钥匙圈和配置文件的IOS IKEv1/IKEv2选择规则-故障排除指南

目录

简介

本文描述使用多个互联网安全关联和密钥管理协议(ISAKMP)配置文件的多个钥匙圈在Cisco IOS软件LAN对LAN VPN方案。当使用时，它包括Cisco IOS软件版本15.3T行为以及潜在问题多个钥匙圈。

两个方案根据有两ISAKMP配置文件的一个VPN通道被提交，在每个路由器。每配置文件有一个不同的钥匙圈用附加的同样IP地址。方案显示出， VPN通道可以从连接的一端仅被发起由于配置文件选择和验证。

本文的以下部分汇总钥匙圈配置文件的选择标准Internet Key Exchange (IKE)发起者和IKE响应方的。当不同的IP地址由在IKE响应方时的钥匙圈使用，配置正确地工作，但是使用同样IP地址制造在第一个方案提交的问题。

随后部分说明为什么出现默认钥匙圈(全局配置)，并且特定钥匙圈也许导致问题，并且使用互联网密钥交换版本2 (IKEv2)协议为什么避免该问题。

最终部分与生成的典型的错误一起提交IKE配置文件的选择标准两个的IKE发起者和响应方的，当一不正确配置文件选择时。

配置

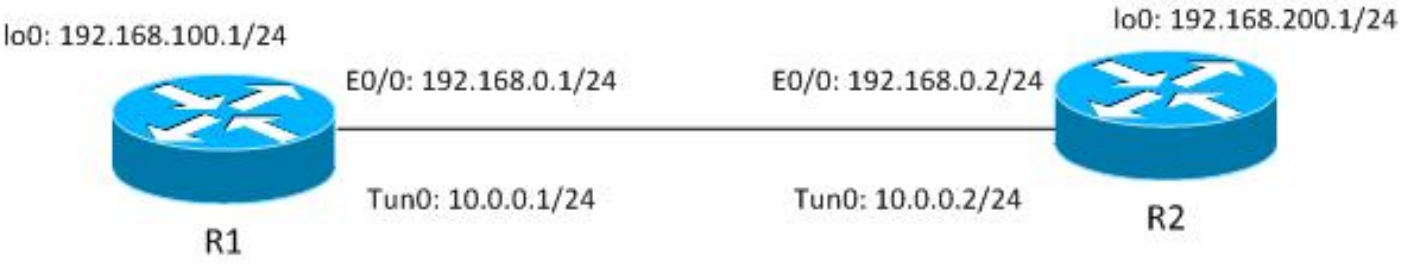
注意：

确定Cisco CLI分析器(仅限注册用户)支持**显示**命令。请使用Cisco CLI分析器为了查看show命令输出分析。

使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

拓扑

Router1 (R1)和Router2 (R2)使用虚拟隧道接口(VTI) (通用路由封装[GRE])接口为了访问其环回。该VTI由Internet协议安全性(IPSec)保护。



R1和R2有两ISAKMP配置文件，其中每一与另外钥匙圈。所有钥匙圈有同一个密码。

R1网络和VPN

R1网络和VPN的配置是：

```
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网络和VPN

R2网络和VPN的配置是：

```
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
```

所有钥匙圈使用同样对端IP地址并且使用密码‘cisco’。

在R1， profile2使用VPN连接。Profile2是第二配置文件在配置里，在配置里使用第二个钥匙圈。因为您将看到，钥匙圈命令是关键。

示例情景

在第一个方案中， R1是ISAKMP发起者。通道正确地协商，并且流量保护正如所料。

当phase1协商失败时，第二个场景使用同一拓扑，但是有R2作为ISAKMP发起者。

互联网密钥交换版本1 (IKEv1)需要skey计算的一预先共享密钥，用于为了解密/加密主模式数据包5 (MM5)和随后的IKEv1数据包。skey从Diffie-Hellman (DH)计算和预先共享密钥派生。需要确定预先共享密钥，在MM3 (响应方)后或MM4 (发起者)接收，因此skey，用于MM5/MM6，能计算。

对于在MM3的ISAKMP响应方，没有确定特定ISAKMP简档，因为那发生，在IKEID在MM5后接收。反而，所有钥匙圈被搜索预先共享密钥，并且第一或最佳匹配从全局配置的钥匙圈选择。该钥匙圈用于为了计算使用MM5 MM6的解密和加密的skey。在MM5的解密和在ISAKMP简档以后和相关的钥匙圈以后，如果同一个钥匙圈选择，确定， ISAKMP响应方进行验证;如果同一个钥匙圈没有选择，连接丢弃。

因此，为ISAKMP响应方，您应该以多个条目使用单个钥匙圈若情况许可。

R1作为IKE发起者(请更正)

此方案描述什么发生，当R1是IKE发起者：

1. 请使用这些调试R1和R2 ：

