Reglas de selección IOS IKEv1/IKEv2 para los llaveros y los perfiles - guía de Troubleshooting

Contenido

Introducción

Este documento describe el uso de los llaveros múltiples para los perfiles múltiples del Internet Security Association and Key Management Protocol (ISAKMP) en un escenario de VPN del LAN a LAN del software del ® del Cisco IOS. Él cubre el comportamiento del Cisco IOS Software Release 15.3T así como los problemas potenciales cuando se utilizan los llaveros múltiples.

Dos escenarios se presentan, sobre la base de un túnel VPN con dos perfiles ISAKMP en cada router. Cada perfil tiene un diverso llavero con la misma dirección IP asociada. Los escenarios demuestran que el túnel VPN se puede iniciar solamente a partir de un lado de la conexión debido a la selección y la verificación del perfil.

Las siguientes secciones del documento resumen el Criterio de selección para el perfil del llavero para el iniciador del Internet Key Exchange (IKE) y el respondedor IKE. Cuando diversos IP Addresses son utilizados por el llavero en el respondedor IKE, la configuración trabaja correctamente, pero el uso de la misma dirección IP crea el problema presentado en el primer escenario.

Las secciones posteriores explican porqué la presencia de un llavero predeterminado (configuración global) y los llaveros específicos pudieron llevar a los problemas y porqué el uso

del protocolo del intercambio de claves de Internet versión 2 (IKEv2) evita ese problema.

Las secciones del final presentan el Criterio de selección para el perfil IKE para ambos para el iniciador IKE y el respondedor, junto con los errores frecuentes que ocurren cuando se selecciona un perfil incorrecto.

Configuración

> Notas:
>
> El analizador del CLI de Cisco (clientes registrados solamente) apoya los ciertos comandos show. Utilice el analizador del CLI de Cisco para ver una análisis de la salida del comando show.
>
> Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Topología

Interfaces virtuales de la interfaz del túnel del uso del router1 (r1) y del router2 (r2) (VTI) ([GRE] del Generic Routing Encapsulation) para acceder sus loopback. Ese VTI es protegido por la seguridad de protocolos en Internet (IPSec).

El r1 y el r2 tienen dos perfiles ISAKMP, cada uno con diverso llavero. Todos los llaveros tienen la misma contraseña.

Red del r1 y VPN

La configuración para la red del r1 y el 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 del r2 y VPN

La configuración para la red del r2 y el 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 llaveros utilizan el mismo IP Address de Peer y utilizan la contraseña “Cisco.”

En el r1, profile2 se utiliza para la conexión VPN. Profile2 es el segundo perfil en la configuración, que utiliza el segundo llavero en la configuración. Pues usted verá, la orden del llavero es crítica.

“Situaciones de ejemplo”

En el primer escenario, el r1 es el iniciador ISAKMP. El túnel está negociando correctamente, y el tráfico se protege como se esperaba.

El segundo escenario utiliza la misma topología, pero tiene r2 como el iniciador ISAKMP cuando la negociación phase1 está fallando.

La versión 1 (IKEv1) del intercambio de claves de Internet necesita una clave previamente compartida para el cálculo del skey, que se utiliza para desencriptar/cifra el paquete 5 (MM5) del modo principal y los paquetes subsiguientes IKEv1. El skey se deriva del cómputo del Diffie-Hellman (DH) y de la clave previamente compartida. Que la clave previamente compartida necesita ser determinada después de que MM3 (respondedor) o se recibe MM4 (iniciador), de modo que el skey, que se utiliza en MM5/MM6, puede ser computado.

Para el respondedor ISAKMP en MM3, el perfil específico ISAKMP todavía no se determina porque sucede ése después de que el IKEID se reciba en MM5. En lugar, todos los llaveros se buscan para una clave previamente compartida, y el primer o mejor que corresponde con llavero de la configuración global se selecciona. Ese llavero se utiliza para calcular el skey que se utiliza para el desciframiento de MM5 y el cifrado de MM6. Después del desciframiento de MM5 y después del perfil y del keyring asociado ISAKMP se determinan, el respondedor ISAKMP realiza la verificación si se ha seleccionado el mismo keyring; si el mismo llavero no se selecciona, se cae la conexión.

Así, para el respondedor ISAKMP, usted debe utilizar un solo llavero con las entradas múltiples siempre que sea posible.

