目 录

1 IPsec

1.1 IPsec简介

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。关于 IKE 的详细介绍请参见“安全配置指导”中的“IKE”，本节不做介绍。

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。

IPsec 为 IP 层的数据报文提供的安全服务具体包括以下几种：

- 数据机密性（Confidentiality）：发送方通过网络传输用户报文前，IPsec 对报文进行加密。
- 数据完整性（Data Integrity）：接收方对发送方发送来的 IPsec 报文进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证（Data Authentication）：接收方认证发送 IPsec 报文的发送端是否合法。
- 抗重放（Anti-Replay）：接收方可检测并拒绝接收过时或重复的 IPsec 报文。

IPsec 具有以下优点：

- 支持 IKE（Internet Key Exchange，互联网密钥交换），可实现密钥的自动协商功能，减少了密钥协商的开销。可以通过 IKE 建立和维护 SA（Security Association，安全联盟），简化了 IPsec 的使用和管理。
- 所有使用 IP 协议进行数据传输的应用系统和服务都可以使用 IPsec，而不必对这些应用系统和服务本身做任何修改。
- 对数据的加密是以数据包为单位的，而不是以整个数据流为单位，这不仅灵活而且有助于进一步提高 IP 数据包的安全性，可以有效防范网络攻击。

1.1.1 安全协议及封装模式

1. 安全协议

IPsec 包括 AH 和 ESP 两种安全协议，它们定义了对 IP 报文的封装格式以及可提供的安全服务。

- AH协议（IP协议号为 51）定义了AH头在IP报文中的封装格式，如 图 1-3 所示。AH可提供数据来源认证、数据完整性校验和抗重放功能，它能保护报文免受篡改，但不能防止报文被窃听，适合用于传输非机密数据。AH使用的认证算法有HMAC-MD5 和HMAC-SHA1。

- ESP协议（IP协议号为 50）定义了ESP头和ESP尾在IP报文中的封装格式，如 图 1-3 所示。ESP可提供数据加密、数据来源认证、数据完整性校验和抗重放功能。与AH不同的是，ESP将需要保护的用户数据进行加密后再封装到IP包中，以保证数据的机密性。ESP使用的加密算法有DES、3DES、AES等。同时，作为可选项，ESP还可以提供认证服务，使用的认证算法有HMAC-MD5 和HMAC-SHA1。虽然AH和ESP都可以提供认证服务，但是AH提供的认证服务要强于ESP。

在实际使用过程中，可以根据具体的安全需求同时使用这两种协议或仅使用其中的一种。设备支持的 AH 和 ESP 联合使用的方式为：先对报文进行 ESP 封装，再对报文进行 AH 封装。

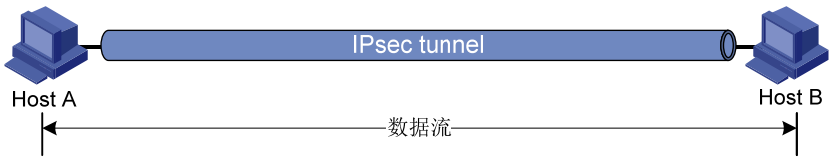
2. 封装模式

IPsec 支持两种封装模式：

- 传输模式（Transport Mode）

该模式下的安全协议主要用于保护上层协议报文，仅传输层数据被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对ESP封装）被放置在原IP头后面。若要求端到端的安全保障，即数据包进行安全传输的起点和终点为数据包的实际起点和终点时，才能使用传输模式。如 图 1-1 所示，通常传输模式用于保护两台主机之间的数据。

图1-1 传输模式下的 IPsec 保护



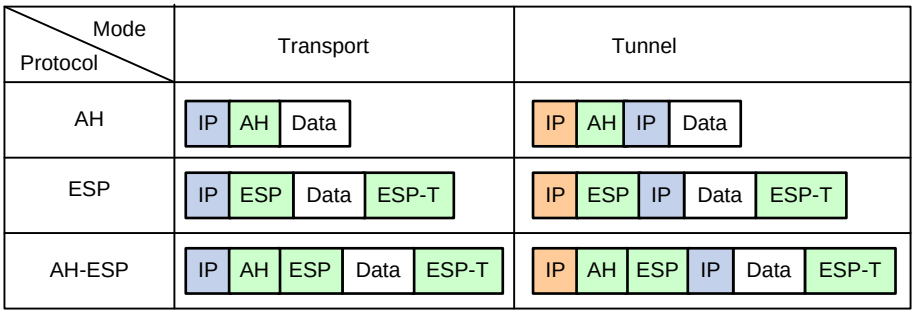
- 隧道模式（Tunnel Mode）

该模式下的安全协议用于保护整个IP数据包，用户的整个IP数据包都被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对ESP封装）被封装在一个新的IP数据包中。这种模式下，封装后的IP数据包有内外两个IP头，其中的内部IP头为原有的IP头，外部IP头由提供安全服务的设备添加。在安全保护由设备提供的情况下，数据包进行安全传输的起点或终点不为数据包的实际起点和终点时（例如安全网关后的主机），则必须使用隧道模式。如 图 1-2 所示，通常隧道模式用于保护两个安全网关之间的数据。

图1-2 隧道模式下的 IPsec 保护

不同的安全协议及组合在隧道和传输模式下的数据封装形式如 图 1-3 所示。

图1-3 安全协议数据封装格式



1.1.2 安全联盟

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（HMAC-MD5 或 HMAC-SHA1）、加密算法（DES、3DES 或 AES）、特定流中保护数据的共享密钥以及密钥的生存时间等。

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。

SA 有手工配置和 IKE 自动协商两种生成方式：

- 手工方式：通过命令行配置 SA 的所有信息。该方式的配置比较复杂，而且不支持一些高级特性（例如定时更新密钥），优点是可以不依赖 IKE 而单独实现 IPsec 功能。该方式主要用于需要安全通信的对等体数量较少，或小型静态的组网环境中。
- IKE 自动协商方式：对等体之间通过 IKE 协议自动协商生成 SA，并由 IKE 协议维护该 SA。该方式的配置相对比较简单，扩展能力强。在中、大型的动态网络环境中，推荐使用 IKE 自动协商建立 SA。

手工方式建立的 SA 永不老化。通过 IKE 协商建立的 SA 具有生存时间，该类型的 SA 有两种形式的生存时间：

- 基于时间的生存时间，定义了一个 SA 从建立到失效的时间；
- 基于流量的生存时间，定义了一个 SA 允许处理的最大流量。

可同时存在基于时间和基于流量两种方式的 SA 生存时间，只要 SA 的生存时间到达指定的时间或流量时，该 SA 就会失效。SA 失效前，IKE 将为 IPsec 对等体协商建立新的 SA，这样，在旧的 SA 失效前新的 SA 就已经准备好。在新的 SA 开始协商而没有协商好之前，使用当前旧的 SA 保护通信。一旦协商出新的 SA，立即采用新的 SA 保护通信。

1.1.3 认证与加密

1. 认证算法

IPsec 使用的认证算法主要是通过杂凑函数实现的。杂凑函数是一种能够接受任意长度的消息输入，并产生固定长度输出的算法，该算法的输出称为消息摘要。IPsec 对等体双方都会计算一个摘要，接收方将发送方的摘要与本地的摘要进行比较，如果二者相同，则表示收到的 IPsec 报文是完整未经篡改的，以及发送方身份合法。目前，IPsec 强制使用基于 HMAC（Hash-based Message Authentication Code，基于散列的消息鉴别码）的认证算法，包括 HMAC-MD5 和 HMAC-SHA1。其中，HMAC-MD5 算法的计算速度快，而 HMAC-SHA1 算法的安全强度高。

2. 加密算法

IPsec 使用的加密算法属于对称密钥系统，这类算法使用相同的密钥对数据进行加密和解密。目前设备的 IPsec 使用三种加密算法：

- DES：使用 56 比特的密钥对一个 64 比特的明文块进行加密。
- 3DES：使用三个 56 比特（共 168 比特）的密钥对明文块进行加密。
- AES：使用 128 比特、192 比特或 256 比特的密钥对明文块进行加密。

这三个加密算法的安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。

3. 加密引擎

IPsec 的认证和加/解密处理在设备上既可以通过软件实现，也可以通过硬件加密引擎实现。通过软件实现的 IPsec，由于复杂的加密/解密、认证算法会占用大量的 CPU 资源，将会影响设备整体处理效率；通过硬件加密引擎实现的 IPsec，由于复杂的算法处理由硬件完成，因此可以提高设备的处理效率。

若设备支持通过硬件加密引擎进行认证和加/解密处理，则设备会首先将需要处理的数据发送给硬件加密引擎，由硬件加密引擎对数据进行处理之后再发送回设备，最后由设备进行转发。

关于加密引擎的详细介绍请参见“安全配置指导”中的“加密引擎”。

1.1.4 IPsec实现方式

要实现建立 IPsec 隧道为两个 IPsec 对等体之间的数据提供安全保护，首先要配置相应的安全策略，通过安全策略定义哪些报文属于要保护的范围，并定义用于保护这些报文的安全参数。之后，将安全策略应用于设备的某接口上。当 IPsec 对等体根据安全策略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）。

通过将 IPsec 安全策略应用到设备的接口上，使得设备对通过该接口收发的数据报文依据接口上应用的安全策略进行 IPsec 保护。

目前，在基于接口的 IPsec 实现方式下仅支持基于 ACL 建立 IPsec 隧道。

基于 ACL（Access Control List，访问控制列表）方式下，需要通过定义 ACL 来指定两个对等体之间需要被保护的数据流的范围，并需要将引用了该 ACL 的 IPsec 安全策略应用到相应的接口上。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。

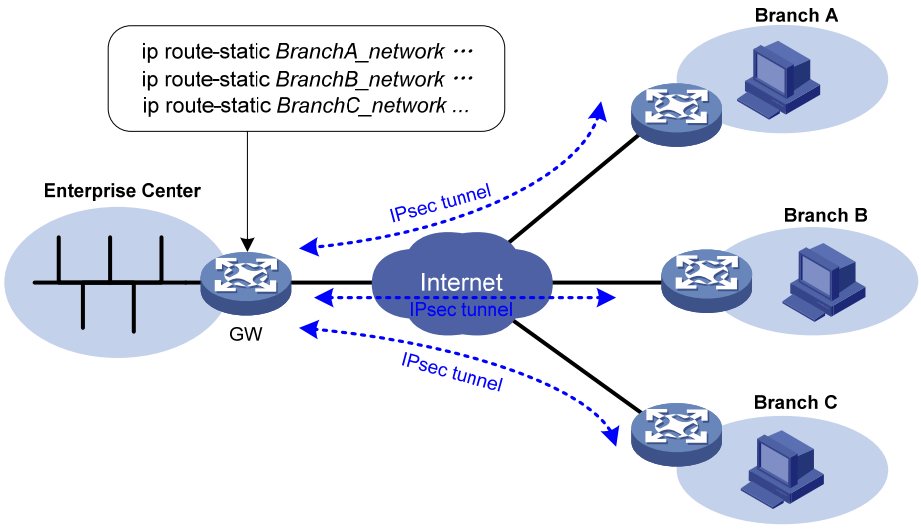
目前，设备支持的数据流的保护方式包括以下三种：

- 标准方式：一条 IPsec 隧道保护一条数据流。ACL 中的每一个规则对应的数据流分别由一条单独创建的 IPsec 隧道来保护。缺省采用该方式。
- 聚合方式：一条 IPsec 隧道保护 ACL 中定义的所有数据流。ACL 中的所有规则对应的数据流只会由一条创建的 IPsec 隧道来保护。该方式仅用于和老版本的设备互通。
- 主机方式：一条 IPsec 隧道保护一条主机到主机的数据流。ACL 中的每一个规则对应的不同主机之间的数据流分别由一条单独创建的 IPsec 隧道来保护。这种方式下，受保护的网段之间存在多条数据流的情况下，将会消耗更多的系统资源。

1.1.5 IPsec反向路由注入功能

如 图 1-4 所示，某企业在企业分支与企业总部之间的所有流量通过IPsec进行保护，企业总部网关上需要配置静态路由，将总部发往分支的数据引到应用IPsec安全策略的接口上来。当企业分支众多或者内部网络规划发生变化时，就需要同时增加或调整总部网关上的静态路由配置，该项工作量大且容易出现配置错误。

图1-4 IPsec VPN 总部-分支组网图



RRI（Reverse Route Injection，反向路由注入）功能可以很好的解决以上问题。RRI 是一种自动添加到达 IPsec VPN 私网静态路由的机制，可以实现为受 IPsec 保护的流量自动添加静态路由的功能。如上 IPsec VPN 组网中，当企业总部侧网关设备 GW 上配置 RRI 功能后，每一个 IPsec 隧道建立之后，GW 都会自动为其添加一条相应的静态路由。通过 RRI 创建的路由表项可以在路由表中查询到，其目的地址为受保护的对端网络，下一跳地址为 IPsec 隧道的对端地址，它使得发往对端的流量被强制通过 IPsec 保护并转发。

RRI 创建的静态路由和手工配置的静态路由一样，可以向内网设备进行广播，允许内网设备选择合适的路由对 IPsec VPN 流量进行转发。

在大规模组网中，这种自动添加静态路由的机制可以简化用户配置，减少在企业总部网关设备上配置静态路由的工作量，并且可以根据 IPsec SA 的创建和删除进行静态路由的动态增加和删除，增强了 IPsec VPN 的可扩展性。

1.1.6 协议规范

与 IPsec 相关的协议规范有：

- RFC 2401：Security Architecture for the Internet Protocol
- RFC 2402：IP Authentication Header
- RFC 2406：IP Encapsulating Security Payload
- RFC 4552：Authentication/Confidentiality for OSPFv3

1.2 建立IPsec隧道的配置方式

注意

通常情况下，由于 IKE 协议采用 UDP 的 500 端口进行通信，IPsec 的 AH 和 ESP 协议分别使用 51 或 50 号协议来工作，因此为保障 IKE 和 IPsec 的正常运行，需要确保应用了 IKE 和 IPsec 配置的接口上没有禁止掉属于以上端口和协议的流量。

基于ACL方式：由ACL来指定要保护的数据流范围，利用ACL的丰富配置功能，结合实际的组网环境灵活制定IPsec安全策略。该方式的配置方法为：通过配置IPsec安全策略并将IPsec安全策略绑定在接口上来完成IPsec的配置。具体配置请参见“1.3 基于ACL建立IPsec隧道”。在IPv4 网络和IPv6 网络中，基于ACL建立IPsec隧道的配置步骤相同。

1.3 基于ACL建立IPsec隧道

1.3.1 基于ACL建立IPsec隧道配置任务简介

基于 ACL 建立 IPsec 隧道的基本配置思路如下：

(1) 配置 ACL：指定要保护的数据流。IPsec 不需要通过在 ACL 规则中指定 VPN 参数来保护 VPN 间的数据流。

(2) 配置 IPsec 安全提议：指定安全协议、认证算法、加密算法、封装模式等。

(3) 配置 IPsec 安全策略：一个 IPsec 安全策略是若干具有相同名字、不同顺序号的 IPsec 安全策略表项的集合。在同一个 IPsec 安全策略中，顺序号越小的 IPsec 安全策略表项优先级越高。IPsec 安全策略将要保护的数据流和 IPsec 安全提议进行了关联（即定义对何种数据流实施何种保护），并指定了 IPsec SA 的生成方式（手工方式、IKE 协商方式）、对等体 IP 地址（即保护路径的起点或终点）、所需要的密钥和 IPsec SA 的生存时间等。

