# IPsec 技术白皮书

# 目录


1 概述 ..... 1

1.1 产生背景 ..... 1

1.2 技术优点 ..... 1

2 技术实现 ..... 1

2.1 IPsec 基本概念 ..... 1

2.1.1 安全联盟 ..... 1

2.1.2 安全协议 ..... 2

2.1.3 安全机制 ..... 3

2.1.4 封装模式 ..... 3

2.2 IKE 协议 ..... 4

2.2.1 IKE 的优点 ..... 4

2.2.2 IPsec 与 IKE 的关系 ..... 5

2.2.3 IKE 的安全机制 ..... 5

2.2.4 IKE 协议版本 ..... 6

2.3 IKEv1 协商建立 IPsec SA ..... 6

2.3.1 基本过程 ..... 6

2.3.2 协商模式 ..... 6

2.3.3 主模式 ..... 6

2.3.4 野蛮模式 ..... 7

2.3.5 国密主模式 ..... 7

2.4 IKEv2 协商建立 IPsec SA ..... 8

2.4.1 IKEv2 的协商过程 ..... 8

2.4.2 IKEv2 引入的新特性 ..... 9

2.5 IPsec 运行机制 ..... 9

2.6 定义保护数据流的方法 ..... 11

2.6.1 ACL 方式 ..... 11

2.6.2 路由方式 ..... 12

3 技术特色 ..... 13

3.1 高效安全的硬件加密引擎 ..... 13

3.2 高安全性的量子加密 ..... 14

3.3 全面支持国密算法 ..... 14

3.4 稳定可靠的智能选路 ..... 14

3.5 自动反向路由注入 ..... 15
3.6 保护 IPv6 路由协议 ..... 16
3.7 保护 SDWAN 报文 ..... 16
3.8 掩码过滤与流量重叠检测 ..... 17
3.9 流量不进行 NAT 转换 ..... 18
3.10 对端地址备份与回切 ..... 19
3.10.1 对端地址备份 ..... 19
3.10.2 对端地址回切 ..... 19
3.11 灵活切换封装协议 ..... 19
3.12 基于 iMC 的 IPsec 统一运维 ..... 19
4 典型组网应用 ..... 20
4.1 局域网安全互联场景 ..... 20
4.2 移动用户远程接入场景 ..... 20
4.3 NAT 穿越场景 ..... 20
4.4 反向路由注入场景 ..... 21
4.5 IPsec 智能选路场景 ..... 21
4.6 总部双链路场景 ..... 22
4.7 VPN 多实例场景 ..... 22
5 参考文献 ..... 23

# 1 概述

## 1.1 产生背景

随着互联网技术的快速发展，越来越多的企业选择通过互联网进行信息交互，但是由于 IP 协议没有足够的安全性保障，且网络中存在大量的安全威胁和数据泄漏风险，无法保证网络传输数据的安全性。为了解决以上问题，IPsec 应运而生。

IPsec（IP Security，IP 安全）是 IETF 制定的三层隧道加密协议，IPsec 协议工作在 IP 层，可以为 IP 网络提供透明的安全服务。IPsec 通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

## 1.2 技术优点

IPsec 具有如下技术优点：

- 数据机密性（Confidentiality）：发送方通过网络传输报文前，IPsec 对报文进行加密，保证数据的机密性，防止数据被恶意窃听。
- 数据完整性（Data Integrity）：接收方对收到的 IPsec 报文的 Hash 值进行检查，从而判断数据在传输过程中是否被篡改。
- 数据来源认证（Data Origin Authentication）：接收方对收到的 IPsec 报文的数字签名进行认证，从而判断报文来源的真实性。
- 所有基于 IP 协议进行传输的数据都可以使用 IPsec 进行保护，而不需要对原始报文进行任何修改。
- IPsec 借助 IKE 协议，可实现密钥的自动协商，简化了 IPsec 的配置。
- IPsec 对数据的加密以数据包为单位，支持抗重放功能，可以有效防范网络攻击。

# 2 技术实现

## 2.1 IPsec基本概念

IPsec 包括如下基本概念：安全联盟、安全协议、安全机制、封装模式。

### 2.1.1 安全联盟

#### 1. SA 简介

SA（Security Association，安全联盟）是 IPsec 的基础，也是 IPsec 的本质。IPsec 在两个端点之间提供安全通信，这类端点被称为 IPsec 对等体。SA 是 IPsec 对等体间对某些要素的约定，例如，使用的安全协议（AH、ESP 或两者结合使用）、协议报文的封装模式（传输模式或隧道模式）、认证算法（HMAC-MD5、HMAC-SHA1、SM3 等）、加密算法（DES、3DES、AES、SM 等）、特定流中保护数据的共享密钥以及密钥的生存时间等。

SA 是单向的，在两个对等体之间的双向通信，最少需要两个 SA 来分别对两个方向的数据流进行安全保护。同时，如果两个对等体希望同时使用 AH 和 ESP 来进行安全通信，则每个对等体都会针对每一种协议来构建一个独立的 SA。

SA 由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址和安全协议号。其中，SPI 是用于标识 SA 的一个 32 比特的数值，它在 AH 和 ESP 头中传输。

#### 2. SA 生成方式

SA 有手工配置和 IKE 自动协商两种生成方式：

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

#### 3. SA 老化机制

手工方式建立的 SA 和 IKE 协商建立的 SA 老化机制不同：

- 手工方式建立的 SA 永不老化。通过 IKE 协商建立的 SA 具有生存时间，当生存时间到达时，旧的 SA 会被删除。
- IKE 协商建立的 SA 在生存时间到达前会提前协商一个新的 SA 来替换旧的 SA。从 SA 建立到启动新 SA 协商的这段时间是软超时时间。缺省情况下，系统会基于 SA 的生存时间使用默认算法计算一个软超时时间。系统允许配置一个软超时缓冲来控制软超时时间，计算公式为：软超时时间=生存时间－软超时缓冲。

IKE 协商建立的 SA 有两种形式的生存时间：

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

可同时存在基于时间和基于流量两种方式的 SA 生存时间，只要其中一种到达，就会删除旧的 SA。

### 2.1.2 安全协议

IPsec 协议不是一个单独的协议，它是 IP 层网络数据安全的一整套安全体系结构，包括安全协议 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）以及用于网络认证及加密的一些算法等。其中，AH 协议和 ESP 协议提供了不同封装方式的安全服务，IKE 协议用于密钥交换。

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

- AH 协议（IP 协议号为 51）定义了 AH 头在 IP 报文中的封装格式，AH 可提供数据来源认证、数据完整性校验和抗重放功能，它能保护报文免受篡改，但不能防止报文被窃听，适合用于传输非机密数据。AH 使用的认证算法有 HMAC-MD5 和 HMAC-SHA1 等。AH 协议不支持 NAT 穿越功能。
- ESP 协议（IP 协议号为 50）定义了 ESP 头和 ESP 尾在 IP 报文中的封装格式，ESP 可提供数据加密、数据来源认证、数据完整性校验和抗重放功能。与 AH 不同的是，ESP 将需要保护的用户数据进行加密后再封装到 IP 包中，以保证数据的机密性。ESP 使用的加密算法有

DES、3DES、AES 等。同时，作为可选项，ESP 还可以提供认证服务，使用的认证算法有 HMAC-MD5 和 HMAC-SHA1 等。虽然 AH 和 ESP 都可以提供认证服务，但是 AH 协议提供的认证范围包括整个 IP 数据包，而 ESP 协议的认证范围仅包括 IP 数据包的载荷部分，因此 AH 提供的认证服务要强于 ESP。

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

### 2.1.3 安全机制

#### 1. 认证算法

IPsec 使用的认证算法主要是通过杂凑函数实现的。杂凑函数是一种能够接受任意长度的消息输入，并产生固定长度输出的算法，该算法的输出称为消息摘要。IPsec 对等体双方都会计算一个摘要，接收方将发送方的摘要与本地的摘要进行比较，如果二者相同，则表示收到的 IPsec 报文是完整未经篡改的，以及发送方身份合法。目前，IPsec 使用基于 HMAC（Hash-based Message Authentication Code，基于散列的消息鉴别码）的认证算法、SM3 认证算法等。HMAC 认证算法包括 HMAC-MD5 和 HMAC-SHA。其中，HMAC-MD5 算法的计算速度快，而 HMAC-SHA 算法的安全强度高。

