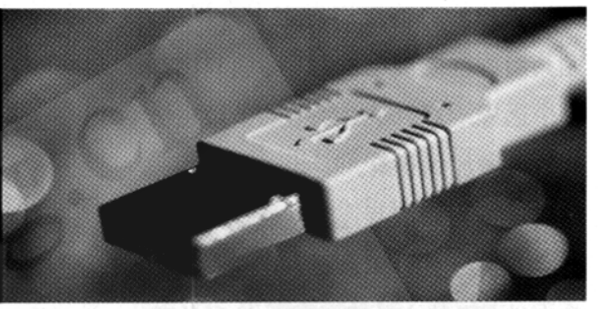
多远程销售点的安全信息系统

夏火松 蔡淑琴 (华中科技大学管理学院 430074)

摘要：企业对安全需求是多方面的，VPN的出现使用户除了可以显著地降低成本外还可获得多方面的好处，本文探讨了VPN技术在多远程销点信息系统中的作用、原理和基本分析与设计。

关键词：虚拟专用网络（VPN） 多远程销售点 信息系统安全



1 引言

开发多远程销售点的安全信息系统是根据某大型企业集团的要求提出的，该集团是以资产为纽带、按国有资产授权经营方式组建的以工程机械为主导产品的国家重点联系的首批300户国有大型企业之一的集团。主导产品为1～5立方米轮式装载机系列，产品技术水平居行业领先地位。技术装备精良，拥有100多台套大型加工中心、机器人自动焊接生产线等具有国际先进水平的设备。多年来一直保持行业市场占有率第一、销售量第一、销售收入第一，被誉为“中国工程机械行业的排头兵”企业。由于市场环境不断变化,企业的市场不仅在跨区域运作,而且有走向国际化的趋势，在市场日益竞争激烈的环境下，提出了“销售自动化”的需求：希望建成一个整机、配件、服务、信息“四位一体”的系统。

我们提出该集成销售管理信息系统拟建立多远程销售点的安全信息系统通过构造VPN（虚拟专用网，Virtual Private Network）建立一个安全可靠、快速反应和交易成本低廉的集成销售管理信息系统，能够在尽可能短的时间内在不同的机构之间办好各种手续，大大节约了时间和简化了手续。各个相关机构通过VPN连接在一起，合同、提单、保险单等电子数据信息通过Internet等公用网络传输，既保证了信息传输的安全性，又大大节约了时间。对用户来说，VPN最大的吸引力在哪里？据估算，如果企业放弃租用专线而采用VPN，其整个网络的成本可节约21%-45%，至于那些以电话拨号方式连网存取数据的公司，采用VPN则可以节约通信成本50%-80%。此外，VPN还使企业不必投入大量的人力和物力去安装和维护WAN设备和远程访问设备，这些工作都可以交给ISP。VPN使用户可以降低如下的成本：移动用户通信成本，VPN可以通过减少长途费或800费用来节省移动用户的花费；租用线路成本，VPN可以以每条连接的40%到60%的成本对租用线路进行控制和管理，对于国际用户来说，这种节约是极为显著的，对于话音数据，节约金额会进一步增加；主要设备成本，VPN通过支持拨号访问外部资源，使企业可以减少不断增长的调制解调器费用；另外，由于VPN独立于初始协议，这就使得远端的接入用户可以继续使用传统设备，保护了用户在现有硬件和软件系统上的投资。

2 安全信息系统与VPN技术的实现原理

在分布式计算环境中安全信息系统主要是对信息的传输、存储和访问提供安全保护，以防止信息被窃取、篡改和非法操作。信息系统的安全的基本要素是保密性、完整性、可用性服务、鉴别、访问控制和抗否认等安全服务。完整的信息安全保障体系包括保护、检测、响应、恢复等四个方面。按美国可信计算机评估准则TCSEC安全从弱到强分为4类7级：D、C1、C2、B1、B2、B3、A1。VPN使得远程端点之间可以通过公共分组网络实现相互之间的连接。通过在公共分组交换网络中建立隧道，并通过隧道实现两个远程端点之间的对点连接，使其效果、安全性和采用专用线

路实现点对点连接一样。就是三个远程端点之间采用专用线路实现点对点连接和采用VPN通过Internet实现相互连接。采用专用线路实现点对点连接，必须在任意两个端点之间开通专用线路。专用线路的月租是随着带宽和距离成线性增长的，这三条远距离专用线路的通信费用肯定十分昂贵，尤其当远程端点增加时，即使只增加一个远程端点，专用线路的条数也会从3条增加到6条。因此采用专用线路实现远程端点互连，不是轻易能够做到的。对于VPN，每一个端点只需和本地ISP建立物理连接，这种物理连接可以采用专用线路，但由于端点用户设备和本地ISP之间的距离一般较短，其通信费用和两个之间的远距离专用线路相比，要便宜很多，尤为可贵的是，不管和多少个远程端点建立隧道连接，端点用户设备和本地ISP之间的物理连接只需一条，当远程端点从3个增加到4个时，只需重新配置边缘路由器，分别和新增加的远程端点建立隧道即可。对用户来说，远程端点之间的隧道完成等同于专用线路，PPP报文通过隧道在两个远程端点之间传送和通过专用线路在两个远程端点之间传送，对用户来说，完全一样。目前使用的点对点隧道协议主要有两个：一个是点对点隧道协议（PPTP）；另一个是第二隧道协议（L2TP）。这两种隧道协议的工作机制大致相同。

无论在控制连接建立过程、会话建立过程还是PPP连接建立过程中，均可以采用认证协议对双方身份进行确认，以保证建立安全的隧道和PPP连接。对通过Internet传输的隧道协议，可以采用IPSEQ协议进行加密，以保证封装在IP报文中的隧道协议在通过Internet时不被截获和篡改。

