Regole di selezione IOS IKEv1/IKEv2 per keyring e profili - Guida alla risoluzione dei problemi

Sommario

Introduzione

Questo documento descrive l'uso di più portachiavi per più profili Internet Security Association e Key Management Protocol (ISAKMP) in uno scenario VPN da LAN a LAN con software Cisco IOS®. Illustra il comportamento del software Cisco IOS versione 15.3T e i potenziali problemi quando si usano più portachiavi.

Vengono presentati due scenari, basati su un tunnel VPN con due profili ISAKMP su ciascun router. Ogni profilo ha un keyring diverso con lo stesso indirizzo IP collegato. Gli scenari dimostrano che il tunnel VPN può essere avviato solo da un lato della connessione a causa della selezione e della verifica del profilo.

Nelle sezioni seguenti del documento vengono riepilogati i criteri di selezione per il profilo di codifica per l'iniziatore IKE (Internet Key Exchange) e il risponditore IKE. Quando il keyring del risponditore IKE utilizza indirizzi IP diversi, la configurazione funziona correttamente, ma l'uso dello stesso indirizzo IP crea il problema illustrato nel primo scenario.

Nelle sezioni seguenti vengono illustrati i motivi per cui la presenza di un keyring predefinito

(configurazione globale) e di keyring specifici potrebbe causare problemi e il motivo per cui l'utilizzo del protocollo IKEv2 (Internet Key Exchange versione 2) consente di evitare tali problemi.

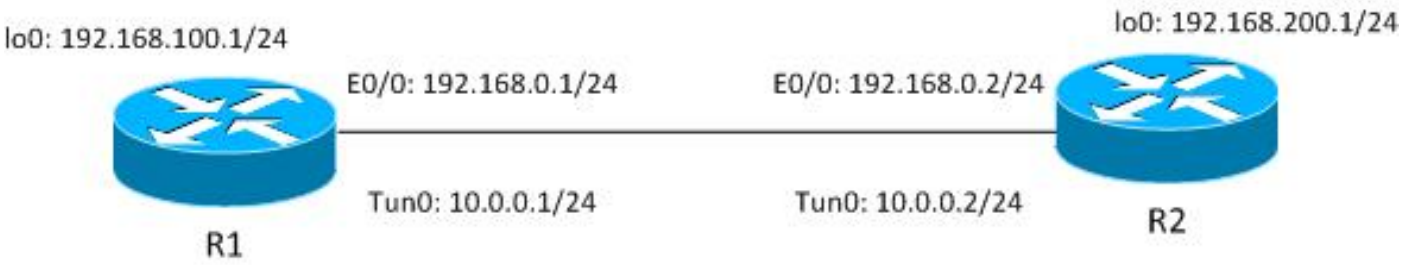
Nelle sezioni finali vengono illustrati i criteri di selezione per il profilo IKE sia per l'iniziatore IKE che per il risponditore, insieme agli errori tipici che si verificano quando viene selezionato un profilo errato.

Configurazione

> **Note:**
>
> Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi **show.** Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando **show**.
>
> consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Topologia

Il router1 (R1) e il router2 (R2) utilizzano le interfacce Virtual Tunnel Interface (VTI) (Generic Routing Encapsulation [GRE]) per accedere ai propri loopback. La VTI è protetta da IPSec (Internet Protocol Security).



Sia R1 che R2 hanno due profili ISAKMP, ciascuno con un keyring diverso. Tutti i portachiavi hanno la stessa password.

Rete R1 e VPN

La configurazione per la rete R1 e la VPN è:

```
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
```

Rete R2 e VPN

La configurazione per la rete R2 e la VPN è:

```
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
```

Tutte le stringhe di chiave utilizzano lo stesso indirizzo IP peer e la password ' cisco'.

In R1, il profilo2 viene utilizzato per la connessione VPN. Profile2 è il secondo profilo della configurazione che utilizza il secondo anello di chiave della configurazione. Come vedrete, l'ordine dei keyring è critico.

Scenari di esempio

Nel primo scenario, R1 è l'iniziatore ISAKMP. Il tunnel sta negoziando correttamente e il traffico è protetto come previsto.

Il secondo scenario utilizza la stessa topologia, ma ha R2 come iniziatore ISAKMP quando la negoziazione di fase 1 non riesce.

