DOI:10.13686/j.cnki.dzyzy.2007.03.015

第 16 卷第 3 期 地 质 与 资 源 Vol. 16 No. 3
2007 年 9 月 GEOLOGY AND RESOURCES Sep. 2007
文章编号:1671 - 1947(2007)03 - 0234 - 04 中图分类号:TP393.02 文献标识码:A

虚拟专用网技术在远程数据传输中的应用

蒋 宁
(沈阳师范大学 科信软件学院,辽宁 沈阳 110034)

摘 要:野外地质调查工作者作为远程用户需要与其所在的地质调查研究机构进行数据的安全传输.应用虚拟专用网络技术可以在使用公用网络进行数据传输时保证其安全.本文讨论了虚拟专用网的分类、关键技术,通过分析某地质研究所的网络拓扑,给出了一个虚拟专用网的解决方案,对其中的基于 Windows Server 2003 的虚拟专用网服务器进行了详细配置.

关键词:网络安全;虚拟专用网;远程数据传输;地质调查

远程数据传输已经成为现代地质调查研究工作不可缺少的一种形式.这一方面在于随着野外数据采集数字化程度的日益提高,经常需要及时将野外采集的数据远程传输到地质调查研究机构的办公内网进行数据存储和处理;另一方面也在于在野外地质调查过程中有时需要从地质调查机构的办公内网和数据库中调用有关技术资料.由于地质调查工作所获得的数据大多为珍贵的第一手资料,在远程数据传输中要确保其安全.如果使用 Internet 网络的方式进行数据传输,很难以保证数据的安全性.因此建立一个经济、高效、快捷、安全的网络系统来进行远程数据传输成为远程办公的迫切要求.

1 远程数据传输解决方案

在 Internet 还没有普及时,只有税务、电力、银行等系统才有能力承担组建和使用专线的费用.随着技术的发展,利用虚拟专用网技术组建专用网络已经非常经济,而且速度能够达到专线水平.

而对于移动用户,需要进行远程数据传输时,传统上使用的是直拨技术.但直拨技术解决方案适合于小规模、地域较近的接入访问,不适合频繁出差用户进行远程办公.对于移动用户,专线方式显得无能为力,因为用户所在的地点是不确定的、暂时的.虚拟专用网技术方案适合于地域分布较广、数量较大的接入访问[1],能够解决远程数据传输的实际需要.更为重要的是,虚拟专用网技术能够充分保障移动远程用户的数据安全.

收稿日期:2007 - 02 - 12;修回日期:2007 - 04 - 26.张哲编辑.

通过 Internet 组建虚拟专用网的方法主要有两种:一是购买专业的路由器等设备,一是使用专业软件.与前者相比,后者更加经济,配置更加简单,而且效果与前者组建的虚拟专用网是相同的.可以根据原有网络的实际情况和需要进行虚拟专用网的组建.

综上,远程数据传输的解决方案采用虚拟专用网,组建时考虑实际需要来进行组建.

2 关于 VPN 技术

2.1 VPN 的定义

虚拟专用网(Virtual Private Network, VPN)是利用接入服务器、路由器及专用设备在公用网络(包括 IP 网络、公用电话网、帧中继网及 ATM 网等)上建立专用网络,数据通过安全的隧道在公用网络中传输.虚拟专用网是专用网络(DDN 专线或者电话拨号连接的线路)的延伸,它使用公用网络组建自己的网络.也就是说,用户觉察不到他在利用公用网络获得专用网的服务.从客观上可以认为 VPN 就是一种具有私有和专用特点网络通信环境.它是通过虚拟的组网技术,而非构建物理的专用网络的手段来达到的.通过 VPN 可以通过公用网络在两台计算机之间安全地传输数据.由于 VPN 可以利用原有的 IP 网络、帧中继网、ATM 网等来建设,所以可以大大减少网络建设费用[2].

2.2 VPN 分类

VPN 的分类方法有很多种,根据应用环境的不同,VPN 可以分为 3 种基本类型[3]:远程接入 VPN

(指企业员工通过公用网络以远程拨号的方式来访问企业内部网络) ; 内部网 VPN(指企业通过公用网络将各分支机构的局域网和总部的局域网连接起来) ; 外部网 VPN(指企业之间为了方便信息交流, 将各自的内部网 VPN 连接起来构成一个大的虚拟企业内部网络) .

