毕业设计(论文)

题　　目：基于 VPN技术的校园网络安全的设计与实现

毕业设计（论文）原创性声明和使用授权说明

原创性声明

本人郑重承诺：所呈交的毕业设计（论文），是我个人在指导教师的指导下进行的研究工作及取得的成果。尽我所知，除文中特别加以标注和致谢的地方外，不包含其他人或组织已经发表或公布过的研究成果，也不包含我为获得_____及其它教育机构的学位或学历而使用过的材料。对本研究提供过帮助和做出过贡献的个人或集体，均已在文中作了明确的说明并表示了谢意。

作 者 签 名：_____ 日 期：_____

指导教师签名：_____ 日 期：_____

使用授权说明

本人完全了解_____大学关于收集、保存、使用毕业设计（论文）的规定，即：按照学校要求提交毕业设计（论文）的印刷本和电子版本；学校有权保存毕业设计（论文）的印刷本和电子版，并提供目录检索与阅览服务；学校可以采用影印、缩印、数字化或其它复制手段保存论文；在不以赢利为目的前提下，学校可以公布论文的部分或全部内容。

作者签名：_____ 日 期：_____

学位论文原创性声明

本人郑重声明：所呈交的论文是本人在导师的指导下独立进行研究所取得的研究成果。除了文中特别加以标注引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写的成果作品。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律后果由本人承担。

作者签名：　　日期：　　年　　月　　日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学校保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权_____大学可以将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

涉密论文按学校规定处理。

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

注 意 事 项

1.设计（论文）的内容包括：

1）封面（按教务处制定的标准封面格式制作）

2）原创性声明

3）中文摘要（300 字左右）、关键词

4）外文摘要、关键词

5）目次页（附件不统一编入）

6）论文主体部分：引言（或绪论）、正文、结论

7）参考文献

8）致谢

9）附录（对论文支持必要时）

2.论文字数要求：理工类设计（论文）正文字数不少于 1 万字（不包括图纸、程序清单等），文科类论文正文字数不少于 1.2 万字。

3.附件包括：任务书、开题报告、外文译文、译文原文（复印件）。

4.文字、图表要求：

1）文字通顺，语言流畅，书写字迹工整，打印字体及大小符合要求，无错别字，不准请他人代写

2）工程设计类题目的图纸，要求部分用尺规绘制，部分用计算机绘制，所有图纸应符合国家技术标准规范。图表整洁，布局合理，文字注释必须使用工程字书写，不准用徒手画

3）毕业论文须用 A4单面打印，论文 50 页以上的双面打印

4）图表应绘制于无格子的页面上

5）软件工程类课题应有程序清单，并提供电子文档

5.装订顺序

1）设计（论文）

2）附件：按照任务书、开题报告、外文译文、译文原文（复印件）次序装订

3）其它

毕 业 设 计 (论 文) 中 文 摘 要

针对当前高校跨地域分布导致的校园网安全建设中所遇到的问题，文章结合VPN技术的特点，提出将VPN技术应用在高校网络的建设中，给出了一种基于VPN技术的高安全性网络解决方案，用于提供高效、安全、灵活和经济的网络数据传输，该技术的应用可以提供可靠的校区互联、移动办公和校际交流三个方面的拓展功能。

关键词：校园网 VPN技术 虚拟专用网 IPSec VPN SSL VPN

毕 业 设 计 (论 文)外 文 摘 要

Title ： Research of VPN technology to campuses' network

Abstract ：

The construction of campuses' network meets some questions caused by campuses crossing regions. The article proposes application the VPN technology in the construction of campuses' network, produces the high secure network solution based on the VPN technology which is used to provide highly effective, safe, active and economical network data transmission. It can provide reliable communication with campus's regions, the mobile work and the intercollegiate exchange three aspects development function.

Keywords: campuses' network， VPN technology， virtual private network ， IPSec VPN SSL VPN

目录

1　绪 论

1.1 研究背景

随着计算机技术和信息通信技术的不断发展,网络作为计算机与通信技术融合的产物,从刚刚出现到现在的大规模普及,已经越来越和人们的生活密不可分,可以说计算机网络已经和人们的日常生活息息相关。从 1995 年因特网的诞生到现在网络的普及，可以说网络在短短十几年中呈现出了几何爆炸式的增长，发展之快是史料未及的。但随之而来的问题也凸显了出来，由于网络协议在当初设计时是基于双方互信的机制，为今天的互联网埋下了“不可信”的隐患，嗅探、篡改、重放等网络攻击随处可见，网上政务、商务、银行等组织团体的业务发展受到了严重的阻滞。人们需要给自己的信息加密，防止在传输的过程中信息泄露，保证网络传输的安全可靠。特别是进入新世纪以后，随着中国加入 WTO,我国许多大公司都在别的国家设立了分支机构，如何使这些分支机构、办事处能随时随地的连接到总部的主站上来，也是一个待解决的问题。从网络诞生的那一刻起，高校校园网络就一直充当着网络研究平台和人才培养基地的重要作用。一直以来，校园网以其开放性和快速性已经成为高校信息交流必不可少的工具,尤其最近以来，随着我国经济的发展，高校也进行了扩招，许多学校建立了自己的新校区和分校区，如何让各个校区之间的数据能够安全的进行传输;校园的资源是开放的，因为每位师生都可以访问校园网资源。但校园网资源又是独有的，在校园网覆盖范围之外，特别是偏远的教工和学生需要接入学校或者访问校内资源，这时如果按照传统方法是不能满足这些需求的，另外，校园网内一些重要的服务如财务、一卡通、图书馆等如何既能确保优先传输，又要保证传输安全。所以针对以上这些问题，我们需要在校园网中建立一种行之有效，既节省成本、又方便易行的网络安全体系机构，而 VPN刚好可以满足我们以上需求。

