第 5 章 虚拟专用网技术

防火墙可以对进出网络的信息和行为进行控制，将用户内部可信任的网络与外部不可信任的网络隔离。然而，越来越多的企业在全国乃至世界各地建立分支机构并开展业务。随着办公场地和分支机构的分散化以及日渐庞大的移动办公群体的出现，分散在不同地点的企业也需要考虑安全传输问题。虚拟专用网(Virtual Private Network，VPN)技术应运而生，既可以实现企业网络的全球化，又能最大限度地利用公共资源。

本章主要内容：

- VPN 概述。
- VPN 的类型。
- 数据链路层 VPN 协议。
- 网络层 VPN 协议。
- 传输层 VPN 协议。
- 会话层 VPN 协议。

5.1 VPN 概述

局域网一般由某个企业拥有并管理，可以通过防火墙设置统一的安全管理策略，对进出局域网的信息和行为进行控制，将用户内部可信任的网络与外部不可信任的网络隔离。因此，相对于开放的 Internet，在局域网传输企业内部机密信息具有较高的安全性。

随着经济全球化进程的日益加快，VPN 技术应运而生。有了 VPN，移动用户在路途中也可以利用 Internet 或其他公共网络对内部服务器进行远程访问。从用户的角度看，VPN 就是在用户计算机(即 VPN 客户机)和 VPN 服务器之间点到点的连接，由于数据通过一条仿真专线传输，用户感觉不到公共网络的实际存在，能够像在专线上一样处理内部信息。因此，VPN 不是真正的专用网络，却能够实现专用网络的功能。

5.1.1 VPN 的概念

一个企业可能在多个地点存在分支机构，并且相互之间经常需要通过 Internet 传输机密信息。当员工出差在外时，可能需要通过 Internet 访问公司内部网络的保密数据。对于这些情况，如何才能保证数据在传输过程中不被窃听、不被篡改、不会丢失呢？要实现这一

点有两种方法。

第一种方法是建立自己的专用网络，即将不同地区的各个局域网直接用专线连接，局域网和专线使用权完全属于本企业，有较高的安全性。但这种方法在我国难以实施，因为企业没有路权，不能私自开挖道路并铺设通信电缆或光缆。另外，架设专线非常昂贵。例如，我国铁路企业沿铁轨两侧有一定范围的路权，因此可以铺设铁路通信专线，即铁通网络的前身，但其专用网络耗资 600 余亿元。显然，这对于绝大多数企业来说并不现实。

第二种方法是通过专用隧道技术在公共网络上仿真一条点到点专线，从而达到信息安全传输的目的，这就是 VPN。VPN 在公共网络中传递只有内部网关才能解密的加密信息，从而在不同地区内部网关两两之间都形成一条端到端的加密隧道，这样不用实际铺设专线，也可以实现在全球范围内将内部网络连通并保证传输安全的目的。

与长途拨号及长途专线服务相比，使用 VPN 只需要本地 ISP（Internet Service Provider，Internet 服务提供商）提供正常的 Internet 接入服务，其成本也低廉得多。

5.1.2　VPN 的组成与功能

VPN 的组成如图 5.1 所示。VPN 客户机（如移动用户）通过本地 ISP 连接公共网络（如 Internet），经企业内部 VPN 服务器认证后，就可以建立一条跨越公共网络的安全连接，实现与企业其他地区分支机构内部网络之间安全的通信。

