目 录

1 IPsec

说明

若无特殊说明，本文中的 IKE 均指第 1 版本的 IKE 协议。

1.1 IPsec简介

IPsec（IP Security）是 IETF 制定的三层隧道加密协议，它为 Internet 上传输的数据提供了高质量的、可互操作的、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。特定的通信方之间通过建立 IPsec 隧道来传输用户的私有数据，并在 IP 层提供了以下安全服务：

- 数据机密性（Confidentiality）：IPsec 发送方在通过网络传输包前对包进行加密。
- 数据完整性（Data Integrity）：IPsec 接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据来源认证（Data Authentication）：IPsec 在接收端可以认证发送 IPsec 报文的发送端是否合法。
- 防重放（Anti-Replay）：IPsec 接收方可检测并拒绝接收过时或重复的报文。

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）的服务，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。

IPsec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构，包括网络认证协议AH（Authentication Header，认证头）、ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）和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“2 IKE”，本节不做介绍。

IPsec 提供了两种安全机制：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。

设备可支持 IPsec 对 IPv4 报文和 IPv6 报文的保护。

1.1.1 IPsec基本概念

1. 安全协议

AH 协议和 ESP 协议的功能及工作原理如下：

- AH 协议（IP 协议号为 51）定义了认证的应用方法，提供数据源认证、数据完整性校验和防报文重放功能，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报文头，此报文头插在标准 IP 包头后面，对数据提供完整性保护。可选择的认证算法有 MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。
- ESP 协议（IP 协议号为 50）定义了加密和可选认证的应用方法，提供加密、数据源认证、数据完整性校验和防报文重放功能。ESP 的工作原理是在每一个数据包的标准 IP 包头后面添加一个 ESP 报文头，并在数据包后面追加一个 ESP 尾。与 AH 协议不同的是，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。常见的加密算法有 DES、3DES、AES 等。同时，作为可选项，用户可以选择 MD5、SHA-1 算法保证报文的完整性和真实性。

在实际进行 IP 通信时，可以根据实际安全需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过，AH 提供的认证服务要强于 ESP。同时使用 AH 和 ESP 时，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，封装之后的报文从内到外依次是原始 IP 报文、ESP 头、AH 头和外部 IP 头。

2. 安全联盟（Security Association，SA）

IPsec 在两个端点之间提供安全通信，端点被称为 IPsec 对等体。

SA 是 IPsec 的基础，也是 IPsec 的本质。SA 是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP 还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES、3DES 和 AES）、特定流中保护数据的共享密钥以及密钥的生存周期等。建立 SA 的方式有手工配置和 IKE 自动协商两种。

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 由一个三元组来标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 或 ESP）。

SPI 是用于唯一标识 SA 的一个 32 比特数值，它在 AH 和 ESP 头中传输。在手工配置 SA 时，需要手工指定 SPI 的取值。使用 IKE 协商产生 SA 时，SPI 将随机生成。

通过 IKE 协商建立的 SA 具有生存周期，手工方式建立的 SA 永不老化。IKE 协商建立的 SA 的生存周期有两种定义方式：

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

生存周期到达指定的时间或指定的流量，SA 就会失效。SA 失效前，IKE 将为 IPsec 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，继续使用旧的 SA 保护通信。在新的 SA 协商好之后，则立即采用新的 SA 保护通信。

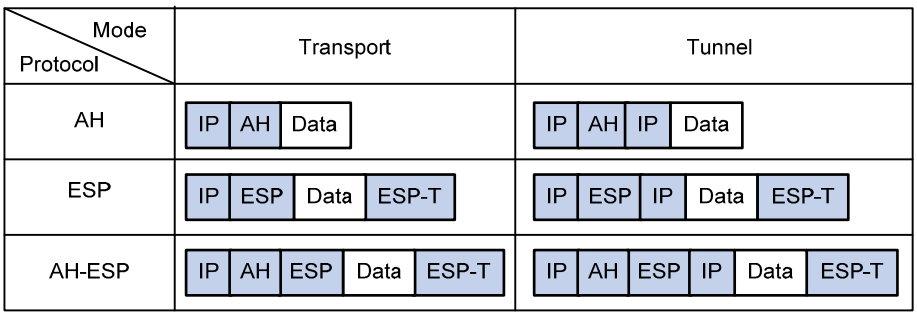
3. 封装模式

IPsec 有如下两种工作模式：

- 隧道（tunnel）模式：用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。通常，隧道模式应用在两个安全网关之间的通讯。
- 传输（transport）模式：只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。

不同的安全协议在tunnel和transport模式下的数据封装形式如图 1-1所示。

图1-1 安全协议数据封装格式



4. 认证算法与加密算法

(1) 认证算法

认证算法的实现主要是通过杂凑函数。杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPsec 对等体计算摘要，如果两个摘要是相同的，则表示报文是完整未经篡改的。IPsec 使用两种认证算法：

- MD5：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1：SHA-1 通过输入长度小于 2 的 64 次方 bit 的消息，产生 160bit 的消息摘要。

MD5 算法的计算速度比 SHA-1 算法快，而 SHA-1 算法的安全强度比 MD5 算法高。

(2) 加密算法

加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。目前设备的 IPsec 实现三种加密算法：

- DES（Data Encryption Standard）：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- 3DES（Triple DES）：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
- AES（Advanced Encryption Standard）：使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密。

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。对于普通的安全要求，DES 算法就可以满足需要。

5. 协商方式

有如下几种协商方式建立 SA：

- 手工方式（manual）配置比较复杂，创建 SA 所需的全部信息都必须手工配置，而且不支持一些高级特性（例如定时更新密钥），但优点是可以不依赖 IKE 而单独实现 IPsec 功能。
- IKE 自动协商（isakmp）方式相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护 SA。
- GDOI 方式用于构建 Group Domain VPN（Group Domain Virtual Private Network，组加密传输虚拟专用网络），SA 和密钥由 KS（Key Server，密钥服务器）集中管理并下发给 GM（Group Member，组成员）。

当与之进行通信的对等体设备数量较少时，或是在小型静态环境中，手工配置 SA 是可行的。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立 SA。

6. 安全隧道

安全隧道是建立在本端和对端之间可以互通的一个通道，它由一对或多对 SA 组成。

1.1.2 IPsec虚拟隧道接口

1. 概述

IPsec 虚拟隧道接口是一种支持路由的三层逻辑接口，它可以支持动态路由协议，所有路由到 IPsec 虚拟隧道接口的报文都将进行 IPsec 保护，同时还可以支持对组播流量的保护。使用 IPsec 虚拟隧道接口建立 IPsec 隧道具有以下优点：

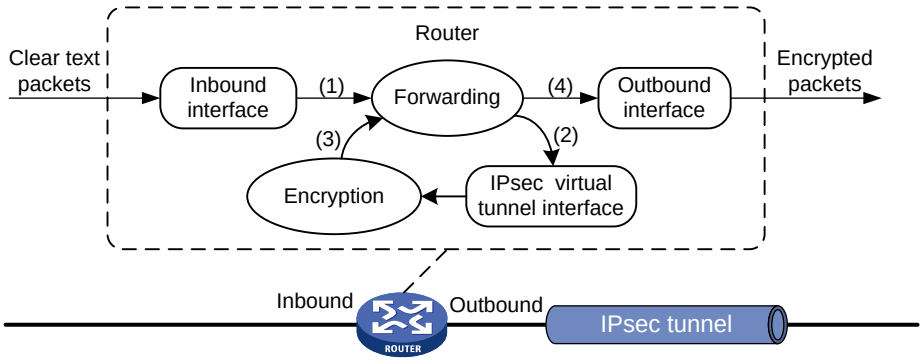
- 简化配置：通过路由来确定对哪些数据流进行 IPsec 保护。与通过 ACL 指定数据流范围的方式相比，这种方式简化了用户在部署 IPsec 安全策略时配置上的复杂性，使得 IPsec 的配置不会受到网络规划的影响，增强了网络规划的可扩展性，降低了网络维护成本。
- 减少开销：在保护远程接入用户流量的组网应用中，在 IPsec 虚拟隧道接口处进行报文封装，与 IPsec over GRE 或者 IPsec over L2TP 方式的隧道封装相比，无需额外为入隧道流量加封装 GRE 头或者 L2TP 头，减少了报文封装的层次，节省了带宽。
- 业务应用更灵活：IPsec 虚拟隧道接口在实施过程中明确地区分出“加密前”和“加密后”两个阶段，用户可以根据不同的组网需求灵活选择其它业务（例如 NAT、QoS）实施的阶段。例如，如果用户希望对 IPsec 封装前的报文应用 QoS，则可以在 IPsec 虚拟隧道接口上应用 QoS 策略；如果希望对 IPsec 封装后的报文应用 QoS，则可以在物理出接口上应用 QoS 策略。

2. 工作原理

IPsec 虚拟隧道接口对报文的加封装/解封装发生在隧道接口上。用户流量到达实施 IPsec 配置的设备后，需要 IPsec 处理的报文会被转发到 IPsec 虚拟隧道接口上进行加封装/解封装。

如图 1-2所示，IPsec虚拟隧道接口对报文进行加封装的过程如下：

图1-2 IPsec 虚接口隧道加封装原理图



(1) Router 将从入接口接收到的 IP 明文送到转发模块进行处理；

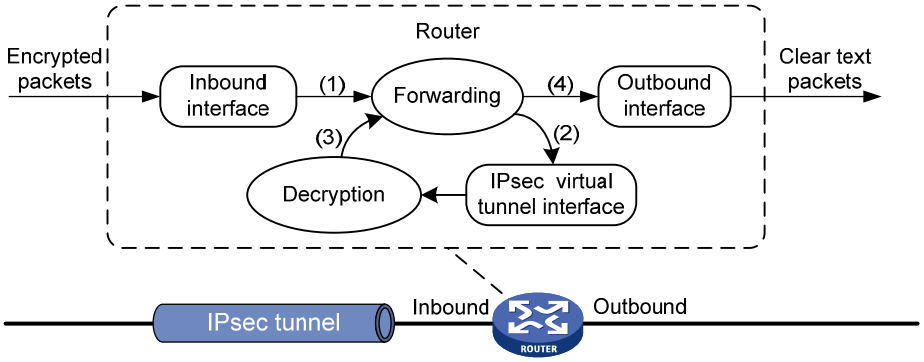
(2) 转发模块依据路由查询结果，将 IP 明文发送到 IPsec 虚拟隧道接口进行加封装：原始 IP 报文被封装在一个新的 IP 报文中，新 IP 头中的源地址和目的地址分别为隧道接口的源地址和目的地址；

(3) IPsec 虚拟隧道接口完成对 IP 明文的加封装处理后，将 IP 密文送到转发模块进行处理；

(4) 转发模块进行第二次路由查询后，将 IP 密文通过隧道接口的实际物理出接口转发出去。

如图 1-3所示，IPsec虚拟隧道接口对报文进行解封装的过程如下：

图1-3 IPsec 虚接口隧道解封装原理图



(1) Router 将从入接口接收到的 IP 密文送到转发模块进行处理；

(2) 转发模块识别到此 IP 密文的目的地为本设备的隧道接口地址且 IP 协议号为 AH 或 ESP 时，会将 IP 密文送到相应的 IPsec 虚拟隧道接口进行解封装：将 IP 密文的外层 IP 头去掉，对内层 IP 报文进行解密处理；

(3) IPsec 虚拟隧道接口完成对 IP 密文的解封装处理之后，将 IP 明文重新送回转发模块处理；

(4) 转发模块进行第二次路由查询后，将 IP 明文从隧道的实际物理出接口转发出去。

从上面描述的加封装/解封装过程可见，IPsec 虚拟隧道接口将报文的 IPsec 处理过程区分为两个阶段：“加密前”和“加密后”。需要应用到加密前的明文上的业务（例如 NAT、QoS），可以应用到隧道接口上；需要应用到加密后的密文上的业务，则可以应用到隧道接口对应的物理出接口上。

1.1.3 使用IPsec保护IPv6 路由协议

使用 IPsec 保护 IPv6 路由协议是指，使用 AH/ESP 协议对 IPv6 路由协议报文进行加/解封装处理，并为其提供认证和加密的安全服务，目前支持 OSPFv3、IPv6 BGP、RIPng 路由协议。

IPsec 对 IPv6 路由协议报文进行保护的处理方式和目前基于接口的 IPsec 处理方式不同，是基于业务的 IPsec，即 IPsec 保护某一业务的所有报文。该方式下，设备产生的所有需要 IPsec 保护的 IPv6 路由协议报文都要被进行加封装处理，而设备接收到的不受 IPsec 保护的以及解封装（解密或验证）失败的 IPv6 路由协议报文都要被丢弃。

在基于接口的 IPsec 处理方式下，设备对配置了 IPsec 安全功能的接口上发送的每个报文都要判断是否进行 IPsec 处理。目前，该方式有两种实现，一种是基于 ACL 的 IPsec，只要到达接口的报文与该接口的 IPsec 安全策略中的 ACL 规则匹配，就会受到 IPsec 保护；另一种是基于路由的 IPsec，即 IPsec 虚拟隧道接口方式，只要被路由到虚拟隧道接口上的报文都会受到 IPsec 保护。

相对于基于接口的 IPsec，基于业务的 IPsec 既不需要 ACL 来限定要保护的流的范围，也不需要指定 IPsec 隧道的起点与终点，IPsec 安全策略仅与具体的业务绑定，不管业务报文从设备的哪个接口发送出去都会被 IPsec 保护。

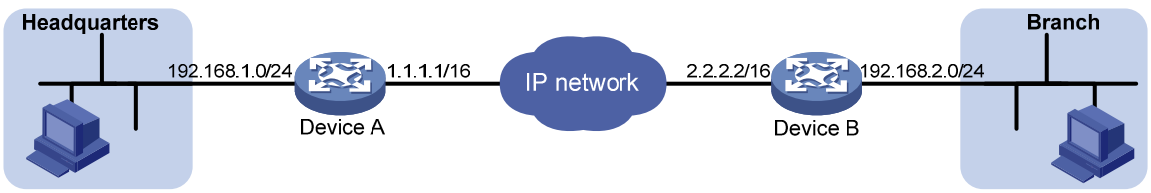
由于 IPsec 的密钥交换机制仅仅适用于两点之间的通信保护，在广播网络一对多的情形下，IPsec 无法实现自动交换密钥，因此必须使用手工配置密钥的方式。同样，由于广播网络一对多的特性，要求各设备对于接收、发送的报文均使用相同的 SA 参数（相同的 SPI 及密钥）。因此，目前仅支持手工安全策略生成的 SA 对 IPv6 路由协议报文进行保护。

1.1.4 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，当企业分支众多时，企业总部网关需要配置大量静态路由，将总部发往分支的数据引到应用IPsec策略的接口上来，另外，当企业分支内部网络规划发生变化时，同时需要调整总部网关上的静态路由，工作量巨大且容易出现配置错误。

RRI（Reverse Route Injection，反向路由注入）功能的出现，可以很好得解决这些问题。RRI 是一种自动添加到达 IPsec VPN 私网或 IPsec 隧道网关静态路由的机制，可实现为受 IPsec 保护的流量自动添加静态路由的功能。

图1-4 IPsec VPN 组网图



如上 IPsec VPN 组网中，在总部网关设备 Device A 上配置 RRI 功能后，Device A 上将自动添加一条到达分支所在私网网段 192.168.2.0/24 的路由，等价于在其上手工配置如下静态路由：

ip route-static 192.168.2.0 255.255.255.0 2.2.2.2

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 隧道对端地址或指定的地址，它使得发往对端的流量将被强制通过 IPsec 加密后转发。

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。该功能在企业总部有多台网关设备的组网应用中，如进行负载均衡、双机热备的情况下，甚至是 IPsec VPN 流量通过默认网关无法到达对端网关设备的时候，都能及时生成新的路由来转发 IPsec VPN 流量，因此非常有用。

在 MPLS L3VPN 组网环境中，配置了 RRI 的 IPsec VPN 网关设备能够依据应用 IPsec 策略的接口所绑定的 VPN 实例，在相应 VPN 实例的 IP 路由表中添加静态路由。

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，大大增强 VPN 网络的可扩展性。

1.1.5 协议规范

与 IPsec 相关的协议规范有：

- RFC2401：Security Architecture for the Internet Protocol
- RFC2402：IP Authentication Header
- RFC2406：IP Encapsulating Security Payload
- RFC4552：Authentication/Confidentiality for OSPFv3
- RFC4301：Security Architecture for the Internet Protocol
- RFC4302：IP Authentication Header
- RFC4303：IP Encapsulating Security Payload (ESP)

