用於金鑰環和配置檔案的IOS IKEv1/IKEv2選擇規則 — 故障排除指南

目錄

簡介

本檔案介紹在Cisco IOS®軟體LAN到LAN VPN的情況中，多個金鑰環用於多個網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)設定檔的情況。它涵蓋了Cisco IOS軟體版本15.3T的行為，以及使用多個按鍵時的潛在問題。

根據每台路由器上帶有兩個ISAKMP配置檔案的VPN隧道提出了兩種方案。每個配置檔案具有不同的金鑰環，並且連線了相同的IP地址。這些場景顯示，由於配置檔案選擇和驗證，只能從連線的一側啟動VPN隧道。

本文檔的下一部分概述了網際網路金鑰交換(IKE)發起方和IKE響應方的金鑰環配置檔案的選擇標準。當IKE響應器上的金鑰環使用不同的IP地址時，配置工作正常，但是使用相同的IP地址會導致第一個場景中出現的問題。

後續部分解釋了為什麼預設金鑰環（全域性配置）和特定金鑰環的存在都可能導致問題，以及為什麼使用Internet金鑰交換版本2(IKEv2)協定可以避免該問題。

最後部分提供了IKE啟動器和響應器的IKE配置檔案的選擇標準，以及選擇不正確的配置檔案時發生的典型錯誤。

組態

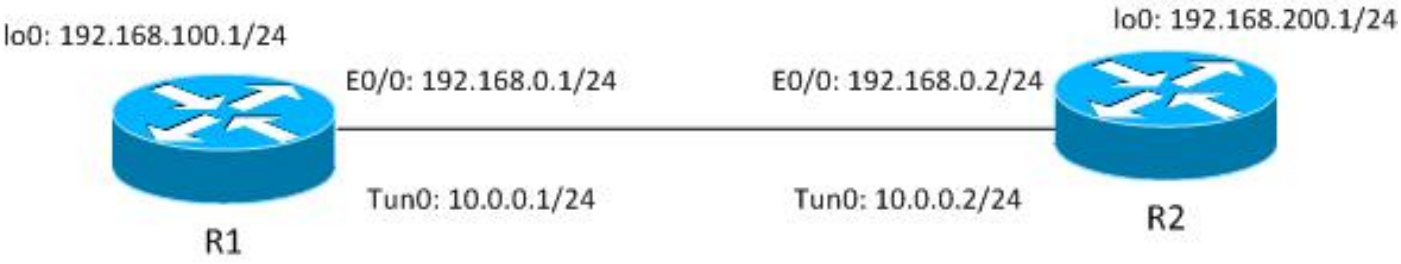
附註：

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 **show 指令。**使用 Cisco CLI Analyzer 檢視 **show 指令輸出的分析。**

使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

拓撲

Router1(R1)和Router2(R2)使用虛擬通道介面(VTI)（通用路由封裝[GRE]）介面來存取其回送。VTI受Internet協定安全(IPSec)保護。



R1和R2都有兩個ISAKMP配置檔案，每個配置檔案具有不同的金鑰環。所有金鑰環具有相同的密碼。

R1網路和VPN

R1網路和VPN的配置為：

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.2 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp profile profile1
   keyring keyring1
   match identity address 192.168.0.102 255.255.255.255 !non existing host
crypto isakmp profile profile2
   keyring keyring2
   match identity address 192.168.0.2 255.255.255.255 !R2
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile2
```

```
!
interface Loopback0
 description Simulate LAN
 ip address 192.168.100.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.

ip route 192.168.200.0 255.255.255.0 10.0.0.2
```

R2網路和VPN

R2網路和VPN的配置為：

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.1 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.1 key cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2

crypto isakmp profile profile1
   keyring keyring1
   match identity address 192.168.0.1 255.255.255.255 !R1
crypto isakmp profile profile2
   keyring keyring2
   match identity address 192.168.0.100 255.255.255.255 !non existing host
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile1
!
interface Loopback0
 ip address 192.168.200.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.2 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.1
 tunnel protection ipsec profile profile1
!
interface Ethernet0/0
 ip address 192.168.0.2 255.255.255.0

ip route 192.168.100.0 255.255.255.0 10.0.0.1
```

