

IOS IKEv1/IKEv2-selectieregels voor sleutelementen en profielen - Handleiding voor probleemoplossing

Inhoud

[Inleiding](#)

[Configuratie](#)

[Topologie](#)

[R1-netwerk en VPN](#)

[R2-netwerk en VPN](#)

[Bijvoorbeeld scenario's](#)

[R1 als IKE-initiator \(corrigeren\)](#)

[R2 als IKE-initiator \(onjuist\)](#)

[Debugs voor verschillende voorgedeelde sleutel](#)

[Selectiecriteria voor sleutelementen](#)

[Selectieknop voor IKE-initiator selecteren](#)

[Selectievolgorde op IKE-responder - verschillende IP-adressen](#)

[Selectieknop voor IKE-transponder - Dezelfde IP-adressen](#)

[Mondiale configuratie trainen](#)

[Toetsing op IKEv2 - probleem doet zich niet voor](#)

[Selectiecriteria voor IKE-profiel](#)

[IKE-profiel, selectievolgorde op IKE-initiator](#)

[IKE-profiel, selectievolgorde op IKE-responder](#)

[Samenvatting](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het gebruik van meerdere toetsenborden voor meerdere profielen van Internet Security Association en Key Management Protocol (ISAKMP) in een VPN-scenario van Cisco IOS LAN-to-LAN. Het bestrijkt het gedrag van Cisco IOS-software release 15.3T evenals mogelijke problemen wanneer meerdere zoekringen worden gebruikt.

Er worden twee scenario's gepresenteerd, gebaseerd op een VPN-tunnel met twee ISAKMP-profielen op elke router. Elk profiel heeft een andere toets met hetzelfde IP-adres als bijlage. De scenario's tonen aan dat de VPN-tunnel slechts van één kant van de verbinding kan worden geïnitieerd vanwege profielselectie en verificatie.

In de volgende delen van het document worden de selectiecriteria voor het sleutelprofiel voor zowel de IKE-initiator (Internet Key Exchange) als de IKE-responder samengevat. Wanneer de verschillende IP adressen door de toetsencombinatie op de IKE-responder worden gebruikt, werkt de configuratie correct, maar het gebruik van hetzelfde IP-adres maakt het probleem aan dat in het eerste scenario wordt gepresenteerd.

De volgende secties verklaren waarom de aanwezigheid van zowel een standaard sleutelring (mondiale configuratie) als specifieke sleutelringen tot problemen zou kunnen leiden en waarom het gebruik van het Internet Key Exchange Protocol, versie 2 (IKEv2), dat probleem vermijdt.

In de laatste secties worden de selectiecriteria voor het IKE-profiel weergegeven voor zowel IKE-initiator als responder, samen met de typische fouten die optreden wanneer een onjuist profiel is geselecteerd.

Configuratie

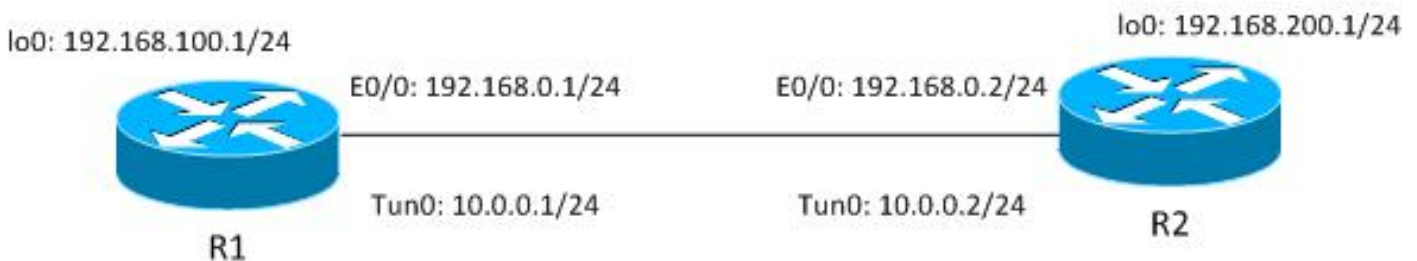
Opmerkingen:

De [Cisco CLI Analyzer](#) (alleen geregistreerde klanten) ondersteunt bepaalde **show**-opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van de opdrachtoutput te bekijken.

Raadpleeg [Important Information on Debug Commands \(Belangrijke informatie over opdrachten met debug\)](#) voordat u opdrachten met **debug** opgeeft.

Topologie

Router1 (R1) en Router2 (R2) gebruiken Virtual Tunnel Interface (VTI) (Generic Routing Encapsulation [GRE]) om toegang te hebben tot zijn loopback-ups. Dat VTI wordt beschermd door Internet Protocol Security (IPSec).



Zowel R1 als R2 hebben twee ISAKMP-profielen, elk met verschillende toetsenborden. Alle sleutelringen hebben hetzelfde wachtwoord.

R1-netwerk en VPN

De configuratie voor het R1-netwerk en VPN is:

```
crypto keyring keyring1
pre-shared-key address 192.168.0.2 key cisco
crypto keyring keyring2
pre-shared-key address 192.168.0.2 key cisco
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
```

```

crypto isakmp profile profile1
  keyring keyring1
  match identity address 192.168.0.102 255.255.255.255 !non existing host
crypto isakmp profile profile2
  keyring keyring2
  match identity address 192.168.0.2 255.255.255.255 !R2
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
mode tunnel
!
crypto ipsec profile profile1
set transform-set TS
set isakmp-profile profile2
!
interface Loopback0
description Simulate LAN
ip address 192.168.100.1 255.255.255.0
!
interface Tunnell
ip address 10.0.0.1 255.255.255.0
tunnel source Ethernet0/0
tunnel destination 192.168.0.2
tunnel protection ipsec profile profile1
!
interface Ethernet0/0
ip address 192.168.0.1 255.255.255.

ip route 192.168.200.0 255.255.255.0 10.0.0.2