1.2 建立IPsec隧道的配置方式

IPsec 隧道的建立有多种配置方式，请根据实际组网中对 IPsec 隧道的使用需求来选择配置方式：

- 基于ACL方式：由ACL来指定要保护的数据流范围，通过配置安全策略并将安全策略绑定在实际的物理接口上来完成IPsec的配置。这种方式可以利用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。具体配置请参见“1.3 基于ACL建立IPsec安全隧道”。
- 基于路由方式：即基于IPsec虚拟隧道接口建立IPsec安全隧道。这种方式下，由路由来选择需要保护的数据流，通过配置安全框架并在IPsec虚拟隧道接口上应用安全框架来完成IPsec的配置。这种方式简化了网络配置及网络管理上的复杂度，增强了大型VPN网络的可扩展性。具体配置请参见“1.4 基于IPsec虚拟隧道接口建立IPsec安全隧道”。
- 基于业务方式：IPsec安全策略直接与具体的业务绑定，保护某一业务的所有报文，无需ACL或者路由来指定要保护的数据流。目前，支持对IPv6 路由协议的保护。通过配置手工方式的IPsec安全策略，并在IPv6 路由协议上应用安全策略来完成IPsec的配置。具体配置请参见“1.5 配置IPsec保护IPv6 路由协议”。

在 IPv4 网络和 IPv6 网络中，建立 IPsec 隧道的配置步骤是相同的，均可支持基于 ACL 方式和基于路由方式。

1.3 基于ACL建立IPsec安全隧道

1.3.1 IPsec配置任务简介

基于 ACL 建立 IPsec 安全隧道的基本配置思路如下：

(1) 通过配置访问控制列表，用于匹配需要保护的数据流；

(2) 通过配置 IPsec 安全提议，指定安全协议、认证算法和加密算法、封装模式等；

(3) 通过配置 IPsec 安全策略，将要保护的数据流和 IPsec 安全提议进行关联（即定义对何种数据流实施何种保护），并指定 SA 的协商方式、对等体 IP 地址（即保护路径的起/终点）、所需要的密钥和 SA 的生存周期等；

(4) 最后在设备接口上应用 IPsec 安全策略即可完成 IPsec 隧道的配置。

表1-1 IPsec 配置任务简介

配置任务		说明	详细配置
IPsec基本配置	配置访问控制列表	必选	1.3.2
	配置IPsec安全提议		1.3.3
	配置IPsec安全策略		1.3.4
	在接口上应用IPsec安全策略组		1.3.5
使能加密引擎		可选	1.3.6
使能解封装后IPsec报文的ACL检查开关		可选	1.3.7
配置IPsec抗重放功能		可选	1.3.8
配置报文信息预提取功能		可选	1.3.9
配置IPsec无效SPI恢复功能		可选	1.3.10
配置IPsec反向路由注入功能		可选	1.3.11
使能加密前/加密后分片功能		可选	1.3.12

提示

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。

1.3.2 配置访问控制列表

ACL（Access Control List，访问控制列表）是用来实现流识别功能的。网络设备为了过滤报文，需要配置一系列的匹配条件对报文进行分类，当设备的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文进行分析、识别之后，根据预先设定的策略对报文进行不同的处理。

1. ACL规则中关键字的使用

IPsec 通过配置 ACL 来定义需要过滤的数据流。在 IPsec 的应用中，ACL 规则中的 **permit** 关键字表示与之匹配的流量需要被 IPsec 保护，而规则中的 **deny** 关键字则表示与之匹配的那些流量不需要保护。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，如果该规则为 **permit**，则该规则就定义了需要建立 SA 来保护的数据流量的范围。

在 IPsec 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 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 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 网段到 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 网段到 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 IPsec 报文将被进行解封装处理，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，否则丢弃。

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保护的 IPsec 报文将被接收并处理，入方向上未被保护的 IPsec 报文将被丢弃。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，影响正常的业务流传输。
- 合理使用 **deny** 规则，尤其是在一个安全策略下有多条优先级不同的子安全策略时，避免本应该与优先级较低的子安全策略的 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子安全策略的 ACL **deny** 规则匹配上，而在接收端被当作未被 IPsec 保护的报文丢弃。

deny 规则的错误配置示例：（以下配置信息仅截取了 ACL 的相关内容，其它步骤省略）

Router A 连接的 1.1.2.0/24 网段到 Router B 连接的 3.3.3.0/24 网段之间的报文，在应用了 IPsec 策略 test 的出接口上，优先与顺序号为 1 的安全策略进行匹配，并匹配上了 ACL 3000 的 rule 1 deny ip，因此 Router A 认为它不需要 IPsec 保护，到达 Router B 后将被丢弃。

Router A 上的配置如下：

```
acl number 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 number 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 test 1 isakmp
 security acl 3000
 ike-peer aa
 transform-set 1
```

```
#
ipsec policy test 2 isakmp
 security acl 3001
 ike-peer bb
 transform-set 1
```

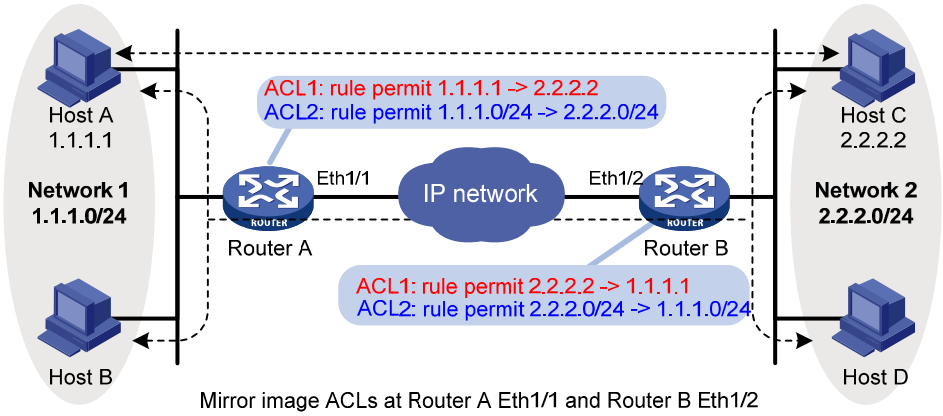
Router B 上的配置如下：

```
acl number 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 test 1 isakmp
 security acl 3001
 ike-peer aa
 transform-set 1
```

2. ACL规则的配置

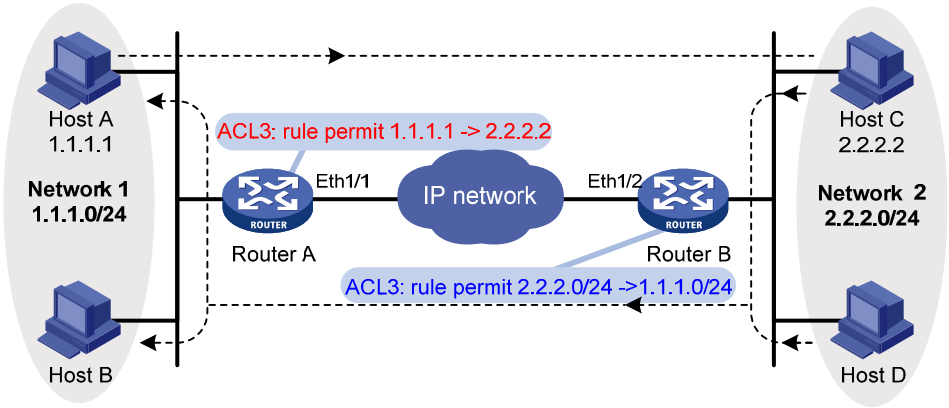
为保证SA的成功建立，建议将IPsec对等体上的访问控制列表镜像配置，即保证两端要保护的数据流范围是镜像的。例如，图 1-5中Router A和Router B上的ACL配置都是完全镜像对称的，因此用于保护主机Host A与主机Host C之间、子网Network 1 与子网Network 2 之间流量的SA均可成功建立。

图1-5 镜像 ACL 配置



若IPsec对等体上的访问控制列表配置非镜像，那么只有一种情况下，SA的协商是可以建立的。这种情况就是，一端的访问控制列表规则定义的范围是另外一端的子集。如图 1-6所示，Router A上的访问控制列表允许的范围（Host A->Host C）是Router B上访问控制列表（Network 2->Network 1）的子集。

图1-6 非镜像 ACL 配置



但需要注意的是，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起的协商是可以成功的，例如 Host A->Host C；从粗粒度一方向细粒度一方发起的协商是不能成功的，例如 Host C->Host B、Host D->Host A 等。

3. 数据流的保护方式

目前，设备支持的数据流的保护方式包括以下两种：

- 标准方式：一条隧道保护一条数据流。ACL 中的每一个规则对应的数据流都会由一条单独创建的隧道来保护；
- 聚合方式：一条隧道保护 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隧道来保护。该方式目前仅在一端设备使用 Comware V3 软件版本，而另一端使用 Comware V5 软件版本时使用，且仅在 IKE 协商安全策略的情况下可配。

说明

- ACL 的具体配置请参见“ACL 和 QoS 配置指导”中的“ACL”。
- 若在接口上同时使能 IPsec 和 QoS，同一个 IPsec 安全联盟的数据流如果被 QoS 分类进入不同队列，会导致部分报文发送乱序。由于 IPsec 具有防重放功能，IPsec 入方向上对于防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 结合使用时，必须保证 IPsec 分类与 QoS 分类规则配置保持一致。IPsec 的分类规则完全由引用的 ACL 规则确定，QoS 分类规则的配置请参考“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

1.3.3 配置IPsec安全提议

IPsec 安全提议是 IPsec 安全策略或者 IPsec 安全框架的一个组成部分，它用于保存 IPsec 需要使用的特定安全协议、加密/认证算法等，为 IPsec 协商 SA 提供各种安全参数。

表1-2 配置安全提议

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*	必选 缺省情况下，没有任何IPsec安全提议存在 系统中最多可以创建10000个IPsec安全提议
配置IPsec安全提议采用的安全协议		**transform** { **ah** | **ah-esp** | **esp** }	可选 缺省情况下，采用ESP协议
配置安全算法	配置ESP协议采用的加密算法	**esp encryption-algorithm** { **3des** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** | **des** }	三者至少选其一 缺省情况下，未指定安全算法 对于配置ESP协议采用的加密算法，在FIPS模式下，设备不支持DES和3DES算法，缺省加密算法为AES-128；在非FIPS模式下，缺省加密算法为DES 对于配置ESP协议采用的认证算法，在FIPS模式下，设备不支持MD5算法，缺省认证算法为SHA-1；在非FIPS模式下，缺省认证算法为MD5。 对于配置AH协议采用的认证算法，在FIPS模式下，设备不支持MD5算法，缺省认证算法为SHA-1，在非FIPS模式下，缺省认证算法为MD5。 在FIPS模式下，必须同时设置加密算法和认证算法 只有选择了相应的IPsec安全协议后，该安全协议所需的安全算法才可配置。例如，如果使用**transform**命令选择了**esp**，那么只有ESP所需的安全算法才可配置，而AH所需的安全算法则不能配置。ESP协议允许对报文同时进行加密和认证，或只加密，或只认证。
	配置ESP协议采用的认证算法	**esp authentication-algorithm** { **md5** | **sha1** }	
	配置AH协议采用的认证算法	**ah authentication-algorithm** { **md5** | **sha1** }	
配置安全协议对IP报文的封装形式		**encapsulation-mode** { **transport** | **tunnel** }	可选 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安全隧道两端地址相同的情况下 若要配置应用于IPv6路由协议的手工安全策略，则该安全策略引用的安全提议仅支持传输模式的封装模式

说明

可对 IPsec 安全提议进行修改，但对已协商成功的 SA，新修改的 IPsec 安全提议并不起作用，即 SA 仍然使用原来的 IPsec 安全提议（除非使用 **reset ipsec sa** 命令重置），只有新协商的 SA 将使用新的 IPsec 安全提议。

1.3.4 配置IPsec安全策略

IPsec 安全策略规定了对什么样的数据流采用什么样的安全提议。一条 IPsec 安全策略由“名字”和“顺序号”共同唯一确定。

IPsec 安全策略分为以下几种类型：

- 手工配置方式：需要用户手工配置密钥、SPI 等参数，在隧道模式下还需要手工配置安全隧道两个端点的 IP 地址。
- IKE 协商方式：由 IKE 自动协商生成各参数。
- GDOI 方式：由 GM 从 KS 上获取所在 GDOI 组的安全策略信息（保护的数据流信息、加密算法、认证算法、封装模式等）。

1. 手工配置IPsec安全策略

(1) 配置准备

手工配置 IPsec 安全策略时，除完成该安全策略需要引用的访问控制列表及 IPsec 安全提议的配置之外，为保证 SA 的协商成功，安全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、安全算法和报文封装形式；
- 当前端点的对端地址与对端的本端地址应保持一致；
- 应分别设置出方向 SA 和入方向 SA 的参数，且保证 SA 的唯一性，即不同 SA 必须对应不同的 SPI；
- 本端和对端 SA 的 SPI 及密钥必须是完全匹配的。即，本端的入方向 SA 的 SPI 及密钥必须和对端的出方向 SA 的 SPI 及密钥相同；本端的出方向 SA 的 SPI 及密钥必须和对端的入方向 SA 的 SPI 及密钥相同；
- 两端 SA 使用的密钥应当以相同的方式输入。即，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。而且，任何一端出入方向的 SA 使用的密钥也应当以相同的方式输入。

对于要应用于 IPv6 路由协议的 IPsec 安全策略，无需配置访问控制列表和隧道地址，但是应该符合以下要求：

- 本端出方向 SA 的 SPI 及密钥必须和本端入方向 SA 的 SPI 及密钥保持一致；
- 同一个范围内的，所有设备上的安全策略所引用的安全提议采用的安全协议、安全算法和报文封装形式要相同，而且所有设备上的 SA 的 SPI 及密钥均要保持一致。该范围与协议相关：对于 OSPFv3，它是 OSPFv3 邻居之间或一个 OSPFv3 区域内；对于 RIPng，它是 RIPng 直连邻居之间或一个 RIPng 进程内；对于 IPv6 BGP，它是 IPv6 BGP 邻居之间或一个对等体组内。

(2) 手工配置 IPsec 安全策略

表1-3 手工配置 IPsec 安全策略

操作		命令	说明
进入系统视图		**system-view**	-
用手工方式创建一条IPsec安全策略，并进入IPsec安全策略视图		**ipsec policy** *policy-name seq-number* **manual**	必选 缺省情况下，没有任何IPsec安全策略存在
配置IPsec安全策略引用的访问控制列表		**security acl** [**ipv6**] *acl-number*	若IPsec安全策略要应用于IPv6路由协议，则无需此配置，其它情况必选 缺省情况下，IPsec安全策略没有指定访问控制列表 可支持保护VPN间的数据流 一条IPsec安全策略只能引用一条访问控制列表，如果设置IPsec安全策略引用了多于一个访问控制列表，最后引用的那条访问控制列表才有效。
配置IPsec安全策略所引用的IPsec安全提议		**transform-set** *transform-set-name*	必选 缺省情况下，IPsec安全策略没有引用任何IPsec安全提议 通过手工方式建立SA，一条IPsec安全策略只能引用一个安全提议，并且如果已经引用了IPsec安全提议，必须先取消原先的IPsec安全提议才能引用新的IPsec安全提议。
配置隧道的起点与终点	配置安全隧道的本端地址	**tunnel local** [**ipv6**] *ip-address*	若IPsec安全策略要应用于IPv6路由协议，则无需此配置，其它情况必选 缺省情况下，没有配置安全隧道的本端地址和对端地址
	配置安全隧道的对端地址	**tunnel remote** [**ipv6**] *ip-address*	
配置SA的安全参数索引参数		**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*	必选
配置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 authentication-hex** { **inbound** | **outbound** } **ah** [**cipher** | **simple**] *hex-key*	二者必选其一 **sa string-key**命令在FIPS模式下不可用
	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-key*	
	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-key*	至少选其一 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 **sa string-key**命令在FIPS模式下不可用
	配置ESP协议的认证密钥（以16进制方式输入）	**sa authentication-hex** { **inbound** | **outbound** } **esp** [**cipher** | **simple**] *hex-key*	
	配置ESP协议的加密密钥（以16进制方式输入）	**sa encryption-hex** { **inbound** | **outbound** } **esp** [**cipher** | **simple**] *hex-key*	

说明

- 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。
- 对于手工方式创建的 IPsec 安全策略，不能直接修改它的创建方式，而必须先删除该 IPsec 安全策略然后再重新创建。

2. 配置使用IKE协商方式的IPsec安全策略

在采用 IKE 方式配置 IPsec 安全策略时，有以下两种方式：

- 直接配置 IPsec 安全策略，在 IPsec 安全策略视图中定义需要协商的各参数；
- 引用 IPsec 安全策略模板创建 IPsec 安全策略，在 IPsec 安全策略模板中定义需要协商的各参数。应用了该类安全策略的设备不能发起协商，仅可以响应远端设备的协商请求。由于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) 配置准备

