IOS IKEv1 en IKEv2 Packet Exchange-processen voor profielen met meerdere certificaten

Inhoud

Inleiding

Dit document beschrijft de Internet Key Exchange Versie 1 (IKEv1) en de Internet Key Exchange Versie 2 (IKEv2)-pakketuitwisselingsprocessen wanneer certificatie wordt gebruikt en de mogelijke problemen die zich kunnen voordoen.

Hieronder volgt een lijst met onderwerpen die in dit document worden beschreven:

- De selectiecriteria voor het certificaat van de IKE-initiator (Internet Key Exchange) en de IKE-responder
- De IKE-profielmatchcriteria wanneer meerdere IKE-profielen zijn afgestemd (voor overlap- en non-overlap-scenario's)
- De standaardinstellingen en het gedrag wanneer er geen trust-points worden gebruikt onder de IKE-profielen
- De verschillen tussen de IKEv1 en de IKEv2 wat betreft profiel- en certificeringsselectiecriteria

Opmerking: Zie de juiste sectie voor informatie over het oplossen van een specifiek probleem. Aan het einde van dit document wordt ook een korte samenvatting gegeven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS VPN-configuratie
- IKEv1- en IKEv2-protocollen (pakketuitwisseling)

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS versie 15.3T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De problemen die in dit document worden beschreven, ontstaan wanneer meerdere trust-points en meerdere IKE profielen worden gebruikt.

De eerste voorbeelden die in dit document worden gebruikt hebben een IKEv1 LAN-to-LAN tunnel met twee trust-points op elke router. Eerst lijkt de configuratie misschien juist. De VPN-tunnel kan echter alleen van één kant van de verbinding worden geïnitieerd vanwege de manier waarop de opdracht **CA trust-point** wordt gebruikt voor het profiel van Internet Security Association en Key Management Protocol (ISAKMP) en voor de volgorde van de ingeschreven certificaten in de lokale winkel.

Een ander gedrag wordt ingesteld met de opdracht **CA trust-point** voor het ISAKMP-profiel wanneer de router de ISAKMP-initiator is. Een probleem kan zich voordoen omdat de ISAKMP-initiator vanaf het begin op de hoogte is van het ISAKMP-profiel, zodat de opdracht **CA trust-point** die voor het profiel is geconfigureerd de lading voor het certificaatverzoek in hoofdmodus 3 (MM3) kan beïnvloeden. Wanneer de router echter de ISAKMP-responder is, bindt hij het inkomende verkeer aan een specifiek ISAKMP-profiel nadat het het hoofdmode Packet 5 (MM5) ontvangt, dat de IKE-id bevat die nodig is om de verbinding te maken. Dit is de reden dat het niet mogelijk is om

een **ca trust-point** opdracht toe te passen voor het pakket met hoofdmodus 4 (M4) omdat het profiel niet bepaald is vóór de MM5.

De volgorde van het certificaat vraagt om lading in de MM3 en M4 en de impact op het gehele onderhandelingsproces wordt in dit document uitgelegd, evenals de reden dat de verbinding alleen aan één kant van de VPN-tunnel kan worden gelegd.

Hier volgt een samenvatting van de IKEv1-initiator en het gedrag van de respondenten:

	IKEv1-initiator	IKEv1-responder
Aanvraag sturen	Hiermee worden alleen specifieke verzoeken verzonden voor de trust-points die onder het profiel zijn geconfigureerd	Zendt verzoeken om alle beschikbare trust-points toe
Valideren aanvraag	Valideert tegen specifieke trust-points die onder het profiel zijn geconfigureerd	Valideert tegen specifieke trust-points die onder het profiel zijn geconfigureerd

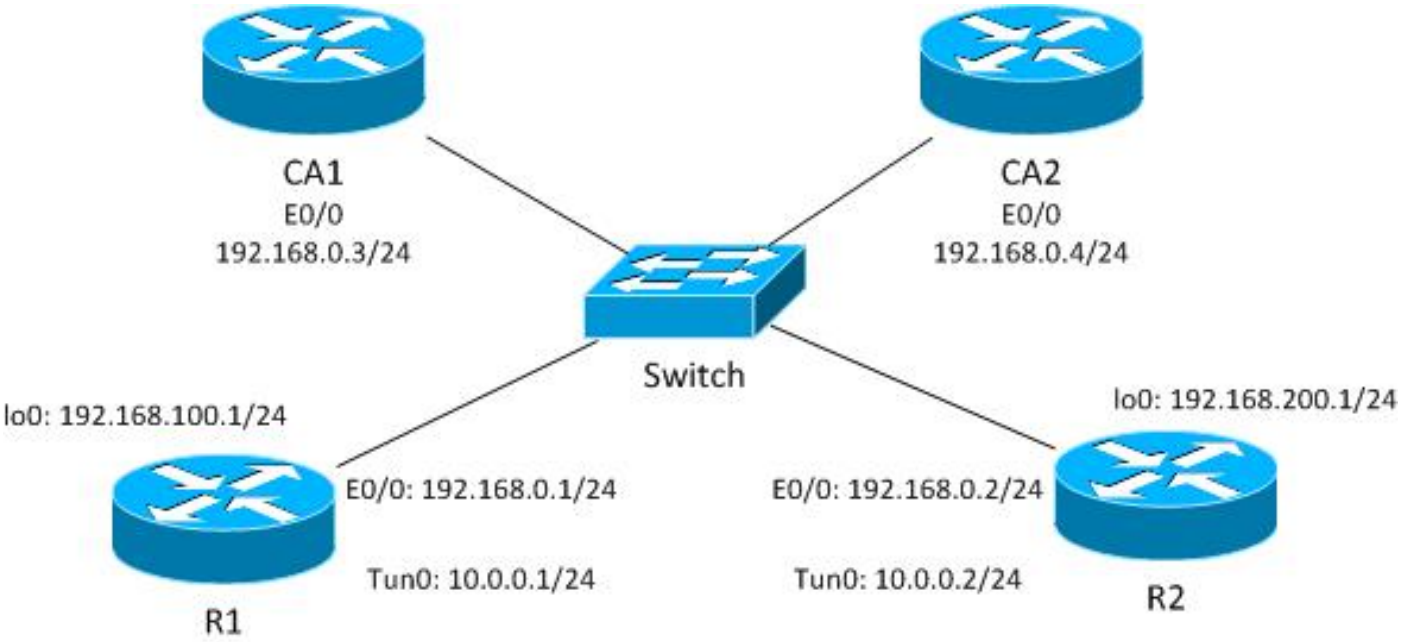
Cisco raadt u aan om de **ca trust-point** opdracht niet te gebruiken voor de ISAKMP-responders die meerdere ISAKMP-profielen hebben en wereldwijd geconfigureerd trust-points gebruiken. Voor ISAKMP-initiators met meerdere ISAKMP-profielen raadt Cisco u aan het selectieproces van het certificaat te beperken met de opdracht **CA-trust-punt** in elk profiel.