所有金鑰環使用相同的對等IP地址並使用密碼「cisco」。

在R1上，profile2用於VPN連線。Profile2是配置中的第二個配置檔案，它在配置中使用第二個金鑰

環。正如您將看到的，金鑰環順序非常重要。

範例案例

在第一個方案中，R1是ISAKMP啟動器。通道正在正確協商，流量按預期得到保護。

第二種方案使用相同的拓撲，但在第1階段協商失敗時，將R2作為ISAKMP啟動器。

網際網路金鑰交換版本1(IKEv1)需要預先共用金鑰以進行金鑰計算，該金鑰用於解密/加密主模式封包5(MM5)和後續的IKEv1封包。該金鑰源自Diffie-hellman(DH)計算和預共用金鑰。在收到MM3（響應方）或MM4（發起方）之後需要確定該預共用金鑰，以便可以計算MM5/MM6中使用的金鑰。

對於MM3中的ISAKMP響應方，尚未確定特定的ISAKMP配置檔案，因為在MM5中接收IKEID後會發生這種情況。相反，將搜尋所有金鑰環以查詢預共用金鑰，並從全域性配置中選擇第一個或最佳匹配金鑰環。金鑰環用於計算MM5的解密和MM6的加密所使用的金鑰。在MM5的解密之後，確定ISAKMP配置檔案和相關金鑰環之後，如果選擇了相同的金鑰環，則ISAKMP響應器執行驗證；如果未選擇相同的金鑰環，則連線將被丟棄。

因此，對於ISAKMP響應程式，應儘可能使用一個包含多個條目的金鑰環。

R1作為IKE啟動器（正確）

此案例描述當R1是IKE啟動器時會發生的情況：

1. 對R1和R2使用以下調試：

```
R1# debug crypto isakmp
R1# debug crypto ipsec
R1# debug crypto isakmp aaa
```

2. R1啟動隧道，傳送包含策略建議的MM1資料包，並接收MM2作為響應。然後準備MM3:

```
R1#ping 192.168.200.1 source lo0 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1

*Jun 19 10:04:24.826: IPSEC(sa_request): ,
 (key eng. msg.) OUTBOUND local= 192.168.0.1:500, remote= 192.168.0.2:500,
   local_proxy= 192.168.0.1/255.255.255.255/47/0,
   remote_proxy= 192.168.0.2/255.255.255.255/47/0,
   protocol= ESP, transform= esp-aes esp-sha256-hmac  (Tunnel),
   lifedur= 3600s and 4608000kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Jun 19 10:04:24.826: ISAKMP:(0): SA request profile is profile2
*Jun 19 10:04:24.826: ISAKMP: Found a peer struct for 192.168.0.2, peer
port 500
*Jun 19 10:04:24.826: ISAKMP: Locking peer struct 0xF483A970, refcount 1
for isakmp_initiator
*Jun 19 10:04:24.826: ISAKMP: local port 500, remote port 500
*Jun 19 10:04:24.826: ISAKMP: set new node 0 to QM_IDLE
*Jun 19 10:04:24.826: ISAKMP:(0):insert sa successfully sa = F474C2E8
*Jun 19 10:04:24.826: ISAKMP:(0):Can not start Aggressive mode, trying
Main mode.
```

```
*Jun 19 10:04:24.826: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-03 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-02 ID
*Jun 19 10:04:24.826: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC,
IKE_SA_REQ_MM
*Jun 19 10:04:24.826: ISAKMP:(0):Old State = IKE_READY  New State =
IKE_I_MM1

*Jun 19 10:04:24.826: ISAKMP:(0): beginning Main Mode exchange
*Jun 19 10:04:24.826: ISAKMP:(0): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_NO_STATE
*Jun 19 10:04:24.826: ISAKMP:(0):Sending an IKE IPv4 Packet.
*Jun 19 10:04:24.827: ISAKMP (0): received packet from 192.168.0.2 dport
500 sport 500 Global (I) MM_NO_STATE
*Jun 19 10:04:24.827: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.827: ISAKMP:(0):Old State = IKE_I_MM1  New State =
IKE_I_MM2

*Jun 19 10:04:24.827: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.827: ISAKMP:(0): local preshared key found
*Jun 19 10:04:24.827: ISAKMP : Looking for xauth in profile profile2
*Jun 19 10:04:24.827: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 10:04:24.827: ISAKMP:      encryption 3DES-CBC
*Jun 19 10:04:24.827: ISAKMP:      hash MD5
*Jun 19 10:04:24.827: ISAKMP:      default group 2
*Jun 19 10:04:24.827: ISAKMP:      auth pre-share
*Jun 19 10:04:24.827: ISAKMP:      life type in seconds
*Jun 19 10:04:24.827: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Jun 19 10:04:24.827: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:actual life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 10:04:24.827: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 10:04:24.827: ISAKMP:(0)::Started lifetime timer: 86400.

*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.827: ISAKMP:(0):Old State = IKE_I_MM2  New State =
IKE_I_MM2

*Jun 19 10:04:24.828: ISAKMP:(0): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_SA_SETUP
```