在配置 IKE 协商 IPsec 安全策略之前，需要完成以下配置：

- 配置所引用的访问控制列表和 IPsec 安全提议。
- 配置IKE对等体。具体配置请参见“2.5 配置IKE对等体”。

为保证 IKE 协商成功，IPsec 安全策略中所有配置的参数必须在本端和对端相匹配。

(2) 配置使用 IKE 协商方式的安全策略

- 直接配置使用 IKE 协商方式的 IPsec 安全策略

表1-4 直接配置使用 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IPsec安全策略，并进入IPsec安全策略视图	**ipsec policy** *policy-name seq-number* **isakmp**	必选 缺省情况下，没有IPsec安全策略存在
配置用于描述IPsec安全策略的IPsec连接名	**connection-name** *name*	可选 缺省情况下，无IPsec连接名
配置IPsec安全策略引用的访问控制列表	**security acl** [**ipv6**] *acl-number* [**aggregation**]	必选 缺省情况下，IPsec安全策略没有指定访问控制列表

操作	命令	说明
配置IPsec安全策略所引用的IPsec安全提议	**transform-set** *transform-set-name*&<1-6>	必选 缺省情况下，IPsec安全策略没有引用任何提议 通过IKE协商建立SA，一条IPsec安全策略最多可以引用六个IPsec安全提议，IKE协商将在安全隧道的两端搜索能够完全匹配的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不能建立，需要被保护的报文将被丢弃。
在IPsec安全策略中引用IKE对等体	**ike-peer** *peer-name*	必选 IPsec安全策略中不能引用已经被安全框架引用的IKE对等体，反之亦然
配置使用此IPsec安全策略发起协商时使用PFS特性	**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }	可选 缺省情况下，IPsec安全策略发起协商时没有使用PFS特性 如果本端配置了PFS特性，则发起协商的对端也必须配置PFS特性，而且本端和对端指定的DH组必须一致，否则协商会失败 PFS（Perfect Forward Secrecy，完善的前向安全性）特性请参见“2.1.1 IKE的安全机制” **dh-group1**参数在FIPS模式下不可用
配置SA的生存周期	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	可选 缺省情况下，IPsec安全策略的SA生存周期为当前全局的SA生存周期值 IKE为IPsec协商建立SA时，采用本地设置的和对端提议的生存周期中较小的一个
使能IPsec安全策略	**policy enable**	可选 缺省情况下，IPsec安全策略处于使能状态
退回系统视图	**quit**	-
配置全局SA的生存周期	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	可选 缺省情况下，SA基于时间的生存周期为3600秒，基于流量的生存周期为1843200千字节

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

IPsec 安全策略模板可配置的参数与 IKE 方式的 IPsec 安全策略相同，只是很多参数是可选的。

- 必须配置的参数：IPsec 安全提议和 IKE 对等体，
- 可选配的参数：访问控制列表、PFS 特性和生存周期。与直接方式不同的是，用于定义保护对象范围的访问控制列表在这种方式下是可选的，该参数在未配置的情况下，相当于支持最大范围的保护，即接受协商发起端的访问控制列表设置。

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**	-
创建一个IPsec安全策略模板，并进入IPsec安全策略模板视图	**ipsec policy-template** *template-name seq-number*	必选 缺省情况下，没有任何IPsec安全策略模板存在
配置IPsec安全策略引用的访问控制列表	**security acl** [**ipv6**] *acl-number*	可选 缺省情况下，IPsec安全策略没有指定访问控制列表
配置IPsec安全策略所引用的安全提议	**transform-set** *transform-set-name*&<1-6>	必选 缺省情况下，IPsec安全策略没有引用任何提议 通过IKE协商建立SA，一条IPsec安全策略最多可以引用六个IPsec安全提议，IKE协商将在安全隧道的两端搜索能够完全匹配的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不能建立，需要被保护的报文将被丢弃
在IPsec安全策略中引用IKE对等体	**ike-peer** *peer-name*	必选
配置使用此IPsec安全策略发起协商时使用PFS特性	**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }	可选 缺省情况下，IPsec安全策略发起协商时没有使用PFS特性 如果本端配置了PFS特性，则发起协商的对端也必须配置PFS特性，而且本端和对端指定的DH组必须一致，否则协商会失败 PFS（Perfect Forward Secrecy，完善的前向安全性）特性请参见“2.1.1 IKE的安全机制” **dh-group1**参数在FIPS模式下不可用
配置SA的生存周期	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	可选 缺省情况下，IPsec安全策略的SA生存周期为当前全局的SA生存周期值 IKE为IPsec协商建立SA时，采用本地设置的和对端提议的生存周期中较小的一个

操作	命令	说明
使能IPsec安全策略	**policy enable**	可选 缺省情况下，IPsec安全策略处于使能状态
退回系统视图	**quit**	-
配置全局SA的生存周期	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	可选 缺省情况下，SA基于时间的生存周期为3600秒，基于流量的生存周期为1843200千字节
引用IPsec安全策略模板创建一条IPsec安全策略	**ipsec policy** *policy-name seq-number* **isakmp template** *template-name*	必选 缺省情况下，没有IPsec安全策略存在

说明

使用 IKE 协商方式时，ACL 只支持模糊匹配。

1.3.5 在接口上应用IPsec安全策略组

IPsec 安全策略组是所有具有相同名字、不同顺序号的 IPsec 安全策略的集合。在同一个 IPsec 安全策略组中，顺序号越小的 IPsec 安全策略，优先级越高。

为使定义的 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（逻辑的或物理的）上应用一个 IPsec 安全策略组，以对数据进行保护。当取消 IPsec 安全策略组在接口上的应用后，此接口便不再具有 IPsec 的安全保护功能。

当从一个接口发送数据时，将按照从小到大的顺序号查找 IPsec 安全策略组中每一条安全策略。如果数据匹配了一条 IPsec 安全策略引用的访问控制列表，则使用这条 IPsec 安全策略对数据进行处理；如果数据没有匹配 IPsec 安全策略引用的访问控制列表，则继续查找下一条 IPsec 安全策略；如果数据与所有 IPsec 安全策略引用的访问控制列表都不匹配，则直接被发送（IPsec 不对数据加以保护）。

IPsec 安全策略除了可以应用到串口、以太网口等实际物理接口上之外，还能够应用到 Tunnel、Virtual Template 等虚接口上。这样就可以根据实际组网要求，在如 GRE、L2TP 等隧道上应用。

表1-6 在接口上应用 IPsec 安全策略组

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*	-
应用指定的IPsec安全策略组	**ipsec policy** *policy-name*	必选

说明

一个接口只能应用一个 IPsec 安全策略组。通过 IKE 方式创建的 IPsec 安全策略可以应用到多个接口上，通过手工创建的 IPsec 安全策略只能应用到一个接口上。

1.3.6 使能加密引擎功能

加密引擎是设备上的一个协处理器，为 IPsec 的处理提供一个加/解密算法接口。分为两种情况：

- 若加密引擎功能处于使能状态，则由加密引擎进行 IPsec 处理；
- 若加密引擎功能处于禁止状态或加密引擎异常，并且主体软件备份功能处于使能状态，则由主体软件 IPsec 模块进行 IPsec 处理；若主体软件备份功能处于禁止状态，则报文被丢弃。

表1-7 使能加密引擎功能

操作	命令	说明
进入系统视图	**system-view**	-
使能加密引擎功能	**cryptoengine enable** [**slot** *slot-number*]	可选 缺省情况下，加密引擎功能处于使能状态

1.3.7 使能解封装后IPsec报文的ACL检查功能

在隧道模式下，对于解封装之后的入方向 IPsec 报文，有可能出现报文的内部 IP 头不在当前 IPsec 安全策略配置的 ACL 保护范围内的情况，如网络中恶意构造的攻击报文头可能不在此范围，所以需要重新检查报文内部 IP 头是否在 ACL 保护范围内。使能该功能后可以保证 ACL 检查不通过的报文被丢弃，从而提高网络安全性。

表1-8 使能解封装后 IPsec 报文的 ACL 检查功能

操作	命令	说明
进入系统视图	**system-view**	-
使能解封装后IPsec报文的ACL检查功能	**ipsec decrypt check**	可选 缺省情况下，解封装后IPsec报文的ACL检查功能处于使能状态

1.3.8 配置IPsec抗重放功能

通常，重放报文是指已经处理过的报文。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，如果收到报文的序列号与已经解封装过的报文序列号相同，或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。

由于对重放报文的解封装无实际作用，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，实际上构成了拒绝服务攻击。通过使能 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。

另外，在某些特定环境下，业务数据报文的序列号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。

表1-9 配置 IPsec 抗重放功能

操作	命令	说明
进入系统视图	**system-view**	-
使能IPsec抗重放检测功能	**ipsec anti-replay check**	可选 缺省情况下，IPsec抗重放检测功能处于使能状态
配置IPsec抗重放窗口宽度	**ipsec anti-replay window** *width*	可选 缺省情况下，IPsec抗重放窗口宽度为32

提示

- IPsec 抗重放检测功能缺省是使能的，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。

说明

按照 IPsec 协议，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。因此该功能使能与否与对手工方式生成的 IPsec SA 没有影响。

1.3.9 配置报文信息预提取功能

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 使用被封装报文的外层 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，则需要配置报文信息预提取功能来实现。

关于 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1-10 配置报文信息预提取功能

操作	命令	说明
进入系统视图	**system-view**	-
进入安全策略视图/安全策略模板视图	**ipsec policy** *policy-name seq-number* [**isakmp** | **manual**]	二者必选其一
	ipsec policy-template *template-name seq-number*	

操作	命令	说明
配置报文信息预提取功能	**qos pre-classify**	必选 缺省情况下，报文信息预提取功能处于关闭状态

1.3.10 配置IPsec无效SPI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）导致本端 IPsec SA 丢失时，会造成 IPsec 流量黑洞现象：一端（接收端）的 IPsec SA 已经完全丢失，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。

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 SA，若接收方找不到处理该报文的 SA，则认为此报文的 SPI 无效。使能了 IPsec 无效 SPI 恢复功能的接收端收到无效 SPI 的 IPsec 报文后，就触发本端 IKE 向对端发送 INVALID SPI NOTIFY 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。

由于 IKE 向对方发送 INVALID SPI NOTIFY 消息有可能会给设备带来发生 DoS（Denial of Sevice）攻击的风险，因此缺省情况下的 IPsec 无效 SPI 恢复功能是关闭的，接收端将默认丢弃无效 SPI 的 IPsec 报文。

表1-11 配置 IPsec 无效 SPI 恢复功能

操作	命令	说明
进入系统视图	**system-view**	-
使能IPsec无效SPI恢复功能	**ipsec invalid-spi-recovery enable**	可选 缺省情况下，IPsec无效SPI恢复功能处于关闭状态

1.3.11 配置IPsec反向路由注入功能

RRI 只需要在企业总部网关设备上的 IPsec 策略视图或者 IPsec 安全策略模板视图下配置。

RRI 有静态和动态两种工作机制，配置了 RRI 的设备采用哪种工作机制，由 **reverse-route** 命令中是否指定了参数 **static** 决定。

- 静态工作机制（指定 **static** 参数）：RRI 基于 IPsec 安全策略引用的 ACL 中各规则的目的配置信息来静态生成静态路由（对 ACL 规则中的不同目的信息会生成不同的路由）。该静态路由的下一跳地址可以通过 **reverse-route** 命令中的参数 **remote-peer** *ip-address* 来指定，不指定该参数的情况下为配置的隧道对端的 IP 地址。当 IPsec 策略中的 RRI 功能被关闭，或者策略中引用的 ACL、对端安全网关的 IP 地址配置被删除时，该 IPsec 策略下由 RRI 生成的所有静态路由表项会被删除。当企业分支网络结构基本不变时，可以配置此类型的 RRI 添加到达分支的静态路由。

- 动态工作机制（未指定 **static** 参数）：RRI 基于与分支通信的 IPsec SA 的建立而动态生成静态路由。该静态路由的目的地址为本端学习到的被保护的分支网络地址，下一跳地址可通过 **reverse-route** 命令中的参数 **remote-peer** *ip-address* 来指定，不指定该参数的情况下为本端在 IPsec SA 协商过程中学习到的隧道的对端地址。当 IPsec SA 被删除时，相应的静态路由表项也会同时被删除。当企业分支结构容易发生变化时，如分支用户使用拨号方式动态获取 IP 地址接入 Internet，则可以配置此类型的 RRI 动态添加到达分支的静态路由，可减少因分支变动而对总部网关配置的频繁调整。

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：当设备上还有其它方式配置的到达相同目的地的路由时，如果为它们指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。同时，还可以通过修改静态路由的 Tag 属性值，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。

表1-12 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**	-
进入安全策略视图/安全策略模板视图	**ipsec policy** *policy-name seq-number* [**isakmp** | **manual**]	二者必选其一
	ipsec policy-template *template-name seq-number*	
开启IPsec反向路由注入功能	**reverse-route** [**remote-peer** *ip-address* [**gateway** | **static**] | **static**]	必选 缺省情况下，IPsec反向路由注入功能处于关闭状态
配置IPsec反向路由注入生成的静态路由的优先级	**reverse-route preference** *preference-value*	可选 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
配置IPsec反向路由注入生成的静态路由的Tag值	**reverse-route tag** *tag-value*	可选 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

说明

- IPsec 反向路由注入功能在隧道模式和传输模式下都支持。
- 若对 IPsec 反向路由注入静态路由属性进行修改，则在静态工作机制下的 RRI 会根据新的路由属性重新生成静态路由，而在动态工作机制下的 RRI 不会修改已生成的静态路由的路由属性，修改后的静态路由属性仅对新增的静态路由有效。

1.3.12 使能加密前/加密后分片功能

加密前分片功能是指，如果待封装报文封装后的大小超过接口 MTU 值，则对报文先分片再封装。

加密后分片功能是指，对待封装报文先进行封装，封装后的报文尺寸如果超过接口 MTU 值，则再进行分片。

若设备的某接口上应用了 IPsec GDOI 安全策略，则必须使能加密前分片功能，否则会导致本端接口上封装后被分片的报文在对端因无法重组而解密失败。

表1-13 使能加密前/加密后分片功能

操作	命令	说明
进入系统视图	**system-view**	-
使能加密前分片功能	**ipsec fragmentation before-encryption enable**	二者可选其一 缺省情况下，加密前分片功能处于开启状态
使能加密后分片功能	**undo ipsec fragmentation before-encryption enable**	

说明

IPsec GDOI 安全策略的相关介绍请参见“安全配置指导”中的“Group Domain VPN”。

1.4 基于IPsec虚拟隧道接口建立IPsec安全隧道

1.4.1 IPsec虚拟隧道接口配置任务简介

基于 IPsec 虚拟隧道接口建立 IPsec 安全隧道的基本配置思路如下：

(1) 通过配置 IPsec 安全提议，指定安全协议、认证算法和加密算法、封装模式等；

(2) 通过配置 IPsec 安全框架，选择保护数据流时使用的安全提议，设置 IKE 对等体的参数（即 IKE 协商的模式、所需要的密钥等）和 SA 的生存周期等；

(3) 通过配置 IPsec 虚拟隧道接口，并在 IPsec 虚拟隧道接口视图下应用 IPsec 安全框架使得 IPsec 虚拟隧道的配置生效。

说明

与使用 IPsec 安全策略建立 IPsec 隧道相比，定义 IPsec 安全框架时无须指定需要保护的数据流的范围，即 IPsec 安全框架默认保护流的范围是所有流。

表1-14 IPsec 虚拟隧道接口配置任务简介

配置任务	说明	详细配置
配置IPsec安全提议	必选 IPsec虚拟隧道接口引用的IPsec安全提议只能支持隧道模式	1.3.3
配置IPsec安全框架	必选	1.4.2
配置IPsec虚拟隧道接口	必选	1.4.3
在IPsec虚拟隧道接口上配置QoS报文信息预提取功能	可选	1.4.4

配置任务	说明	详细配置
在IPsec虚拟隧道接口上配置QoS策略	可选	1.4.5
使能加密引擎功能	可选	1.3.6
配置IPsec抗重放功能	可选	1.3.8

1.4.2 配置IPsec安全框架

由前文可知，IPsec 安全策略由“名字”和“顺序号”共同唯一确定，相同名字的策略为一个 IPsec 策略组。每条策略可以通过 ACL 配置来保护不同的数据流。将 IPsec 安全策略组应用到接口上后，当有用户流量经该接口转发时，IPsec 会根据各策略来筛选感兴趣的流来进行保护，这样在一个接口下会生成多条 IPsec 隧道。

一个 IPsec 安全框架相当于一个 IPsec 安全策略，与 IPsec 安全策略不同的是，IPsec 安全框架由“名字”唯一确定，且不支持配置 ACL。IPsec 安全框架定义了对数据流进行 IPsec 保护所使用的 IPsec 安全提议，以及用于自动协商 SA 所需要的 IKE 协商参数。在 IPsec 虚拟隧道接口下应用 IPsec 安全框架后只会生成一条 IPsec 隧道，并对所有路由到该隧道接口的数据流进行 IPsec 保护。

目前，IPsec 安全框架只能应用于 DVPN 虚拟隧道接口和 IPsec 虚拟隧道接口下，根据 IPsec 安全框架协商出的 SA 将会对所有路由到隧道接口下的 IP 流量进行 IPsec 保护。

