使用證書在PIX防火牆和Windows 2000 PC之間配置L2TP Over IPSec

目錄

簡介

Cisco Secure PIX防火牆軟體版本6.x或更高版本支援基於IPsec的第2層隧道協定(L2TP)。運行Windows 2000的使用者可以使用本機IPsec客戶端和L2TP客戶端來建立到PIX防火牆的L2TP隧道。流量流經由IPsec安全關聯(SA)加密的L2TP通道。

注意：不能使用Windows 2000 L2TP IPsec客戶端通過Telnet連線到PIX。

注意：PIX上的L2TP不支援分割隧道。

要使用預共用金鑰和Microsoft Windows 2003 Internet Authentication Service(IAS)RADIUS伺服器進行使用者身份驗證，配置從遠端Microsoft Windows 2000/2003和XP客戶端到PIX/ASA安全裝置公司辦公室的L2TP over IPsec，請參閱Windows 2000/XP PC和PIX/ASA 7.2之間使用預共用金鑰配置示例是。

要使用加密方法配置從遠端Microsoft Windows 2000和XP客戶端到公司站點的L2TP over IP安全(IPsec)，請參閱使用預共用金鑰將L2TP over IPSec從Windows 2000或XP客戶端配置到Cisco VPN 3000系列集中器。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊適用於以下軟體和硬體版本：

- PIX軟體版本6.3(3)
- Windows 2000，帶或不帶SP2(有關SP1的資訊，請參閱Microsoft tip Q276360 。)

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

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

Cisco Secure PIX版本6.x或更高版本中的證書支援包括Baltimore、Microsoft、VeriSign和Entrust伺服器。目前，PIX不接受沒有IPsec保護的L2TP請求。

此示例說明如何為本文檔前面提到的場景配置PIX防火牆。Internet金鑰交換(IKE)身份驗證使用**rsa-sig**命令（證書）。 在本範例中，驗證是由RADIUS伺服器執行。

