高海英　薛元星　辛　阳　等编著

VPN技术

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS


VPN技术

国家信息化安全教育认证(ISEC)系列教材

VPN技术

高海英　薛元星　辛　阳　等编著

机械工业出版社

本书在深入研究和广泛参考大量同类作品的基础上，系统介绍了 VPN 的基本知识和框架结构，分析了网络中存在的与 VPN 相关的安全问题，提供了解决这些问题的技术，比如遂道技术、加密技术、QoS 技术以及相关的产品和厂商。

本书主要面向参加国家信息化安全教育认证（ISEC）考试的人员，同时可供电信、电力、金融、公安等企事业单位的网络安全管理员使用，也可作为网络、通信等专业高年级本科生和研究生学习网络安全课程的参考书使用。

图书在版编目（CIP）数据

VPN 技术/高海英等编著. —北京：机械工业出版社，2004.3
（国家信息化安全教育认证（ISEC）系列教材）
ISBN 7-111-14167-9

Ⅰ.V... Ⅱ.高... Ⅲ.虚拟网络—资格考核—教材
Ⅳ.TP393.01

中国版本图书馆 CIP 数据核字（2004）第 019299 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
责任编辑：戴　琳
责任印制：李　妍

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2004 年 4 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·10 印张·240 千字
0001—5000 册
定价：18.00 元

国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
井乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

教材编委会

主　任：宋　玲
副主任：赵小凡　张会生　欧阳满　蔡金荣　沈志工
成　员：洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

在信息科技对社会和经济发展起着关键作用的今天，普通及专业用户对网络服务及其应用的要求也愈来愈高，一种成本更低、使用更灵活的虚拟专网（VPN）在这一市场环境中应运而生。VPN 技术是建立在互联网的公共网络架构之上，替代连接合作伙伴之间的标准广域网，并通过一定的技术手段达到类似私有专网的数据安全传输。作为网络安全的一个有机组成部分，虚拟专用网扮演着重要的角色。

本书在写作过程中重点强调了实用性，首先对 VPN 的理论知识作了阐述，然后从实用的角度详细讲解了虚拟专用网的构建、维护管理，并且介绍了国内外 VPN 主流产品，对读者选购 VPN 产品有一定的参考价值。

全书共包括 7 章内容。第 1 章对 VPN 的工作原理、优缺点、应用领域、常见的 VPN 体系结构和应用平台作了介绍；第 2 章介绍了 VPN 的隧道技术，详细讲解了几种隧道协议：PPTP、L2TP、IPSec、SSL 协议，并且对 VPN 的加密技术、QoS 技术作了阐述；第 3 章针对 VPN 系统传递信息时所遇到的威胁，以及如何防御进行了详细地介绍，并且讨论了加密技术和认证技术；第 4 章详细描述了构建 VPN 的标准，以及如何构建 Access VPN 方案、Intranet VPN 方案、Extranet VPN 方案，介绍了 VPN 的构建步骤，并且给出了 3 个 VPN 成功案例；第 5 章详细阐述 VPN 的管理与维护工作，介绍了如何检测 VPN 故障，怎样对用户进行管理，怎样分析故障来源并排除故障；第 6 章主要介绍一些国内外 VPN 领域的主流产品并分析了产品的性能，提供了购买 VPN 产品的方法；第 7 章分析了 VPN 未来的发展方向和趋势。

本书主要面向参加国家信息化安全认证（ISEC）考试的人员，同时适用于网络工程师和管理人员、VPN 技术人员以及对虚拟专用网感兴趣的广大读者。

参加本书编写工作的还有赵海洋博士、薛勇硕士、黄明硕士、马艳庆硕士、高新波老师，另外在写作过程中也得到了宁宇鹏博士、阎慧博士以及北邮信息安全中心杨义先教授、北京正阳天马信息技术有限公司刘旸先生的热情帮助，在此表示感谢！

