

IPSec IOS и отладки IKE - Устранение проблем Основного режима IKEv1

Содержание

[Введение](#)

[Базовая проблема](#)

[Сценарий](#)

[Используемые отладки](#)

[Настройка маршрутизатора IOS](#)

[Крипто - настройка](#)

[Другая сторона](#)

[Отладка](#)

[Сторона респондента IOS](#)

[Сообщение 1 \(MM1\) основного режима](#)

[Сообщение 2 \(MM2\) основного режима - передача нашего ответа](#)

[Сообщение 3 \(MM3\) основного режима](#)

[Сообщение 4 \(MM4\) основного режима](#)

[Сообщение 5 \(MM5\) основного режима - инициатор передает его идентичность](#)

[Сообщение 6 \(MM6\) основного режима - респондент передает его идентичность.](#)

[Завершение фазы 1.](#)

[Сообщение 1 \(QM1\) быстрого режима](#)

[Сообщение 2 \(QM2\) быстрого режима](#)

[Сообщение 3 \(QM3\) быстрого режима - фаза два должна быть завершена и туннельный интерфейс](#)

[Маршрутизатор IOS - инициатор](#)

[Сообщение 1 \(MM1\) основного режима - исходный контакт](#)

[Сообщение 2 \(MM2\) основного режима - отвечает на исходный контакт](#)

[Сообщение 3 \(MM3\) основного режима - обнаружение NAT и обмен Диффи-Хеллмана](#)

[Сообщение 4 \(MM4\) основного режима - обнаружение NAT и обмен Диффи-Хеллмана](#)

[Сообщение 5 \(MM5\) основного режима - передает идентичность](#)

[Сообщение 6 \(MM6\) основного режима - идентичность удаленного узла, фаза 1 установлена](#)

[Сообщение 1 \(QM1\) быстрого режима - узел запускает фазу 2](#)

[Сообщение 2 \(QM2\) быстрого режима](#)

[Сообщение 3 \(QM3\) быстрого режима - установление фазы 2](#)

[Туннельная проверка](#)

[Дополнительные сведения](#)

Введение

Когда основной режим и предварительный общий ключ (PSK) используются, этот документ предоставляет сведения для понимания отладок на программном обеспечении Cisco IOS.

Этот документ также предоставляет сведения о том, как преобразовать определенные линии отладки в конфигурации.

Эти темы не обсуждены:

- Проходящий трафик после туннеля был установлен
- Базовые понятия IPsec или Протокола IKE

Базовая проблема

IKE и отладки IPsec имеют тенденцию становиться загадочными. Центр технической поддержки Cisco (TAC) часто использует эти дефекты для понимания, где расположена проблема с **установлением** VPN-туннеля IPsec.

Сценарий

Когда сертификаты используются для аутентификации, основной режим, как правило, используется между туннелями между локальными сетями (LAN-to-LAN), или в случае удаленного доступа (ezvpn).

Те отладки от устройства Cisco IOS, которое выполняется 15.2 (1) выпуск ПО T.

Два главных сценария описаны в этом документе:

- Сторона инициатора IOS
- Сторона респондента IOS

В этом документе основанный на VTI туннель между двумя узлами установлен, на основе IPv6.

Примечания:

Используйте [Средство поиска команд Command Lookup Tool \(только зарегистрированные клиенты\)](#) для получения дополнительных сведений о командах, используемых в этом документе.

