文章编号：1005-8451（2010）06-0058-04

VPN技术在站段网络建设中的应用

张 辉，李菊萍
（西安铁路局 宝鸡工务段网络室，宝鸡 721000）

摘 要：本文首先对VPN的需求进行分析，介绍了VPN技术和隧道技术，提出铁路段办公网与车间班组互联方案，采用VPN技术为段办公网的安全提供技术保障。

关键词：VPN技术；安全；办公网应用
中图分类号：TP393 文献标识码：A

宝鸡工务段是西安铁路局工务系统内最大的站段之一，管辖西宝线、宝中线、宝成线及宝天线。除机关办公使用的计算机外，其余计算机安装在沿线各车间和班组，分布范围较散，且相隔距离较远。

目前段机关通过网桥接入方式接入车站机房。车间班组通过铁通的综合信息平台与段机关联通，车间班组需要实时将信息传送到段机关及铁路局，段机关及铁路局也需要将反馈的信息实时向车间班组下发。但段机关作为连接的中心点，所有的数据都经过段服务器进行分发。

1 VPN需求分析

随着铁路的迅速发展，工务段管辖的车间班组相继多了起来，信息交互也越来越频繁，随着各种业务应用系统的实施，重要的数据和信息在网络中传输也越来越多，安全性要求也越来越高，目前仅仅依靠综合信息平台接入，段服务器转发的组网模式已经越来越不适应工务段对信息传输平台的要求了。

从安全方面考虑，铁通提供的综合信息平台没有经过加密处理，重要数据和信息均是以明文在网上传输，如果别有用心的人利用Sniffer等网络监听分析工具，极易篡改、窃取甚至破坏企业数据，给企业造成不可估量的损失；由于传输平台没有认证功能，企业内部员工的越权访问、误操作、有意或无意的泄密、甚至是少数员工恶意的破坏，都会对企业的信息和数据造成很大的威胁；由于传输平台没有访问控制和安全隔离的功能，给外部非法人员提供了入侵的机会，非法人员可以通过专用的黑客程序（此类工具在Internet上可以任意下载），或者盗取授权员工的访问权限，很容易进入企业系统内部。由于工务段车间班组联网网点数目众多，相应的受攻击的几率较大，一旦通过计算机终端进入总部服务器，后果将不堪设想。

从管理方面考虑，工务段处于高速发展阶段，

收稿日期：2009-11-13
作者简介：张 辉，技术员；李菊萍，助理工程师。

机的组成部分，是推行数字化校园的有力载体，其内容将随需求愈加充实，其构成亦愈加丰富，它可以渗透到学校的教学、科研、管理和后勤等多方面应用，并随着科技进步和管理内容的增多而加以深化。我校在校园一卡通系统建设的成功基础上，通过对校园一卡通系统中累积起来的各种数据进行统计分析，得到一系列学生行为的分析结果和就餐消费分析结果，不仅为领导决策提供了有用的参考信息，也为将来构建完整的数字化校园决策支持系统提供了实践经验和实现方法。

参考文献：

[1] 张薇涛，李向阳，邹秀香.校园一卡通系统的应用研究[J].山东师范大学学报（自然科学版），2009（23）：126-129.

[2] 张升平.数字化校园之校园一卡通的建设[J].重庆工商大学学报（自然科学版），2008（25）：56-59.

[3] 段智敏，王如龙，孙美青，余 维.基于一卡通的数字化校园资源整合研究与实现[J].计算机工程与科学，2008（30）：8-11.

[4] 王玉芬，张治斌，李长江.数据仓库在高校决策支持中的应用研究[J].陕西理工学院学报，2007（23）：17-19.