(4) 在接口上应用 IPsec 安全策略。

表1-1 基于 ACL 建立 IPsec 隧道配置任务简介

配置任务		说明	详细配置
配置ACL		必选	1.3.2
配置IPsec安全提议		必选	1.3.3
配置IPsec安全策略	配置手工方式的安全策略	二者必选其一	1.3.4
	配置IKE协商方式的安全策略		1.3.5
在接口上应用IPsec安全策略		必选	1.3.6
配置解封装后IPsec报文的ACL检查功能		可选	1.3.7
配置IPsec抗重放功能		可选	1.3.8
配置IPsec抗重放窗口和序号的同步功能		可选	1.3.9
配置共享源接口安全策略		可选	1.3.10
配置QoS预分类功能		可选	1.3.11
配置IPsec报文日志记录功能		可选	1.3.12
设置IPsec隧道模式下封装后外层IP头的DF位		可选	1.3.13
配置IPsec反向路由注入功能		可选	1.3.14
配置IPsec告警功能		可选	1.4
配置IPsec分片功能		可选	1.5
配置本端允许建立IPsec隧道的最大数		可选	1.6
开启IPsec协商事件日志功能		可选	1.7

1.3.2 配置ACL

1. ACL规则中关键字的使用

IPsec 通过配置 ACL 来定义需要保护的数据流。在 IPsec 应用中，ACL 规则中的 **permit** 关键字表示与之匹配的流量需要被 IPsec 保护，而 **deny** 关键字则表示与之匹配的流量不需要保护。一个 ACL 中可以配置多条规则，首个与数据流匹配上的规则决定了对该数据流的处理方式。

在IPsec安全策略中定义的ACL既可用于过滤接口入方向数据流，也可用于过滤接口出方向数据流。

- 设备出入方向的数据流都使用 IPsec 安全策略中定义的 ACL 规则来做匹配依据。具体是，出方向的数据流正向匹配ACL规则，入方向的数据流反向匹配ACL规则。例如，对于应用于IPsec安全策略中的某 ACL 规则：**rule** 0 **permit ip source** 1.1.1.0 0.0.0.255 **destination** 2.2.2.0 0.0.0.255，设备使用其正向过滤出方向上从 1.1.1.0/24 网段发往 2.2.2.0/24 网段的数据流，反向过滤入方向上从 2.2.2.0/24 网段发往 1.1.1.0/24 网段的数据流。
- 在出方向上，与 ACL 的 **permit** 规则匹配的报文将被 IPsec 保护，未匹配上任何规则或与 **deny** 规则匹配上的报文将不被 IPsec 保护。
- 在入方向上，与 ACL 的 **permit** 规则匹配上的未被 IPsec 保护的报文将被丢弃；目的地址为本机的被 IPsec 保护的报文将被进行解封装处理。缺省情况下解封装后的 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。若解封装后 IPsec 报文的 ACL 检查功能处于关闭状态，则解封装后的 IP 报文不与 ACL 匹配，直接进行后续处理。

需要注意的是：

- 仅对确实需要 IPsec 保护的数据流配置 **permit** 规则，避免盲目地使用关键字 **any**。这是因为，在一个 **permit** 规则中使用 **any** 关键字就代表所有指定范围上出方向的流量都需要被 IPsec 保护，所有对应入方向上被 IPsec 保护的报文将被接收并处理，入方向上未被 IPsec 保护的报文都将被丢弃。这种情况下，一旦入方向收到的某流量是未被 IPsec 保护的，那么该流量就会被丢弃，这会造成一些本不需要 IPsec 处理的流量丢失，影响正常的业务传输。
- 当一个安全策略下有多条优先级不同的安全策略表项时，合理使用 **deny** 规则。避免本应该与优先级较低的安全策略表项的 ACL **permit** 规则匹配而被 IPsec 保护的出方向报文，因为先与优先级较高的安全策略表项的 ACL **deny** 规则匹配上，而没有被 IPsec 保护，继而在接收端被丢弃。

下面是一个 **deny** 规则的错误配置示例。Router A 和 Router B 上分别配置如下所示的 IPsec 安全策略，当 Router A 连接的 1.1.2.0/24 网段用户访问 Router B 连接的 3.3.3.0/24 网段时，报文在 Router A 的应用了 IPsec 安全策略 testa 的出接口上优先与顺序号为 1 的安全策略表项匹配，并匹配上了 IPv4 ACL 3000 的 rule 1，因此 Router A 认为它不需要 IPsec 保护，而未进行 IPsec 封装。该报文到达 Router B 后，在应用了 IPsec 安全策略 testb 的入接口上与 IPv4 ACL 3001 的 rule 0 匹配，并被判断为应该受 IPsec 保护但未被保护的报文而丢弃。

Router A 上的关键配置如下：

```
acl advanced 3000
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
 rule 1 deny ip
acl advanced 3001
 rule 0 permit ip source 1.1.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
 rule 1 deny ip
#
ipsec policy testa 1 isakmp <---优先级高的安全策略表项
 security acl 3000
 ike-profile aa
 transform-set 1
#
ipsec policy testa 2 isakmp <---优先级低的安全策略表项
 security acl 3001
 ike-profile bb
 transform-set 1
```

Router B 上的关键配置如下：

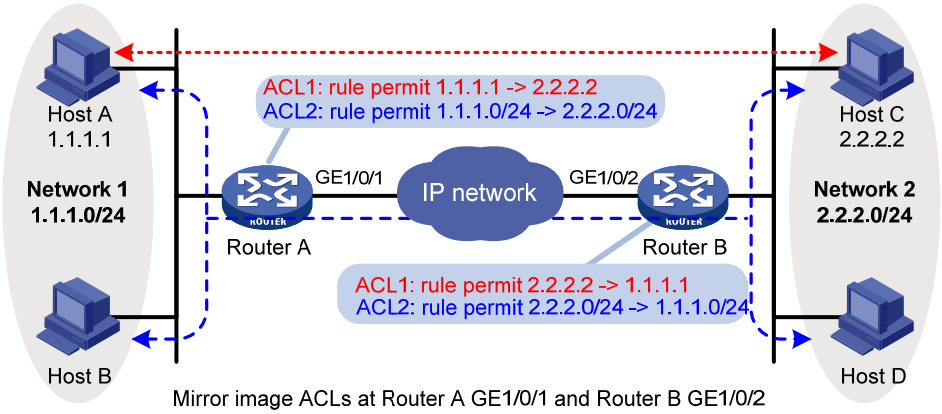
```
acl advanced 3001
 rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 1.1.2.0 0.0.0.255
 rule 1 deny ip
#
ipsec policy testb 1 isakmp
 security acl 3001
 ike-profile aa
 transform-set 1
```

为保证 Router A 连接的 1.1.2.0/24 网段用户访问 Router B 连接的 3.3.3.0/24 网段的报文可被正确处理，建议将 Router A 上的 IPv4 ACL 3000 中的 deny 规则删除。

2. ACL规则的镜像配置

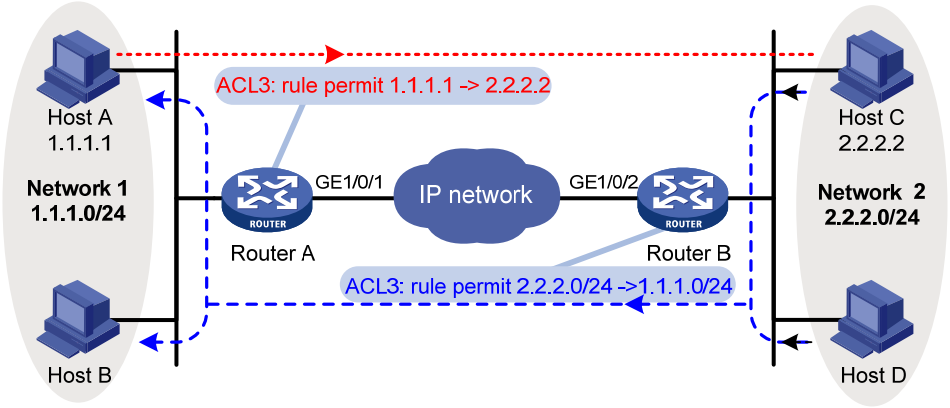
为保证IPsec对等体上能够成功建立SA，建议两端设备上用于IPsec的ACL配置为镜像对称，即保证两端定义的要保护的数据流范围的源和目的尽量对称。例如，图 1-5 中Router A和Router B上的ACL配置都是完全镜像对称的，因此用于保护主机Host A与主机Host C之间、子网Network 1 与子网Network 2 之间流量的SA均可成功建立。

图1-5 镜像 ACL 配置



若IPsec对等体上的ACL配置非镜像，那么只有在一端的ACL规则定义的范围是另外一端的子集时，SA协商可以成功。如 图 1-6 所示，Router A上的ACL规则允许的范围（Host A->Host C）是Router B上ACL规则允许的范围（Network 2->Network 1）的子集。

图1-6 非镜像 ACL 配置



需要注意的是，在这种 ACL 配置下，并不是任何一端发起的 SA 协商都可以成功，仅当保护范围小（细粒度）的一端向保护范围大（粗粒度）的一端发起的协商才能成功，反之则 SA 协商失败。这是因为，协商响应方要求协商发起方发送过来的数据必须在响应方可以接受的范围之内。其结果就是，从细粒度一端向粗粒度一端发送报文时，细粒度侧设备发起的 SA 协商可以成功，例如 Host A->Host C；从粗粒度一方向细粒度一方发送报文时，粗粒度侧设备发起的 SA 协商不能成功，例如 Host C->Host A、Host C->Host B、Host D->Host A 等。

1.3.3 配置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。

可对 IPsec 安全提议进行修改，但对已协商成功的 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。

表1-2 配置 IPsec 安全提议

操作		命令	说明
进入系统视图		**system-view**	-
创建IPsec安全提议，并进入IPsec安全提议视图		**ipsec transform-set** *transform-set-name*	缺省情况下，不存在IPsec安全提议
配置IPsec安全提议采用的安全协议		**protocol** { **ah** | **ah-esp** | **esp** }	缺省情况下，采用ESP安全协议
配置安全算法	配置ESP协议采用的加密算法	**esp encryption-algorithm** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** | **gmac-128** | **gmac-192** | **gmac-256** | **gcm-128** | **gcm-192** | **gcm-256** | **null** } *	只有采用ESP协议（**esp**或**ah-esp**）时必选 缺省情况下，ESP协议未采用加密算法 此命令可以同时配置多个加密算法，算法优先级以配置顺序为准 aes-ctr-128、aes-ctr-192、aes-ctr-256、camellia-cbc-128、camellia-cbc-192、camellia-cbc-256、gmac-128、gmac-192、gmac-256、gcm-128、gcm-192、gcm-256加密算法仅适用于IKEv2协商
	配置ESP协议采用的认证算法	**esp authentication-algorithm** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *	只有采用ESP协议（**esp**或**ah-esp**）时必选 缺省情况下，ESP协议未采用认证算法 此命令可以同时配置多个加密算法，算法优先级以配置顺序为准 aes-xcbc-mac认证算法仅适用于IKEv2协商
	配置AH协议采用的认证算法	**ah authentication-algorithm** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *	只有采用AH（**ah**或**ah-esp**）协议时必选 缺省情况下，AH协议未采用认证算法 此命令可以同时配置多个加密算法，算法优先级以配置顺序为准 aes-xcbc-mac认证算法仅适用于IKEv2协商

操作	命令	说明
配置安全协议对IP报文的封装模式	**encapsulation-mode** { **transport** | **tunnel** }	缺省情况下，安全协议采用隧道模式对IP报文进行封装 传输模式必须应用于数据流的源地址和目的地址与IPsec隧道两端地址相同的情况下
（可选）配置使用IPsec安全策略发起协商时使用PFS特性	**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **dh-group24** | **dh-group19** | **dh-group20** }	缺省情况下，使用IPsec安全策略发起协商时不使用PFS特性 PFS（Perfect Forward Secrecy，完善的前向安全性）特性请参见“安全配置指导”中的“IKE” 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。不配置PFS特性的一端，按照对端的PFS特性要求进行IKE协商
（可选）开启ESN功能	**esn enable** [**both**]	缺省情况下，ESN功能处于关闭状态

1.3.4 配置手工方式的IPsec安全策略

1. 配置限制和指导

为保证 SA 能够成功生成，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 安全提议应采用相同的安全协议、加密/认证算法和报文封装模式。
- 当前端点的 IPv4 对端地址应与对端应用 IPsec 安全策略的接口的主 IPv4 地址保持一致；当前端点的 IPv6 对端地址应与对端应用 IPsec 安全策略的接口的第一个 IPv6 地址保持一致。
- 应分别设置 **inbound** 和 **outbound** 两个方向的 IPsec SA 参数，且保证每一个方向上的 IPsec SA 的唯一性：对于出方向 IPsec SA，必须保证三元组（对端 IP 地址、安全协议、SPI）唯一；对于入方向 IPsec SA，必须保证 SPI 唯一。
- 本端和对端 IPsec SA 的 SPI 及密钥必须是完全匹配的。即，本端的入方向 IPsec SA 的 SPI 及密钥必须和对端的出方向 IPsec SA 的 SPI 及密钥相同；本端的出方向 IPsec SA 的 SPI 及密钥必须和对端的入方向 IPsec SA 的 SPI 及密钥相同。
- 两端 IPsec SA 使用的密钥应当以相同的方式输入，即如果一端以字符串方式输入密钥，另一端必须也以字符串方式输入密钥。

2. 配置手工方式的IPsec安全策略

表1-3 配置手工方式的 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
创建一条手工方式的IPsec安全策略，并进入IPsec安全策略视图	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **manual**	缺省情况下，不存在IPsec安全策略
（可选）配置IPsec安全策略的描述信息	**description** *text*	缺省情况下，无描述信息

操作		命令	说明
指定IPsec安全策略引用的ACL		**security acl** [**ipv6**] { *acl-number* | **name** *acl-name* }	缺省情况下，IPsec安全策略未引用ACL 一条安全策略只能引用一个ACL
指定IPsec安全策略所引用的安全提议		**transform-set** *transform-set-name*	缺省情况下，IPsec安全策略未引用IPsec安全提议 一条手工方式的IPsec安全策略只能引用一个安全提议
指定IPsec隧道的对端IP地址		**remote-address** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定IPsec隧道的对端地址 IPsec隧道的本端IPv4地址为应用安全策略的接口的主IP地址；本端IPv6地址为应用安全策略的接口的第一个IPv6地址
配置IPsec SA的入方向SPI		**sa spi inbound** { **ah** | **esp** } *spi-number*	缺省情况下，不存在IPsec SA的入方向SPI
配置IPsec SA的出方向SPI		**sa spi outbound** { **ah** | **esp** } *spi-number*	缺省情况下，不存在IPsec SA的出方向SPI
配置IPsec SA使用的密钥	配置AH协议的认证密钥（以16进制方式输入）	**sa hex-key authentication** { **inbound** | **outbound** } **ah** { **cipher** | **simple** } *string*	缺省情况下，未配置IPsec SA使用的密钥 根据本安全策略引用的安全提议中指定的安全协议，配置AH协议或ESP协议的密钥，或者两者都配置 对于ESP协议，以字符串方式输入密钥时，系统会自动地同时生成认证算法的密钥和加密算法的密钥 如果先后以不同的方式输入了密钥，则最后设定的密钥有效
	配置AH协议的认证密钥（以字符串方式输入）	**sa string-key** { **inbound** | **outbound** } **ah** { **cipher** | **simple** } *string*	
	配置ESP协议的认证密钥和加密密钥（以字符串方式输入）	**sa string-key** { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *string*	
	配置ESP协议的认证密钥（以16进制方式输入）	**sa hex-key authentication** { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *string*	
	配置ESP协议的加密密钥（以16进制方式输入）	**sa hex-key encryption** { **inbound** | **outbound** } **esp** { **cipher** | **simple** } *string*	

