

Cisco VPN 完全配置指南

路由器连接的故障诊断与排除（1）

一、ISAKMP/IKE 阶段 1 连接

可以使用下面的命令来故障诊断和排除 ISAKMP/IKE 阶段 1 的连接

- `show crypto isakmp sa` 显示具有管理连接的状态
- `debug crypto isakmp` 显示构建管理连接的步骤和通过管理连接构建数据连接的步骤
- `debug crypto pki {messages| transactions}` 显示路由器和 CA 之间对于证书申请和验证功能的交互
- `debug crypto engine` 显示与加密和解密数据包有关的事件，同时应用于阶段 1 和阶段 2 的连接
- `clear crypto isakmp` 删除所有特定的管理连接

（1）`show crypto isakmp sa` 命令

QM_IDLE 代表成功建立了到达相关对等设备的连接，MM_NO_STATE 或 AG_NO_STATE 代表连接的初始建立存在问题。

```
spoke1# show crypto isakmp sa
dst          src          state          conn-id slot
192.1.1.40    192.1.1.42    QM_IDLE        2          0
```

下面两种最常见的问题导致管理连接不能建立

- 忘记了在远端设备的接口上激活 `crypto map` 或配置文件
- 在远端对等设备上没有匹配的 ISAKMP/IKE 阶段 1 的策略

如果看到 MM_KEY_EXCH 或 AG_INIT_EXCH 的状态，很可能设备验证失败，对于预共享密钥或 RSA 加密随机数来说，确保已经正确地配置了预共享密钥，对于证书确保：

- 证书没有过期
- 在两台对等设备上的日期和时间是正确的
- 证书还没有被吊销

（2）`debug crypto isakmp` 命令

（一）L2L 会话使用该命令

成功建立一个 IPSec L2L 会话

```
ISAKMP (0:0): received packet from 192.1.1.42 dport 500 sport 500 Global (N) NEW SA (1)
ISAKMP: Created a peer struct for 192.1.1.42, peer port 500
ISAKMP: Locking peer struct 0x64DB0004, IKE refcount 1 for crypto_isakmp_process_block
ISAKMP: local port 500, remote port 500 insert sa successfully
sa = 651706A4
ISAKMP: (0:0:N/A:0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP: (0:0:N/A:0):Old State = IKE_READY New State = IKE_R_MM1
```

```

ISAKMP: (0:0:N/A:0): processing SA payload. message ID = 0
    output omitted
ISAKMP: (0:0:N/A:0): Looking for a matching key for 192.1.1.42 (2)
    in default
ISAKMP: (0:0:N/A:0): : success
ISAKMP: (0:0:N/A:0): found peer pre-shared key matching
    192.1.1.42
ISAKMP: (0:0:N/A:0): local preshared key found
ISAKMP : Scanning profiles for xauth ...
ISAKMP: (0:0:N/A:0): Checking ISAKMP transform 1 against (3)
    priority 1 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash SHA
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP: (0:0:N/A:0): atts are acceptable. Next payload is 0 (4)
    output omitted
ISAKMP: (0:1:SW:1): sending packet to 192.1.1.42 my_port 500
    peer_port 500 (R) MM_SA_SETUP
ISAKMP (0:134217729): received packet from 192.1.1.42 dport 500 (5)
    sport 500 Global (R) MM_SA_SETUP
ISAKMP: (0:1:SW:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM2 New State = IKE_R_MM3
ISAKMP: (0:1:SW:1): processing KE payload. message ID = 0
ISAKMP: (0:1:SW:1): processing NONCE payload. message ID = 0
ISAKMP: (0:0:N/A:0): Looking for a matching key for 192.1.1.42
    in default
ISAKMP: (0:0:N/A:0): : success
ISAKMP: (0:1:SW:1): found peer pre-shared key matching 192.1.1.42
ISAKMP: (0:1:SW:1): SKEYID state generated (6)
ISAKMP: (0:1:SW:1): processing vendor id payload
ISAKMP: (0:1:SW:1): vendor ID is Unity
ISAKMP: (0:1:SW:1): processing vendor id payload
ISAKMP: (0:1:SW:1): vendor ID is DPD
ISAKMP: (0:1:SW:1): processing vendor id payload
ISAKMP: (0:1:SW:1): speaking to another IOS box!
ISAKMP: (0:1:SW:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM3 New State = IKE_R_MM3
ISAKMP: (0:1:SW:1): sending packet to 192.1.1.42 my_port 500 peer_

