# キーリングとプロファイルに関する IOS IKEv1/IKEv2 選択ルール - トラブルシューティング ガイド

## 内容



## 概要

このドキュメントでは、Cisco IOS® ソフトウェア LAN 間 VPN シナリオで複数の Internet Security Association and Key Management Protocol ( ISAKMP ) プロファイルに対して複数のキーリングを使用する方法について説明します。複数のキーリングを使用した場合の Cisco IOS ソフトウェア リリース 15.3T の動作と潜在的な問題を取り上げます。

ルータごとに 2 つずつの ISAKMP プロファイルを使用する VPN トンネルをベースにした 2 つのシナリオを紹介します。プロファイルごとに IP アドレスが同じ別々のキーリングがアタッチされています。このシナリオでは、プロファイルの選択と検証を通して、VPN トンネルを接続の片側からのみ開始できることを示します。

次の項では、インターネット キー エクスチェンジ ( IKE ) イニシエータと IKE レスポンダの両方のキーリング プロファイルの選択基準について簡単に説明します。IKE レスポンダのキーリングで複数の IP アドレスが使用されている場合、その構成は正しく動作しますが、同じ IP アドレスを使用することによって、最初のシナリオで提示された問題が発生します。

その次の項では、デフォルト キーリング ( グローバル コンフィギュレーション ) と特定のキーリ

ングの両方の存在が問題に発展する理由と、その問題の解決にインターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルを使用する理由について説明します。

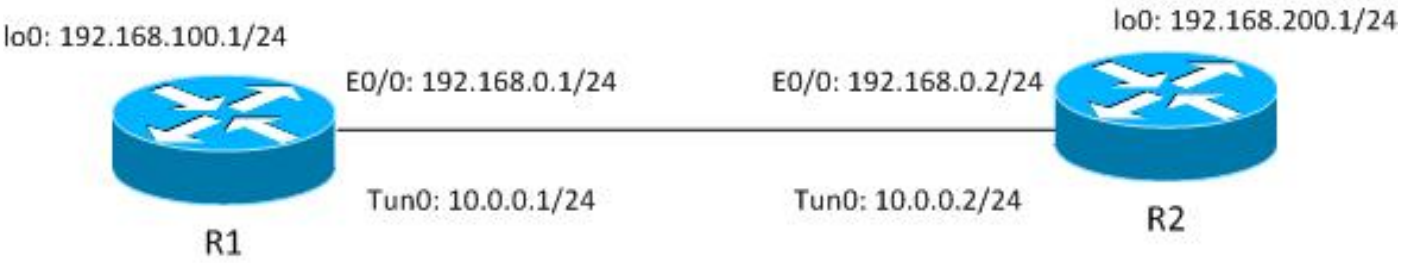
最後の項では、IKE イニシエータと IKE レスポンダの両方の IKE プロファイルの選択基準と、間違ったプロファイルが選択されたときに発生する一般的なエラーを示します。

# コンフィギュレーション

> **注：**
>
> Cisco CLI アナライザ（登録ユーザ専用）は、特定の show コマンドをサポートします。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。
>
> **debug コマンドを使用する前に、「**デバッグ コマンドの重要な情報」を参照してください。

## トポロジ

Router1（R1）と Router2（R2）では、そのループバックにアクセスするために、仮想トンネル インターフェイス（VTI）（Generic Routing Encapsulation（GRE）インターフェイス）が使用されています。この VTI はインターネット プロトコル セキュリティ（IPsec）によって保護されています。




R1 と R2 の両方にキーリングが異なる 2 つの ISAKMP プロファイルが設定されています。すべてのキー リングに同じパスワードが設定されています。

## R1 ネットワークと VPN

R1 ネットワークと VPN の設定は次のとおりです。

```
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 ネットワークと VPN

R2 ネットワークと VPN の設定は次のとおりです。