1.3.5 配置IKE协商方式的IPsec安全策略

IKE 协商方式的 IPsec 安全策略有以下两种配置方式：

- 直接配置 IPsec 安全策略：在安全策略视图中定义需要协商的各参数；
- 引用 IPsec 安全策略模板配置 IPsec 安全策略：首先在 IPsec 安全策略模板中定义需要协商的各参数，然后通过引用 IPsec 安全策略模板创建一条 IPsec 安全策略。应用了该类 IPsec 安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。由于 IPsec 安全策略模板中未定义的可选参数由发起方来决定，而响应方会接受发起方的建议，因此这种方式适用于通信对端（例如对端的 IP 地址）未知的情况下，允许这些对端设备向本端设备主动发起协商。

1. 配置限制和指导

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 安全提议中应包含具有相同的安全协议、认证/加密算法和报文封装模式的 IPsec 安全提议。
- 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。IKE 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的本端地址应保持一致。

对于 IKE 协商建立的 IPsec SA，遵循以下原则：

- 采用隧道两端设置的 IPsec SA 生存时间中较小者。
- 可同时存在基于时间和基于流量两种方式的 IPsec SA 生存时间，只要到达指定的时间或指定的流量，IPsec SA 就会老化。

2. 直接配置IKE协商方式的IPsec安全策略

表1-4 直接配置 IKE 协商方式的 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
创建一条IKE协商方式的IPsec安全策略，并进入IPsec安全策略视图	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp**	缺省情况下，不存在IPsec安全策略
（可选）配置IPsec安全策略的描述信息	**description** *text*	缺省情况下，无描述信息
指定IPsec安全策略引用的ACL	**security acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**aggregation** | **per-host**]	缺省情况下，IPsec安全策略没有指定ACL 一条IPsec安全策略只能引用一个ACL
指定IPsec安全策略引用的IPsec安全提议	**transform-set** *transform-set-name*&<1-6>	缺省情况下，IPsec安全策略未引用IPsec安全提议
指定IPsec安全策略引用的IKE profile	**ike-profile** *profile-name*	缺省情况下，IPsec安全策略未引用IKE profile。若系统视图下配置了IKE profile，则使用系统视图下配置的IKE profile进行性协商，否则使用全局的IKE参数进行协商 只能引用一个IKE profile IKE profile的相关配置请参见“安全配置指导”中的“IKE”
指定IPsec安全策略引用的IKEv2 profile	**ikev2-profile** *profile-name*	缺省情况下，IPsec安全策略未引用IKEv2 profile。 只能引用一个IKEv2 profile IKEv2 profile的相关配置请参见“安全配置指导”中的“IKEv2”

操作	命令	说明
指定IPsec隧道的本端IP地址	**local-address** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，IPsec隧道的本端IPv4地址为应用IPsec安全策略的接口的主IPv4地址，本端IPv6地址为应用IPsec安全策略的接口的第一个IPv6地址 此处指定的IPsec隧道本端IP地址必须与IKE使用的标识本端身份的IP地址一致 在VRRP组网环境中，必须指定IPsec隧道本端的IP地址为应用IPsec安全策略的接口所在备份组的虚拟IP地址
指定IPsec隧道的对端IP地址	**remote-address** { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定IPsec隧道的对端IP地址
配置IPsec SA的生存时间	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec安全策略下的IPsec SA生存时间为当前全局的IPsec SA生存时间
（可选）配置IPsec SA的空闲超时时间	**sa idle-time** *seconds*	缺省情况下，IPsec安全策略下的IPsec SA空闲超时时间为当前全局的IPsec SA空闲超时时间
（可选）开启TFC（Traffic Flow Confidentiality）填充功能	**tfc enable**	缺省情况下，TFC填充功能处于关闭状态
退回系统视图	**quit**	-
配置全局的IPsec SA生存时间	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec SA基于时间的生存时间为3600秒，基于流量的生存时间为1843200千字节
（可选）开启全局的IPsec SA空闲超时功能，并配置全局IPsec SA空闲超时时间	**ipsec sa idle-time** *seconds*	缺省情况下，全局的IPsec SA空闲超时功能处于关闭状态

3. 引用IPsec安全策略模板配置IKE协商方式的IPsec安全策略

IPsec 安全策略模板与直接配置的 IKE 协商方式的 IPsec 安全策略中可配置的参数类似，但是配置较为简单，除了 IPsec 安全提议和 IKE profile 之外的其它参数均为可选。应用了引用 IPsec 安全策略模板配置的 IPsec 安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。IPsec 安全策略模板中未定义的可选参数由发起方来决定，而响应方会接受发起方的建议，例如 IPsec 安全策略模板下的用于定义保护对象范围的 ACL 是可选的，该参数在未配置的情况下，相当于支持最大范围的保护，即完全接受协商发起端的 ACL 设置。这种方式配置的 IPsec 安全策略适用于通信对端（例如对端的 IP 地址）未知的情况下，允许这些对端设备向本端设备主动发起协商。

表1-5 引用 IPsec 安全策略模板配置 IKE 协商方式的 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建一个IPsec安全策略模板，并进入IPsec安全策略模板视图	**ipsec** { **ipv6-policy-template** | **policy-template** } *template-name seq-number*	缺省情况下，不存在IPsec安全策略模板
（可选）配置IPsec安全策略模板的描述信息	**description** *text*	缺省情况下，无描述信息
（可选）指定IPsec安全策略模板引用的ACL	**security acl** [**ipv6**] { *acl-number* | **name** *acl-name* } [**aggregation** | **per-host**]	缺省情况下，IPsec安全策略模板没有指定ACL 一条IPsec安全策略模板只能引用一个ACL
指定IPsec安全策略模板引用的安全提议	**transform-set** *transform-set-name*&<1-6>	缺省情况下IPsec安全策略模板未引用IPsec安全提议
指定IPsec安全策略模板引用的IKE profie	**ike-profile** *profile-name*	缺省情况下，IPsec安全策略模板未引用IKE profie 只能引用一个IKE profile，且不能引用已经被其它IPsec安全策略或IPsec安全策略模板引用的IKE profie IKE profile的相关配置请参见“安全配置指导”中的“IKE”
指定IPsec安全策略模板引用的IKEv2 profile	**ikev2-profile** *profile-name*	缺省情况下，IPsec安全策略未引用IKEv2 profile。 只能引用一个IKEv2 profile IKEv2 profile的相关配置请参见“安全配置指导”中的“IKEv2”
（可选）指定IPsec隧道的本端IP地址	**local-address** { *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，IPsec隧道的本端IPv4地址为应用IPsec安全策略的接口的主IPv4地址，本端IPv6地址为应用IPsec安全策略的接口的第一个IPv6地址 此处指定的IPsec隧道本端IP地址必须与IKE对等体使用的标识本端身份的IP地址一致 在VRRP组网环境中，必须指定IPsec隧道本端的IP地址为应用IPsec安全策略的接口所在备份组的虚拟IP地址
（可选）指定IPsec隧道的对端IP地址	**remote-address** { [**ipv6**] *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定IPsec隧道的对端IP地址
（可选）配置IPsec SA的生存时间	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec安全策略模板下的IPsec SA生存时间为当前全局的IPsec SA生存时间
（可选）配置IPsec SA的空闲超时时间	**sa idle-time** *seconds*	缺省情况下，IPsec安全策略模板下的IPsec SA空闲超时时间为当前全局的IPsec SA空闲超时时间
（可选）开启TFC（Traffic Flow Confidentiality）填充功能	**tfc enable**	缺省情况下，TFC填充功能处于关闭状态

操作	命令	说明
退回系统视图	**quit**	-
（可选）配置全局的IPsec SA生存时间	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	缺省情况下，IPsec SA基于时间的生存时间为3600秒，基于流量的生存时间为1843200千字节
（可选）开启全局的IPsec SA空闲超时功能，并配置全局IPsec SA空闲超时时间	**ipsec sa idle-time** *seconds*	缺省情况下，全局的IPsec SA空闲超时功能处于关闭状态
引用安全策略模板创建一条IKE协商方式的安全策略	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **isakmp template** *template-name*	缺省情况下，不存在IPsec安全策略

1.3.6 在接口上应用IPsec安全策略

为使定义的 IPsec SA 生效，应在每个要加密的数据流和要解密的数据流所在接口上应用一个 IPsec 安全策略，以对数据进行保护。当取消 IPsec 安全策略在接口上的应用后，此接口便不再具有 IPsec 的安全保护功能。IPsec 安全策略除了可以应用到串口、以太网接口等实际物理接口上之外，还能够应用到 Virtual Template 等虚接口上。

当从一个接口发送数据时，接口将按照顺序号从小到大的顺序逐一匹配引用的 IPsec 安全策略中的每一条安全策略表项。如果数据匹配上了某一条安全策略表项引用的 ACL，则停止匹配，并对其使用当前这条安全策略表项进行处理，即根据已经建立的 IPsec SA 或者触发 IKE 协商生成的 IPsec SA 对报文进行封装处理；如果数据与所有安全策略表项引用的 ACL 都不匹配，则直接被正常转发，IPsec 不对数据加以保护。

应用了 IPsec 安全策略的接口收到数据报文时，对于目的地址是本机的 IPsec 报文，根据报文头里携带的 SPI 查找本地的 IPsec SA，并根据匹配的 IPsec SA 对报文进行解封装处理；对于那些本应该被 IPsec 保护但未被保护的报文进行丢弃。

表1-6 在接口上应用 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
应用IPsec安全策略	**ipsec apply** { **policy** | **ipv6-policy** } *policy-name*	缺省情况下，接口上未应用IPsec安全策略 一个接口下最多只能应用一个IPv4/IPv6类型的IPsec安全策略，但可以同时应用一个IPv4类型的IPsec安全策略和一个IPv6类型的IPsec安全策略。IKE方式的IPsec安全策略可以应用到多个接口上，但建议只应用到一个接口上；手工方式的IPsec安全策略只能应用到一个接口上

1.3.7 配置解封装后IPsec报文的ACL检查功能

在隧道模式下，接口入方向上解封装的 IPsec 报文的内部 IP 头有可能不在当前 IPsec 安全策略引用的 ACL 的保护范围内，如网络中一些恶意伪造的攻击报文就可能有此问题，所以设备需要重新检查解封装后的报文的 IP 头是否在 ACL 保护范围内。开启该功能后可以保证 ACL 检查不通过的报文被丢弃，从而提高网络安全性。

表1-7 配置解封装后 IPsec 报文的 ACL 检查功能

操作	命令	说明
进入系统视图	**system-view**	-
开启解封装后IPsec报文的ACL检查功能	**ipsec decrypt-check enable**	缺省情况下，解封装后IPsec报文的ACL检查功能处于开启状态

1.3.8 配置IPsec抗重放功能

注意

IPsec 抗重放检测功能缺省是开启的，是否关闭该功能请根据实际需求慎重使用。使用较大的抗重放窗口宽度会引起系统开销增大，导致系统性能下降，与抗重放检测用于降低系统在接收重放报文时的开销的初衷不符，因此建议在能够满足业务运行需要的情况下，使用较小的抗重放窗口宽度。

重放报文，通常是指设备再次接收到的已经被 IPsec 处理过的报文。IPsec 通过滑动窗口（抗重放窗口）机制检测重放报文。AH 和 ESP 协议报文中带有序列号，如果收到的报文的序列号与已经解封装过的报文序列号相同，或收到的报文的序列号出现得较早，即已经超过了抗重放窗口的范围，则认为该报文为重放报文。

对重放报文的解封装无意义，并且解封装过程涉及密码学运算，会消耗设备大量的资源，导致业务可用性下降，造成了拒绝服务攻击。通过开启 IPsec 抗重放检测功能，将检测到的重放报文在解封装处理之前丢弃，可以降低设备资源的消耗。

在某些特定环境下，业务数据报文的接收顺序可能与正常的顺序差别较大，虽然并非有意的重放攻击，但会被抗重放检测认为是重放报文，导致业务数据报文被丢弃，影响业务的正常运行。因此，这种情况下就可以通过关闭 IPsec 抗重放检测功能来避免业务数据报文的错误丢弃，也可以通过适当地增大抗重放窗口的宽度，来适应业务正常运行的需要。

只有 IKE 协商的 IPsec SA 才能够支持抗重放检测，手工方式生成的 IPsec SA 不支持抗重放检测。因此该功能开启与否对手工方式生成的 IPsec SA 没有影响。

表1-8 配置 IPsec 抗重放功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPsec抗重放检测功能	**ipsec anti-replay check**	缺省情况下，IPsec抗重放检测功能处于开启状态

操作	命令	说明
（可选）配置IPsec抗重放窗口宽度	**ipsec anti-replay window** *width*	缺省情况下，IPsec抗重放窗口宽度为64

1.3.9 配置IPsec抗重放窗口和序号的同步功能

IPsec 抗重放窗口和序号的同步功能是指，以指定的报文间隔将接口上 IPsec 入方向抗重放窗口的左侧值和出方向 IPsec 报文的抗重放序号进行备份。当配置了防重放窗口和序号的同步间隔的 IPsec 安全策略被应到接口上时，若 IPsec 冗余备份功能处于开启状态，则可以保证主备切换时 IPsec 流量不间断和抗重放保护不间断。

表1-9 配置 IPsec 抗重放序号同步功能

操作		命令	说明
进入系统视图		**system-view**	-
开启IPsec冗余备份功能		**ipsec redundancy enable**	缺省情况下，IPsec冗余备份功能处于关闭状态
进入相应视图	IPsec安全策略视图	**ipsec** { **policy** | **ipv6-policy** } *policy-name seq-number* [**isakmp** | **manual**]	-
	IPsec安全策略模板视图	**ipsec** { **policy-template** | **ipv6-policy-template** } *template-name seq-number*	
（可选）配置防重放窗口和序号的同步间隔		**redundancy replay-interval inbound** *inbound-interval* **outbound** *outbound-interval*	缺省情况下，同步入方向防重放窗口的报文间隔为1000，同步出方向IPsec SA防重放序号的报文间隔为100000

1.3.10 配置共享源接口IPsec安全策略

为了提高网络的可靠性，通常核心设备到 ISP（Internet Service Provider，互联网服务提供商）都会有两条出口链路，它们互为备份或者为负载分担的关系。由于在不同的接口上应用安全策略时，各个接口将分别协商生成 IPsec SA。因此，则在主备链路切换时，接口状态的变化会触发重新进行 IKE 协商，从而导致数据流的暂时中断。这种情况下，两个接口上的 IPsec SA 就需要能够平滑切换。

通过将一个 IPsec 安全策略与一个源接口绑定，使之成为共享源接口 IPsec 安全策略，可以实现主备链路切换时受 IPsec 保护的业务流量不中断。具体机制为：应用相同 IPsec 安全策略的多个物理接口共同使用一个指定的源接口（称为共享源接口）协商 IPsec SA，当这些物理接口对应的链路切换时，如果该源接口的状态不变化，就不会删除该接口协商出的 IPsec SA，也不需要重新触发 IKE 协商，各物理接口继续使用已有的 IPsec SA 保护业务流量。

