IPSec 故障处理

文档版本	01
发布日期	2019-12-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 引言

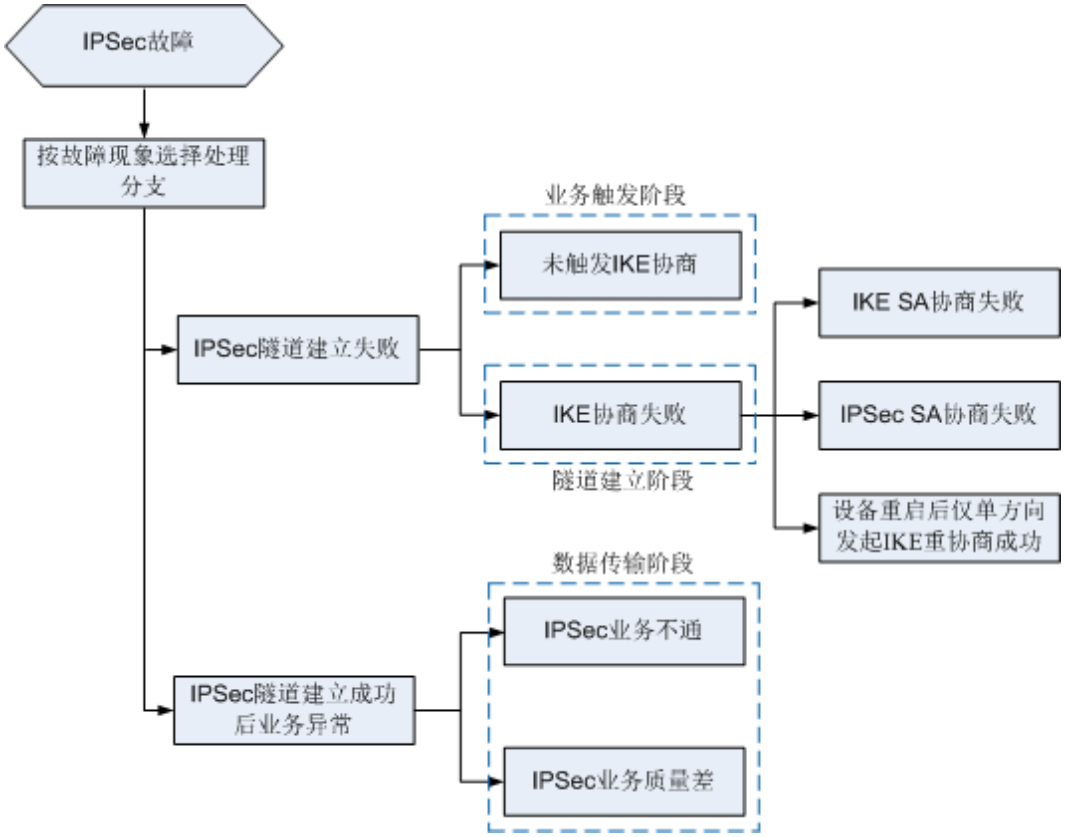
本文档介绍了IPSec VPN故障的最常见解决方案和咨询问题，包括故障处理指导、典型故障案例、IPSec的常见问题和解决方法，这些解决方案直接来自华为技术支持所解决的业务请求，这些解决方案可以在IPSec的VPN连接深入故障处理之前实现。本文档提供了在开始故障处理前的检查项，需要对常见的操作步骤进行的检查并联系华为技术支持工程师。

2 故障处理思路

IPSec故障有两种现象：IPSec隧道建立失败或IPSec隧道建立成功后业务异常。

如图2-1所示，列出了IPSec故障的处理思路。

图 2-1 故障处理思路



IKE SA或IPSec SA协商失败是IPSec故障的核心问题，可以结合**IPSec隧道建立失败故障分析**章节中IKE协商过程进行深入分析；其它IPSec故障问题一般为设备基本特性的错误配置，如接口、ACL、路由、NAT等，需要结合具体场景来处理。

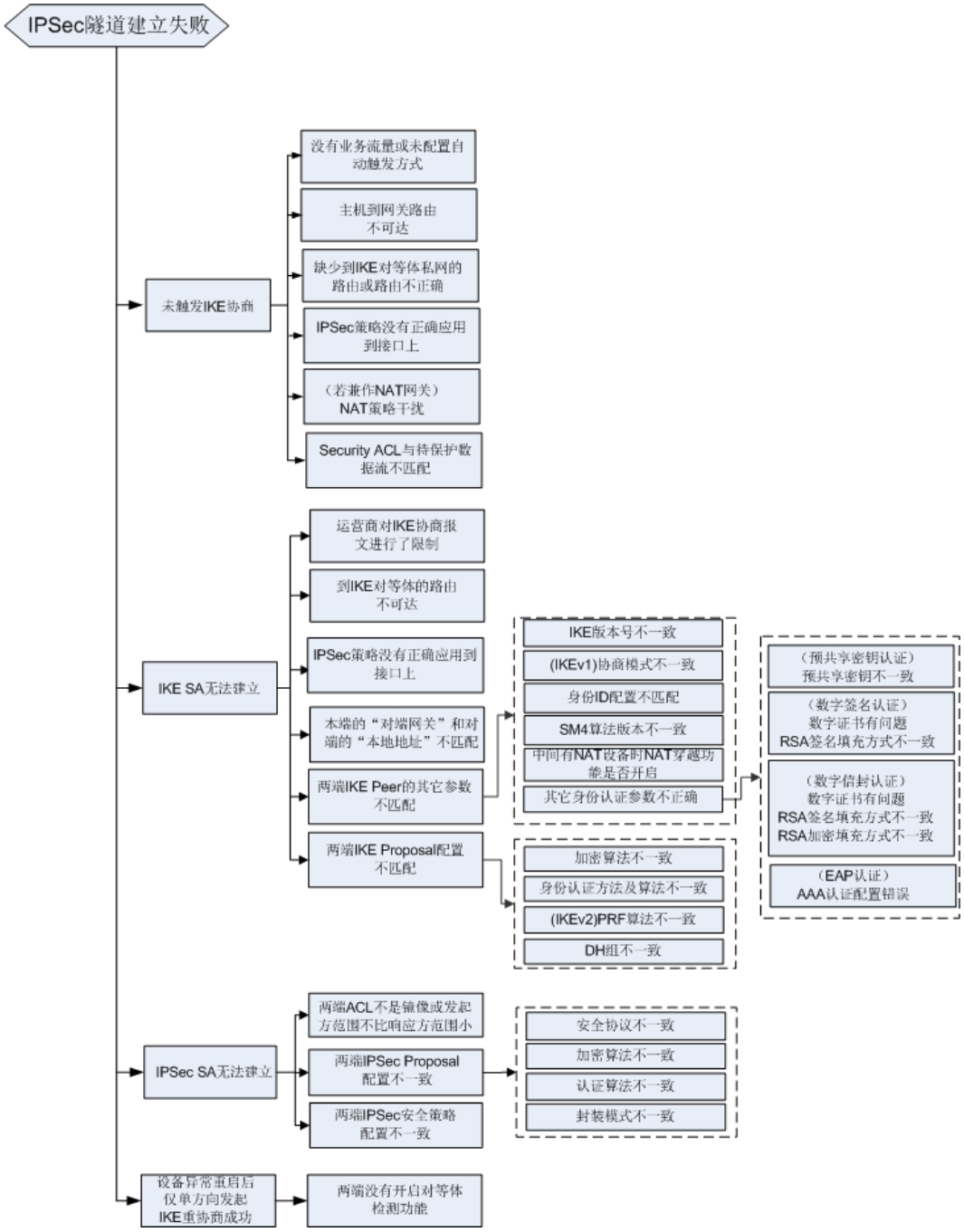
网络管理员在例行检查或者接到故障上报时，可以参照图2-1找到故障处理指南。对于一些复杂的故障，可以依据故障现象，结合**IPSec工作原理**，逐层分析其触发原因，直到根本原因。网络管理员了解了总体思路，有助于问题的定位和处理。

IPSec隧道建立失败和IPSec业务异常的故障树如下所示。

2.1 IPSec 隧道建立失败故障树

IPSec隧道建立失败故障树如**图2-2**所示。

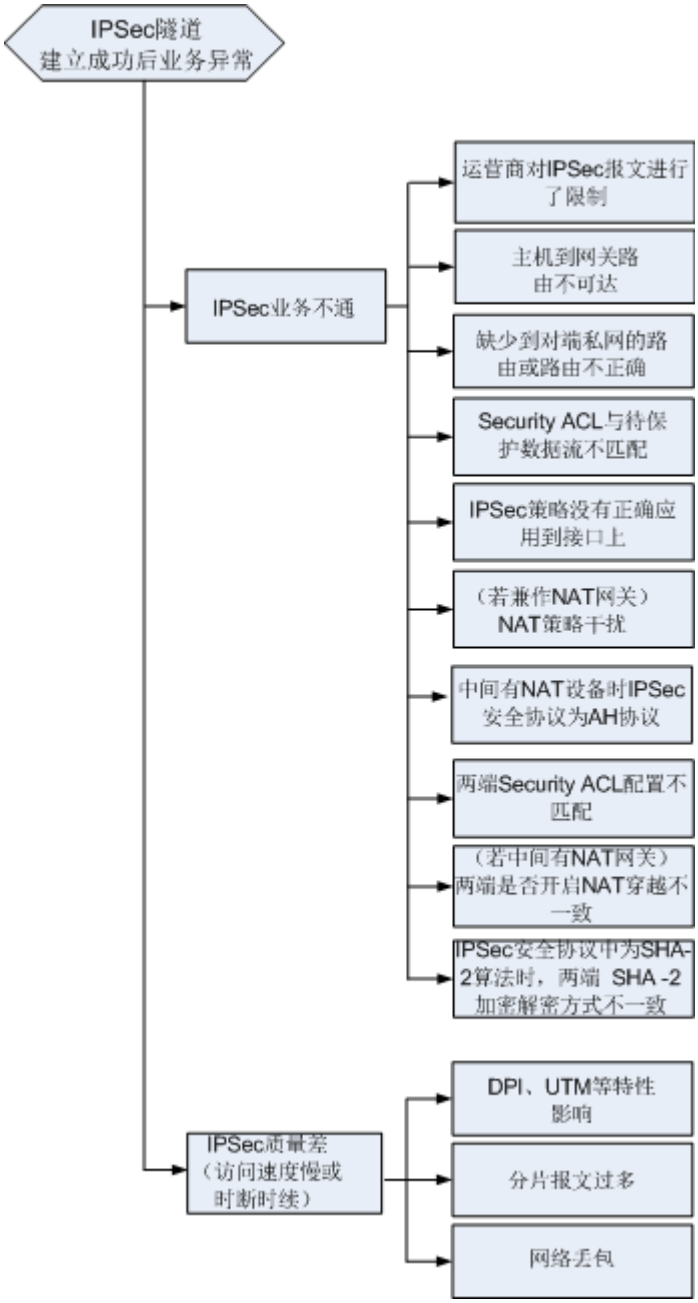
图 2-2 IPSec 隧道建立失败故障树



2.2 IPSec 业务异常故障树

IPSec业务异常故障树如图2-3所示。

图 2-3 IPSec 业务异常故障树

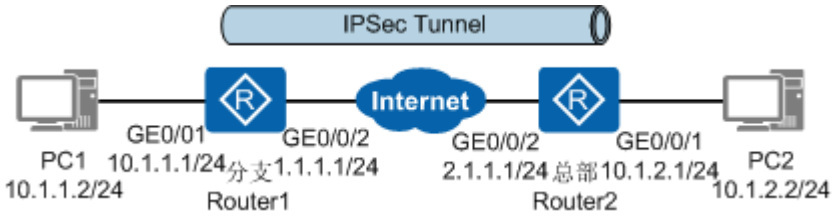


3 故障处理指南

3.1 故障处理索引

这里对IPSec故障处理指南进行梳理，根据问题的现象进行分类，建立索引表，如**表3-1**所示。

图 3-1 IPSec 组网图



如**图3-1**所示，在Router1和Router2上分别执行命令**display ipsec sa**查看到SA状态。

表 3-1 故障处理索引表

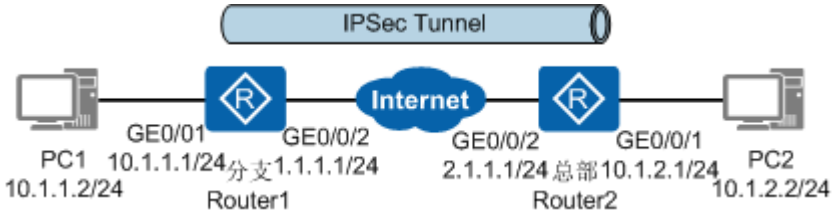
故障现象	具体处理指南
Router1上没有显示信息，IPSec隧道建立失败。同时执行命令**display ipsec statistics**，发现**outbound ok**为0，说明本端IKE协商报文没有发出，没有触发协商IPSec隧道。	**3.2 未触发IKE协商**
Router1上IKE SA没有建立，IPSec隧道建立失败。同时执行命令**display ipsec statistics**，发现**outbound ok**不为0，说明IKE报文已经发出。	**3.3 IKE SA协商失败**
Router1上IPSec SA没有建立，IPSec隧道建立失败。	**3.4 IPSec SA协商失败**
Router1上SA建立成功，Router2上SA建立失败。	**3.5 设备异常重启后仅单方向发起IKE重协商成功**
Router1和Router2上查看到IPSec SA的信息，IPSec隧道已建立成功但是存在如下问题： • 分支和总部两端的用户完全不能互相访问。 • 分支和总部两端的用户单向访问正常，反向不通。例如，总部用户可以访问分支服务器，分支用户不能访问总部服务器。 • 分支和总部两端的用户访问部分网段正常，部分不通。 • 在点到多点网络中还可能存在分支用户访问总部正常，但不同分支用户之间访问不通。 • 在IPSec网关兼做NAT网关的场景中还可能出现所有流量都经NAT转换发送出去，没有流量进入VPN的问题。	**3.6 IPSec隧道建立成功后业务不通**
Router1和Router2上查看到IPSec SA的信息，IPSec隧道已建立成功但是存在如下问题： • 业务访问速度慢。 • 业务访问时断时续，也可能彻底中断。	**3.7 IPSec隧道建立成功后业务质量差**

3.2 未触发 IKE 协商

3.2.1 现象描述

如图3-2所示，Router间部署IPSec后，PC之间互访不通。

图 3-2 IPSec 组网图



在Router1上执行命令**display ike sa**查看SA状态，没有显示信息，说明IPSec隧道建立失败。

```
<Router1> display ike sa
```

在Router1上执行命令**display ipsec statistics**查看IPSec统计信息。

```
<Router1> display ipsec statistics
.......
  negotiate about packet statistics:
    IKE fwd packet ok: 0, err: 0
    IKE ctrl packet inbound ok: 0, outbound ok: 0
    SoftExpr: 0, HardExpr: 0, DPDOper: 0
    trigger ok: 0, switch sa: 0, sync sa: 0
    recv IKE nat keepalive: 0, IKE input: 0
```

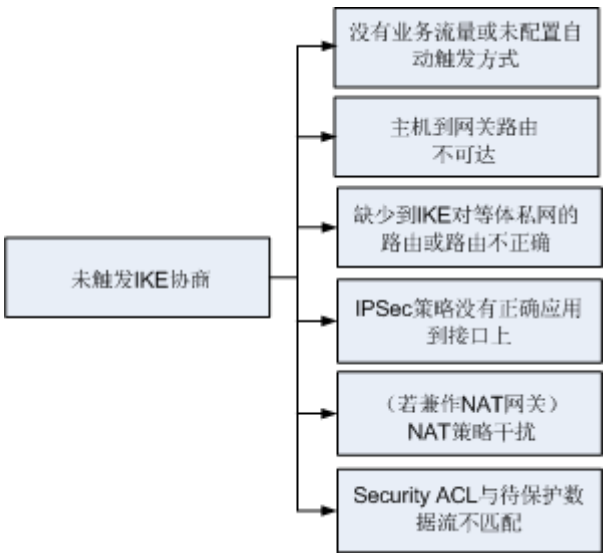
- IPSec SA建立的触发方式为自动触发方式

  outbound ok为0，说明本端IKE协商报文没有发出，没有触发协商IPSec隧道。

- IPSec SA建立的触发方式为流量触发方式

  trigger ok为0，说明没有数据流触发IKE协商。如果**trigger ok**不为0，**outbound ok**为0，说明本端IKE协商报文没有发出，没有触发协商IPSec隧道。

3.2.2 可能原因



3.2.3 定位步骤

操作步骤

步骤1 执行命令**display ipsec policy**检查IPSec SA的触发方式。

```
<Huawei> display ipsec policy
==========================================
IPSec policy group: "10"
Using interface: GigabitEthernet1/0/0
==========================================
    Sequence number: 10
    Policy Alias: map1-10
    Security data flow: 3100/IPv4
    Peer name    :  rut2
    Perfect forward secrecy: DH group 14
    Proposal name:  prop1
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    SA trigger mode: Traffic-based   //IPSec SA的触发方式
......
```

因为IPSec SA的触发方式默认为流量触发方式，所以触发IKE协商的前提条件为有业务流量，用户可以通过Ping方式来触发IKE协商。用户可以在ISAKMP方式安全策略视图下执行命令**sa trigger-mode auto**配置IPSec SA的触发方式为自动触发方式，这样可以避免无业务流量时无法触发IKE协商。

步骤2 检查私网路由及公网路由是否可达。

执行命令**ping**确认是否可以Ping通私网和公网路由。如果Ping不通，则请确保链路正常、接口Up、路由等网络配置正确。

步骤3 检查IPSec策略是否正确应用到隧道接口上。

执行命令**display ipsec interface brief**查看隧道接口是否有IPSec策略信息，如果没有，则需在该接口上应用IPSec策略。

```
<Huawei> display ipsec interface brief
-----------------------------------------------
  IPSec policy        : policy1
  Using interface     : GigabitEthernet1/0/0
  IPSec policy number : 10
  IPSec policy Type   : policy
-----------------------------------------------
```

步骤4 检查Security ACL与待保护数据流是否匹配。

执行命令**display ipsec policy**查看Security ACL序号，然后再执行命令**display acl** *acl-number*检查ACL配置与待保护数据流是否匹配，如果不匹配，则请修改正确。

```
<Huawei> display ipsec policy
==========================================
IPSec policy group: "10"
Using interface: GigabitEthernet1/0/0
==========================================
    Sequence number: 10
    Policy Alias: map1-10
    Security data flow: 3100/IPv4   //Security ACL
    Peer name    :  rut2
    Perfect forward secrecy: DH group 14
    Proposal name:  prop1
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    SA trigger mode: Traffic-based
......
```



```
<Huawei> display acl 3100
Advanced ACL 3100, 1 rule ( Reference counter 1 )
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 (0 times matched)
```

步骤5 检查是否有NAT策略干扰IPSec保护数据流。

转发流程中IPSec模块位于NAT模块（NAT Server、目的NAT、源NAT）之后，故应确保NAT Server、目的NAT不影响IPSec对保护的数据流的处理。

执行命令**display ipsec interface brief**查看应用了IPSec策略的接口，然后执行命令**display current-configuration interface** *interface-type interface-number*查看IPSec接口是否配置了NAT策略。

如果应用IPSec安全策略的接口同时配置了NAT，由于设备先执行NAT，会导致IPSec不生效，此时需要：

- NAT引用的ACL规则deny目的IP地址是IPSec引用的ACL规则中的目的IP地址，避免对IPSec保护的数据流进行NAT转换。
- IPSec引用的ACL规则匹配经过NAT转换后的IP地址。

步骤6 若以上方法均没有定位出问题所在，请收集以下信息，并联系技术支持人员。

1. 收集配置信息、上述步骤的操作结果，并记录到文件中。
2. 执行命令**debugging**收集IPSec隧道建立过程中的信息。

   ```
   <Huawei> terminal monitor
   <Huawei> terminal debugging
   <Huawei> debugging ikev1 all   //采用IKEv1协商时收集的debugging信息
   <Huawei> debugging ikev2 all   //采用IKEv2协商时收集的debugging信息
   <Huawei> debugging ipsec all
   <Huawei> debugging adp-ipsec   //V200R007及之前版本，执行此命令收集debugging信息
   ```

3. 关闭**debugging**后，一键式收集设备的所有诊断信息并导出文件。
   a. 执行命令**display diagnostic-information** *file-name*采集设备诊断信息并保存为文件。

      ```
      <Huawei> display diagnostic-information dia-info.txt
      Now saving the diagnostic information to the device
       100%
      Info: The diagnostic information was saved to the device successfully
      ```

   b. 当诊断信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。

      您可以在用户视图下执行**dir**命令，确认文件是否正确生成。
4. 收集设备的日志和告警信息并导出文件。
   a. 执行**save logfile**命令，将缓冲区的日志和告警信息保存为文件。

      ```
      <Huawei> save logfile all
      Info: Save logfile successfully.
      Info: Save diagnostic logfile successfully.
      ```

   b. 当日志和告警信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。
5. 收集接口的报文信息，通过TFTP等方式将其从设备上导出。

   ```
   <Huawei> system-view
   [Huawei] acl 3100
   [Huawei-acl-adv-3100] acl 3100   //定义数据流
   [Huawei-acl-adv-3100] rule 5 permit ip source 10.1.1.1 0 destination 10.2.1.1 0
   [Huawei-acl-adv-3100] rule 5 permit ip source 10.2.1.1 0 destination 10.1.1.1 0
   [Huawei-acl-adv-3100] quit
   [Huawei] packet-capture ipv4-packet 3100 interface GigabitEthernet 1/0/1
   [Huawei] packet-capture startup packet-num 1500   //开启获取报文头信息功能
   [Huawei] packet-capture queue 0 to-file 1.cap   //将获取的报文头信息保存到设备上
   ```


获取报文头后，请删除其相关配置。

----结束

参考信息

数据流触发IKE协商分析：

5.1.2.1 IPSec报文转发流程

案例：

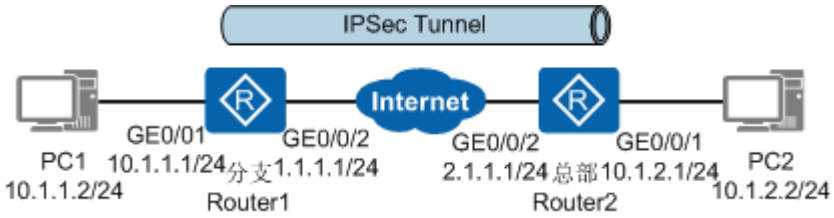
4.1.3 AR路由器由于待保护数据流匹配了NAT Server导致IPSec隧道建立后无法远程登录对端

3.3 IKE SA 协商失败

3.3.1 现象描述

如图3-3所示，Router间部署IPSec后，PC之间互访不通。

图 3-3 IPSec 组网图



1. 在Router1上执行命令**display ike sa**查看SA状态，发现IKE SA没有建立，导致IPSec隧道建立失败。

```
<Router1> display ike sa
IKE SA information :
  Conn-ID    Peer          VPN           Flag(s)            Phase
 ------------------------------------------------------------------------------

  1342       0.0.0.0                     RD|A               v2:1

 Number of IKE SA : 0
 ------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

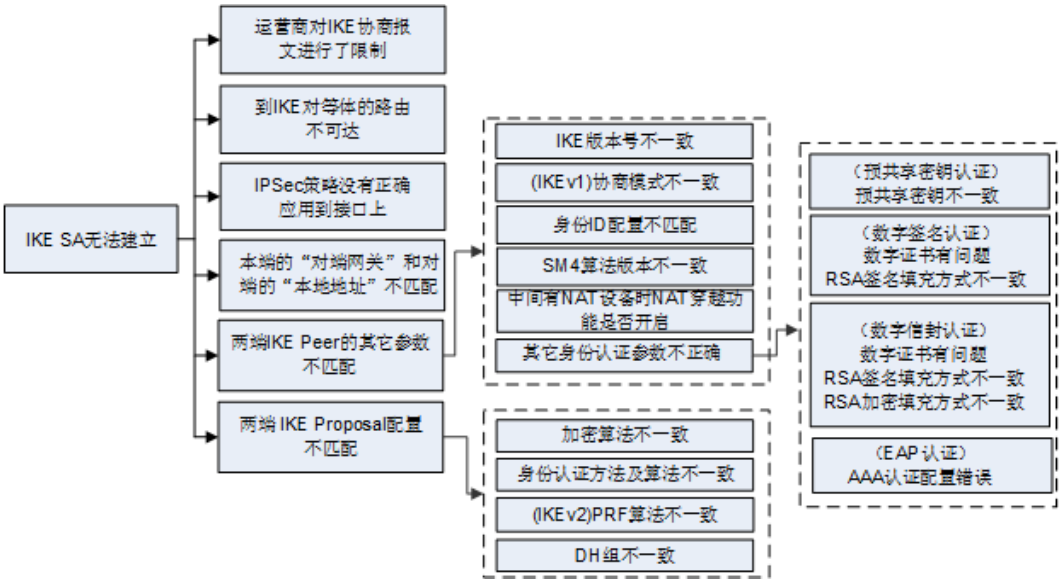
2. 在Router1上执行命令**display ipsec statistics**查看IPSec统计信息，发现**outbound ok**不为0，说明IKE报文已经发出。

```
<Router1> display ipsec statistics
.......
 negotiate about packet statistics:
   IKE fwd packet ok: 0, err: 0
   IKE ctrl packet inbound ok: 0, outbound ok: 4
   SoftExpr: 0, HardExpr: 0, DPDOper: 0
```



```
  trigger ok: 0, switch sa: 0, sync sa: 0
  recv IKE nat keepalive: 0, IKE input: 0
```

3.3.2 可能原因



3.3.3 定位步骤

定位流程

用户可以执行命令**display ike error-info**（V200R008及之后版本支持）查看IKE SA协商失败的原因来快速定位故障，也可以参考如下步骤来定位故障。

操作步骤

步骤1 确认IKE协商响应端是否收到IKE协商报文。

执行命令**display ipsec statistics**查看IKE协商发起方和响应方的IKE报文的统计计数。

```
<Router1> display ipsec statistics
.......
  negotiate about packet statistics:
    IKE fwd packet ok: 0, err: 0
    IKE ctrl packet inbound ok: 0, outbound ok: 0
    SoftExpr: 0, HardExpr: 0, DPDOper: 0
    trigger ok: 0, switch sa: 0, sync sa: 0
    recv IKE nat keepalive: 0, IKE input: 0
```

- 发起方**outbound ok**不为0，但响应方**IKE ctrl packet inbound ok**为0，说明响应端没有收到IKE协商报文，原因可能为：
  - 运营商网络对IKE报文（默认端口号为500或4500的UDP报文）进行了限制。请联系运营商或技术支持人员。
  - Router1和Router2之间路由不可达，请根据步骤2进行排查。
  - 发起方“对端网关”和对端的“本地地址”不匹配，即发起方**remote-address**命令配置错误。请根据步骤3进行排查。
- 发起方**outbound ok**不为0，且响应方**IKE ctrl packet inbound ok**不为0，但是响应方**outbound ok**为0，说明响应方收到了IKE协商报文，但是没有发出响应报文。原因可能为：

  - IPSec策略没有正确的应用到接口上。请执行命令**display ipsec interface brief**检查并确保在接口上已正确地应用IPSec策略。
  - 响应方“对端网关”和对端的“本地地址”不匹配，即响应方**remote-address**命令配置错误。请根据步骤3进行排查。

- 发起方**outbound ok**不为0，**IKE ctrl packet inbound ok**为0，且响应方**IKE ctrl packet inbound ok**和**outbound ok**均不为0，说明响应方收到了IKE协商报文，并且发出了响应报文，但是发起方没有收到响应报文。原因可能为：

  Router1上配置了到达Router2的路由，但是Router2上没有到达Router1的路由。请根据步骤2进行排查。

步骤2 检查IKE对等体的路由可达性。

在IPSec隧道两端接口上执行命令**undo ipsec policy**取消应用IPSec安全策略，然后执行命令**ping -a** *source-ip-address destination-ip-address*进行可达性检查。

如果Ping不通，则请确保链路正常、接口Up、路由等网络配置正确。排除接口、路由等问题后，重新在接口上执行命令**ipsec policy**应用IPSec安全策略。

步骤3 检查本端的“对端网关”和对端的“本地地址”是否匹配。

执行命令**display ike peer**查看IKE Peer的对端IP地址或域名是否匹配。如果不匹配，请在IKE对等体视图下执行命令**remote-address**修改正确。

