文章编号:1673-9469(2012)01-0100-03

利用SSL VPN实现卡车调度系统中的远程设备管理

崔鑫拓[1],夏亮亮[2],徐博会[1]
(1. 河北工程大学 资源学院,河北 邯郸 056038;2. 中国矿业大学(北京) 地球科学与测绘工程学院,北京 100083)

摘要: 由于露天矿区一般比较偏远,受到交通等因素的影响,卡车调度系统中的设备维护非常不方便。本文利用SSL VPN的方式,从远程网络连入系统内部网络中,对内部的设备进行远程管理和维护,在方便管理及降低维护成本的同时,也满足了移动办公的需求。

关键词: 卡车调度;SSL VPN;远程管理
中图分类号: TN711.1 **文献标识码:** A

Remote device managing in truck dispatching system basing on SSL VPN

CUI Xin-tuo[1], XIA Liang-liang[2], XU Bo-hui[1]
(1. College of Natural Resource, Hebei University of Engineering, Hebei Handan 056038, China; 2. China College of Geoscience and Surveying Engineering, University of Mining & Technology, Beijing 100083, China)

Abstract: As open pit mine area is generally far away from the city and affected by transportation and other facts, so that the maintenance of equipment in the truck dispatch system is very inconvenient. The remote management and maintenance of the internal device were realized by the means of SSL VPN, which connected the remote network to the system of internal network. Doing these can not only be facilitated for management and reduce maintenance costs, but also meet the needs of the mobile office.

Key words: truck dispatching system; SSL VPN; remote management

卡车调试系统是集计算机技术、无线数据通讯技术、全球卫星定位系统技术等为一体的高新技术系统,它可以为露天采矿的卡车运输提供自动、优化的管理[1]。该系统中包含了车载GPS终端设备、无线通讯塔、移动信号车、服务器等网络设备,由于条件限制,这些设备经常需要远程管理及调试。本文以"长山壕露天矿运输车辆安全生产信息采集管理调度系统"为实例,利用SSL VPN实现该项目中的网络设备的远程管理,并且满足移动办公的需求,从而有利的提高了卡车调试系统中设备的管理效率,降低了维护成本。SSL VPN是一种采用SSL协议来实现远程接入的VPN技术,与传统的IPSec VPN相比,SSL VPN能够更简单、更安全的实现信息远程连通[2]。由于大部分浏览器都内嵌了SSL协议,所以SSL VPN无需任何客户端,不需要配置,可以直接使用浏览器完成SSL的VPN建立[3],使得SSL VPN的使用变得非常简单。同时,用户用浏览器登录SSL VPN设备后,拨通网络访问资源即可获得一个虚拟IP,即可以访问按照安全策略允许访问的内网地址和端口[4],和IPSec VPN不同的是,这种方式并非工作在网络层[5],所以不会有接入地点的限制,因此满足了移动办公的需求。另外,SSL安全通道是在客户到所访问的资源之间建立的,确保端到端的真正安全。无论在内部网络还是在因特网上数据都不是透明的。客户对资源的每一次操作都需要经过安全的身份验证和加密[6],从而保证了传输的安全性。

收稿日期:2011-10-26
作者简介:崔鑫拓(1985-),男,内蒙古通辽人,硕士研究生,从事计算机在矿产开发中的应用研究。

1 组网需求

为了尽量保证安全,保护系统内部的服务器不受到外部用户的攻击,远程用户访问系统内部服务器时,首先与 SSL VPN 网关建立 HTTPS 连接,由 SSL VPN 网关将访问请求转发给系统内部的网络设备[7]。本文采用 H3C MSR 系列路由器做为 SSL VPN 网关,IP 设置为 192.168.2.1; 为 SSL VPN 网关和远程接入用户颁发证书的 CA (Certificate Authority,认证机构) 地址为 192.168.2.2,CA 建立在内部服务器上。

图1 组网图

Fig.1 The network structure

2 配置 SSL VPN

本文采用 H3C MSR 系列路由器作为 SSL VPN 网关,具体配置包括如下几方面内容:

1) 指定 SSL VPN 服务使用的 SSL 服务器端策略: 管理员和用户对 SSL VPN 网关和内网资源进行管理和访问时,都需要首先通过 HTTPS 登录 SSL VPN 网关的 Web 页面。因此,SSL VPN 网关上需要指定使用的 SSL 服务器端策略,以便确定 SSL VPN 服务使用的 SSL 参数。

2) 指定 SSL VPN 服务使用的 TCP 端口号: SSL VPN 网关作为 HTTPS 服务器为管理员和用户提供 Web 登录页面,可以根据需要指定 HTTPS 服务的 TCP 端口号。

3) 开启 SSL VPN 服务: 只有开启 SSL VPN 服务后,管理员和用户才能通过 Web 页面访问 SSL VPN 网关。

4) 通过 Web 页面对 SSL VPN 进行配置。包括建立域、创建管理员、用户及资源等,同时分配资源及用户权限。

在配置 SSL 服务器端策略时,需要指定其使用的 PKI 域,以便通过该 PKI 域获取服务器端的证书。因此,在进行 SSL 服务器端策略配置之前,需要先配置证书服务器。本文采用微软的 SCEP 来为 PKI 域提供数字证书,建立在一台内部的服务器上。

