Internet Security Standard IPSec Analysis and Application

网络安全标准 IPSec 分析及应用

姜 圳 张礼勇 （哈尔滨理工大学 150040）
王喜莲 张宏科（北方交通大学 100044）

摘要：IP 安全是保证 Internet 网络安全的重要部分，IPSec 为网络提供了安全标准。本文从 IPSec 安全标准体系结构入手，详细分析了对 IP 数据包进行 IPSec 处理所制定的各项标准，包括安全协议、认证和加密算法、安全联盟及密钥交换机制，同时对 IPSec 两种操作模式进行了比较，给出了基于 IPSec 构建虚拟专用网（VPN）的一种典型应用。

关键词：IPSec VPN 安全联盟 密钥交换 操作模式

1 IPSec 协议概述

IPSec 制定了新一代 Internet 网的安全标准，为传输的数据提供了身份认证、完整性、机密性及抗重播的服务。

(1) 身份认证：确信数据的发送方就是你所要求的发送方。

(2) 完整性：保证收到的信息就是原始信息，在传输过程中没被修改。

(3) 机密性：保证数据在传输过程中没被别人偷看。

(4) 抗重播：防止数据包被重复发送。

1995 年发表的 IP 安全文档为 RFC1825 ~ RFC1828，1998 年又制定了新的 RFC 标准取代了上述标准，相应文档如下：

RFC2401：Security Architecture for the Internet Protocol (SA)--IP安全结构，定义了IPSec的基本结构，安全目标、安全服务、实施方案等，是IPSec体系的基础。

RFC2402: IP Authentication Header (AH)---IP认证头，定义了IP认证报头格式，服务类型及包处理规则，提供身份认证、数据完整性及抗重播功能。

RFC2406: Encapsulating security payload (ESP)---封装安全载荷，定义了ESP头格式、服务类型及包处理规则，提供数据机密性、完整性、身份认证及抗重播功能。

RFC2409: Internet Key Exchange (IKE)---因特网密钥交换，定义了通信双方动态建立安全联盟的过程，包括密钥产生、协商和交换，IKE是建立在RFC2408定义的安全联盟和密钥管理协议（ISAKMP）框架上的。

RFC2407: Domain of Interpretation，定义了IKE如何协商及协商内容。

RFC2403 和 RFC2405 分别定义了用于 ESP 的认证算法和加密算法及其实现方案。

RFC2404 定义了用于 AH 的认证算法。

还有一些文档完成对密钥交换步骤、协议的具体实现算法等的定义。

IPSec 可为 IP 层及其上层协议（如 UDP、TCP）提供安全保证。IPSec 机制的算法独立，可方便地进行算法改进或增加新算法，其默认算法保证了实施的互操作性。IPSec 可实现主机之间、网关之间及主机与网关之间的数据安全传输，还可以提供嵌套的安全服务。新一代 IP 协议 IPv6 已将 IPSec 作为其组成部分制定，而IPSec也可作为IPv4的扩展协议为其提供IP层的安全保障。IPSec 的应用将有效地保障 Internet 网络的安全性。

