

IPv6 校园网环境下 IPSec VPN 的安全性研究

时 晨, 申普兵, 杨 瑾, 沈向余

(西安通信学院, 陕西 西安 710106)

摘 要: IPv6 在安全性上比 IPv4 有了明显的提高, 但不能很好地保证应用层和协议本身的安全性。IPSec 是网络层的安全协议标准, 它提供了 IP 层上多种安全服务, 其隧道模式为 VPN 的实现提供了必要的安全保障, VPN 也为网关之间的通信提供了安全隧道。通过介绍 IPv6 校园网研究现状, 分析了 IPv6 带来的安全问题, 描述了 IPSec 网络层安全协议标准以及 VPN 技术的基本原理, 详细阐述了 IPSec VPN 的优越性以及如何在 IPv6 校园网中进行安全部署, 并指出了可能存在的不足以及进一步改进的方向。

关键词: IPv6; 校园网; IPSec VPN; 安全性

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2010)10-0167-04

Research on IPSec VPN Security Based on IPv6 Campus Network

SHI Chen, SHEN Pu-bing, YANG Jin, SHEN Xiang-yu

(Xi'an Communications Institute, Xi'an 710106, China)

Abstract: IPv6 is more safer than IPv4, but it could not assure the security of application layer and the protocol. IPSec is security protocol standard of network layer, it offers several security services on IP layer. Its tunnel mode provides essential safeguard for the implementation of VPN, and VPN also affords safe tunnel for communication between gateway. The research areas of IPv6 campus network is introduced, and the security problems of IPv6 are analyzed. The IPSec security protocol standard of network layer and basic theory of VPN technology are described, and the advantages of IPSec VPN and how to deploy safety based on IPv6 campus network are discussed. Based on the potential disadvantages, the development directions are expressed.

Key words: IPv6; campus network; IPSec VPN; security

0 引 言

目前一些重点高校已经完成 IPv6 校园网的基础建设, 用于连接各个高校 IPv6 的下一代科研教育骨干网(CERNET2)也已经搭建起来, 为未来基于 IPv6 网应用的推广打下了基础, 但它们基本上还只停留在网络的基础应用和实验测试使用阶段^[1], 基于 IPv6 的网络安全的解决方案也只处于起步阶段。IPv6 的安全性问题已经成为近年来的研究热点之一。构建基于 IPSec 的虚拟专用网络(VPN)已成为 IPv6 网络安全研究领域的一个重要方向, 为保证 IPv4 向 IPv6 过渡过程中的安全通信提供了一条新的途径。

1 IPv6 校园网的安全问题

目前基于 IPv4 的校园网显示出诸多弊端, IPv6 的

安全性虽然有了明显的提高, 但仍不能保证应用层和协议本身的安全性。对于安全性的定义, 有 3 个公认的目标, 即完整性、机密性和身份验证^[2]。IPv6 的新特性使其在网络机密性、完整性方面有了更好的改进, 在可控性和抗否认攻击性方面有了新的保证。例如: 端到端的安全得到保证、地址分配与源地址的检查、防止未授权的访问、增强 DNS 的抗攻击性、更加灵活的扩展头更有利于加密、防止网络放大攻击以及碎片攻击等。但同时 IPv6 技术本身也带来了新的安全问题:

(1) PKI 至今没有一个系统的管理策略;

(2) 与 IPv4 的防火墙、VPN、IDS、漏洞扫描、网络过滤、防病毒网关等联合安全体系还相差很远;

(3) 协议还需要完善, 目前还难以实现严格的用户限制功能;

(4) 无状态地址自动配置给合法网络用户使用 IPv6 网络带来了方便, 但也引入了安全隐患, 因为协议认为任何可自动配置的节点都是合法的节点, 并能即插即用顺利地接入到本地网络中;

(5) ICMPv6 是 IPv6 的重要组成部分, 但可被利

收稿日期: 2010-02-03; 修回日期: 2010-05-20

基金项目: 2009 年度通信和指挥自动化装备军内科研项目(编号略)

作者简介: 时 晨(1986-), 女, 陕西西安人, 硕士研究生, 研究方向为网络安全; 申普兵, 教授, 研究方向为网络安全。

用来产生拒绝服务攻击,利用 ICMPv6 可以冒充其他节点产生恶意消息(目的不可达、超时、参数错误等)来影响正常通信;