2.3　VPN 的安全技术

由于 VPN 传输的是私有信息, 因此数据的安全是 VPN 使用者最为关心的事情. 目前 VPN 主要采用 4 种技术来保证安全, 即隧道技术、加密技术、密钥管理技术及身份认证技术[1] .

隧道技术是 VPN 的关键性技术. 隧道是一种通过互联网络在网络之间传递数据的一种方式. 所传递的数据在传送之前被封装在相应的隧道协议里, 当到达另一端时被解包. 隧道技术相关的协议分为第二层隧道协议和第三层隧道协议. 第二层隧道协议是先把各种网络协议封装到 PPP (Point-to-Point Protocol) 中, 再把整修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传输; 第三层隧道协议是把各种网络协议直接装入隧道协议中, 形成的数据包靠第三层协议进行传输. 第二层隧道协议主要有 PPTP (Point-to-Point Tunneling Protocol) 、L2TP(Layer 2 Tunneling Protocol) 等, 第三层隧道协议主要有 IPSec 等. 其中 PPTP 是为使用电话上网的用户提供安全的 VPN 业务, L2TP 可以在 IP 网、帧中继、X.25 或 ATM 网络上使用. IPSec 为 IP 层及其上层协议提供保护, 对于用户和应用程序来说是透明的.

加密技术是指发送者在发送数据之前对数据加密, 当数据到达接收者时由接收者对数据进行解密. 加密算法如 DES、3DES、IDEA 等.

密钥管理技术的主要任务是在公用数据网上安全地传递密钥而不被窃取, 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.

用户身份认证技术主要用于远程访问的情况. 当一个拨号用户要求建立一个会话时, 就要对用户的身份进行鉴定, 以确定该用户是否为合法用户以及哪些资源可被使用. 身份认证技术最常用的是使用名称与密码或卡片.

2.4　VPN 产品

支持 VPN 的产品种类很多, 包括带 VPN 功能的防火墙、带 VPN 功能的路由器、专用 VPN 设备、软件 VPN 系统等. 使用 VPN 的用户可根据自己的情况来选择 VPN 产品.

一般说来, 选择 VPN 产品时主要考察以下几个方面的性能: 是否集成防火墙; 可支持最大连接数目; VPN 系统对客户机的要求; 网络管理功能.

3　某地质研究所 VPN 系统的解决方案

3.1　VPN 的网络拓扑图

图 1 是某地质研究所的网络拓扑, 单位局域网的工作站运行的操作系统为 Windows XP 或 Windows 2000, 使用代理服务器共享上网. 服务器具有两块网卡, 其中一块网卡连接单位内部局域网, 另一块通过光纤连接到 Internet. 代理服务器上运行的操作系统为 Windows Server 2003.

地质研究所根据远程办公的用户的要求需要组建虚拟专用网. 该地质研究所没有分支机构在外地, 只有经常出差的用户, 这些移动远程用户使用其他地方提供的线路连接到 Internet(例如电话拨号、无线上网、宾馆 Internet 接入等) . 所以组建虚拟专用网时类型选择远程接入 VPN.

Windows Server 2003 操作系统包括虚拟专用网络组件, 安装 Windows Server 2003 时可以自动安装 PPTP 和 L2TP 隧道协议[5]. Windows Server 2003 虚拟专用网组件具有以下特点: 集成了基本防火墙; 允许远程 VPN 连接的最大并发数可在 0～16384 之间设置; 要求 VPN 客户端可以运行 Windows Server 2003、Windows XP、Windows 2000、Windows NT 4.0 和 Windows 98 操作系统, 也可以是任意非 Microsoft 的 PPTP 客户端或者是有 IPSec 的 L2TP 客户端; 网络管理部分有比较完备的功能和良好的界面.