```

```

    port 500 (R) MM_KEY_EXCH
ISAKMP: (0:1:SW:1): Input = IKE_MSG_INTERNAL,
    IKE_PROCESS_COMPLETE
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM3 New State = IKE_R_MM4
ISAKMP (0:134217729): received packet from 192.1.1.42 dport 500    (7)
    sport 500 Global (R) MM_KEY_EXCH
ISAKMP: (0:1:SW:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM4 New State = IKE_R_MM5
ISAKMP: (0:1:SW:1): processing ID payload. message ID = 0
ISAKMP (0:134217729): ID payload
    next-payload : 8
    type          : 1
    address       : 192.1.1.42
    protocol      : 17
    port          : 500
    length        : 12
ISAKMP: (0:1:SW:1):: peer matches *none* of the profiles
ISAKMP: (0:1:SW:1): processing HASH payload. message ID = 0
ISAKMP: received payload type 17
ISAKMP: (0:1:SW:1): processing NOTIFY_INITIAL_CONTACT protocol 1
    spi 0, message ID = 0, sa = 651706A4
ISAKMP: (0:1:SW:1): SA authentication status:    (8)
    authenticated
ISAKMP: (0:1:SW:1): Process initial contact, bring down existing
    phase 1 and 2 SA's with local 192.1.1.40
    remote 192.1.1.42 remote port 500
ISAKMP: (0:1:SW:1): SA authentication status:
    authenticated
ISAKMP: (0:1:SW:1): SA has been authenticated with 192.1.1.42
ISAKMP: Trying to insert a peer 192.1.1.40/192.1.1.42/500/,
    and inserted successfully 64DB0004.
ISAKMP: (0:1:SW:1): IKE_DPD is enabled, initializing timers
ISAKMP: (0:1:SW:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM5 New State = IKE_R_MM5
ISAKMP: (0:1:SW:1): SA is doing pre-shared key authentication
    using id type ID_IPV4_ADDR

    output omitted

ISAKMP: (0:1:SW:1): Input = IKE_MSG_INTERNAL,
    IKE_PROCESS_COMPLETE
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM5 New State =
    IKE_P1_COMPLETE
ISAKMP: (0:1:SW:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE (9)
ISAKMP: (0:1:SW:1): Old State = IKE_P1_COMPLETE New State =

```

```

IKE_P1_COMPLETE
ISAKMP (0:134217729): received packet from 192.1.1.42 dport 500 (10)
    sport 500 Global (R) QM_IDLE
ISAKMP: set new node 482536716 to QM_IDLE
ISAKMP: (0:1:SW:1): processing HASH payload. message ID =
    482536716
ISAKMP: (0:1:SW:1): processing SA payload. message ID = 482536716
ISAKMP: (0:1:SW:1): Checking IPsec proposal 1 (11)
ISAKMP: transform 1, ESP_AES
ISAKMP:   attributes in transform:
ISAKMP:     encaps is 1 (Tunnel)
ISAKMP:     SA life type in seconds
ISAKMP:     SA life duration (basic) of 3600
ISAKMP:     SA life type in kilobytes
ISAKMP:     SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP:     authenticator is HMAC-SHA
ISAKMP:     key length is 128
ISAKMP: (0:1:SW:1):atts are acceptable. (12)

    output omitted

ISAKMP: (0:1:SW:1): Creating IPsec SAs (13)
    inbound SA from 192.1.1.42 to 192.1.1.40 (f/i) 0/ 0
    (proxy 192.168.3.0 to 192.168.2.0)
    has spi 0x705B8268 and conn_id 0 and flags 2
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    has client flags 0x0
    outbound SA from 192.1.1.40 to 192.1.1.42 (f/i) 0/0
    (proxy 192.168.2.0 to 192.168.3.0)
    has spi 1221163868 and conn_id 0 and flags A
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    has client flags 0x0
ISAKMP: (0:1:SW:1): sending packet to 192.1.1.42 my_port 500
    peer_port 500 (R) QM_IDLE
ISAKMP: (0:1:SW:1):Node 482536716, Input = IKE_MESG_FROM_IPSEC,
    IKE_SPI_REPLY
ISAKMP: (0:1:SW:1):Old State = IKE_QM_SPI_STARVE New State =
    IKE_QM_R_QM2
ISAKMP: Locking peer struct 0x64DB0004, IPSEC refcount 2 for
    from create_transforms
ISAKMP: Unlocking IPSEC struct 0x64DB0004 from create_
    transforms, count 1
ISAKMP (0:134217729): received packet from 192.1.1.42 dport 500

