IOS IKEv1/IKEv2-Auswahlregeln für Keyrings und Profile - Leitfaden zur Fehlerbehebung

Inhalt

Einführung

In diesem Dokument wird die Verwendung mehrerer Keyrings für mehrere ISAKMP-Profile (Internet Security Association and Key Management Protocol) in einem LAN-to-LAN-VPN-Szenario der Cisco IOS®-Software beschrieben. Es beschreibt das Verhalten der Cisco IOS Software, Version 15.3T, sowie mögliche Probleme, wenn mehrere Keyrings verwendet werden.

Es werden zwei Szenarien vorgestellt, die auf einem VPN-Tunnel mit zwei ISAKMP-Profilen auf jedem Router basieren. Jedes Profil hat einen anderen Keyring, an den die gleiche IP-Adresse angeschlossen ist. Die Szenarien zeigen, dass der VPN-Tunnel aufgrund der Profilauswahl und Überprüfung nur von einer Seite der Verbindung aus initiiert werden kann.

In den nächsten Abschnitten des Dokuments werden die Auswahlkriterien für das Schlüsselprofil sowohl für den Initiator von Internet Key Exchange (IKE) als auch für den IKE-Responder zusammengefasst. Wenn vom Keyring auf dem IKE-Responder verschiedene IP-Adressen verwendet werden, funktioniert die Konfiguration ordnungsgemäß, aber die Verwendung derselben IP-Adresse verursacht das Problem, das im ersten Szenario dargestellt wird.

In den folgenden Abschnitten wird erklärt, warum sowohl das Vorhandensein eines Standardkeyrings (globale Konfiguration) als auch eines bestimmten Keyrings zu Problemen

führen kann und warum die Verwendung des IKEv2-Protokolls (Internet Key Exchange Version 2) dieses Problem vermeidet.

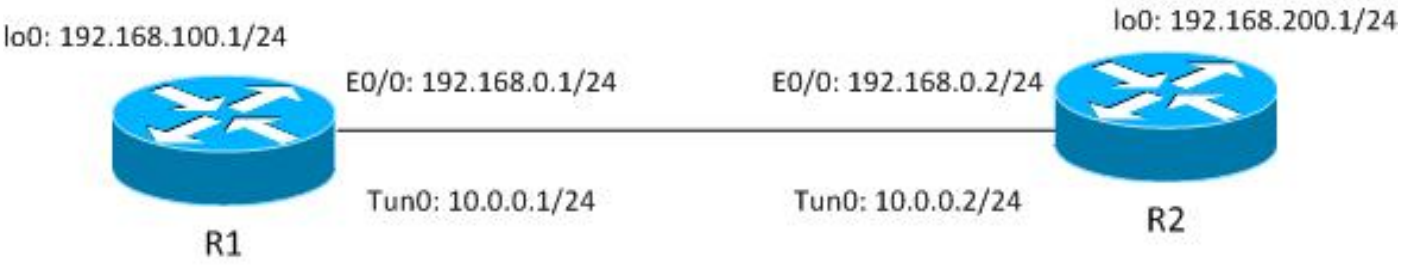
In den letzten Abschnitten werden die Auswahlkriterien für das IKE-Profil für IKE-Initiator und -Responder sowie die typischen Fehler beschrieben, die auftreten, wenn ein falsches Profil ausgewählt wurde.

Konfiguration

> **Hinweise**:
>
> Der Cisco CLI Analyzer (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.
>
> Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug**-Befehlen finden Sie unter Wichtige Informationen.

Topologie

Router1 (R1) und Router2 (R2) verwenden Virtual Tunnel Interface (VTI) (Generic Routing Encapsulation [GRE])-Schnittstellen, um auf die Loopbacks zuzugreifen. Dieses VTI ist durch Internet Protocol Security (IPSec) geschützt.



Sowohl R1 als auch R2 verfügen über zwei ISAKMP-Profile mit jeweils unterschiedlichen Keyrings. Alle Tastenkombinationen haben dasselbe Kennwort.