Het IKEv2-protocol heeft dezelfde problemen als het IKEv1-protocol, maar het verschillende gedrag van de opdracht **Pki-trustpunt** helpt het optreden van de problemen te voorkomen. Dit komt doordat de opdracht **Pki trustpoint** verplicht is voor de IKEv2-initiator, terwijl de opdracht **CA trust-point** optioneel is voor de IKEv1-initiator. Onder bepaalde omstandigheden (meerdere trust-points onder één profiel) kunnen de eerder beschreven problemen optreden. Om deze reden, raadt Cisco aan om symmetrische trust-point configuraties te gebruiken voor beide kanten van de verbinding (de zelfde trust-points die onder beide IKEv2 profielen worden gevormd).

Topologie

Dit is een generieke topologie die voor alle voorbeelden in dit document wordt gebruikt.

> Opmerking: Router 1 (R1) en router 2 (R2) gebruiken Virtual Tunnel Interfaces (VTI's) om toegang te krijgen tot de loopback-ups. Deze VTI's worden door IPSec beschermd.



Voor dit IKEv1 voorbeeld heeft elke router twee trust-points voor elke certificaatinstantie (CA) en worden de certificaten voor elk van de trust-points geregistreerd.

Wanneer R1 de initiator van ISAKMP is, onderhandelt de tunnel correct en wordt het verkeer beschermd. Dit wordt verwacht. Wanneer R2 de ISAKMP-initiator is, mislukt de fase1-onderhandeling.

> Opmerking: Voor de voorbeelden IKEv2 in dit document, is de topologie en het adresseren hetzelfde als dat van het IKEv1 voorbeeld.

Packet Exchange-proces

In dit gedeelte worden de IKEv1- en de IKEv2-configuratievariaties beschreven die gebruikt worden voor het pakketuitwisselingsproces en de mogelijke problemen die zich kunnen voordoen.

IKEv1 met meerdere certificaten

Hier zijn het R1 netwerk en de configuratie van VPN voor IKEv1 met meerdere certificaten:

```
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
```

Hier zijn het R2-netwerk en de VPN-configuratie voor IKEv1 met meerdere certificaten:

```
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
```

In dit voorbeeld heeft R1 twee trust-points: de ene gebruikt **IOSCA1** en de tweede gebruikt **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
```

In dit voorbeeld heeft R2 ook twee vertrouwenspunten: de ene gebruikt IOSCA1 en de tweede gebruikt 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
```

Het is belangrijk op te merken dat er in deze formaties sprake is van één enkel verschil: In het R1 ISAKMP-profiel wordt de opdracht c trust-point gebruikt voor het IOSCA1 trust-point, dat aangeeft dat R1 alleen de certificaten vertrouwt die door dat specifieke trust-punt zijn gevalideerd. In contrast hiermee vertrouwt R2 alle certificaten die worden gevalideerd door alle mondiaal gedefinieerde trust-points.

