

# 使用ISAKMP配置檔案對中心路由器進行VPN客戶端訪問的PIX上的LAN到LAN和EzVPN客戶端配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[VPN客戶端配置](#)

[驗證](#)

[使用debug crypto isakmp和debug crypto ipsec在VPN 1750集線器路由器上進行LAN到LAN調試](#)

[EzVPN客戶端連線使用調試加密isakmp和調試加密ipsec進行調試](#)

[使用debug crypto isakmp和debug crypto ipsec的PIX端上的VPN客戶端調試](#)

[PIX 501 \( LAN到LAN連線 \) 上的調試](#)

[PIX-506-B \( EzVPN客戶端連線 \) 上的調試](#)

[VPN客戶端上的調試](#)

[疑難排解](#)

[疑難排解指令](#)

[相關資訊](#)

## 簡介

本文檔提供在帶有兩個PIX遠端站點的集線器路由器上使用ISAKMP配置檔案配置IPsec隧道的配置示例。一個PIX遠端站點由LAN到LAN組成，另一個由EzVPN遠端訪問模式配置組成。中心路由器配置用於EzVPN通道的本地身份驗證，以及軟體VPN客戶端的RADIUS身份驗證。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行6.3(3)的Cisco安全PIX防火牆裝置501
- 執行Cisco IOS®軟體版本12.3.9a的Cisco路由器1750
- 運行6.3(3)的Cisco安全PIX防火牆裝置506
- 執行4.0的Cisco VPN使用者端(Rel) ( 使用RADIUS伺服器的使用者驗證 )

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。

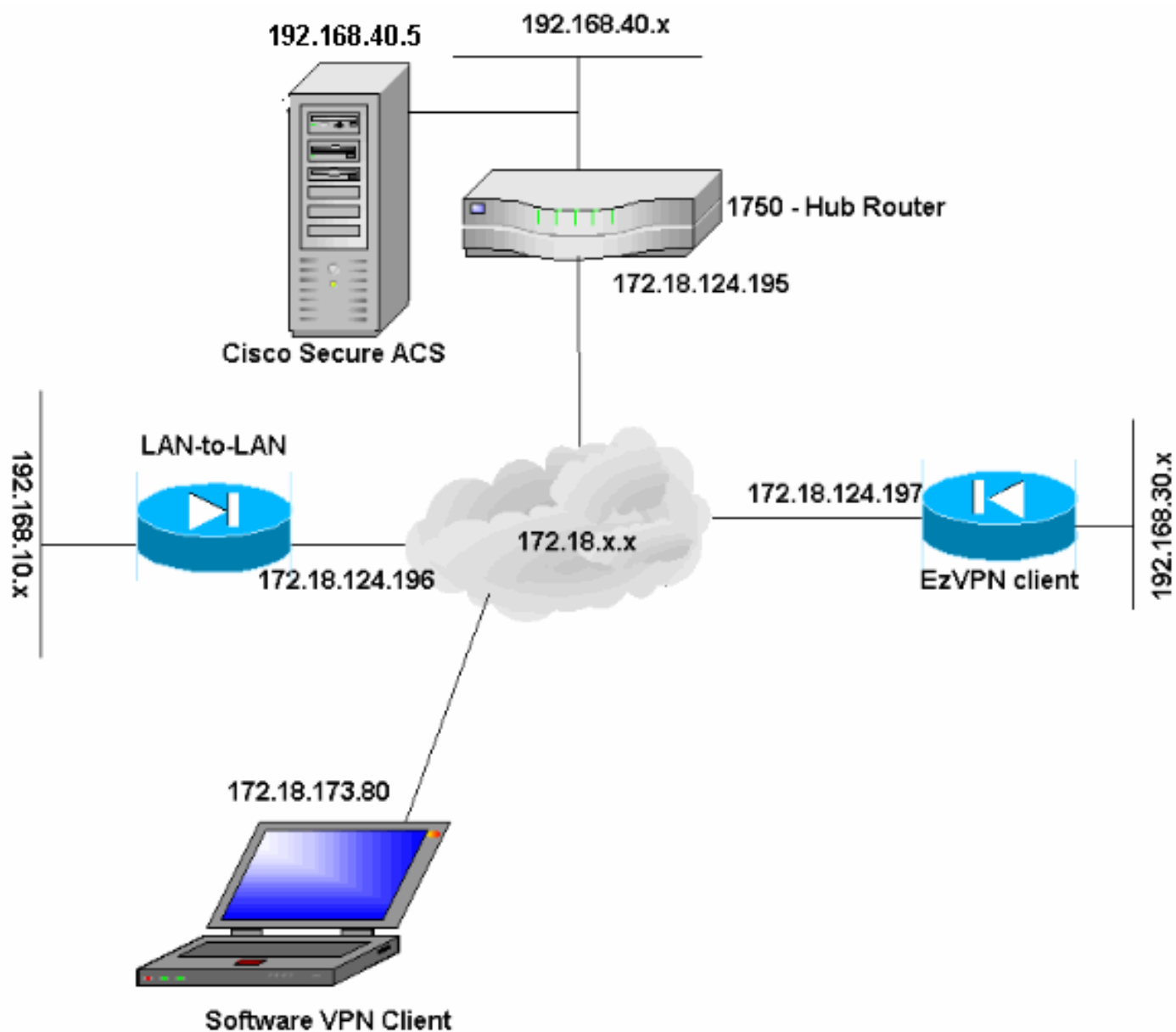
## [設定](#)

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)查詢有關本文檔中使用的命令的其他資訊。

## [網路圖表](#)

本檔案會使用以下網路設定：



## 組態

本檔案會使用以下設定：

- [VPN 1750集線器路由器](#)
- [PIX-501 - LAN到LAN](#)
- [PIX-506-B - EzVPN客戶端](#)
- [VPN使用者端](#)

### VPN 1750集線器路由器

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN1750
!--- Local authentication username and password, for

```

```
EzVPN Client. username jerry password 0 wells123
username cisco password 0 letmein
!--- Enable AAA. aaa new-model
!
!

!--- Default local login. aaa authentication login
default local

!--- RADIUS authentication for VPN Client. aaa
authentication login userauth group radius local

!--- Local authentication for EzVPN Client. aaa
authentication login EZVPN local
aaa authorization exec default local

!--- Local group authorization for VPN Client. aaa
authorization network groupauthor local

!--- Local authorization for EzVPN Client. aaa
authorization network EZVPN local
aaa session-id common
ip subnet-zero
!
!
ip domain name cisco.com
!
ip cef
ip audit po max-events 100

!--- Keyring specification for Phase 1 authentication.
crypto keyring vpn
pre-shared-key address 172.18.124.196 key cisco123
!

!--- Specify ISAKMP policy. crypto isakmp policy 20
encr 3des
hash md5
authentication pre-share
group 2
!

!--- EzVPN Client configuration that specifies the
group, key and IP pool to use. crypto isakmp client
configuration group polo
key mark123
pool ezpool
!

!--- VPN Client configuration that specifies the group,
key and IP pool to use. crypto isakmp client
configuration group tennis
key matchpoint
domain cisco.com
pool vpnpool

!--- ISAKMP profile specification for LAN-to-LAN. crypto
isakmp profile l2lvpn
keyring vpn
match identity address 172.18.124.196 255.255.255.255

!--- ISAKMP profile specification for EzVPN Client.
crypto isakmp profile ezvpnprofile
match identity group polo
```

```
client authentication list EZVPN
isakmp authorization list EZVPN
client configuration address respond

!--- ISAKMP profile specification for software VPN
Client. crypto isakmp profile softclient
match identity group tennis
client authentication list userauth
isakmp authorization list groupauthor
client configuration address respond
!
!

!--- Set transform-set. crypto ipsec transform-set pix501
esp-3des esp-sha-hmac
crypto ipsec transform-set vpnclient esp-3des esp-sha-
hmac
crypto ipsec transform-set ezvpn esp-3des esp-md5-hmac
!

!--- Specify crypto map set and ISAKMP profile for VPN
Client. crypto dynamic-map rtpmap 10
set transform-set vpnclient
set isakmp-profile softclient

!--- Specify crypto map set and ISAKMP profile for EzVPN
Client. crypto dynamic-map rtpmap 20
set transform-set ezvpn
set isakmp-profile ezvpnprofile
!
!
crypto map rtp 5 ipsec-isakmp dynamic rtpmap

!--- Specify crypto map set and ISAKMP profile for LAN-
to-LAN. crypto map rtp 10 ipsec-isakmp
set peer 172.18.124.196
set transform-set pix501
set isakmp-profile 121vpn
match address 101
!
!
!
interface Ethernet0
ip address 192.168.40.1 255.255.255.0
!
interface FastEthernet0
ip address 172.18.124.195 255.255.255.0
speed auto

!--- Apply crypto map on the outside interface. crypto
map rtp
!

!--- VPN Client pool addresses. ip local pool vpnpool
10.50.50.1 10.50.50.10

!--- EzVPN Client pool addresses. ip local pool ezpool
172.25.70.1 172.25.70.10
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
!