在配置 IPsec 安全框架之前，需要完成以下任务：

- 配置需要引用的IPsec安全提议。具体配置请参见“1.3.3 配置IPsec安全提议”。
- 配置IKE对等体。具体配置请参见“2.5 配置IKE对等体”。

为保证 IKE 协商成功，IPsec 安全框架中所有配置的参数必须在本端和对端相匹配。

说明

- 根据 IPsec 安全框架进行 IKE 协商时，选用的本端地址是通过 IPsec 虚拟隧道接口的源地址来指定的，IPsec 安全框架所引用的 IKE 对等体中的 **local-address** 配置不生效。
- 根据 IPsec 安全框架进行 IKE 协商时，使用的对端地址是通过 IPsec 虚拟隧道接口的目的地址指定的，IPsec 安全框架所引用的 IKE 对等体中的 **remote-address** 配置不生效。当 IPsec 虚拟隧道接口的目的地址未配置的时候，本端不能作为发起方主动发起 IKE 协商，只能被动接受对端发起的协商。
- DVPN（Dynamic Virtual Private Network，动态虚拟私有网络）是企业网各分支机构使用动态地址接入公网的情况下，在各分支机构间建立的一种动态 VPN。DVPN 虚拟隧道接口的相关介绍请参见“三层技术-IP 业务配置指导”中的“DVPN”。

表1-15 配置 IPsec 安全框架

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安全框架，并进入IPsec安全框架视图	**ipsec profile** *profile-name*	必选 缺省情况下，没有IPsec安全框架存在
配置IPsec安全框架引用的IPsec安全提议	**transform-set** transform-*name*&<1-6>	必选 缺省情况下，IPsec安全框架没有引用任何IPsec安全提议
在IPsec安全框架中引用IKE对等体	**ike-peer** *peer-name*	必选 IPsec安全框架中不能引用已经被IPsec安全策略引用的IKE对等体，反之亦然
配置使用此IPsec安全框架发起协商时使用PFS特性	**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }	可选 缺省情况下，IPsec安全框架发起协商时没有使用PFS特性 PFS（Perfect Forward Secrecy，完善的前向安全性）特性请参见“2.1.1 IKE的安全机制” **dh-group1**参数在FIPS模式下不可用
配置SA的生存周期	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	可选 缺省情况下，IPsec安全框架的SA生存周期为当前全局的SA生存周期值
退回系统视图	**quit**	-
配置全局SA的生存周期	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	可选 缺省情况下，SA基于时间的生存周期为3600秒，基于流量的生存周期为1843200千字节

1.4.3 配置IPsec虚拟隧道接口

IPsec 虚拟隧道接口就是采用 IPsec 协议对报文进行封装的隧道接口。

使用 IPsec 虚拟隧道接口保护数据流的基本配置思路如下：

(1) 创建一个 Tunnel 接口，并在 Tunnel 接口视图下指定当前隧道的封装模式为 IPsec 虚拟隧道接口；

(2) 配置 IPsec 虚拟隧道接口的源地址，此地址将作为 IKE 协商时本端身份的标识；

(3) 若希望本端 IPsec 虚拟隧道接口主动发起 IKE 协商，则需要配置 Tunnel 接口的目的地址；若只希望被动接纳对端发起的 IKE 协商，则可以不配置 Tunnel 接口目的地址。

(4) 在 IPsec 虚拟隧道接口上应用安全框架，使其具有 IPsec 的安全保护功能。当取消应用在 IPsec 虚拟隧道接口上的安全框架后，IPsec 虚拟隧道接口将不再具有 IPsec 的安全保护功能。

仅当 IPsec 虚拟隧道接口链路状态 up 时，才能表示该接口具备了 IPsec 的安全保护功能。IPsec 虚拟隧道接口链路状态 up 的条件包括：

- Tunnel 接口源地址为设备上有效的本地地址；
- Tunnel 接口上应用了配置正确的 IPsec 安全框架；
- 本端安全网关已经与对端安全网关协商生成了有效的 SA（执行 **display ike sa** 能看到第一阶段 IKE SA 和第二阶段 IPsec SA 已经存在）。

表1-16 配置 IPsec 虚拟隧道接口

操作		命令	说明
进入系统视图		**system-view**	-
创建一个Tunnel接口，并进入Tunnel接口视图		**interface tunnel** *number*	必选 缺省情况下，设备上无隧道接口
配置Tunnel接口的IPv4私网地址		**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	必选其一 缺省情况下，Tunnel接口上没有设置任何私网地址
配置Tunnel接口的IPv6私网地址	配置IPv6全球单播地址或站点本地地址	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-addressIprefix-length* }	
		ipv6 address *ipv6-addressIprefix-length* **eui-64**	
	配置IPv6链路本地地址	**ipv6 address auto link-local**	
		ipv6 address *ipv6-address* **link-local**	
配置隧道封装模式为IPsec虚拟隧道		**tunnel-protocol ipsec** { **ipv4** | **ipv6** }	必选 缺省情况下，隧道的封装模式为GRE
配置Tunnel接口的源地址或源接口，即发送IPsec报文的实际物理接口地址		**source** { *ip-address* | *interface-type interface-number* }	必选 缺省情况下，Tunnel接口上未配置源地址或源接口 若采用配置源接口的形式，则Tunnel接口的源地址为源接口的主IP地址
配置Tunnel接口的目的地址		**destination** *ip-address*	可选 缺省情况下，Tunnel接口上未配置目的地址 对于IKE协商的发起方，目的地址必须配置；对于IKE协商的响应方，目的地址可选择配置
在Tunnel接口上应用安全框架		**ipsec profile** *profile-name*	必选 应用的安全框架必须是已经存在的，且未应用在DVPN隧道接口上

说明

- **interface tunnel**、**tunnel-protocol**、**source** 和 **destination** 命令的详细介绍请参见“三层技术-IP 业务命令参考”中的“隧道”。
- IPsec 安全框架既可以应用在 IPsec 虚拟隧道接口上，也可以应用在 DVPN 虚拟隧道接口上，但是同一个 IPsec 安全框架不能同时应用于两种类型的隧道接口上。
- 一个 Tunnel 接口上只能应用一个 IPsec 安全框架。
- 一个 IPsec 安全框架可应用在多个 IPsec 虚拟隧道接口上，但同时只能在一个 IPsec 虚拟隧道接口上生效，因此通常建议一个 IPsec 安全框架仅应用在一个 IPsec 虚拟隧道接口上。

1.4.4 IPsec虚拟隧道接口上配置报文信息预提取功能

由于 IPsec 的隧道封装将会隐藏原始 IP 数据流的五元组信息（源 IP 地址、目的 IP 地址、源端口、目的端口、协议类型），为了能够利用原始数据流的信息对加封装后的 IPsec 报文进行 QoS 处理，需要在隧道加封装之前提取出原始 IP 数据流的五元组信息。

通过在 IPsec 虚拟隧道接口上配置报文信息预提取功能，可以满足以上需求。IPsec 虚拟隧道接口上预先提取出的报文信息可用来作为物理出接口上实施 QoS 策略（例如，进行流分类、设置 IP 报文的服务优先级、物理接口限速以及拥塞处理等）的依据。

需要注意的是，仅在 IPsec 虚拟隧道接口上单独使用报文信息预提取功能并无实际意义，必须与物理出接口上应用 QoS 策略一起组合使用才有效果，即需要满足以下两个配置才能真正实现对 IPsec 报文的 QoS 处理：

- IPsec 虚拟隧道接口配置报文信息预提取功能；
- IPsec 虚拟隧道接口对应的物理接口上应用 QoS 策略。关于接口上应用 QoS 策略的具体配置请参考“ACL 和 QoS 配置指导”中的“QoS 配置方式”。

表1-17 IPsec 虚拟隧道接口上配置报文信息预提取功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Tunnel接口视图	**interface tunnel** *number*	-
配置报文信息预提取功能	**qos pre-classify**	必选 缺省情况下，未配置报文信息预提取功能 该命令的详细介绍请参考“ACL和QoS命令参考”中的“QoS拥塞管理”

注意

当应用在物理出接口上的QoS策略提供拥塞服务时，这种配合实施的QoS方案可能会导致IPsec报文乱序。其可能的影响是，未能以IPsec报文头中序列号要求的顺序到达对端IPsec网关的IPsec报文，会被对端IPsec网关进行的抗重放检测当作重放报文丢弃。关于IPsec抗重放功能的介绍及配置请参见“1.3.8 配置IPsec抗重放功能”。

1.4.5 IPsec虚拟隧道接口上应用QoS策略

“IPsec 虚拟隧道接口上应用 QoS 策略”方案与“IPsec 虚拟隧道接口上配置报文信息预提取＋物理接口上应用 QoS 策略”方案的实施效果相同，但前者更为简洁有效。

在 IPsec 虚拟隧道接口上应用 QoS 策略后，QoS 策略将在 IPsec 隧道加封装之前的原始报文上实施，并且内外层 IP 报文头的服务优先级设置相同。而且，由于 QoS 的拥塞服务是在 IPsec 隧道封装之前的报文上生效，因此加封装后的报文顺序与原始报文经过 QoS 拥塞处理后的顺序无关，会按照正常的顺序到达对端，也就不会因为 QoS 拥塞处理而产生乱序。

表1-18 在 IPsec 虚拟隧道接口上配置 QoS 策略

操作	命令	说明
进入系统视图	**system-view**	-
进入Tunnel接口视图	**interface tunnel** *number*	-
在Tunnel上应用QoS策略	**qos apply policy** *policy-name* { **inbound** | **outbound** }	必选 该命令的详细介绍请参考“ACL和QoS命令参考”中的“QoS配置方式”

1.5 配置IPsec保护IPv6路由协议

使用 IPsec 安全策略建立 IPsec 安全隧道保护 IPv6 路由协议的基本配置思路如下：

(1) 配置 IPsec 安全提议：指定安全协议、认证算法和加密算法、封装模式等；

(2) 配置手工方式的 IPsec 安全策略：指定 SA 的 SPI 和密钥；

(3) 在路由协议上应用 IPsec 安全策略。

表1-19 IPsec 虚拟隧道接口配置任务简介

配置任务	说明	详细配置
配置IPsec安全提议	必选	1.3.3
配置手工方式的IPsec安全策略	必选 无需配置访问控制列表和隧道地址	1.3.4 1.
在路由协议上应用IPsec安全策略	必选	分别参考“三层技术-IP路由配置指导”中的“IPv6 BGP”、“OSPFv3”和“RIPng”

提示

请不要将一个保护IPv6路由协议的安全策略同时应用到接口上。如果同时应用，则接口收到经IPsec保护的IPv6路由协议报文后，会因ACL检测失败而将其丢弃。

1.6 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 policy** [**brief** | **name** *policy-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec安全策略模板的信息	**display ipsec policy-template** [**brief** | **name** *template-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec安全框架的配置信息	**display ipsec profile** [**name** *profile-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec安全提议的信息	**display ipsec transform-set** [*transform-set-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示SA的相关信息	**display ipsec sa** [**brief** | **policy** *policy-name* [*seq-number*] | **remote** [**ipv6**] *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec处理报文的统计信息	**display ipsec statistics** [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec隧道的信息	**display ipsec tunnel** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除已经建立的SA	**reset ipsec sa** [**parameters** [**ipv6**] *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** [**ipv6**] *ip-address*]
清除IPsec的报文统计信息	**reset ipsec statistics**

1.7 IPsec典型配置举例

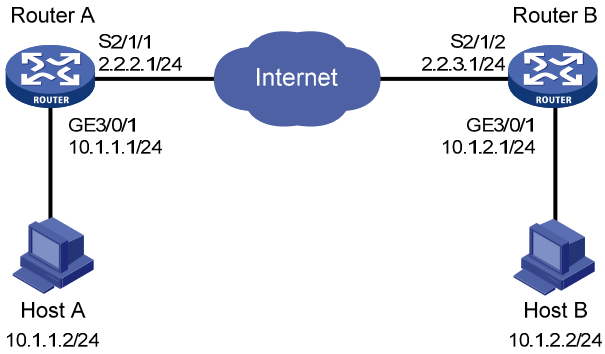
1.7.1 采用手工方式建立保护IPv4 报文的IPsec安全隧道

1. 组网需求

- 在 Router A 和 Router B 之间建立一个安全隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。
- 安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。

2. 组网图

图1-7 IPsec 配置组网图



3. 配置步骤

(1) 配置 Router A

配置一个访问控制列表，定义由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。

```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[RouterA-acl-adv-3101] quit
```

配置到 Host B 的静态路由。

```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 serial 2/1/1
```

创建名为 tran1 的 IPsec 安全提议。

```
[RouterA] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[RouterA-ipsec-transform-set-tran1] transform esp
```

选择算法。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建一条 IPsec 安全策略，协商方式为 manual。

```
[RouterA] ipsec policy map1 10 manual
```

引用访问控制列表。

```
[RouterA-ipsec-policy-manual-map1-10] security acl 3101
```

引用 IPsec 安全提议。

```
[RouterA-ipsec-policy-manual-map1-10] transform-set tran1
```

配置对端地址。

```
[RouterA-ipsec-policy-manual-map1-10] tunnel remote 2.2.3.1
```

配置本端地址。

```
[RouterA-ipsec-policy-manual-map1-10] tunnel local 2.2.2.1
```

配置 SPI。

```
[RouterA-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[RouterA-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
```

配置密钥。

```
[RouterA-ipsec-policy-manual-map1-10] sa string-key outbound esp abcdefg
[RouterA-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
[RouterA-ipsec-policy-manual-map1-10] quit
```

配置串口的 IP 地址。

```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] ip address 2.2.2.1 255.255.255.0
```

在串口上应用 IPsec 安全策略组。

```
[RouterA-Serial2/1/1] ipsec policy map1
```

(2) 配置 Router B

配置一个访问控制列表，定义由子网 10.1.2.0/24 去子网 10.1.1.0/24 的数据流。

```
<RouterB> system-view
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```

配置到 HostA 的静态路由。

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 serial 2/1/2
```

创建名为 tran1 的 IPsec 安全提议。

```
[RouterB] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[RouterB-ipsec-transform-set-tran1] transform esp
```

选择算法。

```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

创建一条 IPsec 安全策略，协商方式为 manual。

```
[RouterB] ipsec policy use1 10 manual
```

引用访问控制列表。

```
[RouterB-ipsec-policy-manual-use1-10] security acl 3101
```

引用 IPsec 安全提议。

```
[RouterB-ipsec-policy-manual-use1-10] transform-set tran1
```

配置对端地址。

```
[RouterB-ipsec-policy-manual-use1-10] tunnel remote 2.2.2.1
```

配置本端地址。

```
[RouterB-ipsec-policy-manual-use1-10] tunnel local 2.2.3.1
```

配置 SPI。

```
[RouterB-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
```

```
[RouterB-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
```
配置密钥。
```
[RouterB-ipsec-policy-manual-use1-10] sa string-key outbound esp gfedcba
[RouterB-ipsec-policy-manual-use1-10] sa string-key inbound esp abcdefg
[RouterB-ipsec-policy-manual-use1-10] quit
```
配置串口的 IP 地址。
```
[RouterB] interface serial 2/1/2
[RouterB-Serial2/1/2] ip address 2.2.3.1 255.255.255.0
```
在串口上应用 IPsec 安全策略组。
```
[RouterB-Serial2/1/2] ipsec policy use1
```
4. 验证配置结果

以上配置完成后，Router A 和 Router B 之间的安全隧道就建立好了，子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的数据流将被加密传输。

1.7.2 采用IKE方式建立保护IPv4 报文的IPsec安全隧道

1. 组网需求

- 如图 1-7所示，在Router A和Router B之间建立一个安全隧道，对Host A所在的子网（10.1.1.0/24）与Host B所在的子网（10.1.2.0/24）之间的数据流进行安全保护。
- 安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。

2. 组网图

见图 1-7。

3. 配置步骤

(1) 配置 Router A

配置一个访问控制列表，定义由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。
```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[RouterA-acl-adv-3101] quit
```
配置到 Host B 的静态路由。
```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 serial 2/1/1
```
创建名为 tran1 的 IPsec 安全提议。
```
[RouterA] ipsec transform-set tran1
```
报文封装形式采用隧道模式。
```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
安全协议采用 ESP 协议。
```
[RouterA-ipsec-transform-set-tran1] transform esp
```
选择算法。
```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

配置 IKE 对等体。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] pre-shared-key abcde
[RouterA-ike-peer-peer] remote-address 2.2.3.1
[RouterA-ike-peer-peer] quit
```

创建一条 IPsec 安全策略，协商方式为 isakmp。

```
[RouterA] ipsec policy map1 10 isakmp
```

引用 IPsec 安全提议。

```
[RouterA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

引用访问控制列表。

```
[RouterA-ipsec-policy-isakmp-map1-10] security acl 3101
```

引用 IKE 对等体。

```
[RouterA-ipsec-policy-isakmp-map1-10] ike-peer peer
[RouterA-ipsec-policy-isakmp-map1-10] quit
```

配置串口的 IP 地址。

```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] ip address 2.2.2.1 255.255.255.0
```

在串口上应用 IPsec 安全策略组。