(6) 利用邻居发现协议,通过发送错误的路由器宣告、错误的重定向消息等,让数据包流向不确定的地方,进而达到拒绝服务、拦截和修改数据包的目的。

由于 IPv4 和 IPv6 必然要共存很长一段时间,这就带来了过渡时期的安全问题,已经发现从 IPv4 向 IPv6 转移时出现的一些安全漏洞,如:攻击者可以通过使用安装了双栈的 IPv6 的主机,建立由 IPv6 到 IPv4 的隧道,绕过防火墙对 IPv6 进行攻击等。对于我们来说,IPv6 校园网同样面临这些问题,尤其是在目前校园网的搭建上,应如何保证 IPv6 孤岛之间通信的安全(见图 1),这就要求必须建立一个安全、经济、高效的隧道来保护通过不可信网络时的信息安全。

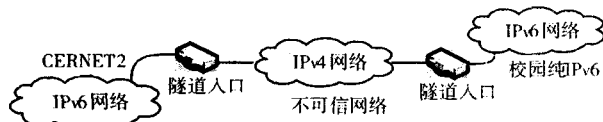


图 1 IPv6 孤岛连接网络拓扑图

2 IPSec VPN 技术原理

2.1 IPSec 协议及原理分析

2.1.1 IPSec 介绍

IPSec 是 VPN 最常用的安全协议^[3]。IPSec 是 IETF IPSec 工作组为了在 IP 层提供通信安全而制定的一套协议簇,能够对数据的存取控制、机密性、完整性和可用性提供保证,并能够防止重放攻击,可应用在 IP 层或在 IP 层与数据链路层之间或在物理线路上。它是一种具有互操作性、高质量、基于加密的规范。IPSec 作为 IPv4 的可选项出现,而在 IPv6 中却是必需的组成部分,因此 IPSec 将能更好地结合在 TCP/IP 协议簇中,更好地保证互联网上数据传输的安全。

2.1.2 IPSec 协议结构

IPSec 协议(见图 2)包括:因特网密钥交换协议(IKE)、验证头(AH)、封装安全载荷(ESP)及安全联盟(SA)。

IPSec 协议使用 IKE 协议实现安全协议的自动安全参数协商,其安全参数包括加密及认证算法、加密及认证密钥、通信的保护模式(传输或隧道模式)、密钥的生存期等^[4]。

IPSec 协议提供两种通信保护机制:ESP 和 AH。它们都能为通信提供抗重放攻击。在隧道模式下,必须使用 ESP 协议对整个 IP 数据进行加密、封装,并附

加一个新的 IP 头,同时可选择使用 AH 协议提供对数据的完整性保护^[5]。

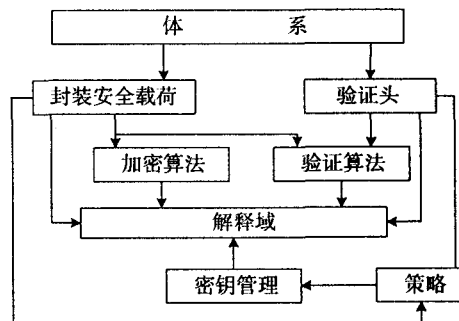


图 2 IPSec 各组件之间的交互方式

SA 是 IPSec 标准中实现安全服务的基础,它定义了一个包含了 IP 封包加密、解密和认证的相关信息的安全“环境”,是指安全服务与服务的载体之间的一个“连接”^[4]。要实现 AH 和 ESP 都必须提供对 SA 的支持,SA 的建立和维护是 IKE 的主要功能。

2.1.3 IPSec 在 IPv6 中的嵌入

IPSec 协议由两种不同模式来提供两方面的保护,传送模式(transport mode)用来保护上层协议,而隧道模式(tunnel mode)用来保护整个 IP 数据报,在这里仅介绍隧道模式,它将要保护的整个 IP 包都需封装到另一个 IP 数据报里,同时在外部和内部 IP 头插入一个 IPSec 头^[4]。

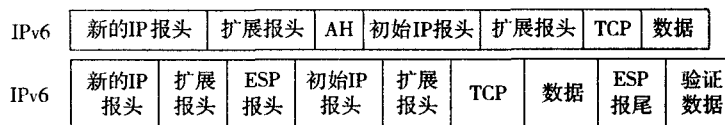


图 3 IPSec 在隧道模式中的嵌入

2.2 VPN 的隧道与安全技术

VPN(Virtual Private Network)是指利用密码技术和访问控制技术在公共网络中建立的专用通信网络^[6]。在 VPN 中,任意两个节点之间的连接没有传统专用网所需的端到端的物理链路,而是利用某种公众网的资源动态组成,虚拟专用网络对用户端透明,用户好像使用一条专用线路进行通信^[7]。

