使用PSK的站點到站點VPN的IOS IKEv2調試故障排除

目錄

簡介

本檔案介紹使用非共用金鑰(PSK)時，Cisco IOS®上的網際網路金鑰交換版本2(IKEv2)偵錯。

必要條件

需求

思科建議您瞭解IKEv2的資料包交換。有關詳細資訊，請參閱IKEv2資料包交換和協定級別調試。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 網際網路金鑰交換版本2(IKEv2)
- Cisco IOS 15.1(1)T或更高版本

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。如果您的網路運作中，請確保您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。

背景資訊

本文提供如何在組態中轉譯特定偵錯行的資訊。

核心問題

IKEv2中的資料包交換與IKEv1中的資料包交換截然不同。在IKEv1中，有一個明確劃分的階段1交換，由六(6)個資料包組成，之後的一個階段2交換由三(3)個資料包組成；IKEv2交換是可變的。有關差異的詳細資訊以及資料包交換的說明，請再次參閱IKEv2資料包交換和協定級別調試。

路由器配置

本節列出本文檔中使用的配置。

路由器1

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.2
 tunnel protection ipsec profile phse2-prof
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0

crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 policy site-pol
 proposal PHASE1-prop
!
crypto ikev2 keyring KEYRNG
 peer peer1
  address 10.0.0.2 255.255.255.0
  hostname host1
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
```

```
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
ip route 192.168.2.1 255.255.255.255 Tunnel0
```

路由器2

```
crypto ikev2 proposal PHASE1-prop
 encryption 3des aes-cbc-128
 integrity sha1
 group 2
!
crypto ikev2 keyring KEYRNG
 peer peer2
  address 10.0.0.1 255.255.255.0
  hostname host2
  pre-shared-key local cisco
  pre-shared-key remote cisco
 !
crypto ikev2 profile IKEV2-SETUP
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRNG
 lifetime 120
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
!
crypto ipsec profile phse2-prof
 set transform-set TS
 set ikev2-profile IKEV2-SETUP
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
interface Tunnel0
 ip address 172.16.0.102 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.1
 tunnel protection ipsec profile phse2-prof
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.1 255.255.255.255 Tunnel0
```

疑難排解

路由器調試

本檔案中使用了以下debug指令：

```
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Router 1(Initiator)消息說明	調試
路由器1收到與對等體ASA 10.0.0.2的加密acl匹配的資料包。啟動SA建立	*11月11日20:28:34.003: IKEv2：收到來自排程器的資料包 *11月11日20:28:34.003:IKEv2：正在處理pak隊列中的專案 *11月11日19:30:34.811:IKEv2:%按地址10.0.0.2獲取預共用金鑰 *11月11日19:30:34.811:IKEv2：將建議方案PHASE1-prop新增到工具包策略 *11月11日19:30:34.811:IKEv2:(1)：選擇IKE配置檔案IKEV2-SETUP *11月11日19:30:34.811:IKEv2：已允許新的ikev2 sa請求 *11月11日19:30:34.811:IKEv2：將傳出協商sa計數增加1
第一對消息是IKE_SA_INIT交換。這些消息協商加密演算法、交換金鑰並執行Diffie-Hellman交換。 相關配置： `crypto ikev2建議 PHASE1-prop encryption 3des aes-cbc-128 integrity sha1組2crypto ikev2 keyring KEYRNG peer1 address 10.0.0.2 255.255.255.0 hostname host1 pre-shared-key local cisco pre-shared-key remote cisco`	*Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState：空閒事件： EV_INIT_SA *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件： EV_GET_IKE_POLICY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件：EV_SET_POLICY *11月11日19:30:34.811:IKEv2:(SA ID = 1)：設定配置的策略 *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件： EV_CHK_AUTH4PKI *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件：EV_GEN_DH_KEY *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件： EV_NO_EVENT *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件： EV_OK_RECD_DH_PUBKEY_RESP *11月11日19:30:34.811:IKEv2:(SA ID = 1)：操作：Action_Null *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 00000 CurState: I_BLD_INIT事件： EV_GET_CONFIG_MODE

	*11月11日19:30:34.811: IKEv2:IKEv2啟動器 — 沒有配置資料要在IKE_SA_INIT交換中傳送 *11月11日19:30:34.811:IKEv2：沒有配置資料傳送到工具包： *Nov 11 19:30:34.811: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=0000000000000000(I)MsgID = 000000 CurState: I_BLD_INIT事件： EV_BLD_MSG *11月11日19:30:34.811:IKEv2：構建供應商特定負載：DELETE-REASON *11月11日19:30:34.811:IKEv2：構建供應商特定負載：（自定義） *11月11日19:30:34.811:IKEv2：構建通知負載：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.811:IKEv2：構建通知負載：NAT_DETECTION_DESTINATION_IP
正在生成IKE_INIT_SA資料包的啟動器。它包含：ISAKMP Header(SPI/version/flags)、SAi1（IKE發起程式支援的加密演算法）、KEi（發起程式的DH公鑰值）和N（發起程式編號）。	*11月11日19:30:34.811: IKEv2:(SA ID = 1)：下一個負載：SA，版本：2.0交型別：IKE_SA_INIT，標誌：INITIATOR消息id:0，長度：344 負載內容： SA下一個負載：KE，保留：0x0，長度：56 最後一個建議：0x0，保留：0x0，長度：52 方案：1，協定ID:IKE，SPI大小：0,#trans:5上次轉換：0x3，保留：0x0：長度：8 型別：1，保留：0x0,id:3DES 上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：4，保留：0x0,id:DH_GROUP_1024_MODP/組2 KE下一個負載：N，保留：0x0，長度：136 DH組：2，保留：0x0 N下一個負載：VID，保留：0x0，長度：24 VID下一負載：VID，保留：0x0，長度：23 VID Next負載：NOTIFY，保留：0x0，長度：21 NOTIFY(NAT_DETECTION_SOURCE_IP)下一個負載：通知，保留：0x0，長度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一個負載：無，保留：0x0，長度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_DESTINATION_
----------Initiator sent IKE_INIT_SA ---------->	
	*11月11日19:30:34.814: IKEv2：收到來自排程器的資料包 *11月11日19:30:34.814:IKEv2：正在處理pak隊列中的專案 *11月11日19:30:34.814:IKEv2：允許新的ikev2 sa請求 *11月11日19:30:34.814:IKEv2：將傳入協商sa計數增加1

