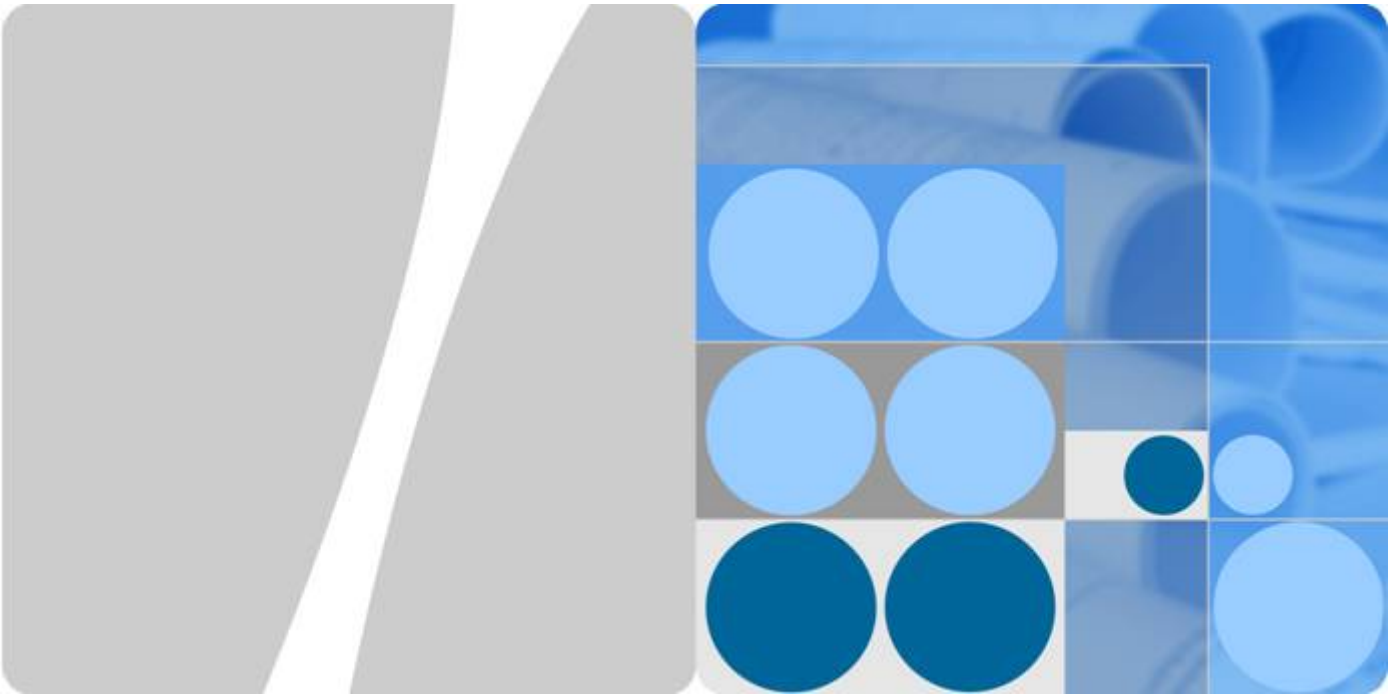


Huawei AR2200-S 系列企业路由器

V200R001C01

特性描述-VPN

文档版本　01

发布日期　2012-01-06

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR2200-SVPN 部分的特性原理、参考标准。

本文档与其它类型手册相结合，便于读者深入掌握特性的实现原理。

本文档主要适用于以下工程师：

- 网络规划工程师
- 调测工程师
- 数据配置工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-01-06)

第一次正式发布。

目 录

1 GRE

关于本章

1.1 介绍

定义

GRE（Generic Routing Encapsulation）是通用路由封装协议，可以对某些网络层协议的数据报进行封装，使这些被封装的数据报能够在 IPv4 网络中传输。

GRE 提供了将一种协议的报文封装在另一种协议报文中的机制，使报文能够在异种网络中传输，而异种报文传输的通道称为 tunnel。

目的

为了使某些网络层协议的报文能够在 IPv4 网络中传输，可以将某些网络层协议的报文进行封装，以此解决了异种网络的传输问题。

GRE 也可以作为 VPN 的第三层隧道协议，为 VPN 数据提供透明传输通道。

1.2 参考标准和协议

本特性的参考资料清单如下：

文档	描述	备注
RFC1701	Generic Routing Encapsulation（GRE）	
RFC1702	Routing Encapsulation over IPv4 networks	
RFC2784	Generic Routing Encapsulation (GRE)	

1.3 可获得性

涉及网元

无需其它网元的配合。

License 支持

无需获得 License 许可，均可获得该特性的服务。

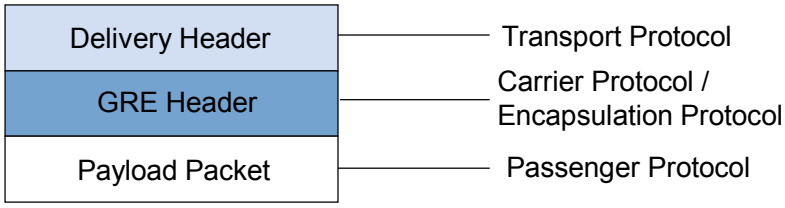
版本支持

产品	最低支持版本
AR2200-S	V200R001C01

1.4 原理描述

系统收到需要进行封装和路由的某网络层协议数据时，将首先对其加上 GRE 报文头，使之成为 GRE 报文，再将其封装在另一协议（如 IP）中。这样，此报文的转发就可以完全由 IP 协议负责。封装后的报文的格式如图 1-1 所示：

图 1-1 封装好的 GRE 报文格式

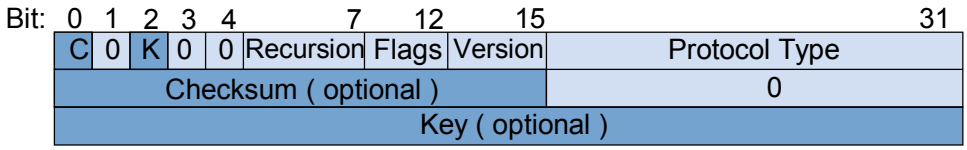


- 净荷（Payload）：系统收到的需要封装和路由的数据报称为净荷。
- 乘客协议（Passenger Protocol）：封装前的报文协议称为乘客协议。
- 封装协议（Encapsulation Protocol）：上述的 GRE 协议称为封装协议，也称为运载协议（Carrier Protocol）。
- 传输协议（Transport Protocol 或者 Delivery Protocol）：负责对封装后的报文进行转发的协议称为传输协议。