对于本配置，有以下配置限制和注意事项：

- 只有 IKE 协商方式的 IPsec 安全策略才能配置为 IPsec 共享源接口安全策略。
- 一个 IPsec 安全策略只能与一个源接口绑定。
- 一个源接口可以同时与多个 IPsec 安全策略绑定。

- 删除与共享源接口 IPsec 安全策略绑定的共享源接口时，将使得该共享源接口 IPsec 安全策略恢复为普通 IPsec 安全策略。
- 若一个 IPsec 安全策略为共享源接口 IPsec 安全策略，但该 IPsec 安全策略中未指定隧道本端地址，则 IKE 将使用共享源接口地址作为 IPsec 隧道的本端地址进行 IKE 协商；如果共享源接口 IPsec 安全策略中指定了隧道本端地址，则将使用指定的隧道本端地址进行 IKE 协商。

表1-10 配置共享源接口 IPsec 安全策略

操作	命令	说明
进入系统视图	**system-view**	-
配置IPsec安全策略为IPsec共享源接口安全策略	**ipsec** { **ipv6-policy** | **policy** } *policy-name* **local-address** *interface-type interface-number*	缺省情况下，IPsec安全策略不是共享源接口IPsec安全策略，即未将IPsec安全策略与源接口绑定

1.3.11 配置QoS预分类功能

注意

若在接口上同时配置IPsec和QoS，同一个IPsec SA保护的数据流如果被QoS分类进入不同队列，会导致部分报文发送乱序。由于IPsec具有抗重放功能，IPsec入方向上对于抗重放窗口之外的报文会进行丢弃，从而导致丢包现象。因此当IPsec与QoS配合使用时，必须保证IPsec分类与QoS分类规则配置保持一致。

当在接口上同时应用了 IPsec 安全策略与 QoS 策略时，缺省情况下，QoS 使用封装后报文的外层 IP 头信息来对报文进行分类。但如果希望 QoS 基于被封装报文的原始 IP 头信息对报文进行分类，则需要配置 QoS 预分类功能来实现。

IPsec 的分类规则完全由引用的 ACL 规则确定，QoS 策略及 QoS 分类的相关介绍请参见“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

表1-11 配置 QoS 预分类功能

操作		命令	说明
进入系统视图		**system-view**	-
进入相应视图	IPsec安全策略视图	**ipsec** { **policy** | **ipv6-policy** } *policy-name seq-number* [**isakmp** | **manual**]	-
	IPsec安全策略模板视图	**ipsec** { **policy-template** | **ipv6-policy-template** } *template-name seq-number*	
开启QoS预分类功能		**qos pre-classify**	缺省情况下，QoS预分类功能处于关闭状态

1.3.12 配置IPsec报文日志信息记录功能

开启 IPsec 报文日志记录功能后，设备会在丢弃 IPsec 报文的情况下，例如入方向找不到对应的 IPsec SA、AH/ESP 认证失败、ESP 加密失败等时，输出相应的日志信息，该日志信息内容主要包括报文的源和目的 IP 地址、报文的 SPI 值、报文的序列号信息，以及设备丢包的原因。

表1-12 配置 IPsec 日志信息记录功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPsec报文日志记录功能	**ipsec logging packet enable**	缺省情况下，IPsec报文日志记录功能处于关闭状态

1.3.13 设置IPsec隧道模式下封装后外层IP头的DF位

IP 报文头中的 DF（Don't Fragment，不分片）位用于控制报文是否允许被分片。在隧道模式下，IPsec 会在原始报文外封装一个新的 IP 头，称为外层 IP 头。IPsec 的 DF 位设置功能允许用户设置 IPsec 封装后的报文外层 IP 头的 DF 位，并支持以下三种设置方式：

- **clear**：表示清除外层 IP 头的 DF 位，IPsec 封装后的报文可被分片。
- **set**：表示设置外层 IP 头的 DF 位，IPsec 封装后的报文不能被分片。
- **copy**：表示外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

封装后外层 IP 头的 DF 位可以在接口视图和系统视图下分别配置，接口视图下的配置优先级高。如果接口下未设置外层 IP 头的 DF 位，则按照系统视图下的全局配置来决定如何设置封装后外层 IP 头的 DF 位。

对于本配置，有以下配置限制和注意事项：

- 该功能仅在 IPsec 的封装模式为隧道模式时有效，仅用于设置 IPsec 隧道模式封装后的外层 IP 头的 DF 位，原始报文 IP 头的 DF 位不会被修改。
- 如果有多个接口应用了共享源接口安全策略，则这些接口上必须使用相同的 DF 位设置。
- 转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后 IPsec 报文的 DF 位，则不允许对 IPsec 报文进行分片，可以避免引入分片延时。这种情况下，要求 IPsec 报文转发路径上各个接口的 MTU 大于 IPsec 报文长度，否则，会导致 IPsec 报文被丢弃。如果无法保证转发路径上各个接口的 MTU 大于 IPsec 报文长度，则建议清除 DF 位。

表1-13 在接口下设置 IPsec 封装后外层 IP 头的 DF 位

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
为当前接口设置IPsec封装后外层IP头的DF位	**ipsec df-bit** { **clear** | **copy** | **set** }	缺省情况下，接口下未设置IPsec封装后外层IP头的DF位，采用全局设置的DF位

表1-14 全局设置 IPsec 封装后外层 IP 头的 DF 位

操作	命令	说明
进入系统视图	**system-view**	-
为所有接口设置IPsec封装后外层IP头的DF位	**ipsec global-df-bit** { **clear** | **copy** | **set** }	缺省情况下，IPsec封装后外层IP头的DF位从原始报文IP头中拷贝

1.3.14 配置IPsec反向路由注入功能

在企业中心侧网关设备上的 IPsec 安全策略视图/IPsec 安全策略模板视图下开启 IPsec 反向路由注入（RRI）功能后，设备会根据协商的 IPsec SA 自动生成一条静态路由，该路由的目的地址为受保护的对端私网，下一跳地址为 IPsec 隧道的对端地址。对于 RRI 生成的静态路由，可以为其配置优先级，从而更灵活地应用路由管理策略。例如：当设备上还有其他方式配置到达相同目的地的路由时，如果为它们指定相同的优先级，则可实现负载分担，如果指定不同的优先级，则可实现路由备份。同时，还可以通过修改静态路由的 Tag 值，使得设备能够在路由策略中根据 Tag 值对这些 RRI 生成的静态路由进行灵活的控制。

需要注意的是：

- 开启 RRI 功能时，会删除相应 IPsec 安全策略协商出的所有 IPsec SA。当有新的流量触发生成 IPsec SA 时，根据新协商的 IPsec 生成路由信息。
- 关闭 RRI 功能时，会删除相应 IPsec 安全策略协商出的所有 IPsec SA。
- RRI 生成的静态路由随 IPsec SA 的创建而创建，随 IPsec SA 的删除而删除。
- RRI 功能在隧道模式和传输模式下都支持。
- 若修改了 RRI 生成的静态路由的优先级或 Tag 属性，则会删除由相应 IPsec 安全策略建立的 IPsec SA 和已添加的静态路由，修改后的属性值在下次生成 IPsec SA 且添加静态路由时生效。
- 在 RRI 功能开启的情况下，对于与未指定目的 IP 地址的 ACL 规则相匹配的报文流触发协商出的 IPsec SA，设备并不会为其自动生成一条静态路由。因此，如果 IPsec 安全策略/IPsec 安全策略模板引用了此类型的 ACL 规则，则需要通过手工配置一条到达对端受保护网络的静态路由。

表1-15 配置 IPsec 反向路由注入功能

操作	命令	说明
进入系统视图	**system-view**	-
进入IPsec安全策略视图	**ipsec** { **policy** | **ipv6-policy** } *policy-name seq-number* **isakmp**	二者选其一
进入IPsec安全策略模板视图	**ipsec** { **policy-template** | **ipv6-policy-template** } *template-name seq-number*	
开启IPsec反向路由注入功能	**reverse-route dynamic**	缺省情况下，IPsec反向路由注入功能处于关闭状态
（可选）配置IPsec反向路由功能生成的静态路由的优先级	**reverse-route preference** *number*	缺省情况下，IPsec反向路由注入功能生成的静态路由的优先级为60

操作	命令	说明
（可选）配置IPsec反向路由功能生成的静态路由的Tag值	**reverse-route tag** *tag-value*	缺省情况下，IPsec反向路由注入功能生成的静态路由的tag值为0

1.4 配置IPsec告警功能

开启 IPsec 的 Trap 功能后，IPsec 会生成告警信息，用于向网管软件报告该模块的重要事件。生成的告警信息将被发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

如果希望生成并输出某种类型的 IPsec 告警信息，则需要保证 IPsec 的全局告警功能以及相应类型的告警功能均处于开启状态。

表1-16 配置 IPsec 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPsec的全局告警功能	**snmp-agent trap enable ipsec global**	缺省情况下，IPsec的全局告警功能处于关闭状态
开启IPsec的指定告警功能	**snmp-agent trap enable ipsec** [**auth-failure** | **decrypt-failure** | **encrypt-failure** | **invalid-sa-failure** | **no-sa-failure** | **policy-add** | **policy-attach** | **policy-delete** | **policy-detach** | **tunnel-start** | **tunnel-stop**] *	缺省情况下，IPsec的所有告警功能均处于关闭状态

1.5 配置IPsec分片功能

通过配置 IPsec 分片功能，可以选择在报文进行 IPsec 封装之前是否进行分片：

- IPsec 封装前分片功能处于开启状态时，设备会先判断报文在经过 IPsec 封装之后大小是否会超过发送接口的 MTU 值，如果封装后的大小超过发送接口的 MTU 值，那么会先对其分片再封装。
- IPsec 封装后分片功能处于开启状态时，无论报文封装后大小是否超过发送接口的 MTU 值，设备会直接对其先进行 IPsec 封装处理，再由后续业务对其进行分片。
- 该功能仅对需要进行 IPsec 封装的 IPv4 报文有效。

表1-17 配置 IPsec 分片功能

操作	命令	说明
进入系统视图	**system-view**	-
配置IPsec分片功能	**ipsec fragmentation** { **after-encryption** | **before-encryption** }	缺省情况下，IPsec封装前分片功能处于开启状态

1.6 配置本端允许建立IPsec隧道的最大数

本端允许建立 IPsec 隧道的最大数与内存资源有关。内存充足时可以设置较大的数值，提高 IPsec 的并发性能；内存不足时可以设置较小的数值，降低 IPsec 占用内存的资源。

表1-18 配置本端允许建立 IPsec 隧道的最大数

操作	命令	说明
进入系统视图	**system-view**	-
配置本端允许建立IPsec隧道的最大数	**ipsec limit max-tunnel** *tunnel-limit*	缺省情况下，不限制本端允许建立IPsec隧道的最大数

1.7 开启IPsec协商事件日志功能

开启 IPsec 协商事件日志记录功能后，设备会输出 IPsec 协商过程中的相关日志。

表1-19 开启 IPsec 协商事件日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IPsec协商事件日志功能	**ipsec logging negotiation enable**	缺省情况下，IPsec协商事件日志功能处于关闭

1.8 IPsec显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IPsec 的运行情况，通过查看显示信息认证配置的效果。

在用户视图下执行 **reset** 命令可以清除 IPsec 统计信息。

表1-20 IPsec 显示和维护

操作	命令
显示IPsec安全策略的信息	**display ipsec** { **ipv6-policy** | **policy** } [*policy-name* [*seq-number*]]
显示IPsec安全策略模板的信息	**display ipsec** { **ipv6-policy-template** | **policy-template** } [*template-name* [*seq-number*]]
显示IPsec安全提议的信息	**display ipsec transform-set** [*transform-set-name*]
显示IPsec SA的相关信息	**display ipsec sa** [**brief** | **count** | **interface** *interface-type interface-number* | { **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **remote** [**ipv6**] *ip-address*]
显示IPsec处理报文的统计信息	**display ipsec statistics** [**tunnel-id** *tunnel-id*]
显示IPsec隧道的信息	**display ipsec tunnel** { **brief** | **count** | **tunnel-id** *tunnel-id* }

操作	命令
清除已经建立的IPsec SA	**reset ipsec sa** [{ **ipv6-policy** | **policy** } *policy-name* [*seq-number*] | **remote** { *ipv4-address* | **ipv6** *ipv6-address* } | **spi** { *ipv4-address* | **ipv6** *ipv6-address* } { **ah** | **esp** } *spi-num*]
清除IPsec的报文统计信息	**reset ipsec statistics** [**tunnel-id** *tunnel-id*]

2 IKE

说明

若无特殊说明，本文中的 IKE 均指第 1 版本的 IKE 协议。

2.1 IKE简介

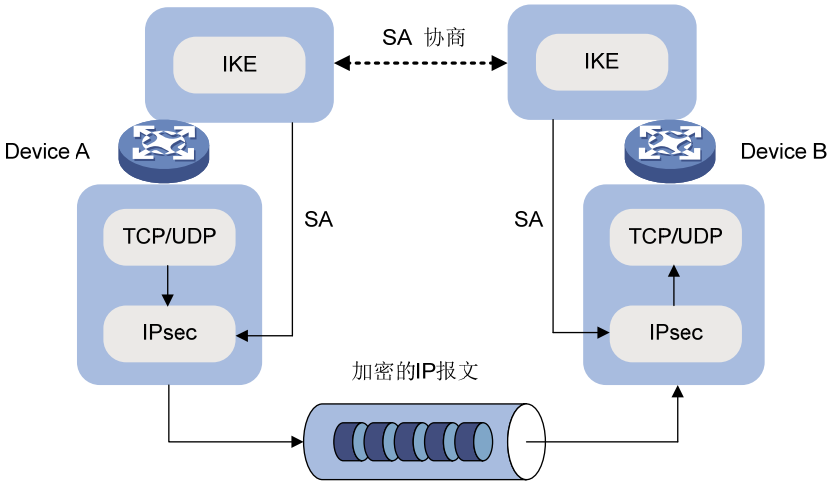
IKE（Internet Key Exchange，互联网密钥交换）协议利用 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）语言定义密钥交换的过程，是一种对安全服务进行协商的手段。

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。IKE 为 IPsec 提供了自动建立 IPsec SA 的服务，具体有以下优点。

- IKE 首先会在通信双方之间协商建立一个安全通道（IKE SA），并在此安全通道的保护下协商建立 IPsec SA，这降低了手工配置的复杂度，简化 IPsec 的配置和维护工作。
- IKE 的精髓在于 DH（Diffie-Hellman）交换技术，它通过一系列的交换，使得通信双方最终计算出共享密钥。在 IKE 的 DH 交换过程中，每次计算和产生的结果都是不相关的。由于每次 IKE SA 的建立都运行了 DH 交换过程，因此就保证了每个通过 IKE 协商建立的 IPsec SA 所使用的密钥互不相关。
- IPsec 使用 AH 或 ESP 报文头中的顺序号实现防重放。此顺序号是一个 32 比特的值，此数溢出之前，为实现防重放，IPsec SA 需要重新建立，IKE 可以自动重协商 IPsec SA。