根据地质科研机构的实际需要, 用 Windows Server 2003 构建 VPN 服务器完全能够实现远程数据传输经济、高效、快捷、安全的目标. 所以将原有的代理服务器配置成 VPN 服务器, 其上运行的操作系统

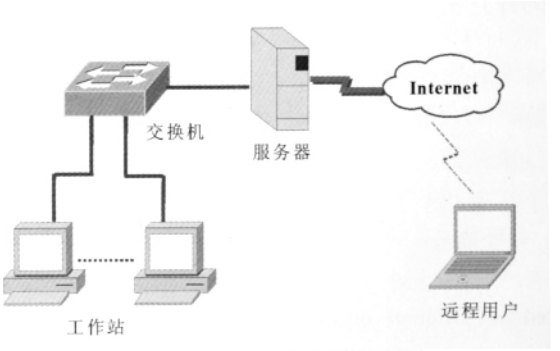

图 1　网络拓扑

Fig. 1　Network topology

仍为 Windows Server 2003. 创建 VPN 路由后，不影响原来的上网，即仍然使用 VPN 服务器做共享上网的代理服务器.

3.2 VPN 服务器及客户机的配置

VPN 服务器、工作站及出差用户的 IP 地址参数如表 1.

表 1 IP 地址参数

Table 1 IP address parameters

设备	IP 地址参数
服务器	内网:192.168.100.1/24,无网关地址
	外网:210.30.208.140/24,网关地址:210.30.208.4
工作站	192.168.100.10~192.168.100.254/24,网关地址:
	192.168.100.1
远程用户	随机

3.2.1 配置 VPN 服务器

在配置 VPN 服务器之前，如果使用 Windows 提供的 Internet 连接共享"共享上网，要停止该服务；如果使用其他的代理软件共享上网，则停用并卸载；如果"路由和远程访问服务"已经启动，则停止.

重新配置"路由和远程访问服务"，选择"两个专用网络之间的安全连接"，启用 VPN 路由. 停止"路由和远程访问服务"之后再启用，目的是为了删除"路由和远程访问服务"原来的设置，从而保证配置的一致.

配置"路由和远程访问服务"中的 NAT(网络地址转换)功能，在公用接口(即连接 Internet 的网卡)上启用 NAT，为单位内部各工作站共享上网. 为了提高安全性，可以同时在此接口上启用基本防火墙.

配置 VPN 服务器作为路由器时，启用"远程访问服务"，允许各出差用户能够使用. 可配置允许远程 VPN 连接的最大并发数，比如 50. 为使用 VPN 连接的用户授予远程访问权限. 在 VPN 服务器上为 VPN 客户端创建用户并设置用户密码，确保用户不能更改密码并且密码永不过期.

3.2.2 配置内网工作站

配置内部网络的各个工作站，包括 IP 地址、子网掩码、网关、DNS 服务器等参数，如表 1 所示，而无需做任何其他设置.

3.2.3 配置远程访问计算机

配置出差用户使用的操作系统使其成为 VPN 客户端. 不同版本的 Windows 系统下配置 VPN 的方式略有不同，但都是创建一个虚拟专用网络连接，创建时需要输入 VPN 服务器的 IP 地址(即连接 Internet 的网卡 IP 地址 210.30.208.140). 出差用户使用 VPN 时，先连接到 Internet 上之后，再运行 VPN 连接，连接 VPN 服务器时用户需要输入用户名和密码等认证信息. 当连接完成后，就可以像在局域网中那样，访问远程的 VPN 服务器和 VPN 服务器所在的网络了.

4 结束语

虚拟专用网作为远程访问的高效低价、安全可靠的解决方案，具有灵活性、安全性、经济性以及可扩展性的特点，可充分满足移动办公安全通信的需求. 本文根据某地质研究所原有网络的特点，应用虚拟专用网技术为其组建成本低、安全性好的远程访问 VPN 系统. 利用该 VPN 系统，被授权的出差用户可以很方便地通过 Internet 实现远程办公，保证远程数据传输的安全.

参考文献:

[1]许娓，陈训威.基于 VPN 技术的远程数据传输解决方案[J].微计算机应用，2002，23(3):161－164.

[2]赵军科，黄道，汪胜.虚拟专用网的技术及其应用[J].微型电脑应用，2002，18(9):38－41.

[3]黄传河，等.网络安全[M].武汉：武汉大学出版社，2004.307－309.

[4]张文艳，姜春霞.用虚拟专用网(VPN)搭建远程应用系统[J].东北电力技术，2005，(11):50－52.

[5]王春海，严健华，樊玉芳.非常网管——网络应用[M].北京：人民邮电出版社，2006.324.