Per il calcolo della chiave non crittografata, è necessaria una chiave già condivisa IKEv1 (Internet Key Exchange versione 1), utilizzata per decrittografare/crittografare il pacchetto 5 (MM5) della modalità principale e i pacchetti IKEv1 successivi. Lo schema è derivato dal calcolo Diffie-Hellman (DH) e dalla chiave già condivisa. Tale chiave precondivisa deve essere determinata dopo la ricezione di MM3 (risponditore) o MM4 (iniziatore), in modo che sia possibile calcolare lo skey, utilizzato in MM5/MM6.

Per il risponditore ISAKMP in MM3, il profilo ISAKMP specifico non è ancora determinato perché ciò accade dopo la ricezione di IKEID in MM5. Al contrario, viene eseguita la ricerca di una chiave già condivisa in tutti gli anelli di chiave e viene selezionato il primo anello di chiave corrispondente o migliore dalla configurazione globale. Tale sequenza di tasti viene utilizzata per calcolare la chiave utilizzata per la decrittazione di MM5 e la crittografia di MM6. Dopo la decrittazione di MM5 e dopo la determinazione del profilo ISAKMP e della sequenza di tasti associata, il risponditore ISAKMP esegue la verifica se è stata selezionata la stessa sequenza di tasti; se la stessa sequenza di tasti non è selezionata, la connessione viene interrotta.

Pertanto, per il risponditore ISAKMP, è consigliabile utilizzare un singolo keyring con più voci quando possibile.

R1 Come iniziatore IKE (corretto)

In questo scenario viene descritto ciò che si verifica quando R1 è l'iniziatore IKE:

1. Utilizzare i seguenti debug per R1 e R2:

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

2. R1 avvia il tunnel, invia il pacchetto MM1 con le proposte di criteri e riceve in risposta MM2. Si prepara quindi il 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
```

Fin dall'inizio, R1 è consapevole della necessità di utilizzare il profilo ISAKMP2 in quanto associato al profilo IPSec utilizzato per tale VTI.

Pertanto, è stato selezionato il keyring corretto (keyring2). La chiave già condivisa da keyring2 viene utilizzata come materiale per le chiavi per i calcoli DH durante la preparazione del pacchetto MM3.

3. Quando R2 riceve il pacchetto M3, non sa ancora quale profilo ISAKMP utilizzare, ma ha bisogno di una chiave già condivisa per la generazione di DH. Per questo motivo R2 esegue una ricerca in tutti gli anelli di chiave per trovare la chiave già condivisa per il peer:

```
*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 chiave per 192.168.0.1 è stata trovata nel primo keyring definito (keyring1).

4. R2 quindi prepara il pacchetto M4 con calcoli DH e con la chiave 'cisco' di 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. Quando R1 riceve MM4, prepara il pacchetto MM5 con IKEID e con la chiave corretta selezionata in precedenza (da 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. Il pacchetto M5, che contiene l'IKEID 192.168.0.1, viene ricevuto da R2. A questo punto, R2 sa a quale profilo ISAKMP deve essere associato il traffico (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 ora esegue la verifica se il keyring selezionato ciecamente per il pacchetto M4 è lo stesso del keyring configurato per il profilo ISAKMP scelto. Poiché keyring1 è il primo nella configurazione, è stato selezionato in precedenza e ora è selezionato. La convalida ha esito positivo ed è possibile inviare il pacchetto 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 riceve MM6 e non deve eseguire la verifica del keyring perché era noto dal primo pacchetto; l'iniziatore è sempre a conoscenza del profilo ISAKMP da utilizzare e della sequenza di tasti associata al profilo. L'autenticazione ha esito positivo e la fase 1 termina correttamente:

```
*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 si avvia normalmente e viene completata correttamente.

Questo scenario funziona correttamente solo a causa dell'ordine corretto delle stringhe di chiave definite in R2. Il profilo da utilizzare per la sessione VPN utilizza la sequenza di chiavi specificata per prima nella configurazione.

R2 come iniziatore IKE (errato)

In questo scenario viene descritto ciò che si verifica quando R2 avvia lo stesso tunnel e viene spiegato perché il tunnel non verrà stabilito. Alcuni registri sono stati rimossi per evidenziare le differenze tra questo e l'esempio precedente:

1. R2 avvia il tunnel:

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

2. Poiché R2 è l'iniziatore, il profilo ISAKMP e il keyring sono noti. La chiave già condivisa da keyring1 viene utilizzata per i calcoli DH e inviata in MM3. R2 riceve MM2 e prepara MM3 in base a tale chiave:

```
*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 riceve MM3 da R2. In questa fase, R1 non sa quale profilo ISAKMP utilizzare, quindi non sa quale anello di chiavi utilizzare. R1 utilizza quindi il primo keyring della configurazione globale, ovvero keyring1. R1 utilizza tale chiave precondivisa per i calcoli DH e invia 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 riceve MM4 da R1, utilizza la chiave già condivisa da keyring1 per calcolare DH e prepara il pacchetto MM5 e l'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 riceve MM5 da R1. Poiché IKEID è uguale a 192.168.0, è stato selezionato profilo2. Keyring2 è stato configurato nel profilo2, quindi keyring2 è selezionato. In precedenza, per il calcolo DH in MM4, R1 aveva selezionato il primo anello di chiavi configurato, ovvero keyring1. Anche se le password sono esattamente le stesse, la convalida per il keyring ha esito negativo perché si tratta di oggetti keyring diversi:

```
*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
```

Debug di una chiave già condivisa diversa

Negli scenari precedenti è stata utilizzata la stessa chiave ('cisco'). Pertanto, anche quando è stato utilizzato il keyring errato, il pacchetto M5 poteva essere decriptato correttamente e scartato in seguito a causa di un errore di convalida del keyring.

Negli scenari in cui vengono utilizzate chiavi diverse, non è possibile decrittografare MM5 e viene visualizzato questo messaggio di errore:

```
*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
```

Criteri di selezione keyring

Riepilogo dei criteri di selezione della sequenza di chiavi. Per ulteriori informazioni, vedere le sezioni successive.

	Iniziatore	Risponditore
Anelli multipli con diversi indirizzi IP	Configurato. Se non è configurato in modo esplicito il più specifico dalla configurazione	La corrispondenza più specifica
Porzioni multiple con gli stessi indirizzi IP	Configurato. Se non configurato esplicitamente **diventa imprevedibile e non è supportata. Non è consigliabile configurare due chiavi per lo stesso indirizzo IP.**	**La configurazione diventa imprevedibil non supportata. Non è consigliabile configurare due chiavi per lo stesso indirizzo IP.**

In questa sezione viene inoltre descritto perché la presenza di un keyring predefinito (configurazione globale) e di keyring specifici potrebbe causare problemi e viene spiegato perché l'uso del protocollo IKEv2 consente di evitare tali problemi.

Ordine di selezione del keyring sull'iniziatore IKE

Per la configurazione con una VTI, l'iniziatore utilizza un'interfaccia tunnel specifica che punta a un profilo IPSec specifico. Poiché il profilo IPSec utilizza un profilo IKE specifico con un keyring specifico, non vi è confusione sul keyring da utilizzare.

La mappa crittografica, che punta anche a un profilo IKE specifico con un keyring specifico, funziona allo stesso modo.

Tuttavia, non è sempre possibile determinare dalla configurazione quale keyring utilizzare. Questo si verifica, ad esempio, quando non è configurato alcun profilo IKE, ovvero il profilo IPSec non è configurato per l'utilizzo del profilo 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
```

Se l'iniziatore IKE tenta di inviare MM1, sceglierà il keyring più specifico:

```
*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
```

Poiché l'iniziatore non dispone di profili IKE configurati quando riceve MM6, non toccherà un profilo e verrà completata con autenticazione e modalità rapida riuscite:

```
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
```

Ordine di selezione del keyring per il risponditore IKE - Indirizzi IP diversi

Il problema con la selezione del keyring si verifica nel risponditore. Quando le stringhe di chiave utilizzano indirizzi IP diversi, l'ordine di selezione è semplice.

Si supponga che il risponditore IKE disponga della configurazione seguente:

```
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
```

Quando il risponditore riceve il pacchetto MM1 dall'iniziatore IKE con indirizzo IP 192.168.0.2, sceglie la corrispondenza migliore (più specifica), anche se l'ordine nella configurazione è diverso.

I criteri per l'ordine di selezione sono:

1. Vengono prese in considerazione solo le chiavi con un indirizzo IP.
2. Viene controllato il routing e l'inoltro virtuale (VRF) del pacchetto in arrivo (VRF [fVRF] front-end).
3. Se il pacchetto si trova nel VRF predefinito, il keyring globale viene controllato per primo. Viene selezionata la chiave più precisa (lunghezza maschera di rete).
4. Se non viene trovata alcuna chiave nel keyring predefinito, vengono concatenati tutti i keyring che corrispondono a questo fVRF.
5. Viene stabilita una corrispondenza con la chiave più precisa (maschera di rete più lunga). Ad esempio, si preferisce l'opzione /32 anziché /24.

I debug confermano la selezione:

```
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
```

Ordine di selezione del keyring per il risponditore IKE - Stessi indirizzi IP

Quando i portachiavi utilizzano gli stessi indirizzi IP, si verificano problemi. Si supponga che il risponditore IKE disponga della configurazione seguente:

```
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
```

Questa configurazione diventa imprevedibile e non è supportata. Non configurare due chiavi per lo stesso indirizzo IP o si verificherà il problema descritto in R2 come iniziatore IKE (errato).

Configurazione globale keyring

Le chiavi ISAKMP definite nella configurazione globale appartengono al keyring predefinito:

```
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
```

Anche se la chiave ISAKMP è l'ultima della configurazione, viene elaborata come la prima sul risponditore 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
```

Pertanto, l'utilizzo sia della configurazione globale che di keyring specifici è molto rischioso e potrebbe causare problemi.

Apertura di chiavi su IKEv2 - Il problema non si verifica

Sebbene il protocollo IKEv2 utilizzi concetti simili a quelli di IKEv1, la selezione tramite sequenza di tasti non causa problemi simili.

In alcuni semplici casi, vengono scambiati solo quattro pacchetti. L'IKEID che determina quale profilo IKEv2 deve essere selezionato sul risponditore viene inviato dall'iniziatore nel terzo pacchetto. Il terzo pacchetto è già crittografato.

La differenza maggiore tra i due protocolli consiste nel fatto che IKEv2 utilizza solo il risultato DH per il calcolo skey. La chiave già condivisa non è più necessaria per calcolare la chiave utilizzata

per la crittografia/decrittografia.

La RFC IKEv2 (5996, sezione 2.14), afferma:

Le chiavi condivise vengono calcolate come segue. Una quantità chiamata SKEYSEED viene calcolata in base ai nonce scambiati durante lo scambio IKE_SA_INIT e al segreto condiviso Diffie-Hellman stabilito durante tale scambio.

Nella stessa sezione, l'RFC nota anche:

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

Tutte le informazioni necessarie vengono inviate nei primi due pacchetti e non è necessario utilizzare una chiave già condivisa quando viene calcolato SKEYSEED.

Confrontare questo dato con quello della RFC IKE (2409, sezione 3.2), che afferma:

SKEYID è una stringa derivata da materiale segreto noto solo ai giocatori attivi nello scambio.

Questo "materiale segreto noto solo ai giocatori attivi" è la chiave pre-condivisa. Nella sezione 5, l'RFC indica anche:

Per le chiavi già condivise: SKEYID = prf(**pre-shared-key**, Ni_b | Nr_b)

Questo spiega perché la progettazione di IKEv1 per le chiavi già condivise causa così tanti problemi. Questi problemi non esistono in IKEv1 quando si utilizzano i certificati per l'autenticazione.

Criteri di selezione profilo IKE

Riepilogo dei criteri di selezione del profilo IKE. Per ulteriori informazioni, vedere le sezioni successive.

	Iniziatore	Risponditore
Selezione profilo	Deve essere configurato (impostato nel profilo IPSec o nella mappa crittografica). Se non è configurato, individuare prima la corrispondenza dalla configurazione. Il peer remoto deve corrispondere solo a un profilo ISAKMP specifico. Se l'identità del peer viene abbinata in due profili ISAKMP, la configurazione non è valida.	Prima corrispondenza dalla configurazione. Il peer remoto deve corrispondere solo a un prof ISAKMP specifico. Se l'identità del peer viene abbinata in due profili ISAKMP, la configurazione non è valida.

In questa sezione vengono inoltre descritti gli errori tipici che si verificano quando viene selezionato un profilo non corretto.

Ordine di selezione del profilo IKE sull'iniziatore IKE

L'interfaccia VTI in genere punta a un profilo IPSec specifico con un profilo IKE specifico. Il router può quindi conoscere il profilo IKE da utilizzare.

Analogamente, la mappa crittografica punta a un profilo IKE specifico e il router sa quale profilo

utilizzare a causa della configurazione.

Tuttavia, possono verificarsi scenari in cui il profilo non è specificato e non è possibile determinare direttamente dalla configurazione quale profilo utilizzare; nell'esempio seguente non viene selezionato alcun profilo IKE nel profilo 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
```

Quando questo iniziatore tenta di inviare un pacchetto MM1 a 192.168.0.2, viene selezionato il profilo più specifico:

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

Ordine di selezione del profilo IKE nel risponditore IKE

L'ordine di selezione del profilo su un risponditore IKE è simile all'ordine di selezione del keyring, in cui ha la precedenza il più specifico.

Si supponga che la configurazione

```
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
```

Quando si riceve una connessione da 192.168.0.1, viene selezionato il profilo 2.

L'ordine dei profili configurati non ha importanza. Il comando **show running-config** posiziona ciascun profilo configurato alla fine dell'elenco.

A volte il risponditore potrebbe avere due profili IKE che usano lo stesso keyring. Se sul risponditore è selezionato un profilo errato ma il keyring selezionato è corretto, l'autenticazione verrà completata correttamente:

```
*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
```

Il risponditore riceve e accetta la proposta QM e tenta di generare gli SPI (Security Parameter Indexes) di IPSec. Nell'esempio riportato di seguito, alcuni debug sono stati rimossi per maggiore chiarezza:

```
*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
```

A questo punto, il risponditore non riesce e segnala che il profilo ISAKMP corretto non corrisponde:

```
 (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
```
A causa della selezione errata del profilo IKE, viene restituito l'errore 32 e il risponditore invia il messaggio PROPOS_NOT_CHOSEN.

Riepilogo

Per IKEv1, viene utilizzata una chiave già condivisa con i risultati DH per calcolare la chiave utilizzata per la crittografia che inizia da MM5. Dopo la ricezione di MM3, il ricevitore ISAKMP non è ancora in grado di determinare quale profilo ISAKMP (e il relativo keyring) utilizzare perché l'IKEID viene inviato in MM5 e MM6.

Il risultato è che il risponditore ISAKMP cerca di cercare tra tutti i keyring definiti globalmente per trovare la chiave per un peer specifico. Per diversi indirizzi IP, viene selezionato il keyring più corrispondente (il più specifico); per lo stesso indirizzo IP, viene utilizzata la prima chiave corrispondente della configurazione. Il keyring è usato per calcolare il cieco usato per la decrittografia di MM5.

Dopo aver ricevuto MM5, l'iniziatore ISAKMP determina il profilo ISAKMP e il relativo keyring. L'iniziatore esegue la verifica se si tratta dello stesso keyring selezionato per il calcolo DH MM4; in caso contrario, la connessione non riesce.

L'ordine delle stringhe di chiave configurate nella configurazione globale è critico. Pertanto, per il risponditore ISAKMP, utilizzare un singolo keyring con più voci quando possibile.

Le chiavi già condivise definite nella modalità di configurazione globale appartengono a un keyring predefinito denominato default. In tal caso valgono le stesse regole.

Per la selezione del profilo IKE per il risponditore, viene trovato il profilo più specifico. Per l'iniziatore viene utilizzato il profilo della configurazione oppure, se non è possibile determinarlo, viene utilizzata la corrispondenza migliore.

Un problema simile si verifica in scenari che utilizzano certificati diversi per profili ISAKMP diversi. L'autenticazione potrebbe non riuscire a causa della convalida del profilo 'ca trust-point' quando viene scelto un certificato diverso. Questo problema sarà trattato in un documento separato.

I problemi descritti in questo articolo non sono specifici di Cisco, ma sono relativi alle limitazioni della progettazione del protocollo IKEv1. IKEv1 utilizzato con i certificati non presenta queste limitazioni e IKEv2 utilizzato sia per le chiavi già condivise che per i certificati non presenta tali limitazioni.

Informazioni correlate

- Sezione Certificate to ISAKMP Profile Mapping della Guida alla configurazione di Internet Key Exchange for IPsec VPN, Cisco IOS release 15M&T
- ca trust-point tramite la sezione clear eou della guida di riferimento dei comandi di Cisco IOS Security: Comandi da A a C
- Documentazione e supporto tecnico – Cisco Systems