[Прежде чем выполнять какие-либо команды отладки, ознакомьтесь с документом "Важные сведения о командах отладки".](#)

Используемые отладки

- debug crypto isakmp
- debug crypto ipsec
- debug crypto kmi

Настройка маршрутизатора IOS

Крипто - настройка

```
crypto isakmp policy 10
authentication pre-share

crypto isakmp key cisco address ipv6 ::/0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport

crypto ipsec profile PRO
set transform-set TRA

interface Tunnel23
ip address 192.168.23.2 255.255.255.0
ipv6 address FE80::23:2 link-local
tunnel source Ethernet0/0
tunnel mode ipsec ipv6
tunnel destination 2001: DB8::3
tunnel protection ipsec profile PRO
```

Другая сторона

```
crypto isakmp policy 10
authentication pre-share

crypto isakmp key cisco address ipv6 ::/0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac
mode transport

crypto ipsec profile PRO
set transform-set TRA

interface Tunnel23
ip address 192.168.23.3 255.255.255.0
ipv6 address FE80::23:3 link-local
tunnel source Ethernet0/0
tunnel mode ipsec ipv6
tunnel destination 2001: DB8::2
tunnel protection ipsec profile PRO
```

Отладка

Сторона респондента IOS

Сообщение 1 (MM1) основного режима

Первоначальное предложение по IKE включает:

- Шифрование

- Хеширование
- Группа Diffie-Hellman (DH)
- Срок действия

```
*Sep 21 08:33:43.377: ISAKMP (0) : received packet from 2001: DB8::2 dport 500
sport 500 Global (N) NEW SA
*Sep 21 08:33:43.377: ISAKMP: Created a peer struct for 2001: DB8::2, peer port
500
*Sep 21 08:33:43.377: ISAKMP: New peer created peer = 0x8E45588
peer_handle = 0x8000000A
*Sep 21 08:33:43.377: ISAKMP: Locking peer struct 0x8E45588, refcount 1 for
crypto_isakmp_process_block
*Sep 21 08:33:43.377: ISAKMP: local port 500, remote port 500
*Sep 21 08:33:43.377: ISAKMP: (0):insert sa successfully sa = 6D12A00
*Sep 21 08:33:43.377: ISAKMP: (0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.377: ISAKMP: (0): Old State = IKE_READY New State = IKE_R_MM1
*Sep 21 08:33:43.377: ISAKMP: (0): processing SA payload. message ID = 0
*Sep 21 08:33:43.377: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::2
*Sep 21 08:33:43.377: ISAKMP: (0): local preshared key found
*Sep 21 08:33:43.377: ISAKMP: Scanning profiles for xauth ...
*Sep 21 08:33:43.377: ISAKMP: (0):Checking ISAKMP transform 1 against priority
10 policy
*Sep 21 08:33:43.377: ISAKMP:      encryption DES-CBC
*Sep 21 08:33:43.377: ISAKMP:      hash SHA
*Sep 21 08:33:43.377: ISAKMP:      default group 1
*Sep 21 08:33:43.377: ISAKMP:      auth pre-share
*Sep 21 08:33:43.377: ISAKMP:      life type in seconds
*Sep 21 08:33:43.377: ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
*Sep 21 08:33:43.377: ISAKMP: (0):atts are acceptable. Next payload is 0
*Sep 21 08:33:43.377: ISAKMP: (0):Acceptable atts:actual life: 0
*Sep 21 08:33:43.377: ISAKMP: (0):Acceptable atts:life: 0
*Sep 21 08:33:43.377: ISAKMP: (0):Fill atts in sa vpi_length:4
*Sep 21 08:33:43.377: ISAKMP: (0):Fill atts in sa life_in_seconds:86400
*Sep 21 08:33:43.377: ISAKMP: (0):Returning Actual lifetime: 86400
*Sep 21 08:33:43.377: ISAKMP: (0):: Started lifetime timer: 86400.

*Sep 21 08:33:43.377: ISAKMP: (0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.377: ISAKMP: (0): Old State = IKE_R_MM1 New State = IKE_R_MM1
```

Связанная конфигурация:

```
crypto isakmp policy 10
authentication pre-share
```

Сообщение 2 (MM2) основного режима - передача нашего ответа

```
*Sep 21 08:33:43.377: ISAKMP: (0): sending packet to 2001: DB8::2 my_port 500
peer_port 500 (R) MM_SA_SETUP
*Sep 21 08:33:43.377: ISAKMP: (0): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.377: ISAKMP: (0):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.377: ISAKMP: (0): Old State = IKE_R_MM1 New State = IKE_R_MM2
```

