Regras de seleção IO IKEv1/IKEv2 para Keyrings e perfis - guia de Troubleshooting

Índice

Introdução

Este documento descreve o uso de keyrings múltiplos para perfis múltiplos do Internet Security Association and Key Management Protocol (ISAKMP) em um cenário VPN do LAN para LAN do software do ® do Cisco IOS. Cobrem o comportamento do Cisco IOS Software Release 15.3T assim como os problemas potenciais quando os keyrings múltiplos são usados.

Duas encenações são apresentadas, com base em um túnel VPN com dois perfis ISAKMP em cada roteador. Cada perfil tem um keyring diferente com o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT anexado. As encenações demonstram que o túnel VPN pode ser iniciado somente de um lado da conexão devido à seleção e à verificação do perfil.

As próximas seções do documento resumem os critérios de seleção para o perfil do keyring para o iniciador do Internet Key Exchange (IKE) e o que responde IKE. Quando os endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes são usados pelo keyring no que responde IKE, a configuração trabalha corretamente, mas o uso do mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT cria o problema apresentado na primeira encenação.

As seções subsequente explicam porque a presença de um keyring do padrão (configuração global) e os keyrings específicos puderam conduzir aos problemas e porque o uso do protocolo da versão 2 do intercâmbio de chave de Internet (IKEv2) evita esse problema.

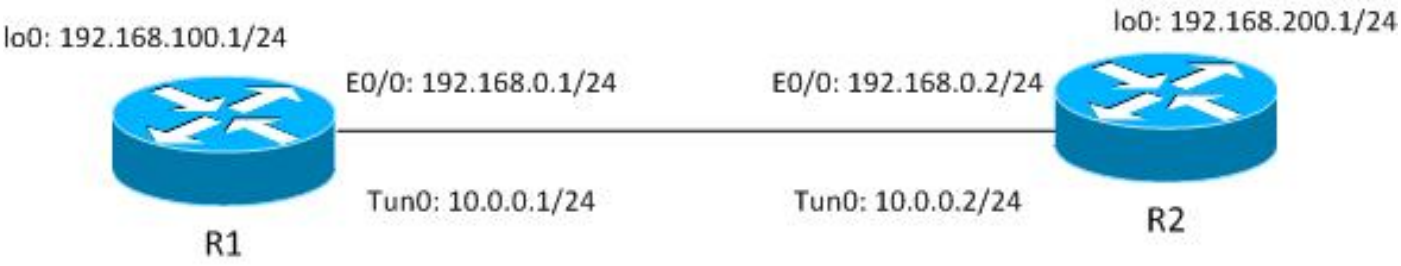
As seções do final apresentam os critérios de seleção para o perfil IKE para ambos para o iniciador IKE e o que responde, junto com os erros típicos que ocorrem quando um perfil incorreto é selecionado.

Configuração

> Notas:
>
> O analisador do CLI Cisco (clientes registrados somente) apoia determinados comandos de exibição. Use o analisador do CLI Cisco a fim ver uma análise do emissor de comando de execução.
>
> Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Topologia

A interface de túnel virtual do uso do roteador1 (r1) e do roteador2 (R2) (VTI) ([GRE] do encapsulamento de roteamento genérico) conecta a fim alcançar seus laços de retorno. Esse VTI é protegido pela segurança de protocolo do Internet (IPsec).



O r1 e o R2 têm dois perfis ISAKMP, cada um com keyring diferente. Todos os keyrings têm a mesma senha.

Rede do r1 e VPN

A configuração para a rede do r1 e o VPN é:

```
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
```

Rede R2 e VPN

A configuração para a rede R2 e o VPN é:

```
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 os keyrings usam o mesmo endereço IP do peer e usam a senha “Cisco.”

No r1, profile2 é usado para a conexão de VPN. Profile2 é o segundo perfil na configuração, que usa o segundo keyring na configuração. Porque você verá, a ordem do keyring é crítica.

Cenários de exemplo

Na primeira encenação, o r1 é o iniciador ISAKMP. O túnel está negociando corretamente, e o tráfego é protegido como esperado.

A segunda encenação usa a mesma topologia, mas tem o R2 como o iniciador ISAKMP quando a negociação phase1 está falhando.

A versão 1 do intercâmbio de chave de Internet (IKEv1) precisa uma chave pré-compartilhada para o cálculo do skey, que é usado a fim decifrar/cifra o pacote 5 do modo principal (MM5) e os pacotes IKEv1 subsequentes. O skey é derivado da computação do Diffie-Hellman (DH) e da chave pré-compartilhada. Que a chave pré-compartilhada precisa de ser determinada depois que MM3 (que responde) ou MM4 (iniciador) é recebido, de modo que o skey, que é usado em MM5/MM6, pode ser computado.

Para o que responde ISAKMP em MM3, o perfil específico ISAKMP não é ainda determinado porque aquele acontece depois que o IKEID é recebido em MM5. Em lugar de, todos os keyrings são procurados por uma chave pré-compartilhada, e o primeiro ou keyring melhor de harmonização da configuração global é selecionado. Esse keyring é usado a fim calcular o skey que é usado para a descriptografia de MM5 e a criptografia de MM6. Após a descriptografia de MM5 e após o perfil e o keyring associado ISAKMP é determinado, o que responde ISAKMP executa a verificação se o mesmo keyring foi selecionado; se o mesmo keyring não é selecionado, a conexão está deixada cair.

Assim, para o que responde ISAKMP, você deve usar um único keyring com entradas múltiplas sempre que possível.

R1 como o iniciador IKE (correto)

Esta encenação descreve o que ocorre quando o r1 é o iniciador IKE:

1. Use estes debuga para o r1 e o 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. O r1 inicia o túnel, envia o pacote MM1 com propostas da política, e recebe MM2 na resposta. MM3 é preparado então:

```
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
```

No início, o r1 sabe que o ISAKMP profile2 deve ser usado porque é limitado sob o perfil IPSec usado para aquele VTI.

Assim, o keyring correto (keyring2) foi selecionado. A chave pré-compartilhada de keyring2 é usada como o material de ajuste para cálculos DH quando o pacote MM3 está sendo preparado.

3. Quando o R2 recebe esse pacote MM3, ainda não sabe que perfil ISAKMP deve ser usado, mas precisa uma chave pré-compartilhada para a geração DH. É por isso o R2 procura todos os keyrings a fim encontrar a chave pré-compartilhada para esse 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
```

A chave para 192.168.0.1 foi encontrada no primeiro keyring definido (keyring1).

4. O R2 prepara então o pacote MM4 com cálculos DH e com a chave 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. Quando o r1 recebe MM4, prepara o pacote MM5 com IKEID e com a chave correta selecionada mais cedo (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. O pacote MM5, que contém o IKEID de 192.168.0.1, é recebido pelo R2. Neste momento, o R2 sabe a que perfil ISAKMP que o tráfego deve ser limitado (o **addresscommand da identidade do fósforo**):

```
*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. O R2 executa agora a verificação se o keyring que esteve selecionado cegamente para o pacote MM4 é o mesmo que o keyring configurado para o perfil ISAKMP escolhido agora. Porque keyring1 é primeiro na configuração, foi selecionado previamente, e é selecionado agora. A validação é bem sucedida, e o pacote MM6 pode 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. O r1 recebe MM6 e não o precisa de executar a verificação do keyring porque se soube do primeiro pacote; o iniciador sabe sempre que perfil ISAKMP a se usar e que keyring é associado com esse perfil. A autenticação é bem sucedida, e Phase1 termina corretamente:

```
*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 começa normalmente e é terminado com sucesso.

Esta encenação trabalha corretamente somente devido à ordem correta de keyrings definida no R2. O perfil que deve ser usado para a sessão de VPN usa o keyring que era primeiro na configuração.

R2 como o iniciador IKE (incorreto)

Esta encenação descreve o que ocorre quando o R2 inicia o mesmo túnel e explica porque o túnel não será estabelecido. Alguns logs foram removidos a fim centrar-se sobre as diferenças entre este e o exemplo anterior:

1. O R2 inicia o 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. Desde que o R2 é o iniciador, o perfil e o keyring ISAKMP são sabidos. A chave pré-compartilhada de keyring1 é usada para computações DH e enviada em MM3. O R2 está recebendo MM2 e está preparando MM3 baseado nessa chave:

```
*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. O r1 recebe MM3 do R2. Nesta fase, o r1 não sabe que perfil ISAKMP a se usar, assim que não sabe que keyring a se usar. O r1 usa assim o primeiro keyring da configuração global, que é keyring1. O uso do r1 que chave pré-compartilhada para computações DH e envia 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. O R2 recebe MM4 do r1, usa a chave pré-compartilhada de keyring1 a fim computar o DH, e prepara o pacote MM5 e o 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. O r1 recebe MM5 do r1. Porque o IKEID iguala 192.168.0, profile2 foi selecionado. Keyring2 foi configurado em profile2 assim que em keyring2 é selecionado. Previamente, para a computação DH em MM4, o r1 selecionou o primeiro keyring configurado, que era keyring1. Mesmo que as senhas sejam exatamente as mesmas, a validação para o keyring falha porque estes são objetos diferentes do keyring:

```
*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
```

Debuga para a chave pré-compartilhada diferente

Os cenários anteriores usaram a mesma chave (“Cisco "). Assim, mesmo quando o keyring incorreto foi usado, o pacote MM5 poderia ser decifrado corretamente e deixado cair mais tarde devido à falha da validação do keyring.

Nas encenações onde as chaves diferentes são usadas, MM5 não pode ser decifrado, e este Mensagem de Erro 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
```

Critérios de seleção do Keyring

Este é um sumário dos critérios de seleção do keyring. Veja as próximas seções para detalhes adicionais.

	Iniciador	Que responde
Keyrings múltiplos	Configurado. Se não configurou explicitamente o	O fósforo o mais específico

com endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes	mais específico da configuração	
Keyrings múltiplos com os mesmos endereços IP de Um ou Mais Servidores Cisco ICM NT	Configurado. Se não a **configuração** explicitamente configurada **torna-se imprevisível e não apoiada. Se não deve configurar duas chaves para o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT.**	**A configuração torna-se imprevi e não apoiada. Se não deve configurar duas chaves para o mesmo endereço IP de Um ou M Servidores Cisco ICM NT.**

Esta seção igualmente descreve porque a presença de um keyring do padrão (configuração global) e keyrings específicos pôde conduzir aos problemas e explica porque o uso do protocolo IKEv2 evita tais problemas.

Ordem de seleção do Keyring no iniciador IKE

Para a configuração com um VTI, o iniciador usa uma interface de túnel específica esses pontos ao perfil IPSec específico. Porque o perfil IPSec usa um perfil específico IKE com um keyring específico, não há nenhuma confusão sobre que keyring a se usar.

O mapa cript., que igualmente aponta a um perfil específico IKE com um keyring específico, funciona da mesma forma.

Contudo, não é sempre possível determinar da configuração que keyring a se usar. Por exemplo, isto ocorre quando não há nenhum perfil IKE configurado - isto é, o perfil IPSec não está configurado a fim usar o 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
```

Se este iniciador IKE tenta enviar MM1, escolherá o keyring o mais 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
```

Desde que o iniciador não tem nenhum perfil IKE configurado quando recebe MM6, não baterá um perfil e terminá-lo-á com autenticação bem sucedida e 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
```

Ordem de seleção do Keyring no que responde IKE - Endereços IP de Um ou Mais

Servidores Cisco ICM NT diferentes

O problema com seleção do keyring está no que responde. Quando os keyrings usam endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes, o ordem de seleção é simples.

Supõe que o que responde IKE tem esta configuração:

```
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
```

Quando este que responde recebe o pacote MM1 do iniciador IKE com endereço IP 192.168.0.2, escolherá o melhor (fósforo da maioria de específico), mesmo quando a ordem na configuração é diferente.

Os critérios para o ordem de seleção são:

1. Somente as chaves com um endereço IP de Um ou Mais Servidores Cisco ICM NT são consideradas.
2. O roteamento virtual e a transmissão (VRF) do pacote recebido são verificados ([fVRF] da parte frontal VRF).
3. Se o pacote está no padrão VRF, o keyring global está verificado primeiramente. A chave a mais precisa (comprimento do netmask) é selecionada.
4. Se nenhuma chave é encontrada no keyring do padrão, todos os keyrings que combinam este fVRF estão concatenados.
5. A chave a mais precisa (o netmask o mais longo) é combinada. Por exemplo, /32 é preferido sobre /24.

Debuga confirmam a seleção:

```
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
```

Ordem de seleção do Keyring no que responde IKE - Os mesmos endereços IP de Um ou Mais Servidores Cisco ICM NT

Quando os keyrings usam os mesmos endereços IP de Um ou Mais Servidores Cisco ICM NT, os problemas ocorrem. Supõe que o que responde IKE tem esta configuração:

```
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 configuração torna-se imprevisível e não apoiada. Se não deve configurar duas chaves para o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT ou o problema descrito no R2 como o iniciador IKE (incorreto) ocorrerá.

Configuração global do Keyring

As chaves ISAKMP definidas na configuração global pertencem ao keyring do padrão:

```
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
```

Mesmo que a chave ISAKMP seja última na configuração, é processada como o primeiro no que responde 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
```

Assim, o uso da configuração global e de keyrings específicos é muito arriscado e pôde conduzir aos problemas.

Keyring em IKEv2 - O problema não ocorre

Embora o protocolo IKEv2 use conceitos similares a IKEv1, a seleção do keyring não causa problemas similares.

Em casos simples, há apenas quatro pacotes trocados. O IKEID que determina que perfil IKEv2 deve ser selecionado no que responde é enviado pelo iniciador no terceiro pacote. O terceiro pacote é cifrado já.

A diferença a mais grande nos dois protocolos é que IKEv2 usa somente o resultado DH para a computação do skey. A chave pré-compartilhada é já não necessária a fim computar o skey usado para a criptografia /descriptografia.

O IKEv2 RFC (5996, seção 2.14), estados:

As chaves compartilhadas são computadas como segue. Uma quantidade chamada SKEYSEED é calculada dos nonces trocados durante a troca IKE_SA_INIT e o segredo compartilhado Diffie-Hellman estabelecidos durante essa troca.

Na mesma seção, RFC as notas igualmente:

```
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 a informação necessária é enviada nos primeiros dois pacotes, e não há nenhuma necessidade de usar uma chave pré-compartilhada quando SKEYSEED é calculado.

Compare isto com o IKE RFC (2409, seção 3.2), que indica:

SKEYID é uma corda derivada do material secreto conhecido somente aos jogadores ativos na troca.

Esse “material secreto conhecido somente aos jogadores ativos” é a chave pré-compartilhada. Na seção 5, RFC as notas igualmente:

Para chaves pré-compartilhada: SKEYID = prf (**chave pré-compartilhada**, Ni_b | Nr_b)

Isto explica porque o projeto IKEv1 para chaves pré-compartilhada causa tão muitos problemas. Estes problemas não existem em IKEv1 quando os Certificados são usados para a autenticação.

Critérios de seleção do perfil IKE

Este é um sumário dos critérios de seleção do perfil IKE. Veja as próximas seções para detalhes adicionais.

	Iniciador	Que responde
Seleção do perfil	Deve ser configurada (ajuste no perfil IPSec ou no crypto map). Se não fósforo configurado, primeiro da configuração. O peer remoto deve combinar somente um perfil específico ISAKMP, se a identidade do par é combinada em dois perfis ISAKMP, a configuração é inválido.	Primeiro fósforo da configuração. O peer remoto deve combinar somente um perfil específico ISAKMP, se a identidade d par é combinada em dois perfis ISAKMP, a configuração é inválido.

Esta seção igualmente descreve os erros típicos que ocorrem quando um perfil incorreto foi selecionado.