GRE 报文头

GRE 头格式如图 1-2 所示：

图 1-2 GRE 头



各字段解释如下：

- C：校验和验证位。如果该位置 1，表示 GRE 头插入了校验和（Checksum）字段；该位为 0 表示 GRE 头不包含校验和字段。
- K：关键字位。如果该位置 1，表示 GRE 头插入了关键字（Key）字段；该位为 0 表示 GRE 头不包含关键字字段。
- Recursion：用来表示 GRE 报文被封装的层数。完成一次 GRE 封装后将该字段加 1。如果封装层数大于 3，则丢弃该报文。该字段的作用是防止报文被无限次的封装。

说明

- RFC1701 规定字段默认值为 0。
- RFC2784 规定当发送和接受端该字段不一致时不会引起异常，且接收端必须忽略该字段。
- 设备实现时该字段仅在加封装报文时用作标记隧道嵌套层数，GRE 解封装报文时不感知该字段，不会影响报文的处理。

- Flags：预留字段。当前必须设为 0。
- Version：版本字段，必须置为 0。Version 为 1 是使用在 RFC2637 的 PPTP 中。
- Protocol Type：乘客协议的协议类型。
- Checksum：对 GRE 头及其负载的校验和字段。
- Key：关键字字段，隧道接收端用于对收到的报文进行验证。

因为目前实现的 GRE 头不包含源路由字段，所以 Bit 1、Bit3 和 Bit 4 都置为 0。

GRE 的特点

GRE 主要有以下特点：

- 机制简单，对隧道两端设备的 CPU 负担小。
- 本身不提供数据的加密，可以与 IPSec 结合使用。
- 不提供流量控制和 QoS。

GRE 隧道接口

隧道接口（Tunnel 接口）是为实现报文的封装而提供的一种点对点类型的虚拟接口，与 Loopback 接口类似，都是一种逻辑接口。

GRE 隧道接口与其他隧道接口类似，都包含以下元素：

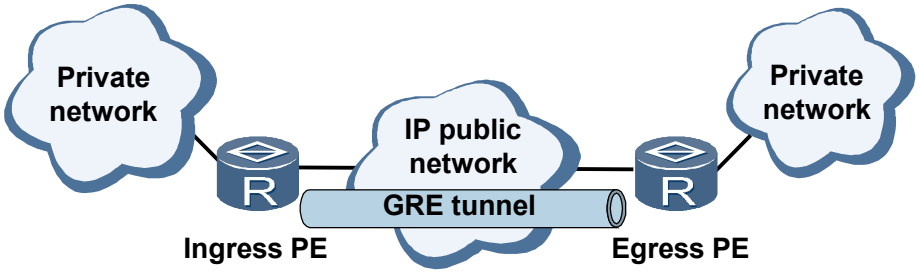
- 源地址：报文传输协议中的源地址。从负责封装后报文传输的网络来看，隧道的源地址就是实际发送报文的接口 IP 地址。
- 目的地址：报文传输协议中的目的地址。从负责封装后报文传输的网络来看，隧道本端的目的地址就是隧道目的端的源地址。
- 隧道接口 IP 地址：为了在隧道接口上启用动态路由协议，或使用静态路由协议发布隧道接口，需要为隧道接口分配 IP 地址。隧道接口的 IP 地址可以不是公网地址，甚至可以借用其他接口的 IP 地址以节约 IP 地址。但是当 Tunnel 接口借用 IP 地址时，由于 Tunnel 接口本身没有 IP 地址，无法在此接口上启用动态路由协议，必须配置静态路由或策略路由才能实现设备间的连通性。
- 封装类型：隧道接口的封装类型是指该隧道接口对报文进行的封装方式。有两种封装方式，分别是 GRE 和 IPv4-IPv6。对于 GRE 隧道接口而言，封装类型则为 GRE。

经过手工配置，成功建立隧道之后，就可以将隧道接口看成是一个物理接口，在其上运行动态路由协议或配置静态路由。

报文在 GRE 中的传输过程

报文在 GRE 隧道中传输包括封装和解封装两个过程。以图 1-3 的网络为例，如果私网报文从 Ingress PE 向 Egress PE 传输，则封装在 Ingress PE 上完成；而解封装在 Egress PE 上进行。

图 1-3 私有网络通过 GRE 隧道互连



封装

Ingress PE 从连接私网的接口接收到私网报文后，首先交由私网上运行的协议模块处理。

私网协议模块检查私网报文头中的目的地址域在私网路由表或转发表中查找出接口，确定如何路由此包。如果发现出接口是 Tunnel 接口，则将此报文发给隧道模块。

隧道模块收到此报文后进行如下处理：

1. 隧道模块根据乘客报文的协议类型和当前 GRE 隧道所配置的 Key 和 Checksum 参数，对报文进行 GRE 封装，即添加 GRE 头。
2. 根据配置信息（传输协议为 IP），给报文加上 IP 头。该 IP 头的源地址就是隧道源地址，IP 头的目的地址就是隧道目的地址。
3. 将该报文交给 IP 模块处理。

   IP 模块根据该 IP 头目的地址，在公网路由表中查找相应的出接口并发送报文。之后，封装后的报文将在该 IP 公共网络中传输。

解封装

解封装过程和封装过程相反。Egress PE 从连接公网的接口收到该报文，分析 IP 头发现报文的目的地址为本设备，且协议字段值为 47，表示协议为 GRE（参见 RFC1701），于是交给 GRE 模块处理。GRE 模块去掉 IP 头和 GRE 报头，并根据 GRE 头的 Protocol Type 字段，发现此报文的乘客协议为私网上运行的协议，于是交由此协议处理。此协议像对待一般数据报一样对此数据报进行转发。

1.4.1 GRE 的安全机制

GRE 本身提供两种比较弱的安全机制：

- 校验和验证
- 识别关键字验证

校验和验证

校验和验证是指对封装的报文进行端到端校验。

RFC1701（Generic Routing Encapsulation）中规定：如果 GRE 报文头中的 C 位（参考 **1.4 原理描述**）为 1，则校验和有效。校验和是 GRE 头中的可选字段。如果 C 位置 1，则发送方将根据 GRE 头及 payload 信息计算校验和，在报文头的 Checksum 字段的位置插入校验和，将包含校验和的报文发送给对端。接收方对接收到的报文计算校验和，并

与报文中的校验和进行比较。如果计算出来的校验和与报文中的校验和一致，则对报文进一步处理，否则丢弃报文。

实际应用时，隧道两端可以根据需要选择是否配置校验和，从而决定是否触发校验功能。

因校验和配置不同，对收发报文的处理方式也不同。简单的说，就是根据报文头的 C 位决定是否检查校验和，根据本端配置决定是否计算校验和并填充到报文中。参见**表 1-1**。

表 1-1 校验和与报文处理

本端	对端	本端对接收报文的处理	本端对发送报文的处理
配置校验和	没有配置校验和	接收报文中 C 位为 0，校验和无效，不检查校验和	发送报文中 C 位置 1，计算校验和，并填充到 Checksum 字段
没有配置校验和	配置校验和	接收报文中 C 位为 1，校验和有效，检查校验和是否与报文中一致	发送报文中 C 位置 0，不计算校验和