```
[RouterA-Serial2/1/1] ipsec policy map1
```

(2) 配置 Router B

配置一个访问控制列表，定义由子网 10.1.2.0/24 去子网 10.1.1.0/24 的数据流。

```
<RouterB> system-view
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```

配置到 Host A 的静态路由。

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 serial 2/1/2
```

创建名为 tran1 的 IPsec 安全提议。

```
[RouterB] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[RouterB-ipsec- transform-set -tran1] transform esp
```

选择算法。

```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

配置 IKE 对等体。

```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] pre-shared-key abcde
[RouterB-ike-peer-peer] remote-address 2.2.2.1
[RouterB-ike-peer-peer] quit
```

创建一条 IPsec 安全策略，协商方式为 isakmp。

```
[RouterB] ipsec policy use1 10 isakmp
```
引用访问控制列表。
```
[RouterB-ipsec-policy-isakmp-use1-10] security acl 3101
```
引用 IPsec 安全提议。
```
[RouterB-ipsec-policy-isakmp-use1-10] transform-set tran1
```
引用 IKE 对等体。
```
[RouterB-ipsec-policy-isakmp-use1-10] ike-peer peer
[RouterB-ipsec-policy-isakmp-use1-10] quit
```
配置串口的 IP 地址。
```
[RouterB] interface serial 2/1/2
[RouterB-Serial2/1/2] ip address 2.2.3.1 255.255.255.0
```
在串口上应用 IPsec 安全策略组。
```
[RouterB-Serial2/1/2] ipsec policy use1
```

4. 验证配置结果

以上配置完成后，Router A 和 Router B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 进行协商建立 SA。IKE 协商成功并创建了 SA 后，子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的数据流将被加密传输。

1.7.3 采用IKE方式建立保护IPv6 报文的IPsec安全隧道

1. 组网需求

- 如图 1-8所示，在Router A和Router B之间建立一个安全隧道，对Host A所在的子网（333::0/64）与Host B所在的子网（555::0/64）之间的数据流进行安全保护。
- 安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。

2. 组网图

图1-8 保护 IPv6 报文的 IPsec 隧道配置组网图

3. 配置步骤

(1) 配置 Router A

配置各接口的 IP 地址，具体略。

配置一个访问控制列表，定义由子网 333::0/64 去子网 555::0/64 的数据流。
```
<RouterA> system-view
[RouterA] acl ipv6 number 3101
[RouterA-acl-adv-3101] rule permit ipv6 source 333::0 64 destination 555::0 64
[RouterA-acl-adv-3101] quit
```
配置到 Host B 的静态路由。
```
[RouterA] ipv6 route-static 555::0 64 222::1
```
创建名为 tran1 的 IPsec 安全提议。
```
[RouterA] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[RouterA-ipsec-transform-set-tran1] transform esp
```

选择算法。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

配置 IKE 对等体。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] pre-share-key abcde
[RouterA-ike-peer-peer] remote-address ipv6 222::1
[RouterA-ike-peer-peer] quit
```

创建一条 IPsec 安全策略，协商方式为 isakmp。

```
[RouterA] ipsec policy map1 10 isakmp
```

引用 IPsec 安全提议。

```
[RouterA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

引用访问控制列表。

```
[RouterA-ipsec-policy-isakmp-map1-10] security acl ipv6 3101
```

引用 IKE 对等体。

```
[RouterA-ipsec-policy-isakmp-map1-10] ike-peer peer
[RouterA-ipsec-policy-isakmp-map1-10] quit
```

在接口 GigabitEthernet3/0/2 上应用 IPsec 安全策略组。

```
[RouterA] interface gigabitethernet 3/0/2
[RouterA-GigabitEthernet3/0/2] ipsec policy map1
```

(2)　配置 Router B

配置各接口的 IP 地址，具体略。

配置一个访问控制列表，定义由子网 555::0/64 去子网 333::0/64 的数据流。

```
<RouterB> system-view
[RouterB] acl ipv6 number 3101
[RouterB-acl-adv-3101] rule permit ipv6 source 555::/64 destination 333::/64
[RouterB-acl-adv-3101] quit
```

配置到 Host A 的静态路由。

```
[RouterB] ipv6 route-static 333::0 64 111::1
```

创建名为 tran1 的 IPsec 安全提议。

```
[RouterB] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[RouterB-ipsec-transform-set-tran1] transform esp
```

选择算法。

```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

```
[RouterB-ipsec-transform-set-tran1] quit
```
配置 IKE 对等体。
```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] pre-share-key abcde
[RouterB-ike-peer-peer] remote-address ipv6 111::1
[RouterB-ike-peer-peer] quit
```
创建一条 IPsec 安全策略，协商方式为 isakmp。
```
[RouterB] ipsec policy use1 10 isakmp
```
引用访问控制列表。
```
[RouterB-ipsec-policy-isakmp-use1-10] security acl ipv6 3101
```
引用 IPsec 安全提议。
```
[RouterB-ipsec-policy-isakmp-use1-10] transform-set tran1
```
引用 IKE 对等体。
```
[RouterB-ipsec-policy-isakmp-use1-10] ike-peer peer
[RouterB-ipsec-policy-isakmp-use1-10] quit
```
在接口 GigabitEthernet3/0/2 上应用 IPsec 安全策略组。
```
[RouterB] interface gigabitethernet 3/0/2
[RouterB-GigabitEthernet3/0/2] ipsec policy use1
```

4. 验证配置结果

以上配置完成后，当 Router A 和 Router B 之间有子网 333::0/64 与子网 555::0/64 之间的报文通过时，将触发 IKE 进行协商建立 SA。IKE 协商成功并创建了 SA 后，子网 333::0/64 与子网 555::0/64 之间的数据流将被加密传输。

1.7.4 使用IPsec虚拟隧道接口建立IPsec安全隧道

1. 组网需求

如图 1-9所示，某企业分支使用拨号方式获取动态IP地址接入Internet，企业总部使用固定的IP地址接入Internet。现有如下组网要求：

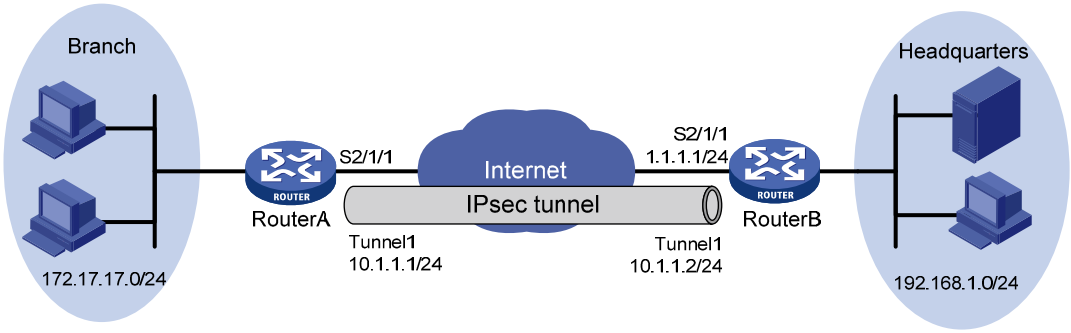
- 企业分支与企业总部之间的所有流量通过 IPsec 安全隧道进行传送；
- 当企业分支的私网 IP 地址段调整时，不需要改变企业总部网关的 IPsec 配置。

为实现如上组网需求，可采用如下配置思路实现：

- 在 Router A 和 Router B 之间使用 IPsec 虚拟隧道接口建立 IPsec 连接，将发送给对端私网的数据流路由到 IPsec 虚拟隧道接口上，由 IPsec 虚拟隧道接口上动态协商建立的 IPsec 安全隧道对分支子网（172.17.17.0/24）与总部子网（192.168.1.0/24）之间的所有数据流进行安全保护。

2. 组网图

图1-9 IPsec 虚拟隧道接口配置组网图



3. 配置步骤

(1) 配置 Router A

配置本端安全网关的名字为 routera。

```
<RouterA> system-view
[RouterA] ike local-name routera
```

配置 IKE 对等体 atob。由于隧道本端的 IP 地址为动态获取，因此需要选择协商模式为 **aggressive**。

```
[RouterA] ike peer atob
[RouterA-ike-peer-atob] exchange-mode aggressive
[RouterA-ike-peer-atob] pre-shared-key simple aabb
[RouterA-ike-peer-atob] id-type name
[RouterA-ike-peer-atob] remote-name routerb
[RouterA-ike-peer-atob] quit
```

创建名字为 method1 的 IPsec 安全提议，采用缺省的参数设置：安全协议为 ESP；加密算法为 DES；认证算法为 MD5。

```
[RouterA] ipsec transform-set method1
[RouterA-ipsec-transform-set-method1] transform esp
[RouterA-ipsec-transform-set-method1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-method1] esp authentication-algorithm md5
[RouterA-ipsec-transform-set-method1] quit
```

创建名字为 atob 的 IPsec 安全框架，用于保护 Router A 和 Router B 之间的数据流。

```
[RouterA] ipsec profile atob
```

引用 IKE 对等体 atob。

```
[RouterA-ipsec-profile-atob] ike-peer atob
```

引用 IPsec 安全提议 method1。

```
[RouterA-ipsec-profile-atob] transform-set method1
[RouterA-ipsec-profile-atob] quit
```

创建一个 IPsec 虚拟隧道接口 Tunnel1，此接口将用于保护 Router A 和 Router B 之间的数据流。

```
[RouterA] interface tunnel 1
```

配置 Tunnel1 的 IPv4 地址为 10.1.1.1/24。

```
[RouterA-Tunnel1] ip address 10.1.1.1 24
```

配置 Tunnel1 的隧道模式为 IPsec over IPv4。

```
[RouterA-Tunnel1] tunnel-protocol ipsec ipv4
```

配置 Tunnel1 的源接口为 Serial2/1/1。

```
[RouterA–Tunnel1] source serial 2/1/1
```

配置 Tunnel1 的目的地址为 1.1.1.1（对端安全网关的隧道接口的源地址）。

```
[RouterA–Tunnel1] destination 1.1.1.1
```

在 Tunnel1 上应用 IPsec 安全框架 atob。

```
[RouterA–Tunnel1] ipsec profile atob
[RouterA–Tunnel1] quit
```

配置 Router A 到 Router B 的静态路由。

```
[RouterA] ip route-static 192.168.1.0 255.255.255.0 tunnel 1
```

(2) 配置 Router B

配置接口 Serial2/1/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface serial 2/1/1
[RouterB-Serial2/1/1] ip address 1.1.1.1 24
[RouterB-Serial2/1/1] quit
```

配置本端安全网关的名字为 routerb。

```
[RouterB] ike local-name routerb
```

配置 IKE 对等体 btoa。由于隧道对端的 IP 地址为动态获取，因此需要选择协商模式为 **aggressive**。

```
[RouterB] ike peer btoa
[RouterB-ike-peer-btoa] exchange-mode aggressive
[RouterB-ike-peer-btoa] pre-shared-key simple aabb
[RouterB-ike-peer-btoa] id-type name
[RouterB-ike-peer-btoa] remote-name routera
[RouterB-ike-peer-btoa] quit
```

创建名字为 method1 的 IPsec 安全提议，采用缺省的参数设置：安全协议为 ESP；加密算法为 DES；认证算法为 MD5。

```
[RouterB] ipsec transform-set method1
[RouterB-ipsec-transform-set-method1] transform esp
[RouterB-ipsec-transform-set-method1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-method1] esp authentication-algorithm md5
[RouterB-ipsec-transform-set-method1] quit
```

创建名字为 btoa 的 IPsec 安全框架，用于保护 Router B 和 Router A 之间的数据流。

```
[RouterB] ipsec profile btoa
```

引用 IKE 对等体 btoa。

```
[RouterB-ipsec-profile-btoa] ike-peer btoa
```

引用 IPsec 安全提议 method1。

```
[RouterB-ipsec-profile-btoa] transform-set method1
[RouterB-ipsec-profile-btoa] quit
```

创建一个 IPsec 虚拟隧道接口 Tunnel1，此接口将用于保护 Router B 和 Router A 之间的数据流。由于对端的公网地址未知，因此隧道接口下不需要配置目的地址。

```
[RouterB] interface tunnel 1
```

配置 Tunnel1 的 IPv4 地址为 10.1.1.2/24。

```
[RouterB–Tunnel1] ip address 10.1.1.2 24
```

配置 Tunnel1 的隧道模式为 IPsec over IPv4。

```
[RouterB-Tunnel1] tunnel-protocol ipsec ipv4
```
配置 Tunnel1 的源接口为 Serial2/1/1。
```
[RouterB-Tunnel1] source serial 2/1/1
```
在 Tunnel1 上应用 IPsec 安全框架 btoa。
```
[RouterB-Tunnel1] ipsec profile btoa
[RouterB-Tunnel1] quit
```
配置 Router B 到 Router A 的静态路由。
```
[RouterB] ip route-static 172.17.17.0 255.255.255.0 tunnel 1
```
4. 验证配置结果

以上配置完成之后，当 Router A 的接口 Serial2/1/1 完成自动拨号后，Router A 会自动发起与 Router B 之间的 IKE 协商。当 IKE 协商完成之后，Router A 和 Router B 上的 IPsec 虚拟隧道接口链路状态都将 up，即可以满足上述组网需求，对总部和分支的数据流进行安全保护。

可以通过如下显示信息看到 Router B 上的 IPsec 虚拟隧道接口链路状态已经 up。
```
[RouterB] display interface tunnel 1 brief
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
Tun1                 UP        UP             TUNNEL           10.1.1.2
```
可以通过如下显示信息看到，RouterB 作为响应方已与 Router A 协商生成了两个阶段的 SA。
```
[RouterB] display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ------------------------------------------------------------
        1          1.1.1.2         RD            1     IPSEC
        2          1.1.1.2         RD            2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO—TIMEOUT RK-REKEY
```
可以通过如下显示信息查看协商生成的 IPsec SA。
```
[RouterB] display ipsec sa
==============================
Interface: Tunnel1
    path MTU: 1443
==============================

  ----------------------------
  IPsec policy name: "btoa"
  sequence number: 1
  acl version: ACL4
  mode: tunnel
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.1.1.1
        remote address: 1.1.1.2
    flow :
        sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: IP
```

```
      dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0x75b6ef44 (1974923076)
      transform: ESP-ENCRYPT-DES ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 15
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3503
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 0x8cf16c54(2364632148)
      transform: ESP-ENCRYPT-DES ESP-AUTH-MD5
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3503
      anti-replay detection: Enabled
        anti-replay window size(counter based) : 32
      udp encapsulation used for nat traversal: N
```

在 Router B 上可以 ping 通 Router A 连接的分支私网地址。

```
[RouterB] ping -a 192.168.1.1 172.17.17.1
  PING 172.17.17.1: 56  data bytes, press CTRL_C to break
    Reply from 172.17.17.1: bytes=56 Sequence=1 ttl=255 time=15 ms
    Reply from 172.17.17.1: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 172.17.17.1: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 172.17.17.1: bytes=56 Sequence=4 ttl=255 time=5 ms
    Reply from 172.17.17.1: bytes=56 Sequence=5 ttl=255 time=4 ms

  --- 172.17.17.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/8/15 ms
```

同样，在 Router A 上可以通过以上显示命令来查看配置的生效情况，由于其上的显示信息形式与 Router B 的类似，此处不再详述。

1.7.5 配置IPsec保护RIPng报文

说明

IPsec 保护其它 IPv6 路由协议（OSPFv3、IPv6 BGP）的具体配置与本例类似，具体内容请参考“三层技术-IP 路由配置指导”中的“OSPFv3”和“IPv6 BGP”。

1. 组网需求

如图 1-10所示，Router A、Router B和Router C相连，并通过RIPng来学习网络中的IPv6 路由信息。具体组网要求如下：

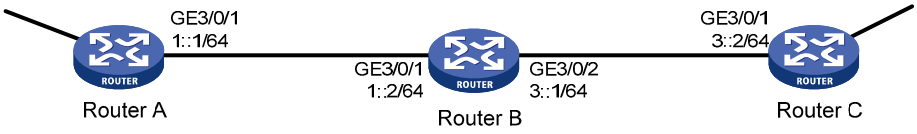
- 在各设备之间建立 IPsec 安全隧道，对它们收发的 RIPng 报文进行安全保护；
- 安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。

配置思路：

- 配置 RIPng 的基本功能
- 配置手工方式的 IPsec 安全策略
- 在 RIPng 进程下或接口上应用 IPsec 安全策略（进程下配置的 IPsec 安全策略对该进程的所有报文有效，接口下的 IPsec 安全策略只对接口下的报文有效）

2. 组网图

图1-10 配置 IPsec 保护 RIPng 报文组网图



3. 配置步骤


说明

RIPng 配置的详细介绍请参考“三层技术-IP 路由配置指导”中的“RIPng”。

(1) 配置 Router A

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<RouterA> system-view
[RouterA] ripng 1
[RouterA-ripng-1] quit
[RouterA] interface gigabiethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ripng 1 enable
[RouterA-GigabitEthernet3/0/1] quit
```

- 配置 IPsec 安全策略

创建并配置名为 tran1 的 IPsec 安全提议（报文封装形式采用传输模式，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96）。