```
<Huawei> display ike peer name 1
-----------------------------------------
  Peer name                     : 1
  IKE version                   : v1v2
  VPN instance                  :
  Remote IP                     : 1.1.1.1(www.huawei.com)   //指定对端IKE对等体地址或域名
  Authentic IP address          :                           //指定认证地址
  Proposal                      : 1
  Pre-shared-key                : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type                 : IP
  Local ID                      :
  Remote ID type                : any
  Remote ID                     :
......
```

- 当对端使用的是内网IP地址，穿越了NAT设备时：
  - 本端只作为IKE协商响应方

    本端采用策略模板方式IPSec安全策略，在模板中引用的IKE对等体可以不指定对端的IP地址（即不配置**remote-address**命令）。
  - 本端可以作为IKE协商发起方

    本端需采用ISAKMP方式IPSec安全策略，且IKE Peer下指定的对端IP地址为NAT转换后的地址。如果使用IP地址进行认证，则本端还必须执行命令**remote-address authentication-address**指定NAT转换前的IP地址为对端认证地址。
- 对端设备的IP地址不固定但有固定域名，并已执行命令**remote-address host-name**指定对端域名时，对端需要配置DDNS，将域名与动态IP地址绑定，本端配置DNS完成域名解析。

  如果对端域名无法解析，可以执行命令**ip host** *host-name ip-address*配置静态域名解析。

步骤4 检查两端IKE peer的其它配置是否正确。

执行命令**display ike peer**查看两端的IKE版本号、IKEv1协商模式、身份ID或者SM4版本号是否一致，如果不一致，请修改一致。


```
<Huawei> display ike peer name 1
-----------------------------------------
  Peer name                     : 1
  IKE version                   : v1   //IKE版本号
  VPN instance                  :
  Remote IP                     : 1.1.1.1(www.huawei.com)
  Authentic IP address          :
  Proposal                      : 1
  Exchange mode                 : main on phase 1   //IKEv1协商模式
  Pre-shared-key                : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type                 : IP
  Local ID                      :
  Remote ID type                : any
  Remote ID                     :
.....
  RSA encryption-padding        : PKCS1   //RSA加密的填充方式
  RSA signature-padding         : PKCS1   //RSA签名的填充方式
  ipsec sm4 version             : standard   //SM4版本号
.....
```

不同认证方式下的身份认证参数配置不同：

- 若采用了预共享密钥认证，应保证两端的预共享密钥一致。
- 若采用了RSA签名或数字信封认证，应保证数字证书的有效性。
  a. 执行命令**display pki certificate**和**display clock**检查证书到期时间和设备时间。

     如果设备时间不在证书有效期内，请在系统视图下执行命令**clock datetime**修改设备的时间。

     如果证书到期，请重新申请证书或者在IKE对等体视图下执行命令**certificate-check disable**不校验证书的有效性（此方式适用于证书失效时用户无法更新证书场景）。
  b. 执行命令**display ike peer**查看两端的RSA签名或RSA加密的填充方式是否一致。

     如果不一致，请在IKE对等体视图下执行命令**rsa encryption-padding**或**rsa signature-padding**修改一致。

当IKE对等体间存在NAT设备时，请确保已经开启了NAT穿越功能。

步骤5 检查两端IKE proposal配置是否一致。

执行命令**display ike proposal**检查两端认证方法、认证算法、加密算法、DH组、PRF算法是否一致，如果不一致，请修改一致。

```
<Huawei> display ike proposal number 10
-----------------------------------------
 IKE Proposal: 10
   Authentication Method     : PRE_SHARED     //认证方法
   Authentication Algorithm  : SHA2-256       //认证算法
   Encryption Algorithm      : AES-256        //加密算法
   Diffie-Hellman Group      : MODP-2048      //DH组
   SA Duration(Seconds)      : 86400
   Integrity Algorithm       : HMAC-SHA2-256  //完整性算法
   Prf Algorithm             : HMAC-SHA2-256  //PRF算法
-----------------------------------------
```

步骤6 若以上方法均没有定位出问题所在，请收集以下信息，并联系技术支持人员。

1. 收集配置信息、上述步骤的操作结果，并记录到文件中。
2. 执行命令**debugging**收集IPSec隧道建立过程中的信息。

```
<Huawei> terminal monitor
<Huawei> terminal debugging
<Huawei> debugging ikev1 all   //采用IKEv1协商时收集的debugging信息
```

```
<Huawei> debugging ikev2 all   //采用IKEv2协商时收集的debugging信息
<Huawei> debugging ipsec all
<Huawei> debugging adp-ipsec   //V200R007及之前版本，执行此命令收集debugging信息
```

3. 关闭**debugging**后，一键式收集设备的所有诊断信息并导出文件。
   a. 执行命令**display diagnostic-information** *file-name*采集设备诊断信息并保存为文件。

   ```
   <Huawei> display diagnostic-information dia-info.txt
   Now saving the diagnostic information to the device
    100%
   Info: The diagnostic information was saved to the device successfully
   ```

   b. 当诊断信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。
   您可以在用户视图下执行**dir**命令，确认文件是否正确生成。
4. 收集设备的日志和告警信息并导出文件。
   a. 执行**save logfile**命令，将缓冲区的日志和告警信息保存为文件。

   ```
   <Huawei> save logfile all
   Info: Save logfile successfully.
   Info: Save diagnostic logfile successfully.
   ```

   b. 当日志和告警信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。
5. 收集接口的报文信息，通过TFTP等方式将其从设备上导出。

   ```
   <Huawei> system-view
   [Huawei] acl 3100
   [Huawei-acl-adv-3100] acl 3100   //定义数据流
   [Huawei-acl-adv-3100] rule 5 permit ip source 10.1.1.1 0 destination 10.2.1.1 0
   [Huawei-acl-adv-3100] rule 5 permit ip source 10.2.1.1 0 destination 10.1.1.1 0
   [Huawei-acl-adv-3100] quit
   [Huawei] packet-capture ipv4-packet 3100 interface GigabitEthernet 1/0/1
   [Huawei] packet-capture startup packet-num 1500   //开启获取报文头信息功能
   [Huawei] packet-capture queue 0 to-file 1.cap   //将获取的报文头信息保存到设备上
   ```

   获取报文头后，请删除其相关配置。

----结束

参考信息

案例：

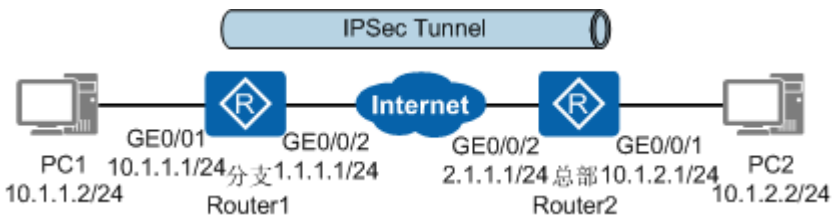
4.1.2 AR路由器由于IPSec参数不一致导致IPSec隧道建立失败

3.4 IPSec SA 协商失败

3.4.1 现象描述

如**图3-4**所示，Router间部署IPSec后，PC之间互访不通。

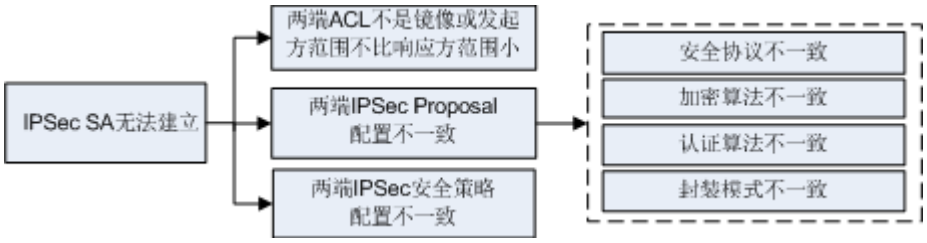
图 3-4 IPSec 组网图



在Router1上执行命令**display ike sa**查看SA状态，发现IPSec SA没有建立，导致IPSec隧道建立失败。

```
<Router1> display ike sa
IKE SA information :
  Conn-ID    Peer          VPN            Flag(s)             Phase
 ------------------------------------------------------------------------------

   8388     2.1.1.1:500                  RD|ST|A             v2:1

 Number of IKE SA : 1
 ------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

3.4.2 可能原因



3.4.3 定位步骤

背景信息

用户可以执行命令**display ike error-info**（V200R008及之后版本支持）查看IPSec SA协商失败的原因来快速定位故障，也可以通过如下步骤来定位故障。

操作步骤

步骤1 检查两端ACL配置是否匹配。

执行命令**display ipsec policy**查看IPSec引用的ACL序号，然后执行命令**display acl** *acl-number*检查两端的ACL规则是否匹配。

```
<Huawei> display ipsec policy
==========================================
IPSec policy group: "10"
Using interface: GigabitEthernet1/0/0
==========================================
    Sequence number: 10
    Policy Alias: map1-10
    Security data flow: 3100/IPv4   //Security ACL
    Peer name    :  rut2
    Perfect forward secrecy: DH group 14
    Proposal name:  prop1
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    SA trigger mode: Traffic-based
......
<Huawei> display acl 3100
Advanced ACL 3100, 1 rule ( Reference counter 1 )
```

```
Acl's step is 5
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255 (0 times matched)
```

配置ACL规则需注意：

- IPSec隧道两端ACL规则定义的协议类型要一致。例如，一端使用IP协议，另一端也必须使用IP协议。
- 当IPSec隧道两端的ACL规则镜像配置时，任意一方发起协商都能保证SA成功建立；当IPSec隧道两端的ACL规则非镜像配置时，只有发起方的ACL规则定义的范围是响应方的子集时，SA才能成功建立。因此，建议IPSec隧道两端配置的ACL规则互为镜像，即一端配置的ACL规则的源地址和目的地址分别为另一端配置的ACL规则的目的地址和源地址。具体来说：

  若两端都配置ISAKMP方式IPSec安全策略，ACL规则必须互为镜像。若一端配置ISAKMP方式IPSec安全策略，另一端配置策略模板方式IPSec安全策略，ISAKMP方式IPSec安全策略的ACL规则的范围可以小于策略模板方式IPSec安全策略的ACL规则，取双方ACL规则交集作为协商结果。
- ACL中各条rule的地址段要避免出现重叠。因为地址段重叠的rule之间容易相互影响，造成数据流匹配rule规则时出现误匹配的情况。
- 同一个IPSec安全策略组中配置的ACL不能包含相同的rule规则。
- 同一个IPSec安全策略组中所有IPSec安全策略引用的ACL的rule之间不能存在交集。例如引用的ACL3001和ACL3002存在交集：

  ```
  acl number 3001
   rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
  acl number 3002
   rule 5 permit ip source 10.1.0.0 0.0.255.255 destination 10.1.0.0 0.0.255.255
  ```
- 协商响应方采用策略模板方式IPSec安全策略时：

  响应方可不定义需要保护的数据流，此时表示接受发起方定义的需要保护的数据流范围；如果响应方要指定需要保护的数据流，则需要与发起方镜像配置或者包含发起方指定的保护的数据流范围。
- 如果应用IPSec安全策略的接口同时配置了NAT，由于设备先执行NAT，会导致IPSec不生效，此时需要：
  - NAT引用的ACL规则deny目的IP地址是IPSec引用的ACL规则中的目的IP地址，避免对IPSec保护的数据流进行NAT转换。
  - IPSec引用的ACL规则匹配经过NAT转换后的IP地址。

步骤2 检查两端IPSec proposal配置是否一致。

执行命令**display ipsec proposal**查看安全协议、加密算法、认证算法和封装模式，请确保两端的配置一致。

```
<Huawei> display ipsec proposal
Number of proposals: 1

IPSec proposal name: p1
 Encapsulation mode: Tunnel                        //封装模式
 Transform         : ah-esp-new                   //安全协议
 AH protocol       : Authentication SHA2-HMAC-256   //AH协议的认证算法
 ESP protocol      : Authentication SHA2-HMAC-256   //ESP协议的认证算法
                     Encryption AES-256             //ESP协议的加密算法
```

步骤3 检查IPsec隧道两端的安全策略配置是否一致。

执行命令**display ipsec policy brief**查看**Mode**字段，请确保两端的协商模式必须保持一致。

如果两端配置不一致，请执行命令**ipsec policy isakmp**修改配置，确保两端的配置一致。

```
<Huawei> display ipsec policy brief
Number of policies group : 1
Number of policies       : 1

Policy name          Mode     ACL        Peer name   Local address    Remote address
------------------------------------------------------------------------------------
policy1-100          isakmp   3002/IPv4   peer1
```

执行命令**display ipsec policy**查看PFS算法，如果本端指定了PFS，对端在发起协商时必须是PFS交换，即本端和对端指定的Diffie-Hellman组必须一致，否则协商会失败。

如果两端配置不一致，请执行命令**pfs**修改配置，确保两端的配置一致。

```
<Huawei> display ipsec policy
=========================================
IPSec policy group: "10"
Using interface: GigabitEthernet1/0/0
=========================================
    Sequence number: 10
    Policy Alias: map1-10
    Security data flow: 3100/IPv4
    Peer name    : rut2
    Perfect forward secrecy: DH group 14   //PFS算法
```

步骤4 若以上方法均没有定位出问题所在，请收集以下信息，并联系技术支持人员。

1. 收集配置信息、上述步骤的操作结果，并记录到文件中。
2. 执行命令**debugging**收集IPSec隧道建立过程中的信息。

   ```
   <Huawei> terminal monitor
   <Huawei> terminal debugging
   <Huawei> debugging ikev1 all   //采用IKEv1协商时收集的debugging信息
   <Huawei> debugging ikev2 all   //采用IKEv2协商时收集的debugging信息
   <Huawei> debugging ipsec all
   <Huawei> debugging adp-ipsec   //V200R007及之前版本，执行此命令收集debugging信息
   ```

3. 关闭**debugging**后，一键式收集设备的所有诊断信息并导出文件。
   a. 执行命令**display diagnostic-information** *file-name*采集设备诊断信息并保存为文件。

      ```
      <Huawei> display diagnostic-information dia-info.txt
      Now saving the diagnostic information to the device
       100%
      Info: The diagnostic information was saved to the device successfully
      ```

   b. 当诊断信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。

      您可以在用户视图下执行**dir**命令，确认文件是否正确生成。
4. 收集设备的日志和告警信息并导出文件。
   a. 执行**save logfile**命令，将缓冲区的日志和告警信息保存为文件。

      ```
      <Huawei> save logfile all
      Info: Save logfile successfully.
      Info: Save diagnostic logfile successfully.
      ```

   b. 当日志和告警信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。
5. 收集接口的报文信息，通过TFTP等方式将其从设备上导出。

   ```
   <Huawei> system-view
   [Huawei] acl 3100
   [Huawei-acl-adv-3100] acl 3100   //定义数据流
   [Huawei-acl-adv-3100] rule 5 permit ip source 10.1.1.1 0 destination 10.2.1.1 0
   [Huawei-acl-adv-3100] rule 5 permit ip source 10.2.1.1 0 destination 10.1.1.1 0
   [Huawei-acl-adv-3100] quit
   [Huawei] packet-capture ipv4-packet 3100 interface GigabitEthernet 1/0/1
   [Huawei] packet-capture startup packet-num 1500   //开启获取报文头信息功能
   [Huawei] packet-capture queue 0 to-file 1.cap   //将获取的报文头信息保存到设备上
   ```


获取报文头后，请删除其相关配置。

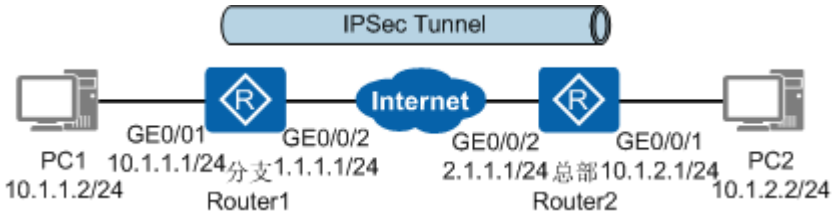
----结束

3.5 设备异常重启后仅单方向发起 IKE 重协商成功

3.5.1 现象描述

如图3-5所示，Router1和Router2之间IPSec隧道建立成功，Router2异常重启后，PC1 Ping不通PC2。

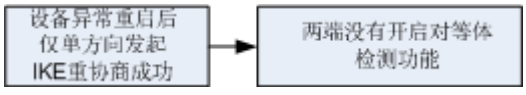
图 3-5 IPSec 组网图



执行命令**display ike sa**，发现Router1的SA建立成功，Router2的SA建立失败。

```
<Router1> display ike sa
IKE SA information :
  Conn-ID    Peer          VPN           Flag(s)            Phase
 ------------------------------------------------------------------------
   8388     2.1.1.1:500                 RD|ST|A            v2:2
   8378     2.1.1.1:500                 RD|ST|A            v2:1

  Number of IKE SA : 2
 ------------------------------------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
<Router2> display ike sa
```

3.5.2 可能原因



流量触发SA协商时，设备异常重启后，经常出现此现象。对于自动触发SA协商，设备异常重启后会自动触发IPSec SA的协商，无需处理。

3.5.3 定位步骤

操作步骤

步骤1 在Router1上手动复位SA。

执行命令**reset ike sa**后，两端IPSec隧道建立成功。

步骤2 两端配置IKE对等体DPD检测功能。

配置后，IPSec隧道断掉后会自动清除SA，并重新触发SA协商。

DPD检测需要在IKE对等体下配置。

两端对等体配置的DPD报文中的载荷顺序需要一致，否则对等体存活检测功能无效。

例如，在IKE对等体huawei下配置DPD报文中的载荷顺序为seq-hash-notify、检测模式为periodic、DPD空闲时间20秒、DPD报文重传间隔10秒、重传次数4次。以Router1为例。

```
<Router1> system-view
[Router1] ike peer huawei
[Router1-ike-peer-huawei] dpd msg seq-hash-notify
[Router1-ike-peer-huawei] dpd type periodic
[Router1-ike-peer-huawei] dpd idle-time 20
[Router1-ike-peer-huawei] dpd retransmit-interval 10
[Router1-ike-peer-huawei] dpd retry-limit 4
```

----结束

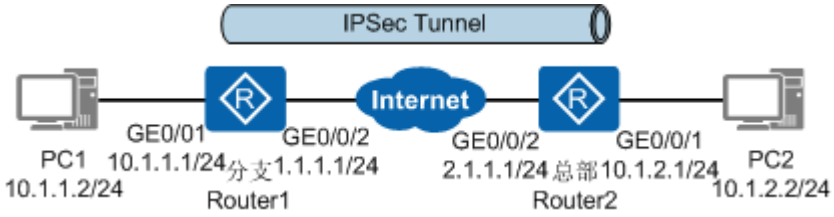
3.6 IPSec 隧道建立成功后业务不通

3.6.1 现象描述

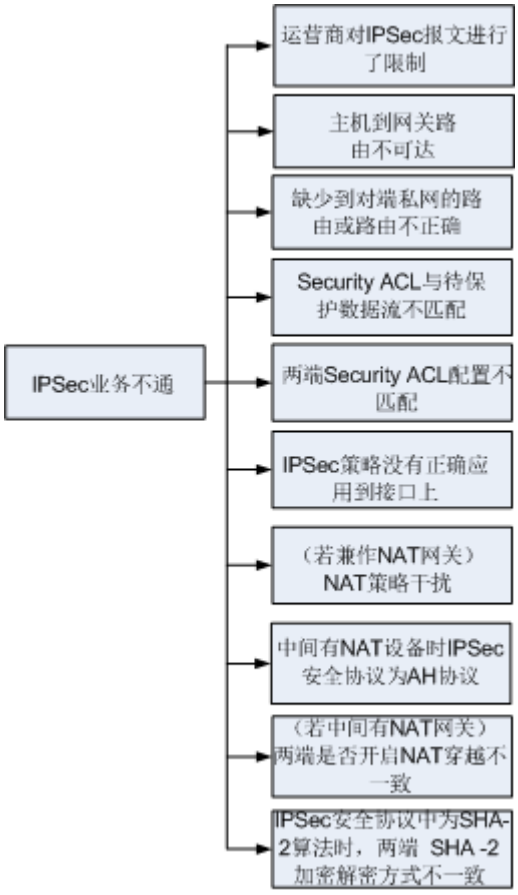
如图3-6所示，在Router1和Router2上执行命令**display ipsec sa**查看到IPSec SA的信息，说明IPSec隧道已建立成功，但存在如下问题：

- 分支和总部两端的用户完全不能互相访问。
- 分支和总部两端的用户单向访问正常，反向不通。例如，总部用户可以访问分支服务器，分支用户不能访问总部服务器。
- 分支和总部两端的用户访问部分网段正常，部分不通。
- 在点到多点网络中还可能存在分支用户访问总部正常，但不同分支用户之间访问不通。
- 在IPSec网关兼做NAT网关的场景中还可能出现所有流量都经NAT转换发送出去，没有流量进入VPN的问题。

图 3-6 IPSec 组网图



3.6.2 可能原因



3.6.3 定位步骤

操作步骤

步骤1 检查运营商网络是否对IPSec报文进行了限制。

通过Debugging、获取报文头或tracert命令等查看是否有AH报文或ESP报文丢包的情况，可以确认运营商网络是否对IPSec报文进行了限制。若运营商网络没有问题请继续执行下面的步骤。

步骤2 检查PC到网关、IPSec对等体到被保护的私网的路由是否可达。

执行命令**ping**检查路由是否可达。如果Ping不通，请执行命令**display interface**和**display ip routing-table**确保接口Up和路由配置正确。

多出口的场景下，还需执行命令**display current-configuration configuration policy-pbr**检查报文否有命中了策略路由，而没有进入IPSec隧道。

步骤3 检查Security ACL配置是否正确。

执行命令**display ipsec sa**查看Security ACL协商出的被保护的数据流，其源和目的网段是否包含真实的业务流。如果协商出的被保护的数据流没有包含真实的业务网段，请执行命令**display acl** *acl-number*检查两端的ACL配置是否正确。

```
<Huawei> display ipsec sa
==============================
```

```
Interface: GigabitEthernet1/0/0
==============================

 ----------------------------
 IPSec policy name: "map1"
 Sequence number  : 1
 Acl group        : 3100
 Acl rule         : 5
 Mode             : ISAKMP
 ----------------------------
   Connection ID     : 83893872
   Encapsulation mode: Tunnel
   Holding time      : 0d 0h 32m 4s
   Tunnel local      : 1.1.3.1:500
   Tunnel remote     : 1.1.5.1:500
   Flow source       : 10.1.0.0/255.255.0.0 0/0
   Flow destination  : 10.2.0.0/255.255.0.0 0/0
......
<Huawei> display acl 3100
Advanced ACL 3100, 1 rule ( Reference counter 1 )
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.0.0.255 (0 times matched)
```

步骤4 检查IPSec安全策略是否正确应用到IPSec隧道接口上。

执行命令**display ipsec policy**检查IPSec策略是否在接口应用，应用的接口是否正确。

```
<Huawei> display ipsec policy
==========================================
IPSec policy group: "10"
Using interface: GigabitEthernet1/0/0   //应用IPSec策略的接口
==========================================
......
```

步骤5 检查是否有NAT策略干扰IPSec保护数据流。

转发流程中IPSec模块位于NAT模块（NAT Server、目的NAT和源NAT）之后，故应确保NAT Server和目的NAT不影响IPSec对保护的数据流的处理。

执行命令**display ipsec interface brief**查看应用了IPSec策略的接口，然后执行命令**display current-configuration interface** *interface-type interface-number*查看IPSec接口是否配置了NAT策略。

如果应用IPSec安全策略的接口同时配置了NAT，由于设备先执行NAT，会导致IPSec不生效，此时需要：

- NAT引用的ACL规则deny目的IP地址是IPSec引用的ACL规则中的目的IP地址，避免对IPSec保护的数据流进行NAT转换。
- IPSec引用的ACL规则匹配经过NAT转换后的IP地址。

步骤6 如果中间有NAT设备，检查两端是否都开启了NAT穿越。

执行命令**display ike peer**查看两端是否开启了NAT穿越，如果未开启，则在IKE对等体视图下执行命令**nat traversal**。

```
<Huawei> display ike peer
Number of IKE peers: 1
------------------------------------------
  Peer name                  : 1
  IKE version                : v1v2
  VPN instance               :
  Remote IP                  : 1.1.1.1(www.huawei.com)
  Authentic IP address       :
  Proposal                   : 1
  Pre-shared-key             : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type              : IP
  Local ID                   :
```

```
  Remote ID type              : any
  Remote ID                   :
......
  NAT-traversal               : Enable   //NAT穿越
......
```

步骤7 检查中间有NAT设备，NAT穿越时安全协议是否为AH协议。

执行命令**display ipsec proposal**查看安全协议。

NAT穿越时安全协议只支持为ESP协议。

如果安全协议为AH协议，则执行命令**transform**修改安全协议为ESP协议。

```
<Huawei> display ipsec proposal
Number of proposals: 1

IPSec proposal name: p1
 Encapsulation mode: Tunnel
 Transform        : esp-new                  //安全协议
 ESP protocol     : Authentication SHA2-HMAC-256
                    Encryption AES-256
[Huawei] ipsec proposal p1
[Huawei-ipsec-proposal-p1] transform esp
```

步骤8 如果IPSec安全协议的认证算法为SHA2算法，检查两端的加解密方式是否一致。

执行命令**display ipsec proposal**查看认证算法是否为SHA2-256、SHA2-384或SHA2-512。

```
<Huawei> display ipsec proposal
Number of proposals: 1

IPSec proposal name: p1
 Encapsulation mode: Tunnel
 Transform        : esp-new
 ESP protocol     : Authentication SHA2-HMAC-256   //认证算法
                    Encryption AES-256
```

认证算法为SHA2-256、SHA2-384或SHA2-512，执行命令**display ipsec statistics**检查收到的加密报文是否被丢弃。如果有收到的加密报文被丢弃，且原因为认证失败，则在系统视图下执行命令**ipsec authentication sha2 compatible enable**或**undo ipsec authentication sha2 compatible enable**使得两端的加密解密方式一致。

IPSec安全协议中使用SHA2算法时，如果IPSec隧道两端设备的厂商不同或两端产品的版本不同，由于不同厂商或者不同产品之间加密解密的方式可能不同，会导致IPSec流量不通。

此时在系统视图下执行命令**ipsec authentication sha2 compatible enable**，开启SHA-2算法兼容功能，使得两端的加密解密方式一致。

```
[Huawei] ipsec authentication sha2 compatible enable
```

步骤9 若以上方法均没有定位出问题所在，请收集以下信息，并联系技术支持人员。

1. 收集配置信息、上述步骤的操作结果，并记录到文件中。
2. 执行命令**debugging**收集IPSec隧道建立过程中的信息。

   ```
   <Huawei> terminal monitor
   <Huawei> terminal debugging
   <Huawei> debugging ikev1 all   //采用IKEv1协商时收集的debugging信息
   <Huawei> debugging ikev2 all   //采用IKEv2协商时收集的debugging信息
   <Huawei> debugging ipsec all
   <Huawei> debugging adp-ipsec   //V200R007及之前版本，执行此命令收集debugging信息
   ```

3. 关闭**debugging**后，一键式收集设备的所有诊断信息并导出文件。

a. 执行命令**display diagnostic-information** *file-name*采集设备诊断信息并保存为文件。

```
<Huawei> display diagnostic-information dia-info.txt
Now saving the diagnostic information to the device
 100%
Info: The diagnostic information was saved to the device successfully
```

b. 当诊断信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。

您可以在用户视图下执行**dir**命令，确认文件是否正确生成。

4. 收集设备的日志和告警信息并导出文件。

a. 执行**save logfile**命令，将缓冲区的日志和告警信息保存为文件。

```
<Huawei> save logfile all
Info: Save logfile successfully.
Info: Save diagnostic logfile successfully.
```

b. 当日志和告警信息文件生成之后，您可以通过TFTP等方式将其从设备上导出。

5. 收集接口的报文信息，通过TFTP等方式将其从设备上导出。

```
<Huawei> system-view
[Huawei] acl 3100
[Huawei-acl-adv-3100] acl 3100   //定义数据流
[Huawei-acl-adv-3100] rule 5 permit ip source 10.1.1.1 0 destination 10.2.1.1 0
[Huawei-acl-adv-3100] rule 5 permit ip source 10.2.1.1 0 destination 10.1.1.1 0
[Huawei-acl-adv-3100] quit
[Huawei] packet-capture ipv4-packet 3100 interface GigabitEthernet 1/0/1
[Huawei] packet-capture startup packet-num 1500   //开启获取报文头信息功能
[Huawei] packet-capture queue 0 to-file 1.cap   //将获取的报文头信息保存到设备上
```

获取报文头后，请删除其相关配置。

----结束

参考信息

案例：

4.1.2 AR路由器由于IPSec参数不一致导致IPSec隧道建立失败

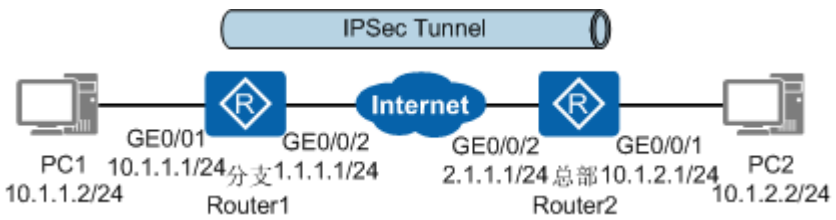
3.7 IPSec 隧道建立成功后业务质量差

3.7.1 现象描述

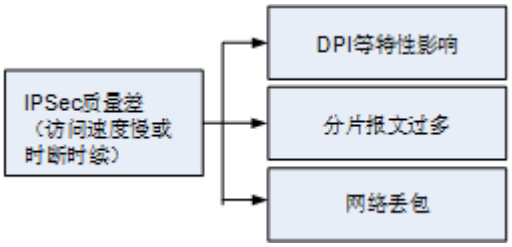
如图3-7所示，在Router1和Router2上执行命令**display ipsec sa**查看到IPSec SA的信息，说明IPSec隧道已建立成功。但存在如下问题：

