瞭解並使用Debug命令對IPsec進行故障排除

目錄

簡介

本文檔介紹用於對Cisco IOS®軟體和PIX/ASA上的IPsec問題進行故障排除的常用調試命令。

背景資訊

請參閱最常見的L2L和遠端訪問IPsec VPN故障排除解決方案，瞭解最常見的IPsec VPN問題解決方案的資訊。

它包含常見步驟的清單，您可以在開始排除連線故障並致電思科技術支援之前嘗試這些步驟。

必要條件

需求

本檔案假設您已設定IPsec。有關詳細資訊，請參閱IPSec協商/IKE協定。

採用元件

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- **Cisco IOS®軟體**IPsec功能集。56i — 表示單一 **Data Encryption Standard (DES)** 功能(在Cisco IOS®軟體版本11.2及更高版本上)。k2 — 表示三重DES功能(在Cisco IOS®軟體版本12.0及更高版本上)。 Cisco 2600系列及更高版本提供三重DES。
- **PIX** – V5.0 以上版本，需要一重或三重 DES 授權金鑰才能啟用。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

Cisco IOS®軟體調試

本節中的主題介紹Cisco IOS®軟體debug命令。有關詳細資訊，請參閱IPSec協商/IKE協定。

show crypto isakmp sa

此命令顯示 **Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)** 在同儕之間構建。

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto ipsec sa

此命令顯示對等體之間構建的IPsec SA。加密的通道建立在10.1.0.1和10.1.0.2之間，適用於網路10.1.0.0和10.1.1.0之間的流量。

你可以看到兩個 **Encapsulating Security Payload (ESP)** SA構建入站和出站。由於沒有AH SA，因此未使用身份驗證報頭(AH)。

此輸出顯示 **show crypto ipsec sa** 指令。

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 10.1.0.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
    #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound esp sas:
      spi: 0x136A010F(325714191)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4608000/52)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
inbound pcp sas:
outbound esp sas:
   spi: 0x3D3(979)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4608000/52)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

show crypto engine connection active

此命令顯示所建立的每個階段2 SA和傳送的流量大小。

因為第2階段 **Security Associations (SAs)** 是單向的，每個SA只顯示一個方向的流量（加密為傳出，解密為傳入）。

debug crypto isakmp

此輸出顯示 **debug crypto isakmp** 指令。

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
encryption DES-CBC
      hash SHA
default group 2
auth pre-share
life type in seconds
life duration (basic) of 240
atts are acceptable. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipsec

此命令顯示IPsec隧道端點的源和目標。 **Src_proxy** 和 **dest_proxy** 是客戶端子網。

二 **sa created** 每個方向顯示一個消息。（如果執行ESP和AH，則會顯示四條消息。）

此輸出顯示 **debug crypto ipsec** 指令。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
```

```
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.2, dest= 10.1.0.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

錯誤消息示例

以下錯誤訊息範例是透過下列的**debug**指令產生的：

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

重播檢查失敗

此輸出顯示 **Replay Check Failed** 錯誤：

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

此錯誤是因為在傳輸媒體中重新排序（尤其是存在並行路徑時），或是在Cisco IOS®內處理的大型封包與小型封包以及負載下之封包路徑不相等所致。

更改轉換集以反映這一點。其 **reply check** 僅在以下情況下才顯示 **transform-set esp-md5-hmac** 已啟用。若要避免此錯誤訊息，請停用 **esp-md5-hmac** 並且僅執行加密。

請參閱Cisco錯誤IDCSCdp19680 (僅限註冊客戶)。

QM FSM錯誤

PIX防火牆或ASA上未啟動IPsec L2L VPN隧道，並顯示QM FSM錯誤消息。

一個可能的原因是代理身份，例如異常流量、 **Access Control List (ACL),** 或加密ACL時，兩端都不匹配。

檢查兩台裝置上的配置，並確保加密ACL匹配。

另一個可能的原因是轉換集引數不匹配。檢驗兩端的VPN網關使用具有完全相同引數的同一轉換集。

本地地址無效

以下輸出顯示錯誤消息示例：

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

此錯誤訊息歸因於以下兩個常見問題之一：

- 其 **crypto map map-name local-address interface-id** 命令會強制路由器使用指定的地址，從而導致路由器使用錯誤的地址作為標識。
- **Crypto map** 應用到錯誤的介面或根本不應用。檢查配置以確保將加密對映應用於正確的介面。

