网络与通信技术
译 丛

Virtual Private Networks

虚拟专用网

David Leon Clark 著
于秀莲 徐惠民 等 译

人民邮电出版社
www.pptph.com.cn

网络与通信

虚拟专用网

David Leon Clark 著

于秀莲 徐惠民 等译

人民邮电出版社

网络与通信技术译丛

虚拟专用网

◆ 著　　David Leon Clark

译　　于秀莲　徐惠民　等

责任编辑　陈万寿

◆ 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:25.25

字数:292 千字　　2000 年 7 月第 1 版

印数:1－5 000 册　　2000 年 7 月北京第 1 次印刷

著作权合同登记　图字:01－1999－3328 号

ISBN 7-115-08607-9/TN·1612

定价:40.00 元

内容提要

本书相当系统地阐述了有关虚拟专用网（VPN）的各种问题，既有技术上对各种协议的全面介绍，也有选择网络方案的各种考虑；既比较了各个主要 VPN 供应商的最新产品，也有 VPN 系统设置的详细过程。

本书适合相当广泛的读者的需要：既可为网络领域的技术人员提供有关 VPN 的专门知识，特别是 VPN 安全性方面的知识，也可为企业的决策者在选择网络建设方案时提供参考，更是对 VPN 技术感兴趣的广大读者的一本很好的入门书。

版权声明

本书原版书名 IT Manager's Guide to Virtual Private Networks

作者 David Leon Clark

序言

有太多的原因使企业对 Internet 感兴趣，如通过 Internet 可以使企业的网络到达任何地方，也可以使网络方便地扩展，当然，通过 Internet 通信还有很高的性能价格比。为了充分利用 Internet 的这些优点，各个企业纷纷将自己的商务伙伴、用户、产品提供商、远程数据库、子公司和移动雇员通过 Internet 与企业网进行连接。同时，多数企业也意识到，如果 Internet 被作为企业通信的骨干网但却没有任何安全预防措施，整个网络将会处于老谋深算的网络黑客的威胁之中。

在以前，企业的选择很单纯：开发自己的专网，雇一个 Internet 服务提供商(ISP)来管理，或者冒巨大风险直接使用 Internet。使用专网必需租用线路、专线或通过拨号接入，还要有专用网络所必需的通信服务器、调制解调器池和免费电话号码等，所有这些的花费是十分惊人的，致使许多企业不敢问津。同样，使用 ISP 也将是昂贵的。但是，最新出现的 VPN 技术逐渐成为一种在 Internet 上建造专用网的明确选择，因为它很便于使用，功能也在不断增强，数据加密的关键标准趋于成熟，例如 IP 安全性标准(IPSec)。《虚拟专用网》将指导您步入这个领域。

作者简介

David Leon Clark 从 1978 年起就在 IT 业工作，现在是一名 IT 顾问。它曾经在 UNISYS、General Electric Information Services、Litton Computer Services 以及 Tandy 等公司或机构工作。他曾多次发起和主持了“财富 100”（Fortune 100）的 IT 论坛和研讨会。

引 言

美国国防部委托学术界研究建立一个高速的、能在原子弹袭击下生存的开放的通信主干网，于是 Vinton Cerf 和后来加入的 Jon Postel 创建了 ARPANET。然而当其创建的网络在 1969 年开通时，他们不会想到其科研成果会演变成有史以来规模最大、增长最快的网络——因特网。这位在加利福尼亚大学洛杉矶分校研究生院与 Postel 研究 ARPANET 的 Cerf 先生，6 年后又与 Robert Kahn 开发了最前卫的 Internet 协议组 TCP/IP。为了更好地了解当今 Internet 的本质，特别是 TCP/IP，介绍一下 ARPANET 在设计伊始的情况对读者会有所启发。

