Reglas de selección de IOS IKEv1/IKEv2 para anillos de claves y perfiles - Guía de resolución de problemas

Contenido

Introducción

Este documento describe el uso de varios anillos de claves para varios perfiles de protocolo de administración de claves y asociación de seguridad de Internet (ISAKMP) en un escenario de VPN de LAN a LAN del software Cisco IOS®. Describe el comportamiento de la versión 15.3T del software del IOS de Cisco, así como los problemas potenciales cuando se utilizan varios anillos de claves.

Se presentan dos escenarios, basados en un túnel VPN con dos perfiles ISAKMP en cada router. Cada perfil tiene un anillo de claves diferente con la misma dirección IP conectada. Los escenarios demuestran que el túnel VPN se puede iniciar solamente desde un lado de la conexión debido a la selección y verificación del perfil.

En las secciones siguientes del documento se resumen los criterios de selección del perfil de llenado de claves tanto para el iniciador de Intercambio de claves de Internet (IKE) como para el respondedor IKE. Cuando la llanura de llaves del respondedor IKE utiliza diferentes direcciones IP, la configuración funciona correctamente, pero el uso de la misma dirección IP crea el problema presentado en el primer escenario.

En las secciones siguientes se explica por qué la presencia de un llavero predeterminado (configuración global) y de claves específicas pueden provocar problemas y por qué el uso del protocolo Internet Key Exchange Version 2 (IKEv2) evita ese problema.

Las secciones finales presentan los criterios de selección para el perfil IKE tanto para el iniciador IKE como para el respondedor, junto con los errores típicos que ocurren cuando se selecciona un perfil incorrecto.

Configuración

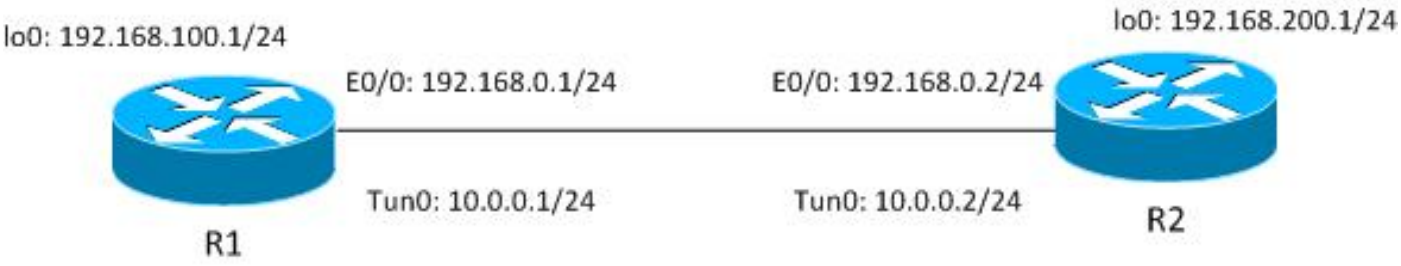
Notas:

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show. Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Topología

El router1 (R1) y el router2 (R2) utilizan interfaces de interfaz de túnel virtual (VTI) (Generic Routing Encapsulation [GRE]) para acceder a sus loopbacks. Esta VTI está protegida por la seguridad de protocolo de Internet (IPSec).



Tanto R1 como R2 tienen dos perfiles ISAKMP, cada uno con un anillo de claves diferente. Todos los teclados tienen la misma contraseña.

Red R1 y VPN

La configuración para la red R1 y VPN es:

```
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
```

Red R2 y VPN

La configuración para la red R2 y VPN es:

```
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
```

Todos los anillos de claves utilizan la misma dirección IP de par y la contraseña ' cisco'.

En R1, el perfil 2 se utiliza para la conexión VPN. Profile2 es el segundo perfil de la configuración, que utiliza el segundo anillo de claves de la configuración. Como verá, el orden de las claves es fundamental.

“Situaciones de ejemplo”

En el primer escenario, R1 es el iniciador ISAKMP. El túnel está negociando correctamente y el tráfico está protegido como se espera.

El segundo escenario utiliza la misma topología, pero tiene R2 como iniciador ISAKMP cuando falla la negociación de la fase 1.

