网络与通信技术译丛

构建虚拟专用网

Steven Brown 著

董晓宇 魏鸿 马洁 等译

人民邮电出版社

图书在版编目（CIP）数据

构建虚拟专用网 /（美）布朗（Brown,S.）著；董晓宇，魏鸿，马洁译。
—北京：人民邮电出版社，2000.11
ISBN 7-115-08767-9

Ⅰ. 构… Ⅱ. ①布… ②董… ③魏… ④马… Ⅲ. 虚拟网络-设计-方案
Ⅳ. TP393.01

中国版本图书馆 CIP 数据核字（2000）第 46330 号

网络与通信技术译丛
构建虚拟专用网

◆ 著 Steven Brown
译 董晓宇 魏 鸿 马 洁 等
责任编辑 张立科
◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@pptph.com.cn
网址 http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销
◆ 开本：800×1000 1/16
印张：31.5
字数：675 千字 2000 年 11 月第 1 版
印数：1－4 000 册 2000 年 11 月北京第 1 次印刷
著作权合同登记 图字：01－2000－2214 号
ISBN 7-115-08767-9/TN·1633

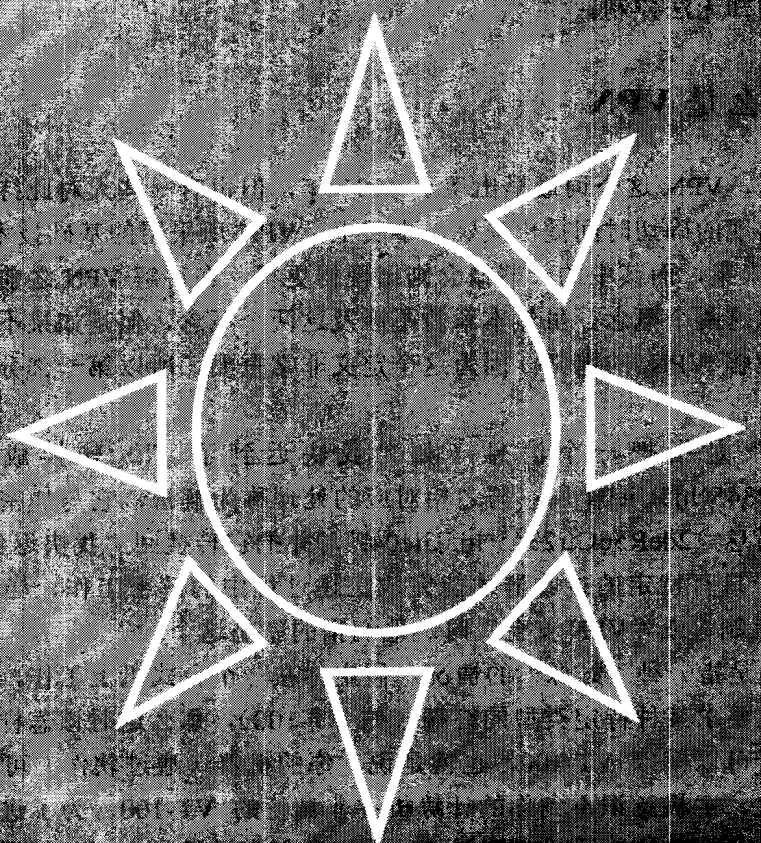
定价：49.00 元

第一部分

VPN 基础

第一章

VPN技术介绍



本章将从市场和管理的观点以及专业人员的角度来讲述 VPN 的定义，以下章节的介绍是建立在读者理解了这个定义的基础之上的。我并不期望你看完第一章之后就能建立一个 VPN，但是希望你能理解这个定义，以及和这项技术有关的一些东西。我们还着眼于构成 VPN 的组件，这里的组件仅指成功地建立和维护一个 VPN 所需掌握的那部分 VPN 技术。

你可能听说过 VPN 是一项新技术，我们将检验这种说法的正确性。我们将着眼于增长率以及 VPN 的支撑点。VPN 紧随 Internet 的传播而增长（这里的传播仅指用户接受 Internet）。不同的 VPN 有它所必须遵循的标准，因此我们要结合公司的实际需要确定应该采用哪种 VPN 服务。

本书对于 VPN 的安全机制部分有所侧重，阅读本书时，我会指导你如何着手建立公司 VPN 的安全机制，你会发现有许多影响公司 VPN 安全的安全性问题，有的可以人为控制，有的却无法控制。

