Regras de seleção IOS IKEv1/IKEv2 para chaves e perfis - Guia de solução de problemas

Contents

Introduction

Este documento descreve o uso de vários teclas para vários perfis de Internet Security Association and Key Management Protocol (ISAKMP) em um cenário de VPN LAN a LAN do software Cisco IOS®. Ele abrange o comportamento do Cisco IOS Software Release 15.3T, bem como possíveis problemas quando vários teclados são usados.

Dois cenários são apresentados, com base em um túnel VPN com dois perfis ISAKMP em cada roteador. Cada perfil tem um teclado diferente com o mesmo endereço IP anexado. Os cenários demonstram que o túnel VPN pode ser iniciado somente de um lado da conexão devido à seleção e verificação do perfil.

As próximas seções do documento resumem os critérios de seleção para o perfil do teclado do iniciador do Internet Key Exchange (IKE) e do respondedor IKE. Quando endereços IP diferentes são usados pelo teclado no respondente IKE, a configuração funciona corretamente, mas o uso do mesmo endereço IP cria o problema apresentado no primeiro cenário.

As seções subsequentes explicam por que a presença de um keyring padrão (configuração global) e de teclas específicas pode levar a problemas e por que o uso do protocolo IKEv2 (Internet Key Exchange Version 2) evita esse problema.

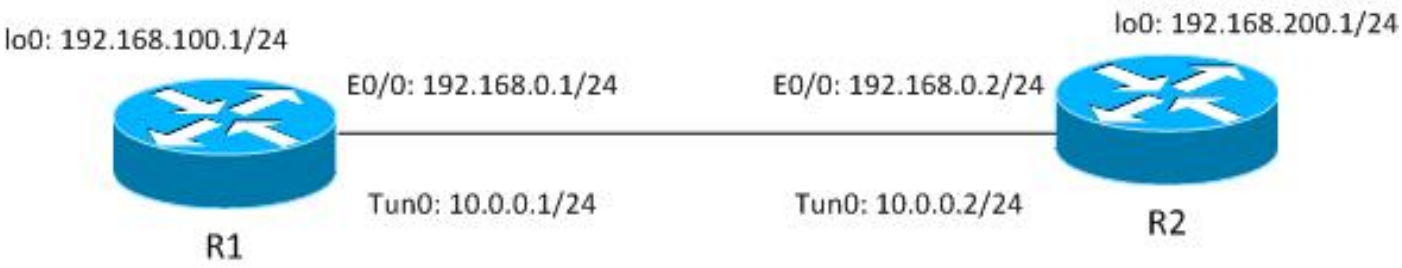
As seções finais apresentam os critérios de seleção do perfil IKE para o iniciador IKE e o respondente, juntamente com os erros típicos que ocorrem quando um perfil incorreto é selecionado.

Configuração

> **Notas:**
>
> O Cisco CLI Analyzer (somente clientes registrados) aceita alguns comandos show. Use o Cisco CLI Analyzer para visualizar uma análise da saída do comando show.
>
> Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Topologia

O Roteador 1 (R1) e o Roteador 2 (R2) usam interfaces de Virtual Tunnel Interface (VTI) (Generic Routing Encapsulation [GRE]) para acessar seus loopbacks. Esse VTI é protegido pelo IPSec (Internet Protocol Security).



R1 e R2 têm dois perfis ISAKMP, cada um com um toque de chave diferente. Todos os teclas têm a mesma senha.

Rede e VPN R1

A configuração para a rede R1 e 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 e VPN R2

A configuração para a rede R2 e 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 teclas usam o mesmo endereço IP de peer e usam a senha ' cisco'.

Em R1, profile2 é usado para a conexão VPN. O Perfil2 é o segundo perfil na configuração, que usa o segundo toque de chave na configuração. Como você verá, a ordem dos teclados é crítica.

Cenários de exemplo

No primeiro cenário, R1 é o iniciador ISAKMP. O túnel está negociando corretamente e o tráfego está protegido como esperado.