	*11月11日19:30:34.814: IKEv2：下一個負載：SA，版本：2.0交換型別 ：IKE_SA_INIT，標誌：啟動器消息id:0，長度：344 負載內容： SA下一個負載：KE，保留：0x0，長度：56 最後一個建議：0x0，保留：0x0，長度：52 方案：1，協定ID:IKE，SPI大小：0,#trans:5上次轉換：0x3，保留：0x0： 度：8 型別：1，保留：0x0,id:3DES 上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：4，保留：0x0,id:DH_GROUP_1024_MODP/組2 KE下一個負載：N，保留：0x0，長度：136 DH組：2，保留：0x0 N下一個負載：VID，保留：0x0，長度：24 *11月11日19:30:34.814: IKEv2：分析供應商特定負載：CISCO-DELETE- REASON VID下一個負載：VID，保留：0x0，長度：23 *11月11日19:30:34.814: IKEv2：分析供應商特定負載：（自定義）VID下一 載：通知，保留： 0x0，長度： 21 *11月11日19:30:34.814: IKEv2：解析通知負載 ：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP)下一個負載：通知，保留：0x0， 度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.814: IKEv2：解析通知負載 ：NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一個負載：無，保留 ：0x0，長度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_DESTINATION_
	*11月11日19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState：空閒事件：EV_RECV_INIT *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: R_INIT事件：EV_VERIFY_MSG *Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: R_INIT事件：EV_INSERT_SA *11月11日19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:

I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_INIT事件：EV_GET_IKE_POLICY
*11月11日19:30:34.814:IKEv2：將建議預設新增到工具包策略
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_INIT事件：EV_PROC_MSG
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_INIT事件： EV_DETECT_NAT
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：處理NAT發現通知
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：處理nat detect src notify
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：遠端地址匹配
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：正在處理nat檢測dst通知
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：本地地址匹配
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：未找到NAT
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_INIT事件： EV_CHK_CONFIG_MODE
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件： EV_SET_POLICY
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：設定配置的策略
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件： EV_CHK_AUTH PKI
*Nov 11 19:30:34.814: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件： EV_PKI_SESH未解決
*11月11日19:30:34.814:IKEv2:(SA ID = 1)：開啟PKI會話
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件：EV_GEN_DH_GEN金鑰(_K)
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件： EV_NO_EVENT
*11月11日19:30:34.815: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件：EV_OK_RECK d_DH_PUBKEY_RE
*11月11日19:30:34.815:IKEv2:(SA ID = 1)：操作：Action_Null
*Nov 11 19:30:34.815: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件：EV_GEN_DH_GEN密碼(_S)
*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID =
00000000 CurState: R_BLD_INIT事件： EV_NO_EVENT

	*11月11日19:30:34.822:IKEv2:% 按地址10.0.0.1獲取預共用金鑰 *11月11日19:30:34.822:IKEv2：將建議預設新增到工具包策略 *11月11日19:30:34.822:IKEv2:(2)：選擇IKE配置檔案IKEV2-SETUP *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: R_BLD_INIT事件： EV_OK_RECD DH_SECRET_RES *11月11日19:30:34.822:IKEv2:(SA ID = 1)：操作：Action_Null *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: R_BLD_INIT事件：EV_GEN_S金鑰ID *11月11日19:30:34.822:IKEv2:(SA ID = 1)：生成skyid *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: R_BLD_INIT事件： EV_GET_CONFIG模式 *11月11日19:30:34.822: IKEv2:IKEv2響應器 — 沒有配置資料要在 IKE_SA_INIT交換中傳送 *11月11日19:30:34.822:IKEv2：沒有配置資料傳送到工具包： *11月11日19:30:34.822:IKEv2:(SA ID = 1):SM跟蹤 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState:R_BLD_INIT事件： EV_MSG *11月11日19:30:34.822:IKEv2：構建供應商特定負載：DELETE-REASON *11月11日19:30:34.822:IKEv2：構建供應商特定負載：（自定義） *11月11日19:30:34.822:IKEv2：構建通知負載 ：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.822:IKEv2：構建通知負載 ：NAT_DETECTION_DESTINATION_IP *11月11日19:30:34.822:IKEv2：構建通知負載 ：HTTP_CERT_LOOKUP_SUPPORTED
	*11月11日19:30:34.822:IKEv2:(SA ID = 1)：下一個負載：SA，版本：2.0交 型別：IKE_SA_INIT，標誌：RESPONDER MSG-RESPONSE Message id:0，長度：449 負載內容： SA下一個負載：KE，保留：0x0，長度：48 最後一個建議：0x0，保留：0x0，長度：44 方案：1，協定ID:IKE，SPI大小：0,#trans:4上次轉換：0x3，保留：0x0： 度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：4，保留：0x0,id:DH_GROUP_1024_MODP/組2 KE下一個負載：N，保留：0x0，長度：136

	DH組：2，保留：0x0 N 下一個負載：VID，保留：0x0，長度：24 VID下一負載：VID，保留：0x0，長度：23 VID Next負載：NOTIFY，保留：0x0，長度：21 NOTIFY(NAT_DETECTION_SOURCE_IP)下一個負載：通知，保留：0x0， 度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一個負載：CERTREQ， 留：0x0，長度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_DESTINATION_ CERTREQ下一個負載：NOTIFY，保留：0x0，長度：105 證書編碼PKIX的雜湊和URL NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)下一個負載：無，保留 ：0x0，長度：8 安全協定ID:IKE，spi大小：0，型別 ：HTTP_CERT_LOOKUP_SUPPORTED	
	*Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: INIT_DONE事件： EV_DONE *11月11日19:30:34.822:IKEv2:(SA ID = 1):Cisco DeleteReason Notify已啟用 *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: INIT_DONE事件： EV_CHK4_ROLE *11月11日19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: INIT_DONE事件：EV_START_TMR *Nov 11 19:30:34.822: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000000 CurState: R_WAIT_AUTH事件： EV_NO_EVENT *11月11日19:30:34.822:IKEv2：新的ikev2 sa請求已接受 *11月11日19:30:34.822:IKEv2：將傳出協商服務計數增加1	
<----------Responder已傳送IKE_INIT_SA命----------		
路由器1收到來自路由器2的IKE_SA_INIT響應資料包。	*11月11日19:30:34.823: IKEv2：收到來自排程器的資料包 *11月11日19:30:34.823: IKEv2：收到來自排程器的資料包 *11月11日19:30:34.823:IKEv2：正在處理pak隊列中的專案	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000000 CurState: INIT_DONE事 ：EV_START_TMR。