2 IPSec 体系结构

RFC 定义了 IPSec 提供的安全服务、基本协

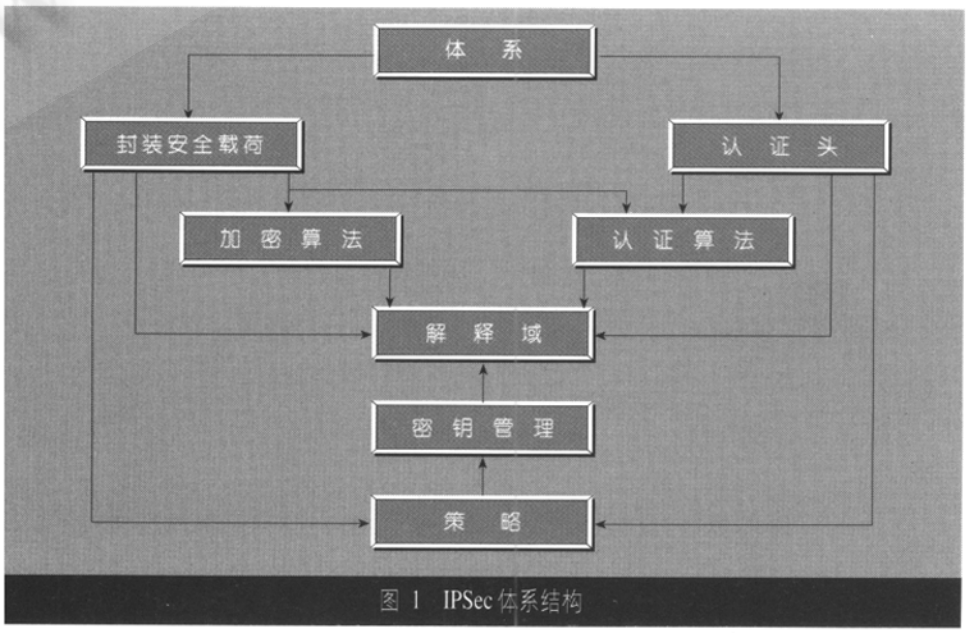

图 1 IPSec 体系结构

议、实施方案、密钥管理等，其各部分之间的关系[1，2]如图1所示。IPSec体系定义了主机与网关应该具备的各种功能。为达到保护IP数据包，通信双方首先依据预定的安全策略确定出为所传数据包应提供何种服务，然后查询是否已有建立起来的安全联盟(SA)，SA决定了使用何种IPSec协议、转码方式、密钥等以保护数据包，如没有已建的SA，则利用手工或通过Internet密钥交换(IKE)自动创建，再对数据包采用相应的安全协议，对其完成加密、认证等处理，然后发送，从而完成了IP数据包的安全保护。可见，完成IPSec处理需要包含安全协议、认证和加密算法、安全联盟及密钥交换各部分。

2.1 安全协议

(1)身份认证头(AH)。AH的作用是为IP数据包提供原始认证，确定其完整正确、防止重法攻击以及使用公共密钥数字签名算法确定发送者的真实身份，避免非法访问。AH的格式及字段[3]如图2所示。净荷长度指明了AH的整个长度。安全参数指标SPI与目的IP地址及安全协议唯一地标明数据报的安全关联(SA)。序列号字段是一个必备的单调递增计数器，每发送一个数据报，该计数器增一，在一次关联传输完2^{32}个数据报分组后，则需建立新的安全关联。这样可以预防重发如接收者收到了重复序列号的数据报，则可丢弃之。身份验证数据字段包含有完整性检查值，目的主机收到信息包后，利用SPI从SA中检出共享密钥，然后计算出验证数据，再与身份验证数据字段中的数据比较，一致则进行下一步，从而保证了数据的完整性。

(2)封装安全载荷头(ESP)。AH是用来保证IP信息的可靠性和完整性，而ESP则保证数据的机密性，并对数据来源进行身份验证及反重播等。ESP既可单独使用，也可与AH一起使用，ESP插在IP报头之后，其格式[4]如图3所示，其中SPI和序列号同AH头。净荷数据包含数据报的加密部分及加密算法需要的补充数据。填充字段的使用是为了加密，如保证算法对数据长度的要求或使数据对齐而填充数据。身份验证数据字段包含有从封装载荷分组中除去认证数据以外的部分计算得到的完整性检查值，因而ESP有效地支持了数据的完整性和保密性。