```

R2-netwerk en VPN

De configuratie voor het R2-netwerk en VPN is:

```

crypto keyring keyring1
pre-shared-key address 192.168.0.1 key cisco
crypto keyring keyring2
pre-shared-key address 192.168.0.1 key cisco
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2

crypto isakmp profile profile1
  keyring keyring1
  match identity address 192.168.0.1 255.255.255.255 !R1
crypto isakmp profile profile2
  keyring keyring2
  match identity address 192.168.0.100 255.255.255.255 !non existing host
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
mode tunnel
!
crypto ipsec profile profile1
set transform-set TS
set isakmp-profile profile1
!
interface Loopback0
ip address 192.168.200.1 255.255.255.0
!
interface Tunnell

```

```
ip address 10.0.0.2 255.255.255.0
tunnel source Ethernet0/0
tunnel destination 192.168.0.1
tunnel protection ipsec profile profile1
!
interface Ethernet0/0
 ip address 192.168.0.2 255.255.255.0

ip route 192.168.100.0 255.255.255.0 10.0.0.1
```

Alle toetsen gebruiken hetzelfde IP-adres en gebruiken het wachtwoord" cisco."

Op R1 wordt profile2 gebruikt voor de VPN-verbinding. Profile2 is het tweede profiel in de configuratie, die de tweede sleutel in de configuratie gebruikt. Zoals u zult zien, is de sleutelvolgorde cruciaal.

Bijvoorbeeld scenario's

In het eerste scenario is R1 de ISAKMP-initiator. De tunnel onderhandelt correct en het verkeer wordt beschermd zoals verwacht.

Het tweede scenario gebruikt dezelfde topologie, maar heeft R2 als de initiator van ISAKMP wanneer fase1 onderhandeling faalt.

Internet Key Exchange versie 1 (IKEv1) heeft een vooraf gedeelde sleutel nodig voor de berekening van de sleutel, die wordt gebruikt om het pakket met de hoofdmodus 5 (M5) en de volgende IKEv1-pakketten te decrypteren/versleutelen. De key is afgeleid van de Diffie-Hellman (DH)-berekening en de pre-gedeelde toets. Deze vooraf gedeelde toets moet worden bepaald nadat MM3 (responder) of M4 (initiator) is ontvangen, zodat de toets, die wordt gebruikt in MM5/MM6, kan worden berekend.

Voor de ISAKMP-responder in M3 is het specifieke ISAKMP-profiel nog niet bepaald, omdat dat gebeurt nadat de IKEID in MM5 is ontvangen. In plaats daarvan worden alle sleutelringen doorzocht naar een vooraf gedeelde sleutel en wordt de eerste of best matchende sleutelring uit de mondiale configuratie geselecteerd. Deze sleutelring wordt gebruikt om de sleutel te berekenen die wordt gebruikt voor de decryptie van MM5 en voor de encryptie van MM6. Na de decryptie van MM5 en na de bepaling van het ISAKMP-profiel en de bijbehorende sleutelring, voert de ISAKMP-responder verificatie uit indien dezelfde sleutelring is geselecteerd; als dezelfde toets niet is geselecteerd, wordt de verbinding verbroken.

Voor de ISAKMP-responder zou u dus, indien mogelijk, één enkele sleutelring met meerdere ingangen moeten gebruiken.

R1 als IKE-initiator (corrigeren)

Dit scenario beschrijft wat er gebeurt wanneer R1 de IKE-initiator is:

1. Gebruik deze debugs voor zowel R1 als R2:

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

2. R1 initieert de tunnel, stuurt het pakket MM1 met beleidsvoorstellen, en ontvangt MM2 in

antwoord. MM3 wordt vervolgens bereid:

```
R1#ping 192.168.200.1 source lo0 repeat 1
```

```
Type escape sequence to abort.
```

```
Sending 1, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.100.1
```

```
*Jun 19 10:04:24.826: IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 192.168.0.1:500, remote= 192.168.0.2:500,
  local_proxy= 192.168.0.1/255.255.255.255/47/0,
  remote_proxy= 192.168.0.2/255.255.255.255/47/0,
  protocol= ESP, transform= esp-aes esp-sha256-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Jun 19 10:04:24.826: ISAKMP:(0): SA request profile is profile2
*Jun 19 10:04:24.826: ISAKMP: Found a peer struct for 192.168.0.2, peer
port 500
*Jun 19 10:04:24.826: ISAKMP: Locking peer struct 0xF483A970, refcount 1
for isakmp_initiator
*Jun 19 10:04:24.826: ISAKMP: local port 500, remote port 500
*Jun 19 10:04:24.826: ISAKMP: set new node 0 to QM_IDLE
*Jun 19 10:04:24.826: ISAKMP:(0):insert sa successfully sa = F474C2E8
*Jun 19 10:04:24.826: ISAKMP:(0):Can not start Aggressive mode, trying
Main mode.
*Jun 19 10:04:24.826: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-03 ID
*Jun 19 10:04:24.826: ISAKMP:(0): constructed NAT-T vendor-02 ID
*Jun 19 10:04:24.826: ISAKMP:(0):Input = IKE_MSG_FROM_IPSEC,
IKE_SA_REQ_MM
*Jun 19 10:04:24.826: ISAKMP:(0):Old State = IKE_READY New State =
IKE_I_MM1

*Jun 19 10:04:24.826: ISAKMP:(0): beginning Main Mode exchange
*Jun 19 10:04:24.826: ISAKMP:(0): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_NO_STATE
*Jun 19 10:04:24.826: ISAKMP:(0):Sending an IKE IPv4 Packet.
*Jun 19 10:04:24.827: ISAKMP (0): received packet from 192.168.0.2 dport
500 sport 500 Global (I) MM_NO_STATE
*Jun 19 10:04:24.827: ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.827: ISAKMP:(0):Old State = IKE_I_MM1 New State =
IKE_I_MM2

*Jun 19 10:04:24.827: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.827: ISAKMP:(0): local preshared key found
*Jun 19 10:04:24.827: ISAKMP : Looking for xauth in profile profile2
*Jun 19 10:04:24.827: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 10:04:24.827: ISAKMP:      encryption 3DES-CBC
*Jun 19 10:04:24.827: ISAKMP:      hash MD5
*Jun 19 10:04:24.827: ISAKMP:      default group 2
*Jun 19 10:04:24.827: ISAKMP:      auth pre-share
*Jun 19 10:04:24.827: ISAKMP:      life type in seconds
*Jun 19 10:04:24.827: ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
*Jun 19 10:04:24.827: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:actual life: 0
```

```

*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 10:04:24.827: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 10:04:24.827: ISAKMP:(0)::Started lifetime timer: 86400.

*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.827: ISAKMP:(0):Old State = IKE_I_MM2 New State =
IKE_I_MM2

*Jun 19 10:04:24.828: ISAKMP:(0): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_SA_SETUP

