قواعد تحديد IOS IKEv1/IKEv2 لحلقات المفاتيح وتوصيفات التعريف - دليل أستكشاف الأخطاء وإصلاحها

المحتويات

المقدمة

يصف هذا المستند إستخدام حلقات مفاتيح متعددة لتوصيفات بروتوكول إدارة المفاتيح واتصالات الإنترنت (ISAKMP) المتعددة في سيناريو شبكة VPN الخاصة ببرنامج Cisco IOS® Software. وهو يغطي سلوك الإصدار 15.3T من برنامج Cisco IOS Software بالإضافة إلى المشاكل المحتملة عند إستخدام حلقات مفاتيح متعددة.

يتم تقديم سيناريوهين، استنادا إلى نفق VPN مع توصيفات ISAKMP على كل موجه. يحتوي كل ملف تعريف على حلقة مفاتيح مختلفة لها نفس عنوان IP مرفق. توضح السيناريوهات أنه يمكن بدء تشغيل نفق VPN من جانب واحد فقط من الاتصال بسبب تحديد ملف التعريف والتحقق من صحته.

تلخص الأقسام التالية من المستند معايير التحديد لملف تعريف حلقة المفاتيح لكل من بادئ تبادل مفاتيح الإنترنت (IKE) ومستجيب IKE. عندما يتم إستخدام عناوين IP مختلفة بواسطة حلقة المفاتيح على المستجيب لـ IKE، فإن التكوين يعمل بشكل صحيح، ولكن إستخدام عناوين IP نفسها ينشئ المشكلة المقدمة في السيناريو الأول.

توضح الأقسام التالية لماذا قد يؤدي وجود كل من حلقة المفاتيح الافتراضية (التكوين

العام) وحلقات المفاتيح المحددة إلى حدوث مشاكل ولماذا يساعد إستخدام بروتوكول تبادل مفتاح الإنترنت الإصدار 2 (IKEv2) على تجنب هذه المشكلة.

تعرض الأقسام النهائية معايير التحديد لملف تعريف IKE لكل من بادئ ومستجيب IKE، مع الأخطاء النموذجية التي تحدث عند تحديد ملف تخصيص غير صحيح.

التكوين

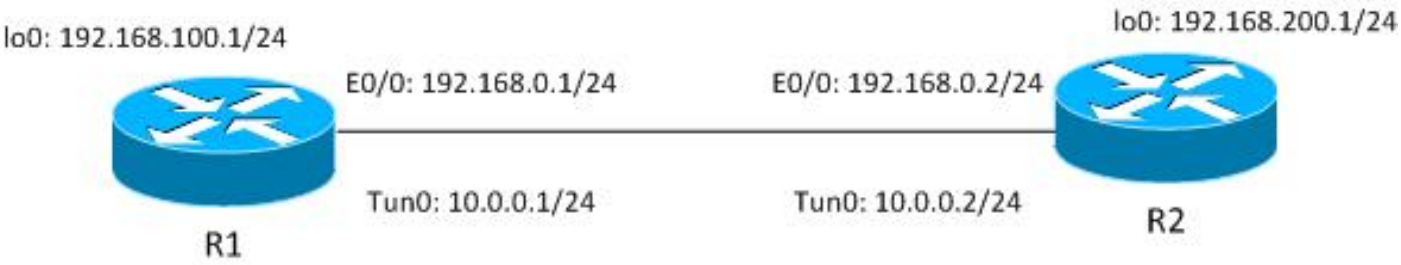
ملاحظات:

يدعم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) (للعملاء المسجلين فقط) أوامر **show** معينة. استخدم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) لعرض تحليل لمخرج الأمر show.

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

طوبولوجيا

يستخدم الموجه 1 (R1) والموجه 2 (R2) واجهات واجهة النفق الظاهرية (VTI) (تضمين التوجيه العام [GRE]) للوصول إلى عمليات الاسترجاع الخاصة به. أن VTI محمي ببروتوكول إنترنت أمن (IPSec).