支援IPSec/PPTP/L2TP的Cisco硬體和VPN客戶端中列出了與PIX的加密客戶端連線的較少涉及的選項。

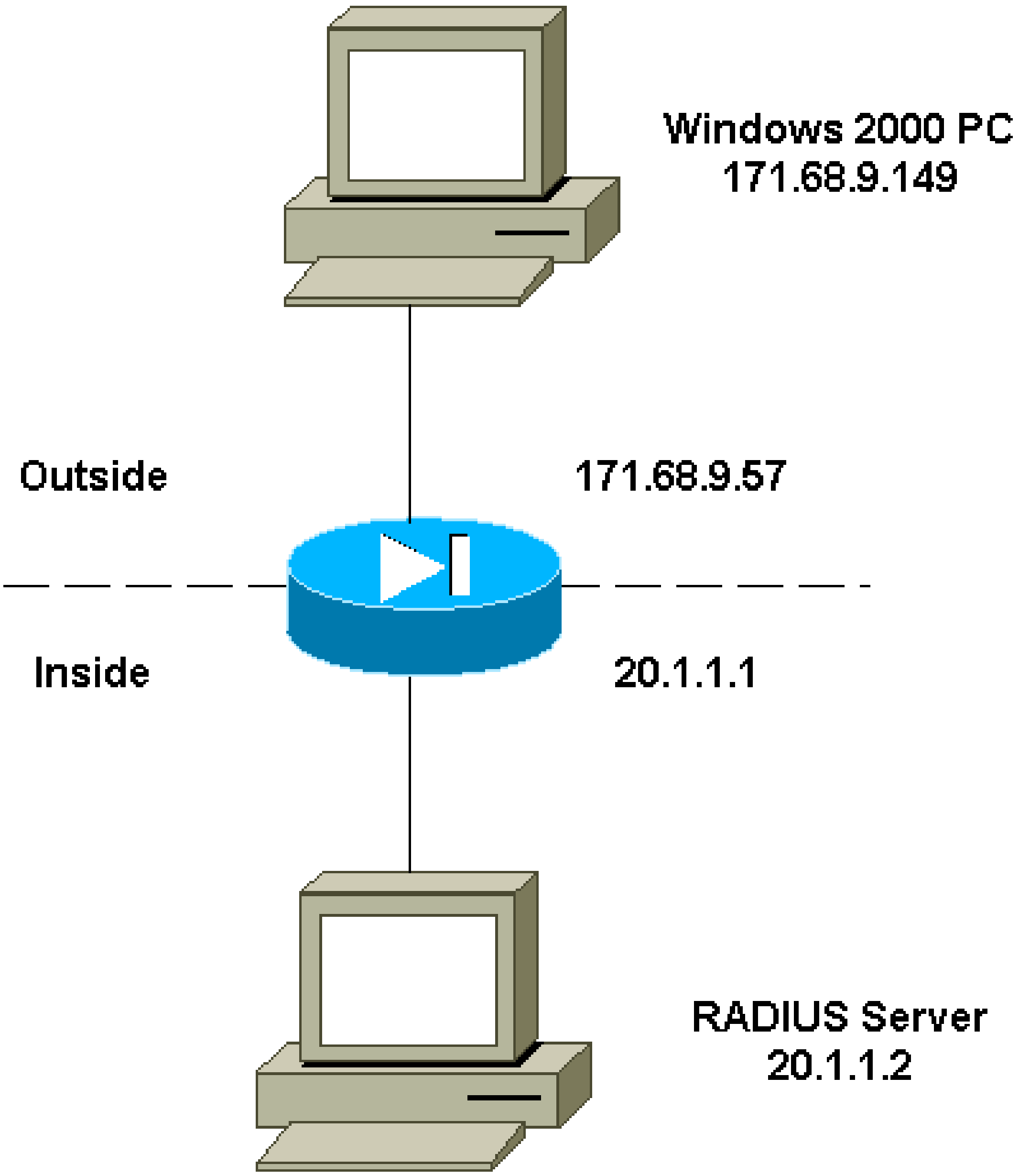
設定

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(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



配置Microsoft L2TP客戶端

有關如何配置Microsoft L2TP客戶端的資訊，請參閱Microsoft的Internet協定安全分步指南 。

如微軟提供的分步指南中所述，客戶端支援許多經過測試的證書頒發機構(CA)伺服器。有關如何設定Microsoft CA的資訊，請參閱Microsoft的《設定證書頒發機構的分步指南》 。

獲取PIX防火牆的證書

有關如何配置PIX以與VeriSign、Entrust、Baltimore和Microsoft的證書進行互操作性的詳細資訊，請參閱CA配置示例。

PIX防火牆配置

本檔案會使用此組態。

PIX防火牆

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-506-2
domain-name sjvpn.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access Control List (ACL) configured to bypass !---
Network Address Translation (NAT) for the L2TP IP pool.
access-list nonat permit ip 20.1.1.0 255.255.255.0
50.1.1.0 255.255.255.0
!--- ACL configured to permit L2TP traffic (UDP port
1701). access-list l2tp permit udp host 171.68.9.57 any
eq 1701
no pager
logging on
logging console debugging
logging buffered debugging
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 171.68.9.57 255.255.255.0
ip address inside 20.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Pool for L2TP address assignment. ip local pool
l2tp 50.1.1.1-50.1.1.5
pdm history enable
arp timeout 14400
!--- NAT configuration that matches previously defined
!--- ACL for the L2TP IP pool. nat (inside) 0 access-
list nonat
route outside 0.0.0.0 0.0.0.0 171.68.9.1 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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
!--- AAA (RADIUS) server configuration. aaa-server
RADIUS (inside) host 20.1.1.2 cisco timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- sysopt command entry to permit L2TP !--- traffic,
while bypassing all ACLs.

sysopt connection permit-l2tp
no sysopt route dnat
!--- The IPsec configuration. crypto ipsec transform-set
l2tp esp-des esp-md5-hmac
```

