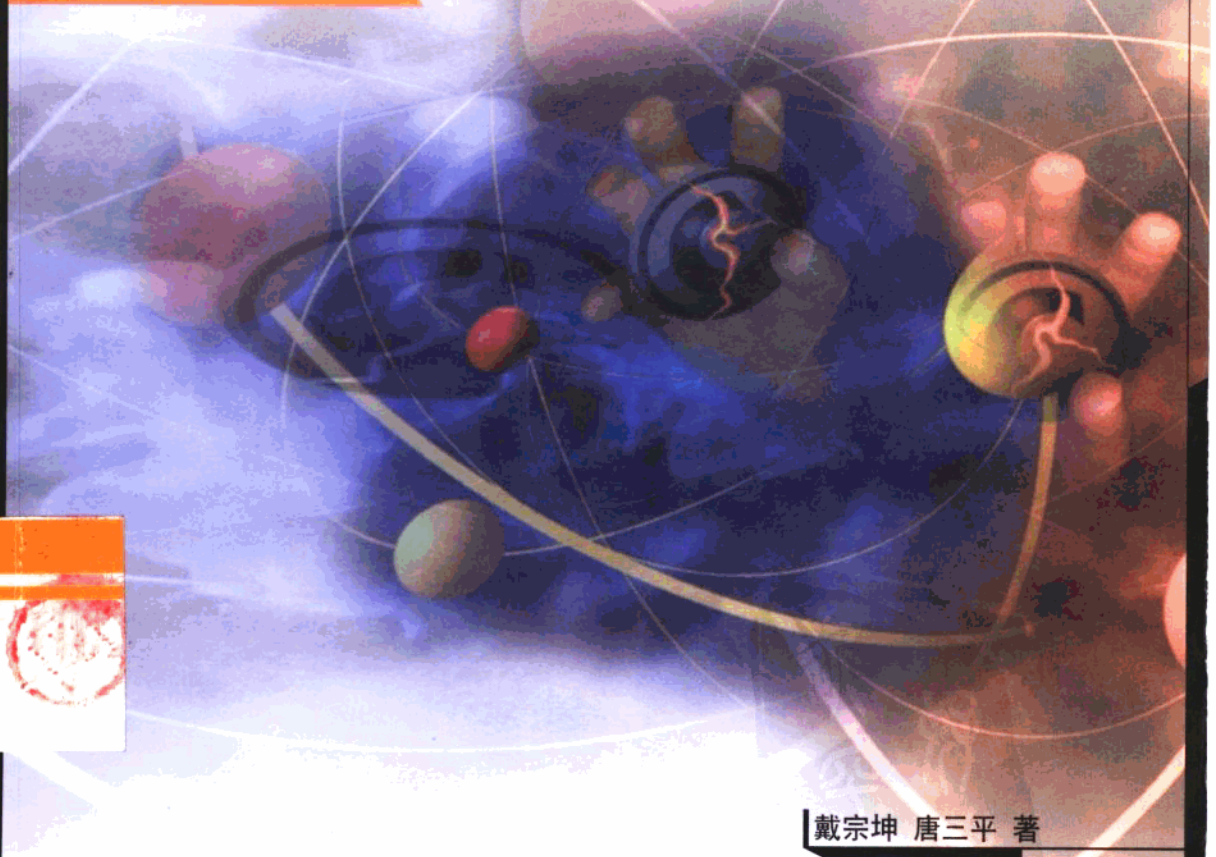
信 息 安 全 丛 书

VIRTUAL PRIVATE NETWORK

VPN与网络安全



戴宗坤 唐三平 著

金城出版社

作者寄语

近一年来，国内关于 VPN 技术和产品的报道、讲座和资料开始在各种媒体上活跃和丰富起来，表明这一具有新创意的传统技术获得了新的发展空间。

VPN 是英文 Virtual Private Network 的缩写，其意为虚拟专用（或私有）网络。它强调这一网络技术的“虚拟”和“私有”特性。VPN 的最早应用可追溯到使用（人工和自动）交换方式的公共电话网络，最近的最为普遍的应用则当数利用因特网技术构建各种各样的网络。VPN 的精妙之处在于它通过逻辑分割而不是物理连接从公共通信基础设施中“隔离出一个专供自己使用的网络”，既省钱又方便；另一方面，VPN 的“虚拟”和“私有”特性隐含着我们通过因特网构建内联网、外联网和远程用户接入网时所渴求的某些安全要素。但是，对于 VPN 技术，毕竟缺乏理论上的系统研究，以致于 VPN 在不同职业的人眼中具有不尽相同的内涵和意义。

什么是 VPN？什么样的 VPN 才能满足我们构建安全网络平台的需求？哪些技术可以支持构建 VPN 网络？其中各有什么特点，各自存在什么问题，应该怎样解决，这正是本书力图说清楚的问题。

本书分两个组成部分。第一部分包括绪论和一至三章，着重研讨 VPN 概念、VPN 应用、VPN 技术构架，安全 VPN 概念和利用安全 VPN 构建安全网络平台；第二部分包括本书其余各章，着重分类详细研究支持构建 VPN 网络的技术和机制，以及有关鉴别服务机制，其中对机制有关的安全风险及对抗措施做了尽可能的描述。书中关于安全 VPN 的概念，关于 VPN 不等同网络安全的论点，关于利用 VPN 支持构建网络安全平台的设想，均系作者所在单位及作者本人几年来在进行技术和产品研发中的经验总结和研究结论，完全系一家之言，欢迎对此提出批评，进行交流，以推动对这一问题的深入研究。

本书由戴宗坤策划并主笔撰写第一部分，戴云燕参与文字录入和校订；唐三平主笔撰写本书的第二部分及附录。