R1 als IKEv1-initiator

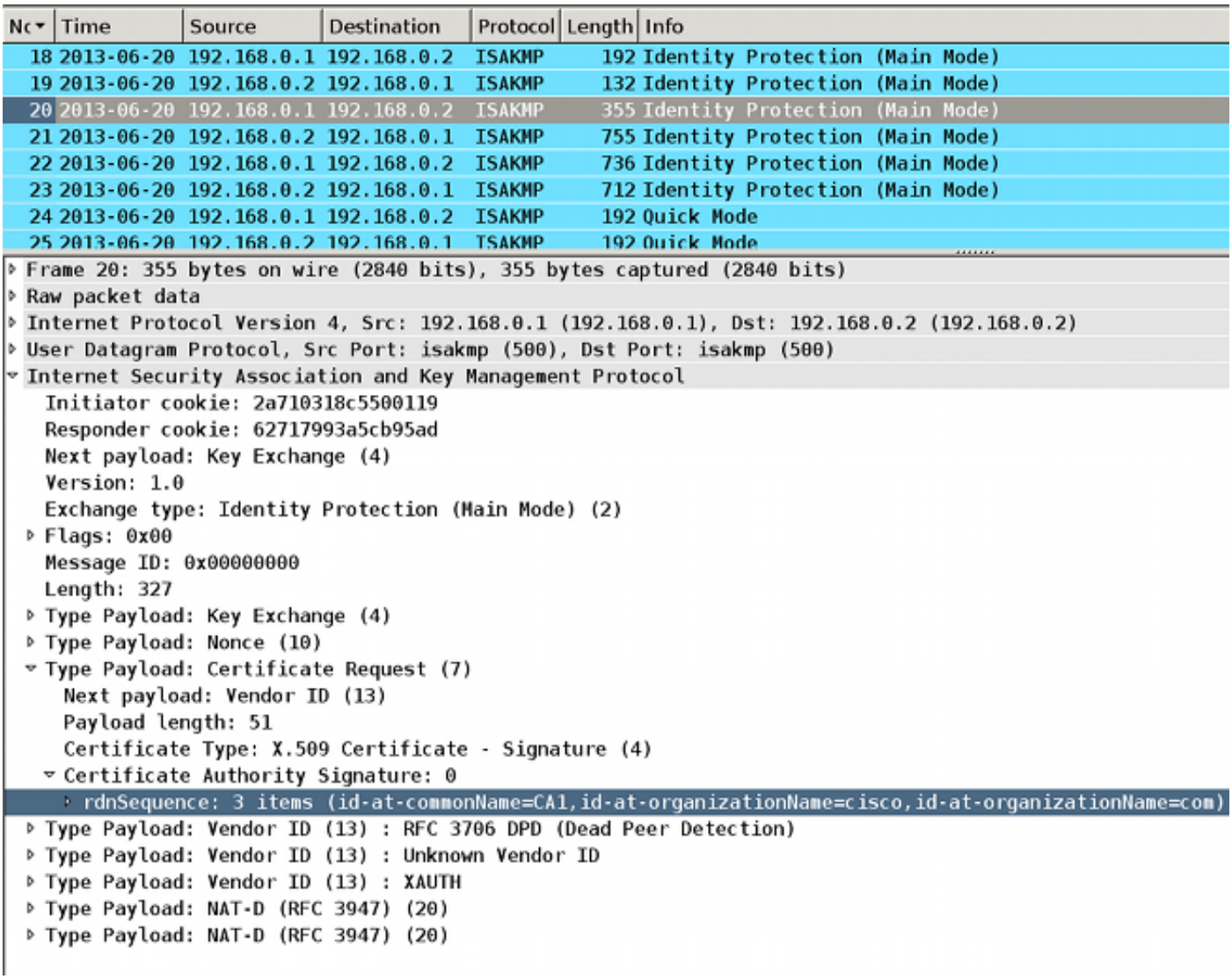
Hier zijn de debugs opdrachten voor zowel R1 als R2:

- R1# debug van cryptografische signalen
- R1# debug van crypto ipsec
- validatie van R1#-debug van cryptografische kaarten

Hier start R1 de tunnel en stuurt het certificaatverzoek naar de 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
```

Het is belangrijk om op te merken dat het pakket slechts één certificaatverzoek bevat, wat slechts voor het trustpunt **IOSCA1** is. Dit is verwacht gedrag met de huidige configuratie van het ISAKMP-profiel (**CN=CA1, O=cisco, O=com**). Er worden geen andere certificaatverzoeken verstuurd, die u met de ingesloten pakketvastlegging kunt controleren:



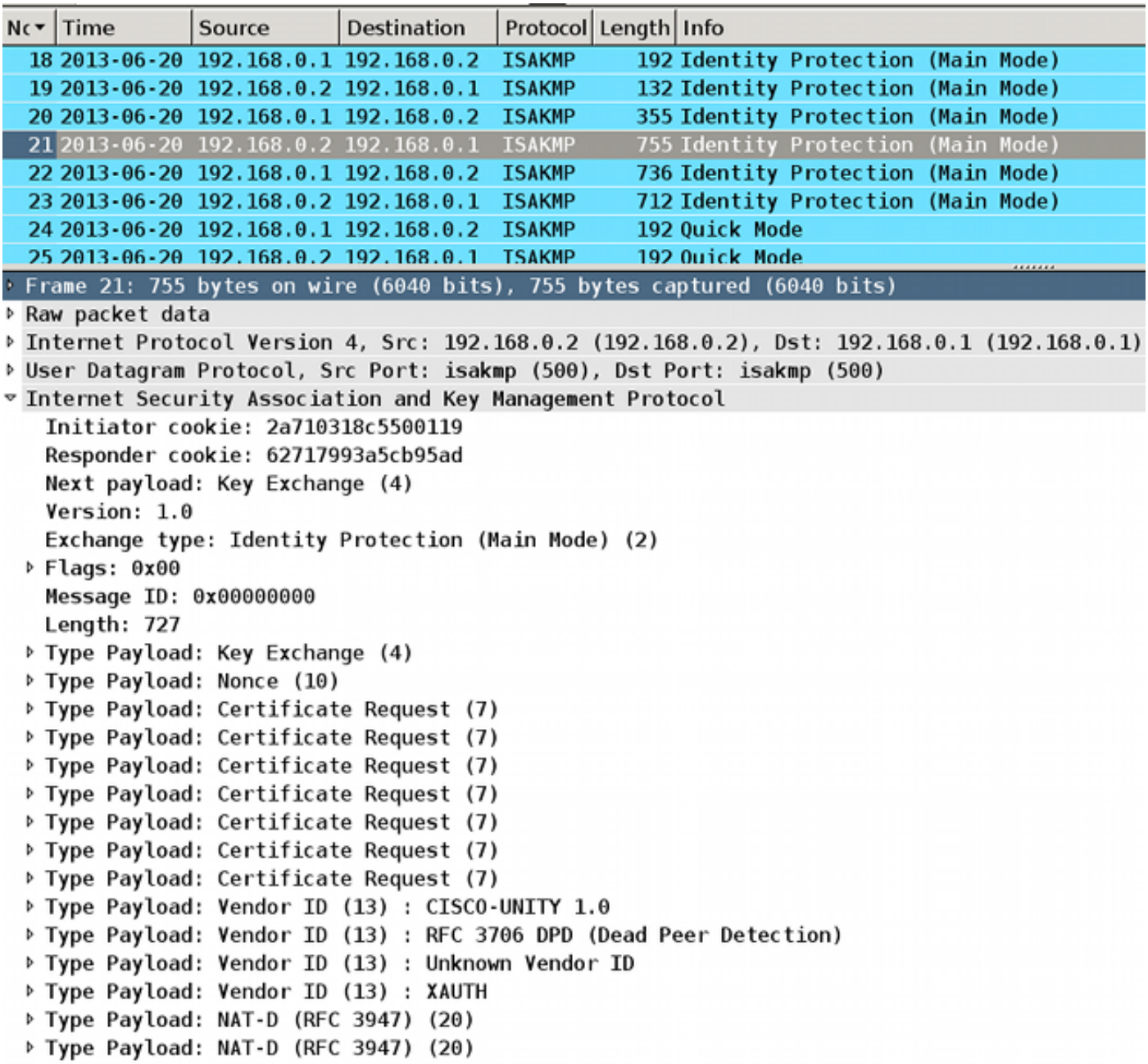
Wanneer R2 het pakket ontvangt, begint het de certificaataanvraag te verwerken, wat een match maakt die het trust-punt en het bijbehorende certificaat bepaalt die voor authenticatie in MM5 gebruikt wordt. De procesvolgorde is hetzelfde als de lading van het certificaat in het ISAKMP-pakket. Dit betekent dat de eerste match wordt gebruikt. In dit scenario is er slechts één match omdat R1 is geconfigureerd met een specifiek trust-punt en slechts één certificaataanvraag verstuurt die is gekoppeld aan het trust-punt.