在被人们称为“因特网之父”的 Cerf 和其它发明者从事 ARPANET 开发的时侯，他们的观点源于 60 年代。当时没有哪个机构会赞同这些颇具大学校园中学生团体味道的主义。创立者们就希望能有一种高速的通信系统，用户社区可以自由访问，以数据的开放共享作为基准。在当时的环境下，网络的安全性是很少或者说根本不予考虑的。毕竟，他们认为安全措施只会妨碍创造性的发挥和各种数据及想法的自由流通。即使是在他们进行科研的环境中，安全也绝不会受到关注。

当 ARPANET 由四所大学的超级计算机连接起来宣告诞生时，创立者们看见自己的梦想变成了现实。实际上，因特网的种子在 ARPANET 开通时就播下了。1972年，两种新的分支网络CSNet和BITNET（来源于"Because It's Time Network"）衍生出来，它们是作为一种允许信息在科学家中间共享的试验品出现的。其它一些分支网络例如 Usenet 则是在几年以后才建立起来的。Usenet 是一种新闻组网络，在上面可以讨论时事与一些指定话题。它也通过共享的信息和思想来提供一个前所未有的论坛，在这个论坛里，你可以探寻其它的话题。1984 年是重要的一年，在这一年里，子网系统最终合并成一个由 500 台主机组成的类似的网络，这就是我们现在所知道的 Internet（因特网）。最后的这次演变在以后的时间里继续发展，逐渐变成今天的 Internet。

网络确实在发生翻天覆地的变化。1989 年，万维网（World Wide Web，即 WWW）产生了，它能连接难以计数的信息资源，当时，它已发展到有 80000 台主机相连。来自远方电子系统的信息和共享文件信息利用这个网格状的网络传送，将网络比喻为新的信息高速公路是最合适不过的了。出于好奇、探险或研究的目的，电脑用户们也开始步入这个新的世界。逐渐地，基于万维网的第一个商业应用也出现了。突然间，我们发现，Internet 已经自成一体了。1991 年出现了超文本标记语言（Hypertext Markup Language，即 HTML）。1993 年则出现了一件值得网络界庆贺的大事，伊利诺伊大学编写并公开了第一个网页浏览器的源文件。通过这个新颖的、令人振奋的网页界面，公众可以随时随地地获取存储在大型数据库中的信息资源。到 1995 年为止，万维网上已连有 2500000 台主机和 9000 个网站。Internet 已成为一种网络装置，它吸引着许多来自不同领域的用户。网上第一个智能广播站开设后广播了第一幅大型动态图像，杂志和报纸也开始在它们的网站上张贴它们的文章，而滚石（Rolling Stones）乐队则抓住这个机会在网上广播了第一次摇滚音乐会。

1995 年，商业上对 Internet 的运用大大增多了。大部分的商人在蓬勃

发展的 Internet 面前惊呆了，企盼已久的他们这时不再犹豫，纷纷投入 Internet 的商业运作。截止至 1995 年，90000 个网站中有超过一半是商业网站。整个美国都能看到 Internet 的真正未来。它能让你从世界上任何一个地方进入（广泛性），它能比较容易地支持你扩大业务的请求（易适应性），然而，更重要的是，有分析表明，对于企业通信网，Internet 是具有最高价效比的选择。但正当越来越多的商家想在 Internet 大干一场时，开放的 Internet 里出现了令人奇怪的事情。Internet 在缺乏中心权威的情况下像珊瑚一样拼命扩张。专题研究显示，在 1989 年到 1998 年的 10 年间，Internet 每年以 340%的速度增长。这样在有些地方，Internet 就不可避免地会引来一些这样的用户，他们毫不理会网络创立者们提倡的和学术界、研究界以及商界遵循的精神。因为社会的开放性和缺乏条令约束必然会吸引来一些新的加入者，尽管这些只是部分原因。但是，这些用户主要是来搞恶作剧的，也许甚至是恶意破坏。这些不法者简直就是信息高速公路上的“地狱天使”。今天，在某些圈子里，他们被恭敬地称作聪明的黑客。

