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。

IKE 的第二阶段的目的是为了其他协议（如 IPsec）生成 SA，这一阶段是通过快速模式交换来实现的，通过一次主模式或野蛮模式交换，许多快速模式都可以完成。IKE 第二阶段协商需要检查发起方和接收方配置的待保护的数据流是否成镜像关系，如果不成镜像关系，将向对端发送 INVALID_ID_INFORMATION，终止 IKE 协商。

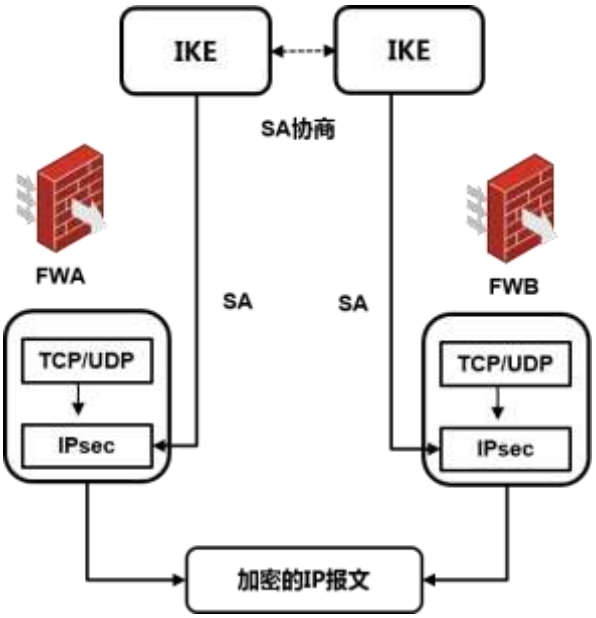
IPsec SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向

的数据流进行安全保护。同时，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。SA 由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址和安全协议号。其中，SPI 是用于标识 SA 的一个 32 比特的数值，它在 AH 和 ESP 头中传输。当 IPsec 对等体根据 IPsec 安全策略和 IPsec 安全框架识别出要保护的报文时，就建立一个相应的 IPsec 隧道并将其通过该隧道发送给对端。此处的 IPsec 隧道可以是提前手工配置或者由报文触发 IKE 协商建立。这些 IPsec 隧道实际上就是两个 IPsec 对等体之间建立的 IPsec SA。由于 IPsec SA 是单向的，因此出方向的报文由出方向的 SA 保护，入方向的报文由入方向的 SA 来保护。对端接收到报文后，首先对报文进行分析、识别，然后根据预先设定的安全策略对报文进行不同的处理（丢弃，解封装，或直接转发）,如果有一端 SA 出现了问题，那么两端的 IPsec SA 可能出现协商失败的情况，此时需要排查下两端协商过程中所需要的参数是否存在问题。接下来的正文中只讨论在两端设备上第一阶段协商正常，第二阶段的 SA 无法协商的排查过程。

二、流程图相关操作说明：

1、第一阶段 IKE SA 是否建立

用 IPsec 保护一个 IP 数据包之前，必须先建立一个安全联盟（IPsec SA），IPsec SA 可以手工创建或动态建立,而 IKE 为 IPsec 提供了自动建立 IPsec SA 的服务，两者的关系如下图所示。IKE 为 IPsec 协商建立 SA，并把建立的参数交给 IPsec，IPsec 使用 IKE 建立的 SA 对 IP 报文加密或认证处理。



IKE 使用了两个阶段为 IPsec 进行密钥协商以及建立 SA：(1)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。

(2)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。在排查 IPsec 隧道问题时首先排查下第一阶段 IKE SA 是否正常建立，如果第一阶段 IKE SA 无法建立，请参考云图《Comware V7 NGFW IPsec VPN 第一阶段问题故障排查》进行排查，如果第一阶段 IKE SA 正常建立，第二阶段 IPsec SA 无法建立，则继续按照以下思路进行排查。

2、检查 IPsec 安全提议

在设备两端建立 IPsec 协商时，如果第一阶段 SA 可以正常建立，那么可以说明设备两端的公网路由是可达的，相关的域间策略或者安全策略也是放通的，在这种情况下，需要用到 debug 命令查看 IPsec 协商过程中在哪一步出了问题，如果两端设备建立 IPsec 隧道数目较少，并且流量不大的情况下，可以在设备上开启 debugging ike all 和 debugging ipsec all 查看协商过程交互的调试信息。如果是在设备上建立多个 IPsec 隧道的情况下，打开 debug 调试时最好指明对端的 remote-address，否则大量的 debug 信息可能会对设备的性能造成较大的冲击，影响设备的使用。本文就第二阶段 debug 调试主要用到的调试命令如下：

