

# IOS IPSec和IKE调试- IKEv1主模式排除故障

## 目录

[简介](#)

[核心问题](#)

[方案](#)

[使用的调试](#)

[IOS 路由器配置](#)

[加密配置](#)

[其他旁拉](#)

[调试](#)

[IOS响应方旁拉](#)

[主模式消息1 \(MM1\)](#)

[主模式消息2 \(MM2\) -发送我们的回复](#)

[主模式消息3 \(MM3\)](#)

[主模式消息4 \(MM4\)](#)

[主模式消息5 \(MM5\) -发起者发送其标识](#)

[主模式消息6 \(MM6\) -响应方发送其标识。阶段1完成。](#)

[快速模式消息1 \(QM1\)](#)

[快速模式消息2 \(QM2\)](#)

[快速模式消息3 \(QM3\) -相位两应该完成和隧道接口上升](#)

[IOS路由器-发起者](#)

[主模式消息1 \(MM1\) -初始联系](#)

[主模式消息2 \(MM2\) -对初始联系的回复](#)

[主模式消息3 \(MM3\) - NAT发现号和Diffie-Hellman交换](#)

[主模式消息4 \(MM4\) - NAT发现号和Diffie-Hellman交换](#)

[主模式消息5 \(MM5\) -发送标识](#)

[主模式消息6 \(MM6\) -远端对等体标识，阶段1设立](#)

[快速模式消息1 \(QM1\) -对等体开始第2阶段](#)

[快速模式消息2 \(QM2\)](#)

[快速模式消息3 \(QM3\) -第2阶段建立](#)

[通道验证](#)

[相关信息](#)

## 简介

本文提供信息了解在Cisco IOS软件的调试，当使用主模式和预先共享密钥(PSK)时。

本文在配置里也提供信息关于怎样翻译某些调试线路。

这些主题没有讨论：

- 通过流量，在通道设立了后
- IPSec或Internet Key Exchange (IKE)基本概念

## 核心问题

IKE和IPSec调试倾向于获得隐秘。Cisco技术支持中心(TAC)经常使用这些Bug了解与IPSec VPN隧道建立的一问题哪里查找。

## 方案

主模式典型地使用在LAN-to-LAN隧道之间，或者在远程访问(EzVPN)的情况下，当证书使用验证时。

那些调试是从运行15.2(1)T软件版本的Cisco IOS设备。

两个主要方案在本文描述：

- IOS发起者侧
- IOS响应方侧

在本文中，在两个站点之间的一个基于VTI的通道根据IPv6设立。

注意：

请使用[命令查找工具\(仅限注册用户\)](#)为了得到关于用于本文的命令的更多信息。

使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

## 使用的调试

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

## IOS 路由器配置

### 加密配置

```
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
```

## 其他旁拉

```
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
```

## 调试

### IOS响应方旁拉

#### 主模式消息1 (MM1)

最初的提议对于IKE包括：

- 加密
- 切细
- Diffie-Hellman (DH)组
- 寿命

```
*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

```

相关的配置：

```

crypto isakmp policy 10
authentication pre-share

```

## 主模式消息2 (MM2) -发送我们的回复

```

*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

```

## 主模式消息3 (MM3)

包括：

- 网络地址转换(NAT)发现
- DH交换第一部分

```

*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_MESG_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_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
*Sep 21 08:33:43.393: ISAKMP: (1011): Old State = IKE_R_MM3 New State =
IKE_R_MM3
```

## 主模式消息4 (MM4)

包括：

- NAT检测有效负载
- DH交换的继续

```
*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_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.405: ISAKMP: (1011): Old State = IKE_R_MM3 New State =
IKE_R_MM4
```

## 主模式消息5 (MM5) -发起者发送其标识

包括：

- 本地身份信息
- 密钥

```
*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_MESG_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

## 主模式消息6 (MM6) -响应方发送其标识。阶段1完成。

包括：

- 从对等体发送的远程标识
- 关于隧道组的最终决策选择

```
*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
```

相关的配置：

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

## 快速模式消息1 (QM1)

```
*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
```

## 相关配置：

```
*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
```

## 快速模式消息2 (QM2)

包括：

- 远程终端发送参数
- 短两个报价的第2阶段寿命选择

```
*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
```

## 相关配置：

```
*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
```

## 快速模式消息3 (QM3) -相位两应该完成和隧道接口上升

```
*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
```

## IOS路由器-发起者

### 主模式消息1 (MM1) -初始联系

包括：

- 供应商ID (VID)
- 产能
- 阶段1建议
- IKE安全关联(SA)
- IPsec已经创建SAS的一个模板

```
*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
```

相关配置：

```
*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
```

## 主模式消息2 (MM2) -对初始联系的回复

包括：

- 对等体选择互联网安全协会和密钥管理协议(ISAKMP)策略使用
- SA IKE

```
*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
```

## 主模式消息3 (MM3) - NAT发现号和Diffie-Hellman交换

包括：

- NAT发现有效负载和哈希
- DH交换开始
- 对端死机检测(DPD)支持

```
*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
```

## 主模式消息4 (MM4) - NAT发现号和Diffie-Hellman交换

包括：

- NAT发现有效负载
- DH交换开始
- 另外的VIDs (DPD , Unity支持)
- 知识谈与另一个IOS设备

```
*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
```

## 主模式消息5 (MM5) -发送标识

包括：

- 远端对等体标识(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_MSG_INTERNAL,
IKE_PROCESS_COMPLETE
*Sep 21 08:33:43.293: ISAKMP: (1011): Old State = IKE_I_MM4 New State =
IKE_I_MM5
```

相关配置：

```
*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
```

## 主模式消息6 (MM6) -远端对等体标识，阶段1设立

包括：

- 重新生成密钥开始的时期
- 远程标识(在这种情况下地址)
- 决策登陆在配置文件

```
*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
```

相关配置：

```
*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

```

## 快速模式消息1 (QM1) -对等体开始第2阶段

包括：

- 远程和本地代理ID
- 变换集

```

*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

```

相关配置：

```

*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

```

## 快速模式消息2 (QM2)

包括：

- 代理身分的确认
- 隧道类型
- 完善的转发秘密(PFS)设置

```

*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\_MESG\_INTERNAL,  
IKE\_PROCESS\_COMPLETE

\*Sep 21 08:33:43.301: ISAKMP: (1011): Old State = IKE\_I\_MM6 New State =  
IKE\_P1\_COMPLETE

## 相关配置：

\*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

## 快速模式消息3 (QM3) -第2阶段建立

包括：

- 设置通过流量的安全策略索引(斯皮)

\*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\_MESG\_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
```

## 通道验证

```
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
```

通道启用和通过流量。

## 相关信息

- [在IPSec的维基百科条款](#);标准和参考包含很多有用的信息。
- [积极模式\)排除故障技术说明的ASA IPsec和IKE调试\(IKEv1](#)
- [主模式\)排除故障TechNote的ASA IPsec和IKE调试\(IKEv1](#)
- [技术支持和文档 - Cisco Systems](#)