يحتوي كل من R1 و R2 على توصيفي ISAKMP، لكل منهما حلقة مفاتيح مختلفة. كل حلقات المفاتيح لها نفس كلمة المرور.

شبكة R1 وشبكة VPN

التكوين لشبكة R1 وشبكة VPN:

```
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
```

شبكة R2 وشبكة VPN

التكوين لشبكة R2 وشبكة VPN:

```
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
```

تستخدم كل حلقات المفاتيح نفس عناوين IP للنظير وتستخدم كلمة المرور ' cisco.'

في R1، يستخدم التوصيف2 لاتصال VPN. التوصيف 2 هو التوصيف الثاني في التكوين الذي يستخدم حلقة المفاتيح الثانية في التكوين. كما سترى، فإن ترتيب حلقة المفاتيح أمر بالغ الأهمية.

أمثلة السيناريوهات

في السيناريو الأول، R1 هو بادئ ISAKMP. يتم التفاوض عبر النفق بشكل صحيح، ويتم حماية حركة المرور كما هو متوقع.

ويستخدم السيناريو الثاني نفس المخطط، ولكنه يحتوي على R2 لتم بادئ ISAKMP عندما يكون تفاوض المرحلة 1 الشاف.

يحتاج Internet Key Exchange الإصدار 1 (IKEv1) إلى مفاتح مشترك مسبقا لحساب مفاتح واحد، يتم إستخدامه لكف تشفير/تشفير حزمة الوضع الرئيسي 5 (MM5) وحزم IKEv1 اللاحقة. يتم اشتقاق المفاتح من حساب Diffie-Hellman (DH) والمفاتح المشترك مسبقا. يجب تحديد هذا المفتاح المشترك مسبقا بعد تلقي MM3 (المستجيب) أو MM4 (البادئ)، بحيث يمكن حساب المفتاح، المستخدم في MM5/MM6.

بالنسبة لمجيب ISAKMP في MM3، لم يتم تحديد ملف تعريف ISAKMP المحدد بعد لأن ذلك يحدث بعد إستلام IKEID في MM5. بدلا من ذلك، يتم البحث في كل حلقات المفاتيح عن مطابقة مفاتيح حلقة لأفضل أو أول تحديد، ويتم تحديد مسبقا مفتاح مشترك من التكوين العام. يستخدم هذا المفتاح لحساب المفتاح المستخدم لفك تشفير MM5 وتشفير MM6. بعد فك تشفير MM5 وبعد تحديد ملف تعريف ISAKMP وحلقة المفاتيح المقترنة، يقوم المستجيب ل ISAKMP بإجراء التحقق إذا تم تحديد نفس حلقة المفاتيح؛ وإذا لم يتم تحديد نفس حلقة المفاتيح، يتم إسقاط الاتصال.

لذلك، بالنسبة لمجيب ISAKMP، يجب عليك إستخدام حلقة مفاتيح واحدة ذات إدخالات متعددة كلما أمكن.

R1 كبادئ IKE (صحيح)

يوضح هذا السيناريو ما يحدث عندما يكون R1 هو بادئ IKE:

1. أستخدم عمليات تصحيح الأخطاء هذه لكل من R1 و R2:

   ```
   R1# debug crypto isakmp
   R1# debug crypto ipsec
   R1# debug crypto isakmp aaa
   ```
2. يقوم R1 بتهيئة النفق، ويرسل الحزمة MM1 مع اقتراحات النهج، ويتلقى MM2 في الاستجابة. ويتم بعد ذلك إعداد 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
```

من البداية، يعرف R1 أنه يجب إستخدام ملف تعريف ISAKMP2 الذي يتضمن ملف تعريف IPSec المستخدم ل VTI هذا.

لذلك، تم إختيار حلقة المفاتيح الصحيحة (keyRing2). يتم إستخدام المفاتيح المشتركة من KeyRing2 كدالة تضمين لحسابات DH عند إعداد حزمة MM3.

3. عندما يستقبل R2 حزمة MM3 لكن، فإنه لا يزال يعرف أي ملف تعريف ISAKMP يجب إستخدامه، ولكنه يحتاج إلى مفتاح مشترك مسبق إلى إنشاء DH. ولهذا السبب يبحث R2 في جميع حلقات المفاتيح للعثور على المفاتيح المشتركة مسبقا لذلك النظير:

```
*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
```

تم العثور على المفاتيح ل 192.168.0.1 في حلقة المفاتيح المحددة الأولى (keyring1).

4. ثم يقوم R2 بتجهيز حزمة MM4 مع حسابات DH ومع مفاتيح "Cisco" من KeyRing1:

```
*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. عندما يستقبل R1 MM4، فإنه يقوم بتجهيز حزمة MM5 باستخدام IKEID مع تحديد المفتاح الصحيح مسبقا (من 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. يتم تلقي حزمة MM5، التي تحتوي على معرف iKEID الخاص ب 192.168.0.1، بواسطة R2. عند هذه النقطة، يعلم R2 ملف تعريف ISAKMP الذي يجب ربط حركة المرور (أمر عناوين **هوية المطابقة**):

```
*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. يجري R2 الآن التحقق إذا كان حلقة المفاتيح التي تم تحديدها بشكل أعمى لحزمة MM4 هي نفسها حلقة المفاتيح التي تم تكوينها لتوصيف ISAKMP الذي تم إختياره الآن. لأن keyRing1 هو أول واحد في التشكيل، فقد تم تحديده سابقا، ويتم تحديده الآن. تم التحقق من الصحة بنجاح، ويمكن إرسال حزمة MM6:

```
*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. يستقبل R1 MM6 والي يحتاج إلى إجراء تحقق من حلقة المفاتيح لأنه كان معروف من الحزمة الأولى؛ فالبادئ يعرف دائما أي ملف تعريف ISAKMP استخدامه أو أي حلقة مفاتيح مقترنة بملف التعريف هذا. تمت المصادقة بنجاح، وانتهت المرحلة 1 بشكل صحيح:

```
*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. تبدأ المرحلة 2 بشكل طبيعي ويتم إكمالها بنجاح.

يعمل هذا السيناريو بشكل صحيح فقط بسبب الترتيب الصحيح لحلقات المفاتيح المحددة في R2. يستخدم ملف التعريف الذي يجب إستخدامه لجلسة عمل الشبكة الخاصة الظاهرية (VPN) حلقة المفاتيح التي كانت الأولى في التكوين.

R2 كبادئ IKE (غير صحيح)

يوضح هذا السيناريو ما يحدث عندما يبدأ R2 النفق نفسه ويشرح سبب عدم إنشاء النفق. تمت إزالة بعض السجلات للتركيز على الفروق بين هذا المثال والمثال السابق:

1. يقوم R2 بتهيئة النفق:

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

2. بما أن R2 هو البادئ، فإن توصيف ISAKMP وحلقة المفاتيح معروفان. يتم إستدعاء المفاتيح المشترك مسبقا من حلقة المفاتيح 1 لحسابات DH ويتم إرساله في MM3. يتلقى R2 MM2 ويقوم بتحضير MM3 استنادا إلى هذه المفاتيح:

```
*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. يتلقى R1 MM3 من R2. في هذه المرحلة، ال يعرف R1 أي ملف تعريف ISAKMP سيتم إستخدامه. وبالتالي، يستخدم R1 إستخدامه، لذلك ال يعرف أي حلقة مفاتيح سيتم إستخدامها. يستخدم R1 هذه المفاتيح المشتركة لأول حلقة مفاتيح من التكوين العام، وهو keyRing1. يستخدم R1 المفاتيح المشتركة مسبقا لحسابات DH ويرسل 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. يستقبل R2 MM4 من R1، ويستخدم المفاتيح المشتركة مسبقا من KeyRing1 لحساب DH، وقيمة MM5 و 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. يتلقى R1 MM5 من R1. نأن ارظن .IKEID يساوي 192.168.0، تم تحديد ملف التعريف2. قبل، في KeyRing2. تحديد KeyRing2 في ملف التعريف 2 لذلك تم تكوين KeyRing2 في MM4، قام R1 بتحديد حلقة المفاتيح الأولى التي تم تكوينها، والتي لحساب DH في 1. على الرغم من أن كلمات المرور هي نفسها تمامًا، يفشل كانت حلقة المفاتيح التحقق من صحة لوحة المفاتيح لأن هذه كانت لوحة مفاتيح مختلفة:

```
*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
```

تصحيح الأخطاء لمفاتيح مشترك مسبق مختلف

أستخدمت السيناريوهات السابقة المفاتيح نفسه ("Cisco"). وبالتالي، حتى عند إستخدام MM5 بشكل صحيح وإسقاطها الاقحة حلقة المفاتيح غير الصحيحة، يمكن فك تشفير حزمة حلقة المفاتيح بسبب فشل التحقق من صحة.

في السيناريوهات التي يتم فيها إستخدام مفاتيح مختلفة، الا يمكن فك تشفير MM5، وتظهر رسالة الخطأ هذه:

```
*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
```

معايير تحديد حلقة المفاتيح

هذا ملخص لمعايير تحديد لوحة المفاتيح. راجع الأقسام التالية للحصول على تفاصيل إضافية.

	بادئ	المستجيب
حلقات مفاتيح متعددة بعناوين IP مختلفة	تم التكوين. إذا لم يتم تكوين الأكثر تحديدا من التكوين بشكل صريح	أكثر التطابق تحديدا
حلقات مفاتيح متعددة لها نفس عناوين IP	تم التكوين. إذا لم يتم تكوينها بشكل صريح **ويصبح التكوين غير متوقع وغير مدعوم. يجب ألا يقوم أحد بتكوين مفاتيحين لنفس عنوان IP.**	**لا يمكن التنبؤ بالتكوين و يتم دعمه. يجب ألا يقوم أحد بتكوين مفاتيحين لنفس ع IP.**

يوضح هذا القسم أيضا لماذا قد يؤدي وجود كل من حلقة المفاتيح الافتراضية (التكوين العام) وحلقات المفاتيح المحددة إلى حدوث مشاكل ويشرح سبب تجنب إستخدام بروتوكول IKEv2 مثل هذه المشاكل.

ترتيب تحديد حلقة المفاتيح على بادئ IKE

للتكوين مع VTI، يستخدم البادئ واجهة نفق معينة تشير إلى ملف تعريف IPSec معين. انظر ألن ملف تعريف IPSec يستخدم ملف تعريف IKE محدد مع حلقة مفاتيح معينة، فلا يوجد أي إرتباك بشأن أي حلقة مفاتيح تستخدم.

وتعمل خريطة التشفير، التي تشير أيضا إلى ملف تعريف IKE محدد بحلقة مفاتيح معينة، بنفس الطريقة.

ومع ذلك، لا يمكن دائما التحديد من التكوين أي حلقة مفاتيح سيتم إستخدامها. على سبيل المثال، يحدث ذلك عندما يتم تكوين أي ملف تعريف IKE - أي عدم تكوين ملف تعريف IKE لاستخدام ملف تعريف IPSec:

```
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
```

إذا حاول بادئ IKE هذا إرسال MM1، فإنه سيختار حلقة المفاتيح الأكثر تحديدا:

```
*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
```

بما أن البادئ الي يحتوي علي توصيفات IKE متكونة عند إستلام MM6، فلن يؤثر علي وضع السريع (QM) الناجح والتصديق بالتماثل وسيكتمل توصيف:

```
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
```

ترتيب تحديد حلقة المفاتيح علي المستجيب ل IKE - عناوين IP مختلفة

توجد المشكلة في تحديد لوحة المفاتيح علي المستجيب. عندما تستخدم حلقات المفاتيح عناوين IP مختلفة، يكون ترتيب التحديد بسيطا.