!--- Encryption access-list applied to the crypto map.
access-list 101 permit ip 192.168.40.0 0.0.0.255
```

```
192.168.10.0 0.0.0.255
!
!--- Define ACS server for VPN Client user
authentication. radius-server host 192.168.40.5 auth-
port 1645 acct-port 1646 key cisco123
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
!
end
```

## PIX-501 - LAN到LAN

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-501
domain-name cisco.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names

!--- Encryption access-list for interesting traffic to
be encrypted. access-list 101 permit ip 192.168.10.0
255.255.255.0 192.168.40.0 255.255.255.0

!--- NAT 0 access-list for encryption traffic to bypass
NAT process. access-list nonat permit ip 192.168.10.0
255.255.255.0 192.168.40.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.196 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface

!--- Bypass NAT for IPsec traffic. nat (inside) 0
access-list nonat
nat (inside) 1 192.168.10.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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-server LOCAL protocol local
floodguard enable

!--- This command avoids applied ACLs or conduits on
encrypted packets. sysopt connection permit-ipsec

!--- Configuration of IPsec Phase 2. crypto ipsec
transform-set fox esp-3des esp-sha-hmac
crypto map fox 10 ipsec-isakmp
crypto map fox 10 match address 101
crypto map fox 10 set peer 172.18.124.195
crypto map fox 10 set transform-set fox
crypto map fox interface outside

!--- Configuration of IPsec Phase 1. isakmp enable
outside

!--- IKE pre-shared key used by peers to authenticate.
isakmp key ***** address 172.18.124.195 netmask
255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:9e09996cdf390036841e71da006ba1f1
: end
```

## PIX-506-B - EzVPN客户端

```
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-506-B
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
```

```

names
pager lines 24
mtu outside 1500
mtu inside 1500

!--- Define IP addresses for the PIX's inside and
outside interfaces. ip address outside 172.18.124.197
255.255.255.0
ip address inside 192.168.30.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 192.168.30.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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-server LOCAL protocol local
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set tiger esp-3des esp-md5-hmac
telnet timeout 5
ssh timeout 5
console timeout 0

!--- Define the EzVPN server IP address. vpnclient
server 172.18.124.195

!--- Specify the mode to be used (client-mode or Network
Extension Mode). vpnclient mode client-mode

!--- Define EzVPN connection parameters. vpnclient
vpngroup polo password *****
vpnclient username jerry password *****

!--- Enable VPN Client on the PIX. vpnclient enable
terminal width 80
Cryptochecksum:1bb41de13c5e15537a50cb1f39f131b9
: end

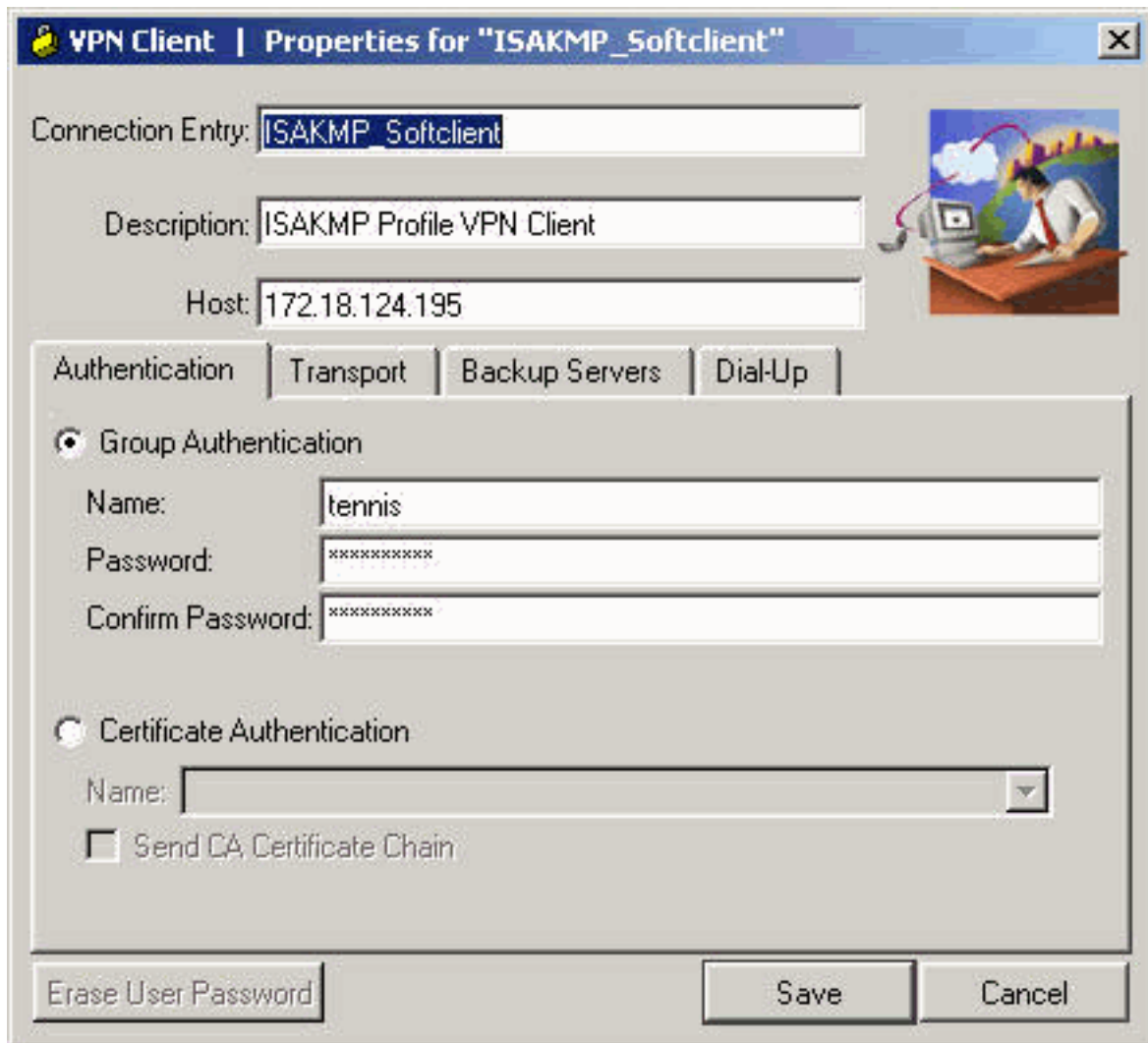
```

## VPN客戶端配置

完成以下步驟以配置VPN客戶端。

1. 啟動VPN客戶端並使用所需的連線條目引數建立新連線。





2. 建立連線專案後，按一下**Connect**，然後使用RADIUS伺服器上設定的使用者引數進行驗證。



## 驗證

本節提供的資訊可用於確認您的組態是否正常運作。請參閱[IP安全性疑難排解 — 瞭解和使用 debug 命令](#)以瞭解其他驗證/疑難排解。如果遇到任何VPN客戶端問題或錯誤，請參閱[VPN客戶端 GUI錯誤查詢工具](#)。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- **show crypto isakmp profile** — 顯示路由器上的所有ISAKMP配置檔案及其配置。
- **show crypto isakmp key** — 顯示所有金鑰環及其預共用金鑰。使用此命令驗證路由器上的加密金鑰環配置。
- **debug crypto ipsec** — 顯示路由器上IPsec SA協商的資訊。

- **debug crypto isakmp** — 顯示已構建的ISAKMP SA和協商的IPsec屬性。在ISAKMP SA協商期間，PIX可能會在某個建議被接受之前將其丟棄為「不可接受」。一旦同意ISAKMP SA，就會協商IPsec屬性。