Сообщение 3 (MM3) основного режима

Включает:

- Обнаружение Технологии NAT

- Часть первая обмена DH

```
*Sep 21 08:33:43.381: ISAKMP (0): received packet from 2001:DB8::2 dport 500
sport 500 Global (R) MM_SA_SETUP
*Sep 21 08:33:43.381: ISAKMP: (0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.381: ISAKMP: (0): Old State = IKE_R_MM2 New State = IKE_R_MM3
*Sep 21 08:33:43.381: ISAKMP: (0): processing KE payload. message ID = 0
*Sep 21 08:33:43.393: ISAKMP: (0): processing NONCE payload. message ID = 0
*Sep 21 08:33:43.393: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::2
*Sep 21 08:33:43.393: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.393: ISAKMP: (1011): vendor ID is DPD
*Sep 21 08:33:43.393: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.393: ISAKMP: (1011): speaking to another IOS box!
*Sep 21 08:33:43.393: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.393: ISAKMP: (1011): vendor ID seems Unity/DPD but major 0
mismatch
*Sep 21 08:33:43.393: ISAKMP: (1011): vendor ID is XAUTH
*Sep 21 08:33:43.393: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.393: ISAKMP: (1011): Old State = IKE_R_MM3 New State =
IKE_R_MM3
```

Сообщение 4 (MM4) основного режима

Включает:

- Информационное наполнение обнаружения NAT
- Продолжение обмена DH

```
*Sep 21 08:33:43.405: ISAKMP: (1011): sending packet to 2001: DB8::2 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Sep 21 08:33:43.405: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.405: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.405: ISAKMP: (1011): Old State = IKE_R_MM3 New State =
IKE_R_MM4
```

Сообщение 5 (MM5) основного режима - инициатор передает его идентичность

Включает:

- Локальная идентификационная информация
- Ключ

```
*Sep 21 08:33:43.425: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) MM_KEY_EXCH
*Sep 21 08:33:43.425: ISAKMP: (1011):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.425: ISAKMP: (1011): Old State = IKE_R_MM4 New State =
IKE_R_MM5
*Sep 21 08:33:43.425: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.425: ISAKMP (1011): ID payload
  next-payload : 8
  type         : 5
  address      : 2001: DB8::2
  protocol     : 17
  port        : 500
  length      : 24
```

```
*Sep 21 08:33:43.425: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.425: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.425: ISAKMP: (1011): processing NOTIFY INITIAL_CONTACT
protocol 1 spi 0, message ID = 0, sa = 0x6D12A00
*Sep 21 08:33:43.425: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.425: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::2
*Sep 21 08:33:43.425: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.425: ISAKMP: (1011): Process initial contact, bring down
existing phase 1 and 2 SA's with local 2001: DB8::3 remote 2001: DB8::2
remote port 500
*Sep 21 08:33:43.425: ISAKMP: Trying to insert a peer 2001: DB8::3/2001:
DB8::2/500/, and inserted successfully 8E45588.
*Sep 21 08:33:43.425: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.425: ISAKMP: (1011): Old State = IKE_R_MM5 New State =
IKE_R_MM5
```

Сообщение 6 (MM6) основного режима - респондент передает его идентичность. Завершение фазы 1.