由于作者水平有限，书中谬误之处在所难免，欢迎广大读者批评指正。

编　者

目　录

第 1 章　VPN 基础

本章导读：

当今，随着网络技术的普及，人们需要随时随地联入企业网。另外，随着企业本身的发展壮大与跨国化，每家企业的分支机构越来越多，企业与各分部之间也需要随时通信，这涉及到远程联网及网络的复杂性问题。为了保证数据在网络传输时的安全，须按传统需要为每个分部建立独立的专用网络，但大量的独立专用网需要进行重复的网络投资，会造成资源浪费，增加管理负担。

为了解决上述问题，人们提出了虚拟专用网（VPN，vitual private network）的概念，即利用公共通信网络（如因特网）实现安全的保密数据通信。其原理是：需要进行机密数据传输的两个端点均连接在公共通信网上，当需要进行机密数据传输时，通过端点上的 VPN 设备在公共网上建立一条虚拟的专用通信通道，并且所有数据均经过加密后再在网上传输，这样就保证了机密数据的安全传输。通过 VPN，授权的业务伙伴就可以在授权范围内使用单位内部的数据，实现数据的安全交换。

本章是对 VPN 技术的一个概要介绍，目的是使读者对 VPN 能够有一个直观的了解，便于学习后面的章节。本章第 1 节介绍了什么是 VPN，然后在第 2 节介绍了 VPN 的工作原理，使得读者对 VPN 的工作机制有初步的认识。第 3 节详细地介绍了 VPN 的优点，使读者明白为什么 VPN 如此吸引人，并且介绍了使用 VPN 所带来的额外开销。第 4 节对几种常见的 VPN 体系结构做了介绍。第 5 节介绍了 VPN 的应用领域，包括内联网 VPN、外联网 VPN 和远程接入 VPN。第 6 节介绍了 VPN 的应用平台。另外，究竟具有什么样特征的产品和服务才能被认为是真正的 VPN 产品和服务呢？本章的第 7 节回答了这个问题。

1.1　什么是 VPN

现在有很多连接都被称作 VPN，用户经常分不清楚，那么一般所说的 VPN 到底是什么呢？顾名思义，虚拟专用网不是真的专用网络，但却能够实现专用网络的功能。虚拟专用网指的是依靠 ISP（因特网服务提供商）和其他 NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中，任意两个节点之间的连接并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的，如图 1-1 所示。

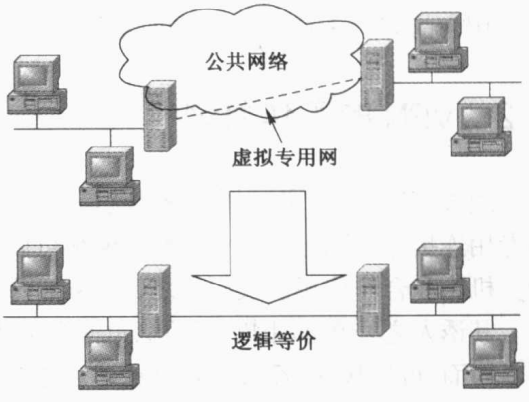

图 1-1　VPN 的含义

IETF 草案理解基于 IP 的 VPN 为“使用

IP 机制仿真出一个私有的广域网"是通过私有的隧道技术在公共数据网络上仿真一条点到点的专线技术。所谓虚拟,是指用户不再需要拥有实际的长途数据线路,而是使用因特网公众数据网络的长途数据线路。所谓专用网络,是指用户可以为自己制定一个最符合自己需求的网络。

用户现在在电信部门租用的帧中继(Frame Relay)与 ATM 等数据网络提供固定虚拟线路(PVC-Permanent Virtual Circuit)来连接需要通信的单位,所有的权限掌握在别人的手中。如果用户需要一些别的服务,需要填写许多的单据,再等上相当一段时间,才能享受到新的服务。更为重要的是,两端的终端设备不但价格昂贵,而且管理这些设备也需要一定的专业人员,无疑增加了成本。此外,帧中继、ATM 数据网络也不会像因特网那样,可立即与世界上任何一个使用因特网的单位连接。而在因特网上,VPN 使用者可以控制自己与其他使用者的联系,同时支持拨号的用户。