1.2 VPN 的发展和现状

1.2.1 VPN 的发展及国外的现状

当前 VPN 技术发展已经历了四代:

第一代，传统的 VPN，以 FR/ATM 技术为主，在虚电路方式的基础上建立起了虚拟连接通道，从而实现物理链路的复用，其安全性是在虚拟隔离的基础之

上。IP 网络的飞速发展，这种传统的 VPN 不再具有优势，应用范围逐步缩小。

第二代，初期的 VPN，是在 PPTP/L2TP 隧道协议的基础之上建立，这种 VPN 对于远程拨号方式的访问更加适合，但在认证及加密方面的功能较弱，其虚连接和数据的安全性能都较低，对于大规模 IP 网络的发展应用需求不能很好的适应，逐步在市场中被淘汰。

第三代，主流 VPN，这种 VPN 的主要技术为 IPSec/MPLS 技术，对于 IP 网络分组及其安全性能需求都能基本满足，是当前应用最为广泛的 VPN。

第四代，不断发展的 VPN，其主要技术为 SSL/TLS 技术，通过对应用层的认证和加密以实现 VPN 安全传输的简单、高效、灵活等需求，但在安全性能方面弱于基于 IPSec 技术的 VPN，其应用功能支持方面也不如 IPSec VPN 全面。

1.2.2 VPN 的发展及国外的现状

在中国，VPN 市场从 2000 年开始才正式起步，并且与信息产业的其它分支类似，经历了由金融、政府和通信等行业带动起步的过程，取得了长足的发展。各大国内网络设备厂商也纷纷来分享 VPN 这个大蛋糕，深信服、华三等厂商脱颖而出，成为国内从事 VPN 系统集成的主要厂商。尽管我国 VPN 市场起步较晚，但近两年发展势头不断加快，到目前为止，一些大中企业已经建立了自己的 VPN，一些学校的校园网也已经尝试利用 VPN 技术进行远程访问，一些高校和科研院所也正在研究 VPN 技术，开发使用 VPN 软件产品，提高全方位的 VPN 技术服务。

1.2.3 VPN 在校园网中应用的现状

目前，校园网对 VPN 技术的关注热度到了一个相对的高潮期，据《中国教育网络》调查，许多高校已经开始或者准备实施 VPN。各高校实施 VPN 的目的大致相同，首先，将校外需要 VPN 的学生或教职工引进来，为其提供 VPN 接入的服务，比如：北航的 VPN 远程访问校园网资源系统正在部署;其次，要保证 VPN 服务的接入服务只为授权者提供，可以在本部与分校区之间建立一条VPN 通道，从而进行信息传递和共享。针对不同高校而言，其自身的需求也是不同的，有的高校需求较为独特，如：东北大学的VPN 建设，其主要目的是在校外的师生访问 IPv6 资源时，为其提供更方便的服务。在当前的高校中，对于 VPN 的需求主要有以下二个方面：

VPN 方案能够在公众的 IP 网络上建立私有的数据传输通道，从而进行分校的合作伙伴、分支办公室及移动办公人员等的远程连接，以降低校园网的访问负担，从根本上节约远程访问费用开支。

第二，满足分校之间相互访问的需求。当前很多高校都在进行不同分校之间的服务器整合研究，以方便进行管理控制，对资源进行统一获取、分配，对各分校 web 通讯的制在学校地理分布上面临着极大的困难。

论文先从 VPN 技术出发，介绍几种常见的 VPN，选择出 VPN 在校园网实施的优势;再对 VPN 技术的现状、分类、发展和实现方式等方面对 VPN 技术做一个全面的介绍，然后对与 VPN 技术相关的理论知识予以介绍，并对 VPN 技术进行了相关的论述，最后，结合学院校园网具体情况，提出将 VPN 技术应用于多校区校园网的实现方案。

论文共分为四部分，具体内容如下：

a) 介绍了论文的选题背景与技术现状，分析 VPN 技术在校园网中应用的可行性和必要性。

b) 对目前两种主流的 VPN 技术 IPSec VPN 及 SSL VPN，从其隧道协议、加解密和认证方法、工作原理等方面做了详细阐述，分析了各自的优缺点并对其主要性能进行了比较。

c) 介绍我校校园网基本概况，根据我校的网络现状与应用需求，提出了我校 VPN 网络的设计方案和我校 VPN 网络的具体实施过程,从而构建符合我校特点的校园网安全体系。

d) 对论文的研究工作做了概括和总结，提出了进一步需要解决的问题与不足。

1.4 小结

本章简要介绍了选题背景和研究目的及意义,在此基础上介绍了国内外VPN的研究与应用概况，重点对高校校园网应用 VPN 的情况进行了论述，介绍了高校校园网应用 VPN 的需求。

VPN 与 VPN技术

VPN 的概念

VPN(virtual Private Networks) 是通过一个公用网络(通常是因特网)建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。通常 VPN 是对企业内部网的扩展，通过它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接,并保证数据的安全传输。

2.2 VPN 的分类

2.2.1按接入方式进行划分

通常情况下，这种划分方式是运营商和用户最为关心的。用户可能是拨号上网，也可能是专线上网，基于 IP 网络的 VPN 也有着对应的接入方式，即专线接入和拨号接入。

a) 专线接入 VPN：这种方式主要是为 ISP 边缘路由器的专线接入用户提供相应的 VPN 解决方案。它是永远在线的，能够节省以往的用户长途专线费用。

b) 拨号接入 VPN:也可以称之为 VPDN,就是向接入 ISP(利用 ISDN 或 PSTN)的用户提供相应的 VPN 解决方案。这种 VPN 是按需连接的，能够为用户节省长途电话费用。

