一、开始

IPsec（IP Security，IP 安全）是 IETF 制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层 VPN（Virtual Private Network，虚拟专用网络）的安全技术。IPsec 通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。IPsec 协议不是一个单独的协议，它为 IP 层上的网络数据安全提供了一整套安全体系结构，包括安全协议 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）以及用于网络认证及加密的一些算法等。其中，AH 协议和 ESP 协议用于提供安全服务，IKE 协议用于密钥交换。IPsec 提供了两大安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。加密机制通过对数据进行加密运算来保证数据的机密性，以防数据在传输过程中被窃听。

SA（Security Association，安全联盟）是 IPsec 的基础，也是 IPsec 的本质。IPsec 在两个端点之间提供安全通信，这类端点被称为 IPsec 对等体。SA 是 IPsec 对等体间对某些要素的约定，例如，使用的安全协议（AH、ESP 或两者结合使用）、协议报文的封装模式（传输模式或隧道模式）、认证算法、加密算法、特定流中保护数据的共享密钥以及密钥的生存时间等。

IKE 使用了两个阶段为 IPsec 进行密钥协商以及建立 SA。第一阶段，通信双方彼此间建立了一个已通过双方身份认证和对通信数据安全保护的通道，即建立一个 IKE SA（本文中提到的 IKE SA 都是指第一阶段 SA）。第一阶段有主模式（Main Mode）和野蛮模式（Aggressive Mode）两种 IKE 协商模式。第二阶段，用在第一阶段建立的 IKE SA 为 IPsec 协商安全服务，即为 IPsec 协商 IPsec SA，建立用于最终的 IP 数据安全传输的 IPsec SA。

第一阶段主模式的 IKE 协商过程中包含三对消息，第一对消息完成了 SA 交换，它是一个协商确认双方 IKE 安全策略的过程；第二对消息完成了密钥交换，通过交换 DH 公共值和辅助数据（如：随机数），最终双方计算生成一系列共享密钥（例如，认证密钥、加密密钥以及用于生成 IPsec 密钥参数的密钥材料），并使其中的加密密钥和认证密钥对后续的 IKE 消息提供安全保障；第三对消息完成了 ID 信息和验证数据的交换，并进行双方身份的认证。野蛮模式交换与主模式交换的主要差别在于，野蛮模式不提供身份保护，只交换 3 条消息。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速

度；在对身份保护要求较高的场合，则应该使用主模式。接下来的正文中只讨论在两端设备上第一阶段协商失败，SA 均未正常生成的情况下的排查过程。

二、流程图相关操作说明：

1、设备公网两端是否互通

对于 IPsec 协商来讲，首先必须要保证进行 IPsec 协商的两端设备之间的网络通畅，否则两端设备之间的报文交互受阻，无法进行 IKE SA 的协商。此时，我们需要分别在两端设备上进行 ping 对端公网地址的操作，来确保网络连通性。如下图所示，其中 172.31.0.20 为实验室模拟的对端公网地址。

```
<H3C>ping 172.31.0.20
Ping 172.31.0.20 (172.31.0.20): 56 data bytes, press CTRL_C to break
56 bytes from 172.31.0.20: icmp_seq=0 ttl=255 time=0.700 ms
56 bytes from 172.31.0.20: icmp_seq=1 ttl=255 time=4.342 ms
56 bytes from 172.31.0.20: icmp_seq=2 ttl=255 time=0.524 ms
56 bytes from 172.31.0.20: icmp_seq=3 ttl=255 time=0.349 ms
56 bytes from 172.31.0.20: icmp_seq=4 ttl=255 time=0.314 ms

--- Ping statistics for 172.31.0.20 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.314/1.246/4.342/1.554 ms
<H3C>
```

因为 IKE 的第一阶段协商是使用 UDP 协议的 500 端口号来进行报文交互，所以仅仅能够保证设备公网两端的 ICMP 报文可以互通只是初步的网络连通性判断，如果需要判断真实的协商报文是否有在中间链路丢弃的情况，需要在触发协商时的两端设备上进行 debug。如果在发起端设备上有发出 IKE 报文但是对端设备无任何显示时，说明对端设备并未收到 IKE 报文，可能是中间链路丢弃的情况。另外需要说明，debug 命令会影响设备性能，需要谨慎使用并尽量使用指明的 remote-address 等配置减少性能压力，下文中 debug 信息不再做多次提示。