從一開始，R1就知道應使用ISAKMP profile2，因為它繫結在用於該VTI的IPSec配置檔案之下。

因此，選擇了正確的金鑰環（金鑰環2）。在準備MM3包時，來自金鑰環2的預共用金鑰用作DH計算的金鑰材料。

3. 當R2收到該MM3資料包時，它仍不知道應使用哪個ISAKMP配置檔案，但它需要預共用金鑰以生成DH。因此，R2搜尋所有金鑰環以查詢該對等體的預共用金鑰：

```
*Jun 19 10:04:24.828: ISAKMP (0): received packet from 192.168.0.1 dport
500 sport 500 Global (R) MM_SA_SETUP
*Jun 19 10:04:24.828: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.828: ISAKMP:(0):Old State = IKE_R_MM2  New State =
IKE_R_MM3

*Jun 19 10:04:24.828: ISAKMP:(0): processing KE payload. message ID = 0
*Jun 19 10:04:24.831: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun 19 10:04:24.831: ISAKMP:(0):found peer pre-shared key matching
192.168.0.1
```

已在第一個定義的金鑰環(keyring1)中找到用於192.168.0.1的金鑰。

4. 然後R2使用keyring1的「cisco」金鑰和DH計算準備MM4資料包：

```
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID is DPD
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): speaking to another IOS box!
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID seems Unity/DPD but major
32 mismatch
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID is XAUTH
*Jun 19 10:04:24.831: ISAKMP:received payload type 20
*Jun 19 10:04:24.831: ISAKMP (1011): His hash no match - this node
outside NAT
*Jun 19 10:04:24.831: ISAKMP:received payload type 20
*Jun 19 10:04:24.831: ISAKMP (1011): No NAT Found for self or peer
*Jun 19 10:04:24.831: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.831: ISAKMP:(1011):Old State = IKE_R_MM3  New State =
IKE_R_MM3

*Jun 19 10:04:24.831: ISAKMP:(1011): sending packet to 192.168.0.1 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Jun 19 10:04:24.831: ISAKMP:(1011):Sending an IKE IPv4 Packet.
```

5. 當R1收到MM4時，它使用IKEID和之前選擇的正確金鑰（來自金鑰環2）準備MM5資料包：

```
*Jun 19 10:04:24.831: ISAKMP (0): received packet from 192.168.0.2 dport
500 sport 500 Global (I) MM_SA_SETUP
*Jun 19 10:04:24.831: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.831: ISAKMP:(0):Old State = IKE_I_MM3  New State =
IKE_I_MM4

*Jun 19 10:04:24.831: ISAKMP:(0): processing KE payload. message ID = 0
*Jun 19 10:04:24.837: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun 19 10:04:24.837: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): vendor ID is Unity
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): vendor ID is DPD
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): speaking to another IOS box!
*Jun 19 10:04:24.837: ISAKMP:received payload type 20
*Jun 19 10:04:24.838: ISAKMP (1011): His hash no match - this node
```

```
outside NAT
*Jun 19 10:04:24.838: ISAKMP:received payload type 20
*Jun 19 10:04:24.838: ISAKMP (1011): No NAT Found for self or peer
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_I_MM4  New State =
IKE_I_MM4

*Jun 19 10:04:24.838: ISAKMP:(1011):Send initial contact
*Jun 19 10:04:24.838: ISAKMP:(1011):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.1
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 10:04:24.838: ISAKMP:(1011):Total payload length: 12
*Jun 19 10:04:24.838: ISAKMP:(1011): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_KEY_EXCH
```

6. R2接收包含IKEID 192.168.0.1的MM5資料包。此時，R2知道應將流量繫結到哪個ISAKMP配置檔案(**match identity** 地址命令):

```
*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.1 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_R_MM4  New State =
IKE_R_MM5

*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.1
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 10:04:24.838: ISAKMP:(0):: peer matches profile1 profile
*Jun 19 10:04:24.838: ISAKMP:(1011):Found ADDRESS key in keyring keyring1
*Jun 19 10:04:24.838: ISAKMP:(1011): processing HASH payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP:(1011): processing NOTIFY INITIAL_CONTACT
protocol 1
       spi 0, message ID = 0, sa = 0xF46295E8
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
       authenticated
*Jun 19 10:04:24.838: ISAKMP:(1011):SA has been authenticated with
192.168.0.1
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
       authenticated
```