Router1驗證並處理回應：(1)計算啟動器DH金鑰，以及(2)也生成啟動器DH金鑰。	*11月11日19:30:34.823: IKEv2:(SA ID = 1)：下一個負載：SA，版本：2.0交 型別：IKE_SA_INIT，標誌：RESPONDER MSG-RESPONSE Message id:0，長度：449 負載內容： SA下一個負載：KE，保留：0x0，長度：48 最後一個建議：0x0，保留：0x0，長度：44 方案：1，協定ID:IKE，SPI大小：0,#trans:4上次轉換：0x3，保留：0x0： 度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：4，保留：0x0,id:DH_GROUP_1024_MODP/組2 KE下一個負載：N，保留：0x0，長度：136 DH組：2，保留：0x0 N 下一個負載：VID，保留：0x0，長度：24 *11月11日19:30:34.823: IKEv2：分析供應商特定負載：CISCO-DELETE- REASON VID下一個負載：VID，保留：0x0，長度：23 *11月11日19:30:34.823: IKEv2：分析供應商特定負載：（自定義）VID下一 載：通知，保留： 0x0，長度： 21 *11月11日19:30:34.823: IKEv2：解析通知負載 ：NAT_DETECTION_SOURCE_IP NOTIFY(NAT_DETECTION_SOURCE_IP)下一個負載：通知，保留：0x0， 度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_SOURCE_IP *11月11日19:30:34.824: IKEv2：解析通知負載 ：NAT_DETECTION_DESTINATION_IP NOTIFY(NAT_DETECTION_DESTINATION_IP)下一個負載：CERTREQ， 留：0x0，長度：28 安全協定ID:IKE，spi大小：0，型別：NAT_DETECTION_DESTINATION_ CERTREQ下一個負載：NOTIFY，保留：0x0，長度：105 證書編碼PKIX的雜湊和URL *11月11日19:30:34.824: IKEv2：解析通知負載 ：HTTP_CERT_LOOKUP_SUPPORTED NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)下一個負載：無，保留 ：0x0，長度：8 安全協定ID:IKE，spi大小：0，型別 ：HTTP_CERT_LOOKUP_SUPPORTED

	*Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_WAIT_INIT事件： EV_RECV_INIT *11月11日19:30:34.824: IKEv2:(SA ID = 1)：正在處理IKE_SA_INIT消息 *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_CHK_NOTIFY *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_VERIFY_MSG *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_PROC_MSG *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_DETECT_NAT *11月11日19:30:34.824:IKEv2:(SA ID = 1)：處理NAT發現通知 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：處理nat detect src notify *11月11日19:30:34.824:IKEv2:(SA ID = 1)：遠端地址匹配 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：正在處理nat檢測dst通知 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：本地地址匹配 *11月11日19:30:34.824:IKEv2:(SA ID = 1)：未找到NAT *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_CHK_NAT T *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_PROC_INIT事件： EV_CHK_CONFIG模式 *Nov 11 19:30:34.824: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件：EV_GEN_DH_SECRET B.C. *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件： EV_NO_EVENT *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件： EV_OK_RECD_DH SECRET_RESP *11月11日19:30:34.831:IKEv2:(SA ID = 1)：操作：Action_Null *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件：EV_GEN_SKEY *11月11日19:30:34.831: IKEv2:(SA ID = 1)：生成skyid *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件： EV_DONE

	*11月11日19:30:34.831:IKEv2:(SA ID = 1):Cisco DeleteReason Notify已啟用 *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: INIT_DONE事件： EV_CHK4_ROLE *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_BLD_AUTH事件： EV_GET_CONFIG模式 *11月11日19:30:34.831:IKEv2：將配置資料傳送到工具包 *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_BLD_AUTH事件： EV_CHK_EAP
發起方啟動IKE_AUTH交換並生成身份驗證負載。IKE_AUTH封包包含：ISAKMP標頭（SPI/版本/標誌）、IDi（發起者身分）、AUTH負載、SAi2（在IKEv1中發起類似於階段2轉換集交換的SA），以及TSi和TSr（發起者和響應者流量選擇器）。它們分別包含用於轉發/接收加密流量的發起方和響應方的源地址和目的地址。地址範圍指定所有進出該範圍的流量都通過隧道傳輸。如果響應方可以接受該建議，它將傳送相同的TS負載作為回應。為與觸發資料包匹配的proxy_ID對建立第一個CHILD_SA。 相關配置： `crypto ipsec transform-set TS esp-3des esp-sha-hmac crypto ipsec profile phse2-prof set transform-set TS set ikev2-profile IKEV2-SETUP`	*Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_BLD_AUTH事件：EV_GEN_AUTH B.C. *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_BLD_AUTH事件： EV_CHK_AUTH型別 *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_BLD_AUTH事件： EV_OK_AUTH GEN *Nov 11 19:30:34.831: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000000 CurState: I_BLD_AUTH事件： EV_SEND_AUTH *11月11日19:30:34.831:IKEv2：構建供應商特定負載：思科 — 花崗岩 *11月11日19:30:34.831:IKEv2：構建通知負載：INITIAL_CONTACT *11月11日19:30:34.831:IKEv2：構建通知負載：SET_WINDOW_SIZE *11月11日19:30:34.831:IKEv2：構建通知負載：ESP_TFC_NO_SUPPORT *11月11日19:30:34.831:IKEv2：構建通知負載：NON_FIRST_FRAGS 負載內容： VID下一負載：IDi，保留：0x0，長度：20 IDi下一個負載：身份驗證，保留：0x0，長度：12 Id型別：IPv4地址，保留：0x0 0x0 AUTH Next payload: CFG， reserved: 0x0, length: 28 身份驗證方法PSK，保留： 0x0，保留0x0 CFG下一個負載：SA，保留：0x0，長度：309 cfg型別：CFG_REQUEST，保留：0x0，保留：0x0 *11月11日19:30:34.831:SA下一個負載：TSi，保留：0x0，長度：40 最後一個建議：0x0，保留：0x0，長度：36 方案：1，協定ID:ESP，SPI大小：4,#trans:3上次轉換：0x3，保留：0x0：長度：8 型別：1，保留：0x0,id:3DES 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96