افترض أن مستجيب IKE لديه هذا التكوين:

```
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
```

عندما يستقبل هذا المستجيب الحزمة MM1 من بادئ IKE بعنوان 192.168.0.2، فإنه سيختار أفضل (أكثر تطابق تحديدا)، حتي عندما يكون الأمر في التكوين مختلفا.

معايير ترتيب التحديد هي:

1. يتم إعتبار المفاتيح التي تحتوي علي عنوان IP فقط.
2. يتم التحقق من التوجيه الظاهري وإعادة التوجيه (VRF) للحزمة الواردة (VRF [fVRF] للطرف الأمامي).
3. إن يكون الربط في التقصير VRF، المفاتح شامل فحصت أول. يتم تحديد المفاتح الأكثر دقة (طول قناع الشبكة).
4. إن ال وجود مفاتح في التقصير مفاتح، كل لوحة مفاتيح أن تلاءم هذه fVRF يكون ربطت.
5. تمت مطابقة المفاتح الأكثر دقة (أطول قناع شبكة). علي سبيل المثال، في ضل /32 علي /24.

يؤدي التصحيح التحديد:

```
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
```

ترتيب تحديد حلقة المفاتيح على المستجيب ل IKE - نفس عناوين IP

عندما تستخدم حلقات المفاتيح نفس عناوين IP، تحدث مشاكل. افترض أن مستجيب IKE لديه هذا التكوين:

```
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
```

يتعذر التنبؤ بهذا التكوين وهو غير مدعوم. يجب ألا يقوم أحد المطلعين بتكوين مفاتيحين لنفس عنوان IP وأن تحدث المشكلة الموصوفة في [R2 كبادئ IKE (غير صحيح)](#).

التكوين العام KeyRing

تنتمي مفاتيح ISAKMP المعرفة في التكوين العام إلى حلقة المفاتيح الافتراضية:

```
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
```

على الرغم من أن مفتاح ISAKMP هو الأخير في التكوين، إلا أنه تتم معالجته كأول مفتاح على المستجيب ل IKE:

```
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
```

وبالتالي، فإن إستخدام كل من التكوين العالمي والمفاتيح المحددة ينطوي على مخاطر كبيرة وقد يؤدي إلى المشاكل.

حلقة المفاتيح على IKEv2 - لا تحدث مشكلة

على الرغم من أن بروتوكول IKEv2 يستخدم مفاهيم مماثلة ل IKEv1، إلا أن تحديد حلقة المفاتيح لا يسبب مشاكل مماثلة.

في الحالات البسيطة، يتم تبادل أربع حزم فقط. يتم إرسال IKEID الذي يحدد ملف تعريف IKEv2 الذي يجب تحديده على المستجيب بواسطة البادئ في الحزمة الثالثة. الحزمة الثالثة مشفرة بالفعل.

يمكن الاختلاف الأكبر في البروتوكولين في أن IKEv2 يستخدم نتيجة DH فقط لحساب مفتاح. لم يعد المفتاح المشترك مسبقا ضروريا لحساب المفاتيح المستخدم للتشفير/فك التشفير.

يذكر IKEv2 RFC (5996، القسم 2. 14):

يتم حساب المفاتيح المشتركة كما يلي. يتم حساب كمية تسمى SKEYSEED من القيود Diffie-Hellman المشترك والسر IKE_SA_INIT الذي تم إنشاؤه أثناء تبادل أثناء تبادل المتبادلة.