## [使用debug crypto isakmp和debug crypto ipsec在VPN 1750集線器路由器上進行LAN到LAN調試](#)

```
May 11 20:44:51.370: ISAKMP (0:0): received packet
      from 172.18.124.196 dport 500 sport 500 Global
      (N) NEW SA
May 11 20:44:51.370: ISAKMP: local port 500, remote port 500
May 11 20:44:51.370: ISAKMP: insert sa successfully sa = 81789610
May 11 20:44:51.374: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
May 11 20:44:51.374: ISAKMP (0:1): Old State = IKE_READY New State = IKE_R_MM1

May 11 20:44:51.374: ISAKMP (0:1): processing SA payload. message ID = 0
May 11 20:44:51.374: ISAKMP: Looking for a matching key for 172.18.124.196
      in default
May 11 20:44:51.374: ISAKMP: Looking for a matching key for 172.18.124.196
      in vpn : success
May 11 20:44:51.374: ISAKMP (0:1): found peer pre-shared key matching
      172.18.124.196
May 11 20:44:51.378: ISAKMP (0:1) local preshared key found
May 11 20:44:51.378: ISAKMP : Scanning profiles for xauth ... l2lvpn ezvpnprofile
May 11 20:44:51.378: ISAKMP (0:1) Authentication by xauth preshared
May 11 20:44:51.378: ISAKMP (0:1): Checking ISAKMP transform 1 against
      priority 20 policy
May 11 20:44:51.378: ISAKMP: encryption 3DES-CBC
May 11 20:44:51.378: ISAKMP: hash MD5
May 11 20:44:51.378: ISAKMP: default group 2
May 11 20:44:51.378: ISAKMP: auth pre-share
May 11 20:44:51.378: ISAKMP: life type in seconds
May 11 20:44:51.378: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
May 11 20:44:51.382: ISAKMP (0:1): atts are acceptable. Next payload is 0
      !--- Phase 1 proposal accepted. May 11 20:44:51.598: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_MAIN_MODE May 11 20:44:51.598: ISAKMP (0:1): Old State = IKE_R_MM1 New State =
      IKE_R_MM1 May 11 20:44:51.602: ISAKMP (0:1): sending packet to 172.18.124.196 my_port 500
      peer_port 500 (R) MM_SA_SETUP May 11 20:44:51.602: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
      IKE_PROCESS_COMPLETE May 11 20:44:51.602: ISAKMP (0:1): Old State = IKE_R_MM1 New State =
      IKE_R_MM2 May 11 20:44:52.130: ISAKMP (0:1): received packet from 172.18.124.196 dport 500 sport
      500 Global (R) MM_SA_SETUP May 11 20:44:52.130: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
      IKE_MM_EXCH May 11 20:44:52.130: ISAKMP (0:1): Old State = IKE_R_MM2 New State = IKE_R_MM3
      ..... May 11 20:44:52.954: ISAKMP (0:1): processing ID payload. message ID = 0 May 11
      20:44:52.954: ISAKMP (0:1): ID payload next-payload : 8 type : 1 address : 172.18.124.196
      protocol : 17 port : 500 length : 12 May 11 20:44:52.958: ISAKMP (0:1): peer matches l2lvpn
      profile
      !--- ISAKMP profile is matched in the router for LAN-to-LAN configuration. May 11 20:44:52.958:
      ISAKMP: Looking for a matching key for 172.18.124.196 in default May 11 20:44:52.958: ISAKMP:
Looking for a matching key for 172.18.124.196
      in vpn : success
May 11 20:44:52.958: ISAKMP (0:1): Found ADDRESS key in keyring vpn
May 11 20:44:52.958: ISAKMP (0:1): processing HASH payload. message ID = 0
May 11 20:44:52.958: ISAKMP (0:1): SA authentication status: authenticated
      !--- Security Associations are authenticated between the peers. May 11 20:44:52.994: ISAKMP
      (0:1): Old State = IKE_P1_COMPLETE
      New State = IKE_P1_COMPLETE
      !--- Phase 1 negotiations completed. .... May 11 20:44:53.002: ISAKMP (0:1): Checking IPsec
      proposal 1 May 11 20:44:53.002: ISAKMP: transform 1, ESP_3DES May 11 20:44:53.002: ISAKMP:
      attributes in transform: May 11 20:44:53.002: ISAKMP: encaps is 1 (Tunnel) May 11 20:44:53.002:
      ISAKMP: SA life type in seconds May 11 20:44:53.002: ISAKMP: SA life duration (basic) of 28800
```

May 11 20:44:53.002: ISAKMP: SA life type in kilobytes May 11 20:44:53.002: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 May 11 20:44:53.002: ISAKMP: authenticator is HMAC-SHA May 11 20:44:53.006: ISAKMP (0:1): **atts are acceptable.**  
*!--- Phase 2 proposal accepted.* May 11 20:44:53.006: IPSEC(validate\_proposal\_request): proposal part #1, (key eng. msg.) **INBOUND local= 172.18.124.195, remote= 172.18.124.196, local\_proxy= 192.168.40.0/255.255.255.0/0/0 (type=4), remote\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),**  
*!--- Encryption access-list verification process.* protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x2 ... **May 11 20:44:53.282: IPSEC(create\_sa): sa created,**  
**(sa) sa\_dest= 172.18.124.195, sa\_prot= 50,**  
**sa\_spi= 0xFBFA852C(4227499308),**  
**sa\_trans= esp-3des esp-sha-hmac , sa\_conn\_id= 2000**  
**May 11 20:44:53.282: IPSEC(create\_sa): sa created,**  
**(sa) sa\_dest= 172.18.124.196, sa\_prot= 50,**  
**sa\_spi= 0x79EFEFCE(2045767630),**  
**sa\_trans= esp-3des esp-sha-hmac , sa\_conn\_id= 2001**  
*!--- SAs are created with connection IDs.* May 11 20:44:53.290: ISAKMP (0:1): received packet from 172.18.124.196 dport 500 sport 500 Global (R) **QM\_IDLE**  
*!--- Tunnel has been established.* May 11 20:44:53.294: ISAKMP (0:1): deleting node 156512779 error FALSE reason "quick mode done (await)" May 11 20:44:53.294: ISAKMP (0:1): Node 156512779, Input = IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH May 11 20:44:53.294: ISAKMP (0:1): Old State = IKE\_QM\_R\_QM2

**New State = IKE\_QM\_PHASE2\_COMPLETE**

*!--- Phase 2 negotiations complete.*

## [EzVPN客戶端連線使用調試加密isakmp和調試加密ipsec進行調試](#)

May 11 20:55:47.266: ISAKMP (0:0): received packet from 172.18.124.197  
dport 500 sport 500 Global (N) NEW SA  
May 11 20:55:47.266: ISAKMP: local port 500, remote port 500  
May 11 20:55:47.270: ISAKMP: insert sa successfully sa = 81797590  
May 11 20:55:47.270: ISAKMP (0:2): processing SA payload. message ID = 0  
May 11 20:55:47.270: ISAKMP (0:2): processing ID payload. message ID = 0  
May 11 20:55:47.274: ISAKMP (0:2): ID payload  
next-payload : 13  
type : 11  
group id : **polo**  
protocol : 17  
port : 0  
length : 12  
May 11 20:55:47.274: ISAKMP (0:2): **peer matches ezvpnprofile profile**  
*!--- Profile match for EzVPN Client connection.* May 11 20:55:47.274: ISAKMP: Looking for a matching key for 172.18.124.197 in default May 11 20:55:47.274: ISAKMP: Looking for a matching key for 172.18.124.197 in vpn May 11 20:55:47.274: ISAKMP: Created a peer struct for 172.18.124.197, peer port 500 May 11 20:55:47.274: ISAKMP: Locking peer struct 0x81791484, IKE refcount 1 for crypto\_ikmp\_config\_initialize\_sa ... May 11 20:55:47.282: ISAKMP (0:2): **Checking ISAKMP transform 1 against**  
**priority 20 policy**  
*!--- ISAKMP policies are checked.* May 11 20:55:47.282: ISAKMP: encryption AES-CBC May 11 20:55:47.282: ISAKMP: keylength of 256 May 11 20:55:47.282: ISAKMP: hash SHA May 11 20:55:47.282: ISAKMP: default group 2 May 11 20:55:47.282: ISAKMP: auth XAUTHInitPreShared May 11 20:55:47.282: ISAKMP: life type in seconds May 11 20:55:47.282: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 May 11 20:55:47.282: ISAKMP (0:2): Encryption algorithm offered does not match policy! May 11 20:55:47.286: ISAKMP (0:2): atts are not acceptable. Next payload is 3 ...  
**May 11 20:55:47.306: ISAKMP (0:2): Checking ISAKMP transform 8 against**  
**priority 20 policy**  
**May 11 20:55:47.306: ISAKMP: encryption 3DES-CBC**  
**May 11 20:55:47.306: ISAKMP: hash MD5**  
**May 11 20:55:47.306: ISAKMP: default group 2**  
**May 11 20:55:47.306: ISAKMP: auth XAUTHInitPreShared**  
**May 11 20:55:47.306: ISAKMP: life type in seconds**  
**May 11 20:55:47.310: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80**