2.2.2 按协议实现类型进行划分

这种划分方式是 ISP 和 VPN 厂商最为关心的。可以根据 VPN 分层类型将其建立于第二层或第三层。

a) 第二层隧道协议：其中包括第二层隧道协议 (L2TP)、第二层转发协议(L2F)、点到点隧道协议 (PPTP)、多协议标记交换(MPLS)等。

b) 第二层隧道协议：其中包括 IP 安全(IPSec)和通用路由封装协议(GRE)，在现阶段，这两种三层协议是最为流行的。

第二、三层隧道协议存在的主要区别就是在网络协议栈中用户数据在第几层被封装，这些协议之间并不存在冲突，通常可以结合使用。

2.2.3 按 VPN 的发起方式进行划分

这种 VPN 分类方式是 ISP 和客户最为关心的。其业务能够由客户自主独立

ISP 提供。

a) 客户发起(基于客户的)：VPN 服务的出发点和目标都是针对客户的，其实施和管理、内部技术组成都是面向客户的、可见的。这就需要隧道服务器方和客户方安装隧道软件。隧道由客户方的软件发起，在公司服务器隧道终止。在这种情况下，ISP 不需要做任何工作来支持隧道的建立。通过对用户的口令和身份符验证，隧道在双方的建立极为容易。在通信过程中，客户方和隧道服务器也可以采取加密的方式。隧道建立之后，用户就可以察觉到 ISP 在此时的通信中不再参与。

b) 服务器发起(基于网络的或客户透明方式)：VPN 软件在 ISP 处或公司的中心部分安装，客户不需要安装。这种方式主要是为了提供给 ISP 全面 VPN 管理服务，服务于 ISP 的 POP 起始和终止，这种情况下，其实施和管理及内部构成技术对客户是完全透明的。

2.2.4 VPN 的服务类型进行划分

按照 VPN 的服务类型可以将其业务分为大致三种类型：接入 VPN(Access VPN)、外联网 VPN(Extranet VPN)和内联网 VPN(Intranet VPN)。通常情况下，内联网 VPN 属于专线 VPN。

a) 接入 VPN：这种 VPN 方式通常是企业中的员工或分支机构通过公网进行企业内部网络的远程访问方式。一般情况下，远程用户不是网络，而是一台计算机，所以 VPN 的组成是主机到网络的拓扑模型。需要指出的是接入 VPN 不同于前面的拨号 VPN，这是一个容易发生混淆的地方，因为远程接入可以是专线方式接入的，也可以是拨号方式接入的。

b) 外联网 VPN：这种 VPN 方式多用于企业发生兼并、收购或企业联盟等情况下，不同企业之间通过公网进行虚拟网络的构建。这种 VPN 的组成是以不对等方式连接起来的网络到网络方式。

c) 内联网 VPN：这种 VPN 方式多为企业的总部与其分支机构之间的虚拟网络构建，这种 VPN 是以对等方式连接起来的网络到网络方式。

VPN 的关键技术

2.3.1隧道技术

隧道技术是 VPN 实现的关键技术之一，是通过某种协议进行另一种协议传

主要通过隧道协议进行这种功能的实现。其中包含了三种协议，隧道、传输和乘客协议。隧道协议主要负责建立、拆卸和保持隧道，传输协议主要进行隧道协议的传送，而乘客协议则是进行协议的封装。通过隧道传递的数据通常为不同协议的数据包或数据帧，通过隧道协议将其重新封装并发送。路由信息由新的帧头提供，确保封装的数据包通过互联网传递而到达目的节点，随后通过解封得到原始的数据包。

2.3.2

在隧道正式连接准备开始前，通常使用用户认证技术对用户的身份进行确认，从而实现系统的用户授权和进一步资源访问控制。通常情况下，认证协议采用的是摘要技术，它是通过 HASH 函数对长报文的长度进行函数变换，映射成为长度固定的摘要。但由于 HASH 函数的特性难以掌握，使得在不同报文中找到长度相同的摘要变得更加困难。在 VPN 中，这种特性使摘要技术有以下两种用途。

a) 数据的完整性验证。发送方发送数据报文及其摘要，接收方对此进行计算对比，报文摘要与发送的摘要相同则表示报文没有经过修改。

b) 用户认证。实质上而言，这种功能在一定程度上是第一种功能的延伸。当某方希望对另一方进行验证，但不希望验证结果传送到网络时，这方可以随机发送一段报文，使对方将该报文摘要及秘密信息发回，另一方可以对摘要进行验证，如果正确，则可以达到对方进行验证的目的。

2.3.3数据加密技术

在数据包的传输过程中，主要靠数据加密技术来对数据包进行隐藏。如果在这个过程中数据包通过的因特网不够安全，即使已经通过了用户认证，VPN 也不是一定安全的。在发送端隧道，用户认证应该首先加密，然后再进行数据传送。在接收端隧道，通过认证的用户应该先将数据包解密，按照密钥类型的差异可以将当前的密码技术进行分类，主要分为两类：对称和非对称加密系统。在实际中，通常对大量的数据加密采用对称密码体制，而对于关键的核心数据加密则通常采用公钥密码体制。

2.3.4访问控制

决定了是否允许访问系统，允许访问系统的资源及资源的使用，通过适当的

VPN

2.4.1 安全保障

虽然实现 VPN 的技术和方式很多，但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接，称之为一个隧道的建立。够通过加密技术来进行隧道数据传输的加密，从而确保数据的了解对象仅限于发送者和接收者，以确保数据的安全性。在这方面，由于 VPN 是直接在公用网上构建的，实现了网络的方便、简单和灵活等性能，但其安全问题也更加突出。企业在运营过程中必须保证 VPN 中的数据传送不受攻击者篡改和偷窥，而且，必须阻止非法用户对私有信息进行访问。Extranet VPN 将企业网扩展到合作伙伴和客户，对安全性提出了更高的要求。

2.4.2 服务质量保证(QoS)