Internet Key Exchange Version 1 (IKEv1) necesita una clave previamente compartida para el cálculo de claves, que se utiliza para descifrar/cifrar el paquete de modo principal 5 (MM5) y los paquetes IKEv1 subsiguientes. La clave deriva del cálculo Diffie-Hellman (DH) y de la clave previamente compartida. La clave previamente compartida debe determinarse después de recibir MM3 (respondedor) o MM4 (iniciador), de modo que se pueda calcular la clave, que se utiliza en MM5/MM6.

Para el respondedor ISAKMP en MM3, el perfil ISAKMP específico todavía no se ha determinado porque esto sucede después de que el IKEID se reciba en MM5. En su lugar, se busca en todos los anillos de claves una clave previamente compartida y se selecciona la primera o la mejor que coincida en la configuración global. Ese llavero se utiliza para calcular la clave que se utiliza para el descifrado de MM5 y el cifrado de MM6. Después del descifrado de MM5 y después de determinar el perfil ISAKMP y el anillo de claves asociado, el respondedor ISAKMP realiza la verificación si se ha seleccionado el mismo anillo de claves; si no se selecciona la misma llavera, se interrumpirá la conexión.

Por lo tanto, para el respondedor ISAKMP, debe utilizar un solo llavero con varias entradas siempre que sea posible.

R1 Como Iniciador IKE (Correcto)

Este escenario describe lo que ocurre cuando R1 es el iniciador IKE:

1. Utilice estos debugs para R1 y R2:

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

2. R1 inicia el túnel, envía el paquete MM1 con propuestas de políticas y recibe MM2 en respuesta. A continuación, se prepara MM3:

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

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

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

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

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

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

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

Desde el principio, R1 sabe que debe utilizarse el perfil ISAKMP2 porque está enlazado al perfil IPSec utilizado para ese VTI.

Por lo tanto, se ha seleccionado el anillo de claves correcto (keyring2). La clave previamente compartida de keyring2 se utiliza como material de codificación para los cálculos DH cuando se está preparando el paquete MM3.

3. Cuando R2 recibe ese paquete MM3, todavía no sabe qué perfil ISAKMP debe usarse, pero necesita una clave previamente compartida para la generación DH. Por eso R2 busca todos los anillos de claves para encontrar la clave previamente compartida para ese par:

```
*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
```

La clave para 192.168.0.1 se ha encontrado en el primer llavero definido (llavero 1).

4. R2 luego prepara el paquete MM4 con cálculos DH y con la clave 'cisco' de 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. Cuando R1 recibe MM4, prepara el paquete MM5 con IKEID y con la clave correcta seleccionada anteriormente (del anillo de claves 2):

```
*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. El paquete MM5, que contiene el IKEID de 192.168.0.1, es recibido por R2. En este punto, R2 sabe a qué perfil ISAKMP se debe enlazar el tráfico (el comando **match identity** address):

```
*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 realiza ahora la verificación si el anillo de claves que se seleccionó ciegamente para el paquete MM4 es el mismo que el anillo de claves configurado para el perfil ISAKMP que se ha elegido. Dado que keyring1 es el primero de la configuración, se seleccionó anteriormente y ahora se selecciona. La validación se realiza correctamente y se puede enviar el paquete MM6:

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

8. R1 recibe el MM6 y no necesita realizar la verificación del anillo de claves porque se conocía desde el primer paquete; el iniciador siempre sabe qué perfil ISAKMP debe utilizar y qué anillo de claves está asociado a ese perfil. La autenticación es correcta y la Fase 1 finaliza correctamente:

```
*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. La fase 2 se inicia normalmente y se completa correctamente.

Este escenario funciona correctamente sólo debido al orden correcto de los anillos de claves definidos en R2. El perfil que se debe utilizar para la sesión VPN utiliza el anillo de claves que fue el primero en la configuración.

R2 Como Iniciador IKE (Incorrecto)

Este escenario describe lo que ocurre cuando R2 inicia el mismo túnel y explica por qué no se establecerá el túnel. Algunos registros se han eliminado para centrarse en las diferencias entre este y el ejemplo anterior:

1. R2 inicia el túnel:

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

2. Dado que R2 es el iniciador, se conocen el perfil ISAKMP y el llaneo de claves. La clave previamente compartida de keyring1 se utiliza para los cálculos DH y se envía en MM3. R2 recibe MM2 y está preparando MM3 basándose en esa clave:

```
*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 recibe MM3 de R2. En esta etapa, R1 no sabe qué perfil ISAKMP debe utilizar, por lo que no sabe qué anillo de claves debe utilizar. R1, por lo tanto, utiliza el primer anillo de claves de la configuración global, que es keyring1. R1 utiliza esa clave previamente compartida para los cálculos DH y envía 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 recibe MM4 de R1, utiliza la clave previamente compartida de keyring1 para calcular DH y prepara el paquete MM5 y el IKEID:

```
*Jun 19 12:28:44.269: ISAKMP:(0):Found ADDRESS key in keyring keyring1
*Jun 19 12:28:44.269: ISAKMP:(1012): processing vendor id payload
*Jun 19 12:28:44.269: ISAKMP:(1012): vendor ID is Unity
```

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

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

5. R1 recibe MM5 de R1. Como IKEID es igual a 192.168.0, se ha seleccionado el perfil2. El anillo de claves 2 se ha configurado en el perfil 2 para que se seleccione el anillo de claves 2. Anteriormente, para el cálculo DH en MM4, R1 seleccionó el primer anillo de claves configurado, que era keyring1. Aunque las contraseñas son exactamente las mismas, la validación para el llenado de claves falla porque son diferentes objetos de llenado de claves:

```
*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
```

Depuraciones para diferentes claves previamente compartidas

Los escenarios anteriores utilizaban la misma clave ('cisco'). Por lo tanto, incluso cuando se utilizó el llenado de claves incorrecto, el paquete MM5 se pudo descifrar correctamente y descartar más tarde debido a una falla en la validación del llenado de claves.

En escenarios donde se utilizan diferentes claves, no se puede descifrar el MM5 y aparece este mensaje de error:

```
*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
```

Criterios de selección de anillo

Este es un resumen de los criterios de selección del anillo de claves. Consulte las secciones siguientes para obtener más información.

	Iniciador	Respondedor
Varios teclados con direcciones IP diferentes	Configurado. Si no se configura explícitamente el más específico de la configuración	La coincidencia más específica
Varios teclados con las mismas direcciones IP	Configurado. Si no se ha configurado explícitamente **la configuración se vuelve impredecible y no se admite. No se deben configurar dos claves para la misma dirección IP.**	**La configuración se vuelve impredecible y no se admite. No deben configurar dos claves para misma dirección IP.**

En esta sección también se describe por qué la presencia de un llavero predeterminado (configuración global) y de claves específicas pueden provocar problemas y se explica por qué el uso del protocolo IKEv2 evita tales problemas.

Orden de selección de anillo clave en el iniciador IKE

Para la configuración con un VTI, el iniciador utiliza una interfaz de túnel específica que apunta a un perfil IPSec específico. Dado que el perfil IPSec utiliza un perfil IKE específico con una clave específica, no hay confusión sobre qué anillo de claves se debe utilizar.

Crypto-map, que también apunta a un perfil IKE específico con una clave específica, funciona de la misma manera.

Sin embargo, no siempre es posible determinar a partir de la configuración qué anillo de claves utilizar. Por ejemplo, esto ocurre cuando no hay ningún perfil IKE configurado; es decir, el perfil IPSec no está configurado para utilizar el perfil IKE:

```
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
```

Si este iniciador IKE intenta enviar MM1, elegirá el anillo de claves más específico:

```
*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
```

Dado que el iniciador no tiene perfiles IKE configurados cuando recibe MM6, no llegará a un perfil y se completará con autenticación y modo rápido (QM) correctos:

```
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
```

Orden de selección de anillo clave en IKE Responder - Diferentes direcciones IP

El problema con la selección del anillo de claves está en el respondedor. Cuando los teclados utilizan direcciones IP diferentes, el orden de selección es sencillo.

Suponga que el respondedor IKE tiene esta configuración:

```
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
```

Cuando este respondedor recibe el paquete MM1 del iniciador IKE con la dirección IP 192.168.0.2, elegirá la mejor coincidencia (la más específica), incluso cuando el orden en la configuración sea diferente.