```
[RouterA] ipsec transform-set tran1
[RouterA-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterA-ipsec-transform-set-tran1] transform esp
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建并配置名为 policy001 的 IPsec 安全策略（协商方式为 manual，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为 abcdefg）。

```
[RouterA] ipsec policy policy001 10 manual
[RouterA-ipsec-policy-manual-policy001-10] transform-set tran1
[RouterA-ipsec-policy-manual-policy001-10] sa spi outbound esp 123456
[RouterA-ipsec-policy-manual-policy001-10] sa spi inbound esp 123456
[RouterA-ipsec-policy-manual-policy001-10] sa string-key outbound esp abcdefg
[RouterA-ipsec-policy-manual-policy001-10] sa string-key inbound esp abcdefg
[RouterA-ipsec-policy-manual-policy001-10] quit
```

- 在 RIPng 进程上应用 IPsec 安全策略

```
[RouterA] ripng 1
[RouterA-ripng-1] enable ipsec-policy policy001
[RouterA-ripng-1] quit
```

(2) 配置 Router B

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<RouterB> system-view
[RouterB] ripng 1
[RouterB-ripng-1] quit
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ripng 1 enable
[RouterB-GigabitEthernet3/0/1] quit
[RouterB] interface gigabitethernet 3/0/2
[RouterB-GigabitEthernet3/0/2] ripng 1 enable
[RouterB-GigabitEthernet3/0/2] quit
```

- 配置 IPsec 安全策略

创建并配置名为 tran1 的 IPsec 安全提议（报文封装形式采用传输模式，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96）。

```
[RouterB] ipsec transform-set tran1
[RouterB-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterB-ipsec-transform-set-tran1] transform esp
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

创建并配置名为 policy001 的 IPsec 安全策略（协商方式为 manual，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为 abcdefg）。

```
[RouterB] ipsec policy policy001 10 manual
[RouterB-ipsec-policy-manual-policy001-10] transform-set tran1
[RouterB-ipsec-policy-manual-policy001-10] sa spi outbound esp 123456
[RouterB-ipsec-policy-manual-policy001-10] sa spi inbound esp 123456
[RouterB-ipsec-policy-manual-policy001-10] sa string-key outbound esp abcdefg
[RouterB-ipsec-policy-manual-policy001-10] sa string-key inbound esp abcdefg
[RouterB-ipsec-policy-manual-policy001-10] quit
```

- 在 RIPng 进程上应用 IPsec 安全策略

```
[RouterB] ripng 1
[RouterB-ripng-1] enable ipsec-policy policy001
```

```
[RouterB-ripng-1] quit
```

(3) 配置 Router C

- 配置各接口的 IPv6 地址（略）
- 配置 RIPng 的基本功能

```
<RouterC> system-view
[RouterC] ripng 1
[RouterC-ripng-1] quit
[RouterC] interface gigabitethernet 3/0/1
[RouterC-GigabitEthernet3/0/1] ripng 1 enable
[RouterC-GigabitEthernet3/0/1] quit
```

- 配置 IPsec 安全策略

创建并配置名为 tran1 的 IPsec 安全提议（报文封装形式采用传输模式，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96）。

```
[RouterC] ipsec transform-set tran1
[RouterC-ipsec-transform-set-tran1] encapsulation-mode transport
[RouterC-ipsec-transform-set-tran1] transform esp
[RouterC-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterC-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterC-ipsec-transform-set-tran1] quit
```

创建并配置名为 policy001 的 IPsec 安全策略（协商方式为 manual，出入方向 SA 的 SPI 均为 123456，出入方向 SA 的密钥均为 abcdefg）。

```
[RouterC] ipsec policy policy001 10 manual
[RouterC-ipsec-policy-manual-policy001-10] transform-set tran1
[RouterC-ipsec-policy-manual-policy001-10] sa spi outbound esp 123456
[RouterC-ipsec-policy-manual-policy001-10] sa spi inbound esp 123456
[RouterC-ipsec-policy-manual-policy001-10] sa string-key outbound esp abcdefg
[RouterC-ipsec-policy-manual-policy001-10] sa string-key inbound esp abcdefg
[RouterC-ipsec-policy-manual-policy001-10] quit
```

- 在 RIPng 进程上应用 IPsec 安全策略

```
[RouterC] ripng 1
[RouterC-ripng-1] enable ipsec-policy policy001
[RouterC-ripng-1] quit
```

4. 验证配置结果

以上配置完成后，Router A、Router B 和 Router C 将通过 RIPng 协议学习到网络中的 IPv6 路由信息，且分别产生用于保护 RIPng 报文的 SA。

可以通过如下 **display** 命令查看 Router A 上 RIPng 的配置信息。如下显示信息表示 RIPng 进程 1 上已成功应用了 IPsec 策略，且携带了有效的 SPI 值。

```
<RouterA> display ripng 1
  Public vpn-instance name :
    RIPng process : 1
       Preference : 100
       Checkzero : Enabled
       Default Cost : 0
       Maximum number of balanced paths : 8
       Update time   :   30 sec(s)  Timeout time         :  180 sec(s)
```

```
      Suppress time :  120 sec(s)  Garbage-Collect time :  120 sec(s)
      Number of periodic updates sent : 186
      Number of trigger updates sent : 1
      IPsec policy name: policy001, SPI: 123456
```

可以通过如下 **display** 命令查看 Router A 上生成的 SA。

```
<RouterA> display ipsec sa
==============================
Protocol: RIPng
==============================

  ----------------------------
  IPsec policy name: "policy001"
  sequence number: 10
  acl version: None
  mode: manual
  ----------------------------
    PFS: N, DH group: none
    tunnel:
    flow:

    [inbound ESP SAs]
      spi: 0x3039(123456)
      transform: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      in use setting: Transport
      connection id: 13
      No duration limit for this sa

    [outbound ESP SAs]
      spi: 0x3039(123456)
      transform: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      in use setting: Transport
      connection id: 14
      No duration limit for this sa
```

Router B 和 Router C 上也会生成相应的 SA 来保护 RIPng 报文，查看方式与 Router A 同，此处略。

1.7.6 IPsec反向路由注入功能典型配置举例

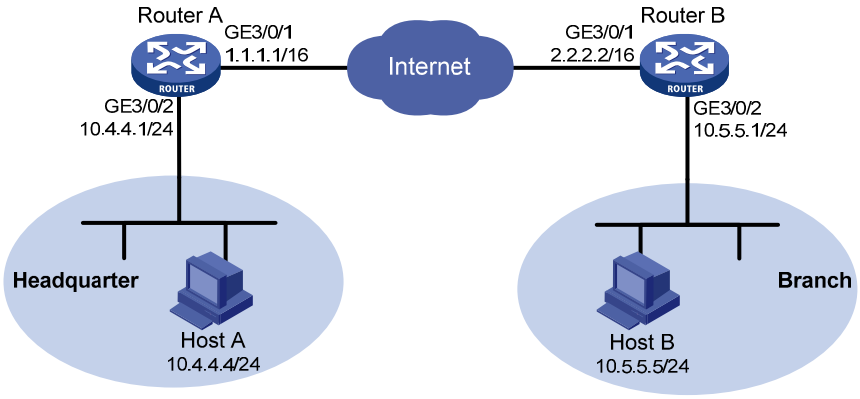
1. 组网需求

企业分支通过 IPsec VPN 接入企业总部，有如下具体需求：

- 在总部网关 Router A 和分支网关 Router B 之间建立一个安全隧道，对总部网络 10.4.4.0/24 与分支网络 10.5.5.0/24 之间的数据流进行安全保护。
- 使用 IKE 自动协商方式建立 SA，安全协议采用 ESP 协议，加密算法采用 DES，认证算法采用 SHA1-HMAC-96。
- 在 Router A 上开启 IPsec 反向路由注入功能，实现总部到分支的静态路由随 IPsec SA 的建立而动态生成，并指定下一跳地址为 1.1.1.2。

2. 组网图

图1-11 IPsec 反向路由注入功能配置组网图



3. 配置步骤

请按照图中所示配置各接口的 IPv4 地址，并保证 Router A 和 Router B 之间路由可达（略）。

(1) 配置 Router A

配置访问控制列表 3101，定义由子网 10.4.4.0/24 去子网 10.5.5.0/24 的数据流。

```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit ip source 10.4.4.0 0.0.0.255 destination 10.5.5 0
0.0.0.255
[RouterA-acl-adv-3101] quit
```

创建名为 tran1 的 IPsec 安全提议。

```
[RouterA] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

配置采用 ESP 安全协议。

```
[RouterA-ipsec-transform-set-tran1] transform esp
```

配置加密算法为 DES，认证算法为 SHA1-HMAC-96。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

配置 IKE 对等体。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] pre-shared-key abcde
[RouterA-ike-peer-peer] remote-address 2.2.2.2
[RouterA-ike-peer-peer] quit
```

创建 IPsec 安全策略 map1，其协商方式为 isakmp。

```
[RouterA] ipsec policy map1 10 isakmp
```

引用 IPsec 安全提议。

```
[RouterA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

引用访问控制列表。

```
[RouterA-ipsec-policy-isakmp-map1-10] security acl 3101
```
引用 IKE 对等体。
```
[RouterA-ipsec-policy-isakmp-map1-10] ike-peer peer
```
开启动态方式的 IPsec 反向路由注入功能，并指定下一跳地址为 1.1.1.2。
```
[RouterA-ipsec-policy-isakmp-map1-10] reverse-route remote-peer 1.1.1.2
[RouterA-ipsec-policy-isakmp-map1-10] quit
```
在接口 GigabitEthernet3/0/1 上应用 IPsec 安全策略组 map1。
```
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ipsec policy map1
[RouterA-GigabitEthernet3/0/1] quit
```
(2) 配置 Router B

配置一访问控制列表 3101，定义由子网 10.5.5.0/24 去子网 10.4.4.0/24 的数据流。
```
<RouterB> system-view
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule permit ip source 10.5.5.0 0.0.0.255 destination 10.4.4.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```
配置到 Host A 所在网段的静态路由。
```
[RouterB] ip route-static 10.4.4.0 255.255.255.0 1.1.1.1
```
创建名为 tran1 的 IPsec 安全提议。
```
[RouterB] ipsec transform-set tran1
```
报文封装形式采用隧道模式。
```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
配置采用 ESP 安全协议。
```
[RouterB-ipsec-transform-set-tran1] transform esp
```
配置加密算法为 DES，认证算法为 SHA1-HMAC-96。
```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```
配置 IKE 对等体。
```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] pre-shared-key abcde
[RouterB-ike-peer-peer] remote-address 1.1.1.1
[RouterB-ike-peer-peer] quit
```
创建 IPsec 安全策略 use1，其协商方式为 isakmp。
```
[RouterB] ipsec policy use1 10 isakmp
```
引用访问控制列表。
```
[RouterB-ipsec-policy-isakmp-use1-10] security acl 3101
```
引用 IPsec 安全提议。
```
[RouterB-ipsec-policy-isakmp-use1-10] transform-set tran1
```
引用 IKE 对等体。
```
[RouterB-ipsec-policy-isakmp-use1-10] ike-peer peer
[RouterB-ipsec-policy-isakmp-use1-10] quit
```
在接口 GigabitEthernet3/0/1 上应用 IPsec 安全策略组 use1。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ipsec policy use1
```

4. 验证配置结果

以上配置完成后，Router A 和 Router B 之间如果有子网 10.5.5.0/24 与子网 10.4.4.0/24 之间的报文通过，将触发 IKE 进行协商建立 SA。

IKE 协商成功并创建了 IPsec SA 后，子网 10.5.5.0/24 与子网 10.4.4.0/24 之间的数据流将被加密传输，Router A 上同时生成静态路由表项，目的地址为分支网络地址 10.5.5.0/24，下一跳地址为 1.1.1.2，可通过如下显示信息查看。

```
[RouterA] display ip routing-table
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