來自X.X.X.X的IKE消息未通過健全性檢查或格式不正確

如果對等體上的預共用金鑰不匹配，則會顯示此debug錯誤。要解決此問題，請檢查兩端的預共用金鑰。

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

主模式進程因對等項而失敗

以下是 **Main Mode** 錯誤消息。主模式的失敗表明兩端的階段1策略不匹配。

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

show crypto isakmp sa命令顯示ISAKMP SA位於 **MM_NO_STATE**.這也表示主模式已失敗。

```
dst      src        state     conn-id     slot
10.1.1.2  10.1.1.1   MM_NO_STATE    1           0
```

驗證階段1策略是否在對等體上，並確保所有屬性都匹配。

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

不支援代理標識

如果IPsec流量的訪問清單不匹配，則在調試中將顯示此消息。

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

每個對等體上的訪問清單需要相互映象（所有條目都需要可逆）。 此示例說明了這一點。

```
Peer A
```

```
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

不支援轉換建議

如果階段2(IPsec)在兩端都不匹配，則顯示此消息。如果轉換集不匹配或不相容，最常發生這種情況。

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

驗證轉換集是否與兩端匹配：

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

遠端對等項無證書無金鑰

此訊息表示路由器上設定的對等位址錯誤或已變更。驗證對等體地址是否正確以及是否可以到達該地址。

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

找不到對等地址X.X.X.X

此錯誤消息通常與 **VPN 3000 Concentrator** 錯誤消息 **Message: No proposal chosen(14)**.這是因為連線是主機到主機。

路由器配置中的IPsec提議順序為為路由器選擇的提議與訪問清單匹配，但不與對等體匹配。

訪問清單的網路更大，其中包含與流量交叉的主機。若要更正此問題，請將此集中器到路由器連線的路由器建議書排在第一行。

這樣可讓主機先與特定主機相符。

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

```
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

IPsec資料包的SPI無效

以下輸出是錯誤訊息的範例：

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

收到的IPsec資料包指定 **Security Parameters Index (SPI)** 在 **Security Associations Database (SADB)**.這可能是臨時情況，原因是：

- 年齡的細微差異 **Security Sssociations (SAs)** 在IPsec對等路由器之間
- 本地SA已被清除
- IPsec對等體傳送的資料包不正確

這可能是攻擊。

建議的操作：對等體可能未確認本地SA已被清除。如果從本地路由器建立新的連線，兩個對等體就可以成功重新建立。

否則，如果問題出現的時間超過了很短的時間，請嘗試建立新的連線或聯絡該對等體的管理員。

IPSEC(initialize_sas):代理ID無效

錯誤 **21:57:57: IPSEC(initialize_sas): invalid proxy IDs** 表示收到的代理標識與根據訪問清單配置的代理標識不匹配。

若要確保兩者相符，請檢查**debug**指令的輸出。

在建議書請求的**debug**命令輸出中，access-list 103 permit ip 10.1.1.0 0.0.0.255 10.1.0.0 0.0.255不匹配。

訪問清單一端是網路特定的，另一端是主機特定的。

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

有效負載5上非零保留

這表示ISAKMP金鑰不匹配。重新按鍵/重設以確保準確性。

提供的雜湊演算法與策略不匹配

如果配置的ISAKMP策略與遠端對等體提議的策略不匹配，路由器將嘗試預設策略65535。

如果兩者都不匹配，則ISAKMP協商失敗。

使用者收到 **Hash algorithm offered does not match policy!** 或 **Encryption algorithm offered does not match policy!** 路由器上的錯誤消息。