Los criterios para el pedido de selección son:

1. Solo se consideran las claves con una dirección IP.
2. El routing y el reenvío virtuales (VRF) del paquete entrante se comprueban (VRF de extremo frontal [fVRF]).
3. Si el paquete se encuentra en el VRF predeterminado, se verifica primero el llaneo de claves global. Se selecciona la clave más precisa (longitud de máscara de red).
4. Si no se encuentra ninguna clave en el llavero predeterminado, se concatenarán todos los llaneos que coincidan con este fVRF.
5. La clave más precisa (máscara de red más larga) coincide. Por ejemplo, se prefiere un /32 en lugar de un /24.

Las depuraciones confirman la selección:

```
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
```

Orden de selección de anillo clave en IKE Responder - Mismas direcciones IP

Cuando los teclados utilizan las mismas direcciones IP, se producen problemas. Suponga que el respondedor IKE tiene esta configuración:

```
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
```

Esta configuración se vuelve impredecible y no se admite. Uno no debe configurar dos claves para la misma dirección IP o el problema descrito en R2 As IKE Initiator (Incorrecto) ocurrirá.

Configuración global de anillo de claves

Las claves ISAKMP definidas en la configuración global pertenecen al anillo de claves predeterminado:

```
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
```

Aunque la clave ISAKMP es la última en la configuración, se procesa como la primera en el respondedor IKE:

```
R1#show crypto isakmp key
Keyring      Hostname/Address                            Preshared Key

default      0.0.0.0        [0.0.0.0]                    cisco3

keyring1     192.168.0.0    [255.255.0.0]                cisco

keyring2     192.168.0.2                                 cisco2
```

Por lo tanto, el uso tanto de la configuración global como de claves específicas es muy riesgoso y podría conducir a los problemas.

Anillo de claves en IKEv2 - No se produce el problema

Aunque el protocolo IKEv2 utiliza conceptos similares a IKEv1, la selección del anillo de claves no causa problemas similares.

En casos simples, hay sólo cuatro paquetes intercambiados. El IKEID que determina qué perfil IKEv2 debe seleccionarse en el respondedor es enviado por el iniciador en el tercer paquete. El tercer paquete ya está cifrado.

La mayor diferencia en los dos protocolos es que IKEv2 utiliza solamente el resultado DH para el cálculo de claves. La clave previamente compartida ya no es necesaria para calcular la clave utilizada para el cifrado/descifrado.

RFC IKEv2 (5996, sección 2.14) establece:

Las claves compartidas se calculan de la siguiente manera. Una cantidad llamada SKEYSEED se calcula a partir de las entradas intercambiadas durante el intercambio IKE_SA_INIT y el secreto compartido Diffie-Hellman establecido durante ese intercambio.

En la misma sección, el RFC también señala:

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

Toda la información necesaria se envía en los dos primeros paquetes y no hay necesidad de utilizar una clave previamente compartida cuando se calcula SKEYSEED.

Compare esto con el IKE RFC (2409, sección 3.2) , que dice:

SKEYID es una cadena derivada del material secreto conocido sólo por los jugadores activos en el intercambio.

Ese "material secreto conocido sólo por los actores activos" es la clave previamente compartida. En la sección 5, el RFC también señala:

Para claves previamente compartidas: SKEYID = prf(**clave precompartida**, Ni_b | Nr_b)

Esto explica por qué el diseño IKEv1 para claves previamente compartidas causa tantos problemas. Estos problemas no existen en IKEv1 cuando los certificados se utilizan para la autenticación.

Criterios de selección del perfil IKE

Este es un resumen de los criterios de selección del perfil IKE. Consulte las secciones siguientes para obtener más información.

	Iniciador	Respondedor
Selección de perfil	Debe configurarse (establecido en el perfil IPSec o en el mapa criptográfico). Si no está configurado, primero debe coincidir con la configuración. El par remoto debe coincidir sólo con un perfil ISAKMP específico, si la identidad del par coincide en dos perfiles ISAKMP, la configuración no es válida.	Primera coincidencia de la configuración. El par remoto debe coincidir sólo con un perfil ISAKMP específico, si la identidad d par coincide en dos perfiles ISAKMP, la configuración no es válida.

Esta sección también describe los errores típicos que se producen cuando se seleccionó un perfil incorrecto.

Orden de selección de perfil IKE en el iniciador IKE

La interfaz VTI normalmente apunta a un perfil IPSec específico con un perfil IKE específico. El router luego sabe qué perfil IKE debe utilizar.