VPN 网应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。如移动办公用户，在 VPN 的服务保证中，确保提供广泛的覆盖性连接是其中一个重要的环节;对于专线 VPN 网络而言，由于其中存在着众多的分支机构，因此，在企业网内部交互式的专线网络则需要提供更加稳定的 VPN;对于如视频等其他网络应用而言，则对网络有着更加明确的要求。上述的网络应用都对网络服务提供提出了不同的服务质量要求。从优化角度考虑，VPN 网络的构建还有着另一个重要的要求，就是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送;而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

2.4.3 可扩充性和灵活性

VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

2.4.4

VPN 管理方面，

VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将些次要的网络管理任务交给服务提供商去完成，但企业自身仍有着很多的网络管理工作要做。因此，在 VPN 业务运营中，必须建立一个完善的 VPN 管理系统。管理目标设定为：具有高扩展性、可靠性、经济性，还能够极大程度上减小网络风险。管理内容主要应该包括、配置管理、设备管理、访问控制、安全管理、QoS 管理、列表管理等。

2.4.5 费用低廉

由于使用因特网进行传输相对于租用专线来说，费用极为低廉，所以 VPN 的出现使企业通过因特网安全又经济的传输私有的机密信息成为可能。

主流 VPN 技术概述

2.5.1 IPSec VPN

a) IPSec 协议简介

IPSec 产生于 IPv6 的制定中，主要用于为 IP 层提供安全性能。在所有主机进行通信的过程中，必须经过 IP 层的处理，因此提高 IP 层的安全性能也是奠定整个网络通信的安全基础。由于 IPv4 的应用仍较为广泛，因此，在后来的 IPSec 制定中还添加了对 IPv4 的支持。

b) IPSec 基本工作原理

从基本工作原理来看，IPSec 与包过滤防火墙有些相似，可以理解为是在包过滤防火墙的基础上进行的一种扩展。当一个 IP 数据包被接收时，包过滤防火墙会在一个规则表中对其头部进行匹配。IPSec 通过对安全策略的数据库进行查询，从而做出对接收的 IP 数据包的处理决定。但相对于包过滤防火墙而言，IPSec 在数据包的处理上，除了转发、丢弃等方法外，还能够进行 IPSec 处理。这多出来的处理方法为网络的安全性能提高起到了极大的积极作用，比包过滤防火墙更进一步。

IPSec 处理就是对 IP 数据包进行认证和加密。相比较而言，包过滤防火墙只能对通过某个站点的 IP 数据包进行控制，可以对某个站点访问的 IP 数据包拒绝，但它不能保证内部传送出去的数据包的安全，也不能确保内部网络中存在的数据

包的安全。只有在对内部数据包实施 IPSec 处理之后，才能在内部和外部的网络数据传输过程中，保证 IP 数据包的真实性、完整性和机密性，通过网络的安全通信才能实现。

IPSec 可以只对 IP 数据包进行认证，也可以只进行加密，还可以同时进行加密和认证。但无论是哪种方法，它的工作模式只有两种，即传输模式和隧道模式。

c) IPSec 中的主要协议

在上文中已经提到 IPSec 的主要功能，就是对网络传输中的 IP 数据包进行加密和认证。为了这项功能的进行，IPSec 还必须实现密钥的交换和管理功能，从而为加密和认证过程提供必须的密钥，并实现对密钥使用的管理。上述三方面的工作是由 AH、IKE 和 ESP 三个协议所规定。下面笔者对这三个协议进行了介绍，在介绍之前，必须先引入安全关联(SA)这一极其重要的术语。安全关联，就是安全服务及其服务载体之间的连接。在 AH 和 ESP 中 SA 是必须使用的，而 IKE 的主要工作就是进行 SA 的建立与维护。只要对 SA 进行支持，才能实现 AH 和 ESP。

如果采用 IPSec 的方式为通信双方建立安全的数据传统通道的话，就必须按照实现协商的安全策略进行，其中包括密钥使用、生存期及加密算法等内容。当双方的安全策略得以协商妥当时，就可以理解为双方建立了 SA。也就是说在数据传输的过程中 SA 能够提供某种 IPSec 的安全保障连接，这个连接是由 AH 或 ESP 提供的。当一个 SA 建立，就决定了 IPSec 处理工作的执行方法，如加密和认证等。SA 可以进行两种方式的组合，分别为传输临近和嵌套隧道。

1）AH(authentication header)

AH 存在着两种实现方式，即传输和隧道方式，当其以传输方式实现的时候，主要是对高层协议提供保护，在这种情况下，数据不采取加密。当其以隧道方式实现的时候，主要用于隧道通过的 IP 包协议。AH 的功能只有认证，没有加密。

AH 的长度是可以变化的，但其长度必须是 32 比特数据报的长度倍数。在 AH 域中，可以进行几个自语的细分，其中包含着为 IP 数据包的密码提供所需数据。

在 IPSec 服务中，认证是一种强制性服务，从实质上讲，就是确保带有源身份信息的数据的完整性，该保护服务的提供所需数据在 AH 的两个子域中包含。

其中一个称为安全参数索引，这个子域中包含长度为 32 比特的某个任意值，提出了该 IP 数据包认证服务使用的密码算法。另外一个子域称之为认证数据，其中包含着为接收方生成的发送方认证数据，主要为接收方提供验证数据，以确保数据的完整性，所以，这部分数据也称之为完整性校验值。这个 IP 数据包的接收方可以使用 SPI 和密钥的算法重新进行认证数据的生成，然后自己对比生成的数据和收到的数据，完成 ICV 校验。

2) ESP

ESP 协议主要用来处理对 IP 数据包的加密，此外对认证也体统某种程度的支持。ESP 是与具体的加密算法相独立的，几乎可以支持各种对称密钥算法，例如，DES，3DES，RCS 等。为了保证各种 IPSec 实现间的互操作性，目前 ESP 必须提供对 56 位 DES 算法的支持。