命令：debugging ike packet remote-address X.X.X.X

例如：通过 debug 命令查看，FW1 设备发出正常 IKE 报文，FW2 设备正常收到，说明网络通畅，没有丢弃 IKE 报文的情况。

```
<FW1>debugging ike packet  remote-address 172.31.0.20
<FW1>terminal debugging
<FW1>terminal monitor
*Aug 20 11:58:03:284 2018 FW1 IKE/7/PACKET: vrf = 0, src = 172.31.0.21, dst =
172.31.0.20/500
Sending packet to 172.31.0.20 remote port 500, local port 500.

<FW2>debugging ike packet  remote-address 172.31.0.21
<FW2>terminal debugging
<FW2>terminal monitor
*Aug 20 11:58:03:392 2018 FW2 IKE/7/PACKET: vrf = 0, src = 172.31.0.20, dst =
172.31.0.21/500
Received packet from 172.31.0.21 remote port 500, local port 500.
```

2、检查安全域、策略等配置

确认两设备间的端口号为 500 的 UDP 报文无法正常通信后，首先需要查看两端设备是否有放通相应的策略。

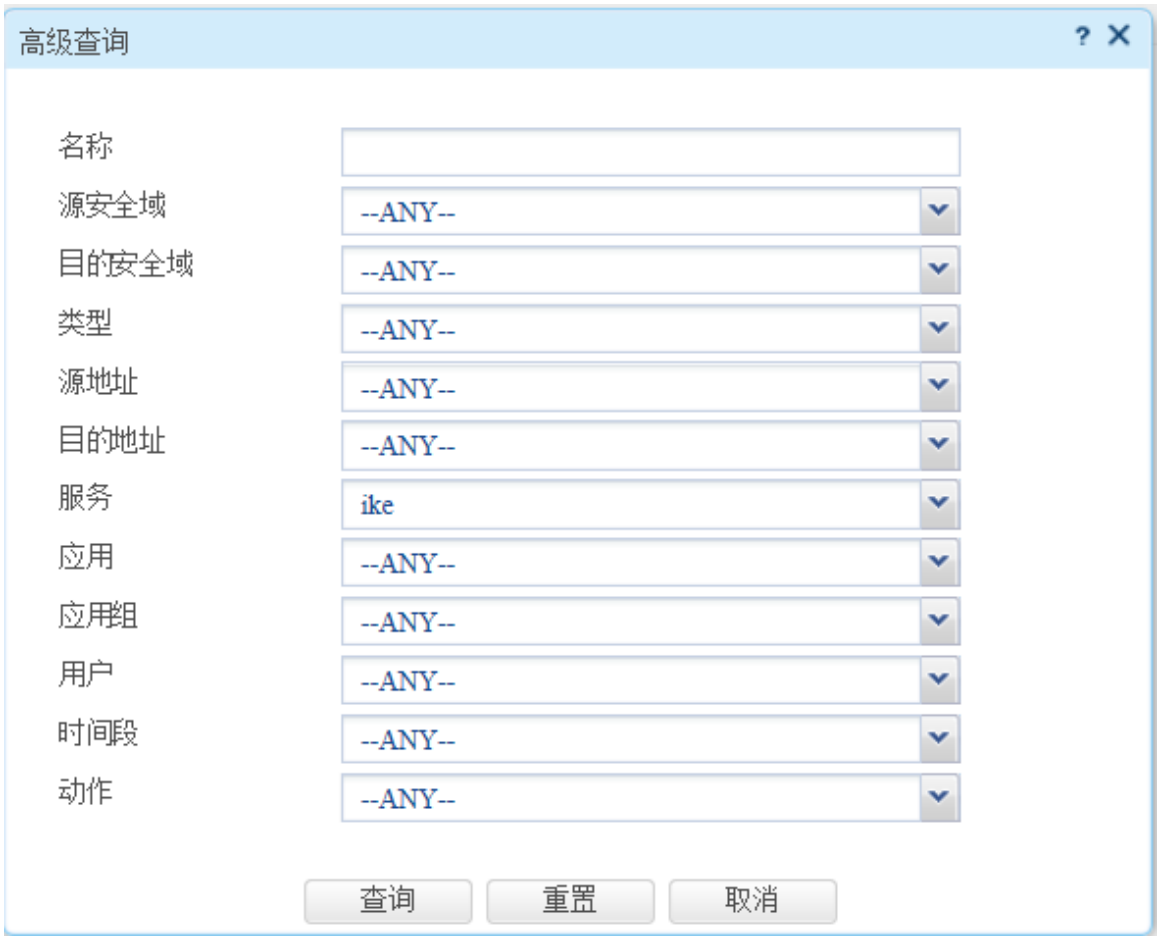
（1）安全域的配置：首先需要检查相应的接口是否加入了安全域：

```
[H3C]dis security-zone
Name: Local
Members:
  None

Name: Trust
Members:
  GigabitEthernet1/0/1
  LoopBack10

Name: DMZ
Members:
  None

Name: Untrust
Members:
  None

Name: Management
Members:
  GigabitEthernet1/0/0
```