	上次轉換：0x0，保留：0x0：長度：8 型別：5，保留：0x0,id：不使用ESN TSi下一個負載：TSr，保留：0x0，長度：24 TS數：1，保留0x0，保留0x0 TS型別：TS_IPV4_ADDR_RANGE，proto id:0，長度：16 起始埠：0，結束埠：65535 開始地址：0.0.0.0，結束地址：255.255.255.255 TSr下一個負載：NOTIFY，保留：0x0，長度：24 TS數：1，保留0x0，保留0x0 TS型別：TS_IPV4_ADDR_RANGE，proto id:0，長度：16 起始埠：0，結束埠：65535 開始地址：0.0.0.0，結束地址：255.255.255.255 NOTIFY(INITIAL_CONTACT)下一個負載：NOTIFY，保留：0x0，長度：8 安全協定ID:IKE，spi大小：0，型別：INITIAL_CONTACT NOTIFY(SET_WINDOW_SIZE)下一負載：NOTIFY，保留：0x0，長度：12 安全協定ID:IKE，spi大小：0，型別：SET_WINDOW_SIZE NOTIFY(ESP_TFC_NO_SUPPORT)下一個負載：通知，保留：0x0，長度： 安全協定ID:IKE，spi大小：0，型別：ESP_TFC_NO_SUPPORT NOTIFY(NON_FIRST_FRAGS)下一個負載：無，保留：0x0，長度：8 安全協定ID:IKE，spi大小：0，型別：NON_FIRST_FRAGS *11月11日19:30:34.832: IKEv2:(SA ID = 1)：下一個負載：ENCR，版本： 2.0交換型別：IKE_AUTH，標誌： INITIATOR消息ID:1，長度：556 負載內容： ENCR下一個負載：VID，保留：0x0，長度：528 *11月11日19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 0000 CurState: I_WAIT_AUTH事件：EV_NO_EVENT
----------發起程式已傳送IKE_AUTH ---------->	
	*11月11日19:30:34.832: IKEv2：收到來自排程器的資料包 *11月11日19:30:34.832:IKEv2：正在處理pak隊列中的專案 *11月11日19:30:34.832: IKEv2:(SA ID = 1)：請求具有mess_id 1；預期為1至 *11月11日19:30:34.832: IKEv2:(SA ID = 1)：下一個負載：ENCR，版本： 2.0交換型別： IKE_AUTH，標誌： INITIATOR消息ID:1，長度：556 負載內容： *11月11日19:30:34.832: IKEv2：分析供應商特定負載：（自定義）VID下一 載： IDi，保留： 0x0，長度： 20 IDi下一個負載：身份驗證，保留：0x0，長度：12 Id型別：IPv4地址，保留：0x0 0x0 AUTH下一個負載：CFG，保留：0x0，長度：28 身份驗證方法PSK，保留： 0x0，保留0x0 CFG下一個負載：SA，保留：0x0，長度：309

	cfg型別：CFG_REQUEST，保留：0x0，保留：0x0 *11月11日19:30:34.832：屬性型別：內部IP4 DNS，長度：0 *11月11日19:30:34.832：屬性型別：內部IP4 DNS，長度：0 *11月11日19:30:34.832：屬性型別：內部IP4 NBNS，長度：0 *11月11日19:30:34.832：屬性型別：內部IP4 NBNS，長度：0 *11月11日19:30:34.832：屬性型別：內部IP4子網，長度：0 *11月11日19:30:34.832：屬性型別：應用程式版本，長度：257 屬性型別：未知 — 28675，長度：0 *11月11日19:30:34.832：屬性型別：未知 — 28672，長度：0 *11月11日19:30:34.832：屬性型別：未知 — 28692，長度：0 *11月11日19:30:34.832：屬性型別：未知 — 28681，長度：0 *11月11日19:30:34.832：屬性型別：未知 — 28674，長度：0 *11月11日19:30:34.832: SA下一個負載：TSi，保留：0x0，長度：40 最後一個建議：0x0，保留：0x0，長度：36 方案：1，協定ID:ESP，SPI大小：4,#trans:3上次轉換：0x3，保留：0x0： 度：8 型別：1，保留：0x0,id:3DES 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：5，保留：0x0,id：不使用ESN TSi下一個負載：TSr，保留：0x0，長度：24 TS數：1，保留0x0，保留0x0 TS型別：TS_IPV4_ADDR_RANGE，proto id:0，長度：16 起始埠：0，結束埠：65535 開始地址：0.0.0.0，結束地址：255.255.255.255 TSr下一個負載：NOTIFY，保留：0x0，長度：24 TS數：1，保留0x0，保留0x0 TS型別：TS_IPV4_ADDR_RANGE，proto id:0，長度：16 起始埠：0，結束埠：65535 開始地址：0.0.0.0，結束地址：255.255.255.255
	*Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_RECV_AUTH *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_CHK_NAT t *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_PROC_ID *11月11日19:30:34.832: IKEv2:(SA ID = 1)：已收到進程ID中的有效引數 *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_CHK_IF

	peer_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL *Nov 11 19:30:34.832: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_GET_POLICY BY PEERID(*11月11日19:30:34.833:IKEv2:(1)：選擇IKE配置檔案IKEV2-SETUP *11月11日19:30:34.833:IKEv2:%按地址10.0.0.1獲取預共用金鑰 *11月11日19:30:34.833:IKEv2:%按地址10.0.0.1獲取預共用金鑰 *11月11日19:30:34.833:IKEv2：將建議預設新增到工具包策略 *11月11日19:30:34.833: IKEv2:(SA ID = 1)：使用IKEv2配置檔案「IKEV2- SETUP」 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_SET_POLICY *11月11日19:30:34.833:IKEv2:(SA ID = 1)：設定配置的策略 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_VERIFY_POLICY_POLICY_BY PEERID(_P) *11月11日19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_CHK EAP *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟蹤 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_WAIT_AUTH事件： EV_POLQEAP B.C. *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_CHK_AUTH型別 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_GET_PREHR主要 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟蹤 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_CHK4_IC *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_CHK_REDIRECT *11月11日19:30:34.833: IKEv2:(SA ID = 1)：不需要重定向檢查，將跳過它 *11月11日19:30:34.833:IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH Event: EV done B.C. *11月11日19:30:34.833：未配置IKEv2:AAA組授權 *11月11日19:30:34.833：未配置IKEv2:AAA使用者授權