```

```

sport 500 Global (R) QM_IDLE
ISAKMP: (0:1:SW:1):deleting node 482536716 error FALSE reason
"QM done (await)"
ISAKMP: (0:1:SW:1):Node 482536716, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
ISAKMP: (0:1:SW:1):Old State = IKE_QM_R_QM2 New State = IKE_QM_ (14)
PHASE2_COMPLETE

```

- (1) 主模式的交换正在开始，还没有策略被共享，路由器仍处于 MM_NO_STATE 状态。
- (2) 路由器首先核实有一个预共享密钥匹配对等设备的地址，在这点上还没有被验证
- (3) ISAKMP/IKE 策略的比较在这里开始
- (4) 这个消息代表匹配的策略已经找到
- (5) 这个验证开始于预共享密钥的地方，记住验证发生在两台路由器上，因此会看见两组相应的验证过程。
- (6) 路由器产生的一个验证随机数发送给远端的对等设备
- (7) 路由器收到了来自远端对等设备的做验证的随机数
- (8) 接收的随机数被核实，对等设备被验证
- (9) 阶段 1 完成了
- (10) 阶段 2（快速模式）开始了
- (11) 路由器为数据连接查找一个匹配的数据传输集
- (12) 为数据连接找到了一个匹配的数据传输集
- (13) 数据连接的 SA 已构建
- (14) 阶段 2 完成

不匹配的 ISAKMP/IKE 阶段 1 策略

```

ISAKMP: (0:0:N/A:0):Checking ISAKMP transform 1 against priority (1)
1 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash SHA
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP: (0:0:N/A:0):Hash algorithm offered does not match policy!
ISAKMP: (0:0:N/A:0):atts are not acceptable. Next payload is 0 (2)
ISAKMP: (0:0:N/A:0):Checking ISAKMP transform 1 against priority (3)
65535 policy
ISAKMP: encryption AES-CBC
ISAKMP: keylength of 128
ISAKMP: hash SHA
ISAKMP: default group 1
ISAKMP: auth pre-share

```

```

ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP: (0:0:N/A:0):Encryption algorithm offered does not
      match policy!
ISAKMP: (0:0:N/A:0):atts are not acceptable. Next payload is 0      (4)
ISAKMP: (0:0:N/A:0):no offers accepted!
ISAKMP: (0:0:N/A:0): phase 1 SA policy not acceptable!
      (local 192.1.1.40 remote 192.1.1.42)
ISAKMP: (0:0:N/A:0):incrementing error counter on sa: construct_
      fail_ag_init
ISAKMP: (0:0:N/A:0): sending packet to 192.1.1.42 my_port 500
      peer_port 500 (R) MM_NO_STATE
ISAKMP: (0:0:N/A:0):peer does not do paranoid keepalives.
ISAKMP: (0:0:N/A:0):deleting SA reason "Phase1 SA policy      (5)
      proposal not accepted" state (R) MM_NO_STATE
      (peer 192.1.1.42)

```

- (1) 路由器正在将远端对等设备的策略 1 和本地策略 1 进行比较检查
- (2) 在第一策略的比较中没有匹配
- (3) 路由器将远端对等设备的策略 1 和路由器的本地策略进行比较检查
- (4) 再次，与对等设备的策略没有匹配
- (5) 管理连接被终止，因为在对等设备之间没有匹配的策略（MM_NO_STATE）