1.1 什么是 VPN

追溯起来，VPN 这个词最早出现于 1997 年，但也有一些人对此持不同意见，他们对这项技术出现的确切时间提出质疑。事实上，VPN 所采用的基础技术是 60 年代出现的 TCP/IP 协议集，而其中的一些概念则出现得更早。在讲解 VPN 之前，还需要介绍一下加密和虚拟这两个概念。虽然本章暂不涉及这两个概念，但是如果不先理解这两个概念，就很难理解 VPN 的定义。因为这个定义非常重要，所以第一部分名为“虚拟专用网基础”。

“加密”是指把一个消息（如“我快迟到了。”）转换成一堆乱码（如“2deR56Gtr2345^hj5Uie04.”）；与之相对应的处理称为解密，它与加密正好相反，也就是说它接收消息“2deR56Gtr2345^hj5Uie04.”，并把它转换回“我快迟到了。”。VPN 安全问题就在于只有特定的接收器才能完成上述过程中的解密工作，当你听到人们提及“VPN 安全机制”或“VPN 安全”时，他们指的就是这个。

“虚拟”是指一种“好像”的情况。假定你在一个台式机上工作，并且要访问一台主机，该主机要求某种特定类型的终端（如 VT-100），那么这时该怎样和主机建立通信呢？你的机器可以模拟 VT-100，也就是说，你的机器（通过软件）可以像 VT-100 一样工作，因此，主机意识不到你的计算机并非真正的 VT-100。为了进一步说明这个问题，现在举一个简单的电话呼叫的例子：人们拿起电话拨号，一旦拨通，就通过电话线

建立了一条通往对端的路径，一直到通话结束，呼叫都被锁定。如果人们放下电话的时候没有把电话挂断，那么电路将仍处于激活状态，原有路径仍被锁定，这就是电话呼叫虚电路。然而，这里所说的“虚电路”和 VPN 中的“虚拟”还有一点主要区别：在电话呼叫的例子中，对话过程中不允许外人加入而 VPN 则允许。

既然我们已经掌握了虚拟和加密的概念，那么就可以接着学习 VPN 的定义了。许多人认为 VPN 是在别的公网之上建立起来的属于他们自己的专网。另一个通俗的定义则认为 VPN 是位于某个可共享的公网（如 Internet 或其他一些骨干网）之上的一条或多条广域网（WAN）链路。而我是这样定义 VPN 的：

VPN 是一个被加密或封装的通信过程，该过程把数据安全地由一端传到另一端，这里数据的安全性由可靠的加密技术来保障，而数据是在一个开放的、没有安全保障的、经过路由传送的网络上传输的。

注意：要掌握以下关键词：加密/封装/安全性/开放性/路由

从上面的定义可以看出，首先，VPN 是一个被加密或封装的通信过程，两个节点之间发生的所有通信都是经过加密的，而且，正是加密过程本身保证了数据的安全性和完整性。另外，你还会注意到，数据是通过一个开放的、没有安全保障的、经过路由传送的网络来进行传输的，因此，与电话呼叫中的虚电路不同，VPN 的数据是通过一个共用线路传输的，并且数据本身有许多可选路径到达最终目的地。

另外一种看法认为 VPN 是一个把加密数据从一点发送到另一点的简单过程，此过程通常在 Internet 上实现。然而，VPN 还可用于专用线路、帧中继/ATM 链路或普通的旧式电话网（POTN）服务，如综合业务数字网（ISDN）和数字用户线路（xDSL）。某些 VPN 的实现，如帧中继拓扑结构，已经有 ISP 提供了。尽管从 ISP 的观点来看，它是一个专用网，但在消费者眼里，它仍旧是一个公网。通过在帧字段中应用 VPN 技术，用户可以额外受益。

既然我们已经了解了 VPN 的定义，也在相应部分提到了拓扑图，那么让我们看一下一些关于 VPN 布局的简单例子。图 1-1 和图 1-2 是 VPN 设置的典型例子。图 1-1 说明一个集团网通过连接到一个公网来进行相互间的通信，这是当今最常用的 VPN 设置。可以看出，这里 Internet 被用作 VPN 技术的传输载体，而图中的“Internet”也可以被“ATM/帧中继”代替。

图 1-2 是另一种集团 VPN 的配置方案，它保留原有的系统。关于 2000 年（Y2K）问题有许多争议，大部分是与这些旧有系统有关的。VPN 依靠加密，而加密软件对原

