使用证书在 PIX 防火墙与 Windows 2000 PC 之间配置 IPSec 上的 L2TP

目录

简介

Cisco Secure PIX 防火墙软件版本 6.x 或更高版本支持第二层隧道协议 (L2TP) over IPsec。运行 Windows 2000 的用户可以使用本地 IPSec 客户端和 L2TP 客户端，以建立连接到 PIX 防火墙的 L2TP 隧道。数据流将通过已由 IPSec 安全关联 (SA) 进行加密的 L2TP 隧道。

注意：不能使用Windows 2000 L2TP IPsec客户端以Telnet至PIX。

注意：拆分隧道在PIX上不适用于L2TP。

要使用预共享密钥将L2TP over IPsec从远程Microsoft Windows 2000/2003和XP客户端配置到PIX/ASA安全设备公司办公室，并使用Microsoft Windows 2003 Internet身份验证服务(IAS)RADIUS服务器进行用户身份验证，请参阅使用预共享密钥配置示例，在Windows 2000/XP PC和PIX/ASA 7.2之间使用IPsec的L2TP。

要使用加密方法配置从远程 Microsoft Windows 2000 和 XP 客户端到企业站点的 L2TP over IP Security (IPsec)，请参阅使用预共享密钥配置从 Windows 2000 或 XP 客户端到 Cisco VPN 3000 系列集中器的 L2TP over IPsec。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息适用于以下软件和硬件版本：

- PIX 软件版本 6.3(3)
- 带或不带SP2的Windows 2000(有关SP1的信息，请参阅Microsoft 提示Q276360。)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

Cisco Secure PIX 版本 6.x 或更高版本中的证书支持包括 Baltimore、Microsoft、VeriSign 和 Entrust 服务器。目前，PIX 不接受不具有 IPSec 保护的 L2TP 请求。

本示例说明如何针对本文档前面提及的情形配置 PIX 防火墙。互联网密钥交换(IKE)身份验证使用**rsa-sig**命令（证书）。 在本示例中，身份验证由 RADIUS 服务器完成。

支持 IPSec/PPTP/L2TP 的 Cisco 硬件和 VPN 客户端中列出了与 PIX 的加密客户端连接中较少涉及的选项。

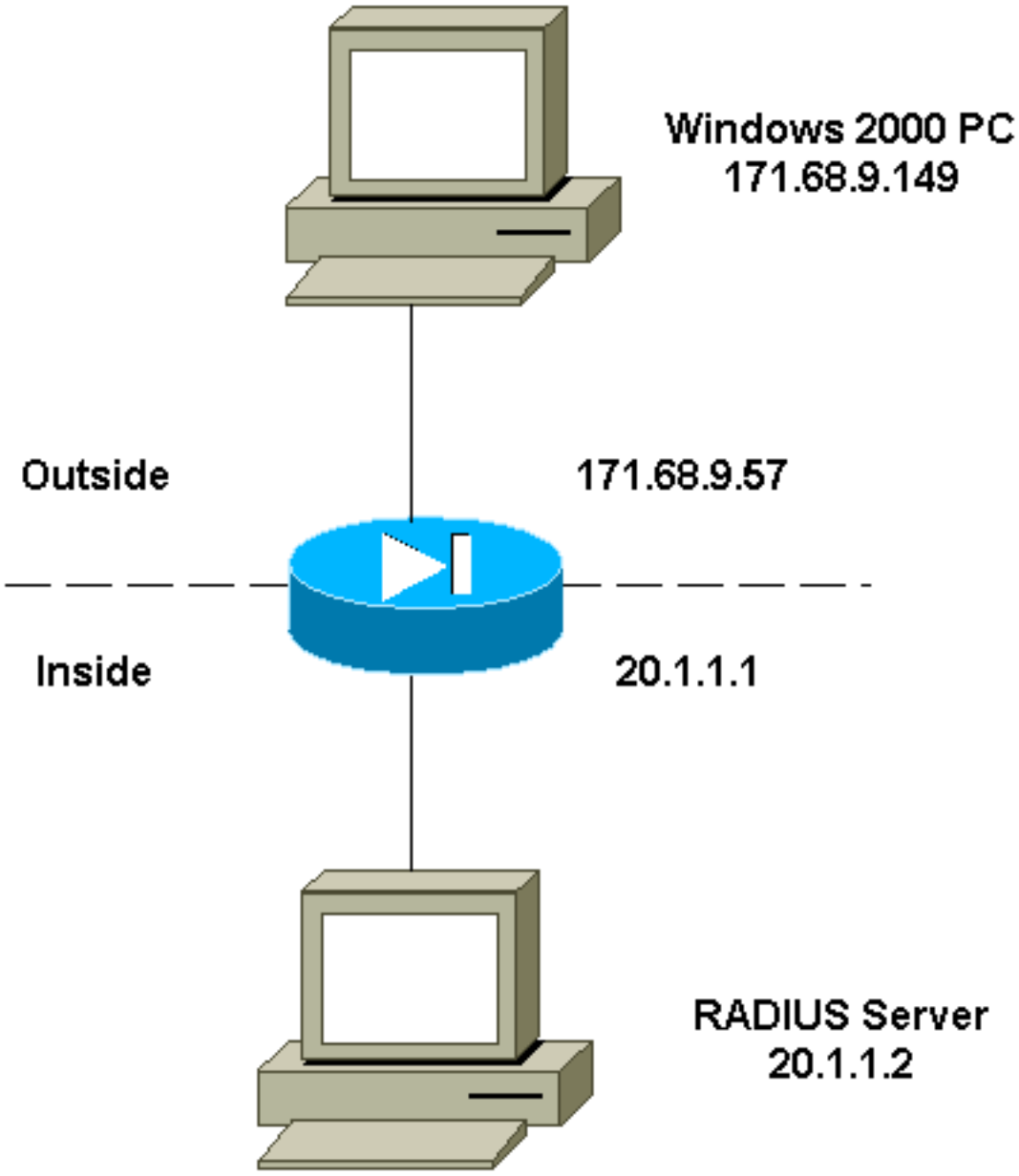
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：使用命令查找工具(仅限注册客户)可查找有关本文档中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置 Microsoft L2TP 客户端