本书在编写过程中，得到四川川大能士信息技术有限公司的环境支持，得到四川大学信息安全研究所全体同志的具体帮助。没有这些优越的外部条件，本书的编写是不可能的。对此，作者谨表衷心地感谢。

作　　者
四川大学信息安全研究所
2000 年 8 月 8 日
Email：Nesec@mail. sc. cninfo. net

绪　言

1．由于通信技术、微电子技术和计算机软件技术的迅猛发展，以计算机技术为基础的网络技术在开放系统互连模型和 TCP/IP 协议簇的规约下，异型计算机之间、异构网络之间互连的技术屏障已被完全打破，由此推进了信息技术的发展。人们曾在 20 世纪 70 至 80 年代苦苦追寻的连接“信息孤岛”的方法已经找到。网络通信技术的发展，微型计算机性价比的不断提高，宽带网络的实现和基础通信设施的逐步完整，使得以电子信息为主要传播形式的声音、图像、符号、文字等信息的交换、共享和管理变得十分容易、简便和可行。从个人、家庭，到企事业团体，到金融系统、政府和军事部门，都在思考、学习和实践着如何利用计算机网络支撑起各自的信息系统，以辅助、优化和替代个人、团体和国家原来采用手工方式利用生产工具完成的各项职能、功能。这种转变方式，不仅直接解放了生产力，提高了工作效率，促进了社会、经济的发展，而且正深刻地影响着每个人认识世界、改造世界的思维方式和行为方式，引起社会、经济和文化的深刻变化。可以说，网络化推进了信息化的进程，我们正在步入信息化社会，这已成为不以个人意志为转移的社会和技术发展潮流。

2．以网络技术为平台的信息系统在解决了信息交换、扩张和共享技术的同时，也对信息的所有权、使用权和拒绝权提出了严重挑战。从某种意义上讲，计算机网络信息系统就是人类社会行为和相互关系在网络技术系统的映射。从这个角度来看，在功能上，计算机网络信息系统将全面、无限地仿真、逼近人类社会的思维方式、行为方式和关系；与此同时，人类社会的负面——丑恶、犯罪等也会全面反映到网络化信息系统中去。国内曾有对利用网络化信息系统实施犯罪进行研究的专家半开玩笑地说，利用计算机网络几乎可以实施除强奸罪以外的任何犯罪活动，足见问题的普遍性和严重性。