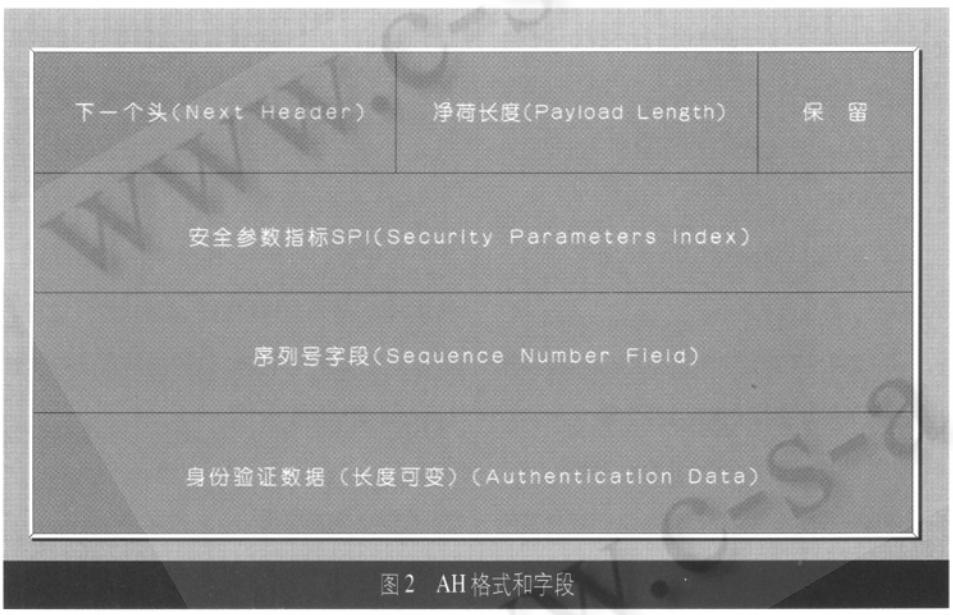

图2 AH格式和字段

图3 封装安全载荷头格式及字段

2.2 认证和加密算法

IPSec安全协议AH和ESP的应用提高了IP层的安全性，而其安全性又依赖于所使用的加密和认证算法的强度。IPSec定义了一套默认的算法，以确保不同的实施方案间的互通性。AH和ESP默认认证算法为HMAC-MD5或HMAC-SHA，ESP的加密算法必须以"加密算法块链(CBC)"模式工作，支持数据加密标准(DES)。虽然IPSec定义了默认的认证和加密算法，但其算法是独立的，可以修改或增加新算法。

2.3 安全联盟(SA)

安全联盟是构成IPSec的基础，是两个通信实体经协商建立起来的一种协定，决定了用来保护数据包安全的IPSec协议、转码方式、密钥及密钥生存期。每一通信方针对使用的每一种协议(AH或ESP)都会构建一个独立的SA，也就是SA是与协议相关的。SA也是单向的，即如果主机A与主机B之间的通信是受

IPSec保护的，则A和B都将分别有一个用来处理发送数据包的SA和一个用来处理接收数据包的SA，但A处理发送包的SA与B处理接收包的SA将共享相同的安全参数，同理B处理发送包的SA与A处理接收包的SA将共享相同的安全参数。

针对发送和接收的SA，都分别存储于一张安全联盟数据库（SADB）表中，用来维护SA记录，相关的还有一个安全策略数据库（SPD），记录对IP包提供安全服务的有关信息，SPD与SADB结合使用，即当A与B通信时，A首先查询SPD，决定提供给数据包何种安全服务，再查询SADB，取出对应的一个或多个SA，若A与B是第一次通信，则没有已建立起的SA存在，则需手工或自动建立，依据SA提供的安全措施及算法完成IPSec处理，然后发送到IP层，对于接收方B如果没有查到合适的SA，则丢弃数据包，如查到，则对包的IPSec头进行处理，最后还应查找SPD，证实对包采取的策略，AH或ESP中的SPI字段与IP包中所应用的SA相对应，

SA既可动态利用Internet密钥交换（IKE）协议配置，也可手工配置，通信双方离线商定SA的各项参数，手工添加SPD和SADB数据库，当由于SA存活时间到或密钥被破解等原因需要删除SA，同样也可手工或由IKE删除。

2.4 Internet密钥交换（IKE）

IKE是一种混合型的协议，它沿用了ISAKMP的基础，Oakley的模式及SKEME的共享和密钥更新技术[1，5，6]，IKE用于动态建立SA，如果SADB库中没有安全策略要求的SA，则IPSec内核便自动调用IKE，IKE与通信双方或中间网关协商具体的SA，IKE最终完成的功能是确定一个通过验证的密钥以及建立在双方同意基础上的IPSec安全联盟。

IKE创建IPSec SA分为两个阶段：第一阶段建立IKE SA，第二阶段利用IKE SA建立IPSec SA，IKE SA保护建立IPSec SA时的通信，即对后续协商内容进行加密，对消息进行验证。

第一阶段的完成可采用"主模式"或"野蛮模式"两种交换方式，两种方式最终都将协商制定出一些参数，包括加密算法、散列算法、验证方法及Diffie-Hellman组），即建立起一个保密而验证无误的IKE SA。两种方式中主模式灵活，野蛮模式速度快，但协商功能有限，而且不能提供身份保证，常在响应者未知发起者地址而要用预共享密钥验证方法时或发起者已知响应者的策略时用。

第二阶段则在已建立好的IKE SA的保护下，通过快速交换模式通信双方协商制定IPSec SA的各项特征，并为其生成密钥。即利用第一阶段协商好的加密算法、散列算法及验证方法完成第二阶段协商的内容的完整性检查及身份验证。而且IKE SA是双向的，无论当初谁是发起者，第二阶段双方都可充当发起者以完成快速交换。

