目 录

IPsec

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。特定的通信方之间在 IP 层通过加密与数据源认证等方式，提供了以下的安全服务：

- 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，因特网密钥交换），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 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 的协议实现

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，因特网密钥交换）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“0IKE”，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。

IPsec 协议中的 AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协议定义了加密和可选认证的应用方法，提供数据可靠性保证。

- AH 协议（IP 协议号为 51）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）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。

IPsec 基本概念

1. 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、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。

2. 封装模式

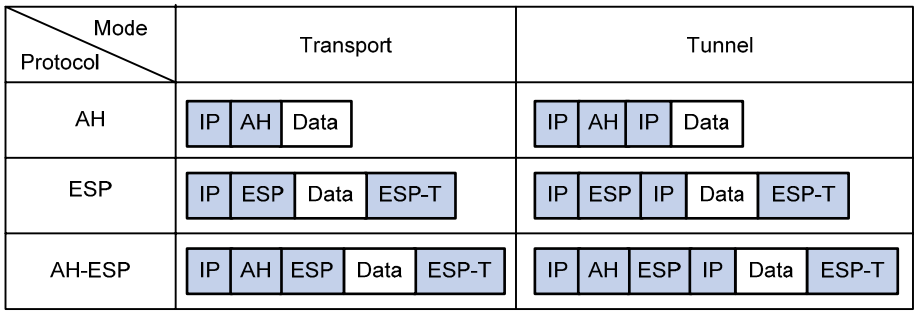
IPsec 有如下两种工作模式：

- 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所示，data为传输层数据。

图 1 安全协议数据封装格式



3. 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。

4. 协商方式

有如下两种协商方式建立 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。

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。

5. 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。

加密卡

IPsec 在设备上可以通过软件实现，还可以通过加密卡实现。通过软件实现，由于复杂的加密/解密、认证算法会占用大量的 CPU 资源，从而影响设备整体处理效率；而通过加密卡，复杂的算法处理在硬件上进行，从而提高了设备的处理效率。

加密卡进行加/解密处理的过程是：设备将需要加/解密处理的数据发给加密卡，加密卡对数据进行处理，然后加密卡将处理后的数据发送回设备，再由设备进行转发处理。

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：

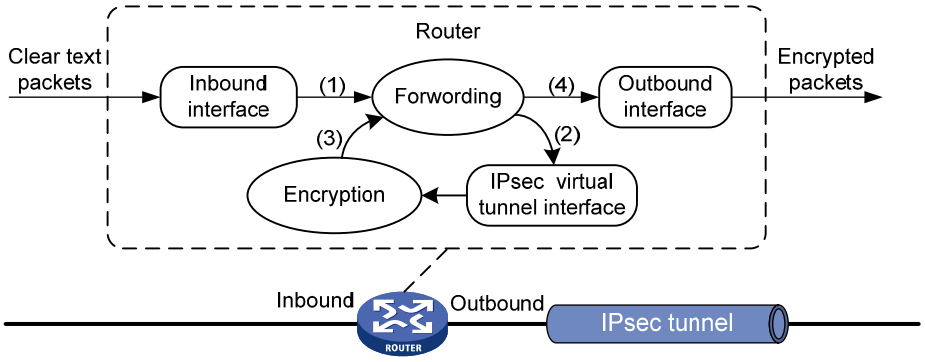
- 简化配置：通过路由来确定对哪些数据流进行 IPsec 保护。与通过 ACL 指定数据流范围的方式相比，这种方式简化了用户在部署 IPsec 安全策略时配置上的复杂性，使得 IPsec 的配置不会受到网络规划的影响，增强了网络规划的可扩展性，降低了网络维护成本。
- 减少开销：在保护远程接入用户流量的组网应用中，在 IPsec 虚拟隧道接口处进行报文封装，与 IPsec over GRE 或者 IPsec over L2TP 方式的隧道封装相比，无需额外为入隧道流量加封装 GRE 头或者 L2TP 头，减少了报文封装的层次，节省了带宽。
- 业务应用更灵活：IPsec 虚拟隧道接口在实施过程中明确地区分出“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 2所示，IPsec虚拟隧道接口对报文进行加封装的过程如下：

