

# 認証を使用するPIX Firewall および Windows 2000 マシン間の L2TP Over IPsec 設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[Microsoft L2TP クライアントの設定](#)

[PIX ファイアウォールの証明書の取得](#)

[PIX ファイアウォールの設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[debug 出力例](#)

[CA での登録の正常なデバッグ](#)

[CA での登録に関する正常でないデバッグ](#)

[関連情報](#)

## 概要

Layer 2 Tunneling Protocol ( L2TP ) over IPsec は、Cisco Secure PIX ファイアウォール ソフトウェア リリース 6.x 以降でサポートされています。Windows 2000 が稼働しているユーザでは、ネイティブの IPsec クライアントと L2TP クライアントを使用して、PIX ファイアウォールへの L2TP トンネルを確立できます。トラフィックは IPsec Security Association ( SA; セキュリティアソシエーション ) によって暗号化されて L2TP トンネルを流れます。

注 : Windows 2000 L2TP IPsecクライアントを使用してPIXにTelnet接続することはできません。

注 : スプリットトンネリングは、PIXのL2TPでは使用できません。

ユーザ認証に Microsoft Windows 2003 Internet Authentication Service ( IAS ) RADIUS サーバと事前共有キーを使用して、リモートの Microsoft Windows 2000/2003 および XP のクライアントから PIX/ASA セキュリティ アプライアンス企業オフィスへの L2TP over IPsec を設定するには、『[事前共有キーを使用した Windows 2000/XP PC と PIX/ASA 7.2 の間の L2TP Over IPsec 設定例](#)』を参照してください。

暗号化方式を使用して、リモートの Microsoft Windows 2000 および XP のクライアントから企業

サイトへの L2TP over IPsec を設定するには、『[Windows 2000 または XP のクライアントから Cisco VPN 3000 シリーズ コンセントレータへの事前共有キーを使用する L2TP over IPsec の設定](#)』を参照してください。

## [前提条件](#)

### [要件](#)

このドキュメントに特有の要件はありません。

### [使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに適用されます。

- PIX ソフトウェア リリース 6.3(3)
- Windows 2000 ( SP2 がインストールされている場合とインストールされていない場合 ) ( SP1 に関する情報は、[Microsoft のヒント Q276360](#) を参照してください )。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

### [表記法](#)

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## [背景説明](#)

Cisco Secure PIX バージョン 6.x 以降では、Baltimore、Microsoft、VeriSign、および Entrust サーバの証明書がサポートされています。現在 PIX では、IPsec で保護されていない L2TP 要求は許可されません。

この例では、前述のシナリオを実現するための PIX ファイアウォールの設定方法を示します。Internet Key Exchange ( IKE; インターネット キー エクスチェンジ ) 認証には rsa-sig コマンドを使用します ( 証明書 )。RADIUS サーバによって認証が行われます。

PIX に対する暗号化クライアント接続にあまり関係しないオプションについては、『[IPsec/PPTP/L2TP をサポートするシスコハードウェアと VPN クライアント](#)』を参照してください。

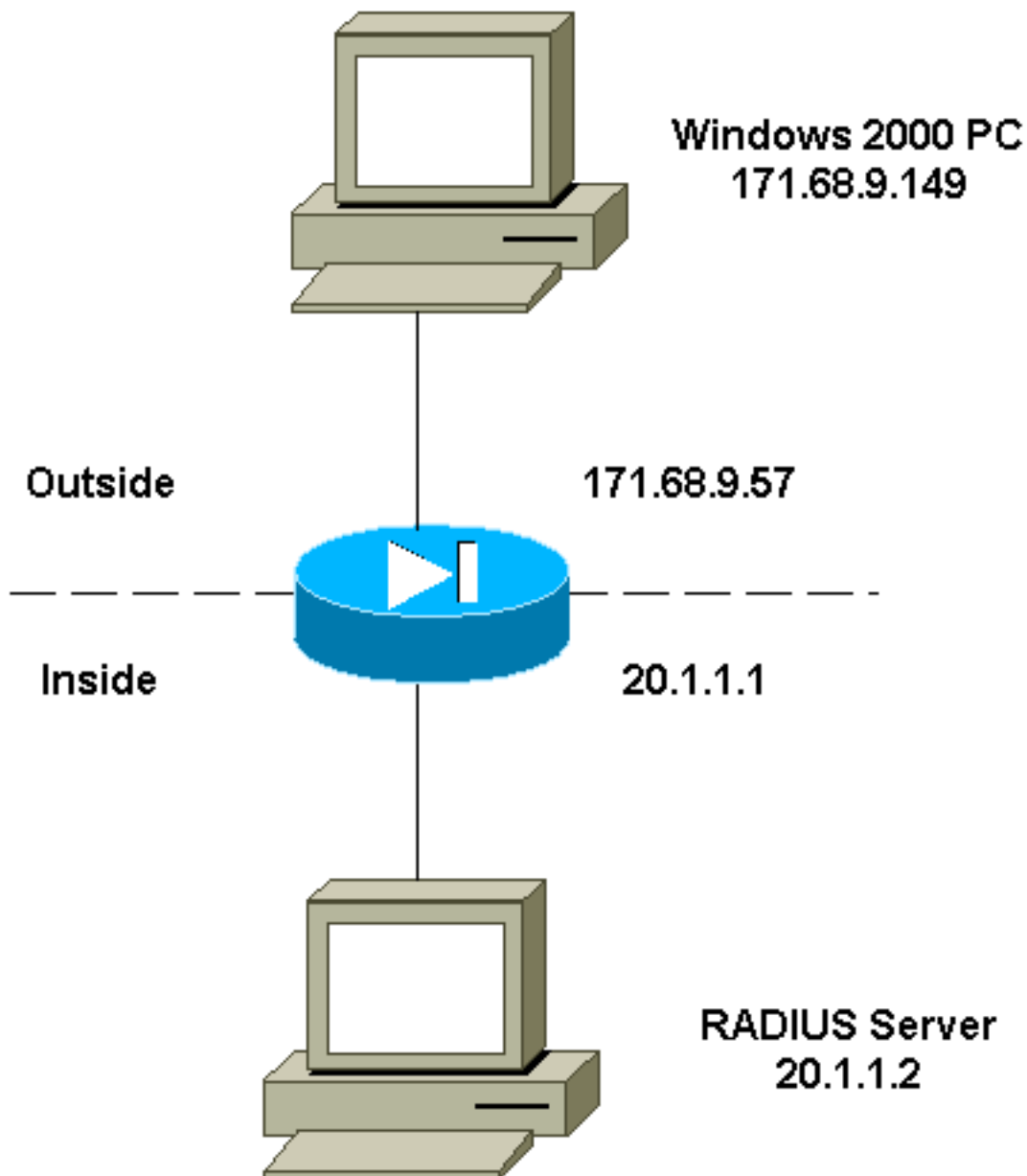
## [設定](#)