```
!--- Only transport mode is supported. crypto ipsec
transform-set l2tp mode transport
crypto ipsec security-association lifetime seconds 3600
crypto dynamic-map dyna 20 match address l2tp
crypto dynamic-map dyna 20 set transform-set l2tp
crypto map mymap 10 ipsec-isakmp dynamic dyna
crypto map mymap client authentication RADIUS
crypto map mymap interface outside
!--- The IKE configuration. isakmp enable outside
isakmp policy 20 authentication rsa-sig
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 86400
ca identity sjvpn 171.68.9.149:/certsrv/mscep/mscep.dll
ca configure sjvpn ra 1 20 crloptional
telnet 171.68.9.0 255.255.255.0 inside
telnet 20.1.1.2 255.255.255.255 inside
telnet timeout 60
ssh timeout 5
!--- The L2TP configuration parameters. vpdn group
l2tpipsec accept dialin l2tp
vpdn group l2tpipsec ppp authentication chap
vpdn group l2tpipsec ppp authentication mschap
vpdn group l2tpipsec client configuration address local
l2tp
vpdn group l2tpipsec client configuration dns 20.1.1.250
20.1.1.251
vpdn group l2tpipsec client configuration wins
20.1.1.250
vpdn group l2tpipsec client authentication aaa RADIUS
vpdn group l2tpipsec client accounting RADIUS
vpdn group l2tpipsec l2tp tunnel hello 60
vpdn enable outside
terminal width 80
Cryptochecksum:06a53009d1e9f04740256d9f0fb82837
: end
[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 ca cert** — 顯示有關您的證書、CA證書和任何註冊機構(RA)證書的資訊。

  ```
  Certificate
  Status: Available
  Certificate Serial Number: 0371630800000000022
  Key Usage: General Purpose
  Subject Name
  Name: PIX-506-2.sjvpn.com
  Validity Date:
  start date: 16:29:10 Apr 27 2001
  end date: 16:39:10 Apr 27 2002


  RA Signature Certificate
  Status: Available
  ```

```
Certificate Serial Number: 0347dc82000000000002
Key Usage: Signature
CN = scott
OU = tac
O = cisco
L = san jose
ST = ca
C = US
EA =<16> zaahmed@cisco.com
Validity Date:
start date: 18:47:45 Jul 27 2000

end date: 18:57:45 Jul 27 2001


CA Certificate
Status: Available
Certificate Serial Number: 1102485095cbf8b3415b2e96e86800d1
Key Usage: Signature
CN = zakca
OU = vpn
O = cisco
L = sj
ST = california
C = US
EA =<16> zaahmed@cisco.com
Validity Date:
start date: 03:15:09 Jul 27 2000

end date: 03:23:48 Jul 27 2002


RA KeyEncipher Certificate
Status: Available
Certificate Serial Number: 0347df0d000000000003
Key Usage: Encryption
CN = scott
OU = tac
O = cisco
L = san jose
ST = ca
C = US
EA =<16> zaahmed@cisco.com
Validity Date:
start date: 18:47:46 Jul 27 2000

end date: 18:57:46 Jul 27 2001
```

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

```
dst src state pending created
171.68.9.57 171.68.9.149 QM_IDLE 0 1
```

- **show crypto ipsec sa** — 顯示當前SA使用的設定。

```
interface: outside
Crypto map tag: mymap, local addr. 171.68.9.57
local ident (addr/mask/prot/port): (171.68.9.57/255.255.255.255/17/1701)
remote ident (addr/mask/prot/port): (171.68.9.149/255.255.255.255/17/1701)
current_peer: 171.68.9.149
dynamic allocated peer ip: 0.0.0.0

PERMIT, flags={reassembly_needed,transport_parent,}
#pkts encaps: 20, #pkts encrypt: 20, #pkts digest 20
#pkts decaps: 45, #pkts decrypt: 45, #pkts verify 45
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
```

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

local crypto endpt.: 171.68.9.57, remote crypto endpt.: 171.68.9.149
path mtu 1500, ipsec overhead 36, media mtu 1500
current outbound spi: a8c54ec8

inbound esp sas:
spi: 0xfbc9db43(4224310083)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (99994/807)
IV size: 8 bytes
replay detection support: Y


inbound ah sas:


inbound pcp sas:


outbound esp sas:
spi: 0xa8c54ec8(2831503048)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
slot: 0, conn id: 2, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (99999/807)
IV size: 8 bytes
replay detection support: Y


outbound ah sas:


outbound pcp sas:
```

- **show vpdn tunnel** — 顯示有關虛擬專用撥接網路(VPDN)中作用中L2TP或2級轉送(L2F)通道的資訊。