R1-Netzwerk und VPN

Die Konfiguration für das R1-Netzwerk und das VPN lautet:

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

crypto isakmp profile profile1
```

```
  keyring keyring1
  match identity address 192.168.0.102 255.255.255.255 !non existing host
crypto isakmp profile profile2
  keyring keyring2
  match identity address 192.168.0.2 255.255.255.255 !R2
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile2
!
interface Loopback0
 description Simulate LAN
 ip address 192.168.100.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.

ip route 192.168.200.0 255.255.255.0 10.0.0.2
```

R2 Netzwerk und VPN

Die Konfiguration für das R2-Netzwerk und das VPN lautet:

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

crypto isakmp profile profile1
  keyring keyring1
  match identity address 192.168.0.1 255.255.255.255 !R1
crypto isakmp profile profile2
  keyring keyring2
  match identity address 192.168.0.100 255.255.255.255 !non existing host
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile1
!
interface Loopback0
 ip address 192.168.200.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.2 255.255.255.0
```

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

ip route 192.168.100.0 255.255.255.0 10.0.0.1
```

Alle Keyrings verwenden dieselbe Peer-IP-Adresse und das Kennwort ' cisco'.

Auf R1 wird profile2 für die VPN-Verbindung verwendet. Profile2 ist das zweite Profil in der Konfiguration, das den zweiten Keyring in der Konfiguration verwendet. Wie Sie sehen werden, ist die Schlüsselzeichenfolge entscheidend.

Beispielszenarien

Im ersten Szenario ist R1 der ISAKMP-Initiator. Der Tunnel verhandelt ordnungsgemäß, und der Verkehr wird wie erwartet geschützt.

Im zweiten Szenario wird dieselbe Topologie verwendet, aber der ISAKMP-Initiator R2 ist vorhanden, wenn Phase1-Aushandlung fehlschlägt.

Internet Key Exchange Version 1 (IKEv1) benötigt einen vorinstallierten Schlüssel für die Schlüsselberechnung, der zur Entschlüsselung/Verschlüsselung des Hauptmodus-Pakets 5 (MM5) und nachfolgender IKEv1-Pakete verwendet wird. Der Schlüssel wird von der Diffie-Hellman (DH)-Berechnung und dem Pre-Shared Key abgeleitet. Dieser Pre-Shared Key muss nach dem Empfang von MM3 (Responder) oder MM4 (Initiator) bestimmt werden, damit der Schlüssel, der in MM5/MM6 verwendet wird, berechnet werden kann.

Für den ISAKMP-Responder in MM3 ist das spezifische ISAKMP-Profil noch nicht bestimmt, da dies geschieht, nachdem IKEID in MM5 empfangen wurde. Stattdessen werden alle Keyrings nach einem Pre-Shared Key durchsucht, und der erste oder am besten geeignete Keyring aus der globalen Konfiguration wird ausgewählt. Dieser Keyring wird verwendet, um den Schlüssel zu berechnen, der für die Entschlüsselung von MM5 und die Verschlüsselung von MM6 verwendet wird. Nach der Entschlüsselung von MM5 und nachdem das ISAKMP-Profil und der zugehörige Keyring ermittelt wurden, überprüft der ISAKMP-Responder, ob der gleiche Keyring ausgewählt wurde. Wenn der gleiche Keyring nicht ausgewählt ist, wird die Verbindung getrennt.

Daher sollten Sie für den ISAKMP-Responder möglichst einen Keyring mit mehreren Einträgen verwenden.

R1 = IKE Initiator (korrekt)

Dieses Szenario beschreibt, was geschieht, wenn R1 der IKE-Initiator ist:

1. Verwenden Sie diese Debugging-Tools für R1 und R2:

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

2. R1 initiiert den Tunnel, sendet das MM1-Paket mit Richtlinienvorschlägen und empfängt als Antwort MM2. MM3 wird dann vorbereitet:

```
R1#ping 192.168.200.1 source lo0 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1

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

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

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

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

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

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

R1 weiß von Anfang an, dass das ISAKMP-Profil2 verwendet werden sollte, da es unter dem für das VTI verwendeten IPSec-Profil gebunden ist.