有大部分系统来说并不适用。因此，和如今运行于客户机/服务器应用中的 TCP 打包器一样，需要给原有系统添加某种类型的安全打包器。

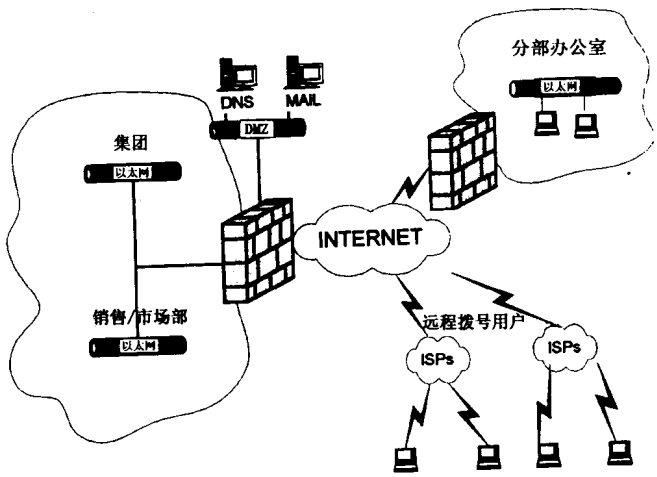


图 1-1　一个集团的 VPN

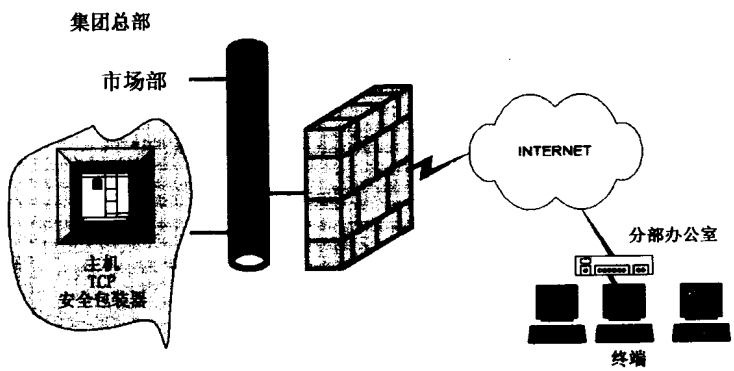


图 1-2　保持原有主机系统的集团 VPN

如果想让 VPN 用于原有的系统，就需要事先确定好是需要访问这些系统本身，还是仅仅访问这些系统中的数据。如果只是要访问系统中的数据，那么要先确定是否可以把数据转移到另一台机器上。如果要访问原有系统本身，则需要为这些机器编写特定的软件来实现 VPN 的加密算法。

VPN 技术的一大特点是它的可伸缩性。随着网络供应商不断增加其骨干网的带宽，VPN 也可以成比例扩展，从而充分利用新增的带宽。由于 VPN 是独立于平台的且不依赖于特定的操作系统，因而公司里几乎所有的设备都可以作为 VPN 客户或 VPN 服务器。

VPN 还允许扩容，大部分 VPN 设备都能处理任何加载于其上的业务。需要时，它允许建立“隧道”或基于加密的端到端连接。你可以建立通往别处的隧道（如集团总部到主要的销售办事处），然后为不同的办事处建立更多的隧道。

你还得确定公司是否需要使用封装。封装是把数据打包并封入一个 IP 分组里的过程。如果想使用 IPX 协议经 Internet 与对端通信，就要把 IPX 分组封入另一个 IP 分组中并发送出去。你还可以把一个 IP 分组封入另一个 IP 分组中，这种结构比原来多了一层保护。因此，如果你要用到 IPX 协议，就需要一个设备把 IPX 分组封入一个 IP 分组里。一些 VPN 设备提供这项功能，甚至连网关也支持这个特性。

1.1.1 VPN 应用的四个领域

我用“领域”这个词是因为最近许多文章中都用它来描述 VPN。领域只是指常用的 VPN 应用范围。通过对以下四个方面的了解，你会发现这里的说法与其他用于描述 Internet 服务的说法之间的共同点。VPN 并不是新生事物，但它们在原有 Internet 服务的基础上增加了一层加密技术。