في نفس القسم، يلاحظ RFC أيضا:

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

يتم إرسال جميع المعلومات الضرورية في الحزم الأولى والثانية، ولا حاجة لاستخدام مفتاح مشترك مسبقا عند حساب SKEYSEED.

قارن ذلك مع IKE RFC (2409، القسم 3.2)، الذي ينص على:

SKEYID هي سلسلة مشتقة من مواد سرية معروفة فقط للمشغلين النشطين في Exchange.

وهذه "المادة السرية التي لا يعرفها إلا اللاعبون الفاعلون" هي المفتاح المشترك مسبقا. في القسم 5، يلاحظ RFC أيضا:

للمفاتيح المشتركة مسبقا: SKEYID = prf(**مفتاح مشترك مسبقا**، NI_b | NR_b)

وهذا يفسر لماذا يتسبب تصميم IKEv1 للمفاتيح المشتركة مسبقا في حدوث العديد من المشاكل. لا توجد هذه المشاكل في IKEv1 عند إستخدام الشهادات للمصادقة.

معايير تحديد ملف تعريف IKE

هذا ملخص لمعايير تحديد ملف تعريف IKE. راجع الأقسام التالية للحصول على تفاصيل إضافية.

	باديء	**المستجيب**
تحديد ملف التعريف	يجب تكوينها (تم تعيينها في ملف تعريف IPSec أو في خريطة التشفير). في حالة عدم التكوين، تتطابق أولا من التكوين. يجب أن يتطابق النظير البعيد مع ملف تعريف ISAKMP محدد واحد فقط، إذا كانت هوية النظير مطابقة في ملف تعريف ISAKMP، يكون التكوين غير صالح.	أول تطابق من التكوين. يجب أن يتطابق النظير البعيد مع ملف تعريف ISAKMP محدد واحد فقط، إذا كانت هوية النظير مطابقة في ملف تعريف ISAKMP، يكون التكوين غير صالح.

يصف هذا القسم أيضا الأخطاء النموذجية التي تحدث عند تحديد توصيف غير صحيح.

أمر تحديد ملف تعريف IKE على باديء IKE

تشير واجهة VTI عادة إلى ملف تعريف IPSec معين بملف تعريف IKE معين. يعرف الموجه بعد ذلك أي ملف تعريف IKE سيتم إستخدامه.

وبالمثل، تشير خريطة التشفير إلى ملف تعريف IKE معين، ويعرف الموجه أي ملف تعريف يجب إستخدامه بسبب التكوين.

ومع ذلك، قد يكون هناك سيناريوهات يكون فيها ملف التعريف غير محدد وحيث لا يمكن تحديد ملف التعريف مباشرة من التكوين الذي يجب إستخدامه، في هذا المثال، لا يتم

تحديد ملف تعريف IKE في ملف تعريف IPSec:

```
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
```

عندما يحاول هذا النظير إرسال حزمة MM1 إلى 192.168.0.2، يتم تحديد ملف التعريف الأكثر تحديدا:

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

أمر تحديد ملف تعريف IKE على المستجيب ل IKE

ترتيب تحديد ملف التعريف على مستجيب IKE مماثل لترتيب تحديد حلقة المفاتيح، حيث تكون الأولوية للأكثر تحديدا.

افترض هذا التكوين:

```
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
```

عند تلقي اتصال من 192.168.0.1، سيتم تحديد ملف التعريف2.

ترتيب ملفات التعريف التي تم تكوينها غير مهم. يعرض الأمر **show running-config** كل ملف تعريف جديد تم تكوينه في نهاية القائمة.