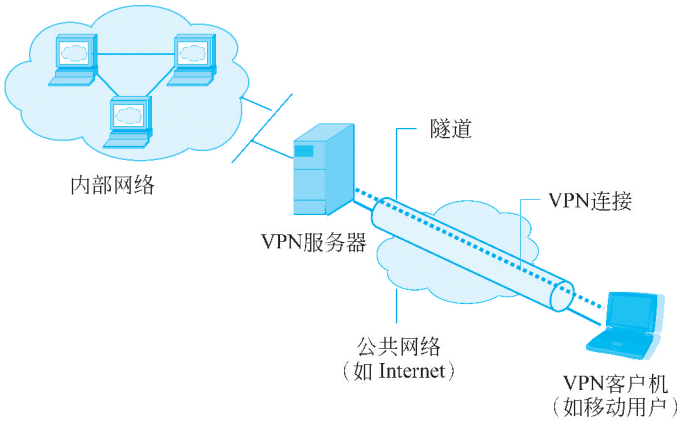

图 5.1　VPN 的组成

VPN 的主要功能如下：

- 数据封装。VPN 技术提供带寻址报头的数据封装机制。
- 认证。VPN 连接中包括两种认证方式——单向认证和双向认证。单向认证是指在 VPN 连接建立之前，VPN 服务器对请求建立连接的 VPN 客户机进行身份认证，核查其是否为合法的授权用户。如果使用双向认证，还需进行 VPN 客户机对 VPN 服务器的身份认证，以防伪装的非法服务器提供错误信息。
- 数据完整性和合法性认证。检查链路上传输的数据是否出自源端以及在传输过程中是否被篡改。VPN 链路中传输的数据包含密码检查，密钥只由发送者和接收者双方共享。
- 数据加密。数据由发送者加密，由接收者解密，以确保其在公共网络上的传输安全。

加解密过程要求发送方和接收方共享密钥。

如果不掌握密钥，即使数据包被截取，也难以识别。密钥长度是一个重要的安全参数。密钥通常可以由多种加密算法综合而成。密钥长度越大，破解的难度也就越大，因此使用最大可能长度的密钥对于确保数据安全是非常关键的。

同一密钥不能长期使用，必须定期更换，因为使用同一密钥加密的信息量越大，破解也就越容易。因此常常有必要在一次连接中使用不同的密钥。

5.1.3 隧道技术

VPN 技术可以在多个层次上实现，其核心是隧道技术，在公共网络中将用户的数据封装在隧道里进行传输。隧道技术与接入方式无关，可以支持各种形式的接入，如拨号、电缆调制解调器、xDSL、ISDN、专线甚至无线接入等。隧道协议一般包括以下几方面：

- 乘客协议。即被封装的协议，如 PPP、Ethernet 等。
- 封装协议。负责隧道的建立、维持和断开，如 PPTP、L2TP、GRE、IPSec 等。
- 承载协议。承载经过封装后的数据包的协议，如 IP、ATM 等。

Internet 上最常见的隧道协议主要有第二层隧道协议和第三层隧道协议，它们的区别主要在于用户数据在网络协议栈的第几层被封装。

- 第二层隧道协议（如 PPTP、L2TP 等）主要用于实现拨号 VPN 业务。
- 第三层隧道协议（如 IPSec 等）主要用于实现专线 VPN 业务。

本章后面将详细介绍各层的 VPN 协议。

表 5.1 以 OSI 参考模型和 TCP/IP 模型为参照，列出了 VPN 技术的实现层次。

表 5.1 VPN 技术的实现层次

OSI 参考模型	TCP/IP 模型	VPN 技术协议	OSI 参考模型	TCP/IP 模型	VPN 技术协议
会话层		SOCKS v5	网络层	网络层	IPSec，MPLS，GRE
传输层	传输层	SSL	数据链路层	数据链路层	PPTP，L2TP

5.1.4 VPN 管理

如同其他网络资源一样，VPN 也必须得到有效的管理。对 VPN 的管理可以从以下 5 方面加以考虑。

1. 用户管理

一般来说，不允许同一个用户同一时刻在不同的服务器上拥有不同的账号。为此，大多数 VPN 网络管理的做法是在主域控制器（Primary Domain Controller，PDC）或远程身份认证拨号用户服务（Remote Authentication Dial-In User Service，RADIUS）服务器上建立主账号数据库，以便 VPN 服务器对某中心认证设备发送认证信任状态。同一个用户账号既可用于拨入远程访问，也可用于基于 VPN 的远程访问。

2. 地址和域名服务器的管理

VPN 服务器必须有可供使用的 IP 地址，以便在连接建立过程中的 IP 控制协议协商阶段将这些 IP 地址分配给 VPN 服务器的虚拟接口和 VPN 客户机。分配给 VPN 客户机的

IP 地址也就是分配给 VPN 客户机虚拟接口的 IP 地址。VPN 服务器还必须配置 DNS 和 WINS 地址，并在协商时将这些地址赋给 VPN 客户机。

3. 认证管理

VPN 服务器在配置时可选择 Windows 或者 RADIUS 提供认证。如果选择 Windows，则由 Windows 认证机制对请求建立 VPN 连接的用户进行身份认证。如果选择 RADIUS，则用户发出的连接请求和身份参数将作为一系列请求消息流发送至 RADIUS 服务器。