May 11 20:55:47.310: ISAKMP (0:2): **atts are acceptable. Next payload is 3**

*!--- Phase 1 attributes are validated.* May 11 20:55:47.530: ISAKMP (0:2): processing KE payload. message ID = 0 May 11 20:55:47.798: ISAKMP (0:2): processing NONCE payload. message ID = 0 May 11 20:55:47.802: ISAKMP (0:2): vendor ID is NAT-T v3 May 11 20:55:47.802: ISAKMP (0:2): vendor ID is NAT-T v2 May 11 20:55:47.802: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_PEER, IKE\_AM\_EXCH May 11 20:55:47.802: ISAKMP (0:2): Old State = IKE\_READY New State = IKE\_R\_AM\_AAA\_AWAIT May 11 20:55:47.806: ISAKMP: got callback 1 May 11 20:55:47.810: ISAKMP (0:2): SKEYID state generated May 11 20:55:47.810: ISAKMP (0:2): constructed NAT-T vendor-03 ID May 11 20:55:47.810: ISAKMP (0:2): SA is doing pre-shared key authentication plus XAUTH using id type ID\_IPV4\_ADDR May 11 20:55:47.814: ISAKMP (0:2): ID payload next-payload : 10 type : 1 address : 172.18.124.195 protocol : 17 port : 0 length : 12 May 11 20:55:47.814: ISAKMP (2): Total payload length: 12 May 11 20:55:47.814: ISAKMP (0:2): sending packet to 172.18.124.197 my\_port 500 peer\_port 500 (R) AG\_INIT\_EXCH May 11 20:55:47.814: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_AAA, PRESHARED\_KEY\_REPLY May 11 20:55:47.818: ISAKMP (0:2): Old State = IKE\_R\_AM\_AAA\_AWAIT New State = IKE\_R\_AM2 May 11 20:55:49.114: ISAKMP (0:2): received packet from 172.18.124.197 dport 500 sport 500 Global (R) AG\_INIT\_EXCH May 11 20:55:49.114: ISAKMP:received payload type 20 May 11 20:55:49.118: ISAKMP:received payload type 20 May 11 20:55:49.118: ISAKMP (0:2): processing HASH payload. message ID = 0 May 11 20:55:49.118: ISAKMP (0:2): processing NOTIFY INITIAL\_CONTACT protocol 1 spi 0, message ID = 0, sa = 81797590 **May 11 20:55:49.118: ISAKMP (0:2): SA authentication status: authenticated**

*!--- Phase 1 has been authenticated.* May 11 20:55:49.118: ISAKMP (0:2): Process initial contact, bring down existing phase 1 and 2 SA's with local 172.18.124.197 authentication status: authenticated May 11 20:55:49.122: ISAKMP (0:2): SA has been authenticated with 172.18.124.197 May 11 20:55:49.122: ISAKMP: Trying to insert a peer 172.18.124.195/172.18.124.197/500/, and inserted successfully. May 11 20:55:49.126: ISAKMP: **set new node 1554218001 to CONF\_XAUTH**

*!--- User authentication phase starts.* May 11 20:55:49.126: ISAKMP (0:2): sending packet to 172.18.124.197 my\_port 500 peer\_port 500 (R) QM\_IDLE May 11 20:55:49.126: ISAKMP (0:2): purging node 155421800118.124.195 remote 172.18.124.197 remote port 500 May 11 20:55:49.130: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_PEER, IKE\_AM\_EXCH May 11 20:55:49.130: ISAKMP (0:2): Old State = IKE\_R\_AM2 New State = IKE\_P1\_COMPLETE May 11 20:55:49.130: ISAKMP (0:2): **Need XAUTH** May 11 20:55:49.130: ISAKMP (0:2): FSM action returned error: 4 May 11 20:55:49.134: ISAKMP (0:2): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE May 11 20:55:49.134: ISAKMP (0:2): Old State = IKE\_P1\_COMPLETE  
New State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT

May 11 20:55:49.134: ISAKMP: got callback 1  
May 11 20:55:49.134: ISAKMP: set new node -1233989434 to CONF\_XAUTH  
May 11 20:55:49.134: ISAKMP/xauth: **request attribute XAUTH\_USER\_NAME\_V2**

*!--- Username request.* May 11 20:55:49.134: ISAKMP/xauth: **request attribute XAUTH\_USER\_PASSWORD\_V2**

*!--- Password request.* May 11 20:55:49.138: ISAKMP (0:2): initiating peer config to 172.18.124.197. ID = -1233989434 May 11 20:55:49.138: ISAKMP (0:2): sending packet to 172.18.124.197 my\_port 500 peer\_port 500 (R) CONF\_XAUTH ... May 11 20:55:51.278: ISAKMP: got callback 1 May 11 20:55:51.278: ISAKMP (0:2): attributes sent in message: May 11 20:55:51.278: Address: 240.2.112.2 May 11 20:55:51.282: ISAKMP (0:2): **allocating address 172.25.70.6**

*!--- IP address assigned to EzVPN Client from the address pool.* May 11 20:55:51.282: ISAKMP: Sending private address: 172.25.70.6 May 11 20:55:51.286: ISAKMP: Sending APPLICATION\_VERSION string: Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-K9O3SY7-M), Version 12.3(9a), RELEASE SOFTWARE (fc4) Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Fri 23-Jul-04 02:20 by kellythw May 11 20:55:51.286: ISAKMP (0:2): responding to peer config from 172.18.124.197. ID = -591421152 May 11 20:55:51.290: ISAKMP (0:2): sending packet to 172.18.124.197 my\_port 500 peer\_port 500 (R) CONF\_ADDR May 11 20:55:51.290: ISAKMP (0:2): deleting node -591421152 error FALSE reason "" May 11 20:55:51.290: ISAKMP (0:2): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_GROUP\_ATTR May 11 20:55:51.290: ISAKMP (0:2): Old State = IKE\_CONFIG\_AUTHOR\_AAA\_AWAIT New State = IKE\_P1\_COMPLETE May 11 20:55:51.294: ISAKMP (0:2): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE May 11 20:55:51.294: ISAKMP (0:2): Old State = IKE\_P1\_COMPLETE New State = IKE\_P1\_COMPLETE May 11 20:55:53.102: ISAKMP (0:2): received packet from 172.18.124.197 dport 500 sport 500 Global (R) QM\_IDLE May 11 20:55:53.102: ISAKMP: set new node -183955662 to QM\_IDLE ... May 11 20:55:53.178: ISAKMP (0:2): IPsec policy invalidated proposal May 11 20:55:53.178: ISAKMP (0:2): Checking IPsec proposal 8 May 11 20:55:53.178: ISAKMP: transform 1, ESP\_3DES May 11 20:55:53.178: ISAKMP: attributes in transform: May 11 20:55:53.178: ISAKMP: encaps is 1 (Tunnel) May 11 20:55:53.178: ISAKMP: SA life type in seconds May 11 20:55:53.182: ISAKMP: SA life duration (basic) of 28800 May 11 20:55:53.182: ISAKMP: SA life type in kilobytes May 11 20:55:53.182: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0



```
May 11 20:55:53.182: ISAKMP: authenticator is HMAC-MD5 May 11 20:55:53.182: ISAKMP (0:2): atts are acceptable.
!--- Proposals are validated. May 11 20:55:53.182: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.18.124.195, remote= 172.18.124.197, local_proxy= 0.0.0.0/0.0.0.0/0 (type=4), remote_proxy= 172.25.70.6/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2 ... local_proxy= 0.0.0.0/0.0.0.0/0 (type=4), remote_proxy= 172.25.70.6/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel), lifedur= 28800s and 4608000kb, spi= 0x866452A1(2254721697), conn_id= 2002, keysize= 0, flags= 0x2 May 11 20:55:53.458: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.18.124.195, remote= 172.18.124.197, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 172.25.70.6/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel), lifedur= 28800s and 4608000kb, spi= 0xCA8A5934(3398064436), conn_id= 2003, keysize= 0, flags= 0xA May 11 20:55:53.458: IPSEC(kei_proxy): head = rtp, map->ivrf = , kei->ivrf = May 11 20:55:53.458: IPSEC(kei_proxy): head = rtp, map->ivrf = , kei->ivrf = May 11 20:55:53.462: IPSEC(kei_proxy): head = rtp, map->ivrf = , kei->ivrf = May 11 20:55:53.462: IPSEC(add mtree): src 172.18.124.195, dest 172.25.70.6, dest_port 0 May 11 20:55:53.462: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.195, sa_prot= 50, sa_spi= 0x866452A1(2254721697), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
May 11 20:55:53.462: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.197, sa_prot= 50, sa_spi= 0xCA8A5934(3398064436), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
!--- Security Association Connection IDs. May 11 20:55:54.442: ISAKMP (0:2): received packet from 172.18.124.197 dport 500 sport 500 Global (R) QM_IDLE May 11 20:55:54.446: ISAKMP (0:2): deleting node -183955662 error FALSE reason "quick mode done (await)" May 11 20:55:54.446: ISAKMP (0:2): Node -183955662, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH May 11 20:55:54.446: ISAKMP (0:2): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE May 11 20:55:54.446: IPSEC(key_engine): got a queue event... May 11 20:55:54.446: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP May 11 20:55:54.446: IPSEC(key_engine_enable_outbound): enable SA with spi 3398064436/50 for 172.18.124.197 May 11 20:55:57.450: ISAKMP (0:2): received packet from 172.18.124.197 dport 500 sport 500 Global (R) QM_IDLE May 11 20:55:57.450: ISAKMP: set new node -1115155724 to QM_IDLE May 11 20:55:57.454: ISAKMP (0:2): processing HASH payload. message ID = -1115155724 May 11 20:55:57.458: ISAKMP (0:2): processing SA payload. message ID = -1115155724 May 11 20:55:57.458: ISAKMP (0:2): Checking IPsec proposal 1 May 11 20:55:57.458: ISAKMP: transform 1, ESP_AES May 11 20:55:57.458: ISAKMP: attributes in transform: May 11 20:55:57.458: ISAKMP: encaps is 1 (Tunnel) May 11 20:55:57.458: ISAKMP: SA life type in seconds May 11 20:55:57.458: ISAKMP: SA life duration (basic) of 28800 May 11 20:55:57.458: ISAKMP: SA life type in kilobytes May 11 20:55:57.458: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 May 11 20:55:57.458: ISAKMP: authenticator is HMAC-SHA May 11 20:55:57.458: ISAKMP: key length is 256 May 11 20:55:57.462: ISAKMP (0:2): atts are acceptable.
May 11 20:55:57.462: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 172.18.124.195, remote= 172.18.124.197, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy= 172.18.124.197/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-aes 256 esp-sha-hmac (Tunnel), lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x2
...
```

```
May 11 20:55:58.362: ISAKMP (0:2): sending packet to 172.18.124.197
my_port 500 peer_port 500 (R) QM_IDLE
```

```
!--- Confirmation of tunnel establishment. May 11 20:55:58.362: ISAKMP (0:2): Node -1115155724, Input = IKE_MSG_FROM_IPSEC, IKE_SPI_REPLY May 11 20:55:59.438: ISAKMP (0:2): received packet from 172.18.124.197 dport 500 sport 500 Global (R) QM_IDLE May 11 20:55:59.438: ISAKMP (0:2): deleting node -1115155724 error FALSE reason "quick mode done (await)" May 11 20:55:59.442: ISAKMP (0:2): Node -1115155724, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH May 11 20:55:59.442: ISAKMP (0:2): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
```