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Hash algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
=RouterB=
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 65535 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
ISAKMP (0:1): no offers accepted!
ISAKMP (0:1): phase 1 SA not acceptable!
```

HMAC驗證失敗

當驗證失敗時，將報告此錯誤消息 **Hash Message Authentication Code** 在IPsec資料包上。這通常發生在封包以任何方式損毀時。

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

如果偶爾遇到此錯誤消息，可以將其忽略。但是，如果這種情況越來越頻繁，則需要調查資料包損壞的來源。這可能是因為加密加速器存在缺陷。

遠端對等體沒有響應

當轉換集不匹配時，會遇到此錯誤消息。確保在兩個對等體上配置匹配的轉換集。

找到的所有 IPSec SA 協議均為不可接受

如果本機與遠端位置間的第 2 階段 IPSec 參數不符，就會顯示這則錯誤訊息。

為了解決這個問題，請在轉換組合指定相同的參數，讓兩者相符並成功建立 VPN。

封包加密/解密錯誤

以下輸出是錯誤訊息的範例：

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```
此錯誤消息可能是由於以下原因之一：

- 分段 — 分段加密資料包是進程交換的，這會強制在進程交換資料包之前將快速交換資料包傳送到VPN卡。

如果在進程交換資料包之前處理了足夠的快速交換資料包，則進程交換資料包的ESP或AH序列號將失效，當資料包到達VPN卡時，其序列號將位於重放視窗之外。

這會導致AH或ESP序列號錯誤（分別為4615和4612），具體取決於您使用的封裝。

- 過時的快取條目 — 另一個可能發生這種情況的情況是，當快速交換機快取條目過時時，第一個快取缺失的資料包會被進程交換。

因應措施

1. 關閉3DES轉換集上的任何型別的身份驗證，然後使用ESP-DES/3DES。這實際上會禁用身份驗證/反重播保護，從而防止出現與未排序（混合）IPsec流量相關的丟包錯誤 **%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615**.
2. 適用於此處所述原因的一種解決方法是設定 **Maximum Transmission Unit (MTU)** 小於1400位元組的入站流大小。輸入以下命令可將傳入流的最大傳輸單位(MTU)大小設定為小於1400位元組：
   ```
   ip tcp adjust-mss 1300
   ```
3. 禁用AIM卡。
4. 關閉路由器介面上的快速/CEF交換。若要移除快速交換，請在介面組態模式下使用以下命令：
   ```
   no ip route-cache
   ```

由於 ESP 序列失敗，所以封包收到錯誤訊息

以下提供錯誤訊息的範例：

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```
這則錯誤訊息通常表示這些可能的狀況之一：

- 由於 QoS 機制設定錯誤，導致加密路由器未按順序轉送 IPsec 加密封包。
- 由於中間裝置上的資料包重新排序，解密路由器接收的IPsec資料包順序混亂。
- 收到的 IPsec 封包遭到分段，需要在驗證與解密前進行重組。

因應措施

1. 在加密路由器或中繼路由器上停用 IPSec 流量的 QoS。
2. 在加密路由器上啟用 IPsec 預先分段。
   ```
   Router(config-if)#crypto ipsec fragmentation before-encryption
   ```
3. 將 MTU 值設為不會遭到分段的大小。
   ```
   Router(config)#interface type [slot_#/]port_#


   Router(config-if)#ip mtu MTU_size_in_bytes
   ```
4. 將Cisco IOS®映像升級為該系列中最新可用的穩定映像。

如果任何路由器上的MTU大小發生更改，則在該介面上終止的所有隧道都將關閉。

計畫在計畫停機時間內完成此解決方法。

嘗試在 7600 系列路由器上建立 VPN 通道時發生錯誤

如果您嘗試在 7600 系列路由器上建立 VPN 通道，就會收到這則錯誤訊息：

```
crypto_engine_select_crypto_engine: can't handle any more
```

由於 7600 系列路由器不支援軟體加密，因此出現這則錯誤訊息。7600 系列路由器不支援未含 IPsec SPA 硬體的 IPsec 通道終止程序。只有 7600 路由器中的 IPSEC-SPA 卡支援 VPN。

PIX調試

show crypto isakmp sa

此命令顯示對等體之間構建的ISAKMP SA。