所以我们说的虚拟专用网一般指的是建筑在因特网上能够自我管理的专用网络,而不是 Frame Relay 或 ATM 等提供固定虚拟线路(PVC)服务的网络。以 IP 为主要通信协议的 VPN,也可称之为 IP VPN。

由于 VPN 是在因特网上临时建立的安全专用虚拟网络,用户就节省了租用专线的费用,在运行的资金支出上,除了购买 VPN 设备,企业所付出的仅仅是向企业所在地的 ISP 支付一定的上网费用,也节省了长途电话费。这就是 VPN 价格低廉的原因。

越来越多的用户认识到,随着因特网和电子商务的蓬勃发展,经济全球化的最佳途径是发展基于因特网的商务应用。随着商务活动的日益频繁,各企业开始允许其生意伙伴、供应商也能够访问本企业的局域网,从而大大简化信息交流的途径,增加信息交换速度。这些合作和联系是动态的,并依靠网络来维持和加强。于是各企业发现,这样的信息交流不但增加了网络的复杂性,还带来了管理和安全性的问题。因为因特网是一个全球性和开放性的、基于 TCP/IP 技术的、不可管理的国际互联网络,因此,基于因特网的商务活动就面临非善意的信息威胁和安全隐患。

还有一类用户,随着自身的的发展壮大与跨国化,企业的分支机构不仅越来越多,而且相互间的网络基础设施互不兼容也更为普遍。因此,用户的信息技术部门在连接分支机构方面也感到日益棘手。

用户的需求正是虚拟专用网技术诞生的直接原因。

1.2 VPN 的工作原理

通过 VPN 的定义可知,VPN 就是通过共享即公用网络在两台机器或两个网络之间建立的专用连接。实际上,VPN 技术使组织可以安全地通过因特网将网络服务延伸至远程用户、分支机构和合作公司。换而言之,VPN 把因特网变成了模拟的专用 WAN。

其诱人之处在于,因特网的触角伸及全球,如今使用网络成了大多数用户和组织的标准惯例。因而,可以快速、经济而安全地建立通信链路。

把因特网用作专用广域网,组织就要克服两个主要障碍。首先,网络经常使用多种协议如 IPX 和 NetBEUI 进行通信,但因特网只能处理 IP 流量。所以,VPN 就需要提供一种方法,将

非 IP 协议从一个网络传送到另一个网络。其次，网上传输的数据包以明文格式传输，因而，只要看得到因特网流量，就能读取包内所含数据。如果公司希望利用因特网传输重要的商业机密信息，这显然是一个问题。

VPN 克服这些障碍的办法就是采用了隧道技术：数据包不是公开在网上传输，而是首先进行加密以确保安全，然后由 VPN 封装成 IP 包的形式，通过隧道在网上传输，如图 1-2 所示。

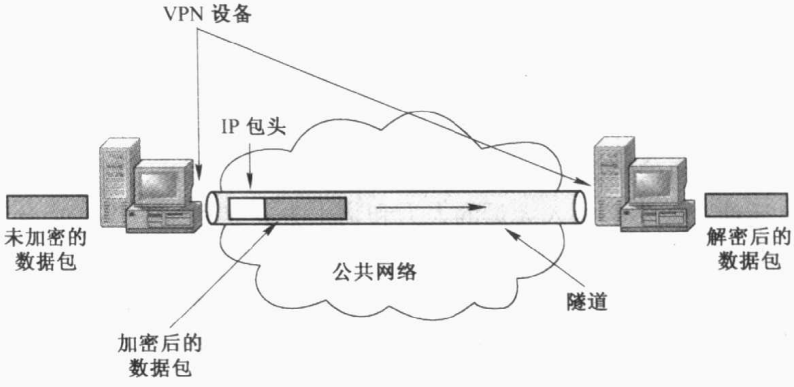

图 1-2　VPN 的隧道技术

为了阐述这一概念，不妨假设你在一个网络上运行 NetWare，而该网络上的客户机想连接至远程 NetWare 服务器。

传统 NetWare 使用的主要协议是 IPX，所以，若使用普通第 2 层 VPN 模型，发往远程网络的 IPX 包就先到达隧道发起设备。该设备可能是远程接入设备、路由器，甚至是台式机（如果是远程客户机至服务器连接的话），它为包做好网上传输的准备。

