

使用IPSec配置Cisco Secure PIX防火牆6.0和Cisco VPN客戶端

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[配置PIX](#)

[配置Cisco VPN客戶端](#)

[驗證](#)

[疑難排解](#)

[疑難排解指令](#)

[調試輸出示例](#)

[相關資訊](#)

簡介

Cisco Secure PIX防火牆軟體版本6.0和更高版本支援來自Cisco VPN客戶端3.x和4.x的連線。此示例配置顯示了兩個不同版本的VPN客戶端，它們連線並加密以PIX作為隧道端點的流量。在此配置中，地址池配置為分配給IP安全(IPSec)。

必要條件

需求

此示例配置假設PIX已經使用適當的靜態、管道或訪問清單運行。本文檔並非旨在說明這些基本概念，而是展示從Cisco VPN客戶端到PIX的連線。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本6.2(1)**注意**：此安裝程式已在PIX軟體版本6.2(1)上測試，但應能運行回到6.0(1)的早期版本以及更高版本。
- Cisco VPN使用者端版本3.6版本**注意**：此安裝程式已在VPN Client v4.0 Rel上測試，但應能運行回到3.0的早期版本和當前版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

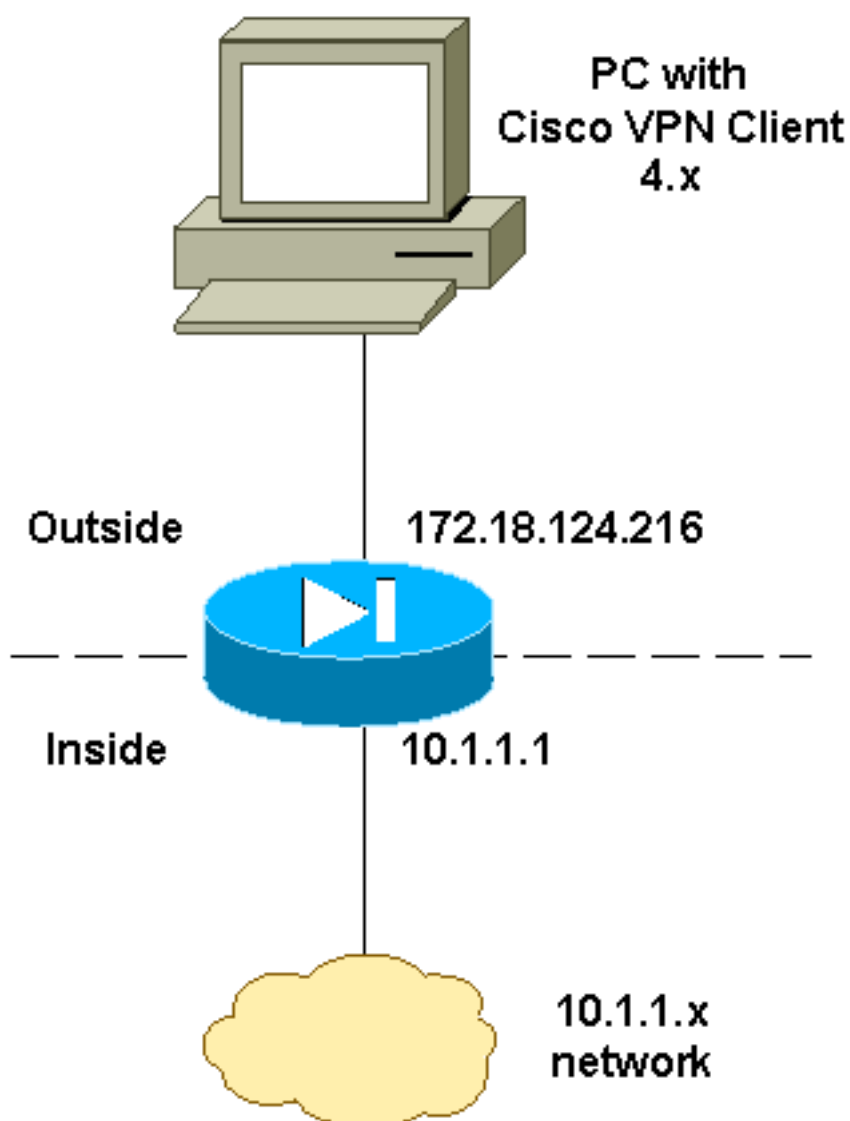
如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