识别关键字验证

识别关键字（key）是指对 Tunnel 接口进行校验。通过这种弱安全机制，可以防止错误识别、接收其它地方来的报文。

RFC1701 中规定：若 GRE 报文头中的 K 位为 1，则在 GRE 头中插入关键字字段，收发双方将进行通道识别关键字的验证。

关键字字段是一个四字节长的数值，在报文封装时被插入 GRE 头。关键字的作用是标志隧道中的流量。属于同一流量的报文使用相同的关键字。在报文解封装时，隧道端将基于关键字来识别属于相同流量的数据报。

只有 Tunnel 两端设置的识别关键字完全一致时才能通过验证，否则将报文丢弃。这里的“完全一致”是指两端都不设置识别关键字；或者两端都设置关键字，且关键字的值相等。

1.4.2 Keepalive 检测

GRE 的数据空洞

目前 GRE 协议并不具备探测链路状态的功能。如果远端端口不可达，隧道并不能及时关闭该 Tunnel 连接，这样会造成源端会不断的向对端转发数据，而对端却因 Tunnel 不通而丢弃所有报文，由此就会形成数据发送的空洞。

Keepalive 检测功能

设备实现了 GRE 隧道的链路状态检测功能（Keepalive 检测功能）。Keepalive 检测功能用于时刻检测隧道链路是否处于 Keepalive 状态，即检测隧道对端是否可达。如果对端不可达，隧道连接就会及时关闭，避免形成数据空洞。

如果 GRE 隧道本端使能 Keepalive 检测功能，则会周期地发送 keepalive 探测报文给对端。若对端可达，则本端会收到对端的回应报文；否则，收不到对端的回应报文。

说明

对于设备实现的 GRE，只要在隧道一端配置 Keepalive，该端就具备 keepalive 功能，而不要求隧道对端也具备该功能。隧道对端收到报文，如果是 Keepalive 探测报文，无论是否配置 Keepalive，都会给源端发送一个回应报文。

不可达计数器

GRE 隧道的源端使能 Keepalive 检测功能后，就创建一个定时器，周期地发送 keepalive 探测报文，同时进行不可达计数。每发送一个探测报文，不可达计数加 1。

对端每收到一个探测报文，就给源端发送一个回应报文。

如果源端的计数器值未达到预先设置的值就收到回应报文，就表明对端可达。如果源端的计数器值到达预先设置的值——重试次数（Retry Times）时，还没收到回送报文，就认为对端不可达。此时，源端将关闭隧道连接。

1.4.3 协议的比较

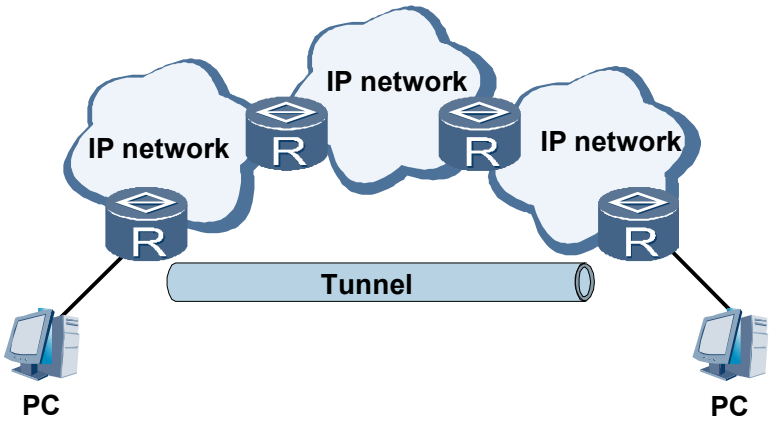
GRE 协议与 IP 协议的比较

协议	特点
GRE	● 多协议的本地网通过单一协议的骨干网传输的服务。 ● 扩大了网络的工作范围，包括那些路由网关有限的协议。 ● 将一些不能连续的子网连接起来。
IP	报文只在支持 IP 协议的传输网中传输。

1.5 应用

1.5.1 扩大跳数受限的网络工作范围

图 1-4 扩大网络工作范围



在图 1-4 中，网络运行 IP 协议，假设 IP 协议限制跳数为 255。如果两台 PC 之间的跳数超过 255，它们将无法通信。在网络中使用隧道可以隐藏一部分步跳，从而扩大网络的工作范围。

1.6 术语与缩略语

术语

术语	解释
GRE	用来对某些网络层协议的报文进行封装，使这些被封装的报文能够在另一网络层协议中传输。GRE 可以作为 VPN 的第三层隧道协议，为 VPN 数据提供透明传输通道。

缩略语

缩略语	英文全称	中文全称
GRE	Generic Routing Encapsulation	通用路由封装协议

2 IPSec

关于本章

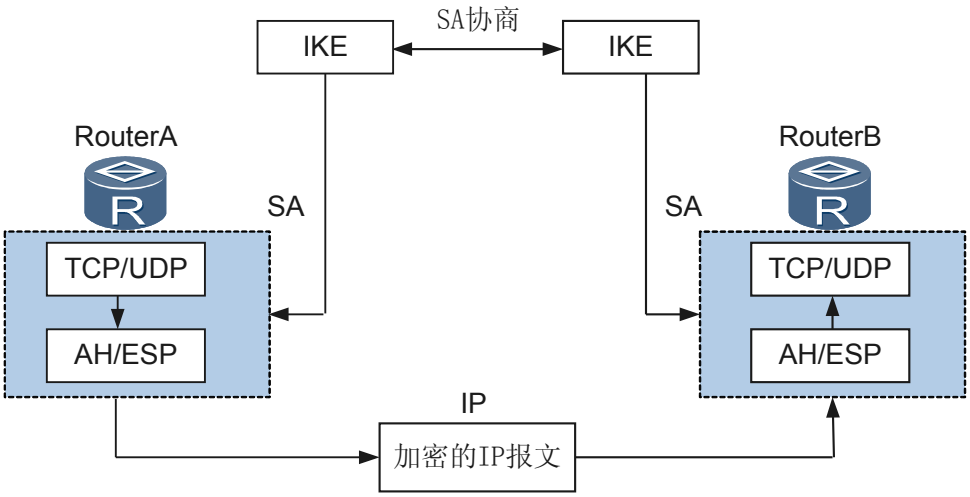
2.1 介绍

定义

IPSec（Internet Protocol Security）协议族是 IETF（Internet Engineering Task Force）制定的一系列协议，它为 IP 数据包提供了高质量的、基于密码学的安全传输特性。特定的通信双方在 IP 层通过加密与数据源认证等方式，保证 IP 数据报在网络上传输的私有性、完整性和防重放。

