عمليات تبادل حزم IOS IKEv1 و IKEv2 لتوصيفات ذات شهادات متعددة

المحتويات

المقدمة

يصف هذا المستند عمليات تبادل حزم مفتاح الإنترنت الإصدار 1 (IKEv1) و Internet Key Exchange الإصدار 2 (IKEv2) عند إستخدام مصادقة الشهادة والمشاكل المحتملة التي قد تحدث.

فيما يلي قائمة بالموضوعات التي تم وصفها في هذا المستند:

- معايير تحديد الشهادة لمنشئ تبادل مفاتيح الإنترنت (IKE) والمستجيب ل IKE
- يتطابق توصيف IKE مع المعايير عند تطابق ملفات تخصيص IKE متعددة (لسيناريوهات التداخل وغير التداخل)
- الإعدادات والسلوك الافتراضيين عند عدم إستخدام نقاط ثقة تحت توصيفات IKE
- الاختلافات بين IKEv1 و IKEv2 فيما يتعلق بمعايير تحديد التوصيفات والشهادات

ملاحظة: للحصول على تفاصيل حول كيفية أستكشاف مشكلة معينة وإصلاحها، ارجع إلى القسم الصحيح. كما يتم توفير ملخص قصير في نهاية هذا المستند.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين Cisco من VPN IOS®
- بروتوكولات IKEv1 و IKEv2 (تبادل الحزم)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 15.3T من Cisco IOS.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تنشأ المشاكل الموصوفة في هذا المستند عند إستخدام نقاط ثقة متعددة وتوصيفات IKE متعددة.

تحتوي الأمثلة الأولية التي يتم إستخدامها في هذا المستند على نفق IKEv1 LAN-to-LAN مع نقطتي ثقة على كل موجه. في البداية، قد يبدو أن التكوين صحيح. ومع ذلك، يمكن بدء نفق VPN فقط من جانب واحد من الاتصال بسبب الطريقة التي يتم بها إستخدام أمر **ca trust-point** لسلوك ملف تعريف اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) ولطلب الشهادات المسجلة في المتجر المحلي.

يتم تكوين سلوك مختلف باستخدام أمر **ca trust-point** لملف تعريف ISAKMP عندما يكون الموجه هو بادئ ISAKMP. قد تحدث مشكلة لأن بادئ ISAKMP على دراية بملف تعريف ISAKMP من البداية، لذلك يمكن أن يؤثر أمر **ca trust-point** الذي تم تكوينه لملف التعريف على الحمولة لطلب الشهادة في حزمة الوضع الرئيسي 3 (MM3). ومع ذلك، عندما يكون الموجه هو مستجيب ISAKMP، فإنه يربط حركة المرور الواردة بملف تعريف ISAKMP معين بعد أن يستلم حزمة الوضع الرئيسي 5 (MM5)، والتي تتضمن معرف IKE الذي يكون ضروريا لإنشاء الربط. هذا هو السبب في أنه من غير الممكن تطبيق أي أمر **ca trust-point** لحزمة الوضع الرئيسي 4 (MM4) لأن ملف التخصيص لا يتم تحديده قبل MM5.

يتم شرح ترتيب حمولة طلب الشهادة في الطرازين MM3 و MM4 والتأثير على عملية التفاوض بالكامل في هذا المستند، بالإضافة إلى سبب أنها تسمح فقط بإنشاء الاتصال من جانب واحد من نفق VPN.

فيما يلي ملخص لسلوكيات البادئ والمستجيب لبروتوكول IKEv1:

	بادئ IKEv1	**مستجيب IKEv1**
إرسال طلب	يرسل طلبات محددة فقط لنقاط الثقة التي تم تكوينها ضمن ملف التعريف	إرسال طلبات لكافة نقاط الثقة المتوفرة
التحقق من صحة الطلب	التحقق من الصحة مقابل نقاط ثقة معينة تم	التحقق من الصحة

	تكوينها ضمن ملف التعريف	مقابل نقاط ثقة معينة تم تكوينها ضمن ملف التعريف

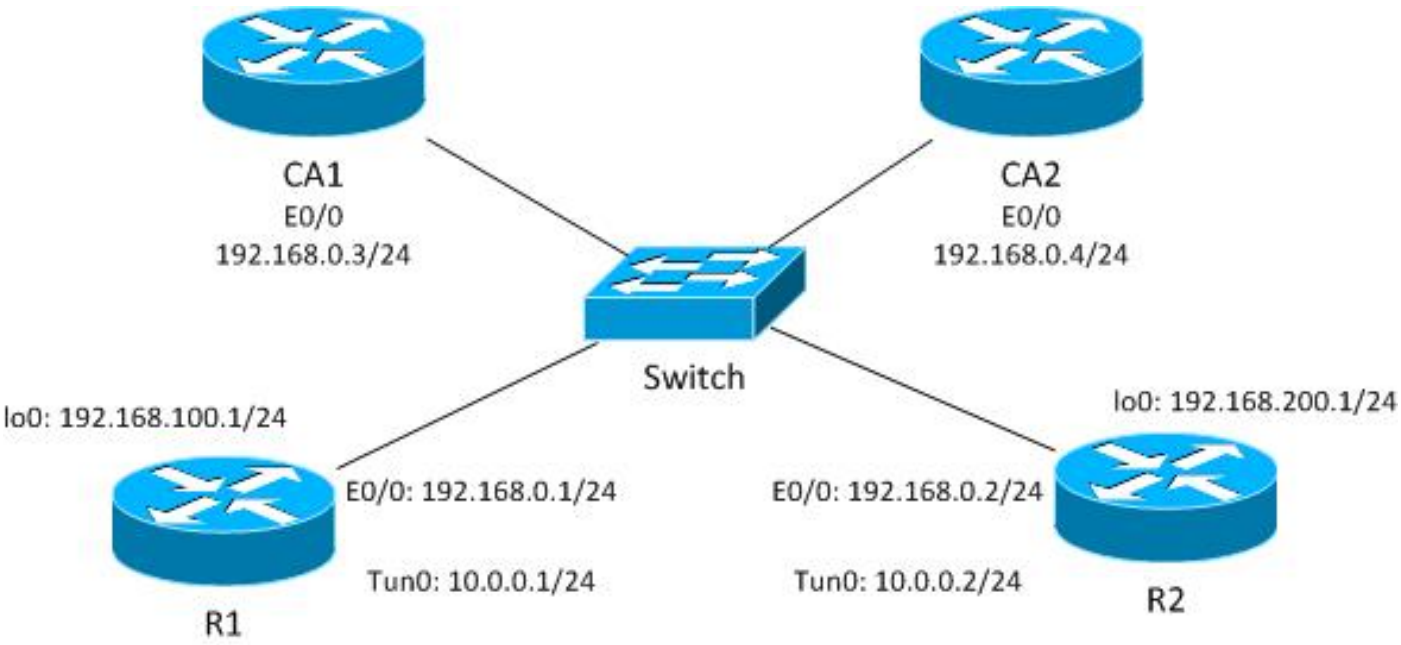
cisco يوصي أن لا يستعمل أنت ال **ca trust-point** أمر ل ISAKMP مستجيب أن يتلقى يتعدد ISAKMP توصيف ويستعمل يشكل شامل نقاط ثقة. بالنسبة لبادئات ISAKMP ذات ملفات تعريف ISAKMP المتعددة، توصي Cisco بتضييق عملية تحديد الشهادة باستخدام أمر **ca trust-point** في كل ملف تعريف.

بروتوكول IKEv2 به نفس مشاكل بروتوكول IKEv1، ولكن السلوك المختلف لأمر **pki trustPoint** يساعد على منع حدوث المشاكل. وذلك لأن الأمر **pki trustPoint** إلزامي لبادئ IKEv2، بينما يكون أمر **ca trust-point** إختياري لبادئ IKEv1. وفي ظل بعض الظروف (نقاط ثقة متعددة في إطار ملف واحد)، قد تحدث المشاكل التي سبق وصفها. ولهذا السبب، توصي Cisco باستخدام تكوينات نقطة ثقة متماثلة لكلا جانبي الاتصال (نفس نقاط الثقة التي تم تكوينها تحت كل من ملفات تعريف IKEv2).

طوبولوجيا

هذا مخطط عام يتم إستخدامه لجميع الأمثلة الواردة في هذا المستند.

ملاحظة: يستخدم الموجه 1 (R1) والموجه 2 (R2) واجهات الأنفاق الظاهرية (VTIs) للوصول إلى عمليات الاسترجاع. تتم حماية هذه الأجهزة الافتراضية الخاصة (VTIs) بواسطة IPSec.



بالنسبة لمثال IKEv1 هذا، يحتوي كل موجه على نقطتي ثقة لكل مرجع مصدق (CA)، ويتم تسجيل الشهادات لكل نقطة من نقاط الضمان.