Ordem de seleção do perfil IKE no iniciador IKE

A relação VTI aponta geralmente a um perfil IPSec específico com um perfil específico IKE. O roteador sabe então que perfil IKE a se usar.

Similarmente, o mapa cript. aponta a um perfil específico IKE, e o roteador sabe que perfil a se usar devido à configuração.

Contudo, pôde haver as encenações onde o perfil não é especificado e onde não é possível determinar diretamente da configuração que perfilam para se usar; neste exemplo, nenhum perfil IKE é selecionado no perfil 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
```

Quando este iniciador tenta enviar um pacote MM1 a 192.168.0.2, o perfil o mais específico está selecionado:

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

Ordem de seleção do perfil IKE no que responde IKE

O ordem de seleção do perfil em um que responde IKE é similar ao ordem de seleção do keyring, onde o mais específico toma a precedência.

Supõe esta configuração:

```
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 uma conexão de 192.168.0.1 é recebida, profile2 estará selecionado.

A ordem de perfis configurados não importa. O comando show runnning-config coloca cada perfil configurado novo na extremidade da lista.

Às vezes o que responde pôde ter dois perfis IKE que usam o mesmo keyring. Se um perfil incorreto está selecionado no que responde mas o keyring selecionado está correto, a autenticação terminará corretamente:

```
*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
```

O que responde recebe e aceita a proposta QM e tenta-a gerar os deslocamentos predeterminados do parâmetro de segurança IPSec (SPI). Neste exemplo, algum debuga foi

removido para maior 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
```

Neste momento, o que responde falha e relata que o perfil correto ISAKMP não combinou:

```
 (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
```

Devido à seleção incorreta do perfil IKE, o erro 32 é retornado, e o que responde envia a mensagem PROPOSAL_NOT_CHOSEN.

Resumo

Para IKEv1, uma chave pré-compartilhada é usada com resultados DH a fim calcular o skey usado para a criptografia que começa em MM5. Depois que recebe MM3, o receptor ISAKMP não pode ainda determinar que perfil ISAKMP (e keyring associado) deve ser usado porque o IKEID é enviado em MM5 e em MM6.

O resultado é que o que responde ISAKMP tenta procurar através de todos os keyrings globalmente definidos a fim encontrar a chave para o par específico. Para endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes, o melhor keyring de harmonização (o mais específico) é selecionado; para o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT, primeiro fechar de harmonização da configuração é usado. O keyring é usado a fim calcular o skey que é usado para a descriptografia de MM5.

Depois que recebe MM5, o iniciador ISAKMP determina o perfil ISAKMP e o keyring associado. O iniciador executa a verificação se este é o mesmo keyring que esteve selecionado para a

computação MM4 DH; se não, a conexão falha.

A ordem dos keyrings configurados na configuração global é crítica. Assim, para o que responde ISAKMP, use um único keyring com entradas múltiplas sempre que possível.

As chaves pré-compartilhada que são definidas no modo de configuração global pertencem a um keyring predefinido chamado padrão. As mesmas regras aplicam-se então.

Para a seleção do perfil IKE para o que responde, o perfil o mais específico é combinado. Para o iniciador, o perfil da configuração é usado, ou, se aquele não pode ser determinado, o melhor fósforo é usado.

Um problema similar ocorre nas encenações que usam Certificados diferentes para perfis diferentes ISAKMP. A autenticação pôde falhar devido “à validação do perfil do confiança-ponto Ca” quando um certificado diferente é escolhido. Este problema será coberto em um documento separado.

As edições descritas neste artigo não são problemas específicos da Cisco, mas são relacionadas às limitações do projeto do protocolo IKEv1. IKEv1 usado com Certificados não tem estas limitações, e IKEv2 usado para ambas as chaves pré-compartilhada e Certificados não tem estas limitações.

Informações Relacionadas

- Certificado à seção do mapeamento do perfil ISAKMP do intercâmbio de chave de Internet para o manual de configuração do IPsec VPN, Cisco IOS Release 15M&T
- confiança-ponto Ca através da seção clara do eou da referência de comandos do Cisco IOS Security: Comandos A ao C
- Suporte Técnico e Documentação - Cisco Systems