拥有的联网网点和计算机终端较多，最紧迫的问题就是信息的汇总、联网网点的信息交互以及计算机终端的集中管理。现有组网方式由于本身的技术限制，不可能提供强大的管理平台，也不可能解决大规模的应用和管理问题。

从经营角度考虑，工务段需要一个实时、安全、高速、快捷和稳定的信息交互平台，以满足信息频繁传输的需要，以便增加工作效率，提高服务质量，加快信息化建设，适应快速发展，提升良好形象。

综上所述，如何快捷地解决工务段的联网问题，如何很好地解决“信息的共享和信息的安全问题”是本方案重点讨论的问题，使整个网络的互联性得到极大提高，安全性达到全面加强，是本系统方案要实现的目标。

2 VPN技术特点

随着互联网技术的发展及Internet接入方式的多样化，为VPN应用提供了条件，不同地区的远程遥测点可通过ADSL、小区宽带、GPRS、CDMA 1X或窄带拨号等各种网络连接方式连入Internet，无需固定公网IP地址，由中心的VPN网关为认证用户分配一个内部私网地址，通过远程认证，实现与监测内部网络的互连，从而组成一个高效统一的虚拟专用网络。

目前VPN技术相当成熟，应用相当广泛，主要采用4种技术：隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术。

2.1 隧道技术

当VPN客户机访问VPN服务器时，并没有传统专网所需的端到端的物理链路，它们是通过一个虚拟的隧道进行访问。一个隧道实际上就是在公网上建立一条数据通道，让数据包通过这条隧道传输，完成数据封装、传输和解包。为创建隧道，隧道的客户机和服务器双方必须使用相同的隧道协议，隧道技术主要有3种协议支持：PPTP，L2TP和IPsec。

（1）点对点隧道协议（PPTP）。

PPTP协议工作在OSI/RM开放模型中的第2层，允许对IP、IPX或NetBEUI数据流进行加密，然后封装在IP包头中通过企业IP网络或互联网发送。通过PPTP，远程用户首先拨号到本地因特网服务提供商ISP的网络服务器NAS去访问总部的内部网络，并不需要直接拨号至总部的网络，这样大大减少了建立和维护专用远程线路的费用。PPTP协议通过身份验证后开始加密，身份验证的过程没有加密，安全性稍低，配置简单，在实现上存在着重大安全隐患。

（2）第2层隧道协议（L2TP）。

L2TP协议是L2FP与PPTP的结合，专门用来进行第2层数据的通道传送，允许对IP、IPX或NetBEUI数据流进行加密，然后通过支持点对点数据报传递的任意网络发送，如IP、X.25、桢中继或ATM。远程用户通过本地PSTN、ISDN或PLMN拨号，利用ISP提供的VPDN特服号，接入ISP在当地的NAS，通过当地的VPDN认证系统对用户身份进行认证，建立一个位于NAS和LNS（本地网络服务器）之间的虚拟专网来访问总部的内部网络。L2TP需要证书服务来验证计算机身份，身份验证过程是加密的，安全性较高，配置稍微复杂，但也不能完全保证数据传输过程中的安全。

（3）安全IP（IPSec）隧道模式。

IPSEC协议工作在OSI/RM开放模型中的第3层，允许对IP负载数据进行加密，然后封装在IP包头中通过企业IP网络或互联网发送，具有认证包头AH和数据加密格式ESP。IPSEC采取数据源验证、无连接数据的完整性验证、数据内容的机密性保护、抗重播保护等形式，有效保护IP数据报的安全。在传输数据包之前将其加密，接收端根据AH和ESP对所有受IPSec保护的数据包进行认证和解密，防止数据包被捕捉并重新投放到网上，安全性高，从而保证了数据包在Internet网上传输时的私有性、完整性和真实性。

2.2 加解密技术

加解密技术是数据通信中一项较成熟的技术，可直接利用。

2.3 密钥管理技术

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，密钥管理技术又分为SKIP与ISAKMP/OAKLEY两种。