[使用debug crypto isakmp和debug crypto ipsec的PIX端上的VPN客戶端調試](#)

May 11 21:16:52.154: ISAKMP (0:0): received packet from 172.18.173.80 dport 500 sport 500 Global (N) NEW SA

May 11 21:16:52.154: ISAKMP: local port 500, remote port 500

May 11 21:16:52.158: ISAKMP: insert sa successfully sa = 8179D054

May 11 21:16:52.158: ISAKMP (0:3): processing SA payload. message ID = 0

May 11 21:16:52.158: ISAKMP (0:3): processing ID payload. message ID = 0

May 11 21:16:52.158: ISAKMP (0:3): ID payload

next-payload : 13

type : 11

group id : **tennis**

protocol : 17

port : 500

length : 14

**May 11 21:16:52.158: ISAKMP (0:3): peer matches softclient profile**

*!--- ISAKMP profile match for VPN Software Clients.* May 11 21:16:52.158: ISAKMP: Looking for a matching key for 172.18.173.80 in default May 11 21:16:52.158: ISAKMP: Looking for a matching key for 172.18.173.80 in vpn May 11 21:16:52.158: ISAKMP: Created a peer struct for 172.18.173.80, peer port 500 May 11 21:16:52.162: ISAKMP: Locking peer struct 0x81791484, IKE refcount 1 for crypto\_ikmp\_config\_initialize\_sa May 11 21:16:52.162: ISAKMP (0:3): Setting client config settings 81EEB340 May 11 21:16:52.162: ISAKMP (0:3): (Re)Setting client xauth list and state May 11 21:16:52.162: ISAKMP (0:3): processing vendor id payload May 11 21:16:52.162: ISAKMP (0:3): vendor ID seems Unity/DPD but major 215 mismatch May 11 21:16:52.162: ISAKMP (0:3): vendor ID is XAUTH May 11 21:16:52.162: ISAKMP (0:3): processing vendor id payload May 11 21:16:52.162: ISAKMP (0:3): vendor ID is DPD May 11 21:16:52.162: ISAKMP (0:3): processing vendor id payload May 11 21:16:52.166: ISAKMP (0:3): vendor ID seems Unity/DPD but major 123 mismatch May 11 21:16:52.166: ISAKMP (0:3): vendor ID is NAT-T v2 May 11 21:16:52.166: ISAKMP (0:3): processing vendor id payload May 11 21:16:52.166: ISAKMP (0:3): vendor ID seems Unity/DPD but major 194 mismatch May 11 21:16:52.166: ISAKMP (0:3): processing vendor id payload May 11 21:16:52.166: ISAKMP (0:3): vendor ID is Unity May 11 21:16:52.166: ISAKMP (0:3) Authentication by xauth preshared May 11 21:16:52.166: ISAKMP (0:3): **Checking ISAKMP transform 1 against priority 20 policy**

*!--- ISAKMP policy that matches against configured policy.* May 11 21:16:52.166: ISAKMP: encryption AES-CBC May 11 21:16:52.170: ISAKMP: hash SHA May 11 21:16:52.170: ISAKMP: default group 2 May 11 21:16:52.170: ISAKMP: auth XAUTHInitPreShared May 11 21:16:52.170: ISAKMP: life type in seconds May 11 21:16:52.170: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B May 11 21:16:52.170: ISAKMP: keylength of 256 May 11 21:16:52.170: ISAKMP (0:3): Encryption algorithm offered does not match policy! May 11 21:16:52.170: ISAKMP (0:3): atts are not acceptable. Next payload is 3 .... May 11 21:16:52.198: ISAKMP (0:3): Checking ISAKMP transform 10 against priority 20 policy May 11 21:16:52.198: ISAKMP: encryption 3DES-CBC May 11 21:16:52.202: ISAKMP: hash MD5 May 11 21:16:52.202: ISAKMP: default group 2 May 11 21:16:52.202: ISAKMP: auth XAUTHInitPreShared May 11 21:16:52.202: ISAKMP: life type in seconds May 11 21:16:52.202: ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B May 11 21:16:52.202: ISAKMP (0:3): atts are acceptable. Next payload is 3 May 11 21:16:52.418: ISAKMP (0:3): processing KE payload. message ID = 0 May 11 21:16:52.686: ISAKMP (0:3): processing NONCE payload. message ID = 0 May 11 21:16:52.690: ISAKMP (0:3): vendor ID is NAT-T v2 May 11 21:16:52.690: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_PEER, IKE\_AM\_EXCH May 11 21:16:52.690: ISAKMP (0:3): Old State = IKE\_READY New State = IKE\_R\_AM\_AAA\_AWAIT May 11 21:16:52.694: ISAKMP: got callback 1 May 11 21:16:52.698: ISAKMP (0:3): SKEYID state generated May 11 21:16:52.698: ISAKMP (0:3): constructed NAT-T vendor-02 ID May 11 21:16:52.702: ISAKMP (0:3): SA is doing pre-shared key authentication plus XAUTH using id type ID\_IPV4\_ADDR May 11 21:16:52.702: ISAKMP (0:3): ID payload next-payload : 10 type : 1 address : 172.18.124.195 protocol : 17 port : 0 length : 12 May 11 21:16:52.702: ISAKMP (3): Total payload length: 12 May 11 21:16:52.702: ISAKMP (0:3): sending packet to 172.18.173.80 my\_port 500 peer\_port 500 (R) AG\_INIT\_EXCH May 11 21:16:52.706: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_AAA, PRESHARED\_KEY\_REPLY May 11 21:16:52.706: ISAKMP (0:3): Old State =

IKE\_R\_AM\_AAA\_AWAIT New State = IKE\_R\_AM2 May 11 21:16:52.746: ISAKMP (0:3): received packet from 172.18.173.80 dport 500 sport 500 Global (R) AG\_INIT\_EXCH May 11 21:16:52.750: ISAKMP (0:3): processing HASH payload. message ID = 0 May 11 21:16:52.750: ISAKMP (0:3): processing NOTIFY INITIAL\_CONTACT protocol 1 spi 0, message ID = 0, sa = 8179D054 May 11 21:16:52.750: ISAKMP (0:3): **SA authentication status: authenticated**

*!---* Phase 1 SAs are authenticated. May 11 21:16:52.750: ISAKMP (0:3): Process initial contact, bring down existing phase 1 and 2 SA's with local 172.18.124.195 remote 172.18.173.80 remote port 500 May 11 21:16:52.750: ISAKMP (0:3): returning IP addr to the address pool May 11 21:16:52.754: ISAKMP:received payload type 20 May 11 21:16:52.754: ISAKMP:received payload type 20 May 11 21:16:52.754: ISAKMP (0:3): SA authentication status: authenticated May 11 21:16:52.754: ISAKMP (0:3): SA has been authenticated with 172.18.173.80 May 11 21:16:52.754: ISAKMP: Trying to insert a peer 172.18.124.195/172.18.173.80/500/, and inserted successfully. May 11 21:16:52.758: IPSEC(key\_engine): got a queue event... May 11 21:16:52.758: ISAKMP: set new node -1991824466 to **CONF\_XAUTH**