图 2 IPsec 虚接口隧道加封装原理图



(2) Router 将从入接口接收到的 IP 明文送到转发模块进行处理；

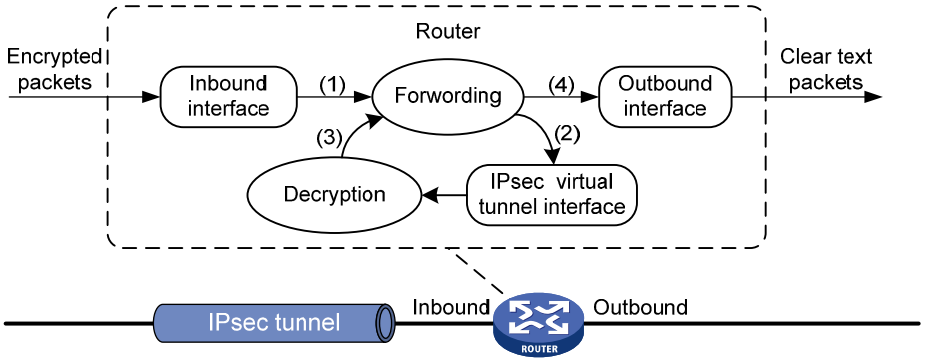
(3) 转发模块依据路由查询结果，将 IP 明文发送到 IPsec 虚拟隧道接口进行加封装：原始 IP 报文被封装在一个新的 IP 报文中，新 IP 头中的源地址和目的地址分别为隧道接口的源地址和目的地址。

(4) 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；

(5) 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接口转发出去。

如 图 3所示，IPsec虚拟隧道接口对报文进行解封装的过程如下：

图 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接口上。

使用 IPsec 保护 IPv6 路由协议


说明

本特性的支持情况与设备的型号有关，请以设备的实际情况为准。

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。

IKE

IKE 简介

在实施 IPsec 的过程中，可以使用 IKE（Internet Key Exchange，因特网密钥交换）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，并且即使第三者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。

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。即使第三者（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，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。

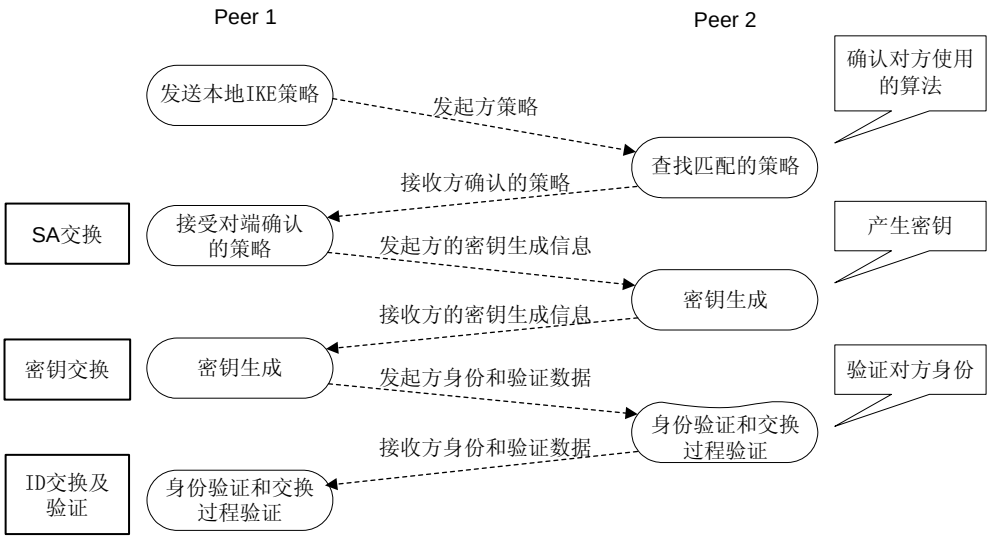
IKE 的交换过程

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 4 主模式交换过程



如 图 4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。

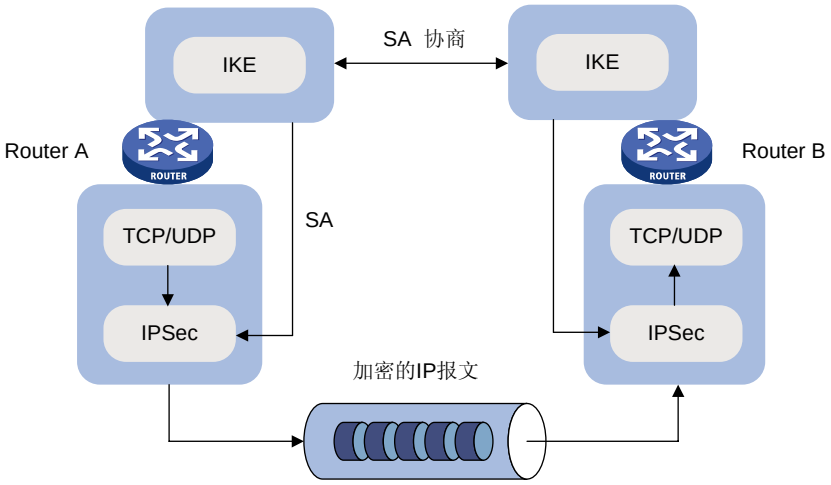
野蛮模式交换与主模式交换的主要差别在于，野蛮模式不提供身份保护，只交换 3 条消息。在对身份保护要求不高的场合，使用交换报文较少的野蛮模式可以提高协商的速度；在对身份保护要求较高的场合，则应该使用主模式。

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，认证中心）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。

IPsec 与 IKE 的关系

图 5 IPsec 与 IKE 的关系图



从 图 5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。