RADIUS 服务器接收到来自 VPN 服务器的用户连接请求后，利用它的认证数据库认证用户身份。另外，RADIUS 服务器上通常还备有一个记录用户其他特性的数据库。这样，对于认证请求，RADIUS 服务器除了作出是与否的判断外，还可向 VPN 服务器提供该用户的其他连接参数，诸如允许的最大连接时间和静态 IP 地址等。

RADIUS 服务器对认证请求作出的回应既可以基于它自己的数据库，也可以通过 ODBC(Open DataBase Connectivity，开放式数据库互连)访问其他数据库。此外，RADIUS 服务器还可作为客户代理访问远程 RADIUS 服务器。

4. 日志管理

VPN 服务器在配置时可选择 Windows 或者 RADIUS 提供记账管理。如果选择 Windows，则账目信息累计在 VPN 服务器上以供日后分析。如果选择 RADIUS，RADIUS 账目信息将发送至 RADIUS 服务器以供累计和分析。

大多数 RADIUS 服务器可以配置成将认证请求记录写进记账文件中。有不少第三方软件商提供记账和审核软件包，可以分析 RADIUS 账目信息，然后生成各种报表。

5. 网络管理

假定安装了简单网络管理协议(SNMP)，那么在 SNMP 环境中，VPN 服务器可作为 SNMP 代理，将管理信息记录在 SNMP 的对象标识中，并通过专用的网络管理软件进行监控、管理。

5.2 VPN 的类型

按照不同的用途，VPN 可以分为 3 类：

- 内联网 VPN。在机构的各个分支机构之间建立的 VPN。
- 远程访问 VPN。在分支机构与远地员工等移动用户之间建立的 VPN。
- 外联网 VPN。在某个机构与其他相关业务单位、合作伙伴等之间建立的 VPN。

5.2.1 内联网 VPN

内联网 VPN 是通过公共网络(如 Internet)将一个组织的各分支机构的局域网连接而成的网络。这种类型的局域网到局域网的连接带来的风险最小，通常认为一个机构自己的分支机构是可信的。这种方式连接而成的 VPN 被称为内联网 VPN，可把它作为企业的中心网络进一步扩展。如图 5.2 所示，两个局域网分别设置了 VPN 服务器，VPN 服务器之间形成信息传输隧道，以保证在隧道中信息传输的机密性。

采用这种类型的 VPN 能够有效地保证重要数据流经 Internet 时的安全性，即中心局域网和各分支机构局域网能够进行安全的通信。

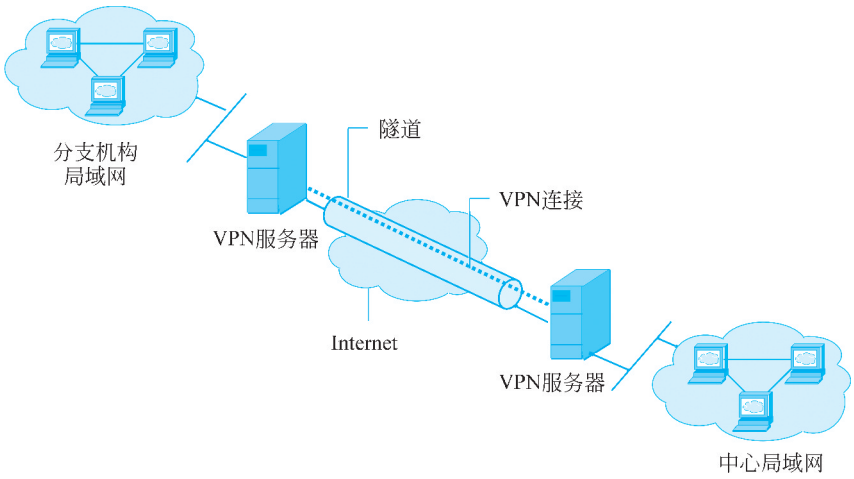

图 5.2　内联网 VPN 连接

VPN 服务器的主要功能如下：

- 认证用户的身份。保证只有合法用户才能通过 VPN 隧道进行数据访问。
- 信息加密。VPN 服务器之间形成加密隧道，保证信息传输的机密性。

5.2.2　远程访问 VPN

传统情况下，远程访问用户（如在外出差的员工）必须使用长途拨号，通过内部局域网的访问服务器进入内部网络进行访问，这种方法存在较大的缺陷：

- 必须使用长途电话，费用较贵，并且使用不方便。
- 绕开了防火墙的控制，留下安全隐患。内部网络的服务器还必须增加拨号访问内部网络的方式，这与防火墙作为内部网络和外部网络之间唯一关口的思路相违背，极易产生安全问题。