Включает:

- Удаленная идентичность передана от узла
- Окончательное решение относительно туннельной группы для выбора

```
*Sep 21 08:33:43.425: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.425: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.425: ISAKMP (1011): ID payload
  next-payload : 8
  type          : 5
  address       : 2001: DB8::3
  protocol      : 17
  port         : 500
  length        : 24
*Sep 21 08:33:43.425: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.425: ISAKMP: (1011): sending packet to 2001: DB8::2 my_port
500 peer_port 500 (R) MM_KEY_EXCH
*Sep 21 08:33:43.425: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.425: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.425: ISAKMP: (1011): Old State = IKE_R_MM5 New State =
IKE_P1_COMPLETE
```

Связанная конфигурация:

```
crypto isakmp identity ...
```

Сообщение 1 (QM1) быстрого режима

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPSec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
```

```

*Sep 21 08:33:43.433: ISAKMP: attributes in transform:
*Sep 21 08:33:43.433: ISAKMP:     encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:     SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:     SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:     SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:     authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:     key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
  local_proxy= ::/0/256/0,
  remote_proxy= ::/0/256/0,
  protocol= ESP, transform= NONE (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY New State =
IKE_QM_SPI_STARVE

```

Соответствующая конфигурация:

```

*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPsec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP: attributes in transform:
*Sep 21 08:33:43.433: ISAKMP:     encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:     SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:     SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:     SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:     authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:     key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
  local_proxy= ::/0/256/0,
  remote_proxy= ::/0/256/0,
  protocol= ESP, transform= NONE (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi

```

```
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY New State =
IKE_QM_SPI_STARVE
```

Сообщение 2 (QM2) быстрого режима

Включает:

- Удаленный конец передает параметры
- Короче двух предложенных сроков службы фазы 2 выбран

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPsec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP: attributes in transform:
*Sep 21 08:33:43.433: ISAKMP: encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP: SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP: SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP: SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP: authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP: key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
local_proxy= ::/0/256/0,
remote_proxy= ::/0/256/0,
protocol= ESP, transform= NONE (Tunnel),
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY New State =
IKE_QM_SPI_STARVE
```

Соответствующая конфигурация:

```
*Sep 21 08:33:43.433: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: set new node 1371333358 to QM_IDLE
*Sep 21 08:33:43.433: ISAKMP: (1011): processing HASH payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing SA payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):Checking IPsec proposal 1
*Sep 21 08:33:43.433: ISAKMP: transform 1, ESP_AES
*Sep 21 08:33:43.433: ISAKMP: attributes in transform:
```



```

*Sep 21 08:33:43.433: ISAKMP:      encaps is 1 (Tunnel)
*Sep 21 08:33:43.433: ISAKMP:      SA life type in seconds
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (basic) of 3600
*Sep 21 08:33:43.433: ISAKMP:      SA life type in kilobytes
*Sep 21 08:33:43.433: ISAKMP:      SA life duration (VPI) of 0x0 0x46 0x50 0x0
*Sep 21 08:33:43.433: ISAKMP:      authenticator is HMAC-SHA
*Sep 21 08:33:43.433: ISAKMP:      key length is 128
*Sep 21 08:33:43.433: ISAKMP: (1011):atts are acceptable.
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1
*Sep 21 08:33:43.433: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 2001: DB8::3:0, remote= 2001: DB8::2:0,
  local_proxy= ::/0/256/0,
  remote_proxy= ::/0/256/0,
  protocol= ESP, transform= NONE (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*Sep 21 08:33:43.433: ISAKMP: (1011): processing NONCE payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011): processing ID payload. message ID =
1371333358
*Sep 21 08:33:43.433: ISAKMP: (1011):QM Responder gets spi
*Sep 21 08:33:43.433: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.433: ISAKMP: (1011): Old State = IKE_QM_READY New State =
IKE_QM_SPI_STARVE

```

Сообщение 3 (QM3) быстрого режима - фаза два должна быть завершена и туннельный интерфейс

```

*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel123,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2 New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP

```

Маршрутизатор IOS - инициатор

Сообщение 1 (MM1) основного режима - исходный контакт

Включает:

- Идентификаторы поставщиков (VID)
- Емкости
- Предложения по фазе 1
- Сопоставление безопасности (SA) IKE
- IPSec уже создает шаблон для SA

***Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23, changed state to up**

*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport 500 sport 500 Global (R) QM_IDLE

*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE reason "QM done (await)"

*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH

***Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE**

*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)

*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP

Соответствующая конфигурация:

***Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23, changed state to up**

*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport 500 sport 500 Global (R) QM_IDLE

*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE reason "QM done (await)"

*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH

***Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE**

*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)

*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP

Сообщение 2 (MM2) основного режима - отвечает на исходный контакт

Включает:

- Узел выбирает политику Протокола ISAKMP для использования
- IKE SA

***Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel23, changed state to up**

*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport 500 sport 500 Global (R) QM_IDLE

*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE reason "QM done (await)"

*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH

***Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE**

*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)

*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP

Сообщение 3 (MM3) основного режима - обнаружение NAT и обмен Диффи-Хеллмана

Включает:

- Информационное наполнение обнаружения NAT и хэш
- Инициирование обмена DH
- Поддержка Dead Peer Detection (DPD)

```

*Sep 21 08:33:43.437: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel123,
changed state to up
*Sep 21 08:33:43.437: ISAKMP (1011): received packet from 2001: DB8::2 dport
500 sport 500 Global (R) QM_IDLE
*Sep 21 08:33:43.437: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "QM done (await)"
*Sep 21 08:33:43.437: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.437: ISAKMP: (1011): Old State = IKE_QM_R_QM2 New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.437: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.437: IPSEC(key_engine_enable_outbound): rec'd enable notify
from ISAKMP

```

Сообщение 4 (MM4) основного режима - обнаружение NAT и обмен Диффи-Хеллмана

Включает:

- Информационное наполнение обнаружения NAT
- Инициирование обмена DH
- Дополнительные VID (DPD, поддержка Unity)
- Знание того, чтобы говорить с другим устройством IOS

```

*Sep 21 08:33:43.273: ISAKMP (0): received packet from 2001: DB8::3 dport 500
sport 500 Global (I) MM_SA_SETUP
*Sep 21 08:33:43.273: ISAKMP: (0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.273: ISAKMP: (0): Old State = IKE_I_MM3 New State = IKE_I_MM4

*Sep 21 08:33:43.273: ISAKMP: (0): processing KE payload. message ID = 0
*Sep 21 08:33:43.281: ISAKMP: (0): processing NONCE payload. message ID = 0
*Sep 21 08:33:43.281: ISAKMP: (0):found peer pre-shared key matching 2001:
DB8::3
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): vendor ID is Unity
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): vendor ID is DPD
*Sep 21 08:33:43.281: ISAKMP: (1011): processing vendor id payload
*Sep 21 08:33:43.281: ISAKMP: (1011): speaking to another IOS box!
*Sep 21 08:33:43.281: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.281: ISAKMP: (1011): Old State = IKE_I_MM4 New State =
IKE_I_MM4

```

Сообщение 5 (MM5) основного режима - передает идентичность

Включает:

- Идентичность удаленного узла (ID)

```

*Sep 21 08:33:43.293: ISAKMP: (1011): Send initial contact
*Sep 21 08:33:43.293: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.293: ISAKMP (1011): ID payload
  next-payload : 8
  type         : 5
  address      : 2001: DB8::2
  protocol     : 17
  port        : 500
  length      : 24

```

```
*Sep 21 08:33:43.293: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.293: ISAKMP: (1011): sending packet to 2001: DB8::3 my_port
500 peer_port 500 (I) MM_KEY_EXCH
*Sep 21 08:33:43.293: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.293: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.293: ISAKMP: (1011): Old State = IKE_I_MM4 New State =
IKE_I_MM5
```