1. 企业内部网 Intranet

企业内部网的 VPN 建立在集团总部与远程销售分部之间或集团总部与通过卫星通信的远程办事处之间。图 1-3 描述了一种典型的企业内部网服务方式。这里唯一的不同是该企业内部网是从外部访问的，即对它的访问来自外部。通常它只在公司网络内部使用，仅能被公司员工访问；企业内部网的 VPN 也可以被公司员工访问，但访问主要来自外部而非内部。

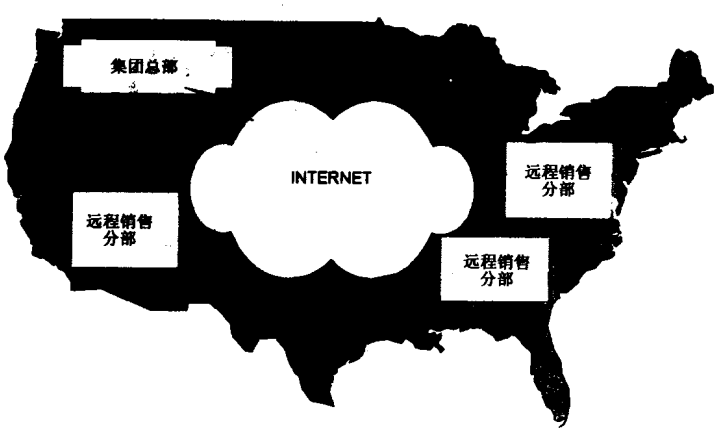


图 1-3 企业内部互联的虚拟专用网

2. 远程访问

远程访问 VPN 建立于集团总部与远程移动用户之间，图 1-4 描述了到 VPN 的最常用的连接方式，通过在远端笔记本电脑上加载加密软件，个人也可以建立一个通向集团总部 VPN 设备的加密隧道。

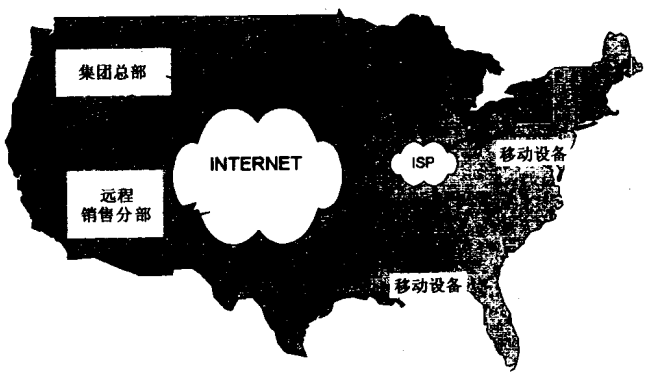


图 1-4 远程访问 VPN

3. 企业外部网 Extranet

企业外部网的 VPN 建立在集团与其用户或供应商之间，如图 1-5 所示，企业外部网允许通过目前用于 Web 浏览器的 HTTP 协议来进行访问，或使用别的经相关部门认可的服务和协议来建立连接。这就是电子商务最具影响力之处。这种方式使集团能够安全有效地与其主要贸易伙伴和客户相处。

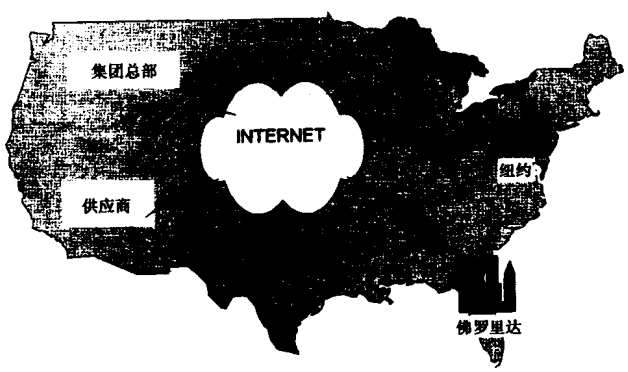


图 1-5 企业外部互联的 VPN

4. 企业内的 VPN

第四个领域是企业内部的 VPN，如今它还未被一般公司广泛采用。公司为什么选

择使用企业内的 VPN 呢？有一部分原因是因为安全性调查指出，公司所面临的最大威胁来自于内部员工。计算机安全协会（CSI）协同 FBI 打击国际计算机犯罪组织在旧金山的办事处，对美国企业、政府机构、金融组织和综合性大学进行了一年一度的调查。下面是“1998 年计算机犯罪和安全调查”（摘自 1998 年的 CSI 年度调查[http://www.gocsi.com/]）的结果。其中第四项表明，最令人头疼的是由员工所造成的经济损失。图 1-6 列出了这些机构经济损失的情况。