远程访问 VPN 则首先由远程用户通过其当地的 ISP 连接到 Internet，然后再通过 Internet 访问内部局域网。这种基于 Internet 的 VPN 连接充分利用了 Internet 的全球连接性，为远程用户免去了高昂的长途费用，并具有较好的安全性。其连接如图 5.3 所示。

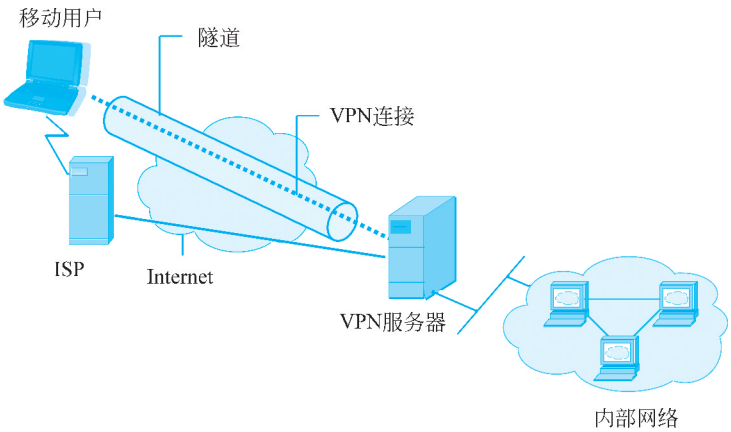

图 5.3　远程访问 VPN 连接

远程用户利用本地 ISP 提供的 VPN 服务启动一条 VPN 连接，然后通过 Internet 与 VPN 服务器相连，从而实现远程用户和内部网络之间安全的信息交互。这种方式尤其适用于移动用户。

在 Windows 2000 之前的操作系统没有内置 VPN 端，需要采用专门的 VPN 客户端软件，如 FortiClient 等。图 5.4 是在 FortiClient 中建立的 3 个 VPN 入口，其中名称为 taxi 的 VPN 已经连接成功，处于启动状态。

图 5.4　VPN 客户端连接

5.2.3　外联网 VPN

外联网 VPN 为企业机构的合作伙伴、相关职能单位提供安全的网络连接。其连接如图 5.5 所示。

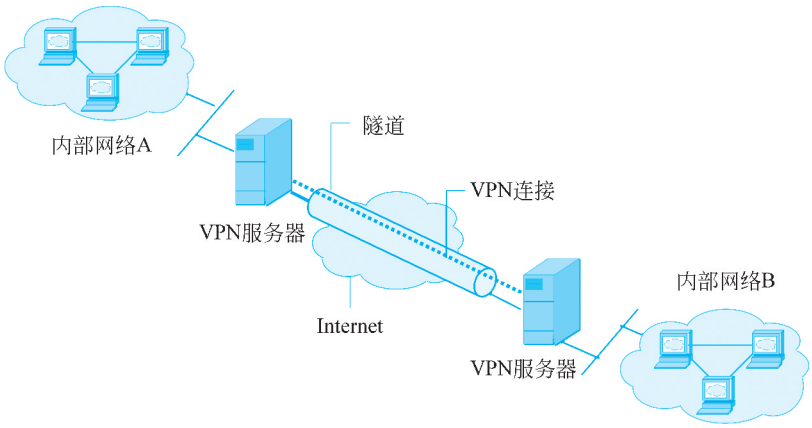

图 5.5　外联网 VPN 连接

外联网 VPN 应能保证包括 TCP 和 UDP 服务在内的各种应用服务的安全，例如 Email、HTTP、FTP、RealAudio、数据库的安全以及一些应用程序（如 Java、ActiveX）的安全。因为不同系统的网络环境可能不同，外联网 VPN 方案应能够适用于各种操作平台、协议、认证方案及加密算法。