命令：debugging ike all

debugging ipsec all

例如：在设备上开启一阶段 debugging ike all 调试信息和二阶段 debugging ipsec all 的调试信息，如下图所示。

```
<FW1>debugging ike all
<FW1>terminal debugging
<FW1>terminal monitor
<FW1>*May 21 16:01:53:609 2019 H3C IKE/7/EVENT: -Context=1; Received packet
successfully.
*May 21 16:01:53:609 2019 H3C IKE/7/PACKET: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
Received packet from 1.1.1.2 source port 500 destination port 500.
*May 21 16:01:53:609 2019 H3C IKE/7/PACKET: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
  I-Cookie: 43dffd8e0826f646
  R-Cookie: e2a54aafea84de94
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
  message ID: d3d40d2
  length: 172
```

```
<FW1>debugging ipsec all
<FW1>terminal debugging
<FW1>terminal monitor
<H3C>*May 21 17:53:43:260 2019 H3C IPSEC/7/PACKET: -Context=1;
--- Received IPsec packet from fast forwarding, Protocl : 50---
*May 21 17:53:43:260 2019 H3C IPSEC/7/PACKET: -Context=1;
Inbound IPsec processing: src IP = 1.1.1.2, dst IP = 1.1.1.1, SPI =
3398360594.
*May 21 17:53:43:260 2019 H3C IPSEC/7/PACKET: -Context=1;
Inbound IPsec processing: ESP auth algorithm: SHA1, ESP encp algorithm: AES-
CBC-128.
*May 21 17:53:43:260 2019 H3C IPSEC/7/PACKET: -Context=1;
Packet will be sent to CCF for sync-decryption.
*May 21 17:53:43:260 2019 H3C IPSEC/7/PACKET: -Context=1;
Inbound fast IPsec ESP processing: Authentication succeeded.
```

通过 display ike sa 查看一阶段 SA 已经建立，并且 Flag 状态为 RD 的情况下，此时 display ipsec sa 查看二阶段 SA 是否建立，如果没有信息，需要首先检查 IPsec 安全提议，IPsec 安全提议是 IPsec 安全策略的一个组成部分，它用于定义 IPsec 需要使用的安全协议、加密/认证算法以及封装模式，为 IPsec 协商 SA 提供各种安全参数。通过 display ipsec transform-set 命令检查两端设备配置的加密算法和认证算法是否一致，如果两端

配置的加密算法和认证算法参数不一致，那么需要对 IPsec 安全提议进行修改，但是对已协商成功的 IPsec SA，新修改的安全提议并不起作用，即仍然使用原来的安全提议，只有新协商的 SA 使用新的安全提议。若要使修改对已协商成功的 IPsec SA 生效，则需要执行 reset ipsec sa 命令之后重新触发新的 ipsec sa 生成。

```
<H3C>display ike  sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               1.1.1.2               RD           IPsec
<H3C>display ipsec transform-set
IPsec transform set: FW1
  State: complete
  Encapsulation mode: tunnel
  ESN: Disabled
  PFS:
  Transform: ESP
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128
```

还有一种情况：当两端设备配置的加密算法和认证算法一致，PFS 算法不一致时，可能会出现 Failed to negotiate IPsec SA 的报错，这是因为 IKEv1 协商时发起方的 PFS 强度必须大于或等于响应方的 PFS 强度，否则协商会失败。如果采用 IKEv2 则不受该限制。

```
<H3C>debugging ike error remote-address 1.1.1.2
<H3C>debugging ipsec error
<H3C>terminal debugging
<H3C>terminal monitor
*May 21 19:12:00:583 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
Failed to negotiate IPsec SA.
```

3、修改 IPsec 安全提议

如果是在命令行配置的情况下，需要首先创建一个安全提议的名称，然后再配置对应的加密算法、认证算法以及 PFS 算法。本文以 FW1 设备为示例，命令行配置如下：

```
[FW1]ipsec transform FW1
[FW1-ipsec-transform-set-FW1]esp encryption-algorithm aes-cbc-128
[FW1-ipsec-transform-set-FW1]esp authentication-algorithm sha1
[FW1-ipsec-transform-set-FW1]pfs dh-group5
```

其中 PFS 算法的配置不是必选的，缺省情况下，使用 IPsec 安全策略发起协商时不使用 PFS 特性。如果对端配置了 PFS 特性，本端没有配置 PFS 特性的话，就会按照对端的 PFS 特性要求进行 IKE 协商。

如果是在 Web 页面配置 IPsec 安全提议，可以点击 Web 页面网络—VPN—IPsec—策略选项，点击新建选项，进入到高级配置视图下，可以配置和修改对应的 IPsec 参数。