- 私有性（Confidentiality）指对用户数据进行加密保护，用密文的形式传送。
- 完整性（Data integrity）指对接收的数据进行认证，以判定报文是否被篡改。
- 防重放（Anti-replay）指防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

图 2-1 IPSec 的 SA 协商图



IPSec 协议族示意框架说明如图 2-1 所示，IPSec 通过认证头 AH（Authentication Header）和封装安全载荷 ESP（Encapsulating Security Payload）这两个安全协议来实现 IP 数据报的安全传送；因特网密钥交换协议 IKE（Internet Key Exchange）提供密钥协商、建立和维护安全联盟的服务，以简化 IPSec 的部署和使用。

- AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。发送端对 IP 头的不变部分和 IP 净荷进行离散运算，生成一个摘要字段；接收端根据接收的 IP 报文，对报文重新计算摘要字段，通过摘要字段的比较，判别报文在网络传输期间是否被篡改。AH 认证头协议没有对 IP 净荷提供加密操作。
- ESP 封装安全载荷协议：除提供 AH 认证头协议的所有功能之外，还可对 IP 报文净荷进行加密。ESP 协议允许对 IP 报文净荷进行加密和认证、只加密或者只认证，ESP 没有对 IP 头的内容进行保护。
- IKE 因特网密钥交换协议：完成 IPSec 通信对等体间的安全联盟 SA(Security Association)协商，协商出对等体间数据安全传输需要的认证算法、加密算法和对应的密钥。

说明

- AH 和 ESP 可以单独使用，也可以同时使用。AH 和 ESP 同时使用时，报文在 IPSec 安全转换时，先进行 ESP 封装，再进行 AH 封装；IPSec 解封装时，先进行 AH 解封装，再进行 ESP 解封装。
- IKE 密钥交换协商并不是必须的，IPSec 所使用的策略和算法等也可以手工配置。

目的

在 IP 网络的传输中，绝大部分数据的内容都是明文传输的，这样就会存在很多潜在的危险，比如：密码、银行帐户的信息被窃取；用户的身份被冒充等。网络中部署 IPSec 后，可对传输的 IP 数据进行保护处理，降低信息泄漏的风险。

受益

运营商受益

满足用户的安全传输需求，增强 IP 网络数据传输的可靠性。

用户受益

- 用户业务数据在 IP 网络传输时，减少了泄漏和被窃听的风险，保障了用户业务传输的安全。
- 减少用户在各级应用层自部署 TLS 等安全特性的开销，节约用户业务部署成本。

2.2 参考标准和协议

本特性的参考资料清单如下：

文档	描述
RFC2401	Security Architecture for the Internet Protocol
RFC2402	IP Authentication Header
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2407	The Internet IP Security Domain of Interpretation for ISAKMP
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC2409	The Internet Key Exchange (IKE)
RFC2367	PF_KEY Key Management API, Version 2
RFC3706	A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC4306	Internet Key Exchange (IKEv2) Protocol
RFC4478	Repeated Authentication in Internet Key Exchange (IKEv2) Protocol

2.3 可获得性

涉及网元

IPSec 特性涉及与对端三层设备的互联互通，对端三层设备需启用 IPSec 功能。

License

无须 Licence 支持。

版本支持

产品	最低支持版本
AR2200-S	V200R001C01

特性依赖

- IPSec 对 IP 报文的传输提供安全保护，设备需启用三层功能。
- IPSec 对 GRE 流量进行保护时，先进行 GRE 的封装，再进行 IPSec 安全转换。

2.4 原理描述

2.4.1 IPSec 基本概念

IPSec 对等体

IPsec 用于在两个端点之间提供安全的 IP 通信，通信的两个端点被称为 IPsec 对等体。

安全联盟

SA（Security Association）安全联盟，定义了 IPSec 通信对等体间将使用哪种摘要和加密算法、什么样的密钥进行数据的安全转换和传输。

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；如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体针对每一种协议都需要构建一个独立的 SA。

SA 由一个三元组来唯一标识，这个三元组包括安全参数索引 SPI（Security Parameter Index）、目的 IP 地址、安全协议名（AH 或 ESP）。SPI 是一个 32 比特数值，它在 AH 和 ESP 头中传输。

安全联盟生成方式

有两种方式建立安全联盟，一种是手工方式（manual），一种是 IKE 动态协商（isakmp）方式。

手工方式建立安全联盟比较复杂，安全联盟所需的全部信息都必须手工配置，手工方式建立的安全联盟永不老化。

IKE 动态协商方式建立安全联盟则相应简单些，只需要通信对端体间配置好 IKE 协商参数，由 IKE 协议自动协商来创建和维护 SA。通过 IKE 协商建立的安全联盟具有生存周期：

- 基于时间的生存周期
- 基于流量的生存周期

生存周期达到指定的时间或指定的流量，安全联盟就会失效。安全联盟失效前，IKE 将为 IPSec 重新协商新的安全联盟。

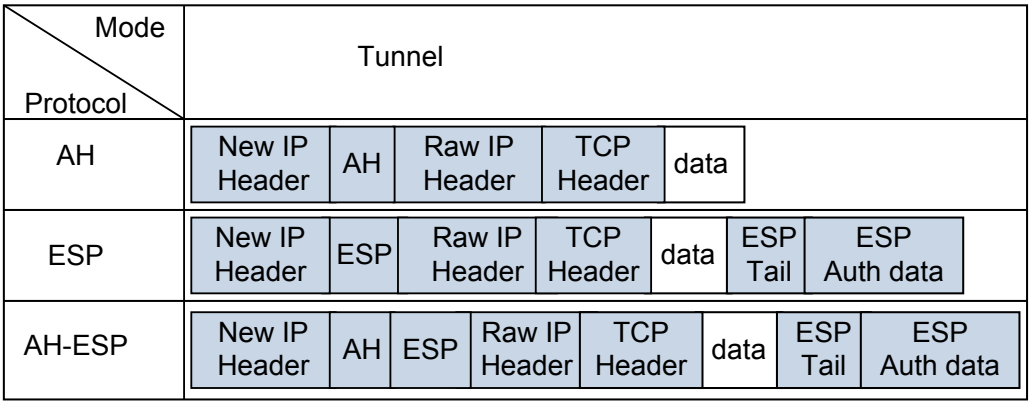
网络中，进行通信的 IPSec 对等体设备数量较少时，或者是在小型静态环境中，手工配置安全联盟是可行的；对于中、大型的动态网络环境中，推荐使用 IKE 动态协商建立安全联盟。