■ 调查显示，在过去的 12 个月内有 64%的人遇到过计算机安全侵害问题，这个数字出现了明显的增长，比“1997 年 CSI/FBI 打击计算机犯罪和安全调查”的结果（48%的人未经授权而使用）增长了 16%，比 1996 年的调查结果（ 42%的人承认未经授权而使用）增长了 22%（注意：如果把计算机病毒和笔记本电脑失窃事件包括进去，这个数字将变为 88%）。

■ 尽管有 72%的人承认因安全受到侵害而蒙受过经济损失，但只有 46%的人能把他们的损失量化。这 241 个机构的可计算的经济损失共计 136 822 000 美元。这个数字比 1997 年的统计结果（100 115 555 美元）增长了 36%。

由于计算机犯罪造成的损失

下表列出了两年多来由于计算机犯罪和安全侵害所造成的总损失。

注意：接受调查的人中有 72% 蒙受过经济损失，但只有 46%的人能够把他们的损失量化。

■ 被调查者发现的安全侵害包括多种多样的严重侵害，举例来说，被调查者当中，44%曾被无权雇员访问过，25%曾遭服务拒绝攻击，24%系统被外部突破，18%私有信息被窃，15%遇到金融诈骗，而 14%的网络或数据遭到破坏。

■ 最严重的经济损失来自内部无权用户的访问（18 个被调查者共损失 50 565 000 美元）；私有信息失窃（20 个被调查者共损失 33 545 000 美元）；通信诈骗（32 个被调查者共损失 17 256 000 美元）；金融诈骗（29 个被调查者共损失 11 239 000 美元）。

■ 认为与 Internet 的连接是一个频繁的入侵点的公司的数量从 1997 年的 47%增加到 1998 年的 54%，与 1996 年的 37%相比增长了 17%。值得注意的是，认为与 Internet 的连接是一个频繁入侵点的人数已经与认为内部系统是频繁入侵点的人数相当。（过去，内部系统曾被认为问题最大。这并不是因为内部的威胁减少，而是来自外部的通过 Internet 连接的威胁增加了。）另外一些数据可以证明这点：在承认非经授权使用的人中，74%曾经从公司外部进行非法使用，而 70%曾经从公司内部进行非法使用。

How money was lost

	Incidents W/ Quantified losses			lowest Reported		Highest Reported		Average loss		Total loss		
	1997	1998	97-98	1997	1998	1997	1998	1997	1998	1997	1998	97-98
Theft of proprietaryinfo.	21	20	41	$1,000	$300	$10,000,000	$25,000,000	$954,666	$1,677,000	$20,048,00	$33,545,000	$53,593,000
Sabotage of data or networks	14	25	39	$150	$400	$1,000,000	$500,000	$164,840	$86,000	$4,285,850	$2,142,000	$6,427,850
Telecom eavesdropping	8	10	18	$1,000	$1,000	$100,000	$200,000	$45,423	$56,000	$1,181,000	$562,000	$1,743,000
System Penetration by outsider	22	19	41	$200	$500	$1,500,000	$500,000	$132,250	$86,000	$2,911,700	$1,637,000	$4,548,700
Inside abuse of Net access	55	67	122	$100	$500	$100,000	$1,000,000	$18,304	$56,000	$1,006,750	$3,720,000	$4,726,750
Financial fraud	26	29	55	$5,000	$1,000	$2,000,000	$2,000,000	$957,384	$388,000	$24,892,000	11,239,000	$36,131,000
Denial of service	n/a	36	36	n/a	$200	n/a	$1,000,000	n/a	$77,000	$n/a	$2,787,000	$2,787,000
Spoofing	4	n/a	4	$1,000	n/a	$500,000	n/a	$128,000	n/a	$512,000	n/a	$512,000
Virus	165	143	308	$100	$50	$500,000	$2,000,000	$75,746	$55,000	$12,498,150	$7,874,000	$20,327,150
unauthorized inside access	22	18	40	$100	$1,000	$1,200,000	$50,000,000	$181,437	$2,809,000	$3,991,605	$50,565,000	$54,556,605
Telecom fraud	35	32	67	$300	$500	$12,000,000	$15,000,000	$647,437	$539,000	$22,660,800	$17,256,000	$39,916,300
Active Wiretapping	n/a	5	5	n/a	$30,000	n/a	$100,000	n/a	$49,000	n/a	$245,000	$245,000
laptop theft	160	162	322	$1,000	$1,000	$1,000,000	$500,000	$38,326	$32,000	$6,132,200	$5,250,000	$11,382,200
									Total	$100,119,555	$136,822,000	$236,941,555