عندما يكون R1 هو بادئ ISAKMP، يتفاوض النفق بشكل صحيح وتكون حركة المرور محمية. وهذا هو السلوك المتوقع. عندما يكون R2 هو بادئ ISAKMP، يفشل تفاوض المرحلة 1.

ملاحظة: بالنسبة لأمثلة IKEv2 في هذا المستند، تكون الطبولوجيا والعنونة هي نفسها الموجودة في مثال IKEv1.

عملية تبادل الحزم

يصف هذا القسم إختلافات تكوين IKEv1 و IKEv2 التي يتم إستخدامها لعملية تبادل الحزم، والمشاكل المحتملة التي قد تحدث.

IKEv1 مع شهادات متعددة

هنا تكوين شبكة R1 والشبكة الخاصة الظاهرية (VPN) ل IKEv1 بشهادات متعددة:

```
crypto isakmp policy 10
 encr 3des
 hash md5
 group 2

crypto isakmp profile prof1
   self-identity fqdn
   ca trust-point IOSCA1
   match identity host R2.cisco.com
   !
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
   mode tunnel
   !
crypto ipsec profile prof1
   set transform-set TS
   set isakmp-profile prof1
   !
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 prof1
 !
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0

ip route 192.168.200.0 255.255.255.0 10.0.0.2
```

هنا تكوين شبكة R2 والشبكة الخاصة الظاهرية (VPN) ل IKEv1 بشهادات متعددة:

```
crypto isakmp policy 10
 encr 3des
 hash md5
 group 2

crypto isakmp profile prof1
   self-identity fqdn
   match identity host R1.cisco.com
   !
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
   mode tunnel
   !
crypto ipsec profile prof1
   set transform-set TS
   set isakmp-profile prof1
   !
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 prof1
 !
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
```

في هذا المثال، يحتوي R1 على نقطتي ثقة: تستخدم إحداها IOSCA1 وتستخدم الثانية IOSCA2:

```
crypto pki trustpoint IOSCA1
 enrollment url http://192.168.0.3:80
   serial-number
   fqdn R1.cisco.com
   ip-address 192.168.0.1
 subject-name CN=R1,OU=IT,O=cisco,O=com
   revocation-check crl
   !
crypto pki trustpoint IOSCA2
 enrollment url http://192.168.0.4:80
   serial-number
   fqdn R1.cisco.com
   ip-address 192.168.0.1
 subject-name CN=R1,OU=IT,O=cisco,O=com
   revocation-check crl
```

في هذا المثال، يحتوي R2 أيضا على نقطتين: واحدة تستخدم IOSCA1 والثانية تستخدم IOSCA2:

```
crypto pki trustpoint IOSCA1
 enrollment url http://192.168.0.3:80
   serial-number
   fqdn R2.cisco.com
   ip-address 192.168.0.2
 subject-name CN=R2,OU=IT,O=cisco,O=com
   revocation-check crl
```

```
!
crypto pki trustpoint IOSCA2
 enrollment url http://192.168.0.4:80
                serial-number
             fqdn R2.cisco.com
          ip-address 192.168.0.2
 subject-name CN=R2,OU=IT,O=cisco,O=com
          revocation-check crl
```

من المهم ملاحظة أختلاف واحد في هذه التكوينات: يستخدم ملف تعريف ISAKMP R1 الأمر **ca trust-point** ل trust-point **IOSCA1**، والذي يشير إلى أن R1 يثق فقط بالشهادات التي تم التحقق منها من خلال نقطة الثقة المحددة هذه. في المقابل، يثق R2 في كل الشهادات التي تم التحقق من صحتها من قبل كل نقاط الثقة المحددة بشكل عام.

R1 كبادئ IKEv1

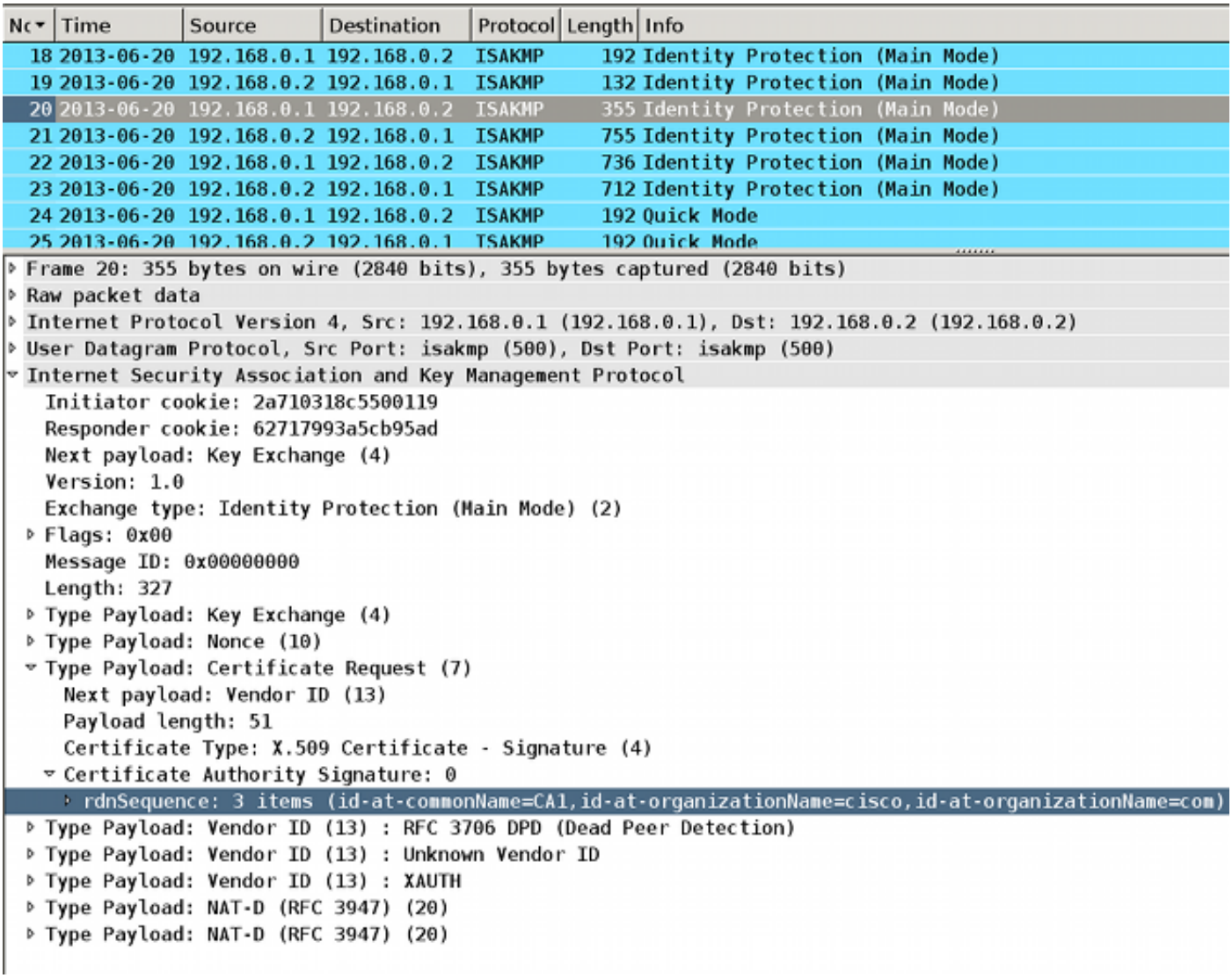
هنا ال debugs أمر ل على حد سواء R1 و R2:

- **R1# debug crypto isakmp**
- **R1# تصحيح أخطاء تشفير IPsec**
- **R1# debug crypto pki التحقق من صحة**

هنا، يبدأ R1 النفق ويرسل الشهادة طلب Mm3:

```
Jun 20 13:00:37.609: ISAKMP:(0): SA request profile is prof1*
Jun 20 13:00:37.610: ISAKMP (0): constructing CERT_REQ for issuer*
                                 cn=CA1,o=cisco,o=com
Jun 20 13:00:37.610: ISAKMP:(0): sending packet to 192.168.0.2*
                     my_port 500 peer_port 500 (I) MM_SA_SETUP
Jun 20 13:00:37.610: ISAKMP:(0):Old State = IKE_I_MM2  New State = IKE_I_MM3*
```

من المهم ملاحظة أن الحزمة تحتوي على طلب شهادة واحد فقط، وهو خاص فقط بنقطة **ثقة IOSCA1**. هذا سلوك متوقع مع التشكيل الحالي من ال isakmp مبرد (**cn=ca1، o=cisco، o=com**). لا يتم إرسال أي طلبات شهادات أخرى، والتي يمكنك التحقق منها باستخدام ميزة التقاط الحزمة المضمنة:



عندما يستقبل R2 الحزمة، فإنه يبدأ بمعالجة طلب الشهادة، مما يؤدي إلى إنشاء تطابق يحدد نقطة الضمان والشهادة المرتبطة التي يتم إستخدامها للمصادقة في MM5. ترتيب العملية هو نفسه كحمولة طلب الشهادة في حزمة ISAKMP. وهذا يعني أن أول تطابق استعملت. في هذا السيناريو، هناك تطابق واحد فقط حيث تم تكوين R1 بنقطة ثقة محددة وإرسال طلب شهادة واحد فقط مقترن بنقطة الثقة.

```
Jun 20 13:00:37.617: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.617: ISAKMP:(1010): peer wants cert issued*
                                    by cn=CA1,o=cisco,o=com
Jun 20 13:00:37.617:  Choosing trustpoint IOSCA1 as issuer*
```

وبعد ذلك، يقوم R2 بإعداد MM4. هذه هي الحزمة التي تحتوي على طلب الشهادة لجميع نقاط الثقة الموثوق بها. بما أن R2 هو المستجيب ISAKMP، فإن جميع نقاط الثقة المعرفة بشكل عام موثوق بها (لم يتم التحقق من تكوين **نقطة ثقة CA**). يتم تحديد نقطتين من نقاط الثقة يدويا (**IOSCA1** و**IOSCA2**)، ويتم تعريف باقي النقاط مسبقا.

```
Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
                                    for issuer cn=CA1,o=cisco,o=com
Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
                                    for issuer cn=CA2,o=cisco,o=com
Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
,for issuer ou=Class 3 Public Primary Certification Authority
```

```
                                                    o=VeriSign, Inc.,c=US
                                Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
                                                  for issuer cn=Cisco SSCA2,o=Cisco Systems
                                Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
                                   for issuer cn=Cisco Manufacturing CA,o=Cisco Systems
                                Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
                                        for issuer cn=Cisco Root CA 2048,o=Cisco Systems
                                Jun 20 13:00:37.617: ISAKMP (1010): constructing CERT_REQ*
                                                    for issuer cn=Cisco Root CA M1,o=Cisco
                                    Jun 20 13:00:37.617: ISAKMP:(1010): sending packet to*
                                    my_port 500 peer_port 500 (R) MM_KEY_EXCH 192.168.0.1
                            .Jun 20 13:00:37.617: ISAKMP:(1010):Sending an IKE IPv4 Packet*
                             ,Jun 20 13:00:37.617: ISAKMP:(1010):Input = IKE_MESG_INTERNAL*
                                                                  IKE_PROCESS_COMPLETE
                                 Jun 20 13:00:37.617: ISAKMP:(1010):Old State = IKE_R_MM3*
                                                                  New State = IKE_R_MM4
```

يمكنك التحقق من الحزمة باستخدام Wireshark. تحتوي حزمة MM4 من R2 على سبعة إدخالات لطلب الشهادة:

Nc	Time	Source	Destination	Protocol	Length	Info
18	2013-06-20	192.168.0.1	192.168.0.2	ISAKMP	192	Identity Protection (Main Mode)
19	2013-06-20	192.168.0.2	192.168.0.1	ISAKMP	132	Identity Protection (Main Mode)
20	2013-06-20	192.168.0.1	192.168.0.2	ISAKMP	355	Identity Protection (Main Mode)
21	2013-06-20	192.168.0.2	192.168.0.1	ISAKMP	755	Identity Protection (Main Mode)
22	2013-06-20	192.168.0.1	192.168.0.2	ISAKMP	736	Identity Protection (Main Mode)
23	2013-06-20	192.168.0.2	192.168.0.1	ISAKMP	712	Identity Protection (Main Mode)
24	2013-06-20	192.168.0.1	192.168.0.2	ISAKMP	192	Quick Mode
25	2013-06-20	192.168.0.2	192.168.0.1	ISAKMP	192	Quick Mode

```
▸ Frame 21: 755 bytes on wire (6040 bits), 755 bytes captured (6040 bits)
▸ Raw packet data
▸ Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
▸ User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
▾ Internet Security Association and Key Management Protocol
    Initiator cookie: 2a710318c5500119
    Responder cookie: 62717993a5cb95ad
    Next payload: Key Exchange (4)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ▸ Flags: 0x00
    Message ID: 0x00000000
    Length: 727
  ▸ Type Payload: Key Exchange (4)
  ▸ Type Payload: Nonce (10)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Certificate Request (7)
  ▸ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
  ▸ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  ▸ Type Payload: Vendor ID (13) : Unknown Vendor ID
  ▸ Type Payload: Vendor ID (13) : XAUTH
  ▸ Type Payload: NAT-D (RFC 3947) (20)
  ▸ Type Payload: NAT-D (RFC 3947) (20)
```

بعد ذلك، يتلقى R1 ال MM4 من R2 مع حقول طلب شهادات متعددة:

```
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by*
cn=CA1,o=cisco,o=com
Jun 20 13:00:37.623: ISAKMP: Examining profile list for trustpoint IOSCA1*
Jun 20 13:00:37.623: ISAKMP: Found matching profile for IOSCA1*
Jun 20 13:00:37.623: Choosing trustpoint IOSCA1 as issuer*
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by*
cn=CA2,o=cisco,o=com
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by ou=Class 3*
Public Primary Certification Authority,o=VeriSign, Inc.,c=US
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by*
cn=Cisco SSCA2,o=Cisco Systems
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by*
cn=Cisco Manufacturing CA,o=Cisco Systems
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by*
cn=Cisco Root CA 2048,o=Cisco Systems
Jun 20 13:00:37.623: ISAKMP:(1010): processing CERT_REQ payload. message ID = 0*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants a CT_X509_SIGNATURE cert*
Jun 20 13:00:37.623: ISAKMP:(1010): peer wants cert issued by*
cn=Cisco Root CA M1,o=Cisco
```

تطابق قاعدة المطابقة الأولى على R1 طلب الشهادة الأول مع نقطة **ثقة IOSCA1**. وهذا يحدد أن R1 يستخدم الشهادة المقترنة ب **IOSCA1** لنقطة الثقة للمصادقة في MM5. يتم إستخدام اسم المجال المؤهل بالكامل (FQDN) كمعرف IKE. وهذا يرجع إلى تكوين **FQDN للهوية الذاتية** في ملف تعريف ISAKMP:

```
=Jun 20 13:00:37.624: ISAKMP (1010): constructing CERT payload for serialNumber*
100+ipaddress=192.168.0.1+hostname=R1.cisco.com,cn=R1,ou=IT,o=cisco,o=com
Jun 20 13:00:37.624: ISAKMP:(1010): using the IOSCA1 trustpoint's*
keypair to sign
```

يتم تلقي MM5 ومعالجته بواسطة R2. يتطابق معرف IKE الذي تم تلقيه (**R1.cisco.com**) مع نسخة ملف تعريف **1** ISAKMP. يتم بعد ذلك التحقق من صحة الشهادة المستلمة ونجاح المصادقة:

```
Jun 20 13:00:37.625: ISAKMP:(1010): processing ID payload. message ID = 0*
Jun 20 13:00:37.625: ISAKMP (1010): ID payload*
next-payload : 6
type : 2
FQDN name : R1.cisco.com
protocol : 17
port : 500
```

```
                                                    length       : 20
                                  Jun 20 13:00:37.625: ISAKMP:(0):: peer matches prof1 profile*
                                                                  .........
                          Jun 20 13:00:37.626: CRYPTO_PKI: (A0013) Certificate validation succeeded*
                                                                  .........
                                  :Jun 20 13:00:37.626: ISAKMP:(1010):SA authentication status*
                                                                    authenticated
```

بعد ذلك، يقوم R2 بإعداد MM6 مع الشهادة المرتبطة ب **IOSCA1**:

```
=Jun 20 13:00:37.627: ISAKMP (1010): constructing CERT payload for serialNumber*
      101+ipaddress=192.168.0.2+hostname=R2.cisco.com,cn=R2,ou=IT,o=cisco,o=com
Jun 20 13:00:37.627: ISAKMP:(1010): using the IOSCA1 trustpoint's keypair to sign*
                Jun 20 13:00:37.632: ISAKMP:(1010): sending packet to 192.168.0.1*
                                      my_port 500 peer_port 500 (R) MM_KEY_EXCH
```

يتم تلقي الحزمة بواسطة R1، ويتحقق R1 من الشهادة والمصادقة:

```
                     Jun 20 13:00:37.632: ISAKMP (1010): received packet from 192.168.0.2*
                                          dport 500 sport 500 Global (I) MM_KEY_EXCH
                Jun 20 13:00:37.632: ISAKMP:(1010): processing ID payload. message ID = 0*
                                    Jun 20 13:00:37.632: ISAKMP (1010): ID payload*
                                                    next-payload : 6
                                                    type         : 2
                                               FQDN name    : R2.cisco.com
                                                         protocol     : 17
                                                        port         : 500
                                                         length       : 20
                                                                        ....
                   Jun 20 13:00:37.632: ISAKMP:(0): Creating CERT validation list: IOSCA1*
                                                                        ....
                Jun 20 13:00:37.633: CRYPTO_PKI: (80013) Certificate validation succeeded*
                                                                        ....
                                  :Jun 20 13:00:37.637: ISAKMP:(1010):SA authentication status*
                                                                    authenticated
                      Jun 20 13:00:37.637: ISAKMP:(1010):Old State = IKE_I_MM6*
                                                          New State = IKE_P1_COMPLETE
```

هذا يتم المرحلة 1. يتم التفاوض على المرحلة الثانية كالمعتاد. تم إنشاء النفق بنجاح وتمت حماية حركة المرور.