- 业务访问速度慢。
- 业务访问时断时续，也可能彻底中断。

图 3-7 IPSec 组网图



3.7.2 可能原因



3.7.3 定位步骤

操作步骤

步骤1 检查CPU占用率是否过高。

执行命令**display cpu-usage**查看CPU的占用率。

当CPU占用率超过80%时，可以检查是否配置了攻击防范等特性。若配置了可以先关闭，然后再检查CPU占用率。

步骤2 检查业务经过的公网是否有丢包。

在IPSec隧道两端的接口分别执行命令**undo ipsec policy**取消应用IPSec策略，然后进行Ping测试，若有丢包说明公网质量有问题，请运营商协助解决。

步骤3 检查IPSec报文是否被分片。

IPSec对IP报文进行再次封装导致IP报文长度变长，IP报文在传送过程中超过链路MTU时将被分片发送，接收端需重组后再解析。分片和重组都需要消耗CPU资源，同时分片报文的加密、解密过程也需要消耗更多的CPU资源。当分片报文比例过大时，CPU资源告急可能会导致访问速度下降、报文丢包。

执行命令**ping -s** *packetsize* **-a** *source-ip-address host*测试不同大小的报文，确定是否有丢包或Ping不通，找到一个临界值（大于临界值时，Ping有丢包或不通现象）。

根据该临界值，在接口视图下执行命令**mtu** *mtu*修改MTU值。

修改后，还是出现部分TCP业务访问速度慢或访问时断时续现象时，请在接口视图下执行命令**tcp adjust-mss** *value*修改TCP最大报文段长度。

TCP MSS指定了TCP最大报文段长度，如果MSS值加上各种开销的报文总长度（MSS+TCP报文头+IP报文头+IPSec报文头）大于链路的MTU值，则数据报文会被分片发送。分片的过程会消耗更多的CPU资源，分片报文的加密解密同样会消耗传输链路中设备的CPU资源。当CPU资源消耗过多，就会造成数据报文的丢失。

同时，对于某些上层应用（例如HTTP等应用层协议等）会将IP报文的DF(Don't Fragment)标记位置为有效，以防止TCP报文分片。如果DF标记位被置为有效，而接口MTU小于MSS的值，此时设备会因为不能强制分片TCP报文而将报文丢弃。

----结束

任务示例

质量差分析：

案例：

4 故障案例

4.1 IPSec 隧道建立失败导致业务不通

4.1.1 AR 路由器 NAT 穿越场景中由于未配置认证地址导致 IPSec 隧道建立失败

关键字

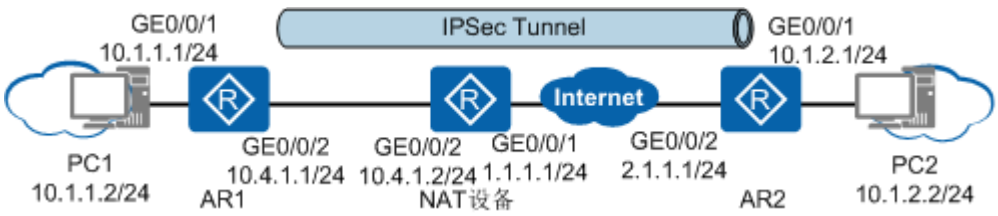
NAT穿越，认证地址，IKEv2协商失败，IPSec隧道建立失败，业务不通

摘要

中间有NAT设备，两端采用IKEv2方式IPSec安全策略时，未配置认证地址，导致IPSec隧道建立失败。

问题描述

如图所示，AR1和AR2分别作为分支和总部的网关，AR1穿越NAT设备与AR2互联，部署IKEv2方式IPSec安全策略后，IPSec隧道建立失败，PC间无法互相访问，业务不通。



执行命令**display ike sa**，发现IKE SA协商失败。


```
<AR2> display ike sa
IKE SA information :
  Conn-ID    Peer          VPN            Flag(s)     Phase
-------------------------------------------------------------------
 1342       1.1.1.1                     NEG|A       v2:1

 Number of IKE SA : 1
-------------------------------------------------------------------

 Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

处理过程

1. 执行命令**display ike error-info**，查看IKE协商失败原因。

   ```
   <AR2> display ike error-info
    current info Num :2
    Ike error information:
    current ike Error-info number :2
   ------------------------------------------------------------------
    peer    port error-reason            version error-time
   ------------------------------------------------------------------
    1.1.1.1 500  authentication fail      v2     2017-09-05 15:22:32
    1.1.1.1 500  config ID mismatch       v2     2017-09-05 15:22:32
   ------------------------------------------------------------------
   ```

   从显示信息可以看出，IKE协商失败原因为**authentication fail**和**config ID mismatch**，说明AR2根据ID未找到匹配的IKE Peer，请检查remote-address是否正确。

2. 执行命令**display ike peer**，检查remote-address是否正确。

   ```
   <AR2> display ike peer
   Number of IKE peers: 1

   ----------------------------------------------
     Peer name                  : spua
     IKE version                : v1v2
     VPN instance               :
     Remote IP                  : 1.1.1.1
     Authentic IP address       :
     Proposal                   : 5
     Pre-shared-key             : %^%#w.]D%IU@fYUn2H->a2iJe$W02.Z%G/L_O+JQvc0<%^
   %#
     Local ID type              : IP
     Local ID                   :
     Remote ID type             :
     Remote ID                  :
     certificate peer-name      :
     PKI realm                  : NULL
     Inband OCSP                : Disable
     Inband CRL                 : Disable
     cert-request empty-payload : Disable
     VPN instance bound to the SA :
     NAT-traversal              : Enable
     AAA authorization domain   :
     DSCP                       :
     Lifetime-notification-message: Disable
     DPD                        : Disable
     RSA encryption-padding     : PKCS1
     RSA signature-padding      : PKCS1
     ipsec sm4 version          : draft-standard
     Certificate-check          : Enable
   ----------------------------------------------
   ```

   从显示信息可以看出，**Remote IP**为1.1.1.1，配置正确，因为NAT穿越场景中，AR2配置的remote-address为NAT转换后的IP地址。但是认证又失败，是因为AR1发送过来的IKE报文中的本端IP地址为10.4.1.1，与AR2配置的IP地址1.1.1.1不匹

配，需执行命令**remote-address authentication-address**指定认证的IP地址为10.4.1.1。

3. 执行命令**remote-address authentication-address**，配置认证的IP地址为10.4.1.1。

```
<AR2> system-view
[AR2] ike peer spua
[AR2-ike-peer-spua] remote-address authentication-address 10.4.1.1
```

配置后，IPSec隧道建立成功，PC间可以相互Ping通，说明两端业务可以互通。

根因

IPSec NAT穿越场景中，AR1发送过来的IKE报文中的本端IP地址为10.4.1.1，与AR2配置的IP地址1.1.1.1不匹配。

解决方案

执行命令**remote-address authentication-address**，配置认证的IP地址为10.4.1.1。

建议与总结

IKEv2场景中，当对端设备使用的是内网IP地址，穿越了NAT设备时，如果需要使用IP地址进行认证，可以通过配置**authentication-address**参数指定NAT转换前的IP地址为对端认证地址。此时需要将NAT转换后的IP地址作为对端地址。

IPSec NAT穿越场景中，建议IKE协商时不使用IP地址进行认证或者AR2采用策略模板方式IPSec安全策略。

4.1.2 AR 路由器由于 IPSec 参数不一致导致 IPSec 隧道建立失败

关键字

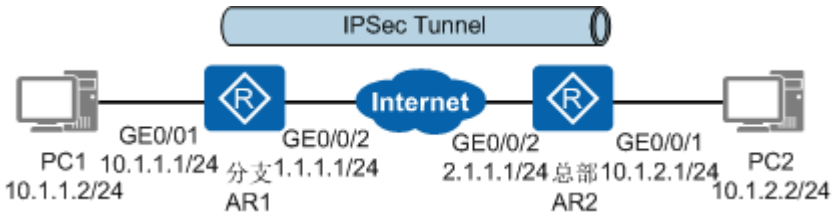
IPSec参数，IPSec隧道建立失败，业务不通

摘要

由于IPSec参数不一致，导致两端建立IPSec隧道失败，业务不通。

问题描述

如图所示，AR1与其他厂商设备AR2之间部署IPSec，AR1作为分支网关，AR2作为总部网关。IPSec隧道建立失败，PC1不能与PC2互访，业务不通。



执行命令**display ike sa**，发现IKE SA协商失败。

```
<AR1> display ike sa
IKE SA information :
  Conn-ID    Peer          VPN           Flag(s)     Phase
```



```
------------------------------------------------------------------
 1342      0.0.0.0                       RD|A        v1:1

Number of IKE SA : 0
------------------------------------------------------------------

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

处理过程

1. 执行命令**display ike error-info**，查看IKE协商失败原因。

```
<AR1> display ike error-info
  current info Num :2
  Ike error information:
  current ike Error-info number :2
------------------------------------------------------------------
 peer    port error-reason            version error-time
------------------------------------------------------------------
 2.1.1.1 500  phase1 proposal mismatch  v1     2017-09-05 15:22:32
 2.1.1.1 500  phase1 proposal mismatch  v1     2017-09-05 15:22:32
------------------------------------------------------------------
```

从显示信息可以看出，IKE协商失败原因为**phase1 proposal mismatch**，说明两端IKE安全提议参数不一致。

2. 查看两端设备的IKE安全提议参数。

对于AR1，执行命令**display ike proposal** [**number** *proposal-number*]，查看两端的IKE安全提议参数。

```
<AR1> display ike proposal number 10
-------------------------------------------
 IKE Proposal: 10
   Authentication Method      : PRE_SHARED
   Authentication Algorithm   : SHA2-256
   Encryption Algorithm       : AES-128
   Diffie-Hellman Group       : MODP-2048
   SA Duration(Seconds)       : 86400
   Integrity Algorithm        : HMAC-SHA2-256
   Prf Algorithm              : HMAC-SHA2-256
-------------------------------------------
```

对于AR2，请联系服务提供商提供其他厂商的IKE安全提议参数，如果无法提供，则在用户视图下执行命令**debugging ikev1 all**查看其他厂商设备发送过来的IKE安全提议信息。

```
Sep 14 2017 11:14:11.630.17 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute ENCRYPTION_ALGORITHM value AES_CBC
Sep 14 2017 11:14:11.630.18 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute KEY_LENGTH value 256
Sep 14 2017 11:14:11.630.19 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute HASH_ALGORITHM value SHA2-256
Sep 14 2017 11:14:11.630.20 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute AUTHENTICATION_METHOD value PRE_SHARED
Sep 14 2017 11:14:11.640.1 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute GROUP_DESCRIPTION value MODP_2048
Sep 14 2017 11:14:11.640.2 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute LIFE_TYPE value SECONDS
Sep 14 2017 11:14:11.640.3 AR1 IKE/7/IKE_Debug:
IKE_INFO 2:2969   Attribute LIFE_DURATION value 86400
```

从两个信息可以看出，两端的加密算法不一致，AR1和AR2的加密算法分别为AES-128、AES-256。

3. 更改IKE安全提议中不一致的参数。

由于两端**Encryption Algorithm**不一致，所以在AR1上修改加密算法。

```
ike proposal 10
 encryption-algorithm aes-256
```

修改后，IPSec隧道建立成功，PC间可以相互Ping通，说明两端业务可以互通。

根因

两端IKE安全提议中的加密算法不一致。

解决方案

在AR1上执行命令**encryption-algorithm aes-256**修改加密算法。

建议与总结

配置IPSec时，务必保证两端IPSec参数一致，特别是与其他厂商设备对接时，有些缺省参数不一样，使用默认的参数时，就会导致IKE SA协商失败。当无法获取友商设备的配置信息时，可以在本端设备执行命令**debugging ikev1 all**或**debugging ikev2 all**查看其他厂商设备发送过来的IPSec参数。

4.1.3 AR 路由器由于待保护数据流匹配了 NAT Server 导致 IPSec 隧道建立后无法远程登录对端

关键字

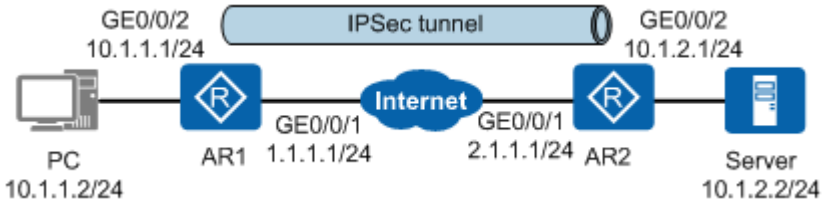
NAT Server，IPSec隧道建立，无法Telnet，远程登录

摘要

IPSec与NAT同时部署在一台设备上，由于待保护数据流匹配了NAT Server，导致两端建立IPSec隧道后，PC能Ping通Server，但PC无法远程登录对端。

问题描述

如图所示，AR1和AR2分别作为分支和总部的网关，并在AR1上部署NAT Server和源NAT策略。部署IPSec后，IPSec隧道建立成功，PC能Ping通Server，但是从PC Telnet Server的10.1.2.2 1054端口不成功。



PC能Ping通Server，但PC无法Telnet对端，检查IPSec配置、ACL、路由等配置，发现没有问题，PC无法Telnet对端可能原因为该数据流没有匹配Security ACL规则。

处理过程

1. 执行命令**display ipsec sa**和**display acl**，查看Telnet时数据流是否匹配上Security ACL规则。

```
<AR1> display ipsec sa
ipsec sa information:
```

```
==============================
Interface: GigabitEthernet0/0/2
==============================
 ----------------------------
  IPSec policy name: "pc2"
  Sequence number  : 1
  Acl group        : 3101
  Acl rule         : 5
  Mode             : Template
 ----------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 1.1.1.1:500
    Tunnel remote     : 2.1.1.1:500
    Flow source       : 10.1.1.0/255.255.255.0 17/1701
    Flow destination  : 10.1.2.0/255.255.255.0 17/39725

    [Outbound ESP SAs]
      SPI: 4055669516 (0xf1bc9b0c)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 1840323/2420
      Outpacket count       : 0
      Outpacket encap count : 0
      Outpacket drop count  : 0
      Max sent sequence-number: 0
      ......

<AR1> display acl 3101
Advanced ACL 3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 (0 matches)
```

从显示信息可以看出，IPSec已经建立成功，但PC Telnet Server时数据流没有匹配上Security ACL规则。因为AR1又兼做NAT网关，其数据流可能匹配了NAT策略。

2. 执行命令**display nat outbound**和**display acl**，检查NAT策略是否包含待保护数据流。

```
<AR1> display  nat outbound
NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface           Acl Address-group/IP/Interface      Type
 ----------------------------------------------------------------------
 GigabitEthernet0/0/2 3300                   1.1.1.1     easyip
 ----------------------------------------------------------------------
  Total : 1

<AR1> display acl 3300
Advanced ACL 3300, 1 rule
Acl's step is 5
 rule 10 permit ip (4 matches)

<AR1> display acl 3300
Advanced ACL 3300, 1 rule
Acl's step is 5
  rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 10 permit ip
 (0 matches)
```

从显示信息可以看出，待保护数据流的已经在NAT策略中被Deny掉。

3. 执行命令**display nat server**，检查待保护数据流的源地址是否被NAT转换。

```
<AR1> display nat server
    Nat Server Information:
    Interface  : GigabitEthernet0/0/2
    Global IP/Port     : current-interface/8080 (Real IP : 1.1.1.1)
    Inside IP/Port     : 10.1.1.2/8080
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
```



```
  Vrrp id          : ----
  Description : ----

 Total :   1
```

从显示信息可以看出，因为报文源地址匹配NAT Server，所以Telnet时数据流被NAT转换。因此，建议将NAT Server改为静态NAT，只有报文的源地址+端口号匹配时被NAT转换。

4. 执行命令**nat static**，配置静态NAT静态映射关系。

```
<AR1> system-view
[AR1] interface gigabitethernet 0/0/2
[AR1-GigabitEthernet0/0/2] nat static protocol tcp global current-interface 8080 inside 10.1.1.2 8080
```

修改后，从PC Telnet Server的10.1.2.2 1054端口成功。

根因

PC Telnet Server时数据流匹配了NAT Server，源地址被NAT转换。

解决方案

将NAT Server改为静态NAT，只有报文的源地址+端口号匹配时被NAT转换

建议与总结

当IPSec与NAT配置在同一台设备时，要确认经过IPSec封装的数据流是否还需要进行NAT转换。

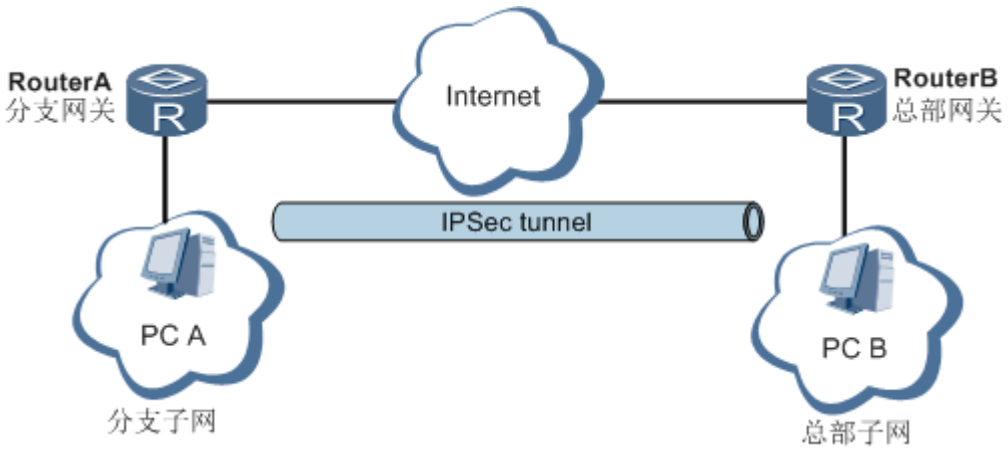
- 如果需要进行NAT转换，则Security ACL要匹配NAT后的地址。
- 如果不需要进行NAT转换，则Security ACL要匹配NAT前的地址。且经过IPSec隧道的数据流不进行NAT转换。

4.2 IPSec 隧道建立成功后业务不通

4.2.1 AR 配置 IPSec 功能后，流量不通

介绍AR 配置IPSec功能后，流量不通的典型案例。

组网情况



RouterA重要配置：

```
#
acl number 3000
 rule 10 permit ip source 192.168.10.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
 rule 20 permit ip source 192.168.20.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
 rule 30 permit ip source 192.168.202.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
 rule 40 permit ip source 192.168.201.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
 rule 50 deny ip
#
ipsec proposal 2
#
ike proposal 2
#
ike peer aaa v1
 pre-shared-key huawei
#
ipsec policy-template hrui 10
 security acl 3000
 ike-peer aaa
 proposal 2
#
ipsec policy huir 10 isakmp template hrui
#
```

现象描述

1. 客户反馈IPSec隧道建立成功后，无法访问公网（该部分流量不需要进行IPSec加密），把IPSec策略从接口上去绑定后，可以正常上网；
2. 客户配置4条ACL规则，但是只有一条ACL流量可以通。

原因分析

1. IPSec的选流ACL中配置了deny规则，而RouterA当前使用的版本(V200R001C01SPC500)不支持deny，默认会将命中deny规则的流量丢弃。修改配置后问题解决(删除deny rule)。

   目前V200R002相关版本会将ACL中deny的报文不做IPSec封装，不会丢弃该报文。
2. 版本间差异，本问题中一端使用V200R001版本，另一端使用V2R2版本。R1版本是基于ACL Number协商SA，R2版本是基于rule协商SA，所以R1版本设备上协商出1个SA，V200R002设备上协商出4个SA，这样导致只有一条ACL流量可以通。升级到相同的R2版本后，问题解决。

操作步骤

1. 将两端设备的版本升级到V200R002及之后版本。

总结与建议

部分特性不同版本间是有一些差异的，建议对接时候采用相同的版本，避免不必要的问题发生。

4.2.2 AR 路由器由于 Security ACL 与 NAT 策略冲突导致建立 IPSec 隧道后业务不通

关键字

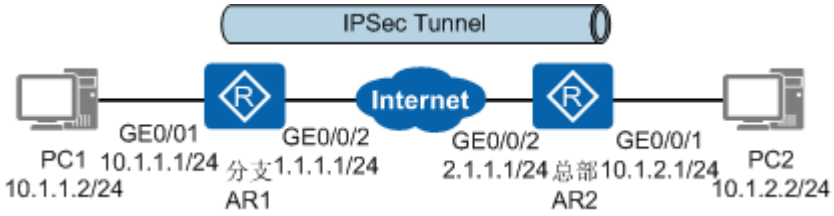
NAT，IPSec隧道建立，业务不通

摘要

IPSec与NAT同时部署在一台设备上，由于Security ACL与NAT策略冲突，导致两端建立IPSec隧道后业务不通。

问题描述

如图所示，AR1和AR2分别作为分支和总部的网关，AR1同时也作为NAT网关，部署IPSec后，IPSec隧道建立成功，但PC间无法互相访问，业务不通。



处理过程

1. 执行命令**display ipsec sa**，查看IPSec隧道信息。

```
<AR1> display ipsec sa
ipsec sa information:
===============================
Interface: GigabitEthernet0/0/2
===============================
 ------------------------------
 IPSec policy name: "pc2"
 Sequence number  : 1
 Acl group        : 3101
 Acl rule         : 5
 Mode             : Template
 ------------------------------
   Connection ID     : 67108879
   Encapsulation mode: Tunnel
   Holding time      : 0d 0h 4m 29s
   Tunnel local      : 1.1.1.1:500
   Tunnel remote     : 2.1.1.1:500
   Flow source       : 10.1.1.0/255.255.255.0 17/1701
   Flow destination  : 10.1.2.0/255.255.255.0 17/39725

   [Outbound ESP SAs]
     SPI: 4055669516 (0xf1bc9b0c)
     Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
     SA remaining key duration (kilobytes/sec): 1840323/2420
     Outpacket count      : 0
     Outpacket encap count : 0
     Outpacket drop count  : 0
     Max sent sequence-number: 0
     ......
```

从显示信息可以看出，IPSec已经建立成功，但PC1 Ping PC2时没有发出加密报文。

执行命令**display acl**，确认Security ACL配置与待保护数据流是否匹配。

```
<AR1> display acl 3101
Advanced ACL 3101, 1 rule
Acl's step is 5
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 (0 matches)
```

检查发现Security ACL配置与待保护数据流匹配，但待保护数据流没有进入IPSec隧道。因为AR1又兼做NAT网关，待保护数据流可能匹配了NAT策略。

2. 执行命令**display nat outbound**和**display acl**，检查NAT策略是否包含待保护数据流。


```
<AR1> display  nat outbound
NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface           Acl     Address-group/IP/Interface  Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/2 3300                   1.1.1.1     easyip
 --------------------------------------------------------------------------
  Total : 1

<AR1> display acl 3300
Advanced ACL 3300, 1 rule
Acl's step is 5
 rule 10 permit ip (4 matches)
```

从显示信息可以看出，NAT策略包含待保护数据流，并且匹配了待保护数据流。由于设备优先处理NAT流程，故在IPSec封装之前，PC访问对端的数据流会首先进行NAT转换。所以需经过IPSec封装的数据流不进行NAT转换。

3. 修改AR1的NAT ACL，使得待保护数据流不匹配NAT策略。

```
acl number 3300
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 10 permit ip
```

配置后，PC间可以相互Ping通，说明两端业务可以互通。

根因

NAT策略包含待保护数据流。由于设备优先处理NAT流程，故在IPSec封装之前，PC访问对端的数据流会首先进行NAT转换。

解决方案

修改AR1的NAT ACL，使得待保护数据流不匹配NAT策略。

建议与总结

当IPSec与NAT配置在同一台设备时，要确认经过IPSec封装的数据流是否还需要进行NAT转换。

- 如果需要进行NAT转换，则Security ACL要匹配NAT后的地址。
- 如果不需要进行NAT转换，则Security ACL要匹配NAT前的地址。且经过IPSec隧道的数据流不进行NAT转换。

4.2.3 AR 路由器由于 SHA2 算法加解密方式不一致导致建立 IPSec 隧道后业务不通

关键字

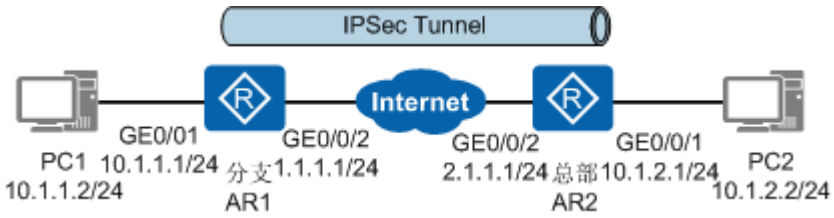
SHA2算法，IPSec隧道建立，业务不通

摘要

IPSec采用SHA2认证算法时，由于SHA2算法加解密方式不一致，导致两端建立IPSec隧道后业务不通。

问题描述

如图所示，AR1（华为路由器）作为分支网关，AR2（思科路由器）作为总部网关，两端建立IPSec隧道后，PC间无法互相访问，业务不通。



处理过程

1. 执行命令**display ipsec sa**，查看IPSec隧道信息。

```
<AR1> display ipsec sa
ipsec sa information:
===============================
Interface: GigabitEthernet0/0/2
===============================
 ----------------------------
  IPSec policy name: "pc2"
  Sequence number  : 1
  Acl group        : 3061
  Acl rule         : 5
  Mode             : Template
 ----------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 1.1.1.1:500
    Tunnel remote     : 2.1.1.1:500
    Flow source       : 10.1.1.0/255.255.255.0 17/1701
    Flow destination  : 10.1.2.0/255.255.255.0 17/39725

    [Outbound ESP SAs]
      SPI: 4055669516 (0xf1bc9b0c)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 1840323/2420
      Outpacket count      : 0
      Outpacket encap count : 0
      Outpacket drop count  : 0
      Max sent sequence-number: 0
      ......
    [Inbound ESP SAs]
      SPI: 1050491168 (0x3e9d3920)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 1840323/2420
      Inpacket count       : 33
      Inpacket decap count  : 0
      Inpacket drop count   : 33
      Max received sequence-number: 33
      ......
```

从显示信息可以看出，IPSec已经建立成功，但是AR1收到加密报文后解密失败而丢弃加密报文，没有发出加密报文。

2. 执行命令**display ipsec statistics**，查看IPSec报文统计信息。

```
<AR1> display ipsec statistics
 IPSec statistics information:
 Number of IPSec tunnels: 1
 the security packet statistics:
   input/output security packets: 33/0
   input/output security bytes: 0/0
   input/output dropped security packets: 33/0
```



```
......
dropped security packet detail:
  can not find SA: 0, wrong SA: 0
  authentication: 33, replay: 0
  front recheck: 0, after recheck: 0
  ......
```

从显示信息可以看出，加密报文丢弃的原因为认证失败。但又检查配置没有问题，其可能原因为IPSec采用SHA2认证算法。

说明

对于ARV200R008C00之前的软件版本，请执行命令**display ipsec statistics esp**，查看IPSec报文统计信息。

3. 执行命令**display ipsec proposal**查看安全提议的认证算法是否为SHA2。

```
<AR1> display ipsec proposal
Number of proposals: 1
IPSec proposal name: tran1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-512
                     Encryption AES-256
```

发现安全提议的认证算法为SHA2-512，因为华为路由器与思科路由器的SHA2算法的加解密方式不一致，所以两端解密报文失败导致报文被丢弃。

4. 执行命令**ipsec authentication sha2 compatible enable**，修改AR1的SHA2算法的加解密方式。

```
<AR1> system-view
[AR1] ipsec authentication sha2 compatible enable
```

修改后，PC1与PC2可以相互Ping通，说明两端业务可以互通。

根因

华为路由器与思科路由器的SHA2算法的加解密方式不一致，导致一端收到加密报文后解密失败而丢弃报文。

解决方案

在AR1的系统视图下执行命令**ipsec authentication sha2 compatible enable**。

建议与总结

配置安全提议的认证算法为SHA2时，务必保证加解密方式一致，特别是与友商设备对接时，加解密方式不一致，需执行命令**ipsec authentication sha2 compatible enable**。

