Abstract

The article first introduced the IPv6 network related background and the technology, and have analyzed the security agreement and the IPSec security ability, the security system constitution of IPv6; And detail introduced IPSec basic agreement authentication expansion text of a telegram (AH) and safe seal load text of a telegram (ESP); The system other parts of IPv6 security, example, the security policy、the encryption and the authentication algorithm, the key management and so on, the article discussed how them to work, they match each other to protect the IPv6 network of security. And analyzed current IPv6 network existence some loopholes and the flaw, as well as some traditional security tools under IPv6 improvement, has simultaneously introduced the safe audit and the risk analysis theory constructs in the next generation network dynamic security model; Finally has carried on the analysis to the IPv6 firewall realization protection network security, has produced in the firewall in a realization protection module, had to the firewall in IPv6 network protective measure had further understood. The article conclusion has carried on the forecast to the IPv6 development, and some questions which needs to improve to the next generation network in have carried on the induction summary, explained the research goal and the harvest , it was clear about the constructed the new security model for the next generation security extremely importantly to send the significance.

Key words: IPv6, IP Sec, Secure Network, AH, APPDRR, Firewall

声　明

本学位论文是我在导师的指导下取得的研究成果，尽我所知，在本学位论文中，除了加以标注和致谢的部分外，不包含其他人已经发表或公布过的研究成果，也不包含我为获得任何教育机构的学位或学历而使用过的材料。与我一同工作的同事对本学位论文做出的贡献均已在论文中作了明确的说明。

研究生签名：[illegible]　　2007 年 7 月 9 日

学位论文使用授权声明

南京理工大学有权保存本学位论文的电子和纸质文档，可以借阅或上网公布本学位论文的部分或全部内容，可以向有关部门或机构送交并授权其保存、借阅或上网公布本学位论文的部分或全部内容。对于保密论文，按保密的有关规定和程序处理。

研究生签名：[illegible]　　2007 年 7 月 9 日

1 绪论

在当前计算机网络飞速发展的步伐下，IPv4 的局限性和缺点越发明显，TCP/IP 的工程师和设计人员在 20 世纪 80 年代初期就意识到了到了对 IPv4 的升级需求，因为当时已经发现 IP 地址空间随着 Internet 的发展只能支持很短时间，过去几年中 IPv4 地址资源的紧缺引发了一系列安全问题，尽管 IPv6 协议在网络安全上做了多项改进，但是其引入也带来了新的安全问题。由于我国 IPv4 地址资源严重不足，除了采用 CIDR、VLSM 和 DHCP 技术缓解地址紧张问题，更多的是采用私有 IP 地址结合网络地址转换(NAT/PAT)技术来解决这个问题。比如 PSTN、ADSL、GPRS 拨号上网、宽带用户以及很多校园网、企业网大都是采用私有 IPv4 地址，通过 NAT 技术接入互联网，这不仅大大降低了网络传输的速度，且安全性等方面也难以得到保障。从根本上看，互联网可信度问题、端到端连接特性遭受破坏、网络没有强制采用 IP Sec 而带来的安全性问题，使 IPv4 网络面临各种威胁。

IP 安全协议[1](IP Sec) IP Sec 是 IPv4 的一个可选扩展协议，而在 IPv6 则是一个必备组成部分。IP Sec 协议可以“无缝”地为 IP 提供安全特性，如提供访问控制、数据源的身份验证、数据完整性检查、机密性保证，以及抗重播(Replay)攻击等。新版路由协议 OSPFv3 和 RIPng 采用 IP Sec 来对路由信息进行加密和认证，提高抗路由攻击的性能。需要指出的是，虽然 IP Sec 能够防止多种攻击，但无法抵御 Sniffer、DoS 攻击、洪水(Flood)攻击和应用层攻击。

IPv6 协议确实比 IPv4 的安全性有所改进，IPv4 中常见的一些攻击方式，将在 IPv6 网络中失效，例如网络侦察、报头攻击、 ICMP 攻击、碎片攻击、假冒地址、病毒及蠕虫等。但数据包侦听、中间人攻击、洪水攻击、拒绝服务攻击、应用层攻击等一系列在 IPv4 网络中的问题， IPv6 仍应对乏力，只是在 IPv6 的网络中事后追溯攻击的源头方面要比在 IPv4 中容易一些。IPv6 是新的协议，在其发展过程中必定会产生一些新的安全问题，主要包括应对拒绝服务攻击(DoS)乏力、包过滤式防火墙无法根据访问控制列表 ACL 正常工作、入侵检测系统(IDS)遭遇拒绝服务攻击后失去作用、被黑客篡改报头等问题。

向 IPv6 迁移的可能漏洞 由于 IPv6 与 IPv4 网络将会长期共存，网络必然会同时存在两者的安全问题，或由此产生新的安全漏洞。已经发现从 IPv4 向 IPv6 转移时出现的一些安全漏洞，例如黑客可以使用 IPv6 非法访问采用了 IPv4 和 IPv6 两种协议的 LAN 的网络资源，攻击者可以通过安装了双栈的使用 IPv6 的主机，建立由 IPv6 到 IPv4 的隧道，绕过防火墙对 IPv4 进行攻击。向 IPv6 协议的转移与采用其他任何一种新的网络协议一样，需要重新配置防火墙，其安全措施必须经过慎重的考虑和测

试，例如 IPv4 环境下的 IDS 并不能直接支持 IPv6，需要重新设计，原来应用在 IPv4 协议的安全策略和安全措施必须在 IPv6 上得到落实。目前，IPv4 向 IPv6 过渡有多种技术，其中基本过渡技术有双栈、隧道和协议转换，但目前这几种技术运行都不理想。

由此可见，分析和研究 IPv6 在网络运行的安全问题非常重要，可以为 IP Sec 的制定提供完善的数据和可靠保证。

1．1 课题研究背景

在我国 IPv6 的发展主要是教育网的发展，带动下一代网络的发展， 目前，CERNET2 试验网以 2.5G 的速度连接北京、上海和广州三个 CERNET2 核心节点，并与国际下一代互联网相连接，开始为清华大学、北京大学、上海交通大学等一批“IPv6 常青藤”高校提供高速 IPv6 服务。它的开通也标志着中国学术互联网的 IPv6 之路已经踏上征程。

国外对 IPv6 网络安全的研究起步较早，已经有了一些基于 IPSec 的试验 VPN，但大都是在专用的平台下实现，与操作系统绑定得都比较紧密，有的甚至就是一个黑盒子。关于不同的 IP Sec 实现间的互操作性，目前还有令人满意的测试报告。具有代表性的有完善 IPv6 中 KAME 计划，IKE 中的 AES－CBC Cipher， AES－XCBC－PRF－128 等算法以及在 VPN 方面应用研究。

国内对 IPv6 网络安全研究还处于初期，主要是在理论方面，完整地实现了 IPSec 整个协议的安全产品还比较缺乏。研究单位主要是北京邮电大学和中国科技大学。研究领域集中在 AES 算法，JFK 协议，Ad Hoc 网络安全系统，VPN 防御 DOS 攻击，IP Sec-NAT 兼容性穿越技术，移动 IPv6，嵌入式 VPN 安全以及 IP 多媒体网络等方面。

1．2 IPv6 网络存在的安全问题

目前，IPv6 网络存在的安全问题[2]主要有如下几个方面：

1. IP 网中许多不安全问题主要是管理造成的。IPv6 的管理与 IPv4 在思路上有可借鉴之处。但对于一些网管技术，如 SNMP 等，不管是移植还是重新另搞，其安全性都必须从本质上有所提高。由于目前针对 IPv6 的网管设备和网管软件几乎没有成熟产品出现，因此缺乏对 IPv6 网络进行监测和管理的手段，缺乏对大范围的网络故障定位和性能分析的手段。没有网管，何谈保障网络高效、安全运行?

2. PKI 管理在 IPv6 中是悬而未决的新问题；

3. IPv6 网络同样需要防火墙、VPN、IDS、漏洞扫描、网络过滤、防病毒网关等

网络安全设备。事实上 IPv6 环境下的病毒已经出现。这方面的安全技术研发还尚需时日；

4. IPv6 协议仍需在实践中完善，例如 IPv6 组播功能仅仅规定了简单的认证功能，所以还难以实现严格的用户限制功能，而移动 IPv6(Mobiel IPv6)也存在很多新的安全挑战。DHCP 必须经过升级才可以支持 IPv6 地址，DHCPv6 仍然处于研究、制订之中。

1．3 IPv6 网络安全研究意义

IPv6 网络安全主要是以 IPSec 作为基石，IPv6 和 IPv4 相比具有诸多优势:地址空间巨大，支持分级路由结构，能进行有状态和无状态的地址培植，具有内置的安全策略(IPSec)，能更好地支持 QoS 以及具有良好的可扩展性等等。2003 年 10 月中国宣布即将启动 CNGI 项目(中国下一代互联网项目)，并在 2005 年底建成世界上最大的 IPv6 网。CNGI 项目将成为整个 IPv6 产业部署进程的孵化器和助推器。在这种国家大力支持的大好形势下，利用我们自身的科研资源和条件，努力抓住发展契机，搭建 IPv6 的实验环境，做一些 IPv6 的研究，推动 IPv6 的应用，为 IPv6 即将到来大规模商用做好技术储备是非常必要和有意义的。而且，现有安全体系并不能完全适应 IPv6 的许多新的应用。随着 IPv6 的迅速发展，基于 IPv6 的下一代互联网的安全性研究就更加突显重要，切实地研究出新的安全方案以解决 IPv6 和现有安全体系的兼容性问题，在当前已成为了非常迫切的事。

1．4 本文研究内容

本文是在南京理工大学与 CERNET2 试验网成功连接及下一代网络 IPv6 实验室建设的基础上，全面认识下一代网络发展情况，联系目前的网络安全技术，分析了 IPv6 网络运行的安全体系，并指出了下一代网络安全研究中的意义。详细介绍了 IPSec 各部分如 AH、ESP、IKE 及 SA 等；并构建了下一代的网络安全模型，然后，介绍传统的防火墙在 IPv6 网络环境下需要做出的一些的改进，并利用在 IPv6 环境中防火墙针对地址限制的一个模块利用数据报头分析的技术实现在地址限制；最后对以后 IPv6 网络的发展存在的问题提出了一些建议，并对以后 IPv6 在校园网建设方面进行展望。

1．5 本文结构

第一章 绪论。主要介绍了本课题研究的背景，以及 IPv6 网络安全在国内外的研

究进展与应用情况，并对下一代网络安全通信协议IP Sec的实验的意义进行了概述，最后对本文研究内容和文章结构进行了介绍。

第二章 IPv6网络技术。主要介绍了IPv6的发展，对IPv6的发展进行了概述，然后对IPv4和IPv6进行了对比分析，并对IPv6优点进行了总结。最后对国内外IPv6的发展做介绍。

第三章 基于IP SEC的IPv6安全机制。分析了IPv6的安全协议IP Sec的安全能力、IP Sec的安全体系的构成、IP Sec的工作方式。论述了IP Sec在IP报文的完整性、机密性、数据来源谁和抗重播等方面的能力，IP Sec 的基本协议：认证扩展报头（AH）和安全封装载荷报文头（ESP）与IP Sec安全体系的其它组成部分如安全策略、加密和认证算法、密钥管理等如何合作，共同完成了对IP报文的安全保护。这些合IP Sec成为完整的网络层协议，对IPv6网络安全的提供了有效保证。

第四章 IPv6网络运行中的安全防御体系。详细阐述了在IPv4向IPv6过渡时期一些安全工具如何实现改进的，对网络安全保障作用，在原有模型APPDRR网络安全模型的基础上加入了新的安全审计和IP Sec安全体制，构建了新一代网络安全模型。

第五章 基于防火墙对IPv6的安全研究。主要介绍了传统防火墙在IPv6网存在的问题，针对三种不同的防火墙的架构模式进行了分析，并根据下一代网络要求提出了改进方法。

第六章 基于IP地址限制的IPv6防火墙实现。主要对防火墙程序中的一个模块进行了阐述，主要的功能是实现对前后两个IP地址进行实时对比，从而实现对子网的保护。

第七章 结论。对研究分析试验中的不足之处进行归纳总结，说明研究目的与收获，并对IPv6网络安全进行了展望。并对下一步IPv6需要解决的问题，提出了自己的看法和观点。

2 IPv6网络技术

2.1 IPv6发展概述

随着互联网的迅速发展，使用Internet技术的TCP/IP协议取得了巨大的成功。但是，TCP/IP协议的研制者设有预料到Internet的规模会发展到今天这么大，从而使得现有的TCP/IP协议面临许多困难。1987年，人们便预计在1996年Internet将接入100,000个网络，这一预测看来是准确的。此外，虽然目前使用的32位IPv4地址结构能够支持40亿台主机和670万个网络，实际的地址分配效率，即使从理论上说也远远低于以上数值。使用A、B和C类地址，使这种低效率的情形变得更为严重。

自八十年代后期，研究人员开始注意到了这个问题，并提出了研究下一代IP协议的设想。1990年，人们预计，按照当时的地址分配速率到1994年3月B类地址将会用尽，并提出了最简单的补救方法：分配多个C类地址以代替B类地址。但这样做也带来新的问题，即进一步增大了已经以惊人的速度增长的主干网路由器上的路由表。因此，Internet网络界面临着困难的选择，或者限制Internet的增长率及其最终规模，或者采用新的技术。

1990年后期，IETF开始了一项长期的工作，选择接替现行IPv4的协议。此后，人们开展了许多工作，以解决IPv4地址的局限性，同时提供额外的功能。1991年11月，IETF组织了路由选择和地址工作组(ROAD)，以指导解决以上问题。1992年9月，ROAD工作组提出了关于过渡性的和长期的解决方案建议，包括采用CIDR路由聚集方案以降低路由表增长的速度，以及建议成立专门工作组以探索采用较大Internet地址的不同方案。

1993年末，IETF成立了IPNG工作部，以研究各种方案，并建议如何开展工作。该工作部制订了IPng技术准则，并根据此准则来评价已经提出的各种方案。在经过深入讨论之后，SIPP(Simple Internet Protocol Plus)工作组提供了一个经过修改的方案，IPng工作部建议IETF将这个方案作为IPng的基础，称为IPv6，并集中精力制定有关的文档。自1995年末起，陆续发表了IPv6规范等一批技术文档。

2.2 IPv4和IPv6的特点

20世纪的互联网协议随着移动互联网、语音/数据的集成以及嵌入式互连设备的

快速发展，以互联网为核心的未来通信模式正在形成。到目前为止，互联网取得了巨大的成功，而这很大程度上归功于其核心通信协议 IPv4 的高度可伸缩性。IPv4 的设计思想成功地造就了目前的国际互联网，并容纳了过去十年中网络规模的几何级数增长，其核心价值体现在简单、灵活和开放性等方面。但是，新应用的不断涌现使互联网呈现出新的特征，传统的互联网协议版本，即 IPv4，已经难以支持互联网的进一步扩张和新业务的特性，比如实时应用和服务质量保证。

对于 IPv4 和 IPv6，其特点比较[2]可见如下：

1．IPv4 的特点

IPv4 的报头格式如图 2.1 所示。

<table>
<tr><td>版本号
(4bit)</td><td>头 标 长 度
(4bit)</td><td>服 务 类 型
(8bit)</td><td>数据包长度(16bit)</td></tr>
<tr><td colspan="3">标识（16bit）</td><td>df mf 标准偏移量</td></tr>
<tr><td>生存时间
(8bit)</td><td colspan="2">传输协议（8bit）</td><td>头标校验和（16bit）</td></tr>
<tr><td colspan="4">发送地址（32bit）</td></tr>
<tr><td colspan="4">信宿地址（32bit）</td></tr>
<tr><td>选项(8bit)</td><td colspan="2">……</td><td>填充</td></tr>
</table>

图 2.1 IPv4 的报头格式

IPv4 的特点[12]体现在以下方面：

（1）有限的地址空间 IPv4 协议中每一个网络接口由长度为 32 位 IP 地址标识，这决定了 IPv4 的地址空间为 232，大约理论上可以容纳 43 亿个主机，这一地址空间难以满足未来移动设备和消费类电子设备对 IP 地址的巨大需求量。加之存在地址分配的大量浪费，有预测表明，以目前 Internet 发展速度计算，所有 IPv4 地址将在 2005～2010 年间分配完。

在二十世纪九十年代的研究人员已经意识到了 IP 地址空间以及分配存在的问题，并开发了一些新技术来改善地址分配和减缓 IP 地址的需求量，比如 CIDR 和 NAT。这些技术一定程度上缓解了地址空间被耗尽的危机，但为基于 IP 的网络增加了复杂性，并且破坏了一些 IP 协议的核心特性，比如端到端原则，因此不能从根本上解决 IPv4 面对的困难。

（2）路由选择效率不高 IPv4 的地址由网络和主机地址两部分构成，以支持层次型的路由结构。子网和 CIDR 的引入提高了路由层次结构的灵活性。但由于历史的原因，IPv4 地址的层次结构缺乏统一的分配和管理，并且多数 IP 地址空间的拓扑结构只有两层或者三层，这导致主干路由器中存在大量的路由表项。庞大的路由表增加了

路由查找和存储的开销，成为目前影响提高互联网效率的一个瓶颈。同时，IPv4 数据包的报头长度不固定，因此难以利用硬件对提取、分析路由信息，这对进一步提高路由器的数据吞吐率也是不利的。

（3）缺乏服务质量保证 IPv4 遵循 Best Effort 原则，这一方面是一个优点，因为它使 IPv4 简单高效；另一方面它对互联网上涌现的新的业务类型缺乏有效的支持，比如实时和多媒体应用，这些应用要求提供一定的服务质量保证，比如带宽、延迟和抖动。研究人员提出了新的协议在 IPv4 网络中支持以上应用，如执行资源预留的 RSVP 协议和支持实时传输的 RTP/RTCP 协议。这些协议同样提高了规划、构造 IP 网络的成本和复杂性。

IPv6 是 Internet 协议的一个新版本，其设计思想是对 IPv4 加以改进，而不是对其进行革命性的改造。在 IPv4 中运行良好的功能在 IPv6 中都给予保留，而在 IPv4 中不能工作或很少使用的功能则被去掉或作为选项。为适应实际应用的要求，在 IPv6 中增加了一些必要的新功能。