So wurde der richtige Keyring (keyring2) ausgewählt. Der vorinstallierte Schlüssel aus keyring2 wird als Schlüsselmaterial für DH-Berechnungen verwendet, wenn das MM3-Paket vorbereitet wird.

3. Wenn R2 dieses MM3-Paket empfängt, weiß er immer noch nicht, welches ISAKMP-Profil verwendet werden soll, benötigt aber einen vorinstallierten Schlüssel für die DH-Generierung. Deshalb durchsucht R2 alle Keyrings, um den Pre-Shared Key für diesen Peer zu finden:

```
*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
```

Der Schlüssel für 192.168.0.1 wurde im ersten definierten Keyring (keyring1) gefunden.

4. R2 erstellt dann das MM4-Paket mit DH-Berechnungen und dem "cisco"-Schlüssel aus dem Keyring1:

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

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

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

5. Wenn R1 MM4 empfängt, bereitet er das MM5-Paket mit IKEID und mit dem richtigen Schlüssel vor (aus keyring2):

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

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

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

6. Das MM5-Paket, das die IKEID 192.168.0.1 enthält, wird von R2 empfangen. Zu diesem Zeitpunkt weiß R2, an welches ISAKMP-Profil der Datenverkehr gebunden werden soll (Befehl **match identity** address (**Identitätsadressbefehl**):

```
*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 überprüft jetzt, ob der Keyring, der für das MM4-Paket blind ausgewählt wurde, mit dem Keyring übereinstimmt, der für das jetzt ausgewählte ISAKMP-Profil konfiguriert wurde. Da keyring1 der erste in der Konfiguration ist, wurde er zuvor ausgewählt und jetzt ausgewählt. Die Validierung ist erfolgreich, und das MM6-Paket kann gesendet werden:

```
*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 empfängt MM6 und muss die Keyring-Überprüfung nicht durchführen, da sie vom ersten Paket bekannt war. Der Initiator weiß immer, welches ISAKMP-Profil verwendet werden soll und welcher Keyring mit diesem Profil verknüpft ist. Die Authentifizierung ist erfolgreich, und Phase1 schließt ordnungsgemäß ab:

```
*Jun 19 10:04:24.838: ISAKMP (1011): received packet from 192.168.0.2
dport 500 sport 500 Global (I) MM_KEY_EXCH
*Jun 19 10:04:24.838: ISAKMP:(1011): processing ID payload. message ID = 0
*Jun 19 10:04:24.838: ISAKMP (1011): ID payload
       next-payload : 8
       type         : 1
       address      : 192.168.0.2
       protocol     : 17
       port         : 500
       length       : 12
```

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

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

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

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

9. Phase 2 startet normal und ist erfolgreich abgeschlossen.

Dieses Szenario funktioniert nur aufgrund der richtigen Reihenfolge der Keyrings, die für R2 definiert sind. Das Profil, das für die VPN-Sitzung verwendet werden soll, verwendet den Keyring, der zuerst in der Konfiguration verwendet wurde.

R2 = IKE Initiator (Falsch)

Dieses Szenario beschreibt, was geschieht, wenn R2 denselben Tunnel initiiert, und erklärt, warum der Tunnel nicht erstellt wird. Einige Protokolle wurden entfernt, um sich auf die Unterschiede zwischen diesem und dem vorherigen Beispiel zu konzentrieren:

1. R2 initiiert den Tunnel:

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

2. Da R2 der Initiator ist, sind das ISAKMP-Profil und der Keyring bekannt. Der Pre-Shared Key von keyring1 wird für DH-Berechnungen verwendet und in MM3 gesendet. R2 empfängt MM2 und bereitet auf der Grundlage dieses Schlüssels MM3 vor:

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

*Jun 19 12:28:44.256: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 12:28:44.256: ISAKMP:(0): processing vendor id payload
*Jun 19 12:28:44.256: ISAKMP:(0): vendor ID seems Unity/DPD but major
69 mismatch
*Jun 19 12:28:44.256: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 12:28:44.256: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.256: ISAKMP:(0): local preshared key found
*Jun 19 12:28:44.256: ISAKMP : Looking for xauth in profile profile1
```

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

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

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

3. R1 empfängt MM3 von R2. Zum gegenwärtigen Zeitpunkt weiß R1 nicht, welches ISAKMP-Profil verwendet werden soll, daher weiß er nicht, welcher Keyring verwendet werden soll. R1 verwendet daher den ersten Keyring aus der globalen Konfiguration, d. h. keyring1. R1 verwendet diesen Pre-Shared Key für DH-Berechnungen und sendet 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 empfängt MM4 von R1, verwendet den Pre-Shared Key von keyring1 zur Berechnung von DH und bereitet das MM5-Paket und die IKEID vor:

```
*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 empfängt MM5 von R1. Da IKEID 192.168.0 entspricht, wurde profile2 ausgewählt. Keyring2 wurde in profile2 konfiguriert, sodass keyring2 ausgewählt ist. Für die DH-Berechnung in MM4 wählte R1 zuvor den ersten konfigurierten Keyring aus, der Keyring1 war. Auch wenn die Kennwörter genau identisch sind, schlägt die Validierung für den Keyring fehl, da es sich um verschiedene Keyring-Objekte handelt:

```
*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
```

Debuggen für einen anderen vorinstallierten Schlüssel

In den vorherigen Szenarien wurde derselbe Schlüssel ("cisco") verwendet. So konnte das MM5-Paket selbst bei Verwendung des falschen Keyrings korrekt entschlüsselt und später aufgrund

eines Fehlers bei der Schlüsselvalidierung verworfen werden.

In Szenarien, in denen verschiedene Schlüssel verwendet werden, kann MM5 nicht entschlüsselt werden, und die folgende Fehlermeldung wird angezeigt:

```
*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
```

Schlüsselkriterien für die Auswahl

Dies ist eine Zusammenfassung der Kriterien für die Auswahl des Keyrings. Weitere Einzelheiten finden Sie in den nächsten Abschnitten.

	Initiator	Responder
Mehrere Keyings mit unterschiedlichen IP-Adressen	Konfiguriert. Wenn nicht explizit die spezifischsten Konfigurationen konfiguriert wurden	Die spezifischste Übereinstimmung
Mehrere Keyings mit denselben IP-Adressen	Konfiguriert. Wenn nicht explizit konfiguriert **Konfiguration wird unvorhersehbar und nicht unterstützt. Es sollten nicht zwei Schlüssel für dieselbe IP-Adresse konfiguriert werden.**	**Die Konfiguration ist nicht vorhersehbar und wird nicht unterstützt. Es sollten nicht zwei Schlüssel für dieselbe IP-Adresse konfiguriert werden.**

In diesem Abschnitt wird auch erläutert, warum sowohl das Vorhandensein eines Standardkeyrings (globale Konfiguration) als auch bestimmter Keyrings zu Problemen führen kann, und erläutert, warum die Verwendung des IKEv2-Protokolls derartige Probleme vermeidet.

Schlüsselauswahlreihenfolge auf IKE-Initiator

Für die Konfiguration mit einem VTI verwendet der Initiator eine spezifische Tunnelschnittstelle, die auf ein bestimmtes IPSec-Profil zeigt. Da das IPSec-Profil ein bestimmtes IKE-Profil mit einem bestimmten Keyring verwendet, besteht keine Verwirrung darüber, welcher Keyring verwendet werden soll.

Crypto-Map, das auch auf ein bestimmtes IKE-Profil mit einem bestimmten Keyring verweist, funktioniert auf dieselbe Weise.