2.2.1 VPN 的隧道技术

隧道技术是 VPN 的基本技术,它解决了专网与公网的兼容问题,能够隐藏发送者、接收者的 IP 地址以及其它协议信息,向用户提供了无缝的、安全的、端端的连接服务,以确保信息资源的安全^[8]。隧道技术在 VPN 的实现中具有如下主要作用:

(1) 远程用户可以通过透明地拨号上网来访问内网,IP 隧道可以任意调整任何形式的有效负载。

(2) 隧道可以利用封装技术,对多个用户、多个不同形式的有效负载进行调整。

(3) 当使用隧道技术访问内网时,内网不会将其 IP 地址报告给公网。

(4) 隧道技术可以对是否滤掉接收者,或对个人隧道连接进行报告进行选择,自主性较强。

2.2.2 VPN 的安全技术

VPN 可以对经过隧道传输的数据进行加密,以保证只有被指定的发送者和接收者才能接触到数据,从而保证数据的私有性和安全性^[9]。

其处理过程如下:

- (1) 被保护的主机将明文信息发送到 VPN 设备;
- (2) 根据网管预先设置的 VPN 设备规则,决定是否让数据通过或是对其进行加密后再通过;
- (3) 对于需要加密的数据,将对整个数据包进行加密,并附上数字签名;
- (4) 为数据包加上特殊的数据报头,其中包括如:目的 VPN 设备所需要的安全信息和初始化参数等;
- (5) 将加密后的数据以及源 IP 地址、目标 VPN 设备的 IP 地址重新封装,之后数据包将允许通过虚拟隧道在公用网络上进行传输;
- (6) 当数据包到达目的 VPN 设备时,解封数据包,核对数字签名,无误后进行解密,得到原始数据。

2.3 IPSec VPN 研究现状及安全分析

2.3.1 IPSec VPN 研究现状

VPN 的出现使得校园网能够通过 Internet 安全、经济地传输机密信息,能够保证 IP 数据报在公网传输过程中不受来自第三方的网络窃听、篡改等安全威胁。目前,可用的 VPN 安全隧道协议有链路层的 PPTP、L2TP 协议、SSL 协议以及网络层的 IPSec 协议。其中 IPSec 是 VPN 最常用的安全协议,以其高度标准性、易用性和高安全性等优点成为当前 VPN 安全隧道技术的主流^[4]。

但是它同样也存在许多问题。IETF 的 IPSec 工作组最近的研究表明,即使所使用的密码强度足够,在记录层上精明的主动攻击仍能打破系统的保密性^[5]。Bruce Schneier 和 Counterpane Internet Security 公司的 Niels Ferguson 对 IPSec 协议提出了批评:“我们认为,IPSec 本身过于复杂,因此无法保证其安全性”。但他们同时也承认,尽管 IPSec 还存在不少问题,仍然比现有的其他 IP 安全协议更好一些^[10]。

2.3.2 IPSec VPN 安全分析

IPSec 在实现数据通信的两端提供安全的数据传输隧道,由自己定义哪些数据包应该受到保护,应该被放在安全隧道中传输^[11]。通过标识隧道的安全属性,可以定义用于保护这些敏感数据的安全参数。更精确地说,这些安全的数据传输隧道是建立在两个 IPSec

对端的一系列 SA 上,这些 SA 参数定义了哪些协议和算法可以被应用到敏感数据、IPSec 对端应用的密钥等。IPSec 的实现是靠两个对端维系的,实际上是一种端到端的安全实现;从技术的角度上说,在端到端客户的路由器上实现是最安全合理的方式,中间的路由器不需要做相应设置。因此 IPSec 实现的是一种与接入网络无关的 VPN 技术,已完成了标准化的工作,可以对 VPN 提供安全保障。

3 IPv6 校园网环境下 IPSec VPN 的安全部署

3.1 基于 IPSec VPN 的 IPv6 校园网络拓扑实例

校园网的主要的应用有(见图 4):