1.1.0.0/16          Direct  0    0            1.1.1.1         GE3/0/1
1.1.1.1/32          Direct  0    0            127.0.0.1       InLoop0
2.2.2.0/24          Static  60   0            1.1.1.2         GE3/0/1
10.4.4.0/24         Direct  0    0            10.4.4.1        GE3/0/2
10.4.4.4/32         Direct  0    0            127.0.0.1       InLoop0
10.5.5.0/24         Static  60   0            1.1.1.2         GE3/0/1
127.0.0.0/8         Direct  0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0            127.0.0.1       InLoop0
```

若删除对应的 IPsec SA，则该静态路由也会被同时删除。

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

在实施 IPsec 的过程中，可以使用 IKE（Internet Key Exchange，互联网密钥交换）协议来建立 SA，该协议建立在由 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）定义的框架上。IKE 为 IPsec 提供了自动协商交换密钥、建立 SA 的服务，能够简化 IPsec 的使用和管理，大大简化 IPsec 的配置和维护工作。

IKE 不是在网络上直接传输密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥，并且即使第三方截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

2.1.1 IKE的安全机制

IKE 具有一套自保护机制，可以在不安全的网络上安全地认证身份、分发密钥、建立 IPsec SA。

1. 数据认证

数据认证有如下两方面的概念：

- 身份认证：身份认证确认通信双方的身份。支持两种认证方法：预共享密钥（pre-shared-key）认证和基于 PKI 的数字签名（rsa-signature）认证。
- 身份保护：身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

2. DH

DH（Diffie-Hellman，交换及密钥分发）算法是一种公共密钥算法。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，也不足以计算出真正的密钥。所以，DH 交换技术可以保证双方能够安全地获得公有信息。

3. PFS

PFS（Perfect Forward Secrecy，完善的前向安全性）特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。对于 IPsec，是通过在 IKE 阶段 2 协商中增加一次密钥交换来实现的。PFS 特性是由 DH 算法保障的。

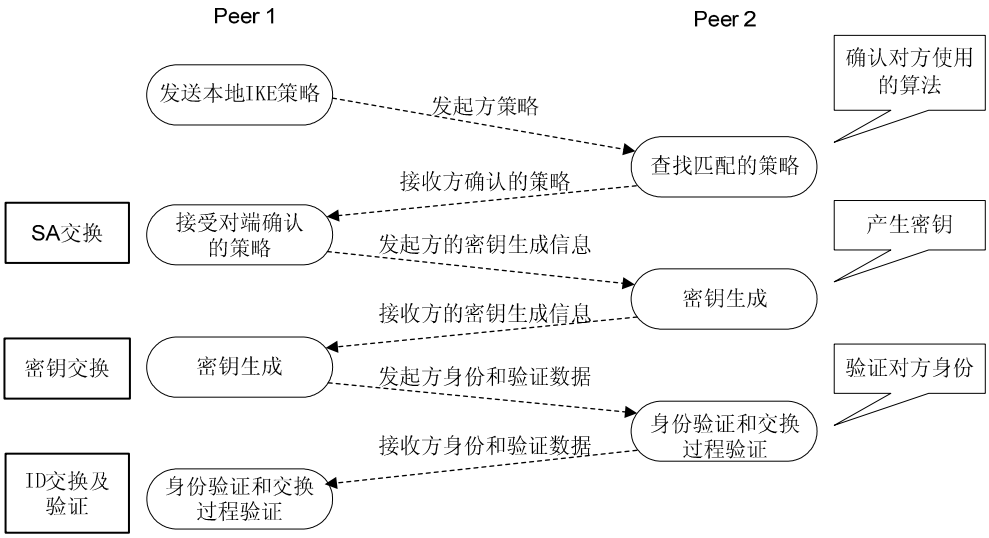
2.1.2 IKE的交换过程

IKE 使用了两个阶段为 IPsec 进行密钥协商并建立 SA：

(1) 第一阶段，通信各方彼此间建立了一个已通过身份认证和安全保护的通道，即建立一个ISAKMP SA。第一阶段有主模式（Main Mode）和野蛮模式（Aggressive Mode）两种 IKE 交换方法。

(2) 第二阶段，用在第一阶段建立的安全隧道为 IPsec 协商安全服务，即为 IPsec 协商具体的 SA，建立用于最终的 IP 数据安全传输的 IPsec SA。

图2-1 主模式交换过程



如图 2-1所示，第一阶段主模式的IKE协商过程中包含三对消息：

- 第一对叫 SA 交换，是协商确认有关安全策略的过程；
- 第二对消息叫密钥交换，交换 Diffie-Hellman 公共值和辅助数据（如：随机数），密钥材料在这个阶段产生；
- 最后一对消息是 ID 信息和认证数据交换，进行身份认证和对整个第一阶段交换内容的认证。

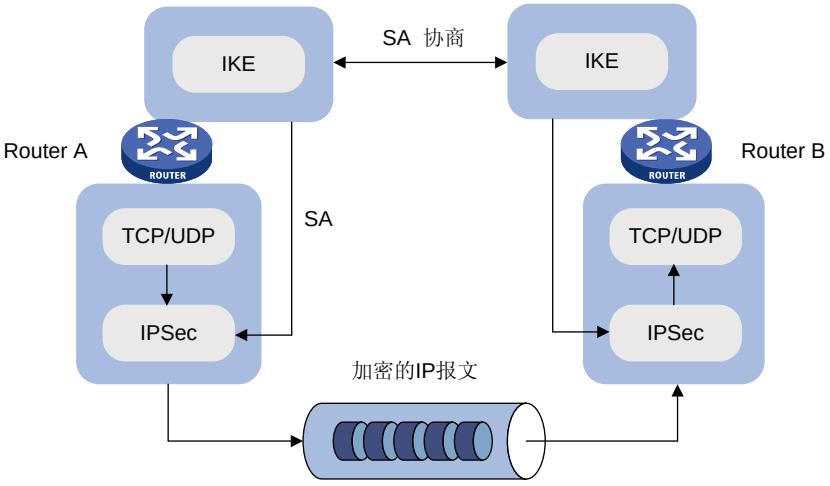
野蛮模式交换与主模式交换的主要差别在于，野蛮模式不提供身份保护，只交换 3 条消息。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度；在对身份保护要求较高的场合，则应该使用主模式。

2.1.3 IKE在IPsec中的作用

- 因为有了 IKE，IPsec 很多参数（如：密钥）都可以自动建立，降低了手工配置的复杂度。
- IKE 协议中的 DH 交换过程，每次的计算和产生的结果都是不相关的。每次 SA 的建立都运行 DH 交换过程，保证了每个 SA 所使用的密钥互不相关。
- IPsec 使用 AH 或 ESP 报文头中的序列号实现防重放。此序列号是一个 32 比特的值，此数溢出后，为实现防重放，SA 需要重新建立，这个过程需要 IKE 协议的配合。
- 对安全通信的各方身份的认证和管理，将影响到 IPsec 的部署。IPsec 的大规模使用，必须有 CA（Certificate Authority，证书颁发机构）或其他集中管理身份数据的机构的参与。
- IKE 提供端与端之间动态认证。

2.1.4 IPsec与IKE的关系

图2-2 IPsec 与 IKE 的关系图



从图 2-2中我们可以看出IKE和IPsec的关系：

- IKE 是 UDP 之上的一个应用层协议，是 IPsec 的信令协议；
- IKE 为 IPsec 协商建立 SA，并把建立的参数及生成的密钥交给 IPsec；
- IPsec 使用 IKE 建立的 SA 对 IP 报文加密或认证处理。

2.1.5 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

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。

- 确定 IKE 交换过程中算法的强度，即确定安全保护的强度（包括身份认证方法、加密算法、认证算法、DH 组）：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”。

表2-1 IKE 配置任务简介

配置任务	说明	详细配置
配置本端安全网关的名字	可选	2.3

配置任务	说明	详细配置
配置IKE安全提议	可选 若IKE对等体中需要指定IKE安全提议，则必配	2.4
配置IKE对等体	必选	2.5
配置Keepalive定时器	可选	2.6
配置NAT Keepalive定时器	可选	2.7
配置对等体存活检测	可选	2.8
配置取消对next payload域的检查	可选	2.9

2.3 配置本端安全网关的名字

当 IKE 协商的发起端使用 FQDN（Fully Qualified Domain Name，完全合格域名）或者 User FQDN 类型的安全网关名字进行协商时（即配置了 **id-type name** 或 **id-type user-fqdn**），本端需要配置本端安全网关的名字，该名字既可以在系统视图下进行配置，也可以在 IKE 对等体视图下配置，若两个视图下都配置了本端安全网关的名字，则采用 IKE 对等体视图下的配置。

表2-2 配置本端安全网关名字

操作	命令	说明
进入系统视图	**system-view**	-
配置本端安全网关的名字	**ike local-name** *name*	可选 缺省情况下，使用设备名作为本端安全网关的名字

2.4 配置IKE安全提议

IKE 安全提议定义了一套属性数据来描述 IKE 协商怎样进行安全通信。用户可以创建多条不同优先级的 IKE 提议，优先级由 IKE 提议的序号表示，数值越小，优先级越高。

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安全提议发送给对端，由对端进行匹配，协商响应方则从自己优先级最高（序号最小）的 IKE 提议开始，按照优先级顺序与对端发送的安全提议进行匹配，直到找到一个匹配的安全提议来使用。匹配的 IKE 提议将被用来建立安全隧道。

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

缺省情况下，系统提供一条缺省的 IKE 提议。此缺省的 IKE 提议具有最低的优先级，具有缺省的加密算法、认证方法、认证算法、DH 组标识和 ISAKMP SA 存活时间。

IPsec 流量超时时，非 FIPS 模式下只进行 IPsec SA 重协商，FIPS 模式下同时进行 IPsec SA 与和它对应的 IKE SA 重协商。

表2-3 配置 IKE 安全提议

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*	必选
指定一个供IKE提议使用的加密算法	**encryption-algorithm** { **3des-cbc** | **aes-cbc** [*key-length*] | **des-cbc** }	可选 缺省情况下： • 在 FIPS 模式下，设备不支持 DES-CBC 和 3DES-CBC，IKE 提议使用 CBC 模式的 128-bit AES-CBC 加密算法。 • 在非 FIPS 模式下，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** { **pre-share** | **rsa-signature** }	可选 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** }	可选 缺省情况下，IKE提议使用SHA1认证算法 在FIPS模式下不支持MD5算法
配置IKE阶段1密钥协商时所使用的DH密钥交换参数	**dh** { **group1** | **group2** | **group5** | **group14** }	可选 缺省情况下： • 在 FIPS 模式下，IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数为 group2，即 1024-bit 的 Diffie-Hellman 组。 • 在非 FIPS 模式下，IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数为 group1，即 768-bit 的 Diffie-Hellman 组。
指定一个IKE提议的ISAKMP SA存活时间	**sa duration** *seconds*	可选 缺省情况下，IKE提议的ISAKMP SA存活时间为86400秒

说明

如果存活时间超时，ISAKMP SA 将自动更新。因为 IKE 协商需要进行 DH 计算，在低端设备上需要经过较长的时间，为使 ISAKMP SA 的更新不影响安全通信，建议设置存活时间大于 10 分钟。

2.5 配置IKE对等体

在采用 IKE 方式配置安全策略时，需要指定 IKE 对等体。IKE 对等体中主要包括以下配置：

- 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。当对端的 IP 地址为动态获取，且采用预共享密钥认证方式时，建议将本端的 IKE 的协商模式配置为野蛮模式。
- 本端作为发起方时可以使用的 IKE 安全提议（可指定多个）。本端作为响应方时，将使用系统视图下已经配置的安全提议与对端发送的安全提议进行协商。
- 根据 IKE 提议使用的认证方法不同，选择所使用的预共享密钥或者 PKI 域。
- 本端在 IKE 第一阶段协商时，所使用的 ID 类型（IP 地址、FQDN 名、User FQDN 名）。在预共享密钥认证的主模式下，只能使用 IP 地址类型的 ID。
- 本端安全网关的名字或 IP 地址。一般情况下本端安全网关的 IP 地址不需要配置，只有要指定特殊的本端安全网关地址时（如指定 loopback 接口地址）才需要配置。
- 对端安全网关的名字或 IP 地址。若本端作为发起方，则需要配置对端安全网关名字或对端安全网关 IP 地址，它们用于发起方在协商过程中寻找对端。
- NAT 穿越功能。当 IPsec/IKE 隧道中存在 NAT 设备时，导致隧道一端为公网地址，另一端为私网地址，则必须在隧道两端均配置 NAT 穿越功能，保证隧道能够正常协商建立。
- 用于 IKE 对等体存活状态检测的 DPD 名称。

表2-4 配置 IKE 对等体

操作	命令	说明
进入系统视图	**system-view**	-
创建一个IKE对等体，并进入IKE-Peer视图	**ike peer** *peer-name*	必选
配置IKE第一阶段的协商模式	**exchange-mode** { **aggressive** | **main** }	可选 缺省情况下，IKE阶段的协商模式使用主模式 在FIPS模式下，设备不支持**aggressive**协商模式
配置IKE对等体引用的IKE安全提议	**proposal** *proposal-number&<1-6>*	可选 缺省情况下，IKE对等体未引用任何IKE安全提议，使用系统视图下已配置的IKE安全提议进行IKE协商
配置采用预共享密钥认证时，所使用的预共享密钥	**pre-shared-key** [**cipher** | **simple**] *key*	二者必选其一 根据IKE提议使用的认证方法选择其中一个配置 在FIPS模式下，密钥至少需要设置为8位，包含数字、大写字母、小写字母和特殊符号。
配置采用数字签名认证时，证书所属的PKI域	**certificate domain** *domain-name*	
选择IKE第一阶段的协商过程中使用ID的类型	**id-type** { **ip** | **name** | **user-fqdn** }	可选 缺省情况下，使用IP地址作为IKE协商过程中使用的ID

操作		命令	说明
配置本端及对端安全网关的名字	配置本端安全网关的名字	**local-name** *name*	可选 对端使用**remote-name**配置的网关名字应与IKE协商发起端所配置的本端安全网关名字保持一致 缺省情况下，未定义本端安全网关的名字，使用系统视图下本端安全网关的名字
	配置对端安全网关的名字	**remote-name** *name*	
配置本端及对端安全网关的IP地址	配置本端安全网关的IP地址	**local-address** [**ipv6**] *ip-address*	可选 对端使用**remote-address**配置的IP地址应与IKE协商发起端使用**local-address**命令所配的安全网关IP地址保持一致 缺省情况下，IKE协商时的本端安全网关IP地址使用应用IPsec安全策略的接口的主IP地址
	配置对端安全网关的IP地址	**remote-address** [**ipv6**] { *hostname* [**dynamic**] | *low-ip-address* [*high-ip-address*] }	
配置IKE/IPsec的NAT穿越功能		**nat traversal**	可选 在IPsec/IKE组建的VPN隧道中，若存在NAT安全网关设备，则必须配置IPsec/IKE的NAT穿越功能 缺省情况下，没有配置NAT穿越功能
配置本端及对端安全网关的子网类型	配置本端安全网关子网类型	**local** { **multi-subnet** | **single-subnet** }	可选 缺省情况下，为单子网类型。这两条命令仅在与NETSCREEN的设备互通时使用
	配置对端安全网关子网类型	**peer** { **multi-subnet** | **single-subnet** }	
为IKE对等体应用一个DPD		**dpd** *dpd-name*	可选 缺省情况下，IKE对等体没有应用DPD 关于DPD的配置请参见“2.8 配置对等体存活检测”

说明

修改 IKE 对等体配置之后，要执行命令 **reset ipsec sa**、**reset ike sa** 来清除原有的 IPsec SA 与 IKE SA，否则重新协商 SA 会失败。

2.6 配置Keepalive定时器

IKE 通过 Keepalive 报文维护 ISAKMP SA 的链路状态。一般在对端配置了等待 Keepalive 报文的超时时间后，必须在本端配置此 Keepalive 报文发送时间间隔。当对端在配置的超时时间内未收到此

Keepalive 报文时，如果该 ISAKMP SA 带有 TIMEOUT 标记，则删除该 ISAKMP SA 以及由其协商的 IPsec SA；否则，将其标记为 TIMEOUT。

表2-5 配置 Keepalive 定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置ISAKMP SA向对端发送Keepalive报文的时间间隔	**ike sa keepalive-timer interval** *seconds*	必选 缺省情况下，ISAKMP SA不向对端发送Keepalive报文
配置ISAKMP SA等待对端发送Keepalive报文的超时时间	**ike sa keepalive-timer timeout** *seconds*	必选 缺省情况下，ISAKMP SA不向对端发送Keepalive报文

说明

本端配置的 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 Keepalive 报文发送时间间隔的三倍。

2.7 配置NAT Keepalive定时器

在 IPsec/IKE 组建的 VPN 隧道中，若存在 NAT 安全网关设备，需配置 NAT 穿越功能来实现 NAT 穿越，但由于在 NAT 网关上的 NAT 映射会话有一定存活时间，因此一旦安全隧道建立后如果长时间没有报文穿越，NAT 会话表项会被删除，这样将导致在 NAT 网关外侧的隧道无法继续传输数据。为防止 NAT 表项老化，NAT 网关内网侧的 ISAKMP SA 会以一定的时间间隔向对端发送 NAT Keepalive 报文，以维持 NAT 会话的存活。

表2-6 配置 NAT Keepalive 定时器

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

2.8 配置对等体存活检测

DPD（Dead Peer Detection，对等体存活检测）用于 IKE 对等体存活状态检测。启动 DPD 功能后，当本端需要向对端发送 IPsec 报文时，若判断当前距离最后一次收到对端 IPsec 报文已经超过触发 DPD 的时间间隔（**interval-time** *interval-time*），则触发 DPD 查询，本端主动向对端发送 DPD 请求报文，对 IKE 对等体是否存活进行检测。如果本端在 DPD 报文的重传时间间隔（**time-out** *time-out*）

内未收到对端发送的 DPD 回应报文，则重传 DPD 请求，缺省重传两次之后，若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。

DPD 和 Keepalive 的区别：

- Keepalive 定期发送查询；
- DPD 只在要发送加密报文前并且长时间（触发 DPD 的时间间隔）未收到对端 IPsec 报文时发送查询。

表2-7 配置对等体存活检测

操作	命令	说明
进入系统视图	**system-view**	-
创建一个DPD，并进入DPD视图	**ike dpd** *dpd-name*	必选
配置触发DPD的时间间隔	**interval-time** *interval-time*	可选 缺省情况下，触发DPD的时间间隔为10秒
配置DPD报文的重传时间间隔	**time-out** *time-out*	可选 缺省情况下，DPD报文的重传时间间隔为5秒

2.9 配置取消对next payload域的检查

next payload 域是在 IKE 协商报文（由几个 payload 组装而成）的最后一个 payload 的通用头中的一个域。按协议规定如果当前载荷处于消息的最后，该域必须为 0，但某些公司的设备会将该域赋其它值，为增强设备的互通性，可以通过下面的配置取消 IKE 协商过程对该域的检查。

表2-8 配置取消对 next payload 域的检查

操作	命令	说明
进入系统视图	**system-view**	-
配置在IKE协商过程中取消对next payload域的检查	**ike next-payload check disabled**	必选 缺省情况下，在IPsec协商过程中对next payload域进行检查

2.10 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 建立的安全隧道。

表2-9 IKE 显示和维护

操作	命令
显示DPD配置的参数	**display ike dpd** [*dpd-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IKE对等体配置的参数	**display ike peer** [*peer-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示当前IKE SA的信息	**display ike sa** [**verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示每个IKE提议配置的参数	**display ike proposal** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除IKE建立的安全隧道	**reset ike sa** [*connection-id*]

2.11 IKE典型配置举例

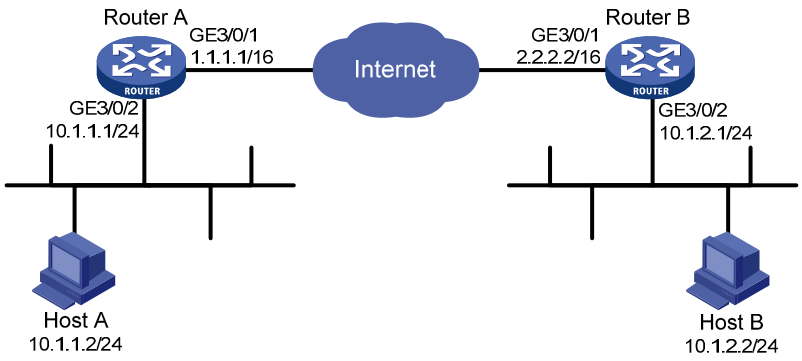
2.11.1 IKE主模式及预共享密钥认证典型配置举例

1. 组网需求

- 在 Router A 和 Router B 之间建立一个安全隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。
- 在 Router A 上配置一条 IKE 提议，其提议号为 10，使用的认证算法为 MD5。Router B 使用缺省的 IKE 提议。
- 使用预共享密钥的认证方法。

2. 组网图

图2-3 IKE 主模式及预共享密钥认证典型组网图



3. 配置步骤

说明

请保证 Router A 与 Router B 之间路由可达。

(1) 配置安全网关 Router A

配置 ACL 3101，定义由子网 10.1.1.0/24 去子网 10.1.2.0/24 的数据流。

```
<RouterA> system-view
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0
0.0.0.255
[RouterA-acl-adv-3101] quit
```

配置 IPsec 安全提议 tran1。

```
[RouterA] ipsec transform-set tran1
```

报文封装形式采用隧道模式。

```
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

安全协议采用 ESP 协议。

```
[RouterA-ipsec-transform-set-tran1] transform esp
```

选择 ESP 协议采用的加密算法和认证算法。

```
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```

创建 IKE 对等体。

```
[RouterA] ike peer peer
```

配置预共享密钥。

```
[RouterA-ike-peer-peer] pre-shared-key abcde
```

配置对端安全网关的 IP 地址。

```
[RouterA-ike-peer-peer] remote-address 2.2.2.2
[RouterA-ike-peer-peer] quit
```

创建一条 IKE 提议 10。