源网络上的 VPN 隧道发起器与目标网络上的 VPN 隧道终结器进行通信。两者就加密方案达成一致，然后隧道发起器对包进行加密，确保安全（为了加强安全，应采用验证过程，以确保连接用户拥有进入目标网络的相应权限。大多数现有的 VPN 产品支持多种验证方式）。

最后，VPN 发起器将整个加密包封装成 IP 包。现在不管原先传输的是何种协议，它都能在纯 IP 因特网上传输。又因为包进行了加密，谁也无法读取原始数据。

在目标网络这头，VPN 隧道终结器收到包后去掉 IP 信息，然后根据达成一致的加密方案对包进行解密，将随后获得的包发给远程接入服务器或本地路由器，它们再把隐藏的 IPX 包发到网络，最终发往相应目的地。

1.3　VPN 的特点

1.3.1　VPN 的优点

对于企业来说，VPN 提供了安全、可靠的 Internet 访问通道，为企业进一步发展提供了可靠的技术保障。而且 VPN 能提供专用线路类型服务，是方便快捷的企业私有网络。企业甚至可以不必建立自己的广域网维护系统，而将这一繁重的任务交由专业的 ISP 来完成。由于 VPN 的出现，用户可以从以下几方面获益：

1) 实现网络安全。高度的安全性,对于现在的网络是极其重要的。新的服务如在线银行、在线交易都需要绝对的安全,而 VPN 以多种方式增强了网络的智能和安全性。首先,它在隧道的起点,在现有的企业认证服务器上,提供对分布用户的认证。另外,VPN 支持安全和加密协议,如 SecureIP(IPsec)和 Microsoft 点对点加密(MPPE)。

2) 简化网络设计。网络管理者可以使用 VPN 替代租用线路来实现分支机构的连接。这样就可以将对远程链路进行安装、配置和管理的任务减少到最小,仅此一点就可以极大地简化企业广域网的设计。另外,VPN 通过拨号访问来自于 ISP 或 NSP 的外部服务,减少了调制解调器池,简化了所需的接口,同时简化了与远程用户认证、授权和记账相关的设备和处理。

3) 降低成本。VPN 可以立即且显著地降低成本。当使用 Internet 时,实际上只需付短途电话费,却收到了长途通信的效果。因此,借助 ISP 来建立 VPN,就可以节省大量的通信费用。此外,VPN 还使企业不必投入大量的人力和物力去安装和维护 WAN 设备和远程访问设备,这些工作都可以交给 ISP。VPN 使用户可以降低如下的成本:

- 移动用户通信成本。VPN 可以通过减少长途费或 800 费来节省移动用户的花费。
- 租用线路成本。VPN 可以以每条连接的 40%～60%的成本对租用线路进行控制和管理 对于国际用户来说,这种节约是极为显著的。对于语音数据,节约金额会进一步增加
- 主要设备成本。VPN 通过支持拨号访问外部资源,使企业可以减少不断增长的调制解调器费用。另外,它还允许一个单一的 WAN 接口服务多种目的,从分支网络互联、商业伙伴的外联网终端、本地提供高带宽的线路连接到拨号访问服务提供者,因此,只需要极少的 WAN 接口和设备。由于 VPN 可以完全管理,并且能够从中央网站进行基于策略的控制,因此可以大幅度地减少在安装配置远端网络接口所需设备上的开销。另外,由于 VPN 独立于初始协议,这就使得远端的接入用户可以继续使用传统设备,保护了用户在现有硬件和软件系统上的投资。

