IOS IKEv1/IKEv2密钥环和配置文件选择规则 — 故障排除指南

目录

简介

本文档介绍在Cisco IOS®软件LAN到LAN VPN场景中对多个互联网安全关联和密钥管理协议(ISAKMP)配置文件使用多个密钥环。它涵盖Cisco IOS软件版本15.3T的行为以及使用多个键环时的潜在问题。

根据VPN隧道，在每台路由器上具有两个ISAKMP配置文件，将提供两种方案。每个配置文件都有不同的密钥环，其IP地址相同。这些场景表明，由于配置文件选择和验证，VPN隧道只能从连接的一端启动。

文档的下一部分汇总了互联网密钥交换(IKE)发起方和IKE响应方的密钥环配置文件的选择条件。当IKE响应器上的密钥环使用不同的IP地址时，配置可以正常工作，但使用相同的IP地址会导致第一个场景中出现的问题。

后续部分解释为什么默认密钥环（全局配置）和特定密钥环都可能导致问题，以及为什么使用Internet密钥交换版本2(IKEv2)协议可以避免此问题。

最后几节为IKE发起方和响应方的IKE配置文件提供选择标准，以及选择不正确的配置文件时出现的典型错误。

配置

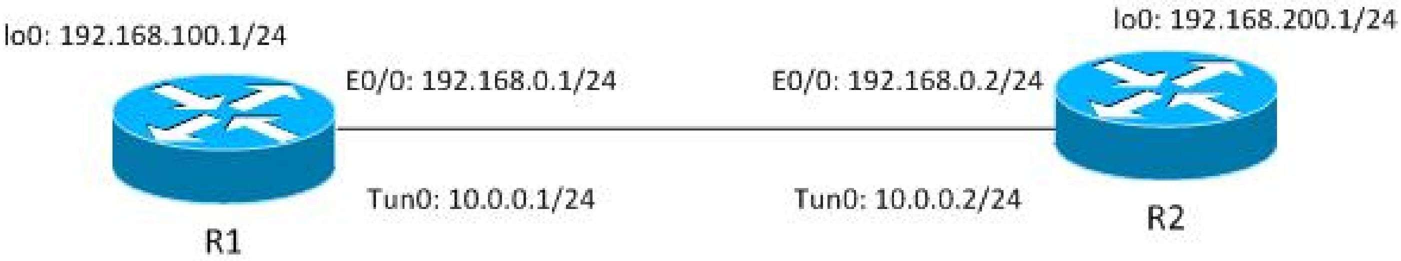
注意：

思科 CLI 分析器（仅适用于注册客户）支持某些 show 命令。要查看对 show 命令输出的分析，请使用思科 CLI 分析器。

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]）接口来访问其环回接口。该VTI受互联网协议安全(IPSec)保护。



R1和R2都有两个ISAKMP配置文件，每个配置文件具有不同的密钥环。所有密钥环的密码都相同。

R1网络和VPN

R1网络和VPN的配置如下：

```
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的配置如下：

```
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
```

所有密钥环使用相同的对等IP地址并使用密码“cisco”。

在R1上，配置文件2用于VPN连接。配置文件2是配置中的第二个配置文件，它使用配置中的第二个密钥环。如您所见，密钥环顺序至关重要。

示例情景

在第一个场景中，R1是ISAKMP发起方。隧道正确协商，流量按预期得到保护。

第二个场景使用相同的拓扑，但当第1阶段协商失败时，R2作为ISAKMP启动器。

互联网密钥交换版本1(IKEv1)需要预共享密钥来计算密钥，该密钥用于解密/加密主模式数据包5(MM5)和后续IKEv1数据包。密钥由Diffie-Hellman(DH)计算和预共享密钥派生。在接收MM3（响应器）或MM4（发起方）后，需要确定该预共享密钥，以便可以计算MM5/MM6中使用的密钥。

对于MM3中的ISAKMP响应器，尚未确定特定ISAKMP配置文件，因为在MM5中接收IKEID后会发生此情况。相反，搜索所有密钥环以查找预共享密钥，并从全局配置中选择第一个或最佳匹配的密钥环。该密钥环用于计算用于MM5解密和MM6加密的密钥。在MM5解密后，在确定ISAKMP配置文件和相关密钥环之后，ISAKMP响应器在选择了相同的密钥环后执行验证；如果未选择同一密钥环，则连接将断开。

因此，对于ISAKMP响应器，应尽可能使用带有多个条目的单个密钥环。

R1作为IKE发起方（正确）

此场景描述当R1是IKE发起方时发生的情况：

1. 对R1和R2使用以下调试：

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

2. R1启动隧道，发送包含策略建议的MM1数据包，并接收MM2作为响应。然后准备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
```