4、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。由于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，所以配置上无法查看两端是否一致，可以通过 debug 信息的来查看。

正常情况下，预共享不一致的话的第一阶段的 ike sa 建立就会有问题，但是存在一种情况，当两端 IPsec 隧道已经建立，有一端修改过预共享密钥的话，可能会存在没有 IPsec sa 的情况，如果主模式下出现了下面的报错，说明预共享密钥协商过程中出了问题，可以通过修改两端预共享密钥一致再测试下。

```
<H3C>debugging ike error remote-address 1.1.1.2
<H3C>debugging ipsec error
<H3C>terminal debugging
<H3C>terminal monitor
*May 23 14:00:46:000 2019 H3C IKE/7/ERROR: -Context=1; 2th byte of the
structure ISAKMP Hash Payload must be 0.
*May 23 14:00:46:000 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
Failed to parse informational exchange packet. Reason INVALID_PAYLOAD_TYPE.
*May 23 14:00:48:015 2019 H3C IPSEC/7/ERROR: -Context=1;
The reason of dropping packet is no available IPsec tunnel.
```

如果是野蛮模式的话，出现了 Failed to verify the peer HASH 的报错，有可能是预共享密钥的配置问题，需要重新配置。

```
<H3C>debugging ike error remote-address 1.1.1.2
<H3C>debugging ipsec error
<H3C>terminal debugging
<H3C>terminal monitor
*May 25 01:24:33:426 2019 H3C IPSEC/7/ERROR: -Context=1;
Inbound IPsec processing: source address=192.168.100.10, destination
address=192.168.10.10, protocol=1. Packet was dropped according to IPsec
policy FW1(sequence number: 10).
*May 25 01:24:50:879 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
Failed to verify the peer HASH.
```

5、修改预共享密钥

由于配置文件中无法查看两端配置的预共享密钥是否一致，这个时候需要重新刷新下两端的预共享密钥确保一致。

例如：将两边的预共享密码修改为 123456789 保持一致。

```
[H3C]ike keychain FW1
[H3C-ike-keychain-FW1]pre-shared-key address 1.1.1.2  255.255.255.255 key
 simple 123456789

[H3C]ike profile FW1
[H3C-ike-profile-FW1] keychain FW1
[H3C-ike-profile-FW1] match remote identity address 1.1.1.2 255.255.255.0
```

如果是在 Web 页面配置，可以点击 web 页面网络—VPN—IPsec—策略选项，在 IKE 策略里

可以配置或者修改预共享密钥的参数。

6、检查感兴趣流

IPsec 隧道可以保护匹配 ACL 的报文，将引用了 ACL 的 IPsec 安全策略应用到接口上后，该接口上匹配 ACL 的报文将会受到 IPsec 保护。这里的接口包括以太网接口等实际物理接口，以及 Tunnel、Virtual Template 等虚接口（loopback 口除外）。只要接口发送的报文与该接口上应用的 IPsec 安全策略中的 ACL 的 permit 规则匹配，就会受到出方向 IPsec SA 的保护并进行封装处理。接口接收到目的地址是本机的 IPsec 报文时，首先根据报文头里携带的 SPI 查找本地的入方向 IPsec SA，由对应的入方向 IPsec SA 进行解封装处理。解封装后的 IP 报文若能与 ACL 的 permit 规则匹配上则采取后续处理，否则被丢弃。因此在配置 IPSec 协商保护的感兴趣流时，两端要保持一致，否则可能会影响 IPSec SA 的协商。通过命令行 display ipsec policy 可以查看 ipsec 保护的感兴趣流，如下图所示。

```
<H3C>display  ipsec  policy
-----------------------------------------
IPsec Policy: FW1
Interface: GigabitEthernet1/0/2
-----------------------------------------

  ------------------------------
  Sequence number: 10
  Mode: ISAKMP
  ------------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3333
  Selector mode: standard
  Local address: 1.1.1.1
  Remote address: 1.1.1.2
  Transform set:  FW1
  IKE profile: FW1
  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: --
<H3C>display acl 3333
Advanced IPv4 ACL 3333, 1 rule,
ACL's step is 5
 rule 0 permit ip source 192.168.10.0 0.0.0.255 destination 192.168.100.0 0.0.0.255 (56 times matched)
```