如果在建设计算机信息系统时只考虑互连互通和资源共享的问题，只考虑系统的功能实现，那么可以毫不夸张地说，这个信息系统是一个对外界裸露的系统（它的网络拓扑、它的网络和信息资源在外部网络看来都是可见的、可获得的、可修改的和可假冒的，等等），因而是一个自身未设防的系统。究其原因有两个：一是系统赖以完成互连互通、信息共享的技术本身存在着固有的安全隐患和漏洞（这可以是计算机和网络操作系统与应用软件设计和升级引起的问题，也可以是实现各种功能的协议和规范存在问题，也可以是软/硬件设施的暴露和直接可获取的问题，也可以是协议应用不当造成的问题等）；二是计算机信息系统在规划、设计和实施中普遍存在的淡薄的安全观念、重应用轻安全的设计思想以及单纯“打补丁”的安全策略遭致的种种安全问题。

3．为此，必须针对上述两方面的原因，首先从体系框架上为自己的计算机网络信息系统构建科学、系统、完整并可适应的安全保障体系，为在全面实施安全保障体系方面出现经费不配套等可控因素时，可在安全保障体系架构下，采取分步骤实施原则对安全保障体系中的安全功能和安全服务措施进行优先级排列。优先级排列的总原则是普遍适用的安全功能优先（如系统准入控制措施），信息系统赖以运行的软硬件基础设施安全措施优先（如机房物

理环境、系统运行的通用软件平台安全等），信息系统通过公共网络实现连接和传输的网络安全平台优先（如连接界面的物理/逻辑隔离，传输过程的鉴别、完整性和保密性措施等），以及重要信息资源、网络资源的保护优先（如资源服务器的保护等）……。以上优先措施都是计算机网络信息系统的基础性安全措施，这些措施明显地具有普遍适用性、宏观性、基础性和粗粒度控制的特点。信息系统在规划和实施过程中，应结合自己的实际情况，优先选择其中的安全功能和服务措施，从基础上构建安全体系的框架，然后才谈得上针对具体个别的应用业务采取深入的细粒度的安全控制和服务措施，以期达到“风险/投资/安全”的动态平衡。在计算机网络信息系统的规划、设计和实施中，必须坚持全面、系统和可适应的安全设计策略，彻底摒弃单纯依靠“打补丁”的安全策略。事实上，单纯依靠“打补丁”的方法不是真正的安全策略，或是不能保证安全的策略。在计算机信息系统中，“打补丁”曾是整个安全策略中的一种应急的、临时的、无可奈何的措施，也是此前计算机系统管理员解决安全问题的惯用手法，它曾经在计算机操作系统和某些通用应用软件平台的推广使用上起过重要作用，至今在计算机信息系统的应急服务中仍不失为一种有效措施。但是随着网络化概念的扩大和延伸，网络化信息系统由原来的较为封闭、安全的运行环境中延伸至一个充满威胁和互相不信任的运行环境中，单纯依靠“打补丁”的安全策略不仅是不可行的，而且是危险的。