```
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
```

すべてのキーリングで同じピア IP アドレスとパスワード "cisco" が使用されます。

R1 では、VPN の接続に profile2 が使用されます。Profile2 は、設定内の 2 つ目のプロファイルで、設定内の 2 つ目のキーリングが使用されます。後述しますが、キーリング順序が極めて重要です。

# シナリオ例

最初のシナリオでは、R1 が ISAKMP イニシエータです。トンネルは正しくネゴシエートされ、トラフィックは想定どおりに保護されます。

2 つ目のシナリオでは、同じトポロジが使用されますが、フェーズ 1 のネゴシエーションが失敗した場合の ISAKMP イニシエータとして R2 が用意されます。

インターネット キー エクスチェンジ バージョン 1（IKEv1）では skey の計算に事前共有キーが必要です。このキーは、メイン モード パケット 5（MM5）とそれに続く IKEv1 パケットの復号化/暗号化に使用されます。skey は Diffie-Hellman（DH）の計算と事前共有キーから抽出されます。この事前共有キーは、MM3（レスポンダ）と MM4（イニシエータ）の受信後に決定して、MM5/MM6 で使用される skey の計算に使用できるようにする必要があります。

MM3のISAKMPレスポンダでは、IKEIDがMM5で受信された後に発生するため、特定のISAKMPプロファイルがまだ決定されません。代わりに、すべてのキーリングが事前共有キーを検索され、グローバル設定から最初または最適なキーリングが選択されます。このキーリングは、MM5の復号化とMM6の暗号化に使用されるキーを計算するために使用されます。MM5の復号化と、ISAKMPプロファイルと関連するキーリングが決定された後、ISAKMPレスポンダは同じキーリングが選択されているかどうかを検証します。同じキー リングが選択されていない場合は、接続がドロップされます。

そのため、ISAKMP レスポンダは、できるだけ、複数のエントリを持つ単一のキーリングを使用する必要があります。

## IKE イニシエータとしての R1（正）

このシナリオでは、R1 が IKE イニシエータの場合にどうなるかについて説明します。

1. R1 と R2 の両方に次のデバッグを使用します。

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

2. R1 は、トンネルを開始して、ポリシー提案を含む MM1 パケットを送信し、応答で MM2 を受信します。その後で、MM3 が準備されます。

```
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
```

最初から、R1 は ISAKMP profile2 を使用する必要があることを認識しています。これは、そのプロファイルが VTI に使用される IPSec プロファイルに基づいてバインドされるためです。

よって、正しいキーリング（keyring2）が選択されます。keyring2 からの事前共有キーが MM3 パケットの準備中に DH を計算するためのキーリング材料として使用されます。

3. R2 がその MM3 パケットを受信したときは、まだ、使用すべき ISAKMP プロファイルを認識していませんが、DH を生成するための事前共有キーを必要とします。これが、R2 がすべてのキーリングを検索してそのピア用の事前共有キーを探す理由です。

```
*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 のキーが最初に定義されたキーリング（keyring1）で見つかります。

4. その後で、R2 が DH の計算結果と keyring1 から "cisco" キーを使用して MM4 パケットを準備します。

```
*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. R1 が MM4 を受信すると、IKEID と以前選択された正しいキー（keyring2 から）を使用して MM5 パケットを準備します。

```
*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. 192.168.0.1のIKEIDを含むMM5パケットが、R2によって受信されます。この時点で、R2は、トラフィックがバインドされるISAKMPプロファイル(**match identity** addressコマンド)を認識します。

```
*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. ここで、R2 は MM4 パケット用に自動的に選択されたキーリングが、選択された ISAKMP プロファイル用に設定されたキーリングと同じかどうかを検証します。keyring1 が設定内の最初のキーリングのため、すでに選択されており、今も選択されたままです。検証が成功して、MM6 パケットを送信できます。