不匹配的预共享密钥

```

ISAKMP: (0:0:N/A:0):atts are acceptable. Next payload is 0      (1)
ISAKMP: (0:1:SW:1): processing vendor id payload
ISAKMP: (0:1:SW:1): vendor ID seems Unity/DPD but major
      245 mismatch
ISAKMP (0:134217729): vendor ID is NAT-T v7
ISAKMP: (0:1:SW:1): processing vendor id payload
ISAKMP: (0:1:SW:1): vendor ID seems Unity/DPD but major
      157 mismatch
ISAKMP: (0:1:SW:1): vendor ID is NAT-T v3
ISAKMP: (0:1:SW:1): processing vendor id payload
ISAKMP: (0:1:SW:1): vendor ID seems Unity/DPD but major
      123 mismatch
ISAKMP: (0:1:SW:1): vendor ID is NAT-T v2
ISAKMP: (0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_PROCESS_
      MAIN_MODE
ISAKMP: (0:1:SW:1):Old State = IKE_R_MM1 New State = IKE_R_MM1
ISAKMP: (0:1:SW:1): constructed NAT-T vendor-07 ID
ISAKMP: (0:1:SW:1): sending packet to 192.1.1.42 my_port 500
      peer_port 500 (R) MM_SA_SETUP
ISAKMP: (0:1:SW:1):Input = IKE_MSG_INTERNAL, IKE_

```

```

PROCESS_COMPLETE
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM1 New State = IKE_R_MM2
ISAKMP (0:134217729): received packet from 192.1.1.42 dport 500 (2)
    sport 500 Global (R) MM_SA_SETUP
ISAKMP: (0:1:SW:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM2 New State = IKE_R_MM3
ISAKMP: (0:1:SW:1): processing KE payload. message ID = 0
ISAKMP: (0:1:SW:1): processing NONCE payload. message ID = 0
ISAKMP: (0:0:N/A:0): Looking for a matching key for 192.1.1.42 in (3)
    default
ISAKMP: (0:0:N/A:0): : success
ISAKMP: (0:1:SW:1): found peer pre-shared key matching 192.1.1.42
ISAKMP: (0:1:SW:1): SKEYID state generated (4)

output omitted

ISAKMP: (0:1:SW:1): sending packet to 192.1.1.42 my_port 500 (5)
    peer_port 500 (R) MM_KEY_EXCH
ISAKMP: (0:1:SW:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP: (0:1:SW:1): Old State = IKE_R_MM3 New State = IKE_R_MM4
ISAKMP (0:134217729): received packet from 192.1.1.42 dport 500
    sport 500 Global (R) MM_KEY_EXCH
ISAKMP: reserved not zero on ID payload! (6)
%CRYPTO-4-IKMP_BAD_MESSAGE: IKE message from 192.1.1.42
    failed its sanity check or is malformed
ISAKMP: (0:1:SW:1): incrementing error counter on sa: PAYLOAD_
MALFORMED

```

- (1) 找到了一个匹配的阶段 1 的策略
 - (2) 预共享密钥验证开始，收到了来自远端对等设备的随机数（使用预共享密钥建立的）
 - (3) 一个匹配的 `crypto isakmp key` 命令在远端对等设备上找到了（对等设备的 IP 地址）
 - (4) 路由器产生了一个随机数来核实验证
 - (5) 该路由器将其随机数的信息发送给远端对等设备
 - (6) 验证随机数失败，密钥被重试多次，对等设备放弃构建管理连接
- 当使用 `show crypto isakmp sa` 时，这个状态会是 `MM_KEY_EXCH`

(二) 远程访问会话使用该命令

成功建立一个到 **Easy VPN** 服务器的 **IPSec** 远程访问会话

```

ISAKMP (0:0): received packet from 192.168.1.100 dport 500
    sport 500 Global (N) NEW SA

output omitted

ISAKMP (0:0): ID payload (1)

```

next-payload : 13
type : 11
group id : admin
protocol : 17
port : 500
length : 13

output omitted

ISAKMP: (0:0:N/A:0): Authentication by
xauth preshared

ISAKMP: (0:0:N/A:0):Checking ISAKMP (2)
transform 1 against priority 10 policy

ISAKMP: encryption AES-CBC
ISAKMP: hash SHA
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 256