```
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
```

2. R1发起通道，发送有策略建议的MM1数据包，并且接收在答复的MM2。MM3然后准备：

```
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
```
从外边， R1知道应该使用ISAKMP profile2，因为一定在用于该VTI的IPSec简档下。

因此，正确钥匙圈(keyring2)选择。当MM3数据包准备时，从keyring2的预先共享密钥使用作为密钥材料DH计算。

3. 当R2 MM3数据包，它仍然不知道的接收应该使用哪ISAKMP简档，但是它需要DH生成的一预先共享密钥。所以R2搜索所有钥匙圈为了查找该对等体的预先共享密钥：

```
*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
```
192.168.0.1的密钥在第一个定义的钥匙圈(keyring1)被找到。

4. R2然后准备MM4数据包有DH计算的和有从keyring1的‘cisco’密钥的：

```
*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. 当R1接收MM4时，准备MM5数据包有IKEID的和有及早选择的正确密钥的(从keyring2)：

```
*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. MM5数据包，包含192.168.0.1 IKEID，由R2接收。这时， R2知道对哪ISAKMP简档流量应该一定(匹配标识addresscommand)：

```
*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. R2当前进行验证，如果为MM4数据包盲目选择的钥匙圈是相同的象为ISAKMP简档配置的钥匙圈当前选择。由于keyring1是第一个在配置里，以前选择，并且当前选择。验证是成功的，并且MM6数据包可以发送：

```
*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. 因为从第一数据包，知道R1接收MM6，并且不需要进行钥匙圈的验证;发起者总是了解使用的哪ISAKMP简档，并且什么钥匙圈关联与该配置文件。验证正确地是成功和阶段1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. 第2阶段通常开始和顺利地完成。

此方案仅正确地工作由于定义的钥匙圈正确定货在R2。应该使用VPN会话的配置文件使用是第一在配置里的钥匙圈。

R2作为IKE发起者(不正确)

此方案描述什么发生，当R2发起同一个通道并且解释通道为什么不会设立。一些日志删除为了着重在此和前一个示例之间的区别：

1. R2发起通道：

```
*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
```

2. 因为R2是发起者， ISAKMP简档和钥匙圈知道。从keyring1的预先共享密钥在MM3使用DH计算和发送。R2接收MM2和准备根据该密钥的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接收从R2的MM3。在此阶段， R1不知道哪ISAKMP简档使用的，因此不知道使用的哪个钥匙圈。R1因而使用从全局配置的第一个钥匙圈，是keyring1。R1使用DH计算和发送的MM4预先共享密钥：

```
*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接收从R1的MM4，使用从keyring1的预先共享密钥为了计算DH，并且准备MM5数据包和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接收从R1的MM5。由于IKEID等于192.168.0， profile2选择。Keyring2在profile2，因此keyring2配置选择。以前，对于在MM4的DH计算， R1选择第一个配置的钥匙圈，是keyring1。即使密码正确地是相同的，钥匙圈的验证发生故障，因为这些是不同的钥匙圈对象：

```
*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
```

另外预先共享密钥的调试

上一个方案使用了同一密钥(‘cisco’)。因此，既使当使用了不正确钥匙圈， MM5数据包可能正确地解密和丢弃的以后由于钥匙圈验证失败。

在不同的密钥使用的方案中， MM5不可能解密，并且此错误消息出现：

```
*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
```