2. IPv6 的主要特点

IPv6 的报头格式如图 2.2 所示。

<table>
<tr><td>4bit 版本号</td><td>4bit 优先级</td><td>24bit 流量标识</td></tr>
<tr><td>数据长度 16bit</td><td>下一报头 8bit</td><td>跳数限制 8bit</td></tr>
<tr><td colspan="3">起始地址 128bit</td></tr>
<tr><td colspan="3">目的地址 128bit</td></tr>
</table>

图 2.2 IPv6 的报头格式

IPv6 的特点体现在以下方面：

(1) 经过扩展的地址和路由选择功能。IP 地址长度由 32 位增加到 128 位，可支持数量大得多的可寻址节点、更多级的地址层次和较为简单的地址自动配置。改进了多目(multicast)路由选择的规模可调性，因为在多目地址中增加了一个“Scope”字段。

(2) 定义了任一成员(anycast) 地址，用来标识一组接口，在不会引起混淆的情况下将简称“任一地址”，发往这种地址的分组将只发给由该地址所标识的一组接口中的一个成员。

(3) 简化的首部格式。IPv4 首部的某些字段被取消或改为选项，以减少报文分组处理过程中常用情况的处理费用，并使得 IPv6 首部的带宽开销尽可能低，尽管地址长度增加了。虽然 IPv6 地址长度是 IPv4 地址的四倍，IPv6 首部的长度只有 IPv4 首部的两倍。

(4) 支持扩展首部和选项。IPv6 的选项放在单独的首部中，位于报文分组中 IPv6

首部和传送层首部之间。因为大多数 IPv6 选项首部不会被报文分组投递路径上的任何路由器检查和处理，直至其到达最终目的地，这种组织方式有利于改进路由器在处理包含选项的报文分组时的性能。IPv6 的另一改进，是其选项与 IPv4 不同，可具有任意长度，不限于 40 字节。

(5) 支持验证和隐私权。IPv6 定义了一种扩展，可支持权限验证和数据完整性。这一扩展是 IPv6 的基本内容，要求所有的实现必须支持这一扩展。IPv6 还定义了一种扩展，借助于加密支持保密性要求。

(6) 支持自动配置。IPv6 支持多种形式的自动配置，从孤立网络节点地址的“即插即用”自动配置，到 DHCP 提供的全功能的设施。

(7) 服务质量能力。IPv6 增加了一种新的能力，如果某些报文分组属于特定的工作流，发送者要求对其给予特殊处理，则可对这些报文分组加标号，例如非缺省服务质量通信业务或“实时”服务。

总之，IPv6 高效的互联网引擎引人注目的是，IPv6 增加了许多新的特性，其中包括：服务质量保证、自动配置、支持移动性、多点寻址（Multicast）、安全性。

基于以上改进和新的特征，IPv6 为互联网换上一个简捷、高效的引擎，不仅可以解决 IPv4 目前的地址短缺难题，而且可以使国际互联网摆脱日益复杂、难以管理和控制的局面，变得更加稳定、可靠、高效和安全。

2.3 IPv6 数据报格式

IPv6 数据报[5]的首部虽然比 IPv4 首部长，但却大大地简化了。IPv4 首部中的一些功能被放在扩展首部中或取消了。

(1) 版本 (Version)。Internet 协议版本号，IPng 版本号为 6。(4 位字段)

(2) 流标号 (Flow Label)。如果一台主机要求网络中的路由器对某些报文进行特殊处理，如非缺省服务质量通信业务或实时服务，则可用这一字段对相关的报文分组加标号。(24 位字段)

(3) 负荷长度 (Payload Length)。IPv6 首部之后，报文分组其余部分的长度，以字节为单位。为了允许大于 64K 字节的负荷，如本字段的值为 0，则实际的报文分组长度将存放在逐个路段(Hop-by-Hop)选项中。(16 位无符号整数)

(4) 下一首部 (Next Header)。标识紧接在 IPv6 首部之后的下一首部的类型。下一首部字段使用与 IPv4 协议相同的值。(8 位选择字段)

(5) 路径段限制 (Hop Limit)。转发报文分组的每个节点将路径段限制字节值减一，如果该字段的值减小为零，则将此报文分组丢弃。(8 位无符号整数)

(6) 源地址。报文分组起始发送者的地址。(128 位字段)

(7) 目的地址。报文分组预期接收者的地址（如果有一个可选的路由选择首部，有可能不是最终接收者)。(128 位字段)

在 IPv6 中，Internet 层选项信息存放在单独的首部中，位于报文分组的 IPv6 首部和传送层首部之间。现已定义了几个这种扩展首部，各由一个下一首部值来标识，包括逐个路段路由选择、分片、验证、隐私权和端到端(End-to-End)等选项首部。

2．4 IPv4 和 IPv6 共存

针对目前 Internet 上的各种 IPv4 与 IPv6 之间通信的情况，人们已经开发出了许多有效的过渡机制[3]。

1．IPv6 的小岛之间通信的情况

针对这一类问题，又可以划分多种情况：

(1) 手工配置多条隧道，适用于具备双协议栈的站点（sites）之间通信。所谓站点，既可以是一台主机，也可以是一系列主机。

(2) 自动隧道配置如 Tunnel Broker，适用于具备双协议站的主机之间通信。

(3) 6to4 机制，适用于站点之间通信，为了实现这个机制，每个站点内部的主机可以仅仅配置 IPv6 协议栈，但是每个站点必须至少有一台"6to4"的路由器作为出入口，支持全球统一的 6to4 TLA（Top Level Aggregation）前缀格式，并实施特殊的封装和转发机制。

(4) 6over4 机制，适用于具备双协议栈的主机之间通信。它利用 IPv4 的 multicast 机制来创建虚拟链路而不是显式的隧道。

2．IPv6 小岛与 IPv4 海洋之间通信的情况

这一类问题下同样有多种情况，目前的过渡机制都是通过以下途径实现的：应用级转发；网络层翻译；为 IPv6 节点暂时分配 IPv4 地址。

(1) 双协议栈有限双协议栈，适用于具备双协议栈的站点的通信。

(2) Socks64（Socket 6 to 4）机制，适用于 IPv6 的站点和 IPv4 站点的通信。它实际上是一种网关的转发机制，实施 socks64 的网关为 IPv6 的节点提供分组的转发和翻译。

(3) SIIT（Stateless IP/ICMP Translator）机制，适用于 IPv6 的站点和 IPv4 站点的通信。它实际上在 IPv4 和 IPv6 的分组报头之间进行翻译，使用 IPv4 映射的 IPv6 地址进行通信。

(4) NAT-PT（Network Address Translation - Protocol Translation）机制，

适用于 IPv6 only 站点和 IPv4 only 站点之间的通信。它进行 IPv6 和 IPv4 地址之间的翻译。

(5) BIS (Bump-in-the-Stack) 机制，适用于具备双协议栈的主机与 IPv4 的世界通信。它在 IPv4 的协议栈中插入三个模块：域名解析器、地址映射器和翻译器。

3. 过渡过程的产生背景

IP 协议是互联网体系结构的核心，它必须具备相对的稳定性。IPv6 作为 Internet Protocol 的新版本，其根本目的是继承和取代 IPv4。因此，人们在规划 IPv6 的时候，就把眼光投向了包括地址在内的上述重要需求，希望能够解决这些目前已经出现和将来可能出现的问题。从 IPv4 到 IPv6 的改变将不可避免的带来 Internet 上新的革命，无论是硬件还是软件都将有全新的发展。但是，原有的 IPv4 协议已经成功的实施了将近二十年，在 Internet 上，甚至有许多通信协议标准比 Internet 还要早，Internet 协议和标准化是有一个简单的原则的[42]。

只要可以应用现有的协议标准，就使用它们；只有当现有的标准不够时才制定新的协议，而且只要能够得到这些新的标准，而它们又能够提供等价的功能，就使用这些新的标准。

所以 IPv6 协议的意图并不是排斥和避免已有的标准。它的产生只是因为传统的 IPv4 不能满足需要。在 IPv6 完全取代 IPv4 之前，不可避免的，这两种协议要有一个可能是相当长的共存时期，IPv6 可能需要在研究所和学术机构中进行足够的试验，才能像 IPv4 一样成功的投入商业运营。因此，从 IPv4 到 IPv6 要有一个过渡时期。

IPv6 在 IPv4 的基础上进行改进，它的一个重要的设计目标是与 IPv4 兼容。制订 IPv6 时，IETF 致力于产生一种开放的标准，因此他们邀请了许多团体来参加标准的制订过程，研究人员、计算机制造商、程序设计人员、管理人员、用户、电话公司以及有线电视产业都对下一代 IP 提出了他们的要求和建议。但是作为一种新的协议，从诞生于实验室和研究所到实际应用于 Internet 是有很大距离的。不可能要求立即将所有节点都演进到新的协议版本，所以在一定的时间内，IPv6 将和 IPv4 共同存在共同运行。如果没有一个过渡方案，再先进的协议也没有实用意义，因此从 IPv4 网络向 IPv6 网络过渡的问题从一开始就列入了开发者的日程表。

在相当时间内，IPv6 节点之间的通信还要依赖于原有 IPv4 网络的设施，而且 IPv6 节点也必不可少的要与 IPv4 节点通信，我们希望这种通信能够高效的完成，对用户隐藏下层细节。同时，IPv4 已经应用了十多年，基于 IPv4 的应用程序和设施已经相当成熟而完备，我们希望以最小的代价来实现这些程序在 IPv6 环境下的应用。所有这些都提出了从 IPv4 网络向 IPv6 网络高效无缝互连的问题。 对于过渡问题和高效无缝互连问题的研究已经取得了许多成果，形成了一系列的技术和标准。

2.5 国际IPv6网络的互联

一个纯IPv6网络的实现与原来IPv4网络并没有差别，在路由协议和域名解析上也不需要特定的机制来支持，仅仅需要对原来的协议和应用程序进行修改就可以了。但是对于一台主机或者一个网络在不同协议之间的通信来说，情况就发生了变化。由于报文在传输中要经过两种运行在不同协议下的网络环境，报文的翻译是一个问题，同时由于两种协议表示地址的方法不同，如何在协议地址之间标示信源和信宿也是必须处理的。

在IPv6的网络流行于全球之前，总是有一些网络首先具有IPv6的协议栈。这时，这些网络就像IPv4海洋中的小岛。过渡的问题可以分成如下两大类：

（1）第一类就是解决这些IPv6的小岛之间互相通信的问题；

（2）第二类就是解决IPv6的小岛与IPv4的海洋之间通信的问题。

解决过渡问题的两种最基本的技术：双协议栈（Dual Stack）和隧道（Tunnel）。我们所讨论的过渡机制（Transition Mechanism）都是在这两种技术的基础之上针对特定的问题的解决方案。但是目前还没有一种机制能够一劳永逸的解决这个问题，每一种具体的机制都是针对具体的情况的。

双协议栈 在实践当中最典型的是IETF提出的叫"双协议栈"的方案。需要提前说明的是，双协议栈技术并不具备创建隧道的能力；但是，后面提到的创建隧道的能力则必须要求有双协议栈技术的支持。

双协议栈方案的工作方式如下：

(1) 如果应用程序使用的目的地址是IPv4地址，则使用IPv4协议。

(2) 如果应用程序使用的目的地址是IPv6中的IPv4兼容地址，则同样使用IPv4协议，所不同的是，此时IPv6就封装（encapsulated）在IPv4当中。

(3) 如果应用程序使用的目的地址是一个非IPv4兼容的IPv6地址，那么此时将使用IPv6协议，而且很可能此时要采用隧道等机制来进行路由、传送。

(4) 如果应用程序使用域名作为目标地址，那么此时先要从DNS服务器那里得到相应的IPv4/IPv6地址，然后根据地址的情况进行相应的处理。

对目前的环境来说，要实现纯粹IPv6的路由是很困难的，因此，人们一般采用IPv6 over IPv4的点对点隧道技术。将IPv6分组打包，放入IPv4分组的数据区，加上IPv4的报头，在IPv4互联网世界中进行路由，到达目的地后再把数据区中的IPv6分组取出来做相应的处理，该继续路由的路由，该收发的收发。这样，就可以实现“双协议栈”的过渡方案。最后，对于实现IPv6协议栈，尽管在细节上，IPv6和IPv4有很大的不同，但是从原理和它们在网络体系结构中的位置来看，是相当的

一致的。这些一致使得开发人员只需要很小的付出就可以实现从IPv4到IPv6协议栈的转换。

隧道技术，就是将具有自身协议的复杂网络作为一般的硬件传输系统对待。前文已经提到，在IPv6的网络流行于全球之前，总是有一些网络首先具有IPv6的协议栈，这些网络就像IPv4海洋中的小岛，隧道就是通过"海底"连接这些小岛的通道，因此而得其名。由于隧道上的链路是逻辑的，或称为虚拟的，因此，这些“小岛”所互连而成的网络就被看作是一个虚拟网络。在IPv6 Native Network之间需要通信或IPv6节点需要与IPv4 的节点通信时，IPv4协议就被当作IPv6数据传输的一个隧道。通过隧道，IPv6分组被作为无结构无意义的数据，封装在IPv4数据报中，被IPv4网络传输。由于IPv4网络把IPv6数据当作无结构无意义数据传输，因此不提供帧自标识能力，所以只有在IPv4连接双方都同意时才能交换IPv6分组，否则收方会将IPv6分组当成IPv4分组而造成混乱。网络从IPv4向IPv6演进的过程就是这些“小岛”渐渐扩大而成为“大陆”的过程。

2．6 IPv6网络在中国的发展

随着IPv4地址空间耗尽的迫近，人们加紧了对下一代互联网协议即IPv6的研究；到2001年年初，IPv6协议的基本框架已经逐步成熟，在越来越广泛的范围内得到实践。由于IPv6和IPv4在协议头格式上不兼容，IETF成立了专门的工作组--ngtrans研究从现有的IPv4网络向IPv6网络的过渡策略和必要的技术。作为向下一代互联网络协议过渡的重要步骤，国际的IPv6试验网--6bone在1996年成立了。现在，6bone已经扩展到全球50多个国家和地区，成为IPv6研究者、开发者和实践者的主要平台。

中国教育和科研计算机网CERNET是中国开展下一代互联网研究的试验网络，它以现有的网络设施和技术力量为依托，建立了全国规模的IPV6试验床[3]。1998年CERNET正式参加下一代IP协议（IPv6）试验网6BONE，同年11月成为其骨干网成员。CERNET在全国第一个实现了与国际下一代高速网INTERNET2的互联，目前国内仅有CERNET的用户可以顺利地直接访问INTERNET2。为致力于面向21世纪网络技术的个人和团体提供全真的网络平台，用于研究同下一代互联网有关的网络技术，特别是安全、服务质量和移动计算；开发新型的网络应用，这些应用在传统的互联网上是几乎不可能或不易实现的；示范上述技术和应用，以及从传统的互联网向下一代网络过渡的方法。总体拓扑试验床分成相对独立而又互连互通的两个部分：正式使用部分和生实验部分。

试验床从6bone获得p-TLA (pseudo-Top Level Aggregation,伪顶级聚类)

3FFE:3200::/24 的地址空间；并且建立了 5 条以 tunnel 为基础的国际 IPv6 虚拟链路，直接通达美国、英国和德国的 IPv6 网络，间接地与几乎所有现有的 6bone 成员互连。试验床按地区分配 NLA1 ID (Next Level Aggregation, level 1 Identifier，次级聚类)。目前，试验床正式使用部分已经发展了 2 个地区级的试验网络；学生试验部分已经建立了 4 个地区 IPv6 网络。

目前，中国是全球最关心 IPv6 发展的国家之一，最主要的原因恐怕就是中国互联网对 IP 地址的渴求了。据统计，我国目前网民的数量已经激增到 2650 万，而总共申请到的 IP 地址却只有约 900 万个。与此形成鲜明对比的是，仅仅是美国斯坦福大学，所能使用的地址数量就已经达到了 2650 万个；IBM 公司则达到 3300 万。因此 IP 地址的短缺对于中国来说，显得尤其紧迫和尖锐。同样由于历史的原因，在技术研究、标准制订、产品开发等诸多方面中国也远远落后于美国。而 IPv6 为中国的互联网事业提供了一个缩小差距的良机。

IPv6 的地址长度和分配方案以一个世界性的网络为出发点，中国将会分配到足够的 IPv6 地址。IPv4 地址缺乏、庞大的人口基数和互联网的迅速扩张使中国更容易首先接受 IPv6，这将转化为一种优势，IPv6 将首先在中国广泛应用，从而推动 IPv6 研究、产品开发和应用的全面进步，使中国在下一代国际互联网的竞争中处于有利位置。

一旦 IPv6 在中国普及推广开来，首先，人们不用再为缺少地址而费尽心机地想出各种替代方法，以牺牲很多 IP 协议所提供的优良功能为代价了。那时，每人都将拥有一个或多个 IP 地址，配备上相应的计算机设备，无论你在天涯海角，都可以做到随时在线，连接全球。其次，IPv6 与移动通信的结合将为目前的互联网开拓一个全新的领域——移动互联网。通过移动互联网，使我们能够在移动中购买商品和服务，我们的移动设备将成为无线钱包，使我们能够随时随地以在线方式选购商品或服务，并为之付款。我们能够使用移动设备查询飞机的航班，风景点的简要情况，以便做出最后的安排；我们还能够利用同一设备查找地图以及要参观的地方；我们还能够找到距离我们最近的餐馆；如果是平时，我们驾车外出，安装在我们汽车里的无线设施将提供实时定位技术，同时也起到导航和安全保护的作用。

此外，在不远的未来，中国的家电厂商们将开发出新一代的信息家电，即我们除了计算机之外，还可给电视机、冰箱、微波炉、空调、洗衣机等家用电器分配固定地址，以利于它们与 Internet 的连接。在信息家电与 Internet 连接后，外出的人就可操作家中的空调、冰箱等，比如，可以通过网络下载做菜方式，自动设定温度和作业时间，减少做菜的手续。

最后，实行 IPv6 协议可以从根本上优化路由器传输效率，使得目前的各种宽带传输技术迈上一个新的台阶。到那时，困扰中国网民很久的网络速度问题，将得到彻

底解决，人们就可以舒舒服服呆在家里，享受超高速网络所带来的欢乐。信息家电连上光纤后，更可直接以交互方式收看电影、听音乐和广播。股民即使在家中，也能通过光纤网络和证券公司等金融机构的业务员在电视上交谈，同时进行交易。