IPSec 封装模式

IPSec 协议有两种封装模式：

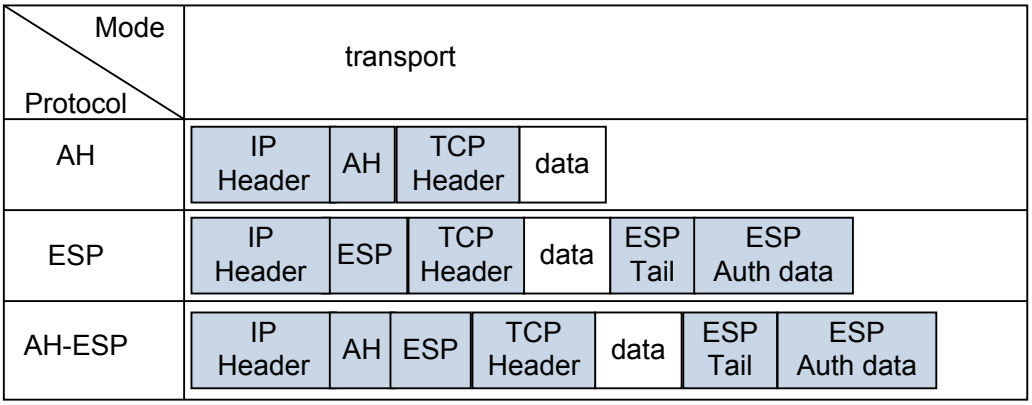
- 隧道模式。在隧道模式下，AH 或 ESP 插在原始 IP 头之前，另外生成一个新 IP 头放到 AH 或 ESP 之前。以 TCP 为例，如图 2-2 所示。

图 2-2 IPSec 隧道模式



- 传输模式。在传输模式下，AH 或 ESP 被插入到 IP 头之后但在传输层协议之前。以 TCP 为例，如图 2-3 所示

图 2-3 IPSec 传输模式



选择隧道模式还是传输模式可以从以下方面考虑：

- 从安全性来讲，隧道模式优于传输模式。它可以完全地对原始 IP 数据报进行认证和加密，而且，可以使用 IPSec 对等体的 IP 地址来隐藏客户机的 IP 地址。
- 从性能来讲，隧道模式因为有一个额外的 IP 头，所以它将比传输模式占用更多带宽。

认证算法与加密算法

- 认证算法

  AH 和 ESP 都能够对 IP 报文的完整性进行认证，以判别报文在传输过程中是否被篡改。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 对等体根据 IP 报文内容，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。一般来说 IPSec 可以使用两种认证算法：

  - MD5（Message Digest 5）：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
  - SHA-1（Secure Hash Algorithm）：SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

- 加密算法

  ESP 能够对 IP 报文内容进行加密保护，以防止报文内容在传输过程中被窥探。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。一般来说 IPSec 使用 DES、3DES（Triple Data Encryption Standard）及 AES（Advanced Encryption Standard）三种加密算法：

  - DES：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
  - 3DES：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。
  - AES：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。

2.4.2 IKE 协议

IKE 协议

IKE 协议建立在 Internet 安全联盟和密钥管理协议 ISAKMP（Internet Security Association and Key Management Protocol）定义的框架上，提供了一套在不安全的网络上安全地分发密钥、验证身份、建立 IPSec 安全联盟的过程，简化了 IPSec 的管理和使用。

IKE 的安全机制

IKE 支持如下安全机制：

- DH（Diffie-Hellman）交换及密钥分发：Diffie-Hellman 算法是一种公开密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）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。
- 完善的前向安全性 PFS（Perfect Forward Secrecy）：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。IPSec 第二阶段的密钥是从第一阶段的密钥导出的，当第一阶段 IKE 密钥被窃取后，攻击者将可能收集到足够的信息来导出第二阶段 IPSec SA 的密钥，PFS 通过执行一次额外的 DH 交换，保证第二阶段密钥的安全。
- 身份验证：身份验证指确认通信双方的身份。对于 pre-shared key 验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。
- 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。

IKEv1 密钥协商和交换

RFC2409（The Internet Key Exchange）中，对 IKEv1 密钥交换和协商定义了两个阶段：第一阶段，协商和建立 IKE 本身使用的安全通道；第二阶段，利用这个已通过了验证和安全保护的安全通道，为 IPSec 协商具体的 IPSec 通信使用的 SA。

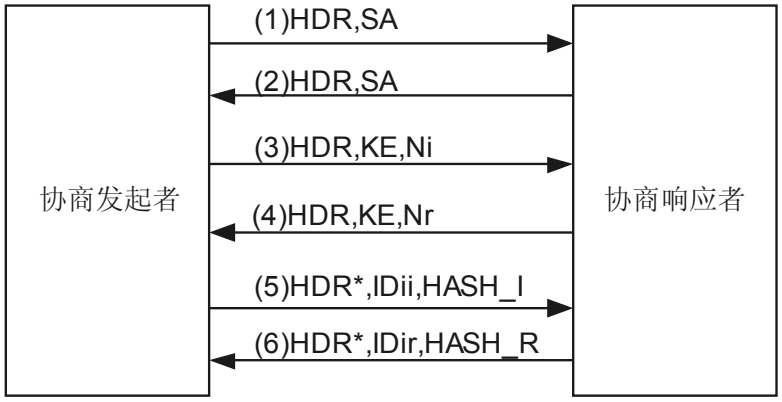
IKEv1 第一阶段交换和密钥协商定义了两种模式：主模式（Main Mode）和野蛮模式（Aggressive Mode），IKEv1 第二阶段交换和密钥协商只有一种模式，快速模式（Quick Mode）。

表 2-1 IKEv1 协商术语含义表

术语	英文含义	中文解释
HDR	ISAKMP header	ISAKMP 头
HDR*		带*表示数据被加密
SA	SA negotiation payload	安全关联载荷
KE	key exchange payload	密钥交换载荷
Nx	nonce payload	Nonce 载荷，x 取值为 i 或 r，分别表示发起方和响应方。Nonce 载荷的内容是一个用于保证存活和防止重放攻击的随机数

术语	英文含义	中文解释
IDx	identification payload	身份载荷，x 取值为 ii 或 ir，表示第一阶段的发起方身份和响应方身份；ci 或 cr 表示第二阶段发起方身份和响应方身份。
HASH_I	Hash Payload	Hash 载荷，用来验证 ISAKMP 消息的完整性、鉴别认证协商实体
HASH_R		