4.2.4 AR 路由器由于两个 Security ACL 规则冲突导致 IPSec 隧道建立后业务不通

关键字

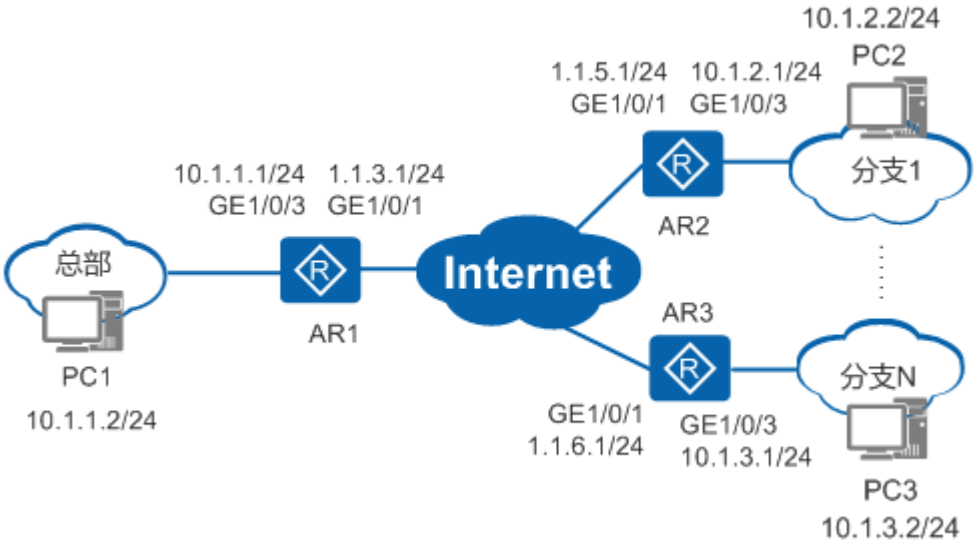
Security ACL，IPSec隧道建立，业务不通

摘要

总部与多个分支对接，由于两个Security ACL规则冲突，导致两端建立IPSec隧道后业务不通。

问题描述

如图所示，某企业使用多个分支和总部AR1进行IPSec对接。多个分支都是固定IP地址，大多数分支到总部都可以正常通信，并且分支之间可以互相通信，唯独其中一个分支（其网关为AR3）的内网PC和总部内网之间不能正常通信。



PC3可以与其他分支PC正常通信，唯独与总部PC不能正常通信，说明IPSec配置、链路都正常。其可能原因为Security ACL规则冲突。

处理过程

1. 执行命令**display ipsec sa**，查看Security ACL协商出的被保护的数据流是否有冲突。

```
<AR1> display ipsec sa
==============================
Interface: GigabitEthernet1/0/1
==============================

 ----------------------------
 IPSec policy name: "map1"
 Sequence number  : 1
 Acl group        : 3000
 Acl rule         : 5
 Mode             : ISAKMP
 ----------------------------
   Connection ID     : 83893872
   Encapsulation mode: Tunnel
   Holding time      : 0d 0h 32m 4s
   Tunnel local      : 1.1.3.1:500
   Tunnel remote     : 1.1.5.1:500
   Flow source       : 10.1.0.0/255.255.0.0 0/0
   Flow destination  : 10.1.0.0/255.255.0.0 0/0
   .....

 ----------------------------
 IPSec policy name: "map1"
 Sequence number  : 2
 Acl group        : 3001
 Acl rule         : 5
 Mode             : ISAKMP
 ----------------------------
   Connection ID     : 83893872
   Encapsulation mode: Tunnel
   Holding time      : 0d 0h 32m 4s
```



```
  Tunnel local      : 1.1.3.1:500
  Tunnel remote     : 1.1.6.1:500
  Flow source       : 10.1.0.0/255.255.0.0 0/0
  Flow destination  : 10.1.3.0/255.255.255.0 0/0
  .......
```

发现总部能够与分支正常通信的ACL数据流范围（ACL 3000的rule 5）包括了不能与分支正常通信的ACL里的数据流（ACL 3001的rule 5），造成Security ACL规则冲突。

2. 修改Security ACL规则。

   修改总部AR1的Security ACL规则。对于分支，这里不再赘述，其Security ACL规则与总部互为镜像即可。

```
acl number 3000
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255

acl number 3001
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
```

   修改后，PC3与PC1可以相互Ping通，说明两端业务可以互通。

根因

总部能够与分支正常通信的ACL数据流范围（ACL 3000的rule 5）包括了不能与分支正常通信的ACL里的数据流（ACL 3001的rule 5），造成Security ACL规则冲突。

解决方案

修改总部AR1的Security ACL规则，使得ACL中各条rule的地址段避免出现重叠。

建议与总结

对于多个分支与总部建立IPSec隧道，配置Security ACL规则时需注意：

- ACL中各条rule的地址段要避免出现重叠。因为地址段重叠的rule之间容易相互影响，造成数据流匹配rule规则时出现误匹配的情况。
- 同一个IPSec安全策略组中配置的ACL不能包含相同的rule规则。
- 同一个IPSec安全策略组中所有IPSec安全策略引用的ACL的rule之间不能存在交集。

4.2.5 AR 路由器由于报文不能分片导致 IPSec 隧道建立后视频业务不通

关键字

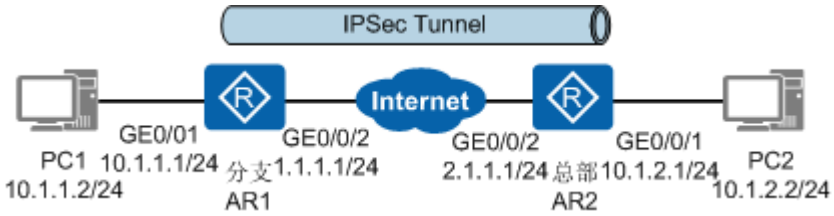
报文分片，TCP MSS，IPSec隧道建立，业务不通

摘要

由于报文不能分片，导致两端IPSec隧道建立后视频业务不通。

问题描述

如图所示，AR1与其他厂商设备AR2之间部署IPSec，AR1作为分支网关，AR2作为总部网关。IPSec隧道建立后，视频会议时总部可以呼通分支，但是分支不能呼通总部（显示对端拒绝）。



因为视频会议时分支不能呼通总部，所以检查ACL、路由配置是否正确，检查发现ACL、路由配置都正确。

处理过程

1. 执行命令**ping -s** *packetsize* **-a** *source-ip-address host*测试不同大小的报文，确定是否有丢包或Ping不通。

```
<AR1> ping -s 1418 -a 10.1.1.1 10.1.2.2
  PING 10.1.2.2: 1418  data bytes, press CTRL+C to break
    Reply from 10.1.2.2: bytes=1418 Sequence=1 ttl=126 time=67 ms
    Reply from 10.1.2.2: bytes=1418 Sequence=2 ttl=126 time=50 ms
    Reply from 10.1.2.2: bytes=1418 Sequence=3 ttl=126 time=50 ms
    Reply from 10.1.2.2: bytes=1418 Sequence=4 ttl=126 time=50 ms
    Reply from 10.1.2.2: bytes=1418 Sequence=5 ttl=126 time=50 ms

  --- 10.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/53/67 ms

<AR1> ping -s 1419 -a 10.1.1.1 10.1.2.2
  PING 10.1.2.2: 1419  data bytes, press CTRL+C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.1.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
100.00% packet loss
```

可以看出，IPSec在传输大包时，大于1418的报文不能正常传输，而不分片报文能够正常传输。因为大包经过IPSec封装后大于接口MTU值，导致IPSec报文被分片，而在网络中不能被正常传输。

2. 执行命令**display ipsec sa**，查看Ping大包时数据流是否进入IPSec隧道。

```
<AR1> display ipsec sa
ipsec sa information:
===============================
Interface: GigabitEthernet0/0/2
===============================
 ----------------------------
  IPSec policy name: "pc2"
  Sequence number  : 1
  Acl group        : 3101
  Acl rule         : 5
  Mode             : Template
 ----------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 1.1.1.1:500
    Tunnel remote     : 2.1.1.1:500
    Flow source       : 10.1.1.0/255.255.255.0 17/1701
    Flow destination  : 10.1.2.0/255.255.255.0 17/39725
```



```
  [Outbound ESP SAs]
    SPI: 4055669516 (0xf1bc9b0c)
    Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
    SA remaining key duration (kilobytes/sec): 1840323/2420
    Outpacket count      : 0
    Outpacket encap count : 0
    Outpacket drop count  : 0
    Max sent sequence-number: 0
    ......
```

从显示信息可以看出，Ping大包时数据流没有进入IPSec隧道，说明IPSec报文没有被发出。又因为Ping小包时数据流可以正常发出，所以初步怀疑IPSec报文被设置了不能分片，导致IPSec报文被丢弃。

3. 执行命令**display ipsec global config**，查看IPSec报文的DF标志位。

```
<AR1> display ipsec global config
IPSec Global Config:
-------------------------------------------------------------------
 IPSec sa global-duration time-based(seconds)   : 3600
 IPSec sa global-duration traffic-based(kbytes) : 1843200
 IPSec anti-replay                              : enable
 IPSec df-bit                                   : copy
 IPSec fragmentation                            : disable
 IPSec invalid-spi-recovery                     : disable
 IPSec nat-traversal source-port                : 8000
-------------------------------------------------------------------
```

从显示信息可以看出，IPSec报文的DF标志位为原始报文的标志位。初步怀疑原始报文的DF标志位为1，不允许对报文进行分片。

说明

IPSec df-bit：IPSec隧道的DF标志位。

- clear：指定DF标志位设置为0，表示允许对报文进行分片。
- set：指定DF标志位设置为1，表示不允许对报文进行分片。
- copy：指定DF标志位为原始报文的标志位。

IPSec fragmentation：IPSec隧道报文的分片方式。

- enable：IPSec加密前分片。
- disable：IPSec加密后分片。

4. 执行命令**ipsec df-bit clear**，设置DF标志位为0。

```
<AR1> system-view
[AR1] ipsec df-bit clear
```

修改后，Ping大包时，可以Ping通，说明视频会议时分支可以呼通总部。

```
<AR1> ping -s 1419 -a 10.1.1.1 10.1.2.2
 PING 10.1.2.2: 1419  data bytes, press CTRL+C to break
   Reply from 10.1.2.2: bytes=1419 Sequence=1 ttl=126 time=67 ms
   Reply from 10.1.2.2: bytes=1419 Sequence=2 ttl=126 time=50 ms
   Reply from 10.1.2.2: bytes=1419 Sequence=3 ttl=126 time=50 ms
   Reply from 10.1.2.2: bytes=1419 Sequence=4 ttl=126 time=50 ms
   Reply from 10.1.2.2: bytes=1419 Sequence=5 ttl=126 time=50 ms

 --- 10.1.2.2 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 50/53/67 ms
```

如果还是出现业务不通或时断时续的现象，说明所处网络无法正常处理分片报文或者处理分片报文导致CPU资源消耗过高。

因为视频会议属于TCP业务，TCP MSS值加上各种开销的报文总长度（MSS+TCP报文头+IP报文头+IPSec报文头）大于链路的MTU值，则数据报文会被分片发送。所以建议执行命令**tcp adjust-mss**，调整TCP MSS值。


```
[AR1] interface gigabitethernet 0/0/2
[AR1-GigabitEthernet0/0/2] tcp adjust-mss 1200
```

根因

原始报文的DF标志位为1，导致IPSec报文的DF标志位为1，不允许对IPSec报文进行分片。当IPSec报文超出MTU值时，IPSec报文被丢弃。

解决方案

执行命令**ipsec df-bit clear**，设置DF标志位为0，允许对IPSec报文进行分片。

建议与总结

- 网络传输故障与IPSec隧道无关，问题完全聚焦于分片的以太报文无法在WAN正常传输。
- 不论是否有IPSec隧道，报文都可能产生分片。但增加了IPSec报文头后，报文长度变大，分片的可能性增大。
- 如果AR所处网络无法正常处理分片报文，可以将TCP MSS调小以避免报文大量分片，规避此问题。

4.3 IPSec 隧道建立成功后业务质量差

4.3.1 AR 路由器由于 TCP MSS 值设置不合理导致用户无法通过 IPSec 隧道访问服务器

关键字

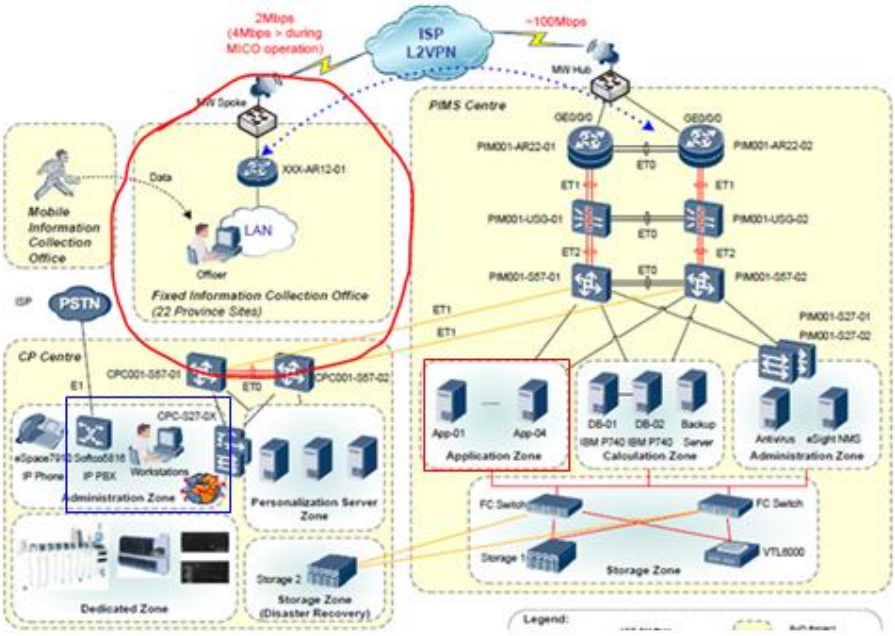
TCP MSS，IPSec，无法访问服务器

摘要

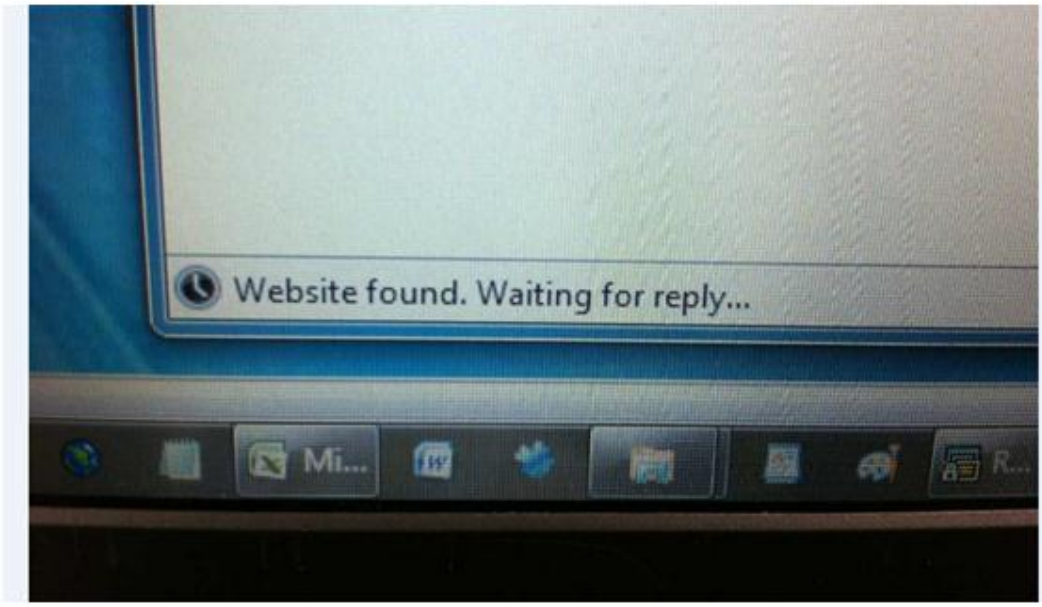
用户在办公室使用多台电脑访问weblogic服务器时，只有一台电脑偶尔能访问成功，其他电脑访问时页面均空白。

问题描述

如图所示，weblogic服务器安装在PIMS Centre的Application Zone中的集群服务器App01到App04上。Fixed Information Collection Office（FICO，图中红圈部分）的xxx-AR12-01设备与PIMS Centre的PIM001-AR22-01或PIM001-AR22-02设备间建立IPSec隧道（即图中蓝色虚箭头线），其穿过ISP L2VPN网络。



用户在FICO使用三台PC和两台笔记本通过IPSec隧道访问weblogic服务器时，仅有一台笔记本偶尔能成功访问，其他电脑访问时页面均空白。如下图所示，客户端持续等待HTTP请求的响应内容。

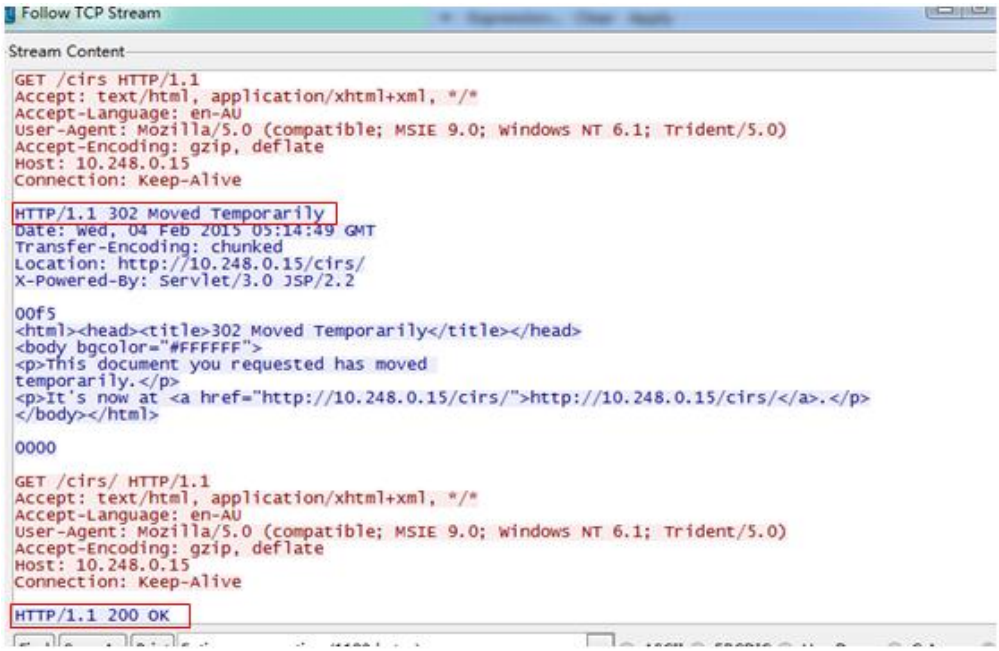


执行**display ipsec sa**命令查看IPSec隧道已建立成功，检查配置没有问题。

处理过程

1. 分别在访问失败和成功的笔记本网口上获取报文头。

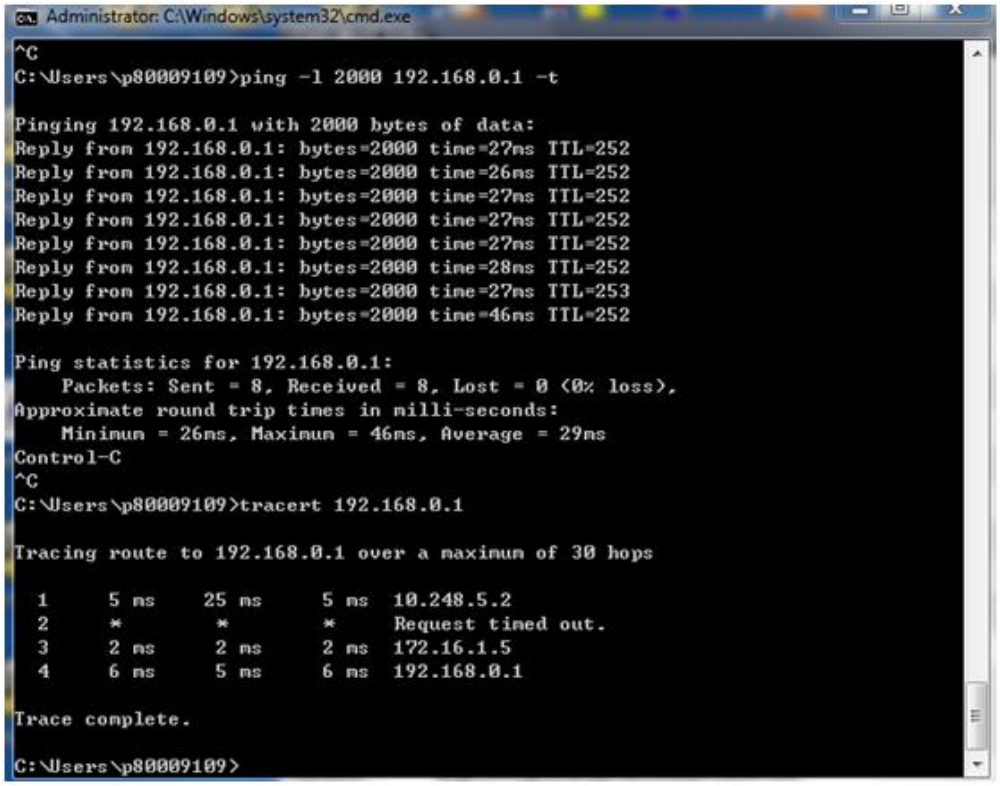
   通过Follow TCP Stream工具查看失败笔记本获取的报文头文件，发现有失败的HTTP请求，服务器有向客户端反馈响应。如下图所示，服务器正常反馈HTTP302响应重定向后，客户端继续请求服务器，服务器返回HTTP200正常响应，但无Text返回，即服务器响应HTTP请求成功后未返回Text内容。



2. 查看weblogic服务器是否异常。

   用户在CP Centre（如图所示标蓝色线部分）访问weblogic服务器，能够正常访问，说明服务器没有问题。同时，也可以排除汇聚交换机故障。

3. 在FICO的电脑上ping服务器地址，如下图所示。



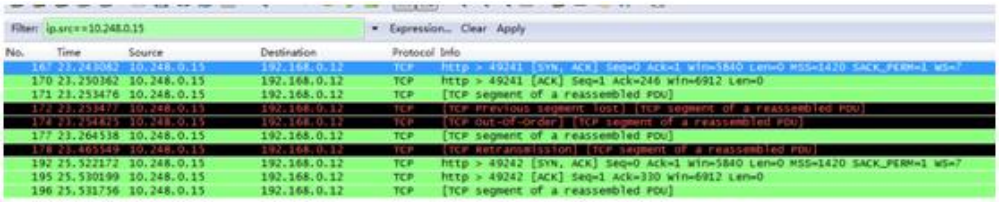
   发现TTL有时为252，有时为253，说明数据包路径会发生变化，怀疑是防火墙session检测将ping应答报文当成攻击报文阻断。

4. 检查防火墙是否有问题。

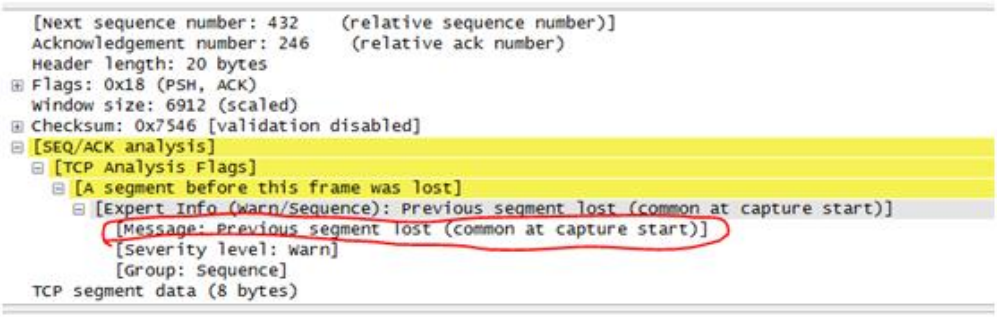
在防火墙上配置**undo firewall session link-state check tcp**命令后，再次测试，依旧无法访问。所以暂时排除防火墙问题。

5. 检查出口路由器或ISP的L2VPN链路。

   查看访问失败的报文，发现如下可疑数据包：

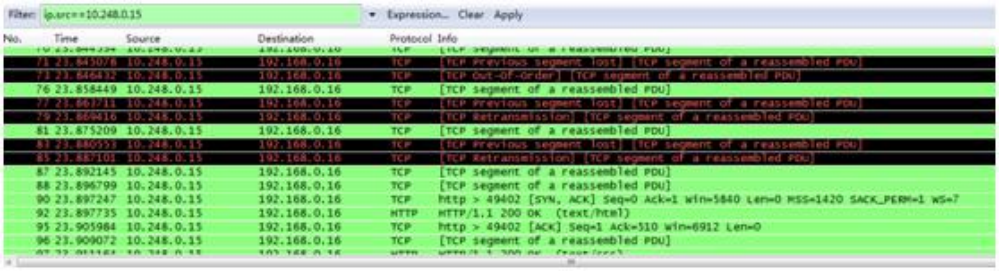


   分析数据包，发现服务器返回的TCP报文提示有前序的分片丢失情况



   在FICO直接向服务器ping大包且不分片则无法ping通，例如**ping** 10.248.0.15 **-l** 1446 **-f**。

   检查访问成功的报文，依然有很多分片丢失的响应报文，即访问成功的机器只是概率性成功。



   问题基本定位为在ISP传输链路途中分片报文丢失，则确定TCP MSS设置不合理。

6. 修改TCP MSS值。

   在出口AR路由器的接口视图下配置**tcp adjust-mss 1200**命令修改接口的TCP最大报文段长度为1200字节。

   修改配置后，在FICO的电脑再次访问weblogic服务器，都可成功访问。问题解决。

根因

TCP MSS（Max Segment Size）指定了TCP最大报文段长度，如果MSS值加上各种开销的报文总长度（MSS+TCP报文头+IP报文头）大于链路的MTU值，则数据报文会被分片发送。

在这场景中，TCP报文总长度（MSS+TCP报文头+IP报文头+IPSec头等）大于链路的MTU值，导致数据报文会被分片发送。而分片的过程会消耗更多的CPU资源，分片报

文的加密解密同样会消耗传输链路中设备的CPU资源。当CPU资源消耗过多，就会造成数据报文的丢失。所以用户在FICO使用三台PC和两台笔记本通过IPSec隧道访问weblogic服务器时，仅有一台笔记本偶尔能成功访问，其他电脑访问时页面均空白。

解决方案

在IPSec场景中，考虑到TCP报文头、IP报文头等开销，推荐用户在出口路由器的接口视图下配置TCP MSS值为1200字节，即可保证ISP链路设备不会再次对报文进行分片而过多的消耗其CPU资源造成丢包，可保证服务正常运行。

建议与总结

在VPN场景中，需要考虑发送的数据报文的大小是否过大造成报文分片。因为分片的过程会消耗更多的CPU资源，分片报文的加密解密同样会消耗传输链路中设备的CPU资源。当CPU资源消耗过多，就会造成数据报文的丢失。同时，对于某些高层应用（例如HTTP等应用层协议等）会将IP报文的DF(Don't Fragment)标记位置为有效，以防止TCP报文分片。如果DF标记位被置为有效，而路由器接口MTU小于MSS的值，此时路由器会因为不能强制分片TCP报文而将报文丢弃。

因此，请保证MSS值加上各种开销的报文总长度不超过MTU值。其中，以太网协议支持的MTU值最大为1500字节，PPPoE协议支持的MTU值最大为1492字节。推荐用户配置TCP MSS值为1200字节。

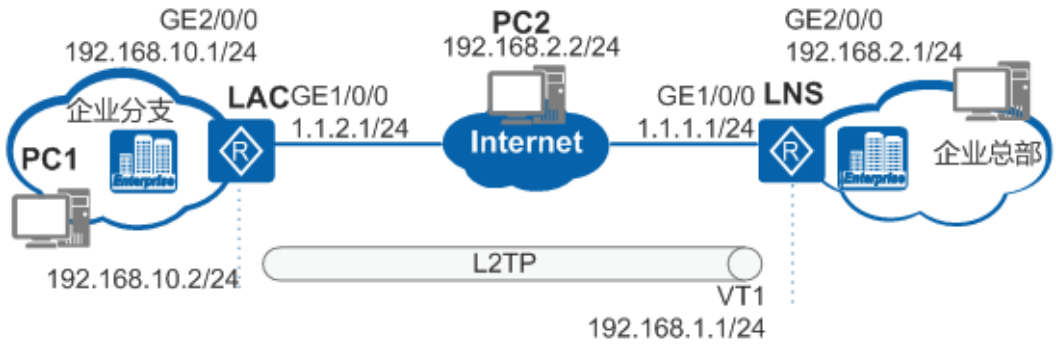
4.4 IPSec 隧道不稳定导致业务不通

4.4.1 AR 路由器由于错误配置 NAT Server 的 UDP 端口映射导致公网用户 L2TP 拨号失败

介绍AR路由器由于错误配置NAT Server的UDP端口映射导致公网用户L2TP拨号失败的故障案例。

组网情况

图 4-1 配置分支机构与总部之间通过 L2TP 方式实现互通组网图



LAC相关配置：

```
#
 l2tp enable
#
aaa
```



```
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 0
 local-user huawei service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 pppoe-server bind Virtual-Template 1
#
l2tp-group 1
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@
 tunnel name lac
 start l2tp ip 1.1.1.1 fullusername huawei
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2
#
interface gigabitethernet1/0/0
 nat server protocol tcp global interface gigabitethernet 1/0/0 www inside 192.168.10.2 www
 nat server protocol tcp global interface gigabitethernet 1/0/0 pop3 inside 192.168.10.2 pop3
 nat server protocol tcp global interface gigabitethernet 1/0/0 smtp inside 192.168.10.2 smtp
 nat server protocol tcp global interface gigabitethernet 1/0/0 ftp inside 192.168.10.2 ftp
 nat server protocol udp global interface gigabitethernet 1/0/0 any inside 192.168.10.2 any
 nat outbound 2001
#
return
```