#### 2. 加密算法

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

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

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

#### 3. 密钥交换算法

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

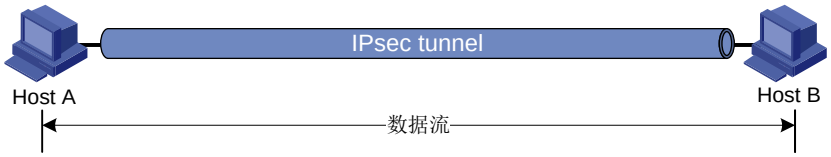
### 2.1.4 封装模式

IPsec 支持两种封装模式：传输模式和隧道模式。

#### 1. 传输模式（Transport Mode）

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

图1 传输模式下的 IPsec 保护




### 2. 隧道模式（Tunnel Mode）

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

图2 隧道模式下的 IPsec 保护


不同的安全协议及组合在隧道和传输模式下的数据封装形式如图 3 所示。

图3 安全协议数据封装格式

| Mode / Protocol | Transport | Tunnel |
|---|---|---|
| AH | IP AH Data | IP AH IP Data |
| ESP | IP ESP Data ESP-T | IP ESP IP Data ESP-T |
| AH-ESP | IP AH ESP Data ESP-T | IP AH ESP IP Data ESP-T |

## 2.2 IKE协议

### 2.2.1 IKE 的优点

用 IPsec 保护一个 IP 数据包之前，必须先建立一个安全联盟（IPsec SA），IPsec SA 可以手工创建或动态建立。IKE 为 IPsec 提供了自动建立 IPsec SA 的服务，具体有以下优点。

- IKE 首先会在通信双方之间协商建立一个安全通道（IKE SA），并在此安全通道的保护下协商建立 IPsec SA，这降低了手工配置的复杂度，简化 IPsec 的配置和维护工作。
- IKE 的精髓在于 DH（Diffie-Hellman）交换技术，它通过一系列的交换，使得通信双方最终计算出共享密钥。在 IKE 的 DH 交换过程中，每次计算和产生的结果都是不相关的。由于每次

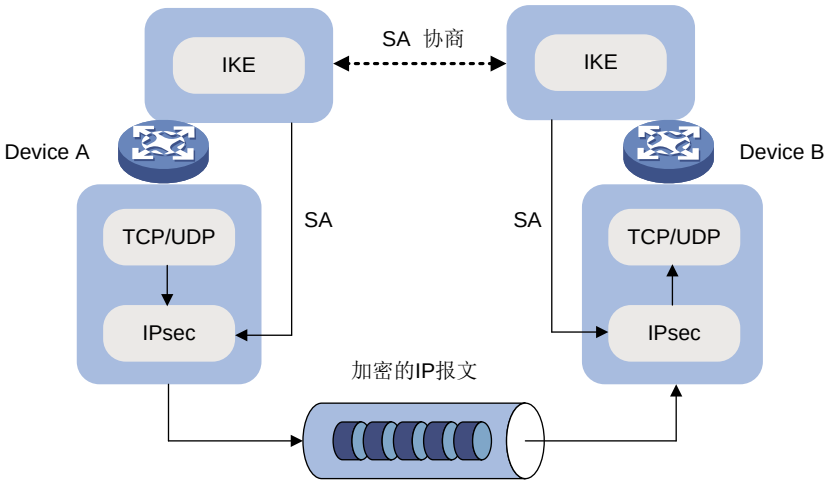
IKE SA 的建立都运行了 DH 交换过程，因此就保证了每个通过 IKE 协商建立的 IPsec SA 所使用的密钥互不相关。

- IPsec 使用 AH 或 ESP 报文头中的顺序号实现防重放。此顺序号是一个 32 比特的值，此数溢出之前，为实现防重放，IPsec SA 需要重新建立，IKE 可以自动重协商 IPsec SA。

### 2.2.2 IPsec 与 IKE 的关系

如图 4 所示，IKE 为 IPsec 协商建立 SA，并把建立的参数交给 IPsec，IPsec 使用 IKE 建立的 SA 对 IP 报文加密或认证处理。

图4 IPsec 与 IKE 的关系图




### 2.2.3 IKE 的安全机制

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

#### 1. 身份认证

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

- 预共享密钥认证：通信双方通过共享的密钥认证对端身份。
- 数字签名认证：通信双方使用由 CA 颁发的数字证书向对端证明自己的身份。

#### 2. DH 算法

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

#### 3. PFS 特性

PFS（Perfect Forward Secrecy，完善的前向安全性）是一种安全特性，它解决了密钥之间相互无关性的需求。由于 IKE 第二阶段协商需要从第一阶段协商出的密钥材料中衍生出用于 IPsec SA 的密钥，若攻击者能够破解 IKE SA 的一个密钥，则会非常容易得掌握其衍生出的任何 IPsec SA 的密

钥。使用 PFS 特性后，IKE 第二阶段协商过程中会增加一次 DH 交换，使得 IKE SA 的密钥和 IPsec SA 的密钥之间没有派生关系，即使 IKE SA 的其中一个密钥被破解，也不会影响它协商出的其它密钥的安全性。

### 2.2.4 IKE 协议版本

#### 1. IKEv1

IKEv1（Internet Key Exchange Version 1，互联网密钥交换协议第 1 版）协议利用 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）语言定义密钥交换的过程，是一种对安全服务进行协商的手段。

#### 2. IKEv2

IKEv2（Internet Key Exchange Version 2，互联网密钥交换协议第 2 版）是第 1 版本的 IKE 协议（本文简称 IKEv1）的增强版本。IKEv2 与 IKEv1 相同，具有一套自保护机制，可以在不安全的网络上安全地进行身份认证、密钥分发、建立 IPsec SA。

#### 3. IKEv2 和 IKEv1 的区别

相对于 IKEv1，IKEv2 需要交互的报文数量较少，且 IKEv2 具有更强的抗攻击能力和密钥交换能力。

## 2.3 IKEv1协商建立IPsec SA

### 2.3.1 基本过程

IKEv1 使用了两个阶段为 IPsec 进行密钥协商以及建立 SA：

(1) 第一阶段，通信双方彼此间建立了一个已通过双方身份认证和对通信数据安全保护的通道，即建立一个 IKEv1 SA（本文中提到的 IKEv1 SA 都是指第一阶段 SA）。

(2) 第二阶段，用在第一阶段建立的 IKEv1 SA 为 IPsec 协商安全服务，即为 IPsec 协商 IPsec SA，建立用于最终的 IP 数据安全传输的 IPsec SA。

### 2.3.2 协商模式

第一阶段的 IKEv1 协商模式包括如下三种方式：

- 主模式（Main Mode）
- 野蛮模式（Aggressive Mode）
- 国密主模式（GM-Main Mode）

### 2.3.3 主模式

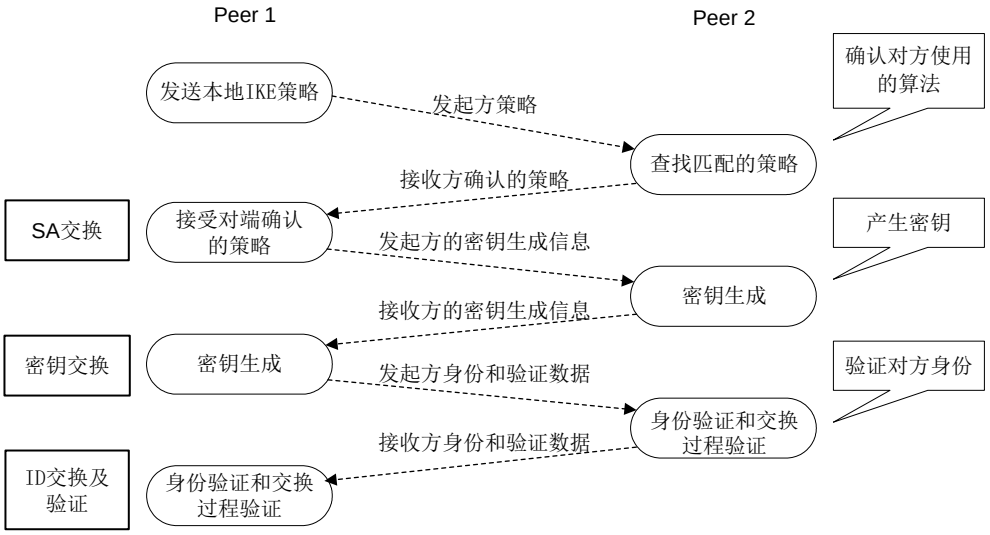
如图 5 所示，第一阶段主模式的 IKEv1 协商过程中包含三对消息，具体内容如下：