O segundo cenário usa a mesma topologia, mas tem R2 como o iniciador ISAKMP quando a negociação da fase 1 está falhando.

O Internet Key Exchange Version 1 (IKEv1) precisa de uma chave pré-compartilhada para o cálculo de skey, que é usado para descriptografar/criptografar o Main Mode packet 5 (MM5) e os pacotes IKEv1 subsequentes. A chave é derivada da computação Diffie-Hellman (DH) e da chave pré-compartilhada. Essa chave pré-compartilhada precisa ser determinada após o recebimento de MM3 (respondedor) ou MM4 (iniciador), de modo que a chave, que é usada em MM5/MM6, possa ser calculada.

Para o respondedor ISAKMP em MM3, o perfil ISAKMP específico ainda não foi determinado porque isso acontece depois que o IKEID é recebido em MM5. Em vez disso, todos os teclados são procurados por uma chave pré-compartilhada e o primeiro ou melhor teclado correspondente da configuração global é selecionado. Essa chave é usada para calcular a chave que é usada para descriptografia de MM5 e criptografia de MM6. Após a decodificação de MM5 e após a determinação do perfil ISAKMP e da chave associada, o respondente ISAKMP efetua a verificação se a mesma chave foi selecionada; se o mesmo toque de tecla não estiver selecionado, a conexão será removida.

Assim, para o respondedor ISAKMP, você deve usar um único chaveiro com várias entradas sempre que possível.

R1 como iniciador IKE (correto)

Este cenário descreve o que ocorre quando R1 é o iniciador IKE:

1. Use estas depurações para R1 e R2:

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

2. R1 inicia o túnel, envia o pacote MM1 com propostas de política e recebe MM2 em resposta. MM3 é preparado em seguida:

```
R1#ping 192.168.200.1 source lo0 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
```

```
Packet sent with a source address of 192.168.100.1

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

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

*Jun 19 10:04:24.827: ISAKMP:(0): processing SA payload. message ID = 0
*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
*Jun 19 10:04:24.827: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Jun 19 10:04:24.827: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Jun 19 10:04:24.827: ISAKMP:(0):Found ADDRESS key in keyring keyring2
*Jun 19 10:04:24.827: ISAKMP:(0): local preshared key found
*Jun 19 10:04:24.827: ISAKMP : Looking for xauth in profile profile2
*Jun 19 10:04:24.827: ISAKMP:(0):Checking ISAKMP transform 1 against
priority 10 policy
*Jun 19 10:04:24.827: ISAKMP:      encryption 3DES-CBC
*Jun 19 10:04:24.827: ISAKMP:      hash MD5
*Jun 19 10:04:24.827: ISAKMP:      default group 2
*Jun 19 10:04:24.827: ISAKMP:      auth pre-share
*Jun 19 10:04:24.827: ISAKMP:      life type in seconds
*Jun 19 10:04:24.827: ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
*Jun 19 10:04:24.827: ISAKMP:(0):atts are acceptable. Next payload is 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:actual life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Acceptable atts:life: 0
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa vpi_length:4
*Jun 19 10:04:24.827: ISAKMP:(0):Fill atts in sa life_in_seconds:86400
*Jun 19 10:04:24.827: ISAKMP:(0):Returning Actual lifetime: 86400
*Jun 19 10:04:24.827: ISAKMP:(0)::Started lifetime timer: 86400.

*Jun 19 10:04:24.827: ISAKMP:(0): processing vendor id payload
```

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

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

Desde o início, R1 sabe que o perfil ISAKMP2 deve ser usado porque está vinculado ao perfil IPSec usado para esse VTI.