黑客入侵的问题困扰 Internet 已近 10 年了。在 Internet 大众文化圈中，黑客们享有摇滚明星般的地位，而他们“英雄般的行为”在社会中却是臭名昭著。开始的时侯，黑客们的恶作剧仅仅限于制造一些宏病毒，使得软件在电脑上运行不稳定而已。后来，黑客们偷偷采取更复杂的手段，他们利用 Sniffer 软件和渗入远端电脑内部的办法来窃取用户密码。现在，黑客会采用多种隐秘的方法，例如像“Ping of Death”那样的危险性攻击，也有会话层截取信息和后门命令攻击等。美国国家计算机安全委员会（National Computer Security Association）于 1997 年 8 月发布了一份专题报告，它是对美国联邦、州或地方政府范围内的商务机构的抽样调查。44%的答卷表示，有记录表明他们的系统曾受到外部攻击。另一个研究则表明美国国防部的军用网每年可能受到 250000 次攻击。

黑客们在 Internet 上创造了和正在创造着危险地带，导致 Internet 上存在着严重的安全问题。在公司经理的心目中，黑客攻击造成的危险如窃取

或破坏数据、瘫痪保护系统或导致整个网络暂时瘫痪，远比公司的各项支出、发展规模和价效比重要。因此，他们就会作出避免在 Internet 上进行重要的商务应用的选择。开放组（Open Group）是一个领导制定安全标准的国际协会，它于 1998 年的一项调查发现，只有 1/7（约 14%）的公司愿意把它们的重大商务应用连接到 Internet 上。

尽管网上商务的安全性十分脆弱，但它潜在的利润却不容忽视。实际上，这种潜在的利润是出乎你的想象的。我们做一个很显然但又十分无奈的假设，如果黑客问题不存在，那么 Internet 将会为企业提供一个理想的通信架构。现在可供选择的解决方案包括租用专线、通过公用数据网（这与公用 Internet 是有区别的）或 Internet 服务提供商（它是专用网的基础），相比之下，这些方案的价格都十分昂贵。美国公众对 Internet 的关注程度持续增长的最令人注目的原因，也许是建立和管理一个自己的专用网所必须考虑的花费。如果通过某种方式，Internet 可被安全地利用，人们的信息财产能在 Internet 安全机构的保护下避免遭受众多黑客的秘密攻击，商家会再被吸引到 Internet 上进行商务来往。

虚拟专用网（VPN）为企业重返 Internet 信息高速公路铺设了一条道路。关键性的加密技术、认证以及隧道协议的无缝整合的进步，使得在公用 Internet 的基础上建立安全的虚拟专用网络成为可能。其中起决定性作用的标准，例如 IP 安全性标准（IPSec）的成熟也发挥了关键作用。换句话说，VPN 能使你基于 Internet 建立和运行一个完全不受黑客攻击的企业网。相比那些依靠租用专线、公用数据网或 ISP 的昂贵的专用网络，VPN 也为企业提供了一个实用的选择。VPN 的出现标志着一个新时代的到来，在这个时代里，许多企业家们将纷纷转到 Internet 上进行重要的商务应用。总的说来，在公司网络社区允许的条件下，VPN 已将 Internet 的潜力充分地发挥出来。也许，高效地利用无处不在的 Internet 的方法曾经只是 Internet 创立者的设想，但是，高效地将无处不在的 Internet 用于安全网络通信的方法却将这个设想付诸实现。