CSI/FBI 1998 Computer Crime Survey

Source:CSI

图 1-6　计算机犯罪情况统计表

注意：以上最重要的是第四点，正是由于这点才引出了企业内 VPN 拓扑结构的建立，如图 1-7 所示。

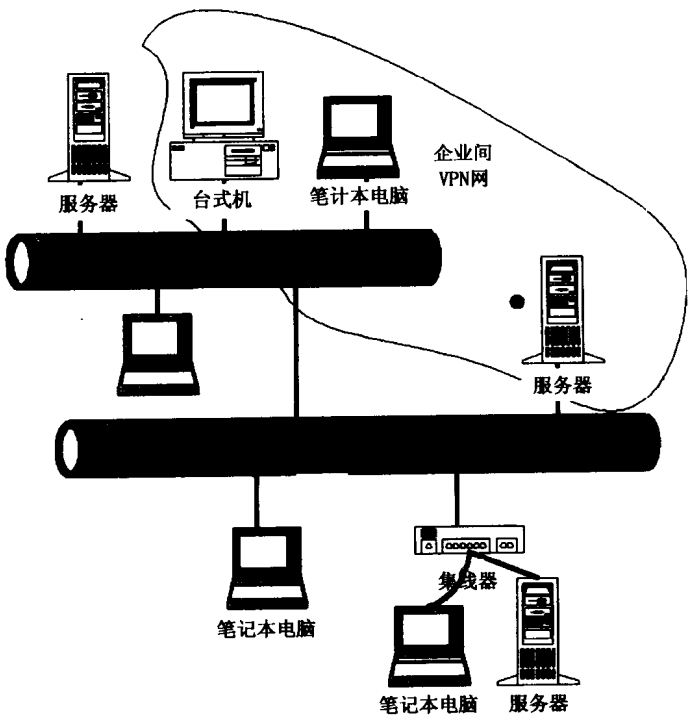


图 1-7 企业内的 VPN

企业内的 VPN 使在公司边界内建立一个 VPN 隧道成为可能，所有公司认为至关重要的通信都可以在不被侵扰的情况下经加密后通过线路传输并且被安全存储。金融记录、行政会议等等都可以在公司网中安全地从源端传输到目的端。

1.2 VPN 的组成部分

VPN 由硬件和软件组成，此外，他们还需要另外一些组件，这些组件只是为了保证 VPN 网络的安全性、有效性和易维护性。也就是说，VPN 的实际需求落实到一些性能上，当某机构需要设计和实现 VPN 时，必须考虑这些性能。不管是由 ISP 提供 VPN 服务还是自己建立，这些组件都是必不可少的。

1. 有效性

有效性是指正常运行时间和访问时间，它对于一天 24 个小时、一周 7 天都有权访问该集团服务器却因为网络问题无法进行访问的用户，一点用处也没有。不幸的是，许多网络问题不是你（有时甚至不是本地 ISP）所能控制的。如果你使用的是帧中继或 ATM 的 VPN，则可以从你的 ISP 那里得到一些有效性方面的保证，但从 Internet 那里，你得不到任何保证。

2. 控制

一些行政部门担心别人会维护和控制其公司的 VPN，这将对安全性造成很大的侵害。实际上，VPN 的管理服务对公司非常有用，他们提供训练、专门的技术、仔细的检测和告警功能。重要的是，不管你的公司有多大，你多半只有一个 VPN；你可能有别的切入点，但集团的 VPN 仍然是只有一个。那么，你将投资多少用于培训、认证和购置设备，以使你的员工跟上 VPN 技术和安全问题的步伐？

3. 兼容性

一个公司内部网络协议构架必须与 Internet 的本地 IP 地址兼容，这样才能以 Internet 为传输媒体使用 VPN 技术。另外，它还必须能把公司的网络协议转换为国际标准化组织（ISO）网络模型的第三层（网络层）。意思是说，你的公司必须知道 IP，并且清楚若你们运行的是 SNA 协议或是 IPX 协议，则必须先把 SNA 或 IPX 协议转换为 IP，才能直接与 Internet 相连。许多设备（如网关）都能实现这个功能，但是这又给网络增加了一层复杂度。另外，如果你想使用 Internet，则必须使用 Internet 上使用的地址规范（基于因特网的协议地址结构）。因此，如果使用 Macintosh 设备，则你需要把机器地址转换为 Internet 上使用的“有效的、公开的”地址。