(1) 第一对消息完成了 SA 交换，它是一个协商确认双方 IKEv1 安全策略的过程；

(2) 第二对消息完成了密钥交换，通过交换 Diffie-Hellman 公共值和辅助数据（如：随机数），最终双方计算生成一系列共享密钥（例如，认证密钥、加密密钥以及用于生成 IPsec 密钥参数的密钥材料），并使其中的加密密钥和认证密钥对后续的 IKEv1 消息提供安全保障；

(3) 第三对消息完成了 ID 信息和验证数据的交换，并进行双方身份的认证。

图5 主模式协商过程




### 2.3.4 野蛮模式

如图 6 所示，第一阶段野蛮模式的 IKEv1 协商过程中包含三条消息，具体内容如下：

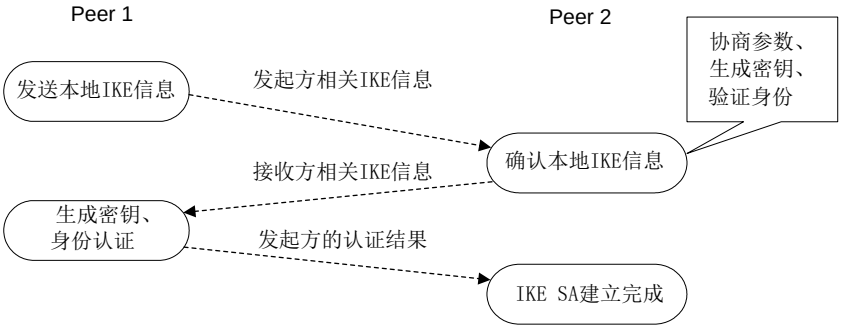
(1) 发起方通过第一条消息发送本地 IKEv1 信息，包括建立 IKEv1 SA 所使用的参数、与密钥生成相关的信息和身份验证信息。

(2) 接收方通过第二条消息对收到的第一个消息进行确认，查找并返回匹配的参数、密钥生成信息和身份验证信息。

(3) 发起方通过第三条消息回应验证结果，并成功建立 IKEv1 SA。

与主模式相比，野蛮模式的优点是建立 IKEv1 SA 的速度较快。但是由于野蛮模式的密钥交换与身份认证一起进行，因此无法提供身份保护。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。

图6 野蛮模式协商过程




### 2.3.5 国密主模式

国密主模式与主模式协商过程类似，不再赘述。

本端的协商模式配置为国密主模式，必须使用 RSA-DE 或者 SM2-DE 数字信封方式进行身份认证。

## 2.4 IKEv2协商建立IPsec SA

### 2.4.1 IKEv2 的协商过程

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

IKEv2 协商包括三种交互过程：

- 初始交换：通过四条消息协商出 IKEv2 SA 和 IPsec SA。
- 创建子 SA 交换：当一个 IKEv2 SA 需要创建多个 IPsec SA 时，使用创建子 SA 交换来协商多于一个的 IPsec SA，另外还可用于进行 IKEv2 SA 的重协商功能。
- 通知交换：用于传递控制信息，例如错误信息或通告信息。

下面简单介绍一下 IKEv2 协商过程中的初始交换过程。

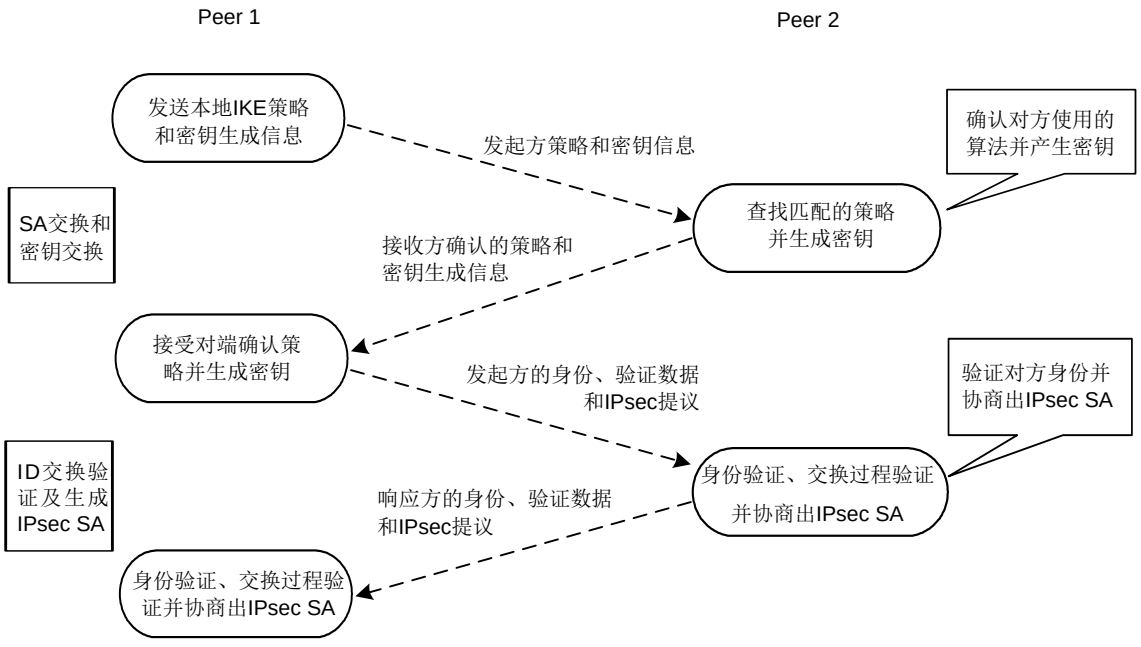
如图 7 所示，IKEv2 的初始交换过程包含四条消息。

(1) 第一对消息：完成 IKEv2 SA 参数的协商以及密钥交换；

(2) 第二对消息：完成通信对等体的身份认证以及 IPsec SA 的创建。

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

图7 IKEv2 的初始交换过程



### 2.4.2 IKEv2 引入的新特性

#### 1. IKEv2 支持 DH 猜想

在 IKEv2 初始交换阶段，发起方采用“猜”的办法，猜一个响应方最可能使用的 DH 组，携带在第一条消息中发送。响应方根据发起方“猜”的 DH 组来响应发起方。如果发起方猜测成功，则这样通过两条消息就可以完成 IKEv2 初始交换。如果发起方猜测错误，则响应方会回应一个 INVALID_KE_PAYLOAD 消息，并在该消息中指明将要使用的 DH 组。之后，发起方采用响应方指定的 DH 组重新发起协商。

这种 DH 猜想机制，使得发起方的 DH 组配置更为灵活，可适应不同的响应方。

#### 2. IKEv2 支持 Cookie-challenge 机制

在 IKEv2 初始交换中的 IKE_INIT_SA 消息是明文传输的，因此该消息有可能被篡改仿冒，响应方接收到第一个消息后无法确认该消息是否来自一个仿冒的地址。如果此时一个网络攻击者伪造大量地址向响应方发送 IKEv2 初始交换请求，根据 IKEv1 协议，响应方需要维护这些半连接状态的 IKE 会话信息，从而耗费响应方大量的系统资源，造成对响应方的 DoS 攻击。

IKEv2 使用 Cookie-challenge 机制来解决这类 DoS 攻击问题。当响应方发现存在的半连接状态的 IKEv2 SA 超过指定的数目时，就会启用 Cookie-challenge 机制。响应方收到 IKEv2 初始连接请求后，构造一个 Cookie 通知载荷并发送给发起方，若发起方能够正确携带收到的 Cookie 通知载荷向响应方重新发起 IKEv2 初始交换请求，则可以继续后续的协商过程。

半连接状态的 IKEv2 SA 是指那些正在协商过程中的 IKEv2 SA。若半连接状态的 IKEv2 SA 数目减少至阈值以下，则 Cookie-challenge 功能将会停止工作。