```
dst      src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

在**show crypto isakmp** 輸出中，狀態必須始終為**QM_IDLE**。如果狀態為**MM_KEY_EXCH**，則表示配置的預共用金鑰不正確，或者對等體IP地址不同。

```
PIX(config)#show crypto isakmp sa
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

當您配置正確的IP地址或預共用金鑰時，可以糾正此問題。

show crypto ipsec sa

此命令顯示對等體之間構建的IPsec SA。在10.1.0.1和10.1.0.2之間為網路10.1.0.0和10.1.1.0之間的流量構建加密隧道。

您可以看到傳入和傳出內建的兩個ESP SA。由於沒有AH SA，因此未使用AH。

示例 **show crypto ipsec sa** 命令會顯示在此輸出中。

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (10.1.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.0.2/255.255.255.255/0/0)
   current_peer: 10.2.1.1
   dynamic allocated peer ip: 10.1.0.2
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
```

```
    #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.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound esp sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

此命令顯示有關IPsec連線的調試資訊，並顯示由於兩端的不相容而被拒絕的第一組屬性。

第二次嘗試匹配（嘗試使用3DES而非DES）， **Secure Hash Algorithm (SHA)** 是可接受的，並且已構建ISAKMP SA。

此偵錯也來自接受本地池中IP地址(10.32.8.1)的撥號客戶端。構建ISAKMP SA後，會協商IPsec屬性並將其視為可接受。

然後PIX設定IPsec SA，如下圖所示。此輸出顯示 **debug crypto isakmp** 指令。

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

此命令顯示有關IPsec連線的debug資訊。

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from  10.1.0.2  to  10.1.0.1
           (proxy 10.32.8.1 to  10.1.0.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  10.1.0.1  to  10.1.0.2
           (proxy 10.1.0.1 to 10.32.8.1)
        has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
           got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
```

```
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

常見的路由器到VPN客戶端問題

無法訪問VPN隧道之外的子網：分割通道

此路由器配置輸出示例說明如何為VPN連線啟用拆分隧道。

其 **split tunnel** 命令與 **crypto isakmp client configuration group hw-client-groupname** 指令。

這允許 **Cisco VPN Client** 使用路由器訪問不在VPN隧道中的其他子網。

這樣做不會影響IPsec連線的安全性。隧道在192.0.2.18網路上形成。

未加密的流量流向未在 **access list 150** 命令，如Internet。

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool
 acl 150
!
!
access-list 150 permit ip 192.0.2.18 0.0.0.127 any
!
```

常見PIX到VPN客戶端問題

本節中的主題介紹在VPN客戶端3.x的幫助下將PIX配置為IPsec時遇到的常見問題。PIX的配置示例基於6.x版。

通道建立後，流量不會流動：無法在PIX後面的網路內部Ping

這是與路由相關的常見問題。確保PIX具有位於內部且未直接連線到同一子網的網路的路由。

此外，內部網路需要具有返回PIX的路由，以查詢客戶端地址池中的地址。

此輸出顯示一個示例。

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on
the inside.

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1
```

```
 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client
for the IPsec session.

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then
the router needs to have route !--- for 10.1.2.0/24 network with next hop as the PIX inside
interface !.

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

通道開啟後，使用者無法瀏覽網際網路：分割通道

此問題最常見的原因是，使用從VPN客戶端到PIX的IPsec隧道，所有流量都通過隧道傳送到PIX防火牆。

PIX功能不允許將流量傳送回接收流量的介面。因此，目的地為Internet的流量不起作用。

要解決此問題，請使用 **split tunnel** 指令。此修復程式的思想是，只有一個人通過隧道傳送特定流量，其餘流量直接到達Internet，而不是通過隧道。

```
vpngroup vpn3000 split-tunnel 90
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

其 **vpngroup vpn3000 split-tunnel 90** 命令啟用拆分隧道 **access-list number 90**.

其 **access-list number 90** 命令定義哪些流量流經通道，其餘流量在存取清單結尾被拒絕。

要拒絕，訪問清單必須相同 **Network Address Translation (NAT)** 在PIX上。

通道開啟後，某些應用無法運作：使用者端上的MTU調整

建立隧道後，雖然您可以ping通PIX防火牆後面的網路上的電腦，但是您無法使用某些應用程式，如Microsoft **Outlook**.

一個常見問題是封包的最大傳輸單位(MTU)大小。IPsec報頭最多可以是50到60個位元組，它們將新增到原始資料包中。

如果封包大小大於1500（Internet的預設值），則裝置需要將其分段。新增IPsec報頭後，大小仍低於1496，這是IPsec的最大值。

其 **show interface** 命令會顯示可訪問的路由器或您自己的內部路由器上該特定介面的MTU。

為了確定從源到目的地的整個路徑的MTU，會隨同傳送各種大小的資料包 **Do Not Fragment (DF)** 設定此位元後，如果傳送的資料包大於MTU，則會將此錯誤消息傳送回源：

```
frag. needed and DF set
```

以下輸出顯示如何尋找IP位址為10.1.1.2和172.16.1.56的主機之間路徑的MTU的範例。