现象描述

LAC作为企业的出口路由器，分支与总部之间通过L2TP拨号建立连接，LAC的出接口GE1/0/0通过PPPoE拨号上网。私网用户PC1进行L2TP拨号时能够成功建立连接。公网用户PC2进行L2TP拨号时提示错误800（PC2到LNS的路由经过LAC的GE1/0/0接口转发），登录LAC执行命令**debugging ppp all**和**debugging l2tp all**采集L2TP的调试信息，无任何打印信息。

原因分析

1. 检查是否是L2TP配置问题，私网用户PC1拨号可以成功发起L2TP隧道连接，L2TP配置没有问题。
2. 检查LAC上的出接口配置，发现出接口GE1/0/0配置了一条UDP全映射。

   ```
   <LAC> system-view
   [LAC] interface gigabitethernet1/0/0
   [LAC-GigabitEthernet1/0/0] display this
   #
   interface GigabitEthernet1/0/0
    ip address 1.1.2.1 255.255.255.0
    nat server protocol tcp global interface gigabitethernet 1/0/0 www inside 192.168.10.2 www
    nat server protocol tcp global interface gigabitethernet 1/0/0 pop3 inside 192.168.10.2 pop3
    nat server protocol tcp global interface gigabitethernet 1/0/0 smtp inside 192.168.10.2 smtp
    nat server protocol tcp global interface gigabitethernet 1/0/0 ftp inside 192.168.10.2 ftp
    nat server protocol udp global interface gigabitethernet 1/0/0 any inside 192.168.10.2 any
    nat outbound 2001
   ```

3. L2TP的隧道建立使用UDP端口号1701，在LAC上发现NAT Server配置UDP端口全映射到私网中，因此当公网用户向LNS发起L2TP拨号时，报文到达LAC的GE1/0/0时会命中NAT Server映射，将报文映射到私网中使报文无法达到LNS，导致公网用户无法成功进行L2TP拨号连接，删除配置后故障解决。

操作步骤

删除LAC上出接口GE1/0/0的NAT Server的UDP端口映射配置。


```
<LAC> system-view
[LAC] interface gigabitethernet1/0/0
[LAC-GigabitEthernet1/0/0] undo nat server protocol udp global interface gigabitethernet 1/0/0 any inside 192.168.10.2 any
```

总结与建议

遇到L2TP无法成功拨入设备，常见的定位思路如下：

1. 检查设备上的配置，排除配置错误。
2. 如果配置没有问题，通过**debugging ppp all**和**debugging l2tp all**，采集调试信息定位问题。
3. 如果无法采集到信息，考虑报文是否达到LNS侧，是否被LNS拒绝或是否转发到了其他网络设备。
4. 配置NAT Server进行端口全映射时，要充分考虑业务特性，例如L2TP、Telnet等，以免造成业务异常或中断。

5 附录

5.1 IPSec 故障分析

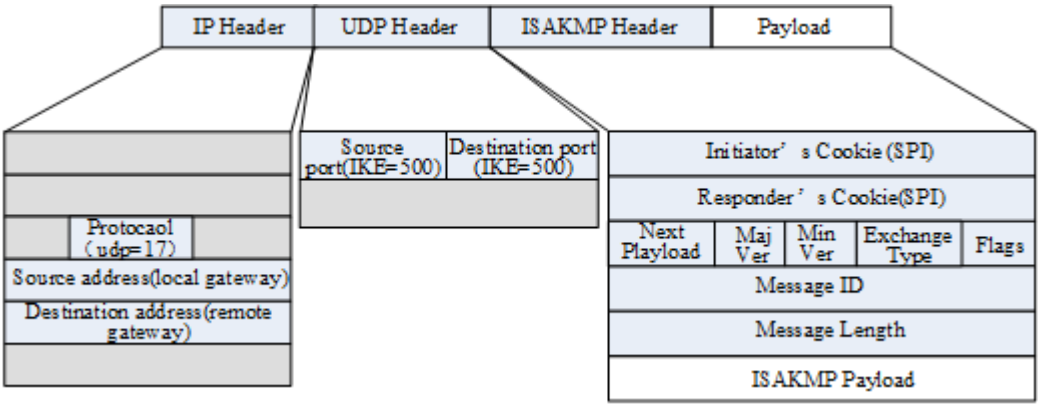
5.1.1 IPSec 隧道建立失败故障分析

5.1.1.1 ISAKMP 报文封装

Internet安全联盟和密钥管理协议ISAKMP是IKE的基础。IKE采用ISAKMP报文进行安全联盟的协商、密钥交换以及对等体身份验证。

ISAKMP报文封装如图5-1所示。

图 5-1 ISAKMP 报文封装



IP 报文头

源地址：为发起IKE协商的IP地址，可能是接口IP地址，也可能是local-address命令配置的IP地址。

目的IP地址：为对端设备的IP地址，由**remote-address**命令配置。

UDP 报文头

IKE协议使用端口号500发起协商、响应协商。在NAT穿越场景下端口号会在网关探测完成后切换到4500。

ISAKMP 报文头

Initiator's Cookie (SPI)：发起端唯一标识一个IKE SA的数值，不能为0。

Responder's Cookie (SPI)：响应端唯一标识一个IKE SA的数值，第一条消息中SPI为0，后续均不为0。

Next Payload：标识消息中下一个载荷的类型。若当前载荷是消息中最后一个载荷，则该字段为0。该字段提供载荷之间的“链接”能力。当需要在消息末尾增加一个新的载荷时，在前一个载荷末尾标识出新增载荷的类型即可。

IKEv1和IKEv2的下一个载荷的类型如表5-1和表5-2所示。

表 5-1 IKEv1 的下一个载荷

下一载荷（Next Payload）	缩写	取值	作用
None	-	0	当前载荷是消息中最后一个载荷。
Security Association	SA	1	用于协商IKE或IPSec安全提议。
Proposal	P	2	用于协商安全协议以及SA采用的相关安全机制。
Transform	T	3	用于传输相关的安全联盟属性来协商出双方支持的提议。
Key Exchange	KE	4	用于在DH密钥交换中交换DH公开值。
Identification	IDi，IDr	5	用于发送身份ID，可以用于接入控制。证书认证中该载荷不必进行匹配。

下一载荷（Next Payload）	缩写	取值	作用
Certificate	CERT	6	用于传送证书或其它与认证相关的信息。
Certificate-Request	CERTREQ	7	用于请求首选证书。
Hash	HASH_I，HASH_R	8	用于验证IKE消息的完整性，或对协商对等体进行认证。
Signature	SIG_I，SIG_R	9	用于认证IKE消息的完整性，还可用作无否认服务。
Norigication	N	10	用于通告错误和状态迁移。
Nonce	Ni，Nr	11	用于传送临时随机数。
Delete	D	12	表示该SPI标识的SA已经被删除。
Vendor ID	V	13	表示发送方能够接受某些协议的扩展。
Properties	-	14	表示属性载荷。
NAT Discovery	NAT-D	20	用于判断设备是否在NAT设备后面。
NAT Original Address	NAT-OA	21	表示IPSec对话方的原始地址。
Reserved	-	15-127	保留。
Private Use	-	128-255	私用。

表 5-2 IKEv2 的下一个载荷

下一载荷（Next Payload）	缩写	取值	作用
No Next Payload	-	0	当前载荷是消息中最后一个载荷。
Reserved	-	1-32	保留。

下一载荷（Next Payload）	缩写	取值	作用
Security Association	SA	33	用于协商IKE或IPSec安全提议。
Key Exchange	KE	34	用于在DH密钥交换中交换DH公开值。
Identification-Initiator	IDi	35	用于发送身份ID，可以用于接入控制。证书认证中该载荷不必进行匹配。
Identification-Responder	IDr	36	
Certificate	CERT	37	用于传送证书或其它与认证相关的信息。
Certificate-Request	CERTREQ	38	用于请求首选证书。
Authentication	Auth	39	用于发送认证方法和认证数据（Hash值）。
Nonce	Ni，Nr	40	用于传送临时随机数。
Notify	N	41	用于通告错误和状态迁移。
Delete	D	42	表示该SPI标识的SA已经被删除。
Vendor ID	V	43	表示发送方能够接受某些协议的扩展，目前用于协商NAT-T能力。
Traffic Selector-Initiator	TSi	44	表示需要IPSec保护的数据流。
Traffic Selector-Responder	TSr	45	
Encrypted	E	46	用于传送其它载荷加密后的数值。

下一载荷（Next Payload）	缩写	取值	作用
Configuration	CP	47	包含CFG_REQUEST、CFG_REPLAY、CFG_SET、CFG_ACK用于地址分配的请求、应答。
Extensible-Authentication	EAP	48	用于承载EAP消息。
Reserved to	IANA	49-127	保留。
Private Use	-	128-255	私用。

Maj Ver/Min Ver：主版本/副版本，ISAKMP版本的标识是用主版本和副版本的字段中的主/副编号来进行的。在IKE中，两个字段合为一个字段。

Version：IKEv1版本该字段值为1.0，IKEv2版本该字段值为2.0。

Exchange Type：交换类型，该字段限制消息的载荷内容和交换消息的顺序。

IKEv1和IKEv2的交换类型如**表5-3**和**表5-4**所示。

表 5-3 IKEv1 的交换类型

交换类型（Exchange Type）	取值
None	0
Base	1
Identity protection	2
Authentication only	3
Aggressive	4
Informational	5
Future use	6-31
DOI specific use	32-239
Private use	240-255

表 5-4 IKEv2 的交换类型

交换类型（Exchange Type）	取值
Reserved	0-33
IKE_SA_INIT	34
IKE_SA_AUTH	35
Create_CHILD_SA	36
Informational	37
Reserved to IANA	38-239
Reserved for Private Use	240-255

Flags：标志表示特定的选项，用于设定ISAKMP交换。以下在标志字段中指定的标志，从最低有效位开始：

- IKEv1：第0位为加密位，为1表示有效载荷已被加密；第1位为提交位，为1表示确保建立SA之后才能收到加密的内容；第2位为认证位，为1表示只对有效载荷进行验证，而不进行加密。其他剩余位没有被定义，必须在传输前设为0。
- IKEv2：第3位为1表示发起方，第4为IKEv2应设为0，第5位为1表示响应方。其他剩余位没有被定义，必须在传输前设为0。

Message ID：第一阶段中该字段为0，在第二阶段为发起方生成的随机数。它作为惟一的消息标志，用于在第二阶段的协商中标识协议状态。

Message Length：标识ISAKMP消息的全长（包含消息头和载荷）。

5.1.1.2 IKEv1 阶段 1 协商过程

IKEv1阶段1的目的是建立IKE SA。IKE SA建立后对等体间的所有ISAKMP消息都将进行加密和验证，这条安全通道可以保证IKEv1阶段2的协商能够安全进行。

IKEv1阶段1支持两种协商模式：

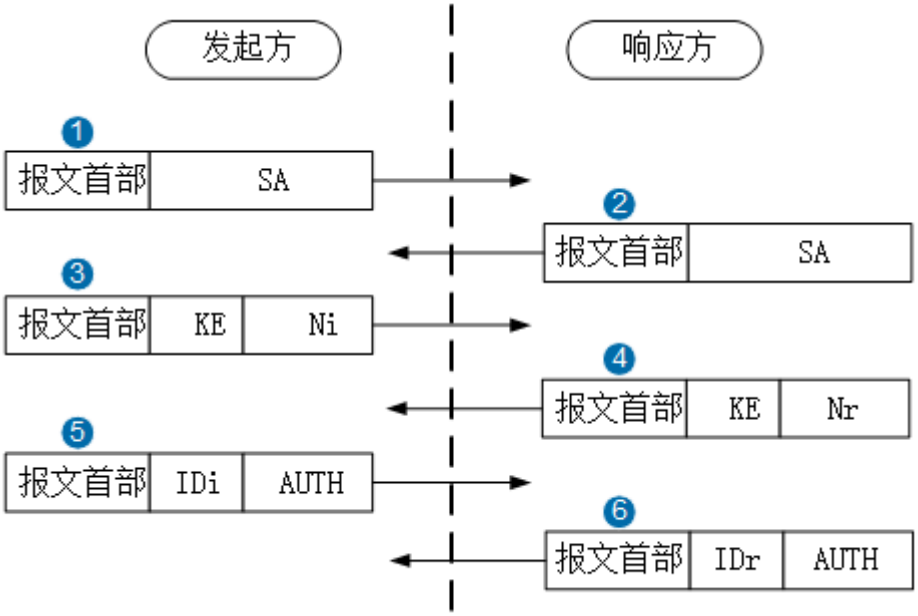
- **主模式（Main Mode）**
- **野蛮模式（Aggressive Mode）**

主模式协商过程

主模式包含三次双向交换，用到了六条信息，交换过程如图5-2所示。

1. 策略交换：对应消息①和②。
2. 密钥信息交换：对应消息③和④。
3. 身份和认证信息交换：对应消息⑤和⑥。

图 5-2 主模式协商过程（预共享密钥认证）

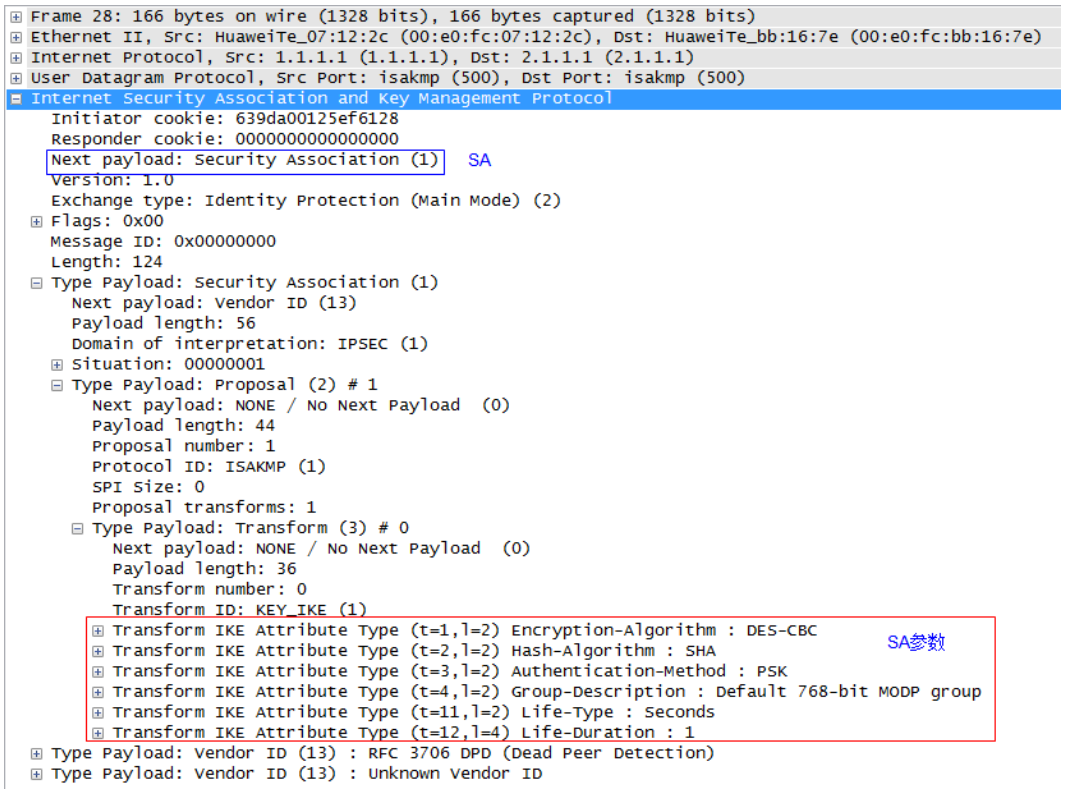


策略交换

消息①：发起方发送封装有IKE安全提议的SA载荷进行安全提议协商，SA中参数包括加密算法、认证方法、身份认证算法、DH组、IKE SA生存周期等。

消息②：响应方查找最先匹配的IKE安全提议，发送一个SA载荷，表明接受协商的IKE安全提议。

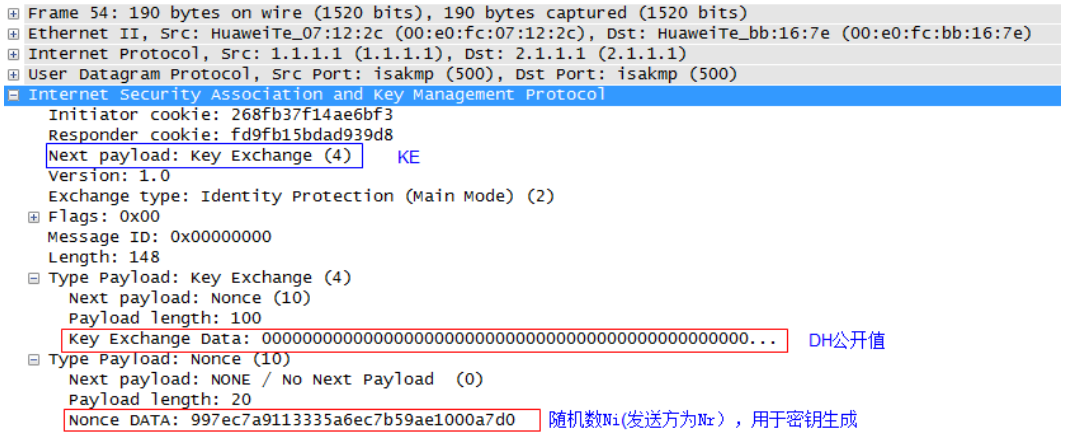
图 5-3 消息①、②



密钥信息交换

消息③、④：发起者和接受者交换DH公开值（KE载荷）和临时随机数（Ni、Nr）。Ni、Nr是计算共享密钥（用来生成加密密钥和认证密钥）所必须的。

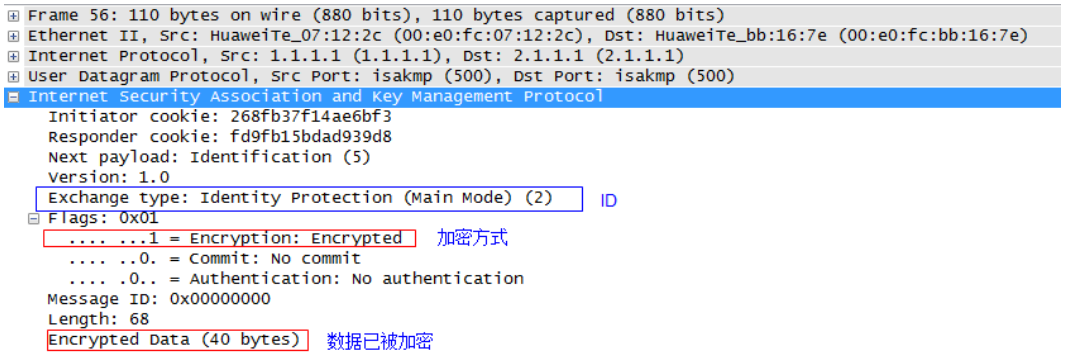
图 5-4 消息③、④



身份和认证信息交换

消息⑤、⑥：双方交换身份ID（ID载荷）和验证Hash值（AUTH载荷）。这两个消息中传递的信息是加密的，加密的密钥由消息③、④中交换的密钥信息生成，所以身份信息受到保护。由于主模式下ID载荷经加密，所以获取报文头中无法看到。

图 5-5 消息⑤、⑥

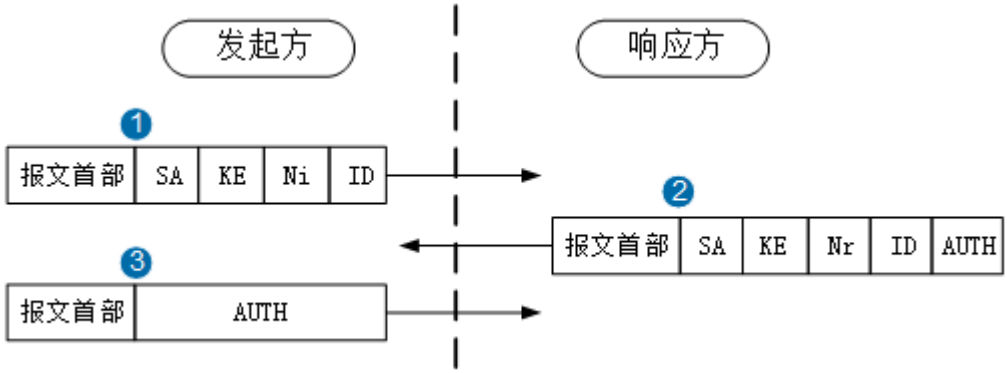


野蛮模式协商过程

野蛮模式只用到三条信息，交换过程如图5-6所示。

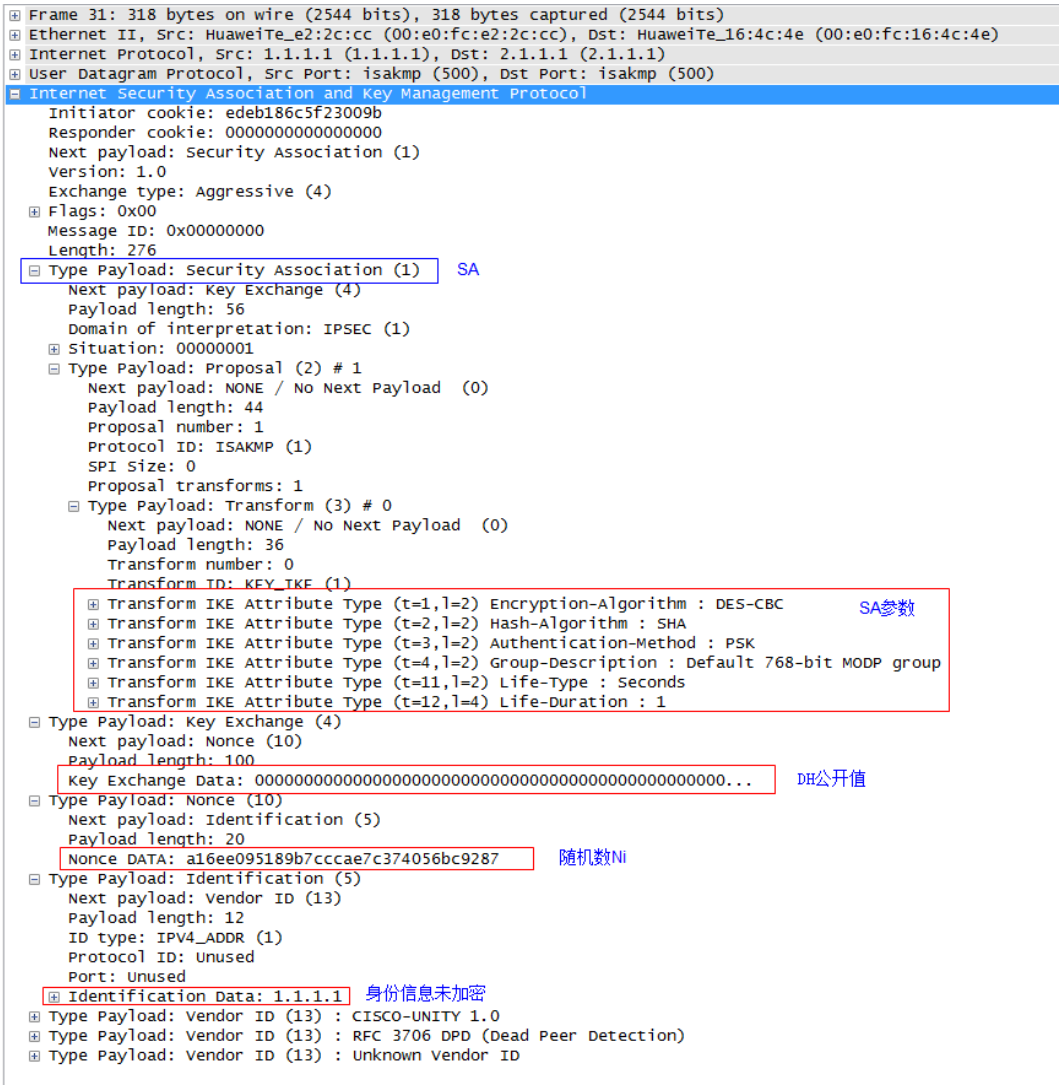
前两条消息①和②用于协商提议，交换Diffie-Hellman公共值、必需的辅助信息以及身份信息，并且消息②中还包括响应方发送身份信息供发起方认证，消息③用于响应方认证发起方。

图 5-6 野蛮模式协商过程（预共享密钥认证）



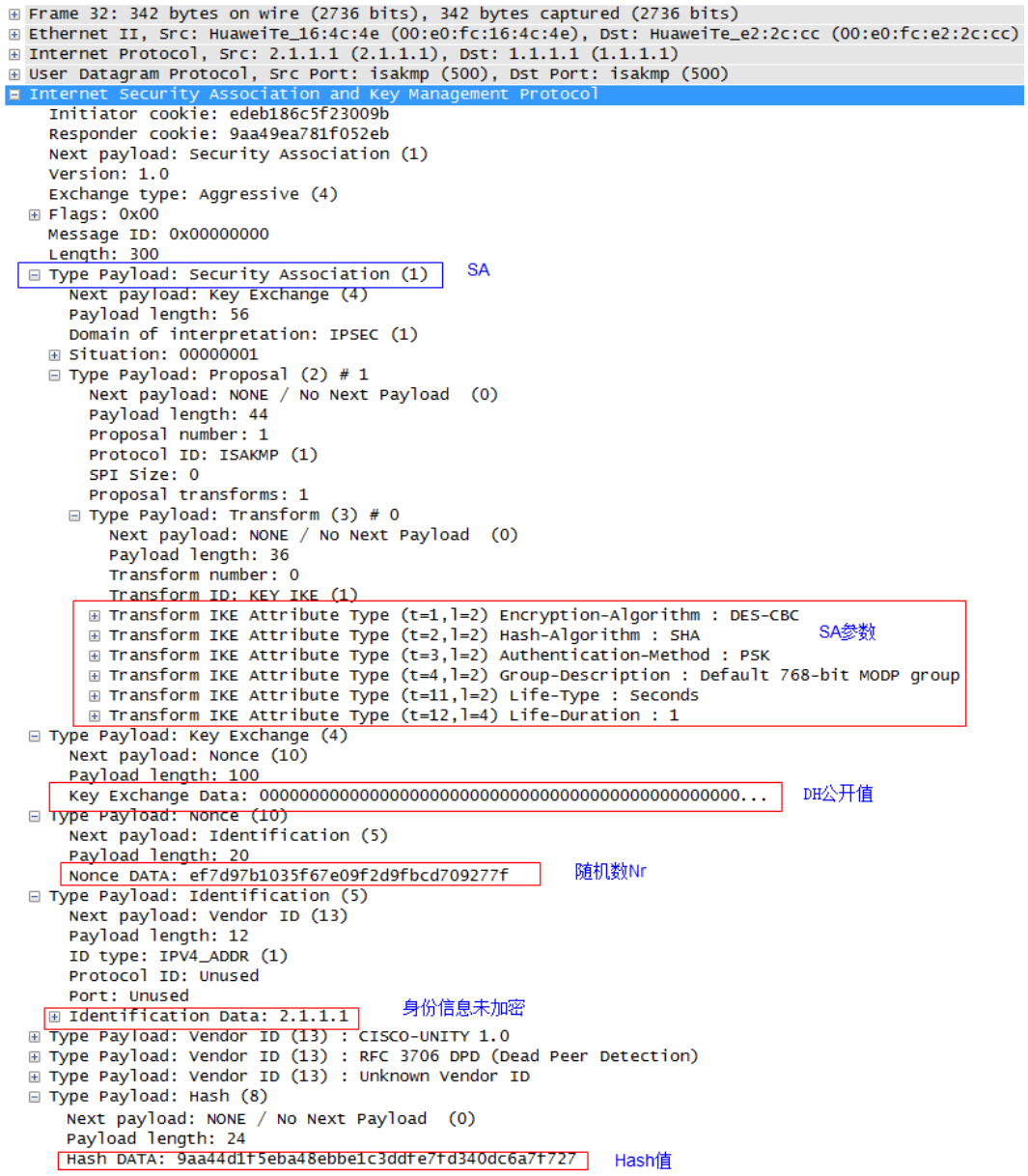
消息①：发起端发送封装有IKE安全提议的SA载荷。在野蛮模式中，只带有一个安全提议（加密算法、认证方法、身份认证算法、DH组、IKE SA生存周期等），响应者可以选择接受或拒绝该安全提议。DH公开值（KE载荷）、临时随机数（Ni载荷）和身份ID（ID载荷）也在其中发送。野蛮模式下，身份信息未经加密，故获取报文头能够看到。

图 5-7 消息①



消息②：响应者发送SA载荷，包含推荐的安全提议。DH公开值（KE载荷）、临时随机数（Nr载荷）和身份ID（ID载荷）、验证Hash值（AUTH载荷）也在其中发送。

图 5-8 消息②



消息③：发起端发送验证Hash值确认协商成功。

图 5-9 消息③

总结

IKEv1阶段1协商完成后，可以执行命令**display ike sa**，查看第一阶段的SA建立情况。当**Flag**参数为**RD**或**RD|ST**表示IKE SA已建立成功。其中，**ST**表示本端是SA协商发起方。

```
<Huawei> display ike sa
IKE SA information :
    Conn-ID      Peer             VPN    Flag(s)       Phase
-------------------------------------------------------------------------
    16         2.1.1.1:500              RD|ST         v1:2
    14         2.1.1.1:500              RD|ST         v1:1

 Number of IKE SA : 2
-------------------------------------------------------------------------
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

协商失败时，执行该命令显示可能为空、Flag参数为空或者Peer参数为0.0.0.0。

隧道两端IKE安全提议、预共享密钥等参数不匹配都将导致IKE SA无法建立。当隧道两端配置的IKE参数不一致时，常出现的debug信息如下。

- 两端的IKE安全提议不一致

  ```
  <Huawei> debugging ikev1 error
  Aug 17 2017 14:29:15.800.1 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 17:5773 Message from peer 2.1.1.1: Got NOTIFY of type NO_PROPOSAL_CHOS
  EN

  Aug 17 2017 14:29:15.800.3 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 0:9946 Ikev1 error-info record(peer address: 2.1.1.1, error reason: ph
  ase1 proposal mismatch,list number: 11).
  ```

- 两端的预共享密钥不一致

  ```
  <Huawei> debugging ikev1 error
  Aug 17 2017 15:18:09.800.1 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 17:5773 Message from peer 2.1.1.1: Got NOTIFY of type PAYLOAD_MALFORME
  D
  <Huawei> debugging ikev1 error
  Aug 17 2017 15:24:53.940.2 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 17:1053 Message from peer 1.1.1.1: Invalid Next Payload of Type 60 in
  Payload Type 5

  Aug 17 2017 15:24:53.940.3 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 17:6847 Message from peer 1.1.1.1: dropping Message due to notificatio
  ```



```
n type INVALID_PAYLOAD_TYPE

Aug 17 2017 15:24:53.940.4 Huawei IKE/7/IKE_Debug:
IKE_ERROR 17:4538 Message from peer 1.1.1.1: Message Sort Error Occurred

Aug 17 2017 15:24:53.940.5 Huawei IKE/7/IKE_Debug:
IKE_ERROR 0:9946 Ikev1 error-info record(peer address: 1.1.1.1, error reason: ma
lformed payload,list number: 200).
```

- 一端未配置**remote-address**

```
<Huawei> debugging ikev1 error
Aug 17 2017 16:13:33.940.3 Huawei IKE/7/IKE_Debug:
IKE_ERROR 0:9946 Ikev1 error-info record(peer address: 1.1.1.1, error reason: pe
er address mismatch,list number: 200).

