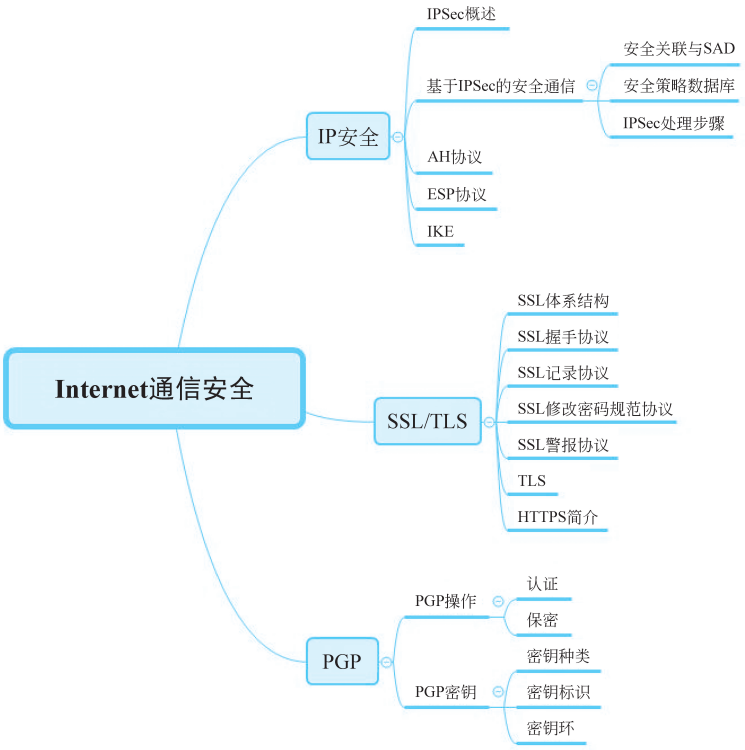
第 5 章 Internet 通信安全

导　　读



TCP/IP 体系结构是当前 Internet 的基础，TCP/IP 网络已基本成为现代计算机网络的代名词。但是，由于 TCP/IP 体系结构在设计之初的局限性，Internet 存在的安全问题日益突出，因此人们设计了不同的安全机制来应对。

事实上，可以在 TCP/IP 体系结构上的任何层次实现安全机制，各层机制有不同的特点，提供不同的安全性。本章介绍在 TCP/IP 不同层次提供安全的 3 种典型协议：IPSec、SSL/TLS 和 PGP。这些安全协议解决了本书图 1-2 的安全模型所关注的问题：如何在公开网络中保护传输数据的安全。

5.1　IP 安 全

在 TCP/IP 协议的分层模型中，IP 层是可能实现端到端安全通信的最底层。通过在

IP 层上实现安全性，不仅可以保护各种带安全机制的应用程序，而且可以保护许多无安全机制的应用程序。IP 协议一般实现在操作系统中，因此在 IP 层实现安全功能时可以不必修改应用程序。

IETF 于 1998 年颁布了一套开放标准网络安全协议 IPSec，其目标是为 IPv4 和 IPv6 提供具有较强的互操作能力、高质量和基于加密的安全。IPSec 将密码技术应用在网络层，提供端对端通信数据的私有性、完整性、真实性和防重放攻击等安全服务。

IPSec 能支持各种应用的原理在于它可以在 IP 层实现加密/认证功能，这样就可以在不修改应用程序的前提下保护所有的分布式应用，包括远程登录、电子邮件、文件传输和 Web 访问等。

IPSec 通过多种手段提供 IP 层安全服务：允许用户选择所需安全协议；允许用户选择加密和认证算法；允许用户选择所需的密码算法的密钥。IPSec 可以安装在路由器或主机上。若 IPSec 安装在路由器上，则可在不安全的 Internet 上提供一个安全的通道；若安装在主机上，则能提供主机端对端的安全性。