第二阶段完成后IKE只定义了安全参数如何协商以及共享参数如何建立，但却没有定义协商内容，即没有定义需要协商解决的可选及必需项属性，这方面内容被定义在IPSec解释域（DOI）中，所以IPSec DOI是IPSec SA必需的一部分，IPSec DOI [7] 定义了身份类型、ISAKMP ID载荷的端口及协议字段，而且还规定了如何为IPSec建立SA。

除以上交换模式外，IKE还定义了用于维护IKE SA的信息交换模式和用于协商新的密钥交换法的新组模式。

3 IPSec操作模式

IPSec对于AH头和ESP头应用于IP包有两种操作模式，即传输模式和隧道模式。通常传输模式用于两个主机间端到端的通信，如客户机和服务器间，该模式要求主机支持IPSec协议。而隧道模式通常用于一端或两端都是网关间的通信，如防火墙和路由器。使用隧道模式的网关，其服务的主机不需要实现IPSec就可安全通信。

3.1 传输模式

传输模式主要是为上层协议提供保护，AH或ESP包头被插在IP包头和IP包的上层协议（如TCP、UDP、ICMP）之间，如图4所示。

传输模式保护的IP分组包，其加密终点就是起通信终点，都是IP头中"目的地址"字段所指定的地址。源地址和目的地址都是可见的。

3.2 隧道模式

隧道模式对整个IP包进行加密，即把整个IP包封装起来，再加上一个新的IP头，如图5所示。

隧道模式保护的IP分组包，其通信终点在原IP头中指定，加密终点在新IP头中指定。通常加密终点是安全网关，通信终点是受安全网关保护的某个主机，该模式适于构建虚拟专用网（VPN）。隧道模式下通信目的地址对公共网不可见。实际应用中并不采用隧道模式中的AH，因为它保护的数据与传输模式中一样。隧道模式支持嵌套服务，即可对一个已经采用隧道模式保护的包再进行一次隧道保护。

值得注意的是两种模式下ESP尾的数据部分进行了加密和认证，事实上就是ESP中的为保证加密要求的"填充项"、"填充项长度"和"下一个头"字段。ESP尾中没有加密的部分即是"身份认证数据"字段，用于存放数据完整性的检验结果。