```
*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 が MM6 を受信しますが、最初のパケットからすでにわかっているため、キーリングを検証する必要がありません。イニシエータは、必ず、使用する ISAKMP プロファイルとそのプロファイルに関連付けられたキーリングを認識しています。認証が成功して、Phase1 が正常に終了します。

```
*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. Phase2 が正常に開始して、正常に終了します。

このシナリオが正しく動作するのは、R2で定義されたキーリングの正しい順序が原因です。VPNセッションに使用する必要があるプロファイルでは、設定の最初のキーリングが使用されます。

## IKE イニシエータとしての R2 ( 誤 )

このシナリオでは、R2 が同じトンネルを開始したときにどうなるかと、トンネルが確立されない理由について説明します。この例と前の例の違いを明確にするために、一部の口グが省略されています。

1. R2 がトンネルを開始します。

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

2. R2 がイニシエータであるため、ISAKMP プロファイルとキーリングを認識しています。keyring1からの事前共有キーはDHの計算に使用され、MM3で送信されます。R2はMM2を受信し、そのキーに基づいてMM3を準備しています。

```
*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はR2からMM3を受信します。この段階で、R1はどのISAKMPプロファイルを使用するかを認識しないため、どのキーリングを使用すればよいかを認識しません。したがって、R1はグローバル設定の最初のキーリング(keyring1)を使用します。R1はDH計算に事前共有キーを使用し、MM4を送信します。

```
*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 が R1 から MM4 を受信して、keyring1 からの事前共有キーを使用して DH を計算し、MM5 パケットと IKEID を準備します。

```
*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はR1からMM5を受信します。IKEIDが192.168.0であるため、profile2が選択されています。profile2 内で keyring2 が設定されているため、keyring2 が選択されます。以前は、MM4でのDHの計算では、R1がキーリング1として最初に設定したキーリングを選択していました。パスワードは完全に同じであっても、キーリングの検証は失敗します。これは異なるキーリングオブジェクトであるためです。

```
*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
```

## 複数の事前共有キーのデバッグ

前回のシナリオでは同じキー ( "cisco" ) が使用されました。 そのため、間違ったキーリングが使用された場合でも、キーリングの検証が失敗するため、MM5 パケットを正常に復号化して、後でドロップすることができます。

複数のキーが使用されるシナリオでは、MM5 を復号化できず、次のエラー メッセージが表示されます。

```
*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
```

# キーリング選択基準

これは、キーリング選択基準のサマリです。詳細については、次の項を参照してください。

| | 依頼者 ( Initiator ) |
|---|---|
| 別々の IP アドレスを持つ複数のキーリング | 設定済み。コンフィギュレーションからの最も固有のものが明示的に |
| 同じ IP アドレスを持つ複数のキーリング | 設定済み。明示的に設定されていない場合 **設定が予測不能になり、サレスに2つのキーを設定しないでください。** |

ここでは、デフォルト キーリング ( グローバル コンフィギュレーション ) と特定のキーリングの両方の存在が問題に発展する理由と、このような問題を IKEv2 プロトコルを使用して回避する理由について説明します。

## IKE イニシエータでのキーリング選択順序

VTI を使用した設定では、イニシエータが特定の IPsec プロファイルを指している特定のトンネル インターフェイスを使用します。IPsec プロファイルでは特定のキーリングを含む特定の IKE プロファイルが使用されるため、使用すべきキーリングの混同が起きません。

特定のキーリングを含む特定の IKE プロファイルを指している暗号マップも同様に機能します。

ただし、必ずしも、使用すべきキーリングをコンフィギュレーションから決定できるとは限りません。たとえば、IKE プロファイルが設定されていない、つまり、IKE プロファイルを使用するように IPsec プロファイルが設定されていない場合です。

```
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
```

この IKE イニシエータは MM1 を送信するときに、最も固有のキーリングを選択します。

```
*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
```

イニシエータが MM6 を受信しても設定された IKE プロファイルが存在しないため、プロファイルがヒットせず、認証と Quick Mode（QM）が正常に終了します。

```
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
```

## KE レスポンダでのキーリング選択順序 - 別の IP アドレス

キーリングの選択に伴う問題がレスポンダで起こります。キーリングで複数の IP アドレスが使用されている場合は、選択順序がシンプルになります。

IKE レスポンダが次のように設定されているとします。

```
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
```

このレスポンダが IP アドレス 192.168.0.2 を持つ IKE イニシエータから MM1 パケットを受信すると、コンフィギュレーション内の順序が違っていても、最適な（最も固有の）一致を選択します。