ISAKMP: (0:0:N/A:0):Hash algorithm offered does not match policy!
ISAKMP: (0:0:N/A:0):atts are not acceptable. Next payload is 3

output omitted

ISAKMP: (0:0:N/A:0):Checking ISAKMP transform 6 against priority
10 policy

ISAKMP: encryption AES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth XAUTHInitPreShared
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: keylength of 128

ISAKMP: (0:0:N/A:0):atts are acceptable. (3)

ISAKMP: (0:2:SW:1): processing KE payload. message ID = 0

ISAKMP: (0:2:SW:1): processing NONCE payload. message ID = 0

output omitted

ISAKMP: (0:2:SW:1):SKEYID state generated

ISAKMP: (0:2:SW:1):SA is doing pre-shared key authentication (4)
plus XAUTH using id type ID_IPV4_ADDR

ISAKMP (0:134217730): ID payload next-payload : 10

type : 1
address : 192.1.1.40
protocol : 17

output omitted

ISAKMP (0:134217730): received packet from 192.168.1.100
dport 500 sport 500 Global (R) AG_INIT_EXCH

ISAKMP:(0:2:SW:1): processing HASH payload. message ID = 0

ISAKMP:(0:2:SW:1): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 652680F0

ISAKMP:(0:2:SW:1):SA authentication status: (5)
authenticated

output omitted

ISAKMP:(0:2:SW:1):SA has been authenticated with 192.168.1.100

output omitted

ISAKMP:(0:2:SW:1):IKE_DPD is enabled, initializing timers (6)

output omitted

ISAKMP:(0:2:SW:1):Need XAUTH (7)

ISAKMP: set new node -753458994 to CONF_XAUTH

ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2

ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2

ISAKMP:(0:2:SW:1): initiating peer config to 192.168.1.100.
ID= -753458994

ISAKMP:(0:2:SW:1): sending packet to 192.168.1.100 my_port 500
peer_port 500 (R) CONF_XAUTH

output omitted

ISAKMP (0:134217730): received packet from 192.168.1.100 (8)
dport 500 sport 500 Global (R) CONF_XAUTH

ISAKMP:(0:2:SW:1):processing transaction payload from
192.168.1.100. message ID = -753458994

ISAKMP: Config payload REPLY

ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2

ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2

ISAKMP:(0:2:SW:1):deleting node -753458994 error FALSE reason
"Done with xauth request/reply exchange"

output omitted

ISAKMP: Config payload ACK

ISAKMP:(0:2:SW:1): (blank) XAUTH ACK Processed (9)

ISAKMP:(0:2:SW:1):deleting node 147119650 error FALSE reason
"Transaction mode done"

ISAKMP:(0:2:SW:1):Input = IKE_MESG_FROM_PEER, IKE_CFG_ACK

ISAKMP:(0:2:SW:1):Old State = IKE_XAUTH_SET_SENT New State =

IKE_P1_COMPLETE

output omitted

*Mar 1 05:06:03.199: ISAKMP (0:134217730): received packet (10)
from 192.168.1.100 dport 500 sport 500 Global (R) QM_IDLE

*Mar 1 05:06:03.203: ISAKMP: set new node -1691114311 to QM_IDLE

*Mar 1 05:06:03.203: ISAKMP:(0:2:SW:1):processing transaction
payload from 192.168.1.100. message ID = -1691114311

*Mar 1 05:06:03.203: ISAKMP: Config payload REQUEST

output omitted

ISAKMP/author: Author request for group admin successfully
sent to AAA

output omitted

ISAKMP:(0:2:SW:1):allocating address 192.168.0.222 (11)

ISAKMP: Sending private address: 192.168.0.222

ISAKMP: Sending subnet mask: 255.255.255.0

ISAKMP: Sending IP4_DNS server address: 192.168.0.10

ISAKMP: Sending IP4_NBNS server address: 192.168.0.12

ISAKMP: Sending ADDRESS_EXPIRY seconds left to use the address:
86395

ISAKMP (0/134217730): Unknown Attr: UNKNOWN (0x7000)

ISAKMP: Sending save password reply value 0

Sending DEFAULT_DOMAIN default domain name: cisco.com

ISAKMP: Sending split include name splitremote network
192.168.0.0 mask 255.255.255.0 protocol 0, src port 0,
dst port 0

ISAKMP: Sending SPLIT_DNS domain name: cisco.com

output omitted

ISAKMP:(0:2:SW:1):Input = IKE_MESG_INTERNAL,

IKE_PHASE1_COMPLETE(12)

ISAKMP:(0:2:SW:1):Old State = IKE_P1_COMPLETE New State = IKE_
P1_COMPLETE

ISAKMP (0:134217730): received packet (13)
from 192.168.1.100 dport 500 sport 500 Global (R) QM_IDLE

output omitted

ISAKMP:(0:2:SW:1): processing SA payload.