#### 3. IKEv2 SA 重协商

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

#### 4. IKEv2 报文确认重传机制

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

## 2.5 IPsec运行机制

如图 8 所示，IPsec 基本运行机制如下：

(1) 定义需要 IPsec 保护的数据流，可以通过配置路由或 ACL 规则来实现，具体请参加定义保护数据流的方法。

(2) 通信两端通过如下方式确认数据保护及认证策略（主要包括安全协议、认证算法、加密算法、共享密钥以及密钥的生存时间等），并建立 IPsec 隧道：

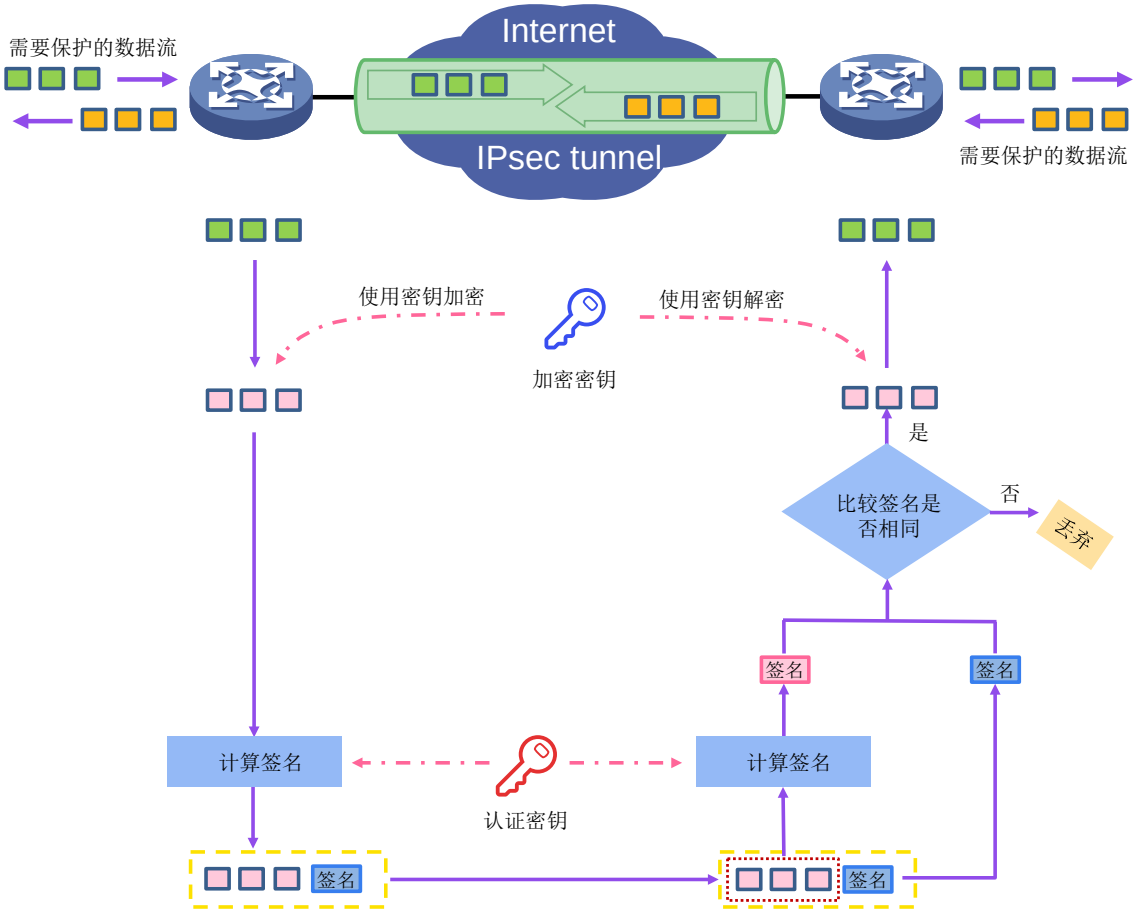
- 静态手工方式：通过手工方式配置 IPsec 隧道的所有信息，配置完成后，隧道即建立。

- IKEv1 自动协商方式：通过 IKEv1 动态协商 IPsec 策略，完成 IKEv1 配置后，由发送的数据流触发建立隧道。
- IKEv2 自动协商方式：通过 IKEv2 动态协商 IPsec 策略，完成 IKEv2 配置后，由发送的数据流触发建立隧道。
- 量子加密方式：通过从量子密钥服务器获取的量子密钥自动协商建立隧道，配置完成后，由发送的数据流触发建立隧道。
- GDOI（Group Domain Virtual Private Network，组域虚拟专用网络）方式：提供了一种基于组的 IPsec 安全模型，属于同一个组的所有成员共享相同的保护策略及密钥，管理复杂度降低，可扩展性更高。
- SDWAN（Software Defined Wide Area Network，软件定义广域网）方式：SDWAN 方式的 IPsec 安全框架，用于在 SDWAN 设备上生成 IPsec SA。该类型的 IPsec 安全框架不限制对端 IP 地址，不需要进行 ACL 配置，即所有路由到 SDWAN 接口的流量都会被 IPsec 保护，配置简单，易于维护。

(3) IPsec 发送方使用加密算法和密钥对需要保护的报文进行加密，加密后的报文通过认证算法和认证密钥生成签名，封装在报文中进行发送。

(4) 响应方通过相同的认证算法和认证密钥，对收到的加密报文重新生成新的签名，然后再与报文中的签名进行对比，若签名不相同则认为报文非法，丢弃该报文；若签名相同则认为报文合法。合法的报文通过解密算法和密钥进行解密，最终响应方得到原始报文。

图8 IPsec 运行机制示意图




## 2.6 定义保护数据流的方法

IPsec 只对特定的数据流进行保护，至于什么样的数据是需要 IPsec 保护的，可以通过以下两种方式定义。

- ACL 方式：通过 ACL 规则筛选需要 IPsec 保护的数据流，匹配 ACL permit 规则的报文将受到 IPsec 保护，未匹配任何 permit 规则的报文将不受 IPsec 保护。该方式可以利用 ACL 丰富的功能，灵活的指定 IPsec 保护报文的方法。
- 路由方式：通过在 Tunnel 隧道接口上创建 IPsec 隧道，路由到 Tunnel 隧道接口上的报文都将受到 IPsec 保护，除非用户指定该报文不需要被 IPsec 保护。该方式可以简化 IPsec 配置的复杂度，同时支持动态路由协议、以及对组播流量进行保护。

### 2.6.1 ACL 方式

将引用了 ACL 的 IPsec 安全策略应用到接口上后，该接口上匹配 ACL 的报文将会受到 IPsec 保护。这里的接口包括以太网接口等实际物理接口，以及 Tunnel、Virtual Template 等虚接口。

具体的保护机制如下：

- 只要接口发送的报文与该接口上应用的 IPsec 安全策略中的 ACL 的 **`permit`** 规则匹配，就会受到出方向 IPsec SA 的保护并进行封装处理。

- 接口接收到目的地址是本机的 IPsec 报文时，首先根据报文头里携带的 SPI 查找本地的入方向 IPsec SA，由对应的入方向 IPsec SA 进行解封装处理。缺省情况下，解封装后的 IP 报文只有与 ACL 的 **permit** 规则匹配才会采取后续处理，否则被丢弃。若关闭解封装后 IPsec 报文的 ACL 检查功能，则解封装后的 IP 报文与 ACL 的 **permit** 规则不匹配时，该报文不会被丢弃。

目前，设备支持的数据流的保护方式包括以下三种：

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

### 2.6.2 路由方式

在隧道接口上应用 IPsec 安全框架后，路由到该隧道接口的报文都会受到 IPsec 的保护，除非用户指定该报文不需要被 IPsec 保护。此方式建立的 IPsec 的封装模式必须为隧道模式。该类应用通常也被称为在 VTI（Virtual Tunnel Interface）上应用 IPsec。

相比于保护匹配 ACL 的报文，保护隧道接口上报文的 IPsec 有以下优势：

- 支持保护组播报文。
- 支持动态路由协议在 IPsec 隧道两端的传播。
- 简化配置。不需要通过 ACL 规则对流量进行筛选，路由表会将流量引导到隧道口上。

隧道接口对报文的封装/解封装发生在隧道接口上。进入设备的报文被路由到应用了 IPsec 安全框架的隧道接口后，此隧道接口会对这些报文进行封装/解封装处理。如图 9 所示，隧道接口对报文进行封装的过程如下：