7. 現在，R2會執行驗證，以檢查為MM4資料包盲選的關鍵環是否與為ISAKMP配置檔案配置的關鍵環相同。因為keyring1是配置中的第一個，所以它以前被選中，現在也被選中。驗證成功，可以傳送MM6資料包：

```
*Jun 19 10:04:24.838: ISAKMP:(1011):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
```

```
        address      : 192.168.0.2
        protocol     : 17
        port         : 500
        length       : 12
*Jun 19 10:04:24.838: ISAKMP:(1011):Total payload length: 12
*Jun 19 10:04:24.838: ISAKMP:(1011): sending packet to 192.168.0.1
my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Sending an IKE IPv4 Packet.
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_R_MM5  New State =
IKE_P1_COMPLETE
```

8. R1收到MM6，不需要執行金鑰環驗證，因為它從第一個資料包中獲知；發起方始終知道要使用的ISAKMP配置檔案以及與該配置檔案關聯的金鑰環。身份驗證成功，Phase1正確完成：

```
*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.2
dport 500 sport 500 Global (I) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
        next-payload : 8
        type         : 1
        address      : 192.168.0.2
        protocol     : 17
        port         : 500
        length       : 12
*Jun 19 10:04:24.838: ISAKMP:(1011): processing HASH payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
         authenticated
*Jun 19 10:04:24.838: ISAKMP:(1011):SA has been authenticated with
192.168.0.2
*Jun 19 10:04:24.838: ISAKMP AAA: Accounting is not enabled
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
*Jun 19 10:04:24.839: ISAKMP:(1011):Old State = IKE_I_MM5  New State =
IKE_I_MM6

*Jun 19 10:04:24.839: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.839: ISAKMP:(1011):Old State = IKE_I_MM6  New State =
IKE_I_MM6

*Jun 19 10:04:24.843: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 19 10:04:24.843: ISAKMP:(1011):Old State = IKE_I_MM6  New State =
IKE_P1_COMPLETE

*Jun 19 10:04:24.843: ISAKMP:(1011):beginning Quick Mode exchange, M-ID
of 2816227709
```

9. 階段2正常啟動並成功完成。

此方案之所以能正確運行，只是因為R2上定義的金鑰環順序正確。應該用於VPN會話的配置檔案使用配置中的第一個金鑰環。

R2作為IKE啟動器（不正確）

此案例描述R2啟動同一隧道時發生的情況，並說明為什麼不會建立隧道。為了著重說明此示例與上一個示例之間的差異，已刪除一些日誌：

1. R2啟動隧道：

```
R2#ping 192.168.100.1 source lo0 repeat 1
```

2. 由於R2是啟動器，因此ISAKMP配置檔案和金鑰環是已知的。來自keyring1的預共用金鑰用於DH計算，並在MM3中傳送。R2接收MM2，並根據該金鑰準備MM3:

```
*Jun 19 12:28:44.256: ISAKMP (0): received packet from 192.168.0.1 dport
500 sport 500 Global (I) MM_NO_STATE
*Jun 19 12:28:44.256: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 12:28:44.256: ISAKMP:(0):Old State = IKE_I_MM1  New State =
IKE_I_MM2

*Jun 19 12:28:44.256: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 12:28:44.256: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.256: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.256: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.256: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.256: ISAKMP:(0): local preshared key found
*Jun 19 12:28:44.256: ISAKMP : Looking for xauth in profile profile1
*Jun 19 12:28:44.256: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 12:28:44.256: ISAKMP:      encryption 3DES-CBC
*Jun 19 12:28:44.256: ISAKMP:      hash MD5
*Jun 19 12:28:44.256: ISAKMP:      default group 2
*Jun 19 12:28:44.256: ISAKMP:      auth pre-share
*Jun 19 12:28:44.256: ISAKMP:      life type in seconds
*Jun 19 12:28:44.256: ISAKMP:      life duration (VPI) of  0x0 0x1
0x51 0x80
*Jun 19 12:28:44.256: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 12:28:44.256: ISAKMP:(0):Acceptable atts:actual life: 0
*Jun 19 12:28:44.257: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 12:28:44.257: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 12:28:44.257: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 12:28:44.257: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 12:28:44.257: ISAKMP:(0)::Started lifetime timer: 86400.

*Jun 19 12:28:44.257: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.257: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.257: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.257: ISAKMP:(0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.257: ISAKMP:(0):Old State = IKE_I_MM2  New State =
IKE_I_MM2

*Jun 19 12:28:44.257: ISAKMP:(0): sending packet to 192.168.0.1 my_port
500 peer_port 500 (I) MM_SA_SETUP
```