如 图 2-1 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。

图2-1 IPsec 与 IKE 的关系图



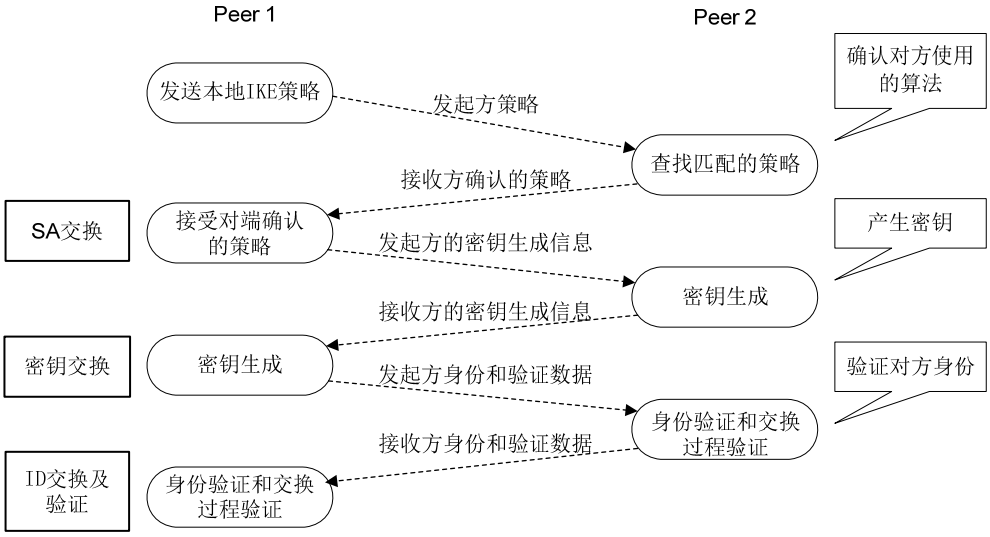
2.1.2 IKE的协商过程

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（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。

(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。

图2-2 主模式交换过程



如 图 2-2 所示，第一阶段主模式的IKE协商过程中包含三对消息，具体内容如下：

- 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 Diffie-Hellman 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。

2.1.3 IKE的安全机制

IKE 可以在不安全的网络上安全地认证通信双方的身份、分发密钥以及建立 IPsec SA，具有以下几种安全机制。

1. 身份认证

IKE 的身份认证机制用于确认通信双方的身份。设备支持三种认证方法：预共享密钥认证、RSA 数字签名认证和 DSA 数字签名认证。

- 预共享密钥认证：通信双方通过共享的密钥认证对端身份。

- 数字签名认证：通信双方使用由 CA 颁发的数字证书向对端证明自己的身份。

2. DH算法

DH 算法是一种公共密钥算法，它允许通信双方在不传输密钥的情况下通过交换一些数据，计算出共享的密钥。即使第三方（如黑客）截获了双方用于计算密钥的所有交换数据，由于其复杂度很高，也不足以计算出双方的密钥。

3. PFS特性

PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，它解决了密钥之间相互无关性的需求。由于 IKE 第二阶段协商需要从第一阶段协商出的密钥材料中衍生出用于 IPsec SA 的密钥，若攻击者能够破解 IKE SA 的一个密钥，则会非常容易得掌握其衍生出的任何 IPsec SA 的密钥。使用 PFS 特性后，IKE 第二阶段协商过程中会增加一次 DH 交换，使得 IKE SA 的密钥和 IPsec SA 的密钥之间没有派生关系，即使 IKE SA 的其中一个密钥被破解，也不会影响它协商出的其它密钥的安全性。

2.1.4 协议规范

与 IKE 相关的协议规范有：

- RFC2408：Internet Security Association and Key Management Protocol (ISAKMP)
- RFC2409：The Internet Key Exchange (IKE)
- RFC2412：The OAKLEY Key Determination Protocol
- Internet-Draft：draft-ietf-ipsec-isakmp-xauth-06.txt
- Internet-Draft：draft-dukes-ike-mode-cfg-02.txt

2.2 IKE配置任务简介

进行 IKE 配置之前，用户需要确定以下几个因素，以便配置过程的顺利进行。

(1) 确定 IKE 交换过程中安全保护的强度，包括认证方法、加密算法、认证算法、DH group。

- 认证方法分为预共享密钥认证和数字签名认证。预共享密钥认证机制简单、不需要证书，常在小型组网环境中使用；数字签名认证安全性更高，常在“中心—分支”模式的组网环境中使用。例如，在“中心—分支”组网中使用预共享密钥认证进行 IKE 协商时，中心侧可能需要为每个分支配置一个预共享密钥，当分支很多时，配置会很复杂，而使用数字签名认证时只需配置一个 PKI 域。
- 不同认证/加密算法的强度不同，算法强度越高，受保护数据越难被破解，但消耗的计算资源越多。
- DH group 位数越大安全性越高，但是处理速度会相应减慢。应该根据实际组网环境中对安全性和性能的要求选择合适的 DH group。

(2) 确定通信双方预先约定的预共享密钥或所属的 PKI 域。关于 PKI 的配置，请参见“安全配置指导”中的“PKI”。

(3) 确定通信双方都采用 IKE 协商模式的 IPsec 安全策略。IPsec 安全策略中若不引用 IKE profile，则使用系统视图下配置的 IKE profile 进行协商，若系统视图下没有任何 IKE profile，则使用全局的 IKE 参数进行协商。关于 IPsec 安全策略的配置，请参见“安全配置指导”中的“IPsec”。

表2-1 IKE 配置任务简介

配置任务	说明	详细配置
配置IKE profile	可选	2.3
配置IKE提议	可选 若IKE profile中需要指定IKE提议，则必配	2.4
配置IKE keychain	可选 若IKE第一阶段协商为预共享密钥认证方式，则必配	2.5
配置本端身份信息	可选	2.6
配置IKE Keepalive功能	可选	2.7
配置IKE NAT Keepalive功能	可选	2.8
配置IKE DPD探测功能	可选	2.9
配置针对无效IPsec SPI的IKE SA恢复功能	可选	2.10
配置对IKE SA数目的限制	可选	2.11
配置为对端分配IPv4地址的IKE本地地址池	可选	2.12
配置IKE告警功能	可选	2.13
开启IKE协商事件日志功能	可选	2.14

2.3 配置IKE profile

IKE profile 中包括以下配置：

(1) 匹配对端身份的规则。响应方首先需要根据发起方的身份信息查找一个本端的 IKE profile，然后使用此 IKE profile 中的信息验证对端身份，发起方同样需要根据响应方的身份信息查找到一个 IKE profile 用于验证对端身份。对端身份信息若能满足本地某个 IKE profile 中指定的匹配规则，则该 IKE profile 为查找的结果。

(2) 根据 IKE 提议中配置的认证方法，配置 IKE keychain 或 PKI 域。

- 如果认证方法为数字签名（**dsa-signature** 或者 **rsa-signature**），则需要配置 PKI 域。
- 如果指定的认证方式为预共享密钥（**pre-share**），则需要配置 IKE keychain。

(3) 本端作为发起方时所使用的协商模式（主模式、野蛮模式）。本端作为响应方时，将自动适配发起方的协商模式。

(4) 本端作为发起方时可以使用的 IKE 提议（可指定多个），先指定的优先级高。响应方会将发起方的 IKE 提议与本端所有的 IKE 提议进行匹配，如果找到匹配项则直接使用，否则继续查找。若未查找到匹配的 IKE 提议，则协商失败。

(5) 本端身份信息。

- 如果本端的认证方式为数字签名，则可以配置任何类型的身份信息。若配置的本端身份为 IP 地址，但这个 IP 地址与本地证书中的 IP 地址不同时，设备将使用 FQDN（Fully Qualified

Domain Name，完全合格域名）类型的本端身份，该身份的内容为设备的名称（可通过 **sysname** 命令配置）。

- 如果本端的认证方式为预共享密钥，则只能配置除 DN 之外的其它类型的身份信息。

(6) IKE DPD（Dead Peer Detection，对等体存活检测）功能，IKE DPD 功能用于检测协商对端是否存活。如果 IKE profile 视图下和系统视图下都配置了 DPD 功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 DPD 功能，则采用系统视图下的 DPD 配置。

(7) IKE profile 的使用范围。限制 IKE profile 只能在指定的地址或指定接口的地址下使用（这里的地址指的是IPsec策略下配置的本端地址，若本端地址没有配置，则为引用IPsec策略的接口IP 地址）。配置了 **match local address** 的 IKE profile 的优先级高于所有未配置 **match local address** 的 IKE profile。

(8) IKE profile 的优先级。IKE profile 的匹配优先级首先取决于其中是否配置了 **match local address**，其次决定于配置的优先级值，最后决定于配置 IKE profile 的先后顺序。

(9) 支持对客户端认证。远程客户端与中心侧网关设备协商建立 IPsec 隧道的过程中，若中心侧网关设备上开启了对客户端认证，则在 IKE 一阶段协商完成之后，中心侧网关设备将会使用 AAA 机制对客户端进行认证，要求每个客户端在接入时，都需要提供用户名和密码。只有通过 AAA 认证的客户端才能继续进行后续的 IPsec 协商。对客户端的认证还需要在网关设备上配置相应的 AAA 认证方法来配合，关于 AAA 认证方法的详细配置请参见“安全配置指导”中的“AAA”。

(10) AAA 授权功能。通过本功能可以获得授权的 IKE 本地地址池的名称，地址池中配置了可分配给对端的 IP 地址。关于 AAA 授权 IKE 本地地址池的具体配置请参见“安全配置指导”中的“AAA”。

表2-2 配置 IKE profile

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IKE profile，并进入IKE Profile视图	**ike profile** *profile-name*	缺省情况下，不存在IKE profile
配置匹配对端身份的规则	**match remote** { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **user-fqdn** *user-fqdn-name* } }	协商双方都必须配置至少一个**match remote**规则，当对端的身份与IKE profile中配置的**match remote**规则匹配时，则使用此IKE profile中的信息与对端完成认证
配置采用预共享密钥认证时，所使用的keychain	**keychain** *keychain-name*	二者至少选其一 缺省情况下，未指定keychain和PKI域
配置采用数字签名认证时，证书所属的PKI域	**certificate domain** *domain-name*	
配置IKE第一阶段的协商模式	**exchange-mode** { **aggressive** | **main** }	缺省情况下，IKE第一阶段发起方的协商模式使用主模式
配置IKE profile引用的IKE提议	**proposal** *proposal-number&<1-6>*	缺省情况下，IKE profile未引用IKE提议，使用系统视图下已配置的IKE提议进行IKE协商

操作	命令	说明
配置本端身份信息	**local-identity** { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }	缺省情况下，未配置本端身份信息。此时使用系统视图下通过**ike identity**命令配置的身份信息作为本端身份信息。若两者都没有配置，则使用IP地址标识本端的身份，该IP地址为IPsec安全策略或IPsec安全策略模板应用的接口的IP地址
（可选）配置IKE DPD功能	**dpd interval** *interval* [**retry** *seconds*] { **on-demand** | **periodic** }	缺省情况下，IKE profile视图下没有配置DPD功能，采用系统视图下的DPD配置。若两者没有配置，则不进行DPD探测
（可选）配置IKE profile的使用范围	**match local address** { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }	缺省情况下，未限制IKE profile的使用范围
（可选）配置IKE profile的优先级	**priority** *priority*	缺省情况下，IKE profile的优先级为100
（可选）开启对客户端的认证	**client-authentication xauth**	缺省情况下，对客户端的认证处于关闭状态
（可选）配置AAA授权功能	**aaa authorization domain** *domain-name* **username** *user-name*	缺省情况下，AAA授权功能处于关闭状态

2.4 配置IKE提议

IKE 定义了一套属性数据来描述 IKE 第一阶段使用怎样的参数来与对端进行协商。用户可以创建多条不同优先级的 IKE 提议。协商双方必须至少有一条匹配的 IKE 提议才能协商成功。

在进行 IKE 协商时，协商发起方会将自己的 IKE 提议发送给对端，由对端进行匹配。

- 若发起方使用的 IPsec 安全策略中没有引用 IKE profile，则会将当前系统中所有的 IKE 提议发送给对端，这些 IKE 提议的优先级顺序由 IKE 提议的序号决定，序号越小优先级越高；
- 若发起方的 IPsec 策略中引用了 IKE profile，则会将该 IKE profile 中引用的所有 IKE 提议发送给对端，这些 IKE 提议的优先级由引用的先后顺序决定，先引用的优先级高。

协商响应方则以对端发送的 IKE 提议优先级从高到低的顺序与本端所有的 IKE 提议进行匹配，直到找到一个匹配的提议来使用。匹配的 IKE 提议将被用来建立 IKE SA。

以上 IKE 提议的匹配原则是：协商双方具有相同的加密算法、认证方法、认证算法和 DH group 标识。匹配的 IKE 提议的 IKE SA 存活时间则取两端的最小值。

表2-3 配置 IKE 提议

操作	命令	说明
进入系统视图	**system-view**	-
创建IKE提议，并进入IKE提议视图	**ike proposal** *proposal-number*	缺省情况下，存在一个缺省的IKE提议
配置IKE提议的描述信息	**description**	不存在IKE提议的描述信息

操作	命令	说明
指定一个供IKE提议使用的加密算法	**encryption-algorithm** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **des-cbc** }	缺省情况下，IKE提议使用CBC模式的56-bit DES加密算法
指定一个供IKE提议使用的认证方法	**authentication-method** { **dsa-signature** | **pre-share** | **rsa-signature** }	缺省情况下，IKE提议使用预共享密钥的认证方法
指定一个供IKE提议使用的认证算法	**authentication-algorithm** { **md5** | **sha** | **sha256** | **sha384** | **sha512** }	缺省情况下，IKE提议使用HMAC-SHA1认证算法
配置IKE第一阶段密钥协商时所使用的DH密钥交换参数	**dh** { **group1** | **group14** | **group2** | **group24** | **group5** }	缺省情况下，IKE第一阶段密钥协商时所使用的DH密钥交换参数为**group1**，即768-bit的Diffie-Hellman group
指定一个IKE提议的IKE SA存活时间	**sa duration** *seconds*	缺省情况下，IKE提议的IKE SA存活时间为86400秒

2.5 配置IKE keychain

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，具体包括以下内容：

- 预共享密钥。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。
- IKE keychain 的使用范围。限制 keychain 的使用范围，即 IKE keychain 只能在指定的地址或指定接口对应的地址下使用（这里的地址指的是 IPsec 安全策略/IPsec 安全策略模板下配置的本端地址，若本端地址没有配置，则为引用 IPsec 安全策略的接口的 IP 地址）。
- IKE keychain 的优先级。配置了 **match local address** 的 IKE keychain 的优先级高于所有未配置 **match local address** 的 IKE keychain。即 IKE keychain 的优先级首先决定于是否配置了 **match local address**，其次取决于配置的优先级，最后决定于配置 IKE keychain 的先后顺序。

表2-4 配置 IKE keychain

操作	命令	说明
进入系统视图	**system-view**	-
创建IKE keychain，并进入IKE keychain视图	**ike keychain** *keychain-name*	缺省情况下，不存在IKE keychain
配置预共享密钥	**pre-shared-key** { **address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] } | **hostname** *host-name* } **key** { **cipher** *cipher-key* | **simple** *simple-key* }	缺省情况下，未配置预共享密钥
（可选）配置IKE keychain的使用范围	**match local address** { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }	缺省情况下，未限制IKE keychain的使用范围

操作	命令	说明
（可选）配置IKE keychain的优先级	**priority** *priority*	缺省情况下，IKE keychain的优先级为100

2.6 配置本端身份信息

本端身份信息适用于所有 IKE SA 的协商，而 IKE profile 下的 **local-identity** 仅适用于本 IKE profile。如果 IKE profile 下没有配置本端身份，则默认使用此处配置的全局本端身份。

- 如果本端采用的认证方式为数字签名，则本端配置的任何类型的身份信息都有效；
- 如果本端采用认证方式为预共享密钥，则本端除 DN 之外的其它类型的身份信息均有效。