R2 كبادئ IKEv1

يوضح هذا المثال العملية التي يبدأ فيها R2 نفس نفق IKEv1 ويشرح سبب عدم إنشائه.

ملاحظة: تتم إزالة أجزاء من السجلات للتركيز فقط على الفروق المتعلقة بالمثال المعروض في القسم السابق.

يرسل R2 ال MM3 مع سبع حمولات طلب شهادة لأن R2 لا يحتوي على نقطة ثقة مرتبطة بملف تعريف ISAKMP

(جميع نقاط الثقة موثوق بها):

```
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                                        issuer cn=CA1,o=cisco,o=com
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                                        issuer cn=CA2,o=cisco,o=com
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                 ,issuer ou=Class 3 Public Primary Certification Authority
                                        o=VeriSign, Inc.,c=US
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                                  issuer cn=Cisco SSCA2,o=Cisco Systems
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                             issuer cn=Cisco Manufacturing CA,o=Cisco Systems
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                           issuer cn=Cisco Root CA 2048,o=Cisco Systems
Jun 17 18:08:44.321: ISAKMP (0): constructing CERT_REQ for*
                                     issuer cn=Cisco Root CA M1,o=Cisco
Jun 17 18:08:44.321: ISAKMP (0): sending packet to 192.168.0.1*
                                  my_port 500 peer_port 500 (I) MM_SA_SETUP
```

عندما يستقبل R1 الحزمة من R2، فإنه يعالج طلب الشهادة ويطابق نقطة ثقة **IOSCA1**، والتي تحدد الشهادة التي يتم إرسالها في MM6:

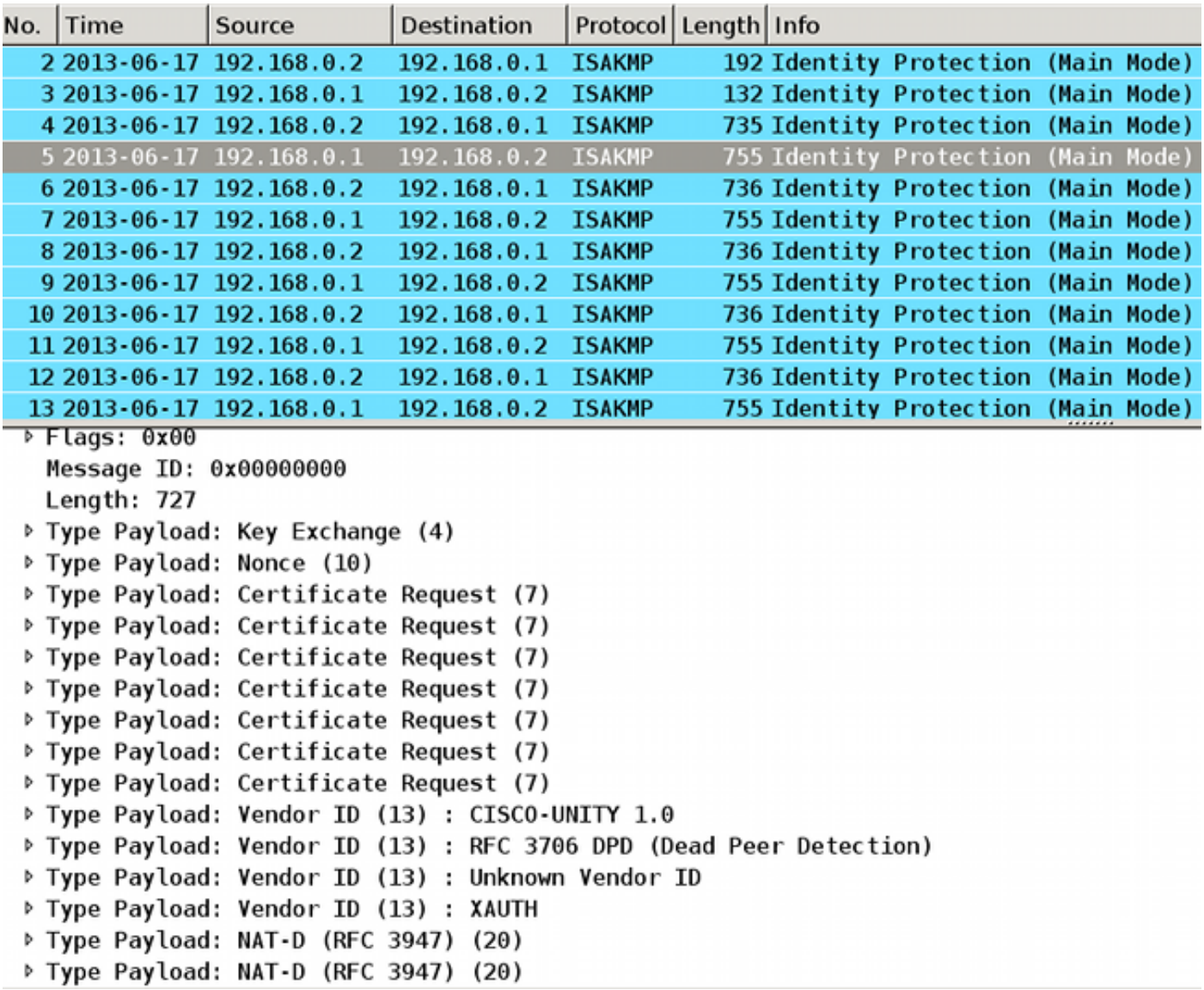
```
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
   Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
                                                cn=CA1,o=cisco,o=com
      Jun 17 18:08:14.321:  Choosing trustpoint IOSCA1 as issuer*
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
   Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
                                                cn=CA2,o=cisco,o=com
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
   Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
ou=Class 3 Public Primary Certification Authority,o=VeriSign, Inc.,c=US
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
   Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
                                          cn=Cisco SSCA2,o=Cisco Systems
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
   Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
                                     cn=Cisco Manufacturing CA,o=Cisco Systems
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
   Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
                                   cn=Cisco Root CA 2048,o=Cisco Systems
.Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload*
                                                        message ID = 0
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert*
```

```
Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by*
                                    cn=Cisco Root CA M1,o=Cisco
```

بعد ذلك، يقوم R1 بإعداد حزمة MM4 مع حمولة طلب الشهادة. توجد الآن عدة حمولة لطلب الشهادة:

```
Jun 17 18:08:14.321: ISAKMP (1099): constructing CERT_REQ for issuer*
                                                cn=CA2,o=cisco,o=com
Jun 17 18:08:14.321: ISAKMP (1099): constructing CERT_REQ for issuer*
                                                cn=CA1,o=cisco,o=com
Jun 17 18:08:14.322: ISAKMP (1099): constructing CERT_REQ for issuer*
                                ,ou=Class 3 Public Primary Certification Authority
                                                o=VeriSign, Inc.,c=US
Jun 17 18:08:14.322: ISAKMP (1099): constructing CERT_REQ for issuer*
                                              cn=Cisco SSCA2,o=Cisco Systems
Jun 17 18:08:14.322: ISAKMP (1099): constructing CERT_REQ for issuer*
                                    cn=Cisco Manufacturing CA,o=Cisco Systems
Jun 17 18:08:14.322: ISAKMP (1099): constructing CERT_REQ for issuer*
                                      cn=Cisco Root CA 2048,o=Cisco Systems
Jun 17 18:08:14.322: ISAKMP (1099): constructing CERT_REQ for issuer*
                                                cn=Cisco Root CA M1,o=Cisco
   Jun 17 18:08:14.322: ISAKMP:(1099): sending packet to 192.168.0.2*
                                my_port 500 peer_port 500 (R) MM_KEY_EXCH
```