有关如何配置 Microsoft L2TP 客户端的信息，可在 Microsoft 分步指南：Internet 协议安全 中找到。

如Microsoft提供的参考分步指南中所述，客户端支持多个经过测试的证书颁发机构(CA)服务器。有关如何设置 Microsoft CA 的信息，可在 Microsoft 分步指南：设置证书颁发机构 中找到。

获得 PIX 防火墙的证书

有关如何配置 PIX 以实现与 VeriSign、Entrust、Baltimore 和 Microsoft 等证书的互操作性的详细信息，请参阅 CA 配置示例。

PIX 防火墙配置

本文档使用以下配置。

PIX 防火墙

```
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]
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ca cert** — 显示有关证书、CA证书和任何注册机构(RA)证书的信息。

```
Certificate
Status: Available
Certificate Serial Number: 03716308000000000022
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 - 显示对等体上的所有当前 IKE SA。**

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

- **show crypto ipsec sa - 显示当前 SA 使用的设置。**

```
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** — 显示有关虚拟专用拨号网络(VPDN)中活动L2TP或2级转发(L2F)隧道的信息。

```
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 - 显示有关 VPDN 中活动 L2TP 或 L2F 会话的信息。**

```
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 - 显示针对 show vpdn session 命令的接口标识值为 PPTP 隧道创建的 PPP 虚拟接口的状态和统计数据。**

```
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 - 显示当前用户身份验证和授权信息。**

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

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

- **debug crypto ipsec — 显示 IPSec 事件。**
- **debug crypto isakmp — 显示关于 IKE 事件的消息。**
- **debug crypto engine - 显示有关执行加密和解密的加密引擎的 debug 消息。**
- **debug ppp io—显示 PPTP PPP 虚拟接口的数据包信息。**
- **debug crypto ca - 显示与 CA 交换的 debug 消息。**
- **debug ppp error - 显示与 PPP 连接协商和操作关联的协议错误和错误统计数据。**
- **debug vpdn error - 显示导致无法建立 PPP 隧道的错误或导致已建立的隧道关闭的错误。**
- **debug vpdn packet - 显示作为 VPDN 的正常隧道建立或关闭一部分的 L2TP 错误和事件。**
- **debug vpdn event - 显示作为正常 PPP 隧道建立或关闭一部分的事件的相关消息。**
- **debug ppp uauth—显示 PPTP PPP 虚拟接口 AAA 用户身份验证调试消息。**

调试输出示例

以下是在 PIX 防火墙上成功执行 debug 的示例。

```
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
```

登记 CA 调试成功

```
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

登记 CA 错误调试

在本示例中，**ca identity 命令中使用了不正确的 URL 语法：**

```
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!
```

如果将注册模式指定为 CA 而不是 RA，将会显示以下 debug：

```
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
```

在该输出中，缺少 crypto map mymap 10 ipsec-isakmp dynamic dyna 命令，并且 debug 中会显示以下消息：

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

相关信息

- RADIUS 技术支持页
- PIX 命令参考
- PIX 支持页
- IPsec 协商/IKE 协议支持页
- 请求注解 (RFC)