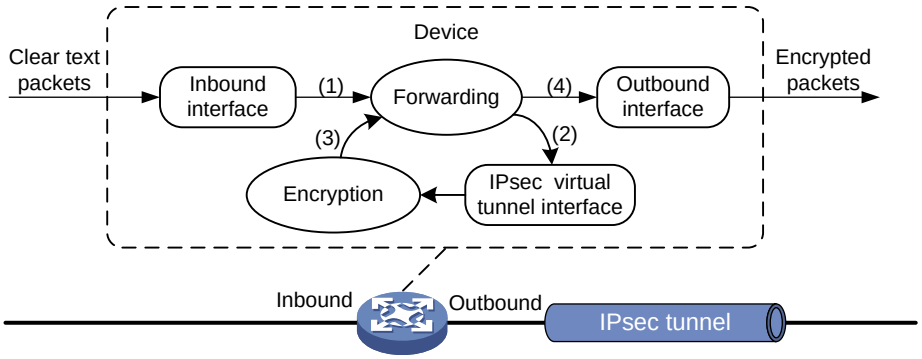
(1) Device 将从入接口接收到的 IP 明文送到转发模块进行路由处理；

(2) 转发模块依据路由查询结果，将 IP 明文发送到隧道接口进行封装：原始 IP 报文加密后被封装在一个新的 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端地址和目的端地址。

(3) 隧道接口完成对 IP 明文的封装处理后，将 IP 密文再次送到转发模块进行路由处理；

(4) 转发模块根据新 IP 头中的目的 IP 地址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。

图9 隧道接口封装报文原理图




如图 10 所示，隧道接口对报文进行解封装的过程如下：

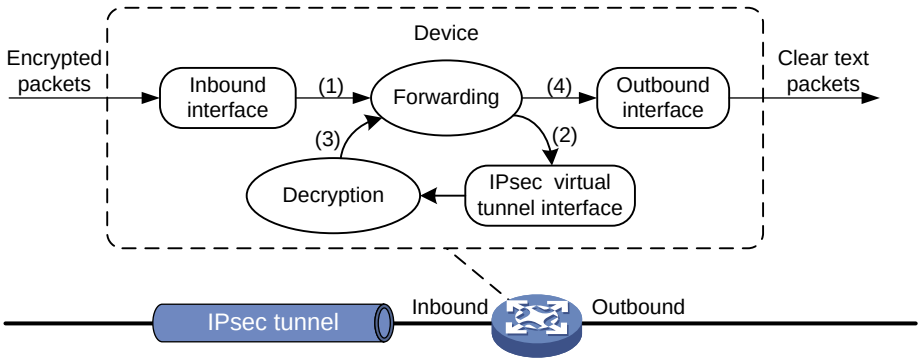
(1) Device 将从入接口接收到的 IP 密文送到转发模块进行路由处理；

(2) 转发模块识别到此IP密文的目的IP地址为本设备隧道接口源端地址且IP协议号为AH或ESP时，会将 IP 密文送到相应的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) 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进行路由处理；

(4) 转发模块根据 IP 明文的目的 IP 地址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。

图10 隧道接口解封装报文原理图




# 3 技术特色

## 3.1 高效安全的硬件加密引擎

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

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

## 3.2 高安全性的量子加密

开启国盾量子加密功能后，IPsec 将使用国盾量子服务器提供的对称密钥，对需要 IPsec 保护的数据进行加密保护，进一步提升 IPsec 业务的安全性。

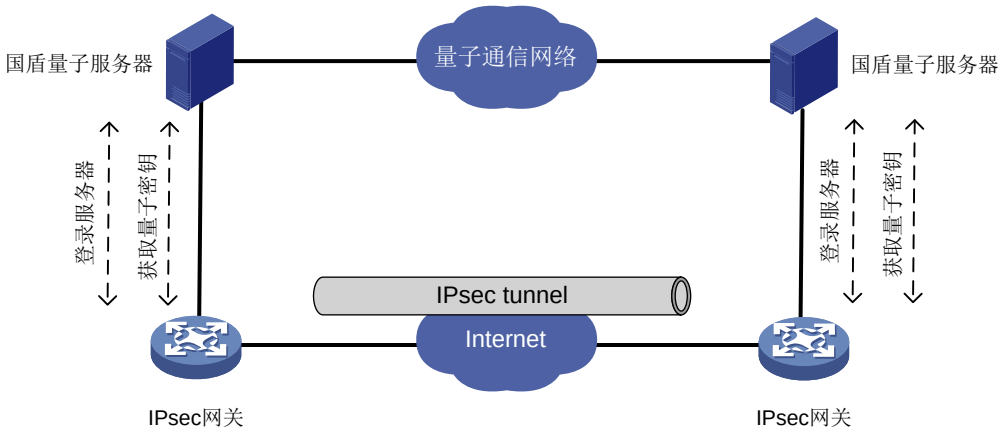
设备从国盾量子服务器获取密钥的过程如下：

(1) 连接国盾量子服务器：国盾量子加密功能的相关配置完成后，设备将与指定的国盾量子服务器建立连接。

(2) 登录国盾量子服务器：建立连接后，设备将向国盾量子服务器发送登录请求，并携带唯一入网标识和身份认证密钥，只有上述参数验证无误后，才能成功登录国盾量子服务器。

(3) 获取国盾量子密钥：登录成功后，设备将在 IKE 一阶段协商完成后，向国盾量子服务器获取经过加密的量子密钥，然后再通过设备上配置的解密密钥进行解密，最终得到供 IPsec 使用的量子密钥。

**图11 国盾量子加密功能示意图**




## 3.3 全面支持国密算法

IPsec 已全面支持国密算法，包括 SM1、SM2、SM3 和 SM4，能够满足国密部署场景的要求。

## 3.4 稳定可靠的智能选路

为了提高网络的稳定性和可靠性，企业通常会在网络出口配置多条链路。不同链路之间存在通信质量差异，实时状态也不尽相同，选择一条高质量的链路对于企业通信来说尤为重要。IPsec 智能选路功能（IPsec Smart Link）在有多条可使用的链路能够到达目的网络的情况下，实时地自动探测链路的时延、丢包率，动态切换到满足通信质量要求的链路上建立 IPsec 隧道。用户也可以根据自己的实际需求手工指定使用的链路。

IPsec 智能选路可以很好地解决以下问题：

- 网络出口多链路进行流量负载分担时，可能会出现一部分链路拥塞、另一部分链路闲置的情况；
- 用户无法基于链路传输质量或者服务费用自己选择链路；

- 当网络出口设备与目的设备之间的链路出现故障时，如果流量被转发到该故障链路上，会造成访问失败。

IPsec 智能选路的过程如下：

(1) 设备根据配置的 IPsec 智能选路策略探测周期定时发送探测报文获取当前使用链路的丢包率和时延。

(2) 当探测结果超过管理员设置的阈值时，设备会根据 IPsec 智能选路链路的优先级顺序从高到低循环切换，从中选择第一条符合质量要求的链路，建立一个相应的 IPsec 隧道，进行数据传输。如果链路都不符合质量要求，且循环次数达到配置的上限值后：

  - 丢包率和延迟存在差异的情况下选择相对最优的链路。
  - 如果丢包率和延迟都一样，则选择优先级最低的链路，等待 10 分钟后再重新探测。

## 3.5 自动反向路由注入

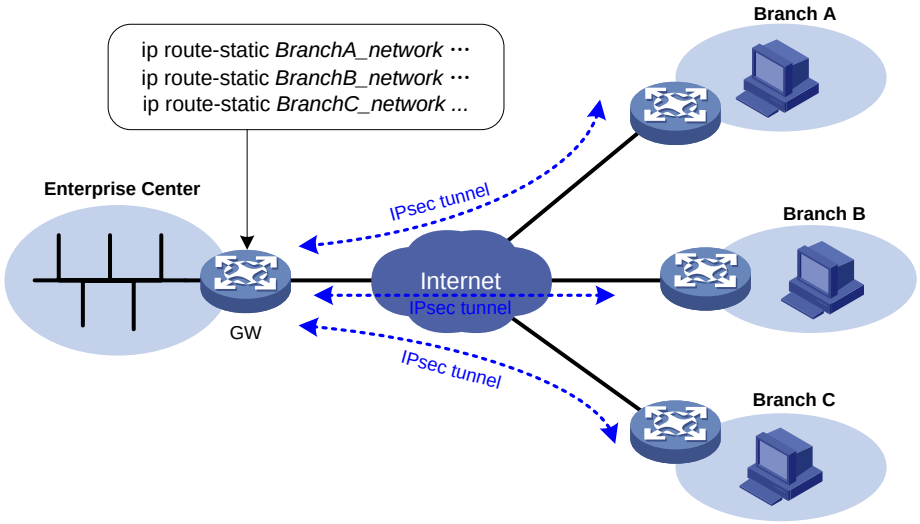
RRI（Reverse Route Injection，反向路由注入）功能是一种自动添加到达 IPsec VPN 私网静态路由的机制，可以实现为受 IPsec 保护的流量自动添加静态路由的功能。在大规模组网中，这种自动添加静态路由的机制可以简化用户配置，减少在企业总部网关设备上配置静态路由的工作量，并且可以根据 IPsec SA 的创建和删除进行静态路由的动态增加和删除，增强了 IPsec VPN 的可扩展性。