注意：后面会讲到关于寻址、路由问题和网络地址转换（NAT），如果你还没有完成这些工作，请参阅 RFC1918。

4. 安全性

安全性是 VPN 的大问题，这点再强调也不为过。VPN 不是公司的私有网络，别人完全可以截获、收集并分析其中的数据。然而，如后面章节所述，相关的威胁和安全性问题是可以解决的。安全问题涉及 VPN 的各个方面，包括实现加密的过程、对数字签名采用的认证措施以及所使用的证书等。在 VPN 设备上实现加密算法的软件同样存在安全问题。如果你所使用的 VPN 需要操作系统支持，那么该操作系统的薄弱环节在哪呢？现在，你应该开始认识到安全性在 VPN 中的重要性，以及为什么全书都一直在强

调 VPN 的安全问题。

5. 互操作性

因为从实现的角度看，VPN 技术相对来说比较新，因而在安全性、用户以及加密水平方面都牵扯到兼容性问题。有许多现成产品可用于为 VPN 技术提供硬件、软件、加密以及认证方案，因此，很难从中选择。这里重要的是要弄清哪种 VPN 适用于你的公司？你需要的是端到端用户的互操作性，还是局域网到局域网形式的 VPN（LAN-to-LAN VPN）连通性？这将帮助你确定所要采用的厂商产品、软件厂商甚至咨询需求。

务必要获得认证。国际计算机安全组织（ICSA）成立于 1989 年，它是一个安全保证组织，负责认证计算机产品的安全，目的是提高安全产品的互用性，并认证其安全性。厂商把他们的产品拿到 ICSA 认证。将来最有可能成为这些安全标准之一的 Internet 协议安全（IPSec）标准就是通过 ICSA 认证的。ICSA 的主页上描述了其肩负的职责。

ICSA 的职责：

ICSA 是一个独立组织，它努力通过对产品、系统和人的了解和持续认证来提高全球计算方面的安全和可信程度。ICSA 的服务除认证外还包括和安全有关的研究讨论发布会、专业会员以及厂商和用户的各种合作。

[http://www.icsa.net/services/product_cert/ipsec/]

6. 可靠性

当公司决定安装某一 ISP 的 VPN 产品时，他们实际上把命运交给了该 ISP。许多主管人员经受的挫折是当他们的网络瘫痪时，他们既无法监控，也无法修理，而只能坐等他人处理。即使是一个典型的拥有一定用户数的 ISP，取得有关的资源也需要一段时间；甚至当问题解决后，一些客户也并不能马上得知，因而延误了时间。

7. 数据和用户认证

VPN 认证由数据认证和用户认证两部分组成：数据认证确认消息已被全部发送并且没有失真，用户认证是允许用户访问网络的过程。任何 VPN 技术都提供这两种认证。你可能希望外部用户能访问你的内部网，这就需要在外界用户进入你的内部网之前进行安全认证和用户认证。必须有一种方法能对内部访问提供适当的检验及对那些授权用户所需的必要服务进行审核。

一旦网上出现漏洞，这里指软硬件中安全方面的薄弱环节，那么该如何避免非授权用户进入呢？该如何区别合法用户与非法用户呢？怎样才能避免发生类似事件呢？正如我们在以下章节所述，密码学、加密和杂凑函数可以实现安全访问和认证。

8. 通信量开销

各种技术都有折衷：速度与性能、安全与灵活性，VPN 也是如此。当我们谈到数据分组大小、加密数据分组、报头等时，就涉及到开销问题。如果 VPN 设备将每一个离开网络适配器的数据分组都单独加密，可以想象这台机器需要多大的 CPU 处理能力。如果 VPN 把每个数据分组都进行封装，就可能增大数据分组的大小，从而影响到带宽的利用。

出于对安全性的考虑，IPSec 安全标准中有一种模式是把开销加到每个数据分组中。这时你会体会到链接的瓶颈，你和 ISP 的连接变得负荷超载，从而需要更大的通道。为了把影响减到最小，你应该确定要保护哪些类型的通信。一般的广播、多点传送以及类似的通信并不需要加密，然而，它们还是需要认证。VPN 设备可以在不增加数据分组大小的情况下为其提供认证机制，并且接收方可以确认数据是没有掺杂的。一个好的 VPN 设备会给出相应选项，使你可选择哪种数据被加密，哪种数据被认证以及哪种数据可以自由传输。