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

## ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



## Microsoft L2TP クライアントの設定

Microsoft L2TP クライアントの設定方法の詳細については、『Step-by-Step Guide to Internet Protocol Security』を参照してください。

このドキュメントに記されているとおり、このクライアントでは多数のテスト済み Certificate Authority ( CA; 認証局 ) サーバがサポートされています。Microsoft CA の設定方法の詳細については、『Step-by-Step Guide to Setting up a Certificate Authority』を参照してください。

## PIX ファイアウォールの証明書の取得

VeriSign、Entrust、Baltimore、および Microsoft の証明書との相互運用性を実現する PIX の設定方法については、『[CA のコンフィギュレーション例](#)』を参照してください。

## PIX ファイアウォールの設定

このドキュメントでは次の設定を使用します。

### PIX ファイアウォール

```
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]
```

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \( 登録ユーザ専用 \) \( OIT \)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show crypto ca cert** : 証明書、CAの証明書、および登録局(RA)証明書に関する情報を表示します。

```
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: 0347df0d0000000000003  
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** : 現在ピアにあるすべての IKE SA を表示します。

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

- **show crypto ipsec sa** : 現在の SA で使用されている設定を表示します。

```
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** : 仮想プライベートダイヤルアップネットワーク(VPDN)内のアクティブなL2TPまたはLevel 2 Forwarding(L2F)トンネルに関する情報を表示します。

```
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:**VPDN内のアクティブなL2TPまたはL2Fセッションに関する情報を表示します。

```
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:**show vpdn sessionコマンドのインターフェイス識別値に関して、PPTPトンネル用に作成されたPPP仮想インターフェイスのステータスと統計情報を表示します。

```
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 :**現在のユーザの認証および許可情報を表示します。

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

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

### トラブルシューティングのためのコマンド

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#)は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注 : [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- **debug crypto ipsec :**IPsec イベントを表示します。
- **debug crypto isakmp :**IKE イベントに関するメッセージを表示します。
- **debug crypto engine :**暗号化と復号化を行う暗号化エンジンに関するデバッグ メッセージを表示します。
- **debug ppp io:**PPTP PPP仮想インターフェイスの packets 情報を表示します。
- **debug crypto ca:**CAと交換されたデバッグメッセージを表示します。
- **debug ppp error :**PPP 接続のネゴシエーションと操作に関するプロトコル エラーとエラー



統計情報を表示します。

- **debug vpdn errors** : PPP トンネルの確立を阻害するエラー、または確立されたトンネルをクローズする原因になるエラーを表示します。
- **debug vpdn packet**:VPDNの通常のトンネル確立またはシャットダウンの一部であるL2TPエラーとイベントを表示します。
- **debug vpdn event** : 通常のPPPトンネル確立またはシャットダウンの一部であるイベントに関するメッセージを表示します。
- **debug ppp uauth**:PPTP PPP仮想インターフェイスAAAユーザ認証デバッグメッセージを表示します。

## debug 出力例

PIX ファイアウォールの正常な状態のデバッグ例を示します。

```
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
```

## CAでの登録の正常なデバッグ

```
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
```

## CA での登録に関する正常でないデバッグ

この例では、ca identity コマンドで誤った URL 構文が使用されています。

```
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!
```

登録モードに RA ではなく CA が指定されたため、デバッグ結果が次のようになりました。

```
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 certificate
Crypto CA thread sleeps!
```

この例では、mode transport コマンドがありません。

```
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
```

この例では、crypto map mymap 10 ipsec-isakmp dynamic dyna コマンドがないために、デバッグで次のようなメッセージが表示されています。

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

## 関連情報

- [RADIUS に関するサポート ページ](#)
- [PIX コマンド リファレンス](#)
- [PIX に関するサポート ページ](#)
- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [Requests for Comments \(RFCs\)](#)