ISAKMP:(0:2:SW:1):Checking IPsec proposal 1

ISAKMP: transform 1, ESP_AES

ISAKMP: attributes in transform:

ISAKMP: authenticator is HMAC-MD5

```
ISAKMP:      key length is 256
ISAKMP:      encaps is 1 (Tunnel)
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of 0x0 0x20 0xC4 0x9B
ISAKMP: (0:2:SW:1):atts are acceptable. (14)
```

output omitted

```
ISAKMP: (0:2:SW:1): Creating IPsec SAs (15)
    inbound SA from 192.168.1.100 to 192.1.1.40 (f/i) 0/0
    (proxy 192.168.0.222 to 0.0.0.0)
    has spi 0x213909D3 and conn_id 0 and flags 2
    lifetime of 2147483 seconds
    has client flags 0x0
    outbound SA from 192.1.1.40 to 192.168.1.100 (f/i) 0/0
    (proxy 0.0.0.0 to 192.168.0.222)
    has spi 2072708995 and conn_id 0 and flags A
    lifetime of 2147483 seconds
    has client flags 0x0
```

output omitted

```
*Mar 1 05:06:03.367: ISAKMP: (0:2:SW:1):Old State = IKE_QM_R_ (16)
    QM2 New State = IKE_QM_PHASE2_COMPLETE
```

output omitted

- (1) Easy VPN 远端设备（客户端）建立了一个 Easy VPN 服务器的连接（路由器）并且指定它想访问“admin”组。
- (2) 阶段 1 的第一个策略不匹配远端设备的策略列表
- (3) 阶段 1 的一些策略被比较后，找到了一个匹配
- (4) 使用预共享密钥开始“admin”组的组验证
- (5) 组验证成功
- (6) DPD 被启动
- (7) XAUTH 已经在 Easy VPN 服务器上启动，服务器提示用户输入用户名和口令
- (8) 服务器收到了来自远端设备的用户名和口令
- (9) 用户验证成功，如果它不成功，将会看到一个 debug 行里面有 retransmitting Phase 2 CONF_XAUTH，服务器会重传 XAUTH 的用户名和口令的查询
- (10) 远端设备发超了 IKE 模式配置
- (11) 远端设备被分配给它的策略，其中一个 IP 地址是 102.168.0.222，如果用户不能分配到一个 IP 地址，将看到下面的 debug 消息，deleting SA reason"Failed to allocate ip address."
- (12) ISAKMP/IKE 阶段 1 完成
- (13) 在阶段 2, 一个匹配的数据传输集搜索
- (14) 找到了一个匹配的数据传输集
- (15) 两 IPSec SA 为数据连接建立了
- (16) 阶段 2 已经完成了

(3) debug crypto pki 命令

此命令用于故障诊断与排除 CA 和路由器之间的交互问题，必须指定两个参数中的一个，messages 或 transactions，messages 参数理论上打印出路由器和 CA 之间发送的消息内容，只用于思科的工作人员。而 transactions 参数是有用的，它是显示发生的事件。