9. IPv6

下一个发展中的 Internet 协议是网际协议的第六个版本（IPv6），它带来了自身的新问题。考虑到 IPv6 的数据分组要比 IPv4 的大，那么，加密技术、隧道协议和封装技术对于需要对这些新的变大了的数据分组进行加密/解密的网络设备会有何影响呢？IPv6 会反过来影响网络性能吗？或网络设备是否具有可伸缩性？就安全性来说，IPSec 已经把 IPv6 加入其标准，但是目前厂商支持的协议并不一致，有的支持 IPv4，有的支持 IPv6，有的支持 IPSec。希望明年或后年能够有一套统一的公共安全协议。这是在考虑实现集团 VPN 的不同技术时要面对的另一个问题。

10. 维护

你需要确定你的公司需要哪种技术和支持。想使用一个受控的 ISP VPN 服务还是用公司现有的资源自己实现？如果你打算自己实现 VPN，那么你有安全支撑吗？你的 IT 分部能跟得上安全问题的步伐吗？必须像查毒软件一样考虑安全升级：查毒软件的有效性受其所知的最新病毒的限制。

在后面的章节中，我会从安全性的不同方面进行讨论，包括如何标识和处理侵袭。读完这些章节，你就能确定是应该自己实现安全措施，还是应该向外界求助。

11. 不可否认性

“不可否认”是指正确认定发送者，使之不能否认已发送过的数据的过程。这种方法广泛应用于制造商、零售商和重要贸易伙伴的商务活动中。电子商务、法律文献和金

融贸易都依赖于了解是谁发的定单。如果存在不确定性，公司就不能确定是谁发布的定单。为了让电子商务在 Internet 上变得可行，就必然需要不可否认性。后面章节将要讲述的证书的权威性和数字签名的作用可以保证这一点。

1.3 谁支持 VPN

许多较小的 ISP 都在提供 VPN 服务方面和大的供应商进行竞争。这并不奇怪，根据其惊人的增长率，所有的 ISP 都会提供某种类型的 VPN 服务。由于 VPN 技术多种多样，ISP 实现 VPN 的方法也不相同。一些大型 ISP 仅注重硬件加密设备，而其他的 ISP 则注重软件解决方案。两者之间的区别在于，硬件加密设备加密和保护数据分组的速度比软件设备要快。关于软件实现 VPN，有一些统计结果与上述说法不符，因此，上述说法不能单独作为一个决定因素。如果公司需要控制成百上千的 VPN 连接，那么就需要考虑使用硬件设施，但是还需要首先测试软件性能。你可能正在为不需要的服务付费。

ISP 也测试最新的、将来可能在 Internet 上使用的 VPN 隧道和安全协议。现在，三个主要的安全协议是第二层转发协议（L2F）、端到端隧道协议（PPTP）和 Internet 安全协议（IPSec）。这些标准将在后续章节中讨论，它们必须被所有的 ISP 支持，它们中的一个、两个或者全部都很可能流行起来。事实上，在写这本书的时候，第二层转发协议（L2F）和端到端隧道协议（PPTP）正被合并为第二层隧道协议（L2TP）。

客户主要关心的另一方面是性能、反应时间和安全性。许多 ISP 在向客户提供业务水平合同（SLA）和服务质量（QOS）合同的同时，也依赖标准来解决安全问题。

1.4 VPN 的增长

Internet 的增长超出了人们的想象，据估计，到 20 世纪末其用户数将超过 2 亿 5 千万。尽管每个调查结果都不一样，但有一点是统一的，那就是现在任何地方 Internet 的访问量都在 6 千万与 1 亿之间，或者超过 1 亿。Internet 的飞速发展、Internet 用户数的迅猛增长以及 Web 通信量和个人域名注册都加速了其发展势头。美国商业部预测到 2000 年加入互联网的企业将会超过 100 万。这清楚地描述了下世纪 Internet 产生以及将会产生的影响。一些研究表明在世纪之交会有 50%～80%多的商务将使用 VPN 设备。它们还指出，仅拥有 200 个远程用户的美国某跨国公司弃专线而选用 Internet 后，在仅仅 4～5 年时间内就节省了 150 多万美金。