3 基于 IPSec 协议的 IPv6 安全机制

基于 IPSec 协议的 IPv6 安全机制 [32] 如图 3.1 所示。

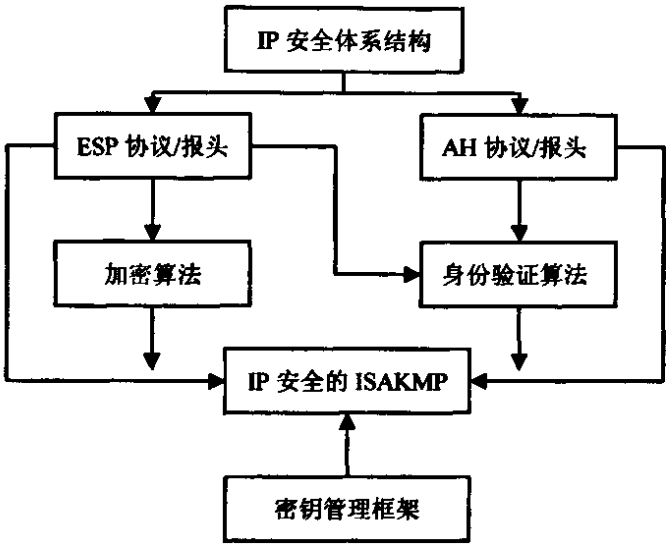

图 3.1 IP Sec 组成部分之间的关系（RFC2411）

3.1 IP 安全（IP security）

IPv6 标准规定：IPv6 的实现遵循 Internet 协议（RFC1825）的安全体系结构[4]。IPv6 提供一个安全机制和一系列安全服务支持，如数据认证、完整性验证、IP 控制层加密这几个方面。IP Sec 的一个最基本的优点是它可以在共享网络访问设备，甚至是所有的主机和服务器上完全实现，这很大程度避免了升级任何网络相关资源的需要。在客户端，IP Sec 架构允许使用在远程访问边界路由器或基于纯软件方式使用普通 MODEM 的 PC 机和工作站。通过传送模式和隧道模式在应用上提供更多的弹性。

（1）传送模式：在远程计算机间直接执行 IP 安全服务。它提供对上层协议和特定 IP 头部域日保护。传送模式通常当 ESP 在一台主机（客户机或服务器）上实现时使用，传送模式使用原始明文 IP 头，并且只加密数据，包括它的 TCP 和 UDP 头。

（2）隧道模式：通过中间系统执行 IP 数据包压缩。适用于主机间、安全网关、或二者之间传输，隧道模式将包括携带着最终源和目的的 IP 地址头部，以及 IP 数据报，整个封装起来,即处理整个 IP 数据包：包括全部 TCP/IP 或 UDP/IP 头和数据，它用自己的地址作为源地址加入到新的 IP 头。当隧道模式用在用户终端设置时，它可以提供更多的便利来隐藏内部服务器主机和客户机的地址。

IP 数据包见图 3.1.1，两种模式的示意图如图 3.1.2 和 3.1.3 所示。

Original IP Header IPv4 or IPv6	Payload : TCP/UDP

图 3.1.1 IP 数据包

Original IP Header IPv4 or IPv6	ESP Header	Encrypted payload(TCP/UDP)	ESP Trailer	Authentication Data

图 3.1.2 传输模式

Original IP Header IPv4 or IPv6	ESP Header	Original IP header	Encrypted payload(TCP/UDP)	ESP Trailer	Authentication Data

图 3.1.3 隧道模式

IPSec 在 IP 数据包中的原始报头和传送报头中添加一个报头，通过 ESP 数据加密，一种新的数据包标记被加入。加密前的 IP 数据包格式和加密后的 IP 数据包格式分别见图 3.1.4 和 3.1.5。

Original IP Header IPv4 or IPv6	Payload : TCP/UDP/Tunneled IP

图 3.1.4 加密前的 IP 数据包格式

Original IP Header IPv4 or IPv6	IP Security Header	Data(maybe encrypted):TCP/UDP/Tunneled IP	IP Security Trailer

图 3.1.5 加密后的 IP 数据包格式

3.2 IP Sec 的四种功能

与 IPv4 相比，IPv6 具有许多优势。首先，IPv6 解决了 IP 地址数量短缺的问题；其次，IPv6 对 IPv4 协议中诸多不完善之处进行了较大的改进。其中最为显著的就是将 IP Sec 集成到协议内部，从此 IP Sec 将不再单独存在，而是作为 IPv6 协议固有的一部分贯穿于 IPv6 的各个领域。

IP SEC提供如下四种不同的形式来保护通过公有或私有IP网络来传送的私有数据[16]：

安全关联（Security Associations，简称SA）；

IP认证头（Authentication Header，简称AH）；

IP封装安全载荷（Encryption and authentication known as Encapsulating Security Payload，简称ESP)；

密钥管理（Key management)。

3.2.1 安全关联(Security Association(SA))

IP Sec中的一个基本概念是安全关联(SA)，是在一次通信中的关联对象（SA）和通信策略。决定了输入和输出业务的AH和ESP机制的控制方式，即安全关联包含验证或者加密的密钥和算法。

一个SA是二个或更多通信实体间的关系或合同，描述是是这些通信实体如何用安全服务方式来进行安全。一次通信对话过程中涉及的所有对象必须都同意这个共享的合约—SA。一种安全关联(SA)能指明如下关系：使用的(加密)算法，认证和加密中的密钥。密码，发信者和接收必须同意的一种密钥，同样的认证或加密算法，以及算法中使用同样的附加参数(这样才相互通信)。

SA是单向连接，为保护两个主机或者两个安全网关之间的双向通信需要建立两个安全关联。SA将密钥和安全机制分离开业，安全关联中密钥管理和唯一作用是更新SA中的变量，能及全用这些变量的其它安全机制。IP的安全协议规定，唯一将使用中的密钥管理协议和安全协议联系起来的是安全参数索引SPI。安全关联提供的安全服务是通过AH和ESP两个安全协议中的一个来实现的。如果要在同一个通信流中使用AH和ESP两个安全协议，那么需要创建两个（或者更多）的安全关联来保护该通信流。一个安全关联需要通三个参数进行识别，它由安全参数索引（AH/ESP报头的一个字段)、目的IP地址和安全协议（AH或者ESP）的安全关联来保护该通信流。一个安全关联需要通三个参数进行识别，它由安全参数索引（AH/ESP报头的一个字段)、目的IP地址和安全协议（AH或者ESP）三者的组合唯一标识。

表3.2.1.1列出AH和ESP报头在传送模式和隧道模式下的区别。

1．安全策略

所谓安全策略[32]，就是控制IP安全机制的使用以及选择合适的安全关联。一种安全关联既可以是面向主机的，也可以是面向用户的。面向主机的SA支持对所有在同一主机范围内的用户，用同一种会话密钥。面向用户的密钥，所有用户的话密钥不一样。

适当的安全策略能决定某种安全关联是面向主机还是面向用户。如果给数据报选择了正确的安全关联和安全参数索引，那么执行一次安全策略，就定义了实话该安全

策略的各变量。安全关联和安全策略记录的结合，组成了一次通信过程的安全内容。

表 3.2.1.1 AH 和 ESP 报头在传送模式和隧道模式下的区别

	传输模式	隧道模式
AH	基本 IP 报头和扩展报头	原始的 IP 数据包外面封装新 IPv6 报头和 AH
ESP	压缩数据包和 IPv6 扩展 ESP 报头	ESP 报头
带 AH 的 ESP	ESP 报头和 AH 扩展报头	

2. 安全关联通信会话

一个用户接入安全关联的属性。用 SPI 表示，SPI 在密钥交换过程中确定。主面利用发送给用户的身份标记 ID 和目的地址，来选择这次通信的安全关联中的 SPI。目的地址可以是单播地址，也可以是多播地址。接收端的主机用沿着目的地址传递的 SPI 值，来识别正确的安全关联 SA。每一个站点必须记住它的伙伴所使用的 SPI，以辨别安全服务的内容。

3.2.2 IP 认证头 AH

认证协议头（Authentication Header，AH）是在所有数据包头加入一个密码。AH 通过一个只有密钥持有人才知道的"数字签名"来对用户进行认证。这个签名是数据包通过特别的算法得出的独特结果；AH 还能维持数据的完整性，因为在传输过程中无论多小的变化被加载，数据包头的数字签名都能把它检测出来。

AH 协议不根据对业务数据进行的分，而提供加密和保护服务，不对 IPv6 数据报加密。这意味着调节和输入/输出的节点，或者加密服务节点仍能执行 AH 协议。RFC1826 第一页提到 IP AH 的协议的用途是，写到“可能也提供非抛弃认证服务，这取决于用哪一种加密算法，如何执行密钥。例如，采用一种像 RSA 那样的不对称数字签名算法，就能提供这种服务”。

IP AH 协议为其 IP 数据报保持认证信息，AH 协议处理并且要利用传输中不改变的 IP 数据报头部域，计算出认证信息，计算中会利用一种秘密认证密钥。至于 IP 数据报头中那些在传输中会改变的部分，例如转发数，计算时不加考虑。缺省的算法使用密钥型散列消息认证码(HMAC),加上本身不能提供非丢弃型认证服务的 MD%或 SHA-1 算法。AH 协议较之 IPv4，能提供更多的安全服务。认证信息有自己的负载，这意味着 Internet 网的基础结构不必改变。

IPv6 的验证主要由验证报头（AH）来完成。验证报头是 IPv6 的一个安全扩展报头，它为 IP 数据包提供完整性和数据来源验证，防止反重放攻击，避免 IP 欺骗攻击。

（1）验证报头的格式

验证报头的格式，如表 3.2.2.1 所示。

表 3.2.2.1 验证报头的格式

下一报头字段(Next Header)	有效载荷长度 (Payload length)	保留字段 (Reserved)
安全参数索引 (Security Parameter Index)		
验证数据字段 (Sequence Number)		
验证数据 (Authentication Data)		

验证报头的格式包括以下一些内容：

① 下一报头字段(Next Header)：确定跟在验证报头后面的有效载荷的类型(如 TCP)

② 有效载荷长度 (Payload length)：验证报头的长度。

③ 安全参数索引 (Security Parameter Index)：用来确定安全关联的安全参数索引。

④ 验证数据字段(Sequence Number)：一个变长字段，它包含完整性检查值(ICV, Integrity Check Value)，用来提供验证和数据完整性。

⑤ 保留字段 (Reserved)：(16 位)供以后使用。

(2) 验证数据 (Authentication Data)

验证数据包含完整性检查值 (ICV)，用来提供验证和数据完整性，用来计算 ICV 的算法由安全关联指定。ICV 是在这种情况下计算的，即 IP 报头字段在传递过程中保持未变，验证报头带有的验证数据置 0，IP 数据包为有效载荷。有些字段在传递的过程中可能改变，包括最大跳数、业务类别和流标签等。IP 数据包的接收者使用验证算法和安全关联中确定的密钥对验证报头重新计算 ICV。如果 ICV 一样，接收者知道数据通过验证并且没有被改过。验证数据包工作过程如图 3.2.2.1 所示。

(3) 防止重放攻击 (Prevent Reply Attack) 重放攻击是一种获得加密数据包，然后发送设定的目的地。收到复制加密数据包后，可能面临破解及其它引起意想不到的后果。序列号计数器可阻止此类攻击，当发送者和接收者之间的通信状态建立的时候，序列号被置 0。当发送者或者接收者传送数据的时候，它随后被加 1。如果接收者发觉一个 IP 数据包具有复制的序列号字段，它将被丢弃，这是为了提供反重放的保护。该字段是强制使用的，即使接收者没有选择反重放服务它也会出现在特定的安全关联中。验证报头带有的验证数据置 0，IP 数据包为有效载荷。

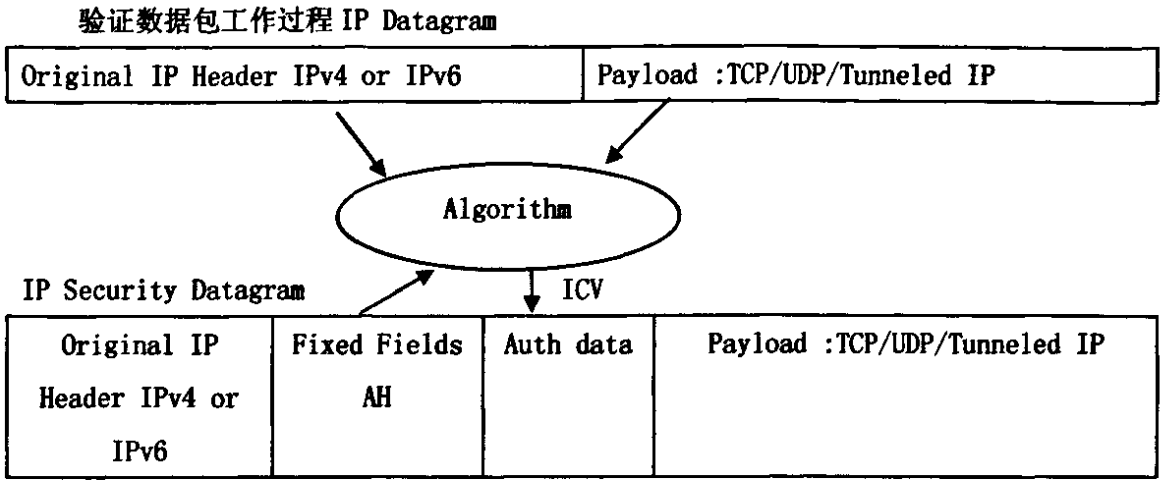

图 3.2.2.1 验证数据包工作过程

3．2．3 封装安全有效载荷数据（Encapsulating Security Payload）

安全加载封装（ESP）通过对数据包的全部数据和加载内容进行全加密来严格保证传输信息的完整性和机密性，这样可以避免其他用户通过监听来打开信息交换的内容，因为只有受信任的用户拥有密钥打开内容。ESP 也能提供认证和维持数据的完整性。ESP 用来为封装的有效载荷提供机密性、数据完整性验证。AH 和 ESP 两种报文头可以根据应用的需要单独使用，也可以结合使用，结合使用时，ESP 应该在 AH 的保护下。

ESP 还提供反应服务、序列完整性检验服务、有限的业务流服务。业务流加密需选择隧道模式执行 ESP。如果在安全网关中进行这项服务则最有效。数据来源认证和无连接的数据完整性检验是一种联合服务，与加密无关。

ESP 协议的执行既可以针对单项也可以针对多项通信业务。与 AH 协议类似的是，ESP 也与(具体的)加密方法独立。为了使之在 Internet 网中具有互操作性。密码块模式(CBC)中的数据加密标准(DES)正在考虑作为标准算法。

ESP 支持传输和隧道两种模式。ESP 对数据加密的数据放在 IP ESP 分组的数据负载部分。ESP 可以用来对整个 IP 数据报加密(隧道模式)或者仅仅对传输层，比如 TCP 和 UDP 数据进行加密(传输模式)。ESP 协议的使用，不能对路由器或者其它并未加入这个选定 ESP 安全关联的中间系统，产生任何不利影响。

加密数据封装起来，对整个原始数据就提供了一种机密保护。对每 IP 数据报加密并解密，会增加 IP 协议的处理代价，增加通信时延。ESP 协议执行的代价都可以不同，它取决与加密算法、密钥尺寸以及各种其它。在高传输量的节点上，采用硬件实现 ESP 可能有好处。

为了在整个因特网提供互操作性，ESP 协议起码要求所有每一执行 ESP 协议的过程，都支持使用。密码块链 CBC 模式中的 DES 算法。当然其它的加密算法和模式也可

以采用。

（1）封装安全有效载荷数据包格式，如图3.2.3.1所示。

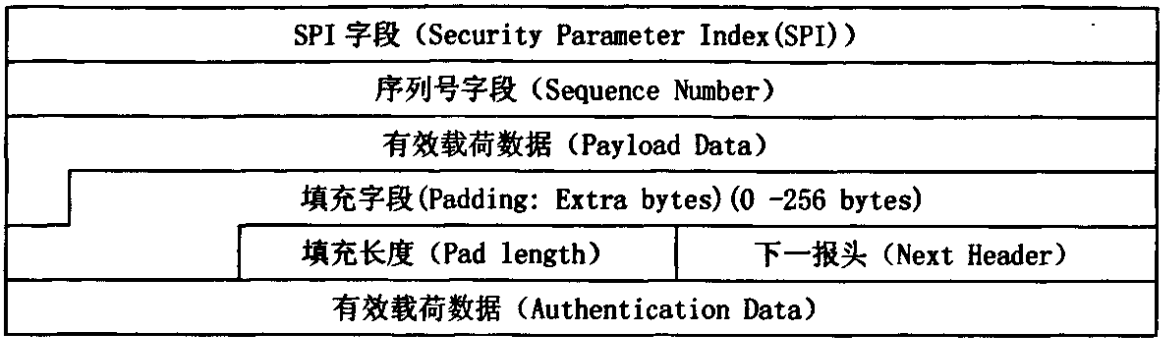

图3.2.3.1 封装安全有效载荷数据包格式

封装安全有效载荷数据包含以下字段：

① SPI 字段（Security Parameter Index(SPI)）：确定安全关联的安全参数索引；

② 序列号字段（Sequence Number:）：用来提供反重放保护，跟验证报头中描述的一样；

③ 有效载荷数据（Payload Data）：存放加密数据；

④ 填充字段(Padding: Extra bytes)：加密算法需要的任何填充字节；

⑤ 填充长度（Pad length）：包含填充长度字段的字节数；

⑥ 下一报头（Next Header）：描述有效载荷数据字段包含的数据类型；

⑦ 有效载荷数据（Authentication Data）：用ICV加密算法加密的所有数据(非加密数据区)。

（2）ESP计算（ESP Computation），在IPv6中，加密是由ESP扩展报头来实现的。ESP用来为封装的有效载荷提供机密性、数据来源验证、无连接完整性、反重放服务和有限的业务流机密性。ESP数据包压缩工作过程，如图3.2.3.2所示。