Aug 17 2017 16:13:33.940.4 Huawei IKE/7/IKE_Debug:
IKE_ERROR 0:3595 Phase 1 Exchange: ike peer configuration not found for peer "1.
1.1.1"
```

- 本端**remote-id**与对端名称不一致

```
<Huawei> debugging ikev1 error
Aug 17 2017 16:25:01.850.2 Huawei IKE/7/IKE_Debug:
IKE_ERROR 25:6956 ERROR - Received remote-name(fw2) does not match with peer rem
ote-name(fw3)

Aug 17 2017 16:25:01.850.3 Huawei IKE/7/IKE_Debug:
IKE_ERROR 0:9946 Ikev1 error-info record(peer address: 2.1.1.1, error reason: co
nfig ID mismatch,list number: 148).
```

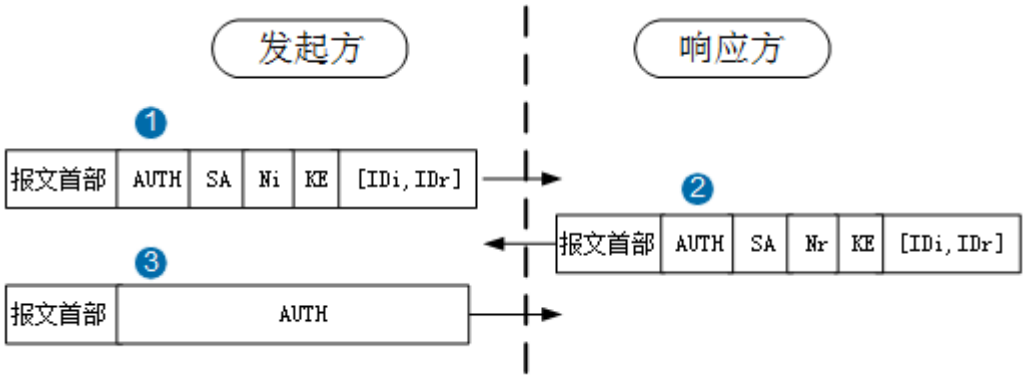
5.1.1.3 IKEv1 阶段 2 协商过程

IKEv1阶段2的目的就是建立用来传输数据的IPSec SA。阶段2的交换模式是快速模式，交换的载荷都是加密的。

协商过程

快速模式交换过程图如图5-10所示。

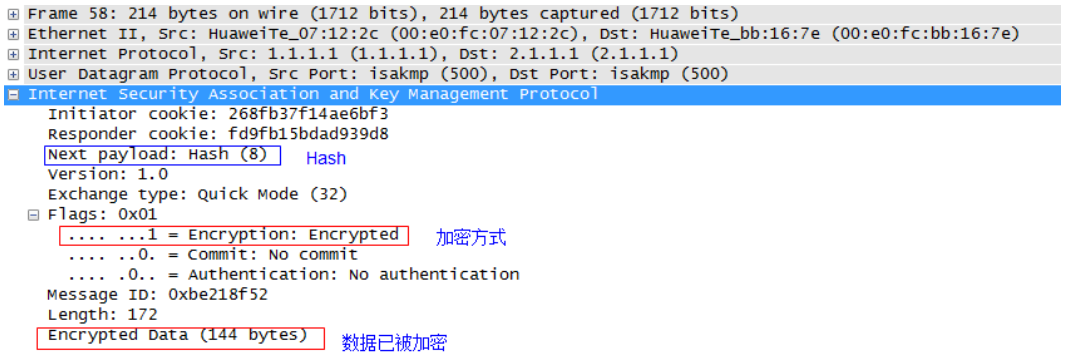
图 5-10 IKEv1 阶段 2 协商过程



消息①、②：协商IPSec安全提议（SA载荷），为PFS功能协商DH密钥组（KE载荷）。交换身份ID（ID载荷为可选）和完整性验证Hash值（AUTH载荷）。

IDi和IDr属于ID载荷，这里是在交换流量选择符，确定双方保护的流量一致（相当于IKEv2的TS载荷的作用）。

图 5-11 消息①、②



消息③：发送完整性验证Hash值确认协商成功。其报文格式类似消息①。

总结

IKEv1阶段2协商完成后，可以执行命令**display ike sa**，查看第二阶段的IPSec SA建立情况。当**Flag**参数为**RD**或**RD|ST**表示SA已建立成功。其中，**ST**表示本端是SA协商发起方。

```
<Huawei> display ike sa
IKE SA information :
    Conn-ID      Peer             VPN    Flag(s)       Phase
-------------------------------------------------------------------------
    16         2.1.1.1:500              RD|ST         v1:2
    14         2.1.1.1:500              RD|ST         v1:1

 Number of IKE SA : 2
-------------------------------------------------------------------------
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

协商失败时，执行该命令显示Flag参数为空。

两端IPSec安全提议、PFS、ACL规则不匹配都将导致IPSec SA建立失败。阶段2报文是加密的，所以无法通过获取报文头检查IPSec安全提议配置。

当隧道两端配置的IPSec参数不一致时，常出现的debug信息如下。

- 两端的ACL规则不匹配

  ```
  <Huawei> debugging ikev1 error
  Aug 17 2017 17:35:52.350.1 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 17:5773 Message from peer 1.1.1.1: Got NOTIFY of type INVALID_ID_INFOR
  MATION

  Aug 17 2017 17:35:52.350.2 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 0:9946 Ikev1 error-info record(peer address: 1.1.1.1, error reason: fl
  ow mismatch,list number: 200).
  <Huawei> debugging ipsec error
  Aug 17 2017 17:35:17.800.1 Huawei IPSEC/7/IPSEC-DEBUG:
  [IPSEC-Error] acl mismatch.(Ifindex=[7], SeqNum=[10],PeerAddress=[2.1.1.1], Peer
  Port=[500])
  ```

- 两端的IPSec安全提议或PFS算法不一致

  ```
  <Huawei> debugging ikev1 error
  Aug 18 2017 09:28:45.350.2 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 0:9946 Ikev1 error-info record(peer address: 2.1.1.1, error reason: ph
  ```



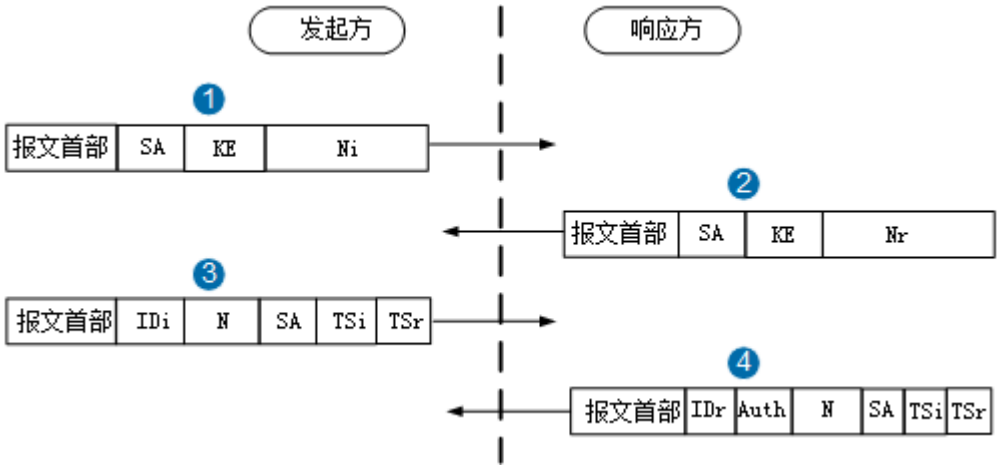
```
ase2 proposal or pfs mismatch,list number: 200).

Aug 18 2017 09:28:45.350.3 Huawei IKE/7/IKE_Debug:
IKE_ERROR 17:6847 Message from peer 2.1.1.1: dropping Message due to notificatio
n type NO_PROPOSAL_CHOSEN
<Huawei> debugging ipsec error
Aug 18 2017 09:29:26.800.1 Huawei IPSEC/7/IPSEC-DEBUG:
[IPSEC-Error] ipsec proposal or pfs mismatch.(Ifindex=[7], SeqNum=[10],PeerAddre
ss=[2.1.1.1], PeerPort=[500])
```

5.1.1.4 IKEv2 协商过程

协商过程

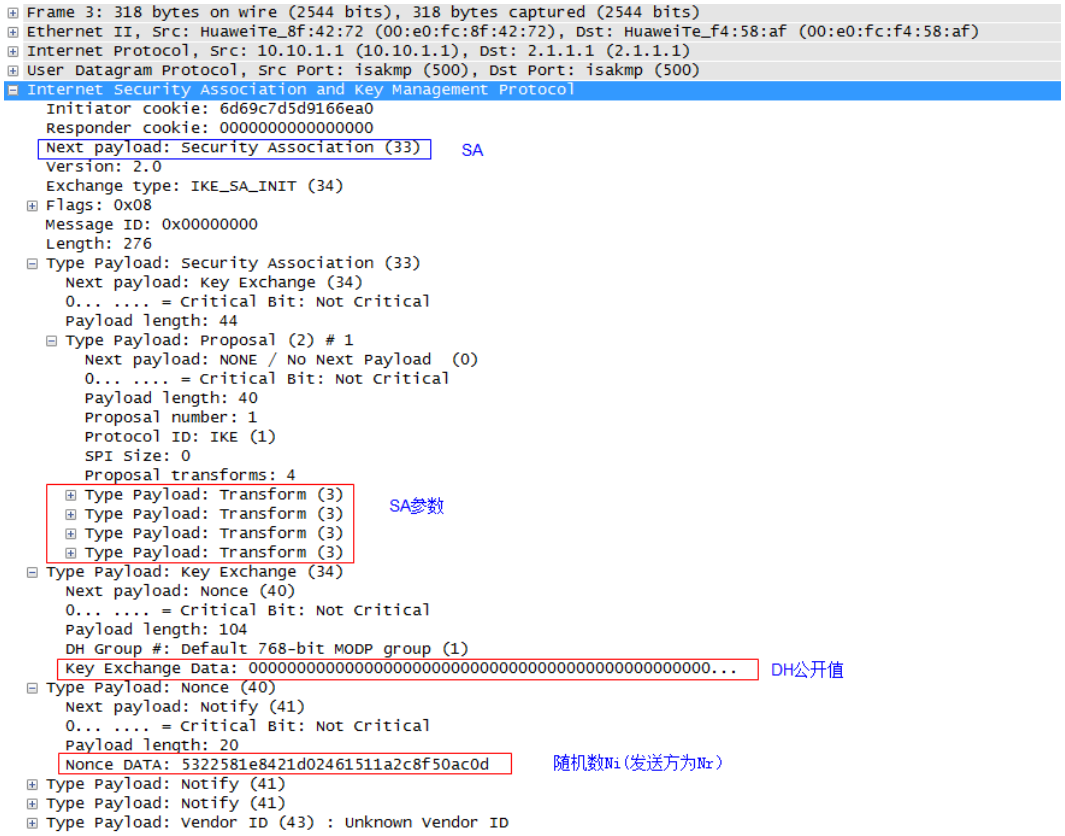
要建立一对IPSec SA，IKEv1需要经历两个阶段：“主模式＋快速模式”或者“野蛮模式＋快速模式”。前者至少需要交换9条消息，后者也至少需要6条消息。而IKEv2，没有主模式和野蛮模式，正常情况使用2次交换共4条消息就可以完成一个IKE SA和一对IPSec SA。IKEv2协商过程图如图5-12所示。

图 5-12 IKEv2 协商过程（预共享密钥认证）



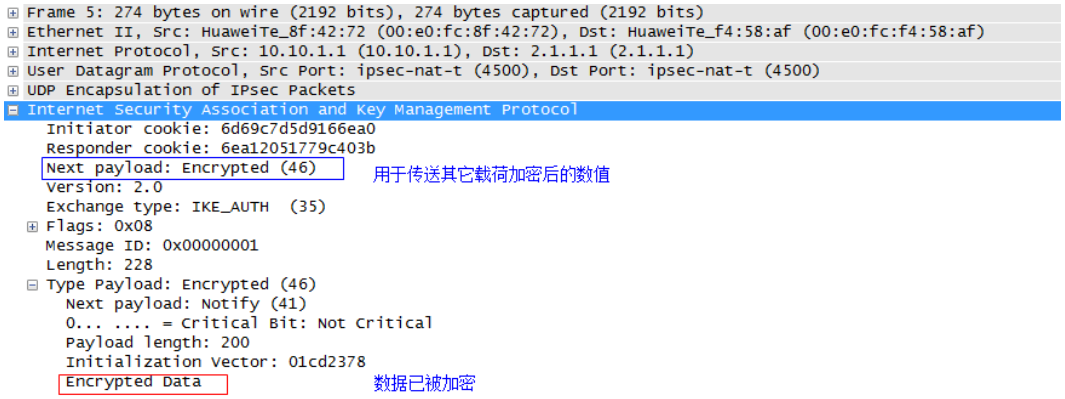
消息①、②：IKE_SA_INIT交换。协商IKE安全提议（SA载荷），交换临时随机数（Ni、Nr载荷）和DH公开值（KE载荷）。

图 5-13 消息①、②



消息③、④：IKE_AUTH交换。双方继续交换身份ID（ID载荷）和Hash值（AUTH载荷），协商IPSec安全提议（SA载荷）、待保护数据流（TS载荷）。N载荷用于错误通知。协商通过后建立IKE SA和一对IPSec SA。

图 5-14 消息③、④



总结

IKEv2协商完成后，可以执行命令**display ike sa**，查看SA建立情况。当**Flag**参数为**RD**或**RD|ST**表示SA已建立成功。其中，**ST**表示本端是SA协商发起方。

```
<Huawei> display ike sa
IKE SA information :
    Conn-ID      Peer              VPN    Flag(s)       Phase
 ------------------------------------------------------------------------
    16          2.1.1.1:500              RD|ST         v2:2
    14          2.1.1.1:500              RD|ST         v2:1

  Number of IKE SA : 2
 ------------------------------------------------------------------------
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

协商失败时，执行该命令可能出现如下情况：

- 第一阶段协商失败：显示为空、**Flag**参数为空或者Peer参数为0.0.0.0。
- 第二阶段协商失败：第一阶段的显示正常，第二阶段不显示或**Flag**参数为空。

两端IKE安全提议、预共享密钥、IPSec安全提议、PFS、ACL规则等不匹配都将导致IKE SA或IPSec SA无法建立。

当两端配置的IPSec参数不一致时，常出现的debug信息如下。

- 两端的IKE安全提议不一致

  ```
  <Huawei> debugging ikev2 error
  Aug 18 2017 14:51:00.410.2 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 56:8841 Ikev2 error Info record(peer address: 2.1.1.1, error reason: p
  hase1 proposal mismatch,list number: 200).
  ```

- 两端的预共享密钥不一致

  ```
  <Huawei> debugging ikev2 error
  Aug 18 2017 15:02:25.540.2 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 63:4087 Authentication failed for the peer 2.1.1.1

  Aug 18 2017 15:02:25.540.4 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 56:8841 Ikev2 error Info record(peer address: 2.1.1.1, error reason: a
  uthentication fail,list number: 4).
  ```

- 本端remote-id与对端名称不一致

  ```
  <Huawei> debugging ikev2 error
  Aug 18 2017 15:39:32.50.4 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 27:27568 ERROR - Peer remote-name(fw3) does not match with

  Aug 18 2017 15:39:32.50.5 FW1 IKE/7/IKE_Debug:
  IKE_ERROR 56:8841 Ikev2 error Info record(peer address: 2.1.1.1, error reason: c
  onfig ID mismatch,list number: 151).
  ```

- 一端未配置**remote-address**

  ```
  <Huawei> debugging ikev2 error
  Aug 18 2017 15:23:04.400.1 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 56:8841 Ikev2 error Info record(peer address: 2.1.1.1, error reason: p
  eer address mismatch,list number: 107).
  ```

- 两端的ACL规则不匹配

  ```
  <Huawei> debugging ikev2 error
  Aug 18 2017 15:27:40.750.1 Huawei IKE/7/IKE_Debug:
  IKE_ERROR 56:8841 Ikev2 error Info record(peer address: 1.1.1.1, error reason: f
  low mismatch,list number: 200).
  <Huawei> debugging ipsec error
  Aug 18 2017 15:29:46.650.1 Huawei IPSEC/7/IPSEC-DEBUG:
  ```



```
[IPSEC-Error] acl mismatch.(Ifindex=[7], SeqNum=[0],PeerAddress=[1.1.1.1], PeerP
ort=[500])
```

- 两端的IPSec安全提议或PFS算法不一致