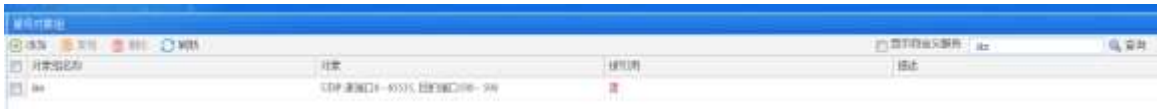
（2）安全策略的配置：最后我们要检查该安全域和本地域之间的安全策略是否放通，其

中策略可以使用包过滤策略、对象策略、安全策略等方式放通，此处我们以安全策略为例，查看是否有放通 Local 安全域与 Trust 安全域之间的安全策略，进入设备 Web 页面，点击上方的“策略”按钮，默认即为显示导航栏中的“安全策略”页面，也可以点击每一条策略后面的编辑按钮来查看其中的明细配置：

在有修改、删除等对安全策略有变更的操作之后，需要点击策略上方的“安全策略配置变更之后，需要**立即加速**才能生效”中的“立即加速”按钮使配置生效。如果策略条目过多，可以通过界面右上角的“高级查询”按钮查询特定流量是否匹配某一条策略，本例中可以通过查询已预定义好的“ike”服务类型来查看匹配到的策略：



其中，我们可以通过查看对象-对象组-服务对象组中查看该服务的定义情况：



3、检查是否有 NAT 配置

对于防火墙设备来说，接口流量会先匹配 NAT 业务模块，经过 NAT 处理完成后再匹配感兴趣流走 IPsec 模块进行协商。所以如果在相关的业务接口上有 NAT 配置会把原先符合感兴趣流条件的流量先进行地址转换，导致转换后的流不符合感兴趣流条件而不匹配 IPsec 模块，无法触发协商过程。

查看设备上 NAT 配置：

命令：display nat all

例如：通过命令查看，目前在 GigabitEthernet1/0/1 接口上有 NAT 相关配置：

```
[H3C]display  nat all
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 1
    Port range: 1-65535
    Address information:
      Start address         End address
      172.31.0.220          172.31.0.221

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: GigabitEthernet1/0/1
    ACL: ---
    Address group ID: 1
    Port-preserved: N        NO-PAT: N  Reversible: N
    Config status: Active

...
```

4、修改 NAT 配置

由于 IPsec VPN 模块经常部署在外网出口设备上，而外网接口上经常会使用 NAT outbound 配置，我们在确认有修改感兴趣流的相关 NAT 配置后，需要对 NAT outbound 的匹配条件做过滤，让感兴趣流不匹配 NAT 模块。此处，我们以感兴趣流是 10.1.1.0/24-20.1.1.0/24 为例：

```
[H3C-GigabitEthernet1/0/1]nat outbound 3999
[H3C-GigabitEthernet1/0/1]display this
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 172.31.0.21 255.255.255.0
 nat outbound 3999
#
return
[H3C-GigabitEthernet1/0/0]display acl 3999
Advanced IPv4 ACL 3999, 2 rule,
ACL's step is 5
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
 rule 5 permit ip
```