3. R1收到來自R2的MM3。在此階段，R1不知道使用哪個ISAKMP配置檔案，因此它不知道使用哪個金鑰環。因此R1使用全域性配置中的第一個金鑰環，即keyring1。R1將該預共用金鑰用於DH計算，並傳送MM4:

```
*Jun 19 12:28:44.263: ISAKMP:(0):found peer pre-shared key matching
192.168.0.2
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID is DPD
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
```

```
*Jun 19 12:28:44.263: ISAKMP:(1012): speaking to another IOS box!
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID seems Unity/DPD but major
151 mismatch
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID is XAUTH
*Jun 19 12:28:44.263: ISAKMP:received payload type 20
*Jun 19 12:28:44.263: ISAKMP (1012): His hash no match - this node
outside NAT
*Jun 19 12:28:44.263: ISAKMP:received payload type 20
*Jun 19 12:28:44.263: ISAKMP (1012): No NAT Found for self or peer
*Jun 19 12:28:44.263: ISAKMP:(1012):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.263: ISAKMP:(1012):Old State = IKE_R_MM3  New State =
IKE_R_MM3
*Jun 19 12:28:44.263: ISAKMP:(1012): sending packet to 192.168.0.2 my_port
500 peer_port 500 (R) MM_KEY_EXC
```

4. R2從R1接收MM4，使用來自keyring1的預共用金鑰計算DH，並準備MM5資料包和IKEID:

```
*Jun 19 12:28:44.269: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is Unity
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is DPD
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): speaking to another IOS box!
*Jun 19 12:28:44.269: ISAKMP:received payload type 20
*Jun 19 12:28:44.269: ISAKMP (1012): His hash no match - this node
outside NAT
*Jun 19 12:28:44.269: ISAKMP:received payload type 20
*Jun 19 12:28:44.269: ISAKMP (1012): No NAT Found for self or peer
*Jun 19 12:28:44.269: ISAKMP:(1012):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.269: ISAKMP:(1012):Old State = IKE_I_MM4  New State =
IKE_I_MM4

*Jun 19 12:28:44.270: ISAKMP:(1012):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 12:28:44.270: ISAKMP (1012): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 12:28:44.270: ISAKMP:(1012):Total payload length: 12
*Jun 19 12:28:44.270: ISAKMP:(1012): sending packet to 192.168.0.1
my_port 500 peer_port 500 (I) MM_KEY_EXCH
```

5. R1收到來自R1的MM5。由於IKEID等於192.168.0，因此已選擇profile2。已在profile2中配置keyring2，因此選擇了keyring2。以前，對於MM4中的DH計算，R1選擇了第一個配置的金鑰環，即keyring1。即使密碼完全相同，對金鑰環的驗證也會失敗，因為這些金鑰環對象不同：

```
*Jun 19 12:28:44.270: ISAKMP (1012): received packet from 192.168.0.2
dport 500 sport 500 Global (R) MM_KEY_EXCH
*Jun 19 12:28:44.270: ISAKMP:(1012):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
*Jun 19 12:28:44.270: ISAKMP:(1012):Old State = IKE_R_MM4  New State =
IKE_R_MM5

*Jun 19 12:28:44.270: ISAKMP:(1012): processing ID payload. message ID = 0
```

```
*Jun 19 12:28:44.270: ISAKMP (1012): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
*Jun 19 12:28:44.270: ISAKMP:(0):: peer matches profile2 profile
*Jun 19 12:28:44.270: ISAKMP:(1012):Found ADDRESS key in keyring keyring2
*Jun 19 12:28:44.270: ISAKMP:(1012):Key not found in keyrings of profile ,
aborting exchange
*Jun 19 12:28:44.270: ISAKMP (1012): FSM action returned error: 2
```