(3)局限性ESP不保护任何IP报头字段,除非这些字段被ESP封装(隧道模式),而AH则为尽可能多的IP报头提供验证服务。所以如果需要确保一个数据包的完整性、真实性和机密性时，需同时使用AH和ESP。先使用ESP，然后把AH报头封装在ESP报头的外面，从而接收方可以先验证数据包的完整性和真实性，再进行解密操作，AH能够保护ESP报头不被修改。

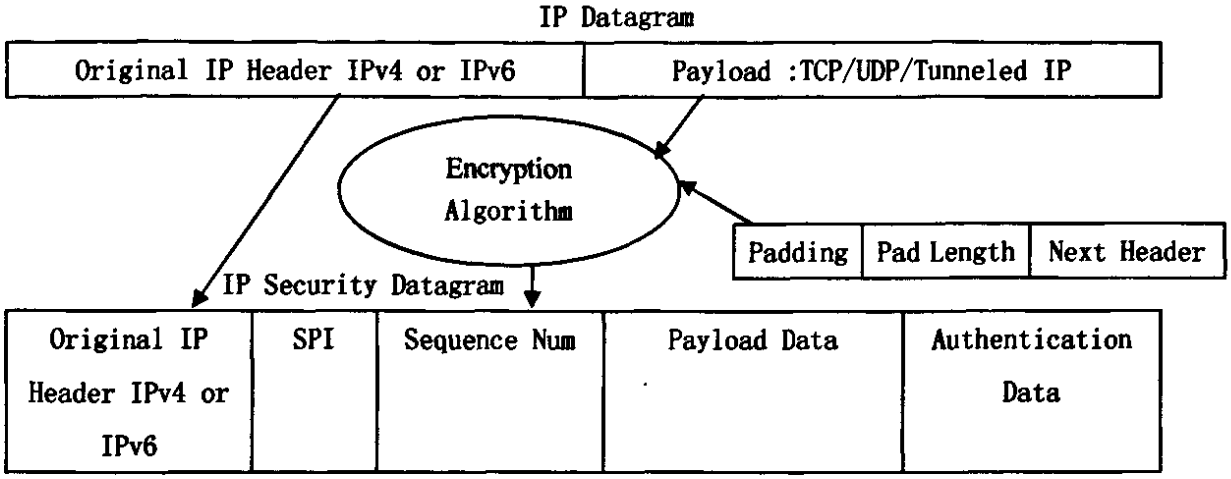

图 3.2.3.2 ESP 数据包压缩工作过程

3.2.4 密钥管理（Key Management）

密钥管理包括密钥确定和密钥分发两个方面，最多需要四个密匙：AH 和 ESP 各两个发送和接收密匙。密钥本身是一个二进制字符串，通常用十六进制表示，例如，一个 56 位的密钥可以表示为 5F39DA752E0C25B4。注意全部长度总共是 64 位，包括了 8 位的奇偶校验。56 位的密匙（DES）足够满足大多数商业应用了。密钥管理包括手工和自动两种方式。

手工管理（Manual）：手工管理方式是指管理员使用自己的密钥及其它系统的密钥手工设置每个系统。这种方法在小型网络环境中使用比较实际。这方面有不少的实例可采用人工密钥的构造方法。自动管理系统（Automated）：可以随时建立新的 SA 密钥，并可以对较大的分布式系统上使用密钥进行定期的更新。

自动管理模式是很有弹性的，但需要花费更多的时间及精力去设置，同时，还需要使用更多的软件。被广泛使用将需要一种 Internet 密钥管理协议，它能够支持 Internet 协议族中了除 IP 安全协议外的一些别的协议，比如，域名服务安全扩展协议(RFC2065)支持签名主机密钥提供三种不同服务：

(1)公共密钥和签名主机密钥存储，以及密钥分配服务。

(2)数据源认证服务。

(3)处理和请求认证服务。

3.2.5 密钥管理协议

IP 安全体系协议中的密钥管理[31]，一般包括两种类型，分别是：用于定义过程和分组格式协议，以建立、协商、修改和取消安全关联。这一类协议的例子有 SKIP 和 ISAKMP(Internet Security Association Management Protocol)。SKIP 是一种非会话密钥管理协议，需和 IP Sec 协议一起使用；它为通信的各方提供秘密和认证服务，它在 IP 层上运行。ISAKMP 提供一种框架，用于认证和密钥交换，但是并不对它们进行定义。ISAKMP 被设计成与密钥相独立，也就是说，支持许多不同的密钥交换

方案。

定义密钥交换功能的协议，这方面的例子包括 OAKLEY 密钥确定协议，它常写成 Oakley，用来实现 ISAKMP 的功能，以及 SKEME(Secure Key Exchange Mechanism)规程。Oakley 描述了密钥交换中称作模式的一系列过程，并细化了每个模式提供的，比如完善的密钥前向加密、身份保护和认证。ISAKMP 的 Oakley 实现方案，描述了这样一个协议，它部分来自 Oakley，部分来自 SKEME，与 ISAKMP 相结合，可获得 ISAKMP 中使用的、认证过的密钥消息。SKEME 是一种多功能密钥交换技术，能提供匿名、抛弃和快速密钥刷新服务。DNS 安全扩展协议具有以上两类协议的某些特征。

总之，密钥交换协议的特性包括：密钥建立方法、认证、对称、完善的前向加密和后向业务保护。

3.3 Internet 密钥交换

Internet 密钥交换(IKE)[6]用于动态建立 SA。IKE 代表 IP Sec 对 SA 进行协商，并对 SADB 数据进行填充。由 RFC2409 文件描述的 IKE 属于一种混合型。它建立在由 Internet 安全联盟和密钥管理协议(ISAKMP)定义的一个框架上，详情见 RFC2408 文件。同时，IKE 还实现了两种管理协议的一部分：Oakley 和 SKEME。此外，IKE 还定义了两种自己的密钥交换方式。

ISAKMP、Oakley 和 SKEME 这三个协议构成 了 IKE 的基础。因此，我们说 IKE 是一种“混合型”协议，它沿用 ISAKMP 的基础、Oakley 的模式及 SKEME 的共享密钥更新技术，定义唯一的验证加密生成技术以及协商共享策略。

3.3.1 ISAKMP

ISAKMP 定义了双方如何沟通，如何构建彼此间以沟通的消息以及保障通信安全所需的状态变换。ISAKMP 提供了对对方的身份进行验证的方法，密钥交换时交换信息的方法，以及对安全服务进行协商的方法。然而，它既未定义一次选定的验证密钥交换如何完成，也未定义安全联盟所需的属性，也就是没有密钥交换文件和解释域文件。

1. 消息和载荷

对于一个用基于 ISAKMP 的密钥管理协议交换的消息来说，它的构建方法：将 ISAKMP 所有载荷链接到一个 ISAKMP 头，如图 3.3.1.1 所示。

发起者和响应者是由通信的对方创建的，并随消息 ID 一起，用来标识状态，以便对进行中的一次 ISAKMP 交换进行定义。“下一个载荷”字段指出在各个 ISAKMP 载荷中，哪一个紧随在这个头之后。ISAKMP 版本的标识是用主版本和副版本字段中的主/副编号来进行的。ISAKMP 交换的具体类型则是由“交换”字段来标识的。ISAKMP

消息的全长是由“消息长度”字段来标识的。至于“旗标”字段，则为接收者提供了与消息有关的特殊信息。注意“旗标”是由一个位掩码来表示的，其中，每个位对应一个具体的选项。总共定义了三个旗标(采用八位长度的字段，易于扩展)：加密、委托和“纯验证”旗标。其中，加密旗标指出跟随在这个头之后的载荷已经加密；委托旗标指出通信的某一方在交换完成 之后收到通知；“纯验证”旗标主要由那些希望为 ISAKMP 引入密钥恢复机制的人使用。

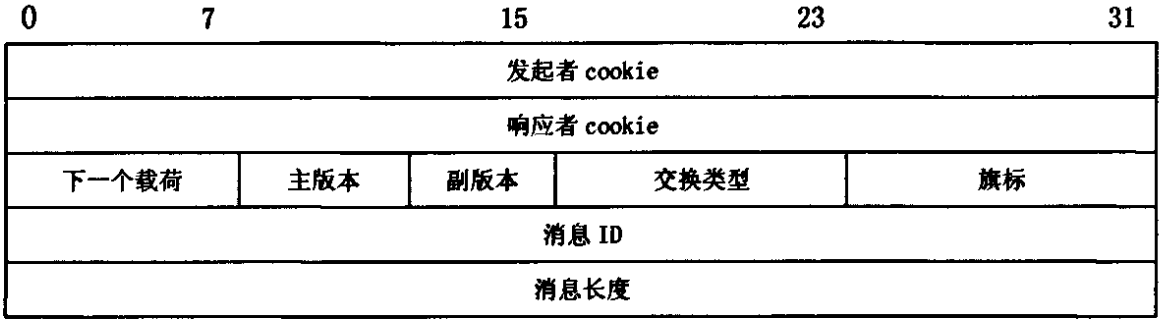

图 3.3.1.1 ISAKMP 的头

目前在 ISAKMP 中，总共定义了 13 种不同的载荷，它们是以相同格式的头开始的，跟随在当前载荷之后的 ISAKMP 载荷的类型由“下一个载荷”字段来指定。一个 ISAKMP 载荷的总长度“载荷长度”字段来表示。至于保留字段，则未使用，必须设为 0。ISAKMP 通用头如图 3.3.1.2 所示。

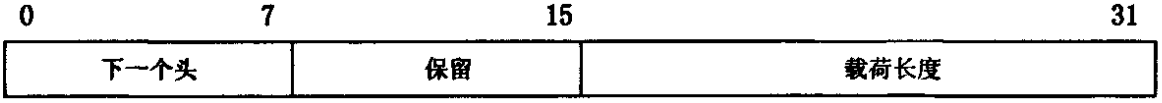

图 3.3.1.2 ISAKMP 通用头

ISAKMP 定义了在一次交换中用来表达特定构建方式的载荷。它们包括：散列载荷、签名载荷 nonce 载荷、厂商 ID 载荷、密钥交换，其中包含执行一次密钥交换所发布的信息，Diffie-Hellman 公开值。

有些载荷是专用的，必须单独。其中包括：安全联盟载荷，用来定义要建立的一个安全联盟无论是不是一个 ISAKMP SA，要用于其他安全协议的 SA。

还有证书请求载荷、验证载荷、提案载荷和转码载荷依赖于一个安全联盟载荷，并由那个安全联盟封装。而且可能不会单独出现。前者定义了对一种安全联盟的提议，后者则对一种提议的转码方式进行了描述。在一条消息中，载荷之间链接到一起，这是用通用头中的“下一个载荷”字段来实现的。

2. ISAKMP 交换的阶段

ISAKMP 描述了协商的两个独立阶段。在第一阶段，通信各方彼此间建立了一个已通过身份验证和安全保护的隧道；在第二阶段，这个通过了验证和安全保护的隧道用于为另一个不同的协议。

阶段1的交换建立了一个ISAKMP“安全联盟(SA)”。这个SA的概念与安全策略的一个抽象和一个密钥和IP Sec SA有着某些共处。要想建立这个SA，通信各方 首先必须协商好它的规则、用来验证方法以及建立它所需的参数。这个SA必须用来对后续的阶段2交换进行验证。对于通信双方能够共享的ISAKMP数量，并不存在任何限制。但在实际应用中，却最好加以限制。

阶段2交换可为其它协议建立安全联盟。由于ISAKMP SA已经通过了，所以可以用它为一次阶段 2 交换中的所有消息提供安全保障。完成了一次阶段 2 之后，在ISAKMP处理过程中的它关联在一起的状态便不复存在了。但ISAKMP SA可存在下去，以确保后续的阶段2交换的安全。阶段2交换的数量没有限制。

3. 策略协商

建立一个共享的安全联盟，那么先协商采用的安全策略。必须能灵活地解析安全联盟、提议能及转码载荷，这样才能使构建和处理复杂的策略。为达到这一目的，ISAKMP 同时动用了安全联盟、提案以及转码载荷。在单独一个安全联盟内，可能包含了一个或多个提案，而且每个提案可能包含了一种或多种转码方式。安全联盟载荷的DOI字段定义了一个的“解释域”。载荷本身便要应用于它，若DOI值为零，表示它用于ISAKMP。针对不同的安全服务，也需要使用不同的DOI值。在RFC2407文件中，规定了用于IP Sec的DOI，它采用的DOI值为SA载荷的“条件”字段包含了一些信息。可使接收方在协商期间做出恰当的策略决定，这些信息是具体的DOI所特有的。由于每个SA载荷都可能在眸在多个提案载荷，所以提案载荷中包含了一个提案编号。SPI长度以及SA采用的协议。紧随在一个提案载荷之后，是一个或多个转码载荷。

3.3.2 Internet密钥交换协议（IKE）

SAKMP本身没有定义具体的密钥交换技术。密钥交换的定义留给其它协议处理。对IP Sec而言，定义的密钥交换就是IKE。IKE利用ISAKMP语言来定义密钥交换，是对安全服务进行协商的手段。IKE交换的最终结果是一个难过验证的密钥以及建立在双方同意基础上的安全服务，即IPSec安全关联（IP Sec SA)。但是，IKE并非公由IPSec专用的。只要其它协议需要，便可用它协商具体的安全服务。

IKE使用了两个阶段的ISAKMP。第一阶段建立IKE安全关联，可以采用“主模式”或“野蛮模式”；第二阶段利用这个既定的安全关联，为IP Sec协商具体的安全，采用“快速模式”。

密钥交换的定义留给其它协议处理。对IP Sec而言密钥交换就是IKE即Internet密钥交换。IKE利用ISAKMP语言定义密钥交换，是对安全服务进行协商的手段。IKE定义了为数众多的交换方式，以相关的选项。IKE交换的最终结果是通过验证的密钥以及建立在双方同意的安全服务“IP Sec SA”。

IKE了两个阶段的ISAKMP。第一阶段建立IKE安全关联，可以采用“主模式”或

“野蛮模式”；第二阶段利用这个既定的安全关联，为IPSec协商具体的安全关联，采用“快速模式”。对于阶段1交换来说，IKE采用的是身份保护交换，以及根据基本ISAKMP文档的野蛮交换法。对些，我们分别叫做“主模式”和“野蛮模式”。但和ISAKMP交换不同，IKE对交换进行了完整的定义，包括所有载荷的内容，以有及处理它们所需要的步骤。对于阶段2来说。IKE定义了一种快速模式交换，它的作用是为除IKE之外的其它协议协商安全服务，主要是IP Sec。IKE定义的另外两种交换均属信息方面的交换。在这种交换中，IKE通信双方可相互间传达有关错误和状态的资讯，而且一种新的组交换模式可使各方协商如何在它们之中使用一个新的Diffiie-Hellman组。

主模式和野蛮模式交换的都是相同的事情：建立一个保密和验证的通信信道(IKE SA)，以及建立验证过的密钥，为双方的IKE通信提供机密性、消息完整性以及消息源验证服务。IKE中定义的其它所有交换都要求一个验证过的IKE SA作为首要条件。所以一次阶段1交换，无论主模式还是野蛮模式，必须在进行其它任何交换之前完成。

IKE SA提供了各种各样的参数，包括加密算法、散列算法、验证方法以及Diffie-Hellman组。并整体进行协商，作法是对ISAKMP SA载荷进行交换。

对IKE交换最深的是“验证方法”。其它属性决定了载荷的内容，以及如何对消息加以保护。而验证方法却决定了如何交换载荷，以及在什么时候交换。取决于由通信双方协商的验证方法，一次IKE交换甚至可以发和改变。可以接受的验证方法包括预共享密钥；使用“数字签名算法(DES)”得到数字签名；RSA算法得到的数字签名；通过交换加密的Nonce,从而实现两种类似的验证方法。

IKE SA和IP Sec SA的区别在于前者是“双向”的，对参与密钥交换的双方来说，事先已经假定了一系列特殊的规则。特别要指出的是，有一方是发起者，另外一方是响应者。但是只要建立好SA，便可以用它对进入及外出的数据同时实施保护。另外，无论当初由谁发起了建立IKE SA的1交换，双方都可主动发起一次阶段2交换，并用IKE SA对其加以保护。

1．主模式交换

主模式在三个步骤中总共用了到六条消息，最终建立了IKE SA。这三个步骤分别是模式协商，一次是Diffie-Hellman交换和一次nonce交换，以及对对方身份和验证。主模式的特点包括身份保护以及对ISAKMP协商能力的完全利用。其中，身份保护在对方希望隐藏自己的身份时显得尤为重要。

2．野蛮模式交换

野蛮模式交换的用途与主模式交换相同，建立一个验证的安全联盟的密钥，随后可用IKE为其它安全协议建立安全联盟。主要的差别在于，野蛮模式只需用到主模式一半的消息。由于对消息的数量进行了限制，野蛮模式同进也限制了它的协商能力，而且不会提供身份保护。IKE丰富的协商功能主要集中在野蛮模式下。

3. 快速模式交换

建立IKE SA之后，用它为其它协议（如IP Sec）生成相应的SA。这些SA是通过快速模式交换来建立的，对一快速模式交换来说，在以前建立好的IKE SA的保护下完成的。通过一次主模式或野蛮模式交换，许多快速模式都可以完成。在一次快速交换模式中，通信双方需要协商拟定IP Sec安全联盟的特征，并为其生成密钥。IKE SA保护快速模式交换的方法是：对其进行加密，并对消息进行验证。消息的验证是通过PRF函数来进行的，通常是协商好的散列函数的一个HMAC版本。它对快速模式交换的整个消息进行验证。

3.3.3 协商

协商的内容：为建立一个IKE SA，通信双方必须协商各种各样的参数，这是通过交换ISAKMP消息完成的。这些交换的消息中，包含了多种ISAKMP载荷。

（1）SA载荷包括如下参数：

① 加密算法，用来保护数据。

② 散列算法hash值。Diffie-Hellman组，定义进行Diffie-Hellman交换时，通信双方需要采用什么样的参数。

③ 伪随机函数Prf（key,msg）通常是一个带密钥的哈希函数，用来产生看是随机，实则确定的输出。Prf既可用于生成密钥，也可用于认证。

④ 认证方法，这是对IKE交换影响最深的参数。其它属性决定载荷的内容，认证方法则决定如何交换载荷，以及在什么时间交换。可以接受的认证方法有：预共享密钥、数字签名、基于公共密钥算法（如RSA）的认证。