```

Vanaf het begin weet R1 dat ISAKMP profile2 gebruikt zou moeten worden omdat het gebonden is aan het IPsec profiel dat gebruikt wordt voor dat VTI.

Zodoende is de juiste sleutelring (sleutelring2) geselecteerd. De vooraf gedeelde sleutel van keyring2 wordt gebruikt als sluitmateriaal voor DH berekeningen wanneer het MM3 pakket wordt voorbereid.

3. Wanneer R2 dat M3-pakket ontvangt, weet het nog steeds niet welk ISAKMP-profiel moet worden gebruikt, maar heeft het een vooraf gedeelde sleutel nodig voor de DH-generatie. Dat is de reden dat R2 alle sleutelringen doorzoekt om de vooraf gedeelde sleutel voor die peer te vinden:

```

*Jun 19 10:04:24.828: ISAKMP (0): received packet from 192.168.0.1 dport
500 sport 500 Global (R) MM_SA_SETUP
*Jun 19 10:04:24.828: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.828: ISAKMP:(0):Old State = IKE_R_MM2 New State =
IKE_R_MM3

*Jun 19 10:04:24.828: ISAKMP:(0): processing KE payload. message ID = 0
*Jun 19 10:04:24.831: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun 19 10:04:24.831: ISAKMP:(0):found peer pre-shared key matching
192.168.0.1

```

De toets voor 192.168.0.1 is gevonden in de eerste gedefinieerde sleutelring (sleutelring1).

4. R2 bereidt vervolgens het M4-pakket voor met DH-berekeningen en met de 'cisco'-toets vanaf sleutelring1:

```

*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID is DPD
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): speaking to another IOS box!
*Jun 19 10:04:24.831: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID seems Unity/DPD but major
32 mismatch
*Jun 19 10:04:24.831: ISAKMP:(1011): vendor ID is XAUTH
*Jun 19 10:04:24.831: ISAKMP:received payload type 20
*Jun 19 10:04:24.831: ISAKMP (1011): His hash no match - this node
outside NAT

```

```

*Jun 19 10:04:24.831: ISAKMP:received payload type 20
*Jun 19 10:04:24.831: ISAKMP (1011): No NAT Found for self or peer
*Jun 19 10:04:24.831: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.831: ISAKMP:(1011):Old State = IKE_R_MM3 New State =
IKE_R_MM3

*Jun 19 10:04:24.831: ISAKMP:(1011): sending packet to 192.168.0.1 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Jun 19 10:04:24.831: ISAKMP:(1011):Sending an IKE IPv4 Packet.

```

5. Wanneer R1 MM4 ontvangt, bereidt zij het MM5-pakket voor met IKEID en de juiste eerder geselecteerde toets (vanaf sleutelring2):

```

*Jun 19 10:04:24.831: ISAKMP (0): received packet from 192.168.0.2 dport
500 sport 500 Global (I) MM_SA_SETUP
*Jun 19 10:04:24.831: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.831: ISAKMP:(0):Old State = IKE_I_MM3 New State =
IKE_I_MM4

*Jun 19 10:04:24.831: ISAKMP:(0): processing KE payload. message ID = 0
*Jun 19 10:04:24.837: ISAKMP:(0): processing NONCE payload. message ID = 0
*Jun 19 10:04:24.837: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): vendor ID is Unity
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): vendor ID is DPD
*Jun 19 10:04:24.837: ISAKMP:(1011): processing vendor id payload
*Jun 19 10:04:24.837: ISAKMP:(1011): speaking to another IOS box!
*Jun 19 10:04:24.837: ISAKMP:received payload type 20
*Jun 19 10:04:24.838: ISAKMP (1011): His hash no match - this node
outside NAT
*Jun 19 10:04:24.838: ISAKMP:received payload type 20
*Jun 19 10:04:24.838: ISAKMP (1011): No NAT Found for self or peer
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_I_MM4 New State =
IKE_I_MM4

*Jun 19 10:04:24.838: ISAKMP:(1011):Send initial contact
*Jun 19 10:04:24.838: ISAKMP:(1011):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.1
    protocol      : 17
    port          : 500
    length        : 12
*Jun 19 10:04:24.838: ISAKMP:(1011):Total payload length: 12
*Jun 19 10:04:24.838: ISAKMP:(1011): sending packet to 192.168.0.2 my_port
500 peer_port 500 (I) MM_KEY_EXCH

```

6. Het MM5-pakket, dat de IKEID van 192.168.0.1 bevat, wordt ontvangen door R2. Op dit moment weet R2 aan welk ISAKMP-profiel het verkeer moet worden gebonden (de match-id adressopdracht):

```

*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.1 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_R_MM4 New State =