2.4 身份认证技术

当VPN客户端连接VPN服务器时，就涉及到

身份验证的问题，身份验证可以采用Windows的身份验证或者RADIUS（远程拨号用户确认服务）身份验证。

Windows的身份验证主要通过用户名和密码来提供认证，认证协议采用Microsoft质询握手身份验证协议MS－CHAP来加强对用户身份的查验。

RADIUS身份验证是通过Windows安装Internet验证服务IAS来实现。这种拨号方式建立的VPN连接，可以实现双重数据加密，使网络数据传输更安全。

VPN的加密方式使得网络信息传输安全性大大提高，数据验证使得接收方可识别数据包是否被非法篡改，保证了数据的完整性。

3 关于VPN专网的安全管理

使用VPN传输私有数据，面临潜在的安全风险，这需要提供安全保障。虽然VPN有单独的网关，对IPSec数据包进行加密/解密处理和身份认证，但它没有很强的访问控制功能，如状态包过滤、网络内容过滤、防DoS攻击等。要防止非法用户对网络资源或私有信息的访问，网络管理员必须对通过VPN连接到网络的计算机和直接连接到LAN的计算机实行同样的安全标准。

为保证VPN的安全性，必须将所有设备放在防火墙之后，防火墙必须封锁任何没有使用的端口，由防火墙打开允许的隧道信息包通过，才能与内部网络进行数据传输。可以通过安全检测设置来限制有权限的访问者，如果不再符合安全法则时，根本不允许接入，从而为私有数据在公用网络上的传输提供了安全和保密。

在监测网络上建立防火墙，能够保证内部网络免受安全威胁及攻击，强大的网络地址转换功能使服务器对外伪装服务身份，保护局域网内部的服务器安全运行，同时支持对特殊网络服务及ARP欺骗病毒的屏蔽功能。对于连接VPN的用户也必须在个人计算机上安装个人防火墙，它可以使非法侵入者不能进入局域网。

4 站段网络平台结构

综合VPN技术特点，在段内办公网上采用了IPSec隧道模式组建VPN专网，其网络拓扑结构如图1。

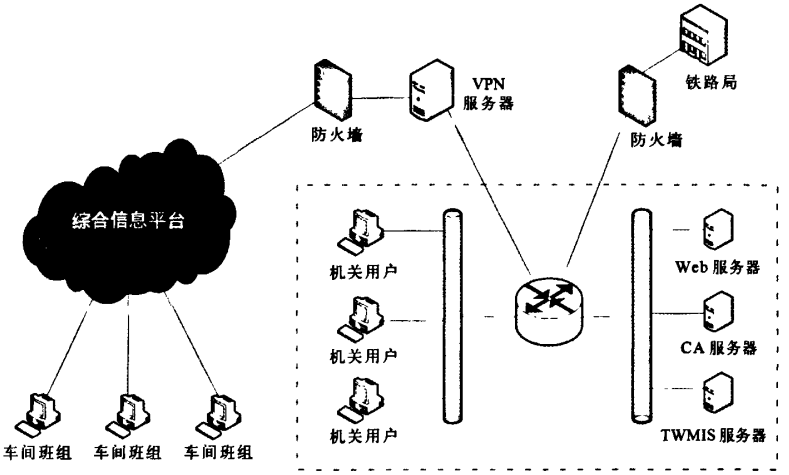

图1 网络拓扑结构

VPN专网的实现，需在内部网络中配置一台VPN服务器与内部网络连接，在中心将VPN硬件网关、监测网络设备及内部办公设备放在防火墙后面，经过防火墙再由一条专用光纤连接到综合信息平台，VPN硬件网关的LAN（局域网）口连接到内网的交换机上，WAN（广域网）口连接到与综合信息平台相连的光纤。

当远程终端通过VPN连接与办公网中的计算机进行通信时，先由综合信息平台将所有的数据传送到VPN服务器，再由VPN服务器将所有的数据传送到目标计算机。

网络管理员通过配置VPN服务器，指定只有符合特定身份要求的用户才能连接VPN服务器获得访问内部信息的权利，没有访问权利的用户无法获得办公网信息。

VPN服务器相当于执行路由和远程访问服务任务的一个增强的Windows Server服务器，一旦一个进入VPN网络的请求被批准，这个VPN服务

器就简单地充当一台路由器向这个VPN客户机提供专用网络的接入。

当远程终端访问办公网网内部资源时，有可能将间谍软件，病毒随着客户端对办公网的访问而进入内网，导致服务器遭受间谍软件、病毒的风险。利用域管理模式和架设CA服务器来创建网络访问准入规则，预先定制好远程终端计算机的安全策略。当远程终端计算机通过VPN服务器连接办公网时，检查用户的计算机是否具备了相应的安全策略。