R1 como iniciador IKE (correcto)

Este escenario describe qué ocurre cuando el r1 es el iniciador IKE:

1. Utilice estos debugs para el r1 y el r2:

```
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
```

2. El r1 inicia el túnel, envía el paquete MM1 con las propuestas de política, y recibe MM2 en la respuesta. MM3 entonces se prepara:

```
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, el r1 sabe que el ISAKMP profile2 debe ser utilizado porque está limitado bajo perfil de ipsec usado para ése VTI.

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

3. Cuando el r2 recibe ese paquete MM3, todavía no sabe qué perfil ISAKMP debe ser utilizado, pero necesita una clave previamente compartida para la generación DH. Por eso el r2 busca todos los llaveros 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 (keyring1).

4. El r2 entonces prepara el paquete MM4 con los cálculos DH y con la clave de “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 el r1 recibe MM4, prepara el paquete MM5 con IKEID y con la clave correcta seleccionada anterior (de 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. El paquete MM5, que contiene el IKEID de 192.168.0.1, es recibido por el r2. En este momento, el r2 sabe a qué perfil ISAKMP que el tráfico debe estar limitado (el **addresscommand de la identidad de la coincidencia**):

```
*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. El r2 ahora realiza la verificación si el llavero que fue seleccionado ciego para el paquete MM4 es lo mismo que el llavero configurado para el perfil ISAKMP ahora elegido. Porque keyring1 es primer en la configuración, fue seleccionado previamente, y ahora se selecciona. La validación es acertada, y el paquete MM6 puede ser enviado:

```
*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. El r1 recibe MM6 y no necesita realizar la verificación del llavero porque era sabido del primer paquete; el iniciador sabe siempre qué perfil ISAKMP a utilizar y qué llavero se asocia a ese perfil. La autenticación es acertada, y Phase1 acaba 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. Phase2 comienza normalmente y se completa con éxito.

Este escenario trabaja correctamente solamente debido a la pedido correcta de los llaveros definida en el r2. El perfil que se debe utilizar para la sesión de VPN utiliza el llavero que era primer en la configuración.

R2 como iniciador IKE (incorrecto)

Este escenario describe qué ocurre cuando el r2 inicia el mismo túnel y explica porqué el túnel no será establecido. Algunos registros se han quitado para centrarse en las diferencias entre esto y el ejemplo anterior:

1. El r2 inicia el túnel:

```
*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
```

2. Puesto que el r2 es el iniciador, se saben el perfil y el llavero ISAKMP. La clave previamente compartida de keyring1 se utiliza para los cómputos DH y se envía en MM3. El r2 está recibiendo MM2 y está preparando MM3 basado 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. El r1 recibe MM3 del r2. En esta etapa, el r1 no sabe qué perfil ISAKMP a utilizar, así que él no sabe qué llavero a utilizar. El r1 utiliza así el primer llavero de la configuración global, que es keyring1. El uso del r1 que clave previamente compartida para los cómputos 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. El r2 recibe MM4 del r1, utiliza la clave previamente compartida de keyring1 para computar el 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. El r1 recibe MM5 del r1. Porque el IKEID iguala 192.168.0, se ha seleccionado profile2. Se selecciona Keyring2 se ha configurado en profile2 así que keyring2. Previamente, para el cómputo DH en MM4, el r1 seleccionó el primer llavero configurado, que era keyring1. Aunque las contraseñas son exactamente lo mismo, la validación para el llavero falla porque éstos son diversos objetos del llavero:

```
*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 para diversa clave previamente compartida

Los escenarios previos utilizaron la misma clave (“Cisco "). Así, incluso cuando el llavero incorrecto fue utilizado, el paquete MM5 se podría desencriptar correctamente y caer más adelante debido al error de la validación del llavero.

En los escenarios donde se utilizan diversas claves, MM5 no puede ser desencriptado, y este mensaje de error aparece:

```
*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
```

Criterio de selección del llavero

Éste es un resumen del Criterio de selección del llavero. Vea las siguientes secciones para los detalles adicionales.

	Iniciador	Respondedor
Llaveros múltiples con	Configurado. Si no configuró explícitamente el más específico de la configuración	La coincidencia más específica

diversos IP Addresses Llaveros múltiples con los mismos IP Addresses	Configurado. Si no la **configuración** explícitamente configurada **se imprevisible y se soporta. Uno no debe configurar dos claves para la misma dirección IP.**	**La configuración se imprevisible soporta. Uno no debe configurar claves para la misma dirección I**

Esta sección también describe porqué la presencia de un llavero predeterminado (configuración global) y los llaveros específicos pudo llevar a los problemas y explica porqué el uso del protocolo IKEv2 evita tales problemas.