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

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

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

4. Em seguida, o R2 prepara o pacote MM4 com cálculos de DH e com a chave 'cisco' do 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 recebe MM4, prepara o pacote MM5 com IKEID e com a chave correta selecionada anteriormente (do 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 por R2. Neste ponto, o R2 sabe a qual perfil ISAKMP o tráfego deve ser associado (o 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. O R2 agora executa a verificação se o keyring selecionado cegamente para o pacote MM4 é o mesmo que o keyring configurado para o perfil ISAKMP agora escolhido. Como o keyring1 é o primeiro na configuração, ele foi selecionado anteriormente e está selecionado agora. A validação foi 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. R1 recebe MM6 e não precisa executar a verificação do toque de chave porque ele foi conhecido do primeiro pacote; o iniciador sempre sabe qual perfil ISAKMP usar e qual keyring está associado a esse perfil. A autenticação foi bem-sucedida e a Fase1 foi concluída 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. A fase 2 é iniciada normalmente e concluída com êxito.

Esse cenário funciona corretamente somente devido à ordem correta dos teclados definida em R2. O perfil que deve ser usado para a sessão VPN usa o teclado que foi o primeiro na configuração.

R2 como iniciador IKE (incorreto)

Esse cenário descreve o que ocorre quando R2 inicia o mesmo túnel e explica por que o túnel não será estabelecido. Alguns registros foram removidos para focar nas diferenças entre este e o exemplo anterior:

1. R2 inicia o túnel:

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

2. Como R2 é o iniciador, o perfil e o teclado de ISAKMP são conhecidos. A chave pré-compartilhada do keyring1 é usada para computação de DH e é enviada em MM3. R2 está recebendo MM2 e preparando MM3 com base 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. R1 recebe MM3 de R2. Neste estágio, R1 não sabe qual perfil ISAKMP usar, portanto, não sabe qual keyring usar. O R1, portanto, usa o primeiro toque de chave da configuração global, que é keyring1. O R1 usa essa chave pré-compartilhada para computação de 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. R2 recebe MM4 de R1, usa a chave pré-compartilhada do keyring1 para computar 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. R1 recebe MM5 de R1. Como o IKEID é igual a 192.168.0, profile2 foi selecionado. Keyring2 foi configurado no perfil2 para que keyring2 seja selecionado. Anteriormente, para a computação DH em MM4, R1 selecionou o primeiro toque de tecla configurado, que era keyring1. Mesmo que as senhas sejam exatamente as mesmas, a validação do chaveiro falha porque são objetos de chaveamento diferentes:

```
*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
```

Depurações para chave pré-compartilhada diferente

Os cenários anteriores usavam a mesma chave ('cisco'). Assim, mesmo quando o chaveiro incorreto foi usado, o pacote MM5 pode ser descriptografado corretamente e descartado posteriormente devido a uma falha de validação do chaveiro.

Nos cenários em que são usadas chaves diferentes, o MM5 não pode ser descriptografado, e esta 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 de chave

Este é um resumo dos critérios de seleção do teclado. Consulte as próximas seções para obter mais detalhes.

	Iniciador	Respondente
Vários teclas com endereços IP diferentes	Configurado. Se não tiver configurado explicitamente o mais específico da configuração	A correspondência mais específi
Vários teclas com os mesmos endereços IP	Configurado. Se não estiver explicitamente configurado **a configuração se torna imprevisível e não é suportada. Não se deve configurar duas chaves para o mesmo endereço IP.**	**A configuração torna-se imprevis não é suportada. Não se deve configurar duas chaves para o m endereço IP.**

Esta seção também descreve por que a presença de um keyring padrão (configuração global) e de teclas específicas pode levar a problemas e explica por que o uso do protocolo IKEv2 evita tais problemas.

Ordem de seleção de chave no iniciador IKE

Para configuração com um VTI, o iniciador usa uma interface de túnel específica que aponta para um perfil de IPSec específico. Como o perfil IPSec usa um perfil IKE específico com um toque de chave específico, não há confusão sobre qual toque de chave usar.

O mapa de criptografia, que também aponta para um perfil IKE específico com um toque de chave específico, funciona da mesma maneira.

