基于VPN技术的企业管理信息系统的开发

The Develop of MIS Based on VPN

摘　要：本文简述了VPN的概念及其基本原理，详细说明了VPN技术在企业组网中的优势及应用VPN技术设计企业网络的原则,并作为实际应用介绍了神华准格尔能源有限责任公司基于VPN管理信息系统的开发实践。

关键词：虚拟专用网　管理信息系统　网络安全

邵良杉　（辽宁工程技术大学系统工程研究所　123000）

1 引言

VPN（Virtual Private Networking）即虚拟专用网,指在公共网络中建立专用网络，数据通过安全的“加密通道”在公共网络中传播。企业只需要租用本地的数据专线，连接上本地的Internet，各地的机构就可以互相传递信息；同时，企业还可以利用Internet的拨号接入设备，让自己的用户拨号到Internet上，就可以连接进入企业网中。建立基于VPN的企业管理信息系统具有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等优点，将会成为今后企业管理信息系统发展的趋势。

"虚拟"的概念是相对传统私有网络的构建方式而言的。对于广域网连接，传统的组网方式是通过远程拨号连接来实现的，而VPN是利用服务提供商所提供的公共网络来实现远程的广域连接。通过VPN，企业可以以明显更低的成本连接它们的远地办事机构、出差工作人员以及业务合作伙伴。VPN在网络中拓扑示意图如1所示。

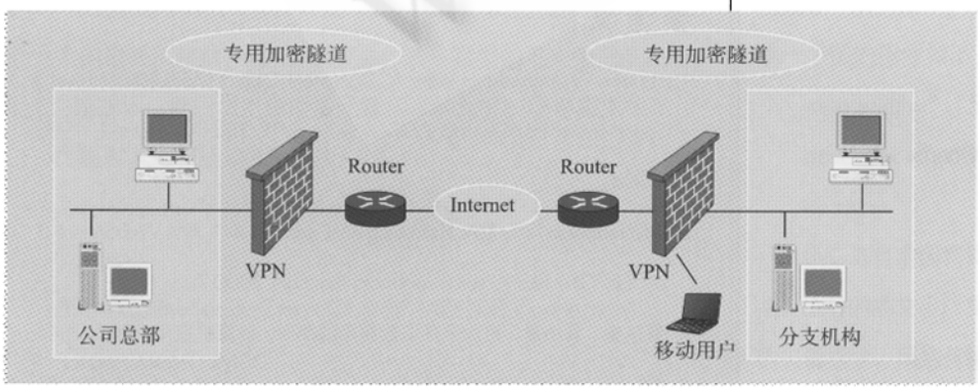

图 1　VPN 网络拓扑图

对于企业而言，利用Internet组建私有网，可以将大笔的专线费用缩减为少量的市话费用和Internet费用。据Infonetics Research的一项调查表明，采用VPN取代租赁线路，企业广域网连接成本下降了20～47%，而远程接入费用更可减少60～80％，这无疑是非常有吸引力的；VPN大大降低了网络复杂度、VPN用户的网络地址可以由企业内部进行统一分配、VPN组网的灵活方便等特性简化了企业的网络管理，另一方面，企业甚至可以不必建立自己的广域网和接入网维护系统，而将这一繁重的任务交由专业的ISP来完成；VPN提高了整个企业网的互联性，良好的扩展性使得企业更好、更快地适应Internet经济的发展，把握商机；另外，在VPN应用中，通过远端用户验证以及隧道数据加密等技术保证了通过公用网络传输的私有数据的安全性。

2 VPN技术原理

VPN技术非常复杂，它涉及到通信技术、密码技术和现代认证技术，是一项交叉科学。目前，企业自建VPN（CPE-BASED VPN）主要包含两种技术：隧道技术与安全技术。

2.1 隧道技术

隧道技术的基本过程是在源局域网与公网的接口处将数据(可以是ISO七层模型中的数据链路层或网络层数据)作为负载封装在一种可以在公网上传输的数据格式中，在目前的局域网与公网的接口处将数据解封装，取出负载。被封装的数据包在互联网上传递时所经过的逻辑路径被称为“隧道”。

要使数据顺利地被封装、传送及解封装，通信协议是保证的核心。目前VPN隧道协议有4种：点到点隧道协义PPTP、第二层隧道协议L2TP、网络层隧道协议

IPSec以及SOCKS v5。它们在OSI七层模型中的位置如表1所示。各协议工作在不同层次，无所谓谁更有优势。但我们应该注意，不同的网络环境适合不同的协议，在选择VPN产品时，应该注意选择。

表1 4种隧道协议在OSI七层模型中的位置

OSI七层模型	安全技术	安全协议
应用层 表示层	应用代理	
会话层 传输层	会话层代理	SOCK Sv5/SSL
网络层	包过滤	IPSec
数据链路层		PPTP/L2F/L2TP
物理层		

2.2 安全技术

VPN是在不安全的Internet中通信，通信的内容可能涉及企业的机密数据，因此其安全性非常重要。评N中的安全技术通常由加密、认证及密钥交换与管理组成。

2.2.1 认证技术

认证技术防止数据的伪造和被篡改，它采用一种称为“摘要”的技术。“摘要”技术主要采用HASH函数将一段长的报文通过函数变换，映射为一段短的报文即摘要。由于HASH函数的特性，两个不同的报文具有相同的摘要几乎不可能。该特性使得摘要技术在VPN中有两个用途：验证数据的完整性、用户认证。

2.2.2 加密技术

IPSec通过ISAKMP / IKE / Oakley协商确定几种可选的数据加密算法，如DES、3DES等。DES密钥长度为56位，容易被破译，3DES使用三重加密增加了安全性。当然国外还有更好的加密算法，但国外禁止出口高位加密算法。基于同样理由，国内也禁止重要部门使用国外算法。国内算法不对外公开，被破解的可能性极小。

2.2.3 密钥交换和管理

VPN中密钥的分发与管理非常重要。密钥的分发有两种方法：一种是通过手工配置的方式，另一种采用密钥交换协议动态分发。手工配置的方法由于密钥更新困难。只适合于简单网络的情况。密钥交换协议采用软件方式动态生成密钥，适合于复杂网络的情况且密钥可快速更新，可以显著提高VPN的安全性。目前主要的密钥交换与管理标准有IKE(互联网密钥交换)、SKIP(互联网简单密钥管理)和Oakley。

3 VPN技术设计企业网络的原则

一般网络设计的原则是安全性、网络优化、管理性，我们按照这3个原则分别说明.