```

IKE_R_MM5

```
*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.1
    protocol      : 17
    port          : 500
    length        : 12
*Jun 19 10:04:24.838: ISAKMP:(0):: peer matches profile1 profile
*Jun 19 10:04:24.838: ISAKMP:(1011):Found ADDRESS key in keyring keyring1
*Jun 19 10:04:24.838: ISAKMP:(1011): processing HASH payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP:(1011): processing NOTIFY INITIAL_CONTACT
protocol 1
    spi 0, message ID = 0, sa = 0xF46295E8
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
    authenticated
*Jun 19 10:04:24.838: ISAKMP:(1011):SA has been authenticated with
192.168.0.1
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
    authenticated
```

7. R2 voert nu verificatie uit als de sleutelring die blind geselecteerd was voor het M4-pakket, dezelfde is als de sleutelring die nu voor het ISAKMP-profiel is geselecteerd. Omdat keyring1 de eerste in de configuratie is, werd het eerder geselecteerd, en nu wordt het geselecteerd. De validatie is succesvol, en het MM6 pakket kan worden verzonden:

```
*Jun 19 10:04:24.838: ISAKMP:(1011):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.2
    protocol      : 17
    port          : 500
    length        : 12
*Jun 19 10:04:24.838: ISAKMP:(1011):Total payload length: 12
*Jun 19 10:04:24.838: ISAKMP:(1011): sending packet to 192.168.0.1
my_port 500 peer_port 500 (R) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011):Sending an IKE IPv4 Packet.
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 19 10:04:24.838: ISAKMP:(1011):Old State = IKE_R_MM5 New State =
IKE_P1_COMPLETE
```

8. R1 ontvangt MM6 en hoeft geen verificatie van de sleutelring uit te voeren omdat deze vanaf het eerste pakket bekend was; de initiatiefnemer weet altijd welk ISAKMP-profiel moet worden gebruikt en welke sleutelring bij dat profiel is gekoppeld. De authenticatie is succesvol en fase1 voltooit correct:

```
*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.2
dport 500 sport 500 Global (I) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.2
    protocol      : 17
    port          : 500
```



```

length      : 12
*Jun 19 10:04:24.838: ISAKMP:(1011): processing HASH payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP:(1011):SA authentication status:
authenticated
*Jun 19 10:04:24.838: ISAKMP:(1011):SA has been authenticated with
192.168.0.2
*Jun 19 10:04:24.838: ISAKMP AAA: Accounting is not enabled
*Jun 19 10:04:24.838: ISAKMP:(1011):Input = IKE_MSG_FROM_PEER,
IKE_MM_EXCH
*Jun 19 10:04:24.839: ISAKMP:(1011):Old State = IKE_I_MM5 New State =
IKE_I_MM6

*Jun 19 10:04:24.839: ISAKMP:(1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 10:04:24.839: ISAKMP:(1011):Old State = IKE_I_MM6 New State =
IKE_I_MM6

*Jun 19 10:04:24.843: ISAKMP:(1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Jun 19 10:04:24.843: ISAKMP:(1011):Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE

*Jun 19 10:04:24.843: ISAKMP:(1011):beginning Quick Mode exchange, M-ID
of 2816227709

```

9. Fase2 start normaal en is succesvol voltooid.

Dit scenario werkt correct alleen vanwege de juiste volgorde van de toetsen die op R2 zijn gedefinieerd. Het profiel dat voor de VPN-sessie zou moeten worden gebruikt, gebruikt de toetsencombinatie die voor het eerst in de configuratie was.

R2 als IKE-initiator (onjuist)

Dit scenario beschrijft wat er gebeurt wanneer R2 dezelfde tunnel initieert en verklaart waarom de tunnel niet zal worden opgezet. Sommige stammen zijn verwijderd om zich te concentreren op de verschillen tussen dit en het vorige voorbeeld:

1. R2 initieert de tunnel:

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

2. Aangezien R2 de initiator is, zijn het ISAKMP-profiel en de sleutelring bekend. De vooraf gedeelde sleutel van keyring1 wordt gebruikt voor DH berekeningen en wordt verzonden in MM3. R2 ontvangt MM2 en bereidt MM3 voor op basis van die sleutel:

```

*Jun 19 12:28:44.256: ISAKMP (0): received packet from 192.168.0.1 dport
500 sport 500 Global (I) MM_NO_STATE
*Jun 19 12:28:44.256: ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Jun 19 12:28:44.256: ISAKMP:(0):Old State = IKE_I_MM1 New State =
IKE_I_MM2

*Jun 19 12:28:44.256: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 12:28:44.256: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.256: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.256: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.256: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.256: ISAKMP:(0): local preshared key found

```

```

*Jun 19 12:28:44.256: ISAKMP : Looking for xauth in profile profile1
*Jun 19 12:28:44.256: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 12:28:44.256: ISAKMP:      encryption 3DES-CBC
*Jun 19 12:28:44.256: ISAKMP:      hash MD5
*Jun 19 12:28:44.256: ISAKMP:      default group 2
*Jun 19 12:28:44.256: ISAKMP:      auth pre-share
*Jun 19 12:28:44.256: ISAKMP:      life type in seconds
*Jun 19 12:28:44.256: ISAKMP:      life duration (VPI) of  0x0 0x1
0x51 0x80
*Jun 19 12:28:44.256: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 12:28:44.256: ISAKMP:(0):Acceptable atts:actual life: 0
*Jun 19 12:28:44.257: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 12:28:44.257: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 12:28:44.257: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 12:28:44.257: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 12:28:44.257: ISAKMP:(0)::Started lifetime timer: 86400.

*Jun 19 12:28:44.257: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.257: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.257: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.257: ISAKMP:(0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.257: ISAKMP:(0):Old State = IKE_I_MM2  New State =
IKE_I_MM2

*Jun 19 12:28:44.257: ISAKMP:(0): sending packet to 192.168.0.1 my_port
500 peer_port 500 (I) MM_SA_SETUP