```
<Huawei> debugging ikev2 error
Aug 19 2017 09:41:40.800.2 Huawei IKE/7/IKE_Debug:
IKE_ERROR 56:8841 Ikev2 error Info record(peer address: 2.1.1.1, error reason: p
hase2 proposal or pfs mismatch,list number: 200).
<Huawei> debugging ipsec error
Aug 19 2017 09:44:25.760.2 Huawei IPSEC/7/IPSEC-DEBUG:
[IPSEC-Error] ipsec proposal or pfs mismatch.(Ifindex=[7], SeqNum=[10],PeerAddre
ss=[2.1.1.1], PeerPort=[500])
```

5.1.1.5 IKE 的 NAT 穿越协商

在IPSec隧道两端之间存在NAT网关时，IKE能够自动完成两端之间的NAT-T能力协商、NAT网关探测并建立SA。

IKEv1 的 NAT 穿越协商

IKEv1的NAT穿越场景中，需要在IKEv1阶段1协商中对NAT执行两种探测：

- 探测是否支持NAT穿越（NAT-T能力）。

  IKEv1使用VID载荷来确定是否支持NAT穿越。

- 探测在网络中是否存在NAT网关。

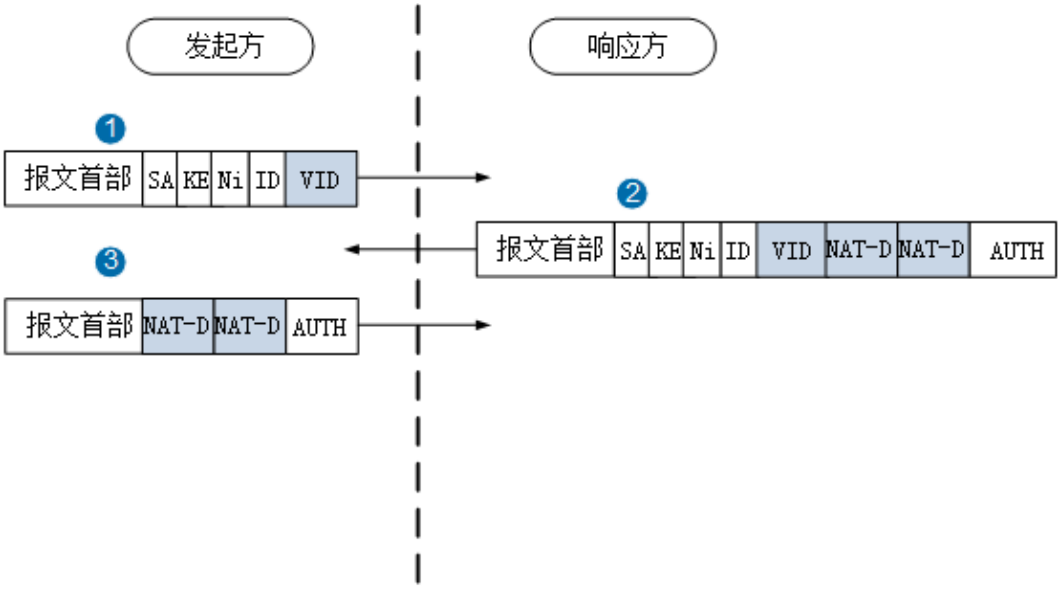
  IKEv1使用NAT-D载荷探测两个IKE对等体之间是否存在NAT网关以及存在的位置（即谁在NAT网关的后面）。

由于NAT网关会改变IKE UDP的源端口，所以响应方必须能处理源端口不是500的IKE报文。

野蛮模式的IKEv1阶段1的NAT穿越协商过程如图5-15所示。

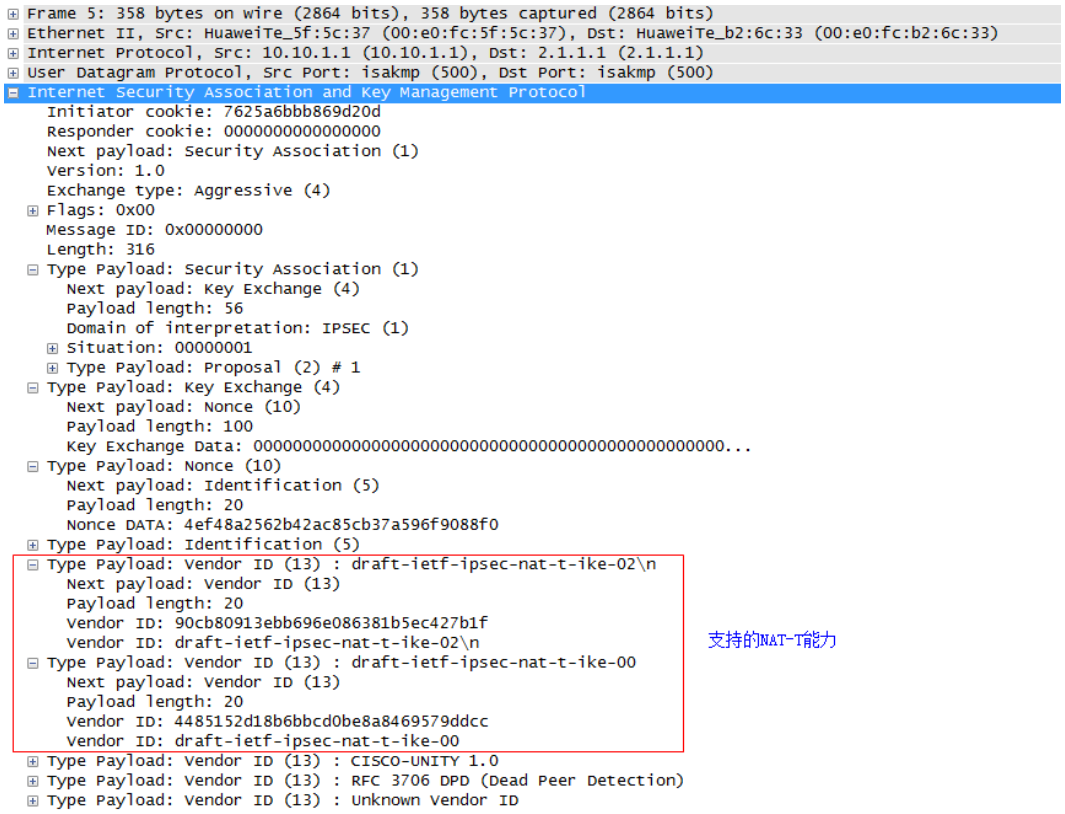
对于主模式的NAT穿越协商过程，这里不再详情介绍。其与**主模式协商过程**相同，只是在消息①、②报文中增加VID载荷，消息③、④报文中增加NAT-D载荷。

图 5-15 野蛮模式的 IKEv1 阶段 1 的 NAT 穿越协商过程（预共享密钥认证）



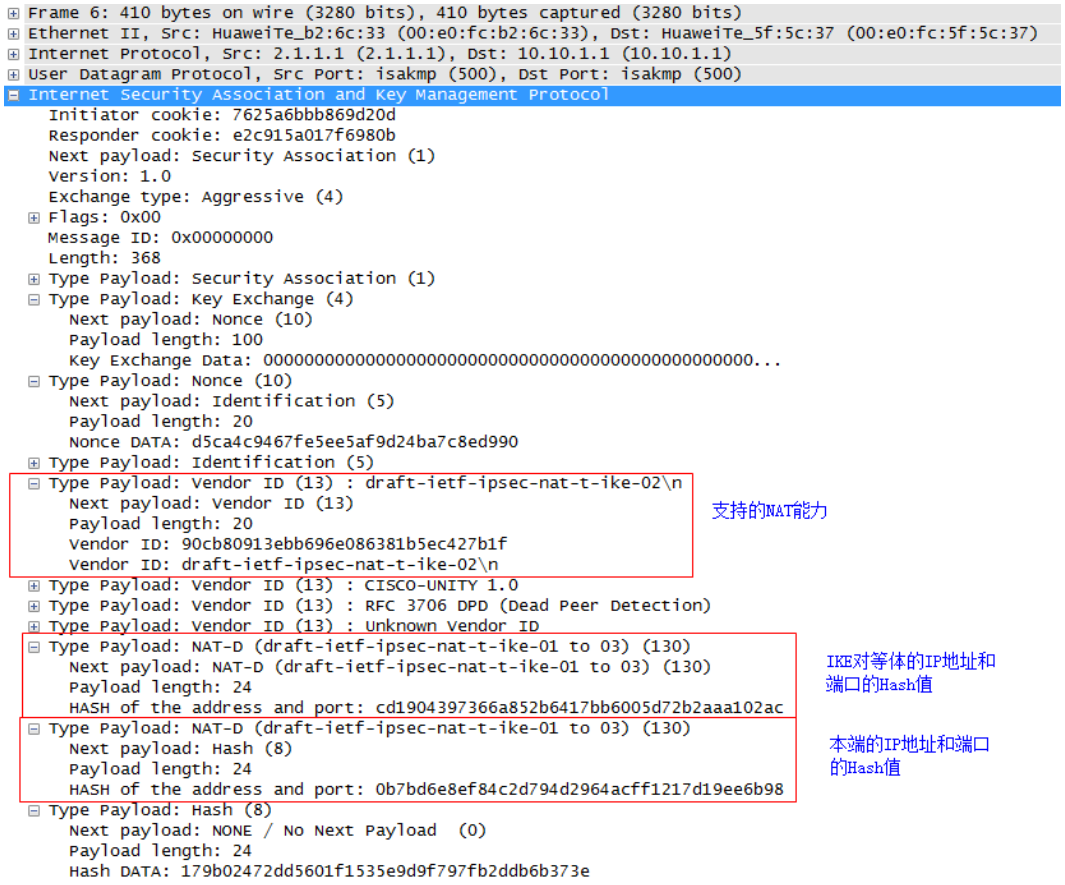
消息①：发起方在IKE消息中插入VID载荷来告知对方自己支持NAT穿越。若双方发的IKEv1消息中都包含该载荷，说明双方都支持NAT-T，协商继续，否则终止。

图 5-16 消息①



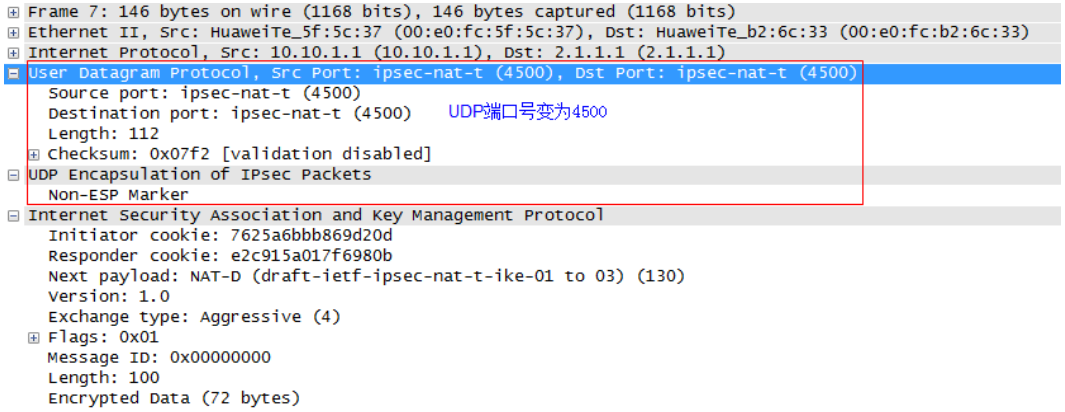
消息②：响应方在IKE消息中插入VID载荷表明自己支持NAT-T能力，同时插入了两个NAT-D载荷。第一个NAT-D载荷包含IKE对等体的IP地址和端口的Hash值，第二个NAT-D载荷包含本端的IP地址和端口的Hash值，接收方也计算这两个Hash值，两方计算的哪个Hash值不相等，表明哪个设备在NAT网关后面。

图 5-17 消息②



消息③：完成NAT-T检测和NAT网关探测后，如果发现NAT网关，则后续UDP报文端口号修改为4500。

图 5-18 消息③



当前UDP封装的是ISAKMP消息，此处增加了一个non-ESP marker（为4个值为0的字节），以示跟封装ESP报文有区别。

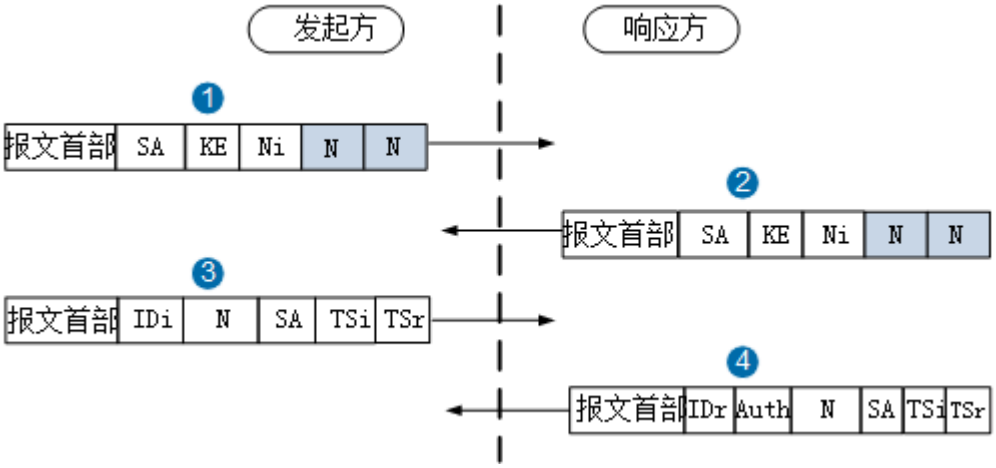
IKEv1阶段2的SA协商时，需确认是否使用NAT穿越以及NAT穿越的封装模式：UDP-Encapsulated-tunnel和UDP-Encapsulated-transport。确认后，后续传输的ESP报文将都采用UDP封装（AH协议不支持NAT穿越，故只能封装ESP报文）。UDP封装ESP报文时，没有non-ESP marker字段，该位置为SPI，为非0字节。

IKEv2 的 NAT 穿越协商

IKEv2的NAT穿越场景中，IKE协商的发起方和响应方在IKE_SA_INIT交换中增加两个N载荷（在Ni和Nr载荷之后），一个消息类型为NAT_DETECTION_SOURCE_IP，标识发起方的IP地址；另一个消息类型为NAT_DETECTION_DESTINATION_IP，标识响应方的IP地址。

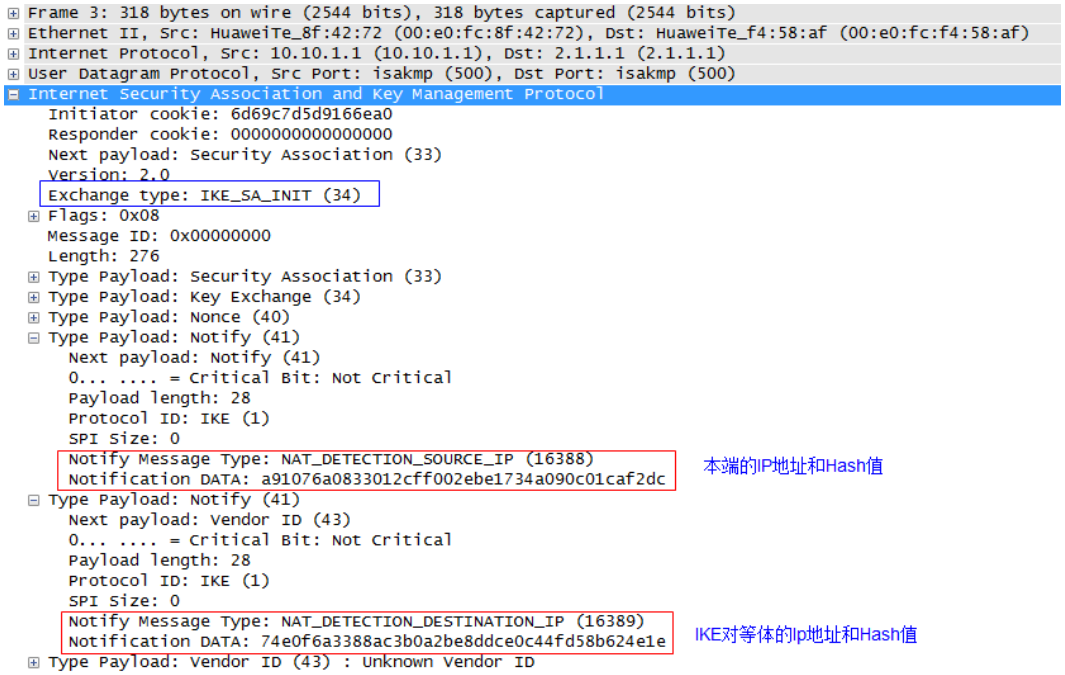
IKEv2的NAT穿越协商过程如图5-19所示。

图 5-19 IKEv2 的 NAT 穿越协商过程（预共享密钥认证）



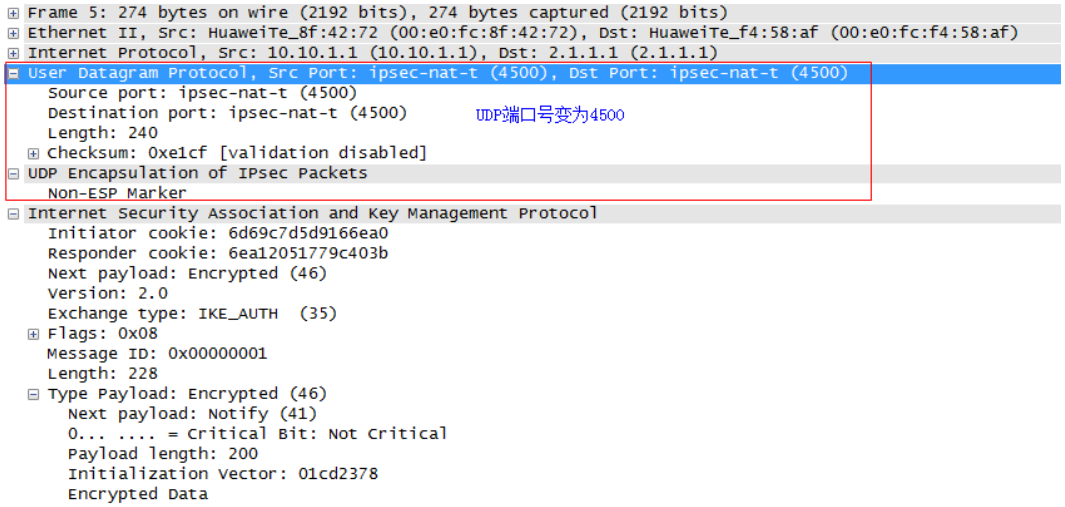
消息①、②：在IKE消息中插入两个N载荷，第一个N载荷包含本端的IP地址和端口的Hash值，第二个N载荷包含IKE对等体的IP地址和端口的Hash值，响应方也计算这两个Hash值，两方计算的哪个Hash值不相等，表明哪个设备在NAT网关后面。

图 5-20 消息①、②



消息③、④：完成IKE_SA_INIT后，如果发现NAT设备，则后续UDP报文端口号修改为4500。

图 5-21 消息③、④



总结

两端必须都开启NAT穿越功能，才能保证IKE协商成功。

IKE协商完成后，可以执行命令**display ike sa**，查看SA建立情况。当**Flag**参数为**RD**或**RD|ST**表示SA已建立成功。其中，**ST**表示本端是SA协商发起方。

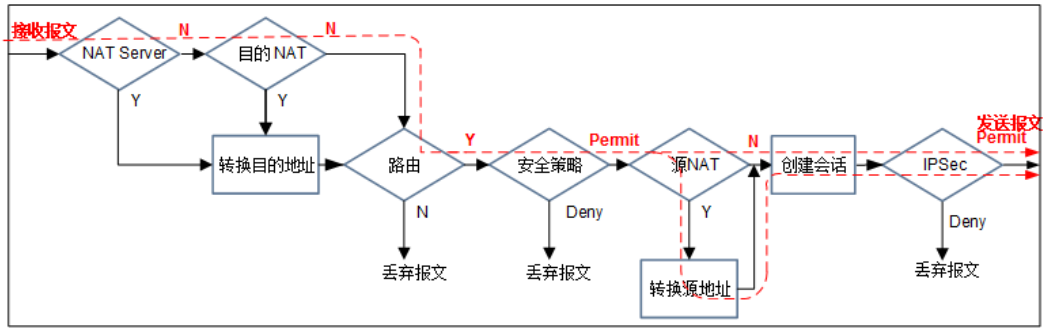
```
<Huawei> display ike sa
IKE SA information :
    Conn-ID      Peer                VPN    Flag(s)       Phase
-------------------------------------------------------------------------
    16           2.1.1.1:4500               RD|ST         v2:2
    14           2.1.1.1:4500               RD|ST         v2:1

 Number of IKE SA : 2
-------------------------------------------------------------------------
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE   NEG--NEGOTIATING
```

5.1.2 IPSec 隧道建立成功后业务异常故障分析

5.1.2.1 IPSec 报文转发流程

IPSec报文转发流程如图5-22所示。

图 5-22 IPSec 报文转发流程



Router处理流程中，IPSec的处理位于NAT、路由、安全策略之后，故应保证NAT策略对IPSec保护的报文不进行处理，IPSec保护的报文能够通过匹配路由和安全策略被送达应用了IPSec安全策略的接口。具体要求如下：

1. 到达Router的报文不能匹配目的NAT的策略，否则报文目的地址将被转换。
2. 路由表中必须有到达IKE对等体私网的路由（一般为缺省路由），路由的出接口为应用了IPSec策略的接口。若没有匹配的路由，报文将被丢弃；若匹配路由的出接口为其它接口，报文也将无法进入IPSec处理模块，以明文形式发送。
3. 进入IPSec模块的报文只有在匹配了**security acl**的情况下才能被保护，否则被丢弃。

说明

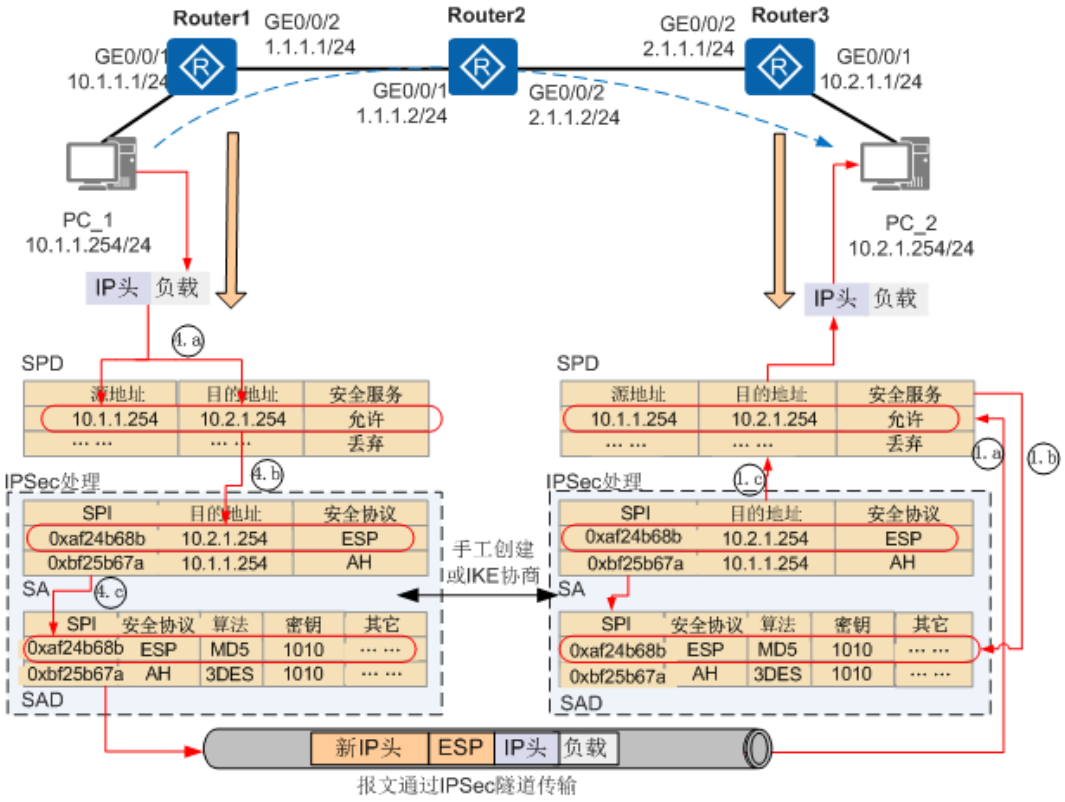
触发IKE协商的数据流也需要走以上流程，中间任何一个环节阻塞都将导致没有数据流触发IKE协商。

5.1.2.2 IPSec 工作原理

安全策略数据库SPD（Security Policy Database）是IPSec SA创建的前提，它定义哪些数据流受安全协议保护。安全关联数据库SADB（Security Associations Database）用于存放IPSec SA的所有属性参数。

下面以点到点VPN单向发送数据（采用隧道模式）为例，对IPSec的工作原理进行详细介绍。如图5-23所示，Router1为分支网关，用Router2模拟运营商设备，Router3为总部网关，PC1和PC2分别为分支和总部私有网络主机。在Router1和Router3上部署IPSec来保护PC1和PC2所在网段主机之间的通信。报文在Router1 GE0/0/2接口和Router3 GE0/0/2之间进行转发时进行IPSec加密保护。

图 5-23 IPSec VPN 工作原理



- Router1
  a. PC1向网关Router1发送IP报文（目的地址为PC2）。
  b. Router1收到源地址是PC1，目的地址是PC2的报文后，查目的地址到PC2路由进行转发。
  c. Router1查找到出接口为GE0/0/2，于是将报文转发到出接口。
  d. 报文转发到出接口后，由于出接口应用了IPSec策略，因此需要对通过的报文进行匹配，如果通过的报文特征符合IPSec定义要保护的数据流（通过ACL定义），则按照两端协商的IPSec进行报文封装。具体步骤如下所示：
     i. 查找SPD，根据报文的源、目的地址确定是否对报文进行IPSec处理。
        - 动作为“允许”的报文需要进行IPSec处理。
        - 动作为“丢弃”的报文不需要进行IPSec处理。

ii. 根据报文的目的地址查找SA。
- 若有相应的表项，则执行步骤C（手工方式下，配置完成后SA和SADB即已经生成）。
- 若没有相应表项，则发起IKE协商。协商成功后，双方设备各自生成SA和SAD。

iii. 根据SPI在SAD中找到相应IPSec SA，根据SA的各项参数对报文进行加密、Hash和封装。

e. 完成报文封装后查找路由，按照路由转发，此时出接口为GE0/0/2。

- Router2

  根据路由转发报文。

- Router3

a. Router3的GE0/0/2接收到报文后，发现目的地址是自己的IP地址，报文送给网络层处理判断报文是IPSec报文（IP协议号：ESP为50；AH为51），报文进入IPSec处理模块进行解密封装。具体步骤如下：

i. （可选）查找SPD，对IP报文（未加密的明文）进行IPSec前反查。

若需要加密的报文没有加密，则丢弃报文。

ii. 根据SPI和报文的目的地址、安全协议号查找SAD和SA，根据SA的各项参数对报文进行解封装、验证和解密。

iii. （可选）查找SPD，对解密后的IP报文进行IPSec后反查。

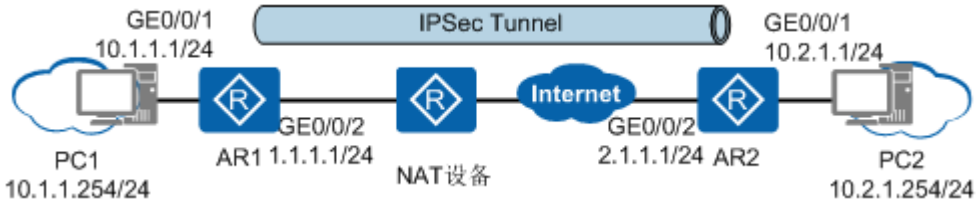
若不需要加密的报文进行了加密，则丢弃报文。

b. 报文解封装后，Router3查询目的地址，发现目的地址和本端出接口是一个网段，于是直接查询ARP表进行转发，出接口为GE0/0/1。

5.1.2.3 IPSec 业务质量差分析

如图5-24所示，Router之间IPSec隧道已建立成功。

图 5-24 点到点 IPSec 组网图



CPU 性能影响

- 由于报文分片消耗CPU资源导致IPSec业务质量下降
  - 考虑MTU值

    一条链路所能传输的最大报文长度被称为MTU（Maximum Transfer Unit），MTU大小与接口类型有关（例如以太网口缺省MTU为1500字节），链路MTU由这条链路上MTU最小的接口决定。当待发送的报文尺寸超过接口MTU时，设备会先对加密后的报文进行分片，然后再发送。接收端收到一个IP报文的所有分片后需要先进行重组，然后再解密。分片及重组都需要消耗CPU资源。

从IPSec报文的封装过程来看，IPSec对收到的原始IP报文再次封装，每次封装都会增加新的开销（每封装一层增加的开销与封装的协议有关，请参见**表5-5**）。假设IPSec处理流程中新增开销总计为80字节，大于1420字节的报文经IPSec封装后将超过1500字节，发送前都需要进行分片。当数据流中的报文大多数是超过1420字节的大包时，CPU资源消耗巨增，IPSec业务的访问速度和质量也会因此而大大下降。

表 5-5 协议开销字节列表

协议	增加的开销（字节）
ESP	缺省为56 ESP报文增加的开销跟使用的加密算法和是否使用验证算法有关
AH	24
GRE	24
NAT-T	8
L2TP	12
PPPoE	8
IPSec隧道模式	20
TCP	8

- 考虑TCP MSS值

  TCP MSS（Max Segment Size）指定了TCP最大报文段长度，如果MSS值加上各种开销的报文总长度（MSS+TCP报文头+IP报文头+IPSec报文头）大于链路的MTU值，则数据报文会被分片发送。分片的过程会消耗更多的CPU资源，分片报文的加密解密同样会消耗传输链路中设备的CPU资源。当CPU资源消耗过多，就会造成数据报文的丢失。

  同时，对于某些高层应用（例如HTTP等应用层协议等）会将IP报文的DF（Don't Fragment）标记位置为有效，以防止TCP报文分片。如果DF标记位被置为有效，而接口MTU小于MSS的值，此时设备会因为不能强制分片TCP报文而将报文丢弃。

- 由于其它特性消耗CPU资源导致IPSec业务质量下降

  IPSec、DPI、UTM、攻击防范等特性都非常消耗CPU资源，故当同时开启IPSec、DPI、UTM等特性时可能会出现IPSec业务访问速度明显变慢的情况，数据流量越大问题越明显。

网络质量影响

IPSec是构建于Internet之上的虚拟网络，所以Internet的传输质量直接影响IPSec业务质量。可以通过旁路VPN定界Internet传输质量问题，若属于Internet质量问题请运营商解决即可。Internet可能存在如下问题：

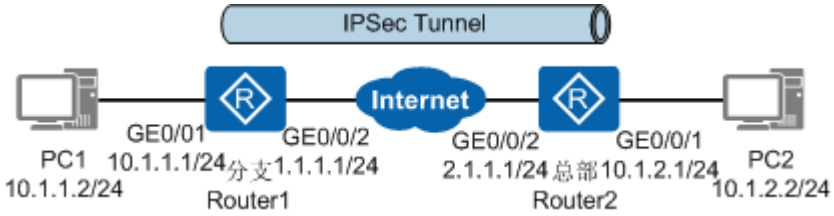
- Internet网络拥塞导致丢包或不通。网络丢包对语音、视频业务质量影响较大，Web浏览业务、文件传输业务会明显变慢；网络不通会直接导致业务不通。
- 运营商对某些类型的报文进行了限制，如UDP报文，会导致NAT穿越场景下IKE协商不通。

- 运营商对IPSec业务使用的端口进行了限制，如500、4500。限制500端口会导致IKE协商不通，限制4500端口会导致NAT穿越场景下IKE协商不通。

5.2 Debugging 信息说明

通过Debugging信息介绍IKE协商报文交互的过程，IPSec组网如图5-25所示。其中Router1为IKE协商发起方，Router2为IKE协商响应方。

图 5-25 IPSec 组网图



IKEv1 阶段 1 协商过程

主模式

IKEv1阶段1协商过程中，主模式包含三次双向交换，用到了六条信息。

1. 发起方：发送封装有IKE安全提议的SA载荷给响应方进行安全提议协商。

   ```
   Sep 28 2017 21:05:59.550.3+08:00 Huawei IKE/7/IKE_Debug:
   IKE_PACKET 17:4686 IKE Packet Contents sent to 2.1.1.1 for message type Send_SA : f317d868
   c8f3069a 00000000 00000000 01100200 00000000 000000d0 0d00003c 00000001 00000001
   00000030 01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e
   800b0001 000c0004 00015180 0d000014 4a131c81 07035845 5c5728f2 0e95452f 0d000014
   90cb8091 3ebb696e 086381b5 ec427b1f 0d000014 4485152d 18b6bbcd 0be8a846 9579ddcc
   0d000014 12f5f28c 457168a9 702d9fe2 74cc0100 0d000014 afcad713 68a1f1c9 6b8696fc 77570100
   00000014 48554157 45492d49 4b457631 44534350
   ```

   响应方：接收到发起方发送的SA载荷，并解析IKE安全提议。

   ```
   Sep 28 2017 21:23:39.960.14+00:00 Huawei IKE/7/IKE_Debug:
   IKE_PACKET 17:4930 IKE Packet Contents sent to 1.1.1.1 for message type Send_SA : f317d868
   c8f3069a 7396dfa0 3f8f51ac 01100200 00000000 000000a8 0d00003c 00000001 00000001 00000030
   01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001
   000c0004 00015180 0d000014 4a131c81 07035845 5c5728f2 0e95452f 0d000014 12f5f28c 457168a9
   702d9fe2 74cc0100 0d000014 afcad713 68a1f1c9 6b8696fc 77570100 00000014 48554157 45492d49
   4b457631 44534350
   IKE_INFO 17:3513 Message from peer 1.1.1.1: validate payload SA
   IKE_INFO 17:813 Message from peer 1.1.1.1: Parsing payload PROPOSAL
   IKE_INFO 17:813 Message from peer 1.1.1.1: Parsing payload TRANSFORM
   IKE_INFO 2:2924   Attribute ENCRYPTION_ALGORITHM value AES_CBC   //加密算法
   IKE_INFO 2:2924   Attribute KEY_LENGTH value 256   //加密算法长度
   IKE_INFO 2:2924   Attribute HASH_ALGORITHM value SHA2-256   //认证算法
   IKE_INFO 2:2924   Attribute AUTHENTICATION_METHOD value PRE_SHARED   //认证方法
   IKE_INFO 2:2924   Attribute GROUP_DESCRIPTION value MODP_1024   //DH密钥交换参数
   IKE_INFO 2:2924   Attribute LIFE_TYPE value SECONDS
   IKE_INFO 2:2924   Attribute LIFE_DURATION value 86400   //IKE SA的生存周期
   ```

2. 响应方：查找最先匹配的IKE安全提议，发送一个SA载荷，表明接受协商的IKE安全提议。

   ```
   Sep 28 2017 21:23:39.960.14+00:00 Huawei IKE/7/IKE_Debug:
   IKE_PACKET 17:4930 IKE Packet Contents sent to 1.1.1.1 for message type Send_SA : f317d868
   c8f3069a 7396dfa0 3f8f51ac 01100200 00000000 000000a8 0d00003c 00000001 00000001 00000030
   01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001
   ```

000c0004 00015180 0d000014 4a131c81 07035845 5c5728f2 0e95452f 0d000014 12f5f28c 457168a9 702d9fe2 74cc0100 0d000014 afcad713 68a1f1c9 6b8696fc 77570100 00000014 48554157 45492d49 4b457631 44534350

发起方：接收到响应方发送的确认SA载荷。

Sep 28 2017 21:05:59.640.3+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4508 **IKE Packet Contents received from 2.1.1.1 for message type Recv_SA** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 01100200 00000000 000000a8 0d00003c 00000001 00000001 00000030 01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001 000c0004 00015180 0d000014 4a131c81 07035845 5c5728f2 0e95452f 0d000014 12f5f28c 457168a9 702d9fe2 74cc0100 0d000014 afcad713 68a1f1c9 6b8696fc 77570100 00000014 48554157 45492d49 4b457631 44534350

3. 发起方：发送封装有密钥生成信息的KE_NONCE载荷给响应方，用来交换DH公开值和临时随机数。

Sep 28 2017 21:05:59.640.17+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4686 **IKE Packet Contents sent to 2.1.1.1 for message type Send_KE_NONCE** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 04100200 00000000 0000017c 0a000104 df472637 7fa66305 d2384b82 b84d4353 68def6ae c4268e3f 67c14e13 806ae6bc 5cc688d4 41a8432b dba680c6 ebda9743 122c7455 f23506e0 48f48f12 c47ec9c7 ded96633 9243bf39 cfc0d4d1 17e90213 6a5f63b8 8515d842 a0700a2e bdb99617 7415fecb c97729df 1da1f800 c5eb8a26 69ac9eb6 8f41b6ee ec7edeed ecc41809 472abea5 77535f28 c00a0b10 ad762132 f46b71f2 ac90f9c4 acb41a85 a7234845 03f436e6 504deb10 61563be5 7272b2d5 9114401a 423b18a4 f0d21ecd bbafc3a1 f28fe579 9341b6ac b21ce40a 97e546c5 213947a6 85d7b0b0 4f1f417b 720277f4 823649ea 419f2e30 ca64b8ac 480f8793 9a145154 bfeba9ac bc9eeb68 752bb8c8 14000014 ab3c6161 89aada4f ddd6d33d 36bdb605 14000024 45adbbf1 55321d99 5b9c9aaf ada3c518 eed6994c 3f45c4d2 696207

响应方：接收到发起方发送的KE_NONCE载荷。

Sep 28 2017 21:23:40.90.12+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4752 **IKE Packet Contents received from 1.1.1.1 for message type Recv_KE_NONCE** : f317d868 c8f3069a 7396dfa0 3f8f51ac 04100200 00000000 0000017c 0a000104 df472637 7fa66305 d2384b82 b84d4353 68def6ae c4268e3f 67c14e13 806ae6bc 5cc688d4 41a8432b dba680c6 ebda9743 122c7455 f23506e0 48f48f12 c47ec9c7 ded96633 9243bf39 cfc0d4d1 17e90213 6a5f63b8 8515d842 a0700a2e bdb99617 7415fecb c97729df 1da1f800 c5eb8a26 69ac9eb6 8f41b6ee ec7edeed ecc41809 472abea5 77535f28 c00a0b10 ad762132 f46b71f2 ac90f9c4 acb41a85 a7234845 03f436e6 504deb10 61563be5 7272b2d5 9114401a 423b18a4 f0d21ecd bbafc3a1 f28fe579 9341b6ac b21ce40a 97e546c5 213947a6 85d7b0b0 4f1f417b 720277f4 823649ea 419f2e30 ca64b8ac 480f8793 9a145154 bfeba9ac bc9eeb68 752bb8c8 14000014 ab3c6161 89aada4f ddd6d33d 36bdb605 14000024 45adbbf1 55321d99 5b9c9aaf ada3c518 eed6994c 3f45c4d2

4. 响应方：发送封装有密钥生成信息的KE_NONCE载荷给发起方，用来交换DH公开值和临时随机数。

Sep 28 2017 21:23:40.130.5+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4930 **IKE Packet Contents sent to 1.1.1.1 for message type Send_KE_NONCE** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 04100200 00000000 0000017c 0a000104 7e6d6a34 5c2d75ac 99191319 b70fa1f5 1ef90be5 dd9ce7a3 72212d62 3b2c72f2 63eb8814 d8cbc79d f36f7eca b2a48213 23a1fdd0 88f8d9d9 7ce43440 a575a8fa b7f53fb5 3eaaea9f 697a46c7 c17b8485 862b8d10 5af8408c 4f956aff a9aa2ca7 97dc36ae 8531c1f6 0ce3bc6b b512598b 23310897 c2e7c175 5389cd01 4825f232 5eac6d43 2a0cbd0d eae4dde3 996bed59 d11e8c0c 31d5324b e832228d 7d3df4fa e117a789 3849c861 681ec20e 627dbbdc e6b74a8b 82f19bd8 22be4e35 8cbe07af 62b3bbc7 10c9ab38 5a6d6203 61586945 c6b436d6 d9c786cc e54a4dc4 bf37ef88 d77786a8 af8986d2 25434234 aca11cad 8822f627 ae0b3154 1ba2939b dce25b94 14000014 ab4da180 3e475ced 49674378 13c48755 14000024 76104f49 2e45250e cd0cb85f f02a5cc9 f76f4563 df2874b2 45411b

发起方：接收到响应方发送的KE_NONCE载荷。

Sep 28 2017 21:05:59.800.6+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4508 **IKE Packet Contents received from 2.1.1.1 for message type Recv_KE_NONCE** : f317d868 c8f3069a 7396dfa0 3f8f51ac 04100200 00000000 0000017c 0a000104 7e6d6a34 5c2d75ac 99191319 b70fa1f5 1ef90be5 dd9ce7a3 72212d62 3b2c72f2 63eb8814 d8cbc79d f36f7eca b2a48213 23a1fdd0 88f8d9d9 7ce43440 a575a8fa b7f53fb5 3eaaea9f 697a46c7 c17b8485 862b8d10 5af8408c 4f956aff a9aa2ca7 97dc36ae 8531c1f6 0ce3bc6b b512598b 23310897 c2e7c175 5389cd01 4825f232 5eac6d43 2a0cbd0d eae4dde3 996bed59 d11e8c0c 31d5324b e832228d 7d3df4fa e117a789 3849c861 681ec20e 627dbbdc e6b74a8b 82f19bd8 22be4e35 8cbe07af 62b3bbc7 10c9ab38 5a6d6203 61586945 c6b436d6 d9c786cc e54a4dc4 bf37ef88 d77786a8 af8986d2 25434234 aca11cad 8822f627 ae0b3154 1ba2939b dce25b94 14000014 ab4da180 3e475ced 49674378 13c48755 14000024 76104f49 2e45250e cd0cb85f f02a5cc9 f76f4563 df2874b2

5. 发起方：发送封装有身份ID和验证数据Hash信息的ID_AUTH载荷给响应方。

Sep 28 2017 21:05:59.830.6+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4686 **IKE Packet Contents sent to 2.1.1.1 for message type Send_ID_AUTH** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 05100200 00000000 0000004c 0800000c 01000000 01010101
00000024 3b69c54a d8478f81 bd61cf3d 9ee8bf59 32846302 a306e6e2 e3645724 9db520af

响应方：接收到发起方发送的ID_AUTH载荷。

Sep 28 2017 21:23:40.210.9+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4752 **IKE Packet Contents received from 1.1.1.1 for message type Recv_ID_AUTH** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 05100201 00000000 0000004c 0800000c 01000000 01010101
00000024 3b69c54a d8478f81 bd61cf3d 9ee8bf59 32846302 a306e6e2 e3645724 9db520af

6. 响应方：发送封装有身份ID和验证数据Hash信息的ID_AUTH载荷给发起方。

Sep 28 2017 21:23:40.220.12+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4930 **IKE Packet Contents sent to 1.1.1.1 for message type Send_ID_AUTH** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 05100200 00000000 0000004c 0800000c 01000000 02010101
00000024 ec4df8c8 6b4ec863 36b71e01 57857ef6 20ea5aec 3713bc3e 79867e66 3b489fbe

发起方：接收到响应方发送的ID_AUTH载荷。

Sep 28 2017 21:05:59.890.15+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4508 **IKE Packet Contents received from 2.1.1.1 for message type Recv_ID_AUTH** :
f317d868 c8f3069a 7396dfa0 3f8f51ac 05100201 00000000 0000004c 0800000c 01000000 02010101
00000024 ec4df8c8 6b4ec863 36b71e01 57857ef6 20ea5aec 3713bc3e 79867e66 3b489fbe

野蛮模式

IKEv1阶段1协商过程中，野蛮模式只用到三条信息。

1. 发起方：发送封装有IKE安全提议、密钥生成信息和身份信息的SA_KE_NONCE_ID_VID载荷给响应方。

Sep 28 2017 21:21:03.960.11+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4686 **IKE Packet Contents sent to 2.1.1.1 for message type Send_SA_KE_NONCE_ID_VID** : a1588ac6 a6a062d4 00000000 00000000 01100400 00000000 000001f4 0400003c 00000001 00000001 00000030 01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001 000c0004 00015180 0a000104 e932c0c6 ad23a42e 52150f0e ce602358 12b88390 ea4ec8d3 3b53063b c1e87f8c 1fa61767 f6b4e370 cac38dd7 0515a745 1d01dd83 6ba29a3a 3a9bdc2c 3b061c58 14ce8cab ae289fb4 70f10c3d 7f6d2b13 1e76eeeb c9110651 d6445cd4 1f48d7b4 84112da5 42cb440d dce58d57 6bc2030a 45fa4dd3 c1ec0853 9b66b104 0a87eaea b81aea68 d0e8ff2e 8634a006 2beba703 4259d6ec f9b878aa 6349e8fa e8dc81ee f3b1f752 0fb99206 be7736d3 45c98c7c 2a092112 73efbc93 b7f778b6 1f07f98c 58261a12 99dae705 0374926a 0a3ae551 ea6435fa 04fd2a9a 0a7626a0 e1833473 8e7c1cdf 53f8c1b0 300adde1 c3e5780c 083e6

响应方：接收到发起方发送的SA_KE_NONCE_ID_VID载荷，并解析IKE安全提议。

Sep 28 2017 21:38:44.370.5+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4752 **IKE Packet Contents received from 1.1.1.1 for message type Recv_SA_KE_NONCE_ID_VID** : a1588ac6 a6a062d4 00000000 00000000 01100400 00000000 000001f4 0400003c 00000001 00000001 00000030 01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001 000c0004 00015180 0a000104 e932c0c6 ad23a42e 52150f0e ce602358 12b88390 ea4ec8d3 3b53063b c1e87f8c 1fa61767 f6b4e370 cac38dd7 0515a745 1d01dd83 6ba29a3a 3a9bdc2c 3b061c58 14ce8cab ae289fb4 70f10c3d 7f6d2b13 1e76eeeb c9110651 d6445cd4 1f48d7b4 84112da5 42cb440d dce58d57 6bc2030a 45fa4dd3 c1ec0853 9b66b104 0a87eaea b81aea68 d0e8ff2e 8634a006 2beba703 4259d6ec f9b878aa 6349e8fa e8dc81ee f3b1f752 0fb99206 be7736d3 45c98c7c 2a092112 73efbc93 b7f778b6 1f07f98c 58261a12 99dae705 0374926a 0a3ae551 ea6435fa 04fd2a9a 0a7626a0 e1833473 8e7c1cdf 53f8c1b0 300adde1 c3e5780c
IKE_INFO 17:3513 Message from peer 1.1.1.1: validate payload SA
IKE_INFO 17:813 Message from peer 1.1.1.1: Parsing payload PROPOSAL
IKE_INFO 17:813 Message from peer 1.1.1.1: Parsing payload TRANSFORM
IKE_INFO 2:2924 Attribute ENCRYPTION_ALGORITHM value AES_CBC //加密算法
IKE_INFO 2:2924 Attribute KEY_LENGTH value 256 //加密算法长度
IKE_INFO 2:2924 Attribute HASH_ALGORITHM value SHA2-256 //认证算法
IKE_INFO 2:2924 Attribute AUTHENTICATION_METHOD value PRE_SHARED //认证方法
IKE_INFO 2:2924 Attribute GROUP_DESCRIPTION value MODP_1024 //DH密钥交换参数
IKE_INFO 2:2924 Attribute LIFE_TYPE value SECONDS
IKE_INFO 2:2924 Attribute LIFE_DURATION value 86400 //IKE SA的生存周期

2. 响应方：查找最先匹配的IKE安全提议，发送封装有IKE安全提议、密钥生成信息、身份信息和验证数据的SA_KE_NONCE_ID_VID_NATD_AUTH载荷给发起方。

Sep 28 2017 21:38:44.420.6+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4930 **IKE Packet Contents sent to 1.1.1.1 for message type**

Send_SA_KE_NONCE_ID_VID_NATD_AUTH : a1588ac6 a6a062d4 60fd9a0c d0d75e72 01100400 00000000 00000238 0400003c 00000001 00000001 00000030 01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001 000c0004 00015180 0a000104 a0bd8569 a2ec9c8e 66509d14 11cdf928 a165526e 6866be8e 846becb3 fe0e9aec 0eef08e4 4b3209b3 45e38d39 5e3c84b5 50025fa9 0352a987 f4b26ec5 49981fcd d07040cd 031f1829 460eaa77 8e3e69d6 b9dba239 889e2708 96f0473f de5867fe 6f5ca16b 00ab7133 4c864f03 aab59f1c 0e3f369c 78f73985 c9862cea 0dda80d7 21451b5b 7cbea87e 7585dd89 2f6795e7 2c06cc0a a4846da0 ced85686 75c51116 173fb7d8 8fe8f460 e66bedcc 67afd20f 90b15ba2 557f9fb6 c0929fc6 d8618b64 054bcdc9 b3e3762e 0d130bcb d1977450 3d64bdb9 cb2587b5 f87a97dc 561e78e4 876e0d45 b68a8ca6 0b3ef91c ac3d

发起方：接收到响应方发送的SA_KE_NONCE_ID_VID_NATD_AUTH载荷。

Sep 28 2017 21:21:04.100.10+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4508 **IKE Packet Contents received from 2.1.1.1 for message type Recv_SA_KE_NONCE_ID_VID_NATD_AUTH** : a1588ac6 a6a062d4 60fd9a0c d0d75e72 01100400 00000000 00000238 0400003c 00000001 00000001 00000030 01010001 00000028 00010000 80010007 800e0100 80020004 80030001 8004000e 800b0001 000c0004 00015180 0a000104 a0bd8569 a2ec9c8e 66509d14 11cdf928 a165526e 6866be8e 846becb3 fe0e9aec 0eef08e4 4b3209b3 45e38d39 5e3c84b5 50025fa9 0352a987 f4b26ec5 49981fcd d07040cd 031f1829 460eaa77 8e3e69d6 b9dba239 889e2708 96f0473f de5867fe 6f5ca16b 00ab7133 4c864f03 aab59f1c 0e3f369c 78f73985 c9862cea 0dda80d7 21451b5b 7cbea87e 7585dd89 2f6795e7 2c06cc0a a4846da0 ced85686 75c51116 173fb7d8 8fe8f460 e66bedcc 67afd20f 90b15ba2 557f9fb6 c0929fc6 d8618b64 054bcdc9 b3e3762e 0d130bcb d1977450 3d64bdb9 cb2587b5 f87a97dc 561e78e4 876e0d45 b68a8ca6 0b3ef91

3. 发起方：发送封装有验证数据的NATD_AUTH载荷给响应方。

Sep 28 2017 21:21:04.140.3+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4686 **IKE Packet Contents sent to 2.1.1.1 for message type Send_NATD_AUTH** : a1588ac6 a6a062d4 60fd9a0c d0d75e72 14100400 00000000 00000088 14000024 f4cc10b9 7b1188c7 c16262a0 a09d5ffb 081754a1 35112614 588dbea3 65fa8099 08000024 877f64e2 d1475aab 08081f20 0d4ba079 cdb78f79 0a70b6b8 9385f12b 9de1c9ab 00000024 f74224a0 14d354e2 6a999f6b 626b158c 71d23e63 80cc8463 cba6eeae 51638100

响应方：接收到发起方发送的NATD_AUTH载荷。

Sep 28 2017 21:38:44.540.13+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4752 **IKE Packet Contents received from 1.1.1.1 for message type Responder_recv_NATD_AUTH** : a1588ac6 a6a062d4 60fd9a0c d0d75e72 14100401 00000000 00000088 14000024 f4cc10b9 7b1188c7 c16262a0 a09d5ffb 081754a1 35112614 588dbea3 65fa8099 08000024 877f64e2 d1475aab 08081f20 0d4ba079 cdb78f79 0a70b6b8 9385f12b 9de1c9ab 00000024 f74224a0 14d354e2 6a999f6b 626b158c 71d23e63 80cc8463 cba6eeae 51638100 00000000

IKEv1 阶段 2 协商过程

IKEv1阶段2协商过程中，只用到三条信息。

1. 发起方：发送封装有IPSec安全提议、身份和验证数据的HASH_SA_NONCE载荷给响应方。

Sep 28 2017 21:21:04.160.5+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4686 **IKE Packet Contents sent to 2.1.1.1 for message type Send_HASH_SA_NONCE** : a1588ac6 a6a062d4 60fd9a0c d0d75e72 08102000 2e398765 000000b8 01000024 a385a80b ae4d3d24 3e63ad1d c749c575 ec522e64 ed8d91ea 5fd1c0d3 52f00bd9 0a000044 00000001 00000001 00000038 01030401 00d7609a 0000002c 010c0000 80010001 00020004 00000e10 80010002 00020004 001c2000 80040001 80050005 80060080 05000014 65426071 2d47e2a9 045c83bd 21534540 05000010 04000000 0a010100 ffffff00 00000010 04000000 0a010200 ffffff00

响应方：接收到发起方发送的HASH_SA_NONCE载荷，并解析IPSec安全提议。

Sep 28 2017 21:38:44.600.3+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4752 **IKE Packet Contents received from 1.1.1.1 for message type Recv_HASH_SA_NONCE** : a1588ac6 a6a062d4 60fd9a0c d0d75e72 08102001 2e398765 000000b8 01000024 a385a80b ae4d3d24 3e63ad1d c749c575 ec522e64 ed8d91ea 5fd1c0d3 52f00bd9 0a000044 00000001 00000001 00000038 01030401 00d7609a 0000002c 010c0000 80010001 00020004 00000e10 80010002 00020004 001c2000 80040001 80050005 80060080 05000014 65426071 2d47e2a9 045c83bd 21534540 05000010 04000000 0a010100 ffffff00 00000010 04000000 0a010200 ffffff00 00000000
IKE_INFO 17:2267
Proposal No: 1
Protocol ID: IPSEC_ESP //安全协议类型
IKE_INFO 2:1997 ENCRYPTION ALGORITHM: AES //加密算法