5、检查 ike profile

在确认上面的基本配置全部无误的情况下，需要注意 IKE Profile 中匹配的本对端地址是否可以唯一确认两端设备，也就是说，最少需要两端设备均配置对端地址、fqdn 或者 user-fqdn。其中，address 为标识对端身份的 IP 地址；fqdn 为标识对端身份的 fqdn 名称字符串，例如 www.test.com，如果不指定 fqdn-name 时，设备使用 sysname 命令配置的设备名称作为 fqdn 类型的身份；user-fqdn 为标识对端身份的 user-fqdn 字符串，例如 abc@test.com,如不指定,设备将使用 sysname 命令配置的名称作为 user-fqdn 类型身份。如果没有配置明确的对端设备地址或 FQDN,协商报文无法知道和哪里做协商。这种情况下，debug 信息一般无回显。

6、修改 ike profile

以配置对端协商的接口 IP 地址为例：

例如：通过命令进行配置，创建一个名字为 1 的 IKE Profile 并配置和该设备协商的对端设备地址：

```
[FW1]ike profile 1
[FW1-ike-profile-1]match remote identity address 172.31.0.22 255.255.255.255
```

或者登录设备 Web 页面，依次点击网络-VPN-IPsec-策略，选择相应的策略并点击后面的编辑按钮，可以在对端 IP 地址/主机名一栏中修改正确的对端 IP 地址或者主机名。

7、检查预共享密钥

在 IKE 需要通过预共享密钥方式进行身份认证时，协商双方需要创建并指定 IKE keychain。IKE keychain 用于配置协商双方的密钥信息，IKE 协商双方配置的预共享密钥必须相同，否则身份认证会失败。以明文或密文方式设置的预共享密钥，均以密文的方式保存在配置文件中。如果预共享密钥配置两端不匹配或者有错误的话，会中断两端协商过程，导致协商失败。这种情况下，需要通过 debug 信息来进行判断，但是针对主模式和野蛮模式的不同情况，会有不同类型的 debug 信息显示。

命令：debugging ike error remote-address X.X.X.X

例如：在主模式的部署方式下，通过 debug 命令查看，如果出现了如下报错，则证明预共享密钥可能有问题需要重新配置。

```
<FW1> debugging  ike error remote-address 172.31.0.24
<FW1>terminal debugging
<FW1>terminal monitor
*Aug 20 11:09:50:559 2018 FW1 IKE/7/ERROR: -Context=1; 2th byte of the structu
re ISAKMP Identification Payload must be 0.
*Aug 20 11:09:50:559 2018 FW1 IKE/7/ERROR: -Context=1; vrf = 0, local = 172.31
.0.22, remote = 172.31.0.24/500
Failed to parse phase 1 packet. Reason INVALID_PAYLOAD_TYPE.
```

例如：在野蛮模式的部署方式下，通过 debug 命令查看，如果出现了如下报错，则证明预

共享密钥可能有问题需要重新配置。

```
<FW1>debugging  ike error remote-address 172.31.0.24
<FW1>debugging ike packet  remote-address 172.31.0.24
<FW1>terminal debugging
<FW1>terminal monitor
*Aug 20 12:06:54:537 2018 FW1 IKE/7/ERROR: vrf = 0, src = 172.31.0.22, dst =
172.31.0.24/4500
Failed to verify the peer HASH.
*Aug 20 12:06:54:537 2018 FW1 IKE/7/PACKET: vrf = 0, src = 172.31.0.22, dst =
172.31.0.24/4500
Construct notification packet: AUTHENTICATION_FAILED.
```

8、修改预共享密钥

因为预共享密钥是以密文的形式存储在配置文件中，所以如果有笔误等情况导致预共享密钥不匹配的情况，无法通过查看配置信息来确认是否一致，只能通过重新刷新两端设备上预共享密钥的配置来修改。此处我们以预共享密钥为 123456 为例：

例如：通过命令进行配置，在 name 为 1 的 IKE Keychain 里配置相应的预共享密钥，并在 name 为 1 的 IKE Profile 里引用相应的 IKE Keychain：

```
[FW1]ike keychain 1
[FW1-ike-keychain-1]pre-shared-key   address   172.31.0.22  32  key   simple
123456
[FW1]ike profile 1
[FW1-ike-profile-1]keychain 1
```

或者登录设备 Web 界面，依次点击网络-VPN-IPsec-策略，选择相应的策略并点击后面的编辑按钮，其中的基本配置中，可以在预共享密钥一栏进行预共享密钥的配置或修改：