```

3. R1 ontvangt MM3 van R2. In dit stadium weet R1 niet welk ISAKMP-profiel moet worden gebruikt, zodat het niet weet welke sleutelring moet worden gebruikt. R1 gebruikt dus de eerste sleutel van de mondiale configuratie, die toetsenbord 1 is. R1 gebruikt die vooraf gedeelde toets voor DH-berekeningen en verstuurt MM4:

```

*Jun 19 12:28:44.263: ISAKMP:(0):found peer pre-shared key matching
192.168.0.2
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID is DPD
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): speaking to another IOS box!
*Jun 19 12:28:44.263: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID seems Unity/DPD but major
151 mismatch
*Jun 19 12:28:44.263: ISAKMP:(1012): vendor ID is XAUTH
*Jun 19 12:28:44.263: ISAKMP:received payload type 20
*Jun 19 12:28:44.263: ISAKMP (1012): His hash no match - this node
outside NAT
*Jun 19 12:28:44.263: ISAKMP:received payload type 20
*Jun 19 12:28:44.263: ISAKMP (1012): No NAT Found for self or peer
*Jun 19 12:28:44.263: ISAKMP:(1012):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.263: ISAKMP:(1012):Old State = IKE_R_MM3  New State =
IKE_R_MM3
*Jun 19 12:28:44.263: ISAKMP:(1012): sending packet to 192.168.0.2 my_port
500 peer_port 500 (R) MM_KEY_EXC

```

4. R2 ontvangt M4 van R1, gebruikt de vooraf gedeelde sleutel van sleutelring1 om DH te berekenen en bereidt het MM5-pakket en het IKEID voor:

```

*Jun 19 12:28:44.269: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is Unity
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is DPD
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): speaking to another IOS box!
*Jun 19 12:28:44.269: ISAKMP:received payload type 20
*Jun 19 12:28:44.269: ISAKMP (1012): His hash no match - this node
outside NAT
*Jun 19 12:28:44.269: ISAKMP:received payload type 20
*Jun 19 12:28:44.269: ISAKMP (1012): No NAT Found for self or peer
*Jun 19 12:28:44.269: ISAKMP:(1012):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Jun 19 12:28:44.269: ISAKMP:(1012):Old State = IKE_I_MM4 New State =
IKE_I_MM4

*Jun 19 12:28:44.270: ISAKMP:(1012):SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
*Jun 19 12:28:44.270: ISAKMP (1012): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.2
    protocol      : 17
    port          : 500
    length        : 12
*Jun 19 12:28:44.270: ISAKMP:(1012):Total payload length: 12
*Jun 19 12:28:44.270: ISAKMP:(1012): sending packet to 192.168.0.1
my_port 500 peer_port 500 (I) MM_KEY_EXCH

```

5. R1 ontvangt M5 van R1. Omdat het IKEID gelijk is aan 192.168.0, is profile2 geselecteerd. Keyring2 is ingesteld in profile2 zodat keyring2 wordt geselecteerd. Eerder, voor de DH-berekening in M4, geselecteerde R1 de eerste geconfigureerde sleutelring, die sleutelring1 was. Hoewel de wachtwoorden precies hetzelfde zijn, faalt de validatie voor de sleutelring omdat dit verschillende sleutelobjecten zijn:

```

*Jun 19 12:28:44.270: ISAKMP (1012): received packet from 192.168.0.2
dport 500 sport 500 Global (R) MM_KEY_EXCH
*Jun 19 12:28:44.270: ISAKMP:(1012):Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
*Jun 19 12:28:44.270: ISAKMP:(1012):Old State = IKE_R_MM4 New State =
IKE_R_MM5

*Jun 19 12:28:44.270: ISAKMP:(1012): processing ID payload. message ID = 0
*Jun 19 12:28:44.270: ISAKMP (1012): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.2
    protocol      : 17
    port          : 500
    length        : 12
*Jun 19 12:28:44.270: ISAKMP:(0):: peer matches profile2 profile
*Jun 19 12:28:44.270: ISAKMP:(1012):Found ADDRESS key in keyring keyring2
*Jun 19 12:28:44.270: ISAKMP:(1012):Key not found in keyrings of profile ,
aborting exchange
*Jun 19 12:28:44.270: ISAKMP (1012): FSM action returned error: 2

```

Debugs voor verschillende voorgedeelde sleutel

De vorige scenario's gebruikten dezelfde toets ('cisco'). Dus zelfs wanneer de onjuiste sleutelring

werd gebruikt, kon het MM5 pakket correct worden gedecrypteerd en later wegens het falen van de sleutelvalidatie worden gedropt.

In scenario's waar verschillende keys worden gebruikt, kan MM5 niet worden gedecrypteerd, en deze foutmelding verschijnt:

```
*Jul 16 20:21:25.317: ISAKMP (1004): received packet from 192.168.0.2 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Jul 16 20:21:25.317: ISAKMP: reserved not zero on ID payload!
*Jul 16 20:21:25.317: %CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.168.0.2
failed its sanity check or is malformed
```

Selectiecriteria voor sleutelementen

Dit is een samenvatting van de selectiecriteria voor sleutelementen. Zie de volgende secties voor meer informatie.

	Initiator	weerleggen
Meervoudige toetsenborden met verschillende IP-adressen	Standaard ingesteld. Indien niet expliciet het meest specifieke ingesteld vanaf de configuratie	De meest specifieke match
Meervoudige toetsen met dezelfde IP-adressen	Standaard ingesteld. Indien niet expliciet ingesteld configuratie wordt onvoorspelbaar en wordt niet ondersteund. Je moet geen twee toetsen instellen voor hetzelfde IP-adres.	De configuratie wordt onvoorspelbaar en wordt niet ondersteund. Je moet geen twee toetsen instellen voor hetzelfde IP-adres.

In dit gedeelte wordt ook beschreven waarom de aanwezigheid van zowel een standaardtoetsencombinatie (mondiale configuratie) als specifieke sleutelringen tot problemen kan leiden en waarom het gebruik van het IKEv2-protocol dergelijke problemen vermijdt.