R1从一开始就知道应使用ISAKMP profile2，因为它绑定在用于该VTI的IPSec配置文件下。

因此，已选择正确的密钥环（密钥环2）。当准备MM3数据包时，密钥环2的预共享密钥用作DH计算的密钥材料。

3. 当R2收到该MM3数据包时，它仍不知道应使用哪个ISAKMP配置文件，但它需要预共享密钥来生成DH。因此，R2会搜索所有密钥环以查找该对等体的预共享密钥：

```
*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
```

在第一个定义的密钥环（密钥环1）中找到192.168.0.1的密钥。

4. 然后R2使用DH计算和密钥环1的“cisco”密钥准备MM4数据包：

```
*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. 当R1收到MM4时，它使用IKEID和之前选择的正确密钥（从密钥环2）准备MM5数据包：

```
*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MM5数据包，其中包含IKEID 192.168.0.1。此时，R2知道应将流量绑定到哪个ISAKMP配置文件(**match identity** address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. 现在，R2会执行验证，如果为MM4数据包盲目选择的密钥环与为ISAKMP配置文件配置的密钥环是否相同。由于keyring1是配置中的第一个，因此它以前被选中，现在被选中。验证成功，可以发送MM6数据包：

```
*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，无需对密钥环进行验证，因为它是从第一个数据包中获知的；发起方始终知道要使用的ISAKMP配置文件以及与该配置文件关联的密钥环。身份验证成功，Phase1正确完成：

```
*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阶段正常启动并成功完成。

此方案之所以能正常运行，只是因为R2上定义的密钥环顺序正确。应用于VPN会话的配置文件使用配置中首先使用的密钥环。

R2作为IKE发起方（不正确）

此场景描述了R2启动同一隧道时发生的情况，并解释了为什么不会建立隧道。为了重点介绍此示例与上一个示例之间的差异，已删除一些日志：

1. R2启动隧道：

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

2. 由于R2是启动器，因此ISAKMP配置文件和密钥环已知。密钥环1的预共享密钥用于DH计算，并在MM3中发送。R2正在接收MM2，并基于该密钥准备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从R2接收MM3。在此阶段，R1不知道要使用哪个ISAKMP配置文件，因此它不知道要使用哪个密钥环。因此，R1使用全局配置中的第一个密钥环，即密钥环1。R1使用该预共享密钥进行DH计算并发送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从R1接收MM4，使用密钥环1的预共享密钥来计算DH，并准备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收到来自R1的MM5。由于IKEID等于192.168.0，因此已选择profile2。在profile2中配置了密钥环2，因此选择了keyring2。以前，对于MM4中的DH计算，R1选择了第一个配置的密钥环，即keyring1。即使密码完全相同，密钥环的验证也会失败，因为密钥环的对象不同：

```
*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
```

不同预共享密钥的调试

以前的场景使用相同的密钥(“cisco”)。 因此，即使使用了不正确的密钥环，MM5数据包也可以正确解密并稍后由于密钥环验证失败而丢弃。

在使用不同密钥的情况下，MM5无法解密，并且出现以下错误消息：

```
*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
```