4．当今的计算机网络已经不是传统的局域网、广域网概念了，虽然原来的局域网、广域网技术中的经典部分仍然可用，但在整个技术体系和运行协议上已发生了根本性变化。其中最重大、最有影响也是最有生命力的技术就是基于 TCP/IP 协议簇支撑下的开放系统互连互通和信息资源的链接共享技术，以这种开放连接技术构成的计算机网络已没有人们在传统意义上的边界意义了。中国工程院院士何德全在《维护信息安全刻不容缓》一文中说：“90 年代进入了互联网时代，每个用户都可以连接、使用乃至控制散布在世界上各个角落的上网计算机。”更有人将互联网络比喻成汪洋大海，接入国际互联网的用户和计算机网络就好比是漂泊在汪洋大海的一叶孤舟，随时有触礁和遭遇风暴翻沉的危险。另一方面，这种网络技术对人们的诱惑力又是无法抵挡和抗拒的。计算机网络用户产品开发和研究人员，不失时机地抓住这一机会，为解决企事业单位通过公共通信网络将地域分散的分支机构“连接在一起”提出了内联网（Intranet）概念，为解决企事业单位通过公共通信网络与合作伙伴和有某种共同利益的外部内联网实现互连互通和信息交换而提出的外联网（Extranet）概念，以及为解决企事业单位职员出差或旅游在外，通过公共通信网络共享内联网资源而提出的远程接入（Remote Access）概念。这些网络连接概念充分利用各种公共通信基础设施的交换能力和对 IP 协议的兼容特性，既解决了源/宿主机跨越各种网络结构的一致性连接问题，又解决了信息流通过公共通信基础设施这一“信息高速公路”的有序和拥塞问题。不难看出，内联网、外联网和远程接入概念，与一般的因特网接入和访问不同，它必须强调是通过公共通信基础设施将一个机构内的各个分支网络或将具有某种共同利益的机构外的分支网络和用户“连接在一个网络中”，很显然，这种网络没有自己所有权的网络设备和通信线缆，而是长期租用或临时租用公共通信基础设施中的某一部分或某些部分供完成自己的业务需求和应用功能使用，由于端设备是按照一个机构内部的策略或与外部约定的共同策略进行配置和运行的，因此这样构成的内联网、外联网和远程接入网具有某种为外部未授权者不可知的策略和逻辑关系，形成逻辑上的“私有性”或“专用性”，而这种网络明显地不具有真正意义上的

物理结构，因此是一种“虚拟的”网络。这种网络连接技术，就是近年来广为流行的 VPN 技术。

5. 本书着重研究 VPN 技术与网络安全的关系与方法。如前所述，以 TCP/IP 协议簇为支撑的网络互连技术极为成功地解决了异型计算机之间、异构网络之间的互连互通问题，它的设计初衷及其使用环境基本未考虑为此互连技术造成的安全隐患和固有的漏洞，这是因为 TCP/IP 协议族的主要协议及因特网原始主干均源于美国国防部的研究计划和项目应用，众所周知，它是一个美国国防部的内部封闭的网络，网络内的用户和设备在严密的管理制度约束和高强度的安全观念培训机制下，其运行环境是安全的。很显然，在一个完全安全的环境中运行的设备和用户不需也不必考虑安全隐患和安全漏洞。由于这一技术对社会、经济发展的巨大价值，美国军方在将这一技术和主干网移交给社会使用时，已将原始主干网络分成无物理连接的两个部分。很显然，TCP/IP 协议簇设计和因特网项目的发起者完全意识到了其中已经和可能存在的安全问题，由于对这些安全问题的分析和研究已不属于本书的范围，本书不予详述。

我们在上一个问题中提到过 VPN 技术在利用公共通信基础设施构成内联网、外联网和远程接入网方面，由于采用了策略管理，在逻辑上具有的“私有性”和“专用性”特点，这相对于纯粹利用公共通信网络进行国际互联网连接和访问已有了一定的安全保障。但是，由于 VPN 的支撑技术和实现方法繁多，应用场合和目的也有很大差异，就某一网络的具体情况而言，所采用的 VPN 技术是否足够保证在与公共网络连接和访问过程的安全，是否足以对抗来自公共网络的各种攻击，必须进行设计和论证。准确地说，VPN 是一种利用公共通信网络（设施）的组网技术概念，而不是安全技术概念（尽管其中一些功能具有安全特性），为此我们提出安全的 VPN 技术概念。这里的安全 VPN 概念，我们将其定义为将鉴别认证、访问控制和密码技术及其管理从体系上与 VPN 组网技术集成为一体的 VPN。通过安全 VPN，可以在利用公共通信网络组建虚拟专用或私有（private）网络的同时实现连接的鉴别和控制，实现数据传输的完整性、机密性功能，实现 VPN 设备的策略管理等具有明显安全特性的功能。

