Содержание

Введение

Этот документ описывает использование множественных брелоков для множественных профилей Протокола ISAKMP в сценарии VPN LAN-LAN программного обеспечения Cisco IOSÂ®. Когда множественные брелоки используются, это покрывает поведение Cisco IOS Software Release 15.3T, а также потенциальные проблемы.

Два сценария представлены, основаны на VPN-туннеле с двумя профилями ISAKMP на каждом маршрутизаторе. Каждый профиль имеет другой брелок с тем же подключенным IP-адресом. Сценарии демонстрируют, что VPN-туннель может инициироваться только с одной стороны соединения из-за выбора профиля и проверки.

Следующие разделы документа суммируют условия выбора для профиля брелока и для инициатора Протокола IKE и для респондента IKE. Когда другие IP-адреса используются брелоком на респонденте IKE, конфигурация работает правильно, но использование того же IP-адреса создает проблему, представленную в первом сценарии.

Последующие разделы объясняют, почему присутствие и брелока по умолчанию (глобальная конфигурация) и определенных брелоков могло бы привести к проблемам и почему использование протокола второй версии протокола Internet Key Exchange (IKEv2) избегает той проблемы.

Заключительные разделы представляют условия выбора для профиля IKE и для для инициатора IKE и для респондента, наряду с типичными ошибками, которые происходят,

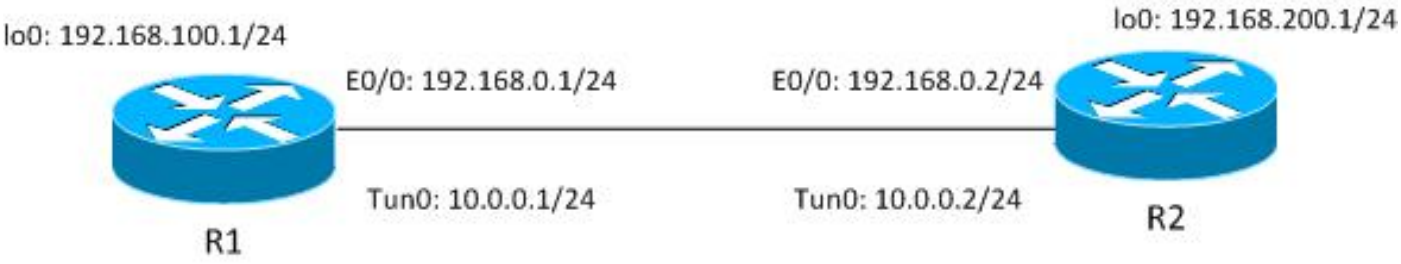
когда выбран неправильный профиль.

!--- конфигурацию

> **Примечания:**
>
> Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые команды show**. Используйте Cisco CLI Анализатор для **просматривания аналитику выходных данных команды show**.
>
> Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

Топология

Router1 (R1) и Router2 (R2) использует Виртуальный туннельный интерфейс (VTI) (Универсальная инкапсуляция маршрутизации [GRE]) интерфейсы для доступа к ее loopback. Это VTI защищено протоколом IPSEC (Internet Protocol Security) (IPSec).



И R1 и R2 имеют два профиля ISAKMP, каждого с другим брелоком. Все брелоки имеют тот же пароль.

Сеть R1 и VPN

Конфигурация для сети R1 и VPN:

```
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
```

Сеть R2 и VPN

Конфигурация для сети R2 и VPN:

```
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
```

Все брелоки используют тот же IP - адрес адресуемой точки и используют пароль 'Cisco'.

На R1 profile2 используется для VPN-подключения. Profile2 является вторым профилем в конфигурации, которая использует второй брелок в конфигурации. Как вы будете видеть, заказ брелока важен.

Примеры сценариев

В первом сценарии R1 является инициатором ISAKMP. Туннель выполняет согласование правильно, и трафик защищен как ожидалось.