تحقق من السجلات باستخدام التقاط الحزمة المضمنة (EPC) وشبكة Wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
2	2013-06-17	192.168.0.2	192.168.0.1	ISAKMP	192	Identity Protection (Main Mode)
3	2013-06-17	192.168.0.1	192.168.0.2	ISAKMP	132	Identity Protection (Main Mode)
4	2013-06-17	192.168.0.2	192.168.0.1	ISAKMP	735	Identity Protection (Main Mode)
5	2013-06-17	192.168.0.1	192.168.0.2	ISAKMP	755	Identity Protection (Main Mode)
6	2013-06-17	192.168.0.2	192.168.0.1	ISAKMP	736	Identity Protection (Main Mode)
7	2013-06-17	192.168.0.1	192.168.0.2	ISAKMP	755	Identity Protection (Main Mode)
8	2013-06-17	192.168.0.2	192.168.0.1	ISAKMP	736	Identity Protection (Main Mode)
9	2013-06-17	192.168.0.1	192.168.0.2	ISAKMP	755	Identity Protection (Main Mode)
10	2013-06-17	192.168.0.2	192.168.0.1	ISAKMP	736	Identity Protection (Main Mode)
11	2013-06-17	192.168.0.1	192.168.0.2	ISAKMP	755	Identity Protection (Main Mode)
12	2013-06-17	192.168.0.2	192.168.0.1	ISAKMP	736	Identity Protection (Main Mode)
13	2013-06-17	192.168.0.1	192.168.0.2	ISAKMP	755	Identity Protection (Main Mode)

```
▸ Flags: 0x00
  Message ID: 0x00000000
  Length: 727
▸ Type Payload: Key Exchange (4)
▸ Type Payload: Nonce (10)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Certificate Request (7)
▸ Type Payload: Vendor ID (13) : CISCO-UNITY 1.0
▸ Type Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
▸ Type Payload: Vendor ID (13) : Unknown Vendor ID
▸ Type Payload: Vendor ID (13) : XAUTH
▸ Type Payload: NAT-D (RFC 3947) (20)
▸ Type Payload: NAT-D (RFC 3947) (20)
```

على الرغم من تكوين R1 لنقطة ثقة واحدة (**IOSCA1**) في ملف تعريف ISAKMP، إلا أن هناك طلبات شهادات متعددة مرسلة. يحدث هذا لأن أمر **ca trust-point** في ملف تعريف ISAKMP يحدد حمولة طلب الشهادة، ولكن فقط عندما يكون الموجه هو بادئ جلسة ISAKMP. إذا كان الموجه هو المستجيب، فهناك العديد من حمولات طلبات الشهادات لجميع نقاط الثقة المحددة بشكل عام لأن R1 لا يعرف بعد ملف تعريف ISAKMP الذي يتم إستخدامه لجلسة عمل IKE.

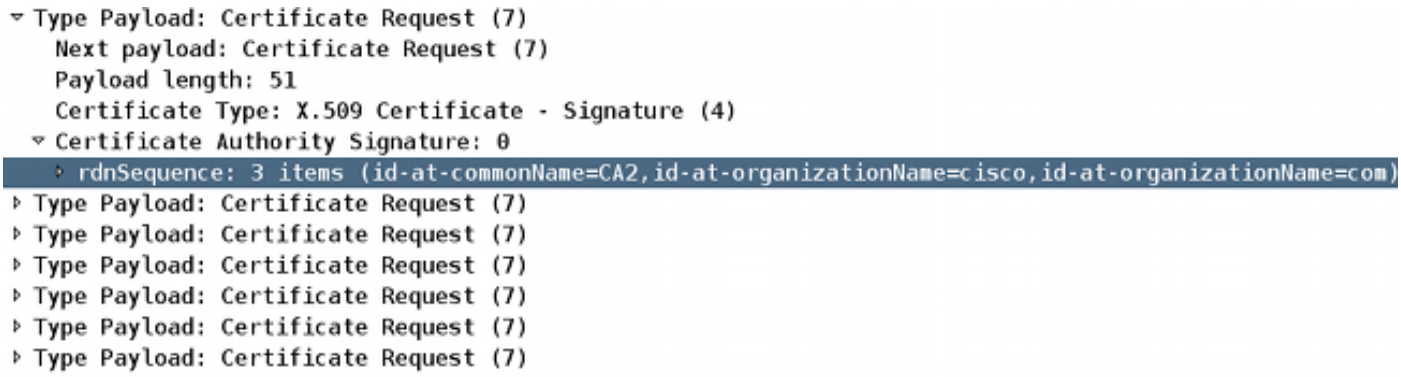
تلتزم جلسة عمل IKE الواردة بملف تعريف ISAKMP محدد بعد إستلام MM5، والذي يتضمن معرف IKE. بعد ذلك، يربط أمر **مطابقة الهوية** لملف التعريف المحدد جلسة IKE بملف التعريف. ومع ذلك، لا يمكن للموجه تحديد ذلك حتى الآن. قد يكون هناك العديد من توصيفات ISAKMP بأمر **نقطة** ثقة **CA** مختلفة تم تكوينها لكل توصيف.

ولهذا السبب، يجب أن يرسل R1 طلب الشهادة لجميع نقاط الثقة التي تم تكوينها بشكل عام.

أحلت [الأمر مرجع](#) ل **ca trust-point** أمر:

يجب أن يكون للموجه الذي يبدأ في IKE والموجه الذي يستجيب لطلب IKE تكوينات متناسقة لنقطة الثقة. على سبيل المثال، قد يستخدم الموجه المستجيب (في الوضع الرئيسي ل IKE) الذي يقوم بتشفير توقيع RSA والمصادقة نقاط الثقة التي تم تعريفها في التكوين العام عند إرسال حمولات CERT-REQ. ومع ذلك، قد يستخدم الموجه قائمة مقيدة من نقاط الاتصال التي تم تعريفها في ملف تعريف ISAKMP للتحقق من الشهادة. إذا تم تكوين النظير (بادئ IKE) لاستخدام شهادة توجد نقطة الثقة الخاصة بها في القائمة العامة للموجه المستجيب ولكن ليس في ملف تعريف ISAKMP للموجه المستجيب، يتم رفض الشهادة. (ومع ذلك، إذا لم يكن الموجه الذي بدأ التشغيل يعرف نقاط الثقة في التكوين العام للموجه المستجيب، فيمكن مصادقة الشهادة بعد.)

تحقق الآن من تفاصيل حزمة MM4 لاكتشاف حمولة طلب الشهادة الأولى:



تتضمن حزمة MM4 التي يتم إرسالها من R1 نقطة **الثقة IOSCA2** في حمولة طلب الشهادة الأولى بسبب ترتيب تثبيت الشهادات، حيث يتم توقيع الأولى من خلال نقطة الثقة **IOSCA2**:

```
R1#sh crypto pki certificates
                                                Certificate
                                          Status: Available
                                Certificate Serial Number (hex): 03
                                 Certificate Usage: General Purpose
                                                    :Issuer
                                                  cn=CA2
                                                  o=cisco
                                                    o=com
                                                   :Subject
                                              Name: R1.cisco.com
                                           IP Address: 192.168.0.1
                                              Serial Number: 100
          serialNumber=100+ipaddress=192.168.0.1+hostname=R1.cisco.com
                                                    cn=R1
                                                    ou=IT
                                                  o=cisco
                                                    o=com
                                                :Validity Date
                                start date: 13:25:01 CET Jun 17 2013
                                end   date: 13:25:01 CET Jun 17 2014
                                  Associated Trustpoints: IOSCA2
                                                                ...
<output omitted, 1 more R1 cert signed by CA1, 2 more CA certs>
```

عقد مقارنة مع حزمة MM3 التي يتم إرسالها من R2 عند تضمين نقطة **ثقة IOSCA1** في حمولة طلب الشهادة الأولى:

```
R2#sh crypto pki certificates
                                                Certificate
                                          Status: Available
                                Certificate Serial Number (hex): 02
                                 Certificate Usage: General Purpose
                                                    :Issuer
                                                  cn=CA1
                                                  o=cisco
```

```
                                                                o=com
                                                               :Subject
                                                     Name: R2.cisco.com
                                                  IP Address: 192.168.0.2
                                                      Serial Number: 101
                  serialNumber=101+ipaddress=192.168.0.2+hostname=R2.cisco.com
                                                                cn=R2
                                                                ou=IT
                                                              o=cisco
                                                                o=com
                                                            :Validity Date
                                          start date: 13:23:49 CET Jun 17 2013
                                          end   date: 13:23:49 CET Jun 17 2014
                                                 Associated Trustpoints: IOSCA1
                                                       Storage: nvram:CA1#2.cer
                                                                           ...
                  <output omitted, 1 more R2 cert signed by CA2, 2 more CA certs>
```

يتلقى R2 الآن الحزمة MM4 من R1 ويبدأ بمعالجة طلب الشهادة. تتطابق حمولة طلب الشهادة الأول مع نقطة **ثقة** IOSCA2:

```
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
                                                      cn=CA2,o=cisco,o=com
                       Jun 17 18:08:44.335:  Choosing trustpoint IOSCA2 as issuer*
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
                                                      cn=CA1,o=cisco,o=com
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
ou=Class 3 Public Primary Certification Authority,o=VeriSign, Inc.,c=US
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
                                                  cn=Cisco SSCA2,o=Cisco Systems
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
                                              cn=Cisco Manufacturing CA,o=Cisco Systems
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
                                                 cn=Cisco Root CA 2048,o=Cisco Systems
                .Jun 17 18:08:44.335: ISAKMP:(1100): processing CERT_REQ payload*
                                                                message ID = 0
Jun 17 18:08:44.335: ISAKMP:(1100): peer wants a CT_X509_SIGNATURE cert*
                  Jun 17 18:08:44.335: ISAKMP:(1100): peer wants cert issued by*
                                                    cn=Cisco Root CA M1,o=Cisco
```