只有符合相应的安全策略的用户才允许登陆，不具备相应安全条件的用户，不允许登陆到VPN服务器，也连不通VPN通道。这样从根本上提高了远程终端计算机的安全性，减少了远程终端遭受蠕虫、病毒、木马以及间谍软件而导致服务器遭受破坏的风险。

这种方案充分利用了综合信息平台，远程终端通过ADSL方式接入综合信息平台，再由和综合信息平台相连（段机关采用了一条10 M光纤）的VPN服务器，来访问位于VPN服务器后面的内部网络。一旦接入VPN服务器，就在远程终端与VPN服务器之间建立一条专用隧道连接。这样，远程终端到综合信息平台的连接和VPN服务器到综合信息平台的连接都是本地网内通信，由于采用加密技术，远程终端到VPN服务器之间的连接是安全的。

5　VPN技术实施的优势

（1）迅速拥有高效稳定的VPN平台，广泛的兼容性使其可以很方便的部署于网络的任何位置。而简单明了又兼备完整逻辑思路的操作模式可以让管理员迅速掌握，从而方便地配置出满足自身需求的个性化配置方案。在客户端不需要安装任何应用软件，不需做任何配置，同时也减轻了网络管理员的工作。

（2）接入后的用户受控于更细致的访问控制粒度。根据组织的构架，用户可以分组管理，而授权粒度则可以按照角色进行管理，为每个用户或每个组分配一个或多个角色。比如可以为某用户分配办公收发文和财务查询的双重角色，这样他即可以访问办公OA的进行收发文又可以访问财务系统进行财务查询。

（3）实现了整体的互联，使分散的部门连到统一的VPN网络。满足整体网络实时互联互通的要求，实现各个点的VPN互联，构建完整的基础网络平台，并可根据权限的设定和网络拓扑的需要分别设定接入节点和权限控制，增强内部基础网络的稳定性和可靠性。

（4）确保数据传输的安全可靠、接入用户的严格认证。段机关与各个车间班组之间，无需更改原有的网络结构、按照实际的运作流程，构建完善、稳定、高效的VPN网络，保障信息化系统的日常运行。

（5）建成标准统一、功能完善、安全可靠的内部网络与信息平台，形成信息安全保障体系。建设的重点任务：加快建设内网平台；整合信息资源；形成结构合理、功能完善、管理规范、安全可靠和灵活实用的网络基础支撑体系。

6　结束语

上述方案成功地解决了段办公网与车间班组之间实时互联问题，提供了远程访问的安全途径，使车间班组能够随时方便地接入工务段内部网络开展业务，共享网络资源。最大限度地发挥各种应用系统的效率，使工务段网络管理更加统一规范，共享数据信息。VPN提供了安全、可靠的访问通道，为工务段信息化建设进一步发展提供了可靠的技术保障，达到科学高效的管理目标。

参考文献：

[1] 高海英，薛元星，辛　阳，等. VPN技术[M]. 北京：机械工业出版社，2004.

[2] [美]Mark Lucas，等. 防火墙策略与VPN配置[M]. 北京：水利水电出版社，2008.

[3] 王　达. 虚拟专用网（VPN）精解[M]. 北京：清华大学出版社，2004.

[4] [美]Mark Lewis. VPN故障诊断与排除[M]. 袁国忠. 北京：人民邮电出版社，2006.

[5] 吉荣廷，杨慧，赵建军. 基于VPN技术与CDMAIX技术实现远程视频无线传输[J]. 铁路计算机应用，2008，12 (2).

[6] 吕鸿杰，谭献海，裴加富. UML&VP在VPN网络系统中的应用[J]. 铁路计算机应用，2008，12 (3).