```
L2TP Tunnel Information (Total tunnels=1 sessions=1)

Tunnel id 4 is up, remote id is 19, 1 active sessions
Tunnel state is established, time since change 96 secs
Remote Internet Address 171.68.9.149, port 1701
Local Internet Address 171.68.9.57, port 1701
15 packets sent, 38 received, 420 bytes sent, 3758 received
Control Ns 3, Nr 5
Local RWS 16, Remote RWS 8
Retransmission time 1, max 1 seconds
Unsent queuesize 0, max 0
Resend queuesize 0, max 1
Total resends 0, ZLB ACKs 3
Retransmit time distribution: 0 0 0 0 0 0 0 0 0


% No active PPTP tunnels

PIX-506-2# sh uauth
Current Most Seen
Authenticated Users 1 2
Authen In Progress 0 2
vpdn user 'vpnclient' at 50.1.1.1, authenticated
```

- **show vpdn session** — 顯示有關VPDN中活動L2TP或L2F會話的資訊。

```
L2TP Session Information (Total tunnels=1 sessions=1)
```

```
Call id 4 is up on tunnel id 4
Remote tunnel name is zaahmed-pc
Internet Address is 171.68.9.149
Session username is vpnclient, state is established
Time since change 201 secs, interface outside
Remote call id is 1
PPP interface id is 1
15 packets sent, 56 received, 420 bytes sent, 5702 received
Sequencing is off
```

- **show vpdn pppinterface** — 顯示為PPTP隧道建立的PPP虛擬介面的狀態和統計資訊，該虛擬介面用於顯示來自**show vpdn session命令的介面標識**值。

```
PPP virtual interface id = 1
PPP authentication protocol is CHAP
Client ip address is 50.1.1.1
Transmitted Pkts: 15, Received Pkts: 56, Error Pkts: 0
MPPE key strength is None
MPPE_Encrypt_Pkts: 0, MPPE_Encrypt_Bytes: 0
MPPE_Decrypt_Pkts: 0, MPPE_Decrypt_Bytes: 0
Rcvd_Out_Of_Seq_MPPE_Pkts: 0
```

- **show uauth** — 顯示當前使用者身份驗證和授權資訊。

```
Current Most Seen
Authenticated Users 1 2
Authen In Progress 0 2
vpdn user 'vpnclient' at 50.1.1.1, authenticated
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

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。

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

- **debug crypto ipsec** — 顯示IPsec事件。
- **debug crypto isakmp** — 顯示有關IKE事件的消息。
- **debug crypto engine** — 顯示有關執行加密和解密的加密引擎的調試消息。
- **debug ppp io** — 顯示PPTP PPP虛擬介面的資料包資訊。
- **debug crypto ca** — 顯示與CA交換的調試消息。
- **debug ppp error** — 顯示與PPP連線協商和操作相關的協定錯誤和錯誤統計資訊。
- **debug vpdn error** — 顯示阻止PPP隧道建立的錯誤或導致已建立的隧道關閉的錯誤。
- **debug vpdn packet** — 顯示L2TP錯誤和事件，這些錯誤和事件是VPDN正常隧道建立或關閉的一部分。
- **debug vpdn event** — 顯示有關屬於正常PPP隧道建立或關閉的事件的消息。
- **debug ppp uauth** — 顯示PPTP PPP虛擬介面AAA使用者身份驗證調試消息。