عندما يقوم R2 بتجهيز حزمة MM5، فإنه يستخدم الشهادة المرتبطة بنقطة **ثقة** IOSCA2:

```
Jun 17 18:08:44.335: ISAKMP:(1100):SA is doing RSA signature authentication*
                                                using id type ID_FQDN
                                    Jun 17 18:08:44.335: ISAKMP (1100): ID payload*
                                                    next-payload : 6
                                                    type         : 2
                                            FQDN name    : R2.cisco.com
                                                    protocol     : 17
                                                    port         : 500
                                                    length       : 20
                        Jun 17 18:08:44.335: ISAKMP:(1100):Total payload length: 20*
    Jun 17 18:08:44.335: ISAKMP:(1100): IKE->PKI Get CertificateChain to be sent*
                                    (to peer state (I) MM_KEY_EXCH (peer 192.168.0.1
    Jun 17 18:08:44.335: ISAKMP:(1100): PKI->IKE Got CertificateChain to be sent*
                                    (to peer state (I) MM_KEY_EXCH (peer 192.168.0.1
                Jun 17 18:08:44.336: ISAKMP (1100): constructing CERT payload for*
              ,serialNumber=101+ipaddress=192.168.0.2+hostname=R2.cisco.com,cn=R2
                                                        ou=IT,o=cisco,o=com
                                                                    R2#
                Jun 17 18:08:44.336: ISAKMP:(1100): using the IOSCA2 trustpoint's*
                                                        keypair to sign
                Jun 17 18:08:44.336: ISAKMP:(1100): sending packet to 192.168.0.1*
                                        my_port 500 peer_port 500 (I) MM_KEY_EXCH
                    .Jun 17 18:08:44.336: ISAKMP:(1100):Sending an IKE IPv4 Packet*
```

يتم تلقي حزمة MM5 بواسطة R1. لأن R1 يثق فقط في نقطة ثقة **IOSCA1** (لملف تعريف ISAKMP **prof1**)، يفشل التحقق من الشهادة:

```
                Jun 17 18:08:44.337: ISAKMP (1100): received packet from 192.168.0.2*
                                        dport 500 sport 500 Global (R) MM_KEY_EXCH
        Jun 17 18:08:44.337: ISAKMP:(1100):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH*
    Jun 17 18:08:44.337: ISAKMP:(1100):Old State =IKE_R_MM4  New State = IKE_R_MM5*

         Jun 17 18:08:44.337: ISAKMP:(1100): processing ID payload. message ID = 0*
                                    Jun 17 18:08:44.337: ISAKMP (1100): ID payload*
                                                    next-payload : 6
                                                    type         : 2
                                            FQDN name    : R2.cisco.com
                                                    protocol     : 17
                                                    port         : 500
                                                    length       : 20
                        Jun 17 18:08:44.337: ISAKMP:(0):: peer matches prof1 profile*
       Jun 17 18:08:44.337: ISAKMP:(1100): processing CERT payload. message ID = 0*
           Jun 17 18:08:44.337: ISAKMP:(1100): processing a CT_X509_SIGNATURE cert*
         Jun 17 18:08:44.337: ISAKMP:(1100): IKE->PKI Add peer's certificate state*
                                        (R) MM_KEY_EXCH (peer 192.168.0.2)
                  Jun 17 18:08:44.337: CRYPTO_PKI: (900C5) Adding peer certificate*
       Jun 17 18:08:44.337: ISAKMP:(1100): PKI->IKE Added peer's certificate state*
                                        (R) MM_KEY_EXCH (peer 192.168.0.2)
       Jun 17 18:08:44.337: ISAKMP:(1100): IKE->PKI Get PeerCertificateChain state*
                                        (R) MM_KEY_EXCH (peer 192.168.0.2)
       Jun 17 18:08:44.337: ISAKMP:(1100): PKI->IKE Got PeerCertificateChain state*
                                        (R) MM_KEY_EXCH (peer 192.168.0.2)
                    Jun 17 18:08:44.337: ISAKMP:(1100): peer's pubkey isn't cached*
    Jun 17 18:08:44.337: ISAKMP:(1100):Profile has no keyring, aborting key search*
           ,Jun 17 18:08:44.337: ISAKMP:(0): Creating CERT validation list: IOSCA1*
     Jun 17 18:08:44.337: ISAKMP:(1100): IKE->PKI Validate certificate chain state*
                                        (R) MM_KEY_EXCH (peer 192.168.0.2)
    Jun 17 18:08:44.337: CRYPTO_PKI:ip-ext-val:IP extension validation not required*
```

```
Jun 17 18:08:44.341: CRYPTO_PKI: (900C5) Check for identical certs*
Jun 17 18:08:44.341: CRYPTO_PKI: (900C5) Create a list of suitable trustpoints*
Jun 17 18:08:44.341: CRYPTO_PKI: (900C5) No suitable trustpoints found*
Jun 17 18:08:44.341: ISAKMP:(1100): PKI->IKE Validate certificate chain state*
                                        (R) MM_KEY_EXCH (peer 192.168.0.2)
Jun 17 18:08:44.341: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from*
     is bad: unknown error returned in certificate validation 192.168.0.2
                                                                      R1#
Jun 17 18:08:44.341: ISAKMP:(1100): Unknown error in cert validation, -1*
```

يعمل هذا التكوين إذا كان ترتيب تسجيل الشهادة في R1 مختلفا لأن أول شهادة معروضة موقعة بواسطة نقطة **الثقة IOSCA1**. كما أن حمولة طلب الشهادة الأولي في MM4 هي نقطة الثقة **IOSCA1**، والتي يتم إختيارها بعد ذلك من قبل R2 والتحقق من صحتها بنجاح على R1 في MM6.

IKEv1 بدون أمر *ca trust-point* في ملف التعريف

بالنسبة للسيناريوهات التي تحتوي على ملفات تعريف ونقاط ثقة متعددة ولكن دون تكوين نقاط ثقة معينة في ملفات التعريف، لا توجد مشاكل لأنه لا يوجد التحقق من صحة نقاط ثقة محددة محددة محددة محددة بواسطة تكوين أمر **نقطة ثقة** من **النوع CA**. ومع ذلك، قد لا تكون عملية التحديد واضحة. بناء على الموجه الذي هو البادئ، يتم تحديد الشهادات المختلفة لعملية المصادقة بالنسبة لترتيب تسجيل الشهادة.

في بعض الأحيان، يمكن دعم الشهادة من قبل جانب واحد فقط من الاتصال، مثل X509 Version 1، والذي لا يعد وظيفة تجزئة نموذجية يتم إستخدامها للتوقيع. قد يتم إنشاء نفق VPN من جانب واحد فقط من الاتصال.

مرجع RFC ل IKEv1

هنا snip من RFC4945:

3-2-7-1 تحديد سلطات التصديق

عند **طلب** تبادل مواد التعبئة داخل النطاق، يجب أن تقوم عمليات التنفيذ بإنشاء CERTREQs لكل مرساة ثقة نظير يعتبرها **السياسة المحلية** موثوق بها **بشكل صريح** أثناء عملية تبادل محددة.
ليس RFC واضحا. قد ترتبط **السياسة المحلية** بشكل صريح بأمر **ca trust-point** الذي تم تكوينه في ملف تعريف ISAKMP للتشفير. المشكلة هي أنه في مرحلتي MM3 و MM4 من العملية، لا يمكنك تحديد ملف تعريف ISAKMP إلا إذا كنت تستخدم عنوان IP للهوية ونقاط الثقة لأن المصادقة في مرحلتي MM5 و MM6 من العملية يجب أن تحدث أولا. ولهذا السبب، تتصل **السياسة المحلية بشكل صريح** بجميع نقاط الثقة التي تم تكوينها على الجهاز.

ملاحظة: هذه المعلومات ليست خاصة ب Cisco، ولكنها خاصة ب IKEv1.

تحديد ملف تخصيص IKEv2 مع الهويات التي تتداخل

قبل وصف شهادات متعددة ل IKEv2، من المهم معرفة الطريقة التي يتم بها تحديد التوصيفات عند إستخدام هوية المطابقة، والتي تكون مرضية لجميع التوصيفات. وهذا ليس السيناريو الموصى به لأن نتائج مفاوضات IKEv2 تعتمد على عوامل متعددة. توجد نفس المشاكل ل IKEv1 عند إستخدام ملفات التخصيص التي تتداخل.