如果使用适当的算法和模式，ESP 还提供验证。如果需要验证。它将以验证报头(AH)的格式实现。这意味着 ESP 可以提供 3 个基本的操作

.只有 IP 数据报的机密性和完整性。

.只有验证。

.IP 数据报的验证及机密性和完整性。

以上 3 个无论实现哪个，都由所选择的算法和算法的模式来驱动。

3) IKE (internet key exchange)

IKE(因特网密钥交换)主要用于 SA 的动态建立。它标示着 IPSec 对 SA 的协商，并对 SA 进行补充。在 RFC2409 的文档描述中，IKE 是一种混合型协议。它在 ISAMP 的基础之上，沿用了 SKEME 的共享、Oakley 的模式和密钥更新技术，从而定义了独特的协商共享策略和验证加密材料生成技术。在 IKE 实现过程中，主要采用了 ISAKMP，可以分为两个阶段，第一，通信的各方建立起了一个安全保护的、通过身份验证的通道，也就是 IKE 安全关联的建立。第二，在这个安全关联的基础之上，为 IPSec 协商出详细的安全关联。因特网密钥交换定义两个交换阶段，即阶段 1 和阶段 2 交换以及两个额外的交换。在阶段 1 的交换中，IKE 采取主模式交换，也就是身份保护交换，此外，还有在 ISAKMP 基础之上制定的野蛮模式交换；在阶段 2 交换中，IKE 则采用快速模式交换。此外，另外两种定义交换都属于信息方面的交换。

4) SA

IPSec 的中心概念之一是安全关联 (security association，SA)。本质上，IPSec 可以认为是 AH+ESP。当两个网络结点在 IPSec 保护下通信时，它们必须协商一个 SA(用于认证)或者协商两个 SA(用于认证和加密)，并协商这两个结点间所共享的会话密钥以便它们能够执行密码操作。建立两个安全网关间的安全双工通信需要对每个方向建立 SA。每个 SA 由 3 个部分唯一标识：

.一个安全参数索引，即 SPI。

.一个 IP 目标地址。

.一个安全协议，AH 或 ESP。

如前所述，定义了两种 SA 模式，即传输模式和隧道模式。传输模式的是两个主机间的安全联合。隧道模式的 SA 是适用于 IP 隧道的 SA。如果 SA 在两个安全网关之间或一个安全网关和一个主机之间产生，此 SA 必须使用隧道模式。可以组合 SA 以提供多层次的安全性以及传输或封装的能力。当 SA 进行组合时，称其结果为一个 SA 束，这时通过它们的传输数据必须进行处理的一系列安全联合。

d) IPSec VPN 的实现

通常情况下，VPN 用户网络的使用地址是 RFC1918 中规定的私有网络地址，当用户之间进行通信时，首先必须建立一个逻辑隧道，将其中包含私有 IP 地址的数据包进行封装，封装方式采用一个公共 IP 地址报头的方式，这样就能够在公共共享网络上进行转发。IPSec 协议对于 IP 数据包只进行安全保护处理，并增添相应的 ESP 和 AH 报头，将原有的 IP 分组封装到 IPSec 分组，但并不能实现 VPN 通信功能。要想实现这个功能，就必须在此基础之上进行再封装，再封装过程可以通过隧道协议实现，如 IP -IP、L2TP 等。IPSec 支持的隧道模式就是一个再封装过程(IP-IP)，可以直接利用这点来实现 IPSec VPN。而通过传输模式实现时，由于不能实现私有网络地址 IP 数据包进行公共共享网络的跨越传输，所以在 VPN 实现中很少得以应用。VPN 功能的实现必须通过传输模式的保护，由其他协议完成 IPSec 的再封装。IPSec VPN 就是指在集成 IPSec 的安全保护下的 IP 隧道方式来实现第三层 VPN 技术，通常支持的 IP 隧道协议包括 IP-IP、GRE、MPLS 等，通常情况下， IPSec VPN 指的就是直接通过 IPSec 的隧道模式而实现的 VPN。