（2）密钥交换载荷，交换双方的Diffie-hellman公开值。

（3）Nonce载荷。

（4）ID载荷，用于认证交换双方的身份。

（5）签名（SIG）载荷和证书（CERT）载荷。完成上述载荷的交换后，协商的双方可以计算出四种密钥和两种散列值。

IPv6网络由于IPSec提供的安全服务，能有效防止长期困扰人们的许多网络攻击，如IP欺骗、拒绝服务攻击、数据篡改和网络探测活动等。IP Sec是目前可提供的最好的网络安全解决方案,它努力使Internet上的安全机制标准化，向更安全的Internet迈进了一大步。IP Sec中可能有许多安全问题需要解决，如FTP、Telnet、DNS和SNMP，但其它安全可通过防火墙或NAT转换来加以解决，但对QOS和DHCP可能会导致IPSec无效或受限。

4 构建 IPv6 网络的安全防御体系

我们不难看出 IPv6 协议确实比 IPv4 的安全性有所改进，IPv4 中常见的一些攻击方式，将在 IPv6 网络中失效，例如网络侦察、报头攻击、 ICMP 攻击、碎片攻击、假冒地址、病毒及蠕虫等。例如数据包侦听、中间人攻击、洪水攻击、拒绝服务攻击、应用层攻击等一系列在 IPv4 网络中的问题， IPv6 仍应对乏力，只是在 IPv6 的网络中事后追溯攻击的源头方面要比在 IPv4 中容易一些。另外 IP Sec 中可能有许多安全问题需要解决，如 FTP、Telnet、 DNS 和 SNMP，但其它安全可通过防火墙或 NAT 转换来加以解决，但对 QOS 和 DHCP 可能会导致 IP SEC 无效或受限。

4．1 IPv6 产生的新问题

IPv6 是新的协议，在其发展过程中必定会产生一些新的安全问题，主要包括应对拒绝服务攻击(DoS)乏力、包过滤式防火墙无法根据访问控制列表 ACL 正常工作、入侵检测系统(IDS)遭遇拒绝服务攻击后失去作用、被黑客篡改报头等问题。此外，在 IPv6 中还有一些问题有待解决，主要包括:

（1）IP 网中许多不安全问题主要是管理造成的。IPv6 的管理与 IPv4 在思路上有可借鉴之处。但对于一些网管技术，如 SNMP 等，不管是移植还是重新另搞，其安全性都必须从本质上有所提高。由于目前针对 IPv6 的网管设备和网管软件几乎没有成熟产品出现，因此缺乏对 IPv6 网络进行监测和管理的手段，缺乏对大范围的网络故障定位和性能分析的手段。没有网管，无法保障网络高效、安全运行。

（2）PKI 管理在 IPv6 中是悬而未决的新问题。

（3）IPv6 网络同样需要防火墙、VPN、IDS、漏洞扫描、网络过滤、防病毒网关等网络安全设备。事实上 IPv6 环境下的病毒已经出现。这方面的安全技术研发还尚需时日。

（4）IPv6 协议仍需在实践中完善，例如 IPv6 组播功能仅仅规定了简单的认证功能，所以还难以实现严格的用户限制功能，而移动 IPv6(Mobiel IPv6)也存在很多新的安全挑战。DHCP 必须经过升级才可以支持 IPv6 地址，DHCPv6 仍然处于研究、制订之中。

4.2 传统网络安全工具在 IPv6 下的改进

IPv4 / IPv6 过渡阶段 IPSec 的实施并不能替代传统的安全设备[13]，防火墙和入侵检测系统等仍有存在的必要，但是 IPSec 的采用却对现有安全体系结构带来了挑战，封装安全载荷（ESP）隧道，给防火墙、人侵检测等安全工具提供了新的思路，即把保密和认证机制融入其中，使传统的安全设备更加完善和强健。结合 IP Sec 和传统安全设备构造新的安全体系，要考虑 IP Sec 带来的问题，同时利用它的认证和保密机制，为传统安全设备在 IPv4 向 IPV6 过渡期间提供更高安全强度的保护能力。

4.2.1 漏洞扫描

漏洞扫描技术是一项重要的主动防范安全技术。不论攻击者是从外部还是从内部攻击某一网络系统，攻击的机会都是系统本身所存在的安全隐患。对于系统管理员来说，漏洞扫描技术是最好的助手，能主动发现主机系统和网络系统的安全隐患，在系统安全保卫战中做到“有的放矢”，及时修补漏洞，构筑坚固的系统安全。

在传统的 IPv4 网络中，漏洞扫描系统一般部署于局域网的网管机上，负责对内部网中的各服务器和联网进行安全检测。在 IPv4 向 IPV6 过渡阶段，漏洞扫描系统所处的网络环境没有发生大的改变。扫描器仍位于局域网内，只是扫描的对象换成了双栈主机或单纯的 IPV6 主机。相应的，IPV6 下的扫描器也部署在局域网内的双栈主机上，利用下层的 IPV6 协议栈在原有 IPv4 扫描器中添加 IPV6 扫描功 SB。漏洞扫描器的核心是漏洞扫描模块。该模块具有一个通用的相对较小的操作引擎子模块，只负责任务管理和过程调度，它并不关心要检测谁、要检测什么或者检测结果意味着什么。这些具体的任务将由周边的子模块来完成。它们又通过组织和调度更小的子模块来完成很多细节工作，尤其是与特定主机类型、特定服务类型、特定的漏洞相关的工作。通过这种分层模块的设计方式，漏洞扫描模块具有很强的扩展性因此，可以通过修改操作引擎模块来扩展 IPV6 扫描功能。

4.2.2 防火墙

防火墙是一种重要安全防护技术，是多层安全防护中必要的一层，其主要作用是在网络入口同关处检查网络通讯，根据设定的安全规则，在保护内部网络安全的前提下，提供内外网络通讯。防火墙为了提供稳定可靠的安全性，必须跟踪流经它的所有通信信息，为了达到控制目的，防火墙首先必须获得所有通信层和其它应用的信息，然后存储这些信息，还要能够重新获得以及控制这些信息。使用防火墙的目的是保护内部脆弱的服务，通过提供对系统的访问控制，实现集中的安全管理，从而达到增强的系统保密性，防火墙提供了制定和执行网络安全策略的手段。

防火墙可以分为包过滤、应用代理和状态检测三种类型。目前在市场上流行的防火墙大多属于状态检测防火墙。在对性能不断追求的同时，防火墙走过最初几年的

X86 架构，开始向 ASIC、NP 等网络设备标准架构蜕变。一方面，防火墙技术和产品已经相对成熟，但还存在一定的技术局限性，防火墙仍不能完全满足用户的需求。网络攻防是一对矛盾，用户需求激发技术创新，网络与应用也在日新月异，因此，防火墙技术将持续快速发展，技术突破将必然带来新的天地。在关键处理技术上实现创新，并对防火墙在各种网络环境中的实际应用、稳定性与易用性，以及整体网络安全解决方案进行研究，一直会是防火墙技术的重要内容。另一方面，防火墙必须在基于芯片加速的深度内容过滤技术上实现真正的突破，并推出实用化的产品以解决当前的网络安全难题。随着算法和芯片技术的发展，防火墙会更多地参与应用层分析、芯片解决计算加速、软件解决过滤精确，防火墙必将以软硬兼施的方案为用户的应用提供更安全的保障。而 VPN、IDS / IPS、防病毒等功能可能以各类加速芯片的形式与防火墙协同工作，形成以芯片技术为主导的全系列硬件型安全网关。各系列的划分将针对用户群的不同需求，并在价格、功能、性能上为各个群体的用户贴身定制。

此外，防火墙下一步的发展与中国下一代网络的建设紧密相关，如 IPv6 网络、P2P 应用、3G 网络等等。这里要特别强调的是防火墙与 IPv6。由于 IPV6 网络的新特性，如端到端的连接、移动 IP 的处理、内联 IP Sec、路径 MTU 探测等，给防火墙带来新的安全挑战。防火墙不仅要及时适应 IPv6 网络的发展，并解决 IPv6 引入后带来的新问题，同时，由于 IPv6 与 IPv4 网络长期共存，网络必然会同时存在 IPv4 的安全问题与 IPv6 的安全问题，或由此造成新的安全问题。下一步要考虑的，不仅仅是更适应于网络发展的防火墙模型，可能还会包括网络安全防范与评估方法等等。在 Internet 无所不在的理念下，防火墙等网络安全产品也必将站在可信赖应用与计算环境为基础的角度上设计并解决安全问题。当前基于不同架构设计实现的防火墙都将面临巨大的挑战，为此付出的代价也将是不同的。

4.2.3 入侵检测系统

入侵检测系统(IDS)[14]是一种主动的网络安全防护措施，是分层安全中日益被普遍采用的防护措施之一，它从系统内部和各种网络资源中主动采集信息，从中分析可能的网络入侵或攻击。入侵检测系统在发现人侵后。会及时做出响应。包括切断网络连接、记录事件和报警等，入侵检测系统将有效地提升黑客进入网络系统的门槛。入侵检测系统按其输入数据的来源来看，可以分为基于主机、基于网络、分布式入侵检测三种类型。目前市场上流行的入侵检测系统是分布式入侵检测系统，它能够同时分析来自主机系统审计日志和网络数据流的入侵检测系统，系统由多个部件组成，采用分布式结构。

人侵检测系统是继“防火墙”、“数据加密”等传统安全保护措施之后又一道安全闸门，它能识别针对计算机和网络资源的恶意行为。

在基于 IPv6 的下一代互联网中，将数据挖掘技术应用于网络入侵检测是入侵检测系统的一个新方向。因为这样可以充分发挥数据挖掘处理大数据量的优势，提高检

测的效率和准确性。网络数据的采集是网络人侵检测系统的重要组成部分。构建基于数据挖掘的入侵检测系统，其主要特点是：能够自动地从海量数据中提取简洁，精确的系统正常特征轮廓，解决了传统的基于误用的人侵检测系统规则的提取和编码的困难。由于该方法具有通用性（可以处理各种结构化的数据）和自动处理的功能，因而可以在许多不同的网络环境中构建相应的入侵检测系统。目前应用于入侵检测系统中的数据挖掘算法主要有关联、序列和分类这3种。

4.2.4 网络安全审计系统

安全审计[10]基本概念(security audit)是指为了检验系统的控制是否足够，为了保证与已经 建立策略和操作实施相符合，发现安全中的漏洞，以及为了建议在控制、策略和实施中做指定的改变，而对系统记录独立观察和考核。

安全审计系统主要用于监视记录网络中的各类操作，实时地综合分析出网络中发生的安全相关事件，如外部入侵行为和内部事件如内部人员的文件自制、信息获取、信息发布、资源变迁等，并根据设置的规则，智能地出违规行为，对违规行为进行记录，报警和阻断。好的审计系统还能对网络中出现的黑客入侵行为进行实时报警和阻断，有效地阻拦来自网络内部和外部，特别是来自因特网的恶意破坏行为。系统自身的审计数据具备防销毁、防篡改的特性，能够为网络犯罪案件的侦破和取证提供精确、宝贵的辅助数据，可在在内部局域网上建立完善的安全预警、安全应急反应体系，为信息系统的安全运行提供保障。

安全审计系统能够对于因特网上最常见的典型应用进行细化的审计，提供符合条件设置的典型应用的详细信息，并能够让用户设置条件，选择需要审计的 Telnet、HTTP、FTP、SMTP、POP3等的各类信息因特网应用，对网络中的数据包进行分析，以提供更加详尽侦查辅助和取证信息。

安全审计是使用某种或几种安全检测工具，采取预先扫描漏洞的方法检查系统的安全漏洞，得到系统薄弱的检查报告，并采用相应的增强系统安全性的措施。

此外，安全审计的实际实现还要采用数据挖掘和数据仓库技术，实现在不同网络环境中终端对终端的监控和管理，在必要时通过多种途径向管理员发出警告或自动采取排错措施，能对数据进行分析、处理和追踪。

1.安全审计和报警模型的实现

安全审计和报警模型的实现如图4.2.4.1所示。整个过程可分布在诸独立的开放系统中，每一个系统则负责该过程的一个或多个方面。

企图使用一个账号收的无效口令来登录系统则可能是安全事件的示例，审计跟踪分析 可揭露出这是利用假口令登录该账号，并且在达到一定次数后产生一个报警。

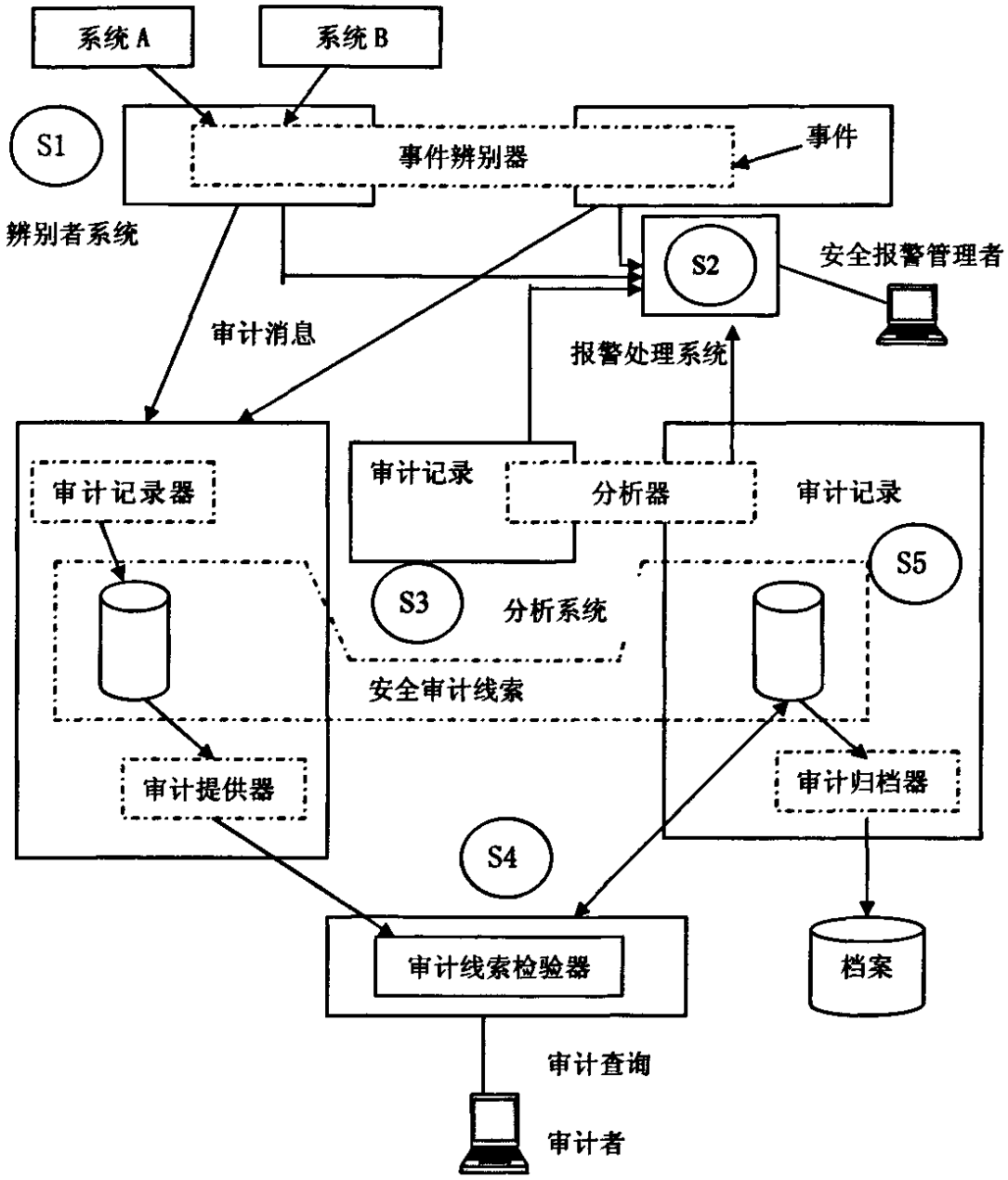

图 4.2.4.1 安全审计和报警模型

S1 有能力按照定义的准则检测安全相关事件并分析它们，但没有安全审计跟踪能力，所以安全报警被送到 S2，安全审计消息则被送到 S3 以便包含在该安全审计线索里。

S3 负责更新安全审计线索。S3 还向 S6 提供对安全审计线索和安全审计线索档案的访问，这样可以按照定义的准则选择安全审计线索审计记录，并汇集成安全报告。

S4 负责归档和检索审计线索记录。

S5 包含一个应用，该应用按照准则审计线索记录和归档的记录，并在超过门限或检测到达到其他报警事件时，向 S2 发出了报警。

2．安全审计的日常管理

安全审计的日常管理可以包括如下四个方面：

（1）选择将被记录和被远程收集的事件。例如，选择典型应用审计，包括 Telnet、HTTP、FTP、SMTP、POP3，并还可以还原各应用的操作过程；文件共享审计，对重要文件服务器、客户机、重要文件和目录进行防护；主机服务端口审计，监测主机突然开放的陌生端口，有效发现主要是否被黑客设置后门，发现系统 中的异常的服务；网络流量监测和历史流量查询功能；用户自定义审计，可以协助用户对特定应用进行审计等。

（2）授予或取消对所选事件进行审计线索日志记录的能力。激活或暂停对所选事件进行审计线索日志记录。

（3）所选审计记录的远程收集。中心管理机或上层管理机定时或根据需要远程从下级管理机、审计代理程序、被监测主机等安全地收集审计数据。

（4）准备安全审计报告。报告应能根据需要，提供专业化报表和分析图形。对于安全事件，应如实报告，包括发生的、产生的结果、分析等。可牟的话，还应对其可能产生的影响和后果做出评估，并提出补救和改进和建议等。

4．3 构建动态安全防御体系

为了保护数据和网络资源，网络安全服务有五个基本目标[37][42]，它们是：

可用性：可用性就是指网络服务对用户而言必须是可用的，也就是确保网络节点在受到各种网络攻击时仍然能够提供相应的服务。

保密性：保密性保证相关信息不泄露给未授权的用户或实体。

完整性：完整性保证信息在传输的过程中没有被非法用户增加、删除与修改，保证非法用户无法伪造数据。

真实性：真实性保证和一个网络节点通信的对端就是真正的通信对端，也就是说要鉴别通信对端的身份。如果没有真实性，那么网络攻击者就可以假冒网络中的某个节点来和其它的节点进行通信，那么他就可以获得那些未被授权的资源和敏感信息。