選択順序の基準は次のとおりです。

1. IP アドレスを持つキーだけが考慮されます。
2. 着信パケットの Virtual Routing and Forwarding（VRF）がチェックされます（フロントエンド VRF（fVRF））。
3. パケットがデフォルト VRF の場合は、グローバル キーリングが最初にチェックされます。最も正確なキー（ネットマスク長）が選択されます。
4. デフォルト キーリングでキーが見つからなかった場合は、この fVRF と一致するすべてのキーリングが連結されます。
5. 最も正確なキー（最長のネットマスク）が照合されます。たとえば、/32 の方が /24 より優先されます。

デバッグが選択を確認します。

```
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
```

## KE レスポンダでのキーリング選択順序 - 同じ IP アドレス

キーリングで同じ IP アドレスが使用されている場合は、問題が発生します。IKE レスポンダが次のように設定されているとします。

```
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
```

この設定は予測不能になり、サポートされません。同じIPアドレスに2つのキーを設定しないでください。設定すると、「R2 As IKE Initiator」で説明されている問題が発生します（不正解）。

## キーリング グローバル設定

グローバル コンフィギュレーションで定義された ISAKMP キーはデフォルト キーリングに属しています。

```
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
```

ISAKMP キーがコンフィギュレーション内で最後であっても、IKE レスポンダでは最初に処理されます。

```
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
```

そのため、グローバル コンフィギュレーションと特定のキーリングの両方を使用することは、非常に危険なことであり、問題に発展する可能性があります。

## IKEv2 上のキーリング - 問題なし

IKEv2 プロトコルでは IKEv1 と同様の概念が使用されますが、キーリング選択で同様の問題は起きません。

単純なケースでは、4 つのパケットだけが交換されます。レスポンダで選択すべき IKEv2 プロファイルを決定する IKEID が 3 つ目のパケットでイニシエータから送信されます。3 つ目のパケットはすでに暗号化されています。

2 つのプロトコルの最も大きな違いは、IKEv2 では skey の計算に DH の結果しか使用されないことです。事前共有キーは、暗号化/復号化に使用される skey の計算に必要ではなくなっています。

IKEv2 RFC（5996、第 2.14 項）では次のように規定されています。

共有キーは次のように計算されます。SKEYSEED という名前の数量は、IKE_SA_INIT 交換中に交換されるノンスと、交換中に設定される Diffie-Hellman 共有秘密から計算されます。

RFC の同じ項で、次のようにも規定されています。

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

必要な情報のすべてが最初の 2 つのパケットで送信され、SKEYSEED を計算するときに事前共有キーを使用する必要がありません。

これと次のように規定されている IKE RFC（2409、第 3.2 項）を比較してください。

SKEYID は、交換中にアクティブ プレーヤーにのみ知られている秘密の内容から抽出された文字列です。

この「アクティブ プレーヤーにのみ知られている秘密の内容」が事前共有キーです。RFC の第 5 項では、次のように規定されています。

事前共有キーの場合：SKEYID = prf(**pre-shared-key**, Ni_b | Nr_b)

これは、事前共有キーの IKEv1 設計が多くの問題を引き起こす理由を説明しています。これらの問題は、証明書が認証に使用される IKEv1 では発生しません。

# IKE プロファイル選択基準

これは、IKE プロファイル選択基準のサマリです。詳細については、次の項を参照してください。

| | |
|---|---|
| プロファイル選択 | **依頼者（Initiator）**<br>設定する必要があります（IPSecプロファイルまたは暗号マップで設定します）。 設定<br>リモートピアは1つの特定のISAKMPプロファイルにのみ一致する必要があります。ピ |

ここでは、間違ったプロファイルが選択された場合に発生する一般的なエラーについても説明します。

## IKE イニシエータでの IKE プロファイル選択順序

VTI インターフェイスは、通常、特定の IKE プロファイルを含む特定の IPsec プロファイルを指しています。そのため、ルータは使用すべき IKE プロファイルを認識しています。