Es ist jedoch nicht immer möglich, aus der Konfiguration herauszufinden, welcher Keyring verwendet werden soll. Dies tritt beispielsweise auf, wenn kein IKE-Profil konfiguriert ist, d. h. das IPSec-Profil ist nicht konfiguriert, um das IKE-Profil zu verwenden:

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

crypto ipsec transform-set TS esp-aes esp-sha256-hmac
```

```
 mode tunnel

crypto ipsec profile profile1
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
```

Wenn dieser IKE-Initiator versucht, MM1 zu senden, wählt er den spezifischsten Keyring aus:

```
*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
```

Da der Initiator beim Empfang von MM6 keine IKE-Profile konfiguriert hat, wird kein Profil angezeigt. Der Initiator verfügt über eine erfolgreiche Authentifizierung und einen 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_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
```

Keyring Selection Order on IKE Responder - Diverse IP Addresses

Das Problem bei der Auswahl des Keyrings liegt beim Responder. Wenn Keyrings unterschiedliche IP-Adressen verwenden, ist die Auswahlreihenfolge einfach.

Nehmen Sie an, der IKE-Responder hat die folgende Konfiguration:

```
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
```

Wenn dieser Responder das MM1-Paket vom IKE-Initiator mit der IP-Adresse 192.168.0.2 empfängt, wählt er die beste (spezifischste) Übereinstimmung aus, selbst wenn die Reihenfolge in der Konfiguration anders ist.

Die Kriterien für die Auswahl der Bestellung sind:

1. Es werden nur Schlüssel mit einer IP-Adresse berücksichtigt.
2. Das virtuelle Routing und die Weiterleitung (VRF) des eingehenden Pakets wird geprüft (Front-End VRF [fVRF]).
3. Wenn sich das Paket im Standard-VRF befindet, wird zuerst der globale Keyring überprüft.

Die genaueste Taste (Netzmasklänge) wird ausgewählt.

4. Wenn im Standardkeyring kein Schlüssel gefunden wird, werden alle Keyrings, die diesem fVRF entsprechen, verkettet.
5. Der genaueste Schlüssel (längste Netzmaske) wird zugeordnet. Beispielsweise wird ein /32 gegenüber einem /24 bevorzugt.

Die Debugger bestätigen die Auswahl:

```
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
```

Keyring Selection Order on IKE Responder - Dieselben IP-Adressen

Wenn Keyrings dieselben IP-Adressen verwenden, treten Probleme auf. Nehmen Sie an, der IKE-Responder hat die folgende Konfiguration:

```
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
```

Diese Konfiguration ist nicht vorhersehbar und wird nicht unterstützt. Es sollten keine zwei Tasten für dieselbe IP-Adresse konfiguriert werden, oder das in R2 beschriebene Problem wird im Fall von IKE Initiator (Falsch) beschrieben.

Globale Schlüsselkonfiguration

Die in der globalen Konfiguration definierten ISAKMP-Schlüssel gehören zum Standardkeyring:

```
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
```

Obwohl der ISAKMP-Schlüssel zuletzt in der Konfiguration vorhanden ist, wird er als erster in der IKE-Antwort verarbeitet:

```
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
```

Daher ist die Verwendung sowohl globaler Konfigurationen als auch spezifischer Keyrings sehr

riskant und kann zu Problemen führen.

Keyring auf IKEv2 - Problem tritt nicht auf

Obwohl das IKEv2-Protokoll ähnliche Konzepte wie IKEv1 verwendet, verursacht die Schlüsselzeichenauswahl keine ähnlichen Probleme.

In einfachen Fällen werden nur vier Pakete ausgetauscht. Die IKEID, die bestimmt, welches IKEv2-Profil auf dem Responder ausgewählt werden soll, wird vom Initiator im dritten Paket gesendet. Das dritte Paket ist bereits verschlüsselt.

Der größte Unterschied in den beiden Protokollen ist, dass IKEv2 nur das DH-Ergebnis für die Skey-Berechnung verwendet. Der vorinstallierte Schlüssel ist nicht mehr erforderlich, um den Schlüssel für die Verschlüsselung/Entschlüsselung zu berechnen.

Der IKEv2 RFC (5996, Abschnitt 2.14) lautet wie folgt:

Die gemeinsam genutzten Schlüssel werden wie folgt berechnet. Eine Menge mit der Bezeichnung SKEYSEED wird aus den während des IKE_SA_INIT-Austauschs ausgetauschten Nonces und dem bei diesem Austausch eingerichteten gemeinsamen geheimen Diffie-Hellman berechnet.