在配置好证书服务器以后,开始对路由器进行 SSL VPN 的相关配置。具体配置于命令行完成。

配置 PKI 实体。

<Device> system-view

[Device] pki entity en

[Device-pki-entity-en] common-name http-server

[Device-pki-entity-en] quit

配置 PKI 域。

[Device] pki domain sslvpn

[Device-pki-domain-sslvpn] ca identifier ca server

[Device-pki-domain-sslvpn] certificate request url http://192.168.2.2/certsrv/mscep/mscep.dll

[Device-pki-domain-sslvpn] certificate request from ra

[Device-pki-domain-sslvpn] certificate request entity en

[Device-pki-domain-sslvpn] quit

生成本地的 RSA 密钥对。

[Device] public-key local create rsa

获取 CA 的证书。

[Device] pki retrieval-certificate ca domain sslvpn

为 Device 申请证书。

[Device] pki request-certificate domain sslvpn

注: 因为证书是有时效的,所以在获取 CA 证书前应该使路由器与 CA 服务器的时间同步,否则申请不成功。

配置 SSL 服务器端策略。

[Device] ssl server-policy myssl

[Device-ssl-server-policy-myssl] pki-domain sslvpn

[Device-ssl-server-policy-myssl] quit

指定 SSL VPN 服务使用的 SSL 服务器端策略为 myssl,端口号为缺省端口号 443。

[Device] ssl - vpn server - policy myssl
开启 SSL VPN 服务。
[Device] ssl - vpn enable

在配置完成之后,可以对配置结果进行验证。远程接入用户在终端主机 Host 上打开 IE 浏览器,输入网址 https://192.168.2.1/svpn/cn/index.htm,如果可以登录 SSL VPN 网关 Device 的登录页面,则 SSL VPN 成功完成配置。

3SSL VPN 业务资源配置及使用

MSR 系列路由器对 SSL VPN 的业务资源支持是很丰富的,包括 WEB 业务、IP 业务、TCP 业务等。在完成 SSL VPN 配置之后,首先要以超级管理员的身份建立一个新的域,并设定域管理员。然后登陆该域,在该域内建立用户,并为各用户设置权限,分配资源。

在本项目中,需要分配的资源包括卡车 GPS 终端、通讯塔、服务器、无线信号车等网络设备。通讯塔和无线信号车是通过 WEB 页面管理的,可以设置为 WEB 业务资源,其他设备均可以设置为 IP 业务资源。

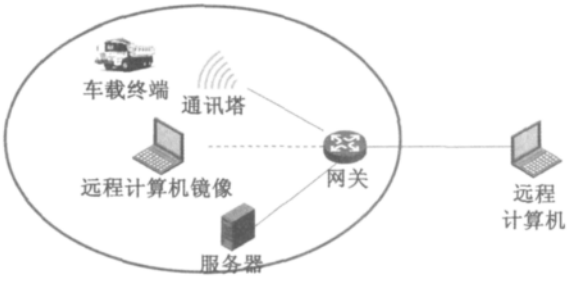

图2 IP业务图示
Fig. 2 The IP service

以用户身份登陆后,使用设置好的资源即可对相应的设备进行远程管理和维护。例如利用远程桌面来管理车载终端,先选择开启 IP 业务,此时远程计算机就拥有了一个系统内部的内网 IP,相当于在内网当中有一个远程计算机的虚拟镜像,远程计算机可以像本地计算机一样对内网的设备进行管理。

利用 Windows 远程桌面连接即可利用远程桌面管理相应的车载终端设备。

4 结束语

在卡车调度系统中,由于交通、天气等因素的限制,对设备的调试和维护带来极大不便。为了方便管理降低维护成本,通常需要远程管理系统中的设备。本文提出的 SSL VPN 是一种方便、安全、低成本的远程接入技术,并且能满足移动办公的需求,使卡车调度系统中的设备管理变得非常方便。

参考文献:

[1] 李锦祥. GPS 技术在卡车调试系统中的应用 [J]. 中国无线电管理, 2002(2): 42 - 44.
[2] 王卫华, 王长杰. 应用原理与安全性分析 [J]. 浪阳职业技术学院学报, 2007, 20(2): 13 - 14.
[3] 吴 冰. 基于 SSL 协议的 VPN 数字图书馆远程访问方案 [D]. 济南: 山东大学, 2008.
[4] 刘广义, 剧海军. MPLS 关键技术研究 [J]. 计算机工程与应用, 2010(4): 27 - 31.
[5] 陈军华, 王忠民. BGP/MPLS VPN 实现原理 [J]. 计算机应用, 2009(23): 18 - 22.
[6] 思科系统(中国)网络技术有限公司. 下一代网络安全 [M]. 北京: 北京邮电大学出版社, 2006.
[7] 代向东, 陈性元, 杜学绘. 基于 PKI 的 VPN 安全管理系统的设计与实现 [J]. 微计算机息, 2006, 22(27): 94 - 96.

(责任编辑 马立)