故障诊断与排除证书申请过程

```
RTR(config)# crypto ca authenticate caserver
Certificate has the following attributes:
Fingerprint:A5DE3C51 AD8B0207 B60BED6D 9356FB00
00:44:00:CRYPTO_PKI:Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&
    message=caserver HTTP/1.0
00:44:00:CRYPTO_PKI:http connection opened
00:44:01:CRYPTO_PKI:HTTP response header:
    HTTP/1.1 200 OK
    Server:Microsoft-IIS/5.0
    Date:Fri, 17 Apr 2005 19:50:59 GMT
    Content-Length:2693
    Content-Type:application/x-x509-ca-ra-cert
    Content-Type indicates we have received CA and RA certificates.
00:42:01:CRYPTO_PKI:WARNING:A certificate chain could not be
    constructed while selecting certificate status
00:42:01:CRYPTO_PKI:WARNING:A certificate chain could not be
    constructed while selecting certificate status
00:42:01:CRYPTO_PKI:Name:CN = caserverRA, O = Cisco System, C = US
00:42:01:CRYPTO_PKI:Name:CN = caserverRA, O = Cisco System, C = US
00:42:01:CRYPTO_PKI:transaction GetCACert completed
00:42:01:CRYPTO_PKI:CA certificate received.
% Do you accept this certificate? [yes/no]:yes
Router(config)# crypto ca enroll caserver
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
    password to the CA Administrator in order to revoke your
certificate.
    For security reasons your password will not be saved in the
configuration.
    Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will be:Router.cisco.com
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [yes/no]:no
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
```

% The 'show crypto ca certificate' command will also show the fingerprint.
Fingerprint: 2CFC6265 77BA6496 3AEFCB50 29BC2BF2
00:43:39:CRYPTO_PKI:transaction PKCSReq completed
00:43:39:CRYPTO_PKI:status:
00:43:39:CRYPTO_PKI:http connection opened
00:43:39:CRYPTO_PKI: received msg of 1924 bytes
00:43:39:CRYPTO_PKI:HTTP response header:
HTTP/1.1 200 OK
Server:Microsoft-IIS/5.0
Date:Fri, Apr Nov 2005 19:51:28 GMT
Content-Length:1778
Content-Type:application/x-pki-message
00:45:29:CRYPTO_PKI:signed attr:pki-message-type:
00:45:29:13 01 33
00:45:29:CRYPTO_PKI:signed attr:pki-status:
00:45:29:13 01 30
00:45:29:CRYPTO_PKI:signed attr:pki-recipient-nonce:
00:45:29:04 10 B4 C8 2A 12 9C 8A 2A 4A E1 E5 15 DE 22 C2 B4 FD
00:45:29:CRYPTO_PKI:signed attr:pki-transaction-id:
00:45:29:13 20 34 45 45 41 44 42 36 33 38 43 33 42 42 45 44 45 39 46
00:45:29:34 38 44 33 45 36 39 33 45 33 43 37 45 39
00:45:29:CRYPTO_PKI:status = 100:certificate is granted
00:45:29:CRYPTO_PKI:All enrollment requests completed.
00:45:29:%CRYPTO-6-CERTRET:Certificate received from
Certificate Authority

(4) debug crypto engine 命令

使用 debug crypto engine 命令

*Mar 1 04:03:17.338: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
*Mar 1 04:03:17.454: CryptoEngine0: generate alg parameter
*Mar 1 04:03:17.554: CRYPTO_ENGINE: Dh phase 1 status: 0 (1)
*Mar 1 04:03:17.682: CryptoEngine0: generate alg parameter
*Mar 1 04:03:17.810: CryptoEngine0: create ISAKMP SKEYID (2)
for conn id 14
*Mar 1 04:03:17.818: CryptoEngine0: generate hmac context
for conn id 14
*Mar 1 04:03:17.838: CryptoEngine0: generate hmac context
for conn id 14
*Mar 1 04:03:17.842: CryptoEngine0: clear dh number for (3)
conn id 1
*Mar 1 04:03:17.850: CryptoEngine0: generate hmac context
for conn id 14
*Mar 1 04:03:17.878: CryptoEngine0: generate hmac context

```
    for conn id 14
*Mar 1 04:03:17.878: CryptoEngine0: validate proposal (4)
*Mar 1 04:03:17.878: CryptoEngine0: validate proposal request
*Mar 1 04:03:17.882: CryptoEngine0: generate hmac context
    for conn id 14
*Mar 1 04:03:17.882: CryptoEngine0: ipsec allocate flow (5)
```

- (1) DH 基于这个和下一个消息是成功的
- (2) 设备验证开始，预共享密钥使用随机数被加密
- (3) DH 不再需要，临时的 DH 连接被清除
- (4) 为 ISAKMP/IKE 阶段 2 的数据连接寻找一个匹配的传输集
- (5) 两数据连接成功被构建

制作 · 张选波