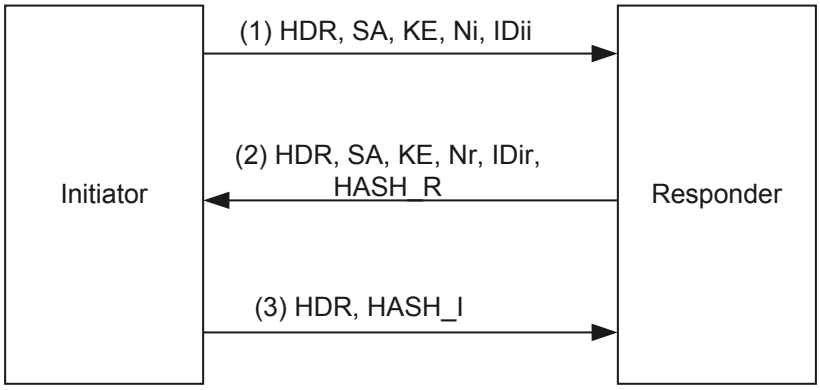
图 2-4 IKEv1 第一阶段主模式协商图



如图 2-4 所示，是 IKEv1 第一阶段主模式协商流程，步骤说明如下：

1. 发起者触发 IKEv1 第一阶段主模式协商，发送一个封装有 IKE 提议（加密算法、认证算法及认证方式）的 SA 载荷，SA 载荷中包括一个或多个 IKE 提议；
2. 响应者发送一个 SA 载荷，封装响应方接受的 IKE 提议（只能有一个提议）；
3. 发起者发送密钥交换载荷，交换 DH 密钥数据；
4. 响应者发送密钥交换载荷，交换 DH 密钥数据；
5. 发起者使用生成的 DH 密钥，加密发送身份信息和 HASH 认证信息；
6. 响应者验证发送者身份，使用生成的 DH 密钥，加密发送自身的身份信息，供发起者认证。

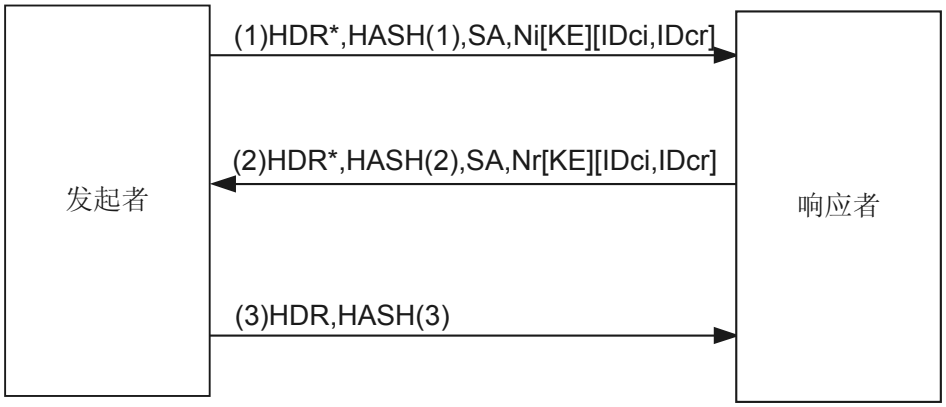
图 2-5 IKEv1 第一阶段野蛮模式协商图



如图 2-5 所示，是 IKEv1 第一阶段野蛮模式协商流程，步骤说明如下：

1. 发起者触发 IKEv1 第一阶段野蛮模式协商，发送一个包括 SA 载荷、密钥交换载荷、Nonce 载荷和身份信息消息；
2. 响应者发送 SA 载荷、密钥交换载荷、Nonce 载荷、身份信息和供发起者使用的 HASH 认证信息；
3. 发起者认证响应者的消息，发送 HASH 认证信息，供响应者认证。

图 2-6 IKEv1 第二阶段快速模式协商



如图 2-6 所示，IKE 对等体的任何一方都可以发起第二阶段协商，具体步骤如下：

1. 发起者发送协商 IPSec SA 的各项参数，可选参数是用于确定是否进行额外的完善的前向安全性 PFS 协商；
2. 响应者发送协商 IPSec SA 的各项参数，可选参数是用于确定是否进行额外的完善的前向安全性 PFS 协商；
3. 发起者应答确认。

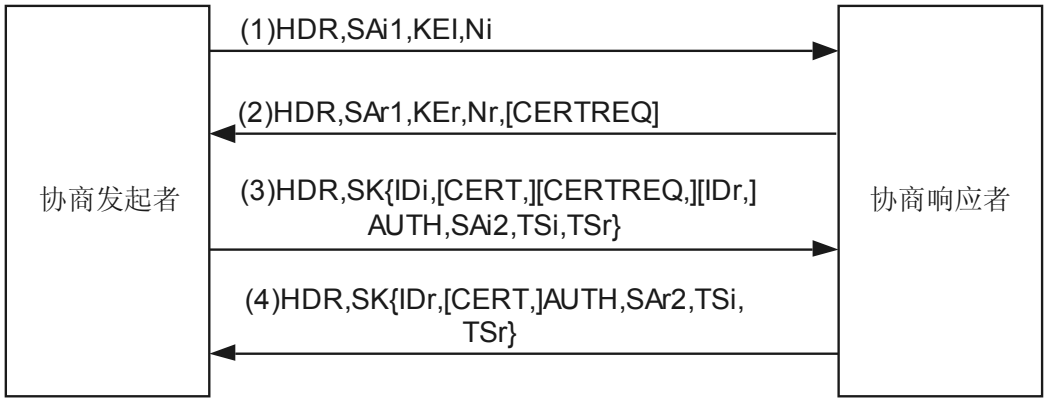
主模式和野蛮模式的区别比较：

- 主模式交换消息为 6 个，野蛮模式为 3 个，野蛮模式能够更快地创建 IKE SA。
- 主模式协商将密钥交换信息与身份、验证信息相分离，这种分离保护了对等体的身份信息。
- 野蛮模式交换的 3 个消息没有经过加密，身份信息也是明文的，容易造成安全隐患。
- 主模式只能采用 IP 地址方式标识对等体，而野蛮模式可以采用 IP 地址方式或者 Name 方式标识对等体。这是因为主模式在交换完 3、4 消息以后，需要使用预共享密钥来计算 SKEYID，当一个设备有多个对等体时，必须查找到该对等体对应的预共享密钥，使用消息 3、4 中的 IP 报文源地址可找到对应的对等体。

IKEv2 密钥协商和交换

IKEv2 保留了 IKEv1 的大部分特性，IKEv2 在 RFC4306 中定义，与 IKEv1 的第一阶段交换和第二阶段交换不同，IKEv2 定义了三种交换，初始交换（Initial Exchanges）、创建子 SA 交换（CREATE_CHILD_SA Exchange）以及通知交换（INFORMATIONAL Exchange）。