Selectieknop voor IKE-initiator selecteren

Voor configuratie met een VTI, gebruikt de initiator een specifieke tunnelinterface die op specifiek IPSec profiel wijst. Omdat het IPSec-profiel een specifiek IKE-profiel met een specifieke sleutel gebruikt, is er geen verwarring over welke sleutel te gebruiken.

Crypto-map, die ook wijst op een specifiek IKE-profiel met een specifieke sleutelring, functioneert op dezelfde manier.

Het is echter niet altijd mogelijk om uit de configuratie te bepalen welke toetsencombinatie moet worden gebruikt. Dit gebeurt bijvoorbeeld wanneer er geen IKE-profiel is geconfigureerd - dat wil zeggen dat het IPSec-profiel niet is ingesteld om IKE-profiel te gebruiken:

```
crypto keyring keyring1
  pre-shared-key address 192.168.0.0 255.255.255.0 key cisco
crypto keyring keyring2
  pre-shared-key address 192.168.0.2 key cisco

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
  mode tunnel

crypto ipsec profile profile1
```

```
set transform-set TS

interface Tunnell
 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
```

Als deze IKE-initiator MM1 probeert te verzenden, kiest u de meest specifieke sleutelring:

```
*Oct 7 08:13:58.413: ISAKMP: Locking peer struct 0xF4803B88, refcount 1 for
isakmp_initiator
*Oct 7 08:13:58.413: ISAKMP:(0):Can not start Aggressive mode, trying Main mode.
*Oct 7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 not available in default
*Oct 7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 found in keyring1
*Oct 7 08:13:58.413: ISAKMP:(0):ISAKMP: Selecting 192.168.0.0,255.255.255.0
as key
*Oct 7 08:13:58.413: ISAKMP:(0):key for 192.168.0.2 found in keyring2
*Oct 7 08:13:58.413: ISAKMP:(0):ISAKMP: Selecting 192.168.0.2,255.255.255.255
as final key
*Oct 7 08:13:58.413: ISAKMP:(0):found peer pre-shared key matching 192.168.0.2
```

Aangezien de initiatiefnemer geen IKE-profielen heeft die worden geconfigureerd wanneer hij MM6 ontvangt, wordt het profiel niet geraakt en zal het volledig zijn met succesvolle verificatie en Quick Mode (QM):

```
Oct 7 08:13:58.428: ISAKMP:(0):: peer matches *none* of the profiles
*Oct 7 08:13:58.428: ISAKMP:(1005): processing HASH payload. message ID = 0
*Oct 7 08:13:58.428: ISAKMP:(1005):SA authentication status:
authenticated
*Oct 7 08:13:58.432: ISAKMP:(1005):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
```

Selectievolgorde op IKE-responder - verschillende IP-adressen

Het probleem met de selectieknop is te vinden op de responder. Wanneer toetsen verschillende IP-adressen gebruiken, is de selectieregel eenvoudig.

Denk dat de IKE-responder deze configuratie heeft:

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.0.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco2
```

Wanneer deze responder het M1-pakket van de IKE-initiator met IP-adres 192.168.0.2 ontvangt, kiest zij de beste (meest specifieke) match, zelfs als de volgorde in de configuratie anders is.

De selectiecriteria zijn:

1. Alleen toetsen met een IP-adres worden in aanmerking genomen.
2. De virtuele routing en Forwarding (VRF) van het inkomende pakket wordt gecontroleerd (voorkant VRF [fVRF]).
3. Als het pakje in het standaard VRF staat, wordt eerst de algemene toets ingeschakeld. De meest nauwkeurige toets (netmask lengte) wordt geselecteerd.
4. Als geen sleutel in de standaardtoetsencombinatie wordt gevonden, worden alle sleutelringen die deze fVRF aanpassen aaneengezet.

5. De meest nauwkeurige toets (langste netmask) is gelijk. Bijvoorbeeld, a /32 wordt preferred boven a/24.

De knoppen bevestigen de selectie:

```
R1#debug crypto isakmp detail
```

```
Crypto ISAKMP internals debugging is on
```

```
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 not available in default
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 found in keyring1
*Oct  2 11:57:13.301: ISAKMP:(0):ISAKMP: Selecting 192.168.0.0,255.255.255.0
as key
*Oct  2 11:57:13.301: ISAKMP:(0):key for 192.168.0.2 found in keyring2
*Oct  2 11:57:13.301: ISAKMP:(0):ISAKMP: Selecting 192.168.0.2,255.255.255.255
as final key
```

Selectieknop voor IKE-transponder - Dezelfde IP-adressen

Wanneer de sleutelringen de zelfde IP adressen gebruiken, komen er problemen voor. Denk dat de IKE-responder deze configuratie heeft:

```
crypto keyring keyring1
pre-shared-key address 192.168.0.2 key cisco
crypto keyring keyring2
pre-shared-key address 192.168.0.2 key cisco
```

Deze configuratie wordt onvoorspelbaar en wordt niet ondersteund. Men zou geen twee toetsen moeten configureren voor hetzelfde IP-adres of het probleem dat in [R2](#) wordt beschreven [als IKE-initiator \(onjuist\)](#) zal optreden.

Mondiale configuratie trainen

De ISAKMP-toetsen die in de wereldwijde configuratie zijn gedefinieerd, behoren tot de standaardtoetsencombinatie:

```
crypto keyring keyring1
pre-shared-key address 192.168.0.0 255.255.0.0 key cisco
crypto keyring keyring2
pre-shared-key address 192.168.0.2 key cisco2
crypto isakmp key cisco3 address 0.0.0.0
```

Hoewel de ISAKMP-toets de laatste is in de configuratie, wordt deze als eerste verwerkt op de IKE-responder:

```
R1#show crypto isakmp key
```

Keyring	Hostname/Address	Preshared Key
default	0.0.0.0 [0.0.0.0]	cisco3
keyring1	192.168.0.0 [255.255.0.0]	cisco
keyring2	192.168.0.2	cisco2

Het gebruik van zowel mondiale als specifieke sleutelringen is dus zeer riskant en kan tot problemen leiden.

Toetsing op IKEv2 - probleem doet zich niet voor

Hoewel het IKEv2-protocol soortgelijke concepten gebruikt als IKEv1, veroorzaakt selectieknop geen vergelijkbare problemen.

In eenvoudige gevallen worden slechts vier pakketten uitgewisseld. Het IKEID dat bepaalt welk IKEv2-profiel op de responder moet worden geselecteerd, wordt door de initiator in het derde pakket verzonden. Het derde pakket is al versleuteld.

Het grootste verschil in de twee protocollen is dat IKEv2 alleen het DH resultaat gebruikt voor de berekening van een sleutel. De vooraf gedeelde sleutel is niet langer nodig om de sleutel te berekenen die gebruikt wordt voor encryptie/decryptie.

De [IKEv2 RFC \(5996, paragraaf 2.14\)](#) stelt:

De gedeelde toetsen worden als volgt berekend. Een hoeveelheid die SKEYSEED wordt genoemd, wordt berekend aan de hand van de tijdens de IKE_SA_INIT uitwisseling uitgewisselde nonces en het gedeelde geheim Diffie-Hellman dat tijdens die uitwisseling werd vastgesteld.

In dezelfde sectie merkt de RFC ook op:

$$\text{SKEYSEED} = \text{prf}(\text{Ni} \parallel \text{Nr}, g^{ir})$$

Alle benodigde informatie wordt in de eerste twee pakketten verzonden en er hoeft geen vooraf gedeelde sleutel te worden gebruikt wanneer SKEYSEED wordt berekend.

Vergelijk dit met de [IKE RFC \(2409, paragraaf 3.2\)](#), waarin staat:

SKEYID is een string afgeleid van geheim materiaal dat alleen bekend is bij de actieve spelers in de ruil.

Dat "geheime materiaal dat alleen bekend is bij de actieve spelers" is de pre-gedeelde sleutel. In paragraaf 5 merkt de RFC ook op:

Voor vooraf gedeelde toetsen: $\text{SKEYID} = \text{prf}(\text{voorgedeeld-key}, \text{Ni}_b \parallel \text{Nr}_b)$

Dit verklaart waarom het IKEv1-ontwerp voor vooraf gedeelde sleutels zo veel problemen veroorzaakt. Deze problemen bestaan niet in IKEv1 wanneer certificaten worden gebruikt voor echtheidscontrole.

Selectiecriteria voor IKE-profiel

Dit is een samenvatting van de selectiecriteria voor IKE-profiel. Zie de volgende secties voor meer informatie.

	Initiator	weerleggen
Profielselectie	Het moet worden ingesteld (in IPSec-profiel of in crypto-kaart). Indien niet ingesteld, eerste match uit de configuratie.	Eerste keer uit de configuratie.
	Afstandspeer dient slechts één specifiek ISAKMP-profiel aan te passen, indien de peer-identiteit wordt gematcht in twee ISAKMP-profielen, is de	Afstandspeer dient slechts één specifiek ISAKMP-profiel aan te passen, indien peer-identiteit wordt gematcht in twee ISAKMP-profielen, is de configuratie ongeldig.

configuratie ongeldig.

In dit gedeelte worden ook de typische fouten beschreven die optreden wanneer een onjuist profiel is geselecteerd.

IKE-profiel, selectievolgorde op IKE-initiator

De VTI interface wijst gewoonlijk op een specifiek IPSec profiel met een specifiek IKE profiel. De router weet dan welk IKE-profiel u wilt gebruiken.

Op dezelfde manier wijst de crypto-kaart op een specifiek IKE profiel, en de router weet welk profiel te gebruiken wegens de configuratie.

Er kunnen echter scenario's zijn waarin het profiel niet is gespecificeerd en het niet mogelijk is om rechtstreeks uit de configuratie te bepalen welk profiel moet worden gebruikt; In dit voorbeeld wordt er geen IKE-profiel in het IPSec-profiel geselecteerd:

```
crypto isakmp profile profile1
  keyring keyring
  match identity address 192.168.0.0 255.255.255.0
crypto isakmp profile profile2
  keyring keyring
  match identity address 192.168.0.2 255.255.255.255

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
mode tunnel

crypto ipsec profile profile1
set transform-set TS

interface Tunnell
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
```

Wanneer deze initiator probeert een pakket van MM1 naar 192.168.0.2 te verzenden, wordt het meest specifieke profiel geselecteerd:

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

IKE-profiel, selectievolgorde op IKE-responder

De volgorde voor profielselectie op een IKE-responder is gelijk aan de volgorde voor hoofdselectie, waar de meest specifieke voorrang krijgt.

Stel deze configuratie in:

```
crypto isakmp profile profile1
  keyring keyring
  match identity address 192.168.0.0 255.255.255.0
crypto isakmp profile profile2
  keyring keyring
  match identity address 192.168.0.1 255.255.255.255
```

Wanneer een verbinding van 192.168.0.1 wordt ontvangen, zal profile2 worden geselecteerd.

De volgorde van de geconfigureerde profielen is niet belangrijk. De **show in werking stellen**-configuratie opdracht plaatst elk nieuw gevormd profiel aan het eind van de lijst.

Soms heeft de responder twee IKE-profielen die dezelfde sleutelring gebruiken. Als een onjuist profiel is geselecteerd op de responder maar de geselecteerde sleutelring correct is, zal de authenticatie correct eindigen:

```
*Oct 7 06:46:39.893: ISAKMP:(1003): processing ID payload. message ID = 0
*Oct 7 06:46:39.893: ISAKMP (1003): ID payload
    next-payload : 8
    type          : 1
    address       : 192.168.0.1
    protocol      : 17
    port          : 500
    length        : 12
*Oct 7 06:46:39.893: ISAKMP:(0):: peer matches profile2 profile
*Oct 7 06:46:39.893: ISAKMP:(0):key for 192.168.0.1 not available in default
*Oct 7 06:46:39.893: ISAKMP:(0):key for 192.168.0.1 found in keyring
*Oct 7 06:46:39.893: ISAKMP:(0):ISAKMP: Selecting 192.168.0.1,255.255.255.255
as final key