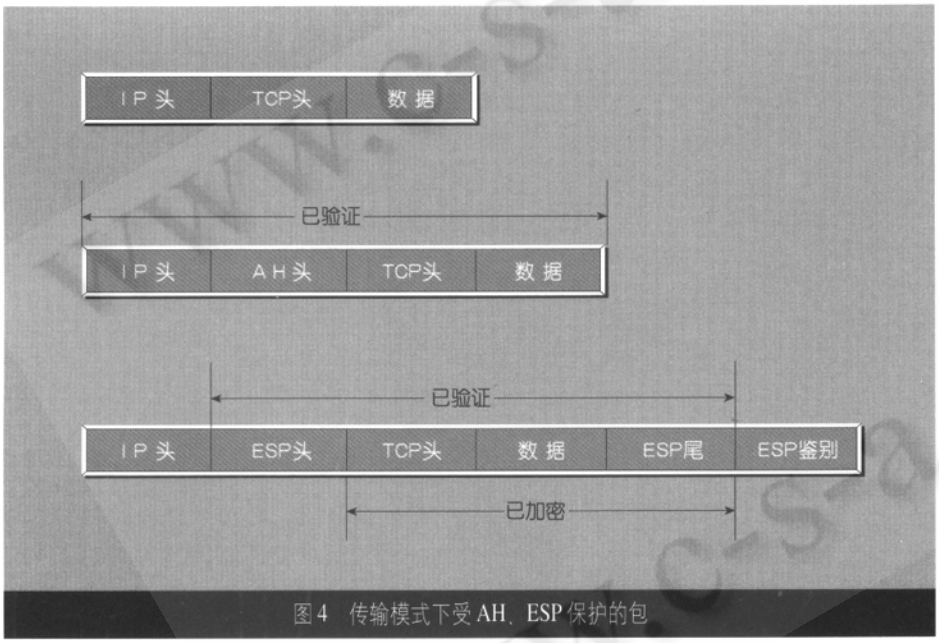

图4 传输模式下受AH、ESP保护的包

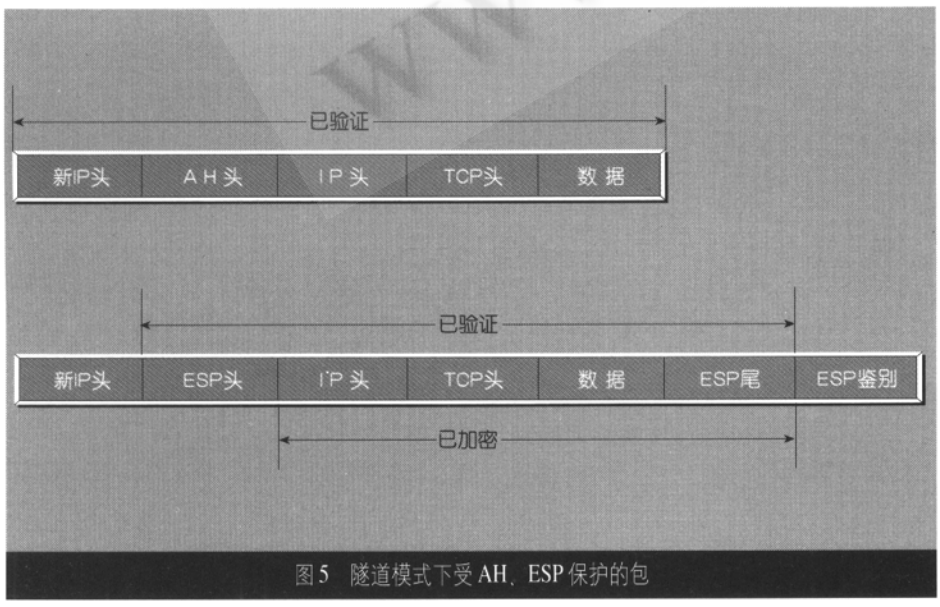

图5 隧道模式下受AH、ESP保护的包

4 典型应用

IPsec的一种典型应用如图6所示，即基于IPsec构建了虚拟专用网（VPN），包括远程访问虚拟网（AccessVPN）、企业内部虚拟网（IntranetVPN）和企业扩展虚拟网（ExtranetVPN），这三种类型的VPN分别与传统的远程访问网络、企业内部的Intranet以及企业网和相关合作伙伴的企业网所构成的Extranet相对应。利用公共Internet网构建VPN，节省了租用专用线路和维护远程访问设备的昂贵开支，却达到了同样的安全保护目的，且易于扩展，可随时随地与访问方通信。

图中"安全网关"便是实现IPsec协议的设备，可以是路由器或防火墙。"安全网关"之间采用隧道模式通信。认证机构是获得公众广泛信任的机构，发放将一个用户与一个公共密钥对"绑定"的证书，用于安全网关协商SA时验证对方身份。本应用中SPD集中存放在策略服务器中，以便于集中管理，SPD必须合理配置才能保证VPN系统的安全通信。

IntranetVPN是进行企业内部各分支机构的互联的很好方式，越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公

司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线，显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵，利用基于IPsec的VPN可以在Internet上组建世界范围内的IntranetVPN，利用Internet的线路保证网络的互联性，而利用隧道、加密等特性可以保证信息在整个IntranetVPN上安全传输。企业希望提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时各个企业之间的合作关系也越来越多，信息交换日益频繁，基于IPsec的ExtranetVPN将客户、供应商、合作伙伴连接到企业内部网，既可向其提供有效的信息服务，又可以保证自身的内部网络的安全。AccessVPN最适用于公司内部经常有流动人员远程移动办公的情况，可使移动用户随时、随地以其所需的方式访问企业资源，但用户必须配置IPsec相关组件，且其安全策略不能依据IP地址配置，如可基于"名字"配置。

5 结束语

IPSec是一种标准的、健壮的、可扩充的机制，它在网络层及上层协议实现对IP包的机密性、完整性、身份验证及抗重播等安全保护，是IP协议的扩充，为IP提供"无缝"的安全保证。Internet对安全性的迫切要求，促使了IPSec技术的快速应用，目前已有多家厂商在努力通过多种途径实现IPSec，如在操作系统中、安全网关中通过软、硬件来实现。利用IPsec构建VPN使企业以最少的投资获得最大的安全通信。IPSec也仍在改进和完善中，如基于非IP协议的IPSec、IPSec的多播源验证和密钥管理等方面。

参考文献

1 Doraswamy Naganand, Harkins Dan. IPSec: the new security standard for the Internet, Intranet and virtual private networks. Prentice Hall. 1999.