```
*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
```

Daarna bereidt R2 de MM4 voor. Dit is het pakket dat het certificaatverzoek voor alle vertrouwde trust-points bevat. Omdat R2 de ISAKMP-responder is, worden alle wereldwijd gedefinieerde trust-points vertrouwd (de configuratie van de ca trust-punten is niet afgevinkt). Twee van de trust-punten worden handmatig gedefinieerd (IOSCA1 en IOSCA2), en de rest wordt vooraf gedefinieerd.

```
*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
 192.168.0.1 my_port 500 peer_port 500 (R) MM_KEY_EXCH
*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
```

U kunt het pakket met Wireshark controleren. Het M4-pakket van R2 bevat zeven items voor certificaataanvraag:



No.	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

Vervolgens ontvangt R1 de M4 van R2 met meerdere velden voor certificaataanvraag:

```
*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
```

De first-match regel op R1 komt overeen met de eerste certificaataanvraag met het IOSCA1-trust-punt. Dit bepaalt dat R1 het certificaat gebruikt dat is geassocieerd met een trust-point **IOSCA1** voor verificatie in de MM5. De Full Qualified Domain Name (FQDN) wordt gebruikt als IKE-ID. Dit is te wijten aan de configuratie **van het** ISAKMP-profiel **met een** eigen identiteit:

```
*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
```

De MM5 wordt ontvangen en verwerkt door R2. De ontvangen IKE-id (**R1.cisco.com**) komt overeen met het ISAKMP-profiel **prof1**. Het ontvangen certificaat wordt dan gevalideerd en de authenticatie is succesvol:

```
*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
```

Vervolgens maakt R2 MM6 op met het certificaat dat aan **IOSCA1** is gekoppeld:

```
*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
```

Het pakket wordt ontvangen door R1 en R1 verifieert het certificaat en de authenticatie:

```
*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
```

Dit is de voltooiing van fase 1. Fase 2 wordt zoals gewoonlijk onderhandeld. De tunnel is opgericht en het verkeer is beschermd.

R2 als IKEv1-initiator

Dit voorbeeld beschrijft het proces wanneer R2 dezelfde IKEv1-tunnel initieert en verklaart waarom deze niet is opgezet.

> Opmerking: Delen van de stammen worden verwijderd om zich uitsluitend te richten op de verschillen ten opzichte van het in de vorige paragraaf weergegeven voorbeeld.

R2 verstuurt de MM3 met zeven betaling van het certificaatverzoek omdat R2 geen vertrouwen heeft dat aan het ISAKMP-profiel is gekoppeld (alle trust-points worden vertrouwd):