4) 容易扩展。如果企业想扩大 VPN 的容量和覆盖范围,企业需做的事情很少,而且能及时实现:企业只需与新的 IPS 签约,建立账户;或者与原有的 ISP 重签合约,扩大服务范围。在远程办公室增加 VPN 能力也很简单:几条命令就可以使 Extranet 路由器拥有 Internet 和 VPN 能力,路由器还能对工作站自动进行配置。

5) 可随意与合作伙伴联网。在过去,企业如果想与合作伙伴联网,双方的信息技术部门就必须协商如何在双方之间建立租用线路或帧中继线路。有了 VPN 之后,这种协商也毫无必要,真正达到了要连就连,要断就断。

6) 完全控制主动权。借助 VPN,企业可以利用 ISP 的设施和服务,同时又完全掌握着自己网络的控制权。比方说,企业可以把拨号访问交给 ISP 去做,由自己负责用户的查验、访问权、网络地址、安全性和网络变化管理等重要工作。

7) 支持新兴应用。许多专用网对许多新兴应用准备不足,如那些要求高带宽的多媒体和协作交互式应用。VPN 则可以支持各种高级的应用,如 IP 语音、IP 传真,还有各种协议,如 RSIP、IPv6、MPLS、SNMPv3 等。

正由于 VPN 能给用户带来诸多的好处,VPN 在全球发展得异常红火,在北美和欧洲,VPN 已经是一项相当普遍的业务;在亚太地区,该项服务也正迅速开展起来。

1.3.2　VPN 的缺点

目前的 VPN 还存在不足，总结起来有下面主要几个方面：

1）尽管 VPN 的设备供应商们可以为远程办公室或 Extranet 服务的专线或帧中继提供有效方式，可是 VPN 的服务提供商们只保证数据在其管辖范围内的性能，一旦出了其“辖区”则安全没有保证。

2）作为一种典型技术，VPN 的应用时间还不长，VPN 的管理流程和平台相对于其他远程接入服务器或其他网络结构的设备来说，有时并不太好用。

3）不同厂商的 VPN 的管理和配置掌握起来是最难的，这需要同时熟悉不同厂商的执行方式，包括不同的术语。

以上分析了 VPN 的优点和缺点，那么哪些用户适于使用 VPN 呢？在满足基本应用要求后，有四类用户比较适合采用 VPN：

1）位置众多，特别是单个用户和远程办公室站点多，例如企业用户、远程教育用户；

2）用户/站点分布范围广，彼此之间的距离远，遍布全球各地，需通过长途电信，甚至国际长途手段联系的用户；

3）带宽和时延要求相对适中；

4）对线路保密性和可用性有一定要求的用户。

相对而言，有四种情况可能并不适于采用 VPN：

1）非常重视传输数据的安全性；

2）不管价格多少，性能都被放在第一位的情况；

3）采用不常见的协议，不能在 IP 隧道中传送应用的情况；

4）大多数通信是实时通信的应用，如语音和视频。但这种情况可以使用公共交换电话网（PSTN）解决方案与 VPN 配合使用。

1.4　VPN 的体系结构

有很多可选的 VPN 结构，有独立于操作系统的黑匣 VPN，有基于路由器的 VPN，有基于防火墙的 VPN，还有基于软件的 VPN。除了这些结构之外，还有很多可以应用到这些设备上的服务和特性等。读过相关材料后，你应该可以安装任何想要的特性：从用户认证和 Web 过滤器到防病毒软件。然而，如同任何其他设备一样，在产品的有效服务数量、运行这些服务所需的处理需求以及这些服务的最终支持之间要做一个权衡。下面对几种常见的 VPN 体系结构分别进行介绍。