Когда phase1 согласование отказывает, второй сценарий использует ту же топологию, но имеет R2 как инициатора ISAKMP.

Версии 1 (IKEv1) Обмена ключами между сетями нужен предварительный общий ключ для skey вычисления, которое используется для дешифрования пакета Основного режима 5 (MM5) и последующие пакеты IKEv1. skey получен из вычисления Diffie-Hellman (DH) и предварительного общего ключа. Тот предварительный общий ключ должен быть определен после MM3 (респондент), или MM4 (инициатор) получен, так, чтобы мог быть вычислен skey, который используется в MM5/MM6.

Для респондента ISAKMP в MM3 еще не определен определенный профиль ISAKMP, потому что это происходит после того, как IKEID получен в MM5. Вместо этого все брелоки ищутся предварительный общий ключ, и первый или лучший соответствующий брелок от глобальной конфигурации выбран. Тот брелок используется для вычисления skey, который используется для расшифровки MM5 и шифрования MM6. После расшифровки MM5 и после того, как определены профиль ISAKMP и привязанный брелок, респондент ISAKMP выполняет проверку, если был выбран тот же брелок; если тот же брелок не выбран, соединение отброшено.

Таким образом, для респондента ISAKMP, необходимо использовать одиночный брелок с несколькими точек входа, когда это возможно.

R1 как (корректный) инициатор IKE

Этот сценарий описывает то, что происходит, когда R1 является инициатором IKE:

1. Используйте эти отладки и для R1 и для 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. R1 инициирует туннель, передает пакет MM1 с предложениями по политике и получает MM2 в ответ. MM3 тогда подготовлен:

```
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
```

С самого начала R1 знает, что ISAKMP profile2 должен использоваться, потому что это связано под Профилем IPSEC, используемым для этого VTI.

Таким образом корректный брелок (keyring2) был выбран. Когда пакет MM3 готовится, предварительный общий ключ от keyring2 используется в качестве материала для кодирования для вычислений DH.

3. Когда R2 получает это пакет MM3, он все еще не знает, какой профиль ISAKMP должен использоваться, но ему нужен предварительный общий ключ для генерации DH. Именно поэтому R2 ищет все брелоки для обнаружения предварительного общего ключа для того узла:

```
*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
```
Ключ для 192.168.0.1 был найден в первом определенном брелоке (keyring1).

4. R2 тогда готовит пакет MM4 с вычислениями DH и с ключом 'Cisco' от 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. Когда R1 получает MM4, он готовит пакет MM5 с IKEID и с корректным ключом, выбранным ранее (от 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. Пакет MM5, который содержит IKEID 192.168.0.1, получен R2. На этом этапе R2 знает, с которым, профилем ISAKMP что трафик должен быть связан (**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. R2 теперь выполняет проверку, если брелок, который был вслепую выбран для пакета MM4, совпадает с брелоком, настроенным для профиля ISAKMP, теперь выбранного. Поскольку keyring1 является первым в конфигурации, это было выбрано ранее, и это выбрано теперь. Проверка успешна, и пакет MM6 может быть передан:

```
*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 получает MM6 и не должен выполнять проверку брелока, потому что это было известно от первого пакета; инициатор всегда знает, какой профиль ISAKMP использовать и какой брелок привязан к тому профилю. Аутентификация успешна, и концы Phase1 правильно:

```
*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 обычно запускается и успешно завершен.

Этот сценарий работает правильно только из-за правильного порядка брелоков, определенных на R2. Профиль, который должен использоваться для сеанса VPN, использует брелок, который был первым в конфигурации.