*Oct 7 06:46:39.893: ISAKMP:(1003):SA authentication status:
    authenticated
*Oct 7 06:46:39.893: ISAKMP:(1003):SA has been authenticated with 192.168.0.1
*Oct 7 06:46:39.893: ISAKMP:(1003):SA authentication status:
    authenticated
```

```
*Oct 7 06:46:39.893: ISAKMP:(1003):Old State = IKE_R_MM5 New State =
IKE_P1_COMPLETE
```

De responder ontvangt het QM-voorstel en accepteert dit en probeert de IPSec Security Parameter Index (SPI's) te genereren. In dit voorbeeld werden enkele insecten voor de duidelijkheid verwijderd:

```
*Oct 7 06:46:39.898: ISAKMP:(1003):Checking IPSec proposal 1
*Oct 7 06:46:39.898: ISAKMP:(1003):atts are acceptable.
*Oct 7 06:46:39.898: IPSEC(validate_proposal_request): proposal part #1
```

Op dit moment faalt de responder en rapporteert het juiste ISAKMP-profiel niet:

```
(key eng. msg.) INBOUND local= 192.168.0.2:0, remote= 192.168.0.1:0,
    local_proxy= 192.168.0.2/255.255.255.255/47/0,
    remote_proxy= 192.168.0.1/255.255.255.255/47/0,
    protocol= ESP, transform= NONE (Tunnel),
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Oct 7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct 7 06:46:39.898: Crypto mapdb : proxy_match
    src addr      : 192.168.0.2
    dst addr      : 192.168.0.1
    protocol      : 47
    src port      : 0
    dst port      : 0
*Oct 7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct 7 06:46:39.898: Crypto mapdb : proxy_match
    src addr      : 192.168.0.2
    dst addr      : 192.168.0.1
    protocol      : 47
    src port      : 0
```

```
dst port      : 0
*Oct 7 06:46:39.898: map_db_check_isakmp_profile profile did not match
*Oct 7 06:46:39.898: map_db_find_best did not find matching map
*Oct 7 06:46:39.898: IPSEC(ipsec_process_proposal): proxy identities not
supported
*Oct 7 06:46:39.898: ISAKMP:(1003): IPsec policy invalidated proposal with
error 32
*Oct 7 06:46:39.898: ISAKMP:(1003): phase 2 SA policy not acceptable!
(local 192.168.0.2 remote 192.168.0.1)
*Oct 7 06:46:39.898: ISAKMP: set new node 1993778370 to QM_IDLE
R2#
*Oct 7 06:46:39.898: ISAKMP:(1003):Sending NOTIFY PROPOSAL_NOT_CHOSEN
protocol 3
```

Omdat de IKE-profielselectie niet correct is, wordt fout 32 teruggegeven en wordt de responder het bericht PROPOSAL_NOT_CHOSEN verstuurd.

Samenvatting

Voor IKEv1 wordt een vooraf gedeelde sleutel gebruikt met DH-resultaten om de sleutel te berekenen die wordt gebruikt voor de codering die begint bij M5. Nadat hij MM3 ontvangt, kan de ISAKMP-ontvanger nog niet bepalen welk ISAKMP-profiel (en bijbehorende sleutelring) moet worden gebruikt omdat IKEID in MM5 en MM6 wordt verzonden.

Het resultaat is dat de ISAKMP-responder probeert door alle globaal gedefinieerde sleutelringen te zoeken om de sleutel voor specifieke peer te vinden. Voor verschillende IP-adressen wordt de best matching-toets (de meest specifieke) geselecteerd; voor hetzelfde IP-adres wordt de eerste matching uit de configuratie gebruikt. De sleutelring wordt gebruikt om de sleutel te berekenen die wordt gebruikt voor de decryptie van MM5.

Nadat hij MM5 heeft ontvangen, bepaalt de ISAKMP-initiator het ISAKMP-profiel en de bijbehorende sleutelring. De initiatiefnemer voert een verificatie uit indien dit dezelfde sleutelring is die voor de M4 DH-berekening is geselecteerd; anders verloopt de verbinding niet .

De volgorde van de toetsenborden in de mondiale configuratie is cruciaal. Voor de ISAKMP-responder gebruikt u dus één muisklik met meerdere ingangen indien mogelijk.

De pre-gedeelde toetsen die in mondiale configuratiemodus worden gedefinieerd, behoren tot een vooraf gedefinieerde sleutelring die standaard wordt genoemd. Dan gelden dezelfde regels.

Voor IKE-profielselectie voor de responder, wordt het meest specifieke profiel aangepast. Voor de initiator wordt het profiel van de configuratie gebruikt, of, als dat niet kan worden bepaald, wordt de beste overeenkomst gebruikt.

Een soortgelijk probleem doet zich voor in scenario's die verschillende certificaten voor verschillende ISAKMP-profielen gebruiken. Verificatie kan mislukken vanwege 'ca trust-point'-profielvalidatie wanneer een ander certificaat is gekozen. Dit probleem wordt in een afzonderlijk document behandeld.

De kwesties die in dit artikel worden beschreven zijn geen Cisco-specifieke problemen maar zijn gerelateerd aan de beperkingen van IKEv1-protocolontwerp. IKEv1, gebruikt met certificaten, heeft deze beperkingen niet en IKEv2, gebruikt voor zowel vooraf gedeelde sleutels als certificaten, heeft deze beperkingen niet.

Gerelateerde informatie

- [Configuratie-gids van Cisco IOS release 15M&T voor configuratie van IPsec-certificaat voor ISAKMP Profile mapping van Internet Key Exchange voor IPsec VPN's](#)
- [Kan een aanspreekpunt maken via een duidelijk gedeelte van de Cisco IOS security opdracht: Opdrachten A tot C](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)