表2-5 配置本端身份信息

操作	命令	说明
进入系统视图	**system-view**	-
配置本端身份信息	**ike identity** { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **fqdn** [*fqdn-name*] | **user-fqdn** [*user-fqdn-name*] }	缺省情况下，使用IP地址标识本端的身份，该IP地址为IPsec安全策略或IPsec安全策略模板应用的接口地址
（可选）配置当使用数字签名认证方式时，本端的身份总从证书的主题字段中获得	**ike signature-identity from-certificate**	缺省情况下，本端身份信息由**local-identity**或**ike identity**命令指定 在采用IPsec野蛮协商模式且使用数字签名认证方式的情况下，与仅支持使用DN类型的身份进行数字签名认证的ComwareV5设备互通时需要配置本命令

2.7 配置IKE Keepalive功能

IKE Keepalive 功能用于检测对端是否存活。在对端配置了等待 IKE Keepalive 报文的超时时间后，必须在本端配置发送 IKE Keepalive 报文的时间间隔。当对端 IKE SA 在配置的超时时间内未收到 IKE Keepalive 报文时，则删除该 IKE SA 以及由其协商的 IPsec SA。

配置 IKE Keepalive 功能时，请遵循以下配置限制和指导：

- 当有检测对方是否存活的需求时，通常建议配置 IKE DPD，不建议配置 IKE Keepalive。仅当对方不支持 IKE DPD 功能且支持 IKE Keepalive 功能时，才考虑配置 IKE Keepalive 功能。配置 IKE Keepalive 功能后，会定时检测对方是否存活，因此会额外消耗网络带宽和计算资源。
- 本端配置的 IKE Keepalive 报文的等待超时时间要大于对端发送的时间间隔。由于网络中一般不会出现超过连续三次的报文丢失，所以，本端的超时时间可以配置为对端配置的发送 IKE Keepalive 报文的时间间隔的三倍。

表2-6 配置 IKE Keepalive 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置通过IKE SA向对端发送IKE Keepalive报文的时间间隔	**ike keepalive interval** *interval*	缺省情况下，不向对端发送IKE Keepalive报文
配置本端等待对端发送IKE Keepalive报文的超时时间	**ike keepalive timeout** *seconds*	缺省情况下，永不超时，一直等待对端发送IKE Keepalive报文

2.8 配置IKE NAT Keepalive功能

在采用 IKE 协商建立的 IPsec 隧道中，可能存在 NAT 设备，由于在 NAT 设备上的 NAT 会话有一定存活时间，一旦 IPsec 隧道建立后如果长时间没有流量，对应的 NAT 会话表项会被删除，这样将导致 IPsec 隧道无法继续传输数据。为防止 NAT 表项老化，NAT 内侧的 IKE 网关设备需要定时向 NAT 外侧的 IKE 网关设备发送 NAT Keepalive 报文，以便维持 NAT 设备上对应的 IPsec 流量的会话存活，从而让 NAT 外侧的设备可以访问 NAT 内侧的设备。

表2-7 配置 IKE NAT Keepalive 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置向对端发送NAT Keepalive报文的时间间隔	**ike nat-keepalive** *seconds*	缺省情况下，向对端发送NAT Keepalive报文的时间间隔为20秒

2.9 配置IKE DPD功能

DPD（Dead Peer Detection，对等体存活检测）用于检测对端是否存活。本端主动向对端发送 DPD 请求报文，对对端是否存活进行检测。如果本端在 DPD 报文的重传时间间隔（**retry** *seconds*）内未收到对端发送的 DPD 回应报文，则重传 DPD 请求报文，若重传两次之后仍然没有收到对端的 DPD 回应报文，则删除该 IKE SA 和对应的 IPsec SA。

配置 IKE DPD 功能时，请遵循以下配置限制和指导：

- IKE DPD 有两种模式：按需探测模式（**on-demand**）和定时探测模式（**periodic**）。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKE 对端通信时，应优先考虑使用按需探测模式。
- 如果 IKE profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKE profile 视图下的 DPD 配置生效，如果IKE profile视图下没有配置DPD探测功能，则采用系统视图下的DPD配置。
- 建议配置的触发 IKE DPD 探测的时间间隔大于 DPD 报文的重传时间间隔，使得直到当前 DPD 探测结束才可以触发下一次 DPD 探测，DPD 在重传过程中不触发新的 DPD 探测。

以定时探测模式为例，若本端的 IKE DPD 配置如下：

ike dpd interval 10 retry 6 periodic

则，具体的探测过程为：IKE SA 协商成功之后 10 秒，本端会发送 DPD 探测报文，并等待接收 DPD 回应报文。若本端在 6 秒内没有收到 DPD 回应报文，则会第二次发送 DPD 探测报文。在此过程中总共会发送三次 DPD 探测报文，若第三次 DPD 探测报文发出后 6 秒仍没收到 DPD 回应报文，则会删除发送 DPD 探测报文的 IKE SA 及其对应的所有 IPsec SA。若在此过程中收到了 DPD 回应报文，则会等待 10 秒再次发送 DPD 探测报文。

表2-8 配置全局 IKE DPD 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置IKE DPD功能	**ike dpd interval** *interval* [**retry** *seconds*] { **on-demand** | **periodic** }	缺省情况下，IKE DPD功能处于关闭状态

2.10 配置针对无效IPsec SPI的IKE SA恢复功能

当 IPsec 隧道一端的安全网关出现问题（例如安全网关重启）导致其 IPsec SA 丢失时，会造成 IPsec 流量黑洞现象：一端（接收端）的 IPsec SA 已经丢失，而另一端（发送端）还持有对应的 IPsec SA 且不断地向对端发送报文，当接收端收到发送端使用此 IPsec SA 封装的 IPsec 报文时，就会因为找不到对应的 SA 而持续丢弃报文，形成流量黑洞。该现象造成 IPsec 通信链路长时间得不到恢复（只有等到发送端旧的 IPsec SA 生命周期超时，并重建 IPsec SA 后，两端的 IPsec 流量才能得以恢复），因此需要采取有效的 IPsec SA 恢复手段来快速恢复中断的 IPsec 通信链路。

IPsec SA 由 SPI 唯一标识，接收方根据 IPsec 报文中的 SPI 在 SA 数据库中查找对应的 IPsec SA，若接收方找不到处理该报文的 IPsec SA，则认为此报文的 SPI 无效。如果接收端当前存在 IKE SA，则会向对端发送删除对应 IPsec SA 的通知消息，发送端 IKE 接收到此通知消息后，就会立即删除此无效 SPI 对应的 IPsec SA。之后，当发送端需要继续向接收端发送报文时，就会触发两端重建 IPsec SA，使得中断的 IPsec 通信链路得以恢复；如果接收端当前不存在 IKE SA，就不会触发本端向对端发送删除 IPsec SA 的通知消息，接收端将默认丢弃无效 SPI 的 IPsec 报文，使得链路无法恢复。后一种情况下，如果开启了 IPsec 无效 SPI 恢复 IKE SA 功能，就会触发本端与对端协商新的 IKE SA 并发送删除消息给对端，从而使链路恢复正常。

由于开启此功能后，若攻击者伪造大量源 IP 地址不同但目的 IP 地址相同的无效 SPI 报文发给设备，会导致设备因忙于与无效对端协商建立 IKE SA 而面临受到 DoS（Denial of Sevice）攻击的风险。因此，建议通常不要打开 **ike invalid-spi-recovery enable** 功能。

表2-9 开启针对无效 IPsec SPI 的 IKE SA 恢复功能

操作	命令	说明
进入系统视图	**system-view**	-
开启针对无效IPsec SPI的IKE SA恢复功能	**ike invalid-spi-recovery enable**	缺省情况下，针对无效IPsec SPI的IKE SA恢复功能处于关闭状态

2.11 配置对IKE SA数目的限制

由于不同设备的能力不同，为充分利用设备的处理能力，可以配置允许同时处于协商状态的 IKE SA 的最大数，也可以配置允许建立的 IKE SA 的最大数。

若设置允许同时协商更多的 IKE SA，则可以充分利用设备处理能力，以便在设备有较强处理能力的情况下得到更高的新建性能；若设置允许同时协商较少的 IKE SA，则可以避免产生大量不能完成协商的 IKE SA，以便在设备处理能力较弱时保证一定的新建性能。

若设置允许建立更多的 IKE SA，则可以使得设备在有充足内存的情况下得到更高的并发性能；若设置允许建立较少的 IKE SA，则可以在设备没有充足内存的情况下，使得 IKE 不过多占用系统内存。

表2-10 配置对本端 IKE SA 数目的限制

操作	命令	说明
进入系统视图	**system-view**	-
配置对本端IKE SA数目的限制	**ike limit** { **max-negotiating-sa** *negotiation-limit* | **max-sa** *sa-limit* }	缺省情况下，不限制允许同时处于协商状态的IKE SA数目，也不限制允许建立的IKE SA的最大数目

2.12 配置为客户端分配IP地址的IKE本地地址池

IKE 本地地址池与 AAA 授权配合使用，可以向对端客户端应答地址请求，从而使得企业分支客户端使用由企业中心网关统一分配的 IP 地址作为私网地址来进行通信，达到由企业中心统一管理的目的。关于 AAA 如何授权 IKE 本地地址池的具体配置请参见“安全配置指导”中的“AAA”。

表2-11 配置对端分配 IP 地址的 IKE 本地地址池

操作	命令	说明
进入系统视图	**system-view**	-
配置为对端分配IPv4地址的IKE本地地址池	**ike address-group** *group-name start-ipv4-address end-ipv4-address* [*mask* | *mask-length*]	缺省情况下，未定义IKE本地IPv4地址池

2.13 配置IKE告警功能

开启 IKE 的告警功能后，IKE 会生成告警信息，用于向网管软件报告该模块的重要事件。生成的告警信息将被发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

如果希望生成并输出某种类型的 IKE 告警信息，则需要保证 IKE 的全局告警功能以及相应类型的告警功能均处于开启状态。

表2-12 配置 IKE 告警功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IKE的全局告警功能	**snmp-agent trap enable ike global**	缺省情况下，IKE的告警Trap功能处于开启状态
开启IKE的指定告警功能	**snmp-agent trap enable ike** [**attr-not-support** | **auth-failure** | **cert-type-unsupport** | **cert-unavailable** | **decrypt-failure** | **encrypt-failure** | **invalid-cert-auth** | **invalid-cookie** | **invalid-id** | **invalid-proposal** | **invalid-protocol** | **invalid-sign** | **no-sa-failure** | **proposal-add** | **proposal–delete** | **tunnel-start** | **tunnel-stop** | **unsupport-exch-type**] *	缺省情况下，IKE的所有告警功能均处于开启状态

2.14 开启IKE协商事件日志功能

开启 IKE 协商事件日志记录功能后，设备会输出 IKE 协商过程中的相关日志。

表2-13 开启 IKE 协商事件日志功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IKE协商事件日志功能	**ike logging negotiation enable**	缺省情况下，IKE协商事件日志功能处于关闭状态

2.15 IKE显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IKE 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以删除 IKE SA。

表2-14 IKE 显示和维护

操作	命令
显示所有IKE提议的配置信息	**display ike proposal**
显示当前IKE SA的信息	**display ike sa** [**verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address*]]
显示IKE的统计信息	**display ike statistics**
清除IKE SA	**reset ike sa** [**connection-id** *connection-id*]
清除IKE的MIB统计信息	**reset ike statistics**

2.16 常见错误配置举例

2.16.1 提议不匹配导致IKE SA协商失败

1. 故障现象

(1) 通过如下命令查看当前的 IKE SA 信息，发现 IKE SA 的状态（Flags 字段）为 Unknown。

```
<Sysname> display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               192.168.222.5         Unknown      IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

(2) 打开 IKE 事件和报文调试信息开关后分别可以看到如下调试信息。

IKE 事件调试信息：

```
The attributes are unacceptable.
```

IKE 报文调试信息：

```
Construct notification packet: NO_PROPOSAL_CHOSEN.
```

2. 故障分析

IKE 提议配置错误。

3. 处理过程

(1) 排查 IKE 提议相关配置。具体包括：检查两端的 IKE 提议是否匹配，即 IKE 提议中的认证方法、认证算法、加密算法是否匹配。

(2) 修改 IKE 提议的配置，使本端 IKE 提议的配置和对端匹配。

2.16.2 未正确引用IKE提议或IKE keychain导致IKE SA协商失败

1. 故障现象

(1) 通过如下命令查看当前的 IKE SA 信息，发现 IKE SA 的状态（Flags 字段）为 Unknown。

```
<Sysname> display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    1               192.168.222.5         Unknown      IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
```

(2) 打开 IKE 事件和报文调试信息开关后分别可以看到如下调试信息。

IKE 事件调试信息：

```
Notification PAYLOAD_MALFORMED is received.
```

IKE 报文调试信息：

```
Construct notification packet: PAYLOAD_MALFORMED.
```

2. 故障分析

故障原因可能为以下两点：

(1) 匹配到的 IKE profile 中没有引用协商过程中匹配到的 IKE 提议。

通过调试信息看到：

```
Failed to find proposal 1 in profile profile1.
```

(2) 匹配到的 IKE profile 中没有引用协商过程中匹配到的 IKE keychain。

通过调试信息看到：

```
Failed to find keychain keychain1 in profile profile1.
```

3. 处理过程

(1) 检查匹配到的 IKE 提议是否在 IKE profile 下引用。以故障分析中的调试信息为例，IKE profile profile1 中需要引用 IKE proposal 1。

(2) 检查匹配到的 IKE keychain 是否在 IKE profile 下引用。以故障分析中的调试信息为例，IKE profile profile1 中需要引用 IKE keychain keychain1。

2.16.3 提议不匹配导致IPsec SA协商失败

1. 故障现象

(1) 通过 **display ike sa** 命令查看当前的 IKE SA 信息，发现 IKE SA 协商成功，其状态（Flags 字段）为 RD。但通过 **display ipsec sa** 命令查看当前的 IPsec SA 时，发现没有协商出相应的 IPsec SA。

(2) 打开 IKE 调试信息开关可以看到以下调试信息：

```
The attributes are unacceptable.
```

或者：

```
Construct notification packet: NO_PROPOSAL_CHOSEN.
```

2. 故障分析

IPsec 安全策略参数配置错误。

3. 处理过程

(1) 排查 IPsec 相关配置。具体包括：检查双方接口上应用的 IPsec 安全策略的参数是否匹配，即引用的 IPsec 安全提议的协议、加密算法和认证算法是否匹配。

(2) 修改 IPsec 安全策略配置，使本端 IPsec 安全策略的配置和对端匹配。

2.16.4 身份信息无效导致IPsec SA协商失败

1. 故障现象

(1) 通过 **display ike sa** 命令查看当前的 IKE SA 信息，发现 IKE SA 协商成功，其状态（Flags 字段）为 RD。但通过 **display ipsec sa** 命令查看当前的 IPsec SA 时，发现没有协商出相应的 IPsec SA。

(2) 打开 IKE 调试信息开关可以看到以下调试信息：

```
Notification INVALID_ID_INFORMATION is received.
```

或者：

```
Failed to get IPsec policy when renegotiating IPsec SA. Delete IPsec SA.
Construct notification packet: INVALID_ID_INFORMATION.
```

2. 故障分析

响应方 IPsec 安全策略配置错误，导致在 IKE 第二阶段协商时找不到 IPsec 安全策略，原因可能为如下几点：

(1) 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。

通过如下显示信息可以看到，IKE SA 在协商过程中没有找到匹配的 IKE profile：