	*Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_CHK_CONFIG模式 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_SET_RECD config_MOD *11月11日19:30:34.833:IKEv2：從工具包接收配置資料： *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_PROC_SA TS *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_VERIFY_AUTH事件： EV_GET_CONFIG_MODE B. *11月11日19:30:34.833：構造配置回覆時出錯 *11月11日19:30:34.833:IKEv2：沒有配置資料傳送到工具包： *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_BLD_AUTH事件： EV_MY_AUTH方法 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_BLD_AUTH事件： EV_GET_PREHR主要 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_BLD_AUTH事件： EV_GEN_AUTH *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_BLD_AUTH事件： EV_CHK4_SIGN *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_BLD_AUTH事件： EV_OK_AUTH GEN *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: R_BLD_AUTH事件： EV_SEND_AUTH *11月11日19:30:34.833:IKEv2：構建供應商特定負載：思科 — 花崗岩 *11月11日19:30:34.833:IKEv2：構建通知負載：SET_WINDOW_SIZE *11月11日19:30:34.833:IKEv2：構建通知負載：ESP_TFC_NO_SUPPORT *11月11日19:30:34.833:IKEv2：構建通知負載 ：NON_FIRST_FRAGS
	*11月11日19:30:34.833: IKEv2:(SA ID = 1)：下一個負載：ENCR，版本：2.0交換型別： IKE_AUTH，標誌：RESPONDER MSG-RESPONSE Messa id:1，長度：252 負載內容： ENCR下一個負載：VID，保留：0x0，長度：224 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE事件： EV_OK *11月11日19:30:34.833:IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE事件： EV_PKI_SESH_CLOSE *11月11日19:30:34.833:IKEv2:(SA ID = 1)：關閉PKI會話 *Nov 11 19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE事件： EV_UPDATE_CAC_STATS *11月11日19:30:34.833: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE事件：EV_INSERT_IKE *11月11日19:30:34.834:IKEv2：儲存mib索引ikev2 1，平台60 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE事件： EV_GEN_LOAD_IPSEC *11月11日19:30:34.834: IKEv2:(SA ID = 1)：排隊的非同步請求 *11月11日19:30:34.834:IKEv2:(SA ID = 1): *11月11日19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)MsgID = 00000001 CurState: AUTH_DONE Event: EV_NO_NO	
<----------Responder sent IKE_AUTH----------		
發起方從響應方接收響應。	*11月11日19:30:34.834: IKEv2：收到來自排程器的資料包 *11月11日19:30:34.834:IKEv2：正在處理pak隊列中的專案	*Nov 11 19:30:34.840: IKEv2:(SA ID 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState: AUTH_DONE 件： EV_OK_RECD_LOAD IPSEC *11月11日19:30:34.840:IKEv2:(SA I 1):Action: Action_Null *11月11日19:30:34.840:IKEv2:(SA I 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState: AUTH_DONE 件： EV_START_ACCT *11月11日19:30:34.840:IKEv2:(SA I 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState: AUTH_DONE 件： EV_CHECK_DUPE *11月11日19:30:34.840:IKEv2:(SA I

		1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState: AUTH_DONE 件： EV_CHK4_ROLE
Router 1會驗證並處理此封包中的驗證資料。然後，Router 1將此SA插入其SAD。	*11月11日19:30:34.834: IKEv2:(SA ID = 1)：下一個負載：ENCR，版本：2.0交換型別：IKE_AUTH，標誌：RESPONDER MSG-RESPONSE消息id:1，長度：252 負載內容： *11月11日19:30:34.834: IKEv2：分析供應商特定負載：（自定義）VID下一載：IDr.，保留：0x0，長度：20 IDr。下一個負載：AUTH，保留：0x0，長度：12 Id型別：IPv4地址，保留：0x0 0x0 AUTH Next payload: SA， reserved: 0x0, length: 28 身份驗證方法PSK，保留： 0x0，保留0x0 SA下一個負載：TSi，保留：0x0，長度：40 最後一個建議：0x0，保留：0x0，長度：36 方案：1，協定ID:ESP，SPI大小：4,#trans:3上次轉換：0x3，保留：0x0：度：8 型別：1，保留：0x0,id:3DES 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：5，保留：0x0,id：不使用ESN TSi下一個負載：TSr，保留：0x0，長度：24 TS數：1，保留0x0，保留0x0 TS型別：TS_IPV4_ADDR_RANGE，proto id:0，長度：16 起始埠：0，結束埠：65535 開始地址：0.0.0.0，結束地址：255.255.255.255 TSr下一個負載：NOTIFY，保留：0x0，長度：24 TS數：1，保留0x0，保留0x0 TS型別：TS_IPV4_ADDR_RANGE，proto id:0，長度：16 起始埠：0，結束埠：65535 開始地址：0.0.0.0，結束地址：255.255.255.255 *11月11日19:30:34.834: IKEv2：解析通知負載：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下一個負載：通知，保留：0x0，長度：12 安全協定ID:IKE，spi大小：0，型別：SET_WINDOW_SIZE *11月11日19:30:34.834: IKEv2：解析通知負載：ESP_TFC_NO_SUPPORT NOTIFY(ESP_TFC_NO_SUPPORT)下一個負載：NOTIFY，保留：0x0，長：8 安全協定ID:IKE，spi大小：0，型別：ESP_TFC_NO_SUPPORT	

	*11月11日19:30:34.834: IKEv2：解析通知負載：NON_FIRST_FRAGS NOTIFY(NON_FIRST_FRAGS)下一個負載：無，保留：0x0，長度：8 安全協定ID:IKE，spi大小：0，型別：NON_FIRST_FRAGS *11月11日19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_WAIT_AUTH事件：EV_RECV_AUTH B.C. *11月11日19:30:34.834:IKEv2:(SA ID = 1):Action: Action_Null *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_CHK_NOTIFY *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件：EV_PROC消息 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_CHK_IF PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PROF_SEL *11月11日19:30:34.834:IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_GET_POLICY_POLICY by_PEERID *11月11日19:30:34.834:IKEv2：將建議階段1-prop新增到工具包策略 *11月11日19:30:34.834: IKEv2:(SA ID = 1)：使用IKEv2配置檔案「IKEV2- SETUP」 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_VERIFY_POLICY_POLICY by_PEERID *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_CHK_AUTH型別 *Nov 11 19:30:34.834: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_GET_PREHR主要 *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件：EV_VERIFY_AUTH B.C. *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件： EV_CHK_EAP *Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: I_PROC_AUTH事件：EV_NOTIFY_AUTH完成(_D)

*11月11日19:30:34.835：未配置IKEv2:AAA組授權
*11月11日19:30:34.835：未配置IKEv2:AAA使用者授權
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: I_PROC_AUTH事件： EV_CHK_CONFIG模式
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: I_PROC_AUTH事件： EV_CHK4_IC
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: I_PROC_AUTH事件： EV_CHK_IKE僅
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: I_PROC_AUTH事件： EV_PROC_SA TS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: AUTH_DONE事件： EV_OK
*11月11日19:30:34.835:IKEv2:(SA ID = 1):Action: Action_Null
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: AUTH_DONE事件： EV_PKI_SESH_CLOSE
*11月11日19:30:34.835:IKEv2:(SA ID = 1)：關閉PKI會話
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: AUTH_DONE事件： EV_UPDATE_CAC_STATS
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: AUTH_DONE事件： EV_INSERT_IKE
*11月11日19:30:34.835:IKEv2：儲存mib索引ikev2 1，平台60
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: AUTH_DONE事件： EV_GEN_LOAD_IPSEC
*11月11日19:30:34.835: IKEv2:(SA ID = 1)：排隊的非同步請求