基于上述考虑，本书将集中对 VPN 技术及其实现、安全 VPN 技术及其实现以及与网络安全有关的问题，结合我们的研究成果进行深入讨论。

目 录

第 1 章　VPN 技术及其应用

1.1　VPN 概念

VPN 是英文 Virtual Private Network 的缩写，现已被人们作为一个专门术语来接受。对于术语 VPN，在研究人员、开发商、网络集成商和应用客户看来，都有侧重面不同的理解和认识。仅从市场角度看，开发商和网络集成商就可以根据自己产品的特点和定位赋予 VPN 以某种定义和解释，这些定义和解释不无道理，但并不一定准确与贴切。Cisco 系统公司的 Paul Ferguson 等人对这种现象进行了剖析，说："VPN 的奇妙之处在于其定义之多，可以给每个公司以同等的机会来声明自己目前的产品就是真正的 VPN 产品。但不管你选择怎样的定义，对组网技术的这种随心所欲的说法是没有意义的。"他认为"VPN 的思路是在公共网络上通过隧道和/或加密技术创建专用（私有）的网络，……它运行起来就像是在嘈杂的广场中的人耳中塞进棉花，自认为广场周围没有其它人存在一样。"显然，对于 VPN 的理解，真是仁者见仁，智者见智。但从字面意义和虚拟组网技术综合起来分析，我们不难从一般意义上给 VPN 以较为准确的定义。

从字面意义上看，术语 VPN 由"虚拟"（Virtual）、"专用或私有"（Private）以及"网络"（Network）三个词组成。如果将三个词进行详考，然后以简明贴切、符合常理并具有内涵的方式将其联系起来，可以认为这种对 VPN 的定义就比较确切了。

为此，首先探讨"网络"一词。网络的最原始的物理意义源于电子学中的网络理论，该理论认为"网络是由电阻器（R）、电容器（C）和电感器（L）及其它电气原件连接而成的电路"。显然，将这一原始定义引伸至对计算机网络进行定义，仍不失其内涵。不过，为了更通俗地具体地说明问题。我们这里将网络的范围界定为"通过某种方法和介质将可以互相通信的任意数量的设备连接起来的一个有机整体"，这里所指的设备包括计算机、打印机、路由器等等，并可配置在地理位置不同的地方。它们以不同的方式进行通信，它们可以根据需要选择不同的电气信号规范、数据链路、传输和应用协议。简言之，"网络"就是这样一些设备的集合，这些设备能以某种协议或规范进行通信，并可成功地在这些设备之间传输和接收数据。

关于"专用或私有（private）"一词，看起来非常直观。就网络通信而言，"专用或私有（private）"的最简化定义可概括为"两个以上设备之间的通信是以某种方式秘密进行的"；另一种定义"专用或私有（private）"的方法是与其反义词——"公共"进行比较。"公共"设备就是公共可存取的设备，并且常常经由一个公共管理实体在共同公共资源关系约束下进行管理。"专用或私有（private）"设备则相反，它们只被预定的实体集合存取，而不允许第三方进行存取的设备，"专用或私有（private）"资源受到拥有排他性存取权力的实体实施的管理。在没有连入因特网的组织网络或其它组织网络中的组织网络中，能找到这种私有网络的例子。由于这样的网络不具有外部连通性，因此没有与外部网络的通信，所以是专用或私有（private）的。

“虚拟”是一个较复杂的概念，译自 Virtual，它本是一个形容词，用于网络技术中，倾向于取意“虚拟”比较贴切。虚拟在这里可有两种互相关联的解释，一是对「逻辑」的另一种通用说法，常指用计算机仿真的虚拟事物（例如比物理存贮器容量更大的可寻址虚拟存储器，是一种管理共享资源存取的方法）；二是指用仿真（或模拟）的方法实现某些实际上并不存在的事物的功能，此处虚拟与「实物」相反。