APPLICATION OF VPN IN REMOTE DATA TRANSMISSION

JIANG Ning

(College of Science and Information Software, Shenyang Normal University, Shenyang 110034, China)

Abstract: Remote office users require secure transmission of data, which can be ensured on public network by virtual private network(VPN) technology. The categories, pivotal security technologies and products of VPN are discussed. A

(Continued on Page 182)

形成;大约 25～26 亿年,本区发生了第二次强烈的构造- 岩浆- 热事件,表现为强烈的构造变形及花岗岩的侵入作用, 并发生了温度为 520～670℃、压力 600～850 MPa 的角闪岩相变质作用, 不仅使含矿建造发生形变,而且使部分初始矿(化) 体发生了塑性流变.随着温压条件降低,进入温度 120～390℃、压力 40～160 MPa 的条件时,已转为成矿热液蚀变作用为主的矿化过程.成矿蚀变作用的热液水来自 天水 "与变质水的混合水,其不仅使含矿建造及初始矿(化) 体发生围岩蚀变,同时大量硫化物选择有利空间发生充填 - 交代作用,从而形成矿体.

综上,作者认为红透山铜锌矿床应属 火山 - 沉积变质热液叠加 '型层控矿床[7].

参考文献:

[1]张秋生,等.辽东半岛早期地壳与矿床[M].北京:地质出版社,1988.
[2]江培谟.地质热力学基础[M].北京:科学出版社,1989.
[3]魏菊英,王关玉.同位素地球化学[M].北京:地质出版社,1987.
[4]韩吟文,马振东.地球化学[M].北京:地质出版社,2003.
[5]李俊华,夏德兴.同位素年龄计算手册[M].北京:原子能出版社,1978.
[6]孙荣圭.辽东清原地区太古代岩石 Rb-Sr 年代[J].地球化学,1989,(1).
[7]袁见齐,朱上庆,翟裕生.矿床学[M].北京:地质出版社,1984.

GEOLOGY AND GENESIS OF THE HONGTOUSHAN COPPER-ZINC DEPOSIT IN LIAONING PROVINCE

ZHANG Sen[1], ZHAO Dong-fang[1], LV Guang-jun[2], SHA De-ming[1], QUAN Heng[1], TIAN Chang-lie[1], YANG Tie-jun[3]
(1. Shenyang Institute of Geology and Mineral Resource, Shenyang 110032, China; 2. Liaoning No. 8 Geologic Party, Benxi 117000, Liaonmg Province, China; 3. Fushun Branch, Liaoning Institute of Nonferrous Geological Exploration, Fushun 113015, Liaoning Province, China)

Abstract: The Hongtoushan Cu-Zn deposit, located in the Hongtoushan rock formation of Archean greenstone in North Liaoning Province, is a large-scale ore deposit with great industrial significance. According to the analysis of H, O, S and Pb isotope characteristics, accompanying with the macroscopic natures, such as the orebody shape, ore texture, structure and wall-rock alteration, it is considered that the matter source of the Hongtoushan Cu-Zn deposit is the Neoarchean volcanic-sedimentary rock series. The ore-forming fluid is originated from atmospheric water and metamorphic water. The heat for ore-forming is from metamorphism. Thus the Hongtoushan Cu-Zn deposit belongs to stratabound type with volcanic-sedimentary and metamorphic hydrothermal overprinting.

Key words: Hongtoushan; Cu-Zn deposit; geologic characteristics; stratabound type with volcanic-sedimentary and metamorphic hydrothermal overprinting; Liaoning Province

作者简介:张森 (1983—),男,黑龙江省泰来县人,2005 年毕业于中国地质大学(武汉),现从事矿床成矿规律研究工作,通信地址 沈阳市北陵大街 25 号,邮政编码 110033.

(Contiued from Page 236)

remote access VPN project is implemented by analyzing the network topology of a geological institution. The VPN server applying Windows Server 2003 in the project is configured in detail.

Key words: VPN; network security; remote data transmission

作者简介:蒋宁(1977—) ,女,辽宁海城人,硕士,讲师,2003 年毕业于中国科学院沈阳计算技术研究所计算机应用专业,现从事计算机网络安全方面的教学与科研工作,通信地址 沈阳师范大学科信软件学院,邮政编码 110034, E-mail//jiangnn2003@yahoo.com.cn