키링 및 프로파일에 대한 IOS IKEv1/IKEv2 선택 규칙 - 트러블슈팅 가이드

목차

소개

이 문서에서는 Cisco IOS® 소프트웨어 LAN-to-LAN VPN 시나리오에서 여러 ISAKMP(Internet Security Association and Key Management Protocol) 프로파일에 대해 여러 키를 사용하는 방법에 대해 설명합니다.Cisco IOS Software Release 15.3T의 동작 및 여러 키링이 사용될 때 발생할 수 있는 문제를 다룹니다.

각 라우터에 2개의 ISAKMP 프로필이 있는 VPN 터널을 기반으로 두 가지 시나리오가 제시됩니다.각 프로필에는 동일한 IP 주소가 연결된 다른 키가 있습니다.이 시나리오에서는 프로파일 선택 및 확인 때문에 연결의 한 쪽에서만 VPN 터널을 시작할 수 있음을 보여줍니다.

문서의 다음 섹션에서는 IKE(Internet Key Exchange) 개시자와 IKE 응답자 모두에 대한 키 링 프로파일의 선택 기준을 요약합니다.IKE 응답기의 키링에서 서로 다른 IP 주소를 사용하는 경우 컨피그레이션이 올바르게 작동하지만 동일한 IP 주소를 사용하면 첫 번째 시나리오에서 문제가 발생합니다.

다음 섹션에서는 기본 키(글로벌 컨피그레이션) 및 특정 키 링이 모두 있는 경우 문제가 발생할 수 있는 이유와 IKEv2(Internet Key Exchange Version 2) 프로토콜을 사용하는 경우 이 문제가 발생하지 않도록 하는 이유에 대해 설명합니다.

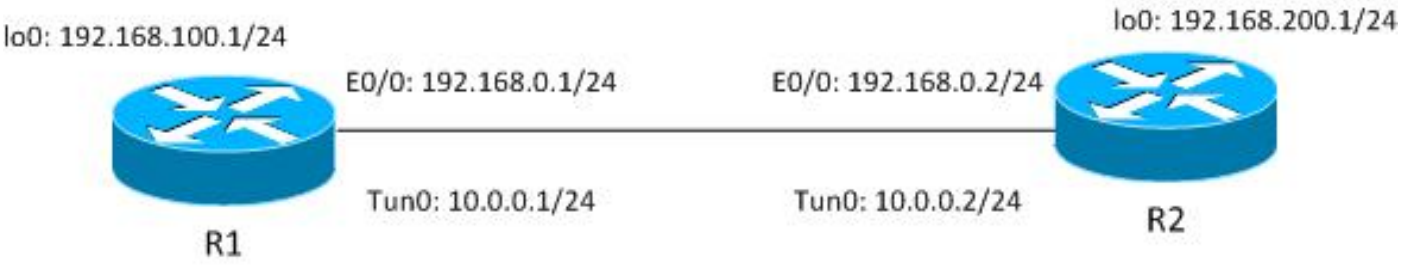
마지막 섹션에서는 IKE 개시자 및 응답자에 대한 IKE 프로파일의 선택 기준과 잘못된 프로파일을 선택할 때 발생하는 일반적인 오류를 보여줍니다.

구성

> **참고:**
>
> Cisco CLI Analyzer(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 Cisco CLI Analyzer를 사용합니다.
>
> **debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

토폴로지

라우터1(R1) 및 라우터2(R2)는 루프백에 액세스하기 위해 VTI(Virtual Tunnel Interface)(GRE[Generic Routing Encapsulation]) 인터페이스를 사용합니다.해당 VTI는 IPSec(Internet Protocol Security)에 의해 보호됩니다.



R1과 R2 모두 ISAKMP 프로파일 2개가 있으며 각각 다른 키링이 있습니다.모든 키에는 동일한 비밀번호가 있습니다.

R1 네트워크 및 VPN

R1 네트워크 및 VPN에 대한 컨피그레이션은 다음과 같습니다.

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

crypto isakmp profile profile1
   keyring keyring1
   match identity address 192.168.0.102 255.255.255.255 !non existing host
crypto isakmp profile profile2
   keyring keyring2
   match identity address 192.168.0.2 255.255.255.255 !R2
!
crypto ipsec transform-set TS esp-aes esp-sha256-hmac
```

```
 mode tunnel
!
crypto ipsec profile profile1
 set transform-set TS
 set isakmp-profile profile2
!
interface Loopback0
 description Simulate LAN
 ip address 192.168.100.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source Ethernet0/0
 tunnel destination 192.168.0.2
 tunnel protection ipsec profile profile1
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.

ip route 192.168.200.0 255.255.255.0 10.0.0.2
```

R2 네트워크 및 VPN

R2 네트워크 및 VPN에 대한 컨피그레이션은 다음과 같습니다.

```
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
```
모든 키링은 동일한 피어 IP 주소를 사용하며 비밀번호 ' cisco'를 사용합니다.

R1에서 profile2는 VPN 연결에 사용됩니다.Profile2는 컨피그레이션의 두 번째 프로필로, 컨피그레이션의 두 번째 키를 사용합니다.보시다시피, 키링 순서는 매우 중요합니다.

예제 시나리오

첫 번째 시나리오에서 R1은 ISAKMP 개시자입니다.터널이 올바르게 협상되고 있으며 트래픽은 예상대로 보호됩니다.

두 번째 시나리오는 동일한 토폴로지를 사용하지만, 1단계 협상이 실패할 경우 R2를 ISAKMP 개시자로 사용합니다.

IKEv1(Internet Key Exchange Version 1)에는 키 계산을 위한 사전 공유 키가 필요합니다. 이 키는 MM5(Main Mode packet 5) 및 후속 IKEv1 패킷의 암호 해독/암호화에 사용됩니다.키는 DH(Diffie-Hellman) 계산 및 사전 공유 키에서 파생됩니다.MM3(responder) 또는 MM4(개시자)를 수신한 후 사전 공유 키를 확인해야 MM5/MM6에서 사용되는 키를 계산할 수 있습니다.

MM3의 ISAKMP 응답기의 경우 IKE를 MM5에서 받은 후 발생하므로 특정 ISAKMP 프로파일이 아직 확인되지 않습니다. 대신 모든 키링에서 미리 공유된 키를 검색하고 전역 구성에서 첫 번째 또는 가장 일치하는 키를 선택합니다.이 키링은 MM5의 암호 해독 및 MM6의 암호화에 사용되는 키를 계산하는 데 사용됩니다. MM5의 암호 해독 후 ISAKMP 프로필 및 연결된 키 링이 확인된 후 ISAKMP 응답자는 동일한 키 링이 선택되었는지 여부를 확인합니다.동일한 키링을 선택하지 않으면 연결이 삭제됩니다.

따라서 ISAKMP 응답기의 경우 가능하면 여러 항목이 있는 단일 키링을 사용해야 합니다.

R1을 IKE 개시자로(수정)

이 시나리오에서는 R1이 IKE 개시자일 때 발생하는 상황을 설명합니다.

1. R1 및 R2 모두에 다음 디버그를 사용합니다.

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

2. R1은 터널을 시작하고 정책 제안과 함께 MM1 패킷을 전송하며 응답으로 MM2를 수신합니다.그런 다음 MM3을 준비합니다.

```
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
```

처음부터 R1은 ISAKMP 프로필2가 해당 VTI에 사용된 IPSec 프로필 아래에 바인딩되어 있으므로 사용해야 한다는 것을 알고 있습니다.

따라서 올바른 키(keyring2)가 선택되었습니다.keyring2의 사전 공유 키는 MM3 패킷이 준비될 때 DH 계산을 위한 키 자료로 사용됩니다.

3. R2에서 MM3 패킷을 수신하면 어떤 ISAKMP 프로필을 사용해야 할지 알 수 없지만 DH 생성을 위해 사전 공유 키가 필요합니다.따라서 R2는 해당 피어의 사전 공유 키를 찾기 위해 모든 키를 검색합니다.

```
*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
```

192.168.0.1의 키가 첫 번째 정의된 키(keyring1)에서 발견되었습니다.

4. 그런 다음 R2는 MM4 패킷을 DH 계산과 keyring1의 'cisco' 키로 준비합니다.

```
*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. R1이 MM4를 수신하면 IKEID가 있는 MM5 패킷과 이전 키(keyring2에서)에서 선택한 올바른 키를 준비합니다.

```
*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. 192.168.0.1의 IKEID를 포함하는 MM5 패킷이 R2에서 수신됩니다. 이 시점에서 R2는 어떤 ISAKMP 프로필에서 트래픽을 바인딩해야 하는지 확인합니다(match identity addresscommand).

```
*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. 이제 R2는 MM4 패킷에 대해 맹목적으로 선택된 키링이 현재 선택한 ISAKMP 프로파일에 대해 구성된 키링과 동일한지 확인합니다.keyring1은 컨피그레이션의 첫 번째 항목이므로 이전에 선택되었으며 지금 선택됩니다.검증이 성공적이며 MM6 패킷을 전송할 수 있습니다.

```
*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. R1은 MM6을 수신하며 첫 번째 패킷에서 알려졌으므로 키링에 대한 확인을 수행할 필요가 없습니다.개시자는 항상 어떤 ISAKMP 프로필을 사용할지, 어떤 키링이 해당 프로필과 연결되어 있는지 알고 있습니다.인증이 성공하고 1단계가 올바르게 완료되었습니다.

```
*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. 2단계가 정상적으로 시작되고 성공적으로 완료되었습니다.

이 시나리오는 R2에 정의된 키링의 올바른 순서 때문에 올바르게 작동합니다. VPN 세션에 사용해야 하는 프로파일은 컨피그레이션에서 처음 사용된 키링을 사용합니다.

R2를 IKE 개시자로(부정확함)

이 시나리오에서는 R2가 동일한 터널을 시작할 때 발생하는 것과 터널이 설정되지 않는 이유를 설명합니다.이 예와 이전 예제의 차이점에 집중하기 위해 일부 로그가 제거되었습니다.

1. R2는 터널을 시작합니다.

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

2. R2는 Initiator이므로 ISAKMP 프로필 및 키링을 알 수 있습니다.keyring1의 사전 공유 키는 DH 계산에 사용되며 MM3에서 전송됩니다. R2는 MM2를 수신하며 해당 키를 기반으로 MM3을 준비하고 있습니다.

```
*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. R1은 R2에서 MM3을 수신합니다. 이 단계에서 R1은 어떤 ISAKMP 프로파일을 사용해야 할지 알지 못하므로 어떤 키링을 사용해야 할지 알 수 없습니다.따라서 R1은 전역 구성의 첫 번째 키인 keyring1을 사용합니다. R1은 DH 계산에 사전 공유 키를 사용하고 MM4를 전송합니다.

```
*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. R2는 R1에서 MM4를 수신하고 keyring1에서 사전 공유 키를 사용하여 DH를 계산하고 MM5 패킷과 IKEID를 준비합니다.

```
*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. R1은 R1에서 MM5를 수신합니다. IKEID가 192.168.0이므로 profile2가 선택되었습니다 .keyring2가 profile2에서 구성되었으므로 keyring2가 선택됩니다.이전에는 MM4에서 DH 계산에 대해 R1이 keyring1인 구성된 첫 번째 키링을 선택했습니다. 비밀번호가 정확히 동일하더라도 키링에 대한 검증이 실패합니다. 이는 서로 다른 키링 객체이기 때문입니다.

```
*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
```

다른 사전 공유 키에 대한 디버깅

이전 시나리오는 동일한 키('cisco')를 사용했습니다. 따라서 잘못된 키링이 사용되었더라도 키링 검증 실패로 인해 MM5 패킷의 암호를 올바르게 해독하고 나중에 삭제할 수 있습니다.

다른 키를 사용하는 시나리오에서 MM5의 암호를 해독할 수 없으며 다음 오류 메시지가 나타납니다 .

```
*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
```

키 선택 기준

키 선택 기준의 요약입니다.자세한 내용은 다음 절을 참조하십시오.

	개시자	응답자
IP 주소가 다른 여러 키링	구성됨.컨피그레이션에서 가장 특정한 를 명시적으로 구성하지 않은 경우	가장 구체적인 일치
동일한 IP 주소를 사용하는 여러 키	구성됨.명시적으로 구성되지 않은 경우 **컨피그레이션은 예측할 수 없으며 지원되지 않습니다.동일한 IP 주소에 대해 두 개의 키를 구성해서는 안 됩니다.**	**컨피그레이션은 예측할 수 없으며 지원되지 않습니다.동일한 IP 주소에 대해 두 개의 키를 구성해서는 안 됩니다.**

이 섹션에서는 기본 키(글로벌 컨피그레이션) 및 특정 키 링이 모두 있는 경우 문제가 발생할 수 있는 이유와 IKEv2 프로토콜을 사용하는 경우 이러한 문제가 발생하지 않는 이유에 대해 설명합니다.

IKE Initiator의 키 선택 순서

VTI를 사용한 컨피그레이션의 경우 초기자는 특정 IPSec 프로파일을 가리키는 특정 터널 인터페이스를 사용합니다.IPSec 프로파일은 특정 키링이 있는 특정 IKE 프로파일을 사용하므로 어떤 키링을 사용해야 할지 혼동이 없습니다.

특정 키가 있는 특정 IKE 프로파일을 가리키는 암호화 맵도 동일한 방식으로 작동합니다.

그러나 어떤 키를 사용할지 컨피그레이션에서 항상 확인할 수는 없습니다.예를 들어, 구성된 IKE 프로파일이 없는 경우, 즉 IKE 프로파일을 사용하기 위해 IPSec 프로파일이 구성되지 않은 경우 이 오류가 발생합니다.

```
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
```

이 IKE 개시자가 MM1을 전송하려고 하면 가장 구체적인 키링을 선택합니다.

```
*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
```

초기자는 MM6을 수신할 때 구성된 IKE 프로파일이 없으므로 프로파일에 도달하지 않으며 성공적인 인증 및 빠른 모드(QM)로 완료됩니다.

```
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
```

IKE Responder의 키 선택 순서 - 다른 IP 주소

키 선택 시 문제가 응답기에 있습니다.키링이 다른 IP 주소를 사용하는 경우 선택 순서는 간단합니다.

IKE 응답자에게 다음 컨피그레이션이 있다고 가정합니다.

```
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
```

이 응답자는 IP 주소가 192.168.0.2인 IKE 개시자로부터 MM1 패킷을 받으면 컨피그레이션의 순서가 다른 경우에도 최상의 일치(가장 특정한) 일치를 선택합니다.

선택 순서의 기준은 다음과 같습니다.

1. IP 주소가 있는 키만 고려됩니다.
2. 수신 패킷의 VRF(Virtual Routing and Forwarding)가 선택됩니다(프런트엔드 VRF[fVRF]).
3. 패킷이 기본 VRF에 있는 경우 전역 키링이 먼저 선택됩니다.가장 정확한 키(넷마스크 길이)가 선택됩니다.
4. 기본 키링에 키가 없는 경우 이 fVRF와 일치하는 모든 키링이 연결됩니다.
5. 가장 정확한 키(가장 긴 넷마스크)가 일치합니다.예를 들어 /32가 /24보다 우선합니다.

디버그가 선택을 확인합니다.

```
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
```

IKE Responder에서 키 선택 순서 - 동일한 IP 주소

키링이 동일한 IP 주소를 사용하는 경우 문제가 발생합니다.IKE 응답자에게 다음 컨피그레이션이 있다고 가정합니다.

```
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
```

이 컨피그레이션은 예측할 수 없으며 지원되지 않습니다.동일한 IP 주소에 대해 두 개의 키를 구성하지 않아야 합니다. 그렇지 않으면 R2 As IKE Initiator(Incorrect)에 설명된 문제가 발생합니다.

전역 구성 키 지정

전역 컨피그레이션에 정의된 ISAKMP 키는 기본 키링에 속합니다.

```
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
```

ISAKMP 키가 컨피그레이션에서 마지막 키이지만 IKE 응답자에서 첫 번째 키로 처리됩니다.