电子数据通过隧道在公共网络上传输，隧道之外的个人或机构无法侵入隧道，即便信息被截获，对方看到的也只是一些毫无意义的乱码，这就保证了信息的安全性。各单位用户通过路由器访问各自子网之外的Intranet和Internet，但其内部是对外屏蔽的，这样外部的用户便不能访问内部子网，保证了子网内部的安全性。

目前VPN主要采用四项技术来保证安全，这四项技术分别是隧道技术（Tunneling）、加解密技术（Encryption & Decryption）、密钥管理技术（Key Management）、使用者与设备身份认证技术（Authentication）。隧道技术是VPN的基本技术，类似于点对点连接技术，它在公用网建立一条数据通道（隧道），让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到PPP中，再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2PT等。L2PT协议是目前IETF的标准，由IETF融合PPTP与L2F而形成。第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec等。IPSec（IP Security）是由一组RFC文档组成，定义了一个系统来提供安全协议选择、安全算法，确定服务所使用密钥等服务，从而在IP层提供安全保障。加解密技术是数据通信中一项较成熟的技术，VPN可直接利用现有加解密技术。

3 多远程销售点安全信息系统的分析

保证多远程销售点安全信息系统的措施一般包括从管理制度、国家法律和技术措施。在此我们从技术措施的传输、存储和访问中，一方面利用基于角色的存取访问多远程销售点信息系统各功能模块，而在次重点考虑的是传输过程的安全。从安全的代价和信息的重要性的合理方案看应选择VPN。考虑目前国内外许多大的网络安全产品公司都推出了自己的VPN产品，如Cisco公司的VPN系列产品，[1]提供了八家供应商的VPN解决方案。国际第二大防火墙厂商NetScreen公司最新提供的简单、易于管理、集成了防火墙和VPN功能的企业级安全产品----NetScreen-500，该产品具有250Mbps的传输性能，同时能支持1万个VPN通道。硬件的支持和网络协议的发展为集成销售管理信息系统开展基于Internet的VPN业务提供了安全的保障。

VPN有三种解决方案分别是：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN），这三种类型的VPN分别与传统的远程访问网络、企业内部的Intranet以及企业网和相关合作伙伴的企业网所构成的Extranet相对应。

远程访问虚拟网：Access VPN通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。AccessVPN能使用户随时、随地以其所需的方式访问企业资源。AccessVPN包括模拟、拨号、ISDN、数字用户线路（xDSL）、移动IP和电缆技术，能够

安全地连接移动用户、远程工作者或分支机构。

企业内部虚拟网：越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用VPN特性可以在Internet上组建世界范围内的IntranetVPN。利用Internet的线路保证网络的互联性，而利用隧道、加密等VPN特性可以保证信息在整个Intranet VPN上安全传输。Intranet VPN通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。

企业扩展虚拟网：随着Internet时代的到来，企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需求，同时各企业间的合作关系也越来越多，信息交换日益频繁。Internet为这一发展趋势提供了良好的基础，而如何利用Internet进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用VPN技术可以组建安全的Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。ExtranetVPN通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。

该公司的多销售点安全信息系统是整体规划、分步实施。第一步建立企业内部虚拟网（Intranet VPN），连接公司各办事处和销售点，系统运行成熟以后再建立扩展虚拟网，最后建立完整的集成电子商务平台。

4 多远程销售点安全信息系统的设计

该系统是一种分布式系统，其组织和获取信息资源的方式一般具有如下几种：第一种就是集中式数据库，优点是方便管理，一致性易控制，信息易获取；缺点是加重了各业务点与集中式数据库频繁交换信息，同时各业务点差异性难以体现，网络的稳定性要求较高。第二种就是分布式数据库/多数据库系统，优点是各业务点有自己的数据库能独立运行自己的业务系统，能自维护；缺点是需要综合信息时需要从各业务点获取信息统计汇总，对共用数据的更新与同步也较为复杂。第三种就是在第二种的基础上增加一个数据存取转发器（ARB：Access Request Broker），由它处理查询用户的信息获取请求。这时较好的一种方式。

该公司的多远程销售点安全信息系统设计采用的是第三种方式，在OS上可以采用Windows2000 server作为NOS，可作为VPN连接的服务器或路由器，Windows2000 professional作为VPN连接的客户机，Windows 2000支持PPTP和IPSec的L2TP协议。可以实现远程访问VPN连接和路由器对路由器的VPN连接。我们采用基于Internet的VPN，主要用PowerBuilder7.0作为前台开发工具[5]，Oracle和SQL Server7作为数据库管理系统，设计基于角色的安全远程销售点信息系统，Web界面的查询设计采用ASP技术，后续的开发将采用JSP技术。

5 结论

企业对安全需求是多方面的，防火墙、VPN、IDS、加密、防病毒等各有不同的作用，都是企业网信息资源的主要手段。安全与效率永远是一对矛盾，企业的信息资源不仅需要高度的安全，也需要高性能、高可用、成本适中的系统。虚拟专用网是一种依靠ISP（Internet服务提供商）和其他NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术，通过因特网等公用网将局域网扩展到远程网络和远程计算机用户的一种成本较低、效益极佳、安全性高的办法。■

参考文献

1 David Leon Clark 著，于秀莲等译，虚拟专用网[M]，人民邮电出版社，2000.7。

2 Priscilla Emery. Understand Knowledge Management [J] e-Business Advisor, April 1999。

3 胡道元，网络设计师教程，清华大学出版社，2001.5。

4 潘建国、陈海强， 基于VPN技术的网络应用[J]，计算机应用研究，2001年1月，87-88。

5 刘红岩，PowerBuilder7.0数据窗口技术详解[M]，电子工业出版社，2000.3。