3.1 安全性

VPN直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。企业必需要确保其VPN上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。

3.2 网络优化

构建VPN的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS（服务质量）通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。一般地，二层和三层的QoS具有以下功能：

（1）流分类：根据不同的用户、应用、服务器或URL地址等对数据流进行分类，然后才可以在不同的数据流上实施不同的QoS策略。流分类是实现带宽管理以及其他QoS功能的基础。ACL就是流分类的手段之一。

（2）流量整形与监管：流量整形是指根据数据流的优先级，在流量高峰时先尽量保证优先级高的数据流的接收/发送，而将超过流量限制的优先级低的数据流丢弃或滞后到流量低谷时接收/发送，使网络上的流量趋于稳定；流量监管则是指带宽大的路由器限制出口的发送速率，从而避免下游带宽小的路由器丢弃超过其带宽限制的数据包，消除网络瓶颈。

（3）拥塞管理与带宽分配：根据一定的比例给不同的优先级的数据流分配不同的带宽资源，并对网络上的流量进行预测，在流量达到上限之前丢弃若干数据包，避免过多的数据包因发送失败同时进行重传而引起更严重的资源紧张，进而提高网络的总体流量。

3.3 VPN管理

VPN要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成，企业自己仍需要完成许多网络管理任务。所以，一个完善的VPN管理系统是必不可少的。

VPN管理的目标为：

（1）减小网络风险：从传统的专线网络扩展到公用网络基础设施上，VPN面临着新的安全与监控的挑战。网络管理需要做到在允许公司分部、客户和合作伙伴对VPN访问的同时，还要确保公司数据资源的完整性。

（2）扩展性：VPN管理需要对日益增多的客户和合作伙伴作出迅捷的反应，包括网络硬、软件的升级、网络质量保证、安全策略维护等。

（3）经济性：保证VPN管理的扩展性的同时不应过多地增加操作和维护成本。

（4）可靠性：VPN构建于公用网之上，不同于传统的专线广域网，其受控性大大降低，故VPN可靠而稳定地运行是VPN管理必需考

虑的问题。

（5）VPN管理主要包括安全管理、设备管理、配置管理、ACL管理、QoS管理等内容。

4 VPN 组网方式

VPN 在企业中的组网方式分以下3种。在各种组网方式下采用的隧道协议有所不同，要仔细选择。

4.1 VPDN(Virtual Private Dial Network)

在远程用户或移动雇员和公司内部网之间的VPN，称为VPDN。实现过程如下：用户拨号NSP(网络服务提供商)的网络访问服务器NAS(Network Access Server)，发出PPP连接请求，NAS收到呼叫后，在用户和NAS之间建立PPP链路，然后，NAS对用户进行身份验证，确定是合法用户，就启动VPDN功能，与公司总部内部连接，访问其内部资源。

4.2 Intranet VPN

在公司远程分支机构的LAN和公司总部LAN之间的VPN。通过Internet这一公共网络将公司在各地分支机构的LAN连到公司总部的LAN，以便公司内部的资源共享、文件传递等，可节省DDN等专线所带来的高额费用。

4.3 Extranet VPN

在供应商、商业合作伙伴的LAN和公司的LAN之间的VPN。由于不同公司网络环境的差异性，该产品必须能兼容不同的操作平台和协议。由于用户的多样性，公司的网络管理员还应该设置特定的访问控制表ACL(Access Control List)，根据访问者的身份、网络地址等参数来确定他所相应的访问权限，开放部分资源而非全部资源给外联网的用户。

由于不同公司的网络相互通信，所以要更多考虑设备的互连、地址的协调、安全策略的协商等问题。这种组网方式也属于网关到网关的连接，选择IPSec协议是明智之举。

5 VPN 技术的具体应用

准格尔能源有限公司是我国投资兴建的集煤炭、电力、铁路运输联营的集团企业，该公司已经初步建立了公司内部的管理信息系统，随着该公司业务的发展，MIS系统的逐步扩展，如准能公司销售管理系统、办公系统等，要求扩展到各个销售处。目前该公司外有北京销售处、秦皇岛销售处、天津销售处、大同销售处等。公司经过分析比较决定，企业自建VPN，采用SOCKS v5协议。在此基础上，开发了公司销售管理信息系统，包括各办事处的销售计划，销售统计，合同管理，财务管理等子系统。

经过实际应用证明，采用VPN技术建立的管理信息系统实现了把企业与驻外办事处及移动用户连接，在保证数据安全的前提下，既节省了成本，又保证了数据的传输速度；使企业的网络花费最小的成本，得到了最大的效益。

参考文献

1 胡英，VPN 技术比较，计算机世界，2002.10.21。

2 Carlton R.Davis,IPSec:Securing VPNs ,清华大学出版社， 2002年1月。

3 何宝宏，IP 虚拟专用技术,人民邮电出版社, 2002 年 4 月。

4 戴宗坤等,VPN与网络安全,电子工业出版社 ， 2002年9月。