如果 IPsec 二阶段的 SA 无法正常协商，通过 debug 信息中出现以下报错时，很有可能是两端的感兴趣流不一致导致的。

```
<H3C>*May 23 18:47:15:470 2019 H3C IPSEC/7/EVENT: -Context=1;
 Could not find tunnel, ike profile name is FW1.
*May 23 18:47:15:470 2019 H3C IPSEC/7/EVENT: -Context=1;
The policy's acl or ike profile does not match the flow, Name = FW1, Seqnum
= 10
*May 23 18:47:15:470 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
Failed to get IPsec policy for phase 2 responder. Delete IPsec SA.
*May 23 18:47:15:470 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
1.1.1.1, remote = 1.1.1.2/500
Failed to negotiate IPsec SA.
```

7、修改感兴趣流

检查两边配置的感兴趣流保护的源目地址是否对称，如果存在不一致的情况，需要修改两边的感兴趣流。

例如：修改 acl 3333 规则里的感兴趣流，并且调用在 IPsec 策略下或者进入到 Web 页面网络—VPN—IPsec—策略,点击编辑进入到保护的数据流选项，可以对要保护的数据流的源目地址、协议以及源目端口等进行修改。

```
[H3C]acl  advanced  3333
[H3C-acl-ipv4-adv-3333]rule  0  permit  ip  source  192.168.10.0  0.0.0.255
 destination 192.168.100.0 0.0.0.255

[H3C]ipsec policy FW1 10 isakmp
[H3C-ipsec-policy-isakmp-FW1-10]security acl 3333
```

8、检查 IPsec 策略

IPsec 隧道两端的配置必须符合以下要求：IPsec 安全策略引用的 IPsec 安全提议中应包含相同的安全协议、认证/加密算法和报文封装模式。IPsec 安全策略引用的 IKE profile 参数相匹配。一条 IKE 协商方式的 IPsec 安全策略中最多可以引用六个 IPsec 安全提议。IPsec 协商过程中，IKE 将会在隧道两端配置的 IPsec 安全策略中查找能够完全匹配的 IPsec 安全提议。如果 IKE 在两端找不到完全匹配的 IPsec 安全提议，则 SA 不能协商成功，需要被保护的报文将被丢弃。IKE 协商的发起方必须配置 IPsec 隧道的对端地址，响应方可选配，且当前端点的对端地址与对端 VPN 网关的本端地址应保持一致。

如果响应方 IPsec 安全策略配置错误，会导致在 IKE 第二阶段协商时找不到 IPsec 安全策略。首先通过 display ike sa verbose 命令查看 IKE 一阶段协商中是否找到匹配的 ike profile。若没有找到 ike profile，则会查找全局的 IKE 参数，因此就要求这种情况下 IPsec 安全策略中不能引用任何 ike profile，否则协商失败；若是找到了 ike profile，查看 ipsec policy 引用的 ike profile 是否正确，如果引用了错误的 ike profile ，会出现无法协商二阶段的 SA，debug 信息中会出现如下报错。

```
*May 23 21:16:18:243 2019 H3C IPSEC/7/EVENT: -Context=1;
 Could not find tunnel, ike profile name is fw1.
*May 23 21:16:18:243 2019 H3C IPSEC/7/EVENT: -Context=1;
The policy's acl or ike profile does not match the flow, Name = FW1, Seqnum
 = 10
*May 23 21:16:18:243 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
 1.1.1.1, remote = 1.1.1.2/500
Failed to get IPsec policy for phase 2 responder. Delete IPsec SA.
*May 23 21:16:18:243 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
 1.1.1.1, remote = 1.1.1.2/500
Failed to negotiate IPsec SA.
```

还有一种情况：如果 IPsec 安全策略中没有配置或者配置了错误的对端隧道 IP 地址，也是无法响应的，在 debug 信息中可能会出现下面的报错。

```
*May 23 22:00:13:027 2019 H3C IPSEC/7/EVENT: -Context=1;
 Could not find tunnel, ike profile name is fw1.
*May 23 22:00:13:027 2019 H3C IPSEC/7/EVENT: -Context=1;
SP is not complete when matching flow.
*May 23 22:00:13:027 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
 1.1.1.1, remote = 1.1.1.2/500
Failed to get IPsec policy for phase 2 responder. Delete IPsec SA.
*May 23 22:00:13:027 2019 H3C IKE/7/ERROR: -Context=1; vrf = 0, local =
 1.1.1.1, remote = 1.1.1.2/500
Failed to negotiate IPsec SA.
```

9、修改 IPsec 策略

完整的 IPsec 策略主要包含安全提议、保护的数据流、隧道的对端 IP 地址、引用正确的 IKE 提议，可以重点检查两端对应的参数是否一致，然后针对相应的参数进行修改，最后需要注意策略引用到接口是否正确。

如果按照上述排查思路排查结果仍然存在异常，请收集完整的 debug 信息、两端设备的完

整配置以及相关的抓包信息返回总部 400 进行分析。