钥匙圈选择标准

这是钥匙圈选择标准的摘要。请参阅以下部分关于其他详细信息。

	发起者	响
用不同的IP地址的多个钥匙圈	已配置的。如果不明确地配置从配置的多数特定	多
多个钥匙圈用同样IP地址	已配置的。如果不明确地配置**配置变得无法预测和不支持的。一个人不应该配置同样IP地址的两密钥。**	配

此部分也描述出现默认钥匙圈(全局配置)，并且特定钥匙圈为什么也许导致问题并且说明使用IKEv2协议为什么避免这样问题。

在IKE发起者的钥匙圈选择顺序

对于与VTI的配置，发起者使用一个特定隧道接口对特定IPSec简档的该点。由于IPSec简档以一个特定钥匙圈使用一特定IKE配置文件，没有使用的钥匙圈的混乱。

加密映射，也指向与一个特定钥匙圈的一特定IKE配置文件，相似地作用。

然而，确定从使用的钥匙圈的配置总是不可能的。例如，这发生，当没有配置的IKE配置文件即-，IPSec简档没有配置为了使用IKE配置文件：

```
*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
```

如果此IKE发起者设法发送MM1，将选择最特定的钥匙圈：

```
*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
```

因为发起者没有配置的IKE配置文件，当接收MM6，不会点击配置文件并且完整与成功认证和快速模式：

```
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
```

在IKE响应方的钥匙圈选择顺序-不同的IP地址

与钥匙圈选择的问题在响应方。当钥匙圈使用不同的IP地址时，选择顺序简单。

假设IKE响应方有此配置：

```
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
```

当此响应方收到从IKE发起者的MM1数据包与IP地址192.168.0.2，将选择最好的(多数特定)匹配，既使当命令在配置里不同的。

选择顺序的标准是：

1. 仅密钥用IP地址考虑。
2. 虚拟路由和转发(VRF)流入数据包被检查(前端VRF [fVRF])。
3. 如果数据包在默认VRF，全局钥匙圈首先被检查。最准确的密钥(网络屏蔽长度)选择。
4. 如果密钥在默认钥匙圈没有被找到，匹配此fVRF的所有钥匙圈被连接。
5. 最准确的密钥(最长的网络屏蔽)匹配。例如， /32在/24更喜欢。

调试确认选择：

```
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
```

在IKE响应方的钥匙圈选择顺序-同样IP地址

当钥匙圈使用同样IP地址时，问题发生。假设IKE响应方有此配置：

```
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
```

此配置变得无法预测和不支持的。一个人不应该配置在作为IKE发起者的R2或问题的两密钥描述的同样IP地址(不正确)将发生。

钥匙圈全局配置

在全局配置里定义的ISAKMP密钥属于默认钥匙圈：

```
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
```

即使Isakmp key在配置里是最后，处理作为第一在IKE响应方：

```
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，使用全局配置和特定钥匙圈是非常危险的，并且也许导致问题。

在IKEv2的钥匙圈-问题不发生

虽然IKEv2协议使用相似的概念对IKEv1，钥匙圈选择不引起相似的问题。

在简单情况下，有被交换的四数据包。确定的IKEID在响应方应该选择哪IKEv2配置文件由在第三数据包的发起者发送。第三数据包已经加密。

在两份协议的最大的差异是IKEv2使用仅DH结果skey计算。预先共享密钥不再是必要为了计算用于加密/解密的skey。

IKEv2 RFC (5996，第2.14部分)，状态：

计算得共享密钥如下。呼叫SKEYSEED的数量从在IKE_SA_INIT交换和Diffie-Hellman共享的机密期间交换的目前计算设立在该交换期间。

在同一个部分，也RFC笔记：