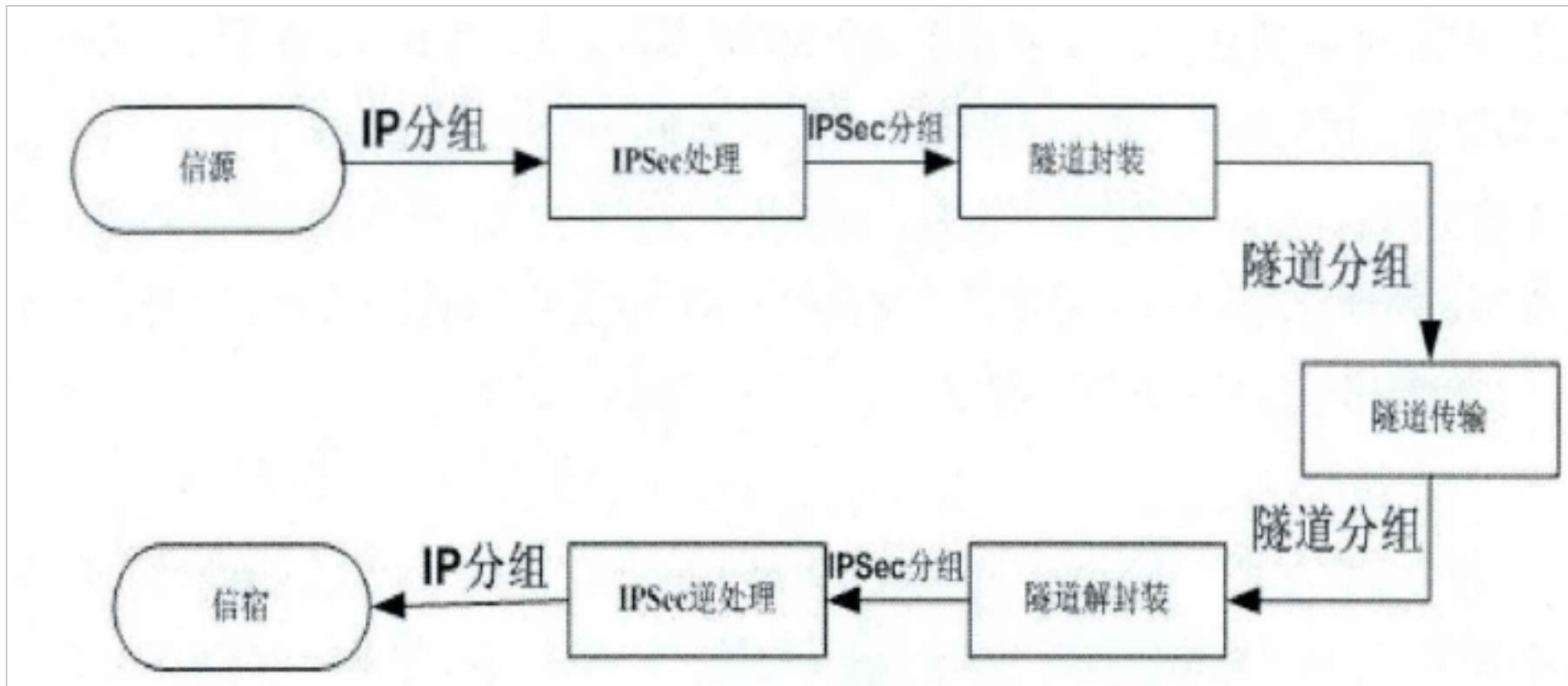

图 2.1 IPSec VPN 通信传输原理

2.5.2 SSL VPN

a) SSL VPN 原理

大多数 SSL VPN 都是 HTTP 反向代理，这样它们非常适合于具有 Web 功能的应用，只要经由 Web 浏览器即可实现对数据的访问， HTTP 反向代理也可实现其他相关的应答与查询服务，例如，对电子邮件与多数企业生产力工具的查询(如 CRM 与 ERP 等服务器与客户机的应用)。为了实现对该类型的应用与访问， SSL VPN 可提供经济、简单的方案实现远程的链接。它属于随插随用型，不需要依靠客户端的软硬件进行辅助。一般 SSL VPN 需要在企业设置的防火墙后安装一个 SSL 代理服务器。若客户想安全的将数据连接到公司的网络上，则用户需在浏览器上输入一个 URL，SSL 服务器将会取得该连接，进而对用户的身份进行验证，最后 SSL 代理服务器将自动提供一个远程用户与多种应用服务器间的相连接。实现起来主要有下面 3 种协议。

l) 握手协议：它建立在可靠的传输协议上，为高层协议提供数据封装、压缩、加密等基本功能。这个协议负责协商客户机与服务器之间会话的加密参数。当一个 SSL 客户机和服务器第一次通信时，它们在一个协议版本上达成一致，选择机密算法和认证方式，通过公钥技术进一步确定一个共享密码。

2) 记录协议：它建立在 SSL 记录协议之上，用在实际的数据传输开始时嵌套，通信双方进行身份认证，协商加密算法，交换加密密钥等。这个协议用于交

换应用数据。应用消息被分割成可管理的数据块，还可以压缩，并产生一个MAC(消息验证码),最后消息在传输过程中就已加密,而接受方需通过校验MAC后方可接收数据进一步解密，对相关数据进行解压后重新组合，并将最后结果传输给程序协议。

3）警告协议：它是提示在协议出现异常情况或两个主机会话结束时而终止。

b) SSL VPN 的优点

1）无需安装客户端软件：只需要标准的 Web 浏览器连接因特网，即可通过网页访问到企业总部的网络资源。

2）适用于多数设备：浏览器可以访问任何设备，如 PDA、移动电话等设备。

3）适用于大多数操作系统：Windows，Unix 及 Linux。

4）支持网络驱动器访问.

5）良好的安全性。

6) SSL 不需要对远程设备或网络做任何改变。

c) SSL VPN 的主要不足

1）SSL VPN 的认证方式比较单一。只能采用证书。而且一般是单项认证。支持其它认证方式往往进行长时间的二次开发。 IPSec VPN 认证方式更为灵活。

2）SSL VPN 应用的局限性很大，只适用于数据库——应用服务器——Web 服务器——浏览器这种模式。

3) SSL 协议只对通信双方所进行的应用通道进行加密,而不是对从一个主机到另一个主机的整个通道进行加密。

4) SSL 不能对应用层的消息进行数字签名。

5）站点到站点连接缺少理想的 SSL 解决方案。

6) SSL VPN 的加密级别通常不如 IPSec VPN 高。

d) 应用范围

目前 SSL VPN 与远程网络进行通信的应用主要是基于 Web 的客户，这些 Web 应用目前主要是内部网页浏览、电子邮件及其它基于 Web 的查询工作。在 SSL VPN 通信中，通常用 SSL Proxy 的技术来提高 VPN 服务器的通信性能和安全身份验证能力。对通常的企业高级用户 (power user)和 LAN-TO-LAN 连接所需要的直接访问企业网络功能而言,IPSec VPN 无可比拟。然而,典型的 SSL VPN

被认为最适合于普通远程员工访问基于Web的应用。虽然 SSL VPN有诸多好处，但 SSL VPN 并不能取代 IPSec VPN。因为，这两种技术具有不同的着重点。SSL VPN 主要应用在 Web 远程的接入，实现应用软件的安全性。 IPSec VPN 是通过对两网站间的专线连接或两台服务器间的互联网连接，实现对点对点间通信的保护，它不仅应用于 Web 还应用于其他方面。