不可否认性：不可否认性保证一个节点不能否认其发送出去的信息。这样就能保证一个网络节点不能抵赖它以前的行为。

而基于 IPv6 的网络协议对 IP Sec 的包含和强制使用，在安全性方面有了较大的提高，能够提供实现以上安全属性的绝大部分的安全服务。但是 IP Sec 不能完全解决网络的安全问题，因此技术方案必须引入针对安全漏洞和网络攻击的研究，通过对安全漏洞的实时检测与修补，对网络攻击的实时监测和防御，结合风险管理的相关措施实现防御的整体性和动态性，其中重点考虑 IPv6 网络的各种安全威胁和隐患，

并引入安全审计和信息综合分析模块来实现防御的智能性，增强体系的健壮能力。

一个最常见的安全模型就是 PDRR 模型。PDRR 模型就是 4 个英文单词的头字符：Protection（防护）、Detection（检测）、Response（响应）、Recovery（恢复）。这四个部分构成了一个动态的信息安全周期，如图 4.3.1 所示。

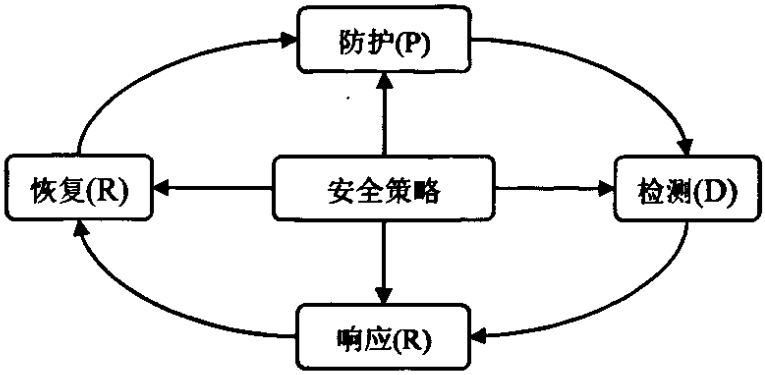

图 4.3.1　PDRR 模型

网络的动态安全模型能够提供给用户更完整、更合理的安全机制，全网动态安全体系可由下面的公式概括：

网络安全=风险分析+制定策略+防御系统+实时监测+实时响应+灾难恢复

网络的安全是一个“APPDRR”的动态安全模型，如图 4.3.2 所示。

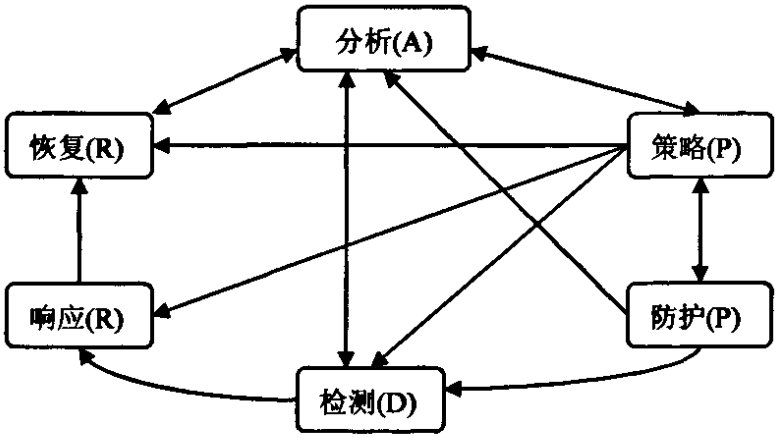

图 4.3.2　APPDRR 安全模型

安全保护是网络的第一道防线，能够阻止对网络的入侵和危害；安全监测是网络的第二道防线，可以及时发现入侵和破坏；实时响应是网络的第三道防线，当攻击发生时维持网络“打不垮”；恢复是第四道防线，使网络在遭受攻击后能以最快的速度“起死回生”，最大程度上降低安全事件带来的损失。进行风险评估和提出安全需求是制定网络安全策略的依据。风险分析（风险评估、风险管理），是指确定网络资产的安全威胁和脆弱性、并估计可能由此造成的损失或影响的过程。风险分析有两种基

本方法：定性分析和定量分析。在制定网络安全策略的时候，要从全局进行考虑，基于风险分析的结果进行决策。

根据已有的研究成果，这里将给出一个初步的 IPv6 网络安全动态防御技术体系的模型:该模型既要体现 APPDRR 模型的典型防护过程，也要体现网络安全管理的因素;既要有强大的对已知风险的处理能力，也要有对新的攻击、安全风险和特性的识别能力，而系统的基础安全支撑技术则主要引入了 IP Sec 的作用并结合 IPv6 网络的安全特性。如图 4.3.3 所示。

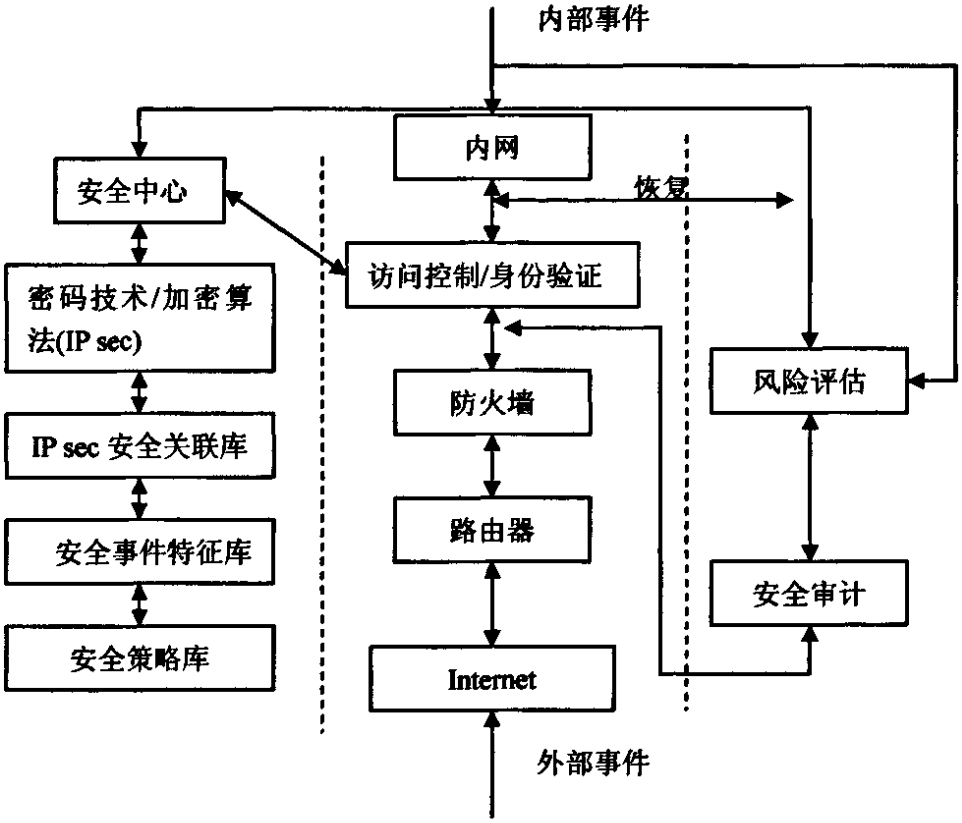

图 4.3.3　动态网络安全模型

模型不但够防御外来事件的攻击也能有效的防止内部事件的破坏，体系的输入成份包括网络威胁和脆弱性(包括网络攻击)和网际协作预警信息，这些都是影响体系安全和处理策略的关键因素。要保护的是系统的全部资产。 体系中包含一个核心过程，来源于安全防护的典型过程，防护—检测—响应—恢复。防护模块负责在攻击发生前基于布置防护屏障，修补系统漏洞，并采用 IP Sec 和密码技术实现数据的保密，认证，和安全接入等功能。从而在自身防御和入侵阻止/延缓两个方面实现综合防范，检测模块负责对异常网络行为和模式进行检测、识别、预警;响应模块根据预警信息对攻击进行反应，恢复模块是使得被保护的网络资源恢复到攻击发生前的状态。防护部分是体系的重要部分，又分成两个部分，一部分是对网络攻击的防护，另一部分是对网络隐患的管理，从而贯彻了主动防御的思想。风险管理模块是支持安全管理的重

要组成部分，一方面通过风险管理，提供相应的防护策略，一方面实现对资产的安全控制和在生命周期过程中的保护。通过若干管理工具，有效支持整个体系的工作过程。体系中包含一个重要的反馈模块，核心部分是综合信息管理模块，它是系统学习进化的重要组成部分，动态性，智能性的有力体现。包括信息收集与分析，知识提取与控制等，信息来源主要包括系统中各个功能单元提供的日志和分析记录等信息，也包括来自与网络的联动预警信息。结合安全审计模块的使用，它把分析得到的新的预警信息传给防护过程的相关环节，以及其它网络实体。并提取出知识级数据来更新相关的数据库。网际协作信息的输出表明该体系不是孤立的，可充分发挥全网的联动扩展的功能。IP Sec 机制和密码管理中心是 IPv6 网络的安全性基础模块。负责对系统的安全接入，安全服务，安全保密等功能提供基础支持。

现代网络安全理论认为，网络安全漏洞和网络攻击是不可能完全避免的。因此，任何网络安全体系的设计必须对此给予足够的重视。安全防护技术体系非常复杂，要有效的保护网络，必须进行综合防范，支持防护、检测、响应和恢复等过程的技术缺一不可。在这过程中防火墙、IDS ，漏洞扫描、病毒防范、安全审计等技术都是必要的安全技术。在 IPv6 网络中，防护技术的整体性，仍然是一个重要指标，虽然它克服了许多 IPv4 网中的安全问题，但是同时也出现了新问题，防御的任务仍然是复杂而且艰巨的。在防护过程中，为了克服单项安全技术的局限，除了提升技术本身的性能和对不安全因素的识别能力以外，一个重要的途径就是通过技术间的联动扩展和数据关联来弥补其固有的不足，这种联动又可分为强调功能单元间的协同的事件级联动和基于信息综合分析的知识级联动。这些信息源主要包括各种安全功能单元的日志信息、审计信息、报警信息、事件信息、系统各种服务信息等等，从信息收集，安全分析，知识提取到策略调整，这种信息的综合处理思想，是提高防范能力的先进思想。但是，网络的安全状况，随着网络技术、黑客技术、网络环境等相关因素的变化而呈现出来的不断变化的特性，仅就攻击和防护技术的发展而言也往往是此消彼长。因此对网络系统的周期性评估和对安全防范能力的即时更新都是必须考虑的因素，在过程上，防范策略要随着网络环境和安全状况的变化不断调整，防护、检测、响应和恢复的各个阶段应紧密协调，其安全策略也要实时更新。同时防护技术体系引入风险管理，它的实施是我们对网络系统安全状况的认识不断深入的良好途径。它也是对于网络动态防御的有力支持。至少包含:漏洞扫描，信息收集与分析控制，攻击实时检测识别，恢复技术，安全数据库的更新维护，系统自适应技术等安全技术单元。从而反映了网络安全的如下内涵:安全系统具有免疫力;扩大安全检测的范畴;引入知识库，使安全系统具有学习进化功能;很好的辅助安全管理;具有强大的系统恢复功能。

总之，上述的安全防御体系可以说为下一代互联网的广泛应用做好了准备，从理论以及应用上保障了网络上各种应用的实施。

5 基于防火墙针对IPv6网络的安全研究

5.1 传统防火墙的架构与工作方式

防火墙可以使用户的网络规划更加清晰明了，全面防止跨越权限的数据访问（因为有些人登录后的第一件事就是试图超越权限限制）。一套完整的防火墙系统通常是由屏蔽路由器和代理服务器组成[40]。屏蔽路由器是一个多端口的IP路由器，它通过对每一个到来的IP包依据组规则进行检查来判断是否对之进行转发。屏蔽路由器从包头取得信息，例如协议号、收发报文的IP地址和端口号、连接标志以至另外一些IP选项，对IP包进行过滤。代理服务器是防火墙中的一个服务器进程，它能够代替网络用户完成特定的TCP/TP功能。一个代理服务器本质上是一个应用层的网关，一个为特定网络应用而连接两个网络的网关。用户就一项TCP/TP应用，比如Telnet或者FTP，同代理服务器打交道，代理服务器要求用户提供其要访问的远程主机名。当用户答复并提供了正确的用户身份及认证信息后，代理服务器连通远程主机，为两个通信点充当中继。整个过程可以对用户完全透明。用户提供的用户身份及认证信息可用于用户级的认证。最简单的情况是：它只由用户标识和口令构成。但是，如果防火墙是通过Internet可访问的，应推荐用户使用更强的认证机制，例如一次性口令或回应式系统等。

屏蔽路由器的最大优点就是架构简单且硬件成本较低，而缺点则是建立分组过滤规则比较困难，加之屏蔽路由器的管理成本及用户级身份认证的缺乏等。好在路由器生产商们已经认识到并开始着手解决这些问题，他们正在开发编辑分组过滤规则的图形用户界面，制订标准的用户级身份认证协议，以提供远程身份认证拨入用户服务代理服务器的优点在于用户级的身份认证、日志记录和帐号管理。其缺点关系到这样一个事实：要想提供全面的安全保证，就要对每一项服务都建立对应的应用层网关。这个事实严重地限制了新应用的采纲。屏蔽路由器和代理服务器通常组合在一起构成混合系统，其中屏蔽路由器主要用来防止IP欺骗攻击。目前采用最广泛的配置是Dualhomed防火墙、被屏蔽主机型防火墙以及被屏蔽子网型防火墙。

通常架设防火墙需要数千甚至上万元的投入，而且防火墙需要运行于一台独立的计算机上，因此只用一台计算机连入互联网的用户是不必要架设防火墙的，况且这样做即使从成本方面讲也太不划算。目前观之，防火墙的重点还是用来保护由许多台计算机组成的大型网络。防火墙可以是非常简单的过滤器，也可能是精心配置的网关，

但它们的原理是一样，都是监测并过滤所有通向外部网和从外部网传来的信息，防火墙保护着内部敏感的数据不被偷窃和破坏，并记下来通讯发生的时间和操作等等，新一代的防火墙甚至可以阻止内部人员故意将敏感数据传输到外界。当用户将单位内部的局部网连入互联网时，大家肯定不愿意让全世界的人随意翻阅你单位内部人员的工资单、各种文件资料或者是数据库，但即使在单位内部也存在数据攻击的可能性。例如一些心怀叵测的电脑高手可能会修改工资表和财务报告。而通过设置防火墙后，管理员就可以限定单位内部员工使用Email、浏览WWW以及文件传输，但不允许外界任意访问单位内部的计算机，同时管理员也可以禁止单位中不同部门之间互相访问。将局部网络放置防火墙之后可以阻止来自外界的攻击。而防火墙通常是运行在一台单独的计算机之上的一个特别的软件，它可以识别并屏蔽非法的请求

5.2 防火墙的体系结构

1. 屏蔽路由器(ScreeningRouter)

屏蔽路由器可以由厂家专门生产的路由器实现，也可以用主机来实现。屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查。路由器上可以安装基于IP层的报文过滤软件，实现报文过滤功能。许多路由器本身带有报文过滤配置选项，但一般比较简单。单纯由屏蔽路由器构成的防火墙的危险包括路由器本身及路由器允许访问的主机。屏蔽路由器的缺点是一旦被攻击后很难发现，而且不能识别不同的用户。

2. 双穴主机网关(DualHomedGateway)

双穴主机网关是用一台装有两块网卡的堡垒主机的做防火墙。两块网卡各自与受保护网和外部网相连。堡垒主机上运行着防火墙软件，可以转发应用程序，提供服务等。与屏蔽路由器相比，双穴主机网关堡垒主机的系统软件可用于维护系统日志、硬件拷贝日志或远程日志。但弱点也比较突出，一旦黑客侵入堡垒主机并使其只具有路由功能，任何网上用户均可以随便访问内部网。

3. 被屏蔽主机网关(ScreenedGatewy)

屏蔽主机网关易于实现也最为安全。一个堡垒主机安装在内部网络上，通常在路由器上设立过滤规则，并使这个堡垒主机成为从外部网络惟一可直接到达的主机，这确保了内部网络不受未被授权的外部用户的攻击。如果受保护网是一个虚拟扩展的本地网，即没有子网和路由器，那么内部网的变化不影响堡垒主机和屏蔽路由器的配置。危险带限制在堡垒主机和屏蔽路由器。网关的基本控制策略由安装在上面的软件决定。如果攻击者没法登录到它上面，内网中的其余主机就会受到很大威胁。这与双穴主机网关受攻击时的情形差不多。

4．被屏蔽子网(ScreenedSubnet)

被屏蔽子网就是在内部网络和外部网络之间建立一个被隔离的子网，用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。在很多实现中，两个分组过滤路由器放在子网的两端，在子网内构成一个 DNS，内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信。有的屏蔽子网中还设有堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。这种配置的危险仅包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。如果攻击者试图完全破坏防火墙，他必须重新配置连接三个网的路由器，既不切断连接又不要把自己锁在外面，同时又不使自己被发现，这样也还是可能的。但若禁止网络访问路由器或只允许内网中的某些主机访问它，则攻击会变得很困难。在这种情况下，攻击者得先侵入堡垒主机，然后进入内网主机，再返回来破坏屏蔽路由器，并且整个过程中不能引发警报。

5．3 防火墙的基本类型

如今市场上的防火墙林林总总，形式多样。有以软件形式运行在普通计算机之上的，也有以固件形式设计在路由器之中的。总的来说主要可以分为两种：分组过滤防火墙、代理服务器[38][8]。

1．分组过滤防火墙(IPFiltingFirewall)