في بعض الأحيان قد يكون لدى المستجيب وصيفان من نوع IKE يستخدمان نفس حلقة المفاتيح. في حالة تحديد وصيف غير صحيح على المستجيب ولكن حلقة المفاتيح المحددة صحيحة تنتهي المصادقة بشكل صحيح:

```
*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
```

يستقبل المستجيب اقتراح QM ويقبله ويحاول إنشاء فهارس معلمات أمان IPSec (SPIs). في هذا المثال، تمت إزالة بعض تصحيح الأخطاء للوضوح:

```
*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
```

عند هذه النقطة، يفشل المستجيب ويفيد بأن ملف تعريف ISAKMP الصحيح لم يتطابق:

```
 (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
```

بسبب تحديد ملف تعريف IKE غير الصحيح، يتم إرجاع الخطأ 32، ويرسل المستجيب الرسالة PROPOSAL_NOT_CHOSEN.

ملخص

بالنسبة ل IKEv1، يتم إستخدام مفتاح مشترك مسبقا مع نتائج DH لحساب المفتاح المستخدم للتشفير الذي يبدأ من MM5. بعد أن يستلم MM3، لا يتمكن مستقبل ISAKMP بعد من تحديد ملف تعريف ISAKMP (وحلقة المفاتيح المرتبطة) التي يجب إستخدامها لأن IKEID يتم إرساله في MM5 و MM6.

والنتيجة هي أن مستجيب ISAKMP يحاول البحث من خلال جميع حلقات المفاتيح المحددة بشكل عام للعثور على المفتاح لنظير معين. لعناوين IP مختلفة، يتم تحديد أفضل حلقة مفاتيح (الأكثر تحديدا) مطابقة؛ ل نفس عنوان IP، يتم إستخدام أول عملية توصيل مطابقة من التكوين. يتم إستخدام حلقة المفاتيح لحساب المفتاح المستخدم لفك تشفير MM5.

بعد أن يستلم MM5، يحدد بادئ ISAKMP ملف تعريف ISAKMP وحلقة المفاتيح المرتبطة. يقوم البادئ بالتدقيق إذا كان هذا هو نفس حلقة المفاتيح التي تم تحديدها لحساب MM4 DH، وإلا فسيفشل التوصيل.

يعد ترتيب حلقات المفاتيح التي تم تكوينها في التكوين العام أمرا بالغ الأهمية. وبالتالي، بالنسبة لمجيب ISAKMP، أستخدم حلقة مفاتيح واحدة ذات إدخالات متعددة كلما أمكن.

تنتمي المفاتيح المشتركة مسبقا والتي تم تعريفها في وضع التكوين العام إلى حلقة مفاتيح معرفة مسبقا تسمى الافتراضي. يتم تطبيق نفس القواعد بعد ذلك.

بالنسبة لتحديد ملف تعريف IKE الخاص بالمستجيب، تتم مطابقة ملف التعريف الأكثر تحديدا. بالنسبة للمبادئ، يتم إستخدام ملف التعريف من التكوين، أو، إذا تعذر تحديد ذلك، يتم إستخدام أفضل تطابق.

تحدث مشكلة مماثلة في السيناريوهات التي تستخدم شهادات مختلفة لتوصيفات ISAKMP مختلفة. قد تفشل المصادقة بسبب التحقق من صحة ملف تعريف 'ca trust-point' عند إختيار شهادة مختلفة. ستتم تغطية هذه المشكلة في مستند منفصل.

المشاكل الموضحة في هذه المقالة ليست مشكلات خاصة ب Cisco، ولكنها تتعلق بقيود تصميم بروتوكول IKEv1. لا يحتوي IKEv1 المستخدم مع الشهادات على هذه القيود، ولا يحتوي IKEv2 المستخدم لكل من المفاتيح والشهادات المشتركة مسبقا على هذه القيود.

معلومات ذات صلة

- إلى شهادة قسم تعيين ملف تعريف ISAKMP من دليل تكوين VPNs IPsec، Cisco IOS الإصدار 15M&T المفتاح الإنترنت لدليل
- ca trust-point قسم من الخلال واضح من cisco ios أمر مرجع: أمر a إلى c
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).