De manera similar, el mapa crypto apunta a un perfil IKE específico, y el router sabe qué perfil utilizar debido a la configuración.

Sin embargo, podría haber escenarios en los que no se especifica el perfil y en los que no es posible determinar directamente a partir de la configuración qué perfil se debe utilizar; en este ejemplo, no se selecciona ningún perfil IKE en el perfil IPSec:

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

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

crypto ipsec profile profile1
 set transform-set TS

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

Cuando este iniciador intenta enviar un paquete MM1 a 192.168.0.2, se selecciona el perfil más específico:

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

Orden de selección de perfil IKE en IKE Responder

El orden de selección del perfil en un respondedor IKE es similar al orden de selección del anillo de claves, donde el más específico tiene prioridad.

Suponga esta configuración:

```
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
```

Cuando se recibe una conexión desde 192.168.0.1, se selecciona el perfil 2.

El orden de los perfiles configurados no importa. El comando **show running-config** coloca cada nuevo perfil configurado al final de la lista.

A veces, el respondedor puede tener dos perfiles IKE que utilicen el mismo anillo de claves. Si se

selecciona un perfil incorrecto en el respondedor pero el llavero seleccionado es correcto, la autenticación finalizará correctamente:

```
*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
```

El respondedor recibe y acepta la propuesta de QM e intenta generar los índices de parámetros de seguridad (SPI) de IPSec. En este ejemplo, se quitaron algunas depuraciones para mayor claridad:

```
*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
```

En este punto, el respondedor falla e informa que el perfil ISAKMP correcto no coincide:

```
 (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
```

Debido a la selección incorrecta del perfil IKE, se devuelve el error 32 y el respondedor envía el mensaje PROPOSAL_NOT_CHOSEN.

Summary

Para IKEv1, se utiliza una clave previamente compartida con resultados DH para calcular la clave utilizada para el cifrado que comienza en MM5. Después de recibir MM3, el receptor ISAKMP todavía no puede determinar qué perfil ISAKMP (y anillo de claves asociado) debe utilizarse porque el IKEID se envía en MM5 y MM6.

El resultado es que el respondedor ISAKMP intenta buscar a través de todos los anillos de claves definidos globalmente para encontrar la clave para un peer específico. Para diferentes direcciones IP, se selecciona la mejor combinación de claves (la más específica); para la misma dirección IP, se utiliza la primera clave coincidente de la configuración. El llavero se utiliza para calcular la clave que se utiliza para el descifrado de MM5.

Después de recibir MM5, el iniciador ISAKMP determina el perfil ISAKMP y el anillo de claves asociado. El iniciador realiza la verificación si se trata del mismo anillo de claves que se seleccionó para el cálculo MM4 DH; de lo contrario, la conexión falla.

El orden de los anillos de claves configurados en la configuración global es crítico. Por lo tanto, para el respondedor ISAKMP, utilice un solo llavero con múltiples entradas siempre que sea posible.

Las claves previamente compartidas que se definen en el modo de configuración global pertenecen a un anillo de claves predefinido denominado default. Las mismas reglas se aplican entonces.

Para la selección del perfil IKE para el respondedor, se hace coincidir el perfil más específico. Para el iniciador, se utiliza el perfil de la configuración o, si no se puede determinar, se utiliza la mejor coincidencia.

Un problema similar ocurre en escenarios que utilizan certificados diferentes para diferentes perfiles ISAKMP. La autenticación puede fallar debido a la validación del perfil 'ca trust-point' cuando se elige un certificado diferente. Este problema se tratará en un documento separado.

Los problemas descritos en este artículo no son problemas específicos de Cisco, sino que están relacionados con las limitaciones del diseño del protocolo IKEv1. IKEv1 utilizado con certificados no tiene estas limitaciones y IKEv2 utilizado tanto para claves previamente compartidas como para certificados no tiene estas limitaciones.

Información Relacionada

- Sección Certificate to ISAKMP Profile Mapping de la Guía de Configuración de Intercambio

de Claves de Internet para VPNs IPsec, Cisco IOS Release 15M&T

- ca trust-point a través de la sección clear eou de la Referencia de Comandos de Seguridad de Cisco IOS: Comandos A a C
- Soporte Técnico y Documentación - Cisco Systems