外联网 VPN 的主要目标是保证数据在传输过程中不被修改，保护网络资源不受外部威胁。安全的外联网 VPN 要求系统在同它的合作伙伴、相关职能单位之间经 Internet 建立端到端的连接时必须通过 VPN 服务器才能进行。在这种系统中，网络管理员可以为合作伙伴的员工指定特定的许可权，例如可以允许对方一定级别的管理人员访问一个受到保护的服务器上的文件等。

外联网 VPN 是一个由加密、认证和访问控制功能组成的集成系统。通常，将 VPN 服务器放在一个不能穿透的防火墙隔离层之后，防火墙阻止所有来历不明的信息传输。所有经过过滤后的数据通过唯一的入口传到 VPN 服务器，VPN 服务器再根据安全策略进一步过滤数据。

VPN 可以建立在网络协议的上层（如应用层），也可建立在较低的层次（如网络层）。在应用层的 VPN 可以用代理服务器实现，即不直接打开任何到内部网络的连接，从而防止 IP 地址欺骗。所有访问都要经过代理服务器，网络管理员就可以知道谁曾企图访问内部网络以及做了多少次尝试。

外联网 VPN 并不假定连接的不同企业的系统之间存在双向信任关系。外联网 VPN 在 Internet 内建立一条隧道，并保证经包过滤后信息传输的安全。外联网 VPN 应该用高强度的加密算法，密钥应尽可能地长。此外，外联网 VPN 应支持多种认证方案和加密算法，因为其他系统可能有不同的网络结构和操作平台。

外联网 VPN 应能够根据尽可能多的参数控制对网络资源的访问，参数包括源地址、目的地址、应用程序的用途、使用的加密和认证类型、个人身份、工作组、子网等。网络管理员应能够对个人用户进行身份认证，而不仅仅根据 IP 地址进行判断。

5.3 数据链路层 VPN 协议

数据链路层 VPN 协议主要包括点对点隧道协议（Point-to-Point Tunneling Protocol，PPTP）和第二层隧道协议（Layer 2 Tunneling Protocol，L2TP），它们是 IPSec 出现前最主要的 VPN 类型，至今仍然被广泛使用，通常用于支持拨号用户远程接入企业或机构的内部 VPN 服务器。

5.3.1 PPTP 与 L2TP 简介

PPTP 是一种支持多协议 VPN 的网络技术，它可以使远程用户通过 Internet 安全地访问内部网络。通过 PPTP，远程用户可以通过 Windows XP、Windows Vista 等操作系统以及其他支持点对点协议（Point-to-Point Protocol，PPP）的系统拨号连接到 Internet 服务提供商，再通过 Internet 与其内部网络连接。

PPTP 工作在 OSI 参考模型的第二层（数据链路层），它在所有通信流之上简单地建立

了一条加密隧道。PPTP 已被嵌入 Windows 98 以后的各种微软公司操作系统中，用于微软公司产品的路由和远程访问服务。

还有一些厂家也做了许多开发工作，例如 Cisco 公司开发的 L2F(Layer 2 Forwarding，第二层转发)隧道协议。

微软、Cisco、Ascend、3COM、Bay 等厂商将 L2F 与 PPTP 融合，产生了 L2TP，并于 1999 年 8 月公布了 L2TP 的标准——RFC 2661。L2TP 和 PPTP 十分相似，L2TP 部分采用了 PPTP，两个协议都允许用户通过公共网络建立安全隧道。L2TP 还支持信道认证，但它没有规定信道保护的方法。

PPTP 和 L2TP 有以下优点：

- PPTP 和 L2TP 最大的优点是简单易行，特别是对使用微软公司操作系统的用户来说更为方便，因为微软公司已把它作为路由软件的一部分。
- PPTP 和 L2TP 位于数据链路层，包括 IPv4 在内的多个网络协议可以采用它们作为链路协议，以支持流量控制。
- PPTP 和 L2TP 通过降低丢包率减少重传，改善网络性能。