No entanto, nem sempre é possível determinar, a partir da configuração, qual keyring usar. Por exemplo, isso ocorre quando não há perfil IKE configurado - ou seja, o perfil IPSec não está configurado para usar o perfil IKE:

```
crypto keyring keyring1
 pre-shared-key address 192.168.0.0 255.255.255.0 key cisco
crypto keyring keyring2
 pre-shared-key address 192.168.0.2 key cisco

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

crypto ipsec profile profile1
 set transform-set TS

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

Se este iniciador IKE tentar enviar MM1, ele escolherá o chaveiro 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
```

Como o iniciador não tem perfis IKE configurados quando recebe MM6, ele não atingirá um perfil e será concluído com autenticação bem-sucedida e Modo Rápido (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 de chave no respondedor IKE - Endereços IP diferentes

O problema com a seleção do teclado está no respondente. Quando os teclados usam endereços IP diferentes, a ordem de seleção é simples.

Suponha que o respondente IKE tenha esta configuração:

```
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 esse respondente receber o pacote MM1 do iniciador do IKE com o endereço IP 192.168.0.2, ele escolherá a melhor correspondência (mais específica), mesmo quando a ordem na configuração for diferente.

Os critérios para a ordem de seleção são:

1. Somente chaves com um endereço IP são consideradas.
2. O VRF (Virtual Routing and Forwarding, roteamento e encaminhamento virtual) do pacote recebido é verificado (VRF de front-end [fVRF]).
3. Se o pacote estiver no VRF padrão, o chaveiro global será verificado primeiro. A chave mais precisa (comprimento da máscara de rede) é selecionada.
4. Se nenhuma tecla for encontrada no teclado padrão, todos os teclados que correspondem a esse fVRF serão concatenados.
5. A chave mais precisa (máscara de rede mais longa) é correspondida. Por exemplo, um /32 é preferido a um /24.

As depurações 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 de chave no respondedor IKE - Mesmos endereços IP

Quando os teclas usam os mesmos endereços IP, ocorrem problemas. Suponha que o respondente IKE tenha esta configuração:

```
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
```

Essa configuração se torna imprevisível e não é suportada. Não se deve configurar duas chaves para o mesmo endereço IP ou o problema descrito em R2 As IKE Initiator (Incorreto) ocorrerá.

Configuração global do teclado

As chaves ISAKMP definidas na configuração global pertencem ao chaveiro padrão:

```
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
```

Embora a chave ISAKMP seja a última na configuração, ela é processada como a primeira no respondente 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 teclas específicas é muito arriscado e pode levar a problemas.

Teclado em IKEv2 - O problema não ocorre

Embora o protocolo IKEv2 use conceitos semelhantes ao IKEv1, a seleção de toques de chaves não causa problemas semelhantes.

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

A maior diferença nos dois protocolos é que o IKEv2 usa somente o resultado DH para

computação de skey. A chave pré-compartilhada não é mais necessária para computar a chave skey usada para criptografia/descriptografia.

A RFC IKEv2 (5996, seção 2.14) , afirma:

As chaves compartilhadas são computadas da seguinte maneira. Uma quantidade chamada SKEYSEED é calculada a partir dos não-ces trocados durante a troca IKE_SA_INIT e o segredo compartilhado Diffie-Hellman estabelecido durante essa troca.

Na mesma seção, o RFC também observa:

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

Todas as informações necessárias são enviadas nos dois primeiros pacotes e não há necessidade de usar uma chave pré-compartilhada quando o SKEYSEED é calculado.

Compare isso com o IKE RFC (2409, seção 3.2) , que afirma:

SKEYID é uma string derivada de material secreto conhecido apenas pelos jogadores ativos na troca.

Esse "material secreto conhecido apenas pelos jogadores ativos" é a chave pré-compartilhada. Na seção 5, o RFC também observa:

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

Isso explica por que o design IKEv1 para chaves pré-compartilhadas causa tantos problemas. Esses problemas não existem no IKEv1 quando os certificados são usados para autenticação.

Critérios de seleção de perfil IKE

Este é um resumo dos critérios de seleção de perfil IKE. Consulte as próximas seções para obter mais detalhes.

	Iniciador	Respondente
Seleção de perfil	Deve ser configurado (definido no perfil de IPSec ou no mapa de criptografia). Se não estiver configurado, primeiro faça a correspondência a partir da configuração. O peer remoto deve corresponder apenas a um perfil ISAKMP específico, se a identidade do peer for correspondida em dois perfis ISAKMP, a configuração será inválida.	Primeira correspondência da configuração. O peer remoto deve corresponder apenas a um perfil ISAKMP específico, se a identidade do peer for correspondida em dois perfis ISAKMP, a configuração será inválida.

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

Ordem de seleção de perfil IKE no iniciador IKE

A interface VTI geralmente aponta para um perfil IPSec específico com um perfil IKE específico. O roteador sabe então qual perfil IKE usar.

Da mesma forma, o mapa de criptografia aponta para um perfil IKE específico e o roteador sabe qual perfil usar devido à configuração.

No entanto, podem existir cenários em que o perfil não é especificado e em que não é possível determinar diretamente a partir da configuração que perfil utilizar; neste exemplo, nenhum perfil IKE está selecionado no perfil IPSec:

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

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

crypto ipsec profile profile1
 set transform-set TS

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

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

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

Ordem de seleção de perfil IKE no respondedor IKE

A ordem de seleção de perfil em um respondente IKE é semelhante à ordem de seleção do toque de chave, onde o mais específico tem precedência.

Considere 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 for recebida, profile2 será selecionado.

A ordem dos perfis configurados não importa. O comando **show running-config** coloca cada novo perfil configurado no final da lista.

Às vezes, o respondente pode ter dois perfis de IKE que usam o mesmo toque de tecla. Se um perfil incorreto for selecionado no respondente, mas o teclado selecionado estiver correto, a autenticação será concluída 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 respondente recebe e aceita a proposta de QM e tenta gerar os Índices de Parâmetro de Segurança (SPIs) do IPSec. Neste exemplo, algumas depurações foram removidas 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
```