*11月11日19:30:34.835:IKEv2:(SA ID = 1):
*Nov 11 19:30:34.835: IKEv2:(SA ID = 1):SM跟蹤 — > SA:
I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID =
00000001 CurState: AUTH_DONE事件： EV_NO_EVENT
*11月11日19:30:34.835:IKEv2:KMI消息8已使用。未採取任何操作。
*11月11日19:30:34.835：已使用IKEv2:KMI消息12。未採取任何操作。
*11月11日19:30:34.835:IKEv2：在模式配置集中沒有要傳送的資料。
*11月11日19:30:34.841:IKEv2：新增與會話8的SPI 0x9506D414關聯的獨立
制代碼0x80000002

*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM跟蹤 — > SA:

	I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: AUTH_DONE事件： EV_OK_RECD_LOAD IPSEC *11月11日19:30:34.841:IKEv2:(SA ID = 1)：操作：Action_Null *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: AUTH_DONE事件： EV_START_ACCT *11月11日19:30:34.841:IKEv2:(SA ID = 1)：無需記帳 *Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: AUTH_DONE事件： EV_CHECK_DUPE *11月11日19:30:34.841: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: AUTH_DONE Event: EV_CHK_role B.C.	
發起程式上的隧道已啟動，狀態顯示READY。	*Nov 11 19:30:34.841: IKEv2:(SA ID = 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState: READYEevent: EV_CHK_IKE_ONLY *11月11日19:30:34.841:IKEv2:(SA ID = 1):SM跟蹤 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(I)MsgID = 00000001 CurState:READY事件：EV_I_OK	*Nov 11 19:30:34.840: IKEv2:(SA ID 1):SM跟蹤 — > SA: I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState: READY Even EV_R_OK *11月11日19:30:34.840:IKEv2:(SA I 1):SM跟蹤 — > SA:I_SPI=F074D8BBD5A59F0B R_SPI=F94020DD8CB4B9C4(R)Ms = 00000001 CurState:READY事件：EV_NO_EVENT

CHILD_SA調試

此交換由單個請求/響應對組成，在IKEv1中稱為2階段。完成初始交換後，IKE_SA的任一端都可以啟動它。

Router 1 CHILD_SA訊息說明	調試	Router 2 CHILD_SA訊
路由器1啟動CHILD_SA交換。這是CREATE_CHILD_SA請求。 CHILD_SA資料包通常包含： • SA HDR(version.flags/exchange type) • Nonce Ni（可選）：如果將CHILD_SA建立為初始交換的一部分，則不得傳送第二個KE負載和nonce) • SA負載	*11月11日19:31:35.873: IKEv2：收到來自排程器的資料包 *11月11日19:31:35.873:IKEv2：正在處理pak隊列中的專案 *11月11日19:31:35.873:IKEv2:(SA ID = 2)：請求具有mess_id 3；預期為3至7	

• KEi(Key-optional):CREATE_CHILD_SA請求可以選擇包含用於附加DH交換的KE負載，從而為CHILD_SA啟用更強的前向保密保證。如果SA提供包括不同的DH組，則KEi必須是發起方期望響應方接受的組的元素。如果它猜測錯誤，則CREATE_CHILD_SA交換將失敗，並且它可以使用不同的KEi重試 • N（通知負載 — 可選）。通知負載用於將資訊資料（例如錯誤條件和狀態轉換）傳輸到IKE對等體。通知負載可以出現在響應消息（通常它指定請求被拒絕的原因）、資訊交換（報告不在IKE請求中的錯誤）或任何其他消息中，以指示傳送者功能或修改請求的含義。如果此CREATE_CHILD_SA交換重新生成除IKE_SA之外的現有SA的金鑰，REKEY_SA型別的前N個負載必須標識要重新生成金鑰的SA。如果此CREATE_CHILD_SA交換不對現有SA重新建立金鑰，則必須省略N負載。	*11月11日19:31:35.873: IKEv2:(SA ID = 2)：下一個負載：ENCR，版本： 2.0 Exchange type: CREATE_CHILD_SA，標誌： INITIATOR Message id: 3，長度： 396 負載內容： SA下一個負載：N，保留：0x0，長度：152 最後一個建議：0x0，保留：0x0，長度：148 方案：1，協定ID:IKE，SPI大小：8,#trans:15上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA512 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA384 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA256 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:MD5 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA512 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA384 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA256	

	上次轉換：0x3，保留：0x0：長度 ：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x3，保留：0x0：長度 ：8 型別：3，保留：0x0,id:MD596 上次轉換：0x3，保留：0x0：長度 ：8 型別：4，保留 ：0x0,id:DH_GROUP_1536_MODP/組 5 上次轉換：0x0，保留：0x0：長度 ：8 型別：4，保留 ：0x0,id:DH_GROUP_1024_MODP/組 2 N 下一個負載：KE，保留：0x0，長度 ：24 KE下一個負載：NOTIFY，保留 ：0x0，長度：136 DH組：2，保留：0x0 *11月11日19:31:35.874: IKEv2：解析 通知負載：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下一個 負載：無，保留：0x0，長度：12 安全協定ID:IKE，spi大小：0，型別 ：SET_WINDOW_SIZE *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: READY事件： EV_RECV_CREATE_CHILD *11月11日19:31:35.874:IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_INIT事件： EV_RECV_CREATE_CHILD *11月11日19:31:35.874:IKEv2:(SA ID	

	= 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_INIT事件：EV_VERIFY_MSG *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_INIT事件：EV_CHK_CC_TYPE *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_IKE事件：EV_REKEY_IKESA *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_IKE事件：EV_GET_POLICY *11月11日19:31:35.874:IKEv2:% 按地址10.0.0.2獲取預共用金鑰 *11月11日19:31:35.874:IKEv2:%按地址10.0.0.2獲取預共用金鑰 *11月11日19:31:35.874:IKEv2：將建議階段1-prop新增到工具包策略 *11月11日19:31:35.874: IKEv2:(SA ID = 2)：使用IKEv2配置檔案「IKEV2-SETUP」 *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_IKE事件： EV_PROC_MSG *Nov 11 19:31:35.874: IKEv2:(SA ID =	