調試輸出示例

這是PIX防火牆上良好調試的一個示例。

```
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
ISAKMP: Created a peer node for 171.68.9.149
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth RSA sig
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x0 0xe 0x10
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a MSWIN2K client

ISAKMP (0): SA is doing RSA signature authentication using id type ID_FQDN
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

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

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing CERT payload. message ID = 0
ISAKMP (0): processing a CT_X509_SIGNATURE cert
CRYPTO_PKI: status = 0: crl check ignored
PKI: key process suspended and continued
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL

CRYPTO_PKI: cert revocation status unknown.
ISAKMP (0): cert approved with warning
ISAKMP (0): processing SIG payload. message ID = 0
ISAKMP (0): processing CERT_REQ payload. message ID = 0
ISAKMP (0): peer wants a CT_X509_SIGNATURE cert
ISAKMP (0): SA has been authenticated


ISAKMP (0): ID payload
next-payload : 6
type : 2
protocol : 17
port : 500
length : 23
ISAKMP (0): Total payload length: 27
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3800855889

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: SA life type in seconds
```

```
ISAKMP: SA life duration (VPI) of 0x0 0x0 0x3 0x84
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x1 0x86 0xa0
ISAKMP: encaps is 2
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 171.68.9.57, src= 171.68.9.149,
dest_proxy= 171.68.9.57/255.255.255.255/17/1701 (type=1),
src_proxy= 171.68.9.149/255.255.255.255/17/1701 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

ISAKMP (0): processing NONCE payload. message ID = 3800855889

ISAKMP (0): processing ID payload. message ID = 3800855889
ISAKMP (0): ID_IPV4_ADDR src 171.68.9.149 prot 17 port 1701
ISAKMP (0): processing ID payload. message ID = 3800855889
ISAKMP (0): ID_IPV4_ADDR dst 171.68.9.57 prot 17 port 1701IPSEC(key_engine):
got a queue event...
IPSEC(spi_response): getting spi 0xfbc9db43(4224310083) for SA
from 171.68.9.149 to 171.68.9.57 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 171.68.9.149, dest 171.68.9.57
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
inbound SA from 171.68.9.149 to 171.68.9.57 (proxy 171.68.9.149 to 171.68.9.57)
has spi 4224310083 and conn_id 1 and flags 0
lifetime of 900 seconds
lifetime of 100000 kilobytes
outbound SA from 171.68.9.57 to 171.68.9.149 (proxy 171.68.9.57 to 171.68.9.149)
has spi 2831503048 and conn_id 2 and flags 0
lifetime of 900 seconds
lifetime of 100000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 171.68.9.57, src= 171.68.9.149,
dest_proxy= 171.68.9.57/0.0.0.0/17/1701 (type=1),
src_proxy= 171.68.9.149/0.0.0.0/17/1701 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 900s and 100000kb,
spi= 0xfbc9db43(4224310083), conn_id= 1, keysize= 0, flags= 0x0
IPSEC(initialize_sas): ,
(key eng. msg.) src= 171.68.9.57, dest= 171.68.9.149,
src_proxy= 171.68.9.57/0.0.0.0/17/1701 (type=1),
dest_proxy= 171.68.9.149/0.0.0.0/17/1701 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 900s and 100000kb,
spi= 0xa8c54ec8(2831503048), conn_id= 2, keysize= 0, flags= 0x0

return status is IKMP_NO_ERROR
```

show log

```
603102: PPP virtual interface 1 - user: vpnclient aaa authentication started
603103: PPP virtual interface 1 - user: vpnclient aaa authentication succeed
109011: Authen Session Start: user 'vpnclient', sid 0
603106: L2TP Tunnel created, tunnel_id is 1, remote_peer_ip is 171.68.9.149
ppp_virtual_interface_id is 1, client_dynamic_ip is 50.1.1.1
username is vpnclient
```