不同預共用金鑰的調試

之前的方案使用相同的金鑰(「cisco」)。 因此，即使使用了不正確的金鑰環，由於金鑰環驗證失敗，MM5資料包仍可以正確解密，並在以後被丟棄。

在使用不同金鑰的情況下，MM5無法解密，並顯示以下錯誤消息：

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
failed its sanity check or is malformed
```

金鑰環選擇條件

以下是金鑰環選擇標準的摘要。請參見後續章節以瞭解更多詳細資訊。

	啟動器	響應
具有不同IP地址的多個金鑰環	Configured.如果沒有從配置中明確配置最具體的	最具
多個IP地址相同的金鑰環	Configured.如果未顯式配置 **配置變得不可預測並且不受支援。不應為同一個IP地址配置兩個金鑰。**	**配置**

本節還介紹了為什麼同時存在預設金鑰環（全域性配置）和特定金鑰環可能導致問題，並解釋了為什麼使用IKEv2協定可以避免這些問題。

IKE發起方上的金鑰環選擇順序

對於使用VTI的配置，啟動器使用指向特定IPSec配置檔案的特定隧道介面。因為IPSec簡檔使用具有特定金鑰環的特定IKE簡檔，所以不會混淆要使用的金鑰環。

Crypto-map也指向具有特定金鑰環的特定IKE配置檔案，其功能也相同。

但是，並非總是能夠根據配置確定要使用的金鑰環。例如，在沒有配置IKE簡檔時會發生這種情況 — 即IPSec簡檔未配置為使用IKE簡檔：

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.255.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
```

```
 mode tunnel

crypto ipsec profile profile1
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
```

如果此IKE啟動器嘗試傳送MM1，它將選擇最具體的金鑰環：

```
*Oct  7 08:13:58.413: ISAKMP: Locking peer struct 0xF4803B88, refcount 1 for
isakmp_initiator
*Oct  7 08:13:58.413: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
*Oct  7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 not available in default
*Oct  7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 found in keyring1
*Oct  7 08:13:58.413: ISAKMP:(0):ISAKMP: Selecting  192.168.0.0,255.255.255.0
as  key
*Oct  7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 found in keyring2
*Oct  7 08:13:58.413: ISAKMP:(0):ISAKMP: Selecting  192.168.0.2,255.255.255.255
as final key
*Oct  7 08:13:58.413: ISAKMP:(0):found peer pre-shared key matching 192.168.0.2
```

由於當啟動器接收MM6時未配置IKE配置檔案，因此它不會命中配置檔案並通過成功的身份驗證和快速模式(QM)完成：

```
Oct  7 08:13:58.428: ISAKMP:(0):: peer matches *none* of the profiles
*Oct  7 08:13:58.428: ISAKMP:(1005): processing HASH payload. message ID = 0
*Oct  7 08:13:58.428: ISAKMP:(1005):SA authentication status:
        authenticated
*Oct  7 08:13:58.432: ISAKMP:(1005):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
```

IKE回應器上的按鍵環選擇順序 — 不同的IP地址

金鑰環選擇的問題在響應程式上。當金鑰環使用不同的IP地址時，選擇順序非常簡單。

假設IKE響應器具有以下配置：

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.0.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco2
```

當此響應方從IP地址為192.168.0.2的IKE發起方收到MM1資料包時，它將選擇最佳（最具體）匹配，即使配置中的順序不同。

選擇順序的標準是：

1. 僅考慮具有IP地址的金鑰。
2. 檢查傳入封包的虛擬路由和轉送(VRF)（前端VRF [fVRF]）。
3. 如果資料包處於預設VRF中，則首先檢查全域性金鑰環。選擇最精確的金鑰（網路掩碼長度）。
4. 如果在預設金鑰環中找不到金鑰，則匹配此fVRF的所有金鑰環都會串聯。
5. 匹配最精確的金鑰（最長網路掩碼）。例如，優先使用/32而非/24。

調試確認選擇：

```
R1#debug crypto isakmp detail
Crypto ISAKMP internals debugging is on

*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 not available in default
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 found in keyring1
*Oct  2 11:57:13.301: ISAKMP:(0):ISAKMP: Selecting  192.168.0.0,255.255.255.0
as  key
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 found in keyring2
*Oct  2 11:57:13.301: ISAKMP:(0):ISAKMP: Selecting  192.168.0.2,255.255.255.255
as final key
```

IKE回應器上的按鍵環選擇順序 — 相同IP位址

當金鑰環使用相同的IP地址時，會出現問題。假設IKE響應器具有以下配置：

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.2 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco
```

此配置變得不可預測並且不受支援。不應為同一IP地址配置兩個金鑰，否則將發生R2中描述的IKE啟動器(不正確)問題。

金鑰環全域性配置

全域性配置中定義的ISAKMP金鑰屬於預設金鑰環：

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.0.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco2
crypto isakmp key cisco3 address 0.0.0.0
```

即使ISAKMP金鑰在配置中是最後一個，它仍被處理為IKE響應器上的第一個金鑰：

