# VPN 技术与解决方案

王海军 王中心 周庆民 成 强 云惠芳 (河南省科学院应用物理研究所 450008)

**摘要**: 本文对 VPN(Virtual Private Network)的概念、分类及常用技术作了基本介绍和评述,并以 Windows NT 为例,介绍了 VPN 的实际实现方案。

**关键词**:虚拟专用网(VPN) 点到点隧道协议(PPTP) 因特网(Internet) 数据安全

在当今的各种新兴网络技术中,虚拟专用网(VPN, Virtual Private Network)无疑是一个十分热门的话题,一批软、硬件公司先后开发并推出了多种平台下的 VPN 解决方案以及相关的产品。随着近年来 Internet 爆炸式的增长,VPN 技术的发展很快,为 Intranet, Extranet 的建设,以及电子商务的发展提供了新的技术解决方案。人们对 VPN 的关注基于它几种令人满意的特性:通过 Internet 进行安全传输,能够节省长途话费的支出,不需专用的连接线路等。人们又对 VPN 的安全、性能、价格等方面有不少疑问和误解,这很正常,因为毕竟 VPN 是一种很新的网络技术,相对于诸如租用线路、帧中继、ISDN、拨号服务等传统实现方法,VPN 技术则提供了一种利用开放的 Internet 主干网优势的全新的解决方案。VPN 可供选择的技术方案和应用平台很多,在安装、配置、管理、费用等方面差异很大,给选择和应用带来很大的困难,关键在于应当尽快熟悉并掌握这方面的技术,在实际的应用中开展相关业务。

## 一、VPN 的概念

从广义上讲,传输媒介并不限于 Internet,也包括帧中继、ATM 网络等,但通常而言,VPN 指的是利用开放、公共、不设防的 Internet 作为基本传输介质,通过安全网络协议,形成专用的虚拟链路,在网上传送 IP 数据包,能够为最终用户提供类似于通常专用网络性能的网络服务技术。由于是在 Internet 上传送 IP 数据包,这种 VPN 通常还称作 Internet - VPN 或 IP—VPN,但现在提到 VPN 即是上面所述的概念。

事实上,VPN 的效果相当于在 Internet 上形成一条虚拟专用线路,这条专线通常称为隧道(tunnel),从作用和效果看,VPN 与 IP 电话类似,但 VPN 对于加密的要求则很高。VPN 由三个部分构成:隧道技术、用户认证和数据加密。隧道技术定义数据的封装形式,并利用 IP 协议以安全方式在 Internet 上传送。后两者则包括安全性的两个方面:用户认证确保未获认证的用户无法访问网络,数据加密则保证敏感数据不会被盗取。

从理论上说,VPN 能够充分利用 Internet 公共骨干网的优势,节省广域网的建设和运行维护费用,加快企业网的建设步伐,提高用户网络运营和管理的灵活性。同时,由于有认证、加密、授权等多种安全机制,能有效鉴别和过滤访问者并保证数据完整性,使得网络可靠且安全。然而,VPN 目前实施的是 PPP 配置,而且方案来自多个厂家,VPN 仅能部分满足企业网络的需要,难以适应多种类型的企业体系结构。

## 二、VPN 的分类

目前业界各大公司都推出各自的 VPN 解决方案和产品,各家的产品侧重不同,采用的 VPN 技术和实施方案也不尽相同。以下介绍几家主要厂商的方案分类:

1. Cisco 公司把 VPN 分为三类

(1) 接入 VPN(Access VPN);

(2) 内部网 VPN(Intranet VPN);

(3) 外部网 VPN(Extranet VPN)。

2. IBM 公司也把 VPN 分为三类

(1)商业伙伴 / 供应商网络(Business Partner / Supplier Network);

(2)分支办公室联结网络(Branch Office Connection Network);

(3)远程接入网络(Remote Access Network)。

3. 3Com 公司则分为两种

(1) ISP / NSP VPN;

(2) 企业 VPN。

4. Ascend 公司的 Multi VPN 分为三个部分

(1) 虚拟远程专用网(Virtual Private Remote Network);

(2) 虚拟专用中继(Virtual Private Trunking);