PPTP 和 L2TP 的缺点如下：

- PPTP 和 L2TP 对 PPP 本身并没有做任何修改，只是将用户的 PPP 帧基于 GRE 封装成 IP 报文。在两台计算机之间创建和打开数据通道。一旦通道打开，源和目的用户身份就不再需要，这样可能带来问题。
- PPTP 和 L2TP 不对两个节点间的信息传输进行监视或控制。
- PPTP 和 L2TP 限制同时最多只能连接 255 个用户，可扩展性不强，且不适合向 IPv6 转移。
- 端用户需要在连接前人工建立加密信道。
- 没有提供内在的安全机制，认证和加密受到限制，没有强加密和认证支持。
- 不支持企业与外部客户以及供应商之间会话的保密性需求，不支持外联网 VPN。

安全性低是 PPTP 和 L2TP 最大的弱点。因此，PPTP 和 L2TP 最适合用于客户远程访问 VPN，而对于安全要求高的内部信息，用 PPTP 和 L2TP 传输与用明文传输的差别并不大。

5.3.2　VPN 的配置

随着使用 VPN 服务的用户稳定增加，微软公司自 Windows 2000 起，已经将其功能集成到操作系统内。在“网络连接”中选择“创建一个新的连接”，出现新建连接向导。首先选择网络连接类型，此处选择“连接到我的工作场所的网络”单选按钮，如图 5.6 所示。然后根据提示依次完成接下来的各个步骤，如图 5.7～图 5.10 所示。

在图 5.9 所示的界面中，可以根据用户当前连接 Internet 的情况选择“不拨初始连接”单选按钮(已提供了网络接入的场合)或者“自动拨此初始连接”单选按钮(从下拉列表中选择设定的初始连接)。若选择“自动拨此初始连接”，可以在图 5.10 所示的界面中输入要连接的 VPN 服务器名称或 IP 地址，然后，单击“下一步”按钮就可以完成 VPN 连接的建立。下面将对该连接的属性进行配置(若选择“不拨初始连接”，可直接进入这一步)。

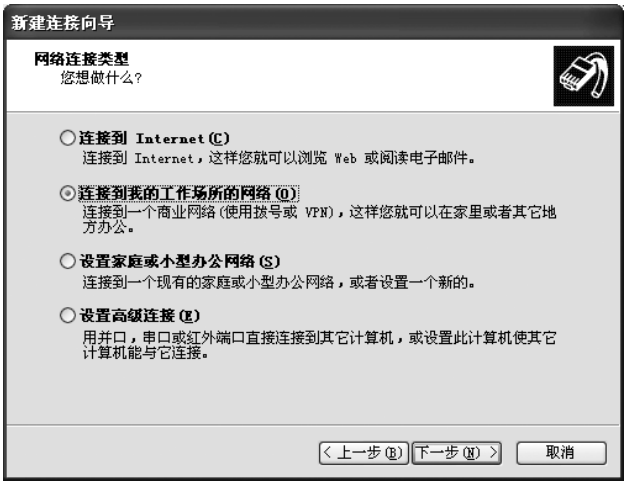

图 5.6　选择新建连接的类型

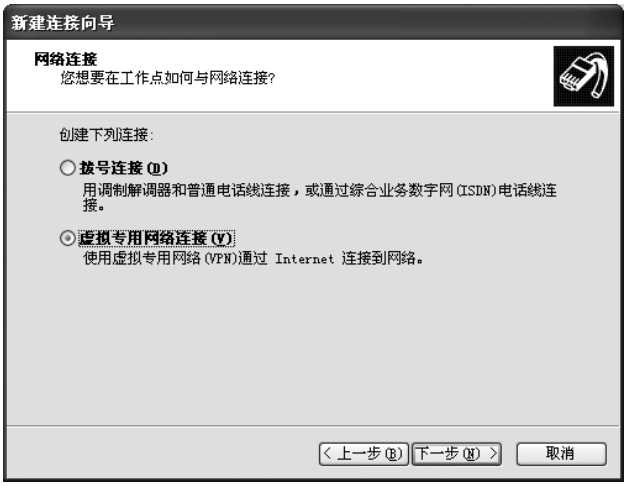

图 5.7　选择连接方式

图 5.8　指定连接名称

图 5.9　建立到公用网络的初始连接

图 5.10　指定 VPN 服务器的名称或 IP 地址

首先，输入用户名和密码，如图 5.11 所示。

图 5.11　输入用户名和密码

设置 VPN 属性要选择“Internet 协议(TCP/IP)”复选框，如图 5.12 所示。一般 VPN