至此，可以将 VPN 与虚拟网络、专用（私有）网络的内涵进一步联系起来。虚拟网络将专用或私有（private）通信引导到通过不是一个组织所共享的网络基础设施。专用或私有（private）资源是利用某些基础性公共共享资源的逻辑分割原则来构建的，而不是利用独立的专有的物理资源及通信服务来构建的，因此这些“专用或私有（private）”资源是虚拟的。由于 VPN 中的“专用或私有（private）”网络并无与此相应的私有物理通信系统，因此专用或私有（private）网络是没有物理实体的虚拟创意。

关于虚拟通信，我们可以这样来理解，两个以上设备之间的虚拟通信是这样一种通信，数据内容对那些没有参与该虚拟通信的那些设备是透明的，而且它们也根本不了解该虚拟通信同层之间的私有关系。

综上所述，VPN——这里专指在公共通信基础设施上构建的虚拟专用或私有（private）网（简称虚拟专用网或虚拟专网，下同），可以被认为是一种从公共网络中隔离出来的网络。VPN 的隔离特性提供了某种程度的通信保密性和虚拟性。虽然 VPN 在本质上并不是完全独立的网络，它与真实网络的差别在于 VPN 以隔离方式通过共享公共通信基础设施，它提供了不与非 VPN 通信共享任何相互连接点的排他性通信环境。

至此，我们可以从通信角度将 VPN 定义为：

“VPN 是一种通信环境，在这一环境中，存取受到控制，目的在于只允许被确定为同一个共同体的内部同层（对等）连接，而 VPN 的构建则是通过对公共通信基础设施的通信介质进行某种逻辑分割来进行的，其中基础通信介质提供基于非排他性网络的通信服务。”

同时，我们可以从组网技术角度将 VPN 定义为：

“VPN 通过共享通信基础设施为用户提供定制的网络连接，这种定制的连接要求用户共享相同的安全性、优先级服务、可靠性和可管理性策略，在共享的基础通信设施上采用隧道技术和特殊配置技术措施，仿真点到点的连接。”

VPN 可以构建在两个端系统之间或两个组织机构之间、一个组织机构内部的多个端系统之间或跨越全局性因特网的多个组织之间，以及单个应用或组合应用之间。

不难理解，任何通信连接只要是全部或部分地通过公共通信基础设施来实现，那么这种连接所组成的网络就不是真正的私有网络，换句话说，除非一个组织部署自己专有的通信介质和层次化传输系统，那么任何网络都存在“虚拟化”连接服务。

1.2 进一步理解 VPN

在网络技术已相当发达的今天，人们之所以对 VPN 产生浓厚兴趣，是因为这种组网技术有其强大的生命力和发展潜力。根据§1.1 所述的 VPN 概念，不难得出结论，就广义而言，包括程控交换电话网络和因特网本身都可纳入 VPN 范畴，但是将 VPN 作为专用术语进行研究并广泛得到生产开发商和市场支持的 VPN 已经不是这种过于广泛意义上的东西了。