密钥环选择标准

这是密钥环选择标准的摘要。有关更多详细信息，请参阅下一节。

	启动器	**响应方**
具有不同IP地址的多个密钥环	已配置。如果未明确配置配置中最具体的	最具体的
具有相同IP地址的多个密钥环	已配置。如果未明确配置 **配置变得不可预测且不受支持。不应为同一IP地址配置两个密钥。**	**配置变得**

本节还介绍默认密钥环（全局配置）和特定密钥环的存在可能导致问题的原因，并说明为什么使用IKEv2协议可避免此类问题。

IKE启动器上的密钥环选择顺序

对于VTI配置，发起方使用指向特定IPSec配置文件的特定隧道接口。由于IPSec配置文件使用具有特定密钥环的特定IKE配置文件，因此不会混淆要使用哪个密钥环。

加密映射（也指向具有特定密钥环的特定IKE配置文件）以相同方式运行。

但是，从配置中确定要使用哪个密钥环并不总是可能。例如，当未配置IKE配置文件时会发生这种情况 — 即，未配置IPSec配置文件以使用IKE配置文件：

```
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发起方尝试发送MM1，它将选择最具体的密钥环：

```
*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
```

由于发起方在收到MM6时未配置IKE配置文件，因此它不会命中配置文件，并将完成成功的身份验证和快速模式(QM):

```
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响应器上的密钥环选择顺序 — 不同IP地址

键环选择问题出在响应器上。当键环使用不同的IP地址时，选择顺序很简单。

假设IKE响应器具有以下配置：

```
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
```

当此响应方从IP地址为192.168.0.2的IKE发起方收到MM1数据包时，它将选择最佳（最具体）匹配，即使配置顺序不同也是如此。

选择顺序的标准为：

1. 仅考虑具有IP地址的密钥。
2. 检查传入数据包的虚拟路由和转发(VRF)（前端VRF [fVRF]）。
3. 如果数据包在默认VRF中，则首先检查全局密钥环。选择最精确的密钥（网络掩码长度）。
4. 如果在默认密钥环中未找到密钥，则匹配此fVRF的所有密钥环都将连接。
5. 匹配最精确的密钥（最长网络掩码）。例如，比起/24,/32是首选。

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
```

IKE响应器上的密钥环选择顺序 — 相同IP地址

当密钥环使用相同的IP地址时，会出现问题。假设IKE响应器具有以下配置：

```
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
```

此配置变得不可预测且不受支持。不应为同一IP地址配置两个密钥，否则R2中描述的问题将作为IKE发起程序(不正确)。

密钥环全局配置

在全局配置中定义的ISAKMP密钥属于默认密钥环：

```
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密钥在配置中是最后一个，它仍作为IKE响应器上的第一个进行处理：

```
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密钥环的风险很大，可能导致问题。

IKEv2上的密钥环 — 问题不发生

尽管IKEv2协议使用与IKEv1类似的概念，但密钥环选择不会导致类似问题。

在简单情况下，只交换四个数据包。确定应在响应器上选择哪个IKEv2配置文件的IKEID由第三个数据包中的发起方发送。第三个数据包已加密。

这两种协议的最大区别是IKEv2仅使用DH结果进行密钥计算。为了计算用于加密/解密的密钥，不再需要预共享密钥。

IKEv2 RFC（5996，第2.14节）指出：

共享密钥的计算方式如下。从在IKE_SA_INIT交换期间交换的非数和在该交换期间建立的Diffie-Hellman共享密钥中计算称为SKEYSEED的数量。

在同一部分，RFC还注意到：

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

前两个数据包中发送了所有必要信息，计算SKEYSEED时无需使用预共享密钥。

请将此与IKE RFC（2409，第3.2节）进行比较，其中指出：

SKEYID是从仅交换中活动玩家知道的秘密材料派生的字符串。

“只有活跃玩家才知道的秘密材料”是预共享密钥。在第5部分，RFC还注意到：

对于预共享密钥：SKEYID = prf(**预共享密钥**,Ni_b | Nr_b)

这解释了为什么预共享密钥的IKEv1设计会导致如此多问题。当证书用于身份验证时，IKEv1中不存在这些问题。

IKE配置文件选择条件

这是IKE配置文件选择条件的摘要。有关更多详细信息，请参阅下一节。

	启动器
配置文件选择	应配置它（在IPSec配置文件或加密映射中设置）。 如果未配置，请首先从配置中匹配。 远程对等体应仅匹配一个特定ISAKMP配置文件，如果对等体身份在两个ISAKMP配置文件中

本节还介绍选择不正确的配置文件时出现的典型错误。

IKE发起方上的IKE配置文件选择顺序

VTI接口通常指向具有特定IKE配置文件的特定IPSec配置文件。然后，路由器会知道要使用哪个IKE配置文件。

同样，加密映射指向特定IKE配置文件，并且路由器知道由于配置而要使用哪个配置文件。

但是，可能存在未指定配置文件以及无法直接从配置中确定要使用哪个配置文件的情况；在本例中，未在IPSec配置文件中选择IKE配置文件：