1.4.1　网络服务商提供的 VPN

这是使公司与因特网联网并享受 VPN 提供的最简单有效的方法。网络服务供应商将在公司现场放置一个设备来创建 VPN 隧道。然而这不是惟一的方案，一些 ISP 可以安装一个前端 PPTP 交换机，它可以自动创建 VPN 隧道。通信的目的端将信息分组进行解密并把数据发送到主机。

防火墙也可能被添加到这种类型的环境中，通常在网络设备前端或其中间。与以往建立DMZ的方法类似，内部路由器连接到防火墙的一个端口上，防火墙的另一个端口连接到外部的路由器上，外部路由器的串行口连接到 ISP 上。要注意 IP 地址、路由以及邮件之类的问题。图 1-3 描述了一个典型的网络设备供应商的 VPN 解决方案。

1.4.2 基于防火墙的 VPN

基于防火墙的 VPN 很可能是 VPN 最常见的一种实现方式，许多厂商都提供这种配置类型。这并不是暗示与别的 VPN 相比，基于防火墙的 VPN 是一个较好的选择，它只是在现有的防火墙技术的基础上再发展而已。如今很难找到一个连向因特网而不使用防火墙的公司。因为这些公司已经连到了因特网上，所需要的只是增加加密软件。很可能，如果公司刚购买了一个防火墙，往往它就有实现 VPN 加密技术的能力。

在考虑基于防火墙的 VPN 时，有很多厂商可供选择，其产品在所有不同的平台上都能有效地使用。一个非常重要的安全性考虑是关于下层操作系统的。防火墙在什么平台上运行？是基于 UNIX、NT，还是别的平台？该操作系统潜在的威胁是什么？没有百分之百的安全的设备，因此，如果你在防火墙设备上建立 VPN，你需要确认底层的操作系统是安全的。图 1-4 为基于防火墙的 VPN。

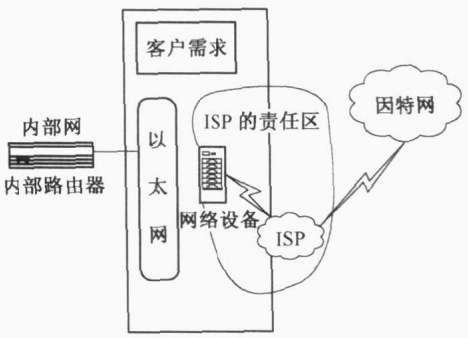

图 1-3 网络服务商提供的 VPN

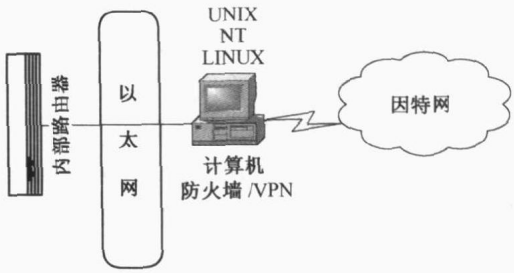

图 1-4 基于防火墙的 VPN

1.4.3 基于黑匣的 VPN

在黑匣方式中，厂商只提供一个黑匣。这是加载了加密软件以创建 VPN 隧道的一个基本的设备。一些黑匣附带有运行于台式客户机上帮助进行设备管理的软件，而另一些可以通过 Web 浏览器进行配置。这些硬件的加密设备比软件类型的加密设备速度更快，它们建立所需的加速隧道，更快地执行加密进程。并非所有的黑匣子都提供集中管理功能，它们通常并不支持自身记录，你需要把这些记录发送到另一个数据库进行查询。

目前，厂商应该支持所有的三种隧道协议：PPTP、L2TP 和 IPSec，但这也不是必然的。厂商必须尽快使专用的加密设备实现起来尽可能容易。在技术问题上，如果容易了，就不会灵活。然而，只要性能良好，对公司来说就足够了。大多数黑匣装备都需要一个独立的防火墙，尽管更多的厂商正准备把基于黑匣的 VPN 和防火墙功能合并起来。图 1-5 就是基于黑匣的 VPN 解决方案。