配置PIX

註：使用[Command Lookup Tool](#)(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

```
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password OnTrBUG1Tp0edmkr encrypted
passwd 2KFQnbNlIdI.2KYOU encrypted
hostname goss-d3-pix515b
domain-name rtp.cisco.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 list to avoid Network Address Translation
(NAT) !--- on the IPSec packets. access-list 101 permit
ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
!
!--- IP addresses on the interfaces ip address outside
172.18.124.216 255.255.255.0 ip address inside 10.1.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm ip local pool ippool 10.1.2.1-10.1.2.254
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
!
!--- Binding ACL 101 to the NAT statement to avoid NAT
!--- on the IPSec packets. nat (inside) 0 access-list
101
!
!--- Default route to the Internet. 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 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 http
server enable http 1.2.3.5 255.255.255.255 inside no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable ! !--- The sysopt command avoids conduit !--- on
the IPSec encrypted traffic.

sysopt connection permit-ipsec
no sysopt route dnat
!
!--- Phase 2 encryption type crypto ipsec transform-set
myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
!
```

```

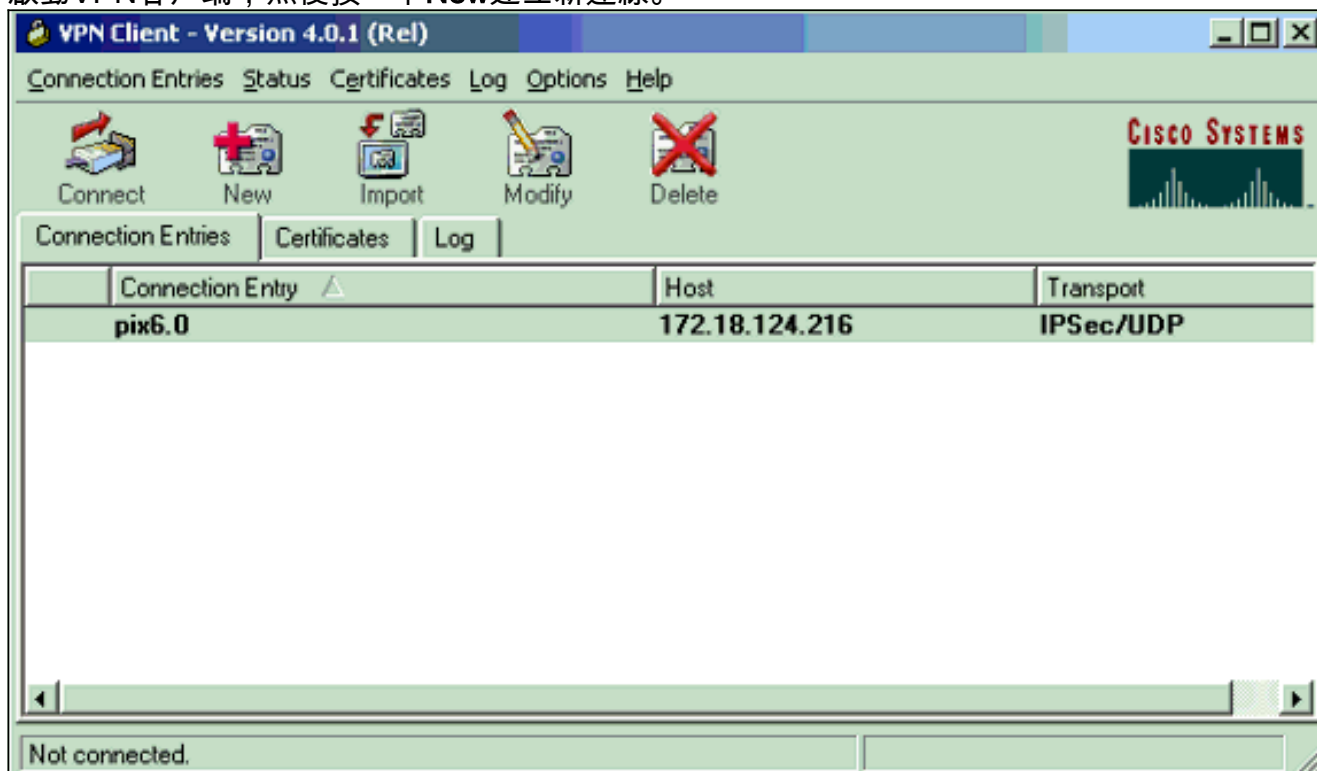
!--- Binding the IPsec engine on the outside interface.
crypto map mymap interface outside
!
!--- Enabling Internet Security Association and !--- Key
Management Protocol (ISAKMP) key exchange. isakmp enable
outside
isakmp identity address
!
!--- ISAKMP policy for VPN Client running 3.x or 4.x
code. isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
!--- IPsec group configuration for either VPN Client.
vpngroup vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password *****
!--- To allow simultaneous access to the !--- internal
network and to the Internet. vpngroup vpn3000 split-
tunnel 101
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:94da63fc0bb8ce167407b3ea21c6642c
: end
[OK]