译者的话

虚拟专用网（VPN）是近几年才兴起的网络新技术，这项技术在我国的应用更是只有一两年的时间。

虚拟专用网是要利用 Internet 的网络环境来建立企业自己的专用网络，以尽可能地利用 Internet 网络资源，节省企业网络建设的投资。

目前 Internet 本身还是一个没有安全保证的网络，建立虚拟专用网的关键就在于保证专用网的安全性。

本书相当系统地叙述了和虚拟专用网有关的各种问题：既有技术上对各种协议的全面介绍，也有选择网络方案的各种考虑；既比较了各个主要 VPN 供应商的最新产品，也有 VPN 系统设置的详细过程。因此本书适合相当广泛的读者的需要：既可为网络领域的技术人员提供有关 VPN 的专门知识，特别是 VPN 安全性方面的知识，也可为企业的决策者在选择网络建设方案时提供参考，更是对 VPN 技术感兴趣的广大读者的一本很好的入门书。

本书的作者从 1978 年就开始在 IT 界工作，担任一些著名企业的 IT 顾问，主持过“财富 100”的 IT 论坛。

目前我国十分缺乏专门介绍 VPN 技术的书籍。希望本书的翻译出版能暂时缓解这种矛盾。由于有关的技术术语国内还没有统一，本书的译文可以商榷的地方肯定不少，欢迎广

大读者批评指正。

本书第 1~7 章由于秀莲翻译，第 8~18 章及附录由徐惠民翻译。全书由徐惠民审定。参加翻译的还有肖波、杨彦豪、腾广松、王琳、李清风和郭旗等。

关于本书

VPN 技术的快速发展和 IP 安全性标准的制订使 Internet 进入了新的时期。Internet 最广为人知的特点是其广泛性、易扩展性以及高价效比，它非常适合作为企业通信网的主干。但是，近年来由于黑客问题的存在，Internet 的名声并不好。和其他的方案相比，在重要的商务和政府应用中采用 Internet 方案的比例是最低的。在一些常见的观点中，对安全的忧虑最为根深蒂固。VPN 技术最终将通过履行它的允诺而确定它向主流观点提出挑战的地位。隧道协议、认证和加密，特别是这三者之间的无缝整合的进步，使得通过公用 Internet 建立一个虚拟安全专用网络成为可能。

本书的目的在于通过对历史的回顾和技术的讲评，包括相互可操作性的标准、特点、利润、重要的产业参与者以及评估需求量的方法，为网络通信提供一个综合性的介绍和指导。本书对于 MIS 团体来说是一本结论性的参考书，而对于非本专业的学习者来说则是一本给出众多主题的参考书。通过众多的图表、示意图和例证的合理组合，读者更易理解本书的内容。

第 1 部分（第 1 、 2 、 3 章）讨论了网络通信的发展及

其对于推动企业网或内部网改造的影响。阅读完本部分，读者将了解到外部的环境压力是如何影响内部的网络通信，以及推广 Internet 使用是历史的潮流，而不是顺其自然的。第 1 章“专用网和虚拟专用网：探索网络安全”阐述了内部网的发展和促使内部网向专用网、外部网或 VPN 转变的环境。这一章也通过区分这三种网络的特点对它们进行了定义。第 2 章“为什么 VPN 能够得到不断发展”阐述了 VPN 产生的原因；政治斗争和有关 VPN 的重要的参与者、重要的隧道协议的历史性的影响与 VPN 的经济性都表明，计算机网络正步入一个新的时期。第 3 章“VPN 的标准”阐述了提供 VPN 解决方案相互可操作性的重要标准。

第 2 部分（第 4 、 5 、 6 章）揭示了潜在的安全问题的严重性。本书的这一部分说明黑客攻击并不是不可琢磨的，许多是可以确认的。另一方面，破坏安全则是由那些狡猾的黑客精心策划、挖空心思导演的一场没完没了的网络战争。第 4 章“历史上的黑客攻击”讲述了媒体披露的几个著名黑客的所作所为。第 5 章“黑客的攻击手段”按 Internet 服务和协议，如 SMTP（Simple Mail Transfer Protocol，或 E-mail）、HTTP（Hypertext Transfer Protocol,超文本传输协议）与 TCP/IP，分类介绍了黑客攻击和破坏防火墙安全的手段。第 6 章“防火墙失效时的后果及措施”讨论了如果防火墙被破坏后应该怎么办以及补救不及时会造成的后果。