R2 как (неправильный) инициатор IKE

Этот сценарий описывает то, что происходит, когда R2 инициирует тот же туннель и объясняет, почему не будет установлен туннель. Некоторые журналы были удалены для фокусирований на различиях между этим и предыдущим примером:

1. R2 инициирует туннель:

```
*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. Так как R2 является инициатором, профиль ISAKMP и брелок известны. Предварительный общий ключ от keyring1 используется для вычислений DH и передается в MM3. R2 получает MM2 и готовит MM3 на основе того ключа:

```
*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 получает MM3 от R2. На данном этапе R1 не знает, какой профиль ISAKMP использовать, таким образом, это не знает который брелок использовать. R1 таким образом использует первый брелок от глобальной конфигурации, которая является keyring1. R1 используют тот предварительный общий ключ для вычислений DH, и передает 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 получает MM4 от R1, использует предварительный общий ключ от keyring1, чтобы вычислить DH и готовит пакет MM5 и 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 получает MM5 от R1. Поскольку IKEID равняется 192.168.0, profile2 был выбран. Keyring2 был настроен в profile2, таким образом, выбран keyring2. Ранее, для вычисления DH в MM4, R1 выбрал первый настроенный брелок, который был keyring1. Даже при том, что пароли являются точно тем же, проверкой для сбоев брелока, потому что это другие объекты 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
```

Отладки для другого предварительного общего ключа

Предыдущие сценарии использовали тот же ключ ('Cisco'). Таким образом, даже когда неправильный брелок использовался, пакет MM5 мог быть дешифрован правильно и отброшен позже из-за сбоя проверки брелока.

В сценариях, где другие ключи используются, не может быть дешифрован MM5, и это сообщение об ошибках появляется:

```
*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
```

Условия выбора брелока

Это - сводка условий выбора брелока. Посмотрите следующие разделы для дополнительных сведений.

Инициатор	Responder
Множественные	Настроенный. Если не явно	Самое определенное соответствие

брелоки с другими IP-адресами	настроенный самое определенное от конфигурации	
Множественные брелоки с теми же IP-адресами	Настроенный. Если не явно настроенная **конфигурация становится непредсказуемой и не поддерживаемая. Не нужно настраивать два ключа для того же IP-адреса.**	**Конфигурация становится непредсказуемой и не поддерживаемая. Не нужно настраивать два ключа для того же IP-адреса.**

Этот раздел также описывает, почему присутствие и брелока по умолчанию (глобальная конфигурация) и определенных брелоков могло бы привести к проблемам и объясняет, почему использование протокола IKEv2 избегает таких проблем.

Порядок выбора брелока на инициаторе IKE

Для конфигурации с VTI инициатор использует определенный туннельный интерфейс, который указывает к определенному Профилю IPSEC. Поскольку Профиль IPSEC использует определенный профиль IKE с определенным брелоком, нет никакого беспорядка по который брелок использовать.

Криптокарта, которая также указывает к определенному профилю IKE с определенным брелоком, функционирует таким же образом.

Однако не всегда возможно определить от конфигурации который брелок использовать. Например, это происходит, когда нет никакого настроенного профиля IKE - т.е. Профиль IPSEC не настроен для использования профиля 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
```

Если этот инициатор IKE попытается передать MM1, то он выберет самый определенный брелок:

```
*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
```

Так как у инициатора нет профилей IKE, настроенных, когда это получит MM6, это не поразит профиль, и будет вместе с успешной аутентификацией и Режимом 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
```

Порядок выбора брелока на респонденте IKE - другие IP-адреса

Проблема с выбором брелока находится на респонденте. Когда брелоки используют другие IP-адреса, порядок выбора прост.

Предположите, что у респондента IKE есть эта конфигурация:

```
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
```

Когда этот респондент получит пакет MM1 от инициатора IKE с IP-адресом 192.168.0.2, это выберет лучшее (самое определенное) соответствие, даже когда заказ в конфигурации является другим.

Критерии для порядка выбора:

1. Только ключи с IP-адресом рассматривают.
2. Виртуальная маршрутизация и передача (VRF) входящего пакета проверены (VRF фронтэнда [FVRF]).
3. Если пакет находится в VRF по умолчанию, глобальный брелок проверен сначала. Самый точный ключ (длина маски подсети) выбран.
4. Если никакой ключ не найден в брелоке по умолчанию, связаны все брелоки, которые совпадают с этим FVRF.
5. С самым точным ключом (самая длинная маска подсети) совпадают. Например,/32 предпочтен по/24.

Отладки подтверждают выбор:

