Sev=Info/4 CM/0x63100017
xAuth application returned

212 19:01:04.236 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

213 19:01:04.496 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

214 19:01:04.496 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

215 19:01:04.496 01/24/02 Sev=Info/4 CM/0x6310000E
Established Phase 1 SA. 1 Phase 1 SA in the system

216 19:01:04.506 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

217 19:01:04.516 01/24/02 Sev=Info/5 IKE/0x6300005D
Client sending a firewall request to concentrator

218 19:01:04.516 01/24/02 Sev=Info/5 IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability=
(Centralized Policy Push).

219 19:01:04.516 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

220 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

221 19:01:04.586 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

222 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
value = 10.1.2.1

223 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): ,
value = 10.1.1.2

224 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS)
: , value = 10.1.1.2

225 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: ,
value = cisco.com

226 19:01:04.586 01/24/02 Sev=Info/4 CM/0x63100019
Mode Config data received

227 19:01:04.606 01/24/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 14.36.100.50,
GW IP = 14.36.100.50

228 19:01:04.606 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

229 19:01:04.606 01/24/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 14.36.100.50

230 19:01:04.606 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

231 19:01:04.786 01/24/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

232 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

233 19:01:05.948 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

234 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

235 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

236 19:01:05.948 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

237 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x5B090EB1 OUTBOUND SPI =
0xF39C2217 INBOUND SPI = 0x72FEDC99)

238 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xF39C2217

239 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x72FEDC99

240 19:01:05.948 01/24/02 Sev=Info/4 CM/0x6310001A
One secure connection established

241 19:01:05.988 01/24/02 Sev=Info/6 DIALER/0x63300003
Connection established.

242 19:01:06.078 01/24/02 Sev=Info/6 DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

243 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x6300002F

Received ISAKMP packet: peer = 14.36.100.50

244 19:01:06.118 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

245 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

246 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

247 19:01:06.118 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

248 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0xCFE65CEB OUTBOUND SPI =
0x6AC28ED0 INBOUND SPI = 0x0A5AD786)

249 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x6AC28ED0

250 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x0A5AD786

251 19:01:06.118 01/24/02 Sev=Info/4 CM/0x63100022
Additional Phase 2 SA established.

252 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

253 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x17229cf3 into key list

254 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

255 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x99dcfe72 into key list

256 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

257 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xd08ec26a into key list

258 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

259 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x86d75a0a into key list

260 19:01:15.032 01/24/02 Sev=Info/6 IKE/0x6300003D
Sending DPD request to 14.36.100.50, seq# = 152233542

261 19:01:15.032 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 14.36.100.50

262 19:01:15.032 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

263 19:01:15.032 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)

from 14.36.100.50

264 19:01:15.032 01/24/02 Sev=Info/5 IKE/0x6300003F
Received DPD ACK from 14.36.100.50, seq# received = 152233542,
seq# expected = 152233542

[相關資訊](#)

- [PIX支援頁](#)
- [PIX命令參考](#)
- [RADIUS 支援頁面](#)
- [Cisco VPN 3000系列集中器支援頁面](#)
- [Cisco VPN 3000系列使用者端支援頁面](#)
- [IPsec協商/IKE通訊協定支援頁面](#)
- [要求建議 \(RFC\)](#)
- [技術支援 - Cisco Systems](#)