- (1) 不同级别部门的互连;
- (2) 远程访问;
- (3) 与其他学校及企业的互连;
- (4) 增强通信、内部资料的安全性。

以(1)为例,校园网 VPN 设计时,各分支机构通过安全网关与公共骨干网 Internet 连接。安装并配置了 IPSec 协议的路由设备等即可作为安全网关,其作用是对进出校园网的数据包进行加密和认证。

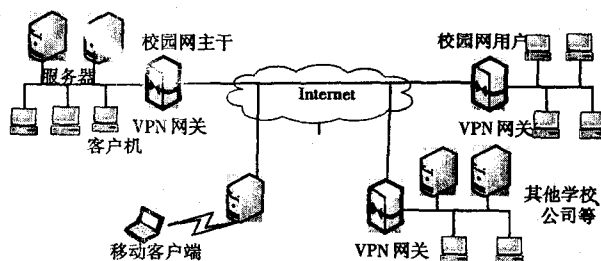


图 4 IPSec VPN 校园网实例

3.2 IPSec VPN 的安全实现

由 IPSec 提供安全的隧道,也就是在安全网关处实现 IPSec,也就是在安全网关后面的主机将通过 VPN 进行被保护的通信(见图 5)。其流程如下:主机 1 产生了一个 IP 包,要传到主机 2,而主机 2 位于另一个网络上;这个 IP 包从主机 1 传出,通过路由到达主机 1 所在网络的边界上,也就是安全路由器或防火墙,防火墙对所有传出的包进行过滤,判定是否需要 IPSec 处理;如果需要进行 IPSec 处理,则执行 IPSec 处

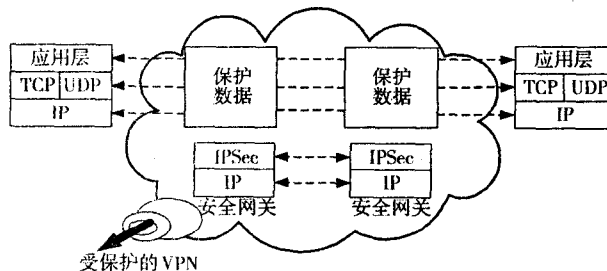


图 5 IPSec 在安全网关中的实施

理,并将该 IP 包进行封装;当到达主机 2 所在网络的防火墙上时,解除封装的报头,再将 IP 包传给主机 2,这样就完成了数据传输的整个过程。

在部署基于 IPSec VPN 的 IPv6 校园网时,还需要注意一些安全方面,以尽可能增强其安全性。

3.2.1 监测校园网流量

安全网关必须能够接收本校园网内部所发出的数据流量,还必须能够阻止来自其它网络的数据流量。在这种方案中,第一道保护线是实现加密认证,利用信息认证代码(MAC)来进行;当确定了数据流来自于本校园网时,为了提供更精确的访问控制,可以使用非加密的报文过滤技术对数据进行再次过滤。

3.2.2 数据保密性

在校园网内部传输数据时,可以根据不同的情况采取不同的保护措施。

(1) 若网络保密性很好,不对终端本身做任何安全性方面的更改,只对安全网关之间的数据进行加密和验证。这样,就只需要管理少数的安全联盟;但是对网络内部的攻击无能为力。对于这样的情况,可以选取 ESP 的隧道模式来解决。

(2) 如果校园网络内部也要求安全性保护,则必须对整条网络路径上的数据流进行加密。具体的做法是:在源端主机和目的端主机之间采用的 ESP 协议按传输模式来工作。这样就要端对端的加密保护和提供端对端的认证,传输模式的 ESP 协议附加有身份验证特性,可以激活该特性来解决此问题。

(3) 在完成上述工作后,将隧道模式的 AH 保护协议附加在两个安全网关之间,这样在终端点之间使用 ESP 协议传输模式,而在安全网关之间采用 AH 协议隧道模式的做法,也就是 IPSec 嵌套(绑定)工作方式。

3.2.3 路由设置

VPN 本质上是一种异构网络,所以校园网边界上必须在安全网关中配置传统的 IP 路由协议,并使用 IP 路由转发协议,并且对安全网关的路由信息交换进行加密和认证,这时使用的就是 IPSec 的 ESP 协议。一旦在安全网关之间建立起 IPSec 隧道后,就可以将安全联盟连接起来,使用 ESP 隧道模式对其提供验证和加密。由此,路由信息被加密保护,这样就可以对外隐藏校园网的拓扑信息。

3.3 IPSec VPN 的安全问题

(1) IPSec VPN 技术是假设终端计算机为安全的,并且在允许访问前必须验证用户的身份。这种方式解决了授权的网络访问,但是一旦得到授权就可能遭到远程用户有意或无意的攻击。

(2) IPSec 穿越 NAT 和个人防火墙的能力不足。

(3) 因为缺乏对应用层的支持,不具备应用层访问控制的能力,无法细粒化地分配访问权限。

(4) IPSec 被设计用来将分布在不同地方的可信网络连接在一起,一般这种连接是相对固定地点的,移动性不如 SSL、VPN。

IPSec 协议为校园网络的建设提供了能力强大、功能灵活的安全框架。但与其它安全协议(SSL、Socks5)相比,显然过于复杂,使用户的理解和管理的困难随之增大^[6]。尽管,例如先加密的压缩算法、与 NAT 的冲突问题、多播环境下的认证失效等问题还未解决,但是从整体上考虑,IPSec 仍然在目前所有 Internet 通信的安全协议技术中是最适用的^[10]。所以,在 VPN 中安全实现 IPSec 有良好的发展前景。

4 结束语

隧道技术是构建 VPN 的核心技术,尽管使用这些隧道协议构建的 VPN 能够在不安全的互联网上进行安全的数据传输(实现加密和鉴别等安全机制),但这些隧道协议的实现本身也不是非常安全和无懈可击的^[12]。比如,IPSec 本身有些复杂,但也有安全漏洞被发现,但总的说来,IPSec 仍是目前最好和最安全的 IP 安全协议。就目前看来,IPSec 是当前,也是将来一段时间研究最热点、使用最广泛的 VPN 隧道协议。校园网就如同一个实验网,它为将来大规模部署 IPv6 网络打下基础。在 IPv6 环境下构建基于 IPSec VPN 的校园网,还需要如入侵检测、防火墙、PKI 等综合的安全体系的完善;并且,IPSec 协议也可以与其他 IP 安全协议相互结合使用,扬长避短,形成一种混合技术,构造一个相对完美的 VPN。

参考文献:

- [1] 苏明,颜世峰. IPv6 校园网入侵检测系统设计[J]. 小型微型计算机系统, 2009, 30(3): 480-483.
- [2] Loshin P. IPv6 详解[M]. 沙斐,程莉,周立,等译. 北京:机械工业出版社, 2000: 69-78.
- [3] Kent S, BBN Corp. Security Architecture for the Internet Protocol[S]. RFC2401, 1998.
- [4] Doras N. IPSec—新一代因特网安全标准[M]. 北京:机械工业出版社, 2000.
- [5] 王作芬,王芙蓉,黄本雄. 虚拟专用网中 IPSec 隧道技术的研究与实现[J]. 计算机工程, 2001, 27(6): 118-119.
- [6] 蒋东毅,吕述望,罗晓广. VPN 的关键技术分析[J]. 计算机工程与应用, 2003(15): 173-177.
- [7] 叶润国,冯彦君,张方舟,等. IPSec VPN 与几种典型网络

(下转第 175 页)