```
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
```

Порядок выбора брелока на респонденте IKE - те же IP-адреса

Когда брелоки используют те же IP-адреса, проблемы происходят. Предположите, что у респондента IKE есть эта конфигурация:

```
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
```

Эта конфигурация становится непредсказуемой и не поддерживаемая. Не нужно настраивать два ключа для того же IP-адреса , или проблема, описанная в R2 Как (Неправильный) Инициатор IKE, произойдет.

Глобальная конфигурация брелока

Ключи ISAKMP, определенные в глобальной конфигурации, принадлежат брелоку по умолчанию:

```
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
```

Даже при том, что ключ ISAKMP является последним в конфигурации, он обработан как первое на респонденте 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
```

Таким образом использование и глобальной конфигурации и определенных брелоков очень опасно и могло бы привести к проблемам.

Брелок на IKEv2 - проблема не происходит

Несмотря на то, что протокол IKEv2 использует подобные понятия для IKEv1, выбор брелока не вызывает подобные проблемы.

В простых случаях существует всего четыре пакета, которыми обмениваются. IKEID, который определяет, какой профиль IKEv2 должен быть выбран на респонденте, передается инициатором в третьем пакете. Третий пакет уже зашифрован.

Самое большое различие в этих двух протоколах - то, что IKEv2 использует только результат DH для skey вычисления. Предварительный общий ключ больше не необходим для вычислений skey, используемого для в отличие от стандарта.

RFC IKEv2 (5996, разделите 2.14) , состояния:

Общие ключи вычислены следующим образом. Количество под названием SKEYSEED вычислено от параметров, которыми обмениваются во время обмена IKE_SA_INIT и общего секретного ключа Диффи-Хеллмана, установленного во время того обмена.

В том же разделе также обращает внимание RFC:

```
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
```

Вся необходимая информация передается в первых двух пакетах, и нет никакой потребности использовать предварительный общий ключ, когда вычислен SKEYSEED.

Сравните это с RFC IKE (2409, разделите 3.2) , который сообщает:

SKEYID является строкой, полученной из секретного материала, известного только активным игрокам в обмене.

Тот "секретный материал, известный только активным игрокам", является предварительным общим ключом. В разделе 5, также обращает внимание RFC:

Для предварительных общих ключей: SKEYID = PRF (**предварительный общий ключ**, Ni_b | Nr_b)

Это объясняет, почему дизайн IKEv1 для предварительных общих ключей вызывает столько проблем. Когда сертификаты используются для аутентификации, эти проблемы не существуют в IKEv1.

Условия выбора профиля IKE

Это - сводка условий выбора профиля IKE. Посмотрите следующие разделы для дополнительных сведений.

	Инициатор	Responder
Выбор профиля	Это должно быть настроено (набор в Профиле IPSEC или в криптокарте). Если не настроенный, сначала совпадите от конфигурации. Удаленный узел должен совпасть только с одним определенным профилем ISAKMP, если с идентификатором узлов совпадают в двух профилях ISAKMP, конфигурация недопустима.	Первое соответствие от конфигурации. Удаленный узел должен совпасть толь одним определенным профилем ISAKM если с идентификатором узлов совпада в двух профилях ISAKMP, конфигураци недопустима.

Этот раздел также описывает типичные ошибки, которые происходят, когда был выбран неправильный профиль.

Порядок выбора профиля IKE на инициаторе IKE

Интерфейс VTI обычно указывает к определенному Профилю IPSEC с определенным профилем IKE. Маршрутизатор тогда знает который профиль IKE использовать.