*!---* User Authentication phase starts. May 11 21:16:52.758: ISAKMP (0:3): sending packet to 172.18.173.80 my\_port 500 peer\_port 500 (R) QM\_IDLE May 11 21:16:52.762: ISAKMP (0:3): purging node -1991824466 May 11 21:16:52.762: ISAKMP: Sending phase 1 responder lifetime 86400 May 11 21:16:52.762: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_PEER, IKE\_AM\_EXCH May 11 21:16:52.762: ISAKMP (0:3): Old State = IKE\_R\_AM2 New State = IKE\_P1\_COMPLETE May 11 21:16:52.762: ISAKMP (0:3): Need XAUTH May 11 21:16:52.762: ISAKMP (0:3): FSM action returned error: 4 May 11 21:16:52.766: ISAKMP (0:3): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE May 11 21:16:52.766: ISAKMP (0:3): Old State = IKE\_P1\_COMPLETE New State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT May 11 21:16:52.766: ISAKMP: got callback 1 May 11 21:16:52.766: ISAKMP: set new node -1773462433 to CONF\_XAUTH May 11 21:16:52.766: ISAKMP/xauth: **request attribute XAUTH\_USER\_NAME\_V2**

*!---* Requests user name. May 11 21:16:52.770: ISAKMP/xauth: **request attribute XAUTH\_USER\_PASSWORD\_V2**

*!---* Requests user password. May 11 21:16:52.770: ISAKMP (0:3): initiating peer config to 172.18.173.80. ID = -1773462433 May 11 21:16:52.770: ISAKMP (0:3): sending packet to 172.18.173.80 my\_port 500 peer\_port 500 (R) CONF\_XAUTH May 11 21:16:52.770: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_START\_LOGIN ... May 11 21:17:00.350: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_PEER, IKE\_CFG\_REQUEST May 11 21:17:00.350: ISAKMP (0:3): Old State = IKE\_P1\_COMPLETE New State = IKE\_CONFIG\_AUTHOR\_AAA\_AWAIT May 11 21:17:00.434: ISAKMP: got callback 1 May 11 21:17:00.438: ISAKMP (0:3): attributes sent in message: May 11 21:17:00.438: Address: 0.2.0.0 May 11 21:17:00.438: ISAKMP (0:3): **allocating address 10.50.50.2**

*!---* Allocates the IP address for software VPN Client from the client IP pool. May 11 21:17:00.438: ISAKMP: Sending private address: 10.50.50.2 May 11 21:17:00.442: ISAKMP: Sending ADDRESS\_EXPIRY seconds left to use the address: 86391 May 11 21:17:00.442: ISAKMP: Sending APPLICATION\_VERSION string: Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-K9O3SY7-M), Version 12.3(9a), RELEASE SOFTWARE (fc4) Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Fri 23-Jul-04 02:20 by kellythw May 11 21:17:00.442: ISAKMP (0/3): Unknown Attr: UNKNOWN (0x7008) May 11 21:17:00.446: ISAKMP (0/3): Unknown Attr: UNKNOWN (0x700A) May 11 21:17:00.446: ISAKMP (0/3): Unknown Attr: UNKNOWN (0x7005) May 11 21:17:00.446: ISAKMP (0:3): responding to peer config from 172.18.173.80. ID = 1330918554 May 11 21:17:00.450: ISAKMP (0:3): sending packet to 172.18.173.80 my\_port 500 peer\_port 500 (R) CONF\_ADDR May 11 21:17:00.450: ISAKMP (0:3): deleting node 1330918554 error FALSE reason "" May 11 21:17:00.450: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_AAA, IKE\_AAA\_GROUP\_ATTR May 11 21:17:00.450: ISAKMP (0:3): Old State = IKE\_CONFIG\_AUTHOR\_AAA\_AWAIT New State = IKE\_P1\_COMPLETE May 11 21:17:00.454: ISAKMP (0:3): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE May 11 21:17:00.454: ISAKMP (0:3): Old State = IKE\_P1\_COMPLETE New State = IKE\_P1\_COMPLETE ... May 11 21:17:01.474: ISAKMP (0:3):

#### **Creating IPsec SAs**

*!---* Creation of IPsec Security Associations. May 11 21:17:01.474: inbound SA from 172.18.173.80 to 172.18.124.195 (f/i) 0/ 0 (proxy 10.50.50.2 to 0.0.0.0) May 11 21:17:01.474: has spi 0x1B139B2F and conn\_id 2000 and flags 2 May 11 21:17:01.474: lifetime of 2147483 seconds May 11 21:17:01.474: has client flags 0x0 May 11 21:17:01.474: outbound SA from 172.18.124.195 to 172.18.173.80 (f/i) 0/ 0 (proxy 0.0.0.0 to 10.50.50.2 ) May 11 21:17:01.474: has spi -895677582 and conn\_id 2001 and flags A May 11 21:17:01.474: lifetime of 2147483 seconds May 11 21:17:01.474: has client flags 0x0 May 11 21:17:01.478: ISAKMP (0:3): sending packet to 172.18.173.80 my\_port 500 peer\_port 500 (R) QM\_IDLE May 11 21:17:01.478: ISAKMP (0:3): Node 896912581, Input = IKE\_MSG\_FROM\_IPSEC, IKE\_SPI\_REPLY May 11 21:17:01.478: ISAKMP (0:3): Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2 May 11 21:17:01.482: IPSEC(key\_engine): got a queue event... May 11 21:17:01.482: IPSEC(initialize\_sas): , (key eng. msg.) INBOUND local= 172.18.124.195, remote= 172.18.173.80, local\_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote\_proxy= 10.50.50.2/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel), lifedur= 2147483s and 0kb, spi= 0x1B139B2F(454269743), conn\_id= 2000, keysize= 0, flags= 0x2 May

```

11 21:17:01.482: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 172.18.124.195,
remote= 172.18.173.80, local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4), remote_proxy=
10.50.50.2/0.0.0.0/0/0 (type=1), protocol= ESP, transform= esp-3des esp-sha-hmac (Tunnel),
lifedur= 2147483s and 0kb, spi= 0xCA9D0B72(3399289714), conn_id= 2001, keysize= 0, flags= 0xA
May 11 21:17:01.486: IPSEC(kei_proxy): head = rtp, map->ivrf = , kei->ivrf = May 11
21:17:01.486: IPSEC(kei_proxy): head = rtp, map->ivrf = , kei->ivrf = May 11 21:17:01.486:
IPSEC(add mtree): src 172.18.124.195, dest 10.50.50.2, dest_port 0 May 11 21:17:01.486:
IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.124.195, sa_prot= 50,
sa_spi= 0x1B139B2F(454269743),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2000
May 11 21:17:01.490: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.18.173.80, sa_prot= 50,
sa_spi= 0xCA9D0B72(3399289714),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 2001
!--- Security Association connection IDs created. May 11 21:17:01.742: ISAKMP (0:3): received
packet from 172.18.173.80 dport 500 sport 500 Global (R) QM_IDLE
!--- Successful tunnel established. May 11 21:17:01.746: ISAKMP (0:3): deleting node 896912581
error FALSE reason "quick mode done (await)" May 11 21:17:01.746: ISAKMP (0:3): Node 896912581,
Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH May 11 21:17:01.746: ISAKMP (0:3): Old State =
IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
May 11 21:17:01.746: IPSEC(key_engine): got a queue event...
May 11 21:17:01.746: IPSEC(key_engine_enable_outbound): rec'd
enable notify from ISAKMP
May 11 21:17:01.746: IPSEC(key_engine_enable_outbound): enable SA
with spi 3399289714/50 for 172.18.173.80

```

## [PIX 501 \( LAN到LAN連線 \) 上的調試](#)

```

PIX-501#
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:172.18.124.195, dest:172.18.124.196
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
!--- ISAKMP attributes check in process. 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 0x1 0x51 0x80 ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.124.195, dest:172.18.124.196
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE 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 another IOS box!

ISAKMP (0): processing vendor id payload

ISAKMP (0): received xauth v6 vendor id

```



```
ISAKMP (0): ID payload
next-payload : 8
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:172.18.124.195, dest:172.18.124.196
spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of 156512779:954320bIPSEC
(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x79efefce(2045767630) for SA
from 172.18.124.195 to 172.18.124.196 for prot 3

return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.195/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.195/500 Ref cnt incremented to:1 Total
VPN Peers:1
crypto_isakmp_process_block:src:172.18.124.195, dest:172.18.124.196
spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 156512779

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-SHA
ISAKMP (0): atts are acceptable.
!--- Phase 1 attributes are negotiated. IPSEC(validate_proposal_request): proposal part #1, (key
eng. msg.) dest= 172.18.124.195, src= 172.18.124.196, dest_proxy= 192.168.40.0/255.255.255.0/0/0
(type=4), src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des
esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0):
processing NONCE payload. message ID = 156512779 ISAKMP (0): processing ID payload. message ID =
156512779 ISAKMP (0): processing ID payload. message ID = 156512779 ISAKMP (0): processing
NOTIFY payload 24576 protocol 3 spi 4227499308, message ID = 156512779 ISAKMP (0): processing
responder lifetime ISAKMP (0): responder lifetime of 3600s ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.195 to 172.18.124.196 (proxy 192.168.40.0 to 192.168.10.0) has spi
2045767630 and conn_id 1 and flags 4 lifetime of 3600 seconds lifetime of 4608000 kilobytes
outbound SA from 172.18.124.196 to 172.18.124.195 (proxy 192.168.10.0 to 192.168.40.0) has spi
4227499308 and conn_id 2 and flags 4 lifetime of 3600 seconds lifetime of 4608000
kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest=
172.18.124.196, src= 172.18.124.195, dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.40.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-sha-
hmac , lifedur= 3600s and 4608000kb, spi= 0x79efefce(2045767630), conn_id= 1, keysize= 0, flags=
0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.196, dest= 172.18.124.195,
```

```
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.40.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xfbfa852c(4227499308), conn_id= 2, keysize= 0, flags= 0x4
!--- Phase 2 tunnel establishment.
```