```
R1#show crypto isakmp key
Keyring      Hostname/Address                            Preshared Key

default      0.0.0.0        [0.0.0.0]                    cisco3

keyring1     192.168.0.0    [255.255.0.0]                cisco

keyring2     192.168.0.2                                 cisco2
```

因此，同時使用全域性配置和特定金鑰環非常危險，並可能導致問題。

IKEv2上的金鑰環 — 未出現問題

雖然IKEv2協定使用與IKEv1類似的概念，但金鑰環選擇不會導致類似的問題。

在簡單情況下，僅交換四個資料包。確定應在響應方上選擇哪個IKEv2配置檔案的IKEID由第三個資料包中的發起方傳送。第三個資料包已加密。

這兩種協定的最大區別在於IKEv2僅使用DH結果進行金鑰計算。計算用於加密/解密的金鑰不再需要

預共用金鑰。

IKEv2 RFC（5996，第2.14節）說明：

共用金鑰的計算方法如下。從IKE_SA_INIT交換期間交換的元數和交換期間建立的Diffie-Hellman共用金鑰計算一個稱為SKEYED的數量。

在同一節中，RFC也指出：

```
SKEYSEED = prf(Ni | Nr, g^ir)
```

所有必要資訊在前兩個資料包中傳送，並且計算SKEYED時無需使用預共用金鑰。

請將其與IKE RFC（2409，第3.2節）比較，其中指出：

SKEY ID是一個字串，它源自只有交易中的活躍玩家才知道的秘密材料。

「只有活動參與者才能知道的秘密材料」是預先共用的金鑰。在第5節中，RFC還指出：

對於預共用金鑰：SKYID = prf(**pre-shared-key**, Ni_b | Nr_b)

這解釋了預共用金鑰的IKEv1設計導致如此多問題的原因。當證書用於身份驗證時，IKEv1中不存在這些問題。

IKE配置檔案選擇條件

這是IKE配置檔案選擇標準的摘要。請參見後續章節以瞭解更多詳細資訊。

配置檔案選擇	**啟動器** 應該對其進行配置（在IPSec配置檔案或加密對映中設定）。 如果沒有設定，請首先與組態 遠端對等體應僅與一個特定的ISAKMP配置檔案匹配，如果在兩個ISAKMP配置檔案中匹配對

本節還介紹選擇不正確的配置檔案時發生的典型錯誤。

IKE發起程式上的IKE配置檔案選擇順序

VTI介面通常指向具有特定IKE配置檔案的特定IPSec配置檔案。然後，路由器知道使用哪個IKE配置檔案。

同樣，加密對映指向特定的IKE配置檔案，並且路由器會因為配置而知道使用哪個配置檔案。

但是在某些情況下，可能未指定配置檔案，並且無法直接從配置確定要使用的配置檔案；在本示例中，未在IPSec配置檔案中選擇IKE配置檔案：

```
crypto isakmp profile profile1
  keyring keyring
  match identity address 192.168.0.0 255.255.255.0
crypto isakmp profile profile2
  keyring keyring
  match identity address 192.168.0.2 255.255.255.255

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
```

```
 mode tunnel

crypto ipsec profile profile1
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
```

當此啟動器嘗試將MM1資料包傳送到192.168.0.2時，選擇最具體的配置檔案：

```
*Oct  7 07:53:46.474: ISAKMP:(0): SA request profile is profile2
```

IKE響應器上的IKE配置檔案選擇順序

IKE響應方上的配置檔案選擇順序與金鑰環選擇順序類似，其中最具體的順序優先。

假設以下設定：

```
crypto isakmp profile profile1
  keyring keyring
  match identity address 192.168.0.0 255.255.255.0
crypto isakmp profile profile2
  keyring keyring
  match identity address 192.168.0.1 255.255.255.255
```

收到來自192.168.0.1的連線時，將選擇profile2。

配置檔案的順序並不重要。show running-config命令會將每個新配置的配置檔案置於清單的末尾。

有時，響應方可能具有使用相同金鑰環的兩個IKE配置檔案。如果在響應器上選擇了不正確的配置檔案，但選定的金鑰環正確，則身份驗證將正確完成：

```
*Oct  7 06:46:39.893: ISAKMP:(1003): processing ID payload. message ID = 0
*Oct  7 06:46:39.893: ISAKMP (1003): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.1
       protocol     : 17
       port         : 500
       length       : 12
*Oct  7 06:46:39.893: ISAKMP:(0):: peer matches profile2 profile
*Oct  7 06:46:39.893: ISAKMP:(0):key for 192.168.0.1 not available in default
*Oct  7 06:46:39.893: ISAKMP:(0):key for 192.168.0.1 found in keyring
*Oct  7 06:46:39.893: ISAKMP:(0):ISAKMP: Selecting  192.168.0.1,255.255.255.255
as final key

*Oct  7 06:46:39.893: ISAKMP:(1003):SA authentication status:
       authenticated
*Oct  7 06:46:39.893: ISAKMP:(1003):SA has been authenticated with 192.168.0.1
*Oct  7 06:46:39.893: ISAKMP:(1003):SA authentication status:
       authenticated