Точно так же точки криптокарты к определенному профилю IKE и маршрутизатор знают который профиль использовать из-за конфигурации.

Однако могли бы быть сценарии, где профиль не задан и откуда не возможно определить непосредственно конфигурации, которые представляют для использования; в данном

примере никакой профиль IKE не выбран в Профиле 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
```

Когда этот инициатор пытается передать пакет MM1 к 192.168.0.2, самый определенный профиль выбран:

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

Порядок выбора профиля IKE на респонденте IKE

Порядок выбора профиля на респонденте IKE подобен порядку выбора брелока, где самое определенное имеет приоритет.

Примите эту конфигурацию:

```
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
```

Когда соединение от 192.168.0.1 будет получено, profile2 будет выбран.

Заказ настроенных профилей не имеет значения. Команда runnning-config показа размещает каждый новый настроенный профиль в конце списка.

Иногда у респондента могло бы быть два профиля IKE, которые используют тот же брелок. Если неправильный профиль будет выбран на респонденте, но выбранный брелок корректен, то аутентификация закончится правильно:

```
*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
```

Респондент получает и принимает предложение по QM и пытается генерировать Индексы Параметра Безопасности IPsec (SPI). В данном примере некоторые отладки были удалены для ясности:

```
*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
```

На этом этапе, сбои респондента и отчёты, что не совпадал корректный профиль ISAKMP:

```
 (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
```

Из-за неправильного выбора профиля IKE возвращена ошибка 32, и респондент передает сообщению ПРОПОЗЭЛ_НОТ_ЧОСЕНА.

Сводка

Для IKEv1 предварительный общий ключ используется с результатами DH для вычисления skey, используемого для шифрования, которое запускается в MM5. После того, как это получает MM3, получатель ISAKMP еще не в состоянии определить, какой профиль ISAKMP (и связанный брелок) должен использоваться, потому что IKEID передается в MM5 и MM6.

Результат состоит в том, что респондент ISAKMP пытается перерыть все глобально определенные брелоки для обнаружения ключа для определенного узла. Для других IP-адресов выбран лучший соответствующий брелок (самое определенное); для того же IP-адреса используется первое соответствие, вводящее от конфигурации. Брелок используется для вычисления skey, который используется для расшифровки MM5.

После того, как это получит MM5, инициатор ISAKMP определяет профиль ISAKMP и

привязанный брелок. Инициатор выполняет проверку, если это - тот же брелок, который был выбран для вычисления MM4 DH; иначе, сбои соединения.

Заказ брелоков, настроенных в глобальной конфигурации, важен. Таким образом, для респондента ISAKMP, используйте одиночный брелок с несколькими точек входа, когда это возможно.

Предварительные общие ключи, которые определены в режиме глобальной конфигурации, принадлежат предопределенному брелоку, названному по умолчанию. Те же правила применяются тогда.

Для выбора профиля IKE для респондента совпадают с самым определенным профилем. Для инициатора профиль от конфигурации используется, или, если это не может быть определено, лучшее соответствие используется.

Подобная проблема происходит в сценариях, которые используют другие сертификаты для других профилей ISAKMP. Когда другой сертификат выбран, аутентификация могла бы отказать из-за проверки профиля 'ca trust-point'. Эта проблема будет покрыта отдельным документом.

Проблемы, описанные в этой статье, не являются определяемыми Cisco проблемами, но отнесены к ограничениям дизайна протокола IKEv1. IKEv1, используемый с сертификатами, не имеет этих ограничений, и IKEv2, используемый и для предварительных общих ключей и для сертификатов, не имеет этих ограничений.

Дополнительные сведения

- Сертификат к разделу Сопоставления Профиля ISAKMP Обмен ключами между сетями для руководства по конфигурации IPSec VPN, Cisco IOS Release 15M&T
- ca trust-point через clear eou раздел Справочник по командам системы безопасности Cisco IOS: Команды A к C
- Cisco Systems – техническая поддержка и документация