如图 12 所示，某企业在企业分支与企业总部之间的所有流量通过 IPsec 进行保护，企业总部网关上需要配置静态路由，将总部发往分支的数据引到应用 IPsec 安全策略的接口上来。如果未配置 RRI，当企业分支众多或者内部网络规划发生变化时，就需要同时增加或调整总部网关上的静态路由配置，该项工作量大且容易出现配置错误。

企业总部侧网关设备 GW 上配置 RRI 功能后，每一个 IPsec 隧道建立之后，GW 都会自动为其添加一条相应的静态路由。通过 RRI 创建的路由表项可以在路由表中查询到，其目的地址为受保护的对端网络，下一跳地址为 IPsec 隧道的对端地址或指定的地址，它使得发往对端的流量被强制通过 IPsec 保护并转发。

RRI 创建的静态路由和手工配置的静态路由一样，可以向内网设备进行广播，允许内网设备选择合适的路由对 IPsec VPN 流量进行转发。也可以为 RRI 创建的静态路由配置优先级，从而更灵活地应用路由管理策略。例如：当设备上还有其他方式配置到达相同目的地的路由时，如果为它们指定相同的优先级，则可实现负载分担，如果指定不同的优先级，则可实现路由备份。同时，还可以通过修改静态路由的 Tag 值，使得设备能够在路由策略中根据 Tag 值对这些 RRI 生成的静态路由进行灵活的控制。

图12 IPsec VPN 总部-分支组网图




## 3.6 保护IPv6路由协议

将 IPsec 安全框架应用到某一 IPv6 路由协议（目前支持保护 OSPFv3、IPv6 BGP、RIPng 路由协议）后，设备产生的需要 IPsec 保护的某一 IPv6 路由协议的所有报文都要进行封装处理，而设备接收到的不受 IPsec 保护的以及解封装失败的业务协议报文都要被丢弃。

由于 IPsec 的密钥交换机制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，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），因此该方式下必须手工配置用来保护 IPv6 路由协议报文的 IPsec SA。

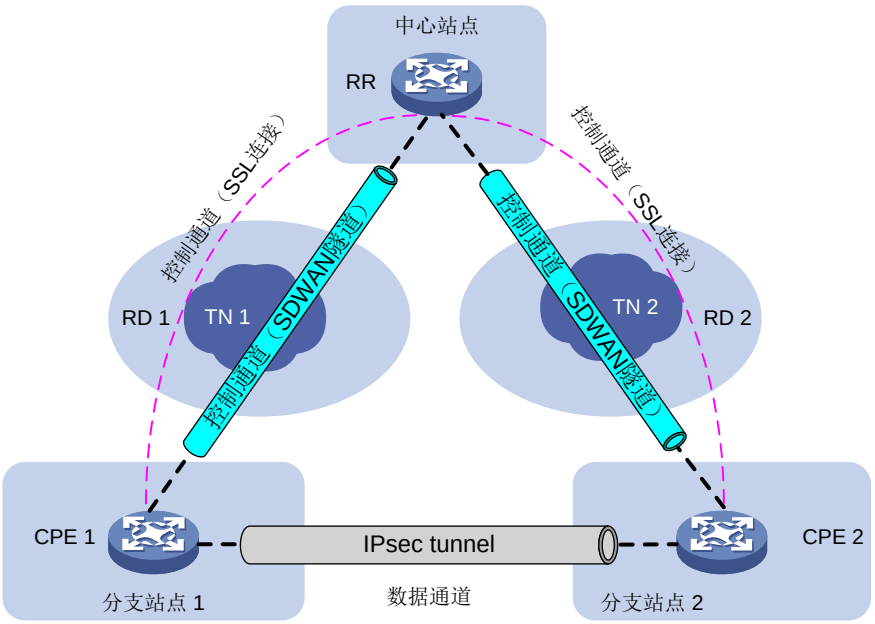
## 3.7 保护SDWAN报文

### 1. SDWAN 简介

SDWAN（Software Defined Wide Area Network，软件定义广域网）是将 SDN 技术应用到广域网的一种 VPN 技术。控制平面通过标准的 MP-BGP 通告 TTE（Transport Tunnel Endpoint，传输隧道端点）信息和 EVPN 路由信息，实现不同站点之间的 MAC 地址、IP 地址的学习和发布；数据平面采用 UDP 封装转发数据报文且能保障数据快速安全传输，为分散在广阔地理范围内的企业网络、数据中心等提供安全可靠的互联服务。

### 2. SDWAN 网络模型

图13 SDWAN 网络模型示意图




如图 13 所示，SDWAN 网络由控制通道和数据通道组成。CPE 各自生成 IPsec SA，并通过与 RR 的控制通道传递给其他 CPE。当 CPE 之间的数据通道有数据需要传输时，CPE 将使用 IPsec SA 对 CPE 之间传输的数据进行 IPsec 加密保护。

例如，当 CPE1 向 CPE2 发送报文时，CPE1 将使用 CPE2 的 IPsec SA 对报文进行加密后，发送给 CPE2，CPE2 收到报文后，使用自己的 IPsec SA 进行解密，并对目的地址为本机但未加密的报文进行丢弃。反之，CPE2 向 CPE1 发送报文时，CPE2 将使用 CPE1 的 IPsec SA 进行加密后，发送给 CPE1，CPE1 收到报文后，使用自己的 IPsec SA 进行解密，并对目的地址为本机但未加密的报文进行丢弃。

由于 IPsec SA 是单向的，设备加密和解密采用不同的 IPsec SA。通常情况下，本端 IPsec SA 仅用于解密，对端 IPsec SA 仅用于加密。

## 3.8 掩码过滤与流量重叠检测

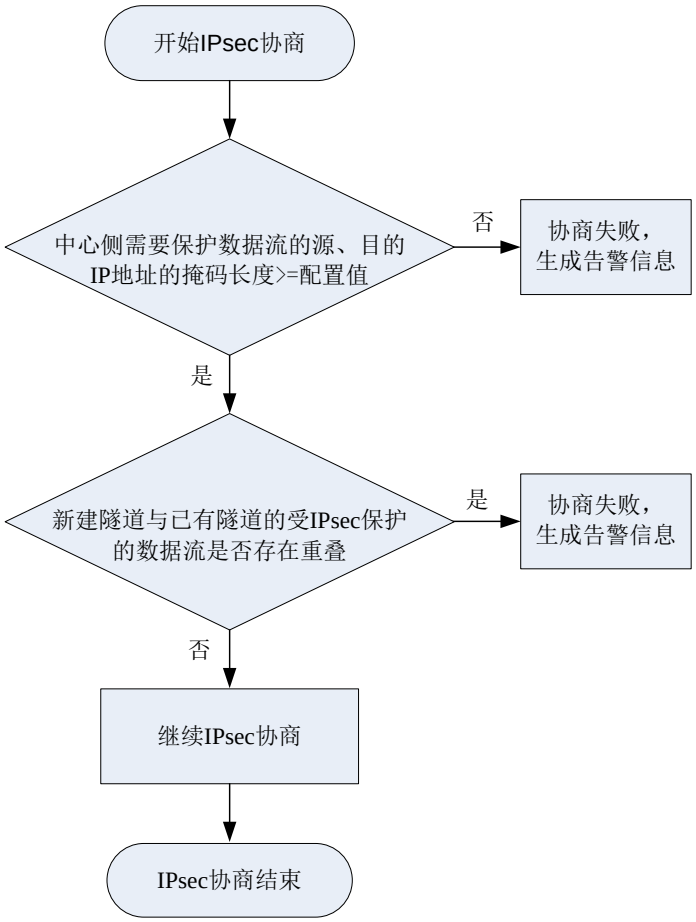
在中心-分支组网环境中，当有新的分支加入组网时，如果新分支侧配置的保护数据流范围与其他分支相比范围过大，可能会导致其他分支的流量被引入到该分支，导致报文转发错误。

