

Configuring L2TP Over IPsec Between PIX Firewall and Windows 2000 PC Using Certificates

Document ID: 4676

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Network Diagram
- Configure the Microsoft L2TP Client
- Get Certificates for the PIX Firewall
- PIX Firewall Configuration

Verify

Troubleshoot

- Troubleshooting Commands
- Sample Debug Output
- Good Debug for Enrolling with CA
- Bad Debug for Enrolling with CA

Related Information

Introduction

Layer 2 Tunneling Protocol (L2TP) over IPsec is supported on Cisco Secure PIX Firewall Software Release 6.x or later. Users that run Windows 2000 can use the native IPsec client and L2TP client in order to establish an L2TP tunnel to the PIX Firewall. The traffic flows through the L2TP tunnel encrypted by IPsec Security Associations (SAs).

Note: You cannot use the Windows 2000 L2TP IPsec client in order to Telnet to the PIX.

Note: Split Tunneling is not available with L2TP on the PIX.

In order to configure L2TP over IPsec from remote Microsoft Windows 2000/2003 and XP clients to a PIX/ASA Security Appliance corporate office using pre-shared keys with a Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server for user authentication, refer to L2TP Over IPsec Between Windows 2000/XP PC and PIX/ASA 7.2 Using Pre-shared Key Configuration Example.

In order to configure L2TP over IP Security (IPsec) from remote Microsoft Windows 2000 and XP clients to a corporate site using an encrypted method, refer to Configuring L2TP over IPsec from a Windows 2000 or XP Client to a Cisco VPN 3000 Series Concentrator Using Pre-Shared Keys.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document applies to these software and hardware versions:

- PIX Software Release 6.3(3)
- Windows 2000 with or without SP2 (See Microsoft tip Q276360 for information on SP1.)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Certificate support in Cisco Secure PIX versions 6.x or later includes Baltimore, Microsoft, VeriSign, and Entrust servers. Currently, PIX does not accept L2TP requests without IPsec protection.

This example shows how to configure the PIX Firewall for the scenario mentioned earlier in this document. The Internet Key Exchange (IKE) authentication uses the **rsa-sig** command (certificates). In this example, authentication is done by a RADIUS server.

Less involved options for encrypted client connections to the PIX are listed at Cisco Hardware and VPN Clients Supporting IPsec/PPTP/L2TP.

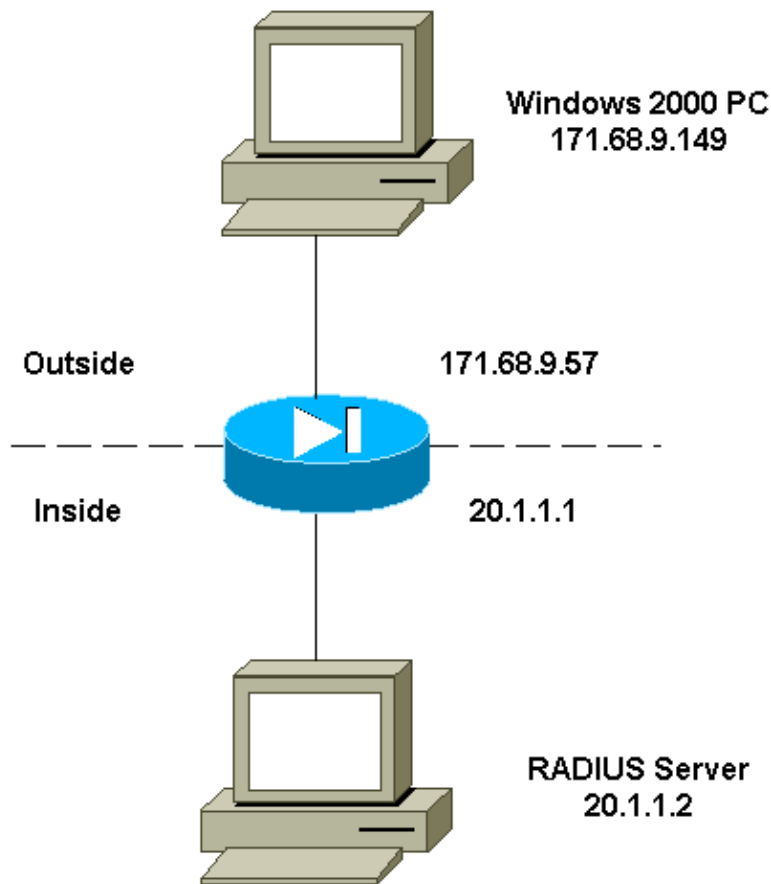
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configure the Microsoft L2TP Client

Information on how to configure the Microsoft L2TP client is found in Microsoft's Step-by-Step Guide to Internet Protocol Security .

As noted in the referenced step-by-step guide from Microsoft, the client supports a number of tested certificate authority (CA) servers. Information on how to set up the Microsoft CA is found in Microsoft's Step-by-Step Guide to Setting up a Certificate Authority .

Get Certificates for the PIX Firewall

Refer to CA Configuration Examples for details on how to configure PIX for interoperability with certificates from VeriSign, Entrust, Baltimore, and Microsoft.

PIX Firewall Configuration

This document uses this configuration.

PIX Firewall
<pre>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</pre>

```
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]

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto ca cert** Displays information about your certificate, the certificate of the CA, and any Registration Authority (RA) certificates.

```

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** Displays all current IKE SAs at a peer.

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

- **show crypto ipsec sa** Displays the settings used by current SAs.

```
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={reassemble_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** Displays information about active L2TP or Level 2 Forwarding (L2F) tunnels in a virtual private dialup network (VPDN).

```
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 queue size 0, max 0
Resend queue size 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 'vpncclient' at 50.1.1.1, authenticated
```

- **show vpdn session** Displays information about active L2TP or L2F sessions in a VPDN.

```
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** Displays the status and statistics of the PPP virtual interface that was created for the PPTP tunnel for the interface identification value from the **show vpdn session** command.

```
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** Displays current user authentication and authorization information.

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

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Displays IPsec events.
- **debug crypto isakmp** Displays messages about IKE events.
- **debug crypto engine** Displays debug messages about crypto engines, which perform encryption and decryption.
- **debug ppp io** Displays the packet information for the PPTP PPP virtual interface.
- **debug crypto ca** Displays debug messages exchanged with the CA.
- **debug ppp error** Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
- **debug vpdn error** Displays errors that prevent a PPP tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn packet** Displays L2TP errors and events that are a part of normal tunnel establishment or shutdown for VPDNs.
- **debug vpdn event** Displays messages about events that are part of normal PPP tunnel establishment or shutdown.
- **debug ppp uauth** Displays the PPTP PPP virtual interface AAA user authentication debugging messages.

Sample Debug Output

This is a sample of a good debug on the PIX Firewall.

```
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
```

Good Debug for Enrolling with CA

```
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

```

Bad Debug for Enrolling with CA

In this example, the incorrect URL syntax was used in the **ca identity** command:

```

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!

```

If the enrollment mode was specified as CA instead of as RA, then you get this 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 certifiicate
Crypto CA thread sleeps!

```

In this example, the **mode transport** command is missing:

```

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

```

In this output, the **crypto map mymap 10 ipsec-isakmp dynamic dyna** command is missing, and this message can appear in the debug:

```

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

```

Related Information

- [RADIUS Technology Support Pages](#)
 - [PIX Command Reference](#)
 - [Documentation for PIX Firewall](#)
 - [PIX Support Page](#)
 - [IPsec Negotiation/IKE Protocols Support Page](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 23, 2009

Document ID: 4676