Соответствующая конфигурация:

```
*Sep 21 08:33:43.293: ISAKMP: (1011): Send initial contact
*Sep 21 08:33:43.293: ISAKMP: (1011): SA is doing pre-shared key authentication
using id type ID_IPV6_ADDR
*Sep 21 08:33:43.293: ISAKMP (1011): ID payload
  next-payload : 8
  type         : 5
  address      : 2001: DB8::2
  protocol     : 17
  port         : 500
  length       : 24
*Sep 21 08:33:43.293: ISAKMP: (1011):Total payload length: 24
*Sep 21 08:33:43.293: ISAKMP: (1011): sending packet to 2001: DB8::3 my_port
500 peer_port 500 (I) MM_KEY_EXCH
*Sep 21 08:33:43.293: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.293: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.293: ISAKMP: (1011): Old State = IKE_I_MM4 New State =
IKE_I_MM5
```

Сообщение 6 (MM6) основного режима - идентичность удаленного узла, фаза 1 установлена

Включает:

- Повторно введите запущенные времена
- Удаленная идентичность (в этом случае адрес)
- Решение приземлиться на профиль

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
  next-payload : 8
  type         : 5
  address      : 2001: DB8::3
  protocol     : 17
  port         : 500
  length       : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/, and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =
IKE_I_MM6
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
```

IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE

***Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE**

Соответствующая конфигурация:

*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH

*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0

*Sep 21 08:33:43.297: ISAKMP (1011): ID payload

next-payload : 8

type : 5

address : **2001: DB8::3**

protocol : 17

port : 500

length : 24

*Sep 21 08:33:43.297: ISAKMP: (0):: **peer matches *none* of the profiles**

*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0

*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated

*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:

DB8::3

*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:

DB8::3/500/, and inserted successfully 9344BE8.

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH

*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =

IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,

IKE_PROCESS_MAIN_MODE

*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =

IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,

IKE_PROCESS_COMPLETE

***Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =**

IKE_P1_COMPLETE

Сообщение 1 (QM1) быстрого режима - узел запускает фазу 2

Включает:

- Удаленные и локальные Proxy Id
- Набор (наборы) преобразований

*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH

*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0

*Sep 21 08:33:43.297: ISAKMP (1011): ID payload

next-payload : 8

type : 5

address : **2001: DB8::3**

protocol : 17

port : 500

length : 24

*Sep 21 08:33:43.297: ISAKMP: (0):: **peer matches *none* of the profiles**

*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0

*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated

*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:

DB8::3

```
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/, and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE
```

Соответствующая конфигурация:

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
    next-payload : 8
    type          : 5
    address       : 2001: DB8::3
    protocol      : 17
    port          : 500
    length        : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/, and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE
```

Сообщение 2 (QM2) быстрого режима

Включает:

- Подтверждение идентичности прокси
- Тип туннеля
- Параметры настройки Совершенной передающей тайны (PFS)

```
*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
    next-payload : 8
```

```

type      : 5
address   : 2001: DB8::3
protocol  : 17
port      : 500
length    : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/, and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE

```

Соответствующая конфигурация:

```

*Sep 21 08:33:43.297: ISAKMP (1011): received packet from 2001: DB8::3 dport
500 sport 500 Global (I) MM_KEY_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): processing ID payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP (1011): ID payload
  next-payload : 8
  type          : 5
  address       : 2001: DB8::3
  protocol      : 17
  port          : 500
  length        : 24
*Sep 21 08:33:43.297: ISAKMP: (0):: peer matches *none* of the profiles
*Sep 21 08:33:43.297: ISAKMP: (1011): processing HASH payload. message ID = 0
*Sep 21 08:33:43.297: ISAKMP: (1011): SA authentication status: authenticated
*Sep 21 08:33:43.297: ISAKMP: (1011): SA has been authenticated with 2001:
DB8::3
*Sep 21 08:33:43.297: ISAKMP: Trying to insert a peer 2001: DB8::2/2001:
DB8::3/500/, and inserted successfully 9344BE8.
*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM5 New State =
IKE_I_MM6

*Sep 21 08:33:43.297: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.297: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_I_MM6

*Sep 21 08:33:43.301: ISAKMP: (1011):Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE_I_MM6 New State =
IKE_P1_COMPLETE