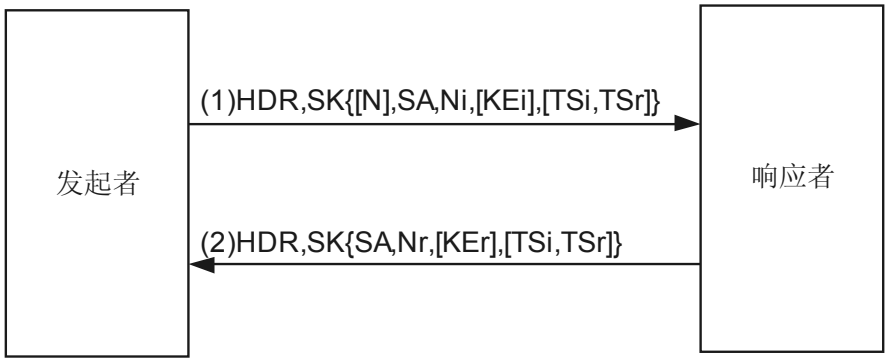
图 2-7 IKEv2 初始交换图



如图 2-7 所示，IKEv2 初始交换流程如下：

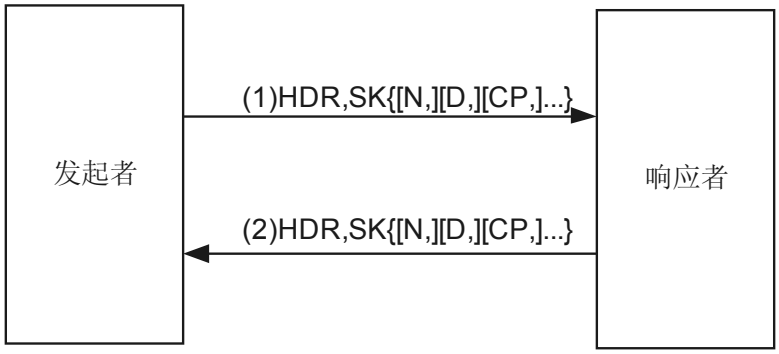
1. 发起者发送 KE 密钥交换载荷和安全联盟参数；
2. 响应者发送 KE 密钥交换载荷和安全联盟参数；
3. 根据密钥交换生成的密钥材料，发起者加密发送证书载荷、流信息载荷，进行认证协商；
4. 根据密钥交换生成的密钥材料，响应者加密发送证书载荷、流信息载荷，进行认证协商。

图 2-8 IKEv2 创建 SA 交换图



如图 2-8 所示，创建子 SA 协商对应两条消息，对应 IKEv1 中的第二阶段协商，协商的发起者可以是 IKE 初始交换的发起者，也可以是 IKE 初始交换的响应者；创建子 SA 协商可额外进行一次 DH 交换，生成新的 KE，TSi 和 TSr 用于协商 IPSec 对等体间的通信流量。

图 2-9 IKEv2 通知交换图



如图 2-9 所示 IKEv2 通知交换用于对等体间传送控制消息，可以是 IKE_SA 的控制消息也可以是子 SA 的控制消息。

2.4.3 IPSec 的实现过程

通过 IPSec，对等体之间能够对不同的数据流实施不同的安全保护（认证、加密或两者同时使用）。简要的实现过程如下。

1. 定义被保护的数据流。通过配置 ACL 来区分数据流；
2. 定义安全提议。通过配置安全提议来确定安全保护所用到的安全协议、认证算法、加密算法和封装模式；
3. 定义安全策略或安全策略组。通过配置安全策略或安全策略组来确定被保护的数据流和安全提议的关联（即定义对何种数据流实施何种保护）、安全通信的 IKE 对等体或手工 SA 参数；
4. 在接口上实施安全策略。

定义被保护的数据流

数据流是一组流量（traffic）的集合，由源地址/掩码、目的地址/掩码、IP 报文承载的协议号、源端口号、目的端口号等来规定。

AR 中，数据流采用 ACL Group 来定义，一个数据流可以小到是两台主机之间单一的 TCP 连接，也可以大到是两个子网之间所有的流量。IPSec 能够以 ACL Group 力度对不同的数据流划分，IPSec 配置的第一步就是定义数据流。

定义安全提议

安全提议规定了对要实施 IPSec 保护的数据流所采用的安全协议、封装模式、认证算法和加密算法等。

AH 和 ESP 安全协议，两者既可单独使用，也可联合使用。其中，AH 支持 MD5 和 SHA-1 认证算法；ESP 协议支持 MD5、SHA-1 认证算法和 DES、3DES、AES 加密算法。支持的封装模式包括传输模式和隧道模式。

对同一数据流，在安全隧道两端的对等体必须设置相同的协议、算法和封装模式。另外，如果两个安全网关之间实施 IPSec，建议采用隧道模式，以隐藏实际通信的源和目的 IP 地址。

定义安全策略或安全策略组

安全策略通过引用安全提议来规定对特定的数据流采用特定的安全协议、算法和报文封装形式。一条安全策略由“名字”和“顺序号”共同唯一确定。安全策略分为手工安全策略和 IKE 协商安全策略，前者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；后者则由 IKE 自动协商生成这些参数。

具有相同名字、不同顺序号的安全策略共同构造一个安全策略组。在一个安全策略组中，顺序号越小的安全策略，优先级越高。

在接口上应用安全策略或安全策略组

在一个接口上应用一个安全策略组，实际上是同时应用了安全策略组中所有的安全策略，从而能够对不同的数据流使用不同的安全联盟，即采用不同的安全策略进行保护。

2.4.4 IKE 的实现过程

IKE 的实现步骤如下：

1. 配置 IKE 协商时的本机 ID

   设置 IKE 协商过程中本端所使用的身份 ID，ID 是区分大小写的。

2. 配置 IKE 安全提议

   确定 IKE 协商过程所使用的验证算法、加密算法、验证方法和 DH 组，同时设置安全联盟的生存周期，如果安全联盟生存时间达到预设置的值，需进行安全联盟的重协商。

3. 配置 IKE 对等体

   设定 IKE 对等体的一系列属性，包括：IKE 协商所使用的版本、IKE 协商使用的 ID 类型、对端的 IP 地址或对端的名称、预共享密钥值、是否需要进行 NAT 穿越，针对 IKEv1，还需配置选用主模式还是野蛮模式进行 IKE 协商。

说明

当上述 IKE 配置完毕后，需要在 IPSec 的安全策略视图下引用 IKE Peer，以完成自动协商的 IPSec 的配置。

2.4.5 IPSec 的 NAT 穿越

NAT 穿越（NAT Traversal）

IPSec 的一个主要应用是建立 VPN，但在实际组网应用中，有一种情况会对部署 IPSec VPN 网络造成障碍：如果发起者位于一个私网内部，远端位于公网侧，而它希望在自己与远端响应者之间直接建立一条 IPSec 隧道，这就涉及到 IPSec 的 NAT 穿越问题，主要问题在于，IKE 在协商过程中如何发现两个端点之间存在 NAT 网关，以及如何使 ESP 报文正常穿越 NAT 网关。

首先，建立 IPSec 隧道的两端需要进行 NAT 穿越能力协商，通过 Vendor ID 载荷指明的一组数据来标识，该载荷数据的定义随所采用 IKE 版本的不同而不同。