4.2 实验结果与分析

首先,在没有任何限制条件下生成了一个完整的攻击图,图中有 106 个节点和 105 条边,其中可以到达攻击目标的攻击路径共有 46 条。

接着,用文中设计的算法,设定最大攻击深度为 5、最大攻击代价为 5,产生的攻击图见图 4。

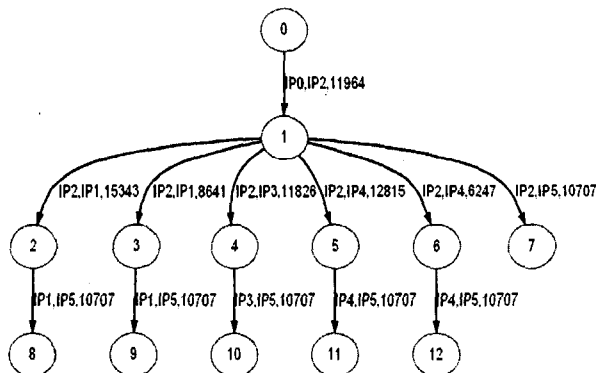


图 4 最大深度 5、最大攻击代价 5 的攻击图

图 4 共有 13 个节点和 12 条边,其中可以到达攻击目标的路径有 6 条,各路径及代价见表 4。

表 4 攻击路径代价表

编号	实际路径	代价
1	(IP0, IP2, 11964)→(IP2, IP1, 15343)→(IP1, IP5, 10707)	2.9
2	(IP0, IP2, 11964)→(IP2, IP1, 8641)→(IP1, IP5, 10707)	3.3
3	(IP0, IP2, 11964)→(IP2, IP3, 11826)→(IP3, IP5, 10707)	3.7
4	(IP0, IP2, 11964)→(IP2, IP4, 12815)→(IP4, IP5, 10707)	3.7
5	(IP0, IP2, 11964)→(IP2, IP4, 6247)→(IP4, IP5, 10707)	4.1
6	(IP0, IP2, 11964)→(IP2, IP5, 10707)	1.7

运行文中的算法后,攻击图的规模被有效地控制,明显减小。

另外,由表 4 可知,路径(IP0, IP2, 11964)→(IP2, IP5, 10707)代价最小,攻击者最容易从该路径入侵;同时每条攻击路径都利用了弱点 11964 和弱点 10707。因此,管理员可以据此采取相应的措施,防止攻击者的入侵。

5 结束语

目前,网络安全管理是一项具有挑战性的工作,保

护网络安全必须对网络攻击技术进行深入的研究。文中研究了攻击模型、攻击图生成等与网络攻击技术有关的内容,着重研究了攻击图生成算法。并通过实验证明了所设计的基于状态转移的攻击模型及基于代价分析的攻击图生成算法可以较为有效地预测攻击者可能采取的所有攻击路径和最佳路径,从而为防范攻击提供依据。

参考文献:

- [1] 陈春霞,黄 皓. 攻击模型的分析与研究[J]. 计算机应用研究,2005,22(7):115-118.
- [2] 张森强,唐朝京. 基于攻击效能的网络攻击法分类与形式化描述[J]. 信息与电子工程,2004,2(3):161-166.
- [3] Jan S, Markus S. Collaborative Attack Modeling[C]// Proceedings of the 2002 ACM Symposium on Applied Computing. New York, NY, USA:ACM,2002:253-259.
- [4] Andrew M, Robert E, Richard L. Attack Modeling for Informational Security and Survivability[DB/OL]. 2001-03. <http://www.cert.org/archive/pdf/01tm001.pdf>.
- [5] 司加全,张 冰,苟大鹏,等. 基于攻击图的网络安全性增强策略制定方法[J]. 通信学报,2009,30(2):123-128.
- [6] 苟大鹏,张 冰,周 渊,等. 一种深度优先的攻击图生成算法[J]. 吉林大学学报(工学版),2009,39(2):446-452.
- [7] Phillips C, Swiler L P. A graph-based system for network vulnerability analysis[C]// Proceedings of the NSPW'98. New York, NY, USA:ACM,1998:71-79.
- [8] Swiler L P, Phillips C, Ellis D, et al. Computer-attack graph generation tool[C]// Proceedings of the DISCEX II'01. Albuquerque, NM:Sandia Nat. Labs.,2001:307-321.
- [9] Browne H K, Arbaugh W A. A Trend Analysis of Exploitations[C]// Proc. of 2001 IEEE Security and Privacy Conference. Oakland, USA: IEEE Press, 2001:214-229.
- [10] 张永铮,云晓春,胡铭曾. 基于特权提升的多维量化属性弱点分类法的研究[J]. 通信学报,2004,25(7):107-114.
- [11] Bugtraq. Security Focus[EB/OL]. 2009-03. <http://www.securityfocus.com/archive/1>.
- [12] Graphviz. Graph Visualization Software[EB/OL]. 2009-06. <http://www.graphviz.org/>.

(上接第 170 页)

- [8] 李 频. 虚拟专用网的主要隧道协议的安全性剖析[J]. 计算机工程,2002,32(13):164-169.
- [9] 戴宗坤,唐三平. VPN 与网络安全[M]. 北京:电子工业出版社,2002.
- [10] Ferguson N, Schneier B. A Cryptographic Evaluation of IPSec

- [R]. [s.l.]:Counterpane Internet Security Inc.,2003.
- [11] 沈 莉. IPv6 的安全协议研究[J]. 电子科技大学学报,2002,31(1):72-75.
- [12] Yuan Ruixi, Strayer W T. Virtual Private Networks: Technologies and Solutions[M]. Boston: Addison Wesley Publishing Company, 2002.