(3) 虚拟 IP 路由(Virtual IP Routing)。

5. Microsoft 的 Windows NT4.0 提供 RAS 支持 PPTP

提供 PPTP 协议及 PPTP 过滤,,还提供了认证协议和数据加密。

不论怎样划分,由于 VPN 属于广域网范畴,VPN 都可归结为专用 VPN 和拨号 VPN 两大类。专用 VPN 利用了公共 Internet 的物理网络资源,以及与 Internet 互联的 NSP/ISP 提供的具有非连接特征的网络的物理资源,用于满足企业 Intranet 的 WAN 扩充。拨号 VPN 则常常利用公共电话网(PSTN)和综合业务数据网(ISDN)的物理资源,满足远程用户的访问需要。由于专用 VPN 通常对于性能、实时和服务质量(QoS)有着较为严格的要求,相对而言,不很适合采用 VPN,而拨号 VPN 作为 RAS (Remote Access Service)的一种,特别适合采用 VPN,它有以下特点:

(1) 位置众多,尤其适合单独移动用户和远程办公站点;

(2) 分布广泛,彼此之间距离较远,不需建立永久连接;

(3) 要求不高,对于带宽和时延没有很严格的限制。

## 三、VPN 的常用技术

正如上面所述,Internet 上的安全的 VPN 指明了 VPN 的两个基本特点,或基本要求:一是安全网络协议,二是安全保证协议。这也正构成了 VPN 技术的两个方面。

大多数 VPN 的解决方案均集中于建立 IP 隧道,IP 隧道的生成不需占用预定的通信信道,是可以控制和管理的。目前常用的支持隧道技术的协议有两种:PPTP (Point to Point Tunneling Protocol)和 L2TP(Layer Two Tunneling Protocol),它们是 IETF 的国际标准。IP 隧道的建立方法是将不同的网络层协议(如 IP、TPX 等)封装在 PPP 数据包中,再采用双层封装的方法将数据包封装在 IP 隧道协议里,仍然作为 IP 包出现,并作为普通 IP 包在 Internet 上进行传输。

大多数 VPN 产品采用 IETF 的 IPSec(IP Security)解决安全性的保密问题。IPSec 是基于第三层的安全技术,通过身份认证,集成检验和数据加密三条途径来保证安全,常用的有 ESP,DES 和 3×DES 等。ESP 即包封安全有效负荷(Encapsulating Security Payload),属第三层协议,是将网络层协议直接装入隧道协议中,并将所形成的数据依靠第三层协议进行传输,DES(Data Encryption Standard)是常用的 56 位加密标准,3×DES(Triple DES)则将加密位数扩大为 168 位。在用户身份验证方面,RADIUS(Remote Authentication Dial－ In User Service)仍是常用标准解决方法,它是一个维护用户配置文件的数据库,通过跟踪用户名、口令、隧道类型、会话起止时间及传输的数据和字节数量等,登录用户拨入会话信息进行用户认证。

## 四、VPN 的选择

VPN 产品通常基于以下四种平台:路由器、防火墙、网络操作系统和专用硬件(如交换机)设备,各种平台下采用的加密算法和认证系统各有特点,一般应仔细关注以下几个方面:

1. 兼容性能和可互用性。VPN 应与主要操作平台、网络设备、应用程序等有良好的兼容性,避免进行交叉升级,并保证网络运行状况不变。

2. 安全加密保证。VPN 对安全要求很高,广泛采用的、符合业界标准的安全保证方案有助于保持较高的安全等级。

3. 可用性。不同的 VPN 方案提供的网络服务质量(QoS)等级和程度差别很大,不同企业体系结构的要求也有很大差异。

4. 管理措施。VPN 通信要求较强的管理和控制能力,与现行管理平台集成的综合管理平台可大大减少管理业务数量,VPN 网管信息自身的安全和保护甚至更重要。

5. 费用。不同平台下的方案费用差异巨大,应考虑的还有其他设备的升级费用,实际运营费用等综合成本的增加。

实际选择中要考虑的问题或许更复杂,首先应明晰自身的网络基本设施和应用环境需要,注重各自不同环境下最为迫切需求的因素,再对具体的方案和产品进行分析比较。必须指出的是,由于 VPN 技术正在迅速发展之中,真正实施应用的方案还很有限,也许无法找出理想的解决方案。

## 五、VPN 的实施

由于 Internet 上通信质量和限制,专用 VPN 只有在区域性较好的高速通信主干道上会有一定程度的良好实现,在现有技术成熟程度和网络质量状况下,我们认为,只有拨号 VPN 有较为满意的应用结果,从费用、兼容性、易用性等方面考虑,基于网络操作系统的 VPN 也许是最理想的,以下简单介绍 Windows NT 下的实施方法:

1. PPTP 服务器的安装与设置

PPTP 允许利用 Internet 从任何地方对 RAS 的安全连接，采用两步进程进行：首先，客户机通过本地 ISP 连接到 Internet 上，然后，利用客户机上的 PPTP 服务，使之与网上的 RAS 服务器加密连接。以下从硬件和软件两方面说明配置方法。