```
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
```

따라서 글로벌 컨피그레이션과 특정 키링의 사용은 매우 위험하며 문제를 야기할 수 있습니다.

IKEv2의 키 링 - 문제가 발생하지 않음

IKEv2 프로토콜은 IKEv1과 유사한 개념을 사용하지만, 키 선택 시 유사한 문제가 발생하지 않습니다.

간단한 경우, 교환되는 패킷은 단 4개입니다.responder에서 어떤 IKEv2 프로필을 선택해야 할지 결정하는 IKEID는 세 번째 패킷에서 initiator가 전송합니다.세 번째 패킷은 이미 암호화되어 있습니다.

두 프로토콜의 가장 큰 차이점은 IKEv2는 키 계산에 DH 결과만 사용한다는 것입니다.암호화/암호 해독에 사용되는 키를 계산하기 위해 사전 공유 키가 더 이상 필요하지 않습니다.

IKEv2 RFC(5996, 섹션 2.14)는 다음과 같습니다.

공유 키는 다음과 같이 계산됩니다.SKEYSEED라는 수량은 IKE_SA_INIT 교환 중에 교환된 논리와 해당 교환 중에 설정된 Diffie-Hellman 공유 암호에서 계산됩니다.

동일한 섹션에서 RFC는 다음과 같은 내용도 기록합니다.

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

필요한 모든 정보는 처음 두 패킷에 전송되며 SKEYSEED를 계산할 때 사전 공유 키를 사용할 필요가 없습니다.

이를 다음과 같은 IKE RFC(2409, 섹션 3.2)와 비교합니다.

SKEYID는 교환의 활성 플레이어에게만 알려진 비밀 자료에서 파생된 문자열입니다.

이 "액티브 플레이어에게만 알려진 비밀 자료"는 사전 공유 키입니다.섹션 5에서 RFC는 다음과 같은 내용도 기록합니다.

사전 공유 키의 경우:SKEYID = prf(**사전 공유 키**, Ni_b) | Nr_b)

따라서 사전 공유 키에 대한 IKEv1 설계로 인해 많은 문제가 발생하는 이유를 설명합니다.인증서가 인증에 사용되는 경우 IKEv1에는 이러한 문제가 없습니다.

IKE 프로파일 선택 기준

IKE 프로필 선택 기준의 요약입니다.자세한 내용은 다음 절을 참조하십시오.

	개시자	응답자
프로필 선택	구성해야 합니다(IPSec 프로파일 또는 암호화 맵에서 설정). 구성되지 않은 경우 먼저 컨피그레이션에서 확인합니다. 원격 피어는 하나의 특정 ISAKMP 프로필만 매칭해야 합니다. 피어 ID가 두 ISAKMP 프로파일에서 매칭되는 경우 컨피그레이션이 유효하지 않습니다.	컨피그레이션에서 첫 번째 일치. 원격 피어는 하나의 특정 ISAKMP 프로필만 칭해야 합니다. 피어 ID가 두 ISAKMP 프로파에서 매칭되는 경우 컨피그레이션이 유효하지 않습니다.

이 섹션에서는 잘못된 프로파일을 선택할 때 발생하는 일반적인 오류에 대해서도 설명합니다.

IKE Initiator의 IKE 프로필 선택 순서

VTI 인터페이스는 일반적으로 특정 IKE 프로파일이 있는 특정 IPSec 프로파일을 가리킵니다.그러면 라우터가 사용할 IKE 프로필을 파악합니다.

마찬가지로, crypto-map은 특정 IKE 프로필을 가리키며, 라우터는 컨피그레이션 때문에 어떤 프로파일을 사용해야 하는지 알고 있습니다.

그러나 프로파일이 지정되지 않았고 사용할 프로파일을 컨피그레이션에서 직접 확인할 수 없는 경우도 있습니다.이 예에서는 IPSec 프로파일에서 IKE 프로파일이 선택되지 않았습니다.

```
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
```

이 이니시에이터가 MM1 패킷을 192.168.0.2에 전송하려고 하면 가장 구체적인 프로파일이 선택됩니다.

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

IKE Responder의 IKE 프로필 선택 순서

IKE 응답기의 프로파일 선택 순서는 가장 특정한 순서가 우선인 키 선택 순서와 유사합니다.

다음 컨피그레이션을 가정합니다.

```
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
```

192.168.0.1에서 연결을 받으면 profile2가 선택됩니다.

구성된 프로파일의 순서는 중요하지 않습니다.show running-config 명령은 새로 구성된 각 프로필을 목록의 끝에 배치합니다.

때로는 응답자에게 동일한 키 링을 사용하는 두 개의 IKE 프로파일이 있을 수 있습니다.응답자에서 잘못된 프로파일을 선택했지만 선택한 키가 올바르면 인증이 올바르게 완료됩니다.

```
*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
```

응답자는 QM 제안을 수신하고 수락하며 IPSec SPI(Security Parameter Indexes)를 생성하려고 시도합니다. 이 예제에서는 명확성을 위해 일부 디버그가 제거되었습니다.

```
*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
```

이 시점에서 responder가 실패하고 올바른 ISAKMP 프로파일이 일치하지 않음을 보고합니다.

```
 (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
```

잘못된 IKE 프로필 선택 때문에 오류 32가 반환되고 응답자가 PROPOSAL_NOT_CHOSEN 메시지를 보냅니다.

요약

IKEv1의 경우 MM5에서 시작하는 암호화에 사용되는 키를 계산하기 위해 사전 공유 키가 DH 결과와 함께 사용됩니다. IKEid가 MM5와 MM6에서 전송되므로 ISAKMP 수신기는 ISAKMP 프로파일(및 관련 키)을 사용할 ISAKMP 프로파일을 아직 확인할 수 없습니다.

그 결과, ISAKMP 응답자는 특정 피어의 키를 찾기 위해 전역적으로 정의된 모든 키링을 검색하려고 합니다.서로 다른 IP 주소의 경우 가장 일치하는 키 링(가장 구체적인)이 선택됩니다.동일한 IP 주소의 경우 컨피그레이션에서 첫 번째 일치하는 키가 사용됩니다.키링은 MM5의 암호 해독에 사용되는 키를 계산하는 데 사용됩니다.

MM5를 수신하면 ISAKMP 이니시에이터가 ISAKMP 프로필 및 관련 키링을 결정합니다.개시자는 MM4 DH 계산을 위해 선택한 것과 동일한 키링인지 확인합니다.그렇지 않으면 연결이 실패합니다.

전역 컨피그레이션에 구성된 키링의 순서는 중요합니다.따라서 ISAKMP 응답자는 가능하면 여러 항목이 있는 단일 키링을 사용합니다.

전역 컨피그레이션 모드에서 정의된 사전 공유 키는 default라는 사전 정의 키링에 속합니다.그러면 동일한 규칙이 적용됩니다.

응답자에 대한 IKE 프로파일 선택의 경우 가장 구체적인 프로파일이 일치합니다.이니시에이터의 경우 컨피그레이션의 프로파일이 사용되거나, 확인할 수 없는 경우 가장 일치하는 프로파일이 사용됩니다.

서로 다른 ISAKMP 프로파일에 서로 다른 인증서를 사용하는 시나리오에서 비슷한 문제가 발생합니다.다른 인증서를 선택한 경우 'ca trust-point' 프로필 유효성 검사 때문에 인증이 실패할 수 있습니다.이 문제는 별도의 문서에서 다룹니다.

이 문서에서 설명하는 문제는 Cisco 고유의 문제가 아니라 IKEv1 프로토콜 설계의 제한과 관련된 문제입니다.인증서와 함께 사용되는 IKEv1에는 이러한 제한이 없으며, 사전 공유 키와 인증서 모두에 사용되는 IKEv2에는 이러한 제한이 없습니다.

관련 정보

- Certificate to ISAKMP Profile Mapping 섹션 for IPsec VPNs Configuration Guide, Cisco IOS Release 15M&T
- Cisco IOS Security 명령 참조의 clear eou 섹션을 통해 ca 신뢰 지점:명령 A - C
- 기술 지원 및 문서 – Cisco Systems