فيما يلي مثال لتكوين بادئ IKEv2:

```
crypto ikev2 proposal prop-1
 encryption 3des
 integrity md5
 group 2
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 profile profile1
 match identity remote address 192.168.0.2 255.255.255.255
 identity local address 192.168.0.1
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP1

crypto ipsec transform-set trans esp-3des esp-sha-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set trans
 set ikev2-profile profile1
!
interface Loopback0
 ip address 192.168.100.1 255.255.255.255
!
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 192.168.0.1 255.255.255.0

ip route 192.168.200.1 255.255.255.255 10.0.0.2
```

يتم إستخدام عنوان نوع الهوية لكلا جانبي الاتصال. المصادقة عبر الشهادات (يمكن أيضا أن تكون مفاتيح مشتركة مسبقا) ليست مهمة لهذا المثال. يحتوي المستجيب على توصيفات متعددة تتطابق جميعها مع حركة مرور IKEv2 الواردة:

```
crypto ikev2 proposal prop-1
 encryption 3des
 integrity md5
 group 2
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 profile profile1
 match identity remote address 192.168.0.1 255.255.255.255
 identity local address 192.168.0.2
 authentication remote rsa-sig
 authentication local rsa-sig
```

```
 pki trustpoint TP1
 !
crypto ikev2 profile profile2
 match identity remote address 192.168.0.1 255.255.255.255
 identity local address 192.168.0.2
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP1
 !
crypto ikev2 profile profile3
 match identity remote address 192.168.0.1 255.255.255.255
 identity local address 192.168.0.2
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP1

crypto ipsec transform-set trans esp-3des esp-sha-hmac
 mode tunnel
 !
crypto ipsec profile profile1
 set transform-set trans
 set ikev2-profile profile1
 !
interface Loopback0
 ip address 192.168.200.1 255.255.255.255
 !
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 192.168.100.1 255.255.255.255 10.0.0.1
```

يرسل البادئ الحزمة IKEv2 الثالثة، ويجب على المستجيب إختيار ملف التعريف بناء على الهوية التي يتم استقبالها. الهوية هي عنوان **192.168.0.1** (IPv4):

```
IKEv2:(SA ID = 1):Searching policy based on peer's identity '192.168.0.1' of
 'type 'IPv4 address
```

تحقق جميع التوصيفات هذه الهوية بسبب أمر **مطابقة الهوية** الذي تم تكوينه. يختار IOS الأخير في التكوين، وهو **profile3** في هذا المثال:

```
'IKEv2:found matching IKEv2 profile 'profile3
```

دخلت to order in دققت الأمر، **العرض crypto ikev2 profile** أمر.

ملاحظة: حتى في حالة وجود عنوان عام (0.0.0.0) في ملف التعريف، فإنه يظل محددا. لا يحاول IOS العثور على أفضل تطابق، بل يحاول العثور على أول تطابق. ومع ذلك، يحدث هذا فقط لأن كافة التوصيفات بها نفس الأمر **تطابق هوية** عن **بعد** الذي تم تكوينه. بالنسبة لتوصيفات IKEv1 و IKEv2 التي تحتوي على قواعد هوية

مطابقة مختلفة، يتم إستخدام أكثر هذه القواعد تحديدا دائما. توصيك Cisco بعدم وجود ملفات التعريف التي تم تكوينها باستخدام أمر **تطابق الهوية المتداخل** لأنه من الصعب توقع ملف التعريف الذي تم تحديده.

في هذا السيناريو، يتم تحديد **profile3** بواسطة المستجيب، ولكن **profile1** يتم إستخدامه لواجهة النفق. وهذا يتسبب في ظهور خطأ عند التفاوض حول معرف الوكيل:

```
Jul 17 09:23:48.187: map_db_check_isakmp_profile profile did not match*
       Jul 17 09:23:48.187: map_db_find_best did not find matching map*
                    :(Jul 17 09:23:48.187: IPSEC(ipsec_process_proposal*
                                        proxy identities not supported
                   Jul 17 09:23:48.187: IKEv2:(SA ID = 1):There was no*
                                    IPSEC policy found for received TS
                                 :(Jul 17 09:23:48.187: IKEv2:(SA ID = 1*
 Jul 17 09:23:48.187: IKEv2:(SA ID = 1):Sending TS unacceptable notify*
```

تدفق IKEv2 عند إستخدام الشهادات

عند إستخدام الشهادات ل IKEv2 للمصادقة، لا يرسل البادئ حمولة طلب الشهادة في الحزمة الأولى:

```
                                        IKEv2 IKE_SA_INIT Exchange REQUEST
                                                    :Payload contents
                        (SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP
                                (NOTIFY(NAT_DETECTION_DESTINATION_IP
```

يرد المستجيب بحمولة طلب الشهادة (الحزمة الثانية) وجميع المرجع المصدق لأن المستجيب ليس لديه معرفة بملف التعريف الذي يجب إستخدامه في هذه المرحلة. يتم إرسال الحزمة التي تحتوي على المعلومات إلى البادئ:

```
                                       IKEv2 IKE_SA_INIT Exchange RESPONSE
                                                   :Payload contents
                          SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY
(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)
```

يقوم البادئ بمعالجة الحزمة ويختار نقطة ثقة تطابق المرجع المصدق المقترح:

```
                IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from
                                        (received certificate hash(es
'IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'TP1
```

يرسل البادئ بعد ذلك الحزمة الثالثة مع كل من طلب الشهادة وحمولة الشهادة. هذه الحزمة مشفرة بالفعل باستخدام مادة الكبلات من مرحلة DH) Diffie-Hellman):

```
                .IKEv2:(SA ID = 1):Building packet for encryption
                                                    :Payload contents
```

```
VID IDi CERT CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) AUTH CFG SA TSi
(TSr NOTIFY(INITIAL_CONTACT) NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT
(NOTIFY(NON_FIRST_FRAGS
```

يتم إرسال الحزمة الرابعة من المستجيب إلى البادئ وتحتوي فقط على حمولة الشهادة:

```
IKEv2 IKE_AUTH Exchange RESPONSE
:Payload contents
(VID IDr CERT AUTH SA TSi TSr NOTIFY(SET_WINDOW_SIZE) NOTIFY(ESP_TFC_NO_SUPPORT
(NOTIFY(NON_FIRST_FRAGS
```

يشبه التدفق الموضح هنا تدفق IKEv1. يجب أن يرسل المستجيب حمولة طلب الشهادة لأعلى بدون معرفة ملف التعريف الذي يجب إستخدامه، مما يؤدي إلى نفس المشاكل التي تم وصفها سابقا ل IKEv1 (من منظور بروتوكول). ومع ذلك، فإن التنفيذ على IOS هو أفضل ل IKEv2 منه ل IKEv1.

نقطة ثقة IKEv2 الإلزامية للبادئ

فيما يلي مثال على محاولة بادئ IKEv2 إستخدام توصيف بمصادقة شهادة وليس به نقطة ثقة مكونة ضمن ذلك التوصيف:

```
crypto ikev2 profile profile1
match identity remote address 192.168.0.2 255.255.255.255
identity local address 192.168.0.1
authentication remote rsa-sig
authentication local rsa-sig
```

يتم إرسال الحزمة الأولى بدون أي حمولة طلب شهادة، كما هو موضح مسبقا. تتضمن الاستجابة من المستجيب حمولة طلب الشهادة لكافة النقاط الموثوق بها المحددة في وضع "التكوين العام". تم تلقي هذا بواسطة البادئ:

```
(Jul 17 17:40:43.183: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s*
(from received certificate hash(es
Jul 17 17:40:43.183: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved*
'trustpoint(s): 'TP1
()Jul 17 17:40:43.183: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject*
Jul 17 17:40:43.183: CRYPTO_PKI: Found a subject match*
()Jul 17 17:40:43.183: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject*
Jul 17 17:40:43.183: CRYPTO_PKI: Found a subject match*
Jul 17 17:40:43.183: CRYPTO_PKI: Trust-Point TP1 picked up*
Jul 17 17:40:43.183: CRYPTO_PKI: 1 matching trustpoints found*
(Jul 17 17:40:43.183: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s*
(from received certificate hash(es
Jul 17 17:40:43.183: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved*
'trustpoint(s): 'TP2
Jul 17 17:40:43.183: CRYPTO_PKI: Trust-Point TP2 picked up*
()Jul 17 17:40:43.183: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject*
Jul 17 17:40:43.183: CRYPTO_PKI: Found a subject match*
()Jul 17 17:40:43.183: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject*
Jul 17 17:40:43.183: CRYPTO_PKI: Found a subject match*
Jul 17 17:40:43.183: CRYPTO_PKI: 1 matching trustpoints found*
```

```
Jul 17 17:40:43.183: IKEv2:(SA ID = 1):Failed to build certificate payload*
```

لا يعرف البادئ نقطة الثقة التي يجب إستخدامها للتوقيع. وهذا هو الفرق الرئيسي عند مقارنة تنفيذ IKEv2 بالإصدار الأول من بروتوكول الإنترنت. يجب أن يحتوي بادئ IKEv2 على نقطة الثقة التي تم تكوينها ضمن ملف تعريف بادئ IKEv2، ولكن هذا ليس ضروريا لمستجيب IKEv2.