第 3 部分包括本书的后 6 章（第 7~12 章）。第 7 章“VPN 技术”对 VPN 技术的概念细节和功能进行了总体介绍。第 8 章“防火墙的结构、技术和服务”介绍了现在这个领域的概况，从基本的防火墙结构到像网络地址转译这样的标准操作特点。在这一章里，将三种用于建立防火墙的主要结构与开放系统互连（OSI）参考模型进行了比较，目的在于使读者对它们的固有作用有较深的了解。这一章也对照比较了现在已应用的防火墙结构技术。最后，以有关标准、Internet 服务和防火墙支持协议的讨论来结束这一章的学习。第 9 章“防火墙发展的新趋势”讲述了防火墙特点及方案的最新进展。在这一章读者将会接触到新的术语，例如防火墙的“砖”。第

10 章“其他 VPN 关键概念和技术”介绍了读者应该了解的 VPN 和相关方面的术语。第 11 章“VPN 和防火墙的安全策略”通过讲述制造商实际的安全管理方案，为读者搭起了一座从概念到现实的联系之桥。在随后的讨论中，读者将了解到如何通过 GUI 接口用“规则库逻辑”来建立一个集中安全体制。这种以规则库为基础建立的集中安全体制，是防火墙网关用来解决数据管理和应用管理的基础。第 12 章“VPN 性能评价和回顾”介绍了 VPN 使用中的细节问题和正在使用的防火墙结构固有的特点的影响。看完这个部分，读者将会比较牢固地掌握 VPN 技术，同时了解到建立一个基于规则库的有效的安全体制的重要性，而且读者还会看到 VPN 解决方案对于自己的网络环境将具有怎样的发展潜力。

第 4 部分致力于讲述商务评估指导方针，它用来评定适合 VPN 解决方案的潜在需求领域。第 13 章“VPN 的实施：商业需求的评估”为 MIS 专业人员提供了一大套指导方针。指导方针将使读者能适当地评定某个领域是否需要成熟的 VPN 方案。第 14 章“VPN 的商业评估：跨国公司”和第 15 章“VPN 的商业评估：中小企业”为 MIS 专业人员和非技术高层管理者提供了指导。这些指导能帮助读者轻松地用有关 VPN 的术语来表达商业需求。

第 5 部分深入探讨了当今众多厂商各种有效的解决方案。第 16 章“VPN 供应商的解决方案”对竞争激烈的 VPN 解决方案进行了大范围的纵览。这里表达了一个信息：厂商解决方案的标准的融合程度非常重要。这一章还给出了对照图表，使读者对 VPN 供应市场的激烈竞争有一个更直观的了解。最后两章，第 17 章“配置防火墙”和第 18 章“配置虚拟专用网”将分别使读者对防火墙和 VPN 的配置有所了解。所借助的产品是普遍使用的 Check Point Software Technologies 公司的 VPN-1 防火墙。

本书是如何组织的

《虚拟专用网》由七个部分组成：简介和由 18 章组成的 5 部分主要内容以及附录。

引言　　引言包括预期的读者、本书涉及的范围、应如何使用本书及本书的编写体例。

第一部分　　这部分包括前三章内容（每章的主题请见前面的“关于本书”），这部分是从哲学的角度对内部网向虚拟专用网发展的全面回顾，接着介绍 VPN 兴起的源由，随后是已存在和正在出现的标准的概况。

第二部分　　这部分由第 4 章到第 6 章组成。它综合介绍了对黑客攻击的策略和技术，以及几则历史上黑客行动的逸闻。这部分还推荐了当防火墙被破坏时几种应对的办法。另外，本部分还给出了有关防火墙安全问题的网站地址。

第三部分　　这部分包括第 7 章到第 12 章，详细介绍了 VPN 技术。也综合讨论了防火墙技术，接着对如何利用防火