Orden de selección del llavero en el iniciador IKE

Para la configuración con un VTI, el iniciador utiliza una interfaz del túnel específica esas puntas al perfil de ipsec específico. Porque el perfil de ipsec utiliza un perfil específico IKE con un llavero específico, no hay confusión sobre la cual llavero a utilizar.

el Crypto-mapa, que también señala a un perfil específico IKE con un llavero específico, funciona de la misma manera.

Sin embargo, no es siempre posible determinar de la configuración que keyring a utilizar. Por ejemplo, esto ocurre cuando no hay perfil IKE configurado - es decir, el perfil de ipsec no se configura para utilizar el perfil IKE:

```
*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
```

Si este iniciador IKE intenta enviar MM1, elegirá el llavero 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
```

Puesto que el iniciador no tiene ningún perfil IKE configurado cuando recibe MM6, no golpeará un perfil y completará con la autenticación satisfactoria y el 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
```

Orden de selección del llavero en el respondedor IKE - Diversos IP Addresses

El problema con la selección del llavero está en el respondedor. Cuando los llaveros utilizan diversos IP Addresses, el orden de selección es simple.

Asuma que el respondedor IKE tiene esta configuración:

```
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
```

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

Los criterios para el orden de selección son:

1. Solamente las claves con una dirección IP se consideran.
2. El ruteo virtual y la expedición (VRF) del paquete entrante se marca ([fVRF] del extremo frontal VRF).
3. Si el paquete está en el valor por defecto VRF, el llavero global se marca primero. Se selecciona la clave más exacta (longitud del netmask).
4. Si no se encuentra ninguna clave en el llavero predeterminado, se concatenan todos los llaveros que hacen juego este fVRF.
5. Se corresponde con la clave más exacta (el netmask más largo). Por ejemplo, /32 se prefiere sobre /24.

Los debugs 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 del llavero en el respondedor IKE - Los mismos IP Addresses

Cuando los llaveros utilizan los mismos IP Addresses, los problemas ocurren. Asuma que el respondedor IKE tiene esta configuración:

```
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
```

Esta configuración se imprevisible y se soporta. Uno no debe configurar dos claves para la misma dirección IP o el problema descrito en el r2 que ocurrirá el iniciador IKE (incorrecto).

Configuración global del llavero

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

```
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
```

Aunque la clave ISAKMP es la más reciente de la configuración, se procesa como el primer 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
```

Así, el uso de la configuración global y de los llaveros específicos es muy aventurado y pudo llevar a los problemas.

Llavero en IKEv2 - El problema no ocurre

Aunque el protocolo IKEv2 utilice los conceptos similares a IKEv1, la selección del llavero no causa los problemas similares.

En los casos simples, hay apenas cuatro paquetes intercambiados. El IKEID que determina que el perfil IKEv2 se debe seleccionar en el respondedor es enviado por el iniciador en el tercer paquete. El tercer paquete se cifra ya.

La diferencia más grande de los dos protocolos es que IKEv2 utiliza solamente el resultado DH para el cómputo del skey. La clave previamente compartida es no más necesaria para computar el skey usado para encripción/desencripción.

El IKEv2 RFC (5996, la sección 2.14), estado:

Las claves compartidas se computan como sigue. Una cantidad llamada SKEYSEED se calcula del nonces intercambiado durante el intercambio IKE_SA_INIT y el secreto compartido de Diffie Hellman establecidos durante ese intercambio.

En la misma sección, RFC las notas también:

```
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
```

Toda la información necesaria se envía en los primeros dos paquetes, y no hay necesidad de

utilizar una clave previamente compartida cuando se calcula SKEYSEED.

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

SKEYID es una cadena derivada del material secreto sabido solamente a los jugadores activos en el intercambio.

Ese “material secreto sabido solamente a los jugadores activos” es la clave previamente compartida. En la sección 5, RFC las notas también:

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

Esto explica porqué el diseño IKEv1 para las claves previamente compartidas causa tan muchos problemas. Estos problemas no existen en IKEv1 cuando los Certificados se utilizan para la autenticación.

Criterio de selección del perfil IKE

Éste es un resumen del Criterio de selección del perfil IKE. Vea las siguientes secciones para los detalles adicionales.

	Iniciador	Respondedor
Selección del perfil	Debe ser configurada (fije en el perfil de ipsec o en la correspondencia de criptografía). Si no coincidencia configurada, primera de la configuración. El peer remoto debe hacer juego solamente un perfil específico ISAKMP, si la identidad del par se corresponde con en dos perfiles ISAKMP, la configuración es inválido.	Primera coincidencia de la configuración. El peer remoto debe hacer juego solamen un perfil específico ISAKMP, si la identida del par se corresponde con en dos perfile ISAKMP, la configuración es inválido.

Esta sección también describe los errores frecuentes que ocurren cuando un perfil incorrecto fue seleccionado.

Orden de selección del perfil IKE en el iniciador IKE

La interfaz VTI señala generalmente a un perfil de ipsec específico con un perfil específico IKE. El router entonces sabe qué perfil IKE a utilizar.

Semejantemente, el crypto-mapa señala a un perfil específico IKE, y el router sabe qué perfil a utilizar debido a la configuración.

Sin embargo, pudo haber los escenarios donde el perfil no se especifica y donde no está posible determinar directamente de la configuración que perfilan para utilizar; en este ejemplo, no se selecciona ningún perfil IKE en el perfil de ipsec:

```
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
```

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 del perfil IKE en el respondedor IKE

El orden de selección del perfil en un respondedor IKE es similar al orden de selección del llavero, donde el más específico toma la precedencia.

Asuma 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 una conexión de 192.168.0.1 se recibe, profile2 será seleccionado.

La orden de los perfiles configurados no importa. El comando show runnning-config pone cada nuevo perfil configurado en el extremo de la lista.

A veces el respondedor pudo tener dos perfiles IKE que utilizan el mismo llavero. Si un perfil incorrecto se selecciona en el respondedor pero el llavero seleccionado está correcto, la autenticación acabará 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 valida la oferta QM e intenta generar seguridad IPSec los índices del parámetro (SPI). En este ejemplo, algunos debugs fueron quitados para mayor clareza:

```
*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 momento, el respondedor falla y señala que el perfil correcto ISAKMP no hizo juego:

```
 (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 vuelve el error 32, y el respondedor envía el mensaje PROPOSAL_NOT_CHOSEN.

Resumen

Para IKEv1, una clave previamente compartida se utiliza con los resultados DH para calcular el skey usado para el cifrado que comienza en MM5. Después de que reciba MM3, el receptor ISAKMP no puede todavía determinar que el perfil ISAKMP (y el keyring asociado) deben ser utilizados porque el IKEID se envía en MM5 y MM6.

El resultado es que el respondedor ISAKMP intenta buscar a través de todos los llaveros global definidos para encontrar la clave para el par específico. Para diversos IP Addresses, se selecciona el mejor llavero que corresponde con (el más específico); para la misma dirección IP, el primer cerrar que corresponde con de la configuración se utiliza. El llavero se utiliza para calcular el skey que se utiliza para el desciframiento de MM5.

Después de que reciba MM5, el iniciador ISAKMP determina el perfil ISAKMP y el keyring asociado. El iniciador realiza la verificación si éste es el mismo llavero que fue seleccionado para el cómputo MM4 DH; si no, la conexión falla.

La pedido de los llaveros configurados en configuración global es crítica. Así, para el respondedor ISAKMP, utilice un solo llavero con las entradas múltiples siempre que sea posible.

Las claves previamente compartidas que se definen en el modo de configuración global pertenecen a un llavero predefinido llamado omiten. Las mismas reglas entonces se aplican.

Para la selección del perfil IKE para el respondedor, se corresponde con el perfil más específico. Para el iniciador, el perfil de la configuración se utiliza, o, si eso no puede ser determinada, se utiliza el mejor emparejamiento.

Un problema similar ocurre en los escenarios que utilizan diversos Certificados para diversos perfiles ISAKMP. La autenticación pudo fallar debido a “la validación del perfil de la confianza-punta Ca” cuando se elige un diverso certificado. Este problema será cubierto en un documento aparte.

Los problemas descritos en este artículo no son problemas del Cisco específico, sino se relacionan con las limitaciones del diseño del protocolo IKEv1. IKEv1 usado con los Certificados no tiene estas limitaciones, e IKEv2 usado para ambas claves previamente compartidas y Certificados no tiene estas limitaciones.

Información Relacionada

- Certificado a la sección de la asignación del perfil ISAKMP del intercambio de claves de Internet para la guía de configuración del IPSec VPN, Cisco IOS Release 15M&T
- confianza-punta Ca a través de la sección clara del eou de la referencia de comandos de la Seguridad de Cisco IOS: Comandos A al C
- Soporte Técnico y Documentación - Cisco Systems