## PIX-506-B ( EzVPN客戶端連線 ) 上的調試

```
ISAKMP (0): ID payload
next-payload : 13
type : 11
protocol : 17
port : 0
length : 8
```

```
ISAKMP (0): Total payload length: 12
ISAKMP (0:0): sending NAT-T vendor ID - rev 2 & 3
ISAKMP (0): beginning Aggressive Mode exchange
crypto_isakmp_process_block:src:172.18.124.195, dest:172.18.124.197
spt:500 dpt:500
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
```

```
ISAKMP (0): Checking ISAKMP transform 1 against priority 65001 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share (init)
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are not acceptable. Next payload is 0
...
```

```
ISAKMP (0): Checking ISAKMP transform 1 against priority 65008 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share (init)
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
```

```
!--- Phase 1 attributes are accepted. 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 another IOS box! ISAKMP (0): processing
vendor id payload ISAKMP (0): received xauth v6 vendor id ISAKMP (0): processing vendor id
payload ISAKMP (0:0): vendor ID is NAT-T ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing ID payload. message ID = 0 ISAKMP (0): processing NONCE payload. message
ID = 0 ISAKMP (0): processing HASH payload. message ID = 0 ISAKMP (0:0): Detected NAT-D payload
ISAKMP (0:0): recalc my hash for NAT-D ISAKMP (0:0): NAT match MINE hash ISAKMP (0:0): Detected
NAT-D payload ISAKMP (0:0): recalc his hash for NAT-D ISAKMP (0:0): NAT match HIS hash ISAKMP
(0): SA has been authenticated
```

```
!--- SAs have been authenticated. crypto_isakmp_process_block:src:172.18.124.195,
dest:172.18.124.197 spt:500 dpt:500 ISAKMP (0): processing NOTIFY payload 24576 protocol 1 spi
0, message ID = 1554218001 ISAKMP (0): processing responder lifetime ISAKMP (0): phase 1
responder lifetime of 86400s ISAKMP (0): not overriding 86400s return status is
IKMP_NO_ERR_NO_TRANS crypto_isakmp_process_block:src:172.18.124.195, dest:172.18.124.197 spt:500
dpt:500 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from
172.18.124.195. message ID = 15250780 ISAKMP: Config payload CFG_REQUEST ISAKMP (0:0): checking
request:
```

```
!--- Extended authentication process check. ISAKMP: attribute XAUTH_USER_NAME (16521)
ISAKMP: attribute XAUTH_USER_PASSWORD (16522)
```

```
ISAKMP (0:0): responding to peer config from 172.18.124.195. ID = 3060977862
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.124.195, dest:172.18.124.197
```

```

spt:500 dpt:500
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 172.18.124.195.
message ID = 15250780
ISAKMP: Config payload CFG_SET
ISAKMP (0:0): checking SET:
ISAKMP: XAUTH_STATUS XAUTH-OK
!--- Extended authentication checked. ISAKMP (0:0): attributes sent in message: Status: 1 return
status is IKMP_NO_ERROR ISAKMP : attributes being requested INTERNAL_IPV_ADDRESS ALT_DEF_DOMAIN
INTERNAL_IPV_NBNS INTERNAL_IPV_DNS ALT_SPLIT_INCLUDE ALT_SPLITDNS_NAME ALT_PFS ALT_CFG_SEC_UNIT
ALT_CFG_USER_AUTH ALT_CFG_IDLE_TIME ALT_CFG_IP_TEL ALT_CFG_AUTH_SRVNAME ALT_CFG_AUTH_SRVPORT
ALT_CFG_AUTH_SRVSEC ALT_BACKUP_SERVERS ... ISAKMP : Checking IPsec proposal 1 ISAKMP: transform
1, ESP_3DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-MD5 ISAKMP (0): atts are
acceptable.
!--- IPsec proposal accepted. IPSEC(validate_proposal_request): proposal part #1, (key eng.
msg.) dest= 172.18.124.195, src= 172.18.124.197, dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 172.25.70.6/255.255.255.255/0/0 (type=1), protocol= ESP, transform= esp-3des esp-md5-
hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0):
processing NONCE payload. message ID = 4111011634 ISAKMP (0): processing ID payload. message ID
= 4111011634 ISAKMP (0): processing ID payload. message ID = 4111011634 ISAKMP (0): processing
NOTIFY payload 24576 protocol 3 spi 2254721697, message ID = 4111011634 ISAKMP (0): processing
responder lifetime ISAKMP (0): responder lifetime of 3600s ISAKMP (0): Creating IPsec SAs
inbound SA from 172.18.124.195 to 172.18.124.197 (proxy 0.0.0.0 to 172.25.70.6) has spi
3398064436 and conn_id 2 and flags 4 lifetime of 3600 seconds lifetime of 4608000 kilobytes
outbound SA from 172.18.124.197 to 172.18.124.195 (proxy 172.25.70.6 to 0.0.0.0) has spi
2254721697 and conn_id 1 and flags 4 lifetime of 3600 seconds lifetime of 4608000
kilobytesIPSEC(key_engine): got a queue event... IPSEC(initialize_sas): , (key eng. msg.) dest=
172.18.124.197, src= 172.18.124.195, dest_proxy= 172.25.70.6/255.255.255.255/0/0 (type=1),
src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xca8a5934(3398064436), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.197, dest= 172.18.124.195,
src_proxy= 172.25.70.6/255.255.255.255/0/0 (type=1),
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
!--- IPsec SAs created. protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and
4608000kb, spi= 0x866452a1(2254721697), conn_id= 1, keysize= 0, flags= 0x4

```

## VPN客戶端上的調試

選擇Start > Programs > Cisco VPN Client > Log Viewer。

```

Cisco Systems VPN Client Version 4.0 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600

```

```

1 15:47:01.430 08/19/04 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 172.18.124.195.

```

```

2 15:47:01.460 08/19/04 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd),
VID(Nat-T), VID(Frag), VID(Unity)) to 172.18.124.195

```

```

3 15:47:01.947 08/19/04 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.195

```

```

4 15:47:01.947 08/19/04 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth),

```

VID(Nat-T), KE, ID, NON, HASH, NAT-D, NAT-D) from 172.18.124.195

5 15:47:01.947 08/19/04 Sev=Info/5 IKE/0x63000001  
Peer is a Cisco-Unity compliant peer

6 15:47:01.947 08/19/04 Sev=Info/5 IKE/0x63000001  
Peer supports DPD

7 15:47:01.947 08/19/04 Sev=Info/5 IKE/0x63000001  
Peer supports DWR Code and DWR Text

8 15:47:01.947 08/19/04 Sev=Info/5 IKE/0x63000001  
Peer supports XAUTH

9 15:47:01.947 08/19/04 Sev=Info/5 IKE/0x63000001  
Peer supports NAT-T

10 15:47:01.977 08/19/04 Sev=Info/6 IKE/0x63000001  
IOS Vendor ID Contruction successful

11 15:47:01.977 08/19/04 Sev=Info/4 IKE/0x63000013  
SENDING >>> ISAKMP OAK AG \*(HASH, NOTIFY:STATUS\_INITIAL\_CONTACT,  
NAT-D, NAT-D, VID(?), VID(Unity)) to 172.18.124.195

12 15:47:01.977 08/19/04 Sev=Info/4 IKE/0x63000082  
IKE Port in use - Local Port = 0x01F4, Remote Port = 0x01F4