```
<Sysname> display ike sa verbose
   -----------------------------------------------
   Connection ID: 3
   Outside VPN:
   Inside VPN:
   Profile:
   Transmitting entity: Responder
   -----------------------------------------------
   Local IP: 192.168.222.5
   Local ID type: IPV4_ADDR
   Local ID: 192.168.222.5

   Remote IP: 192.168.222.71
   Remote ID type: IPV4_ADDR
   Remote ID: 192.168.222.71

   Authentication-method: PRE-SHARED-KEY
   Authentication-algorithm: MD5
   Encryption-algorithm: 3DES-CBC

   Life duration(sec): 86400
   Remaining key duration(sec): 85847
   Exchange-mode: Main
   Diffie-Hellman group: Group 1
   NAT traversal: Not detected
```

但在 IPsec 策略中引用了 IKE profile profile1：

```
[Sysname] display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: Vlan-interface100
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Security data flow: 3000
  Selector mode: aggregation
  Local address: 192.168.222.5
  Remote address: 192.168.222.71
```

```
  Transform set:  transform1
  IKE profile: profile1
  SA duration(time based):
  SA duration(traffic based):
  SA idle time:
```

(2) 查看 IPsec 安全策略中引用的 ACL 配置是否正确。

例如，如发起方 ACL 流范围为网段到网段：

```
[Sysname] display acl 3000
Advanced IPv4 ACL 3000, 1 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

响应方 ACL 流范围为主机到主机：

```
[Sysname] display acl 3000
Advanced IPv4 ACL 3000, 1 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.222.71 0 destination 192.168.222.5 0
```

以上配置中，响应方 ACL 规则定义的流范围小于发起方 ACL 规则定义的流范围，这会导致 IPsec SA 协商失败。

(3) IPsec 安全策略配置不完整。具体包括：没有配置对端地址、没有配置 IPsec 提议、IPsec 提议配置不完整。

例如，如下 IPsec 安全策略中没有配置隧道的对端 IP 地址，因此 IPsec 安全策略是不完整的：

```
[Sysname] display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: Vlan-interface100
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Security data flow: 3000
  Selector mode: aggregation
  Local address: 192.168.222.5
  Remote address:
  Transform set:  transform1
  IKE profile: profile1
  SA duration(time based):
  SA duration(traffic based):
  SA idle time:
```

3. 处理过程

(1) 若在 IKE 第一阶段协商过程中没有找到 IKE profile，建议在响应方 IPsec 安全策略中去掉对 IKE profile 的引用或者调整 IKE profile 的配置使之能够与发起端相匹配。

(2) 若响应方 ACL 规则定义的流范围小于发起方 ACL 规则定义的流范围，建议修改响应方 ACL 的流范围大于或等于发起方 ACL 的流范围。以故障分析（2）中的配置为例，可以将响应方 ACL 流范围修改为：

```
[Sysname] display acl 3000
Advanced IPv4 ACL 3000, 2 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

(3) 将 IPsec 安全策略配置完整。以故障分析中的（3）中的配置为例，需要在 IPsec 安全策略中配置隧道的对端 IP 地址。

3 IKEv2

3.1 IKEv2简介

IPsec 隧道两端通过共享密钥对 IP 报文提供机密性、完整性、以及数据来源认证服务。共享密钥可以手工建立，也可以通过协商方式自动建立。IKE 协议定义了自动协商共享密钥的机制，并用于建立和维护 IPsec 安全联盟。IKEv2（Internet Key Exchange Version 2，互联网密钥交换协议第 2 版）是第 1 版本的 IKE 协议（本文简称 IKEv1）的增强版本，它在保留了 IKEv1 中的大部分特性的基础上引入了一些新特性。

IKEv2 与 IKEv1 相同，具有一套自保护机制，可以在不安全的网络上安全地进行身份认证、密钥分发、建立 IPsec SA。相对于 IKEv1，IKEv2 具有抗攻击能力和密钥交换能力更强以及报文交互数量较少等特点。

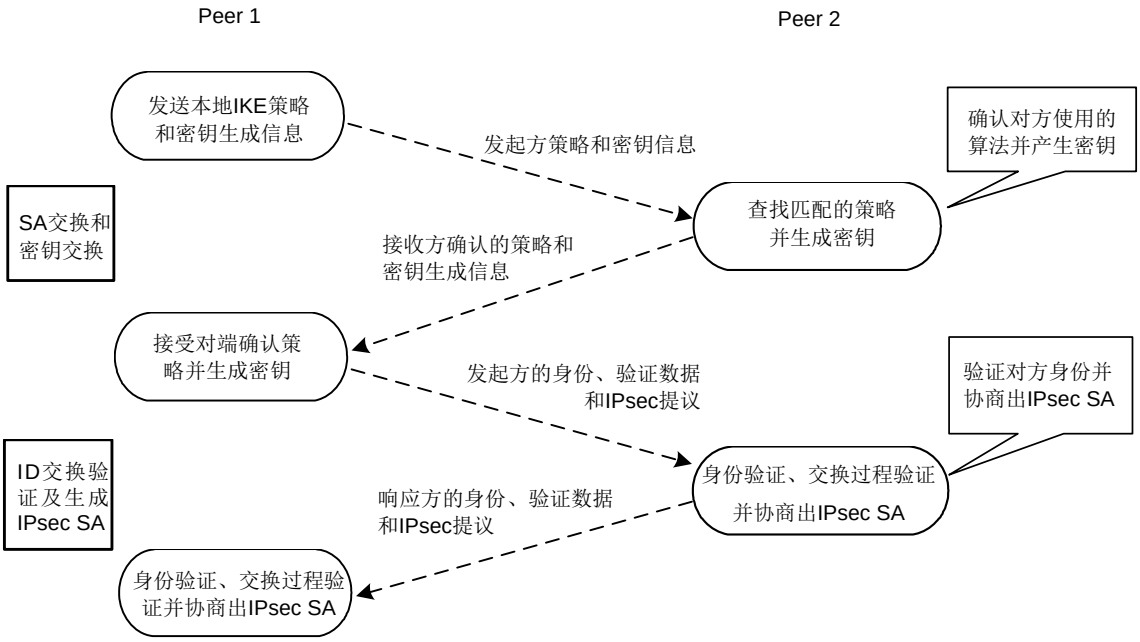
3.1.1 IKEv2 的协商过程

要建立一对 IPsec SA，IKEv1 需要经历两个阶段，至少需要交换 6 条消息。在正常情况下，IKEv2 只需要进行两次交互，使用 4 条消息就可以完成一个 IKEv2 SA 和一对 IPsec SA 的协商建立，如果要求建立的 IPsec SA 的数目大于一对，则每增加一对 IPsec SA 只需要额外增加一次交互，也就是两条消息就可以完成，这相比于 IKEv1 简化了设备的处理过程，提高了协商效率。

IKEv2 定义了三种交互：初始交换、创建子 SA 交换以及通知交换。

下面简单介绍一下 IKEv2 协商过程中的初始交换过程。

图3-1 IKEv2 的初始交换过程



如 图 3-1 所示，IKEv2 的初始交换过程中包含两个交换：IKE_SA_INIT交换（两条消息）和IKE_AUTH交换（两条消息）。

- IKE_SA_INIT 交换：完成 IKEv2 SA 参数的协商以及密钥交换；
- IKE_AUTH 交换：完成通信对等体的身份认证以及 IPsec SA 的创建。

这两个交换过程顺序完成后，可以建立一个 IKEv2 SA 和一对 IPsec SA。

创建子 SA 交换：当一个 IKE SA 需要创建多个 IPsec SA 时，使用创建子 SA 交换来协商多于一个的 SA，另外还可用于进行 IKE SA 的重协商功能。

通知交换：用于传递控制信息，例如错误信息或通告信息。

3.1.2 IKEv2 引入的新特性

1. IKEv2 支持DH猜想

在 IKE_SA_INIT 交换阶段，发起方采用“猜”的办法，猜一个响应方最可能使用的 DH 组携带在第一条消息中发送。响应方根据发起方“猜”的 DH 组来响应发起方。如果发起方猜测成功，则这样通过两条消息就可以完成 IKE_SA_INIT 交换。如果发起方猜测错误，则响应方会回应一个 INVALID_KE_PAYLOAD 消息，并在该消息中指明将要使用的 DH 组。之后，发起方采用响应方指定的 DH 组重新发起协商。这种 DH 猜想机制，使得发起方的 DH 组配置更为灵活，可适应不同的响应方。

2. IKEv2 支持cookie-challenge机制

在 IKE_SA_INIT 交换中消息是明文传输的，响应方接收到第一个消息后无法确认该消息是否来自一个仿冒的地址。如果此时一个网络攻击者伪造大量地址向响应方发送 IKE_SA_INIT 请求，根据 IKEv1 协议，响应方需要维护这些半开的 IKE 会话信息，从而耗费大量响应方的系统资源，造成对响应方的 DoS 攻击。

IKEv2 使用 cookie-challenge 机制来解决这类 DoS 攻击问题。当响应方发现存在的半开 IKE SA 超过指定的数目时，就启用 cookie-challenge 机制。响应方收到 IKE_SA_INIT 请求后，构造一个 Cookie 通知载荷并响应发起方，若发起方能够正确携带收到的 Cookie 通知载荷向响应方重新发起 IKE_SA_INIT 请求，则可以继续后续的协商过程。

半开状态的 IKEv2 SA 是指那些正在协商过程中的 IKEv2 SA。若半开状态的 IKEv2 SA 数目减少到阈值以下，则 cookie-challenge 功能将会停止工作

3. IKEv2 SA重协商

为了保证安全，IKE SA 和 IPsec SA 都有一个生命周期，超过生命周期的 SA 需要重新协商，即 SA 的重协商。与 IKEv1 不同的是，IKEv2 SA 的生命周期不需要协商，由各自的配置决定，重协商总是由生命周期较小的一方发起，可尽量避免两端同时发起重协商造成冗余 SA 的生成，导致两端 SA 状态不一致。

4. IKEv2 报文确认重传机制

与 IKEv1 不同，IKEv2 中所有消息都是以“请求–响应”对的形式出现，IKEv2 通过消息头中的一个 Message ID 字段来标识一个“请求–响应”对。发起方发送的每一条消息都需要响应方给予确认，例如建立一个 IKE SA 一般需要两个“请求-响应”对。如果发起方在规定时间内没有接收到确认报文，则需要对该请求消息进行重传。IKEv2 消息的重传只能由发起方发起，且重传消息的 Message ID 必须与原始消息的 Message ID 一致。

3.1.3 协议规范

与 IKEv2 相关的协议规范有：

- RFC 2408：Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4306：Internet Key Exchange (IKEv2) Protocol
- RFC 4718：IKEv2 Clarifications and Implementation Guidelines
- RFC 2412：The OAKLEY Key Determination Protocol
- RFC 5996：Internet Key Exchange Protocol Version 2 (IKEv2)

3.2 IKEv2配置任务简介

为了配置过程顺利进行，在 IKEv2 配置之前，用户需要确定以下几个因素：

- 确定 IKEv2 初始交换过程中使用的算法的强度，即确定对初始交换进行安全保护的强度（包括加密算法、完整性校验算法、PRF 算法和 DH 组算法）。不同的算法的强度不同，算法强度越高，受保护数据越难被破解，但消耗的计算资源越多。一般来说，密钥越长的算法强度越高。
- 确定本地认证方法以及对端的认证方法。若使用预共享密钥方式，则要确定通信双方预先约定的预共享密钥；若使用 RSA 数字签名方式，则要确定本端所使用的 PKI 域。关于 PKI 的配置，请参见“安全配置指导”中的“PKI”。

表3-1 IKEv2 配置任务简介

配置任务	说明	详细配置
配置IKEv2 profile	必选	3.3

配置任务		说明	详细配置
配置IKEv2安全策略		必选	3.4
配置IKEv2安全提议		可选 若IKEv2安全策略中指定了IKEv2提议，则必配	3.5
配置IKEv2 keychain		只要其中一端配置的认证方式为预共享密钥方式，则必选 如果两端配置的认证方式都是RSA数字签名方式，则不需要配置	3.6
配置IKEv2全局参数	配置IKEv2 cookie-challenge功能	可选 该功能仅对于响应方有意义	3.7.1
	配置IKEv2 DPD探测功能	可选	3.7.2
	配置IKEv2 NAT Keepalive功能	可选	3.7.3
	配置为对端分配IP地址的IKEv2本地地址池	可选	3.7.4

3.3 配置IKEv2 profile

IKEv2 profile 中包括以下配置：

(1) IKEv2 协商时本端和对端采用的身份认证方式。只能指定一个本端身份认证方式，可以指定多个对端身份认证方式。本端和对端可以采用不同的身份认证方式。

(2) 根据 IKEv2 profile 中配置的认证方法，配置 IKEv2 keychain 或 PKI 域。

- 如果任意一方指定的身份认证方式为数字签名（**dsa-signature**、**rsa-signature** 或者 **ecdsa-signature**），则需要配置 PKI 域。
- 如果任意一方指定的身份认证方式为预共享密钥（**pre-share**），则需要配置 IKEv2 keychain。

(3) 本端身份信息。

- 如果本端的认证方式为数字签名，则可以配置任何类型的身份信息。若配置的本端身份为 IP 地址，但这个 IP 地址与本地证书中的 IP 地址不同，设备将使用 FQDN 类型的本端身份，该身份的内容为设备的名称（可通过 **sysname** 命令配置）。
- 如果本端的认证方式为预共享密钥，则只能配置除 DN 之外的其它类型的身份信息。

(4) 匹配对端身份的规则。IKEv2 对等体需要根据对端的身份信息查找一个本端的 IKEv2 profile，然后使用此 IKEv2 profile 中的信息验证对端身份。对端身份信息若能满足本地某个 IKEv2 profile 中指定的匹配规则，则该 IKEv2 profile 为查找的结果。匹配 IKEv2 profile 的顺序取决于 IKEv2 profile 的优先级，优先级高的先匹配。

(5) IKEv2 DPD 探测功能。该功能用于检测协商对端是否存活。如果 IKEv2 profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKEv2 profile 视图下的 DPD 配置生效，如果 IKEv2 profile 视图下没有配置 DPD 探测功能，则采用系统视图下的 DPD 配置。

(6) IKEv2 profile 的使用范围。限制 IKEv2 profile 只能在指定的地址或指定接口的地址下使用（这里的地址指的是IPsec策略下配置的本端地址，若本端地址没有配置，则为引用IPsec策略的接口下地址）。

(7) IKEv2 profile 的优先级。优先级仅用于响应方在查找 IKEv2 profile 时调整 IKEv2 profile 的匹配顺序。

(8) IKEv2 SA 的时间生命周期。本端和对端的 IKEv2 SA 生命周期可以不一致，也不需要进行协商，由生命周期较短的一方在本端 IKEv2 SA 生命周期到达之后发起重协商。

(9) IKEv2 发送 NAT keepalive 报文的时间间隔。在 IKEv2 peer 之间存在 NAT 网关的情况下，设备通过定期向对端发送 NAT keepalive 报文，防止已有的 NAT 会话表项因长时间无流量匹配而被老化。

(10) 配置交换功能。企业分支使用虚拟隧道时，可以通过本功能向企业中心侧安全网关提交 IP 地址分配请求，中心侧安全网关接收该请求，会将成功分配的 IP 地址携带在 IKEv2 协商的响应报文中发送给分支侧设备，分支用此地址作为虚拟隧道地址与中心侧网关通信。企业中心侧网关也可以通过本功能主动推送 IP 地址给企业分支。配置交换包括请求数据、回应数据、主动推数据和回应推数据，请求和推送的数据可以为网关地址，内部地址，路由信息等。

(11) AAA 授权功能，通过 AAA 授权获取一个地址池的名字，地址池中配置了可分配给对端的 IP 地址。关于 AAA 授权 IKE 本地地址池的具体配置请参见“安全配置指导”中的“AAA”。。

表3-2 配置 IKEv2 profile

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IKEv2 profile，并进入IKEv2 Profile视图	**ikev2 profile** *profile-name*	缺省情况下，不存在IKEv2 profile
指定IKEv2本端和对端的身份认证方式	**authentication-method** { **local** | **remote** } { **dsa-signature** | **ecdsa-signature** | **pre-share** | **rsa-signature** }	缺省情况下，未配置本端和对端认证方式
配置采用预共享密钥认证时使用的Keychain	**keychain** *keychain-name*	二者至少选其一 根据**authentication-method**命令使用的认证方法选择其中一个配置
配置采用数字签名认证时使用的PKI域	**certificate domain** *domain-name* [**sign** | **verify**]	
配置本端身份信息	**identity local** { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **email** *email-string* | **fqdn** *fqdn-name* | **key-id** *key-id-string* }	缺省情况下，未配置本端身份信息。此时使用IP地址标识本端的身份，该IP地址为IPsec安全策略应用的接口的IP地址

操作	命令	说明
配置匹配对端身份的规则	**match remote** { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }	协商双方都必须配置至少一个**match remote**规则，当对端的身份与IKEv2 profile中配置的**match remote**规则匹配时，则使用此IKEv2 profile中的信息与对端完成认证
（可选）配置IKEv2 profile的使用范围	**match local address** { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未限制IKEv2 profile的使用范围
（可选）配置IKEv2 profile的优先级	**priority** *priority*	缺省情况下，IKEv2 profile的优先级为100
（可选）配置IKEv2 SA生命周期	**sa duration** *seconds*	缺省情况下，IKEv2 SA的生命周期为86400秒。
（可选）配置IKEv2 DPD探测功能	**dpd interval** *interval* [**retry** *seconds*] { **on-demand** | **periodic** }	缺省情况下，IKEv2 profile视图下没有配置DPD探测功能，采用系统视图下的DPD配置。若两者没有配置，则不进行DPD探测
（可选）配置发送NAT keepalive的时间间隔	**nat-keepalive** *seconds*	缺省条件下，使用全局的IKEv2 NAT keepalive配置
（可选）开启指定的配置交换功能	**config-exchange** { **request** | **set** { **accept** | **send** } }	缺省条件下，所有的配置交换功能均处于关闭状态
（可选）开启AAA授权功能	**aaa authorization domain** *domain-name* **username** *user-name*	缺省条件下，IKEv2的AAA授权功能处于关闭状态

3.4 配置IKEv2安全策略

在进行 IKE_SA_INIT 协商时，系统需要查找到一个与本端相匹配的 IKEv2 安全策略，并使用其中引用的安全提议进行安全参数的协商，匹配的依据为本端安全网关的 IP 地址。

- 若系统中配置了 IKEv2 安全策略，则根据本端安全网关的 IP 地址与所有已配置的 IKEv2 安全策略进行逐一匹配，如果未找到匹配的 IKEv2 安全策略或找到的安全策略中引用的安全提议配置不完整，则 IKE_SA_INIT 协商将会失败。
- 若系统中未配置任何 IKEv2 安全策略，则直接采用缺省的 IKEv2 安全策略 default。
- 系统中存在多个 IKEv2 安全策略的情况下，系统根据安全策略的优先级从高到低的顺序依次匹配。如果通过 **match local address** 命令指定了匹配 IKEv2 安全策略的本端地址，则优先匹配指定了本端地址匹配条件的策略，其次匹配未指定本端地址匹配条件的策略。

表3-3 配置 IKEv2 安全策略

操作	命令	说明
进入系统视图	**system-view**	
创建IKEv2安全策略，并进入IKEv2安全策略视图	**ikev2 policy** *policy-name*	缺省情况下，存在一个名称为default的缺省IKEv2安全策略

操作	命令	说明
指定匹配IKEv2安全策略的本端地址	**match local address** { *interface-type interface-number* | *ipv4-address* | **ipv6** *ipv6-address* }	缺省情况下，未指定用于匹配IKEv2安全策略的本端地址，表示本策略可匹配所有本端地址
指定IKEv2安全策略引用的IKEv2安全提议	**proposal** *proposal-name*	缺省情况下，IKEv2安全策略未引用IKEv2安全提议
指定IKEv2安全策略的优先级	**priority** *priority*	缺省情况下，IKEv2安全策略的优先级为100

3.5 配置IKEv2安全提议

IKEv2 安全提议用于保存 IKE_SA_INIT 交换中使用的安全参数，包括加密算法、完整性验证算法、PRF 算法和 DH 组，其中每类安全参数均可以配置多个，其优先级按照配置顺序依次降低。

一个完整的IKEv2安全提议中至少应该包含一组安全参数，即一个加密算法、一个完整性验证算法、一个 PRF 算法和一个 DH 组。

若同时指定了多个 IKEv2 安全提议，则它们的优先级按照配置顺序依次降低。

表3-4 配置 IKEv2 安全提议

操作	命令	说明
进入系统视图	**system-view**	
创建IKEv2安全提议，并进入IKEv2提议视图	**ikev2 proposal** *proposal-name*	缺省条件下，系统中存在一个名称为default的缺省IKEv2安全提议 该提议中定义的加密算法为**aes-cbc-128**和**3des**，完整性校验算法为**sha1**和**md5**，PRF算法为**sha1**和**md5**，DH组为**group5**和**group2**
指定IKEv2安全提议使用的加密算法	**encryption** { **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **aes-ctr-128** | **aes-ctr-192** | **aes-ctr-256** | **camellia-cbc-128** | **camellia-cbc-192** | **camellia-cbc-256** | **des-cbc** } *	缺省情况下，IKEv2安全提议未定义加密算法
指定IKEv2安全提议使用的完整性校验算法	**integrity** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *	缺省情况下，IKEv2安全提议未定义完整性校验算法
指定IKEv2安全提议使用的DH组	**dh** { **group1** | **group14** | **group2** | **group24** | **group5** | **group19** | **group20** } *	缺省情况下，IKEv2安全提议未定义DH组
指定IKEv2安全提议使用的PRF算法	**prf** { **aes-xcbc-mac** | **md5** | **sha1** | **sha256** | **sha384** | **sha512** } *	缺省情况下，IKEv2安全提议使用配置的完整性校验算法作为PRF算法

3.6 配置IKEv2 keychain

IKEv2 keychain 用来指定与对端进行 IKEv2 协商时使用的共享密钥信息。一个 IKEv2 keychain 下可以指定多个 IKEv2 peer，每个 IKEv2 peer 中包含了一个对称预共享密钥或一个非对称预共享密钥对，以及用于查找该 IKEv2 peer 的匹配参数（对等体的主机名称、IP 地址或地址范围、身份信息）。其中，IKEv2 协商的发起方使用对端的主机名称、IP 地址或地址范围查找 IKEv2 peer，响应方使用对端的 IP 地址、地址范围或身份信息查找 IKEv2 peer。

表3-5 配置 IKEv2 keychain

操作	命令	说明
进入系统视图	**system-view**	-
创建IKEv2 keychain，并进入IKEv2 keychain视图	**ikev2 keychain** *keychain-name*	缺省情况下，不存在IKEv2 keychain
创建IKEv2 peer，并进入IKEv2 peer视图	**peer** *name*	缺省情况下，不存在IKEv2 peer
指定IKEv2 peer的主机名称	**hostname** *name*	缺省情况下，未配置IKEv2 peer的主机名称
指定IKEv2 peer的主机地址	**address** { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] }	缺省情况下，未指定IKEv2 peer的主机地址 不同的IKEv2 peer中不能指定相同的主机地址
指定IKEv2 peer的身份信息	**identity** { **address** { *ipv4-address* | **ipv6** { *ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* }	缺省情况下，未指定IKEv2 peer的身份信息
配置IKEv2 peer的预共享密钥	**pre-shared-key** [**local** | **remote**] { **ciphertext** | **plaintext** } *string*	缺省情况下，未配置IKEv2 peer的预共享密钥

3.7 配置IKEv2全局参数

3.7.1 配置IKEv2 cookie-challenge功能

IKEv2 cookie-challenge 功能用来防止攻击者通过源 IP 仿冒对响应方造成 DoS 攻击。

开启 IKEv2 cookie-challenge 功能的同时需要指定启用 cookie-challenge 功能的阈值，当响应方本地存在的半开状态的 IKEv2 SA 数目达到指定的阈值时，则 cookie-challenge 功能开始生效。

表3-6 配置 IKEv2 cookie-challenge 功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IKEv2 cookie-challenge功能	**ikev2 cookie-challenge** *number*	缺省情况下，IKEv2 cookie-challenge功能处于关闭状态

3.7.2 配置全局IKEv2 DPD探测功能

IKEv2 DPD 探测功能用来探测对端是否存活，包括以下两种模式：

- 按需探测模式（**on-demand**）：根据流量来探测对端是否存活。在本端发送用户报文时，如果发现自最后一次收到对端报文之后，在指定的触发 IKEv2 DPD 的时间间隔内一直未收到对端报文，则发送 DPD 报文探测对端是否存活。
- 定时探测模式（**periodic**）：按照配置的触发 IKEv2 DPD 的时间间隔定时发送 DPD 报文，探测对端是否存活。

当系统视图下和 IKEv2 profile 视图下都配置 DPD 探测功能时，IKEv2 profile 视图下的 DPD 配置覆盖系统视图下的全局 DPD 配置。若 IKEv2 profile 视图下没有配置 DPD 探测功能，则应用全局 DPD 配置。

表3-7 配置全局 IKEv2 DPD 探测功能

操作	命令	说明
进入系统视图	**system-view**	-
配置IKEv2 DPD探测功能	**ikev2 dpd interval** *interval* [**retry** *seconds*] { **on-demand** | **periodic** }	缺省情况下，全局IKEv2 DPD探测功能处于关闭状态

3.7.3 配置IKEv2 NAT Keepalive功能

IKEv2 NAT Keepalive 功能仅对位于 NAT 之后的设备（即该设备位于 NAT 设备连接的私网侧）有意义。NAT 之后的 IKEv2 网关设备需要定时向 NAT 之外的 IKEv2 网关设备发送 NAT Keepalive 报文，以确保 NAT 设备上相应于该流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。因此，配置的发送 NAT Keepalive 报文的时间间隔需要小于 NAT 设备上会话表项的存活时间。本功能必须在探测到 NAT 之后才能生效。

表3-8 配置 IKEv2 NAT Keepalive 功能

操作	命令	说明
进入系统视图	**system-view**	-
配置向对端发送NAT Keepalive报文的时间间隔	**ikev2 nat-keepalive** *seconds*	缺省情况下，探测到NAT后发送NAT Keepalive报文的时间间隔为10秒

3.7.4 配置为对端分配IP地址的IKEv2 本地地址池

IKEv2 本地地址池与 AAA 授权配合使用，可以向对端网关（客户端）分配地址或应答地址请求，从而使得对端网关（企业分支客户端）使用由企业中心网关统一分配的 IP 地址作为私网地址来进行通信，达到由企业中心统一管理的目的。关于 AAA 授权 IKEv2 本地地址池的具体配置请参见“安全配置指导”中的“AAA”。

表3-9 配置为对端分配 IP 地址的 IKEv2 本地地址池

操作	命令	说明
进入系统视图	**system-view**	-
配置为对端分配IPv4地址的IKEv2本地地址池	**ikev2 address-group** *group-name start-ipv4-address end-ipv4-address* [*mask* | *mask-length*]	缺省情况下，未定义IKEv2本地IPv4地址池
配置为对端分配IPv6地址的IKEv2本地地址池	**ikev2 ipv6-address-group** *group-name* **prefix** *prefix/prefix-len* **assign-len** *assign-len*	缺省情况下，未定义IKEv2本地IPv6地址池

3.8 IKEv2显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IKEv2 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以删除 IKEv2 SA。

表3-10 IKEv2 显示和维护

操作	命令
显示IKEv2安全提议的配置信息	**display ikev2 proposal** [*name* | **default**]
显示IKEv2安全策略的配置信息	**display ikev2 policy** [*policy-name* | **default**]
显示IKEv2 profile的配置信息	**display ikev2 profile** [*profile-name*]
显示当前IKEv2 SA的信息	**display ikev2 sa** [**count** | [{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* }] [**verbose** [**tunnel** *tunnel-id*]]]
显示IKEv2统计信息	**display ikev2 statistics**
删除IKEv2 SA及其协商生成的Child SA	**reset ikev2 sa** [[{ **local** | **remote** } { *ipv4-address* | **ipv6** *ipv6-address* }] | **tunnel** *tunnel-id*] [**fast**]
清除IKEv2统计信息	**reset ikev2 statistics**

3.9 常见错误配置举例

3.9.1 IKEv2 提议不匹配导致IKEv2 SA协商失败

1. 故障现象

通过如下命令查看当前的 IKEv2 SA 信息，发现 IKEv2 SA 的状态（Status 字段）为 IN-NEGO。