هنا مقتطف من مرجع الأمر:

في حالة عدم وجود نقطة ثقة معرفة في تكوين ملف تعريف IKEv2، فإن الإعداد الافتراضي هو **التحقق من صحة الشهادة** باستخدام جميع نقاط الثقة المحددة في التكوين العام
من الممكن تحديد نقاط ثقة مختلفة، واحدة للتوقيع وأخرى مختلفة للتحقق من الصحة. لسوء الحظ، لا تحل نقطة الثقة الإلزامية التي تم تكوينها ضمن ملف تعريف IKEv2 كل المشاكل.

R2 كبادئ IKEv2

في هذا المثال، R2 هو بادئ IKEv2:

```
crypto ikev2 profile profile1
match identity remote address 192.168.0.1 255.255.255.255
identity local address 192.168.0.2
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint TP1
pki trustpoint TP2
```

في هذا المثال، R1 هو المستجيب ل IKEv2:

```
crypto ikev2 profile profile1
match identity remote address 192.168.0.2 255.255.255.255
identity local address 192.168.0.1
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint TP1
```

هنا، يرسل R2 الحزمة الأولى دون أي طلب شهادة. يستجيب المستجيب لطلب شهادة لكافة نقاط الثقة التي تم تكوينها. يماثل ترتيب الحمولات IKEv1 ويعتمد على الشهادات التي يتم تثبيتها:

```
R1#show crypto pki certificates
Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
:Issuer
cn=CA2
....
Associated Trustpoints: TP2
```

تقترن أول شهادة تم تكوينها على R1 بنقطة الثقة **TP2**، لذلك تكون حمولة طلب الشهادة الأولى ل CA المقترن بنقطة الثقة **TP2**. وبالتالي، يحدده R2 للمصادقة (قاعدة المطابقة الأولى):

```
R2#
*Jul 17 18:09:04.542: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message
*Jul 17 18:09:04.542: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s
 (from received certificate hash(es
*Jul 17 18:09:04.542: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved
 'trustpoint(s): 'TP2
*Jul 17 18:09:04.542: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for
 the trustpoint TP2
*Jul 17 18:09:04.542: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain
 for the trustpoint PASSED
```

بعد ذلك، يقوم R2 بإعداد إستجابة (الحزمة 3) مع حمولة طلب الاعتماد المقترنة **ب TP2**. لا يمكن ل R1 الثقة بالشهادة نظرا لتكوينها للتحقق من صحتها مقابل نقطة الثقة **TP1**:

```
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s
 (from received certificate hash(es
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved
 'trustpoint(s): 'TP1
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for
 the trustpoint TP1
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain
 for the trustpoint PASSED
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):Get peer's authentication method
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):Peer's authentication method is 'RSA'
*Jul 17 18:09:04.550: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Validating
 certificate chain
*Jul 17 18:09:04.554: IKEv2:(SA ID = 1):[PKI -> IKEv2] Validation of certificate
 chain FAILED
*Jul 17 18:09:04.554: IKEv2:(SA ID = 1):Verification of peer's authentication
 data FAILED
*Jul 17 18:09:04.554: IKEv2:(SA ID = 1):Sending authentication failure notify
*Jul 17 18:09:04.554: IKEv2:(SA ID = 1):Building packet for encryption.
 Payload contents:
 (NOTIFY(AUTHENTICATION_FAILED
```

وكما ذكرنا سابقا، توصي Cisco بعدم إستخدام نقاط ثقة متعددة ضمن ملف تعريف IKEv2. عندما تستخدم نقاط ثقة متعددة، من الضروري التأكد من أن كلا الجانبين يثقان بنفس نقاط الثقة تماما. على سبيل المثال، كل من R1 و R2 به كلا من TP1 و TP2 مكون في ملفات التعريف الخاصة بهما.

ملخص

يقدم هذا القسم ملخصا موجزا للمعلومات الموصوفة في الوثيقة.

يعتمد محتوى حمولة طلب الشهادة على التكوين. إذا تم تكوين نقطة ثقة معينة لتوصيف ISAKMP وكان الموجه هو بادئ ISAKMP، فإن طلب الشهادة في MM3 يحتوي فقط على CA المقترن بنقطة الثقة. ومع ذلك، إذا كان الموجه نفسه هو مستجيب ISAKMP، فإن حزمة MM4 التي يتم إرسالها بواسطة الموجه تتضمن العديد من حمولات طلب الشهادة لجميع نقاط الثقة المحددة بشكل عام (عند عدم أخذ أمر **ca trust-point** في الاعتبار). يحدث هذا لأن المستجيب ISAKMP يمكنه تحديد ملف تعريف ISAKMP الذي يجب إستخدامه فقط بعد أن يستلم MM5 وطلب

الشهادة المضمن في MM4.

حمولة طلب الشهادة في MM3 و MM4 مهمة بسبب قاعدة المطابقة الأولى. تحدد قاعدة المطابقة الأولى نقطة الثقة المستخدمة لتحديد الشهادة، والتي تكون مطلوبة للمصادقة في MM5 و MM6.

يعتمد ترتيب حمولة طلب الشهادة على ترتيب الشهادات المثبتة. يتم إرسال مصدر الشهادة الأولى التي تظهر في إخراج الأمر **show crypto pki** أولا. هذه الشهادة الأولى هي آخر شهادة تم تسجيلها.

من الممكن تكوين نقاط ثقة متعددة لملف تعريف ISAKMP. إذا تم تنفيذ هذا الإجراء، فلا تزال كافة القواعد السابقة مطبقة.

كل المشاكل والتحذيرات أن يكون وصفت في هذا وثيقة إلى ال IKEv1 بروتوكول تصميم. تحدث مرحلة المصادقة في MM5 و MM6، بينما يجب إرسال مقترحات المصادقة (طلبات الشهادات) في مرحلة سابقة (في الأمام) دون معرفة ملف تعريف ISAKMP الذي يجب إستخدامه. هذه ليست مشكلة خاصة ب Cisco وترتبط بقيود تصميم بروتوكول IKEv1.

يشبه بروتوكول IKEv2 بروتوكول IKEv1 فيما يتعلق بعملية تفاوض الشهادة. ومع ذلك، يفرض التنفيذ على نظام التشغيل IOS إستخدام نقاط ثقة محددة للبادئ. هذا لا يحل كل القضايا. عند تكوين نقاط ثقة متعددة لملف تعريف واحد وتكوين نقطة ثقة واحدة على الجانب الآخر، يظل من الممكن مواجهة مشاكل مع المصادقة. توصي Cisco باستخدام تكوينات نقطة ثقة متماثلة لكلا جانبي الاتصال (نفس نقاط الثقة التي تم تكوينها لكل من ملفات تعريف IKEv2).

فيما يلي بعض الملاحظات المهمة حول المعلومات الموضحة في هذا المستند:

ومع تكوينات نقاط الثقة غير المتماثلة لتوصيفات IKEv1 الخاصة بالأقران، قد يبدأ النفق من جانب واحد فقط من النفق. تكوين نقطة الثقة لملف تعريف IKEv1 إختياري.

- ومع تكوينات نقاط الثقة غير المتماثلة لتوصيفات IKEv2 للنظراء، قد يبدأ النفق من جانب واحد فقط من النفق. تكوين نقطة الثقة لملف تعريف IKEv2 إلزامي للبادئ.

- يعتمد ترتيب حمولة طلب الشهادة على ترتيب الشهادات التي تظهر في مخرجات أمر **show crypto pki certificate** (المطابقة الأولى).

- يحدد أمر حمولة طلب الشهادة الشهادة التي تم تحديدها بواسطة المستجيب (المطابقة الأولى).

- عندما تستخدم ملفات تعريف متعددة ل IKEv1 و IKEv2 ولها نفس قواعد هوية المطابقة مكونة، فمن الصعب التنبؤ بالنتائج (متضمن العديد من العوامل).

- توصي Cisco باستخدام تكوينات نقطة الثقة المتماثلة لكل من IKEv1 و IKEv2.

معلومات ذات صلة

- [تبادل مفتاح الإنترنت لدليل تكوين Cisco IOS، IPsec VPNs، الإصدار 15M&T - شهادة لتعيين ملف تعريف ISAKMP]
- [مرجع أمر أمان Cisco IOS: يصدر الأمر a إلى ca trust-point - C من خلال clear eou]
- [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).