使用CA註冊的正確調試

```
CI thread sleeps!
Crypto CA thread wakes up!%
% Start certificate enrollment ..

% The subject name in the certificate will be: PIX-506-2.sjvpn.com


CI thread wakes up!% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.

PIX-506-2(config)#
PIX-506-2(config)#     Fingerprint:  d8475977 7198ef1f 17086f56 9e3f7a89

CRYPTO_PKI: transaction PKCSReq completed
CRYPTO_PKI: status:
Crypto CA thread sleeps!
PKI: key process suspended and continued
CRYPTO_PKI: http connection opened
CRYPTO_PKI:  received msg of 711 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL

CRYPTO_PKI: signed attr: pki-message-type:
13 01 33
CRYPTO_PKI: signed attr: pki-status:
13 01 33
CRYPTO_PKI: signed attr: pki-recipient-nonce:
04 10 70 0d 4e e8 03 09 71 4e c8 24 7a 2b 03 70 55 97
CRYPTO_PKI: signed attr: pki-transaction-id:
13 20 65 66 31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38
38 35 61 36 30 65 32 35 31 31 34 66 62 37
CRYPTO_PKI: status = 102: certificate request pending
CRYPTO_PKI: http connection opened
CRYPTO_PKI:  received msg of 711 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found
while selecting CRL
CRYPTO_PKI: signed attr: pki-message-type:
13 01 33
CRYPTO_PKI: signed attr: pki-status:
13 01 33
CRYPTO_PKI: signed attr: pki-recipient-nonce:
04 10 c8 9f 97 4d 88 24 92 a5 3b ba 9e bc d6 7c 75 57
CRYPTO_PKI: signed attr: pki-transaction-id:
13 20 65 66 31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38
38 35 61 36 30 65 32 35 31 31 34 66 62 37
CRYPTO_PKI: status = 102: certificate request pending
!--- After approval from CA. Crypto CA thread wakes up! CRYPTO_PKI: resend GetCertInitial, 1
Crypto CA thread sleeps! CRYPTO_PKI: resend GetCertInitial for session: 0 CRYPTO_PKI: http
connection opened The certificate has been granted by CA! CRYPTO_PKI: received msg of 1990 bytes
CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while selecting CRL PKI: key
process suspended and continued CRYPTO_PKI: signed attr: pki-message-type: 13 01 33 CRYPTO_PKI:
signed attr: pki-status: 13 01 30 CRYPTO_PKI: signed attr: pki-recipient-nonce: 04 10 c8 9f 97
4d 88 24 92 a5 3b ba 9e bc d6 7c 75 57 CRYPTO_PKI: signed attr: pki-transaction-id: 13 20 65 66
31 32 32 31 30 33 31 37 30 61 30 38 65 32 33 38 38 35 61 36 30 65 32 35 31 31 34 66 62 37
CRYPTO_PKI: status = 100: certificate is granted CRYPTO_PKI: WARNING: Certificate, private key
or CRL was not found while selecting CRL CRYPTO_PKI: All enrollment requests completed.
CRYPTO_PKI: All enrollment requests completed. CRYPTO_PKI: WARNING: Certificate, private key or
CRL was not found while selecting CRL
```

使用CA註冊的調試錯誤

在本例中，**ca identity**命令中使用的URL語法不正確：

```
CI thread sleeps!
Crypto CA thread wakes up!
CRYPTO_PKI: http connection opened
msgsym(GETCARACERT, CRYPTO)!
%Error in connection to Certificate Authority: status = FAIL
CRYPTO_PKI: status = 266: failed to verify
CRYPTO_PKI: transaction GetCACert completed
Crypto CA thread sleeps!
```

如果將註冊模式指定為CA而不是RA，則會收到以下調試：

```
CI thread sleeps!
Crypto CA thread wakes up!
CRYPTO_PKI: http connection opened
Certificate has the following attributes:

Fingerprint: 49dc7b2a cd5fc573 6c774840 e58cf178

CRYPTO_PKI: transaction GetCACert completed
CRYPTO_PKI: Error:  Invalid format for BER encoding while

CRYPTO_PKI: can not set ca cert object.
CRYPTO_PKI: status = 65535: failed to process RA certiifcate
Crypto CA thread sleeps!
```

在本示例中，缺少**mode transport**命令：

```
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x0 0x70 0x80
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      encaps is 2
ISAKMP:      authenticator is HMAC-MD5IPSEC(validate_proposal):
invalid transform proposal flags -- 0x0
```

在此輸出中，缺少**crypto map mymap 10 ipsec-isakmp dynamic dyna**命令，並且調試中可能會出現以下消息：

```
no IPSEC cryptomap exists for local address a.b.c.d
```

相關資訊

- RADIUS技術支援頁面
- PIX命令參考
- PIX支援頁
- IPsec協商/IKE通訊協定支援頁面
- 要求建議 (RFC)