从研究角度看，VPN 实在不能说是新事物、新东西。但这一技术变得具有生命力且为

人们普遍看好，确又是近几年的事。这里有网络设备开发生产供应商的功劳。迄今为止，有关 VPN 课题的学术论文仍寥如星辰，更多的是从市场角度来理解 VPN。

人们知道，电话的发明与使用已有 100 多年历史，人们在打电话时，首先拿起话筒，然后拨一个电话号码。一旦连接成功，就在发话方和受话方之间的一对线路上建立起通信通道，该通道被“固定”下来直至通话结束并挂机。很显然，这条“固定”的通话线路只是发话、受话方两端与第一个电话交换机节点之间的线路才是永远固定的，而中间各个交换机之间的连接线路则是临时（在通话期间）“固定”的，且与通话两端点之间的路径计算方法有关。这就是虚拟电话电路。不难理解，电话交换技术是最早的 VPN 技术。计算机网络技术特别在 WAN 连接技术出现以后，人们又将在共享公共通信网络上的一个或多个 WAN 连接看作是又一类 VPN 技术。当基于 TCP/IP 协议簇的因特网开始风靡全球的时候，人们又将原先的各种建立在公共通信网络上的 WAN 看作是因特网的一部分，即使那些具有特定协议规格的网络体系（如 SNA，Netware 等），也在开发其与 TCP/IP 兼容的技术和产品，以期充分利用因特网这一“信息高速公路”来连接各个专网站点。在 WAN 技术和因特网连接技术以及借助因特网连接专用网络的所有技术中，从通信连接建立的发起，到数据传输，到通信连接关闭这整个期间的“线路都是固定的”，而这一“固定的”线路仍是某种程度的虚拟电路网络。因此从本质上看，VPN 并非近几年才出现的新事物，可以说包括电话交换网络和因特网的应用，自始至终都离不开虚拟电路、虚拟网络技术。

另一方面，人们对 VPN 另眼相看，并开始进行专门研究，确是 20 世纪 90 年代中期以后的事，这与采用隧道封装技术和密码技术共享公共通信网络（特别是因特网）组建内联网、外联网或远程拨入网有极为重要的关系。人们基于两个原因对 VPN 特别感兴趣，一是组建或接入跨越长距离地域的“内部网络”时基础通信设施的巨大投资和维护费用；二是通过公共通信网络途中，通信数据对通信双方之外第三方是暴露的。前者需要解决公共通信基础设施的共享问题，从而在保证互连互通的同时，提高通信系统的效/费比，降低通信成本；后者需要解决利用公开公用通信基础设施过程的“虚拟专用”和通信数据的隐蔽性问题。从这一意义上，将 §1.1 中定义的一般 VPN 概念进行了强化，并赋予新的思想。因此，从创新的意义看，VPN 是一个历史悠久而又新鲜的技术。所谓创新被认为是“一种思想或概念、实践或事物，被个人或组织机构在社会系统成员之间通过某些渠道进行传播，并且认为是或感觉是新的东西。”这样看来，就可以将现今人们热心的 VPN 与传统虚拟连接技术或网络的 VPN 进行联系和比较，从而获得对 VPN 真谛的认识，以避免在谈到网络安全、组网技术时混淆和滥用 VPN 的“虚拟”、“专用”和“安全”的内涵。

现在探讨一个问题，为什么迄今人们（特别是在业界和市场上）对 VPN 的认识和理解的差别如此之大呢？以与网络安全有关的 VPN 技术和产品为例，不少人将 VPN 定位为网络安全产品，甚至将 VPN 的配置与网络安全等同起来，其中显然有很大的误解。首先这与长期来对 VPN 缺乏学术研究力度有关，只是近年来人们在利用公共通信网络组建 VPN 的过程中才逐渐认识到 VPN 组网技术与网络安全具有某种内在联系，因此人们出于解决信息安全前提下的网络安全问题，正不断为 VPN 实现方法和技术注入新的思想、方法；与此同时，目前国际上尚缺乏公认的 VPN 技术标准，因此在产品宣传和市场上必然受到 VPN 产品供应商对 VPN 进行有利于自己产品的导向性解释的影响，这就缺乏标准性和客观性。随着 VPN 产品的市场需求增大，介入 VPN 产品的厂商也会增加，客观现实需要从技术开发、生产、销售、配置方面对 VPN 制定可接受的标准。

此外，VPN 作为注入了新思想的传统技术，人们也需要时间和实践才能准确把握它。

1.3 VPN 的应用前景

在上一节中，我们分析了近年来人们重视、正视 VPN，注入新的机制以逐步丰富和完善 VPN 的实现方法，并积极探寻支撑各种安全网络平台的 VPN 技术，目的在于利用公共通信网络设施在某一相同的安全策略下将具有某种公共利益的网络和/或主机连接成一个可管理的“自己”的专用网络。这样一种“自己专用”的网络，勿需花钱投资建立和维护远程通信线路和网络设备，同时可在一定程度上对穿过公共通信区域（这是一个充满危险的互不信任的环境）的数据内容保持隐蔽性。这就是说，我们可以利用 VPN 技术在公共通信网络基础设施中“虚拟”出一组织机构内或某种共同体内通信的某些部分，在利用公共基础设施资源（带宽、中继或转发设备等）效率的同时，使通信的部分或全部在外部观察者看来是“不可见的”。

显然，推动 VPN 迅速发展的首要原因是网络通信方式变革带来的经济利益。这是因为当前的通信系统具有这样的特征：通信基础设施的组件固定成本高，而传输容量或带宽也高，显然将大量分离的通信服务捆扎到一个共同的高容量通信平台上，可以将通信平台有关的组件的固定高成本分摊在大量客户上，这在服务供应商（SP）看来是一件划算的事；另一方面，在网络用户看来，通过公共通信服务平台上实施虚拟专用网又比自建独立的小型物理通信服务设施更为便宜，显然这是一个服务供应商与网络用户“双赢”的网络方案。推动 VPN 迅速发展的第二个原因是虚拟的专用网通信与因特网通信相比具有隔离和隐蔽的保密性，如果进一步采取相应的安全措施（例如采用加密隧道或隧道技术与密码技术组合等），就可以构成起安全的网络平台。

VPN 作为一种组网技术概念，本身并不是一个具有“固定”形态的实体。由于这样一种技术具有上述的两种独特优势，对于企事业单位、党政机关、金融系统等跨地域组建“自己专用”的网络提供了经济能力可承受且相对安全的技术手段。可以预见，这将是企事业单位、党政机关、金融系统等组成内联网、外联网和实现远程接入网的基本的、主要的方法，与此同时各种 ISP 也必将投入更大的力量，为各种用户提供 VPN 服务。

1.4 VPN 的应用领域

利用 VPN 技术几乎可以解决所有利用公共通信网络进行通信的虚拟专用网络连接的问题。归纳起来，有以下几种应用领域。

1.4.1 远程访问

远程移动用户通过 VPN 技术可以在任何时间、任何地点采用拨号、ISDN、DSL、移动 IP 和电缆技术与公司总部、公司内联网的 VPN 设备建立起隧道或密信道，实现访问连接，此时的远程用户终端设备上必须加装相应的 VPN 软件。推而广之，远程用户可与任何一台主机或网络在相同策略下利用公共通信网络设施实现远程 VPN 访问。这种应用类型也叫 Access VPN（或访问型 VPN），这是基本的 VPN 应用类型。不难证明，其它类型的 VPN 都是 Access VPN 的组合、延伸和扩展。

1.4.2　组建内联网

一个组织机构的总部或中心网络与跨地域的分支机构网络在公共通信基础设施上采用隧道技术和密码技术等 VPN 技术构成组织机构“内部”的虚拟专用网络，当其将公司所有权的 VPN 设备配置在各个公司网络与公共网络之间时，这样的内联网还具有管理上的自主可控、策略集中配置和分布式安全控制的安全特性。利用 VPN 组建的内联网也叫 Intranet VPN。Intranet VPN 是解决内联网结构安全和连接安全、传输安全的主要方法。

1.4.3　组建外联网

使用虚拟专用网络技术在公共通信基础设施上将合作伙伴或有共同利益的主机或网络与内联网连接起来，根据安全策略、资源共享约定规则实施内联网内的特定主机和网络资源与外部特定的主机和网络资源的相互共享，这在业务机构和具有相互协作关系的内联网之间具有广泛的应用价值。这样组建的外联网也叫 Extranet VPN。Extranet VPN 是解决外联网结构安全和连接安全、传输安全的主要方法。当外联网 VPN 的连接和传输中使用了密码技术，必须解决其中的密码分发、管理的一致性问题。