2 S Kent, and R Atkinson. RFC 2401: Security architecture for the Internet protocol. November 1998.

3 S Kent, and R Atkinson. RFC 2402: IP Authentication Header. November 1998.

4 Kent, and R Atkinson. RFC 2406: IP Encapsulating Security Payload (ESP). November 1998.

5 Carrel Dave, Harkins Dan. RFC2409: The Internet Key Exchange.1998.

6 Maughan D, Schertler M, Turner J. RFC2408: Internet Security Association and Key Management Protocol. 1998.

7 Piper D. RFC2407: The Internet IP Security Domain of Interpretation for ISAKMP. 1998.

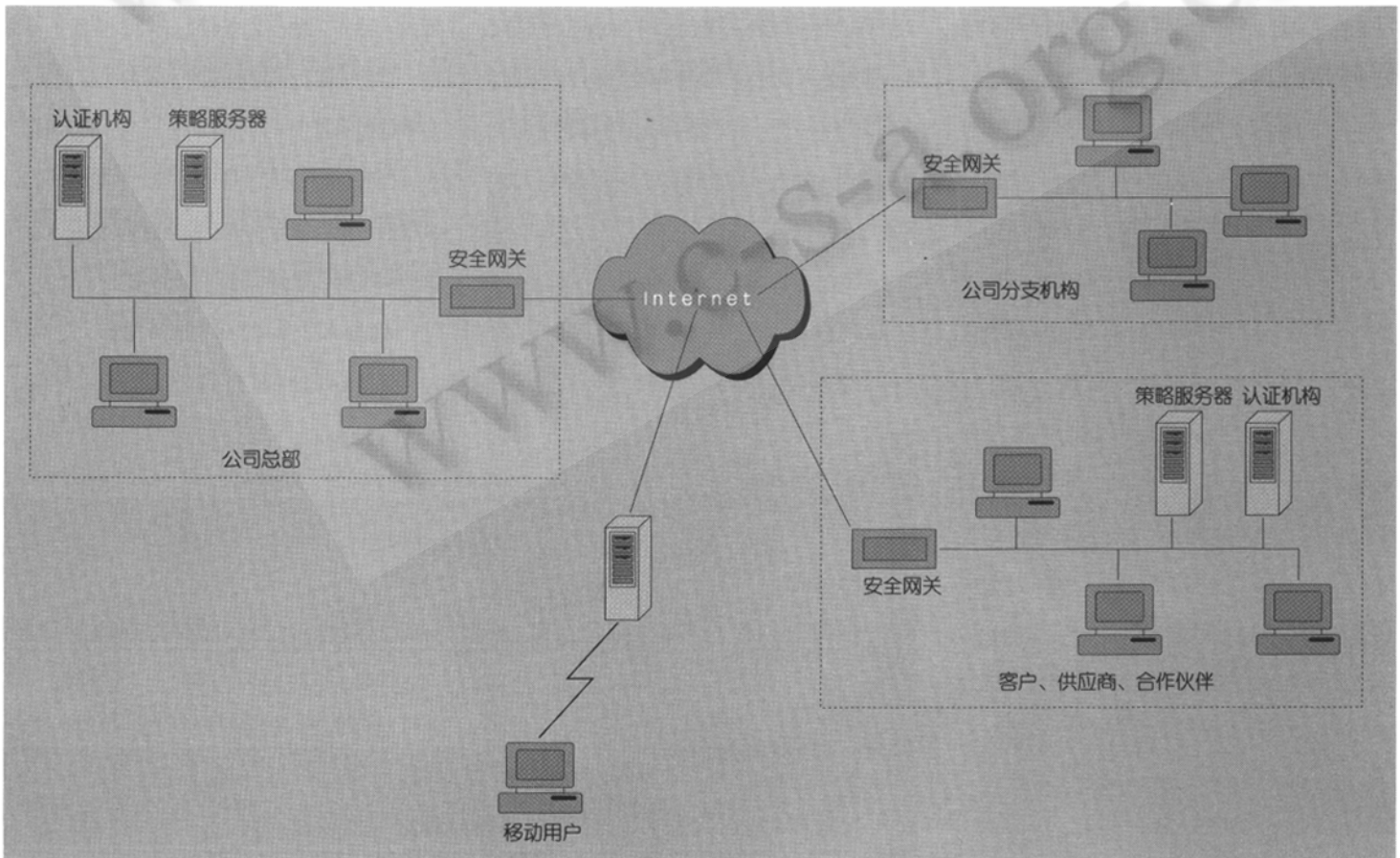

图6 IPSec典型应用