5.1.1　IPSec 概述

1. IPSec 应用

IPSec 提供了跨局域网、广域网甚至跨 Internet 进行端到端安全通信的能力，为主机到主机的通信流提供机密性、完整性、真实性等安全服务。

图 5-1 展示了 IPSec 的典型应用场景。

- 场景 1：分支机构安全互联。某一组织在不同的城市有分支机构，每个分支机构拥有一个局域网；在局域网内部，各主机之间的通信无须保护；但是，不同分支机构之间的通信需要通过公用的 Internet，因此需要以安全的方式交换数据。为此，在分支机构连接外部 Internet 的边界网络设备（如路由器）上部署 IPSec。部署了 IPSec 的边界网络设备将对进入 Internet 的流量进行加密、附加完整性校验码等操作，而对来自 Internet 的流量进行解密、完整性校验等操作。这些操作对局域网内部所有主机都是透明的。基于这些密码操作，流入流出分支结构的 IP 流量得到机密性、完整性、真实性等安全保护。
- 场景 2：远程安全访问。某位员工居家办公或者临时出差在外时需要访问公司内部网络的资源。为了以安全的方式达到这一目的，员工主机和公司网络边缘的网络设备部署 IPSec，对发送和接收的 IP 数据流提供安全保护。在连接企业网络和 Internet 的边缘设备上部署 IPSec 可以对通过网络边界的所有通信提供安全保护，而且这些安全操作对企业网络内部所有主机和设备是透明的，企业网络的内部通信没有安全操作带来的开销。IPSec 实现在传输层以下，对所有应用都是透明的，不需要对应用系统做出任何改变；同时 IPSec 对用户也是透明的，无须对用户进行任何安全相关的培训。

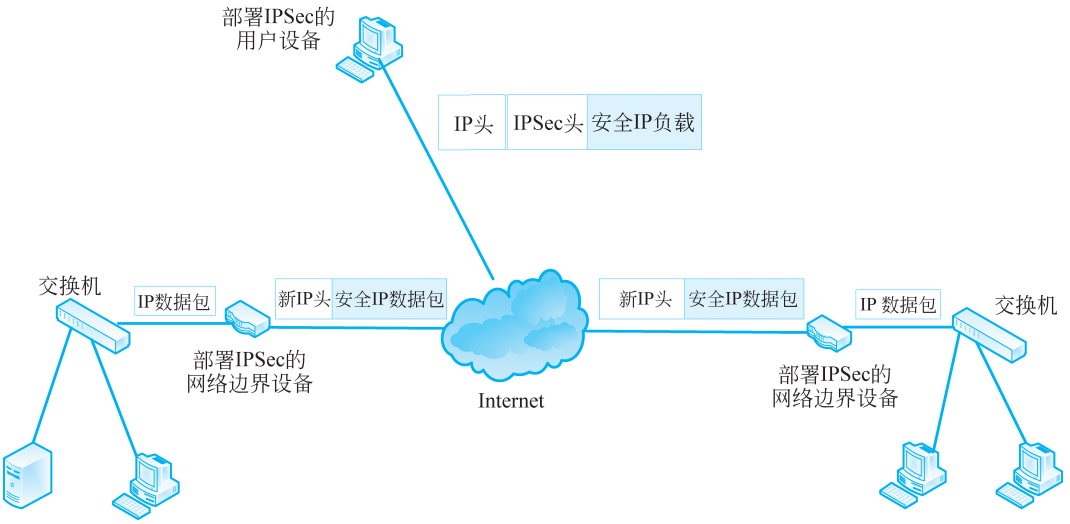


图 5-1 IPSec 的典型应用场景

2. IPSec 体系结构

IPSec 不是定义了一个单独的协议，而是给出了在 IP 层提供安全的一整套体系结构，包括认证头协议（AH）、封装安全载荷协议（ESP）、密钥管理协议（IKE）以及用于加密和认证的一些算法。IPSec 的主要构成组件如图 5-2 所示。