(1)硬件设备连接：

①网卡。PPTP 服务器必须有两块网卡，一块连接公司的内部网络，一块连接 Internet，且须有向 NIC 申请的全球唯一的、合法的 IP 地址。

②多端口串行适配器。RAS 最多可支持 256 个连接，必须增加多端口适配器增加计算机串行端口，它安装在计算机内部，有多个连接插口。

③Modem 池。RAS 虽然支持 PSTN、ISDN、X.25 三种连接方式，但通常都采用模拟 Modem 作为接入设备。

以上硬件设备在选购时应选用 NT 支持的 HCL (Hardware Compatibility List)中的设备，若不在 HCL 中，则须由厂家提供相应的 NT 驱动程序。

(2)软件部件设置：

①采用通常方式安装多端口串行适配器、Modem 和 RAS。

②配置 RAS 协议。由于 NetBEUI 协议简单、高效、开销小、配置简单，且在 LAN 中应用较广，Microsoft 建议采用 NetBEUI 协议构成 RAS 服务器的连接。配置方法：选择 Control→ Panel Network → Services 选项，选择所用协议及访问范围。

③为 RAS 配置 PPTP。操作方法：选择 Control Panel → Network → Protocols 选项，增加 Point to Point Tunneling Protocol，设置 VPN 的数量，并从列表中选择 VPNn - RASPPTPM。

④加入 VPN 设备。VPN 设备作为虚拟设备应与其他物理设备(如 Modem)一样加入到 RAS 中，操作方法：选择 Control Panel → Network → Services 选项，逐个将 RAS 可用设备项下的 VPNn - RASPPTPM 设备加入到 RAS 中。

⑤配置 VPN 端口。每个 VPN 虚拟设备同样应配置端口功能，PPTP 服务器通常应选择 Dial out and Receive Calls 选项或 Receive Calls Only 选项。

⑥设置 RAS 访问权限。通过 Administrative Tools → Remote Access Admin 或 User Manager for Domains 中的 Dialin 设置拨入权限，确保仅仅授权用户可以访问网络，并且与 Windows NT 的 NTFS 文件权限结合限定每个用户的访问权限。

⑦设置认证协议。客户机和服务器交换用户名和口令的方法称为认证协议，RAS Server 支持拨入连接的 PPTP 并支持三种认证协议，在以上配置 RAS 协议时，应选择 Require Microsoft encrypted authentication 选项，并设置 Require data encryption。这是缺省的最高选取项，要求客户机必须选用 MS - CHAP(Microsoft Extension to Challenge Handshake Authentication Protocol)加密口令(RSA MD4 算法)，并对交换数据进行加密。

⑧设置 PPTP 过滤。PPTP 过滤只让 PPTP 包通过，而拒绝其他信息包，增强了 PPTP 服务器的安全性。设置方法：选择 Control Panel → Network → Protocols 选项，选中 Enable PPTP Filtering，并选择 Enable Security 对相应项目进行设置。

2. PPTP 客户机的配置

PPTP 客户机的配置与服务器端完全对应，硬件连接与常规 RAS 客户机一样采用 Modem，基于 Windows NT 的 PPTP 客户机软件配置与服务器端相对应，但须注意以下问题：

(1)PPTP 客户机不进行以上 RAS 访问权限和 PPTP 过滤的设置，这两项安全项目由 PPTP 服务器完成。

(2)端口配置应选择 Dial out only 或 Dial out and Receive calls 选项。

(3)VPN 虚拟设备和 Modem 作为两个拨号设备分别进行设置。

(4)认证协议必须与服务器端对应，以保证通信正常和网络安全。

Windows 95 客户机则须升级才可作为 PPTP 客户机使用，Windows 98 支持 PPTP 可作为 PPTP 客户机使用，其他客户机操作系统不支持 MS - CHAP，安全性无法保证，不宜作为 PPTP 客户机。

这里网络协议采用的是 NetBEUI，配置较为简单，若内部网采用 TCP/IP 协议或 NWLink 协议，则须进行地址分配、路由启动、增添静态路由等内部连接的设置。

## 六、VPN 方案评述

1. 基于网络操作系统的 PPTP 方案有兼容性好，使用方便，配置简单，价格低廉的优点，但性能和可靠性不高。

2. 基于软件的口令和数据加密方法速度较慢，保密性能总体上与硬件加密设备有较大差距。

3. 客户操作系统要求须支持 MS - CHAP 的 Windows 系列操作系统，限制了客户机操作系统的选择。

(来稿时间：1999 年 5 月)