```

配置Cisco VPN客戶端

完成以下步驟，以便使用VPN客戶端建立新連線。

1. 啟動VPN客戶端，然後按一下**New**建立新連線。



2. 輸入新連線的配置資訊。在Connection Entry欄位中，為您的條目分配一個名稱。在Host欄位中，輸入PIX公共介面的IP地址。選擇Authentication頁籤，然後輸入組和密碼（兩次 — 確認）。完成後，按一下「Save」。

VPN Client | Create New VPN Connection Entry

Connection Entry: pix6.0

Description:

Host: 172.18.124.216

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication

Name: vpn3000

Password: xxxxxxx

Confirm Password: xxxxxxx

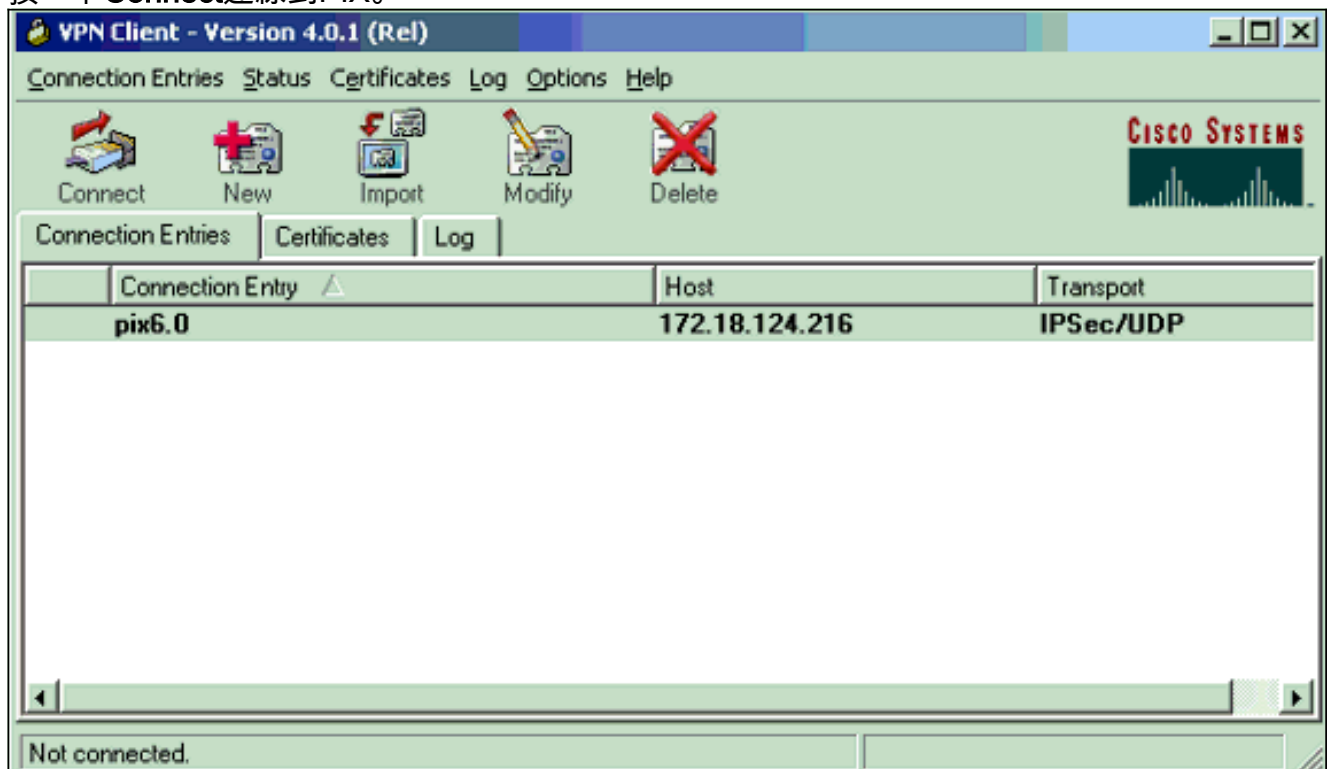
Certificate Authentication

Name:

Send CA Certificate Chain

Erase User Password | Save | Cancel

3. 按一下Connect連線到PIX。



驗證

使用本節內容，確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- `show crypto isakmp sa` — 檢視對等體上的所有當前網際網路金鑰交換(IKE)安全關聯(SA)。
- `show crypto ipsec sa` — 檢視當前SA使用的設定。

疑難排解

使用本節內容，對組態進行疑難排解。

疑難排解指令

附註：使用 `debug` 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- `debug crypto ipsec` — 用於檢視階段2的IPSec協商。
- `debug crypto isakmp` — 用於檢視階段1的ISAKMP協商。
- `debug crypto engine` — 顯示加密的流量。

調試輸出示例

以下是使用Cisco VPN 3.0.x使用者端產生的良好偵錯範例：

```
goss-d3-pix515b#debug crypto isakmp
goss-d3-pix515b#debug crypto ipsec
goss-d3-pix515b#debug crypto engine
goss-d3-pix515b#show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
    tx      Off
    rx      Off
    open    Off
    cable   Off
    txdmp   Off
    rxdmp   Off
    ifc     Off
    rxip    Off
    txip    Off
    get     Off
    put     Off
    verify  Off
    switch  Off
    fail    Off
    fmsg    Off
goss-d3-pix515b# goss-d3-pix515b#
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
```

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
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 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 7 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 8 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b

ISAKMP (0): atts are acceptable. Next payload is 0

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

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

ISAKMP (0): processing ID 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 a Unity client

ISAKMP: Created a peer node for 172.18.124.96

ISAKMP (0): ID payload

next-payload : 10

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 172.18.124.96, dest 172.18.124.216

OAK_AG exchange

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

ISAKMP (0): processing NOTIFY payload 24578 protocol 1

spi 0, message ID = 0

ISAKMP (0): processing notify INITIAL_CONTACT

IPSEC(key_engine): got a queue event...

IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP

IPSEC(key_engine_delete_sas): delete all SAs shared

with 172.18.124.96

ISAKMP (0): SA has been authenticated

return status is IKMP_NO_ERROR

crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216

ISAKMP_TRANSACTION exchange

ISAKMP (0:0): processing transaction payload

from 172.18.124.96. message ID = 0

ISAKMP: Config payload CFG_REQUEST

ISAKMP (0:0): checking request:

ISAKMP: attribute IP4_ADDRESS (1)

ISAKMP: attribute IP4_NETMASK (2)

ISAKMP: attribute IP4_DNS (3)

ISAKMP: attribute IP4_NBNS (4)

ISAKMP: attribute ADDRESS_EXPIRY (5)

Unsupported Attr: 5

ISAKMP: attribute APPLICATION_VERSION (7)

Unsupported Attr: 7

ISAKMP: attribute UNKNOWN (28672)

Unsupported Attr: 28672

ISAKMP: attribute UNKNOWN (28673)

Unsupported Attr: 28673

ISAKMP: attribute UNKNOWN (28674)

ISAKMP: attribute UNKNOWN (28676)

ISAKMP: attribute UNKNOWN (28679)

Unsupported Attr: 28679

ISAKMP (0:0): responding to peer config from 172.18.124.96.

ID = 525416177

return status is IKMP_NO_ERROR

crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216


```
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 805890102

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
    hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (1)
ISAKMP : Checking IPsec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-SHA
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
    hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (2)
ISAKMP : Checking IPsec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
    hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-SHA
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 3,
    hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
```

```
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPsec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-SHA
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans 2,
    hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (6)
ISAKMP : Checking IPsec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
    (key eng. msg.) dest= 172.18.124.216, src= 172.18.124.96,
    dest_proxy= 172.18.124.216/255.255.255.255/0/0 (type=1),
    src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 805890102

ISAKMP (0): processing ID payload. message ID = 805890102
ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 805890102
ISAKMP (0): ID_IPV4_ADDR dst 172.18.124.216 prot 0 port 0
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0x13b00d31(330304817) for SA
    from 172.18.124.96 to 172.18.124.216 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 935083707

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 1
map_alloc_entry: allocating entry 2
ISAKMP (0): Creating IPsec SAs
    inbound SA from 172.18.124.96 to 172.18.124.216
(proxy 10.1.2.1 to 172.18.124.216)
    has spi 330304817 and conn_id 1 and flags 4
    lifetime of 2147483 seconds
    outbound SA from 172.18.124.216 to 172.18.124.96
```

```
(proxy 172.18.124.216 to 10.1.2.1)
has spi 2130279708 and conn_id 2 and flags 4
lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.216, src= 172.18.124.96,
dest_proxy= 172.18.124.216/0.0.0.0/0/0 (type=1),
src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x13b00d31(330304817), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.216, dest= 172.18.124.96,
src_proxy= 172.18.124.216/0.0.0.0/0/0 (type=1),
dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x7ef97d1c(2130279708), conn_id= 2, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3
map_alloc_entry: allocating entry 4
```

ISAKMP (0): Creating IPsec SAs

```
inbound SA from 172.18.124.96 to 172.18.124.216
(proxy 10.1.2.1 to 0.0.0.0)
has spi 4139858833 and conn_id 3 and flags 4
lifetime of 2147483 seconds
outbound SA from 172.18.124.216 to 172.18.124.96 (
proxy 0.0.0.0 to 10.1.2.1)
has spi 1487433401 and conn_id 4 and flags 4
lifetime of 2147483 seconds
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.216, src= 172.18.124.96,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xf6IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.216, dest= 172.18.124.96,
src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x58a86eb9(1487433401), conn_id= 4, keysize= 0, flags= 0x4
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.96, dest 172.18.124.216
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
spi 0, message ID = 1617869510
ISAKMP (0): received DPD_R_U_THERE from peer 172.18.124.96
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
goss-d3-pix515b#
goss-d3-pix515b#
goss-d3-pix515b#no debug crypto isakmp
goss-d3-pix515b#no debug crypto ipsec
goss-d3-pix515b#no debug crypto engine
goss-d3-pix515b#
```

[相關資訊](#)

- [IPSec支援頁面](#)
- [Cisco Secure PIX防火牆命令參考](#)
- [Cisco PIX 500系列安全裝置支援頁面](#)
- [要求建議\(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)