```
<Sysname> display ikev2 sa
Tunnel ID   Local                    Remote                   Status
  ------------------------------------------------------------------------------
  5           123.234.234.124/500        123.234.234.123/500        IN-NEGO
Status:
IN-NEGO: Negotiating, EST: Establish, DEL:Deleting
```

2. 故障分析

IKEv2 提议配置错误。

3. 处理过程

(1) 排查 IKEv2 相关配置。具体包括：检查两端的 IKEv2 提议是否匹配，即 IKEv2 提议中的认证方法、认证算法、加密算法、PRF 算法是否匹配。

(2) 修改 IKEv2 提议的配置，使本端 IKEv2 提议的配置和对端匹配。

3.9.2 IPsec提议不匹配导致IPsec SA协商失败

1. 故障现象

通过 **display ikev2 sa** 命令查看当前的 IKEv2 SA 信息，发现 IKEv2 SA 协商成功，其状态（Status 字段）为 EST。但通过 **display ipsec sa** 命令查看当前的 IPsec SA 时，发现没有协商出相应的 IPsec SA。

2. 故障分析

IPsec 安全策略参数配置错误。

3. 处理过程

(1) 排查 IPsec 相关配置。具体包括：检查双方接口上应用的 IPsec 安全策略的参数是否匹配，即引用的 IPsec 安全提议的协议、加密算法和认证算法是否匹配。

(2) 修改 IPsec 策略配置，使本端 IPsec 安全策略的配置和对端匹配。

3.9.3 无法建立安全隧道

1. 故障现象

双方的 ACL 配置正确，也有相匹配的 IKEv2 安全提议，但安全隧道无法建立或者存在安全隧道却无法通信。

2. 故障分析

这种情况一般是由于网络状态不稳定，安全隧道建立好以后，有一方的设备重启造成了两端的 IKEv2 SA 或者 IPsec SA 不对称。

3. 处理过程

使用 **display ikev2 sa** 命令检查双方是否都已建立 IKEv2 SA。如果有一端存在的 IKEv2 SA 在另一端上不存在，请先使用 **reset ikev2 sa** 命令清除双方不对称存在的 IKEv2 SA，并重新发起协商；如果两端存在对称的 IKEv2 SA，则使用 **display ipsec sa** 命令查看接口上的安全策略是否已建立了对称的 IPsec SA。如果一端存在的 IPsec SA 在另一端上不存在，请使用 **reset ipsec sa** 命令清除双方不对称存在的 IPsec SA，并重新发起协商。