```
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
```

所有必要信息在前两数据包发送，并且没有需要使用预先共享密钥，当SKEYSEED计算时。

此与IKE RFC (2409比较，第3.2部分)，陈述：

SKEYID是从秘密材料派生的字符串仅已知对交换的活动播放机。

该“秘密材料仅已知对活动播放机”是预先共享密钥。在第5部分，也RFC笔记：

预先共享密钥：SKEYID = prf (**预共享密钥**， Ni_b|Nr_b)

这解释预先共享密钥的IKEv1设计为什么引起许多问题。当证书使用验证时，这些问题在IKEv1不存在。

IKE配置文件选择标准

这是IKE配置文件选择标准的摘要。请参阅以下部分关于其他详细信息。

	发起者
配置文件选择	应该配置它(集在IPSec简档或在加密映射)。如果没配置，从配置的第一匹配。 远端对等体只应该匹配一特定ISAKMP简档，如果对等体标识在两ISAKMP配置文件匹配，酉

此部分也描述生成的典型的错误，当一不正确配置文件选择。

IKE在IKE发起者的配置文件选择顺序

VTI接口通常指向与一特定IKE配置文件的一特定IPSec简档。路由器然后知道使用的哪IKE配置文件。

同样地，加密映射指向一特定IKE配置文件，并且路由器知道使用的哪配置文件由于配置。

然而，也许有配置文件没有指定的方案，并且确定直接地从描出使用的配置的地方是不可能的;在本例中， IKE配置文件在IPSec简档没有选择：

```
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
```

当此发起者设法发送MM1数据包到192.168.0.2时，多数特定配置文件选择：

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

IKE在IKE响应方的配置文件选择顺序

在IKE响应方的配置文件选择顺序类似于钥匙圈选择顺序，多数特定获得优先权。

假设采用以下配置：

```
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
```

当从192.168.0.1的一连接接收， profile2将选择。

已配置的配置文件命令不重要。show runnning-config命令放置其中每一新建的已配置的配置文件在列表结束时。

有时响应方也许有使用同一个钥匙圈的两IKE配置文件。如果一不正确配置文件在响应方选择，但是选定钥匙圈正确，验证将正确地完成：

```
*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
```

响应方接收并且接受QM建议并且设法生成IPSec安全参数索引(斯皮)。在本例中，一些调试为了清晰删除：

```
*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
```

这时，响应方出故障并且报告正确ISAKMP简档没有配比：

```
 (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
```

由于不正确IKE配置文件选择，错误32返回，并且响应方传送信息PROPOSAL_NOT_CHOSEN。

摘要

对于IKEv1，预先共享密钥与DH结果一起使用为了计算用于开始在MM5的加密的skey。在它接收MM3后， ISAKMP接收方不能确定哪ISAKMP简档(和相关的钥匙圈)应该使用，因为IKEID在MM5和MM6发送。

结果是ISAKMP响应方设法通过所有全局定义钥匙圈搜索为了查找特定对等体的密钥。对于不同的IP地址，最好的匹配的钥匙圈(多数特定)选择;对于同样IP地址，使用从配置的第一匹配的密钥。钥匙圈用于为了计算使用MM5的解密的skey。

在它接收MM5后， ISAKMP发起者确定ISAKMP简档和相关的钥匙圈。发起者进行验证，如果这是为MM4 DH计算选择的同一个钥匙圈;否则，连接发生故障。

在全局配置方面配置的钥匙圈的定货是关键。因此，为ISAKMP响应方，请以多个条目使用单个钥匙圈若情况许可。

在全局配置模式定义的预先共享密钥属于呼叫默认的一个预定义的钥匙圈。同样规则然后适用。

对于IKE响应方的配置文件选择，多数特定配置文件匹配。对于发起者，使用从配置的配置文件，或者，如果不可能确定那，使用佳匹配。

一相似的问题在使用另外证书不同的ISAKMP配置文件的方案发生。当不同的身份验证选择时，验证也许失效由于‘ca trust-point’配置文件验证。此问题在独立文件将报道。

在此条款描述的问题不是CISCO专用的问题，然而与IKEv1协议设计的限制涉及。IKEv1与证书一起使用没有这些限制，并且用于两预先共享密钥和证书的IKEv2没有这些限制。

相关信息

- 对映射互联网密钥交换的部分的IPsec VPN配置指南的ISAKMP简档的证书， Cisco IOS版本15M&T
- ca trust-point通过Cisco IOS安全命令参考的清楚eou部分：对C的A命令
- 技术支持和文档 - Cisco Systems