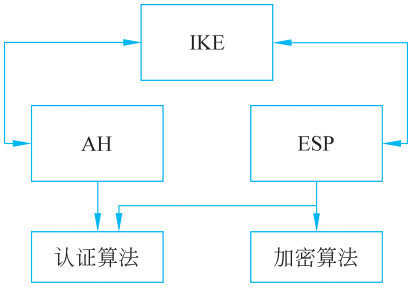


图 5-2 IPSec 组件

IPSec 的安全功能主要通过 IP 认证头（Authentication Header，AH）协议以及封装安全载荷（Encapsulating Security Payload，ESP）协议实现。AH 提供数据的完整性、真实性和防重放攻击等安全服务，但不包括机密性。ESP 除实现 AH 所实现的功能外，还可以实现数据的机密性。

完整的 IPSec 还应包括 AH 和 ESP 中所使用密钥的交换和管理机制，也就是 Internet 密钥交换（Internet Key Exchange，IKE）协议。IKE 用于动态地认证 IPSec 参与各方的身份，并且协商后续数据交换所使用的算法、协议和密钥。

IPSec 规范中要求强制实现的加密算法是 CBC 模式的 DES 和 NULL 算法，而认证算法包括 HMAC-MD5，HMAC-SHA-1 和 NULL 算法。NULL 加密和认证分别是不加密和不认证。

3. IPSec 工作模式

IPSec 的安全功能主要通过 AH 协议和 ESP 协议实现，这两个协议以 IP 扩展头的方式增加了安全相关的处理，可以对 IP 数据包或上层协议数据进行安全保护。

AH 和 ESP 均支持两种模式（传输模式和隧道模式），如图 5-3 所示。

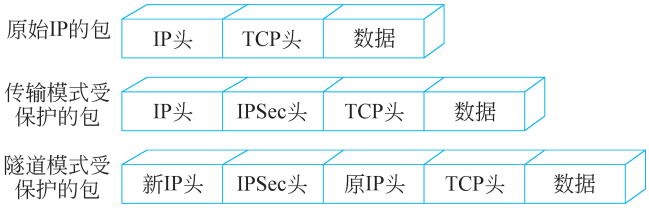


图 5-3　IPSec 工作模式

1）传输模式

传输模式为 IP 的上层协议提供保护，即 IP 数据包的载荷（如 TCP 报文段、UDP 数据报或 ICMP 消息）得到保护，但 IP 头并没有被保护。当一个主机在 IPv4 上运行 AH 或 ESP 时，其载荷是跟在 IP 报头后面的数据；对 IPv6 而言，其载荷是跟在 IP 报头后面的数据和 IPv6 的任何扩展头。

传输模式的 ESP 可以加密和认证 IP 载荷，但不包括 IP 头。传输模式的 AH 可以认证 IP 载荷和 IP 报头的选中部分。传输模式在数据包的 IP 头和载荷之间插入 IPSec 信息；原始 IP 头未进行任何安全处理，以明文方式传输，将暴露给沿途所有路由器。

传输模式一般用于两台主机之间的端到端通信，为直接运行在 IP 层之上的协议（如 TCP、UDP 和 ICMP）提供安全保护。

2）隧道模式

隧道模式对整个 IP 数据包提供保护。为达到这个目的，当 IP 数据包附加 AH 或 ESP 字段之后，整个数据包加安全字段被当作一个新 IP 包的载荷，并且拥有一个新的外部 IP 包头。原来（内部）的整个 IP 包利用隧道在网络之间传输，沿途路由器不能检查内部 IP 包头。由于原来的包被封装，因此新的、更大的包可以拥有完全不同的源地址与目的地址，以增强安全性。

通常，当通信的一端或两端为安全网关（例如部署了 IPSec 的防火墙或路由器）时，使用隧道模式。企业网络内部的主机在没有部署 IPSec 时也可以实现安全通信：当主机生成的未保护包通过网络边缘的防火墙或路由器时，该部署了 IPSec 的防火墙或路由器对整个 IP 数据包进行加密和封装，以提供隧道模式的安全性。例如，假设网络中的主机 A 生成以另一个网络中主机 B 作为目的地址的 IP 数据包，该 IP 包从源主机 A 被发送到 A 所在网络的边界防火墙或安全路由器。如果此数据包需要 IPSec 处理，则防火墙或安全路由器执行 IPSec 处理，给该 IP 包添加外层 IP 头，外层 IP 头的源 IP 地址为此防火墙或安全路由器的 IP 地址，目的地址可能为 B 所在网络的边界防火墙地址。这样，新的 IP 包被传送到 B 的防火墙，而其间经过的中间路由器仅检查外部 IP 头；在 B 的防火墙处，外部 IP 头被剥除，内部的原始 IP 包被送往主机 B。

隧道模式的 ESP 加密和认证（可选）整个内部 IP 包，包括内部 IP 包头；隧道模式的

AH 认证整个内部 IP 包和外部 IP 头中的选中部分。

5.1.2 IPSec 安全通信

1. 安全关联

IPSec 的一个核心概念是安全关联(SA)。安全关联是发送方和接收方之间受到密码保护的单向关系，它对所携带的通信流量提供安全服务：要么对通信实体收到的 IP 数据包进行“进入”保护，要么对外发的数据包进行“流出”保护。如果需要双向安全交换，则需要建立两个安全关联：一个用于发送数据，另一个用于接收数据。

一个安全关联由 3 个参数唯一确定。

- 安全参数索引(SPI)：一个与 SA 相关的位串，仅在本地有意义。这个参数被分配给每一个 SA，并且每一个 SA 都通过 SPI 进行标识。发送方把这个参数放置在每一个流出数据包的 SPI 域中，使得接收系统能选择合适的 SA 处理接收包。SPI 并非全局指定，因此它要与目标 IP 地址、安全协议标识一起唯一标识一个 SA。
- 目标 IP 地址：目前 IPSec SA 管理机制中仅允许单播地址。这个地址表示 SA 的目的端点地址，可以是用户终端系统、防火墙或路由器。目标 IP 地址决定了关联方向。
- 安全协议标识：标识该关联是一个 AH 安全关联还是一个 ESP 安全关联，即使用 AH 协议还是 ESP 协议保护数据流量。

在 IPSec 中，对一个 IP 数据包应用什么样的安全处理由两个数据库的交互来决定：安全关联数据库(Security Association Database，SAD)和安全策略数据库(Security Policy Database，SPD)。

2. SAD

在任何 IPSec 实现中，都有一个安全关联数据库(SAD)。从概念上讲，SAD 包含多个条目，每个条目对应一个 SA，定义与此 SA 相关联的参数，特别是安全相关的参数。一个 SA 通常用以下参数定义。

- 序列号计数器：AH 或 ESP 报头中序列号的 32 位值。
- 序列号溢出标志：标志序列号计数器是否溢出；溢出时，停止在此 SA 上继续传输包。
- 反重放窗口：用于判定一个 AH 或 ESP 数据包是否是重放。
- AH 信息：认证算法、密钥、密钥生存期和 AH 的相关参数。
- ESP 信息：加密和认证算法、密钥、初始值、密钥生存期和 ESP 的相关参数。
- 生存期：一个特定的时间间隔或字节计数；超过后，此 SA 要么终止，要么由一个具有新 SPI 的新 SA 替代。
- IPSec 协议模式：隧道、传输或通配符。
- Path MTU：路径最大传输单元(不需要分段传输的最大包长度)和迟滞变量。

3. SPD

IP 流量和特定 SA 的关联是通过 SPD 实现的。在概念上，一个 SPD 包括多个条目；

每一个条目定义一个IP流量的子集并指向一个SA，即将一个特定SA应用于此IP流量子集。在更复杂的情况下，多个IP流量子集可与一个SA相连或者多个SA与一个IP流量子集相关。读者可以参见相关的IPSec文档。

每个SPD条目由IP和上层协议的某些字段定义，这些字段称为选择子(selector)，因为基于这些字段可以选择一个特定的流量子集并指向一个特定的SA。选择子包括以下协议字段。

- 目的IP地址：可以是单一IP地址、一组或一定范围的地址和地址掩码。后两者要求多个目的系统共享相同的SA(例如位于防火墙之后)。
- 源IP地址：可以是单一IP地址、一组或一定范围的地址和地址掩码。后两者要求多个源系统共享相同的SA(例如位于防火墙之后)。
- 用户标识：来自操作系统的用户标识。用户操作系统提供该标识，而不是IP或上层报头域提供。
- 数据敏感性级别：用于系统提供信息流安全级别(如秘密或未分类)。
- 传输层协议：从IPv4或IPv6的邻接头域中获得，可以是单个协议号，也可以是一组或一定范围的协议号。
- 源端口和目的端口：可以是单个TCP或UDP端口、一组端口和端口通配符。

表5-1是一个简单的SPD例子，其中*代表通配符，Action则表示将要应用于此IP流量子集的安全策略：PROTECT、BYPASS或DISCARD。

各条目含义如下。

- IP地址100.1.2.3的主机发往子网198.1.2.0/24的IP流量，将用传输模式ESP进行保护；
- IP地址100.1.2.3的主机发往服务器198.1.3.2的HTTP请求数据，将用传输模式ESP进行保护；
- IP地址100.1.2.3的主机发往服务器198.1.3.2的HTTPS数据，不用IPSec进行保护；
- IP地址100.1.2.3的主机发往子网198.1.3.3/24的IP流量，将被丢弃，不被发送出去。

表5-1 一个简单的SPD例子

Protocol	LocalIP	Port	RemoteIP	Port	Action
*	100.1.2.3	*	198.1.2.0/24	*	PROTECT：ESP in transport-mode
TCP	100.1.2.3	*	198.1.3.2	80	PROTECT：ESP in transport-mode
TCP	100.1.2.3	*	198.1.3.2	443	BYPASS
*	100.1.2.3	*	198.1.3.2/24	*	DISCARD

4. IPSec处理

当实现IPSec时，每一个发往外部的IP数据包在发送之前都由IPSec先进行安全相关的处理，而每一个收到的IP包在传递给上一层协议前也由IPSec首先进行处理。

发送 IP 数据包的处理过程如图 5-4 所示，包括以下步骤。

① 搜索 SPD，试图发现应用于此 IP 包的安全策略。

② 如果没有找到，则丢弃此 IP 包并产生一个错误信息；否则转下一步。

③ 如果对这个 IP 包的处理策略是 DISCARD，则丢弃；如果是 BYPASS，那么 IPSec 不再对此 IP 包进行安全处理。

④ 如果对这个 IP 包的处理策略是 PROTECT，则搜索 SAD 以匹配一个应用于此 IP 数据包的 SA；如果没有找到，则执行 IKE 生成一个 SA 并加入 SAD 中。

⑤ SAD 中匹配的 SA 决定如何对这个 IP 数据包进行处理：加密、认证或者两者同时执行，采用隧道模式还是传输模式，以及使用的算法和密钥。

⑥ 发送此 IP 包。

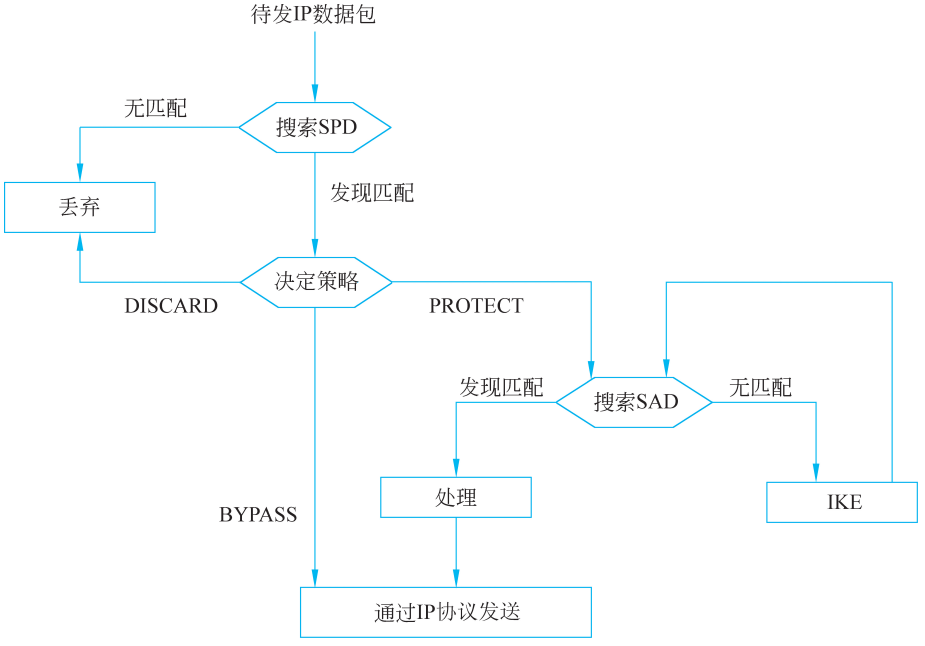


图 5-4　IP 数据包的发送

接收 IP 数据包的处理过程如图 5-5 所示，包括以下步骤。

① 判断包的类型，即是未经安全处理的 IP 数据包，还是经过 IPSec 处理的安全数据包。

② 对于未经安全处理的 IP 数据包，搜索 SPD。如果发现一个匹配并且策略是 BYPASS，则处理并剥除 IP 头并将载荷交给上层相应的协议；如果发现一个匹配并且策略是 PROTECT 或 DISCARD，或者未发现匹配，则将丢弃此数据包。

③ 对于经过 IPSec 处理的安全数据包，搜索 SAD。如果没有发现匹配，则丢弃；如果发现一个匹配，则应用匹配的 SA 进行处理并将 IP 数据包的载荷交给上层协议。

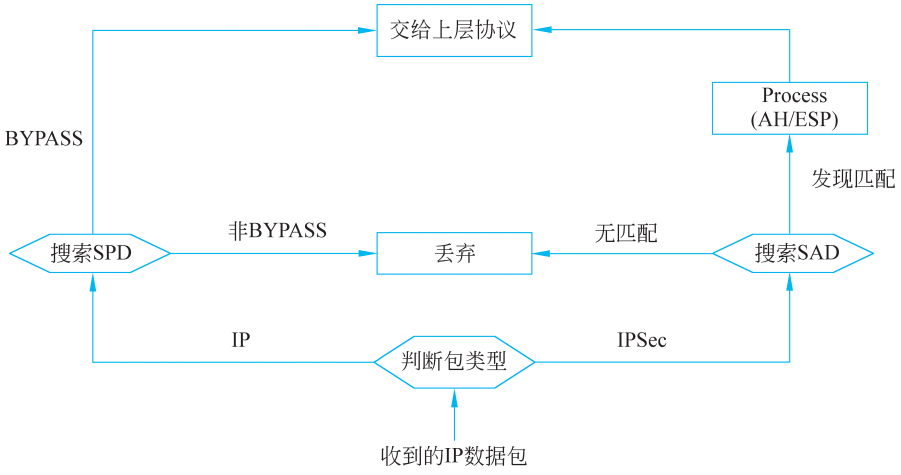


图 5-5　IP 数据包的接收

5.1.3　AH 协议

IP 认证头(AH)协议为 IP 数据包提供数据完整性校验和身份认证,还有可选择的抗重放攻击保护,但不提供数据加密服务。数据完整性确保包在传输过程中内容不可更改;认证确保终端系统或网络设备能对用户或应用程序进行认证,并且相应地提供流量过滤功能,同时还能防止地址欺诈攻击和重放攻击。认证基于消息鉴别码(MAC),双方必须共享同一个密钥。

由于 AH 不提供机密性保证,因此它不需要加密算法。AH 可用来保护一个上层协议(传输模式)或一个完整的 IP 数据报(隧道模式)。它可以单独使用,也可以和 ESP 联合使用。

认证头由如下几个域组成,如图 5-6 所示。

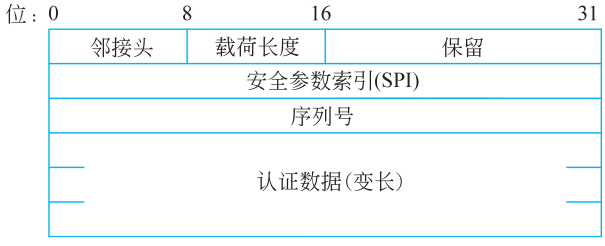


图 5-6　IPSec 认证头

- 邻接头(8 位):标识 AH 字段后面下一个负载的类型。
- 有效载荷长度(8 位):字长为 32 位的认证头长度减 2。例如,认证数据域的默认长度是 96 位或 3 个 32 位字,另加 3 个字长的固定头,总共 6 个字,则载荷长度域的值为 4。
- 保留(15 位):保留给未来使用。当前,这个字段的值设置为 0。

- 安全参数索引(32 位)：这个字段与目的 IP 地址和安全协议标识一起共同标识当前数据包的安全关联。
- 序列号(32 位)：单调递增的计数值，提供了反重放的功能。在建立 SA 时，发送方和接收方的序列号初始化为 0，使用此 SA 发送的第一个数据包序列号为 1，此后发送方逐渐增大该 SA 的序列号并把新值插入序列号字段。
- 认证数据(变长)：变长域，包含了数据包的完整性校验值(Integrity Check Value，ICV)或包的 MAC。这个字段的长度必须是 32 位字的整数倍，可以包含填充。

1. AH 传输模式

AH 传输模式只保护 IP 数据包的不变部分，它保护的是端到端的通信，通信的终点必须是 IPSec 终点，如图 5-7 所示。

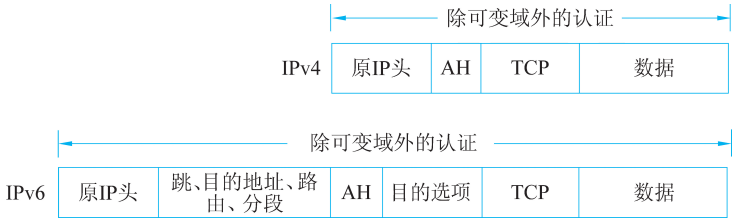


图 5-7　AH 传输模式

在 IPv4 的传输模式 AH 中，AH 插入原始 IP 头之后，且在 IP 载荷(如 TCP 分段)之前。认证包括除 IPv4 报头中可变的、被 MAC 计算置为 0 的域以外的整个包。

在 IPv6 中，AH 被作为端到端载荷，即不被中间路由器检查或处理。因此，AH 出现在 IP 头以及跳、路由和分段扩展头之后。目的选项作为可选报头在 AH 前面或后面，由特定语义决定。同样，认证包括除 IPv6 报头中可变的、被 MAC 计算置为 0 的域以外的整个包。

2. AH 隧道模式

AH 用于隧道模式时，整个原始 IP 包被认证，AH 被插入原始 IP 头和新 IP 头之间。原 IP 头中包含通信的原始地址，而新 IP 头则包含 IPSec 端点的地址，如图 5-8 所示。

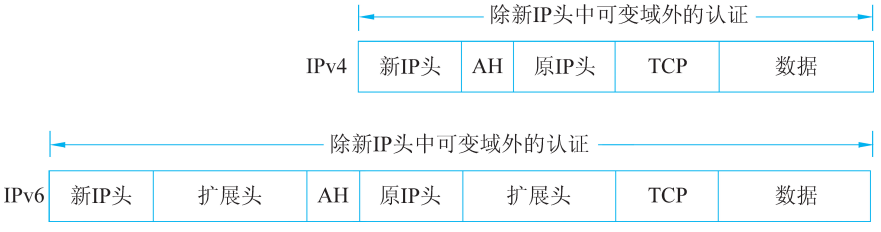


图 5-8　AH 隧道模式

通过使用隧道模式，整个内部 IP 包(包括整个内部 IP 头)均被 AH 保护。外部 IP 头(IPv6 中的外部 IP 扩展头)除可变且不可预测的域外均被保护。隧道模式可用来替换端到端安全服务的传输模式。但由于这一协议中没有提供机密性，相当于没有隧道封装这一保护措施，因此它没有什么用处。

5.1.4　ESP 协议

封装安全载荷(ESP)协议为 IP 数据包提供数据完整性校验、身份认证和数据加密，还有可选择的抗重放攻击保护；即除 AH 提供的所有服务外，ESP 还提供数据保密服务，包括报文内容保密和流量限制保密。ESP 用一个密码算法提供机密性，数据完整性则由身份验证算法提供。ESP 通过插入一个唯一的、单向递增的序列号提供抗重放服务。保密服务可以独立于其他服务而单独选择，数据完整性校验和身份认证用作保密服务的联合服务。只有选择了身份认证，才可以选择抗重放服务。

ESP 可以单独使用，也可以和 AH 联合使用，还可以通过隧道模式使用。ESP 可以提供主机到主机、防火墙到防火墙、主机到防火墙之间的安全服务。

图 5-9 是 ESP 包的格式，它包含如下各域。

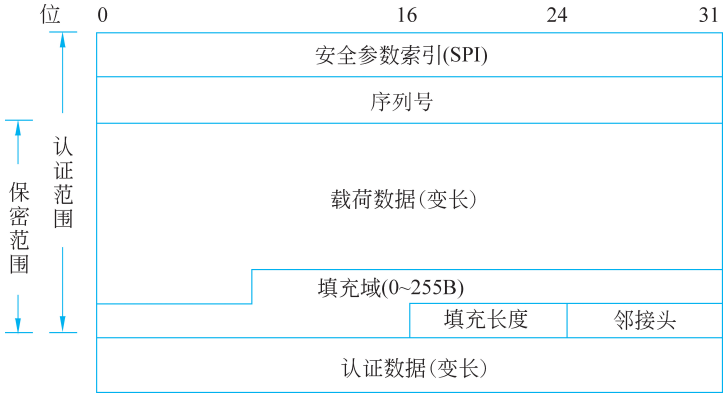


图 5-9　ESP 包格式

- 安全参数索引 SPI(32 位)：标识安全关联。ESP 中的 SPI 是强制字段，总是要提供。
- 序列号(32 位)：单调递增计数值，提供反重放功能。这是强制字段，并且总是要提供，即使接收方没有选择对特定 SA 的反重放服务。如果开放了反重放服务，则计数值不允许折返。
- 载荷数据(变长)：变长的字段，包括被加密保护的传输层分段(传输模式)或 IP 包(隧道模式)。该字段的长度是字节的整数倍。
- 填充域(0～255 字节)：可选字段，但所有实现都必须支持该字段。该字段满足加密算法的需要(如果加密算法要求明文是字节的整数倍)，还可以提供通信流量的保密性。发送方可以填充 0～255 字节的填充值。
- 填充长度(8 位)：紧跟填充域，指示填充数据的长度，有效值范围是 0～255。
- 邻接头(8 位)：标识载荷中第一个报头的数据类型(如 IPv6 中的扩展头或上层协议 TCP 等)。
- 认证数据(变长)：一个变长域(必须为 32 位字长的整数倍)，包含根据除认证数据域外的 ESP 包计算的完整性校验值。该字段长度由所选择的认证算法决定。