```
Router#debug ip icmp
ICMP packet debugging is on
```

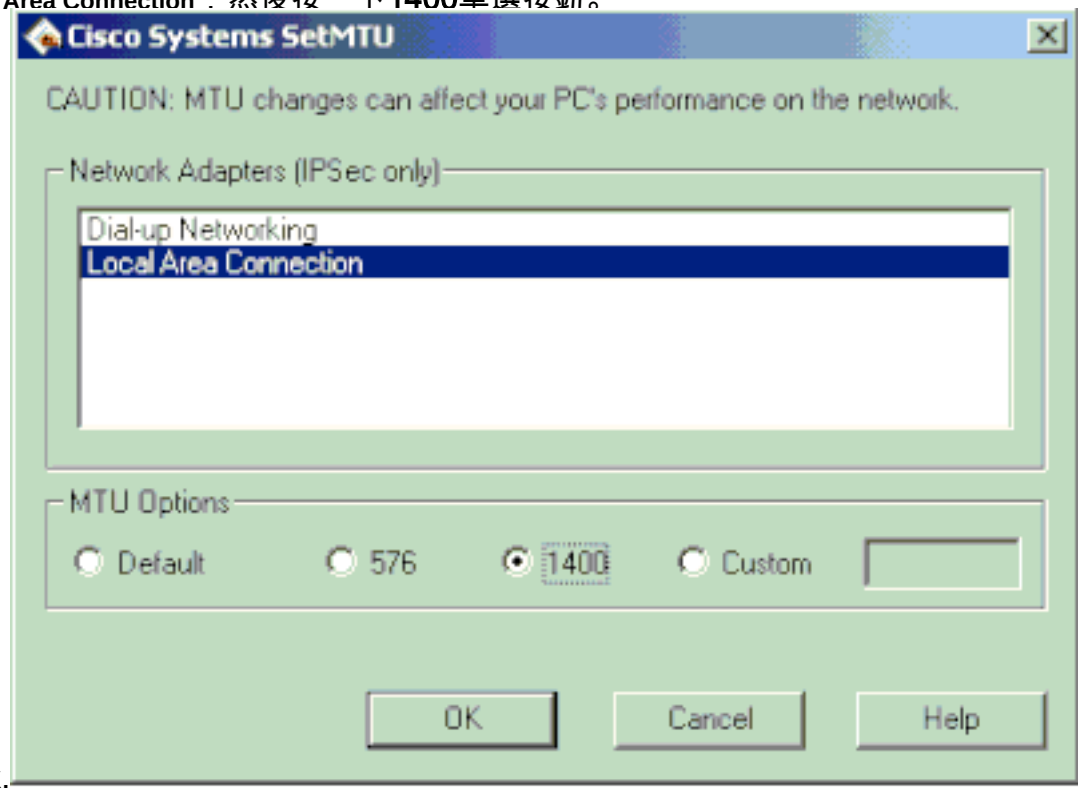
```
!--- Perform an extended ping.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1550
Timeout in seconds [2]:


!--- Make sure you enter y for extended commands.

Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:


!--- Set the DF bit as shown.


Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

VPN客戶端附帶一個MTU調整實用程式，允許使用者調整Cisco VPN客戶端的MTU。

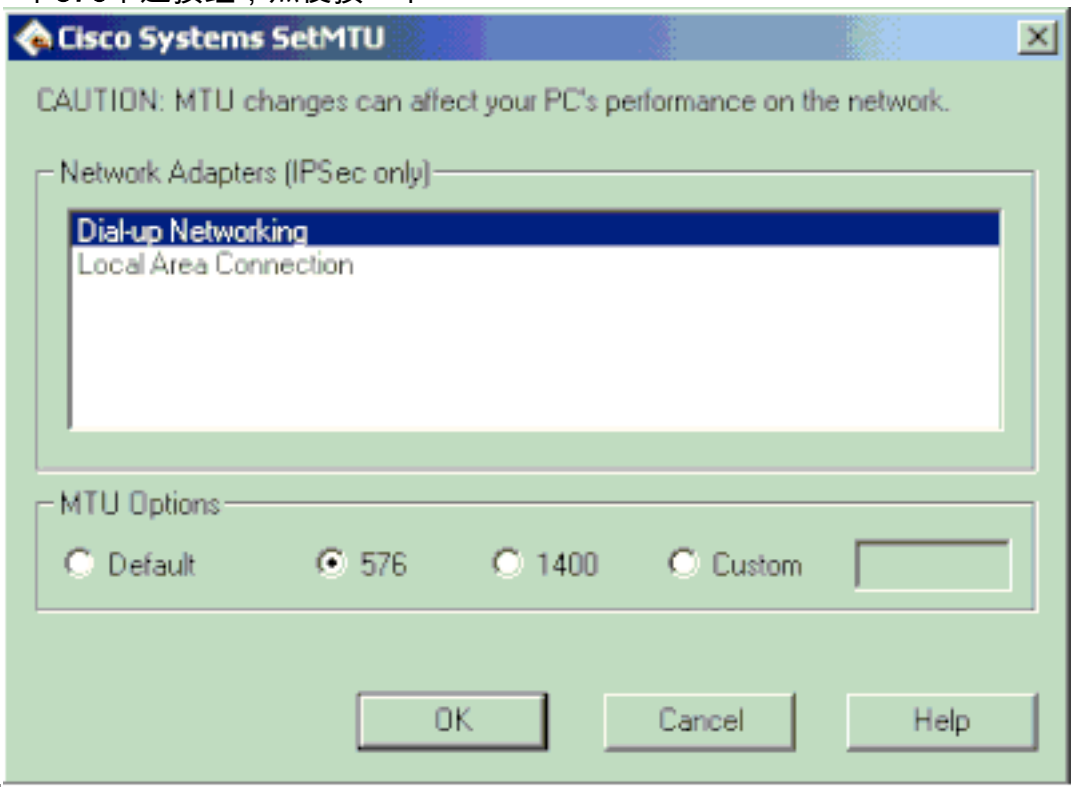
在使用乙太網(PPPoE)客戶端使用者的情況下，調整PPPoE介面卡的MTU。

完成以下步驟以調整VPN客戶端的MTU實用程式。

1. 選擇 **Start > Programs > Cisco System VPN Client > Set MTU.**
2. 選擇 **Local Area Connection** ，然後按一下1400單選按鈕。



3. 按一下 **OK.**
4. 重複步驟1，然後選擇 **Dial-up Networking.**
5. 按一下576單選按鈕，然後按一下 **OK.**



缺少sysopt命令

使用 **sysopt connection permit-ipsec** 命令，以允許IPsec流量通過PIX防火牆，而不檢查以下內容 **conduit** 或 **access-list** 命令語句。

預設情況下，任何入站會話都必須由 **conduit** 或 **access-list** 命令語句。使用IPsec保護的流量時，輔助訪問清單檢查可以是冗餘的。

要始終允許IPsec身份驗證/加密入站會話，請使用 **sysopt connection permit-ipsec** 指令。

驗證存取控制清單(ACL)

典型IPsec VPN配置中使用了兩個訪問清單。

一個訪問清單用於將目的地為VPN隧道的流量從NAT進程中免除。

另一個存取清單定義要加密的流量。這包括LAN到LAN設定中的加密ACL或遠端存取設定中的分割通道ACL。

當這些ACL配置錯誤或遺漏時，流量可能僅沿一個方向流過VPN隧道，或者根本沒有通過隧道傳送。

請確保您已配置完成IPsec VPN配置所需的所有訪問清單，並且這些訪問清單定義了正確的流量。

當您懷疑ACL是您的IPsec VPN出現問題的原因時，此清單包含要檢查的專案。

- 確保NAT豁免和加密ACL指定正確的流量。
- 如果您有多個VPN通道和多個加密ACL，請確保這些ACL不會重疊。
- 請勿使用ACL兩次。即使NAT免除ACL和加密ACL指定了相同的流量，也可使用兩個不同的訪問清單。
- 確保您的裝置配置為使用NAT免除ACL。也就是說，使用 **route-map** 命令；使用 **nat (0)** 命令。LAN到LAN和遠端訪問配置均需要NAT免除ACL。

要詳細瞭解如何驗證ACL語句，請參閱最常見的L2L和遠端訪問IPsec VPN故障排除解決方案中的驗證ACL是否正確部分。

相關資訊

- **IPsec協商/IKE通訊協定支援頁面**
- **PIX支援頁**
- **技術筆記**
- **技術支援與文件 - Cisco Systems**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。