在中心侧配置掩码过滤功能后，当中心侧设备与分支侧设备进行 IPsec 隧道协商时，如果中心侧需要保护数据流的源和目的 IP 地址的掩码长度大于或等于本功能配置的值，则允许继续协商；否则，IPsec 隧道协商失败，设备将生成掩码过滤失败的告警信息，提示用户当前需要保护数据流的掩码设置过小。当 IPsec 隧道协商失败时，管理员需要针对当前组网环境，重新规划分支侧的 ACL 配置。例如，分支 A 和分支 B 分别与总部进行 IPsec 协商，分支 A 配置的 ACL 规则中的 source 为 192.168.1.0/24，分支 B 配置的 ACL 规则中的 source 为 192.168.0.0/8。则匹配分支 A 的流量同时也匹配分支 B，由于设备匹配 ACL 规则时为顺序匹配，因此可能会导致本该发往分支 A 的流量发往分支 B。

为了进一步防止受 IPsec 保护的数据流发生重叠，设备会检测新建隧道与已有隧道的受 IPsec 保护的数据流是否存在重叠。若重叠，则 IPsec 隧道协商失败，设备将生成 IPsec 流量重叠检测失败的告警信息，提示用户当前需要保护的数据流存在流量重叠。当 IPsec 隧道协商失败时，管理员需要针对当前组网环境，重新规划分支侧的 ACL 配置。

中心侧设备判断是否存在 IPsec 流量重叠的方法为：检测待保护数据流的目的 IP 地址范围是否与已有隧道保护的数据流的目的 IP 地址范围重叠。若重叠，则认为待保护的数据流与已有隧道保护的数据流发生了重叠。IPsec 隧道协商过程中的掩码过滤和流重叠检测流程如图 14 所示。

**图14 IPsec 掩码过滤和流量重叠检测流程图**




## 3.9 流量不进行NAT转换

缺省情况下，在一个接口上同时配置了 IPsec 与 NAT 的情况下，对于出方向报文，设备先进行 NAT 转换，再进行 IPsec 处理。若需要进行 IPsec 处理的流量进行了 NAT 转换，那么该流量将无法匹配 ACL 规则，从而导致该流量不能按照预期进行 IPsec 处理。此时，必须通过相关的配置对需要 NAT 转换的流量和需要 IPsec 处理的流量进行准确的区分。而准确的区分可能导致配置复杂，难以维护。

开启流量不进行 NAT 转换功能后，当前接口上需要进行 IPsec 处理的流量将不会进行 NAT 转换，减轻划分 NAT 与 IPsec 流量的工作量，进而降低接口上 IPsec 与 NAT 共存时配置的复杂度。

## 3.10 对端地址备份与回切

### 3.10.1 对端地址备份

为了保障业务的稳定性，企业总部的 IPsec 网关配置了多条链路进行冗余备份。企业分支的 IPsec 网关上需要配置对端地址备份功能，当企业总部的某条链路不可用时，企业分支尝试向企业总部的其他备份地址发起协商，建立 IPsec 隧道。

IPsec 支持指定多个对端 IP 地址，形成对端 IP 地址列表。建立 IPsec 隧道时，本端依次按配置顺序向列表中的 IP 地址发起 IPsec 协商：协商成功，则与该地址建立 IPsec 隧道；否则尝试向列表中的下一个 IP 地址建立 IPsec 隧道，直至列表中最后一个 IP 地址。IPsec 同时支持指定首选地址，即该地址拥有最高优先级，每次触发协商时都会优先向该地址发起协商，每个地址列表中最多可配置一个首选地址。

若该首选地址协商失败，则尝试向 IP 地址列表中的下一个 IP 地址发起协商，直到 IP 地址列表中的最后一个 IP 地址。

### 3.10.2 对端地址回切

IPsec 对端地址关联 Track 项之后，能够实现对对端地址状态的探测。当探测到首选地址或备份地址不可用时，设备会立即选择其他备份地址建立 IPsec 隧道。如果同时打开了对端地址回切功能，在首选地址恢复到可用状态时，设备将重新与首选地址建立 IPsec 隧道。如果没有打开对端地址回切功能，在首选地址恢复到可用状态时，设备不会重新与首选地址建立 IPsec 隧道。

## 3.11 灵活切换封装协议

IPsec 报文支持两种传输层协议封装，即 UDP 协议和 TCP 协议。

缺省情况下，IPsec 报文使用 UDP 协议进行封装，在网络中传输。当网络中存在阻止或限制 UDP 报文的情况时，可以将 IPsec 报文封装成 TCP 报文进行传输，从而摆脱此限制。

## 3.12 基于iMC的IPsec统一运维

IPsec VPN 是公认的理想 VPN 解决方案之一，但是依然面临如下难题：

- IPsec VPN 技术复杂，配置命令多，如何快速完成业务规划部署；
- 如何监控 IPsec VPN 网络的运行状态；
- 如何监控用户租用 VPN 的性能；
- 如何快速定位 IPsec VPN 设备的故障。

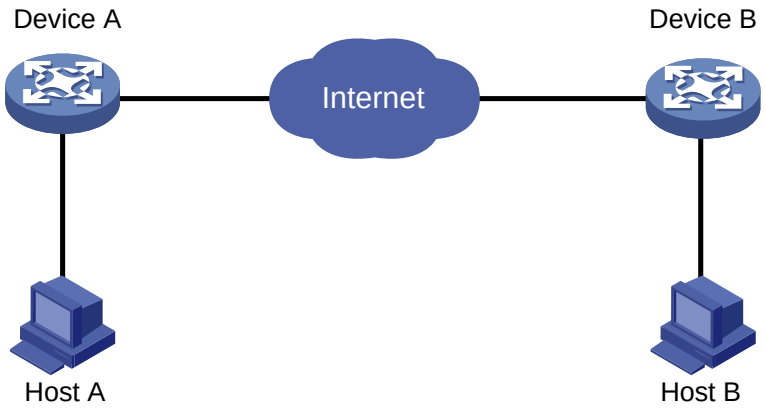
基于 iMC 系统的 VPN 解决方案可以解决上述问题。用户可以通过 iMC iVM 系统有效地监控 VPN 网络的运行状况，并查看租用 VPN 的性能，方便用户在 VPN 上开展各项业务。通过该系统还可以快速定位设备故障，对 VPN 设备进行管理和维护。

# 4 典型组网应用

## 4.1 局域网安全互联场景

如图 15 所示，在两个局域网网关之间建立一条 IPsec 隧道，可以实现对局域网之间传输的数据进行安全保护。

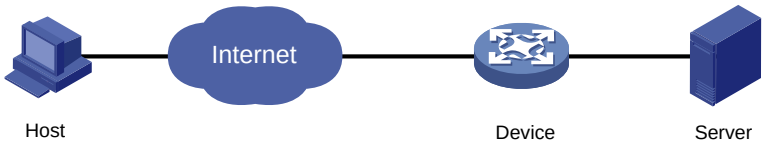
图15 局域网安全互联场景配置组网图




## 4.2 移动用户远程接入场景

如图 16 所示，在移动用户远程接入企业内网场景中，可以在用户主机和企业网关之间建立一条 IPsec 隧道，对用户主机和企业内网服务器之间的数据流进行安全保护。

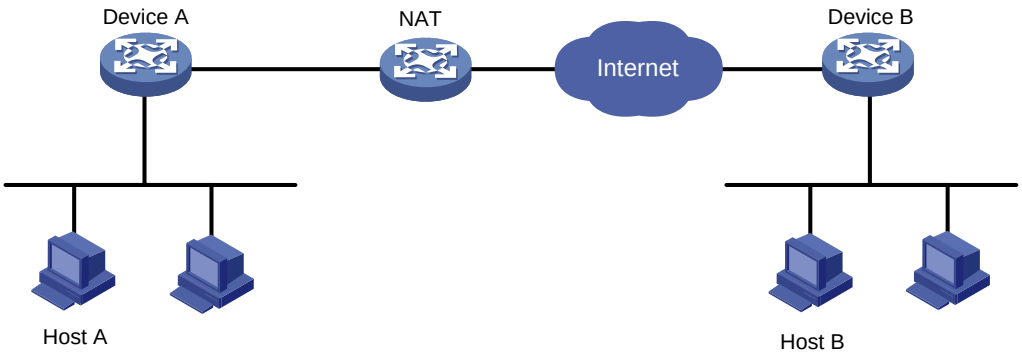
图16 移动用户远程接入场景配置组网图




## 4.3 NAT穿越场景

如图 17 所示，在两个局域网网关之间建立一条 IPsec 隧道，若网关之间存在 NAT 设备，IPsec 支持 NAT 穿越功能，从而实现对局域网之间传输的数据进行安全保护。