	2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_IKE事件： EV_SET_POLICY *11月11日19:31:35.874:IKEv2:(SA ID = 2)：設定配置的策略 *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件： EV_GEN_DH主要 *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件： EV_NO_EVENT *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件： EV_OK_RECD DH_PUBKEY_RESP *11月11日19:31:35.874:IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.874: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件 ：EV_GEN_DE密碼(_S) *Nov 11 19:31:35.881: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件： EV_NO_EVENT	

	*Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件：EV_OK_RECD DH_SECRET_RESP *11月11日19:31:35.882:IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件： EV_BLD *11月11日 19:31:35.882:IKEv2:ConstructNotify負載:SET_WINDOW_SIZE 負載內容： SA下一個負載：N，保留：0x0，長度：56 最後一個建議：0x0，保留：0x0，長度：52 方案：1，協定ID:IKE，SPI大小：8,#trans:4上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度：8 型別：4，保留：0x0,id:DH_GROUP_1024_MODP/組2 N 下一個負載：KE，保留：0x0，長度：24 KE下一個負載：NOTIFY，保留：0x0，長度：136 DH組：2，保留：0x0 NOTIFY(SET_WINDOW_SIZE)下一個負載：無，保留：0x0，長度：12	

	安全協定ID:IKE，spi大小：0，型別：SET_WINDOW_SIZE	
	*11月11日19:31:35.869:IKEv2:(SA ID = 2)：下一個負載：ENCR，版本：2.0交換型別 ：CREATE_CHILD_SA，標誌：INITIATOR消息id:2，長度：460 負載內容： ENCR下一個負載：SA，保留 ：0x0，長度：432 *11月11日19:31:35.873:IKEv2：構建通知負載：SET_WINDOW_SIZE 負載內容： SA下一個負載：N，保留：0x0，長度 ：152 最後一個建議：0x0，保留：0x0，長度 ：148 方案：1，協定ID:IKE，SPI大小 ：8,#trans:15上次轉換：0x3，保留 ：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA512 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA384 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA256 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度：8 型別：2，保留：0x0,id:MD5 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA512 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA384 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA256 上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:SHA96	Router 2會收到此封包。

	上次轉換：0x3，保留：0x0：長度：8 型別：3，保留：0x0,id:MD596 上次轉換：0x3，保留：0x0：長度：8 型別：4，保留 ：0x0,id:DH_GROUP_1536_MODP/組5 上次轉換：0x0，保留：0x0：長度：8 型別：4，保留 ：0x0,id:DH_GROUP_1024_MODP/組2 N 下一個負載：KE，保留：0x0，長度：24 KE下一個負載：NOTIFY，保留 ：0x0，長度：136 DH組：2，保留：0x0 NOTIFY(SET_WINDOW_SIZE)下一個負載：無，保留：0x0，長度：12 安全協定ID:IKE，spi大小：0，型別 ：SET_WINDOW_SIZE	
	*11月11日19:31:35.882:IKEv2:(SA ID = 2)：下一個負載：ENCR，版本：2.0交換型別 ：CREATE_CHILD_SA，標誌 ：RESPONDER MSG-RESPONSE消息id:3，長度：300 負載內容： SA下一個負載：N，保留：0x0，長度：56 最後一個建議：0x0，保留：0x0，長度：52 方案：1，協定ID:IKE，SPI大小 ：8,#trans:4上次轉換：0x3，保留 ：0x0：長度：12 型別：1，保留：0x0,id:AES-CBC 上次轉換：0x3，保留：0x0：長度 ：8 型別：2，保留：0x0,id:SHA1 上次轉換：0x3，保留：0x0：長度 ：8 型別：3，保留：0x0,id:SHA96 上次轉換：0x0，保留：0x0：長度 ：8 型別：4，保留 ：0x0,id:DH_GROUP_1024_MODP/組	現在，Router 2會為CHIL 立應答。這是CREATE_C 應。CHILD_SA資料包通常 • SA HDR(version.fla type) • Nonce Ni（可選）： CHILD_SA建立為初 部分，則不得傳送第 和nonce。 • SA負載 • KEi(Key- optional):CREATE_ 求可以選擇包含用於 的KE負載，從而為C 用更強的前向保密保 SA提供包括不同的D KEi必須是發起方期 受的組的元素。如果 ，CREATE_CHILD_ 敗，並且它必須使用 KEi重試。 • N（通知負載 — 可選 載用於將資訊資料（ 和狀態轉換）傳輸到 。通知負載可以出現

	2 N 下一個負載：KE，保留：0x0，長度：24 KE下一個負載：NOTIFY，保留：0x0，長度：136 DH組：2，保留：0x0 *11月11日19:31:35.882: IKEv2：解析通知負載：SET_WINDOW_SIZE NOTIFY(SET_WINDOW_SIZE)下一個負載：無，保留：0x0，長度：12 安全協定ID:IKE，spi大小：0，型別：SET_WINDOW_SIZE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_WAIT Event: EV_RECV_CREATE子項(_J) *11月11日19:31:35.882:IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件：EV_CHK4_NOTIFY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件：EV_VERIFY_MSG *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件：EV_PROC_MSG *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA:	（通常它指定請求被 ）、資訊交換（報告 求中的錯誤）或任何 ，以指示傳送者功能 的含義。如果此 CREATE_CHILD_S 新生成除IKE_SA之外 SA的金鑰，REKEY 前N個負載必須標識 成金鑰的SA。如果此 CREATE_CHILD_S 有SA重新建立金鑰 N負載。 Router 2將回應發出並完成 啟用。

	I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件： EV_CHK4_PFS *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件： EV_GEN_DH_SECRET *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件： EV_NO_EVENT *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件： EV_OK_RECD_DH SECRET_RESP *11月11日19:31:35.890:IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件： EV_CHK_IKE_REKEY *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_PROC事件： EV_GEN_SKEID *11月11日19:31:35.890:IKEv2:(SA ID = 2)：生成skyid *Nov 11 19:31:35.890: IKEv2:(SA ID =	

	2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_DONE事件： EV_ACTIVATE_NEW SA *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_DONE事件： EV_UPDATE_CAC_STATS *11月11日19:31:35.890:IKEv2：啟用 新ikev2 sa請求 *11月11日19:31:35.890: IKEv2：無法 減少傳出協商的計數 *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_DONE事件： EV_CHECK_DUPE *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState: CHILD_I_DONE事件： EV_OK *Nov 11 19:31:35.890: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 00000003 CurState：退出事件 ：EV_CHK_PENDING *11月11日19:31:35.890: IKEv2:(SA ID = 2)：已處理郵件ID為3的響應，請求可 以從4到8傳送 *11月11日19:31:35.890:IKEv2:(SA ID = 2):SM跟蹤 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(I)MsgID = 0000003 CurState：退出事件 ：EV_NO事件(_E)	