```
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
```

当此启动器尝试将MM1数据包发送到192.168.0.2时，将选择最具体的配置文件：

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

IKE响应器上的IKE配置文件选择顺序

IKE响应器上的配置文件选择顺序类似于键环选择顺序，其中最具体优先。

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
```

当收到来自192.168.0.1的连接时，将选择profile2。

配置的配置文件的顺序并不重要。**show running-config**命令将每个新配置的配置文件置于列表末尾。

有时，响应方可能有两个使用相同密钥环的IKE配置文件。如果响应器上选择的配置文件不正确，但所选的密钥环正确，则身份验证将正确完成：

```
*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
```

响应方接收并接受QM建议并尝试生成IPSec安全参数索引(SPI)。 在本例中，为了清楚起见，删除了一些调试：

```
*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
```

此时，响应方发生故障，并报告正确的ISAKMP配置文件不匹配：

```
 (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
```

由于IKE配置文件选择不正确，返回错误32，响应方发送消息PROPOSAL_NOT_COSEN。

摘要

对于IKEv1，预共享密钥与DH结果一起使用，以计算从MM5开始的用于加密的密钥。在接收MM3后，ISAKMP接收器尚无法确定应使用哪个ISAKMP配置文件（和关联的密钥环），因为IKEID在MM5和MM6中发送。

结果是，ISAKMP响应器尝试搜索所有全局定义的密钥环，以查找特定对等体的密钥。对于不同的IP地址，选择最匹配的密钥环（最具体）；对于同一IP地址，使用配置中的第一个匹配密钥。密钥环用于计算用于解密MM5的密钥。

在收到MM5后，ISAKMP发起方确定ISAKMP配置文件和关联密钥环。如果该密钥环与为MM4 DH计算选择的密钥环相同，则发起方会执行验证；否则，连接将失败。

在全局配置中配置的密钥环的顺序至关重要。因此，对于ISAKMP响应器，请尽可能使用具有多个条目的单个密钥环。

在全局配置模式下定义的预共享密钥属于称为default的预定义密钥环。同样的规则也适用。

对于响应器的IKE配置文件选择，匹配最具体的配置文件。对于启动器，使用配置中的配置文件，或者，如果无法确定，则使用最佳匹配。

在对不同ISAKMP配置文件使用不同证书的场景中也会出现类似问题。选择其他证书时，身份验证可能会因“ca trust-point”配置文件验证而失败。此问题将在单独的文档中介绍。

本文中描述的问题不是思科特定的问题，而是与IKEv1协议设计的局限性有关。与证书一起使用的IKEv1没有这些限制，用于预共享密钥和证书的IKEv2也没有这些限制。

相关信息

- Internet Key Exchange for IPsec VPNs配置指南的Certificate to ISAKMP Profile Mapping部分，Cisco IOS版本15M&T
- ca trust-point至clear eou部分的Cisco IOS安全命令参考：命令A到C
- 技术支持和文档 - Cisco Systems