```
[RouterA] ike proposal 10
```

指定 IKE 提议使用的认证算法为 MD5。

```
[RouterA-ike-proposal-10] authentication-algorithm md5
```

使用预共享密钥认证方法。

```
[RouterA-ike-proposal-10] authentication-method pre-share
```

配置 ISAKMP SA 的存活时间为 5000 秒。

```
[RouterA-ike-proposal-10] sa duration 5000
[RouterA-ike-proposal-10] quit
```

创建一条 IPsec 安全策略，协商方式为 isakmp。

```
[RouterA] ipsec policy map1 10 isakmp
```

引用安全提议。

```
[RouterA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

引用访问控制列表。

```
[RouterA-ipsec-policy-isakmp-map1-10] security acl 3101
```
引用 IKE 对等体。
```
[RouterA-ipsec-policy-isakmp-map1-10] ike-peer peer
[RouterA-ipsec-policy-isakmp-map1-10] quit
```
配置接口 GigabitEthernet3/0/2 的 IP 地址。
```
[RouterA] interface gigabitethernet 3/0/2
[RouterA-GigabitEthernet3/0/2] ip address 10.1.1.1 255.255.255.0
[RouterA-GigabitEthernet3/0/2] quit
```
配置接口 GigabitEthernet3/0/1 的 IP 地址。
```
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ip address 1.1.1.1 255.255.255.0
```
在接口 GigabitEthernet3/0/1 上应用 IPsec 安全策略组。
```
[RouterA-GigabitEthernet3/0/1] ipsec policy map1
```
配置到 Host B 所在子网的静态路由。
```
[RouterA] ip route-static 10.1.2.0 255.255.255.0 2.2.2.2
```
(2)　配置安全网关 Router B

配置 ACL 3101，定义由子网 10.1.2.0/24 去子网 10.1.1.0/24 的数据流。
```
<RouterB> system-view
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```
创建 IPsec 安全提议 tran1。
```
[RouterB] ipsec transform-set tran1
```
报文封装形式采用隧道模式。
```
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
```
安全协议采用 ESP 协议。
```
[RouterB-ipsec-transform-set-tran1] transform esp
```
选择 ESP 协议采用的加密算法和认证算法。
```
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```
配置 IKE 对等体。
```
[RouterB] ike peer peer
```
配置预共享密钥。
```
[RouterB-ike-peer-peer] pre-shared-key abcde
```
配置对端安全网关的 IP 地址。
```
[RouterB-ike-peer-peer] remote-address 1.1.1.1
[RouterB-ike-peer-peer] quit
```
创建一条 IPsec 安全策略，协商方式为 isakmp。
```
[RouterB] ipsec policy use1 10 isakmp
```
引用访问控制列表。
```
[RouterB-ipsec-policy-isakmp-use1-10] security acl 3101
```

引用 IPsec 安全提议。

```
[RouterB-ipsec-policy-isakmp-use1-10] transform-set tran1
```

引用 IKE 对等体。

```
[RouterB-ipsec-policy-isakmp-use1-10] ike-peer peer
[RouterB-ipsec-policy-isakmp-use1-10] quit
```

配置接口 GigabitEthernet3/0/2 的 IP 地址。

```
[RouterB] interface gigabitethernet 3/0/2
[RouterB-GigabitEthernet3/0/2] ip address 10.1.2.1 255.255.255.0
[RouterB-GigabitEthernet3/0/2] quit
```

配置接口 GigabitEthernet3/0/1 的 IP 地址。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] ip address 2.2.2.2 255.255.255.0
```

在接口 GigabitEthernet3/0/1 上应用 IPsec 安全策略组。

```
[RouterB-GigabitEthernet3/0/1] ipsec policy use1
```

配置到 Host A 所在子网的静态路由。

```
[RouterB] ip route-static 10.1.1.0 255.255.255.0 1.1.1.1
```

4. 验证配置结果

以上配置完成后，Router A 和 Router B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 协商。由于 Router A 上配置了提议 10，其中使用的认证算法为 **md5**，但 Router B 上使用的是缺省的 IKE 提议，默认的认证算法为 **sha**。因此，在进行 IKE 提议匹配的时候，从优先级最高的提议开始匹配，因为 Router B 上没有和 Router A 上提议 10 相匹配的 IKE 提议，所以双方能够匹配的只有缺省的 IKE 提议。另外，在进行提议匹配的时候，存活时间是不用进行匹配的，它由 IKE 协商双方决定。

```
[RouterA] display ike proposal
 priority authentication authentication encryption Diffie-Hellman duration
              method       algorithm    algorithm     group       (seconds)
------------------------------------------------------------------------------
  10       PRE_SHARED     MD5          DES_CBC         MODP_768       5000
  default  PRE_SHARED     SHA          DES_CBC         MODP_768       86400
[RouterB] display ike proposal
 priority authentication authentication encryption Diffie-Hellman duration
              method       algorithm    algorithm     group       (seconds)
------------------------------------------------------------------------------
  default  PRE_SHARED     SHA          DES_CBC         MODP_768       86400
```

可通过如下显示信息查看到 IKE 协商成功后生成的两个阶段的 SA。

```
[RouterA] display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  ----------------------------------------------------------
     1             2.2.2.2         RD|ST         1     IPSEC
     2             2.2.2.2         RD|ST         2     IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO-TIMEOUT RK-REKEY
```

IKE 第二阶段协商生成的 IPsec SA 用于保护子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的数据流，可通过如下显示信息查看。

```
[RouterA] display ipsec sa
==============================
Interface: GigabitEthernet3/0/1
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "map1"
  sequence number: 10
  acl version: ACL4
  mode: isakmp
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.1.1.1
        remote address: 2.2.2.2
    flow:
        sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 10.1.2.0/255.255.255.0  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0x3d6d3a62(1030568546)
      transform: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      in use setting: Tunnel
      connection id: 1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3590
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 0x553faae(89389742)
      transform: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      in use setting: Tunnel
      connection id: 2
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3590
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N
```

2.11.2 IKE野蛮模式及NAT穿越典型配置举例

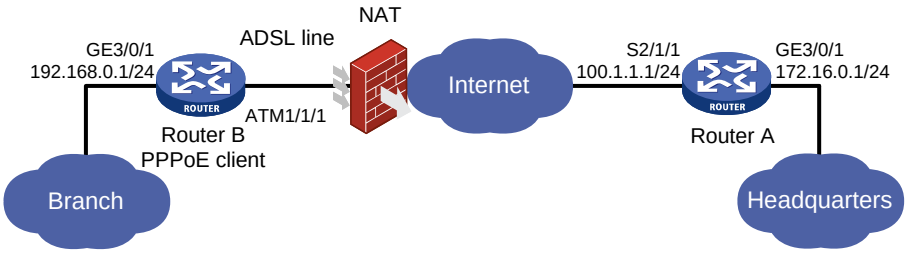
1. 组网需求

本例将 IPsec 和 ADSL 相结合，是目前实际中广泛应用的典型案例。

- 公司分支局域网通过 Router B 接入到 ATM 网络，Router B 作为 PPPoE 的 client 端，通过 ADSL 卡直接连接公网的 DSLAM 接入端。Router B 与公网连接的接口 IP 地址为 ISP 动态分配的私网 IP 地址。
- 公司总部局域网通过 Router A 接入到 ATM 网络，Router A 与公网连接的接口 IP 地址为固定的公网 IP 地址。
- 采用 IKE 协商的方式创建 IPsec 安全隧道保护总部与分支之间的数据安全。

2. 组网图

图2-4 IKE 野蛮模式及 NAT 穿越典型组网图



3. 配置步骤

配置关键点：

- 由于 IPsec 隧道一端安全网关（Router B）的 IP 地址为动态获取，因此 IKE 的协商模式采用野蛮模式（**aggressive**）。
- 由于 IPsec 隧道的两端一端为公网地址，另一端为私网地址，因此需要在隧道两端上均配置 NAT 穿越功能。

(1) 配置 Router A

配置本端安全网关设备名称。

```
<RouterA> system-view
[RouterA] ike local-name routera
```

配置 ACL。

```
[RouterA] acl number 3101
[RouterA-acl-adv-3101] rule 0 permit ip source 172.16.0.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
[RouterA-acl-adv-3101] quit
```

配置 IKE 安全提议。

```
[RouterA] ike proposal 1
[RouterA-ike-proposal-1] authentication-algorithm sha
[RouterA-ike-proposal-1] authentication-method pre-share
[RouterA-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterA-ike-proposal-1] dh group2
```

配置 IKE 对等体 peer。

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] exchange-mode aggressive
[RouterA-ike-peer-peer] pre-shared-key abc
[RouterA-ike-peer-peer] id-type name
```

```
[RouterA-ike-peer-peer] remote-name routerb
[RouterA-ike-peer-peer] nat traversal
[RouterA-ike-peer-peer] quit
```
创建 IPsec 安全提议 tran1。
```
[RouterA] ipsec transform-set tran1
[RouterA-ipsec-transform-set-tran1] encapsulation-mode tunnel
[RouterA-ipsec-transform-set-tran1] transform esp
[RouterA-ipsec-transform-set-tran1] esp encryption-algorithm 3des
[RouterA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterA-ipsec-transform-set-tran1] quit
```
创建 IPsec 安全策略 policy 并指定通过 IKE 协商建立 SA。
```
[RouterA] ipsec policy policy 10 isakmp
```
配置 IPsec 安全策略 policy 引用 IKE 对等体 peer。
```
[RouterA-ipsec-policy-isakmp-policy-10] ike-peer peer
```
配置 IPsec 安全策略 policy 引用访问控制列表 3101。
```
[RouterA-ipsec-policy-isakmp-policy-10] security acl 3101
```
配置 IPsec 安全策略 policy 引用 IPsec 安全提议 tran1。
```
[RouterA-ipsec-policy-isakmp-policy-10] transform-set tran1
[RouterA-ipsec-policy-isakmp-policy-10] quit
```
配置 IP 地址。
```
[RouterA] interface serial 2/1/1
[RouterA-Serial2/1/1] ip address 100.1.1.1 255.255.255.0
[RouterA-Serial2/1/1] ipsec policy policy
[RouterA-Serial2/1/1] quit
```
配置以太网口。
```
[RouterA] interface gigabitethernet 3/0/1
[RouterA-GigabitEthernet3/0/1] ip address 172.16.0.1 255.255.255.0
[RouterA-GigabitEthernet3/0/1] quit
```
配置到分公司局域网的静态路由。
```
[RouterA] ip route-static 192.168.0.0 255.255.255.0 serial 2/1/1
```
(2) 配置 Router B

配置本端安全网关的名称。
```
<RouterB> system-view
[RouterB] ike local-name routerb
```
配置 ACL。
```
[RouterB] acl number 3101
[RouterB-acl-adv-3101] rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 172.16.0.0
0.0.0.255
[RouterB-acl-adv-3101] quit
```
配置 IKE 安全提议。
```
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] authentication-algorithm sha
[RouterB-ike-proposal-1] authentication-method pre-share
[RouterB-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterB-ike-proposal-1] dh group2
```

配置 IKE 对等体 peer。

```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] exchange-mode aggressive
[RouterB-ike-peer-peer] pre-shared-key abc
[RouterB-ike-peer-peer] id-type name
[RouterB-ike-peer-peer] remote-name routera
[RouterB-ike-peer-peer] remote-address 100.1.1.1
[RouterB-ike-peer-peer] nat traversal
[RouterB-ike-peer-peer] quit
```

创建 IPsec 安全提议 tran1。

```
[RouterB] ipsec transform-set tran1
[RouterB-ipsec-transform-set-tran1] encapsulation-mode tunnel
[RouterB-ipsec-transform-set-tran1] transform esp
[RouterB-ipsec-transform-set-tran1] esp encryption-algorithm 3des
[RouterB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[RouterB-ipsec-transform-set-tran1] quit
```

创建 IPsec 安全策略 policy 并指定通过 IKE 协商建立 SA。

```
[RouterB] ipsec policy policy 10 isakmp
```

配置 IPsec 安全策略 policy 引用 IKE 对等体 peer。

```
[RouterB-ipsec-policy-isakmp-policy-10] ike-peer peer
```

配置 IPsec 安全策略 policy 引用访问控制列表 3101。

```
[RouterB-ipsec-policy-isakmp-policy-10] security acl 3101
```

配置 IPsec 安全策略 policy 引用 IPsec 安全提议 tran1。

```
[RouterB-ipsec-policy-isakmp-policy-10] transform-set tran1
[RouterB-ipsec-policy-isakmp-policy-10] quit
```

配置拨号访问控制列表。

```
[RouterB] dialer-rule 1 ip permit
```

创建 Dialer0，使用由 ISP 分配的用户名和密码进行拨号和 PPP 认证的相关配置，并配置 MTU。

```
[RouterB] interface dialer 0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp pap local-user test password simple 123456
[RouterB-Dialer0] ip address ppp-negotiate
[RouterB-Dialer0] dialer user 1
[RouterB-Dialer0] dialer-group 1
[RouterB-Dialer0] dialer bundle 1
[RouterB-Dialer0] ipsec policy policy
[RouterB-Dialer0] mtu 1492
[RouterB-Dialer0] quit
```

配置到总公司局域网的静态路由。

```
[RouterB] ip route-static 172.16.0.0 255.255.255.0 dialer 0
```

配置以太网口。

```
[RouterB] interface gigabitethernet 3/0/1
[RouterB-GigabitEthernet3/0/1] tcp mss 1450
[RouterB-GigabitEthernet3/0/1] ip address 192.168.0.1 255.255.255.0
[RouterB-GigabitEthernet3/0/1] quit
```

配置 VE 口。

```
[RouterB] interface virtual-ethernet 0
[RouterB-Virtual-Ethernet0] pppoe-client dial-bundle-number 1
[RouterB-Virtual-Ethernet0] mac-address 0011-0022-0012
[RouterB-Virtual-Ethernet0] quit
```

对 ADSL 卡的 ATM 口进行配置。

```
[RouterB] interface atm 1/1/1
[RouterB-Atm1/1/1] pvc 0/100
[RouterB-atm-pvc-Atm1/1/1-0/100] map bridge virtual-ethernet 0
[RouterB-atm-pvc-Atm1/1/1-0/100] quit
```

2.12 常见错误配置举例

配置参数建立 IPsec 安全隧道时，可以打开 IKE 的 Error 调试开关，帮助我们查找配置问题。其命令是：

```
<Router> debugging ike error
```

2.12.1 非法用户身份信息

1. 故障现象

非法用户身份信息

2. 故障分析

用户身份信息是发起 IPsec 通信的用户用来标识自己的数据。在实际应用中我们可以通过用户身份标识实现对不同的数据流建立不同的安全隧道进行保护。目前我们是通过用户的 IP 地址和名字来标识用户。

可以看到调试信息：

```
got NOTIFY of type INVALID_ID_INFORMATION
```

或者

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

3. 处理过程

检查协商两端接口上配置的 IPsec 安全策略中的 ACL 内容是否相容。建议用户将两端的 ACL 配置成互为镜像的。ACL 镜像的含义请参考 IPsec 配置中“配置访问控制列表”内容。

2.12.2 提议不匹配

1. 故障现象

提议不匹配

2. 故障分析

可以看到调试信息：

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

或者：

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

协商双方没有可以匹配的提议。

3. 处理过程

对于阶段 1，检查 IKE proposal 是否有与对方匹配的。对于阶段 2 协商，检查双方接口上应用的 IPsec 安全策略的参数是否匹配，引用的 IPsec 安全提议的协议、加密算法和认证算法是否有匹配的。

2.12.3 无法建立安全隧道

1. 故障现象

无法建立安全隧道

2. 故障分析

实际应用中有时会发现在不稳定的网络状态下，安全隧道无法建立或者存在安全隧道却无法通信，而且检查双方的 ACL 的配置正确，也有匹配的提议。

这种情况一般是安全隧道建立好以后，有一方的设备重启造成的。

3. 处理过程

- 使用 **display ike sa** 命令检查双方是否都已建立阶段 1 的 SA。
- 使用 **display ipsec sa policy** 命令查看接口上的安全策略是否已建立了 IPsec SA。
- 根据以上两步的结果查看，如果有一方存在的 SA 在另一方上不存在，请先使用 **reset ipsec sa** 命令清除双方不对称存在的 IPsec SA，再使用 **reset ike sa** 命令清除双方不对称存在的 IKE SA，并重新发起协商。

2.12.4 ACL配置错误

1. 故障现象

ACL 配置错误，导致协商成功之后数据流不通

2. 故障分析

多台设备之间先后建立不同的安全隧道，出现同一设备有不同对端的情况。若此设备不配置 ACL 规则，则分别由对端发起报文来与之建立保护粒度不同的安全隧道。由于安全隧道的优先级由它们创建的顺序决定，当这一设备的出方向报文首先匹配到较粗粒度的安全隧道时，将导致此设备无法与其它较细粒度对端互通。

3. 处理过程

为避免这种情况发生，当同一设备有不同对端时，建议用户在此设备上配置 ACL 来区别数据流，且与不同对端尽量避免配置有重复范围的 ACL 子规则。若需要有重复范围的子规则，应该将细粒度的子规则配置为较高的优先级。