9、检查算法是否匹配

针对算法的匹配来说，如果两端设备均为我司设备的话相对容易排查，在第一阶段协商失败时检查两端设备的 IKE Proposal 中的加密和认证算法名字是否一致即可。但是在真实现网环境中经常会遇到我司防火墙和其他厂家设备对接的问题，其中配置的算法名称可能并不是完全相同或者对应,这种情况下,可以通过 debug 信息来确认两端的算法是否匹配。

命令：debugging ike error remote-address X.X.X.X

例如：通过 debug 命令查看，如果出现了如下报错，则证明两端的 ike 提议中的算法可能不匹配而需要重新配置。

```
<FW1> debugging  ike error remote-address 172.31.0.22
<FW1>debugging ike packet  remote-address 172.31.0.22
<FW1>terminal debugging
<FW1>terminal monitor
*Aug 26 16:38:14:322 2018 F1070 IKE/7/PACKET: -Context=1; vrf = 0, local =
172.31.0.24, remote = 172.31.0.22/500
The profile 1 is matched.
*Aug 26 16:38:14:323 2018 F1070 IKE/7/ERROR: -Context=1; vrf = 0, local =
172.31.0.24, remote = 172.31.0.22/500
Failed to find matched proposal in profile 1.
```

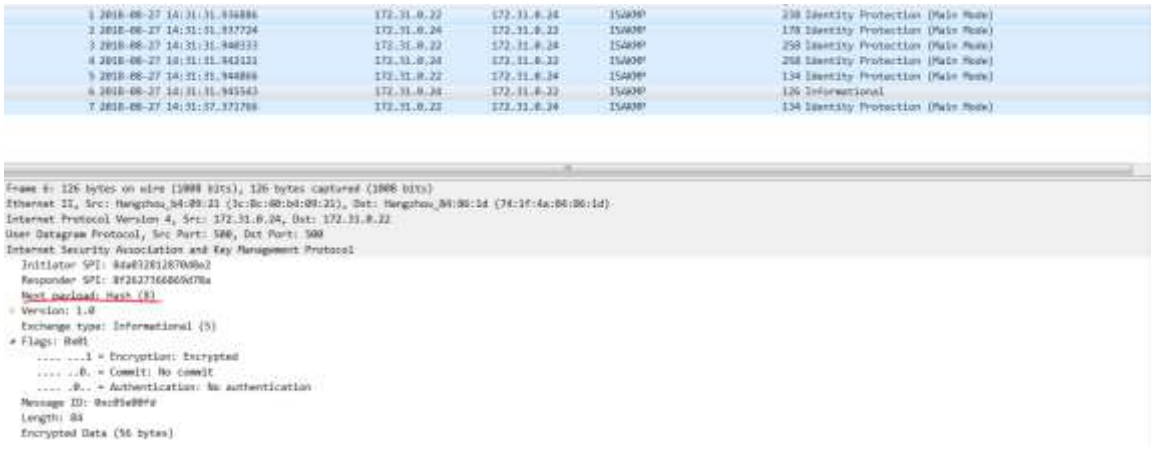
由于 IKE 提议和 IKE Keychain 均属于 IKE Profile 的内容，而 IKE Profile 中内容都是需要两端相互匹配的，所以在这里我们针对 IKE 提议中的算法和 IKE Keychain 中的预共享密钥的不匹配所显示的 debug 信息做出进一步的对比分析和说明。

在两种错误匹配情况下，其实均属于 IKE Profile 匹配有问题，这种情况下，IKE 交互过程中会出现回应通告报文的情况，具体的交互报文可以通过 debug ike packet 来看到，如果报文中的 next payload 字段为 HASH 且 exchange mode 为 Info 的话，则可以考查 IKE Profile 中的各项是否匹配有问题：

```
*Aug 27 03:38:25:004 2018 F5020 IKE/7/PACKET: -Context=1; vrf = 0, local = 172.31.0.22, remote = 172.31.0.24/500


  I-Cookie: 9baddd93481ff594

  R-Cookie: a84e58647a21e526

  next payload: HASH

  version: ISAKMP Version 1.0

  exchange mode: Info

  flags: ENCRYPT

  message ID: 7fca8760

  length: 84

*Aug 27 03:38:25:004 2018 F5020 IKE/7/PACKET: -Context=1; vrf = 0, local = 172.31.0.22, remote = 172.31.0.24/500

Sending an IPv4 packet.
```