Im gleichen Abschnitt stellt die RFC außerdem Folgendes fest:

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

Alle erforderlichen Informationen werden in den ersten beiden Paketen versendet. Bei der Berechnung der SKEYSEED-Datei muss kein vorinstallierter Schlüssel verwendet werden.

Vergleichen Sie dies mit dem IKE-RFC (2409, Abschnitt 3.2), in dem Folgendes aufgeführt ist:

SKEYID ist eine Zeichenfolge, die aus geheimen Materialien abgeleitet wird, die nur den aktiven Spielern im Austausch bekannt sind.

Dieses "Geheimmaterial, das nur den aktiven Spielern bekannt ist" ist der Pre-Shared Key. In Abschnitt 5 stellt die RFC außerdem Folgendes fest:

Für vorinstallierte Schlüssel: SKEYID = prf(**Pre-shared-key**, Ni_b | Nr_b)

Dies erklärt, warum das IKEv1-Design für vorinstallierte Schlüssel so viele Probleme verursacht. Diese Probleme sind in IKEv1 nicht vorhanden, wenn Zertifikate für die Authentifizierung verwendet werden.

IKE-Profilauswahlkriterien

Dies ist eine Zusammenfassung der IKE-Profilauswahlkriterien. Weitere Einzelheiten finden Sie in den nächsten Abschnitten.

	Initiator	Responder
Profilauswahl	Sie sollte konfiguriert werden (im IPSec-Profil oder in der Crypto Map festgelegt). Wenn nicht konfiguriert, muss zuerst eine	Erste Übereinstimmung aus der Konfiguration Der Remote-Peer sollte nur einem bestimmte ISAKMP-Profil entsprechen. Wenn die Peer-

	Übereinstimmung aus der Konfiguration gefunden werden. Der Remote-Peer sollte nur einem bestimmten ISAKMP-Profil entsprechen. Wenn die Peer-Identität in zwei ISAKMP-Profilen zugeordnet wird, ist die Konfiguration ungültig.	Identität in zwei ISAKMP-Profilen zugeordnet ist die Konfiguration ungültig.

In diesem Abschnitt werden auch die typischen Fehler beschrieben, die auftreten, wenn ein falsches Profil ausgewählt wurde.

IKE-Profilauswahlreihenfolge für IKE-Initiator

Die VTI-Schnittstelle verweist in der Regel auf ein bestimmtes IPSec-Profil mit einem spezifischen IKE-Profil. Der Router weiß dann, welches IKE-Profil verwendet werden soll.

Ebenso verweist die Crypto-Map auf ein bestimmtes IKE-Profil, und der Router weiß, welches Profil aufgrund der Konfiguration verwendet werden soll.

Es kann jedoch vorkommen, dass das Profil nicht angegeben wird und dass aus der Konfiguration nicht direkt ermittelt werden kann, welches Profil verwendet werden soll. In diesem Beispiel ist im IPSec-Profil kein IKE-Profil ausgewählt:

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

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

crypto ipsec profile profile1
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
```

Wenn dieser Initiator versucht, ein MM1-Paket an 192.168.0.2 zu senden, wird das spezifischste Profil ausgewählt:

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

IKE-Profilauswahlreihenfolge für IKE-Responder

Die Profilauswahlreihenfolge für einen IKE-Responder ähnelt der Reihenfolge für die Schlüsselauswahl, in der die spezifischste Reihenfolge Vorrang hat.

Nehmen wir an, diese Konfiguration:

```
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
```

Wenn eine Verbindung von 192.168.0.1 empfangen wird, wird profile2 ausgewählt.

Die Reihenfolge der konfigurierten Profile spielt keine Rolle. Mit dem Befehl **show running-config** wird jedes neu konfigurierte Profil am Ende der Liste platziert.

Manchmal verfügt der Responder über zwei IKE-Profile, die den gleichen Keyring verwenden. Wenn auf dem Responder ein falsches Profil ausgewählt wurde, der ausgewählte Keyring jedoch korrekt ist, wird die Authentifizierung korrekt abgeschlossen:

```
*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
```

Der Responder empfängt und akzeptiert den QM-Vorschlag und versucht, die IPSec Security Parameter Indixes (SPIs) zu generieren. In diesem Beispiel wurden einige Debuggen aus Gründen der Klarheit entfernt:

```
*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
```

An diesem Punkt schlägt der Responder fehl und berichtet, dass das richtige ISAKMP-Profil nicht übereinstimmt:

```
 (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
```

Aufgrund der falschen Auswahl des IKE-Profils wird Fehler 32 zurückgegeben, und der Responder sendet die Meldung PROPOSAL_NOT_CHOSEN.

Zusammenfassung

Für IKEv1 wird ein vorinstallierter Schlüssel mit DH-Ergebnissen verwendet, um den für die Verschlüsselung verwendeten Schlüssel zu berechnen, der mit MM5 beginnt. Nachdem MM3 empfangen wurde, kann der ISAKMP-Empfänger noch nicht bestimmen, welches ISAKMP-Profil (und der zugehörige Keyring) verwendet werden soll, da die IKEID in MM5 und MM6 gesendet wird.

Das Ergebnis ist, dass der ISAKMP-Responder versucht, alle global definierten Keyrings zu durchsuchen, um den Schlüssel für einen bestimmten Peer zu finden. Für verschiedene IP-Adressen wird der am besten übereinstimmende Keyring (der am spezifischsten) ausgewählt. für dieselbe IP-Adresse wird die erste übereinstimmende Keying-Nachricht aus der Konfiguration verwendet. Der Keyring wird verwendet, um den Schlüssel zu berechnen, der für die Entschlüsselung von MM5 verwendet wird.

Nachdem der ISAKMP-Initiator MM5 empfangen hat, bestimmt er das ISAKMP-Profil und den zugehörigen Keyring. Der Initiator überprüft, ob es sich um denselben Keyring handelt, der für die MM4-DH-Berechnung ausgewählt wurde. Andernfalls schlägt die Verbindung fehl.

Die Reihenfolge der Keyrings, die in der globalen Konfiguration konfiguriert sind, ist entscheidend. Verwenden Sie daher für den ISAKMP-Responder möglichst einen Keyring mit mehreren Einträgen.

Die im globalen Konfigurationsmodus definierten vorinstallierten Schlüssel gehören zu einem vordefinierten Keyring, der als Standard bezeichnet wird. Dann gelten die gleichen Regeln.

Für die IKE-Profilauswahl für den Responder wird das spezifischste Profil zugeordnet. Für den Initiator wird das Profil aus der Konfiguration verwendet, oder, wenn dies nicht bestimmt werden kann, wird die beste Übereinstimmung verwendet.

Ein ähnliches Problem tritt in Szenarien auf, in denen unterschiedliche Zertifikate für verschiedene ISAKMP-Profile verwendet werden. Die Authentifizierung kann aufgrund der Profilvalidierung von 'ca trust-point' fehlschlagen, wenn ein anderes Zertifikat ausgewählt wird. Dieses Problem wird in einem separaten Dokument behandelt.

Die in diesem Artikel beschriebenen Probleme sind keine Cisco spezifischen Probleme, sondern stehen in Zusammenhang mit den Einschränkungen des IKEv1-Protokolldesigns. IKEv1, das mit Zertifikaten verwendet wird, weist diese Einschränkungen nicht auf, und IKEv2, das sowohl für vorinstallierte Schlüssel als auch für Zertifikate verwendet wird, weist diese Einschränkungen nicht auf.

Zugehörige Informationen

- Zertifikat für ISAKMP-Profilzuordnung im Konfigurationsleitfaden für IPsec-VPNs für Internet Key Exchange for IPsec, Cisco IOS Release 15M&T
- ca trust-point durch einen klaren Abschnitt der Cisco IOS Security Command Reference: Befehle A bis C
- Technischer Support und Dokumentation - Cisco Systems