```
IKE_INFO 2:2924   Attribute SA_LIFE_TYPE value SECONDS
IKE_INFO 2:2924   Attribute SA_LIFE_DURATION value 3600   //以时间为基准的IPSec SA的生存周期
IKE_INFO 2:2924   Attribute SA_LIFE_TYPE value KILOBYTES
IKE_INFO 2:2924   Attribute SA_LIFE_DURATION value 1843200   //以流量为基准的IPSec SA的生存周期
IKE_INFO 2:2924   Attribute ENCAPSULATION_MODE value TUNNEL   //封装模式
IKE_INFO 2:2924   Attribute AUTHENTICATION_ALGORITHM value SHA_256  //认证算法
IKE_INFO 2:2924   Attribute KEY_LENGTH value 256   //加密算法长度
```

2. 响应方：查找最先匹配的IPSec安全提议，发送封装有IPSec安全提议、身份信息和验证数据的HASH_SA_NONCE载荷给发起方。

```
Sep 28 2017 21:38:44.630.10+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4930 IKE Packet Contents sent to 1.1.1.1 for message type
Send_HASH_SA_NONCE : a1588ac6 a6a062d4 60fd9a0c d0d75e72 08102000 2e398765 000000b8
01000024 4ae6231b 8ecc7d32 6b652050 1287c765 9ad89e4a 31a9c0bc e0047c96 b7d0bf7f 0a000044
00000001 00000001 00000038 01030401 00cd88b8 0000002c 010c0000 80010001 00020004
00000e10 80010002 00020004 001c2000 80040001 80050005 80060080 05000014 89e510df
9582036a db91abe2 1dd56bca 05000010 04000000 0a010100 ffffff00 00000010 04000000 0a010200
ffffff00
```

发起方：接收到响应方发送的HASH_SA_NONCE载荷。

```
Sep 28 2017 21:21:04.310.2+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4508 IKE Packet Contents received from 2.1.1.1 for message type
Recv_HASH_SA_NONCE : a1588ac6 a6a062d4 60fd9a0c d0d75e72 08102001 2e398765 000000b8
01000024 4ae6231b 8ecc7d32 6b652050 1287c765 9ad89e4a 31a9c0bc e0047c96 b7d0bf7f 0a000044
00000001 00000001 00000038 01030401 00cd88b8 0000002c 010c0000 80010001 00020004
00000e10 80010002 00020004 001c2000 80040001 80050005 80060080 05000014 89e510df
9582036a db91abe2 1dd56bca 05000010 04000000 0a010100 ffffff00 00000010 04000000 0a010200
ffffff00 00000000
```

3. 发起方：发送封装有验证数据的HASH载荷给响应方。

```
Sep 28 2017 21:21:04.330.5+08:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4686 IKE Packet Contents sent to 2.1.1.1 for message type Send_HASH : a1588ac6
a6a062d4 60fd9a0c d0d75e72 08102000 2e398765 00000040 00000024 fa2b29f7 22f0d27f 25e9e1e1
9c46fbdb d57ebeff 53d7317e 3baaaeea 047189e2
```

响应方：接收到发起方发送的HASH载荷。

```
Sep 28 2017 21:38:44.720.11+00:00 Huawei IKE/7/IKE_Debug:
IKE_PACKET 17:4752 IKE Packet Contents received from 1.1.1.1 for message type Recv_HASH :
a1588ac6 a6a062d4 60fd9a0c d0d75e72 08102001 2e398765 00000040 00000024 fa2b29f7 22f0d27f
25e9e1e1 9c46fbdb d57ebeff 53d7317e 3baaaeea 047189e2 00000000 00000000 00000000
```

IKEv2 阶段过程

采用IKEv2协商安全联盟比IKEv1协商过程要简化的多。要建立一对IPSec SA，IKEv1需要经历两个阶段：“主模式＋快速模式”或者“野蛮模式＋快速模式”，前者至少需要交换9条消息，后者也至少需要6条消息。而IKEv2正常情况使用2次交换共4条消息就可以完成一对IPSec SA的建立，如果要求建立的IPSec SA大于一对时，每一对IPSec SA只需额外增加1次创建子SA交换，也就是2条消息就可以完成。

1. 发起方：发送封装有IKE安全提议、密钥生成信息和验证数据的SA_INIT载荷给响应方。

```
Sep 28 2017 21:25:09.790.14+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6660 IKEv2 Exch Type: SA_INIT

Sep 28 2017 21:25:09.800.2+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6570 Sent Msg: SA | KE | NONCE | NOTIFY | NOTIFY | V_ID | V_ID |
```

响应方：接收到发起方发送的SA_INIT载荷，并解析IKE安全提议。

```
Sep 28 2017 21:42:50.180.10+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6733 IKEv2 Exch Type: SA_INIT

Sep 28 2017 21:42:50.180.1+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6636 Recv Msg: SA | KE | NONCE | NOTIFY | NOTIFY | V_ID | V_ID |
IKE_INFO 47:2699 Number of proposal : 1
IKE_INFO 47:2868
```



```
 Proposal No 1:
 Protocol ID: ISAKMP
IKE_INFO 47:2521 ENCRYPTION ALGORITHM: AES_256   //加密算法
IKE_INFO 47:2274 INTEGRITY ALGORITHM: SHA_256   //加密算法
IKE_INFO 47:2243 PRF ALGORITHM: SHA2_256   //伪随机数产生函数的算法
IKE_INFO 47:2308 GROUP_TYPE: MODP_1024   //DH密钥交换参数
```

2. 响应方：查找最先匹配的IKE安全提议，发送封装有IKE安全提议、身份信息和验证数据的SA_INIT载荷给发起方。

```
Sep 28 2017 21:42:50.190.9+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6774 IKEv2 Exch Type: SA_INIT

Sep 28 2017 21:42:50.190.11+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6684 Sent Msg: SA | KE | NONCE | NOTIFY | NOTIFY | V_ID | V_ID |
```

发起方：接收到响应方发送的SA_INITE载荷。

```
Sep 28 2017 21:25:09.870.13+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6619 IKEv2 Exch Type: SA_INIT

Sep 28 2017 21:25:09.870.14+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6522 Recv Msg: SA | KE | NONCE | NOTIFY | NOTIFY | V_ID | V_ID |
```

3. 发起方：发送封装有IPSec安全提议、身份信息和验证数据的IKE_AUTH载荷给响应方。

```
Sep 28 2017 21:25:09.920.5+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6660 IKEv2 Exch Type: IKE_AUTH

Sep 28 2017 21:25:09.920.7+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6570 Sent Msg: NOTIFY | NOTIFY | ID_I | AUTH | SA | TS_I | TS_R |
```

响应方：接收到发起方发送的IKE_AUTH，并解析IPSec安全提议。

```
Sep 28 2017 21:42:50.330.1+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6733 IKEv2 Exch Type: IKE_AUTH

Sep 28 2017 21:42:50.330.2+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6636 Recv Msg: NOTIFY | NOTIFY | ID_I | AUTH | SA | TS_I | TS_R |
IKE_INFO 47:2699 Number of proposal : 1
IKE_INFO 47:2868
 Proposal No 1:
 Protocol ID: IPSEC_ESP   //安全协议类型
IKE_INFO 47:2521 ENCRYPTION ALGORITHM: AES_256   //加密算法
IKE_INFO 47:2282 AUTHENTICATION ALGORITHM: SHA_256   //认证算法
```

4. 响应方：查找最先匹配的IPSec安全提议，发送封装有IPSec安全提议、身份信息和验证数据的IKE_AUTH载荷给发起方。

```
Sep 28 2017 21:42:50.360.9+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6774 IKEv2 Exch Type: IKE_AUTH

Sep 28 2017 21:42:50.360.11+00:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6684 Sent Msg: NOTIFY | NOTIFY | ID_R | AUTH | SA | TS_I | TS_R |
```

发起方：接收到响应方发送的IKE_AUTH载荷。

```
Sep 28 2017 21:25:10.50.10+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6619 IKEv2 Exch Type: IKE_AUTH

Sep 28 2017 21:25:10.50.11+08:00 Huawei IKE/7/IKE_Debug:
IKE_INFO 47:6522 Recv Msg: NOTIFY | NOTIFY | ID_R | AUTH | SA | TS_I | TS_R |
```

常见故障类 Debugging 信息及处理建议

常见故障类Debugging信息及处理建议如表5-6所示。

表 5-6 常见故障类 Debugging 信息

Debugging信息	描述	处理建议
Message from peer *peer-ip*: Got NOTIFY of type NO_PROPOSAL_CHOSEN	来自对等体的消息：获得类型为NO_PROPOSAL_CHOSEN的通知。 *peer-ip*指IKE对等体IP地址。	两端的IKE安全提议不一致，请排查。
Message from peer *peer-ip*: Got NOTIFY of type PAYLOAD_MALFORMED	来自对等体的消息：获得类型为PAYLOAD_MALFORME的通知。 *peer-ip*指IKE对等体IP地址。	两端的预共享密钥不一致，请排查。
Message from peer *peer-ip*: Invalid Next Payload of Type 60 in Payload Type 5	来自对等体的消息：有效载 荷类型5中的类型60的下一个有效载荷无效。 *peer-ip*指IKE对等体IP地址。	两端的预共享密钥不一致，请排查。
Message from peer *peer-ip*: dropping Message due to notification type INVALID_PAYLOAD_TYPE	来自对等体的消息：由于通知类型为INVALID_PAYLOAD_TYPE而丢弃消息。 *peer-ip*指IKE对等体IP地址。	两端的预共享密钥不一致，请排查。
Phase 1 Exchange: ike peer configuration not found for peer "*peer-ip*"	阶段1交换：对等体配置未找到对等体*peer-ip*。 *peer-ip*指IKE对等体IP地址。	本端的remote-address配置错误，请排查。
ERROR - Received remote-name(*remote-name*) does not match with peer remote-name(*remote-name*)	接收到的remote-name与peer remote-name不匹配。 *remote-name*：对端名称。	本端remote-id与对端名称不一致，请排查。

Debugging信息	描述	处理建议
Message from peer *peer-ip*: Got NOTIFY of type INVALID_ID_INFORMATION	来自对等体的消息：获得类型为INVALID_ID_INFORMATION的通知。 *peer-ip*指IKE对等体IP地址。	两端的ACL规则不匹配，请排查。
Message from peer *peer-ip*: dropping Message due to notification type NO_PROPOSAL_CHOSEN	来自对等体的消息：由于通知类型为NO_PROPOSAL_CHOSEN而丢弃消息。 *peer-ip*指IKE对等体IP地址。	两端的IPSec安全提议或PFS算法不一致，请排查。
Authentication failed for the peer *peer-ip*	对等体认证失败。 *peer-ip*指IKE对等体IP地址。	两端的预共享密钥不一致，请排查。
Unable to find IPSEC Policy for peer *peer-ip*	无法为对等体找到IPSec策略。 *peer-ip*指IKE对等体IP地址。	一端未配置remote-address，请排查。
ERROR - Peer remote-name(*remote-name*) does not match with	对等体remote-name不匹配。 *remote-name*：对端名称。	本端remote-id与对端名称不一致，请排查。

Debugging信息	描述	处理建议
Ikev1 error-info record(peer address: *peer-address*, error reason: *error-reason*,list number: *list-number*) Ikev2 error-info record(peer address: *peer-address*, error reason: *error-reason*,list number: *list-number*)	IKEv1/IKEv2协商失败的信息。 ● *peer-address*：对等体IP地址。 ● *error-reason*：IKE协商失败原因。 ● *list-number*：序号。	请根据IKE协商失败的常见原因进行排查： ● phase1 proposal mismatch：两端IKE安全提议参数不匹配。 ● phase2 proposal mismatch：两端IPSec安全提议参数不匹配。 ● responder dh mismatch：响应方的DH算法不匹配。 ● initiator dh mismatch：发起方的DH算法不匹配。 ● encapsulation mode mismatch：封装模式不匹配。 ● flow mismatch：两端Security ACL不匹配。 ● version mismatch：两端IKE版本号不匹配。 ● peer address mismatch

Debugging信息	描述	处理建议
		：两端的IKE Peer地址不匹配。 ● config ID mismatch：本端remote-id与对端名称不一致。 ● mismatch：两端的协商模式不匹配。 ● authentication fail：两端预共享密钥不一致。 ● unsupported version：不支持的IKE版本号。 ● malformed payload：畸形载荷，两端预共享密钥不一致。 ● route limit：路由注入的数目达到规格。

6 相关信息

AR系列接入路由器配置指南-IPSec