分组过滤(PacketFilter)是在网络层中对数据包实施有选择的通过，依据系统事先设定好的过滤逻辑，检查数据流中的每个数据包，根据数据包的源地址、目标地址、以及包所使用端口确定是否允许该类数据包通过。在互联网这样的信息包交换网络上，所有往来的信息都被分割成许许多多一定长度的信息包，包中包括发送者的 IP 地址和接收者的 IP 地址。当这些包被送上互联网时，路由器会读取接收者的 IP 并选择一条物理上的线路发送出去，信息包可能以不同的路线抵达目的地，当所有的包抵达后会在目的地重新组装还原。分组过滤式的防火墙会检查所有通过信息包里的 IP 地址，并按照系统管理员所给定的过滤规则过滤信息包。如果防火墙设定某一 IP 为危险的话，从这个地址而来的所有信息都会被防火墙屏蔽掉。这种防火墙的用法很多，比如国家有关部门可以通过分组过滤防火墙来禁止国内用户去访问那些违反我国有关规定或者“有问题”的国外站点，例如 www.playboy.com、www.cnn.com 等等。分组过滤路由器的最大的优点就是它对于用户来说是透明的，也就是说不需要用户名和密码来登录。这种防火墙速度快而且易于维护，通常作为第一道防线。分组过滤路由器的弊端也是很明显的，通常它没有用户的使用记录，这样我们就不能从访问记录中发现黑客的攻击记录。而攻击一个单纯的分组过滤式的防火墙对黑客来说是比较容易的，他们在这一方面已经积了大量的经验。“信息包冲击”是黑客比较常用的一种攻

击手段，黑客们对分组过滤式防火墙发出一系列信息包，不过这些包中的 IP 地址已经被替换掉了(FakeIP)，取而代之的是一串顺序的 IP 地址。一旦有一个包通过了防火墙，黑客便可以用这个 IP 地址来伪装他们发出的信息。在另一些情况下黑客们使用一种他们自己编制的路由器攻击程序，这种程序使用路由器协议(RoutingInformation Protcol)来发送伪造的路由信息，这样所有的包都会被重新路由到一个入侵者所指定的特别地址。对付这种路由器的另一种技术被称之为"同步淹没"，这实际上是一种网络炸弹。攻击者向被攻击的计算机发出许许多多个虚假的"同步请求"信号包，当服务器响应了这种信号包后会等待请求发出者的回答，而攻击者不做任何的响应。如果服务器在 45 秒钟里没有收到反应信号的话就会取消掉这次请求。但是当服务器在处理成千上万个虚假请求时，它便没有时间来处理正常的用户请求，处于这种攻击下的服务器和死锁没什么两样。此种防火墙的缺点是很明显的，通常它没有用户的使用记录，这样我们就不能从访问记录中发现黑客的攻击记录。

此外，配置繁琐也是分组过滤防火墙的一个缺点。它阻挡别人进入内部网络，但也不告诉你何人进入你的系统，或者何人从内部进入网际网路。它可以阻止外部对私有网络的访问，却不能记录内部的访问。分组过滤另一个关键的弱点就是不能在用户级别上进行过滤，即不能鉴别不同的用户和防止 IP 地址盗用。分组过滤型防火墙是某种意义上的绝对安全的系统。

2．代理服务器(ProxyServer)

代理服务器通常也称作应用级防火墙。分组过滤防火墙可以按照 IP 地址来禁止未授权者的访问。但是它不适合单位用来控制内部人员访问外界的网络，对于这样的企业来说应用级防火墙是更好的选择。所谓代理服务，即防火墙内外的计算机系统应用层的链接是在两个终止于代理服务的链接来实现的，这样便成功地实现了防火墙内外计算机系统的隔离。代理服务是设置在 Internet 防火墙网关上的应用，是在网管员允许下或拒绝的特定的应用程度或者特定服务，同时，还可应用于实施较强的数据流监控、过滤、记录和报告等功能。一般情况下可应用于特定的互联网服务，如超文本传输(HTTP)、远程文件传输(FTP)等。代理服务器通常拥有高速缓存，缓存中存有用户经常访问站点的内容，在下一个用户要访问同样的站点时，服务器就用不着重复地去处理同样的内容，既节省了时间也节省了网络资源。

5．4 IPv6 分组过滤防火墙系统存在的问题

目前 IPv6 普遍采用的分组过滤的防火墙系统主要存在的问题有：

（1）通常的防火墙都要对分组所采用的协议、TCP/IP 的端口号进行过滤，但采

用ESP加密后，这些信息将无法获得，因此会降低防火墙的性能。

（2）由于隧道模式的ESP对全部分组加密，不怀好意的外部主机可采用隧道模式的ESP要求与局域网内的主机建立连接，防火墙将不能发现这类攻击。

为了解决以上问题，针对上述的几种不同的防火墙系统结构，提出如下不同的改进方案，给防火墙加入认证和保密机制，它们将提供不同的安全强度。

1．对分组过滤体系结构的研究与实现

这种结构是最简单的一种防火墙系统，这只在内部局域网与Internet之间配置一个分组过滤路由器，由于该路由器根据过滤规则对Internet的IP数据报进行允许通过或阻塞的决定。此类方案虽然具有便宜和对服务设施透明等优点，但它是最不安全的防火墙系统，因为局域网内的任何主机可以直接和外部主机交换数据，路由器一旦被穿透，每一个主机都可能直接受到攻击。

对这种结构的防火墙的一种简单的改进手段是在分组过滤路由器的过滤原则中加入检测该分组中有无AH和ESP扩展头的过滤规则，这样可以强制使用IPv6检测，从而实现简单的认证，但这样无法实现对分组数据的进一步的认证，从而无法拒绝假冒分组。那么能否让路由器实现对AH扩展头的校验呢，这将带来另一个问题：若让路由器能够校验IPv6中AH数据报头，则必须有相应的密钥，一种解决方法是路由器要求终端主机密钥发过来，但这样路由器也可以产生正确的AH数据报头，这样路由器虽然可以校验认证信息，但公钥算法会消耗大量的CPU资源，当许多主机通过一个路由器通信时，大量的计算将使路由器成为一个阻碍通信的瓶颈，大大的影响网络的吞吐率，因此，这种实现也是不现实的。

可见，对于分组过滤路由器防火墙系统的改进，只能提供简单的对IPv6的认证，下面介绍一个可以实现对分组数据进行认证和保密的防火墙系统。

2．对被屏蔽主要体系结构的研究与实现

被屏蔽主机体系结构是较为常用的一种防火墙，它在内部局域网与Internet之间配置了一个分组过滤路由器和一个堡垒主机。其中，堡垒主机设置在内部局域网上的，而分组过滤路由器放置在堡垒主机与Internet之间，过滤规则要求所有主机仅能接入到堡垒主机，而所有直接去往内部局域网的外部流量将全部被阻塞。显然，被屏蔽主机体系结构较之分组过滤体系结构有更高的安全性。因为该种方案结构可在网络层(分组过滤)和应用层(应用代理)实现双重过滤。

下面介绍如何改进该防火墙系统，使其能够对所有分组数据实现认证和保密。显然，由于分组过滤体系结构中的原因，路由器不能实现这个功能，它只能实现对IPv6的简单认证，考虑到堡垒主机是外部唯一能接入的主机，且所有外部流量都必须流经堡垒主机，因此，可以由堡垒主机实现对IP数据报的AH数据报头的校验。由于一部分过滤信息被加密，分组过滤路由器的工作得到简化，只需对明文部分路由信息进行

过滤，而堡垒主机除了实现原先的工作(如：应用代理、日志功能等)外，还需要对解密后的部分信息(如：端口号、内部地址等)进行过滤，并根据对 AH 数据报头的校验结果进行接入控制。改进后的防火墙层次结构和相应的工作流程图如图 5.4.1 所示。

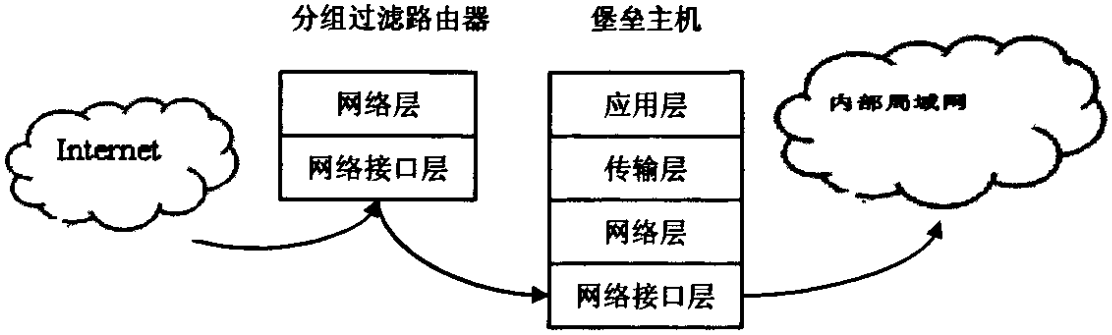

图 5.4.1　改进后的防火墙层次结构和相应的工作流程图

下面介绍具体的实现步骤：

(1)分组过滤路由器由网络接口层接收到外部主机传输的帧，提到 IP 数据报，提交到网络层处理，由于 IPv6 隧道模式采用 ESP 加密封装技术，路由器只对外部数据报头中的源地址及网关地址(此外，分组过滤路由器相当于安全网关)等明文信息进行过滤，依据过滤规则转发或丢弃该数据报，并根据规则决定是否回发一个 ICMP 消息，以及是否通知堡垒主机将该分组及相应的执行动作等情况写入日志。

(2)堡垒主机收到路由器转发的数据报后，在网络层需做如下工作：首先去掉外部 IP 头，然后由 ESP 数据报头的 SPI(Security Parameters Index)域的值计算得到密钥，接着对实际的内部 IP 分组进行解密或对 AH 数据报头进行校验(解密和认证的顺序取决于发端相应操作的顺序)。若不能确认收到的分组的确是则分组数据报头中标识的源 IP 端发出的，则丢弃该分组，若能通过认证，则依据过滤规则对解密后的实际 IP 分组中的某些信息(如：端口号等)进行过滤，不符合条件的分组将被丢弃，过滤后的分组中的数据载荷部分将上将传输层处理。

(3)传输层将处理后的数据载荷向上交给应用层，应用层中包含了使用传输层协议去传送数据的所有协议，如：FTP、SMTP 等协议。堡垒主机在该层的功能相当于一个应用网关，它运行特定的应用软件来过滤掉该系统认为不安全的应用业务。

(4)堡垒主机将通过以上过滤的分组进行重新打包，发向实际的局域网内部的主机，并根据规则对丢弃的分组进行处理。

以上介绍了对被屏蔽主的防火墙系统的改进，可以看到改进后的防火墙可以实现对 IPv6 分组的认证和保密，需要指出的是，在该方案中，由于 IPv6 中很占 CPU 时间的密码算法的使用。使得堡垒主机和负担将加重，因此对其相应的设计也应加强，目前已经有一些解决方法，如：采用额外的硬件实现密码算法的计算，或采用多个并行

的堡垒主机等。另外，由于加密只在外部主机堡垒主机之间进行，虽然这样可以减轻内部子网的主机处理加密的负担，并简化了密钥分发任务，但存在这样的一个问题：即堡垒主机与局域网内主机以及局域网内主机之间的数据交换是采用明文信息(若由堡垒主机实现子网内流量的加密和认证，则其工作量将增加一倍以上，这将大大影响该系统的吞吐率)，这对于大型局域网，特别是具有保密部门的局域网是非常不利的。下面介绍的这类防火墙改进系统可以有效地解决上述问题。

3. 对被屏蔽子网体系结构的研究与实现

被屏蔽子网体系结构采用两个分给过滤路由器和一个堡垒主机，这三者单独构成一个子网，位于内部局域网和 Internet 之间，称之为被屏蔽子网。外部路由器介于 Internet 与被屏蔽子网之间，而内部路由器保护子网与内部可信局域网之间，两个路由器可以进行不同级别的过滤，被屏蔽子网只允许 Internet 和局域网接入到堡垒主机中，其他所有试图绕过它的流量都将被阻塞掉。与被屏蔽主机方案相比，本方案提供了更高的安全性。其中，内部路由器提供了第二道防线，它只接收来自堡垒主机的分组。在被屏蔽主机方案中，对系统的改进使其具备了对来自 Internet 的分组的认证和保密能力。这种改进同样适用于本方案中，与此同时，在本方案中由于内部路由器是到达内部局域网的唯一入口，可以考虑由其实现内部局域网的安全要求。其实现步骤如下：

(1)外部路由器和堡垒主机的工作是外部进入内部局域网的唯一入口，堡垒主机的安全级别越高，被屏蔽路由器网关是比较安全的。

(2)内部路由器对于来自堡垒主机的流量，首先根据源地址等信息以及子网 内各主机的安全级别进行再次过滤，然后根据该分组的局域网内实际地址，对该分组进行 ESP 封装加密(密钥的来源可取自堡垒主机)，然后转发分组至目的端。

(3)内部路由器在处理由局域网内通往 Internet 的流量时，首先对该分组解密，然后根据各主机的不同权限和该系统的安全策略进行过滤，通过的流量由堡垒主机进行封装加密后转发。

(4)若局域网内各主机有不同的安全级别(如：一些保密单位主机要求限制对其的访问)，可强制所有通往保密主机的流量都由内部路由器路由，进而可由内部路由器解密后实现接入控制。

以上方案的实现，需要在局域网内存在一套独立的密钥的分配协议，这可以考虑在安装防火墙系统时由客户端软件实现。

6 基于 IP 地址限制 IPv6 防火墙的实现

IPv6 网络防火墙实现起来要比传统的防火墙要困难，不但要实现对子网和堡垒主机的保护，下面就以其中的一个模块的实现方式进行论述，如图 6.1 所示。这个模块主要是实现的功能是对读入的 IP 地址定时比较，从而发现有没有 IP 欺诈行为，从而对这类地址进行 IP 限制，实现对堡垒主机与子网的保护。

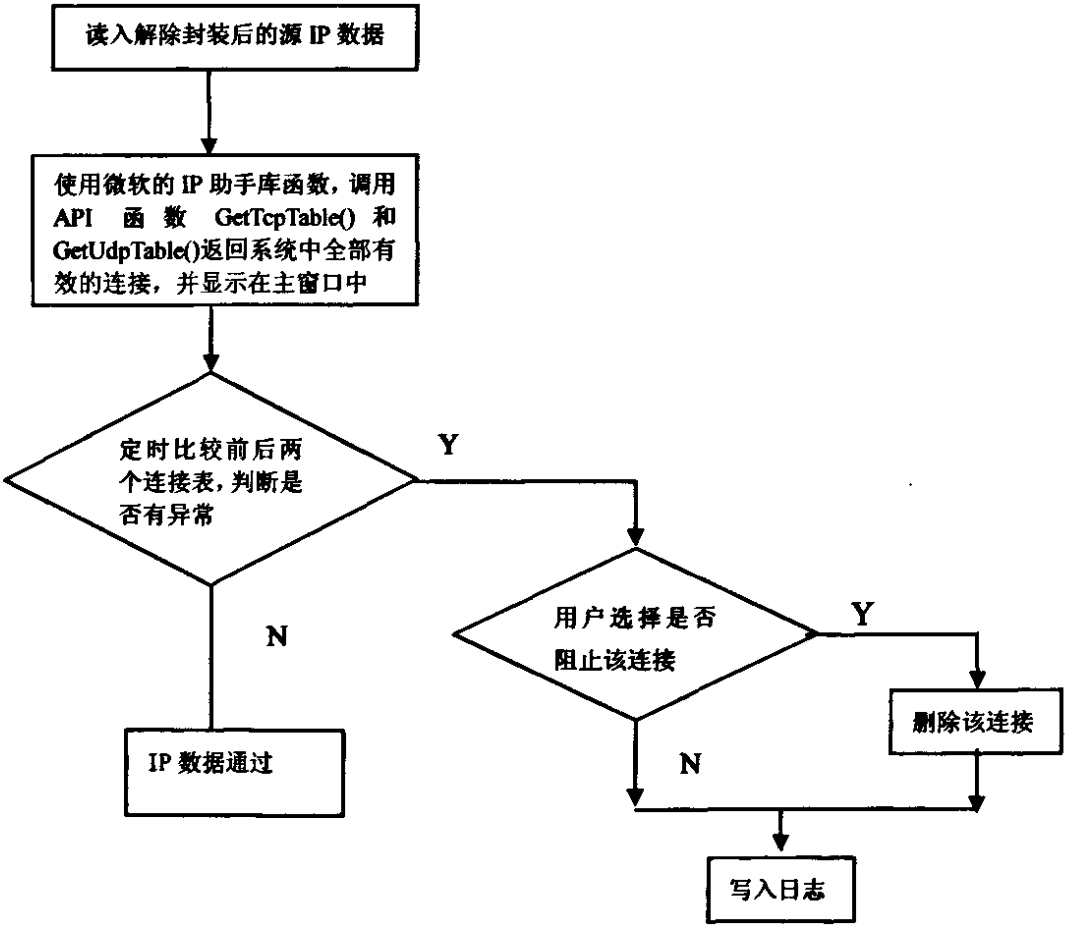

图 6.1 模块示意图

实现策略：在防火墙系统初始化成功后，这个模块就开始监听网卡中的数据包，每接收一个数据包，就利用系统 API 函数对数据包进行拆包分析，先判断该数据包的源 IP 是不是被阻止的 IP，如果是，直接删除该连接，否则进行下一步判断，是否为内部网发送的数据，如果是内部网发，而且又设置了自动允许网络通过，则系统自动允许该连接通过，进行下一个数据包的判断。否则的话，则转入常规判断，进行一步一步的筛选，判断，过滤，例如判断是否前后两个同样 IP 的数据包垮域访问了，或

者根据用户在设置防火墙的安全水准高低不符合该安全水准的安全度了，将会出现一个警告提示框，询问用户是否阻止该连接，其中分为阻止该 IP，阻止远程端口，阻止本机端口等等，根据用户的选择，系统进行删除该连接，允许该连接通过等，将信息写入日志文件，以备日后查询。

6．1 定义模块的功能

由于 ICMPv6 是 IPv6 的体系的结构总体的一个组成，由所有 IPv6 实现完全支持。ICMPv6 具备了 IPv4 的中的 ICMP 的所有功能，并且抛弃了一些不再使用的过时消息类型，提供了一些简化功能。实现上，ICMPv6 合并了 IPv4 中多个协议功能，其中主要有以下协议功能。ICMP、IGMP、ARP。并提供了多种网络功能：错误报告、网络诊断、邻居发现、多播实现。