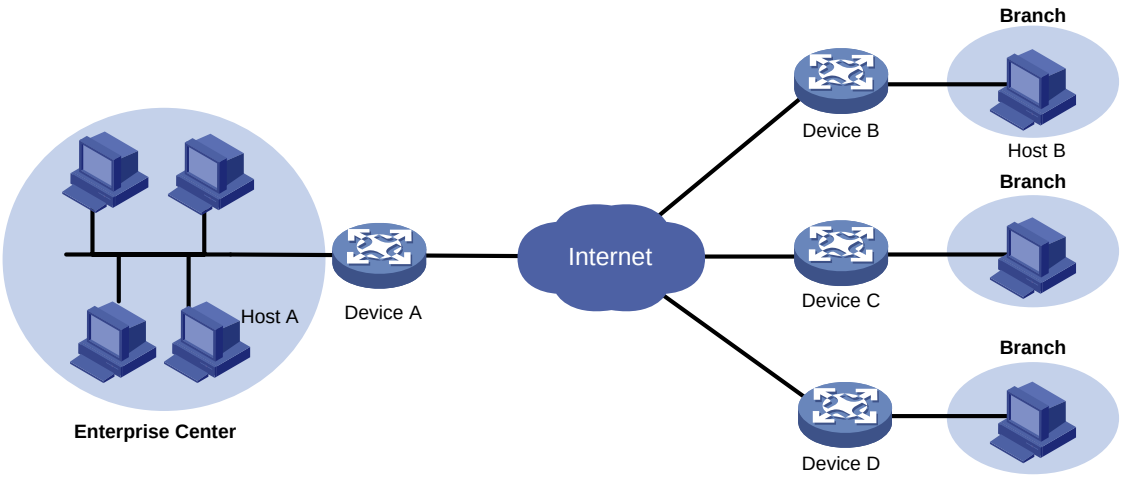
图17 NAT 穿越场景配置组网图




## 4.4 反向路由注入场景

如图 18 所示，企业分支通过 IPsec VPN 接入企业总部，在企业总部网关上开启 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。

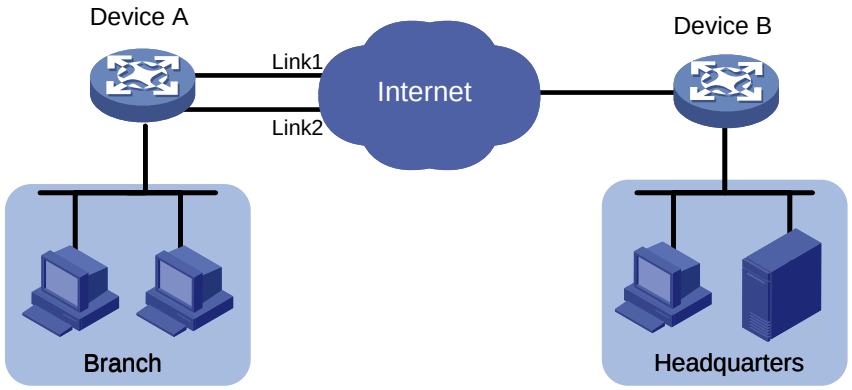
图18 反向路由注入场景配置组网图




## 4.5 IPsec智能选路场景

如图 19 所示，企业分支使用 IPsec VPN 接入企业总部，通过在分支上配置 IPsec 智能选路功能，实现 IPsec 隧道在两条链路上动态切换。

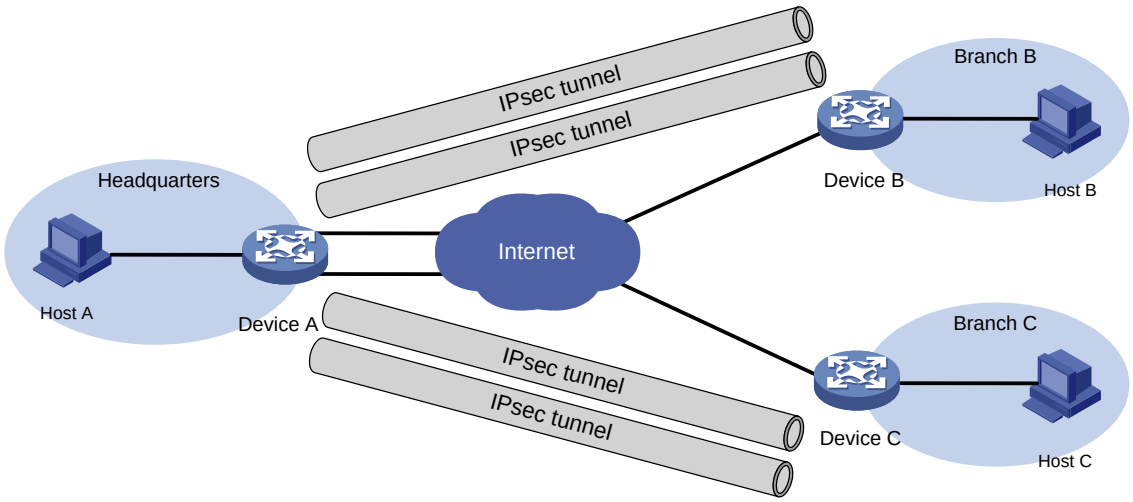
图19 IPsec 智能选路场景配置组网图




## 4.6 总部双链路场景

如图 20 所示，企业总部有两条出口链路接入 Internet，企业分支各有一条出口链路接入 Internet，企业总部和各分支之间根据 NQA 探测结果，选择高质量、低延迟的链路动态建立 IPsec 隧道。

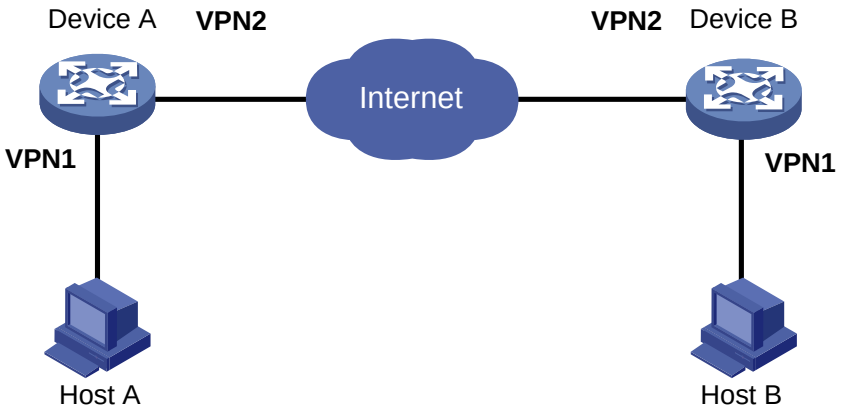
图20 总部双链路备份场景配置组网图




## 4.7 VPN多实例场景

如图 21 所示，企业总部网关企业分支网关的内网口和外网口属于不同的 VPN 实例的场景中，企业总部和企业分支之间建立一条 IPsec 隧道，对局域网之间的数据流进行安全保护。

图21 VPN 多实例场景配置组网图




# 5 参考文献


- RFC2408：Internet Security Association and Key Management Protocol (ISAKMP)
- RFC2409：The Internet Key Exchange (IKE)
- RFC2412：The OAKLEY Key Determination Protocol
- Internet-Draft：draft-ietf-ipsec-isakmp-xauth-06.txt
- Internet-Draft：draft-dukes-ike-mode-cfg-02.txt
- RFC 2408：Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4306：Internet Key Exchange (IKEv2) Protocol
- RFC 4718：IKEv2 Clarifications and Implementation Guidelines
- RFC 2412：The OAKLEY Key Determination Protocol
- RFC 5996：Internet Key Exchange Protocol Version 2 (IKEv2)