```
*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
```

Wanneer R1 het pakket van R2 ontvangt, verwerkt het het certificaatverzoek en komt het IOSCA1 trust-point overeen, dat het certificaat bepaalt dat in MM6 wordt verzonden:

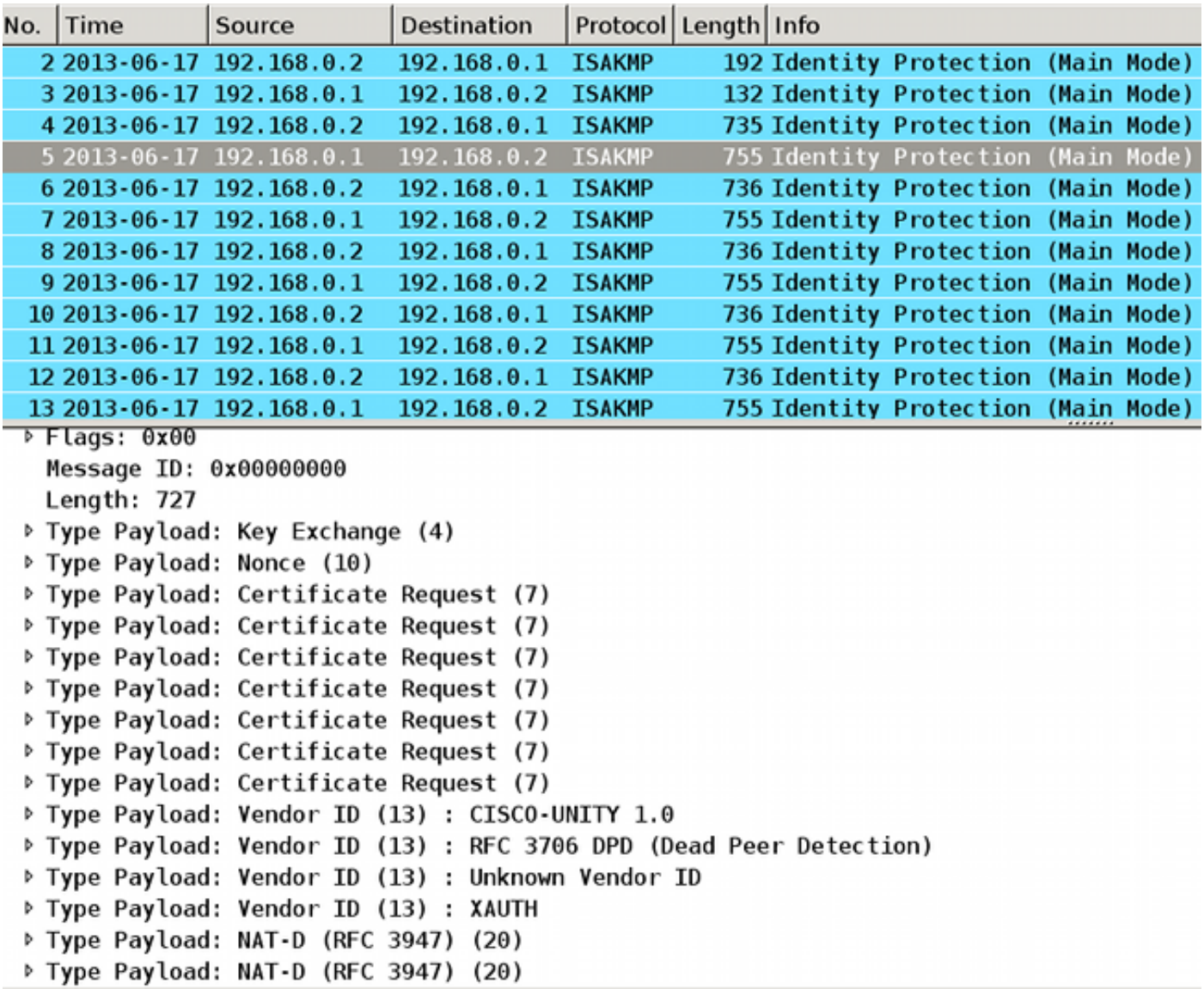
```
*Jun 17 18:08:14.321: ISAKMP:(1099): processing CERT_REQ payload.
 message ID = 0
*Jun 17 18:08:14.321: ISAKMP:(1099): peer wants a CT_X509_SIGNATURE cert
*Jun 17 18:08:14.321: ISAKMP:(1099): peer wants cert issued by
 cn=CA1,o=cisco,o=com
*Jun 17 18:08:14.321:  Choosing trustpoint IOSCA1 as issuer
*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
```

Daarna bereidt R1 het M4-pakket voor met de lading van de certificaataanvraag. Nu zijn er meerdere aanvragen voor een certificaat:

```
*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
```

Controleer de logbestanden met Ingesloten Packet Capture (EPC) en 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)

Hoewel R1 in het ISAKMP-profiel is geconfigureerd voor één trust-point (**IOSCA1**), worden er meerdere certificaatverzoeken verstuurd. Dit komt voor omdat de opdracht **CA trust-point** in het ISAKMP-profiel de lading van de certificaataanvraag bepaalt, maar alleen wanneer de router de initiator van de ISAKMP-sessie is. Als de router de responder is, zijn er meerdere certificatenbetalingen voor alle globaal gedefinieerde trust-points, omdat R1 het ISAKMP-profiel nog niet kent dat voor de IKE-sessie gebruikt wordt.

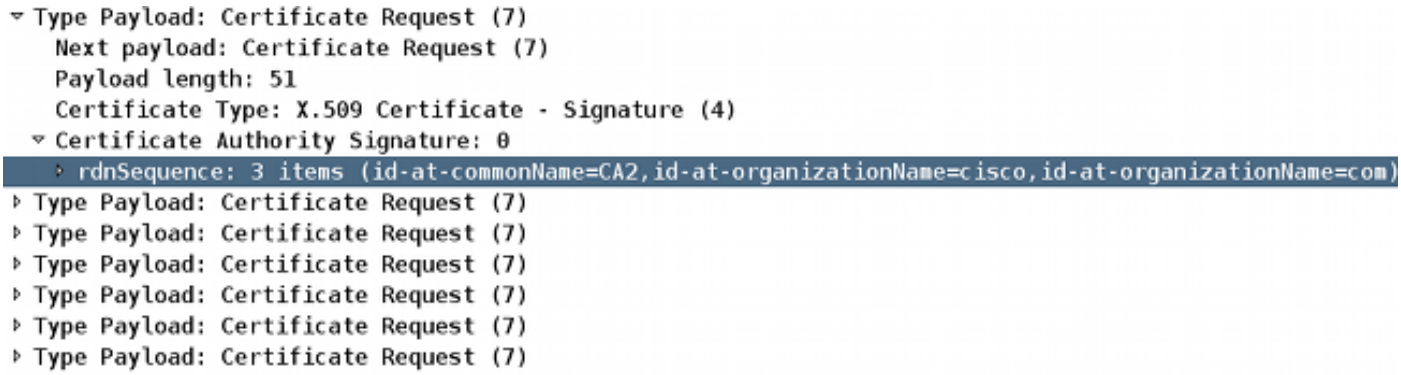
De inkomende IKE-sessie is gebonden aan een specifiek ISAKMP-profiel na ontvangst van de

MM5, die de IKE-ID bevat. Vervolgens bindt de opdracht **matchidentiteit** voor het specifieke profiel de IKE-sessie aan het profiel. De router kan dit echter nog niet bepalen. Er kunnen meerdere ISAKMP-profielen zijn met verschillende **ca trust-point** opdrachten ingesteld voor elk profiel.

Om deze reden moet R1 het certificaatverzoek voor alle wereldwijd gevormde trust-punten verzenden.

Raadpleeg de opdrachtreferentie voor de opdracht **CA trust-punt**:

Een router die IKE initieert en een router die op het IKE-verzoek reageert moet symmetrische trustpuntconfiguraties hebben. Een reagerende router (in IKE Main Mode) die RSA-signaalencryptie en -verificatie uitvoert, kan bijvoorbeeld trustpoints gebruiken die in de mondiale configuratie zijn gedefinieerd bij het verzenden van de CERT-REQ-nuttige ladingen. De router kan echter wel een beperkte lijst van trustpunten gebruiken die in het ISAKMP-profiel zijn gedefinieerd voor de verificatie van de certificaten. Als de peer (de IKE-initiator) is geconfigureerd om een certificaat te gebruiken waarvan het vertrouwenspunt in de globale lijst van de antwoordrouter staat maar niet in het ISAKMP-profiel van de antwoordrouter, wordt het certificaat afgewezen. (Als de initiatiefnemende router echter niet op de hoogte is van de trustpunten in de mondiale configuratie van de reagerende router, kan het certificaat nog steeds worden geauthentiseerd.)
Controleer nu de M4-pakketgegevens om de eerste payload van een certificaataanvraag te ontdekken:



Het M4-pakket dat van R1 wordt verzonden, bevat het IOSCA2-trustpunt in het eerste certificaatverzoek om betaling vanwege de volgorde waarin de certificaten zijn geïnstalleerd; het eerste wordt ondertekend door het trustpunt **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>
```

Maak een vergelijking met het MM3-pakket dat van R2 wordt verzonden wanneer het IOSCA1-trust-punt is opgenomen in het eerste certificaat aanvraag om een lading:

```
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>
```

Nu ontvangt R2 het M4-pakket van R1 en begint het de certificaataanvraag te verwerken. Het eerste certificaatverzoek heeft betrekking op de lading van de IOSCA2-trust:

```
*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
```

Wanneer R2 het M5-pakket voorbereidt, gebruikt het het certificaat dat is gekoppeld aan het IOSCA2-trust-punt:

```
*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.
```

Het M5-pakket wordt ontvangen door R1. Omdat R1 alleen het IOSCA1-trust-punt vertrouwt (voor ISAKMP-profiel prof1), verloopt de certificeringsvalidering niet:

```
*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
 192.168.0.2 is bad: unknown error returned in certificate validation
R1#
*Jun 17 18:08:44.341: ISAKMP:(1100): Unknown error in cert validation, -1
```

Deze configuratie werkt als de volgorde van de certificaatinschrijving op R1 verschillend is omdat het eerste weergegeven certificaat door het **IOSCA1** trust-punt wordt ondertekend. Ook is de eerste lading van het certificaat in de MM4 het trustpunt **IOSCA1**, dat vervolgens door R2 wordt gekozen en met succes op R1 in de MM6 wordt gevalideerd.

IKEv1 zonder c-*trust-point* opdracht in het profiel

Voor scenario's met meerdere profielen en trust-points, maar zonder een specifieke configuratie van het trust-punt in de profielen, zijn er geen kwesties omdat er geen validatie is van specifieke trust-points die zijn bepaald door een commandoconfiguratie van **ca trust-punten**. Het selectieproces is echter mogelijk niet duidelijk. Afhankelijk van de router die de initiator is, worden de verschillende certificaten geselecteerd voor het authenticatieproces in relatie tot de volgorde van inschrijving van certificaten.

Soms kan een certificaat slechts door één kant van de verbinding worden ondersteund, zoals in x509 versie 1, die geen typische hashfunctie is die wordt gebruikt om te tekenen. De VPN-tunnel kan alleen aan één kant van de verbinding worden gemaakt.

RFC-referentie voor IKEv1

Hier volgt een fragment uit RFC4945:

3.2.7.1. Specificatie van certificeringsinstanties

Bij **het** in-band **aanvragen** van uitwisseling van testmateriaal, dienen implementaties CERTREQ's te genereren voor elk peer trust anker dat **lokaal beleid** tijdens een bepaalde beurs **expliciet** als betrouwbaar wordt beschouwd.
De RFC is niet helder. Het **lokale beleid** zou **expliciet** kunnen betrekking hebben op de **ca trust-point** opdracht die in het crypto ISAKMP-profiel is geconfigureerd. Het probleem is dat u in de fase MM3 en M4 van het proces geen ISAKMP-profiel kunt selecteren tenzij u een IP-adres voor de identiteit en de trust-punten gebruikt omdat de verificatie in de fase M5 en M6 van het proces eerst moet plaatsvinden. Om deze reden heeft **het lokale beleid expliciet** betrekking op alle trust-points die op het apparaat zijn geconfigureerd.

> Opmerking: Deze informatie is niet specifiek voor Cisco, maar specifiek voor IKEv1.