*Oct  7 06:46:39.893: ISAKMP:(1003):Old State = IKE_R_MM5  New State =
IKE_P1_COMPLETE
```

響應方接收並接受QM建議並嘗試生成IPSec安全引數索引(SPI)。 在此範例中，為了清楚起見，刪除了某些調試：

```
*Oct  7 06:46:39.898: ISAKMP:(1003):Checking IPSec proposal 1
*Oct  7 06:46:39.898: ISAKMP:(1003):atts are acceptable.
*Oct  7 06:46:39.898: IPSEC(validate_proposal_request): proposal part #1
```

此時，響應程式失敗，並報告正確的ISAKMP配置檔案不匹配：

```
 (key eng. msg.) INBOUND local= 192.168.0.2:0, remote= 192.168.0.1:0,
   local_proxy= 192.168.0.2/255.255.255.255/47/0,
   remote_proxy= 192.168.0.1/255.255.255.255/47/0,
   protocol= ESP, transform= NONE  (Tunnel),
   lifedur= 0s and 0kb,
   spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Oct  7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct  7 06:46:39.898: Crypto mapdb : proxy_match
       src addr     : 192.168.0.2
       dst addr     : 192.168.0.1
       protocol     : 47
       src port     : 0
       dst port     : 0
*Oct  7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct  7 06:46:39.898: Crypto mapdb : proxy_match
       src addr     : 192.168.0.2
       dst addr     : 192.168.0.1
       protocol     : 47
       src port     : 0
       dst port     : 0
*Oct  7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct  7 06:46:39.898: map_db_find_best did not find matching map
*Oct  7 06:46:39.898: IPSEC(ipsec_process_proposal): proxy identities not
supported
*Oct  7 06:46:39.898: ISAKMP:(1003): IPSec policy invalidated proposal with
error 32
*Oct  7 06:46:39.898: ISAKMP:(1003): phase 2 SA policy not acceptable!
(local 192.168.0.2 remote 192.168.0.1)
*Oct  7 06:46:39.898: ISAKMP: set new node 1993778370 to QM_IDLE
R2#
*Oct  7 06:46:39.898: ISAKMP:(1003):Sending NOTIFY PROPOSAL_NOT_CHOSEN
protocol 3
```

由於IKE配置檔案選擇不正確，因此返回錯誤32，響應方將傳送消息PROPOSAL_NOT_CHOSEN。

摘要

對於IKEv1，使用預共用金鑰和DH結果來計算從MM5開始的加密所使用的金鑰。在接收MM3後，ISAKMP接收方尚無法確定應使用哪個ISAKMP配置檔案（以及關聯的金鑰環），因為IKEID是在MM5和MM6中傳送的。

結果是ISAKMP響應程式嘗試搜尋所有全域性定義的金鑰環，以便查詢特定對等體的金鑰。對於不同的IP地址，選擇最佳匹配金鑰環（最具體）；對於同一IP地址，使用配置中的第一個匹配金鑰。金鑰環用於計算用於解密MM5的金鑰。

在收到MM5後，ISAKMP啟動器會確定ISAKMP配置檔案和相關金鑰環。如果該金鑰環是為MM4 DH計算選擇的金鑰環，則發起方執行驗證；否則，連線失敗。

在全域性配置中配置的金鑰環的順序非常重要。因此，對於ISAKMP響應程式，應儘可能使用包含多個條目的單個金鑰環。

在全域性配置模式下定義的預共用金鑰屬於名為default的預定義金鑰環。同樣的規則也適用。

為響應方選擇IKE配置檔案，將匹配最具體的配置檔案。對於啟動器，使用配置中的配置檔案；如果無法確定該配置檔案，則使用最佳匹配。

對於不同的ISAKMP配置檔案使用不同證書的情況也存在類似問題。當選擇不同的證書時，身份驗證可能會由於「ca trust-point」配置檔案驗證而失敗。此問題將在單獨文檔中說明。

本文中描述的問題不是思科特有的問題，而是與IKEv1協定設計的侷限性有關。用於證書的IKEv1沒有這些限制，用於預共用金鑰和證書的IKEv2沒有這些限制。

相關資訊

- Cisco IOS版本15M&T的Internet Key Exchange for IPsec VPN配置指南的證書到ISAKMP配置檔案對映部分
- Cisco IOS Security Command Reference(思科IOS安全命令參考)的ca trust-point through clear eou部分：命令A到C
- 技術支援與文件 - Cisco Systems