而 NAT 网关发现是通过 NAT-D 载荷来实现的，该载荷用于两个目的：在 IKE Peer 之间发现 NAT 的存在；确定 NAT 设备在 Peer 的哪一侧。NAT 侧的 Peer 作为发起者，需要定期发送 NAT-Keepalive 报文，以确保 IPSec 安全流量在 NAT 网关上不被老化删除。

说明

AH 协议对 IP 报文的验证范围涵盖了整个 IP 报文，对 IP 报文头的任何修改将导致 AH 检查失败，因此使用 AH 保护的 IPSec 隧道是不能穿越 NAT 的。ESP 协议支持 NAT 的穿越。

IPSec 穿越 NAT 的处理方法

IPSec 穿越 NAT，简单来说就是在原报文的 IP 头和 ESP 头（不考虑 AH 方式）间增加一个标准的 UDP 报头。这样，当 ESP 报文穿越 NAT 网关时，NAT 对该报文的外层 IP 头和增加的 UDP 报头进行地址和端口号转换；转换后的报文到达 IPSec 隧道对端时，与普通 IPSec 处理方式相同。在发送响应报文时也采用同样的方法。

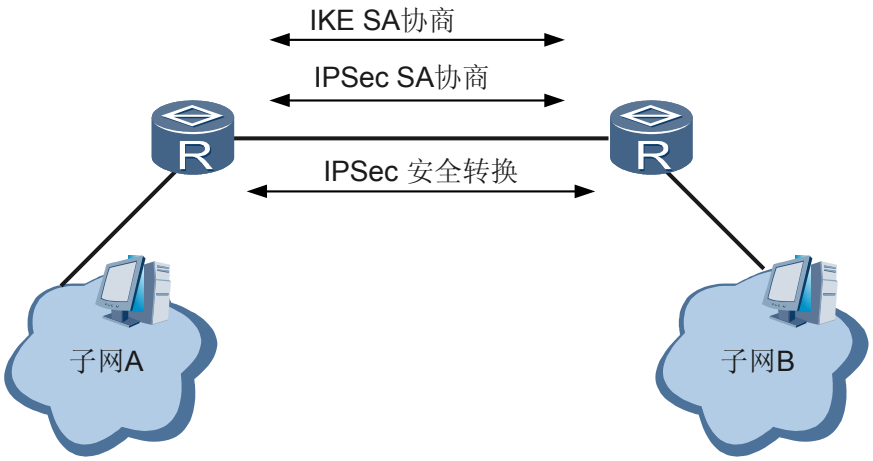
注意

目前 AR 仅支持 IPSec 隧道模式的 NAT 穿越，不支持 IPSec 传输模式的 NAT 穿越。

2.5 应用

2.5.1 站点间安全互联

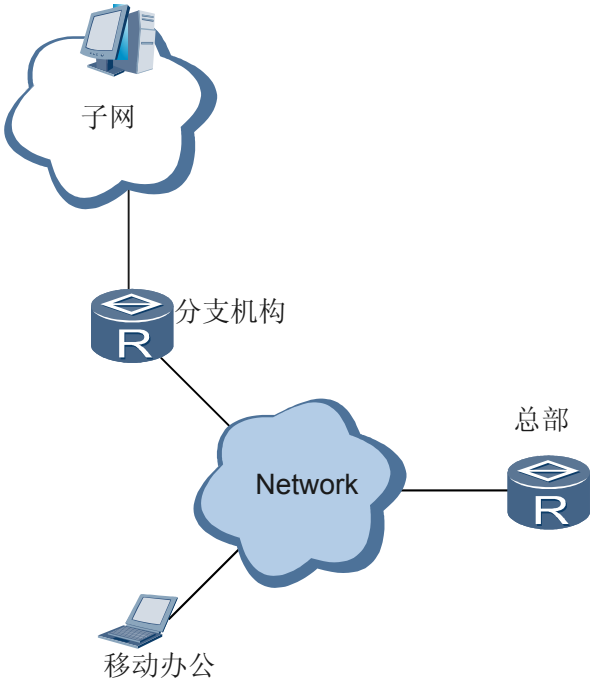
图 2-10 站点间安全互联



如图 2-10 所示，企业站点间部署 IPSec 功能，使用 IPSec 建立安全传输通道。企业站点之间的数据流通过 IPSec 隧道进行安全保护传送。

2.5.2 远程站点与企业总部安全互联

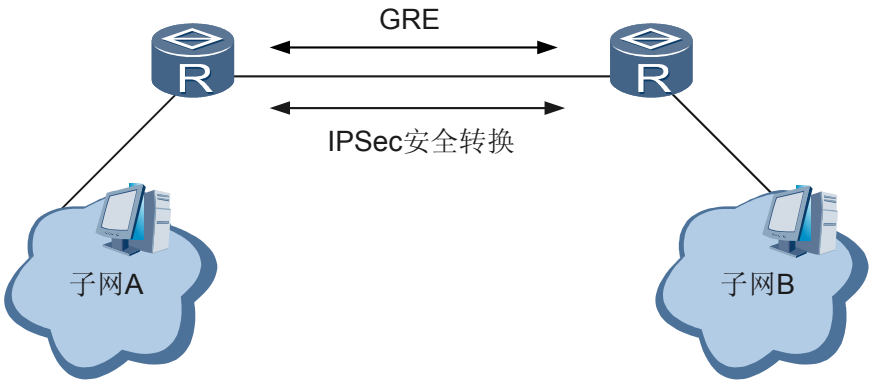
图 2-11 远程站点与企业总部安全互联



如图 2-11 所示，远程分支机构、远程用户通过 IPSec 动态接入企业总部网络。企业总部的 IP 地址是固定的，远端机构或远端 PC 机需预先配置；远程机构或远端 PC 机的 IP 地址可动态获取，总部不需要预先知道。

2.5.3 GRE over IPSec

图 2-12 GRE over IPSec



IPSec 只支持 IP 协议，通过 GRE over IPSec，可以弥补 IPSec 协议的不足。如图 2-12 所示，在 GRE Tunnel 上部署路由协议，在两个 Tunnel 端点，针对 IPSec 服务，仅配置对 GRE 流量的保护。GRE over IPSec 可极大提升组网的灵活性。

2.6 术语与缩略语

缩略语	英文全称	中文全称
IKE	The Internet Key Exchange	Internet 密钥交换
ISAKMP	The Internet Security Association and Key Management Protocol	Internet 安全联盟和密钥管理协议
IPSec	The Internet security protocol	Internet 安全协议
SPI	Security Parameter Index	安全参数索引
AH	Authentication Header	认证报头
ESP	Encapsulating Security Payload	安全有效载荷
SA	Security Association	安全联盟
GRE	Generic Routing Encapsulation	通用路由封装