路由器1收到來自路由器2的響應資料包，並完成啟用CHILD_SA。	*11月11日19:31:35.882:IKEv2:(SA ID = 2)：下一個負載：ENCR，版本：2.0交換型別 ：CREATE_CHILD_SA，標誌 ：RESPONDER MSG-RESPONSE Message id:3，長度：300 負載內容： ENCR下一個負載：SA，保留 ：0x0，長度：272 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件：EV_CHK IKE_REKEY *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_BLD_MSG事件：EV_GEN_SKEID *11月11日19:31:35.882: IKEv2:(SA ID = 2)：生成skyid *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_DONE事件 ：EV_ACTIVATE_NEW_SA *11月11日19:31:35.882:IKEv2：儲存mib索引ikev2 3，平台62 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_DONE事件：EV_UPDATE_CAC_STATS *11月11日19:31:35.882: IKEv2：啟用新ikev2 sa請求 *11月11日19:31:35.882: IKEv2：無法	

	減少傳入協商的計數 *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_DONE事件：EV_CHECK_DUPE *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_DONE事件： EV_OK *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState: CHILD_R_DONE事件：EV_START_DEL_TG MR *11月11日19:31:35.882:IKEv2:(SA ID = 2):Action: Action_Null *Nov 11 19:31:35.882: IKEv2:(SA ID = 2):SM跟蹤 — > SA: I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 00000003 CurState：退出事件：EV_CHK_PENDING *11月11日19:31:35.882: IKEv2:(SA ID = 2)：已傳送消息ID為3的響應，請求可以在4到8的範圍內被接受 *11月11日19:31:35.82:IKEv2:(SA ID = 2):SM跟蹤 — > SA:I_SPI=0C33DB40DBAADE6 R_SPI=F14E2BBA78024DE3(R)MsgID = 0000003 CurState：退出事件：EV_NO事件(_E)	

通道驗證

ISAKMP

指令

<#root>

show crypto ikev2 sa detailed

Router 1輸出

<#root>

```
Router1#
show crypto ikev2 sa  detailed


 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote              fvrf/ivrf         Status
1         10.0.0.1/500          10.0.0.2/500        none/none         READY
      Encr: AES-CBC, keysize: 128,
         Hash: SHA96, DH Grp:2,
         Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/10 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
      Local spi: E58F925107F8B73F     Remote spi: AFD098F4147869DA
      Local id: 10.0.0.1
      Remote id: 10.0.0.2
      Local req msg id:  2       Remote req msg id:  0
      Local next msg id: 2       Remote next msg id: 0
      Local req queued:  2       Remote req queued:  0
      Local window:      5       Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : Yes
```

路由器2輸出

<#root>

```
Router2#
show crypto ikev2 sa detailed


 IPv4 Crypto IKEv2  SA

Tunnel-id Local           Remote              fvrf/ivrf          Status
2         10.0.0.2/500    10.0.0.1/500        none/none          READY
      Encr: AES-CBC, keysize: 128, Hash: SHA96,
         DH Grp:2, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 120/37 sec
      CE id: 1006, Session-id: 4
      Status Description: Negotiation done
```

```
      Local spi: AFD098F4147869DA       Remote spi: E58F925107F8B73F
      Local id: 10.0.0.2
      Remote id: 10.0.0.1
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
```

IPsec

指令

<#root>

show crypto ipsec sa

註：與IKEv1不同，在此輸出中，PFS DH組值在第一次隧道協商期間顯示為「PFS(Y/N): N，DH組：無」，但在重新生成金鑰後，將顯示正確的值。這不是錯誤，即使此行為已在Cisco錯誤ID CSCug67056中說明。（只有已註冊的思科使用者才能存取內部思科工具或資訊。）
IKEv1和IKEv2之間的區別在於，在後一種情況下，子SA是作為身份驗證交換本身的一部分而建立的。在加密對映下配置的DH組僅在重新生成金鑰期間使用。因此，在第一次重新生成金鑰之前，您將看到「PFS(Y/N):N，DH組：none」。
使用IKEv1時，您會看到不同的行為，因為子SA建立發生在快速模式期間，而CREATE_CHILD_SA消息具有攜帶金鑰交換有效載荷的設定，該有效載荷指定DH引數以派生新的共用金鑰。

Router 1輸出

<#root>

```
Router1#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0,
         local addr 10.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port):
         (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.2 port 500
```

```
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt:
     10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt:
     10, #pkts verify: 10
#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.: 10.0.0.1,
     remote crypto endpt.: 10.0.0.2
 path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
 current outbound spi: 0xF6083ADD(4127734493)
 PFS (Y/N): N, DH group: none

 inbound esp sas:
  spi: 0x6B74CB79(1802816377)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 18, flow_id: SW:18,
     sibling_flags 80000040,
     crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec):
     (4276853/3592)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

 inbound ah sas:

 inbound pcp sas:

 outbound esp sas:
  spi: 0xF6083ADD(4127734493)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 17, flow_id: SW:17,
     sibling_flags 80000040,
     crypto map: Tunnel0-head-0
    sa timing: remaining key
     lifetime (k/sec): (4276853/3592)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

 outbound ah sas:

 outbound pcp sas:
```

路由器2輸出

<#root>

Router2#

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/256/0)
   current_peer 10.0.0.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #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.: 10.0.0.2,
         remote crypto endpt.: 10.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x6B74CB79(1802816377)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF6083ADD(4127734493)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 17, flow_id: SW:17,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime
         (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x6B74CB79(1802816377)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 18, flow_id: SW:18,
         sibling_flags 80000040,
         crypto map: Tunnel0-head-0
        sa timing: remaining key
         lifetime (k/sec): (4347479/3584)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

您也可以在兩台路由器上檢查show crypto session命令的輸出；此輸出將隧道會話狀態顯示為UP-ACTIVE。

<#root>

```
Router1#
```

show crypto session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.2 port 500
  IKEv2 SA: local 10.0.0.1/500 remote 10.0.0.2/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map

Router2#
```

show cry session

```
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.0.0.1 port 500
  IKEv2 SA: local 10.0.0.2/500 remote 10.0.0.1/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

相關資訊

- IKEv2封包交換和通訊協定層級偵錯
- 思科技術支援與下載

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）。