2.6 小结

本章从 VPN 原理出发，介绍了 VPN 的主要类型和 VPN 的特点以及 VPN 的关键技术，并结合主流技术，着重介绍了 IPSec VPN 和 SSL VPN 的原理和优缺点，并对这两种 VPN 的应用场合做了简单的介绍。

3　校园网 VPN 安全的实现

3.1 校园网现状分析

常州 TT 学院校园网始建于 2008 年，经过近四年的建设和发展，已经初具规模，校园网覆盖范围包括老校区和新校区的办公楼、图书馆、机房、学生宿舍楼和教学楼。新老两个校区为双链路千兆单模光纤互联，分别由老校区核心交换机 CISCO 6509 接入到新校区核心交换 HUAWEI S8505 与核心路由器 NE40。

各个校区之中各个楼宇间用千兆光纤连接，网络骨干速度为千兆，楼内垂直为百兆或者千兆，水平为百兆到桌面。网络拓扑分为核心层、汇聚层和接入层三级结构，核心层为交换机思科 6509，汇聚层交换机为思科的 3550 系列，接入层为交换机是思科 2950 等，全校 IP 地址分配采用的是 DHCP 分配。

校园网接入商有 3 个，分别为中国教育科研网，从常州 TT 学院接入，带宽为 1000M，一条为常州电信提供的 1000M 带宽的光纤接入，还有一条是常州联通提供的 1000M 带宽的光纤接入。学校建成了自己的服务器群，提供的服务有 WEB 主页服务，DNS 域名解析，E-MAIL 电子邮件，FTP 文件下载、VOD 视频点播等服务，出口有华为的 NE40 路由器，用于连接不同服务商接入互联网。校园网内部采用的是认证计费方式是 SAM 服务器与交换机配合使用，对学生宿舍区提供基于 802.IX 协议的认证计费，提供包时收费，对办公区和教学区不采取认证计费，直接接入校园网。校园网信息点有 8000 个左右。

由于随着我校互联网用户的逐步增多，原有的 IP 地址规模已经不能满足日益增长的校内用户的数量,所以我校采用了内部 IP 地址,在网络出口处使用 NAT 地址转换技术，实现内网 IP 地址与外网 IP 地址的转换，如在办公区使用 10.195.0.0/16 这个段的IP 地址,在教学区使用 10.196.0.0/16 这个段的 IP 地址等，在校园网的用户访问互联网时通过路由器上的公有 IP 地址池映射出去，这一设计尽管大大节省了公有 IP 地址，但另一方面带来的坏处就是使校园网外用户无法访问到校内的网络资源，例如学校图书馆所购买的电子资源大部分都有限制访问的 IP 地址范围，图书馆支付费用后，数据库服务商是根据访问者的 IP 地址来判断是否经过授权的用户。所以需要建立一套可管理、可认证、安全的远程访问电子图书馆的解决方案。

由于安全等原因，校园网内的部分资源只允许在校园网内部进行访问。如对校园新闻的访问、校园网内的单位或个人的服务器或计算机的访问、使用校内邮件服务器发送邮件、对校园新闻的访问时，只允许在校园网内部进行访问。这在一定程度上阻碍了教师在家通过校内网办公、浏览校内新闻、校内通知公告等，在校内网的服务器出现异常时，系统管理人员不在校内时，系统不能得到及时维护，学校的老师出差在外，不能查看校内的项目服务器或进行数据传送。

学校有自己的财务网络和校园一卡通系统，实现财务网络与一卡通安全的在校园网内进行通信。未来视频会议和远程教育有着良好的发展前景，满足这些潜在的需求。可见，现有的校园网络已不能满足以上这些网络需求， 所以我们就有必要建立一套安全的校园网络。

3.2 校园网 VPN 方案设计

3.2.1 需求分析

根据以上论述可知，校园网内 VPN 的需求总体来说可分为 3 类，第一类是远程访问校内站点的需求，许多师生需要在异地远程访问校内的各种服务器，例如查看新闻、收发邮件、查询成绩等，这些需求都要通过远程访问校内资源来实现；第二类是解决分校访问互通的问题，我院有两个校区，一个新校区，一个老校区，如何使这两个校区间的服务如：一卡通、财务专网能够安全地整合在一起，形成一条专门的安全通道，保证这些需要加密的资源能够安全、快速的在校园网中传输；第三类就是远程访问图书馆资源，如何合理的分配图书馆资源，认证远程用户，能否使远程访问图书馆成为一套可管理、可认证、安全的系统。

3.2.2 VPN 系统的设计原则

校园网 VPN 的设计必须遵循以下原则：

a) 安全保障

VPN 系统的首要职责是保障安全，保障互联网数据传输安全的基本机制包括：身份认证、信息保密、信息完整性。因此校园网 VPN 系统起码要有以上三方面的安全保障。

b) 保证多平台兼容

作为 VPN 产品的一个重要指标就是要能够作到在任何时间及任何地点进行访问，使得移动办公用户能够随时随地的保持联网以及保证安全的网络连接。

c) 提供有效的访问控制

校园网 VPN 系统为多种应用服务提供保护，因此应该提供一定的访问控制策略，让不同的用户有不同的访问权限。

d) 有效的管理平台

VPN 服务器同时应该提供客户方和服务器方友好而有效的管理配置界面，方便用户的使用。同时还要对客户方和服务器方的通信进行详细的日志记录、安全审计，为安全检测工作提供服务。