Nesse ponto, o respondente falha e informa que o perfil ISAKMP correto não corresponde:

```
 (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 respondente envia a mensagem PROPOSTA_NOT_CHOSEN.

Summary

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

O resultado é que o respondedor ISAKMP tenta pesquisar por todas as teclas definidas globalmente para encontrar a chave para um peer específico. Para endereços IP diferentes, o melhor chaveiro correspondente (o mais específico) é selecionado; para o mesmo endereço IP, a primeira chave correspondente da configuração é usada. O chaveiro é usado para calcular a chave que é usada para descriptografia de MM5.

Depois de receber MM5, o iniciador ISAKMP determina o perfil ISAKMP e o chaveiro associado. O iniciador efetua a verificação se este é o mesmo keyring selecionado para a computação MM4 DH; caso contrário, a conexão falhará.

A ordem dos teclados configurados na configuração global é crítica. Assim, para o respondedor ISAKMP, use um único chaveiro com várias entradas sempre que possível.

As chaves pré-compartilhadas definidas no modo de configuração global pertencem a um chaveiro predefinido chamado padrão. As mesmas regras se aplicam então.

Para a seleção do perfil IKE para o respondente, o perfil mais específico é comparado. Para o iniciador, o perfil da configuração é usado ou, se isso não puder ser determinado, a melhor correspondência é usada.

Um problema semelhante ocorre em cenários que usam certificados diferentes para perfis ISAKMP diferentes. A autenticação pode falhar devido à validação do perfil 'ca trust-point' quando um certificado diferente for escolhido. Esse problema será abordado em um documento separado.

Os problemas descritos neste artigo não são problemas específicos da Cisco, mas estão relacionados às limitações do projeto do protocolo IKEv1. O IKEv1 usado com certificados não tem essas limitações, e o IKEv2 usado para chaves e certificados pré-compartilhados não tem essas limitações.

Informações Relacionadas

- Seção Certificado de Mapeamento de Perfil ISAKMP do Guia de Configuração de Internet Key Exchange para VPNs IPsec, Cisco IOS versão 15M&T
- ca trust-point através da seção clear eou da Referência de Comandos de Segurança do Cisco IOS: Comandos A a C
- Suporte Técnico e Documentação - Cisco Systems