在用户上网时对 IP 数据读入，在前面的防火墙对 IP 地址利用密钥算法解除封装后，定时 IP 地址数据进行比较，从而实现更及时，更有效的保护。

在 IPv6 数据报各项域中需要注意的是“下一个头”这一项有些特殊，“下一个头”是指在 IPv6 中，在需要的时候将可选择的互联网信息编码放在单独的头中，即在基本头和下一层头之间放置扩展头。这种扩展头包括：逐跳选项头、路由选项头、分段选项头、目的选项头、认证选项头和封装安全载荷选项头等 6 种头。而且每个扩展头都被一个明确的“下一个头”域的值所确定，每个 IPv6 数据包根据需要可以有 0 个，1 个或多个扩展头，每个扩展头由前一个头的“下一个头”域所确定。

有了 IPv6 数据包的结构，就可以去拆分 IPv6 数据包了，我们知道 IPv6 数据包中源 IPv6 地址是从 63 位开始到 191 位的 128 位组成，目的 IPv6 地址是从 192 位到 320 位的 128 位组成。所以在第一步判断中只需将一个 IPv6 数据包的这两段数据取出来与数据中的阻止 IP 是否一致就行了，所以，通过 IP 助手库函数(iphlpapi.dll)，用其中的 GetTcpTable 函数能返回当前系统中全部有效的 TCP 连接，接到任何一个连接之后，我们便可看到接收的是一个 16 进制的 IPv6 数据包，用 Mid(String, Start As Long, [Length]) 方法即 Mid(string,8,16) 可得到源 IPv6 地址，用 Mid(string,24,16)便可得到目标 IPV6 地址。

下面在 visual studio 6.0 的环境下对这一模块进行了定义。

需要注意的是该项目的核心部分，即怎样获取网络信息的部分，并不是由个人直接实现的，大部分均是直接调用的 IP 助手库中的 API 函数，由于 SOCKET API 在 windows 平台和 linux 平台下基本上是一样的，所以用一些系统提供的 API 函数，可以解决比较复杂的问题。下面主要介绍一个网络模块，中间用到了大量的 API 函数。

6.2 实现步骤

（1）第一步：定义一些 ICMPv6 协议，ICMPv6 是 IPv6 标准必须的一部分，它的作用是 IPv6 协议利用它的作用，使用 IPv6 通信的主机和路由器就可以报告错误并发送简单的回显消息。

```
Public MIBICMPSTATS As MIBICMPSTATS
Public Type MIBICMPSTATS
    dwEchos As Long
    dwEchoReps As Long
End Type
Public MIBICMPINFO As MIBICMPINFO
Public Type MIBICMPINFO
    icmpOutStats As MIBICMPSTATS
End Type
Public MIB_ICMP As MIB_ICMP
Public Type MIB_ICMP
    stats As MIBICMPINFO
End Type
Public Declare Function GetIcmpStatistics Lib "iphlpapi.dll" (pStats As MIBICMPINFO)
As Long
Public Last_ICMP_Cnt As Integer 'ICMP count
```

（2）第二步：定义一些 TCP 协议的属性,定义在传输时要针对 IP 地址建立一个上一时段重新对比数据。

```
Type MIB_TCPROW
  dwState As Long
  dwLocalAddr As Long
  dwLocalPort As Long
  dwRemoteAddr As Long
  dwRemotePort As Long
End Type
Type MIB_TCPTABLE
  dwNumEntries As Long
  table(100) As MIB_TCPROW
End Type
```

```
Public MIB_TCPTABLE As MIB_TCPTABLE
Declare Function GetTcpTable Lib "iphlpapi.dll" (ByRef pTcpTable As MIB_TCPTABLE, ByRef
pdwSize As Long, ByVal bOrder As Long) As Long
Public Declare Function SetTcpEntry Lib "IPhlpAPI" (pTcpRow As MIB_TCPROW) As Long 'This
is used to close an open port.
Public IP_States(13) As String
Private Last_Tcp_Cnt As Integer 'TCP connection count
```

（3）第三步：定义 winsock 相关内容，把不同时间的地址实现转化。

```
Private Const AF_INET = 2
Private Const IP_SUCCESS As Long = 0
Private Const MAX_WSADescription = 256
Private Const MAX_WSASYSStatus = 128
Private Const SOCKET_ERROR As Long = -1
Private Const WS_VERSION_REQD As Long = &H101
Type HOSTENT
    h_name As Long        ' official name of host
    h_aliases As Long     ' alias list
    h_addrtype As Integer ' host address type
    h_length As Integer   ' length of address
    h_addr_list As Long   ' list of addresses
End Type
Type servent
  s_name As Long          ' (pointer to string) official service name
  s_aliases As Long       ' (pointer to string) alias list (might be null-seperated
with 2null terminated)
  s_port As Long          ' port #
  s_proto As Long         ' (pointer to) protocol to use
End Type
Private Type WSADATA
   wVersion As Integer
   wHighVersion As Integer
   szDescription(0 To MAX_WSADescription) As Byte
   szSystemStatus(0 To MAX_WSASYSStatus) As Byte
   wMaxSockets As Long
   wMaxUDPDG As Long
```

```
    dwVendorInfo As Long
End Type
Public Declare Function ntohs Lib "WSOCK32.DLL" (ByVal netshort As Long) As Long
'inet_addr 将 IP 地址从点数格式转换成无符号长整型
Private Declare Function inet_addr Lib "WSOCK32.DLL" (ByVal CP As String) As Long
' inet_pton() API 函数，将 IP 地址从 点数格式转换成 ASCII，该函数是 socket API 为适应 IPv6 所做的改动，可以将 IP 地址转化为字符串地址，该函数对应在 IPv4 下的方法是 inet_ntoa,功能和它是一样的。
Private Declare Function inet_pton( )  Lib "WSOCK32.DLL" (ByVal inn As Long) As Long
'getipnodebyaddr() API 函数，该函数的作用是由 IP 地址获得名字，它同样有 IPv4 的版本 gethostbyaddr()
Private Declare Function getipnodebyaddr Lib "WSOCK32.DLL" (Addr As Long, ByVal addr_len As Long, ByVal addr_type As Long) As Long
'getipnodebyname() API 函数,它的作用是由信息中包含的主机名获取它对应的 IP 地址，它的 IPV4 专用函数是 gethostbyname,功能是一样的。
Private Declare Function getipnodebyname Lib "WSOCK32.DLL" (ByVal host_name As String) As Long
'WSAStartup 该函数的第一个参数指明程序请求使用的 Socket 版本，其中高位字节指明副版本、低位字节指明主版本；操作系统利用第二个参数返回请求的 Socket 的版本信息。当一个应用程序调用 WSAStartup 函数时，操作系统根据请求的 Socket 版本来搜索相应的 Socket 库，然后绑定找到的 Socket 库到该应用程序中。以后应用程序就可以调用所请求的 Socket 库中的其它 Socket 函数了。该函数执行成功后返回 0。
Private Declare Function WSAStartup Lib "WSOCK32.DLL" (ByVal wVersionRequired As Long, lpWSADATA As WSADATA) As Long
Private Declare Function WSACleanup Lib "WSOCK32.DLL" () As Long
' RtlMoveMemory 若该函数的返回值非 0，则为存储器的地址。由于 VB 不能直接操作地址，所以还必须调用 RtlMoveMemory 函数将数据写入地址中
Private Declare Sub RtlMoveMemory Lib "kernel32" (hpvDest As Any, ByVal hpvSource As Long, ByVal cbCopy As Long)
'将数据转换为内存二进制形式字符串
Declare Sub CopyMemory Lib "kernel32" Alias "RtlMoveMemory" (Dest As Any, Src As Any, ByVal cb&)
Declare Function lstrlen Lib "kernel32" (ByVal lpString As Any) As Integer
Private Blocked As Boolean
'使用微软的 IP 助手库函数（iphlpapi.dll）是一个捷径。其中的 GetTcpTable 函数能返回当前
```

系统中全部有效的 TCP 连接,在这个项目中我们在 frmMain 窗体中用到了 GetTcpTable 函数,GetAscIP()函数的功能是得到一个数据流中的 IPV6 地址

```
Public Function GetAscIP(ByVal inn As Long) As String
  Dim nStr&
    Dim lpStr As Long
    Dim retString As String
     '定义一个 128 位的字符串，用于接收 IPv6 地址
    retString = String(128, 0)
     '调用 API 函数，将 IP 地址转化为 ASCII 型
    lpStr = inet_pton(inn)
    If lpStr Then
        nStr = lstrlen(lpStr)
        If nStr > 128 Then nStr = 128
        CopyMemory ByVal retString, ByVal lpStr, nStr
        retString = Left(retString, nStr)
        GetAscIP = retString
    Else
         '如果不能转化的话,说明数据包在传输过程中出错了,提示不能得到 IP
        GetAscIP = "不能得到 IP"
    End If
End Function
```

通过以上的几个主要步骤，就能实现对 IP 地址的限制，从而实现一些对内部子网和堡垒主机的实时保护。

以上就是对这个模块的一些方面做了简单的一些阐述,一些方面还没有完全考虑成熟，这些完全成熟的方面也是下一步的要完善的。由于 IPv6 防火墙在网络在的功能巨大，要实现各种功能是一项复杂的工程。

7 结 论

基于IPv6的下一代网络，正在受到越来越多的国家和研究单位的关注。中国、日本、韩国和欧洲以及美洲都在IPv6研发中投入了巨大的精力和时间。现在各国都在建立IPv6试验网，并对下一步大规模的IPv6普及作了一定的部署。但是，随着IPv6的提出，网络安全也面临了新的课题，如何在新环境下构造一个安全的网络，实现网络数据安全传输、交换、保存都是有待研究和解决的问题。

本文首先对IPv6的概况以及一些相关技术如IPv6寻址、IPv6报头、IP Sec的体系结构进行简单介绍，对于IPv4协议安全方面的一些缺点进行了分析，讨论了OSI的网络安全体系结构，给出IPv6新的网络安全机制，详细描述了IP Sec所提供的网络安全服务与实现原理，并对IP Sec的两个安全协议:AH和ESP作了较深入的阐述。

IPv4 /IPv6的过渡是一个相对漫长的过程，如何在两者之间进行过渡是一个很重要的研究课题。本文对于主要三种主要的过渡技术:双栈、隧道和转换技术，并对目前流行的过渡方案如DSTM, ISATAP, NAT PT等没有做主要介绍。在向IPv6协议的转换过程中，传统的网络安全工具仍然不可或缺，但是它们都必须加以改进以适应IPv6协议的要求。本文在对漏洞扫描、防火墙、入侵检测以及安全审计等网络安全工具在IPv6的环境下如何进行改进进行了深入分析，并强调了安全审计技术在网络安全工具中的重要作用。

在基于以上安全工具在IPv6下改进的基础上，提出了一种基于IPv6的下一代网络的动态安全防御体系，并对其应用前景作了展望。防火墙提供了一个经济有效的手段来解决通过公用网络安全的问题。它在基于IPv6的下一代网络中将会起到十分重要的作用。

本文最后对IPv6防火墙实现IP地址限制的一个模块进行了分析讲解，在VB实现对IPv6数据的分解。从另一个方面理解在现有的网络安全手段。但是也有很多没有实现的功能。因此，在以后关于IPv6的安全研究方面还必须解决下面的一些问题:

1. IP Sec的安全增强技术，解决IP Sec的密钥分配和管理问题，使它真正能够对IPv6 的安全起到支持的作用;

2. IPv6中邻居发现协议和自动配置的安全增强问题，必须研究更好的方法来保护邻居发现和自动配置过程;

3. 过渡机制下的安全风险和管理手段。随着IPv6的发展，将有较长的一段时期处于IPv6与IPv4共存的状况，保证这个时期的安全性十分重要;

4. IPv6环境下的安全产品和安全工具的研发和使用。当前许多安全产品还没有完成向IPv6的过渡和升级，同时新的条件下安全产品的相互配合和管理使用急需规

范。新的适合IPv6的隔离安全模型及其相关实现技术也可能成为研究的热点；

5．移动IPv6的安全问题如身份认证、数字签名等安全相关技术，这已经成为下一代网络中的研究热点。

致 谢

本论文是在我的导师钱焕延教授悉心指导下完成的。在论文的选题、设计、实现、论文撰写等方面。钱老师都给了我耐心的指导和无私的帮助。

钱老师的精益求精治学作风，严谨求实的科学态度，精辟的学术观点和宽广的学术视野，平易近人的工作作风对我今后的发展将产生的影响，在此，向钱老师表示衷心的感谢！

论文得以顺利完成，要感谢现代教育技术中心提供的良好的学习环境、先进的设备和丰富的资料。借助校园网提供的优越条件使我不仅在理论上对所研究的课题有了深入的认识而且对实际中的应用有了深入的了解。这对我在夯实基础理论和积累科研实践经验方面起到了有益的促进作用。

感谢中国教育与科研计算机网提供的关于下代网络及 IPv6 的宝贵信息，它对下一代网络技术的发展的评论使我受益匪浅。

我要衷心感谢我在河南职业技术师范学院的同学李学勇，还有我教研室的同学，还有寝室的几个兄弟，他们对我的论文写作给了极大的意见和帮助。

最后，我要感谢我的父母，在我上学期间一直给支持。他们无私的奉献是我在人生道路上克服困难，取得进步的最大动力。

参考文献

[1] Eric Maild .网络安全基础教程 马海军，王译波等译 第2版 北京：清华大学出版社， 2005.7

[2] Silia Hagen. IPv6精髓 第4版 北京：清华大学出版社 2004.5:

[3] Marcus Goncalves, Kittty Nilles. IPv6网络 黄锡伟 杨震 译 第3版 北京：人民邮电出版社 2000.4:15-80

[4] 姚小兰 . 网络安全管理与防护 北京理工大学出版社 2002.5:

[5] Pete Losin. IPv6详解 沙斐 ，程莉 ，周立 等译 第3版 北京：机械工业出版社 2000.4

[6] 林闯，汪洋，李泉. 网络安全的随机模型方法与评价技术.《计算机学报》Volume 128,No.12 Dec.2005 ：128-130

[7] 徐超汉，柯宗贵 计算机网络安全实用技术. 第 2 版 北京：电子工业出版社 2005.3

[8] 潘志翔，岑进锋 黑客攻防编程解析. 第1版 北京：机械工业出版社 2003.1

[9] Christian Huitema IPv6 The New Internet Protocol Second Edition Prentice-Hall Interational,Inc 1999.5

[10] 戴宗坤.信息安全实用技术. 第2版 重庆：重庆大学出版社 2005. 5

[11] 王宝会，王大印，范开菊 计算机信息安全教程. 第2版 北京：电子工业出版社 2006.1

[12] Joseph Davies 理解IPv6. 张晓彤，晏国晟，曾庆峰 译. 第1版 北京：清华大学出版社 2004.3

[13] 王达.网管员必读—网络安全. 第2版 北京：电子工业出版社 2006.1

[14] Burce Schneier. 应用密码学. 第3版 北京：机械工业出版社 2000.1

[15] 刘韵洁，张智江 等.下一代网络. 第1版 北京：人民邮电出版社，2005.3

[16] S.Deering,RHInden:RFC2460 Internet Protocol,Version (IPv6) pecificatilon, December 1998

[17] S.kent,R.Atkingson:RFC2401 Security Architecture for the Internet Protocol, November 1998

[18] S.kent,R.Atkingson:RFC2402 IP Authentication Header. November 1998

[19] S.kent,R.Atkingson:RFC2406 IP Encapsulating Security Payload (ESP), November 1998

[20] Oppliger, R. Computer. Security at the Internet layer. Volume 31 , Issue 9, sept . 1998

[21] Steven Brown: Implementing Virtual Networks, McGraw-Hill Companies, Inc. 人民邮电出版社影印版，2000年9月

[22] Hagino, J. Implemenging IPv6:experiences at KAME project. Applications and the internet Workshops, 2003. Proceedings. 2003 Symaposium on 25-31 Jan, 2003

[23] Srivsatava, V. Wargo, C. Lai. Aviation application over IPv6:performance issues Aerospace Conference, 2004. Proceeding. 2004IEEE volume3, Mardh 2004:5-14

[24] P. Hoffman:RFC2406 Algorithms for Internet Key Exchange version 1(IKEv1), May 2005

[25] P. Hoffman:RFC3664 The AES-XCBC-PEF-128 Algorithm for the Internet Key Exchange Protocol(IKE), January 2004

[26] S. Fanke, R. Glenn, S. Kelly:RF3602 The AES-CBC Cipher Algorithm and Its Use with IP Sec, September 2003

[27] P. Metzger, W. Simpson:RFC1828 IP Authentication using Keyed MD5, August 1995

[28] M. Carugi, D. McDysan:RFC4031 Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks(PPVPNs), April 2005

[29] 赵海滨，唐鼎，潘春建，侯自强. IPv6核心路由器设计. 第2版 北京：清华大学出版社，2005.6

[30] 王雅萍，郭放. 下一代校园网设计研究团组织. 第2版 北京：电子工业出版社，2005.5(24)

[31] 郎燕峰. IKE协议的缺陷分析改进建议. 中国金融电脑 2005.4：14

[32] 康金钟，杨明，康志伟. 基于IPv6协议的IP Sec网络安全研究. 长沙电力学院学报 ，2005.4：18

[33] 张千里，陈光英. 网络安全新技术. 第1版 北京：清华大学出版社，2003.4

[34] 杨义先 钮心忻. 网络安全理论与技术. 第2版 北京：人民邮电出版社，2003.2

[35] 叶丹. 网络安全实用技术. 第1版 北京：清华大学出版社，2002.7

[36] 冯登国. 计算机网络与通信安全. 第2版 北京：清华大学出版社，2001.5

[37] 龚俭，陆晟，王倩. 计算机网络安全导论. 第1版 南京：东南大学出版社，2002.6

[38] 肖军模，刘军，周海刚. 网络信息安全. 第2版 北京：机械工业出版社，2003.9

[39] 张炜，郝嘉林，梁煜编著. 计算机网络技术基础教程. 第2版 北京：清华大学出

版社，2005.9.1
[40] 李振强，赵晓宇，马严. IPv6 技术揭密. 第 3 版 北京：人民邮电出版社 2006.4.1
[41] 华为 3COM 技术有限公司编著. IPv6 技术.第 1 版 北京：清华大学出版社 2004.10
[42] 周逊.IPv6-下一代互联网的核心.第 2 版 北京：电子工业出版社 2003.8
[42] 胡建伟. 网络安全与保密. 第 4 版 西安：西安电子科技大学出版社 2003.11