3.2.3 VPN 系统的功能模型

根据 VPN 的设计原则和校园网的实际需求，校园网 VPN 系统的功能模型包括四个基本功能模块，身份鉴别模块、访问控制模块、数据转发模块、后台管理模块。

a) 身份鉴别模块：VPN 客户端鉴别 VPN 服务器时采用数字证书方式进行身份鉴别；服务器鉴别客户端时分不同情况采用不同的鉴别方式。在远程访问 VPN 中，服务器采用用户名/密码方式鉴别客户端身份，在内网 VPN 中，服务器采用数字证书方式鉴别客户端身份。

b) 访问控制模块：访问控制模块根据预先设定的访问控制策略，决定访问主体是否可以访问被操作对象。该模块提供访问规则库。

c) 数据转发模块：该功能是核心模块，负责以协商好的加密算法将加密数据发送给对方，或者接收秘文数据，并解密。

d) 后台管理模块：负责对 VPN 服务器的工作信息进行日志入库，便于日后审计。该模块向用户提供汇总报告，按日期、时间、访问 OS、会话持续时间等汇总网络的使用情况。

3.2.4 VPN 解决方案的选择

VPN 有三种解决方案，用户可以根据自己的需求进行选择。这三种解决方案分别是：远程访问虚拟网(Access VPN)、内部虚拟网 (Intranet VPN)和扩展虚拟网 (Extranet VPN)。

a) Access VPN：如果校园网内的师生有移动或者远程办公的需要，就可以考虑使用 Access VPN。

Access VPN 可以为单位内部人员流动多的远程办公服务。出差员工可通过

当地的 ISP 提供的 VPN 服务实现对单位 VPN 网关的私有连接。而 RADIUS 服务器通过对员工的授权与验证实现网络的安全连接。

b) Intranet VPN：可以更方便实现同一单位内部分支结构的网络互联。Intranet VPN 以特有共享设施为基础，实现对单位总部、分支机构与远程办事处的链接。单位拥有与特有网络的同步服务政策，包含服务质量、安全、可靠性与可管理性。

利用 Internet 的线路保证网络的互连性，而利用隧道、加密等 VPN 特征可以保证信息在整个 Internet VPN 上安全传输。降低 WAN 产生的费用。可以在全网络范围内灵活的应用拓扑结构。 新的站点能更快更容易的被连接。 通过设备供应商 WAN 的连接冗余，可以延长网络的可用时间。

c) Extranet VPN：如果是提供 B2B 之间的安全访问服务，则可以考虑 Extranet VPN。Extranet VPN 通过一个使用专用连接的共享基础设施，将远程网络连接到单位内部网。单位拥有与专有网络相同的政策，包括安全、服务质量、可靠性与可管理性。

Extranet VPN 可以为用户提供相对便利的服务，可以轻易的对外部网进行部署与管理，外部网的链接可以依据部署内部网与远端访问 VPN 相类同的构架与协议进行部署管理。主要的区别在于接入许可的差异，外部网用户的链接只有一次与其合作人链接的机会。

由于在校园网内部既要实现远程局域网互联，即新老校区的网络互联，还要实现远程用户访问校园网资源，所以我们选择 Access VPN 和 Intranet VPN 作为校园网 VPN 的架构。

3.2.5 技术路线

现在较成熟的技术主要有 IPSec VPN、SSL VPN 和 MPLS VPN， IPSec VPN 和 SSL VPN 是两种从属于技术路线中相区别的 VPN 构架，通常情况下 IPSec VPN 是运行于网络层中的构架，可以为全部网络层上的相关数据与相对透明的安全通信提供保护，而 SSL VPN 是在 HTTP 协议基础上运行于应用层与 TCP 层间的，总体上，两者都可提供相对安全的远程接入，但是， IPSec VPN 技术通常是运行于网络中的数据流并为其提供连接与保护，其安全等级更适合为不同的网络提供更安全的通信保障，相对于此，SSL VPN 可以更好的为远程分散提供安全接

MPLS VPN 则一般作为运营商和大型用户进行部署，适合于大型动态的网络，校园网由于技术和资金的限制，在目前情况使 IPSec 与 SSL 混合是比较理想的方案。

3.2.6

在 VPN 构建中，硬件 VPN 可以在硬件中　处理加密和解密，因此具有良好的性能，但是成本较高，要投入较多的资金。软件 VPN 方案价格低廉，而且更加具有灵活性。但是在性能、安全、可靠性以及可管理性方面往往不如硬件方案。结合我院实际，我们可以采用软硬结合的 VPN 解决方案。在现有的防火墙和路由器上，采用 IPSec VPN 实现网络互联，然后在校园网出口处架设 Linux 为平台的软件 VPN 远程接入方案。

3.2.7 方案设计

根据以上分析，结合校园网实际，校园网 VPN 方案设计如下：

a) 两个校区之间采用 Intranet VPN。在新校区与老校区之间建立 Intranet VPN。新校区与老校区之间有光纤进行连接，而且网络出口在新校区，而且在校园网中有财务部、人事部和一卡通等部门，都要经过这条链路与新校区的进行连接，在这种情况下，我们可以采用 IPSec VPN 技术，在老校区与新校区这条原有的链路上，对上述应用进行加密，从而对数据的传输起到保护作用。

对于一般用户的访问，可以在策略上允许所有的用户可以互相访问，使其感觉在一个网络中一样。安全级别也可不用设置的太高，因为设置太高会浪费系统资源，从而出现用户访问过慢的现象。对于像一些特殊部门的校园网用户，如财务、人事等部门的用户，可以采用二层网络隔离的方法先接入校园网，然后通过二层 OSPF 协议传输到核心交换机上，最后在两个校区之间进行加密传输。

对于新老两个校区来说，需要在两个校区的设备中配置路由，使这些访问对方校区的资源都经过 VPN，而且还要考虑到设备的稳定性和交换能力，而且要尽量考虑到设备的成本和利用率。所以采用两边带有 VPN 功能的路由器是个合适的选择。通过对两边路由器路由、用户策略的配置，从而实现在新校区与老校区之间建立起 VPN 通道，使数据可以根据实现设置的路由到达指定目的地址。具体设计见图 3.1: