警示消息有两种：一种是 Fatal 错误，如传递数据过程中，发现错误的 MAC，双方就需要立即中断会话，同时消除自己的缓冲区中相应的会话记录；第二种是 Warning 消息，这种情况下通信双方通常都只是记录日志，而对通信过程不造成任何影响。SSL 握手协议可以使得服务器和客户能够相互鉴别对方，协商具体的加密算法和 MAC 算法以及保密密钥，用来保护在 SSL 记录中发送的数据。

20.1.5 改变密码约定协议

SSL 改变密码约定协议是使用 SSL 记录协议服务的 SSL 高层协议的 3 个特定协议之一，也是其中最简单的一个。协议由单个消息组成，该消息只包含一个值为 1 的单个字节。该消息的唯一作用就是将未决状态复制为当前状态，更新用于当前连接的密码组。为了保障 SSL 传输过程的安全性，双方应该每隔一段时间改变加密规则。

20.1.6 应用数据协议

SSL 应用数据协议包括常用的应用层协议，如超文本传输协议（Hyper-Text Transfer Protocol，HTTP）、文件传输协议（File Transfer Protocol，FTP）等。

20.2 IPSec

1．概述

IPSec 协议是 IETF 于 1998 年 11 月公布的 IP 安全标准，它是在 IP 层上对数据包进行高强度的安全处理，提供包括访问控制、无连接的完整性、数据源认证、抗重播保护、保密性和有限传输流保密性在内的服务，这些服务提供对 IP 及其上层协议的保护。IPSec 提供了一种标准的、健壮的、包容广泛的、易于扩展的、完整的基础网络安全方案，目前被广泛应用于实现端到端的安全、虚拟专用网和安全隧道，是一种可为任何形式的 Internet 通信提供安全保障的协议。

IPSec 协议是一个协议簇，它包含 ESP 协议、AH 协议和 IKE 协议等，图 20-3 显示了 IPSec 的体系结构、组件及各组件间的相互关系。

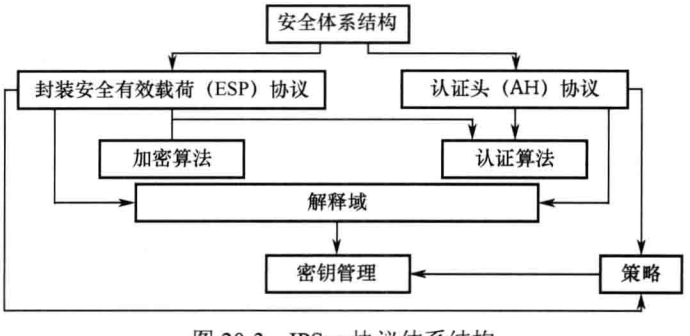

图 20-3 IPSec 协议体系结构

（1）ESP（Encapsulating Security Payload，封装安全载荷）

ESP 机制通过将整个 IP 分组或将上层协议部分（即传输层协议数据，如 TCP、UDP 或 ICMP 协议数据）封装到一个 ESP 载荷之中，然后对此载荷进行相应的安全处理，如加

密处理、鉴别处理等，以实现通信的机密性和安全性保护。

（2）AH（Authentication Header，验证报头）

AH 机制主要用于为通信提供完整验证性服务，还能为通信提供加密和抗重放攻击服务。

（3）加密算法

描述各种加密算法如何应用于 ESP 中，默认的算法为 DES-CBC 算法。

（4）验证算法

描述各种身份验证算法如何应用于 AH 协议和 ESP 协议中的身份验证选项，默认的有 HMAC-MD5 和 HMAC-SHA1 算法。

（5）密钥管理

密钥管理的一组方案 IKE（Internet 密钥交换协议）是默认的密钥交换协议。

（6）解释域

彼此相关各部分的标准符及运作参数，它实际是一个存放所有 IPSec 安全参数的数据库，这些参数可被与 IPSec 服务相应的系统参考并调用。

（7）策略

它决定两个实体之间是否能够通信和如何通信，策略的核心由三部分组成：SA（Security Association）、SAD（Security Association Database）、SPD（Security Policy Database）。安全策略数据库（Security Policy Database，SPD）对 IPSec 策略加以维护。在 SPD 数据库中，每个条目都定义了所要保护的通信类别、保护方法以及谁共享这种保护。进入或离开 IP 堆栈的数据包都必须检索 SPD 数据库，调查可能的安全应用。每一个 SPD 条目都要定义一个对数据包的处理动作，这个动作是丢弃、透传或应用 IPSec 处理中的一种。其中，如果 SPD 项定义的动作为应用 IPSec 处理，则会指向一个或一套安全联盟（SA），表示对数据包应用安全保护。SA 表示策略实施的具体细节，包括源地址、目的地址、应用协议、SPI（安全策略索引）、所用算法、密钥、长度；SAD 为进入和外出包处理维持一个活动的 SA 列表。

2．AH 协议和 ESP 协议

IPSec 协议主要使用验证报头协议（AH）和封装安全载荷协议（ESP）来提供数据的安全保证，这两个协议可以独立使用也可以组合使用以提供 IPv4 和 IPv6 环境下所需要的安全服务。

ESP（Encapsulation Security Payload）是一个安全协议头，属于 IPSec 的一种协议，通过对原始有效负载进行加密和认证并将分组封装在一个 ESP 报头和 ESP 报尾之间，提供了对 IP 数据包的机密性、数据的完整性以及可选的数据源身份认证和抗重放攻击的服务。应用 ESP 时，要在 IP 报头之后、上层协议（要保护的数据）之前插入一个 ESP 头，同时在报文最后加入一个 ESP 尾将整个 IP 数据包封装起来。图 20-4 描述了传输模式下 ESP 封装 IP 报文的格式。

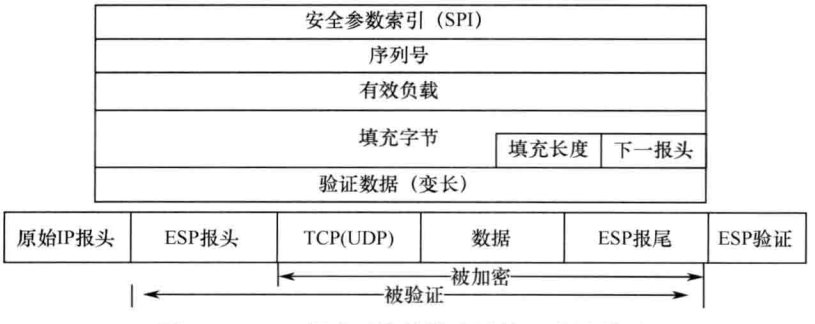

图 20-4　ESP 报头及传输模式封装 IP 报文格式

AH 协议是一种 IPSec 协议，用于为 IP 通信提供数据完整性、数据原始身份验证和一些可选的、有限的抗重播服务，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 不提供任何的保密性服务，它的作用是为 IP 数据流提供高强度的密码认证，以保证数据包在被改变后能被察觉的完整性机制、验证数据包的来源的认证机制。AH 通过在整个 IP 数据包中使用一个消息验证码（MAC）来提供完整性和认证服务。一个消息验证码就是一个特定的单项散列函数，它接受一个任意长度的消息和一个密钥，生成一个固定长度的输出，称作消息摘要或指纹。MAC 不同于一般的杂凑函数，因为它是需要密钥的，最常用的 MAC 是 HMAC。IPSec 在发送数据包和接收数据包之后都可以根据一组数据计算出 MAC，其结果放到 AH 包头的验证数据区。如果两次的值一样则说明数据包没有被修改过。AH 协议具有传输和隧道两种模式和外出与进入处理方式。图 20-5 描述了传输模式下 AH 保护 IP 报文的格式。

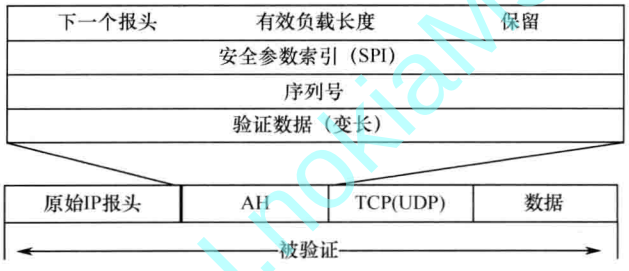

图 20-5　AH 报头及传输模式封装 IP 报文格式

3．安全关联数据库

安全关联数据库（SAD）用于存放安全关联（SA）。安全关联（SA）是 IPSec 的基础，它决定保护什么、如何保护以及谁来保护通信数据，是两个通信实体经过协商建立起来的一种协定，规定用来保护数据安全的模式、算法及密钥、生存期、抗重放窗口、计数器等等。SA 是单向的，因此两个 IPSec 对等体之间的 IPSec SA 成对出现，分别用于各自的进入和外出处理。SA 还与协议相关，每一种协议都有一个 SA。安全关联由一个三元组唯一标识：安全参数索引（SPI）、IP 目的地址及安全协议（AH 或 ESP）标识符。IPSec SA 可用 IKE 协议自动协商或进行手工设置获得，并进行有效性判断，规定的安全服务通过使用 AH 或 ESP 协议体现。

安全关联数据库（SAD）用于存放安全关联（SA），每一个 IPSec 实现都必须有一个名义上的安全关联数据库，新建立的 SA 要写入 SAD，每个 SA 在 SAD 中有一个入口。SAD 定义了在主机、安全网关上实现输入、输出 IP 通信的策略。每个入口定义一个 SA 的参数，对于输出处理，SAD 入口被 SPD 中的入口指定；对于输入处理，SAD 中的每个入口由接收到的报文域中的目的 IP 地址、IPSec 协议类型和 SPI 索引来查找。

4．安全策略数据库

IPSec 策略由 IPSec 安全策略数据库（SPD）维护，每个策略条目都在入口定义了要保护的是哪种类型的通信、如何保护以及如何共享这种保护，所有进入或外出的 IP 数据流都要检索 SPD 数据库，查找可能的安全应用。SPD 处理策略是 SA 处理过程的核心部分，它定义了提供给 IP 数据报的服务和方式，每一个 SPD 条目都定义了对输入和输出数据报文

的处理行为，是丢弃、透传或者应用 IPSec 三种中的一种。应用 IPSec 处理是数据报文在通过 IPSec 代理时进行 IPSec 处理，对于需要处理的数据报，SPD 将会确切地指出应该提供的安全服务、协议类型、应该使用的算法等信息。SPD 是 IPSec 在系统中维护的系统安全策略集，一条安全策略可以指定一个或多个 SA 策略应用于一个指定的数据报文流上，但在 SPD 中的策略项必须保存这些 SA 的顺序，在实现时必须可以为输入和输出报文定义一个 SA 的处理顺序。

SPD 对于输入、输出必须要有不同的入口，每一个 IPSec 实现必须有一个可供管理的接口，允许用户或系统管理员管理 SPD。SPD 主要包括策略入口的有序列表，每一个策略入口由一个或多个选择符标志，这些选择符定义了被这一策略入口包含的 IP 数据流、策略或者 IPSec 处理的粒度。每一个入口可能定义了丢弃、透传和应用这三种动作中的一个，如果是应用，那么该入口将会提供相应信息用来检索保护该类型数据包的 SA。如果 SA 尚未建立，那么就需要请求 IKE 与远端主机协商一个。数据包到 IPSec 策略的映射关系是由选择符决定的，选择符来源于数据包的各个字段，包括：目的地址、源地址、名字、传输层协议和源目的端口。这些选择符的值可能是一个特定取值、一个范围或者是不透明。策略的表示方式直接影响到 IPSec 的灵活性和表示能力，在实现中利用了 Internet 安全关联和密钥管理协议中提案载荷的格式来描述策略。

5．IPSec 的工作模式

IPSec 协议（包括 AH 和 ESP）可分别工作在传输模式和隧道模式，前者是用来保护 IP 报头之后的上层协议和数据，后者保护包括 IP 报头的整个 IP 报文分组。

（1）传输模式

传输模式用来保护 IP 报头之后的有效载荷，在 IP 报头和上层协议报头之间插入一个 IPSec 报头，其通信的终点必须是一个加密的终点，用于保障端到端的通信安全。

图 20-6 说明了传输模式下 IPSec 保护 IP 分组的格式。在这种模式下，IP 报头与原始 IP 分组中的 IP 报头相同，只是 IP 协议字段被改为 ESP（50）或 AH（51），并重新计算 IP 报头的校验和，IPSec 源端点不会修改 IP 报头中的目的地址。

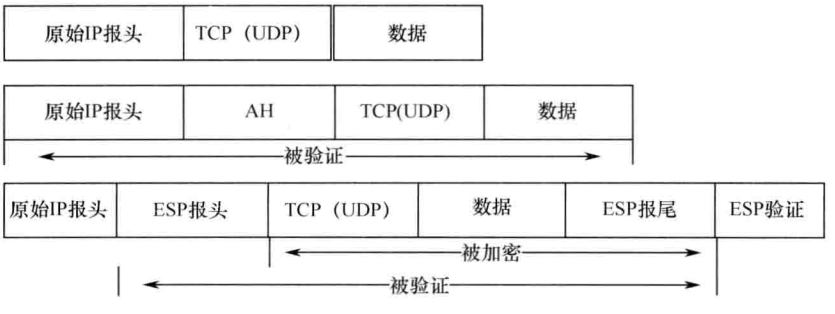

图 20-6　传输模式下 IP 报文封装格式

（2）隧道模式

隧道模式用来保护整个 IP 数据包。要保护的整个 IP 包都封装到一个新的 IP 包里，同时在外部 IP 报头和内部报头之间插入一个 IPSec 头，如图 20-7 所示。当隧道模式被网关使用时，可用来保护与其连接的子网，VPN 网络中采用的便是隧道模式。在隧道模式中，

通信的终点是由受保护的内部 IP 报头指定的地址，而 IPSec 的终点则是那些由外部 IP 报头指定的地址。IPSec 处理结束后，VPN 网关会剥离外部 IP 报头后，再将原始 IP 包转发到它最终的目的地。

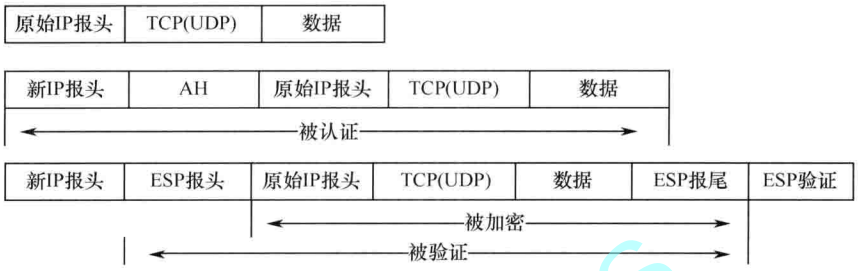

图 20-7　隧道模式下 IP 报文封装格式

在隧道模式中，数据包的内部 IP 头是由主机创建的，外部 IP 头是由提供安全服务那个 IPSec 网关（既可以是主机，也可以是路由器）添加的。IPSec 支持嵌套隧道，所谓嵌套隧道就是对一个已经按隧道模式封装了的数据包再进行一次 IPSec 隧道处理，从而支持多级网络安全保护。例如，一家公司有一个安全网关，为防止竞争者和黑客的侵犯，在该公司网络内部另有一个安全网关，防止某些内部员工进入敏感子网。此时，若对一个保护网络内部的保护子网进行访问就要用到嵌套式隧道。图 20-8 描绘了 AH 和 ESP 联合嵌套时的使用方式。

图 20-8　AH 和 ESP 联合嵌套封装 IP 报文

6. IKE 协议（Internet 自动密钥交换协议）

SA 定义了通信中应用的安全服务的细节，所以在进行 IPSec 通信之前必须在两台通信实体之间协商建立 SA。SA 分为两种：IKE SA 和 IPSec SA。对等体之间的 IKE SA 用于对控制数据流的保护（如 IPSec 的协商报文），协商对 IKE 数据流进行加密以及对对等体进行认证的算法，对等体之间只有一个 IKE SA。IPSec SA 用于协商对等体之间的 IP 数据流进行加密的算法，对哪些数据流进行加密由策略定义决定。IPSec SA 是单向的，因此它总是成对出现的，对等体之间可以有多个 IPSec SA，用于保护不同的 IP 主机组或者 IP 数据流。

SA 可以手工建立，但很明显这种情况适合于规模小、机器分配相对固定的环境。因此 IETF 定义的主要功能是自动确定和维护 IKE SA 和 IPSec SA 的 IKE 协议。IKE 分两个阶段运行，以分别确定 ISAKMP SA 和 IPSec SA。

阶段 1：IKE 对等体互相验证对方身份并确定回话密钥。这个阶段通过使用 DH 交换、cookie 和 ID 载荷交换创建一个 ISAKMP SA（也叫 IKE SA）。之后，发起方和响应方之间的所有 IKE 通信都将通过 IKE SA 进行加密和完整性保护。IKE 的第一阶段主要是在安全对等体之间建立一条安全信道，以便第二阶段协商能够安全进行。阶段 1 的协商模式包括主模式和野蛮模式。