13 15:47:01.977 08/19/04 Sev=Info/5 IKE/0x63000071

**Automatic NAT Detection Status:**

**Remote end is NOT behind a NAT device**

**This end is NOT behind a NAT device**

*!--- NAT device detection process.* 14 15:47:01.986 08/19/04 Sev=Info/5 IKE/0x6300002F Received  
ISAKMP packet: peer = 172.18.124.195 15 15:47:01.986 08/19/04 Sev=Info/4 IKE/0x63000014  
RECEIVING <<< ISAKMP OAK INFO \*(HASH, NOTIFY:STATUS\_RESP\_LIFETIME) from 172.18.124.195 16  
15:47:01.986 08/19/04 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400  
seconds 17 15:47:01.986 08/19/04 Sev=Info/5 IKE/0x63000046 This SA has already been alive for 0  
seconds, setting expiry to 86400 seconds from now 18 15:47:01.996 08/19/04 Sev=Info/5  
IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.195 19 15:47:01.996 08/19/04 Sev=Info/4  
IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from 172.18.124.195 20 15:47:02.689  
08/19/04 Sev=Info/4 IPSEC/0x63700008 IPsec driver successfully started 21 15:47:02.689 08/19/04  
Sev=Info/4 IPSEC/0x63700014 Deleted all keys 22 15:47:02.689 08/19/04 Sev=Info/6  
IPSEC/0x6370002B Sent 85 packets, 0 were fragmented. 23 15:47:06.044 08/19/04 Sev=Info/4  
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH, ATTR) to 172.18.124.195 24 15:47:06.064  
08/19/04 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.18.124.195 25 15:47:06.064  
08/19/04 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS \*(HASH, ATTR) from  
172.18.124.195 26 15:47:06.064 08/19/04 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS  
\*(HASH, ATTR) to 172.18.124.195 27 15:47:06.103 08/19/04 Sev=Info/5 IKE/0x6300005D Client  
sending a firewall request to concentrator 28 15:47:06.103 08/19/04 Sev=Info/5 IKE/0x6300005C  
Firewall Policy: Product=Cisco Systems Integrated Client, Capability=(Centralized Protection  
Policy). 29 15:47:06.113 08/19/04 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS \*(HASH,  
ATTR) to 172.18.124.195 30 15:47:06.132 08/19/04 Sev=Info/5 IKE/0x6300002F Received ISAKMP  
packet: peer = 172.18.124.195 31 15:47:06.132 08/19/04 Sev=Info/4 IKE/0x63000014 RECEIVING <<<  
ISAKMP OAK TRANS \*(HASH, ATTR) from 172.18.124.195 32 15:47:06.132 08/19/04 Sev=Info/5  
IKE/0x63000010 **MODE\_CFG\_REPLY: Attribute = INTERNAL\_IPV4\_ADDRESS: , value = 10.50.50.2**

*!--- Assigned IP address for the VPN Client.* 33 15:47:06.132 08/19/04 Sev=Info/5 IKE/0xA3000017  
MODE\_CFG\_REPLY: The received (INTERNAL\_ADDRESS\_EXPIRY) attribute and value (842150403) is not  
supported 34 15:47:06.132 08/19/04 Sev=Info/5 IKE/0x6300000E MODE\_CFG\_REPLY: Attribute =  
MODECFG\_UNITY\_DEFDOMAIN: , value = cisco.com 35 15:47:06.132 08/19/04 Sev=Info/5 IKE/0x6300000E  
MODE\_CFG\_REPLY: Attribute = APPLICATION\_VERSION, value = Cisco Internetwork Operating System  
Software IOS (tm) C1700 Software (C1700-K9O3SY7-M), Version 12.3(9a), RELEASE SOFTWARE (fc4)  
Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Fri 23-Jul-04 02:20 by kellythw 37  
15:47:06.171 08/19/04 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM \*(HASH, SA, NON, ID,  
ID) to 172.18.124.195 38 15:47:06.444 08/19/04 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet:  
peer = 172.18.124.195 39 15:47:06.454 08/19/04 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP

```
OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME from 172.18.124.195 40 15:47:06.454
08/19/04 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 3600 seconds 41
15:47:06.454 08/19/04 Sev=Info/5 IKE/0x63000045 RESPONDER-LIFETIME notify has value of 4608000
kb 42 15:47:06.454 08/19/04 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to
172.18.124.195 43 15:47:06.454 08/19/04 Sev=Info/5 IKE/0x63000058 Loading IPsec SA
(MsgID=83D109EC OUTBOUND SPI = 0x422186D5 INBOUND SPI = 0x5D94CB41) 44 15:47:06.454 08/19/04
Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x422186D5
```

```
45 15:47:06.454 08/19/04 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x5D94CB41
```

```
46 15:47:09.307 08/19/04 Sev=Info/4 IPSEC/0x63700014
Deleted all keys
```

```
47 15:47:09.307 08/19/04 Sev=Info/4 IPSEC/0x63700010
Created a new key structure
```

```
48 15:47:09.307 08/19/04 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xd5862142 into key list
```

```
49 15:47:09.307 08/19/04 Sev=Info/4 IPSEC/0x63700010
Created a new key structure
```

```
50 15:47:09.307 08/19/04 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x41cb945d into key list
```

```
51 15:47:09.307 08/19/04 Sev=Info/4 IPSEC/0x6370002E
Assigned VA private interface addr 10.50.50.2
```

```
52 15:47:16.568 08/19/04 Sev=Info/6 IKE/0x6300003D
Sending DPD request to 172.18.124.195, seq# = 2346900535
```

```
53 15:47:16.568 08/19/04 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 172.18.124.195
```

```
54 15:47:16.578 08/19/04 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 172.18.124.195
```

```
55 15:47:16.578 08/19/04 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK) from 172.18.124.195
```

```
56 15:47:16.578 08/19/04 Sev=Info/5 IKE/0x6300003F
Received DPD ACK from 172.18.124.195, seq# received = 2346900536,
seq# expected = 2346900536
```

## 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](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

**註：**發出debug指令之前，請先參閱有關Debug指令的重要資訊。

- **show crypto isakmp sa** — 顯示對等體上的所有當前網際網路金鑰交換(IKE)SA。

```
VPN1750#show crypto isakmp sa
dst          src          state          conn-id slot
172.18.124.195 172.18.173.80 QM_IDLE        3      0
!--- VPN Client. 172.18.124.195 172.18.124.197 QM_IDLE 2 0 !--- EzVPN between hub router and
```

PIX-506-B. 172.18.124.195 172.18.124.196 QM\_IDLE 1 0 !--- EzVPN between hub router and PIX-501.

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

```
VPN1750#show crypto ipsec sa
interface: FastEthernet0
  Crypto map tag: rtp, local addr. 172.18.124.195

protected vrf:
local ident (addr/mask/prot/port): (192.168.40.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 172.18.124.196:500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

  local crypto endpt.: 172.18.124.195, remote crypto endpt.:
172.18.124.196
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
  current outbound spi: DB79E16D

inbound esp sas:
  spi: 0xAF634F08(2942521096)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
    sa timing: remaining key lifetime (k/sec): (4433404/3282)
    IV size: 8 bytes
    replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0xDB79E16D(3682197869)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
    sa timing: remaining key lifetime (k/sec): (4433404/3282)
    IV size: 8 bytes
    replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:
local ident (addr/mask/prot/port): (172.18.124.195/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (50.50.50.7/255.255.255.255/0/0)
current_peer: 172.18.173.80:500
  PERMIT, flags={}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
#pkts decaps: 47, #pkts decrypt: 47, #pkts verify 47
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

  local crypto endpt.: 172.18.124.195, remote crypto endpt.:
```

```
172.18.173.80
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 72149A7D

inbound esp sas:
spi: 0x3467B12A(879210794)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2006, flow_id: 7, crypto map: rtp
sa timing: remaining key lifetime (k/sec): (4381078/3577)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x72149A7D(1913952893)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2007, flow_id: 8, crypto map: rtp
sa timing: remaining key lifetime (k/sec): (4381086/3577)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:
local ident (addr/mask/prot/port): (172.18.124.195/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.25.70.8/255.255.255.255/0/0)
current peer: 172.18.124.197:500
PERMIT, flags={}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.195, remote crypto endpt.:
172.18.124.197
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 2DE8E3C9

inbound esp sas:
spi: 0xED6381E5(3982721509)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: 3, crypto map: rtp
sa timing: remaining key lifetime (k/sec): (4561846/3283)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x2DE8E3C9(770237385)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
```



```
slot: 0, conn id: 2003, flow_id: 4, crypto map: rtp
sa timing: remaining key lifetime (k/sec): (4561846/3281)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

protected vrf:
local ident (addr/mask/prot/port): (172.18.124.195/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.18.124.197/255.255.255.255/0/0)
current_peer: 172.18.124.197:500
  PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.18.124.195, remote crypto endpt.:
172.18.124.197
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 87066AED

inbound esp sas:
spi: 0x8C8106A4(2357266084)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2004, flow_id: 5, crypto map: rtp
  sa timing: remaining key lifetime (k/sec): (4525643/3285)
  IV size: 8 bytes
  replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x87066AED(2265344749)
  transform: esp-3des esp-md5-hmac ,
  in use settings ={Tunnel, }
  slot: 0, conn id: 2005, flow_id: 6, crypto map: rtp
  sa timing: remaining key lifetime (k/sec): (4525643/3285)
  IV size: 8 bytes
  replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

## 相關資訊

- [排除PIX在已建立的IPSec隧道上傳遞資料流量的故障](#)
- [IP安全性疑難排解 — 瞭解和使用debug命令](#)
- [PIX 500系列防火牆產品支援頁](#)
- [IPSec技術支援頁面](#)
- [Cisco VPN使用者端支援頁面](#)
- [PIX命令參考](#)



- [要求建議 \(RFC\)](#)
- [RADIUS 支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)