```

Сообщение 3 (QM3) быстрого режима - установление фазы 2

Включает:

- Значение политики безопасности индексирует (SPI) для передачи трафика

```
*Sep 21 08:33:43.305: ISAKMP: (1011): Sending an IKE IPv6 Packet.
*Sep 21 08:33:43.305: ISAKMP: (1011): deleting node 1371333358 error FALSE
reason "No Error"
*Sep 21 08:33:43.305: ISAKMP: (1011):Node 1371333358, Input =
IKE_MSG_FROM_PEER, IKE_QM_EXCH
*Sep 21 08:33:43.305: ISAKMP: (1011): Old State = IKE_QM_I_QM1 New State =
IKE_QM_PHASE2_COMPLETE
*Sep 21 08:33:43.305: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*Sep 21 08:33:43.305: IPSEC(crypto_ipsec_create_ipsec_sas): Map found
Tunnel23-head-0
*Sep 21 08:33:43.305: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting
with the same proxies and peer 2001: DB8::3
*Sep 21 08:33:43.305: IPSEC(create_sa): sa created,
(sa) sa_dest= 2001: DB8::2, sa_proto= 50,
sa_spi= 0x45F16A9A(1173449370),
sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 305
sa_lifetime(k/sec)= (4608000/3439)
*Sep 21 08:33:43.305: IPSEC(create_sa): sa created,
(sa) sa_dest= 2001: DB8::3, sa_proto= 50,
sa_spi= 0x221A7153(572158291),
sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 306
sa_lifetime(k/sec)= (4608000/3439)
R2(config-if)#
*Sep 21 08:33:43.309: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel23, changed state to up
```

Туннельная проверка

```
sh crypto ipsec sa
```

```
interface: Tunnel23
  Crypto map tag: Tunnel23-head-0, local addr 2001: DB8::2

protected vrf: (none)
local ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (::/0/0/0)
current_peer 2001: DB8::3 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 2001: DB8::2,
remote crypto endpt.: 2001: DB8::3
path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb Ethernet0/0
current outbound spi: 0x221A7153(572158291)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x45F16A9A(1173449370)
  transform: esp-aes esp-sha-hmac ,
  in use settings = {Tunnel, }
  conn id: 305, flow_id: SW:305, sibling_flags 80000041, crypto map:
Tunnel23-head-0
  sa timing: remaining key lifetime (k/sec): (4183789/3408)
  IV size: 16 bytes
```



```
replay detection support: Y
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x221A7153(572158291)
```

```
transform: esp-aes esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
```

```
conn id: 306, flow_id: SW:306, sibling_flags 80000041, crypto map:
```

```
Tunnel23-head-0
```

```
sa timing: remaining key lifetime (k/sec): (4183790/3408)
```

```
IV size: 16 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE
```

```
R2(config-if)#do ping fe80::23:3
```

```
Output Interface: tunnel23
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to FE80::23:3, timeout is 2 seconds:
```

```
Packet sent with a source address of FE80::23:2%Tunnel23
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/20 ms
```

```
R2(config-if)#do sh crypto ipsec sa | i caps|ident
```

```
local ident (addr/mask/prot/port): (::/0/0/0)
```

```
remote ident (addr/mask/prot/port): (::/0/0/0)
```

```
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
```

```
#pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
```

Туннель подключен и проходящий трафик.

Дополнительные сведения

- [Статья Википедии относительно IPsec](#) ; стандарт и ссылки содержат много полезных сведений.
- [IPsec ASA и отладки IKE \(агрессивный режим IKEv1\) устраняющий неполадки Технических примечаний](#)
- [IPsec ASA и отладки IKE \(Основной режим IKEv1\) Технические примечания по поиску и устранению проблем](#)
- [Cisco Systems – техническая поддержка и документация](#)