同様に、暗号マップは特定の IKE プロファイルを指しており、ルータはコンフィギュレーションによって使用すべきプロファイルを認識しています。

ただし、プロファイルが指定されないシナリオや、コンフィギュレーションからは使用すべきプロファイルを直接決定できないシナリオがあります。この例では、IPsec プロファイル内で IKE プロファイルが選択されていません。

```
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
```

このイニシエータが 192.168.0.2 に MM1 パケットを送信しようとすると、最も固有のプロファイルが選択されます。

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

## IKE レスポンダでの IKE プロファイル選択順序

IKE レスポンダ上のプロファイル選択順序は、最も固有のものが優先されるキーリング選択順序と同様です。

次の設定を想定します。

```
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
```

192.168.0.1 からの接続を受信すると、profile2 が選択されます。

設定されたプロファイルの順序は関係ありません。show runnning-config コマンドは、新しく設定されたプロファイルをリストの最後に配置します。

レスポンダに同じキーリングを使用する 2 つの IKE プロファイルが割り当てられる場合があります。レスポンダで間違ったプロファイルが選択されても、選択されたキーリングが正しければ、認証が正常に終了します。

```
*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
```

レスポンダは QM 提案を受信して、受け入れ、IPSec セキュリティ パラメータ インデックス（SPI）を生成しようとします。 この例では、わかりやすくするために一部のデバッグが省略されています。

```
*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
```

この時点で、レスポンダが失敗して、正しい ISAKMP プロファイルが一致しなかったことを報告します。

```
 (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
```

間違った IKE プロファイルを選択したために、エラー 32 が返され、レスポンダはメッセージ PROPOSAL_NOT_CHOSEN を送信します。

# 要約

IKEv1では、MM5で始まる暗号化に使用される鍵を計算するために、事前共有キーがDHの結果と

ともに使用されます。MM3を受信した後、ISAKMPレシーバは、IKEIDがMM5およびMM6で送信されるため、使用するISAKMPプロファイル（および関連キー）を定義はISAKMP

そのため、ISAKMP レスポンダは、特定のピアのキーを見つけるために、グローバルに定義されたすべてのキーリングを検索しようとします。IP アドレスが異なる場合は、最適な一致するキーリング（最も固有の）が選択されます。IP アドレスが同じ場合は、コンフィギュレーションからの最初の一致するキーリングが使用されます。このキーリングは MM5 の復号化に使用される skey の計算に使用されます。

MM5 を受信すると、ISAKMP イニシエータが ISAKMP プロファイルと関連するキーリングを決定します。イニシエータは、これが MM4 DH の計算に選択されたものと同じキーリングかどうかを検証します。そうでない場合は、接続が失敗します。

グローバル コンフィギュレーション内で設定されたキーリングの順序が極めて重要です。そのため、ISAKMP レスポンダは、できるだけ複数のエントリを持つ単一のキーリングを使用します。

グローバル コンフィギュレーション モードで定義された事前共有キーは default という名前の事前定義のキーリングに属しています。その後で、同じルールが適用されます。

レスポンダの IKE プロファイル選択では、最も固有のプロファイルが照合されます。イニシエータでは、コンフィギュレーションからのプロファイルが使用されます。それが決定できない場合は、最適な一致が使用されます。

ISAKMP プロファイルごとに異なる証明書を使用するシナリオで同様の問題が発生します。別の証明書が選択されると、"ca trust-point" プロファイル検証によって、認証が失敗する可能性があります。この問題については、別のドキュメントで説明します。

この記事に記載されている問題は、シスコ固有の問題ではなく、IKEv1 プロトコル設計の制限に関係しています。証明書で使用される IKEv1 にはこれらの制限がなく、事前共有キーと証明書の両方に使用される IKEv2 にもこれらの制限はありません。

# 関連情報

- 『IPSec VPN 用のインターネット キー エクスチェンジ コンフィギュレーション ガイド、Cisco IOS リリース 15M&T』の「証明書と ISAKMP プロファイルのマッピング」の項
- 『Cisco IOS セキュリティ コマンド リファレンス』の「ca trust-point through clear eou」の項コマンド A ~ C
- テクニカル サポートとドキュメント – Cisco Systems