Selectie van IKEv2-profiel met identificatiemiddelen die elkaar overlappen

Voordat meerdere certificaten voor IKEv2 worden beschreven, is het belangrijk om te weten hoe de profielen worden geselecteerd wanneer de matchidentiteit wordt gebruikt, wat voor alle profielen is voldaan. Dit is geen aanbevolen scenario omdat de resultaten van de IKEv2-onderhandeling afhankelijk zijn van meerdere factoren. Dezelfde problemen bestaan voor IKEv1 wanneer profielen worden gebruikt die elkaar overlappen.

Hier is een voorbeeld van de configuratie van de IKEv2-initiator:

```
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
```

Het identiteitstype wordt gebruikt voor beide zijden van de verbinding. Verificatie via certificaten (kan ook vooraf gedeelde sleutels zijn) is niet belangrijk voor dit voorbeeld. De responder heeft meerdere profielen die allemaal overeenkomen met het inkomende IKEv2-verkeer:

```
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
```

De initiator verstuurt het derde IKEv2-pakket en de responder moet het profiel kiezen op basis van de identiteit die wordt ontvangen. De identiteit is een IPv4-adres (**192.168.0.1**):

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

Alle profielen voldoen aan deze identiteit vanwege de opdracht **overeenkomende identiteit** die is geconfigureerd. IOS kiest de laatste in de configuratie, die **profile3** is in dit voorbeeld:

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

Om de bestelling te verifiëren, voer de opdracht van het **tooncrypto ikev2-profiel in**.

> Opmerking: Zelfs wanneer het profiel een algemeen adres (0.0.0.0) heeft, wordt het nog geselecteerd. De IOS probeert niet de beste overeenkomst te vinden; het probeert de eerste wedstrijd te vinden . Dit gebeurt echter alleen omdat alle profielen dezelfde **matchen hebben als de** opdracht **op afstand** is ingesteld. Voor de IKEv1- en de IKEv2-profielen met verschillende matrixidentiteitsregels wordt altijd de meest specifieke gebruikt. Cisco raadt u aan om de profielen niet te hebben die met de **overlappende** opdracht van de **matchidentiteit** zijn geconfigureerd omdat het moeilijk is om het geselecteerde profiel te voorspellen.

In dit scenario wordt **profile3** geselecteerd door de responder, maar **profile1** wordt gebruikt voor de tunnelinterface. Hierdoor wordt een fout weergegeven wanneer de proxy-ID is onderhandeld:

```
*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
```

IKEv2 Flow wanneer certificaten worden gebruikt

Wanneer certificaten voor IKEv2 worden gebruikt om voor echtheid te zorgen, stuurt de initiator de certificaataanvraag niet in het eerste pakket:

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

De responder antwoordt met het certificaatverzoek om lading (tweede pakket) en alle CA's omdat de responder geen kennis heeft van het profiel dat in dit stadium moet worden gebruikt. Het pakket met de informatie wordt naar de initiator verzonden:

```
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)
```

De initiator verwerkt het pakket en kiest een trust-punt dat met de voorgestelde CA overeenkomt:

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

De initiatiefnemer stuurt vervolgens het derde pakket met zowel het certificaatverzoek als de certificaatlading. Dit pakket is al versleuteld met materiaal dat vastzit in de Diffie-Hellman (DH) fase:

```
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)
```

Het vierde pakket wordt vanuit de responder naar de initiator verzonden en bevat alleen de certificaatlading:

```
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)
```

De hier beschreven stroom is gelijk aan de IKEv1-stroom. De responder moet de certificaataanvraag vooraf verzenden zonder kennis te hebben van het profiel dat moet worden gebruikt, hetgeen dezelfde problemen veroorzaakt die eerder zijn beschreven voor IKEv1 (vanuit protocolperspectief). Echter, de implementatie op IOS is beter voor IKEv2 dan voor IKEv1.

IKEv2 Verplicht vertrouwenspunt voor de initiatiefnemer

Hier is een voorbeeld van wanneer een IKEv2-initiator probeert een profiel te gebruiken met certificatie en geen vertrouwen-punt heeft dat onder dat profiel is ingesteld:

```
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
```

Het eerste pakket wordt verzonden zonder payload van een certificaat, zoals eerder beschreven. De reactie van de responder bevat de payload van het certificaat voor alle trust-punten die in de Global Configuration-modus zijn gedefinieerd. De initiatiefnemer ontvangt dit:

```
*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
```

De initiatiefnemer kent het trust-point niet dat moet worden gebruikt om te tekenen. Dit is het belangrijkste verschil wanneer de IKEv2-implementatie wordt vergeleken met de IKEv1. De IKEv2-initiator moet het trust-point hebben dat is ingesteld onder het IKEv2-initiatorprofiel, maar het is niet nodig voor de IKEv2-responder.

Hier is een fragment uit de opdrachtreferentie:

Als er geen betrouwbaarheidspunt is gedefinieerd in de IKEv2-profielconfiguratie, is de standaardinstelling om **het certificaat** te **valideren** met behulp van alle trustpoints die zijn gedefinieerd in de mondiale configuratie

Het is mogelijk verschillende "trust-points" te definiëren; één om te tekenen en een ander om te valideren. Helaas lost het verplichte trust-point dat onder het IKEv2-profiel is geconfigureerd niet alle problemen op.