也可以登陆设备 Web 界面，依次点击系统-维护-报文捕获中进行抓包分析。

分析预共享密钥和算法分别不匹配时候的报文交互过程发现该通告报文，如图所示：



另外，之前第 7 步检查预共享密钥时的 debug 报错在两端设备算法不匹配的时候也是会出现的，但是不同点在于算法不匹配会多出一条 IKE 载体的报错内容：

```
*Aug 26 16:38:19:944 2018 F1070 IKE/7/ERROR: -Context=1; 2th byte of the structure ISAKMP Identification Payload must be 0.
*Aug 26 16:38:19:945 2018 F1070 IKE/7/PACKET: -Context=1; vrf = 0, local = 172.31.0.24, remote = 172.31.0.22/500
Received ISAKMP SK Payload.
*Aug 26 16:38:19:945 2018 F1070 IKE/7/ERROR: -Context=1; 2th byte of the structure ISAKMP SK Payload must be 0.
*Aug 26 16:38:19:945 2018 F1070 IKE/7/ERROR: -Context=1; vrf = 0, local = 172.31.0.24, remote = 172.31.0.22/500
Failed to parse phase 1 packet. Reason INVALID_PAYLOAD_TYPE.
```

对比和预共享密钥不匹配时的报错情况，预共享密钥有问题时会先报告 ISAKMP 载体中字段不匹配，然后就会报告第一阶段协商失败，原因是非法的载体类型。而当设备两端算法不匹配时，报错信息先报告 ISAKMP 载体字段有问题，然后报告接受到了 SK 载体，并检查出 SK 载体中字段有问题，最后也报告了第一阶段协商失败的原因是非法载体类型。其中，SK 载体为提供 IKE 交换密钥的算法和方式等，所以只有在算法不一致时会报该错误。

10、修改算法

由于第一阶段协商有问题，所以只需要考虑 IKE Proposal 的配置问题。此处我们以加密算法为 3des-cbc，认证算法为 md5 为例：

例如：通过命令进行配置，创建一个 ID 为 65535 的 IKE 提议并配置其加密和认证算法：

```
[FW1]ike proposal 65535
[FW1-ike-proposal-65535]encryption-algorithm 3des-cbc
[FW1-ike-proposal-65535]authentication-algorithm md5
```

或者登录设备 Web 页面，依次点击网络-VPN-IKE 提议，选择需要修改的提议项，点击后面的编辑按钮，如图所示：

然后在弹出的对话框中选择正确的算法配置后点击确定按钮。

11、检查感兴趣流

对于 IPsec VPN 业务来说，必须有感兴趣流的匹配来确定哪些流量需要做 IPsec 协商。所以如果两端设备的感兴趣流配置不对应或者有错误的情况下，就不能正确的触发两端设备的 IPsec 协商。以正确的两端感兴趣流配置和引用为例：

```
[F1070]dis ipsec policy
-----------------------------------------
IPsec Policy: 1
Interface: Reth1
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3100
  Selector mode: standard
  Local address:
  Remote address: 172.31.0.22
  Transform set:  1
  IKE profile: 1
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Traffic-based
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): --
  SA soft-duration buffer(traffic based): --
  SA idle time: --
[F1070]dis acl ad
[F1070]dis acl 3100
Advanced IPv4 ACL 3100, 1 rule,
ACL's step is 5
 rule 0 permit ip source 20.1.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

```
[H3C]dis ipsec policy
-----------------------------------------
IPsec Policy: 1
Interface: GigabitEthernet1/0/0
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3500
  Selector mode: standard
  Local address:
  Remote address: 172.31.0.24
  Transform set:  1
  IKE profile: 1
  IKEv2 profile:
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA idle time:
[H3C]dis acl 3500
Advanced IPv4 ACL 3500, 1 rule,
ACL's step is 5
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
```

12、修改感兴趣流配置

如果判断为感兴趣流配置有误，则需要修改感兴趣流配置，针对相关的 IPsec 策略下所引用的 security acl,修改成正确的可以触发协商的源目的地址池。或者登录设备 Web 界面，依次点击网络-VPN-IPsec-策略，选择相应的策略并点击后面的编辑按钮：

其中基本配置中的保护的数据流的条目中可以进行感兴趣流的修改。

若上述操作结果均显示正常，请把上述分析过程操作记录、设备诊断信息以及抓包信息，反馈给安全产品支持部分析处理。