R2 als IKEv2-initiator

In dit voorbeeld is R2 de IKEv2-initiator:

```
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
```

In dit voorbeeld is R1 de IKEv2-responder:

```
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
```

Hier, verstuurt R2 het eerste pakket zonder een certificaatverzoek. De responder reageert met een certificaataanvraag voor alle geconfigureerde trust-points. De volgorde van de lading is vergelijkbaar met de IKEv1 en is afhankelijk van de geïnstalleerde certificaten:

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

Het eerste geconfigureerde certificaat op R1 is gekoppeld aan het **TP2**-trust-punt, zodat de eerste certificatenaanvraag is voor de lading voor de CA die is gekoppeld aan het **TP2**-trust-punt. Zo selecteert R2 het voor authenticatie (eerste matrixregel):

```
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
```

Vervolgens bereidt R2 een antwoord (pakket 3) voor met de lading van de certificatieaanvraag die aan **TP2** is gekoppeld. R1 kan het certificaat niet vertrouwen omdat het is geconfigureerd voor validatie tegen het **TP1** trust-punt:

```
*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)
```

Zoals eerder vermeld, raadt Cisco u aan om geen meerdere trust-points onder één IKEv2-profiel te gebruiken. Wanneer je meerdere trust-points gebruikt, is het noodzakelijk om te verzekeren dat beide kanten exact dezelfde trust-points hebben. Bijvoorbeeld, zowel R1 als R2 hebben zowel TP1 als TP2 in hun profielen gevormd.

Samenvatting

Deze sectie verschaft een korte samenvatting van de informatie die in het document wordt beschreven.

De inhoud van de lading van het certificaat is afhankelijk van de configuratie. Als een specifiek trust-punt voor het ISAKMP-profiel is geconfigureerd en de router de ISAKMP-initiator is, dan bevat het certificaatverzoek in de MM3 alleen de CA die bij het trust-punt is gekoppeld. Als dezelfde router echter de ISAKMP-responder is, dan bevat het M4-pakket dat door de router wordt verzonden meerdere certificaten en aanvragen voor alle wereldwijd gedefinieerde trust-points (wanneer de opdracht **ca trust-point** niet in aanmerking wordt genomen). Dit gebeurt omdat de ISAKMP-responder het ISAKMP-profiel kan bepalen dat alleen gebruikt moet worden nadat de M5 en het certificaatverzoek dat in de MM4 is opgenomen, zijn ontvangen.

Het certificaat vraagt om lading in de MM3 en de MM4 is belangrijk vanwege de eerste wedstrijdregel. De eerste matchregel bepaalt het vertrouwenspunt dat wordt gebruikt voor de selectie van certificaten, wat nodig is voor de authenticatie in de MM5 en de MM6.

De volgorde van de lading van het certificaat is afhankelijk van de volgorde van de geïnstalleerde certificaten. De emittent van het eerste certificaat dat in de output van de opdracht **voor** het **certificaat van** het **cryptografische certificaat** verschijnt wordt eerst verstuurd. Dit eerste certificaat is het laatste dat is ingeschreven.

Het is mogelijk om meerdere trust-points te configureren voor een ISAKMP-profiel. Als dit wordt uitgevoerd, zijn alle vorige regels nog van toepassing.

Alle problemen en voorbehouden die in dit document worden beschreven, zijn het gevolg van het IKEv1-protocolontwerp. De fase van de echtheidscontrole vindt plaats in de MM5 en de MM6, terwijl de voorstellen voor de echtheidscontrole (certificaatverzoeken) in een vroeger stadium (vooraan) moeten worden verstuurd zonder kennis van het ISAKMP-profiel dat moet worden gebruikt. Dit is geen Cisco-specifiek probleem en heeft te maken met de beperkingen van het IKEv1-protocolontwerp.

Het IKEv2-protocol is vergelijkbaar met de IKEv1 wat betreft het onderhandelingsproces voor certificaten. Echter, de implementatie op het IOS dwingt het gebruik van specifieke trust-points voor de initiatiefnemer. Dit lost niet alle problemen op. Wanneer meerdere trust-points voor één profiel zijn geconfigureerd en één enkel trust-point aan de andere kant is geconfigureerd, is het nog mogelijk om problemen met authenticatie te krijgen. Cisco raadt u aan om symmetrische trust-point configuraties te gebruiken voor beide kanten van de verbinding (de zelfde trust-points die voor beide IKEv2 profielen zijn gevormd).

Hier volgen een paar belangrijke opmerkingen over de informatie die in dit document wordt beschreven:

- Met asymmetrische trust-point configuraties voor de IKEv1 profielen van peers zou de tunnel van slechts één kant van de tunnel kunnen beginnen. De configuratie van het vertrouwen-punt voor het IKEv1-profiel is optioneel.

- Met asymmetrische trust-point configuraties voor de IKEv2 profielen van peers, zou de tunnel van slechts één kant van de tunnel kunnen beginnen. De configuratie van het trust-punt voor het IKEv2-profiel is verplicht voor de initiator.

- De opdracht voor het betalen van het certificaat is afhankelijk van de volgorde van de certificaten die worden weergegeven in de uitvoer van de opdracht **voor** het **certificaat van** het **cryptografiecertificaat** (eerste match).

- De certificaataanvraag voor de lading bepaalt het certificaat dat door de responder wordt geselecteerd (eerste match).

- Wanneer u meerdere profielen gebruikt voor de IKEv1 en de IKEv2 en dezelfde matrixidentiteitsregels hebt ingesteld, is het moeilijk om de resultaten te voorspellen (te veel factoren zijn betrokken).

- Cisco raadt aan om symmetrische trust-point configuraties te gebruiken voor zowel IKEv1 als IKEv2.

Gerelateerde informatie

- Configuratie-gids voor IPsec VPN's, Cisco IOS release 15M&T - certificaataanvraag voor ISAKMP-profiel en -toewijzing
- Cisco IOS security opdracht: Opdracht A tot c - ca trust point door duidelijke e
- Technische ondersteuning en documentatie – Cisco Systems